COMODO
Creating Trust Online®

Comodo
Certificate Manager
Software Version 4.6

MRAO Administrator Guide
Guide Version 4.6.063014

Comodo CA Limited,
3rd Floor, 26 Office Village, Exchange Quay,
Trafford Road, Salford,
Greater Manchester M5 3EQ,
United Kingdom.

Table of Contents

1 Introduction to Comodo Certificate Manager 9
1.1 Guide Structure 9
1.2 Definitions of Terms 10
1.2.1 Organizations and Departments 10
1.2.2 Certificate Types 10
1.2.3 Administrative Roles 10
1.2.4 Security Roles - Comparative Table 19
1.2.5 Multiple Security Roles 23
1.2.6 Organizations and Departments 23
1.2.7 Reports 24
1.3 Logging into Your Account 25
1.4 The Main Interface - Summary of Areas 26
1.5 Release Notes 33
2 The Dashboard 37
3 Certificates Management 44
3.1 SSL Certificates Area 45
3.1.1 Overview of the Interface 45
3.1.1.1 Sorting and Filtering Options 49
3.1.1.2 SSL Certificate 'Details' Dialog 52
3.1.1.2.1 Resending Notification Email for Certs with 'Issued' State 54
3.1.1.2.2 Viewing Installation Details of Certificates 54
3.1.1.2.3 Restarting Apache after Auto-Installation of SSL Certificate 55
3.1.1.3 Comodo SSL Certificates 56
3.1.1.3.1 Definition of Terms 56
3.1.2 Request and Issuance of SSL Certificates to Web Servers and Hosts 57
3.1.2.1 Prerequisites 57
3.1.2.2 Automatic Installation and Renewal 58
3.1.2.2.1 Method 1 - Enterprise Controller Mode 59
3.1.2.2.2 Method 2 - CCM Controller Mode 71
3.1.2.3 Initiating SSL Enrollment using Application Forms 80
3.1.2.3.1 Method 1 - Self Enrollment Form 81
3.1.2.3.1.1 Initiating the Self Enrollment Process 81
3.1.2.3.1.2 The Self Enrollment Form 81
3.1.2.3.1.3 Form Parameters 84
3.1.2.3.2 Method 2 - Built-in Enrollment Form 89
3.1.2.3.2.1 Accessing the Built-in Application Form 89
3.1.2.3.2.2 The Built-In Application Form 89
3.1.2.3.2.3 Form Parameters 90
3.1.2.3.3 Certificate Collection 94
3.1.2.3.3.1 Collection of SSL Certificate Through Email 94
3.1.2.3.3.2 Collection of SSL certificate by Administrator 95
3.1.2.3.4 Downloading and Importing SSL Certificates 96
3.1.2.4 Certificate Requests - Approving, Declining, Viewing and Editing 96
3.1.2.5 Certificate Renewal 98
3.1.2.5.1 Certificate Renewal by Administrators 98

3.1.2.5.2 Certificate Renewal by the End-User....100
3.1.2.6 Certificate Revocation, Replacement and Deletion....101
3.2 The Client Certificates Area....102
3.2.1 Overview....102
3.2.1.1 Sorting and Filtering Options....103
3.2.1.2 'Certs' Dialog....104
3.2.2 Adding Cert End-Users....107
3.2.2.1 Manually Adding End-Users....107
3.2.2.1.1 'Add New Person' form - Table of Parameters....108
3.2.2.2 Loading Multiple End-Users from a Comma Separated Values (.csv) File....109
3.2.2.2.1 Procedure Overview....109
3.2.2.2.2 Requirements for .csv file....109
3.2.2.2.2.1 For Organizations with Principal Name Support Enabled....110
3.2.2.2.2.2 For Organizations without Principal Name Support....111
3.2.2.2.3 General Rules....112
3.2.2.2.4 The Import Process....112
3.2.2.2.5 Errors in .csv file....114
3.2.2.3 Auto Creation of End-Users via Certificate Self Enrollment Form....114
3.2.3 Editing End-Users....114
3.2.4 Deleting an End-User....116
3.2.5 Request and Issuance of Client Certificates to Employees and End-Users....116
3.2.5.1 Self Enrollment by Access Code....116
3.2.5.1.1 Prerequisites....116
3.2.5.1.2 Procedure Overview....117
3.2.5.1.3 Initiating the Enrollment Process....118
3.2.5.1.3.1 The Access Code Based Self Enrollment Form....118
3.2.5.1.3.2 Form Parameters....119
3.2.5.1.4 Validation of the Application....120
3.2.5.1.5 Certificate Collection....123
3.2.5.2 Self Enrollment by Secret Identifier....123
3.2.5.2.1 Prerequisites....124
3.2.5.2.2 Procedure Overview....125
3.2.5.2.3 Initiating the Enrollment Process....125
3.2.5.2.3.1 Secret Identifier Based Self Enrollment Form....125
3.2.5.2.3.2 Form Parameters....127
3.2.5.2.4 Certificate Collection....127
3.2.5.3 Enrollment by Invitation....128
3.2.5.3.1 Prerequisites....128
3.2.5.3.2 Procedure Overview....128
3.2.5.3.3 Initiating the Enrollment Process....129
3.2.5.3.4 Validation of the Email Address....130
3.2.5.3.5 Certificate Collection....132
3.2.6 Revocation of Client Certificates....133
3.2.6.1 Revocation of Client Certificates by End-Users....133
3.2.6.1.1 Procedure Overview....133
3.2.6.1.2 Revocation form....134

