SECTIGO CERTIFICATE MANAGER
Administrator's Guide

SCMAG

February 2020

Sectigo Certificate Manager

Incommon Administrator's Guide, 20.2 SCMAG

Copyright © 2008, 2019, Sectigo.

All rights reserved.

Primary Author: Liza Rekadze

Contributing Authors: Jordan Clifford

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

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

Table of Contents

Preface

Audience x
Related Documentation x
Conventions x

Understanding SCM

What is SCM? 1
Administrative Roles 1
End-User, Owner, Requester, and Developer Roles 2
Organizations and Departments 2
Certificate Types 3
Reports and Activity Logs 4
Logging Into an SCM Account 4
Understanding the Main SCM UI 6
- The Welcome Window 7
- The Dashboard Overview 7
- The Certificates Configuration Overview 8
- The Network Certificate Discovery Overview 9
- The Code Signing on Demand Overview 10
- The Reports Overview 11
- The Administrator Management Overview 12
- The Settings Overview 14
- Miscellaneous Areas of the SCM UI 16

Understanding the SCM Dashboard

The SCM Dashboard Overview 20
Accessing the Chart Data 22
Filtering Data 22
Understanding Charts 22
- The Expiring Certificates Chart 23
- The DCV Expiring Domains Chart 25
- The Certificate Types (Managed) Chart 26
- The SSL Certificates by Validation Level Chart 27
- The SSL Types Chart 28
- Certificates Requested vs Issued 29
- The Certificates by CA Chart 30
- The Certificate Requests Chart 32
- Certificates by Duration 33
- The DCV Status Chart 34
- The Certificates by Organization Chart 36

The Key Strength Chart 37
The Signature Algorithm Chart 39
Public Key Algorithm 40
CSoD Usage 41
The CSoD Certificates Usage Chart 42

Managing Certificates

Certificate Management Overview 43
Managing SSL Certificates 44
How to Sort and Filter SSL Certificates 49
How to View and Modify SSL Certificate Details 52
Using the Certificate Details Panel 53
Using the Certificate Chain Details Panel 55
Uploading a Certificate Private Key for Storage and Management by the PKS 56
Downloading an SSL Certificate Private Key 59
Resending Notification Email for Issued SSL Certificates 62
Viewing Installation Details of Certificates 63
Restarting Apache Server After Auto-Installation of SSL Certificates 64
Updating the Auto-Renewal Status 64
About Sectigo SSL Certificate Types and Validation Levels 65
How to Request and Issue SSL Certificates to Web Servers and Hosts 67
Using the SSL Certificate Enrollment Form and Built-In Wizard 70
Self-Enrollment Form 70
Bulk Enrollment of SSL Certificates 76
Manual CSR Generation Via the Built-in Enrollment Wizard 89
Automatic CSR Generation Via the Built-in Enrollment Wizard 96
Automatic CSR Generation, Installation, and Renewal of SSL Certificates 102
Automatic CSR Generation in Azure Key Vault 113
Certificate Collection 119
Download and Import of SSL Certificates 121
Approving, Declining, Viewing, and Editing Certificate Requests 121
How to Renew SSL Certificates 122
Certificate Renewal by Administrators 123
Certificate Renewal by End-Users 124
Automatic Certificate Renewal Scheduling 125
How to Revoke, Replace, and Delete SSL Certificates 127
Managing Client Certificates 129
How to Sort and Filter Client Certificates 130
How to Specify the Client Certificate Details 131
How to Add End-Users for Client Certificates 134
Adding End-Users Manually 134
Loading Multiple End-Users from a CSV File 137
Enabling Automatic Creation of End-Users via a Self-Enrollment Form 139
How to Modify End-Users 139
How to Delete End-Users 141
How to Request and Issue Client Certificates to Employees and End-Users 141
Enabling the End-User Self-Enrollment by Access Code 141
Enabling the End-User Self-Enrollment by Secret Identifier 149
Enabling the End-User Enrollment by Invitation 154
How to Revoke Client Certificates 160
How to View the End-User Certificates 161

Managing the Code Signing Certificates 164
How to Sort and Filter Code Signing Certificates 166
How to View the Code Signing Certificates Details 167
How to Add Code Signing Certificates to SCM 170
Adding Code Signing Certificates Manually 170
Loading Multiple Certificates from a CSV File 172
Enabling Automatic Creation of End-Users via Self-Enrollment 174
How to Request and Issue Code Signing Certificates 174
Managing Device Certificates 181
How to Sort and Filter Device Certificates 183
How to View the Device Certificate Details 185
How to Request and Issue Device Certificates 188
Issuing Device Certificates by Proxy CA Through Active Directory 189
Issuing Device Certificates by MS CA Through Active Directory 189
Issuing Device Certificates Through SCEP 192
Issuing Device Certificates Through Self-Enrollment 195
About the Device Certificate Collection 196
Resending the Device Certificate Collection Email 197
Revoking Device Certificates 198

Managing Code Signing Certificates Through CSoD

Overview of the SCM Support for CSoD 200
Configuring Automatic Approval of Code Signing Requests 202
Adding End-Users with a Developer Role 202
Obtaining a Certificate for CSoD 204
Signing Code Using CSoD 209
How to Upload Files for Signing 210
How to Approve a Code Signing Request 212
How to Download Code Signed Files 215

Managing Administrators

Understanding the SCM Administrator Roles 218
The MRAO Role 218
The RAO Role 220
RAO SSL 220
RAO Client Certificate 221
RAO Code Signing 222
RAO Device Certificate 223
The DRAO Role 224
DRAO SSL 224
DRAO Client Certificate 225
DRAO Code Signing 225
DRAO Device Certificate 226
Comparing Security Roles 227
Handling Multiple Security Roles 231
Understanding Administrator Management 232
Sorting and Filtering Administrators 234
Adding Administrators 236
How to add Standard Administrator Accounts 236
How to Add IdP Administrator Accounts 241

Editing and Deleting Administrators 244
Creating IdP User Account Templates 244

Configuring Agents

SCM Agents Overview 249
How to Sort and Filter Agents 250
Configuring Network Agents 252
How to Fulfill Network Agent User Permission Requirements 253
Network Agent Installation Permissions 253
Network Agent Node Discovery and Auto-Installation Permissions 253
How to Fulfill Network Agent Hardware Requirements 254
How to Install a Network Agent 255
How to Configure the Agent for Auto-Installation, Renewal, and Internal Scanning 256
Configuring the Local Controller Mode 257
Configuring Central Controller Mode 259
Configuring the Network Agent for Network Discovery Tasks 263
Configuring MS Agents 266
MS Agent Hardware Requirements 267
How to Install an MS Agent 267
How to Enable Certificate Discovery 271
How to Configure MS AD Certificate Templates for Use With Enroll on Behalf 271
Setting Up MS AD Certificate Templates for Enroll on Behalf 271
Setting Up the CA Properties for Enroll on Behalf 273
Setting Up the Requester Properties for Enroll on Behalf 276
How to Map MS AD Certificate Templates to SCM Certificate Types 277
Viewing Mapped MS AD Certificate Templates 277
Adding MS AD Certificate Template Mapping 278
Modifying an MS AD Certificate Template 282
Deleting MS AD Certificate Templates 283
How to Enable Provisioning of Device Authentication Certificates 284
How to Configure a Standalone MS Agent for Certificate Discovery and Issuance via AD Servers 285
How to Configure Clustered MS Agent for Certificate Discovery and Issuance Via AD Servers 287
How to Enable LDAPS Communication with MS AD 291
Configuring CSoD Agents 292
How to Install a CSoD Agent 292
Setting Up the CSoD Agent in In-House Hosted Mode 294
Setting Up the CSoD Agent in Hosted Mode 297
Installing the Osslsigncode Tool 297
Tuning the Environment 299
In-House Hosted Mode Configuration 300
Cloud Service Mode Configuration 305
Configuring the Private Key Agent 306
How to Install the PKS Agent 307
How to Upload Private Keys 308
How to Download Private Keys 311
How to Back Up and Restore the PKS 314
How to Remove Private Keys from the PKS 316
How to View the Agent Activities 317

Configuring JVM Parameters for Agents 319
How to Modify JVM Parameters on Windows 319
How to Modify JVM Parameters on Linux 319
Configuring Agent HTTP Proxy Servers 320

Configuring Settings

The Settings Configuration Overview 321
Configuring Organizations 323
How to Manage Organizations 327
How to Sort and Filter Organizations 330
How to Create a New Organization 331
Using the General Settings Area of the Add New Organization Dialog 332
Using the EV Details Area of the Add New Organization Dialog 334
Using the Client Certificate Area of the Add New Organization Dialog 336
Customizing Client Certificate Types for an Organization 339
Viewing Preimposed Client Certificate Type Customization for an Organization 343
Using the SSL Certificate Area of the Add New Organization Dialog 344
Customizing SSL Certificate Types for an Organization 349
Restricting the SSL Types and Their Validity Periods 350
Customizing Server Software Types for an Organization 351
Using the Code Signing Certificate Area of the Add New Organization Dialog 353
Using the Device Certificate Area of the Add New Organization Dialog 353
Using the Bulk Import Functionality for Organizations and Departments 355
Preparing the File for Bulk Import 355
Importing JSON Files Into SCM 358
How to Modify an Existing Organization 360
Using the General Settings Area of the Edit Organization Dialog 361
Imposing Access Restrictions to the SCM UI 361
Customizing Notification Email Templates 363
Validating an Organization 363
Managing Departments of an Organization 365
Sorting and Filtering Departments 366
Creating New Departments 367
Configuring Client Certificate Settings for a Department 368
Modifying Departments of an Organization 370
Managing Domains Belonging to a Department 370
Deleting an Existing Department 371
Managing Domains of an Organization 371
Deleting an Existing Organization 372
How to Configure ACME Accounts for Organizations and Departments 373
About the Organization's Validation Status and Server Validation Level in ACME Accounts 381
Configuring Departments 381
Managing and Configuring Domains 382
About Wildcard Domains 384
How to Manage Domains 384
Delegating Domains 385
Sorting and Filtering Domains 386
Using Tool Tips 389
Configuring DCV 389
Sorting and Filtering DCV Status of Domains 391
Creating a New Domain 393

Validating New Domains 395
Delegating and Redelegating Existing Domains 404
Viewing, Validating, and Approving New Domains 405
Approving Creation and Delegation of Domains 408
Viewing Requisition and Approval Details of a Domain 408
Configuring Notifications 410
How to Sort and Filter Notifications 412
How to Add Notifications 413
How to Create Notifications About Expiration of Client Certificates 417
How to Create Notifications About Revocation of Client Certificates 419
How to Create Notifications About the Code Signing Certificate Download 421
How to Create Notifications About Revocation of Code Signing Certificates 423
How to Create Notifications About Expiration of Code Signing Certificates 425
How to Create Notifications About a Request for a Code Signing Certificate 427
How to Create Notifications About the SSL Certificate Approval 429
How to Create Notifications About the SSL Certificate Waiting for Approval 431
How to Create Notifications About a Declined Request for an SSL Certificate 433
How to Create Notifications About Expiration of SSL Certificates 435
How to Create Notifications About Failed Attempts to Issue SSL Certificates 437
How to Create Notifications About Revocation of an SSL Certificate 439
How to Create Notifications that Summarize Results of a Discovery Scan 441
How to Create Notifications About a Remote Installation of an SSL Certificate 443
How to Create Notifications About Failed Attempts to Install SSL Certificates Remotely 445
How to Create Notifications About a Failure to Install or Renew an SSL Certificate Automatically 447
How to Create Notifications About an SSL Certificate Ready for Manual Installation 449
How to Create Notifications About Expiration of Device Certificates 451
How to Create Notifications About Revocation of Device Certificates 453
How to Create Notifications About Device Certificates Waiting for Approval 455
How to Create Notifications About Creation of a New Client Administrator 457
How to Create Notifications About a Domain Waiting for Approval 459
How to Create Notifications About Approval of a Domain 461
How to Create Notifications About a DCV Expiration 463
How to Create Notifications About Completion of DCV 465
How to Create Notifications About DCV Required for a New Domain 467
How to Create Notifications About a New Request for a CSoD Certificate 469
How to Create Notifications About Revocation of a CSoD Certificate 471
How to Create Notifications About Successful Certificate Enrollment 472
Configuring Key Escrow and Encryption 473
How to Configure Key Escrow for an Organization 474
How to Configure Key Escrow for a Department 475
About the Master Keys Requirements for the Client Certificate Issuance 476
How to View and Configure Encryption Settings 477
How to Encrypt Private Keys 478
How to Re-Encrypt Private Keys 479
How to Recover an End-User's Private Key from Escrow 483
Configuring Access Control 484
How to Add a New IP Range 486
How to Modify and Delete an IP Range 488
Configuring a Private Key Store 489
Configuring Certificates 489

How to Configure SSL Certificate Types 489
Customizing SSL Certificate Types 490
How to Configure Client Certificate Types 492
Customizing Client Certificate Types 495
How to Configure Device Certificate Types 496
Adding Device Certificate Types 498
Modifying and Deleting a Device Certificate Type 499
How to Define Custom Fields 501
Adding a New Custom Field 502
Modifying an Existing Custom Field 504
Removing an Existing Custom Field 505
Configuring Templates 506
How to Set Up Email Templates 506
Modifying Email Templates 507
How to Set Up Self Enrollment Custom Text and Links 508
Managing SCM Agents 509
Defining Auto-Assignment Rules for External Certificates 509
Configuring SCM for Microsoft Intune 514
Configuring the Azure Key Vault Integration 514

Performing Certificate Discovery Tasks

Certificate Discovery Tasks Overview 525
Evaluating Network Assets 526
How to View Certificate Information Via Network Discovery 527
Manually Assigning a Certificate to Organizations and Departments 534
Generating a Report on Discovered Certificates 535
How to View the Web Server Information 536
How to View Certificates Via Active Directory 538
Performing Network Discovery Tasks 540
How to Add IP Ranges and Perform Scans 544
How to Modify a Discovery Task 552
How to Import Multiple Network Discovery Tasks from a CSV File 553
How to Delete a Discovery Task 553
How to View History of Network Discovery Tasks 554
How to View Scan Results 557
Performing the AD Discovery Tasks 560
How to Add Domains and Start Scans 562
How to Modify AD Discovery Tasks 567
How to Delete AD Discovery Tasks 568
How to View History of AD Discovery Tasks 568
How to View Results of AD Discovery Scan Tasks 572
How to Sort and Filter MS AD Discovery Tasks 573

Generating Reports

SCM Reports Overview 575
Generating Activity Log Reports 580
Generating Client Certificates Reports 580
Generating Discovery Scan Log Reports 582
How to Generate a Summary Report 582
How to Generate a Detailed Report 583

Generating SSL Certificates Reports 585
Generating Code Signing Certificates Reports 587
Generating Code Signing Requests Reports 589
Generating Administrators Reports 591
Generating XML Data Reports 591
Generating DCV Reports 591
Generating Agent Log Events Reports 593
Generating Notification Log Statistics Reports 593
How to Generate Email Reports 593
How to Generate Notification Type Reports 594
How to Generate Full Log Reports 595
Generating Private Key Agent Activity Log Reports 596
Generating Network Discovery Tasks Reports 596
Generating Device Certificate Reports 597

Using SCM with Microsoft Intune

Microsoft Intune Configuration Overview 599
Configuring SCEP 599
How to Register the Application 600
How to Determine the Tenant Name 600
How to Create Trusted Certificate Profiles 601
How to Create a SCEP Profile 601
How to Authenticate SCM to Microsoft Azure 603
Issues and Limitations Related to Different Platforms 604
Configuring Intune Export 605

Configuring and Testing the Sectigo EST Service

Configuring Sectigo EST Service 612
How to Create an Adapter 612
How to Create a Template 614
Testing Enrollments 615
How to Install Dependencies on Windows 615
How to Install Dependencies on Linux 615
How to Perform Basic Validation 616
How to Perform Enrollment 616

Using the Sectigo ACME Service

Sectigo ACME Service Overview 618
ACME Clients Overview 619
ACME Server URLs 619
How to Use Certbot 619

Performing Miscellaneous Tasks

Accessing the Product Version and Feature Details 624
Accessing and Editing the User Profile 625
Logging Out of SCM 627
Deprecation of Private Certificates for Internal Hosts 627
Responsibilities Associated with Ordering SSL Certificates 628

Integrating IdP for Single Sign-On 628
Troubleshooting SSO Connections 629

Appendix A Email Notification Templates

Email Template Variables A-1

Appendix B CSV Import Format Requirements

Network Discovery Task CSV File Format B-1
Adding Multiple Assignment Rules B-2
End-User CSV File Format and Importing Guidelines B-3
Code Signing Certificate CSV File Format and Importing Guidelines B-5

Appendix C Sectigo Root and Intermediate Certificates

Sectigo Root and Intermediate Certificate(s) C-1
Importing the Sectigo Root Certificate C-1
Importing the Sectigo Intermediate Certificate C-2

Preface

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 the administrator security role.

Audience

Sectigo Certificate Manager Administrator's Guide is intended for customer 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 lifecycle management of web server, client, code signing, and device authentication certificates through a unified interface.

This chapter describes the following topics:

- What is SCM?
- Administrative Roles
- End-User, Owner, Requester, and Developer Roles
- Organizations and Departments
- Certificate Types
- Reports and Activity Logs
- Logging Into an SCM Account
- Understanding the Main SCM UI

1.1 What is SCM?

SCM enables nominated administrators to manage the lifespan, issuance, deployment, renewal, and revocation of certificates on an organization, department, and per-user 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.

1.2 Administrative Roles

There are three primary administrator roles in SCM:

- **Master Registration Authority Officer (MRAO)**—The highest level administrator in SCM. MRAOs have access to all functional areas and may delegate control over the certificates, domains, and notifications of any organization or department. They have full rights over the creation and privileges of Registration Authority Officers, Department Registration Authority Officers, and end-users of any organization and department.
- **Registration Authority Officer (RAO)**—RAOs are created by a MRAO to manage the certificates and end-users of specific SCM organizations. RAOs have control over certificates that are ordered on behalf of their organizations. They also have control over domains and users that have been delegated to their organization or department. RAOs can create peer RAOs for their organizations. They can edit or remove RAOs of their organization if appropriate privileges have been assigned to them by a MRAO. For more information o n the various RAO roles, see "RAO SSL" on page 220, "RAO Client Certificate" on page 221, "RAO Code Signing" on page 222, "RAO Device Certificate" on page 223.

- **Department Registration Authority Officer (DRAO)**—DRAOs are created by, and subordinate to the RAO. DRAOs are assigned control over certificates, users, and domains belonging to departments of organizations. DRAOs can create peer DRAOs for their departments. They can edit or remove DRAOs of their department if appropriate privileges have been assigned to them by an MRAO or RAO. For more information on the various DRAO roles, see "DRAO SSL" on page 224, "DRAO Client Certificate" on page 225, "DRAO Code Signing" on page 225, "DRAO Device Certificate" on page 226.

1.3 End-User, Owner, Requester, and Developer Roles

In the context of SCM, End-Users, Owners, Requesters, and Developers are defined as follows:

- **End-User**—A person that has been issued with a client[1] certificate or requested a client certificate or has made an application for an SSL certificate using the self-enrollment form. End-users cannot access SCM; they exist in SCM only as a function of their request for or ownership of a client certificate. A new End-User and the client certificate for that end-user can be created in SCM as follows:
  - Manually by an administrator in the **Client Certificate** area of the SCM UI.
  - When the end-user orders a client certificate using the self-enrollment form.
  - When the end-user is imported into SCM from a `.csv` file.

  For more information, see "Managing Client Certificates" on page 129.

  A new end-user can also be added via SSL certificate applications made through the self-enrollment form. If the applicant does not already exist as an end-user, SCM automatically adds this applicant when the form is submitted. End-users that are created automatically in this way cannot have a client certificate.

  All end-users and client certificates owned or requested by each end-user are listed in the **Client Certificates** area of SCM UI.
- **Owner** of the certificate—An administrator who first approved the request for the certificate. Therefore, the privileges of the Owner depend on the administrator's role.
- **Requester** of the certificate—Someone who created and successfully submitted the initial application for the certificate. Any class of administrator or end-user can be a requester. SSL certificates and client certificates can be requested by individuals that do not yet exist in SCM as either end-users or administrators if they applied using the self-enrollment or external application forms.
- **Developer**—Someone who can use the CSoD service to sign the executables and script files. This is applicable only if the SCM CSoD feature is enabled for the account. SCM can store the issued code signing certificate and use it for signing code files uploaded by the developer who can then download the signed file from SCM. A new user can be added as a developer. In addition, an existing end-user can be assigned the developer role.

1.4 Organizations and Departments

Organizations and departments are created by administrators for the purpose of requesting, issuing, and managing certificates for domains and employees. For more information, see "How to Create a New Organization" on page 331.

1. Client certificates are also known as S/MIME certificates.

Each organization can have multiple departments. Organizations are typically managed by a RAO, while departments are typically managed by a DRAO. A MRAO can manage all organizations and all departments.

Once an organization or department has been created, the following may occur:

- MRAOs can create new or assign existing RAOs to manage that organization.
- MRAOs can initiate the process of validating organizations for the purpose of requesting and issuance of OV SSL certificates to organizations and departments under these MRAOs.
- MRAOs and RAOs can create multiple departments within that organization. For more information, see "Configuring Organizations" on page 323.
- MRAOs can create new or assign existing RAOs to manage individual departments.
- MRAOs can delegate domains to an organization or department.
- RAOs and DRAOs can directly request that certificates be issued to domains which have been delegated to their organizations and departments. These administrators can also approve and decline certificate requests from individuals using the external application form.
- End-users can be assigned membership of an organization or department and provisioned with client certificates for the domain that is associated with that organization or department.
- Administrators can manage the client certificates of end-users belonging to an organization or department via the **Client Certificates** area of the SCM UI and can manage SSL certificates for the organization via the **SSL Certificates** area. Code signing certificates are managed from the **Code Signing** area.
- If enabled, MRAOs and RAOs SSL can create and modify ACME accounts for organizations and departments; DRAOs SSL can create and modify ACME accounts for their delegated departments.
- A wide range of organization-specific 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.
- MRAOs, RAOs, and DRAOs can utilize the Certificate Discovery feature to audit, and then monitor all existing certificates on the network by assigning them to either an organization or one of its departments.
- Certificate reports and activity logs can be viewed and exported for that organization and specific department.

1.5 Certificate Types

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 users to confirm 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 (VPN).

1.6 Reports and Activity Logs

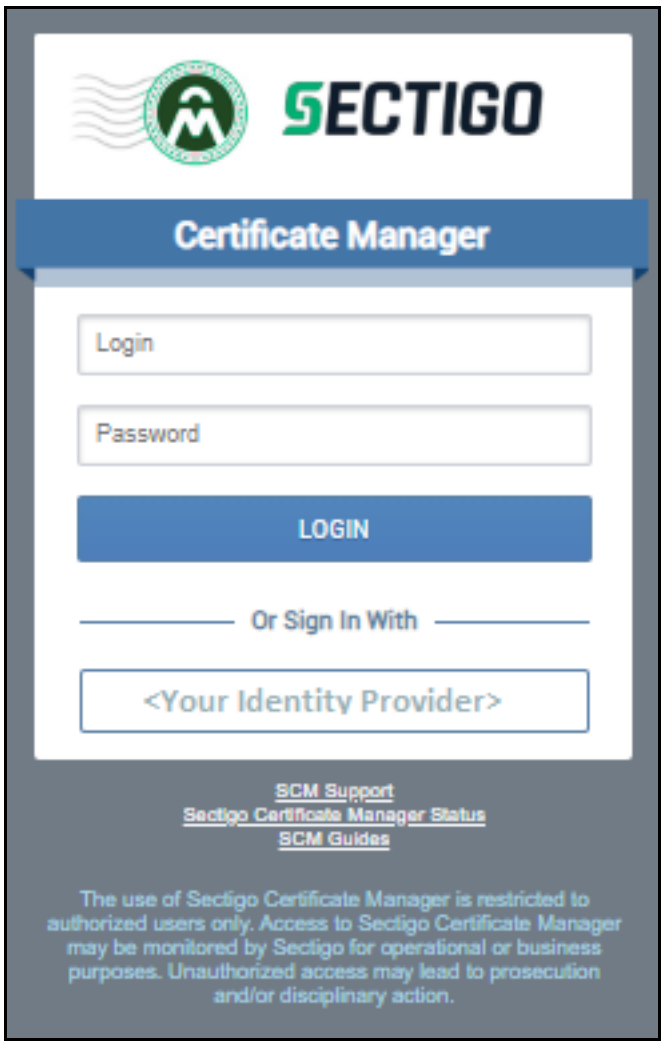
Reports on various SCM artifacts and activities can be viewed and exported for an organization and department via the **Reports** area of the SCM UI. You can view reports depending on your security role. The following types of reports are available:

- **Activity Log** reports enable MRAOs to view all actions that have occurred within the interface within specific time periods.
- **SSL Certificates** reports enable MRAOs and RAOs SSL, and DRAOs SSL to monitor all statistics related to SSL certificates including usage, ownership, issuance, provisioning, and status.
- **Discovery Scan Log** reports enable MRAOs, RAOs SSL, and DRAOs SSL to view the discovery scan log. A discovery scan is an audit of all SSL certificates installed on your network.
- **Client Certificates** reports enable MRAOs, RAOs Client Certificate, and DRAOs Client Certificate to monitor all statistics related to client certificates including usage, ownership, issuance, provisioning, and status.
- **Code Signing Certificates** reports enable MRAOs, RAOs Code Signing, and DRAOs Code Signing to monitor all statistics related to code signing certificates including usage, ownership, issuance, provisioning, and status.
- **Admin** reports enable MRAOs to view details of the enrolled administrators of all privilege levels.
- **XML Data** reports enable MRAOs to view details of all organizations, departments, their administrators, and all the certificates in XML format.
- **DCV** reports enable MRAO, RAOs SSL, and DRAOs SSL to view details on all of their registered domains, including DCV statuses and expiration dates.
- **Notification Log Statistics** reports enable MRAOs to view details of the notifications emails sent to RAOs and DRAOs for various SCM events.
- **Private Key Agent Activity Log** reports enable MRAOs to monitor actions executed by the private key agent installed on the local network.
- **Discovery Tasks** reports enable MRAOs, RAOs, and DRAOs to view discovery tasks configured for their organizations and departments.
- **Device Certificates** reports enable MRAOs, RAOs Device Certificate, and DRAOs Device Certificate to monitor all statistics related to device certificates, including key usage, ownership, issuance, provisioning, and status.

1.7 Logging Into an SCM Account

You can access SCM through your organization's unique SCM URL. By default, the format of this URL is `https://cert-manager.com/customer/<customerurl>/`. It allows you to enter the SCM credentials provided by your account manager or, if configured for your organization, log in using an Identity Provider (IdP) for single sign-on functionality.

To log in using an IdP, your IdP must be integrated with the SCM server and then associated with your SCM account.



To log in using SCM credentials, navigate to your SCM account login page, enter the credentials, and then click **LOGIN**, as shown in the preceding illustration.

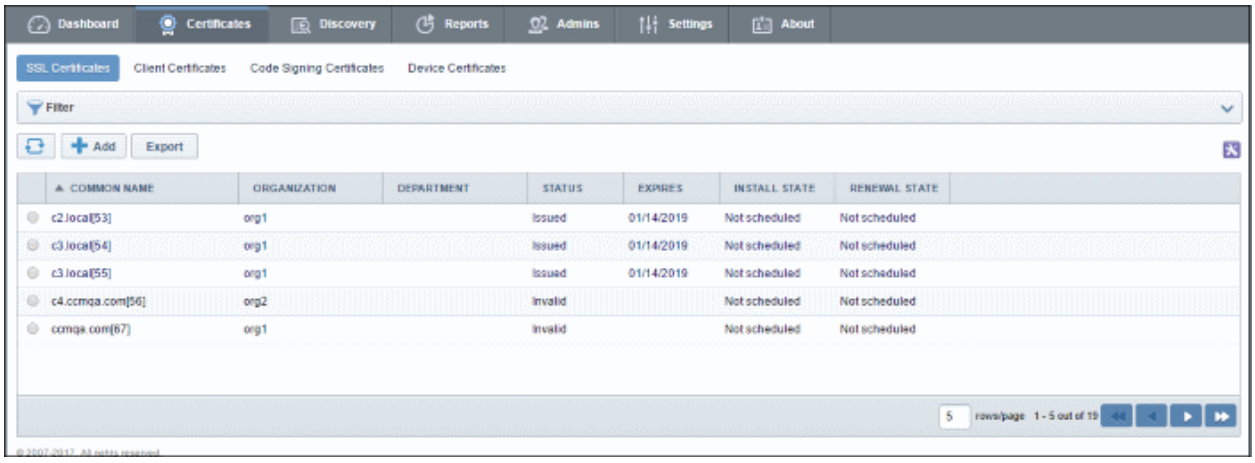
Depending on how your account was set up, you may be prompted to change your password after the first login. You can also change your password at any time using the **My Profile** area of the SCM UI (see "Miscellaneous Areas of the SCM UI" on page 16).

To log into SCM using IdP credentials, navigate to your SCM account login page, click the link to your IdP login page, and then enter your SSO credentials.

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.

1.8 Understanding the Main SCM UI

The SCM UI has a tab structure which provides access to most of the settings, as shown in the following illustration.



The main functional areas of SCM are presented as a series of seven (or fewer, depending on your permissions level) tabs: **Dashboard**, **Certificates**, **Discovery**, **Code Signing on Demand**, **Reports**, **Admins**, **Settings**, and **About**.

The **Certificates** tab contains subsections for managing the certificate types that have been enabled for your company, with a maximum of four subsections available: **SSL Certificates**, **Client Certificates**, **Code Signing Certificates**, and **Device Certificates**. For more information, see "The Certificates Configuration Overview" on page 8.

The **Discovery** tab allows you to set up scans to discover existing certificates on your network. The **Discovery** tab has three subsections: **Network Assets**, **Network Discovery Tasks**, and **MS AD Discovery Tasks**. For more information, see "The Network Certificate Discovery Overview" on page 9.

The **Code Signing on Demand** tab is displayed only if the CSoD feature is enabled for your account. This tab contains two subsections—**Requests** and **Developers**—which allow you to configure CSoD, add and manage developers, as well as approve or reject code signing requests from developers. "The Code Signing on Demand Overview" on page 10.

The **Settings** tab contains subsections for **Organizations**, **Domains**, **Notifications**, **Encryption**, **Access Control**, **Private Key Store**, **Templates**, **Certificates**, **Agents**, **Assignment Rules**, and **Intune**. For more information, see "The Settings Overview" on page 14.

The **Reports** tab contains subsections for generating reports for activity log, client certificates, discovery scan log, SSL certificates, code signing certificates, code signing requests, administrators, XML data, DCV report, agent log events, notification log statistics, private key agent, network discovery tasks, and device certificates. For more information, see "The Reports Overview" on page 11.

The **Admins** tab allows you to create, manage, and modify permissions for new and existing administrators. For more information, see "The Administrator Management Overview" on page 12.

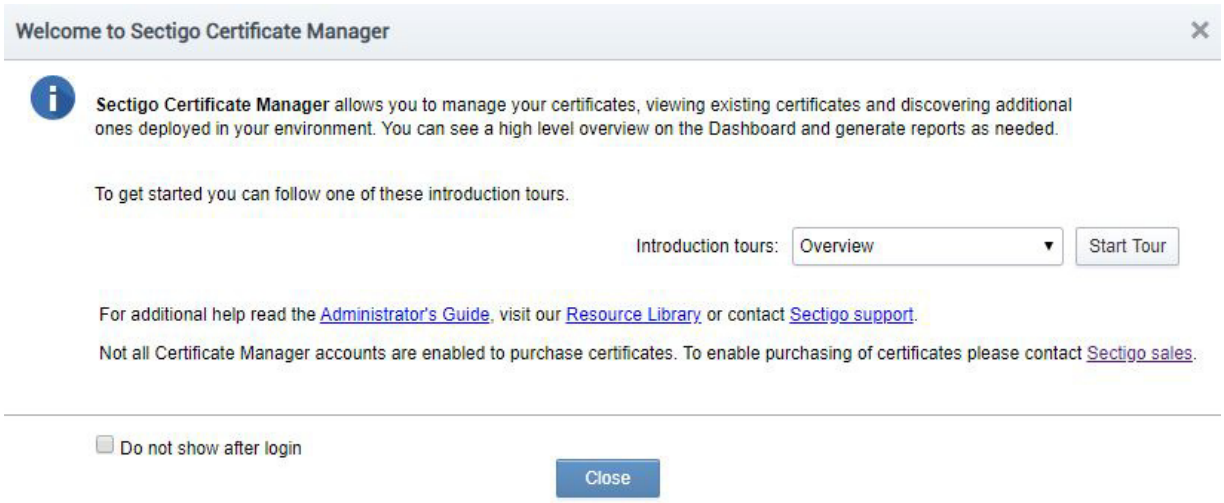
The **About** tab allows you to view the version of SCM you are using, as well as the features that are enabled and disabled for the account. For more information, see "Miscellaneous Areas of the SCM UI" on page 16.

You can access additional resources via the **Welcome** dialog by clicking the **Help** icon located at the top right corner of the SCM UI. For more information, see "The Welcome Window" on page 7.

1.8.1 The Welcome Window

When you first access SCM, you may be presented with the **Welcome** dialog shown in the following illustration. This dialog provides links to the following resources:

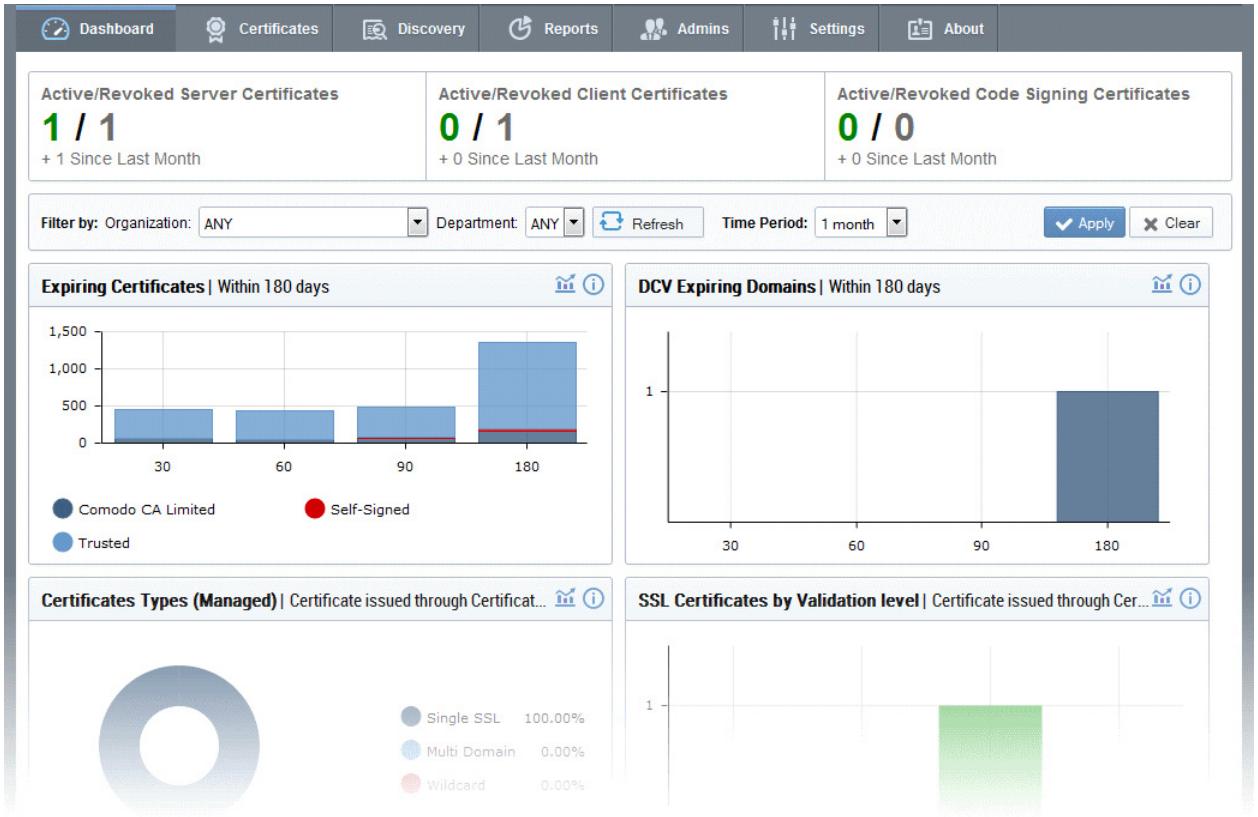
- The introduction tour
- SCM Administrator's Guide
- The resource library
- Sectigo support



You can launch the Welcome dialog at any time later by clicking the SCM **Help** icon.

1.8.2 The Dashboard Overview

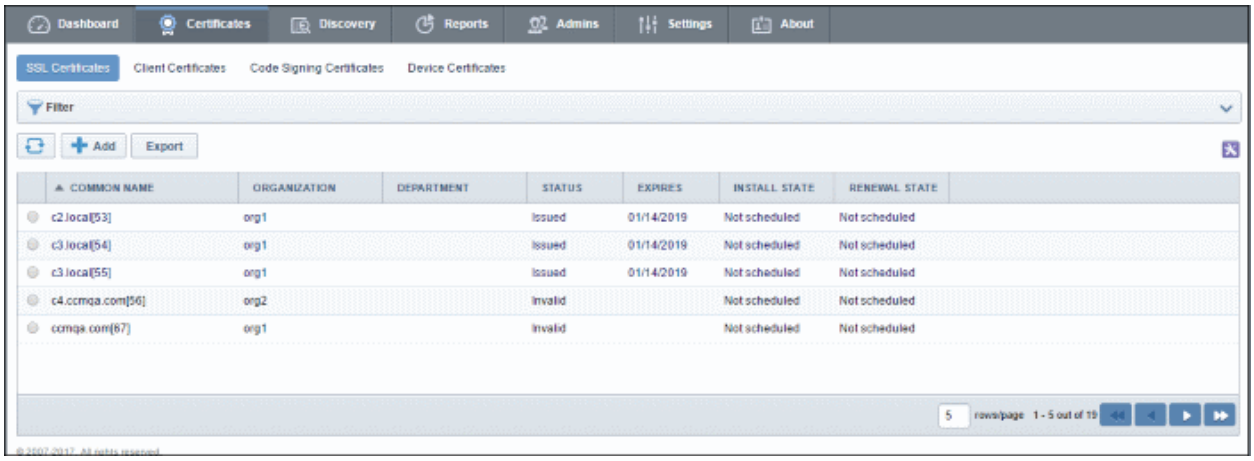
The **Dashboard** area of the SCM UI, as shown in the following illustration, contains charts that visualize data on the certificates on your network, such as certificates approaching expiry, issued and requested certificates, DCV status, breakdown of certificates by types, issuers, and so on.



For more information, see "Understanding the SCM Dashboard" on page 20.

1.8.3 The Certificates Configuration Overview

The **Certificates** area shown in the following illustration allows you to manage different types of certificates.



The availability of the certificate management actions depends on your security role, as follows:

- **MRAOs** can access all areas and functionality of the section and have full visibility and control over all types of certificates.
- **RAOs SSL** can access all areas and functionality of the **SSL Certificates** section. In addition, a RAO SSL can view and manage SSL certificates belonging to organizations delegated to these administrators.
- **RAOs Client Certificate** can access all areas and functionality of the **Client Certificates** section. In addition, a RAO Client Certificate can view and manage client certificates and end-users belonging to organizations delegated to these administrators.
- **RAOs Code Signing** can access all areas and functionality of the **Code Signing Certificates** section. In addition, a RAO Code Signing can view and manage code signing certificates issued to end-users belonging to organizations delegated to these administrators.
- **RAOs Device Certificate** can access all areas and functionality of the **Device Certificates** section. In addition, a RAO Device Certificate can view and manage device certificates issued to devices and endpoints belonging to organizations delegated to these administrators.
- **DRAOs SSL** can access all areas and functionality of the **SSL Certificates** section. In addition, a RAO SSL can view and manage SSL certificates belonging to departments delegated to these administrators.
- **DRAOs Client Certificate** can access all areas and functionality of the **Client Certificates** section. In addition, a DRAO Client Certificate can view and manage client certificates and end-users belonging to departments delegated to these administrators.
- **DRAOs Code Signing** can access all areas and functionality of the **Code Signing Certificates** section. In addition, a DRAO Code Signing can view and manage code signing certificates issued to end-users belonging to departments delegated to these administrators.
- **DRAOs Device Certificate** can access all areas and functionality of the **Device Certificates** section. In addition, a DRAO Device Certificate can view and manage device certificates issued to devices and endpoints belonging to departments delegated to these administrators.

For more information, see "Managing Certificates" on page 43.

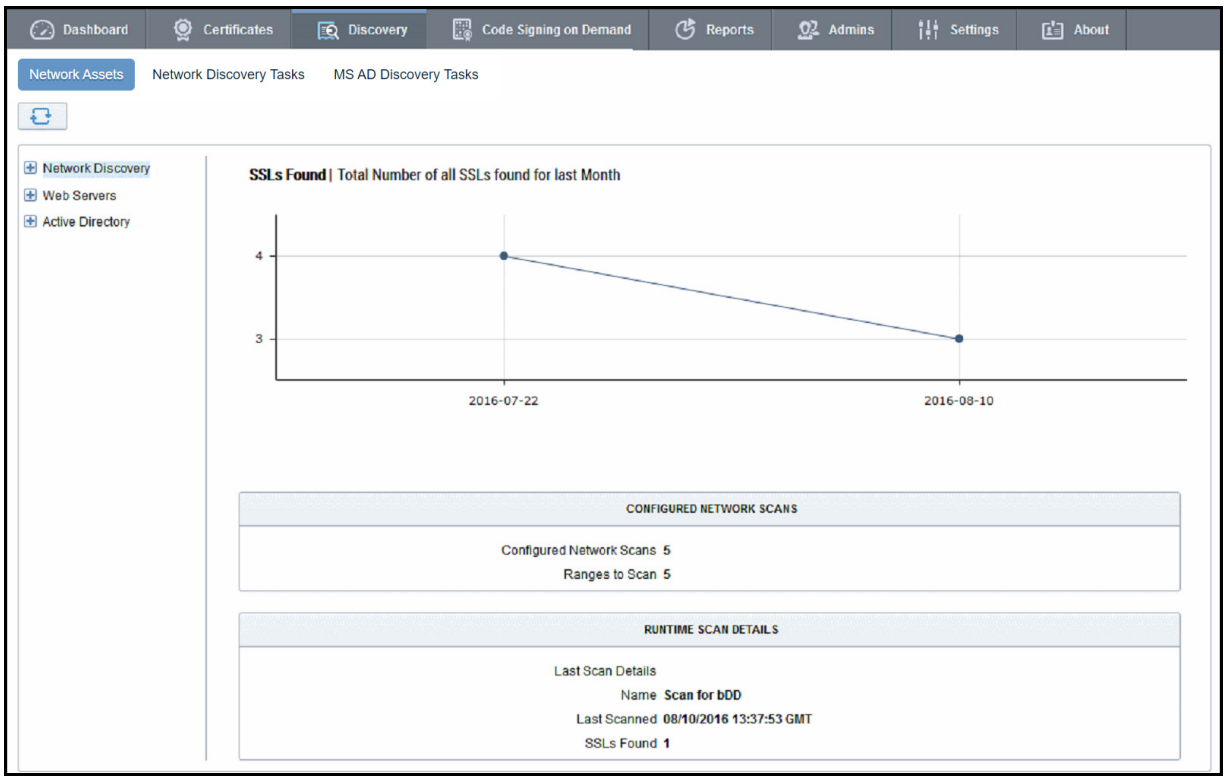
1.8.4 The Network Certificate Discovery Overview

The **Discovery** area shown in the following illustration allows you to perform the network certificate discovery tasks. To use this functionality, you have to install a Network Agent—a software that identifies certificates on your network and auto-installs SSL certificates.

The **Discovery** area is structured as follows:

- The **Network Discovery Tasks** area allows you to configure Network Agents for the network and to commence certificate discovery tasks.
- The **MS AD Discovery Tasks** area allows you to scan for all types of certificates on objects in an AD server.
- The **Network Assets** area displays the discovery scan results which include the following:
  - Managed certificates that have been issued through SCM.
  - External (also known as unmanaged) certificates that either (1) have been acquired from other CAs; (2) are Sectigo certificates obtained through channels other than SCM; (3) self-signed certificates. You can assign external certificates to an organization or department to bring them under the SCM management.

  In addition, the **Network Assets** area displays web servers and domains found on scanned networks. If AD servers have been integrated with SCM, then the area would also show all certificates found by scans run on AD servers.



The **Discovery** area is accessible only by MRAO, RAO SSL, and DRAO SSL administrators. The availability of the discovery actions depends on your security role, as follows:

- **MRAOs** can set up agents and run certificate scans on any organization or department. **MRAOs** can operate in the in-house hosted mode (see "The Code Signing on Demand Overview" on page 10).
- **RAOs SSL** can set up agents and run certificate scans on organizations that have been delegated to them. **RAOs SSL** can also run scans on departments of those organizations.
- **DRAOs SSL** can set up agents and run certificate scans on departments that have been delegated to them.

For more information, see "Performing Certificate Discovery Tasks" on page 525.

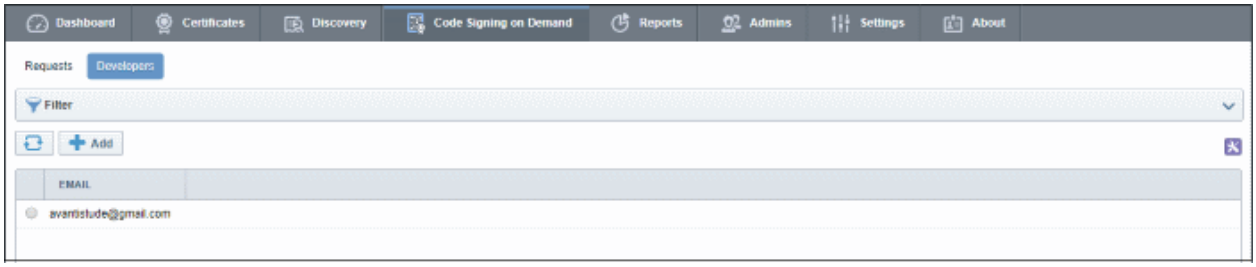
1.8.5 The Code Signing on Demand Overview

The **Code Signing on Demand** area shown in the following illustration is visible only if this feature is enabled for your account.

The CSoD service is available in the following two modes:

- **In-House Hosted** mode allows developers to upload software to a local portal. The code signing process is handled by a locally-installed agent that generates CSoD-enabled code signing certificates which developers can use to sign files. The certificates and their private keys are stored in encrypted form in a local database created by the agent. The following deployment types are available in hosted mode:
  - Standard deployment, when the CSoD Agent is installed on a single machine. The use of a hardware security module (HSM) is optional.

    - Clustered deployment, when CSoD Agents are installed on multiple servers for redundancy. The use of HSM and network file sharing is mandatory.
- **Cloud Service** mode provides the signing service that is hosted on Sectigo's secure cloud servers. The service generates CSoD-enabled code signing certificates for developers to sign files. The certificates and their private keys are generated and stored in encrypted format in Sectigo's data center for the lifetime of the certificate, tightly protected by Sectigo's military grade security infrastructure.



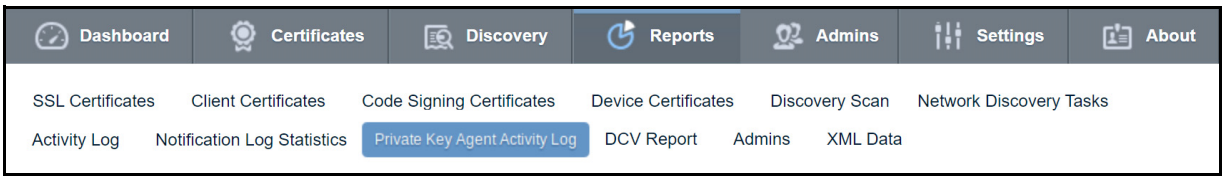
The **Code Signing on Demand** area is accessible only by MRAOs, RAOs Code Signing, and DRAOs Code Signing. The availability of the actions depends on your security role, as follows:

- MRAOs:
    - In the **In-House Hosted** mode, a MRAO can set up and configure CSoD agents on the local network, add and manage developers for any organization and department, as well as approve code signing requests from developers pertaining to any organization and department.
    - In the **Cloud Service** mode, a MRAO can add and manage developers for any organization and department, as well as approve code signing requests from developers pertaining to any organization and department.
- RAOs Code Signing can add and manage developers for any organizations and subordinate departments that have been delegated to these administrators. RAOs Code Signing can also approve code signing requests from developers pertaining to organizations and subordinate departments that have been delegated to these RAOs.
- DRAOs Code Signing can add and manage developers only for the departments that have been delegated to these administrators. DRAOs Code Signing can approve code signing requests only from developers pertaining to departments that have been delegated to these DRAOs.

For more information, see "Managing Code Signing Certificates Through CSoD" on page 200.

1.8.6 The Reports Overview

The **Reports** area shown in the following illustration allows you to view a variety of reports depending on your privilege level.



The availability of the reports depends on your security role, as follows:

MRAOs can view all types of reports for all organizations and departments.

RAOs SSL can view the following:

- Certificate discovery reports on scans that have been run on behalf of their delegated organizations and departments.
- SSL certificate reports appropriate for their organizations and departments.
- DCV report and discovery tasks reports for their delegated organizations and departments.

RAOs Client Certificate can view client certificates reports for their organizations and departments.

RAOs Code Signing can view the following:

- Code signing certificate report for their organizations and departments.
- Code signing requests reports for their organizations and departments.

RAOs Device Certificate can view device certificates reports for their organizations and departments.

DRAOs SSL can view the following:

- Certificate discovery reports on scans that have been run on behalf of their delegated departments.
- SSL certificate reports appropriate for their departments.
- DCV report and Discovery Tasks reports for their delegated departments.

DRAOs Client Certificate can view client certificates reports for their departments.

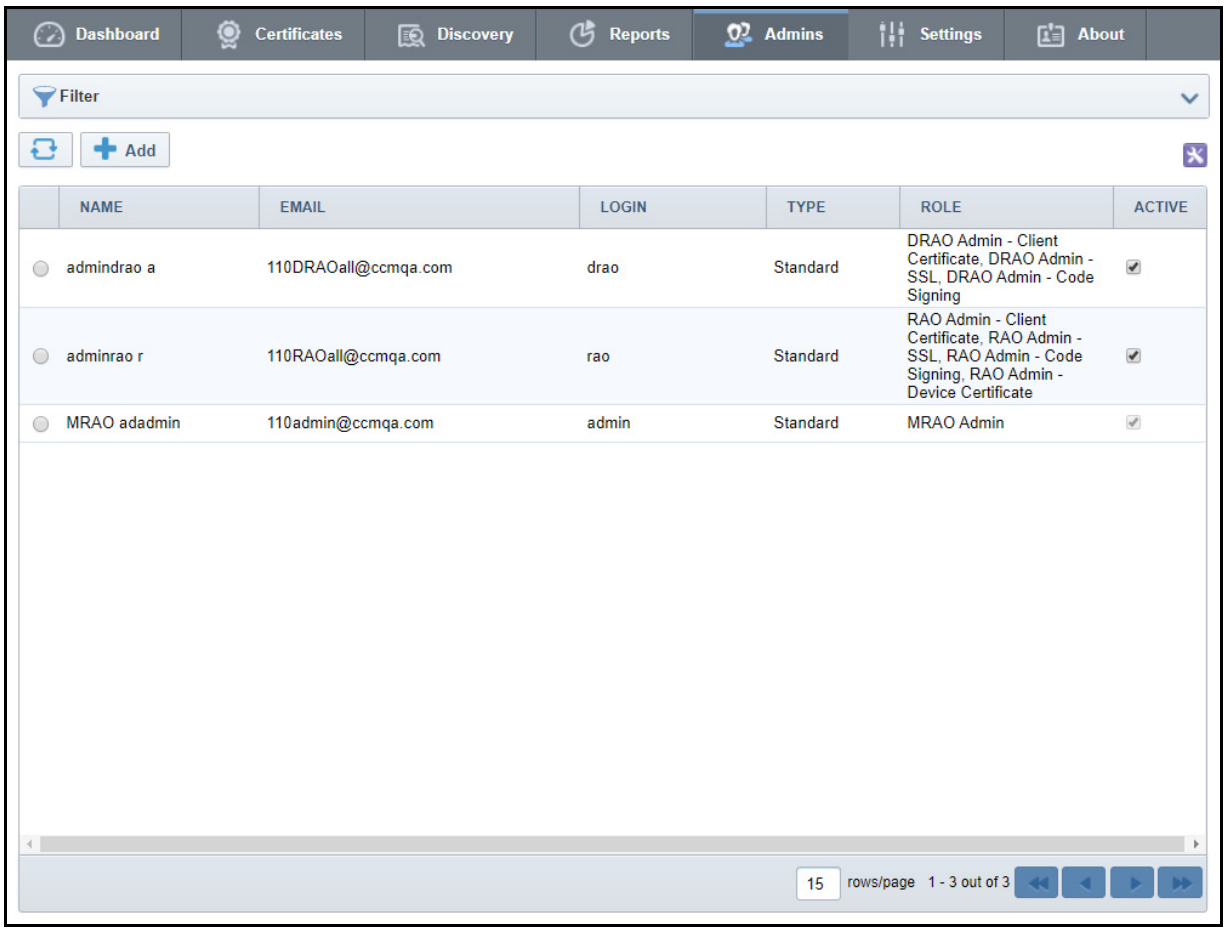
DRAOs Code Signing can view the following:

- Code signing certificate reports for their departments.
- Code signing requests reports for their departments.

DRAOs Device Certificate can view device certificates reports for their departments.

1.8.7 The Administrator Management Overview

The **Admins** area shown in the following illustration allows the administrator to view a list of administrative personnel. The contents of the list and availability of controls depend on your privilege level.



MRAOs have full visibility of all administrators across every organization and department and can perform the following actions on administrators of any class or type:

- View
- Add
- Delete
- Edit
- Approve
- Reject
- Activate
- Deactivate

RAOs SSL, RAOs Client Certificate, RAOs Code Signing, and RAOs Device Certificate can perform the following actions:

- View RAOs and DRAOs of their delegated organizations and any subordinate departments who are responsible for the same certificate types as themselves.
- Edit RAOs and DRAOs of their delegated organizations and any subordinate departments who are responsible for the same certificate types as themselves.
- Request the creation of fellow RAOs who are responsible for the same certificate types as themselves.

- Approve the creation of DRAOs who are responsible for the same certificate types as themselves.
- Reject the creation of DRAOs who are responsible for the same certificate types as themselves.

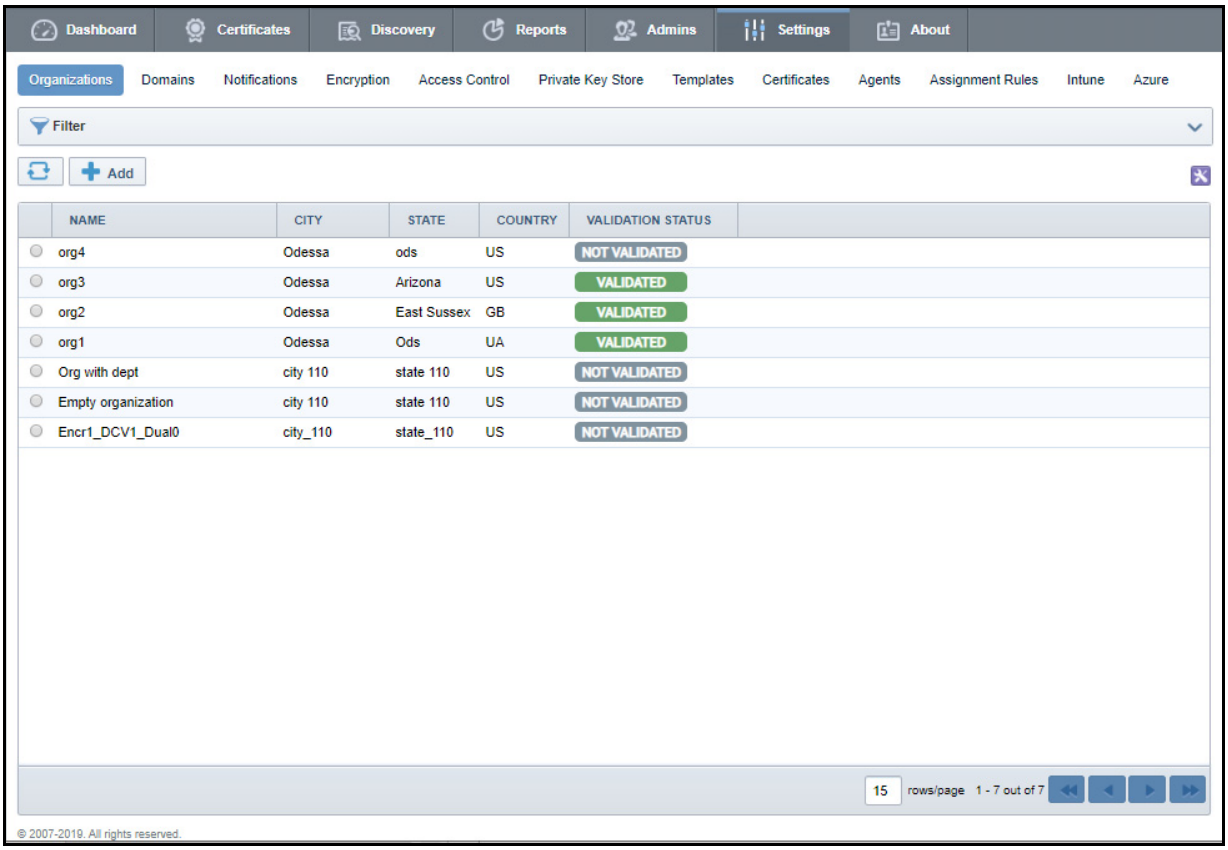
DRAOs SSL, DRAOs Client Certificate, DRAOs Code Signing, and DRAOs Device Certificate can perform the following actions:

- View DRAOs of their delegated departments who are responsible for the same certificate types as themselves.
- Request the creation of fellow DRAOs who are responsible for the same certificate types as themselves.
- Edit their own details.

For more information, see "Managing Administrators" on page 218.

1.8.8 The Settings Overview

The **Settings** area shown in the following illustration is related to the general configuration of SCM. The number of tabs that are visible depends on your security role level.



The **Organizations** area is visible to MRAOs and RAOs, as follows:

- RAOs can view, edit, request new domains, and add departments to organizations that have been delegated to these administrators.

- MRAOs can view, edit, request new domains, create new departments, and delete any organization or department.
- MRAOs can initiate organization validation. After passing validation, administrators can apply for certificates for the organization and department.

The **Departments** area is visible to DRAOs who see a **Departments** area instead of the **Organizations** area. The **Departments** area allows DRAOs to view all departments that have been delegated to them and to request new domains for those departments.

The **Domains** area is visible to MRAOs who can view all domains that have been requested or created. MRAOs can also submit domain requests for validation, select the validation method, activate, deactivate, edit domains, and delegate a domain to any organization or department. RAOs can view domains for organization that they control, can delegate domains to subordinate departments, and can request new domains for their organization. DRAOs can view existing domains and request the addition of new ones.

The **Notifications** area allows you to set up and manage email notifications sent to various personnel, including notifications triggered by the SSL certificate status, by the client certificate status, and by discovery scan summaries.

The **Encryption** area allows you to initialize a new master key pair or to re-encrypt the private keys of client certificates held in escrow.

The **Access Control** area allows MRAOs to grant access to the SCM login page only for the specified IP range.

The **Private Key Store** area allows MRAOs to configure backup of the private keys of SSL certificates.

The **Templates** area enables MRAOs to add custom links and text to self-enrollment pages through the **Enrollment Form** tab. On the **Email Templates** tab, MRAOs and RAOs can customize the contents of templates for event-based email notifications. DRAOs can edit templates for their department via the **Edit Department** dialog accessible by navigating to **Settings > Departments**, and then clicking **Edit**.

The **Certificates** area allows MRAOs to customize the types and validity periods of SSL and client certificates available through the built-in application form and self-enrollment form. In addition to the standard fields that appear in the built-in application form and self-enrollment form, MRAOs can configure to add custom fields in these forms.

The **Agents** area enables installation of the following SCM agents for the certificate discovery, auto-installation, and code signing-on-demand services:

- Network Agents for Certificate Discovery and Auto-Installation scan for certificates on network servers and configure certificate auto-installation.
- MS Agents for AD Server Integration install the MS Agent on an AD server to discover certificates, endpoints, users, and other assets. After integration, you can issue device certificates to AD objects.
- Code Signing on Demand Agents install on a single server or multiple servers. This agent can handle code signing requests from developers.

- Private Key Agents receives commands from SCM for CSR generation, storing private keys, and the generation of PKCS (Public Key Cryptography Standards) #12 certificates.

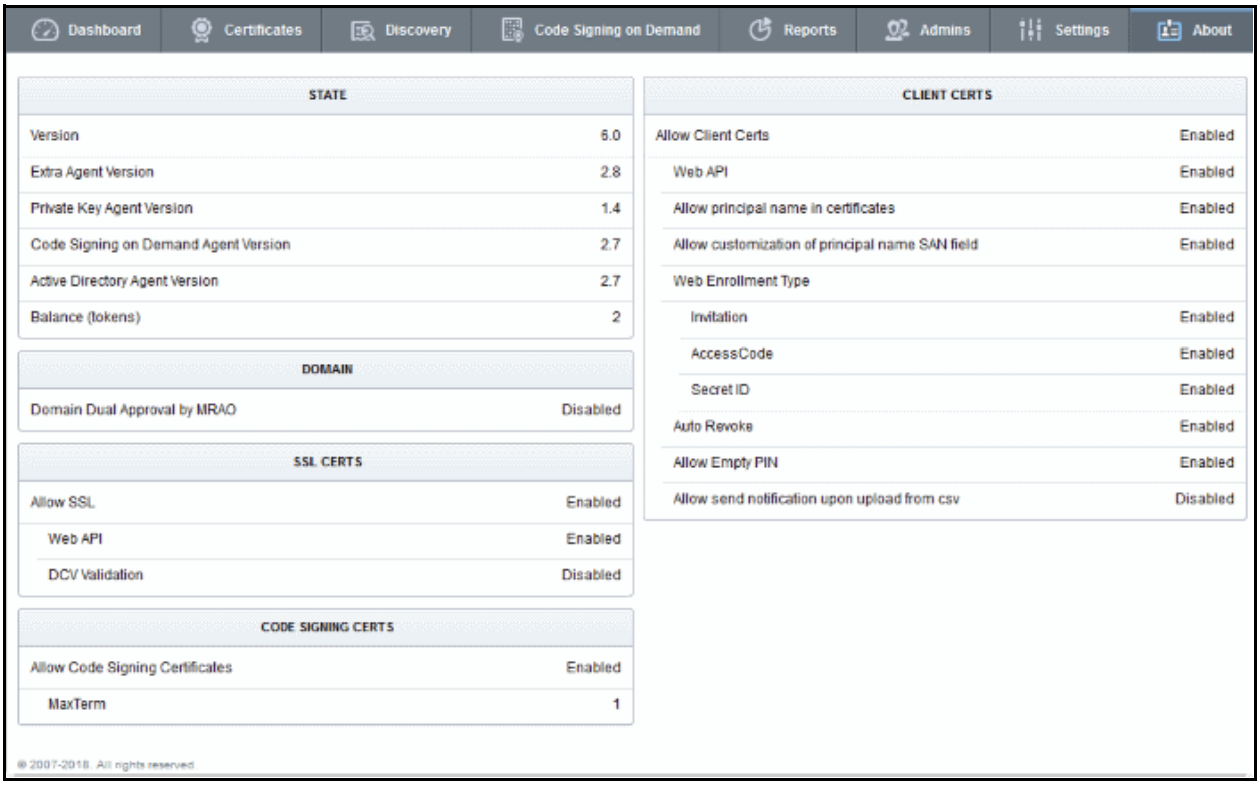
The **Assignment Rules** area enables MRAO and RAO administrators to define rules for automatically assigning external certificates identified by discovery scans to required organizations and departments, as well as apply the rules while configuring discovery scans.

The **Intune** area enables enrollment of client and device certificates integration with Microsoft Intune, as described in "Using SCM with Microsoft Intune" on page 599.

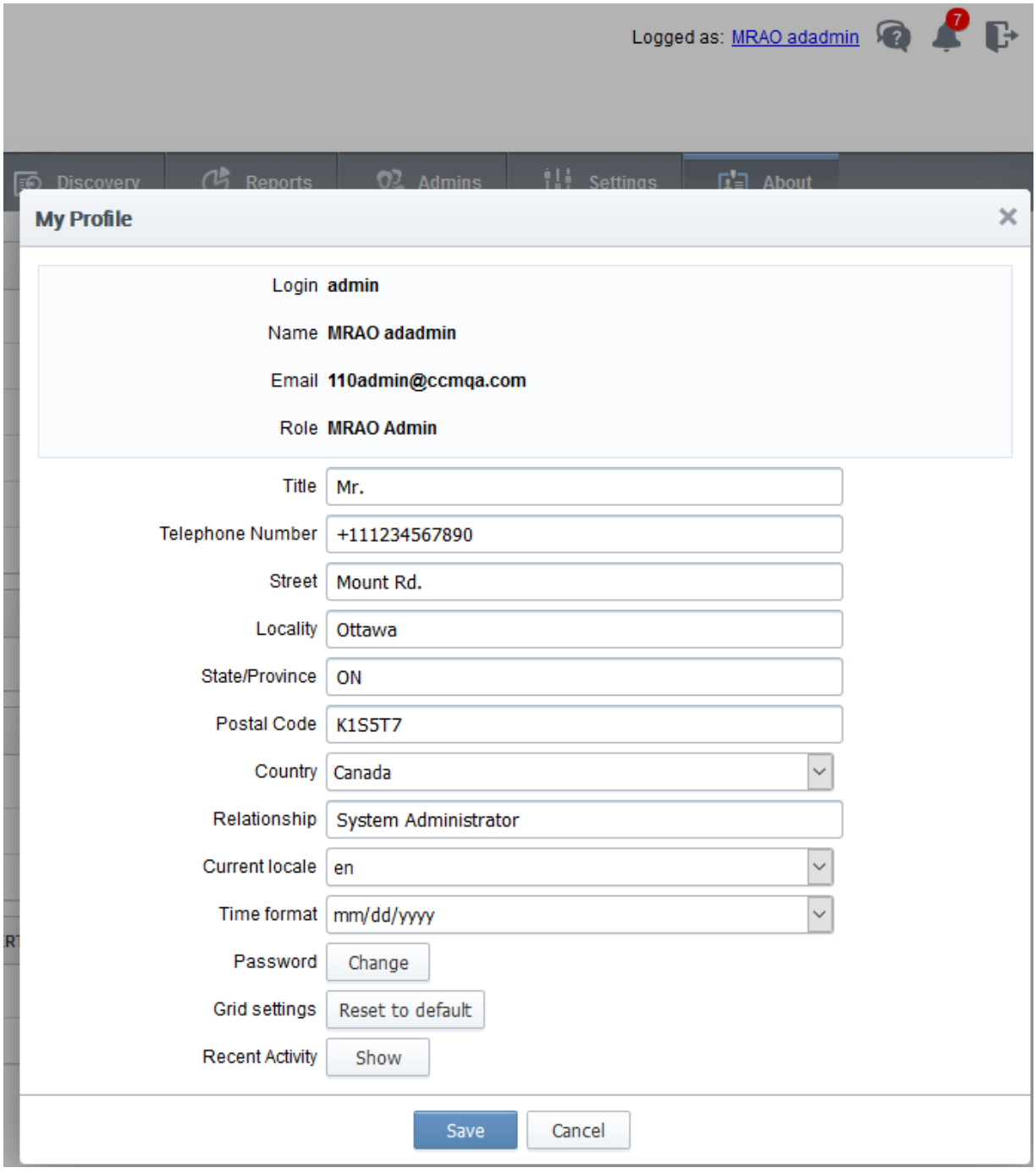
The **Azure** area enables administrators to connect SCM with Microsoft Azure for certificate generation in Azure Key Vault.

1.8.9 Miscellaneous Areas of the SCM UI

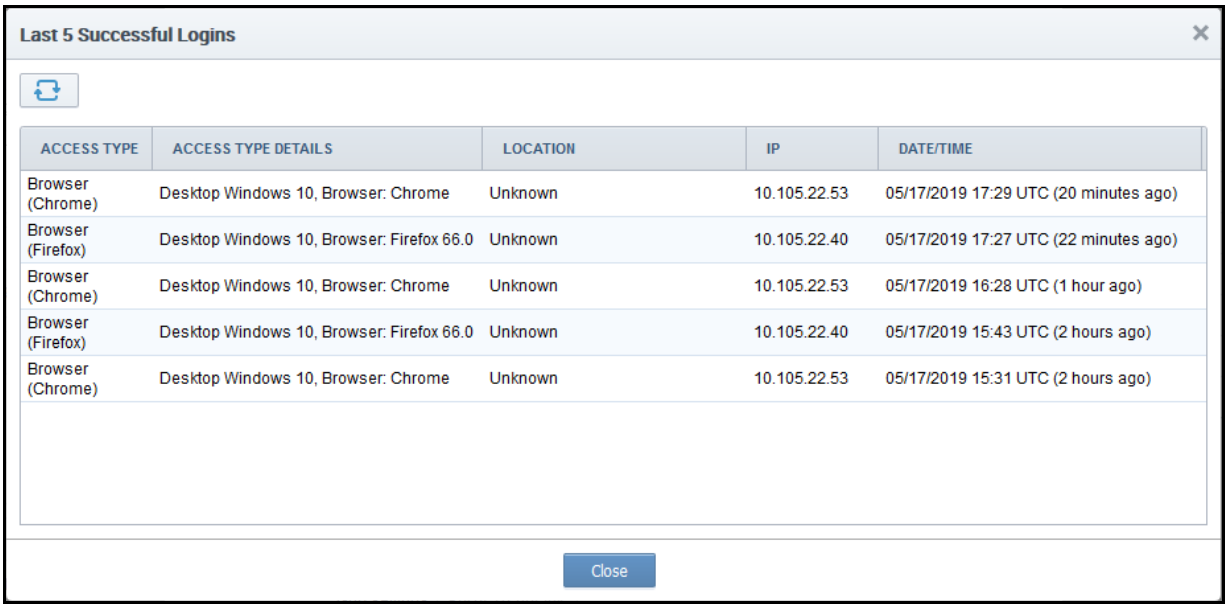
The **About** area shown in the following illustration allows you to view the version of SCM, as well as the features that are enabled and disabled for your account.



My Profile settings shown in the following illustration enable you, as the currently logged-in administrator, to view and edit address details, change the UI language setting, time format, and change the password. To open **My Profile**, click the link located to the right of **Logged as.**

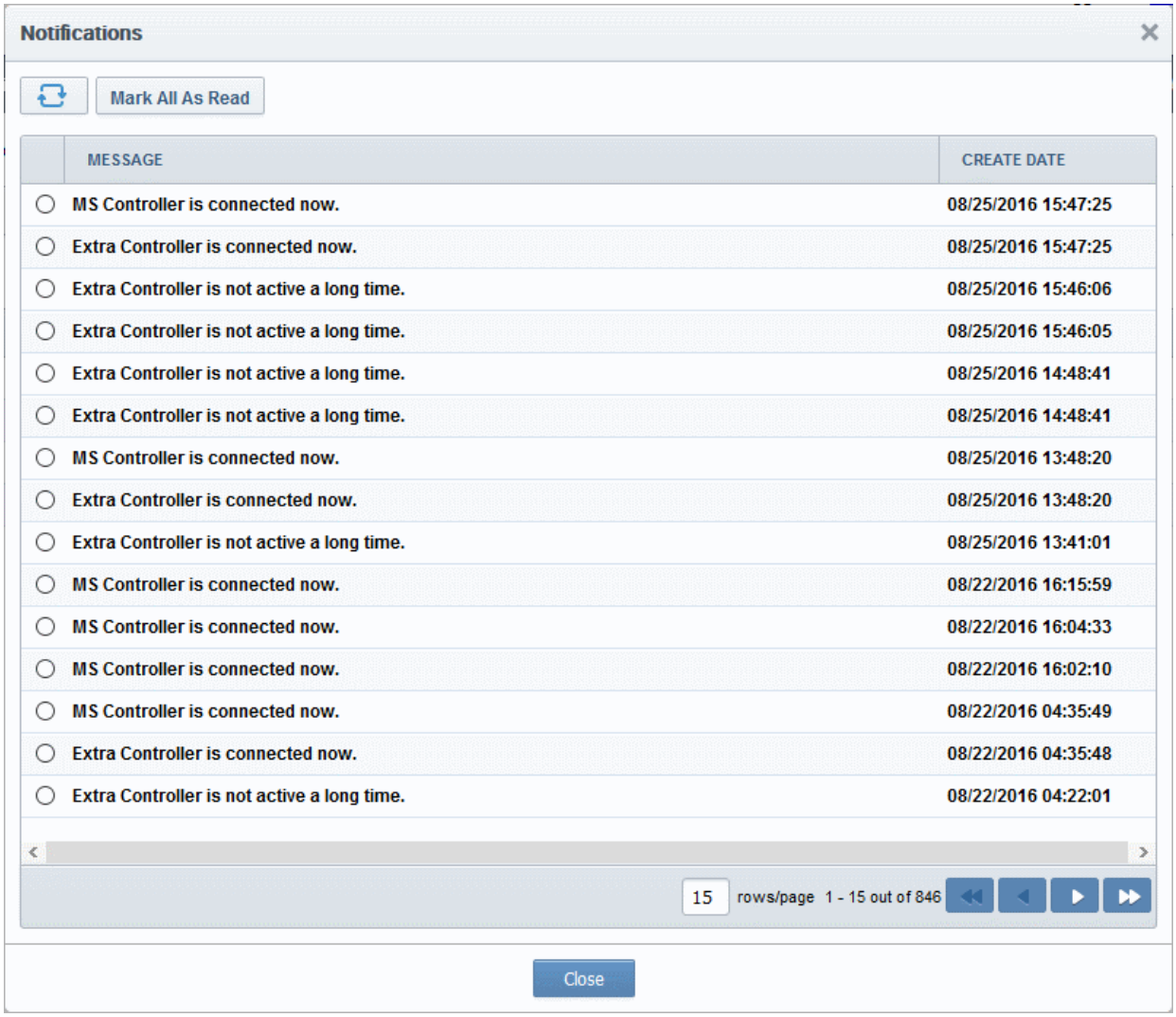


My Profile also allows you to view details of your last five successful login attempts by clicking **Recent Activity > Show**, as demonstrated in the following illustration.



If you experience any problems with using the SCM management console, you can click the **Help** icon to open the Sectigo's support page at `https://sectigo.com/support`

The **Notification** icon provides indication of the number of message that have not been read. To view these messages, you can click this icon. The types of messages displayed are related to validation, agent, and so on, as shown in the following illustration. The unread messages are displayed in bold. To view a full message, select it, and then click **Details**. To remove a message from the list, select this message, and then click **Delete**.



To log out of SCM, click **Logout**.

2

Understanding the SCM Dashboard

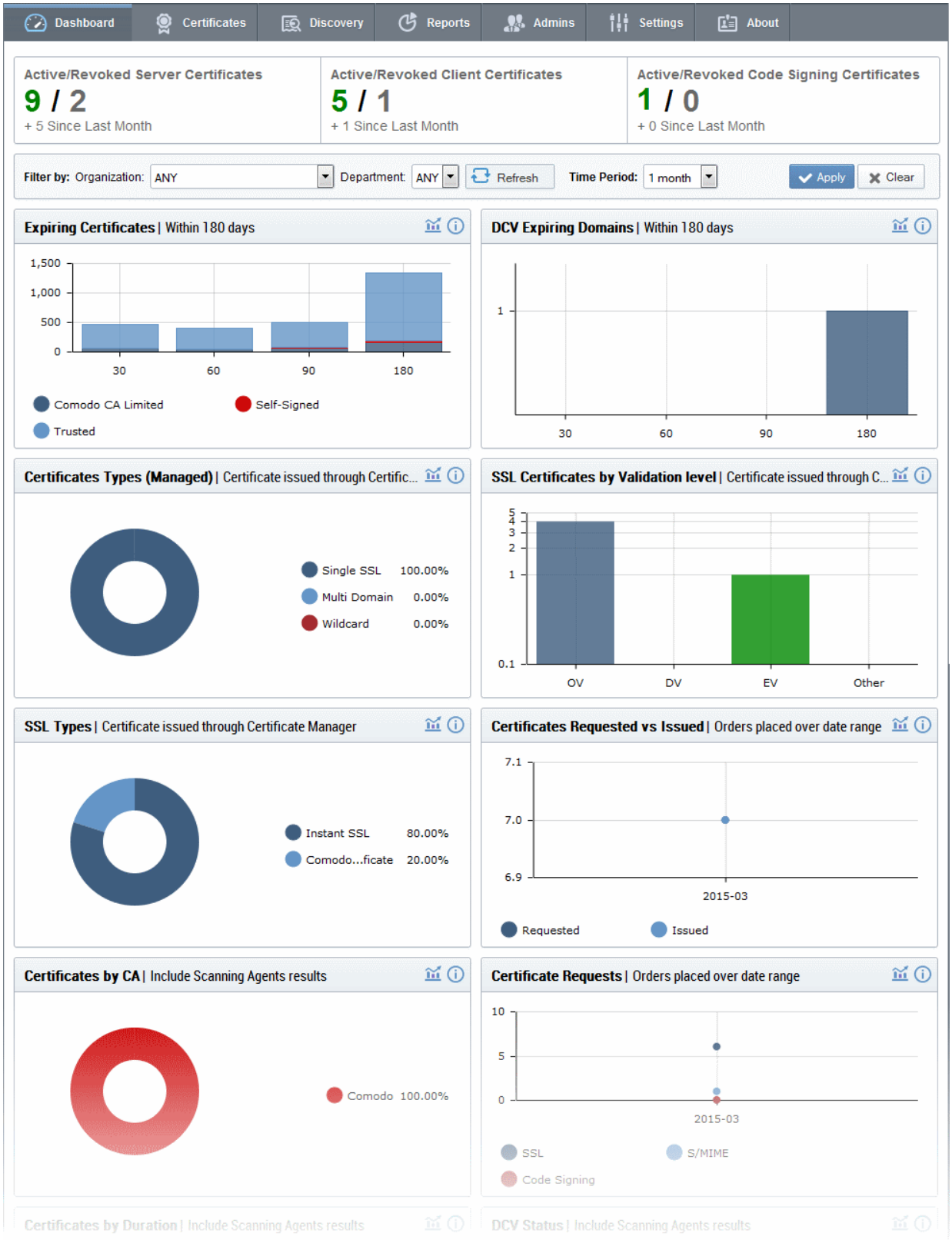
This chapter describes how to use the SCM dashboard for viewing data on various parameters of certificates.

This chapter describes the following topics:

- The SCM Dashboard Overview
- Accessing the Chart Data
- Filtering Data
- 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 the SCM UI. The dashboard provides an overview of all SSL, client, and code signing 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.

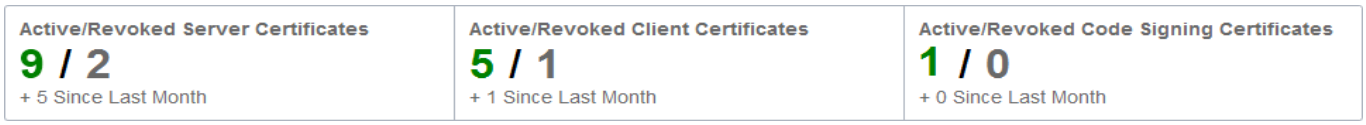

Dashboard
Certificates
Discovery
Reports
Admins
Settings
About
Active/Revoked Server Certificates
9 / 2
+ 5 Since Last Month
Active/Revoked Client Certificates
5 / 1
+ 1 Since Last Month
Active/Revoked Code Signing Certificates
1 / 0
+ 0 Since Last Month
Filter by: Organization: ANY
Department: ANY
Refresh
Time Period: 1 month
Apply
Clear
Expiring Certificates | Within 180 days
1,500
1,000
500
0
30
60
90
180
Comodo CA Limited
Self-Signed
Trusted
DCV Expiring Domains | Within 180 days
1
30
60
90
180
Certificates Types (Managed) | Certificate issued through Certific...
Single SSL 100.00%
Multi Domain 0.00%
Wildcard 0.00%
SSL Certificates by Validation level | Certificate issued through C...
5
4
3
2
1
0.1
OV
DV
EV
Other
SSL Types | Certificate issued through Certificate Manager
Instant SSL 80.00%
Comodo...ficate 20.00%
Certificates Requested vs Issued | Orders placed over date range
7.1
7.0
6.9
2015-03
Requested
Issued
Certificates by CA | Include Scanning Agents results
Comodo 100.00%
Certificate Requests | Orders placed over date range
10
5
0
2015-03
SSL
S/MIME
Code Signing
Certificates by Duration | Include Scanning Agents results
DCV Status | Include Scanning Agents results

2.2 Accessing the Chart Data

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

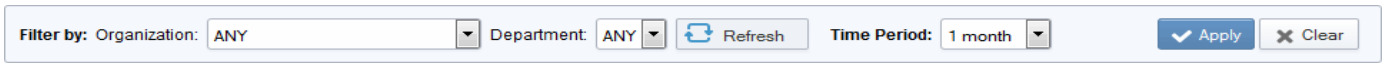
- MRAO administrators can view charts for all certificate types, domains, and web servers pertaining to all organizations and departments.
- RAO SSL, RAO Client Certificate, and RAO Code Signing administrators can view charts relevant to the certificate types, domains, and web servers of the organizations 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.

The area at the top of the dashboard displays a up-to-date summary of active and revoked certificates, as the following illustration shows.



2.3 Filtering Data

The data displayed in the dashboard can be filtered based on (1) the time period and (2) by organization and department, as the following illustration shows.



You can add a filter as follows:

- Select an organization and, optionally, department using the respective lists.
- Use the **Time Period** list to select the time period for which you wish to view data.
- Click **Apply**.

To reset the filters, click **Clear**.

2.4 Understanding Charts

The following charts are available through the dashboard:

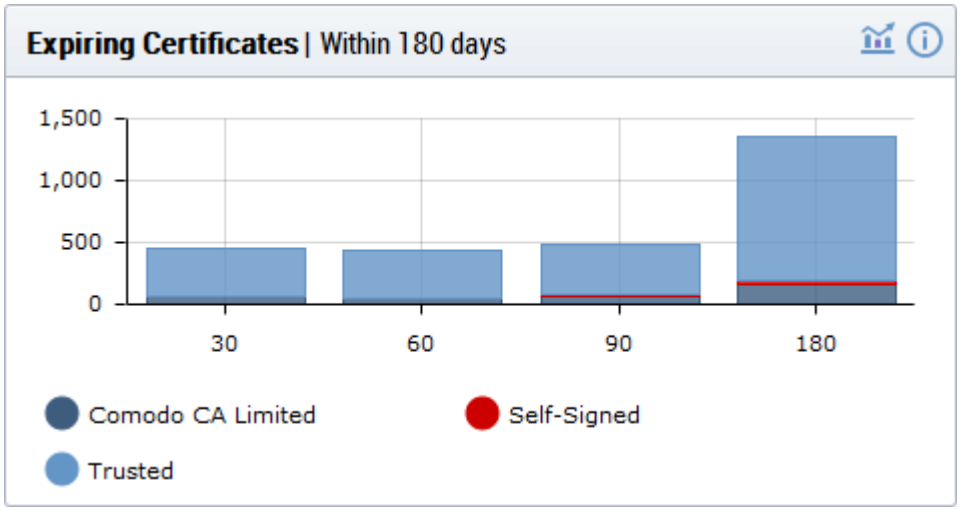
- **Expiring Certificates** chart visualizes data on certificates expiring within the next 180 days per each certificate issuer.
- **DCV Expiring Domains** chart visualizes data on domains for which domain control validation expires within the next 180 days.
- **Certificates Types (Managed)** chart visualizes data on managed certificates.
- **SSL Certificates by Validation Level** chart visualizes data on Domain Validated (DV), Organization Validated (OV), and Extended Validation (EV) levels.

- **SSL Types** chart visualizes data on certificates issued through SCM and is broken down by brand names such as Instant SSL, Premium SSL, EV SSL, and so on.
- **Certificate Requests vs Issued** chart visualizes data on how many certificate requests were placed and how many of these requests have progressed to certificates being issued.
- **Certificates by CA** chart visualizes data on the amount of certificates issues by different CA, such as Sectigo, VeriSign, GoDaddy, Thawte, self-signed, and so on.
- **Certificate Requests** chart visualizes data on the category of requested certificates, such as SSL requests, client requests, and so on.
- **Certificates By Duration** chart visualizes data on the amount of certificates issued for a specific duration, such as 1 year, 2 years, 3 years, and so on.
- **DCV Status** chart visualizes data on the current stage in the DVC process held by the certificate-hosting domains.
- **Certificates by Organization** chart visualizes data on certificates divided by the organizations to which these certificates have been issued.
- **Certificates by Key Strength** chart visualizes data on the strength of key with which the certificates were signed, such as 1024 bit, 2048 bit, and so on.
- **Certificates by Signing Algorithm** chart visualizes data on hashing and signing algorithms used, such as SHA1withRSA, and so on.
- **Certificates by Public Key Algorithm** chart visualizes data on the encryption algorithm used, such as RSA, DSA, and so on.
- **CSoD Usage** chart visualizes data on code signing requests divided by the total requests received and signed.
- **CSoD Certificates Usage** chart visualizes data on code signing requests divided by certificates belonging to different developers.

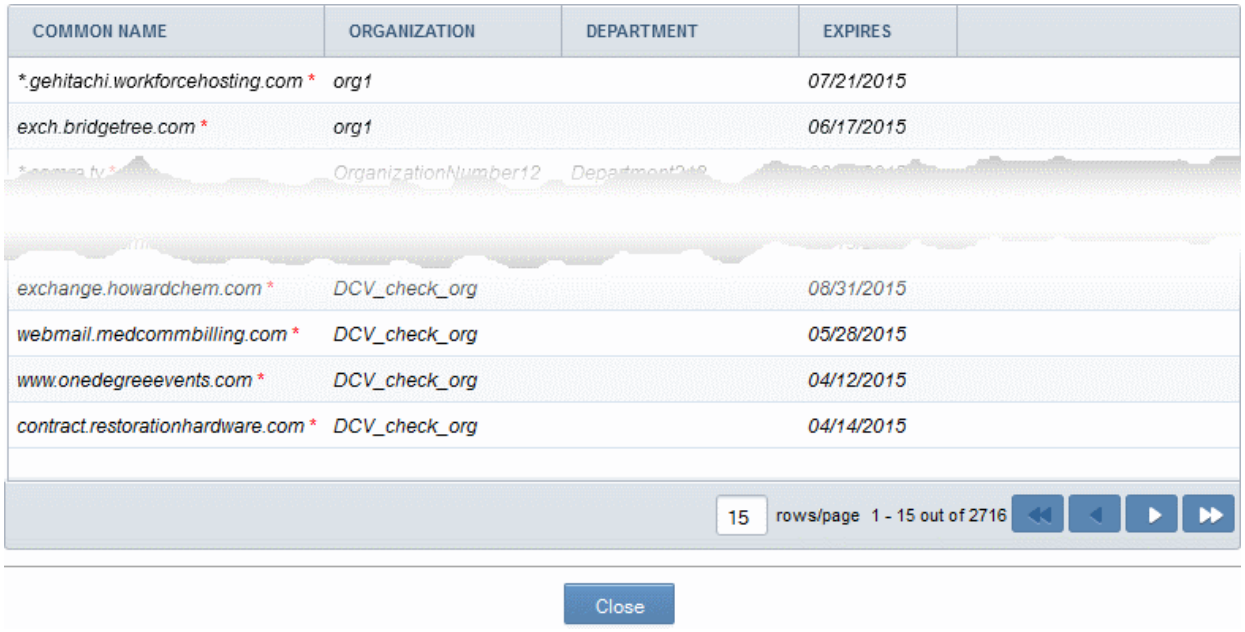
In every chart, clicking the information icon located at the top right corner of that particular chart area displays a tool tip explaining the chart parameters. In addition, hovering the cursor over a legend or chart sector displays additional information.

2.4.1 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.



Hovering the cursor over a legend or chart displays the number of certificates in each category. Clicking the chart icon displays a report with the breakdown of the chart statistics, as shown in the following illustration.



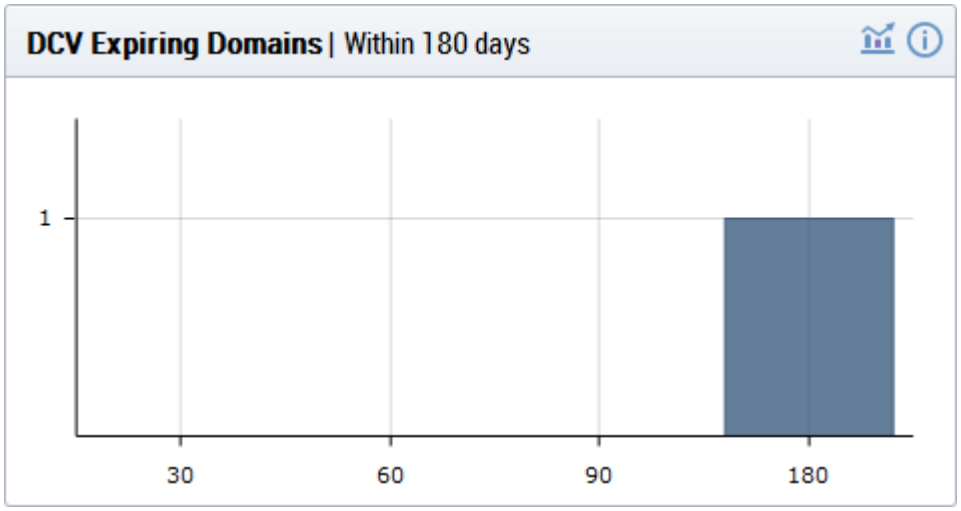
The following information is available:

- The **Common Name** column contains the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- The **Organization** column contains name of the organization that has been issued the certificate.
- The **Department** column contains the specific 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.

- The **Expires** column contains the expiration date of the certificate.

2.4.2 The DCV Expiring Domains Chart

The **DCV Expiring Domains** 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.



Hovering the cursor over a legend or chart displays the number of domains within that time frame. Clicking the chart icon displays a report with the breakdown of the chart statistics, as shown in the following illustration.

NAME	DELEGATION STATUS	DATE REQUESTED	DCV STATUS
*.dithers.com	Approved	09/05/2013	Validated
dithers.com	Approved	09/05/2013	Validated

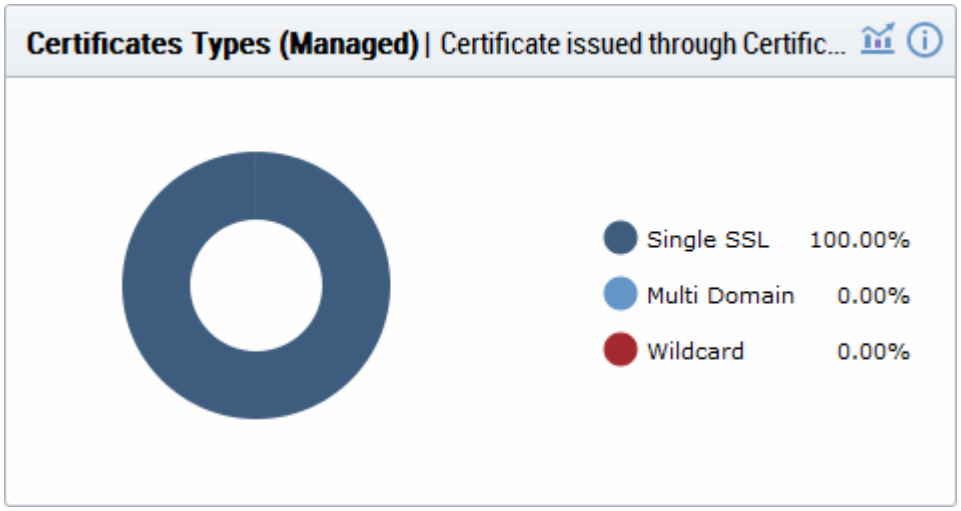
15 rows/page 1 - 2 out of 2

The following information is available:

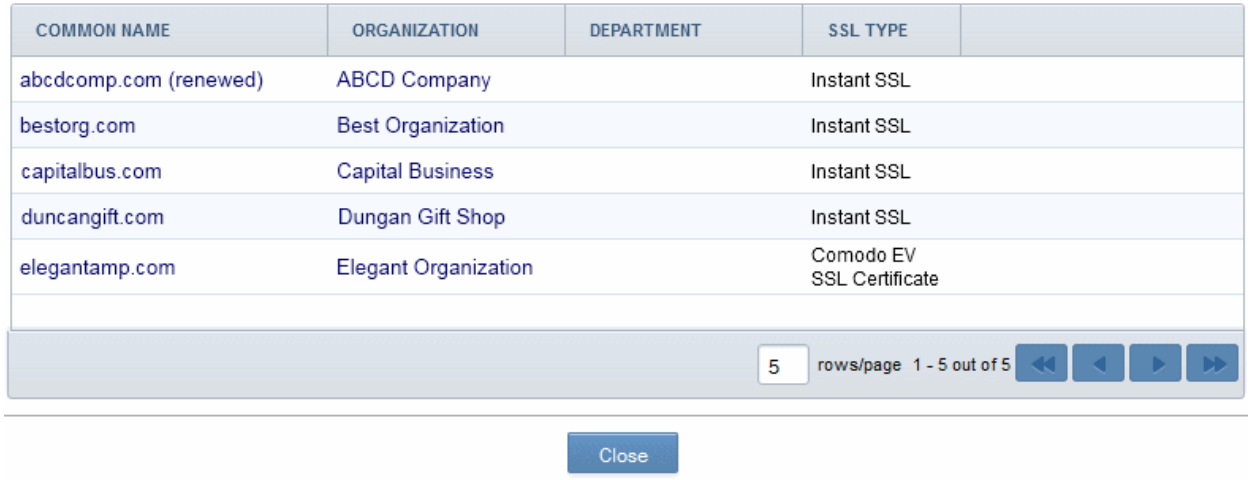
- The **Name** column contains the domain name.
- The **Delegation Status** column indicates whether domain is active or inactive.
- The **Date Requested** column indicates the date on which the domain was requested.
- The **DCV Status** column indicates the request and approval status of the domain.

2.4.3 The Certificate Types (Managed) Chart

The **Certificate Types (Managed)** chart shown in the following illustration summarizes the different types of managed SSL certificates issued through SCM and installed on servers within your network.



Hovering the cursor over a legend item or section of the chart displays details, such as the actual quantity of certificates of that type. Clicking the chart icon displays a report with the breakdown of the chart statistics.



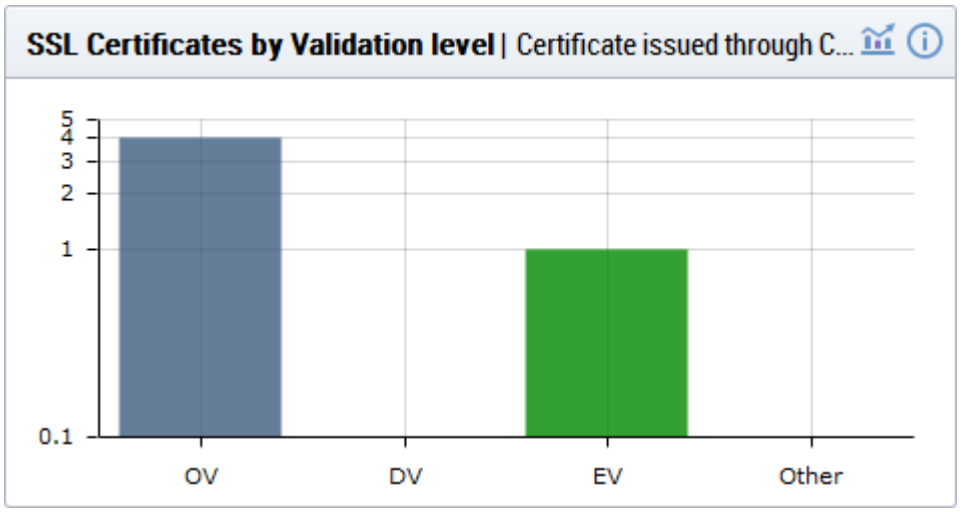
The following information is available:

- The **Common Name** column contains the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- The **Organization** column contains the name of the organization that has been issued with the certificate.

- The **Department** column contains the specific 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.
- The **SSL Type** column contains the type of the certificate with its brand name.

2.4.4 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.



Hovering the cursor over a bar displays the exact number of certificates in that category. Clicking the chart icon displays a report with the breakdown of the chart statistics, as the following illustration shows.

COMMON NAME	ORGANIZATION	DEPARTMENT	SUB TYPE
abcdcomp.com (renewed)	ABCD Company		OV
bestorg.com	Best Organization		OV
capitalbus.com	Capital Business		OV
duncangift.com	Dungan Gift Shop		OV
elegantamp.com	Elegant Organization		EV

15 rows/page 1 - 5 out of 5

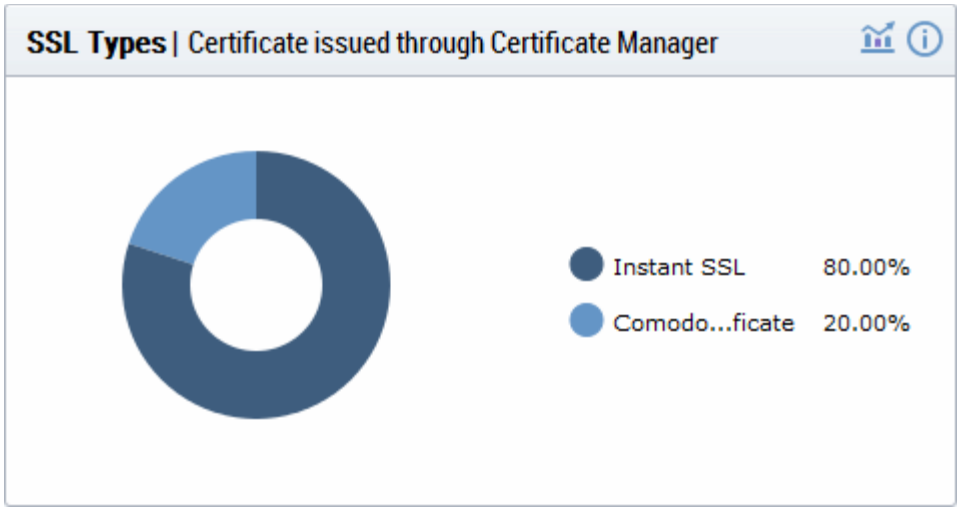
Close

The following information is available:

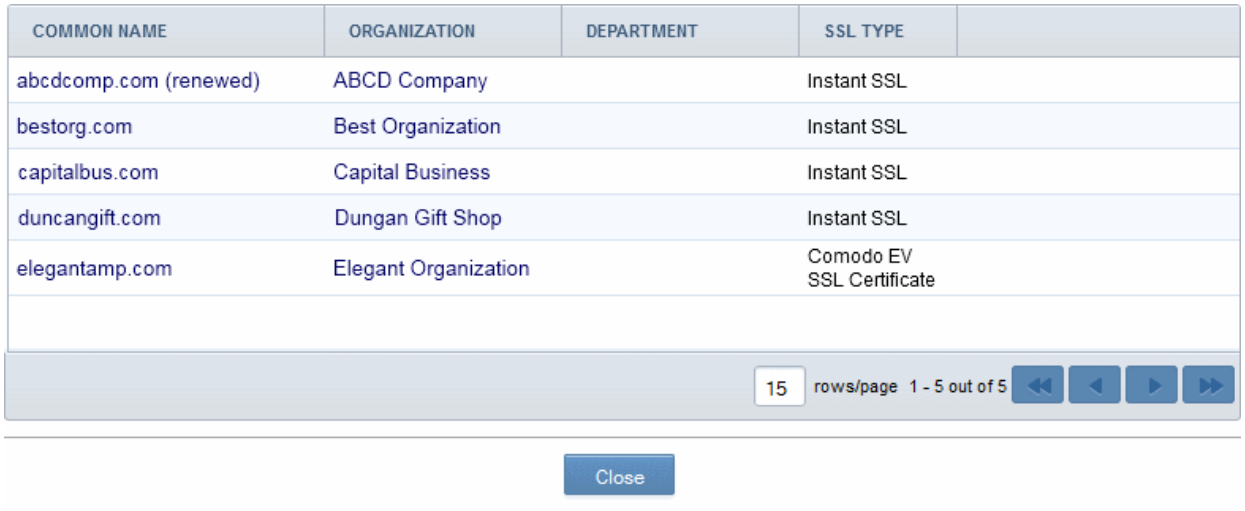
- The **Common Name** column contains the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- The **Organization** column contains the name of the organization that has been issued with the certificate.
- The **Department** column contains the specific 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.
- The **Sub Type** column indicates the validation level of the certificate, such as OV or EV.

2.4.5 The SSL Types Chart

The **SSL Types** chart shown in the following illustration details the quantities of SSL certificates issued by SCM according to the certificate brand name.



Hovering the cursor over a legend or sector displays additional information. Clicking the chart icon displays a report with the breakdown of the chart statistics, as shown in the following illustration.



COMMON NAME	ORGANIZATION	DEPARTMENT	SSL TYPE
abcdcomp.com (renewed)	ABCD Company		Instant SSL
bestorg.com	Best Organization		Instant SSL
capitalbus.com	Capital Business		Instant SSL
duncangift.com	Dungan Gift Shop		Instant SSL
elegantamp.com	Elegant Organization		Comodo EV SSL Certificate

15 rows/page 1 - 5 out of 5

Close

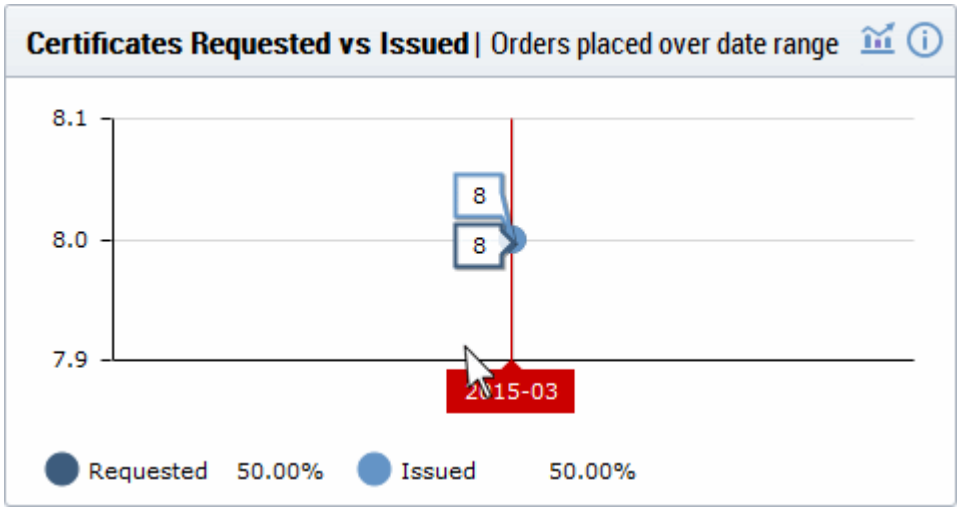
The following information is available:

- The **Common Name** column contains the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- The **Organization** column contains the name of the organization that has been issued with the certificate.
- The **Department** column contains the specific 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.
- The **SSL Type** column indicates the brand name of the certificate.

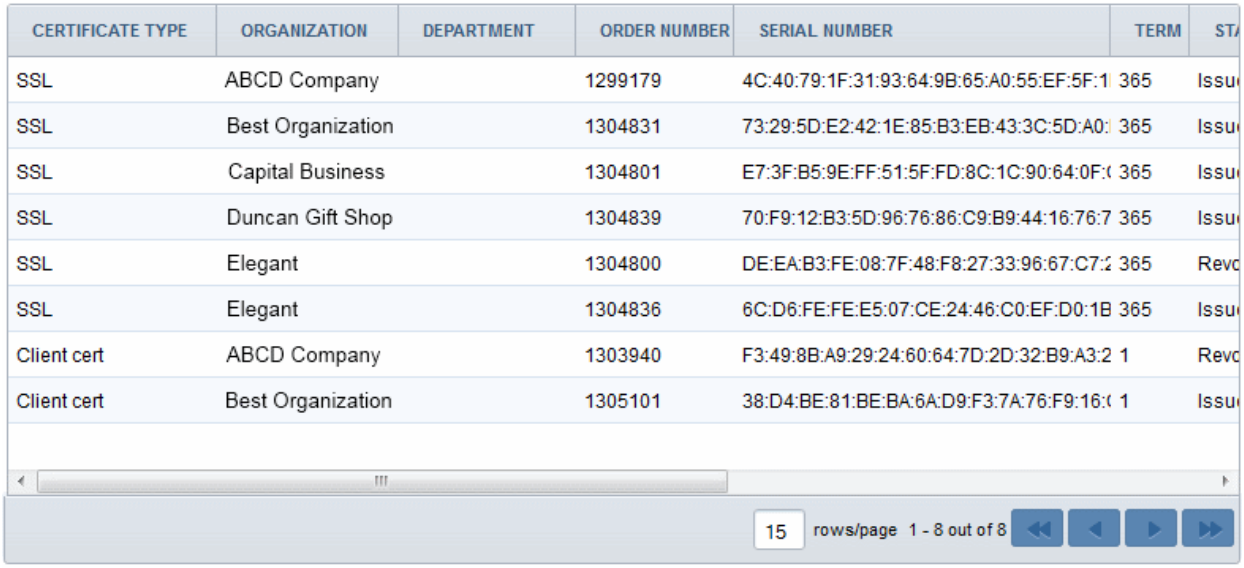
  NOTE: Issued certificates are displayed in blue.

2.4.6 Certificates Requested vs Issued

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



Hovering the cursor over the cart nodes displays additional information about the number of certificates that were requested and issued on that date. Clicking the chart icon displays a report with the breakdown of the chart statistics, as shown in the following illustration.



CERTIFICATE TYPE	ORGANIZATION	DEPARTMENT	ORDER NUMBER	SERIAL NUMBER	TERM	ST
SSL	ABCD Company		1299179	4C:40:79:1F:31:93:64:9B:65:A0:55:EF:5F:1	365	Issu
SSL	Best Organization		1304831	73:29:5D:E2:42:1E:85:B3:EB:43:3C:5D:A0:	365	Issu
SSL	Capital Business		1304801	E7:3F:B5:9E:FF:51:5F:FD:8C:1C:90:64:0F:(	365	Issu
SSL	Duncan Gift Shop		1304839	70:F9:12:B3:5D:96:76:86:C9:B9:44:16:76:7	365	Issu
SSL	Elegant		1304800	DE:EA:B3:FE:08:7F:48:F8:27:33:96:67:C7:2	365	Revo
SSL	Elegant		1304836	6C:D6:FE:FE:E5:07:CE:24:46:C0:EF:D0:1B	365	Issu
Client cert	ABCD Company		1303940	F3:49:8B:A9:29:24:60:64:7D:2D:32:B9:A3:2	1	Revo
Client cert	Best Organization		1305101	38:D4:BE:81:BE:BA:6A:D9:F3:7A:76:F9:16:(	1	Issu

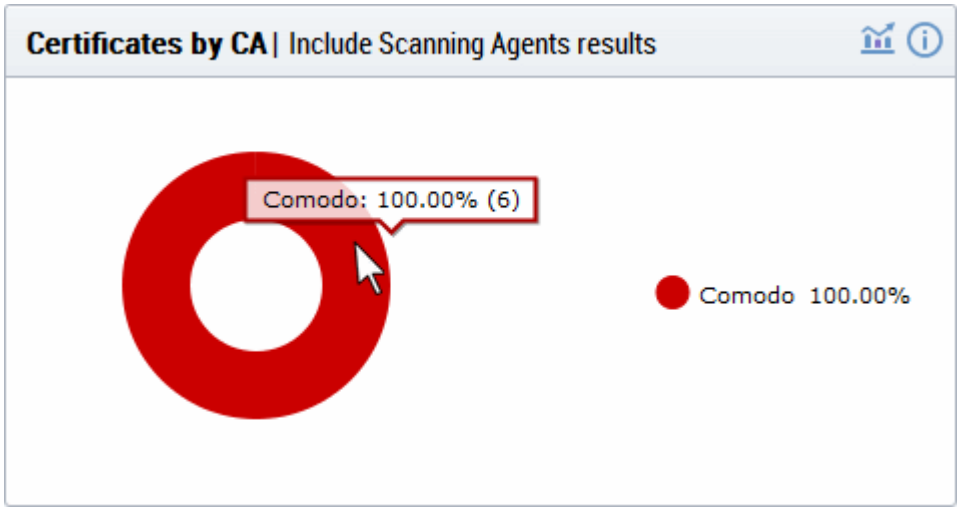
15 rows/page 1 - 8 out of 8

The following information is available:

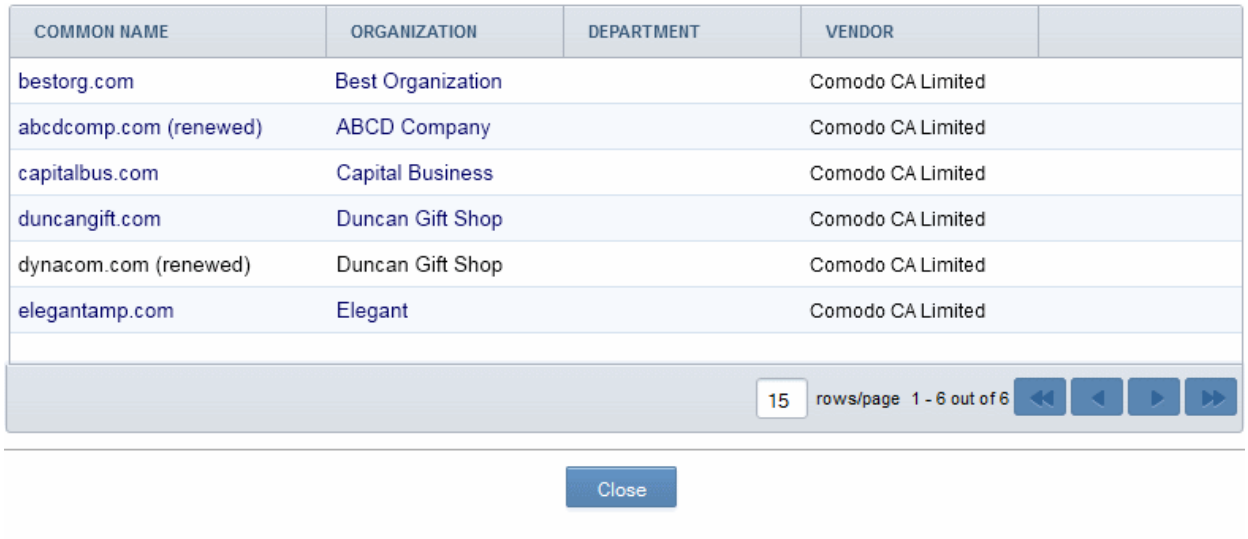
- The **Certificate Type** column contains the type of the issued or requested certificate.
- The **Organization** column contains the name of the organization that has been issued with the certificate.
- The **Department** column contains the specific department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- The **Order Number** column contains the number assigned by the CA for the request.
- The **Serial Number** column displays the unique identifier of the certificate.
- The **Term** column contains 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.
- The **Status** column contains the current status of the certificate.
- The **Requested** column contains the date when the certificate was requested by the end-user or the administrator.
- The **Collected** column contains the date when the certificate was collected by the end-user or the administrator.
- The **Expires** column contains the certificate expiry date.

2.4.7 The Certificates by CA Chart

The **Certificates by CA** chart shown in the following illustration provides a breakdown of your certificates by signer, therefore 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.



Hovering your cursor over a legend or chart sector displays the number of certificates by a specific signer and indicates the percentage of the total certificates that these certificates account for. Clicking the chart icon displays a report with the breakdown of the chart statistics, as shown in the following illustration.



COMMON NAME	ORGANIZATION	DEPARTMENT	VENDOR
bestorg.com	Best Organization		Comodo CA Limited
abcdcomp.com (renewed)	ABCD Company		Comodo CA Limited
capitalbus.com	Capital Business		Comodo CA Limited
duncangift.com	Duncan Gift Shop		Comodo CA Limited
dynacom.com (renewed)	Duncan Gift Shop		Comodo CA Limited
elegantamp.com	Elegant		Comodo CA Limited

15 rows/page 1 - 6 out of 6

Close

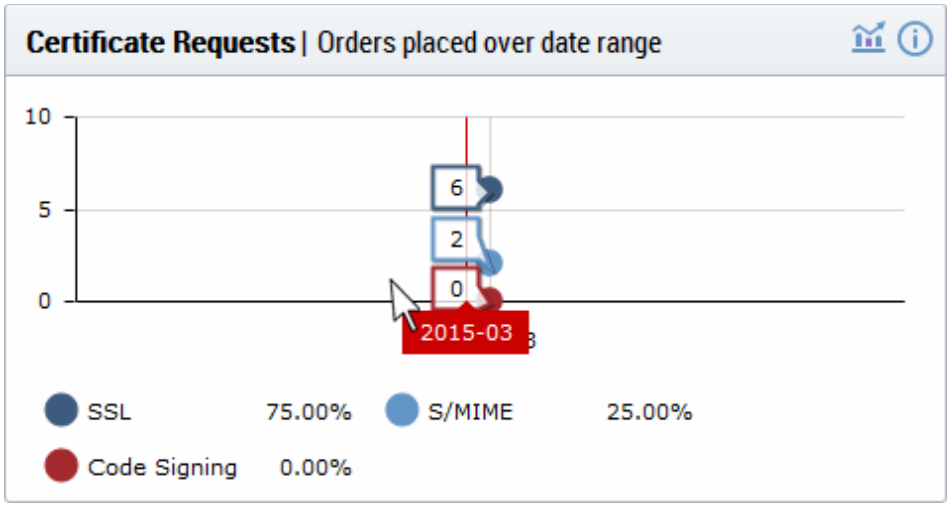
The following information is available:

- The **Common Name** column contains the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- The **Organization** column contains the name of the organization that has been issued with the certificate.
- The **Department** column contains the specific 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.
- The **Vendor** column contains the domain name of the vendor that issued the certificate.

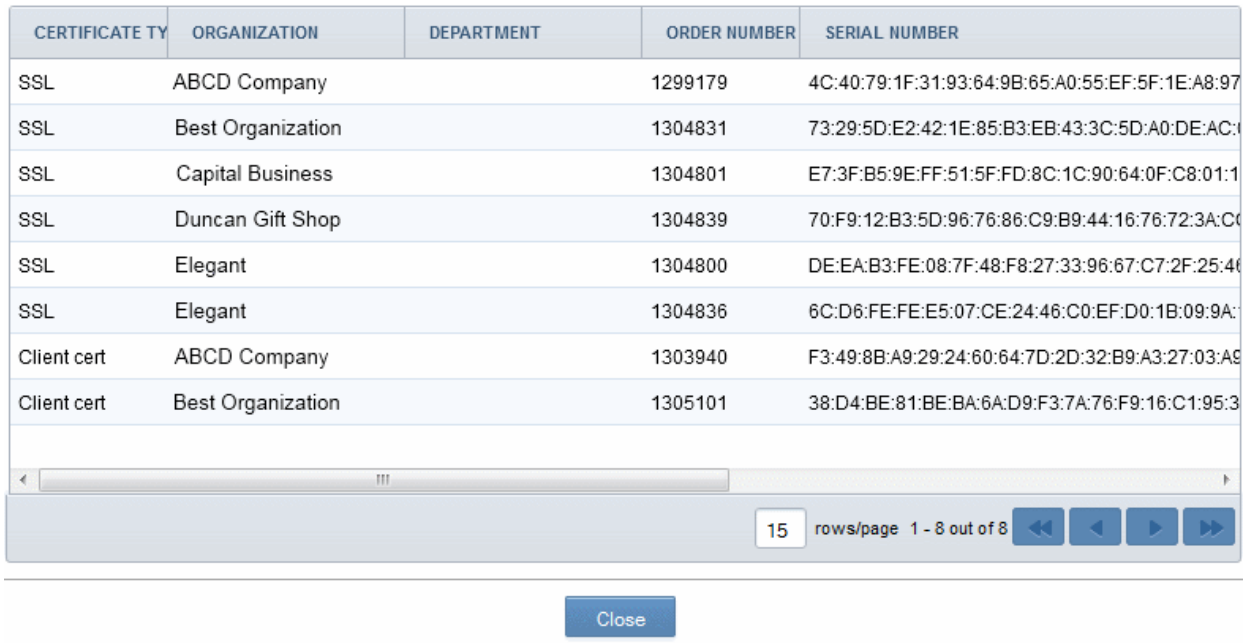
NOTE: Issued certificates are displayed in blue.

2.4.8 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, and code signing certificates.



Hovering the cursor over the chart nodes displays the exact number of certificates that were requested. Clicking the chart icon displays a report with the breakdown of the chart statistics, as shown in the following illustration.



CERTIFICATE TY	ORGANIZATION	DEPARTMENT	ORDER NUMBER	SERIAL NUMBER
SSL	ABCD Company		1299179	4C:40:79:1F:31:93:64:9B:65:A0:55:EF:5F:1E:A8:97
SSL	Best Organization		1304831	73:29:5D:E2:42:1E:85:B3:EB:43:3C:5D:A0:DE:AC:
SSL	Capital Business		1304801	E7:3F:B5:9E:FF:51:5F:FD:8C:1C:90:64:0F:C8:01:1
SSL	Duncan Gift Shop		1304839	70:F9:12:B3:5D:96:76:86:C9:B9:44:16:76:72:3A:C
SSL	Elegant		1304800	DE:EA:B3:FE:08:7F:48:F8:27:33:96:67:C7:2F:25:4
SSL	Elegant		1304836	6C:D6:FE:FE:E5:07:CE:24:46:C0:EF:D0:1B:09:9A:
Client cert	ABCD Company		1303940	F3:49:8B:A9:29:24:60:64:7D:2D:32:B9:A3:27:03:A
Client cert	Best Organization		1305101	38:D4:BE:81:BE:BA:6A:D9:F3:7A:76:F9:16:C1:95:3

15 rows/page 1 - 8 out of 8

Close

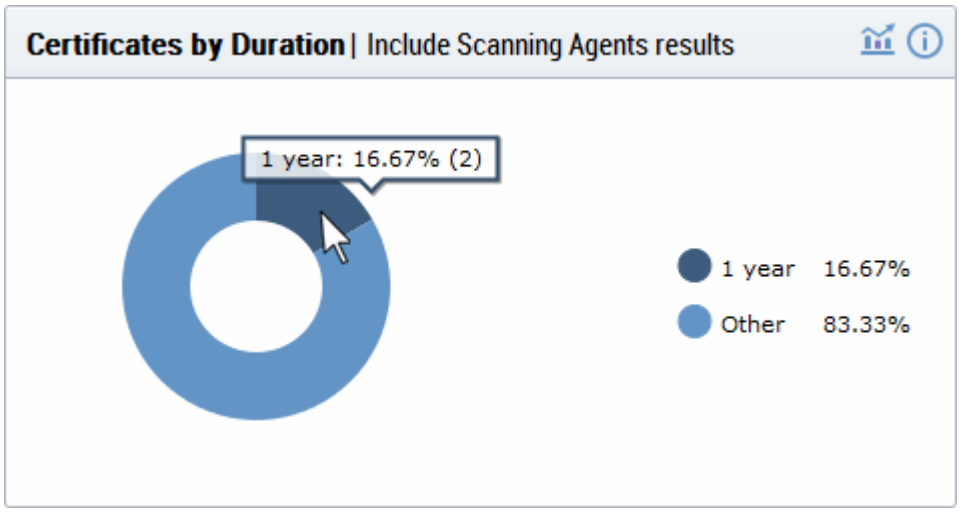
The following information is available:

- The **Certificate Type** column contains the type of the issued or requested certificate.

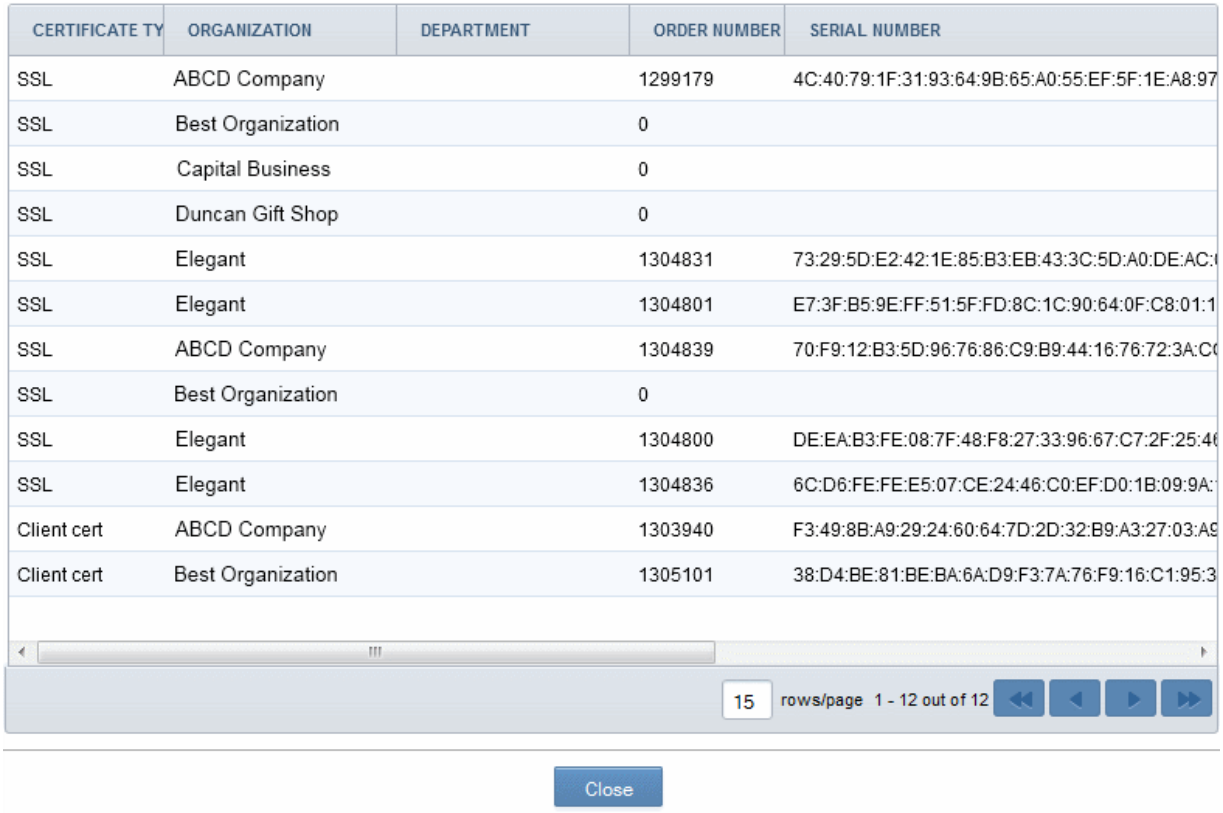
- The **Organization** column contains the name of the organization that has been issued with the certificate.
- The **Department** column contains the specific department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- The **Order Number** column contains the number assigned by the CA for the request.
- The **Serial Number** column displays the unique identifier of the certificate.
- The **Term** column contains 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.
- The **Status** column contains the current status of the certificate.
- The **Requested** column contains the date when the certificate was requested by the end-user or the administrator.
- The **Collected** column contains the date when the certificate was collected by the end-user or the administrator.
- The **Expires** column contains the certificate expiry date.

2.4.9 Certificates by Duration

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



Hovering the cursor over a chart legend or section displays the exact number of certificates with a specific term length and indicates the percentage of the total certificates that these certificates account for. Clicking the chart icon displays a report with the breakdown of the chart statistics, as shown in the following illustration.



CERTIFICATE TY	ORGANIZATION	DEPARTMENT	ORDER NUMBER	SERIAL NUMBER
SSL	ABCD Company		1299179	4C:40:79:1F:31:93:64:9B:65:A0:55:EF:5F:1E:A8:97
SSL	Best Organization		0	
SSL	Capital Business		0	
SSL	Duncan Gift Shop		0	
SSL	Elegant		1304831	73:29:5D:E2:42:1E:85:B3:EB:43:3C:5D:A0:DE:AC:
SSL	Elegant		1304801	E7:3F:B5:9E:FF:51:5F:FD:8C:1C:90:64:0F:C8:01:1
SSL	ABCD Company		1304839	70:F9:12:B3:5D:96:76:86:C9:B9:44:16:76:72:3A:C
SSL	Best Organization		0	
SSL	Elegant		1304800	DE:EA:B3:FE:08:7F:48:F8:27:33:96:67:C7:2F:25:4
SSL	Elegant		1304836	6C:D6:FE:FE:E5:07:CE:24:46:C0:EF:D0:1B:09:9A:
Client cert	ABCD Company		1303940	F3:49:8B:A9:29:24:60:64:7D:2D:32:B9:A3:27:03:A9
Client cert	Best Organization		1305101	38:D4:BE:81:BE:BA:6A:D9:F3:7A:76:F9:16:C1:95:3

15 rows/page 1 - 12 out of 12

Close

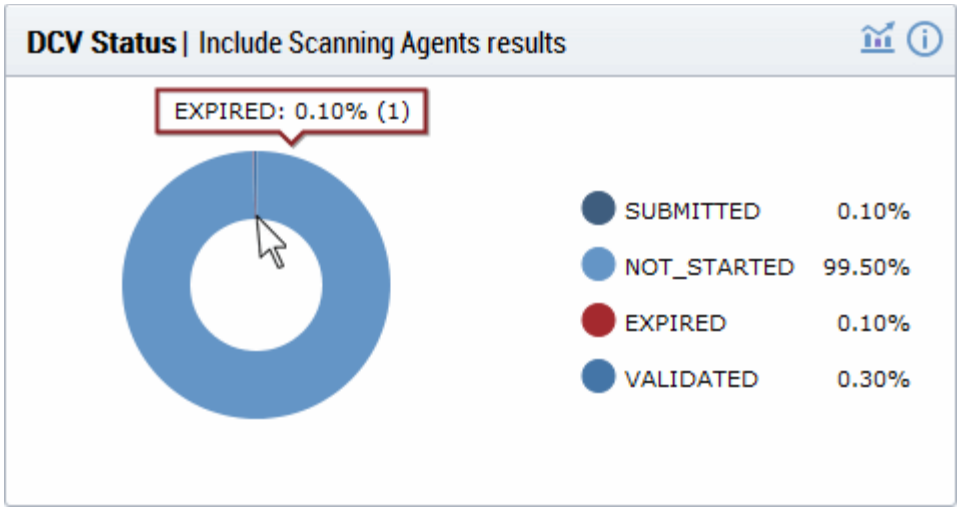
The following information is available:

- The **Certificate Type** column contains the type of the issued or requested certificate.
- The **Organization** column contains the name of the organization that has been issued with the certificate.
- The **Department** column contains the specific 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.
- The **Order Number** column contains the number assigned by the CA for the request.
- The **Serial Number** column displays the unique identifier of the certificate.
- The **Term** column contains 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.
- The **Status** column contains the current status of the certificate.
- The **Requested** column contains the date when the certificate was requested by the end-user or the administrator.
- The **Collected** column contains the date when the certificate was collected by the end-user or the administrator.
- The **Expires** column contains the certificate expiry date.

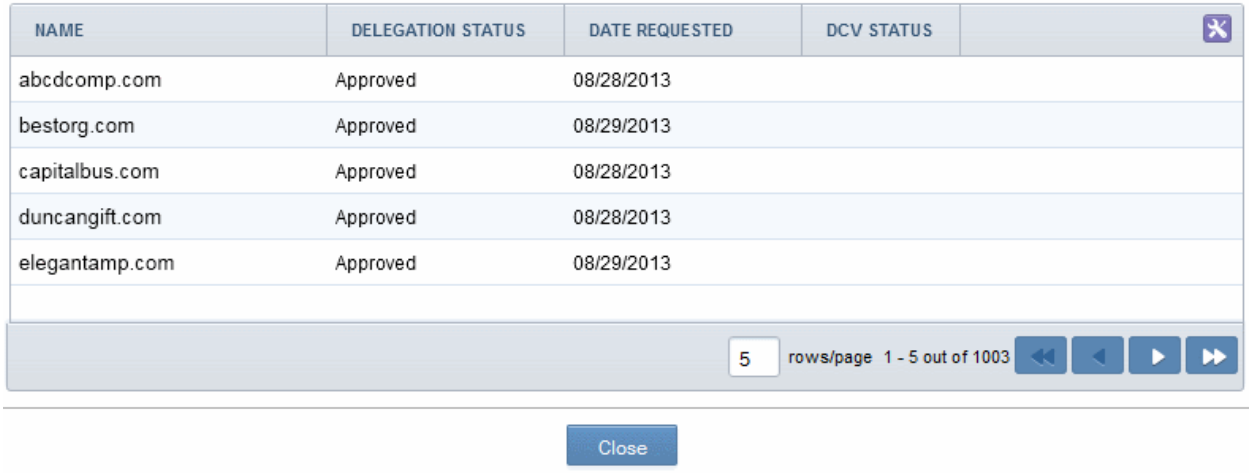
2.4.10 The DCV Status Chart

The **DVC Status Chart** chart shown in the following illustration displays a summary of the DCV status of domains registered within the certificate manager. DCV is required in order for Sectigo

to issue certificates to your public domains and subdomains. It is recommended to start by completing DCV on a registrable domain (in the format of *domain.com*). Having a domain pass DCV speeds up the processing of the certificate applications due to the fact that all subdomains, including wildcards, would also be considered complete.



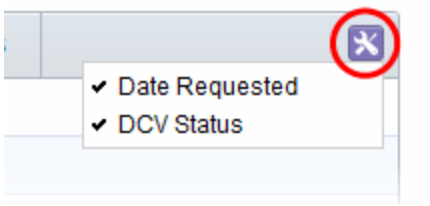
Hovering the cursor over a chart legend or section displays the quantity of domains with a particular status and their percentage of the total domains. Clicking the chart icon displays a report with the breakdown of the chart statistics, as shown in the following illustration.



The following information is available:

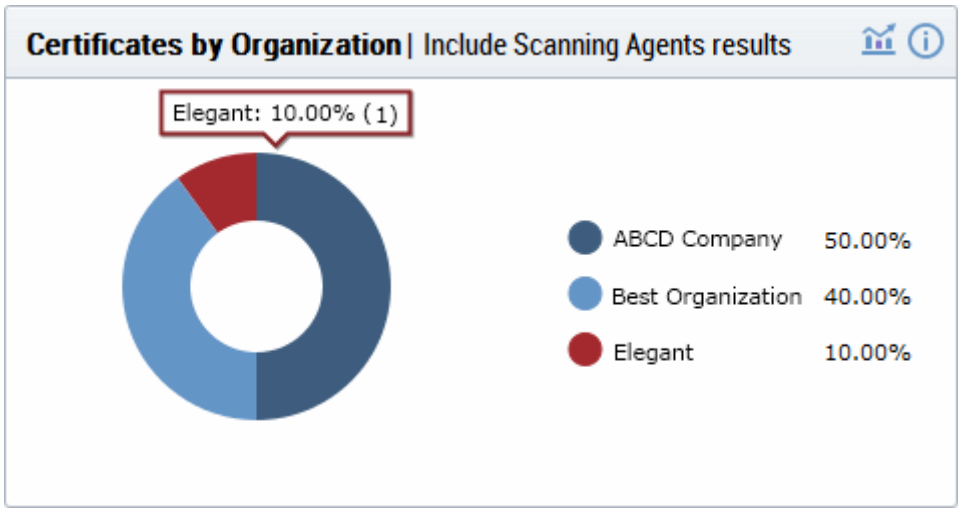
- The **Name** the domain name.
- The **Delegation Status** column indicates the status of the domain within SCM, such as approved, requested, and so on.
- The **Date Requested** column indicates the date on which the domain was requested.
- The **DCV Status** column indicates the validation status of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

You can specify columns to be displayed by clicking the settings icon at the top right of the table, and then selecting the columns.

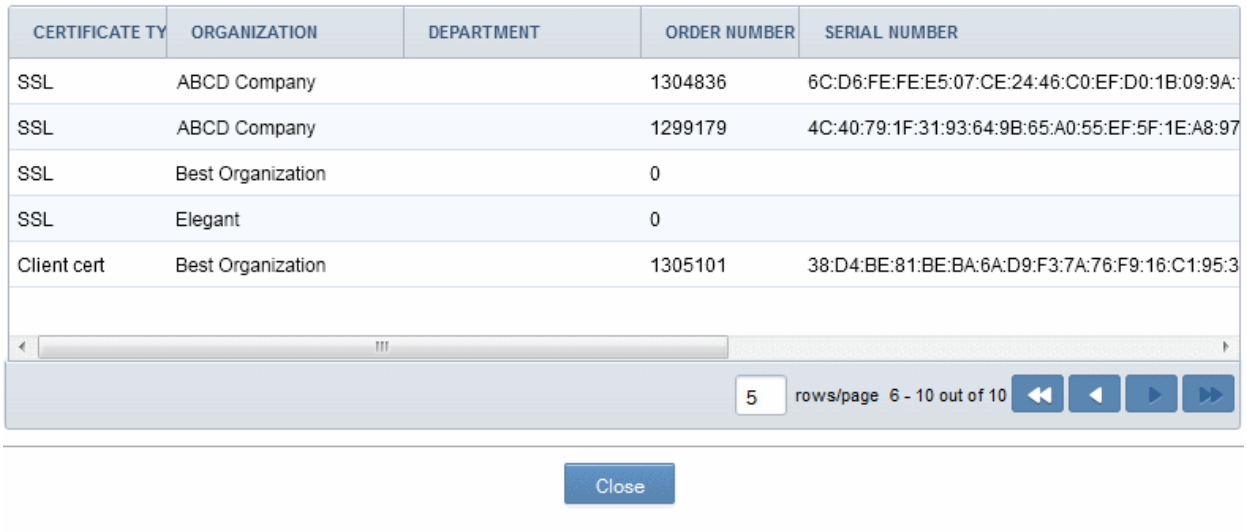


2.4.11 The Certificates by Organization Chart

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



Hovering the cursor over a chart legend or section displays the precise number and percentage of total certificates issued to a particular organization. Clicking the chart icon displays a report with the breakdown of the chart statistics, as shown in the following illustration.

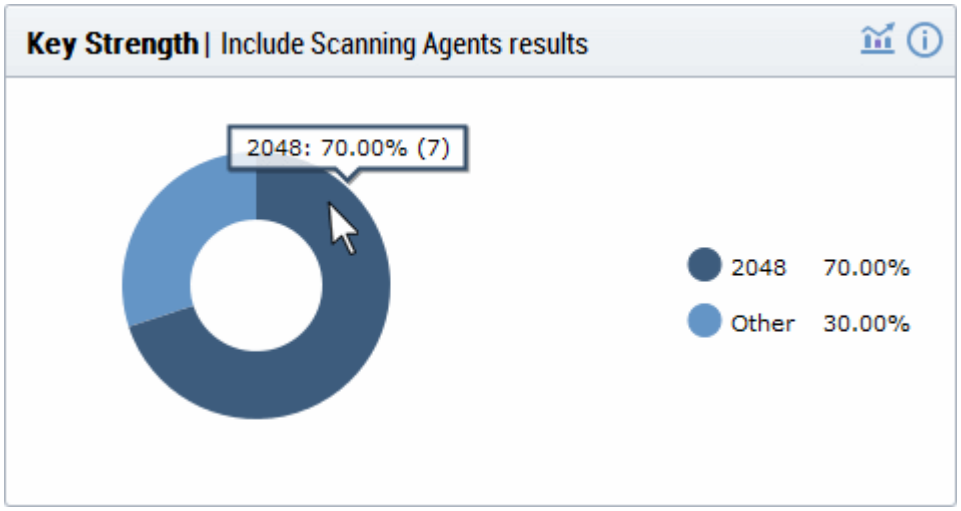


The following information is available:

- The **Certificate Type** column contains the type of the issued or requested certificate.
- The **Organization** column contains the name of the organization that has been issued with the certificate.
- The **Department** column contains the specific 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.
- The **Order Number** column contains the number assigned by the CA for the request.
- The **Serial Number** column displays the unique identifier of the certificate.
- The **Term** column contains 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.
- The **Status** column contains the current status of the certificate.
- The **Requested** column contains the date when the certificate was requested by the end-user or the administrator.
- The **Collected** column contains the date when the certificate was collected by the end-user or the administrator.
- The **Expires** column contains the certificate expiry date.

2.4.12 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 which need to be replaced in order to be compliant with the 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.



Hovering the cursor over a chart legend or section displays the exact number of certificates with a particular signature size and their percentage of the total certificates. Clicking the chart icon displays a report with the breakdown of the chart statistics, as shown in the following illustration.

COMMON NAME	ORGANIZATION	DEPARTMENT	EXPIRES	KEY ALGORITHM	KEY SIZE
abcdcomp.com	ABCD Company		03/10/2016	RSA	2048
elegantamp.com	Elegant				0
abcdcorp.com	ABCD Company				0
abcdmail.com	ABCD Company				0
bestorg.com (renewed)	Best Organization		11/02/2015	RSA	2048

5 rows/page 1 - 5 out of 10

Close

The following information is available:

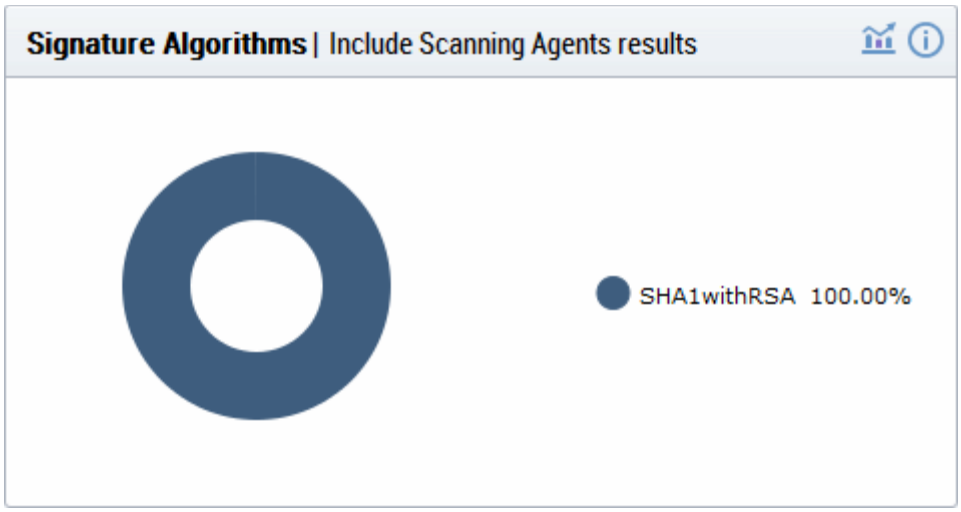
- The **Common Name** column contains the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- The **Organization** column contains the name of the organization that has been issued with the certificate.
- The **Department** column contains the specific 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.
- The **Expires** column contains the date of the certificate expiry.

- The **Key Algorithm** column displays the type of algorithm used, by the public and private keys, for encryption. For example, RSA, DSA, EC, and so on.
- The **Key Size** column displays the key size used, on the public and private keys, for encryption. For example, 1024, 2048, 4096, and so on.

NOTE: Issued certificates are displayed in blue.

2.4.13 The Signature Algorithm Chart

The **Signature Algorithm** 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 a 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.



Hovering the cursor over a chart legend or section displays the exact number of certificates using a particular signature algorithm and their percentage of the total certificates. Clicking the chart icon displays a report with the breakdown of the chart statistics, as the following illustration shows.

COMMON NAME	ORGANIZATION	DEPARTMENT	EXPIRES	SIGNATURE ALGORI
abcdcomp.com	ABCD Company		03/10/2016	SHA1withRSA
elegantamp.com	Elegant			
abcdcorp.com	ABCD Company			
abcdmail.com	ABCD Company			
bestorg.com (renewed)	Best Organization		11/02/2015	SHA1withRSA

5 rows/page 1 - 5 out of 11

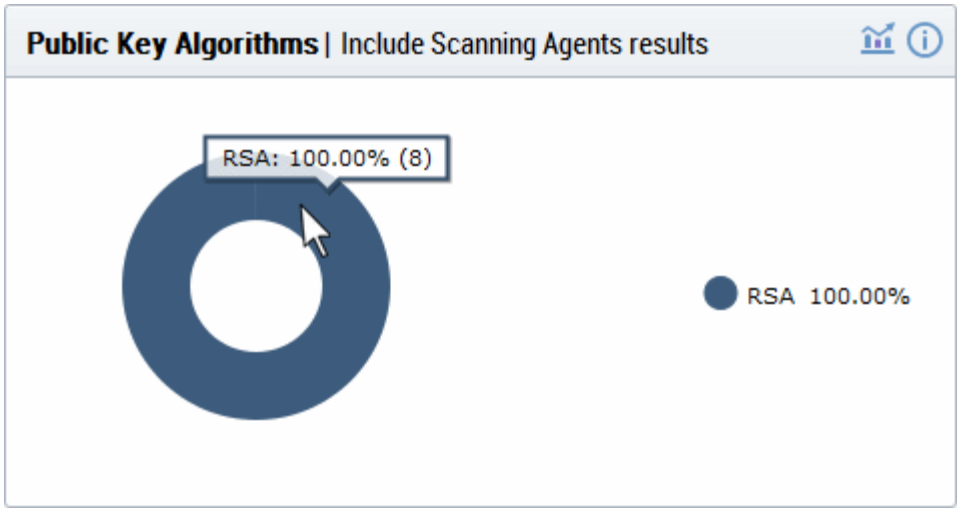
Close

The following information is available:

- The **Common Name** column contains the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- The **Organization** column contains the name of the organization that has been issued with the certificate.
- The **Department** column contains the specific 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.
- The **Expires** column contains the date of the certificate expiry.
- The **Signature Algorithm** column displays the type of signature algorithm used by the certificate. For example, SHA1 with RSA, SHA 256 with RSA,S HA384 with RSA, and so on.

2.4.14 Public Key Algorithm

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



Hovering the cursor over a chart legend or section displays the exact number of certificates using a particular public key algorithm and their percentage of the total certificates. Clicking the chart icon displays a report with the breakdown of the chart statistics, as shown in the following illustration.

COMMON NAME	ORGANIZATION	DEPARTMENT	EXPIRES	SIGNATURE ALGORI	KEY ALG
abcdcomp.com	ABCD Company		03/10/2016	SHA1withRSA	RSA
elegantamp.com	Elegant				
abcdcorp.com	ABCD Company				
abcdmail.com	ABCD Company				
bestorg.com (renewed)	Best Organization		11/02/2015	SHA1withRSA	RSA

5 rows/page 1 - 5 out of 11

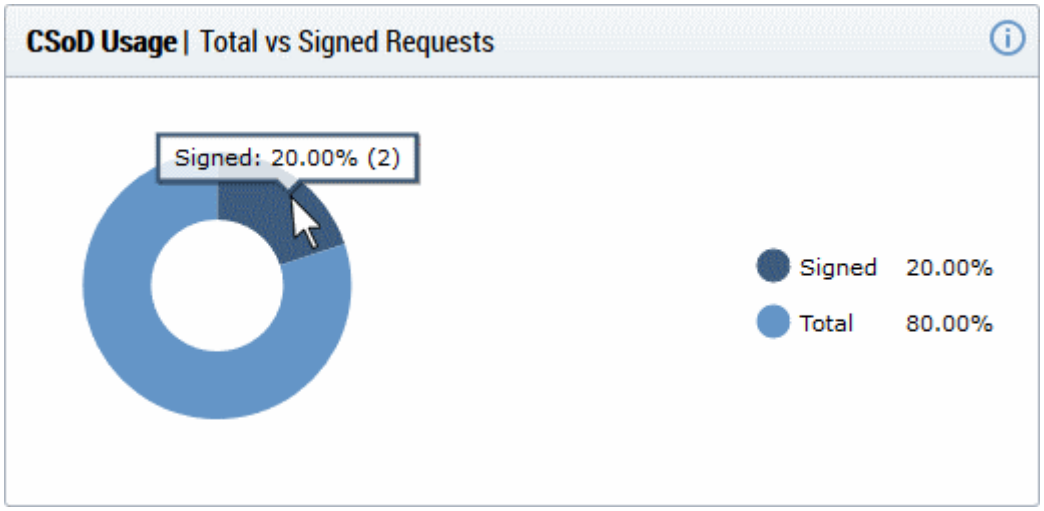
Close

The following information is available:

- The **Common Name** column contains the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- The **Organization** column contains the name of the organization that has been issued with the certificate.
- The **Department** column contains the specific 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.
- The **Expires** column contains the date of the certificate expiry.
- The **Signature Algorithm** column displays the type of signature algorithm used by the certificate. For example, SHA1 with RSA, SHA 256 with RSA,S HA384 with RSA, and so on.
- The **Key Algorithm** column displays the type of algorithm used, by the public and private keys, for encryption. For example, RSA, DSA, EC, and so on.

2.4.15 CSoD Usage

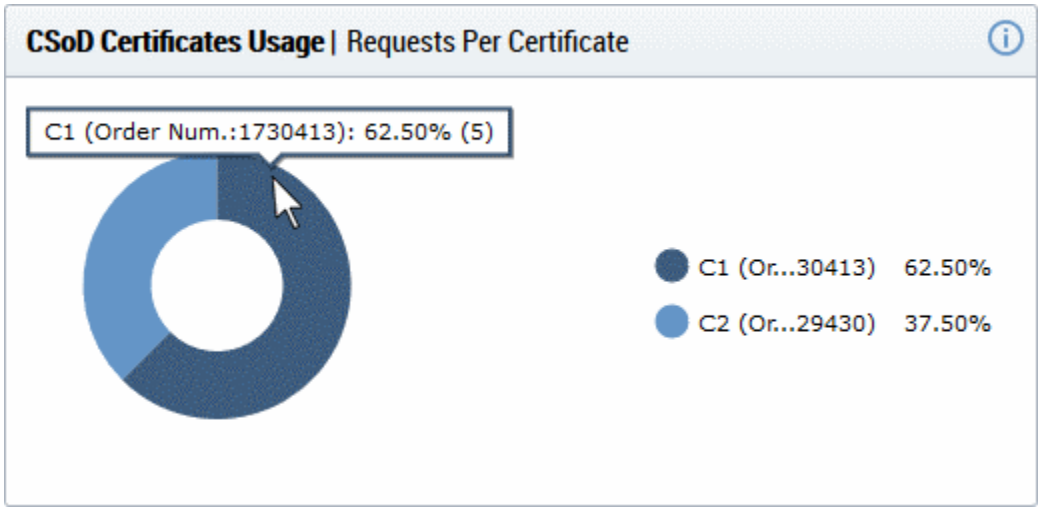
The **CSoD Usage** chart shown in the following illustration displays the number of CSoD requests received and the number of those that were eventually signed.



Hovering the cursor over a chart section displays the percentage and the exact number of requests in a particular category.

2.4.16 The CSoD Certificates Usage Chart

The **CSoD Certificates Usage** chart shown in the following illustration displays the CSoD requests broken down by signing certificate.



Hovering the cursor over a chart section displays the certificate order number, percentage, and the exact number of requests signed with that certificate.

3

Managing Certificates

This chapter describes how to use the certificate management UI and explains the processes behind the administration and provisioning of various types of certificates.

This chapter describes the following topics:

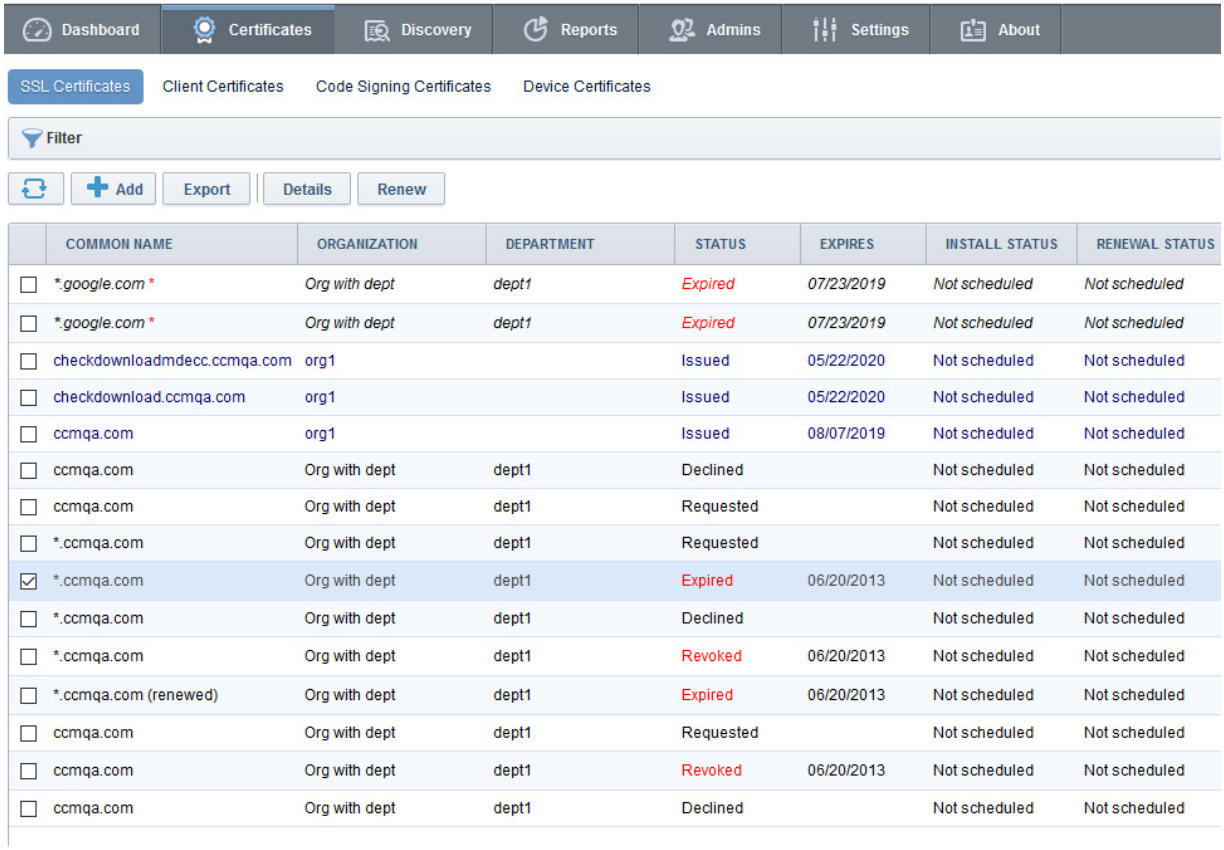
- Certificate Management Overview
- Managing SSL Certificates
- Managing Client Certificates
- Managing the Code Signing Certificates
- Managing Device Certificates

3.1 Certificate Management Overview

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

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

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

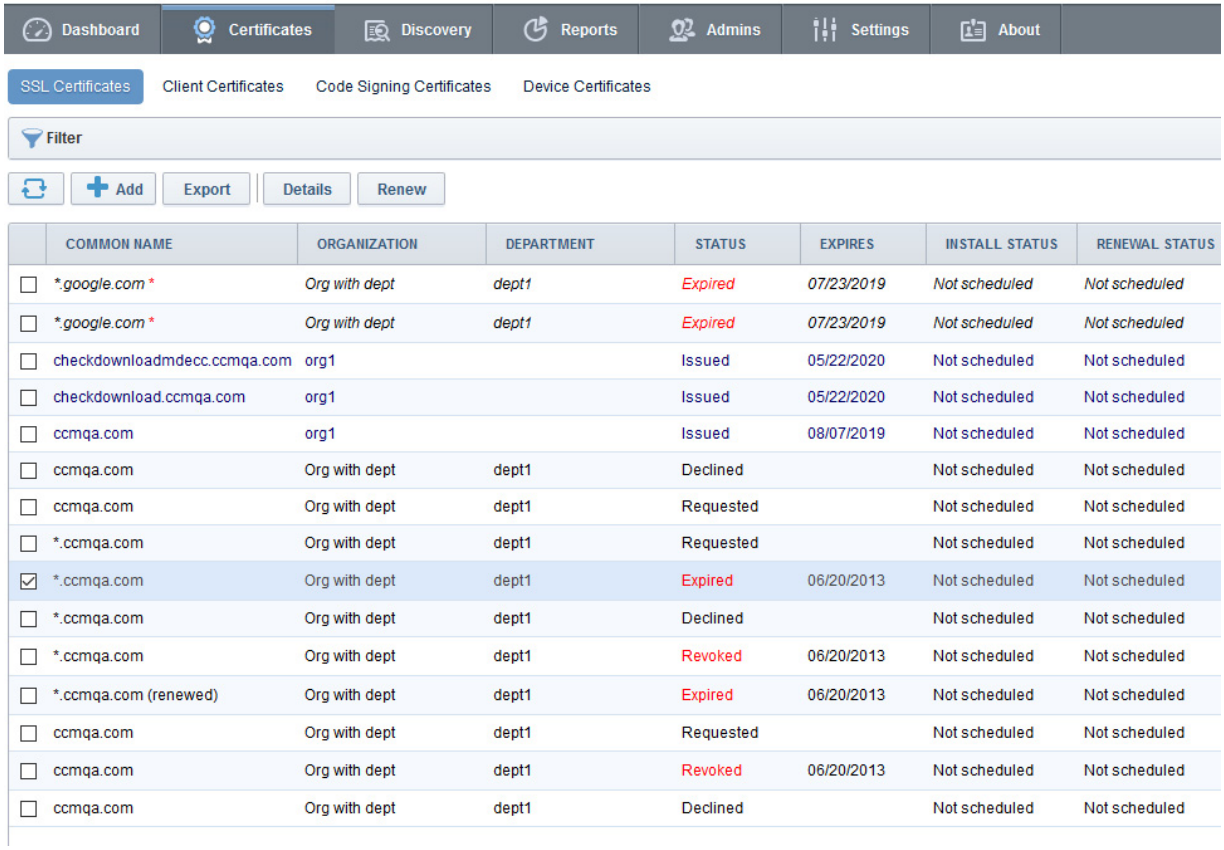


In addition to using the **Certificates** UI, you can run a discovery scan on your servers to audit and monitor the entire network for all installed SSL certificates, including certificates issued by vendors other than Sectigo. Once completed, the discovered certificates are automatically imported into the **Certificates** area. For more information, see "Performing Certificate Discovery Tasks" on page 525.

3.2 Managing SSL Certificates

The **SSL Certificates** area shown in the following illustration provides MRAOs, nominated RAO SSL, and nominated DRAO SSL administrators with the information and controls necessary to manage the lifecycle 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 parameters are available for SSL certificates:

- The **Common Name** column contains the domain name that was used during the SSL certificate request. This domain name refers to the **Common Name** in the SSL certificate itself.
- The **Organization** column contains of the name of the organization that requested or has been issued with the certificate listed in the **Common Name** column.
- The **Department** column contains the specific 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.
- The **Status** column contains the current status of the certificate, which may be one of the following:
  - **Requested**—A certificate application was made for auto-installation or using either the self-enrollment form or the built-in application form. Once the applicant has requested the certificate, their request appears in the **SSL Certificates** area with a Requested status. You can view, edit, approve, or decline this request. A certificate can be requested by (1) an applicant using the self-enrollment form; (2) a MRAO administrator, for any organization or department, using auto-installation tool, self-enrollment form, or the built-in application form; (3) a RAO SSL administrator, for organizations and departments of which they have been delegated control; they can use the auto-installation tool, self-enrollment form, or the built-in application form; (4) a DRAO SSL administrator, for departments of which they have been delegated control; they can use the auto-installation tool, self-enrollment form, or the built-in application form.
  - **Approved**—A certificate request that was made using the auto-installation tool or self-enrollment form has been approved by one of (1) a MRAO 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.

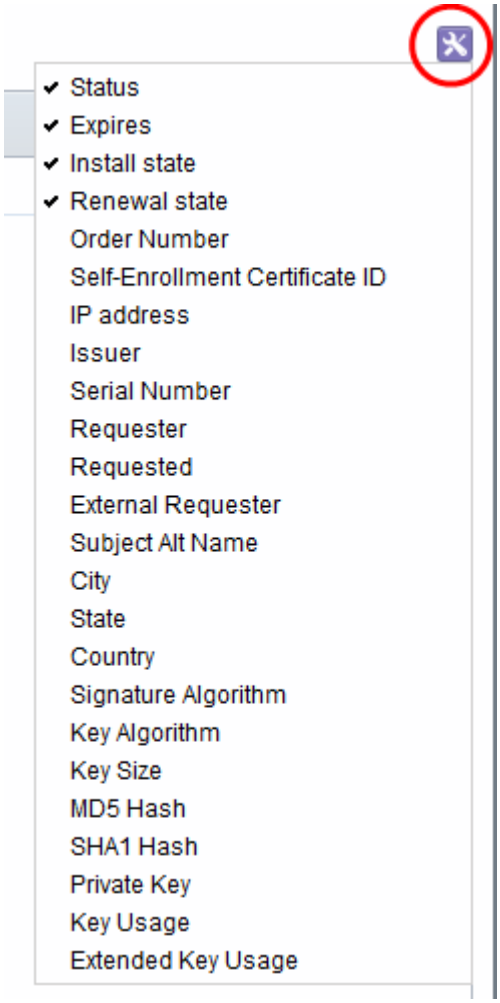
- **Applied**—The request has been sent to the CA for validation.
- **Issued** (*n* is a number of found certificates)—The certificate was issued by Sectigo and collected by the certificate manager. A blue Issued status indicates that the certificate was issued by a CA but has not been installed. Placing the cursor over the **Common Name** column shows the name of the vendor associated with this certificate. A number in parentheses to the right of the certificate's status indicates the number of servers on which this specific certificate is installed. Placing a cursor over the **Status** column triggers the display of all IP address and port combinations on which this certificate was found.
- **Revoked**—The certificate is invalid because it has been revoked. Placing the cursor over the **Common Name** column shows the name of the vendor that is associated with this certificate. A number in parentheses to the right of the certificate's status indicates the number of servers on which this specific certificate is installed. Placing a cursor over the **Status** column triggers the display of all IP address and port combinations on which this certificate was found.
- **Declined**—A certificate request that was made using the self-enrollment form or the built-in application form has been rejected by one of (1) a MRAO administrator who can decline any certificate requests from any organization or department; (2) a RAO SSL administrator who can decline certificate requests for organizations over which they have been delegated control; (3) a DRAO SSL administrator who can decline certificate requests for departments over which they have been delegated control.
- **Invalid**—The CA did not process the certificate request because of an error the applicant made in the enrollment form (for example, a Certificate Signing Request (CSR) contains incorrect information).
- **Rejected**—The CA rejected the request after a validation check.
- **External** (*n* is a number of found certificates)—Certificates were detected by a network discovery scan but had not been ordered and issued through SCM, including any pre-existing Sectigo certificates that may have been ordered from the website or partner APIs. A red External status indicates that the certificate's term has expired. Placing the cursor over the **Common Name** column shows the name of the vendor associated with this certificate. A number in parentheses to the right of the certificate's status indicates the number of servers on which this specific certificate is installed. Placing a cursor over the **Status** column triggers the display of all IP address and port combinations on which this certificate was found.

- The **Expires** column contains the date when the certificate expires.
- The **Install Status** column indicates the current status 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.
- The **Renewal Status** column indicates the current status 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.
- The **Order Number** column contains the order number of the certificate request, as assigned by the CA when the request was made.
- The **Self-Enrollment Certificate ID** column displays the unique enrollment ID assigned to the certificate request.
- The **IP Address** column contains all the IP address and port combinations on which the certificate is installed.
- The **Issuer** column contains details of the CA that issued the certificate, as well as the name of the certificate.
- The **Serial Number** column contains the serial number of the certificate that is unique and can be used to identify the certificate.
- The **Requester** column contains the name of the SCM administrator that has requested the certificate through the auto-install tool, or the built-in enrollment form, or email of the end-user who has requested the certificate through the self-enrollment form.
- The **Requested** column contains the date of the certificate request.
- The **External Requester** column contains the email address of the external requester on behalf of which the administrator has requested the certificate through the built-in enrollment form. 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. This behavior is subject to any **External Requester** constraints configured for the specified organization.
- The **Subject Alt Name** column contains the domains names for which the certificate is used.
- The **City** column contains the name of the city entered when the organization or department was created.
- The **State** column contains the name of the state or province entered when the organization or department was created.
- The **Country** column contains the name of the country entered when the organization or department was created.
- The **Signature Algorithm** column contains the signature algorithm of the certificate public key.
- The **Key Algorithm** column contains the type of algorithm used for the encryption.
- The **Key Size** column contains the key size used by the certificate for encryption.
- The **MD5 Hash** column contains the MD5 hash (thumb print or fingerprint) for the certificate.
- The **SHA1 Hash** column contains the SHA1 hash (thumb print or fingerprint) for the certificate.
- The **Private Key** column indicates whether or not the certificate private key is managed by SCM.
- The **Key Usage** column contains the cryptographic purposes for which the certificate can be used. For example, key encipherment and signing.
- The **Extended Key Usage** column indicates the higher level capabilities of the certificate. For example, web server authentication and client authentication.
- The control buttons of various types are displayed above the column header and depend on the status of the selected certificate, as follows:
    - **Details** allows you to view information about the certificate. For more information, see "How to View and Modify SSL Certificate Details" on page 52.
    - **Revoke** revokes the certificate.

- **Install** activates the auto-installer tool to install the certificate on the target web server. For more information, see "How to Request and Issue SSL Certificates to Web Servers and Hosts" on page 67.
- **Replace** replaces the existing certificate with a new one, after prompting you to specify a new CSR.
- **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.
- **Decline** declines the certificate request. This request is not sent to Sectigo for processing.
- **Edit** allows you to modify SSL certificate parameters. This option is available only for certificates with a status of Requested, Rejected, or Invalid.
- **Renew** opens the **Renew Certificate** dialog prepopulated 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 in the status of Issued, Expired, and External.
- **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 125.

NOTE: You can add more column headers from the drop-down button beside the last item in the column, as shown in the following illustration.

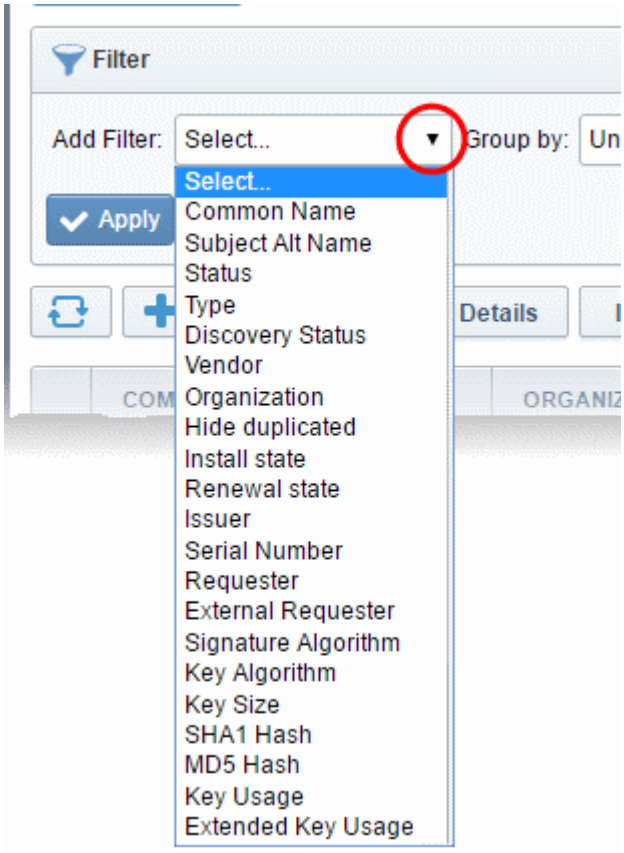


3.2.1 How to Sort and Filter SSL Certificates

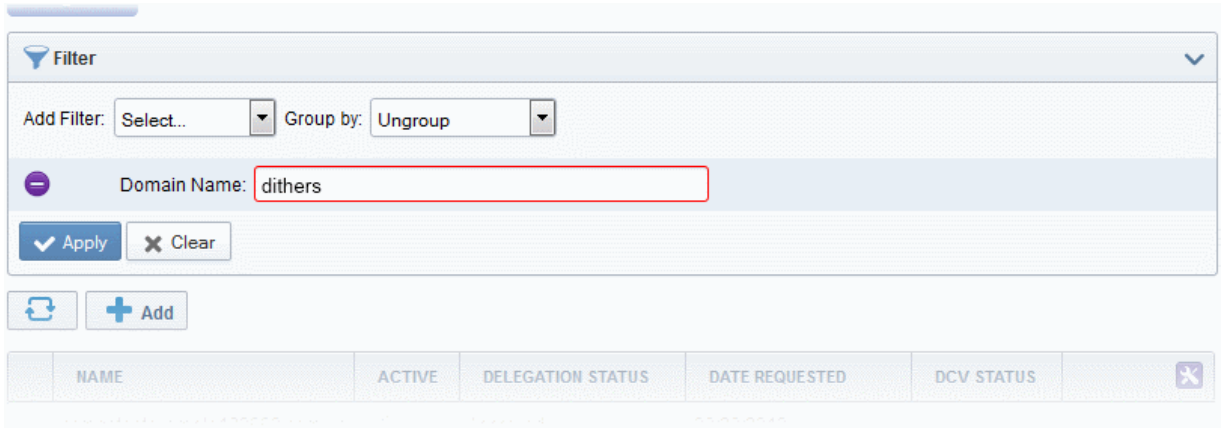
You can sort items in order of the entries in the column by clicking a column header, and you can use filters to search for particular SSL certificates.

You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.

To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appear depending on the selection from the **Add Filter** list.



Then you enter or select the filter parameter as per the selected criteria.



The following are the available filter criteria and parameters:

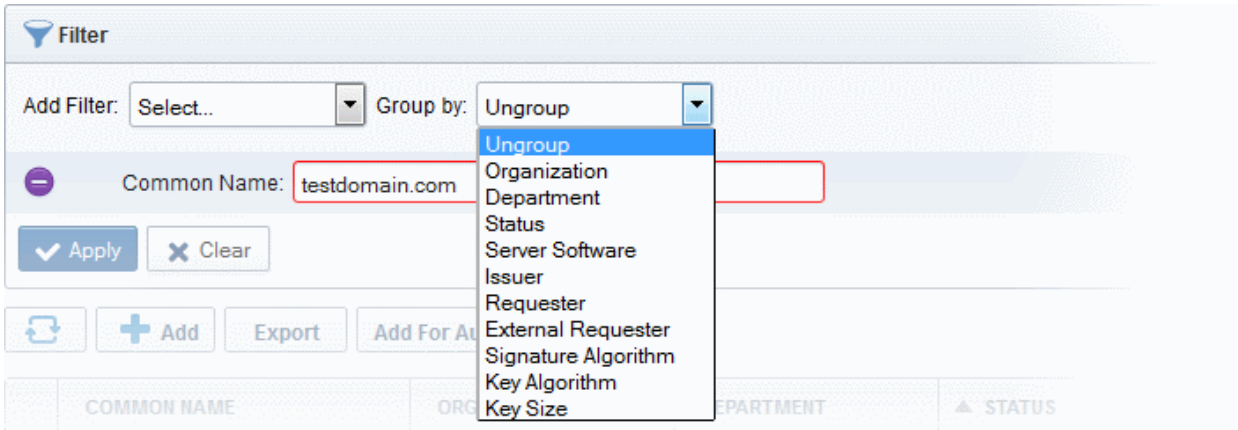
- **Common Name**—The common name or domain name for the certificate, full or in part.
- **Subject Alt Name**—The subject alternative name for the certificate, full or in part.
- **Status**—The status of the certificate, as per the value in the status list.
- **Type**—The type of the certificate, as per the value in the type list.

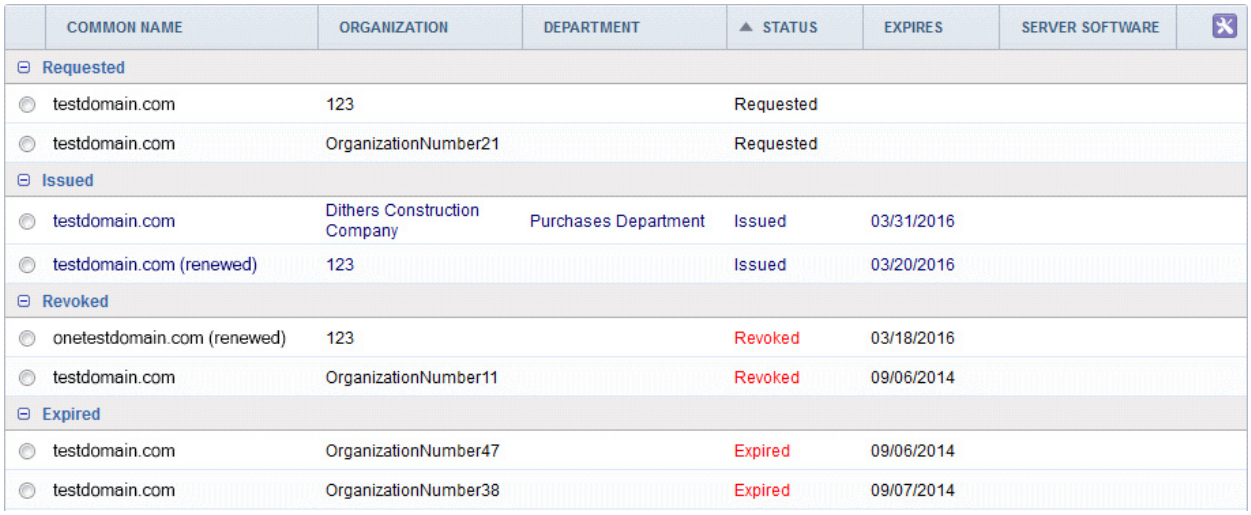
- **Discovery Status**—The status indicating whether or not the certificate is deployed, as per the value in the discovery status list.
- **Vendor**—The CA, as per the value in the vendor list.
- **Organization**—The organization or department to which the certificate belongs, as per values in the organization and department lists.
- **Hide Duplicated**—If selected, removes duplicate certificates from the list.
- **Issuer**—The name of the certificate issuer.
- **Serial Number**—The serial number of the certificate, in full or part.
- **Requester**—The name of the SCM administrator that has requested the certificate through the auto-install tool, the built-in enrollment form, or email of the end-user that requested the certificate through the self-enrollment form, in full or in part.
- **External Requester**—The email address of the external requester on whose behalf the administrator has requested the certificate through the built-in enrollment form, in full or part.
- **Signature Algorithm**—The signature algorithm of the certificate.
- **Key Algorithm**—The key algorithm of the certificate.
- **Key Size**—The key size in bits.
- **SHA1 Hash**—The SHA1 Hash (thumb print or fingerprint) of the certificate.
- **MD5 Hash**—The MD5 Hash (thumb print or fingerprint) of the certificate.
- **Key Usage**—Filters certificates by cryptographic capabilities.
- **Extended Key Usage**—Filters certificates by higher-level purpose. For example, web server authentication.

NOTE: You can add more than one filter at a time to refine the filtering. To remove a filter criterion, click minus (-) located to the left of the filter.

Using the **Group by** list shown in the following illustration, you can select the criteria by which the results are to be grouped. For example, to filter the certificates with a specific common name starting with testdomain.com and group the results by their status, select **Common Name** from the **Add Filter** list, enter testdomain.com, and then select **Status** from the **Group by** list. Certificates that contain testdomain.com in their common name are displayed as a list, grouped based on their status.

You can remove the filter options by clicking **Clear**.





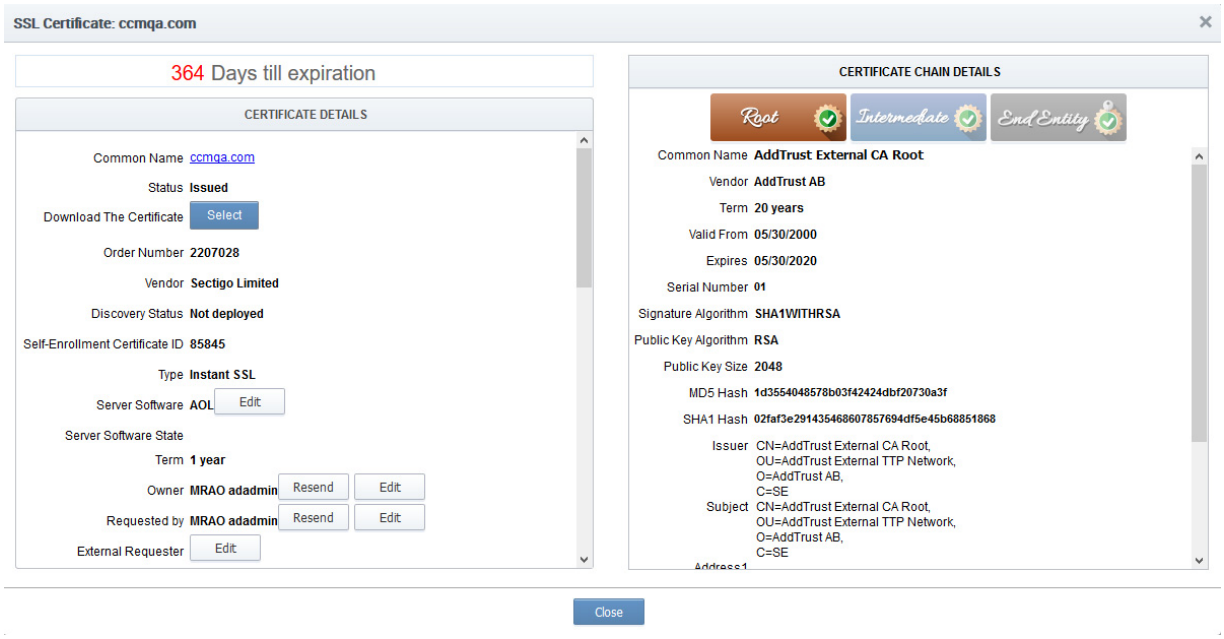
COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	SERVER SOFTWARE
Requested					
testdomain.com	123		Requested		
testdomain.com	OrganizationNumber21		Requested		
Issued					
testdomain.com	Dithers Construction Company	Purchases Department	Issued	03/31/2016	
testdomain.com (renewed)	123		Issued	03/20/2016	
Revoked					
onetestdomain.com (renewed)	123		Revoked	03/18/2016	
testdomain.com	OrganizationNumber11		Revoked	09/06/2014	
Expired					
testdomain.com	OrganizationNumber47		Expired	09/06/2014	
testdomain.com	OrganizationNumber38		Expired	09/07/2014	

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **SSL Certificates** screen, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

3.2.2 How to View and Modify SSL Certificate Details

You can view and modify the SSL certificate details as follows:

- In the main UI, select **Certificates** > **SSL Certificates**.
- Select a certificate in the list and click **Details** to open a screen that contains two panels: **CERTIFICATE DETAILS** and **CERTIFICATE CHAIN DETAILS**, as shown in the following illustration. This screen allows you to do the following:
  - Download the certificate in different formats for installation onto servers.
  - Upload the certificate's private key to the SCM's PKS.
  - Download the certificate's private key from the PKS.
  - View the full certificate chain and installation details.
  - Resend the notification email to the requester of the issued certificate.
  - Restart Apache after auto-installation of the certificate.
  - Update the auto-renewal status.



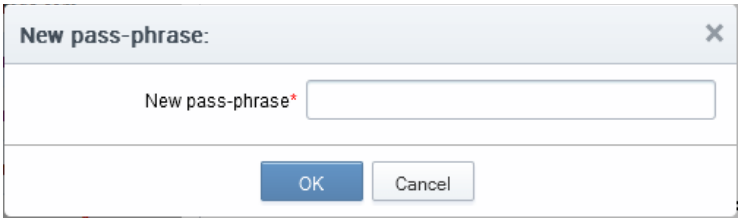
3.2.2.1 Using the Certificate Details Panel

The top portion of the **CERTIFICATE DETAILS** panel displays the number of days remaining before the certificate expires. The lower portion shows the SCM-related and server-related information about the certificate and contains other controls. The contents of the **CERTIFICATE DETAILS** panel is dependent on the current status of the certificate.

The following table lists all the possible settings and elements of the **CERTIFICATE DETAILS** panel.

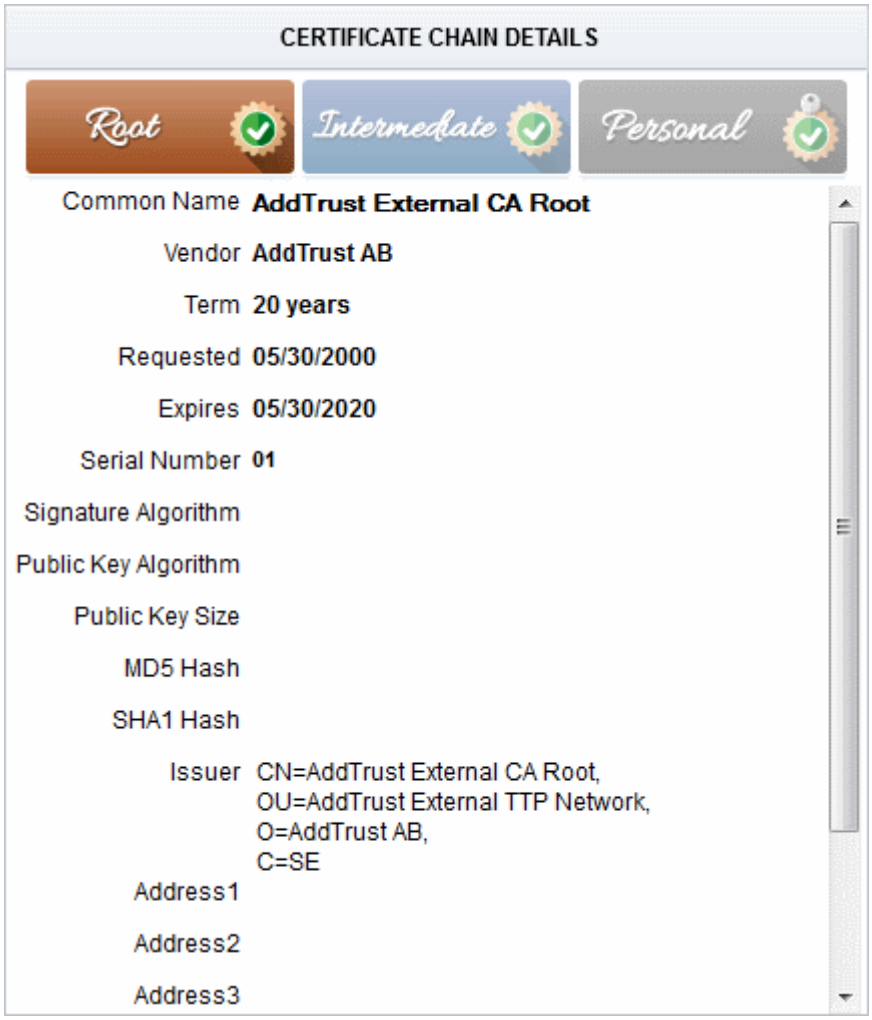
Field	Description
Common Name	The domain name that was used during the SSL certificate request. This domain name refers to the common name in the SSL certificate itself.
Status	The status of the certificate.
Download	Allows to download the certificate in different formats.
Private Key	For certificates enrolled by manually entering the CSR, allows you to upload the certificate's private key to the PKS. For certificates requested via by SCM and whose keys are managed by the private key store, allows you to download the private key of the certificate in a `.key` 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.
Passphrase	The passphrase of the certificates enrolled by auto-generation of CSR by SCM and whose keys are managed by PKS. 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 a `.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 and configured.

Order Number	The order number of the certificate request.
Vendor	A vendor that is associated with the certificate. The vendor setting for self-signed SSL certificates is Self-Signed.
Discovery Status	The following are valid values: • Deployed—A certificate that is installed on the network (as found by the certificate discovery scan). • Not Deployed—Any certificate that is listed in the **SSL Certificates** area but which was not detected as installed on the network during a certificate discovery scan.
Self-Enrollment Certificate ID	The unique identifier of the certificate.
Type	The brand name of the certificate.
Server Software	The server type for which the certificate was issued. Clicking **View** allows you to view the installation status of the deployed certificate. Clicking **Edit** allows you to change the server software for which the certificate is intended.
Server Software State	The status of the server on which the certificate is installed.
Term	The length of time during which the certificate is to be valid, from the time of issuance. For certificates that have not yet been approved, this is the certificate lifetime that was requested during the application process.
Owner	The name of the certificate owner, who is typically the administrator that first approved the request for the certificate.
Requested by	The email address of the end-user who requested this certificate through the self-enrollment application form or The name of the administrator who requested this certificate using the auto-install tool or built-in application form.
External Requester	The email address of the applicant 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. This behavior is subject to any **External Requester** constraints configured for the specified organization.
Requested	The date when the certificate was requested.
Approved	The date when the certificate was approved.
Expires	The date when the certificate expires.
Comments (optional)	The information for administrator.

Organization	The name of the organization on whose behalf the certificate was requested.
Department	The name of the department on whose behalf the certificate was requested.
Address 1: Address 2: Address 3: City: State or Province: Postal Code:	The address of the organization as entered while requesting the certificate. Only those address fields that were allowed to be displayed while applying for the certificate are shown. The remaining fields are displayed as Details Omitted.
Serial Number	The serial number of the issued certificate.
Signature Algorithm	The signature algorithm of the public key of the certificate.
Public Key Algorithm	The encryption algorithm of the public key of the certificate.
Public Key Size	The key length of the public key in bits.
Revoked	The date when the certificate was revoked (if applicable).
MD5 Hash	The MD5 Hash (thumb print or fingerprint) value of the certificate.
SHA1 Hash	The SHA1 Hash (thumb print or fingerprint) value of the certificate.
Key Usage	The cryptographic purpose for which the certificate can be used. For example, key encipherment and signing.
Extended Key Usage	Higher level capabilities of the certificate. For example, web server authentication.
Change Passphrase	New or modified self-enrollment passphrase of the certificate. This phrase is required to revoke certificates should the situation arise. 
Auto-renewal	Option to automatically renew the certificate. The auto-renewal can be enabled or disabled by clicking Edit.

3.2.2.2 Using the Certificate Chain Details Panel

The **CERTIFICATE CHAIN DETAILS** panel shown in the following illustration displays the details of the root and intermediate certificates linked to the SSL certificate chain. Clicking **Root**, **Intermediate**, and **Personal** displays the certificate details of the Root, Intermediate, and the self-SSL certificate respectively.



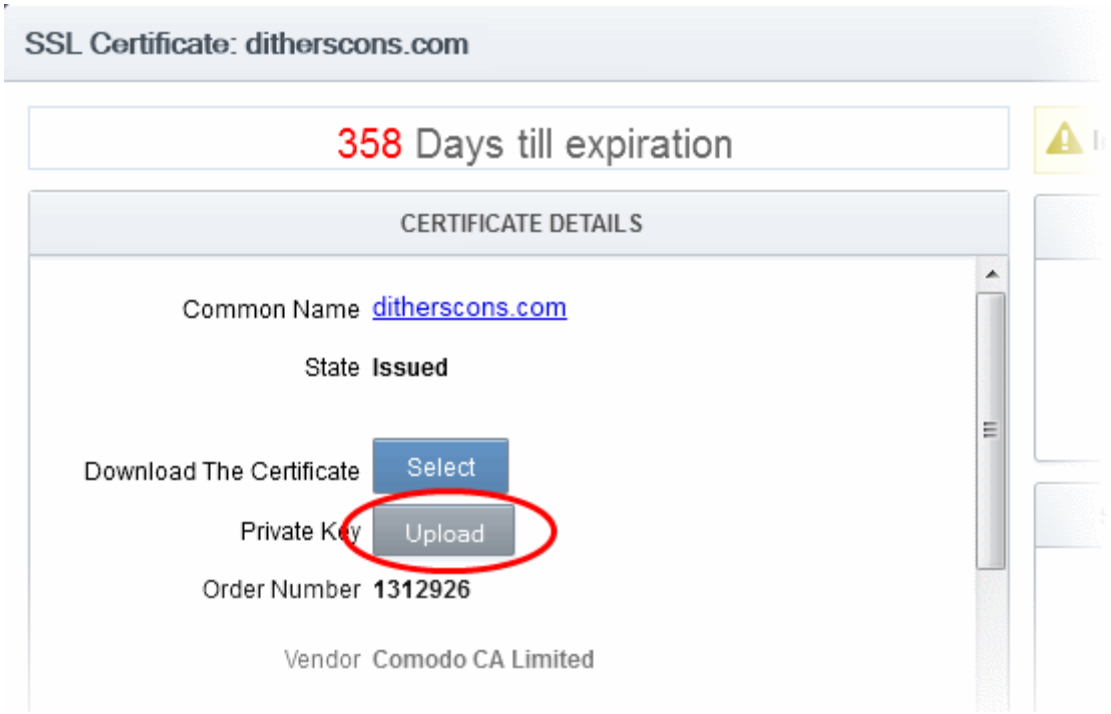
3.2.2.3 Uploading a Certificate Private Key for Storage and Management by the PKS

The **CERTIFICATE DETAILS** area for the issued SSL certificates allows you to upload the private key associated with this certificate with the purpose of its storage and management by the PKS configured in their local network. Managing the private key in the PKS facilitates the following:

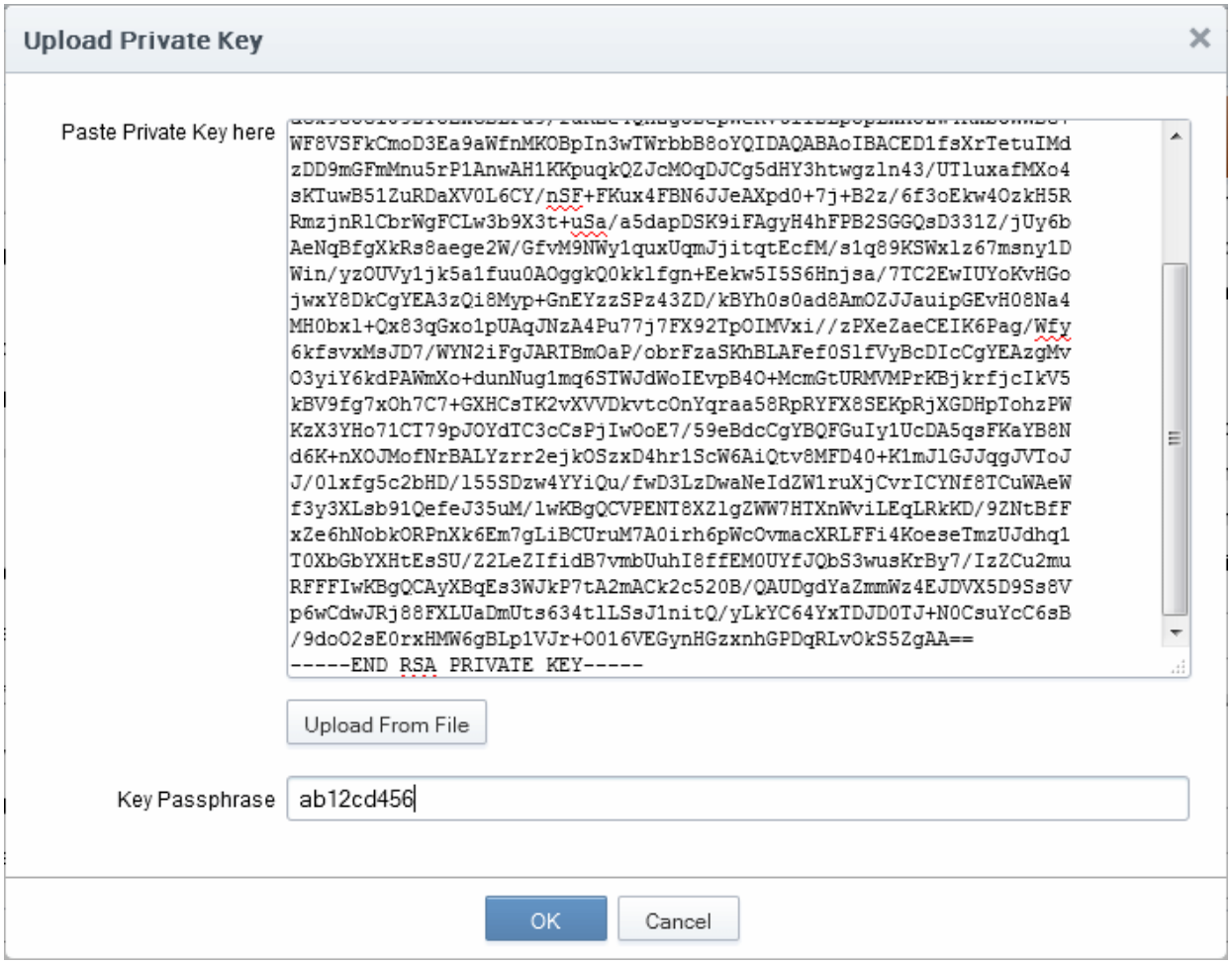
- Downloading the certificate in a `.pfx/.p12` format for importing to any server.
- Automatic uploading of the CSR during the certificate renewal process.

Prior to using this functionality, ensure that your account has been enabled for the PKS. The Private Key Agent should have been installed on your local network and configured by navigating to **Settings** > **Private Key Store**. For more information, see "Configuring Settings" on page 321.

As shown in the following illustration, the **CERTIFICATE DETAILS** panel for an issued SSL certificate displays **Upload** to the right of the **Private Key** field.

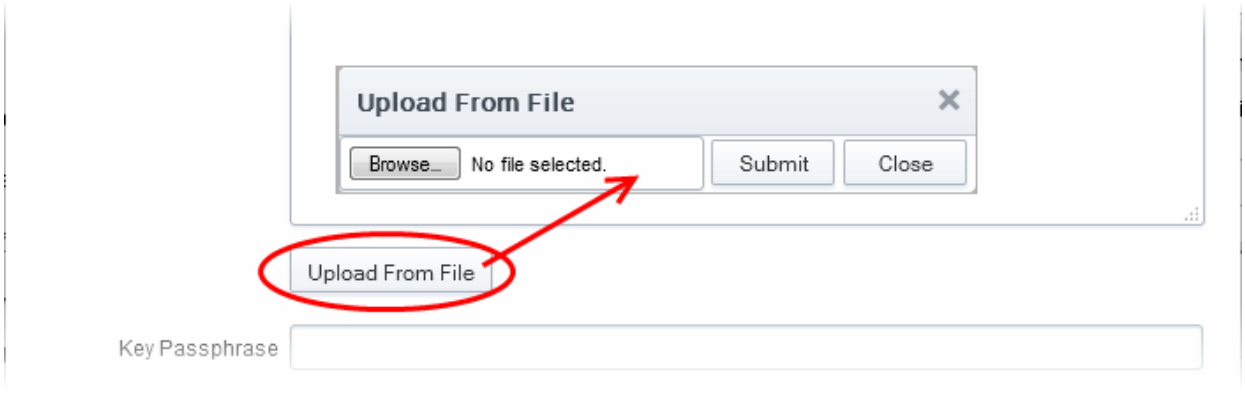


Clicking **Upload** opens the **Upload Private Key** dialog shown in the following illustration.



You use this dialog as follows:

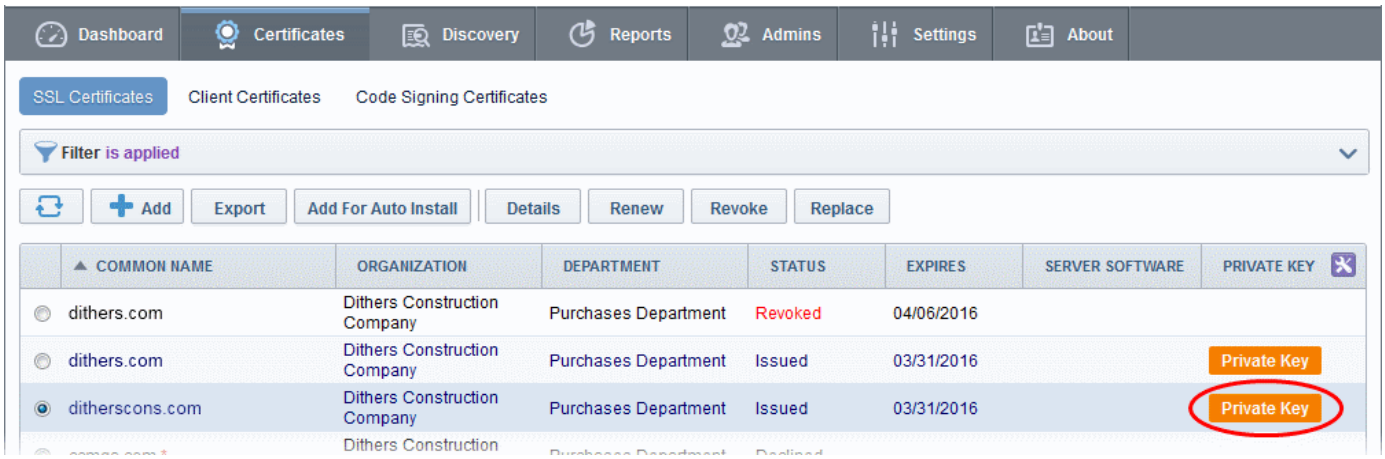
- Enter the private key associated with the certificate by either directly pasting it in the **Paste Private Key here** field, or saving it as a text file and then uploading this file via **Upload From File**, as the following illustration shows.



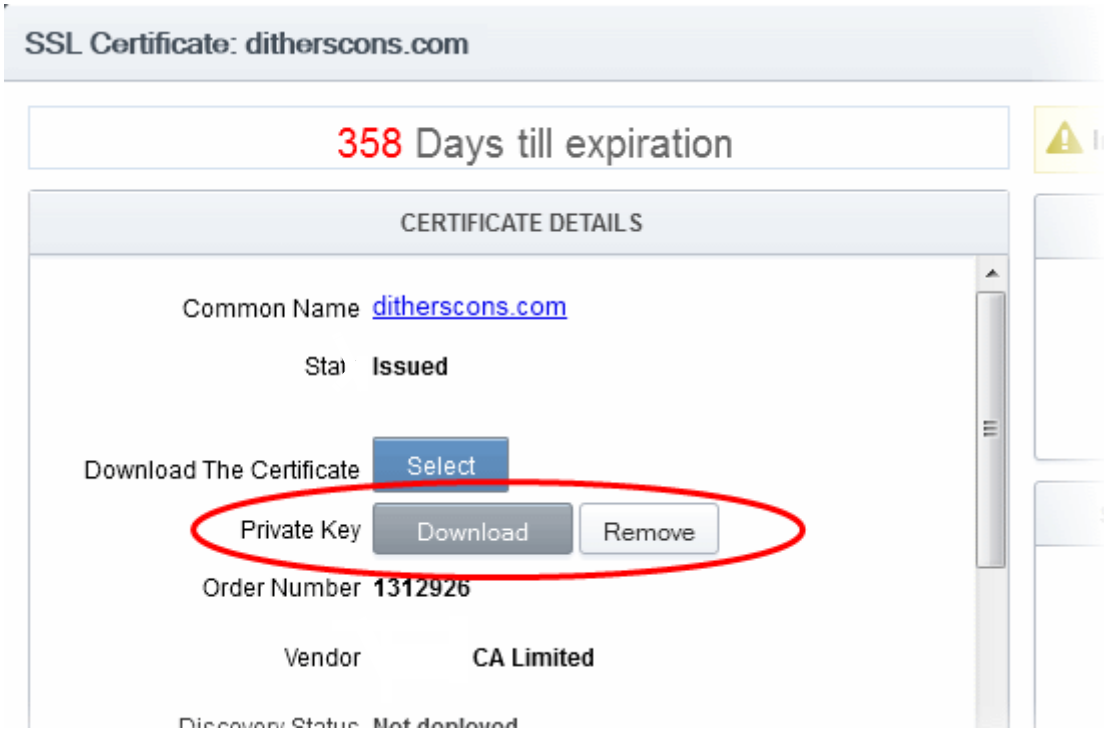
- Enter a passphrase for the key. The passphrase is required for importing the certificate with the key pair to the server for installation.

- Click **OK** and close the dialog.

Upon completion of the preceding procedure, SCM sends a command to the agent to store the private key, therefore making this key available for management by the PKS, which is indicated by the **Private Key** label displayed in the **Private Key** column in the **SSL Certificates** screen, as shown in the following illustration.



In addition, you can download the private key from the **CERTIFICATE DETAILS** panel, as the following illustration shows.



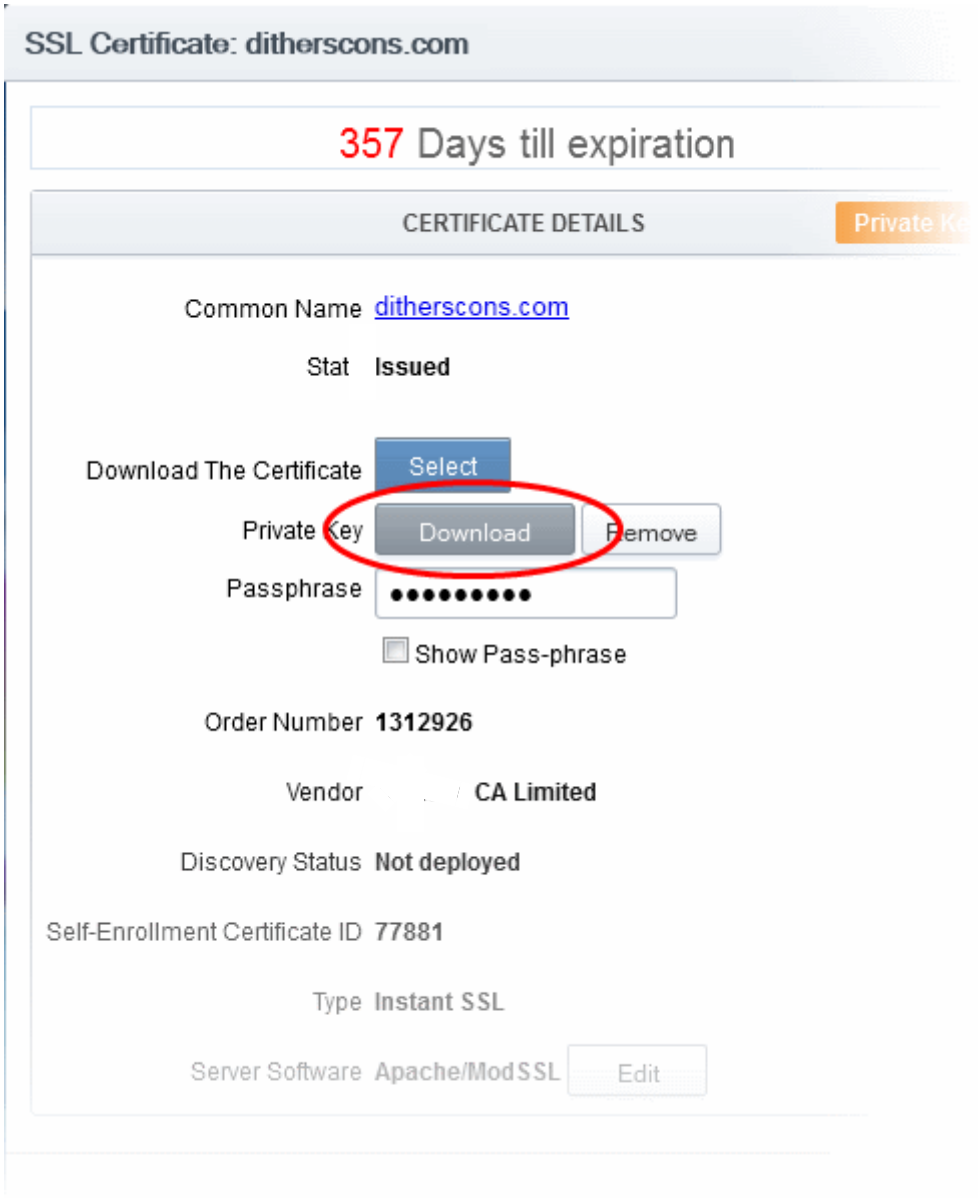
3.2.2.4 Downloading an SSL Certificate Private Key

The details screen for SSL certificates whose private keys are stored in PKS and managed by it allows you to download the private key in the `.key` format. This includes certificates applied

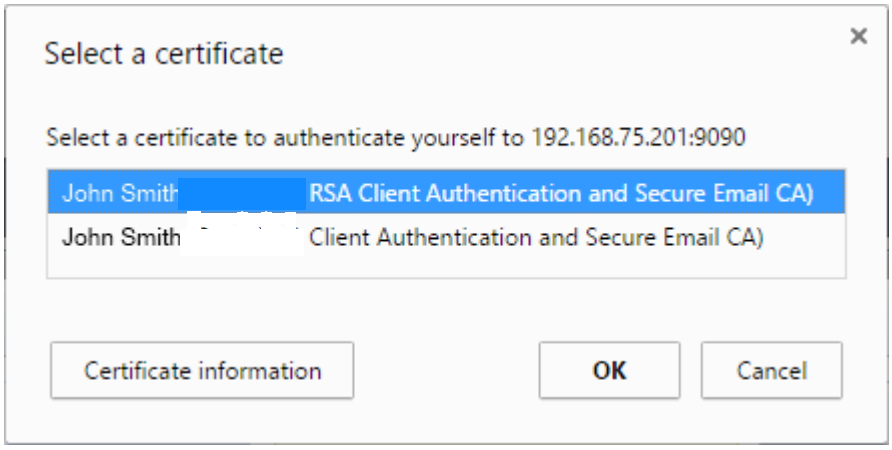
using the auto-CSR generation tool in SCM (see "Automatic CSR Generation Via the Built-in Enrollment Wizard" on page 96) and certificates for which the private keys were manually uploaded to the PKS (see "Uploading a Certificate Private Key for Storage and Management by the PKS" on page 56).

In order to download a private key, you should have been logged in to SCM through a computer in the same local network on which the Private Key Agent is installed. In addition, there should be a personal authentication certificate installed on this computer. During the download process, SCM sends a download command to the Private Key Agent which, in turn, requests for your authentication and checks for authentication certificate. Once authenticated, the Private Key Agent enables you to download the private key in the `.key` format directly from it, without uploading it to SCM. This ensures that the private key does not leave your network, though SCM initiates the download.

As shown in the following illustration, the **CERTIFICATE DETAILS** panel for an SSL certificate managed by PKS displays **Download** to the right of the **Private Key** field.



Clicking **Download** sends a command to the Private Key Agent, which, in turn, requests an authentication and searches for your personal authentication certificate in the computer from which you logged in. If more than one certificate is found, the **Select a certificate** dialog shown in the following illustration is displayed allowing you to choose the certificate.



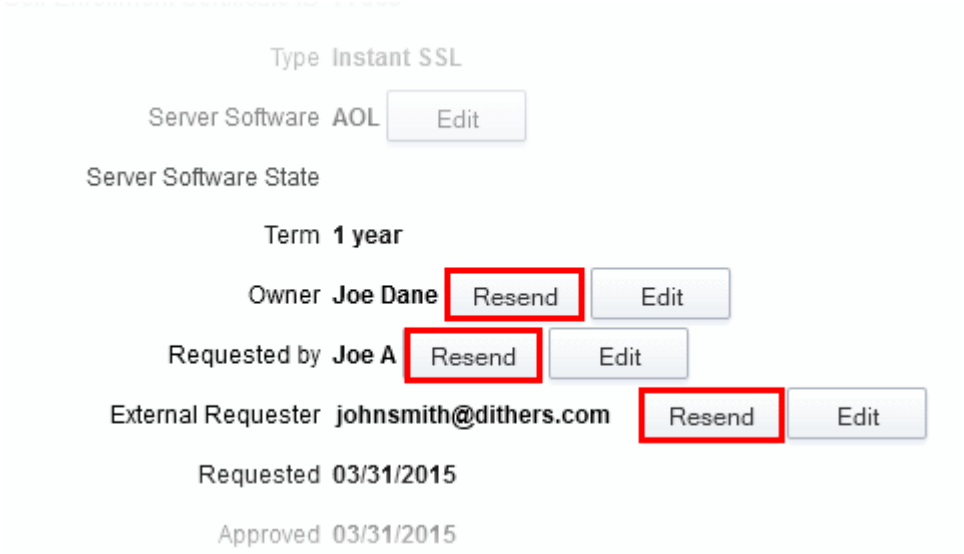
Upon authentication verification, the download dialog is displayed, enabling you to download the private key.

3.2.2.5 Resending Notification Email for Issued SSL Certificates

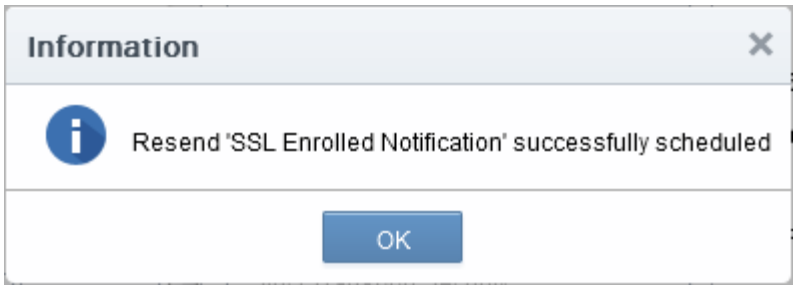
The **CERTIFICATE DETAILS** screen for the issued SSL certificates allows you to resend the certificate enrollment notification to the domain administrator, the applicant that applied for the certificate through the self-enrollment form, or the applicant on whose behalf the administrator has applied for the certificate through the built-in enrollment form.

An automated notification email for collection of certificate is sent to the domain administrator once SCM issues the certificate. However, if the certificate is not downloaded by the domain administrator for a long time, the SCM administrator can resend the notification for certificate collection.

The **CERTIFICATE DETAILS** panel of the details screen for the issued SSL certificates displays **Resend** to the right of the **Owner**, **Requested by**, and **External Requester** (if applicable) fields, as the following illustration shows.



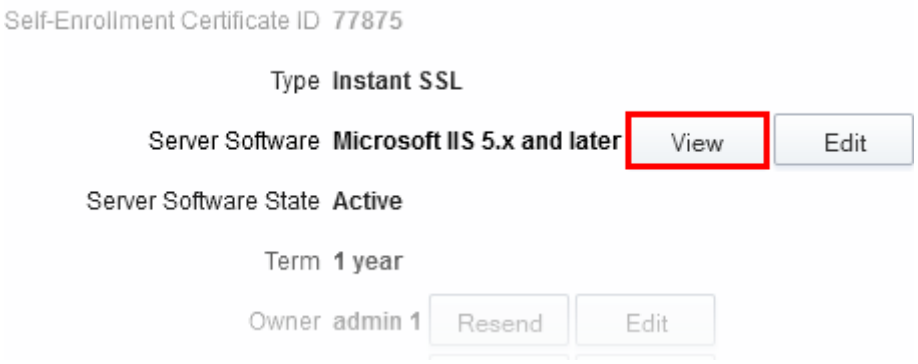
Clicking **Resend** creates a schedule for SCM to resend the notification email and displays the **Information** dialog shown in the following illustration.



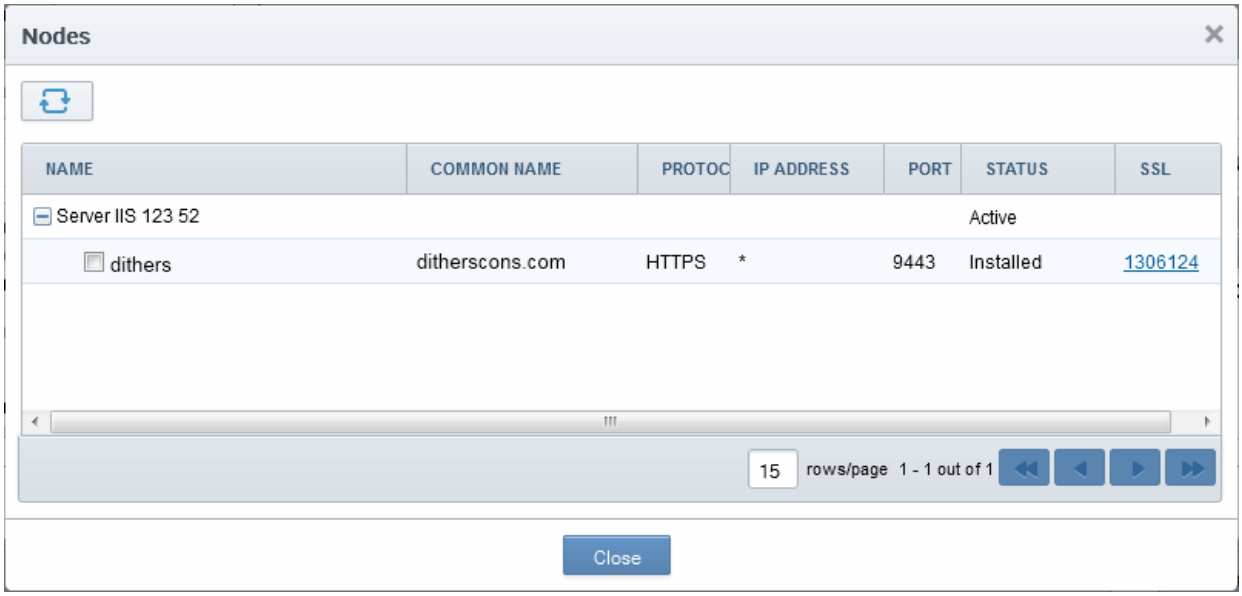
3.2.2.6 Viewing Installation Details of Certificates

The details screen for the SSL certificates added for auto-installation to IIS or Apache allows you to view the installation status of the certificate.

The **CERTIFICATE DETAILS** panel of the details screen for the SSL certificate added for auto-installation displays **View** to the right of the **Server Software** field, as the following illustration shows.

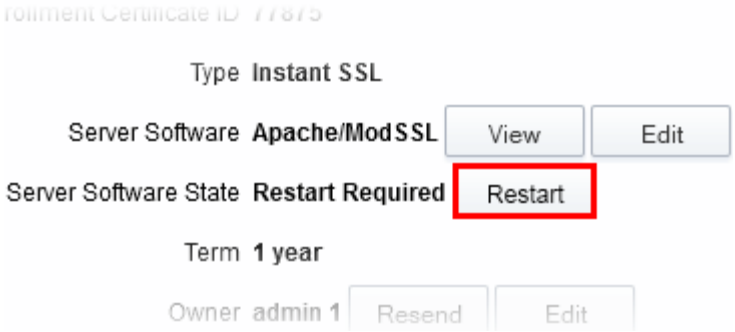


Clicking **View** displays a **Nodes** dialog that provides details on the agent responsible for auto-installation, the node server upon which the certificate is installed, as well as the installation status.



3.2.2.7 Restarting Apache Server After Auto-Installation of SSL Certificates

The Apache server has to be restarted to finalize the installation of a SSL certificate. You can do this remotely from the SCM UI by clicking **Restart** on the **CERTIFICATE DETAILS** panel of the details screen, as shown in the following illustration. After rebooting, the **Server Software State** changes to Active.



3.2.2.8 Updating the Auto-Renewal Status

You can use the details screen to update the auto-renewal status of a certificate as follows:

- In the main UI, navigate to **Certificates** > **SSL Certificates**, select a certificate, and then click **Details**.
- Scroll down the **CERTIFICATE DETAILS** panel and click **Edit** beside the **Auto-renewal** field.
- 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.

For more information, see "Automatic Certificate Renewal Scheduling" on page 125.

3.2.3 About Sectigo SSL Certificate Types and Validation Levels

Sectigo issues SSL certificates with the following validation levels:

- OV certificates that include full business and company validation from a certificate authority using currently established and accepted manual vetting processes.
- EV level allows browsers with the Enterprise Validation support to display more information for EV certificates than for previous SSL certificates.

Sectigo issues the following types of SSL certificates:

- Single Domain Certificates (SDC) secure a single fully qualified domain name.
- Wildcard Certificates (WC) secure the domain and unlimited subdomains of that domain.
- Multi-Domain Certificates (MDC) secure up to 100 different domain names on a single certificate.

The following table describes each Sectigo SSL certificate in accordance to its variant and validation level.

Certificate Name	Variant	Validation Level	Description	Validity Period
Sectigo Trial SSL Certificate	SDC	OV	Secures a single domain.	30 days
Sectigo Intranet SSL Certificate	SDC	OV	Secures a single internal host.	1 year - 3 years
Sectigo InstantSSL Certificate	SDC	OV	Secures a single domain.	1 year - 3 years
Sectigo InstantSSL Pro Certificate	SDC	OV	Secures a single domain.	1 year - 3 years
Sectigo PremiumSSL Certificate	SDC	OV	Secures a single domain.	1 year - 3 years
Sectigo PremiumSSL Wildcard Certificate	WC	OV	Secures domain and unlimited subdomains of that domain.	1 year - 3 years
Sectigo PremiumSSL Legacy Certificate	SDC	OV	Secures a single domain	1 year - 3 years

Certificate Name	Variant	Validation Level	Description	Validity Period
Sectigo PremiumSSL Legacy Wildcard Certificate	WC	OV	Secures domain and unlimited subdomains of that domain.	1 year - 3 years
Sectigo SGC SSL Certificate	SDC	OV	Secures a single domain.	1 year - 3 years
Sectigo SGC SSL Wildcard Certificate	WC	OV	Secures domain and unlimited subdomains of that domain.	1 year - 3 years
EliteSSL Certificate	SDC	OV	Secures a single domain.	1 year - 3 years
GoldSSL Certificate	SDC	OV	Secures a single domain.	1 year - 3 years
PlatinumSSL Certificate	SDC	OV	Secures a single domain.	1 year - 3 years
PlatinumSSL Wildcard Certificate	WC	OV	Secures domain and unlimited subdomains of that domain.	1 year - 3 years
PlatinumSSL Legacy Certificate	SDC	OV	Secures a single domain.	1 year - 3 years
PlatinumSSL Legacy Wildcard Certificate	WC	OV	Secures domain and unlimited subdomains of that domain.	1 year - 3 years
PlatinumSSL SGC Certificate	SDC	OV	Secures a single domain.	1 year - 3 years

Certificate Name	Variant	Validation Level	Description	Validity Period
PlatinumSSL SGC Wildcard Certificate	WC	OV	Secures domain and unlimited subdomains of that domain.	1 year - 3 years
Sectigo Multi-Domain SSL Certificate	MDC	OV	Secures multiple fully qualified domains on a single certificate.	1 year - 3 years
Sectigo EV SSL Certificate	SDC	EV	Secures a single domain.	1 year - 2 years
Sectigo EV SGC SSL Certificate	SDC	EV	Secures a single domain.	1 year - 2 years

3.2.4 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:

- Automatic installation allows you to configure SCM 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 CA, the certificate is collected and automatically installed on the web server. For more information, see "Automatic CSR Generation, Installation, and Renewal of SSL Certificates" on page 102.
- Manual installation allows you or applicants authorized by you to obtain certificates via SCM's 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 Certificate Enrollment Form and Built-In Wizard" on page 70.

Requesting and issuing of SSL certificates typically occurs as follows:

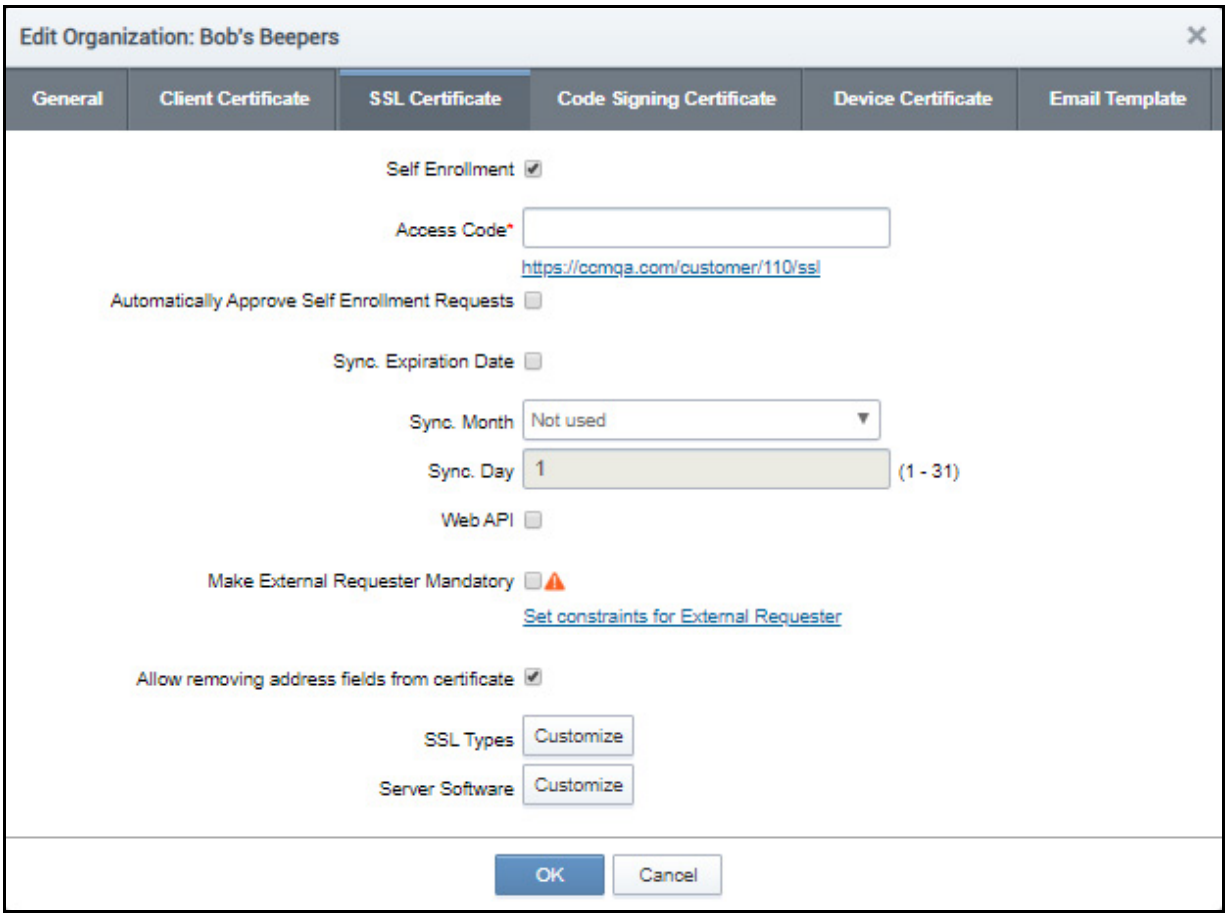
- The applicant confirms completion of the prerequisites.
- A certificate request is made via the certificate auto-installer or application form or wizard.
- The certificate appears in the **SSL Certificates** area of the SCM UI with the status of Requested. The MRAO, RAO SSL, or DRAO SSL administrator receives an email notification that a certificate request is awaiting approval.
- 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 via the SCM UI, the certificate is issued and the application status changes to Issued in the **Certificates** area. You then can install the certificate remotely by clicking Install in the SCM UI.

  - 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" on page 119).
- Once an administrator approved 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 121).
- 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 when the certificate application form is successfully submitted.

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.
- For applications through the central controller mode, the administrator has installed the agent on a control server and configured it to communicate with the remote hosts (see "Configuring Network Agents" on page 252).
- For applications through local controller mode, the administrator has installed the agent on all hosts on which certificates are to be automatically installed. The agent is responsible for creating the CSR, fetching the certificates, and installing in the host through (see "Configuring Network Agents" on page 252).
- The administrator has created at least one organization or department to which that domain belongs (see "How to Manage Organizations" on page 327).
- If the administrator wishes to enable external SSL applications, the administrator has selected **Self Enrollment** in the **SSL Certificates** area of the **Create Organizations** or **Edit Organizations** dialog, as the following illustration shows.



- If the administrator wishes to enable external SSL application using the self-enrollment form, the administrator has specified an **Access Code** in the SSL area of the **Create Organizations** or **Edit Organizations** dialog, as the preceding illustration shows. Sectigo recommends using a combination of alpha and numeric characters that cannot be guessed easily.
- For the built-in wizard and the self-enrollment form, the applicant has already created the CSR using their web server software prior to beginning the application. This helps avoid potential errors on the certificate enrollment by allowing the common name (CN) to be automatically drawn from the CSR. Please note that CSR must be at least 2048 bit and contain at least the following fields:
  - Common name (fully qualified domain name)
  - Organization
  - Organization unit
  - Locality
  - State / Province
  - Country (two-character ISO code)
- Optionally, the administrator has selected **Sync. Expiration Date** and specified the day of the month when the certificate is to expire.
- For automatic CSR generation with either manual or automatic installation, the administrator should have installed a Private Key Agent and configured it. See "Configuring the Private Key Agent" on page 306.

3.2.4.1 Using the SSL Certificate Enrollment Form and Built-In Wizard

SSL administrators or applicants authorized by them can request certificates by completing an application form. Upon a successful submission and validation by Sectigo, the certificate is issued and a notification email is sent to the applicant. The applicant can download the certificate and install it as planned.

SCM offers the following two types of SSL certificate application forms:

1. A **self-enrollment form** that allows you to apply or direct applicants to the request form to order SSL certificates. Applicants using this method must validate their application for the certificate manager as follows:
   - By entering the appropriate access code for the organization or department. 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.

   and
   - The email address the applicant enters must be from the domain for which the certificate application is being made. This domain must have been assigned to the organization or department.

   For more information, see "Self-Enrollment Form" on page 70.
2. The enrollment wizard that allows you to login and request SSL certificates by navigating to **Certificates > SSL Certificates** in the main SCM UI. The wizard allows you to enroll for SSL certificates in one of the following ways:
   - Manual CSR generation, when 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 the SSL Certificate Enrollment Form and Built-In Wizard" on page 70.
   - Auto CSR Generation, when SCM generates the CSR for the domain name with the private key stored by the Private Key Agent installed on a server at the customer premises. Upon completion of the certificate issuance, you can download the certificate with the public-private key pair from SCM and import to the servers on which it needs to be installed. For more information, see "Automatic CSR Generation Via the Built-in Enrollment Wizard" on page 96.

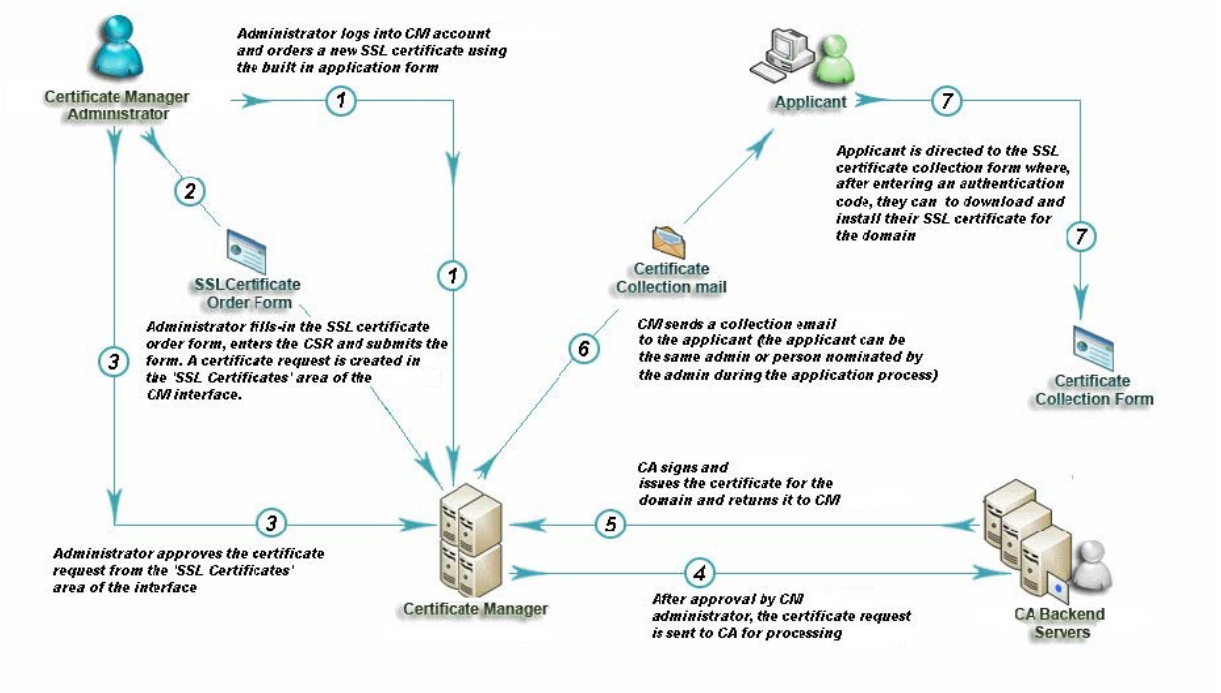
After submitting the application form, the certificate becomes accessible via navigating to **Certificates > SSL Certificates** and the certificate's status is Requested. Then an SSL administrator with the required level of privileges should approve the request. Upon approval, SCM forwards the application to Sectigo for validation and further processing. 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 respective web server.

For more information on certificate collection, see "Certificate Collection" on page 119. For more information on downloading and installing certificates, see "Download and Import of SSL Certificates" on page 121.

Note that it is possible for one organization to have multiple certificates for different domain names. For more information, see "Using the General Settings Area of the Edit Organization Dialog" on page 361

3.2.4.1.1 Self-Enrollment Form

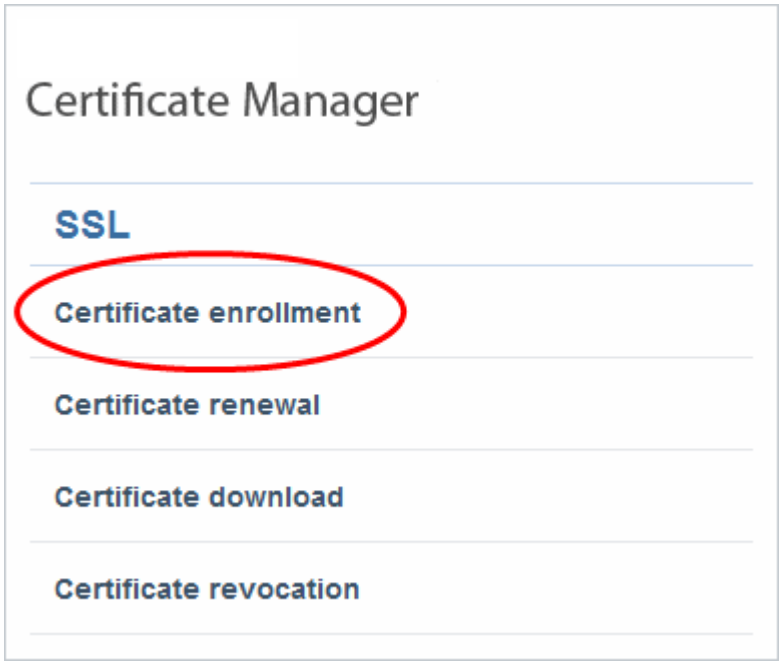
The following diagram illustrates the process of using the self-enrollment form.



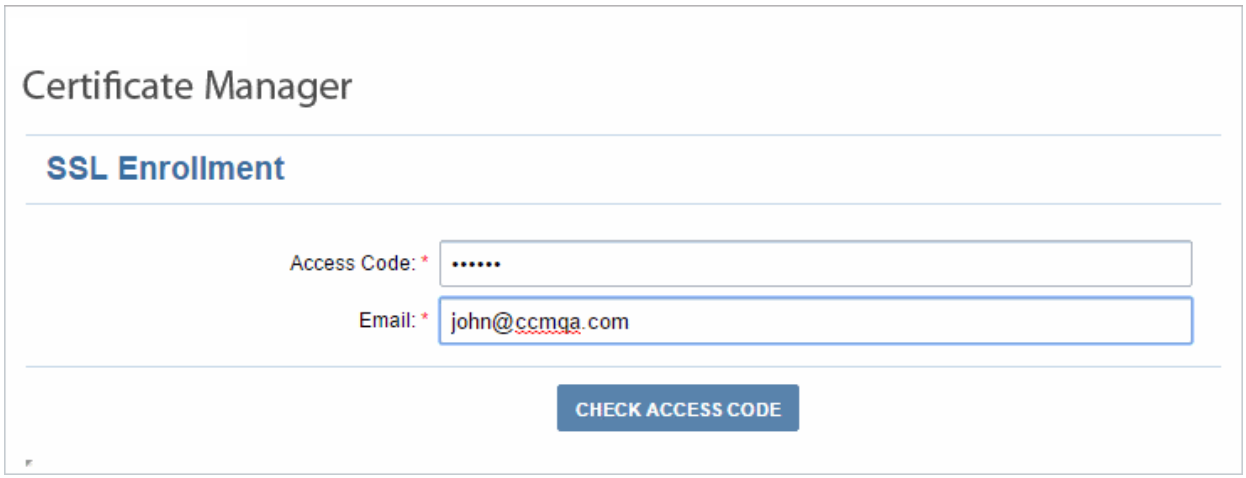
After completing initial steps, you have to provide the enrollment details to all and any end-users to whom you wish to issue SSL certificates. The communication must contain the following information:

- A link to the self-enrollment form in the default format of `https://cert-manager.com/customer/<customer_url>/ssl`.
- The access code specified in the organization or department's SSL settings area.

Furthermore, the email address that the applicant enters at the self-enrollment form must match the domain that has been assigned to the organization or department.

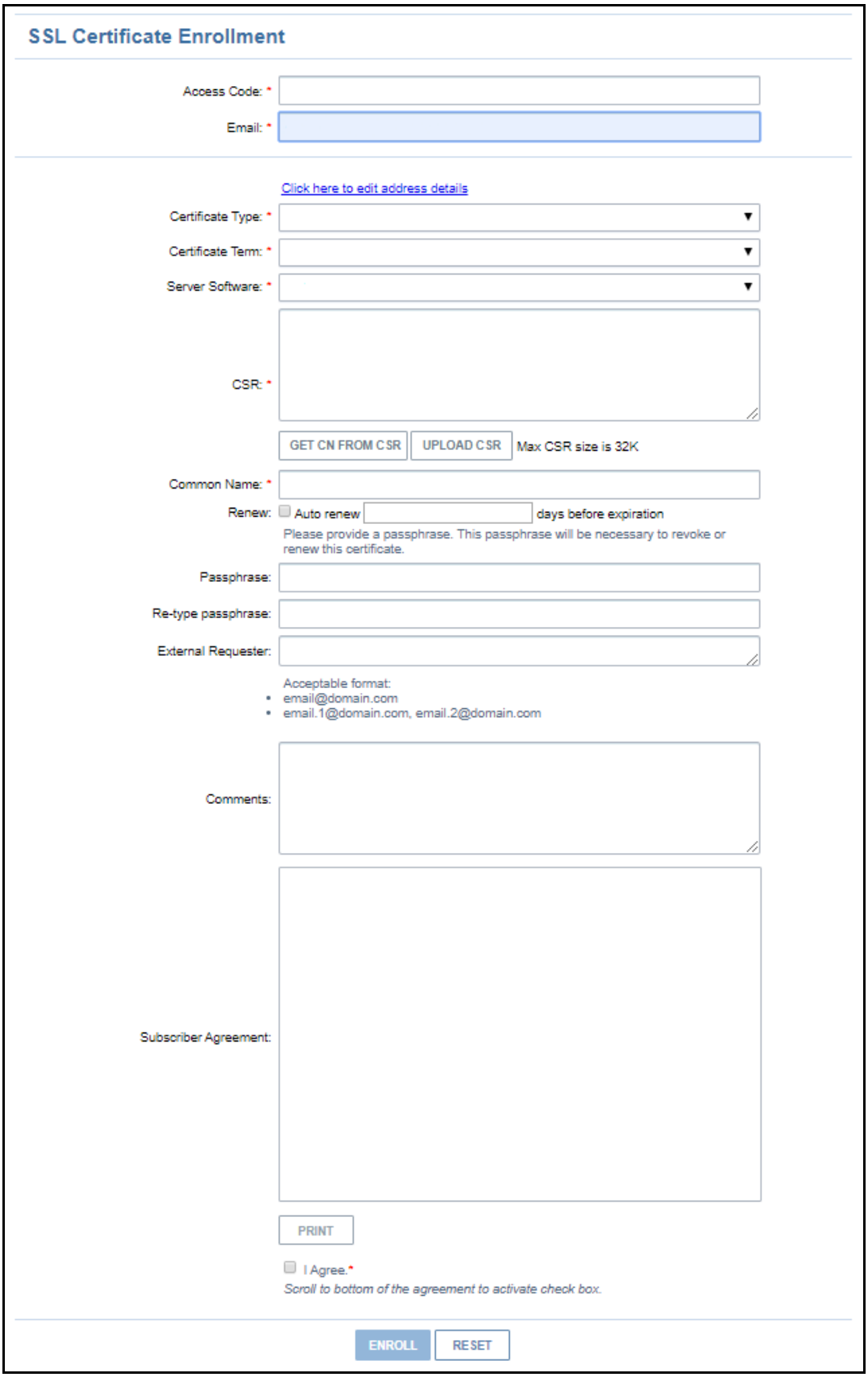


Clicking **Certificate enrollment** opens the self-enrollment form shown in the following illustration.