3.2.6.1.3 Form Parameters....134
3.2.7 Viewing End-User's Certificate....134
3.3 The Code Sign Certificates Area....136
3.3.1 Sorting and Filtering Options....138
3.3.2 Code Sign Certificates View Dialog....139
3.3.3 Adding Certificates to be Managed....141
3.3.3.1 Manually Adding Certificates....141
3.3.3.2 Loading Multiple Certificates from a Comma Separated Values (.csv) File....142
3.3.3.2.1 Procedure Overview....142
3.3.3.2.2 Requirements for .csv file....142
3.3.3.3 Auto Creation of End-Users by Initiating Self Enrollment....143
3.3.4 Request and Issuance of Code Signing Certificates....143
3.3.4.1 Prerequisites....143
3.3.4.2 Procedure Overview....144
3.3.4.3 Initiating the Enrollment Process....144
3.3.4.4 Validation of Email address and Requisition....146
3.3.4.5 Downloading and Installing the Certificate....148
4 Admin Management....148
4.1 Section Overview....148
4.1.1 Sorting and Filtering Options....151
4.2 Adding Administrators....152
4.2.1 'Add New Client Admin' form - Table of Parameters....154
4.2.2 Example: Adding a New Administrator with multiple privileges....156
4.2.2.1 The 'Certificate auth' Field....158
4.3 Editing Administrators....159
4.4 Deleting an Administrator....161
5 Settings....161
5.1 Overview....161
5.2 Organizations....162
5.2.1 Section Overview....162
5.2.1.1 Example Scenarios....163
5.2.2 Organization Management....165
5.2.2.1 Organizations Area Overview....165
5.2.2.2 Summary of Fields and Controls....166
5.2.2.3 Sorting and Filtering Options....167
5.2.2.4 Creating a New Organization....168
5.2.2.4.1 General Settings....169
5.2.2.4.2 General Settings - Table of Parameters....170
5.2.2.4.3 EV Details Tab....171
5.2.2.4.4 EV Details - Table of Parameters....171
5.2.2.4.5 Client Cert Settings Tab....173
5.2.2.4.6 Client Cert Settings - Table of Parameters....173
5.2.2.4.6.1 Customize an Organization's Client Certificate Types....175
5.2.2.4.6.2 Defining Key Usage Template for an Organization's Client Certificates....177
5.2.2.4.7 SSL Certificates Settings Tab....179
5.2.2.4.8 SSL Certificates - Table of Parameters....180

5.2.2.4.8.1 Customize an Organization's SSL Certificate Types....182
5.2.2.4.8.2 Customize an Organization's Server Software Types....184
5.2.2.4.9 'Code Signing Certificates' Settings tab....186
5.2.2.4.10 Code signing Certificates - Table of Parameters....186
5.2.2.5 Editing an Existing Organization....186
5.2.2.5.1 Imposing Access Restrictions to CCM interface....187
5.2.2.6 Validating an Organization....189
5.2.2.7 Managing the Departments of an Organization....190
5.2.2.7.1 Departments Dialog - Table of Parameters....191
5.2.2.7.2 Sorting and Filtering Options....192
5.2.2.7.3 Creating Departments....193
5.2.2.7.4 Editing Departments belonging to an Organization....195
5.2.2.7.5 Managing Domains Belonging to a Department....195
5.2.2.7.6 Deleting an Existing Department....196
5.2.2.8 Managing the Domains of an Organization....196
5.2.2.9 Deleting an Existing Organization....197
5.3 Departments....197
5.4 Domains....198
5.4.1 Section Overview....198
5.4.1.1 Wildcard Domains....199
5.4.2 Domain Management....199
5.4.2.1 The Domains Area....199
5.4.2.1.1 Domain Delegations....200
5.4.2.1.1.1 Summary of Fields and Controls....200
5.4.2.1.1.2 Sorting and Filtering Options....201
5.4.2.1.1.3 Tool Tip....203
5.4.2.1.2 DCV....203
5.4.2.1.2.1 Summary of Fields and Controls....204
5.4.2.1.2.2 Sorting and Filtering Options....204
5.4.2.2 Creating a New Domain....206
5.4.2.2.1 Create Domain - Table of Parameters....207
5.4.2.2.2 Validating the Domain....207
5.4.2.2.2.1 Changing DCV method for Validation Pending Domains....211
5.4.2.3 Delegating/Re-delegating an Existing Domain....211
5.4.2.4 Viewing, Validating and Approving Newly Created Domains....212
5.4.2.4.1 View Domain - Summary of Fields and Controls....213
5.4.2.4.2 Approval of Creation and Delegation of Domains....214
5.4.2.4.3 Viewing Requisition and Approval Details of a Domain....214
5.4.2.4.4 Request Details - Table of Parameters....215
5.5 Notifications....216
5.5.1 Adding a Notification....219
5.5.2 Notification Types....221
5.5.2.1 'Client Certificate Expiration' Create Notification Form....221
5.5.2.1.1 Table of Parameters....222
5.5.2.2 'Client Certificate Revoked' Create Notification Form....223
5.5.2.2.1 Table of Parameters....223

5.5.2.3 'Code Signing Certificate Downloaded' Create Notification Form....224
5.5.2.3.1 Table of Parameters....224
5.5.2.4 'Code Signing Certificate Revoked' Create Notification Form....225
5.5.2.4.1 Table of Parameters....225
5.5.2.5 'Code Signing Certificate Expiration' Create Notification Form....226
5.5.2.5.1 Table of Parameters....226
5.5.2.6 'Code Signing Certificate Requested' Create Notification Form....227
5.5.2.6.1 Table of Parameters....227
5.5.2.7 'SSL Approved' Create Notification Form....228
5.5.2.7.1 Table of Parameters....229
5.5.2.8 'SSL Awaiting Approval' Create Notification Form....229
5.5.2.8.1 Table of Parameters....230
5.5.2.9 'SSL Declined' Create Notification Form....231
5.5.2.9.1 Table of Parameters....232
5.5.2.10 'SSL Expiration' Create Notification Form....232
5.5.2.10.1 Table of Parameters....233
5.5.2.11 'SSL Issuance Failed' Create Notification Form....234
5.5.2.11.1 Table of Parameters....234
5.5.2.12 'SSL Revoked' Create Notification Form....235
5.5.2.12.1 Table of Parameters....236
5.5.2.13 'Discovery Scan Summary' Create Notification Form....236
5.5.2.13.1 Table of Parameters....237
5.5.2.14 'Remote SSL Certificate Installed ' Create Notification Form....238
5.5.2.14.1 Table of Parameters....238
5.5.2.15 'Remote SSL Certificate Installation Failed ' Create Notification Form....239
5.5.2.15.1 Table of Parameters....239
5.5.2.16 'Client Admin Creation' Create Notification Form....240
5.5.2.16.1 Table of Parameters....241
5.5.2.17 'Domain Awaiting Approval' Create Notification Form....241
5.5.2.17.1 Table of Parameters....242
5.5.2.18 'Domain Approved' Create Notification Form....243
5.5.2.18.1 Table of Parameters....244
5.5.2.19 'DCV Expiration' Create Notification Form....244
5.5.2.19.1 Table of Parameters....245
5.5.2.20 'DCV Validated' Create Notification Form....246
5.5.2.20.1 Table of Parameters....246
5.5.2.21 'DCV Needed-New Domain' Create Notification Form....247
5.5.2.21.1 Table of Parameters....247
5.6 Encryption and Key Escrow....248
5.6.1 Introduction and basic concepts....248
5.6.2 Setting up Key Escrow for an Organization....248
5.6.3 Setting up Key Escrow for a Department....250
5.6.4 Master Keys Required Prior to Client Cert Issuance....252
5.6.5 Encryption....254
5.6.5.1 Summary of Fields and Controls....254
5.6.6 Encrypting the Private Keys....254