To access the application form, you need to authenticate the request by entering the correct access code for the organization or department and then typing an email address from a domain that has been assigned to that organization or department.

Clicking **Check Access Code** contacts SCM and requests to verify that the applicant has the right to apply for a certificate. If both the access code and email address are successfully validated, the applicant is allowed access to the full certificate application form shown in the following illustration.


SSL Certificate Enrollment
Access Code: *
Email: *
Click here to edit address details
Certificate Type: *
Certificate Term: *
Server Software: *
CSR: *
GET CN FROM CSR
UPLOAD CSR
Max CSR size is 32K
Common Name: *
Renew:
Auto renew
days before expiration
Please provide a passphrase. This passphrase will be necessary to revoke or renew this certificate.
Passphrase:
Re-type passphrase:
External Requester:
Acceptable format:
email@domain.com
email.1@domain.com, email.2@domain.com
Comments:
Subscriber Agreement:
PRINT
I Agree.*
Scroll to bottom of the agreement to activate check box.
ENROLL
RESET

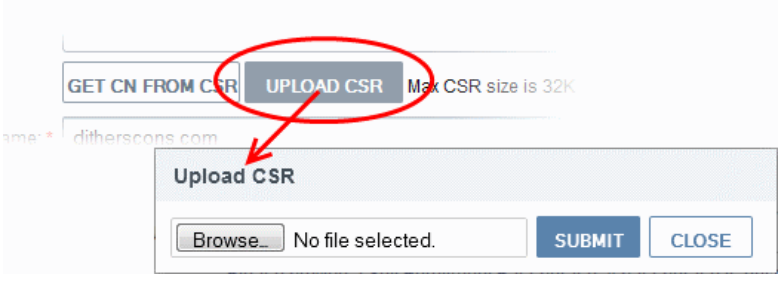
In the preceding form, the access code and email address fields are prepopulated. The domain that the user specifies in the CN field must be the same domain as the applicant's email address and that email account must be active so the applicant can receive and open emails.

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

It is possible for the certificate manager account holders to use their own custom form templates instead of the default form supplied by Sectigo. Contact your account manager for more information.

The following table provides descriptions of the self-enrollment form fields and elements. The mandatory fields are marked with the red asterisk on the form.

Field	Description
Access Code	Applicants that request a certificate using the self-enrollment form need to enter the access code that identifies a particular organization or department and is used to authenticate certificate requests made using the self-enrollment form. Organizations and departments are uniquely identified by a combination of the organization's Access Code and Common Name (domain) properties specified as part of the **General** properties. Multiple organizations or departments can have the same access code or the same common name, however no single entity can share both. You should choose a complex access code which contains a combination of alpha and numeric characters that cannot easily be guessed. This code needs to be communicated to the applicants along with the URL of the sign-up form.
Email	Applicant should enter their full email address. The email address must be for a domain that has been assigned to the organization or department.
Address Details[a] Address 1 Address 2 Address 3 City State or Province Postal Code	The fields are auto-populated from the details in the **General Settings** area of the organization or department on whose behalf the certificate request is being made. These fields cannot be modified, however for the OV-level certificates the applicant can choose to omit them from the certificate by selecting **Remove**. The allowed address details appear in the issued certificate, and the removed details appear as omitted details. For EV-level certificates, it is mandatory to include address details of the organization, incorporating or registration agency, certificate requester and the contract signer. Therefore, these fields cannot be removed from the EV self-enrollment forms.
Certificate Type	The certificate type selected by the applicant. The specific certificate types included in the list (and available to the applicant) can be customized according to the needs of the organization.
Certificate Term	The life time of the certificate selected by the applicant from the **Certificate Type** list. The available term lengths for different certificate types included in the list (and available to the applicant) can be customized according to the needs of the organization.

Field	Description
Server Software	The server software selected by the applicant that is used to operate their web server. Installation support documentation is available from the Sectigo's support portal.
CSR	A CSR based on which Sectigo is to process your application and issue the certificate for the domain. The CSR can be entered either by pasting it directly into this field or by uploading the CSR saved as a `.txt` file by clicking **Upload CSR**. In public key infrastructure systems, a CSR is a message sent from an applicant to a CA in order to apply 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. Upon uploading or pasting the CSR, the form automatically parses the CSR. If you require assistance in generating a CSR, you should consult the Sectigo knowledge base article for your web server type. In case of applications for a Multi-Domain Certificate (MDC), the CSR you generate only needs to be for a single common name (also known as the Primary Domain Name). You should type the additional domains that you require in the **Subject Alternative Name** field on this form.
Get CN from CSR	Auto-populates the **Common Name** field upon the correct entry of the CSR, therefore helping avoid human error by ensuring the domain name in the application form matches the domain in the CSR. If the domain name mentioned in the form does not match the one in the CSR, then Sectigo cannot issue the certificate. In case of applications for an MDC, in order to successfully order such certificates, the applicant needs only list the additional domains in the SAN field on this form. In certain circumstances, however, the applicant may have created a CSR that already contains these SANs, in which case clicking **Get CN from CSR** also auto-populates the **Subject Alternative Names** form fields in addition to the **Common Name** field.
Upload CSR	The applicant can upload the CSR saved as a `.txt` file in the local computer instead of copying and pasting the CSR into the CSR field, as shown in the following illustration. 

Field	Description
Common Name	The correct fully qualified domain name for the organization or department entered by the applicant. The maximum allowed character length for this field is 64. For single domain certificates, it is the domain name in the format of example.com. For wildcard certificates, it is the domain name in the format of *.example.com. For MDC, it is the primary domain name in the format of example.com.
Renew	Applicants can specify 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 (mandatory for MDC)	If the certificate Type is set to Multi-Domain Certificate (MDC), then the applicant should list the Subj Alt Name additional domains separated by commas in this field.
Passphrase	The passphrase needed to revoke the certificate when using the external revocation page at `https://cert-manager.com/customer/<customer_uri>/ssl?action=revoke`
Re-type Passphrase (mandatory if Passphrase is set)	Confirmation of the passphrase.
External Requester	The full email address of the user entered by the applicant on behalf of the user who is subject of the application. The email address must be from the same domain name for which the certificate is applied. The certificate collection email is sent to this email address.
Comments	Information for the administrator entered by the applicant.
Subscriber Agreement	Applicant must accept the terms and conditions before submitting the form by reading the agreement and clicking I Agree. The Subscriber Agreement differs depending on the type of SSL certificate selected from the **Certificate Type** list. If Sectigo EV SSL certificate or Sectigo EV multi-domain SSL certificate is selected, **I Agree** is not shown and the agreement is accepted when the application is submitted.
Enroll	Submits the application and enrolls the new certificate request.
Reset	Clears all data entered on the form.

a. The option to hide address fields is only available if configured for your organization or department.

NOTE: In addition to the standard fields in the self-enrollment form, custom fields such as **Employee Code**, **Telephone** can be added by the MRAO administrator.

3.2.4.1.2 Bulk Enrollment of SSL Certificates

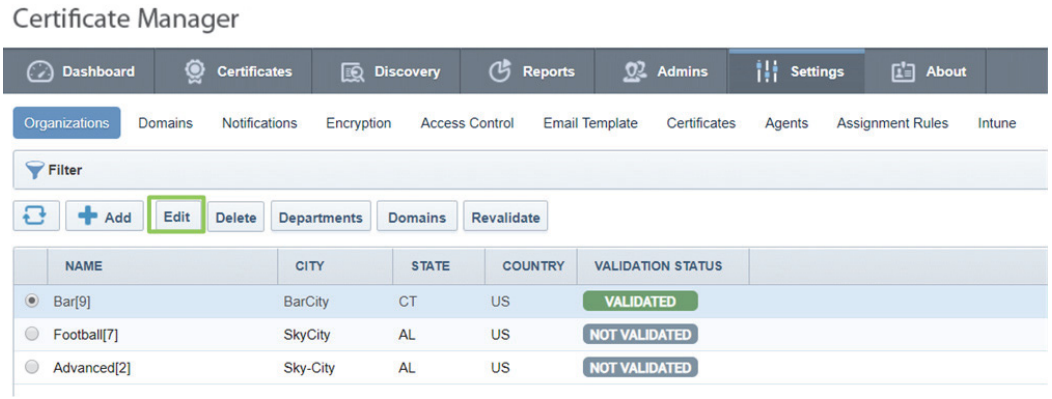
SCM allows end-users to submit requests for bulk enrollment of certificates. This must be authorized for the customer account by the Sectigo administrator and an access code must be provided by a MRAO, RAO, or DRAO administrator.

To submit bulk enrollment requests, you, as a MRAO, RAO, or DRAO administrator, must ensure the following conditions are met:

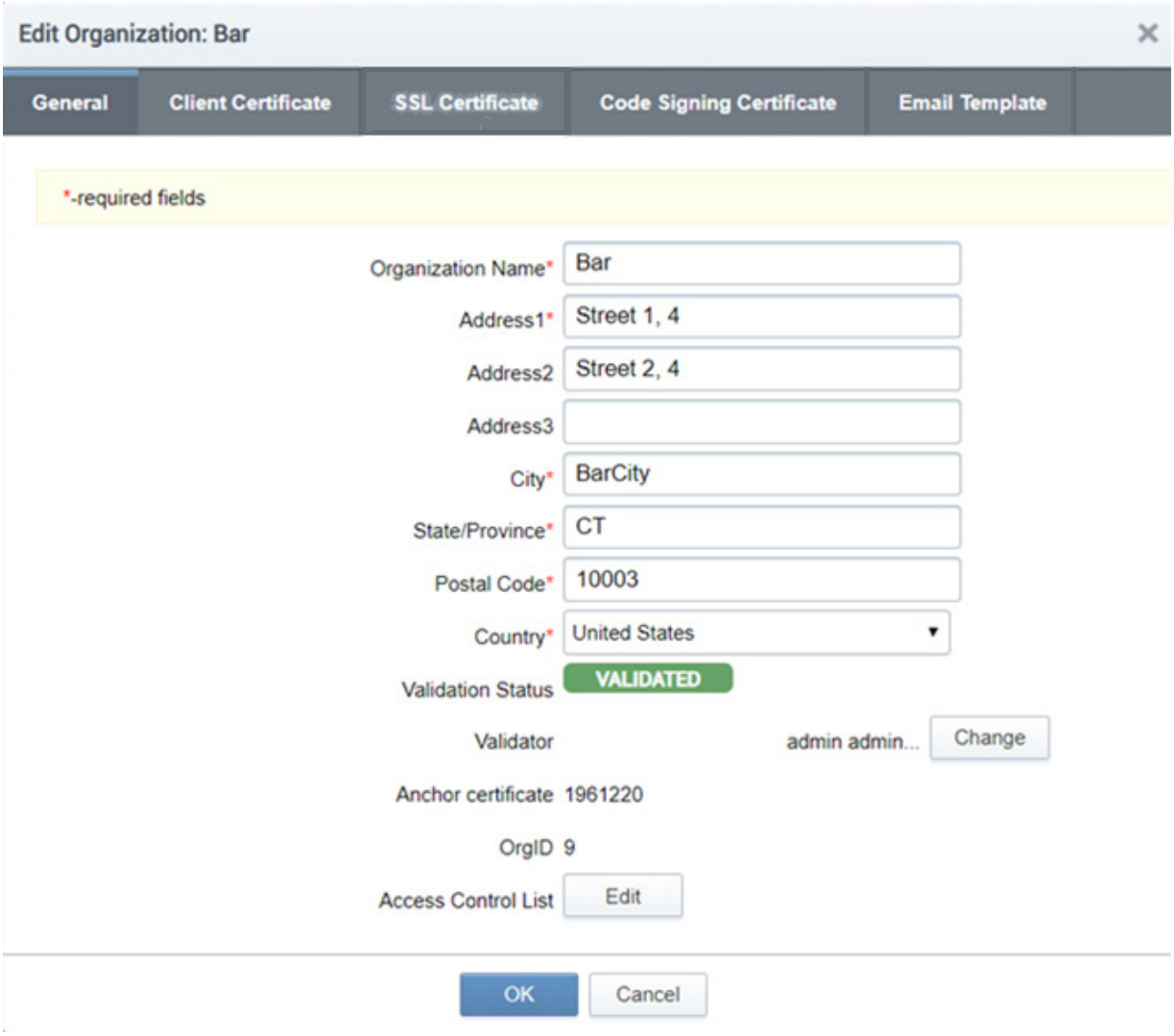
- The customer account must have at least one domain delegated to the organization or department under which the bulk requests are to be submitted with an Approved delegation status for the SSL certificate type allowed.
- The organization or department under which bulk requests are submitted must have **Self-Enrollment** enabled for SSL certificate enrollment, including the specified unique access code.
- The organization or department under which the bulk requests are to be submitted cannot have the **External Requester Mandatory** option selected.
- A Private Key Agent must be downloaded, installed, and connected to SCM.
- There must be no active custom fields made mandatory for enrollment form.

You can enable the bulk enrollment for the organization as follows:

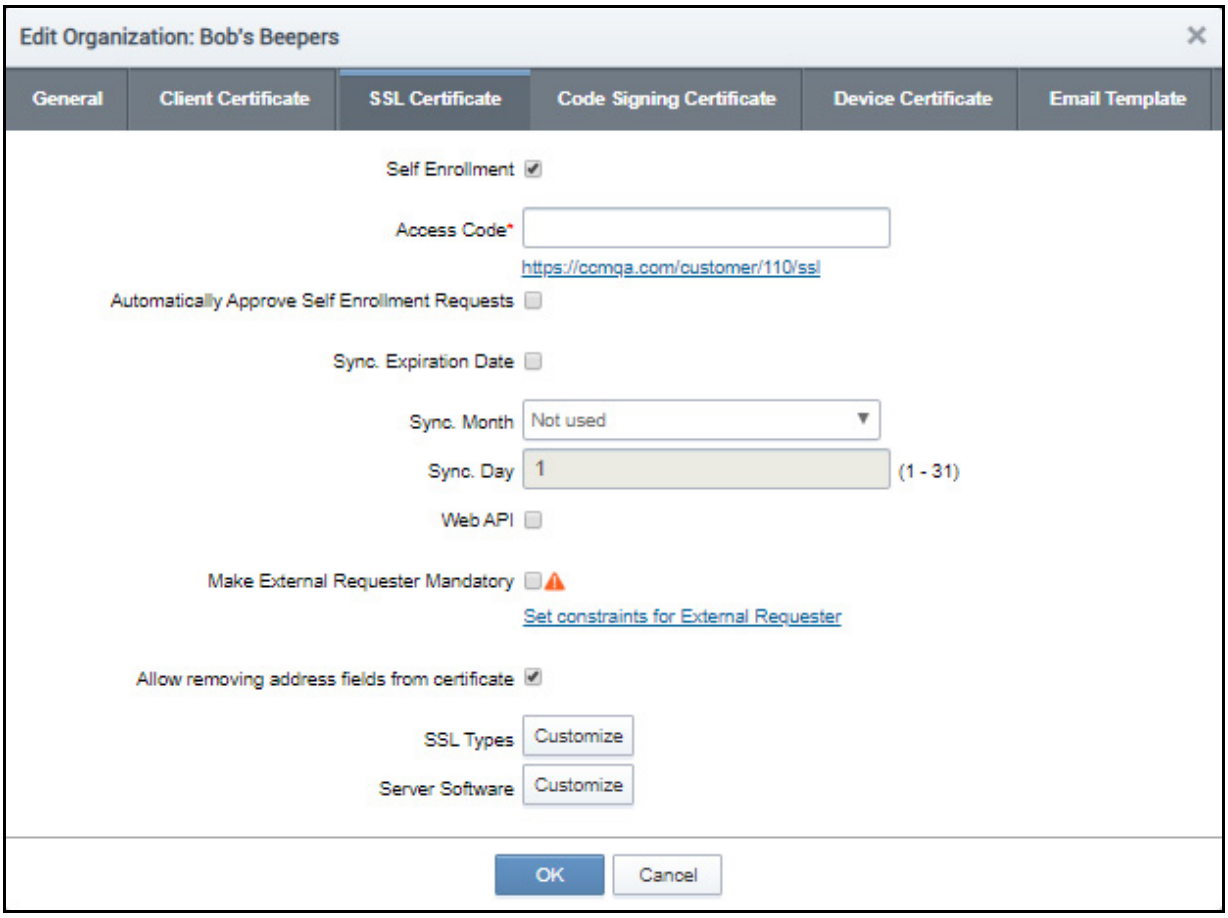
- From the main UI, navigate to **Settings > Organizations**, and select the organization to which the bulk enrollment requester belongs, as shown in the following illustration.



  If the requester belongs to a department within an organization that has been granted bulk enrollment permissions, then select the department name.
- Click **Edit** to open the **Edit Organization** or **Edit Department** dialog shown in the following illustration.

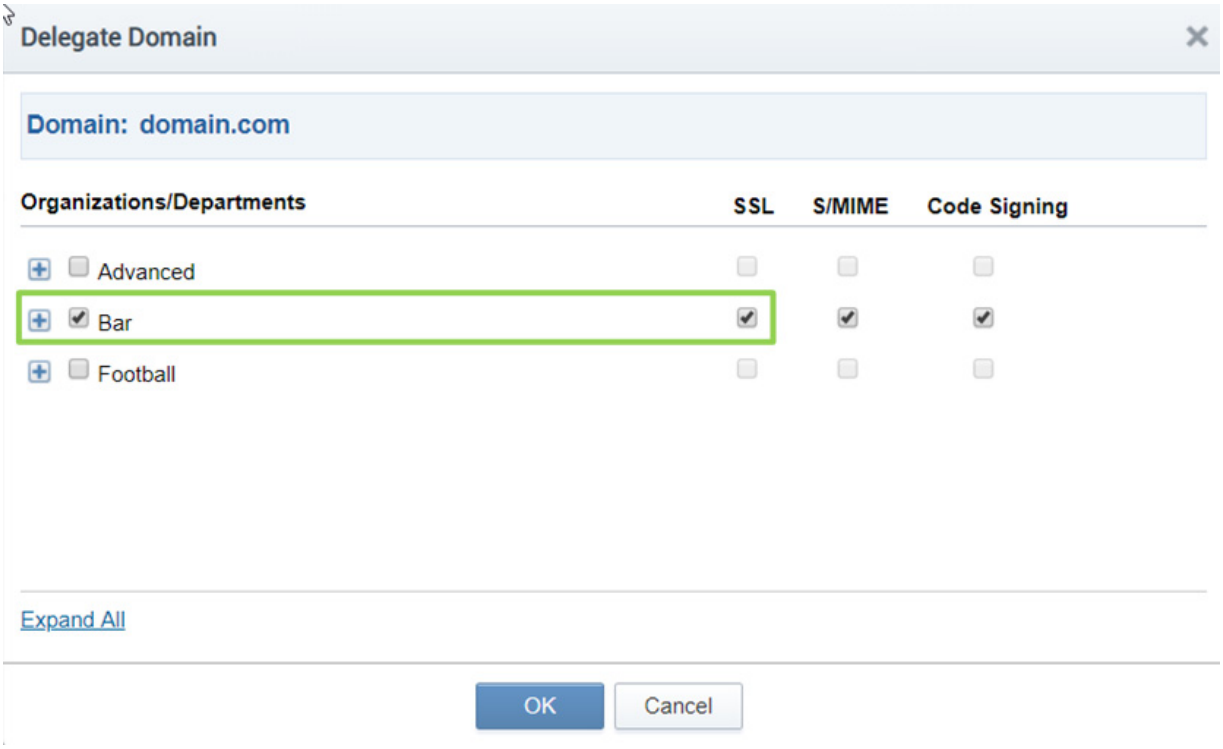


- Select **SSL Certificate** and complete the dialog shown in the following illustration by selecting **Self Enrollment,** entering the value in the **Access Code** field, and ensuring that **Make External Requester Mandatory** field is not selected.

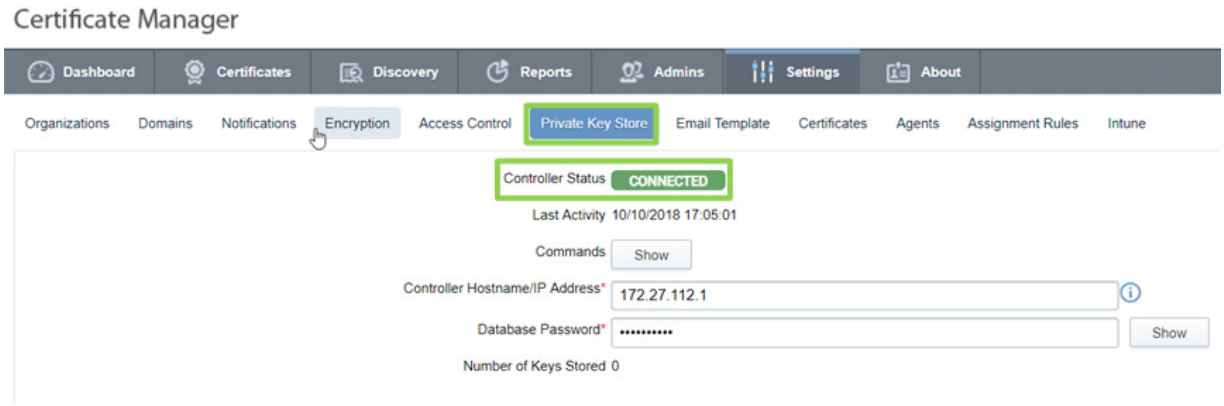


Before a request for bulk enrollment can be submitted, the requester must be authorized under a domain that can submit SSL requests under the organization or department whose access code was specified on the SSL Bulk Request Submission page. The organization or department must have at least one domain delegated to it, with the SSL certificate type permitted. You can verify this as follows:

- From the main UI, navigate to **Settings > Domains**, and select the organization to which the bulk enrollment requester belongs.
- Select the domain for which bulk enrollment is enabled, then click **Delegate** to open the **Delegate Domain** dialog shown in the following illustration, verify the **SSL** setting, and click **OK**.



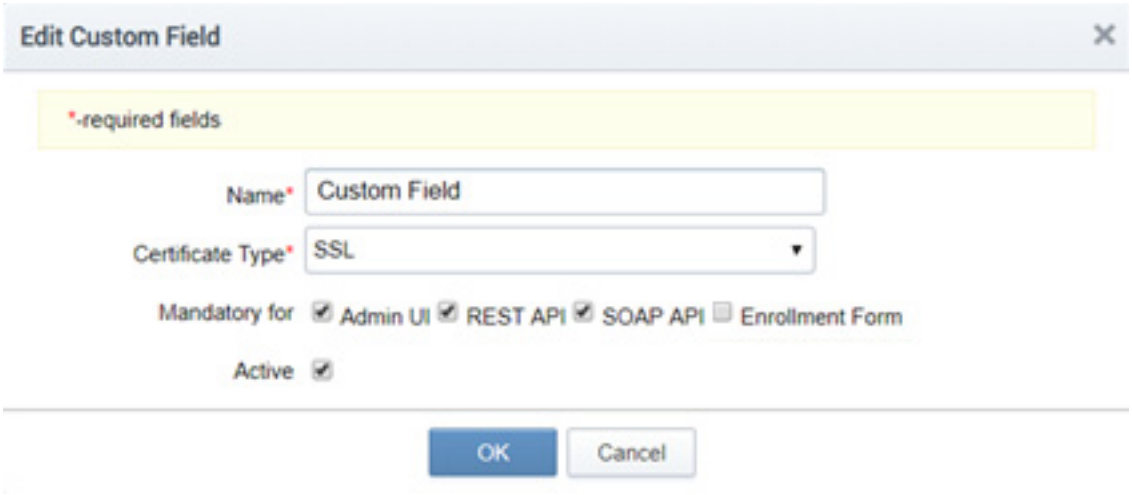
Once the permission to grant SSL certificates is verified, you need to ensure that the Private Key Agent is downloaded, installed, and connected. You can verify this by navigating to **Settings** from the main UI, and, if the connection has been established, the **Private Key Store** option would be available, with the **Controlled Status** displayed as **Connected**, as shown in the following illustration.



If custom fields are required for bulk enrollment, the following settings must be modified:

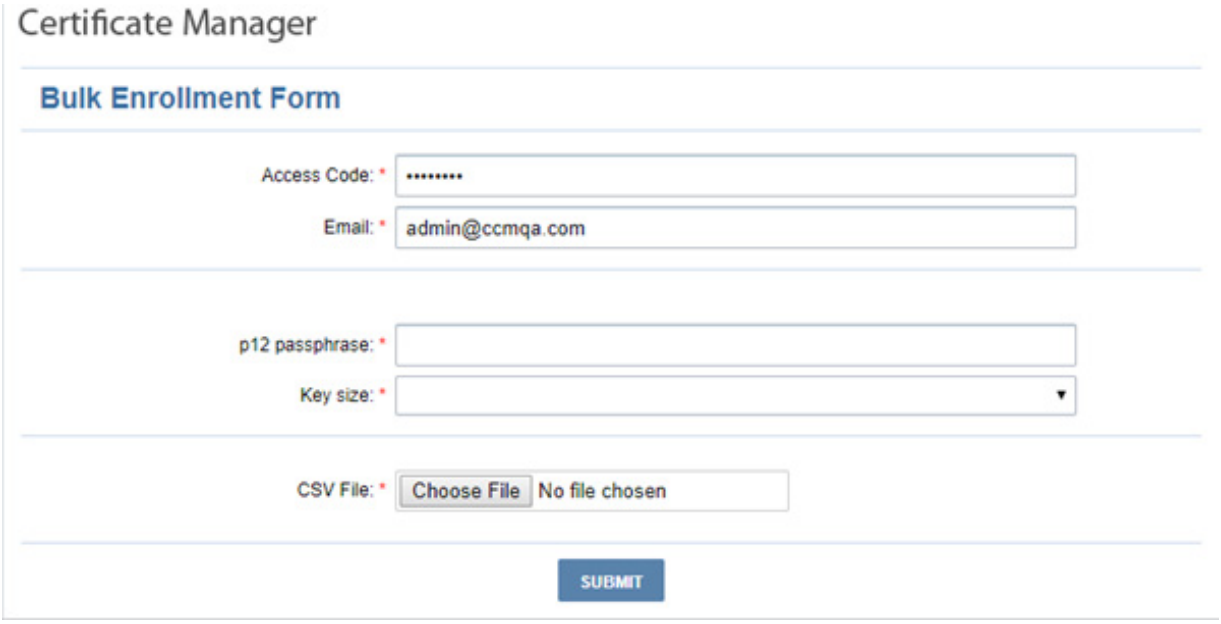
- From the main UI, navigate to **Settings > Certificates**, and click **Custom Fields**, as shown in the following illustration.
- Verify that there are no active custom fields that have been (1) configured for the SSL certificate type or (2) made mandatory for the enrollment form.

If there is such field, select it and click **Edit** to open the **Edit Custom Field** dialog shown in the following illustration. Ensure that either **Enrollment Form** or **Active** is selected, but not both, and then click **OK**.



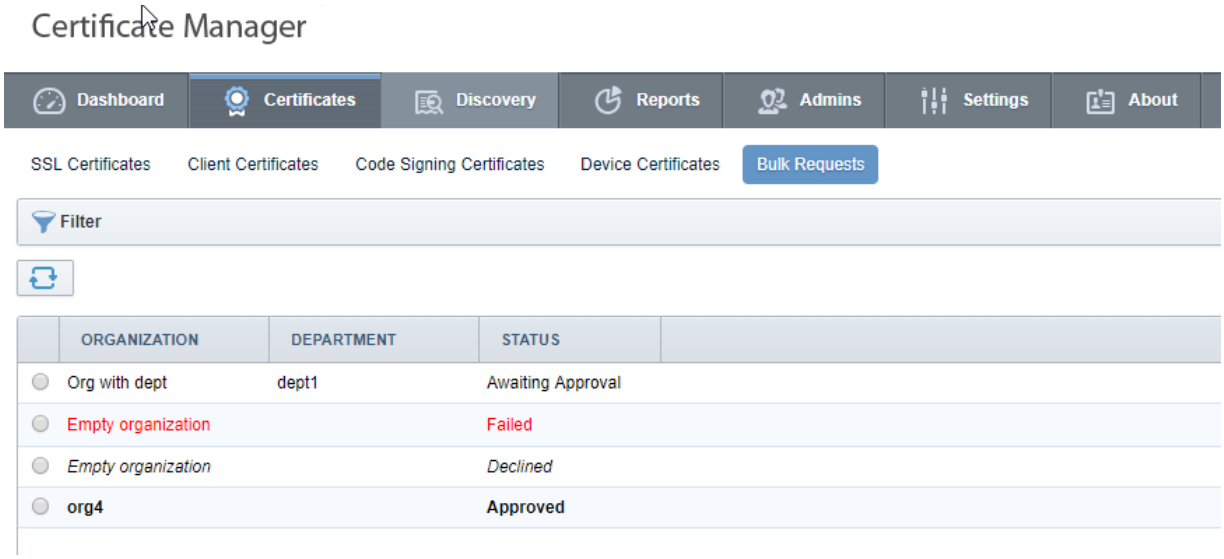
For bulk enrollment to occur, the requester needs to know the URL of the SSL Bulk Enrollment Submission page [1] and the access code of the configured organization or department. In addition, the domain name of the requester email specified in the SSL Bulk Enrollment Submission page during the submission of the request must match the domain configured via **Settings > Domains**. Then the bulk enrollment request can be completed using a self-enrollment form described in "Self-Enrollment Form" on page 70, as follows:

- Use the provided access code to log in.
- Complete fields in the **Bulk Enrollment Form** shown in the following illustration.



1. The URL is formed by appending `/bulkenroll` to the customer's URL. For example, `https://scmqa.com/customer/<customer_URL_extension>/bulkenroll`

Once the form is submitted, the request is displayed in the **Bulk Requests** area accessible by navigating to **Settings > Certificates** in the main UI, as shown in the following illustration.



Before taking effect, the request has to be verified. That is, each of its Single Certificate Requests (SCR) have to be either approved or declined in whole or in part by a MRAO, RAO, or DRAO of the organization or department under which the request has been submitted.

If the MRAO, RAO, or DRAO approves portions of the bulk enrollment request (meaning they have approved or declined each of the SCR separately), those SCRs that still await approval or have been declined cannot prevent already approved SCRs from being processed. However, the issued certificates from one bulk enrollment request cannot be downloaded via the provided links, unless all the SCRs requested through that bulk enrollment have their final status as per description in the following table. Once the SCR is approved, it is passed through several validation checks in SCM.

Bulk Enrollment Request Processing Stage	Possible Status of Bulk Enrollment Request	Possible Status of SCR Within the Request [a]	Possible Status of the Individual Certificate Request Corresponding to the Approved SCR [b]	Interdependency Between Bulk Enrollment Request Status, Its SCRs, and Individual Requests
Post-submission	Interim statuses: Awaiting Approval	Interim statuses: Awaiting Approval	N/A	Bulk enrollment request and all of its SCRs are in the Awaiting Approval status.

Bulk Enrollment Request Processing Stage	Possible Status of Bulk Enrollment Request	Possible Status of SCR Within the Request [a]	Possible Status of the Individual Certificate Request Corresponding to the Approved SCR [b]	Interdependency Between Bulk Enrollment Request Status, Its SCRs, and Individual Requests
Approval	Interim status is one of: Awaiting Approval, Approving, Approved Final status is one of: Declined, Failed	Interim status is one of: Awaiting Approval, Approved Final status is one of: Declined, Failed	N/A	1. There is at least one SCR in this bulk enrollment request Awaiting Approval: the status of the entire bulk enrollment request is Awaiting Approval. 2. The entire bulk enrollment request has been approved in one action (even if some of its SCRs have been declined) and it takes time to execute the related updates: status of the bulk enrollment request becomes Approved. 3. All SCRs within the bulk enrollment request have been approved or declined (that is, they have status of either Approved or Declined), and at least one of the SCRs has status of Approved, and the related updates have been completed: the status of the bulk enrollment request becomes Approved. 4. All SCRs of one bulk enrollment request in whole or in part have status of Declined: the status of bulk enrollment request becomes Declined. In this case the bulk enrollment request cannot proceed any further. 5. All SCRs in the bulk enrollment request have Failed statuses (did not pass validation): the status of the bulk enrollment request is Failed. In this case the bulk enrollment request cannot proceed any further.

Bulk Enrollment Request Processing Stage	Possible Status of Bulk Enrollment Request	Possible Status of SCR Within the Request [a]	Possible Status of the Individual Certificate Request Corresponding to the Approved SCR [b]	Interdependency Between Bulk Enrollment Request Status, Its SCRs, and Individual Requests
Consideration[c]	Interim status is one of: Awaiting Approval, Approving, Approved	Interim status: Approved Final status is one of: Failed, Issued, Declined	Interim status is one of: Requested, Applied Final status is one of: Issued, Invalid, Rejected	Status changes of SCRs and individual requests taking place at this stage have no influence over the status of the bulk enrollment request. 1. The SCR is in the Approved status so an individual certificate request corresponding to it is created with its initial status of Requested: the status of the corresponding SCR remains Approved. 2. The status of an individual request is changed from Requested to Applied: the status of the corresponding SCR remains Approved. 3. The status of an individual request is changed from Requested or Applied to Invalid or Rejected: the status of the corresponding SCR of the bulk becomes Failed. 4. The status of individual request is changed from Applied to Issued: the status of the corresponding SCR of the bulk becomes Issued.

a. Certificate request and its status can be monitored via the Bulk Certificate Requests UI by clicking Details after selecting the desired bulk enrollment request under Bulk Request on the Settings > Certificates in the SCM UI.
b. The certificate request and its status can be monitored via the Settings > Certificates > SSL Certificates in the SCM UI.
c. The declined status is a final status of an SCR designated at the Approval stage and no individual requests are created for these SCRs. These SCRs do not pass to the Consideration stage but remain in the Declined status until the end of the bulk enrollment request process.

After the bulk enrollment request is approved in whole or in part, for every approved SCR an individual SSL certificate request is created with a status of Requested and is accessible via the main UI's **Settings > Certificates > SSL Certificates**.

NOTE: Individual requests do not have to be approved.

The rest of the validation steps are the same as the ones performed during the creation of a new SSL request through the SCM UI. Once all the SCRs included in one bulk enrollment request have been processed, an email with links [1] is sent to the requester allowing them to download certificates issued as part of this bulk enrollment.

The following table describes two types of notifications that are available as part of the bulk enrollment process.

Notification Type (Email Template Name) [a]	Timeline	Configuration Requirements	Method	Default Title and Body of the Notification Email Template [b]
SSL Bulk Awaiting Approval	Bulk enrollment is submitted	Needs to be configured [c] (if the customer wants it to be sent)	Emailed to the MRAO, RAO, or DRAO, as configured for this notification (sent if configured)	Title: ---- SSL bulk enrollment is AWAITING APPROVAL---- Body: [d] An SSL certificate bulk enrollment submitted in CSV format for '{Common Name}' is awaiting approval. Request Details: Common Name : {} Subject Alternative Names : {} SSL Type : {} Term : {} Server : {} Requested : {} Self-Enrollment Certificate ID : {}

1. The link for downloading certificates expires after two 2 days since issuance. If the certificates is not downloaded within this time frame, the MRAO, RAO, or DRAO must send the requester another email containing new links for download.

Notification Type (Email Template Name) [a]	Timeline	Configuration Requirements	Method	Default Title and Body of the Notification Email Template [b]
SSL Bulk Enroll Completed	Bulk enrollment has attained final status other than Declined	No need to configure (sent automatically)	Emailed to the address specified by the requester during bulk enrollment submission	Title: ---- SSL bulk processing has finished with status: {}---- Body: [e] An SSL certificate bulk enrollment has been processed. Bulk Certificate Details: Status : {} Status Message : {comment provided by the MRAO, RAO, or DRAO while approving this SCR} Common Name : {} Subject Alternative Names : {} Number of licenses : {} SSL Type : {} Term : {} Server : {} Requested : {} Approved : {} Expires : {} Order Number : {} Self-Enrollment Certificate ID : {} Comments : {} Downloadable From : {link}

a. The name by which it can be found in the **Settings > Templates > Email Templates** area.
b. The body and title of these notifications, as well as other parameters can be easily changed by the MRAO from the **Settings > Templates > Email Templates** area.
c. Notifications should be configured in this case via **Settings > Notifications**.
d. The same text is repeated for every SCR of this bulk request.
e. The same text is repeated for every SCR of this bulk request.

About Bulk Enrollment Request Statuses

Each bulk enrollment request, as well as its SCRs and the individual requests corresponding to these SCRs, has a set of applicable statuses that succeed one another throughout the bulk enrollment processing which consists of the following stages:

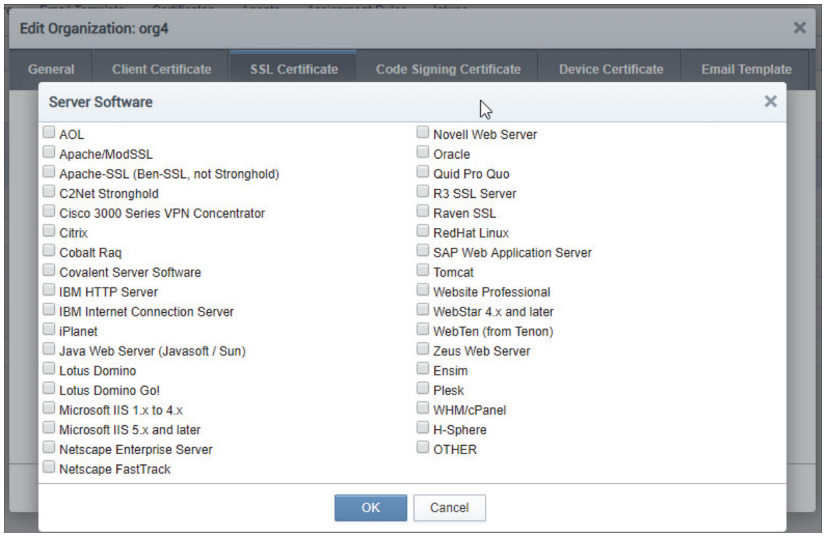
- Post-submission: a request is submitted and appears in the SCM UI.
- Approval: bulk enrollment is either approved or declined in whole or in part by a MRAO, RAO, or DRAO.
- Consideration [1]: an individual certificate request is created for each approved SCR to which the certificate is linked. The certificate status of each SCR is kept unchanged unless the certificate status is finalized (becomes Issued, Invalid, or Rejected). Once finalized, the corresponding SCR status is finalized.
- Conclusion: once all SCRs in a bulk enrollment request are finalized, the request is finalized and the issued certificates are available for download.

NOTE: A bulk enrollment request can be modified before it reaches the Awaiting Approval status.

The data for 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 in one line and separated by commas, except the last parameter in the line. This is applicable even if the parameter is optional and left blank, which can only be Subject Alternative Names (SAN). If a parameter contains one or more commas within its string, this parameter must be placed in inverted commas.

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

- Common Name—string.
- SAN—the whole value must be in quotes, domains inside, comma separated.
- Certificate Type—string, must be the same type name as displayed in the SCM UI.
- Certificate Term—string, must be the same as it appears in the SCMUI to allow for customized certificate terms.
- Server Software—string, must be the same server name as it appears in the Server Software dialog in the SCM UI. Any values shown in the following illustration must be entered as a string.



For example, to request enrollment for an EliteSSL Certificate for 1 year with a common name of scmqa.com without SANs and for server software Microsoft IIS 5.*n* or later, the following line would be included in the CVS file:

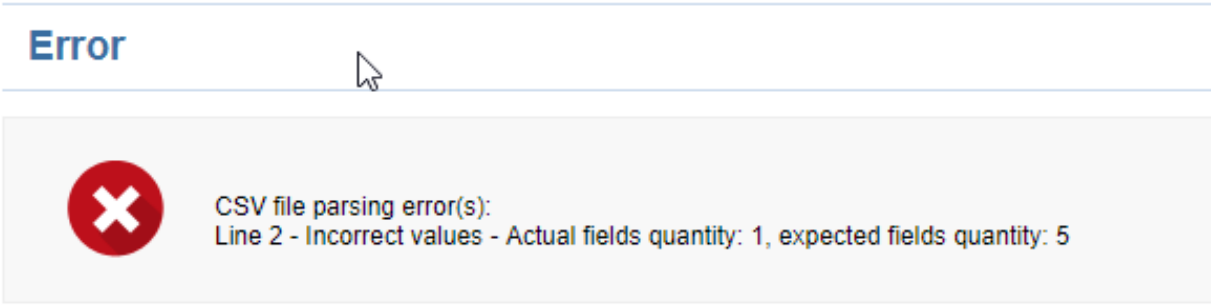
```
scmqa.com, , EliteSSL Certificate, 1 year, Microsoft IIS 5.n or later
```

1. Since SCRs of a bulk enrollment request can be approved separately, the Approval and Consideration stages may overlap. Typically, a request can reach the Consideration stage only if it has not been declined by the MRAO, RAO, or DRAO during the Approval stage as long as at least one SCR for the request has been approved. Therefore, although some SCRs within one request may have already been issued certificates or have been deemed invalid (after having been considered by the MRAO, RAO, or DRAO and had their status finalize), others may be newly-approved or still awaiting approval, placing them just before the Consideration stage. If an SCR is declined at the Approval stage, it cannot pass from Approval to Consideration.

As another example, to request enrollment for an AMT Multi-Domain SSL Certificate for 2 years with a common name of scmqa.com with SANs fly.com, new.com, and for a server software Tomcat, the following line would be included in the CVS file:

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

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.



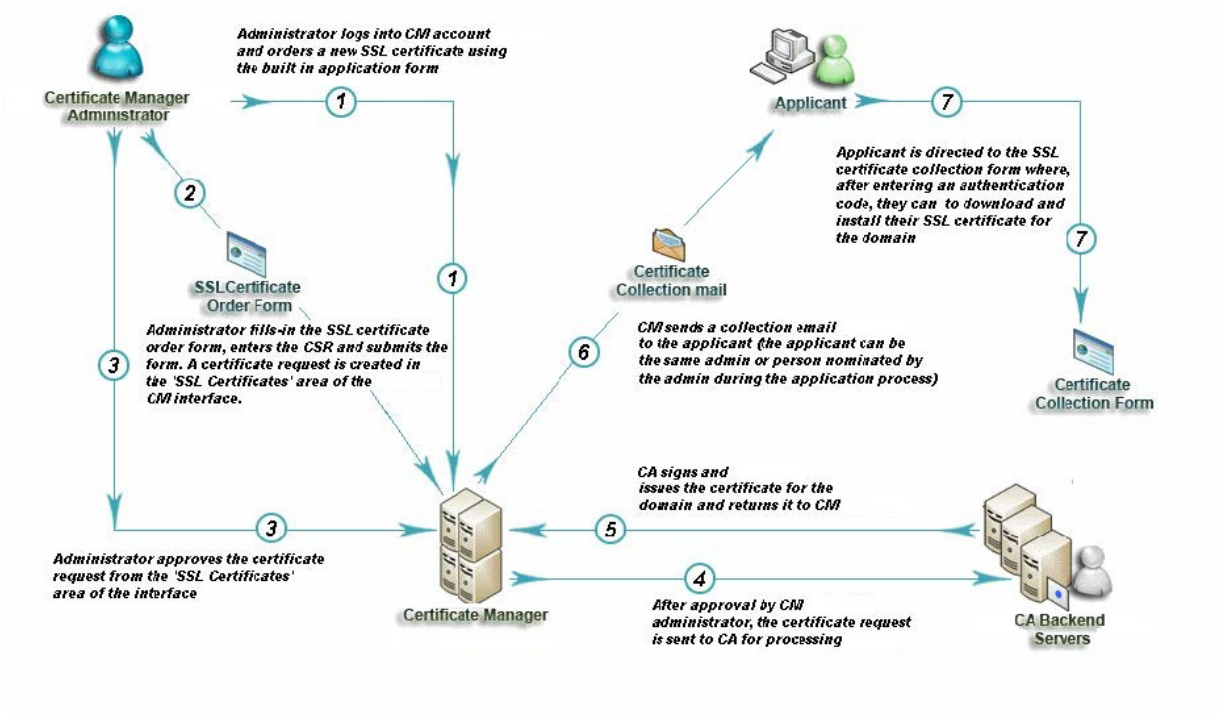
The following table lists errors that may arise during parsing of a CSV file.

Error ID	Reason	Error Message	Comment
1	The CSV file contains a line without a common name.	CSV file parsing error(s): Line *<line ID in the CSV file>* - Required field 'commonName' is not specified.	Displayed in red bold font above every field.
2	The CSV file contains a line without a certificate type.	CSV file parsing error(s): Line *<line ID in the CSV file>* - Required field 'certType' is not specified.	Displayed in red bold font above every field.
3	The CSV file contains a line without a certificate validity period (term).	CSV file parsing error(s): Line *<line ID in the CSV file>* - Required field 'certTerm' is not specified	
4	The CSV file contains a line without a server software.	CSV file parsing error(s): Line *<line ID in CSV file affected>* - Required field 'serverSoftware' is not specified	
5	The CSV file contains a line in which not all parameters are separated by commas.	CSV file parsing error(s): Line *<line ID in the CSV file>* - Please use commas only to delimit domain alternative names (for example - domain_one.com, domain_two.com, etc.)	

Error ID	Reason	Error Message	Comment
6	The certificate type specified in a line of the CSV file is not found among certificate types allowed for the organization for which this request is being submitted. Or this certificate type does not exist.	CSV file parsing error(s): Line *<line ID in the CSV file>* - field 'certType' contains disallowed value: <value>	
7	The certificate type specified in a line of CSV file is allowed for the organization for which the request is being submitted. However, the certificate term specified in the same line is not permitted for that certificate type for this organization.	CSV file parsing error(s): Line *<line ID in the CSV file>* - field 'certTerm' contains disallowed value: <value>	
8	Server software specified in a line of the CSV file is not found among the server software allowed for the organization for which the request is being submitted.	CSV file parsing error(s): Line *<line ID in the CSV file>* - field 'serverSoftware' contains disallowed value: *<value>*	
9	The number of commas in a line of the CSV file is other than four.	CSV file parsing error(s): Line *<line ID in the CSV file>* - Incorrect values - Actual fields quantity: *<value>*, expected fields quantity: *<value>*	
10	A line in the CSV file contains Subject Alternative Names, whereas the certificate type specified in the same line is not multi-domain.	CSV file parsing error(s): Line *<line ID in the CSV file>* - Field 'san' contains non-empty value: '*<0>*'. Subject alternative names are not allowed for '*<specified certType>*' certificate type.	

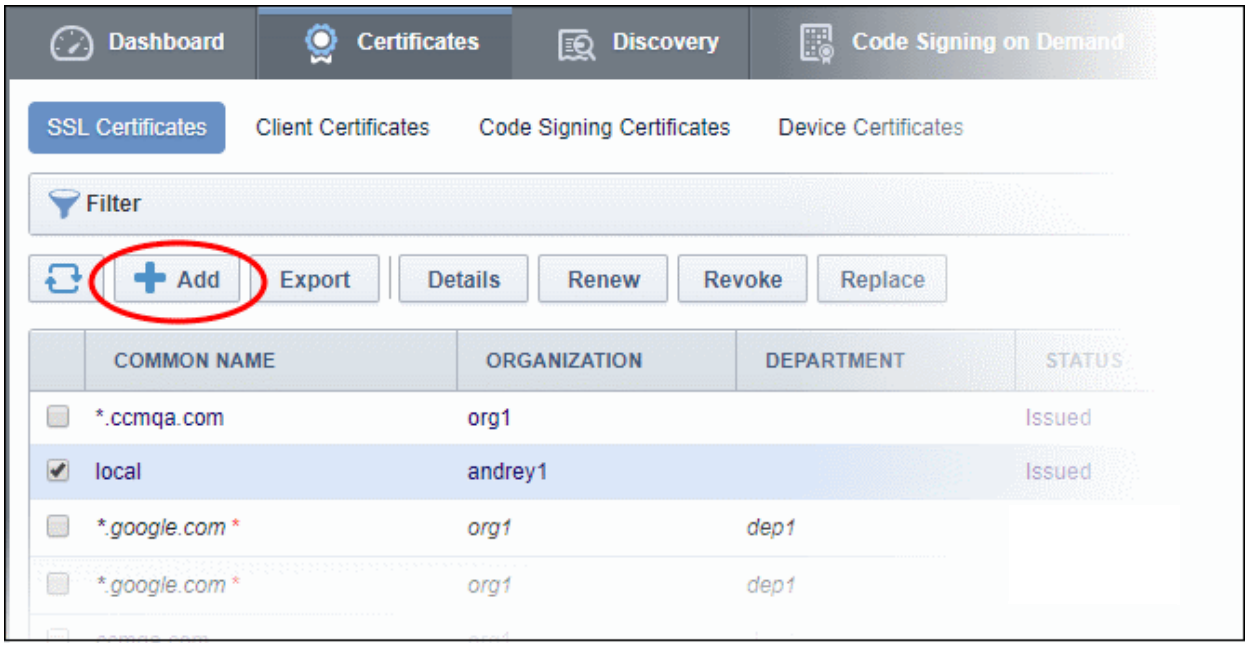
3.2.4.1.3 Manual CSR Generation Via the Built-in Enrollment Wizard

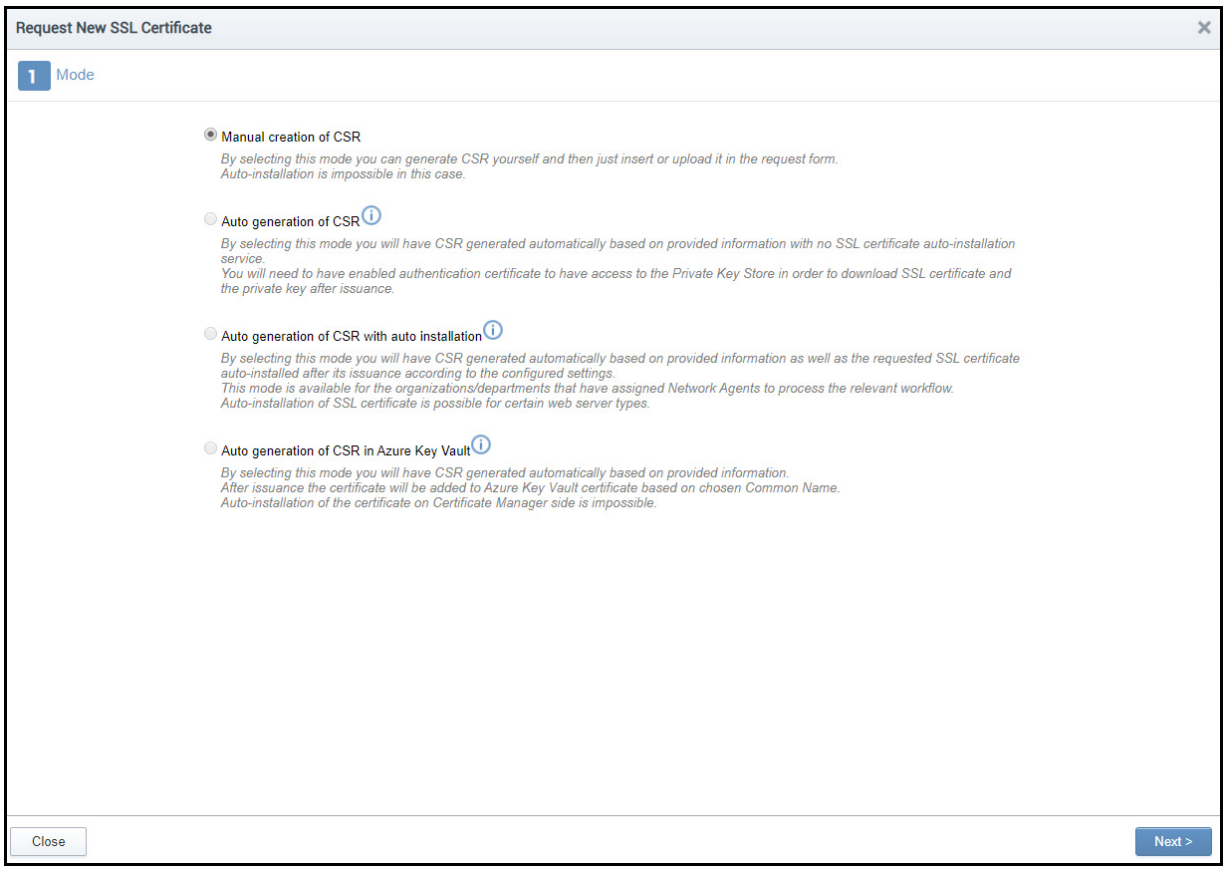
The following diagram illustrates the process of using the built-in wizard for manual CSR generation.



You can manually apply for new certificates as follows:

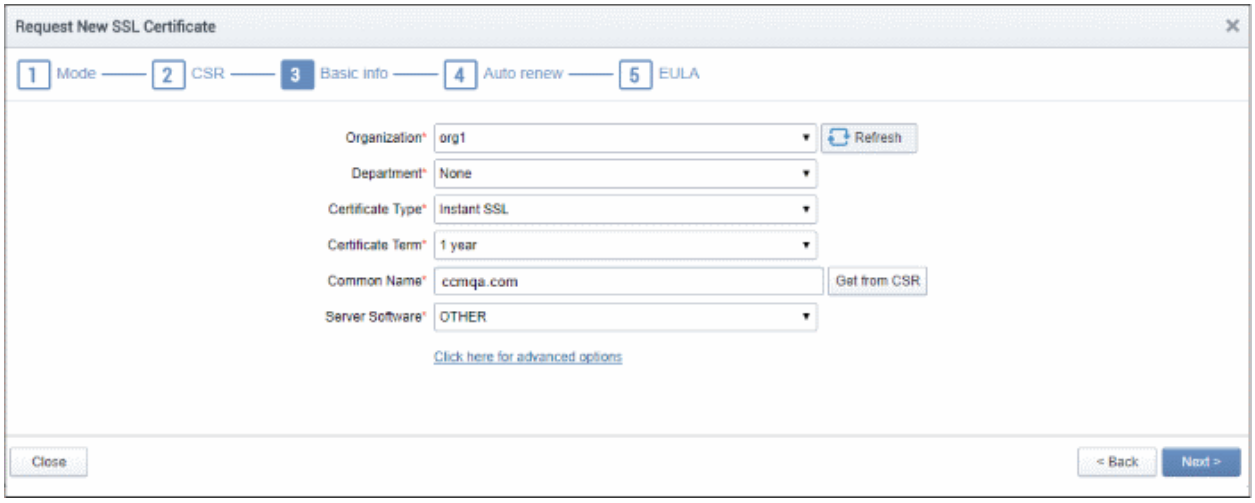
- Navigate to **Certificates > SSL Certificates** from the main UI, and then click **Add**, as shown in the following illustration. This opens the **Request New SSL Certificate** wizard.



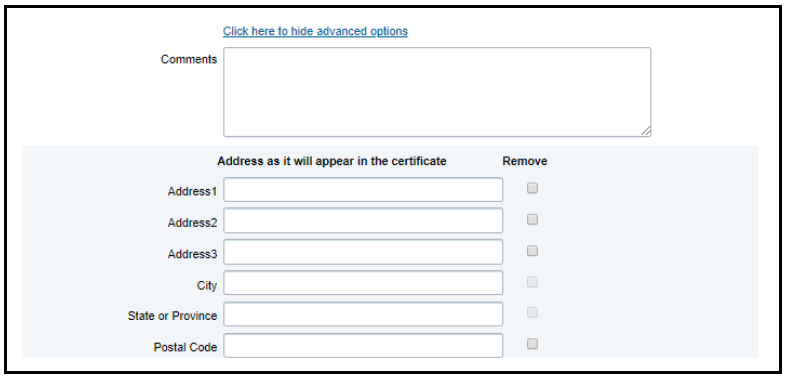


- In the **Request New SSL Certificate** wizard, select the first option **Manual creation of CSR**, and then click **Next** to open the **CSR** page shown in the following illustration.

- Paste your CSR into the **CSR** field or upload it as a `.txt` file in order for Sectigo to process your application and issue the certificate for the domain.
- Click **Next** to open the **Basic info** wizard page shown in the following illustration.



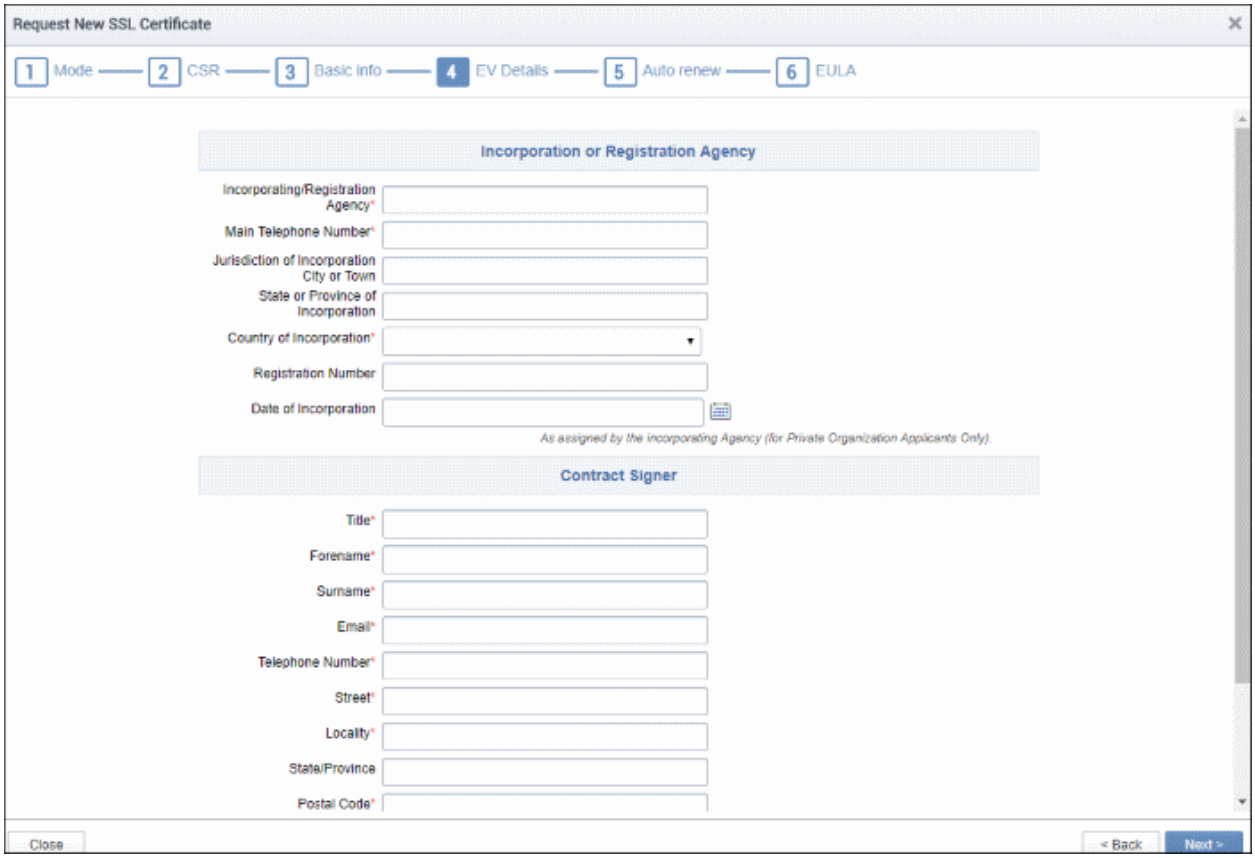
Field	Description
Organization	The organization to which the SSL certificate will belong.
Department	The department to which the SSL certificate will belong. For the certificate to be applied to all departments, select **Any**.

Field	Description
Certificate Type	The certificate type that you wish to add for auto-installation. The specific certificate types displayed in the list depend on the SSL Types allowed for the selected organization.
Certificate Term	The validity period of the certificate. For example, 1 year, 2 years, 3 years. The validity periods available for a particular organization depends on its configuration.
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. Each domain name should be separated by a comma. This field appears only if a multi domain or UCC certificate type is selected.
Requester	Auto-populated with the name of the administrator making the application.
External Requester	The email address of an external requester on whose behalf the application is made. The requester is still the administrator that is completing this form (to view this, open the **Certificates** area and click **View** next to the subject certificate). The email address of the external requester is displayed as the **External Requester** in the **View** dialog of an issued certificate.
Click here for advanced options	Expands the advanced options shown in the following illustration. 

Field		Description
	Comments	Comments pertaining to the certificate.
	Address fields[a]	The address fields in the certificate are auto-populated from the details in the **General Properties** area (see general settings of the organization or department on whose behalf this certificate request is being made). These fields cannot be modified but, in the case of OV-level certificates, you can choose to omit them from the certificate by selecting **Remove** next to the fields. The allowed address details appear in the issued certificate and the removed details appear as **Details Omitted**. For the EV level certificates, you must include and display address details of the organization, corporation or registration agency, certificate requester and the contract signer. Therefore fields for entering the these address details are displayed, as shown in the following illustration, and the option to remove certain fields is not available on the EV self-enrollment form upon selecting **Sectigo EV SSL Certificate** or **Sectigo EV Multi-Domain SSL Certificate** from the **Certificate Type** list.

a. The option to hide address fields is only available if configured for your organization or department.

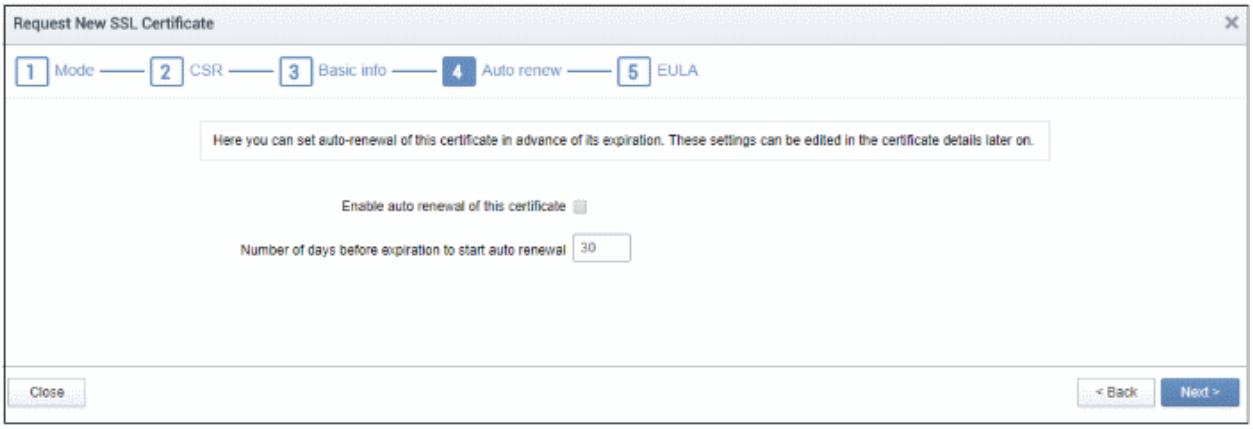
- Click **Next** to open the E**V Details** page of the wizard that allows you to select EV certificate types, as the following illustration shows.



- Complete fields of the E**V 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** area when adding a new organization (see "Using the EV Details Area of the Add New Organization Dialog" on page 334). If the EV type for your account is RA, the fields in this wizard page are auto-populated.

- Click **Next** to open the **Auto renew** page of the wizard shown in the following illustration.



- Follow this procedure to configure the auto-renewal options:
  - Select **Enable auto renewal of this certificate** to have SCM apply for a new certificate when the current one approaches expiry.
  - Select **Create new key pair while renewing** to specify that you want to generate a new key pair for the renewed certificate. Leaving this option disabled means SCM is to reuse the key pair of the old certificate.
  - Use the **Number of days before expiration to start auto renewal** field to specify the number of days 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.
- Click **Next** to open the final page of the wizard shown in the following illustration.

- Use the **EULA** page of the wizard to read the EULA fully and accept by the 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 certificated approved (see "Approving, Declining, Viewing, and Editing Certificate Requests" on page 121).

3.2.4.1.4 Automatic CSR Generation Via the Built-in Enrollment Wizard

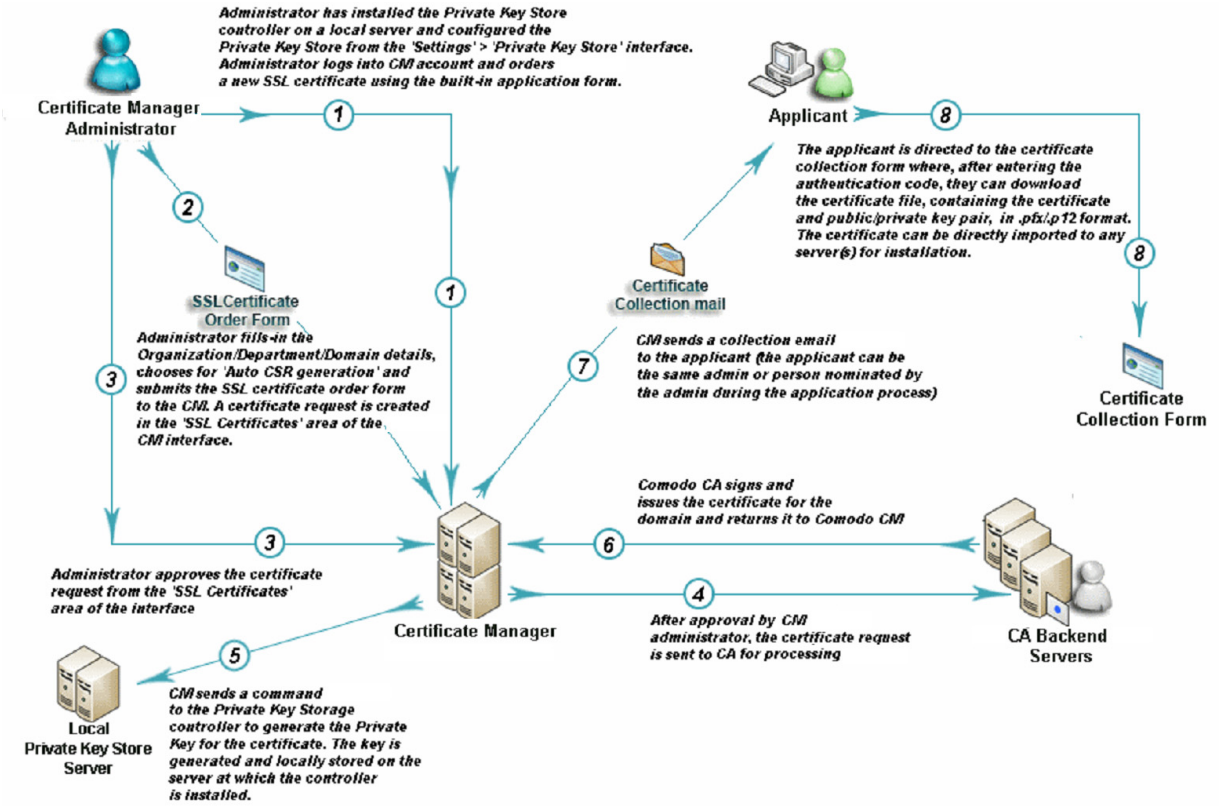
SCM can use the information entered for the organization, department, common name, and server software to automatically generate a CSR at the start of the application process.

During the CSR generation, SCM issues a command to the Private Key Agent to create the private key for the certificate. The Private Key Agent is installed on a local server on a customer network and can be configured by navigating to **Settings > Private Key Store** from the main SCM UI. The private key is stored in a database created by the agent on the local server and does not leave the customer network; the private key is not uploaded to SCM.

Upon approval and issuance, the certificate can be collected by you, or the applicant defined in the Certificate Details dialog, 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 a `.pfx` or `.p12` format. The certificate can be imported to and installed on any server.

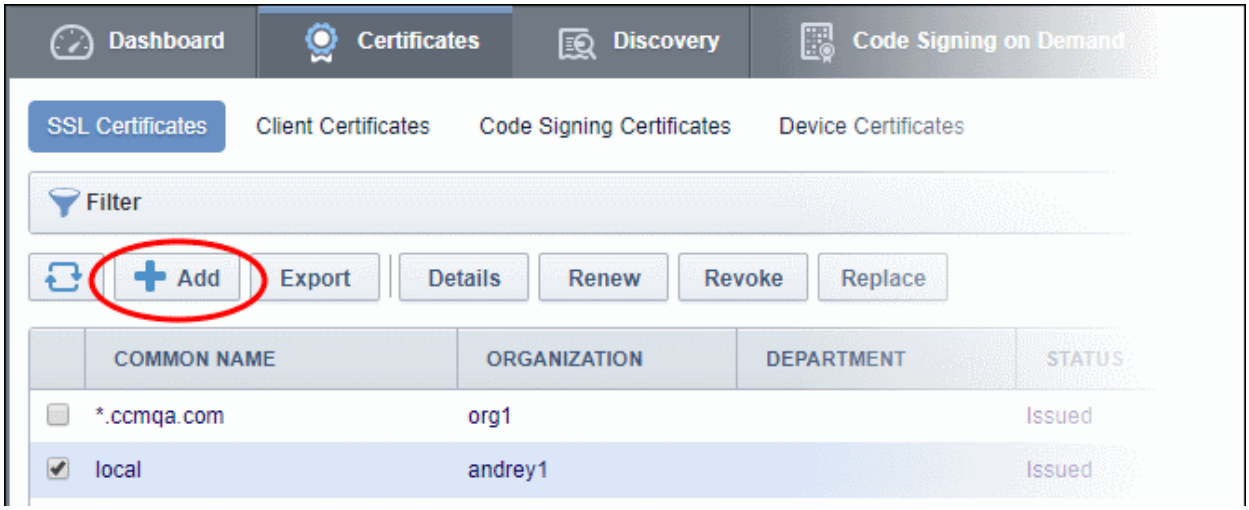
Prior to starting the auto-enrollment, you need to install the Private Key Agent on a local server. The agent should be connected to SCM to receive commands, generate and store the private keys. For more information, see "Configuring the Private Key Agent" on page 306.

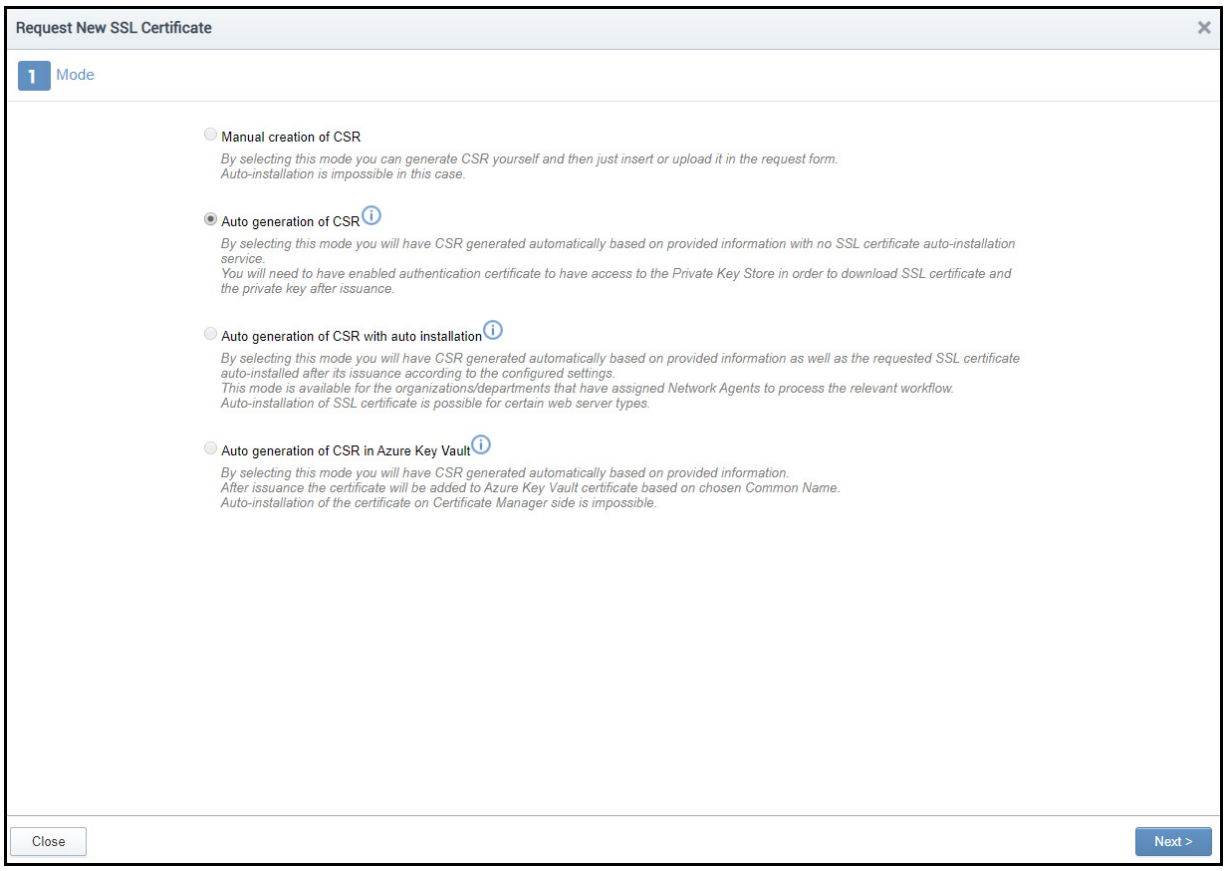
The following diagram illustrates the process of using the built-in wizard to generate the CSR automatically



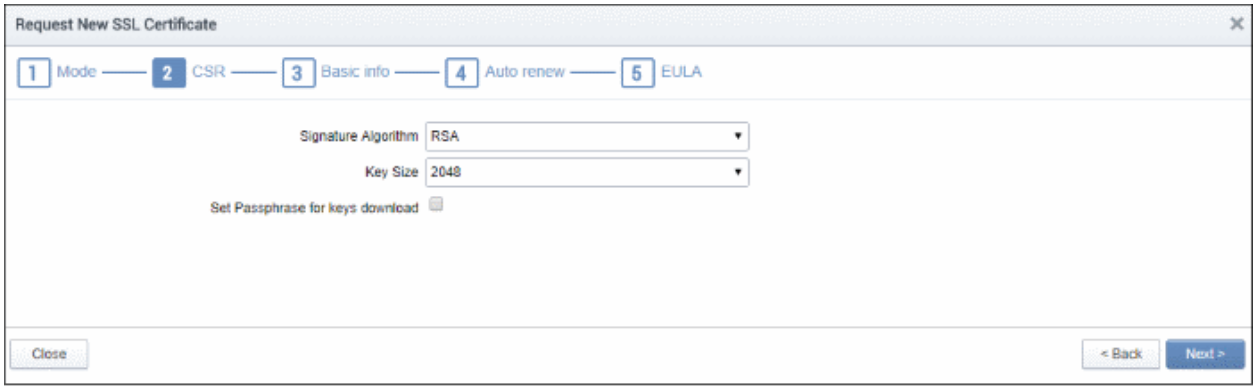
You can trigger an auto-generation of new certificates as follows:

- Navigate to **Certificates > SSL Certificates** from the main UI, and then click **Add**, as shown in the following illustration. This opens the **Request New SSL Certificate** wizard.





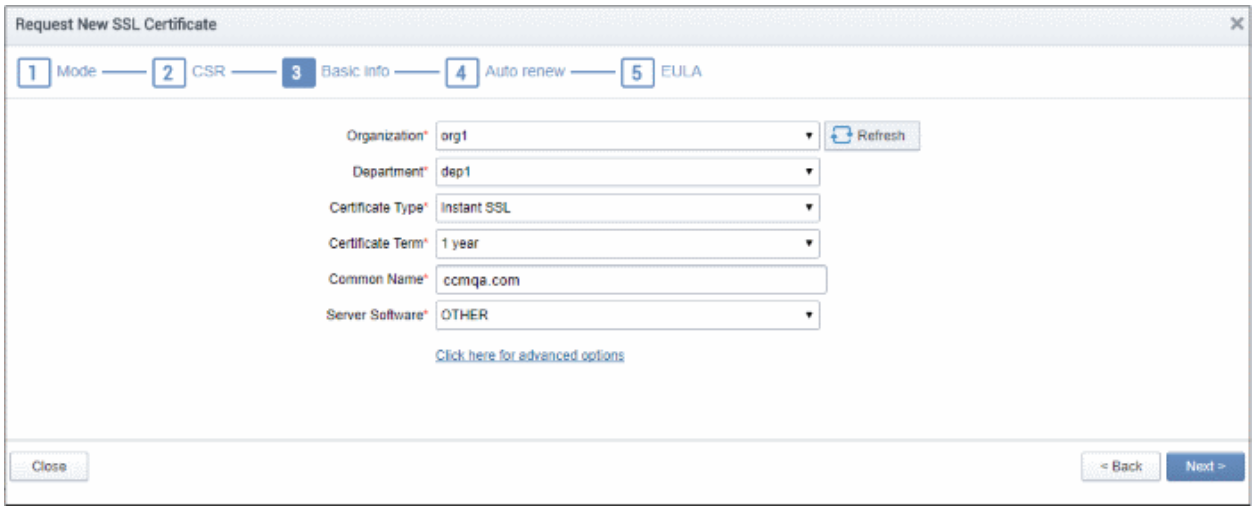
- In the **Request New SSL Certificate** wizard, select the second option **Auto generation of CSR**, and then click **Next** to open the **CSR** page shown in the following illustration.



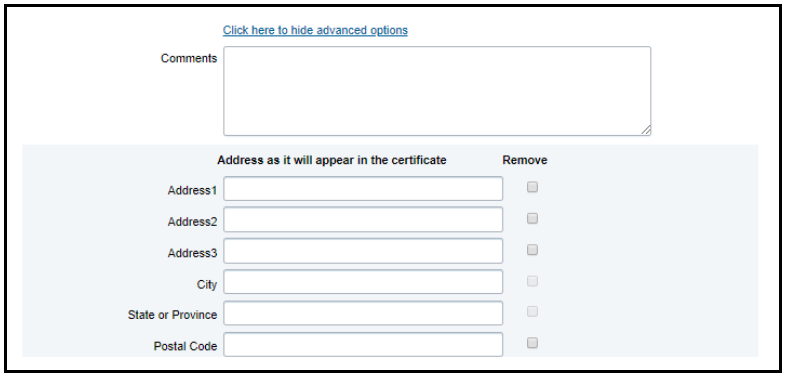
- Specify the CSR parameters, as follows:
  - In the **Signature Algorithm** field, select the digital signature algorithm you want to use in the certificate. Currently, only RSA is supported.
  - In the **Key Size** field, select either 2048 or 4096. The former is the recommended industry standard and 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.
  - 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**.

- Click **Next** to open the next page of the wizard shown in the following illustration, and then specify values based on the information provided in the following table. The mandatory settings are marked by a red asterisk.

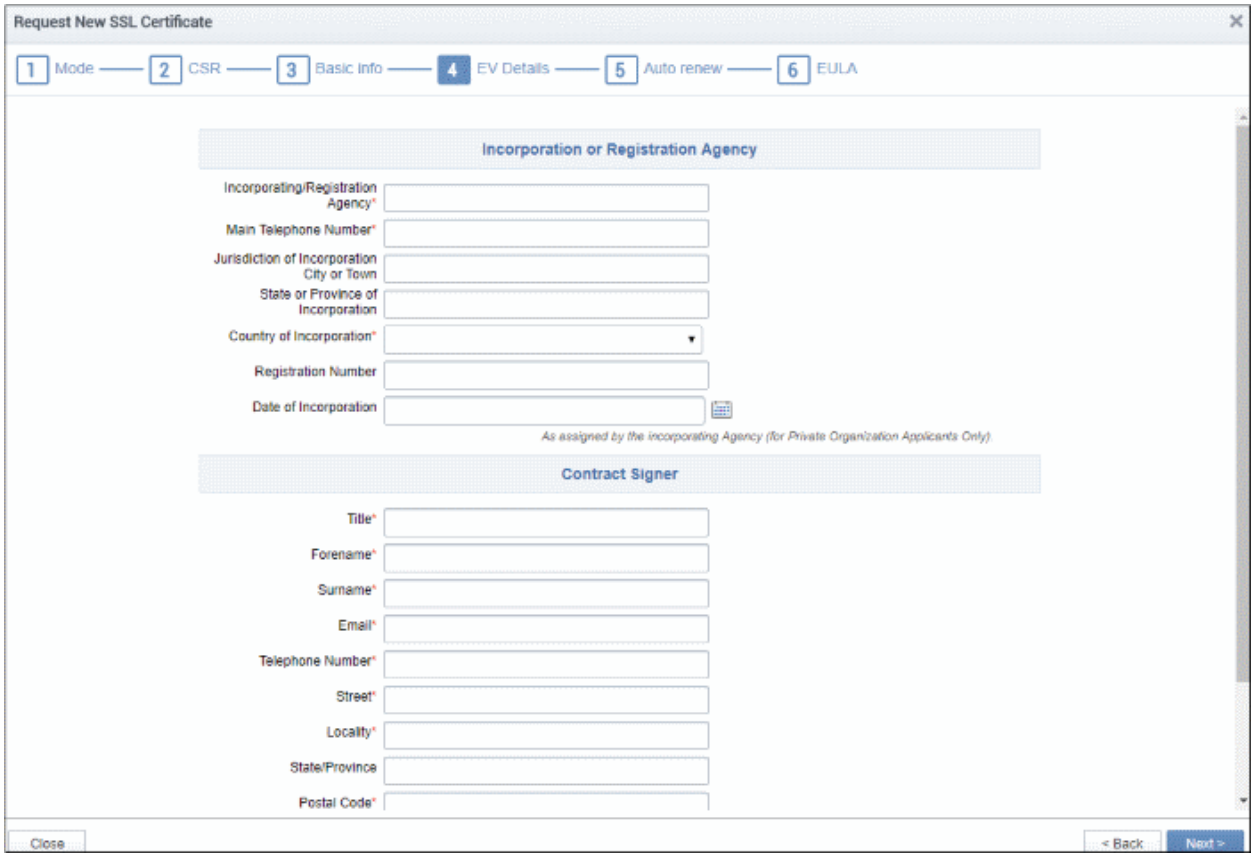


Field	Description
Organization	The organization to which the SSL certificate will belong.
Department	The department to which the SSL certificate will belong. For the certificate to be applied to all departments, select **Any**.
Certificate Type	The certificate type that you wish to add for auto-installation. The specific certificate types displayed in the list depend on the SSL Types allowed for the selected organization.
Certificate Term	The validity period of the certificate. For example, 1 year, 2 years, 3 years. The validity periods available for a particular organization depends on its configuration.
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. Each domain name should be separated by a comma. This field appears only if a multi domain or UCC certificate type is selected.
Requester	Auto-populated with the name of the administrator making the application.

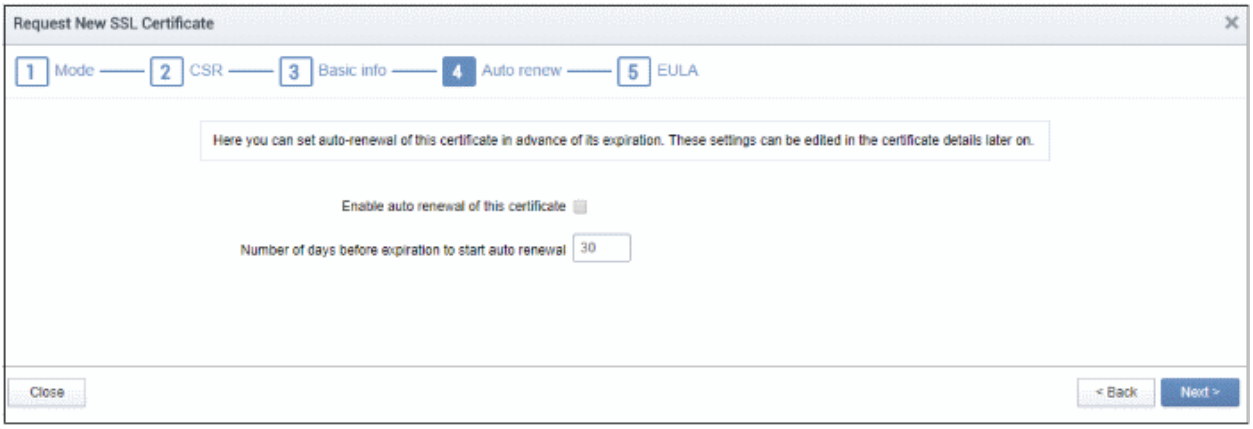
Field		Description
External Requester		The email address of an external requester on whose behalf the application is made. The requester is still the administrator that is completing this form (to view this, open the **Certificates** area and click **View** next to the subject certificate). The email address of the external requester is displayed as the **External Requester** in the **View** dialog of an issued certificate.
Click here for advanced options		Expands the advanced options shown in the following illustration. 
	Comments	Comments pertaining to the certificate.
	Address fields[a]	The address fields in the certificate are auto-populated from the details in the **General Properties** area (see general settings of the organization or department on whose behalf this certificate request is being made). These fields cannot be modified but, in the case of OV-level certificates, you can choose to omit them from the certificate by selecting **Remove** next to the fields. The allowed address details appear in the issued certificate and the removed details appear as **Details Omitted**. For the EV level certificates, you must include and display address details of the organization, corporation or registration agency, certificate requester and the contract signer. Therefore fields for entering the these address details are displayed, as shown in the following illustration, and the option to remove certain fields is not available on the EV self-enrollment form upon selecting **Sectigo EV SSL Certificate** or **Sectigo EV Multi-Domain SSL Certificate** from the **Certificate Type** list.

a. The option to hide address fields is only available if configured for your organization or department.

- Click **Next** to open the E**V Details** page of the wizard that allows you to select EV certificate types, as the following illustration shows.



- Complete fields of the E**V 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** area when adding a new organization (see "Using the EV Details Area of the Add New Organization Dialog" on page 334.
- Click **Next** to open the **Auto renew** page shown in the following illustration.



- Follow this procedure to configure the auto-renewal options:
  - Select **Enable auto renewal of this certificate** to have SCM apply for a new certificate when the current one approaches expiry.

- 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.

- Click **Next** to open the final page of the wizard shown in the following illustration.

- Use the **EULA** page of the wizard to read the EULA fully and accept by the selecting **I Agree**, and then click **OK** to submit the application.

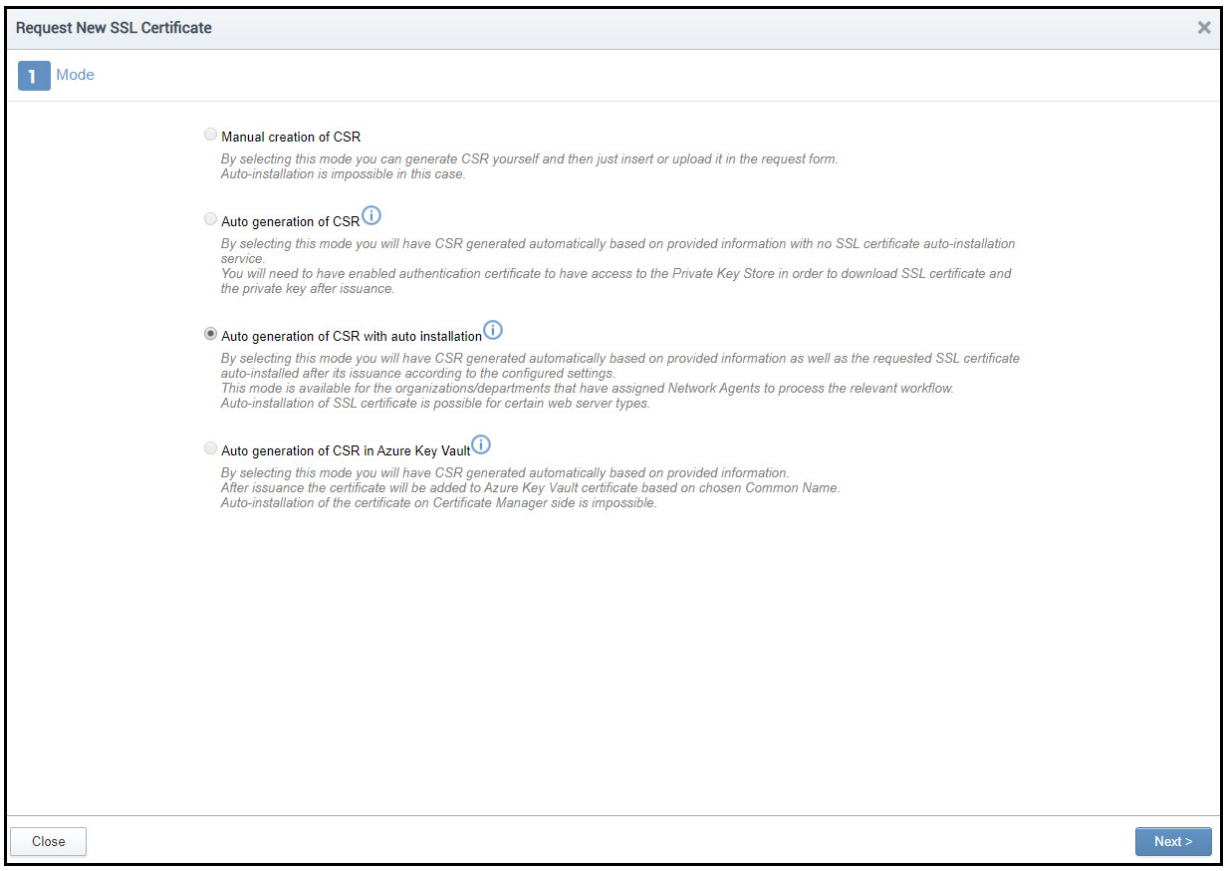
Upon completion of the wizard, the certificate is added to the **SSL Certificates** screen with a status of **Requested**. The next phase of the process is to have the requested certificated approved (see "Approving, Declining, Viewing, and Editing Certificate Requests" on page 121).

3.2.4.1.5 Automatic CSR Generation, Installation, and Renewal of SSL Certificates

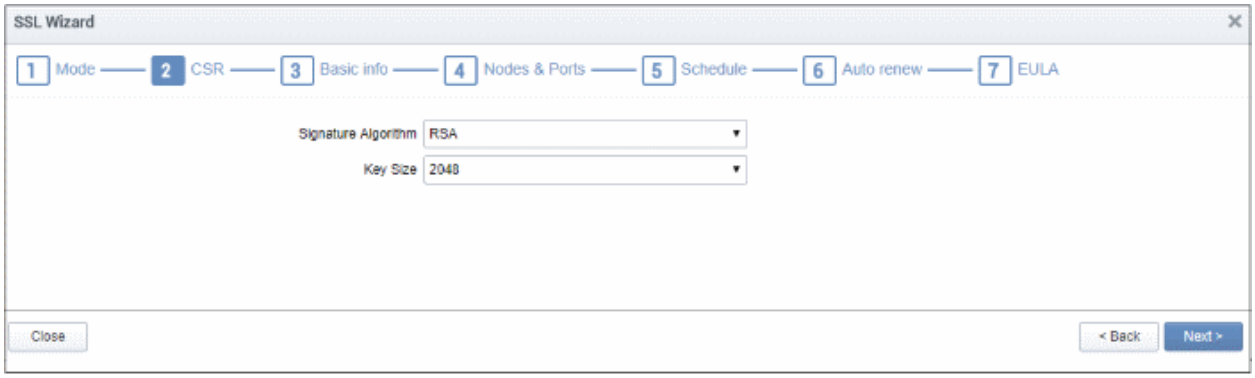
Before managing the automatic installation and renewal of SSL certificates, you must have a Network Agent configured appropriately. For more information, see "Configuring Network Agents" on page 252.

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

1. Navigate to **Certificates > SSL Certificates**.
2. Click **Add** to start the **SSL Wizard** shown in the following illustration.

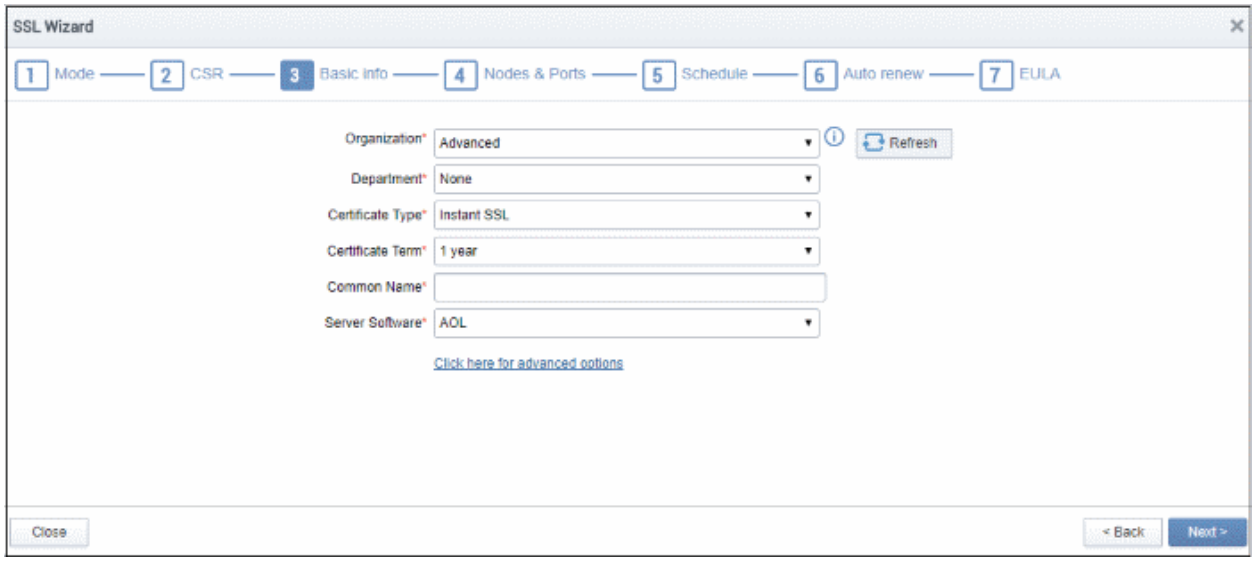


3. Select **Auto generation of CSR with auto installation**.
4. Click **Next** to continue to the CSR details section shown in the following illustration.

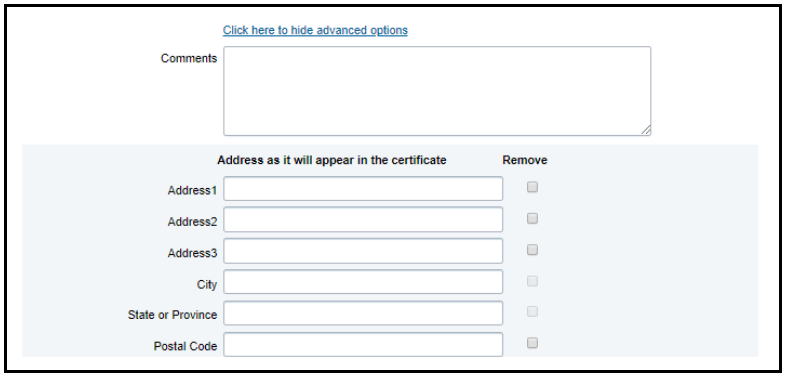


5. Specify the CSR parameters, as follows:
   - In the **Signature Algorithm** field, select the digital signature algorithm you want to use in the certificate. Currently, only RSA is supported.
   - In the **Key Size** field, select either 2048 or 4096. The former is the recommended industry standard 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.

6. Click **Next** to open the next page of the wizard shown in the following illustration, and then specify values based on the information provided in the following table. The mandatory settings are marked by a red asterisk.

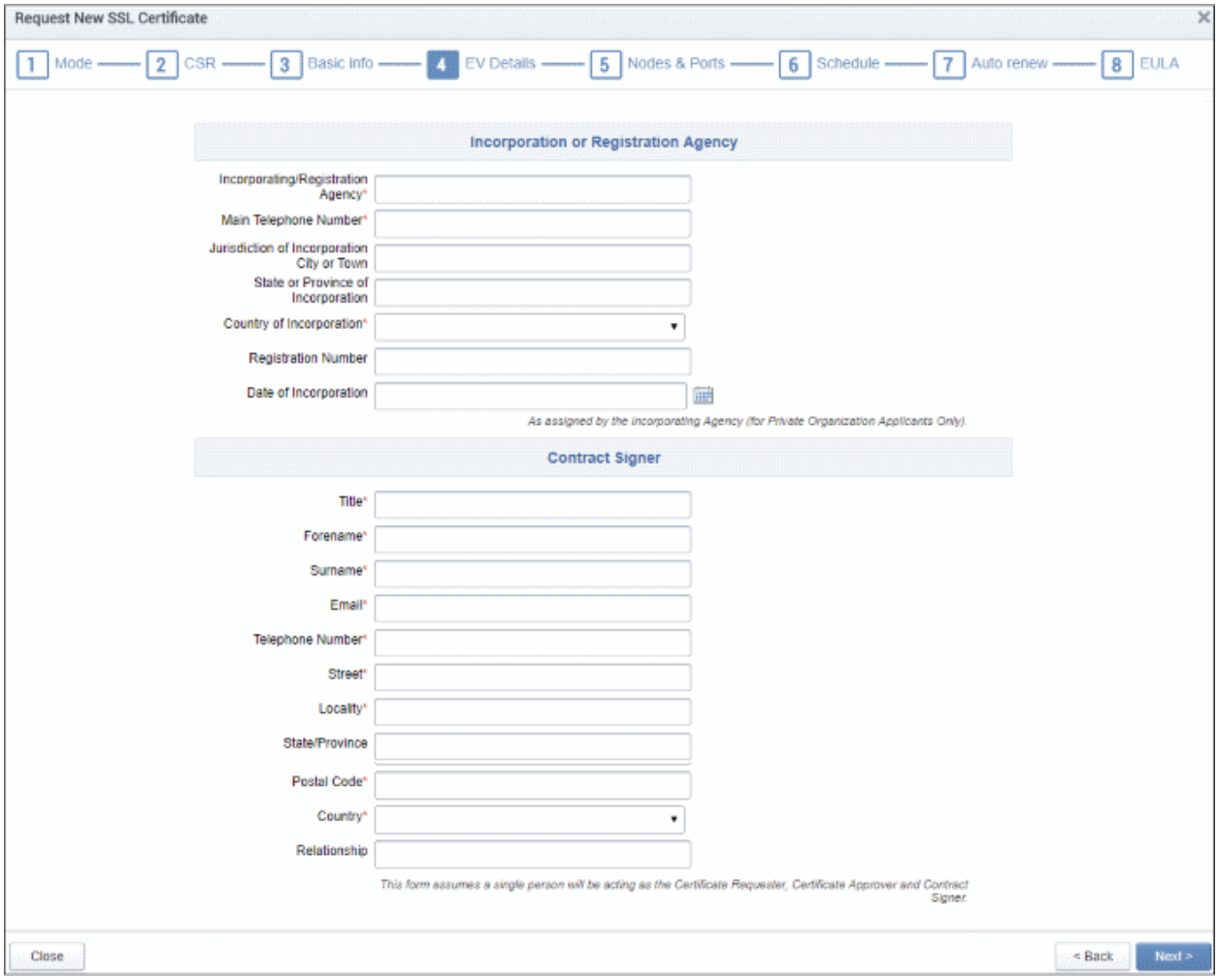


Field	Description
Organization	The organization to which the SSL certificate will belong.
Department	The department to which the SSL certificate will belong. For the certificate to be applied to all departments, select **Any**.
Certificate Type	The certificate type that you wish to add for auto-installation. The specific certificate types displayed in the list depend on the SSL Types allowed for the selected organization.
Certificate Term	The validity period of the certificate. For example, 1 year, 2 years, 3 years. The validity periods available for a particular organization depends on its configuration.
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. Each domain name should be separated by a comma. This field appears only if a multi domain or UCC certificate type is selected.
Requester	Auto-populated with the name of the administrator making the application.

Field		Description
External Requester		The email address of an external requester on whose behalf the application is made. The requester is still the administrator that is completing this form (to view this, open the **Certificates** area and click **View** next to the subject certificate). The email address of the external requester is displayed as the **External Requester** in the **View** dialog of an issued certificate.
Click here for advanced options		Expands the advanced options shown in the following illustration. 
	Comments	Comments pertaining to the certificate.
	Address fields[a]	The address fields in the certificate are auto-populated from the details in the **General Properties** area (see general settings of the organization or department on whose behalf this certificate request is being made). These fields cannot be modified but, in the case of OV-level certificates, you can choose to omit them from the certificate by selecting **Remove** next to the fields. The allowed address details appear in the issued certificate and the removed details appear as **Details Omitted**. For the EV level certificates, you must include and display address details of the organization, corporation or registration agency, certificate requester and the contract signer. Therefore fields for entering the these address details are displayed, as shown in the following illustration, and the option to remove certain fields is not available on the EV self-enrollment form upon selecting **Sectigo EV SSL Certificate** or **Sectigo EV Multi-Domain SSL Certificate** from the **Certificate Type** list.

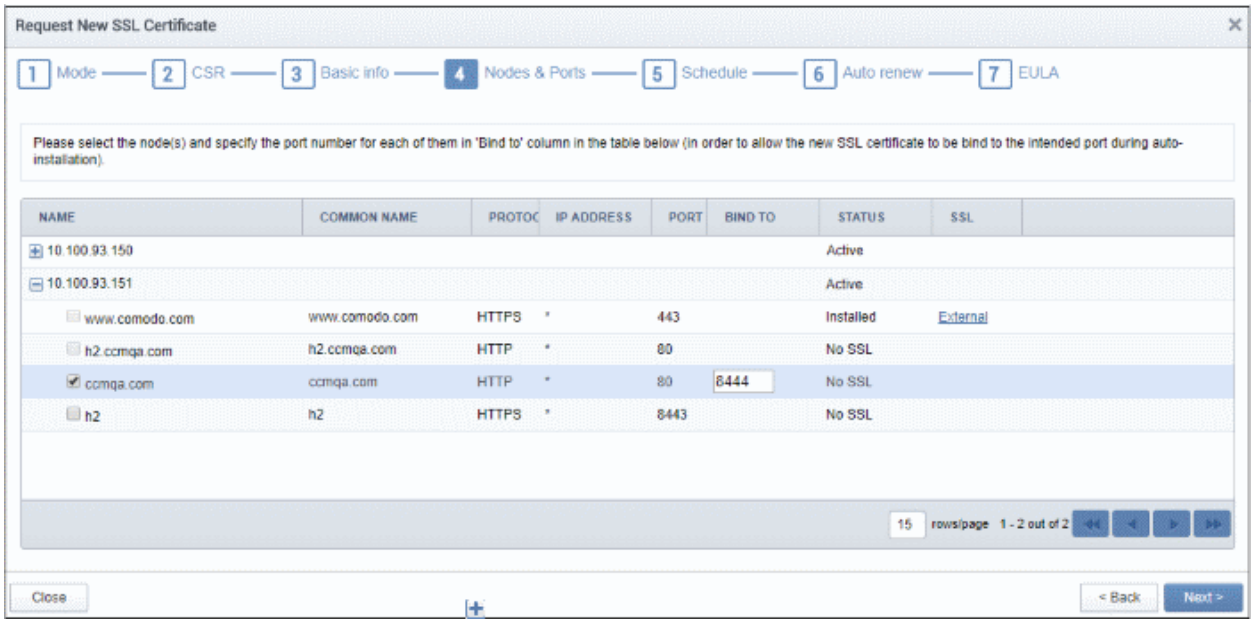
a. The option to hide address fields is only available if configured for your organization or department.

7. Click **Next** to open the **EV Details** page of the wizard that allows you to select EV certificate types, as shown in the following illustration.



The information that needs to be provided via the wizard page shown in the preceding illustration depends on the EV mode activated for your account. Typically, this is same information that is provided in the EV Details area when adding a new organization (see "Using the EV Details Area of the Add New Organization Dialog" on page 334). If the EV type is RA for your account, this information is auto-populated.

8. Click **Next** to open the **Nodes & Ports** page of the wizard shown in the following illustration.



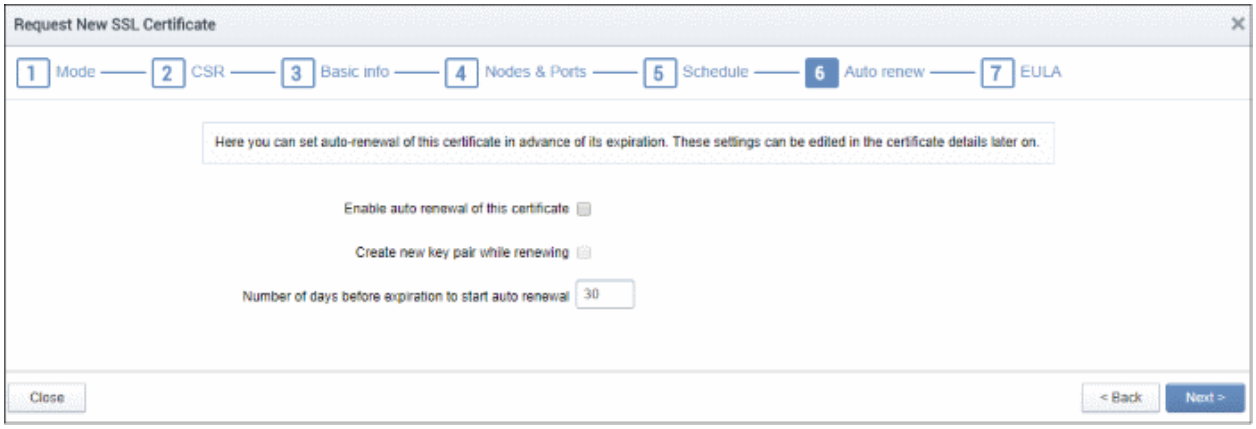
9. Select the server(s) hosting your target domain(s).
10. Select the domain(s) on which you want to install the certificate, and then supply a value for the **Bind To** column which corresponds to the port number to which the SSL certificate should be bound after issuance. This value is only editable for a protocol with HTTP status.
11. Click **Next** to open the **Schedule** page of the wizard shown in the following illustration.

12. Use the **Schedule** page to choose whether you want to start auto-installation manually or schedule it for a later time, as follows:
    - Select **Triggered auto-installation** to start the auto-installation manually after completing the wizard. To do this, navigate to **Certificates > SSL Certificates** from the main UI, select the certificate, and then click **Install**.
    - Select **Scheduled auto-installation** 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.

13. If you selected **Scheduled auto-installation** populate the **Schedule** fields based on the 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.

14. Click **Next** to open the **Auto renew** page shown in the following illustration.



15. 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.

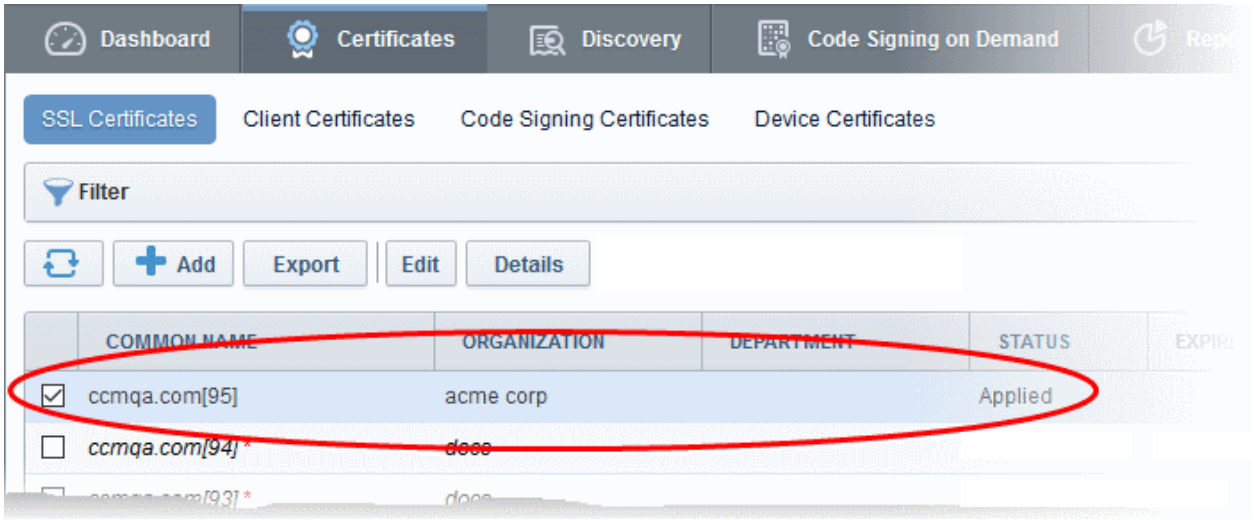
       If auto-renewal is enabled, certificates requested using the **Auto generation of CSR with auto installation** setting are installed automatically at the time of renewal.
16. Click **Next** to open the final page of the wizard shown in the following illustration.

17. Read the End User License Agreement (EULA) and accept it by the selecting **I Agree**, and then click **OK** to submit the application.

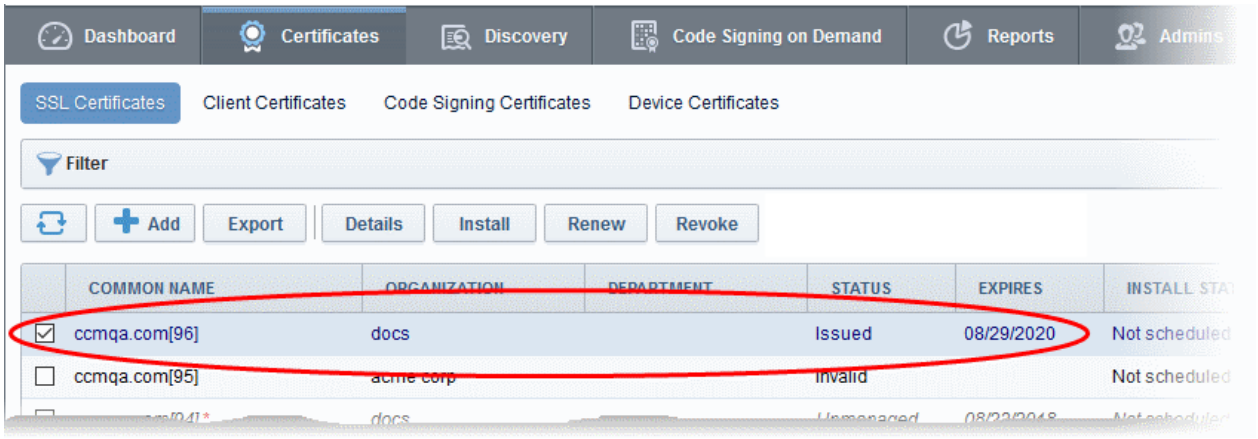
Upon completion of the wizard, the certificate is added to the **SSL Certificates** UI with a status of **Requested**.

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 certificated approved (see "Approving, Declining, Viewing, and Editing Certificate Requests" on page 121).

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

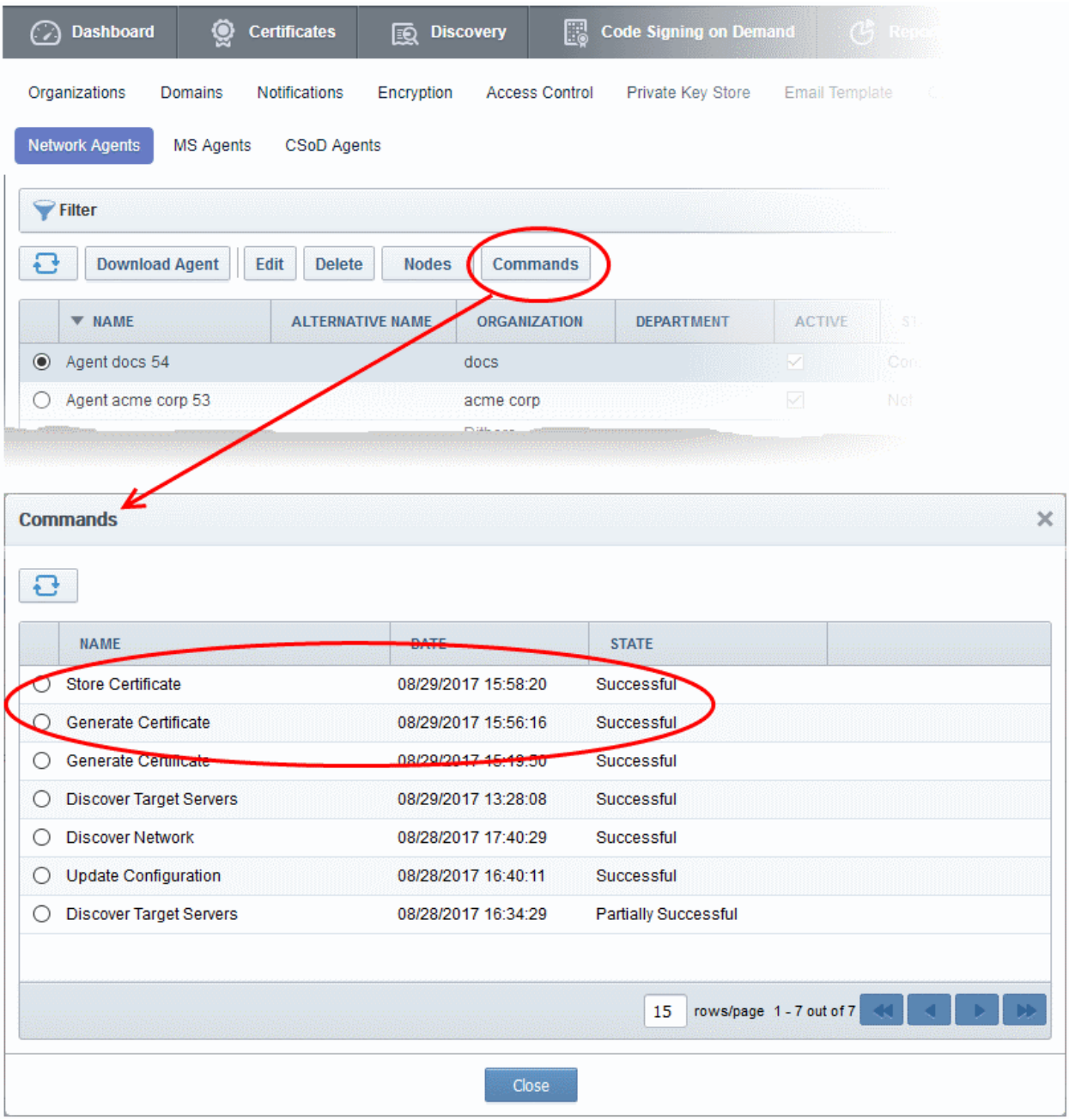


The agent tracks the order number and downloads the certificate once it is issued. The certificate is then stored and its status changes to **Issued**, as the following illustration shows.



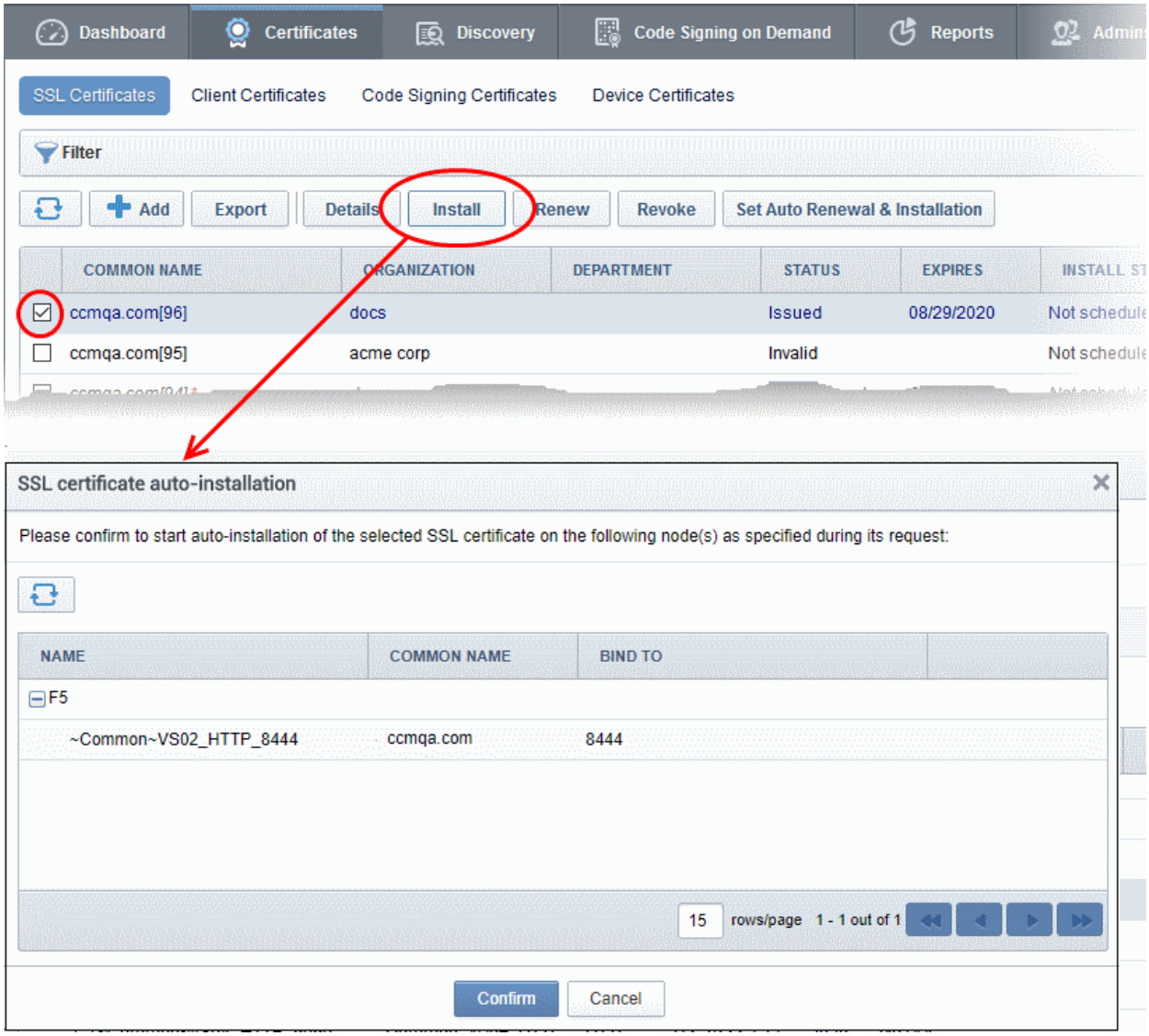
You can check whether or not the agent has stored the certificate as follows:

1. Navigate to **Settings > Agents > Network Agents**.
2. Select the agent and click **Commands** shown in the following illustration.
3. Observe the results of the successful execution of **Store Certificate** command. Upon completion, the certificate is stored on the server by the agent.



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

1. Select a certificate from the **Certificates > SSL Certificates**, and click **Install**, as shown in the following illustration.

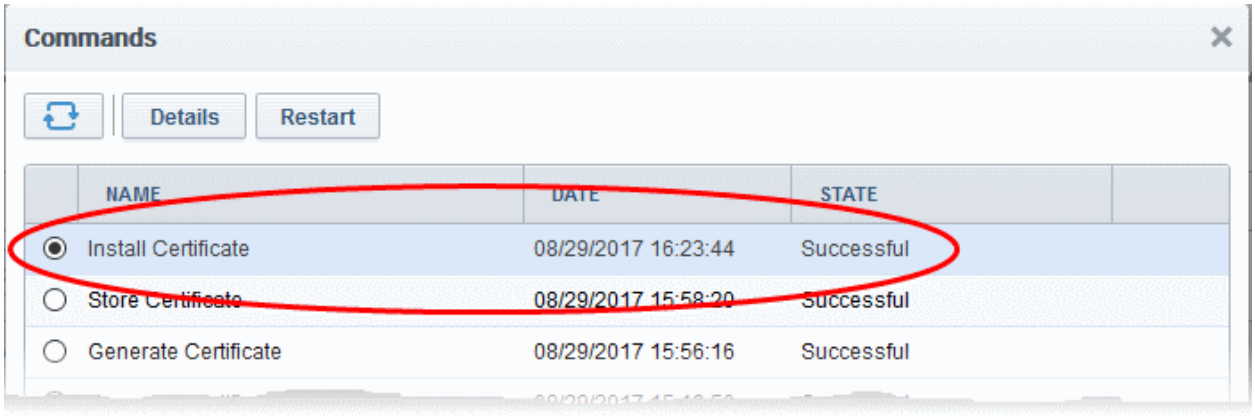


The certificate installation begins instantly. Once the installation starts, the **Install Status** of the certificate changes to **Started**, as shown in the following illustration.

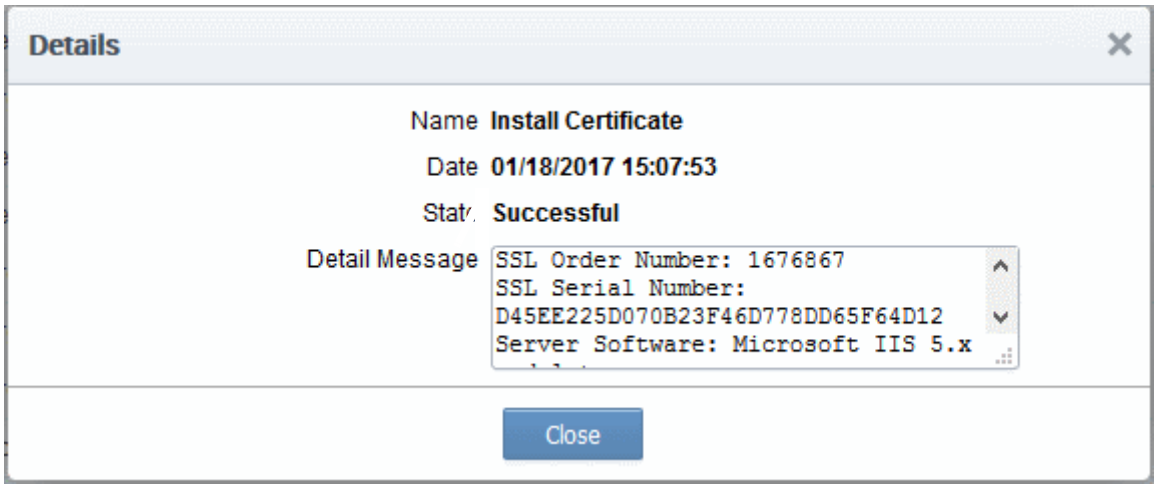
When the installation completes, various servers process the certificates in the following ways:

- On IIS servers, Tomcat, and F5 BIG-IP, the certificate is activated immediately and the install status changes to **Successful**.
- On Apache, the certificate becomes active after the server is restarted. The install status 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 64 for more information.

After restarting the server, the certificate is activated and the install status changes to **Successful**. To check whether or not the agent has installed the certificate, navigate to **Settings > Agents > Network Agents** from the main UI, select the agent, and then click **Commands** to see a successful execution of the **Install Certificate** command. To view the command details, select the command and click **Details**.



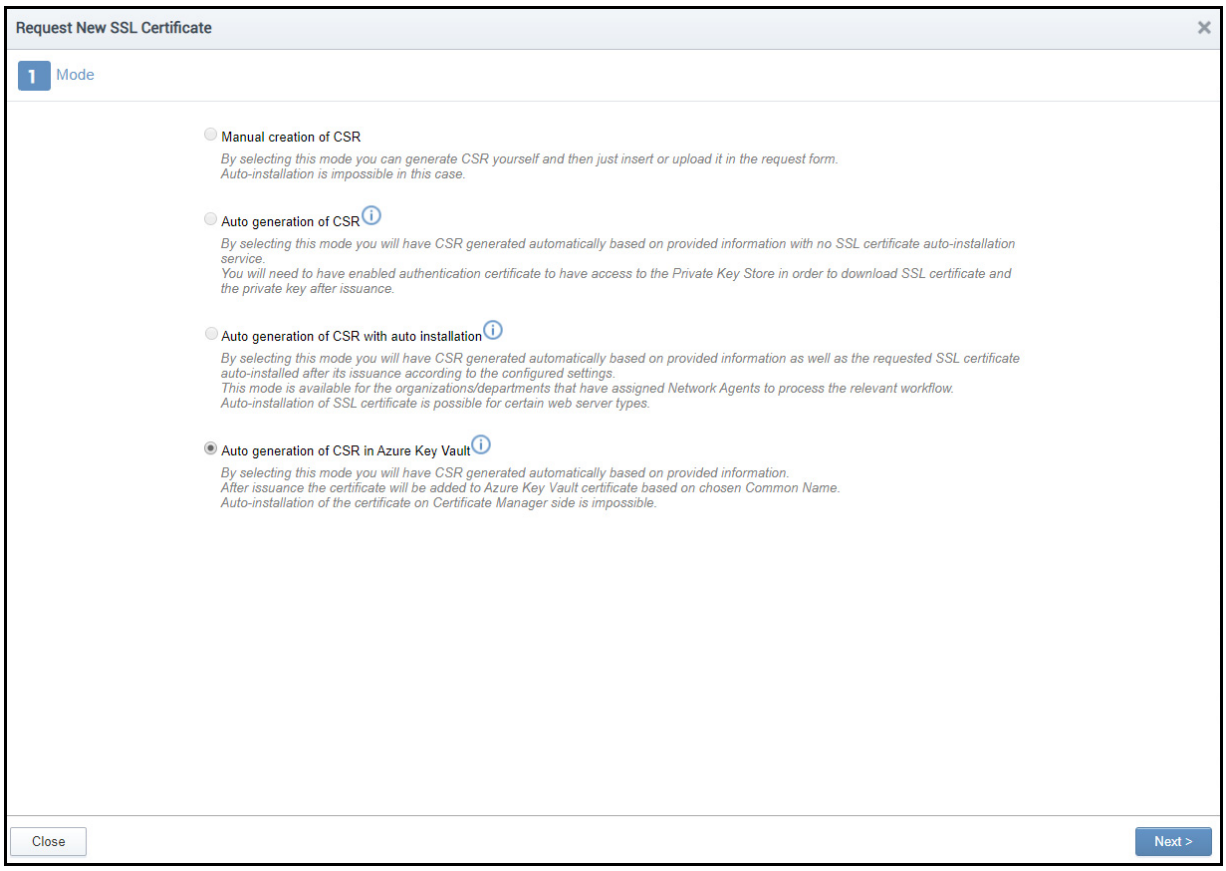
To view the command details, select the command and click **Details** to open the **Details** dialog shown in the following illustration.



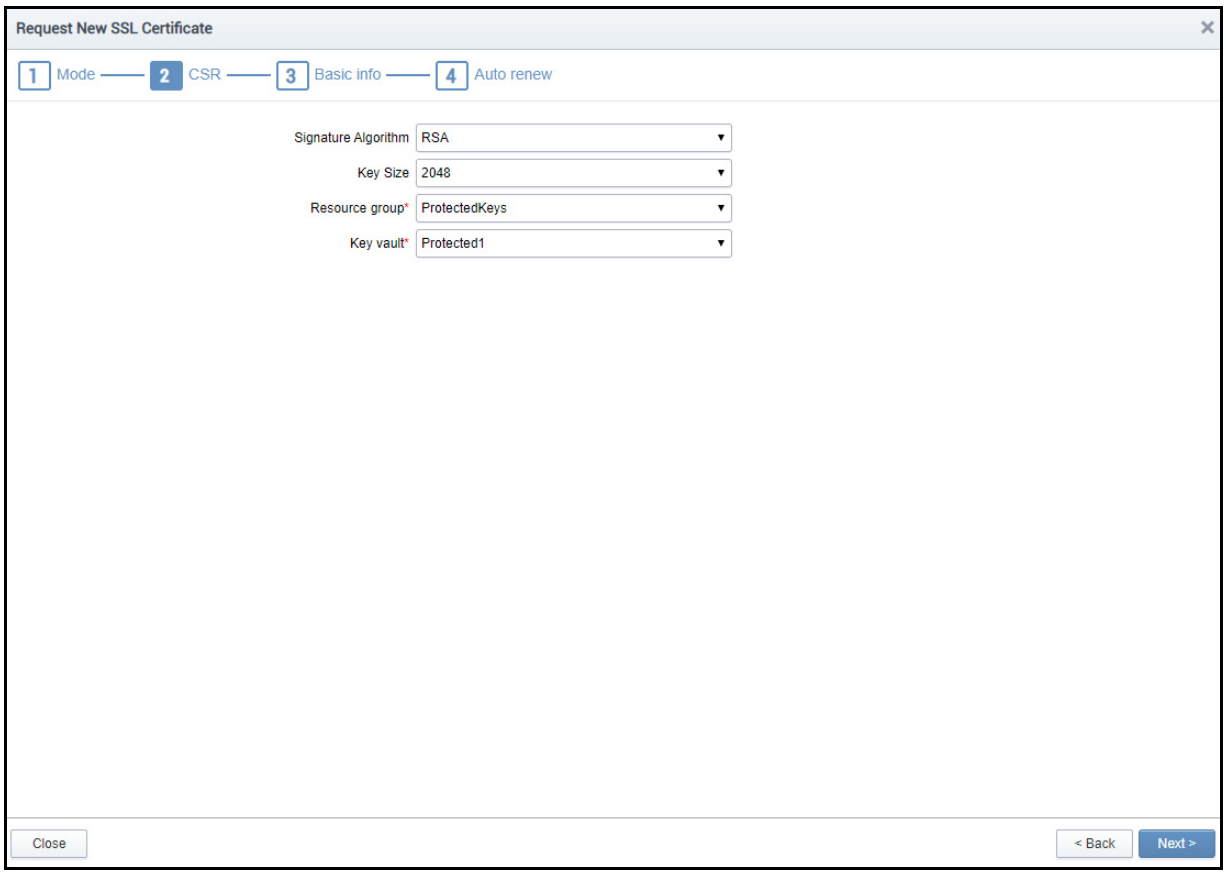
3.2.4.1.6 Automatic CSR Generation in Azure Key Vault

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

1. Navigate to **Certificates > SSL Certificates** and click **Add** to open the **Request New SSL Certificate** wizard, as shown in the following illustration.



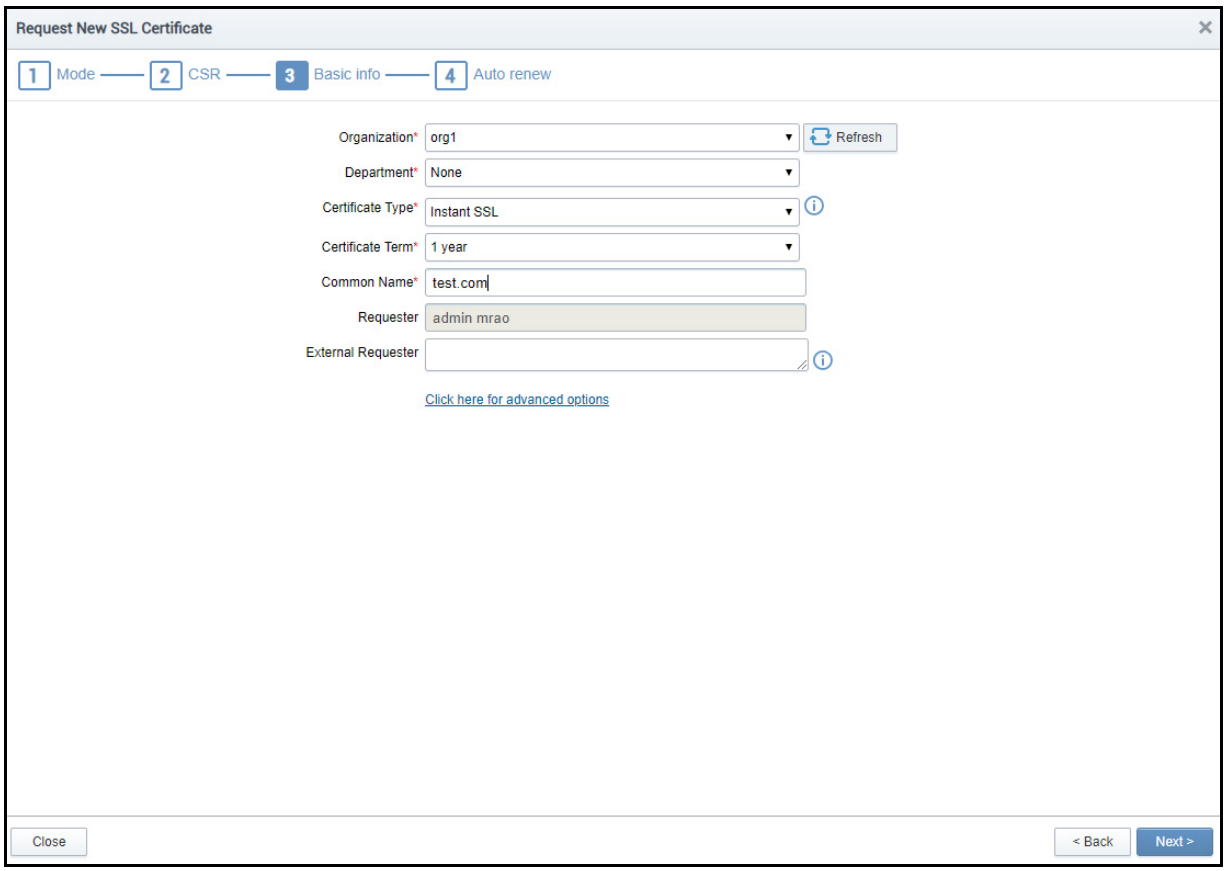
2. Select **Auto generation of CSR in Azure Key Vault**.
3. Click **Next** to open the **CSR** page shown in the following illustration.



4. Specify the CSR parameters based on the information provided in the following table.

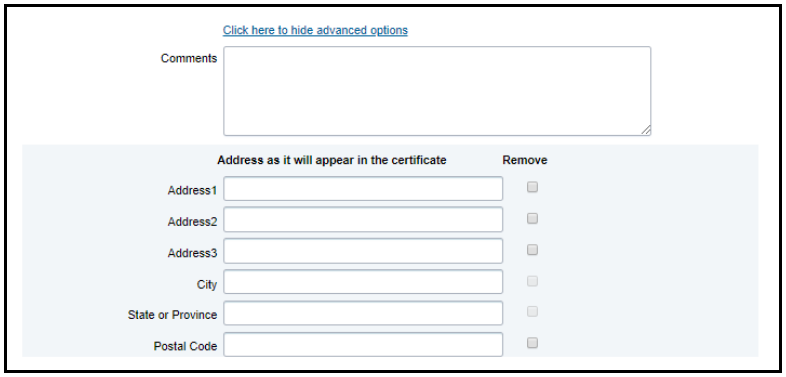
Field	Description
Signature Algorithm	Select the digital signature algorithm you want to use in the certificate. Currently, only RSA is supported.
Key Size	Select either 2048 or 4096. The former is the recommended industry standard and provides very high security for public-facing and internal hosts. 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.
Resource group	Select the resource group containing the appropriate Key Vault.
Key vault	Select the Key Vault in which the CSR is to be generated.

5. Click **Next** to open the **Basic info** page of the wizard shown in the following illustration.



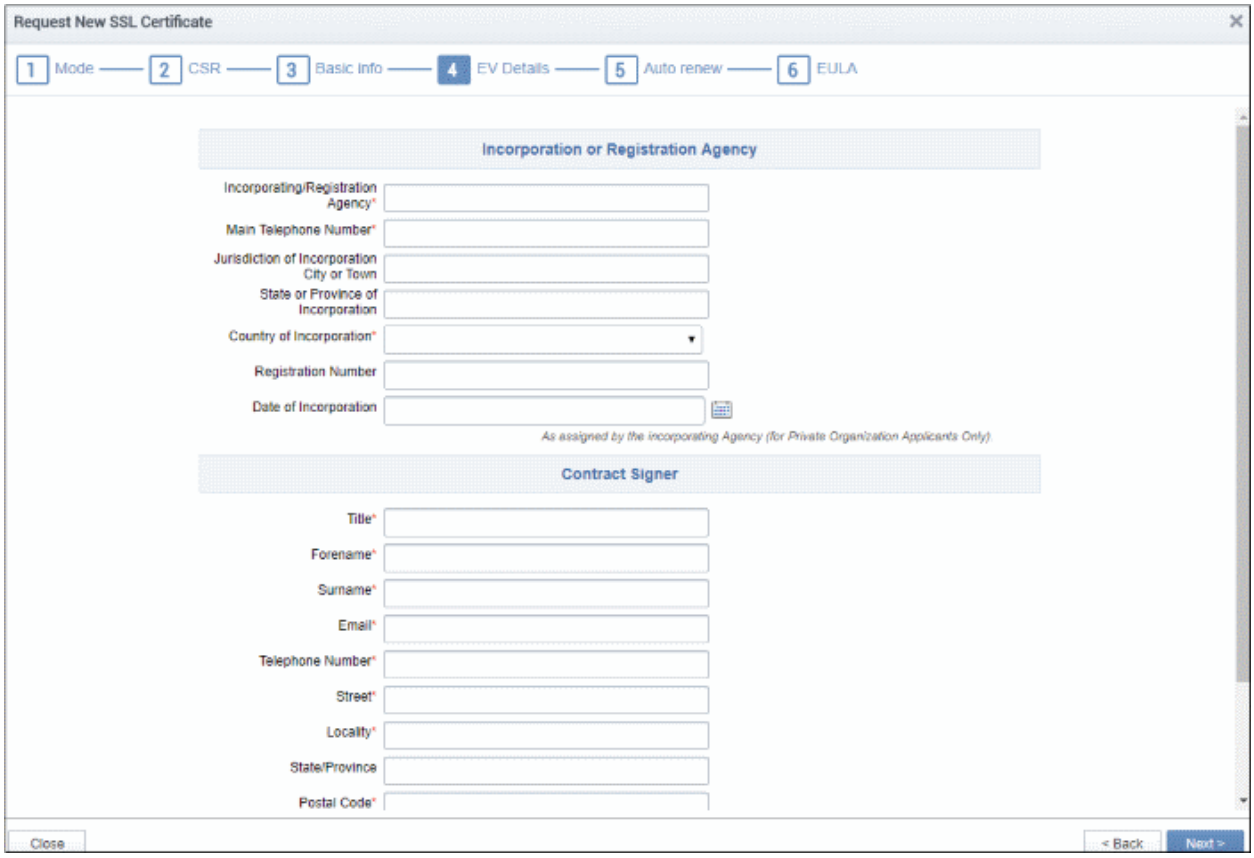
6. Complete the **Basic info** fields based on the information provided in the following table.

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 Type	The certificate type that you wish to add for auto-installation. The specific certificate types displayed in the list depend on the SSL Types allowed for the selected organization.
Certificate Term	The validity period of the certificate. For example, 1 year, 2 years, 3 years. The validity periods available for a particular organization depends on its configuration.
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. Each domain name should be separated by a comma. This field appears only if a multi domain or UCC certificate type is selected.

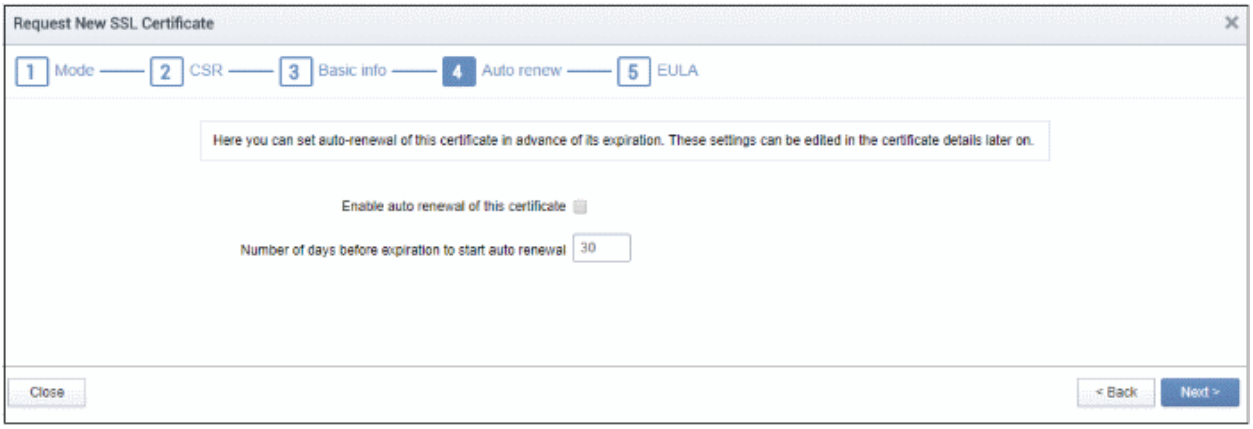
Field		Description
Requester		Auto-populated with the name of the administrator making the application.
External Requester		The email address of an external requester on whose behalf the application is made. The requester is still the administrator that is completing this form (to view this, open the **Certificates** area and click **View** next to the subject certificate). The email address of the external requester is displayed as the **External Requester** in the **View** dialog of an issued certificate.
Click here for advanced options		Expands the advanced options shown in the following illustration. 
	Comments	Comments pertaining to the certificate.
	Address fields[b]	The address fields in the certificate are auto-populated from the details in the **General Properties** area (see general settings of the organization or department on whose behalf this certificate request is being made). These fields cannot be modified but, in the case of OV-level certificates, you can choose to omit them from the certificate by selecting **Remove** next to the fields. The allowed address details appear in the issued certificate and the removed details appear as **Details Omitted**. For the EV level certificates, you must include and display address details of the organization, corporation or registration agency, certificate requester and the contract signer. Therefore fields for entering the these address details are displayed, as shown in the following illustration, and the option to remove certain fields is not available on the EV self-enrollment form upon selecting **Sectigo EV SSL Certificate** or **Sectigo EV Multi-Domain SSL Certificate** from the **Certificate Type** list.

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.
b. The option to hide address fields is only available if configured for your organization or department.

7. Click **Next** to open the **EV Details** page of the wizard, as shown in the following illustration.



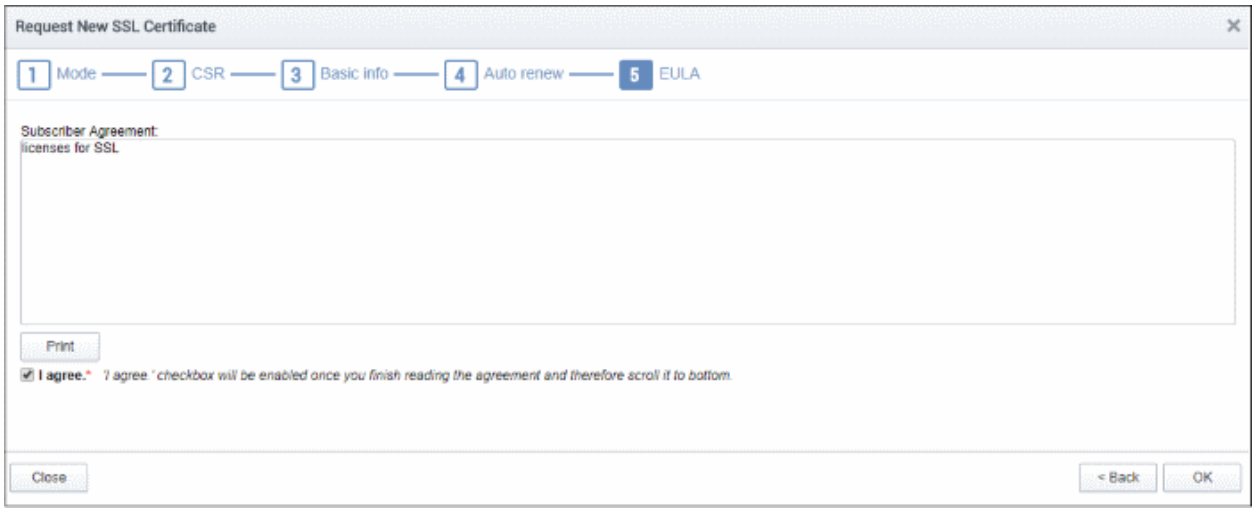
8. Complete fields of the **EV Details** page. The fields you need to complete depend on the EV mode activated for your account. Typically, it would be the same information as provided in the **EV Details** area when adding a new organization (see "Using the EV Details Area of the Add New Organization Dialog" on page 334).
9. Click **Next** to open the **Auto renew** page shown in the following illustration.



10. Follow this procedure to configure the auto-renewal options:
    - Select **Enable auto renewal of this certificate** to have SCM apply for a new certificate when the current one approaches expiry.

- 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, as shown in the following illustration.



12. Read the EULA fully and accept by the 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 certificated approved (see "Approving, Declining, Viewing, and Editing Certificate Requests" on page 121).

3.2.4.1.7 Certificate Collection

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 applicant. The applicant can download the certificate by clicking the link provided in the email.

The certificate collection email whose example is shown in the following illustration contains a summary of the certificate details, a link to the certificate collection form, and a unique certificate ID that is used for validation.

Hello,

You have successfully enrolled for a SSL certificate.

You now need to complete the following steps:

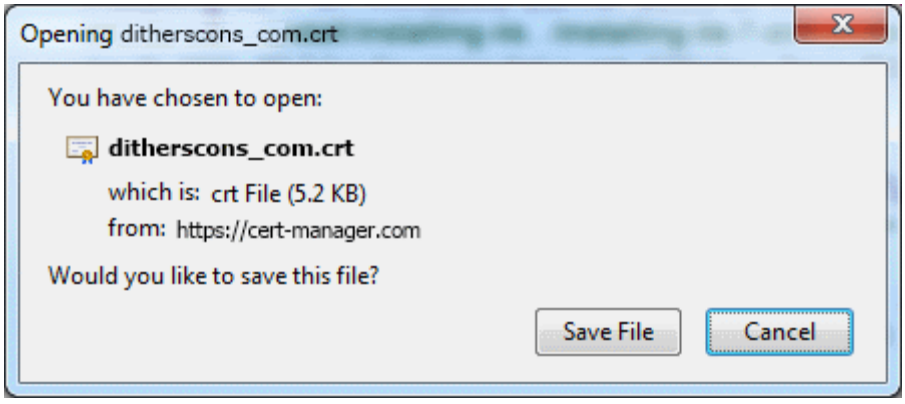
* Click the following link to download your SSL certificate
Format(s) most suitable for your server software:
as Certificate (w/ chain), PEM encoded: https://ccmqa.com/customer/110/ssl?action=download&sslId=84106&format=x509

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

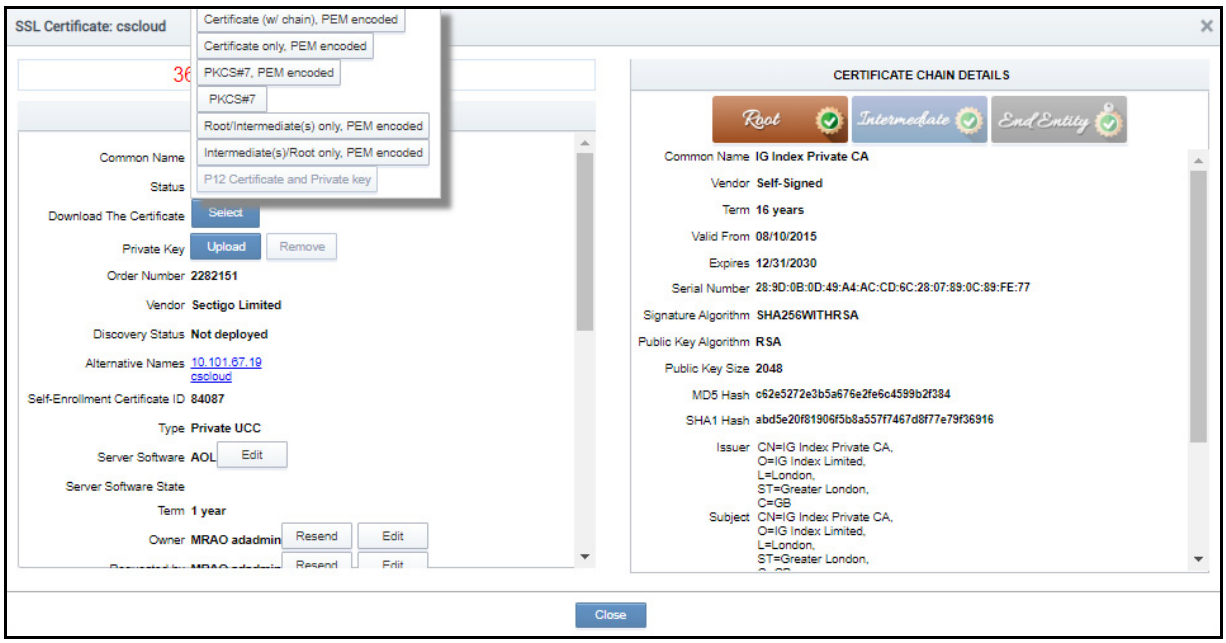
Issuing CA certificates only:
as Root/Intermediate(s) only, PEM encoded: https://ccmqa.com/customer/110/ssl?action=download&sslId=84106&format=x509IO
as Intermediate(s)/Root only, PEM encoded: https://ccmqa.com/customer/110/ssl?action=download&sslId=84106&format=x509IOR

* Import your new certificate into your server (Please contact your administrator for help with this).
* Your renew id: uuMjRAlGHlxLS36EYcnK

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 :



MRAO, RAO SSL, and DRAO SSL administrators can download the certificate and provide it to the applicant. To do this, you use the SCM UI to navigate to **Certificates > SSL Certificates**, select the certificate, and click **Details**, as shown in the following illustration.



The details dialog shown in the preceding illustration allows you to download the issued certificate in different formats by clicking **Select** and trigger the download in the format of your choice.

If the private key is managed by the SCM's PKS, you have the option to download the certificate along with the private key. 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.

Certificates can only be download in the `.p12` format after you have authenticated yourself with a customer certificate at the computer from which you are accessing SCM.

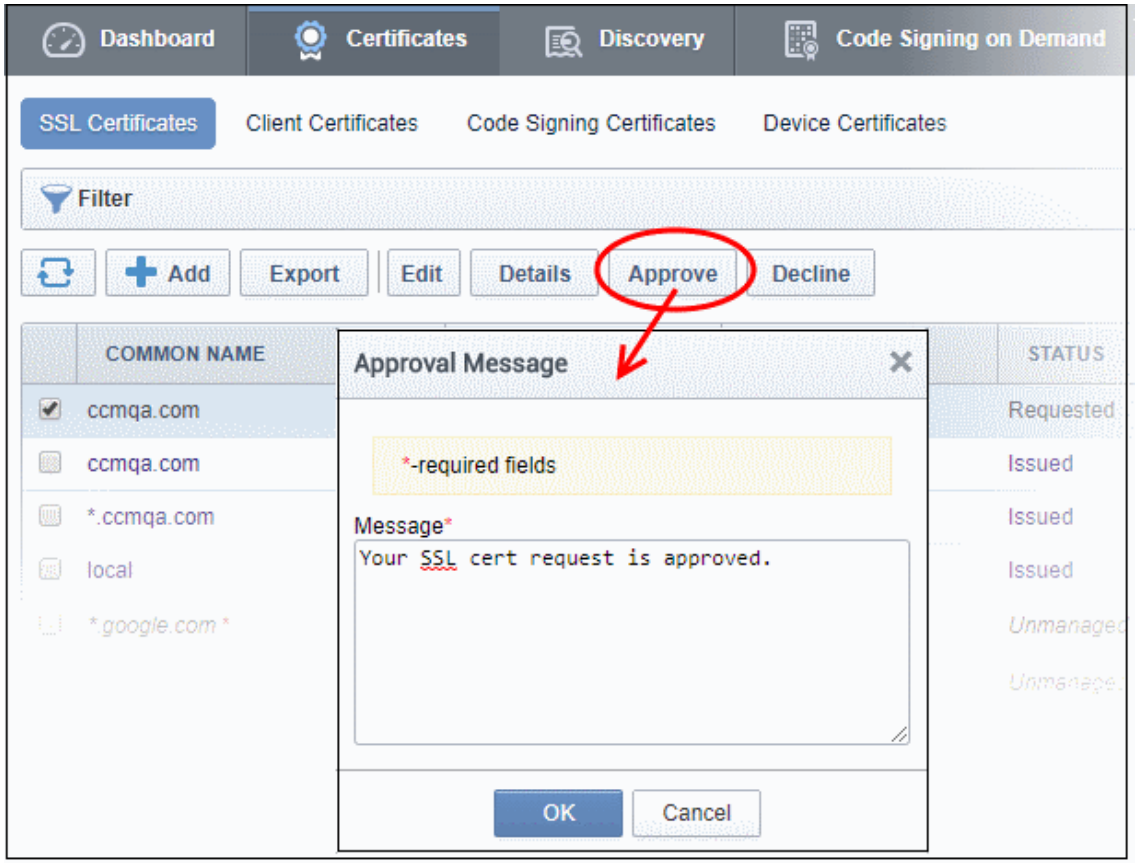
3.2.4.1.8 Download and Import of SSL Certificates

Once the application process has been successfully completed, the applicant needs to download the certificate, save it in a secure location on their hard drive, and then import it into the certificate store on their computer.

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.

3.2.4.2 Approving, Declining, Viewing, and Editing Certificate Requests

After a successful application via either the auto-installer, SSL certificate enrollment form, or built-in wizard, a certificate request appears in the **Certificates > SSL Certificates** area of the SCM UI. 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, as shown in the following illustration. 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 the administrator who can approve their own request.



You can view information about the certificate by clicking **Details**.

You can modify the application before submitting it to Sectigo for processing by clicking **Edit**.

You can submit the application to Sectigo for processing by clicking **Approve** and typing in a message with the approval notification email.

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 44.

3.2.5 How to Renew SSL Certificates

SSL administrators can use SCM UI to either renew certificates manually or enable an automatic renewal. External applicants can renew the certificates manually via the self-renewal form.

3.2.5.1 Certificate Renewal by Administrators

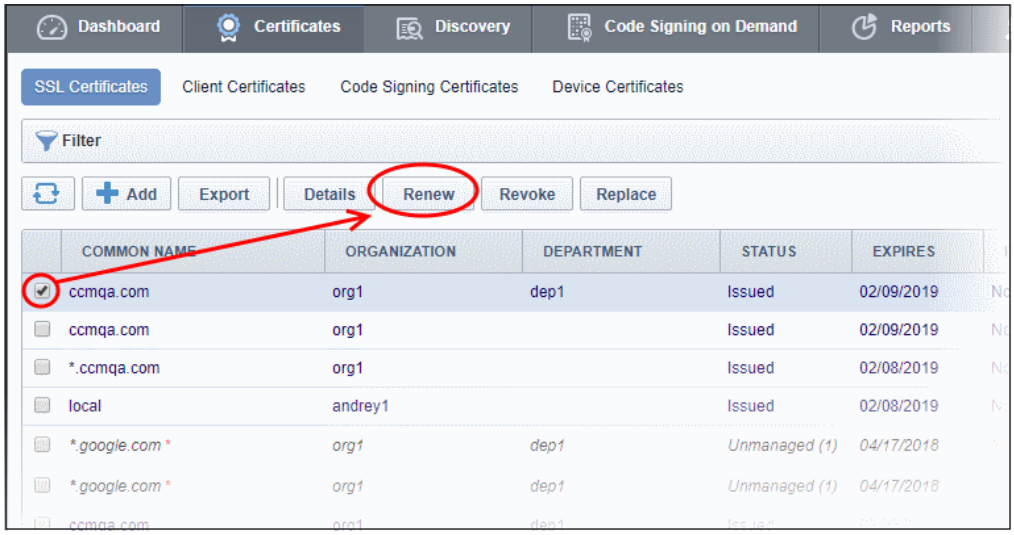
The **SSL Certificates** screen allows you to renew both managed and external (also known as unmanaged) certificates, with the renewal process being different for these two certificate types.

Managed certificates are the ones issued via SCM based on a specific combination of domain and organization. In this case, a CSR must be 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, to request renewal of such certificates, it is not required to submit a CSR because SCM can reuse the existing CSR.

External certificates are those certificates which are found during a discovery scan but were issued via SCM. To request renewal of such certificate, 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 or modified the organization's address details, 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, navigate to **Certificates > SSL Certificates**, select a managed certificate of any status, and then click **Renew**, as the following illustration shows. This instructs SCM to automatically request a renewal with the same information as the existing certificate.



Once issued, the renewed certificate becomes available for collection and installation. For more information, see "Certificate Collection" on page 119.

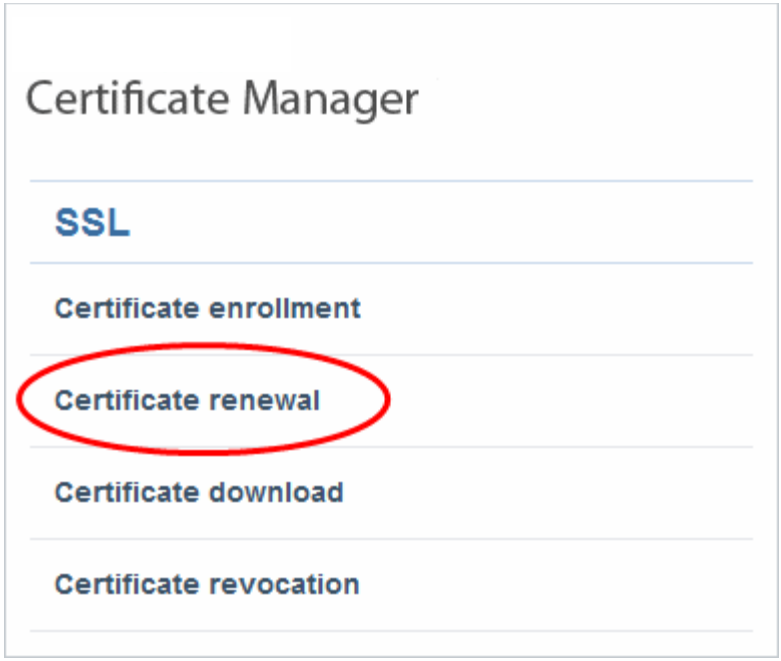
To renew an external certificate, navigate to **Certificates > SSL Certificates**, select the external certificate, and then click **Renew**. This opens the **Renew SSL Certificate** form that you must complete.

Complete the wizard by following instructions provided in section "Manual CSR Generation Via the Built-in Enrollment Wizard" on page 89.

Once issued, the renewed certificate becomes available for collection and installation. For more information, see "Certificate Collection" on page 119.

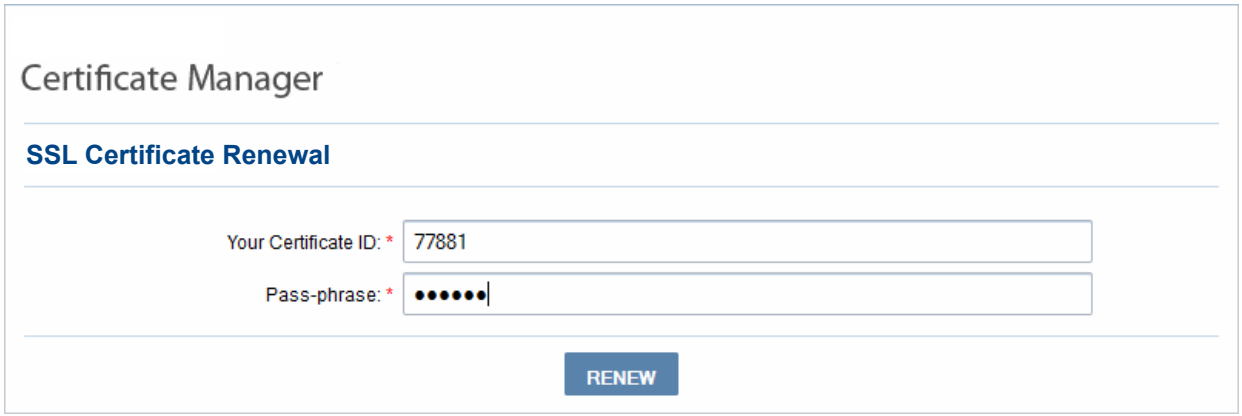
3.2.5.2 Certificate Renewal by End-Users

End-users can renew their SSL certificates through the self-renewal application form available at a location similar to `https://cert-manager.com/customer/<customer_url>/ssl`.



Clicking **Certificate renewal** opens the initial page of the self-renewal form shown in the following illustration. Before proceeding to the full renewal application form, the end-user has to authenticate the request by doing the following:

- Entering the correct certificate ID that is available from the certificate collection email and via the **Certificates > SSL Certificates** screen of SCM. You, as an administrator, may need to communicate the certificate ID to external applicants.
- Entering the certificates renewal or certificated revocation passphrase which was created during enrollment for the original certificate.



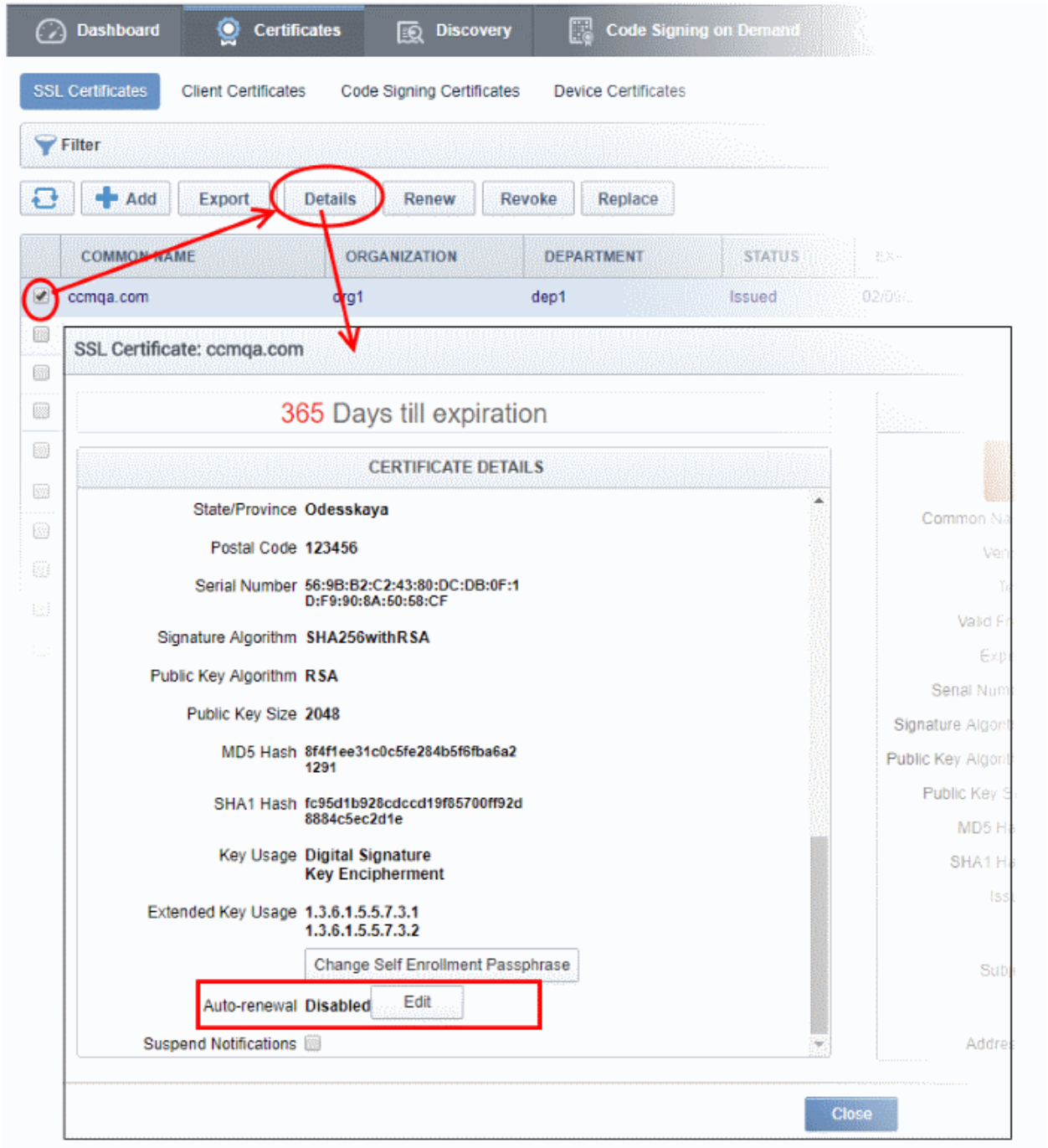
Clicking **Renew** on the **SSL Certificate Renewal** dialog shown in the preceding illustration automatically renews the certificate with the same information as in the existing certificate.

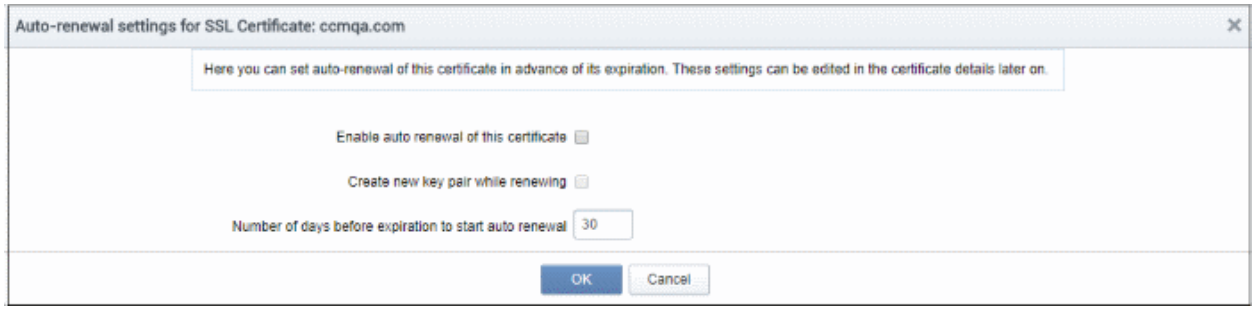
Once issued, the renewed certificate becomes available for collection and installation. For more information, see "Certificate Collection" on page 119.

3.2.5.3 Automatic Certificate Renewal Scheduling

To schedule or configure an automatic renewal of SSL certificates, follow this procedure:

- From the main SCM UI, navigate to **Certificates > SSL Certificates**, select a certificate, and then click **Details**.
- Scroll down the **CERTIFICATE DETAILS** screen and click **Edit** located to the right of **Auto-renewal**, as shown in the following illustration.


Dashboard
Certificates
Discovery
Code Signing on Demand
SSL Certificates
Client Certificates
Code Signing Certificates
Device Certificates
Filter
Add
Export
Details
Renew
Revoke
Replace
COMMON NAME
ORGANIZATION
DEPARTMENT
STATUS
ccmqa.com
org1
dep1
Issued
SSL Certificate: ccmqa.com
365 Days till expiration
CERTIFICATE DETAILS
State/Province Odesskaya
Postal Code 123456
Serial Number 56:9B:B2:C2:43:80:DC:DB:0F:1D:F9:90:8A:50:58:CF
Signature Algorithm SHA256withRSA
Public Key Algorithm RSA
Public Key Size 2048
MD5 Hash 8f4f1ee31c0c5fe284b5f6fba6a21291
SHA1 Hash fc95d1b928cdccd19f85700ff92d8884c5ec2d1e
Key Usage Digital Signature
Key Encipherment
Extended Key Usage 1.3.6.1.5.5.7.3.1
1.3.6.1.5.5.7.3.2
Change Self Enrollment Passphrase
Auto-renewal Disabled
Edit
Suspend Notifications
Close



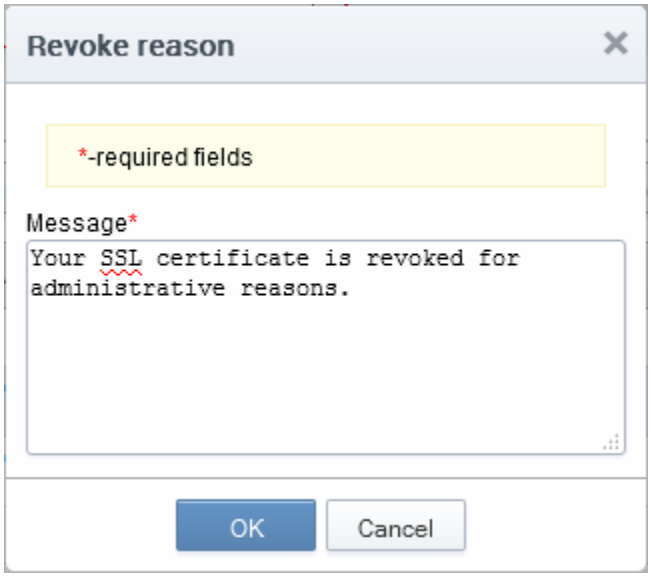
- Follow this procedure to configure the auto-renewal options:
  - Select **Enable auto renewal of this certificate** to have SCM apply for a new certificate when the current one approaches expiry.
  - Select **Create new key pair while renewing** to specify that you want to generate a new key pair for the renewed certificate. Leaving this option disabled means SCM is to reuse the key pair of the old certificate. Note that this option is available for certificates with automatic CSR generation and auto-installation.
  - 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.
  - Click **OK**.

For information on other options available in the SSL certificate details screen, see "How to View and Modify SSL Certificate Details" on page 52.

3.2.6 How to Revoke, Replace, and Delete SSL Certificates

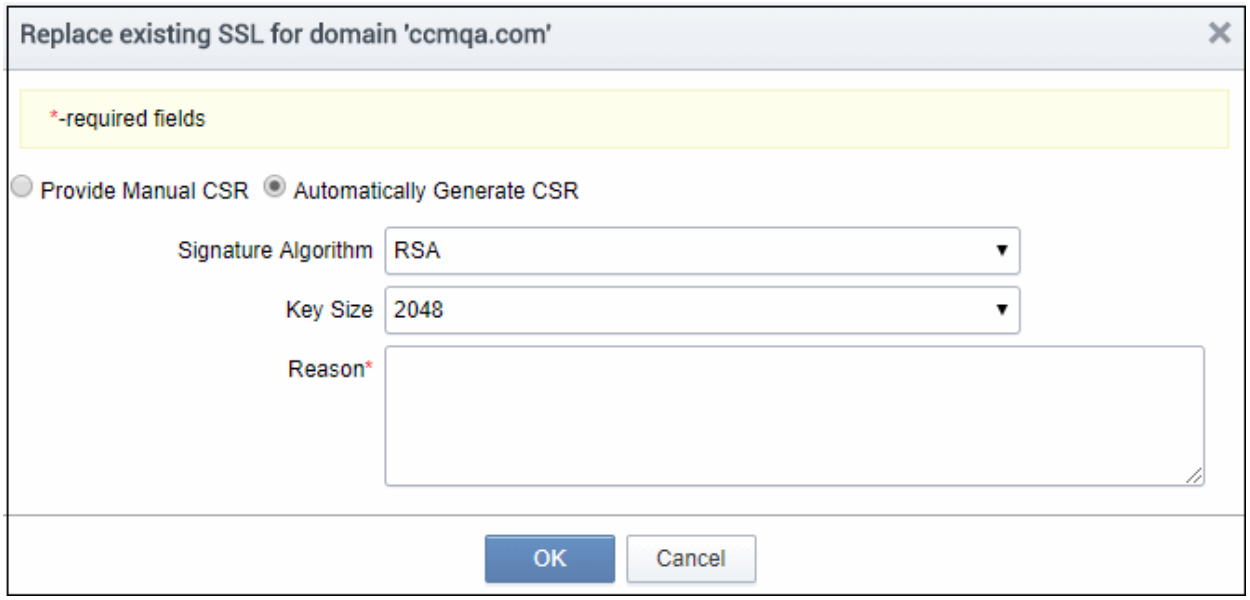
To revoke an SSL certificate, follow this procedure:

- From the main SCM UI, navigate to **Settings > Notifications** and check whether or not an SSL revoke notification has been configured for the requester. To create a new revoke notification, click **Add** and set the **Notification type** to **SSL Revoked**.
- From the main SCM UI, navigate to **Certificates > SSL Certificates**, select a certificate, and click **Revoke**.
- Use the **Revoke reason** dialog shown in the following illustration to provide an explanation to be submitted together with the revocation notification email.
- To completed the process, click **OK**.



To replace an existing SSL certificate, follow this procedure:

- From the main SCM UI, navigate to **Certificates > SSL Certificates**, select a certificate, and click **Replace** to open the **Replace existing SSL for domain** dialog shown in the following illustration.



- Use the **Replace existing SSL for domain** dialog to specify whether you want to create a new CSR manually or automatically.
- Provide a reason for replacement.
- Click **OK**.
- Depending on your selection, follow instructions provided in section "Manual CSR Generation Via the Built-in Enrollment Wizard" on page 89 or "Automatic CSR Generation Via the Built-in Enrollment Wizard" on page 96.

To delete a certificate, select it and click **Delete**. Note that you can only delete external certificates.

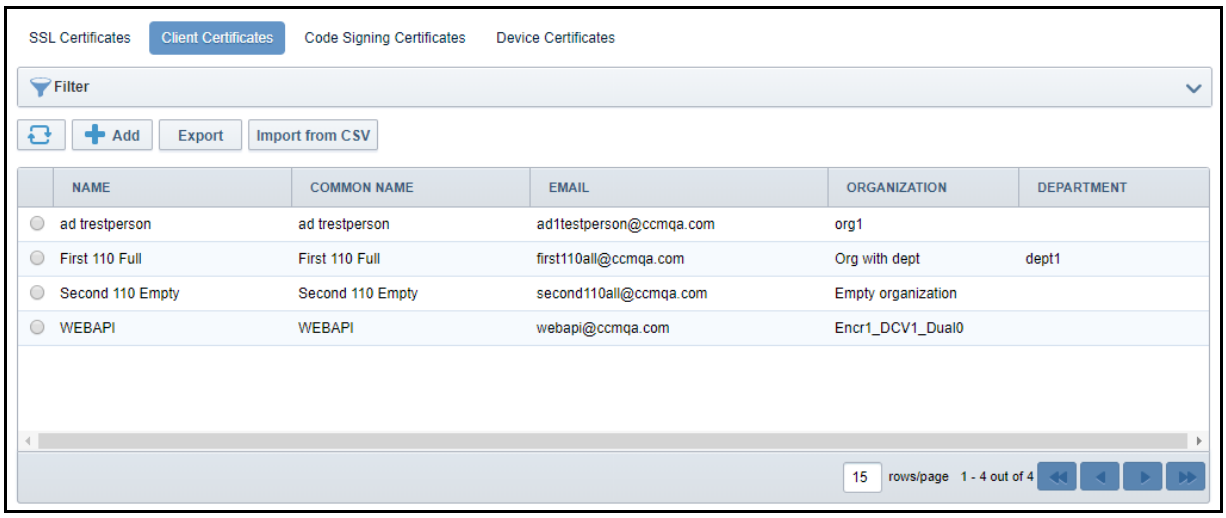
3.3 Managing Client Certificates

Depending on your security role, the **Client Certificates** area shown in the following illustration allows you to manage end-user client certificates and their owners' details.

MRAO administrators can view the client certificates and 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 these administrators.

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



The following parameters are available for client certificates:

- The **Name** column contains the end-user name.
- The **Email** column contains the end-user email address.
- The **Organization** column contains of the name of the organization to which the end-user belongs.
- The **Department** column contains of the name of the department to which the end-user belongs (if applicable).

Depending on the status of the selected certificate, you can perform the following actions on end-users and their client certificates:

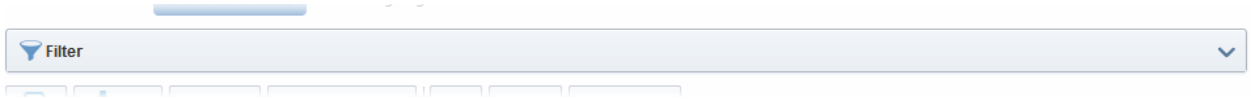
- **Add**—Allows you to add a new end-user and configure a client certificate for that user.
- **Export**—Allows you to export the currently displayed list to a spreadsheet in the `.csv` format.

- **Import from CSV**—Allows you to import a list of new end-users in the `.csv` format into the SCM database.
- **Refresh**—Allows you to update the currently displayed list of users, such as remove any users that have been recently deleted, add any that have been recently created, and update details such as organization, email and so on if these details have recently changed.
- **Edit**—Allows you to modify the end-user details.
- **Delete**—Allows you to delete the end-user.
- **Certificates**—Allows you to view and manage the end-user's certificates.

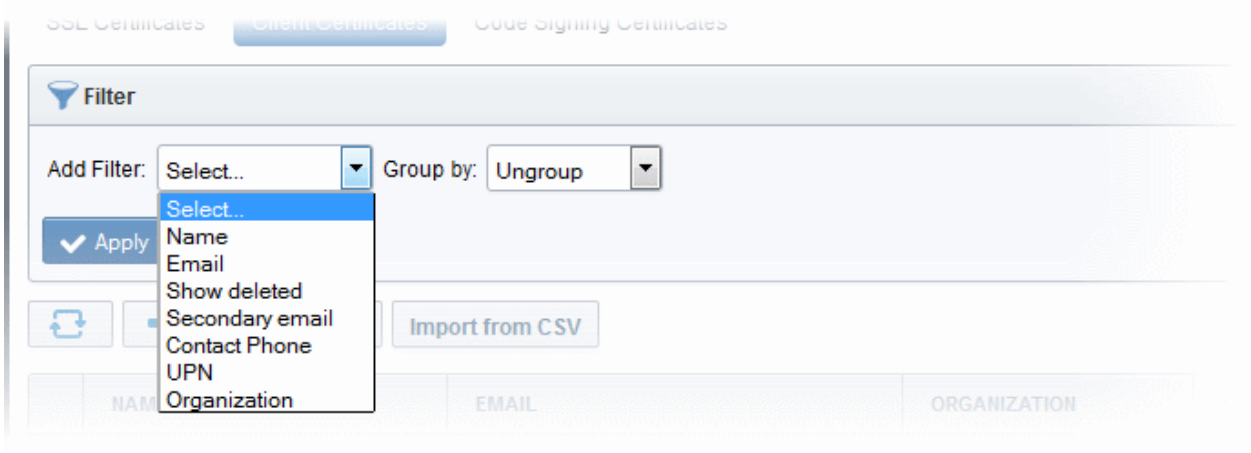
3.3.1 How to Sort and Filter Client Certificates

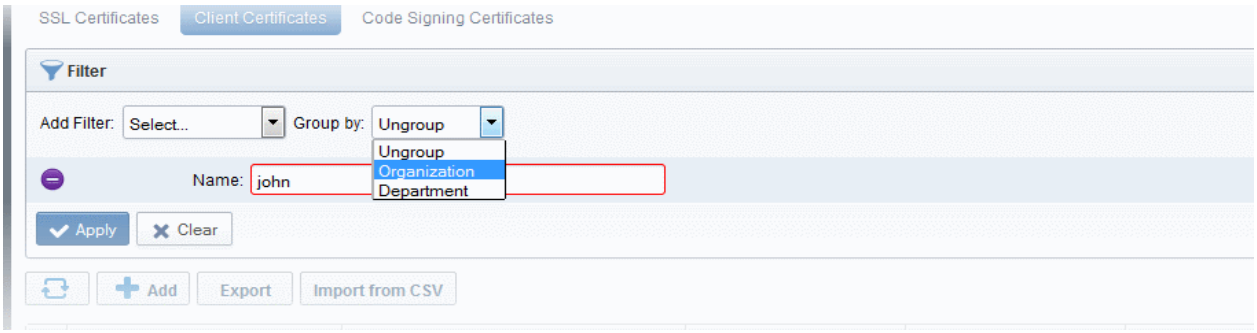
You can sort items in order of the entries in the column by clicking a column header, and you can use filters to search for particular client certificates.

You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.

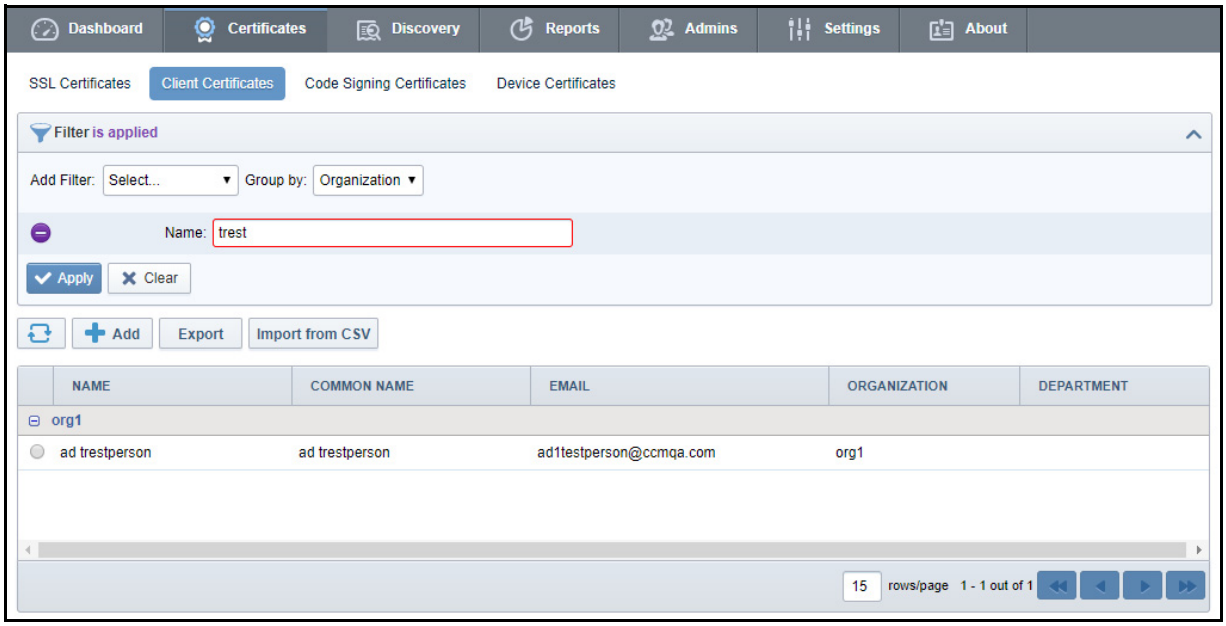


To add filters, you make a selection in the **Add Filter** list shown in the following illustrations, and then group the results with other options that appears depending on the selection from the **Add Filter** list. For example, you can filter certificates by Name and group by Organization. You can add more than one filter at a time.





Click **Apply** to trigger the display of the filtered items based on the entered parameters, as the following illustration shows. To remove the filter options, click **Clear**.

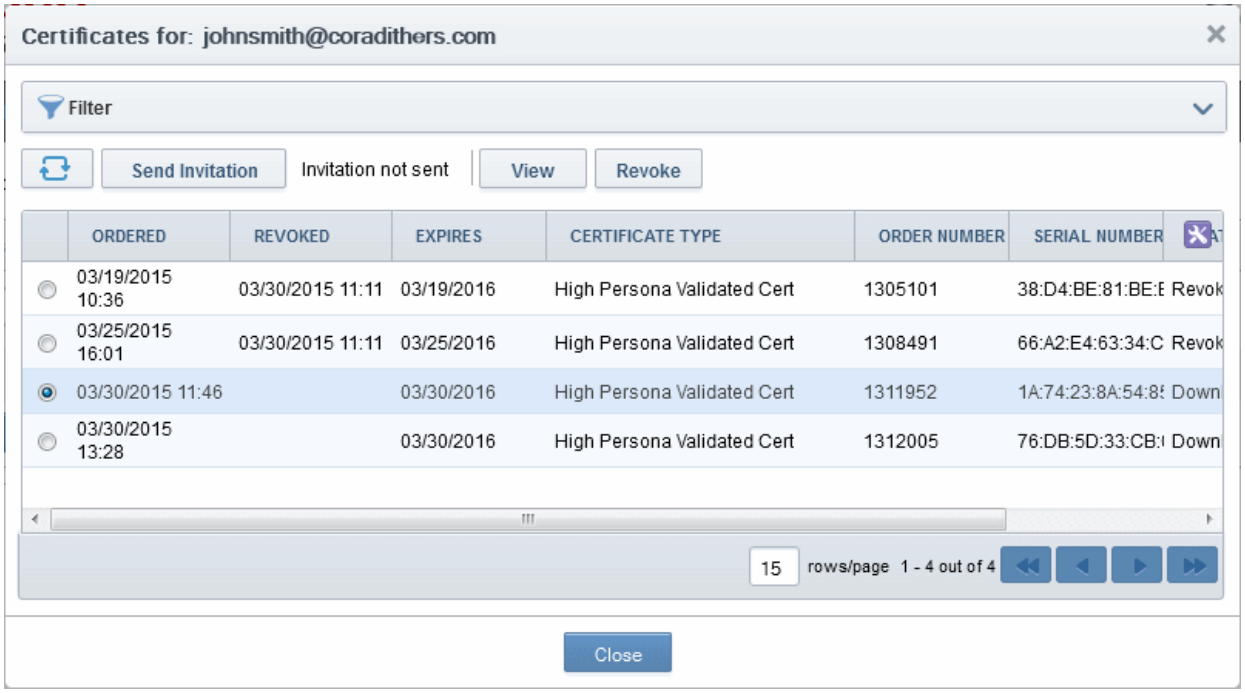


Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **Client Certificates** screen, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

3.3.2 How to Specify the Client Certificate Details

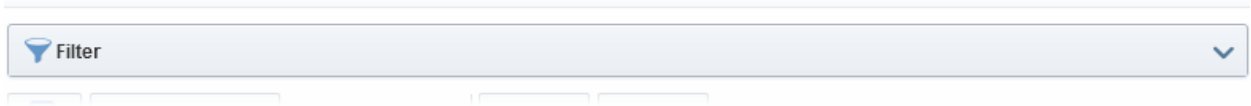
You can view all certificates that belong to a specific end-user as follows:

- In the main UI, select **Certificates** > **Client Certificates**, and select an end-user from the list.
- Click **Certificates** to open **Certificates for** screen shown in the following illustration. The certificates for the selected end-user are listed in chronological order, with the newest certificate listed fist. If a certificate has been revoked, the date of revocation is displayed in the **Revoked** column. You can use this screen to revoke, download, view, and send a certificate invitation.

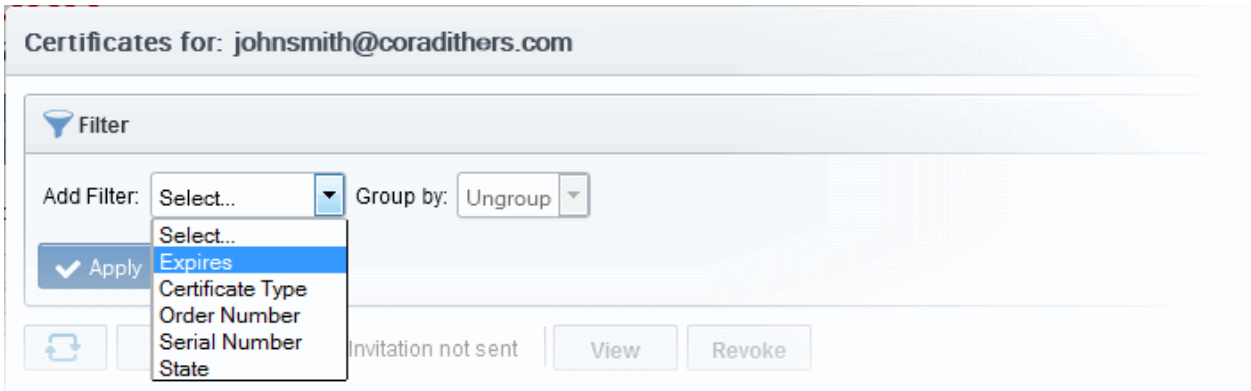


You can sort items in alphabetical order by clicking a column header, and you can use filters to search for particular certificates.

You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.



To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection from the **Add Filter** list.



The following are the available filter criteria and parameters:

- **Expires**—Allows you to filter certificates that are expiring in next 3, 7, 14, 30, 60 and 90 days.
- **Certificate Type**—Allows you to filter certificates based on their validation type.
- **Order Number**—Allows you to search for a certificate with a specific order number.
- **Serial Number**—Allows you to search for a certificate with a specific serial number.
- **Status**—Allows you to filter certificates based on their status.

Using the **Group by** list shown in the preceding illustration, you can select the criteria by which the results are to be grouped.

You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **Client Certificates** screen, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

You can perform the following actions on end-users and their client certificates:

- **View**—Allows you to view the end-user's certificates.
- **Revoke**—Allows you to revoke an end-user's certificate. Once revoked, the date and time of revocation is displayed in this column.
- **Download**—Allows you to download a copy of the end-user's certificate. When this is done, SCM creates a copy of each end-user's certificate which SCM saves on the server. This duplicate certificate is protected in two ways: (1) The key pair of each end-user's certificate is encrypted by a master public key. For more information, see "Configuring Key Escrow and Encryption" on page 473; (2) Password protected with the password defined by you. In this case, the end-user is asked for this password every time they attempt to download a certificate.
- **Send Invitation**—Allows you to send an email to the end-user with instructions on how to apply for and collect their client certificate. For more information, see "How to Request and Issue Client Certificates to Employees and End-Users" on page 141.
- **Refresh**—Reloads the list.

SCM stores individual private keys of end-user's client certificates so that they can be retrieved at a later date by you or the end-user. All end-users' key pairs are stored in encrypted form, therefore preventing security breaches.Each end-user's key pair is encrypted using a master public key that is stored by SCM. In order to decrypt this end- user's key pair, you must paste the corresponding master private key into the provided space. You can set a password to protect access to private key in a `.p12` file as well. Although you can bypass the PIN, you should be aware that not all programs would subsequently allow the certificate to be imported. The following is a non-exhaustive and not up-to-date list of OS-browser combinations that permit to import a `.p12` file with an empty password field.

Browser	Windows 8	Windows 7	Vista	XP	Mac OS
IE6	N/A	N/A	N/A	Possible	N/A
IE7	N/A	N/A	Possible	Possible	N/A
IE 8 and later	Possible	Possible	Possible	Possible	N/A

Browser	Windows 8	Windows 7	Vista	XP	Mac OS
Firefox 2	Possible	Possible	Possible	Possible	Possible
Firefox 3 and later	Not Possible	Not Possible	Not Possible	Not Possible	Not Possible
Opera 9	Possible	Possible	Possible	Possible	Possible
Opera 10	Possible	Possible	Possible	Possible	Possible
Chrome	Possible	Possible	Possible	Possible	Possible
Safari	Possible	Possible	Possible	Possible	Possible

If you download an end-user's certificate via this method, this certificate will be revoked.

3.3.3 How to Add End-Users for Client Certificates

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

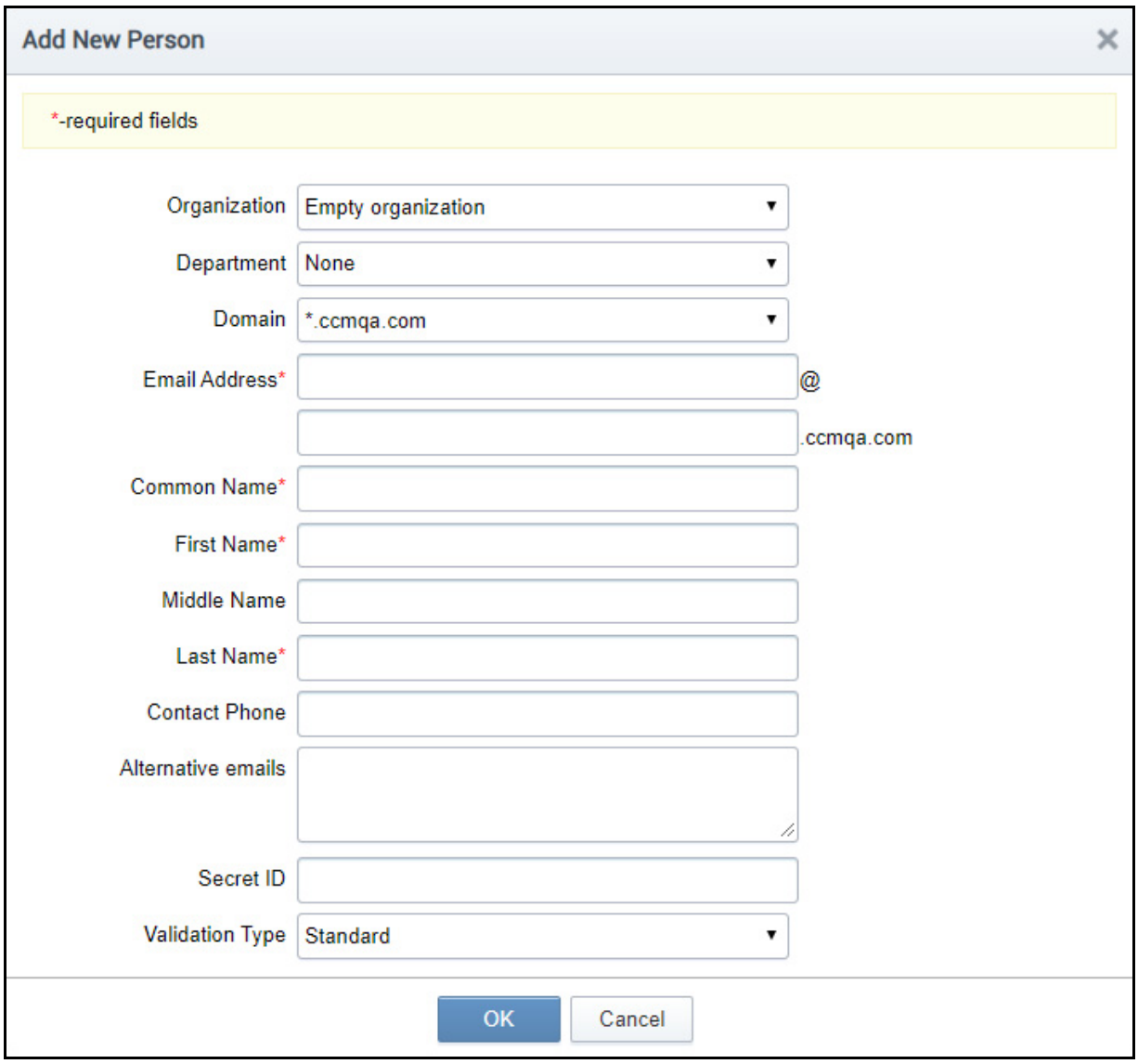
- Manually (see "Adding End-Users Manually" on page 134).
- By loading multiple end-users from a `.csv` file (see "Loading Multiple End-Users from a CSV File" on page 137).
- By enabling an automatic creation of end-users via the certificate self-enrollment form (see "Enabling Automatic Creation of End-Users via a Self-Enrollment Form" on page 139).

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

3.3.3.1 Adding End-Users Manually

You can add end-users manually as follows:

- In the main UI, select **Certificates** > **Client Certificates**, and then click **Add** to open the **Add New Person** dialog shown in the following illustration.



- Complete the fields based on the information provided in the following table, and then click **OK**.

Field	Description
Organization	The organization to which the new end-user belongs.
Department	The department to which the new end-user belongs.
Domain	The domain with which the user is associated.
Email Address	The user's email address.
Common Name	The common name to be included in the certificate. For client certificates, you typically specify the end-user's full name.

Field	Description
First Name	The end-user first name. The combined length of First Name and Last Name values cannot exceed 64 characters.
Middle Name	The end-user middle name.
Last Name	The end-user last name. The combined length of First Name and Last Name values cannot exceed 64 characters.
Contact Phone	The contact phone number for the end-user.
Alternative emails	The alternative email addresses for the end-user.
Secret ID	An identifier for the details of an existing end-user in SCM. Assigning SIDs to end-users simplifies the client certificate enrollment process for those end-users and reduces errors. This is because, as the details of the end-user are already stored, the end-user needs only specify the email address. To enable enrollment by SID, you must fill out this field.
Validation Type (visible if it is enabled by your Sectigo account manager)	The type of client certificate that is issued to an applicant. The valid values are Standard and High, and is based on the degree of user authentication that is carried out prior to issuance. Standard certificates can be issued quickly and take advantage of the user authentication mechanisms that are built into SCM. A user applying for a Standard certificate is authenticated using the following criteria: • The user must apply for a certificate from an email address at a domain that has been delegated to the issuing organization. • The organization has been validated as the owner of that - domain. • The user must know either a unique access code or secret ID that should be entered at the certificate enrollment form. You have to communicate these values to the end-user via out-of-band communication. The end-user must be able to receive an automated confirmation email sent to the email address of the certificate that they are applying for. The email contains a validation code that the end-user needs to enter at the certificate collection web page. High personal validation certificates require that the user undergo the preceding validation steps and face-to-face meeting with the issuing organization. The additional validation steps must be completed prior to you selecting a High personal validation type.

Field	Description
Principal Name	The email address that should appear as principal name in the certificate to be issued. For the organizations or departments enabled for principal name support, the client certificates issued to the end-users of the organization or department include an additional name: Principal Name, in addition to the `RFC822` name in the **Subject Alternative Name (SAN)** field. If included, the principal name becomes the primary email address of the end-user to whom the certificate is issued. This can be customized at a later time by editing the end-user if a **Principal Name Customization** is enabled for the organization or department. To check whether an organization or department is enabled for principal name support, follow this procedure: • Navigate to **Settings > Organizations**, click **Edit** in the row of an organization, and then select the **Client Certificate** area or • Navigate to **Settings > Organizations > Department** in the row of an organization, click **Edit** in the row of the respective department, and then select the **Client Certificate** area. This field is disabled for the organizations for which the principal name support is not enabled. If the principal name support is enabled for an organization and not enabled for a department, this field is auto-populated with the email address entered in the **Email Address** field.
Copy E-Mail	Auto-fills the **Principal Name** field with the email address entered in the **E-mail Address** field.

The end-user's details can be modified at any time by selecting the user, then clicking Edit at the top of the SCM UI. If any information in the **Add New Person** dialog is changed, with the exception of secret ID, any previously issued client certificates for this email address shall be automatically revoked. SCM maintains a user name history. If a user name is changed, you can still search for client certificates using both the old and new names.

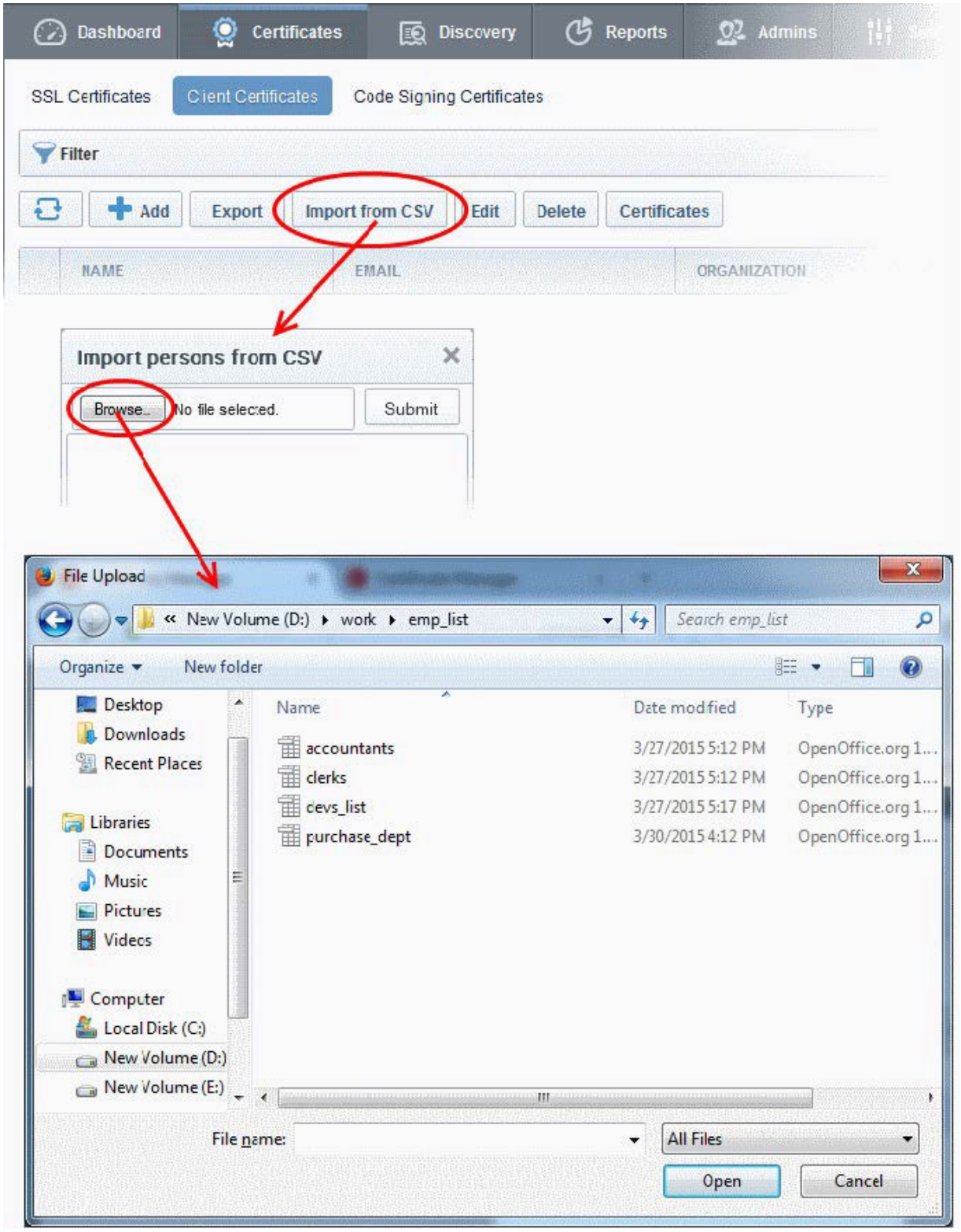
3.3.3.2 Loading Multiple End-Users from a CSV File

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

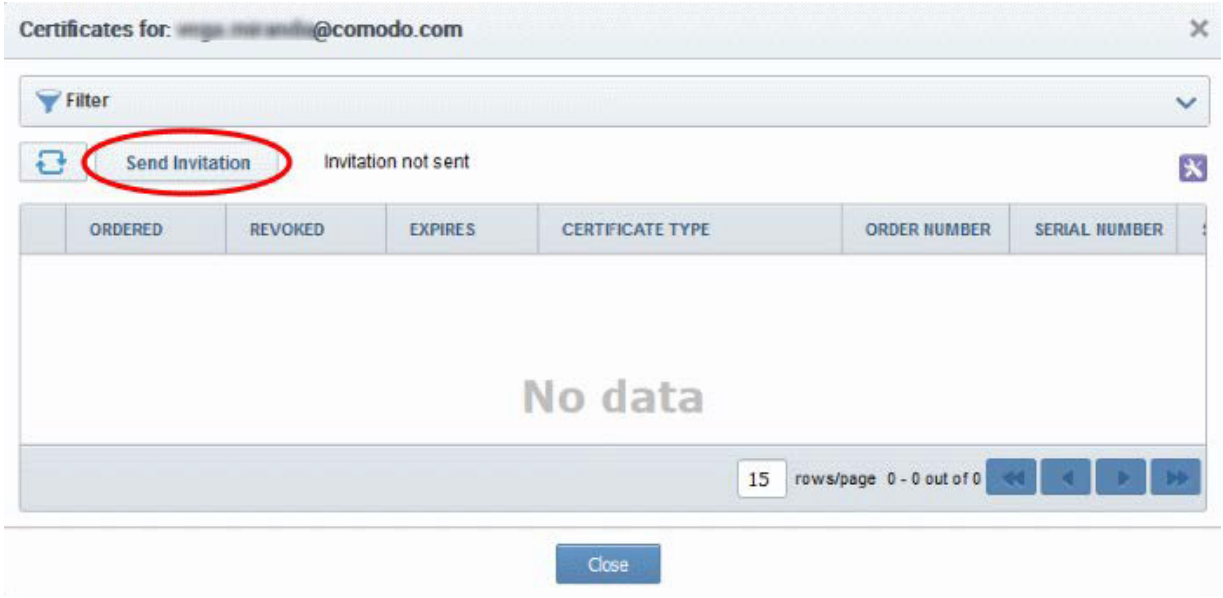
To load multiple end-users, follow this procedure:

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

  For information on how to structure `.csv` files for importing multiple end-users, see Appendix B CSV Import Format Requirements.
- In SCM, navigate to **Certificates > Client Certificates** and click **Import from CSV**, as shown in the following illustration.
- Browse to your `.csv` file and click **Submit** to trigger an SCM email notification containing a link to the self-enrollment form and the secret identifier to each end-user included in the `.csv` file.



- When the import completes, navigate to **Certificates > Client Certificates**, click the end-user record to open the **Certificate for end-user@exampledomain.com** dialog, and then click **Send Invitation**, as the following illustration shows.



A notification email containing a link to the **User Registration** form is sent to the applicant. The applicant can check for invitation from the email account the provided to add a user record.

Upon completion of the preceding steps, end-users can collect and install their certificates.

NOTE: Only the end-users included in the lines without errors are loaded to SCM, whereas the end-users included in the lines with errors are loaded.

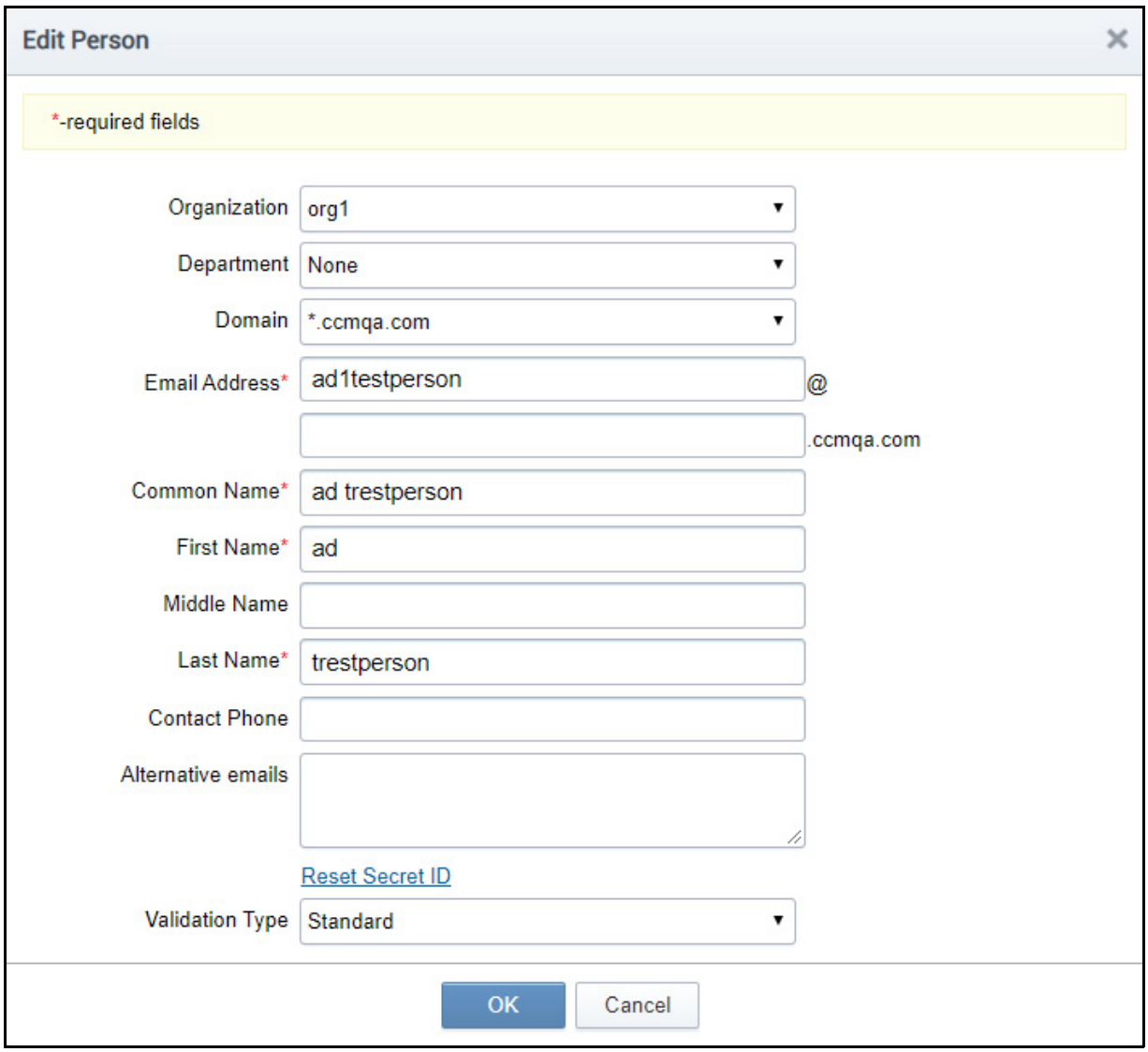
3.3.3.3 Enabling Automatic Creation of End-Users via a Self-Enrollment Form

End-users applying via the SSL or client certificate enrollment form are automatically added to the **Client Certificates** area of the SCM UI.

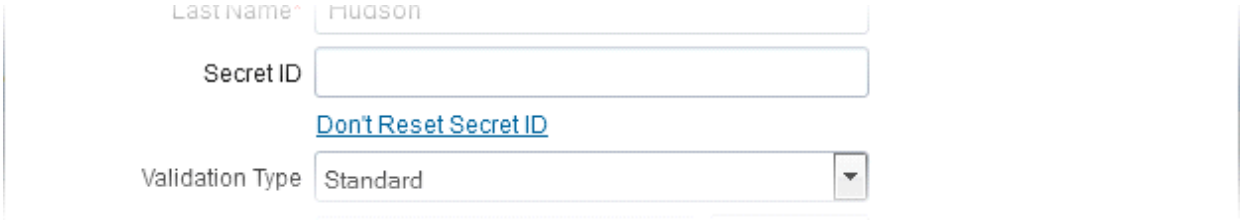
For more information, see "How to Request and Issue Client Certificates to Employees and End-Users" on page 141.

3.3.4 How to Modify End-Users

You can modify the end-user details at any time by selecting the end-user's name and clicking **Edit**, as shows in the following illustration.



If any information in this dialog is changed, with the exception of the secret ID, any previously issued client certificates for this email address are automatically revoked. The **Secret ID** field is not displayed for security reasons. If the secret ID needs to be modified, you can click **Reset Secret ID** to display the **Secret ID** field that allows you to specify a new secret ID, as shown in the following illustration. To retain the existing secret ID, click **Don't Reset Secret ID**.



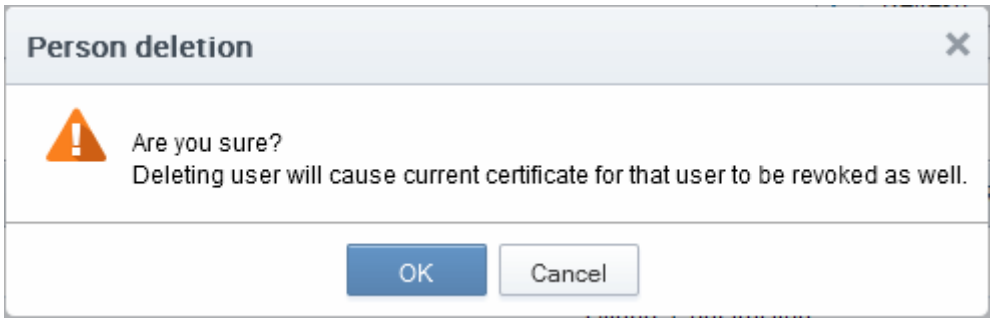
The **Validation Type** field is only visible if enabled by your Sectigo account manager. For more information, see "Adding End-Users Manually" on page 134.

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

To customize the principal name for the end-user, enter the new principal name as it should appear in the **Subject Alternative Name** (SAN) field of the certificate in the **Principal Name** field. If enabled for your account, you can revert the principal name changes to the email address of the end-user, click **Copy E-Mail**.

3.3.5 How to Delete End-Users

You can delete any end-user by selecting their name, clicking **Delete**, and then clicking **OK** on the **Person deletion** dialog, as shows in the following illustration.



Once the end-user is deleted, their certificate is revoked.

3.3.6 How to Request and Issue Client Certificates to Employees and 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:

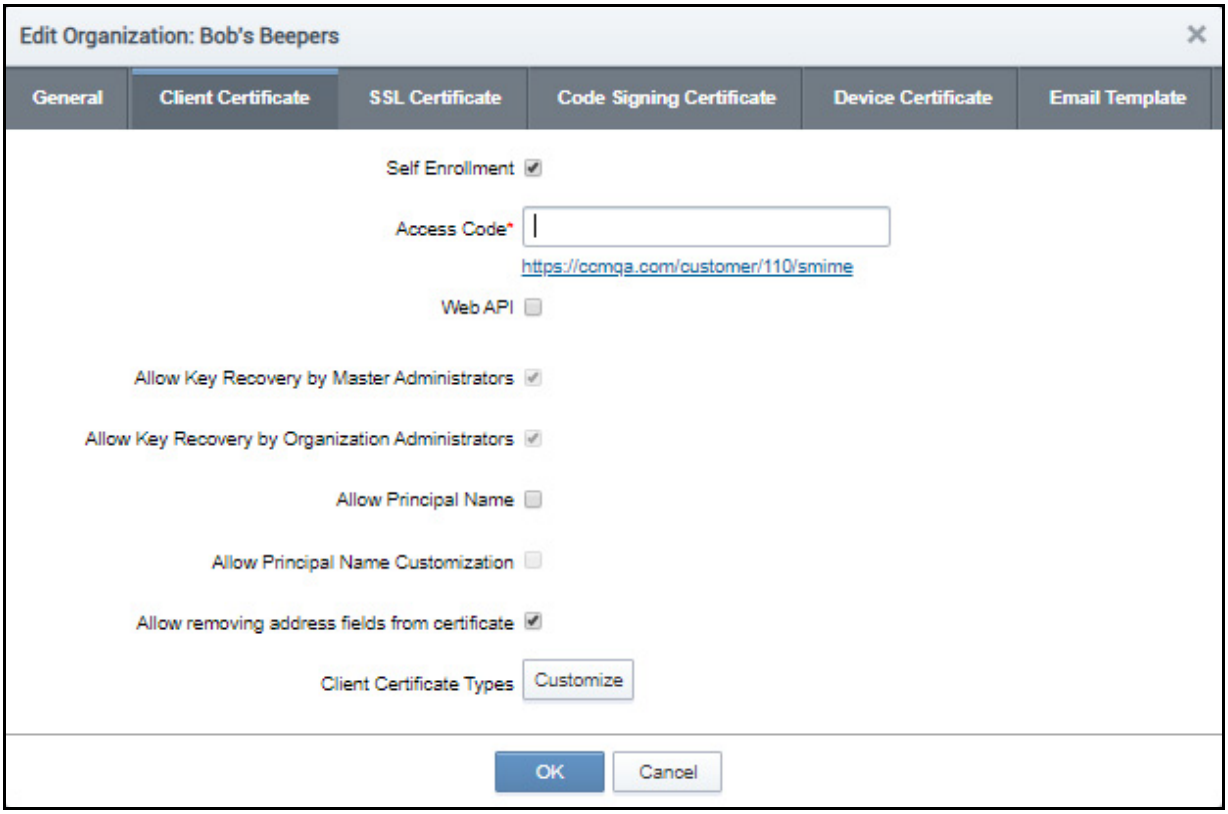
- Self-enrollment of end-users by access code—Involves directing end-users to apply for their own client certificate by accessing the self-enrollment form. You have to inform the end-user of the URL at which the self-enrollment form is hosted and the access code of the organization to which the end-user belongs. This should be done by out-of-band communication such as email. See "Enabling the End-User Self-Enrollment by Access Code" on page 141 for more information.
- Self-enrollment of end-users by secret identifier—Involves directing end-users to apply for their own client certificate by accessing the self-enrollment form. You have to inform the end-user of the URL at which the self-enrollment form is hosted and the secret ID of the organization to which the end-user belongs. This should be done by out-of-band communication such as email. See "Enabling the End-User Self-Enrollment by Secret Identifier" on page 149 for more information.
- Enrollment by administrator's invitation—Involves sending invitation notifications to end-users previously added to SCM. You can send the invitation from the SCM UI. 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 154 for more information.

3.3.6.1 Enabling the End-User Self-Enrollment by Access Code

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

The following requirements must be met for the self-enrollment to succeed:

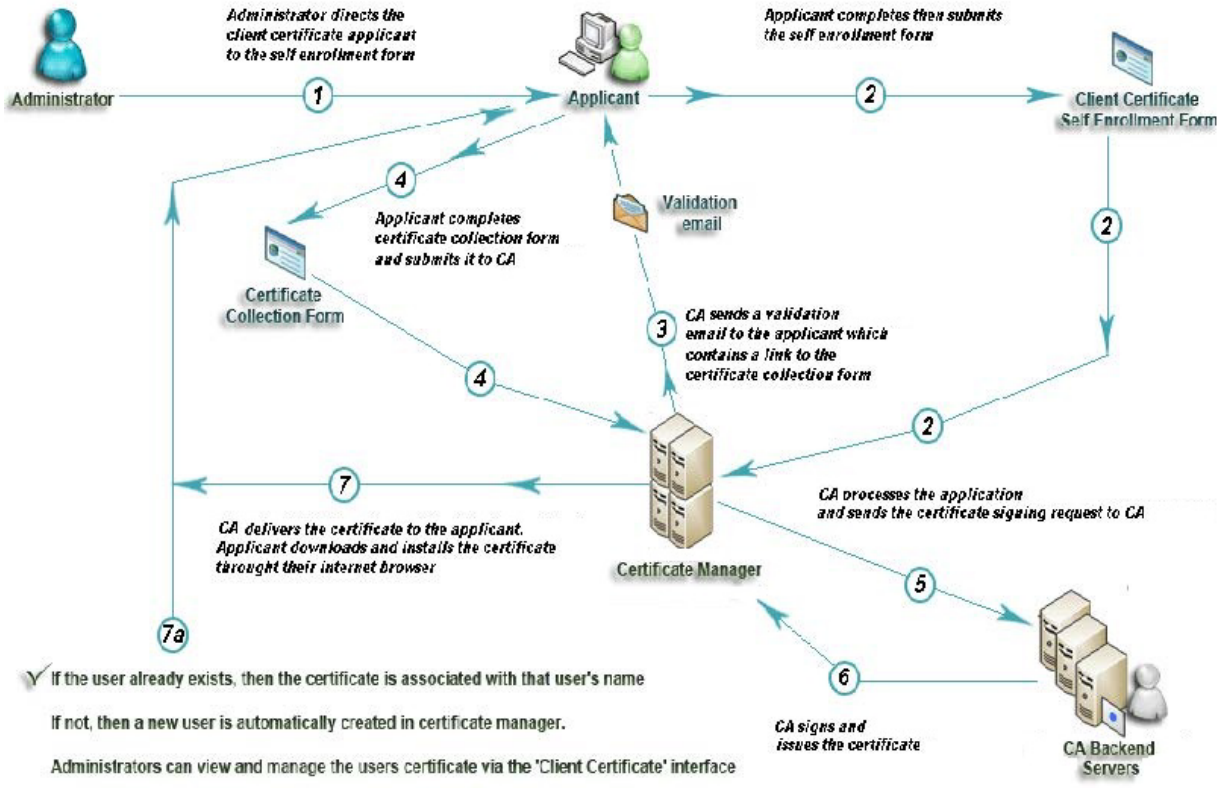
- The domain from which the client certificate is to be issued must have been enabled for client certificates, prevalidated by Sectigo, and activated by your Sectigo account manager (for example, if you wish to issue client certificates to end-user@mycompany.com, then mycompany.com must have been prevalidated by Sectigo). If you request a certificate for a brand new domain, then this domain first 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 an organization or department. See "How to Create a New Organization" on page 331 and "How to Modify an Existing Organization" on page 360 for more information.
- A RAO Client Certificate or DRAO Client Certificate administrator has been delegated control of this organization or department
- You enabled **Self Enrollment** in the **Client Certificates** area of the **Create/Edit** organizations dialog, as the following illustration shows.
- You set a value in the **Access Code** field in the **Client Certificates** area of the **Create/Edit** organizations dialog, as the following illustration shows. This value must be a combination of alpha and numeric characters.



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

- You direct the personal certificate applicant to the access code-based self-enrollment form, ensuring that the application is done from the end-user's computer (see "Enabling the End-User Self-Enrollment by Access Code" on page 141).
- The applicant completes and then submits the self-enrollment form, specifying the correct access code for the organization's domain (see "Self-Enrollment Form" on page 70).

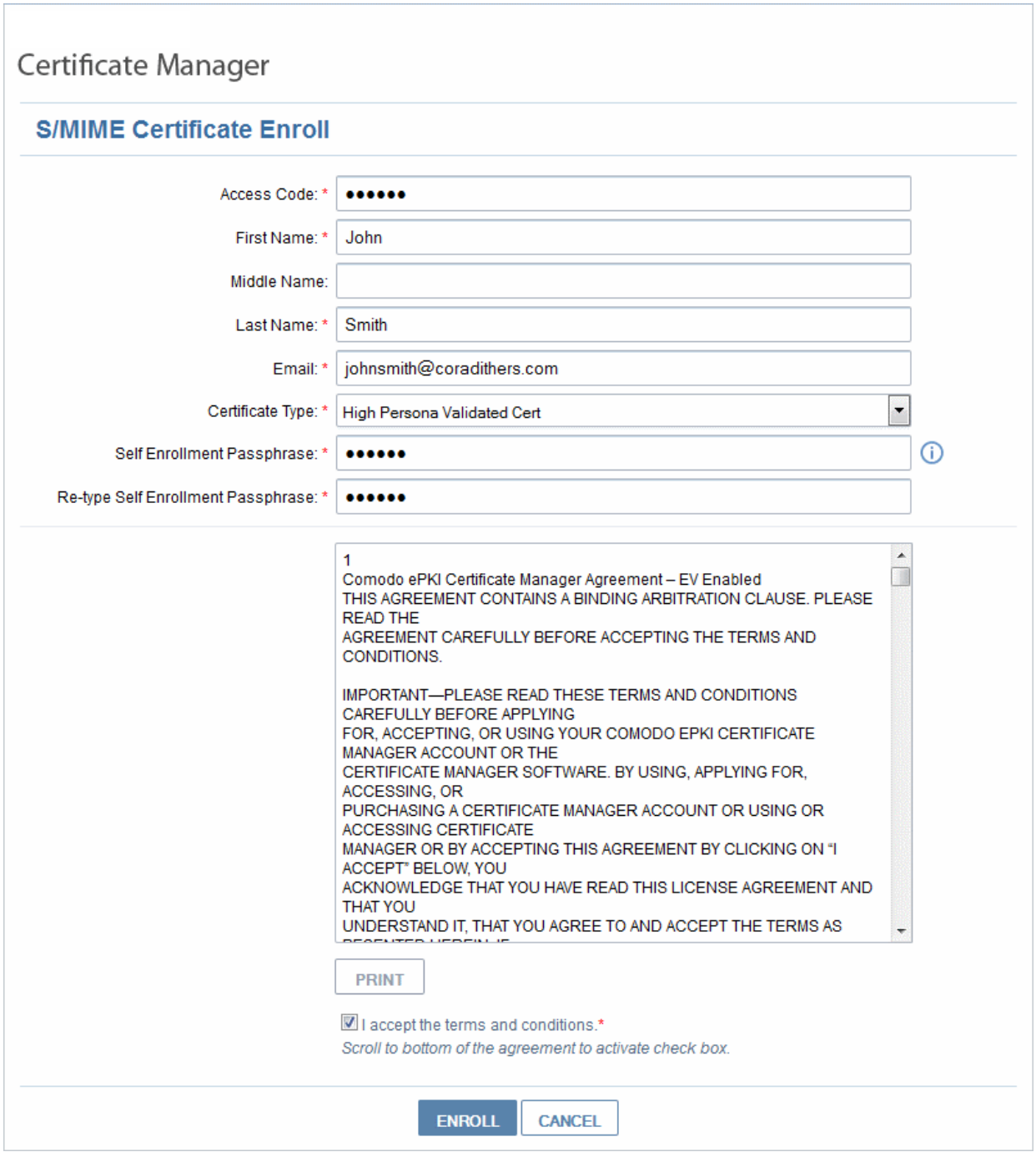
- SCM sends a validation notification to the applicant containing a link to the **Account Validation** form and a request code.
- The applicant completes the **Account Validation** form and the certificate request is sent to Sectigo servers. If the application is successful, the applicant can download and install their personal certificate (see "Certificate Collection" on page 119).
- 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** area), but not as an end-user of the client certificate, then SCM automatically adds this applicant as a new end-user to the **Client Certificates** UI.



After fulfilling all the preceding requirements, you have to communicate the enrollment details via an out-of-band communication method such as email to all end-users to whom you wish to issue client certificates. The communication must contain the following information:

- A link to the access code-based self-enrollment form shown in the following illustration and available at `https://cert-manager.com/customer/<customer_url>/smime?action=enroll&swt=ac`
- The client access code specified in the organization's **Client Certificates** area.

Note that the domain of the email address that the end-user specifies in the self-enrollment form must match a common name (domain) associated with the organization or department; the applicant must be able to receive emails at this address; the access code the end-user enters at the self-enrollment form must match the access code specified by you for that specific organization.

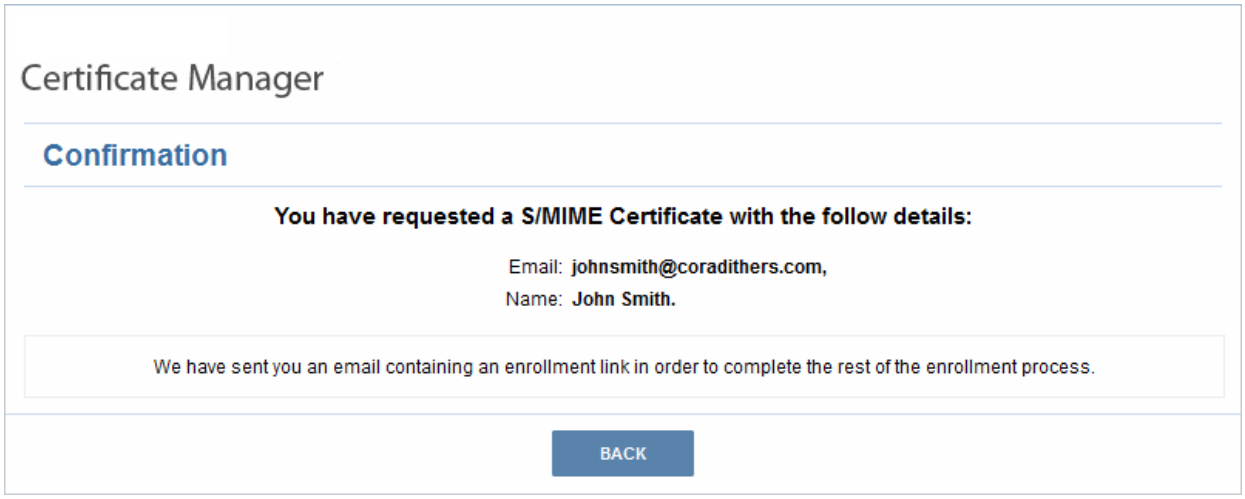

Certificate Manager
S/MIME Certificate Enroll
Access Code: *
First Name: *
John
Middle Name:
Last Name: *
Smith
Email: *
johnsmith@coradithers.com
Certificate Type: *
High Persona Validated Cert
Self Enrollment Passphrase: *
Re-type Self Enrollment Passphrase: *
1
Comodo ePKI Certificate Manager Agreement – EV Enabled
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE
AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.
IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING
FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE MANAGER ACCOUNT OR THE
CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR, ACCESSING, OR
PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR ACCESSING CERTIFICATE
MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU
ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND THAT YOU
UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS
PRINT
I accept the terms and conditions.*
Scroll to bottom of the agreement to activate check box.
ENROLL
CANCEL

The following table provides descriptions of the form fields and elements. The mandatory fields are marked with the red asterisk on the form.

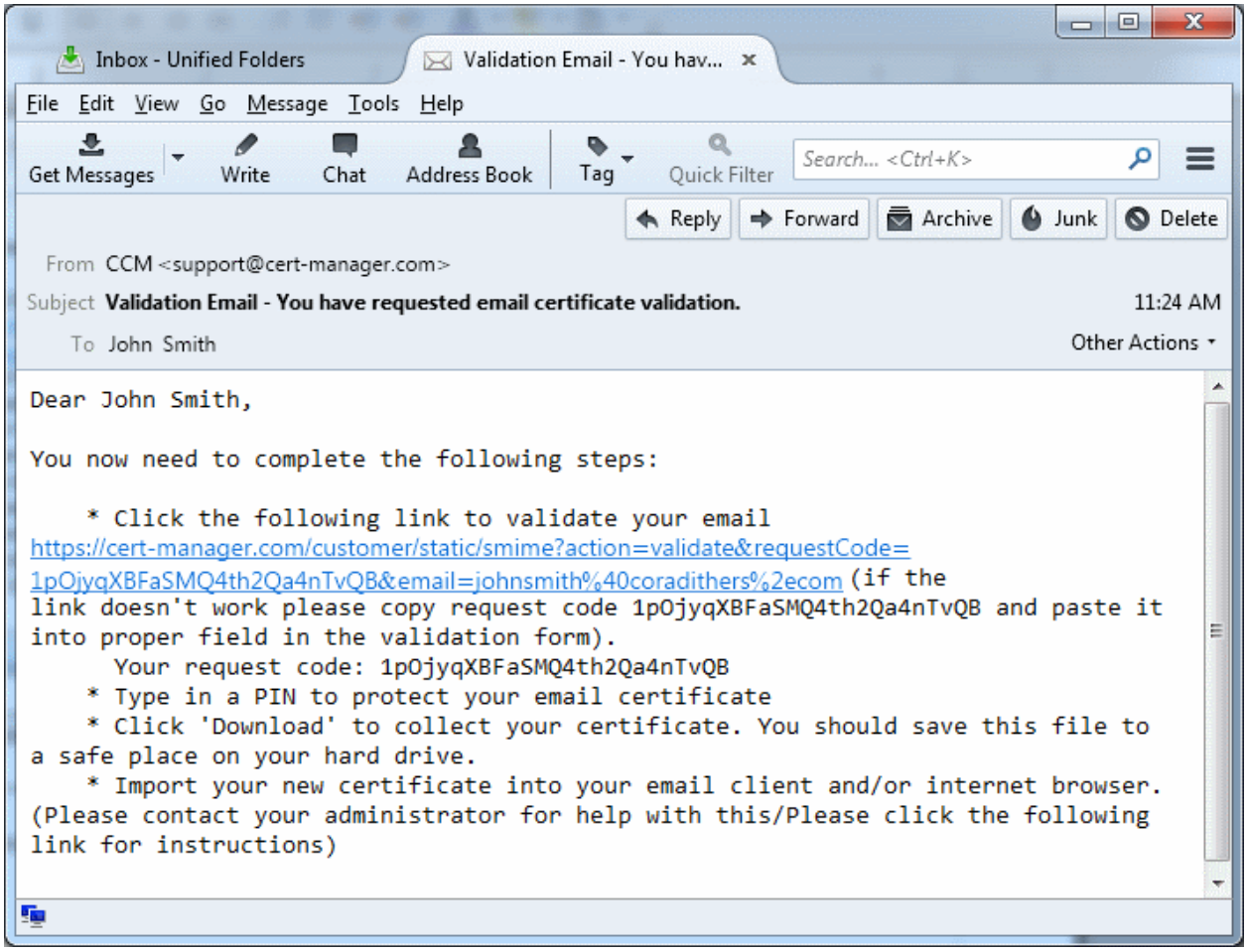
Field	Description
Access Code	The identifier for a particular organization or department and is used to authenticate certificate requests that are made using the self-enrollment form. Organization and departments are uniquely identified by combination of the organization's access code and the common name (domain) specified in **General** properties. Multiple organizations or departments can have the same access code or the same common name, but no single entity can share both. You should choose a complex access code containing a combination of alpha and numeric characters that cannot easily be guessed. This code should be conveyed to the applicant along with the URL of the sign-up form. Applicants that request a certificate using the self-enrollment form have to enter this code.
First Name	The applicant's first name.
Middle Name	The applicant's middle name.
Last Name	The applicant's last name.
Email	The applicant's email address for the domain belonging to the organization.
Passphrase	The passphrase required for renewal or revocation of the certificate.
Re-type Passphrase	The passphrase required for renewal or revocation of the certificate.
EULA acceptance	Acceptance of the terms and conditions before submitting the form.
Enroll	Submits the application and enrolls the applicant for the client certificate.
Cancel	Clears all data entered on the form.

In addition to the standard fields in the enrollment form, custom fields such as **Employee Code**, **Telephone** can be added by the MRAO administrator. See "How to Define Custom Fields" on page 501 for more information.

After completing the form and clicking **Enroll**, a confirmation dialog shown in the following illustration is displayed.