5.6.7 Re-encryption 255
5.6.8 Recovering a User's Private Key from Escrow 257
5.7 Access Control 258
5.7.1 Overview 258
5.7.1.1 Access Control Options - Table of Parameters 259
5.7.1.2 Filtering Options 259
5.7.2 Adding a New IP Range 260
5.7.2.1 Add IP Range - Table of Parameters 261
5.7.3 Editing an IP Range 262
5.8 Certificates 262
5.8.1 Section Overview 262
5.8.2 SSL Types 263
5.8.2.1 Customize SSL Certificate Types 264
5.8.3 Client Cert Types 265
5.8.3.1 Customize Client Certificate Types 267
5.8.4 Custom Fields 268
5.8.4.1 Adding a new Custom Field 269
5.8.4.2 Editing an Existing Custom Field 271
5.8.4.3 Removing an Existing Custom Field 272
5.9 Email Templates 273
5.9.1 Viewing and Editing the Email Templates 274
6 Certificate Discovery and Agents 276
6.1 Certificate Discovery Area 277
6.1.1 Discovery Tasks 277
6.1.1.1 Sorting and Filtering Options 278
6.1.1.2 Prerequisites 280
6.1.1.3 Overview of Process 280
6.1.1.4 Adding IP Range and Start Scanning 280
6.1.1.5 Editing a Discovery Task 286
6.1.1.6 Deleting a Discovery Task 286
6.1.1.7 Viewing History of Discovery Tasks 287
6.1.1.8 View Scan Results 290
6.1.2 Agents 292
6.1.2.1 Sorting and Filtering Options 294
6.1.2.2 Configuring the Agent for Auto-Installation and Internal Scanning - Overview of the Process 295
6.1.2.3 Prerequisites 295
6.1.2.4 Configuring the Agent for Auto-Installation and Internal Scanning - Detailed Explanation of the Process 295
6.1.2.5 Configuring the Certificate Controller Agent through Web Interface 304
6.1.2.5.1 Agent Configuration 305
6.1.2.5.2 Server Management 308
7 Reports 311
7.1 Overview 311
7.2 Reports - Security Roles Access Table 314
7.3 Activity Log Report 315
7.3.1 Report Type: Activity Log - Table of Parameters 315
7.4 Client Certificates Reports 315

7.4.1 Report Type: Client Certificates - Table of Parameters....316
7.5 Discovery Scan Log Reports....317
7.5.1 Discovery Scan Log Report: Summary type....317
7.5.1.1 Report Type: Discovery Scan Log :Summary - Table of Parameters....318
7.5.2 Discovery Scan Log Report: Detail type....319
7.5.2.1 Report Type: Discovery Scan Log :Detail - Table of Parameters....320
7.6 SSL Certificates Reports....320
7.6.1 Report Type: SSL Certificates - Table of Parameters....321
7.7 Code Signing Certificates Report....323
7.7.1 Report Type: Code Signing Certificates - Table of Parameters....323
7.8 Admins Report....324
7.9 XML Data Report....325
7.10 DCV Report....326
7.10.1 Report Type: DCV Report - Table of Parameters....327
7.11 Notification Log Statistics Report....328
7.11.1 Notification Log Statistics - Email....328
7.11.1.1 Report Type: Notification Log Statistics :Emails - Table of Parameters....328
7.11.2 Notification Log Statistics - Notification Type....329
7.11.2.1 Report Type: Notification Log Statistics :Notification Type - Table of Parameters....329
7.11.3 Notification Log Statistics - Full Log....329
7.11.3.1 Report Type: Notification Log Statistics :Full Log - Table of Parameters....330
8 Version and Feature Information....330
9 My Profile....331
10 Logging Out of Comodo Certificate Manager....333
Appendix 1 - Your responsibilities when ordering SSL Certificates....334
About Comodo....335

1 Introduction to Comodo Certificate Manager

Comodo Certificate Manager (CCM) centralizes and streamlines the life-cycle management of web server, SMIME and code signing certificates through a unified interface. The system features full integration with Comodo Certificate Authority and 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, CCM reduces the need for manual certificate management and thus creates a more efficient, productive and secure certification environment.

1.1 Guide Structure

This guide is intended to take you through the step-by-step process of organization, configuration and use of Comodo Certificate Manager service.