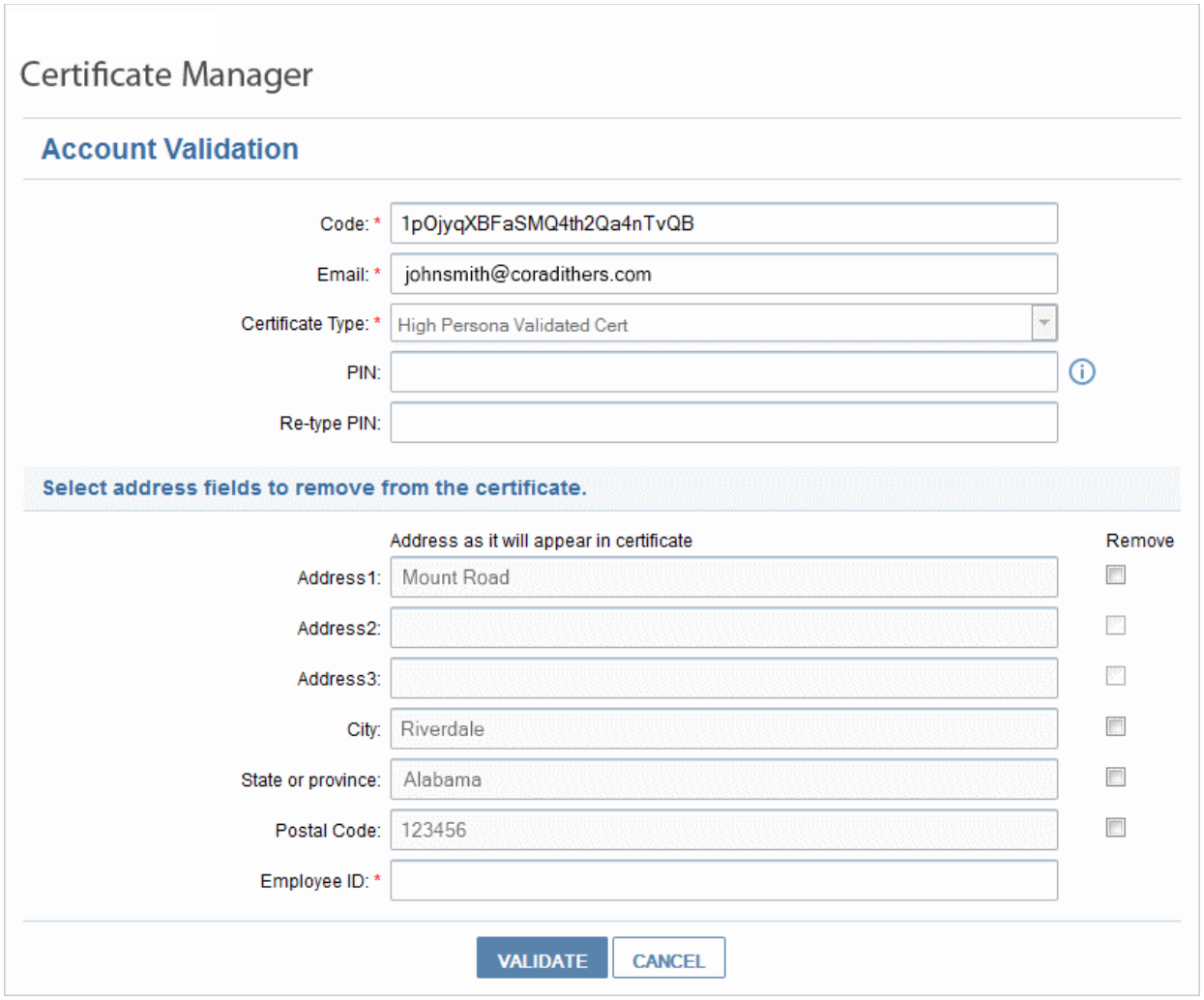


The applicant receives an email shown in the following illustration. This email contains a URL to validate the application, a request validation code, and instructions to download the certificate.



You can modify the contents of these emails by navigating to the **Settings > Templates > Email Template** area.

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 remaining fields have to completed based on the information provided in the following table. The mandatory fields are marked by the red asterisk.

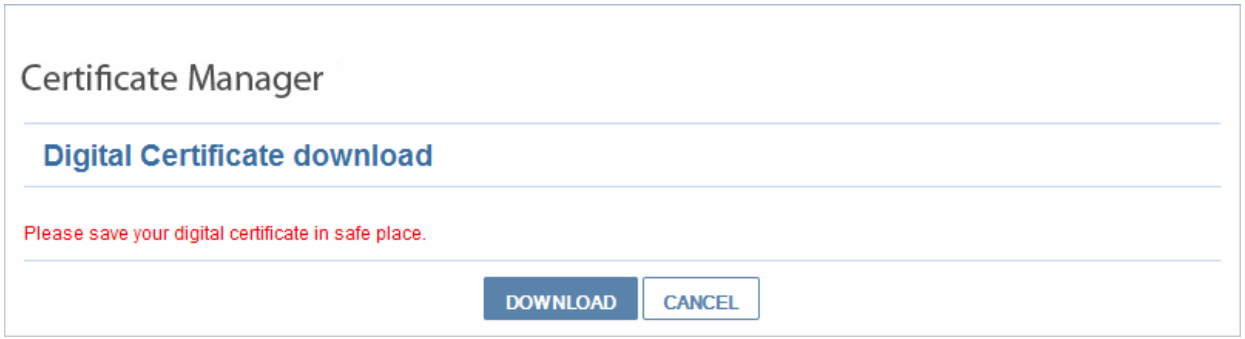


Field	Description
Code	The validation request code. This field is auto-populated when the applicant clicks the validation link in the email.
Email	The email address of the applicant. This field is auto-populated.
PIN	A PIN for the certificate to protect it.
Re-type PIN	Confirmation of the PIN.

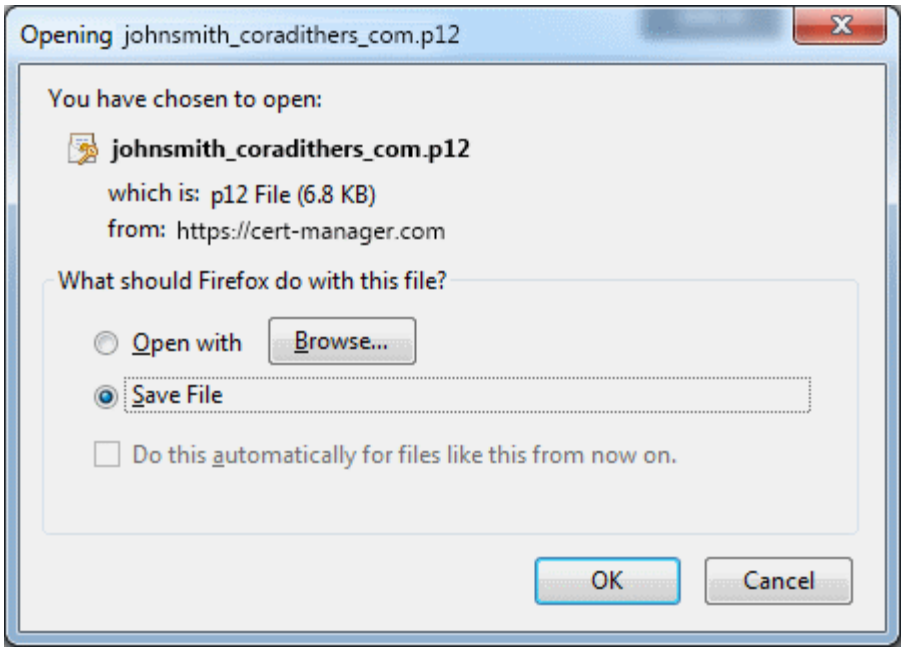
Field	Description
Address fields[a]	The address fields are automatically populated with the address details of the organization or department to which the user belongs. The applicant can choose to remove these details from the client certificate, in which case these details are not be included in the certificate that is issued. The **View Certificate Details** dialog displays Details Omitted next to these fields.

a. The option to hide address fields is only available if configured for your organization or department.

After completing the validation process, a certificate collection form appears, as shown in the following illustration. This form allows the end-user to download and save the certificate on their computer.



This form allows the end-user to download and save the certificate on their computer, as shown in the following illustration.



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

If an end-user does not exist in SCM (that is, not visible via **Certificates > Client Certificates**), 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** with the following parameters:

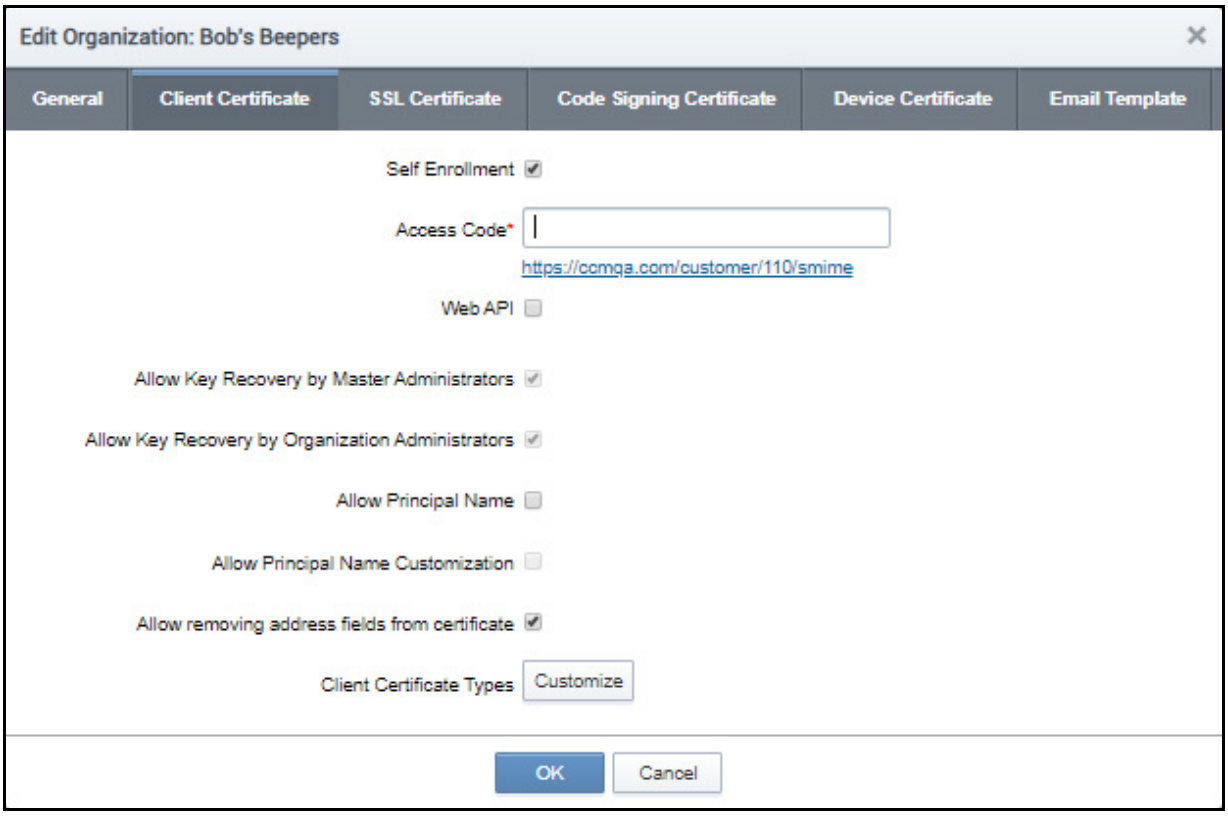
- **Name**—The name that the end-user specified at the client self-enrollment form.
- **Email**—The email address that the certificate was issued to, as specified at the client self-enrollment form.
- **Organization**—The name of the organization to which this end-user belongs.
- **Existing end-users**—If the end-user already exists, then the certificate is associated with their end-user name.

3.3.6.2 Enabling the End-User Self-Enrollment by Secret Identifier

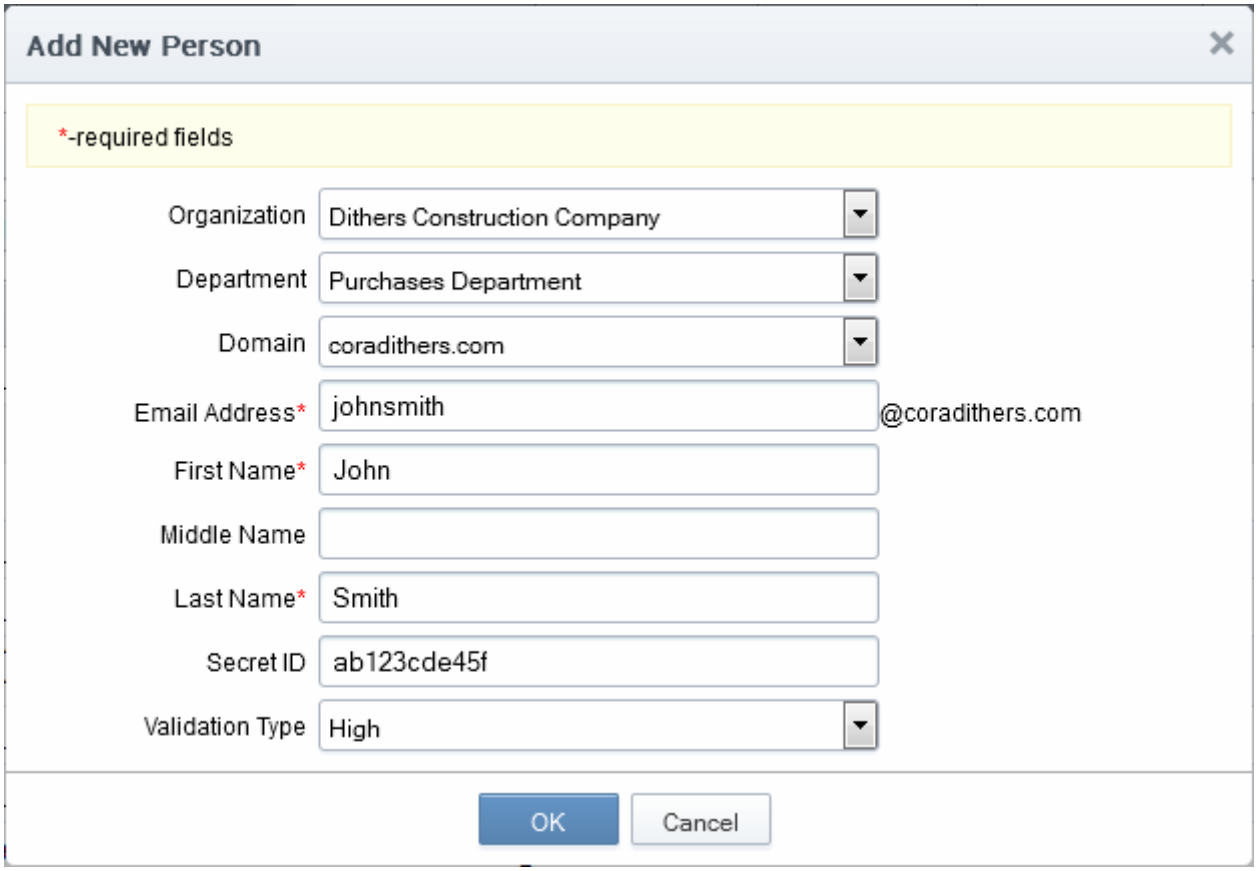
You can define a self-enrollment form which uses an organization's secret identifier for authentication. End-users can use the form to apply for certificates.

The following requirements must be met for the self-enrollment 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 wish 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 "How to Create a New Organization" on page 331 and "How to Modify an Existing Organization" on page 360 for more information.
- A RAO Client Certificate or DRAO Client Certificate administrator has been delegated control of this organization or department
- You enabled **Web API** field in the **Client Certificates** area of the **Create Organizations** or **Edit Organizations** dialog, as the following illustration shows



The administrator has specified a secret ID for the end-user through either the **Add User** or **Edit User** dialog, or when importing from a CSV file (see "Loading Multiple Certificates from a CSV File" on page 172). The secret code should be a combination of alpha and numeric characters.



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

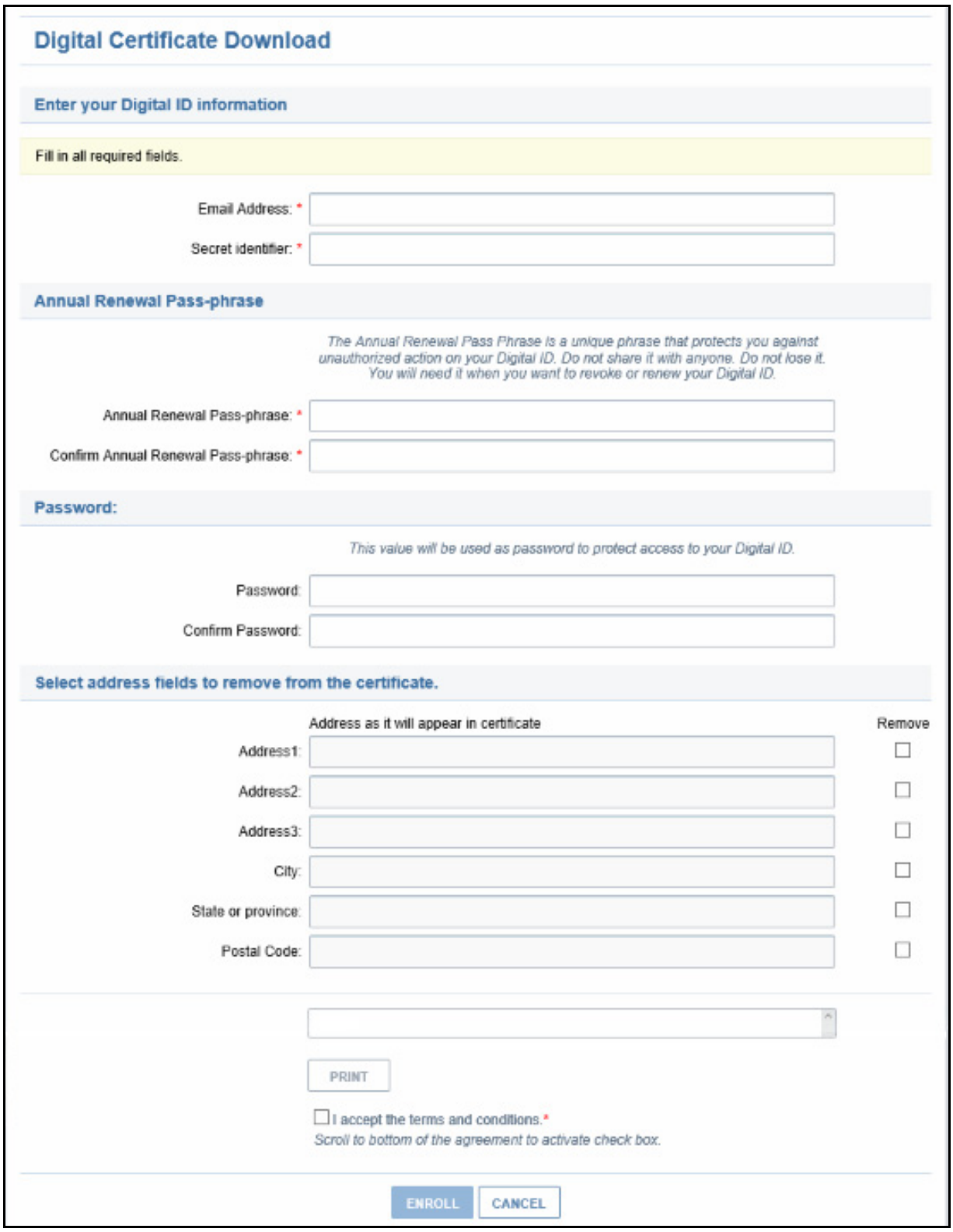
- You direct the personal certificate applicant to the access secret ID-based self-enrollment form, ensuring that the application is done from the end-user's computer.
- The applicant completes and then submits the self-enrollment form, specifying the correct secret ID assigned to them (see "Self-Enrollment Form" on page 70).
- The certificate request is sent to Sectigo servers. If the application is successful, the applicant can download and install their personal certificate.

After fulfilling all the preceding requirements, you have to communicate the enrollment details via an out-of-band communication method such as email to all end-users to whom you wish to issue client certificates. The communication must contain the following information:

- A link to the access secret ID-based self-enrollment form shown in the following illustration and available at `https://cert-manager.com/customer/<customer_url>/smime?action=enroll&swt=ac`
- The secret identifier specified for the end-user.

This allows the end-user to access and complete the form, and then submit it.

Note that the domain of the email address that the end-user specifies in the self-enrollment form must match a common name (domain) associated with the organization or department; the applicant must be able to receive emails at this address; the secret ID the end-user enters at the self-enrollment form must match the secret ID specified by you for that specific organization.

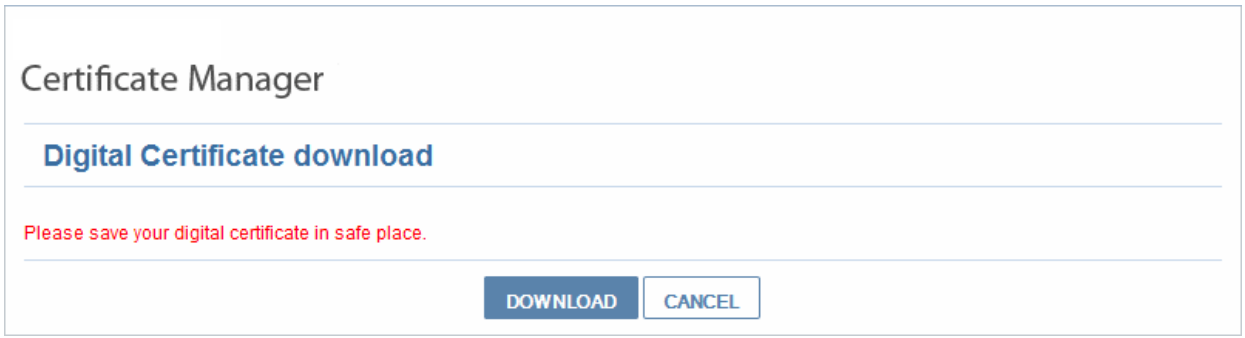

Digital Certificate Download
Enter your Digital ID information
Fill in all required fields.
Email Address: *
Secret identifier: *
Annual Renewal Pass-phrase
The Annual Renewal Pass Phrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. Do not lose it. You will need it when you want to revoke or renew your Digital ID.
Annual Renewal Pass-phrase: *
Confirm Annual Renewal Pass-phrase: *
Password:
This value will be used as password to protect access to your Digital ID.
Password:
Confirm Password:
Select address fields to remove from the certificate.
Address as it will appear in certificate
Remove
Address1:
Address2:
Address3:
City:
State or province:
Postal Code:
PRINT
I accept the terms and conditions.*
Scroll to bottom of the agreement to activate check box.
ENROLL
CANCEL

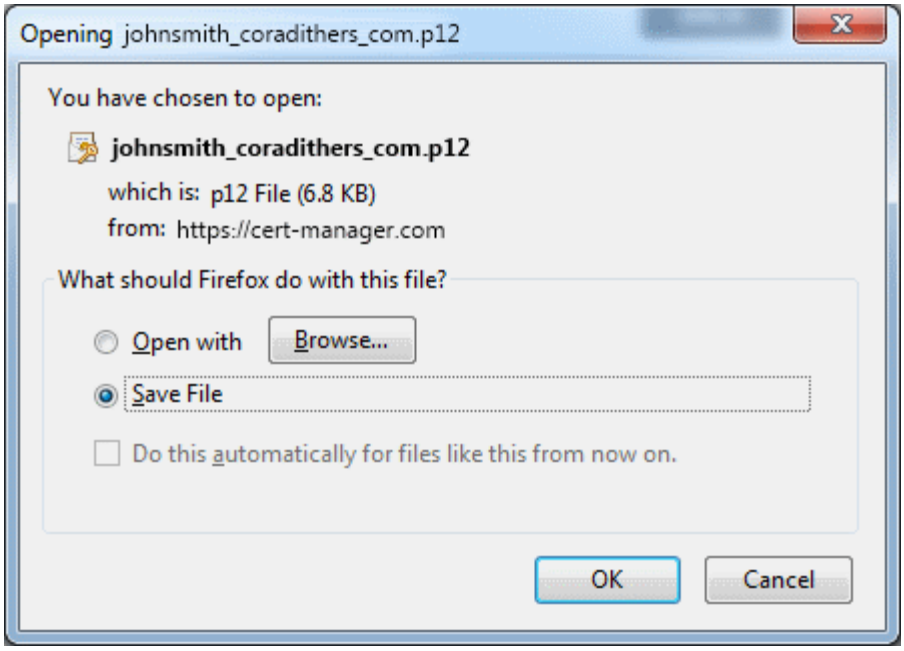
The following table provides descriptions of the form fields and elements. The mandatory fields are marked with the red asterisk on the form.

Field	Description
Email Address	The applicant's email address for the domain belonging to the organization.
Secret identifier	The secret ID specified for the applicant, as communicated to the applicant by the administrator.
Annual Renewal Pass- Phrase	Phrase required for renewal or revocation of the certificate.
Password	The password for 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 entered in the first field and reentered in the second field for confirmation. The password should be at least eight characters long.
Address fields[a]	The address fields are automatically populated with the address details of the organization or department to which the user belongs. The applicant can choose to remove these details from the client certificate, in which case these details are not be included in the certificate that is issued. The **View Certificate Details** dialog displays Details Omitted next to these fields.
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.
Cancel	Clears all data entered on the form.

a. The option to hide address fields is only available if configured for your organization or department.

After completing the validation process, a certificate collection form appears, as shown in the following illustration. This form allows 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 access to this file is protected by a PIN which the end-user is asked to enter when they import the certificate into the certificate store of their computer.

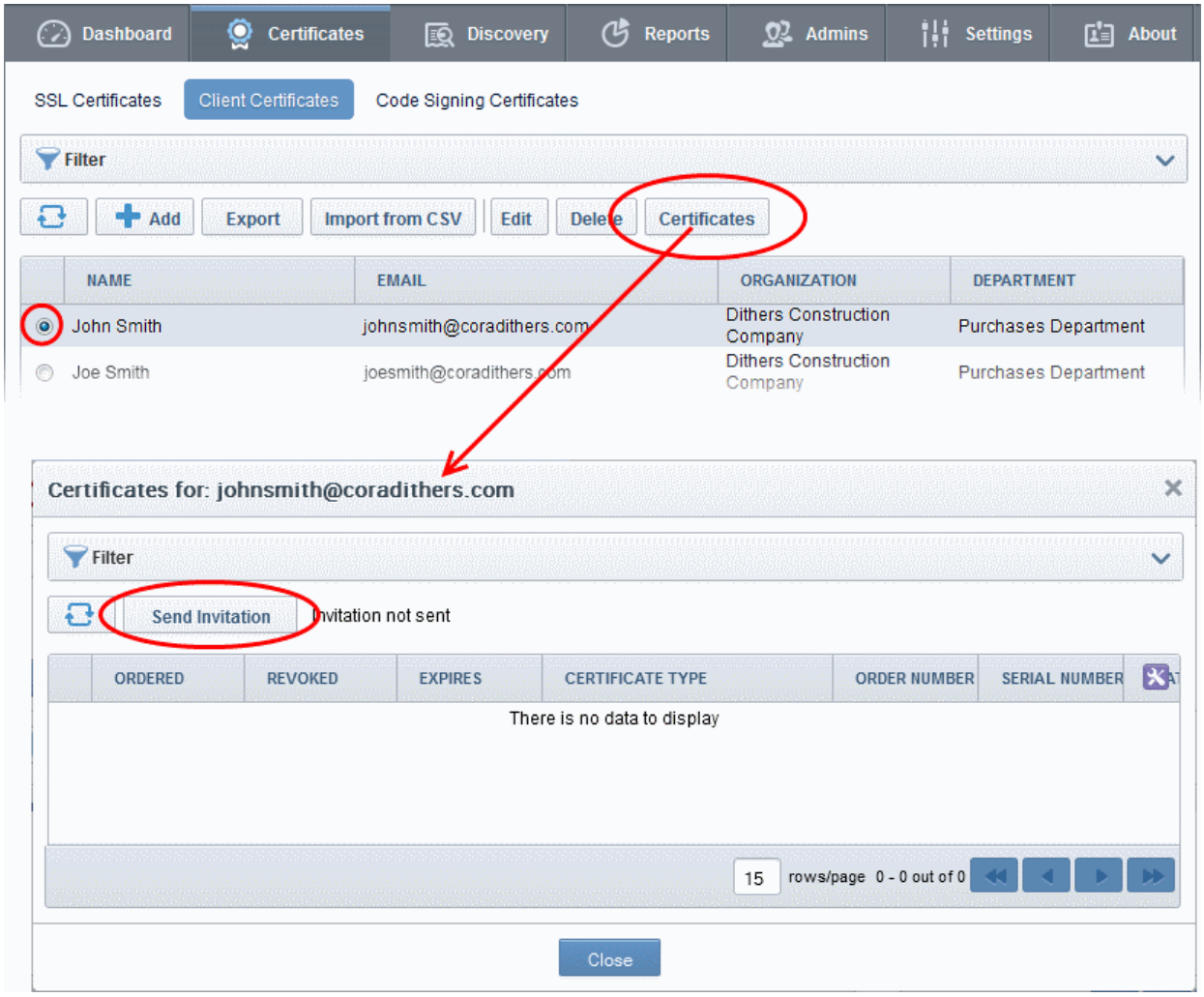
3.3.6.3 Enabling the End-User Enrollment by Invitation

You can invite the end-user to enroll from the SCM UI. For this process to succeed, the following requirements must be met:

- The domain to which the client certificate is to be issued has been enabled for client certificates.
- The domain to which the client certificate is to be issued has been validated by Sectigo.
- The domain to which the client certificate is to be issued has been activated by your Sectigo account manager. For example, if you wish to issue a client certificate to end-user@mycompany.com, then mycompany.com must have been validated by Sectigo.

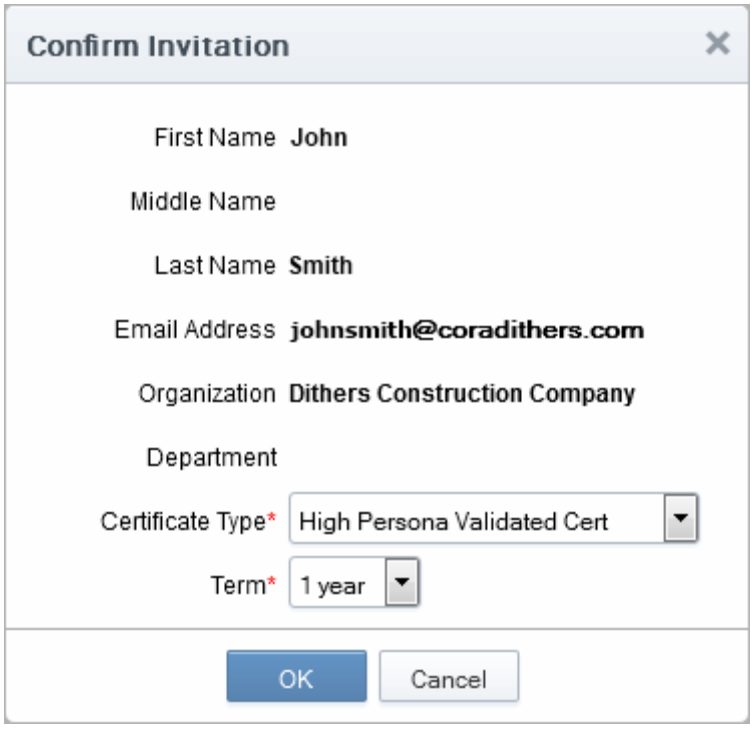
  If you request a certificate for a new domain, then this domain must undergo validation. Once validated, it is added to your list of prevalidated domains and future certificates will be issued immediately.
- The domain to which the client certificate is to be issued has been delegated to the organization or department. For more information, see "How to Create a New Organization" on page 331 and "How to Modify an Existing Organization" on page 360.
- 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** area of the SCM UI.

Client certificates can be provisioned to employees after the employee has been enrolled in SCM. You use the SCM UI to send an enrollment invitation containing a link to the registration form to the end-user by navigating to **Certificates > Client Certificates**, clicking the end-user record to open the **Certificate for end-user@exampledomain** dialog, and then clicking **Send Invitation**, as the following illustration shows.

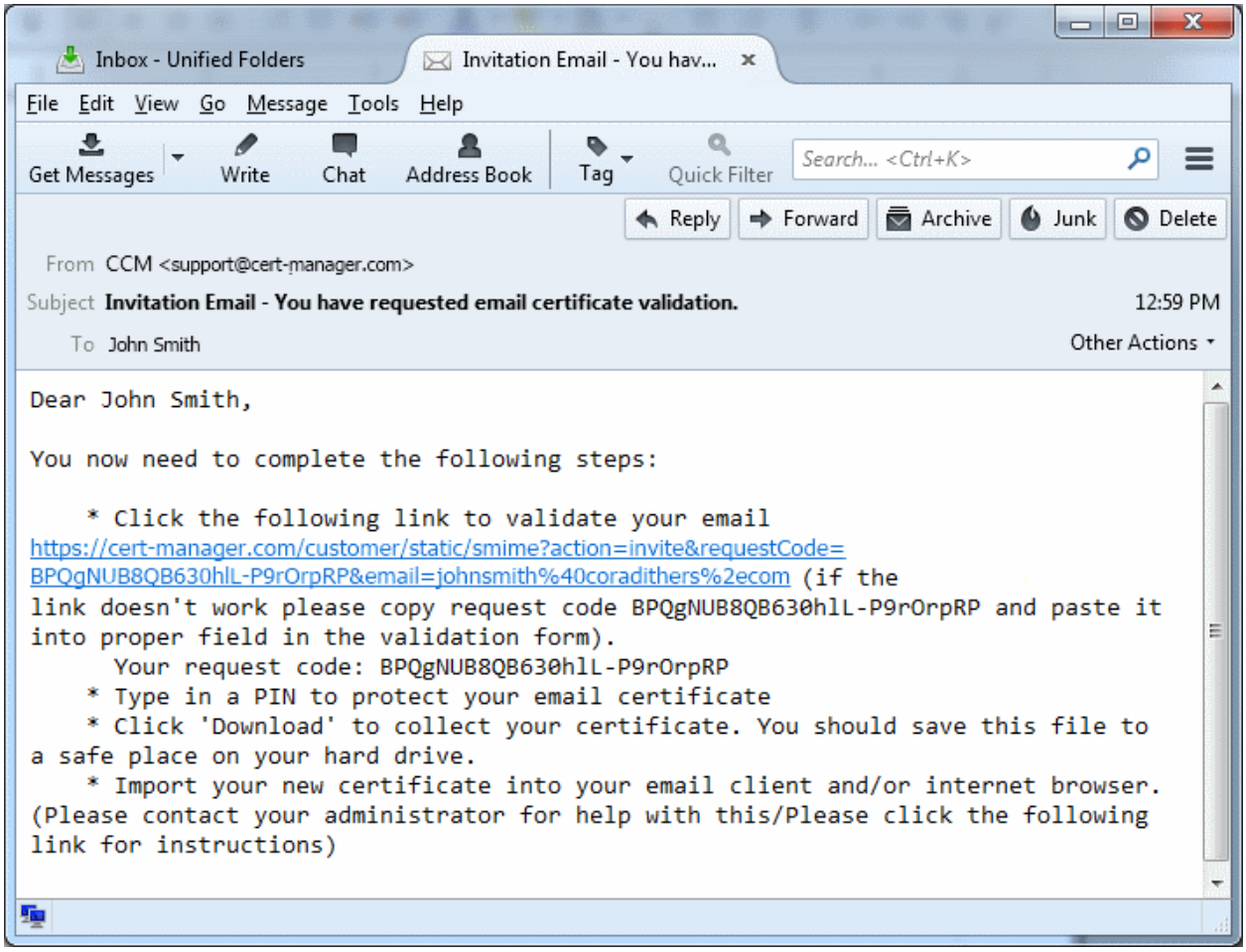


The **Confirm Invitation** dialog shown in the following illustration displays the details of the user and allows you to specify the client certificate type and validity period, as follows:

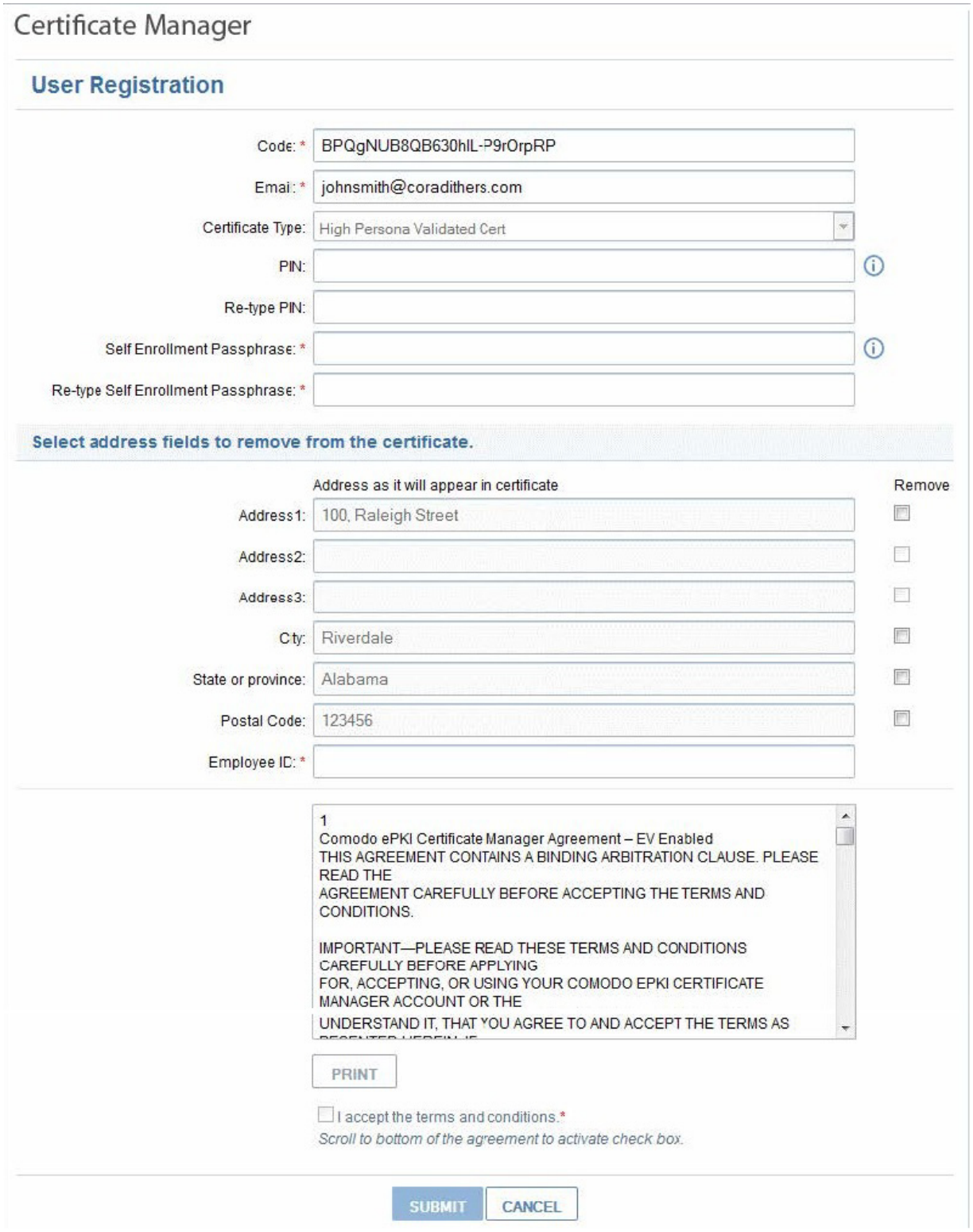
- **Certificate Type**—If the organization's account has been enabled for High Personal Validated Certificates and you have specified a validation type as high for this end-user, then the certificate type value would be available for selection in the **Certificate Type** list offering you a choice between sending an invitation for a High Personal Validated or Standard Personal Validated certificate. The default value is High Personal Validated.
- **Term**—Allows you to select the validity period for the certificate to be issued to the end-user. The range of values is limited to the validity periods allowed for your organization.



After you click **OK**, an invitation email shown in the following illustration is sent to the end-user, providing a link to the **User Registration** form and a request code that the end-user needs in order to validate that they are the correct applicant. Clicking the link in the email automatically populates the request **Code** and **Email** fields in the **User Registration** form.



You can modify the contents of these emails by navigating to the **Settings > Templates > Email Template** area.

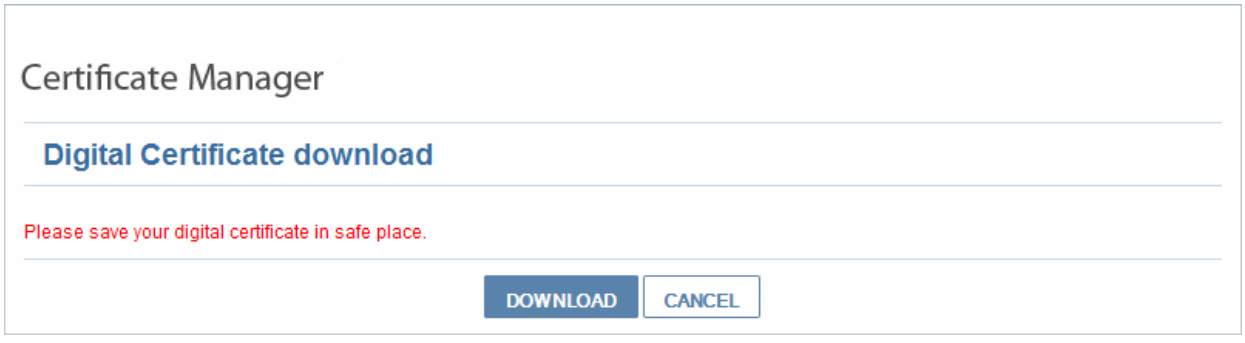

Certificate Manager
User Registration
Code: *
BPQgNUB8QB630hlL-P9rOrpRP
Email: *
johnsmith@coradithers.com
Certificate Type:
High Persona Validated Cert
PIN:
Re-type PIN:
Self Enrollment Passphrase: *
Re-type Self Enrollment Passphrase: *
Select address fields to remove from the certificate.
Address as it will appear in certificate
Remove
Address1:
100, Raleigh Street
Address2:
Address3:
City:
Riverdale
State or province:
Alabama
Postal Code:
123456
Employee ID: *
1
Comodo ePKI Certificate Manager Agreement – EV Enabled
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE
AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.
IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING
FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE MANAGER ACCOUNT OR THE
UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS
PRINT
I accept the terms and conditions.*
Scroll to bottom of the agreement to activate check box.
SUBMIT
CANCEL

The following table provides descriptions of the form fields and elements. The mandatory fields are marked with the red asterisk on the form.

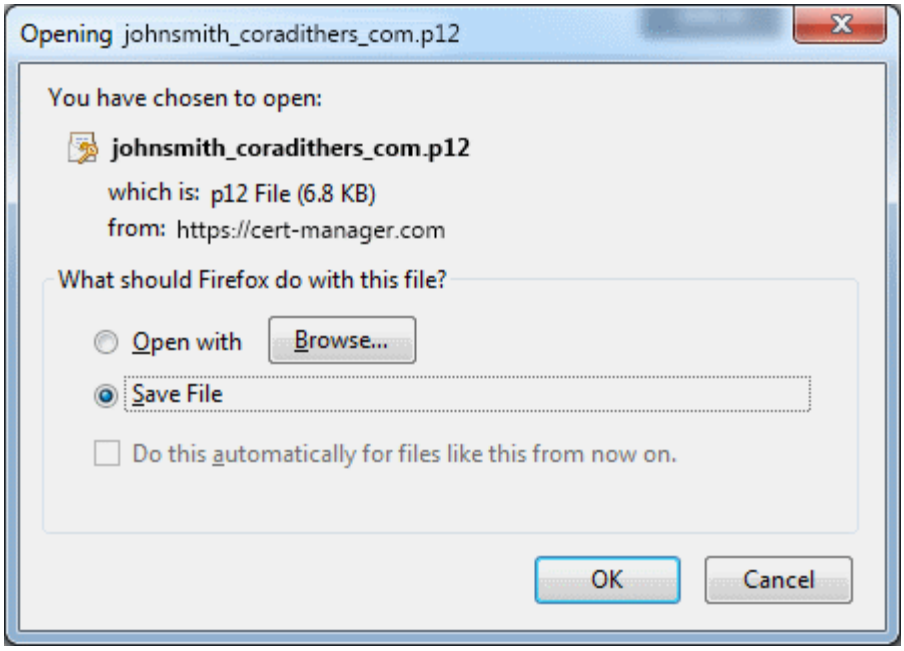
Field / Element	Description
Code	The validation request code. Auto-populated when the applicant clicks the validation link contained in the email.
Email	Email address of the applicant. This field is auto-populated.
PIN	A PIN to protect the certificate.
Re-type PIN	Confirmation of the PIN.
Self-Enrollment Passphrase	Phrase required for revocation of the certificate.
Address fields[a]	The address fields are automatically populated with the address details of the organization or department to which the user belongs. The applicant can choose to remove these details from the client certificate, in which case these details are not be included in the certificate that is issued. The **View Certificate Details** dialog displays Details Omitted next to these fields.
EULA Acceptance	Acceptance of the terms and conditions before submitting the form.
Submit	Submits the application.
Cancel	Clears all data entered on the form.

a. The option to hide address fields is only available if configured for your organization or department.

After completing the validation process, a certificate collection form appears, as shown in the following illustration. This form allows the end-user to download and save the certificate on their computer.



This form allows the end-user to download and save the certificate on their computer, as shown in the following illustration.



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

3.3.7 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.

You, as an administrator, revoke a client certificate from the main UI by navigating to **Certificates** > **Client Certificates**, selecting the end-user name, and then clicking **Certificates** to open **Certificates for** dialog, where the certificates for the selected end-user are listed in chronological order of issuance. To complete the revocation, you select the client certificate and click **Revoke**.

The end-user can directly revoke their client certificate via a certificate revocation form, as follows:

- The end-user asks you to grant them access to the interface, which you do by pointing them to `https://cert-manager.com/customer/<customer_uri>/smime?action=revoke`
- The end-user accesses the revocation interface and fills the revocation form with the email address and the passphrase that they set during the self-enrollment or user registration, and then they submit the form resulting in the revocation of the certificate.

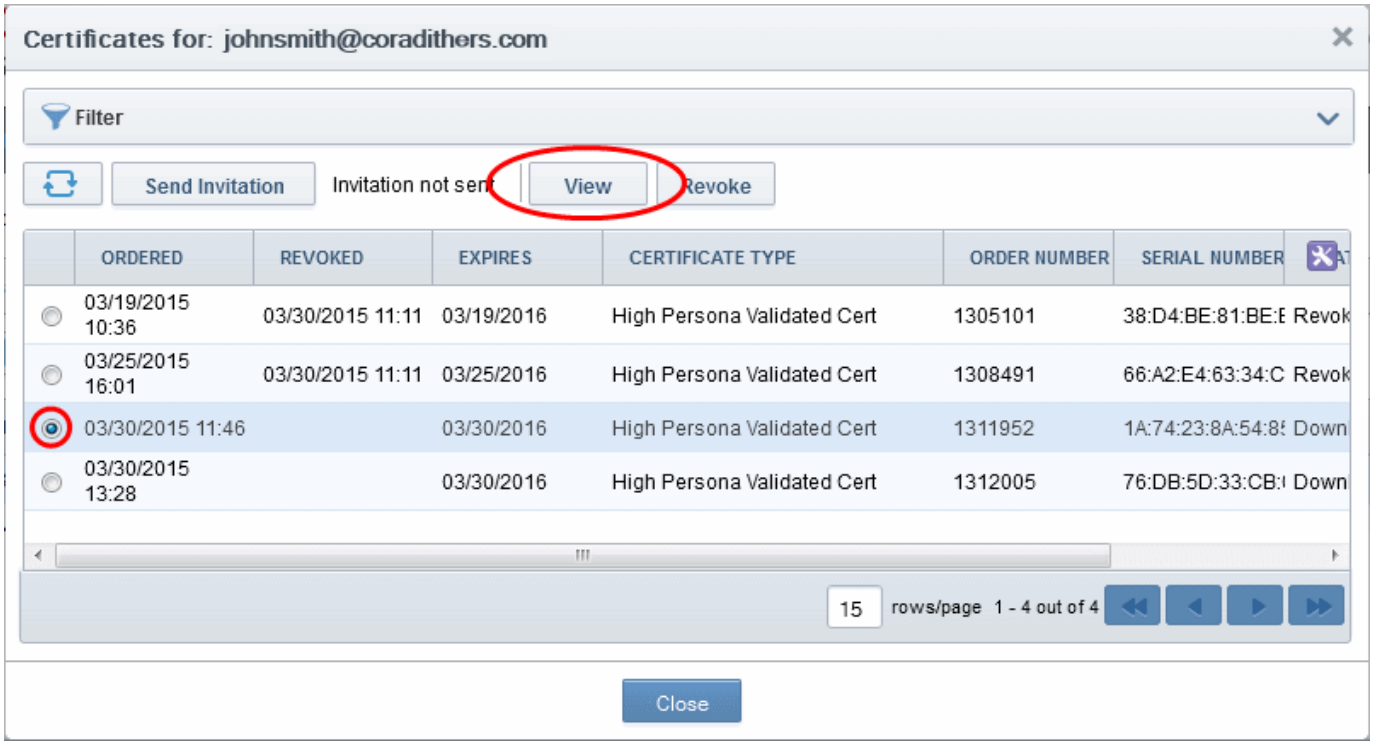
The following table lists fields and controls available in the certificate revocation form. The mandatory fields and marked with a red asterisk.

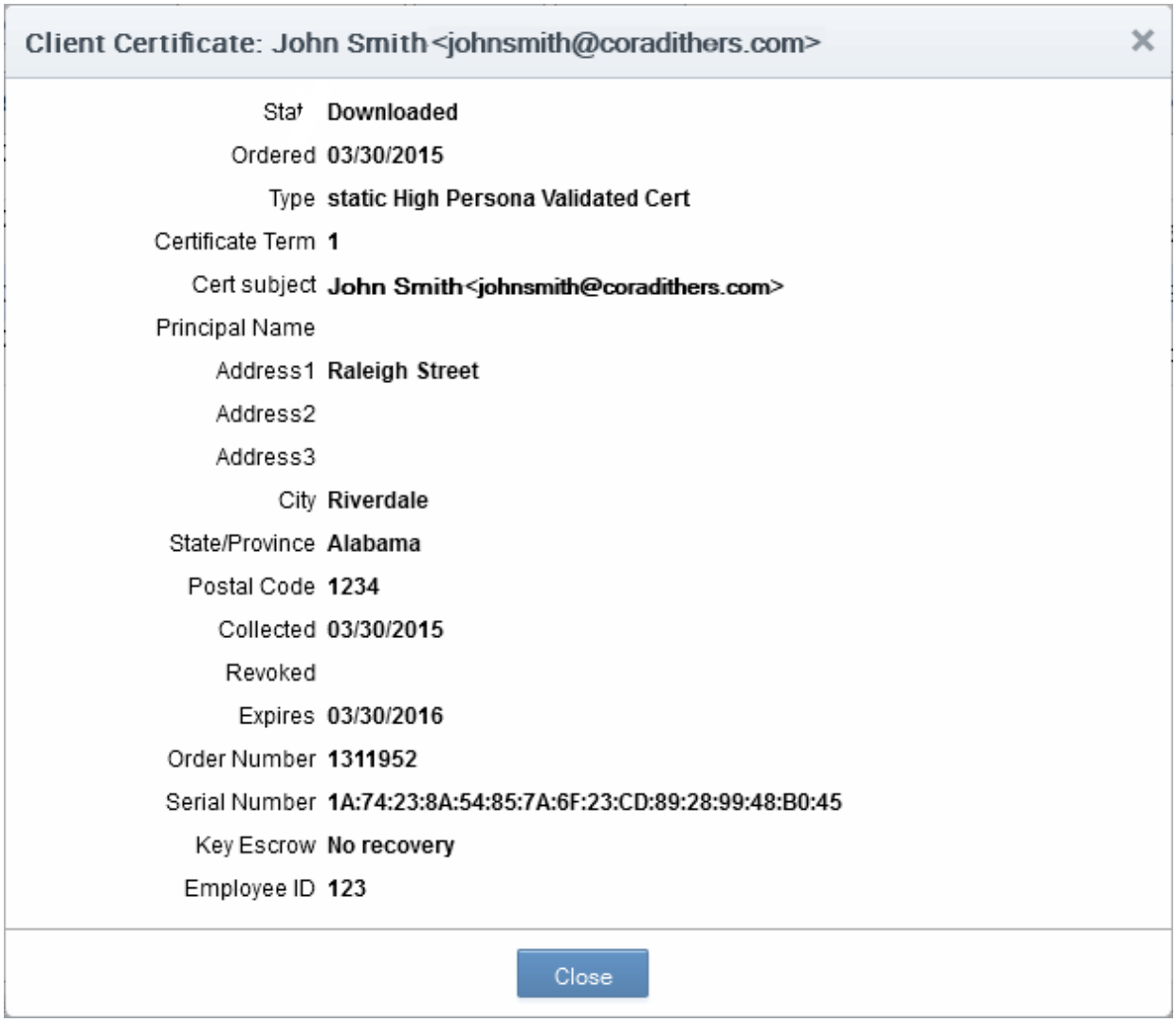
Field	Description
Email	The end-user's full email address.

Field	Description
Passphrase	The end-user's passphrase of the client certificate. This must match the passphrase entered during self-enrollment or user registration.
Revoke	Revokes the certificate
Cancel	Cancels the revocation process.

3.3.8 How to View the End-User Certificates

You can view the certificates applied for, downloaded by, or issued to end-users from the main UI by navigating to **Certificates** > **Client Certificates**, selecting the end-user whose certificate is to be viewed, clicking **Certificates** to open the **Certificates for** dialog, and then clicking **View**, as shown in the following illustration.




Client Certificate: John Smith <johnsmith@coradithers.com>
Stat Downloaded
Ordered 03/30/2015
Type static High Persona Validated Cert
Certificate Term 1
Cert subject John Smith<johnsmith@coradithers.com>
Principal Name
Address1 Raleigh Street
Address2
Address3
City Riverdale
State/Province Alabama
Postal Code 1234
Collected 03/30/2015
Revoked
Expires 03/30/2016
Order Number 1311952
Serial Number 1A:74:23:8A:54:85:7A:6F:23:CD:89:28:99:48:B0:45
Key Escrow No recovery
Employee ID 123
Close

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

Field	Value	Description
Status		The current status of the certificate.
	Invited	The end-user has been sent an invitation email by you.
	Requested	The request has been sent to the CA for approval.
	Applied	The end-user has validated the email and applied for the certificate.
	Issued	The certificate was issued by the CA and collected by the certificate manager. A blue font color indicates that the certificate was issued by the CA but has not been installed.
	Downloaded	The end-user has downloaded the certificate.
	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.
Type		The type of the client certificate, prefixed with the customer name.
Certificate Term		The validity period of the certificate.
Certificate subject		The name and email address of the end-user.
Principal Name		The principal name included in the certificate.
Address 1: Address 2: Address 3: City: State or Province: Postal Code:		The address of the organization, as provided while requesting the certificate. Only those address fields that were allowed to be displayed while applying for the certificate are shown in this field, and the rest of the fields are displayed as Details Omitted.
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.

Field	Value	Description
Serial Number		The serial number of the certificate.
Key Escrow		Indicates whether or not the key escrow is available for the certificate recovery by you.
Employee ID		The end-user identifier within their organization or department.

3.4 Managing the Code Signing Certificates

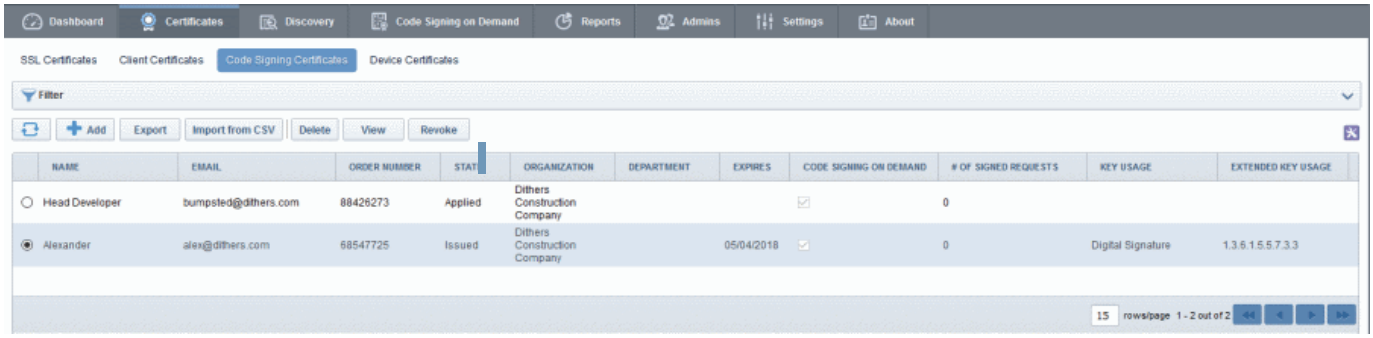
Depending on your security role, the **Code Signing Certificates** area shown in the following illustration provides MRAOs, nominated RAO Code Signing, and nominated DRAO Code Signing administrators with the information and controls necessary to issue and manage the lifecycle of the code signing certificates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

MRAOs can request and manage code signing certificates and end-users 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 and end-users for departments that have been delegated to them.

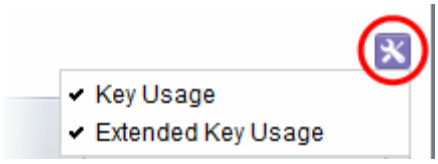
Organizations can further simplify the code signing process by using the SCM's code signing on-demand service, which is available in both hosted and cloud versions and can sign `.exe`, `.dll`, `.cab`, `.msi`, `.js`, `.vbs`, `.ps1`, `.ocx`, `.sys`, `.wsf`, `.cat`, `.msp`, `.cpl`, `.efl` formats. To have this functionality enabled, contact your Sectigo account manager.



The following table lists parameters available for the code signing certificates.

Field	Value	Description
Name		The applicant's name.
Email		The email address of the applicant.

Field	Value	Description
Order Number		The order number of the certificate request made to the CA.
Status		The status of the certificate during its issuance process.
	Init	Only applicable to certificates added to the Code Signing on Demand (CSoD) service. Indicates that the certificate issuance process has been initiated by the agent.
	Invited	Indicates that the applicant has been sent an invitation email by the administrator.
	Requested	Indicates that a request for the certificate has been sent to the CA for approval.
	Applied	Indicates that the applicant has validated the email and applied for the certificate.
	Issued	Indicates that the certificate was issued by the CA and collected by SCM, but has not yet been downloaded by the applicant. For the certificates issued for CSoD, the agent automatically downloads the certificate.
	Downloaded	Indicates that the applicant has downloaded the certificate.
	Revoked	Indicates that the certificate is invalid because it was revoked.
	Expired	Indicates that the certificate in question is invalid because its validity period has expired.
	Rejected	The CA rejected the request after validation check.
Organization		The name of the organization to which the applicant belongs.
Department		The name of the department to which the applicant belongs.
Expires		The expiry date of the certificate.
Code Signing on Demand		Indicates whether or not the certificate is enrolled for CSoD service. This is only displayed if CSoD is enabled for the account.
# of Signed Requests		The number of files signed with the certificate. Only applies to certificates generated by the CSoD service.
Key Usage		The cryptographic purposes for which the certificate can be used. For example, key digital signing, encryption, and so on.

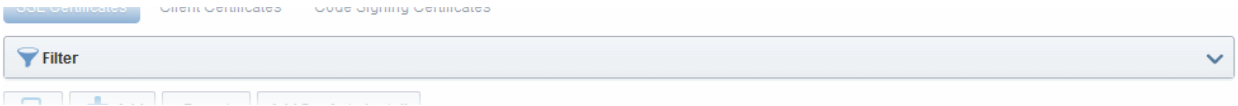
Field	Value	Description
Extended Key Usage		Higher level capabilities of the certificate. You can enable or disable columns by clicking the tool button located to the right of the column headers, as the following illustration shows. 
Control Buttons	Add	Applies for a new code signing certificate. You need to specify a user for the certificate as part of the application.
	Export	Saves the list of code signing certificates in an CSV format.
	Import from CSV	Imports a list of code signing certificates into SCM in comma separated values format.
	Refresh	Updates the currently displayed list of users. Removes any users that have been recently deleted and adds the ones that have been recently created. Updates details such as organization, email and so on, if those details have recently changed.
Certificate Control Buttons [a]	View	Displays the certificate details.
	Resend Invitation	Resends the invitation email to the applicant, thus validating the applicant's email address and allowing them to request their certificate.
	Revoke	Revokes the certificate.
	Delete	Removes the certificate.

a. Depend on the status of the selected certificate.

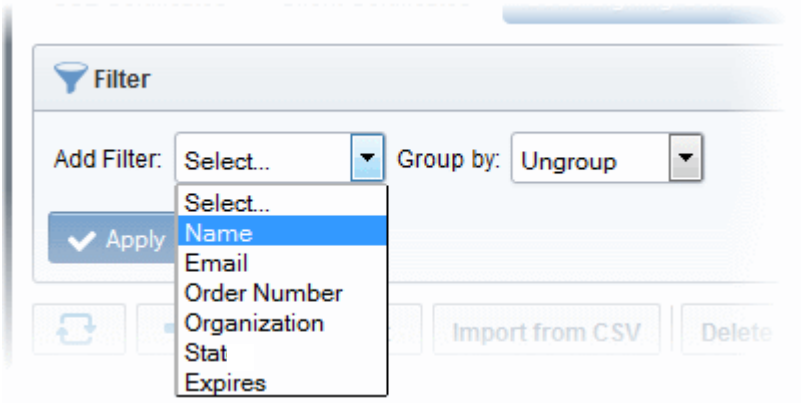
3.4.1 How to Sort and Filter Code Signing Certificates

You can sort items in order of the entries in the column by clicking a column header, and you can use filters to search for particular certificates.

You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.

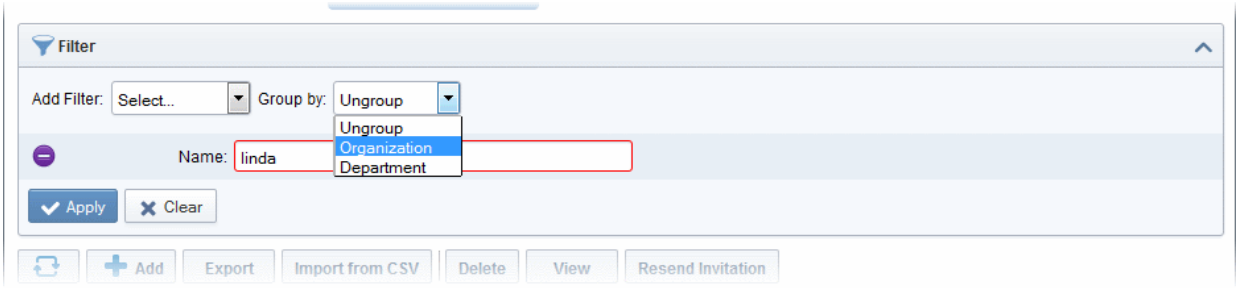


To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection from the **Add Filter** list.



Note that you can add more than one filter at a time to refine the filtering. To remove a filter criterion, click minus (-) located to the left of the filter.

Using the **Group by** list shown in the following illustration, you can select the criteria by which the results are to be grouped.



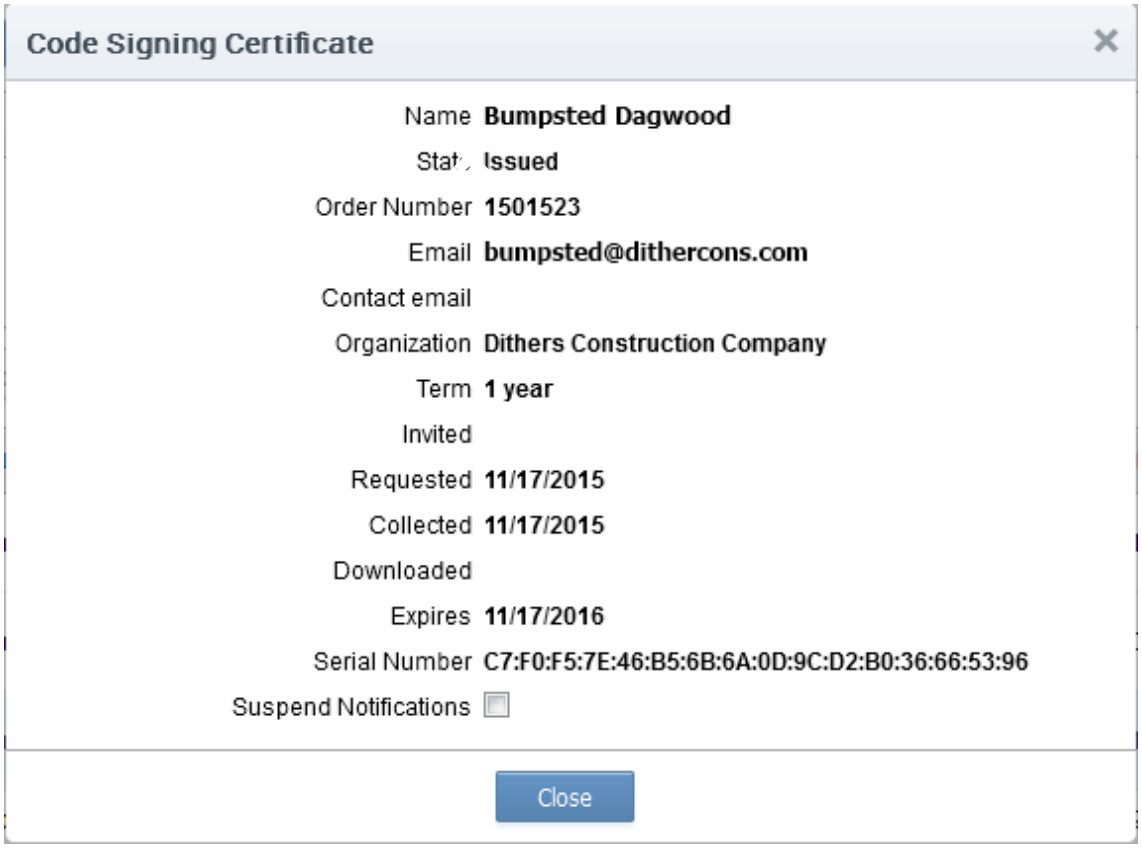
To apply filters and grouping, click **Apply**. You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **Code Signing Certificates** screen, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove all filters.

3.4.2 How to View the Code Signing Certificates Details

You can view and modify the code signing certificate details as follows:

- In the main UI, select **Certificates** > **Code Signing Certificates**, and then click **View** to open the **Code Signing Certificated** dialog shown in the following illustration.


Code Signing Certificate
Name Bumpsted Dagwood
Stat Issued
Order Number 1501523
Email bumpsted@dithercons.com
Contact email
Organization Dithers Construction Company
Term 1 year
Invited
Requested 11/17/2015
Collected 11/17/2015
Downloaded
Expires 11/17/2016
Serial Number C7:F0:F5:7E:46:B5:6B:6A:0D:9C:D2:B0:36:66:53:96
Suspend Notifications
Close

The following table lists settings available in the **Code Signing Certificate** dialog.

Field	Description
Status	The current status of the certificate.
	Invited—Indicates that the end-user has been sent an invitation email by the administrator.
	Requested—Indicates that a request for the certificate has been sent to the CA for approval.
	Applied—Indicates that the end-user has validated the email and applied for the certificate.
	Issued—Indicates that the certificate was issued by the CA and collected by SCM, but has not yet been downloaded by the end-user.
	Downloaded—Indicates that the end-user has downloaded the certificate.
	Revoked—Indicates that the certificate is invalid because it was revoked.
	Expired—Indicates that the certificate in question 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.
Email	The email address of the end-user.
Contact Email	The contact email address or alternative email address of the applicant. The contact email address may be the customer facing email address such as, for example, support@company.com.
Organization	The name of the organization to which the end-user belongs.
Term	The life term of the certificate.
Invited	The date when the invitation was sent to the applicant.
Requested	The date the request was made by SCM to the CA.
Collected	The date of the certificate collection by SCM from the CA.
Downloaded	The date of the certificate download by the end-user.
Expires	The expiry date of the certificate.
Serial Number	The serial number of the certificate as assigned by the CA.

Field	Description
Suspend Notifications	Disables all the automated notifications for events such as certificate download, expiry, revocation from the SCM to the administrator and the end-user, for this certificate.

3.4.3 How to Add Code Signing Certificates to SCM

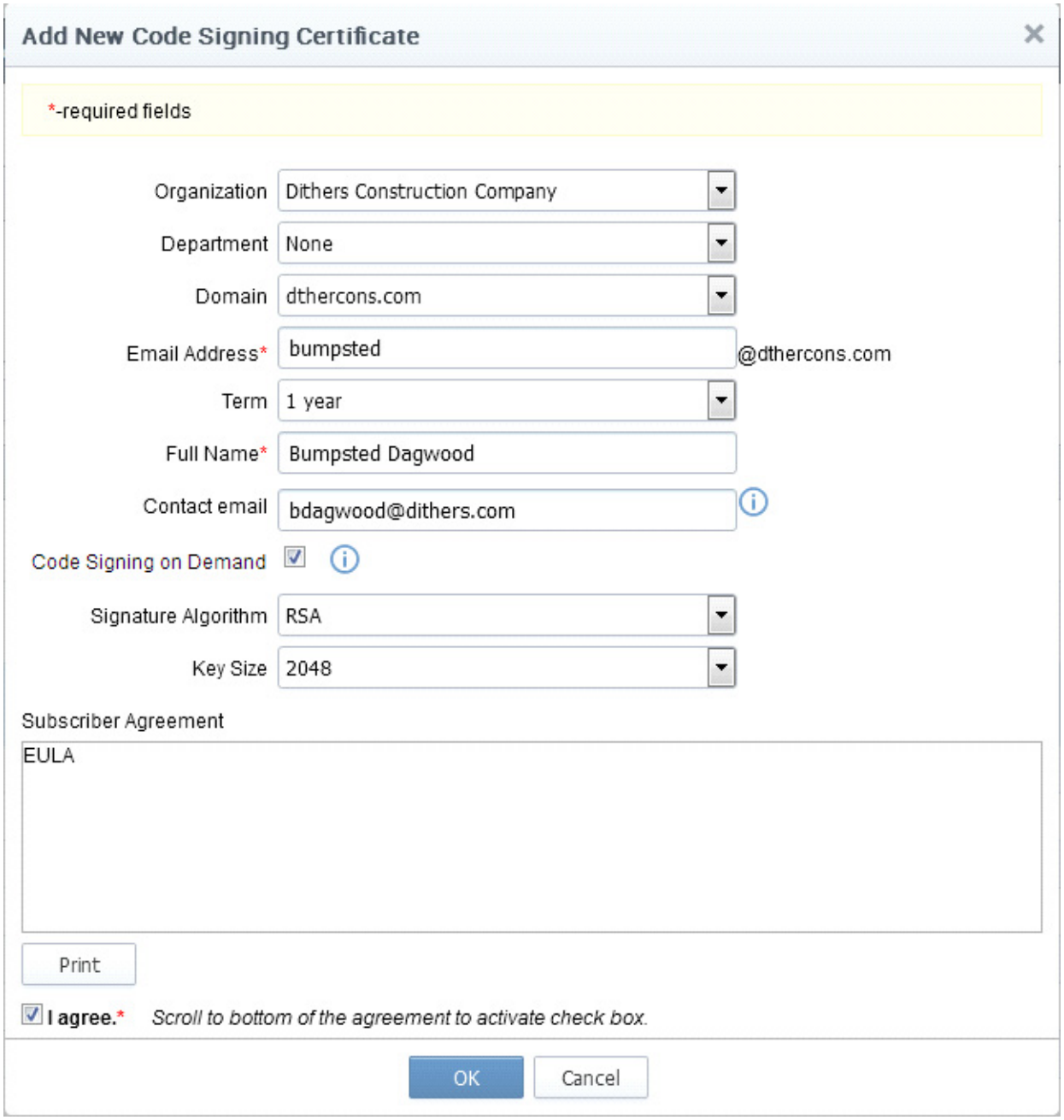
You can add code signing certificates to SCM in one of the following ways:

- Manually (see "Adding Code Signing Certificates Manually" on page 170).
- By loading end-users from a `.csv` file (see "Loading Multiple Certificates from a CSV File" on page 172).
- By enabling an automatic creation of end-users via the certificate self-enrollment form (see "Enabling Automatic Creation of End-Users via Self-Enrollment" on page 174).

3.4.3.1 Adding Code Signing Certificates Manually

You can add code signing certificates for both CSoD and manual signing as follows:

- In the main UI, select **Certificates** > **Code Signing Certificates**, and then click **Add** to open the **Add New Code Signing Certificate** dialog shown in the following illustration.



- Complete the fields based on the information provided in the following table, and then click **OK**. The mandatory fields are marked with red asterisks.

Field	Description
Organization	The organization to which the applicant is to belong.
Department	The department to which the new applicant is to belong.

Field	Description
Domain	The domain pertaining to the department.
Term	The validity period of the certificate.
Email Address	The applicant's email address.
Full Name	The full name of the applicant.
Contact Email	The contact email address of the applicant that should be included in the certificate. The contact email address may be the customer facing email address such as, for example, support@company.com.
Code Signing on Demand	Indicates whether or not the certificate is to be issued to a developer for use in the CSoD. The CSoD must have been set up for your account and you must have added a Developer role to SCM.
Signature Algorithm	The signature algorithm to be used by the certificate. Appears only if **Code Signing on Demand** is enabled.
Key size	The key-size (in bits) of the certificate Appears only if **Code Signing on Demand** is enabled.
Subscriber Agreement	The EULA for the certificate. Read through the EULA and accept to it by selecting **I Agree** for the application to proceed. Appears only if **Code Signing on Demand** is enabled.

If the applicant is an existing user, the corresponding certificate is automatically added to SCM. If the applicant is a new user, an invitation mail is sent to initiate the self-enrollment process. See "How to Request and Issue Code Signing Certificates" on page 174 for more information.

3.4.3.2 Loading Multiple Certificates from a CSV File

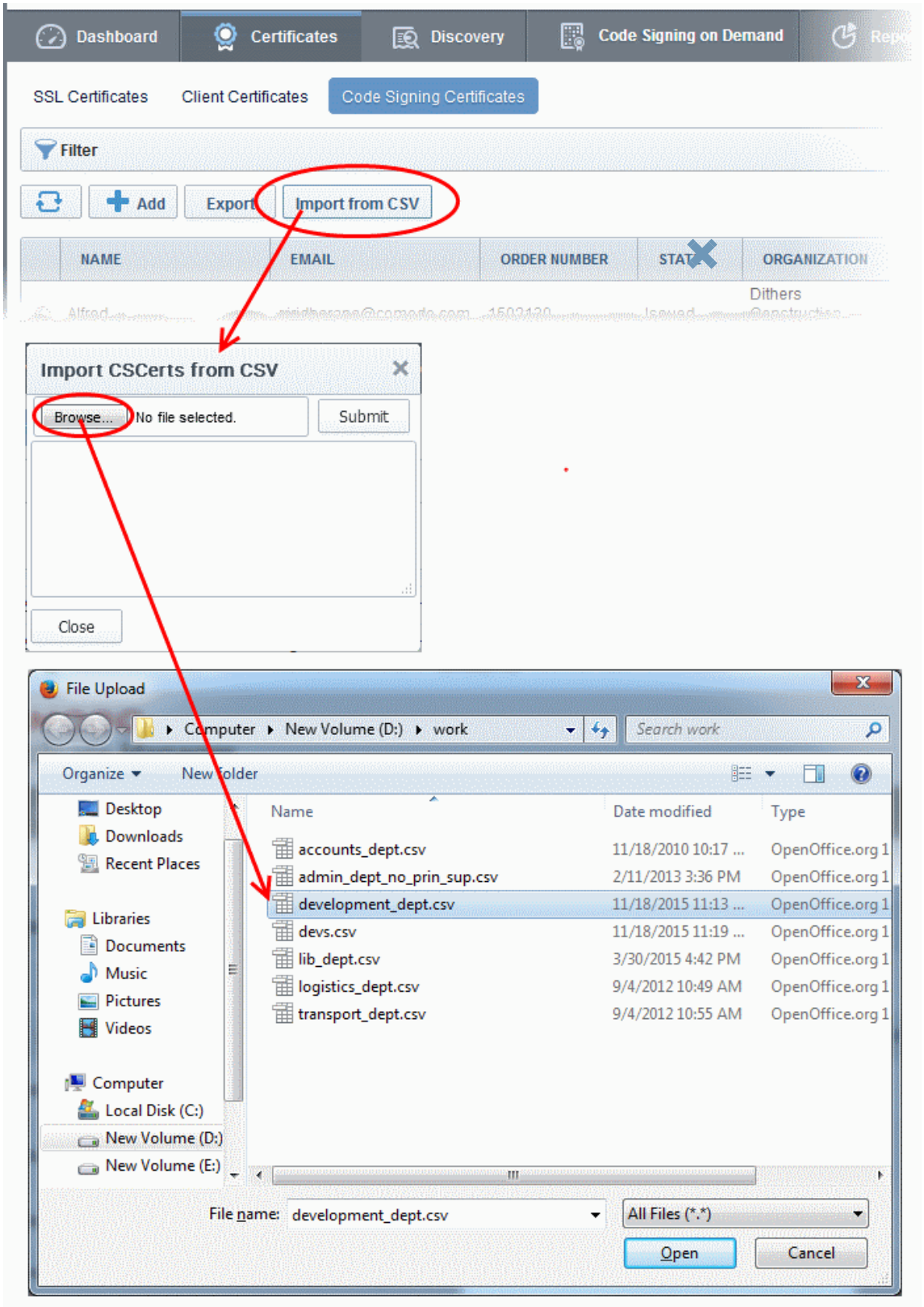
You can import a list of code signing certificates into SCM in comma separated values (`.csv`) format. After importing the list, the certificates belonging to existing users are automatically added and invitation emails are sent automatically to new users to initiate the self-enrollment process.

NOTE: Only the certificates for manual signing can be added by importing the users from a .csv file. Developers for issuance of certificates for CSoD cannot be imported from a .csv file.

To load certificates via a CSV file that contains a list of end-users, follow this procedure:

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

  For information on how to structure `.csv` files for importing multiple certificates, see Appendix B CSV Import Format Requirements.
- In SCM, navigate to **Certificates > Code Signing Certificates**, and click **Import from CSV** to open **Import CS certificates from CSV** dialog, as shown in the following illustration.
- Browse to your `.csv` file and click **Submit** to trigger an upload to SCM, for importing the applicants from it.


Dashboard
Certificates
Discovery
Code Signing on Demand
SSL Certificates
Client Certificates
Code Signing Certificates
Filter
Add
Export
Import from CSV
NAME
EMAIL
ORDER NUMBER
ORGANIZATION
Dithers
Import CSCerts from CSV
Browse...
No file selected.
Submit
Close
File Upload
Computer
New Volume (D:)
work
Search work
Organize
New folder
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
New Volume (D:)
New Volume (E:)
Name
Date modified
Type
accounts_dept.csv
admin_dept_no_prin_sup.csv
development_dept.csv
devs.csv
lib_dept.csv
logistics_dept.csv
transport_dept.csv
File name:
development_dept.csv
All Files (*.*)
Open
Cancel

Upon a successful completion of the import, all the imported data appears in the list of certificates in the **Code Signing Certificates** and **Organization** areas of the SCM UI.

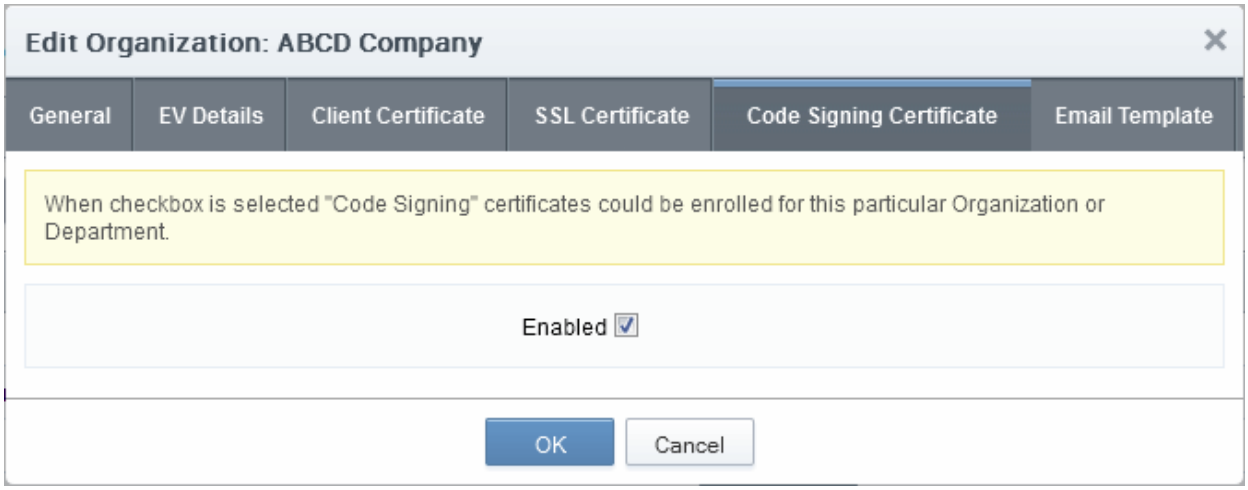
3.4.3.3 Enabling Automatic Creation of End-Users via Self-Enrollment

Certificates issued to end-users by the self-enrollment process initiated by you are automatically added to the **Certificates > Code Signing Certificates** area of the SCM UI. For more information, see "How to Request and Issue Code Signing Certificates" on page 174.

3.4.4 How to Request and Issue Code Signing Certificates

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

- The domain for which the code signing certificate is to be issued has been enabled for code signing certificates, prevalidated by Sectigo, and activated by your Sectigo account manager. (for example, if you wish to issue code signing certificates to `end-user@mycompany.com`, then `mycompany.com` must have been prevalidated by Sectigo.) All certificate requests made on prevalidated domains or sub-domains thereof are issued automatically. If you request a certificate for a brand new domain, then this domain first has to undergo validation by Sectigo. Once validated, this 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. See "How to Create a New Organization" on page 331 and "How to Modify an Existing Organization" on page 360 for more information.
- 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 by selecting **Enabled** in the **Code Signing Certificate** area of the **Add New/ Edit** organizations dialog, as shown in the following illustration.

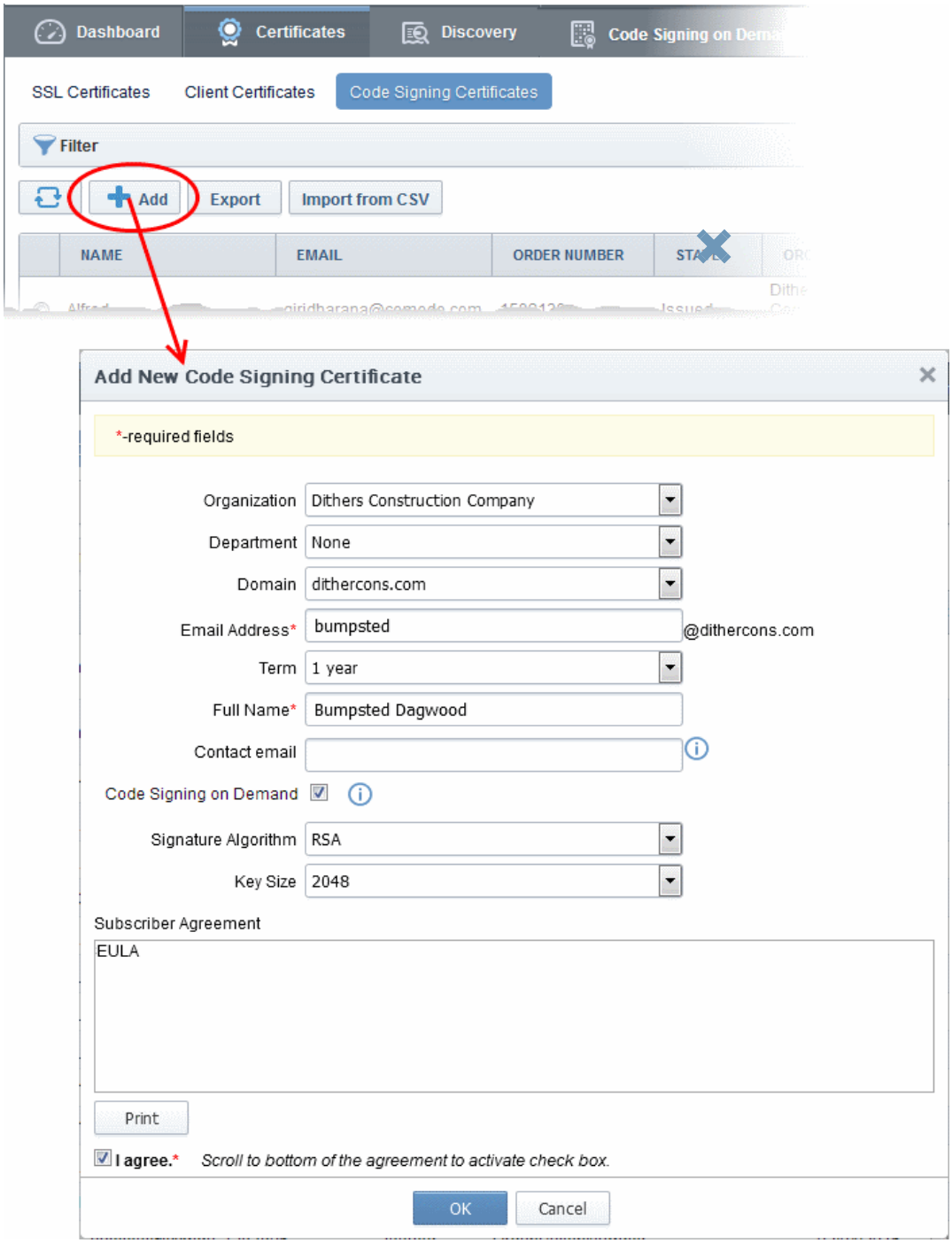


Upon fulfillment of the preceding requirements, the following needs to occur in order for the code signing certificates to be provisioned to end-users via a self-enrollment process:

- You sends an invitation email to the end-user, providing links to begin the enrollment process.
- The end-user validates their email address, and then completes the online application form for the certificate.
- The certificate request is sent to Sectigo servers by SCM.
- If the application is successful, SCM sends an email with a certificate download link to the end-user
- The certificate is added to the end-user account in SCM and can be managed from the **Code Signing Certificates** area of the SCM UI.

You can send an invitation mail to the end-user as follows:

- From the main SCM UI, navigate to **Certificates > Code Signing Certificates** and click **Add** to open the **Add New Code Signing Certificate** dialog shown in the following illustration.



The following table provides descriptions of the form fields and elements. The mandatory fields are marked with the red asterisk on the form.

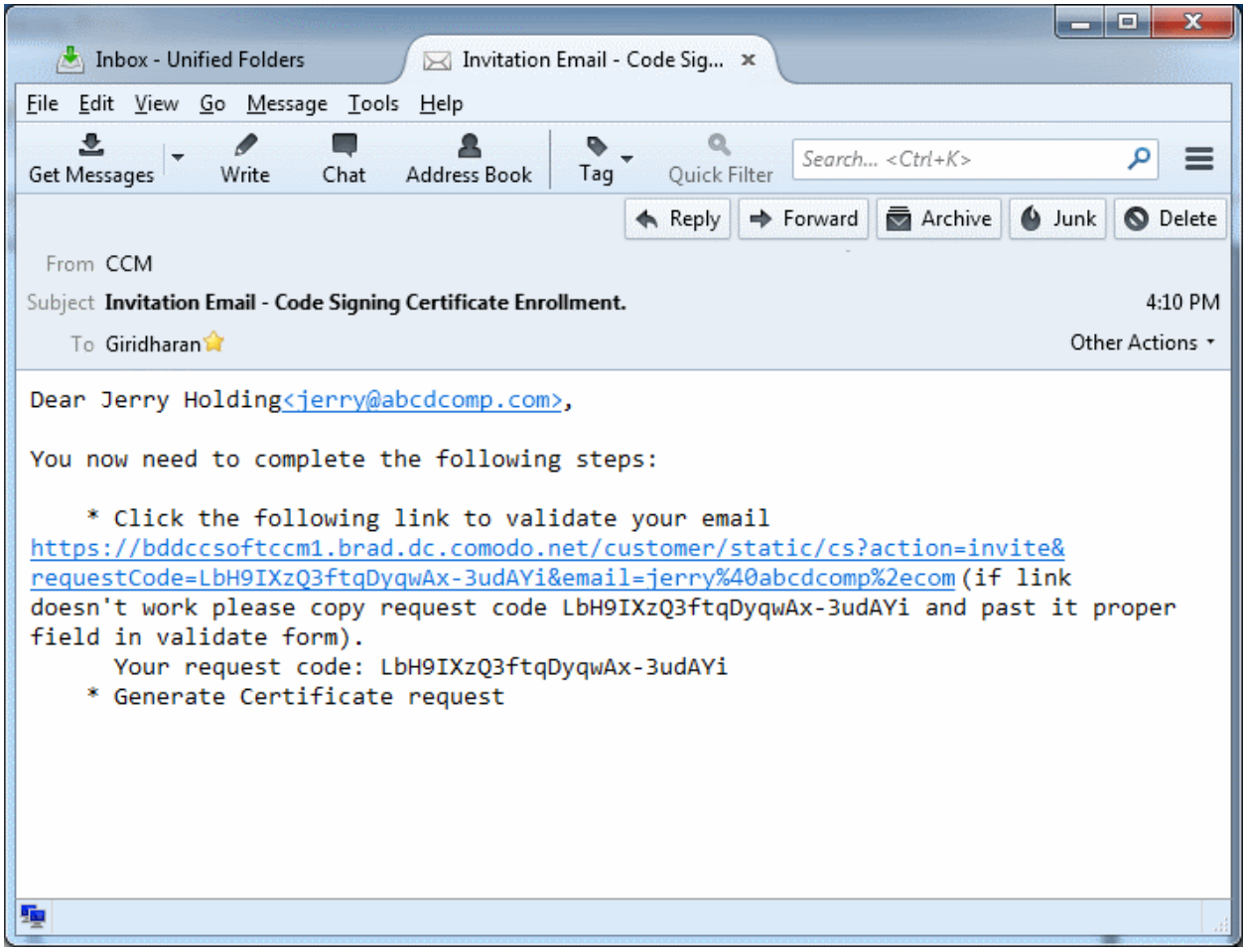
Field	Description
Organization	The organization to which the applicant belongs.

Field	Description
Department	The department to which the applicant belongs.
Domain	The domain pertaining to the department.
Term	The certificate validity period.
Email Address	The email address of the applicant. The invitation message is sent to this address. This is validated before commencing the request process.
Full Name	The full name of the applicant.
Contact Email	The contact email address of the applicant that should be included in the certificate.
Code Signing on Demand	Indicates whether or not to allow the certificate to be used by the CSoD service.

Upon completion, an invitation email is automatically sent to the applicant. The certificate status changes to INVITED in the **Code Signing Certificates** area of SCM UI.

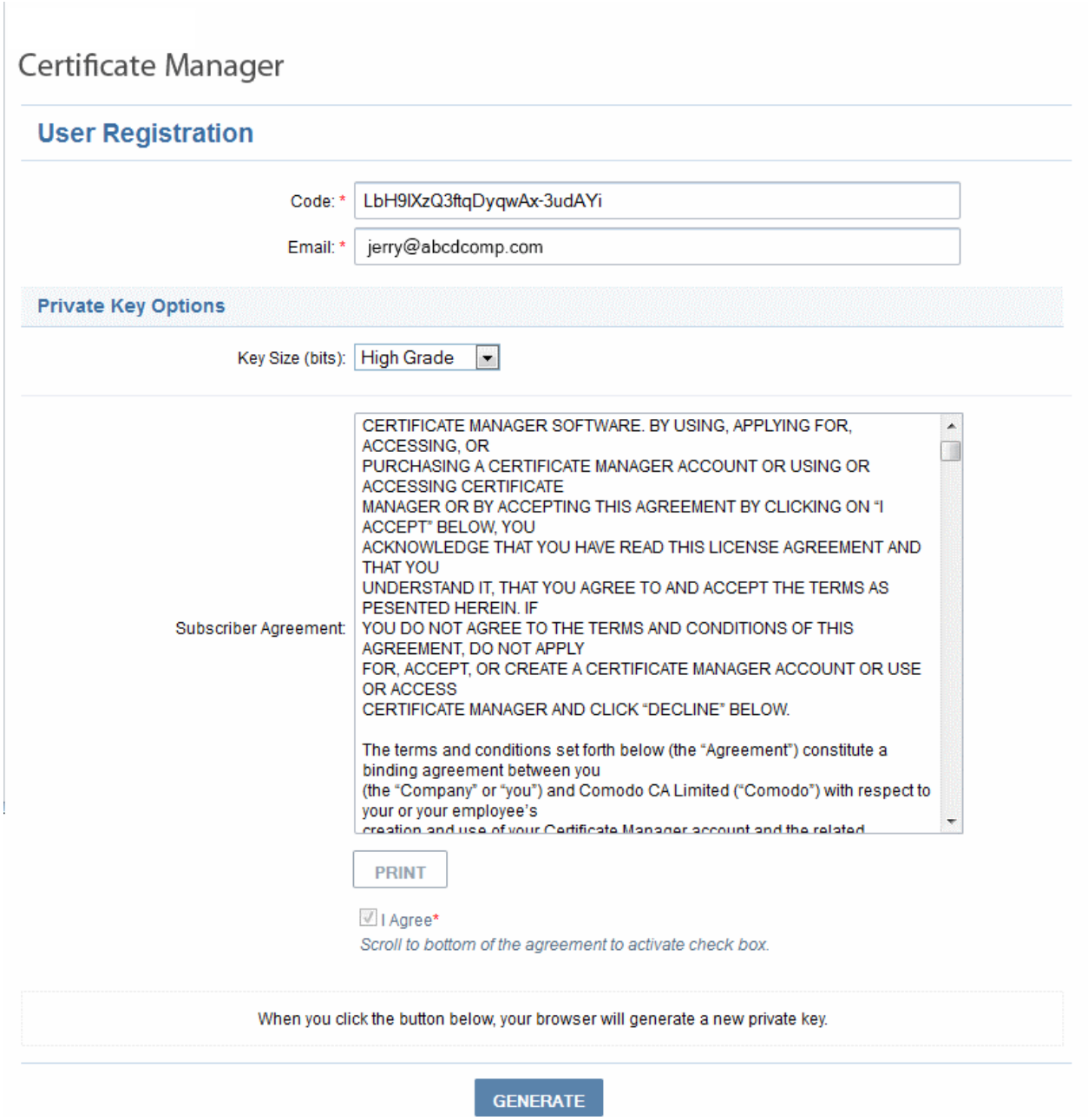
For new applicants added by importing a CSV file, the invitations is sent automatically.

The following illustration shows a invitation email that the applicant receives, with a link to validate their email address.



You can modify the contents of these emails by navigating to the **Settings > Templates > Email Template** area.

Upon clicking the link in the mail, the email address is validated and the applicant is taken to the **User Registration** dialog shown in the following illustration.

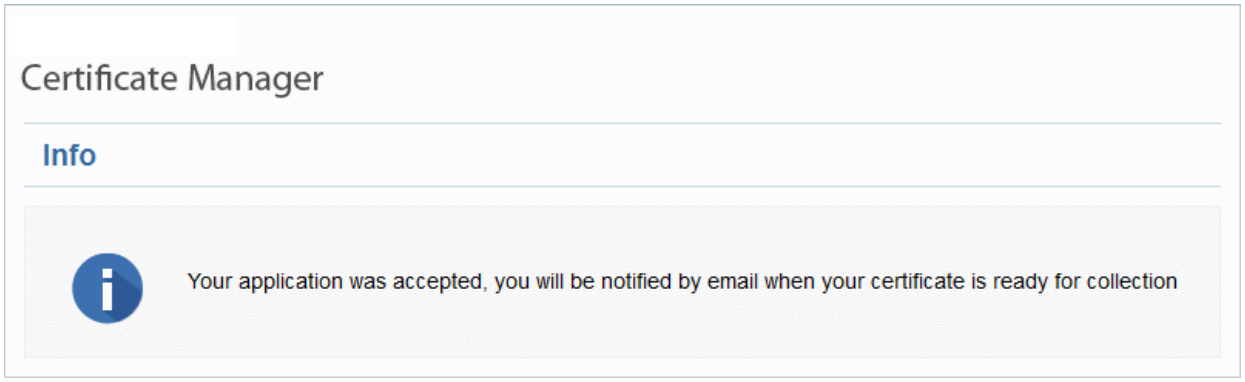


The following table provides descriptions of the form fields and elements. The mandatory fields are marked with the red asterisk on the form.

Field	Description
Code	Auto-populated with the certificate request code, on clicking the validation link in the email. If not, the end-user can copy the request code from the email and paste in this field.
Email	Auto-populated with the email address of the applicant.

Field		Description
Advanced Private Key Options	CSP	The cryptographic service provider for the certificate (default is Microsoft Cryptographic Provider v1.0).
	Key Size	The key size for the private key of the certificate (default is 2048 bit). Note: The private key is generated locally by the crypto module of the browser or operating system. The key never leaves the computer and no copy is ever transmitted to the certificate issuer. Sectigo does not collect a copy of the private key at any time and cannot be recovered if it is lost. The certificate is useless without it. Hence the end-users are strongly advised to backup their private key during the certificate installation process.
	Exportable	The applicant can choose whether or not the certificate is exportable.
	User Protected	If enabled, allows to set password and security levels during the certificate collection process. The operating system prompts for a password and permission every time the certificate is accessed to code sign.
Subscriber Agreement		Applicant must accept the terms and conditions before submitting the form.
Generate		Starts the certificate generation process.

The applicant needs to complete the form, accept the subscriber agreement, and clicking **Generate**. The certificate request is automatically generated and a request is sent to SCM.



Upon completion, the certificate status is set to Requested in the **Code Signing Certificates** area of the SCM UI. SCM processes the request and sends a certificate request to a Sectigo server, after which the certificate status is set to Applied.

After the applicant follows the link and downloads the certificate, the certificate's status is changed to Downloaded. The certificate can be installed by the user and used to digitally sign the executables.

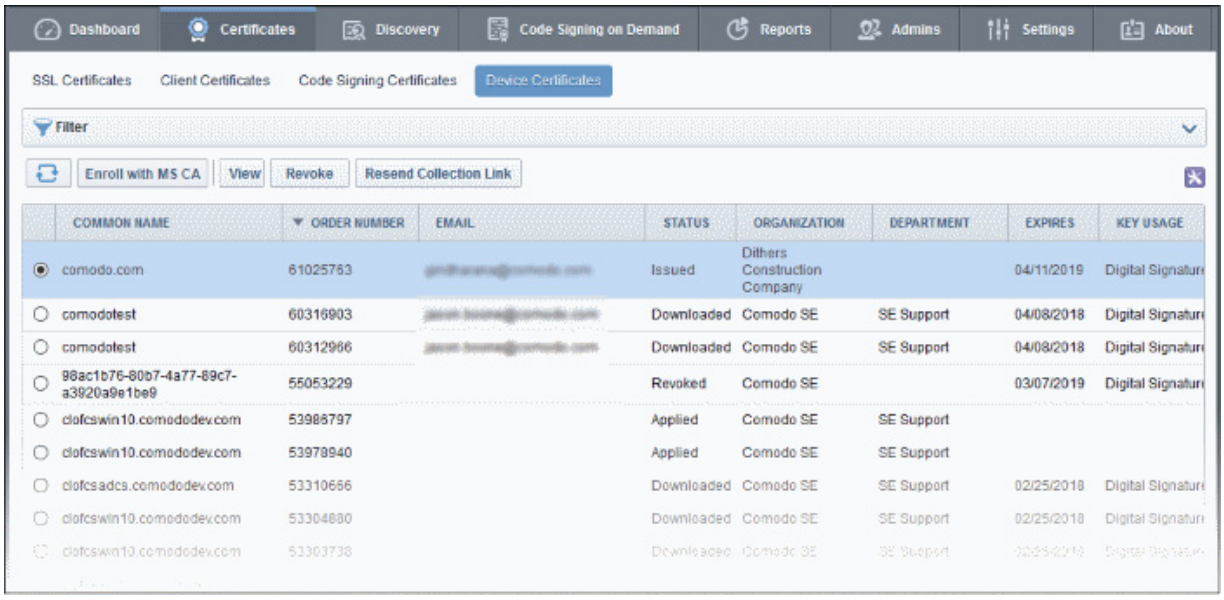
3.5 Managing Device Certificates

Depending on your security role, the **Device Certificates** area shown in the following illustration allows you to manage certificates issued to devices that have been added to SCM via active directory or self-enrollment. In addition to the request and issuance of device certificates, SCM can issue certificates from private CAs. To enable device certificates or add a private CA to your SCM account, contact your Sectigo account manager.

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

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

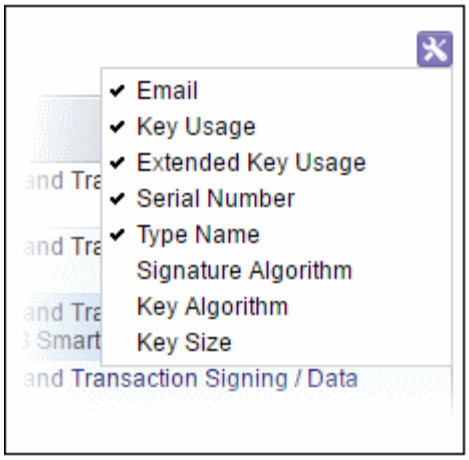
DRAO Device Certificate administrators can view the device certificates of departments that have delegated to these administrators.



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

Column	Value	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.
Order Number		The order number of the certificate.
Email		The email address of the applicant that was provided during self-enrollment.

Column	Value	Description
Status		The current status of the certificate:
	Awaiting Approval	A device certificate request has been placed with SCM using the self- enrollment method.
	Requested	A device certificate request has been placed with SCM by either (1) the MS Agent installed on the AD server to which the device is enrolled; (2) by the device through SCEP; (3) through an API call by the Mobile Device Manager (MDM) software used by the organization. You can view, edit, approve, decline, or revoke the request.
	Declined	A certificate request that was made using the self-enrollment form has been rejected by one of the following administrators: • A MRAO who can decline any certificate requests from any organization or department; • A DRAO Device Certificate who can decline certificate requests for organizations over which they have been delegated control. • A DRAO Device Certificate who can decline certificate requests for departments over which they have been delegated control.
	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.
	Downloaded	The certificate has been downloaded by the MS Agent or device.
	Expired	The certificate is invalid because its validity period has expired.
	Revoked	The certificate is invalid because it was revoked.
	Rejected	The certificate request was declined by the administrator.
Organization		The name of the organization to which the certificate belongs.
Department		The name of the department to which the certificate belongs, if applicable).
Expires		The expiration date of the certificate.
Key Usage		The cryptographic purposes for which the certificate can be used. For example, signing, non repudiation, authentication and encryption.
Extended Key Usage		Higher level capabilities of the certificate.
Serial Number		A unique number which identifies the certificate.
Type Name		The name of the device certificate.

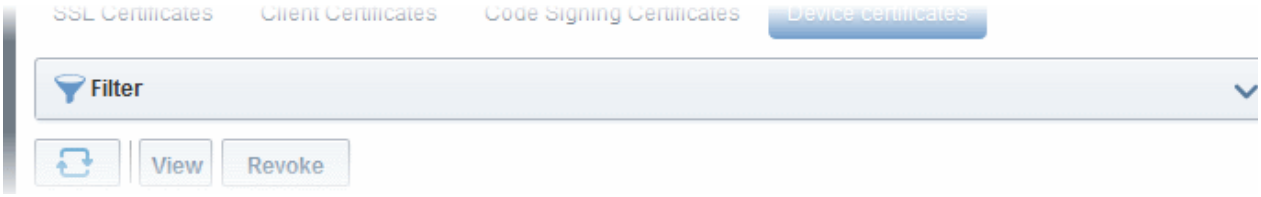
Column	Value	Description
You can add more column headers using a tool button beside the last item in the column:  		
Signature Algorithm		The signature algorithm of the public key of the certificate.
Key Algorithm		The type of algorithm used for encryption.
Key Size		The key size used by certificate for encryption.
Control Buttons	Refresh	Updates the currently displayed list of certificates.
	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 / Decline	Enables you to approve or 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 Collection Mail.
	Download	Download an issued certificate. This applies to certificates from MS CA.

a. The types of certificate control buttons that are displayed in the table header depends on the status of the selected certificate

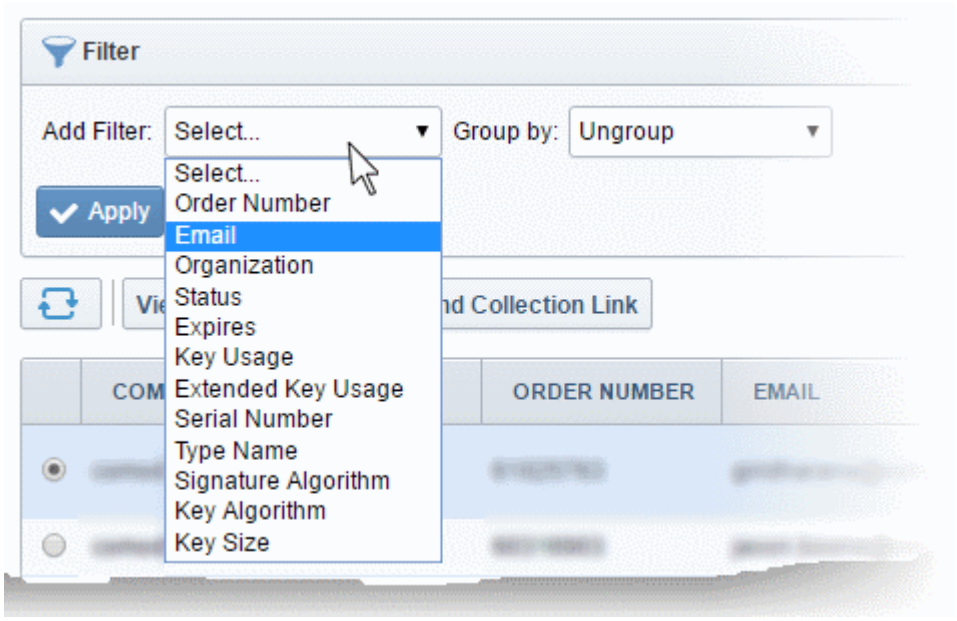
3.5.1 How to Sort and Filter Device Certificates

You can sort items in order of the entries in the column by clicking a column header, and you can use filters to search for particular device certificates.

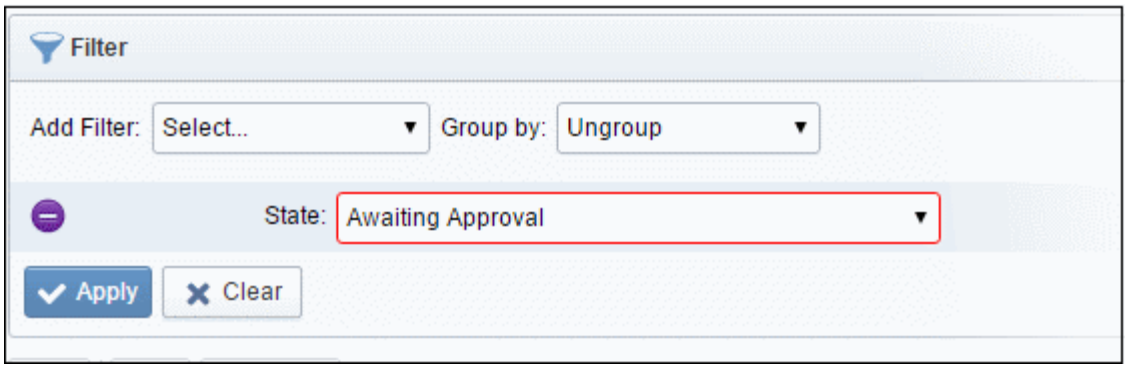
You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.



To add filters, you make a selection in the **Add Filter** list shown in the following illustrations, and then group the results with other options that appears depending on the selection from the **Add Filter** list. You can add more than one filter at a time.



Click **Apply** to trigger the display of the filtered items based on the entered parameters, as the following illustration shows. To remove the filter options, click **Clear**.



The following table describes the filter criteria and their filter parameters available for the device certificates:

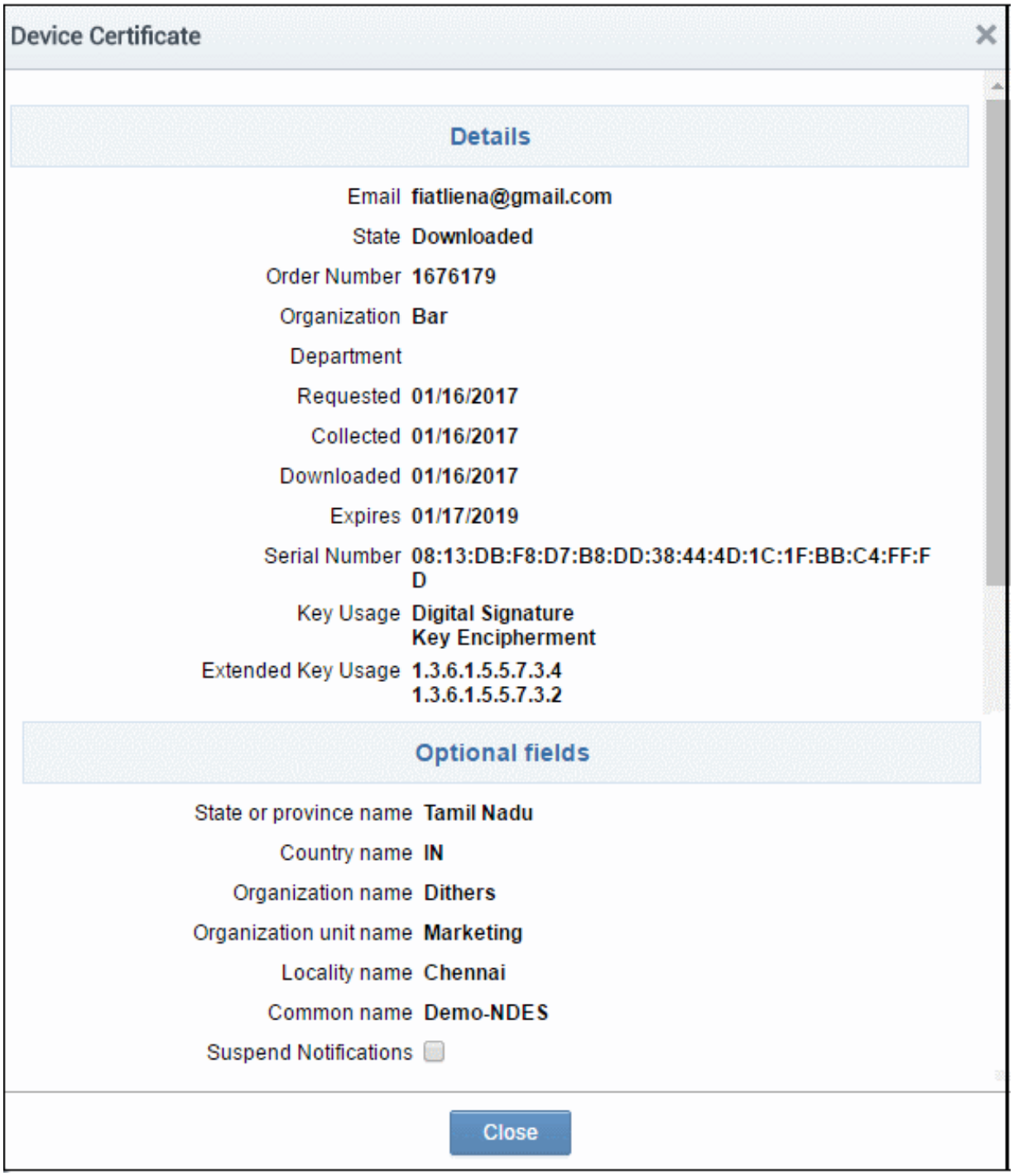
Filter Criteria	Filter Parameter
Order Number	Search for a particular order number.
Email	Find certificates by applicant email address.
Organization	Find certificates belonging to a specific organization or department
Status	Filter by certificate status.
Expires	Find certificates which expire within a certain number of days.
Key Usage	Filter certificates by cryptographic capabilities.
Extended Key Usage	Filter certificates by higher level purpose.
Serial Number	Enter the serial number of the certificate in full or part.
Type Name	Filter certificates by their type.
Signature Algorithm	Filter by signature algorithm of the certificate.
Key Algorithm	Filter by key algorithm of the certificate.
Key Size	Filter by key size in bits.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **Device Certificates** area, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

3.5.2 How to View the Device Certificate Details

You can view a device certificate details as follows:

- In the main UI, select **Certificates** > **Device Certificates**, and select a certificate to view to open the Device Certificate Details dialog shown in the following illustration.
- Click **Certificates** to open **Certificates for** screen shown in the following illustration.



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

Field	Value	Description
Email		The email of the end-user.

Field	Value	Description
Status	Awaiting Approval	Indicates that a device certificate request has been placed with SCM using the self-enrollment form.
	Requested	Indicates that a request has been received for the certificate. Requests need to be approved by the administrator.
	Declined	Indicates that a certificate request that was made using the self-enrollment form has been rejected by an administrator.
	Applied	Indicates that the request has been approved and sent to Sectigo.
	Issued	Indicates that the certificate has been issued by the CA and collected by SCM.
	Downloaded	Indicates that the certificate has been downloaded by the MS Agent or the device.
	Expired	Indicates that the certificate is invalid because its term has expired.
	Revoked	Indicates that the certificate is invalid because it was revoked.
	Rejected	Indicates that the CA rejected the request after a validation check.

Field	Value	Description
Order Number		Order number of the certificate. Does not apply to certificates enrolled via MS CA.
Organization		The name of the organization to which the device certificate belongs.
Department		The name of the department to which the device certificate belongs.
Requested		The date the certificate request was sent to Sectigo from SCM or date of certificate request from MS CA by the administrator.
Collected		The date the certificate was collected by SCM from Sectigo.
Downloaded		The date the certificate was downloaded by the end-user or the administrator.
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.
Optional fields		Available for certificates applied for via the self-enrollment method. Displays details such as organization name, common name, and so on.
Suspend Notifications		Disables automatic notifications to administrators and end-users for events like certificate download, expiry, and revocation.

3.5.3 How to Request and Issue Device Certificates

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

- **Through 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 which have been integrated with SCM. AD integration is achieved through the Network Device Enrollment Service (NDES). See "Issuing Device Certificates by Proxy CA Through Active Directory" on page 189 for details.
  - MS CA: Device certificates can also be requested from MS CA. See "Issuing Device Certificates by Proxy CA Through Active Directory" on page 189 for details.
- **Through SCEP**—SCM has the SCEP server integrated. You can push a configuration profile to the devices for enrollment of certificates to SCM. See "Issuing Device Certificates Through SCEP" on page 192 for details.

- **Through 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=.
- **Through Self Enrollment**—Device certificates can be requested by applicants using the self-enrollment form available by clicking the link provided by an administrator. See "Issuing Device Certificates Through Self-Enrollment" on page 195 for details.

3.5.3.1 Issuing Device Certificates by Proxy CA Through Active Directory

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

- The AD certificate service has been installed on the AD server with NDES role.
- The AD server has been added to SCM by installing the MS Agent and must be connected. The agent must have been enabled as CA Proxy during its installation. See "Configuring Network Agents" on page 252 for details.
- A RAO or DRAO Device Certificate administrator has been delegated control of this organization or department

Typically, the process consists of the following:

- The AD Domain administrator creates a Group Policy Object (GPO) with a certificate template and applies it to the devices.
- The devices generate the certificate request and forward them to NDES configured with the MS Agent as CA proxy.
- NDES forwards the certificate requests to the MS Agent. The agent creates certificate requests and forwards them to SCM.
- The certificate requests are added to the **Certificates > Device Certificates** UI for approval, with a status of the certificate as Requested.
- A MRAO, RAO or DRAO with appropriate privileges approves the request and SCM forwards the request to Sectigo, with the status of the certificate changing to Applied. Upon issuance of the certificate, SCM collects the certificates. The status of the certificate is changed to Issued.
- The MS Agent tracks the order. Once the certificate is issued, the agent downloads the certificates and forwards them to NDES server. The status of the certificate is changed to Downloaded.
- NDES server pushes the certificates to the target devices.

For an overview of basic deployment steps for NDES, see https://technet.microsoft.com/en- us/library/hh831498.aspx.

3.5.3.2 Issuing Device Certificates by MS CA Through Active Directory

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

- The AD certificate service has been installed on the AD server with MS CA role.
- MS AD certificate templates have been configured appropriately.
- The AD server has been added to SCM by installing the MS Agent and is connected. **Enroll on Behalf** should have been set on the agent during installation. See "Configuring Network Agents" on page 252 for details.
- Certificate generation is performed by a MRAO administrator.

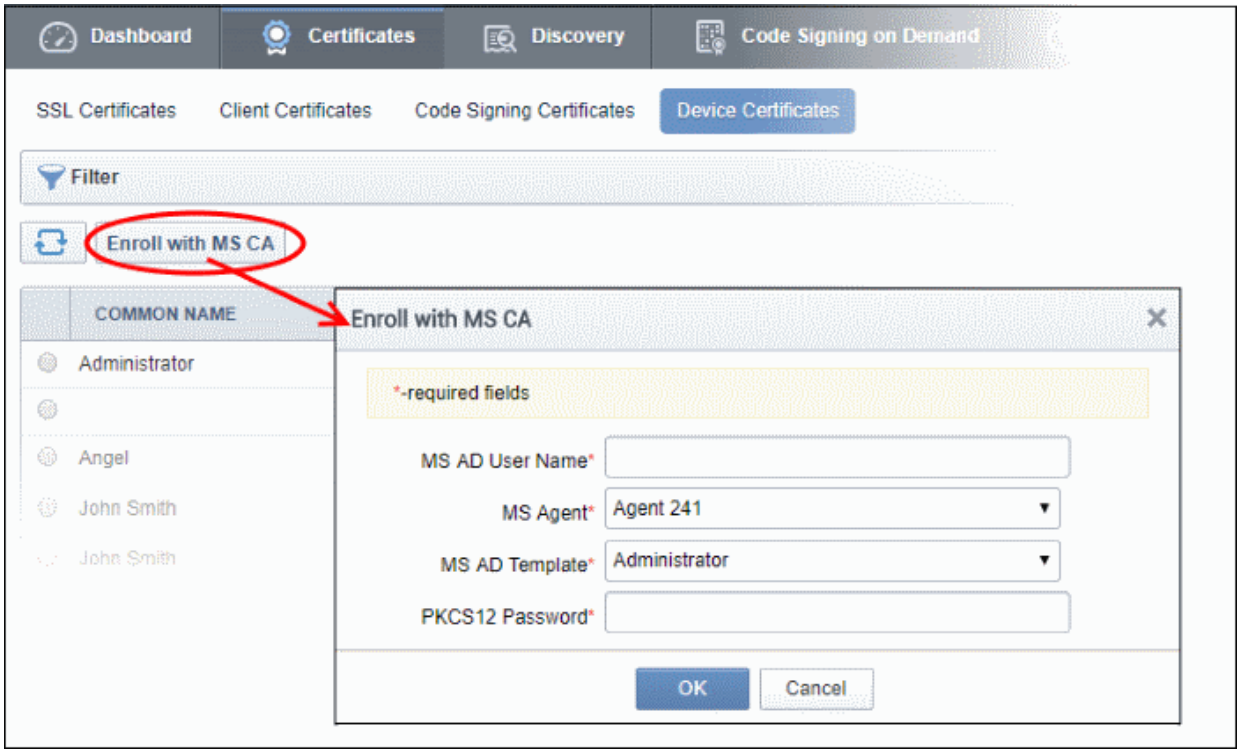
Typically, the process involves the following:

- A MRAO initiates the process via the SCM UI.

- The MRAO enters required details, including user name who has permission to make certificate requests, MS Agent to be used, MS AD template, and password for importing and installing the certificate.
- MS CA generates the certificate according to the template.
- The status of the certificate is Approved, and then after a few minutes it changes to Issued.
- You click **Download** to collect the certificate, then you can install it on the device or send it to the user.

You enroll a device certificate via MS CA as follows:

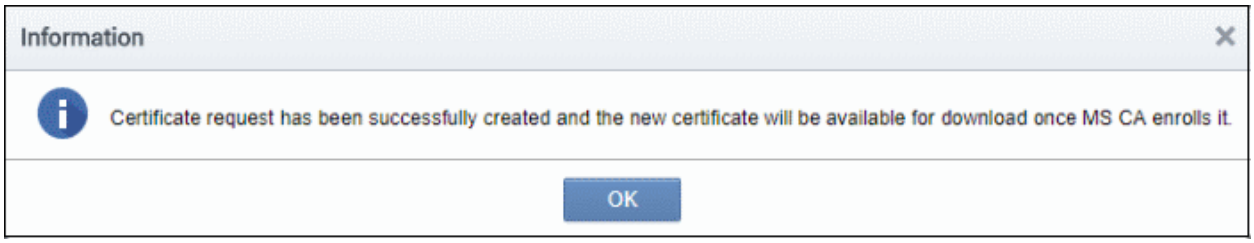
- From the main UI, navigate to **Certificates > Device Certificates** and click **Enroll with MS CA** to open the corresponding dialog, as the following illustration shows.



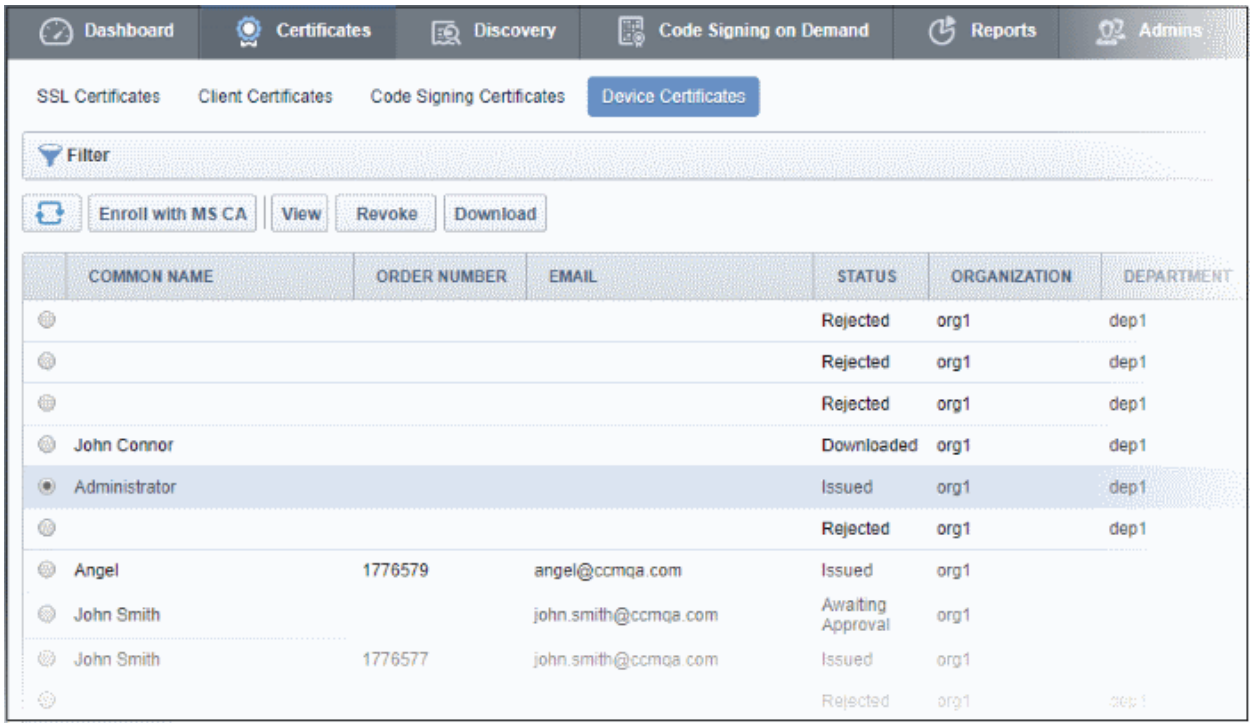
The following table lists and describes fields available in the **Enroll with MS CA** dialog.

Field	Description
MS AD User Name	The AD user name with privileges to create requests for certificates.
MS Agent	The MS Agent through which the certificate request is generated.
MS AD Template	The MS AD template to use.
PKCS12 Password	The password to be used for importing and installing the certificate after downloading.

Upon completion of the dialog, a message notifying about the successful creation of the request is displayed, as shown in the following illustration.

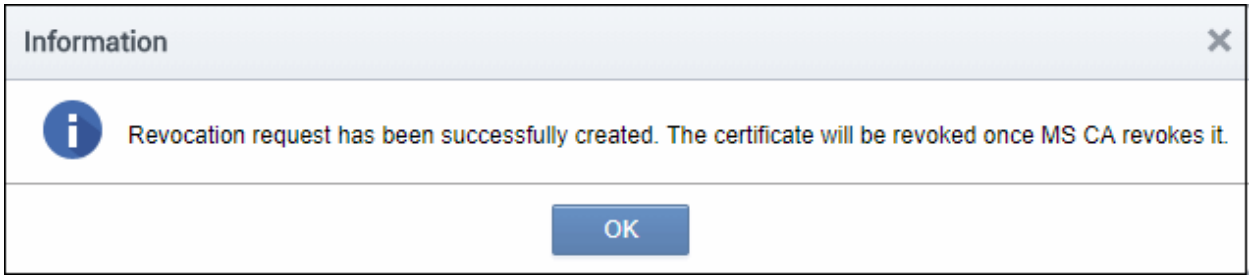


The status of the certificate is Approved; after a few minutes it changes to Issued, as shown in the following illustration.



To download a certificate to the default download directory on your computer, select that certificate and click **Download**. This changes the status from Issued to Downloaded.

To revoke a device certificate with Issued or Downloaded status, select that certificate, click **Revoke**, provide a reason for revocation, and then click **OK**, as the following illustration shows.



This changes the status of the certificate to Revoked.

3.5.3.3 Issuing Device Certificates Through SCEP

SCM allows you to issue device certificates by creating configuration profiles which are pushed to target devices. The configuration profile can be created using software such as the iOS configuration utility.

To issue device certificates through SCEP, you create new device certificate types and enable them for SCEP enrollment. Each device certificate type is assigned with a device type ID to identify it in the configuration profile applied to the devices.

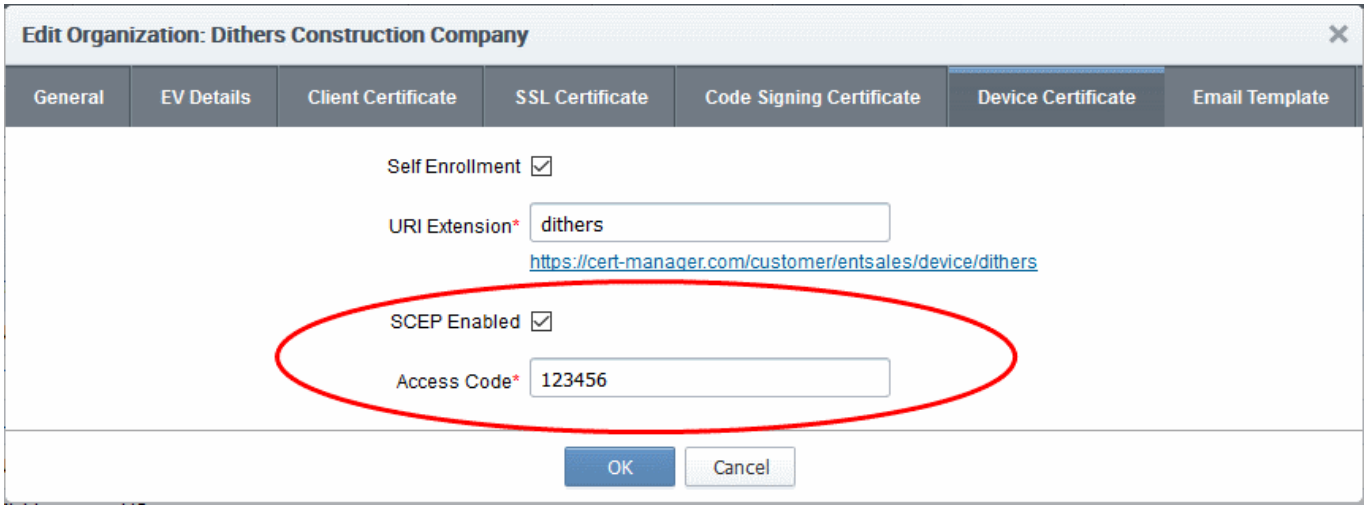
The following requirements must be met for the process to succeed:

- Private CAs must be enabled for your account in order to add device certificate types. Contact your Sectigo account manager for details.
- SCEP enrollment needs to be enabled for an organization or department, and an access code must be specified. This can be done when adding or editing an organization or department.

You enable SCEP enrollment for an organization as follows:

- From the main UI, navigate to **Settings**, select **Organizations**, and then click **Add** or select an organization and click **Edit**.

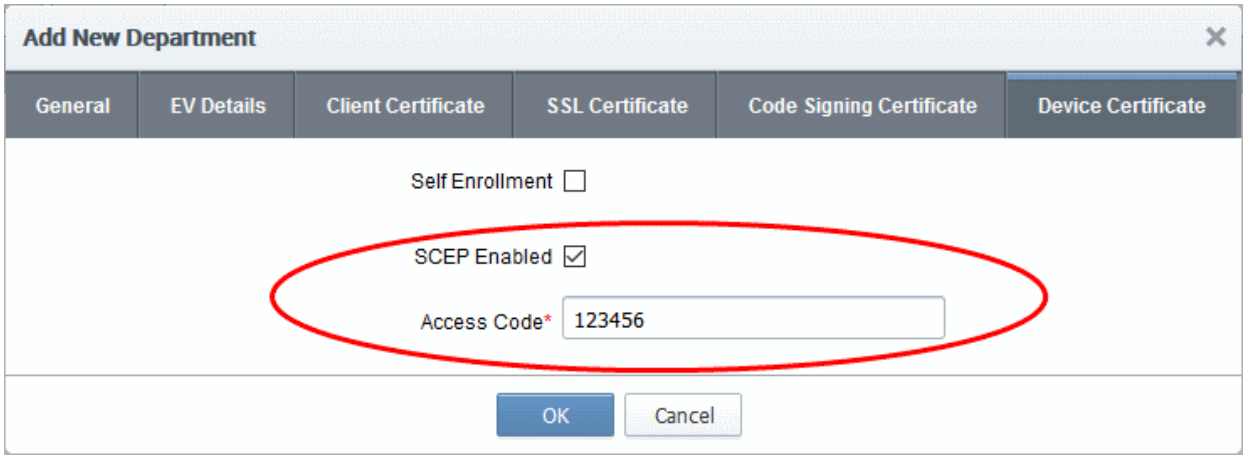
- In the **Add New Organization** or **Edit Organization** dialog that opens, select **Device Certificate**, as the following illustration shows.
- Select **SCEP Enabled**. This triggers a display of the **Access Code** field.



Enter the access code. This code must consist of a combination of alpha and numeric characters. The access code for the organization should be entered as the `challengePassword` parameter in the profile applied to devices which belong to that organization.

You enable the SCEP enrollment for departments as follows:

- From the main UI, navigate to **Settings** and select **Organization.**
- In the **Organizations** area, select an organization and then select the **Departments** area to view its departments.
- Click **Add** on the **Departments** area, or select an existing department and click **Edit**.
- In the **Add New Department** or **Edit Department** dialog that opens, select **Device Certificate**, as the following illustration shows.
- Select **SCEP Enabled**. This triggers the display of the **Access Code** field.

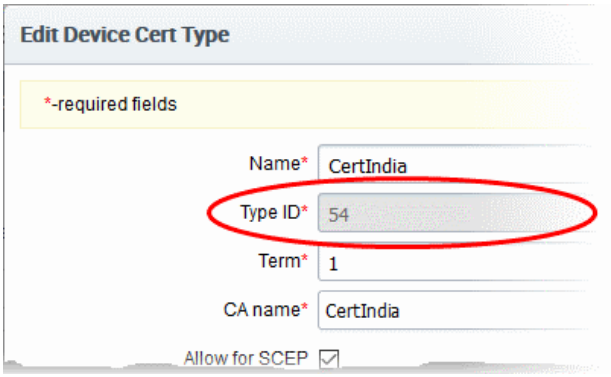


Enter the access code. This code must consist of a combination of alpha and numeric characters.

You need to include the URL of the SCEP server in the configuration profile for OTA enrollment. The URL should be in the following format:

```
http://<SCM Server>/customer/<customer name>/scep/
device;deviceTypeId=<DeviceTypeId>/pkiclient.exe
```

The following table describes the URI parameters:

Parameter	Description
<SCM Server>	The address of the SCM server you use.
<customer name>	Your SCM company name.
<DeviceTypeId>	The identification number assigned to the type of device certificate to be enrolled. The type ID can be viewed from the SCM interface as follows: • Navigate to **Settings > Certificates > Device Certificate Types**. • Select the device certificate type and click **Edit**. The **Type ID** is displayed in the **Edit Device Certificate Type** dialog. 

The URI protocol should be `http` as opposed to `https`, since the SCEP protocol relies on signed messages during a transaction. For example:

```
http://cert-manager.com/customer/AmeCorporation/scep/device;deviceTypeId=54/
pkiclient.exe
```

Typically, the process involves the following:

- 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 organization or department is included in the profile. This means the certificate request generated by the device contains the access code as the `challengePassword` parameter.
- Once applied, the device generates the certificate request and forwards it to SCM.
- The certificate requests are added to the **Device Certificates** area for approval. The status of the certificate is indicates as Requested.
- 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. Upon issuance of the certificate, SCM collects the certificates. The status of the certificate changes to Issued.
- 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.

3.5.3.4 Issuing Device Certificates Through Self-Enrollment

Self-enrollment allows applicants to request device certificates from Sectigo, as well as from private CAs which have been added to the SCM account. Contact your Sectigo account manager to add a private CA to your SCM account.

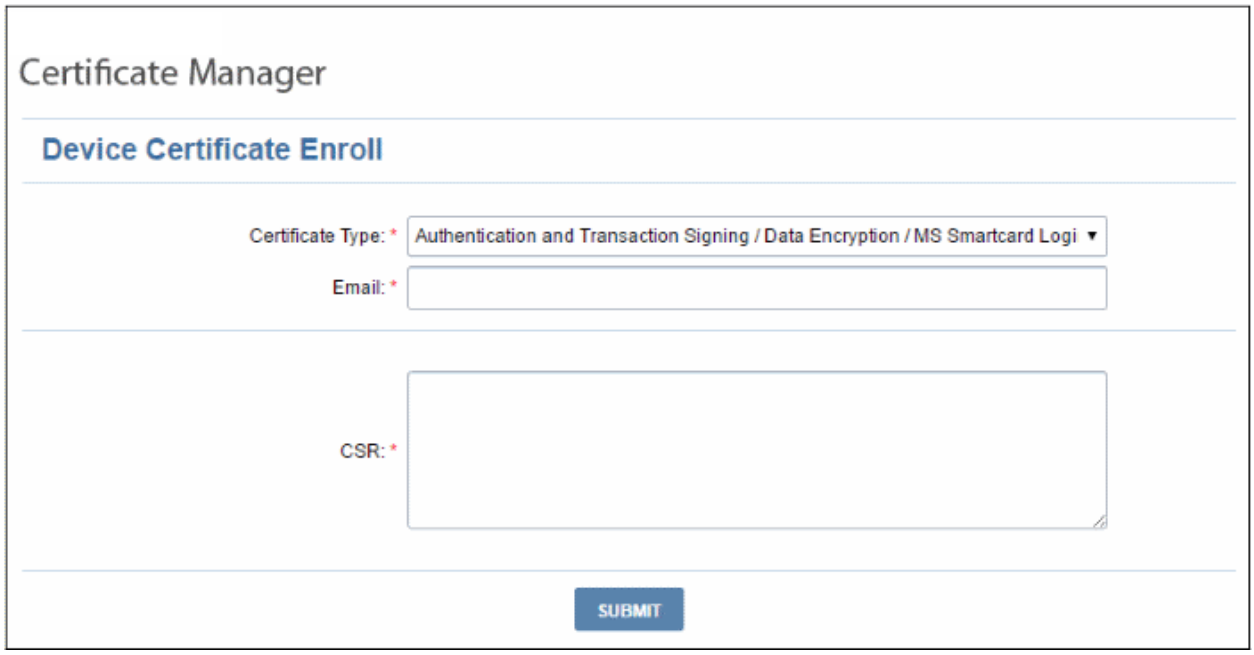
The following requirements must be met for the process to succeed:

- The issuance of device certificates is enabled for your account.
- Device certificates are set to be available for self-enrollment through **Settings > Certificates > Device Certificate Types**.
- The issuance of device certificate through self-enrollment is enabled for the organization or department under **Settings > Organizations** or **Settings > Department**, then **Add** or **Edit** clicked to transition to the **Device Certificate** area.
- The RAO Device Certificate or DRAO Device Certificate administrator has been delegated control of this Organization or Department

Typically, the process involves the following:

- You confirm completion of the preceding steps.
- You send the self-enrollment link to the applicant.
- Applicant completes and then submits the self-enrollment form shown in the following illustration.
- The certificate request is approved by appropriate administrators.
- If the application is successful, the applicant can download and install their device certificate (see "Certificate Collection" on page 119).

Upon fulfillment of the requirements, you need to communicate enrollment link details via email to each end- user. The end-user can access the form at the given URL, complete and submit it.



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

The following table lists the self-enrollment fields and their values. The mandatory fields are marked with red asterisks.

Field	Description
Certificate Type	The device certificate type. Only device certificate types enabled for self-enrollment are available.
Email Address	The applicant's full email address. The device certificate collection notification is sent to this email address.
CSR	The public key.
Submit	Submits the application and enrolls the applicant for the device certificate.

3.5.3.5 About the Device Certificate Collection

Once the enrollment form is submitted and approved by appropriate administrators, the device certificate collection mail is sent to the email address provided in the enrollment form.

SCM delivers the certificate to the applicant in the formats shown in the following illustration. The access to this file is protected by a PIN which the applicant is asked to enter when they import the certificate into the certificate store on their computer.

Your Device Certificate for CCMQA.COM is enrolled.

The Device Certificate for CCMQA.COM has been enrolled.

Please download it using the links:

as PKCS#7, Base64 encoded: https://ccmqa.com/customer/110/device/download/135/3

as PKCS#7, Bin encoded: https://ccmqa.com/customer/110/device/download/135/4

as X509, Base64 encoded: https://ccmqa.com/customer/110/device/download/135/0

as X509 Certificate only, Base64 encoded: https://ccmqa.com/customer/110/device/download/135/1

as X509 Root/Intermediate(s) only, Base64 encoded: https://ccmqa.com/customer/110/device/download/135/2

as X509 Intermediate(s)/Root only, Base64 encoded: https://ccmqa.com/customer/110/device/download/135/5

Certificate Details:

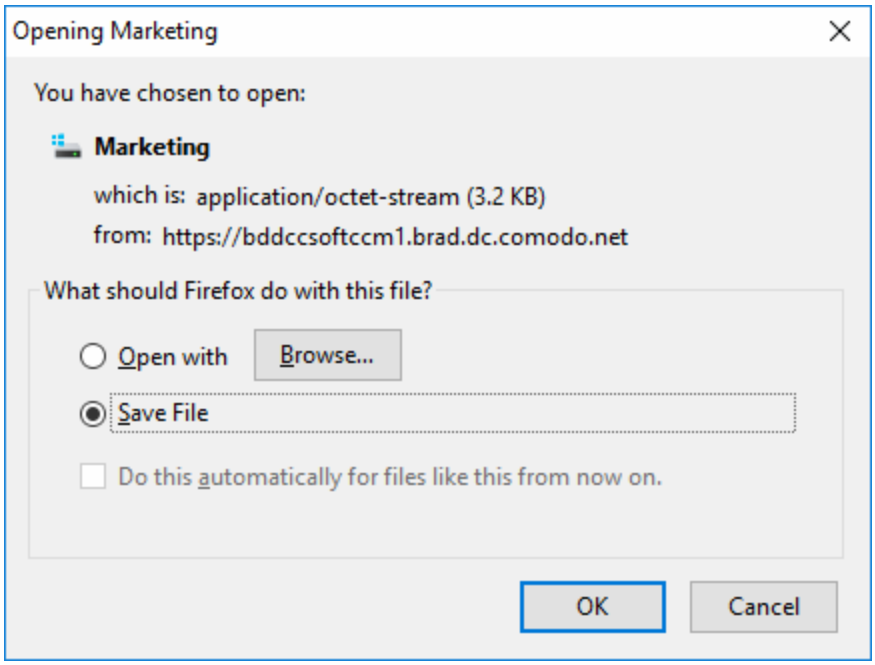
Common Name : CCMQA.COM

Term : 365 Days

Requested : 08/13/2019 13:52 GMT

Expires : 08/12/2020 23:59 GMT

Order Number : 2194588

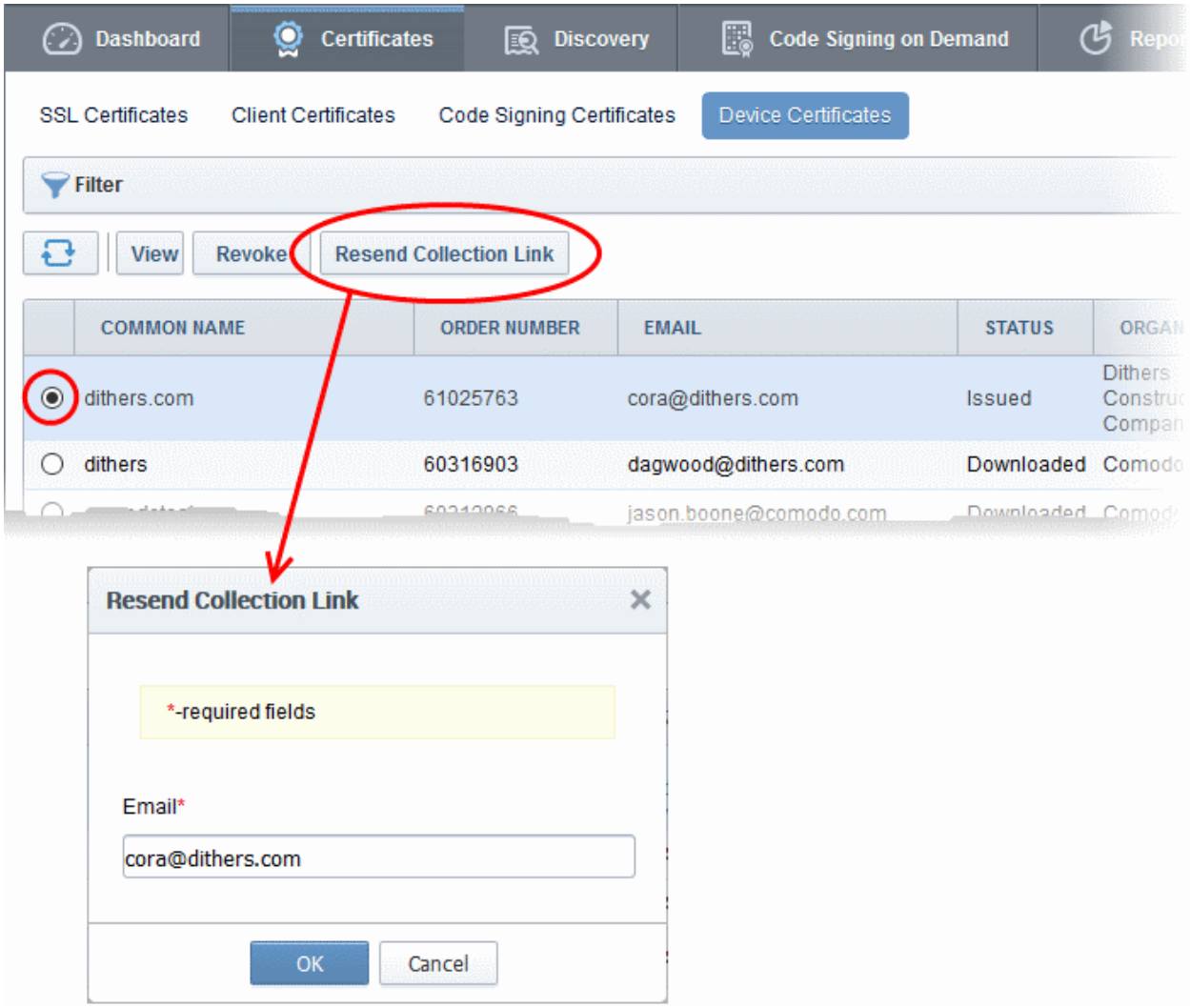


3.5.3.6 Resending the Device Certificate Collection Email

SCM automatically sends a collection email to applicants once a device certificate has been issued. However, if the certificate is not downloaded for a some time, then you may want to resend the mail. The resend dialog also allows you to change the recipient email address if the device has been registered to a different user.

You can resend the certificate collection email as follows:

- From the main UI, navigate to **Certificates > Device Certificates** and select the certificate with a status of Issued for which you want to resend the collection mail.
- Click **Resend Collection Link**, as shown in the following illustration, to open the **Resend Collection Link** dialog.

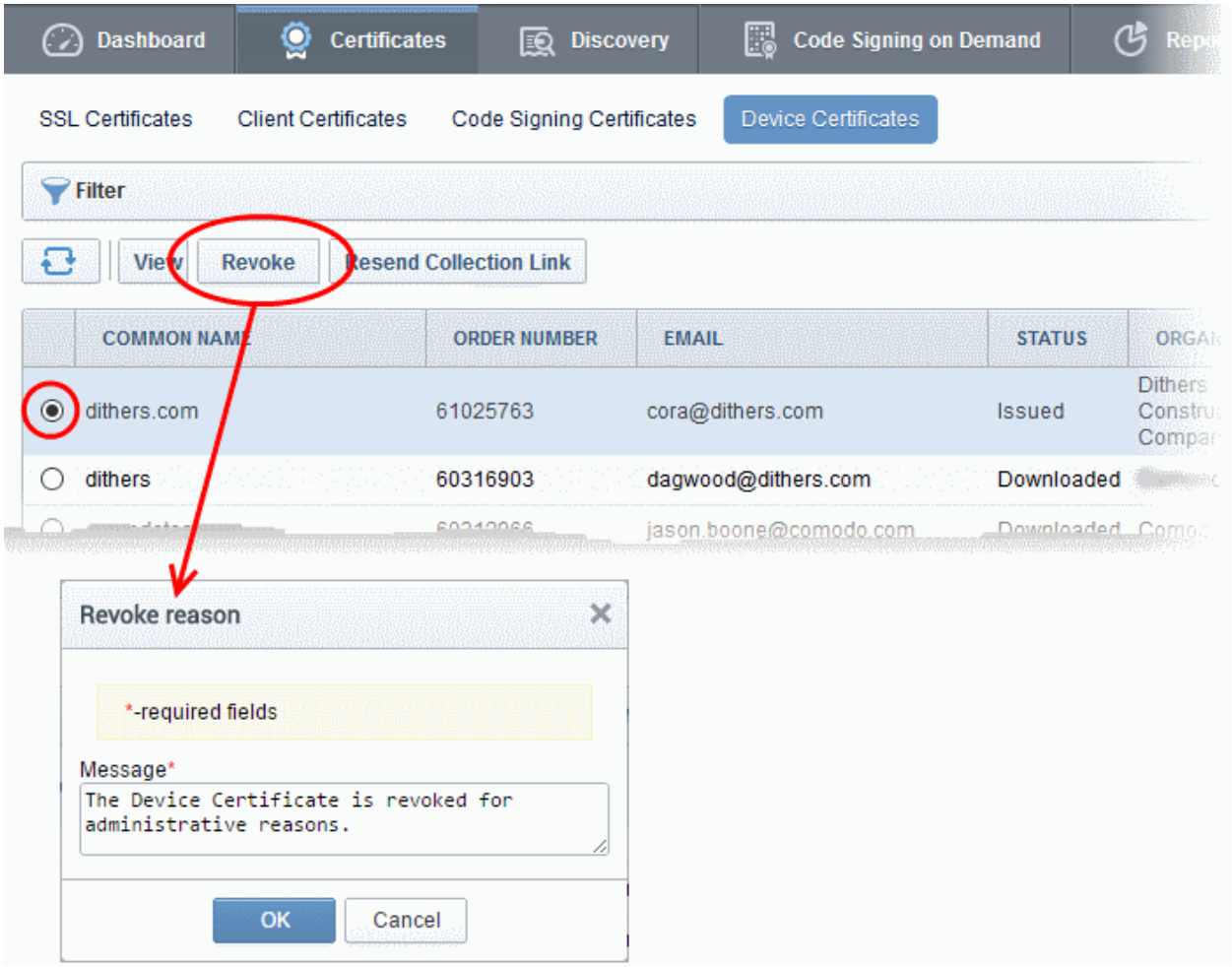


The recipient email address defaults to the address entered during certificate enrollment. If you want to send the mail to a different address, enter the new address in the **Email** field. The collection mail is sent to the specified address.

3.5.3.7 Revoking Device Certificates

The device certificate issued to end-users can be revoked by appropriate administrators any time before the certificate expiry date.

To revoke a device certificate, navigate to **Certificates > Device Certificates**, select the certificate from the list and click **Revoke**, as shown in the following illustration.



- Provide a reason for revocation and click **OK**.

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

4

Managing Code Signing Certificates Through CSoD

This chapter describes how to process and manage Code Signing on-Demand (CSoD) using SCM.

This chapter describes the following topics:

- Overview of the SCM Support for CSoD
- Configuring Automatic Approval of Code Signing Requests
- Adding End-Users with a Developer Role
- Obtaining a Certificate for CSoD
- Signing Code Using CSoD

4.1 Overview of the SCM Support for CSoD

CSoD offers fast, intuitive, and highly secure way to digitally sign software. SCM allows to sign the following file types:

- Windows executables:
  - `.exe`
  - `.dll`
  - `.ocx`
  - `.sys`
- Windows installation packages:
  - `.cab`
  - `.msi`
- Java packages:
  - `.jar`
  - `.war`
- Android application packages:
  - `.apk`
- PowerShell scripts:
  - `.ps1`
  - `.psm1`

SCM can also perform hash signing, whereby the end-users upload a hash of their files for signing instead of the actual files. The end-user then needs to embed the hash with their files.

CSoD is available in two deployment options:

- In-house hosted mode:
  - Developers upload software to a local portal. The code signing process is handled by a locally installed agent that generates CSoD-enabled code signing certificates for developers to sign files. The certificates and their private keys are stored in the encrypted form in a local database created by the agent.
  - HSM integration. You can also configure the agent to generate and store the code signing certificate on a local Hardware Security Module (HSM). Keys are generated in the PKCS # 11 format and saved in a non-extractable format on the HSM device. HSM integration is mandatory if you use the agent in cluster mode. All CSoD agents should be configured to connect to a single HSM.
- Cloud mode:
  - The signing service is hosted on Sectigo's secure cloud servers. The service generates CSoD-enabled code signing certificates for developers to sign files. The certificates and their private keys are generated and stored in encrypted format in Sectigo's data center for the lifetime of the certificate, tightly protected by Sectigo's military-grade security infrastructure.
  - HSM integration. Contact your account manager if you want to set up the HSM integration while using a cloud service mode.

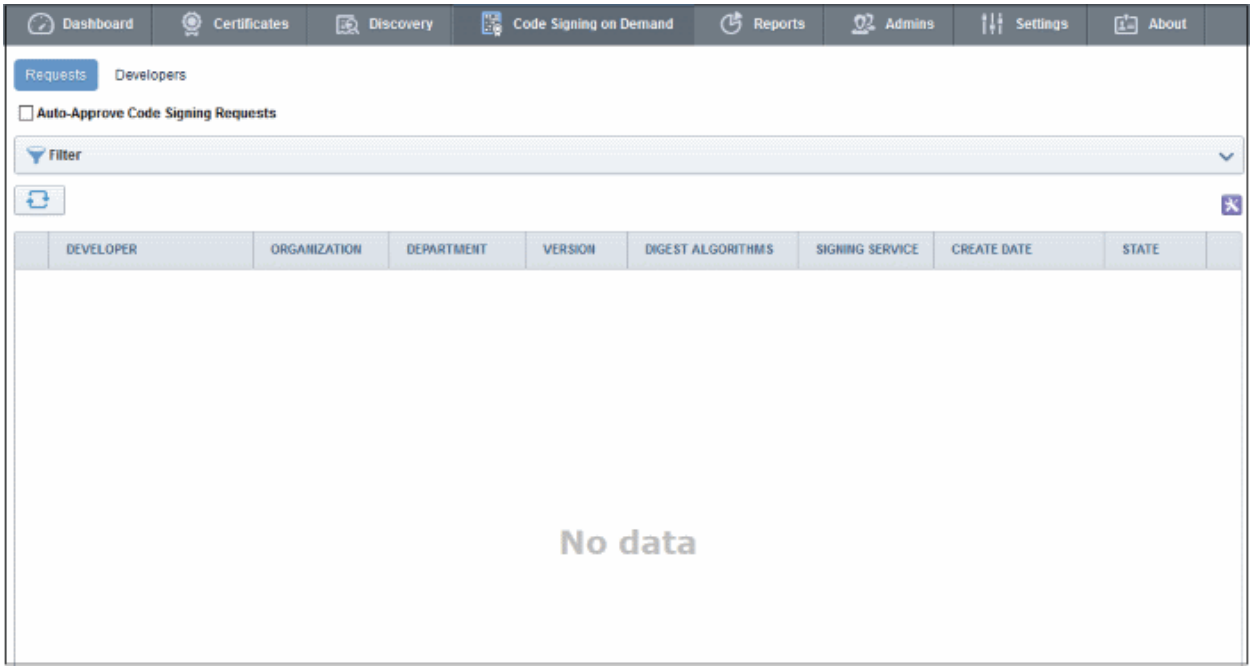
Both modes require you to create a new Developer role in SCM. The developer is responsible for uploading software and collecting the signed code after this is approved by the administrator.

The CSoD service in SCM is only available if enabled for your account. Contact your Sectigo account manager if you wish to add this service. If enabled, the visibility of the CSoD area is restricted to the following types of administrator roles:

- A MRAO can configure the agent, add developers, and manage code signing requests for any organization or department.
- A RAO Code Signing can add developers and manage code signing requests for organizations and departments that have been delegated to them.
- A DRAO Code Signing can add developers and manage code signing requests for departments that have been delegated to them.

Using the **Code Signing on Demand** area of the SCM UI shown in the following illustration, you can sign requests, as well as manage end-users granted a Developer role. This area is divided into two main sections:

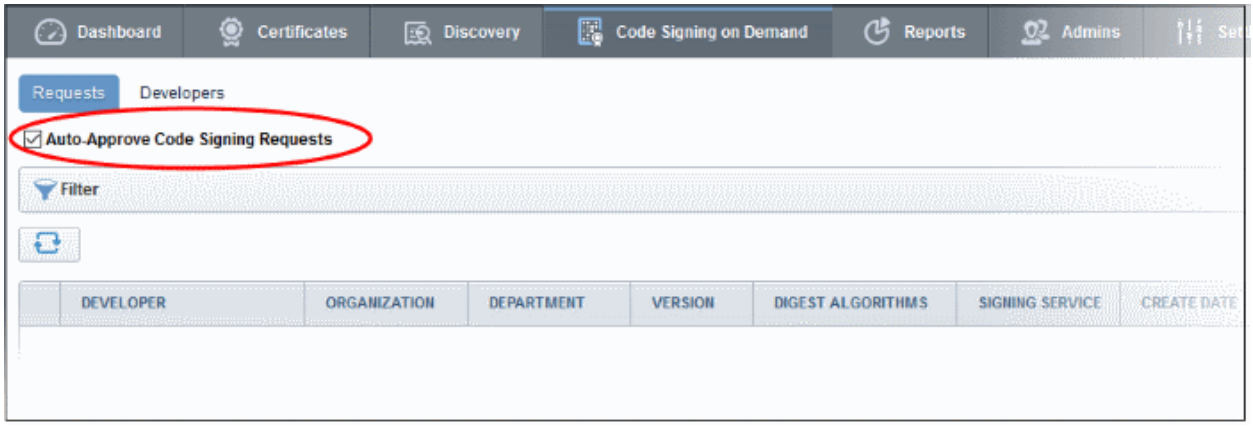
- The **Requests** screen allows you to view, approve, and decline code signing requests from developers.
- The **Developers** screen allows you to add and manage Developer accounts in SCM.



4.2 Configuring Automatic Approval of Code Signing Requests

Before the agent signs a file, the code signing request needs to be approved either manually (default) or automatically, in which case the agent signs as soon as the files are uploaded by the end-user.

You enable automatic signing of requests from the **Code Signing on Demand** area of the SCM UI and selecting **Auto-Approve Code Signing Requests**, as shown in the following illustration.



4.3 Adding End-Users with a Developer Role

A Developer role in SCM provides permissions to perform the following:

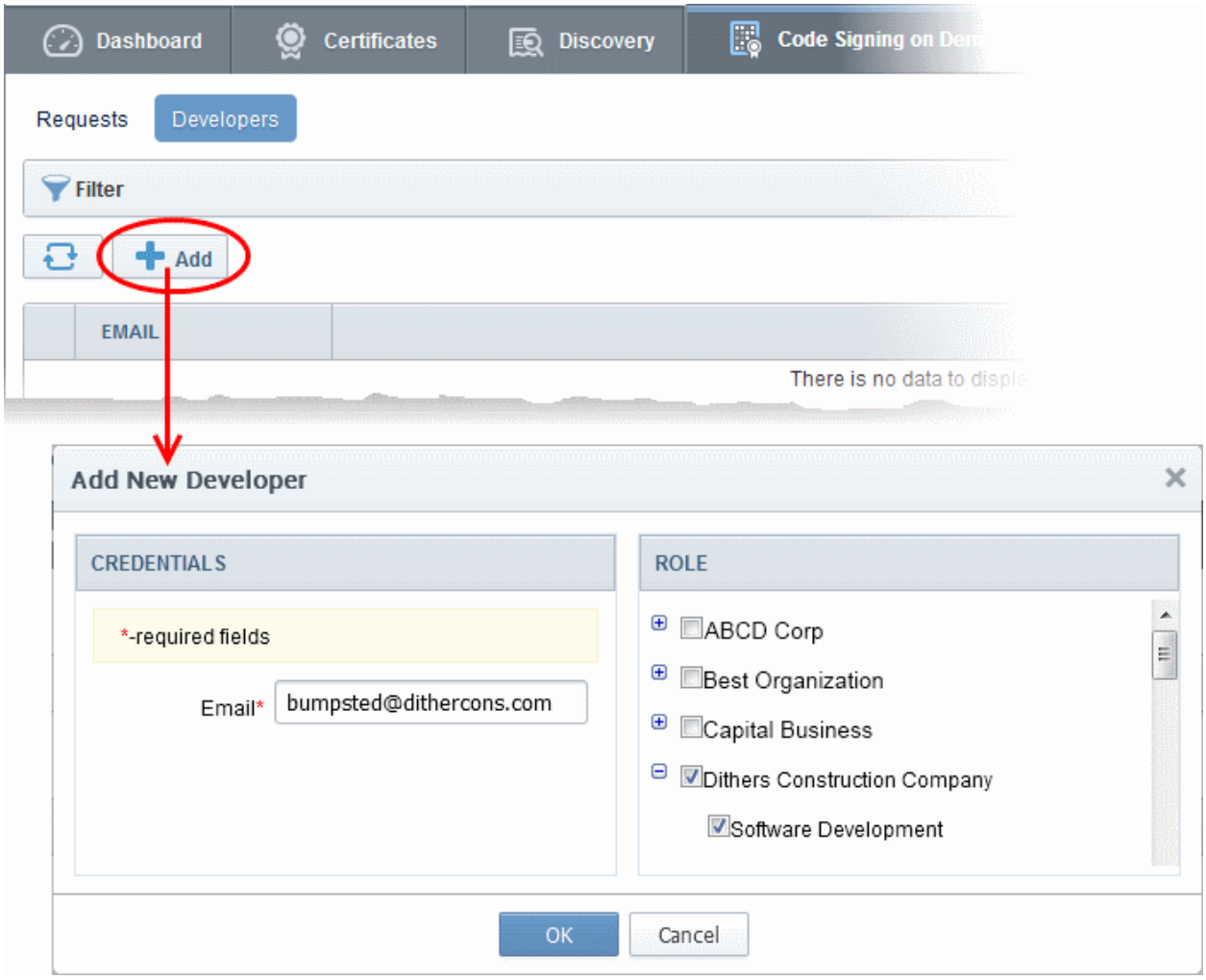
- Login to the CSoD service.

- Upload files or hashes for code signing.
- Download the signed file or signed hash.

You can create a developer as a new user, or add developer privileges to an existing SCM user. A MRAO or RAO needs to approve the developer's actual signing requests, unless you enable auto-approve in the CSoD configuration screen.

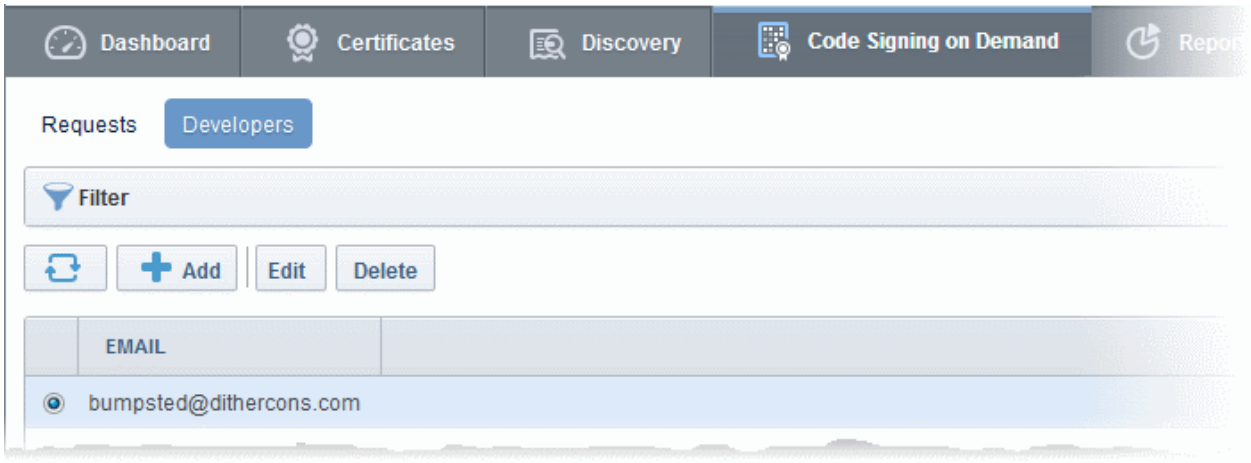
You add a Developer as follows:

- From the main UI, navigate to **Code Signing on Demand > Developers** and click **Add** to open the **Add New Developer** dialog shown in the following illustration.

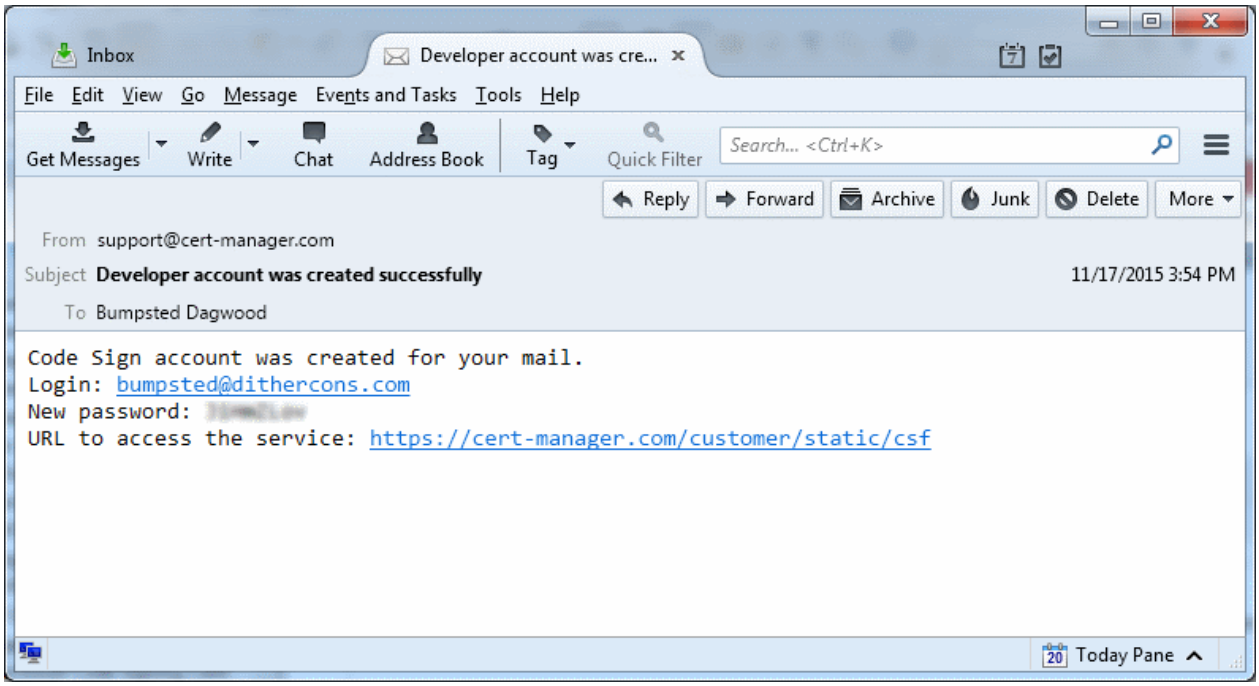


- Use the **Email** field located in the **CREDENTIALS** panel to enter the email address of the end-user to whom the Developer role is being granted.
- Use the **ROLE** panel to select organizations and departments to which the developer is to belong, and then click **OK**.

Upon completion, the end-user is added to the list, as shown in the following illustration.



A notification email similar to the one shown in the following illustration is sent to the end-user containing their credentials to access the CSoD service.



You can edit the end-user to modify their assigned organizations and departments, reset their password, or remove them.

4.4 Obtaining a Certificate for CSoD

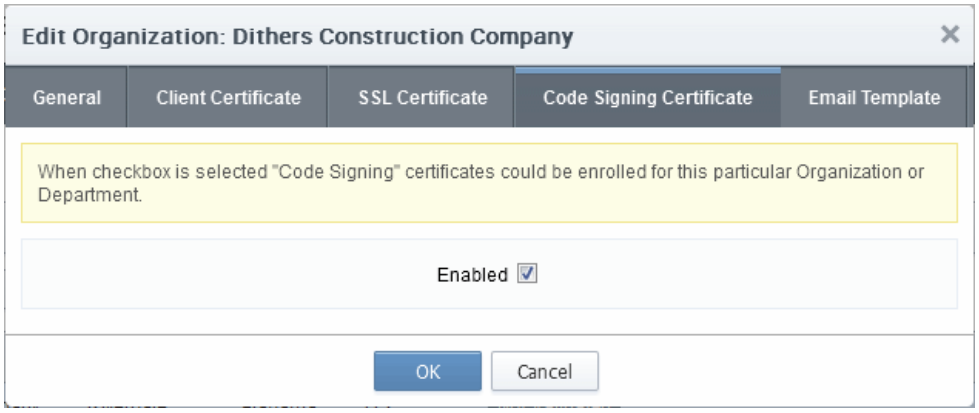
The following requirements must be met prior to issuing code signing certificates:

- You created a Developer role for the end-user, as described in "Adding End-Users with a Developer Role" on page 202.

- The domain from which the certificate is to be issued has been enabled for code signing certificates, and has been activated for your account by your account manager.

  For example, if you wish to issue code signing certificates to end-user@mycompany.com, then mycompany.com must have been validated by Sectigo.

  All certificate requests made on validated domains or sub-domains are issued automatically. Certificate requests for new domains first have to undergo validation.
- The domain has been delegated to an organization or department. For more information, see "How to Create a New Organization" on page 331 and "How to Modify an Existing Organization" on page 360.
- A RAO Code Signing or DRAO Code Signing has been delegated control of the organization or department.
- You enabled code signing certificates for the organization in the **Code Signing** area of the organization's settings, as shown in the following illustration. To access this settings, you need to edit the organization.



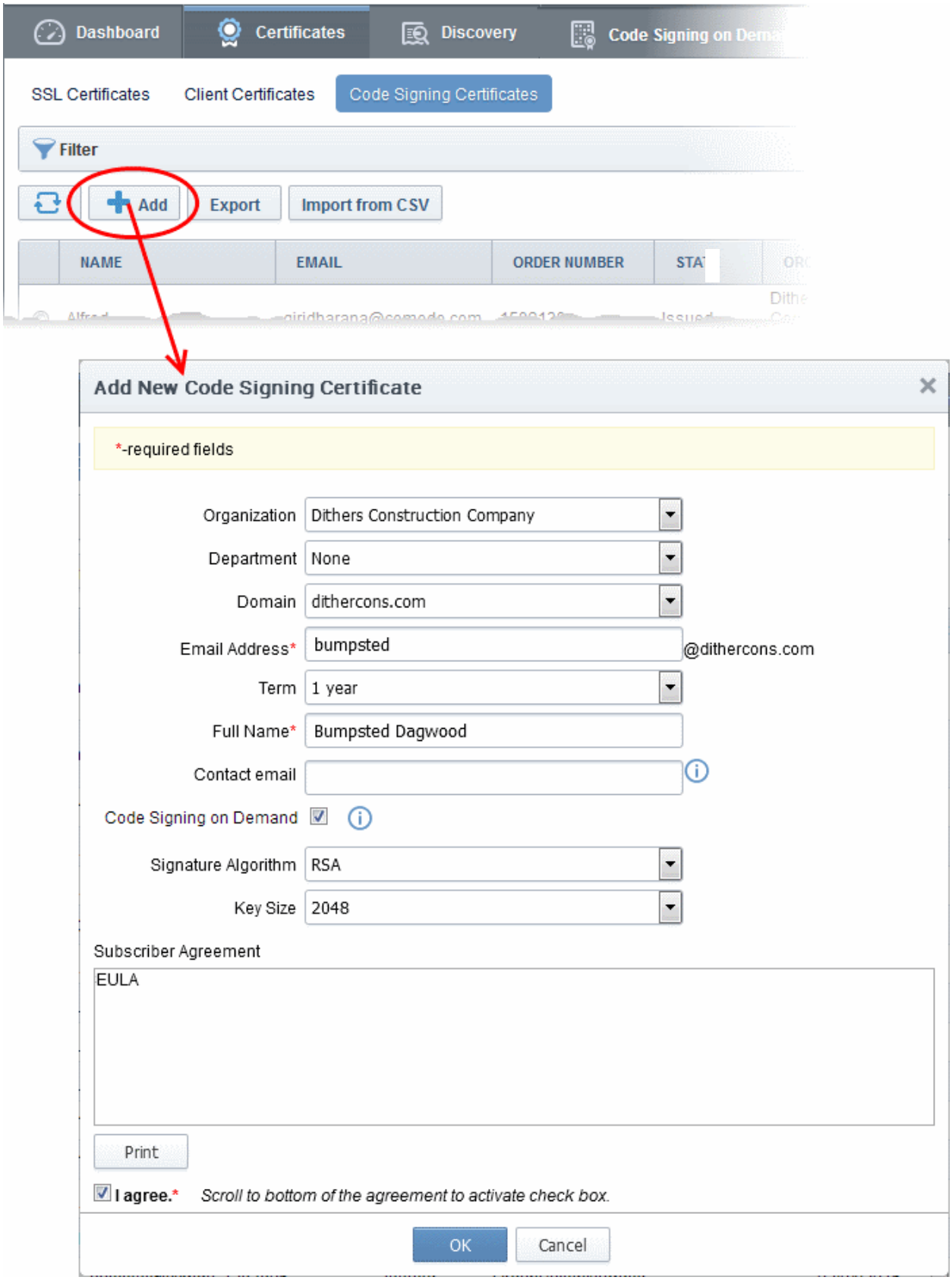
- If deploying via the hosted mode, the CSoD Agent needs to be installed on the local network and connected to SCM.
- If deploying via the cloud mode and the agents are installed on multiple computers, then they must be configured to generate and store keys on a HSM appliance. If you install the agent on a single computer, then it is optional to use a HSM appliance to generate and store keys.

Upon fulfillment of the preceding requirements, you can add a new code signing certificate for the end-user (Developer). Depending on the deployment mode, the following typically occurs:

- In the hosted mode, the CSoD agent generates and stores the key pair locally and submits the CSR to Sectigo. Once the certificate is issued, the CSoD agent automatically downloads the certificate and stores it on your local network. If a HSM appliance is used, the key pair is generated and stored on the HSM. Upon issuance of the certificate, the agent downloads the certificate and stores it on the HSM appliance.
- In the cloud mode, the CSoD cloud service generates and stores the key pair and submits the CSR to Sectigo. Once the certificate is issued, the service collects the certificate and stores it in the Sectigo data center. If the HSM service is used, the key pair is generated and stored on the HSM. Upon issuance of the certificate, the service collects the certificate and stores it on the HSM.

You enroll a code signing certificate for the end-user as follows:

- From the main UI, navigate to **Certificates > Code Signing Certificates** and click **Add** to open the **Add New Code Signing Certificate** application form shown in the following illustration.
- Complete all the required fields on the form, ensuring the following:
  - The correct end-user email address is used.
  - The correct organization and department are specified for the end-user.
  - The **Code Signing on Demand** is enabled.


Dashboard
Certificates
Discovery
Code Signing on Dema
SSL Certificates
Client Certificates
Code Signing Certificates
Filter
Add
Export
Import from CSV
NAME
EMAIL
ORDER NUMBER
STA
Add New Code Signing Certificate
*-required fields
Organization
Dithers Construction Company
Department
None
Domain
dithercons.com
Email Address*
bumpsted
@dithercons.com
Term
1 year
Full Name*
Bumpsted Dagwood
Contact email
Code Signing on Demand
Signature Algorithm
RSA
Key Size
2048
Subscriber Agreement
EULA
Print
I agree.*
Scroll to bottom of the agreement to activate check box.
OK
Cancel

The following table provides descriptions of the form fields and elements. The mandatory fields are marked with the red asterisk on the form.

Field	Description
Organization	The organization to which the developer belongs.
Department	The department to which the developer belongs.
Domain	The domain to which you want to issue the certificate. This is a domain that is assigned to the organization or department.
Term	The validity period of the certificate.
Email Address	The email address of the applicant.
Full Name	The full name of the applicant.
Contact Email	The contact email address of the applicant that should be included in the certificate. It may be the customer facing email address.
Code Signing on Demand	Indicates whether or not the certificate is to be used by the CSoD service.
Signature Algorithm	The signature algorithm to be used by the certificate. Recommended = 2048 bit or higher.
Key Size	The key size (in bits) by the certificate.
Subscriber Agreement	The EULA for the certificate.

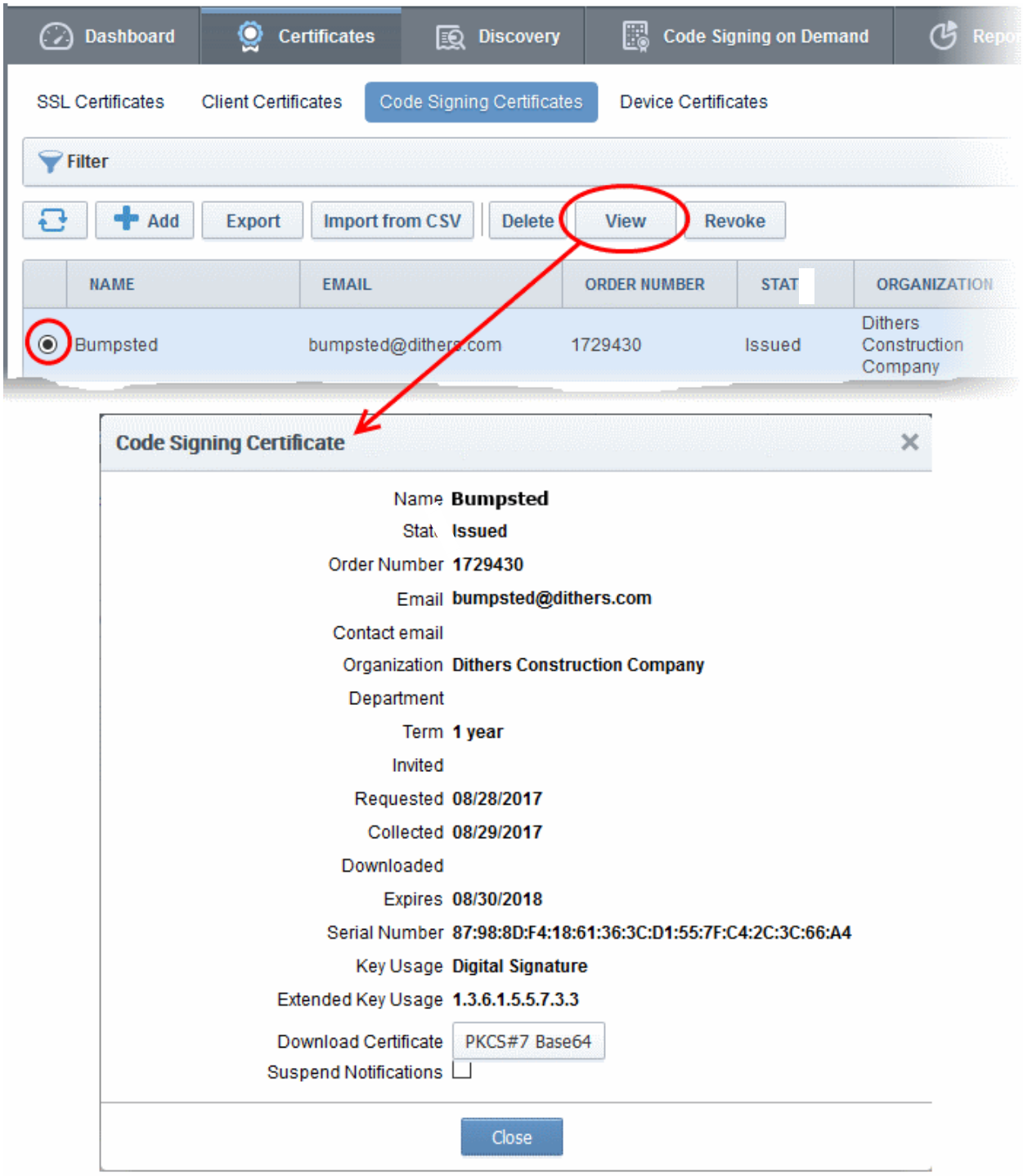
Upon completion, the certificate is added with the status of Init, indicating that the certificate enrollment has been initiated.

Once issued, the status of the certificate changes to Issued.

The certificate can now be used to sign code submitted by the end-user. Each signing action needs to be approved by you unless you enable the automatic approval.

To view and the certificate, select it and click **View**, as shown in the following illustration.

To download the certificated in the PKCS#7 format, click **Download Certificate**.



4.5 Signing Code Using CSoD

Once you have created the end-user with a Developer role and obtained at least one CSoD-enabled code signing certificate, your end-user can upload files or hashes for signing. For information on the supported file types, see "Overview of the SCM Support for CSoD" on page 200.

For hash signing, end-users can upload a text file containing the SHA or MD5 hash value of their software which is to be signed with their code signing certificate. The end-users can embed the signed hash and certificate with their binary, which is useful if (1) the source files are large and the developer wishes to avoid longer upload times; (2) the company policy allows code signing of binaries to be performed only within a local system. For more information, see "Obtaining a Certificate for CSoD" on page 204.

NOTE: The hash signing is only available if enabled for your account. Contact your Sectigo account manager if you wish to add this service.

The following table provides a summary of the two deployment modes.

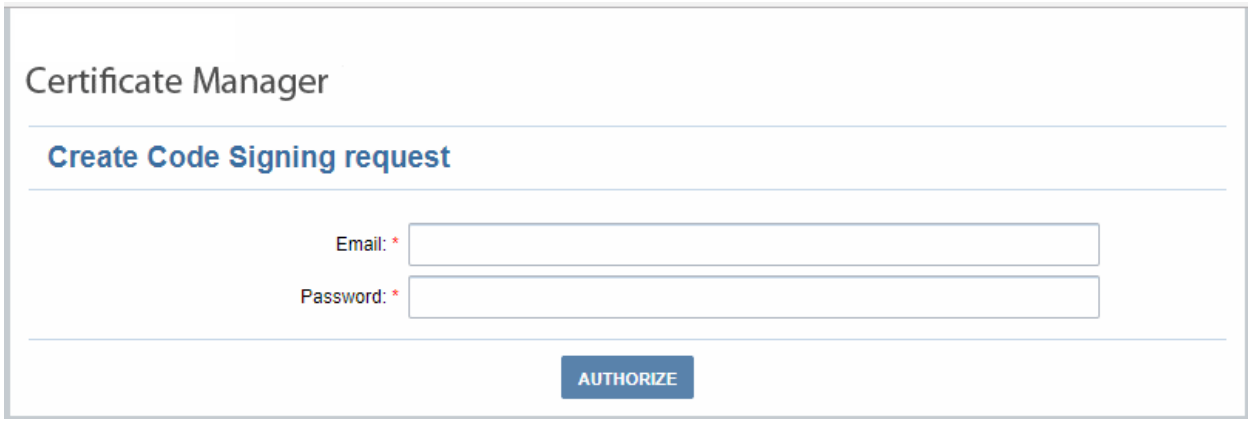
In-House Hosted Mode	Cloud Service Mode
The CSoD service is enabled in hosted mode for your account. The CSoD Agent is installed on your network and connected to SCM. Developer accounts have been created and issued with a CSoD code signing certificate.	The CSoD service is enabled in cloud mode for your account. Developer accounts have been created and issued with a CSoD code signing certificate.

The code signing procedure includes the following:

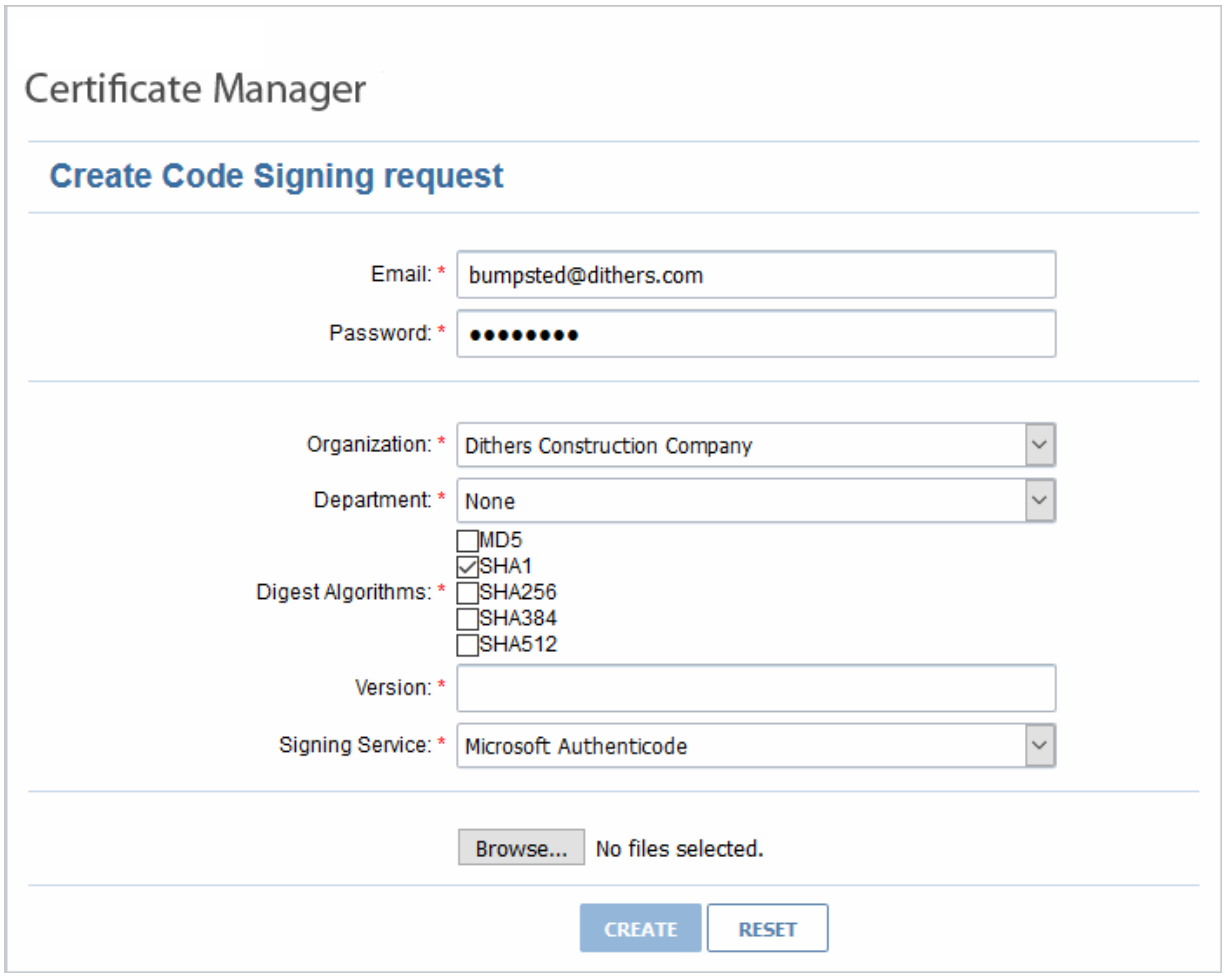
1. Uploading files for signing: The developer logs into the CSoD service portal, enters the details of the files to be signed, selects the signing service, and uploads their code or hash. This creates a request which can be viewed via the **Code Signing on Demand > Requests** UI. For more information, see How to Upload Files for Signing.
2. Approving a code signing request (optional if the automatic approval is enabled): You view the request, check the files to be signed, and approve the request from the **Code Signing on Demand > Requests** UI. For more information, see How to Approve a Code Signing Request.
3. Downloading code-signed files: After the signing process is complete, the status of the request changes to Signed, and a notification mail is sent to the developer with a URL to download the signed files. For more information, see How to Download Code Signed Files.

4.5.1 How to Upload Files for Signing

Once an end-user with a Developer role has been added, they can login to SCM using the link in their confirmation email and entering the user credentials into the **Create Code Signing Request** dialog shown in the following illustration. By default, the format of this URL is `https://cert-manager.com/customer/<customer_uri>/csod`.



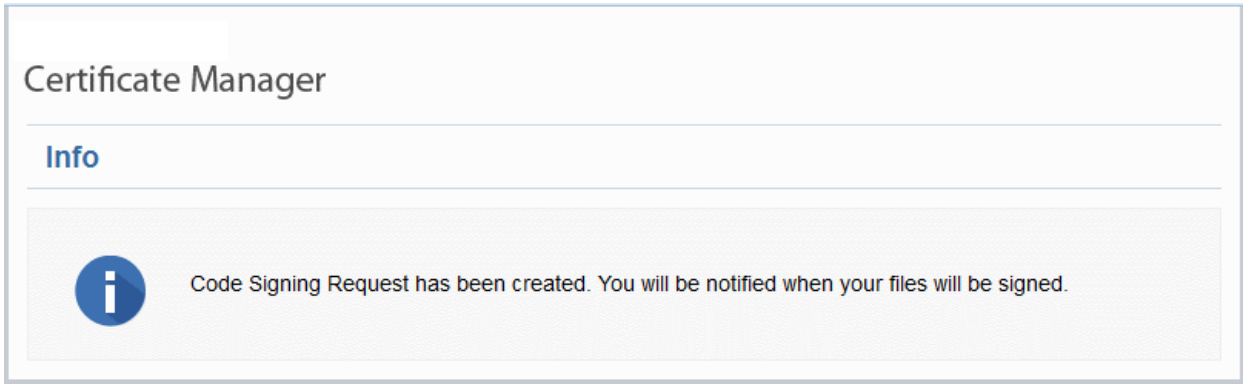
The end-users can then upload files using the form shown in the following illustration.



- **Organization**—The organization to which the end-user belongs. The organization selected here is shown in the certificate as the publisher of the software.
- **Department**—The department to which the end-user belongs, if applicable.

- **Digest Algorithm**—The algorithm to use to create the file hash code (also knows as digest). The hash-code is used by client software to verify the integrity of the signed code. Recommended = SHA256 and upwards.
- **Version**—The version number of the software to be signed.
- **Signing Service**—The appropriate signing service for the type of file to sign, as follows:
  - **Files**—Either one of Microsoft Authenticode, Java, or Android as the signing service.
  - Hash values—Hash signing as the signing service. Must generate a hash code of the file with the SHA or MD5 algorithm to generate a `.sha` or `.md5` file respectively. Alternatively, it can be a `.txt` file containing the hash value.
- **Browse**—Allows to select one or more file or hash to upload for signing.
- **Create**—Submits the signing request to the CSoD service.

Upon completion, a confirmation dialog shown in the following illustration is displayed.



The code signing request is visible via **Code Signing on Demand > Requests**.

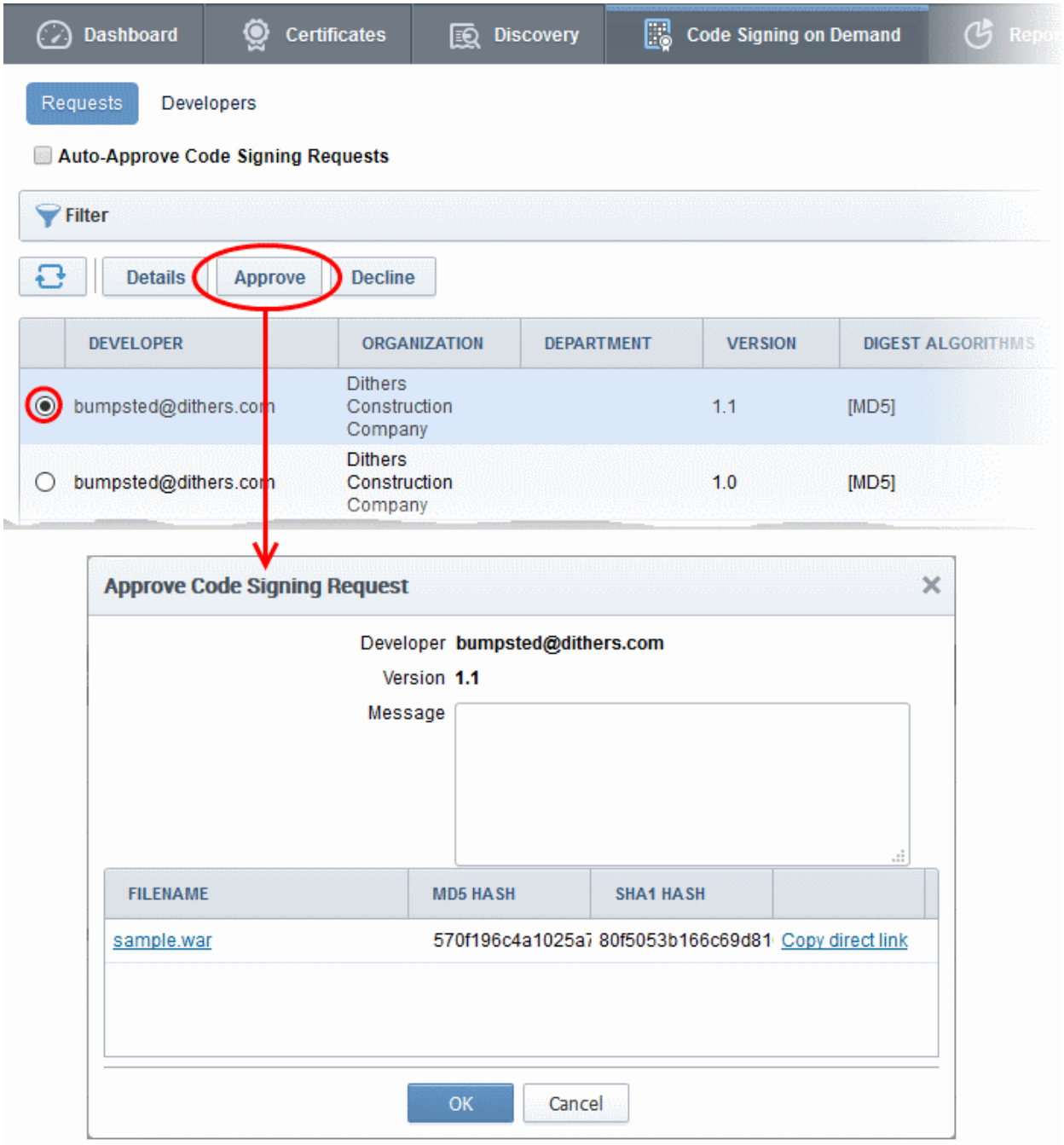
4.5.2 How to Approve a Code Signing Request

After the end-user has uploaded files for signing, the code signing request appears in the **Code Signing on Demand > Requests** areas of the SCM UI shown in the following illustration. By default, you need to review and approve the request before the service signs the files.

You can view the request details by clicking **Details**, as shown in the following illustration.

The details dialog shows the end-user name, file details, and the MD5 and SHA1 hash values of the files. To download and view the file, click its name.

To proceed with signing, you select the request and click **Approve**, as shown in the following illustration.



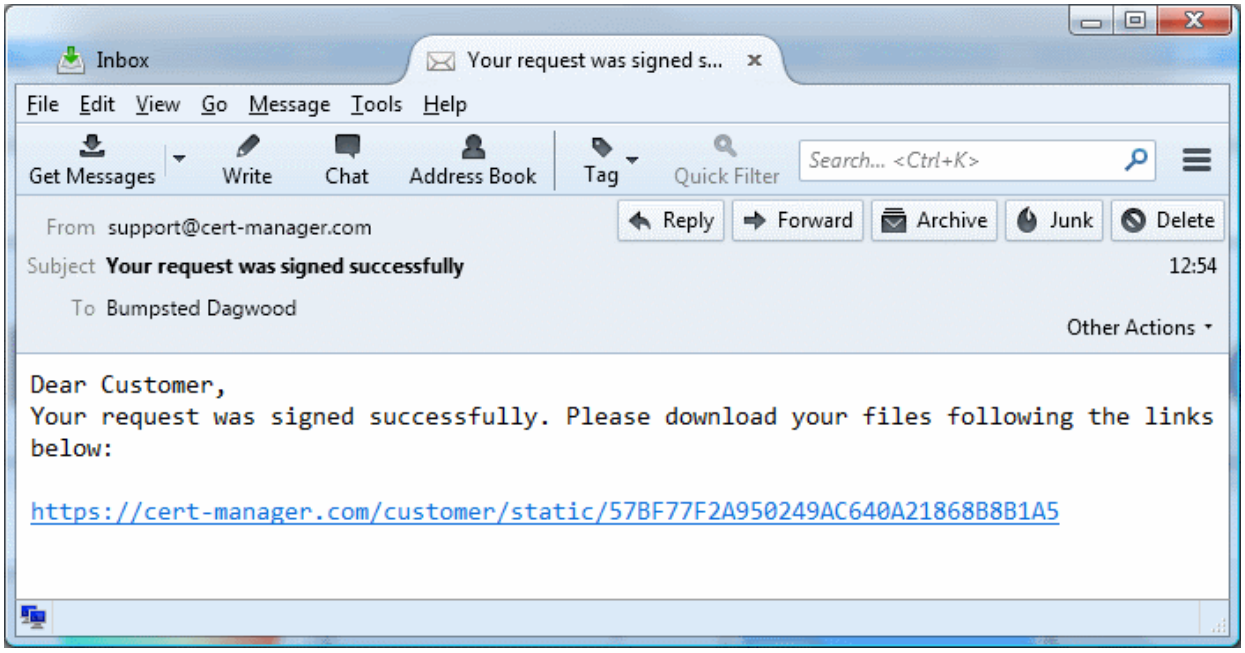
When you enter an approval message and click **OK**, the request is approved and its status changes to In Progress.

Once the signing process is complete, the request status changes to Signed and a notification mail is sent to the end-user to download the signed file. The end-user must download the signed files within three days of the notification. After three days, the files are removed from the database.

If required, you can resend the email by clicking **Resend Signed Notification**.

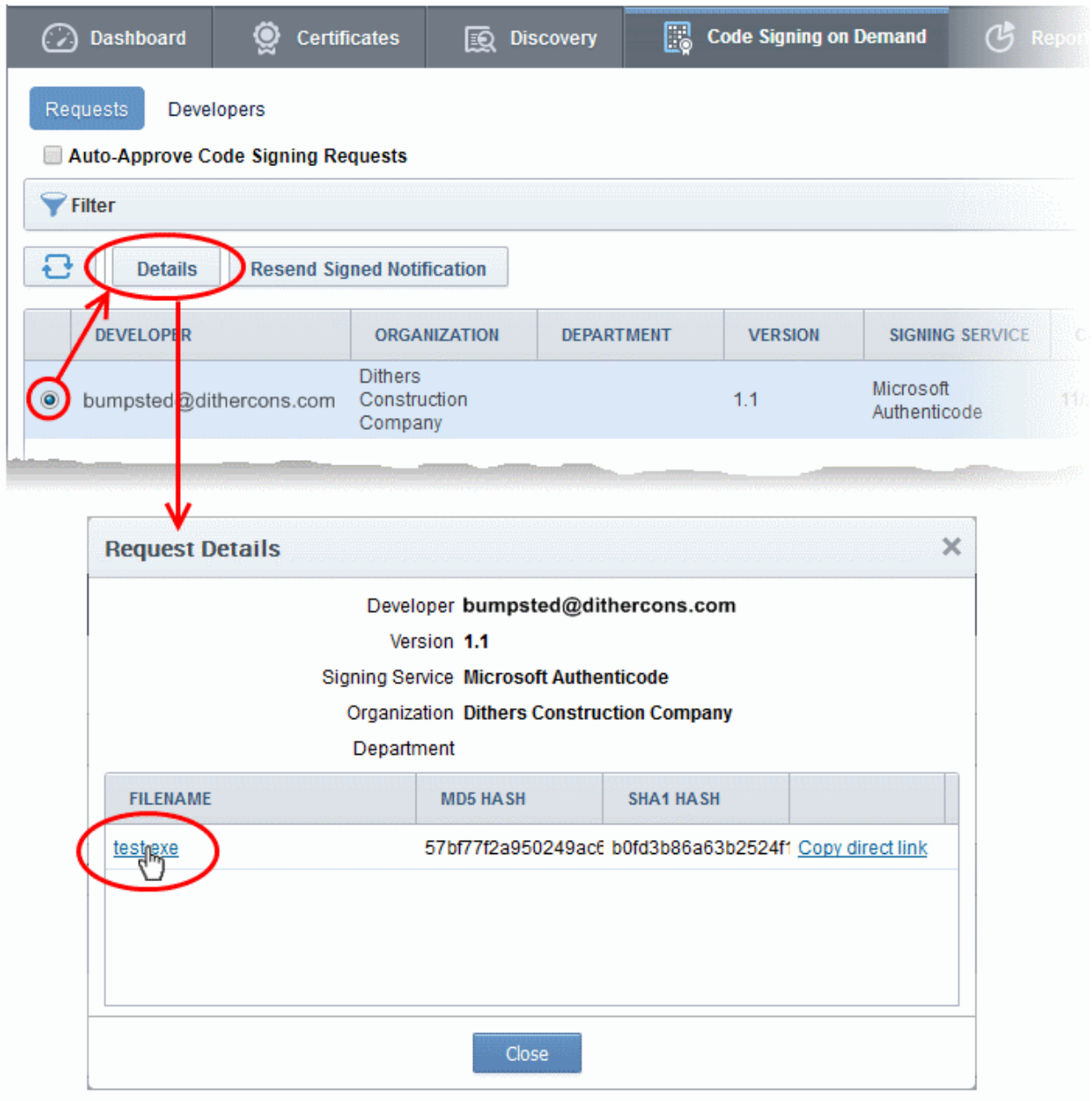
4.5.3 How to Download Code Signed Files

After completing the signing process, the end-user receives an email similar to the one shown in the following illustration with links to download each signed file.



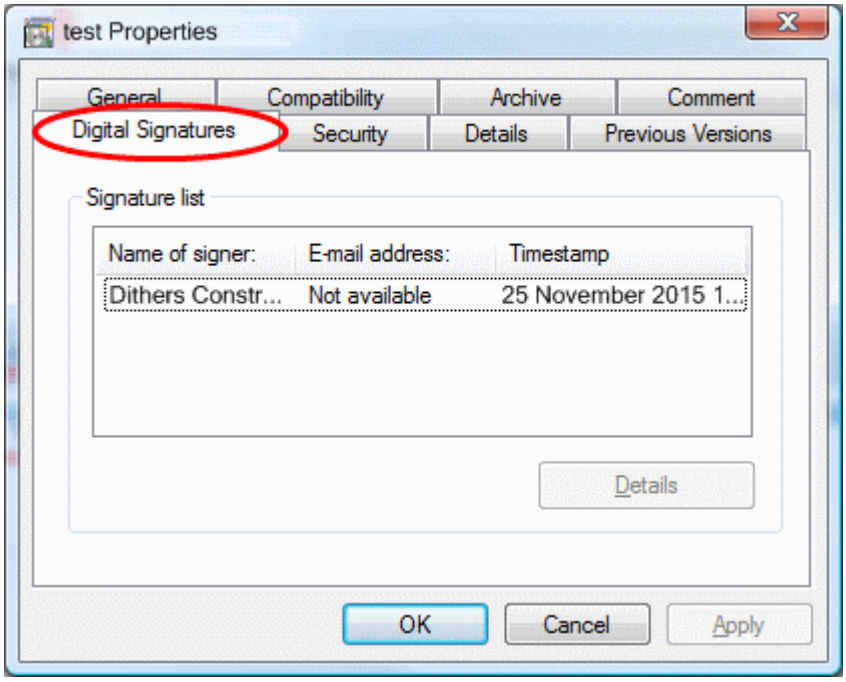
If a hash was uploaded, the end-user can download the signed hash and embed it into the binary to create a digitally signed file. The end-user must download the signed files within three days of the notification. After three days, the files are removed from the database.

You can view the request and download signed files details by clicking **Details**, as shown in the following illustration.



The signed file can be downloaded by clicking its name in the **Request Details** dialog shown in the preceding illustration.

To check whether or not the file is signed and see the details of the signer, right-click the file, select **Properties > Digital Certificates**, as shown in the following illustration.


test Properties
General
Compatibility
Archive
Comment
Digital Signatures
Security
Details
Previous Versions
Signature list
Name of signer:
E-mail address:
Timestamp
Dithers Constr...
Not available
25 November 2015 1...
Details
OK
Cancel
Apply

5

Managing Administrators

This chapter describes the SCM administrator roles, such as MRAO, RAO, and DRAO, and how to create and manage new and existing administrators.

This chapter describes the following topics:

- Understanding the SCM Administrator Roles
- Understanding Administrator Management
- Sorting and Filtering Administrators
- Adding Administrators
- Editing and Deleting Administrators
- Creating IdP User Account Templates

5.1 Understanding the SCM Administrator Roles

The primary administrator privileges and restrictions are divided as follows:

- The MRAO Role
- The RAO Role
- The DRAO Role

5.1.1 The MRAO Role

The following privileges and restrictions apply to the MRAO role:

- MRAOs have full visibility of and control over the provisioning and lifecycle management of all certificate types.
- New MRAOs can only be created and managed by an existing MRAO.
- MRAOs are visible only to other MRAOs in the **Admins** area of the SCM UI.
- MRAOs can create new organizations and departments, and well as delegate them to RAOs and DRAOs respectively.
- MRAOs can initiate the process of validating organizations for the purpose of requesting and issuance of Organization Validated (OV) SSL certificates to organizations and departments administered by this particular MRAO.
- MRAOs can create and manage RAOs and DRAOs for any organization or department.
- MRAOs have full access and executive rights to add, modify, and delegate domains of any organization or department.
- MRAOs can initiate Domain Control Validation (DCV) process on any domain added to any organization or department.
- MRAOs can view any type of report for any organization or department.

- MRAOs can set up one or more Network Agents on a local network for any department or organization. A Network Agent can:
  - allow administrators to scan internal hosts for installed SSL certificates, which can then be tracked using the SCM administrator console;
  - facilitate the automatic installation of SSL certificates on Apache, Apache Tomcat, and IIS web servers.
- MRAOs can set up a Private Key Store (PKS) on their local network to store and manage the private keys of certificates managed by SCM. The PKS requires an agent installed on a local server. The agent is then responsible for handling commands to store private keys and for generating CSRs for certificates created using the CSR generation feature.
- MRAOs can enable RAO Client Certificate and DRAO Client Certificate types of administrator with the ability to recover the private keys of client certificates for those organizations or departments that they administer.
- MRAOs can recover from escrow the private keys of client certificates that belong to any organization or department with key recovery (escrow) enabled on them (if enabled).
- MRAOs can view activity logs of all organizations and departments.
- MRAOs are the only administrators with sufficient privileges to manage SSL types and client certificate types of certificates.
- MRAOs can add custom fields in the built-in application and self-enrollment forms for SSL and client certificates requisition.
- MRAOs can request their account manager to add client certificates with specific capabilities to their account.

  For example, Signing Only, Encryption Only, Dual Use (signing + encryption), Smart Card Logon, and Authentication, among others.

  It is also possible to create custom certificate types with combinations of capabilities.

  MRAOs can restrict specific types of client certificate on a per-organization basis.
- MRAOs can set up and configure the Code Signing on Demand (CSoD) service. In addition, if CSoD service is enabled for the account, MRAOs can create developers and approve code signing requests generated by developers for all organizations and departments.
- MRAOs can integrate Active Directory (AD) servers belonging to any organization or department by installing a Microsoft (MS) Agent.
- MRAOs can issue a self-signed certificate with MS Certificate Authority (CA).
- MRAOs can view network assets, such as certificates, installed on various endpoints as identified by manual or scheduled discovery scans.
- MRAOs can view AD objects and certificates installed on these ADs which were identified by scans run by the MS Agent.
- MRAOs can map MS AD certificate templates from an AD server to private CA certificate types in SCM, enabling SCM to issue private certificates with custom parameters such as key usage, extended key usages, key sizes, validity period, and so on.
- MRAOs can assign external (also known as unmanaged) certificates identified by discovery or AD server scans to organizations and departments, and then bring them under the SCM management.
- MRAOs can approve device certificate requests from MS Agents (installed on AD servers with the Active Directory Certificate Services (AD CS) or Network Device Enrollment Service (NDES) role) or requested directly from devices via the Simple Certificate Enrollment Protocol (SCEP).
- MRAOs can enroll for device certificates from the MS CA through the AD.

- MRAOs can enable organizations and departments for enrollment of device certificates via SCEP.
- MRAOs can create and manage ACME accounts for organizations and departments (if enabled).

5.1.2 The RAO Role

Depending on the certificate type a specific RAO is responsible for managing, the RAO role is divided into the following subroles:

- RAO SSL
- RAO Client Certificate
- RAO Code Signing
- RAO Device Certificate

The privileges of a RAO are defined by the organization and, optionally, departments delegated to this RAO.

5.1.2.1 RAO SSL

RAOs SSL can request and manage SSL certificates for domains that have been delegated to their organizations. Specifically, the RAO SSL role provides the following privileges and limitations:

- RAOs SSL can view and control SSL certificates that belong to their delegated organization.
- RAOs SSL can approve or decline requests for SSL certificates made using the self-enrollment form for their organizations and departments.
- RAOs SSL cannot manage SSL certificates belonging to organizations for which these RAOs SSL have not been granted permissions.
- RAOs SSL can manage SSL certificates but not other certificate types such as, for example, client certificates, code signing certificates, or device certificates. This limitation is applicable to the certificates belonging to the organization for which this RAO SSL is the SSL administrator.
- RAOs SSL can only manage organizations that have been delegated to them in the **Organizations** area of the SCM UI.
- RAOs SSL can upload private keys of SSL certificates belonging to their organizations and their subordinate departments for management by the PKS, configured in the local network. RAOs SSL can also download the private keys of the certificates.
- A MRAO can make the same individual a RAO Client Certificate, RAO SSL, and RAO Code Signing for the same organization during the administrator creation or editing process. For more information, see "The MRAO Role" on page 218.
- RAOs SSL cannot create new organizations, neither can they edit the **General** settings of any organization in the SCM UI, even those organizations of which they are SSL certificate administrator.
- RAOs SSL can create departments only within organizations that have been delegated to these administrators.
- RAOs SSL cannot approve or request the creation of administrators that have more privileges than themselves. They can, however, request the creation of fellow RAOs SSL only for organizations that have been delegated to them if a MRAO has enabled this feature for them. In addition, they can request and approve the creation of DRAOs SSL.
- RAOs SSL cannot request or approve the creation of any type of administrator for organizations that have not been delegated to these RAOs SSL.

- RAOs SSL cannot request or approve creation of administrators of any other certificate type, even for organizations that have been delegated to these RAOs SSL.
- RAOs SSL can delegate domains to subordinate departments of organizations that they administer.
- RAOs SSL can initiate DCV process for the domains delegated to subordinate departments of organizations that they administer if they have been given **Allow DCV** privileges. Note that a RAO SSL with **Allow DCV** privileges can be created only by a MRAO.
- RAOs SSL can set up Network Agents in a local network for scanning internal hosts with internally facing IP addresses for installed SSL certificates for organizations that are delegated to them and any subordinate departments . Network Agents also facilitate the automatic installation of SSL certificates on Apache, Apache Tomcat, and IIS web servers.
- RAOs SSL can view the network assets, such as certificates installed on various servers, endpoints, and web servers with websites and domains hosted on them, as identified by manual or scheduled discovery scans configured for the networks belonging to their organizations and their subordinate departments.
- RAOs SSL can assign external SSL certificates identified by discovery scans and AD server scans to their organizations and departments, in order to bring them under management through SCM.
- RAOs SSL can view the SSL certificate reports and discovery scan report for the organizations to which they have been assigned rights. For more information, see "Generating Reports" on page 575.
- RAOs SSL cannot access or manage the **Encryption** settings via SCM, as this area of the UI can only be managed by RAOs Client Certificate.
- RAOs SSL can only view activity logs for their organizations
- RAOs SSL can create and manage ACME accounts for organizations and departments delegated to them (if enabled).

5.1.2.2 RAO Client Certificate

RAOs Client Certificate can access, manage, request, and approve the requests of client certificates for domains that have been delegated to these RAOs Client Certificate organizations. Specifically, the RAO Client Certificate role provides the following privileges and limitations:

- RAOs Client Certificate can view and control client certificates which belong to organizations under these RAOs' delegation. RAOs Client Certificate do not have permissions over the client certificates of organizations which they do not control.
- RAOs Client Certificate can only manage client certificates and cannot manage other certificate types, such as SSL certificates, code signing certificates, or device certificates. This limitation is applicable to the certificates belonging to the organization of which they are RAOs Client Certificate.
- A MRAO can make the same individual a RAO Client Certificate, RAO SSL, RAO Code Signing, and RAO Device Certificate for the same organization during the administrator creation or editing process. For more information, see "The MRAO Role" on page 218.
- RAOs Client Certificate can only see those organizations that have been delegated to them in the **Organizations** area of the SCM UI.
- RAOs Client Certificate cannot create new organizations, nor can they edit the **General** settings of any organization via SCM. This limitation is applicable even to those organizations of which they are RAOs Client Certificate.
- RAOs Client Certificate can request their MRAO to add client certificates with specific capabilities to their account. If the certificates are not available on the account, then the MRAO can request Sectigo to have these certificates added, including such certificates as Signing Only, Encryption Only, Dual Use (signing + encryption), Smart Card Logon and Authentication and so on. It is also possible to create custom client certificate types with

combinations of capabilities. RAOs Client Certificate can also restrict issuance of specific types of client certificates to end-users in their organization.

- RAOs Client Certificate can create departments only within organizations that have been delegated to them.
- RAOs Client Certificate cannot approve or request the creation of administrators that have more privileges than themselves. They can request the creation of fellow RAOs Client Certificate only for organizations that have been delegated to them if a MRAO has enabled this feature for them.
- RAOs Client Certificate can request and approve the creation of DRAOs Client Certificate.
- RAOs Client Certificate cannot request or approve the creation of any type of administrator for organizations that have not been delegated to them, nor can they request or approve creation of administrators of any other certificate type. This limitation is applicable to even those organizations that have been delegated to these RAOs Client Certificate.
- RAOs Client Certificate can delegate domains to subordinate departments of organizations that they administer.
- When creating a new department, RAOs Client Certificate can allow or disallow MRAOs to recover the private keys of client certificates that belong to this department. In addition, RAOs Client Certificate can allow or disallow RAOs Client Certificate (themselves) to recover the private keys of client certificates belonging to this department. They can also allow or disallow DRAOs Client Certificate to recover the private keys of client certificates belonging to this department. Moreover, RAOs Client Certificate can perform any combination of these operations.
- RAOs Client Certificate can only view activity logs for their organization via SCM.

5.1.2.3 RAO Code Signing

RAOs Code Signing can access, manage, request, and approve the requests of code signing certificates for domains that have been delegated to their organizations. Specifically, the RAO Code Signing role provides the following privileges and limitations:

- RAOs Code Signing can view and control the code signing certificates belonging to end-users of the organization for which these RAOs Code Signing have been assigned rights. They have no access to manage the code signing certificates of end-users that belong to organizations for which these RAOs have not been granted permissions.
- RAOs Code Signing can only manage code signing certificates. These RAOs cannot manage other certificate types such as SSL, client, or device certificates. This limitation is applicable to those SSL, client, and device certificates belonging to the organization of which they re RAO Code Signing.
- A MRAO can make the same individual a RAO Client Certificate, RAO SSL, RAO Code Signing, and RAO Device Certificate for the same organization during the administrator creation or editing process. For more information, see "The MRAO Role" on page 218.
- RAOs Code Signing can only see those organizations that have been delegated to them in the **Organizations** area of the SCM UI.
- RAOs Code Signing cannot create new organizations, nor can they edit the **General** settings of any organization via SCM. This limitation is applicable to even those organizations of which they are RAO Code Signing.
- RAOs Code Signing can create departments only within organizations that have been delegated to these RAOs.
- RAOs Code Signing cannot approve or request the creation of administrators that have more privileges than themselves. They can, however, request the creation of fellow RAOs Code Signing for organizations that have been delegated to them if a MRAO has enabled this feature for these RAOs.

- RAOs Code Signing can request and approve the creation of DRAOs Code Signing. However, they cannot request or approve the creation of any type of administrator for organizations that have not been delegated to them, nor can they request or approve creation of administrators of any other certificate type. This limitation is applicable even to those organizations that have been delegated to these RAOs.
- RAOs Code Signing can delegate domains to subordinate departments of organizations that they administer.
- RAOs Code Signing can create developers for the CSoD service and approve code signing requests generated by developers only for the organizations and departments that are delegated to them. This is applicable only if the CSoD service is enabled for the account.
- RAOs Code Signing can only view activity logs of their organization via SCM.

5.1.2.4 RAO Device Certificate

RAOs Device Certificate can access, manage, request, and approve the requests of device certificates for devices enrolled in the AD servers or networks belonging to organizations and their departments delegated to these RAOs. Specifically, the RAO Device Certificate role provides the following privileges and limitations:

- RAOs Device Certificate can view and control the device certificates issued to the devices belonging to the organization for which these RAOs have been assigned rights. RAOs Device Certificate have no access to manage the device certificates that belong to organizations for which they have not been granted permissions.
- RAOs Device Certificate can only manage device certificates. They cannot manage other types of certificates such as SSL, client, or code signing certificates. This limitation is applicable to those SSL, client, and code signing certificates belonging to the organization for which they are RAOs Device Certificate.
- A MRAO can make the same individual a RAO Client Certificate, RAO SSL, RAO Code Signing, and RAO Device Certificate for the same organization during the administrator creation or editing process. For more information, see "The MRAO Role" on page 218.
- RAOs Device Certificate can only see those organizations that have been delegated to them in the **Organizations** area of the SCM UI.
- RAOs Device Certificate cannot create new organizations, nor can they edit the **General** settings of any organization via SCM. This limitation is applicable to even those organizations for which they are RAOs Device Certificate.
- RAOs Device Certificate can create departments only within organizations that have been delegated to these RAOs.
- RAOs Device Certificate cannot approve or request the creation of administrators that have more privileges than themselves. RAOs Device Certificate can request creation of fellow RAOs Device Certificate only for organizations that have been delegated to them if a MRAO has enabled this feature for them. RAOs Device Certificate can also request and approve creation of DRAOs Device Certificate; They cannot request or approve creation of any type of administrator for organizations that have not been delegated to these RAOs. In addition, RAOs Device Certificate cannot request or approve creation of administrators of any other certificate type. This limitation is applicable even to those organizations that have been delegated to these RAOs.
- RAOs Device Certificate can delegate domains to subordinate departments of organizations that these RAOs administer. RAOs Device Certificate can approve requests for device certificates from MS Agents installed on AD servers with AD CS or NDES role, or directly from the devices through SCEP for request and issuance of device certificates.
- RAOs Device Certificate can enable their organizations and departments for enrollment of device certificates via SCEP.
- RAOs Device Certificate can only use SCM to view activity logs for their organization.

5.1.3 The DRAO Role

Depending on the certificate type a specific DRAO is responsible for managing, the DRAO role is divided into the following subroles:

- DRAO SSL
- DRAO Client Certificate
- DRAO Code Signing
- DRAO Device Certificate

The privileges of a DRAO are defined by the departments delegated to this DRAO.

5.1.3.1 DRAO SSL

DRAOs SSL can request and manage SSL certificates for domains that have been delegated to their departments by a RAO or MRAO. Specifically, the DRAO SSL role provides the following privileges and limitations:

- DRAOs SSL can view and control SSL certificates that belong to their delegated departments. DRAOs SSL can only request SSL certificates for domains that have been delegated to their department. DRAOs SSL can approve or decline requests for SSL certificates made using the self-enrollment form for their departments.
- DRAOs SSL cannot manage SSL certificates belonging to departments for which these DRAOs have not been granted permissions. They can only see their own departments listed in the **Departments** area of the SCM UI. The **Organizations** area is not visible to DRAOs SSL.
- DRAOs SSL cannot view nor can they request certificates of any other type, including other certificate types belonging to the department for which they are DRAOs SSL.
- DRAOs SSL can upload private keys of SSL certificates belonging to their departments for management by the PKS, configured in the local network. They can also download the private keys of the certificates.
- A RAO can make the same individual a DRAO Client Certificate, DRAO SSL, DRAO Code Signing, and DRAO Device Certificate for the same department during the administrator creation or editing process. For more information, see "The RAO Role" on page 220.
- DRAOs SSL cannot request the creation of administrators that have more privileges than themselves. DRAOs SSL can request the creation of fellow DRAOs SSL only for departments that have been delegated to them if the RAO has enabled this feature for them. In addition, these DRAOs SSL cannot request creation of any type of administrator for departments that have not been delegated to them. DRAOs SSL cannot request creation of administrators of any other certificate type. This limitation is applicable to even those departments that have been delegated to these DRAOs SSL.
- DRAOs SSL can request the addition of new domains only for departments that have been delegated to these DRAOs.
- DRAOs SSL can initiate DCV process for the domains delegated to the departments they administer if these DRAOs have been provided with the **Allow DCV** privileges. DRAOs SSL with such privileges can be created only by a MRAO or RAO SSL who have the same privileges.
- DRAOs SSL can setup Network Agents in a local network for scanning internal hosts with internally facing IP addresses for installed SSL certificates for the departments that are delegated to these DRAOs. Agents also facilitate the automatic installation of SSL certificates on Apache, Apache Tomcat, and IIS web servers.
- DRAOs SSL can view the network assets such as certificates installed on various servers, endpoints, and web servers with websites and domains hosted from them, as identified by

manual or scheduled discovery scans run on networks belonging to the department under the DRAO SSL delegation.

- DRAOs SSL can assign external SSL certificates identified from discovery scans to their department in order to bring them under management through SCM.
- DRAOs SSL can view reports, edit access control lists, and modify email templates for the department that has been delegated to these DRAOs.
- DRAOs SSL cannot access or manage the **Encryption** settings via SCM, as this area can only be managed by DRAOs Client Certificate.
- DRAOs SSL cannot view activity logs via the SCM UI.
- DRAOs SSL can create and manage ACME accounts for departments delegated to them (if enabled).

5.1.3.2 DRAO Client Certificate

DRAO Client Certificate can access, request, and manage client certificates for domains that have been delegated to their departments by a MRAO or RAO. Specifically, the DRAO Client Certificate role provides the following privileges and limitations:

- DRAOs Client Certificate can view the client certificates belonging to end-users of the departments which have been delegated to these DRAOs. DRAOs Client Certificate cannot manage client certificates of end-users that do not belong to their departments. DRAOs Client Certificate can only see their own departments listed in the **Departments** area of the SCM UI. The **Organizations** area is not visible to DRAOs Client Certificate.
- DRAOs Client Certificate can only request client certificates for domains that have been delegated to their departments.
- DRAOs Client Certificate cannot view nor request certificates of any other type, including those certificate types that belong to the department of which they are DRAOs Client Certificate.
- A RAO can make the same individual a DRAO Client Certificate, DRAO SSL, DRAO Code Signing, and DRAO Device Certificate for the same department during the administrator creation or editing process. For more information, see "The RAO Role" on page 220.
- DRAOs Client Certificate cannot request creation of administrators that have more privileges than themselves. They can request the creation of fellow DRAOs Client Certificate only for departments that have been delegated to them if the RAO has enabled this feature for them. They cannot request creation of any type of administrator for departments that have not been delegated to them. Moreover, these DRAOs cannot request creation of administrators of any other certificate type. This limitation is applicable to even those departments that have been delegated to these DRAOs.
- DRAOs Client Certificate can request the addition of new domains only for the departments that have been delegated to these DRAOs.
- If enabled for their department, DRAOs Client Certificate can recover the private keys of client certificates belonging to their department.
- DRAOs Client Certificate can view reports, edit access control lists and modify email templates for the departments that has been delegated to these DRAOs.
- DRAOs Client Certificate cannot view activity logs via SCM.

5.1.3.3 DRAO Code Signing

DRAOs Code Signing can access, request, and manage code signing certificates for departments of an organization that have been delegated to them by a MRAO or RAO. Specifically, the DRAO Code Signing role provides the following privileges and limitations:

- DRAOs Code Signing can view and request code signing certificates for the departments that have been delegated to these DRAOs. They cannot manage code signing certificates

belonging to departments which have not been delegated to them. They can only see their own departments listed in the **Departments** area of the SCM UI. The **Organizations** area is not visible to DRAOs Code Signing.

- DRAOs Code Signing can only request code signing certificates for domains that have been delegated to their departments.
- DRAOs Code Signing cannot view nor request certificates of any other type, including the types of certificate belonging to the departments of which they are DRAOs Code Signing.
- A RAO can make the same individual a DRAO Client Certificate, DRAO SSL, DRAO Code Signing, and DRAO Device Certificate for a single department during the administrator creation or editing process. For more information, see "The RAO Role" on page 220.
- DRAOs Code Signing cannot approve or request the creation of administrators that have more privileges than themselves. They can request the creation of fellow DRAOs Code Signing only for departments that have been delegated to them if a RAO has enabled this feature for them. DRAOs Code Signing cannot request creation of any type of administrator for departments that have not been delegated to them. Moreover, they cannot request creation of administrators of any other certificate type. This limitation is applicable to even those departments that have been delegated to these DRAOs.
- DRAOs Code Signing can request creation of new domains only for departments that have been delegated to them.
- DRAOs Code Signing can view reports, edit access control lists and modify email templates for the department that has been delegated to them.
- DRAOs Code Signing cannot access or manage the **Encryption** settings via the SCM UI, as this area can only be managed by a DRAO Client Certificate.
- DRAOs Code Signing can create developers for CSoD service and approve code signing requests generated by developers only for the departments that are delegated to these DRAOs. Note that this is applicable only if the CSoD service is enabled for the account.
- DRAOs Code Signing cannot view activity logs via SCM.

5.1.3.4 DRAO Device Certificate

DRAO Device Certificate can access, request, and manage device certificates for departments of an organization that have been delegated to them by a MRAO or RAO. Specifically, the DRAO Device Certificate role provides the following privileges and limitations:

- DRAOs Device Certificate can view and approve device certificate requests for the departments that have been delegated to these DRAOs. They cannot manage device certificates belonging to departments which have not been delegated to them. They can only see their own departments listed in the **Departments** area of the SCM UI. The **Organizations** area is not visible to DRAOs Device Certificate.
- DRAOs Device Certificate cannot view nor request certificates of any other type, including those types of certificate belonging to the department of which they are DRAO Device Certificate.
- A RAO can make the same individual a DRAO Client Certificate, DRAO SSL, DRAO Code Signing, and DRAO Device Certificate for the same department during the administrator creation or editing process. For more information, see "The RAO Role" on page 220.
- DRAOs Device Certificate cannot approve or request creation of administrators that have more privileges than themselves. They can request creation of fellow DRAOs Device Certificate only for departments that have been delegated to them if a RAO has enabled this feature for them. DRAOs Device Certificate cannot request creation of any type of administrator for departments that have not been delegated to them. Moreover, DRAOs Device Certificate cannot request creation of administrators of any other certificate type. This limitation is applicable even to those departments that have been delegated to these DRAOs.

- DRAOs Device Certificate can request creation of new domains only for departments that have been delegated to them.
- DRAOs Device Certificate can view reports, edit access control lists and modify email templates for the department that has been delegated to these DRAOs.
- DRAOs Device Certificate cannot access or manage the **Encryption** settings via the SCM UI, as this area can only be managed by a DRAO Client Certificate.
- DRAOs Device Certificate cannot view activity logs.

5.1.4 Comparing Security Roles

The following table provides a series of comparison matrices of all security roles in SCM.

Action	Controls	MRAO	RAO	DRAO
Organization and Department Management				
Configure other administrators	Add, View Delete, Edit	Any MRAO. Any RAO of any certificate type. Any DRAO of any certificate type.	Creation DRAOs of subordinate departments who are responsible for same certificate type. Creation of RAOs of delegated organization who are responsible for same certificate type.	Creation of DRAOs of delegated department who are responsible for the same certificate type if enabled by a RAO or MRAO.
Approve or reject administrator creation requests	Approve, Reject	Any RAO of any certificate type. Any DRAO of any certificate type.	DRAOs of subordinate departments who are responsible for the same certificate type.	Not supported
Activate or deactivate administrators		Any MRAO. Any RAO of any certificate type. Any DRAO of any certificate type.	RAOs of delegated organization who are responsible for the same certificate type. DRAOs of subordinate departments who are responsible for same certificate type.	Not supported
Create and manage organizations	Add, Delete, Edit	Supported	Not supported	Not supported
Approve or reject organization creation	Approve	Supported	Not supported	Not supported

Action	Controls	MRAO	RAO		DRAO	
Create and manage departments	Add, Delete, Edit	Supported	Subordinate departments of delegated organization		Not supported	
Approve department creation	Approve	Supported	Subordinate departments of delegated organization		Not supported	
Create and manage ACME accounts		Supported	RAO SSL for delegated organizations and their departments		DRAO SSL for delegated departments	
Certificate Management						
Directly submit certificate requests to the issuing certificate authority for certificate auto-installation by SCM (IIS, Apache, and Apache Tomcat only)	Add, Renew, Approve, Decline, Install	Any organization Any department	Delegated organizations. Subordinate departments.		Delegated departments	
			RAO SSL	Yes	DRAO SSL	Yes
			RAO Client Certificate	No	DRAO Client Certificate	No
			RAO Code Signing	No	DRAO Code Signing	No
Directly submit certificate requests using the built-in application form.	Add, Renew, Replace	Any organization. Any department. Any certificate type.	Delegated organizations. Subordinate departments. Only those certificate types for which the RAO is responsible.		Delegated departments. Only those certificate types for which the DRAO is responsible.	
Approve or decline certificate requests that have been made using the self-enrollment form.	Approve, Decline	Any organization. Any department. Any certificate type.	Delegated organizations. Subordinate departments. Only those certificate types for which the RAO is responsible.		Delegated departments. Only those certificate types for which the DRAO is responsible.	

Action	Controls	MRAO	RAO		DRAO	
Manage certificates	View, Edit, Revoke	Any organization. Any department. Any certificate type.	Delegated organizations. Subordinate departments. Only those certificate types for which the RAO is responsible.		Delegated departments. Only those certificate types for which the DRAO is responsible.	
Set up and manage Private Key Agent.		Yes	No		No	
Download and upload the private key of an SSL certificate.		Any organization. Any department.	Delegated organizations. Subordinate departments.		Delegated departments.	
			RAO SSL	Yes	DRAO SSL	Yes
			RAO Client Certificate	No	DRAO Client Certificate	No
			RAO Code Signing	No	DRAO Code Signing	No
Certificate discovery	Add Classless Inter-Domain Routing (CIDR). Delete CIDR. Set up Network Agent for internal scanning.	Yes	RAO SSL	Yes	DRAO SSL	Yes
			RAO Client Certificate	No	DRAO Client Certificate	No
			RAO Code Signing	No	DRAO Code Signing	No
Request domains for...	Add	Any organization. Any department.	Delegated organizations. Subordinate departments.		Delegated departments.	
Approve or reject domain requests for...	Approve, Reject	Any organization. Any department.	Subordinate departments.		No	

Action	Controls	MRAO	RAO		DRAO	
Delegate domains to...	Delegate	Any organization. Any department.	Subordinate departments. RAOs can only delegate domains to the departments belonging to the organization that have been delegated to them; RAOs cannot re-delegate to remove a domain's delegation.		No	
Activate or deactivate domains for...		Any organization. Any department.	No		No	
Initiate DCV	Select method of DCV, as applicable to the domain.	Any organization. Any department.	RAO SSL	Yes[a]	DRAO SSL	Yes[b]
			RAO Client Certificate	No	DRAO Client Certificate	No
			RAO Code Signing	No	DRAO Code Signing	No
Key Escrow						
Manage encryption of client certificates	Initialize, Re-encrypt	Any delegated RAO. Any delegated DRAO.	**Client Certificate:** Delegated organizations. Subordinate departments.		**Client Certificate:** Delegated organizations	
Recover private keys from escrow[c]	Decrypt	Any enabled organization Any enabled department.	**Client Certificate:** Delegated organizations. Subordinate departments.		**Client Certificate:** Delegated organizations	
Can permit administrators other than themselves to recover private keys for a particular organization or department	Allow key recovery by...	MRAO. RAO Client Certificate.	**Client Certificate:** MRAO. RAO Client Certificate. DRAO Client Certificate.		**Client Certificate:** No	

Action	Controls	MRAO	RAO	DRAO
Notifications, Reports, and Miscellaneous				
Configure access control settings	Add, Delete, Edit CIDR	Yes	Yes	Yes
View notifications for...	Add, Delete, Edit	Any organization. Any department	Delegated organizations. Subordinate departments.	Delegated department
Create notifications for...	Add, Delete, Edit	Any organization. Any department	Delegated organizations. Subordinate departments.	Delegated department
View reports for...		Any organization. Any department	Delegated organizations. Subordinate departments.	Delegated DRAO
Manage SSL type availability	Type, Term	Yes	No	No
Modify email templates for	Edit	Any organization. Any department.	Delegated organizations. Subordinate departments.	Delegated department

a. On domains added to delegated organizations and subordinate departments.
b. On domains added to delegated department.
c. Escrow privileges are configured at the same time an organization or department is created. When setting up an organization, a MRAO can specify any, all, or none of the following:
- Whether or not the MRAO (themselves) should be able to recover the private keys of client certificates of that organization.
- Whether or not the RAO Client Certificate administrator of the organization should be able to recover private keys of client certificates of that organization.