- Section 1, **Introduction to Comodo Certificate Manager** - Contains a high level overview of the solution and serves as an introduction to the main themes and concepts that are discussed in more detail later in the guide - including security roles, Organizations, Reports and a summary of the main areas of the interface.
- Section 2, **The Dashboard** - Contains an overview of the dashboard that provides a at-a-glance graphical summary of key life-cycle information (such as certificates approaching expiry, certificates issued/requested and DCV status).
- Section 3, **Certificates Management** - Contains an overview of the area's main functionality and detailed explanations on how to request, collect and manage SSL certificates for web servers and hosts, client certificates for employees and corporate clients (end-users) and code signing certificates for digitally signing executables and scripts.
- Section 4, **Admin Management** - Covers the creation and management of Certificate Manager Administrators and the assigning of privileges and responsibilities to those Administrators.
- Section 5, **Settings** - Contains overviews and tutorials pertaining to the functional areas housed under the 'Settings' tab, including guidance on how to create a **new Organization**, **manage Organizations**, **add domains** and associate them with an Organization or Department, limit which IP addresses can access the CCM interface in **Access Control**, set up **Notifications**, customize overall and Organization based **SSL types** availability and manage **Encryption** settings. To view detailed information about each area, click on the links below:
  - **Organizations** (including full details on how to **Manage and Create Organizations**)
  - **Domains**
  - **Encryption and Key Escrow**
  - **Notifications**
  - **Access Control**
  - **Certificates**
  - **Email Template**
- Section 6, **Certificate Discovery** - explains how to scan and monitor a network for all installed SSL certificates including certificates that may or may not have been issued using CCM, any third party vendor certificates and any self-signed certificates. This section also explains how to download and install agents that are used for automatic installation of certificates and for certificate scan.
- Section 7, **The Reports section** - Contains an overview of the area, descriptions of each report type and guidance on how to access the required report type.
- Section 8, **Version and Feature information** - explains how to view the version of CCM and the features enabled for the subscription.
- Section 9, **My Profile** - explains how to changes the time format and the password.
- Section 10, **Logging out of Comodo Certificate Manager** explains the process for logging out.
- Appendix 1 - **Your responsibilities when ordering SSL Certificate** contains a very short summary of certificate

issuance guidelines.

1.2 Definitions of Terms

1.2.1 Organizations and Departments

Organizations and Departments are created by administrators for the purposes of requesting, issuing and managing Comodo digital certificates. Each Organization can have multiple Departments.

Organizations are typically managed by a Registration Authority Officer (RAO) while Departments are typically managed by a Domain Registration Authority Officer (DRAO). A Master Registration Authority Officer (MRAO) can manage all Organizations and all Departments.

Once an Organization or Department has been created:

- Appropriately privileged officers can request and delegate domains to that Organization/Department
- Appropriately privileged officers can request, approve/decline requests and manage certificates on behalf of that Organization or Department.
- End-users can enroll into (or be assigned membership of) that Organization or Department and be provisioned with client certificates

1.2.2 Certificate Types

Comodo Certificate Manager can be used to request and manage the following types of digital certificate:

SSL 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 will confirm the identity of the organization that is operating the website; encrypt all information passed between the site and the visitor and will ensure the integrity of all transmitted data.

Client Certificates - Client certificates are issued to individuals and can be used to encrypt and digitally sign email messages; to digitally sign documents and files and to authenticate the identity of an individual prior to granting them access to secure online services.

Code Signing Certificates - Code Signing Certificates are used to digitally sign software executables and scripts. Doing so helps users to confirm that the software is 'genuine' by verifying content source (authentication of the publisher of the software) and content integrity (that the software has not been modified, corrupted or hacked since the time it was originally signed).

1.2.3 Administrative Roles

There are 3 classes of Administrator in Comodo Certificate Manager:

- **Master Registration Authority Officer (MRAO)** - The highest level of administrator in Comodo Certificate Manager (CCM) is the Master Registration Authority Officer (MRAO). An MRAO has access to all functional areas and may delegate control over the certificates, domains and notifications of any Organization or Department. An MRAO also has full rights over the creation and privileges of Registration Authority Officers (RAOs), Department Registration Authority Officers (DRAOs) and end-users of any Organization or Department.
- **Registration Authority Office (RAO)** - A Registration Authority Officer (RAO) is an administrative role created by an MRAO for the purposes of managing the certificates and end-users belonging to one or more CCM Organizations. They have control over the certificates that are ordered on behalf of their Organization(s); over Domains that have been delegated to their Organization/Dept by an MRAO; over any Departments of their Organization and over that Organization's end-user membership. RAOs can also create peer RAOs for their Organizations and edit or remove existing RAOs of their Organizations, if appropriate privileges are assigned by the MRAO.
- **Department Registration Authority Officer (DRAO)** - Department Registration Authority Officers are created by, and subordinate to, the RAO class of Administrator. They are assigned control over the certificates, users and domains belonging to a Department(s) of an Organization. DRAOs can also create peer DRAOs for their Departments and edit or remove existing RAOs of their Departments, if appropriate privileges are assigned by the MRAO or RAO.