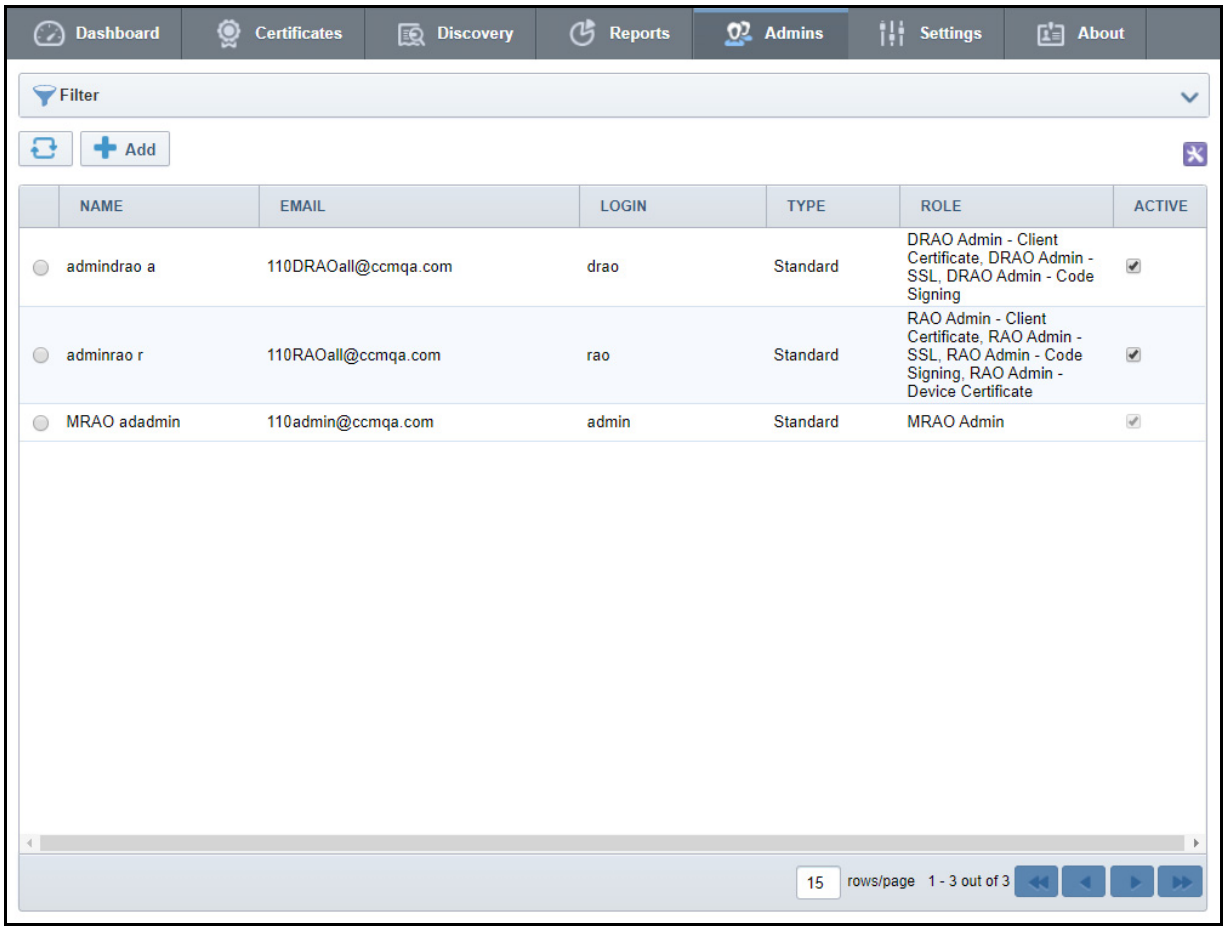
If granted the preceding escrow privileges, the RAO Client Certificate administrator would be able to specify any, all, or none of the following for any departments they create:
- Whether or not the MRAO should be able to recover the private keys of client certificates of that department.
- Whether or not the RAO Client Certificate administrators (themselves) should be able to recover the private keys of client certificates belonging to that department.
- Whether or not the DRAO Client Certificate administrators should be able to recover the private keys of client certificates belonging to that department.

5.1.5 Handling Multiple Security Roles

Multiple security roles may be selected for any particular administrator. A MRAO can assign SSL, client, and code signing administrative privileges to the same RAO for a particular organization. A RAO that has been granted administrative rights over multiple certificate types can assign similar multi-role privileges to a subordinate DRAO for a particular department.

5.2 Understanding Administrator Management

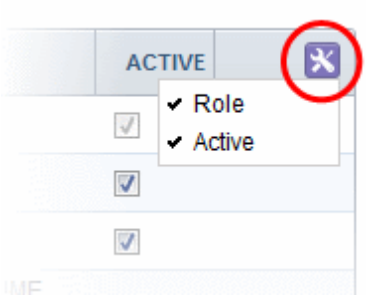
In SCM, the administrator management is performed through the **Admins** tab shown in the following illustration. This tab allows you to create, manage, and modify permissions for new and existing administrators.



The following table describes parameters are available in the **Admins** tab.

Field	Value	Description
Name		The administrator's full name.
Email		The administrator's email address. This is to be used for client certificate enrollment and notifications.
Login		The login user name of the administrator.
Type		The type of the administrator.
	Standard	Indicates that the administrator is created in SCM.

Field	Value	Description
	IdP Template	Indicates that the administrator is added via an Identity Provider (IdP) template.
	IdP User	Indicates that the administrator is added in SCM and was authenticated by an IdP.
Role	MRAO Admin	The MRAO is the top level administrator and can access all areas and functionality of the SCM.
	RAO Admin SSL	RAO SSL has privileges to access, manage, request, and approve the requests of SSL certificates for departments and domains belonging to their organization.
	RAO Admin Client Certificate	RAO Client Certificate has privileges to access, manage, request, and approve the requests of client certificates for departments and domains that have been delegated to their organization.
	RAO Admin Code Signing	RAO Code Signing has privileges to access, manage, request, and issue the code signing certificates for end-users belonging to their organization.
	RAO Admin Device Certificate	RAO Device Certificate has privileges to access, manage, and approve device certificates issued for devices enrolled through an AD server or through SCEP, belonging to their organization.
	DRAO Admin SSL	DRAO SSL has privileges to access, manage, and request SSL certificates for departments of an organization that have been delegated to them by a MRAO or RAO.
	DRAO Admin Client Certificate	DRAO Client Certificate has privileges to access, manage, request client certificates for domains that have been delegated to their department.
	DRAO Admin Code Signing	DRAO Code Signing has privileges to access, manage, request, and issue the code signing certificates for end-users belonging to their department.
	DRAO Admin Device Certificate	DRAO Device Certificate has privileges to access, manage, approve and issue the device certs for devices enrolled through an AD server or through SCEP, belonging to their department.
Active	Boolean	Indicates whether the administrator is active or not. Also allows the MRAO and delegated RAO to switch other administrators between active and inactive statuses according to their privilege levels.

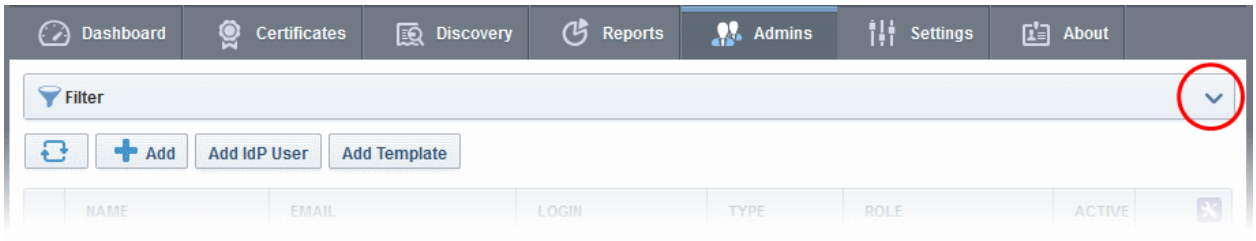
Field	Value	Description
You can use the tool button to select columns to be displayed in the table: 		
Control Buttons	Refresh	Refreshes the list.
	Add	Enables the MRAO and RAO to add new administrators.
	Add IdP User	Enables the MRAO to enroll new administrators via IdP credentials.
	Add Template	Enables the MRAO to define privileges for administrators that enrolled via IdP link in the login dialog.
Administrator Control Buttons[a]	Edit	Enables a MRAO and RAO to modify the details of the selected administrator.
	Delete	Deletes the administrator. If an administrator is deleted, the details of that administrator can be viewed but they are no longer editable.
	View	Enables a MRAO to view the details of a RAO or DRAO added by another RAO, pending approval.
	Approve	Enables a MRAO to approve a RAO or DRAO added by a RAO. The newly added administrator becomes active only on approval by the MRAO.
	Reject	Enables a MRAO to reject a RAO or DRAO added by a RAO, pending approval.
	Reset Lockout	Enables a MRAO to unlock the login screen that has been locked due to consecutive five wrong attempts to login.
	Send/Resend IdP Invitation	Enables a MRAO and RAO to send invitation to existing administrators to allow them to login via their IdP credentials.

a. The availability of these buttons depends on the selected administrator type.

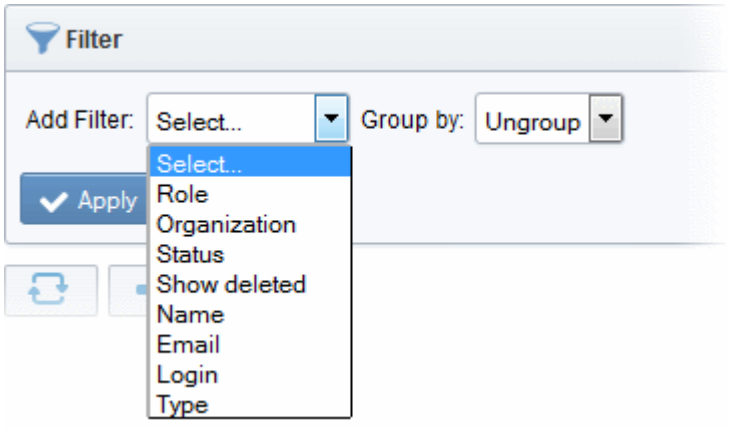
5.3 Sorting and Filtering Administrators

You can sort items in alphabetical order in a column by clicking a column header, and you can use filters to search for specific administrators.

You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.



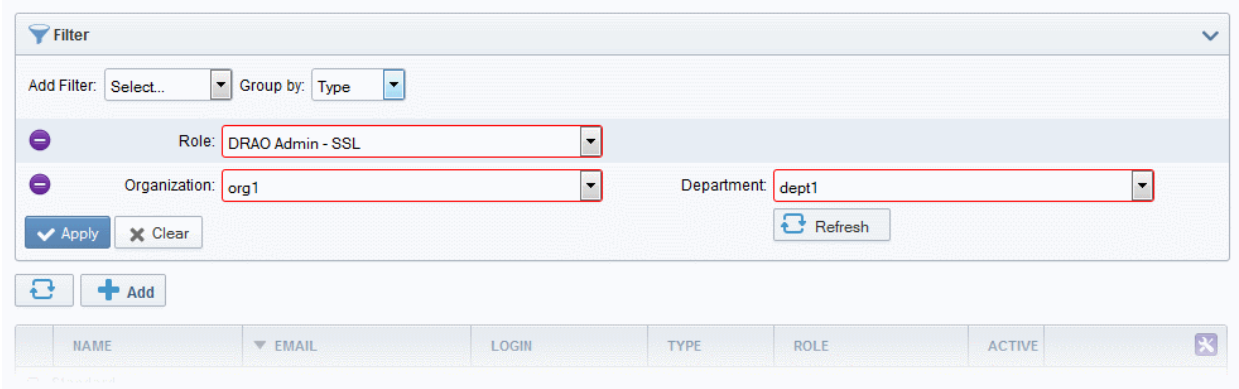
To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection from the **Add Filter** list.



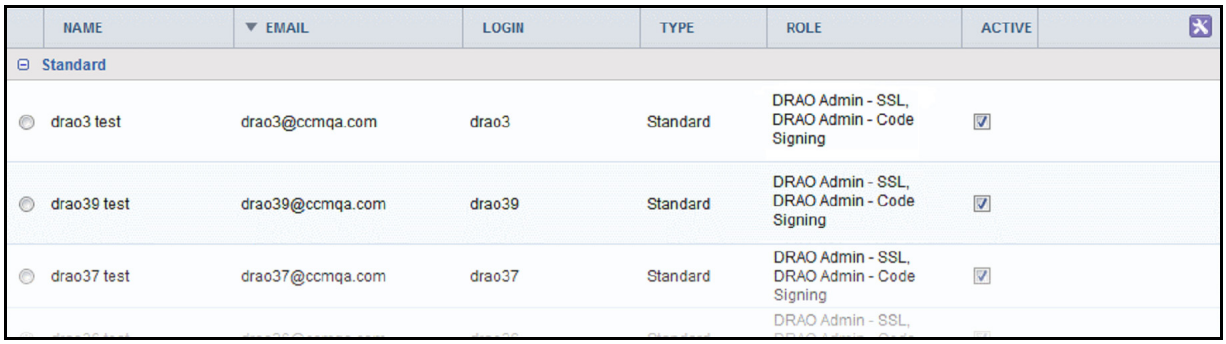
For example, if you want to search for DRAO SSL administrators belonging to org1 organization and dept1 department and group them based on their types, you follow this procedure:

- Select **Role** from the **Add Filter** list.
- Select **Organization** from the **Add Filter** list.

  This displays organization and department filters, as the following illustration shows.
- Select org1 organization and dept1 department from the **Organization** and **Department** lists respectively.
- Select **Type** from the **Group by** list, and then click **Apply**.



The following illustration shows the filtered items based on the entered and selected criteria that are displayed.



Clicking **Clear** removes filters.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **Admins** screen, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

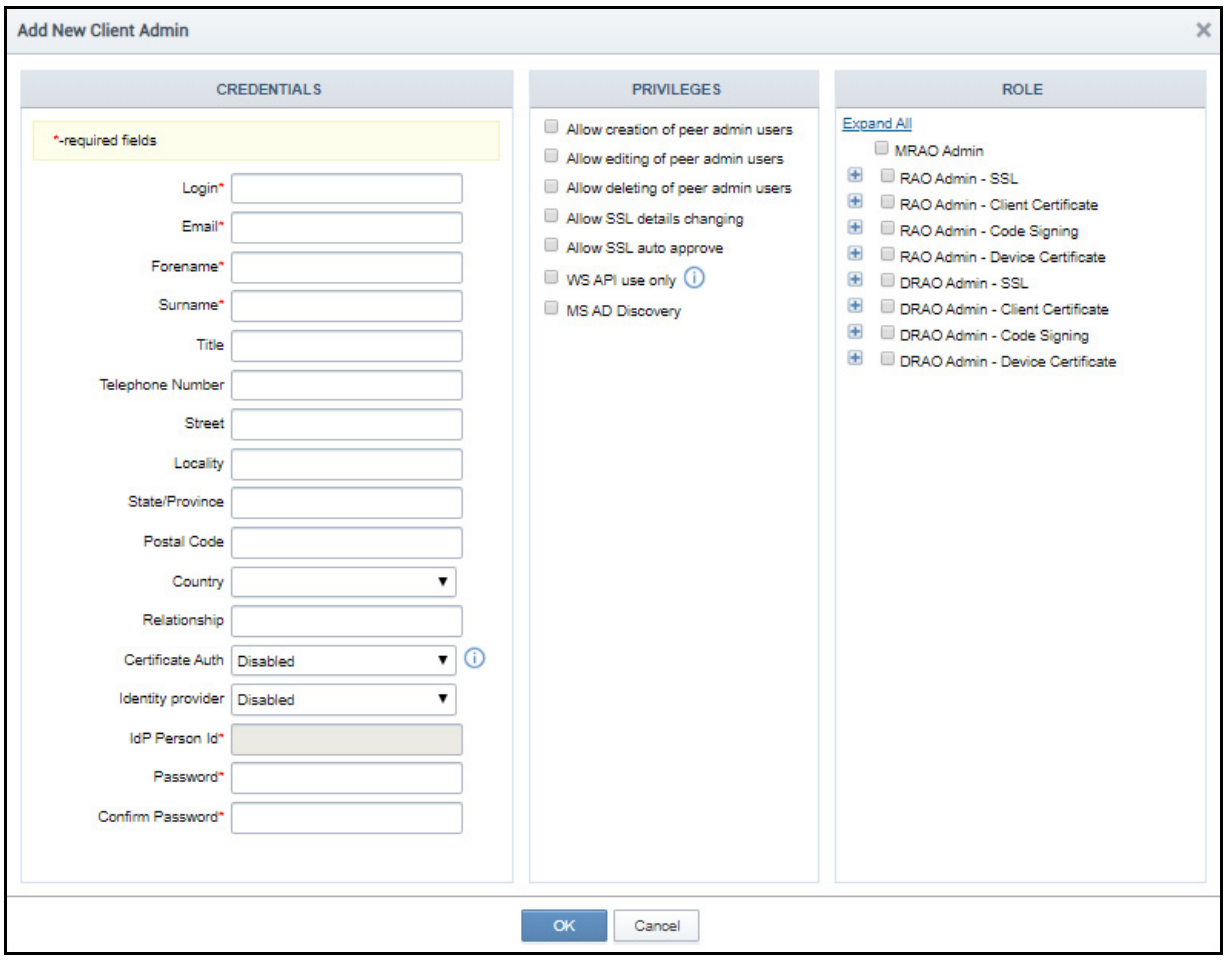
5.4 Adding Administrators

SCM allows you to add new users with administrator role either manually or by inviting them to login via the Identity Provider (IdP) credentials, if the latter is enabled for your account.

5.4.1 How to add Standard Administrator Accounts

You can add an administrator account as follows:

1. From the main UI, navigate to **Admins**.
2. Click **Add** to open the **Add new Client Admin** dialog shown in the following illustration.



3. Complete the **Add New Client Admin** fields based on the information provided in the following table.

Field	Description
Credentials	
Login	The login user name for the new administrator.
Email	The full email address of the new administrator.
Forename	The first name of the new administrator.
Surname	The surname of the new administrator.
Title	The title for the new administrator.
Telephone Number	The contact phone number for the new administrator.

Field	Description
Street Locality State / Province Postal Code Country	The address details of the new administrator.
Relationship	The role of the new administrator. For example, RAO SSL.
Certificate Auth	Specifies whether or not the new administrator must authenticate themselves to SCM with their client certificate over a https connection prior to being granted login rights. The list is auto-populated with the client certificates issued by SCM for the new administrator based on their email address specified in the **Email** field. If authentication is required, the administrator can select the certificate from the list. The new administrator can login to SCM only if the specified certificate is installed on the computer from which they attempt to login. If authentication is not needed, you can select Disabled from the list, as shown in the preceding illustration.
Identity Provider	Select the Identity Provider account to be used by the administrator to log into SCM. You can enable IdP login for the administrator at any time by sending an IdP invitation or by editing the administrator account.
IdP Person Id	The unique identifier for the administrator in the IdP realm. The identifier can be obtained from meta data provided by the IdP service provider.[a]
Password, Confirm password	The password for the new administrator to access the SCM interface and reenter this password for confirmation. The new administrator has to change the password upon their first login.
Privileges	
Allow creation of peer admin users	The new administrator can add other administrators of their own level or of lower level in the hierarchy, depending on the options selected.
Allow editing of peer admin users	The new administrator can edit other administrators of their own level or of lower level in the hierarchy, depending on the options selected.
Allow deleting of peer admin users	The new administrator remove other administrators of their own level or of lower level in the hierarchy, depending on the options selected.

Field	Description
Allow domain validation without Dual Approval	The new administrator's privileges are sufficient so that the domain creation or delegation approved by this administrator is activated immediately, without the requirement of approval by a second MRAO. This field is available to MRAOs only if enabled for their account.
Allow DCV	Enables the new administrator to initiate the DCV process for newly created domains. This field is available to a MRAO, RAO SSL, and DRAO SSL only if enabled for their account.
Allow SSL details changing	Enables the new MRAO, RAO SSL, and DRAO SSL to change the details of SSL certificates by navigating to **Certificates > SSL Certificates**.
Allow SSL auto approve	The SSL certificates requested by the MRAO is automatically approved, and those requested by a RAO SSL and DRAO SSL are automatically approved by the administrator of same level and await approval from higher level administrator.
WS API use only	The administrator account can only be used for the API integration. The SCM UI access is not allowed for this account.
MS AD Discovery	Enables the new administrator to access the **Settings > MS Agents** interface, integrate an AD server to SCM by downloading and installing the MS Agent, and view the certificates and web servers discovered by the MS Agents by scanning respective AD servers.

Role[b]
The new administrator can be assigned to a particular organization or department by selecting the appropriate organization or department from the list that appears after selecting a role. All organizations are listed by default. Clicking the plus sign (+) beside the organization name expands the tree structure to display the departments associated with the organization. Clicking Expand All expands the tree structure to display all the departments under each organization. Clicking Collapse All in the expanded view collapses the tree structure of all the organizations and hides the departments under each organization.

Field		Description
Administrative Role	MRAO	A MRAO can manage all certificates for all listed organizations. This disables the organization selection.
	RAO SSL	A RAO SSL can manage only SSL certificates and only for selected organizations.
	RAO Client Certificate	A RAO Client Certificate can manage only client certificates and only for selected organizations.
	RAO Code Signing	A RAO Code Signing can manage only the code signing certificates issued to end-users belonging to the selected organizations.
	RAO Device Certificate	A RAO Device Certificate can manage only the device authentication certificates issued to devices belonging to the selected organizations.
	DRAO SSL	A DRAO SSL can manage only SSL certificates and only for selected departments.
	DRAO Client Certificate	A DRAO Client Certificate can manage only client certificates and only for selected departments.
	DRAO Code Signing	DRAO Code Signing can manage only the code signing certificates issued to end-users belonging to the selected departments.
	DRAO Device Certificate	A DRAO Device Certificate can manage only the device authentication certificates issued to devices belonging to the selected departments.

a. Usually the **IdP Person Id** value for a user can be obtained from the value of the **Person Principal Name** (**PPn**) field in the meta data. This may vary for different IdP service providers. Contact your IdP service provider for help.
b. The same RAO can be assigned as RAO SSL, RAO Client Certificate, and RAO Code Signing as required. Similarly, same DRAO can be assigned as RAO SSL, RAO Client Certificate, and RAO Code Signing as required. Select the Organization or Department to which the new administrator will have access.

4. Click **OK**.

Administrators created by a MRAO and RAO with the Admin Creation Privileges are immediately added to the SCM. However, the administrators created by other RAOs have to await for an approval from the MRAO. The new administrators are added to SCM only if the MRAO approves them by selecting the administrator and clicking **Approve** located at the top of the Admins area of the SCM UI. The details of the new administrator created by a MRAO can be modified at any time by selecting the administrator and clicking **Edit**. The details of the new administrator created by an RAO can be edited at any time after the new administrator has been approved by the MRAO.

If the **Certificate Auth** field is enabled, administrators currently being created can only login to SCM after authenticating themselves with a certificate. That is, SCM requests the certificate specified during creation of the administrator in addition to their login and password details.

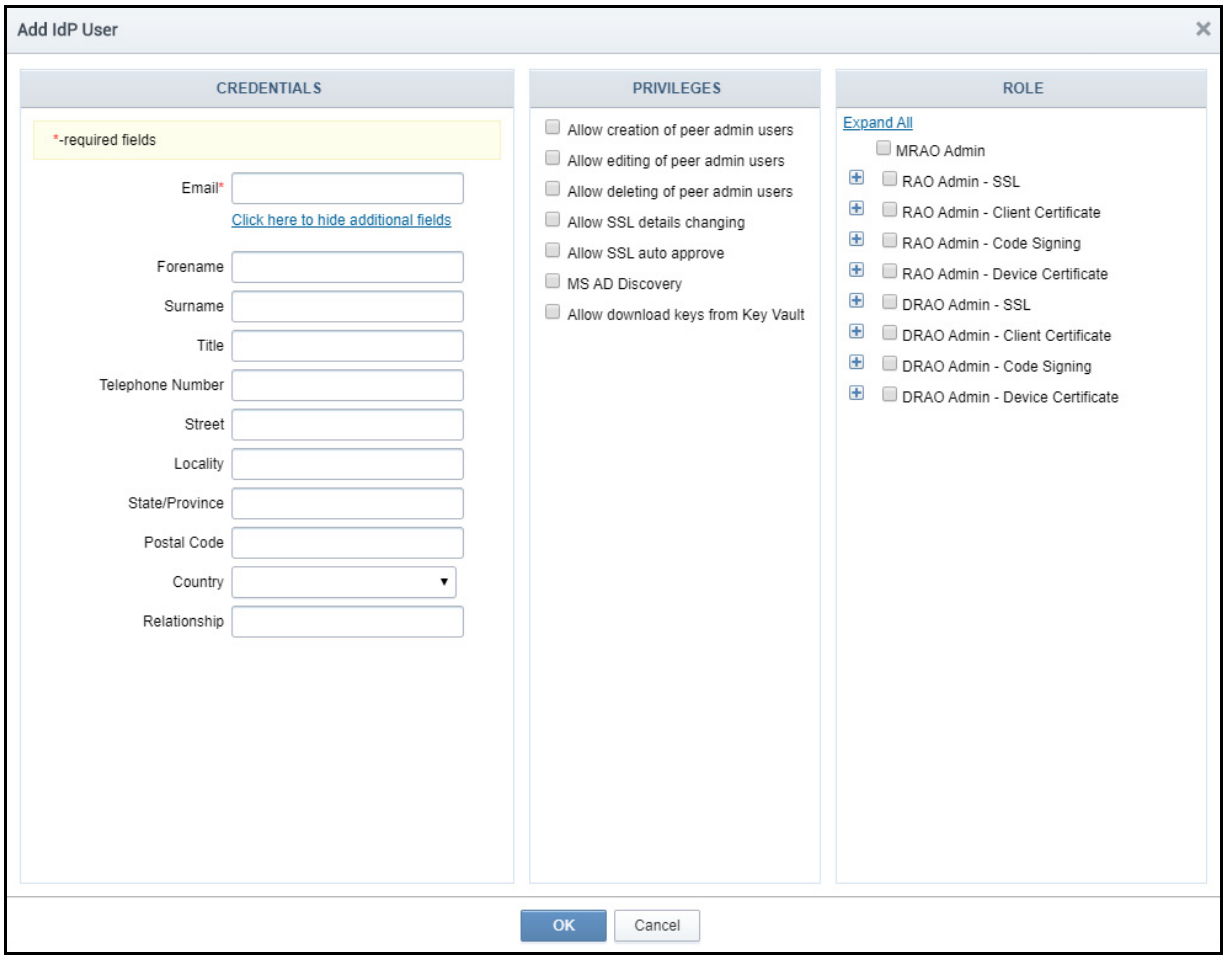
If an administrator has replaced their certificate used for the certificate authentication, SCM resynchronizes their certificate information, in which case you need to select the appropriate certificate again as follows:

1. From the main UI, navigate to the **Admins**, select the administrator, and click **Edit** to reopen the administrator configuration dialog.
2. Select the new authentication certificate from the **Certificate Auth** field.
3. Click **OK**.

5.4.2 How to Add IdP Administrator Accounts

You can add an IdP administrator account as follows:

- Navigate to the **Admins** section.
- Click **Add IdP User** to open the **Add IdP User** dialog shown in the following illustration.



- Complete the **Add IdP User** fields based on the information provided in the following table.

Field	Description
Credentials	
Email	The full email address of the new administrator.
Forename	The first name of the new administrator.
Surname	The surname of the new administrator.
Title	The title for the new administrator.
Telephone Number	The contact phone number for the new administrator.
Street Locality State / Province Postal Code Country	The address details of the new administrator.
Relationship	The role of the new administrator. For example, RAO SSL.
Privileges	
Allow creation of peer admin users	The new administrator can add other administrators of their own level or of lower level in the hierarchy, depending on the options selected.
Allow editing of peer admin users	The new administrator can edit other administrators of their own level or of lower level in the hierarchy, depending on the options selected.
Allow deleting of peer admin users	The new administrator remove other administrators of their own level or of lower level in the hierarchy, depending on the options selected.
Allow SSL details changing	Enables the new MRAO, RAO SSL, and DRAO SSL to change the details of SSL certificates by navigating to **Certificates > SSL Certificates**.
Allow SSL auto approve	The SSL certificates requested by the MRAO is automatically approved, and those requested by a RAO SSL and DRAO SSL are automatically approved by the administrator of same level and await approval from higher level administrator.
MS AD Discovery	Enables the new administrator to access the **Settings > MS Agents** interface, integrate an AD server with SCM by downloading and installing the MS Agent, and view the certificates and web servers discovered by the MS Agents by scanning respective AD servers.

Field		Description
Role[a]		
The new administrator can be assigned to a particular organization or department by selecting the appropriate organization or department from the list that appears after selecting a role. All organizations are listed by default. Clicking the plus sign (+) beside the organization name expands the tree structure to display the departments associated with the organization. Clicking Expand All expands the tree structure to display all the departments under each organization. Clicking Collapse All in the expanded view collapses the tree structure of all the organizations and hides the departments under each organization.		
Administrative Role	MRAO	A MRAO can manage all certificates for all listed organizations. This disables the organization selection.
	RAO SSL	A RAO SSL can manage only SSL certificates and only for selected organizations.
	RAO Client Certificate	A RAO Client Certificate can manage only client certificates and only for selected organizations.
	RAO Code Signing	A RAO Code Signing can manage only the code signing certificates issued to end-users belonging to the selected organizations.
	RAO Device Certificate	A RAO Device Certificate can manage only the device authentication certificates issued to devices belonging to the selected organizations.
	DRAO SSL	A DRAO SSL can manage only SSL certificates and only for selected departments.
	DRAO Client Certificate	A DRAO Client Certificate can manage only client certificates and only for selected departments.
	DRAO Code Signing	DRAO Code Signing can manage only the code signing certificates issued to end-users belonging to the selected departments.
	DRAO Device Certificate	A DRAO Device Certificate can manage only the device authentication certificates issued to devices belonging to the selected departments.

a. The same RAO can be assigned as RAO SSL, RAO Client Certificate, and RAO Code Signing as required. Similarly, same DRAO can be assigned as RAO SSL, RAO Client Certificate, and RAO Code Signing as required. Select the Organization or Department to which the new administrator will have access.

- Click **OK**.

The new IdP-enabled administrator must be approved by another MRAO by navigating to **Admins**, selecting that administrator from the list, and clicking **Approve**.

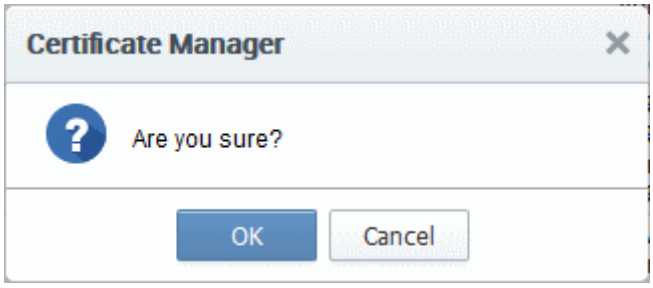
Once an IdP user is created and approved, the new IdP-enabled administrator is sent an email containing a link to activate their account and access the SCM login page (see "Logging Into an SCM Account" on page 4).

5.5 Editing and Deleting Administrators

You can modify any parameter of any administrator at any time by navigating to the **Admins** tab, selecting the administrator, and clicking **Edit**.

When deleting an administrator, you would encounter the following dialog which allows you to proceed by clicking **OK**.

Note that there must always be at least one MRAO, therefore you cannot delete the last MRAO.

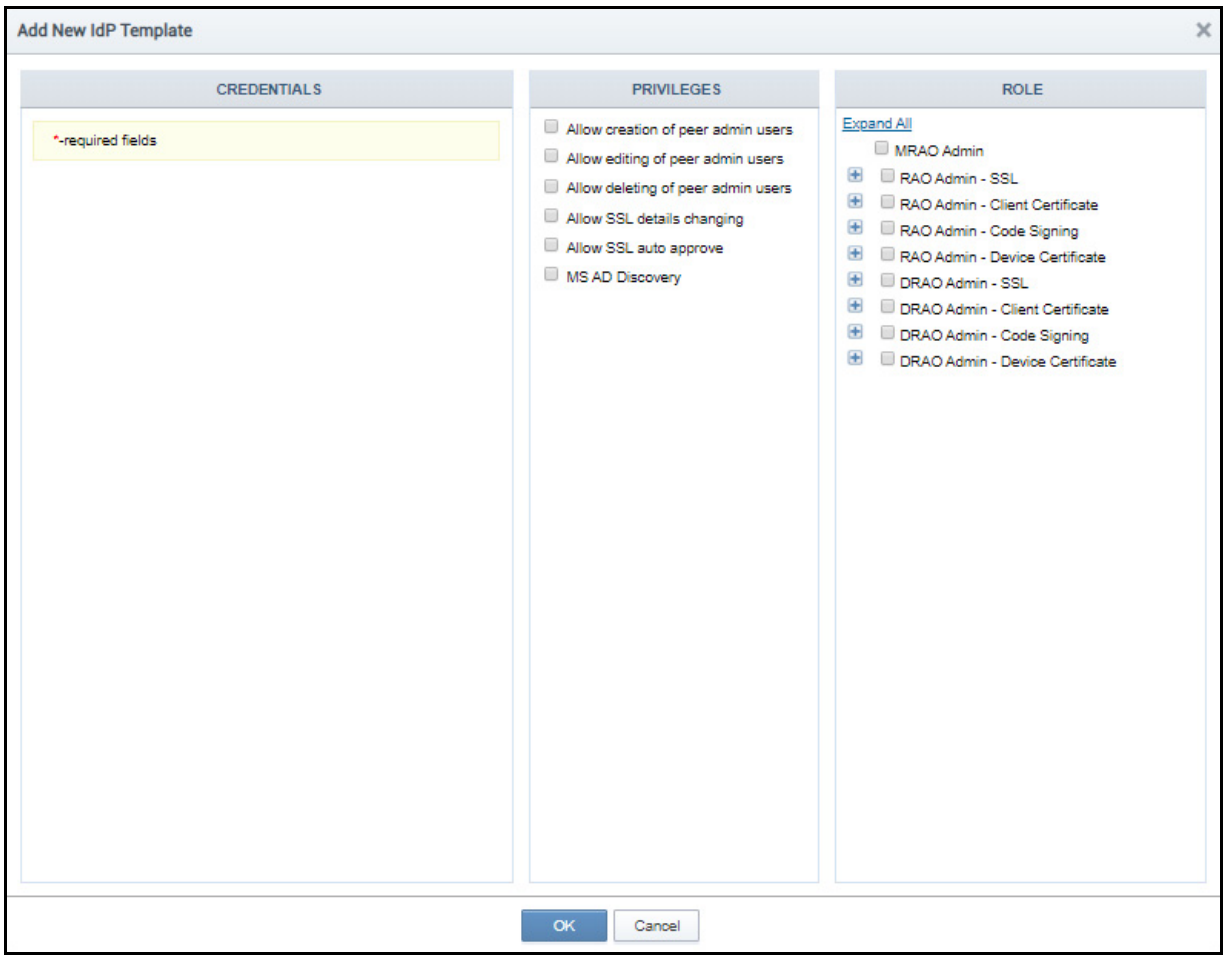


5.6 Creating IdP User Account Templates

MRAOs, as well as RAOs with administrator creation privileges, can create an IdP template on their SCM account and use it to assign roles and define privileges. Users that were not previously enrolled but were invited to log into SCM using their IdP credentials are assigned roles and privileges as defined in the template.

To add an IdP template, do the following:

1. From the main UI, navigate to **Admins**.
2. Click **Add Template** to open the **Add New IdP Template** dialog, as shown in the following illustration.



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

Field/Element	Description
Privileges	
Allow creation of peer admin users	The new administrator can add other administrators of their own level or of lower level in the hierarchy, depending on the options selected.
Allow editing of peer admin users	The new administrator can edit other administrators of their own level or of lower level in the hierarchy, depending on the options selected.
Allow deleting of peer admin users	The new administrator can remove other administrators of their own level or of lower level in the hierarchy, depending on the options selected.

Field/Element	Description
Allow domain validation without Dual Approval	The new administrator's privileges are sufficient so that the domain creation or delegation approved by this administrator is activated immediately, without the requirement of approval by a second MRAO. This field is available to MRAOs only if enabled for their account.
Allow DCV	Enables the new administrator to initiate the DCV process for newly created domains. This field is available to MRAOs, RAOs SSL, and DRAOs SSL only if enabled for their account.
Allow SSL Details changing	Enables the new MRAO, RAO SSL, and DRAO SSL to change the details of SSL certificates by navigating to **Certificates > SSL Certificates**.
Allow SSL auto approve	The SSL certificates requested by the MRAO is automatically approved, and those requested by a RAO SSL and DRAO SSL are automatically approved by the administrator of same level and await approval from higher level administrator.
MS AD Discovery	Enables the new administrator to access the **Settings > MS Agents** interface, integrate an AD server to SCM by downloading and installing the MS Agent, and view the certificates and web servers discovered by the MS Agents by scanning respective AD servers.

Role[a]
The new administrator can be assigned to a particular organization or department by selecting the appropriate organization or department from the list that appears after selecting a role. All organizations are listed by default. Clicking the plus sign (+) beside the organization name expands the tree structure to display the departments associated with the organization. Clicking Expand All expands the tree structure to display all the departments under each organization. Clicking Collapse All in the expanded view collapses the tree structure of all the organizations and hides the departments under each organization.

Field/Element		Description
Administrative Role	MRAO	A MRAO can manage all certificates for all listed organizations. This disables the organization selection.
	RAO SSL	A RAO SSL can manage only SSL certificates and only for selected organizations.
	RAO Client Certificate	A RAO Client Certificate can manage only client certificates and only for selected organizations.
	RAO Code Signing	A RAO Code Signing can manage only the code signing certificates issued to end-users belonging to the selected organizations.
	RAO Device Certificate	A RAO Device Certificate can manage only the device authentication certificates issued to devices belonging to the selected organizations.
	DRAO SSL	A DRAO SSL can manage only SSL certificates and only for selected departments.
	DRAO Client Certificate	A DRAO Client Certificate can manage only client certificates and only for selected departments.
	DRAO Code Signing	DRAO Code Signing can manage only the code signing certificates issued to end-users belonging to the selected departments.
	DRAO Device Certificate	A DRAO Device Certificate can manage only the device authentication certificates issued to devices belonging to the selected departments.

a. The same RAO can be assigned as RAO SSL, RAO Client Certificate, and RAO Code Signing as required. Similarly, same DRAO can be assigned as RAO SSL, RAO Client Certificate, and RAO Code Signing as required. Select the organization or department to which the new administrator will have access.

Once a template is created, you can allow new users to login to SCM without being pre-enrolled. Once a new user logs into SCM using their IdP credentials, they are assigned all the permissions outlined in the new template. For more information on logging into SCM, see "Organizations and Departments" on page 2.

6

Configuring Agents

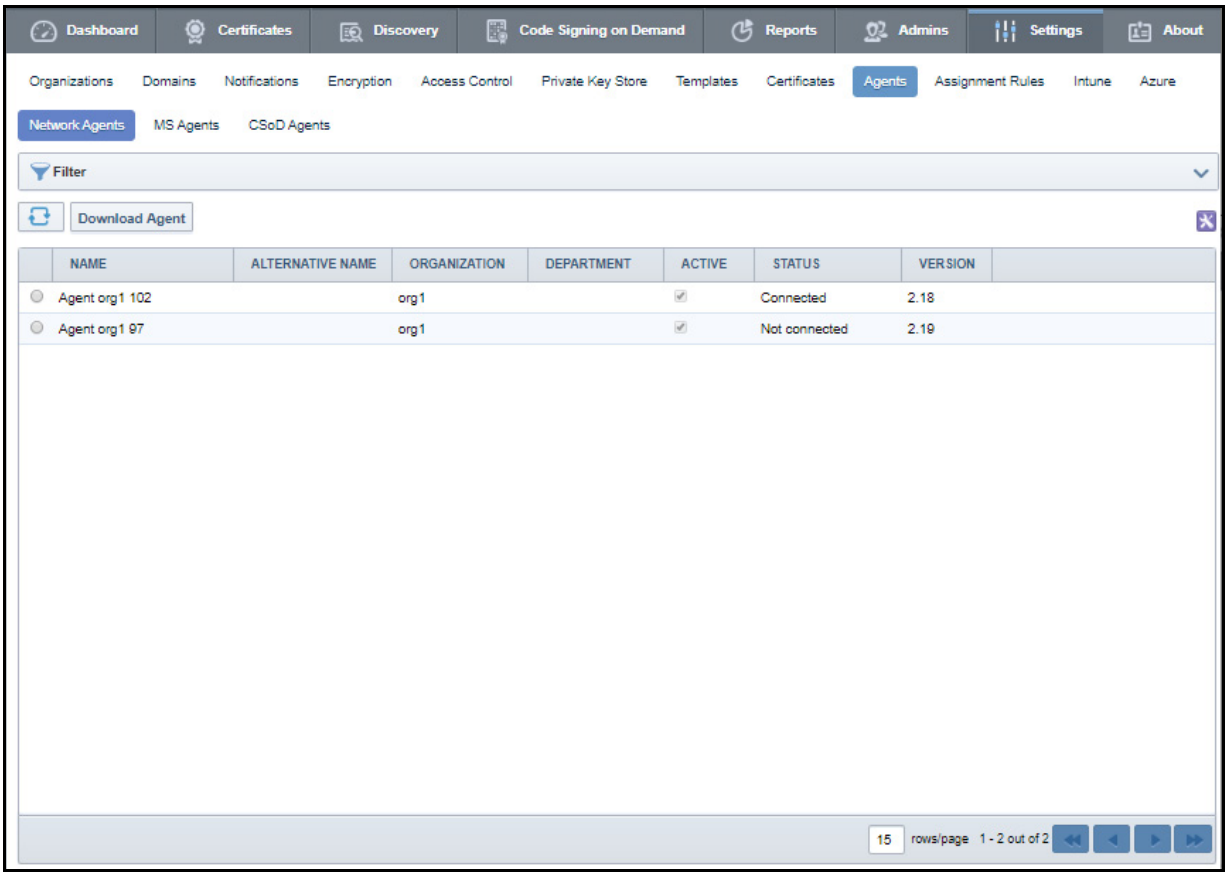
This chapter describes the configuration and use of the various agents available in SCM.

This chapter describes the following topics:

- SCM Agents Overview
- Configuring Network Agents
- Configuring MS Agents
- Configuring CSoD Agents
- Configuring JVM Parameters for Agents

6.1 SCM Agents Overview

SCM agents allow you to automate various processes such as certificate discovery and installation. Agents can be managed through the **Agents** area shown in the following illustration.



There are four types of agents: network agents, MS agents, CSoD agents, and private key agents.

The network agent performs the following:

- SSL web server certificate discovery on networks.
- Automated request and installation of SSL certificates, in one of the following modes:
  - Central controller mode—The network agent is installed on a single host that communicates with web servers and automatically requests and install certificates on them.
  - Local controller mode—The network agent is installed on each web server for which certificate auto-installation and renewal is required.

The MS agent is installed on AD servers for the purpose of integrating them with SCM. This agent performs the following:

- Discovery of assets such as web servers, domains, certificates, and so on.
- Maps MS AD certificate templates to SCM certificate types to act as a Private CA.
- Installed on AD servers, MS agents can be used to provision certificates from MS CA and also act as a CA proxy.

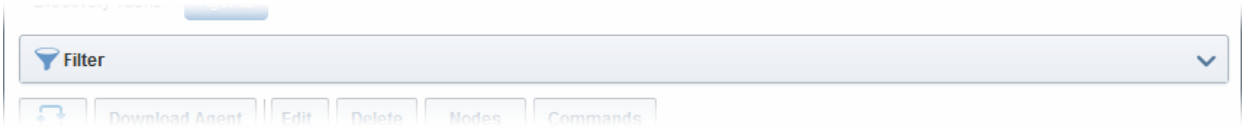
The CSoD agent handles code signing operations for developers in one of the following modes:

- In-house hosted mode—The CSoD service back end is run on Sectigo's secure cloud servers while the rest of the lifecycle is run in-house. The In-House Hosted CSoD can be run as follows:
  - Standard—With an agent installed on a single server.
  - Clustered—With agents installed on multiple servers for redundancy.
- Cloud service mode—The CSoD service is provisioned entirely on Sectigo's secure cloud servers.

The PK agent receives commands from SCM for CSR generation, storing private keys, and the generation of PKCS#12 certificates.

6.1.1 How to Sort and Filter Agents

You can sort items in the alphabetical order by clicking a column header, and you can use filters to search for particular agent.

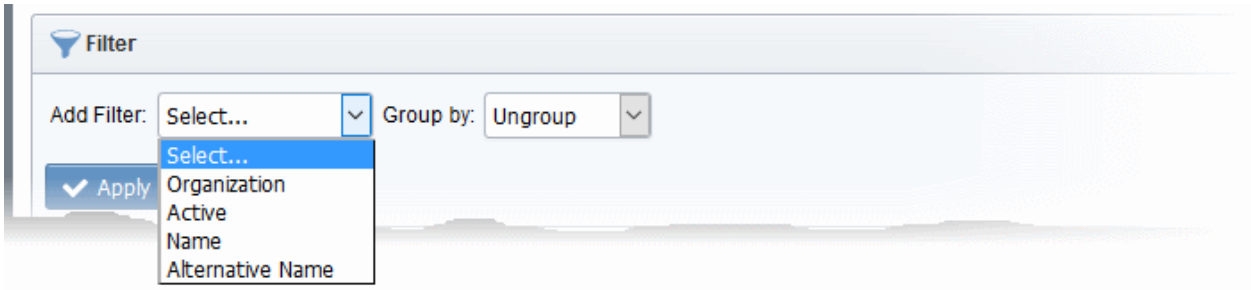


To add filters, you make a selection in the **Add Filter** list and then group the results with other options that appear depending on the selection from the **Add Filter** list. The options available in the **Add Filter** list depends on the kind of agent you are filtering.

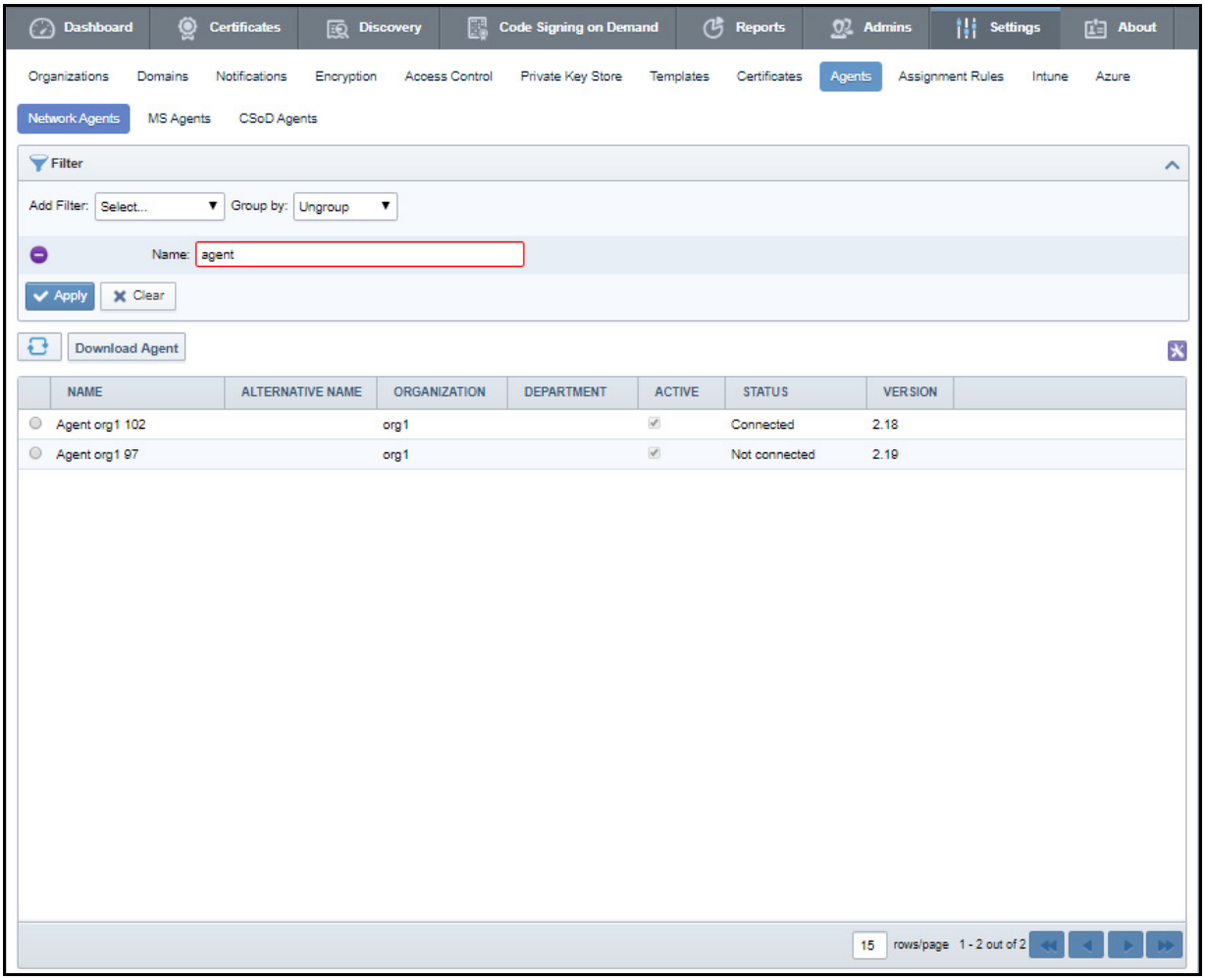
For example, you can search for a **Network Agent** of a specific name that belongs to a specific organization and department by doing the following:

- Select **Name** from the **Add Filter** list and enter the name of the agent in full or part.

- Select **Organization** or **Department** in the **Group by** list.
- Click **Apply**.



The filtered items based on the entered and selected parameters are displayed, as shown in the following illustration.



You can remove the filter options by clicking **Clear**.

Search filters, once configured for the interface, are saved automatically. When you reopen the area, the configured filters are active and only the search results are displayed. Click **Clear** to remove filters.

6.2 Configuring Network Agents

SCM uses network agents to achieve the following:

- **Discovery of SSL certificates**—An agent installed on a web server or any local computer on the network scans and monitors for installed SSL certificates. It is possible for administrators to configure SCM to scan externally-facing IP addresses directly from the **Discovery Tasks** area of SCM. However, SCM can only scan internal hosts if an agent which is configured to communicate with the SCM servers is installed on the local network. After scanning the local network, the agent sends a report back to SCM.
- **Automatic installation of certificates**—An agent installed on a web server periodically contacts SCM for requests for certificates that have been enabled for auto-installation. If a request exists, it automatically generates a CSR on the web server and presents the application for administrator approval via SCM. On approval, the agent submits the CSR to Sectigo and tracks the order number. Once the certificate is issued by the CA, the agent downloads the certificate and allows the administrator to install it. An agent installed on a single server can be configured to communicate with, and install certificates on, other remote servers in the network. The automatic installation of certificates is limited as outlined in the following table:

Vendor	Linux	Windows
Apache 2.x	Local/Remote auto-installation	N/A
Tomcat	Local/Remote auto-installation	Local auto-installation
Microsoft IIS	N/A	Local/Remote auto-installation
F5 BIG-IP	Remote auto-installation	Remote auto-installation

NOTE: In order to execute certificate installation tasks, the auto-installer functionality must be enabled for your account. Otherwise, the agent can perform certificate discovery.

The configuration options available to you depend on your administrator security role, as follows:

- A MRAO can set up a network agent for installing certificates and scanning internal servers of any organization or department, for certificates requested, issued, expired, revoked, and replaced.
- A RAO SSL can set up a network agent for installing certificates and scanning internal servers of organizations and their departments that have been delegated to this administrator, for certificates requested, issued, expired, revoked, and replaced.
- A DRAO SSL can set up a network agent for installing certificates and scanning internal servers of departments that have been delegated to them for certificates requested, issued, expired, revoked, and replaced.

6.2.1 How to Fulfill Network Agent User Permission Requirements

There is a number of platform-dependent permissions that are required for installing the Sectigo network agent and performing certificate discovery.

6.2.1.1 Network Agent Installation Permissions

In order to install a network agent, the following permission requirements must be satisfied:

- Windows:
  - Local admin rights
- Linux:
  - sudo permissions
  - execute permission attribute

6.2.1.2 Network Agent Node Discovery and Auto-Installation Permissions

The following permissions are required when the network agent is configured to perform node discovery and certificate auto-installation.

Web Server	Permissions	
Windows		
IIS	For Standalone Windows Servers (IIS): • User is part of local Administrators Group • Windows Server Role - File Server (File and Storage Services > File and iSCSI Services > File Server) • User Account Control: Run all administrators in Admin Approval Mode (Disabled)	For Domain joined: • Domain User is part of local Administrator Group
Apache Tomcat	• User account that is a member of the Local Administrators group	
F5 BIG-IP	• User must be a fully privileged administrator in the F5 BIG-IP application. Up to version 13.	
Linux		
Apache	• User account with SSH access (default port: 22) • User account with ACL permission specific files and folders: - `rwx /opt` - `rwx` to tomcat `server.xml` - `rwx` to tomcat `conf` - `rwx` to storage location of jks	
F5 Big-IP	• User must be a fully privileged administrator in the F5 BIG-IP application. Up to version 13.	

6.2.2 How to Fulfill Network Agent Hardware Requirements

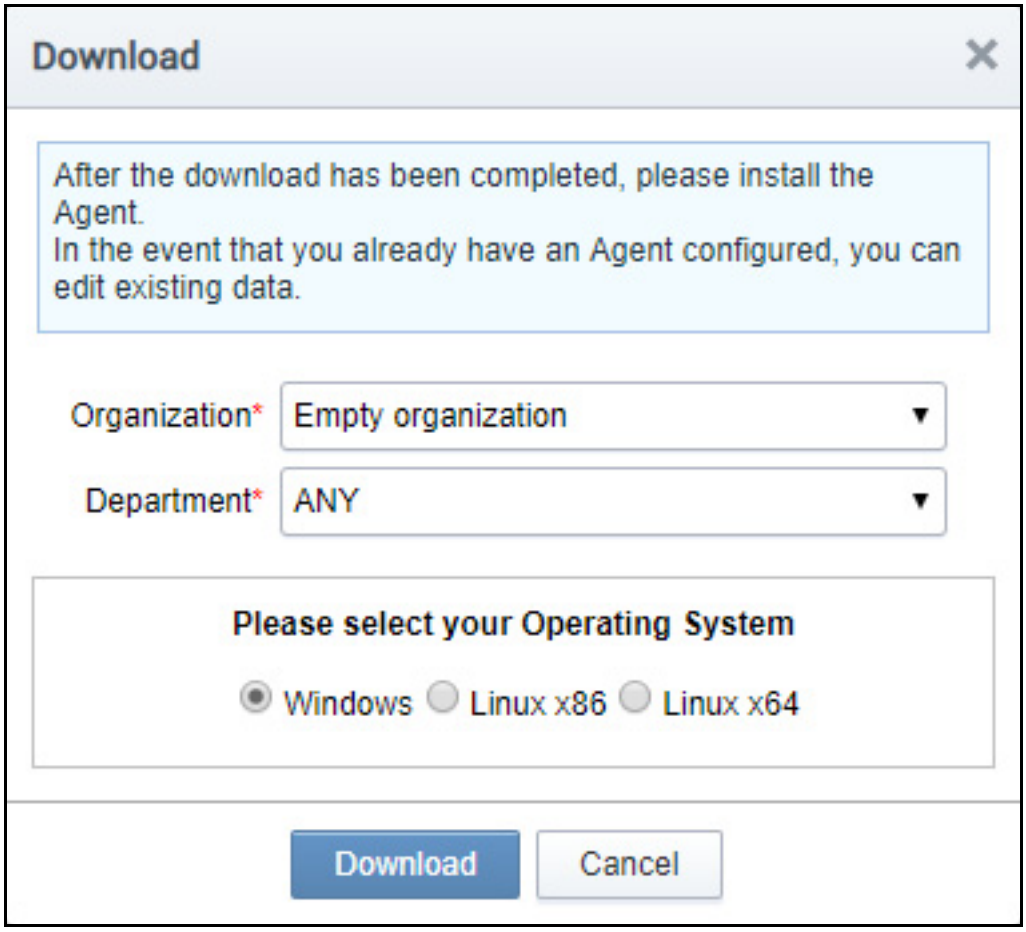
The system requirements outlined in the following table must also be met prior to the installation of a network agent.

Component		Value
Windows		
Operating System		Windows 2008 or later
CPU	Minimum	1.4 GHz 64-bit or 32-bit processor
	Recommended	2.0 GHz 64-bit or 32-bit processor or greater
RAM	Minimum	2 GB
	Recommended	4 GB or greater
Internet Access		Yes (can be proxied)
Outbound Port		TCP: 443
Internal ports (Certificate Discovery)		TCP: 443 (default), (Any ports that serves up a website)
Internal ports (Node Discovery & Auto-Install)		TCP: 22 (default SSH port), 445
Linux		
Operating System		CentOS/RHEL 6.x/7.x, Debian 8 (Jessie)/9 (Stretch), Ubuntu LTS 14.04/16.04/18.04
CPU	Minimum	1.4 GHz 64-bit processor
	Recommended	2.0 GHz 64-bit processor or greater
RAM	Minimum	2 GB
	Recommended	4 GB or greater
Internet Access		Yes
Outbound Port		TCP: 443
Internal ports (Certificate Discovery)		TCP: 443 (default), (Any ports that serves up a website)
Internal ports (Node Discovery & Auto-Install)		TCP: 22 (default SSH port)

6.2.3 How to Install a Network Agent

You can download and install a network agent as follows:

1. Navigate to **Settings > Agents > Network Agents** and click **Download Agent** to open the **Download** dialog, as shown in the following illustration.



2. In the **Download** dialog, select the organization or department to which you want to assign certificates discovered by the agent.
3. Select your server's operating system.
4. Click **Download.**

   If a network agent is already installed, the installation of a new network agent replaces the existing agent and all data related to the previous agent, including the local key store and all certificates, is lost.
5. To install the agent, right-click the setup file and select **Run as Administrator**. Alternatively, for Linux, run the installation from the command line using one of the following commands: `sudo ./ccmextraagentinstall-X64.bin` or `sudo ./ccmextraagentinstall-X86.bin`

   If the installer does not execute, ensure the binary has the following executable bit:

   ```
   sudo chmod 77 ccmextraagentinstall-X64.bin or sudo chmod 77 ccmextraagentinstall-X86.bin
   ```
6. Read the EULA, accept the terms of use by selecting **I Agree**, and click **Next**.

7. Select **Express** or **Custom** installation and click **Next**:
   - If you selected **Express**, click **Install > Finish**.
   - If you selected **Custom**, specify an install location for the network agent, click **Next**, and then make any required changes to the **Agent Properties** fields based on the information provided in the following table

Field	Description
Enter SCM Server's address	The URL of your SCM instance. This field is automatically populated and it should not be modified.
Enter Account's URI on Comodo Certificate Manager	The URI for your account configured by SCM. This field is automatically populated and it should not be modified. The URI of your SCM account is displayed at the end of your SCM instance URL. For example if the URL is `https://demo.cert-manager.com/customer/demo`, the last part after `customer` is the URI.
Enter the Secret Key[a]	An auto-generated authentication key for the purpose of connecting to SCM. You can enter an existing key, if required. After downloading the agent, it is displayed in the SCM interface with a status of N/A. You can modify the key by navigating to **Settings > Agents > MS Agents** in SCM, selecting the key and clicking **Edit**. This enables you to change the value of the **Secret Key** field to your preferred key, copy and store it. After you click **OK**, you can enter the copied key in the **Enter the Secret Key** field.
Enter the password for the KeyStore[b]	The password required for access to the KeyStore.

a. The Secret Key must be 10-128 characters.
b. The KeyStore password must be 10-128 characters.

8. Click **Next**.
9. Specify the **Enable CCM Extra Agent AutoUpdate** value. If selected, the network agent is automatically updated to new versions as they become available.
10. Click **Finish**.

Once the installation is complete, the agent is listed in SCM.

6.2.4 How to Configure the Agent for Auto-Installation, Renewal, and Internal Scanning

SCM can automatically install SSL certificates on servers. This can be done through the following agent configurations:

- **Local Controller Mode**—This requires an agent to be installed on each individual web server. The agents then communicate with SCM to coordinate automatic CSR generation and certificate installation. The agent polls SCM for certificate requests for servers that have

been enabled for automatic installation. If a request exists, it automatically generates a CSR for the web server and presents the application for administrator approval in SCM. After approval, the agent submits the CSR to Sectigo and tracks the order number. After issuance, the agent downloads the certificate and allows you to install it from the SCM interface. For more information, see "Configuring the Local Controller Mode" on page 257.

- **Central Controller Mode**—This requires a one-time installation of the agent software on a control server in your network. The agent communicates with each remote host and coordinates automatic CSR generation and certificate installation. The agent periodically polls SCM for certificate requests. If a request exists, the agent automatically generates a CSR for the web server and presents the application for approval via SCM. After approval, the agent submits the CSR to Sectigo and tracks the order number. After issuance, the agent downloads the certificate and enables you to install it from SCM. For more information see "Configuring Central Controller Mode" on page 259.

Auto-installation is available for all SSL certificate types.

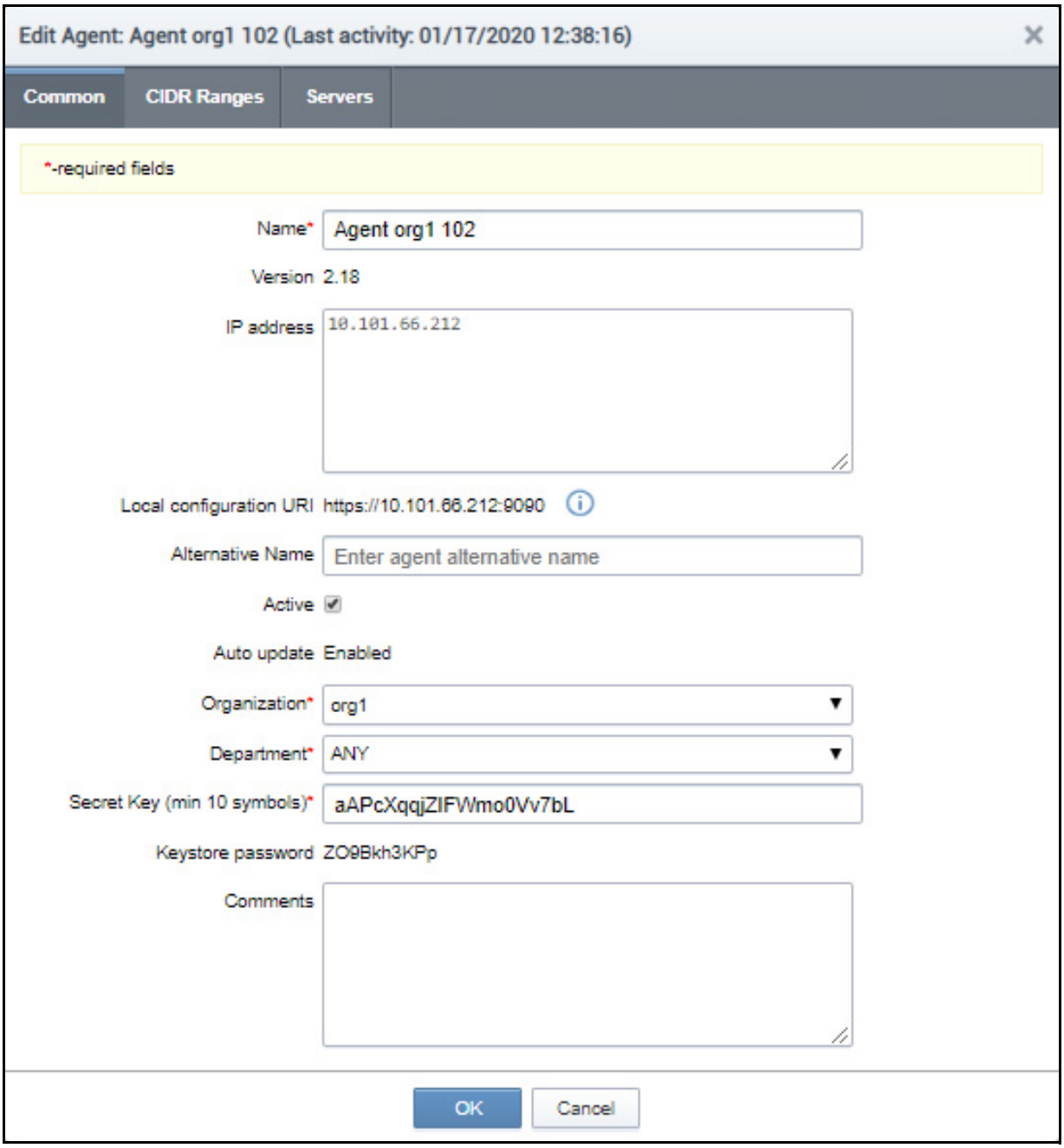
Before attempting to configure an agent for auto-installation and internal scanning, you need to define at least one organization. During setup, an organization must be designated as the owner of certificates discovered by the agent.

6.2.4.1 Configuring the Local Controller Mode

Local controller mode requires an agent to be installed on each web server upon which certificates are to be auto-installed or renewed. Once you have installed each network agent, you must configure each agent.

To configure an agent, do the following:

1. Navigate to **Settings > Network Agents**.
2. Select the agent from the list and click **Edit** to open the **Edit Agent** window, as shown in the following illustration**.**



3. Add or alter values required based on the information provided in the following table.

Field	Description
Name	The name of the agent.
Version	The version number of the agent.

Field	Description
IP Address	The IPv6 loopback address, IPv4 loopback address, IPV6 IP address, IPv4 IP address, or the physical address of the server on which the agent is installed.
Local Configuration URI	The IP of the server on which the agent is installed. This URL is used to access the agent via a web browser for managing.
Alternative Name	A brief description of the agent.
Active	Activates the agent.
Auto update	Enables the agent for auto-update.
Organization	The organization associated with the agent.
Department	The department associated with the agent.
Secret Key	The secret key generated by the agent to authenticate itself to the remote SCM server. The secret key must have 10 characters. You can copy and save the secret key in a safe location for use in a new agent, in case the agent has to be reinstalled in the same server, to authenticate itself to the SCM server for scanning the same internal network.
KeyStore password	The key store password generated by the agent. The network agent stores the SSL certificates and private keys in a Java KeyStore (JKS) file created on the agent. This password allows you to extract the certificates and private keys from the KeyStore, if required.
Comments	Descriptive comment on the purpose of the agent.

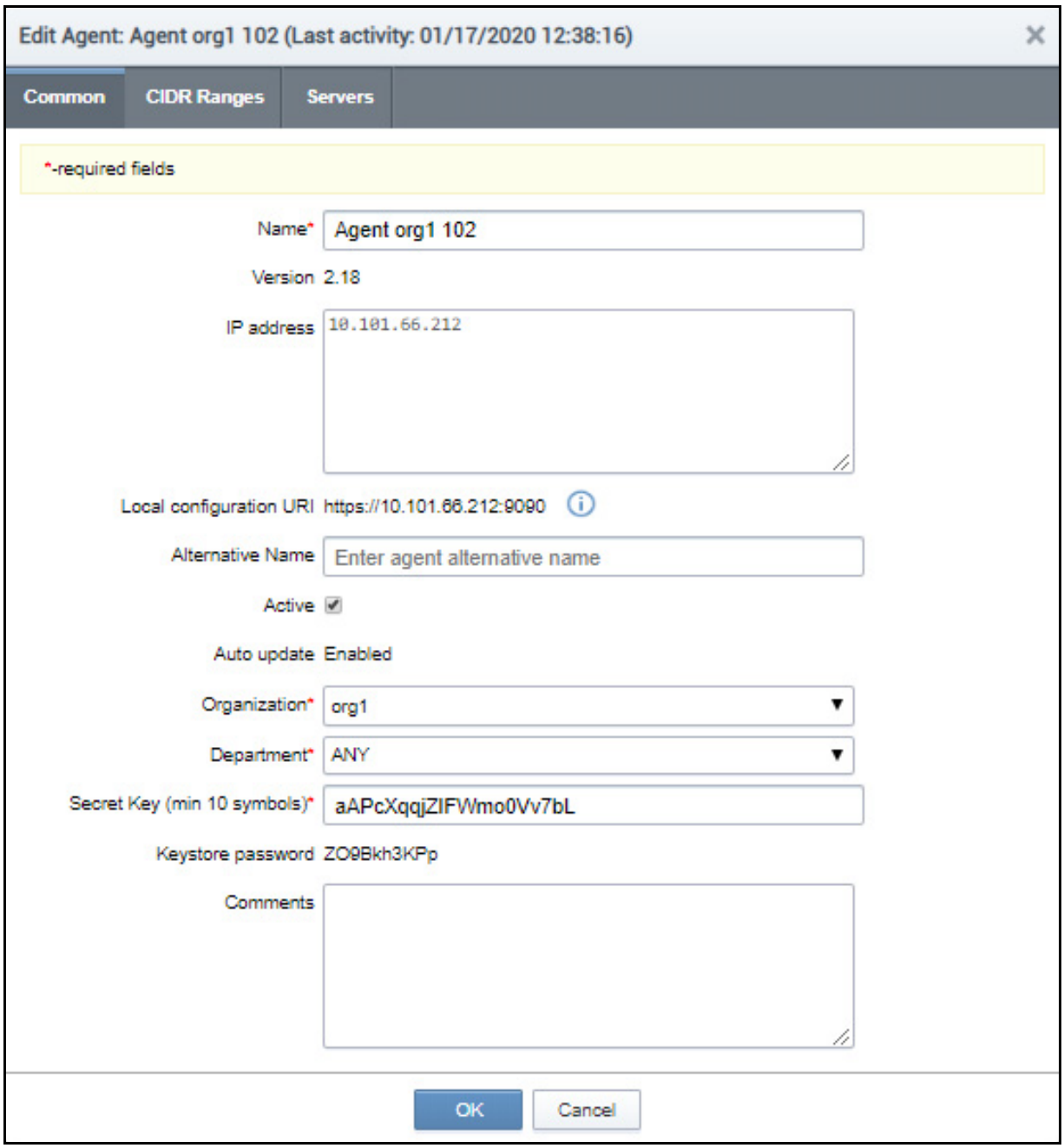
If you want to configure the agent for internal scanning, see "Configuring the Network Agent for Network Discovery Tasks" on page 263.

6.2.4.2 Configuring Central Controller Mode

You can enable central controller mode by adding remote servers in the network to enable agent communication with them. The agent polls SCM periodically for certificate requests for the remote servers. If a request exists, it automatically generates a CSR on the web server and present the application for administrator approval via SCM. On approval, the agent submits the CSR to Sectigo and tracks the order number. Once the certificate is issued by the CA, the agent downloads the certificate and enables the installation of the certificate from the SCM.

To add remote servers to the agent, do the following:

1. Navigate to **Settings > Network Agents**.
2. Select the agent from the list and click **Edit** to open the **Edit Agent** window, as shown in the following illustration**.**

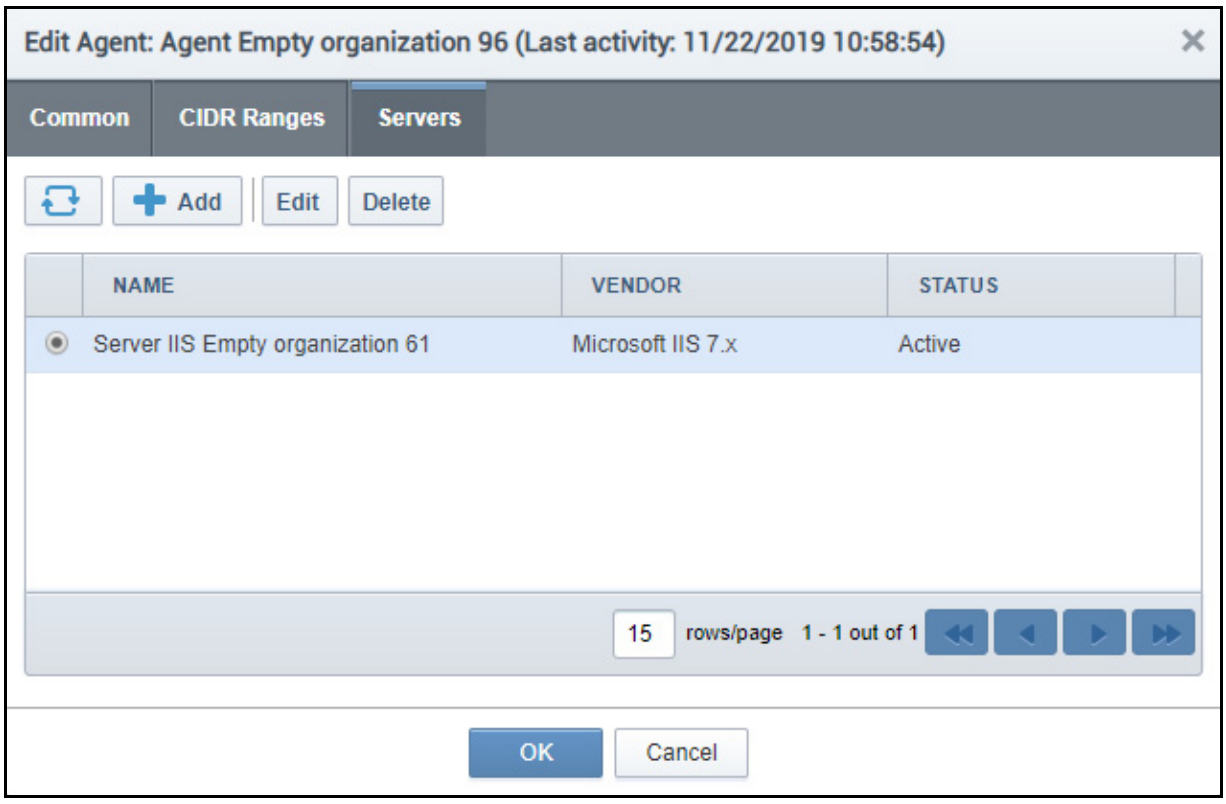


3. Add or alter values based on the information provided in the following table.

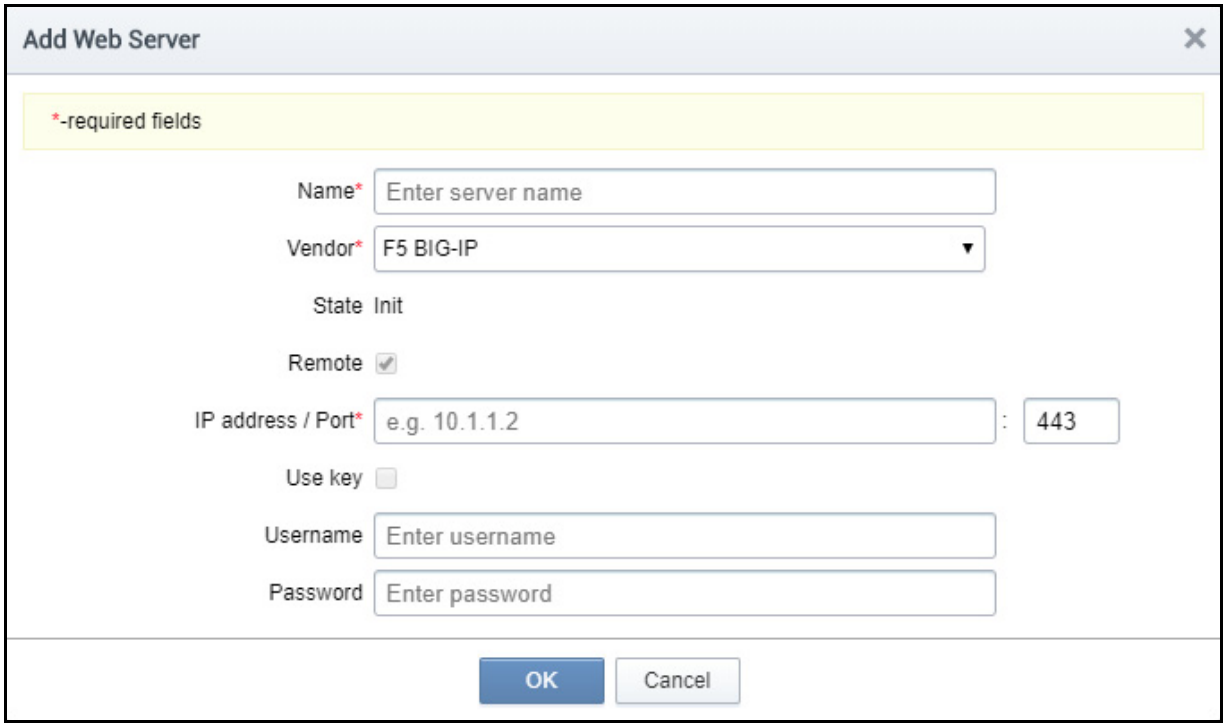
Field	Description
Name	The name of the agent.
Version	The version number of the agent.

Field	Description
IP Address	The IPv6 loopback address, IPv4 loopback address, IPV6 IP address, IPv4 IP address, or the physical address of the server on which the agent is installed.
Local Configuration URI	The IP of the server on which the agent is installed. This URL is used to access the agent via a web browser for managing.
Alternative Name	A brief description of the agent.
Active	Activates the agent.
Auto update	Enables the agent for auto-update.
Organization	The organization associated with the agent.
Department	The department associated with the agent.
Secret Key	The secret key generated by the agent to authenticate itself to the remote SCM server. The secret key must have 10 characters. You can copy and save the secret key in a safe location for use in a new agent, in case the agent has to be reinstalled in the same server, to authenticate itself to the SCM server for scanning the same internal network.
KeyStore password	The key store password generated by the agent. The network agent stores the SSL certificates and private keys in a Java KeyStore (JKS) file created on the agent. This password allows you to extract the certificates and private keys from the KeyStore, if required.
Comments	Descriptive comment on the purpose of the agent.

4. Select **Servers**, as shown in the following illustration.



5. Select a server and click **Add.** The **Add Web Server** dialog is shown in the following illustration.



6. Add values based on the information provided in the following table.

Field		Description
Name		The name of the server.
Vendor		The vendor of the server.
State		Indicates whether or not the server is connected. If the state is **Init**, the agent is in the process of connecting to the web server. Once connected, the web server is displayed as **Active**.
Remote		Indicates whether the server is remote or local. This should be selected when adding remote servers for agentless automatic certificate installation.
IP address / Port[a]		The IP address and connection port of the server for remote connection.
Use key[b]		Indicates whether or not the agent should use SSH key-based authentication to access the server.
Access Credentials	Username, Password[c]	The local administrator credentials required to log into the server.
	Private Key File Path[d]	The path to the SSH private key file required to access the server.

a. Visible only if **Remote** is selected.
b. Only applies to Apache servers and Tomcat web servers installed on Linux systems.
c. **Username/Password** are only enabled if **Use key** is not selected.
d. **Private Key File Path** is only enabled if **Remote** and **Use key** are selected.

Once added, a remote server state is displayed as **Init** (initialized). The agent discovers the newly added server and connects to it within a few minutes, at which point the server state changes to **Active** and the agent is configured to auto-install the certificates in the remote server as well as to scan the internal network. Next, the agent authenticates itself to the remote SCM server via combination of the secret key and awaits further instructions and starts polling SCM every minute to check for any instructions (for example, **Scan Now** command which, when activated, instructs SCM to instruct the agent to scan specific CIDRs. The agent performs this scan and sends the results back). The agent properties can be configured through the agent's web interface accessible at `http://<IP_address>/<host_name_of_the_server_on_which_the_agent_is_installed>:9090`. You can change the connection settings, polling interval, certificate management settings, and server settings from the web interface.

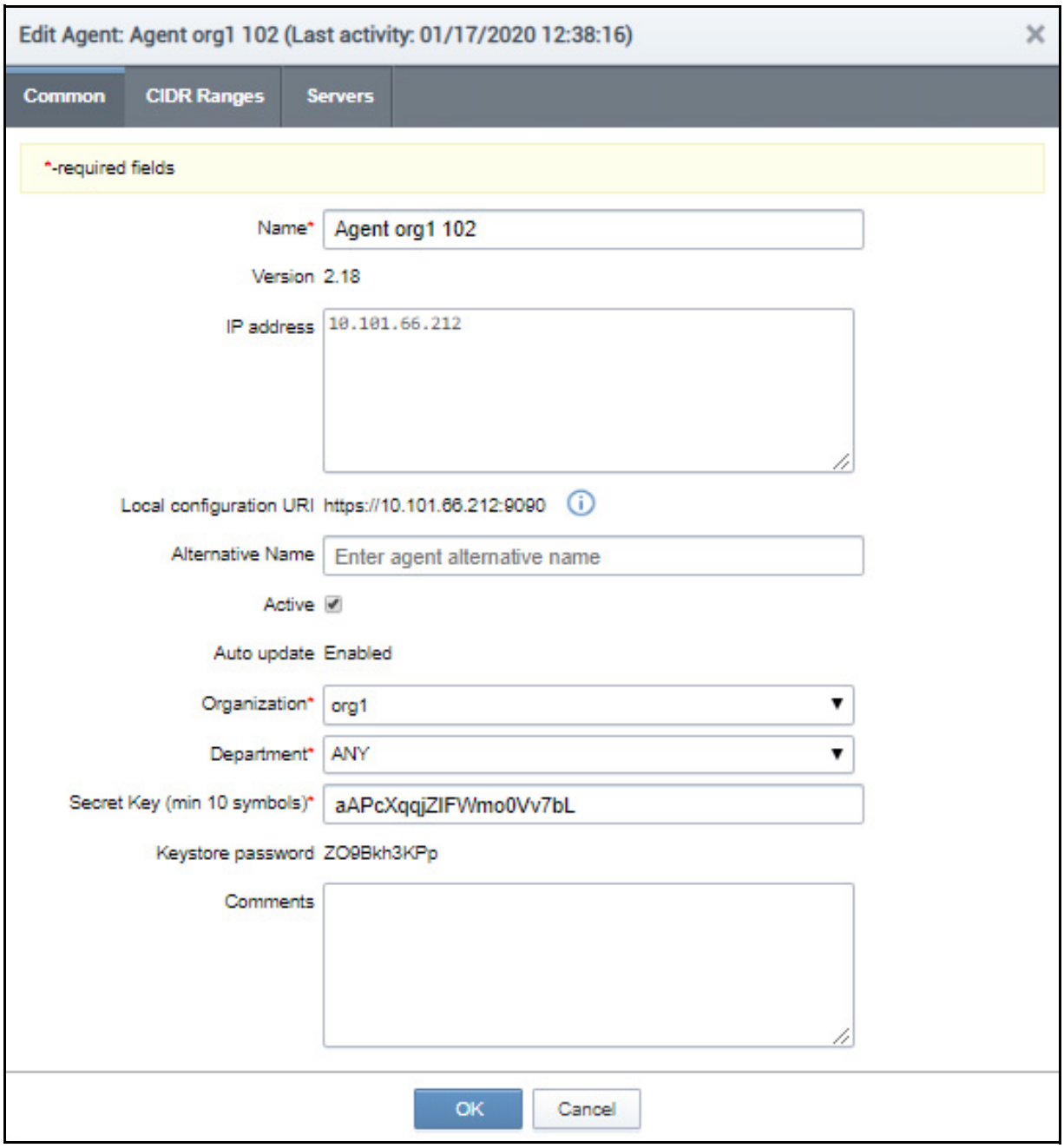
If you want to configure the agent for internal scanning, see "Configuring the Network Agent for Network Discovery Tasks" on page 263.

6.2.4.3 Configuring the Network Agent for Network Discovery Tasks

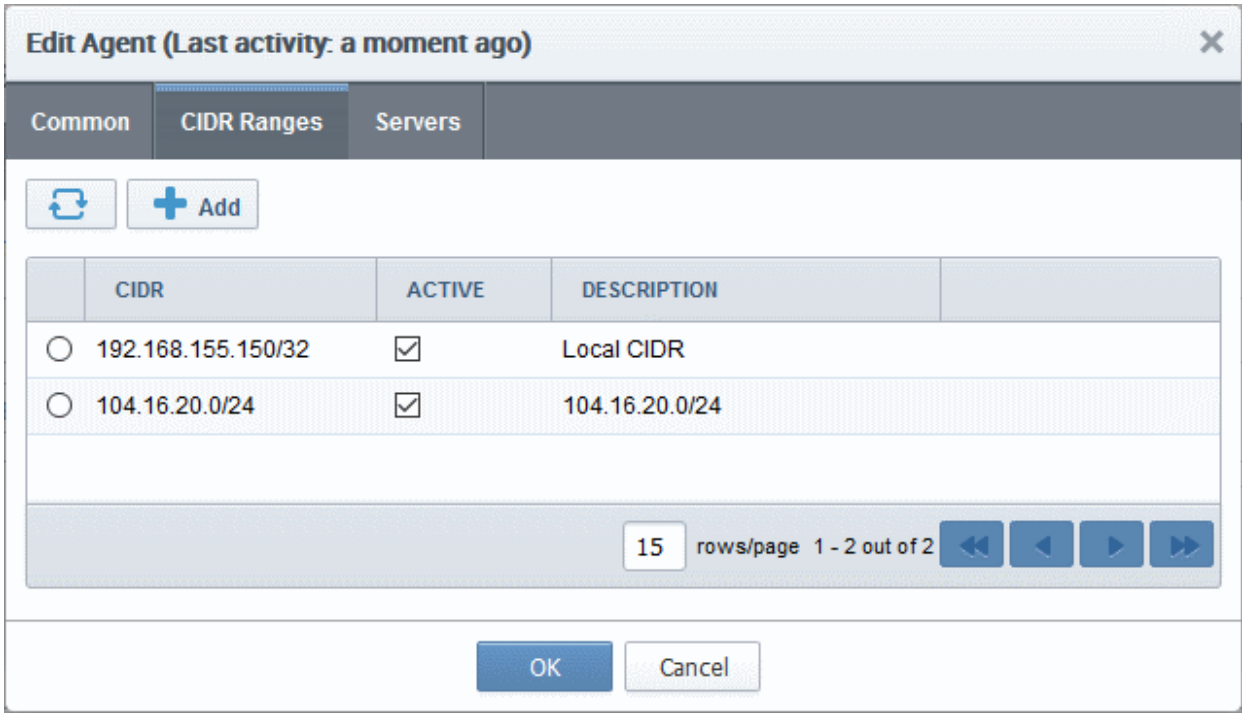
You can configure a network agent for SSL web server certificate discovery on networks. This is achieved by adding Classless Inter-Domain Routing (CIDR) ranges to an agent and performing manual or scheduled network scans.

To add CIDR ranges for scanning, do the following:

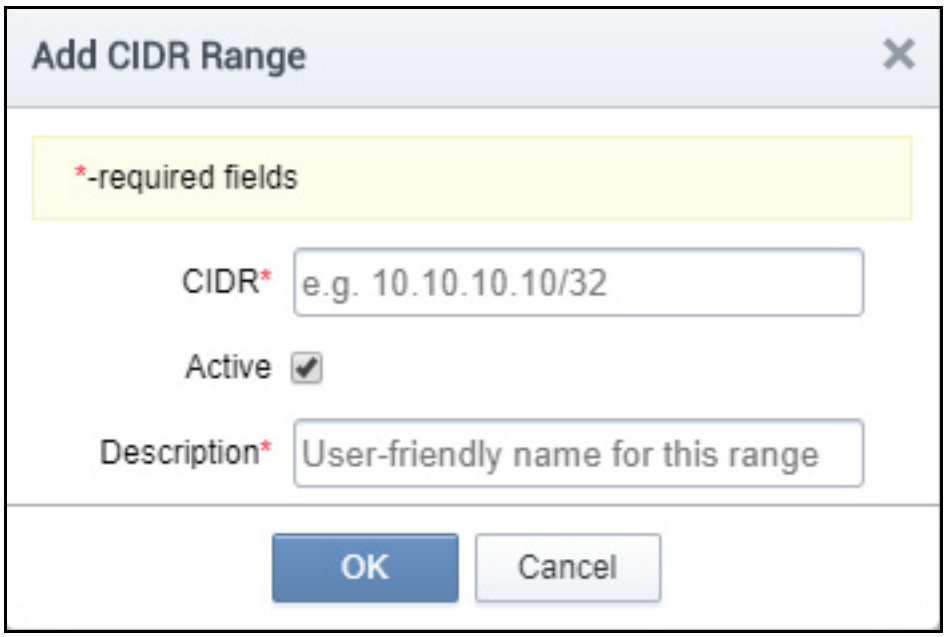
1. Navigate to **Settings > Network Agents**.
2. Select the agent from the list and click **Edit** to open the **Edit Agent** window, as shown in the following illustration**.**



3. Select **CIDR Ranges**, as shown in the following illustration.

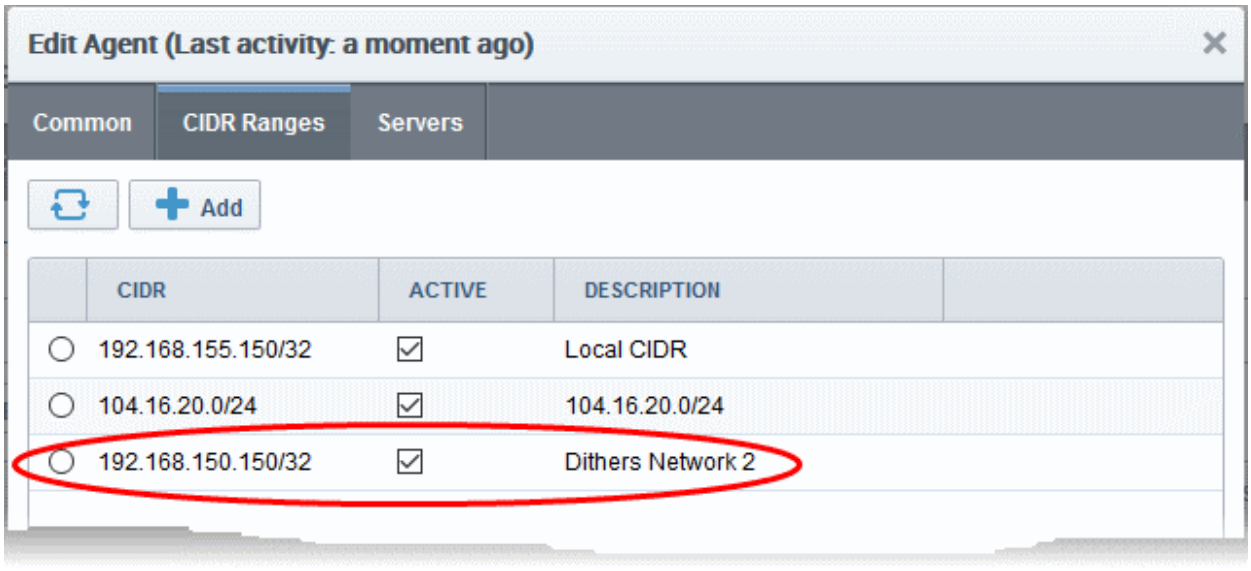


4. Click **Add** to open the **Add CIDR Range** dialog shown in the following illustration.



5. Enter the internal IP address range to scan.
6. Activate the agent by selecting **Active**.
7. Provide a description for the range.
8. Click **OK**.

Upon completion, the new CIDR range is added to the **CIDR Ranges** area, as shown in the following illustration.



NOTE: More ranges can be added by repeating this process.

Once you have added your required CIDR ranges, you can begin performing manual and scheduled scans. For more information, see "Performing Network Discovery Tasks" on page 540.

You can view certificate discovery scan results by navigating to **Reports > Discovery Scan Log**. Notice the newly discovered certificates that are added to the **SSL Certificates** area, as per the assignment rules defined for the discovery task. If no assignment rule has been applied, all external certificates are assigned to the organization or department that was specified for the agent. See "How to View Scan Results" on page 557 for more information.

Restrictions can be applied to limit the visibility and accessibility of network locations. See "Imposing Access Restrictions to the SCM UI" on page 361 for more information.

You can edit a CIDR range as follows:

1. Select the CIDR range and click the **Edit.**
2. Make any required changes in the **Edit CIDR Range** dialog.

You can delete a CIDR range as follows:

1. Select the CIDR range and click **Delete**.
2. Click **OK**.

6.3 Configuring MS Agents

You can add AD servers to SCM in order to fetch certificates installed on servers, devices, and endpoints, as well as for provisioning Device Authentication Certificates (DAC).

As a redundancy measure, SCM allows you to create clusters of MS agents installed on different AD servers to act as a single agent. If any agent fails, the other agents in the cluster seamlessly continue certificate discovery and provisioning through the AD server.

MS agents require the installation and configuration of MS Active Directory (AD) and AD Certificate Services (CS) role. It is recommended that you install the MS agent on a domain joined server where AD CS has not been configured. This is because AD CS can be installed automatically by an MS agent if it is not already set up on your system. For information on setting up AD CS, see https://social.technet.microsoft.com/wiki/contents/articles/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes.aspx.

MS AD certificate templates can be mapped to SCM certificate types for use with the CA Proxy feature.

6.3.1 MS Agent Hardware Requirements

The system requirements outlined in the following table must also be met prior to the installation of an MS agent.

Component		Requirement
Operating System		Windows Server 2008 R2/2012/2012 R2/ 2016 (Standard or later)
Workgroup		Domain joined
CPU	Minimum	1.4 GHz (dual-core) 64-bit processor
	Recommended	2.8 GHz (quad-core) 64-bit processor or greater
RAM	Minimum	4 GB
	Recommended	12 GB or greater
Internet Access		Yes
Storage	Minimum	60 GB
	Recommended	100 GB or greater

6.3.2 How to Install an MS Agent

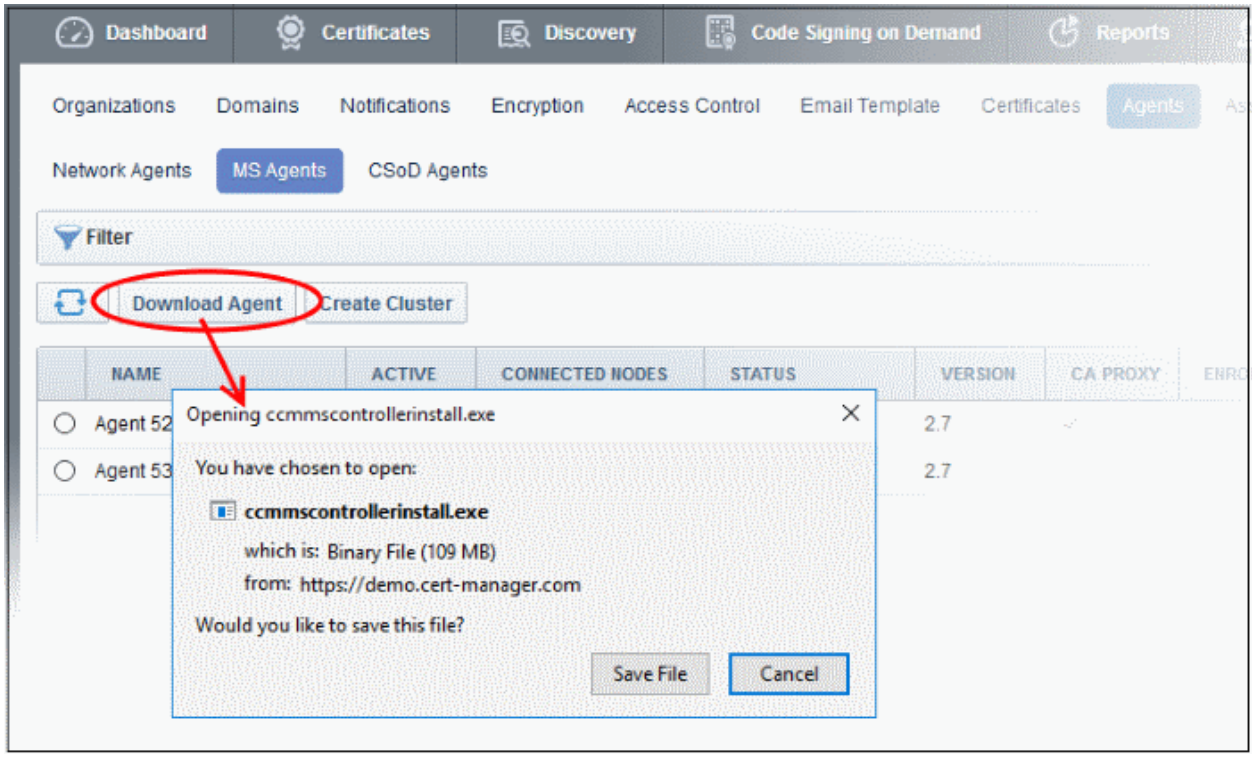
SCM administrators can install MS agents from SCM. Before the installation of an MS agent, the following requirements must be met:

- Supported Windows server platform (2008, R2, 2012, 2016)
- Server joined to the AD domain

NOTE: The system should not be co-located with any components that are part of the existing Microsoft CA.

You can download and install an MS agent as follows:

1. Navigate to **Settings > Agents > MS Agents** and click **Download Agent**, as shown in the following illustration.



2. Run the setup wizard and, in the first dialog, click **Next**.

   If an MS agent is already installed, the installation of a new MS agent replaces the existing agent and all data related to the previous agent is lost.
3. Read the EULA, accept the terms of use by selecting **I Agree**, and click **Next**.
4. Specify an install location for the network agent and click **Next**.
5. On the **CCM Ms Agent Mode** dialog, make selections based on the following information:
   - **Install MS Agent for Discovery Only**—Enables only the discovery of AD objects.
   - **Install SCM MS Agent as CA Proxy**—Device certificates are to be generated through NDES. It is suggested that you install the agent on a server without MS CA. This also enables the discovery of AD objects.
   - **Enroll on Behalf**—Device certificates are to be generated through MS CA. This also enables the discovery of AD objects.
   - **Install CCM Ms Agent as CA Proxy** and **Enroll on Behalf**—When both options are enabled, it is suggested that you install the agent on a server without MS CA. This also enables the discovery of AD objects.
6. Enter your Domain Administrator or Enterprise Administrator account credentials.

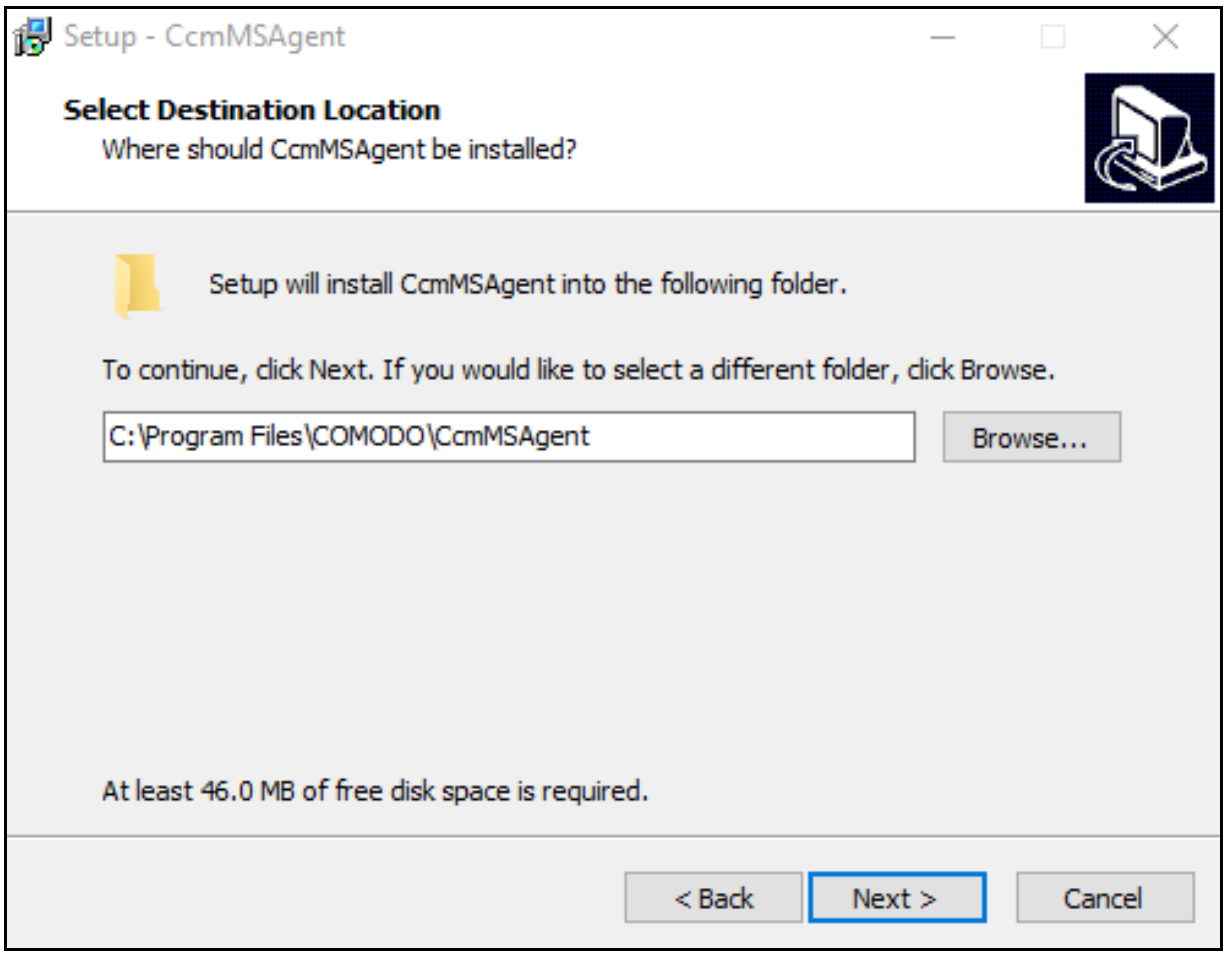
7. Make any required changes to the **Agent Properties** fields based on the information provided in the following table, and click **OK**.

Field	Description
Enter SCM Server's address	The URL of your SCM instance. This field is automatically populated and it should not be modified.
Enter Account's URI on Comodo Certificate Manager	The URI for your account configured by SCM. This field is automatically populated and it should not be modified. The URI of your SCM account is displayed at the end of your SCM instance URL. For example if the URL is `https://demo.cert-manager.com/customer/demo`, the last part after `customer` is the URI.
Enter the Secret Key[a]	An auto-generated authentication key for the purpose of connecting to SCM. You can enter a existing key, if required. After downloading the agent, it is displayed in the SCM interface with a status of N/A. You can modify the key by navigating to **Settings > Agents > MS Agents** in SCM, selecting the key and clicking **Edit**. This enables you to change the value of the **Secret Key** field to your preferred key, copy and store it. After you click **OK**, you can enter the copied key in the **Enter the Secret Key** field.

a. The Secret Key must be 10-128 characters.

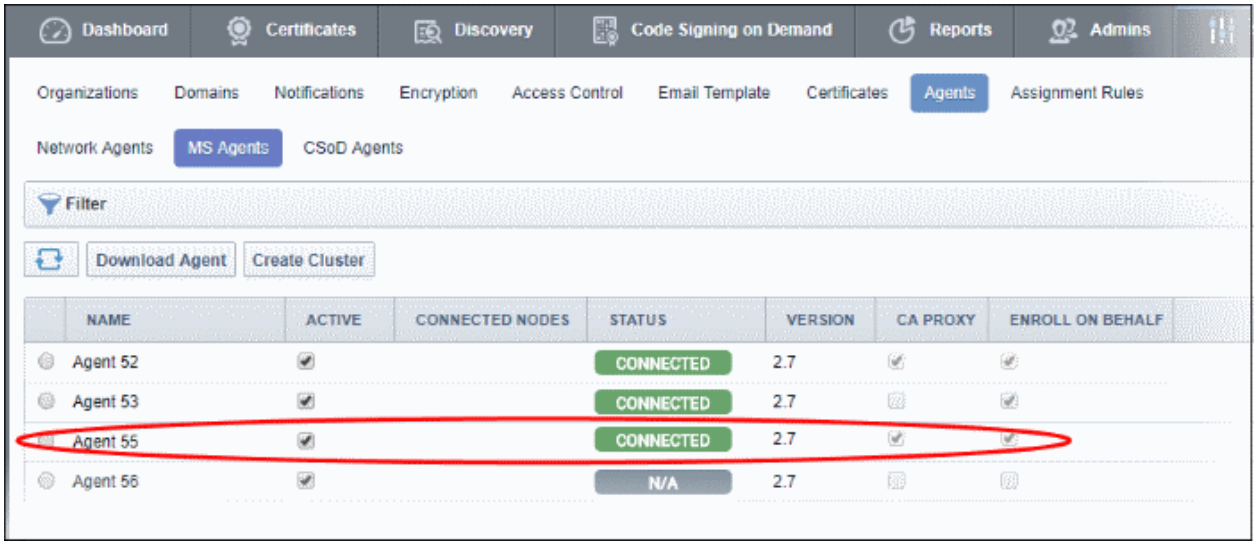
8. Specify the **Enable CCM Extra Agent Autoupdate** value. If selected, the network agent is automatically updated to new versions as they become available.

Specify a start menu folder via a dialog shown in the following illustration. The default location is `COMODO\ccmMSAgent`. You can select a different folder by clicking **Browse.**



9. Click **Next**.
10. Click **Install** and **Finish**.

Once the installation is complete, the agent is listed in SCM, as shown in the following illustration.



6.3.3 How to Enable Certificate Discovery

To enable certificate discovery, you start by downloading the MS agent by navigating to **Settings > Agents > MS Agents** and installing it on each AD server that is to be managed. Once installed, the agent periodically scans the server, fetches the network or object structure, detects all certificates on the domain, then forwards this information to the SCM server. The results can be viewed by navigating to **Discovery > Network Assets**. See "Performing the AD Discovery Tasks" on page 560.

NOTE: The MS agent can be configured to hide various AD details when discovering certificates. For information on hiding AD details, contact your Sectigo account manager.

6.3.4 How to Configure MS AD Certificate Templates for Use With Enroll on Behalf

An Enterprise Administrator or Domain Administrator can create custom certificate templates on their AD server for use with the Enroll on Behalf feature.

The procedure for creating new MS AD certificate templates depends on your version of the Windows Server platform. For more information on creating new MS AD certificate templates, see https://docs.microsoft.com.

6.3.4.1 Setting Up MS AD Certificate Templates for Enroll on Behalf

Prior to starting the template creation, an MS agent should be installed on the AD server. The agent must be configured for use with the **Enroll on Behalf** feature. For more information, see "Configuring MS Agents" on page 266.

The following settings are for user and computer-based templates for the SCM **Enroll on Behalf** feature.

To create the template, do the following:

1. Open the Windows command prompt.
2. Run the `certtmpl.msc` command.

3. Right click on an existing template and click **Duplicate**.
4. Complete all the fields based on the information provided in the following table [1].

Tab	Field	Description	Setting
General	Template display name	The name to be displayed for the certificate template.	No requirement
	Validity period	The validity term for certificates created using this template.	1 year (suggested)
	Renewal period	The period of time before certificate expiry during which auto-renewal can be triggered if re-enrollment is supported.	6 weeks (suggested)
Compatibility	Show resulting changes	Shows which other settings will or will not be available if a particular selection is made during template configuration.	Selected (suggested)
	Certification Authority	The version of Windows Server supported by the MS agent.	Most recent (required)
	Certificate recipient	The OS and version of Windows Server used in your environment.	Most applicable
Security	Group or user names	The users or groups with access to the template.	Domain Admins added (required)
	Permissions for Authenticated Users	The permissions approved or denied for each user or group with access to the certificate template.	**Read** and **Enroll** allowed (required) **Full Control** (suggested)
Request Handling	Purpose	The function served by certificates created using this template.	Signature and encryption
	Allow private key to be exported	When selected, private keys can be exported to a location other than the local certificate storage.	Selected
	Enroll subject without requiring any user input	Allows for auto-enrollment without any user interaction.	Selected

1. The table covers only the required and suggested settings for the new certificate template. If your final template does not function as intended, contact Sectigo support.

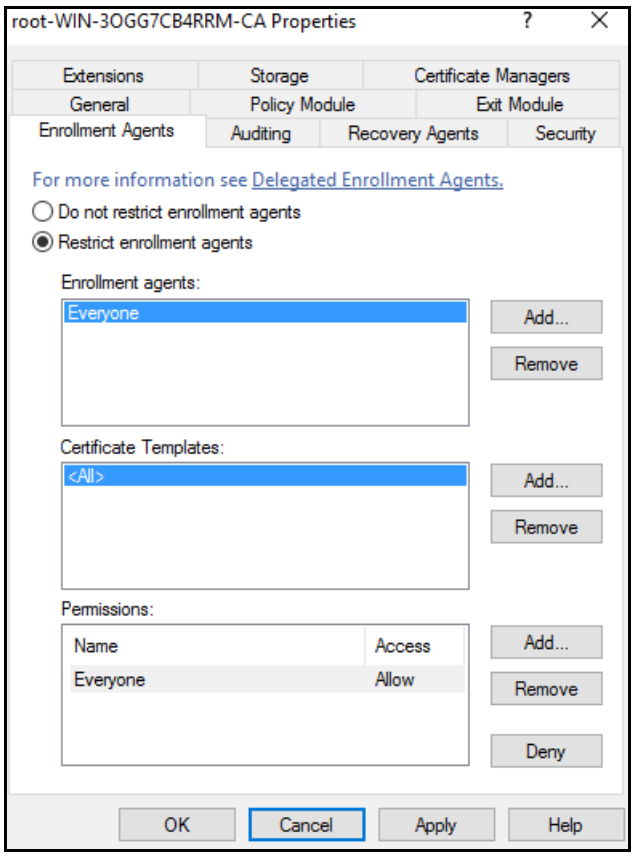
5. For user-based templates, click **OK** and then follow instructions from "Setting Up the CA Properties for Enroll on Behalf" on page 273. For computer-based templates, continue configuring the fields based on the information provided in the following table.

Tab	Field	Description	Setting
Subject Name	Build from this Active Directory information	When selected, the **Subject Name** is automatically populated based on the selection in the **Subject name format** field.	Selected
	Subject name format	The AD field from which the certificate **Subject Name** is generated.	DNS name
	E-mail name	When selected, the user's email is included in the **Subject Alternate Name (SAN)** field.	Selected
Issuance Requirements	This number of authorized signatures	The number of signatures required before certificates created using this template can be issued.	Minimum 1
	Policy type required in signature	Specifies the application policy that must be included in the signing certificate used to sign the requested certificate.	Application policy
	Application policy	Specifies the issuance policy that must be included in the signing certificate used to sign the requested certificate.	Certificate Request Agent
	Same criteria as for enrollment	When selected, certificate renewal has the same requirements as certificate enrollment.	Selected

6.3.4.2 Setting Up the CA Properties for Enroll on Behalf

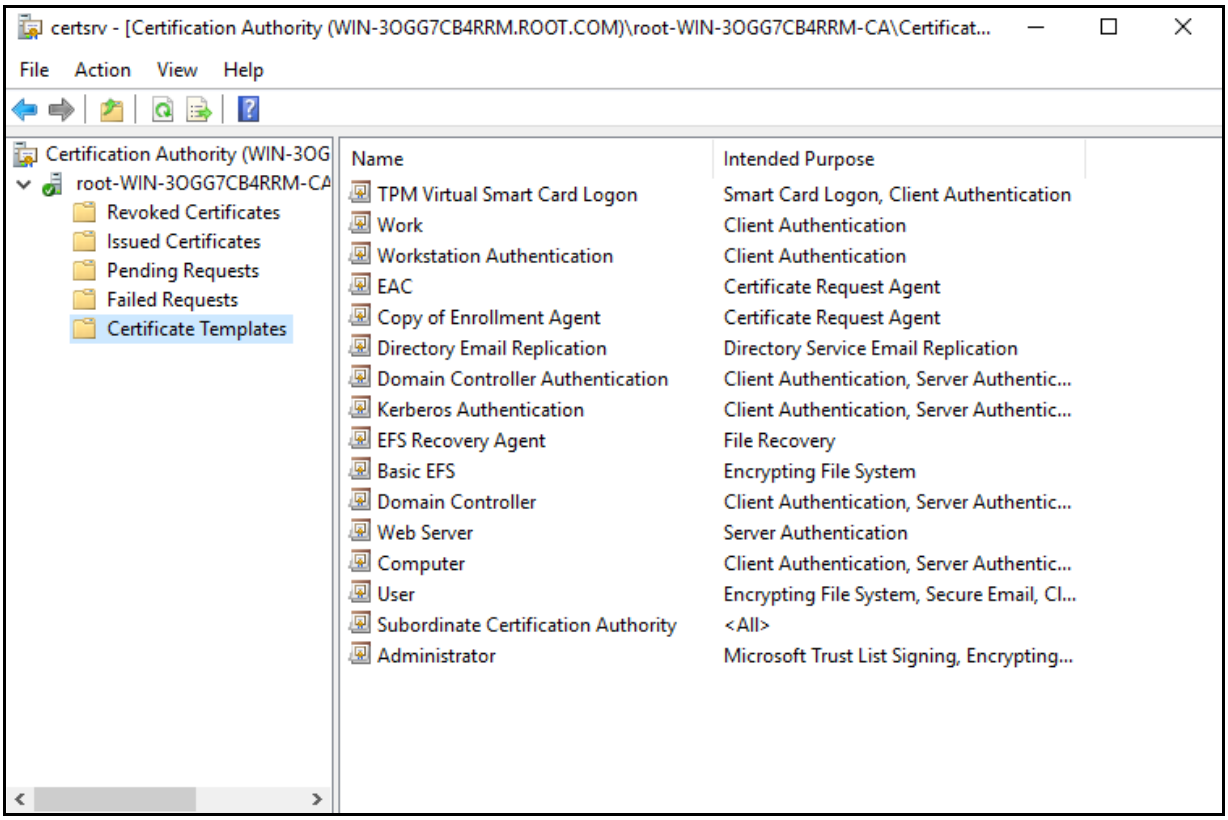
You can configure the CA properties as follows:

1. Open the Windows command prompt.
2. Run the `certsrv.msc` command.
3. Right-click the CA name and navigate to **Properties** > **Enrollment Agents**.
4. Select **Enrollment Agents**, as shown in the following illustration, and then complete the fields based on the information provided in the following table.

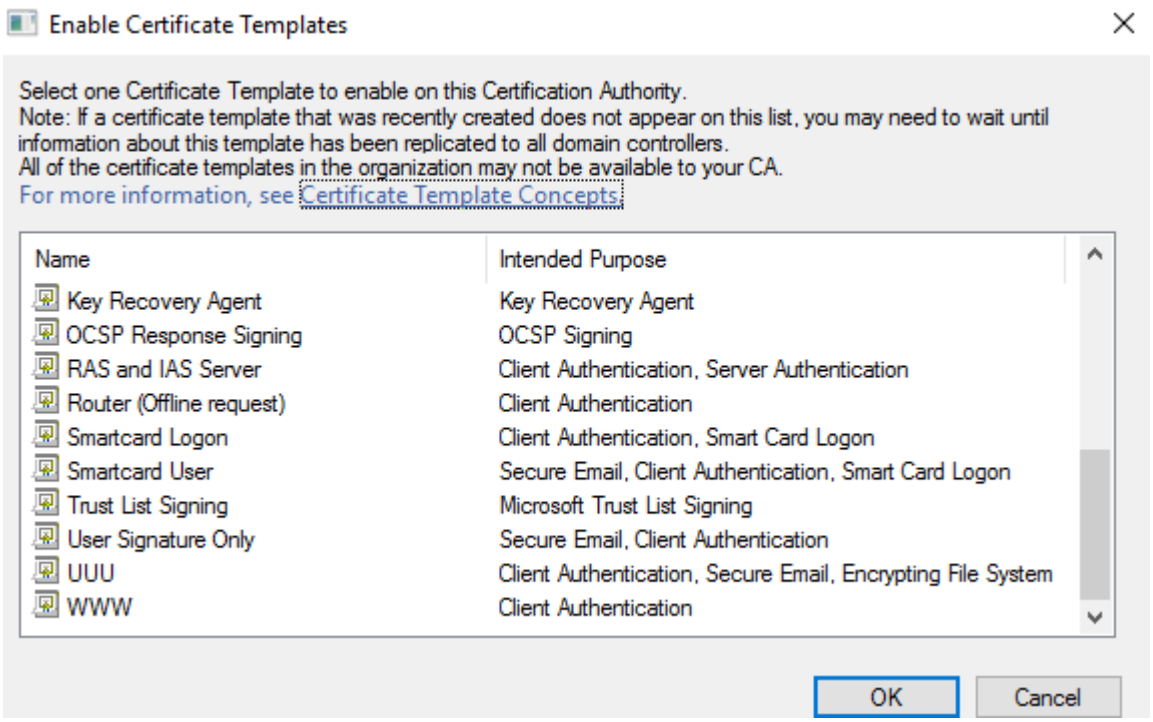


Field	Description	Setting
Restrict enrollment agents	Restrict users or agents who can enroll for a certificate on behalf of another agent.	Selected
Enrollment agents	The users or agents who are authorized to enroll for a certificate on behalf of another client.	Everyone
Certificate Templates	The MS AD certificate templates that can be used by the CA and enrollment agents.	All
Permissions	The permissions assigned to the users or agents authorized in the **Enrollment agents** field.	Everyone: Allow

5. Click **OK**.
6. Double-click the CA name and click **Certificate Templates**, as shown in the following illustration.



7. Right-click within this file list area and click **New > Certificate Template to Issue**.
8. Add to the CA the template that you modified earlier.

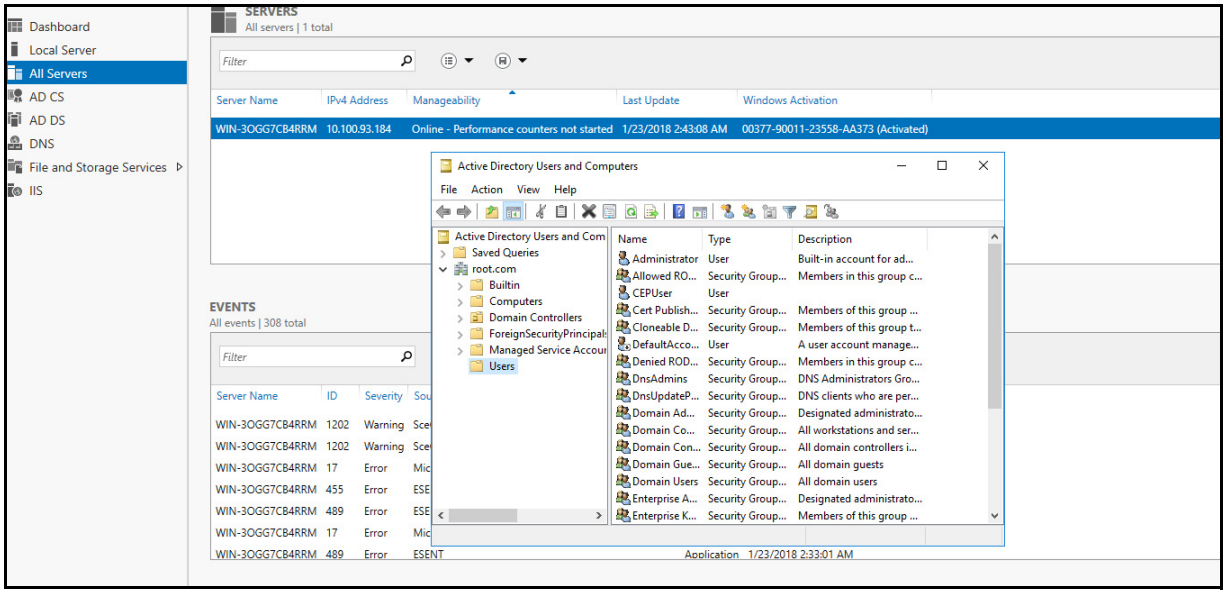


9. Restart the CA server.

6.3.4.3 Setting Up the Requester Properties for Enroll on Behalf

You can configure the requester properties as follows:

1. Open **Server Manager**.
2. In the left panel, select **All Servers**.
3. Right-click any CA server name and select **Active Directory Users and Computers**.
4. If required, change the domain to get the one that matches the user specified as Domain Administrator during MS agent installation.
5. Select the **Users** sub-menu (or the relevant organization unit) for this domain (that matches the user which was specified as Domain Administrator during MS agent installation), as shown in the following illustration.



6. Right-click on the administrator who was specified as Domain Administrator during MS agent installation (who provisions the certificate requests), and click **Properties**.
7. Configure the **Administrator Properties** fields based on the information provided in the following table:.

Tab	Field	Description	Setting
General	First Name	The administrator's first name.	No requirement
	Last Name	The administrator's surname.	No requirement
	Description	A description providing additional information about the administrator.	No requirement
	E-Mail	The administrator's email.	Required
Member Of	Member of	The groups that the administrator is included in.	Member of **Domain Admins** group

6.3.5 How to Map MS AD Certificate Templates to SCM Certificate Types

SCM can issue private certificates with custom parameters by mapping SCM certificate types to custom AD certificate templates.

Prior to starting the process, the MS agent should have been installed on the network server of the organization or department from which the templates are to be mapped and an appropriate MS AD certificate template must have been created. For more information, see "Configuring MS Agents" on page 266.

NOTE: Private certificates must be enabled for your account in order to map them to MS AD templates. Contact your account manager for more information.

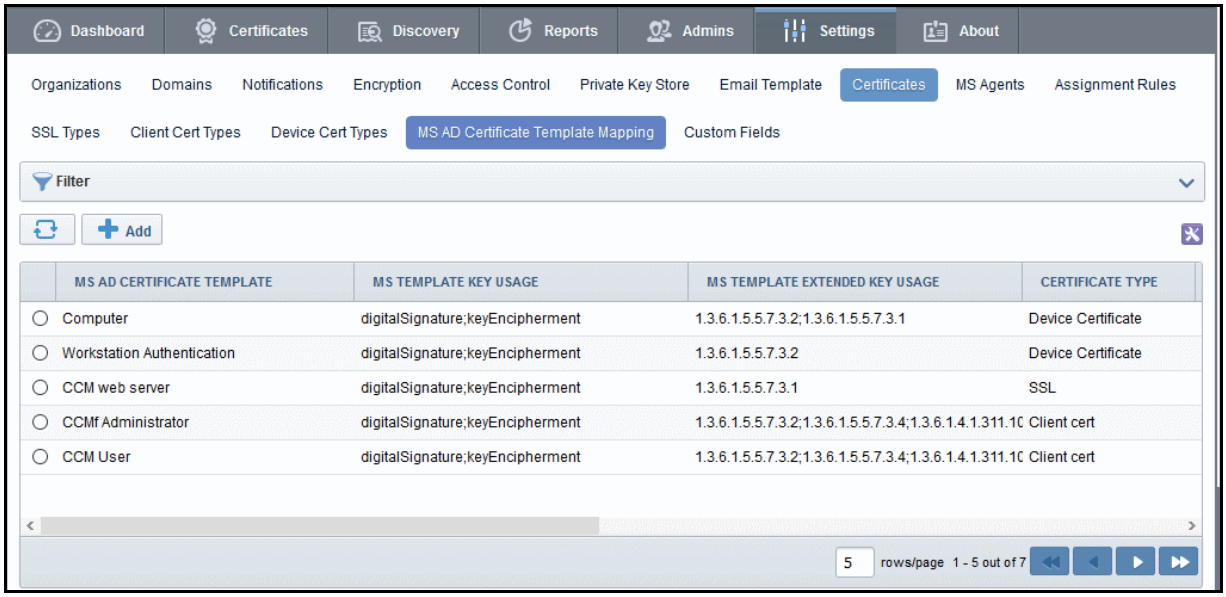
Certificate types with mapped templates can only be enrolled through an AD server using the certificate enrollment service or a group enrollment policy.

For SSL certificates, SCM currently only supports MS AD template mapping for the Private UCC SSL certificate type.

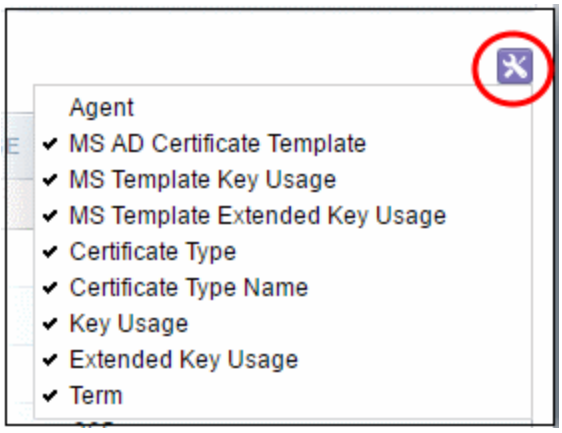
For device certificates, you can request your account manager to add private CAs to your account and create device certificate types, as required based on information accessible by navigating to **Settings > Certificates > Device Certificate Types**. For more information, see "Adding Device Certificate Types" on page 498. These device certificate types can be mapped to MS AD certificate templates.

6.3.5.1 Viewing Mapped MS AD Certificate Templates

The **MS AD Certificate Template Mapping** area shown in the following illustration allows you to add certificate templates available on an AD server to SCM and map appropriate certificate types to them. Templates can also be updated or deleted later.



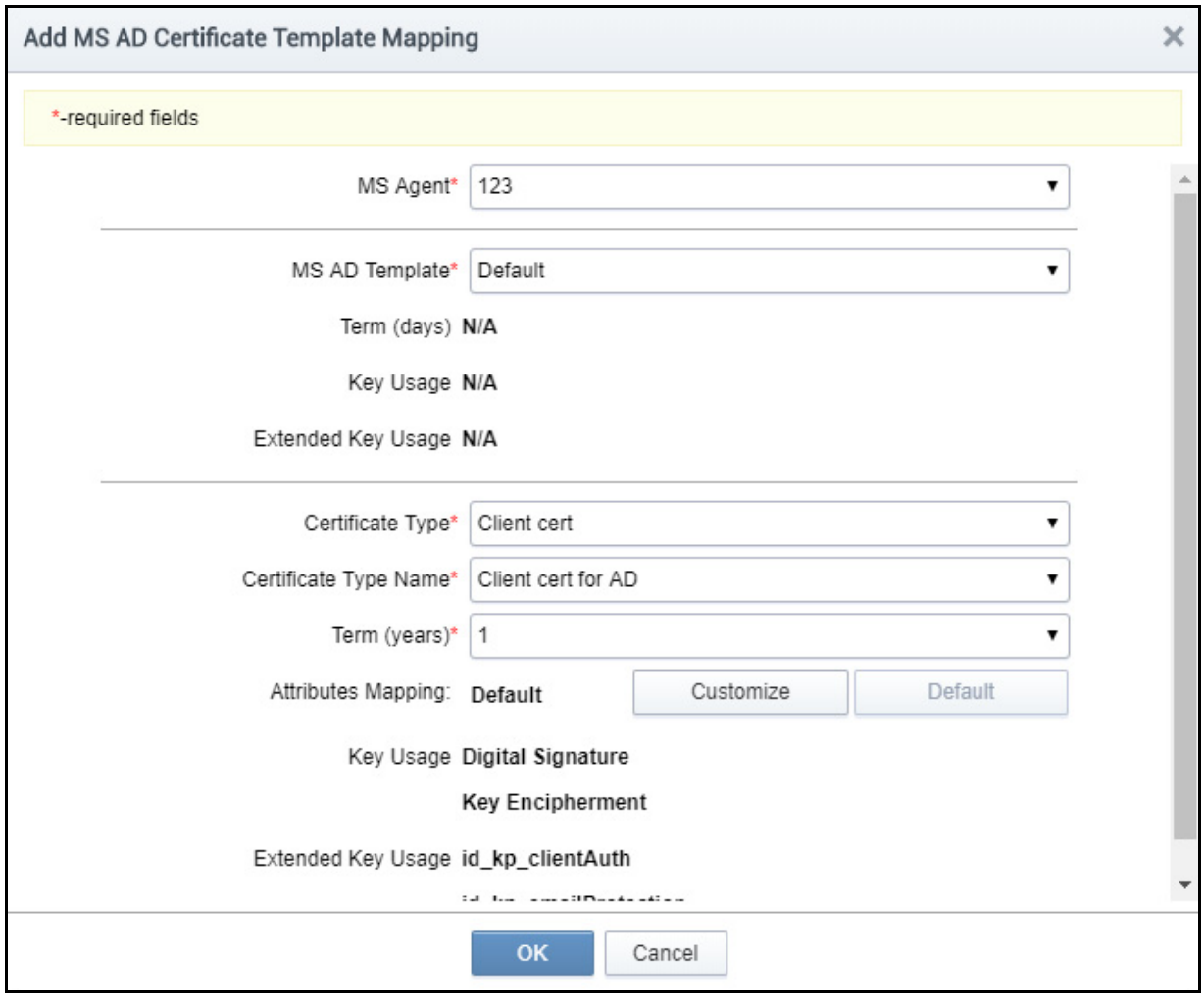
The following table lists settings and elements of the **MS AD Certificate Template Mapping** area.

Field / Element		Description
MS AD Certificate Template		The name of the certificate template in the AD server.
MS Template Key Usage		Key usage defined in the certificate template.
MS Template Extended Key Usage		Extended key usage defined in the certificate template.
Certificate Type		Certificate type configured for the certificate template.
Certificate Type Name		The name of the certificate type configured for the certificate template.
Key Usage		Key usage defined for the certificate.
Extended Key Usage		Extended key usage defined for the certificate.
Term		The validity period of the certificate.
You can use the tool button to select columns to be displayed in the table:  		
Control Buttons	Add	Allows MRAOs to add a mapped certificate template on an AD server to SCM.
	Refresh	Refreshes the list.
	Edit	Allows you to modify the certificate type for the certificate template. Visible only when a certificate template is selected.
	Delete	Deletes the mapped certificate template from the list. Visible only when a certificate template is selected.

6.3.5.2 Adding MS AD Certificate Template Mapping

MRAO administrators can add certificate templates from AD servers to SCM in order to define a certificate type for that template. You can add an AD certificate template as follows:

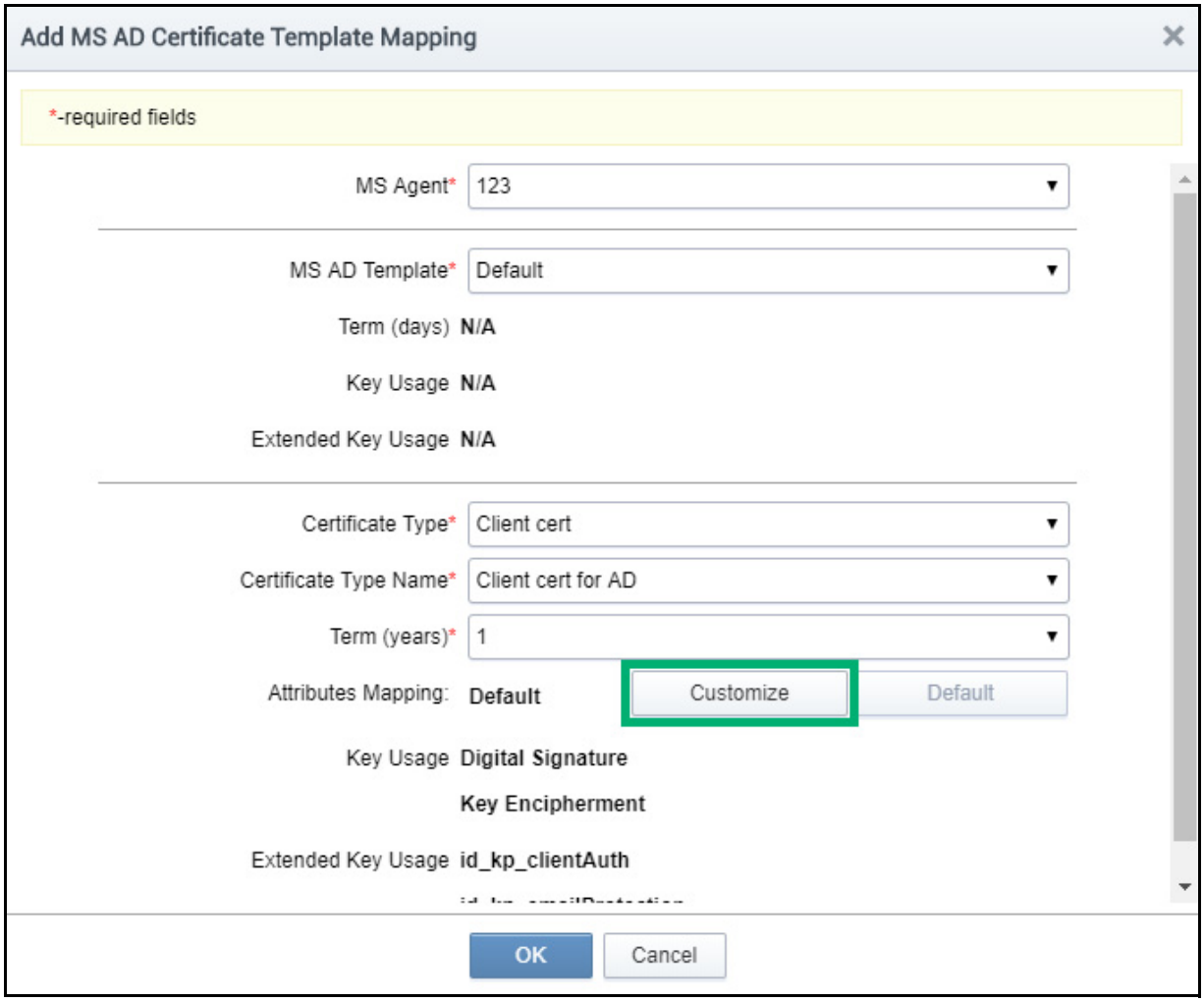
1. From the main UI, navigate to **Settings > Certificates > MS AD Certificate Template Mapping** and click **Add**.
2. Complete the **MS AD Certificate Template Mapping** dialog shown in the following illustration using field descriptions provided in the table.



Field / Element	Description
MS Agent	An MS agent through which a certificate request is brought from MS AD to SCM.
MS Template	The configured and mapped certificate template found on the AD server.
Term	The validity period of the certificate, as defined in the selected template.
Key Usage	Key usage defined in the selected template.
Extended Key Usage	Extended key usage defined in the selected template.
Certificate Type	The type of the certificate that is requested using this template. The valid values are SSL, Client Certificate, Device Certificate.

Field / Element	Description
Certificate Type Name	The name of the Sectigo certificate type configured to be issued when a certificate request is brought into SCM by the selected MS agent.
Term	The validity period configured for the selected Sectigo certificate type in SCM.
Attributes Mapping	When Client Certificate is the selected Certificate Type, attributes brought from MS AD can be mapped to equivalent values in SCM. This mapping can override settings specified in the MS AD Certificate Template.
Key Usage	The key usage of the Sectigo certificate type, as defined in SCM.
Extended Key Usage	The extended key usage of the Sectigo certificate type, as defined in SCM.

3. For client certificates, click **Attributes Mapping > Customize** on **MS AD Certificate Template Mapping** dialog, as shown in the following illustration, and then complete the fields based on the information provided in the table.



4. Complete the **Attributes Mapping** fields based on the information provided in the following table.

Field / Element		Description
Attribute		Indicates the terms utilized by SCM. Click on an attribute to select from a list of predefined attributes used in SCM.
	Common Name	Generally the domain to which the certificate is to be issued. An email can also be included in the CN field. The maximum allowed character length for this field is 64.
	DNS	DNS hostname.
	Department Name	The name of the department in which the user works.
	Email	The email address of the user. If the **Email** attribute is mapped to a value and **Send to CA** is selected, the user's email address is included in the certificate's **Subject** and **SAN** fields.
	First Name	The user's first name.
	Last Name	The user's surname.
	Organization Name	The name of the company for which the user works.
	SPN	The unique identifier of the service instance.
	Secondary Email	Additional email address for the user.
	UPN	The email address that should appear as principal name in the certificate to be issued. For the organizations or departments enabled for principal name support, the client certificates issued to the end-users of the organization or department include an additional name: **Principal Name**, in addition to the RFC822 name in the **Subject Alternative Name (SAN)** field.
	Contact Phone	The phone number provided for the user.
Value		Indicates the equivalent terms utilized in MS AD or a static value unrelated to MS AD. When you start typing a value, a list of suggested AD attributes is populated. If a static value is used, it must be encased in quotation marks.

Field / Element		Description
Send to CA		Allows for attributes to be included (selected) or excluded from (not selected) the transition of the incoming request to the CA. If a check box is disabled (grayed out), it means that the attribute is mandatory for the CA and must be included in the request.
Controls	Add	Adds an SCM attribute to be mapped. Duplicate attributes are not permitted.
	Reset	Resets all attributes and values to the default customized mapping.
	Delete	Prevents the attribute from being populated in the **Person** profile and from being included in the certificate request sent to Sectigo. Some attributes represent a mandatory detail of the connected **Person** profile and cannot be deleted.

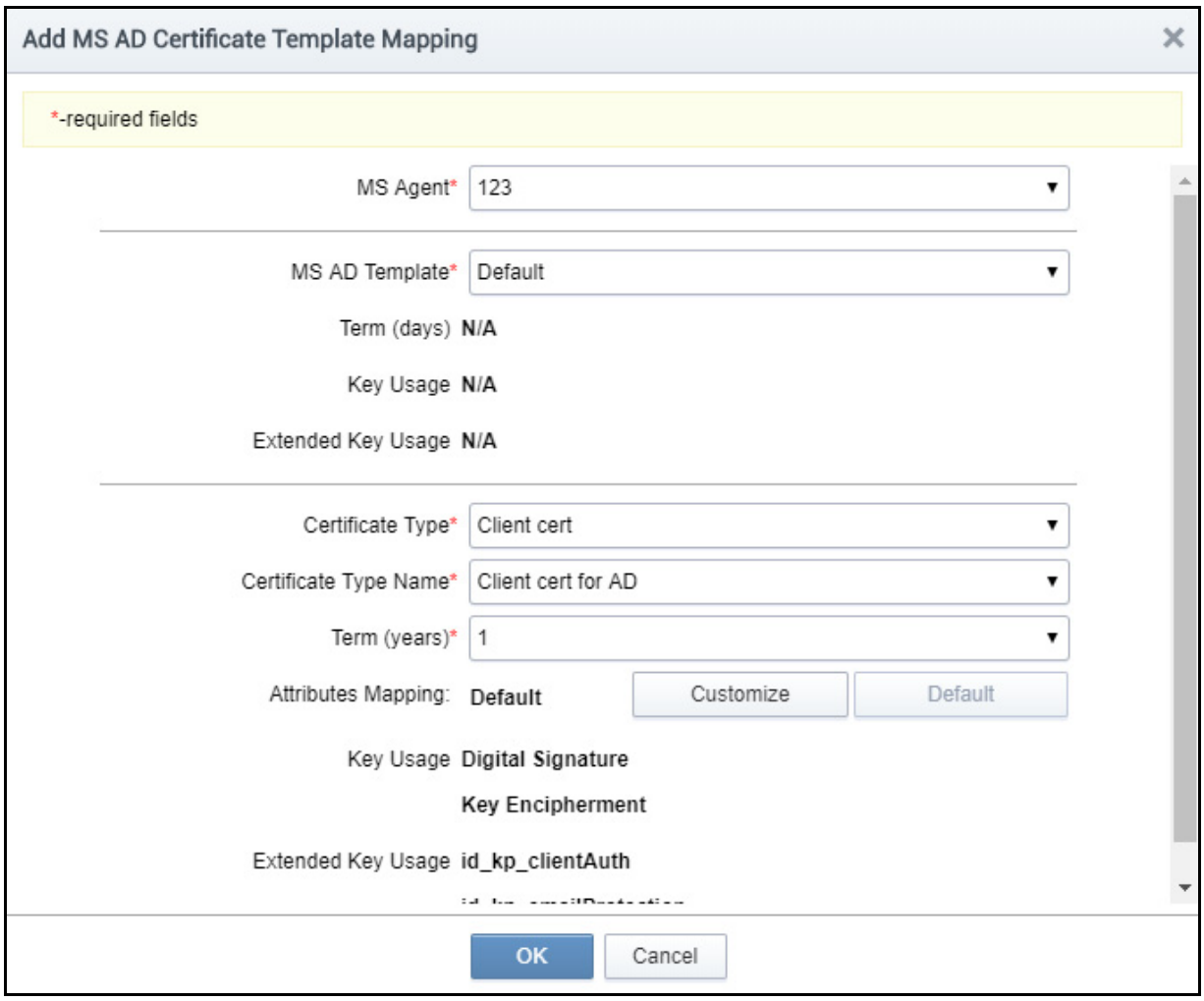
5. Click **OK**.

6.3.5.3 Modifying an MS AD Certificate Template

An existing AD certificate template can be updated at any time to adhere to your requirements. You can edit an AD certificate template as follows:

1. Navigate to **Settings > Certificates > MS AD Certificate Template Mapping**, select a template, and then click **Edit**.
2. Complete the **Edit MS AD Certificate Template Mapping** dialog shown in the following illustration using the field descriptions provided in "Adding MS AD Certificate Template Mapping" on page 278.

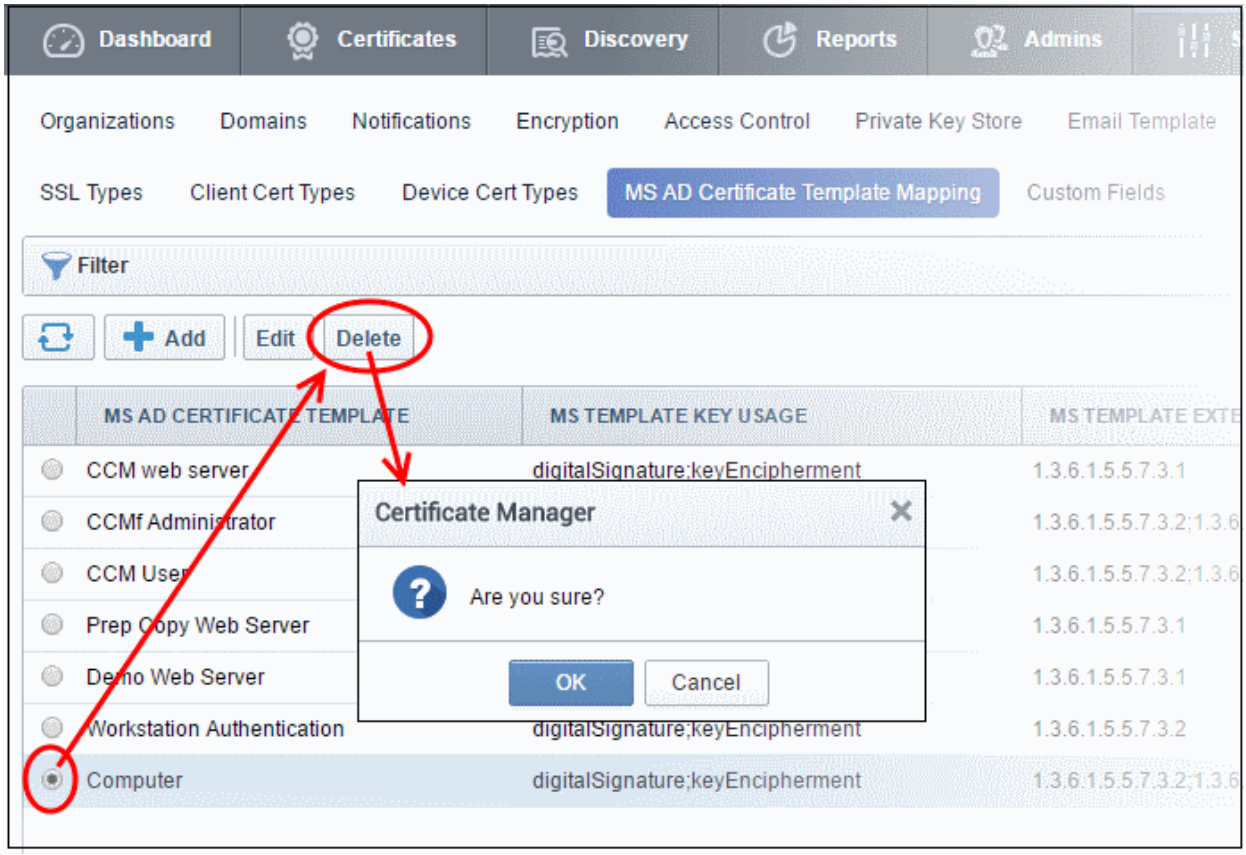
   NOTE: The **MS Agent** field is read-only when editing an existing MS AD certificate template.



6.3.5.4 Deleting MS AD Certificate Templates

A certificate template can be deleted from the list when it is no longer required, as follows:

- From the main SCM UI, navigate to **Settings > Certificates > MS AD Certificate Template Mapping**, select a template, and then click **Delete**, as shown in the following illustration.



6.3.6 How to Enable Provisioning of Device Authentication Certificates

MS agents installed on AD servers can be used to provision certificates from MS CA and act as a CA proxy.

To provision device authentication certificates via CA proxy, the AD server must have an integrated Network Device Enrollment Service (NDES) and a group policy for enrolling device certificates for devices added to AD. Once done, the MS agent receives certificate requests and forwards them to SCM. The agent tracks all orders and, after the device certificate has been issued by SCM, collects the certificate and forwards it to the NDES server. The NDES server, in turn, forwards the certificate to the device. See "Managing Device Certificates" on page 181 for more information.

In order for the MS agent to act as a CA proxy, that role must be enabled during the agent installation.

To provision device authentication certificates via MS CA, the agent should be enabled for this feature during its installation. To do so, ensure that **CA Proxy** setting is disabled. If you accidentally enable it, the agent changes the certificate service from MS CA to CA proxy. Once installed, you can request certificates from MS CA by navigating to **Certificates > Device Certificates**, clicking **Enroll with MS CA** and completing the authentication process.

After certificate issuance, you can manage the certificate as you usually do by performing such tasks as downloading, viewing, revoking them, and generating reports.

6.3.7 How to Configure a Standalone MS Agent for Certificate Discovery and Issuance via AD Servers

Installing an MS agent on your AD server allows you to discover certificates on AD objects and issue certificates to AD-connected devices. You have the option to generate device certificates using the proxy CA or MS CA.

For the configuration to succeed, the following server requirements must be met:

- To generate device certificates from a single source (proxy CA or MS CA), one server is sufficient.
- A minimum of two servers are required to generate certificates using both proxy CA and MS CA. One agent needs to be installed on each server.
- If you install MS agent on the server with MS CA, ensure that **CA Proxy** is disabled. Otherwise, the agent changes the certificate service from MS CA to proxy CA.

Consider the following configuration examples:

Example 1:

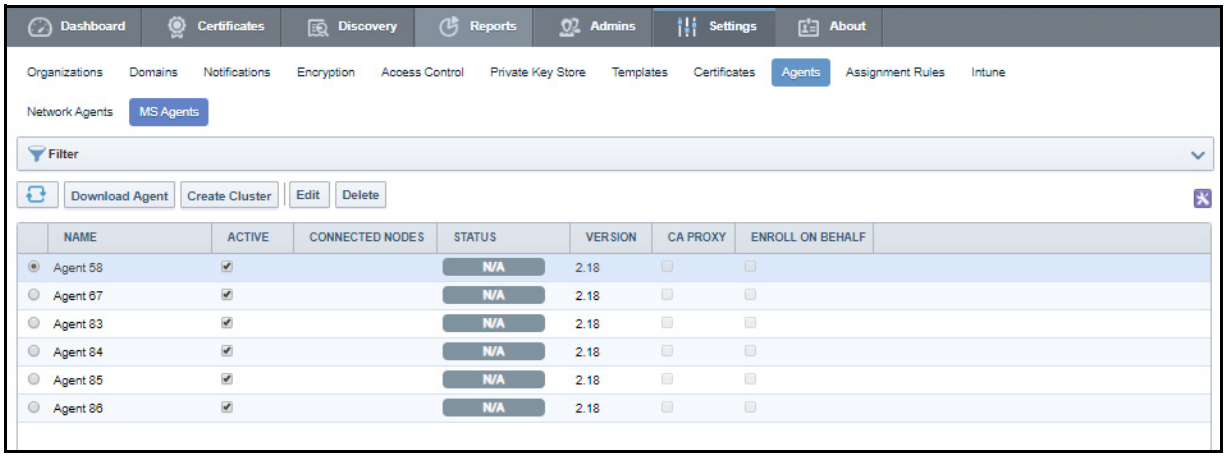
- Server A is used for SCM CA proxy. MS agent is installed with both options enabled.
- Server B is used for MS CA. MS agent is installed with only **Enroll on Behalf** enabled

Example 2:

- Server A is used for SCM CA proxy. MS agent is installed with both options enabled. Certificates are enrolled from SCM and are connected to server B for enrolling certificates from MS CA.
- Server B is used for MS CA. MS agent is not installed.
- Server C (no MS CA) has agent installed with both options enabled. CA proxy can act as cluster and connects to server B to enroll certificates from MS CA.
- Server D has MS agent installed in with **Enroll on Behalf** only. CA proxy is disabled. The agent connects to server B to enroll MS CA certificates. This is a cluster arrangement.

You can configure the agent as follows:

1. Navigate to **Settings > Agents > MS Agents**. The **MS Agent** area is shown in the following illustration.



2. Select an agent and click **Edit**.
3. Make any required alteration to the **Agent Properties** fields based on the information provided in the following table.

Field		Description
Name		The name of the agent.
Version		The version number of the agent.
Active		Activates the agent.
CA Proxy Enabled		Indicates whether or not the agent is enabled as a CA proxy to receive device certificate requests from the NDES server.
Secret Key (min 10 symbols)		An auto-generated authentication key for the purpose of connecting to SCM. You can enter an existing key.
Comments		Descriptive comment on the purpose of the agent.
Default Parameters for NDES Enrollment		
Organization		The default organization from which address details are used for certificate enrollment if no data was specified in the certificate request.
Department		The default department from which address details are used for certificate enrollment if no data was specified in the certificate request.
MS AD Domains Restrictions		
Restriction method	only listed	When selected, the agent only works with MS AD domains specified in the **List of domains to be affected** field.
	excluding listed	When selected, the agent works with all accessible MS AD domains except those included in the **List of domains to be affected field**.
List of domains to be affected		The list of MS AD domains to which the selected **Restriction method** apply.

4. Click **OK**.

Once an MS agent is installed on an AD server, you can configure AD discovery scan tasks and start provisioning device certificates. For more information, see "Performing the AD Discovery Tasks" on page 560 and "How to Request and Issue Device Certificates" on page 188.

6.3.8 How to Configure Clustered MS Agent for Certificate Discovery and Issuance Via AD Servers

SCM allows you to create agent clusters by grouping stand-alone MS agents which are installed on different servers. Once integrated, the stand-alone agents are imported into the cluster and act as a single agent. Clustered agents ensure that if one or more agents go down, their certificate discovery and issuance functions are taken over by another agent in the cluster. This prevents delays and data loss during issuance and discovery operations.

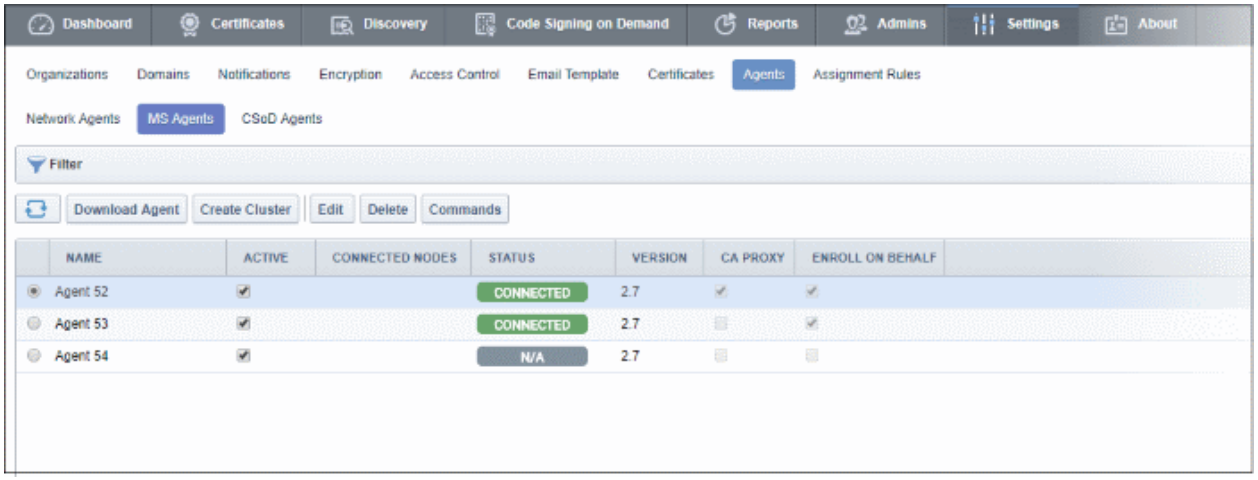
Any number of agents can be included in a cluster. For the configuration to succeed, the MS agents to be included in the cluster must have been installed on AD servers, connected to SCM or MS CA and configured with the following parameters enabled:

- CA Proxy
- Enroll on Behalf
- Active

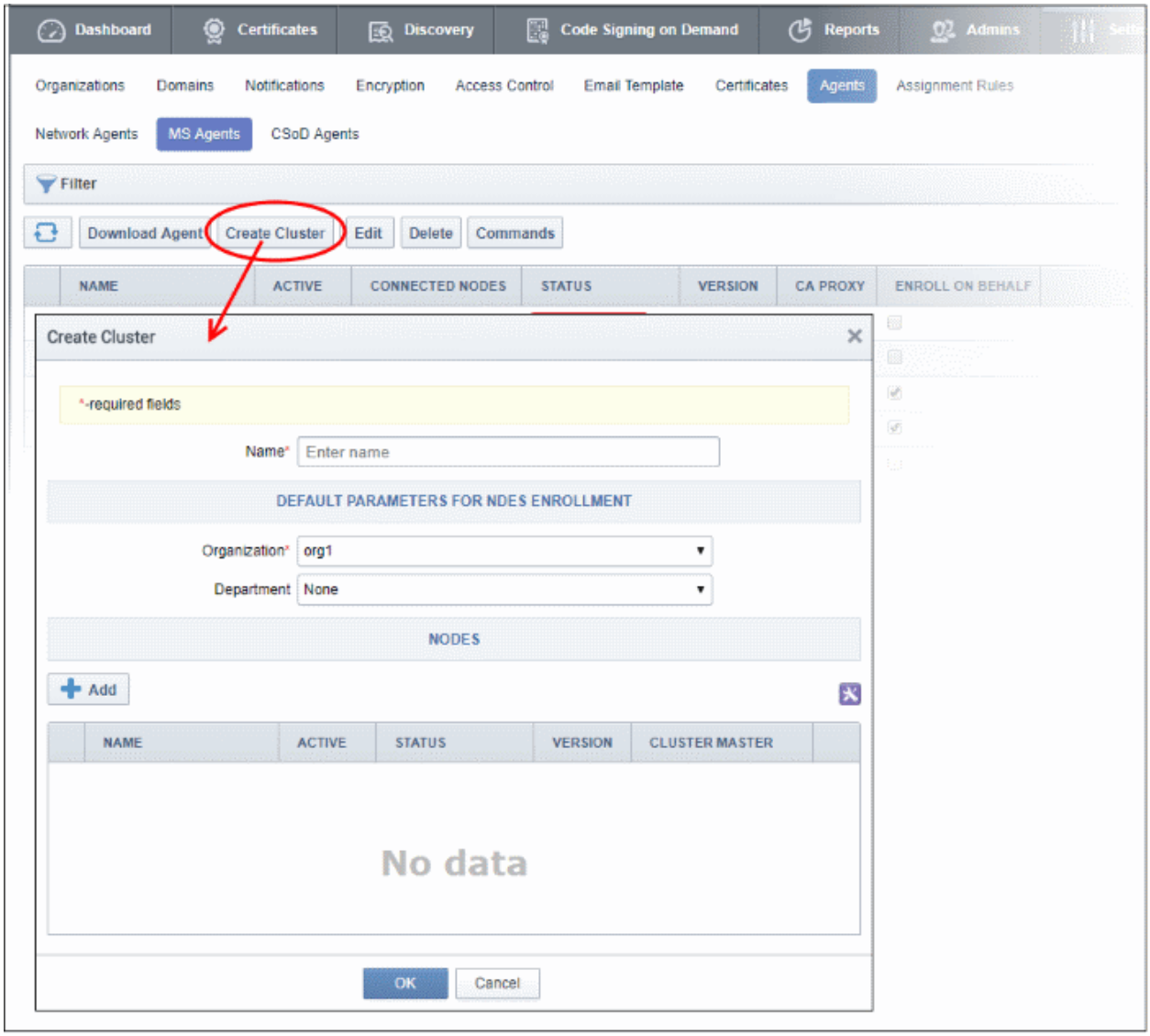
For more information, see "How to Configure a Standalone MS Agent for Certificate Discovery and Issuance via AD Servers" on page 285.

You can create an agent cluster as follows:

1. Navigate to the **Settings > Agents > MS Agents** area, as shown in the following illustration.



2. Click **Create Cluster** to open the **Create Cluster** dialog shown in the following illustration.

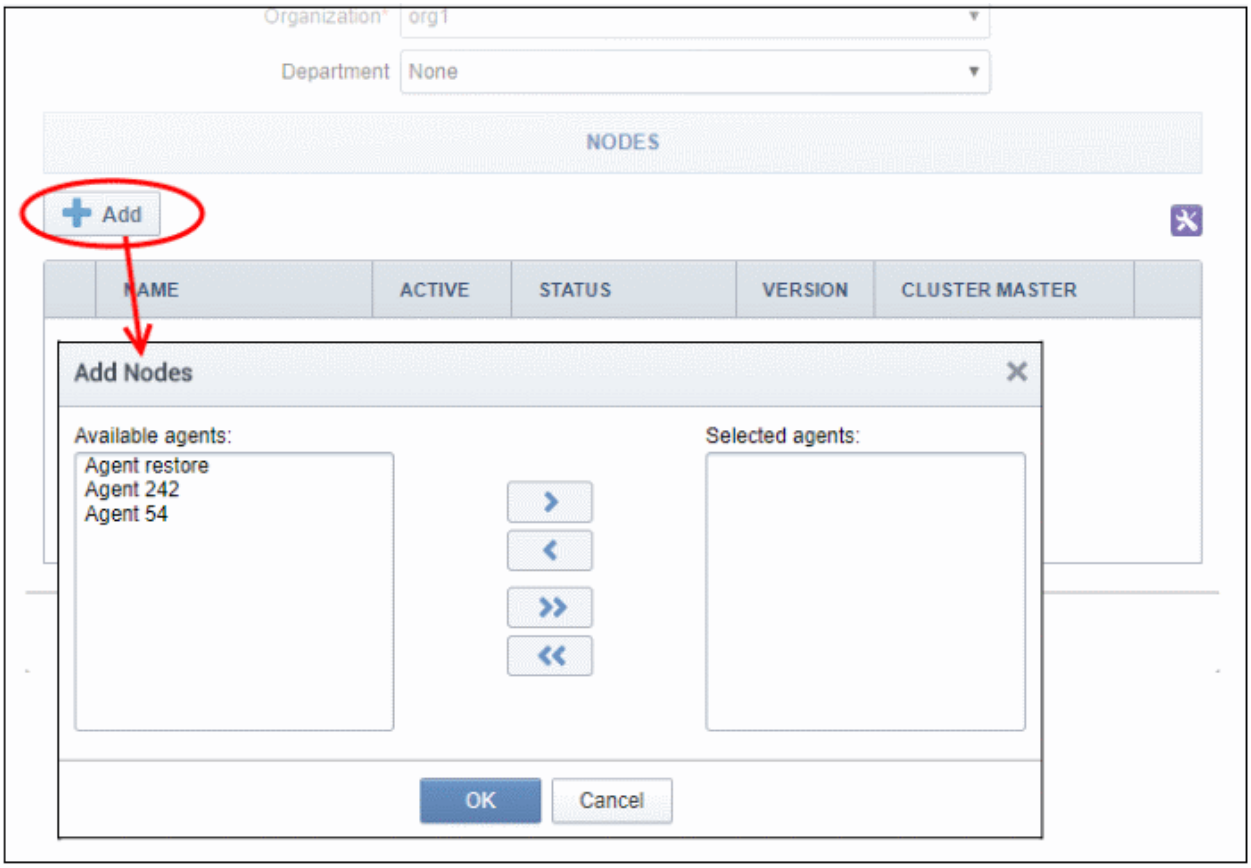


3. Modify the **Create Cluster** fields based on the information provided in the following table, and then click **OK**.

Field / Element	Description
Name	The name for the clustered agent.
Organization	The organization to assign to the agent cluster for issuing certificates through NDES and MS CA.
Department	The department to assign to the agent cluster for issuing certificates through NDES and MS CA.
Add	Adds stand-alone agents to the cluster.

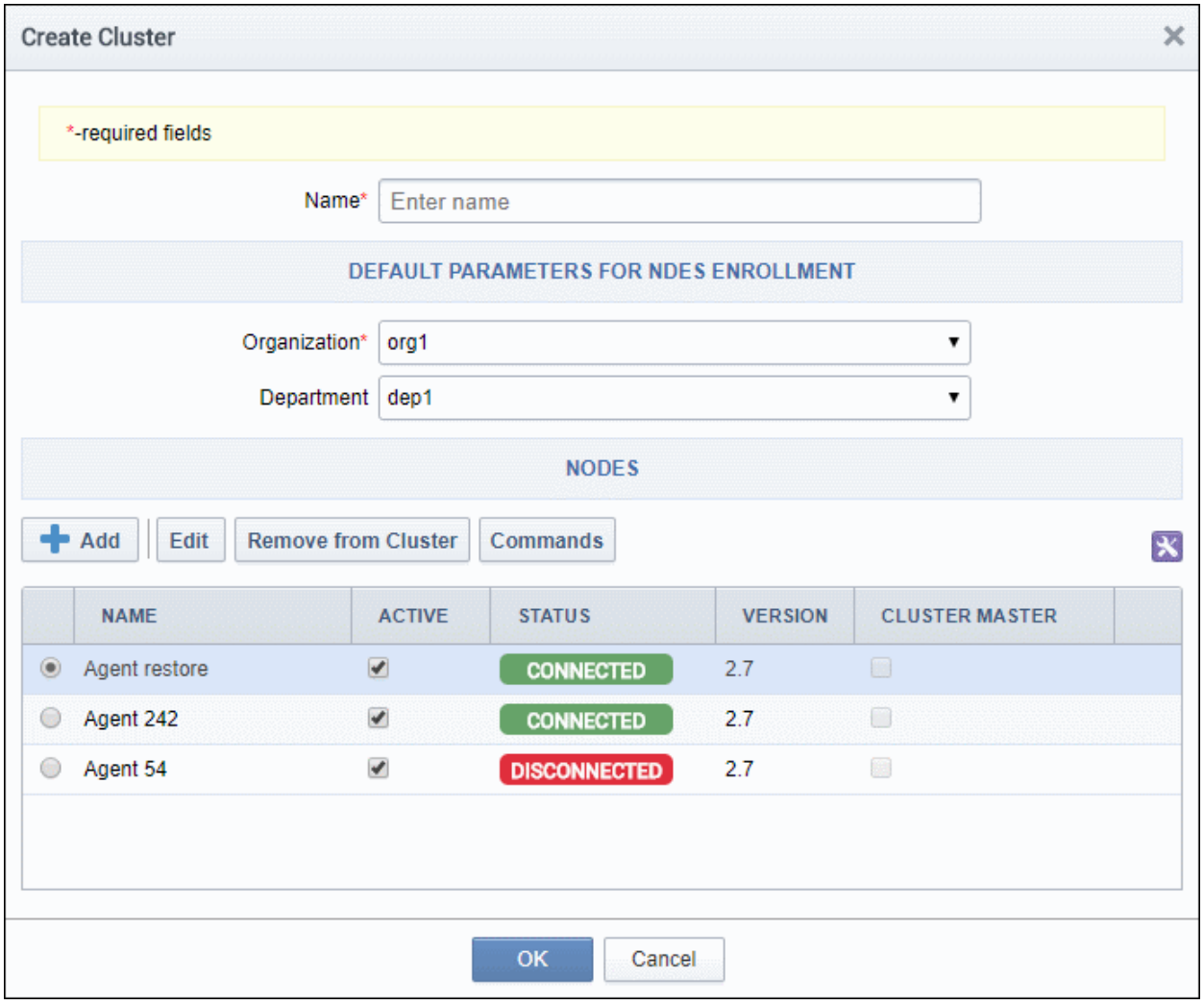
You can add existing stand-alone MS agents to a cluster. If the agents are of the latest version, active, and connected to SCM and MS CA. You can add agents to a cluster as follows:

1. Click **Add** in the **Create Cluster** dialog and use the arrows to move agents into or out of the **Selected agents** column, as shown in the following illustration.



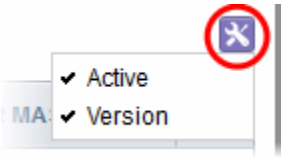
2. Click **OK**.

Once completed, the agents are added to the cluster and displayed as a list. These agents are then available for further configuration, as shown in the following illustration.



The following table lists settings for clustered agents.

Column	Description
Name	The name of the agent.
Active	Indicates whether or not the agent is active.
Status	The current connection status of the agent. The valid values are: • Connected—Indicates that the agent is connected to SCM / MS CA. • Disconnected—Indicates that the agent is not connected to SCM / MS CA. • N/A—Indicates that the agent has never established connection to SCM / MS CA.
Version	The version number of the agent.

Column	Description
Cluster master	Indicates whether the node is set as the master agent in the cluster. SCM automatically assigns one of the agents in the cluster as master agent in order to receive the commands for discovery scans and certificate issuance. The cluster master is selected depending on the order of connection and the current connection status. If connection to the cluster master is lost, the next agent is set as the cluster master.
You can use the tool button to select columns to be displayed in the table: 	
Controls	Add—Adds nodes to the cluster.
Agent Controls	Edit—Shows the general settings and scan configuration of the agent, and edits the name of the agent.
	Remove from Cluster—Releases the agent from the cluster. The released agent is added to SCM as a stand-alone agent.
	Commands—Shows commands executed by the agent. Commands include configuration updates and scanning the AD server.
	Restore[a]—Downloads the agent setup file for existing agents. This is useful if you if you have already configured, downloaded and installed the agent on a server but need to re-install the agent for some reason. The new agent setup file is configured with the same parameters (agent name, secret key, CA proxy, update settings, scan schedule, and so on).

a. Applicable only for agents that are active.

Once configured and the agents are added, the next step is to configure the scan settings, as described in "Performing the AD Discovery Tasks" on page 560.

6.3.9 How to Enable LDAPS Communication with MS AD

You enable LDAPS communication between the MS agent and MS AD as follows:

1. Obtain an SSL certificate.

   The SSL certificate must comply with the requirements outlined by Microsoft for an LDAPS certificate. The current requirements can be found at https://support.microsoft.com/en-ca/help/321051/how-to-enable-ldap-over-ssl-with-a-third-party-certification-authority. These requirements are subject to change by Microsoft at any time without notice.
2. Run `regedit`.
3. Navigate to `HKEY_LOCAL_MACHINE>SOFTWARE>COMODO>CCM`

4. Create a value of the type `REG_DWORD = UseLDAPS`.
5. Specify a Data value of `0` if using LDAP, or `1` if using LDAPS.

   Since LDAPS communication imposes additional requirements, LDAP is the default communication protocol.
6. Restart the agent using the `certsrv.mcs` snap-in.

6.4 Configuring CSoD Agents

The CSoD agent handles code signing operations for developers in one of the following modes:

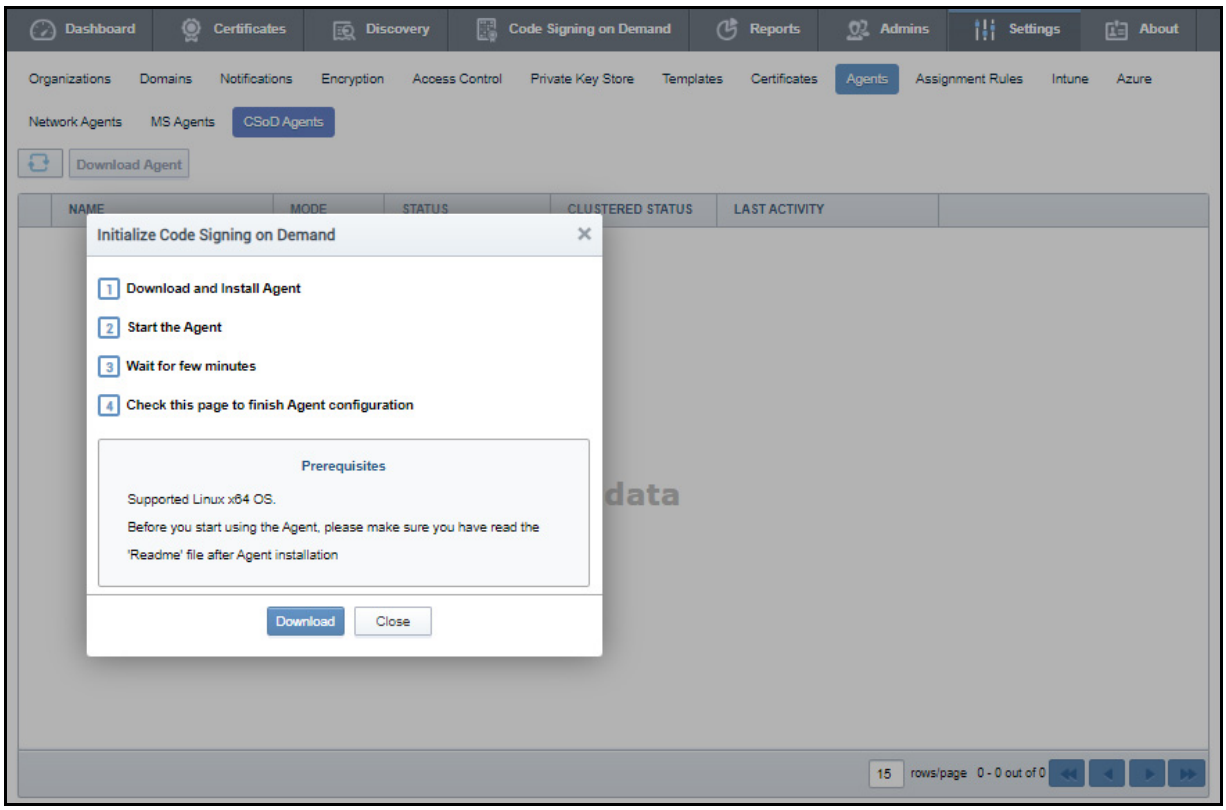
- In-house hosted mode—The CSoD service back end is run on Sectigo's secure cloud servers while the rest of the lifecycle is run in-house. The in-house hosted CSoD can be run as follows:
  - Standard—With an agent installed on a single server.
  - Clustered—With agents installed on multiple servers for redundancy.
- Cloud service mode—The CSoD service is provisioned entirely on Sectigo's secure cloud servers.

Each CSoD agent can be configured for backup and restore operations and for auto-approval of code-signing requests. The configuration options available to you depend on the mode of service enabled for your account.

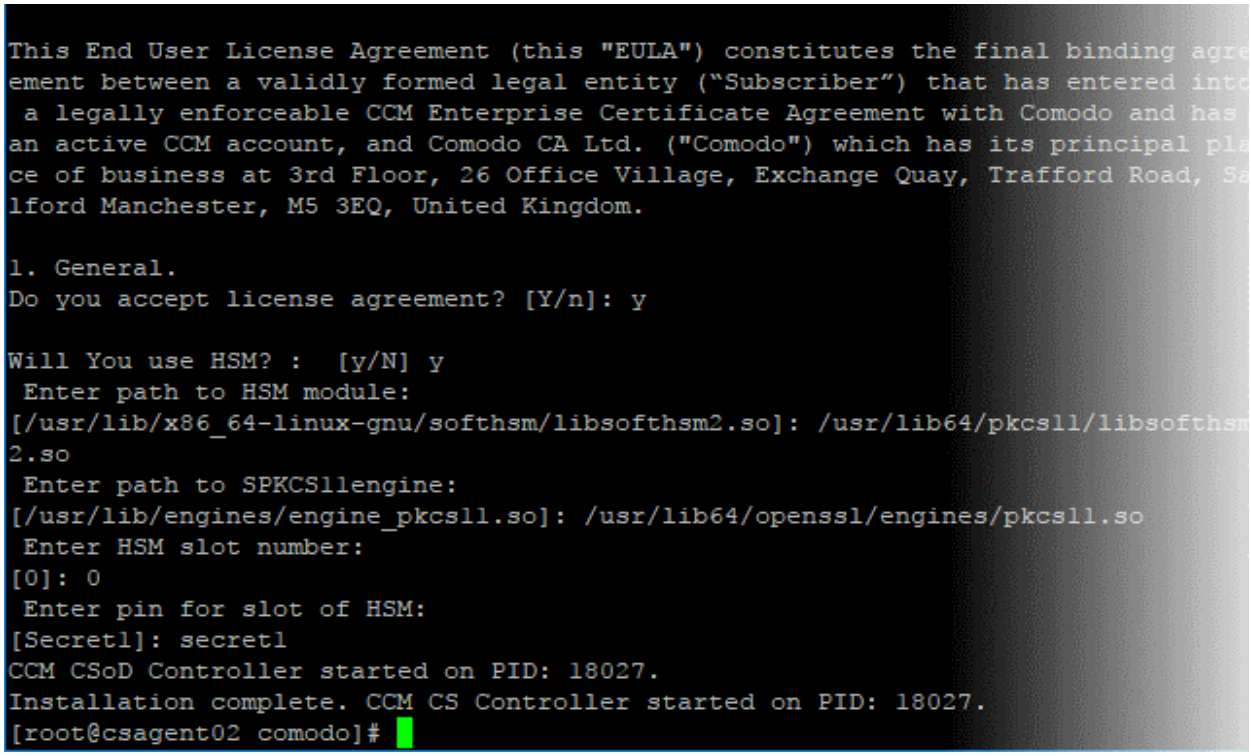
6.4.1 How to Install a CSoD Agent

You can download and install CSoD agents as follows:

1. Use the SCM UI to navigate to **Settings > Agents > CSoD Agents** and click **Download Agent**, as shown in the following illustration.



2. Once the download is complete, transfer the file to your Linux server.
3. Install the CSoD agent on the server from the command line, as shown in the following illustration.



4. Read the EULA, accept the terms of use by selecting **I Agree**, and click **Next**.
5. Enter `Y` if you want to use a Hardware Security Module (HSM). The use of a HSM is mandatory for cluster mode. Enter `N` if you wish the agent to generate and store the keys in its vault. If you decide to use a HSM, enter the following parameters:
   - Network path to the HSM module
   - Path to PKCS#11 Engine
   - HSM Slot Number to be used
   - PIN number for the HSM Slot

   For cluster mode, the CSoD agents should be configured to use the same HSM appliance and the same directories for output and input files. Typically, the path of the agent is `/opt/COMODO/CCMcscontroller/conf/agent.properties`, which may vary depending on your Linux environment. The example folder configuration is as follows:
   - `sign_input_path=/mnt/smb/csod/in`
   - `sign_output_path=/mnt/smb/csod/out`

The agent connects to the SCM server once installation is complete. You can configure the agent from SCM.

Your HSM appliance may need some additional configuration to generate keys. Refer to the instructions in the user manual of your appliance.

6.4.1.1 Setting Up the CSoD Agent in In-House Hosted Mode

The CSoD service is available in both hosted and cloud versions and is capable of signing the following file types:

- Windows executables:

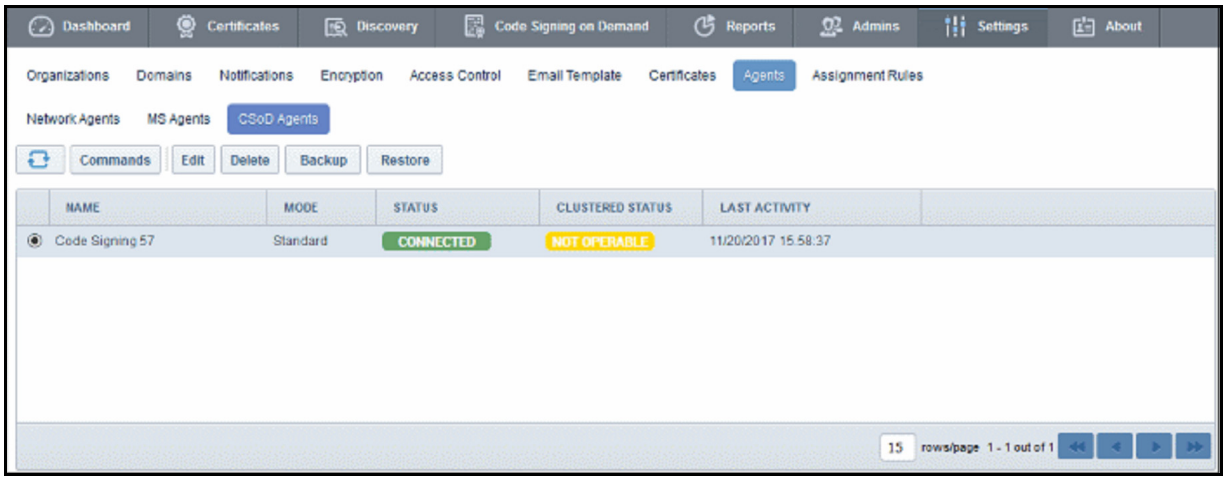
    - `.exe`
    - `.dll`
    - `.ocx`
    - `.sys`
- Windows installation packages:
    - `.cab`
    - `.msi`
- Java packages:
    - `.war`
    - `.jar`
- Android application files:
    - `.apk`
- PowerShell scripts:
    - `.ps1`
    - `.psm1`

CSoD agents can be installed on a single computer or on multiple computers.

If installed on a single computer, the use of a HSM is optional. If you choose to install the agent on multiple computers (cluster mode), then the network HSM and Network File System are mandatory.

You can configure a CSoD agent as follows:

1. Navigate to **Settings > Agents > CSoD Agents** area shown in the following illustration, select an agent and click **Edit.**



2. Make any required alteration to the **CSoD Agent Properties** fields based on the information provided in the following table, and click **OK**.

Column	Description
Name	The name of the agent.

Column		Description
Mode		The valid values are: • Standard—Indicates that the agent is not using the HSM. • HSM—Indicates that the agent is using HSM.
Status		The current connection status of stand-alone and clustered agents. The valid values are: • Connected—Indicates that the agent is communicating with SCM. • Not Connected—Indicates that the agent is not communicating with SCM. • N/A—Indicates that no connection has been established.
Clustered Status		Indicates whether or not the agent is configured to use HSM. The valid values are: • Not Operable—Indicates that the agent is installed in standard mode or the agent has not been correctly configured to use HSM. • Operable—Indicates that the agent is correctly configured to work with HSM and can be used as cluster. • N/A—Indicates that the agent has been downloaded and SCM is yet to identify whether the agent satisfies the criteria of cluster.
Last Activity		The date and time of the agent's last communication with SCM.
Controls	Download Agent	Downloads and creates a new CSoD agent for installation. This may be available in the interface again after the first download depending on the mode in which the primary agent was installed. The valid values are: • Standard mode—Indicates that the download button does not appear in the interface again if you installed in standard mode and are not using HSM. • Clustered mode—Indicates that the download button does be available again If you installed the agent in clustered mode and configured it to use HSM, you can download the agent and install it on another computer. The agent must be configured to use the same HSM. In addition, you have to download and install a new agent for each new computer. Also, a single agent setup file cannot be used on multiple computers.
	Commands	View commands executed by the agent. Commands include Generate CSR and Manage private keys.
	Refresh	Updates the list of agents.
Agent Controls	Edit	Modifies the agent name and the host name or IP address of the computer on which the agent is installed.
	Delete	Removes the agent.
	Backup	Copies the CSoD database to a remote SFTP server.
	Restore	Restores code signing keys from backup.

6.4.1.2 Setting Up the CSoD Agent in Hosted Mode

You can install the CSoD agent on a single computer and choose not to use an HSM appliance. SCM also supports the installation of a CSoD agent on multiple computers for redundancy.

In standard mode, the following requirements must be met:

- The CSoD agent is downloaded and installed on a single server.
- The Osslsigncode tool is installed on the same server.

In cluster mode, the following requirements must be met:

- CSoD agents are downloaded and installed on multiple servers.

  Note that you cannot use the same agent setup file on different servers.
- The use of HSM and Network File System is mandatory.
- The Osslsigncode tool is also be installed on all servers.
- All agents are configured to use the same HSM appliance and the same directories for output and input files.
- The input and output folders are configured in the CSoD agent properties. Typically, the path of the agent is `/opt/COMODO/CCMcscontroller/conf/agent.properties` (this may vary depending on the Linux environment). The example folder configuration is as follows:

  ```
  sign_input_path=/mnt/smb/csod/in
  sign_output_path=/mnt/smb/csod/out
  ```
- **Download Agent** is available in the **CSoD Agents** area once the configuration to the HSM and input and output files is complete. This control allows you to download a new CSoD agent for installation on another computer.

6.4.1.2.1 Installing the Osslsigncode Tool

You can download the tool from `http://sourceforge.net/projects/osslsigncode/.`

For cluster mode, the tool should be installed on all servers on which the CSoD agent is installed The tool's installation procedure depends on the version of the tool and your environment.

It is recommended that you install the osslsigncode tool to `/usr/bin`. Otherwise, the CSoD agent may not be able to access it and you would need to manually provide access.

The following is the latest CentOS configuration:

```
yum install gcc intltool libxml2-devel glib2-devel libcurl* openssl* bzip2* gdk*
wget http://ftp.gnome.org/pub/GNOME/sources/libgsf/1.14/libgsf-1.14.34.tar.xz
tar -xf libgsf-1.14.30.tar.xz
cd libgsf-1.14.30
./configure --prefix=/usr
make
make install
cp /usr/lib/pkgconfig/libgsf-1.pc /usr/lib64/pkgconfig/libgsf-1.pc
pkg-config libgsf-1 --modversion
cd ..
cd osslsigncode-1.7.1
./configure
make ; make install
```

The following is the latest Debian configuration:

```
apt-get install libbz2-dev libgdk-pixbuf2.0-dev glib2.0-dev libxml2-dev intltool libcurl4-openssl-dev libssl-dev
wget http://ftp.gnome.org/pub/GNOME/sources/libgsf/1.14/libgsf-1.14.34.tar.xz
tar -xf libgsf-1.14.34.tar.xz
cd libgsf-1.14.34
./configure --prefix=/usr
make
make install
cd ..
cd osslsigncode-1.7.1
./configure
make ; make install
```

Other Linux

i. Download and unzip osslsigncode-1.7.1.tar.gz from http://sourceforge.net/projects/osslsigncode/

ii. See README.txt. The usual installation has 3 steps:

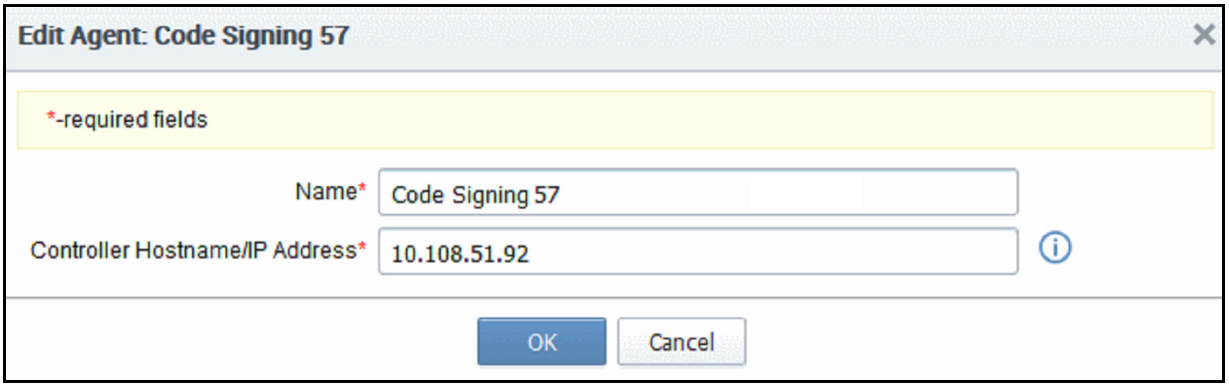
```
./configure
make
make install
```

6.4.1.2.2 Tuning the Environment

An CSoD agent typically needs to be configured for use with a publicly trusted certificate. This is because most browsers restrict access to sites that do not use a publicly trusted certificate.

To use a different certificate, do the following:

1. Make sure the server on which the agent is installed has a valid host name. If it does not, then you need to assign one. In addition, create a DNS record for the server so it is accessible through your network.
2. Navigate to **Settings > Agents > CSoD Agents** in SCM.
3. Select an agent and click **Edit.** The **Edit Agent** dialog is shown in the following illustration.
4. Replace the default host name or IP address with the host name of the agent server.



5. Retrieve a publicly trusted certificate for the server.

   The host name should be specified in the **Common Name** field in the certificate.
6. Put the certificate and private key into the Java Key Store (JKS) with a password. For example:
   - File: `cs-agent.jks`
   - Password: `yourpassword`
7. Copy the file into the `conf` directory of the agent's install directory. Typically, it is `/opt/COMODO/CCMcscontroller/conf`.
8. Update the `agent.properties` file located in `/opt/COMODO/CCMcscontroller/conf/`, and specify JKS file and password. For example:
   - `ssl.keystore=cs-agent.jks`
   - `ssl.keystore.password=12345`

9. Restart the agent. Typically, the commands are `/etc/init.d/CCMcscontroller stop` and `/etc/init.d/CCMcscontroller start`.

You need to ensure that port 9092 is open, as the agent uses this port for incoming requests. In addition, ensure that the `hostname` command returns the assigned host name.

After installation, the agent automatically connects to SCM and starts running immediately. To check the connection status, navigate to **Code Signing on Demand > Configuration**.

On first connection, the agent downloads the latest configuration files from SCM and generates a password for its database. Then the agent periodically polls SCM to retrieve instructions.

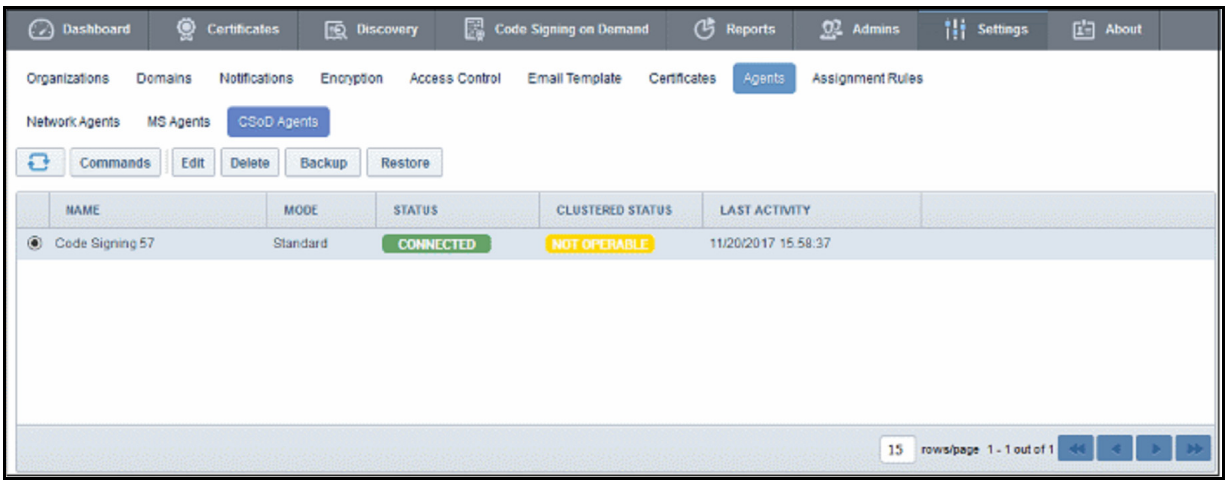
You also need to configure input and output directories for code signed files. For a clustered mode environment, in order for the SCM to work seamlessly with all the agents, the following must occur:

- All the CSoD agents should be configured to work with the same HSM.
- Network file system should be available. All the CSoD agents should be configured to have the same directory for input files and the same directory for output files. The input and output folder configuration is done at the agent properties level. Typically, the path of the agent is `/opt/COMODO/CCMcscontroller/conf/agent.properties`, which may vary depending on the Linux environment. The following is an example configuration:
  - `sign_input_path=/mnt/smb/csod/in`
  - `sign_output_path=/mnt/smb/csod/out`

6.4.2 In-House Hosted Mode Configuration

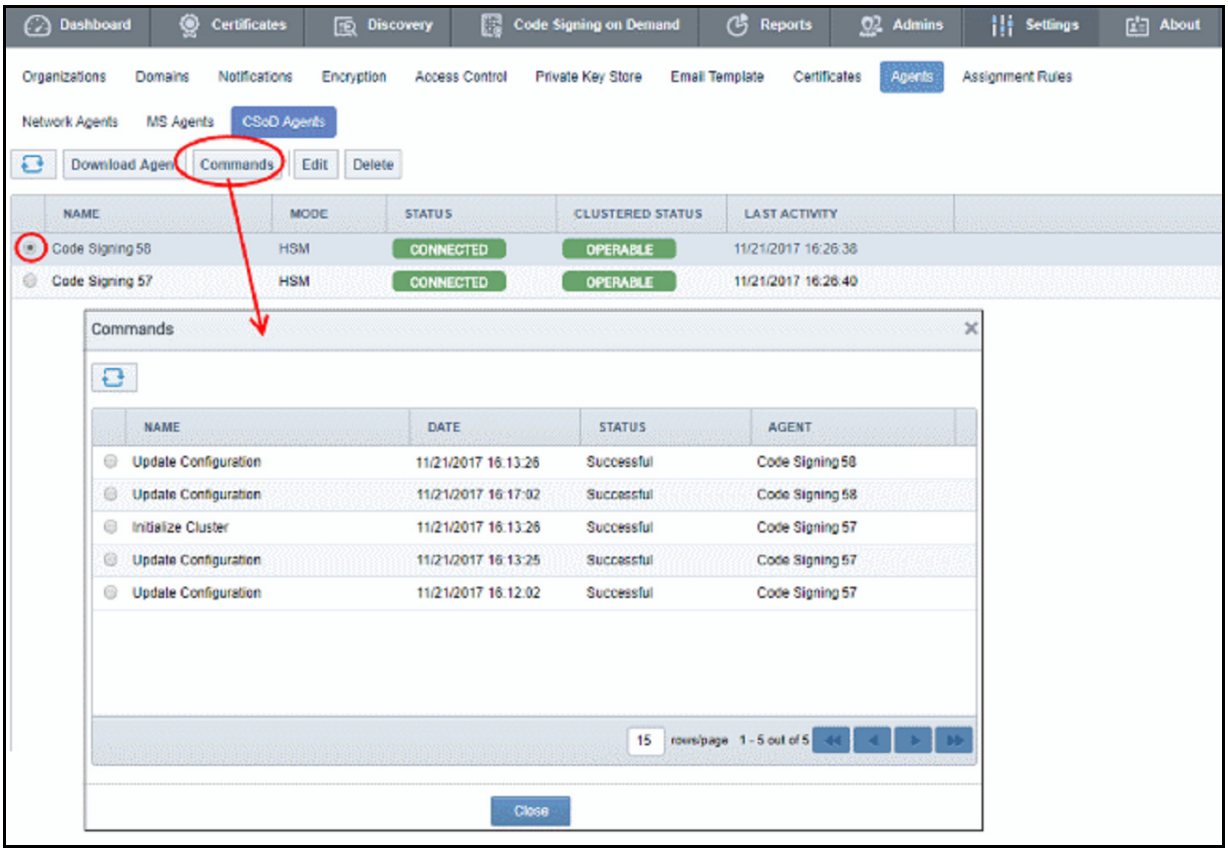
When configured in in-house hosted mode, the CSoD agent creates an encrypted database on your network which is used to store your certificates and private keys. What installed in standard mode, a CSoD agent can be configured to automatically back up this database to a specific location.

From the **CSoD Agents** area, you can view activities of the CSoD agent, as well as back up and restore code signing certificates and their private keys (standard mode only).



You can view a list of commands sent by SCM to the agent and their status as follows:

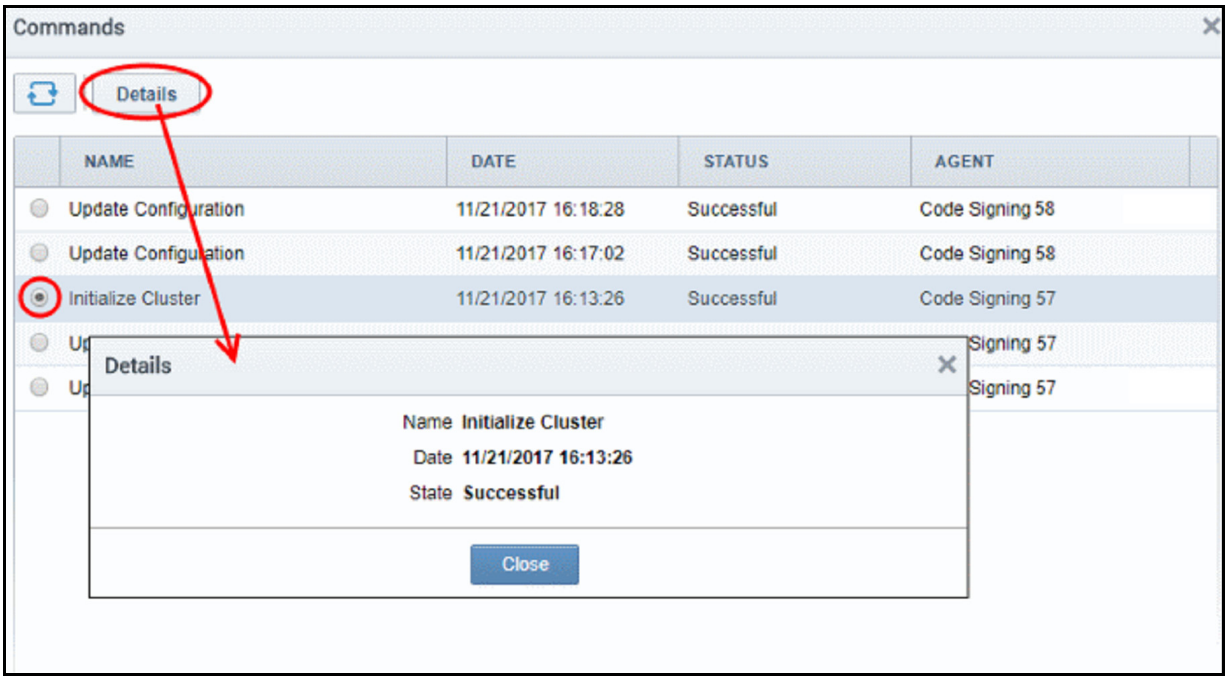
1. Navigate to **Settings > Agents > CSoD Agents.**
2. Select an agent and click **Commands**. From the **Commands** dialog, you can view all commands received by the agent, as shown in the following illustration.



The following table lists the fields displayed in the **Commands** dialog.

Column	Description
Name	The label of the command received from SCM.
Date	The date and time the command was received.
Status	The execution status and result of the command.

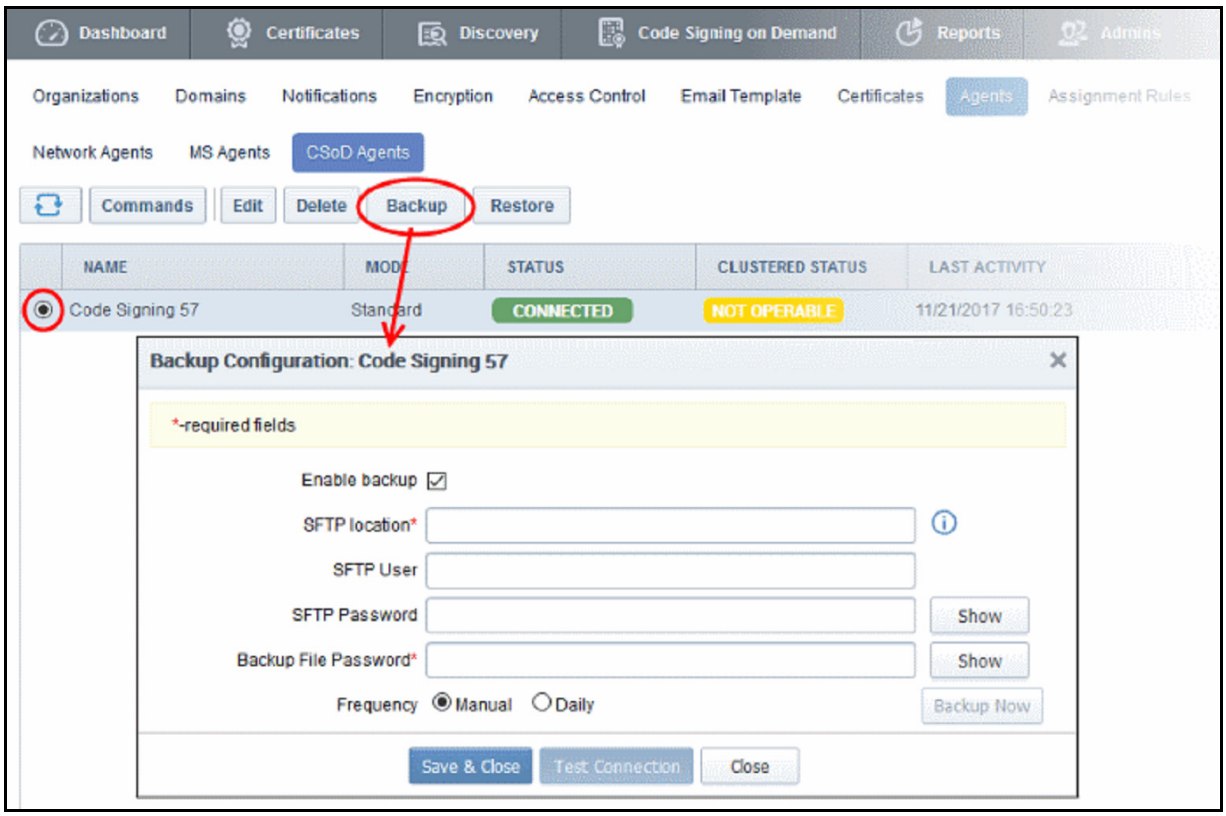
Selecting a command and clicking **Details** displays the details of the command, as shown in the following illustration.



You can schedule regular backups of the CSoD database to a remote SFTP server, or run on-demand backup operations when required. Certificates and private keys can be restored from the backup (in standard mode).

You can configure a CSoD database backup as follows:

1. Navigate to **Settings > Agents > CSoD Agents**.
2. Select an agent and click **Backup**, as shown in the following illustration.



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

Field	Description
Enable backup	Activates the backup capability.
SFTP Location	Path on the SFTP server where the backup should be stored.
SFTP User	The user name of an appropriately privileged account on the SFTP server. The agent uses this account to access the SFTP server.
SFTP Password	The password of the account.
Backup File Password	The password for your backup file. This is required when restoring from the backup.
Frequency	The schedule at which backups should occur. The valid values are: • Manual—Indicates that the backup is to run automatically. Clicking **Backup Now** runs an on-demand backup. • Daily—Indicates that the backups are to be created daily at the time specified in the **Next backup at** list. Select the time in UTC when it should run.

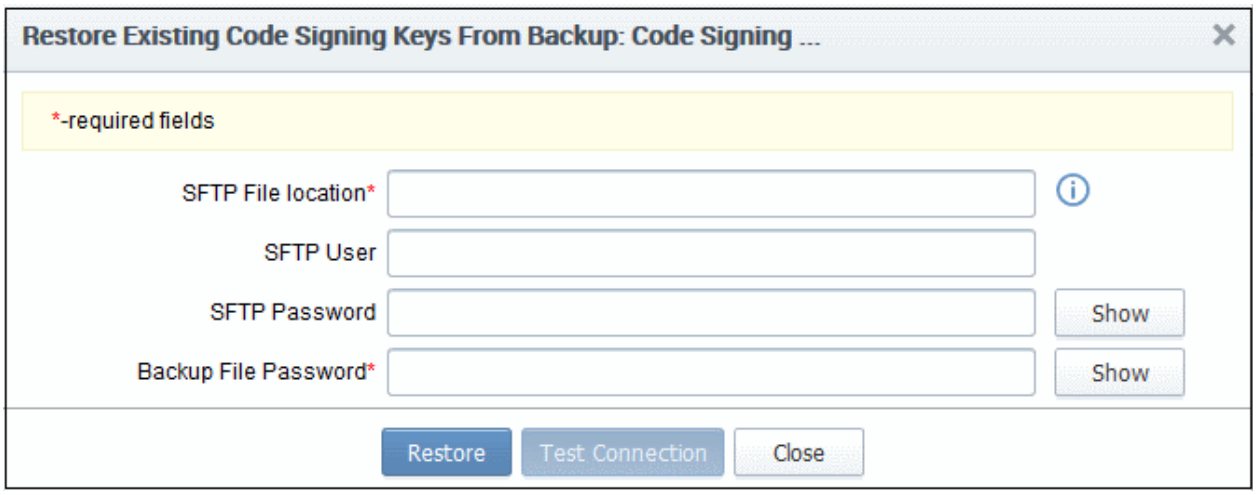
4. On the **Backup Configuration** dialog, click **Test Connection** to check the connection between SCM and the backup server.

5. Click **Save & Close** to apply your changes. Alternatively, click **Close** to cancel the backup configuration.
6. To run an instant backup, click **Backup Now**.

If there are problems with an agent and certificates belonging to the developer are lost, you can install a new agent and restore the certificates from a backup, as follows:

1. Navigate to **Settings > Agents > CSoD Agents**.
2. Download and install the new agent.

   For information on installing CSoD agents, see "How to Install a CSoD Agent" on page 292.
3. Select the agent and click **Restore**.
4. Specify the location of the backup file and provide access credentials using the **Restore Existing Code Signing Keys from Backup** dialog shown in the following illustration.



5. Complete the **Restore Existing Code Signing Keys From Backup** fields based on the information provided in the following table.

Field	Description
SFTP File Location	The path on the SFTP server where the CSoD service backup is stored. For example, `sftp://my_sftp/backup/pkagent_yyyymmdd_HHmmss.jks`
SFTP User	The user name of an account with privileges to access the backup on the SFTP server.
SFTP Password	The password of the account.
Backup File Password	The password of the backup file.

6. On the **Restore Existing Code Signing Keys From Backup** dialog, click **Test Connection** to check the connection between SCM and the backup server.
7. Click **Restore** to restore the backup file. Alternatively, click **Close** to cancel the backup restoration.

Upon completion, the code signing certificates and their keys are restored to the database created by the new agent.

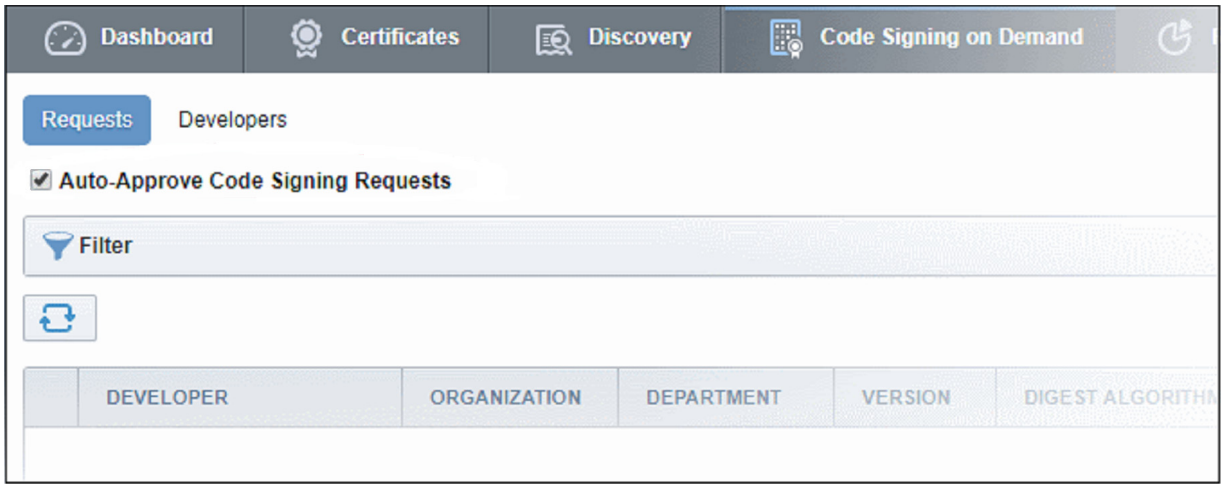
By default, code signing requests from developers must be approved by an administrator. Requests can be viewed, managed, and approved by navigating to **Code Signing on Demand** > **Requests**.

Alternatively, you can configure the agent for auto-approval if you want to skip the manual approval process. If enabled, the agent signs files right after they are uploaded by the developer. To do so, you enable **Auto-Approve Code Signing Requests**, as shown in the following illustration, and the service starts the signing process immediately after files are uploaded by the developer.

6.4.3 Cloud Service Mode Configuration

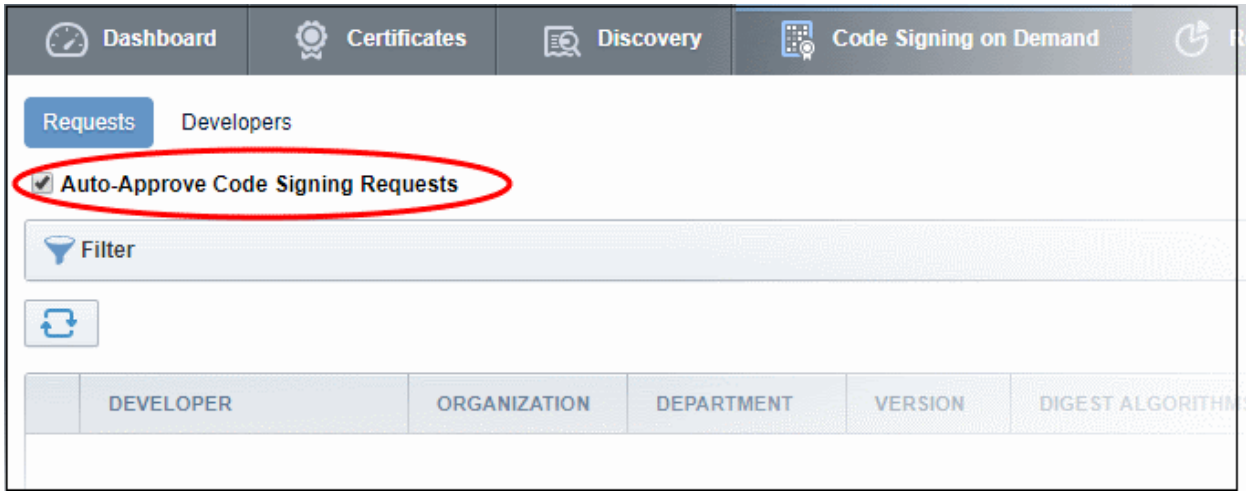
CSoD in cloud service mode can be configured to auto-approve code signing requests from developers. If Cloud Service is enabled for your account, you should contact your Sectigo account manager for any other service requests.

You can configure the CSoD service by selecting **Code Signing on Demand** and then clicking **Requests**, as shown in the following illustration.



By default, code signing requests from developers must be approved by an administrator via the **Requests** area before the actual signing occurs.

If you want signing to start without administrator approval, enable **Auto-Approve Code Signing Requests**. The service starts the signing processes immediately after files are uploaded by the developer.



6.5 Configuring the Private Key Agent

A Private Key Store (PKS) allows you to securely archive the private keys of certificates generated by the auto-CSR. In addition, it allows you to upload the private keys of existing certificates to the store. Certificates containing the public-private key pair can then be downloaded in a `.pfx` or `.p12` format.

The PK agent receives commands from SCM for CSR generation and for storing private keys. As a MRAO, you can configure a backup of the private keys on a remote SFTP server to restore keys should they become missing.

Private keys can be uploaded to the PKS in one of the following ways:

- By selecting **Auto generation of CSR** on the built-in certificate order form when enrolling for a certificate using that form. If selected, SCM instructs the PKS agent to generate a CSR and a key pair with the signature algorithm and key size chosen by you. When this takes place, the agent stores the private key and uploads only the CSR to SCM. After the certificate issuance, you can download the certificate, including private and public keys, in a `.pfx` or `.p12` format. At the time of the download request, the PKS retrieves a copy of the certificate from SCM over an encrypted connection, merges it with the private key, and provisions the certificate to the requester. This ensures the private key does not pass outside your network. See "Automatic CSR Generation Via the Built-in Enrollment Wizard" on page 96 for more information.
- By manually uploading a private key, which is done for the SCM-managed certificates that do not have a corresponding private key in the PKS. This is performed through the **Certificate Details** dialog. Once uploaded, SCM instructs the PKS agent to save a copy of the key and, once this operation is complete, deletes its own copy. After placing the private key in the store, you can download the certificate, including the private key, in a `.pfx` or `.p12` format. For more information, see "How to Upload Private Keys" on page 308.

The PKS eases the renewal process of SSL certificates. On renewal of a certificate whose private key is stored and managed by the PKS, SCM automatically retrieves the existing CSR from the

store and issues the renewal certificate, without the need for the administrator to generate a new CSR and upload it to SCM. A new private key is generated for the new certificate and is retained in the PKS.

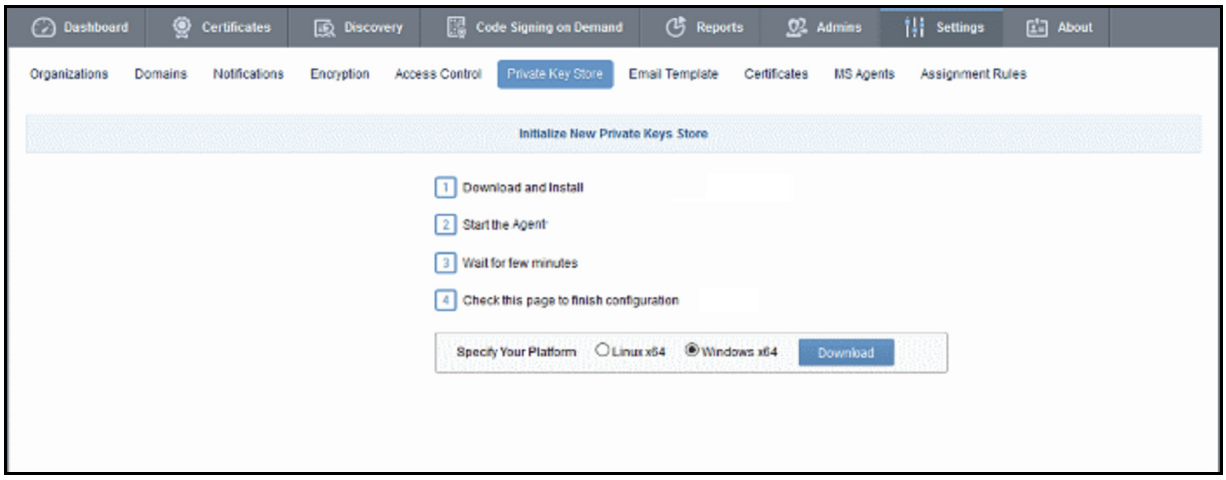
To use the auto-CSR generation functionality, the PKS must be enabled for your account.

6.5.1 How to Install the PKS Agent

To set up a PKS on your local network, you install an agent software on a server and configure it in SCM.

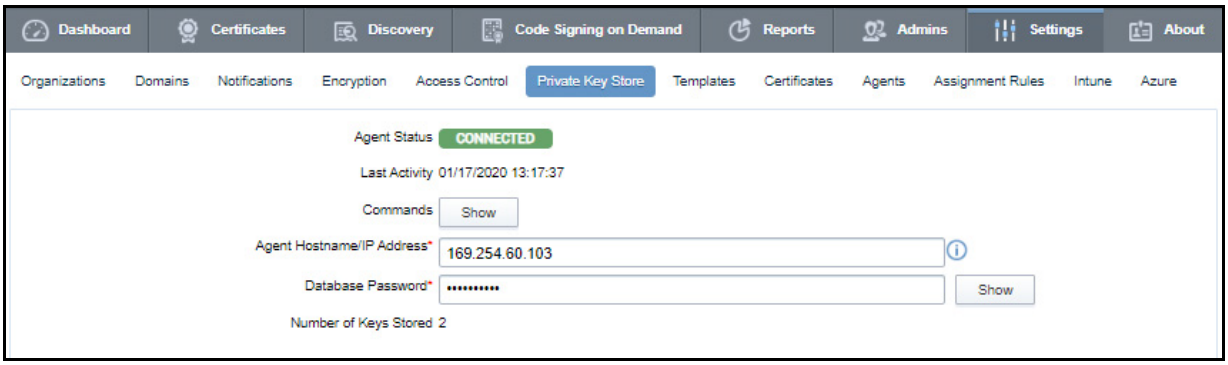
You download and install the PKS agent as follows:

1. Navigate to **Settings > Private Key Store**, as shown in the following illustration.



2. Specify your operating system and click **Download**.
3. Read the EULA fully, accept the terms of use by selecting **I accept the agreement**, and then click **Next**.
4. Review the installation location and click **Install**.
5. Click **Finish**.

During the first run, the agent connects to SCM, obtains the configuration files, updates its configuration, and generates a password for its database. When done, the **Private Key Store** area displays the status as **Connected** and shows the IP address of the server on which the agent is installed, as shown in the following illustration. Then the agent periodically polls SCM to retrieve instructions.



The following table lists settings and elements available in the **Private Key Store** agent details area. Mandatory settings are marked by red asterisks.

Field / Element	Description
Agent Status	Indicates whether or not the agent is currently connected to SCM.
Last Activity	Displays the date and time of last polling of the agent to SCM.
Activity Log	Opens the **Commands** dialog that displays the list of command received by the agent form SCM and their execution status.
IP Address	Displays the IP address of the server on which the agent is installed.
Database Password	Displays the password for accessing the local database created by the agent at the server. The password is auto-generated and cannot be changed by the administrator. Clicking **Show** displays the password. This password is required for downloading the private keys through the SCM.
Number of Keys Stored	Shows the number of private keys stored and managed by the private key agent.

6.5.2 How to Upload Private Keys

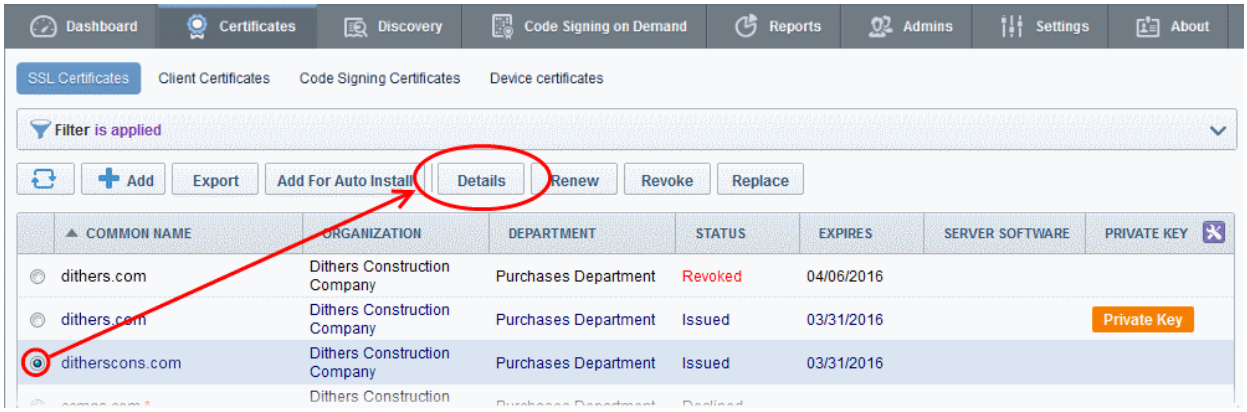
You can upload, store, and manage the private keys of existing SCM-managed certificates to the PKS, which facilitates the following:

- Downloading the certificate in a `.pfx` or `.p12` format for importing to another server.
- Auto-upload of the CSR during the certificate renewal process.

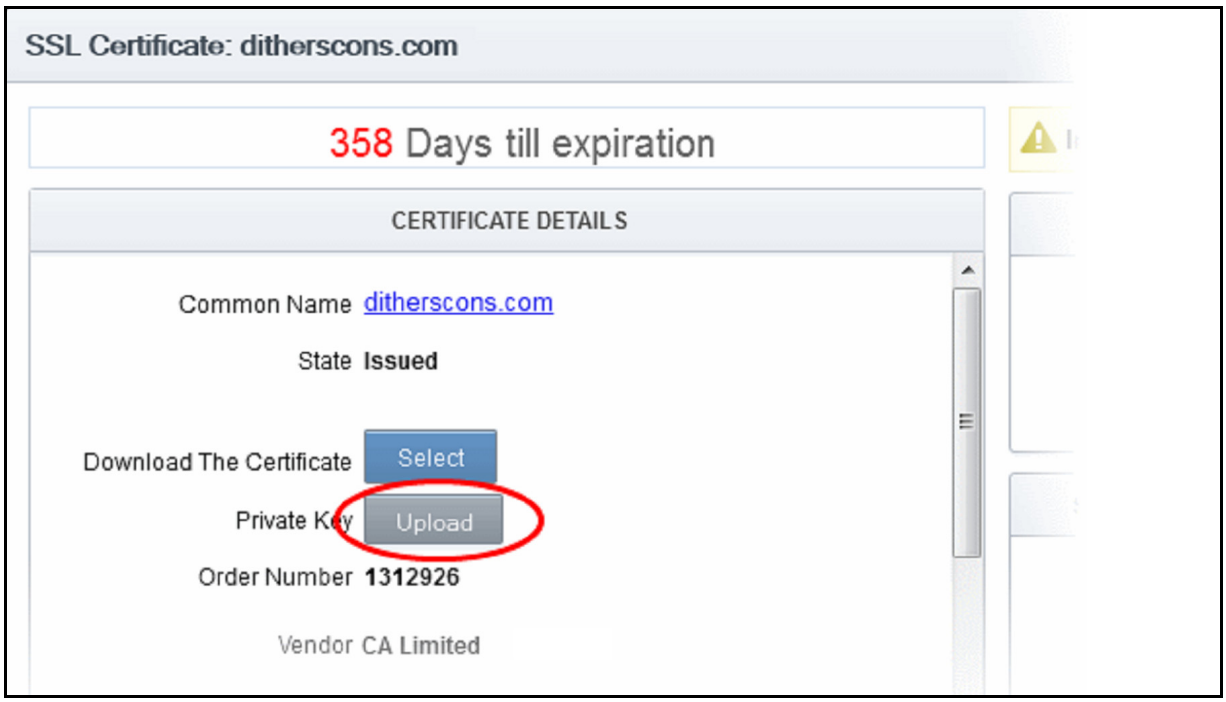
You upload a private key as follows:

1. Navigate to **Certificates > SSL Certificates**.
2. Select the certificate for uploading the private key and click **Details**, as shown in the following illustration.

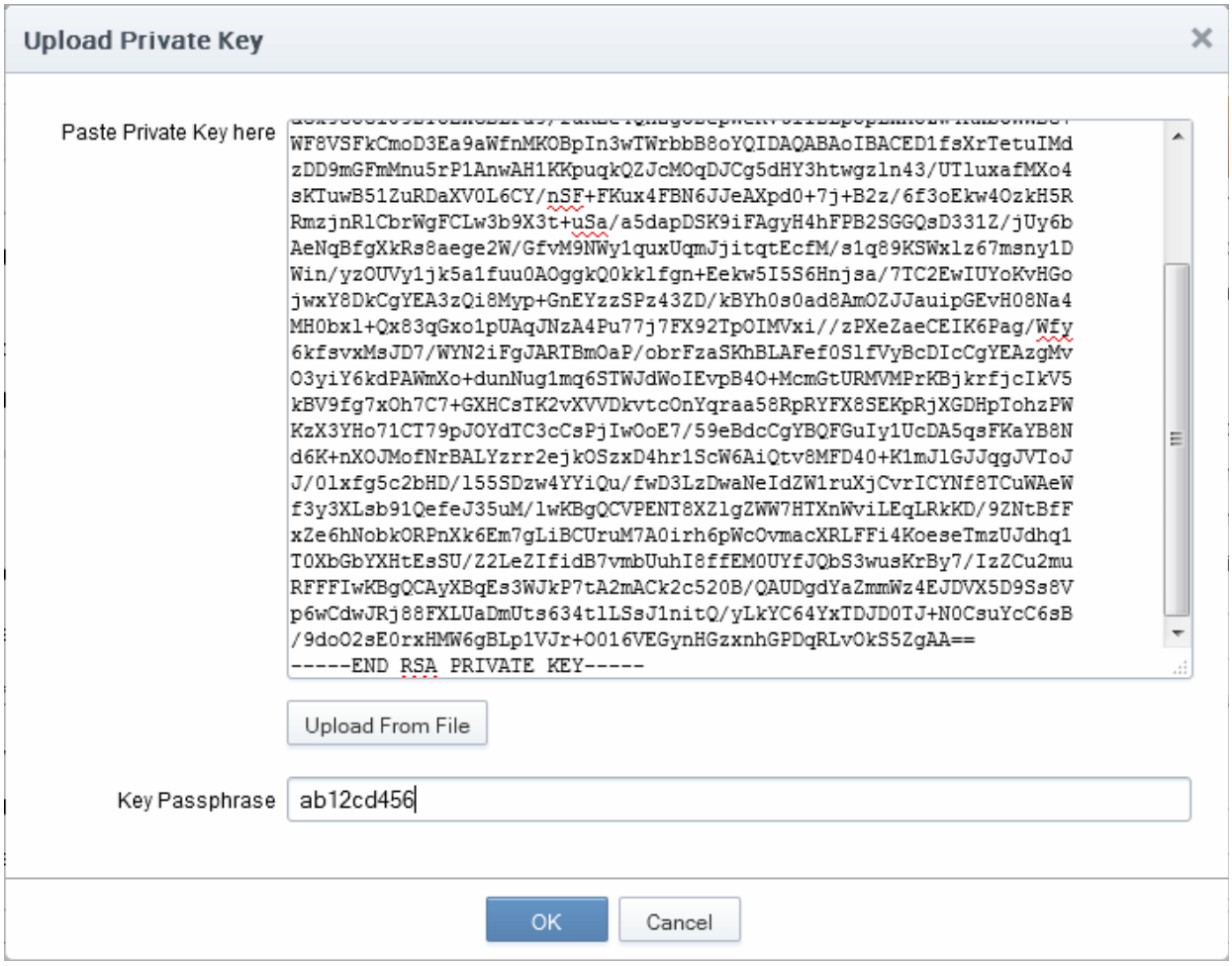
   You can search for a certificate by using filter options.



3. Click **Upload** on the **SSL Certificate** dialog, as shown in the following illustration.



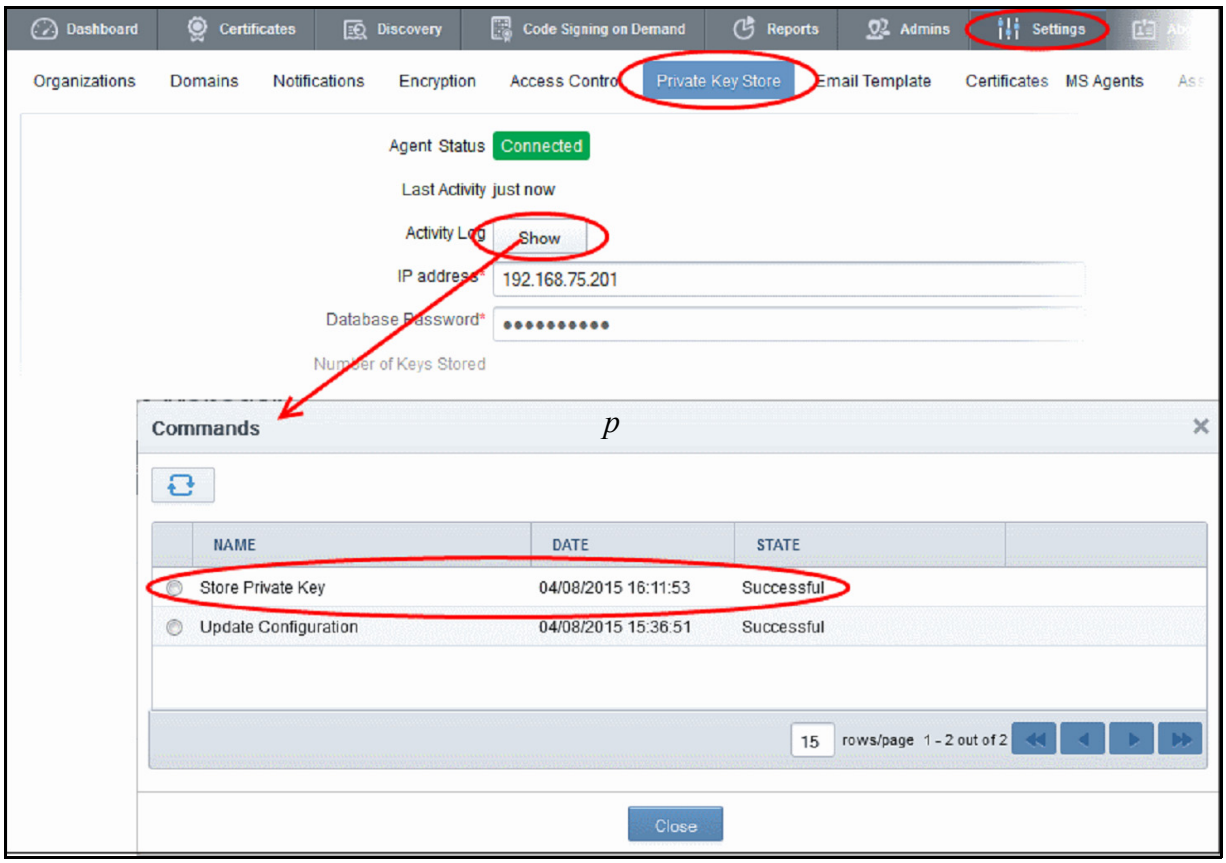
4. Enter the private key associated with the certificate on the **Upload Private Key,** as shown in the following illustration, and then upload the private key via one of the following methods:
   - By directly pasting it in the **Paste Private Key here** field.
   - By saving it as a text file and clicking **Upload From File**.



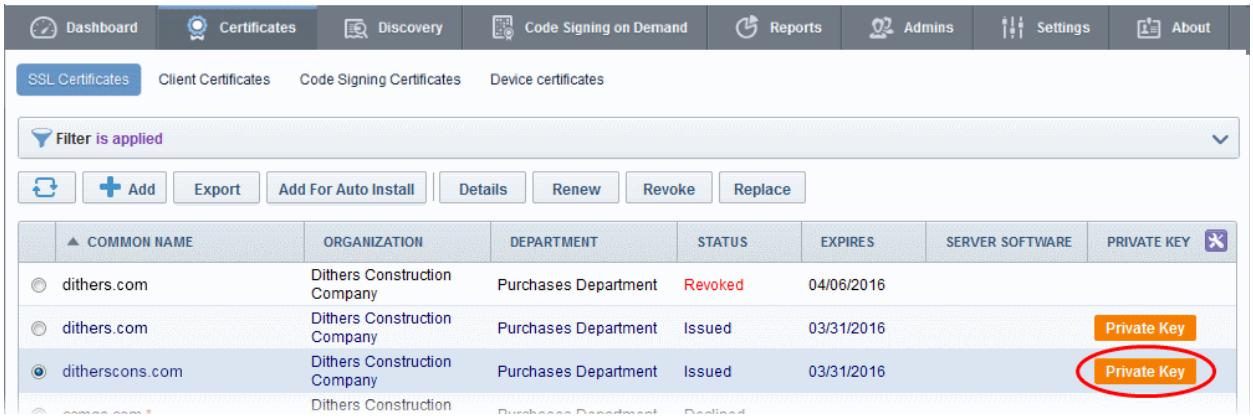
5. Enter a unique **Key Passphrase**.

   This is required when importing the certificate with the key pair on to a server.

Upon completion, SCM instructs the agent to store the private key. You can confirm the execution of the store command via the activity log of the agent. To do so, click **Show** located next to the **Activity Log**, as shown in the following illustration.



The private key is now stored and managed by the PKS. Its availability is indicated under the **Private Key** column in the **SSL Certificates** area, as shown in the following illustration.



6.5.3 How to Download Private Keys

You can download the private key associated with a managed certificate from the PKS. This includes certificates applications for which were submitted via an auto-CSR generation tool in SCM, as well as certificates for which the private keys were manually uploaded to the PKS.

You should have been logged-in to SCM through a computer in the same local network on which the private key agent is installed and should have a personal authentication certificate installed on your computer.

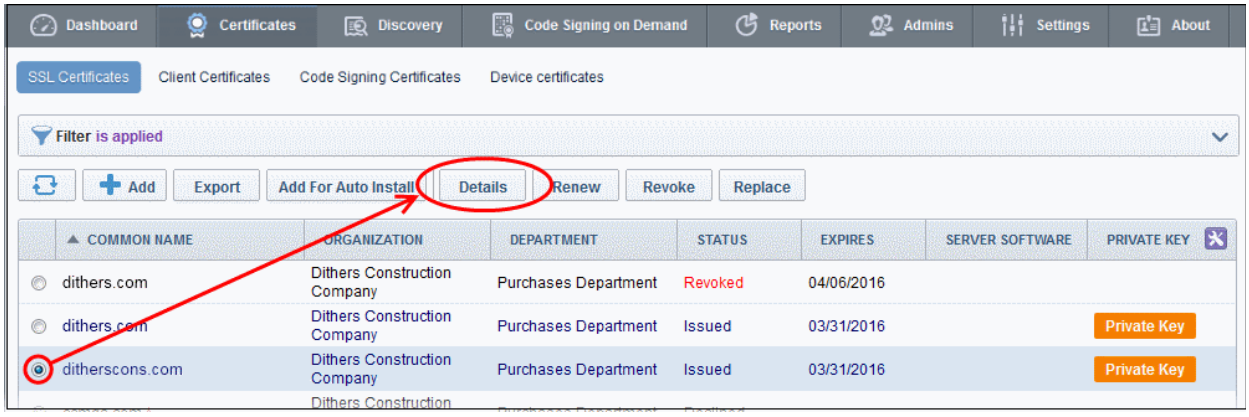
During the download process, SCM sends a download command to the agent, which, in turn, requests for authentication of the administrator and checks for their authentication certificate. Once authenticated, the private key agent enables the administrator to download the private key in a `.key` format.

NOTE: Even though the download is initiated via SCM, the private key is not transferred to the SCM servers, therefore the private key never passes outside your network.

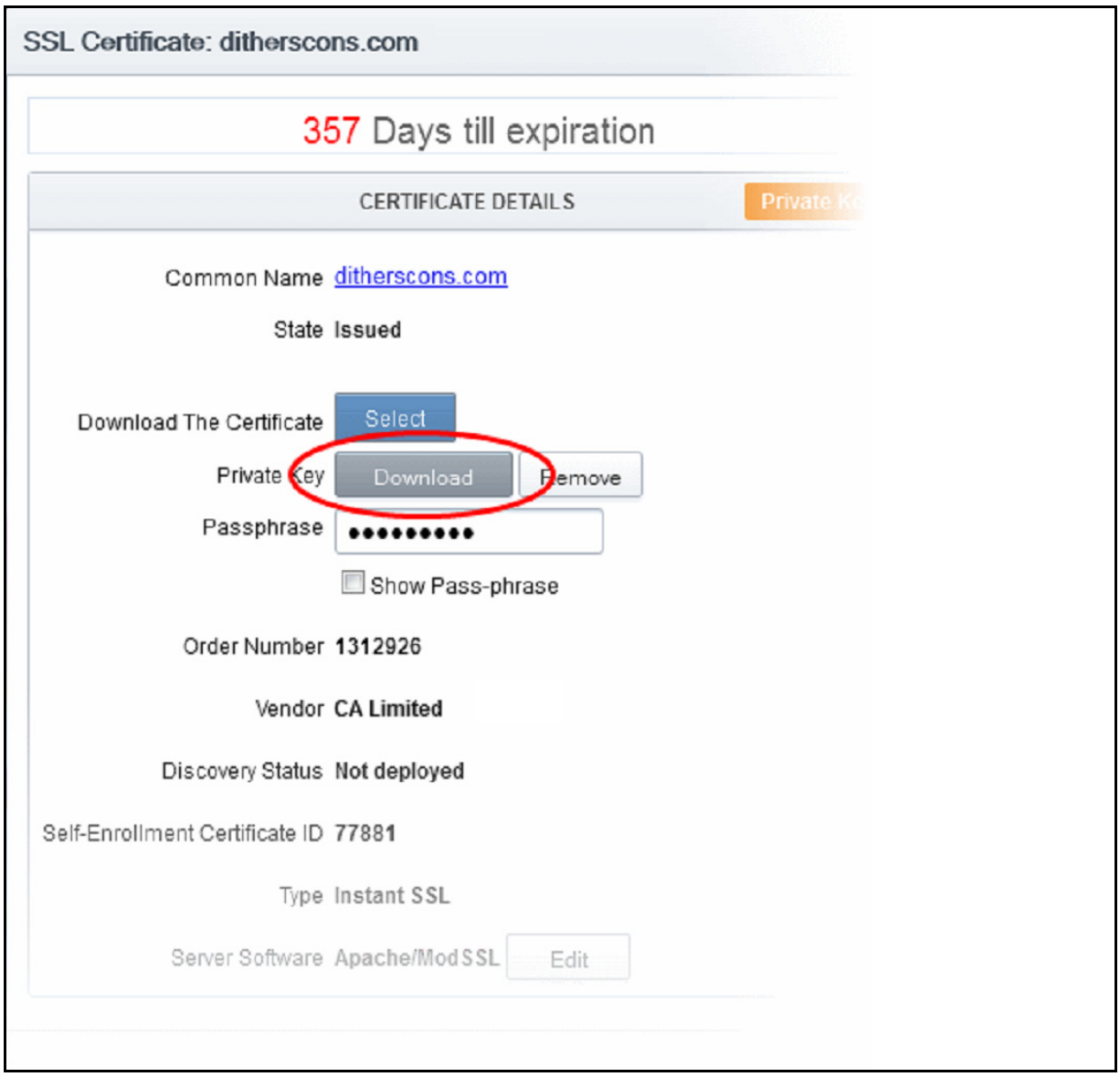
You download the private key as follows:

1. Navigate to **Certificates > SSL Certificates**.
2. Select the certificate for downloading the private key, and click **Details** to open the **Certificate Details** dialog, as shown in the following illustration.

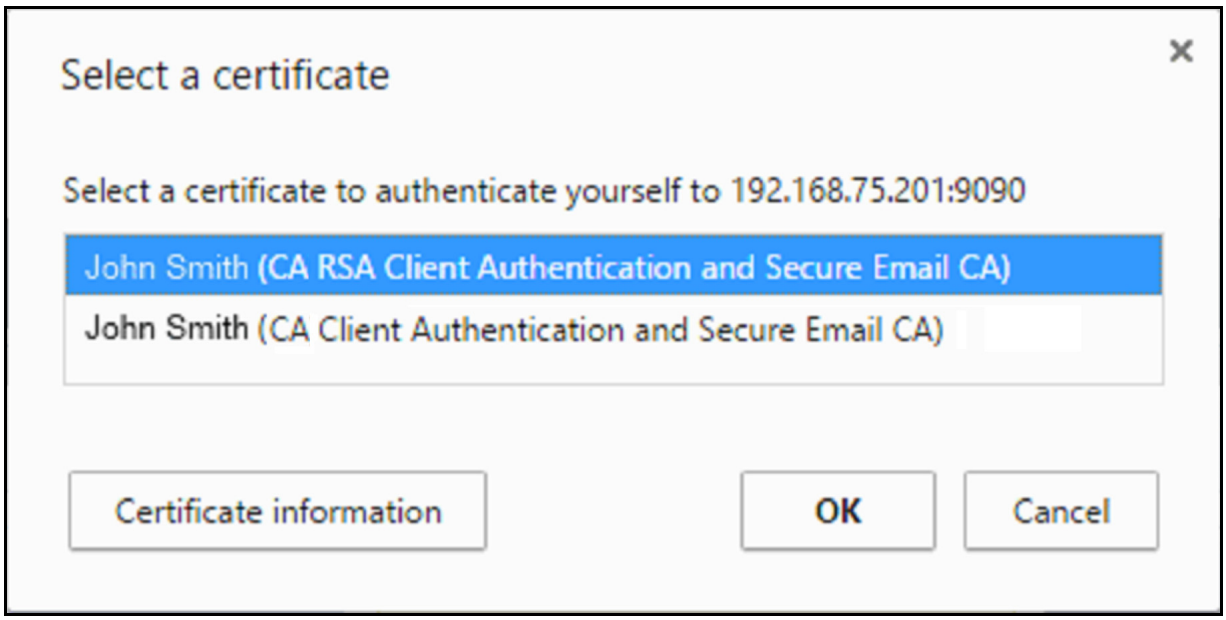
   You can search for a certificate by using filter options.



3. Click **Download** on the **SSL Certificate** dialog, as shown in the following illustration.



The PKS agent requests for authentication and searches for the personal authentication certificate of the administrator in the computer from which the administrator has logged in. If certificates are found, the **Select Certificate** dialog is displayed for the administrator to select the appropriate certificate and click **OK**, as shown in the following illustration.

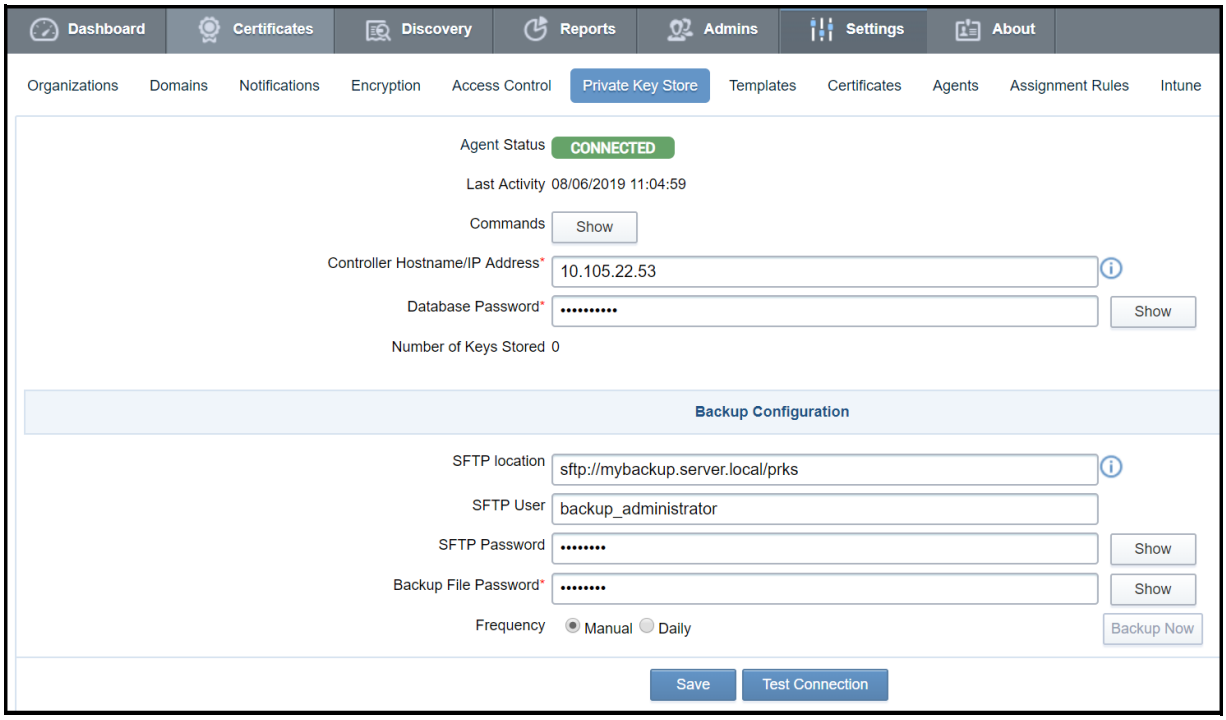


Upon authentication verification, the download dialog is displayed.

6.5.4 How to Back Up and Restore the PKS

You can configure backup for the PKS at a remote SFTP server and run periodic backups manually, as follows:

1. Navigate to **Settings > Private Key Store**, as shown in the following illustration.



2. Complete the **Backup Configuration** fields based on the information provided in the following table.

Field	Description
SFTP location	The path of the backup location in the SFTP server at which the PKS backup is to be created.
SFTP User	The user name of your user account in the SFTP server.
SFTP Password	The password of your user account in the SFTP server.
Backup File Password	The password for your backup file. This is required when restoring from the backup.
Frequency	The schedule at which backups should occur. The valid values are: • Manual—Indicates that the backup is to run automatically. Clicking **Backup Now** runs an on-demand backup. • Daily—Indicates that the backups are to be created daily at the time specified in the **Next backup at** list. Select the time in UTC when it should run.

3. Click **Save** for your configuration to take effect.

Upon completion, you can run the backup any time by clicking **Backup Now** in the **Private Key Store** area. It is recommend to enable automatic backups or to run the backup every time a new private key is uploaded to the PKS or a new certificate is enrolled via an auto-CSR generation tool.

If the PKS agent is lost, you can restore the keys from the backup by creating another PKS in the same or different server on your local network and configuring it from the **Private Key Store** area.

You restore a private key as follows:

1. Navigate to **Settings > Private Key Store**.
2. Complete the **Restore Existing Private Keys Store From Backup** fields based on the information provided in the following table.

Field	Description
SFTP location	The path of the backup location in the SFTP server at which the PKS backup is to be created.
SFTP User	The user name of your user account in the SFTP server.
SFTP Password	The password of your user account in the SFTP server.
Backup File Password	The password for your backup file. This is required when restoring form the backup.

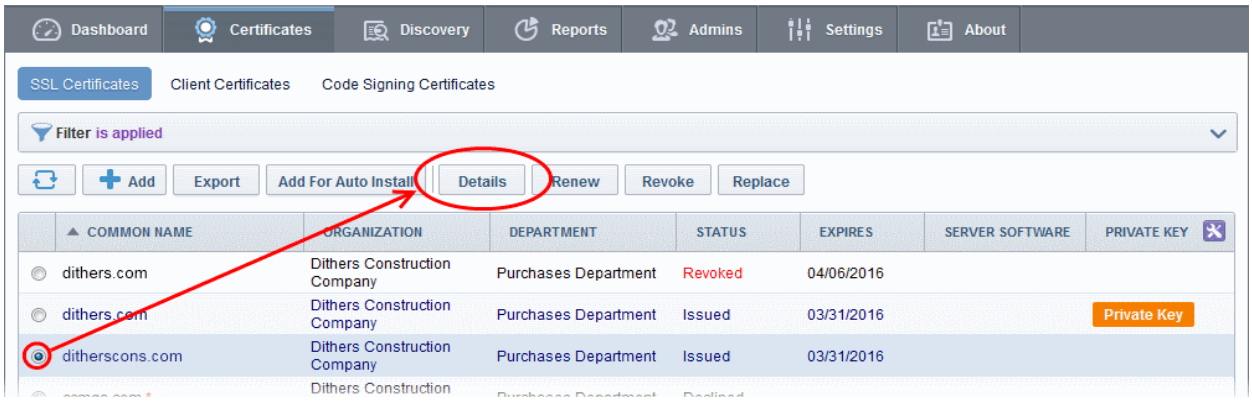
3. Click **Restore**.

6.5.5 How to Remove Private Keys from the PKS

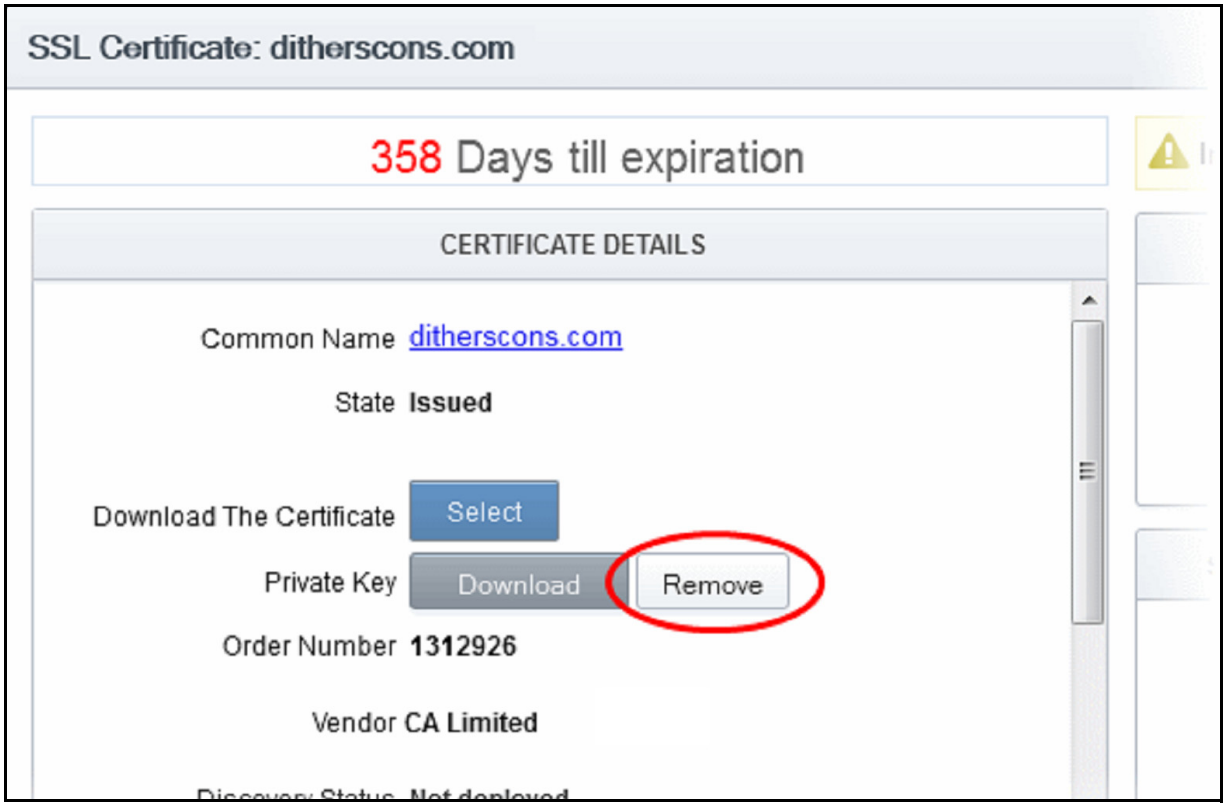
Private keys can be removed from the PKS when they are no longer required, as follows:

1. Navigate to **Certificates > SSL Certificates**.
2. Select the certificate whose private key is to be removed, and then click **Details** to open the **Certificate Details** dialog, as shown in the following illustration.

   You can search for a certificate by using filter options.



3. Click **Remove** on the **SSL Certificate** dialog, as shown in the following illustration.

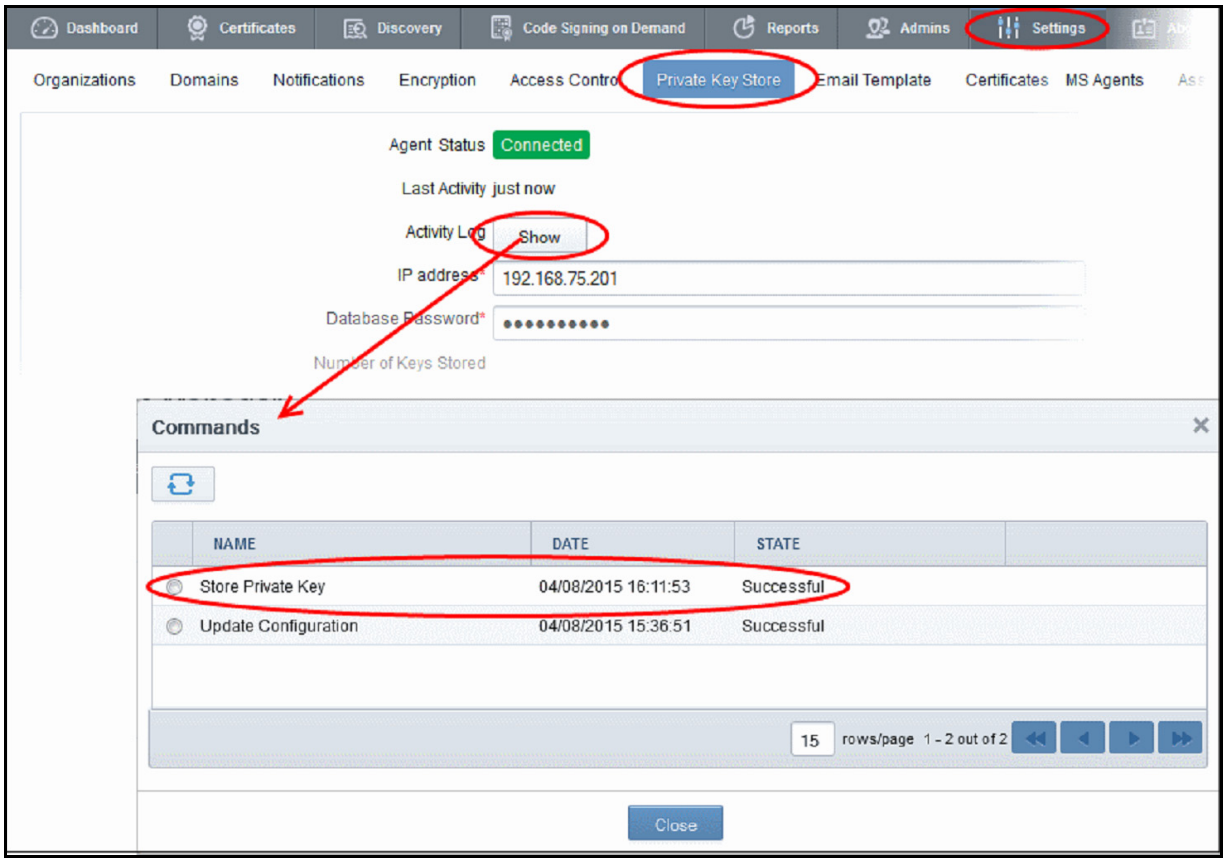


6.5.6 How to View the Agent Activities

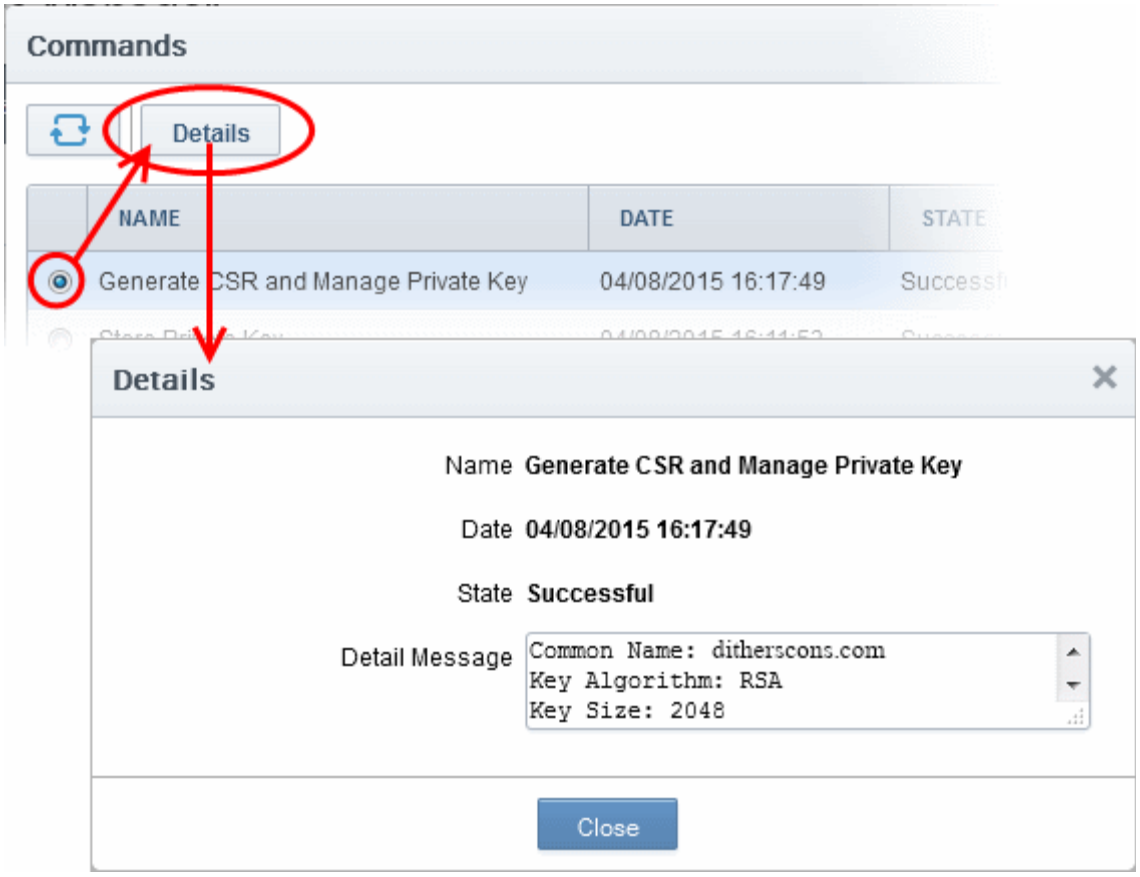
You can view the list of commands received by the agent from the SCM and their status.

You can view a list of PKI agent commands as follows:

1. Navigate to **Settings > Private Key Store** and click **Show** located next to the **Activity Log**, as shown in the following illustration.



This opens the **Commands** dialog with the list of commands received by the agent in chronological order, as shown in the following illustration. Selecting a command and clicking **Details** displays the information about the command.



The following table lists settings available in the **Details** dialog.

Field	Description
Name	The command received from SCM during the consecutive polls. The valid values are: • No Command—Default command. Indicates that there is no pending tasks for the agent. • Update Configuration—Indicates that the configuration synchronization is required. For example, during first start of the agent or agent configuration changed on the SCM side by the administrator. • Generate CSR and Manage Private Key—Indicates enrollment for a new certificate with an auto-CSR generation tool. The agent generates the key pair and CSR. The private key is stored in the database and the CSR is transferred to the SCM side for further certificate enrollment. • Store Private Key—Indicates that an administrator manually uploads a private key associated with a managed certificate for storage and management by the PKS.
Date	The precise date and time when the command was received.
Status	The execution status and result of the command.

6.6 Configuring JVM Parameters for Agents

You can configure Java Virtual Machine (JVM) parameters for all agent types. These settings are preserved when performing agent updates. The agents available to you are dependent on your operating system, as follows:

- Windows—network agent, private key agent, and MS agent
- Linux—network agent, private key agent, and CSoD agent

The JVM may need to be configured for the following reasons:

- To switch to a different SSL trustStore.

  This can be done using the `javax.net.ssl.trustStore` system property.
- To control the authentication schemes used when connecting via a proxy.

  This can be done using the `jdk.http.auth.tunneling.disabledSchemes` system property.

6.6.1 How to Modify JVM Parameters on Windows

When working with a network agent or private key agent that is installed on Windows, do the following:

1. Navigate to the agent's `bin` directory (located within the agent's `CCMExtraAgent` or `CCMPkController` directory respectively).

   Your path may be similar to the following examples:

   `C://Program Files (x86)\COMODO\CCMExtraAgent\bin`

   `C://Program Files (x86)\COMODO\CCMPkController\bin`
2. Open `ccmextragentw.exe` or `ccmpkcontrollerw.exe` to bring up the agent's properties.
3. Navigate to the **Java** tab.
4. Use **Java Options** to add or modify JVM parameters as required.
5. Restart the service to have the changes applied.

When working with an MS agent installed on Windows, do the following:

1. Navigate to the agent's `Conf` directory (located within the agent's `CcmMSAgent` directory).
2. Open the `start-agent.ini` file.
3. Add or modify JVM parameters as required.
4. Save the changes and close the file.
5. Restart the service to have the changes applied.

6.6.2 How to Modify JVM Parameters on Linux

1. Navigate to the agent's `Conf` directory (located within the agent's `CcmExtraAgent`, `CCMPkController`, or `CCMCSController` directory).
2. Open the `start-agent.ini` file.
3. Add or modify JVM parameters as required.
4. Save the changes and close the file.

5. Restart the service to have the changes applied.

6.7 Configuring Agent HTTP Proxy Servers

If the use of an HTTP proxy server is required in your organization, you need to configure the agent.properties file to enable communication between your agent and SCM.

You can configure an agent for use with an HTTP proxy server as follows:

1. Navigate to your agent.properties file.

   For example, the path for a network agent might be the following:
   `Windows(C:)/Program Files (x86)/COMODO/CCMExtraAgent/conf/agent.properties`
2. In the `agent.properties` file, specify your proxy settings based on the information in the following table.

Proxy Setting	Description
proxy.pacurl	Specifies the URL of a proxy auto-configuration (PAC) file. If using a PAC file, it is not necessary to fill out the remaining proxy settings.
proxy.host, proxy.port	Specify a proxy server explicitly.
proxy.user, proxy.password	Specify the appropriate username and password if the proxy server requires authentication.

3. Save the file.
4. Restart the agent using the `certsrv.mcs` snap-in.

7

Configuring Settings

This chapter describes how to configure all settings available in SCM.

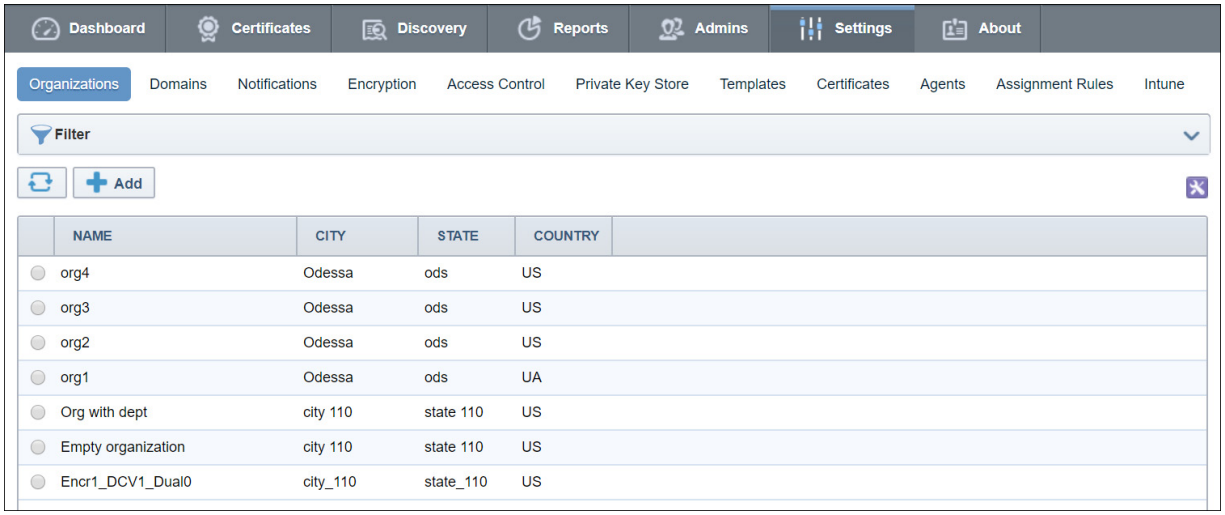
This chapter describes the following topics:

- The Settings Configuration Overview
- Configuring Organizations
- Configuring Departments
- Managing and Configuring Domains
- Configuring Notifications
- Configuring Key Escrow and Encryption
- Configuring Access Control
- Configuring a Private Key Store
- Configuring Certificates
- Configuring Templates
- Managing SCM Agents
- Defining Auto-Assignment Rules for External Certificates
- Configuring SCM for Microsoft Intune
- Configuring the Azure Key Vault Integration

7.1 The Settings Configuration Overview

In SCM, the certificate management is performed through the **Settings** tab which allows you to perform most of the SCM configurations.

The **Settings** tab shown in the following illustration contains a maximum of eleven areas. This number depends on the privilege level of the currently logged-in administrator.



The **Organizations** area enables MRAO and RAO administrators to view existing organizations, add, edit, and delete organizations, as well as assign departments and domains to the organizations. MRAOs can initiate organization validation so the organization is authorized for certificate issuance.

The **Departments** area is visible only to DRAO class administrators who see this area instead of the **Organizations** area. The **Departments** area allows DRAOs to view all departments that have been delegated to them and to request new domains for those departments.

The **Domains** area contains a list of all domains that have been created in SCM. The interface allows you to add new domains, edit domain details, activate or deactivate a domain, delegate the domain to an organization or department, and to select the validation type.

The **Notifications** area defines email notifications to specific personnel based on a range of criteria and triggers.

NOTE: It is recommended that as a MRAO, RAO Client Certificate, or DRAO Client Certificate administrator, you familiarize yourself with the information in this document before creating your first organization or department, mainly because once the key escrow options have been defined they cannot be reversed.

The **Access Control** area enables administrator to grant access only for specified IP range.

The **Templates** area enables MRAO administrators to add custom links and text to self-enrollment pages through the **Enrollment Forms** tab. On the **Email Templates** tab, MRAO and RAO administrators can customize the contents of templates for event-based email notifications. DRAO administrators can edit templates for their department via the **Edit Department** dialog accessible by navigating to **Settings > Departments**, and then clicking **Edit**.

The **Private Key Store** area allows the MRAO to configure the agent software which manages the private keys and their backups.

The **Certificates** area enables MRAO administrators to select the types and validity period of certificates available through the built-in application form and self-enrollment form. MRAO administrators can also add custom fields to these forms.

NOTE: The custom fields can be added only if this feature is enabled for your account. Contact your Sectigo account manager for more information.

The **Agents** area enables MRAO administrators download Network Agents and MS Agents, view existing agents, modify agent settings, and auto-install SSL certificates. Once installed, MS Agents fetch details about the network and all types of certificates installed on all servers, devices and AD objects in the network. MS Agents are installed on the AD server to integrate the AD to the SCM console. It is also used to discover all types of certificates in the AD server. This area also contains CSoD Agents that are used to automate the process of issuance of code signing certificates to developers and code sign the uploaded files.

The **Assignment Rules** area allows MRAO administrators to create rules that assign certificates found during a discovery scan to a specific organization or department.

The **Intune** area allows MRAO administrators to configure SCM to use Microsoft Intune. For more information, see "Using SCM with Microsoft Intune" on page 599.

7.2 Configuring Organizations

The creation of organizations and departments and the association of these entities with a domain is an important step towards the issuance and effective management of SSL, code signing, client, and device authentication certificates via the SCM UI, for the following reasons:

- Organizations are umbrella entities created by administrators for the purposes of requesting, issuing, and managing certificates for domains and employees.
- Organizations can be subdivided into departments for the purpose of certificate and end-user management.
- Each organization can have multiple departments. Furthermore, each organization and each department can have multiple domains delegated to it.
- It is possible to assign organization-level administrators (RAO) and department-level administrators (DRAO).
- Depending on their roles, organization-level administrators can manage certificates, domains, and users belonging to their organization and any of its departments. They are also able to create new departments and appoint department administrators.
- Depending on their roles, department-level administrators can view and manage only those certificates, domains, and users belonging to the department for which they have been delegated responsibility.

The following table lists naming conventions used by SCM for organizations and administrators.

SCM Entity	Administrator Types
Organization	RAO Administrator SSL RAO Administrator Client RAO Admin Code Signing RAO Admin Device Certificate

SCM Entity	Administrator Types
Department	DRAO Administrator SSL DRAO Administrator Client DRAO Administrator Code Signing DRAO Administrator Device Certificate
MRAOs have complete visibility of and control over all organizations and departments.	

Although it is recommended that you plan any organizational and administrative structure beforehand, it is possible to rearrange and reconfigure it later. Organizations, departments, domains, and administrators are each created and configured as independent entities in SCM. It is the association and delegation of these entities into a coherent superstructure which forms the key to an effective certificate management hierarchy for your enterprise. For more information, contact your Sectigo account manager.

In order to maximize the effectiveness of your SCM implementation, it is important that you first decide the structure of your organizational and administrative hierarchy. SCM allows you to create and delegate hierarchies that are as simple or sophisticated as you require.

The following example outlines a hypothetical issuance scenario followed by two or three alternative solutions that are possible through SCM.

Example 1:

Scenario: You wish to issue only SSL certificates for a single first-level domain and two sub-domains.

Solution 1—Simple:

- Create a single organization.
- Do not create departments.
- Delegate all the domain and the subdomains to this single organization.
- The MRAO manages all SSL certificates for all domains.

Organization Name	Department Name	Administrator	Could be used to manage certificates for
Organization 1		MRAO	http://website_1.com
			http://payments.website_1.com
			http://mail.website_1.com

Solution 2—Intermediate:

- Create three organizations.

- Do not create departments.
- Delegate each domain to a separate organization.
- Create three RAO SSL administrators.
- Delegate one RAO SSL administrator to each of the organizations.

Organization Name	Department Name	Administrator	Could be used to manage certificates for
Organization 1		RAO SSL ADMIN 1	http://website_1.com
Organization 2		RAO SSL ADMIN 2	http://payments.website_1.com
Organization 3		RAO SSL ADMIN 3	http://mail.website_1.com

Solution 3—Intermediate:

- Create a single organization.
- Create three departments under this organization.
- Delegate each domain to one of these departments.
- Create one RAO SSL administrator.
- Delegate the RAO SSL to control the organization (and its departments).
- Create three DRAO SSL administrator.
- Delegate one DRAO SSL administrator to each of the departments.

Organization Name	Department Name	Administrator	Could be used to manage certificates for
Organization 1	Department 1	DRAO SSL ADMIN 1	http://website_1.com
	Department 2	DRAO SSL ADMIN 2	http://payments.website_1.com
	Department 3	DRAO SSL ADMIN 3	http://mail.website_1.com

Example 2:

Scenario: Your company issues both SSL certificates and client certificates. Your company operates two distinct websites, each with its own unique first-level domain name and two subdomains.

Solution 1—Very Simple:

- Create a single organization.

- Do not create departments.
- Delegate both first-level domains and all subdomains to this single organization.
- The MRAO manages all SSL certificates and all client certificates for all domains.

Organization Name	Department Name	Administrator	Could be used to manage certificates for
Organization 1		MRAO	http://website_1.com
			http://payments.website_1.com
			http://mail.website_1.com
			http://website_2.com
			http://payments.website_2.com
			http://mail.website_2.com

Solution 2—Sophisticated:

- Create two organizations.
- Create three departments in each organization.
- Delegate one first-level domain and its subdomains to each of the three departments in an organization.
- Create one RAO administrator. Assign this single RAO with SSL and client administrative roles.
- Delegate the RAO to control both organizations (and all their departments, domains, and subdomains).
- Create three DRAO SSL administrators.
- Create six DRAO Client Certificate administrators.
- Delegate one DRAO administrator per certificate type to each of the three departments.

As a result, you have two organizations, each with three departments. Each of these departments is associated with a distinct first-level domain or subdomain. Each department has *two*

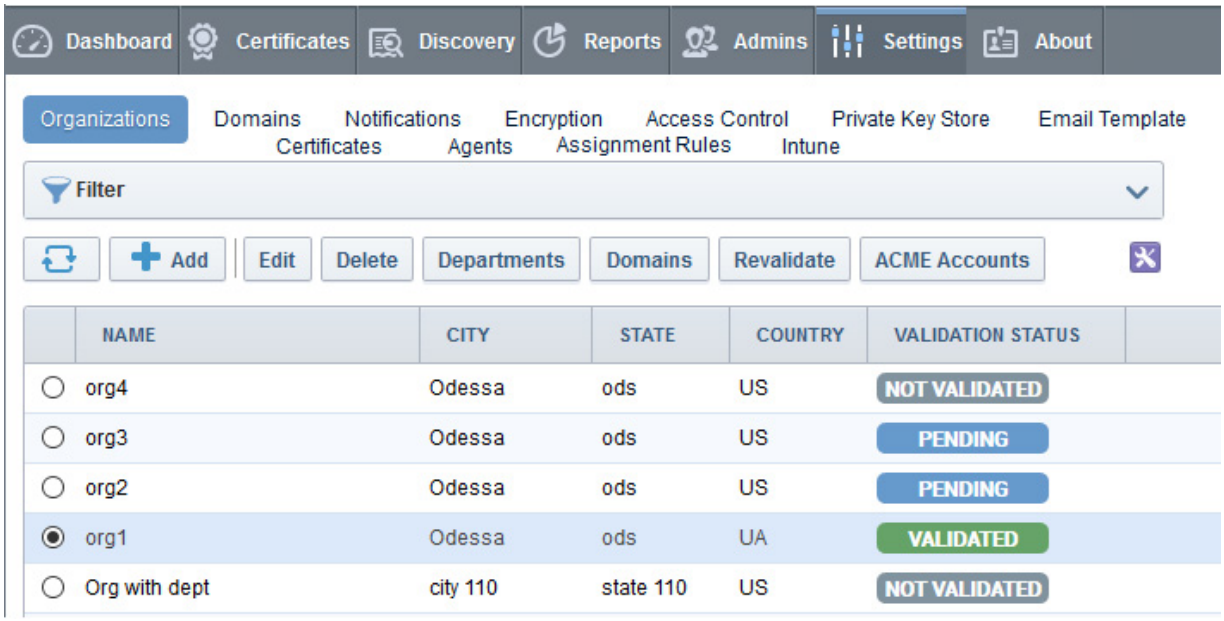
departmental administrators, each responsible for a particular certificate type. All of these DRAOs are subordinate to the RAO who is, in turn, subordinate to the MRAO.

Organization Name	Department Name	Administrator	Could be used to manage certificates for
Organization 1	Organization 1 - Department 1	DRAO SSL ADMIN 1	http://website_1.com
		DRAO Client Certificate ADMIN 1	http://website_1.com
	Organization 1 - Department 2	DRAO SSL ADMIN 2	http://payments.website_1.com
		DRAO Client Certificate ADMIN 2	http://payments.website_1.com
	Organization 1 - Department 3	DRAO SSL ADMIN 3	http://mail.website_1.com
		DRAO Client Certificate ADMIN 3	http://mail.website_1.com
Organization 2	Organization 2 - Department 1	DRAO SSL ADMIN 1	http://website_2.com
		DRAO Client Certificate ADMIN 4	http://website_2.com
	Organization 2 - Department 2	DRAO SSL ADMIN 2	http://payments.website_2.com
		DRAO Client Certificate ADMIN 5	http://payments.website_2.com
	Organization 2 - Department 3	DRAO SSL ADMIN 3	http://mail.website_2.com
		DRAO Client Certificate ADMIN 6	http://mail.website_2.com

7.2.1 How to Manage Organizations

You manage organizations by navigating to **Settings > Organizations** from the main UI, as shown in the following illustration.

NOTE: This area is not visible to a DRAO who instead sees the Departments area.



The **Organizations** area does the following:

- Lists all organizations available to you as an administrator as per your privilege level.
- Facilitates the creation and deletion of organizations and departments.
- Facilitates the modification of settings for any existing organization or department.
- Allows you to delegate domains to an organization or department.
- Allows you to initiate the organization validation process
- Allows you to search and filter organizations by name and department.

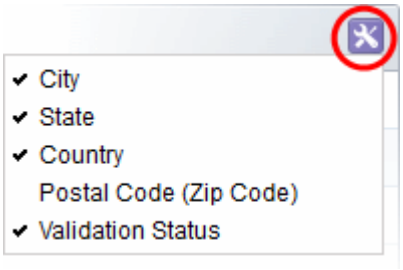
The following are the relevant administrative roles and their capabilities:

- A MRAO can see a list of all the organizations and their departments in the **Organizations** area. MRAOs can create new organizations and departments and have full control over the management of all the organizations and departments. They can initiate the process of validating organizations for the purpose of requesting and issuance of OV SSL certificates to organizations and departments.
- A RAO can only see their own organizations in the **Organizations** area. They cannot create new organizations but can manage and create departments for the organizations delegated to them.
- A DRAO cannot view the **Organizations** area. They have visibility only of the **Departments** area.

The following table provides a summary of the ability of administrator types to manage organizations and departments.

MRAO	RAO	DRAO
Can create and manage any organization. Can create and manage any department.	Can manage the delegated organization. Can create and manage subordinate departments.	Can manage delegated departments.

The following table lists the settings and elements of the **Organizations** area.

Field	Value	Description
Name		The name of the organization.
City		The city where the organization is located.
State		The state or province.
Country		The two-character country code.
Postal Code		The postal code or zip code of the location.
Validation Status		An indication of whether or not the organization is validated for the request and issuance of OV SSL certificates.
You can use the tool button to select columns to be displayed in the table: 		
Control Buttons	Add	Enables MRAOs to create a new organization for the purposes of issuing certificates to end-users and domains. Not visible to RAOs and DRAOs.
	Refresh	Refreshes the list.

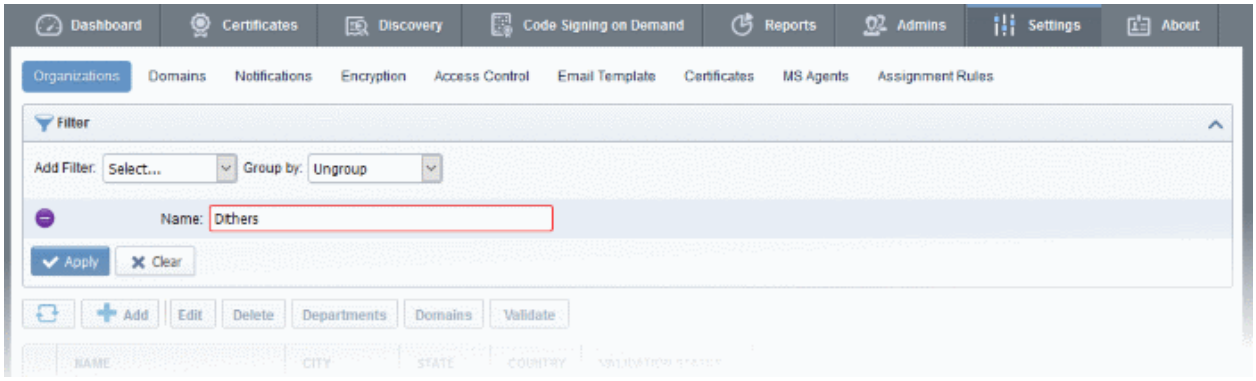
Field	Value	Description
Organization Control Buttons [a]	Edit	Enables you to modify General, Client, SSL and Code Signing Certificate settings pertaining to an existing organization.
	Delete	Deletes the organization. Not visible to RAOs and DRAOs.
	Departments	Enables you to view and manage departments that belong to that organization.
	Domains	Enables you to view, edit, and delegate domains to the organization and the departments within the organization.
	Validate	Enables you to initiate the organization validation process.
	ACME Accounts	Enables creation and management of ACME accounts for the organization.

a. The organization control buttons appear only on selecting an organization. These buttons differ depending on the organization's validation status and on the features enabled for the organization's account.

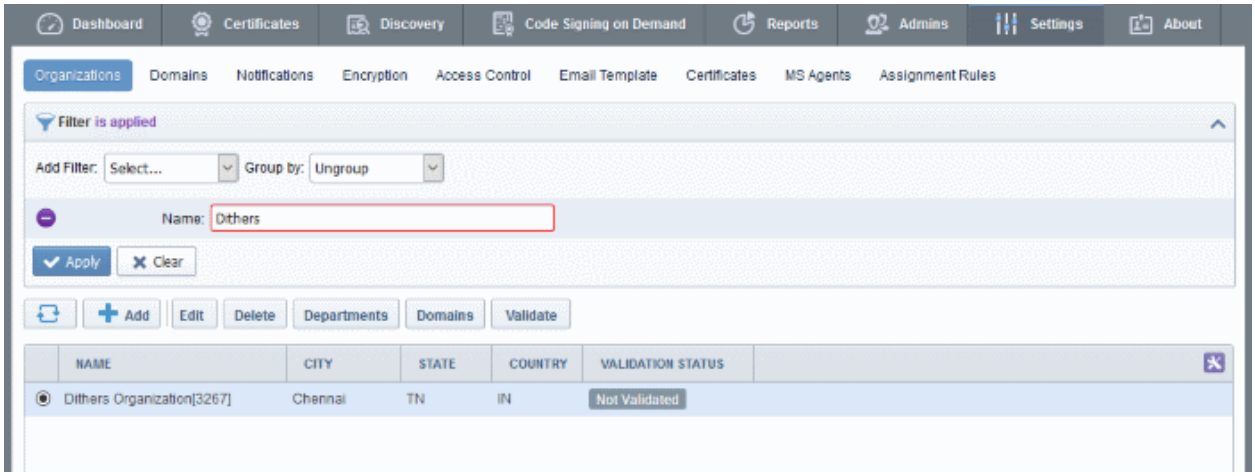
7.2.2 How to Sort and Filter Organizations

You can sort items in the alphabetical order by clicking a column header, and you can use filters to search for particular organizations.

You apply filters via the **Filter** stripe. To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection in the **Add Filter** list.



Then you enter or select the filter parameter as per the selected criteria.



You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **Organizations** screen, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

7.2.3 How to Create a New Organization

You create a new organization by navigating to **Settings > Organizations**, and then clicking **Add**.

A MRAO needs to create an organization before you can order certificates for employees, websites, code signing, or devices.

Organizations are uniquely identified by a combination of the organization's **Access Code** and the **Common Name** specified in the **General** properties. More than one organization can share the same access code or common name, but no two organizations can share both.

If OV certificates are enabled for the SCM account, the organizations for which OV certificates are requested, need to be validated by Sectigo. See "Validating an Organization" on page 363 for more information.

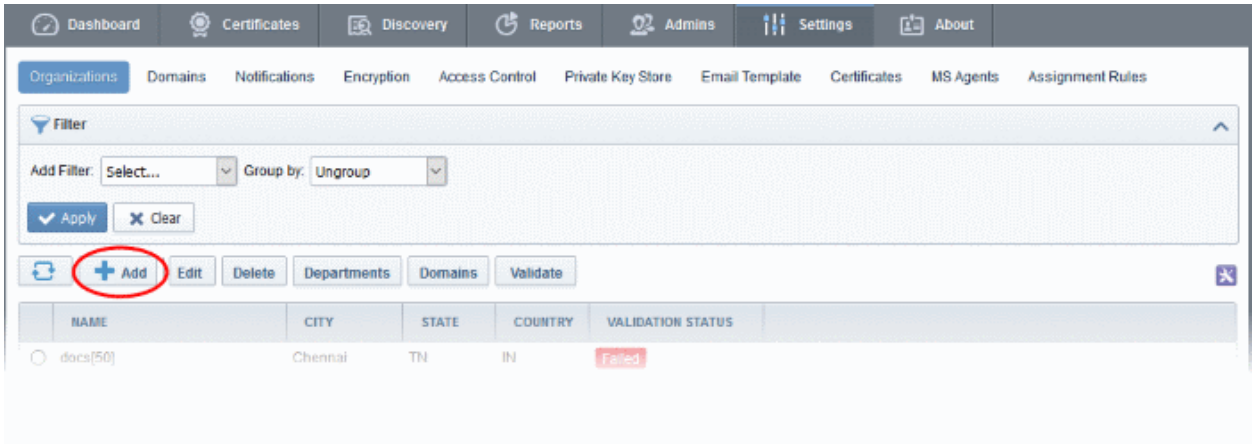
Once an organization is created, an appropriately privileged administrator can do the following:

- Request SSL certificates using the SCM interface for the domain that is associated with that organization. They can approve or reject certificate requests.
- Create multiple departments within an organization and associate each department with a distinct domain.
- Assign membership of that organization to end-users and provision them with client certificates for the common name (domain) that is associated with that organization. The list of end-users is viewable by navigating to **Certificates > Client Certificates** via the main UI.
- Manage the client certificates of end-users belonging to that organization by navigating to **Certificates > Client Certificates** via the main UI.
- Manage SSL certificates for the organization by navigating to **Certificates > SSL Certificates** via the main UI.

- Manage code signing certificates for the organization by navigating to **Certificates > Code Sign Certificates** via the main UI.
- Manage device certificates for the organization by navigating to **Certificates > Device Certificates** via the main UI.
- Edit the general, client certificate, and SSL certificate parameters that apply to that organization by selecting an organization and clicking **Edit** in the **Organizations** area.
- Utilize the certificate discovery tool to audit, and then monitor all certificates on the network.
- Configure a wide range of email notifications for the organization.
- View, filter, and export a variety of reports and activity logs for the organization.

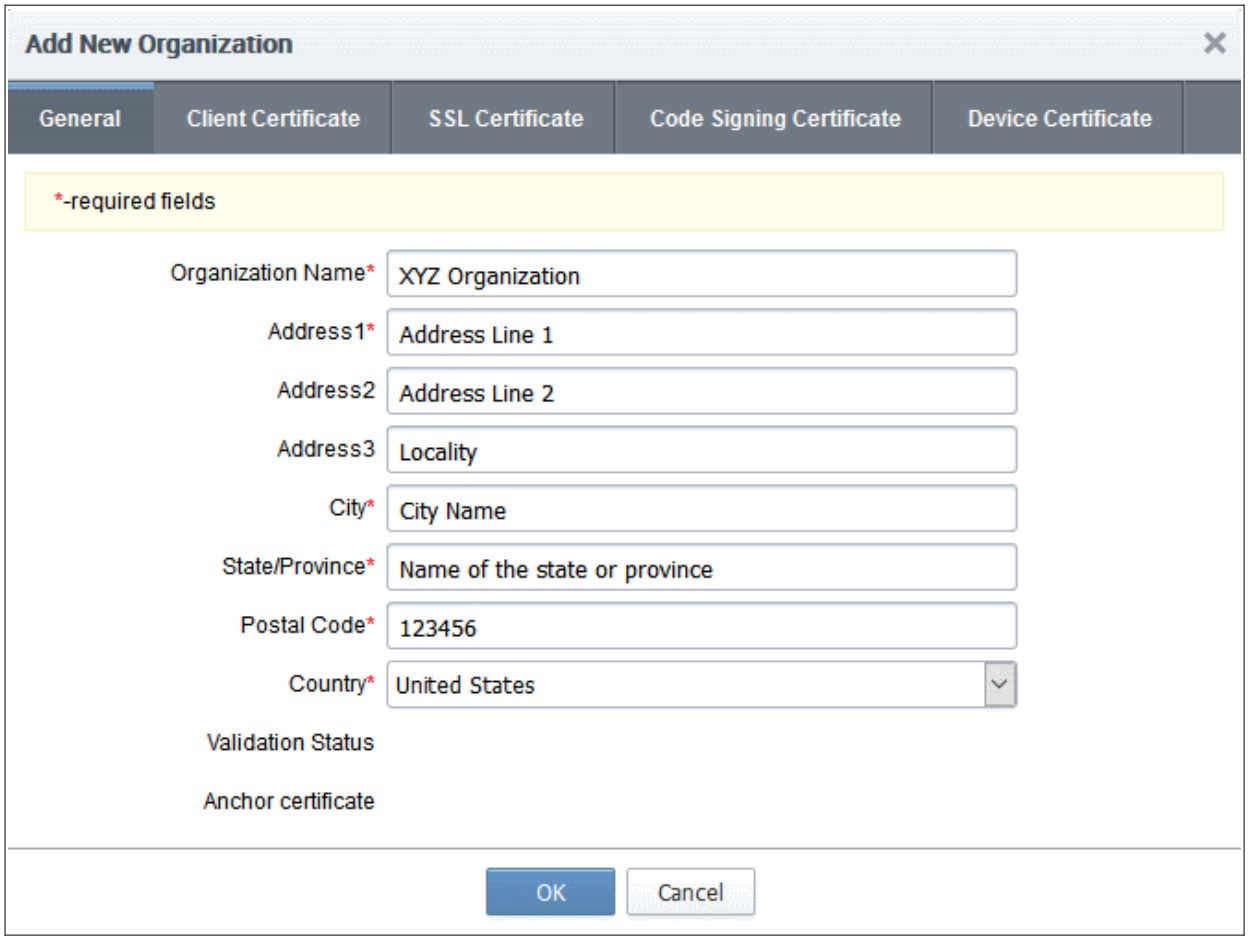
MRAOs can add new organizations by clicking **Add**, as shown in the following illustration. This opens the **Add New Organization** dialog which includes the following setting areas:

- General
- EV Details
- Client Certificate
- SSL Certificate
- Code Signing Certificate
- Device Certificate



7.2.3.1 Using the General Settings Area of the Add New Organization Dialog

The **General** settings area of the **Add New Organization** dialog shown in the following illustration allows MRAOs to configure high-level details related to an organization.



The **Organization Name** and **Address** values specified for an organization populate the **Subject** field of any SSL certificates requested and issued for this organization.

You need to ensure that values entered in the fields match those used when generating a CSR.

The details entered in the **General** section are used for client, SSL and code signing certificates requested on behalf of that organization.

In order to issue OV SSL certificates for organizations and their departments, your SCM account should have been enabled for OV certificates, and the organization should be validated by Sectigo. The validation process for newly created organizations can be initiated by MRAOs and when the process is completed successfully, the **Validation Status** field displays Validated. The **Anchor Certificate** displays as ON and this is used for an OV reference by SCM whenever an organization validated SSL certificate is requested for an organization or its departments. The validation status can be one of (1) Not Validated, indicating that the validation process has not been started; (2) Validated, indicating that the organization has been validated and anchor certificate issued; (3) Pending, indicating that the validation process started and not completed; (4) Failed, indicating that the validation process failed for the organization; (5) Expired, indicating that the validation period of 36 months is expired for the organization.

Client and SSL certificates may only be automatically issued to common names of domains and sub-domains delegated to the organization which Sectigo has prevalidated. If you apply for certificates on a new domain, then Sectigo first needs to validate your ownership of the domain before the certificate can be issued for it. See "Delegating and Redelegating Existing Domains" on page 404 for more information.

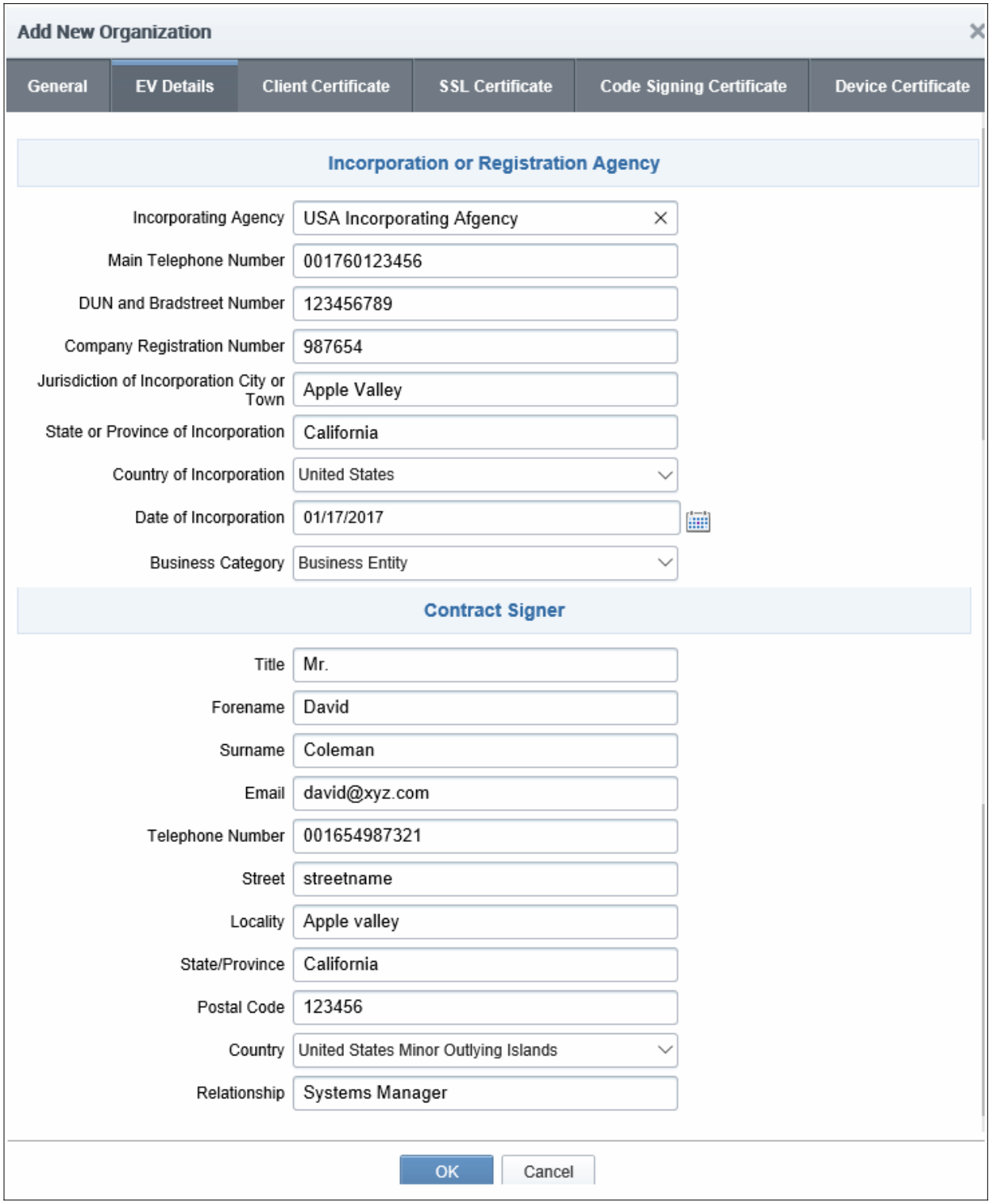
The following table lists the settings and elements of the **General** area, where mandatory fields are marked with the red asterisk.

Field	Description
Organization Name	The name of the organization to be created.
Address 1	The new organization's address (used for issuing SSL and client certificates).
Address 2	The new organization's address (used for issuing SSL and client certificates).
Address 3	The new organization's address (used for issuing SSL and client certificates).
City	The city where the organization is located (used for issuing SSL and client certificates).
State / Province	The state or province (used for issuing SSL and client certificates).
Postal Code	The postal code (used for issuing SSL and client certificates).
Country	The two-characters country code (used for issuing SSL and client certificates).
Validation Status	The progress of OV for the organization. This field is displayed only if OV certificates are enabled for the SCM account.
Anchor Certificate	The status of the organization's anchor certificate. An anchor certificate is a record of verified address and company registration information about the organization. It is used as a reference to accelerate validation whenever an OV SSL certificate is requested for the organization. The anchor certificate is only issued after organization validation has been completed once. The anchor certificate field is shown only if OV certificates are enabled for your account.

7.2.3.2 Using the EV Details Area of the Add New Organization Dialog

The **EV Details** area shown in the following illustration allows appropriately privileged administrators to enter the details of the organization that are required for validation purpose before the issuance of EV SSL certificates for the organization and its departments. The details provided in these fields are auto-populated in the EV SSL certificate request form. If you leave these fields blank, the details are fetched from the EV SSL certificate request form and automatically filled when the request is submitted.

The **EV Details** tab is displayed only if Extended Validation Registration Authority (EVRA) feature is enabled for your account. Contact your Sectigo account manager regarding this feature.



The following table lists the settings and elements of the **EV Details** area.

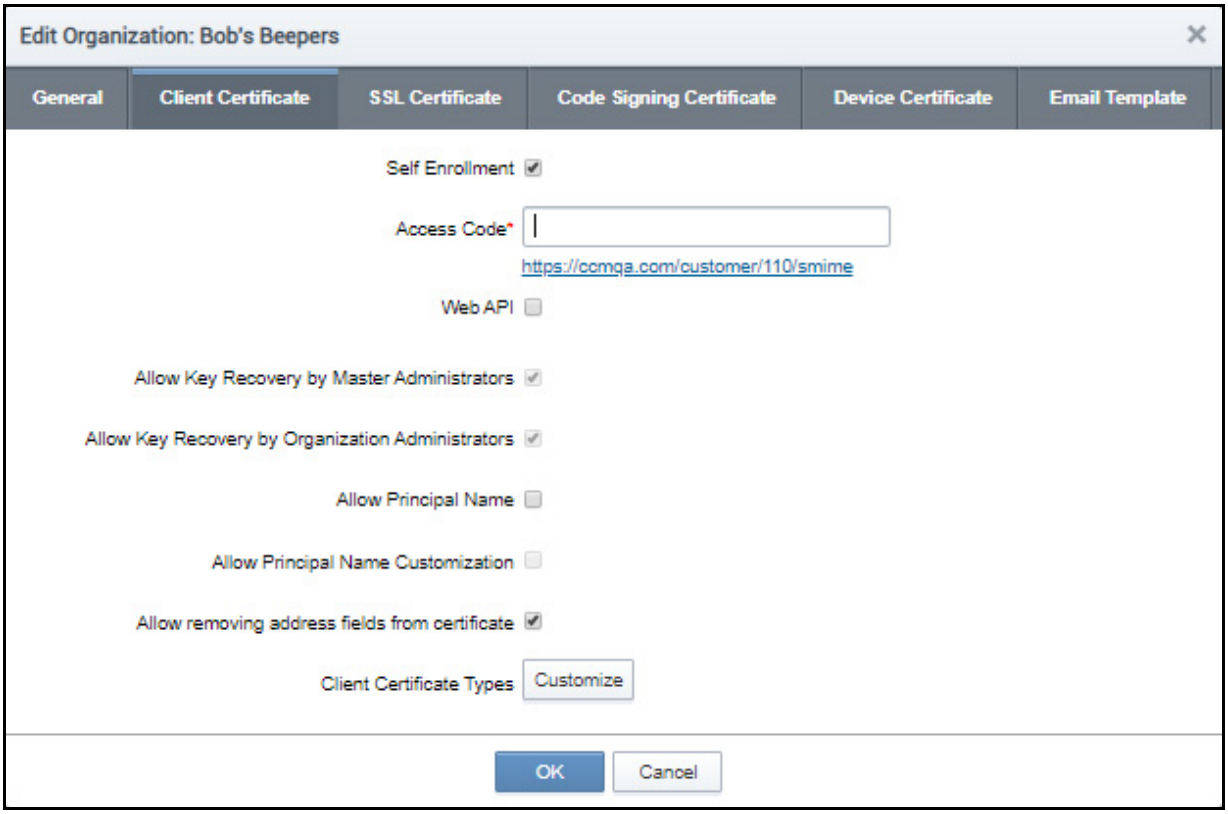
Field	Description
Incorporating Agency	The name of the incorporating agency in whose records the name of the organization exists as a legal entity.
Main Telephone Number	The primary telephone number of the incorporating agency.
DUN and Bradstreet Number	The nine digit number issued by D&B to the organization.
Company Registration Number	The registration number issued to the organization.
Locality	The locality where the organization is established.
State or Province of Incorporation	The state or province where the organization is located.
Country of Incorporation	The country where the organization is established.
Date of Incorporation	The date on which the organization was registered.
Business Category	The business category of the organization. The valid values are Private Organization, Government Entity, Business Entity, Non-Commercial Entity.
Title	The title of the contract signer. [a]
Forename	The first name of the contract signer.
Surname	The last name of the contract signer.
Email	The email address of the contract signer.
Telephone	The primary telephone number of the contract signer.
Street	The street where the contract signer is located.
Locality	The name of the locality where the contract signer is located.
State / Province	The state or province where the contract signer is located.
Postal Code	The postal code of the area where the contract signer is located.
Country	The country where the contract signer is located.
Relationship	The relationship of the contract signer with the organization.

a. Contract Signer is a person representing the organization that has signed the EV SSL contract with Sectigo.

7.2.3.3 Using the Client Certificate Area of the Add New Organization Dialog

The **Client Certificate** area shown in the following illustration allows appropriately privileged administrators to do the following with regards to the certificates issued to end-users associated with the currently selected organization:

- Enable or disable certificate self-enrollment for client certificates in the organization. This determines whether users can apply for certificates using the external application forms.
- Determine certificate types and term lengths that are available to the organization.
- Define the Web API capabilities and expiry synchronization settings relating to client certificates issued to the organization's end-users.
- Enable or disable private key recovery by MRAO and RAO administrators.
- Enable or disable principal name support for the organization.



The following table lists the settings and elements of the **Client Certificate** area, where mandatory fields are marked with the red asterisk.

Field	Description
Self Enrollment	Allows the end-users that belong to the organization to apply for a personal certificate using the enrollment form hosted (by default) at `https://SCM/customer/<customer_uri>/smime`. You can communicate the self-enrollment URI and the access code specified for the organization to an end-user, enabling the end-user for self-enrollment. Users that apply for a client certificate using the enrollment form are automatically created as a new end-user in this organization or department if they do not already exist. The list of end-users is viewable by navigating to **Certificates > Client Certificates** in the main UI. It is possible for the SCM account holders to use their own custom form templates rather than the default form supplied by Sectigo. Contact your account manager for more details on enabling this functionality.
Access Code [a]	Identifies a particular organization or department and is used to authenticate certificate requests that are made using the self-enrollment form. Organization and departments are uniquely identified by combination of the organization's access code and the common name (domain) specified in the **General** properties. Multiple organizations or departments can have the same access code or the same common name, but no single entity can share both. You should choose a complex access code containing a combination of alpha and numeric characters. This code should be conveyed to the applicant along with the URI of the sign up form. Applicants that request a certificate using the self-enrollment form need to enter this code.
Web API	Allows applicants to enroll for certificates through the Web Service API. This requires special agreement with Sectigo. For detailed instructions, refer to the Web Service API documentation.
Secret Key [b]	Specifies a phrase that is unique for all organizations. This phrase restricts access for enrolling certificates for that organization. Used in pair with Organization ID, which is visible only for already created organizations.
Allow Key Recovery by Master Administrators	If selected, allows the MRAO to recover the private keys of client certificates issued by this organization. At the point of creation, each client certificate is encrypted with the MRAO's master public key before being placed into escrow. If this field is selected, then the organization cannot issue client certificate until the MRAO has initialized their master key pair in the **Encryption** area.

Field	Description
Allow Key Recovery by Organization Administrators	If selected, allows the RAO to recover the private keys of client certificates issued by this organization. At the point of creation, each client certificate is encrypted with the RAO's master public key before being placed into escrow. If this field is selected, then the organization cannot issue client certificate until the RAO has initialized their master key pair in the **Encryption** area.
Allow Principal Name	Enables the principal name support for the organization. If enabled, the client certificates issued to the end-users of the organization includes an additional name—**Principal Name**, in addition to the RFC822 name in the **Subject Alternative Name (SAN)** field. If included, the principal name is the primary email address of the end-user to whom the certificate is issued. But this can be customized at a later time by editing the end-user if **Principal Name Customization** is enabled for the organization or department.
Allow Principal Name Customization [c]	Enables customization of the principal names by you.
Allow removing address fields from certificate	If selected, the option to hide an organization's address details is available when requesting the certificate.
Client Certificate Types - Customize (control)	Allows you to specify the client certificate types and validity periods that are available for this organization through the self enrollment forms. Clicking **Customize** opens the **Bind Client Certificate Types** dialog. All choices made via this dialog apply only to this specific organization. The **Client Certificate Types** area contains a very similar interface that allows MRAOs to determine universal certificate type and validity periods that apply to all organization If a particular certificate type or validity period is not visible in the **Bind Client Certificate Types** dialog, then it may need enabling in the **Client Certificate Types** area.

a. Appears only if Self-Enrollment is selected.
b. Appears only if Web API is selected.
c. Activated only on selecting Allow Principal Name.

7.2.3.3.1 Customizing Client Certificate Types for an Organization

The level of the client certificate type customization depends on your security role, as follows:

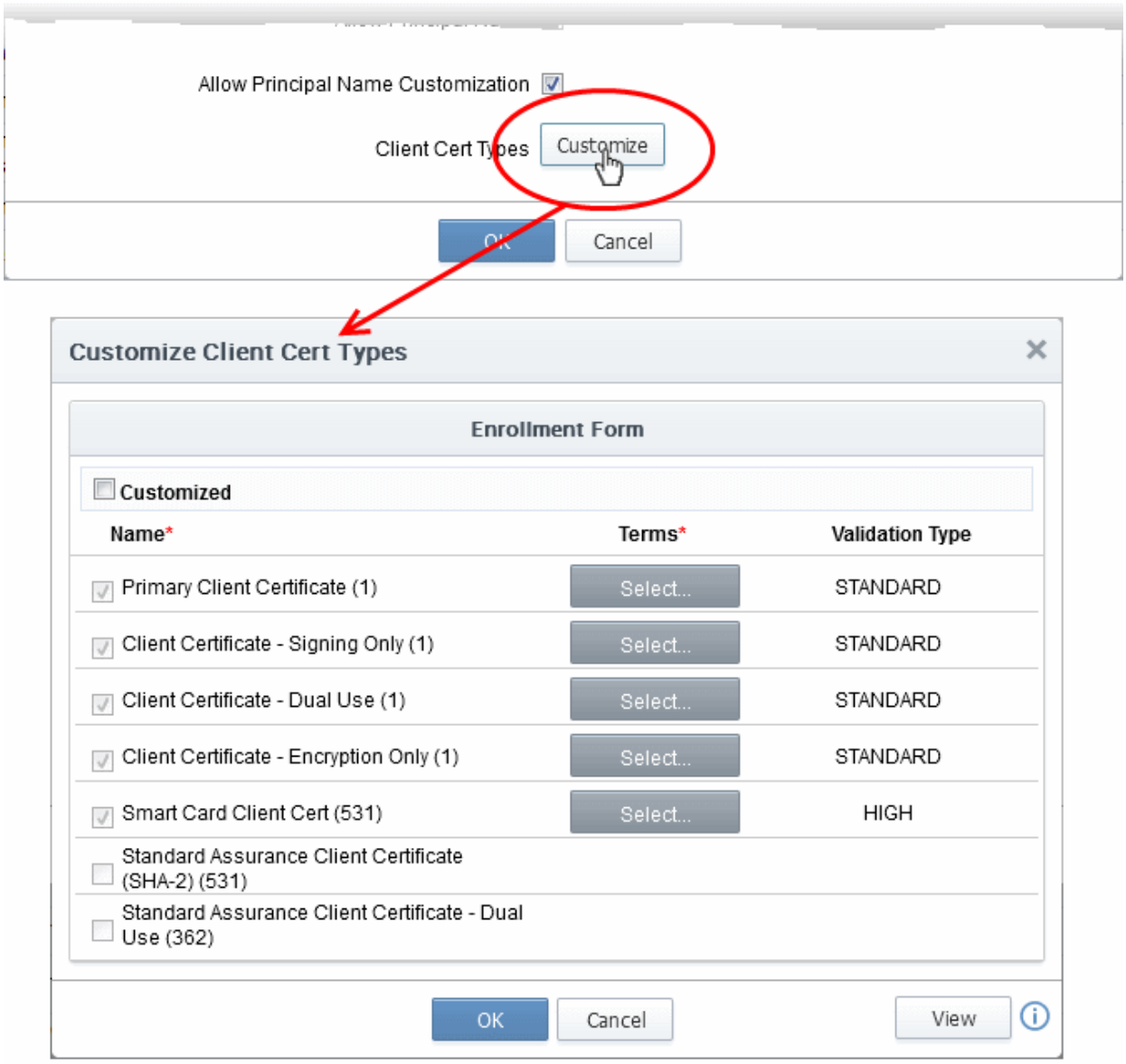
- A MRAO can customize client certificate type availability for all organizations and departments.
- A RAO Client Certificate can customize client certificate type availability only for organizations and departments that are delegated to them.
- A DRAO Client Certificate cannot customize client certificate type availability.

The types and validity period of client certificates that are available to any particular organization can be customized using the **Customize Client Certificate Types** dialog. Creating a targeted certificate roster simplifies the certificate selection procedure at the application forms and helps avoid applications for certificates which are inappropriate for an organization.

To perform the customization, use the main UI to navigate to **Settings > Certificates > Client Certificate Types** shown in the following illustration to view the list of client certificate types enabled for your account.

Sectigo offers different types of client certificates for different purposes, such as Signing Only, Encryption Only, Dual Use (Signing + Encryption), Smart Card Logon and Authentication, and so on. MRAO administrators can request their Sectigo account manager to enable multiple types of client certificates for their account.

You can also create custom client certificate types with combinations of capabilities depending on the requirements of your organization. To do so, you navigate to **Settings > Organizations**, select an organization in the list and click **Edit**. Then you navigate to the **Client Certificates** tab and click **Customize**. This opens the **Customize Client Certificate Types** dialog for that organization, as the following illustration shows. This allows you to restrict the client certificate types that is available applicants via a self-enrollment form for that organization.



By default, the **Customized** option is disabled, and therefore all certificate types are available through the self-enrollment forms.

Prior to customization, a MRAO can also view the client certificate type customization as imposed by the RAO administrator of an organization and can modify the same.

You can use the **Customize Client Certificate Types** dialog to restrict the client certificate types and their validity periods as follows:

- Select **Customized**.
- Select the names of the certificates you wish to be available for the organization. Leave the others disabled.

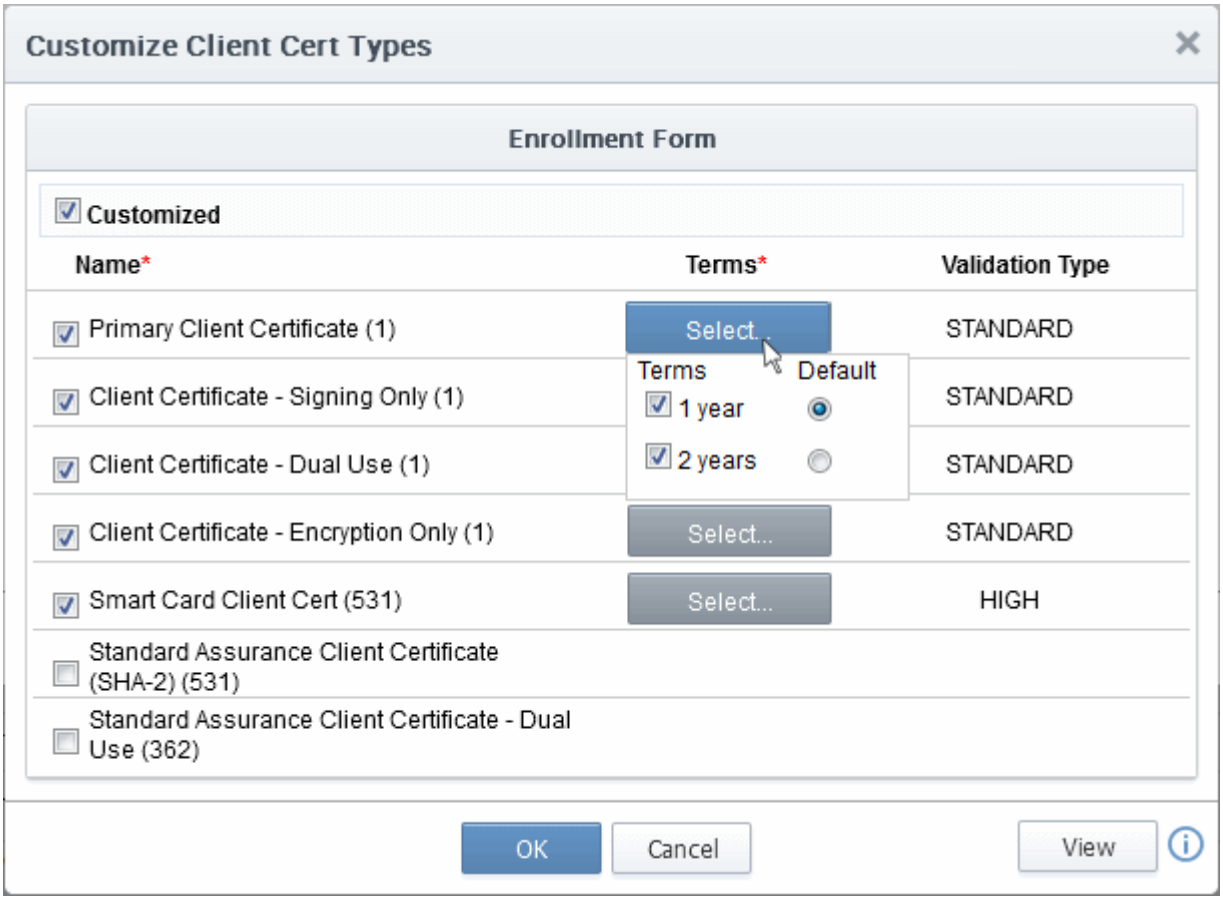
- Click **Select** located next to the certificate name to choose the available validity periods. If you want to set the selected validity period (term) as default for that certificate type, select **Default**, as shown in the following illustration.
- Review the **Validation Type** column value for the selected certificate. The validation types for each client certificate type are configured by the MRAO via **Settings > Certificates > Client Certificate Types** and apply to all organizations. The types cannot be changed per organization. The standard validation type can be issued quickly, taking advantage of the SCM's user authentication mechanisms.

  Under the Standard Personal Validation type, the end-user is authenticated using the following criteria:

  - The end-user must apply for a certificate from an email address at a domain that has been delegated to the issuing organization.
  - The organization has been independently validated by an web-trust accredited CA as the owner of that domain.
  - The end-user must know either a unique access code or secret ID that should be entered at the certificate enrollment form. These will have been communicated by you to the end-user via out-of-band communication.
  - The end-user must be able to receive an automated confirmation email sent to the email address of the certificate for which they are applying. The email contains a validation code that the end-user needs to enter at the certificate-collection web page.

  The High Personal Validation type requires that the end-user to undergo the preceding validation steps and have a face-to-face meeting with the issuing organization.

  Additional validation steps must be completed prior to you selecting **High Personal Validation** type.



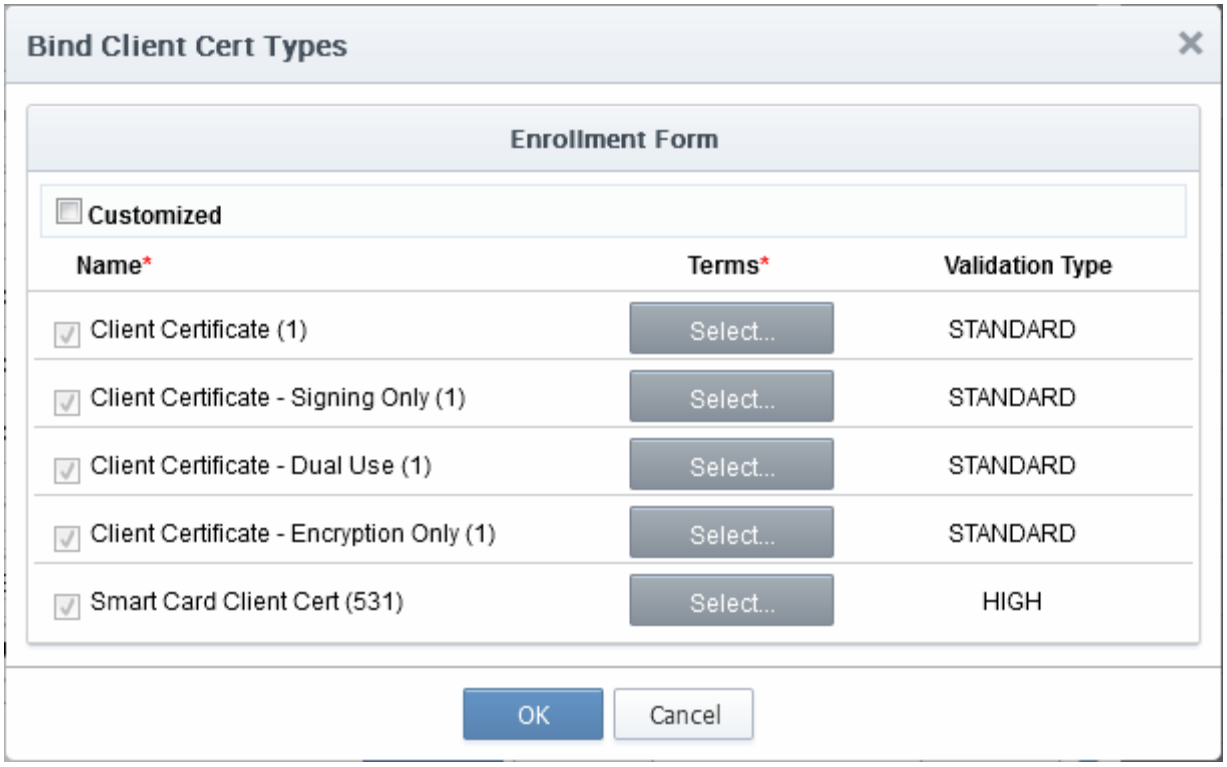
For the changes to take effect, you need to log out and then log back in.

Only the types and terms of client certificates that are selected in the **Bind Client Certificate Types** dialog are available in the **Type** field of the self-enrollment form.

7.2.3.3.2 Viewing Preimposed Client Certificate Type Customization for an Organization

While editing an existing organization, a MRAO can view the client certificate type customization imposed by the RAO of that organization, before imposing their own customization, by clicking **View** in the **Bind Client Certificate Types** dialog shown in the following illustration.

NOTE: **View** is activated when **Customized** is not selected in the **Customize Client Certificate Types** dialog.



The **Bind Client Certificate Types** dialog shown in the preceding illustration also allows MRAOs to modify the customization of the client certificate type availability for the organization by the RAO, and all selections made in this dialog apply only to that specific organization.

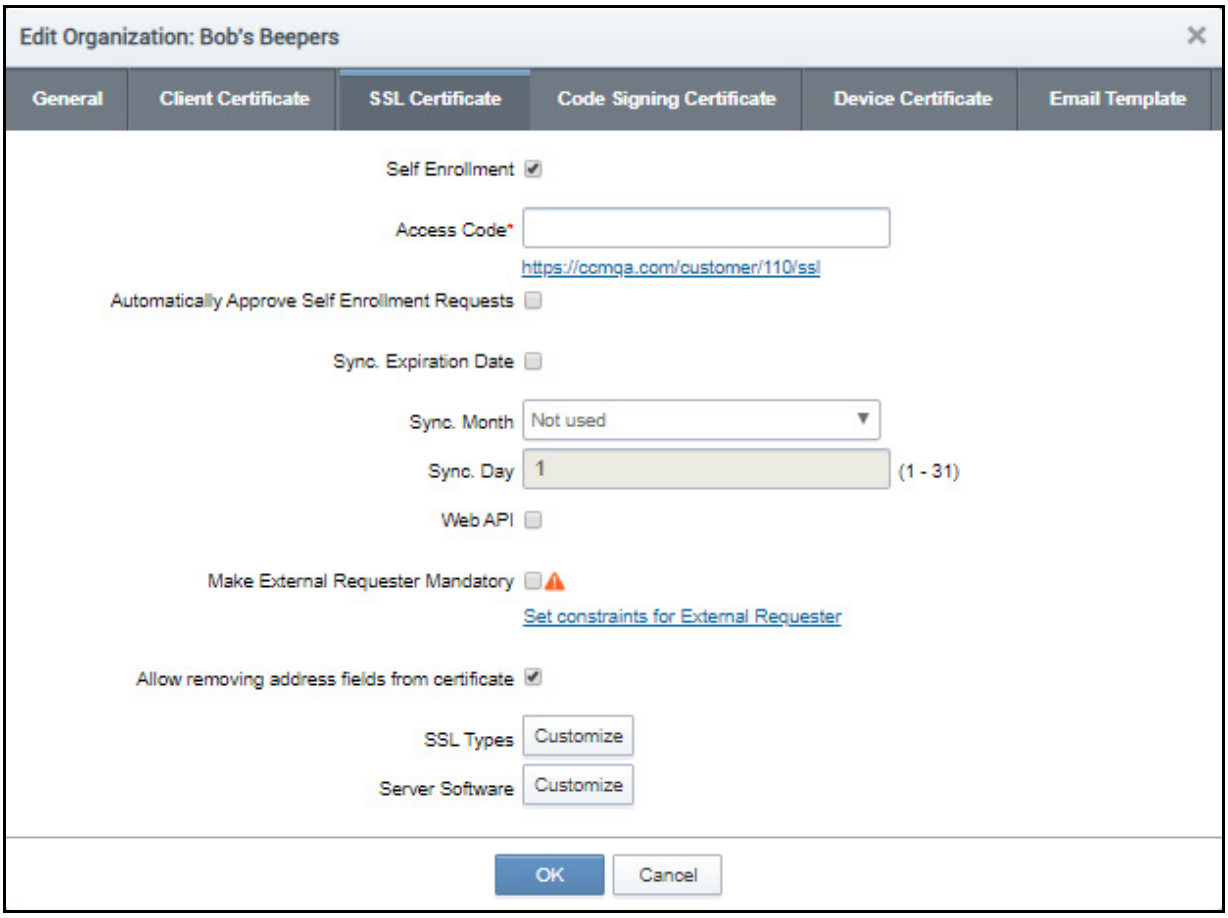
NOTE: The **Client Certificate Types** dialog contains a very similar interface and allows MRAOs to determine universal certificate types and validity periods that apply to all organizations.

7.2.3.4 Using the SSL Certificate Area of the Add New Organization Dialog

The **SSL Certificate** area shown in the following illustration allows MRAO administrators to do the following with regards to the certificates issued to the domain associated with the currently selected organization:

- Enable or disable certificate self-enrollment for the organization. This determines whether or not users can apply for certificates using the external application forms.

  Disabling **Self Enrollment** automatically disables **Self Enrollment via SAML** if it was enabled. If **Self Enrollment** is re-enabled, a new token is generated automatically and any URL redirects created with the previous token will break.
- Determine certificate types and term lengths that are available to the organization.
- Define the Web API capabilities and expiry synchronization settings relating to SSL certificates issued to the organization's domains.
- Specify the types of server software that are permitted for the organization.


Edit Organization: Bob's Beepers
General
Client Certificate
SSL Certificate
Code Signing Certificate
Device Certificate
Email Template
Self Enrollment
Access Code*
https://ccmqa.com/customer/110/ssl
Automatically Approve Self Enrollment Requests
Sync. Expiration Date
Sync. Month
Not used
Sync. Day
1
(1 - 31)
Web API
Make External Requester Mandatory
Set constraints for External Requester
Allow removing address fields from certificate
SSL Types
Customize
Server Software
Customize
OK
Cancel

The following table lists the settings and elements of the **SSL Certificate** area, where mandatory fields are marked with the red asterisk.

Field	Description
Self Enrollment	Enables external requests for SSL certificates to be made using the self-enrollment form hosted (by default) at `https://SCM/customer/<customer_uri>/smime`. Certificates requested using the self-enrollment form appear in **Certificates > SSL Certificates** before they are submitted to Sectigo for validation. MRAOs must review and approve or decline the request. Approved requests are forwarded to Sectigo for processing and if the application is made for a domain that has been prevalidated for your account, then the certificate is issued immediately; if the application is made for a new domain, then Sectigo first needs to validate your company's ownership of that domain prior to issuing the certificate. After successful validation, the new domain is added to your list of prevalidated domains so future certificates can be processed immediately. To successfully complete the request, the applicant must provide the correct access code for the organization. You should provide this code to the applicant using any out-of-bands methods (like email). Certificates can be requested by individuals that do not exist in SCM if they provide the correct access code and the email address entered on the form is from the same domain as the organization's CN. In such circumstances, a new end-user is automatically created with the end-user name `requesterSSL <domain.com>`, where domain.com is the domain name for which the application is being made. This end-user is automatically assigned membership of the organization for which the SSL certificate was ordered. The end-user is not issued a client certificate.
Access Code	Identifies an organization or department and is used to authenticate certificate requests that are made using the self-enrollment form. Organizations and departments are uniquely identified by a combination of their access code and the common name (domain) specified in the General properties area. Multiple organizations or departments can have the same access code or the same common name, but no single entity can share both. You should choose a complex alphanumeric access code. This code should be conveyed to the applicant along with the URL of the self-enrollment form. Applicants that request a certificate using the self-enrollment form need to enter this code. This field is only visible if **Self Enrollment** is selected.

Field	Description
Self Enrollment via SAML	Enables the use of Single Sign On (SSO) with Security Assertion Markup Language (SAML). SAML allows Sectigo to recognize users based on the SSO credentials/details from their organization's Identity Provider (IdP). When **Self Enrollment via SAML** is enabled, authorized end-users are automatically recognized through their IdP and are granted immediate access to the self-enrollment forms instead of having to use an access code. When **Self Enrollment via SAML** is enabled, the **Access Code** field remains mandatory for **Self Enrollment**. Because this code is mandatory, self-enrollment is possible through use of the access code. This can be helpful if a user's identity cannot be validated through their IdP for any reason (such as not being connected to their company's network). For more information on **Self Enrollment via SAML** prerequisites, please speak to your Sectigo account manager. This field appears only if **Self Enrollment** is selected.
Token	When **Self Enrollment via SAML** is enabled, an identifier for the **Token** field is randomly generated. This unique token is automatically inserted into the self-enrollment link and notifies Sectigo that the end-user is from your organization. To generate a different token, click **Generate**. This field can only be randomly generated. It is erased every time **Self Enrollment** or **Self Enrollment via SAML** are deactivated. This field appears only if **Self Enrollment via SAML** is selected.
Automatically Approve Self Enrollment Requests	When **Automatically Approve Self Enrollment Requests** is enabled, SSL certificate requests submitted through the self-enrollment form are automatically approved. Departments do not inherit the **Automatically Approve Self Enrollment Requests** setting from their parent organization. As EV certificates require additional approval, this setting is not applied.

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td rowspan="3">Sync. Expiration Date</td><td colspan="2">Provides means to modify and synchronize the expiration month and day of all certificates issued to the organization.
When Sync. Expiration Date is enabled, the following settings can be used:</td></tr>
<tr><td>Sync. Month</td><td>Identifies a specific month of the year during which all certificates issued to the domain are to expire.</td></tr>
<tr><td>Sync. Day</td><td>Identifies a specific day of the month on which certificates issued to the domain are to expire.
Specifying a certain day of the month for all SSL certificates issued to an organization can greatly simplify the certificate management process, especially in enterprises with large volumes of certificates.
The valid value is between 1 and 31 if no specific month is selected. When a month is specified, the valid value reflects the number of days in that month (1-31, 1-30, 1-28).
Certificate validity periods cannot exceed the duration selected on the SSL certificate application form. That is, if a specific month is also selected in the Sync. Month field, then the certificate expires on the occurrence of that precise date that is closest to the certificate term of that precise date that is closest to the certificate term selected on the SSL certificates self-enrollment form or built-in application form. If a specific month is not selected in the Sync. Month field, then the certificate is to expire on the numbered day of the month that is nearest to the certificate term selected on the SSL certificate's self-enrollment form or built-in application form.
For example, a 2-year certificate issued on August 12, 2014 is supposed to expire on August 12, 2016 (730 days later). However, if you specified 16 as the Sync. Day, the certificate expires on July 16, 2016 (704 days later). If you specified 16 as the Sync. Day and August as the Sync. Month, the certificate expires on August 16, 2015 (338 days later).
Specifying a Sync. Day only affects certificates issued from that point forward. The expiry date of certificates that have already been issued does not change. Their Sync. Expiration Date applies to all renewals of existing certificates.</td></tr>
<tr><td>Web API</td><td colspan="2">Allows applicants to enroll for certificates through the Web Service API. This requires a special agreement with Sectigo.</td></tr>
<tr><td>Make External Requester Mandatory</td><td colspan="2">When enabled, External Requester becomes mandatory for all SSL certificate enrollment forms and makes SSL certificate enrollment via MS Agent (CA Proxy) impossible.</td></tr>
</table>

Field	Description
Allow removing address fields from certificate	If selected, the option to hide an organization's address details is available when requesting the certificate.
Secret Key	Specifies a phrase that is unique for all organizations. This phrase restricts access for enrolling certificates for that organization. User in pair with **Organization ID**, which is visible only for existing organizations. This field appears only if **Web API** is selected.
SSL Types	Allows you to specify the certificate types and validity period that are available for this organization. Clicking **Customize** opens the **Bind SSL Types** dialog. All choices made via this dialog apply only to this specific organization. You can make different certificate types and terms available to the applicant depending on whether the application is made using the built-in application form or the self-enrollment form. The **SSL Types** area contains a similar interface that allows MRAOs to determine universal certificate settings that apply to all organizations. If a certificate type or validity period is not visible in the **Bind SSL Types** dialog, then it may need to be enabled in the **SSL Types** area.
Server Software	Allows you to specify types of server software that are permitted for this organization. The server software selected in this field is available in the server software list of both the built-in application form and self-enrollment form.

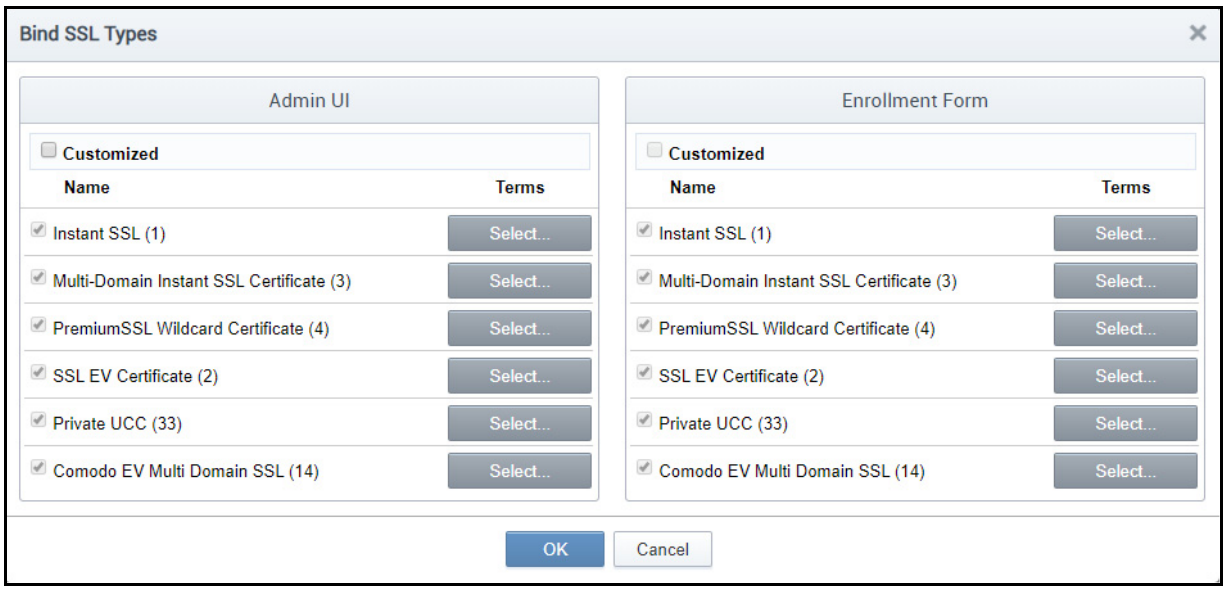
7.2.3.4.1 Customizing SSL Certificate Types for an Organization

The level of SSL certificate type customization depends on your security role, as follows:

- A MRAO can customize SSL certificate type availability for all organizations and departments.
- A RAO SSL can customize SSL certificate type availability only for organizations and their departments that are delegated to this administrator.
- A DRAO cannot customize SSL certificate type availability.

The types and validity period of SSL certificates that are available to any particular organization can be customized using the **Bind SSL Types** dialog shown in the following illustration. Creating a targeted certificate roster simplifies the certificate selection procedure at the application forms and helps avoid applications for certificates which are inappropriate for an organization.

To perform the customization, click **Customize** located beside the **SSL Types** field in the **SSL Certificate** area of the **Add New Organization** dialog to open the **Bind SSL Types** dialog for that organization, as shown in the following illustration.



Each SSL Type has a unique SSL ID assigned to it. These IDs are required for certain REST operations and are indicated in brackets beside each SSL Type.

The **Admin UI** panel determines SSL certificate types to be made available to applicants using the built-in application form for that organization.

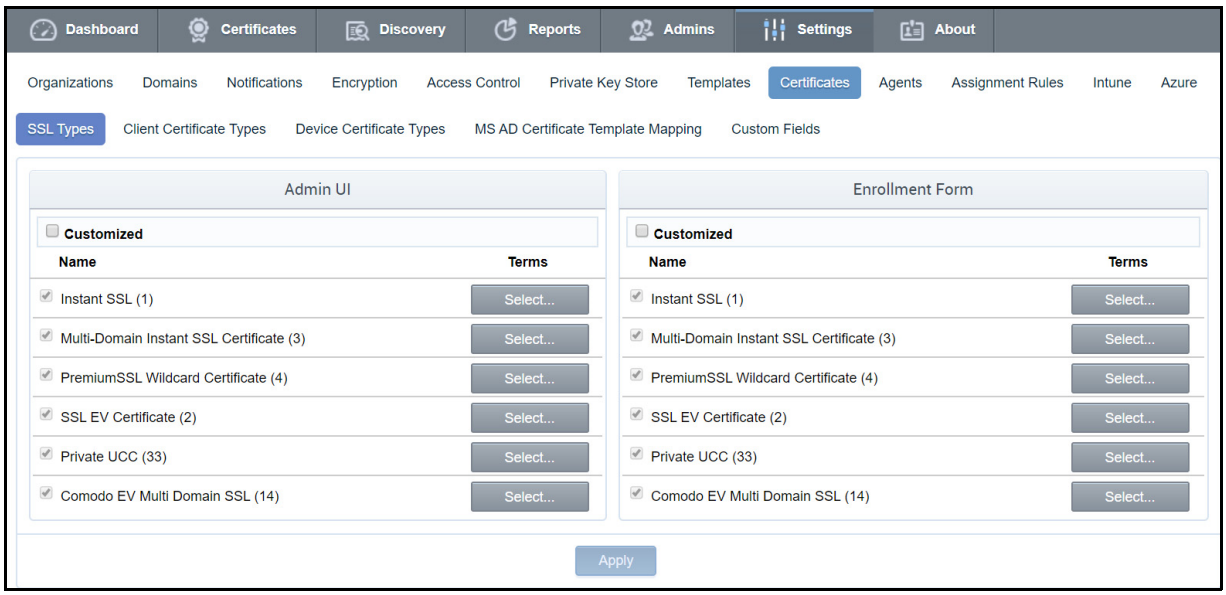
The **Enrollment Form** panel determines SSL certificate types to be made available to applicants using the self-enrollment form for that organization.

The **Customized** option shown in the following illustration is disabled by default, therefore making all certificate types available through both types of application form.

7.2.3.4.2 Restricting the SSL Types and Their Validity Periods

You can restrict the SSL types and their validity periods (terms) as follows:

- Select **Customized** in either the **Admin UI** or **Enrollment Form** panel.
- Select the names of the certificates to be available to the organization.
- Click **Select** next to the certificate name to indicate which validity periods are to be available.



For the changes to take effect, you need to log out and then log back in again.

Only the types and terms of SSL certificates that are selected in the **Bind SSL Types** dialog are available in the **Type** and **Term** fields of the organization's application forms and only apply to that organization.

The **SSL Types** dialog contains a very similar interface and allows MRAOs to determine universal certificate types and validity periods that apply to all organizations.

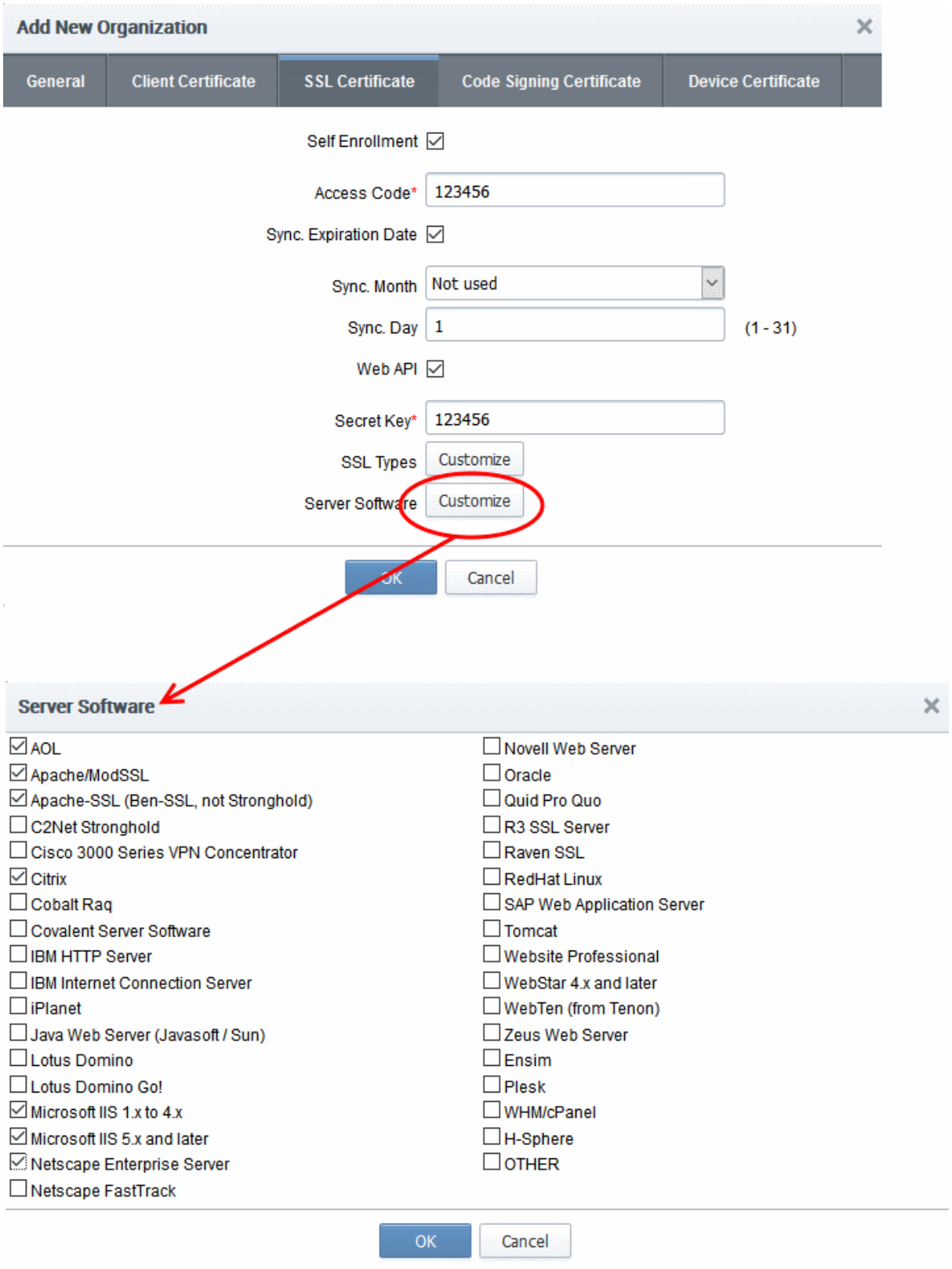
7.2.3.4.3 Customizing Server Software Types for an Organization

The level of the server software type customization depends on your security role, as follows:

- A MRAO can customize server software types that can be used for all organizations and departments.
- A RAO SSL can customize server software types that can be used for only for organizations and departments that are delegated to them.
- A DRAO cannot customize server software types.

The types of server software that can be used for an organization can be customized using the **Server Software** dialog. Only allowed server software is listed in the Server Software list in both the self-enrollment form and built-in application form for that organization.

To perform the customization, click **Customize** located beside the **Server Software** field in the **SSL Certificate** area of the **Add New Organization** dialog to open the **Server Software** dialog for that organization, as shown in the following illustration.



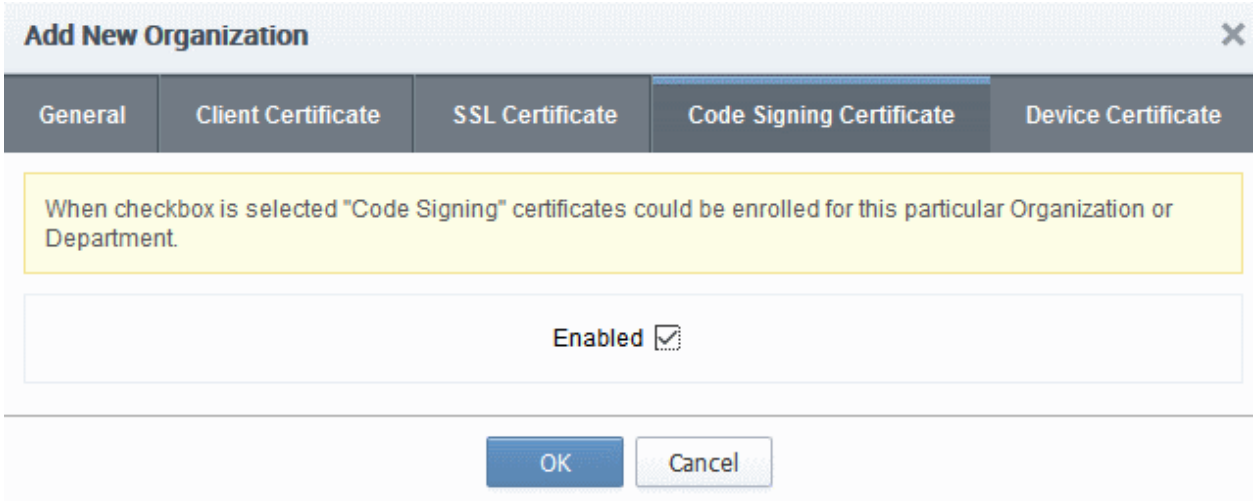
By default, no server software is selected.

To restrict the server software types, select only the names of the server software you wish to allow for the organization.

For the changes to take effect, you need to log out and then log back in.

7.2.3.5 Using the Code Signing Certificate Area of the Add New Organization Dialog

The **Code Signing Certificate** area shown in the following illustration allows appropriately privileged administrators to enable request and issuance of code signing certificates for the organization. The settings specified in this area relate only to those client certificates issued to the domain associated with the currently selected organization.



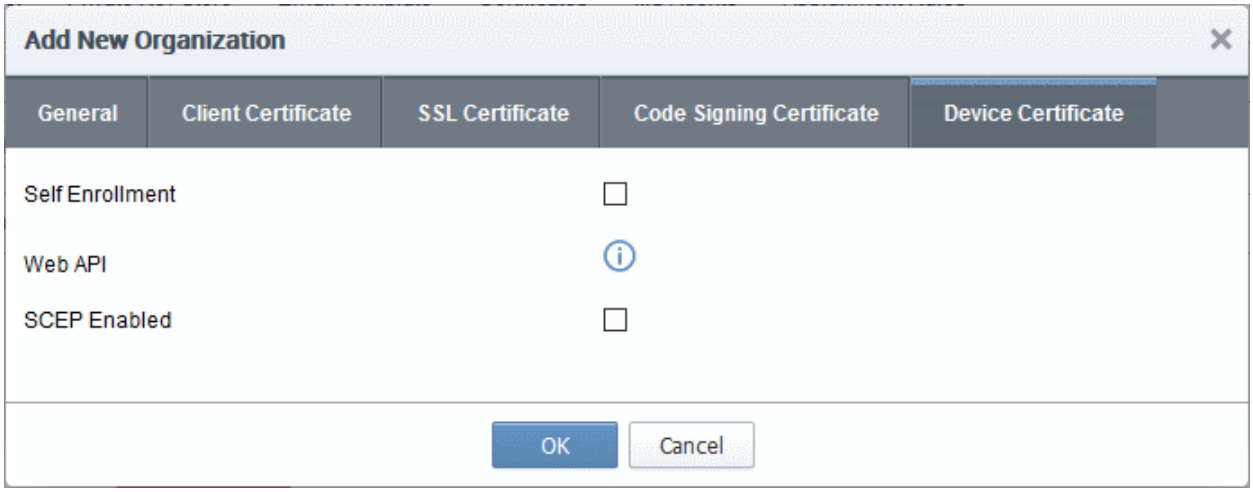
The following table lists settings and elements of the **Code Signing Certificate** area.

Field	Description
Enabled	Enables the request and issuance of code signing certificates to end-users that are members of this organization.

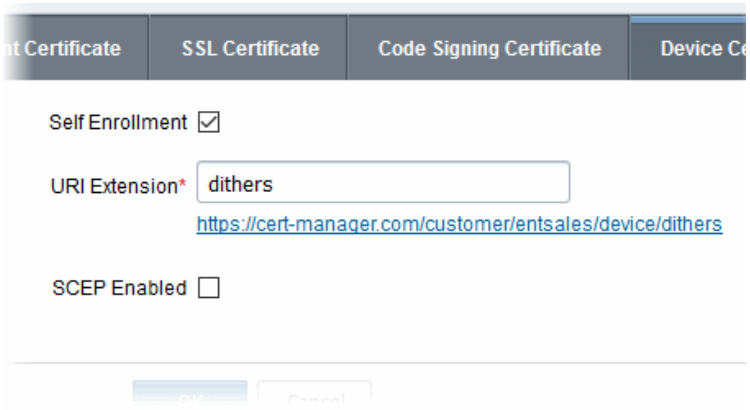
7.2.3.6 Using the Device Certificate Area of the Add New Organization Dialog

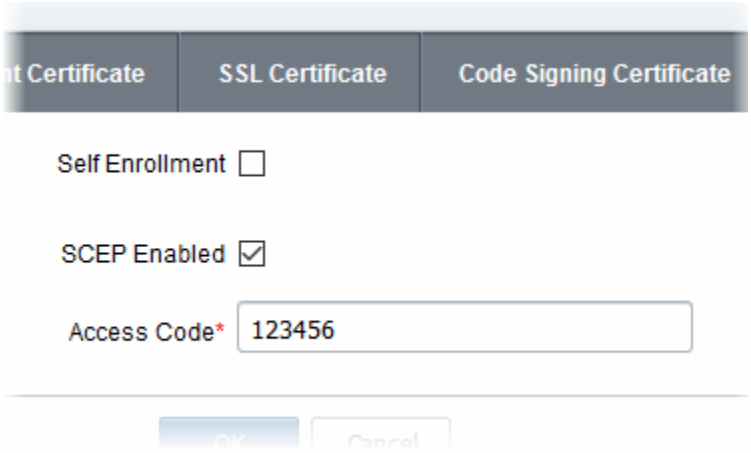
The **Device Certificate** area shown in the following illustration allows appropriately privileged administrators to do the following with regards to the certificates issued to the devices associated with the currently selected organization:

- Enable or disable certificate self-enrollment for device certificates in the organization. This determines whether users can apply for device certificates using the external application forms.
- Define the Web API capabilities and expiry synchronization settings relating to device certificates issued to the organization's devices.
- Enable or disable enrollment of device certificates via SCEP.



The following table lists settings and elements of the **Device Certificate** area.

Field	Description
Self Enrollment	Allows end-users to request device certificates by completing the self-enrollment form. You can specify a URL extension if one is not already set. The URL of the form is automatically shown below the **URL Extension** field. This URL should be passed to applicants so they can apply for device certificates. 

Field	Description
SCEP Enabled	Enables enrollment of device certificates via SCEP for an organization. You need to specify an access code after enabling this option. The code should be included in the configuration profile for OTA enrollment of device certificates. The code is to be included in the profile, as the challengePassword parameter in the certificate request generated by the device. 

7.2.3.7 Using the Bulk Import Functionality for Organizations and Departments

Organizations and departments can be imported into SCM in bulk by MRAO administrators. To do this, the following software is required:

- **Linux OS** with **GNU bash**, version 4.4.12 or later.
- **curl** application.
- **jq** program available at https://stedolan.github.io.jq/ .
- **import-org.sh** script, which you can obtain by contacting your Sectigo account manager. It is recommended that you store this script in a separate folder on your Linux-powered computer.

  The **Allow Key Recovery by Master Administrators** and **Allow Key Recovery by Organization Administrators** options cannot be enabled for the organizations and departments imported into SCM. If you want this functionality, you must manually create the organizations and departments in SCM.

7.2.3.7.1 Preparing the File for Bulk Import

The data on the organizations and departments to be imported must be arranged in a separate file. This file must satisfy the following conditions:

- It must be a text file in UTF-8 encoding.
- It must contain JSON objects representing the organizations or departments to be imported.
- Each JSON object must start on a new line.
- The JSON objects for organizations must precede the JSON objects for departments.

The following table provides an overview of the JSON object parameters and the constraints attached to them.

Key	Type	Description	Constraints
`parentOrgName`	Applicable to and mandatory for departments only	Identifies the name of the organization to which the department belongs.	Must not exceed 64 characters. Must precisely correspond to the name of an organization that already exists in SCM or that is to be imported by one of the preceding JSON objects in this file.
`name`	Mandatory	If the JSON object contains "`parentOrgName`", this parameter identifies the name of a department (its value populates the **Department Name** field in the profile of this department). If the JSON object does not contain "`parentOrgName`", this parameter identifies the name of an organization (its value populates the **Organization Name** field in the profile of this organization).	Must not exceed 64 characters. Must be unique across the file and SCM customer account when it represents the organization name. Department names do not need to be unique.
`address1`	Mandatory	The value of this parameter populates the **Address1** field in the profile of this organization or department.	Must not exceed 128 characters.
`address2`	Optional	The value of this parameter populates the **Address2** field in the profile of this organization or department.	Must not exceed 128 characters.
`address3`	Optional	The value of this parameter populates the **Address3** field in the profile of this organization or department.	Must not exceed 128 characters.

Key	Type	Description	Constraints
`city`	Mandatory	The value of this parameter populates the **City** field in the profile of this organization or department	Must not exceed 32 characters.
`stateProvince`	Mandatory	The value of this parameter populates the **State / Province** field in the profile of this organization or department	Must not exceed 32 characters.
`postalCode`	Mandatory	The value of this parameter populates the **Postal Code** field in the profile of this organization or department.	Must not exceed 10 characters.
`country`	Mandatory	The value of this parameter populates the **Country** drop-down in the profile of this organization or department.	Must contain 2 characters and represent the country code defined in the ISO 3166 standard. If you do not know your country code, see https://www.iso.org/obp/ui/#search.

JSON objects are comprised of key-value pairs. If any parameter is duplicated, the most recent key-value pair is processed. For example, if "`name`": "`Sectigo`" appears three times in one JSON object, only the third occurrence is processed.

The following table provides and example of JSON objects for an organization and a department.

	JSON Object

Organization	`{`
	`"name":"<organization name>",`
	`"address1":"<organization address, part 1>",`
	`"address2":"<organization address, part 2>",`
	`"address3":"<organization address, part 3>",`
	`"city":"<city name>",`
	`"stateProvince":"<state / province name>",`
	`"postalCode":"<postal code>",`
	`"country":"<country code, for example, US>"`
	`}`

	JSON Object

Department	{
	"parentOrgName": "*<organization name>*",
	"name":"*<department Name>*",
	"address1":"*<department address, part 1>*",
	"address2":"*<department address, part 2>*",
	"address3":"*<department address, part 3>*",
	"city":"*<city name>*",
	"stateProvince":"*<state / province name>*",
	"postalCode":"*<postal code>*",
	"country":"*<country code, for example, DE>*"
	}

7.2.3.7.2 Importing JSON Files Into SCM

You can validate and import your JSON file as follows:

1. In the console, run `jq'.'`*<CUSTOMER_JSON_FILE_NAME>*.
2. Correct any errors that are returned.
3. Run the following command to initiate the API calls to SCM:

   `$./import-org.sh --datafile=`*<CUSTOMER_JSON_FILE_NAME>* `--username=`*<MRAOADMIN>*

   `--passwd=`*<CUSTOMER_PASSWORD>* `--uri=`*<SCM_CUSTORMER_URL_EXTENSION>*

   `--scmurl=https://cert-manager.com/api/organization/v1`

   or

   `https://hard.cert-manager.com/api/organization/v1`

   If your JSON file is not located in the same location as the `import-org.sh` script, specify the full path to the JSON file.

   Command example:

   ```
   ./import-org.sh --datafile=organizations.json --username=mraoadmin --
   passwd=7ygvcft6 --uri=customer --scmurl=https://cert-manager.com/api/
   organization/v1
   ```

   Each JSON object in your file forms a separate API request to SCM.
4. Navigate to the folder with the `import-org.sh` script to see if all API calls to SCM have been successful. The API call outcomes are explained in the following table.

Outcome	Description
API call failed	If any rejected files have been created in this folder, it means that one or more API call to SCM has failed. This rejected file contains all the JSON objects in which errors have been detected. The `logs` folder contains the following files: • The `process.log` file with the records of all successful API calls. • The `errors.log` file with the records of all failed API calls and what errors occurred for each.

Outcome	Description
API call successful	If there is no rejected file in this folder, it means that all API calls to SCM have been successful. The `logs` folder contains only the `process.log` file with the records of all successful API calls.

5. If there is a rejected file, do the following:
   a. Check the records in the `errors.log` file to find out what errors occurred.
   b. Correct the data in the rejected file (if needed) and rename it. The following table provides descriptions for the most frequent error codes.

      If the rejected file is not renamed, any errors in subsequent API calls are added to that file. This can cause confusion, as some errors in the file may no longer be accurate.

Error Code	Description
-14	Parent organization "<organization name>" not found.
-14	Country code "<specified country code>" is invalid.
-803	"<Org>" with such name already exists.
-1001	Following errors detected: Value of "parentOrgName" size must be between 0 and 64.
-1001	Following errors detected: Value of "name" size must be between 0 and 64.
-1001	Following errors detected: Value of "address1" size must be between 0 and 128.
-1001	Following errors detected: Value of "address2" size must be between 0 and 128.
-1001	Following errors detected: Value of "address3" size must be between 0 and 128.
-1001	Following errors detected: Value of "city" size must be between 0 and 32.
-1001	Following errors detected: Value of "stateProvince" size must be between 0 and 32.
-1001	Following errors detected: Value of "postalCode" size must be between 0 and 64.
-1001	Following errors detected: Value of "country" size must be between 2 and 2.
-1001	Following errors detected: Value of "name" may not be empty.
-37	Access denied.

The following is an example of a record related to a JSON object in the `errors.log` file:

```
2019.04.15.18:56:34   Error creating organization:
{"name":"org3","address1":"adr1,
st55","city":"NewShine","stateProvince":"ODS","postalCode":"34562","countr
y":"fjd"}.
```

```
2019.04.15.18:56:34   STATUSCODE: 400
2019.04.15.18:56:34   HTTP/1.1 400 Bad Request
Server: Apache-Coyote/1.1
Set-Cookie: CCMSESSIONID=EC5CAF72391EBD8D0D2A0F8A71DA4F1A; Path=/; Secure;
HttpOnly
Content-Type: application/json;charset=UTF-8
Content-Length: 107
Date: Mon, 15 Apr 2019 15:56:34 GMT
Connection: close
{"code":-1001,"description":"Following errors detected: Value of 'country'
size must be between 2 and 2. "}400
2019.04.15.18:56:34   Copy to rejected.
```

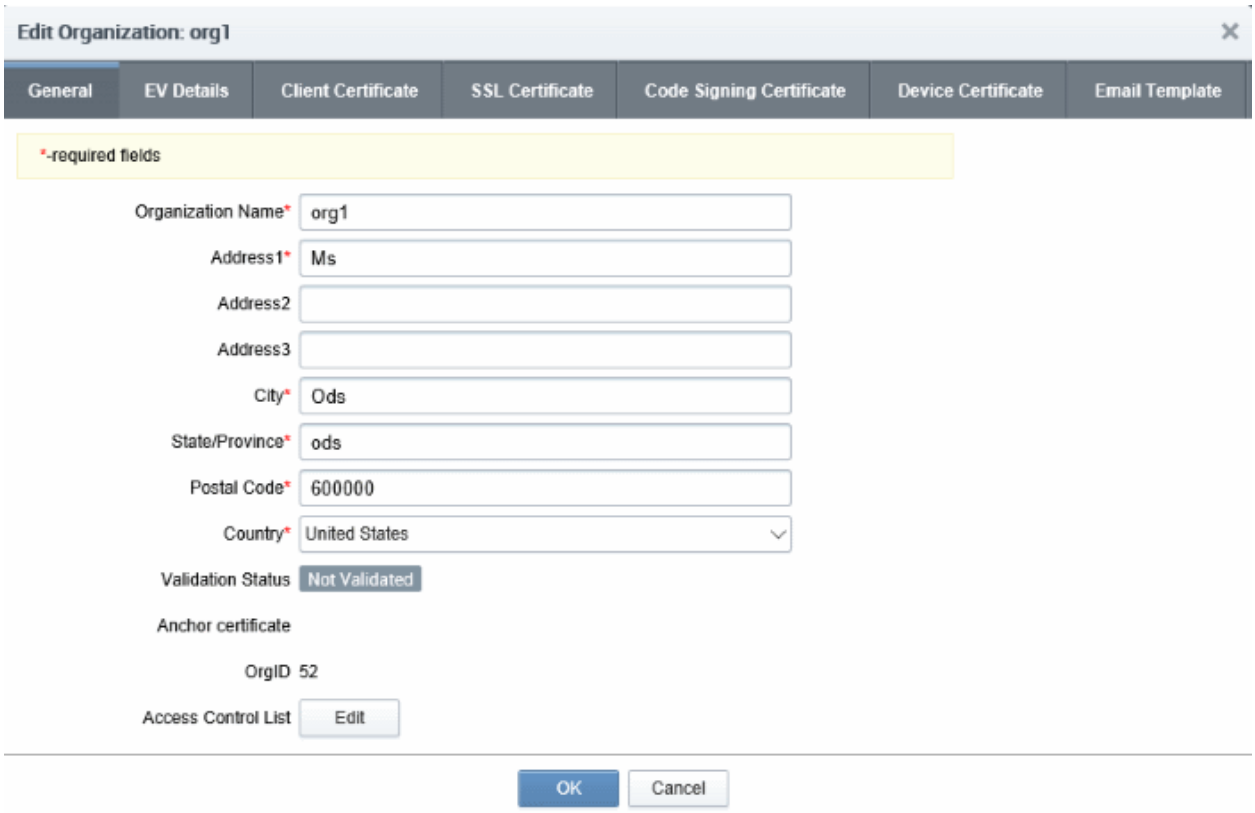
c. Initiate another API call to SCM as described in step 4 using the renamed file (formerly the rejected file).

d. Check if all these API calls have been successful as described in step 5.

Once all steps are completed, you can proceed with the configuration of organization and department settings as required.

7.2.4 How to Modify an Existing Organization

You edit an organization by navigating to **Settings > Organizations** in the main UI, and then clicking **Edit** to open the **Edit Organization** dialog shown in the following illustration.



Using the **Edit Organization** dialog shown in the preceding illustration, MRAOs and RAOs can view the **General**, **EV Details**, **Client Certificate**, **SSL Certificate**, and **Code Signing Certificate** areas pertaining to an existing organization at any time. In addition, MRAOs can modify information on all these areas, whereas RAOs can modify all of these areas except **General**.

The **Email Template** area allows you to directly edit the content of the automated notification emails as set per settings in the notifications area. See "Configuring Templates" on page 506 for more information.

7.2.4.1 Using the General Settings Area of the Edit Organization Dialog

The **General** settings area of the **Edit Organization** dialog shown in the preceding illustration is similar to the **Add New Organization** dialog described in "Using the General Settings Area of the Add New Organization Dialog" on page 332, with the addition of the **Access Control List** option which enables you to configure and limit incoming access to the SCM interface to certain IP addresses and ranges. That is, after specifying one or more IP addresses or ranges in CIDR notation, only administrators attempting to login from these specified addresses are permitted access.

NOTE: The **Access Control** area of the SCM UI available via **Settings > Access Control** contains a very similar interface and allows MRAOs to limit incoming access to the SCM UI. These settings override any settings made through the **Edit Organization** dialog. In addition, RAOs and DRAOs can restrict access only to IP ranges that fall within the range that the MRAO has set through the top-level **Access Control** area.

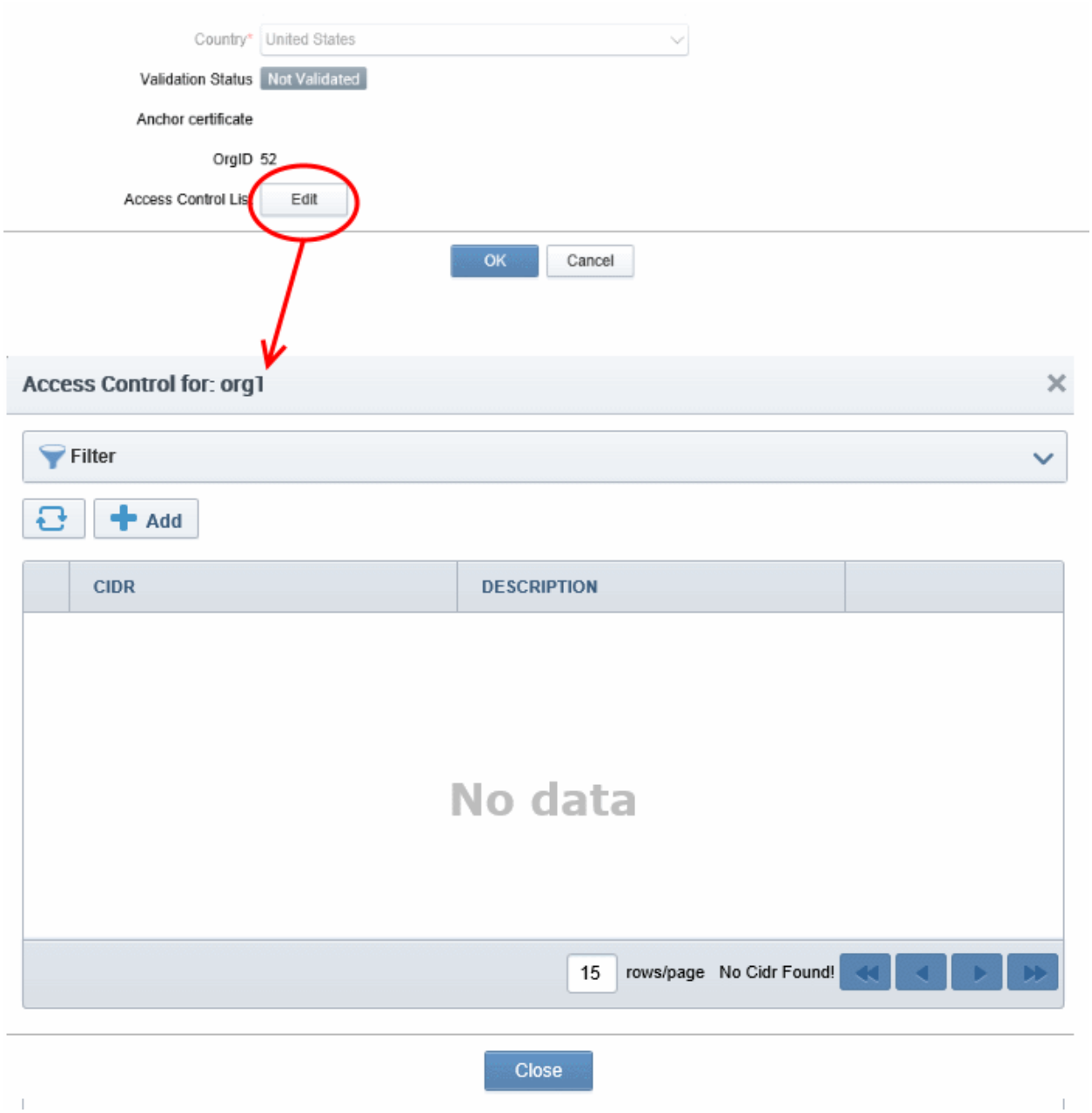
Any changes you make to the settings of an existing organization do not affect certificates that have already been issued to domains belonging to that organization.

7.2.4.1.1 Imposing Access Restrictions to the SCM UI

The level of the SCM UI access restrictions that you can impose depends on your security role, as follows:

- A MRAO-imposed restrictions apply to the management of the certificates, administrators, end-users, and settings for all the organizations and departments.
- A RAO-imposed restrictions apply to the management of the certificates, administrators, end-users, and settings for the organizations and their subordinate departments that have been delegated to this administrator.
- A DRAO-imposed restrictions apply to the management of the certificates, end-users, and settings for the departments that have been delegated to this administrator.

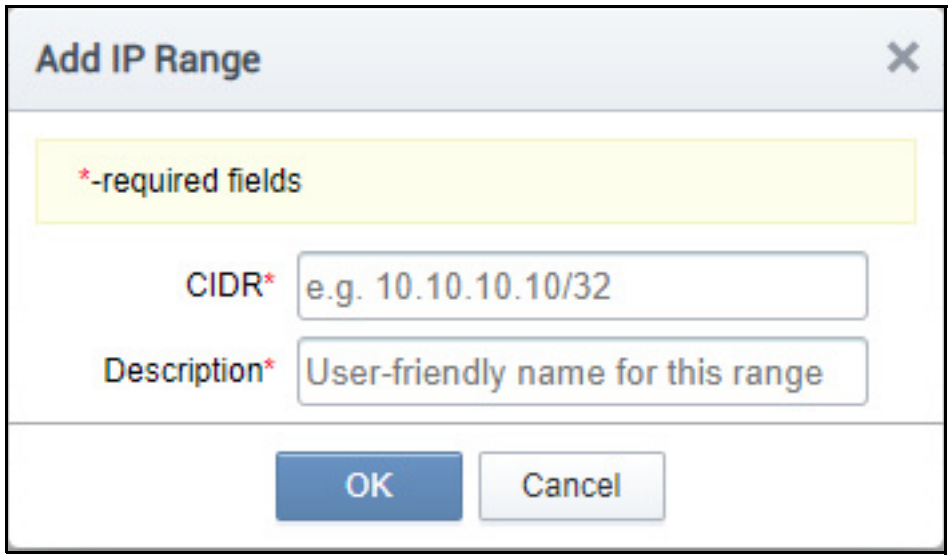
To limit incoming access to the SCM UI, click **Edit** located beside **Access Control List** field of the **Edit Organization** dialog. This opens the **Access Control** dialog, as shown in the following illustration.



Column / Control	Description
CIDR	Indicates Classless Internet Domain Routing (CIDR). You should specify the IP range that consists of the IP address followed by a network prefix, such as, for example 123.456.78.91/16 .
Description	Contains a short description for the IP range as entered by the you while creating the CIDR.
Edit	Enables you to edit CIDR details.

Column / Control	Description
Delete	Enables you to delete the CIDR.
Add	Opens the **Add IP Range** dialog.
Refresh	Updates the list of IP ranges.

To add a new IP range, click **Add** to open the **Add IP Range** dialog shown in the following illustration, enter the IP value followed by a network prefix (for example, 123.456.78.91/16), and then add a short description of the IP range.



Upon completion, the specified IP range is added as a new CIDR and the access to SCM from the new IP range is allowed.

7.2.4.1.2 Customizing Notification Email Templates

SCM can send automatic email notifications to certificate applicants, administrators, and end-users after such events as certificate approval, collection, and revocation. These notifications are created using email templates. Email templates specify what information should be included in each type of notification.

For more information on configuring email templates, see "Modifying Email Templates" on page 507.

7.2.4.2 Validating an Organization

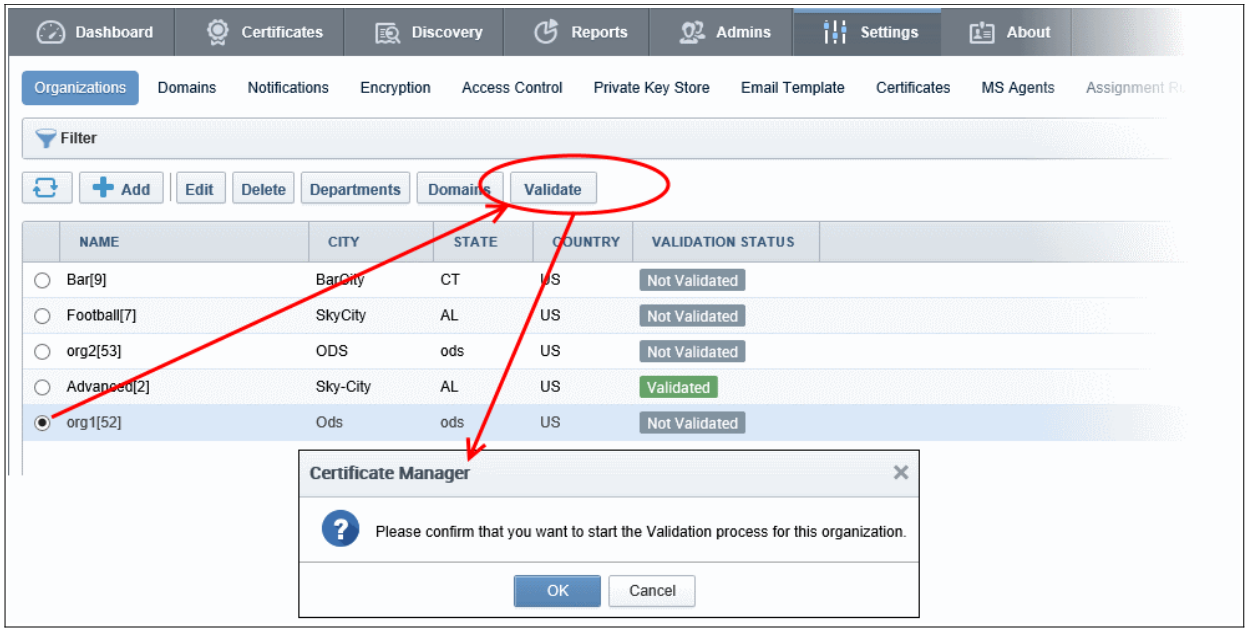
MRAOs can validate an organization by navigating to **Settings > Organizations** from the main UI, selecting an organization in the list, and clicking **Validate**, as shown in the following illustration.

Before you can issue OV SSL certificates for an organization or department, the organization must first be validated by Sectigo. The validation status of new organizations is initially Not Validated and the **Anchor Certificate** field is blank.

Upon a successful validation, the organization's validation status becomes Validated and the anchor certificate status changes to ON. The anchor certificate contains all verified information about the organization (address, contact details, and so on). The information in the anchor certificate is then used to accelerate the issuance of subsequent OV level certificates for the organization.

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

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



To view the validation status, navigate to **Settings > Organizations** from the main UI, select the organization, and click **Edit**. The **General** area displays the validation status.

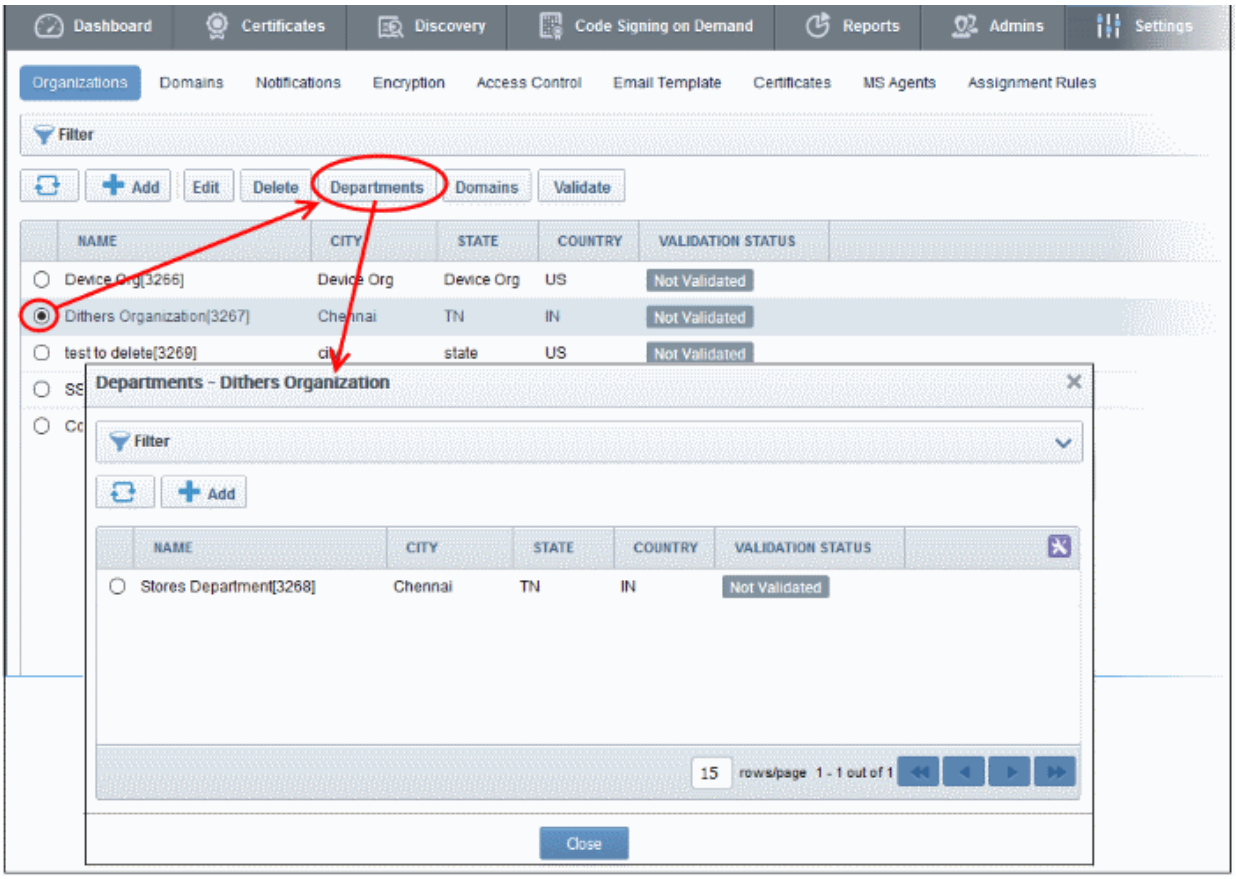
The following are various stages of the validation status:

- **Not Validated** indicates that the validation process has not been started.
- **Validated** indicates that the organization is validated and anchor certificate is issued. The organization and departments under it can request for OV SSL certificates.
- **Pending** indicates that the validation process has started but not completed. The address details of the organization in the **General** area are locked.

- **Failed** indicates that the validation process failed for the organization.
- **Expired** indicates that the validation period of 36 months has expired for the organization.

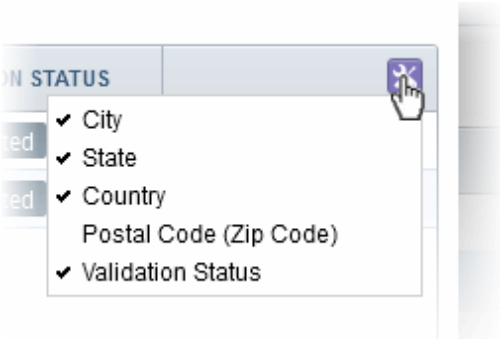
7.2.4.3 Managing Departments of an Organization

MRAO and RAO administrators can view and edit departments belonging to an organization by selecting this organization and clicking **Departments**. This opens a dialog that lists all departments belonging to the organization, as well as controls to edit, delete, add, and manage domains, as shown in the following illustration.



The following table lists settings and elements of the **Departments** dialog.

Column / Element	Description
Name	The department that have been delegated to the currently logged-in administrator.
City	The city entered at the time of creating the department.
State	The state entered at the time of creating the department.
Country	The country entered at the time of creating the department.
Postal Code (Zip Code)	The postal or zip code entered at the time of creating the department.

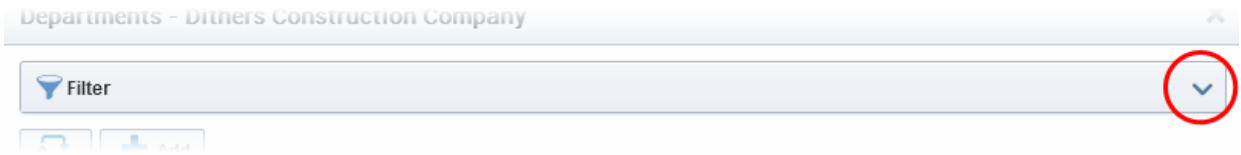
Column / Element		Description
Validation Status		Indicates whether or not the department is validated for the request and issuance of OV SSL certificates.
You can use the tool button to select columns to be displayed in the table: 		
Controls	Add	Adds General, Client Certificate, SSL Certificate, or Code Signing Certificate settings pertaining to an existing department.
	Refresh	Updates the list of departments.
Department Controls [a]	Edit	Modifies General, Client Certificate, SSL Certificate, Code Signing Certificate, and E-mail Template settings pertaining to an existing department.
	Delete [b]	Deletes the department.
	Domains	Allows to view, edit, and delegate domains of the departments.

a. The department controls appear only when a department is selected.
b. Not visible to DRAOs.

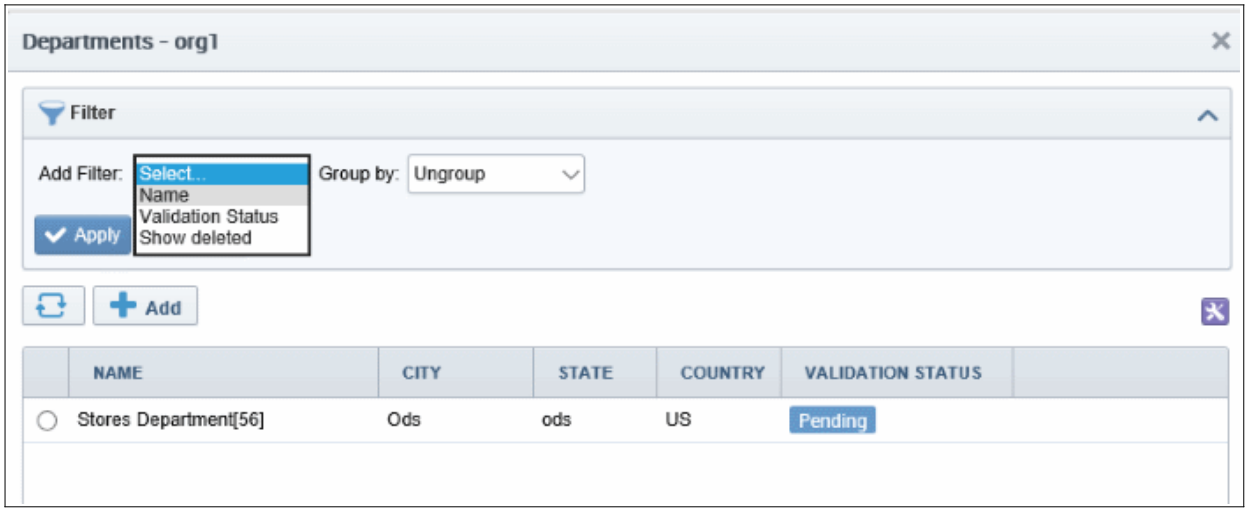
7.2.4.4 Sorting and Filtering Departments

You can sort items in the alphabetical order by clicking a column header, and you can use filters to search for particular department.

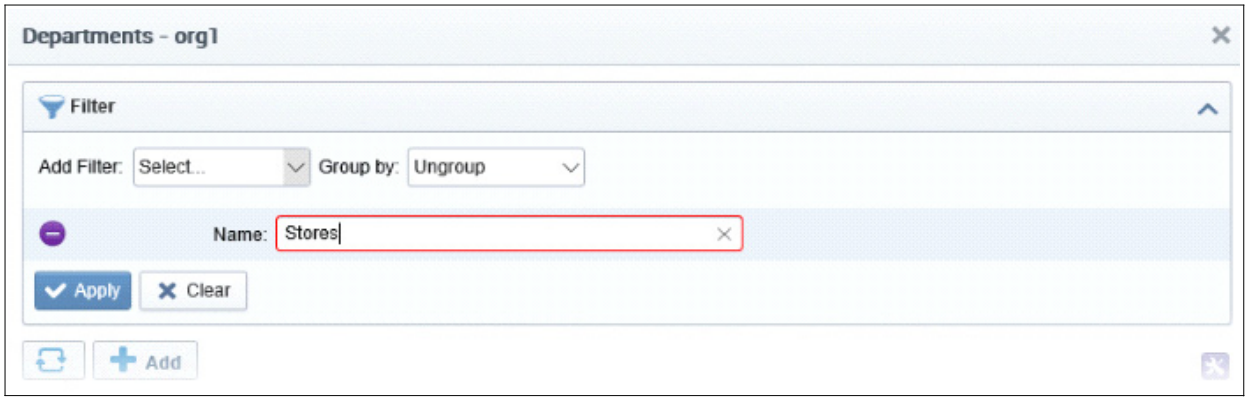
You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.



To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection from the **Add Filter** list.



Then you enter or select the filter parameter as per the selected criteria.



After you click **Apply**, filtered items based on the entered parameters are displayed:

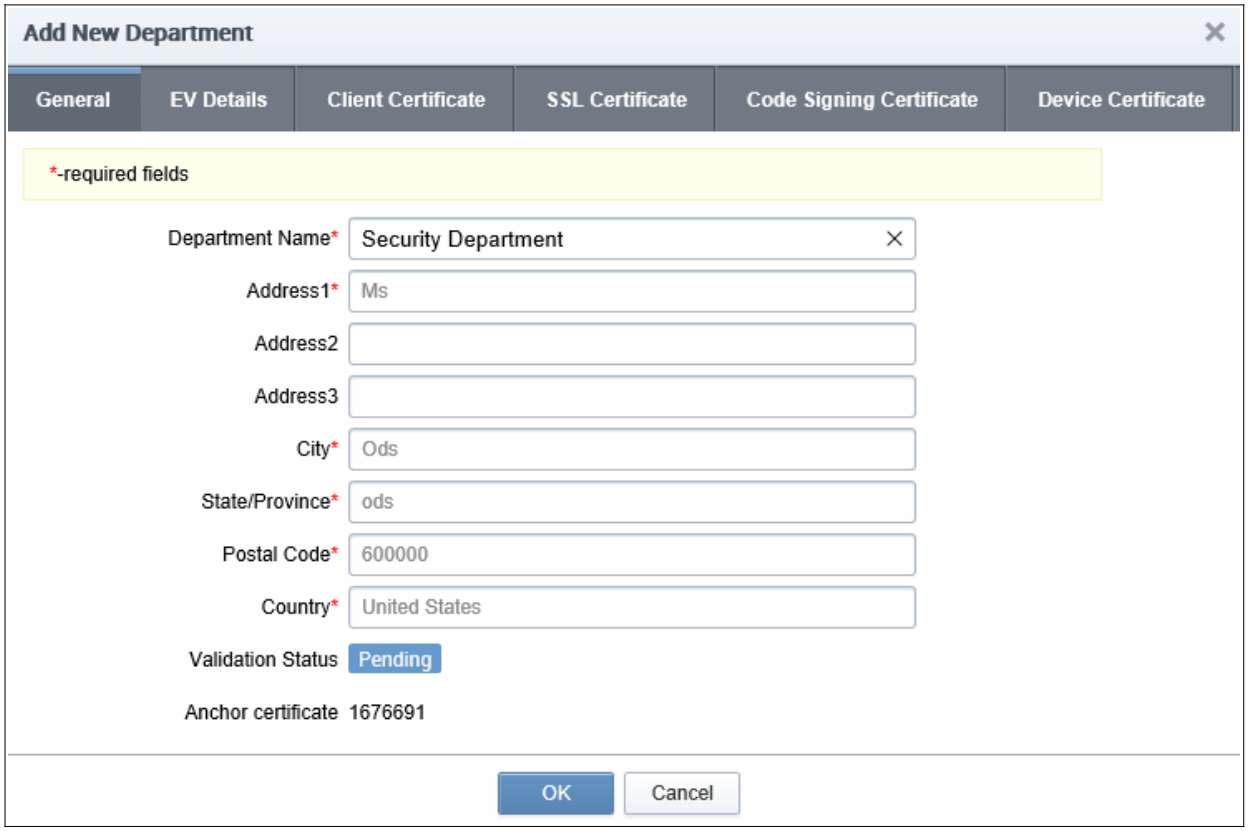
You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **Departments** screen, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

7.2.4.4.1 Creating New Departments

An organization can have departments managed by a DRAO administrator. A MRAO or RAO creates a department under an organization and assign domains to it. This allows you to provide certificates to end-users and websites of the department.

You create a new department by navigating to **Settings > Organizations**, selecting the organization under which you want to create a new department, then clicking **Departments**, and then clicking **Add** to open the **Add New Department** dialog shown in the following illustration.



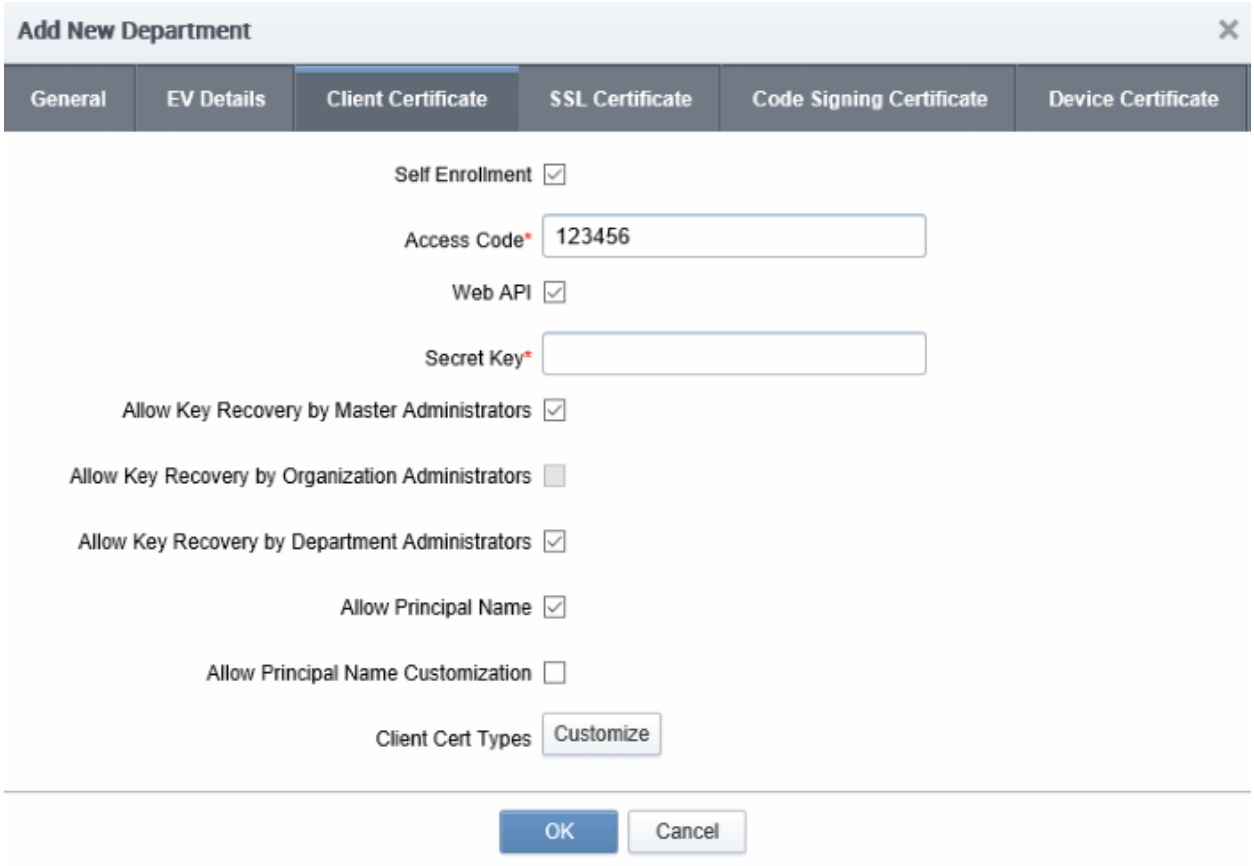
The **Add New Department** dialog includes the following setting areas, which, apart from the **Client Certificate** area, are the same as those in the **Add New Organization** dialog:

- **General** (see "Using the General Settings Area of the Add New Organization Dialog" on page 332).
- **EV Details** (see "Using the EV Details Area of the Add New Organization Dialog" on page 334)
- **Client Certificate** (see "Configuring Client Certificate Settings for a Department" on page 368)
- **SSL Certificate** (see "Using the SSL Certificate Area of the Add New Organization Dialog" on page 344
- **Code Signing Certificate** (see "Using the Code Signing Certificate Area of the Add New Organization Dialog" on page 353
- **Device Certificate** (see "Using the Device Certificate Area of the Add New Organization Dialog" on page 353).

If the parent organization is already validated by Sectigo, the address details are auto-populated with the parent organization's address. However, you have to name the department.

7.2.4.4.2 Configuring Client Certificate Settings for a Department

The **Client Certificate** area of the **Add New Department** dialog shown in the following illustration is the same as the one described in "Using the Client Certificate Area of the Add New Organization Dialog" on page 336, with the exception of several additional settings related to key recovery.



Allow Key Recovery by Master Administrators—Enabled by default if pre-enabled by a MRAO, in which case the MRAO can recover the private keys of client certificates issued by this organization. While being created, each client certificate is encrypted with the MRAO's master public key before being placed into escrow. In addition, if enabled, the organization cannot issue client certificates until the MRAO initializes their master key pair in the **Encryption** area.

Allow Key Recovery by Organization Administrators—Enabled by default if pre-enabled by a MRAO, in which case a RAO can recover the private keys of client certificates issued by this organization. While being created, each client certificate is encrypted with the RAO's master public key before being placed into escrow. In addition, if enabled, the organization cannot issue client certificates until the RAO initializes their master key pair in the **Encryption** area.

Allow Key Recovery by Department Administrators—Enabled by default if pre-enabled by a MRAO, in which case a DRAO can recover the private keys of client certificates issued by this department. While being created, each client certificate is encrypted with the DRAO's master public key before being placed into escrow. In addition, if enabled, the department cannot issue client certificates until the DRAO initializes their master key pair in the **Encryption** area.

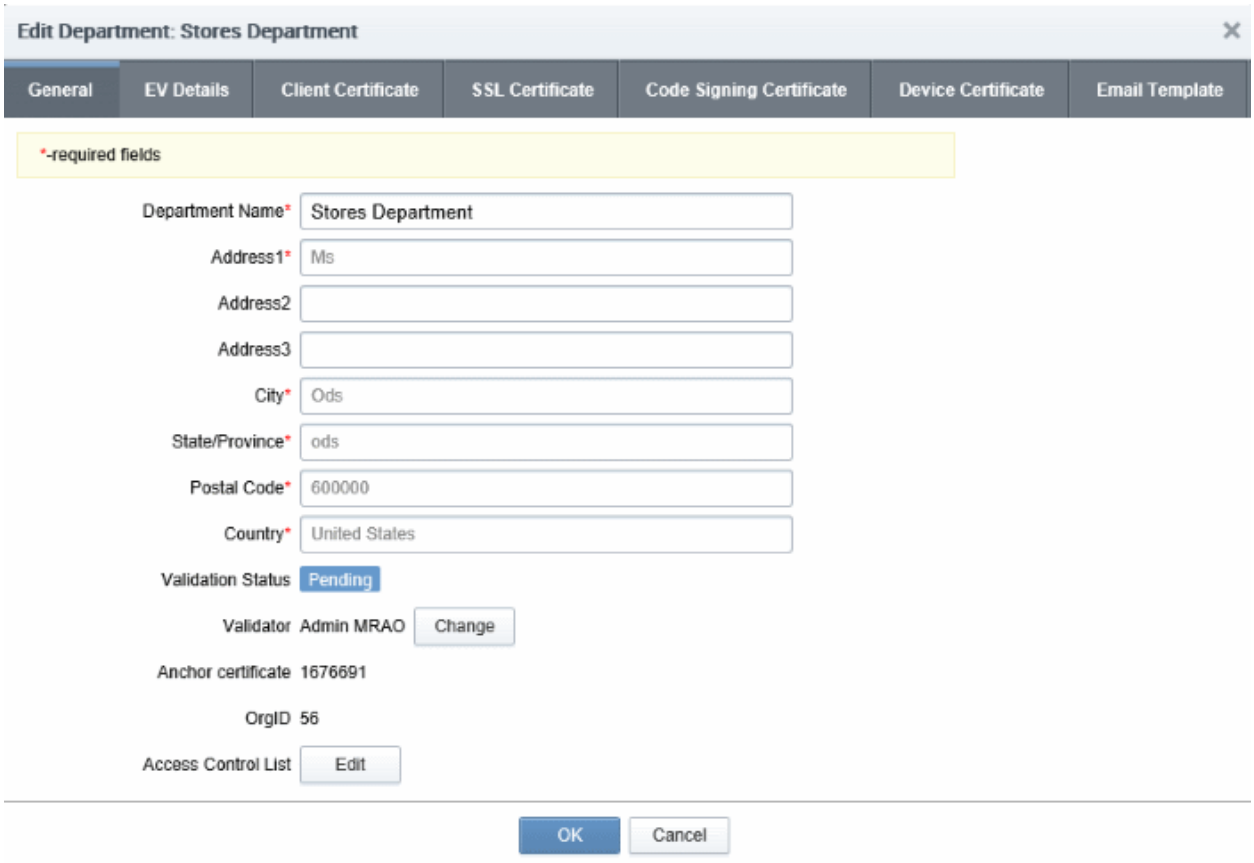
For more information, see "Configuring Key Escrow and Encryption" on page 473.

These settings are active only if a MRAO has enabled the appropriate key recovery options when configuring client certificate settings for the organization, as described in "Using the Client Certificate Area of the Add New Organization Dialog" on page 336.

7.2.4.4.3 Modifying Departments of an Organization

You can modify departments of any organization at any time as follows:

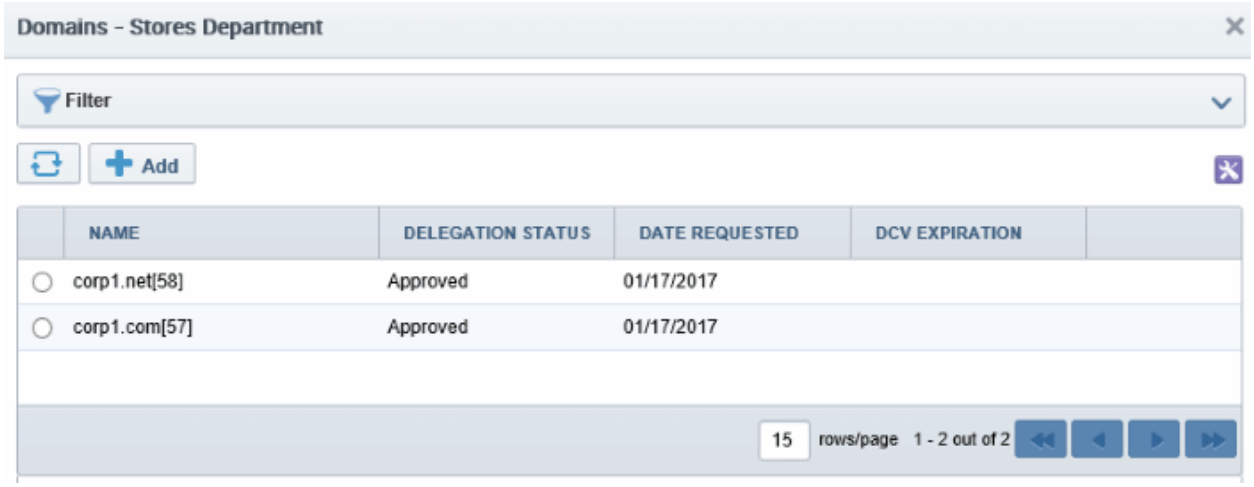
- From the main UI, navigate to **Settings > Organizations** and select the organization whose department you want to modify.
- Click **Departments** and select the department to be modified.
- Click **Edit** to open the **Edit Department** dialog shown in the following illustration.



The **General** area of the **Edit Department** dialog shown in the preceding illustration is the same as the one described in "Creating New Departments" on page 367, with the exception of an additional field **Access Control List** described in "Imposing Access Restrictions to the SCM UI" on page 361.

7.2.4.4.4 Managing Domains Belonging to a Department

You can view, edit, and delegate domains delegated to a department by selecting this department and clicking **Domains** to open the **Domains** dialog shown in the following illustration.



For more information, see "Managing and Configuring Domains" on page 382.

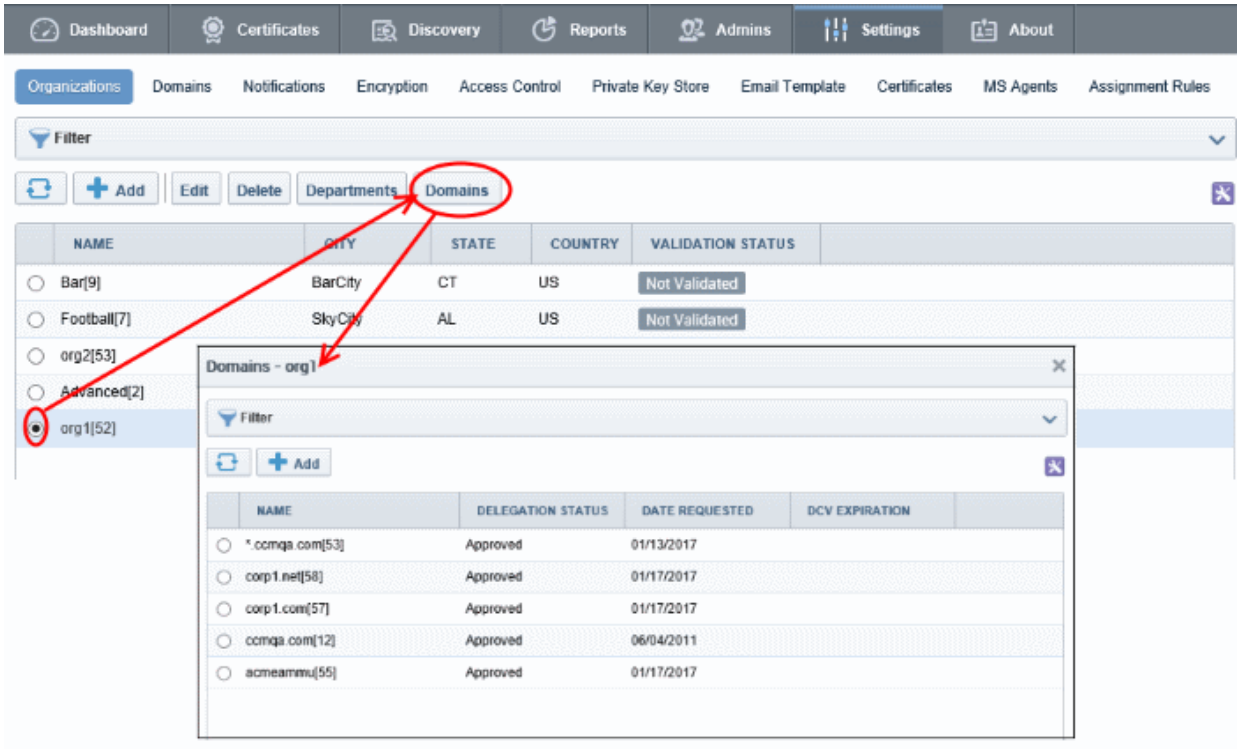
7.2.4.4.5 Deleting an Existing Department

If there is no longer a need to issue certificates from a particular department, you can delete this department by selecting it and clicking **Delete**.

NOTE: Deleting an organization automatically revokes any certificates issued to that department and deletes any end-users that are its members. That is the reason SCM prompts to confirm deletion of any organization.

7.2.4.5 Managing Domains of an Organization

You can view and manage domains delegated to an organization by navigating to **Settings > Organizations**, selecting the organization whose domains you wish to manage, and then clicking **Domains** to open the **Domains** dialog shown in the following illustration. This dialog lists all domains assigned to the organization and its departments.



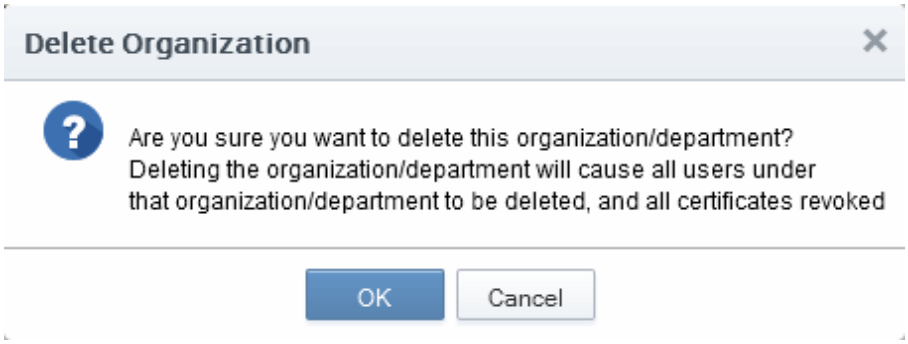
To assign a new domain, click **Add**.

To edit or delete a domain, click either **Edit** or **Delete** respectively.

For more information, see "Managing and Configuring Domains" on page 382.

7.2.4.6 Deleting an Existing Organization

MRAOs can delete an organization by navigating to **Settings > Organizations** from the main UI, selecting an organization in the list, and clicking **Delete**, and then clicking **OK** in the confirmation dialog shown in the following illustration.



When an organization is deleted, the following occurs:

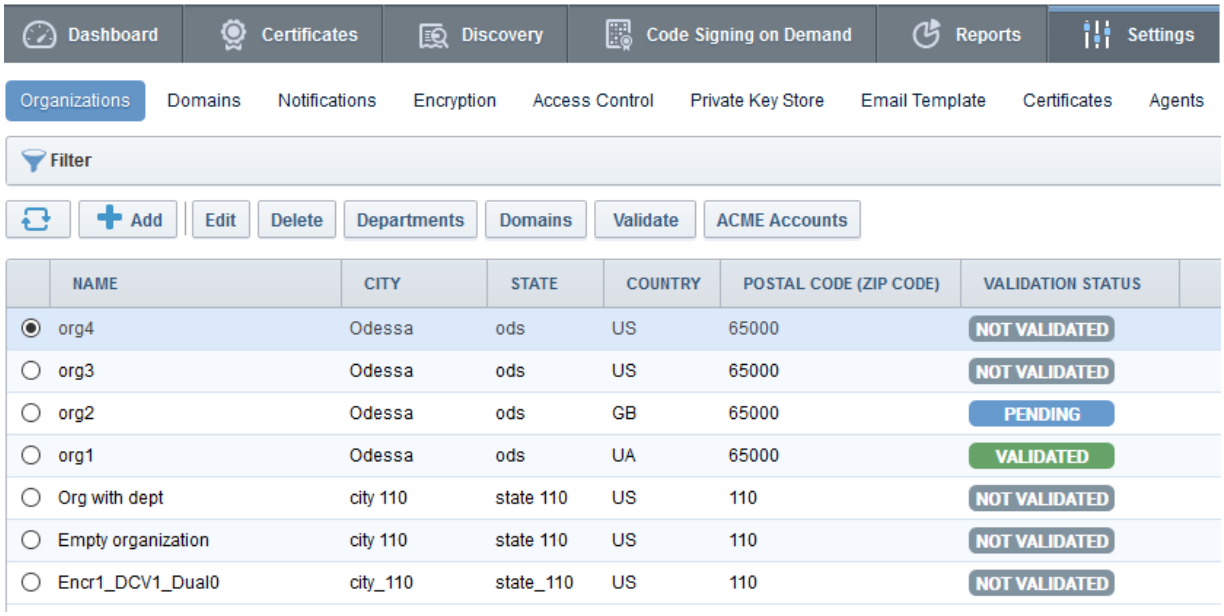
- It is no longer be possible to obtain new certificates for the organization.
- All certificates issued to the organization are revoked

- All end-users which belong to the organization are removed from SCM.

7.2.5 How to Configure ACME Accounts for Organizations and Departments

SCM provides support for Automatic Certificate Management Environment (ACME) protocol that automates interactions between a CA and its customers' web servers. SCM offers means of creating ACME accounts which can then be used for SSL certificate enrollment and management, as described in "Using the Sectigo ACME Service" on page 618. To use this functionality, contact your Sectigo account manager.

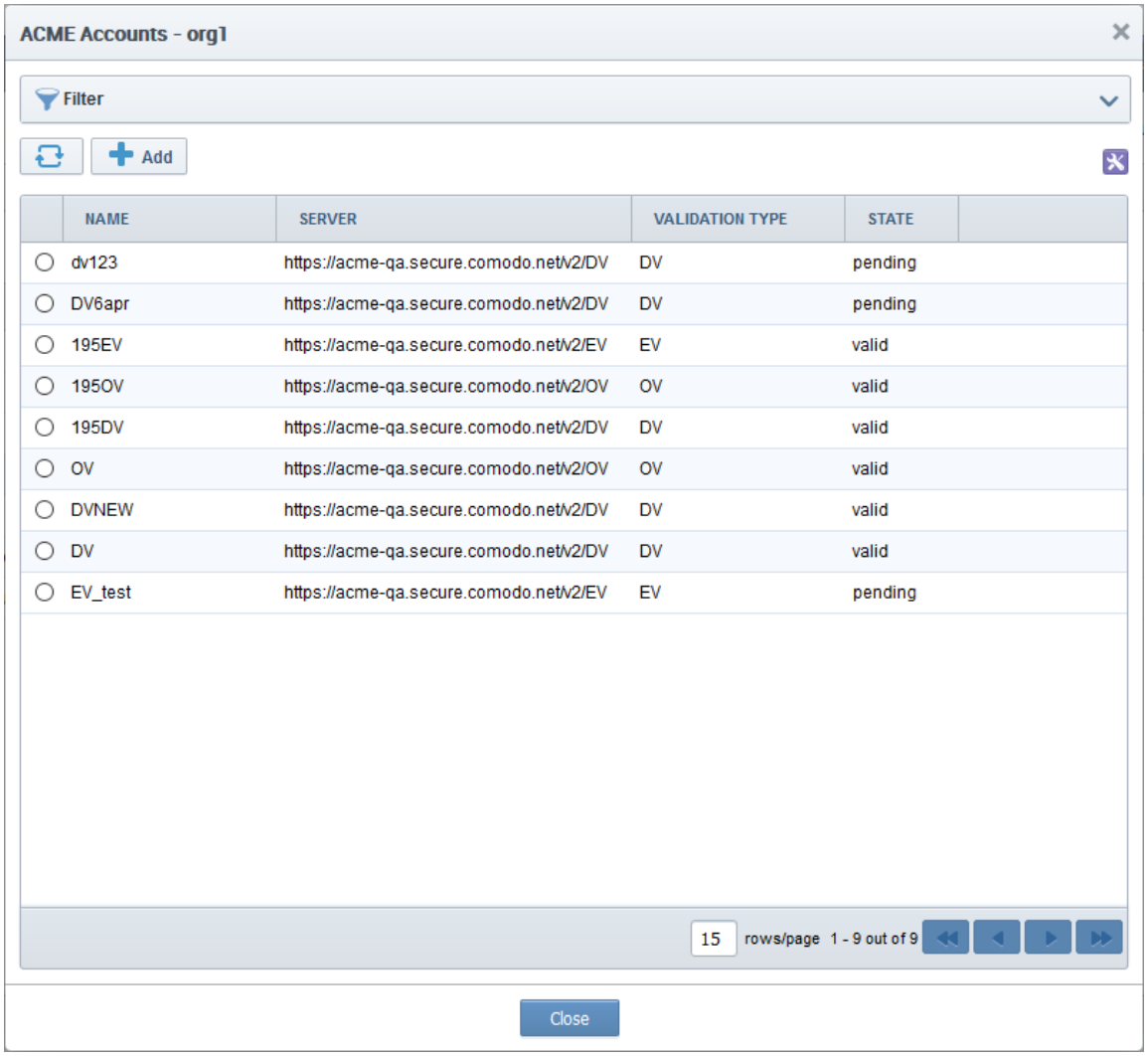
MRAO and RAO administrators can create ACME accounts for an organization and manage these accounts via the SCM UI by navigating to **Settings > Organizations**, selecting the organization from the list, as shown in the following illustration, and then clicking **ACME Accounts**.



In some cases, the organization's validation status plays a role in the ACME account creation. For more information, see "About the Organization's Validation Status and Server Validation Level in ACME Accounts" on page 381.

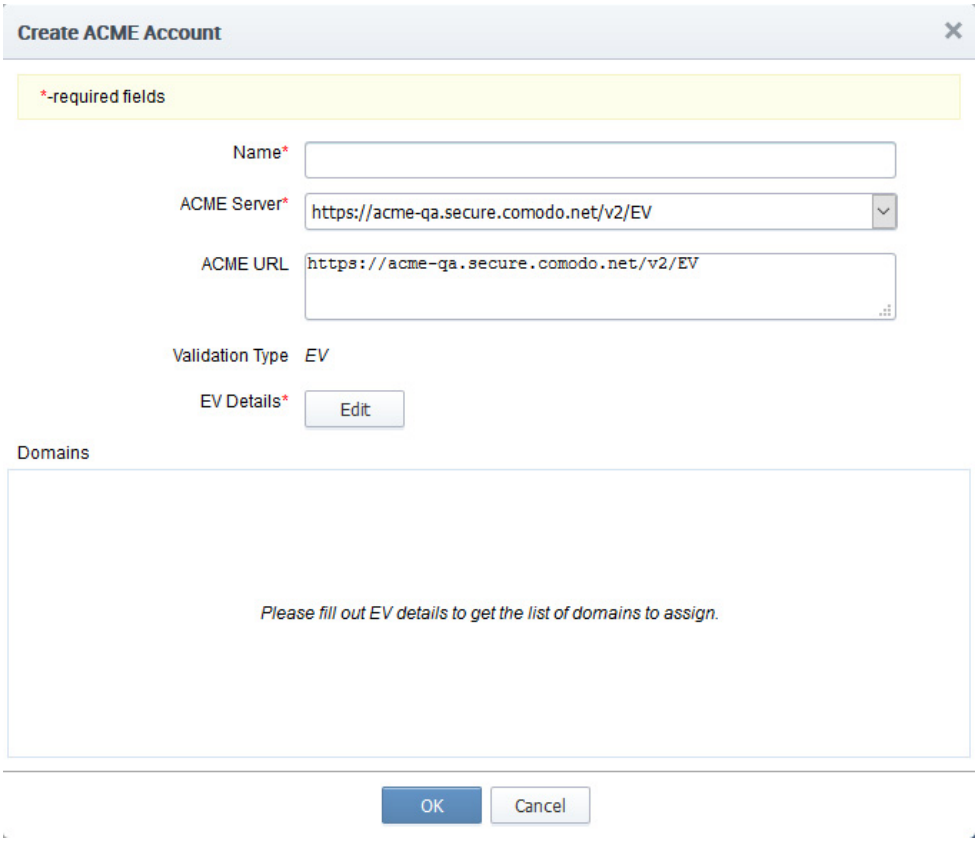
If the organization of your choice does not have any ACME accounts associated with it, the **ACME Accounts** dialog for that organization does not contain any data and the only available action is to add a new ACME account.

If the organization already has ACME accounts, the **ACME Accounts** dialog for that organization displays a list of existing accounts, as shown in the following illustration.

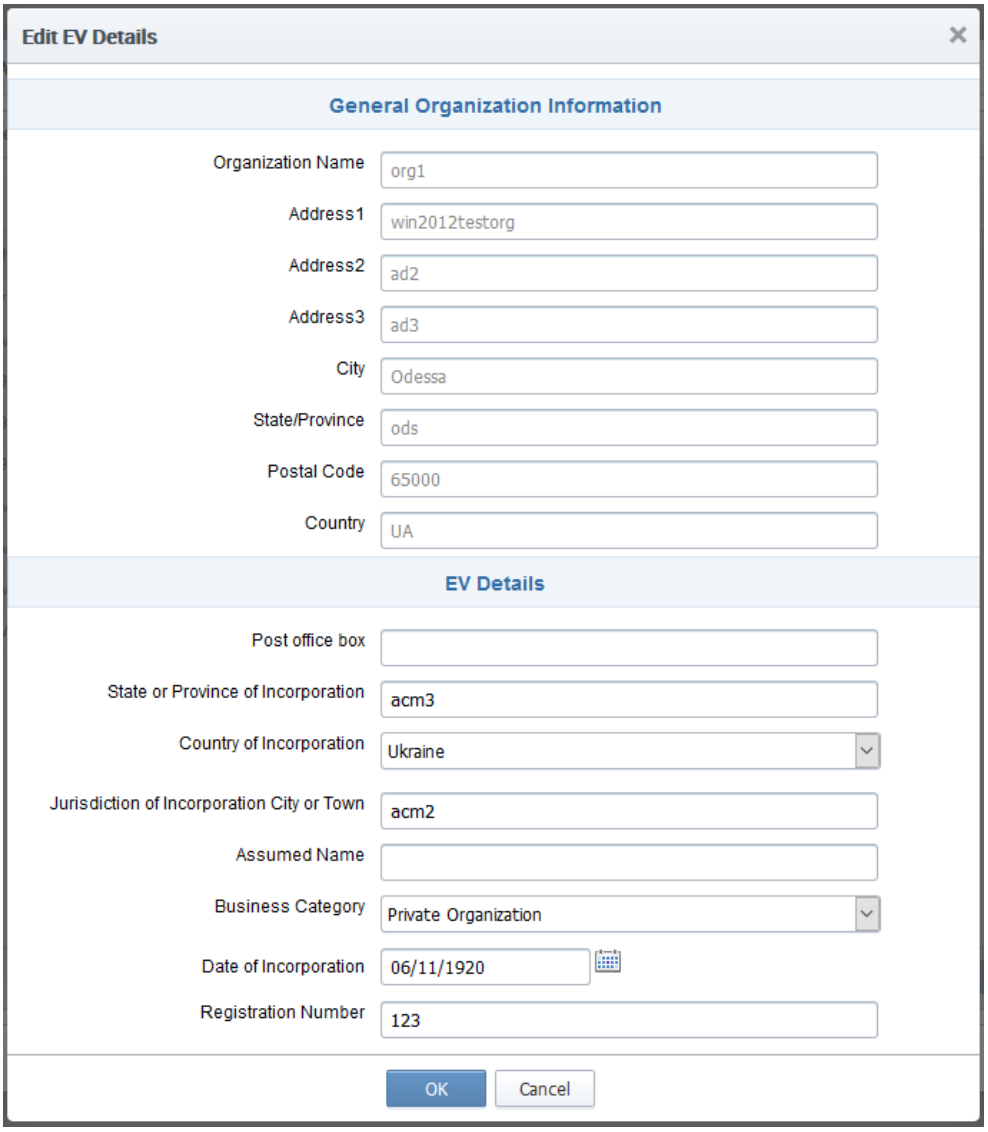


You proceed with creating an ACME account for a specific organization as follows:

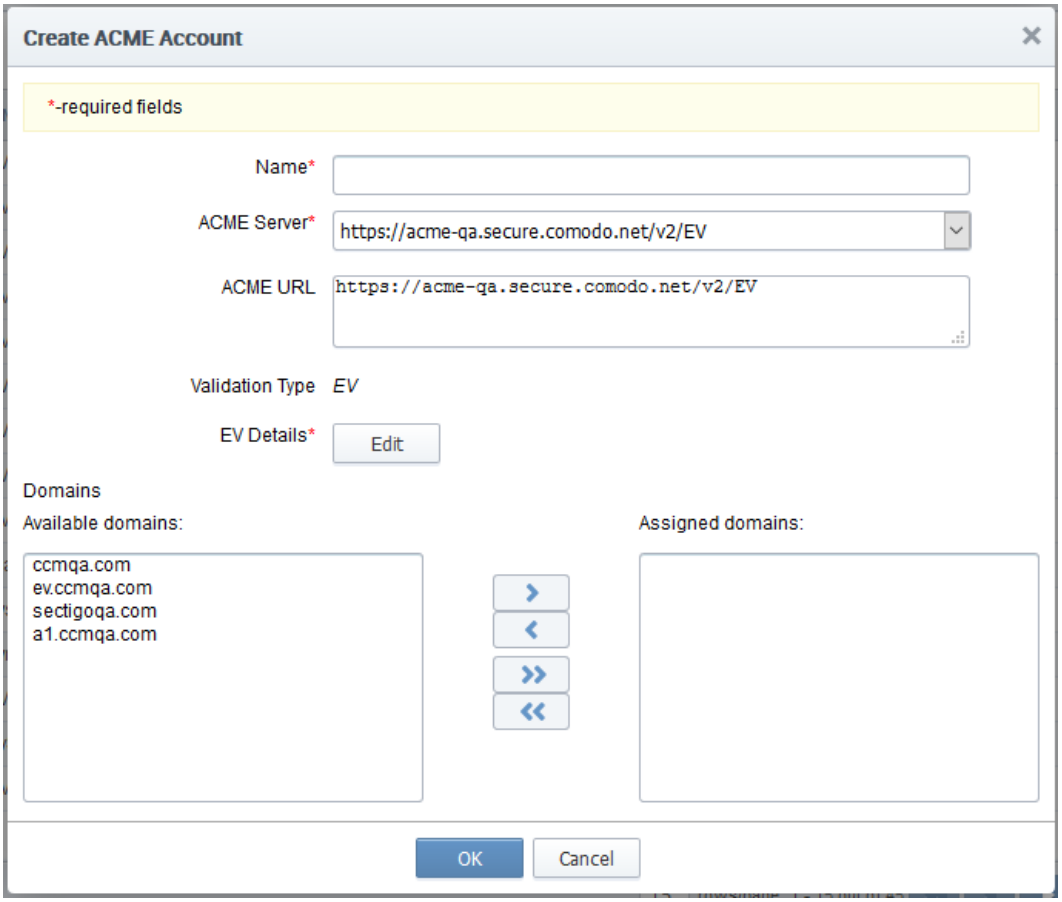
- Click **Add** on the **ACME Accounts** dialog to open the **Create ACME Account** dialog shown in the following illustration.



- Provide a descriptive name for the account.
- Use the **ACME Server** field to create an association between the new account and the ACME server tied to the issuing CA. Three options are available by default: DV, OV or EV CAs. The selected validation option is reflected in the **Validation Type** field.
- The **ACME URL** field shows the actual URL of the ACME account. It is recommended that you take a note of this URL, as this information is required to access the Sectigo ACME service to proceed with the SSL certificates enrollment.
- The **Validation Type** value is based on the selection you made in the **ACME Server** field. You proceed as follows:
  - If the **Validation Type** is set to EV, click **EV Details > Edit** to complete the **Edit EV Details** dialog for the organization, as shown in the following illustration.

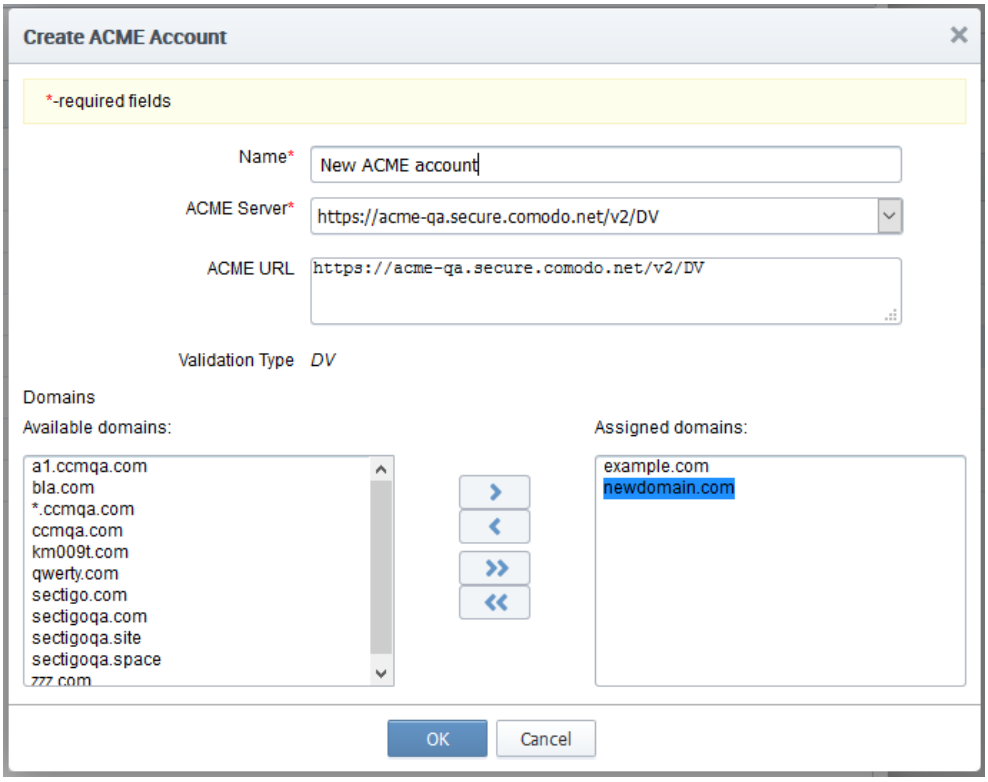


After you click **OK** on the **Edit EV Details** dialog, the **Domains** area of the **Create ACME Account** dialog displays a list of available domains from which you can select the ones you wish to assign to the new ACME account, as the following illustration shows.



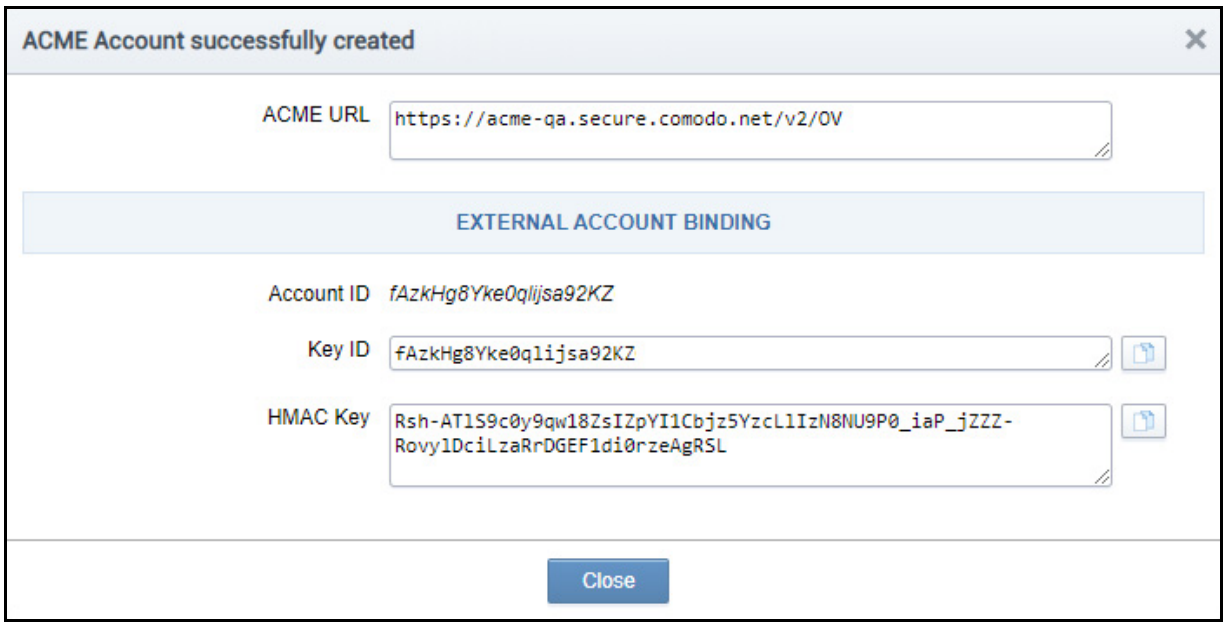
Selecting domains for an ACME account controls the boundaries of the account. In addition, the current validation status of the domain affects the ACME client.

- If the **Validation Type** for the new account is set to DV or OV, then the domains are already available and you need to select the ones to assign to the new ACME account, as shown in the following illustration.



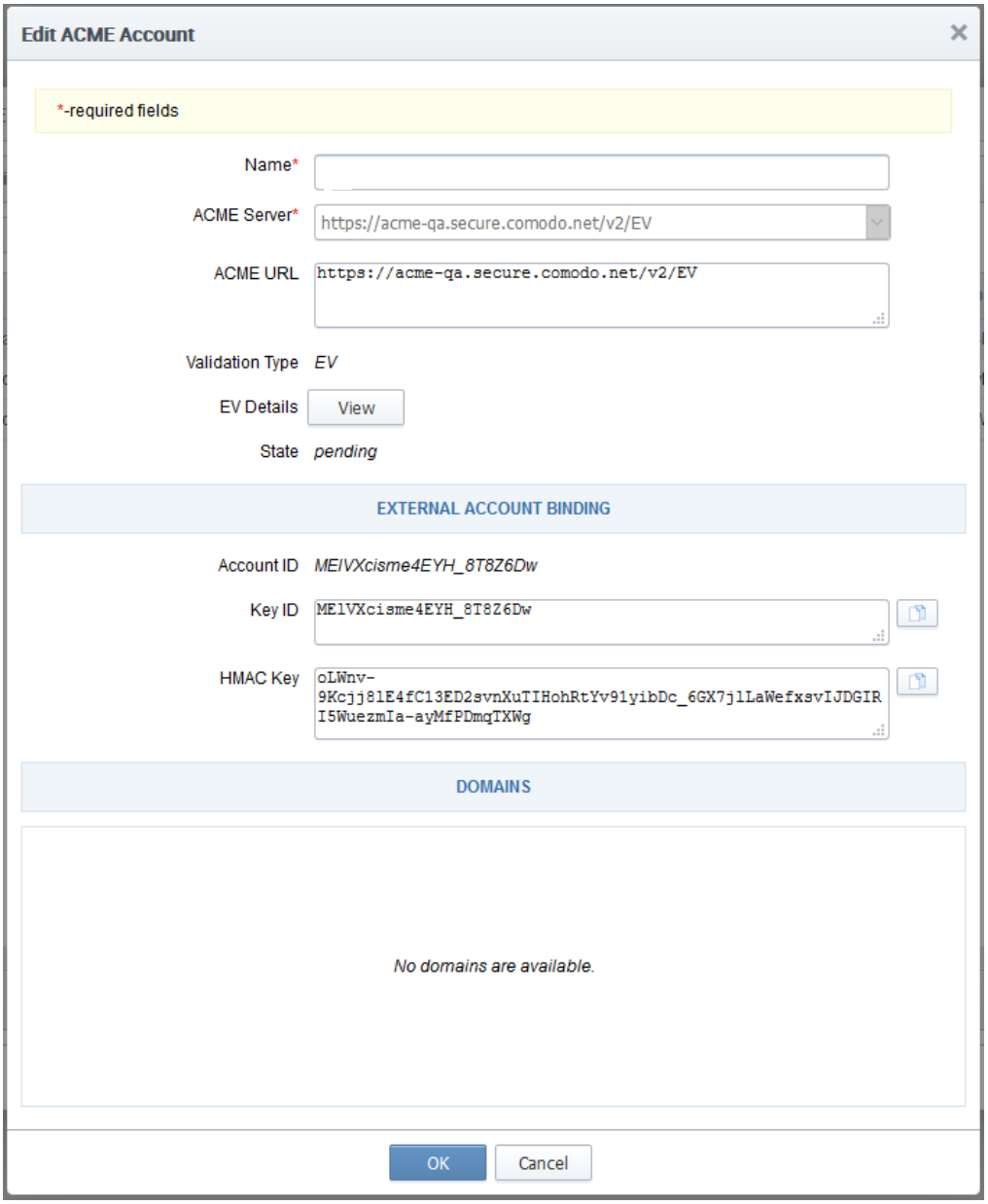
- Click **OK** to finalize the ACME account creation.
- The account is issued two identifiers: Key ID and HMAC Key which are based on the external account binding (EAB) ID and key respectively and act similarly to a user name and password pair. They, along with the ACME URL, are required when accessing the Sectigo ACME service to proceed with the SSL certificates enrollment.
- The account is assigned a value which populates the Account ID field.
- The account is added to the list of accounts in the **ACME Accounts** dialog for that organization.

Upon the successful creation of an ACME account, the Key ID, HMAC Key, and Account ID are displayed as shown in the following illustration:



You can modify an existing ACME account for a specific organization as follows:

- Using the **ACME Accounts** dialog, select an account from the list and click **Edit** to open the **Edit ACME Account** dialog shown in the following illustration.



- Use the **Edit ACME Account** dialog to do the following:
  - Provide the account name.
  - Modify the organization's EV details, in cases when the validation type is EV.
  - Assign domains.
  - If the account status is Pending, you can copy values from the Key ID and HMAC Key fields to clipboard. The EAB information is not displayed for accounts with any other status.
- Click **OK** to save your changes.

To delete one of organization's ACME accounts, select the account in the **ACME Accounts** dialog and click **Delete**.

As a MRAO or RAO administrator, you can also create ACME accounts for departments of organizations delegated to you and manage these accounts, as follows:

- From the main SCM UI, navigate to **Settings > Organizations**.
- Select the organization from the list.
- Click **Departments**.
- Select a department which needs an ACME account created or an existing account modified, and then click **ACME Accounts**.
- Follow the same procedures as you would for creating or editing ACME accounts for an organization.

7.2.5.1 About the Organization's Validation Status and Server Validation Level in ACME Accounts

When creating an ACME account, it is recommended to be aware of the following correlation between the organization's validation status and the validation level of the server associated with the account:

- The organization's validation status does not play a role when creating an ACME account associated with a DV server.
- If the new ACME account is associated with an OV server, the organization's validation status must be Validated.
- If the new ACME account is associated with an EV server, there must already be an anchor certificate with domains available for this ACME account. Otherwise, domains cannot be assigned to an ACME account.

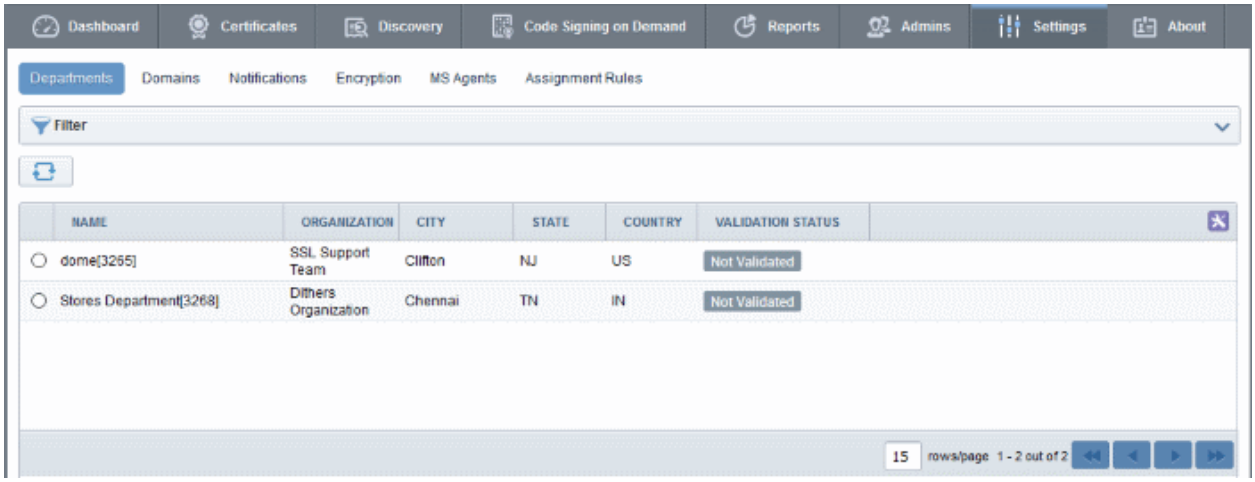
For more information, see the following:

- "Using the General Settings Area of the Add New Organization Dialog" on page 332
- "Using the EV Details Area of the Add New Organization Dialog" on page 334
- "Using the SSL Certificate Area of the Add New Organization Dialog" on page 344

7.3 Configuring Departments

The **Departments** area is visible only to DRAO administrators who can modify general and email template settings for a department by navigating to **Settings > Departments** from the main UI, selecting a department, and then clicking **Edit**, as shown in the following illustration.

MRAOs and RAOs see the **Organizations** area instead, which allows them to manage departments of an organization by first selecting an organization, and then clicking **Departments**, as described in "Managing Departments of an Organization" on page 365. The **Departments** area is, in effect, a limited view of the information available in the **Organizations** area, containing data and controls related to the department for which the DRAO is responsible.



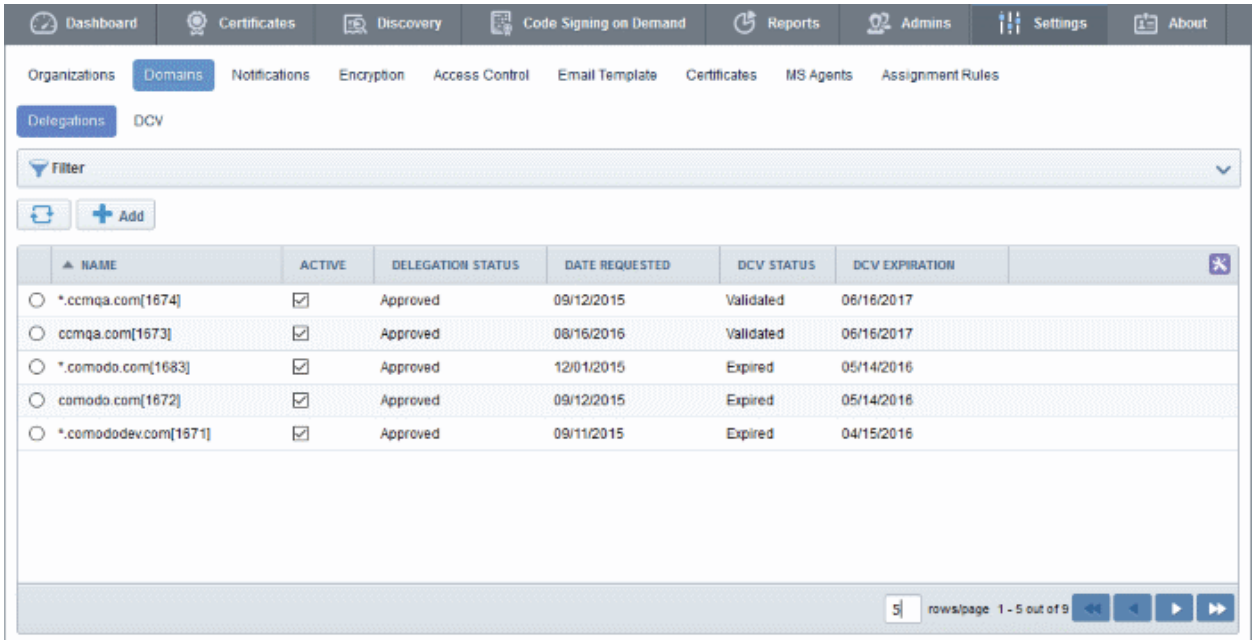
The **Departments** area is similar to the **Departments** dialog that appears after clicking **Departments** in the **Organizations** area.

As a DRAO administrator, you can create and modify ACME accounts for departments delegated to you. You do so by selecting a department from the list, clicking **ACME Accounts**, and then following procedures described in "How to Configure ACME Accounts for Organizations and Departments" on page 373.

7.4 Managing and Configuring Domains

Subject to your security role, the **Domains** area shown in the following illustration allows you to perform the following:

- View all domains associated with organizations and departments.
- Create new domains.
- Initiate DCV.
- Delegate domains to organizations and departments.
- Restrict the certificate types that can be issued on specific domains.



The level of the domain management depends on your security role, as follows:

- A MRAO can create, edit, and assign domains to any organization or department.
- A MRAO can request, approve, and manage certificates for any domain. The domains created by MRAO are automatically approved.
- A RAO can create, edit, and assign domains to organizations and departments that have been delegated to them.
- A RAO can initiate DCV, request, approve, and manage certificates for such domains. The domains created or approved by a RAO are to be validated and approved by two MRAOs with appropriate privileges. The delegation can also be approved by a single MRAO with domain validation without dual approval privileges.
- A DRAO can create, edit, and assign domains to departments that have been delegated to them.
- A DRAO can initiate DCV, request, approve, and manage certificates for such domains. The domains created by DRAO are to be validated and approved first by the RAO of the organization to which the department belongs, and then by two MRAOs with appropriate privileges. The delegation can also be approved by a single MRAO with domain validation without dual approval privileges. The Domain Awaiting Approval notification is sent to MRAO only after the domain created by DRAO is first approved by RAO.

Dual MRAO approval for created domains and DCV options are visible only if the respective features are enabled for your account.

The following table provides a summary of the preceding information.

Action	MRAO	RAO	DRAO
Creating domains	Yes	Yes	Yes

Action	MRAO	RAO	DRAO
Initiate DVC	Yes	Yes	Yes
Delegating domains	Can delegate domains to any organization and department.	Can delegate domains only to those organizations and departments that have been delegated to them.	Can delegate domains only to those departments that have been delegated to them.
Validating and approving created domains	Yes	Yes Can approve domains created by DRAOs of the departments under the organization, prior to approval by the MRAO.	No

A single domain can be delegated to more than one organization and department, as required.

7.4.1 About Wildcard Domains

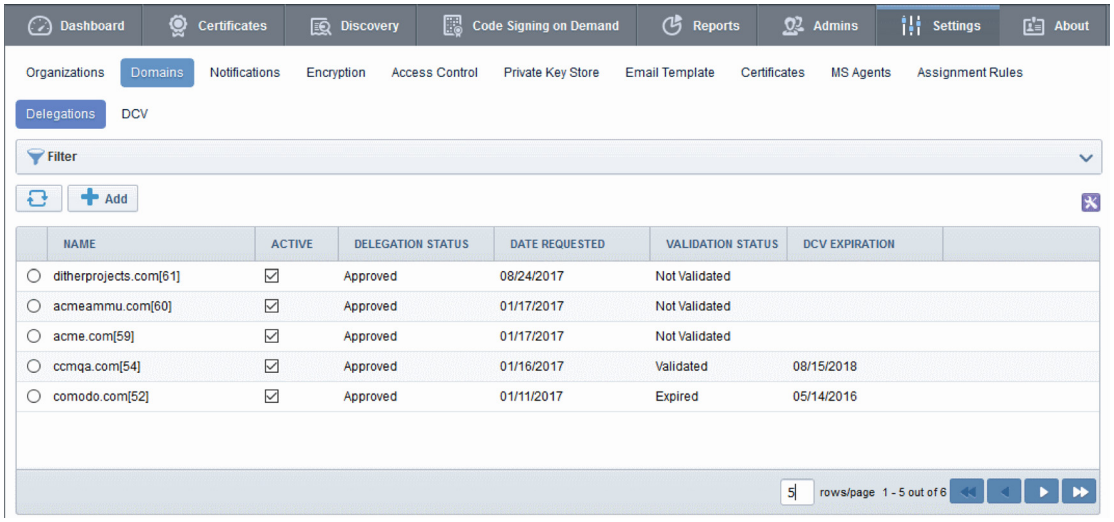
After a wildcard passes validation, the primary domain and all subdomains belonging to it are automatically validated only for the same organization or department.

For example, if `*.example.com` is delegated to and validated for Test Organization, then all subdomains (for example, `anything.example.com`, `something.example.com`) are automatically validated and approved for Test Organization.

If a subdomain of `example.com` is delegated to a different organization or department, then it must be approved by a MRAO and must pass validation again.

7.4.2 How to Manage Domains

You manage domain by navigating to **Settings > Domains** from the main UI to open the domain management area shown in the following illustration.



The domain management area has the following two subareas:

- **Delegations** area indicates whether or not the domain has been assigned to an organization or department. SCM cannot issue certificates to a domain unless it has been delegated to an organization or department. This interface shows all enrolled domains, along with their delegation status.

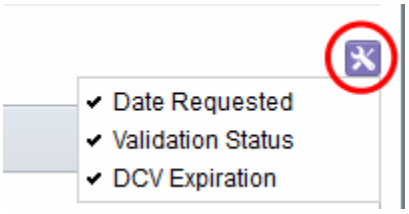
  A single domain can be delegated to any number of organization or department. You can add new domains and delegate them from this interface. You can also approve domain delegations made by other administrators.
- **DCV** area indicates status of all enrolled domains and allows you to initiate the DCV process. This area is only be visible if the DCV feature is enabled for your account.

7.4.2.1 Delegating Domains

You access the domain delegation interface, navigate to **Settings > Domains > Delegations**. This area shows a list of requested and approved domains and, depending on your security role, allows you to do the following:

- A MRAO can add new domains (which are approved automatically), view details of any domain, delegate a domain to any organization or department, approve any domain request, and initiate domain control validation on any domain.
- A RAO can view existing and add new domains to organizations that have been delegated to them, delegate domains to their organizations and departments and approve domain requests from DRAOs. Domains created or approved by a RAO need to be approved by two MRAOs with appropriate privileges. If Allow domain validation without Dual Approval was selected during the MRAO creation process, then requests can be approved by a single MRAO.
- A DRAO can view and add new domains to departments that have been delegated to them, as well as delegate domains to their departments. Domains requested a DRAO must be approved by the organization RAO, and then by two MRAOs. If Allow Domain Validation without dual approval was selected during the MRAO creation process, then requests can be approved by a single MRAO. An approval notification is only be sent to the MRAO after the domain has been approved by the RAO.

The following table lists settings and elements of the **Delegations** area.

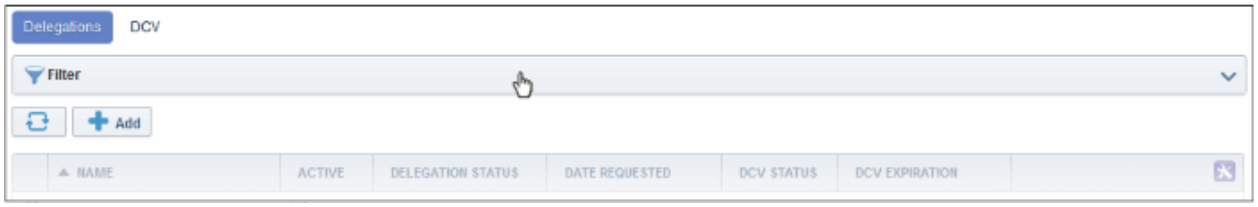
Column / Element	Description
Name	All available domains created for this account. The list is displayed in ascending alphabetical order. The domains which are awaiting approval are displayed in red.
Active	Allows you to toggle the domain between the active and inactive statuses. If inactive, the status of the domain is shown as suspended.
Delegation Status	Indicates the request or approval status of the domain.
Date Requested	Indicates the date on which the domain was requested.
Validation Status	Indicates the DCV status of the domain. This column is visible only if the respective feature is enabled for your account.
DCV Expiration	The date on which the DCV for the domain is to expire.
You can use the tool button to select columns to be displayed in the table: 	
Controls	Add—Requests a new domain for an existing organization or department.
	Refresh—Updates the list of displayed domains.
Domain Control Buttons [a]	View—Enables you to view details of the domains. The MRAO can also validate and approve the domains created by self or other administrators using this control.
	Delegate—Enables you to associate or delegate an existing domain to organizations and departments as required. Not visible to DRAOs.
	Delete—Deletes the domain. Available only for domains yet to be approved.

a. The domain control buttons are visible only when domain is selected.

7.4.2.2 Sorting and Filtering Domains

You can sort items in the alphabetical order by clicking a column header, and you can use filters to search for particular domains.

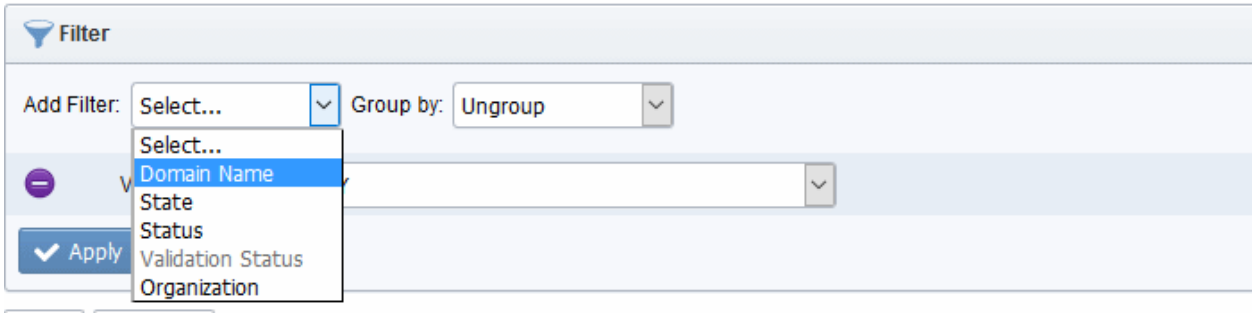
You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.



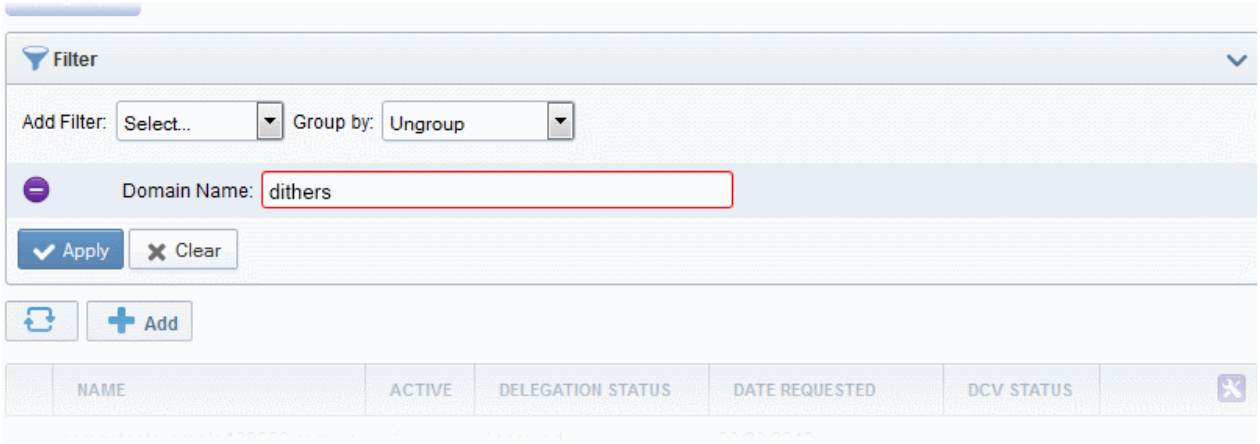
Filter Option	Description
Domain Name	The domain name to search for a particular domain.
State	• Active—Domains that have been enabled for certificate issuance. • Inactive—Domains that have been not been enabled for certificate issuance. • ANY—Both active and inactive domains.
Status	Approval status, as one of the following: • Requested—Domains requested by RAOs and DRAOs. These domains are awaiting approval by a MRAO. • Approved—Domains which have been approved by a MRAO. Certificates can be issued to approved domains providing they have also passed domain control validation. • ANY—Both requested and approved domains.
Validation Status	Domain control validation status. Valid values are: • Not Validated—Domains which have not yet passed DCV. This could be because the MRAO is yet to initiate DCV on the domain, or because DCV is currently in progress.[a] • Validated—Domains which have passed domain control validation. • Expired—Domains for which DCV has expired. DCV needs to be rerun on domains after 1 year. Certificates already issued to the domain remain valid even if DCV expires. However, you need to repeat DCV if you want to obtain new certificates for the domain. • ANY—All certificates, regardless of the DCV status.
Organization [b]	The organization from the list to view only those domains that belong to the organization.

a. Since internal domains do not require DCV, they are considered Not Validated.
b. Not visible to RAOs and DRAOs.

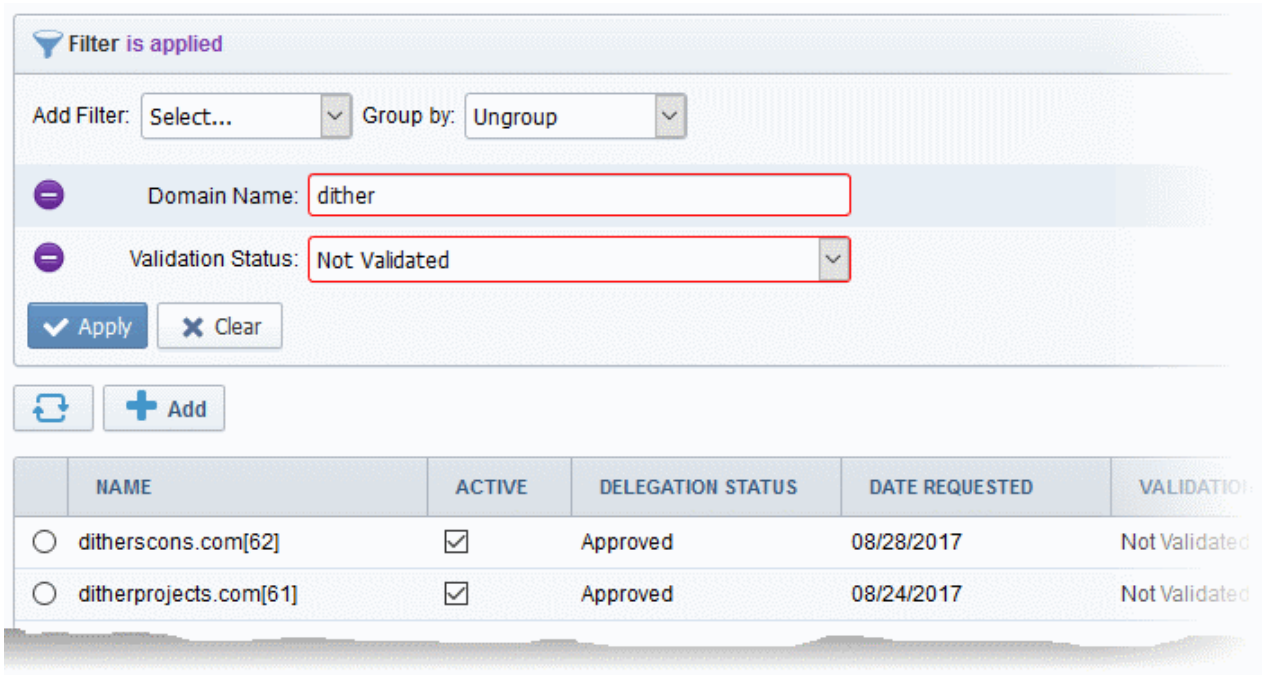
To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection from the **Add Filter** list.



Then you enter or select the filter parameter as per the selected criteria.



The filtered items based on the entered parameters are displayed:



You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **Domains** screen, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

7.4.2.3 Using Tool Tips

You can mouse over a domain to quickly view to which organizations and departments it has been delegated, as shown in the following illustration. In addition, tool tips indicate if the domain is awaiting approval from a MRAO.

7.4.2.4 Configuring DCV

You can configure DCV by navigating to **Settings > Domains > DCV** from the main UI. The **DCV** area shown in the following illustration displays registered domains, along with their DCV status and the date when DCV expires. Using this area, you can initiate DCV on domains. A public domain must pass DCV before Sectigo can issue a certificate to it.

DCV expires after 1 year and must be renewed. Existing certificates for the domain remain valid even if DCV expires. However, you need to pass DCV again in order to obtain new certificates for the domain.

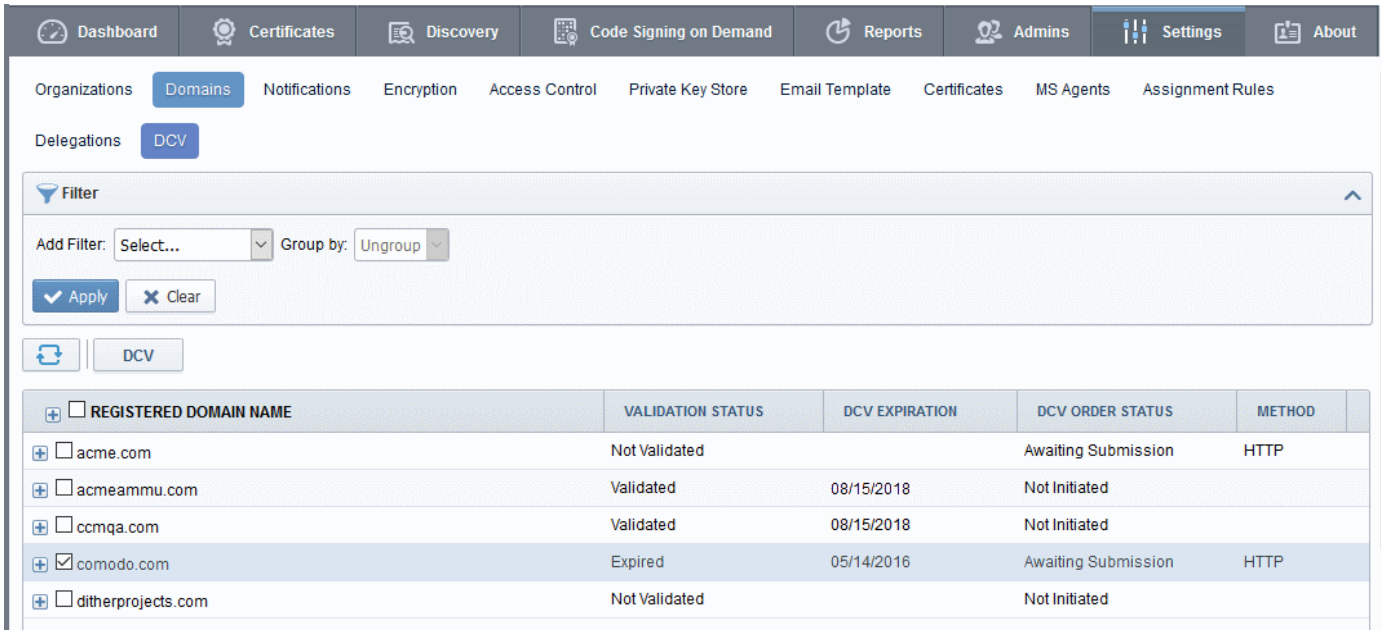
Depending on your security role, the **DCV** area allows you to do the following:

- A MRAO can initiate DCV on any registered domain.
- A RAO SSL can initiate DCV on domains which have been delegated to the RAO's organizations. DCV requests from a RAO must be approved by a MRAO.
- A DRAO SSL can initiate DCV on domains which have been delegated to the DRAO's departments. DCV requests from a DRAO must be approved by a MRAO.

You can use the following DCV methods:

- Email—SCM sends an automated email with a validation link to the email address of the domain administrator holding control over the domain hosted on the company's web server. The domain is validated on the domain administrator visiting the validation link in the mail.
- DNS CNAME—SCM sends a hash value that must be entered as DNS CNAME for the domain. SCM validates by checking the DNS CNAME of the domain.
- HTTP/HTTPS File—SCM sends a `.txt` file which is to be placed at the root of the web server. SCM validates the domain based on the presence of the sent file.

If a wildcard domain is created and delegated to an organization or department, SCM validates only the registered High Level Domain (HLD). If the HLD is successfully validated, all the subdomains within the name space of the HLD are considered validated.



The following table lists settings and elements of the **DVC** area.

Column/Element	Description
Registered Domain	All available domains created for this account. Clicking the ' + ' beside a domain name displays the subdomains of the registered domain.
Validation Status	Indicates whether the domain has passed DCV or not. Status can be one of the following: • Not Validated—DCV has not been initiated or is in-progress for the registered HLD.[a] • Validated—The registered HLD has passed DCV. • Expired—DCV on the domain has expired and has to be renewed. The DCV process has to be restarted for the domain.
DCV Expiration	The date when DCV for the domain expires. The DCV has to be done again after the expiry period.
DCV Order Status	Progress of validation on the domain. Valid values are: • Not Initiated—DCV has not been started for the registered HLD. • Awaiting Submittal—DCV has been initiated but the request has not yet been sent to the domain administrator (who has control of the web server on which the domain is hosted). The Awaiting... status is only available for the following DCV methods: HTTP / HTTPS; CNAME. • Submitted—The DCV request has been sent to the domain administrator for implementation. • Validated—The registered HLD has passed DCV. • Expired—DCV has expired on the domain. The DCV process has to be restarted for the domain.

Column/Element	Description
Method	The DCV method chosen by you for validating the domain.
DCV Control Button [b]	Enables MRAOs, and RAOs SSL, and DRAOs SSL to initiate or restart the DCV process for the selected domain.

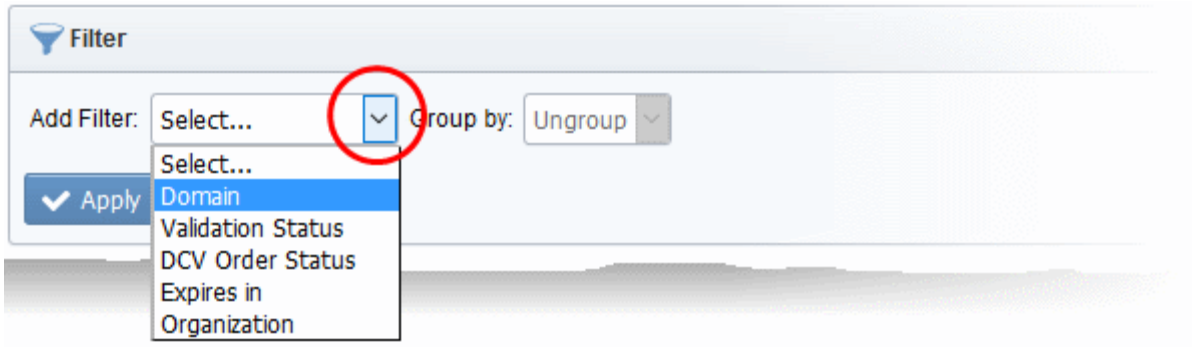
a. Because internal domains do not require DCV, they are considered Not Validated.
b. Appears only when a domain is selected.

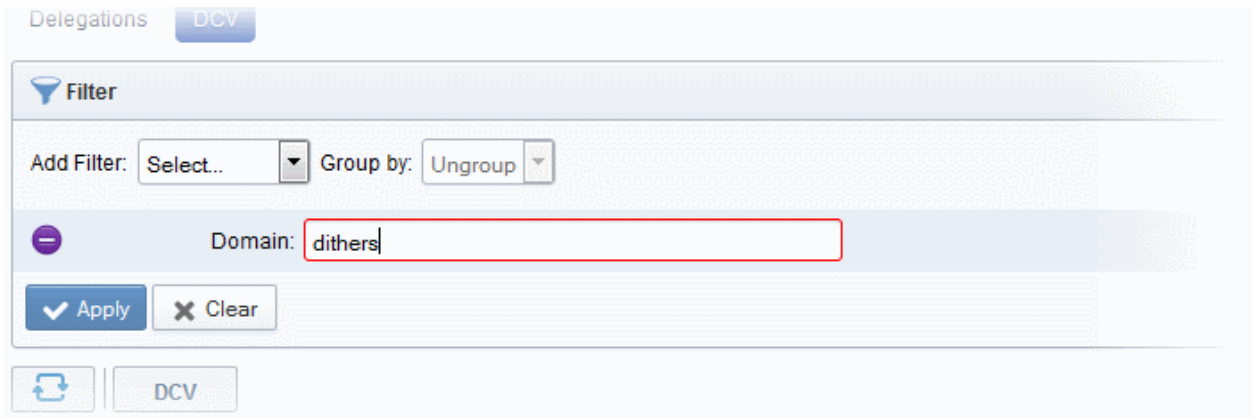
7.4.2.4.1 Sorting and Filtering DCV Status of Domains

You can sort items in the alphabetical order by clicking a column header, and you can use filters to search for particular domains.

You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as shown in the following illustration.

To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection from the Add Filter list.



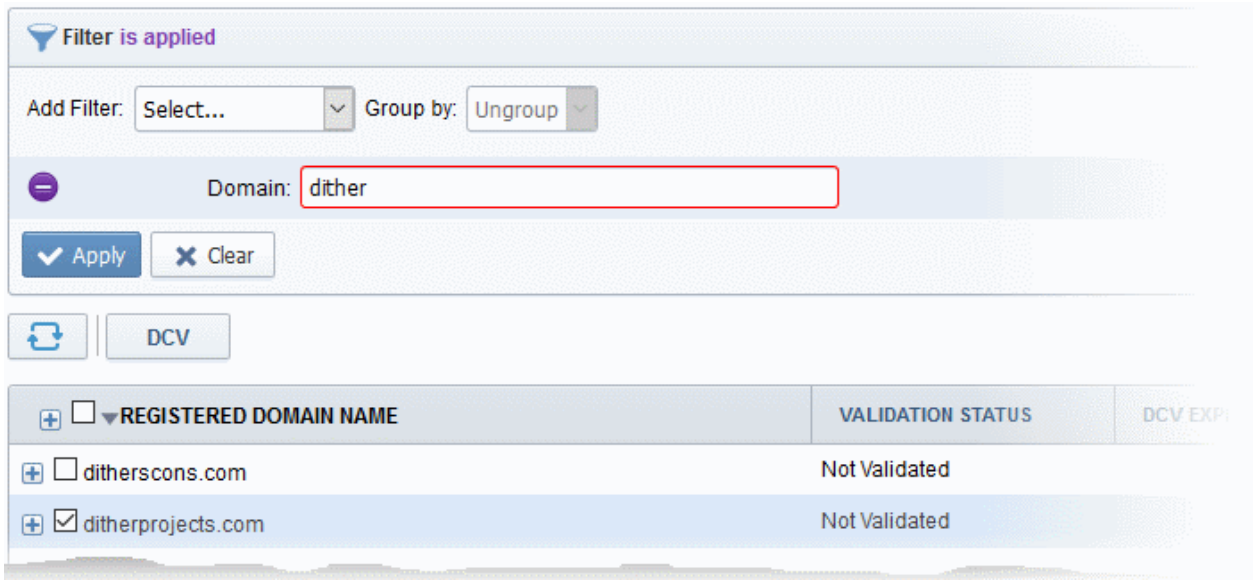


The following table lists the available filter criteria and filter parameters.

Filter Option	Description
Domain	Allows to filter the list of domains by name.
Validation Status	Allows to filter domains based on their validation status, as follows: • ANY—Shows all domains. No filters are applied. • Not Validated—Shows domains which have not yet passed DCV. A public domain must pass DCV before Sectigo can issue certificates to it. You should initiate the DCV process on required domains.[a] • Validated—Shows domains which have successfully passed DCV. • Expired—Domains on which DCV has expired. DCV lasts for one year before it must be renewed. Existing certificates remain valid, but you must pass DCV on the domain again before you can order new certificates for it.
DCV Order Status	Filter domains based on their DCV order status, as follows: • ANY—Displays the list of all the domains. • Not Started—Shows domains for which the DCV process has not yet been started. • Awaiting Submittal—Shows domains for which the DCV process was initiated but the request has not yet been submitted for approval by a MRAO. • Submitted—Shows domains for which DCV has been submitted to a MRAO for approval. • Validated—Shows only domains which have passed DCV. • Expired—Displays a list of domains on which DCV has expired.
Expires in	Filters domains based on the remaining days for their DCV expiry. You can choose the domains whose DCV request expires as follows: • Any • Next 3 days • Next 7 days • Next 14 days • Next 30 days • Next 60 days • Next 90 days
Organization	Filters only the domains associated with the organization selected from the list. Not visible to RAOs and DRAOs.

a. Because internal domains do not require DCV, they are considered Not Validated.

After the filters have been applied, filtered items based on the entered parameters are displayed, as shown in the following illustration.



You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **DVC** screen, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

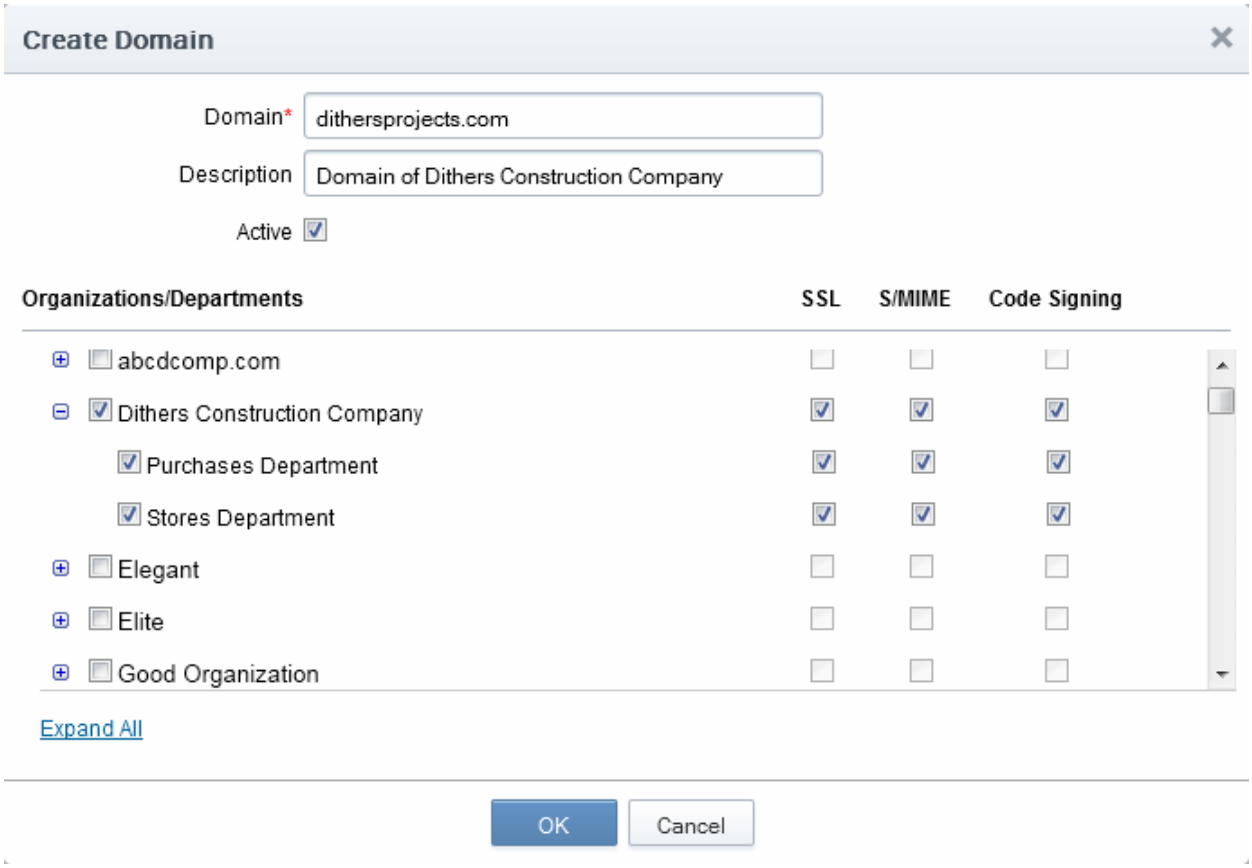
7.4.2.5 Creating a New Domain

Before you can request certificates, you first need to create domains then delegate them to organizations or departments. The delegated public domains must pass DCV that is initiated by a MRAO, RAO SSL, or DRAO SSL with sufficient privileges.

Only approved and validated domains are facilitated for the request and approval of the SSL certificates and the issuance of client certificates to the end-users falling within the domain.

You can also restrict the certificate types that can be requested for the domain depending on the purpose for which its use is authorized.

To create a new domain, navigate to **Settings > Domains** and click **Add** to open the **Create Domain** dialog shown in the following illustration.



The following table lists settings and elements of the **Create Domain** dialog.

Field / Element	Description
Domain	The name of the domain.
Description	A short description of the domain.
Organizations/ Departments	Enables you to delegate the currently created domain to an organization or department. All organizations are listed by default. Clicking the ' + ' button beside the organization name expands the tree structure to display the departments associated with the organization. The created domain can be associated with organizations and departments by making the respective selections. A single domain can be delegated to more than one organization or department. Clicking **Expand All** expands the tree structure to display all the departments under each organization.
SSL, Client Certificate, Code Signing	Enables you to allow or restrict the types of certificates that can be requested for the created domain. The certificate types can be restricted according to the purpose of the domain created.
Active	Enables you to toggle the status of the domain between active (default) and inactive states.

7.4.2.5.1 Validating New Domains

Any public domain added to SCM must pass DCV before Sectigo can issue certificates to it. DCV requires your company to prove it has control of the domain. The domain administrator can confirm control via email validation, or by placing a `.txt` file in a publicly accessible location, or by making a DNS CNAME entry.

SCM administrators can initiate DCV on an individual basis or, if all domains share a common WhoIs email record, may initiate DCV on multiple domains at once.

The type of actions you can perform with regards the new domain validation depends on your security level, as follows:

- A MRAO can initiate DCV on any registered domain.
- A RAO SSL can initiate DCV on domains which have been delegated to the RAO's organizations. DCV requests from an RAO must be approved by a MRAO.
- A DRAO SSL can initiate DCV on domains which have been delegated to the DRAO's departments. DCV requests from a DRAO must be approved by a MRAO.

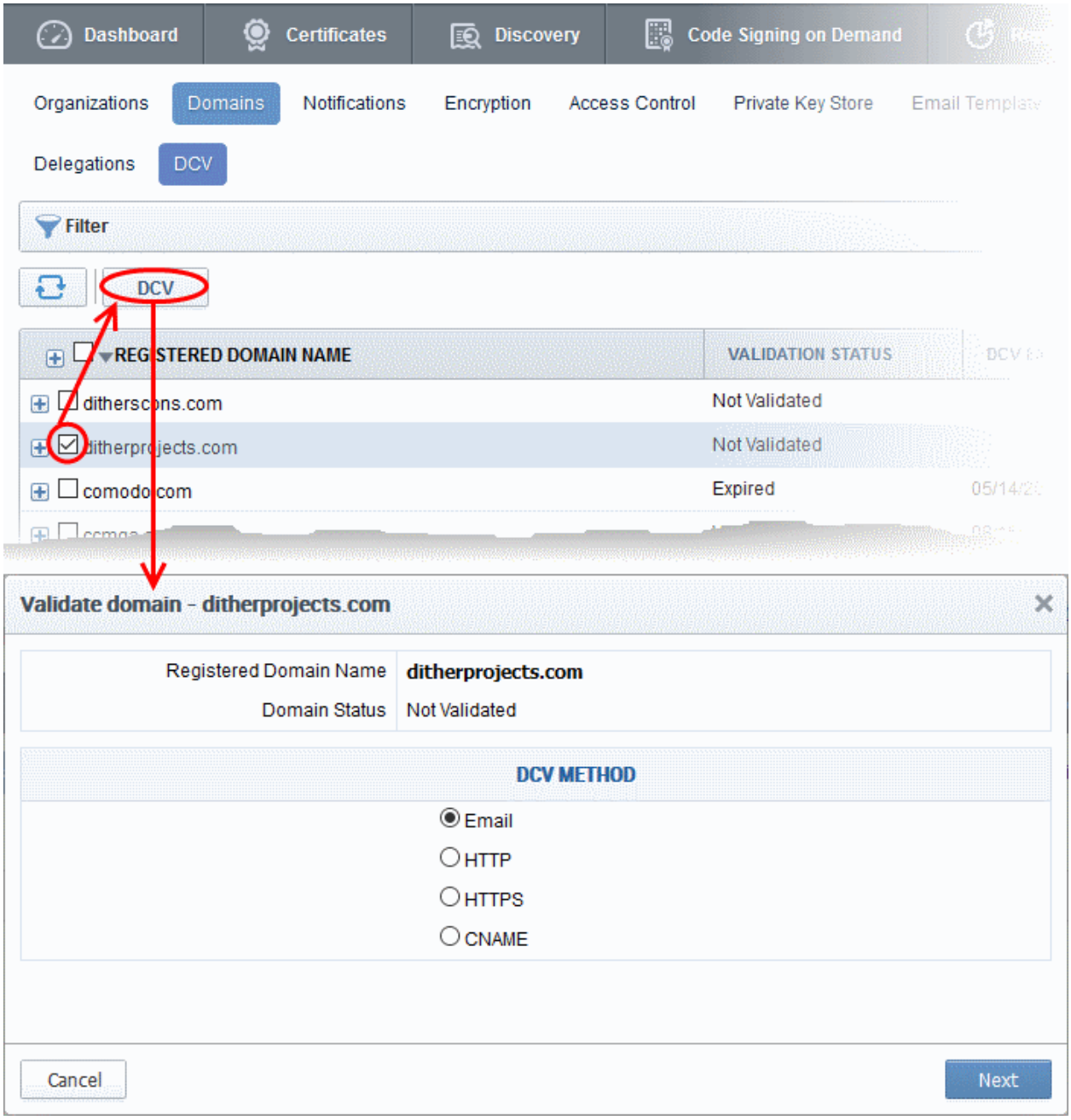
The following are possible methods of completing DCV:

- Email—SCM sends a challenge-response email to a mail address on the domain. You can choose the email address during setup. The email contains a link to validate your ownership of the domain. The email method can be used for both validating a single domain and multiple domains at a time.
- DNS CNAME—SCM generates a hash value that must be entered as DNS CNAME for the domain. SCM validates by checking the DNS CNAME of the domain.
- HTTP/HTTPS File—SCM generates a `.txt` file which is to be placed on the root of the web server. SCM checks for the presence of the file.