The RAO and DRAO class of administrator are sub-divided into specific roles by certificate type:

- **RAO SSL administrators**

- **RAO SMIME administrators**
- **RAO Code Signing administrators**
- **DRAO SSL administrators**
- **DRAO SMIME administrators**
- **DRAO Code Signing administrators**

Therefore, the privileges of any particular RAO or DRAO administrator are broadly defined by the elements described in sections **1.2.1**, **1.2.2** and **1.2.3**:

1. The Organization or Department that they are delegated to
2. The specific type of certificate that they are delegated responsibility for
3. Their specific administrative class (whether they are an RAO or a DRAO)

CCM also uses the following terms to identify personnel:

- **End-User**
- **Owner**
- **Requester**

The following table contains detailed summaries of the privileges that apply to each type of administrator and also features descriptions of the 'end-user', 'owner' and 'requester' types of personnel.

MRAO Administrator

Security Role / Type of Administrator	Definition
MRAO **(Master Registration Authority Officer)**	The MRAO is the top level administrator and can access all areas and functionality of the Certificate Manager interface. • MRAOs have full visibility of and control over the provisioning and life-cycle management of all certificate types • New MRAOs can only be created and managed by an existing MRAO. • MRAO level administrators are visible only to other MRAOs in the '**Admin Management**' area of the CCM interface. • MRAO admins can create new Organizations and Departments and delegate them to RAO and DRAO class administrators respectively. • MRAO admins can initiate the process of validating organizations for the purpose of requesting and issuance of OV SSL certificates to organizations and departments under them. • MRAOs are able to create and manage RAO and DRAO class administrators for any Organization or Department • MRAOs have full access and executive rights to add, modify and delegate Domains to any Organization or Department • MRAO 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 setup Certificate Controller Agents on a local network for any Department or Organization. Agents allows admins to scan internal hosts for installed SSL certificates which can then be tracked using the CCM admin console. Agents also facilitate the

Security Role / Type of Administrator	Definition
	automatic installation of SSL certificates on Apache, Apache Tomcat and IIS web servers. • MRAOs can enable RAO SMIME and DRAO SMIME types of administrator with the ability to recover the private keys of client certificates for those Organizations / Departments that they administer. • If desired, it is possible for MRAO Administrators to recover from escrow the private keys of client certificates that belong to any Organization or Department • MRAOs can view Activity Logs for all Organizations and Departments • MRAOs are the only individuals with sufficient privileges to manage 'SSL Types' and 'Client Cert Types'. • MRAOs have privileges to add custom fields in the Built-in Application and Self-Enrollment Forms for SSL and Client certificates requisition. • If enabled by Comodo, MRAOs can define Key Usage Templates (KUT) for client certificates belonging to ALL Organizations. Key Usage Templates dictate whether client certificates are capable of (1) Signing, (2) Encryption or (3) BOTH Signing and Encryption.

RAO Administrators

Security Role / Type of Administrator	Definition
RAO SSL **(Registration Authority Officer - SSL Certificates)**	Administrators with the security role 'RAO SSL' have privileges to request and manage SSL certificates for domains that have been delegated to their Organization • RAO SSL admins have visibility and control over SSL certificates that belong to their delegated Organization. They can approve or decline requests for SSL certificates made using the **Self-Enrollment form** for their Organization(s) and sub-ordinate Department(s). • They have no access to manage SSL certificates belonging to Organizations for which they have not been granted permissions. • RAO SSL admins can only manage SSL Certificates and have no privileges to manage other certificate types (such as client certificates and code signing certificates) - including those that belong to the Organization that he or she is the SSL Administrator of. • RAO SSL admins will see only those Organizations that have been delegated to them in the 'Organizations' area. • It is possible for a MRAO to make the same individual an 'RAO SMIME ' AND a 'RAO SSL' AND a RAO Code Signing for an single organization during the Administrator creation or editing process (for more details, see section **Admin Management**). • RAO SSL admins cannot create new Organizations. Neither can they edit the General settings of any Organization - even those

Security Role / Type of Administrator	Definition

	Organizations of which they are SSL Certificate administrator.
	• RAO SSL administrators can create Departments only within Organizations that have been delegated to them
	• RAO SSL admins cannot approve or request the creation of administrators that have more privileges than themselves. They can:
	  • Request the creation of fellow RAO SSL admins only for Organizations that have been delegated to them if MRAO has enabled this feature for them
	  • Request and approve the creation of DRAO SSL admins
	  • Cannot request or approve the creation of any type of administrator for Organizations that have not been delegated to them
	  • Cannot request or approve creation of administrators of any other certificate type - even for those Organizations that have been delegated to them
	• RAO SSL admins can delegate Domains to sub-ordinate Departments of Organizations that they administrate.
	• RAO SSL admins can initiate DCV process for the Domains delegated to sub-ordinate Departments of Organizations that they administrate if they were given 'Allow DCV' privileges. RAO SSL with 'Allow DCV' privileges can be created only by the MRAO.
	• RAO SSL Admins can setup Certificate Controller Agents in a local network for scanning internal hosts with internally facing IP addresses for installed SSL certificates for the Organization(s) that are delegated to them and any sub-ordinate Departments there of. Agents also facilitate the automatic installation of SSL certificates on Apache, Apache Tomcat and IIS web servers.
	• RAO SSL admins can view the **SSL certificates Reports** and **Certificate Discovery Reports** for the Organization that they were assigned rights to.
	• RAO SSL admins cannot access or manage Encryption Settings.
	• RAO SSL admins can only view Activity Logs for their Organization(s).
	• An 'at-a-glance' summary of Administrator security roles and access rights is available **here**.