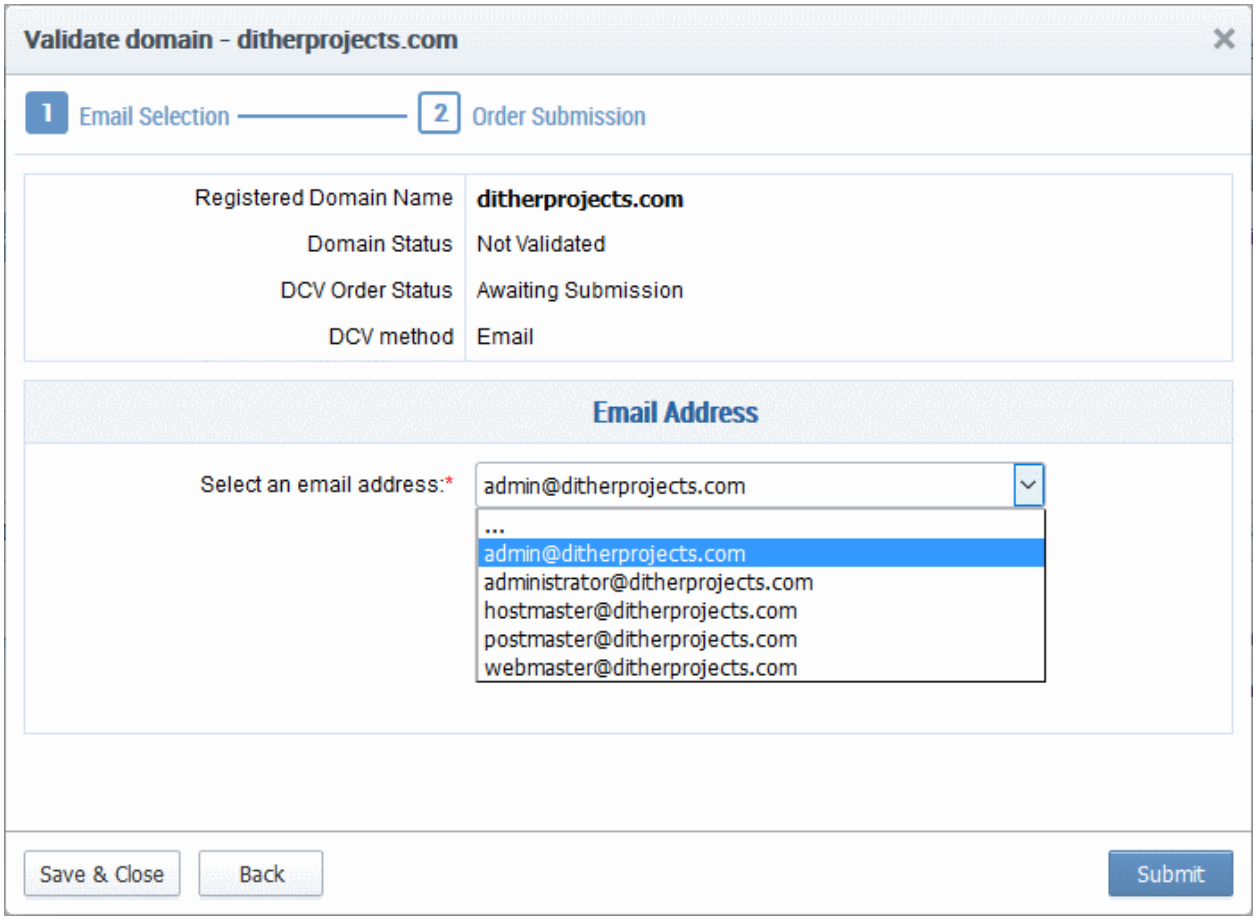
If a wildcard domain is created and delegated to an organization or department, SCM validates only the registered HLD. If the HLD is successfully validated, all the subdomains within the name space of the HLD are considered validated.

To initiate DCV for a single public domain, perform the following:

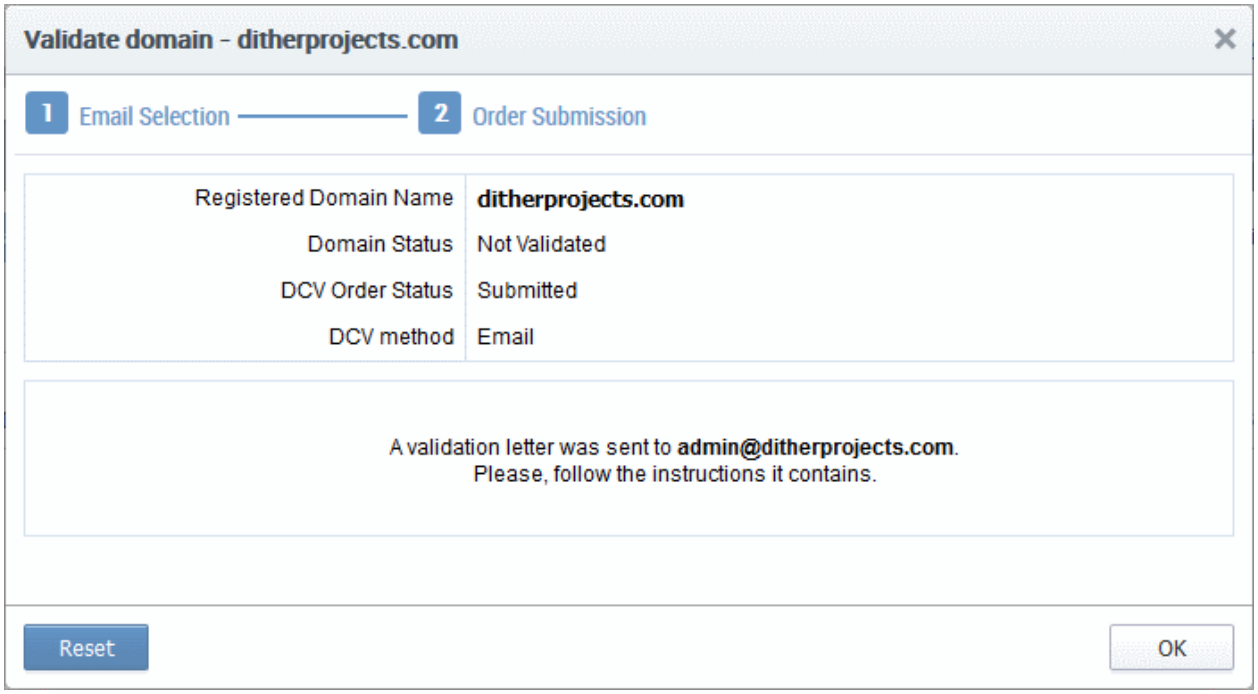
- Open the **DCV** area by navigating **Settings > Domains > DCV** from the main UI.
- Initiate DCV by selecting the domain and clicking **DCV** to open the **Validate Domain** wizard shown in the following illustration.



- Select the DCV method from and click **Next**.
  - If you selected **Email**, you can proceed to selecting the email address of the domain administrator for sending the validation email, as shown in the following illustration.

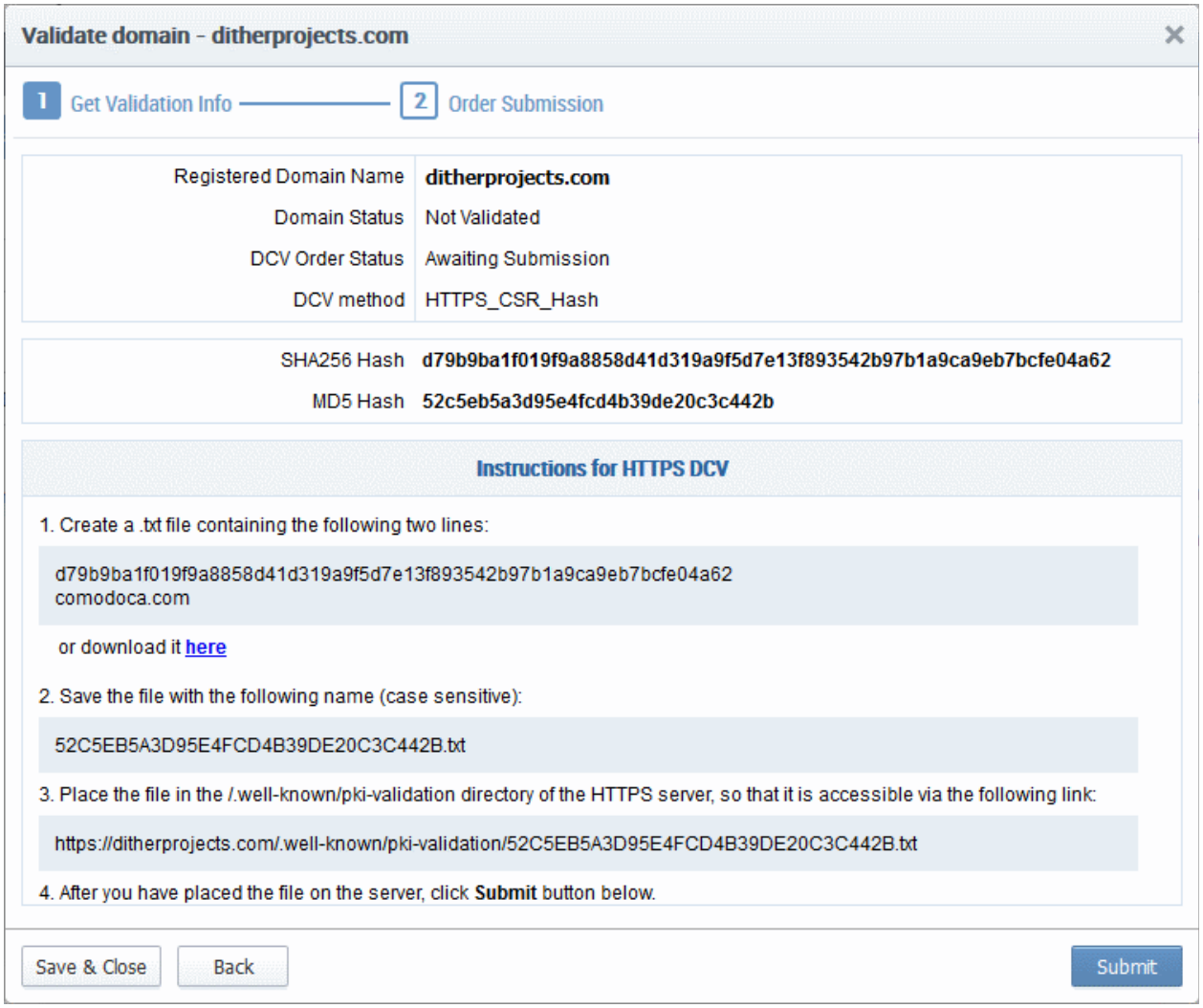


To send the email immediately, you click **Submit** and the DCV order status of the domain changes to Submitted, as shown in the following illustration. To send the email at a later time, click **Save & Close**, in which case, when you restart the DCV process for the domain, the email becomes auto-selected.



Upon receiving the email, the domain administrator should click the validation link in it and enter the validation code in the validation from that appears on clicking the validation link in order to complete the validation process. Once completed, the DCV order status of the domain changes to Validated.

- If you selected **HTTP / HTTPS**, you can proceed to downloading the `.txt` file for sending to the domain administrator. SCM creates a hash value for the `.txt` file and stores it for future reference on validating the domain. The DCV status of the domain changes to Awaiting Submission, as shown in the following illustration.



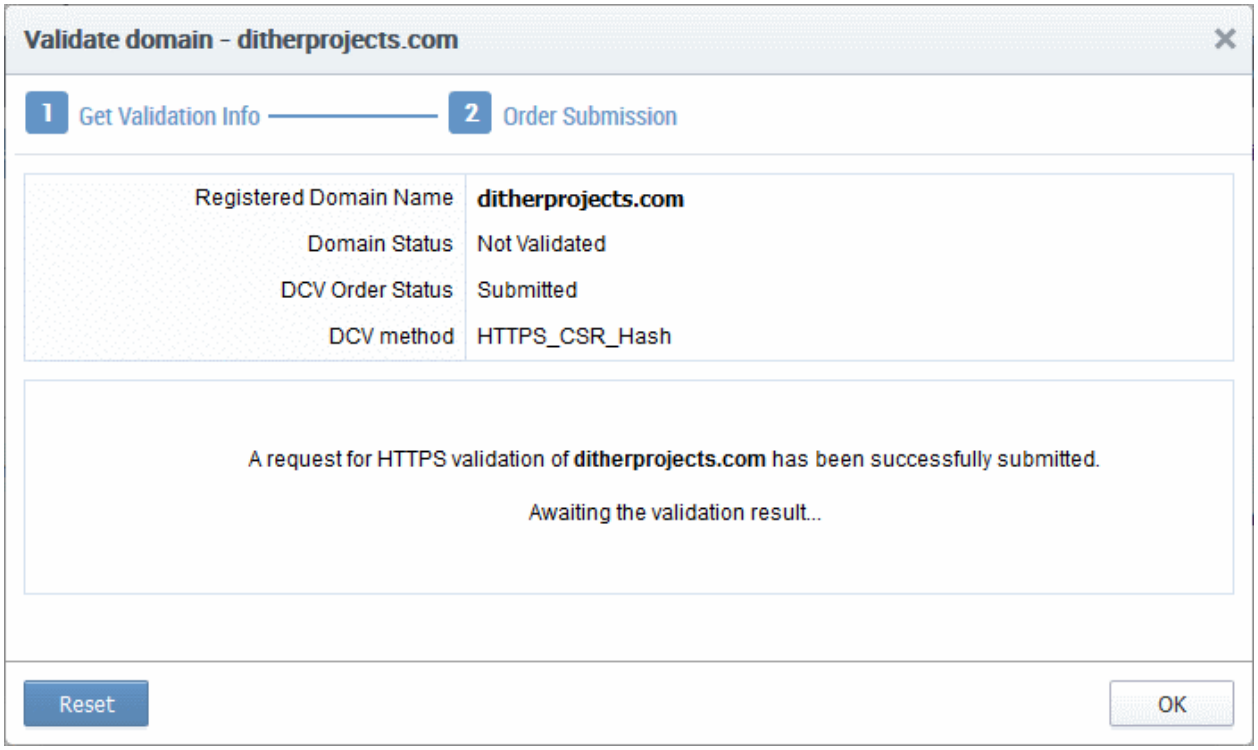
After you click **Download** and save the `.txt` file or create a new notepad file, you copy and paste the string you received and save the file with the name provided to you.

You click **Save & Close** to save the generated hash value for future comparison.

Then you send the `.txt` file to the domain administrator through any out-of-band communication method such as email and request the domain administrator to place the file in the root of the HTTP/HTTPS server, making the file accessible by one of the paths specified.

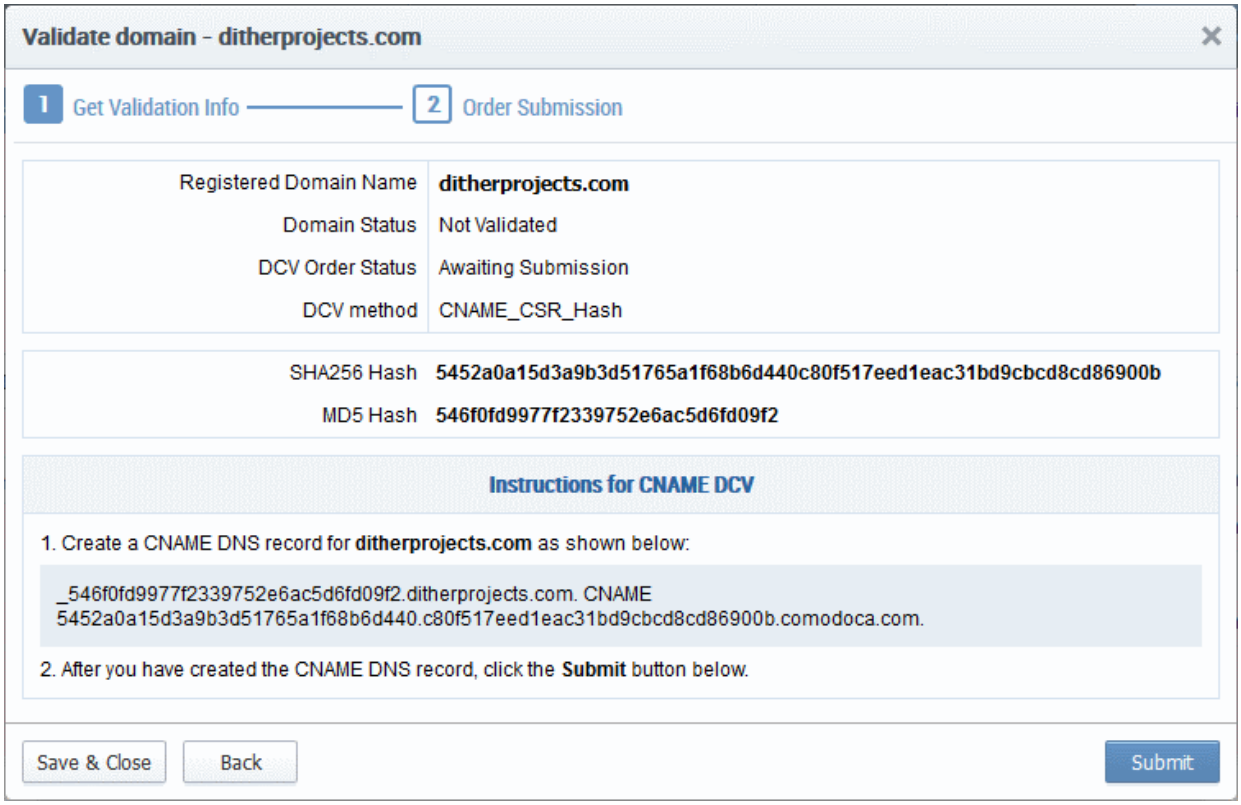
Once the domain administrator has placed the `.txt` file on the HTTP or HTTPS server, open the **DCV** area and resume the DCV process by selecting the domain and clicking **DCV**.

To complete the process, you click **Submit**, after which the DCV order status of the domain changes to Submitted, as shown in the following illustration.



Upon completion, SCM checks whether or not the file has been placed in the web server root and validate the domain. On successful validation, the DCV order status of the domain changes to Validated.

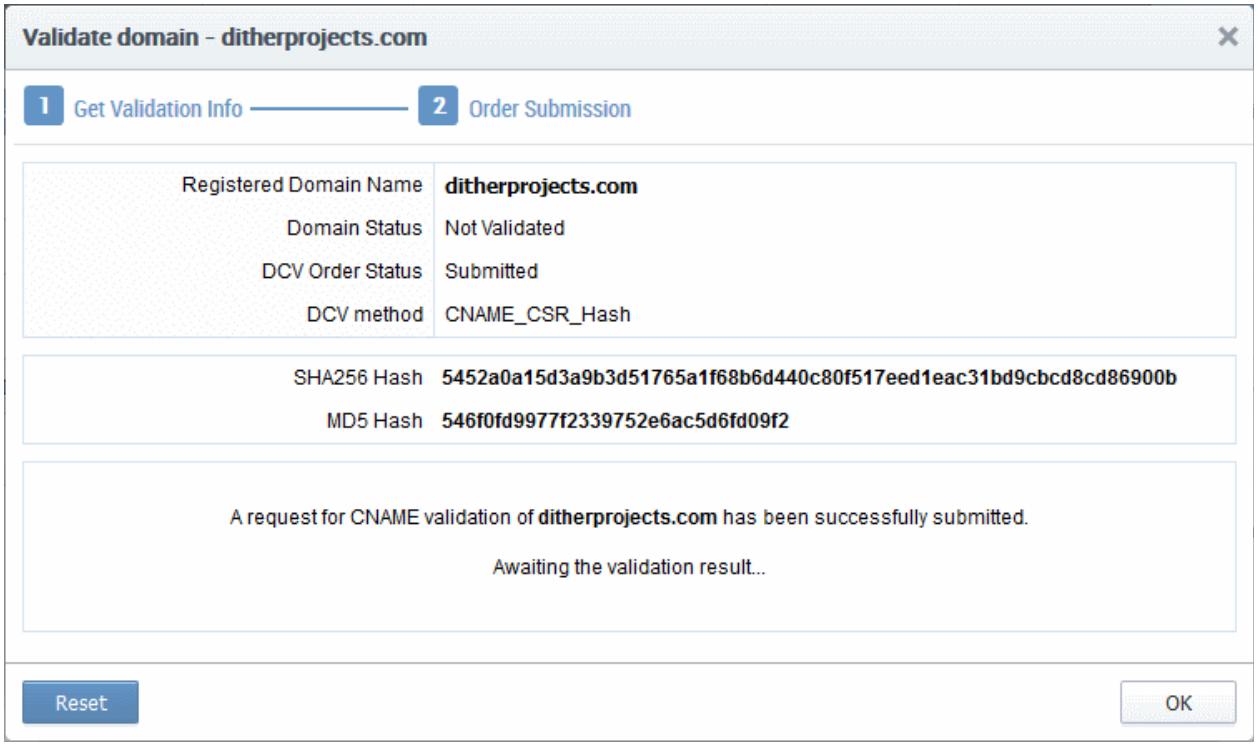
- If you selected **DNS CNAME**, SCM creates a DNS CNAME record for the requested domain and stores its hash value for future reference. You can get the DNS CNAME record for the requested domain. The DCV status of the domain changes to Awaiting Submission, as shown in the following illustration.



After you copy the CNAME DNS record given to you and pass it to the domain administrator through any out-of-band communication method such as email and request the domain administrator to create the record for the domain.

You click **Save & Close** to allow SCM to save the hash value generated for future comparison. After the domain administrator has created the record, you open the **DCV** and resume the DCV process by selecting the domain and clicking the **DCV**.

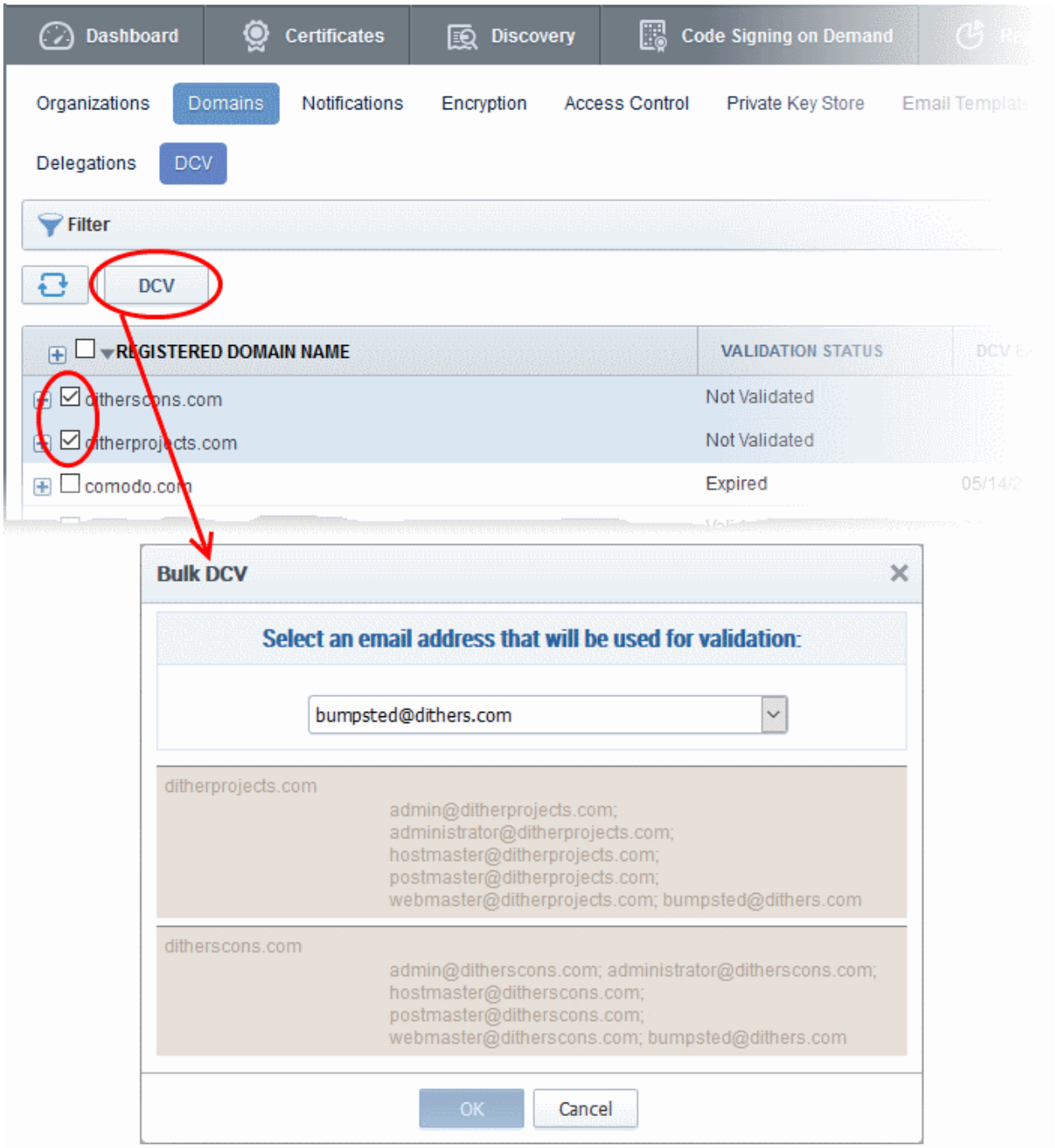
To finish the process, you click **Submit**, upon which the DCV order status of the domain changes to Submitted, as shown in the following illustration.



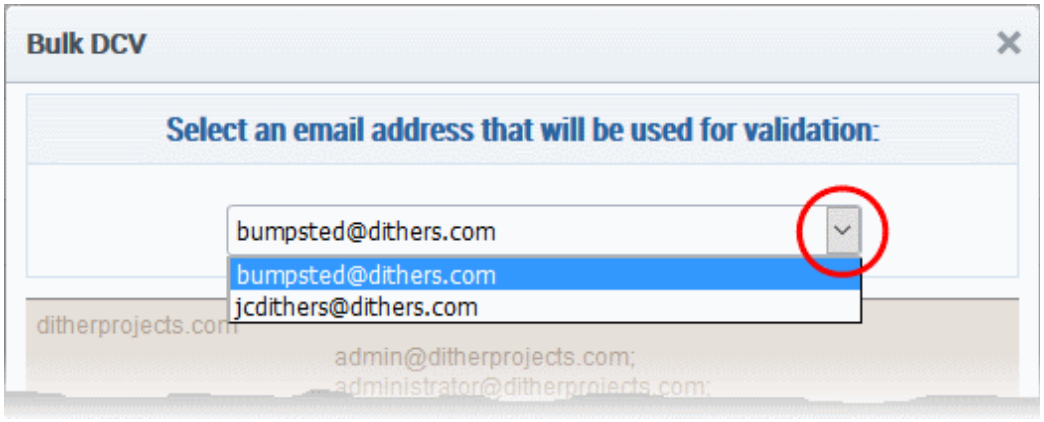
Upon completion, SCM checks whether or not the record has been created. If it is found, the DCV order status of the domain changes to Validated.

To simultaneously initiate validation of multiple domains that share a common domain administrative email account in the WhoIs database, perform this procedure:

- Open the **DCV** area by navigating to **Settings > Domains > DCV**.
- Select the domains that share common domain administrator email address and click **DCV** to open the **Bulk DCV** dialog shown in the following illustration.



The **Bulk DCV** dialog contains lists of possible domain administrator email addresses and the email addresses fetched from the WhoIs database for each domain. Common email addresses identified from the lists are available.



- Proceed by selecting the email address of the administrator who can receive and respond to the validation mail, and then click **OK**.

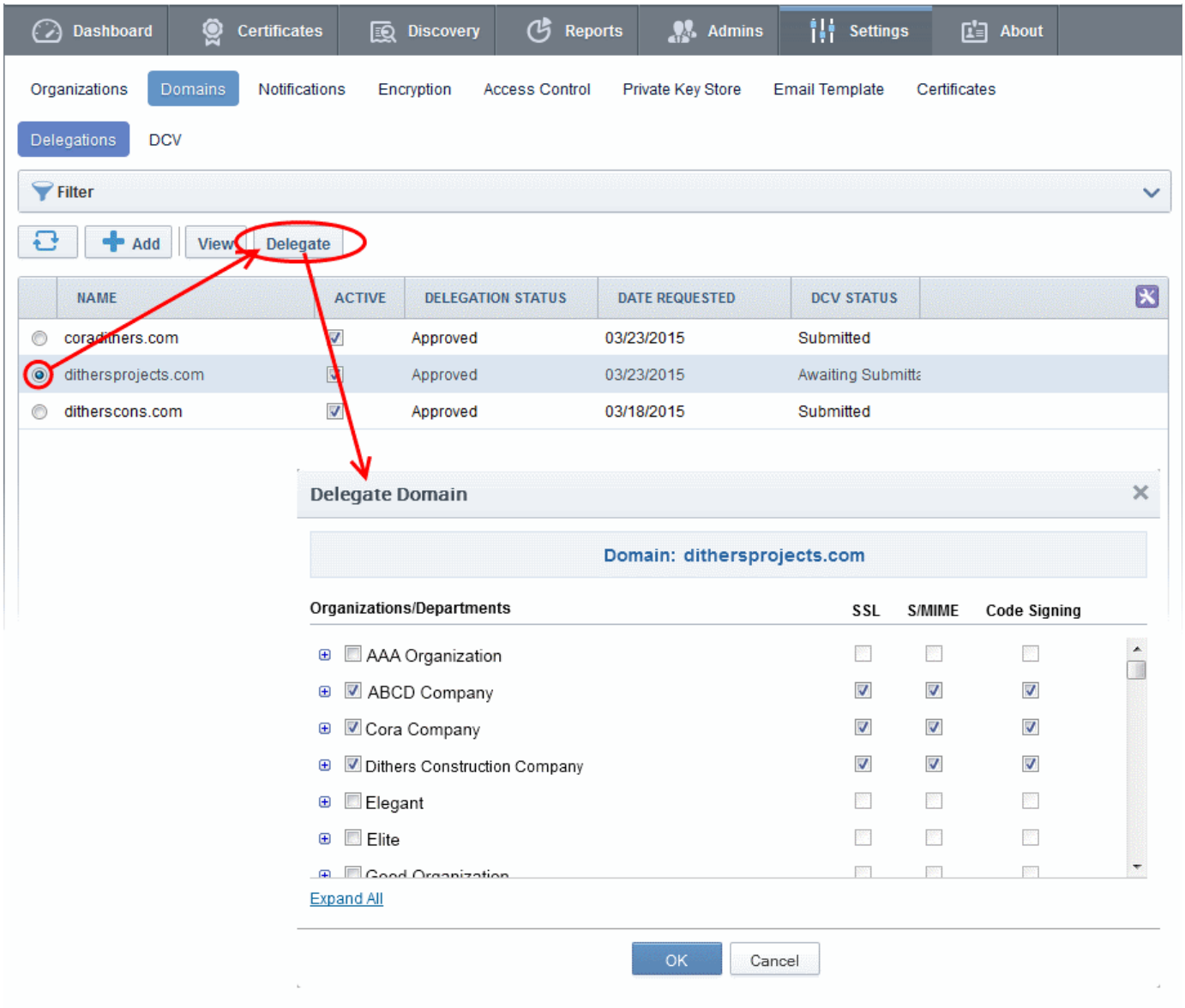
An automated email is sent to the selected domain administrator email address. The DCV order status of the domains changes to Submitted. Upon receiving the email, the domain administrator should click the validation link in it to open the validation form and enter the validation code contained in the email. Once completed, the DCV order status of the domains changes to Validated.

Using the **DCV** area, a MRAO, RAO SSL, and DRAO SSL with appropriate privileges can change the DCV method for the domains whose validation is pending, as follows:

- Open the **DCV** area by navigating to **Settings > Domains > DCV**.
- Click **DCV** located in the row of the domain with the DCV status of Awaiting Submittal or Submitted to start the DCV wizard.
- Click **Back** to move the wizard to the previous step of selecting the DCV method.
- Select the new DCV method and continue the process.

7.4.2.6 Delegating and Redelegating Existing Domains

You can delegate or redelegate the domain to organizations and departments according to the requirement specified in the **Delegate Domain** dialog that you access by navigating to **Settings > Domains > Delegations**, then selecting the domain and clicking **Delegate**, as shown in the following illustration. In addition, the same UI area displays domains that were added by RAO and DRAO administrators without delegating them to any organization or department.



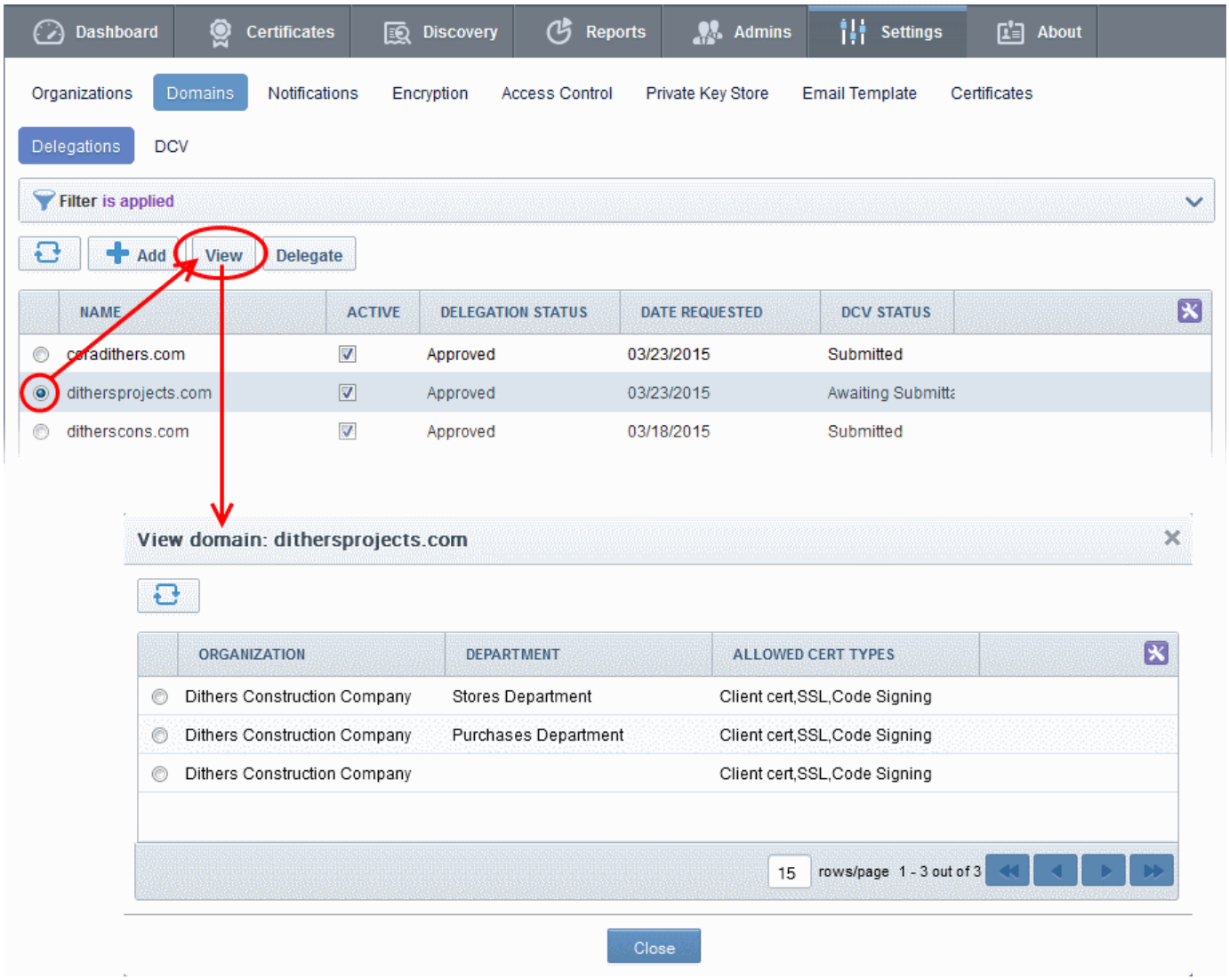
This interface also allows you to do the following:

- Select certificates to be made available for the domain on delegation to the specific organization or department based on purpose of delegating the domain to the organization or department.
- Validate the domain before delegating or redelegating it to specific organization or department by clicking **Validate**, which sends an automated email to the domain control administrator to check the domain control authority.

The domains delegated and redelegated by the MRAO are activated immediately, however the domains delegated by other type of administrators are to be approved by the MRAO in order to become active.

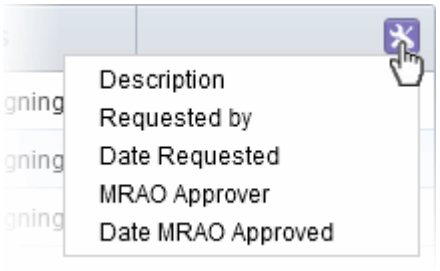
7.4.2.7 Viewing, Validating, and Approving New Domains

Appropriately privileged administrators can view a list of organizations and departments to which a domain has been delegated and for which the certificate types have been enabled. To do this, you select the domain and click **View** to open the **View domain** dialog shown in the following illustration.



The preceding dialog also allows you to view the requisition details of the domain and MRAO to validate and approve the domains created by other administrators. The domain becomes active only after the MRAO approves it and only then it is enabled for request and issuance of SSL certificates, client certificates, and code signing certificates.

The following table summarizes information available in the **View domain** dialog.

Column / Element	Description
Organization	The organization to which the domain has been delegated. The delegations which are pending approval by the MRAO are displayed in red.
Department	The department to which the domain has been delegated. The delegations which are pending approval by the MRAO are displayed in red.
Description	A short description of the domain, as entered by the administrator during creation of the domain.
Requested by	The name of the administrator who created the domain.
Date Requested	The date at which the domain was added to SCM.
MRAO Approver	The name of the MRAO administrator who has approved the creation or delegation of the domain.
Date Approved	The date when the domain was approved by a MRAO.
Allowed Certificate Types	The certificate types that are enabled and available for the domain.
You can use the tool button to select columns to be displayed in the table: 	
Controls	Refresh—Updates the list of displayed organizations and departments and their details.
Delegation Controls [a]	Details—Enables the administrator to view the requisition details of the domain.
	Approve—Enables a MRAO administrator to approve the creation and delegation of the domain by RAO and DRAO administrators. [b]
	Reject—Enables a MRAO administrator to decline the creating and delegation of the domain by RAO and DRAO administrators. [c]

a. Control buttons are visible only on selecting a domain
b. Visible only for domains with Requested status and only to MRAO and RAO administrators.
c. Visible only for domains with Requested status and only to MRAO and RAO administrators.

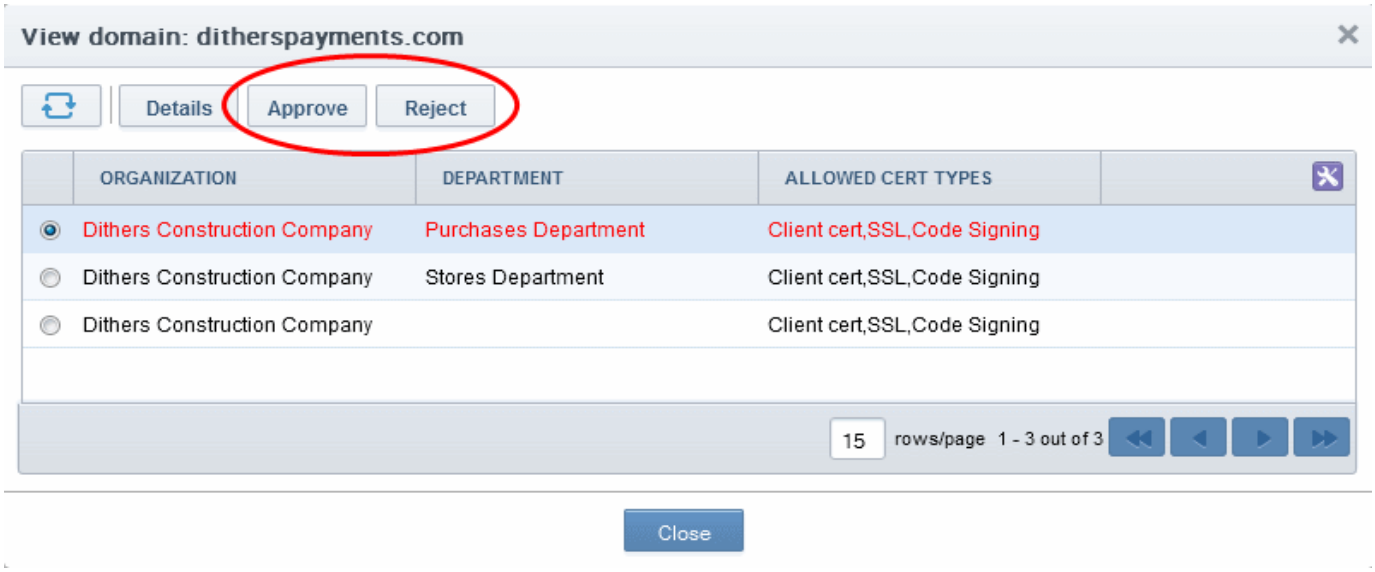
7.4.2.7.1 Approving Creation and Delegation of Domains

The following process typically applies to the domain creation and delegation:

- Domains that are created and delegated by a MRAO are automatically validated and approved.
- Domains that are created and delegated by a RAO are to be validated by the MRAO to become active.
- Domains that are created and delegated by a DRAO are to be first validated and approved by the a RAO of the organization to which the department delegated with the domain belongs, and then by the MRAO to become active.
- Domains which are awaiting approval are displayed in red in the **Domains** area of the SCM UI.
- MRAOs and RAOs can check the validity of the domain and approve or reject the request for the domain.

You can approve or reject a domain delegation as follows:

- Open the **View domain** dialog shown in the following illustration.
- Select the organization or department for which the domain delegation has been requested.
- Click either **Approve** or **Reject**.

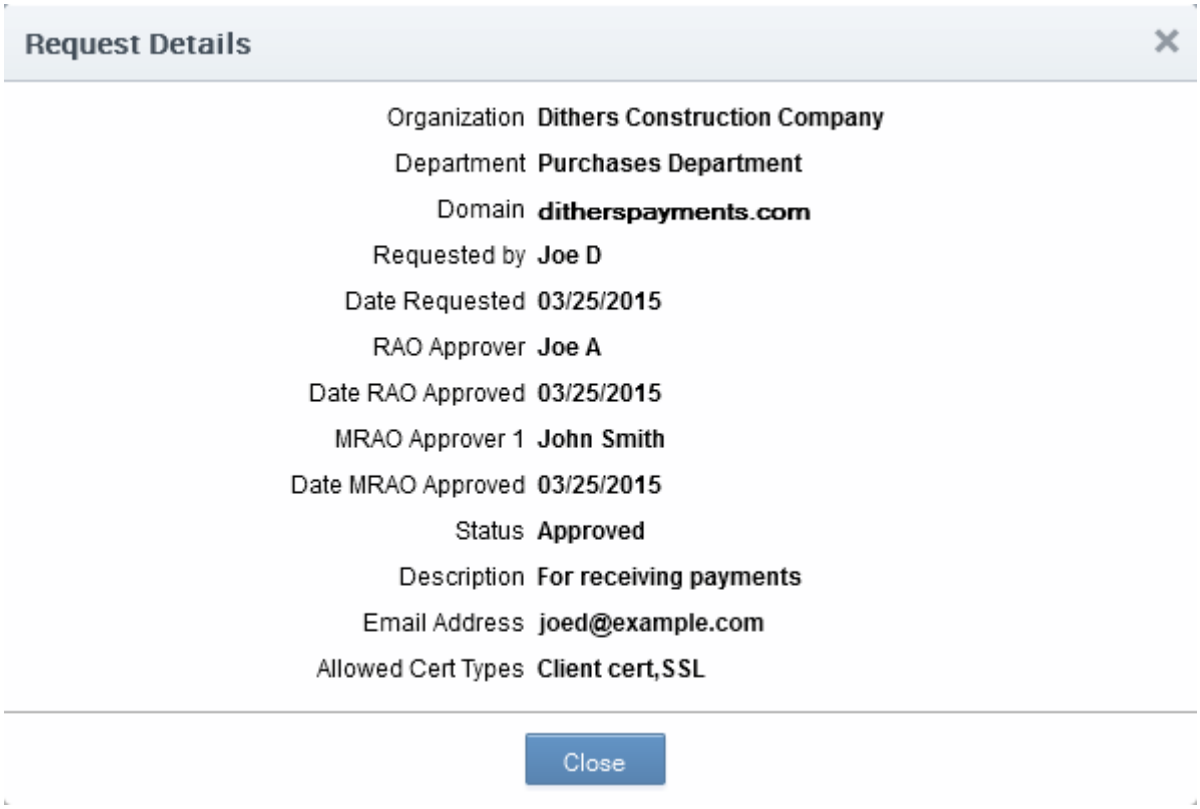


If a domain is created or delegated by a DRAO, it is displayed in red only to the RAO of the organization to which the department belongs, indicating that it is awaiting approval. Once the domain has been validated and approved by the RAO, it becomes visible to the MRAO for validation or approval.

If a domain is created by a RAO, it is displayed in red to the MRAO indicating that this domain is awaiting validation or approval. Once a requested domain is validated and approved by the MRAO, a domain approval notification is sent and the domain is enabled for request and issuance of SSL certificates, client certificates, and code signing certificates.

7.4.2.7.2 Viewing Requisition and Approval Details of a Domain

You can view the request and approval details of the domain delegation by selecting an organization or department and clicking **Details** from the **View domain** dialog, as shown in the following illustration.



The following table lists the details available in the **Request Details** dialog.

Parameter	Description
Organization	The name of the organization to which the domain is delegated.
Department	The name of the department to which the domain is delegated.
Domain	The name of the selected domain.
Requested by	The name of the administrator who has requested for the approval of the delegation of the domain to the organization or department.
Date Requested	The date of requisition for delegation of the domain.
RAO Approver	The name of the RAO SSL administrator who approved the domain, if the domain was requested by a DRAO SSL administrator.
Date RAO Approved	The date when the domain was approved by the RAO SSL administrator.

Parameter	Description
MRAO Approver	The name of the MRAO administrator who approved the domain.
Date MRAO Approved	The date when the domain was approved by the MRAO.
Status	Indicates whether the domain has been approved or awaiting approval for delegation.
State	Indicates whether the domain is active or inactive, as set by the administrator.
Description	A short description for the domain, as entered by the administrator while creating the domain.
E-mail Address	The email address of the administrator who requested the delegation of the domain.
Allowed Certificate Types	The certificate types which could be requested and issued for the domain.

7.5 Configuring Notifications

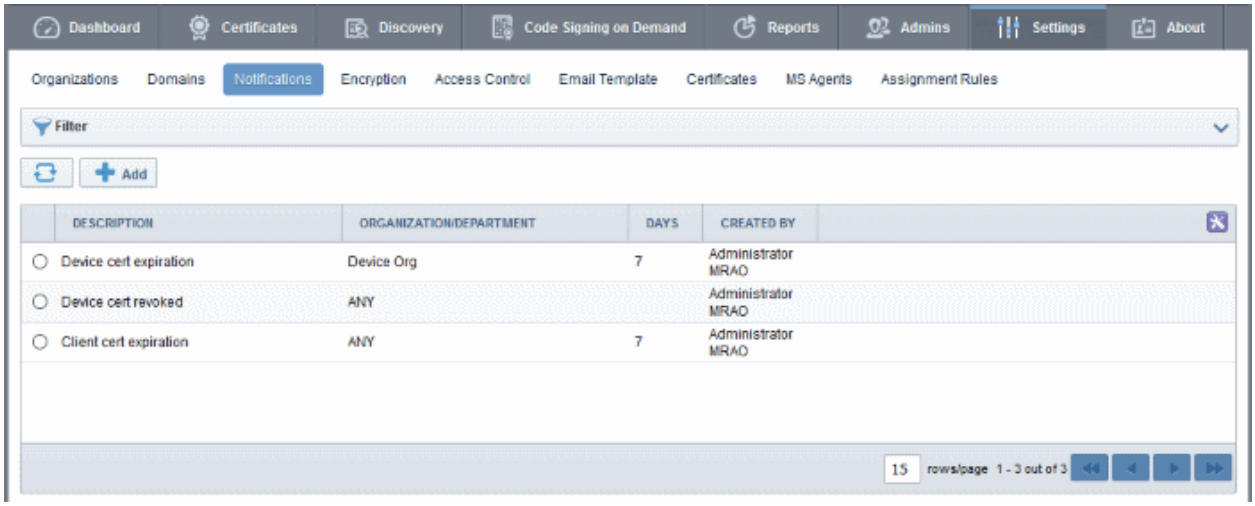
The **Notifications** area shown in the following illustration enables you to define and manage email notifications to various personnel. The notifications include those triggered by events such as requisition, issuance, download, installation, expiry of certificates, requisition, approval and validation of domains and their delegations, creation of administrators, certificate discovery scan reports and so on.

You manage and configure notifications by navigating to **Settings > Notifications** from the main UI.

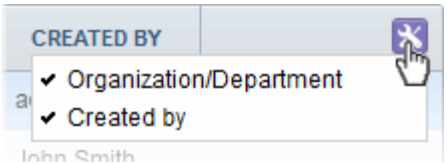
Using this area of the SCM UI, you can also customize the email templates of the notifications. See "Modifying Email Templates" on page 507 for more information.

The level of the notification management depends on your security role, as follows:

- MRAOs can see a list of all notification types specified by all administrator levels, including themselves. They can create new notification types and edit settings for notification for any organization and any department.
- RAOs can only view notification that they specified for end-users belonging the organizations and departments delegated to them. They can create and manage notifications only for the notification types for which they have authority, and only for the organizations and departments delegated to them.
- DRAOs can view the notifications specified for the users belonging to departments delegated to these administrators. They can create and manage notifications only for the notification types for which they have authority, and only for the departments delegated to them.



The following table lists settings and elements of the **Notifications** area.

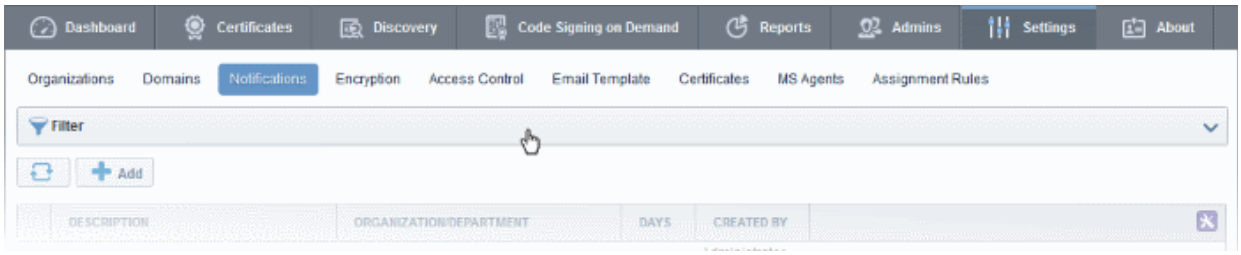
Column / Element	Description
Description	A short description for the notification, as entered by the administrator during creation.
Organization/Department	The organizations and departments for which the notification was created. The notification mails are sent only to administrators of these organizations and departments.
Days	The number of days in advance of the event the notification is sent.
Created by	The name of the administrator who created the notification.
You can use the tool button to select columns to be displayed in the table: 	
Controls	Add—Adds a new notification.
	Refresh—Updates the list of displayed notifications.
Notification Controls [a] [b]	Edit—Enables you to edit the notification.
	Delete—Deletes the notification.

a. Visible only on selecting a notification.
b. You can edit or delete an existing notification when all of the following conditions are met: (1) You have authority for all of the organizations and departments contained within the scope of the notification. (2) You have authority for the notification type. (3) The creator of the notification is of the same or lower administrative level than that of the administrator.

7.5.1 How to Sort and Filter Notifications

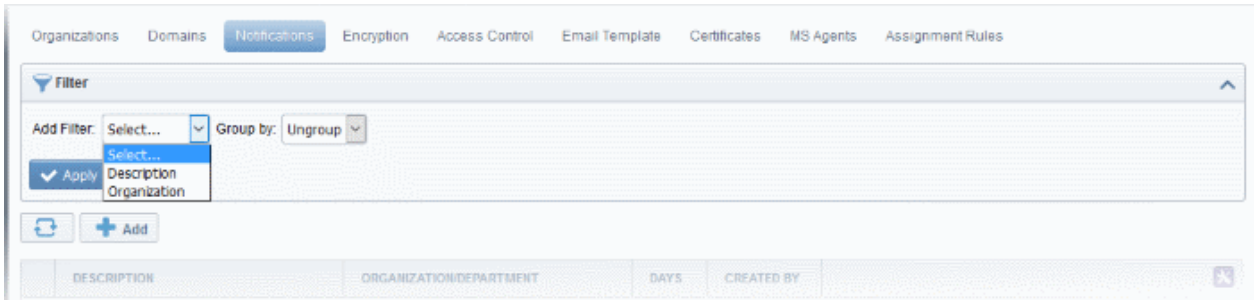
You can sort items in the alphabetical order by clicking a column header, and you can use filters to search for particular domains.

You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.

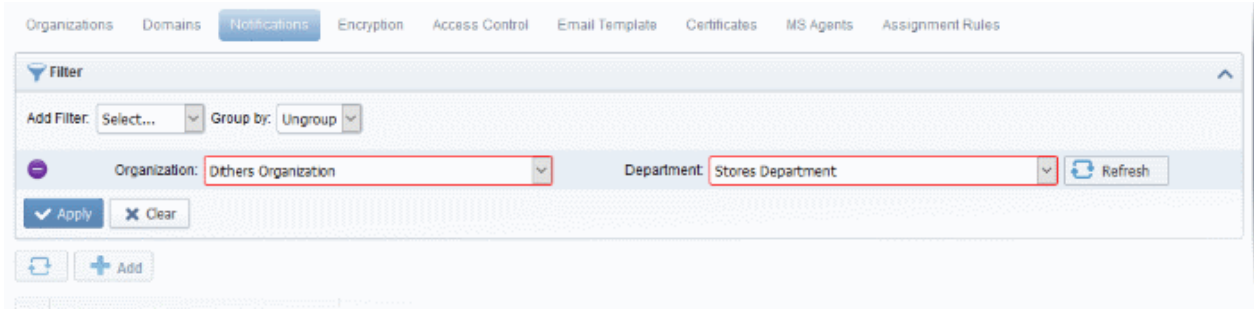


To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection from the **Add Filter** list.

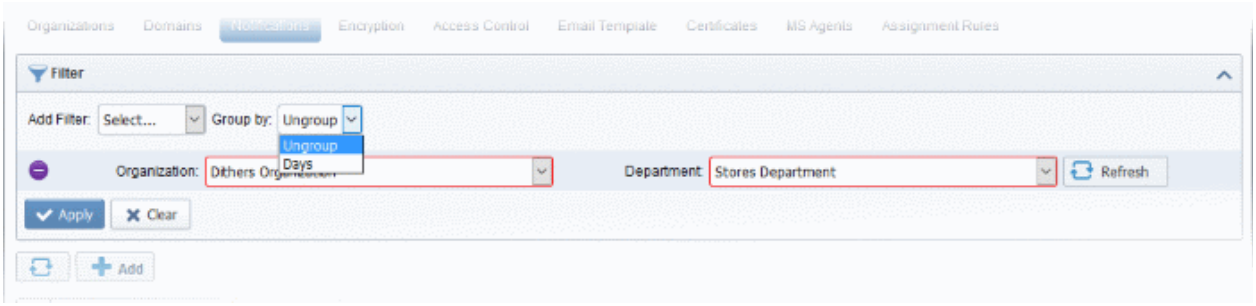
For example, if you want to filter the notification type set for an organization or department, select Organization from the **Add Filter** list.



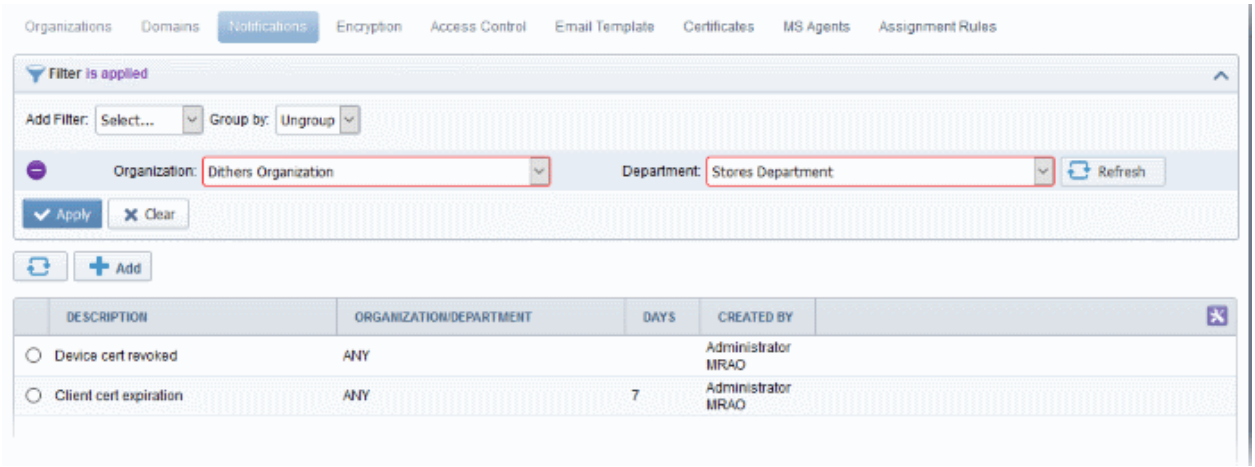
Then select a specific organization and department from the **Organization** and **Department** lists, as shown in the following illustration.



To group the results based on the days parameter, select Days from the **Group by** list, and click **Apply**.



The filtered items based on the selected parameters are displayed, as shown in the following illustration.

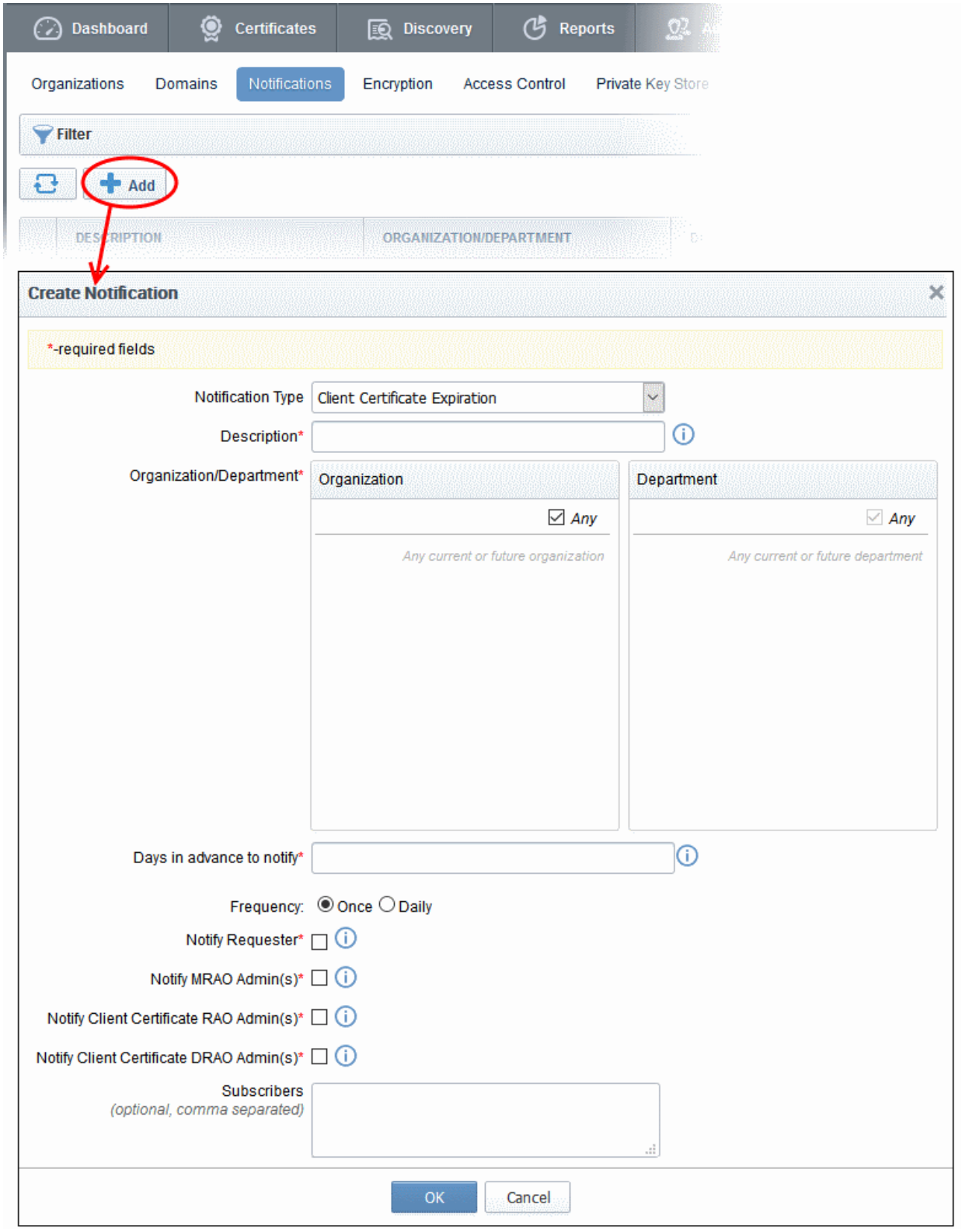


You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **Notifications** screen, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

7.5.2 How to Add Notifications

You can add a new notification by clicking **Add** in the **Notifications** area, and then filling out the **Create Notification** dialog shown in the following illustration.

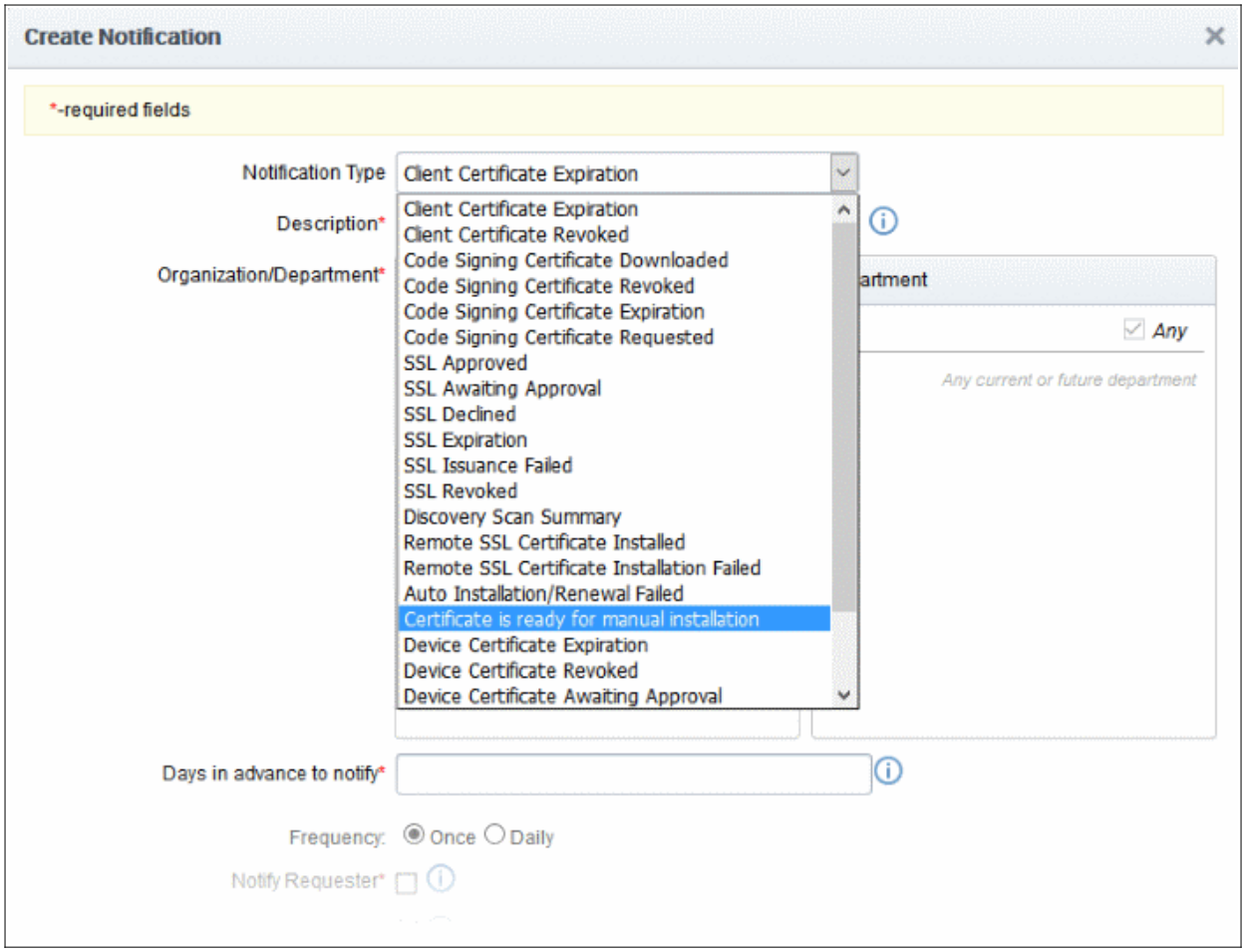


When adding a notification, you must first select its type.

There are several types of notifications available for selection, as shown in the following illustration. The list of notification types depends on your role as an administrator. For example, RAO SSL and DRAO SSL administrators can see the options corresponding only to SSL certificates.

You can create notifications in accordance with the permissions enabled for your account and the administrative roles assigned to you.

Similarly, you can view existing notifications for any of the organizations or departments contained within scope of the notification that have been delegated to you under the appropriate certificate type. In addition, you have to have authority for the notification type.



The following table summarizes the notification types that are available for you based on your administrative role.

Notification	Certificate Type	Administrator
Client Certificate Expiration	Client Certificate	MRAO, RAO Client Certificate, DRAO Client Certificate

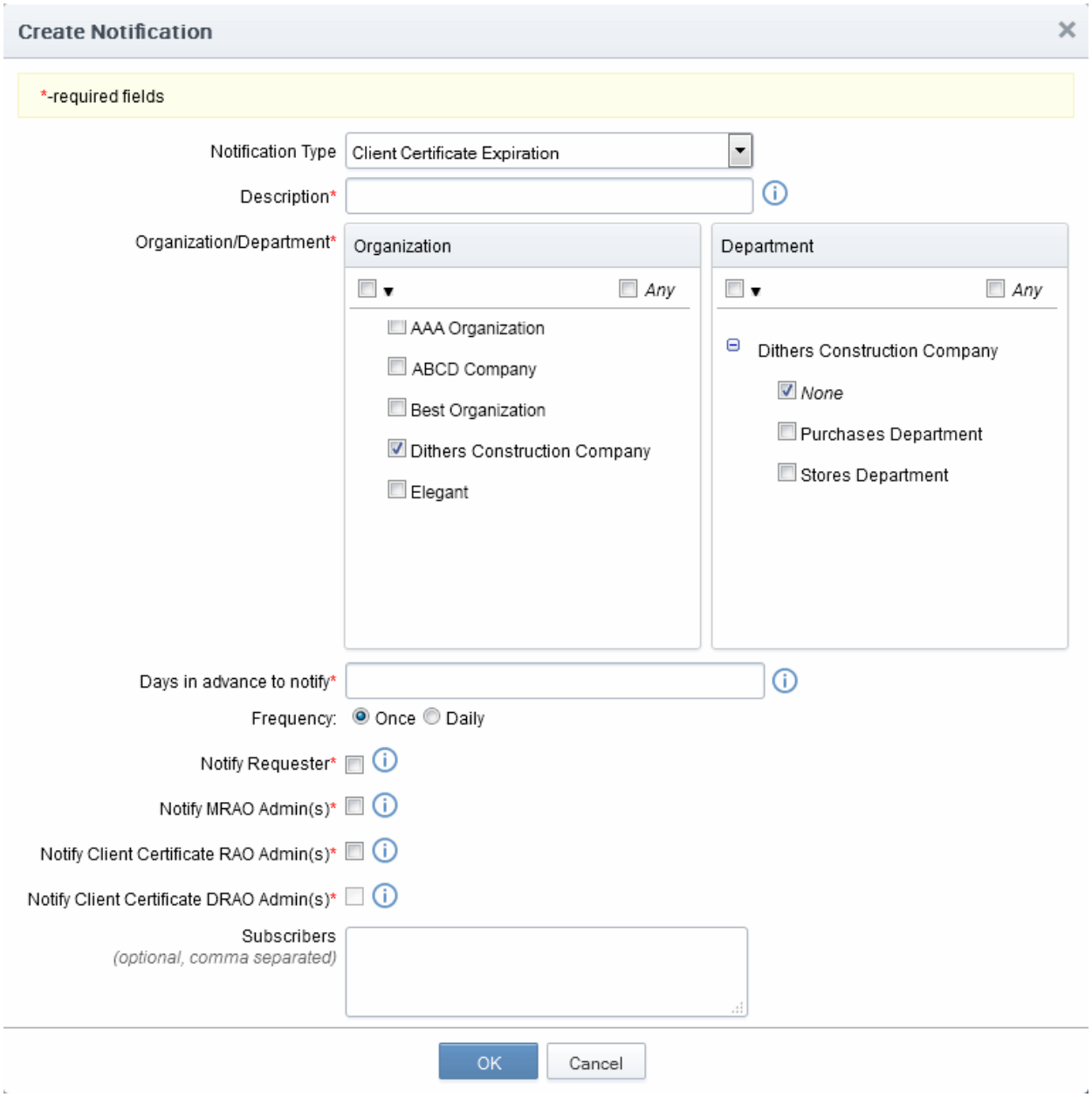
Notification	Certificate Type	Administrator
Client Certificate Revoked	Client Certificate	MRAO, RAO Client Certificate, DRAO Client Certificate
Client Certificate Enrolled (DL)	Client Certificate	MRAO, RAO Client Certificate, DRAO Client Certificate
Code Signing Certificate Downloaded	Code Signing Certificate	MRAO, RAO Code Signing, DRAO Code Signing
Code Signing Certificate Revoked	Code Signing Certificate	MRAO, RAO Code Signing, DRAO Code Signing
Code Signing Certificate Expiration	Code Signing Certificate	MRAO, RAO Code Signing, DRAO Code Signing
Code Signing Certificate Requested	Code Signing Certificate	MRAO, RAO Code Signing, DRAO Code Signing
Code Signing Certificate Enrolled (DL)	Code Signing Certificate	MRAO, RAO Code Signing, DRAO Code Signing
SSL Approved	SSL Certificate	MRAO, RAO SSL, DRAO SSL
SSL Awaiting Approval	SSL Certificate	MRAO, RAO SSL, DRAO SSL
SSL Declined	SSL Certificate	MRAO, RAO SSL, DRAO SSL
SSL Expiration	SSL Certificate	MRAO, RAO SSL, DRAO SSL
SSL Issuance Failed	SSL Certificate	MRAO, RAO SSL, DRAO SSL
SSL Revoked	SSL Certificate	MRAO, RAO SSL, DRAO SSL
Discovery Scan Summary	Other	All
Remote SSL Certificate Installed	SSL Certificate	MRAO, RAO SSL, DRAO SSL
Remote SSL Certificate Installation Failed	SSL Certificate	MRAO, RAO SSL, DRAO SSL
Auto-Installation/Renewal Failed	SSL Certificate	MRAO, RAO SSL, DRAO SSL
Certificate Ready for Manual Installation	SSL Certificate	MRAO, RAO SSL, DRAO SSL
SSL Enrolled (DL)	SSL Certificate	MRAO, RAO SSL, DRAO SSL
Device Certificate Expiration	Device Authentication Certificate	MRAO, RAO Device Certificate, DRAO Device Certificate

Notification	Certificate Type	Administrator
Device Certificate Revoked	Device Authentication Certificate	MRAO, RAO Device Certificate, DRAO Device Certificate
Device Certificate Awaiting Approval	Device Authentication Certificate	MRAO, RAO Device Certificate, DRAO Device Certificate
Device Certificate Approved	Device Authentication Certificate	MRAO, RAO Device Certificate, DRAO Device Certificate
Device Certificate Declined	Device Authentication Certificate	MRAO, RAO Device Certificate, DRAO Device Certificate
Device Certificate Enrolled (DL)	Device Authentication Certificate	MRAO, RAO Device Certificate, DRAO Device Certificate
Client Admin Creation	Other	All
Domain Awaiting Approval	Other	All
Domain Approved	Other	All
DCV Expiration	Domain Control Validation	MRAO, RAO SSL, DRAO SSL
DCV Validated	Domain Control Validation	MRAO, RAO SSL, DRAO SSL
DCV Needed-New Domain	Domain Control Validation	MRAO, RAO SSL, DRAO SSL
Code Sign Request Created	Code Signing	MRAO, RAO Code Signing
Code Signing CSoD Revoked	Code Signing	MRAO, RAO Code Signing

NOTE: The notification types related to DCV are available only if the DCV feature is enabled for your account.

7.5.3 How to Create Notifications About Expiration of Client Certificates

You can communicate the terms of expiration of client certificates by selecting the **Client Certificate Expiration** notifications type in the **Create Notification** dialog, as shown in the following illustration.



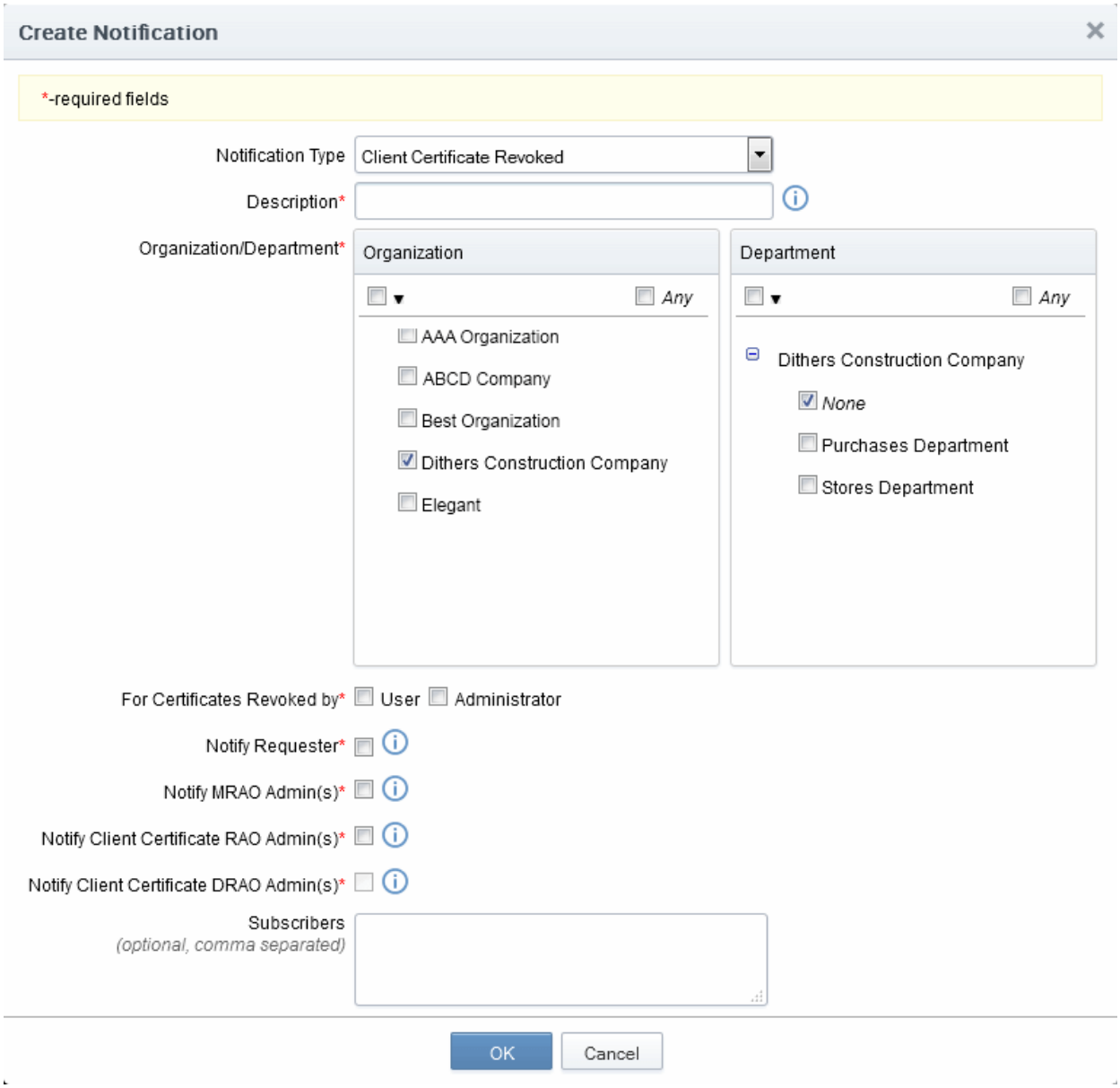
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization/Department	The organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Days in advance to notify	Information about the number of days the end-user is to be notified about expiration of the certificate before the event. You can also specify whether the notification has to be sent to the members once or daily until the expiration date.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify Client Certificate RAO Admins	Enables you to send the notification for RAO Client Certificate administrators of the organization.
Notify Client Certificate DRAO Admins	Enables you to send the notification to DRAO Client Certificate administrators of the department.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.4 How to Create Notifications About Revocation of Client Certificates

You can notify specific personnel about revocation of a client certificate by selecting the **Client Certificated Revoked** notification type in the **Create Notification** dialog, as shown in the following illustration.



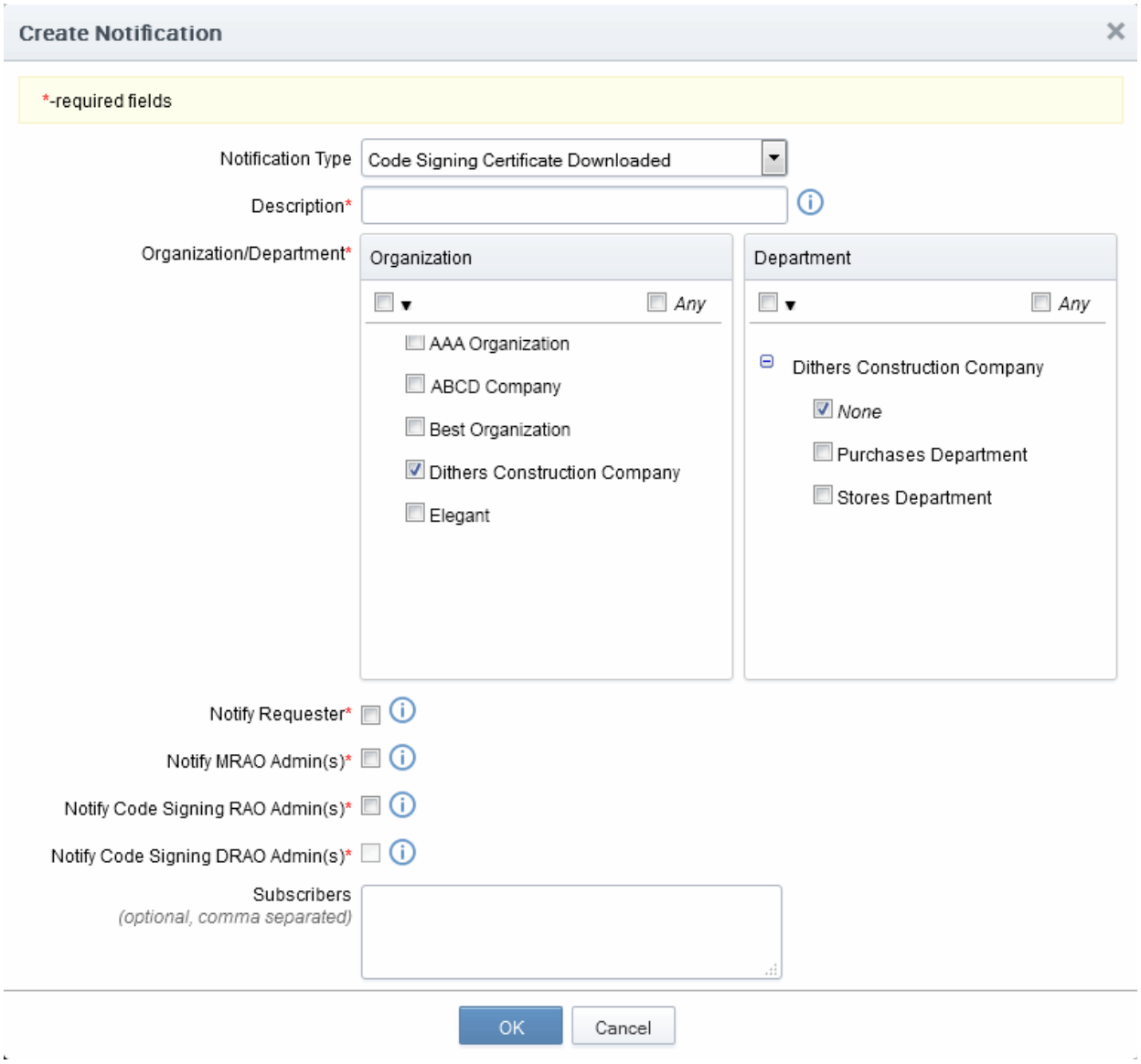
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization/Department	The organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.

Field / Element	Description
For Certificates Revoked by	A person (administrator or end-user) whose revoke action is to trigger notification.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify Client Certificate RAO Admins	Enables you to send the notification to RAO Client Certificate administrators of the organization.
Notify Client Certificate DRAO Admins	Enables you to send the notification to DRAO Client Certificate administrators of the department.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.5 How to Create Notifications About the Code Signing Certificate Download

You can notify specific personnel about the fact that a code signing certificate has been downloaded by the administrator. To do so, you select the **Code Signing Certificated Downloaded** notification type in the **Create Notification** dialog, as shown in the following illustration.



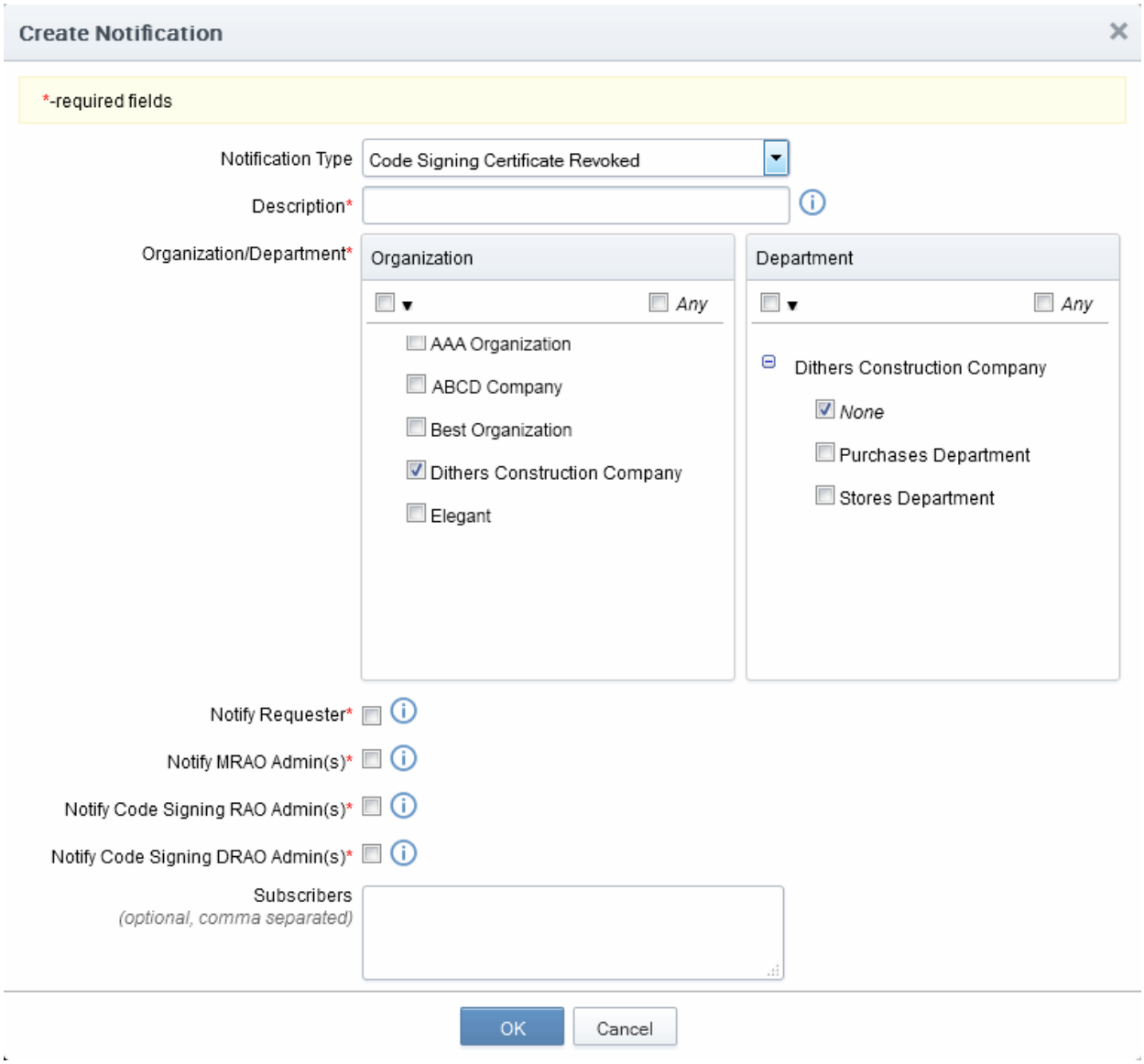
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization/Department	The organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.

Field / Element	Description
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify Code Signing RAO Admins	Enables you to send the notification to RAO Code Signing administrators of the selected organization or departments.
Notify Code Signing DRAO Admins	Enables you to send the notification to DRAO Code Signing administrators of the selected department.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.6 How to Create Notifications About Revocation of Code Signing Certificates

You can notify specific personnel about revocation of a code signing certificate. To do so, select the **Code Signing Certificated Revoked** notification type in the **Create Notification** dialog, as shown in the following illustration.



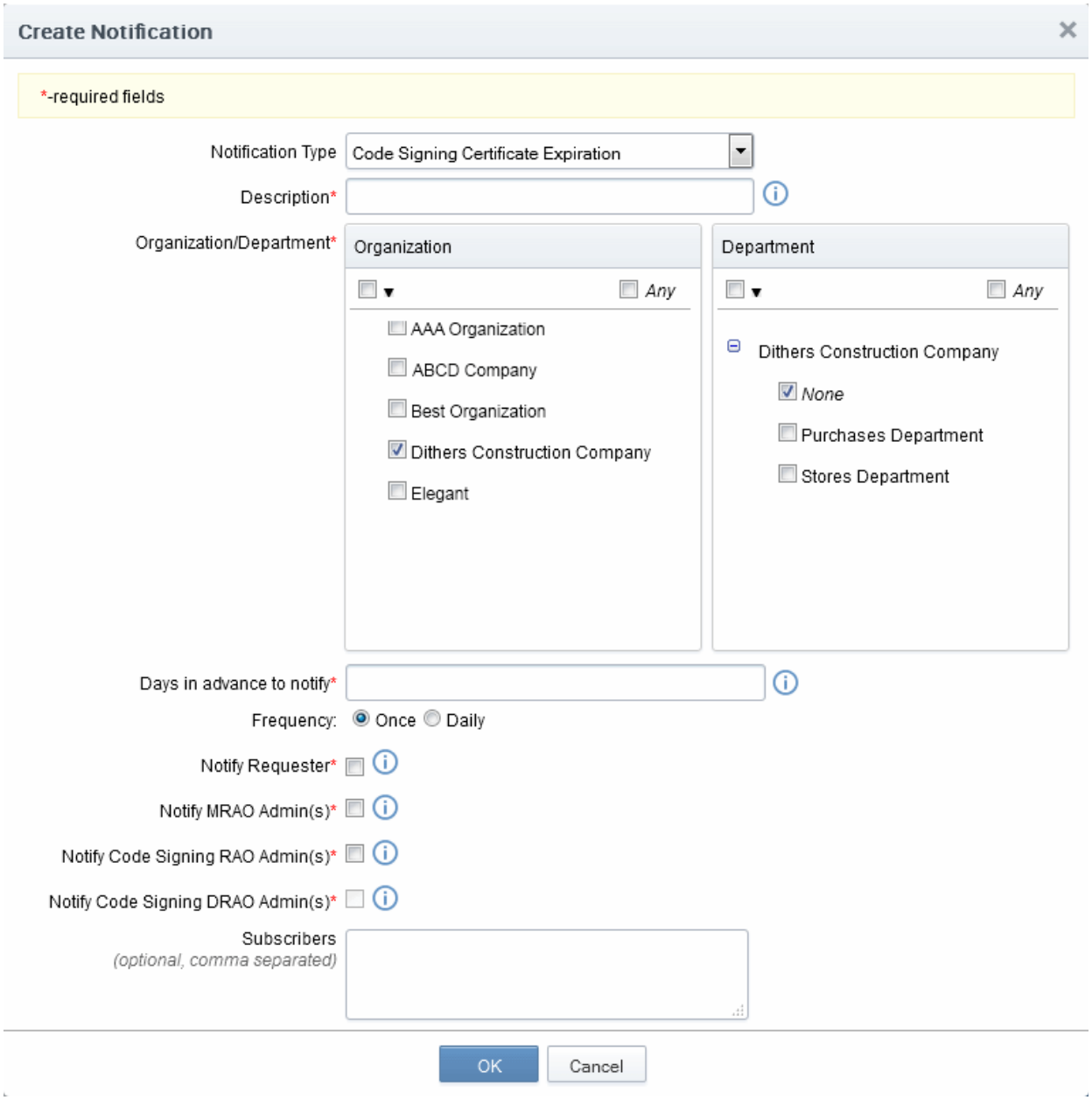
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization/Department	The organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.

Field / Element	Description
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify Code Signing RAO Admins	Enables you to send a notification to RAO Code Signing administrators of the organizations or departments.
Notify Code Signing DRAO Admins	Enables you to send a notification to DRAO Code Signing administrators of the departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.7 How to Create Notifications About Expiration of Code Signing Certificates

You communicate to the affected personnel the details of expiration of code signing certificates by selecting the **Code Signing Certificate Expiration** notification type in the **Create Notification** dialog, as shown in the following illustration.



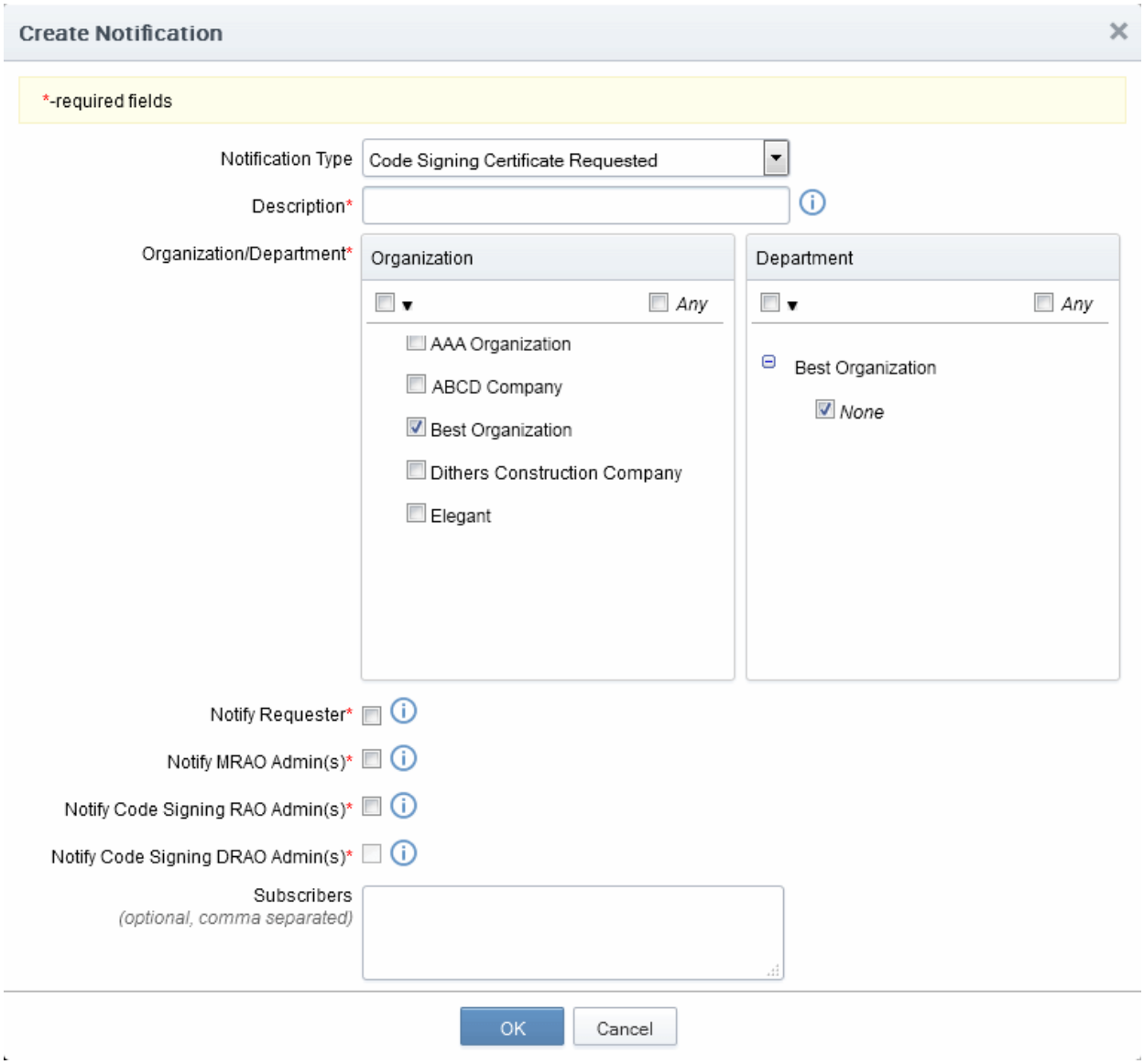
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization/Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Days in advance to notify	Information about the number of days the end-user is to be notified about expiration of the certificate before the event. You can also specify whether the notification has to be sent to the members once or daily until the expiration date.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify Code Signing RAO Admins	Enables you to send the notification to RAO Code Signing administrators of the selected organization or departments.
Notify Code Signing DRAO Admins	Enables you to send the notification to DRAO Code Signing administrators of the selected department.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.8 How to Create Notifications About a Request for a Code Signing Certificate

You communicate to specified personnel the fact that a request for a code signing certificate was submitted by the administrator on their behalf. You do so by selecting the **Code Signing Certificated Requested** notification type in the **Create Notification** dialog, as shown in the following illustration.



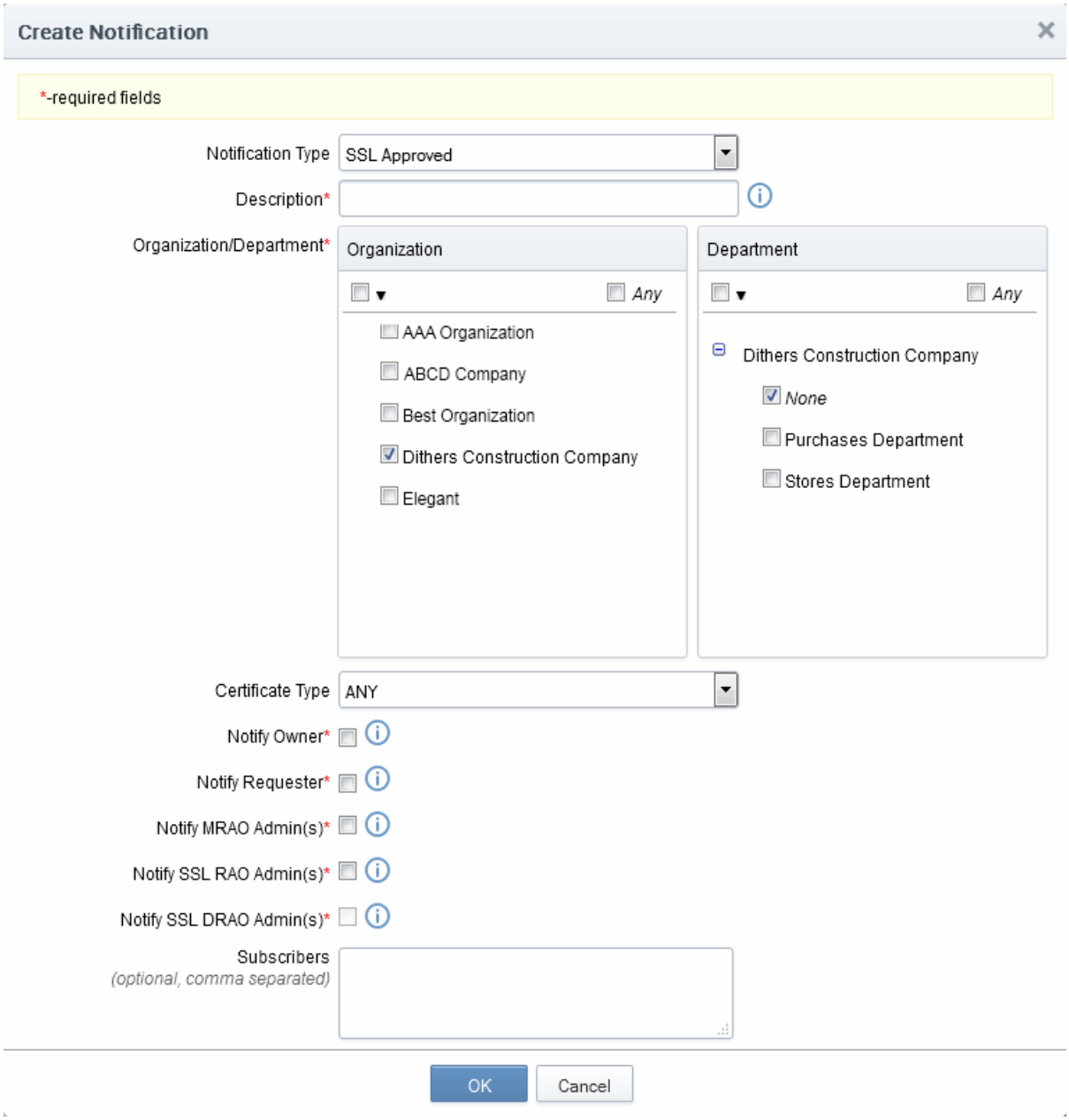
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization/Department	The organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.

Field / Element	Description
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify Code Signing RAO Admins	Enables you to send the notification to RAO Code Signing administrators of the selected organizations or departments.
Notify Code Signing DRAO Admins	Enables you to send the notification to DRAO Code Signing administrators of the selected department.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.9 How to Create Notifications About the SSL Certificate Approval

You communicate to specified personnel the fact that a request for an SSL certificate was approved by the administrator. You do so by selecting the **SSL Approved** notification type in the **Create Notification** dialog, as shown in the following illustration.



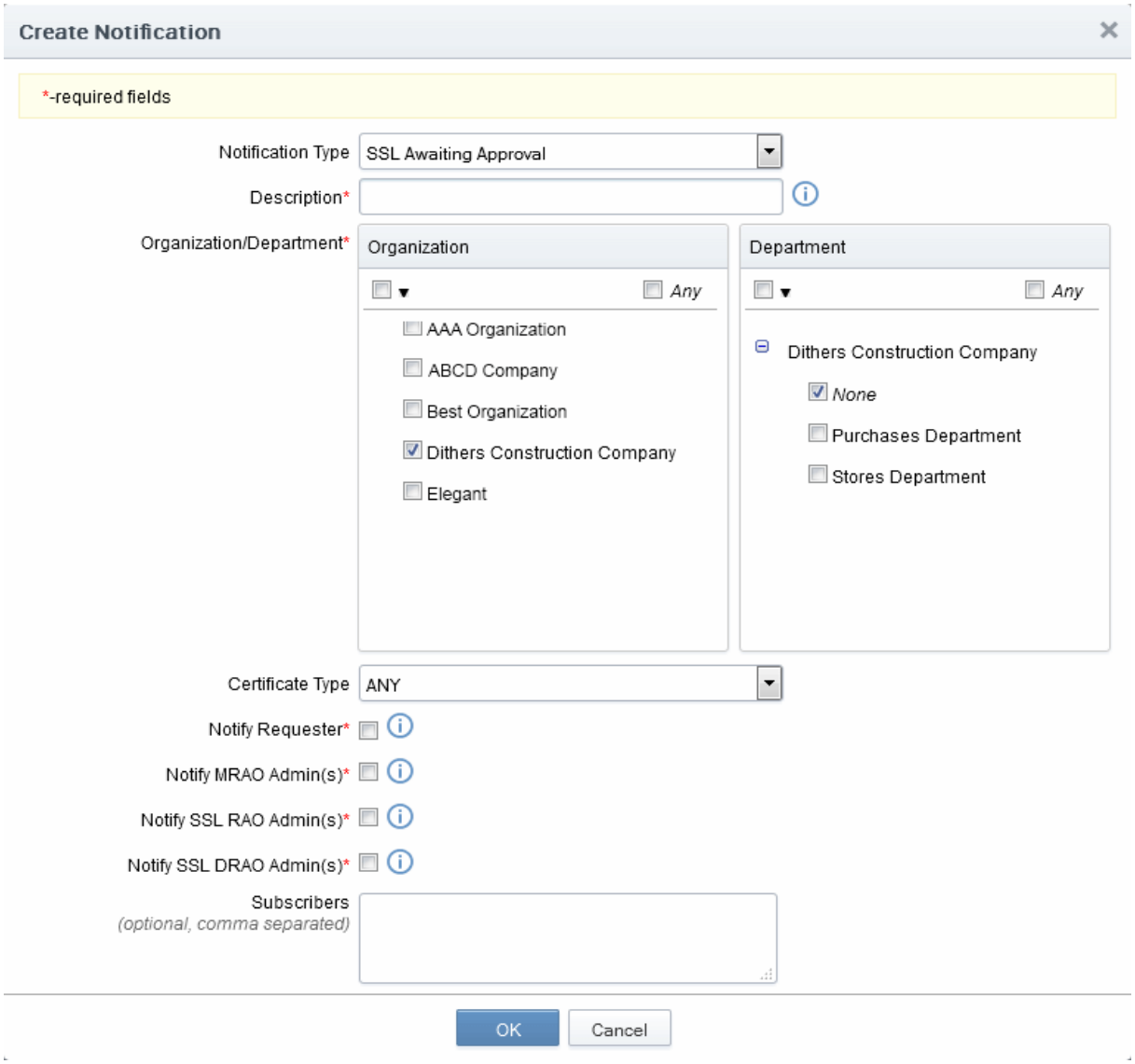
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization/Department	The organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Certificate Type	The type of SSL certificate for which the notification is to be set.
Notify Owner	Enables you to send the notification for the owner of the certificate, who is typically the Administrator that first approved the request for the certificate.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admin	Enables you to send the notification to MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification for DRAO SSL administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.10 How to Create Notifications About the SSL Certificate Waiting for Approval

Each SSL certificate request must be approved by the administrator. Before the request is approved, its status is Awaiting Approval. You can communicate the status of an SSL certificate after the certificate was requested by selecting the **SSL Awaiting Approval** notification type in the **Create Notification** dialog, as shown in the following illustration.



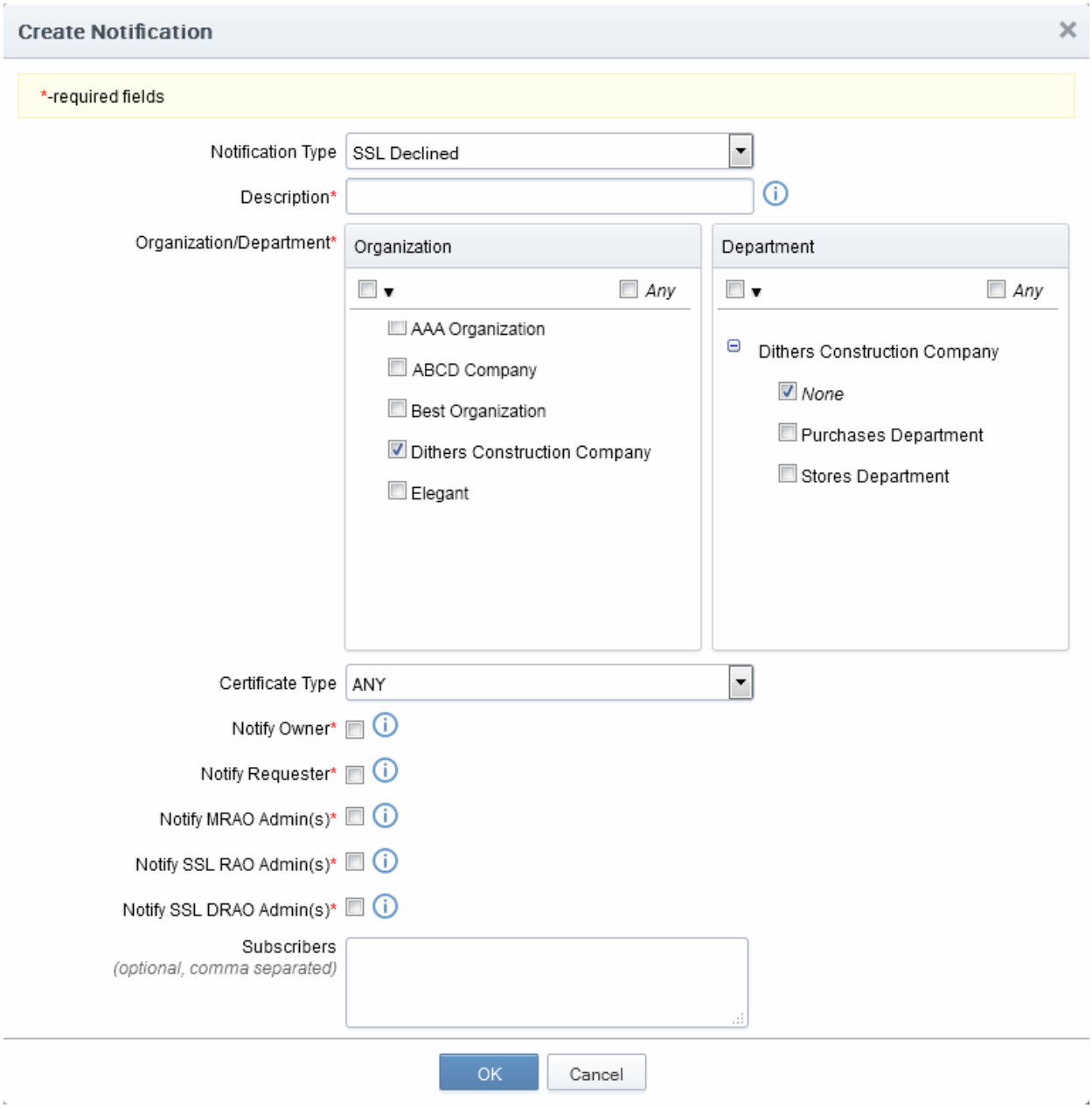
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization/Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Certificate Type	The type of SSL certificate for which the notification is to be set.

Field / Element	Description
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify SSL RAO Admins	Enables you to send a notification to RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to DRAO SSL administrators of the selected departments.

7.5.11 How to Create Notifications About a Declined Request for an SSL Certificate

You can communicate to specified personnel the fact that a request for an SSL certificate was declined by the administrator. You do so by selecting the **SSL Declined** notification type in the **Create Notification** dialog, as shown in the following illustration.



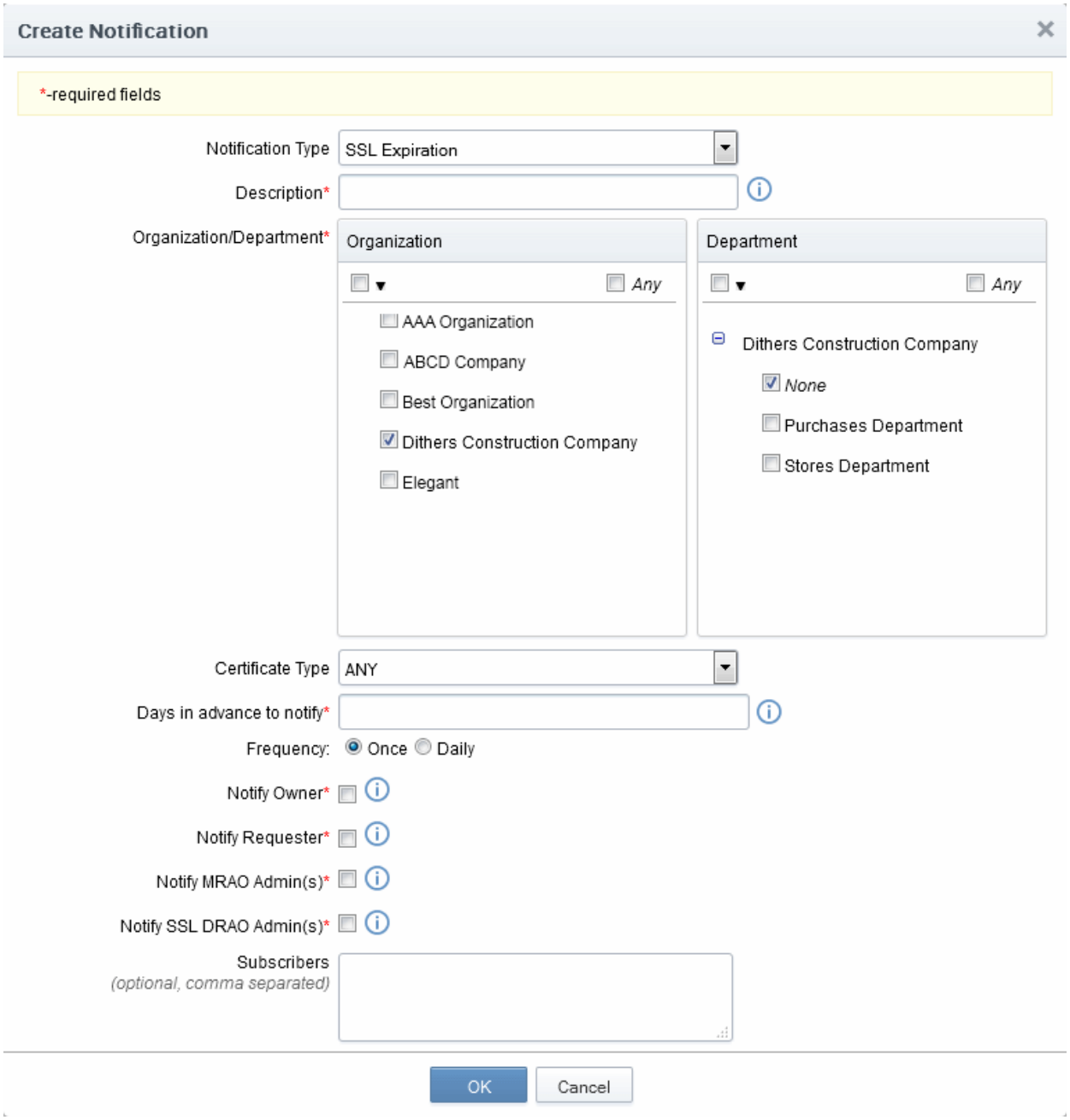
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization/Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Certificate Type	The type of SSL certificate for which the notification is to be set.
Notify Owner	Enables you to send the notification for the owner of the certificate, who is typically the Administrator that first approved the request for the certificate.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to DRAO SSL administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.12 How to Create Notifications About Expiration of SSL Certificates

You can notify specified personnel of the fact that their SSL certificate is due to expire. This should be done in advance. You do so by selecting the **SSL Expiration** notification type in the **Create Notification** dialog, as shown in the following illustration.



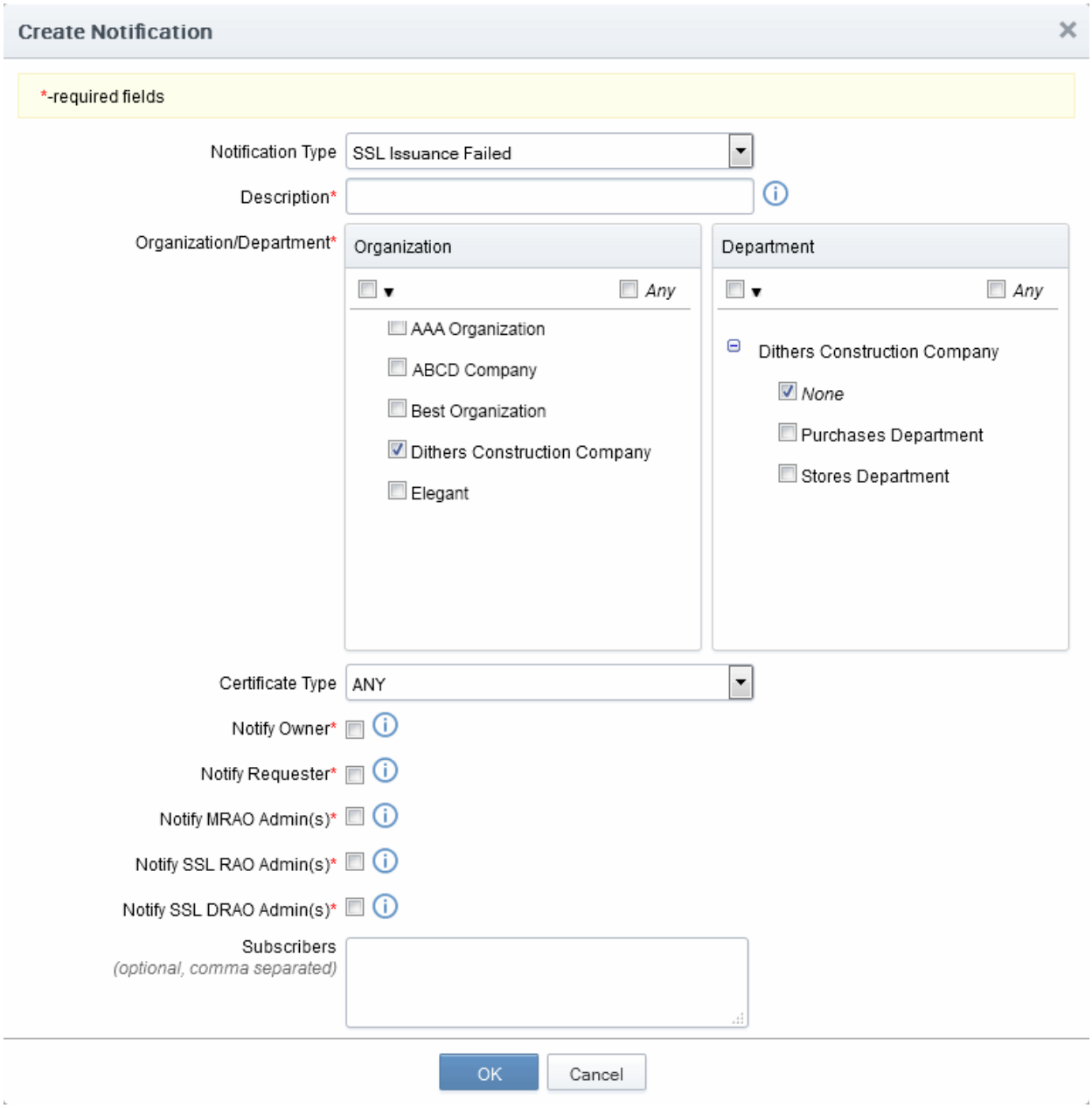
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization/Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Certificate Type	The type of SSL certificate for which the notification is to be set.
Days in advance to notify	The number of days before the expiration date the notification is to be sent about expiration of the certificate. You can also specify whether the notification has to be sent only once or daily until the expiration date.
Notify Owner	Enables you to send the notification for the owner of the certificate.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to DRAO SSL administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.13 How to Create Notifications About Failed Attempts to Issue SSL Certificates

You can notify specified personnel of the fact that an SSL certificate issuance has failed for them. You do so by selecting the **SSL Issuance Failed** notification type in the **Create Notification** dialog, as shown in the following illustration.



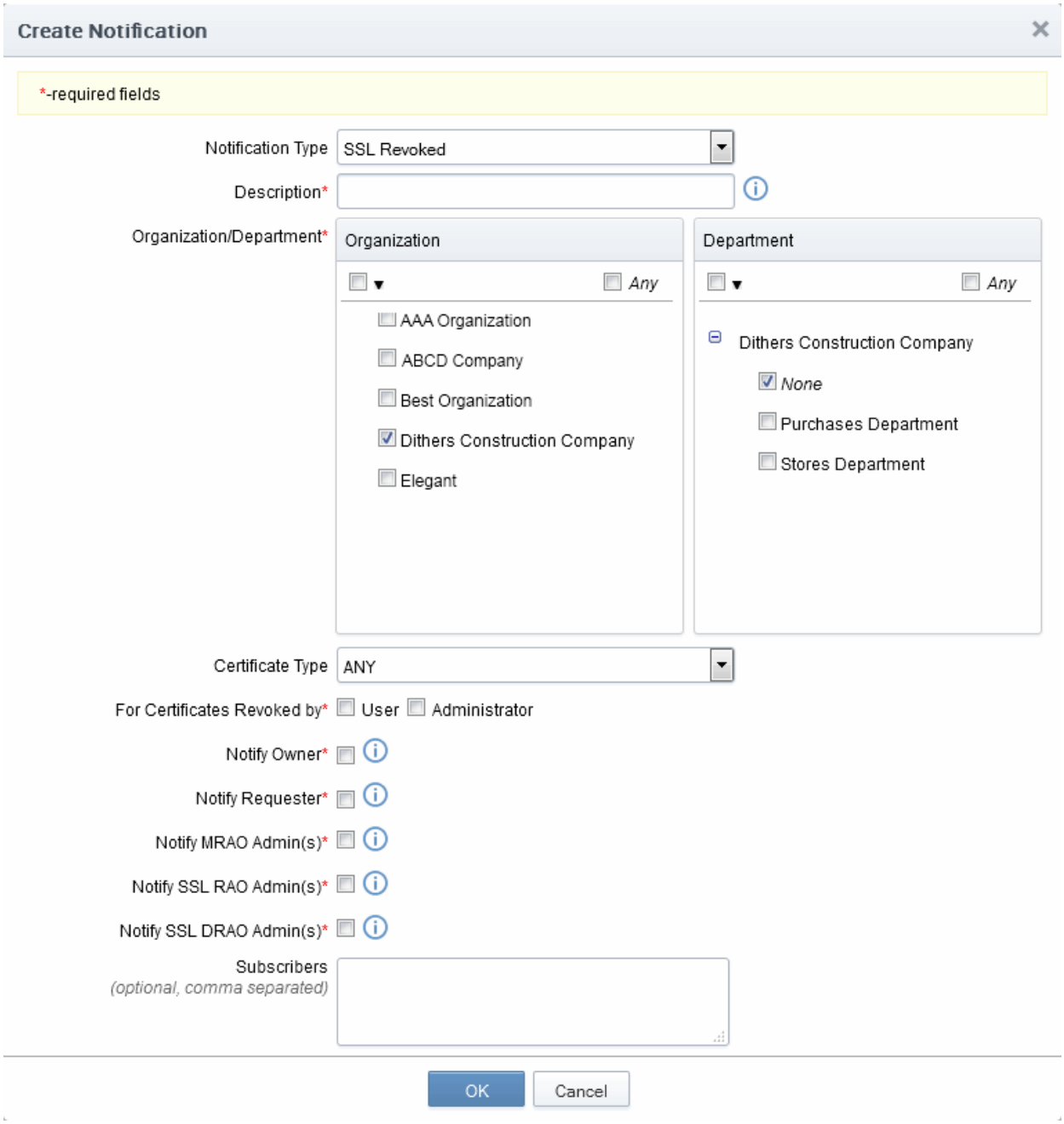
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization / Department	The organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Certificate Type	The type of SSL certificate for which the notification is to be set.
Notify Owner	Enables you to send the notification to the owner of the certificate.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to DRAO SSL administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.14 How to Create Notifications About Revocation of an SSL Certificate

You can issue a notification about the fact that the SSL certificate has been revoked (by either you or the end-user). You do so by selecting the **SSL Revoked** notification type in the **Create Notification** dialog, as shown in the following illustration.



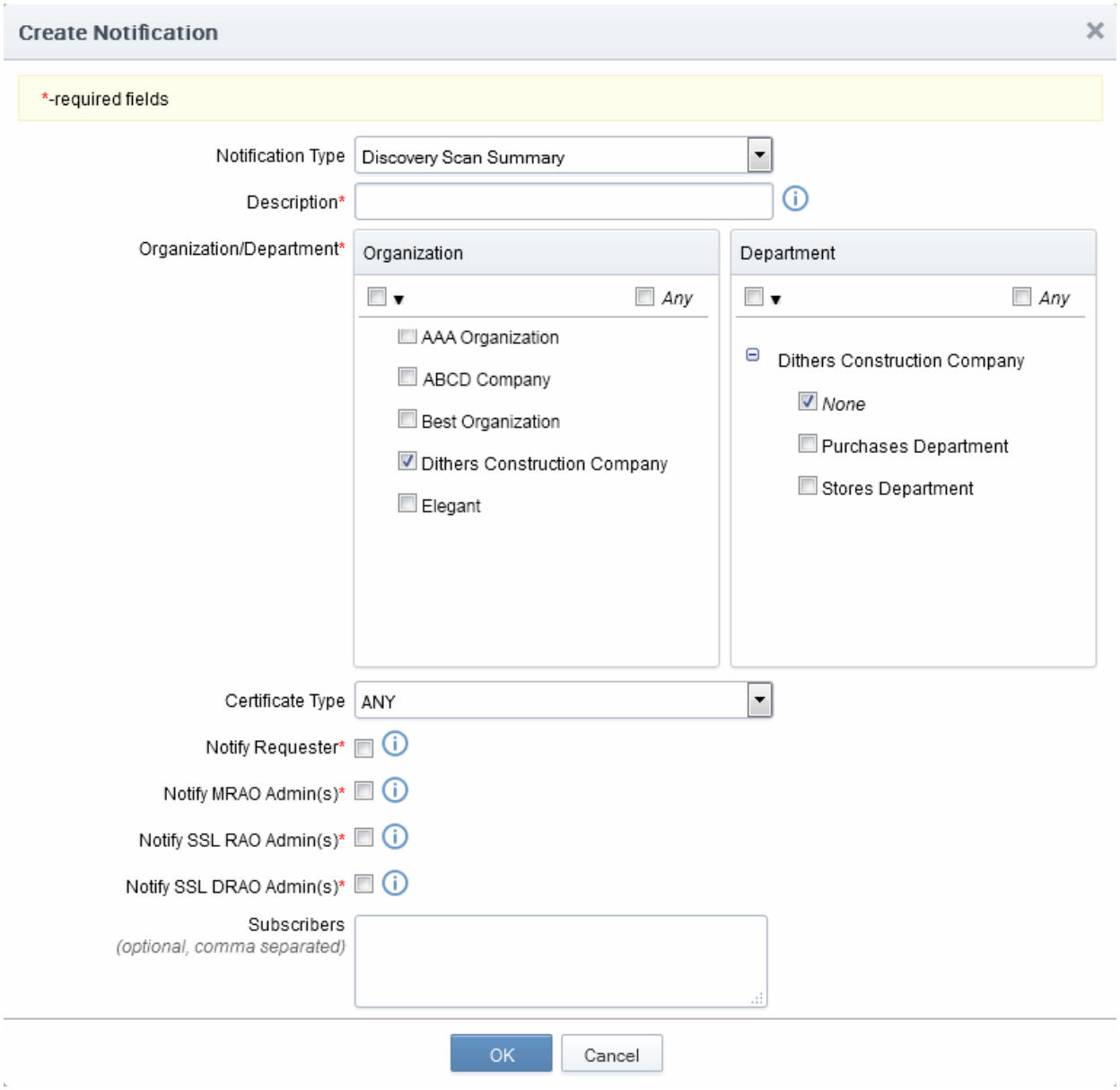
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization/Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Certificate Type	The type of SSL certificate for which the notification is to be set.
For Certificates Revoked by	Enables you to select a person (administrator or end-user) whose revoke action is to trigger notification.
Notify Owner	Enables you to send the notification for the owner of the certificate.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables you to send the notification to DRAO SSL administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.15 How to Create Notifications that Summarize Results of a Discovery Scan

You can notify specified personnel of the certificate discovery scan results. You do so by selecting the **Discovery Scan Summary** notification type in the **Create Notification** dialog, as shown in the following illustration.



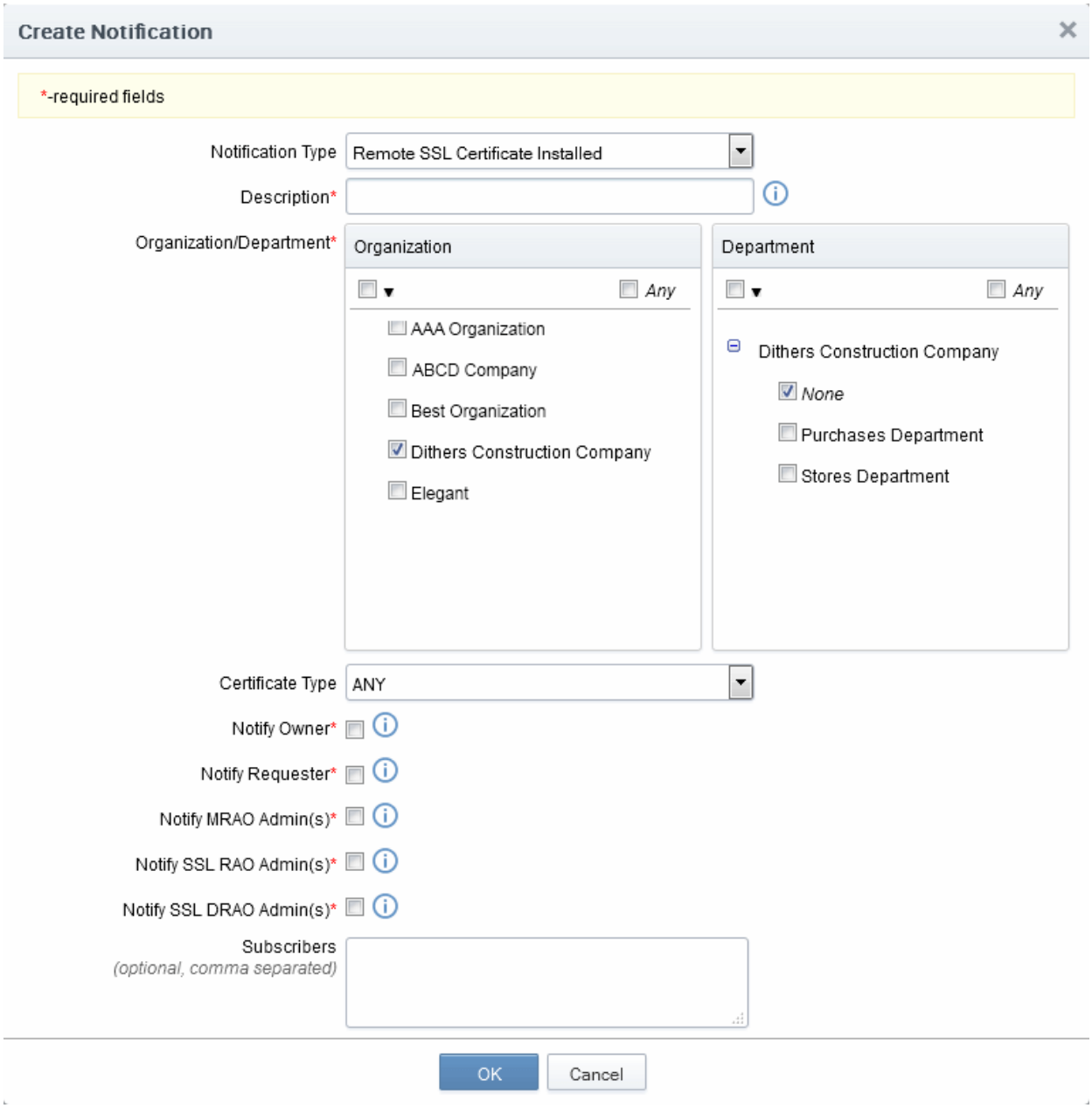
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization/Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.

Field / Element	Description
Certificate Type	The type of SSL certificate for which the notification is to be set.
Notify MRAO Admin	Enables you to send the notification to MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to RAO SSL administrators of the selected organization or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification for DRAO SSL administrators of the selected department.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.16 How to Create Notifications About a Remote Installation of an SSL Certificate

You can notify specified personnel of the fact that an SSL certificate was installed remotely for them. You do so by selecting the **Remote SSL Certificate Installed** notification type in the **Create Notification** dialog, as shown in the following illustration.



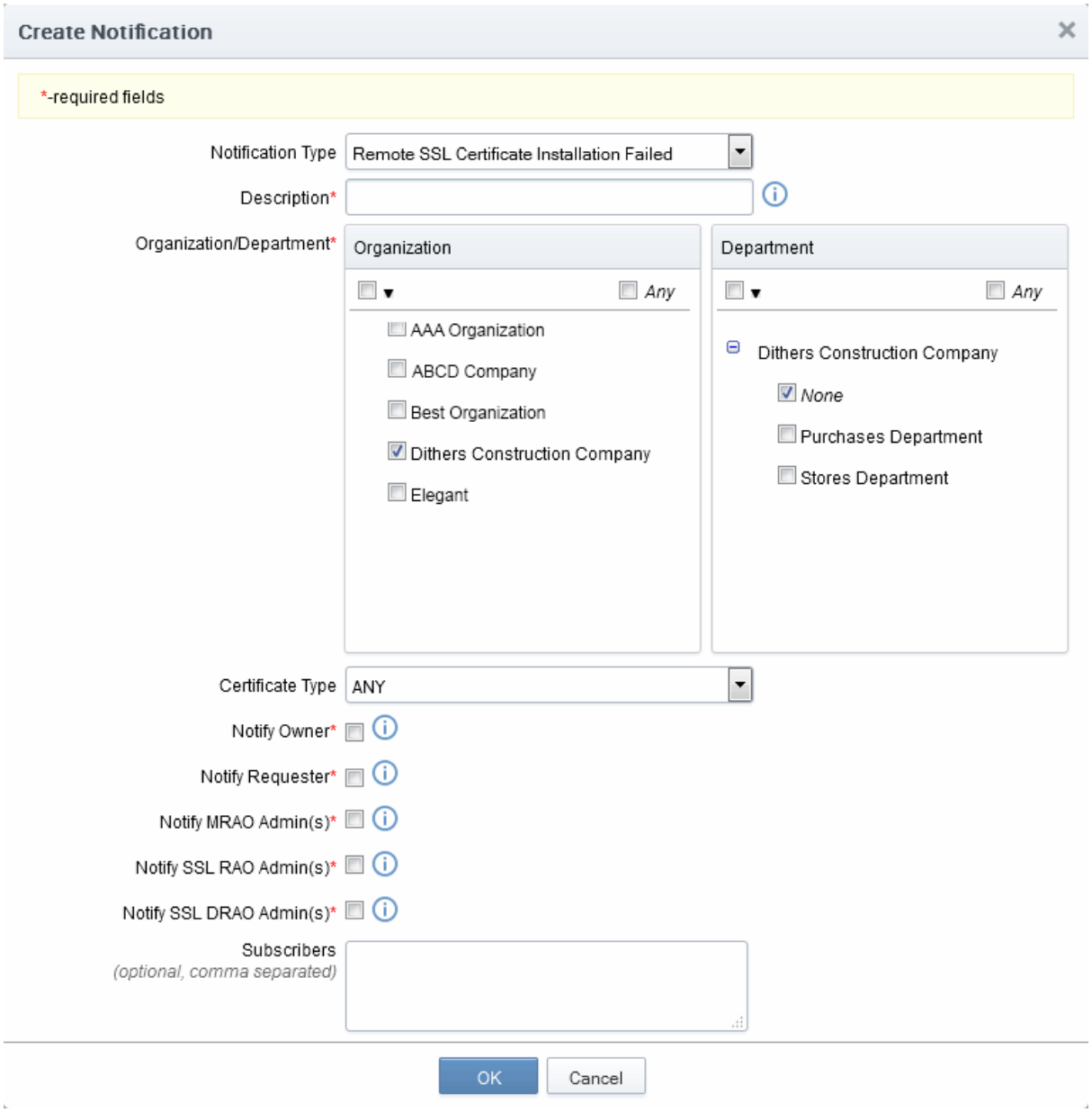
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization/Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Certificate Type	The type of SSL certificate for which the notification is to be set.
Notify Owner	Enables you to send a notification to the owner of the certificate. This is typically the administrator who first approved the request for the certificate.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to DRAO SSL administrators of the selected department.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.17 How to Create Notifications About Failed Attempts to Install SSL Certificates Remotely

You can notify specified personnel of the fact that an SSL certificate failed to install remotely for them. You do so by selecting the **Remote SSL Certificate Installation Failed** notification type in the **Create Notification** dialog, as shown in the following illustration.



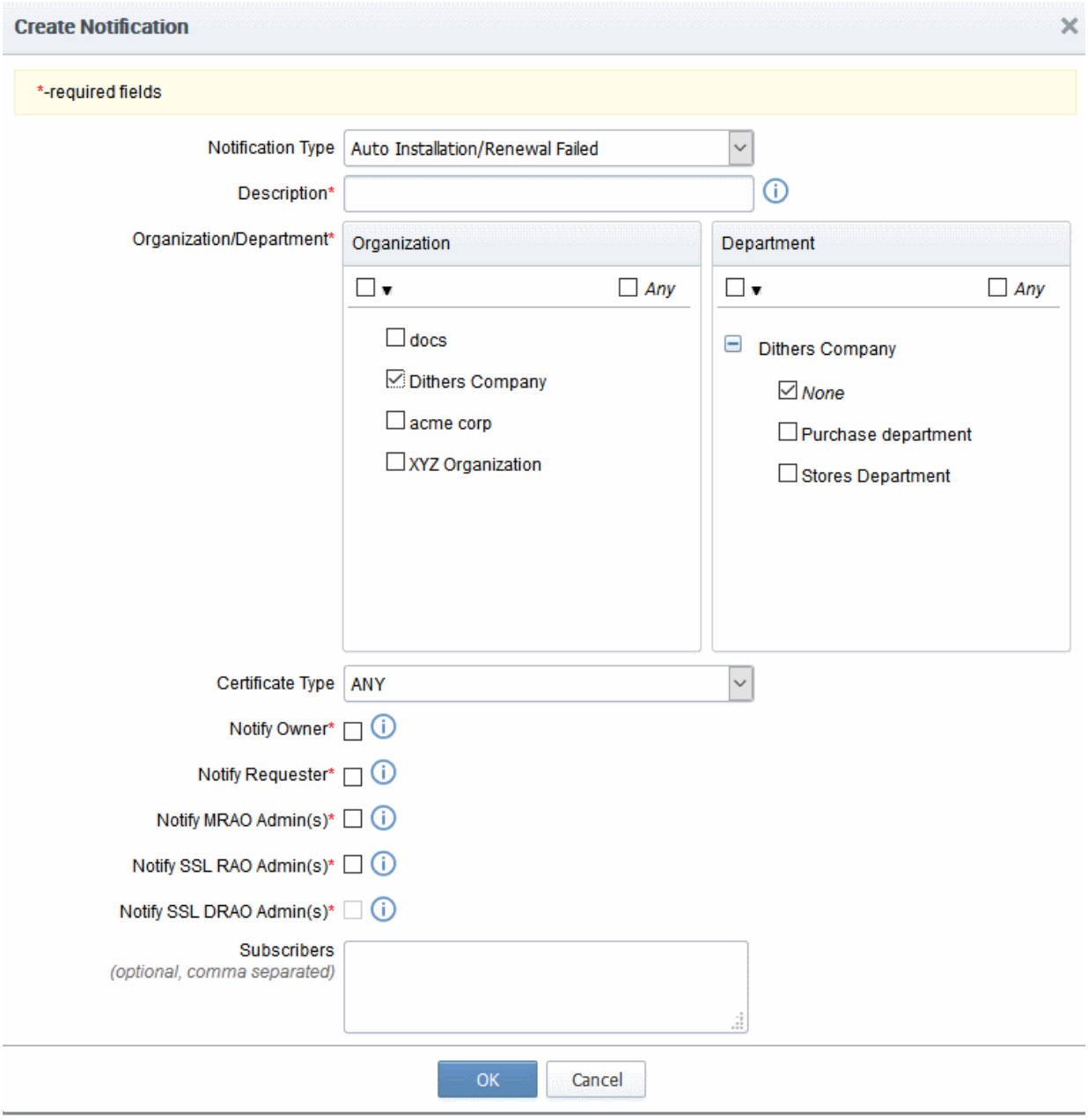
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization/Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.

Field / Element	Description
Certificate Type	The type of SSL certificate for which the notification is to be set.
Notify Owner	Enables you to send the notification to the would-be owner of the certificate.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to DRAO SSL administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.18 How to Create Notifications About a Failure to Install or Renew an SSL Certificate Automatically

You can notify specified personnel of the fact that an SSL certificate failed to install or be renewed automatically for them. You do so by selecting the **Auto Install/Renewal Failed** notification type in the **Create Notification** dialog, as shown in the following illustration.



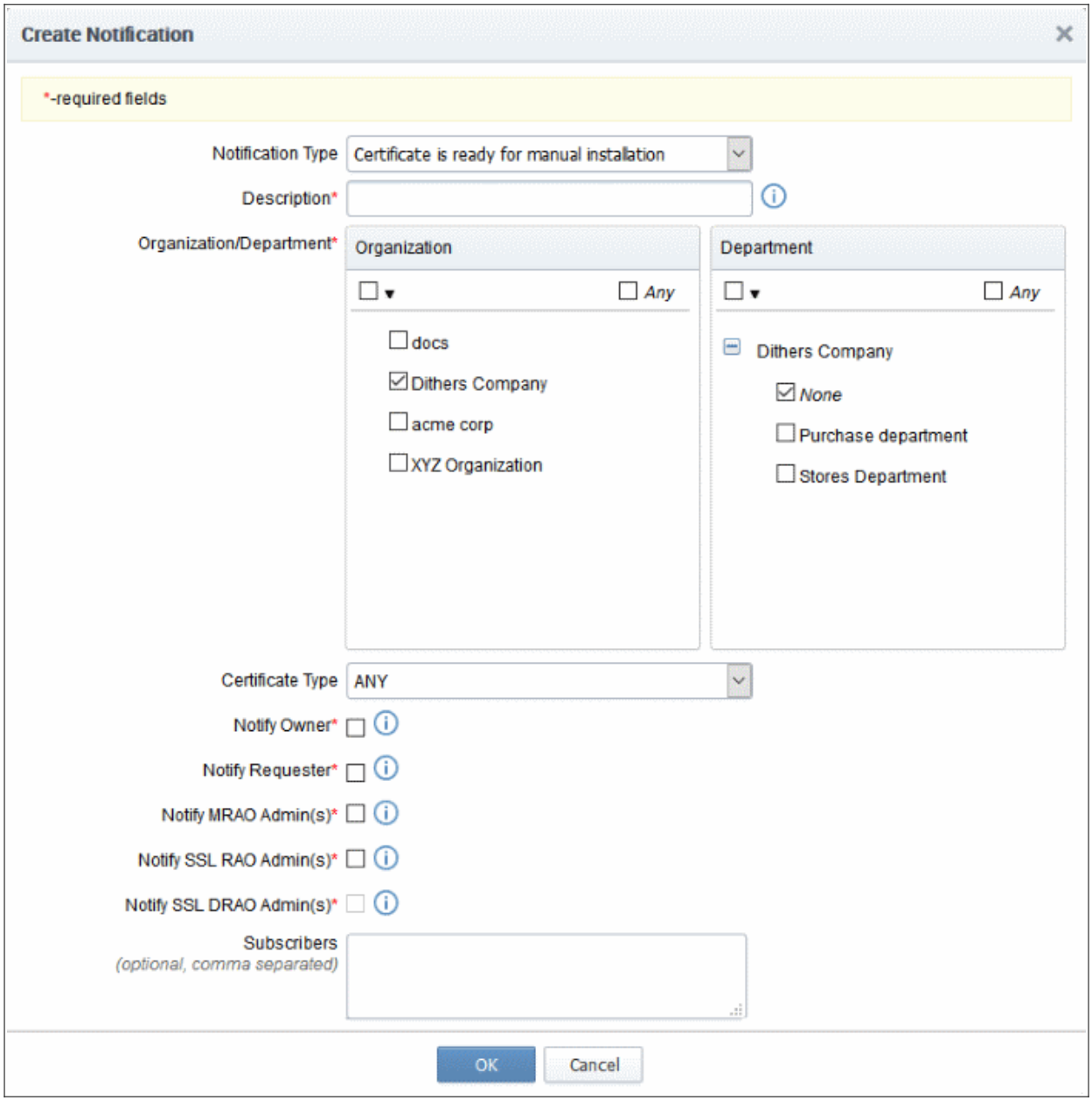
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Certificate Type	The type of SSL certificate for which the notification is to be set.
Notify Owner	Enables you to send the notification to the owner of the certificate.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to DRAO SSL administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.19 How to Create Notifications About an SSL Certificate Ready for Manual Installation

You can notify specified personnel of the fact that an SSL certificate is ready to be installed manually for them. You do so by selecting the **Certificate is ready for manual installation** notification type in the **Create Notification** dialog, as shown in the following illustration.



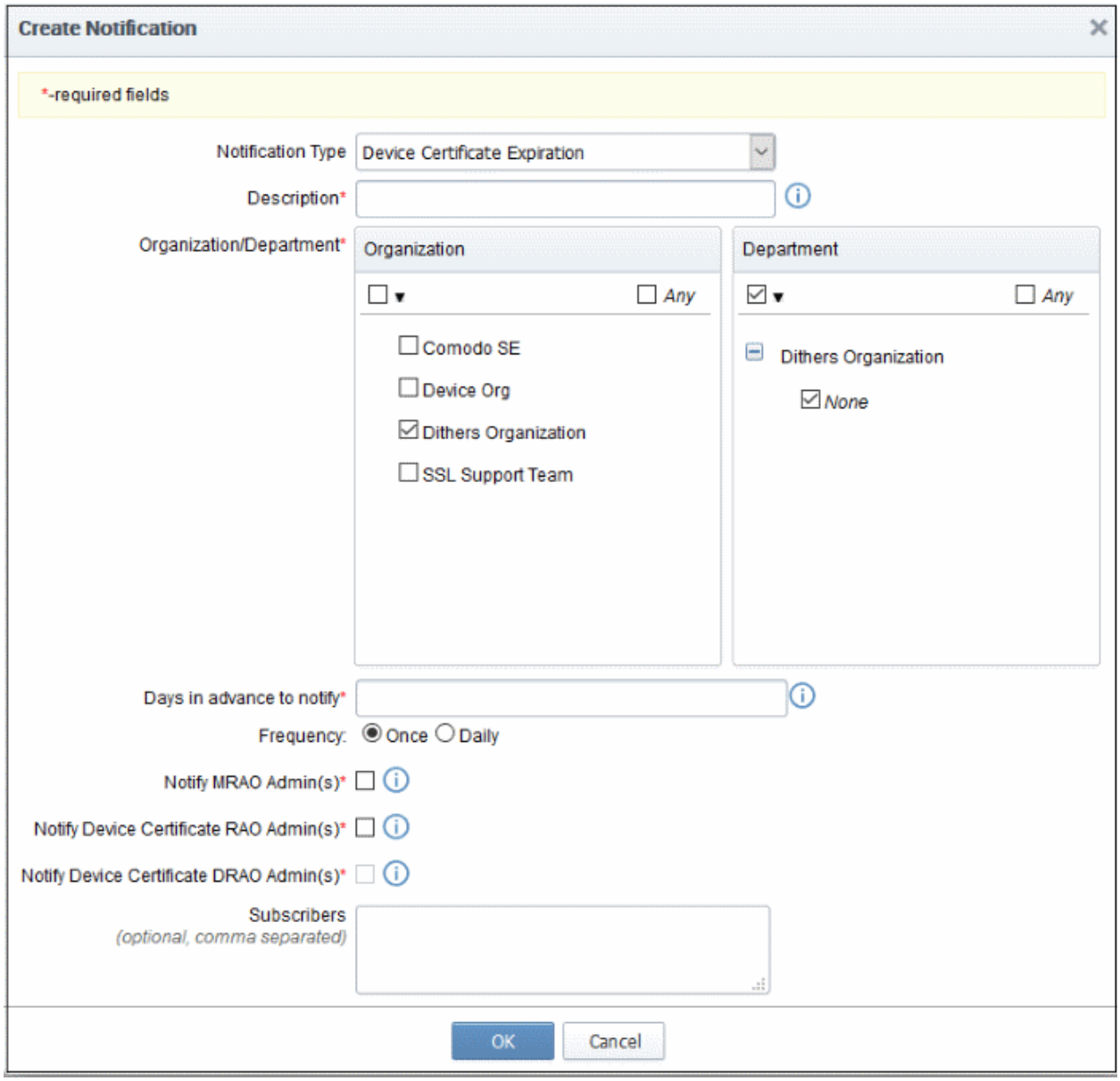
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Certificate Type	The type of SSL certificate for which the notification is to be set.
Notify Owner	Enables you to send a notification to the owner of the certificate. This is typically the administrator who first approved the request for the certificate.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to DRAO SSL administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.20 How to Create Notifications About Expiration of Device Certificates

You communicate the details of expiration of device certificates by selecting the **Device Certificate Expiration** notification type in the **Create Notification** dialog, as shown in the following illustration.



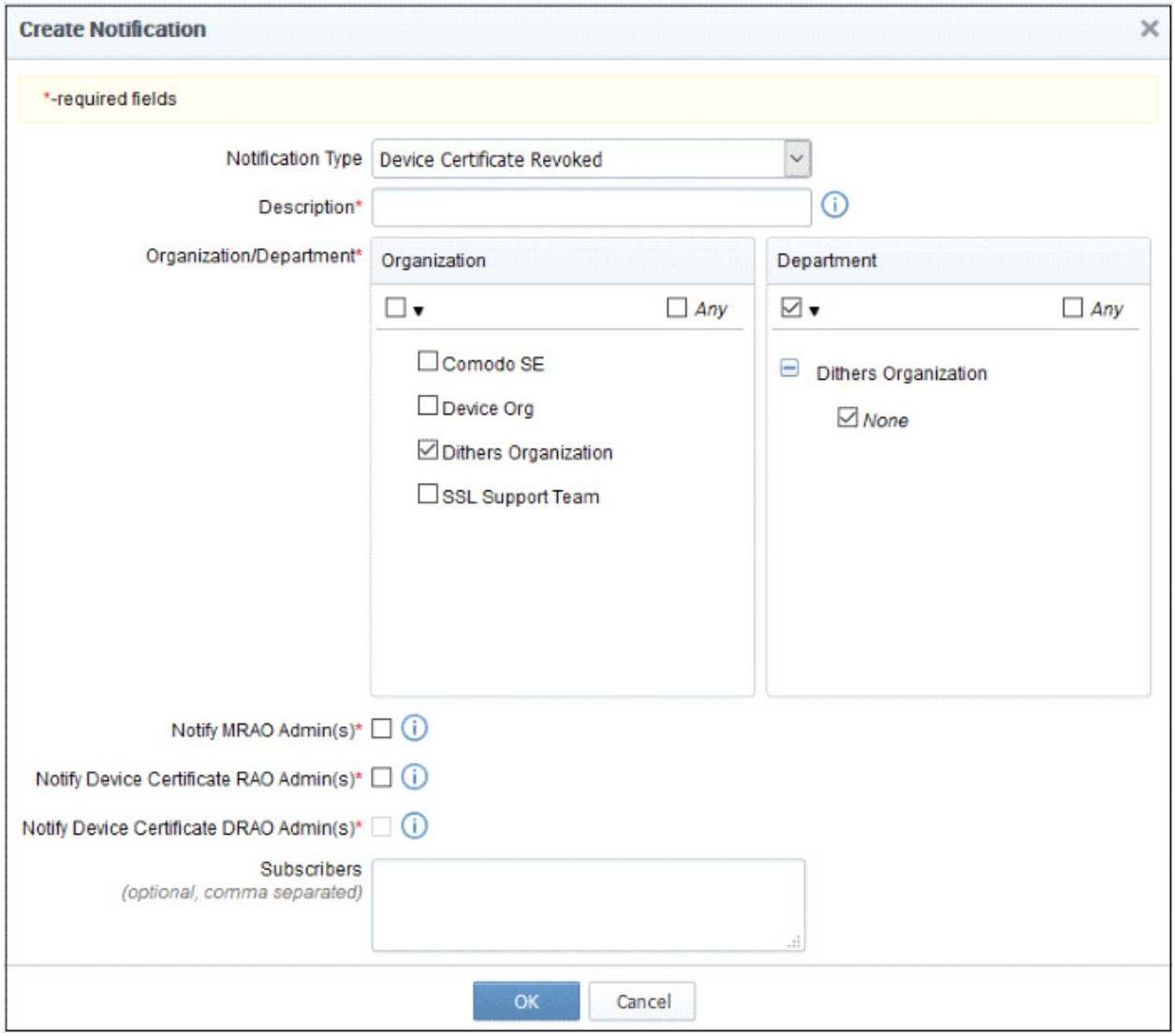
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.

Field / Element	Description
Days in advance to notify	Information about the number of days the end-user is to be notified about expiration of the certificate before the event. You can also specify whether the notification has to be sent to the members once or daily until the expiration date.
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify Device Certificate RAO Admins	Enables you to send the notification to RAO Device Certificate administrators of the selected organizations.
Notify Device Certificate DRAO Admins	Enables you to send the notification to DRAO Device Certificate administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.21 How to Create Notifications About Revocation of Device Certificates

You can notify specific personnel about revocation of a device certificate by selecting the **Device Certificated Revoked** notification type in the **Create Notification** dialog, as shown in the following illustration.



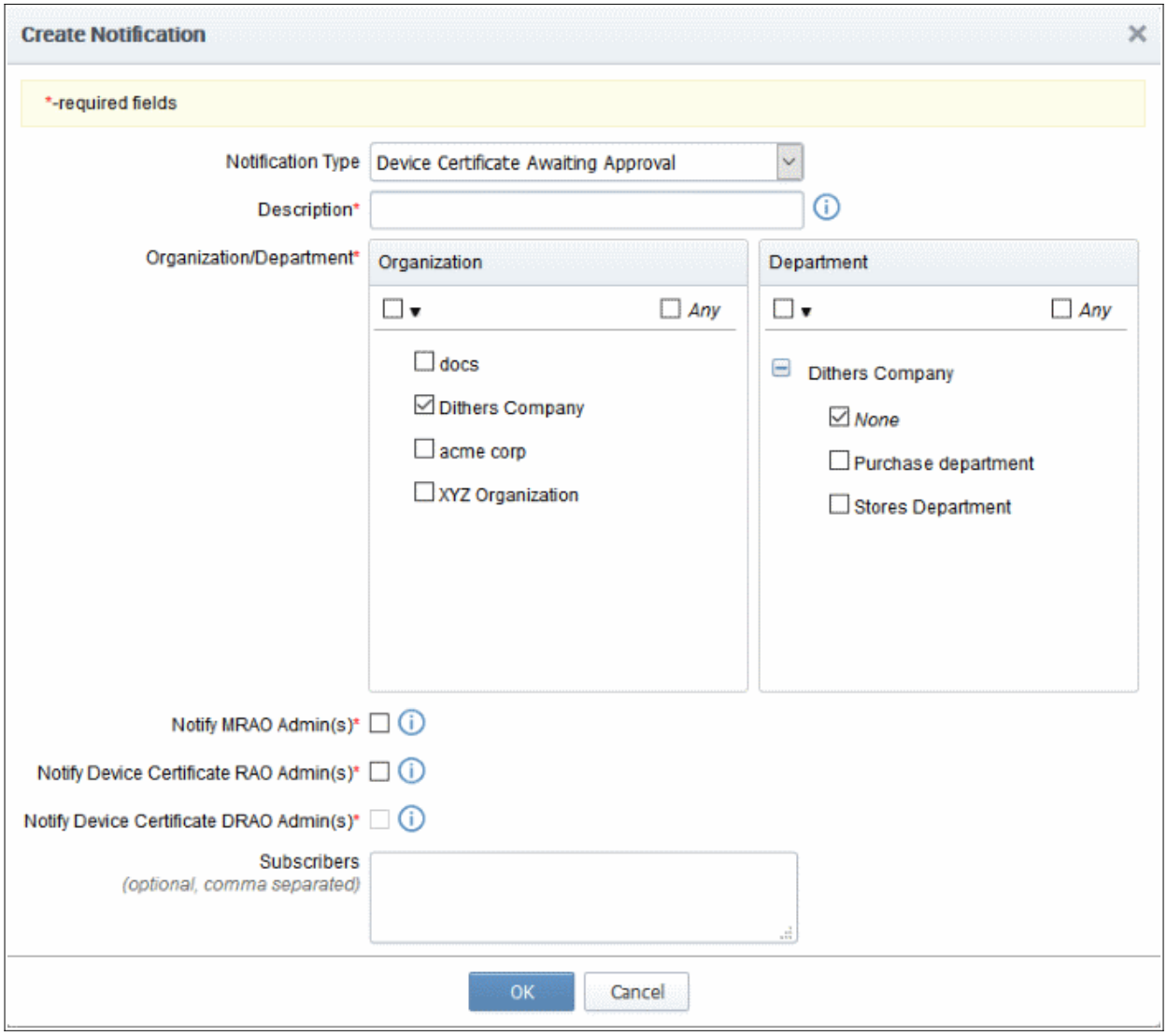
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
For Certificates Revoked by	Enables you to select a person (administrator or end-user) whose revoke action is to trigger notification.

Field / Element	Description
Notify Requester	Enables you to send the notification to the person who requested the certificate.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify Device Certificate RAO Admin	Enables you to send the notification to RAO Device Certificate administrators of the organization.
Notify Device Certificate DRAO Admin	Enables you to send the notification to DRAO Device Certificate administrators of the department.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.22 How to Create Notifications About Device Certificates Waiting for Approval

Each device certificate request must be approved by a MRAO or RAO administrator. Before the request is approved, its status is Awaiting Approval. You can communicate the status of a device certificated after the certificate was requested by selecting the **Device Certificate Awaiting Approval** notification type in the **Create Notification** dialog, as shown in the following illustration.



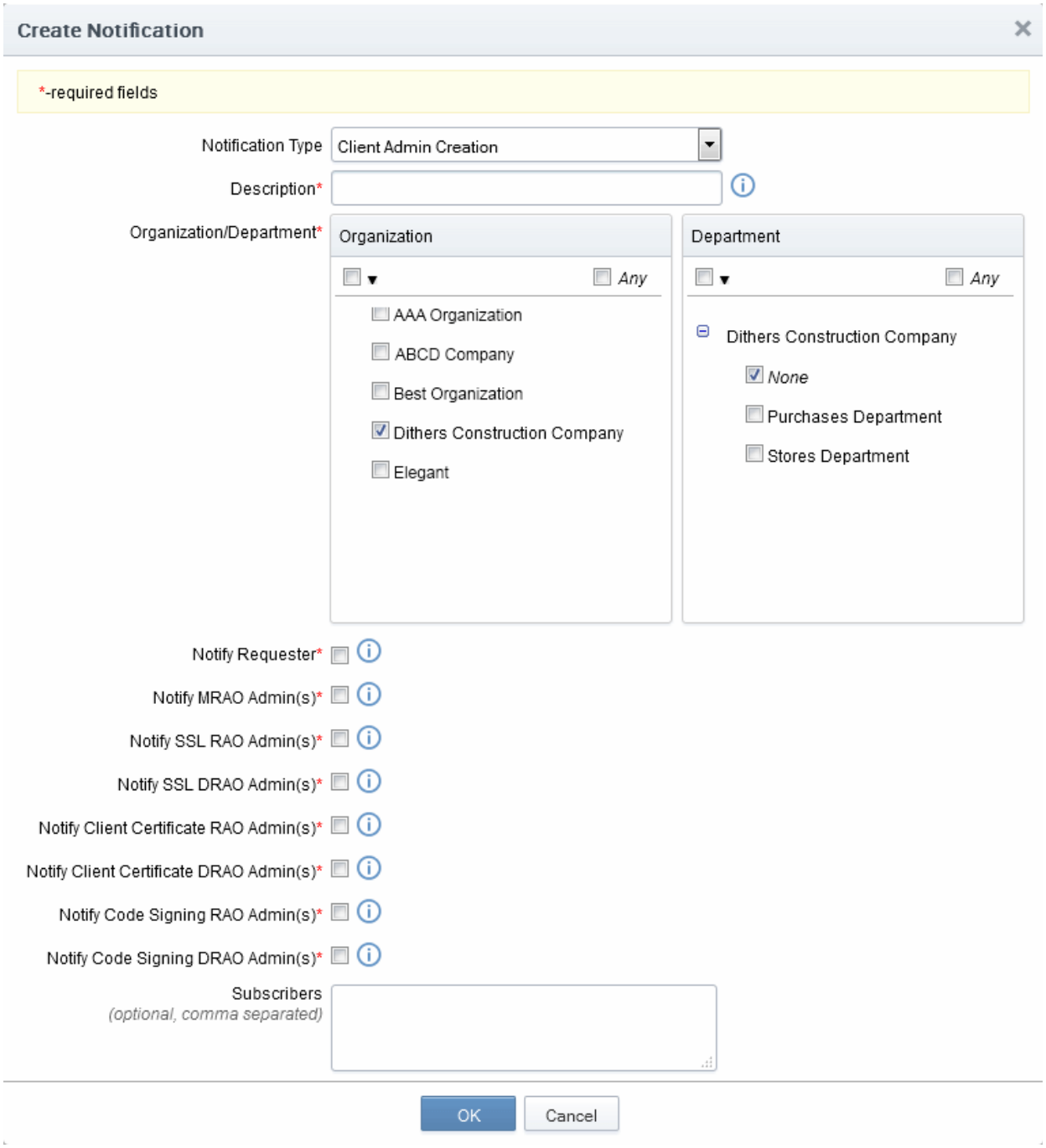
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Notify MRAO Admins	Enables you to send the notification to MRAOs.

Field / Element	Description
Notify Device Certificate RAO Admins	Enables you to send the notification to RAO Device Certificate administrators of the selected organizations.
Notify Device Certificate DRAO Admins	Enables you to send the notification to DRAO Device Certificate administrators of the selected department.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.23 How to Create Notifications About Creation of a New Client Administrator

You can notify specific personnel about creation of new MRAO, RAO, or DRAO administrators. You do so by selecting the **Client Admin Creation** notification type in the **Create Notification** dialog, as shown in the following illustration.



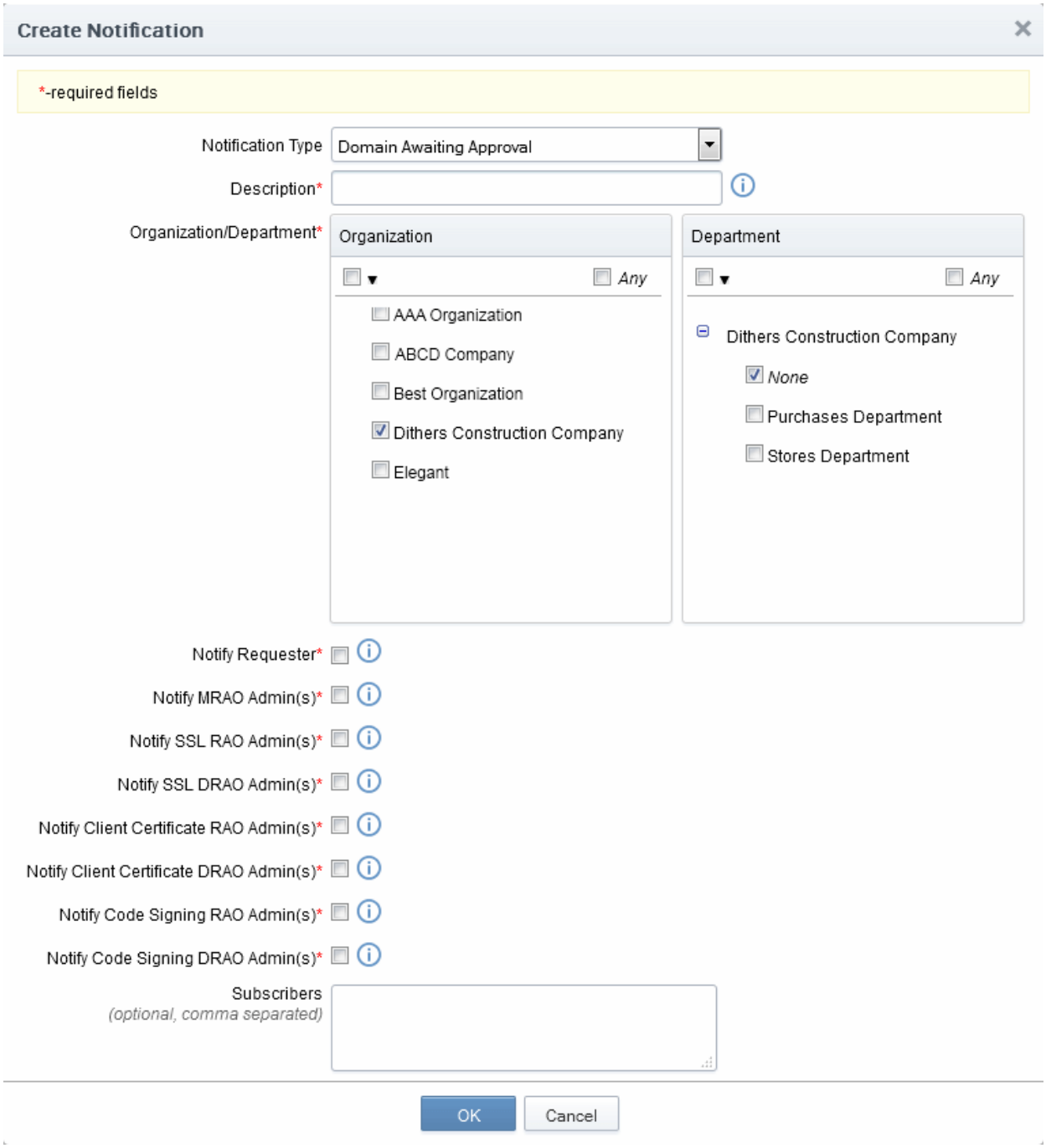
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Notify Requester	Enables you to send a notification to the person who requested the administrator status.
Notify MRAO Admins	Enables you to send notifications to MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to all RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables you to send notifications to all DRAO SSL administrators of the selected departments.
Notify Client Certificate RAO Admins	Enables you to send notifications to all RAO Client Certificate administrators of the selected organizations and departments.
Notify Client Certificate DRAO Admins	Enables you to send notifications to all DRAO Client Certificate administrators of the selected departments.
Notify Code Signing RAO Admins	Enables you to send notifications to all RAO Code Signing administrators of the selected organizations and departments.
Notify Code Signing DRAO Admins	Enables you to send notifications to all DRAO Code Signing administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.24 How to Create Notifications About a Domain Waiting for Approval

Each domain delegation request must be approved by a MRAO or RAO administrator. Before the request is approved, its status is Awaiting Approval. You can set up a notification about a request of a domain delegation to an organization or department by selecting the **Domain Awaiting Approval** notification type in the **Create Notification** dialog, as shown in the following illustration.



The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

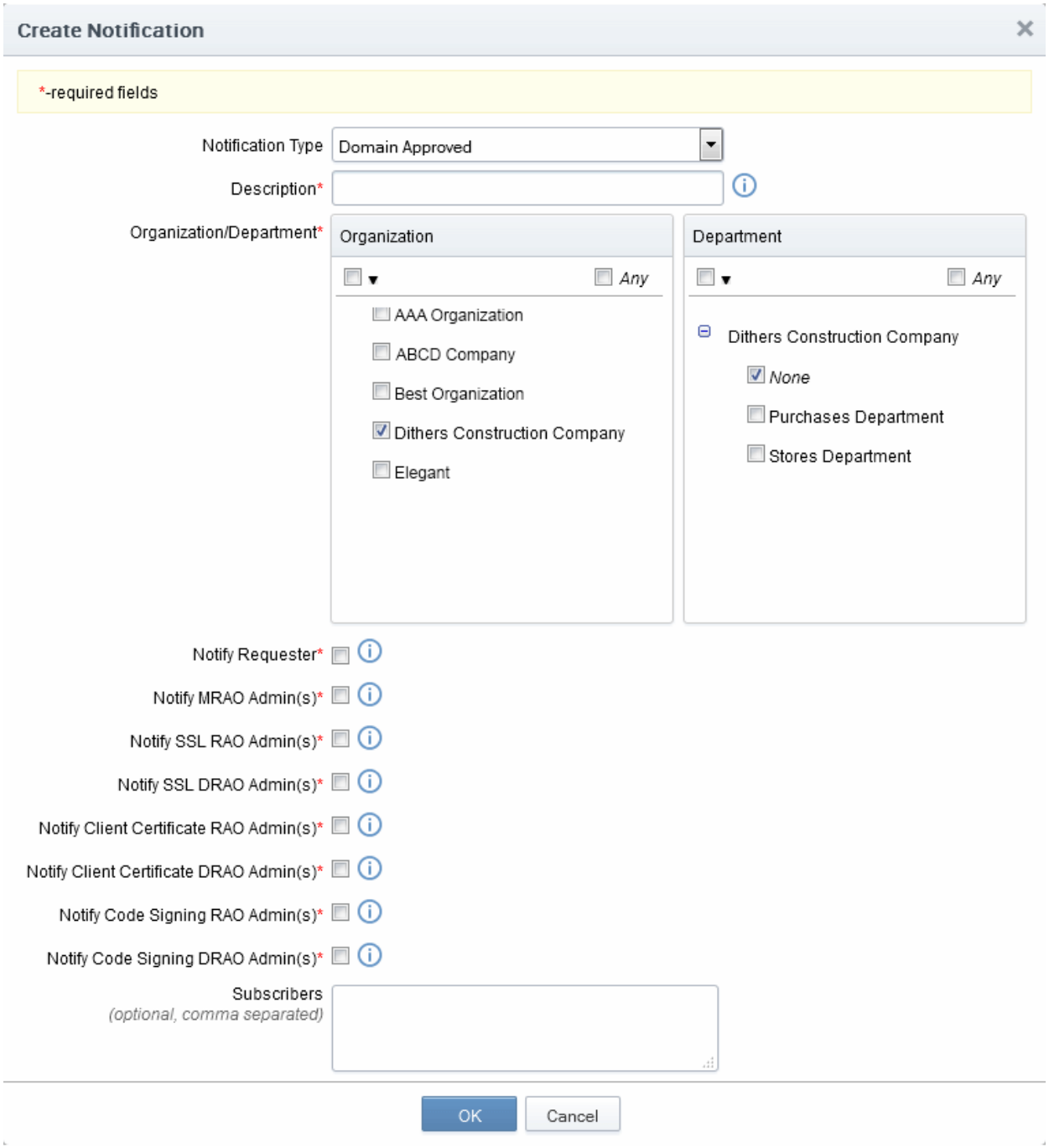
Field / Element	Description
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Notify Requester	Enables you to send the notification to the person who requested the delegation of a created domain to an organization or department.
Notify MRAO Admins [a]	Enables you to send the notification to all MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to all RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to all DRAO SSL administrators of the selected departments.
Notify Client Certificate RAO Admins	Enables you to send notifications to all RAO Client Certificate administrators of the selected organizations and departments.
Notify Client Certificate DRAO Admins	Enables you to send notifications to all DRAO Client Certificate administrators of the selected departments.
Notify Code Signing RAO Admins	Enables you to send notifications to all RAO Code Signing administrators of the selected organizations and departments.
Notify Code Signing DRAO Admins	Enables you to send notifications to all DRAO Code Signing administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

a. The notification is sent to MRAO only after the domain requested by a DRAO is approved by a RAO administrator.

7.5.25 How to Create Notifications About Approval of a Domain

You can notify specific personnel about an approval of a domain creation or delegation for an organization or department. To do so, you select the **Domain Approved** notification type in the **Create Notification** dialog, as shown in the following illustration.

Note that each domain creation or delegation request must be approved by two MRAO administrators, unless **Allow domain validation without Dual Approval** was selected during the MRAO creation process, in which case requests can be approved by a single MRAO.



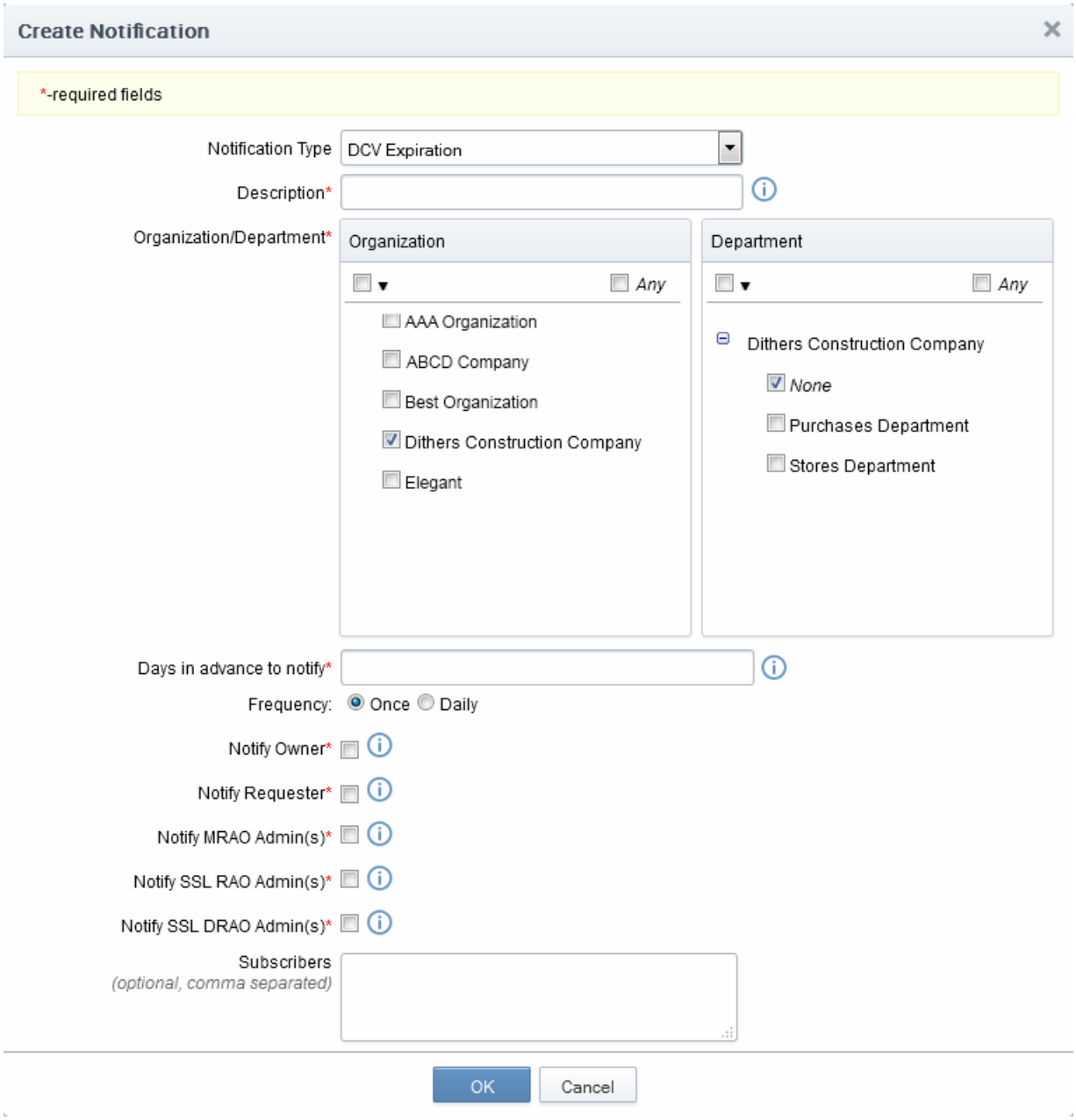
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Notify Requester	Enables you to send the notification to the person who requested the delegation of a created domain to an organization or department.
Notify MRAO Admins	Enables you to send the notification to all MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to all RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to all DRAO SSL administrators of the selected departments.
Notify Client Certificate RAO Admins	Enables you to send notifications to all RAO Client Certificate administrators of the selected organizations and departments.
Notify Client Certificate DRAO Admins	Enables you to send notifications to all DRAO Client Certificate administrators of the selected departments.
Notify Code Signing RAO Admins	Enables you to send notifications to all RAO Code Signing administrators of the selected organizations and departments.
Notify Code Signing DRAO Admins	Enables you to send notifications to all DRAO Code Signing administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.26 How to Create Notifications About a DCV Expiration

You can issue a notification about an upcoming expiration of a DCV. To do so, you select the **DCV Expiration** notification type in the **Create Notification** dialog, as shown in the following illustration.



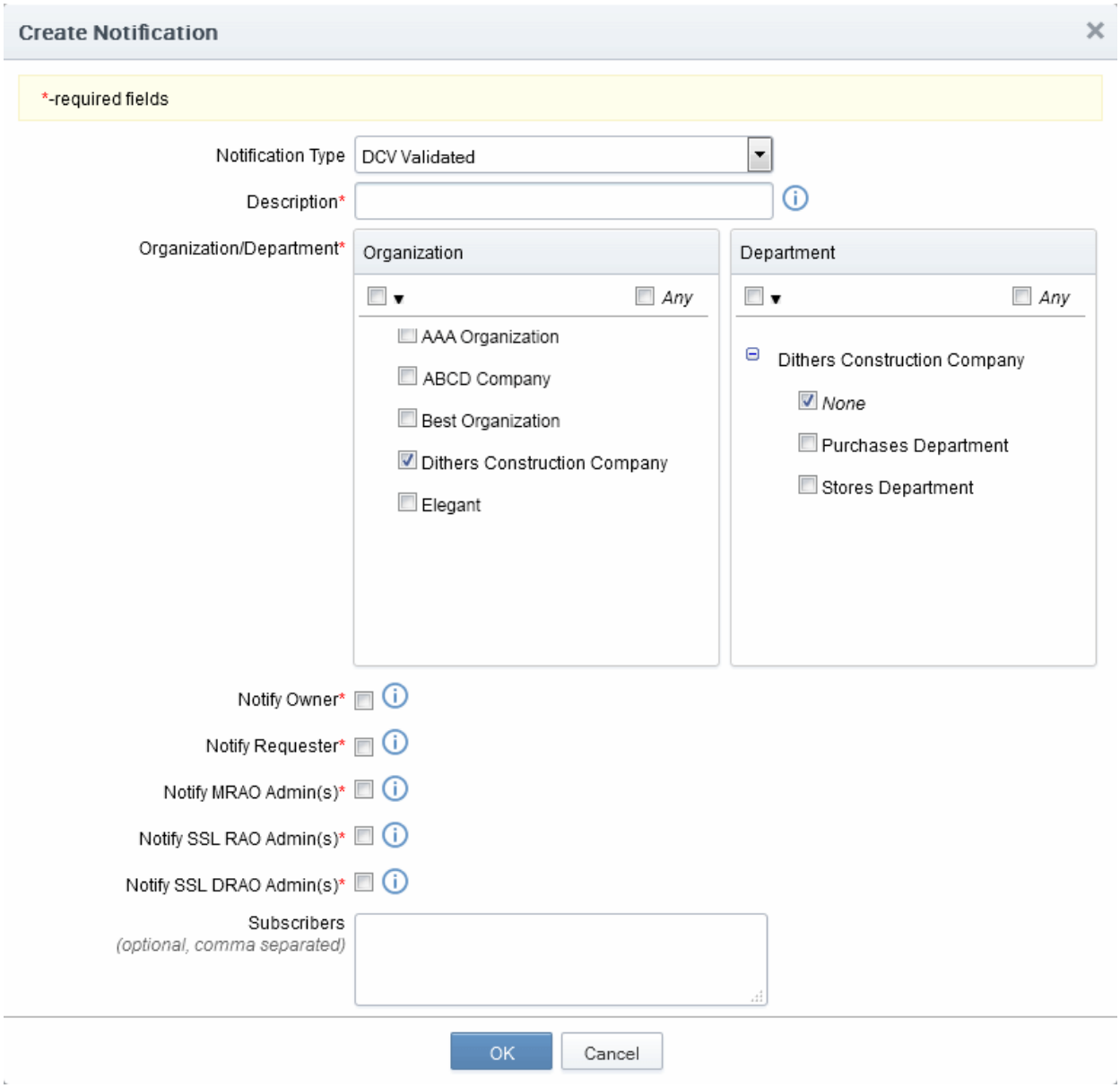
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.

Field / Element	Description
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Days in advance to notify	The number of days before the expiration date the notification is to be sent about expiration of the DCV. You can also specify whether the notification is to be sent only once or daily until the expiration date.
Notify Owner	Enables you to send the notification for the owner of the certificate.
Notify Requester	Enables you to send the notification to the person who requested the delegation of a created domain to an organization or department.
Notify MRAO Admins	Enables you to send the notification to all MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to all RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to all DRAO SSL administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.27 How to Create Notifications About Completion of DCV

You can notify specific personnel about a successful completion of DCV. To do so, you select the **DCV Validated** notification type in the **Create Notification** dialog, as shown in the following illustration.



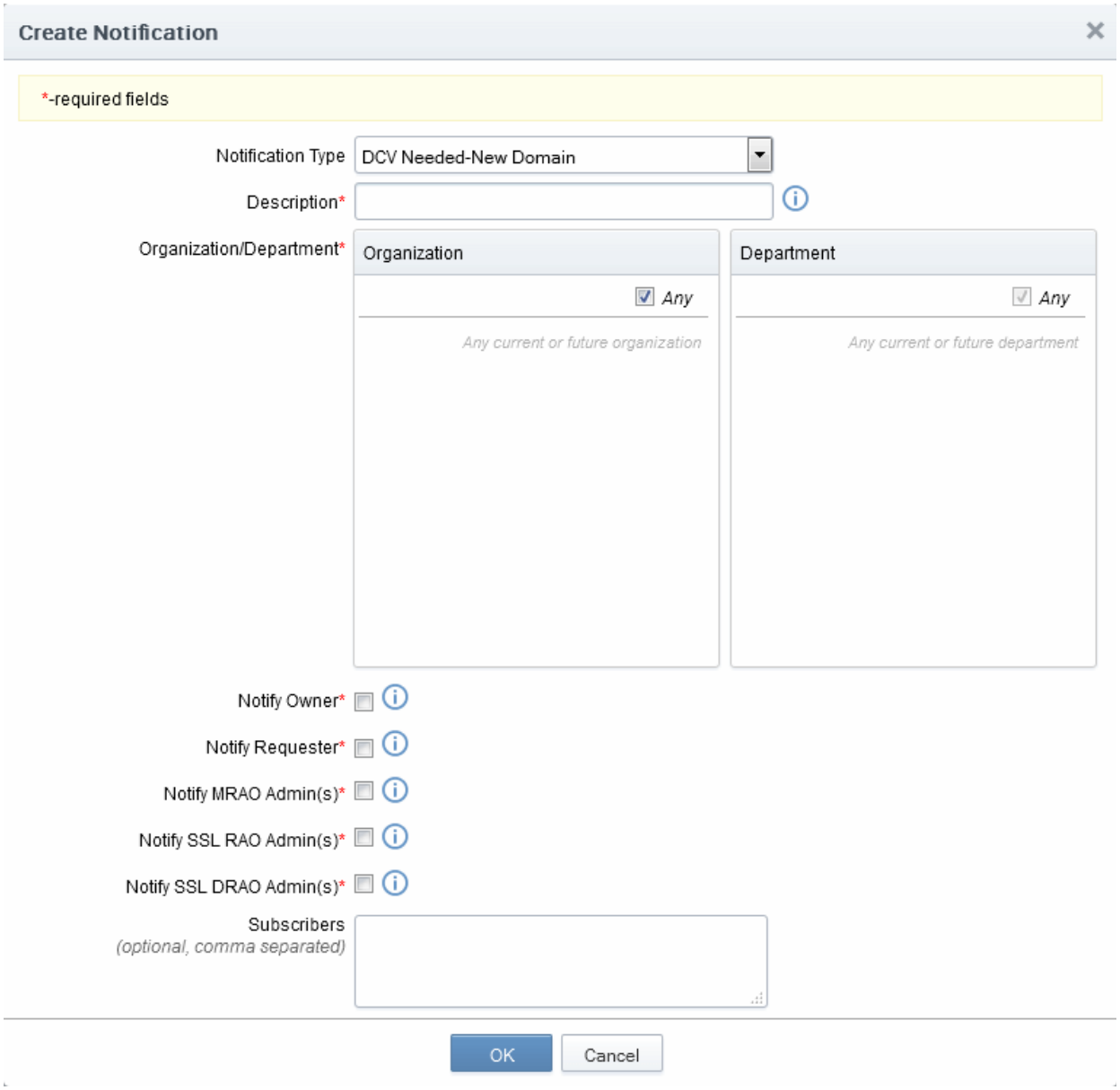
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Notify Owner	Enables you to notify the owner of the certificate.

Field / Element	Description
Notify Requester	Enables you to send the notification to the person who requested the delegation of a created domain to an organization or department.
Notify MRAO Admins	Enables you to send the notification to all MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to all RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to all DRAO SSL administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.28 How to Create Notifications About DCV Required for a New Domain

You can notify specific personnel about the fact that a new domain has been created and is awaiting validation. To do so, you select the **DCV Needed-New Domain** notification type in the **Create Notification** dialog, as shown in the following illustration.



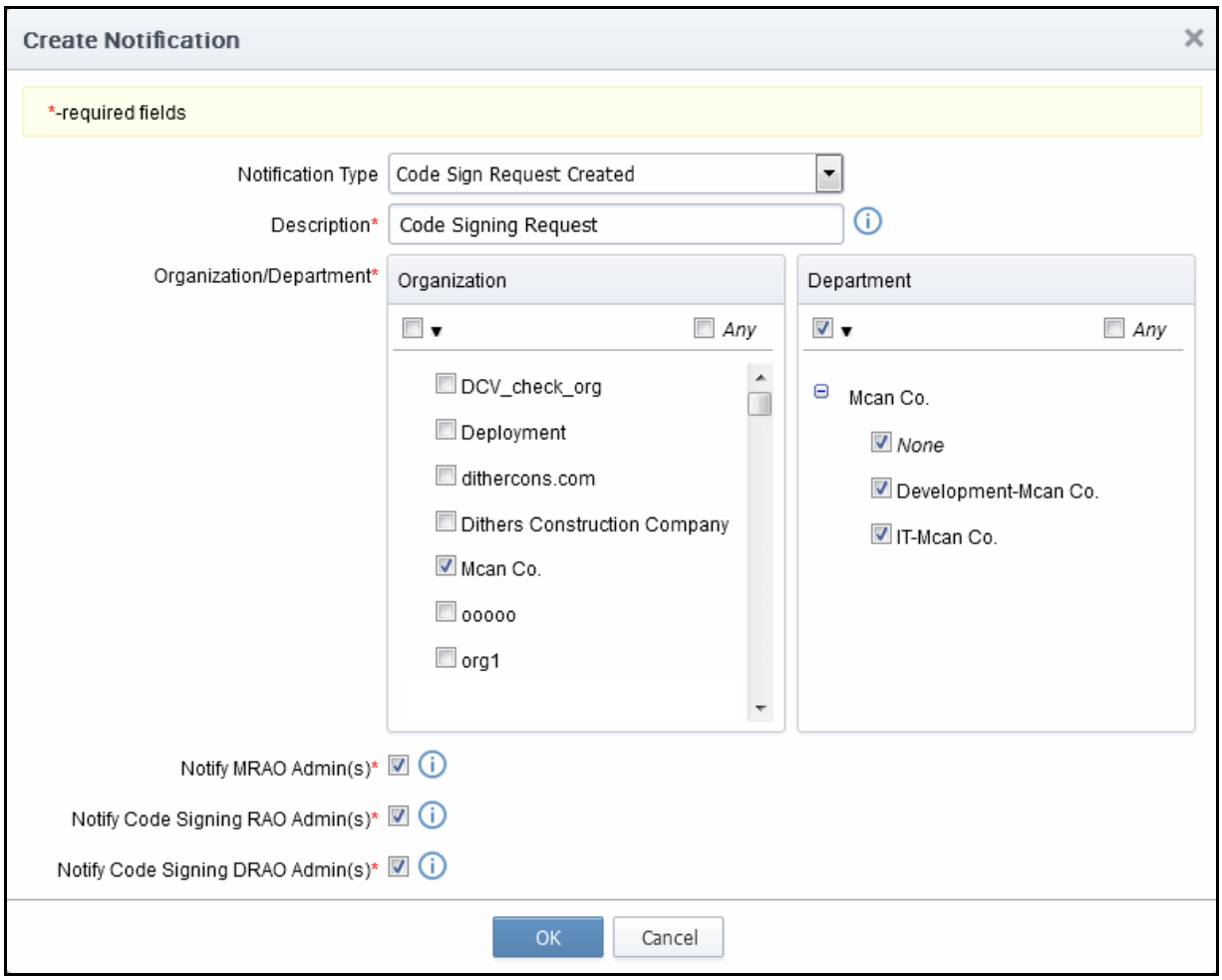
The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.

Field / Element	Description
Notify Owner	Enables you to notify the owner of the certificate.
Notify Requester	Enables you to send the notification to the person who requested the delegation of a created domain to an organization or department.
Notify MRAO Admins	Enables you to send the notification to all MRAOs.
Notify SSL RAO Admins	Enables you to send the notification to all RAO SSL administrators of the selected organizations or departments.
Notify SSL DRAO Admins	Enables the administrator to send the notification to all DRAO SSL administrators of the selected departments.
Subscribers	The email addresses of other people to whom the notifications are to be sent.

7.5.29 How to Create Notifications About a New Request for a CSoD Certificate

You can notify specified personnel of the fact that a request for a CSoD certificate has been created by a software developer. You do so by selecting the **Code Sign Request Created** notification type in the **Create Notification** dialog, as shown in the following illustration.

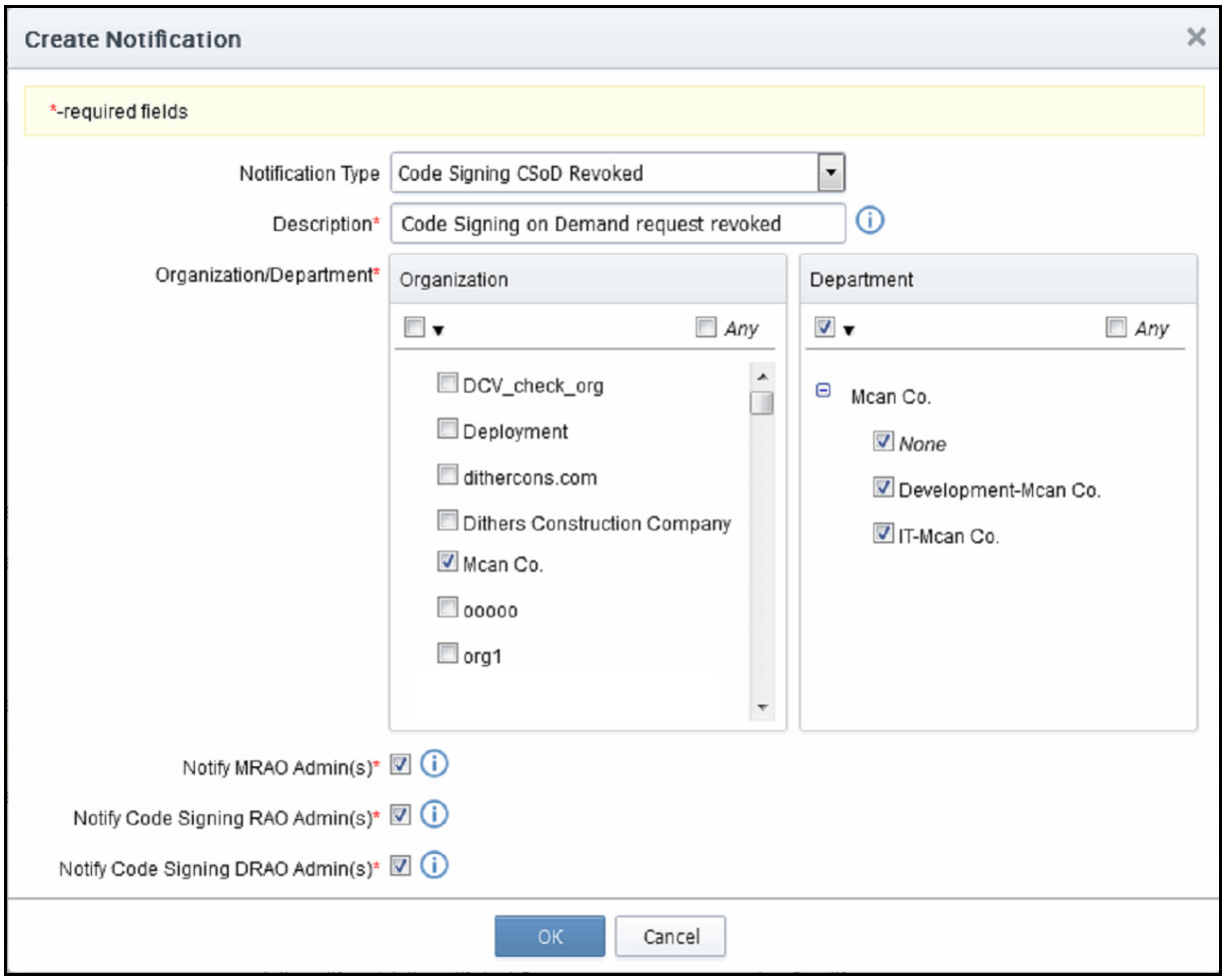


The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

Field / Element	Description
Description	A short description of the notification.
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Notify MRAO Admins	Enables you to send the notification to MRAOs.
Notify Code Signing RAO Admins	Enables you to send the notification to RAO Code Signing administrators of the selected organizations or departments.
Notify Code Signing DRAO Admins	Enables you to send the notification to DRAO Code Signing administrators of the selected department.

7.5.30 How to Create Notifications About Revocation of a CSoD Certificate

You can notify specified personnel of the fact that a CSoD certificate has been revoked by an administrator. You do so by selecting the **Code Sign CSoD Revoked** notification type in the **Create Notification** dialog, as shown in the following illustration.



The following table lists settings and elements available in the **Create Notification** dialog. Mandatory settings are marked by red asterisks.

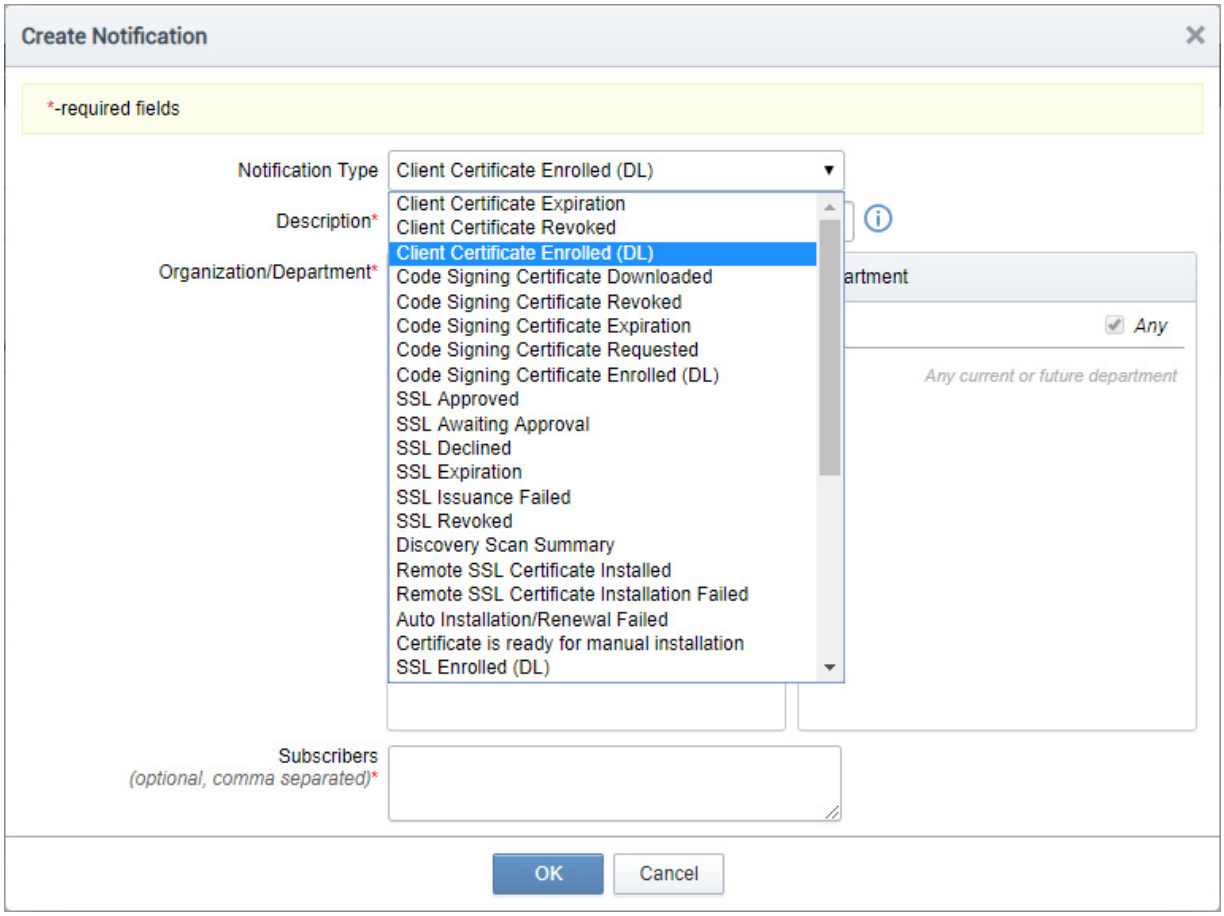
Field / Element	Description
Description	A short description of the notification.
Organization / Department	Organizations or departments which should receive the notification. To enable all current organizations and departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current organizations and departments and any that are added in the future.
Notify MRAO Admins	Enables you to send the notification to MRAOs.

Field / Element	Description
Notify Code Signing RAO Admins	Enables you to send the notification to RAO Code Signing administrators of the selected organizations or departments.
Notify Code Signing DRAO Admins	Enables you to send the notification to DRAO Code Signing administrators of the selected department.

7.5.31 How to Create Notifications About Successful Certificate Enrollment

You can notify specific personnel about successful certificate enrollment by selecting **Client Certificate Enrolled (DL)**, **Code Signing Certificate Enrolled (DL)**, **SSL Enrolled (DL)**, or **Device Certificate Enrolled (DL)** as the **Notification Type** in the **Create Notification** dialog, as shown in the following illustration.

NOTE: These notifications do not interfere with the default email notifications sent following a successful certificate enrollment or similar event.



The following table lists the settings and elements available in the **Create Notification** dialog when **Client Certificate Enrolled (DL)**, **Code Signing Certificate Enrolled (DL)**, **SSL Enrolled**

(DL), or **Device Certificate Enrolled (DL)** are selected as the **Notification Type**. Mandatory settings are marked by red asterisks.

Field	Description
Description	A short description of the notification.
Organization / Department	The organizations or departments under which the certificate request must be submitted for the this notification rule to apply. To enable all available organizations or departments to receive this notification, select the check box on the left. Select **Any** to enable the notification for all current and future organizations and departments.
Subscribers	The email addresses of all personnel to be notified about the successful certificate enrollment.

7.6 Configuring Key Escrow and Encryption

SCM can store the individual private keys of end-user's client certificates so that these keys can be recovered at a later date by appropriately privileged administrators. All end-user client certificates are stored in encrypted form.

It is possible to specify that keys in escrow be independently retrieved by any of the three administrator levels: MRAO, RAO Client Certificate, and DRAO Client Certificate. SCM can store up to two encrypted versions of the private keys of client certificates of an organization and up to three versions for a department. Each version is separately encrypted by three different master public keys: the MRAO master key, the organization master key, and the departmental master key.

The master public keys are stored by SCM. The corresponding master private keys, which are required for decryption and retrieval, are not stored in SCM. These keys must be saved in a secure location by the administrator who is creating the organization or department.

There is one master key pair per organizational tier which is generated (if required) during the creation of that organizational tier (for example, during creation of the organization or department). Therefore, one master key pair is used by all RAO Client Certificate administrators of a particular organization.. Similarly, if key retrieval is required at the departmental level, then one pair of master keys—Department Master Key—is used by all DRAO Client Certificate administrators of a particular department.

If **Allow key recovery by MRAO/RAO/DRAO** option is enabled when an organization or department is created, then these master key pairs must be initialized prior to issuing client certificates. It is not possible to issue client certificates until the master private keys have been initialized. See "About the Master Keys Requirements for the Client Certificate Issuance" on page 476 for more information.

Retrieving the private key of an end-user's client certificate from escrow causes the revocation of that certificate. This is true if any one of the aforementioned administrative types chooses to retrieve from escrow. A private key can be retrieved from escrow by clicking **Download** for a

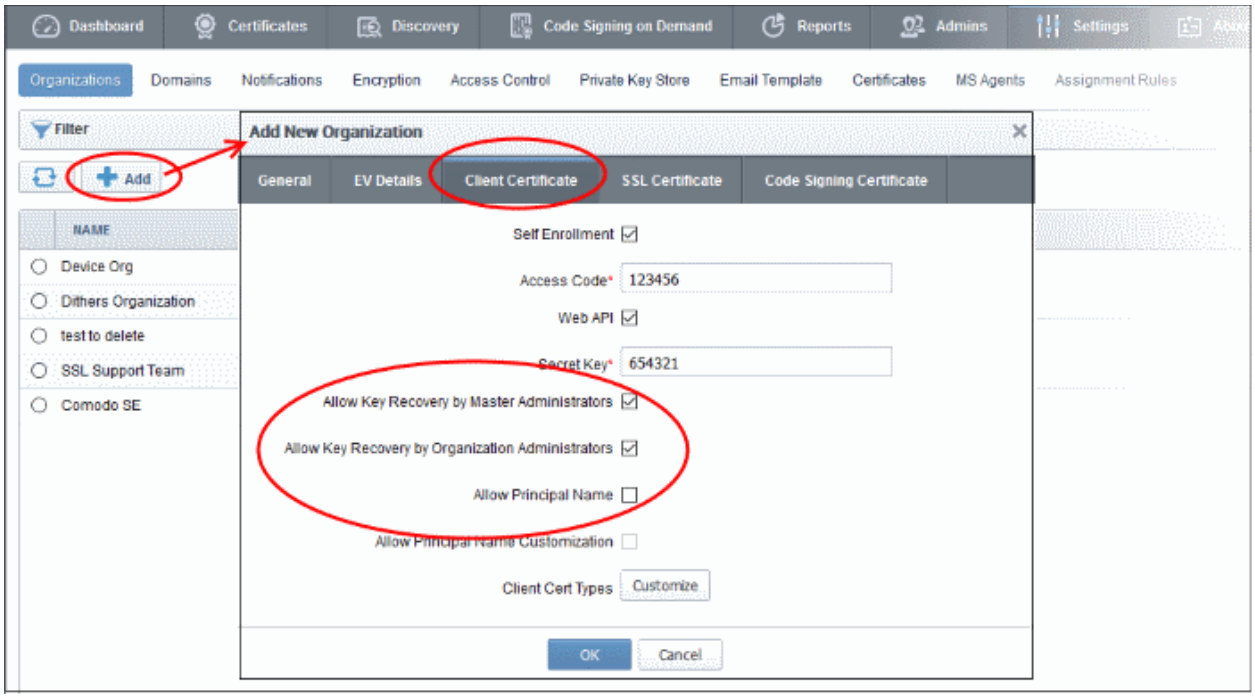
specific certificate. See "How to Recover an End-User's Private Key from Escrow" on page 483 for more information.

7.6.1 How to Configure Key Escrow for an Organization

Key recovery options are selected by a MRAO during the creation of an organization. Once configured, they cannot be modified.

You define the key recovery options as follows:

- From the main UI, navigate to **Settings > Organizations**, and then click **Add** to open the **Add New Organization** dialog, as shown in the following illustration.



- Select **Client Certificate** to view and configure the following key recovery options:
  - **Allow Key Recovery by Master Administrators**—If selected, the MRAO can recover the private keys of client certificates issued by this organization. At the time of creation, each client certificate is encrypted with the MRAO's master public key before being placed into escrow. In addition, if this option is selected, the organization cannot issue client certificate until the MRAO has initialized their master key pair in the **Encryption** tab.
  - **Allow Key Recovery by Organization Administrators**—If selected, the RAO can recover the private keys of client certificates issued by this organization. At the time of creation, each client certificate is encrypted with the RAO's master public key before being placed into escrow. In addition, if this option is selected, the organization cannot issue client certificate until the RAO has initialized their master key pair in the **Encryption** tab.
  - **Allow Principal Name**—If selected, the Principal Name support is enabled for the organization, in which case the client certificates issued to the end-users of the organization include an additional name—Principal Name—in addition to the RFC822 name in the **Subject Alternative Names (SAN)** field. If included, the Principal Name becomes the primary email address of the end-user to whom the certificate is issued.

This can be configured at a later time by editing the end-user if **Principal Name Customization** option is enabled for the organization or department.

- **Allow Principal Name Customization**—If selected, the customization of the principal names by the administrator is enabled.

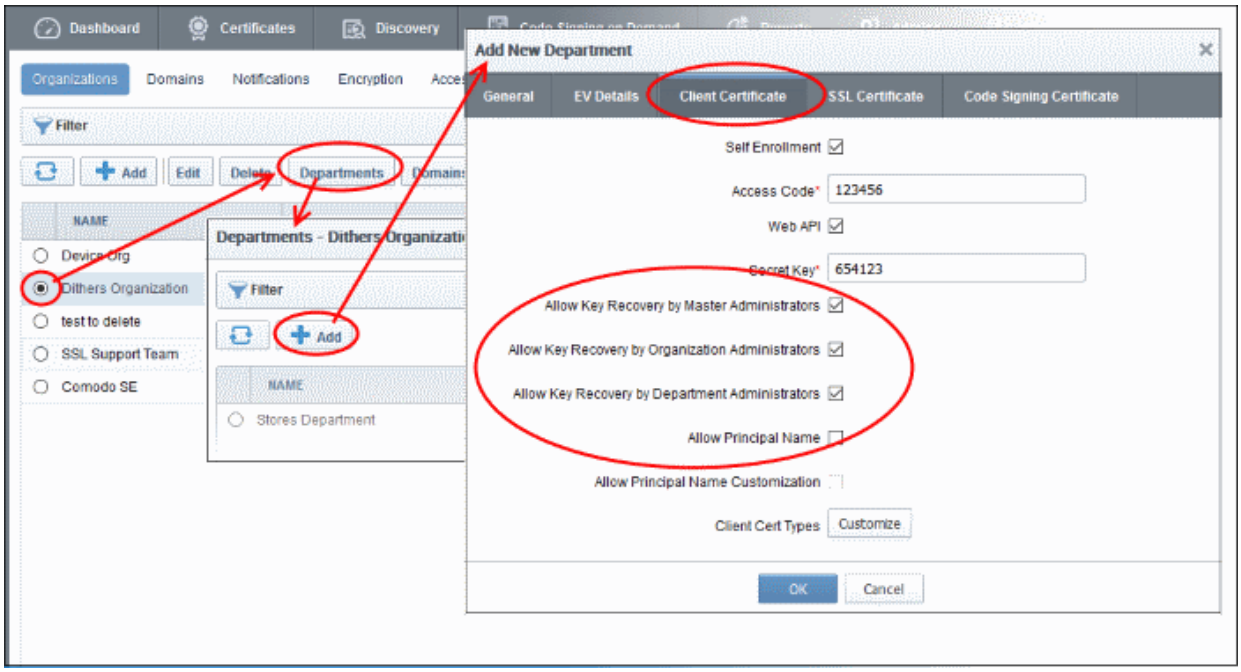
- Select **General** and complete its fields.
- Optionally, if required, complete fields in the **SSL Certificate** and **Code Signing Certificate** tabs.
- Click **OK** to add the organization.

7.6.2 How to Configure Key Escrow for a Department

Key recovery options are selected by a MRAO or RAO Client Certificate during the creation of the department. Once configured, they cannot be modified.

You define key recovery options as follows:

- From the main UI, navigate to **Settings > Organizations > Departments**, and then click **Add** to open the **Add New Department** dialog, as shown in the following illustration.



- Select **Client Certificate** to view and configure the following key recovery options. Note that these options are only active if a MRAO enabled the appropriate key recovery options when configuring client certificate options for the organization:
  - **Allow Key Recovery by Master Administrators**—If selected, the MRAO can recover the private keys of client certificates issued by this department. At the time of creation, each client certificate is encrypted with the MRAO's master public key before being placed into escrow. In addition, if this option is selected, the department cannot issue a client certificate until the MRAO has initialized their master key pair in the **Encryption** tab.
  - **Allow Key Recovery by Organization Administrators**—If selected, the RAO Client Certificate can recover the private keys of client certificates issued by this department. At the time of creation, each client certificate is encrypted with the RAO's master public key before being placed into escrow. In addition, if this option is selected, the department

cannot issue a client certificate until the RAO has initialized their master key pair in the **Encryption** tab.

- **Allow Key Recovery by Department Administrators**—If selected, the DRAO Client Certificate can recover the private keys of client certificates issued by this department. At the time of creation, each client certificate is encrypted with the DRAO's master public key before being placed into escrow. In addition, if this option is selected, the department cannot issue a client certificate until the DRAO has initialized their master key pair in the **Encryption** tab.
- **Allow Principal Name**—If selected, the principal name support is enabled for the department, in which case the client certificates issued to the end-users of the department include one more name—Principal Name—in addition to the RFC822 name in the **Subject Alternative Names (SAN)** field. If included, the principal name becomes the primary email address of the end-user to whom the certificate is issued. This can be configured at a later time by editing the end-user if **Principal Name Customization** option is enabled for the organization or department.
- **Allow Principal Name Customization**—If selected, the customization of the principal names by the administrator is enabled.

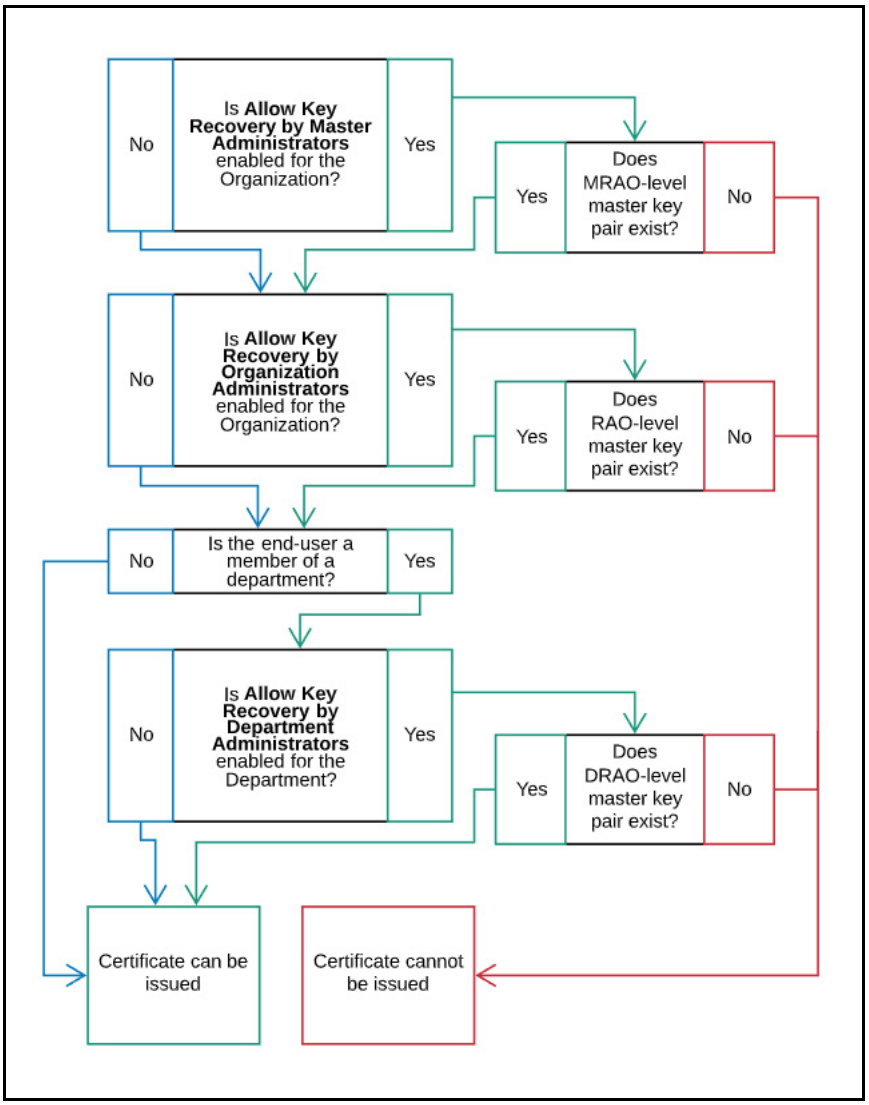
- Select **General** and complete its fields.
- Optionally, if required, complete fields in the **SSL Certificate** and **Code Signing Certificate** tabs.
- Click **OK** to add the department.

7.6.3 About the Master Keys Requirements for the Client Certificate Issuance

If a master key pair has not been initialized, then the organization or department cannot issue client certificates. If key escrow is required through all tiers (MRAO, Organization, and Department), then a master key pair must have been initialized for each level. To check the initialization status for their level, the currently logged-in administrator should select **Encryption**.

NOTE: Administrators can only see the initialization status of the master key pair for their own administrative level (Master, Organization, or Department).

The following illustration outlines the requirements for the master key pairs for the successful issuance of client certificates.



7.6.4 How to View and Configure Encryption Settings

The **Encryption** settings area shown in the following illustration allows MRAO, RAO Client Certificate, and DRAO Client Certificate administrators to encrypt the private keys of the end-users' client certificates. If key recovery was specified during the creation of an organization or department, then you must compete this configuration, as client certificates cannot be issued until the master key pairs have been initialized.

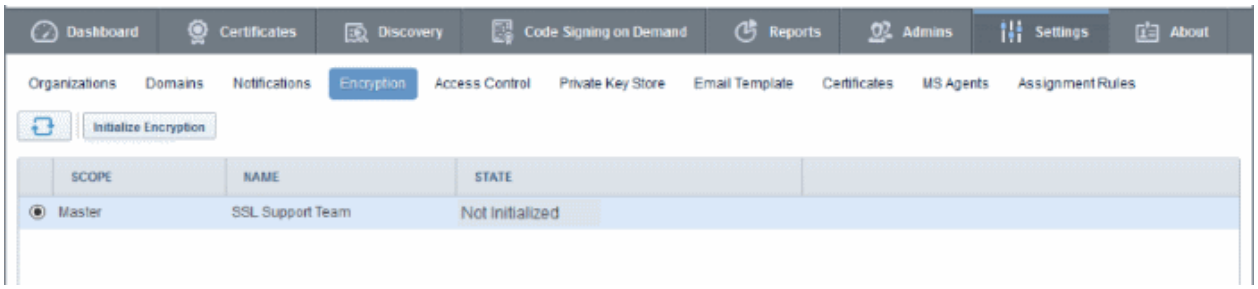
The following columns and controls are available:

- **Scope**—The hierarchy level of the organization or department. Valid values are Master, Organization, Department.
- **Name**—The name of the organization or department.
- **Status**—The status of private key encryption.
- **Refresh**—Reloads the list.

- **Initialize Encryption**—Starts the initial encryption process. This control is available only when the private key encryption has not been done earlier and the status is Not Initialized, for and organization/department.

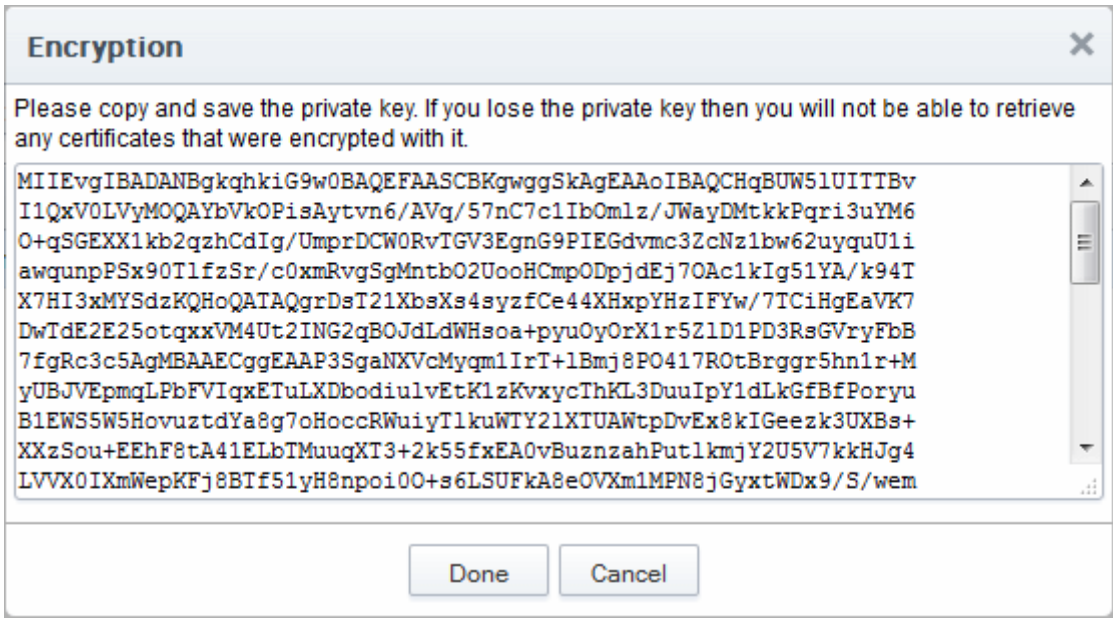
  The visibility of this control depends on the scope selections and the status of private key encryption.
- **Re-encrypt**—Starts the re-encryption process of the private keys of the certificates of the end- users of belonging to an organization/department. This control is available only if the private keys are already encrypted.

  The visibility of this control depends on the scope selections and the status of private key encryption.



7.6.5 How to Encrypt Private Keys

You can initialize the private key encryption by clicking **Initialize Encryption**, as described in "How to View and Configure Encryption Settings" on page 477. This starts the process and generates a master private key which you need to copy and paste in a `.txt` file, and then store in a secure location.



The master private key is not stored within SCM. It is recommended that the private key is saved key in a secure password-protected location. It is required if the administrator decides to either re-encrypt the keys or download the end-user's client certificate.

When you click **Done** on the **Encryption** dialog, the status is changed to Public key is loaded, as shown in the following illustration

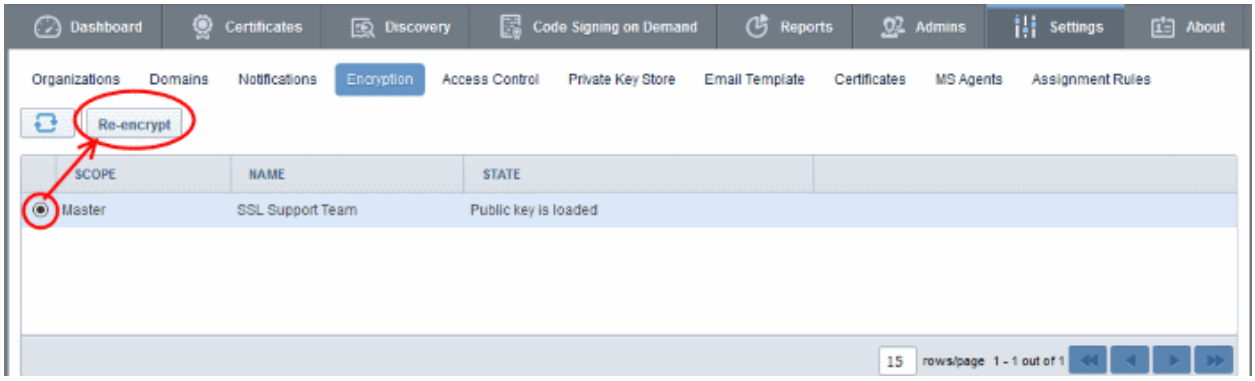
All the private keys of the end-user client certificates are now encrypted using the master public key of the administrator that began this process. Decryption requires the private key that was saved earlier.

7.6.6 How to Re-Encrypt Private Keys

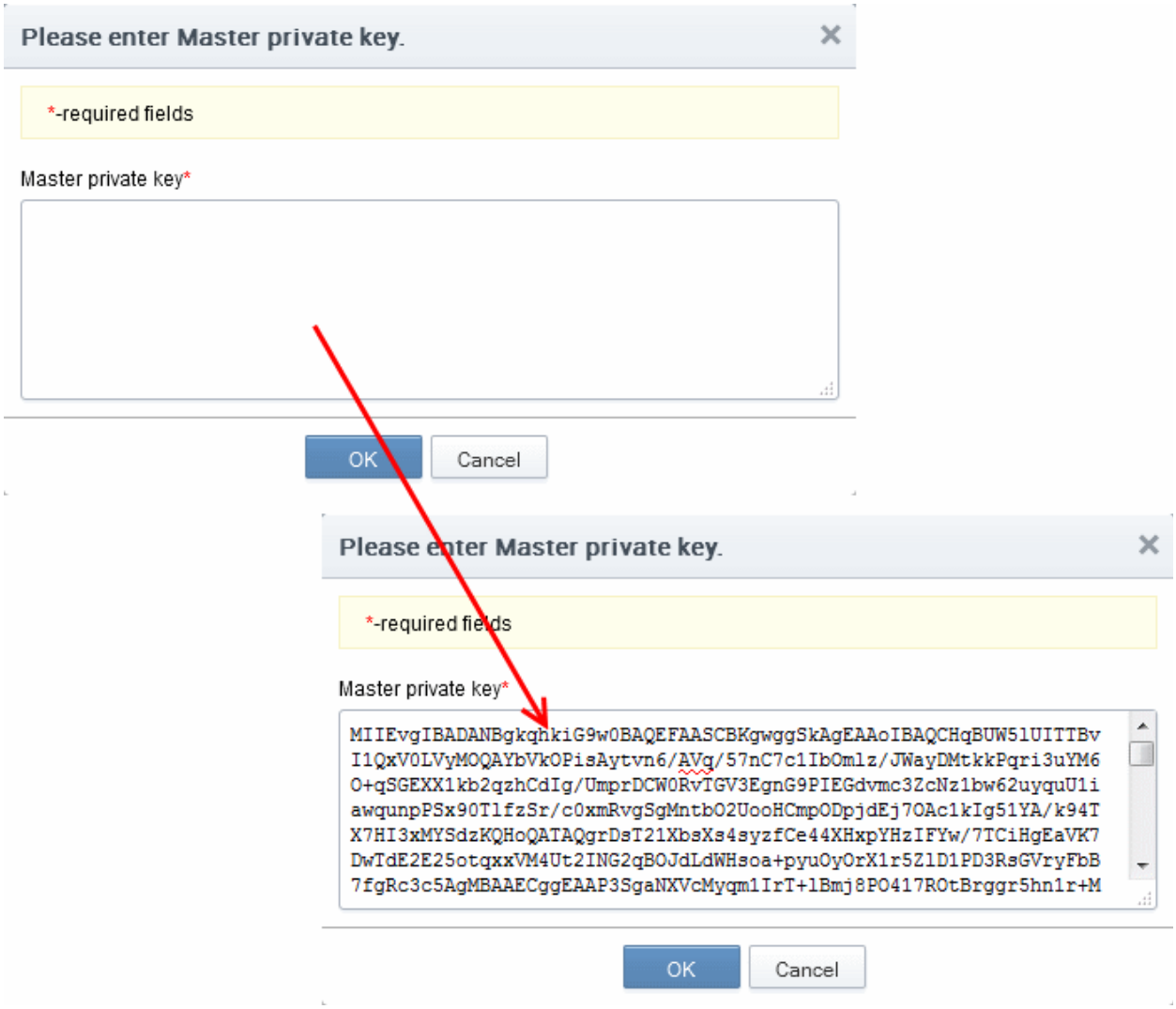
MRAO, RAO Client Certificate, and DRAO Client Certificate administrators can use re-encryption to change the master key pair and then automatically re-encrypt the existing end-user's key pairs with the new master public key. This may be necessary if the original private key becomes compromised or administrative personnel leave the company.

You perform re-encryption as follows:

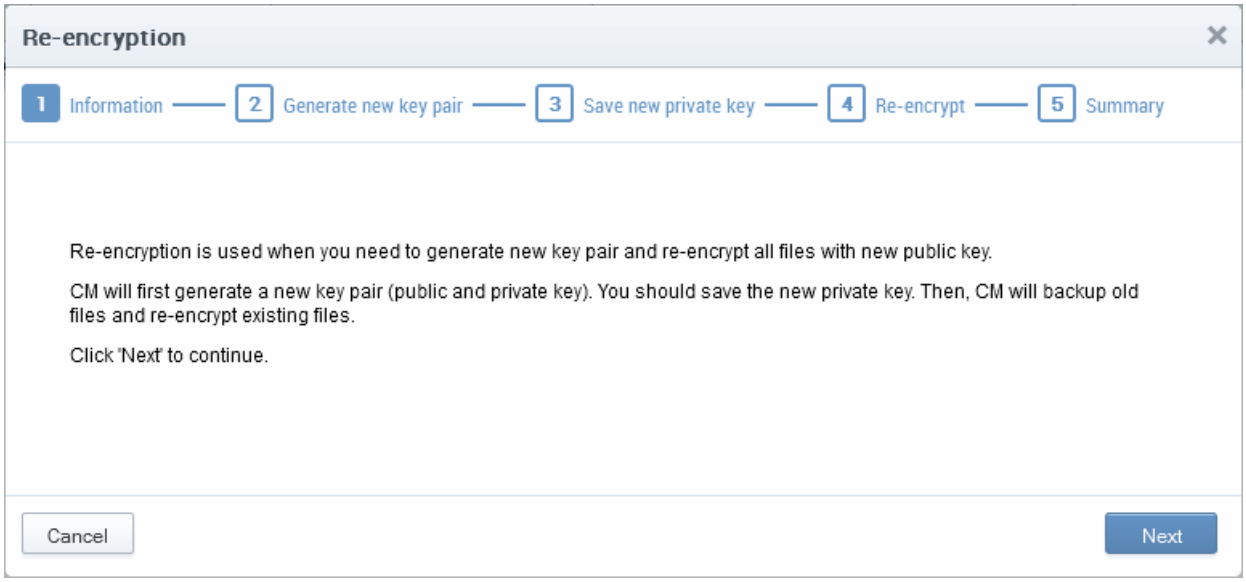
- Select the scope and click **Re-encrypt** for the organization or department, as shown in the following illustration.



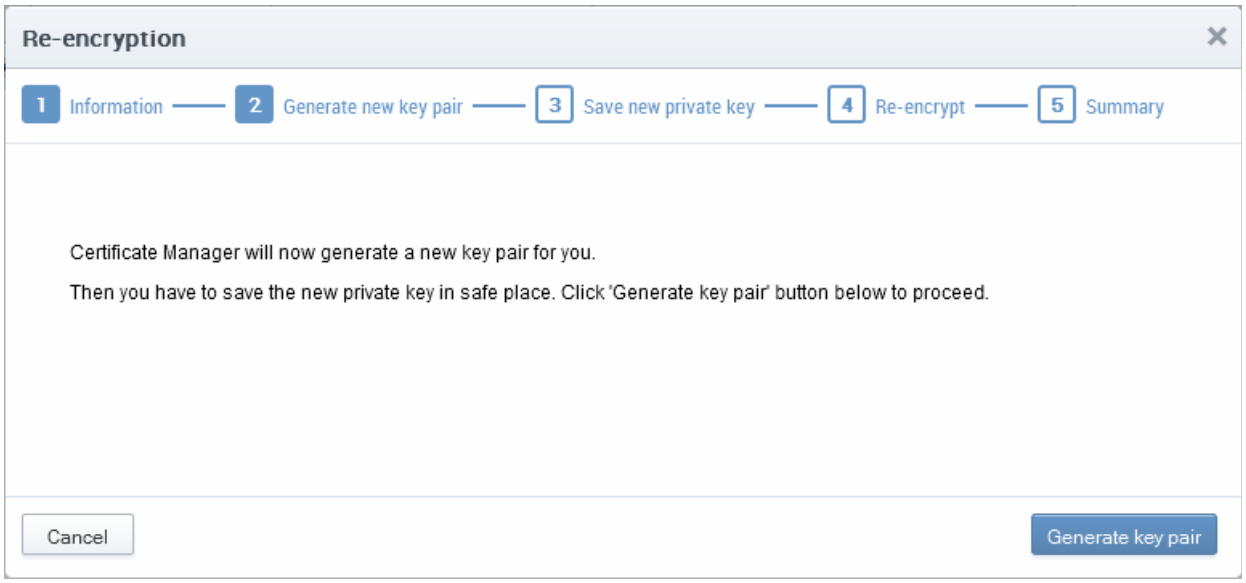
You are prompted to paste the existing master private key to start the process, as shown in the following illustration.



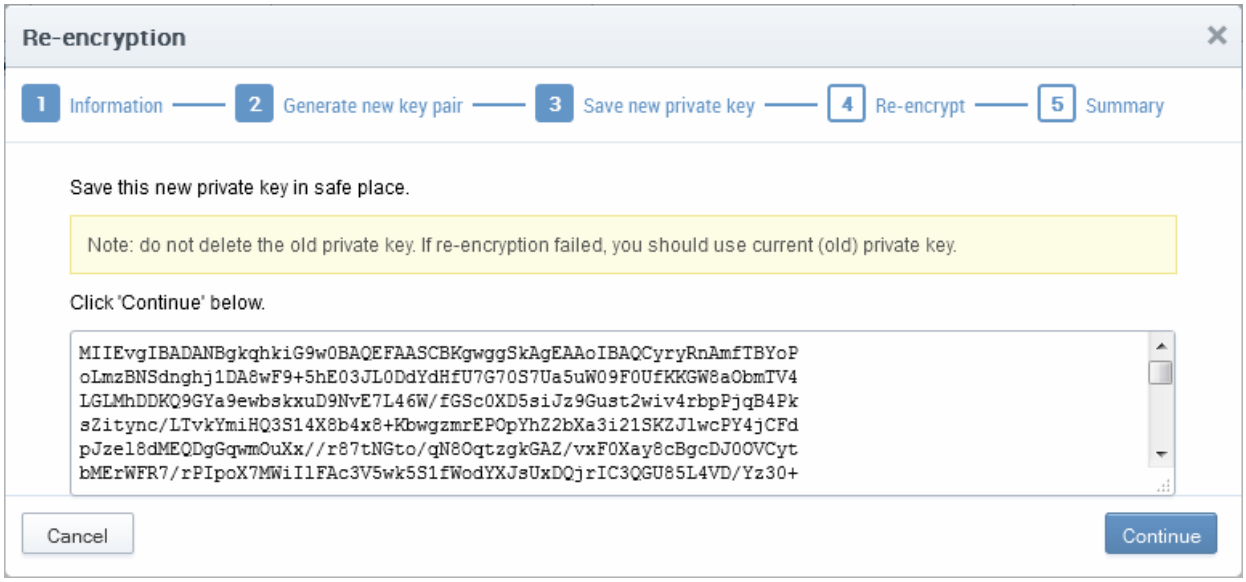
- Paste the master key and click **OK** to open the **Re-encryption** dialog shown in the following illustration.



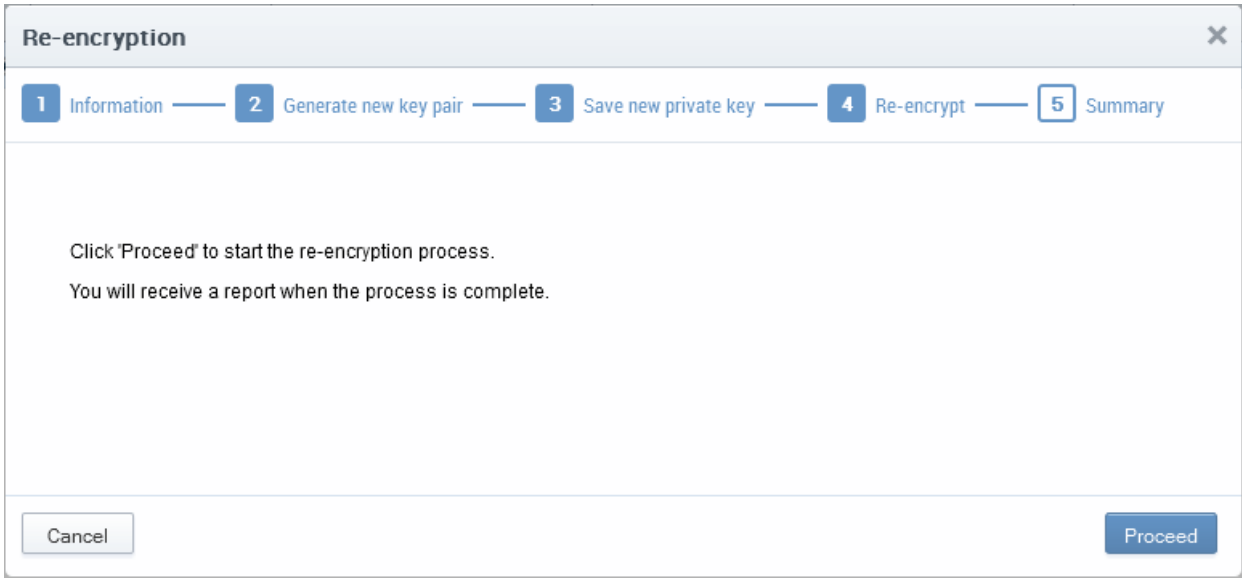
- Click **Next** to continue.



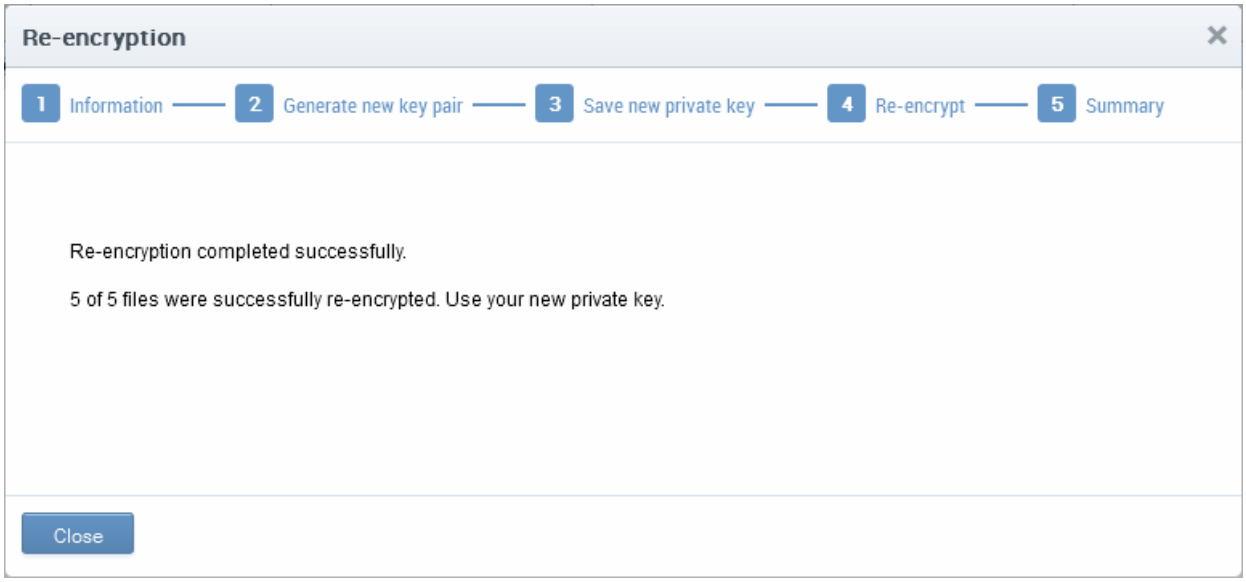
- Click **Generate key pair** to generate the new keys.



- Copy and paste the private key into a `.txt` file, then save it in a secure password-protected location, and then click **Continue** to start the re-encryption of the private keys.



- Click **Proceed** to begin re-encrypting the private keys of client certificates. Upon successful re-encryption, a summary screen shown in the following illustration is displayed.



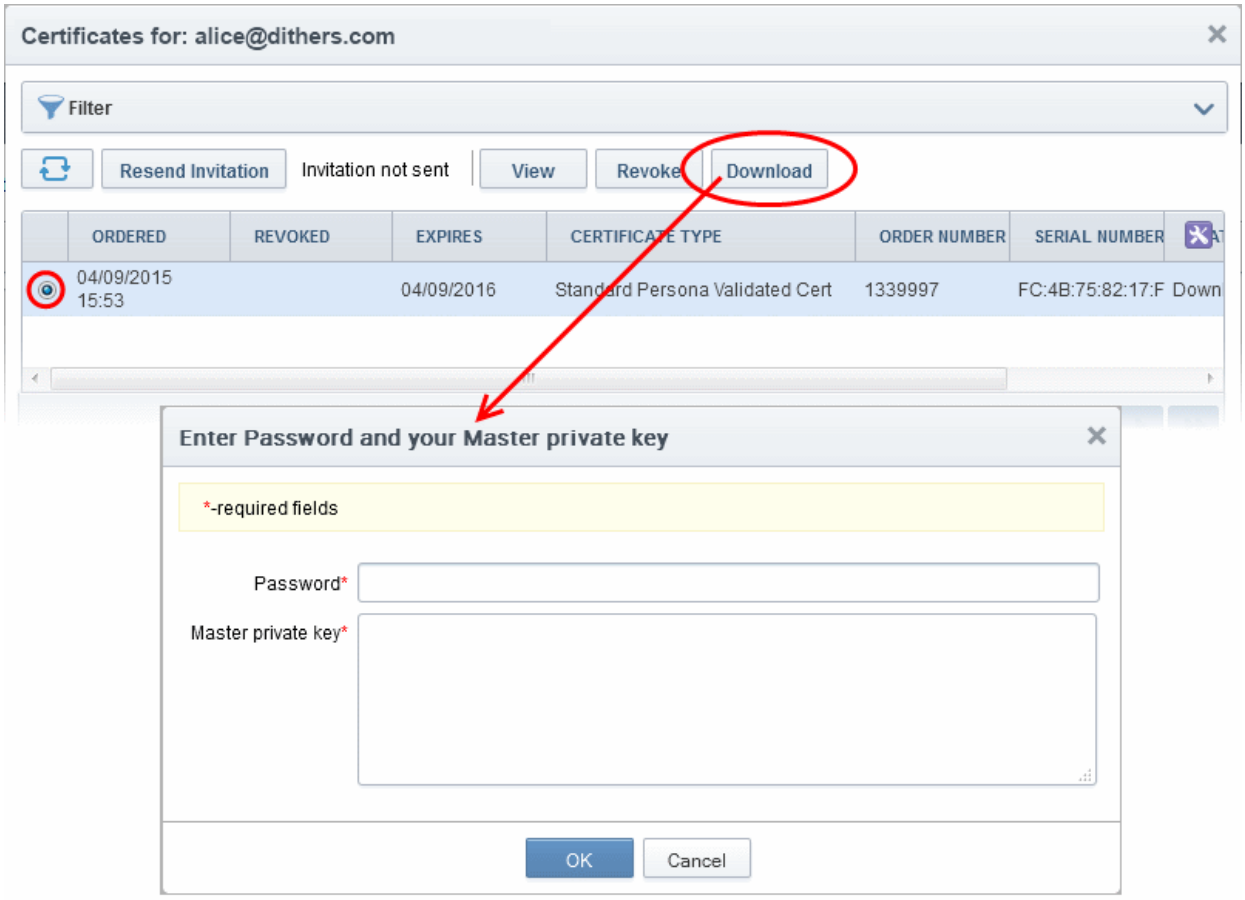
7.6.7 How to Recover an End-User's Private Key from Escrow

You may need to recover an end-user's private key in order to decrypt data if, for example, the original client certificate belonging to an end-user was lost or if the end-user left the company.

The end-user's private key can be downloaded as follows:

- Navigate to **Certificates > Client Certificates**, select the end-user and click **Certificates** to open the **Certificates for** dialog that contains the list of all the certificates belonging to the end-user, in chronological order of the issuance.
- Select the certificate and click **Download**.

You should have your master private key ready, as it is required to complete this process.



To decrypt the end-user's key pair, you paste the corresponding master private key into the space provided in order to download any end-user's client certificates. You can also set a password to protect access to the private key in a `.p12` file as well.

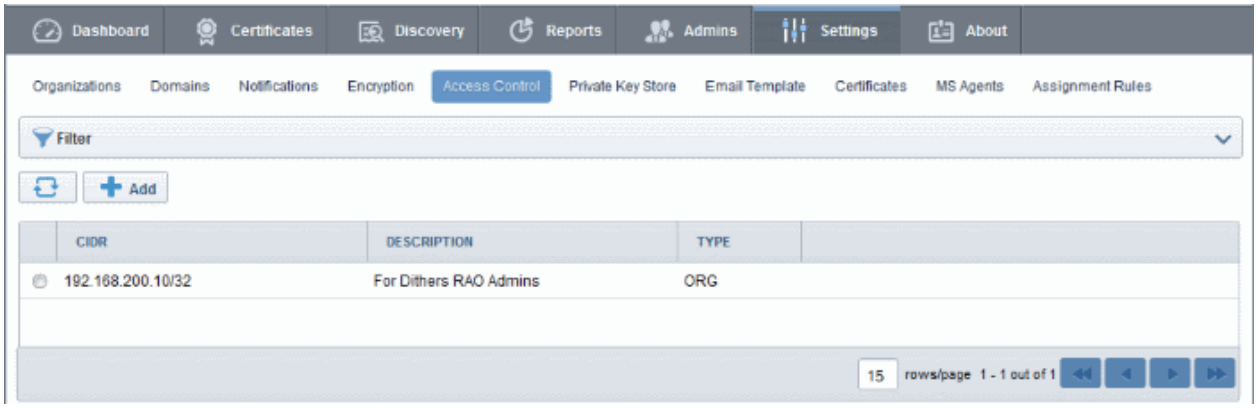
Successfully downloading the private key of a client certificate revokes that certificate.

7.7 Configuring Access Control

The **Access Control** settings area shown in the following illustration is visible only to MRAOs who can configure and limit incoming access to the SCM UI to certain IP addresses and ranges. This is used for granting access to certain IP addresses and therefore preventing unauthorized or unsecured access to the SCM UI.

After specifying one or more IP addresses or ranges in CIDR notation, only administrators attempting to login from these specified addresses are allowed access. Any user who is blocked from accessing the SCM UI because of restrictions is presented with a generic 403 Access Denied error.

The access restrictions can be applied for all administrators or selectively for MRAO administrators only, RAOs only, or DRAO administrators only.



The following columns and controls are available:

- **CIDR**—An IP range, as an IP address followed by network prefix. For example, 123.456.78.91/16.
- **Description**—A short description for the allowed CIDR.
- **Type**—The administrative role for which the CIDR is defined, such as All, MRAO, ORG (RAO)
- **Add**—Allows you to add a new IP range to allow access.
- **Refresh**—Updates the list of IP ranges.
- **Edit**—Enables you to edit CIDR's details.

  This control is visible only on selecting a CIDR entry.
- **Delete**—Enables you to delete the CIDR.

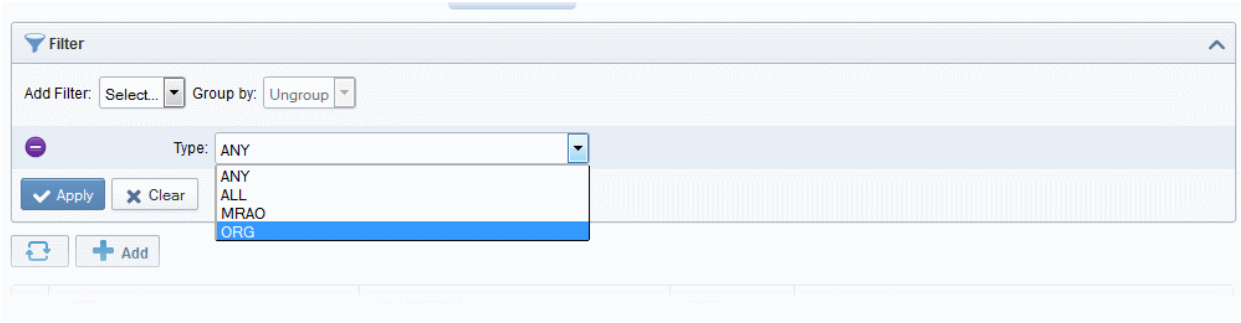
  This control is visible only on selecting a CIDR entry.

You can sort items in by clicking a column header and you can use filters to search for particular CIDR entries.

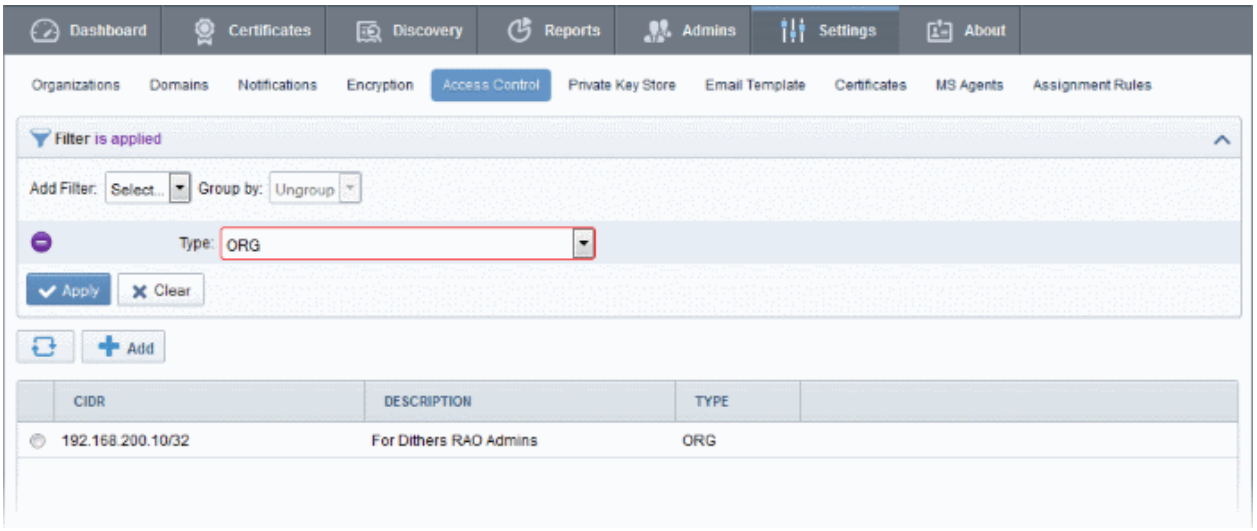
You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.

To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection from the Add Filter list.

The only available filter option for CIDR is **Type**, which enables you to filter the CIDR details based on administrative roles.



After the filters have been applied, filtered items based on the entered parameters are displayed, as shown in the following illustration.

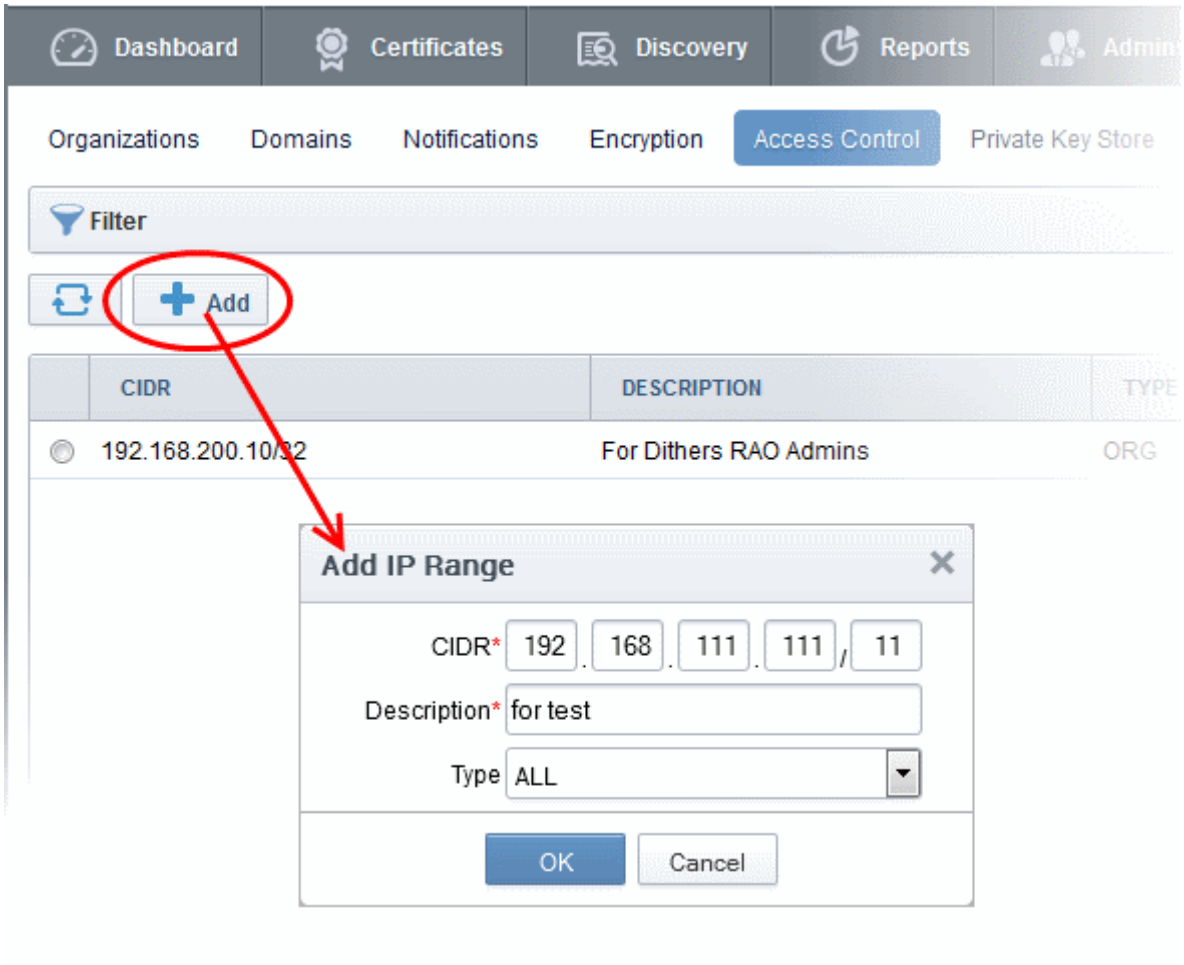


You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the **Access Control** screen, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

7.7.1 How to Add a New IP Range

You can add a new IP range by clicking **Add** on the **Access Control** area, as shown in the following illustration.



The following table lists settings and elements available in the **Add IP Range** dialog. Mandatory settings are marked by red asterisks.

Field	Description
CIDR	The incoming IP ranges followed by a network prefix from which the access to the SCM UI is to be granted. All other IP addresses are blocked. If no IP range is specified in the Access Control, then the default setting is to allow access from any IP.
Description	A short description of the IP range being added.

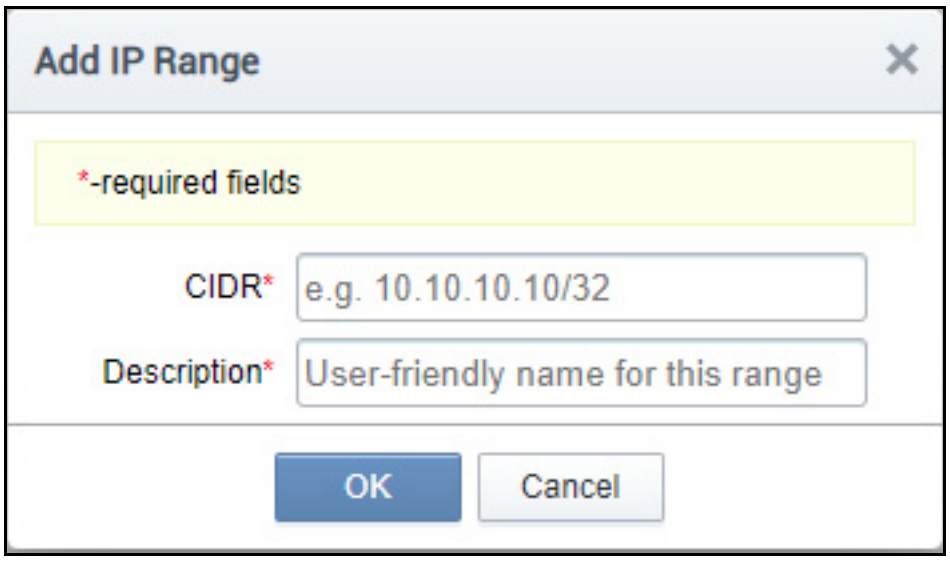
Field	Description
Type	Enables you to select whether the IP address restriction has to be imposed to all administrators, MRAO administrators, or RAO administrators. The valid values are the following: • All—The IP address-based access restriction is imposed for all administrators, including the MRAO administrator. • MRAO—The IP address-based access restriction is imposed only on the MRAO administrator. • ORG—The IP address-based access restriction is imposed on all RAO and DRAO administrators, but not the MRAO administrator.

Additions and changes to the access control list do not take effect for your current session; instead, they take effect on your next login.

The administrator can also configure and limit incoming access to the SCM UI to certain IP addresses and ranges for the organizations individually.

7.7.2 How to Modify and Delete an IP Range

You can modify an existing IP range by clicking **Edit** on the **Access Control** area, as shown in the following illustration.



Changes to the access control list do not take effect for your current session; instead, they take effect on your next login.

To remove a CIDR entry, select it and click **Delete**.

7.8 Configuring a Private Key Store

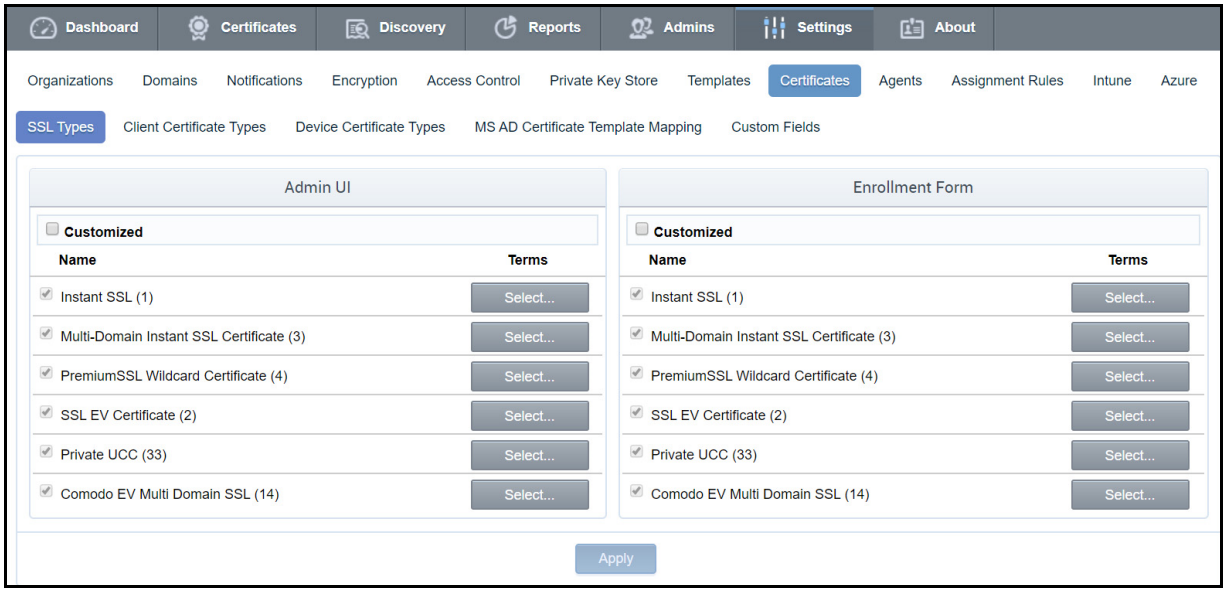
SCM enables MRAOs to create and maintain a secure Private Key Store (PKS) on their local network.

For more information, see "Configuring the Private Key Agent" on page 306

7.9 Configuring Certificates

The **Certificates** area shown in the following illustration allows MRAO administrators to configure the type and validity period (term) of certificates available to SCM organizations via a built-in application form and self-enrollment form. MRAOs can use the **Custom Fields** sub-area to add fields to these forms, assuming this feature is enabled for their account with Sectigo.

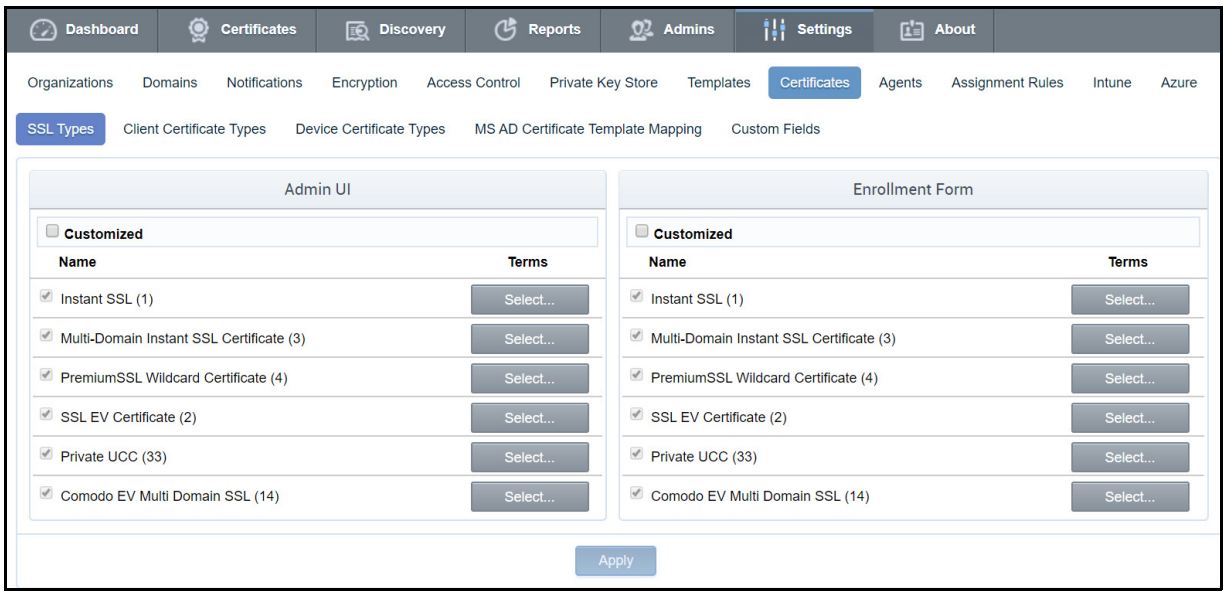
In addition, the **Certificates** area allows administrators to map Microsoft AD templates to SCM certificate types in order to issue device and private UCC SSL certificates. For more information, see "How to Map MS AD Certificate Templates to SCM Certificate Types" on page 277.



NOTE: Each SSL Type has a unique SSL ID assigned to it. These IDs are required for certain REST operations and are indicated in brackets beside each SSL Type.

7.9.1 How to Configure SSL Certificate Types

The **SSL Types** area shown in the following illustration allows MRAO administrators to configure the types and terms of SSL certificates available to SCM organizations in the built-in and self-enrollment application forms. It can be useful to limit the types of certificates available in order to simplify the certificate selection procedure for end-users on the forms.



The **Admin UI** pane specifies SSL certificate types that are to be available to applicants using the built-in application form.

The **Enrollment Form** pane specifies SSL certificate types that are to be available to applicants using the self-enrollment form. It is possible to make different certificates available via the built-in wizard than those available through the self-enrollment form.

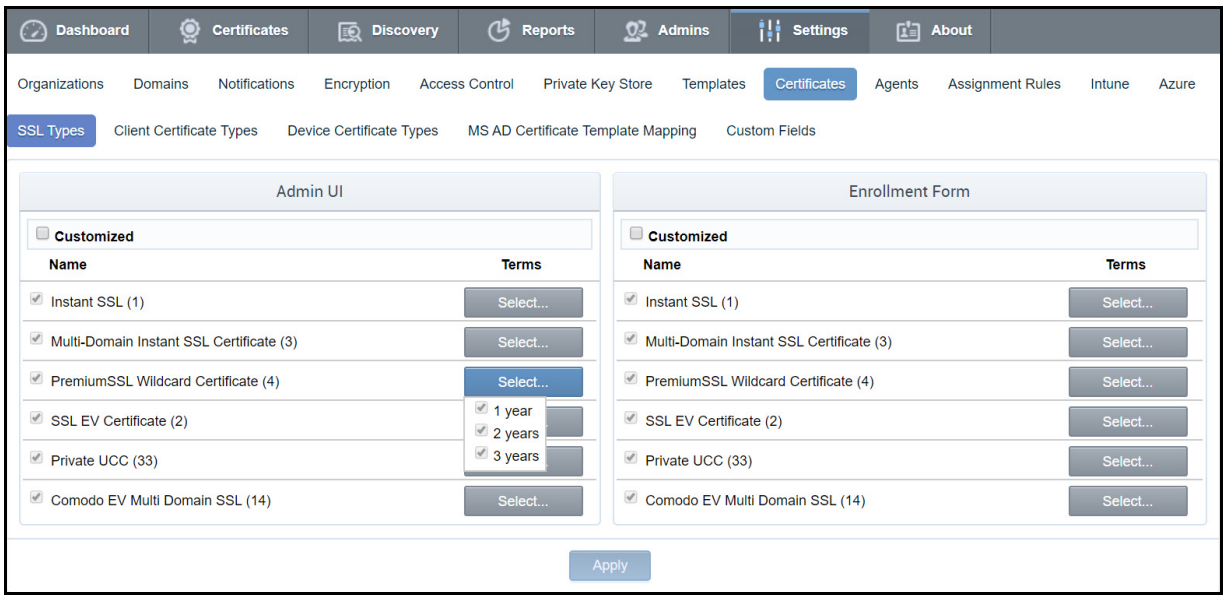
The following table lists settings of the **SSL Types** area.

Field	Description
Customized	Enables customization of the SSL types. If not selected (default), all certificate types are available through both the built-in application form and the self-enrollment form.
Name	SSL types that are assigned to your account by your account manager. If a certificate or its validity period is not present, you should contact your account manager to have it added.
Terms	Validity periods available for the certificate type.

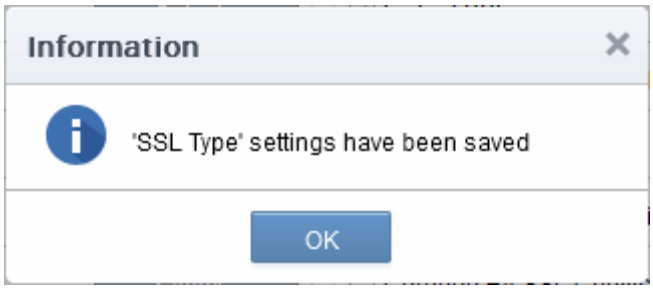
7.9.1.1 Customizing SSL Certificate Types

MRAO administrators can restrict the SSL certificate types and their validity periods as follows:

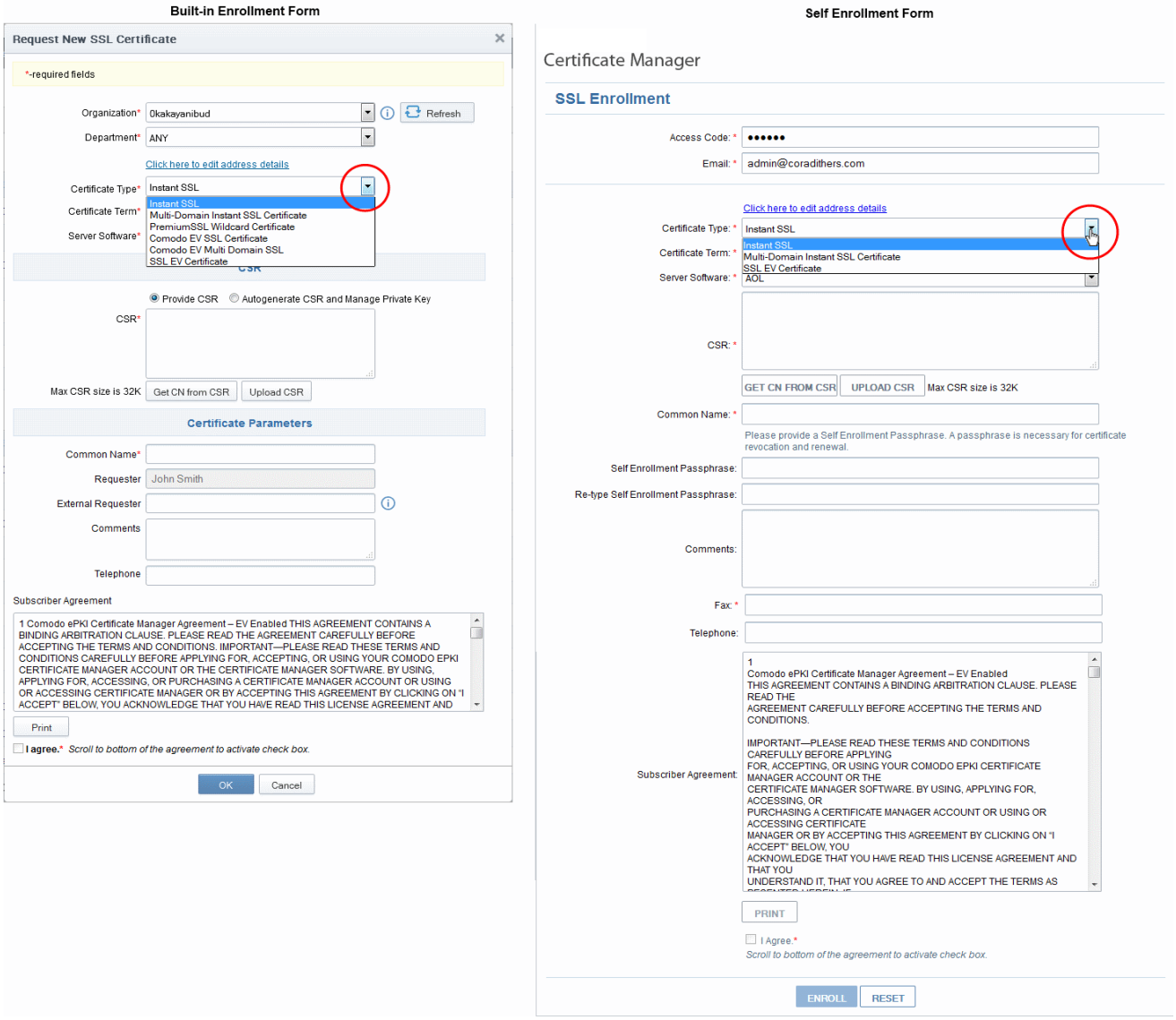
- Select **Customized** in either the **Admin UI** pane (for enrollments via a built-in application form) or **Enrollment Form** pane (for enrollments via a self-enrollment form).
- Select the names of the certificates to be available.
- Click **Select** next to the certificate whose validity periods are to be available, as shown in the following illustration.
- Click **Apply**.



The confirmation dialog shown in the following illustration informs you that your changes have been saved.



Only the types and validity periods of SSL certificates that are selected in the **SSL Types** area are available in the **Type** and **Term** lists of the built-in application form and the self-enrollment form, as shown in the following illustration.



The selection of SSL certificate types and their validity periods applies to all organizations. To restrict SSL certificate types for a specific organization, see "Customizing SSL Certificate Types for an Organization" on page 349.

7.9.2 How to Configure Client Certificate Types

Sectigo offers different client certificate types for different purposes, depending on the Key Usage Templates (KUTs) bound to the certificate. KUTs can be applied to client certificates for the purposes of Signing Only, Encryption Only, Dual Use (Signing + Encryption) or Smart Card Logon and Authentication.

The following table presents a sample of available KUTs for client certificate types.

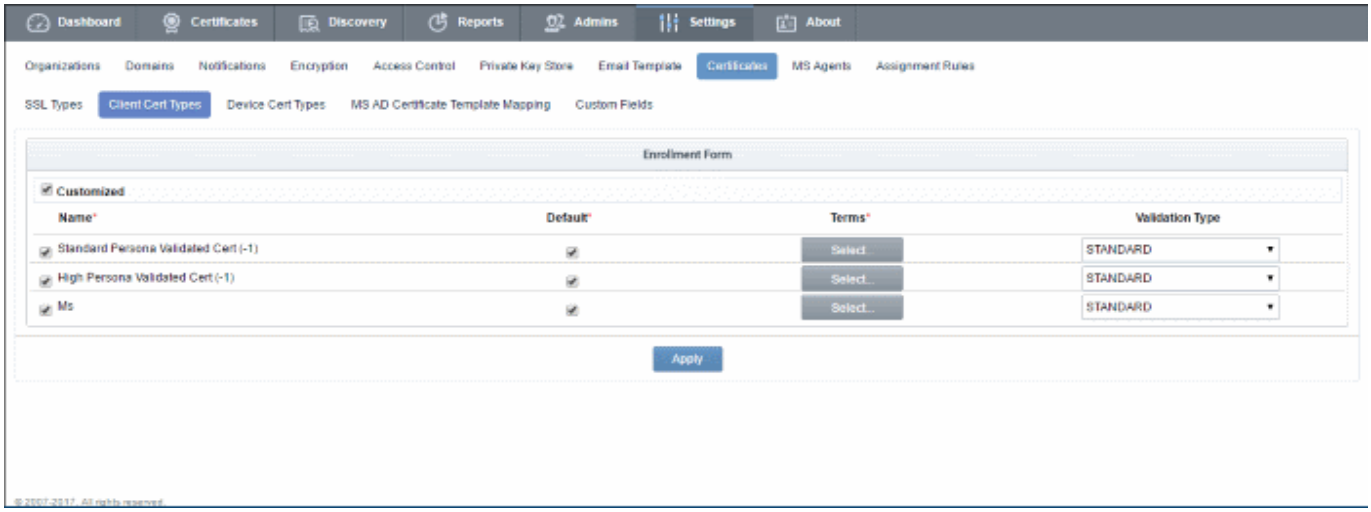
Name	Purpose
Signing Only	Digital signing.
Dual Use	Digital signing and encryption.
Encryption Only	Encryption and decryption only.
Authentication Only	Authentication only.
Sectigo Dual Use	Dual use certificates (digital signing and encryption), as defined by Sectigo Certification Practice Statement (CPS).
SOAP Signing & Encryption	Digital signing and encryption of SOAP messages.
Data Encipherment	Data encipherment.
AD User	Authentication to AD server.
Smart Card Logon and Authentication	For use with smart card login and authentication.
EFS	Encryption of files.

MRAO administrators can request their Sectigo account manager to create and enable client certificates of multiple types for their account.

It is also possible to create custom client certificate types by applying a single KUT or selected combinations of them.

The **Client Certificate Types** area shown in the following illustration display the list of client certificate types enabled for the account and allows the MRAO administrator to customize the types of client certificates and their validity periods that are available for end-users for all organizations and departments through a self-enrollment form (both access code-based and secret ID-based).

It can be useful to create a targeted certificate roster, as it simplifies the certificate selection procedure at the application forms and helps avoid applications for certificates which are inappropriate.



The following table lists the settings and elements of the **Client Certificate Types** area.

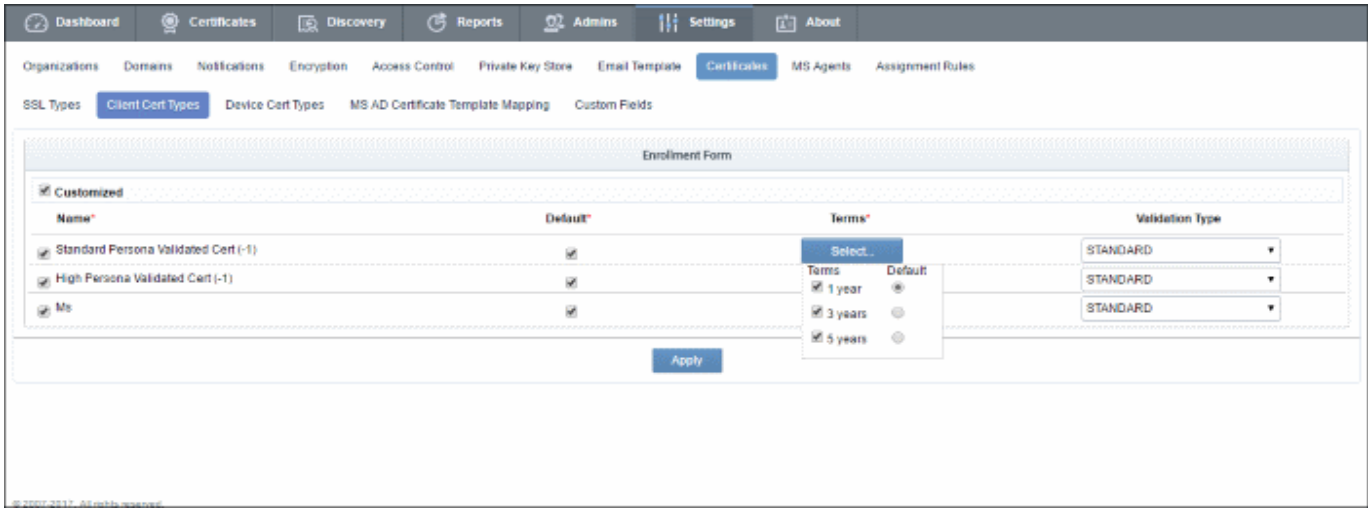
Field / Element	Description
Customized	Enables customization of the client certificate types. If not selected (default), all certificate types are available through both the built-in application form and the self-enrollment form.
Name	Client certificate types that are assigned to your account by your account manager. If a certificate or its validity period is not present, you should contact your account manager to have it added.
Default	Enables setting the certificate type as default type for the organizations. The client certificate types for which the default is selected become default options in the self-enrollment forms when applying for client certificate by end-users. At least one certificate type has to be selected as default type.
Terms	Validity periods available for the certificate type.

Field / Element	Description
Validation Type	The type of validation to be applied to the end-user. The valid values are Standard and High. The difference between the two lies in the degree of end-user authentication carried out prior to the certificate issuance. Standard validation type can be completed quickly and takes advantage of the end-user authentication mechanisms that are built into SCM. Under the Standard Personal Validation type, the end-user is authenticated using the following criteria: • The end-user must apply for a certificate from an email address at a domain that has been delegated to the issuing organization. • The organization has been independently validated by a web- trust-accredited CA, as the owner of that domain. • The end-user must know either a unique access code or secret ID that should be entered in the certificate enrollment form. These have been communicated by the administrator to the end-user via email. • The end-user must be able to receive an automated confirmation email sent to the email address of the certificate for which they are applying. The email should contain a validation code that the end-user needs to enter in the certificate collection web page. High validation type requires the end-user to undergo the validation steps listed above and face-to-face meeting with the issuing organization. Additional validation steps must be completed prior to the administrator selecting High personal validation type.

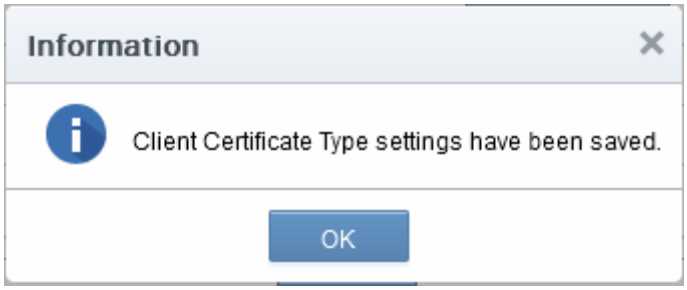
7.9.2.1 Customizing Client Certificate Types

MRAO administrators can specify client certificate types as follows:

- Select **Customized** in the **Client Certificate Types** area shown in the following illustration.
- Select the certificates to be available.
- Optionally, select **Default** to display this certificate type as the default option in both the access code-based and secret ID-based self-enrollment forms.
- Click **Select** next to the certificate whose validity periods are to be available, as shown in the following illustration. To set the selected validity period as default for the selected certificate type, select the **Default**.
- Select the validation type.
- Click **Apply**.



The confirmation dialog shown in the following illustration informs you that your changes have been saved.



Only the types and validity periods of client certificates that are selected in the **Client Certificate Types** area are available in the **Type** list of the self-enrollment form.

The selection of client certificate types defined in this area applies to all organizations. To restrict client certificate types for a specific organization, see "Customizing SSL Certificate Types for an Organization" on page 349. The certificate types or validity periods that are disabled in this area are not available even in the **Bind Client Certificate Types** area. To add a specific certificate type or validity period for a particular organization. It is recommended that RAO SSL administrators seek advice of a MRAO administrator.

7.9.3 How to Configure Device Certificate Types

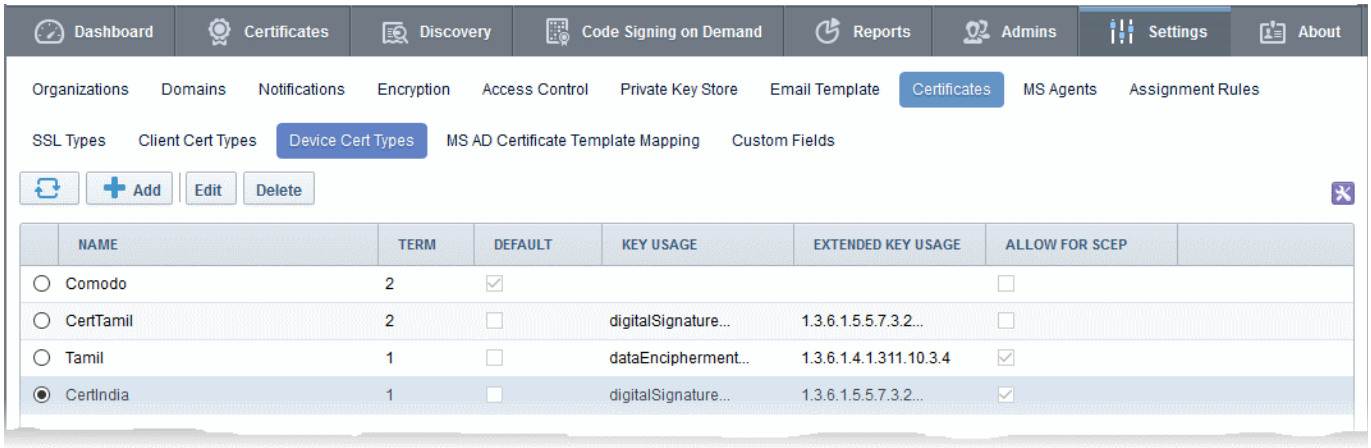
In addition to issuing device certificates via AD and API, SCM allows MRAO administrators to add device certificates from private certificate authorities. These certificates can be requested by applicants through self-enrollment forms or enrolled through SCEP. Certificates from private CAs, if enabled for your account, also can be deployed via the API.

The capabilities of a device certificate are determined by the KUTs bound to it. For example, device certificate types can be created for Digital Signing, Non Repudiation purposes, and so on.

The following table presents a sample of available KUTs for device certificate types.

Name	Purpose
Key Usage	
Data Encipherment	Data encryption
Digital Signature	Digital signing
Key Agreement	Key agreement
Key Encipherment	Key encryption
Non Repudiation	Non repudiation
Extended Key Usage	
Client Authentication	User authentication
Email Protection	Digital signature, key agreement, non-repudiation, key encipherment
MS Smart Card Logon	Smart card authentication
MS Encrypted File System	Encryption of files

MRAO administrators can specify device certificate types via the **Device Certificate Types** area shown in the following illustration.



The following table lists the settings and elements of the **Device Certificate Types** area.

Field / Element	Description
Name	The name of the device certificate.

Field / Element	Description
Term (days)	The validity period of the device certificate.
Default	A default device certificate is added in order for the device certificate feature to be active. This is usually done by Sectigo at the time of activation. This default certificate is available via self-enrollment.
Key Usage	The cryptographic purposes for which the certificate can be used. For example, data encipherment and digital signing.
Extended Key Usage	Higher level capabilities of the certificate. For example, client authentication, email protection.
Allow for SCEP	Indicates whether or not the device certificate type can be obtained through a SCEP enrollment.
Add [a]	Allows you to add a new device certificate type.
Edit [b]	Allows you to update the device certificates.

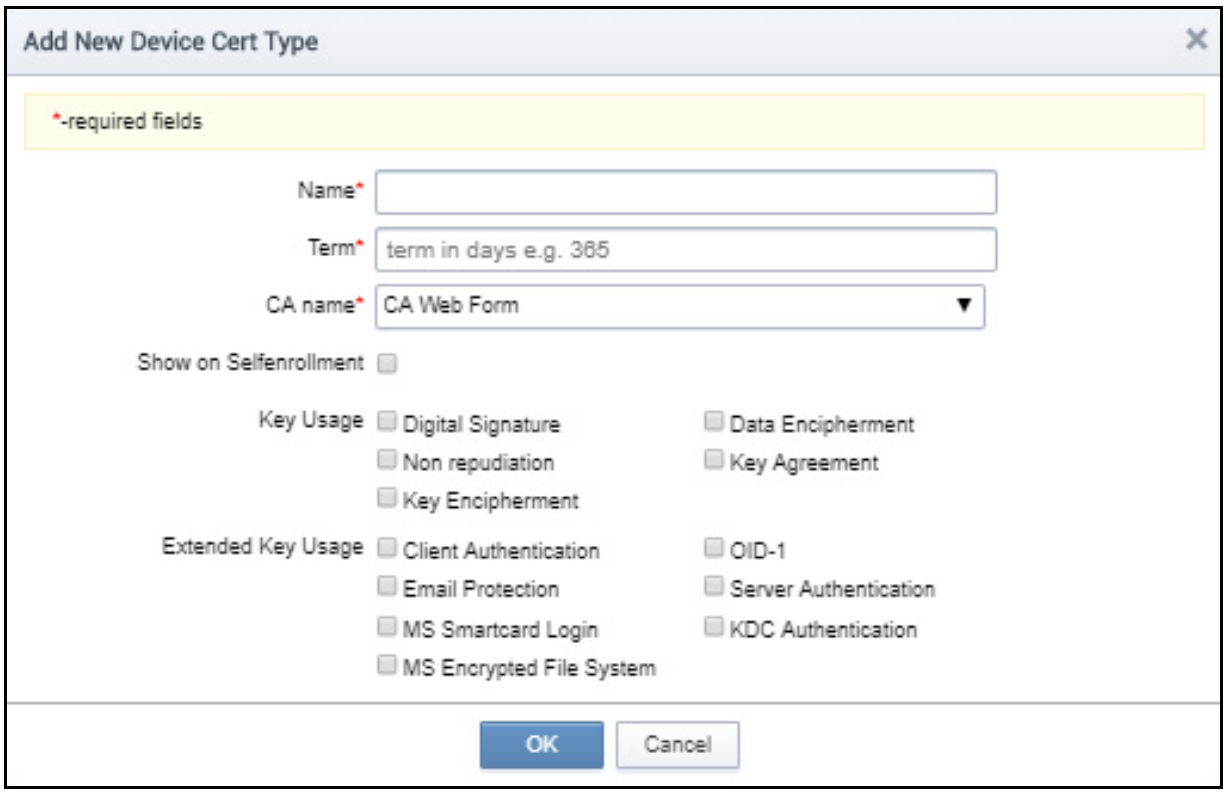
a. The type of control buttons that are displayed above the column header depends on the status of the selected certificate.
b. See the footnote for Add.

Clicking the column headers sorts the column items.

7.9.3.1 Adding Device Certificate Types

MRAO administrators can add new device certificate types for self-enrollment as follows:

- From the main UI, navigate to **Settings > Certificates > Device Certificate Types**.
- Click **Add** to open the **Add New Device Certificate Type** dialog shown in the following illustration.
- Complete the dialog using field descriptions provided in the following table.



Field	Description
Name	The name for the device certificate.
Term (days)	The validity period of the device certificate.
CA Name	The private CAs that are added for your account.
Allow for SCEP	Enables enrollment via SCEP for this device certificate type.
Show on Self Enrollment	Enables device certificates of this type to be available for selection in the self-enrollment form for device certificates.
Key Usage and Extended Key Usage	Determines the cryptographic capabilities of the device certificate.

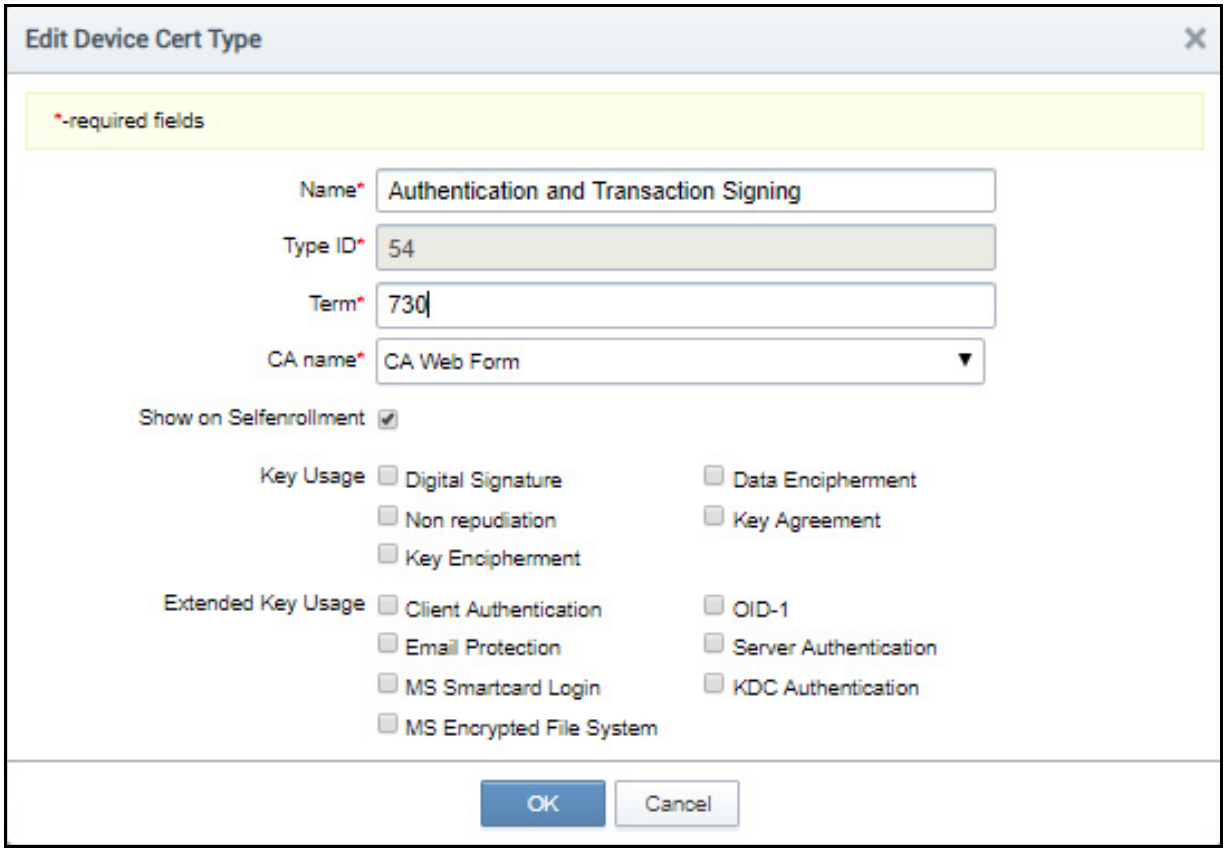
After clicking **OK**, the new device certificate type is added as configured and is available for enrollment via the self-enrollment form, API integration, and SCEP.

7.9.3.2 Modifying and Deleting a Device Certificate Type

MRAO administrators can modify or delete a device certificate type in the list, unless it is the default device certificate type, as follows:

- From the main UI, navigate to **Settings > Certificates > Device Certificate Types**.

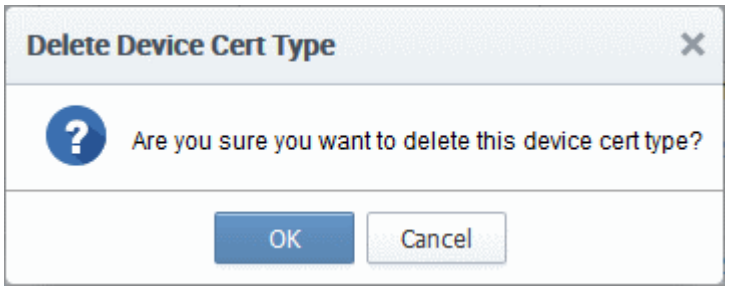
- Select the certificate type and click **Edit** to open the **Edit Device Certificate Type** dialog shown in the following illustration.
- Complete the dialog using field descriptions provided in the following table.



The **Edit Device Certificate Type** dialog is similar to the **Add New Device Certificate Type** dialog described in "Adding Device Certificate Types" on page 498, except an additional **Type ID** field which displays the auto-generated read-only number for that certificate type. Other fields can be edited.

After you click **OK**, certificates already issued and installed for this updated device certificate type are not affected.

To delete a device certificate type, select it and click **Delete**. A confirmation dialog shown in the following illustration is displayed.



Certificates already issued and installed for the deleted device certificate type are not affected.

7.9.4 How to Define Custom Fields

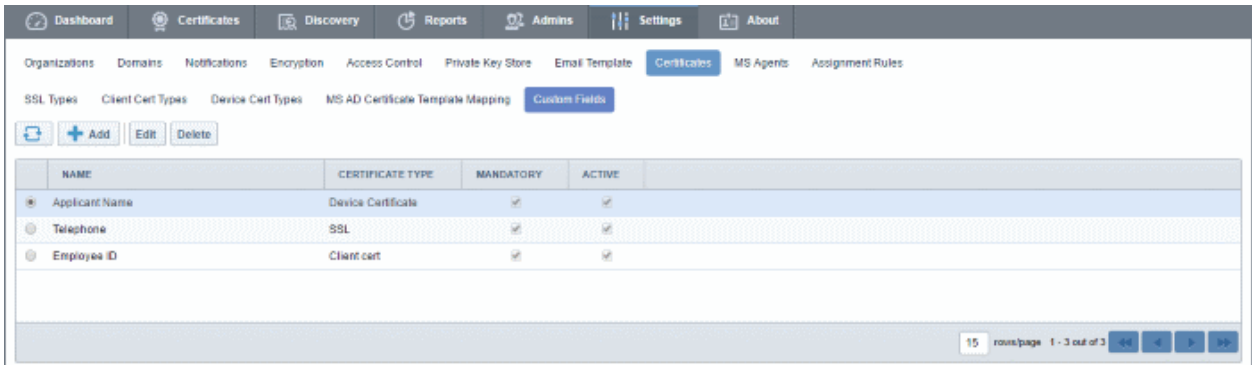
An SSL certificate, client certificate, or device certificate has a set of standard fields that contain information about the owner, domain, organization, department, address, and so on. Some businesses may wish to also track additional information such as, for example, an employee code, telephone number, and so on. SCM allows customers to include such additional information by adding custom fields to enrollment forms, assuming this functionality is enabled for the customer account.

MRAO administrators can add these fields to the enrollment forms of both SSL and client certificates. They can also specify whether the new fields should be mandatory or optional.

MRAOs can configure custom fields by navigating to **Settings > Certificates > Custom Fields** from the main UI, as shown in the following illustration. The name of the field, the certificate type to which it should apply (SSL, client or device certificates), whether or not the field should be mandatory and whether or not the custom field should be active are all configurable settings.

Custom fields can be edited at any time. Deactivating a custom field removes it from the enrollment forms, however all associated data is retained. Deleting a field deletes all data associated with the field.

Once added, the custom fields appear on the enrollment and renewal forms for the certificates.



The following table lists settings and elements of the **Custom Fields** area.

Field / Element	Description
Name	The name of the custom field.
Certificate Type	The type of the certificate to which the custom field is applicable. The valid values are SSL, Client Certificate, Device Certificate.
Mandatory	Defines whether the field is mandatory or optional.

Field / Element	Description
Active	Defines whether the custom field is active or inactive. If inactive, it is hidden in the future application forms. However, existing data for this field is retained in the database.
Add	Allows you to add a new custom field.
Refresh	Updates the currently displayed list of custom fields.
Edit [a]	Allows you to edit the parameters of a particular custom field.
Delete [b]	Deletes the custom field. Unlike deactivation, deleting a field also deletes all data associated with this field.

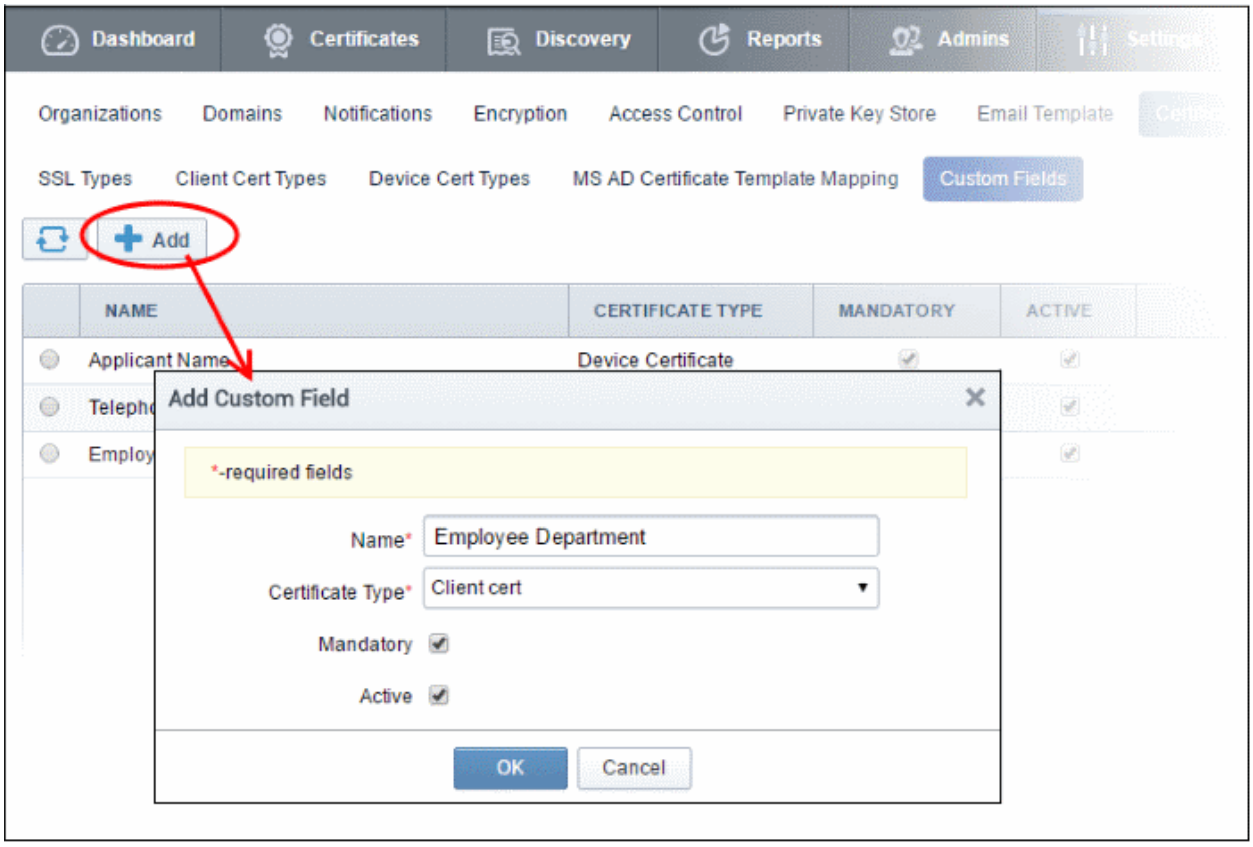
a. Controls appear only after selecting a particular custom field.
b. Controls appear only after selecting a particular custom field.

7.9.4.1 Adding a New Custom Field

An MRAO administrator can add custom fields for SSL, client, and device certificate types. The new fields are displayed in the self-enrollment and built-in application forms of the chosen certificate type.

You add a new custom field as follows:

- From the main UI, navigate to **Settings > Certificates > Custom Fields**.
- Click **Add** to open the **Add Custom Field** dialog shown in the following illustration.
- Complete the dialog using field descriptions provided in the following table.



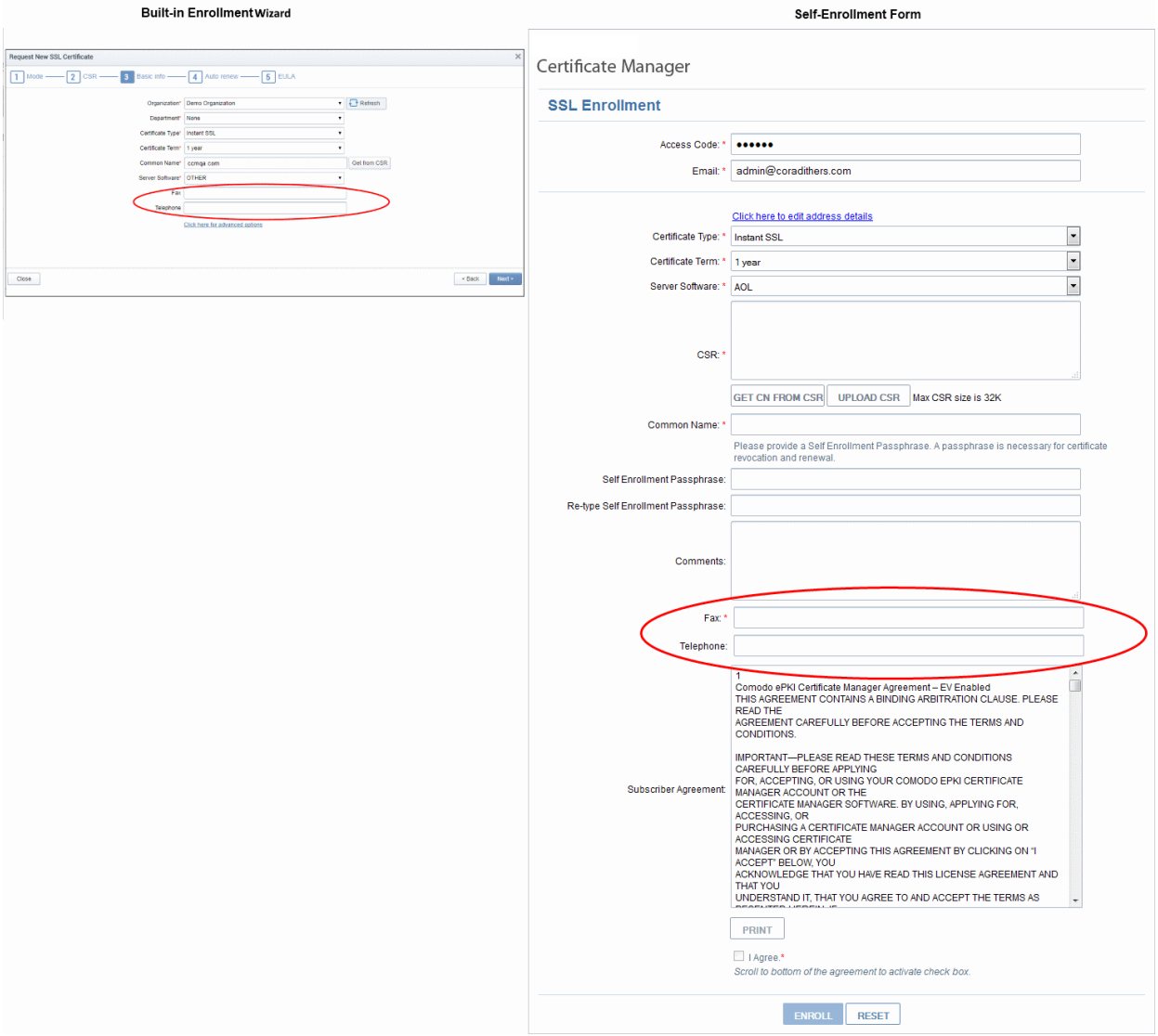
Field	Description
Name	The name of the field to be added. Maximum length is 256 characters. This becomes the label of the field on the enrollment form.
Certificate Type	The certificate type to which the new field should apply.
Mandatory	Indicates whether the field is mandatory or optional.
Active	Activates or deactivates the field. Deactivating a custom field removes it from the enrollment forms but all associated data is retained.

After completing the **Add Custom Field** dialog, click **OK**. If you selected Active, the new field is added to the application forms for the selected certificate type.

The total number of custom fields that you can add is specified by your Sectigo account manager. If you reach the maximum permitted, **Add** is no longer displayed in the interface. Contact your Sectigo account manager to have more fields added to your account.

Once a custom field is added, the field appears in both the self-enrollment form and the built-in application form for the selected certificate type.

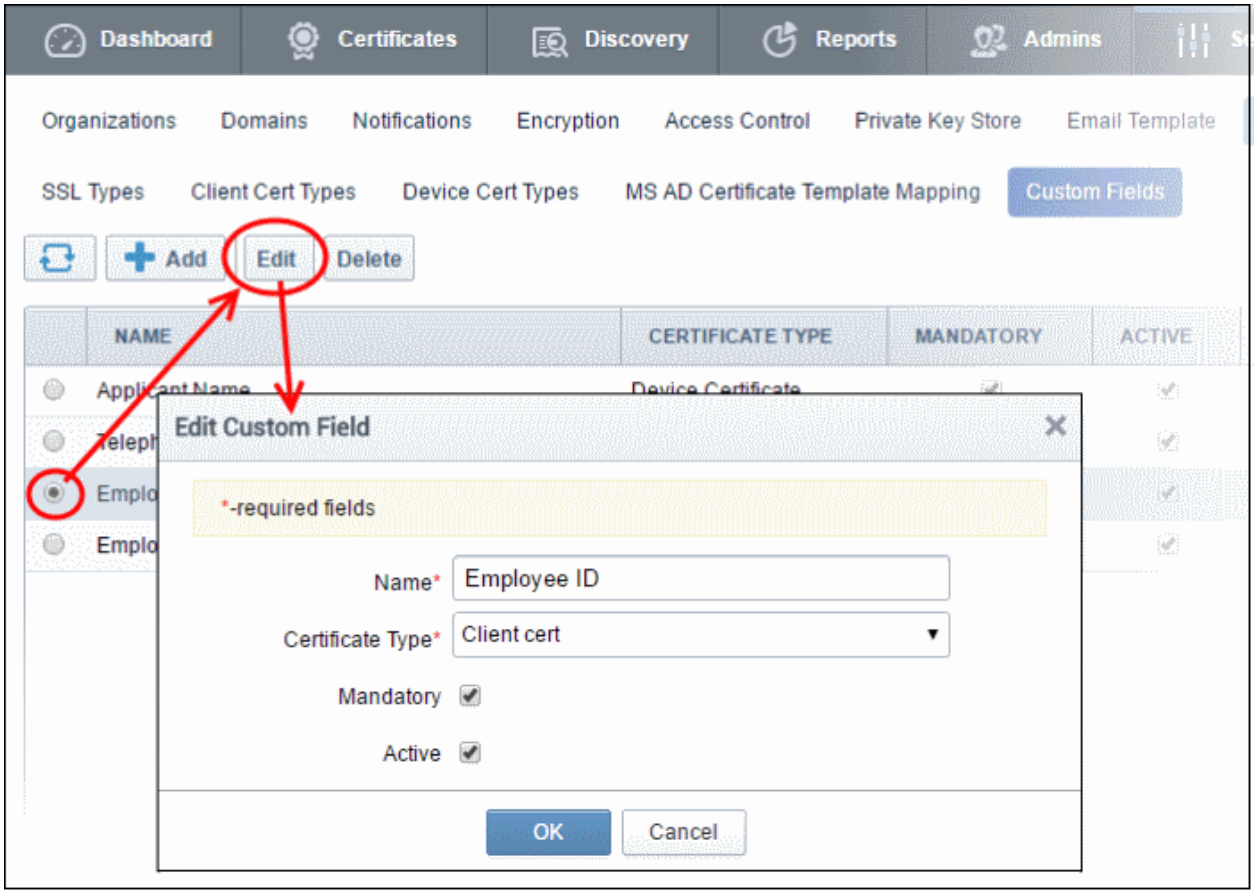
As an example, the built-in and self-enrollment application forms for an SSL certificate are shown in the following illustration. Both examples include two custom fields: Fax Number and Telephone.



The added custom fields are available in for both SSL and client certificate types via enrollment forms as well as through a web API.

7.9.4.2 Modifying an Existing Custom Field

To modify an existing custom field, you select the field and click Edit to open the **Edit Custom Field** dialog shown in the following illustration.



The fields of the preceding dialog are described in "Adding a New Custom Field" on page 502.

7.9.4.3 Removing an Existing Custom Field

If an custom field is unnecessary, you can remove it by either disabling or deleting it.

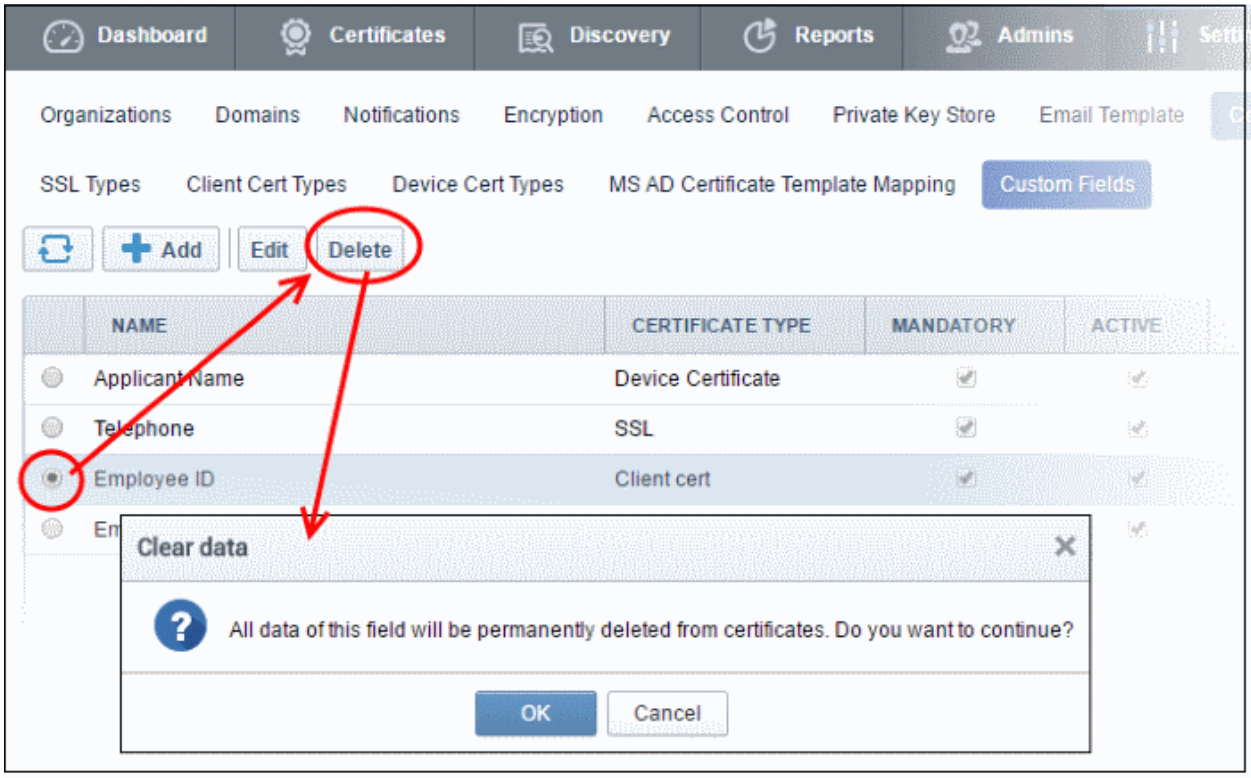
Typically, Sectigo recommends disabling rather than deleting a custom field, which enables retaining of all associated data. You can always reinsert the field, if required. If you find that you can no longer add new custom fields, it is because you have reached the maximum number of fields permitted for your account.

To disable a custom field, MRAOs can disable **Active** on the **Edit Custom Field** dialog, as described in "Modifying an Existing Custom Field" on page 504. If a field becomes inactive, it is not displayed in future application forms, but the existing data relevant to the field is retained in the database. You cannot add a new custom field to replace the inactive field if the maximum number of fields has been reached.

MRAO administrators can delete a field if it is not to be used in the future. All previously stored data associated with the deleted field is removed from the database. If a field is deleted, you can replace it with a new custom field.

A MRAO deletes a field as follows:

- From the main UI, navigate to **Settings > Certificates > Custom Fields**.
- Select the field to delete and click **Delete**, as shown in the following illustration.



7.10 Configuring Templates

SCM allows you to create templates for email notifications and self-enrollment forms. The **Templates** section includes the following:

- The **Email Template** area allows you to create templates for use with automatic email notifications sent to certificate applicants, administrators, and end-users when certificate updates, approvals, collection, revocation, and so on take place.

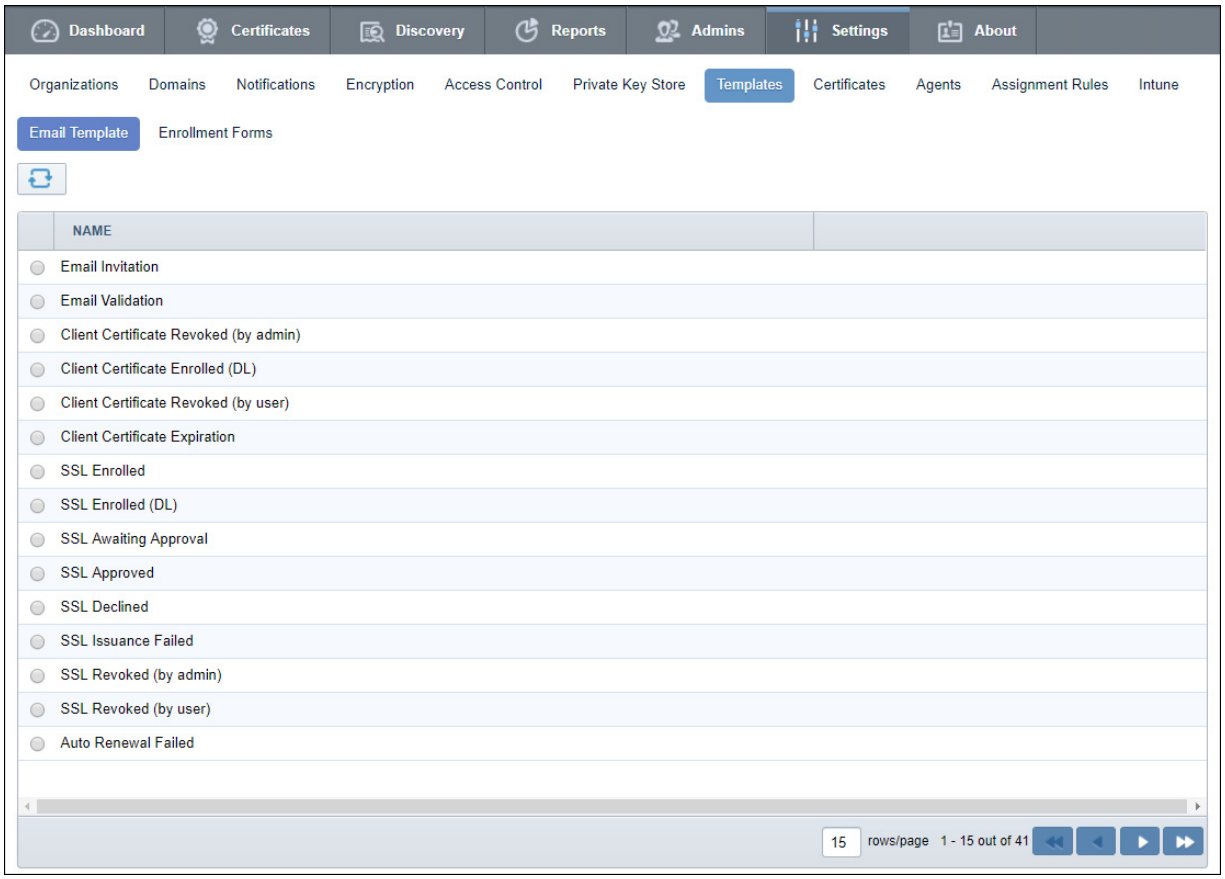
  You define notifications in the **Notifications** area (see "Configuring Notifications" on page 410).
- The **Enrollment Forms** area allows MRAOs to specify custom text and links to be included on self-enrollment pages for SSL, client, and device certificates.

7.10.1 How to Set Up Email Templates

The **Settings > Templates > Email Templates** area shown in the following illustration allows MRAOs to configure the content of the email templates for any certificate type for any organization or department. The **Name** column of this area lists the types of automated email notifications sent during different stages.

RAOs can edit email templates for their organizations by navigating to **Settings > Organizations**.

DRAOs can edit email templates for their departments by navigating to **Settings > Organizations > Departments**.



7.10.1.1 Modifying Email Templates

Email templates can be configured for individual organizations or your enterprise as a whole. Templates at the enterprise level inherit the default settings created by Sectigo and act as the defaults for templates at the organization level. If a template is altered at the enterprise level, unaltered templates at the organization level are automatically updated to reflect that change. Templates that have been altered are automatically updated if changes are made to default templates.

To modify enterprise and organization email templates messages, do the following:

1. Navigate to **Settings > Templates > Email Templates** (enterprise templates) or **Settings > Organizations > Edit > Email Template** (organization templates).
2. Select the template you want to modify and click **Edit**.

3. Complete the **Edit Email Template** fields based on the information provided in the following table.

Field	Description
Title	The subject line of the email to be sent.
Body	The primary content of the email message.
Send notification in HTML format	When enabled, the email notifications are sent in HTML format.
Insert Variable	Activate to insert variables into the body of the email message. Variables are replaced with values and details from the corresponding certificate or domain when the email notification is sent. The variables available depend on the selected template.
Revert to default[a]	Activate to revert the template back to its default state. This action cannot be reversed; all changes are lost.
Show Default	When activated, the default template is displayed.

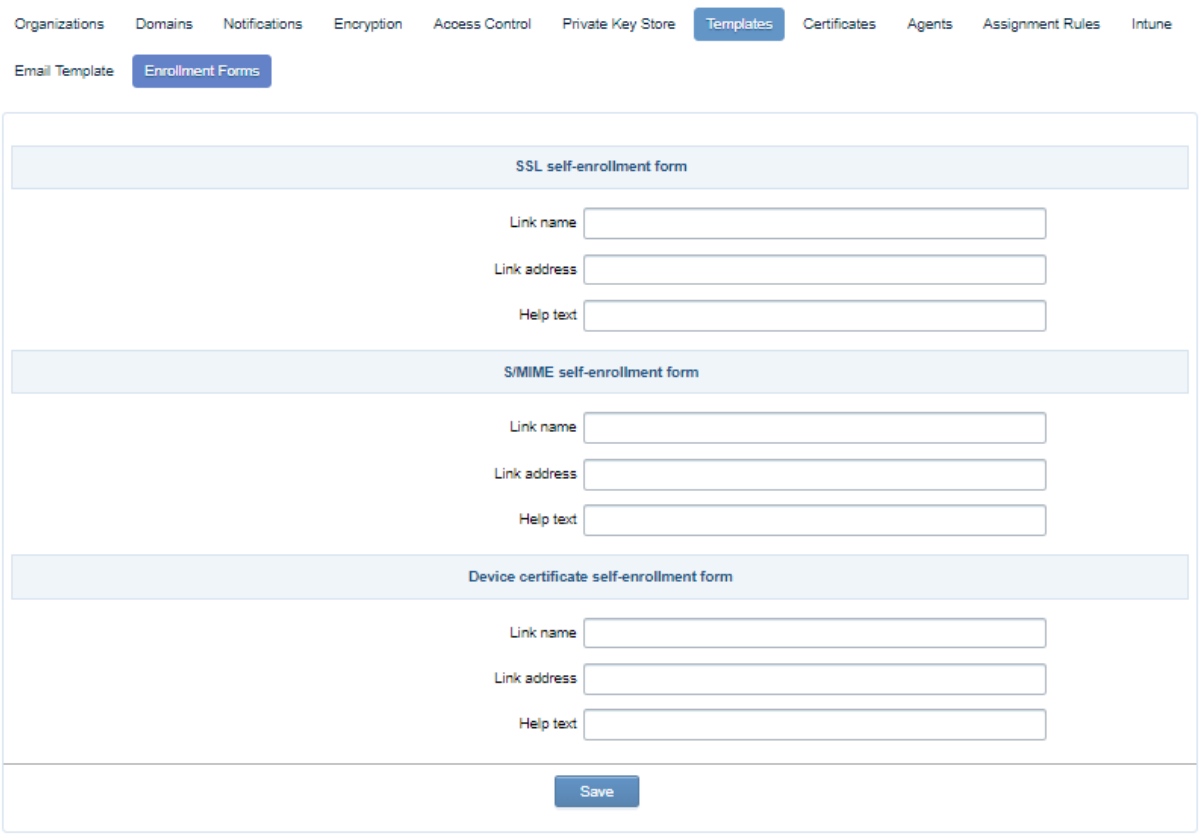
a. When used at the Organization level, the template reverts to the default specified at the Enterprise level. When used at the Enterprise level, the template reverts to the default specified by Sectigo.

4. Click **OK**.

7.10.2 How to Set Up Self Enrollment Custom Text and Links

You configure self-enrollment custom text and links by navigating to **Settings > Templates > Enrollment Forms**, as shown in the following illustration, and then enabling specific functionality based on the descriptions in the following table.

NOTE: The forms available for use are dependent on the certificate types available for your account.



Field / Element	Description
Link name	The link text to be displayed on the self-enrollment page. When an end-user clicks the link, they are redirected to the URL specified in the **Link address** field.
Link address	The URL to which the text links.
Help text	The text that is displayed on the self-enrollment page to provide additional information or direction to users. The input limit is 2048 characters.

7.11 Managing SCM Agents

SCM agents allow you to automate various processes, such as certificate discovery and installation.

For more information, see "Configuring Agents" on page 249.

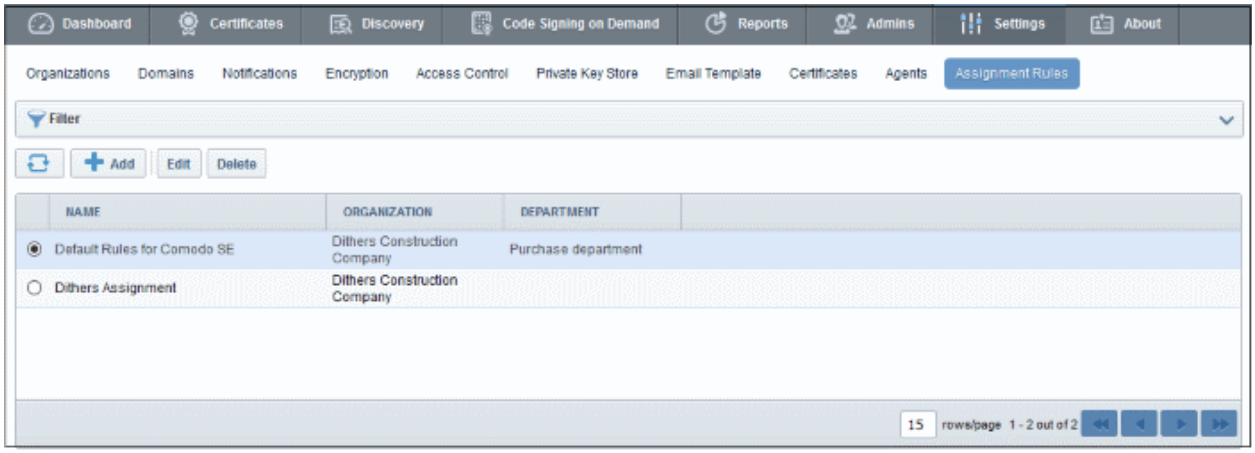
7.12 Defining Auto-Assignment Rules for External Certificates

Depending on your security role as an administrator, you can create rules to automatically assign external (also known as unmanaged) certificates found after a discovery scan to a specific organization or department. These rules assign certificates to a particular entity based on one or

more conditions set by you. The rules can be applied while configuring network discovery tasks and MS AD discovery tasks, so that each external certificate found by a discovery scan and satisfying conditions in any of the rules applied to the scan is automatically assigned to the respective organizations and departments. For more information, see "Certificate Discovery Tasks Overview" on page 525.

The **Assignment Rules** area shown in the following illustration allows you to create rules for use in discovery scans, as follows:

- From the main UI, navigate to **Settings > Assignment Rules**.
- Ensure that your security role allows you to perform this task, based on the following guidelines:
  - MRAOs can create and manage rules to assign discovered certificates on any network to any organization and department.
  - RAOs can create and manage rules to assign certificates discovered on their networks to organizations and subdepartments which have been delegated to them.
  - DRAO can create and manage rules to assign certificates discovered on their networks to departments which have been delegated to them.
- Based on the list of available rules, proceed to creating new rules or manage existing rules.

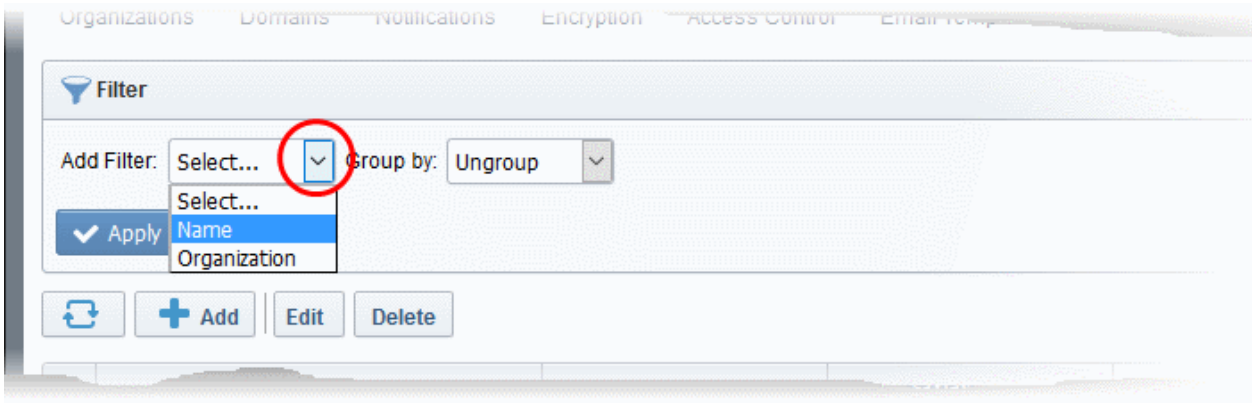


The following table lists settings available in the **Assignment Rules** area.

Column	Description
Name	The name of the external certificate assignment rule.
Organization	The name of the organization to which the certificates matching the criteria specified in the rule is to be auto-assigned.
Department	The name of the department to which the certificates matching the criteria specified in the rule is to be auto-assigned.

You can sort items in the alphabetical order by clicking a column header, and you can use filters to search for particular templates.

To add filters, you make a selection in the **Add Filter** list and then group the results with other options that appears depending on the selection from the Add Filter list.

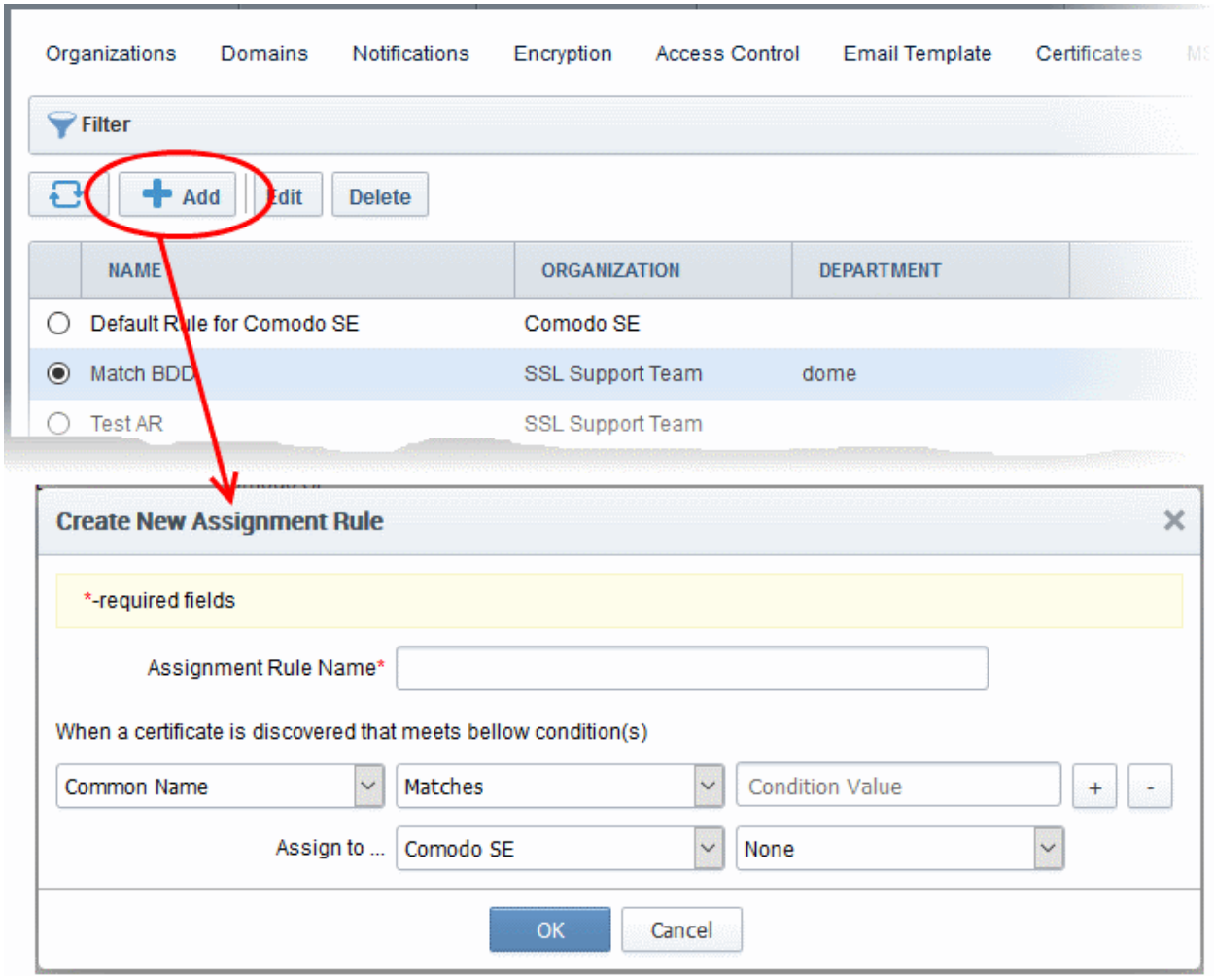


Filter Criteria	Filter Parameter
Name	Enter the name of the rule in full or part.
Organization	Select the organization or department to which the certificate is to be assigned as per the rule, from the Organization and Department lists.

You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the area, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

To create a new rule, click **Add** in the **Assignments Rules** area, as shown in the following illustration.



- Enter a name shortly describing the rule in the **Assignment Rule Name** field.
- Set the condition for identifying the certificate to be auto-assigned as per the rule:
  - Select the field of the certificate to be searched from the first list.
  - Select the relationship between the field value and the condition value from the second list.
  - Enter the condition value in the text field.

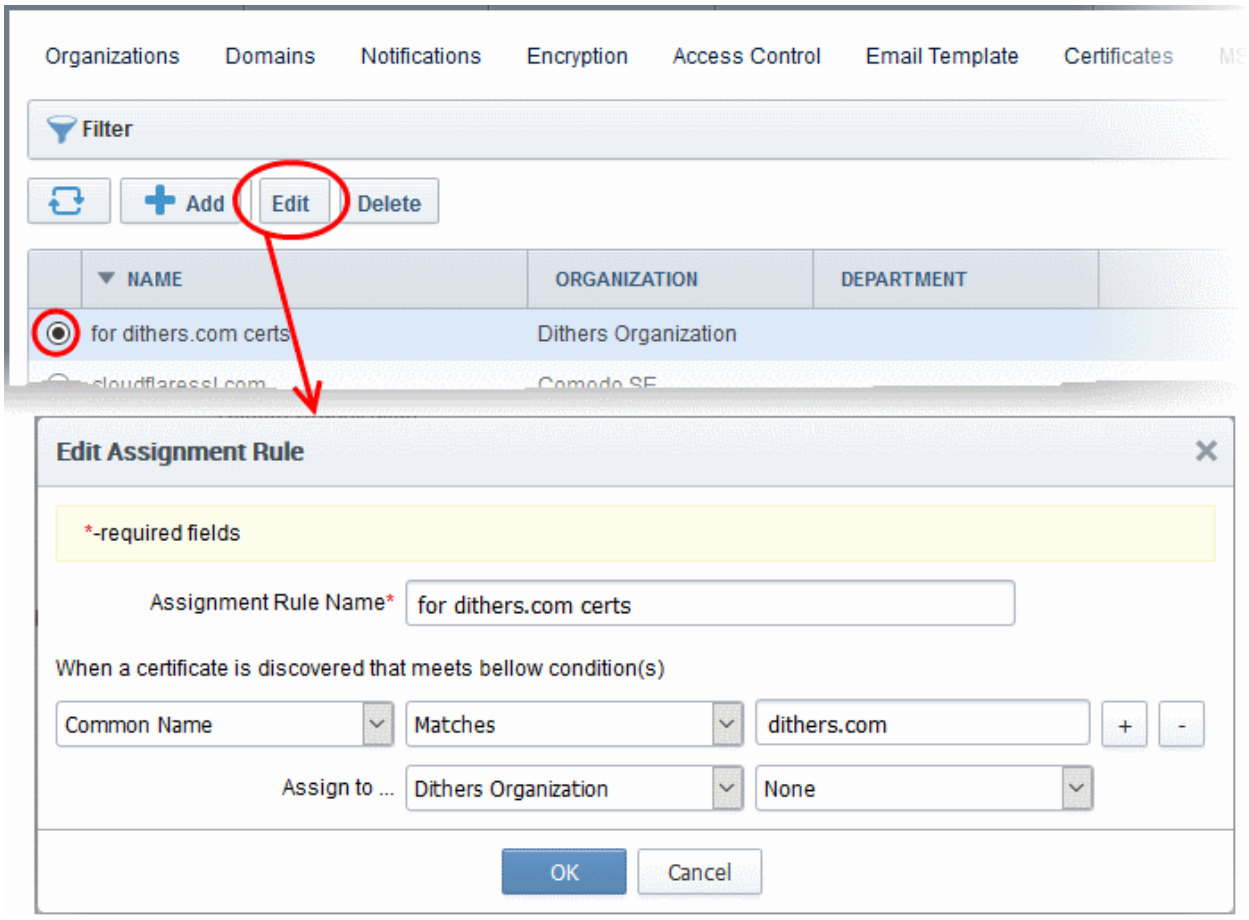
  For example, if you want to auto-assign certificates with common name dithers.com, then select Common Name from the first list, select Matches from the second list, and enter dithers.com in the text field.
- Choose the organization or department to which the certificates meeting the conditions are to be auto-assigned using the respective **Assign to** lists
- Click **OK**.

Upon completion, the rule is added to the list. The rule is available for selection while configuring a discovery task.

To add more rules, repeat the process.

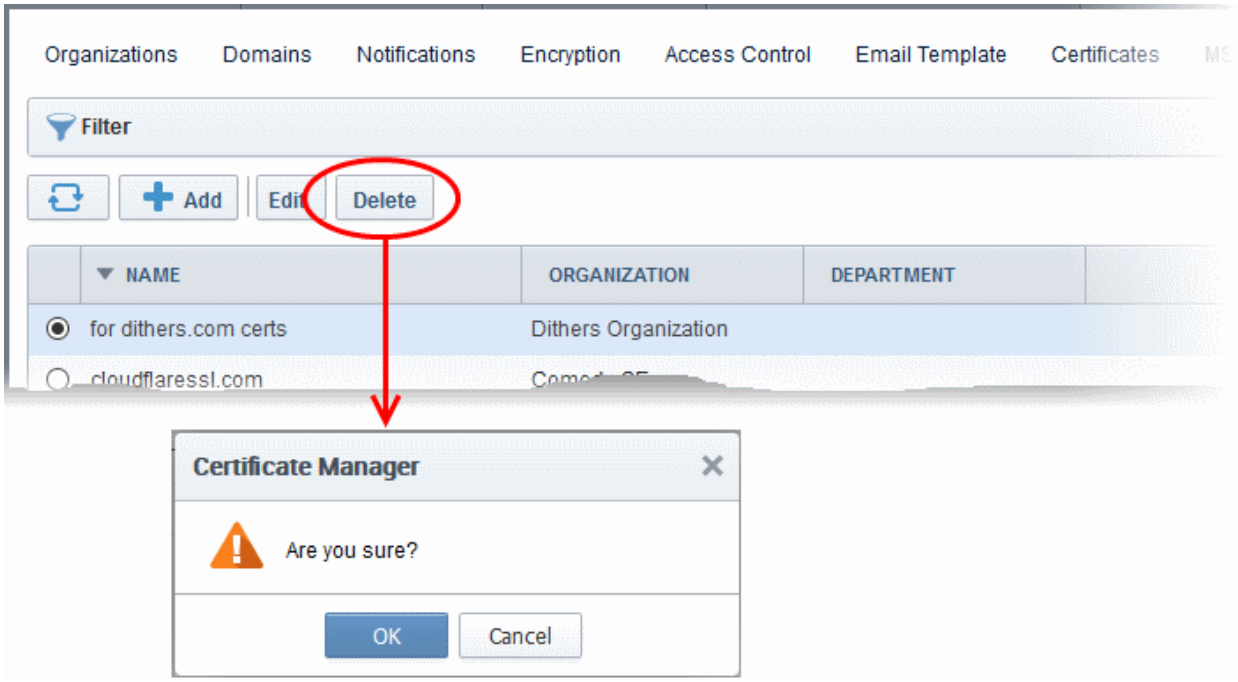
You can modify an existing rule as follows:

- Select the rule and click the **Edit** to open the **Edit Assignment Rule** dialog shown in the following illustration.



The preceding dialog is similar to the **Add Assignment Rule** dialog. For description of the fields, see the explanation of adding a new rule.

To remove a rule, select the rule and click **Delete**, as shown in the following illustration.



7.13 Configuring SCM for Microsoft Intune

SCM can be integrated with Microsoft Azure and Microsoft Intune can be configured for enrollment of client certificates as well as device certificates.

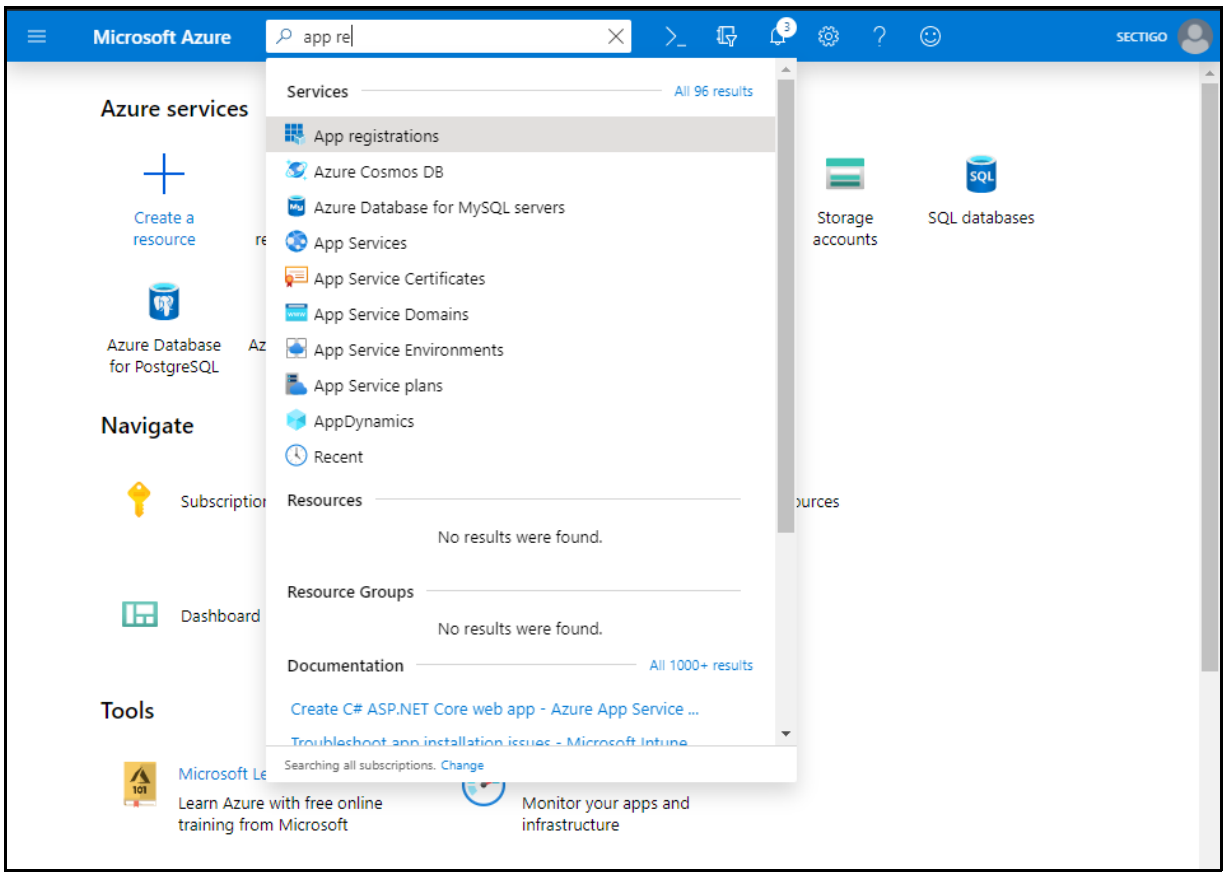
For more information, see "Using SCM with Microsoft Intune" on page 599.

7.14 Configuring the Azure Key Vault Integration

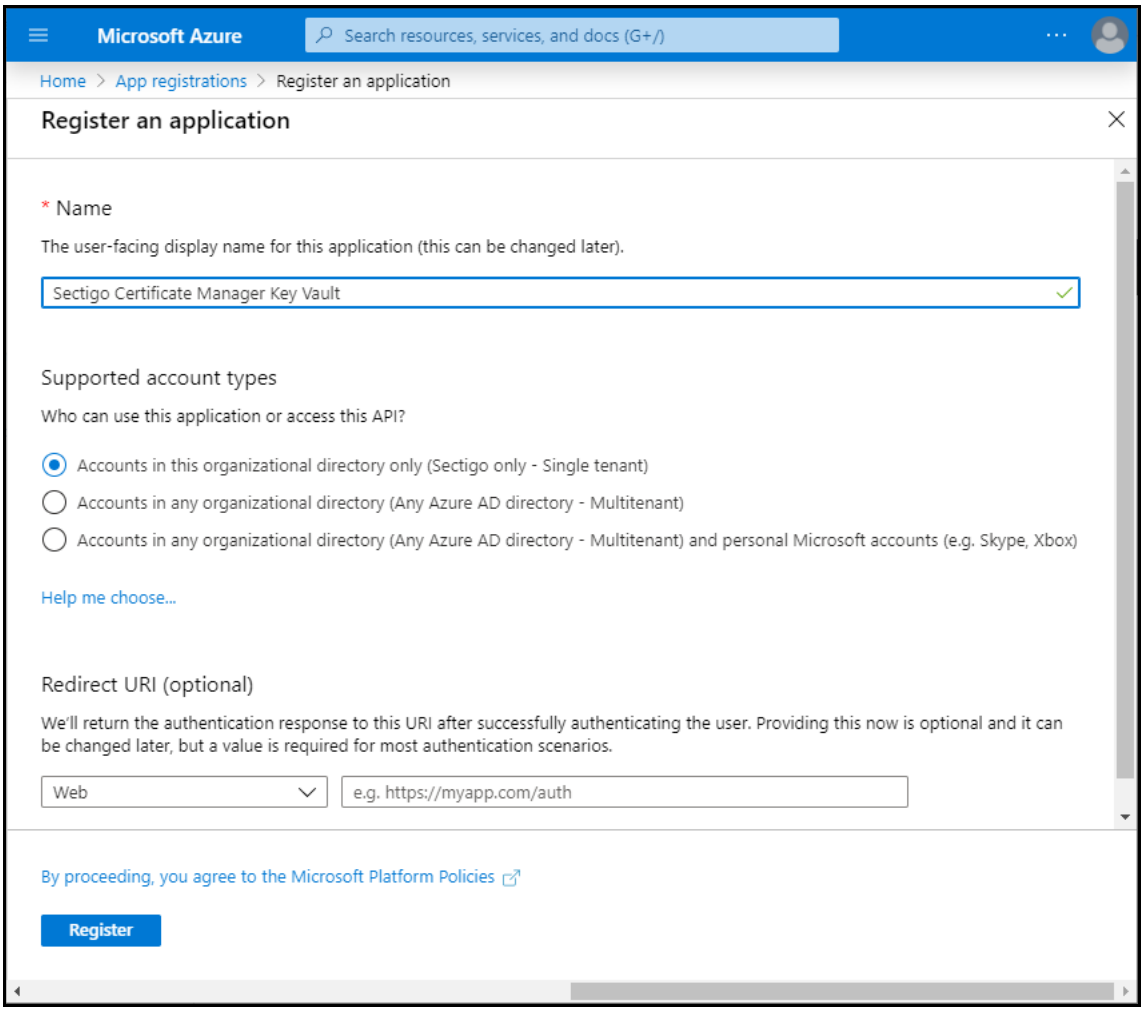
This section assumes that you have an active Azure subscription, at least one resource group configured, and at least one key vault assigned to the resource group.

To register a new application in Azure, do the following:

1. From the Azure Portal, navigate to **App registrations** as shown in the following illustration.



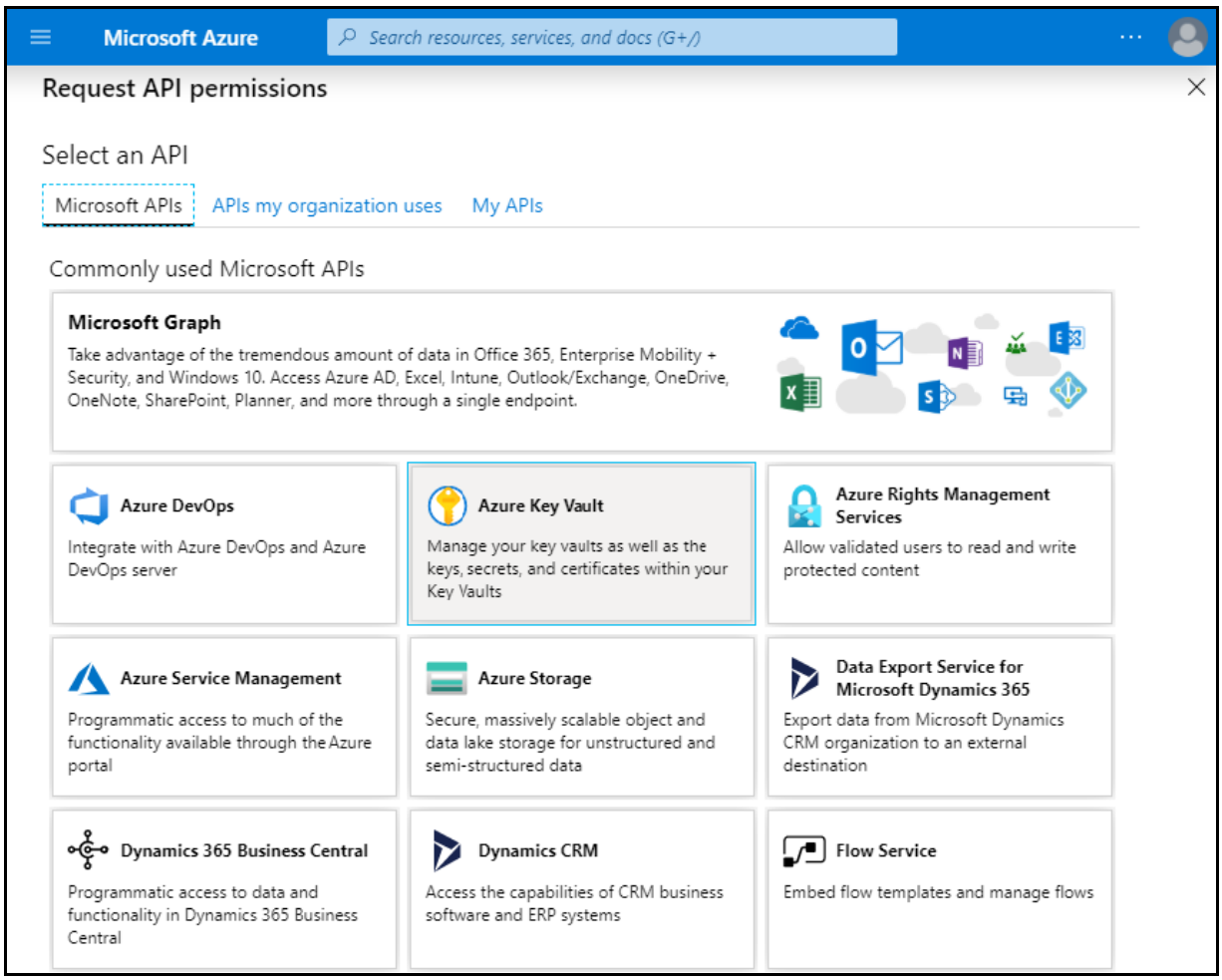
2. Click **New Registration** to open the **Register an application** page shown in the following illustration.



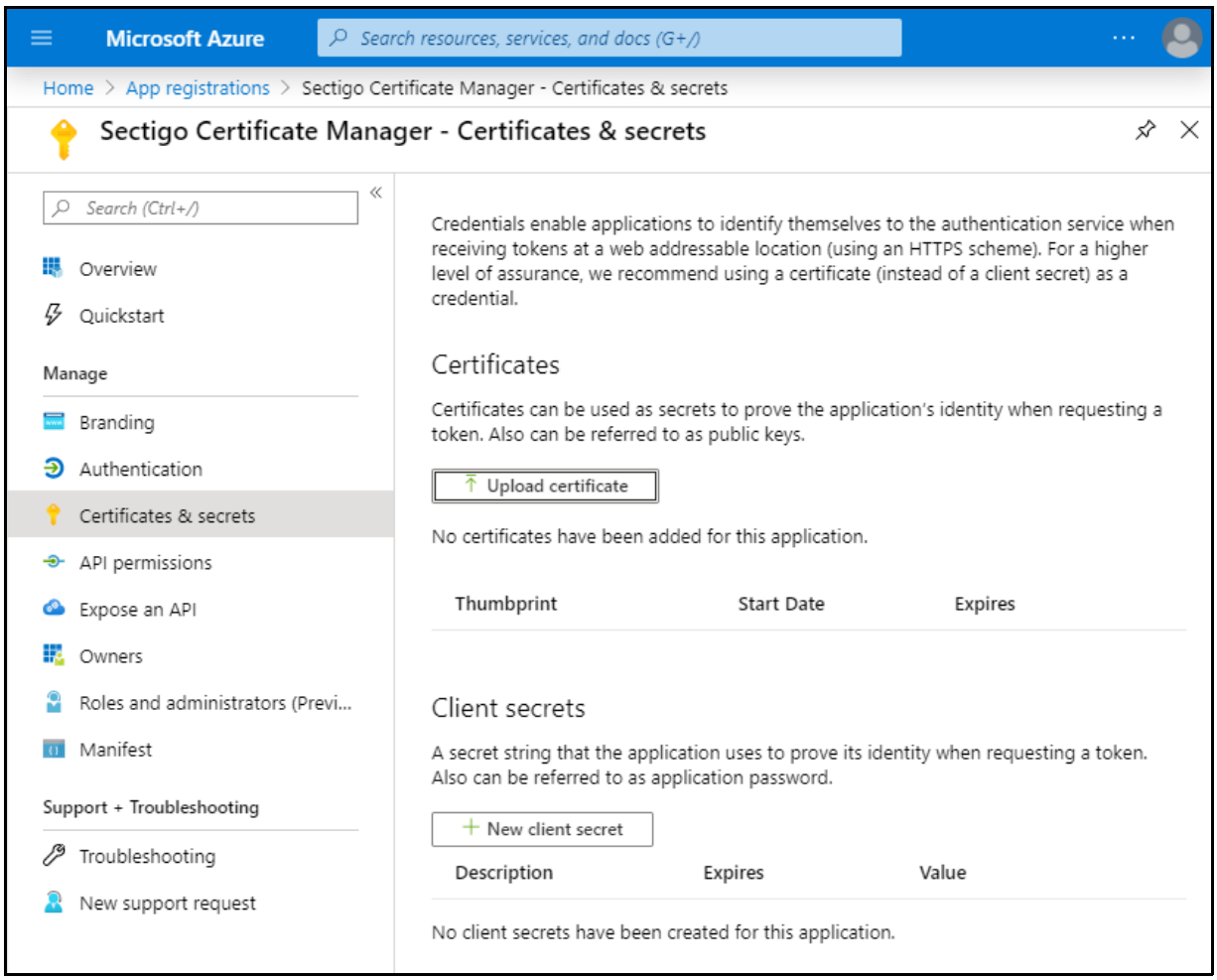
3. Complete the **Register an application** fields based on the information provided in the following table.

Field	Value
The user-facing display name for this application	Sectigo Certificate Manager Key Vault (recommended)
Supported account types	Default
Redirect URI	Default

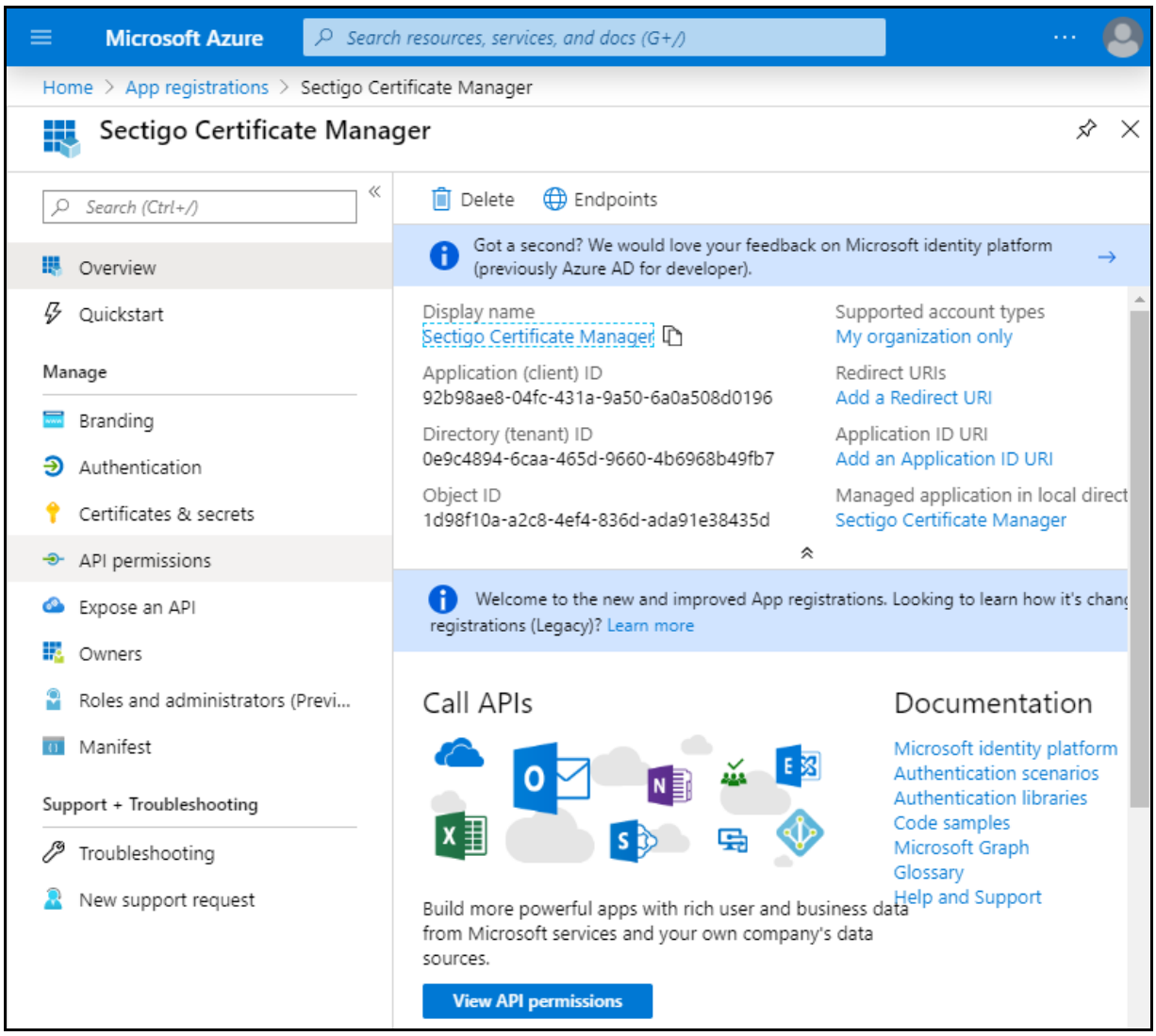
4. Click **Register**.
5. Select **API permissions** and click **Add a permission** to open the **Request API permissions** area, as shown in the following illustration.



6. Select **Azure Key Vault**, and select **user_impersonation**.
7. Click **Add permissions**.
8. Select **Certificates & secret** and click **New client secret**, as shown in the following illustration.



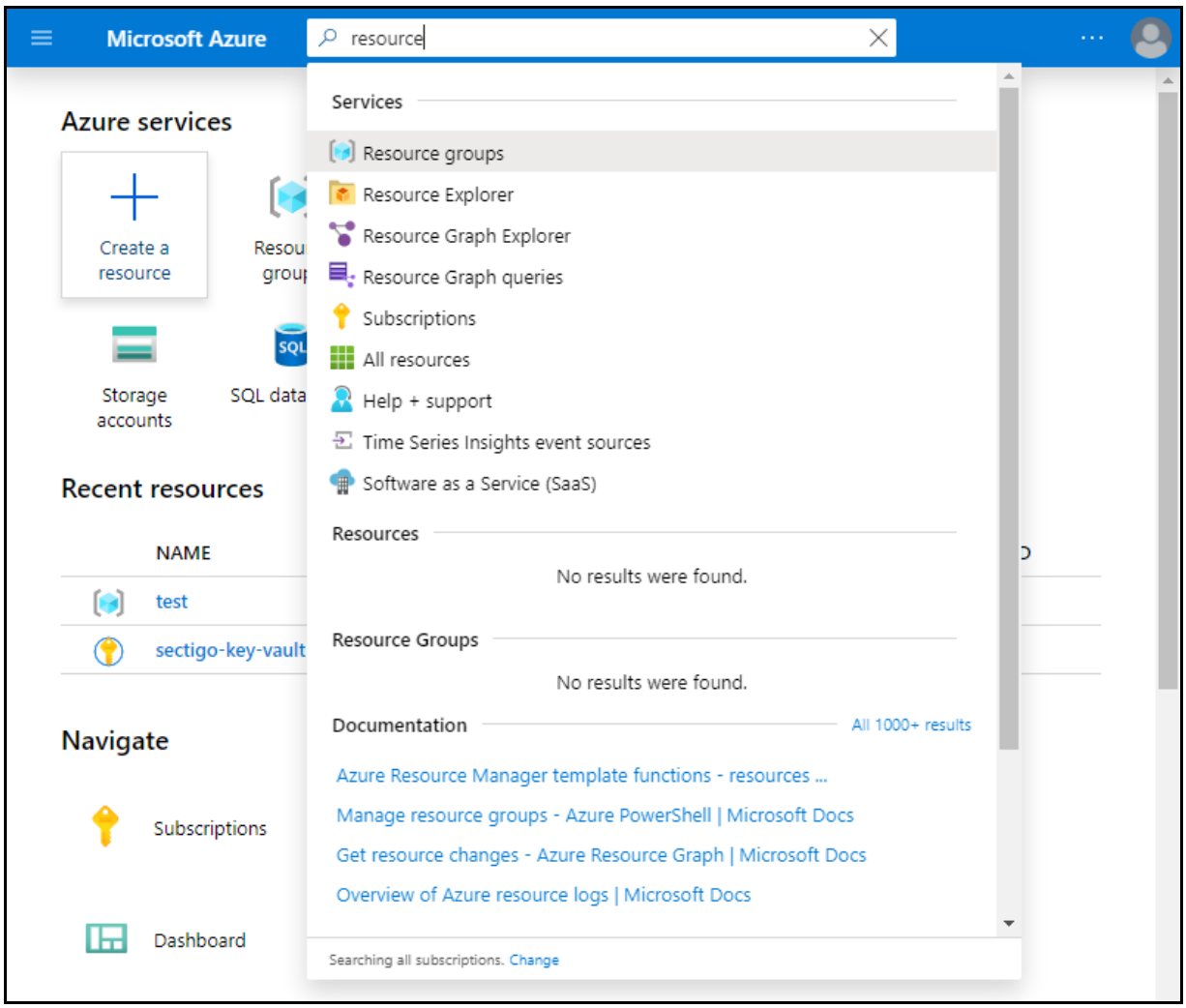
9. In the **Add a client secret** area, provide a description (such as SCM Access) and select **Never**.
10. Click **Add**.
11. Record the secret **Value.**
12. Record the **Application ID** and **Directory ID** from the **Overview** section, as shown in the following illustration.



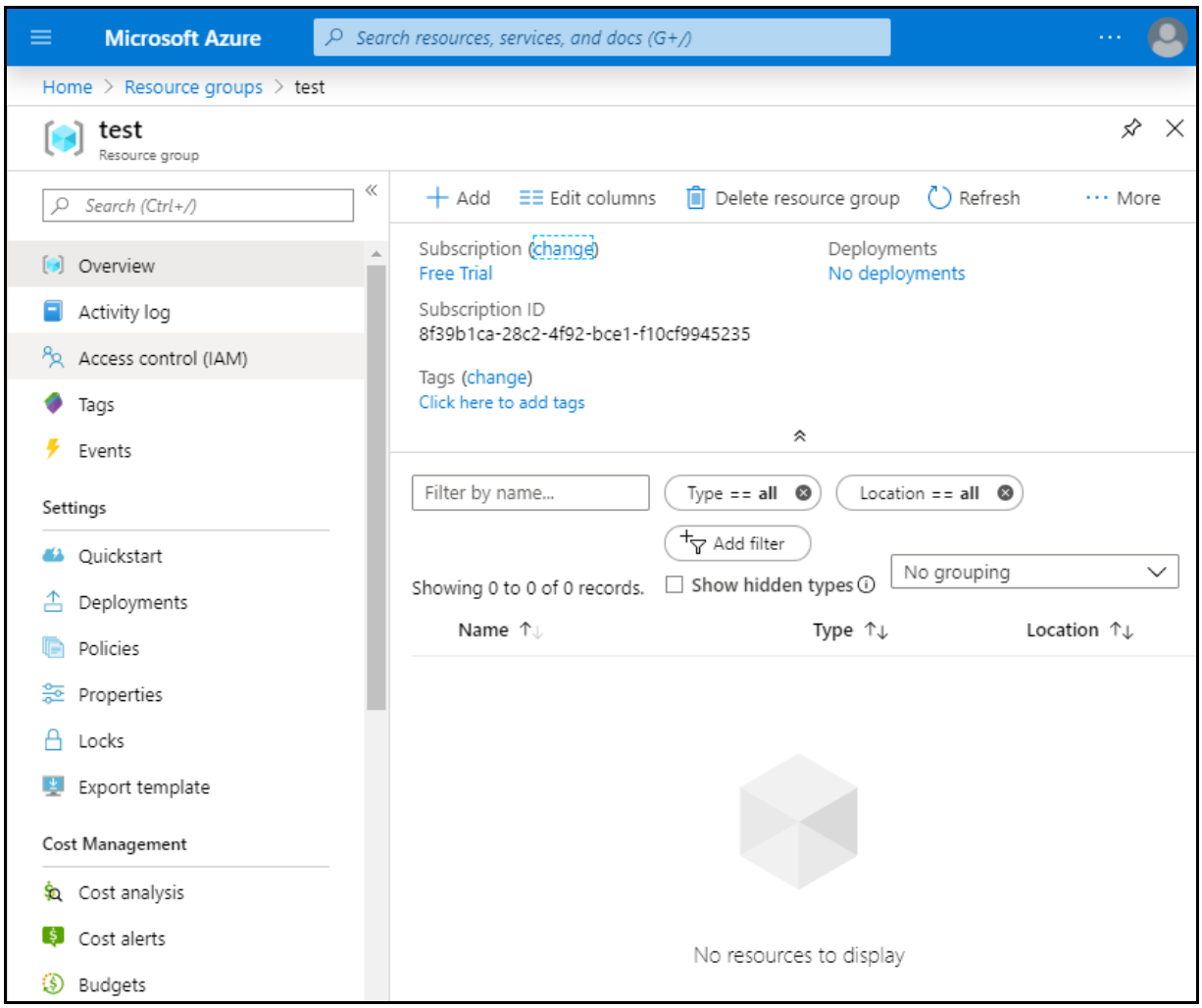
To give the registered application access to resource groups and key vaults, do the following:

1. From the Azure Portal, navigate to **Resource Groups**, as shown in the following illustration.

   NOTE: Access can also be given at the **Subscription** level, if necessary.



2. Select the resource group containing the appropriate Key Vault.
3. Select **Access control**, as shown in the following illustration.

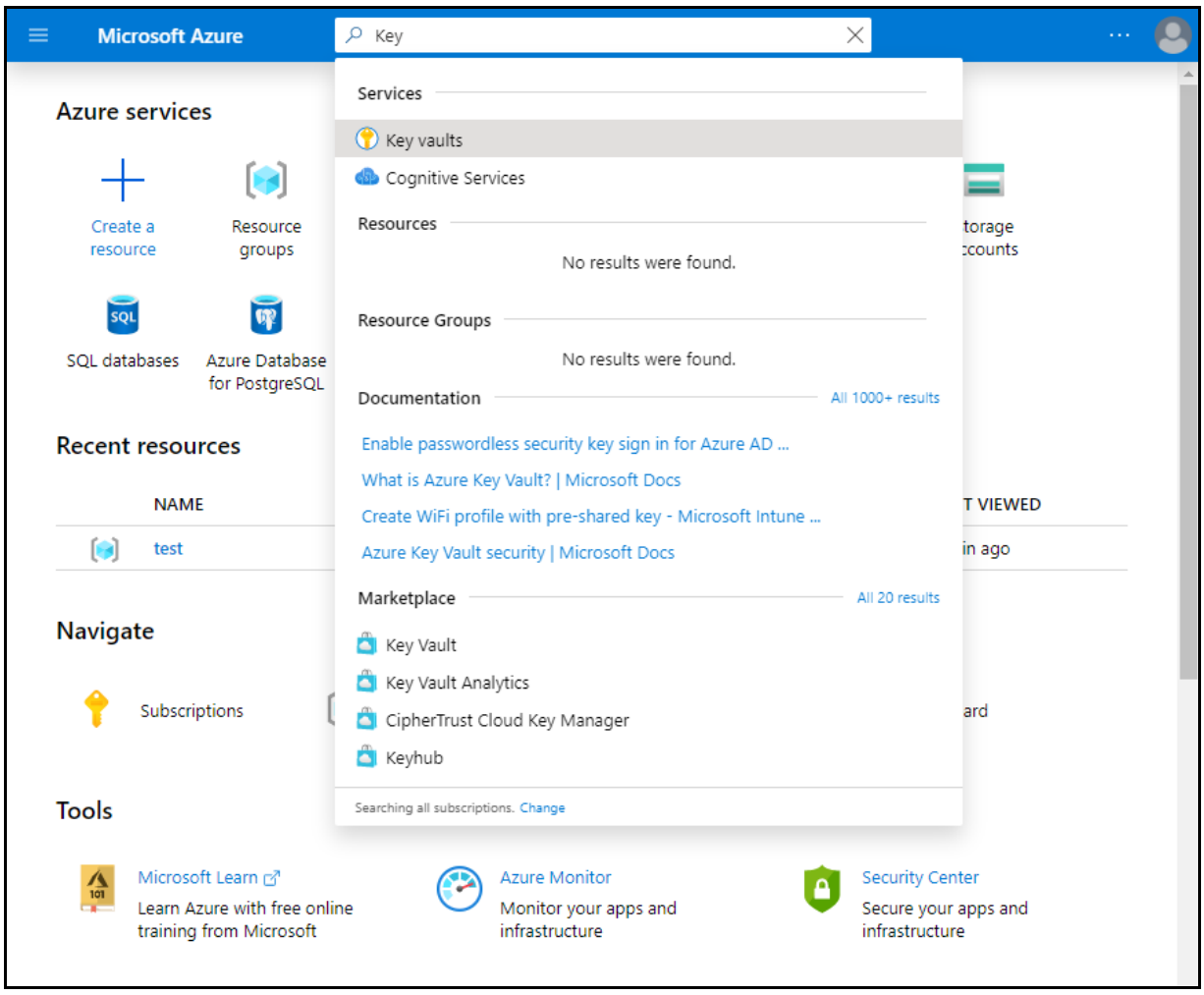


4. Click **Add > Role Assignment**.
5. Complete the **Add role assignment** fields based on the information provided in the following table.

Field	Value
Role	Key Vault Contributor
Assign access to	Azure AD user, group, or service principal
Select	Sectigo Certificate Manager If you provided a different name when you performed the application registration, select that name instead.

To enable the registered application to create a certificate in the Key Vault, do the following:

1. From the Azure Portal, navigate to **Key Vaults**, as shown in the following illustration.



2. Select the appropriate key vault.
3. Select **Access policies** for this key vault.
4. Click **Add Access Policy**.
5. Complete the **Add access policy** fields based on the information provided in the following table.

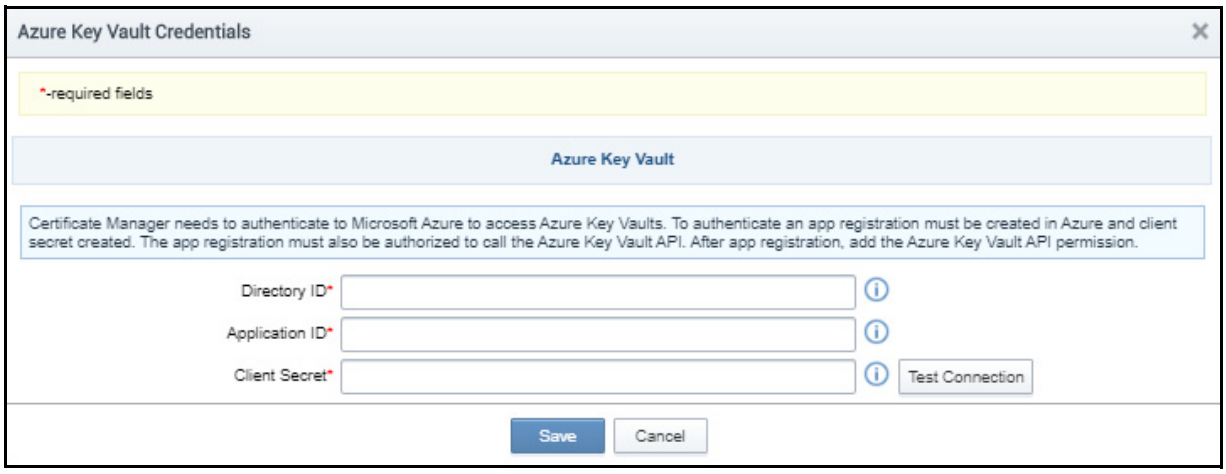
Field	Value
Configure from template	Certificate Management
Key permissions	Default
Secret permissions	Default
Certificate permissions	Default

Field	Value
Select principal	Sectigo Certificate Manager If you provided a different name when you performed the application registration, select that name instead.
Authorized application	Default

6. Click **Add**.

To configure SCM for interaction with Azure Key Vault, do the following:

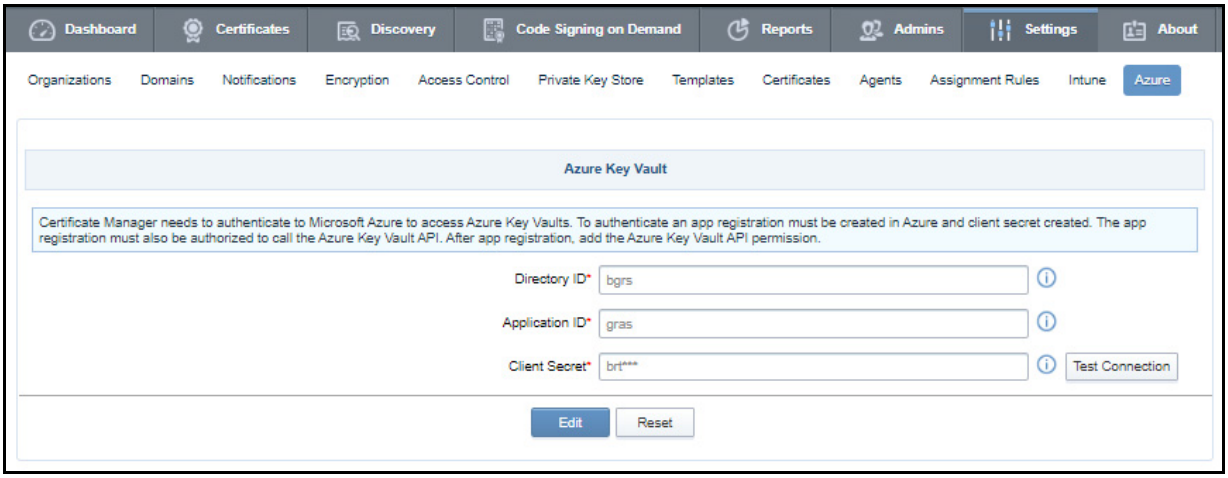
1. From SCM, navigate to **Settings > Azure**, as shown in the following illustration.



2. Click **Add Registration** and enter the saved **Application ID**, **Directory ID**, and **Client Secret**.
3. Click **Test Connection** to validate the data.
4. Click **Save**.

To edit or remove a connection between SCM and Azure Key Vault, do the following:

1. From SCM, navigate to **Settings > Azure**, as shown in the following illustration.



2. Click **Edit** to make changes or click **Reset** to remove the connection.

For information on enrolling a certificate in the Azure Key Vault, see "Automatic CSR Generation in Azure Key Vault" on page 113.

8

Performing Certificate Discovery Tasks

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

This chapter describes the following topics:

- Certificate Discovery Tasks Overview
- Evaluating Network Assets
- Performing Network Discovery Tasks
- Performing the AD Discovery Tasks

8.1 Certificate Discovery Tasks Overview

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

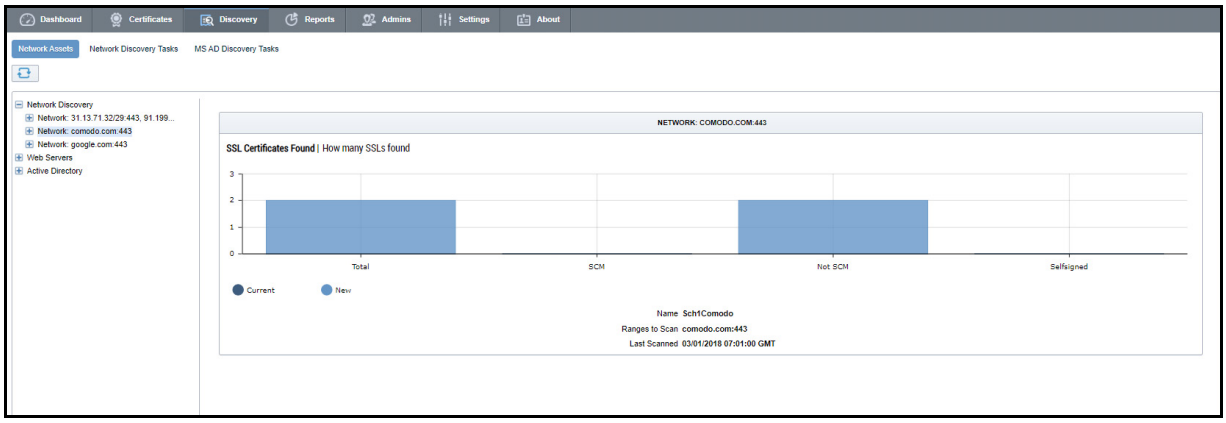
- SSL certificates installed on your network servers. This includes certificates issued to domains, network devices, certificates issued by third party vendors, and self-signed certificates.
- Certificates installed on servers, devices, and endpoints on AD domains. AD scans discover the network and object structure, and locate all types of certificates, including SSL, client certificates, code signing certificates, and device authentication certificates.

Network Agents installed on network servers facilitate the discovery process in networks. In addition, the agents are used for automatic installation of SSL certificates on Apache HTTP, Apache Tomcat, IIS 7, 7.5, 8, and F5 BIG IP servers. See "Configuring Network Agents" on page 252 more information.

MS Agents installed on AD servers facilitate the discovery process in active directory domains. In addition, these agents perform the following:

- Acts as a CA proxy and can be used to provision authentication certificates for devices added via NDES.
- Allow certificate templates on AD servers to be mapped to SCM certificate types. This enables SCM to act as a private CA for an organization or department. Domain administrators can create custom certificate templates on their server as required and request SCM administrators to map these templates to private certificate types. Domain administrators can enroll for certificates from the AD server by selecting the respective template.
- Can be used to provide authentication certificates to devices. See "Configuring MS Agents" on page 266 for more information.

The **Discovery** area of the SCM UI shown in the following illustration lets you configure and run network discovery scans, AD scans, and to view certificates and network objects identified by the scans.

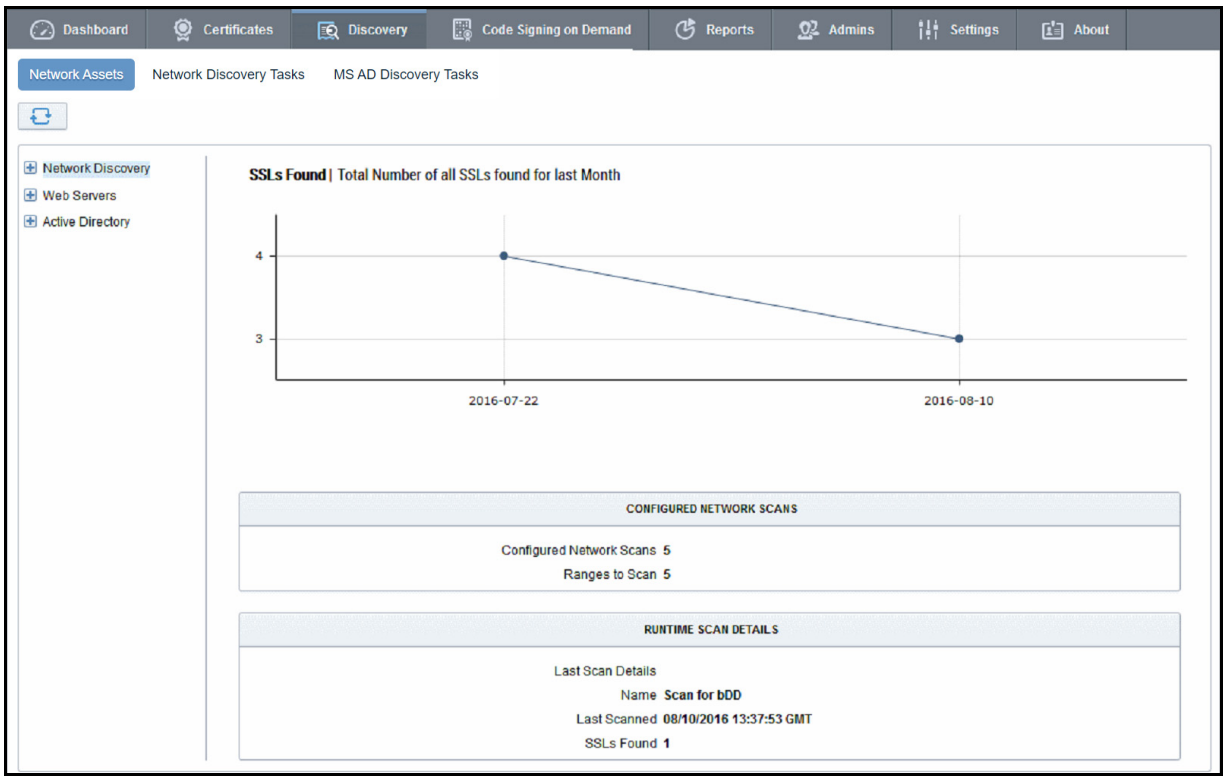


The **Discovery** area contains the following sub-areas:

- The **Network Assets** area allows you to view the results from scans. The results include certificates and web servers discovered on the network and devices added to SCM by the AD integration. For more information, see "Evaluating Network Assets" on page 526.
- The **Network Discovery Tasks** area allows you to add, schedule, and run discovery tasks on networks. For more information, see "Performing Network Discovery Tasks" on page 540.
- The **MS AD Discovery Tasks** area allows you to add, schedule, and run discovery tasks on AD Servers. For more information, see "Performing the AD Discovery Tasks" on page 560.

8.2 Evaluating Network Assets

The **Network Assets** area shown in the following illustration displays discovered SSL, client, code signing, and device authentication certificates installed on servers and other devices connected to the network. It also displays a list of web servers identified on the network and any domains hosted on them. The network assets are displayed as a tree structure on the left. If you have integrated an AD server, then devices enrolled to AD are also shown on the left.



For information on how to use each network asset category, see the following:

- "How to View Certificate Information Via Network Discovery" on page 527
- "How to View the Web Server Information" on page 536
- "How to View Certificates Via Active Directory" on page 538

8.2.1 How to View Certificate Information Via Network Discovery

Depending on your security role as an administrator, **Network Discovery** allows you to view a summary of all certificates installed on every scanned network and a history of previous scans. You can also generate reports on discovered certificates and assign external certificates identified by discovery scans to respective organizations.

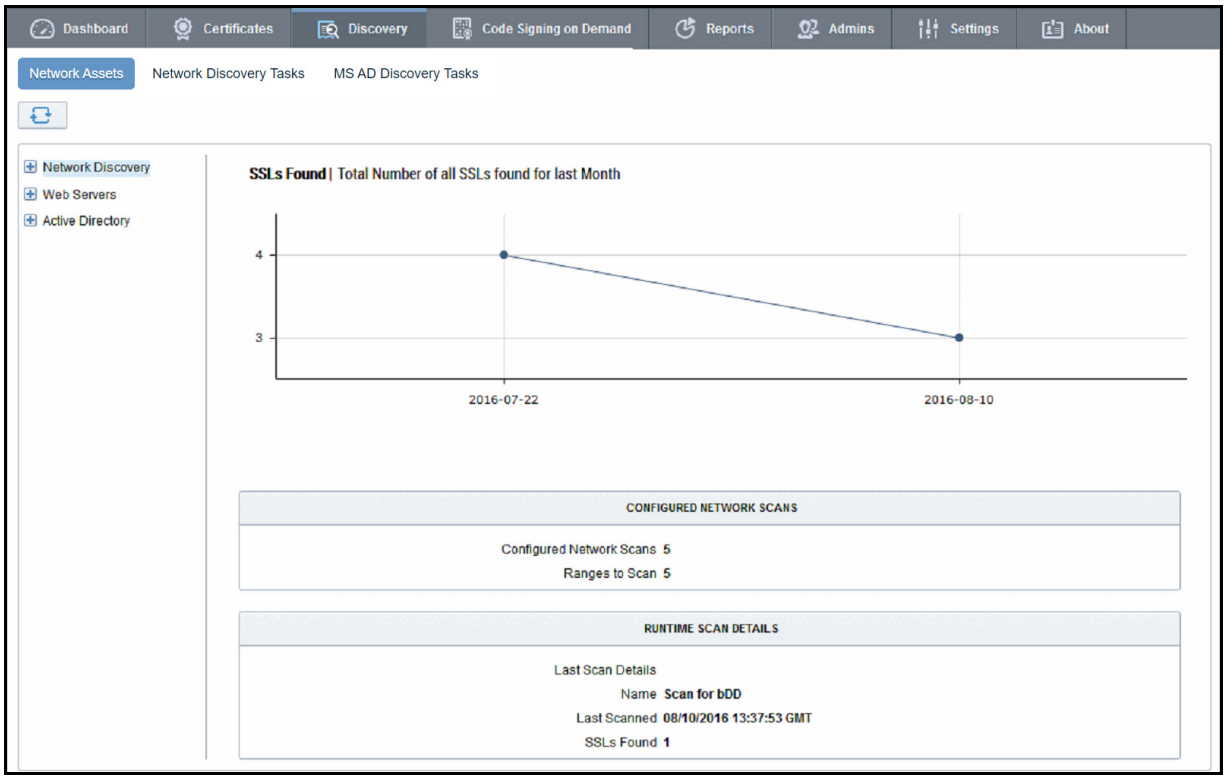
NOTE: An external (also known as unmanaged) certificate is a certificate that has not been obtained via SCM. SCM identifies all managed and external certificates on a network and allows you to assign them to an organization or department.

A MRAO can view certificates installed on all networks on which the scans were run.

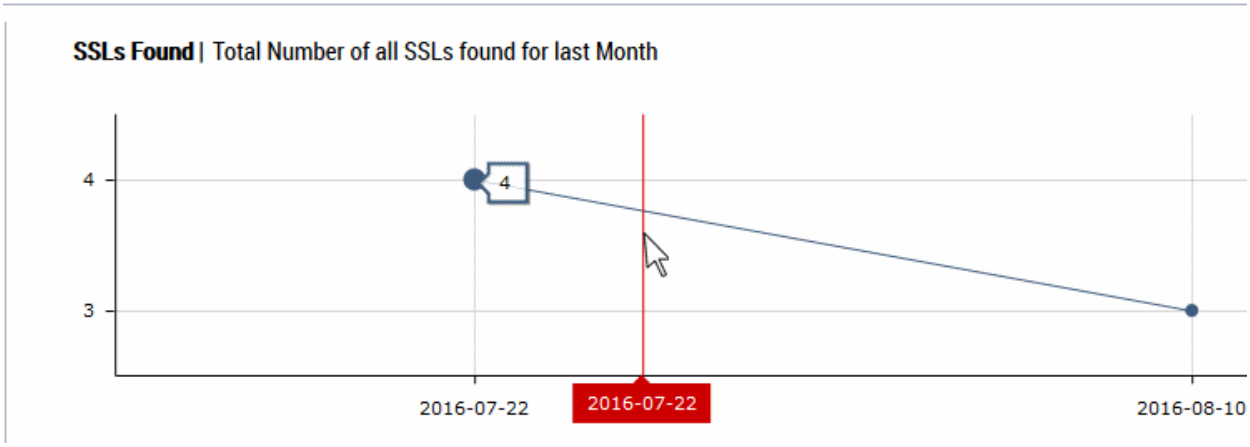
A RAO SSL can view certificates installed on networks of organizations and their departments that have been delegated to these administrators.

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

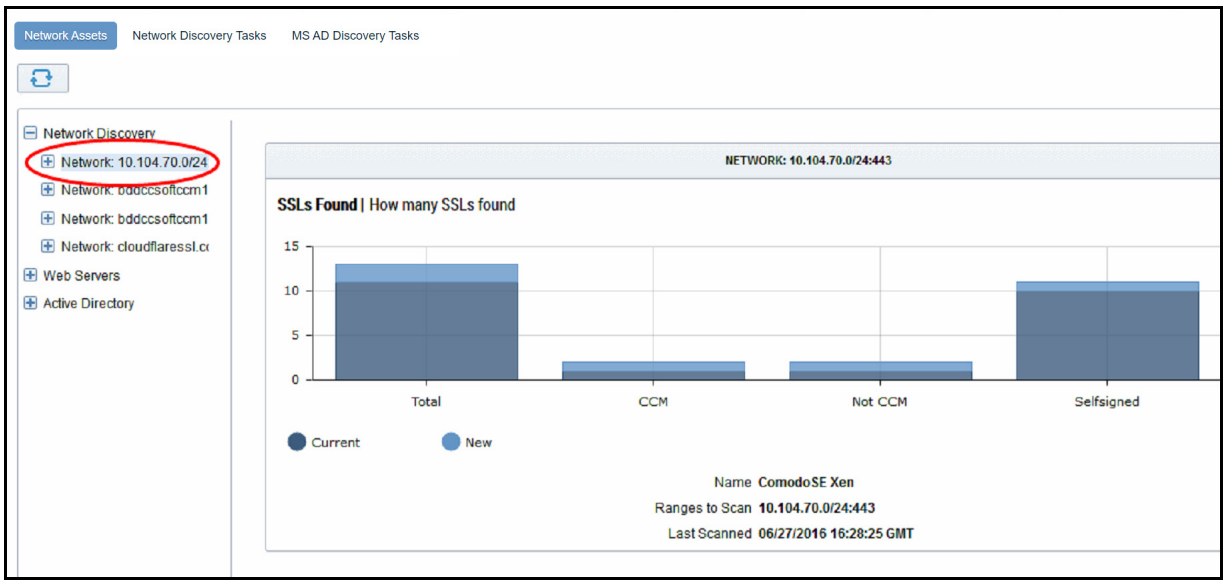
To view a summary of SSL certificates installed on all scanned networks, you use th main SCM UI to navigate to **Discovery > Network Assets > Network Discovery**, as shown in the following illustration.



The area displays a time graph of 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, as shown in the following illustration.

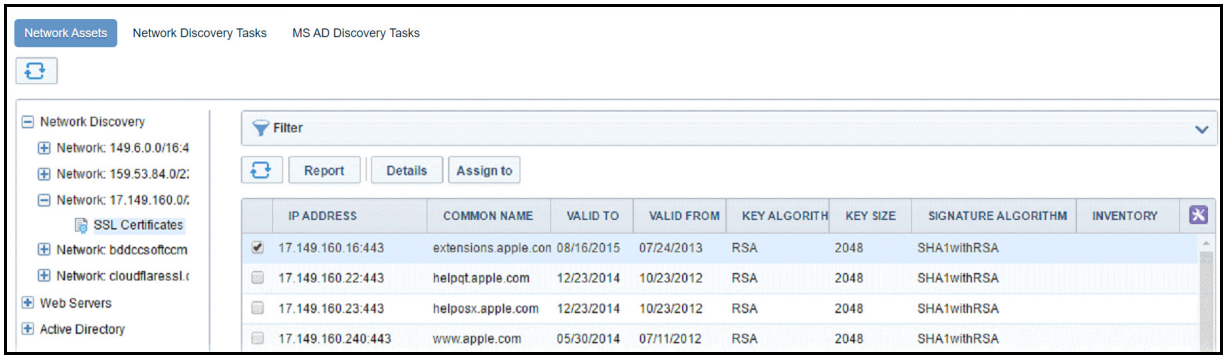


To view a summary of SSL certificates installed on a specific network, you expand the **Network Discovery** category and select the network, as shown in the following illustration.



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. The details of the discovery scan task name, network, and IP ranges scanned, as well as date and time of the last run scan are also shown.

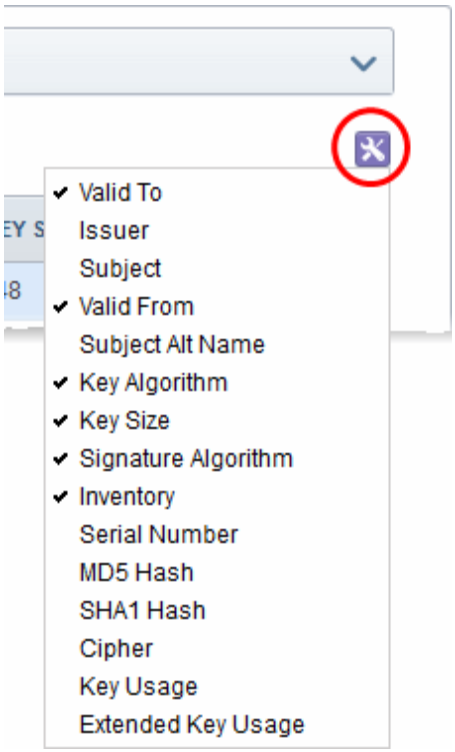
You can also view a list of SSL certificates installed on a specified network, as shown in the following illustration.



The detailed list of certificates detected from the network during the last scan is displayed. Selecting a certificate allows to view details and to manually assign external certificates to required organization and department.

Using the **Network Discovery** area, you can also create a report on the discovered certificates.

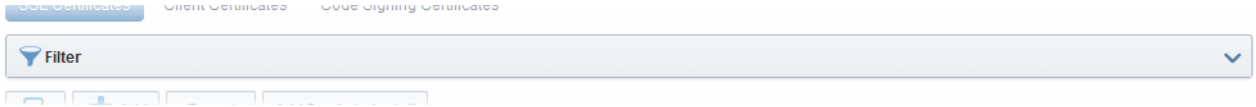
The following table lists settings and elements of the **Network Discovery** area.

Column	Description
IP Address	The IP address of the server on which the certificate was discovered.
Host Name	The name of the server on which the certificate was discovered.
Valid to	The expiry date of the certificate.
Valid From	The issuance date of the certificate.
Key Algorithm	The type of algorithm used for encryption.
Key Size	The key size used by the certificate for encryption.
Signature Algorithm	The type of algorithm used for the signing of the certificate.
Inventory	Indicates whether the certificate is managed or external. Clicking **Managed** opens the **Certificate Details** area of the certificate. Selecting **External** displays the option for assigning it to the required organization or department. SCM also allows you to configure automatic assignment of external certificates identified by a discovery scan to respective organizations and departments.
You can use the tool button to select columns to be displayed in the table: 	

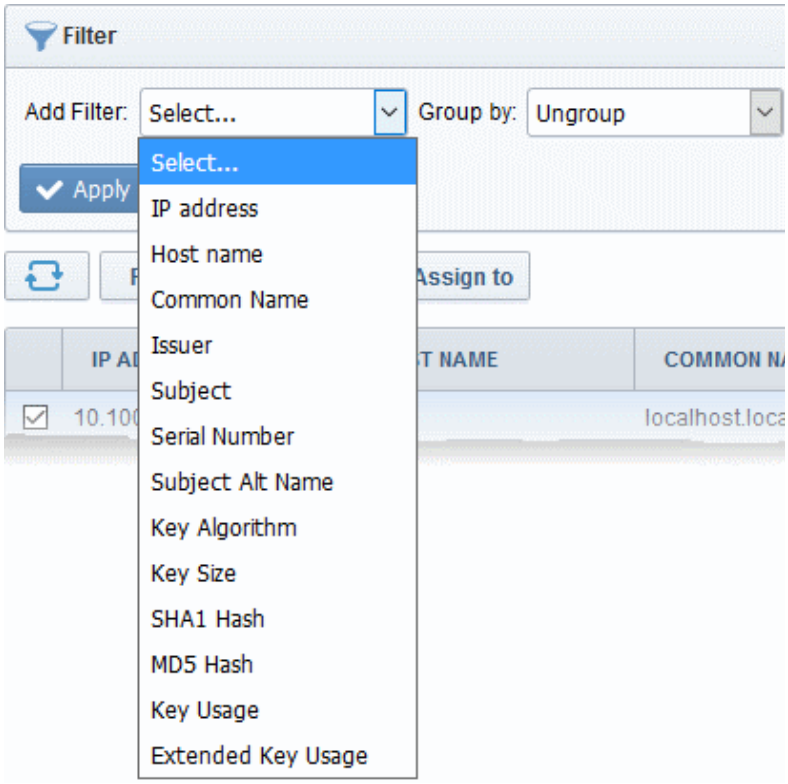
Column	Description
Issuer	Details of the CA that issued the certificate and the name of the certificate.
Subject	Details of the common name, organizational unit, organization, and so on, contained in the **Subject** field of the certificate.
Subject Alt Name	The names of domains for which the certificate is used.
Serial Number	The serial number of the certificate that is unique and can be used to identify 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.
Cipher	The cipher suite used for encryption.
Key Usage	The cryptographic purposes for which the certificate can be used. For example, key encipherment and signing.
Extended Key Usage	Higher level capabilities of the certificate. For example, web server authentication and client authentication.

You can sort items in the alphabetical order by clicking a column header, and you can use filters to search for particular department.

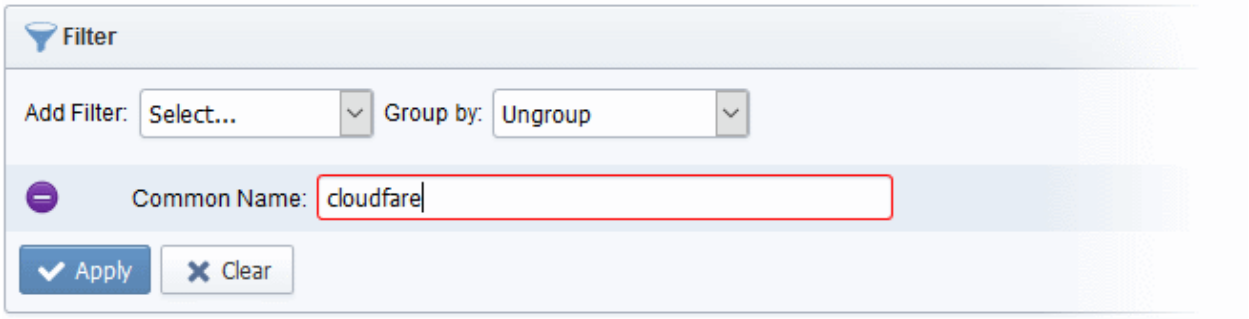
You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.



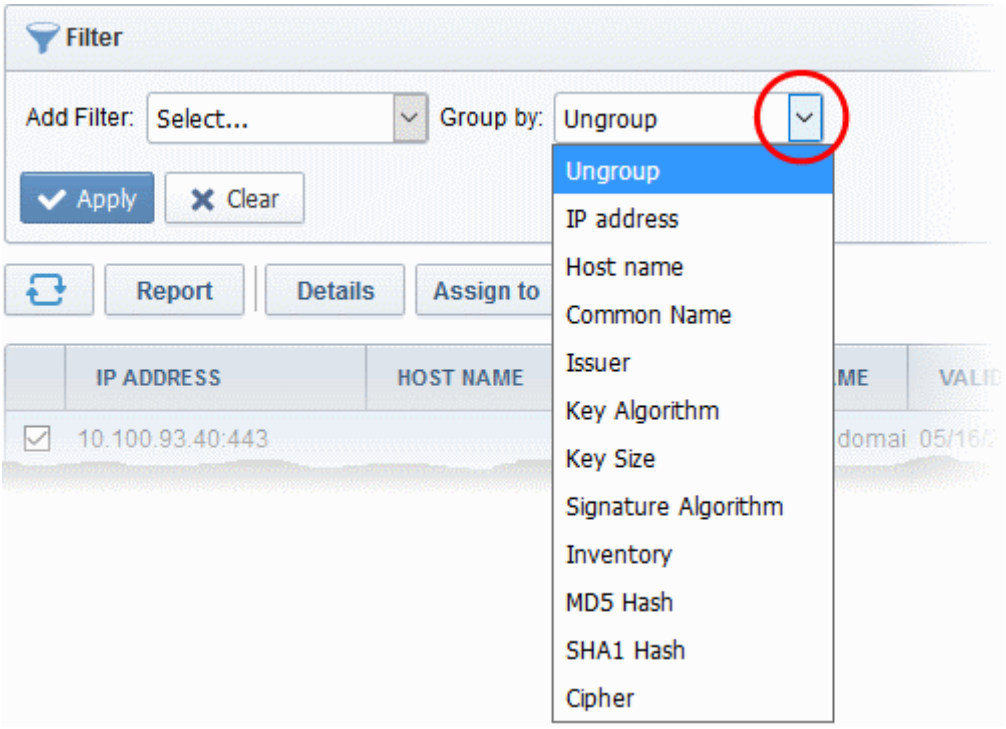
To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection from the **Add Filter** list.



Then you enter or select the filter parameter as per the selected criteria.



After you click **Apply**, filtered items based on the entered parameters are displayed, as shown in the following illustration.

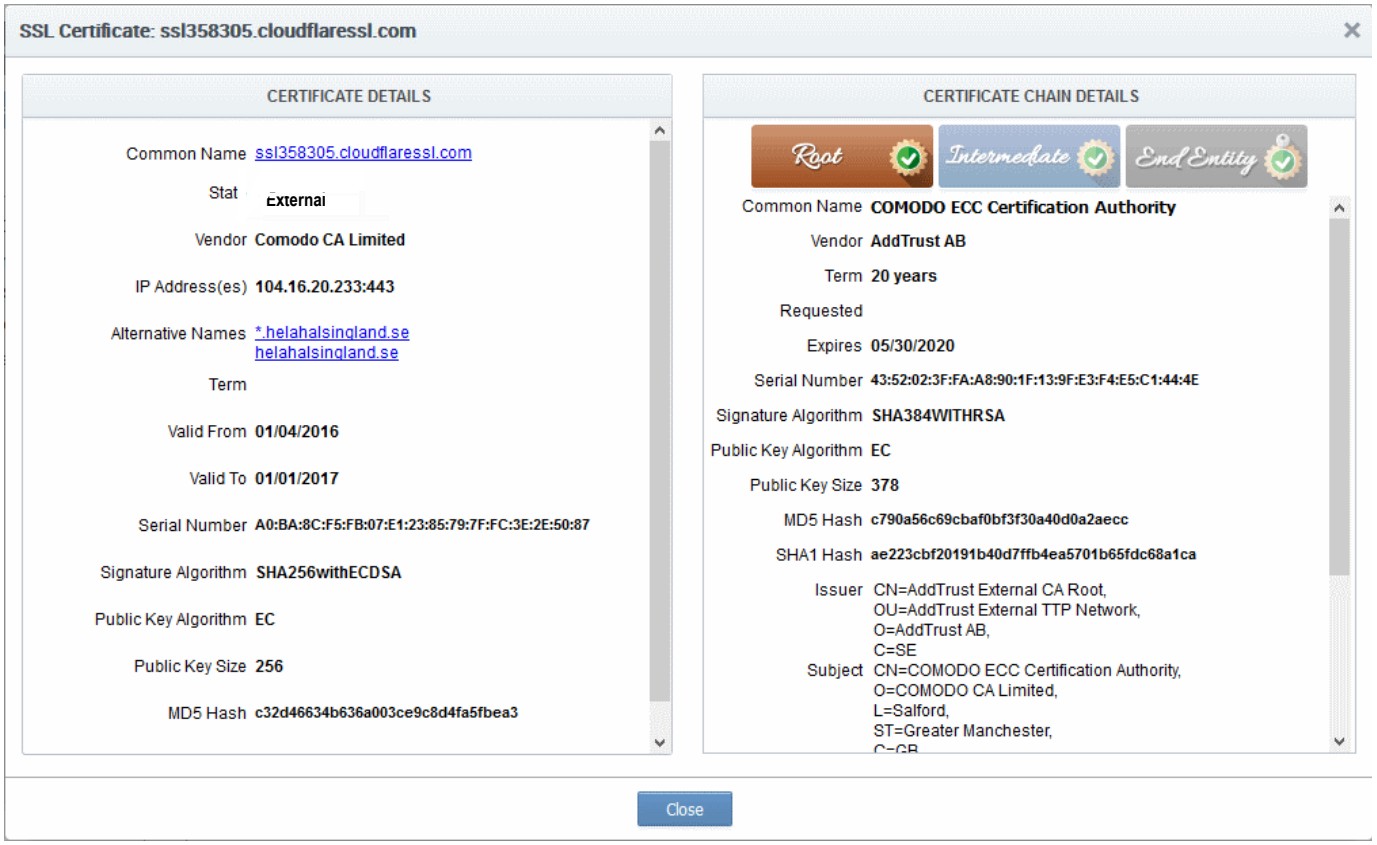


For example, if you want to filter the certificates with a specific common name starting with cloudfare.com and group the results by their Issuer, then select **Common Name** from the **Add Filter** list, enter cloudfare.com and select Issuer from the **Group by** list. The certificates with cloudfare.com in their common name will be displayed as a list, grouped based on their issuers.

You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the area, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

The **Certificate Details** dialog shown in the following illustration displays the complete details of the selected SSL certificate with its certificate chain details. You can view this dialog by selecting the certificate from the list and clicking **Details**. Alternatively, you can click **Managed** in the **Inventory** column



See "How to View and Modify SSL Certificate Details" on page 52 for more information.

8.2.1.1 Manually Assigning a Certificate to Organizations and Departments

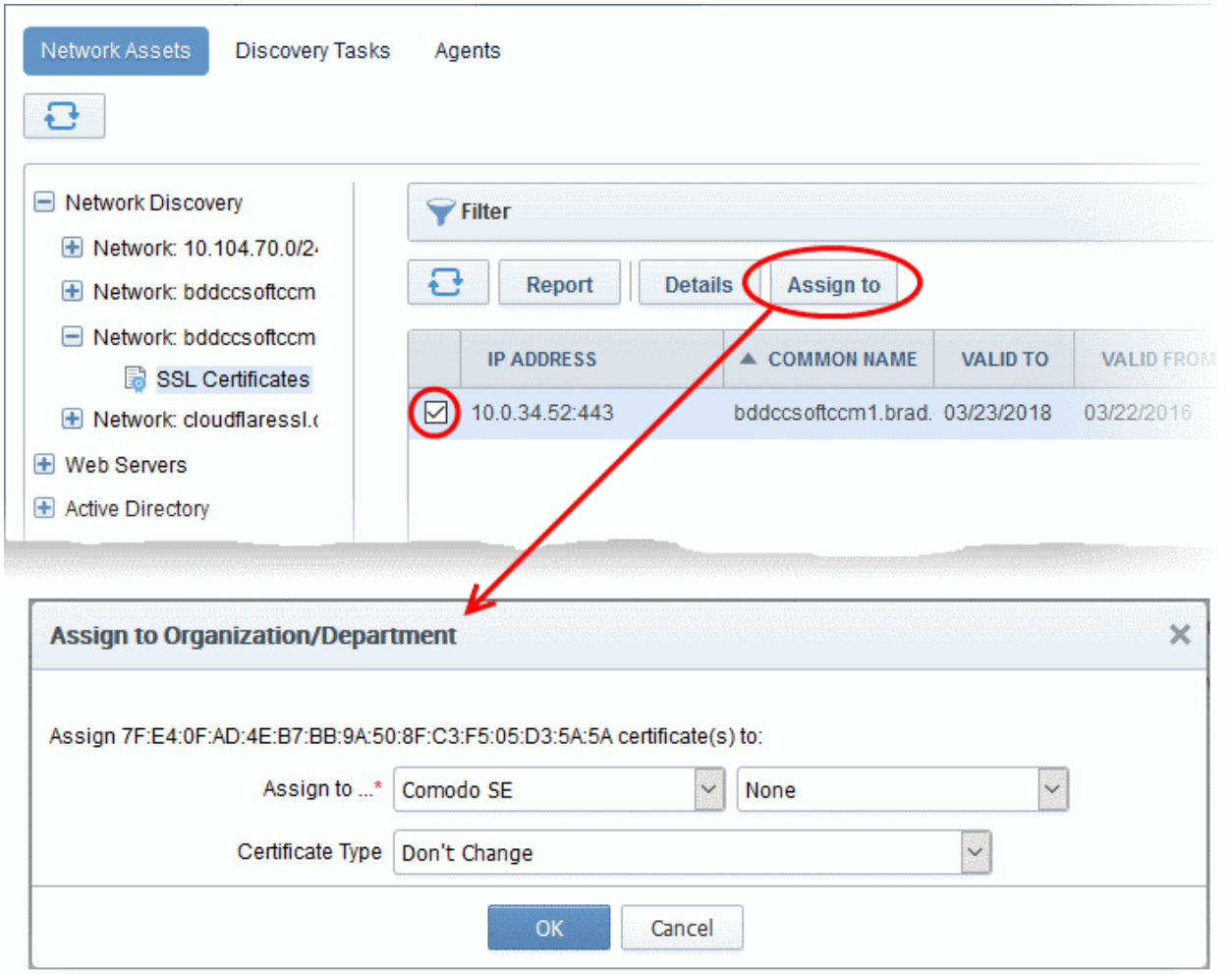
Managed certificates (issued via SCM) are preassigned to their respective organizations or departments specified during their enrollment setup process. There are also external certificates that can be found installed on the network by discovery scans. These certificates are not preassigned to any organization or department by default.

You can configure a discovery scan to automatically assign the external certificates identified by it to respective organizations and department by specifying auto-assignment rules. For more information, see the following:

- "How to Add IP Ranges and Perform Scans" on page 544
- "Managing SCM Agents" on page 509

You can manually assign certificates as follows:

- From the main SCM UI, to navigate to **Discovery > Network Assets > Network Discovery** and expand it to view the list of scanned networks.
- Expand a specific network and select **SSL Certificates** to access a list of SSL certificates installed on the network.
- Select the external certificate from the list and click **Assign To** to open **Assign to Organization/Department** dialog, as shown in the following illustration.



Use the **Assign To** field to specify the organization and, optionally, department to which the certificate should be assigned, and then click **OK**.

8.2.1.2 Generating a Report on Discovered Certificates

You can generate a report on the certificates discovered on the specified network in the **Network Assets** area, as follows:

- From the main SCM UI, to navigate to **Discovery > Network Assets > Network Discovery** and expand it to view the list of scanned networks.
- Expand a specific network and select **SSL Certificates** to access a list of SSL certificates installed on the network.
- Click **Report**.

The report is generated as a spreadsheet containing the list of certificate with their details. You can download the report in a `.xls` format.

8.2.2 How to View the Web Server Information

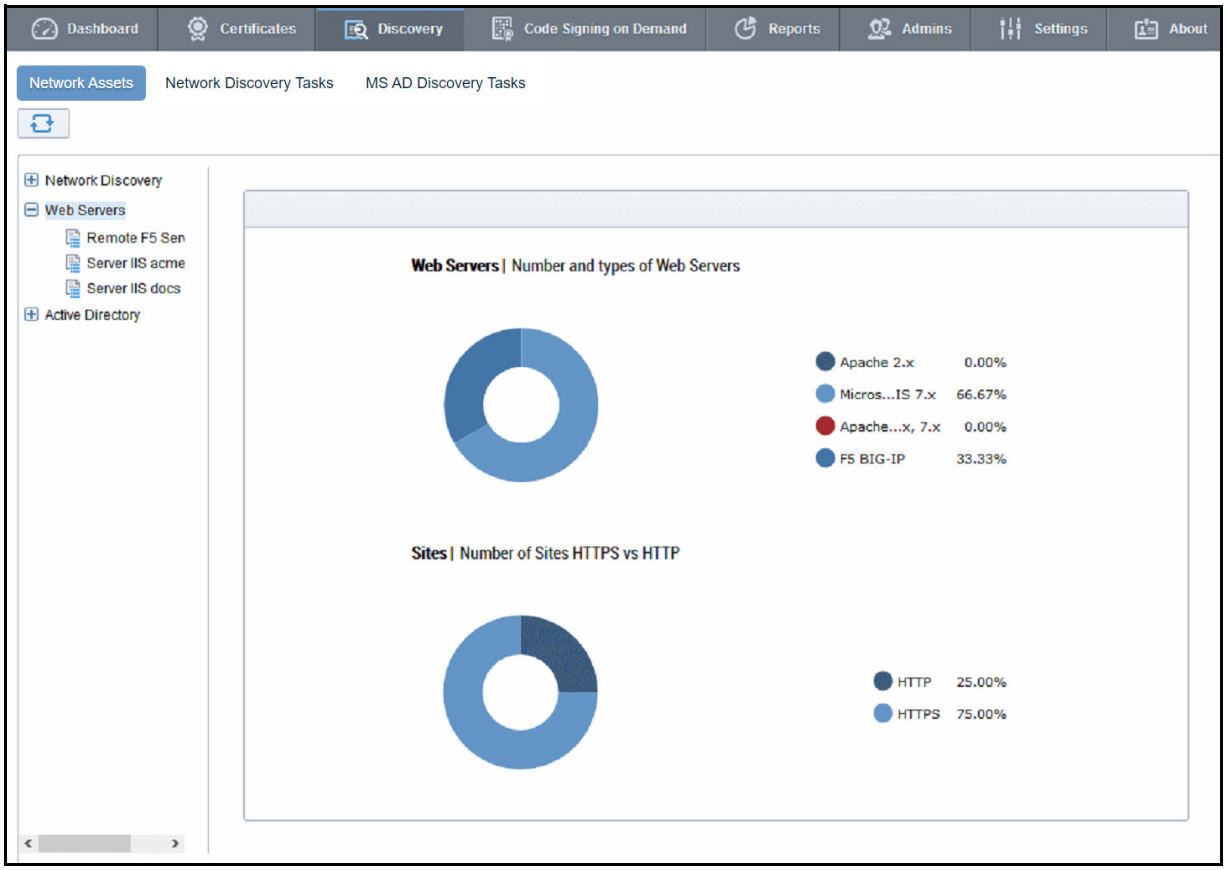
Depending on your security role as an administrator, **Web Servers** allows you to view a summary of all web servers identified on every scanned network. The results include all domains hosted on each server.

A MRAO can view details of all web servers from all networks on which the scans have been ran.

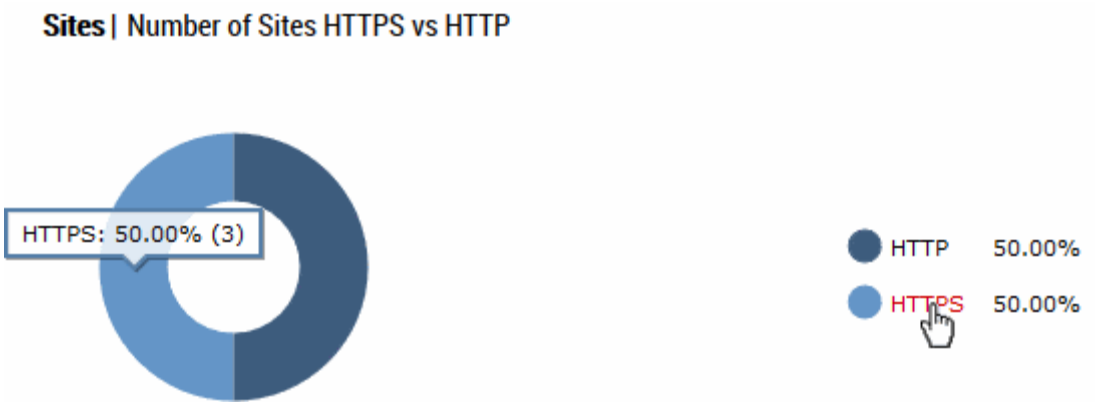
A RAO SSL can view details of web servers pertaining to organizations and their departments that have been delegated to these administrators.

A DRAO SSL can view details of web servers pertaining to departments that have been delegated to these administrators.

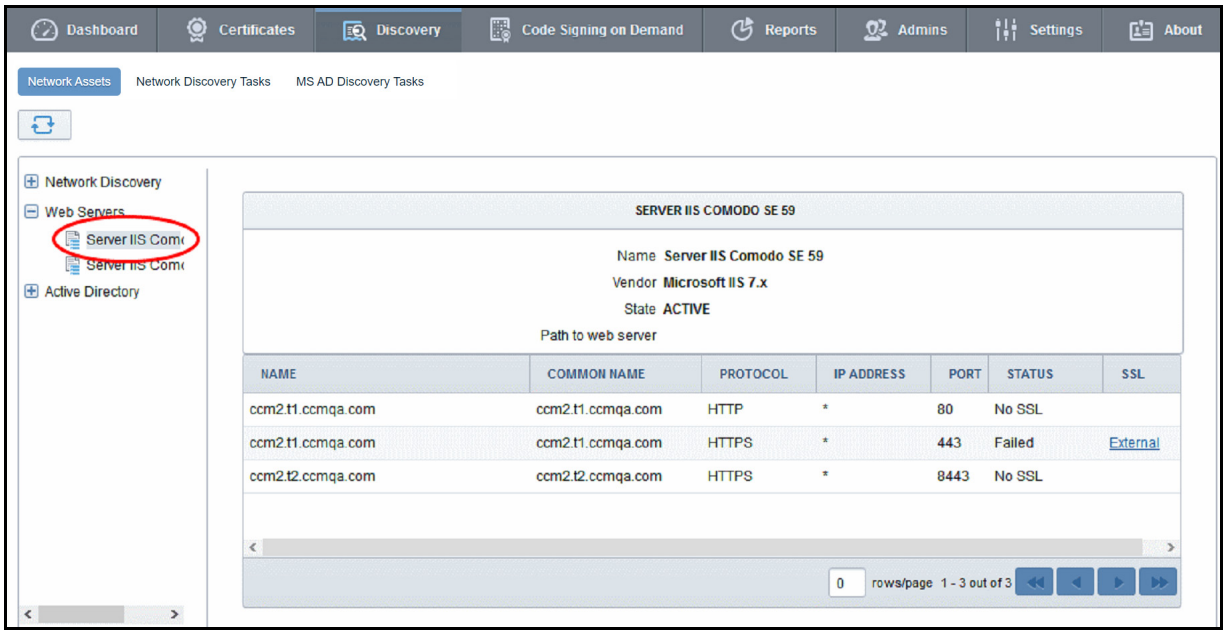
To view summary of web servers identified on all scanned networks, you use th main SCM UI to navigate to **Discovery > Network Assets > Web Servers**, as shown in the following illustration.



The area displays the percentage of scanned web servers using different operating systems and the percentage of those servers using HTTPS versus HTTP. Hovering over a chart segment or legend item displays additional details, such as the exact number of servers or sites in that category.



To view details of websites or domains hosted on each server in scanned networks, select that server, as shown in the following illustration.



The following table lists settings of the **Web Servers** area.

Column	Description
Name	The name of the website or domain.
Common Name	The registered domain name for website or domain.
Protocol	The data transfer protocol used by the website.
IP Address	The address where the site is hosted.
Port	The server port number through which the site is served.

Column	Description
Status	Indicates whether or not the site is secured with SSL/TLS.
SSL	For HTTPS sites, indicates whether the certificate used by the site is managed by SCM or not. Clicking the entry opens the **Certificate Details** area.

8.2.3 How to View Certificates Via Active Directory

Depending on your security role as an administrator, **Active Directory** allows you to view all certificates installed on endpoints in your network, including device authentication certificates.

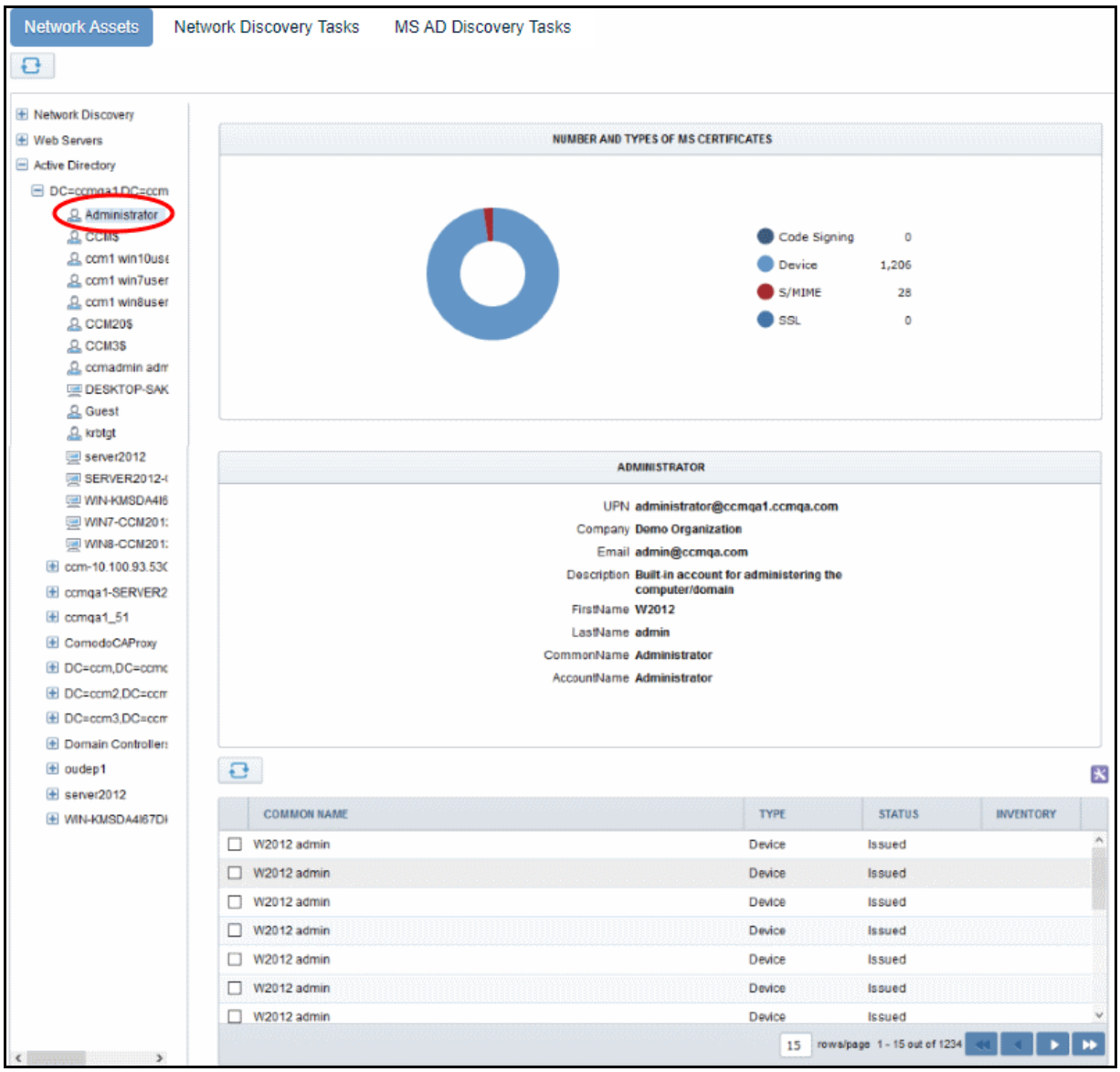
MRAOs can view details from all AD servers and networks for all organizations, assuming the following conditions have been met:

- AD servers have been added to SCM by installing the MS Agent on them.
- **Enroll on Behalf** was enabled on the MS Agent during installation in order to generate certificates using MS CA.
- The agent periodically scans the AD server, fetches network structure and users, and forwards these details to SCM.

See "Configuring MS Agents" on page 266 for more information.

You view network structure and details of certificates installed on endpoints as follows:

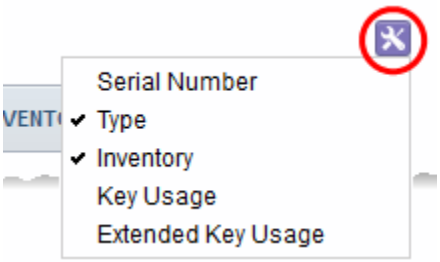
- Use the main SCM UI to navigate to **Discovery > Network Assets > Active Directory**, as shown in the following illustration.
- Expand **Active Directory**, select the network and expand it to see the lists all objects in the network that have a certificate.
- Select an object to view details of its certificates.



As shown in the preceding illustration, the chart displays the types and quantities of certificates discovered for the **Active Directory** object, the center panel displays additional details about the selected AD object, and the lower panel presents a list of all discovered certificates for the object:

The following table lists elements of the **Active Directory** area.

Column	Description
Common Name	The domain name, user name, or device name for which the certificate was issued.
Type	The type of the certificate, such as SSL, client, code signing or a device authentication certificate.

Column	Description
Inventory	Indicates whether the certificate is managed or external. Clicking **Managed** opens the **Certificate Details** area of the certificate. Selecting **External** displays the option for assigning it to the required organization or department. SCM also allows you to configure automatic assignment of external certificates identified by a discovery scan to respective organizations and departments.
You can use the tool button to select columns to be displayed in the table: 	
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	Higher level capabilities of the certificate. For example, web server authentication and client authentication.

You can hover over a chart segment to view additional details such as the exact number of servers or websites in that category.

You can select a certificate and click the **Details** to see more information related to the certificate.

8.3 Performing Network Discovery Tasks

The **Network Discovery Tasks** area shown in the following illustration allows you to scan and monitor a network for all installed SSL certificates, including Sectigo certificates that may or may not have been issued using SCM, any third party vendor certificates, and any self-signed certificates.

Depending on your security role as an administrator, you can configure discovery tasks for different networks to be scanned and can optionally set a schedule for them for periodical scanning.

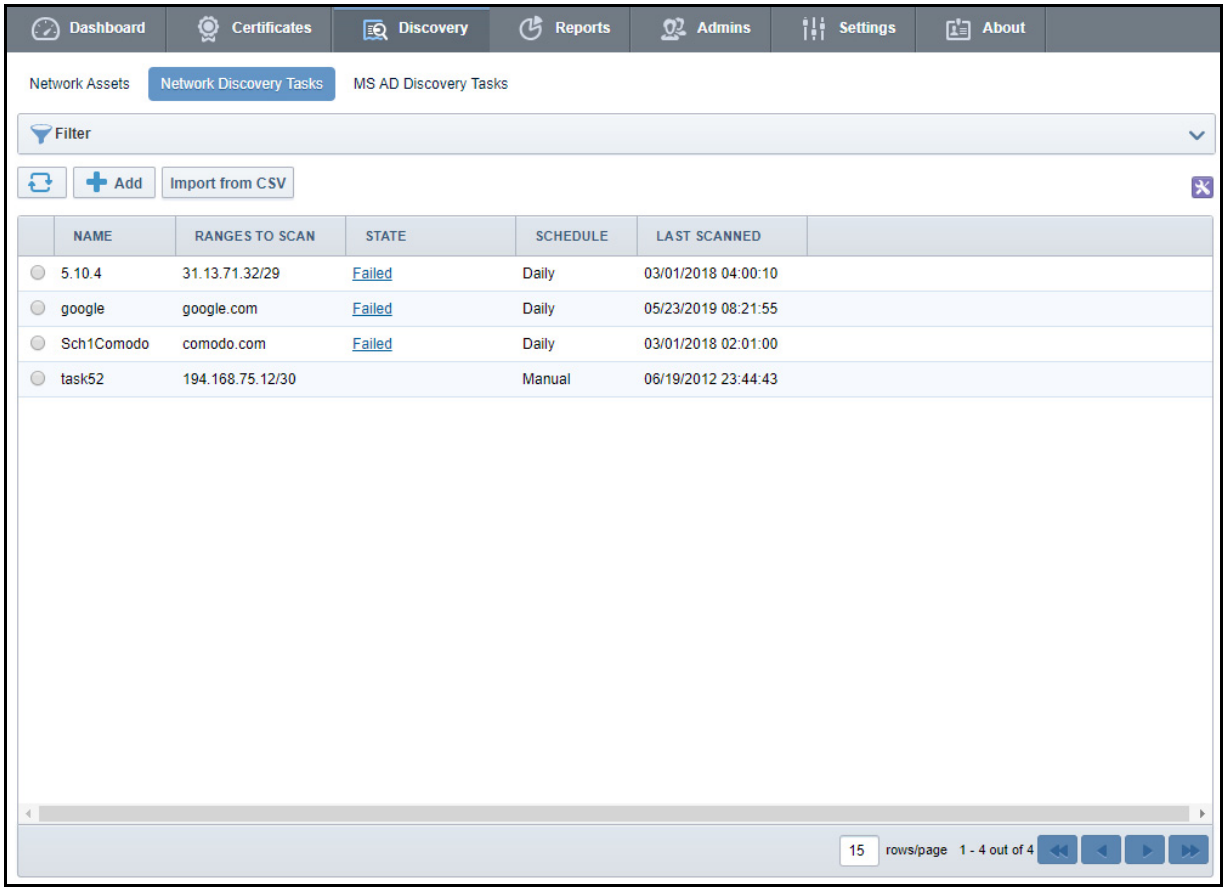
A MRAO can scan for certificates installed on any network pertaining to the organization or department.

A RAO can scan for certificates installed on networks pertaining to organizations and their departments that have been delegated to this administrator.

A DRAO can scan for certificates installed on networks pertaining to departments that have been delegated to this administrator.

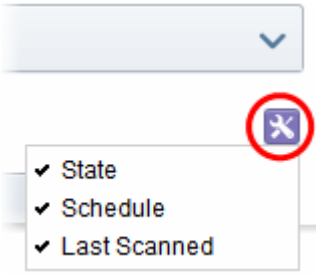
Each discovery task can also be added with auto-assignment rules so that external certificates identified from that discovery scan are assigned to the respective organizations or departments and added to the **SSL Certificates** area.

The **Network Discovery Tasks** area displays a list of tasks added to SCM and allows you to create new discovery tasks and modify existing tasks.



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

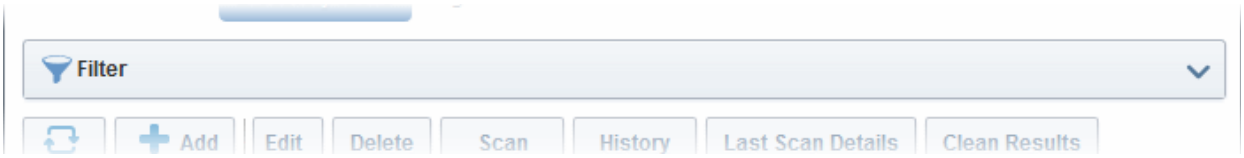
Field / Element	Value	Description
Name		The name of the certificate discovery task.
Ranges to Scan		The IP ranges that are to be scanned during this task.
State		The status of the scan that indicates whether it is successful, failed, in progress, or canceled. Clicking the state displays respective result. For example, clicking Successful displays the number of certificates discovered.

Field / Element	Value	Description
Schedule		Indicates whether the scan is to be run manually or scheduled.
Last Scanned		The date and time of the last scan performed.
You can use the tool button to select columns to be displayed in the table: 		
Controls	Add	Adds a new certificate discovery task.
	Refresh	Updates the list of displayed discovery tasks.
Discovery Task control Buttons [a]	Edit	Enables you to edit the selected discovery task, such as change the IP range.
	Delete	Enables you to delete a discovery task from the list.
	Scan	Enables you to start a new scan for the selected discovery task.
	Cancel	Cancels a discovery scan.[b]
	History	Displays the details of past scans performed for the selected discovery task and allows you to download scan reports.
	Last Scan Details	Displays the results of the last scan for the selected discovery task.
	Clean Results	Removes all the discovered certificates from the **SSL Certificates** area.

a. Visible only on selecting a domain.
b. Appear after starting a new scan.

You can sort items in the alphabetical order by clicking a column header, and you can use filters to search for particular department.

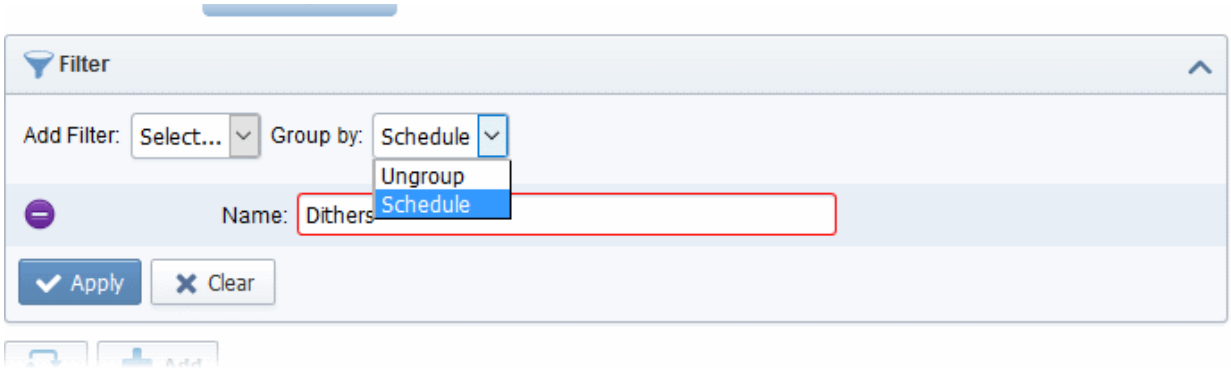
You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.



To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection from the **Add Filter** list.

Filter Criteria	Filter Parameter
Name	Enter the name of the discovery task fully or in part

Then you enter or select the filter parameter as per the selected criteria.



After you click **Apply**, filtered items based on the entered parameters are displayed:

You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the area, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

Prior to starting the process, you need to ensure that the Network Agent has been installed and configured, as described in "Configuring Network Agents" on page 252.

You start by running a scan of networks in order to find all deployed SSL certificates. SCM automatically integrates all newly discovered certificates and adds (1) to **SSL Certificates** area, all managed certificates and external certificates auto-assigned to respective organizations or departments based on assignment rules applied to the discovery task, and (2) to lists of certificates under respective networks in the **Network Assets** area, all managed certificates and all external certificates including those not assigned to any organization or department. You can manually assign external certificates to organizations and departments to which they pertain in order to bring them under management through the **SSL Certificates** area. For more

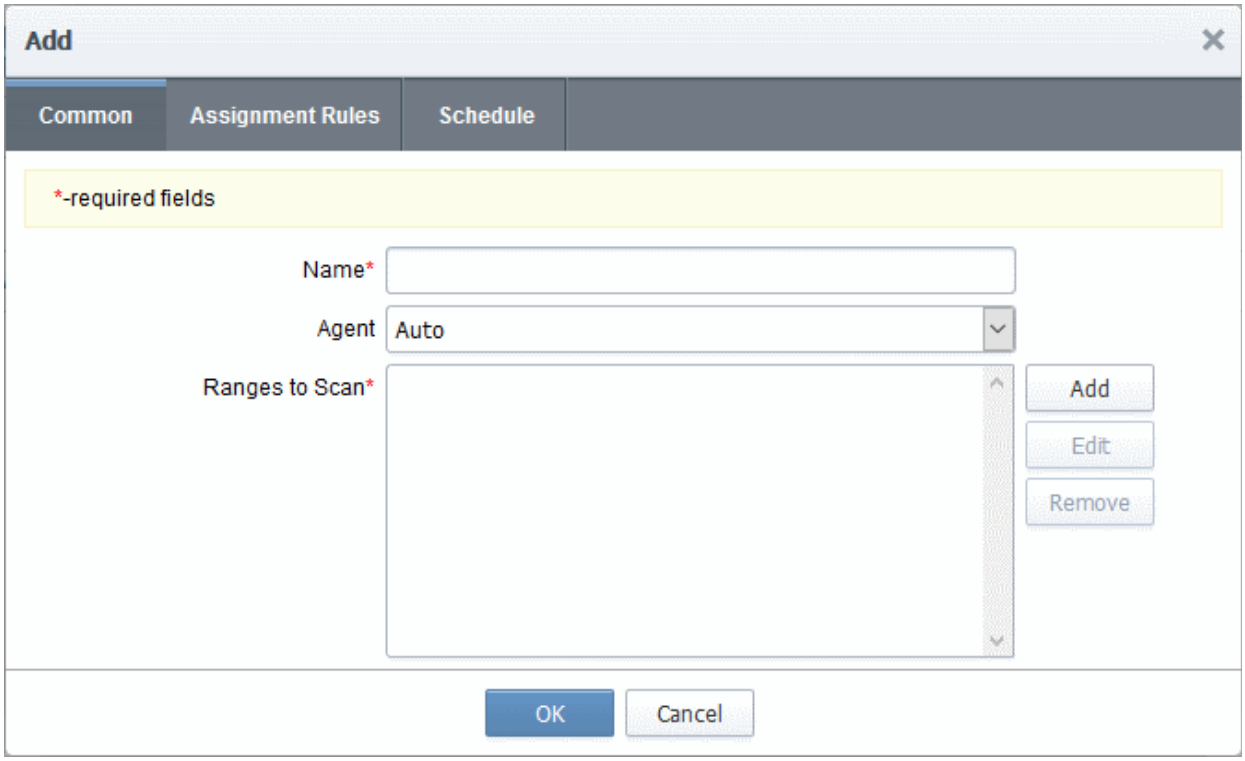
information, see "Performing Network Discovery Tasks" on page 540. If necessary, SCM updates the status of existing certificates that were issued using SCM. External certificates can become managed after their renewal. You can view the results of the scan can be viewed in the discovery scan log.

8.3.1 How to Add IP Ranges and Perform Scans

To add a new network discovery scan task, you navigate to **Discovery > Network Discovery Tasks** and click **Add** to open the scan configuration form shown in the following illustration.

The **Common** area is used to configure scan settings, the **Assignment Rules** area is used to apply auto-assignment rules, and the **Schedule** area is used to schedule the scan.

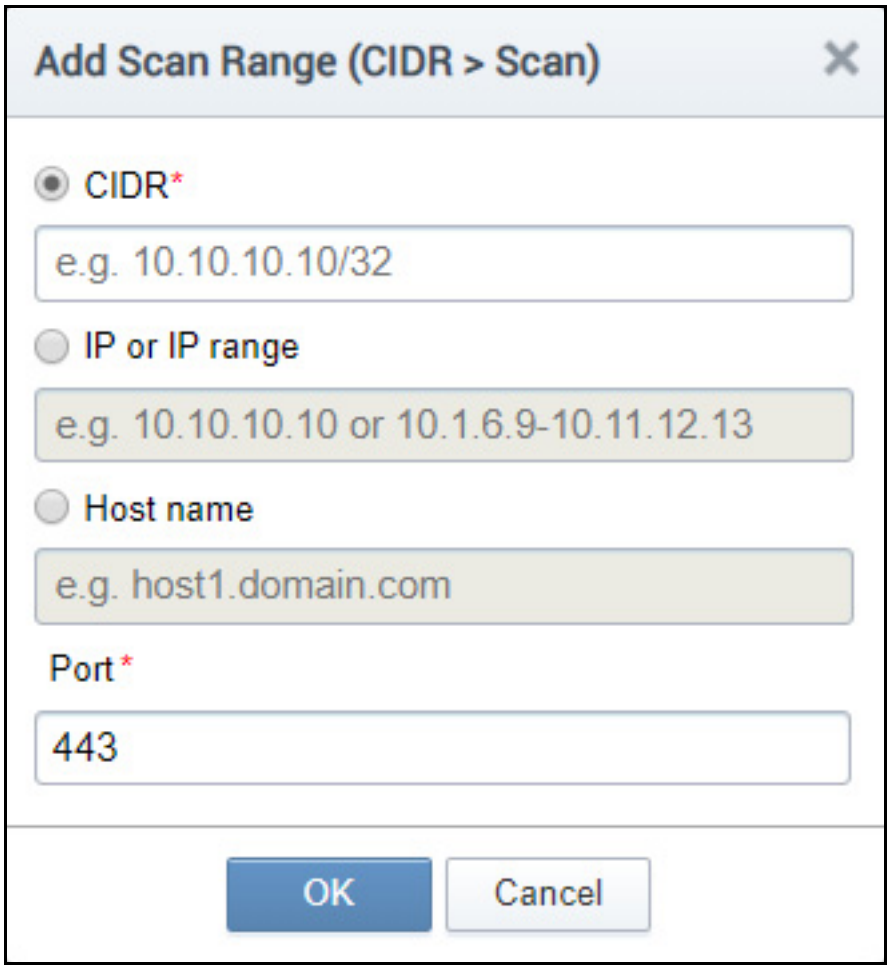
Complete the **Common** area shown in the following illustration based on descriptions provided in the following table.



Field / Element	Description
Name	The name to describe the discovery task.
Agent	The SCM agent to be used for scanning. SCM uses agents installed on internal servers to scan for certificates.

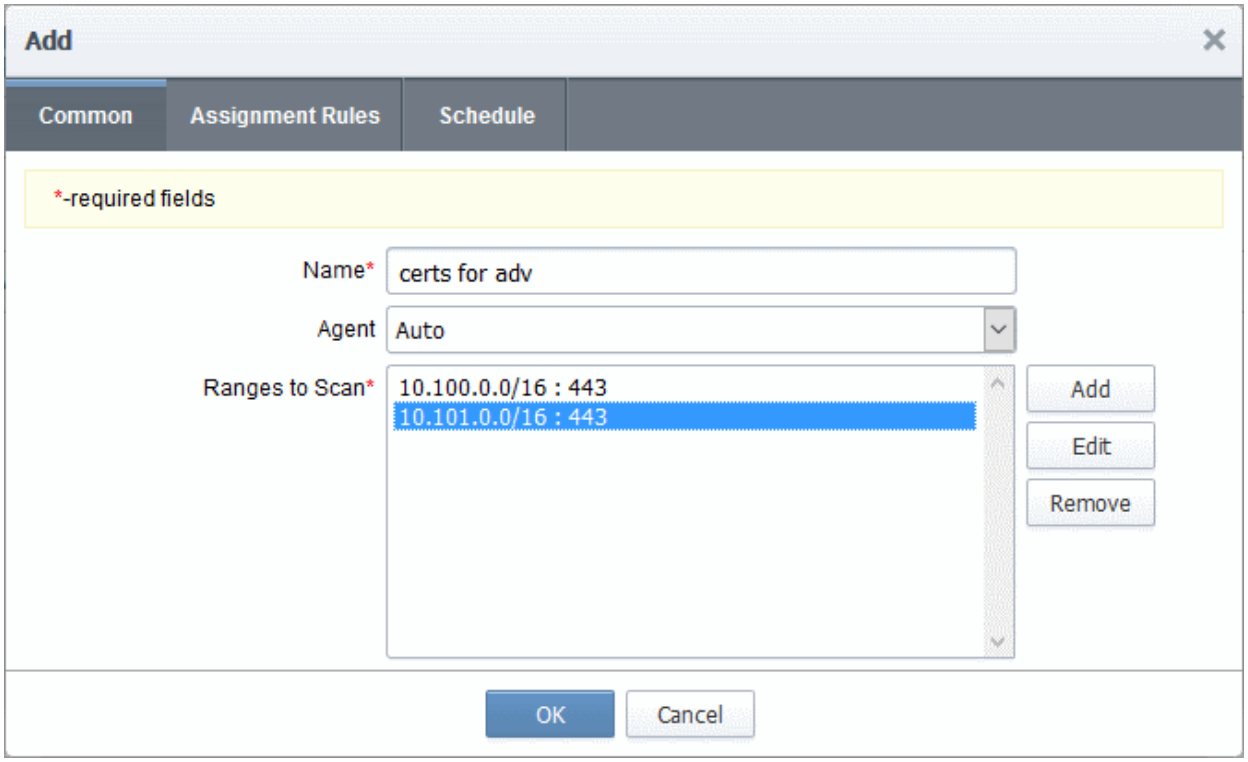
Field / Element	Description
Ranges to Scan	The IP address ranges of servers to be scanned.
Add	Adds IP ranges for scanning.
Edit	Edits the selected scan range.
Remove	Deletes the selected scan range.
OK	Adds the discovery task to the list.
Cancel	Cancels the task.

If adding IP ranges, you need to complete the following dialog based on the information provided in the following table.

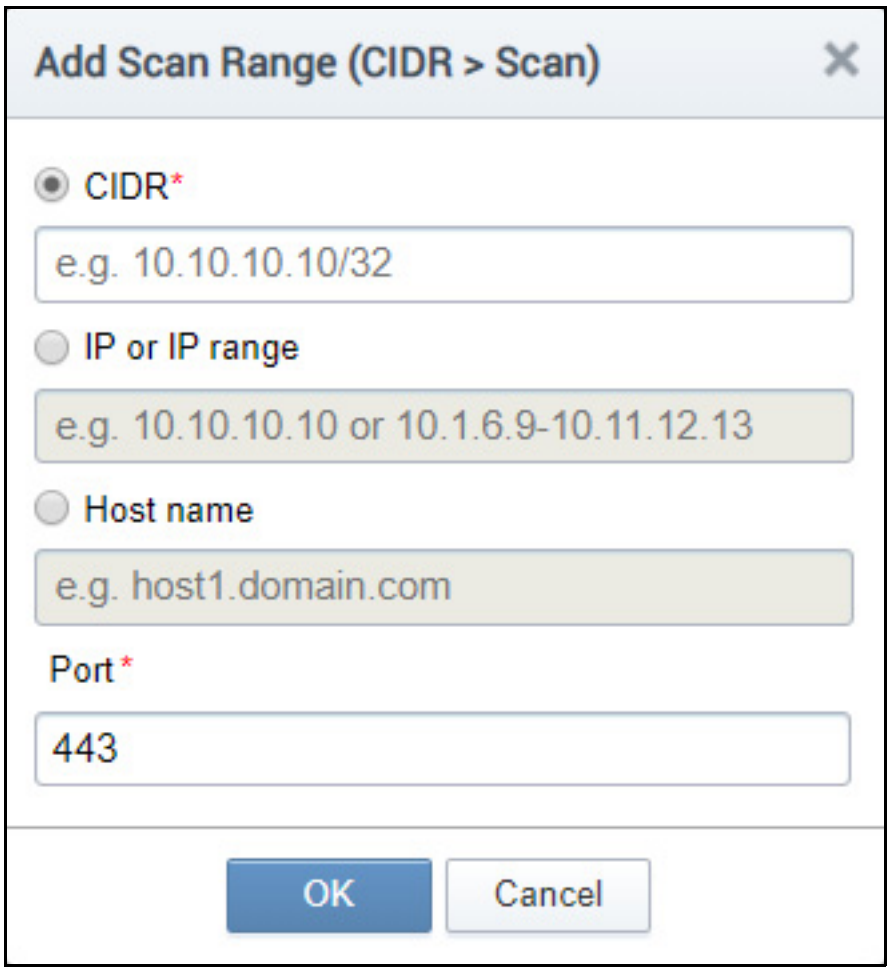


Field	Description
CIDR	The IP address you wish to scan followed by a network prefix, such as 123.456.78.91/16.
IP or IP range	The IP address or IP range to scan.
Host name	The host name to scan.
Ports to Scan	The port numbers for IP range.
OK	Adds specified data into the scan list.
Cancel	Cancels the process

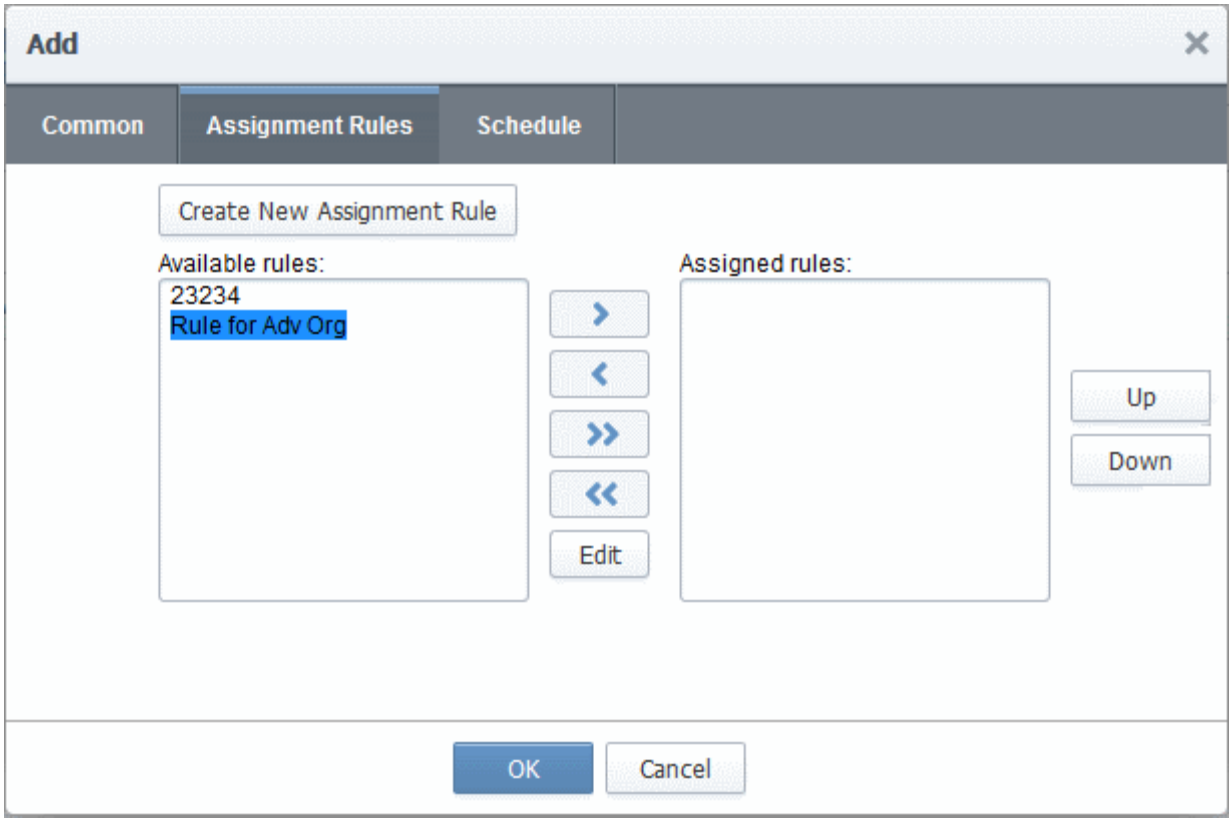
You can add more scan ranges for the same discovery task. Repeat the process if necessary.



Upon completion, the entered scan ranges are displayed. You can modify or remove the scan range after selecting it and clicking **Edit** or **Remove**.



Complete the **Assignment Rules** area shown in the following illustration to add rules which assign external certificates identified by the scan to an organization or department.

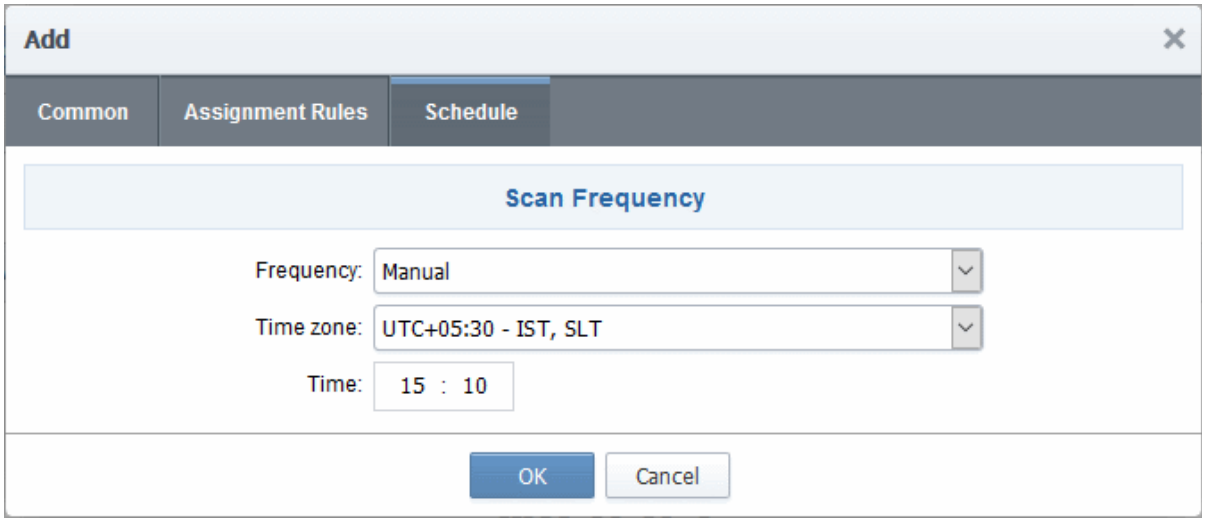


Use the arrows to add rules to the discovery task. Rules can be configured in the **Assignment Rules** area, as described in "Managing SCM Agents" on page 509.

To create a new rule, click **Create New Assignment Rule**. When the rule is added to the **Available Rules** list, select it and move to the **Assigned Rules** list.

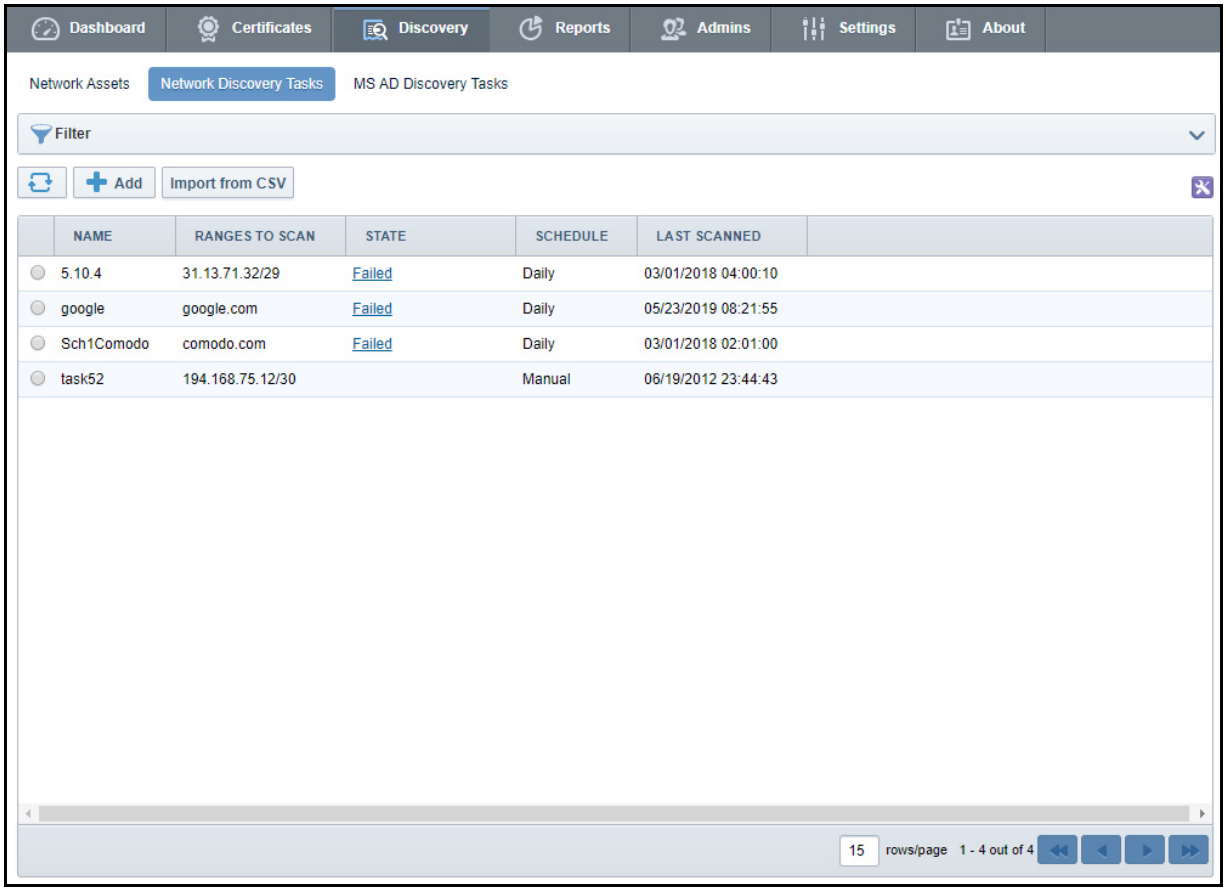
To modify a rule, select it and click **Edit**.

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

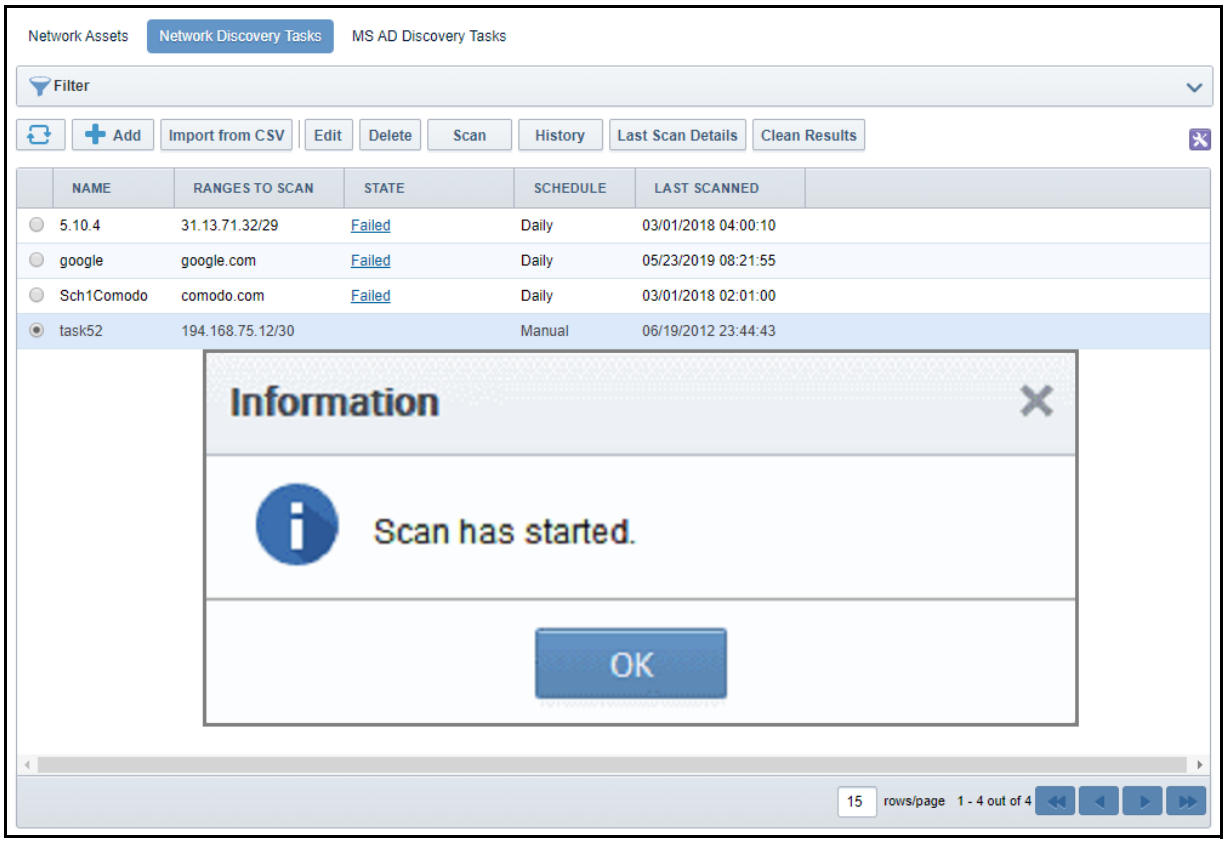


Available scan frequencies are Manual (on demand), Daily, Weekly, Monthly, Quarterly, Semi-Annually and Annually.

The newly created discovery task is displayed in the list, as shown in the following illustration.



You may repeat the process to add more network discovery tasks. To run a scan, select the respective discovery task from the list and click the **Scan** to commence the discovery scan for the selected task, as shown in the following illustration.



You can manually start a scan only for discovery tasks scheduled to be run manually. Other scan runs as per the schedule set for the task.

SCM allows you to run multiple discovery tasks at the same time: after a scan has started, select another task and click **Scan**.

Discovery scanning uses a 2 second timeout for each IP/Port combination with 10 threads running at once, as follows:

```
((# IP Addresses) * (# ports per address)) / 300 = Number of minutes for scan
```

This information can be used to estimate how long a scan takes.

The timeout interval and number of threads per minute may be subject to minor fluctuation. It is recommended that you treat these figures as an approximate calculation of scanning times.

Example:

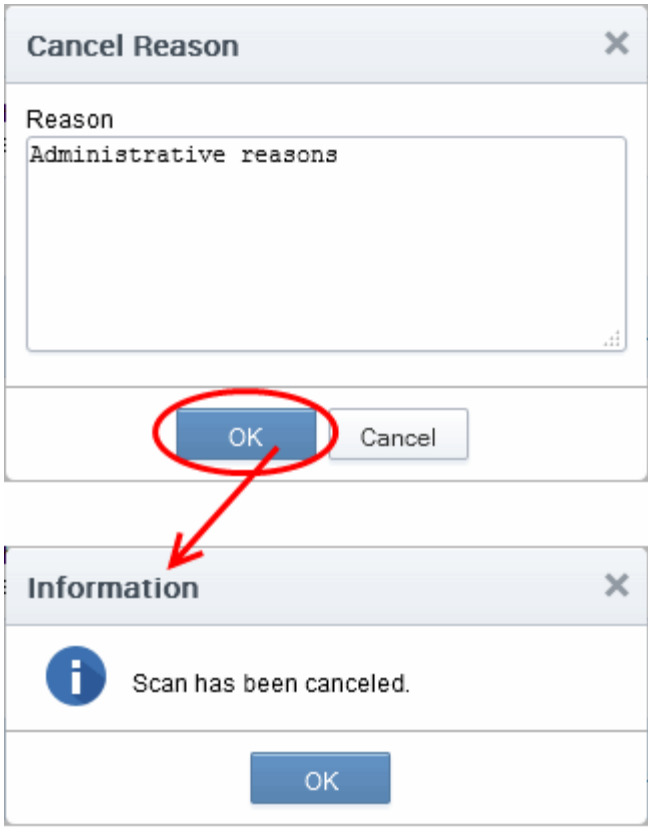
Scanning a single range xxx.xxx.0.0/16 for a single port (443) equals 65,536 IP addresses.

((65536)(1))/300 = approx 218 minutes.

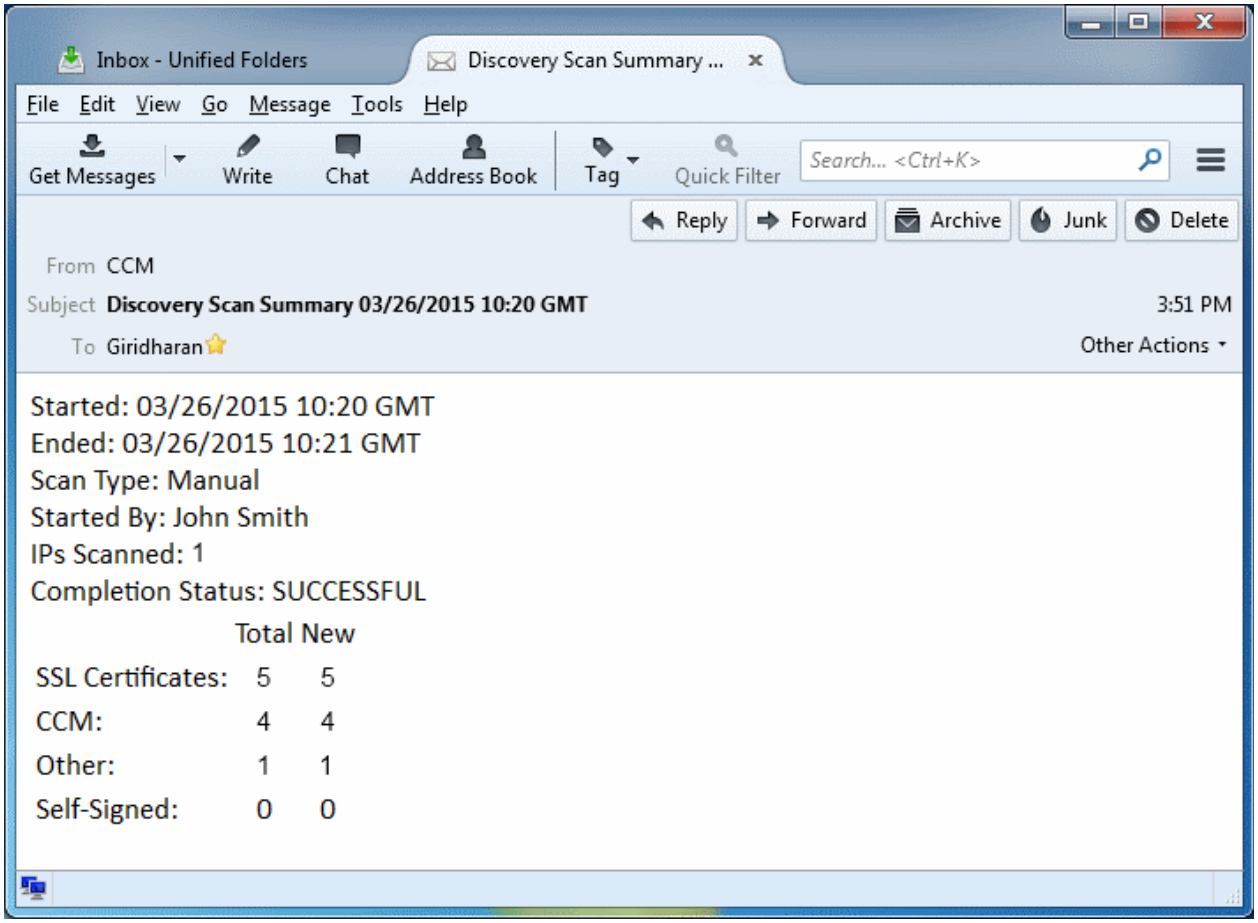
The progress of the scan can be viewed in the row of the selected discovery task under the **State** column.

To cancel the scanning process, click **Cancel**, and the entire system reverts to the state that existed before the scan started (for example, any data collected during scanning cannot be applied until the scanning process is completed).

If you cancel the scanning, you should specify the reason for it in the **Cancel Reason** dialog shown in the following illustration.



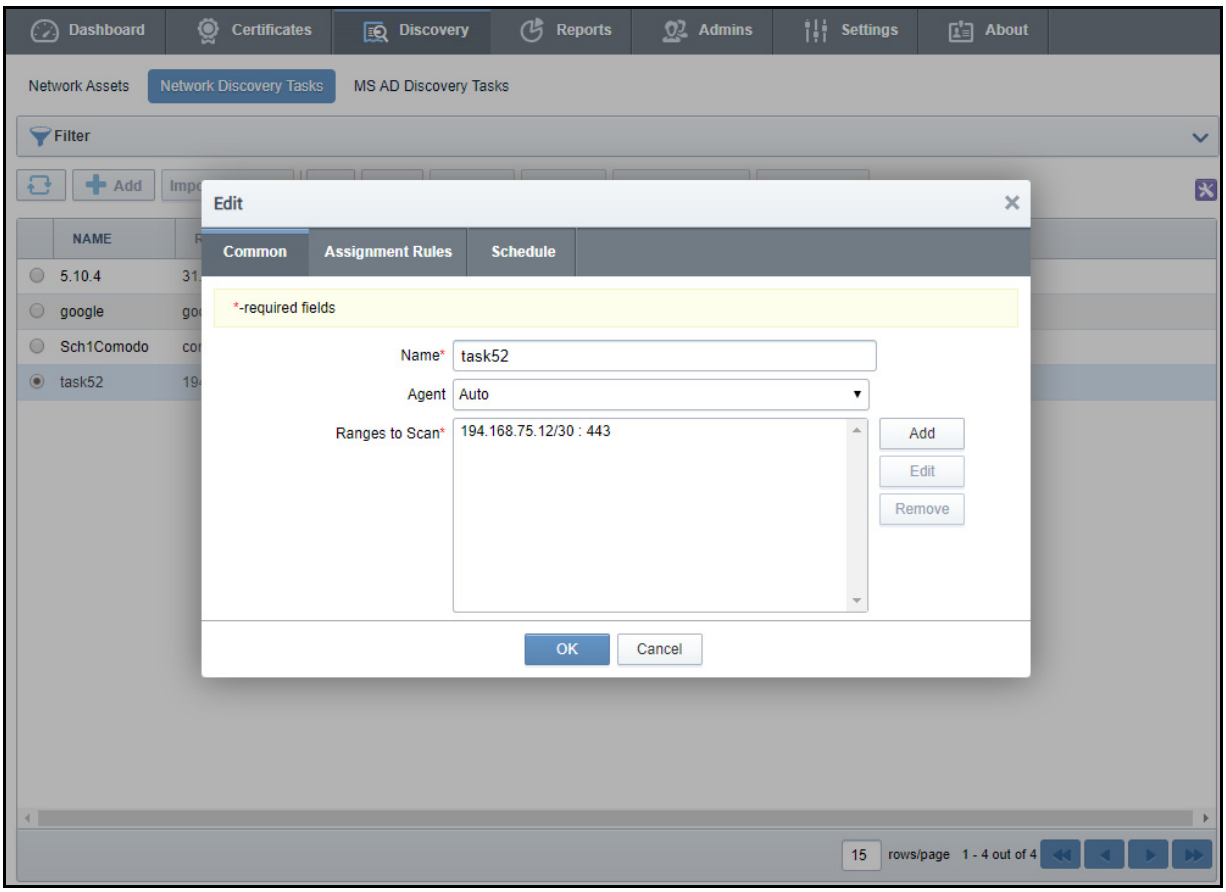
After the scan is complete, you are notified of the result via email, assuming the email notification was configured in the **Discovery Scan Summary** notifications area, as shown in the following illustration.



The results of the scan can be viewed via the **SSL Certificates** area and the **Reports** area.

8.3.2 How to Modify a Discovery Task

You can edit an existing discovery task by selecting it in the list and clicking **Edit**, as shown in the following illustration. The **Edit** dialog is similar to the **Add** dialog and allows you to change the task name, select another agent, add a new scan range, edit existing scan ranges, or remove it. In the **Schedule** area, the scan frequency can be modified. See "How to Add IP Ranges and Perform Scans" on page 544 for more information.



8.3.3 How to Import Multiple Network Discovery Tasks from a CSV File

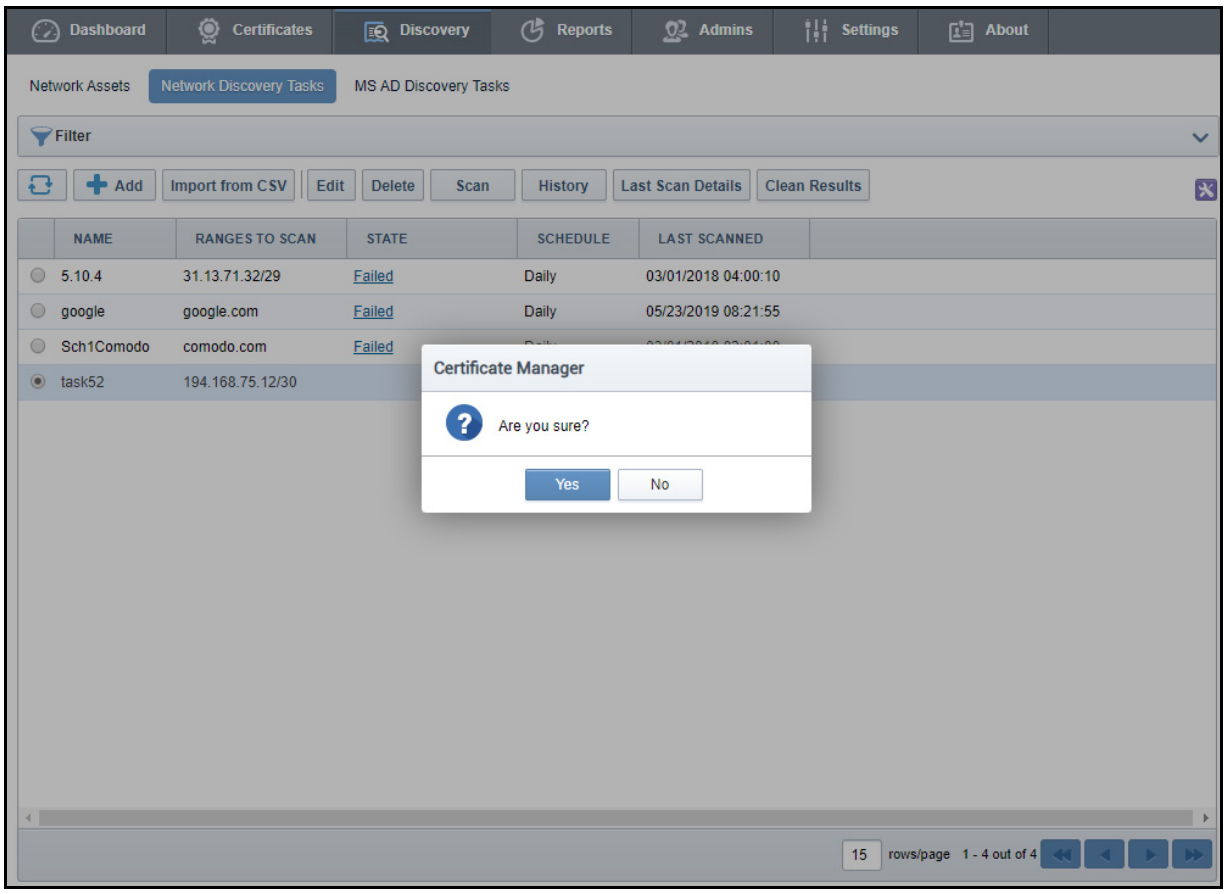
To add multiple network discovery tasks using a .csv file, do the following:

1. Navigate to **Discovery > Network Discovery Tasks**.
2. Click **Import from CSV**.
3. Click **Choose File** and browse to your .csv file.
4. Select your .csv file and click **Submit**.
5. Once the upload is complete, click **Close**.