RAO SMIME **(Registration Authority Officer - SMIME Certificates)**	Administrators with the security role 'RAO SMIME' have privileges to access, manage, request and approve the requests of Client Certificates for domains that have been delegated to their Organization • RAO SMIME admins have visibility and control over the client certificates belonging to End-Users of the Organizations for which they have been assigned rights. They have no access to manage the Client Certificates of End-Users that belong to Organizations which they have not been granted permissions. • RAO SMIME admins can only manage SMIME certificates and have no privileges to manage other certificate types (such as SSL Certificates and Code Signing Certificates) - including those that belong to the Organization of which they are SMIME Administrator.

Security Role / Type of Administrator	Definition

	• It is possible for a MRAO to make the same individual an 'RAO SMIME ' AND a 'RAO SSL' AND a RAO Code Signing for an single organization during the Administrator creation or editing process (for more details, see section **Admin Management**).
	• RAO SMIME admins will see only those Organizations that have been delegated to them in the 'Organizations' area.
	• RAO SMIME admins cannot create new Organizations. Neither can they edit the General settings of any Organization - even those Organizations of which they are SMIME administrator.
	• If enabled for their Organization(s), RAO SMIME admins can define Key Usage Templates (KUT) for client certificates that belong their own Organizations and Departments. Key Usage Templates dictate whether client certificates are capable of (1) Signing, (2) Encryption or (3) BOTH Signing and Encryption. The templates which are made available to an RAO SMIME will be specified by the MRAO.
	• RAO SMIME administrators can create Departments only within Organizations that have been delegated to them
	• RAO SMIME admins cannot approve or request the creation of administrators that have more privileges than themselves. They can:
	  • Request the creation of fellow RAO SMIME admins only for Organizations that have been delegated to them if MRAO has enabled this feature for them
	  • Request and approve the creation of DRAO SMIME admins
	  • Cannot request or approve the creation of any type of administrator for Organizations that have not been delegated to them
	  • Cannot request or approve creation of administrators of any other certificate type - even for those Organizations that have been delegated to them
	• RAO SMIME admins can delegate Domains to sub-ordinate Departments of Organizations that they administrate.
	• When creating a new Department, an RAO SMIME admins can:
	  • Enable or disable the ability of MRAOs to recover the private keys of client certificates that belong to this Department
	  • Enable or disable the ability of RAO SMIME admins (themselves) to recover the private keys of client certificates that belong to this Department
	  • Enable or disable the ability of DRAO SMIME admins to recover the private keys of client certificates that belong to this Department
	  • All or any combination of the above
	• RAO SMIME admins can only view Activity Logs for their Organization.
	• An 'at-a-glance' summary of Administrator security roles and

Security Role / Type of Administrator	Definition
	access rights is available **here**.

RAO Code Signing
(Registration Authority Officer - Code Signing Certificates)
	Administrators with the security role 'RAO Code Signing' have privileges to access, manage, request and approve the requests of Code Signing Certificates for domains that have been delegated to their Organization
	• RAO Code Signing Administrators have visibility and control over the code signing certificates belonging to End-Users of the Organization for which they have been assigned rights. They have no access to manage the Code Signing Certificates of End-Users that belong to Organizations of which they have not been granted permissions.
	• RAO Code Signing admins can only manage Code Signing Certificates. They have no privileges to manage other types such as SSL or SMIME - including those SSL/SMIME certificates belonging to the Organization of which they are Code Signing Certificate Administrator.
	• It is possible for a MRAO to make the same individual an 'RAO SMIME' AND a 'RAO SSL' AND a RAO Code Signing for an single organization during the Administrator creation or editing process (for more details, see section **Admin Management**).
	• RAO Code Signing admins will see only those Organizations that have been delegated to them in the 'Organizations' area.
	• RAO Code Signing admins cannot create new Organizations. Neither can they edit the General settings of any Organization - even those Organizations of which they are Code Sigining Certificate administrator.
	• RAO Code Signing administrators can create Departments only within Organizations that have been delegated to them
	• RAO Code Signing admins cannot approve or request the creation of administrators that have more privileges than themselves. They can:
	  • Request the creation of fellow RAO Code Signing admins only for Organizations that have been delegated to them if MRAO has enabled this feature for them
	  • Request and approve the creation of DRAO Code Signing admins
	  • Cannot request or approve the creation of any type of administrator for Organizations that have not been delegated to them
	  • Cannot request or approve creation of administrators of any other certificate type - even for those Organizations that have been delegated to them
	• RAO Code Signing admins can delegate Domains to sub-ordinate Departments of Organizations that they administrate.
	• RAO Code Signing admins can only view Activity Logs for their Organization.
	• An 'at-a-glance' summary of Administrator security roles and access rights is available **here**.