NOTE: For more information on how to structure .csv files for importing network discovery tasks, see Appendix B CSV Import Format Requirements.

8.3.4 How to Delete a Discovery Task

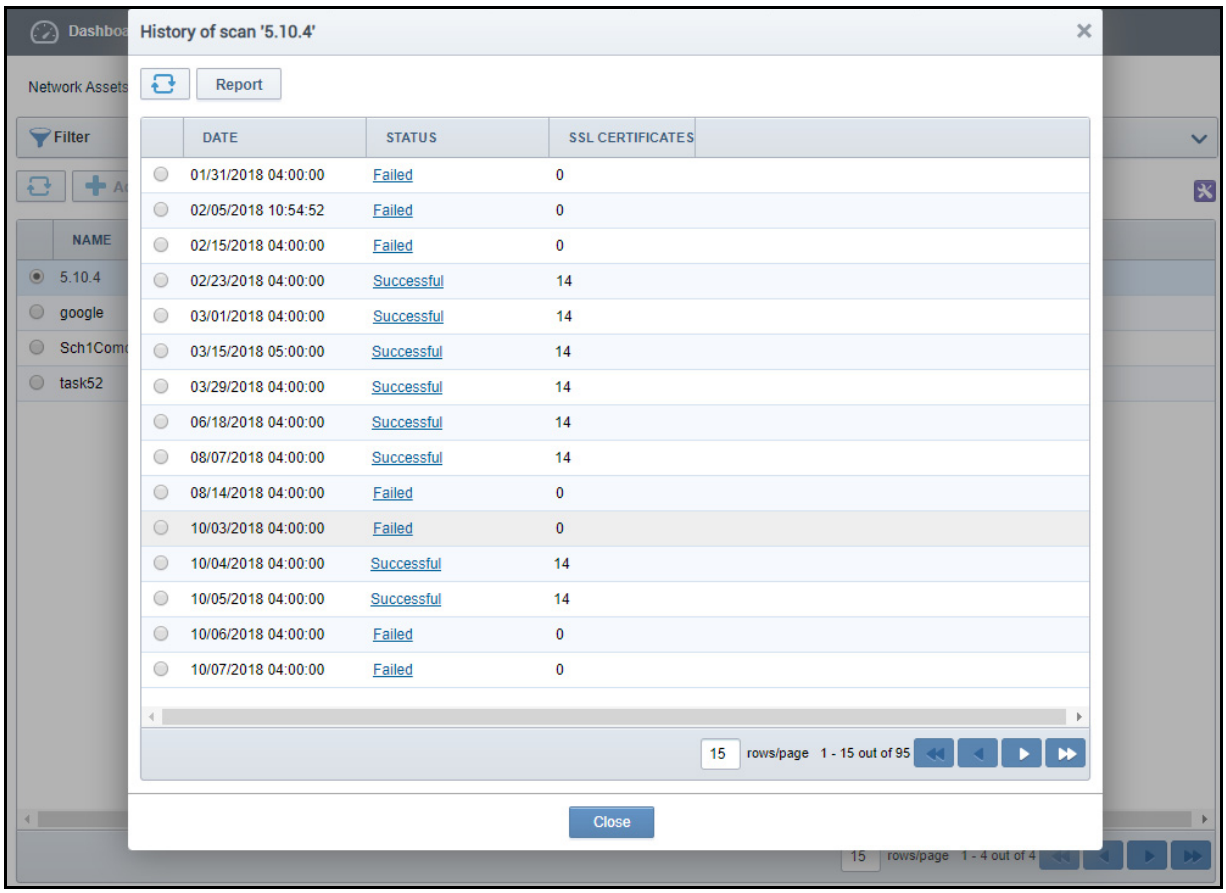
To delete a discovery task from the list, select it and click **Delete**, as shown in the following illustration.



8.3.5 How to View History of Network Discovery Tasks

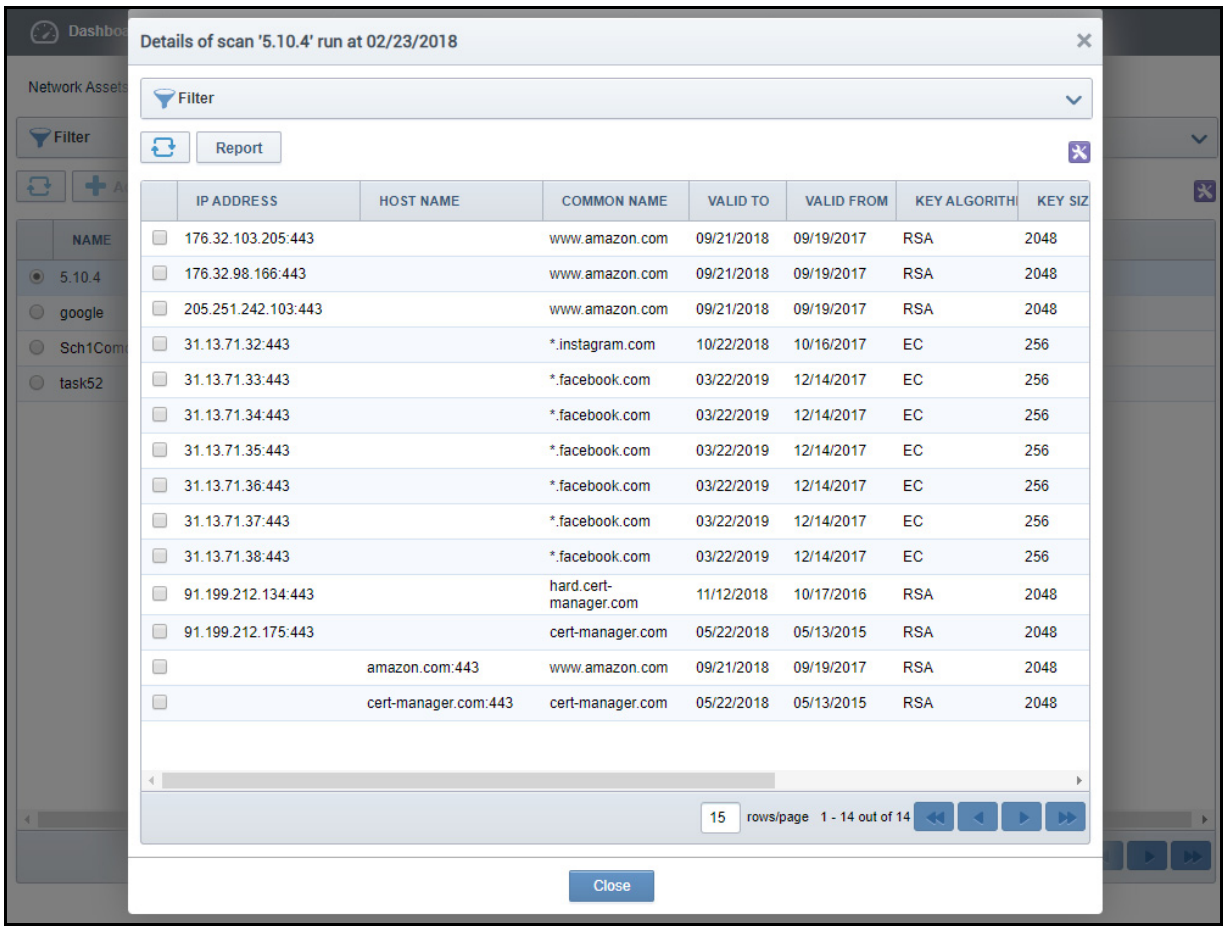
SCM allows you to view the previous five scan results of each discovery task. You can also download a report on each task and assign external, discovered certificates to an organization or department.

To view the history of a discovery task, select it and click **History** to open the **History of scan** dialog, as shown in the following illustration.

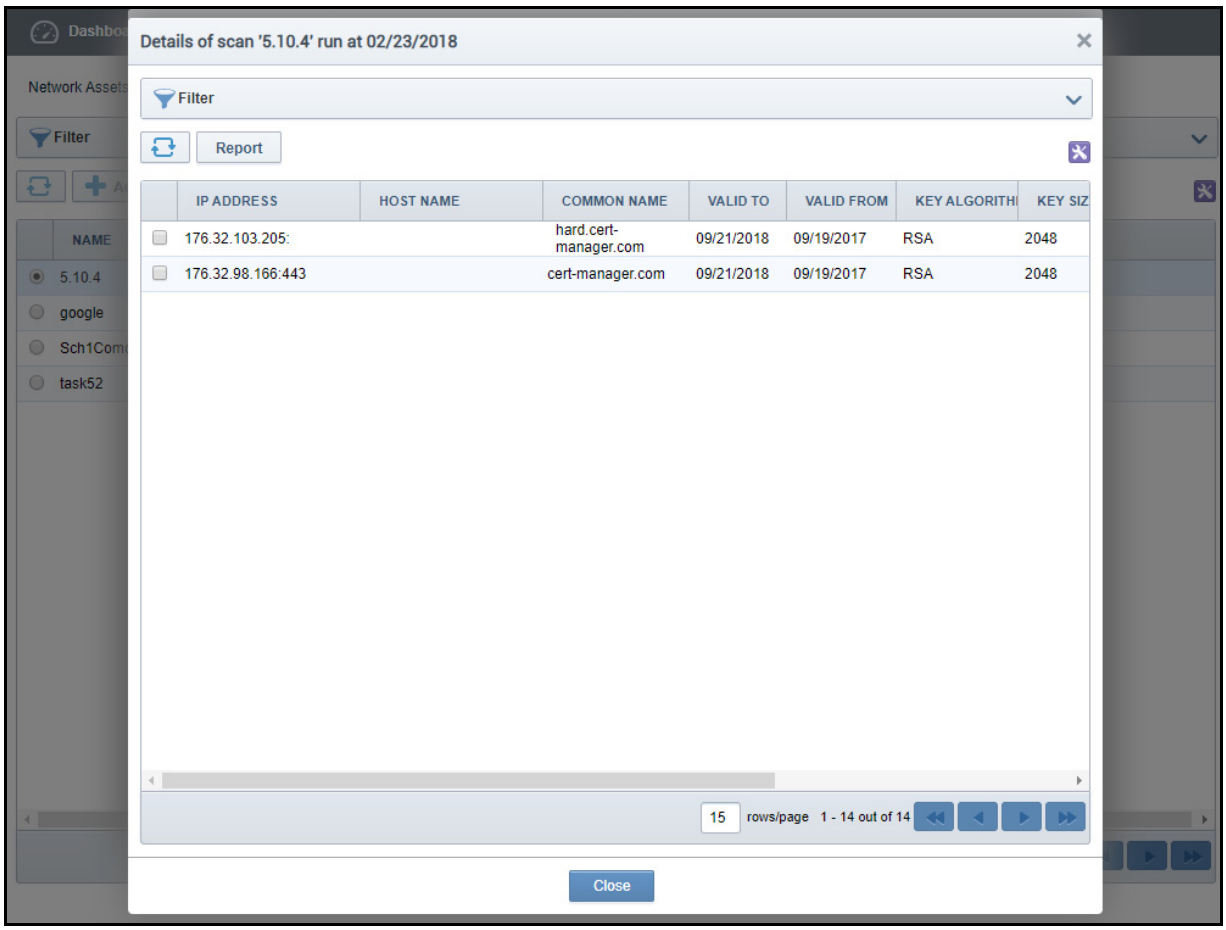


You can use the **History of scan** dialog as follows:

- Click **Report** to download all discovery scan reports in a `.csv` file format.
- To view the list of certificates discovered during a scan, select the scan and click **Details** to open the **Details of scan** dialog, as shown in the following illustration.



- The **Details of scan** dialog shown in the preceding illustration lets you view the full certificate information.
- To manually assign external certificates to an organization or department, select one or more certificates and click **Assign to**. For more information, see "Manually Assigning a Certificate to Organizations and Departments" on page 534.
- To view details of the latest certificates discovered by a discovery task, click **Last Scan Details**, as shown in the following illustration.



8.3.6 How to View Scan Results

After each discovery scan, SCM updates the lists of certificates in the **Network Assets** area and **SSL Certificates** area.

The following certificates are assigned to the **SSL Certificates** area:

- Managed certificates.
- External certificates which are assigned to an organization or department.

The following certificates are assigned to the **Network Assets** area:

- Managed certificates.
- External certificates which are assigned to an organization or department.
- External certificates which are not assigned to an organization or department.

The **Network Assets** area displays certificates discovered from all nodes of every scanned network, including web servers, domains, and certificates discovered from AD servers integrated to SCM, as follows:

- The **Network Discovery** subarea displays scanned networks as expandable nodes. Selecting a node displays all certificates identified on it, including managed certificates, external certificates that have been assigned to an organization or department by a rule, and external

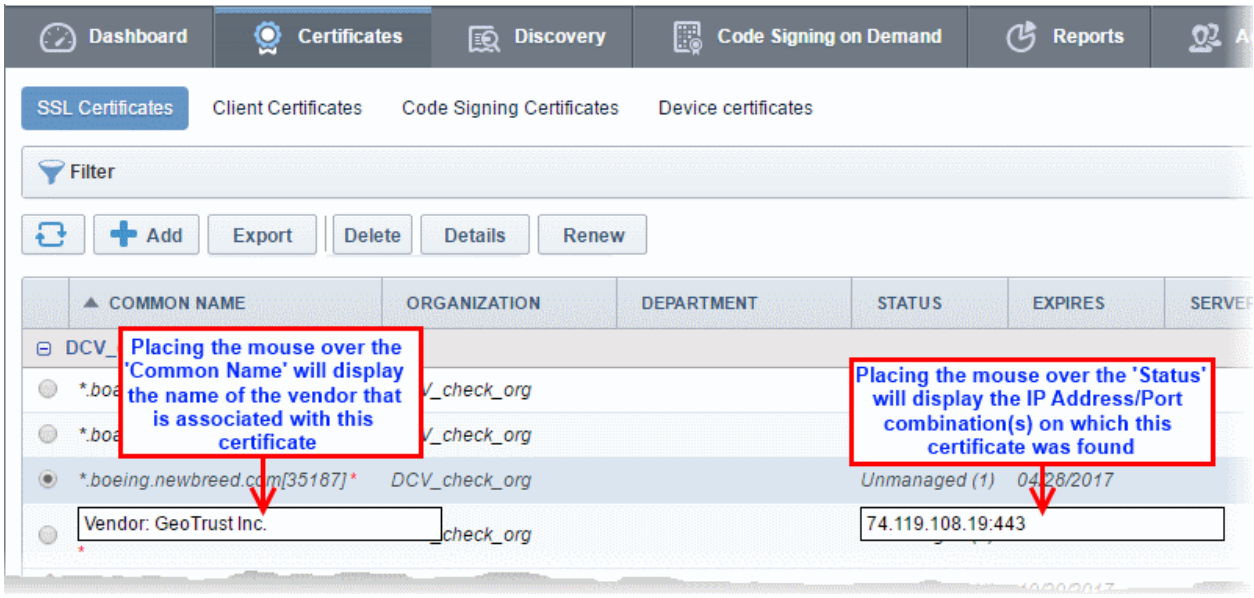
certificates that have not been assigned to an organization or department. You can view details of each certificate and manually assign external certificates to an organization or department. Doing so grants them managed status and thus makes them visible in the **SSL Certificates** area. For more information, see "How to View Certificate Information Via Network Discovery" on page 527.

- The **Web Servers** subarea displays a summary of all web servers identified from every network scanned. It also displays a list of websites or domains hosted on each identified server. For more information, see "How to View the Web Server Information" on page 536.
- The **Active Directory** subarea displays AD domains as expandable nodes. These are the domains that have been integrated to SCM by installing the MS Agent. Expanding a node and selecting an object, such as a user account, device, or computer, displays a list of all certificates associated with that object. You can view details of each certificate and manually assign external certificates to organizations or departments. Doing so makes them available in the **SSL Certificates** area. For more information, see "How to View Certificates Via Active Directory" on page 538.

After a discovery scan, SCM adds newly discovered external certificates which have been assigned to an organization or department to the **SSL Certificates** area. SCM also updates the status of any existing certificates. There are, therefore, the following two types of SSL certificates that could be discovered:

- Certificates issued by SCM (managed certificates)—SCM updates the certificate's existing entry with any status changes that may have occurred. These certificates stay assigned to the organizations to which they are currently assigned.
- Certificates that were not issued by SCM (external certificates)—If the certificate was not issued by SCM, they are assigned external status which encompasses the following:
  - Self-signed certificates.
  - Certificates issued by Sectigo but not via SCM.
  - Certificates issued by third-party vendors or other CAs.

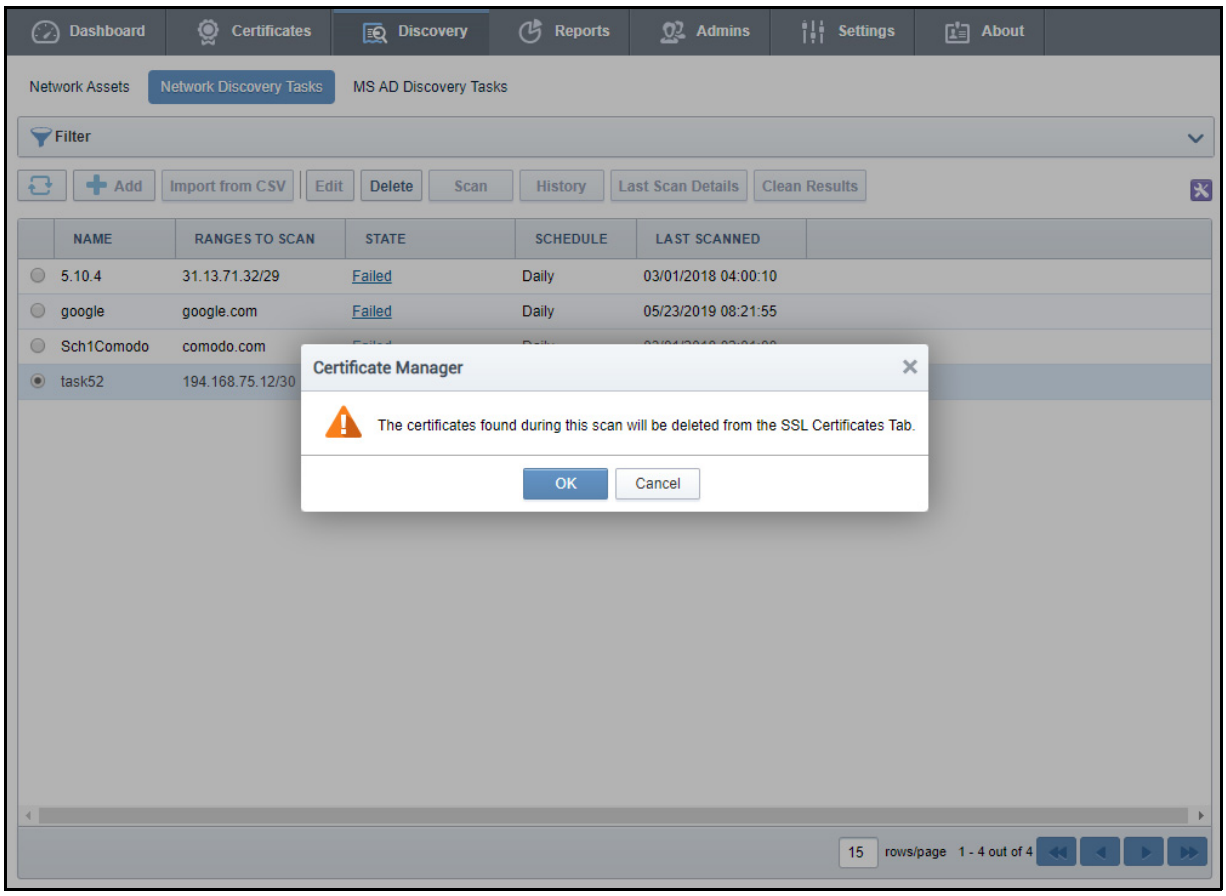
  Only those external certificates that are assigned to an organization or department (either manually or by an assignment rule) are added to the **SSL Certificates** area at the end of a discovery scan. Discovered certificates which are not assigned to any organization or department are not added to the **SSL Certificates** area. These certificates can be viewed via the **Network Assets** area.



You can bring an external certificate under the control of SCM by renewing that certificate (this means you would be effectively replacing that certificate with an equivalent Sectigo certificate). As shown in the preceding illustration, clicking **Renew** begins the ordering process for a new Sectigo SSL certificate with the same parameters.

The following table provides a summary of the certificate type, status, and viewing information.

Certificate Type		**View in the SSL Certificates Area**	
		Status	**View**
SSL certificate not issued by SCM	Self-signed certificate	External	Self-signed certificates are marked with red cross alongside their common name. Self-signed means that the certificate was not signed (issued) by a trusted CA. As such, these certificates are not recognized by the Internet browsers such as IE, Firefox, Opera, Safari, and Chrome. From the **SSL Certificates** area, you can do the following: • View details of these certificates. • Renew these certificates by replacing them with Sectigo equivalents.
	Issued by Sectigo but not via SCM	External	From the **SSL Certificates** area, you can do the following: • View details of these certificates. • Revoke these certificates. • Renew these certificates.
	Issued by a third-party vendor	External	From the **SSL Certificates** area, you can do the following: • View details of these certificates. • Renew these certificates by replacing them Sectigo equivalents.



You can download the results of a discovery scan from the **Reports** area. The discovery scan log report contains information about overall scan options and discovered SSL certificates information.

It is recommended that you perform the following on a regular basis:

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

To remove the certificates discovered from a particular discovery scan, you navigate to **Discovery > Discovery Tasks**, select the discovery task and click **Clean Results**, as shown in the following illustration.

8.4 Performing the AD Discovery Tasks

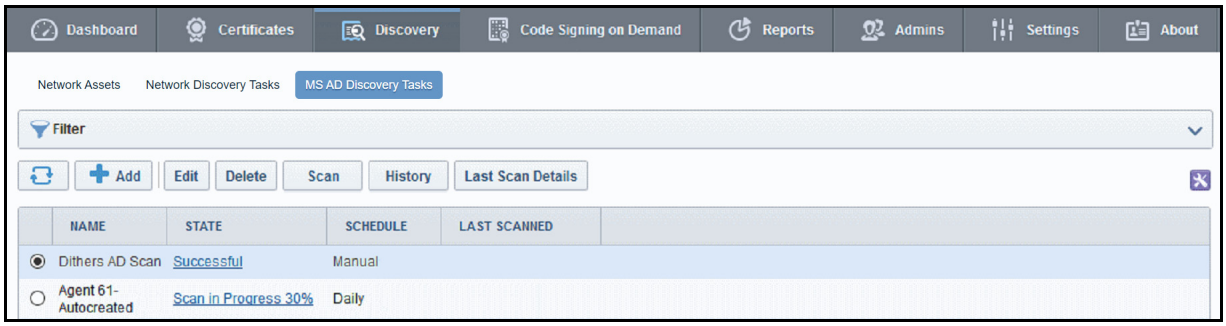
The **MS AD Discovery Tasks** area lets you configure scans on AD servers which have been integrated with SCM. Scan results can be viewed via the **Network Assets** area. AD scans locate all certificates installed on servers, devices, and endpoints on active directory domains. Each

scan identify the network or object structure and locate all types of certificates, including SSL, client certificates, code signing certificates, and device authentication certificates.

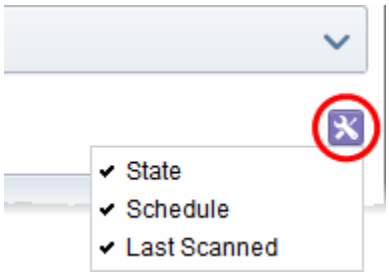
You can add auto-assignment rules to scans, therefore assigning external certificates to a specific organization or department.

You need to install the MS Agent on your active directory server and integrate it with SCM in order to run scans. For more information, see "Configuring MS Agents" on page 266.

To start the AD discovery process, use the main UI to navigate to **Discovery > MS AD Discovery Tasks**, as shown in the following illustration.



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

Column	Value	Description
Name		The name of the certificate discovery task.
State		The status of the scan. Valid values are successful, failed, in progress, canceled. Click the state to view result details. For example, clicking Successful displays the number of certificates discovered.
Schedule		Indicates whether the scan is to be run manually or as scheduled.
Last Scanned		The date and time of the last scan performed.
You can use the tool button to select columns to be displayed in the table: 		

Column	Value	Description
Controls	Add	Adds a new AD discovery task.
	Refresh	Updates the list of displayed tasks.
Discovery Task control Buttons [a]	Edit	Enables you to edit the selected discovery task, such as change the scan name, domains to be scanned, assignment rules, and schedule.
	Delete	Enables you to delete a AD discovery task from the list.
	Scan	Enables you to start a new scan for the selected discovery task.
	Cancel[b]	Enables you to stop a running discovery scan.
	History	Displays the details of past scans performed for the selected discovery task and allows you to download scan reports.
	Last Scan Details	Displays the results of the last scan for the selected discovery task.
	Clean Results	Removes all the discovered certificates from the **SSL Certificates** area.

a. Visible only on selecting a domain.
b. Appears after starting a new scan for a discovery task.

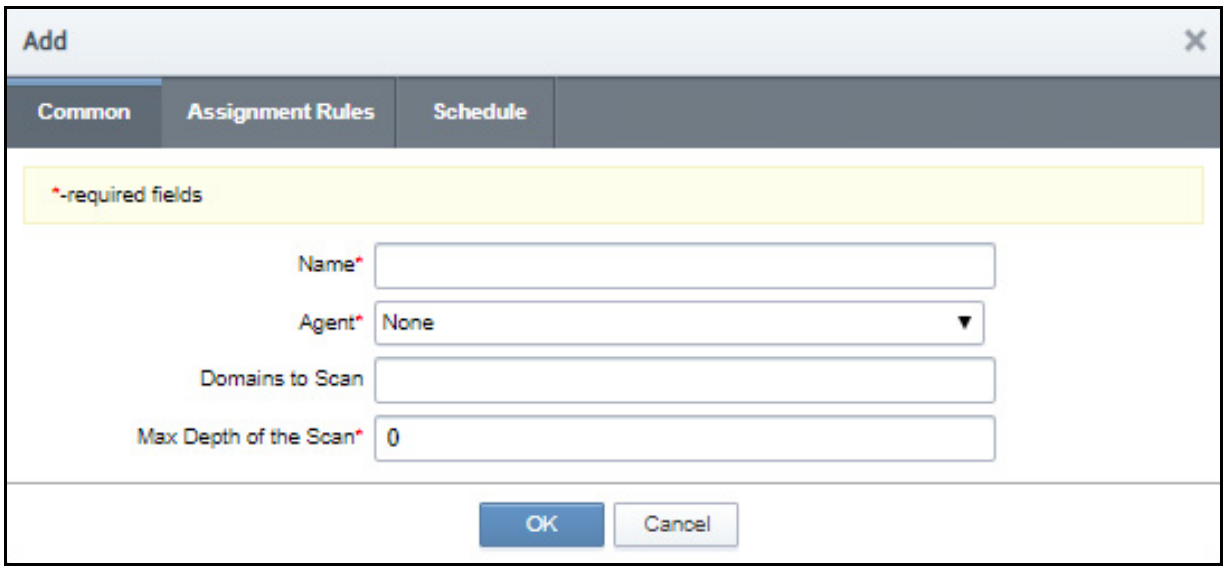
Before attempting to run a scan on an AD domain, ensure that the MS Agent has been installed on required AD server and the server has been integrated with SCM. See "Configuring MS Agents" on page 266 for more information.

Typically, the process includes the following:

- Scanning an AD domain in order to find the network object structure, endpoints, user accounts, and all deployed certificates.
- Discovered items are shown in the SCM interface as follows:
  - All discovered certificates are listed under the respective certificate types in the **Certificates** area.
  - All items discovered on the AD domain are shown in the **Network Assets** area, as described in "How to View Certificates Via Active Directory" on page 538, including certificates and artifacts such as devices, user accounts, and endpoints.
- SCM updates the status of existing certificates that were issued using SCM, if required.
- External certificates can become managed via renewal of a particular certificate.

8.4.1 How to Add Domains and Start Scans

To add a new MS AD discovery scan task, navigate to **Discovery > MS AD Discovery Tasks** and click **Add** to open the scan configuration form, as shown in the following illustration.

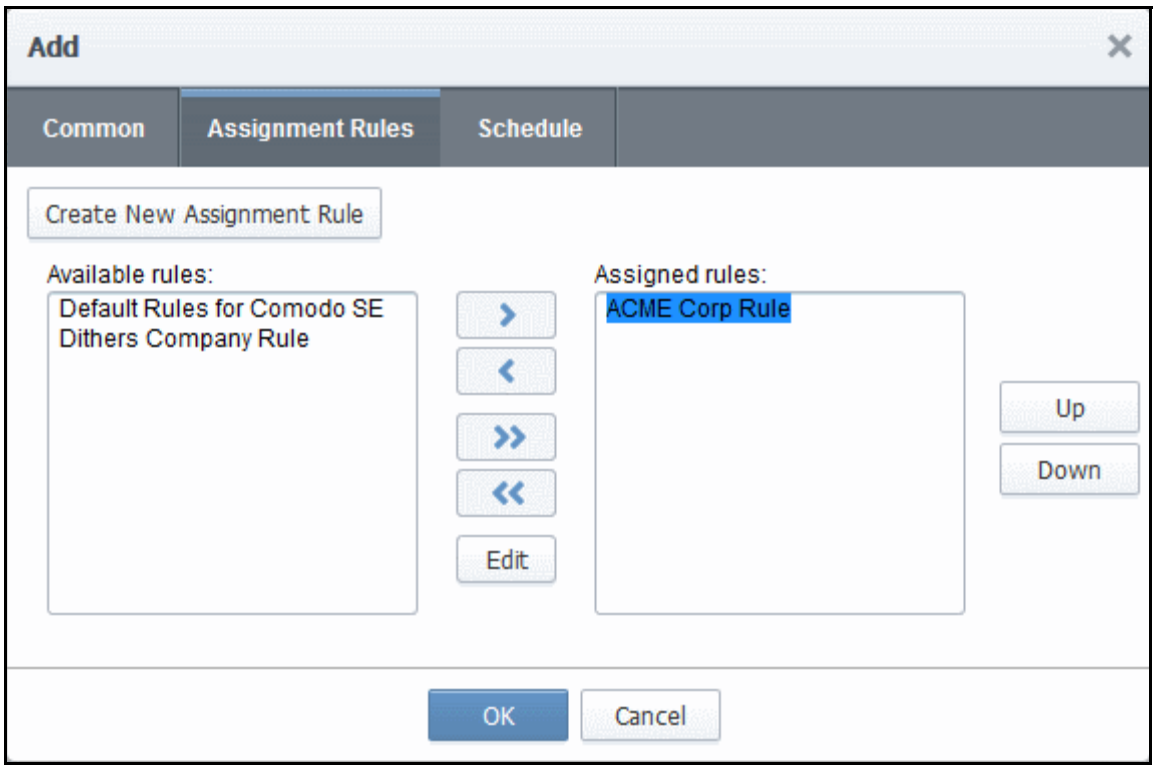


The **Add** dialog shown in the preceding illustration allows you to configure scan settings, apply auto-assignment rules, and schedule scans.

The following table lists settings available in the **Add** dialog.

Field	Description
Name	The name to describe the AD discovery task.
Agent	The MS Agent or AD agent cluster to be used for scanning.
Domains to Scan	The AD domains to scan.
Max Depth of the Scan	The number of network hierarchy levels to be scanned. The depth of the scan should cover all required endpoints, users, and other AD objects in the network. 0 = Unlimited

To add rules which assign external certificates identified by the scan to an organization or department, you select **Assignment Rules**, as shown in the following illustration.

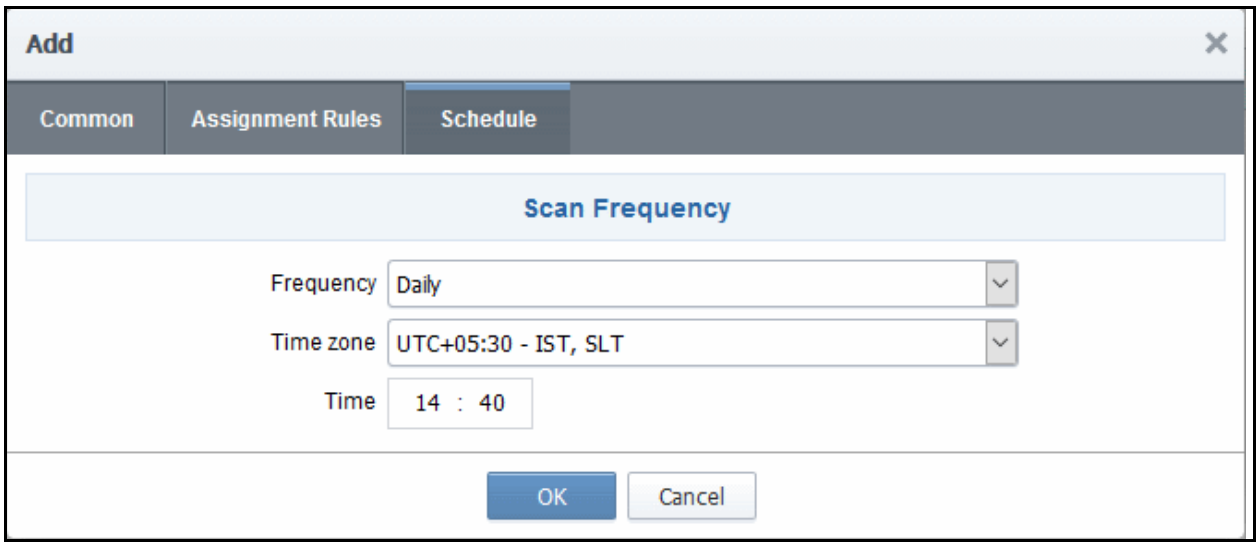


Use the arrows to add rules to the discovery task. Rules can be configured in the **Assignment Rules** area, as described in "Managing SCM Agents" on page 509.

To create a new rule, click **Create New Assignment Rule**. When the rule is added to the **Available Rules** list, select it and move to the **Assigned Rules** list.

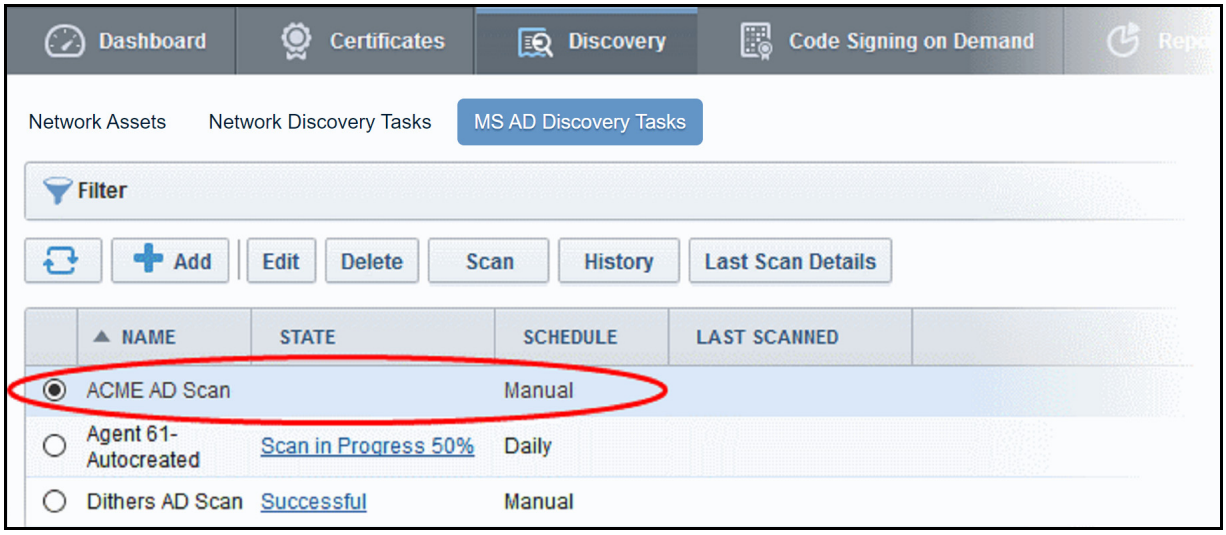
To modify a rule, select it and click **Edit**.

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

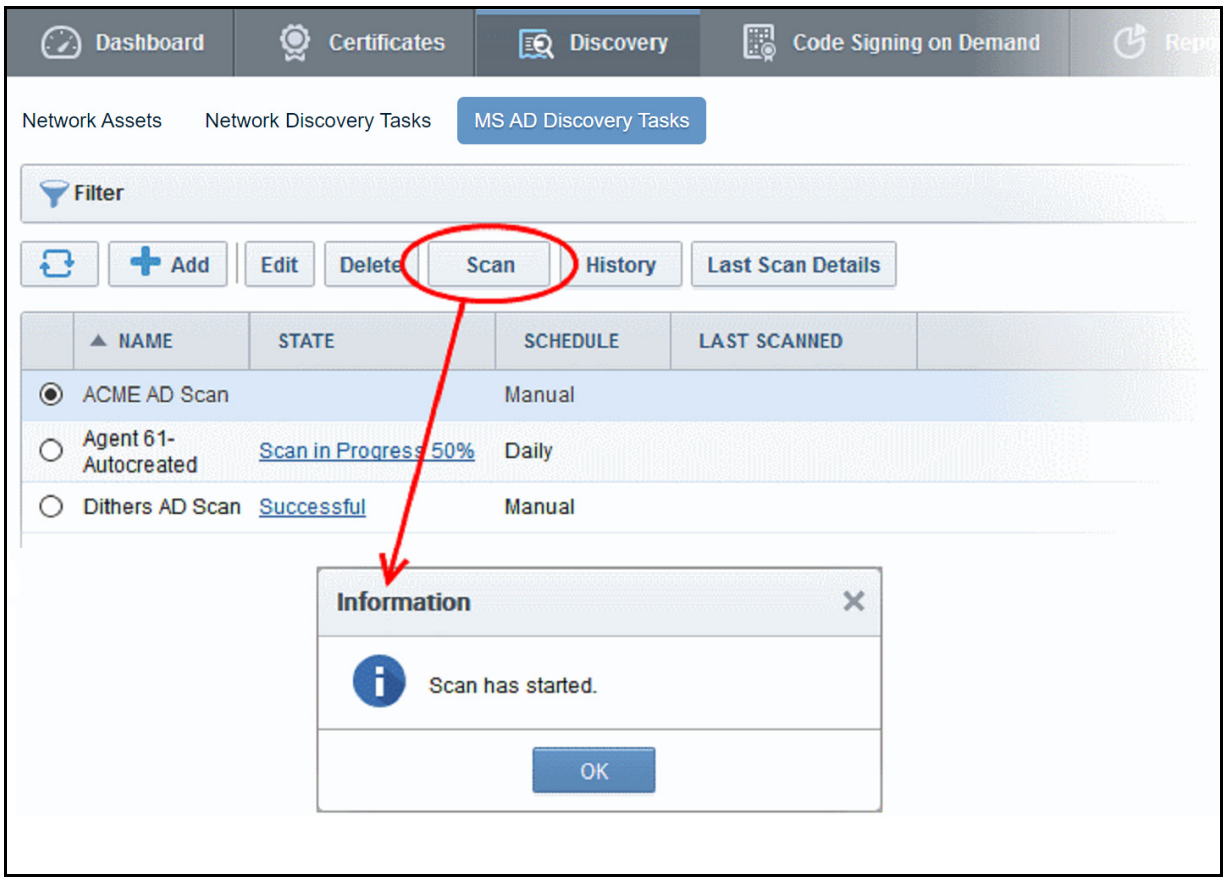


Available scan frequencies are Manual (on demand), Daily, Weekly, Monthly, Quarterly, Semi-Annually and Annually.

The newly created discovery task is displayed in the list, as shown in the following illustration.



You may repeat the process to add more network discovery tasks. To run a scan, select the respective discovery task from the list and click the **Scan** to commence the discovery scan for the selected task, as shown in the following illustration.

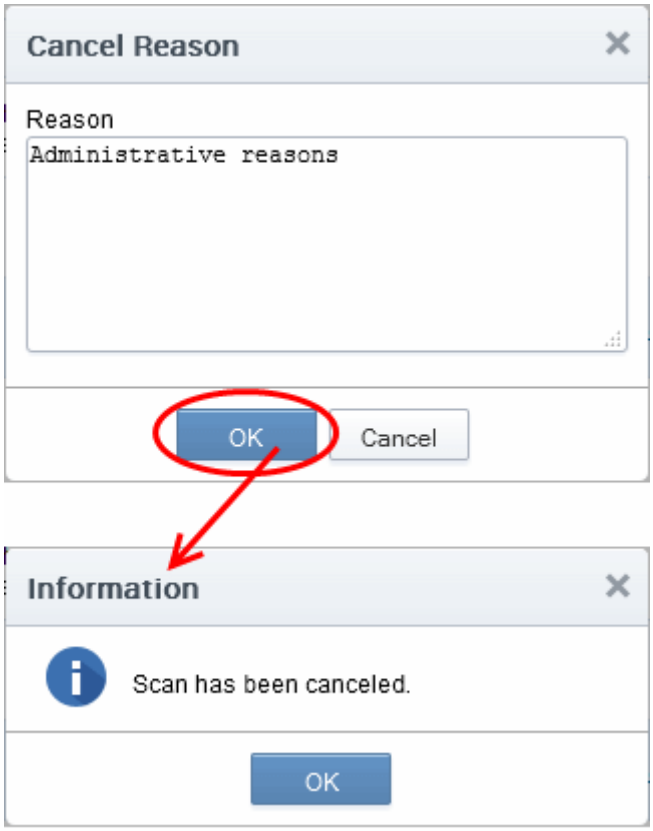


You can manually start a scan only for discovery tasks scheduled to be run manually. Other scan runs as per the schedule set for the task.

SCM allows you to run multiple discovery tasks at the same time: after a scan has started, select another task and click **Scan**.

To cancel the scanning process, click **Cancel**, and the entire system reverts to the state that existed before the scan started (for example, any data collected during scanning cannot be applied until the scanning process is completed).

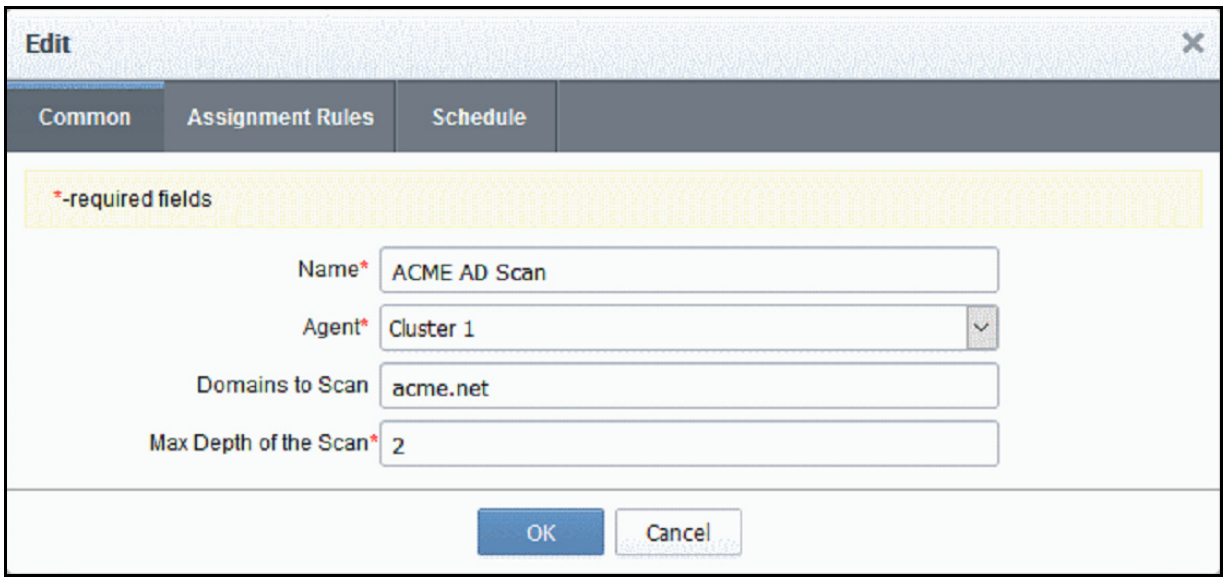
If you cancel the scan, you should specify the reason for it in the **Cancel Reason** dialog shown in the following illustration.



Upon completion, the results can be viewed by navigating to **Discovery > Network Assets > Active Directory** (see "How to View Certificates Via Active Directory" on page 538) or by navigating to **Certificates > Reports** from the main UI.

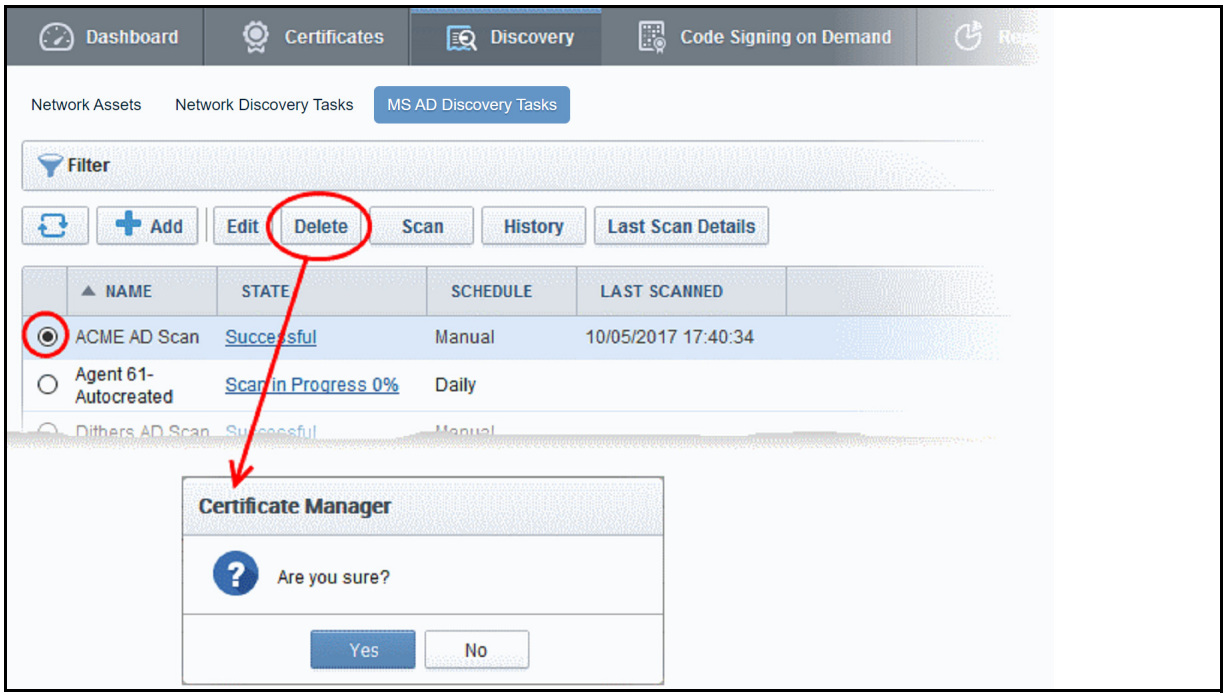
8.4.2 How to Modify AD Discovery Tasks

You can modify an existing AD discovery task by selecting it in the list and clicking **Edit**, as shown in the following illustration. The **Edit** dialog is similar to the **Add** dialog and allows you to change the task name, select another agent, select a different domain, add or remove assignment rules, change the schedule, and so on. See "How to Add Domains and Start Scans" on page 562 for more information.



8.4.3 How to Delete AD Discovery Tasks

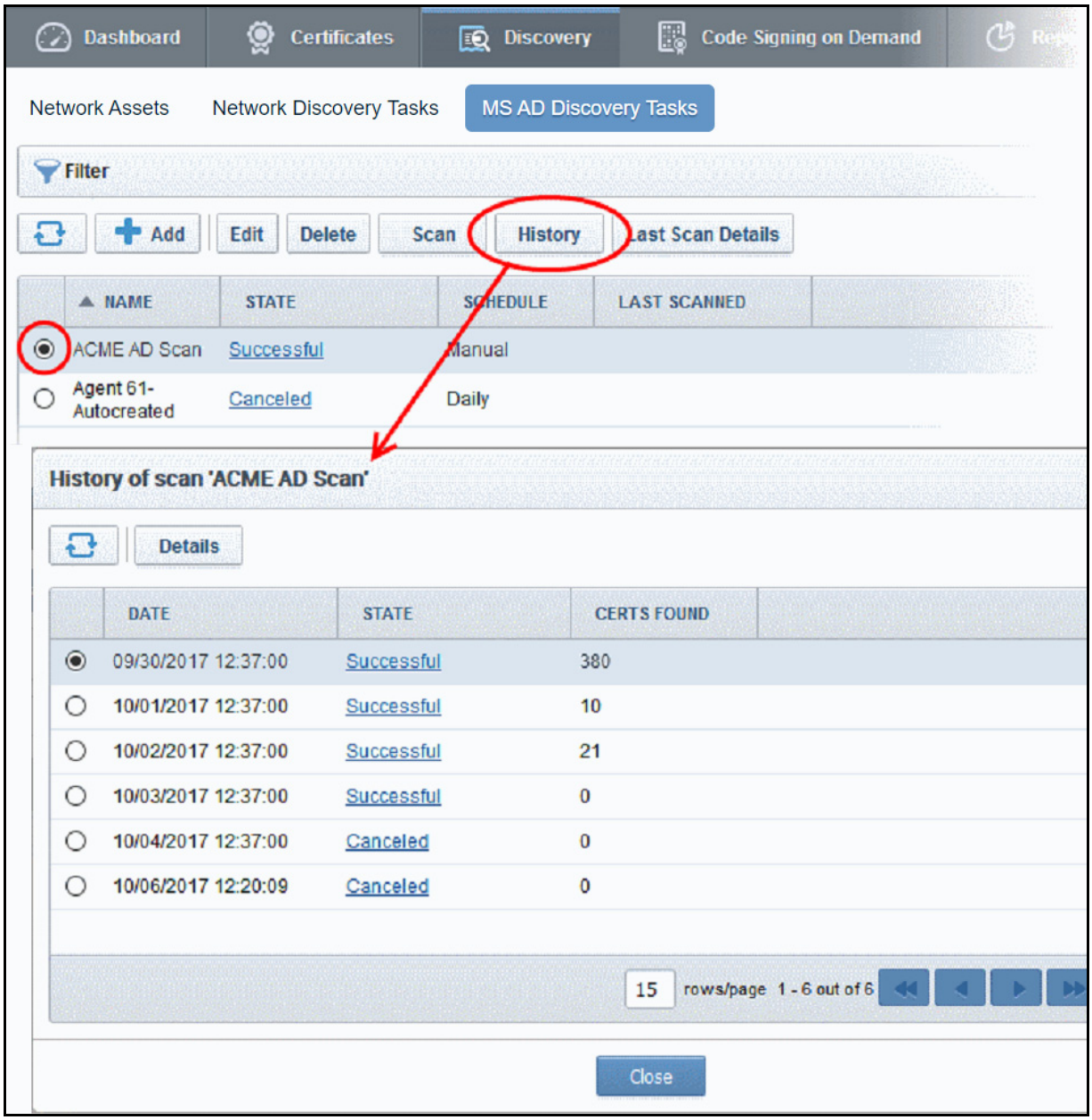
To delete an AD discovery task from the list, select it and click **Delete**, as shown in the following illustration.



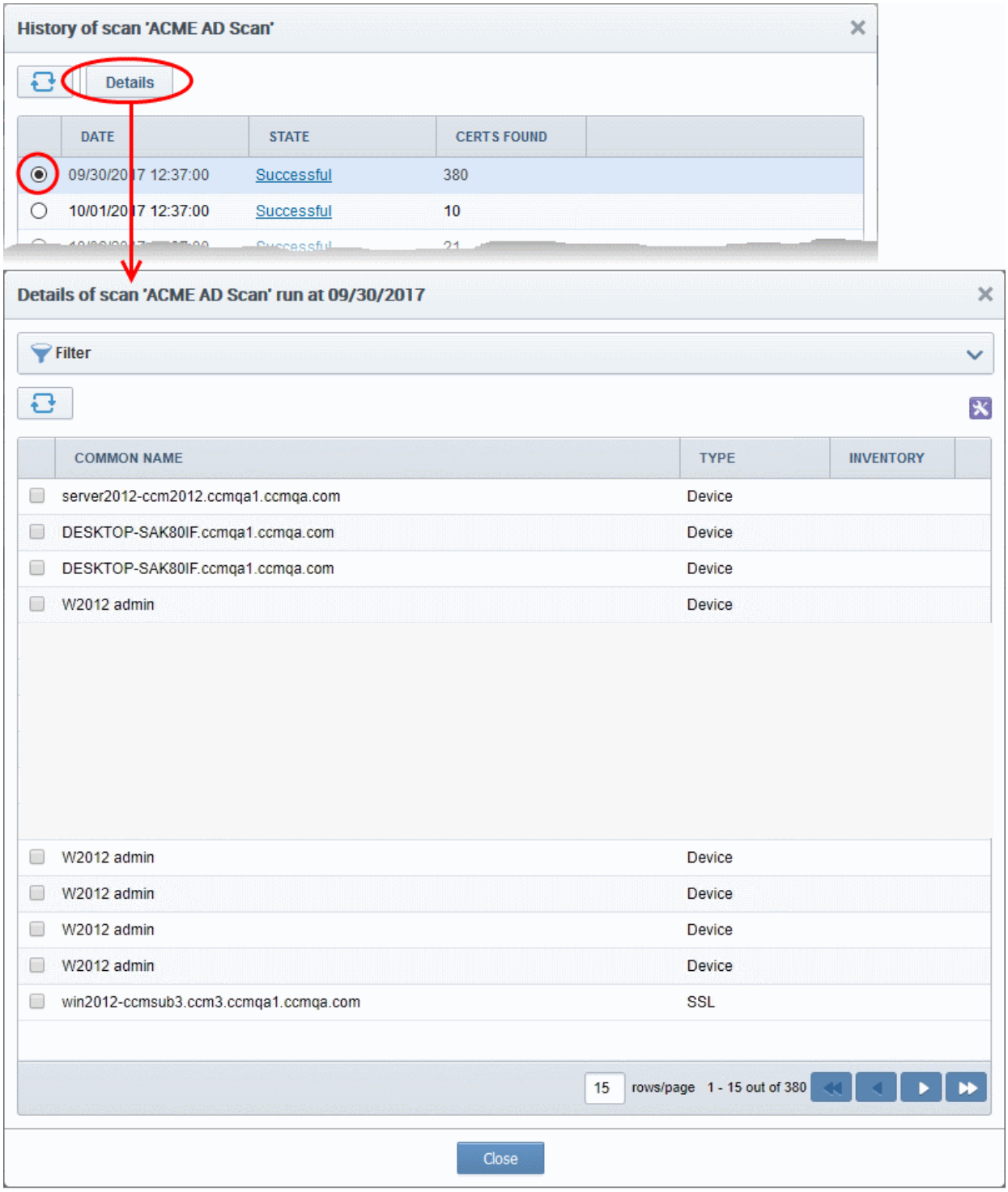
8.4.4 How to View History of AD Discovery Tasks

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

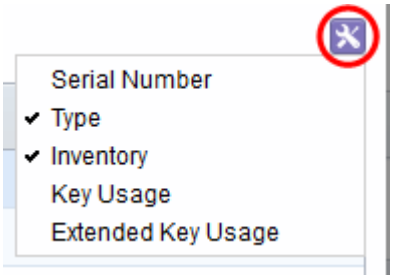
To view the task history of a discovery task, navigate to **Discovery > MS AD Discovery Tasks** from the main UI, select the task and click **History** to open the **History of scan** dialog that displays a list of previous scans run for the task, as shown in the following illustration.



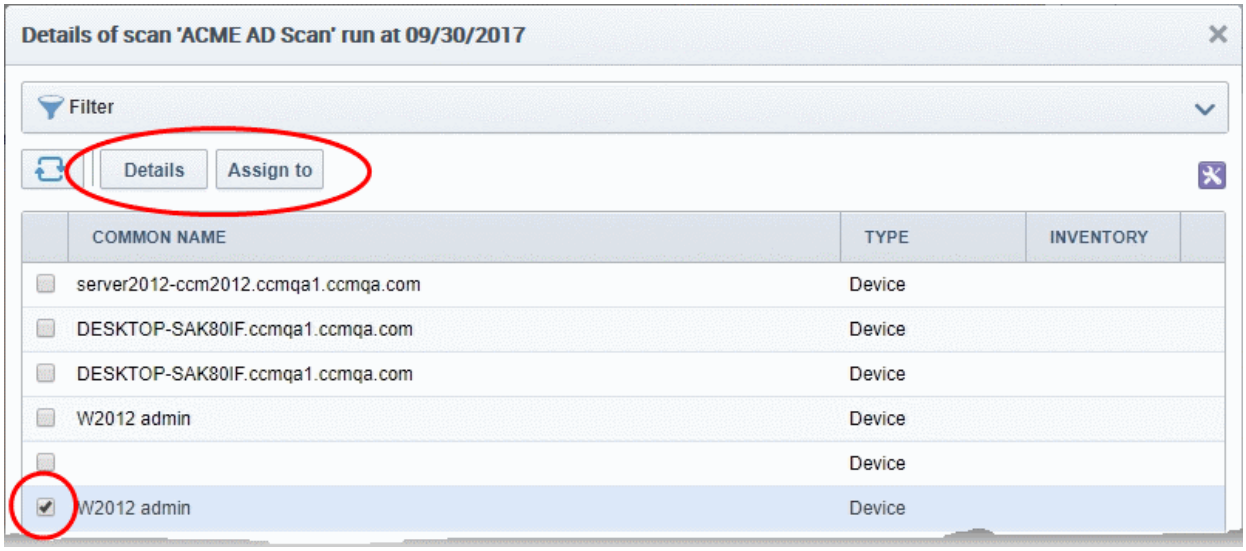
- To view all certificates discovered during the scan, click **Details** to open the **Details of scan** dialog, as shown in the following illustration.


History of scan 'ACME AD Scan'
Details
DATE
STATE
CERTS FOUND
09/30/2017 12:37:00
Successful
380
10/01/2017 12:37:00
Successful
10
Details of scan 'ACME AD Scan' run at 09/30/2017
Filter
COMMON NAME
TYPE
INVENTORY
server2012-ccm2012.ccmqa1.ccmqa.com
Device
DESKTOP-SAK80IF.ccmqa1.ccmqa.com
Device
DESKTOP-SAK80IF.ccmqa1.ccmqa.com
Device
W2012 admin
Device
W2012 admin
Device
W2012 admin
Device
W2012 admin
Device
W2012 admin
Device
win2012-ccmsub3.ccm3.ccmqa1.ccmqa.com
SSL
15
rows/page
1 - 15 out of 380
Close

The following table lists settings available in the **Details of scan** dialog.

Column	Description
Common Name	The value in the Common Name field of the certificate. This varies according to the certificate type. SSL certificates usually display a domain name. Client certificates may display an email address or host name, and device certificates usually display the host name of the device.
Type	The certificate type, as in SSL (for web server), client (for email certificates, client certificates), code signing, or device certificate.
Inventory	Indicates whether the certificate is managed or external. Clicking **Managed** opens the **Certificate Details** area of the certificate. Selecting **External** displays the option for assigning it to the required organization or department. SCM also allows you to configure automatic assignment of external certificates identified by a discovery scan to respective organizations and departments.
You can use the tool button to select columns to be displayed in the table: 	
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	Higher level capabilities of the certificate. For example, web server authentication and client authentication.

To manually assign external certificates to an organization or department, select one or more certificates and click **Assign to**, as shown in the following illustration. For more information, see "Manually Assigning a Certificate to Organizations and Departments" on page 534.



To view details of the latest certificates discovered by an AD discovery task, click **Last Scan Details**.

8.4.5 How to View Results of AD Discovery Scan Tasks

After each discovery scan, SCM updates the lists of certificates in the **Active Directory** area, as well as the **Certificates** area for each certificate type.

The following certificates are assigned to the **Active Directory** area:

- Managed certificates.
- External certificates which are assigned to an organization or department.
- External certificates which are not assigned to an organization or department.
- Network objects including domains, users, and devices enrolled to the AD domain, based on the following:
  - AD domains that have been integrated with SCM by installing the MS Agent.
  - Each AD tree shows objects found on the domain, including user accounts, devices, and endpoints, as well as all certificates associated with that object.
  - You can view details of each certificate and manually assign external certificates to organizations or departments, which makes them visible in the **SSL Certificates** area.

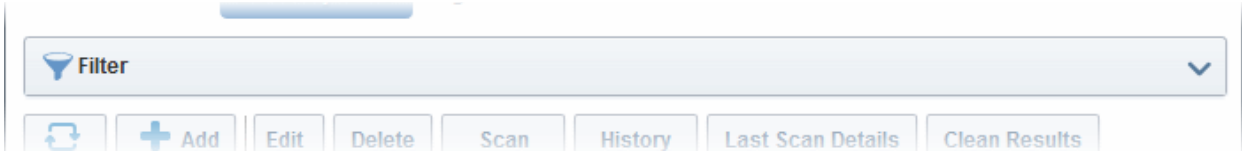
It is recommended that you perform the following on a regular basis:

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

8.4.6 How to Sort and Filter MS AD Discovery Tasks

You can sort items in the alphabetical order by clicking a column header, and you can use filters to search for particular department.

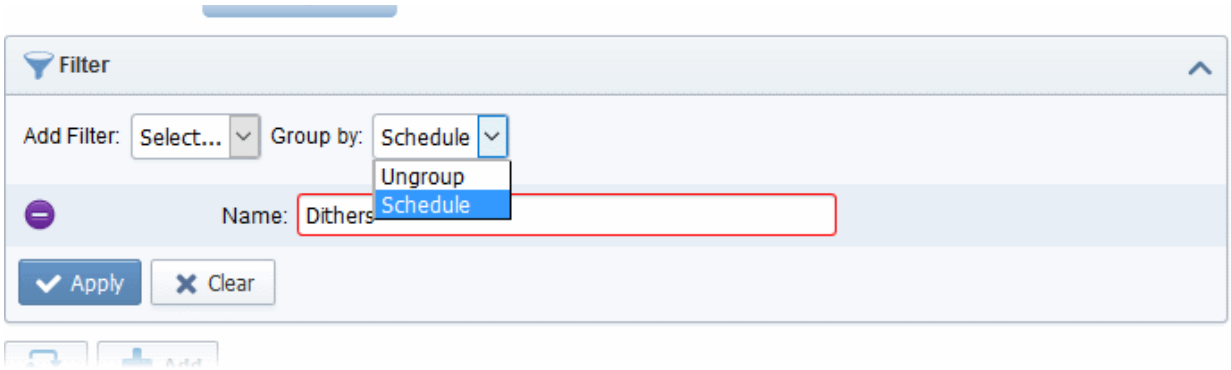
You apply filters by clicking on the down arrow at the right end of the **Filter** stripe, as the following illustration shows.



To add filters, you make a selection in the **Add Filter** list shown in the following illustration, and then group the results with other options that appears depending on the selection from the **Add Filter** list.

Filter Criteria	Filter Parameter
Name	Enter the name of the discovery task fully or in part

Then you enter or select the filter parameter as per the selected criteria.



After you click **Apply**, filtered items based on the entered parameters are displayed:

You can remove the filter options by clicking **Clear**.

Note that the search filters, once configured for the interface, are saved automatically. When you reopen the area, the configured filters will be active and only the search results will be displayed. Click **Clear** to remove filters.

9

Generating Reports

This chapter describes how to generate and view various reports available in SCM.

This chapter describes the following topics:

- SCM Reports Overview
- Generating Activity Log Reports
- Generating Client Certificates Reports
- Generating Discovery Scan Log Reports
- Generating SSL Certificates Reports
- Generating Code Signing Certificates Reports
- Generating Code Signing Certificates Reports
- Generating Code Signing Requests Reports
- Generating Administrators Reports
- Generating XML Data Reports
- Generating DCV Reports
- Generating Agent Log Events Reports
- Generating Notification Log Statistics Reports
- Generating Private Key Agent Activity Log Reports
- Generating Network Discovery Tasks Reports
- Generating Device Certificate Reports

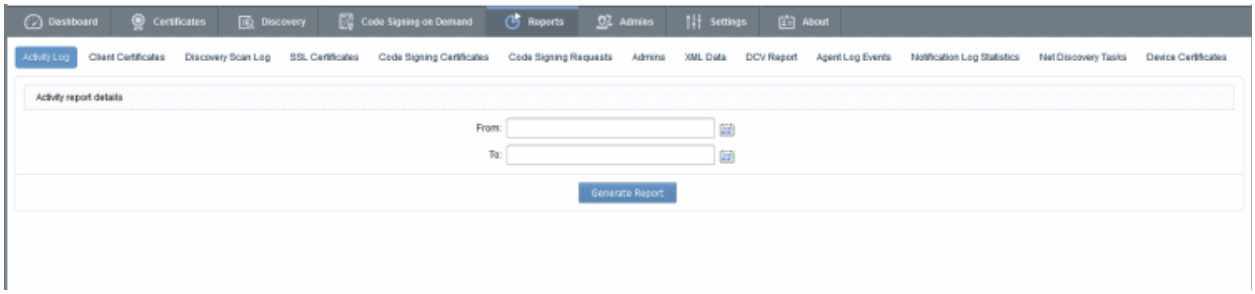
9.1 SCM Reports Overview

The **Reports** tab shown in the following illustration lets you generate and view reports that summarize the usage, provisioning, and monitoring of all types of certificates. The following reports are available:

- The **Activity Log** report allows you to view history of all events concerning all types of certificates.
- The **Client Certificates** report allows you to view history of all events related to client certificates.
- The **Discovery Scan Log** report allows you to view information about scan options and discovered SSL certificates.
- The **SSL Certificates** report allows you to view history of all events related to SSL certificates.
- The **Code Signing Certificates** report allows you to view history of all events related to code signing certificates.

- The **Code Signing Requests** report allows you to view CSoD requests and related activities.
- The **Admins** report allows MRAOs to view a list of all administrators and their privilege levels.
- The **XML Data** report allows MRAOs to download a comprehensive XML report on organizations, departments, administrators, and certificates.
- The **DCV** report allows MRAO, RAO SSL, and DRAO SSL administrators to download a report on registered domains and their DCV status.
- The **Agent Log Events** is a report available to MRAOs on the discovery scan and certificate installation activities of SCM agents.
- The **Notification Log Statistics** report allows MRAOs to download reports with details about notification emails.
- The **Private Key Agent Activity** report allows 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.
- The **Network Discovery Tasks** report allows MRAO, RAO SSL, and DRAO SSL administrators to view details of configured network discovery tasks.
- The **Device Certificates** report presents history of all events related to device certificates.

The reports are especially useful when troubleshooting any issues related to the provisioning, installation, and management of certificates.



The **Reports** area contains fourteen subareas, depending on the features enabled for your account.

The following table contains details on all available report types.

Report	Description
Activity log	Enables MRAOs to generate and view reports providing a highly detailed log of all actions recorded by SCM for the selected period of time. For example, administrator login times, modifications to users, certificate requests, changes in certificate statuses, and so on.

Report	Description
Client Certificates	Enables you to generate and view reports on client certificate activities. Reports are delivered in a .csv format and can be filtered to show only certificates with a specific current status, such as the following: • Any • Enrolled—Downloaded • Enrolled—Pending Download • Revoked • Expired • Not Enrolled The reports can be further sorted by organization or department, status, specific date and time interval.
Discovery Scan Log	Enables you to generate and view log reports from the scanning processes. Reports are delivered in a .csv format. The reports can be further sorted by organizations and departments.
SSL Certificates	Enables you to generate and view reports regarding SSL certificate activity. Reports are delivered in a .csv format and can be filtered to show only certificates with a specific current status, such as the following: • Any • Enrolled—Downloaded • Enrolled—Pending Download • Revoked • Expired The reports can be further sorted by organization or department, status, specific date and time interval.
Code Signing Certificates	Enables you to generate and view reports regarding code signing certificate activity. Reports are delivered in a .csv format and can be filtered to show only certificates with a specific current status, such as the following: • Any • Enrolled—Downloaded • Enrolled—Pending Download • Revoked • Expired The reports can be further sorted by organization or department, status specific date and time interval.
Code Signing Requests	Enables MRAO, RAO Code Signing, DRAO Code Signing administrators to view reports containing the details of CSoD requests and their activities. Reports are delivered in a .csv format and can be filtered to show only certificates with a specific current status, such as the following: • Any • Created • In Progress • Declined • Signed • Expired • Failed The reports can be further sorted by organization or department, status, specific date and time interval.

Report	Description
Admins	Enables MRAOs to generate and view reports providing the details of the enrolled administrators of all privilege levels.
XML Data	Enables MRAOs to generate a report containing complete details of all the organizations, departments, their administrators, and all the certificates in an XML format.
DCV Report	Enables MRAO, RAO SSL, and DRAO SSL administrators to generate and view a report on registered domains with their DCV status. Reports are delivered in a .csv format and can be filtered to show only certificates with a specific current status, such as the following: • Any • Not Started • Awaiting Submittal • Submitted • Validated • Validated Renewing • Expired The reports can be further sorted by organization or department, status specific date and time interval. DCV reports are available only if the DCV feature has been enabled for your account.
Agent Log Events	Enables MRAOs to generate reports on certificate discovery and remote installation activity logs of Network Agents.
Notification Log Statistics Report	Enables MRAOs to generate reports containing complete details of all notification emails sent to other administrators. Reports are delivered in a .csv format.
Private Key Agent Activity Log	Enables MRAOs to generate the report containing actions executed by the Private Key Agent, such as generation of CSR and storage of a PK for certificates applied using the auto-CSR generation and PK management feature, storage of PK manually uploaded by the administrators, and so on. Reports are delivered in a .csv format.
Network Discovery Tasks	Enables MRAO, RAO SSL, and DRAO SSL administrators to generate reports on configured network discovery tasks. Reports are delivered in a .csv format.
Device Certificates	Enables you to generate and view reports regarding device certificates. Reports are delivered in a .csv format and can be filtered to show only certificates with a specific current status, such as the following: • Any • Requested • Enrolled—Pending Download • Issued • Revoked • Expired The reports can be further sorted by organization or department, status specific date and time interval.

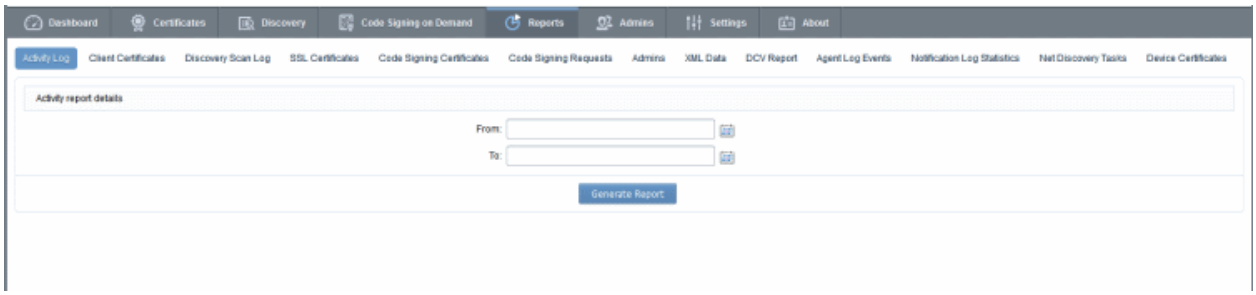
The following table provides a summary of administrators and reports types that these administrators can generate.

Report / Organization	MRAO	RAO				DRAO			
		SSL	Client	Code Signing	Device Certificate	SSL	Client	Code Signing	Device Certificate
Activity Log	Yes	No				No			
Client Certificates	Yes	No	Yes	No	No	No	Yes	No	No
Discovery Scan Log	Yes	Yes	No	No	No	Yes	No	No	No
SSL Certificates	Yes	Yes	No	No	No	Yes	No	No	No
Code Signing Certificates	Yes	No	No	Yes	No	No	No	Yes	No
Code Signing requests	Yes	No	No	Yes	No	No	No	Yes	No
Admins	Yes	No				No			
XML Data	Yes	No				No			
DCV Report	Yes	Yes	No	No	No	Yes	No	No	No
Agent Log Events	Yes	No				No			
Private Key Agent Activity Log	Yes	No				No			
Notification Log Statistics Report	Yes	No				No			
Network Discovery Tasks	Yes	Yes	No	No	No	Yes	No	No	No
Device Certificates	Yes	No	No	No	Yes	No	No	No	Yes

Organization / Department	MRAO	RAO SSL, RAO Client Certificate, RAO Code Signing, RAO Device Certificate	RAO SSL, RAO Client Certificate, RAO Code Signing, RAO Device Certificate
	All organizations are available for selection.	Only the organizations and their sub-ordinate departments that have been delegated to them are available for selection.	Only the departments that have been delegated to them are available for selection.

9.2 Generating Activity Log Reports

The **Activity Log** area shown in the following illustration enables MRAOs to generate and view reports that reflect all activities (for example, administrator login times, modifications to users, certificate requests, changes in certificate statuses, and so on) recorded by the SCM for a selected period of time.



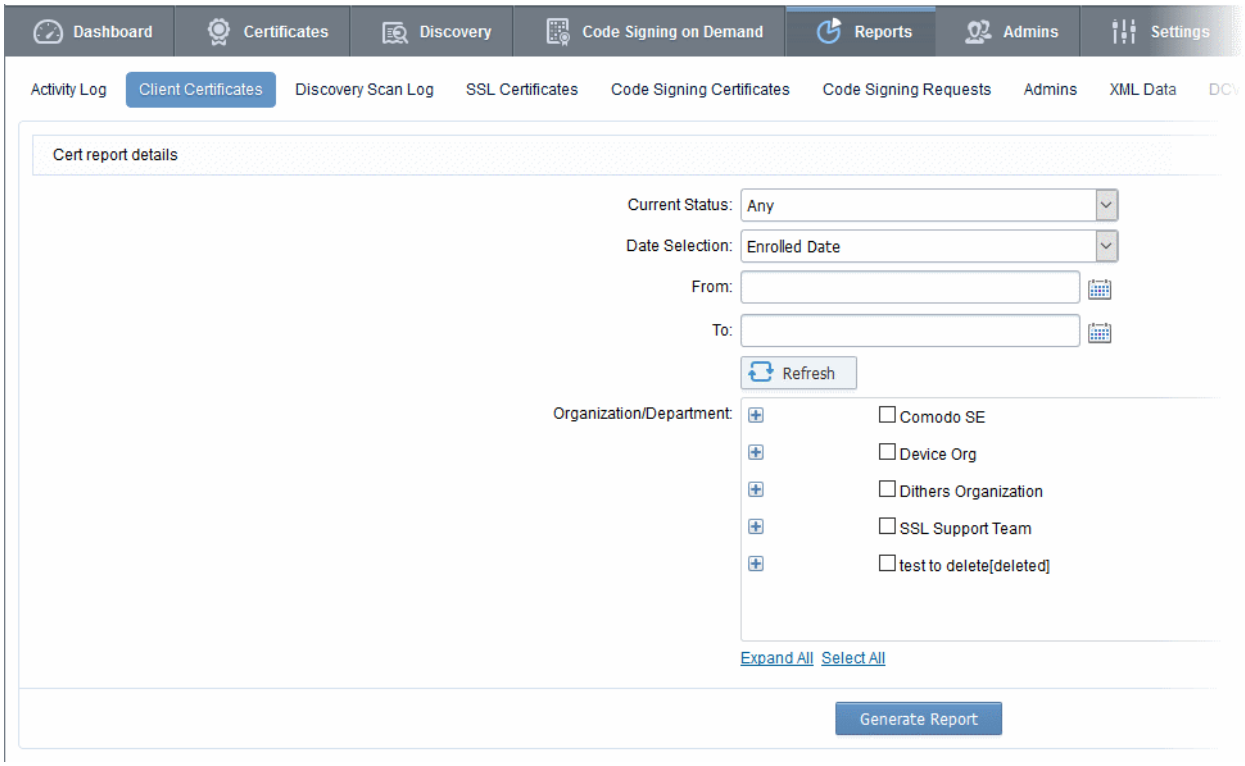
The following table lists settings available in the **Activity Log** report area.

Setting / Element	Description
From and To	Enables you to generate a report in a .csv format for activity log for a specified period of time. If no dates are specified, the report is generated for all log entries, regardless of the entry date.
Generate Report	Starts the report generation.

9.3 Generating Client Certificates Reports

The **Client Certificates** area shown in the following illustration enables MRAO, RAO Client Certificate, and DRAO Client Certificate administrators to generate and view reports that reflect an activity and other statistics related to usage, provisioning, and monitoring of client certificates. You can filter the reports by certificate status. The certificate statuses can be Any,

Enrolled—Downloaded, Enrolled—Pending Download, Revoked, Expired, and Not Enrolled. Reports can also be filtered by organization, status specific dates and time interval.



The following table lists settings available in the **Client Certificates** report area.

Setting / Element	Description
Current Status	Current status of the client certificates. Valid values are: • Any—Generates a report for all client certificates regardless of their current status. • Enrolled—Downloaded—Generates a report of only those client certificates that have been successfully enrolled by the end-user and subsequently downloaded. • Enrolled—Pending Download—Generates a report of only those client certificates that have been successfully enrolled by the end-user but have not yet been downloaded. • Revoked—Generates a report for client certificates that have been revoked. • Expired—Generates a report only for client certificates that have expired and are due for renewal. • Not Enrolled—Generates a report containing only those end-users that belong to an organization and are listed in the **Client Certificates** area as a client certificate user but haven't enrolled for their client certificate.
Date Selection	Specific date for collecting a report. It can be date of certificate enrollment, date of certificate download, date of certificate revocation or expiration. The choices dependent on the status selected in the **Current Status** field. If no dates are specified, the report is generated for all the scans, regardless of the dates.

Setting / Element	Description
Organization / Department	Specific organizations or departments for which the report is to be generated. If multiple organizations or departments are selected, then you receive a single report that covers those selected organizations or departments. Each organization is displayed on a separate row in the Organizations column and each department is displayed in a separate row in the Departments column. If no organization or department is selected, the report is generated for all the organizations and departments delegated to you.
Refresh	Update the information on the form.
Generate Report	Starts the report generation.

9.4 Generating Discovery Scan Log Reports

The **Discovery Scan Log** area enables MRAO, RAO SSL, and DRAO SSL administrators to generate and view log reports from the scanning processes. You can choose to generate either a summary or detailed report.

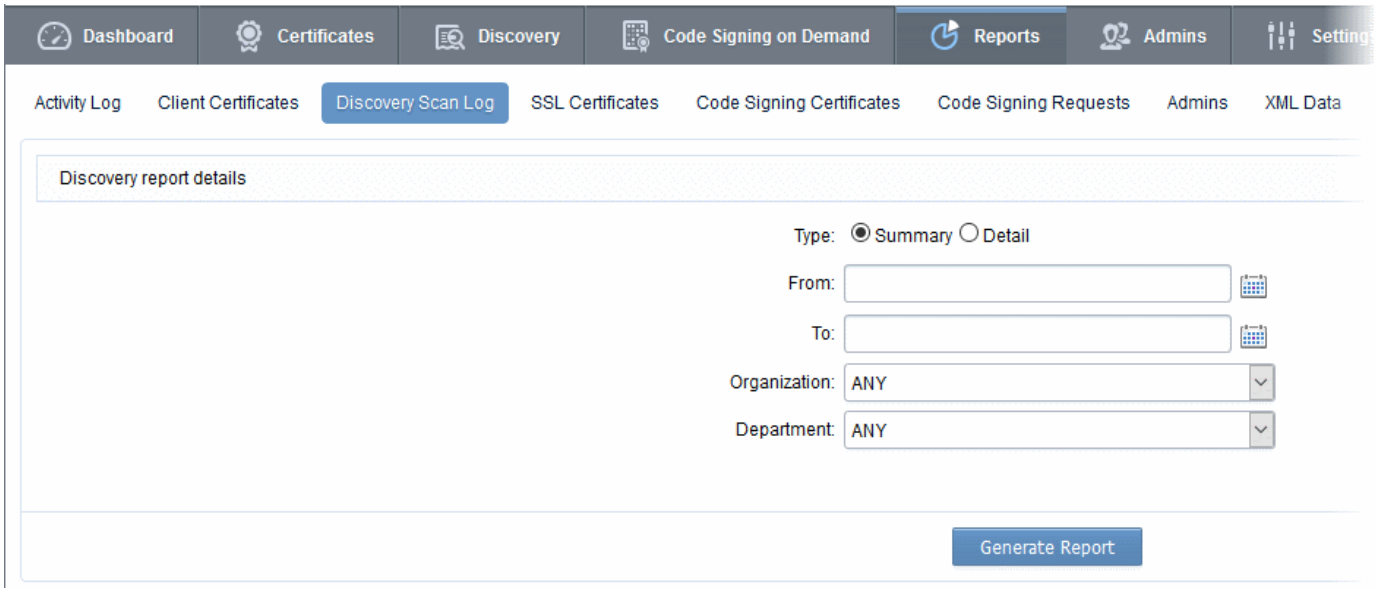
9.4.1 How to Generate a Summary Report

The summary type discovery scan log report is generated for a specified time period in the `.csv` format. This report provides the following information corresponding to each scan run in the specified period:

- Certificate ID
- Start date
- End date
- IP ranges scanned
- IP addresses scanned
- SSL certificates found
- New SSL certificates found
- Sectigo certificates found
- New Sectigo SSL certificates found
- Other SSL certificates found
- New other SSL certificates found
- Self-signed certificates found
- New self-signed certificates found
- Scan type (manual or scheduled)
- Completion status: Scan Completed, Scan Failed (with the fail reason), Scan Canceled by User.
- Reason for failure (for failed scan)
- The person who requested the scan (for manual scans)
- The person who canceled the scan (for manual and scheduled scans)

- Reason for canceling the scan (in case of canceled scan)
- Settings (CIDR range, port settings, and so on)

When you select the **Summary** type, the area shown in the following illustration appears.



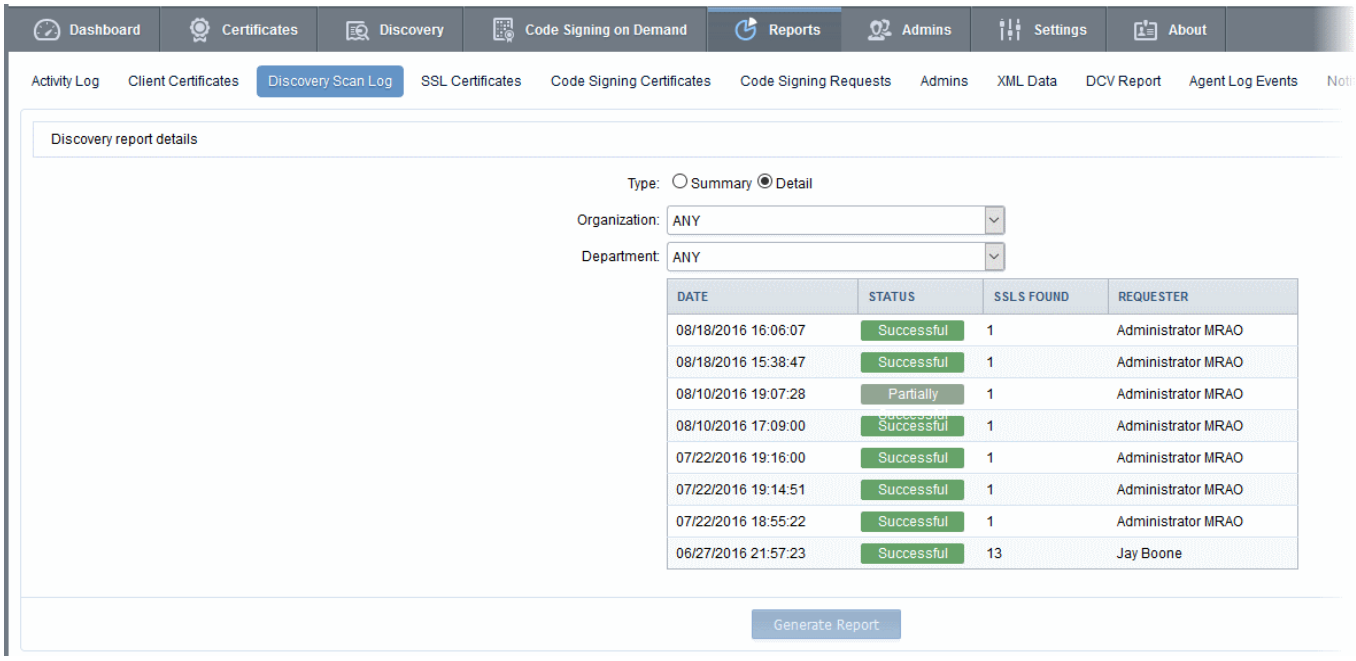
The following table lists settings available in the summary report area.

Setting / Element	Description
Type	Either a detailed report or a summary report.
Scan Date	The report time period. If no dates are specified, the report is generated for all the scans, regardless of the dates.
Organization	The organization for which the discovery scan log is to be generated. Selecting Any generates a report for the organizations that have been delegated to the specific administrator. This option is not visible to DRAO administrators.
Department	The department belonging to the selected organization for which the discovery scan log is to be generated. Selecting Any generates a report for the departments belonging to the selected organization. For DRAO administrators, selecting Any generates a report for all the departments that are delegated to them.
Generate Report	Starts the report generation.

9.4.2 How to Generate a Detailed Report

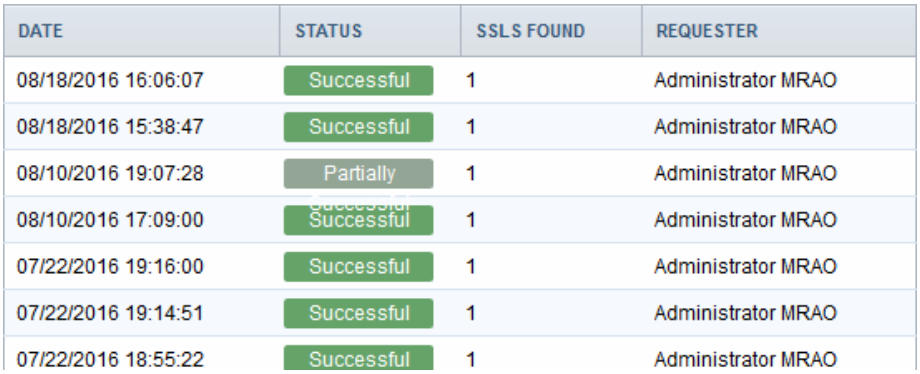
The detailed discovery scan log report shown in the following illustration is generated in a `.csv` format for a specific manual or scheduled scan and contains in-depth details of the certificates found during the selected scan. The report contains the following information:

- Organization
- Department
- IP address / port
- Common name
- Valid from
- Valid to
- Issuer
- Subject
- Serial number
- Subject alt name
- City
- State
- Country
- Key algorithm
- Key size
- MD5 hash
- SH1 hash
- Date and time found
- Cipher



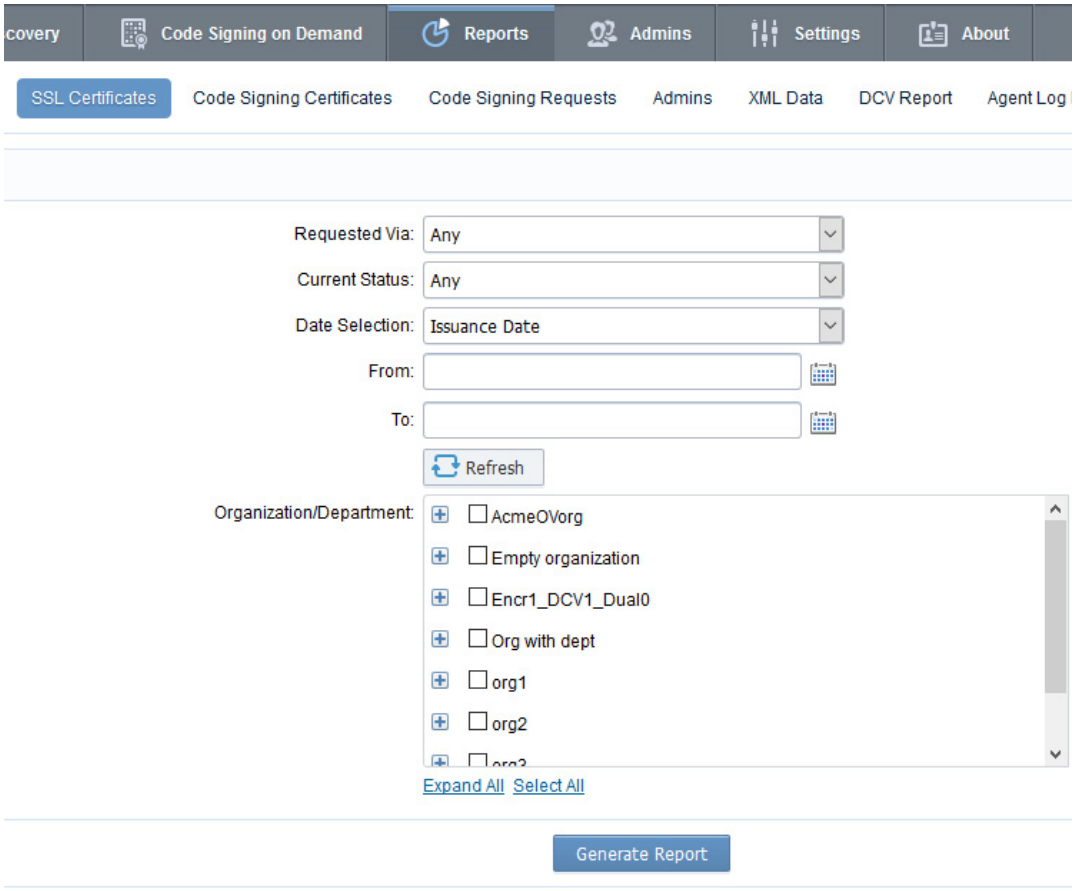
The following table lists settings available in the details report area.

Field / Element	Description
Type	Either detailed report or a summary report.

Field / Element	Description
Organization	The organization for which the discovery scan log is to be generated. Selecting Any generates a report for the organizations that have been delegated to the specific administrator. This option is not visible to DRAO administrators.
Department	The department belonging to the selected organization for which the discovery scan log has to be generated. Selecting Any generates a report for the departments belonging to the selected organization. For DRAO administrators, selecting Any generates a report for all departments that are delegated to them.
List of most recent scans	Allows you to select a scan for which the detailed discovery scan report is to be generated. 
Generate Report	Starts the report generation.

9.5 Generating SSL Certificates Reports

The **SSL Certificates** report area shown in the following illustration enables MRAO, RAO SSL, and DRAO SSL administrators to generate and view reports that reflect an activity and other statistics related to usage, provisioning, and monitoring of SSL certificates. You can generate the following types of reports: Requested, Issued, Revoked, and Expired SSL certificates. Additionally, you can filter the certificates by date of request, issuance, revocation, or expiration.



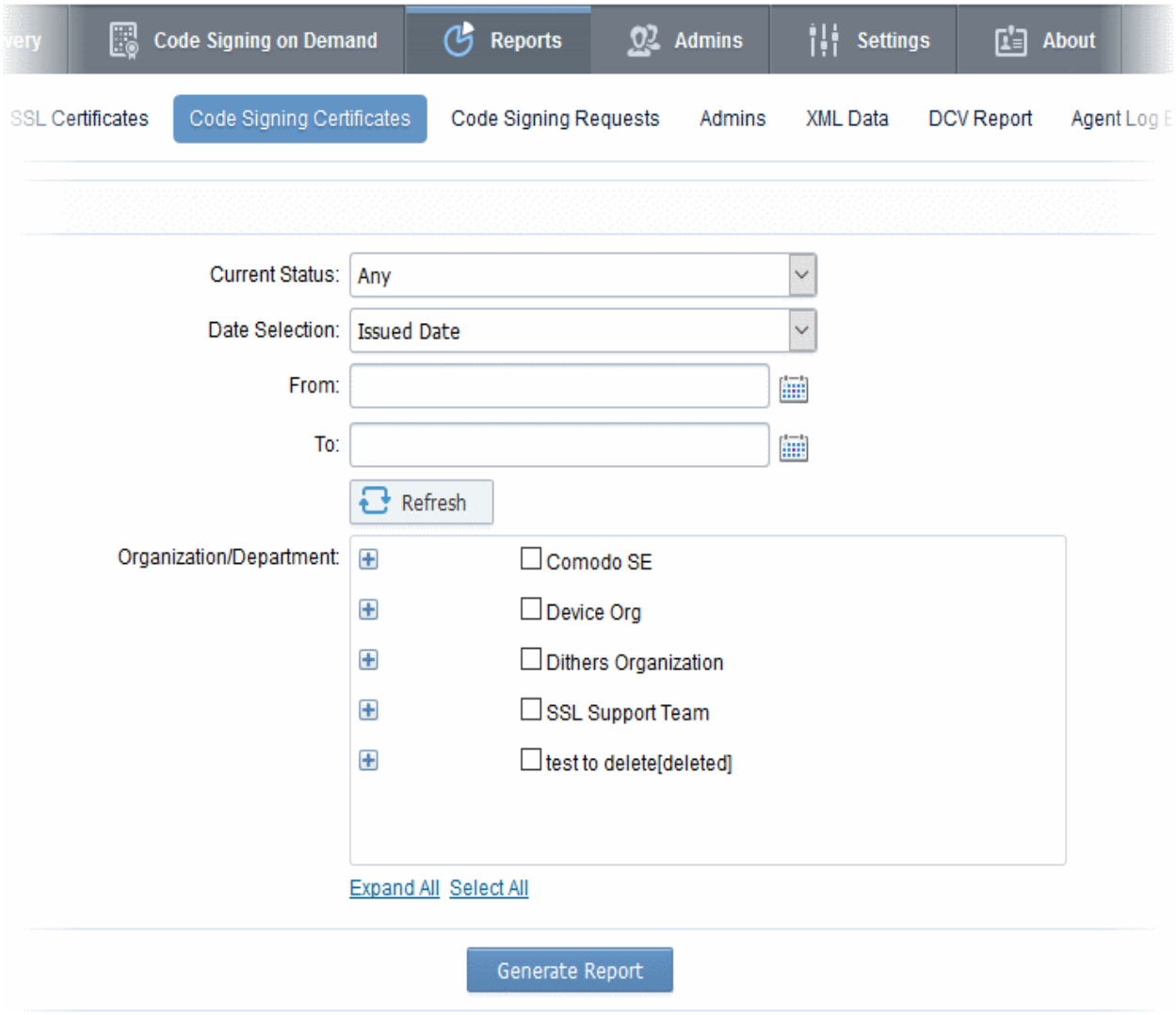
The following table lists settings available in the **SSL Certificates** report area.

Setting / Element	Description
Requested Via	The type of service or entity which requested certificates that are subject to this report: • Any—Generates a report for all SSL certificates regardless of how they were requested. • Web form—Generates a report for SSL certificates requested via a self-enrollment form. • Client Admin—Generates a report for those SSL certificates requested by a customer administrator. • Web API—Generates a report for SSL certificates requested through the use of a web API. • Discovery—Generates a report for SSL certificates identified by a discovery scan. • SCEP—Generates a report for SSL certificates requested via a SCEP. • MS Agent—Generates a report for SSL certificates requested by an MS agent. • Bulk Request—Generates a report for SSL certificates requested in bulk. • ACME—Generates a report for SSL certificates requested by the Sectigo ACME service.

Setting / Element	Description
Current Status	The current status of certificates for which the report is to be generated: • Any—Generates a report for all SSL certificate types regardless of their current status. • Requested—Generates a report for SSL certificates that have been requested. • Issued—Generates a report of those SSL certificates that have been issued successfully. • Revoked—Generates a report for SSL certificates that have been revoked. • Expired—Generates a report for SSL certificate types that have expired and are due for renewal.
Date Selection	A specific date parameter for the report. This could be one of Issuance Date, Request Date, Revocation Date, Expiration Date. The choices dependent on the status selected in the Current Status list. If no dates are specified, the report is generated for all the scans, regardless of the dates.
Organization / Department	Specific organizations or departments for which the report is to be generated. If multiple organizations or departments are selected, then you receive a single report that covers those selected organizations or departments. Each organization is displayed on a separate row in the Organizations column and each department is displayed in a separate row in the Departments column. If no organization or department is selected, the report is generated for all the organizations and departments delegated to you.
Refresh	Updates the information on the form.
Generate Report	Starts the report generation.

9.6 Generating Code Signing Certificates Reports

The **Code Signing Certificates** report area shown in the following illustration enables MRAO, RAO Code Signing, and DRAO Code Signing administrators to generate and view reports that reflect an activity and other statistics related to usage, provisioning, and monitoring of code signing certificates. You can filter reports by certificate status, organization, specific dates and time interval.



The following table lists settings available in the **Code Signing Certificates** report area.

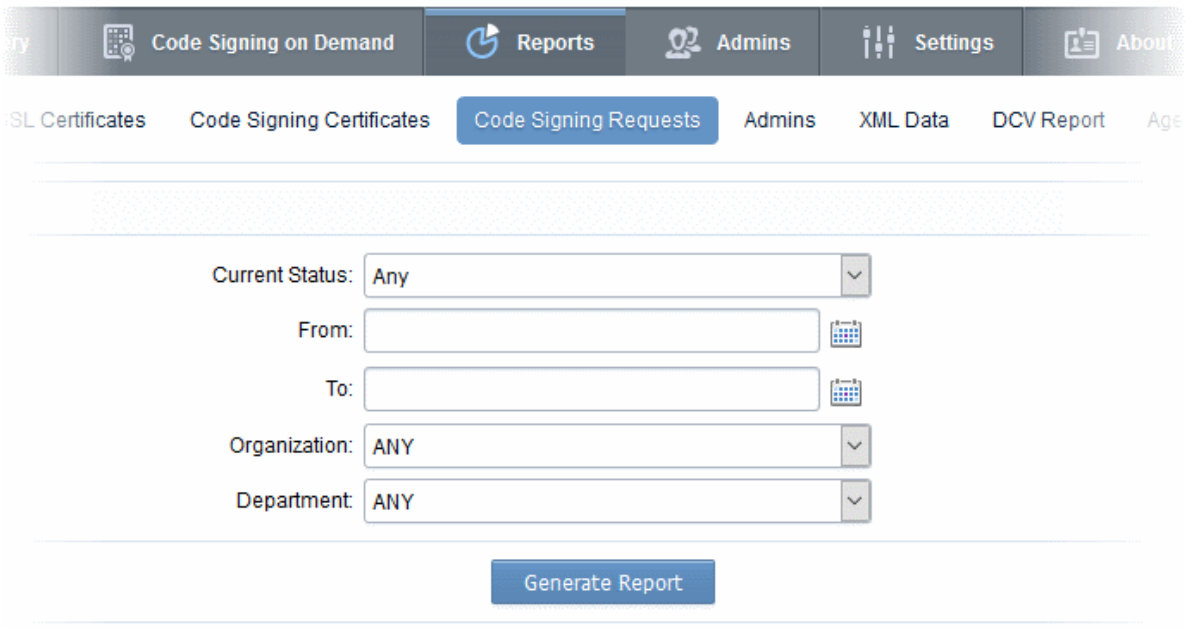
Setting / Element	Description
Current Status	Current status of the client certificates that are subject to the report generation. Valid values are: • Any—Generates a report for all code signing certificates regardless of their current status. • Enrolled—Downloaded—Generates a report of those code signing certificates that have been successfully enrolled for by the end-user and subsequently downloaded. • Enrolled—Pending Download—Generates a report of those certificates that have been successfully enrolled for by the end-user but have not yet been downloaded. • Revoked—Generates a report for certificates that have been revoked. • Expired—Generates a report only for certificates that have expired and are due for renewal.

Setting / Element	Description
Date Selection	Specific date for collecting a report. It can be date of sending invitation by the administrator, certificate enrollment, date of certificate request, date of certificate issuance, download, date of certificate revocation or expiration. The choices dependent on the status chosen in the **Current Status** field. If no dates are specified, the report is generated for all the scans, regardless of the dates.
Organization / Department	Specific organizations or departments for which the report is to be generated. If multiple organizations or departments are selected, then you receive a single report that covers those selected organizations or departments. Each organization is displayed on a separate row in the Organizations column and each department is displayed in a separate row in the Departments column. If no organization or department is selected, the report is generated for all the organizations and departments delegated to you.
Refresh	Updates the information in the form.
Generate Report	Starts the report generation.

9.7 Generating Code Signing Requests Reports

The **Code Signing Requests** report area shown in the following illustration enables MRAO, RAO Code Signing, and DRAO Code Signing administrators to generate and view reports that reflect activity and other statistics related to requests made for CSoD by developers. You can filter reports by certificate status, organization, specific dates and time interval.

NOTE: The Code Signing Requests reports area is only visible if CSoD feature is enabled for your account.

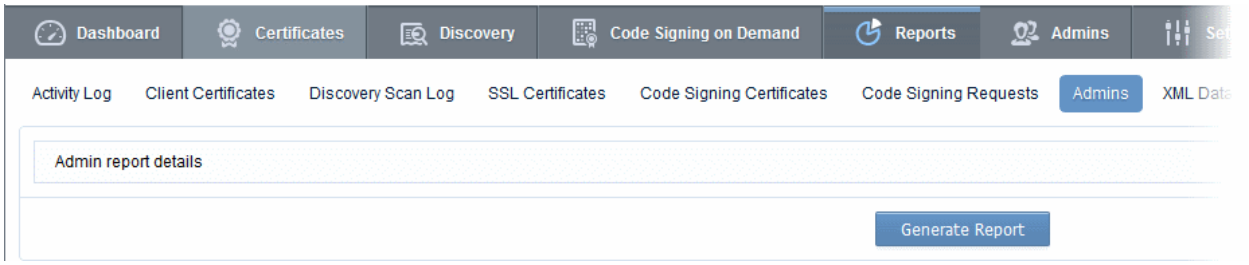


The following table lists settings available in the **Code Signing Requests** report area.

Setting / Element	Description
Current Status	The current status of the certificates that are subject to the report generation. Valid values are: • Any—Generates a report for all code signing certificates regardless of their current status. • Created—Generates a report of those code signing requests that have a status of Created. • In progress—Generates a report of those requests that have a status of In progress. • Declined—Generates a report of those requests that were declined by MRAO, RAO Code Signing, or DRAO Code Signing administrator. • Signed—Generates a report of those requests that were declined by MRAO, RAO Code Signing, or DRAO Code Signing administrator. • Expired—Generates a report of those requests that expired. • Failed—Generates a report of those requests that failed.
Date Selection	The time period for report generation.
Organization / Department	Specific organizations or departments for which the report is to be generated. If no organization or department is selected, the report is generated for all the organizations and departments delegated to you.
Generate Report	Starts the report generation.

9.8 Generating Administrators Reports

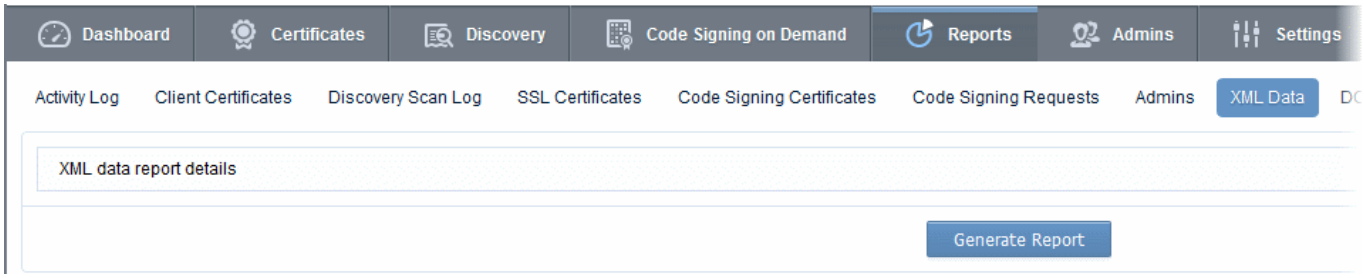
The **Admins** report area shown in the following illustration enables MRAOs to generate and view reports on all enrolled administrators, their roles, and the organizations an departments delegated to them.



Once generated, the report provides details of the name, login information, email, and role of each administrator.

9.9 Generating XML Data Reports

The **XML Data** report area shown in the following illustration enables MRAOs to generate and view reports that contain details about all organizations, departments, their administrators and certificates. These reports are generated in an XML format.



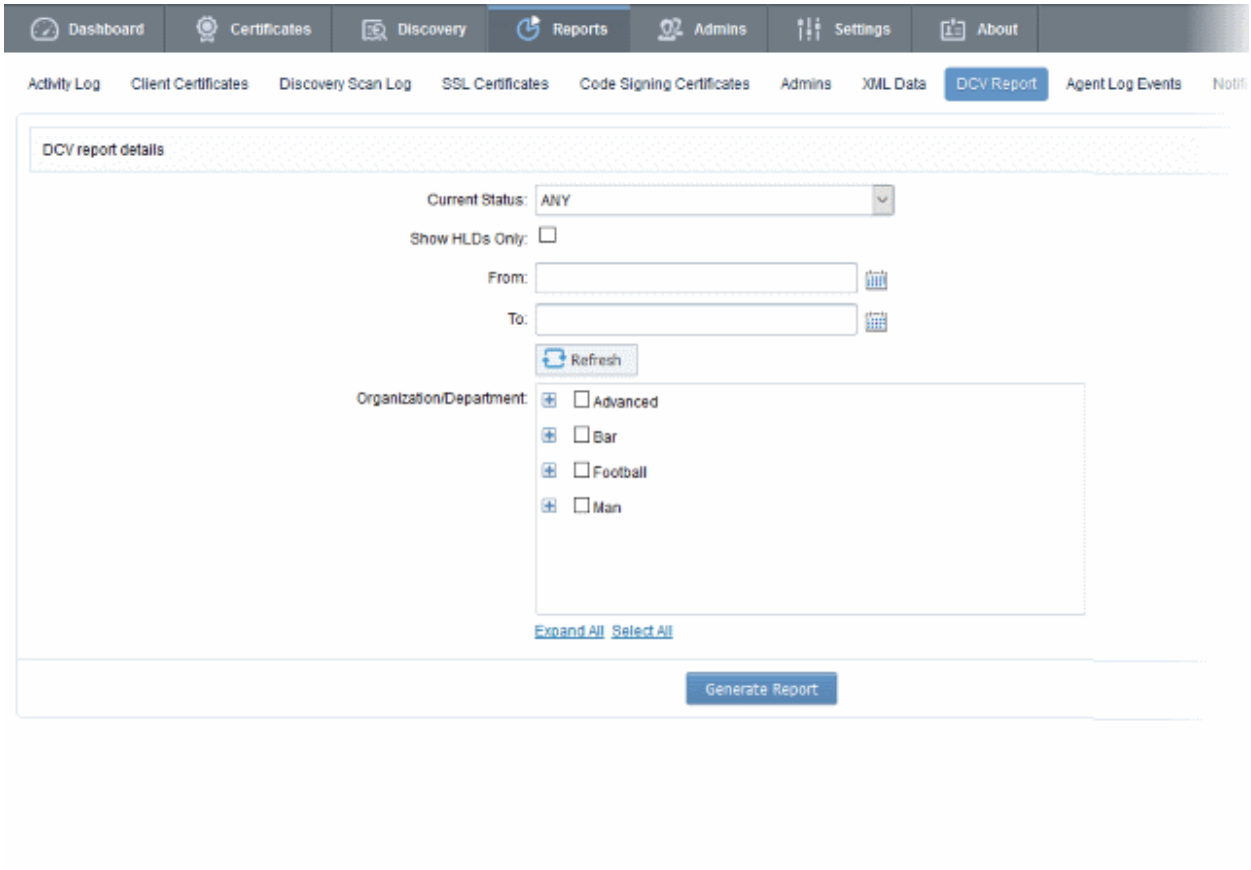
The XML file allows you to create a local database of details about an organization. The XML file can also be imported into an existing database.

9.10 Generating DCV Reports

The **DCV Report** area shown in the following illustration enables MRAO, RAO SSL, and DRAO SSL administrators to generate and view reports on the validation status of all domains. The DCV status can be one of Not Validated, Validated, Expired.

DCV reports can be generated only for high-level domains, if required.

Reports can be filtered by validation status, organization or department, and date.



NOTE: DCV reports are only available if the DCV feature is enabled for your account.

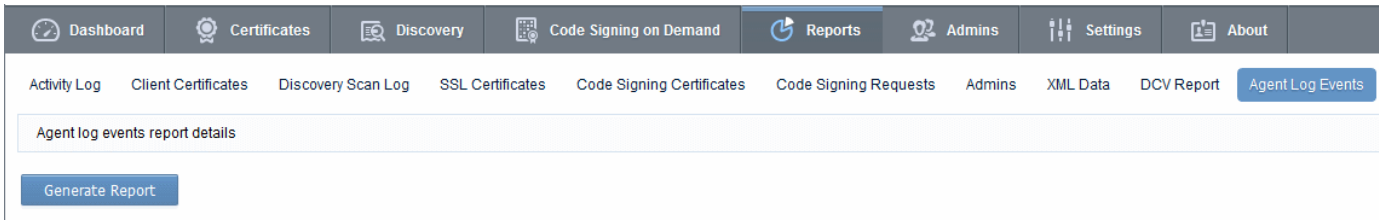
The following table lists settings available in the **DCV Reports** area.

Setting / Element	Description
Current Status	A specific current DCV status of domains that are subject to the report generation. Valid values are: • Any—Creates a report on the validation status of every domain. • Not Validated—Report covers domains that have been added to SCM but DCV has not been completed. • Validated—Report includes domains that have passed DCV, and for which DCV has not expired. New certificates can be ordered for these domains. • Expired—Report on domains where DCV has expired and needs to be renewed. DCV lasts for 1 year before it has to be renewed (re-run). All existing certificates issued to the domain remain valid for their original terms. However, you cannot obtain new certificates for the domain until it passes DCV again.
Show HLDs Only	The status of top level domains only. For example, the report would cover example.com but would not cover subdomain.example.com If the high-level domain has passed DCV, then all subdomains are also considered as validated.

Setting / Element	Description
Expiration Date	Specific time frame when DCV expires.
Organization / Department	Organizations and departments to which domains belong. If multiple organizations or departments are selected, then you receive a single report that covers those selected organizations or departments. Each organization is displayed on a separate row in the Organizations column and each department is displayed in a separate row in the Departments column. If no organization or department is selected, the report is generated for all the organizations and departments delegated to you.
Refresh	Updates the information in the form.
Generate Report	Starts the report generation.

9.11 Generating Agent Log Events Reports

The **Agent Log Events** report area shown in the following illustration enables MRAOs to generate and view reports containing complete details of the scanning and certificate installation activities of the Network Agents.



The report is generating as an XML file.

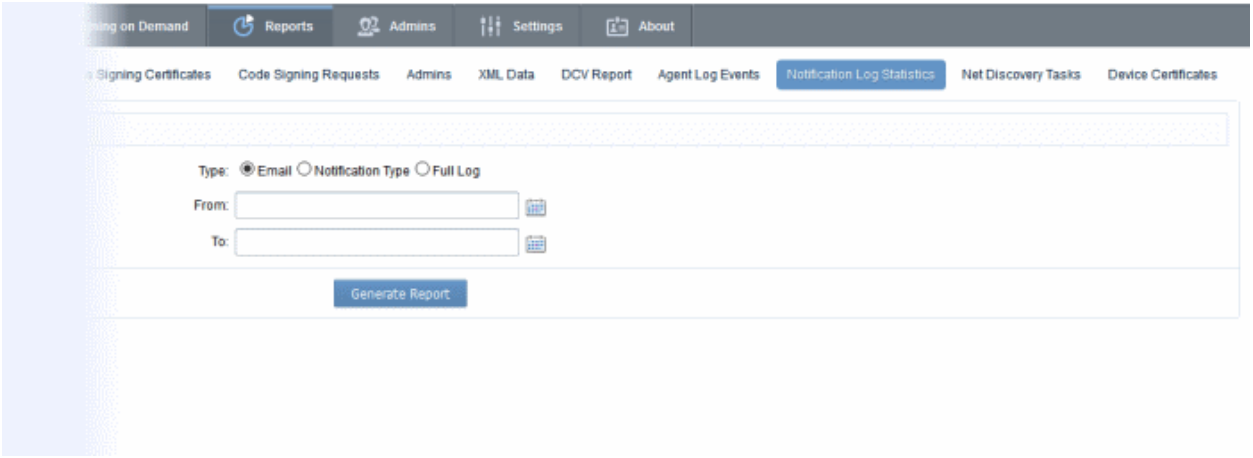
9.12 Generating Notification Log Statistics Reports

The **Notification Log Statistics Report** area enables MRAOs to generate and view log reports on the notification emails sent to RAO and DRAO administrators for various events, as configured by navigating to **Settings > Notifications** from the main UI.

SCM supports these reports as email, notification, or full log.

9.12.1 How to Generate Email Reports

The email log report shown in the following illustration can be generated in a `.csv` format for a specified time period. This report displays the number of notification emails sent to each RAO and DRAO administrator during the specified period.

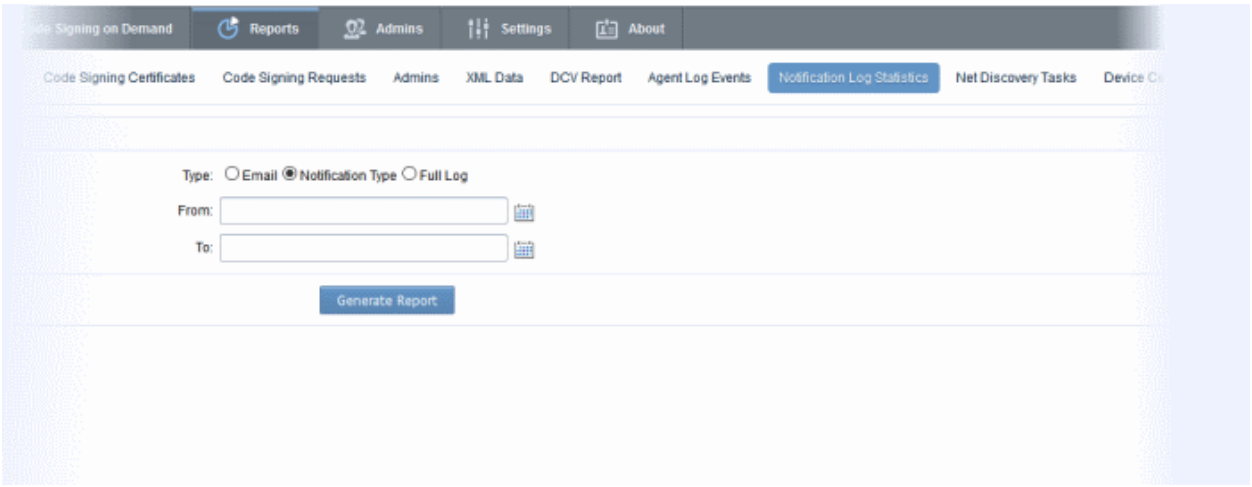


The following table lists settings available in the **Email** report area.

Setting / Element	Description
Type	Either email report, notification type report, or a full log report.
Date Range	The time period within which notification emails were sent. If no dates are specified, the report is generated for all the notification emails, regardless of the dates.
Generate Report	Starts the report generation

9.12.2 How to Generate Notification Type Reports

The notification type log report shown in the following illustration can be generated in a `.csv` format for a specified time period. This report displays the number of notification emails sent for each notification type to all RAO and DRAO administrator during the specified period.



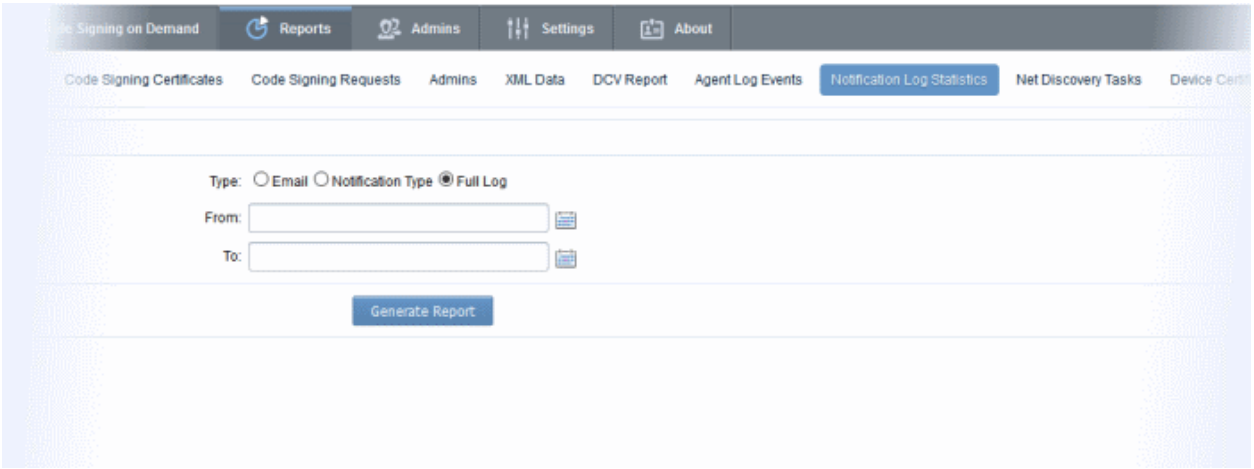
The following table lists settings available in the **Notification Type** report area.

Setting / Element	Description
Type	Either email report, notification type report, or a full log report.
Date Range	The time period within which notification emails were sent for different notification types. If no dates are specified, the report is generated for all the notifications, regardless of the dates.
Generate Report	Starts the report generation

9.12.3 How to Generate Full Log Reports

The full log report shown in the following illustration can be generated in a `.csv` format for a specified time period. This report displays a list of emails sent for various notification types to different RAO and DRAO administrators, for each notification type. The report provides the following information:

- Notification type
- Email address of the administrator to which the notification email was sent.
- Subject line of the notification email.
- Date and time when the email as sent.



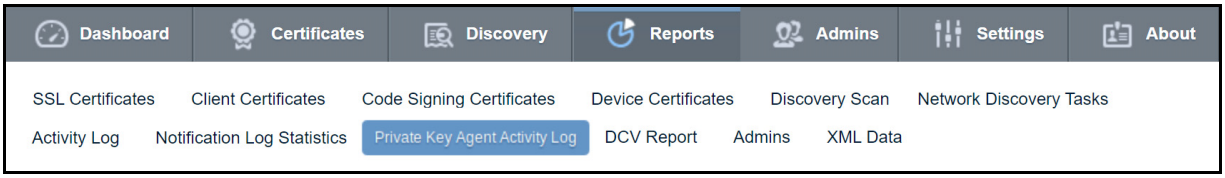
The following table lists settings available in the **Full Log** report area.

Setting / Element	Description
Type	Either email report, notification type report, or a full log report.
Date Range	The time period within which notification emails were sent. If no dates are specified, the report is generated for all the notifications, regardless of the dates.

Setting / Element	Description
Generate Report	Starts the report generation

9.13 Generating Private Key Agent Activity Log Reports

The **Private Key Agent Activity Log** report area shown in the following illustration enables MRAOs to generate and view reports that reflect all activity by the Private Key Agent. The activities of the agent include CSR generation, storage of private keys perform via auto-CSR, and a record of keys manually uploaded or downloaded by administrators. Reports can be generated for events for a selected period of time and can be downloaded in a `.csv` format.

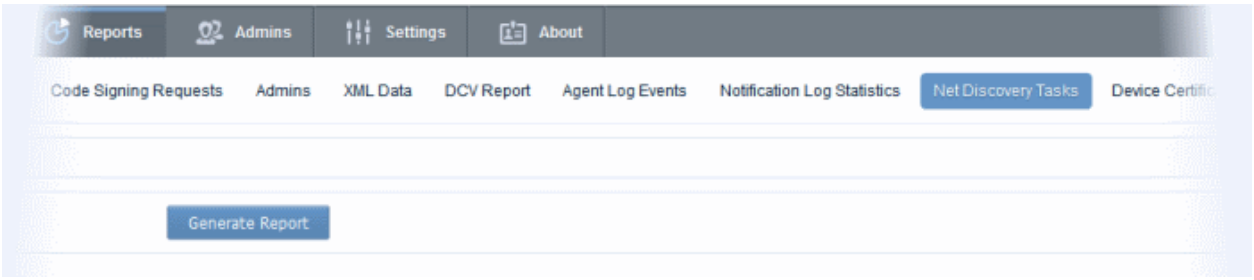


The following table lists settings available in the **Private Key Agent Activity Log** report area.

Setting / Element	Description
Date Range	The time period that is subject to the report. If no dates are specified, the report is generated for all the notifications, regardless of the dates.
Generate Report	Starts the report generation

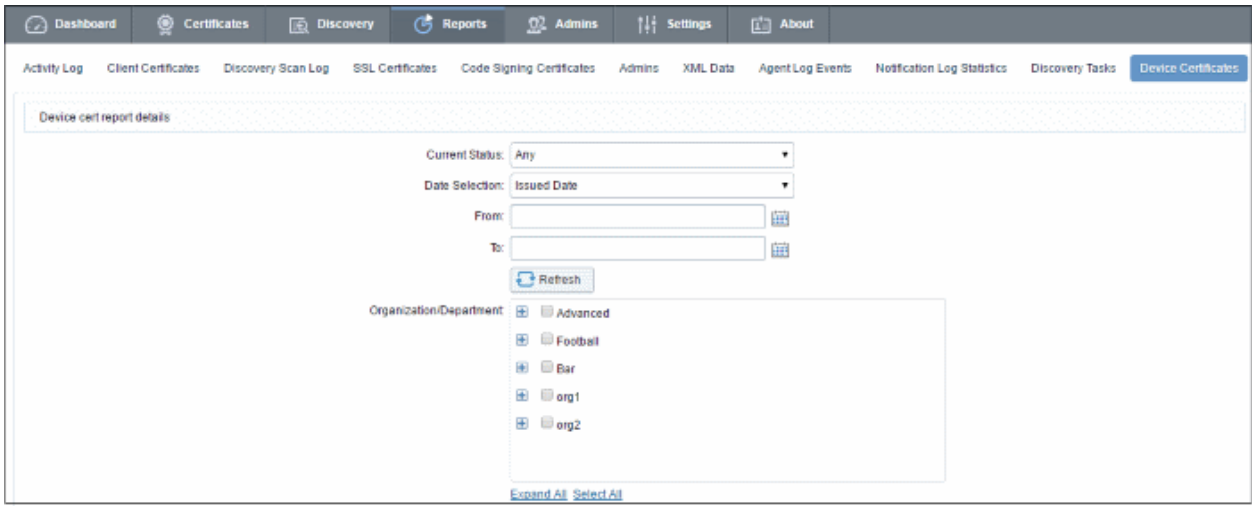
9.14 Generating Network Discovery Tasks Reports

The **Network Discovery Tasks** report area shown in the following illustration enables MRAOs to generate reports on discovery tasks for all organizations and departments, and enables RAOs and DRAOs to generate reports on discovery tasks configured for their delegated organizations and departments. Reports can be generated for events for a selected period of time and can be downloaded in a `.csv` format.



9.15 Generating Device Certificate Reports

The **Device Certificates** report area shown in the following illustration enables MRAOs to generate reports on device certificates assigned to all organizations and departments, and enables RAOs and DRAOs to generate reports on device certificates assigned to their delegated organizations and departments. Reports can be generated for a specific certificate status, date of issuance of certificates, their revocation, request, expiry dates, and by the organization and department. The report can be downloaded in a `.csv` format.



The following table lists settings available in the **Device Certificates** report area.

Setting / Element	Description
Current Status	The current status of the device certificate. Valid values are: • Any—Generates a report for all device certificates regardless of their current status. • Awaiting Approval—Device certificates which are pending approval from a MRAO or RAO. • Approved—Device certificates that have been approved but not yet downloaded. • Applied—Device certificates that were requested via the self-enrollment form and are awaiting approval. • Issued—Device certificates that have been successfully issued by Sectigo. • Downloaded—Device certificates that have been downloaded by administrators or end-users. • Revoked—Device certificates that have been revoked by Sectigo. These certificates are no longer valid. • Expired—Device certificates whose Valid To date has passed and are due for renewal.
Date Selection	A specific date event and range for the report. Date events can be date of request, date of issuance, date of revocation, or date of expiry. The choices depend on the status selected in the **Current Status** field. If no dates are specified, the report is generated for all time.

Setting / Element	Description
Organization / Department	Specific organizations or departments that are subject to the report. If multiple organizations or departments are selected, then you receive a single report that covers those selected organizations or departments. Each organization is displayed on a separate row in the Organizations column and each department is displayed in a separate row in the Departments column. If no organization or department is selected, the report is generated for all the organizations and departments delegated to you.
Refresh	Updates the information in the form.
Generate Report	Starts the report generation.

10

Using SCM with Microsoft Intune

This chapter provides information on how to integrate SCM with Microsoft Azure and configure Microsoft Intune for enrollment and management of client and device certificates.

This chapter describes the following topics:

- Microsoft Intune Configuration Overview
- Configuring SCEP
- Configuring Intune Export

10.1 Microsoft Intune Configuration Overview

The SCM integration with Microsoft Azure provides the means to use one of the following methods for enrolling and managing certificates on mobile devices:

- Microsoft Intune configured for SCEP allows you to issue and manage certificates. For more information, see "Configuring SCEP" on page 599.
- Microsoft Intune Export allows you to export certificates and private keys from SCM to Intune. For more information, see "Configuring Intune Export" on page 605.

10.2 Configuring SCEP

SCEP is a certificate enrollment protocol standard designed to provide scalability to digital certificate issuance.The process of integrating SCM with Microsoft Azure and configuring Microsoft Intune for SCEP involves the following:

- Configuration—a one-time administrative event that is performed on the Microsoft side.
- Certificate enrollment—an on-going process that involves assigning each device in Microsoft Intune.

The following configuration steps are to be performed by the Microsoft Intune administrator:

- Registration in Microsoft Azure: a new application must be registered under the Microsoft Azure account to allow the application to receive an identifier (`AAD_APP_ID`) and key (`AAD_APP_KEY`) that SCM can use to communicate with Intune. The tenant name must also be obtained from Microsoft Azure.
- Profile setup: trusted and SCEP profiles must be configured in Microsoft Intune, and then assigned to the corresponding devices and users.
- SCM setup: SCM must be supplied with the registration attributes defined in the previous steps. Certificates can be enrolled on mobile devices powered by iOS and Android platforms. This requires a Microsoft application called the Intune Company Portal to be installed in order to enable the device interaction with Microsoft Intune.

Everything else, including reading of profiles, request and validation of the certificate, as well as the subsequent certificate enrollment and notification about the process completion occurs seamlessly in the background of the device.

NOTE: The application configuration and profile registration processes are platform-dependent. The procedures described in this document are applicable to the iOS-powered devices only, unless stated otherwise.

10.2.1 How to Register the Application

By registering the application in Microsoft Azure, you enable SCM to access the Intune SCEP Validation API, as follows:

1. Sign in to Microsoft Azure portal at https://portal.azure.com
2. Search for **Azure Active Directory**.
3. Select **Manage > App registrations**.
4. Select **New registration**, and then perform the following:
   a. Enter an application name (for example, Sectigo Certificate Manager SCEP).
   b. Select the account type as **Accounts in this organization only**.
   c. Enter the sign-on URL (for example, `https://<SCM_IP>/customer/<Customer_URL_extension>`), and then click **Register**.
5. From your newly-created application page, select **Manage > API permissions** and perform the following:
   a. Click **Add a permission** and select **Microsoft APIs > Intune**.
   b. Click **Application permissions**, select **SCEP challenge validation**, and then click **Add permissions**.

      It is essential to perform this step, as Microsoft Intune differentiates between added permissions and granted permissions.
6. Click **Keys**, enter a description (for example, SCM Key 1), and set the desired duration for the key (for example, **never expires**).

Since the key value is an equivalent to password and is not accessible after you leave the window, it is recommended that you copy and save it in a private location. In addition, the key value, application ID, and tenant name are required for completing the SCM configuration section, as described in "How to Authenticate SCM to Microsoft Azure" on page 603.

10.2.2 How to Determine the Tenant Name

The tenant name is required when performing configuration. You can obtain this information as follows:

- Sign in to Microsoft Azure portal at https://portal.azure.com
- Select **Azure services > Azure Active Directory > Overview a**nd locate the tenant name at the top part of the page (typically, in the form `somedomain.com`).

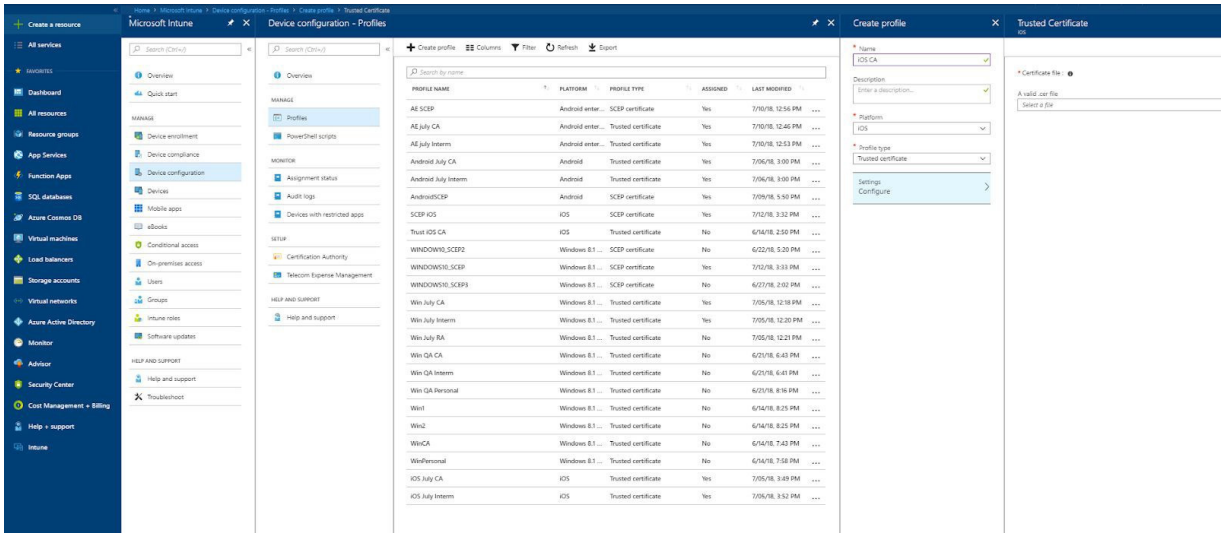
  Alternatively, you can click **Switch Directory** and find the tenant name adjacent to **Current directory**.

10.2.3 How to Create Trusted Certificate Profiles

Trusted certificate profiles must be created for each platform individually. These profiles must then be assigned to the corresponding devices. Each profile contains a certificate that allows a device to trust the SCEP server. You can create and assign such profiles as follows:

1. Sign in to Microsoft Azure portal at https://portal.azure.com
2. Select **Azure services > More services > Intune**.
3. Select **Device configuration > Manage > Profiles > Create profile**, as shown in the following illustration, and then do the following:
   a. Enter the profile name. It is recommended to combine information about the platform and type of trusted certificate (for example, iOS CA).
   b. Select platform (for example, iOS).
   c. Select **Trusted certificate** as profile type.
   d. Upload the trusted certificate file in DER format. This file is issued by your CA as a public certificate. It can also come from any device that trusts your issuing CA.
   e. Click **OK**.
4. Click **Create** to finalize the trusted profile creation.
5. Select the newly created profile.
6. Specify **Assignments** as follows:
   a. Select either a group to assign or **All devices**.
   b. Click **Save**.

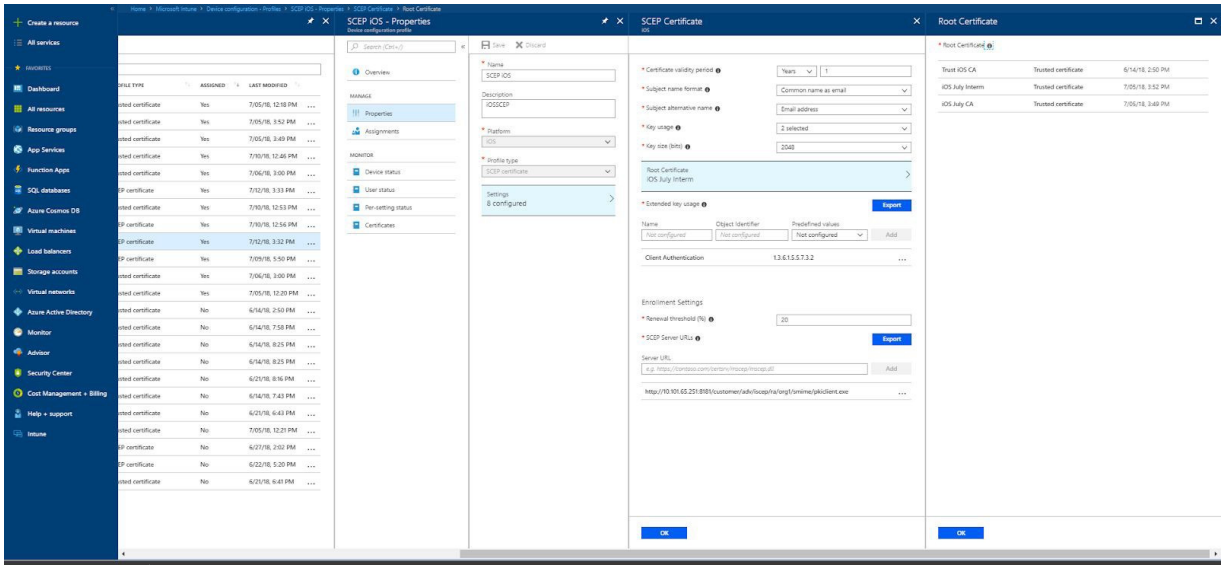
These steps must be performed for each trusted certificate, and twice for each platform. The trusted certificate files are provided by Sectigo.



10.2.4 How to Create a SCEP Profile

You can create a SCEP profile and point it to SCM as follows:

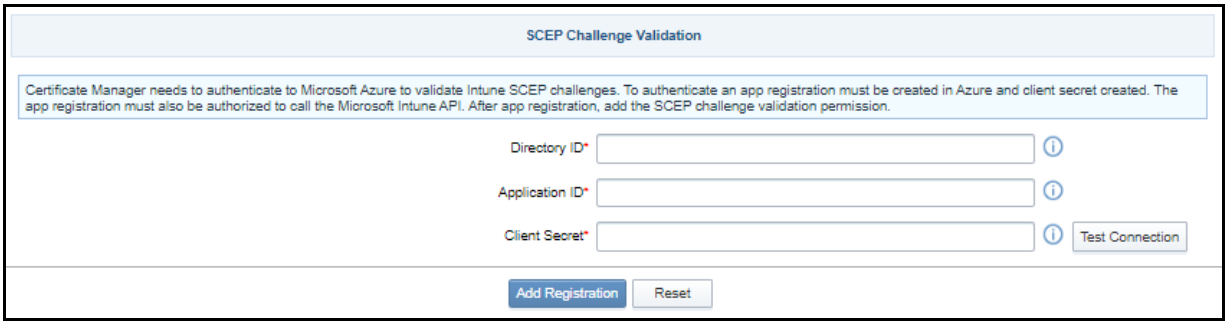
1. Sign in to Microsoft Azure portal at https://portal.azure.com
2. Select **Azure services > More services > Intune**.
3. Select **Device configuration > Manage > Profiles > Create profile**, as shown in the following illustration, and then do the following:
   a. Enter the profile name. It is recommended to combine information about the platform and type of trusted certificate (for example, iOS SCEP).
   b. Select platform (for example, iOS).
   c. Select **SCEP Certificate** as profile type.
   d. Set the certificate validity period to 1 year.
   e. Set the **Subject name format** to **Common name as email**.
   f. Set the **Subject Alternative Name** to one of the values, such as an email address. It is recommended that you only set one option, as multiple options may cause errors in the Intune company profile. Optionally, you may select a **User Principal Name (UPN)** to be included in the client certificate, in which case this additional name (UPN) is appended to the RFC822 name in the Subject Alternative Name field. In order for a UPN to be sent with the request, the **Allow Principal Name** option must be enabled for the appropriate organization or department in SCM (see "Using the Client Certificate Area of the Add New Organization Dialog" on page 336).
   g. Set **Key usages** to **Digital signature** and **Key encipherment**.
   h. Set **Key size** to **2048**.
   i. Set **Root Certificate profile** to the intermediate trusted profile created in "How to Create Trusted Certificate Profiles" on page 601.
   j. Specify **Extended key usage** by selecting **Client Authentication** and clicking **Add**.
   k. If the SCEP profile is created for enrollment of a client certificate, enter the SCEP URL as `http://<hostname>/customer/<customer_URL_extension>/iscep/default/<access_code_of_organization_or_department_specified_for_client_certificates_enrollment_using_SCEP>/smime/pkiclient.exe;` If the profile is created for enrollment of a device certificate, enter the SCEP URL as `http://<SCM_IP>/customer/<customer_URL_extension>/iscep/default/<access_code_of_organization_or_department_specified_for_device_certificates_enrollment_using_SCEP>/device/<type_id_of_the_enrolled_device_certificate_type>/pkiclient.exe`, and then click **OK** and **Save**.
4. Click **Create** to finalize profile creation.
5. Select the newly created profile.
6. Specify **Assignments** as follows:
   a. Select either a group to assign or **All devices**.
   b. Click **Save**.



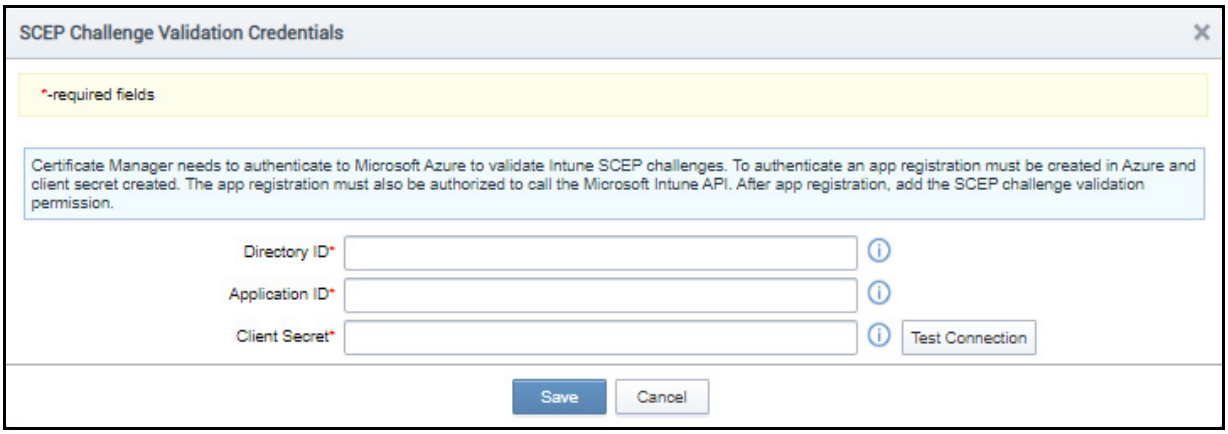
10.2.5 How to Authenticate SCM to Microsoft Azure

The SCEP functionality must be manually enabled for your organization by your Sectigo account Manager. Once enabled, you must complete the SCEP challenge validation by providing the application registration artifacts to SCM. Once enabled, SCEP enrollment requests can pass from SCM through the Intune API.

You can authenticate SCM to Microsoft Azure by navigating to **Settings > Intune**. The **SCEP Challenge Validation** area is shown in the following illustration.



If the application has been registered in Microsoft Azure (see "Configuring SCEP" on page 599), the fields are already populated with values which you can modify by clicking **Edit** or remove it by clicking **Reset**. If the application has not been registered in Microsoft Azure, proceed by clicking **Add Registration** and completing the **SCEP Challenge Validation Credentials** dialog shown in the following illustration.



Alternatively, you may chose not to do it yourself but instead delegate this task to a Sectigo administrator by providing them with the data to enter.

For device certificates, you navigate to **Settings > Certificates > Device Certificate Types** to ensure that the desired certificate types have been configured and **Allow for SCEP** enabled (see "How to Configure Device Certificate Types" on page 496). The **SCEP Enabled** must also be activated for the organization or department under which you intend to enroll device certificates or client certificates through Microsoft Intune.

When defining the **Subject name format** during the SCEP profile creation, as described in "How to Create a SCEP Profile" on page 601, only existing attributes must be used; otherwise, the request fails.

There are other settings that are used by the Microsoft Intune library. Empty fields are automatically accepted as default values.

10.2.6 Issues and Limitations Related to Different Platforms

On iOS-powered devices, Apple MDM Push Certificate must be installed to allow access to Microsoft Intune. The process includes downloading the MDM Certificate from Microsoft Azure and sending it to the Apple portal. For more information, see the following:

- *Get an Apple MDM push certificate* at https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get
- *Intune and the APNs certificate: FAQ and common issues* at https://techcommunity.microsoft.com/t5/Intune-Customer-Success/Intune-and-the-APNs-certificate-FAQ-and-common-issues/ba-p/280121

On Android-powered devices, Microsoft Azure displays the enrollment status as Failed for a few minutes after accepting the new certificate by the device owner following a successful certificate enrollment. This status changes to Successful in the background during the device synchronization.

On both iOS- and Android-powered devices, if a SCEP profile is created for a device certificate, it is accessible via the following URL:

`http://<SCM_IP>/customer/<customer_URL_extension>/iscep/default/<access_code_of_organization_or_department_specified_for_device_certificates_enrollment_using_SCEP>/device/<type_id_of_the_enrolled_device_certificate_type>/pkiclient.exe`

On Windows, if a SCEP profile is created for a device certificate, it is accessible via the following URL:

`http://<SCM_IP>/customer/<customer_URL_extension>/iscep/chain/<access_code_of_organization_or_department_specified_for_device_certificates_enrollment_using_SCEP>/device/<type_id_of_the_enrolled_device_certificate_type>`

On Windows, it is recommended to delete `pkiclient.exe` that may be appended automatically to the SCEP URL during enrollment.

To enroll a certificate, the Intune Company Portal must be installed on a device using the application store associated with the particular platform. That is, Google Play for Android or Apple App Store for IOS. If everything is configured correctly, enrollment is completed after the first sign-on to the Intune Company Portal. The Intune Company Portal may take measures in order to enforce security. For example, it can run on password-protected devices. Each group for which enrollment of device certificates through Intune is enabled must have only one set of Profiles assigned. This also implies that these profiles must be created for use on one particular platform.

10.3 Configuring Intune Export

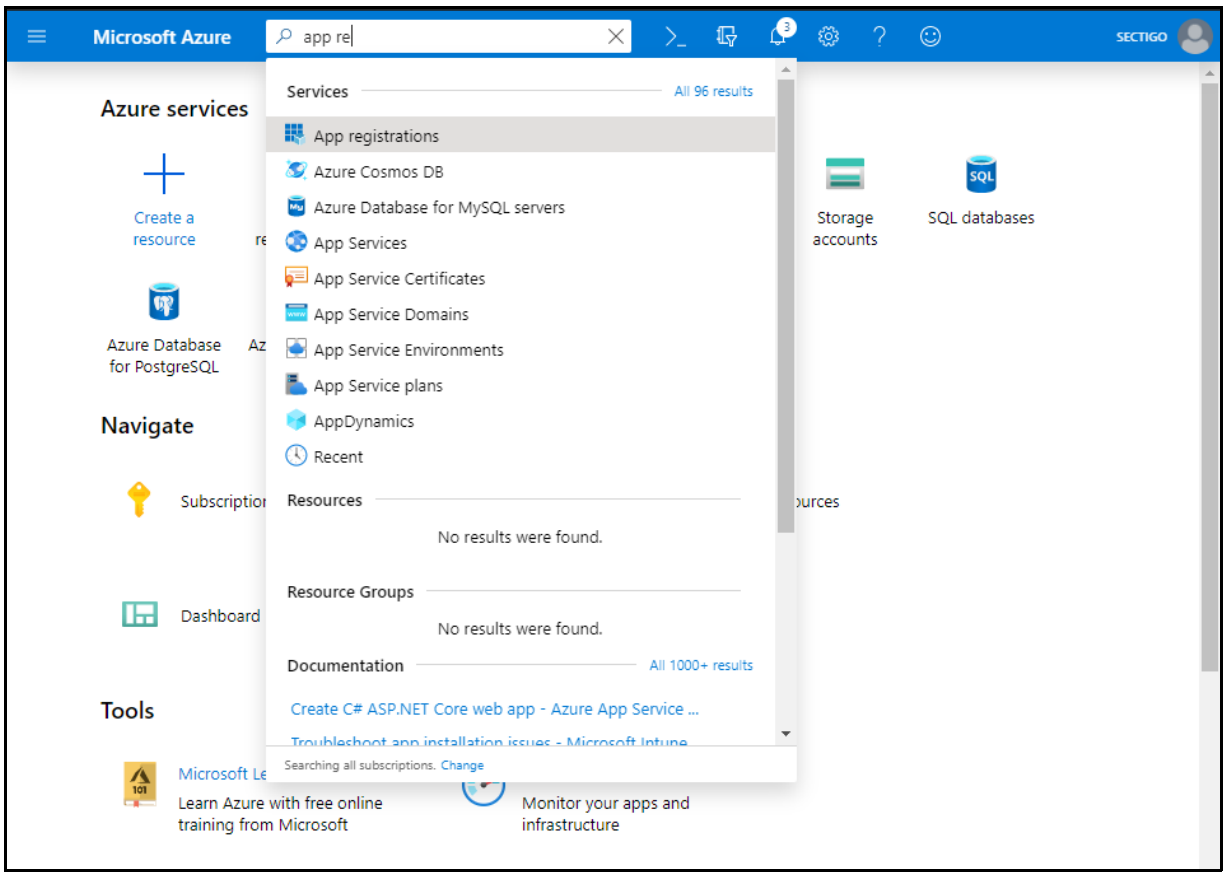
Intune Export allows you to export certificates and private keys from SCM to Intune for use with mobile device management.

Before configuring Intune Export, you must ensure that SCM can map to your Intune account. SCM can map persons to users in your Intune account when one of the following requirements is satisfied:

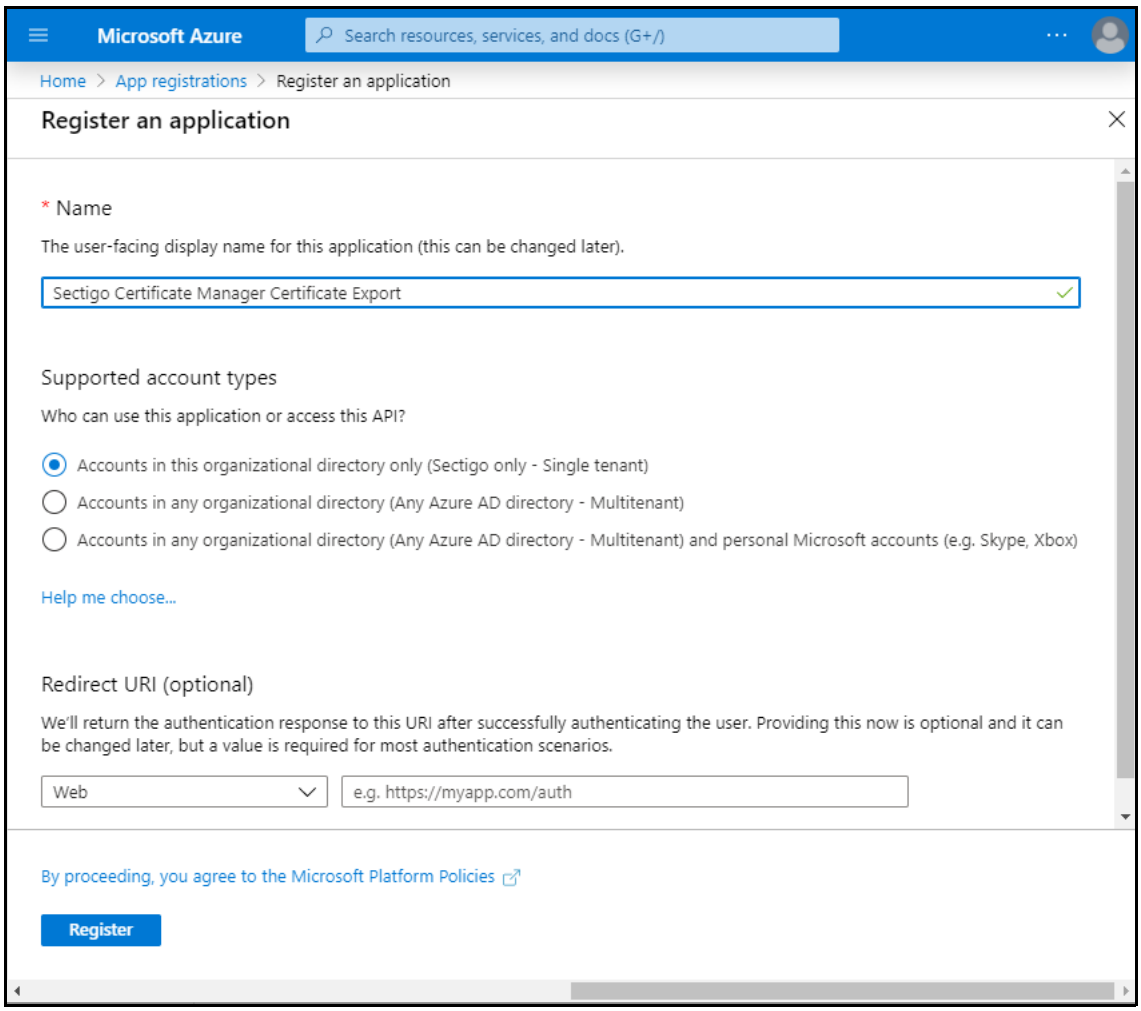
- The **UPN** for the person account (client certificate) in SCM must be the same as the **user name** in Azure. It is recommended that you choose this approach.
- The **Email** for the person account (client certificate) in SCM must be the same as the **mail** attribute in Azure. For more information on how to configure the Azure's **mail** attribute, consult Microsoft's documentation.

To register SCM as an application in Azure, do the following:

1. From the Azure Portal, navigate to **App registrations**, as shown in the following illustration.



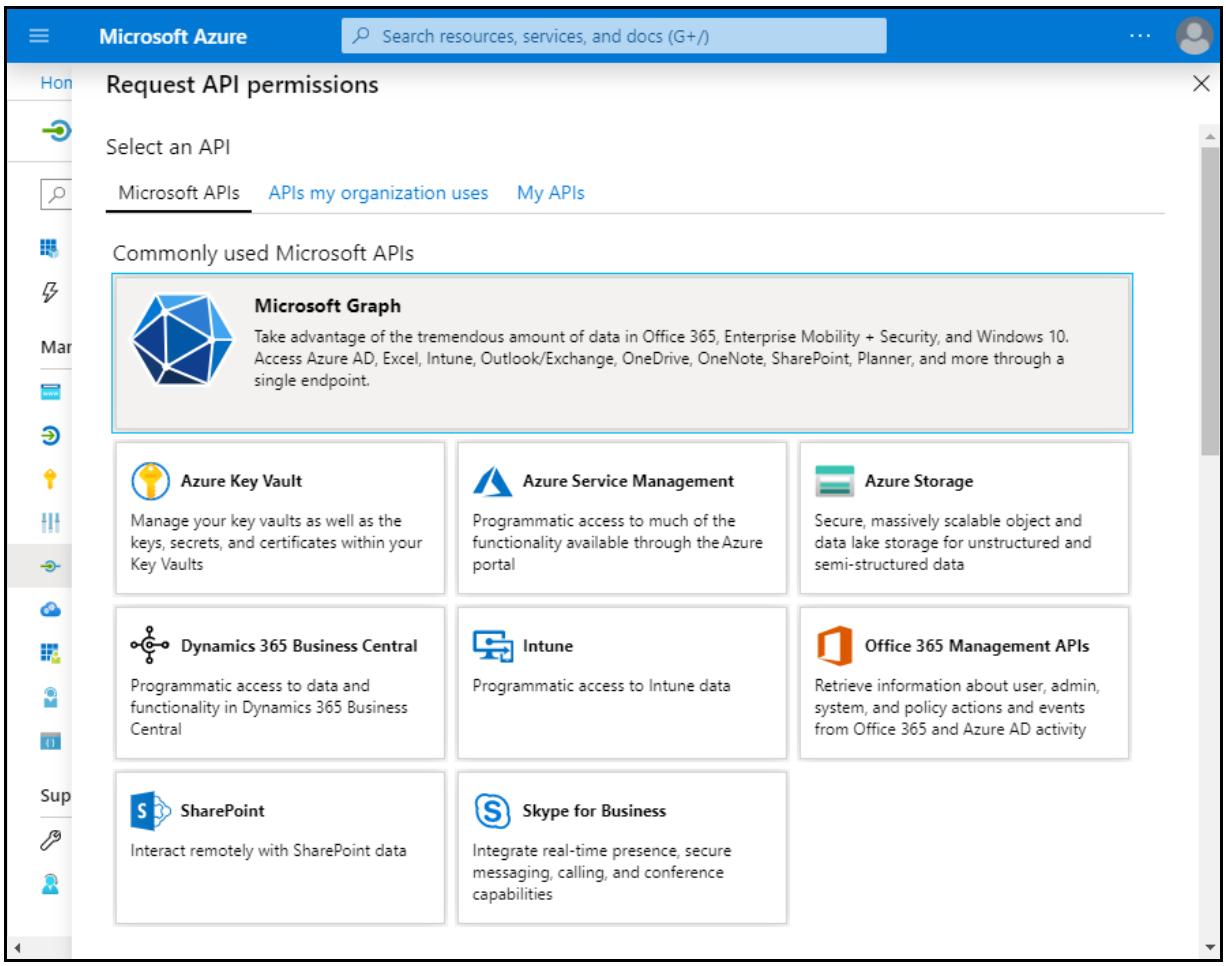
2. Click **New Registration** to open the **Register an application** page shown in the following illustration.



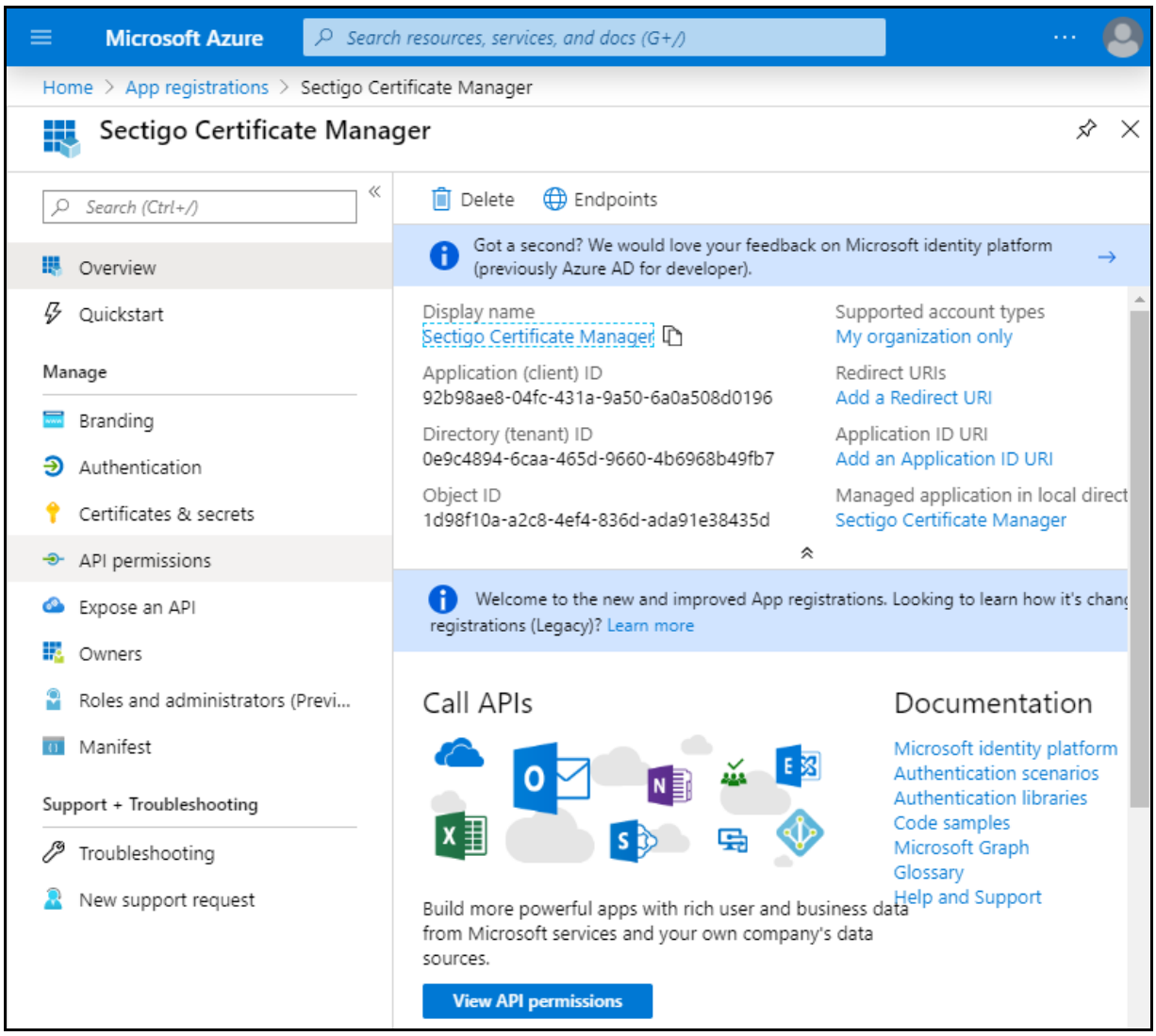
3. Complete the **Register an application** fields based on the information provided in the following table.

Field	Value
The user-facing display name for this application	Sectigo Certificate Manager Certificate Export (recommended)
Supported account types	Default
Redirect URI	Default

4. Click **Register**.
5. Select **API permissions** and click **Add a permission** to open the **Request API permissions** area, as shown in the following illustration.



6. Select **Microsoft Graph**, and then select **Application permissions**.
7. Use search to locate and enable the following permissions:
   - User.Read.All
   - Directory.Read.All
   - DeviceManagementConfiguration.ReadWrite.All
8. Click **Add permissions**.
9. If you are an administrator in Azure, click **Grant admin consent for Sectigo**. If you are not an administrator in Azure, you need to wait for an Azure administrator to approve the permissions before continuing.
10. Select **Certificates & secret** and click **New client secret**.
11. In the **Add a client secret** area, provide a description (for example, SCM Access) and select **Never**.
12. Click **Add**.
13. Record the secret **Value.**
14. Record the **Application ID** and **Directory ID** from the **Overview** section, as shown in the following illustration.



To configure your Intune infrastructure for using imported PKCS certificates, do the following:

1. Navigate to at https://docs.microsoft.com/en-us/intune/protect/certificates-imported-pfx-configure and use the Microsoft documentation complete the following steps:
   a. Download, install, and configure the PFX Certificate Connector.
   b. Build PFXImport PowerShell Project `cmdlets`.

      It is recommended that you complete this step using the Intune Resource Access branch located at https://github.com/mkarasik/Intune-Resource-Access instead of the one suggested in the Microsoft documentation.
   c. Create the encryption public key.

      You must export the key to a file using the following command:

      ```
      Export-IntunePublicKey -ProverName "<ProviderName>" -KeyName
      "<KeyName>" -FILEFORMAT "PEM" -FilePath "<File path\Filename.PFX>"
      ```

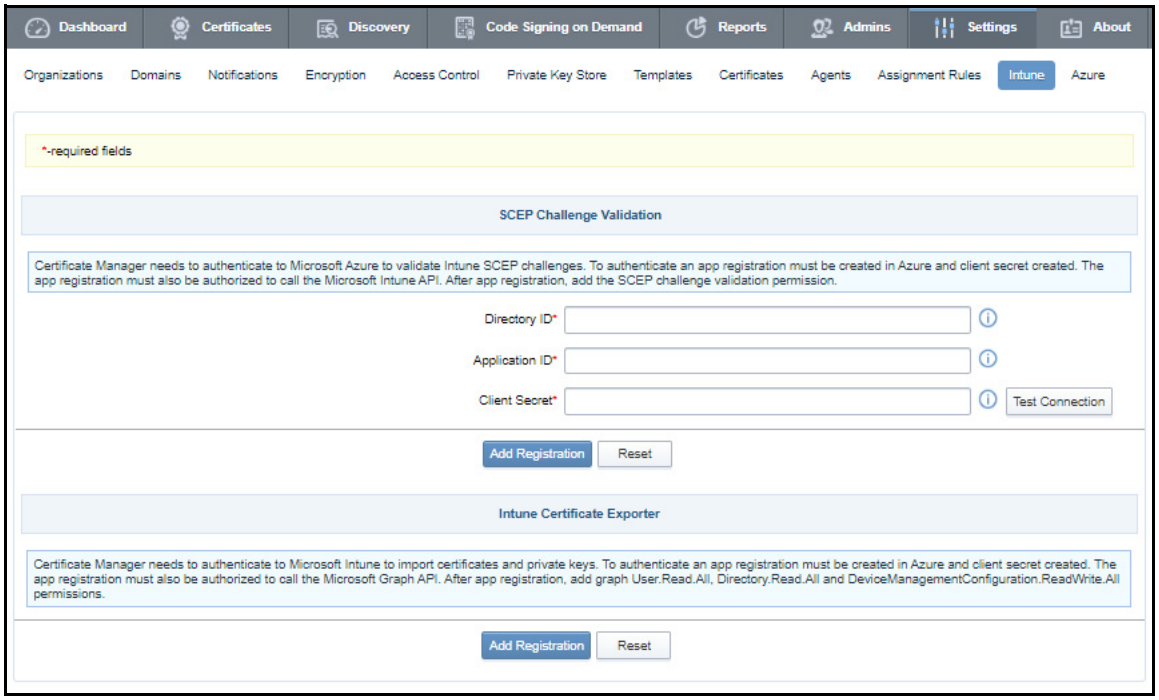
      When following the Microsoft documentation, skip the **Import PFX Certificates** and **To import the PFX certificate** sections.

d. Create a PKCS imported certificate profile.

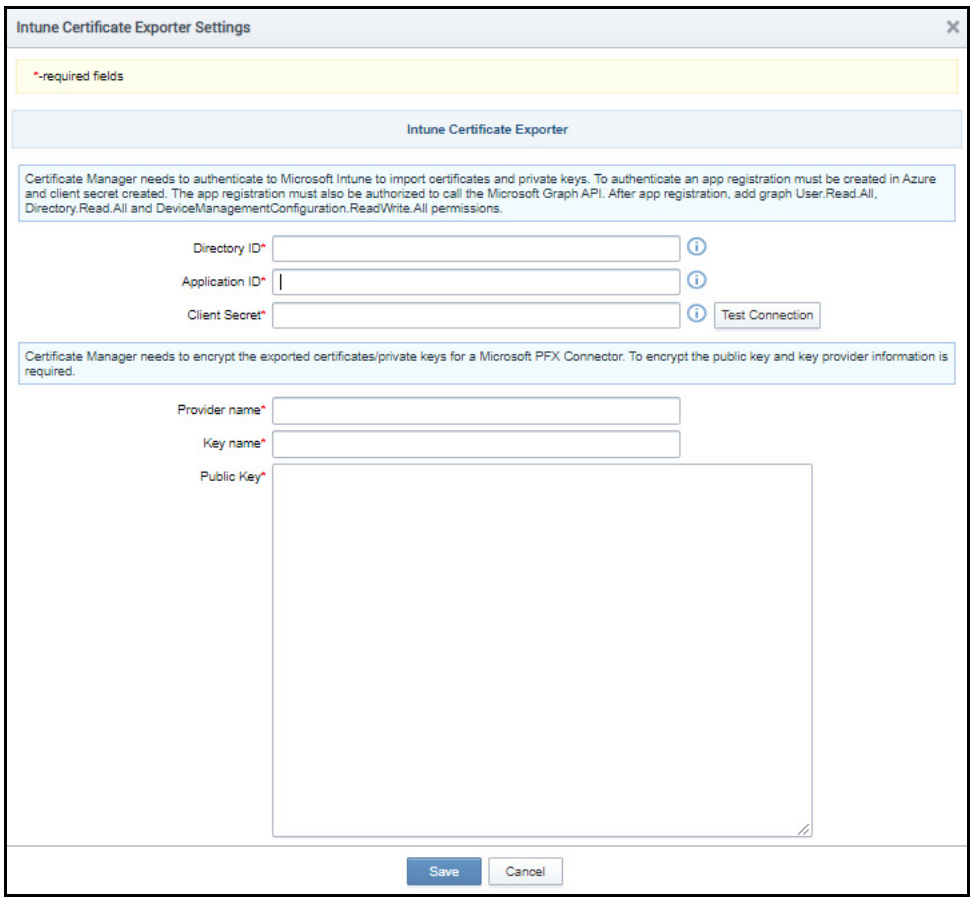
2. Record your **Provider name**, **Key name**, and **Public Key**.

To configure SCM for Intune Export, do the following:

1. From SCM, navigate to **Settings > Intune**, as shown in the following illustration.



2. Under **Intune Certificate Exporter**, click **Add Registration** to open the **Intune Certificate Exporter Settings** area shown in the following illustration.



3. Complete the **Directory ID**, **Application ID**, and **Client Secret** fields using the values you recorded during the application registration.
4. Click **Test Connection** to validate the data.
5. Complete the **Provider name**, **Key name**, and **Public Key** fields using the values you recorded during the Intune configuration.
6. Click **Save**.

11

Configuring and Testing the Sectigo EST Service

The Sectigo EST service supports enrolling certificates from an account in SCM. This chapter describes how to set up this service to perform test enrollments of certificates using an open source Enrollment over Secure Transport (EST) client.

This chapter describes the following topics:

- Configuring Sectigo EST Service
- Testing Enrollments

11.1 Configuring Sectigo EST Service

Prior to configuring the Sectigo EST service, ensure that Sectigo performed the following:

- Provisioned you with a customer instance of EST.
- Provided you the instance hostname and authentication credentials.

To start the configuration process, login to the EST configuration application in a browser of your choice by navigating to `https://<instance_hostname>/login`.

Configuring EST consists of the following two steps:

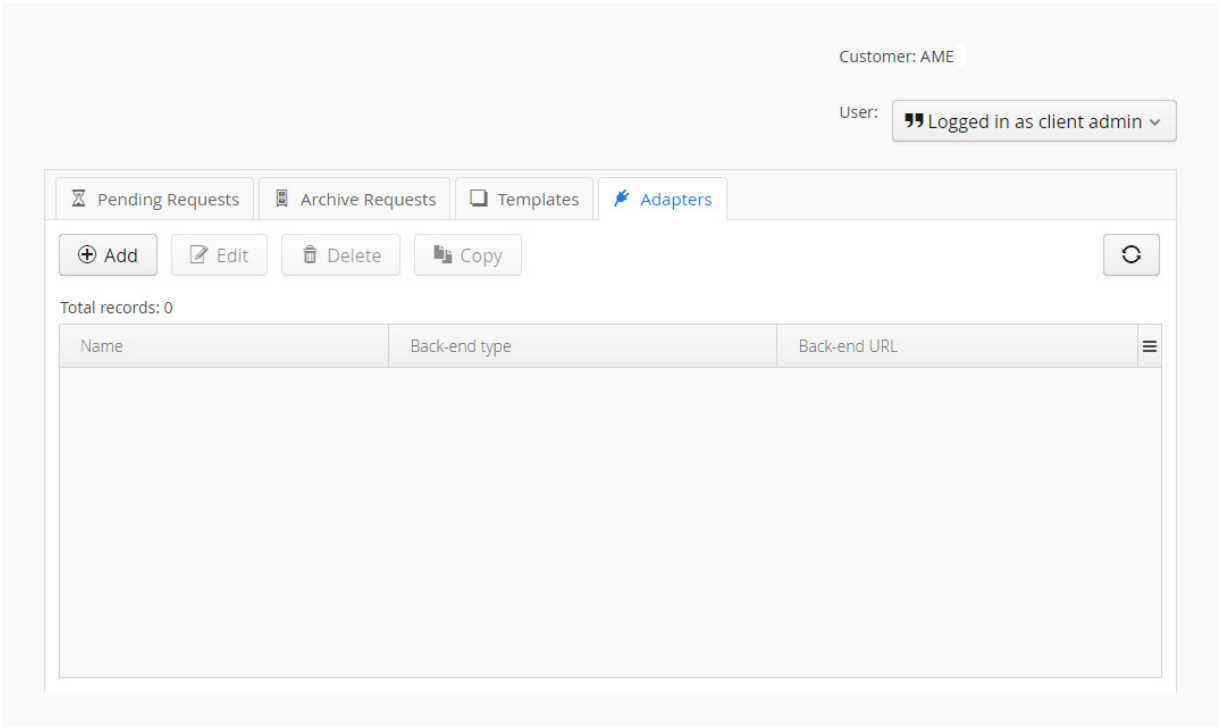
1. Creating one or more adapters to connect to the Sectigo certificate issuance system (see "How to Create an Adapter" on page 612).
2. Creating one or more templates that map an incoming request to an adapter (see "How to Create a Template" on page 614).

   NOTE: Sectigo may precreate the adapters and make them available to you.

11.1.1 How to Create an Adapter

An adapter connects the EST service to a Sectigo certificate issuance system. You create an adapter as follows:

- Select the **Adapters** tab shown in the following illustration.



- Click **Add**.
- Provide the adapter with any name.
- Select the correct backend.

  The backend types map to the corresponding certificate types in SCM. The **SCM S/MIME** backend type is client certificates in SCM.
- Enter the **Back-end URL** as `https://cert-manager.com` and your customer URL extension for the **Back-end Customer URL Extension**. If you typically log into SCM using a URL such as `https://cert-manager/customer/ame`, then `ame` is your customer URL extension.
- Enter the login credentials for an administrator's account within SCM.

  To validate the URL and credentials, click **Test Connection**. The administrator role must have access to the organization or department configured in the attribute matching, as outlined in the table below.
- Click **Next** to move to the **Attribute Matching** page and set the attribute values.

  The list of available and required backend attributes differs depending on the selected backend. Required attributes are marked with a red asterisk. Some of the attributes are always populated with values from the request, whereas others are always configured using a default value. Values from the request are included in a drop-down list and always start with a dollar sign (`$`).

Attribute	Description
certType	The identifier of the certificate type to issue. To determine the correct value, contact Sectigo customer support. For the SCM Device backend, select the desired device certificate type and click **Edit** to view the details of the certificate type, with the **Type ID** listed as a numeric value. Enter that value in the **Default** column.

Attribute	Description
csr	Always enter `$csr` in the **Request Attributes** column and leave **Default** empty.
orgId	The identifier of the organization or department under which this certificate should be enrolled. Select an organization or department in SCM and click **Edit** to view the details of the organization or department, with the **OrgID** listed as numeric value. Enter that value in the **Default** column.
term	For SCM S/MIME and SCM SSL backends, this setting represents the length of time in days during which the certificate should be valid. For SCM Device backend, the term is configured as part of the certificate type and is not listed.
email	The email address that SCM saves with the certificate and includes in the certificate if the certificate type requires one. Enter `$csr.subject.e` in the **Request Attributes** column to use the value in the CSR.
firstName	The first name that SCM saves with the certificate and includes in the certificate if the certificate type requires one. Enter `$csr.subject.givenName` in the **Request Attributes** column to use the value in the CSR.
lastName	The last name that SCM saves with the certificate and includes in the certificate if the certificate type requires one. Enter `$csr.subject.surname` in the **Request Attributes** column to use the value in the CSR.
middleName	The middle name that SCM saves with the certificate and includes in the certificate if the certificate type requires one. Enter `$csr.subject.I` in the **Request Attributes** column to use the value in the CSR.
serverType	Always enter -1 in the **Default** column.
subjAltNames	List of subject alternative names to add to the certificate. Values are comma separated and are added as dNSName entries.
comments	The string that SCM saves with the certificate.
externalRequester	The string that SCM saves with the certificate to document the requester. Must be in `email@domain` format; multiple comma separated values are allowed.
numberServers	Leave empty.

- Click **Save** to create the adapter.

11.1.2 How to Create a Template

A template connects a URL to an adapter and controls who can request that particular certificate type.

You create a template as follows:

- Select the **Templates** tab.

- Click **Add**.
- Provide the template with any name.
- Optionally, select an alias for the template.

  The alias extends the EST enrollment URL in such a way that the complete URL is shown. The est-client-python library used later to perform test enrollments does not support an alias without an additional code described later. Other EST libraries might not support aliases in the enrollment URL.
- Select the adapter that you created following the instruction in section "How to Create an Adapter" on page 612.
- Make selections from the list of **Issuing Certificate Authorities** that you want to be returned to the client if it makes the `/cacerts` request.
- Select the required authentication method. If you select **By password**, enter the desired password; the user name is always `admin`.
- Select **Save** to create the template.

11.2 Testing Enrollments

The test enrollments described in this section are performed using est-client-python (see https://github.com/laurentluce/est-client-python) and depend on your operating system (OS).

11.2.1 How to Install Dependencies on Windows

On Windows OS, follow this procedure:

- Install OpenSSL.

  Multiple OpenSSL binary packages are available for Windows. One such package can be found at https://slproweb.com/products/Win32OpenSSL.html.
- Add OpenSSL bin folder to the `PATH` environment variable. The est-client-python library launches openssl processes to perform some tasks.
- Install Python 2.7.*n*.
- Install required Python packages:

```
python.exe -m pip install pyopenssl
python.exe -m pip install requests
```

- Download est-client-python library from https://github.com/laurentluce/est-client-python.

11.2.2 How to Install Dependencies on Linux

Most Linux distributions have OpenSSL and Python already installed. Follow this procedure to complete the installation:

- Install required Python packages:

```
python.exe -m pip install pyopenssl
python.exe -m pip install requests
```

- Download est-client-python library from https://github.com/laurentluce/est-client-python.

11.2.3 How to Perform Basic Validation

You can use the following sample Python code to validate that the EST service can be contacted. Before executing, replace all sample values with the correct values. If the validation is successful, CA certificates in PEM form are printed.

```
import sys
import time
# If this code doesn't live within the root folder of the est-client-python
folder,
# uncomment the following line and include the path
# sys.path.append(<path to est-client-python folder>)
import est.client

host = <instance_hostname>
port = 443

client = est.client.Client(host, port, None)
# The est-client-python library doens't support URL aliases to select a specific
template,
# comment these two lines out if testig with a template that doesn't specify an
alias
alias = <template_alias>
client.url_prefix = 'https://%s:%s/.well-known/est/%s' % (host, port, alias)

# Get EST server CA certs
ca_certs = client.cacerts()
print ca_certs
```

11.2.4 How to Perform Enrollment

You can add the following sample Python code after the initial setup code created when validating the basics to perform an enrollment. Before executing, replace all sample values with the correct values. If successful, the certificate in PEM form are printed.

```
client.set_basic_auth("admin",<template_password>)

common_name = 'enrollment_test'
email_address = 'enrollment_test@acme.com'
private_key, csr = client.create_csr(common_name, None, None, None, None, None,
email_address)

print csr

retry = True
while retry:
    try:
        client_cert = client.simpleenroll(csr)
        retry = False
    except est.errors.TryLater as ex:
        time.sleep(ex.seconds)

print client_cert
```

12

Using the Sectigo ACME Service

This chapter describes the Sectigo ACME service and provides information on the supported ACME clients.

This chapter describes the following topics:

- Sectigo ACME Service Overview
- ACME Clients Overview

12.1 Sectigo ACME Service Overview

The Automatic Certificate Management Environment (ACME) protocol is designed to automate interactions between web servers and CAs with the goal of providing automation for certificate installation, renewal, and domain validation. For more information, see https://tools.ietf.org/html/rfc8555.

Sectigo's implementation of the ACME protocol is known as Sectigo ACME service. It enables the following:

- SSL certificate enrollment through a third-party ACME client.

  All validation levels—DV, OV, and EV—are supported, as well as SDC, MDC, and WC certificate types (see "About Sectigo SSL Certificate Types and Validation Levels" on page 65).

  NOTE: Domains that are prevalidated in SCM are not issued validation challenges through ACME. Domains that are not prevalidated in SCM are subject to ACME validation challenges. Validation done through ACME does not change the **Validation Status** of domains in SCM.

- Re-issuance of existing SSL certificates with a new certificates to add or remove one or more domains.
- Automatic and manual renewal of SSL certificates.
- Visualization and revocation of SSL certificates via SCM, as described in "Managing SSL Certificates" on page 44, "Understanding the SCM Dashboard" on page 20, and "Generating SSL Certificates Reports" on page 585. This requires creation of an externally-bound account in SCM.

  For information on external account binding (EAB), see the ACME specification at https://tools.ietf.org/html/rfc8555#section-7.3.4.

  For information on SCM ACME accounts, see the following:

  - "How to Configure ACME Accounts for Organizations and Departments" on page 373
  - "Configuring Departments" on page 381

  The SSL certificates enrolled via the Sectigo ACME service are considered external in SCM. These certificates can be revoked from within SCM, as they have been issued by Sectigo CA.

12.2 ACME Clients Overview

ACME clients communicate with Sectigo ACME servers to request and manage certificates. Sectigo currently supports the Certbot client.

12.2.1 ACME Server URLs

The Sectigo ACME server URLs are as follows:

- https://acme.sectigo.com/v2/InCommonRSAOV
- https://acme.sectigo.com/V2/InCommonECCOV
- https://acme.sectigo.com/V2/EV

12.2.2 How to Use Certbot

Certbot enables enrollment, installation, and management of SSL certificates.

For information on the Certbot installation, navigate to https://certbot.eff.org/ and generate a list of instructions by selecting your server software and operating system.

Your experience using Certbot may differ depending on the server software, operating system, and Certbot plugins you have installed.

A complete list of Certbot commands can be found at https://certbot.eff.org/docs/using.html#certbot-command-line-options. The following table provides a subset of common Certbot commands.

Command		Description
`run`		Tells the authenticator plugin and a different installer plugin to initiate the acquisition and installation of a certificate.
	`--authenticator -a`	Specifies the authenticator plugin to be used.
	`--installer -i`	Specifies the installer plugin to be used.
`renew`		Renews all previously obtained certificates that are near expiry.
`--force-renewal`		Renews a certificate regardless of the remaining time until expiration.
`--expand`		Updates an existing certificate with a new certificate that includes one or more new domains.

Command	Description
`--non-interactive`	Runs the command line without requesting further user input. This may require the addition of other commands (such as `--agree-tos`).
`--agree-tos`	Indicates that you agree to the Sectigo ACME terms of service.
`--eab-kid`	Specifies the key identifier for external account binding. This is the EAB ID in an SCM ACME account.
`--eab-hmac-key`	Specifies the HMAC key for external account binding. This is the EAB Key in an SCM ACME account.
`--cert-name`	Specifies the name for returned certificate in your system.
`unregister`	Unregister a Sectigo ACME account. Once unregistered, the ACME account is deactivated on the ACME server and cannot be restored.

The following table provides sample command lines for performing various ACME tasks using Certbot.

NOTE: The following examples do not necessarily represent the command lines required in your specific environment.

Register Account
`certbot register --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonRSAOV --eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt- 5OjMEteSBISa7-fvWAWDyMpczV-nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw`
Obtain a DV Certificate
Apache authenticator
`certbot certonly --apache --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonRSAOV --eab-kidbxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV-nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name dv01`
NGINX authenticator

```
certbot certonly --apache --non-interactive --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonRSAOV --
eab-kidbxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-
fvWAWDyMpczV-nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --
cert-name dv01
```

Standalone authenticator

```
certbot certonly --standalone --non-interactive --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonRSAOV --
eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-
fvWAWDyMpczV-nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --
cert-name dv01
```

Obtain an OV Certificate

Apache authenticator

```
certbot certonly --apache --non-interactive --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonECCOV --
eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-
fvWAWDyMpczV-nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --
cert-name ov01
```

NGINX authenticator

```
certbot certonly --nginx --non-interactive --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonECCOV --
eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-
fvWAWDyMpczV-nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --
cert-name ov01
```

Standalone authenticator

```
certbot certonly --standalone --non-interactive --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonECCOV --
eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt- 5OjMEteSBISa7-
fvWAWDyMpczV-nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --
cert-name ov01
```

Obtain an EV Certificate

Apache authenticator

```
certbot certonly --apache --non-interactive --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/EV --eab-
kidbxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV-
nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name
ev01
```

NGINX authenticator

```
certbot certonly --nginx --non-interactive --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/EV --eab-
kidbxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV-
nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name
ev01
```

Standalone authentication

```
certbot certonly --standalone --non-interactive --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/EV --eab-kid
bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV-
nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name
dv01
```

Obtain and Install a Certificate

Apache authenticator/installer

```
certbot run --apache --non-interactive --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonRSAOV --
eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-
fvWAWDyMpczV-nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --
cert-name dv01
```

NGINX authenticator/installer

```
certbot run --nginx --non-interactive --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonRSAOV --
eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-
fvWAWDyMpczV-nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --
cert-name dv01
```

Obtain and Install a Certificate Using a Different Authenticator and Installer

Webroot authenticator / Apache installer

```
certbot run -a webroot -i apache -w /var/www/html --non-interactive --agree-tos --
email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonRSAOV
--eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-
fvWAWDyMpczV-nRXc7PkSMtuvW31YQlxA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --
cert-name dv01
```

Expand a Certificate to Include Further Domains (Apache)

```
certbot certonly --expand --apache -d scmexample.com,scmdomaintobeadded.com --agree-
tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/
InCommonRSAOV --eab-kid Ls3dE7b4vy_947D7MScwqg --eab-hmac-key
LT3_ebbI5bQ_dadLjdS86z_c4nevXcBg4T5Ci7CLqKpB3nLw6e8Y08VWacEeahHQXsb8KeRh2C2PoxHKwpL
uiQ
```

Force the Renewal of a Certificate (Apache)

```
certbot certonly --force-renewal --apache --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonRSAOV --
eab-kid Ls3dE7b4vy_947D7MScwqg --eab-hmac-key
LT3_ebbI5bQ_dadLjdS86z_c4nevXcBg4T5Ci7CLqKpB3nLw6e8Y08VWacEeahHQXsb8KeRh2C2PoxHKwpL
uiQ --domain scmexample.com
```

Duplicate an Existing Certificate (Apache)

```
certbot certonly --duplicate --apache --agree-tos --email
<CUSTOMER_EMAIL>@<DOMAIN.COM> --server https:acme.sectigo.net/v2/InCommonRSAOV --
eab-kid Ls3dE7b4vy_947D7MScwqg --eab-hmac-key
LT3_ebbI5bQ_dadLjdS86z_c4nevXcBg4T5Ci7CLqKpB3nLw6e8Y08VWacEeahHQXsb8KeRh2C2PoxHKwpL
uiQ --domain scmexample.com
```

Unregister an ACME Account

```
certbot unregister --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server
https:acme.sectigo.net/v2/InCommonRSAOV --domain scmexample.com --account
18f63f589759f00d14718ecf8325bba4
```

The following Certbot commands are not currently supported by the Sectigo ACME service:

- `--test-cert`
- `--staging`
- `revoke`

  NOTE: Certificate revocation is available through the SCM UI.

- `--must-staple`
- `--staple-ocsp`

13

Performing Miscellaneous Tasks

This chapter contains information on various miscellaneous tasks that can be preformed using SCM.

This chapter describes the following topics:

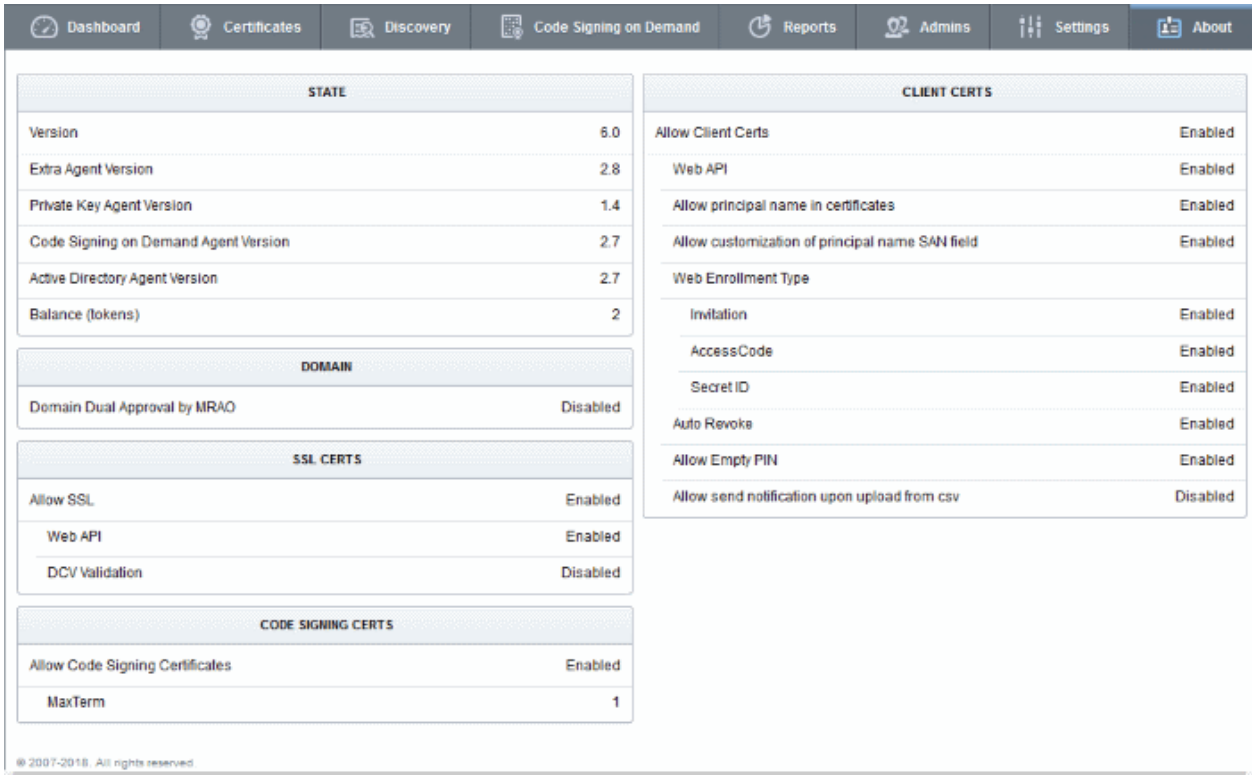
- Accessing the Product Version and Feature Details
- Accessing and Editing the User Profile
- Logging Out of SCM
- Deprecation of Private Certificates for Internal Hosts
- Responsibilities Associated with Ordering SSL Certificates
- Integrating IdP for Single Sign-On
- Troubleshooting SSO Connections

13.1 Accessing the Product Version and Feature Details

Depending on your security role, the **About** area of the main SCM UI shown in the following illustration allows you to view SCM version information, as well as features that have been enabled for your account.

MRAO administrators can see all features, whereas RAO and DRAO administrators can see features of the certificate types over which they have administrative rights.

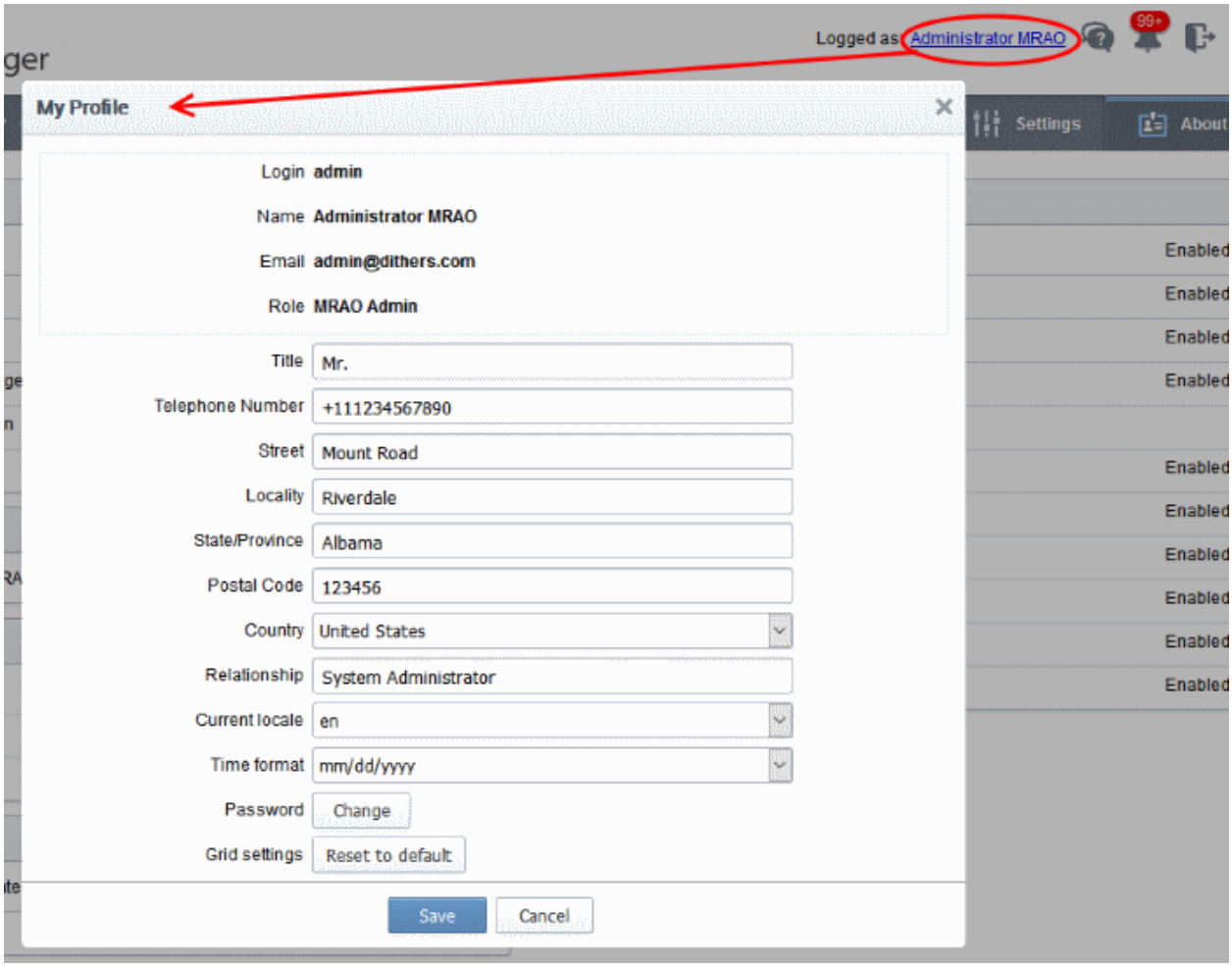
If any of the features are to be enabled or disabled, the MRAO administrator can contact Sectigo and request them.



13.2 Accessing and Editing the User Profile

The **My Profile** area shown in the following illustration contains a detailed summary for the administrator that is currently logged in to SCM. You can view your login name, your full name, the email address that is associated with your account, and your administrative role. In addition, you can view and edit the address details and preferences.

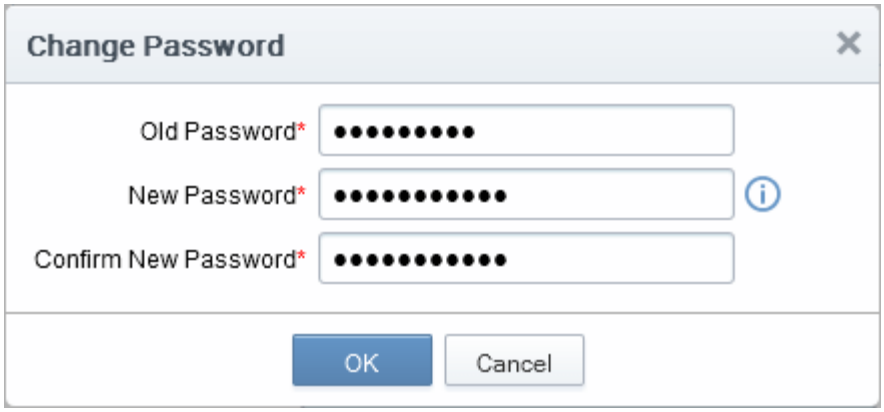
To access this area, click the user name link located beside **Logged as**, as shown in the following illustration.



This area also allows you to edit your address details, as well as preferences that include the following:

- Interface Language—SCM interface is available in multiple languages. The **Current locale** field enables you to change the interface language according to your preferences. The settings take effect when saved.
- Grid Settings—Click **Reset to default** to adjust the column widths and sorting preferences customized in various areas of SCM to default values.
- Date Format—Select mm/dd/yyyy or dd/mm/yyyy date format.

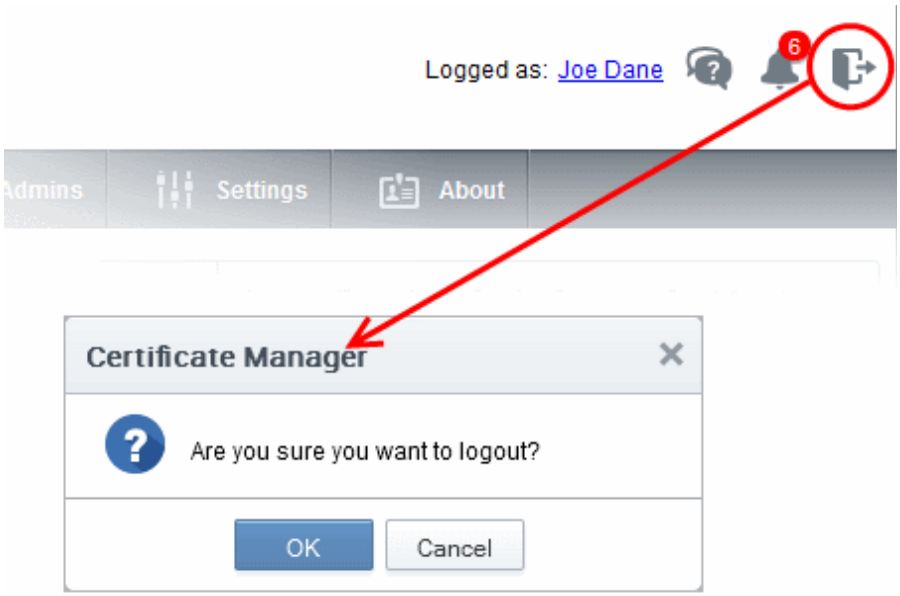
  Note that this only affects the way dates are represented in the SCM UI (for example, the Expires column of the SSL Certificates area. The manner in which dates are displayed in the certificates themselves is not affected (this is not modifiable and is set in the format of MM/dd/yy).
- Password—To change the administrator's password, click **Change** located next to **Password**, and then proceed with the password change using the **Change Password** dialog shown in the following illustration.



To view the password policy, hover over the **Information** icon.

13.3 Logging Out of SCM

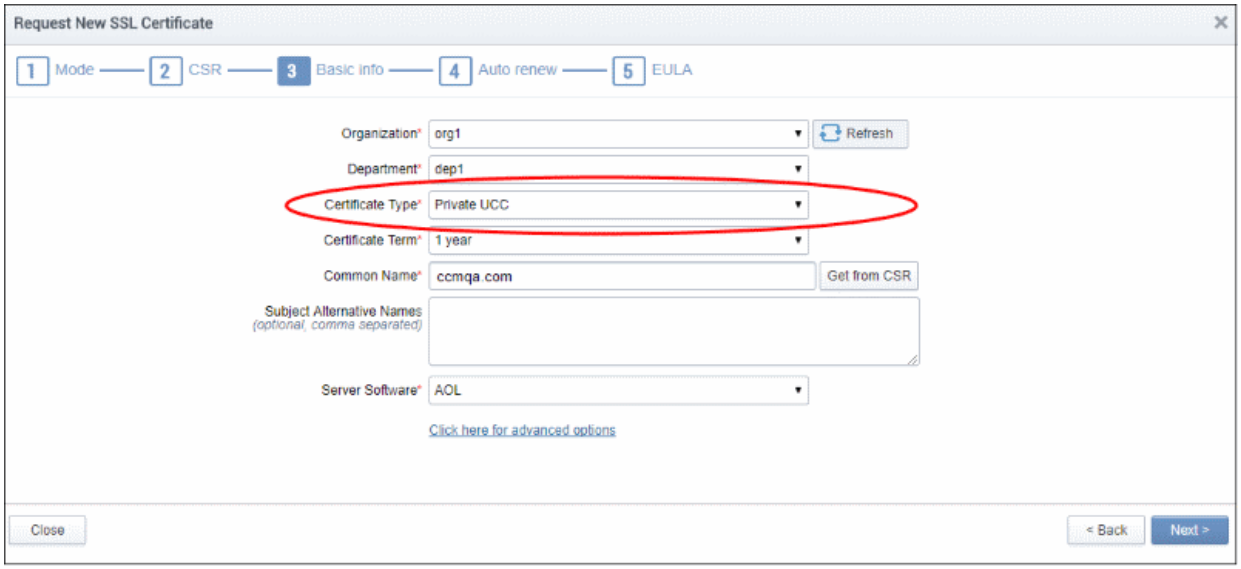
You can log out of SCM by clicking the **Logout** icon, as shown in the following illustration.



13.4 Deprecation of Private Certificates for Internal Hosts

Some companies use publicly trusted SSL certificates from a CA to secure internal hosts, reserved IP addresses, and intranets. However, after November 1, 2015 CA's are no longer able to issue publicly trusted certificates that contain internal names. All such certificates must have been revoked by November 1, 2016.

Companies that relied on these publicly trusted certificates for internal services risked service disruption, error messages, user confusion, and loss of security.



13.5 Responsibilities Associated with Ordering SSL Certificates

In order to make the certificate issuance process as fast and seamless as possible for immediate certificate issuance, the certificate manager account holder has a number of responsibilities, such as the following:

- You have the right to use the domain name contained in the SSL application. You must only approve applications for domain names you own.
- The named individual in the Corporate Secure Email Certificate is a bonafide employee or representative of your company.
- Making an illegitimate certificate application could affect your SCM account and the contract you signed with Sectigo. It could be a breach of the Certificate Manager Subscriber Agreement.

13.6 Integrating IdP for Single Sign-On

In order for SCM to securely connect to your IdP server, a communication channel needs to be established between the two via an exchange of meta data. For information on how to facilitate this exchange of meta data, contact your Sectigo account manager.

Once the communication channel is established, your IdP is added to SCM and associated with your account by your Sectigo account manager. You can choose from the following options:

- IdP login link on the SCM login page—Your SCM account login page contains an IdP login link. For more information, see "Organizations and Departments" on page 2.

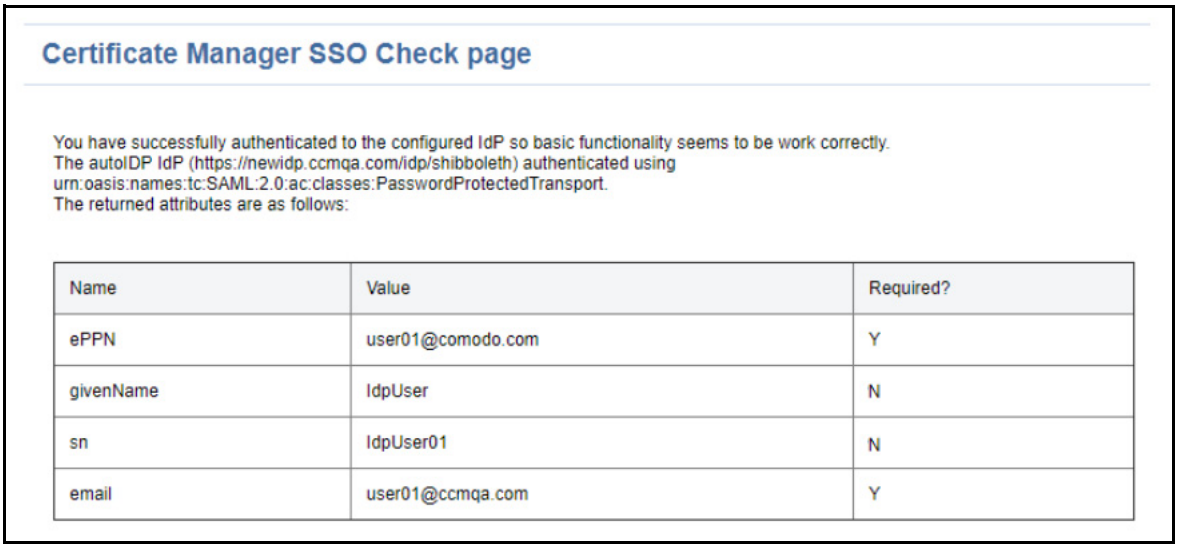
  If you do not want links displayed on your login page, a unique IdP login URL is provided by your Sectigo account manager. You can then communicate this URL to your administrators.
- Multi-factor Authentication—If required, multi-factor authentication (MFA) can be enabled for your account. In addition to an IdP user name and password, administrators need to authenticate themselves with a second factor authentication such as a One Time Password

(OTP) sent to their phone. If you decide to enable multi-factor authentication, you must specify the preferred mode for second factor authentication.

- Direct IdP Login—New users that log into SCM using their IdP credentials can be automatically assigned administrator permissions if you have created an IdP User Account Template. For more information, see "Creating IdP User Account Templates" on page 244.

13.7 Troubleshooting SSO Connections

The Certificate Manager SSO Check page is designed to show information about your IdP configuration and provide insight on where SSO may be failing. The **Certificate Manager SSO Check Page** is shown in the following illustration.



To troubleshoot your SSO connection, enter your company URI using one of the following URLs and navigate to the page in your web browser:

- `https://cert-manager.com/customer/<your_company_URI>/ssocheck`
- `https://hard.cert-manager.com/customer/<your_company_URI>/ssocheck`

Navigation to this page can produce multiple outcomes. The primary outcomes are as follows:

- No IdP Assigned: You have no assigned IdP.
- Multiple Assigned IdPs: You have more than one assigned IdP. Select the IdP you want to test and click **Check**.
- Authentication Failed: You were unable to connect with the IdP.
- Authentication Successful: You successfully connected to the IdP, and the following table is returned:

Any **Required** attributes that are returned with no **Value** indicate that your IdP is not returning the required attributes. This error could also be caused by incorrect mapping between your IdP and SCM's attribute names. These issues must be corrected before SSO is possible.

For further help troubleshooting SSO connections, contact your Sectigo account manager.

Appendix A Email Notification Templates

This appendix provides supplementary information for use when creating email notification templates.

This appendix describes the following topics:

- Email Template Variables

A.1 Email Template Variables

The following table provides descriptions of email notification template variables.

Variable	Description
Auto Renewal Failed	
commonName	The domain that was specified during the certificate request.
department	The department associated with the certificate request.
expires	The certificate expiry date.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization associated with the certificate request.
ownerEmail	The email address of the administrator who approved the certificate request.
ownerName	The name of the administrator who approved the certificate request.
requested	The date when the certificate was requested.
term	The validity period of the certificate, in days.
Certificate is ready for manual installation	
commonName	The domain that was specified during the certificate request.

Variable	Description
department	The department associated with the certificate request.
expires	The certificate expiry date.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization associated with the certificate request.
ownerEmail	The email address of the administrator who approved the certificate request.
ownerName	The name of the administrator who requested the automatic renewal of the certificate.
requested	The date when the certificate was requested.
term	The validity period of the certificate, in days.
Client Admin Created	
clientAdminCredentials	The credentials of the newly created administrator.
clientAdminEmail	The email address of the newly created administrator.
clientAdminLogin	The username of the newly created administrator.
clientAdminName	The name of the newly created administrator.
clientAdminRole	The highest role assigned to the newly created administrator.
creatorCredentials	The credentials of the administrator who created the new administrator account.
creatorEmail	The email address of the administrator who created the new administrator account.
creatorLogin	The username of the administrator who created the new administrator account.
creatorName	The name of the administrator who created the new administrator account.
notifyName	The name of the notification recipient.
Client Certificate Enrolled (DL)	
clientCertType	The client certificate type specified by the requester.
collected	The date that the certificate was collected by SCM from Sectigo.

Variable	Description
department	The department to which the end-user is assigned.
downloaded	The date the certificate was downloaded by the end-user or the administrator.
email	The email address of the certificate requester.
expires	The certificate expiry date.
name	The name of the certificate requester.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization to which the end-user is assigned.
requested	The date when the certificate was requested.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
term	The validity period of the certificate, in days.
watcher	The name of the subscriber who is receiving the notification.
Client Certificate Expiration	
department	The department to which the end-user is assigned.
expires	The certificate expiry date.
organization	The organization to which the end-user is assigned.
subject	The details (such as, Common Name, Organizational Unit, and Organization) contained in the **Subject** fields of the certificate.
Client Certificate Revoked (by admin)	
department	The department to which the end-user is assigned.
organization	The organization to which the end-user is assigned.
revoker	The administrator who revoked the certificate.
subject	The details (such as, Common Name, Organizational Unit, and Organization) contained in the **Subject** field of the certificate.
Client Certificate Revoked (by user)	
department	The department to which the end-user is assigned.

Variable	Description
organization	The organization to which the end-user is assigned.
revoker	The administrator who revoked the certificate.
subject	The details (such as, Common Name, Organizational Unit, and Organization) contained in the **Subject** field of the certificate.
Code Sign CSoD Revoked	
department	The department to which the end-user is assigned.
filesList	The list of files to be signed by the certificate.
organization	The organization to which the end-user is assigned.
serialNumber	The serial number on the certificate.
Code Sign Developer Created	
csRequestUrl	The URL for the code signing request portal.
email	The email address of the developer.
password	The developer's password for creating CSoD requests.
Code Sign Developer New Email	
csRequestUrl	The URL for the code signing request portal.
email	The email address of the developer.
password	The developer's password for creating CSoD requests.
Code Sign Developer Reset Password	
csRequestUrl	The URL for the code signing request portal.
email	The email address of the developer.
password	The developer's password for creating CSoD requests.
Code Sign Request Created	
email	The email address of the certificate requester.
filesList	The list of files to be signed by the certificate.
ver	The version number of the software.

Variable	Description
Code Sign Request Declined	
admin	The administrator who declined the certificate request.
declineDate	The date when the request was declined.
email	The email address of the certificate requester.
reason	The reason specified for why the request was declined.
Code Sign Request Signed	
email	The email address of the code requester.
filesList	The list of files to be signed by the certificate.
ver	The version number of the software.
Code Signing Certificate Downloaded	
collected	The date that the certificate was collected by SCM from Sectigo.
department	The department associated with the certificate request.
email	The email address of the certificate.
expires	The certificate expiry date.
name	The name of the certificate requester.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization associated with the certificate request.
requested	The date when the certificate was requested.
term	The validity period of the certificate, in days.
Code Signing Certificate Email Invitation	
department	The department associated with the certificate request.
email	The email address of the certificate requester.
link	The URL link used to validate the recipient's email.
name	The name of the certificate requester.

Variable	Description
organization	The organization associated with the certificate request.
requestCode	The request code.
Code Signing Certificate Enrolled (DL)	
collected	The date that the certificate was collected by SCM from Sectigo.
department	The department associated with the certificate request.
email	The email address of the certificate requester.
expires	The certificate expiry date.
name	The name of the certificate requester.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization associated with the certificate request.
requested	The date when the certificate was requested.
term	The validity period of the certificate, in days.
watcher	The name of the subscriber who is receiving the notification.
Code Signing Certificate Expired	
department	The department associated with the certificate request.
downloaded	The date the certificate was downloaded by the end-user or the administrator.
email	The email address of the certificate requester.
expires	The certificate expiry date.
name	The name of the certificate requester.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization associated with the certificate request.
requested	The date when the certificate was requested.
term	The validity period of the certificate, in days.
Code Signing Certificate Issued	

Variable	Description
collected	The date that the certificate was collected by SCM from Sectigo.
department	The department associated with the certificate request.
email	The email address of the certificate requester.
expires	The certificate expiry date.
link	The download link for the certificate.
name	The name of the certificate requester.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization associated with the certificate request.
requested	The date when the certificate was requested.
term	The validity period of the certificate, in days.
Code Signing Certificate Requested	
department	The department associated with the certificate request.
email	The email address of the certificate requester.
name	The name of the certificate requester.
organization	The organization associated with the certificate request.
requested	The date when the certificate was requested.
term	The validity period of the certificate, in days.
Code Signing Certificate Revoked	
department	The department associated with the certificate request.
downloaded	The date the certificate was downloaded by the end-user or the administrator.
email	The email address of the certificate requester.
expires	The certificate expiry date.
name	The name of the certificate requester.
orderNumber	The order number assigned by Sectigo for the certificate request.

Variable	Description
organization	The organization associated with the certificate request.
requested	The date when the certificate was requested.
revokerEmail	The email address of the administrator who revoked the certificate.
revokerName	The name of the administrator who revoked the certificate.
term	The validity period of the certificate, in days.
DCV Expiration	
domainNames	The list of domains nearing expiry.
expiredDays	The number of days until the listed domains expire.
DCV Needed-New Domain	
domainName	The name of the new domain that requires DCV.
DCV Validated	
domainName	The name of the domain that has passed DCV.
Device Certificate Approved	
DeviceType	The device certificate type specified by the requester.
commonName	The device name that was specified during the certificate request.
department	The department associated with the certificate request.
isTermYear	Returns 0 if the validity period is a multiple of 365.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization associated with the certificate request.
requested	The date when the certificate was requested.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
termYears	The validity period of the certificate, in years.
term	The validity period of the certificate, in days.
type	Indicates which action (approved or declined) was taken on the certificate.

Variable	Description
Device Certificate Awaiting Approval	
commonName	The device name that was specified during the certificate request.
department	The department associated with the certificate request.
organization	The organization associated with the certificate request.
Device Certificate Declined	
DeviceType	The device certificate type specified by the requester.
commonName	The device name that was specified during the certificate request.
department	The department associated with the certificate request.
isTermYear	Returns 0 if the validity period is a multiple of 365.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization associated with the certificate request.
requested	The date when the certificate was requested.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
termYears	The validity period of the certificate, in years.
term	The validity period of the certificate, in days.
type	Indicates which action (approved or declined) was taken on the certificate.
Device Certificate Enrolled	
DeviceCertType	The device certificate type specified by the requester.
commonName	The device name that was specified during the certificate request.
department	The department associated with the certificate request.
downloadUrl_PKCS7	The download URL (with description) for the certificate as PKCS#7, Base64.
downloadUrl_X509_All	The download URL (with description) for the certificate as X.509, Base64.

Variable	Description
downloadUrl_X509_Cert_Only	The download URL (with description) for the certificate as X.509, Base64.
downloadUrl_X509_Interm_Reverse	The download URL (with description) for the certificate as X.509, Base64, Intermediates/root only, Reverse.
downloadUrl_X509_Interm	The download URL (with descriptions) for the certificate as X.509, Base64, Intermediates/root only.
downloadUrls	All download URLs (with descriptions) for the certificate.
expires	The certificate expiry date.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The department associated with the certificate request.
requested	The date when the certificate was requested.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
term	The validity period of the certificate, in days.
Device Certificate Enrolled (DL)	
collected	The date that the certificate was collected by SCM from Sectigo.
commonName	The device name that was specified during the certificate request.
department	The department associated with the certificate request.
deviceCertType	The device certificate type specified by the requester
expires	The certificate expiry date.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization associated with the certificate request.
requested	The date when the certificate was requested.
requester	The certificate requester.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
term	The validity period of the certificate, in days.
watcher	The name of the subscriber who is receiving the notification.

Variable	Description
Device Certificate Expiration	
approver	The name of the administrator who approved the certificate request.
commonName	The device name that was specified during the certificate request.
department	The department associated with the certificate request.
expires	The certificate expiry date.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization associated with the certificate request.
requested	The date when the certificate was requested.
term	The validity period of the certificate, in days.
Device Certificate Revoked	
commonName	The device name that was specified during the certificate request.
department	The department associated with the certificate request.
expires	The certificate expiry date.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization associated with the certificate request.
requested	The date when the certificate was requested.
revokerEmail	The email address of the administrator who revoked the certificate.
revokerName	The name of the administrator who revoked the certificate.
term	The validity period of the certificate, in days.
Discovery Scan Summary	
completionStatus	The completion status of the discovery scan.
ended	The date of completion for the discovery scan.
foundComodoNew	The total number of new SCM certificates discovered.

Variable	Description
foundComodo	The total number of SCM certificates discovered.
foundNew	The total number of new certificates discovered.
foundOtherNew	The total number of new certificates discovered that were not requested through SCM.
foundOther	The total number of certificates discovered that were not requested through SCM.
foundSelfNew	The total number of new self-signed certificates discovered.
foundSelf	The total number of self-signed certificates discovered.
found	The total number of certificates found.
ipsScanned	The total number of IP addresses scanned.
scanType	Indicates which scan type (manual or scheduled) was specified for the discovery scan.
startedBy	The name of the requester who initiated the scan.
started	The date that the scan was initiated.
Domain Approved	
approvedDate	The date that the domain was approved.
department	The department associated with the new domain request.
domainName	The name of the new domain.
orgName	The name of the organization associated with the new domain request.
orgType	The organization type (organization or department) associated with the new domain request.
organization	The organization associated with the new domain request.
whois	The WHOIS information for the new domain.
Domain Awaiting Approval	
appRole	The role of the administrator who approved the domain delegation request.
approvedDate	The date that the domain was approved.

Variable	Description
approver	The name and email of the administrator who approved the domain delegation request.
createdDate	The date that the domain creation request was created.
department	The department associated with the new domain request.
domainName	The name of the new domain.
orgName	The name of the organization associated with the new domain request.
orgType	The organization type (organization or department) associated with the new domain request.
organization	The organization associated with the new domain request.
reqEmail	The email of the administrator who created the domain delegation request.
reqName	The name of the administrator who created the domain delegation request.
reqRole	The role of the administrator who created the domain delegation request.
requester	The name and email of the requester who created the domain delegation request.
whois	The WHOIS information for the new domain.
Email Invitation	
name	The name of the email recipient.
requestCode	The request code.
url	The URL link used to validate the recipient's email.
Email Validation	
name	The name of the email recipient.
requestCode	The request code.
url	The URL link used to validate the recipient's email.
IdP Login Invitation	
name	The name of the email recipient.

Variable	Description
url	The URL link of the IdP login page.
SSL Approved	
SSLType	The SSL certificate type specified by the requester.
approved	The date that the certificate request was approved.
comments	The comments included in the certificate when it was requested.
commonName	The domain that was specified during the certificate request.
department	The department for which the certificate was requested.
expires	The certificate expiry date.
isTermYear	Returns 0 if the validity period is a multiple of 365.
message	A message included by the administrator who approved the certificate request.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization for which the certificate was requested.
requested	The date when the certificate was requested.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
serverType	The server type for which the certificate was requested.
servers	The server numbers of the certificate.
subjectAlternativeNames	The list of subject alternative names included in the certificate.
termYears	The validity period of the certificate, in years.
term	The validity period of the certificate, in days.
type	Indicates which action (approved or declined) was taken on the certificate.
SSL Awaiting Approval	
SSLType	The SSL certificate type specified by the requester.
approved	The date that the certificate request was approved.

Variable	Description
comments	The comments included in the certificate when it was requested.
commonName	The domain that was specified during the certificate request.
department	The department for which the certificate was requested.
expires	The certificate expiry date.
isTermYear	Returns 0 if the validity period is a multiple of 365.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization for which the certificate was requested.
requested	The date when the certificate was requested.
requesterEmail	The email address of the certificate requester.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
serverType	The server type for which the certificate was requested.
servers	The server numbers of the certificate.
subjectAlternativeNames	The list of subject alternative names included in the certificate.
termYears	The validity period of the certificate, in years.
term	The validity period of the certificate, in days.
SSL Certificate Remote Installation Failed	
SSLType	The SSL certificate type specified by the requester.
approved	The date that the certificate request was approved.
approverEmail	The email of the administrator who approved the certificate request.
approverName	The name of the administrator who approved the certificate request.
comments	The comments included in the certificate when it was requested.
commonName	The domain that was specified during the certificate request.
csr	The content of the certificate signing request.

Variable	Description
CustomerName	The name of the customer.
department	The department for which the certificate was requested.
expires	The certificate expiry date.
IsCmCert	Indicates whether the certificate was enrolled through SCM.
message	An error message indicating why the certificate installation failed.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization for which the certificate was requested.
requested	The date when the certificate was requested.
requesterEmail	The email address of the certificate requester.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
serverType	The server type for which the certificate was requested.
servers	The server numbers of the certificate.
subjectAlternativeNames	The list of subject alternative names included in the certificate.
term	The validity period of the certificate, in days.
SSL Certificate Installed Remotely	
SSLType	The SSL certificate type specified by the requester.
approved	The date that the certificate request was approved.
comments	The comments included in the certificate when it was requested.
commonName	The domain that was specified during the certificate request.
department	The department for which the certificate was requested.
expires	The certificate expiry date.
isCmCert	Indicates whether the certificate was enrolled through SCM.
orderNumber	The order number assigned by Sectigo for the certificate request.

Variable	Description
organization	The organization for which the certificate was requested.
requested	The date when the certificate was requested.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
serverType	The server type for which the certificate was requested.
servers	The server numbers of the certificate.
subjectAlternativeNames	The list of subject alternative names included in the certificate.
term	The validity period of the certificate, in days.
SSL Declined	
SSLType	The SSL certificate type specified by the requester.
approved	The date that the certificate request was approved.
comments	The comments included in the certificate when it was requested.
commonName	The domain that was specified during the certificate request.
department	The department for which the certificate was requested.
expires	The certificate expiry date.
isTermYear	Returns 0 if the validity period is a multiple of 365.
message	A message included by the administrator who declined the certificate request.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization for which the certificate was requested.
requested	The date when the certificate was requested.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
serverType	The server type for which the certificate was requested.
servers	The server numbers of the certificate.
subjectAlternativeNames	The list of subject alternative names included in the certificate.

Variable	Description
termYears	The validity period of the certificate, in years.
term	The validity period of the certificate, in days.
type	Indicates which action (approved or declined) was taken on the certificate.
SSL Enrolled	
SSLType	The SSL certificate type specified by the requester.
approved	The date that the certificate request was approved.
comments	The comments included in the certificate when it was requested.
commonName	The domain that was specified during the certificate request.
department	The department for which the certificate was requested.
downloadURL	All download URLs (with descriptions) for the certificate.
downloadUrlPEMCO	The download URL (with description) for the certificate only, PEM encoded (filename.pem).
downloadUrlPEM	The download URL (with description) for the certificate (with chain), PEM encoded (filename.pem).
downloadUrlPKCS7PEM	The download URL (with description) for the certificate as PKCS#7, PEM encoded.
downloadUrlPKCS7	The download URL (with description) for the certificate as PKCS#7.
downloadUrlX509CO	The download URL (with description) for the certificate only, PEM encoded (filename.cer).
downloadUrlX509IOR	The download URL for the CA's certificate as Intermediate(s)/ Root only.
downloadUrlX509IO	The download URL for the CA's certificate as Intermediate(s)/ Root only.
downloadUrlX509	The download URL (with description) for the certificate (with chain), PEM encoded (filename.cer).
Expires	The certificate expiry date.
isTermYear	Returns 0 if the validity period is a multiple of 365.
orderNumber	The order number assigned by Sectigo for the certificate request.

Variable	Description
organization	The organization for which the certificate was requested.
renewID	The renew ID of the certificate.
requested	The date when the certificate was requested.
selfEnrolCertID	The unique enrollment ID assigned to the certificate request.
serverType	The server type for which the certificate was requested.
servers	The server numbers of the certificate.
subjectAlternativeNames	The list of subject alternative names included in the certificate.
termYears	The validity period of the certificate, in years.
term	The validity period of the certificate, in days.
SSL Enrolled (DL)	
SSLType	The SSL certificate type specified by the requester.
approved	The date that the certificate request was approved.
collected	The date that the certificate was collected by SCM from Sectigo.
comments	The comments included in the certificate when it was requested.
commonName	The domain that was specified during the certificate request.
department	The department for which the certificate was requested.
expires	The certificate expiry date.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization for which the certificate was requested.
renewID	The renew ID of the certificate.
requested	The date when the certificate was requested.
requester	The certificate requester.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
serverType	The server type for which the certificate was requested.

Variable	Description
servers	The server numbers of the certificate.
subjectAlternativeNames	The list of subject alternative names included in the certificate.
term	The validity period of the certificate, in days.
watcher	The name of the subscriber who is receiving the notification.
SSL Expiration	
SSLType	The SSL certificate type specified by the requester.
approved	The date that the certificate request was approved.
approver	The name of the administrator who approved the certificate request.
comments	The comments included in the certificate when it was requested.
commonName	The domain that was specified during the certificate request.
department	The department for which the certificate was requested.
expires	The certificate expiry date.
isCmCert	Indicates whether the certificate was enrolled through SCM.
isTermYear	Returns 0 if the validity period is a multiple of 365.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization for which the certificate was requested.
requested	The date when the certificate was requested.
requester	The certificate requester.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
serverType	The server type for which the certificate was requested.
servers	The server numbers of the certificate.
subjectAlternativeNames	The list of subject alternative names included in the certificate.
termYears	The validity period of the certificate, in years.

Variable	Description
term	The validity period of the certificate, in days.
SSL Issuance Failed	
SSLType	The SSL certificate type specified by the requester.
approved	The date that the certificate request was approved.
approverEmail	The email of the administrator who approved the certificate request.
approverName	The name of the administrator who approved the certificate request.
comments	The comments included in the certificate when it was requested.
commonName	The domain that was specified during the certificate request.
csr	The content of the certificate signing request.
department	The department for which the certificate was requested.
expires	The certificate expiry date.
isCmCert	Indicates whether the certificate was enrolled through SCM.
isTermYear	Returns 0 if the validity period is a multiple of 365.
message	An error message indicating why the certificate issuance failed.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization for which the certificate was requested.
requested	The date when the certificate was requested.
requesterEmail	The email address of the certificate requester.
seelfEnrollCertID	The unique enrollment ID assigned to the certificate request.
serverType	The server type for which the certificate was requested.
servers	The server numbers of the certificate.
subjectAlternativeNames	The list of subject alternative names included in the certificate.
termYears	The validity period of the certificate, in years.

Variable	Description
term	The validity period of the certificate, in days.
SSL Revoked (by admin)	
SSLType	The SSL certificate type specified by the requester.
adminEmail	The email of the administrator who revoked the certificate.
adminName	The name of the administrator who revoked the certificate.
approved	The date that the certificate request was approved.
comments	The comments included in the certificate when it was requested.
commonName	The domain that was specified during the certificate request.
department	The department for which the certificate was requested.
expires	The certificate expiry date.
isCmCert	Indicates whether the certificate was enrolled through SCM.
isTermYear	Returns 0 if the validity period is a multiple of 365.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization for which the certificate was requested.
requested	The date when the certificate was requested.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
serverType	The server type for which the certificate was requested.
servers	The server numbers of the certificate.
subjectAlternativeNames	The list of subject alternative names included in the certificate.
termYears	The validity period of the certificates, in years.
term	The validity period of the certificates, in days.
SSL Revoked (by user)	
SSLType	The SSL certificate type specified by the requester.
approved	The date that the certificate request was approved.

Variable	Description
comments	The comments included in the certificate when it was requested.
commonName	The domain that specified during the certificate request.
department	The department for which the certificate was requested.
expires	The certificate expiry date.
isTermYear	Returns 0 if the validity period is a multiple of 365.
orderNumber	The order number assigned by Sectigo for the certificate request.
organization	The organization for which the certificate was requested.
requested	The date when the certificate was requested.
requesterEmail	The email address of the certificate requester.
selfEnrollCertID	The unique enrollment ID assigned to the certificate request.
serverType	The server type for which the certificate was requested.
servers	The server numbers of the certificate.
subjectAlternativeNames	The list of subject alternative names included in the certificate.
termYears	The validity period of the certificate, in years.
term	The validity period of the certificate, in days.

Appendix B CSV Import Format Requirements

This appendix provides supplementary information for use when creating email notification templates.

This appendix describes the following topics:

- Network Discovery Task CSV File Format
- End-User CSV File Format and Importing Guidelines
- Code Signing Certificate CSV File Format and Importing Guidelines

B.1 Network Discovery Task CSV File Format

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

Column	Field	Description
A	Task Name	The name to be displayed for this network discovery task in SCM.
B	Agent Name [a]	The name of the agent that is to be used. If left empty, an agent is automatically assigned based on the ranges specified in the **Scan Ranges** column.
C	Scan Ranges	The IP or IP range to be scanned. Ranges can be specified using a hyphen and can include a host name. CIDR format is supported.
D	Ports	The ports to be scanned. Multiple ports can be included using a comma-separated list enclosed in quotations (“233, 235, 255”). Port ranges can also be specified using a hyphen.
E	Assignment Rule	The assignment rule to be applied to certificates discovered using this network discovery task.

Column	Field	Description
F	Schedule	The times when this network discovery task is to be run. The supported values are: Manual, Once, Daily, Weekly, Monthly, Quarterly, SemiAnnually, Annually. Tasks are scheduled for one minute following the upload of the CSV file and all tasks other than Manual and Daily are run on Sundays. You can also indicate a time zone by adding / followed by your UTC timezone.

a. You must have at least one agent configured to interact with your required scan ranges. For more information on configuring a network agent, see "Configuring Network Agents" on page 252.

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

	A	B	C	D	E	F
1	Example Task Name	Agent Advanced 105	10.10.10.120/32	443	Assignment Rule 1	Monthly/UTC+09:00
2	Example Task Name 2	auto	10.10.10.121	443	Assignment Rule 1	Daily
3						

B.1.1 Adding Multiple Assignment Rules

You can add multiple assignment rules to a single network discovery task by creating a baseline discovery task, and then creating subsequent rows with a new **Assignment Rule** and increasing **Scan Ranges**. You must specify the same **Task Name**, **Agent Name**, **Ports**, and **Schedule** for the newly added rows.

For example, the following `.csv` file creates a new network discovery task.

	A	B	C	D	E	F	G
1	Discovery Task 1	auto	10.10.10.120	443	Assignment Rule 1	Manual	
2	Discovery Task 1	auto	10.10.10.120-10.10.10.121	443	Assignment Rule 2	Manual	
3	Discovery Task 1	auto	10.10.10.120-10.10.10.122	443	Assignment Rule 3	Manual	
4							

The discovery task was created using the following properties:

- Task Name: Discovery Task 1
- Agent: Auto
- Scan Range: 10.10.10.120-10.10.10.122

  Even though the same **Scan Range** was specified multiple times, SCM only scans the total range once.
- Ports: 443
- Assignment Rules: Assignment Rule 1, Assignment Rule 2, Assignment Rule 3
- Schedule: Manual

B.2 End-User CSV File Format and Importing Guidelines

The fields per-user in the CSV file differ depending on whether or not principal name support is enabled for the organization. For more information about the principal name, see "Using the Client Certificate Area of the Add New Organization Dialog" on page 336.

The following table lists fields, with their possible values and formats, that can be imported from the CSV file for each end-user. For organizations for which the principal name support is enabled, the **Principal Name** field is available. For organizations for which the principal name support is not enabled, the **Principal Name** field is not available.

Out of the fields that must be included in each entry, six fields are mandatory and one field (Department) is mandatory only if multiple end-users are being imported by a DRAO Client Certificate; MRAO, RAO Client Certificate, as well as DRAO Client Certificate administrators that are also MRAO or RAO Client Certificate administrators, can leave this field blank. Optional fields without values must also be included but left blank.

The **Secret ID** field can be used to add a layer of authentication to the process. If specified, the end-user has to enter the identifier in the certificate enrollment form.

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

Field	Required	Minimum Characters	Maximum Characters	Format	Supported Characters
First Name	Yes	1	128		A-Z a-z 0-9 . - space
Middle Name	No	0	128		A-Z a-z 0-9 . - space
Last Name	Yes	1	128		A-Z a-z 0-9 . - space

Field	Required	Minimum Characters	Maximum Characters	Format	Supported Characters
Email (Primary)	Yes	3	128		A-Z a-z 0-9 . - _
Email (Alternative)	Yes	3	128	Valid email address	A-Z a-z 0-9 . - _
Validation Type	No			Valid email addresses separated by a space	high empty standard
Organization	Yes	1	128		Any
Department	No	0	128		Any
Secret ID	No	0	128		Any
Phone	No	0	128		Any
Country	Yes	2	2	Valid two-letter country code	A-Z a-z
Principal Name	No	1	128		Any

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

"First1","Middle1","Last1","User----1-al@abc.com","User1-sec-al@abc.com","standard","System","sysdep,"Secret1",380487000001,"UA","User1-al@abc.com"

NOTE: If an organization is enabled for the principal name support and a department belonging to the organization is not enabled for the principal name support, when loading end-users of the department, the Principal Name field must be included but should be left blank. You can check if an organization or department is enabled for the principal name support from the main SCM Settings UI by either (1) navigating to Settings > Organizations, clicking Edit for the respective organization, and then clicking Client Certificate or (2) navigating to Settings > Organizations > Department of the respective organization, clicking Edit for the respective department, and then clicking Client Certificate.

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

"First1","Middle1","Last1","User----1-al@abc.com","User1-secal@abc.com","stadard","System","sysdep,"Secret1",380487000001,"UA",

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

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

B.3 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

Field	Required	Minimum Characters	Maximum Characters	Format	Supported Characters
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 C Sectigo Root and Intermediate Certificates

This appendix provides supplementary information for use when importing Sectigo Root and Intermediate Certificates.

This appendix describes the following topics:

- Sectigo Root and Intermediate Certificate(s)
- Importing the Sectigo Root Certificate
- Importing the Sectigo Intermediate Certificate

C.1 Sectigo Root and Intermediate Certificate(s)

For SCM certificates to be trusted internally, the Root and Intermediate CA certificate(s) 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.

C.2 Importing the Sectigo Root Certificate

The following steps outline importing the Sectigo Root certificate into the Trust Root Certification Authority certificate store in Active Directory. In order to perform these steps you must be a Domain Administrator with access to the system where Active Directory is installed.

To import the Sectigo Root certificate, do the following:

1. Log on as an administrator to the Windows system where Active Directory is installed.
2. Navigate to **Windows Control Panel > Administrative Tools > Group Policy Management**.
3. In the **Group Policy Management** window, expand **(your domain name) > Domains > (your domain name)**.
4. Right click **Default Domain Policy** and select **Edit**.
5. In the **Group Policy Management Editor** window, expand **Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities**.
6. Right click on **Trusted Root Certification Authorities** and select **Import**.

7. On the **Welcome to the Certificate Import Wizard** window, click **Next**.
8. On the **File to Import** window, click **Browse**.
9. Locate and select the **Sectigo Root Certificate** that will be imported.
10. Click **Next**.
11. In the **Certificate Store**, select **Place all certificates to the following store** and set the **Certificate store** to **Trusted Root Certification Authorities**.
12. Click **Next > Finish > OK**.

C.3 Importing the Sectigo Intermediate Certificate

The following steps outline importing the Sectigo Intermediate Certificate into the Intermediate Certificate Authority certificate store in Active Directory. In order to perform these steps you must be a Domain Administrator with access to the system where Active Directory is installed.

To import the Sectigo Intermediate certificate, do the following:

1. Log on as an administrator to the Windows system where Active Directory is installed.
2. Navigate to **Windows Control Panel > Administrative Tools > Group Policy Management**.
3. In the **Group Policy Management** window, expand **(domain name) > Domains > (domain name)**.
4. Right click on **Default Domain Policy** and select **Edit**.
5. Right click on **Intermediate Certification Authorities** and select **Import**.
6. On the **Welcome to the Certificate Import Wizard** window, click **Next**.
7. On the **File to Import** window, click **Browse**.
8. Locate and select the **Sectigo Intermediate Certificate** that will be imported.
9. Click **Next**.
10. In the **Certificate Store**, select **Place all certificates to the following store** and set the **Certificate store** to **Intermediate Certification Authorities**.
11. Click **Next > Finish > OK**.