DRAO Administrators

Security Role / Type of Administrator	Definition

DRAO SSL
(Department Registration Authority Officer - SSL Certificates)
	Administrators with the security role 'DRAO SSL' have privileges to access, manage and request SSL certificates for domains that have been delegated to their Department by an RAO or MRAO
	• DRAO SSL admins have visibility and control over SSL certificates that belong to their delegated Department(s). A DRAO SSL admin can only request SSL certificates for domains that have been delegated to their Department. They can approve or decline requests for SSL certificates made using the **Self-Enrollment form** for their Department(s).
	• They have no access to manage SSL certificates belonging to Departments for which they have not been granted permissions. They will only see their own Departments(s) listed in the 'Departments' area. The 'Organizations' area is not visible to DRAOs.
	• DRAO SSL admins have no visibility of and cannot request certificates of any other type - including those other certificate types that belong to the Department of which they are DRAO SSL .
	• It is possible for an RAO to make the same individual a 'DRAO SMIME' , 'DRAO SSL', 'DRAO Code Signing' for a single Department during the Admin creation or editing process (for more details, see section **Admin Management**).
	• DRAO SSL admins cannot request the creation of administrators that have more privileges than themselves. They can:
	  • Request the creation of fellow DRAO SSL admins only for Departments that have been delegated to them if the RAO administrator has enabled this feature for them
	  • Cannot request the creation of any type of administrator for Departments that have not been delegated to them
	  • Cannot request creation of administrators of any other certificate type - even for those Departments that have been delegated to them
	• DRAO SSL admins can request the addition of new Domains only for to Departments that have been delegated to them.
	• DRAO SSL admins can initiate DCV process for the Domains delegated to their Department(s) administrate if they were given 'Allow DCV' privileges. DRAO SSL admin with such privileges can be created only by MRAO or RAO SSL having the same privilege.
	• DRAO SSL Admins can setup Certificate Controller Agents in a local network for scanning internal hosts with internally facing IP addresses for installed SSL certificates for the Department(s) that are delegated to them. Agents also facilitate the automatic installation of SSL certificates on Apache, Apache Tomcat and IIS web servers.
	• DRAO SSL admins can view Reports, edit Access Control Lists and modify Email Templates for the Department that has been delegated to them.
	• DRAO SSL admins cannot access or manage Encryption Settings.
	• DRAO SSL admins cannot view Activity Logs.

Security Role / Type of Administrator	Definition
	• An 'at-a-glance' summary of Administrator security roles and access rights is available **here**.

DRAO SMIME
(Department Registration Authority Officer - SMIME Certificates)
	Administrators with the security role 'DRAO SMIME' have privileges to access, manage and request Client Certificates for domains that have been delegated to their Department by an RAO or MRAO
	• DRAO SMIME admins have visibility over the client certificates belonging to end-users of the Department(s) which have been delegated to them. They have no access to manage the Client Certificates of end-users that belong to Departments which they have not been delegated. They will only see their own Departments(s) listed in the 'Departments' area. The 'Organizations' area is not visible to DRAOs.
	• A DRAO SMIME admin can only request SMIME certificates for domains that have been delegated to their Department.
	• DRAO SMIME admins have no visibility of and cannot request certificates of any other type - including those other certificate types that belong to the Department of which they are DRAO SMIME.
	• It is possible for an RAO to make the same individual a 'DRAO SMIME' , 'DRAO SSL', 'DRAO Code Signing' for a single Department during the Admin creation or editing process (for more details, see section **Admin Management**).
	• DRAO SMIME admins cannot request the creation of administrators that have more privileges than themselves. They can:
	  • Request the creation of fellow DRAO SMIME admins only for Departments that have been delegated to them if the RAO administrator has enabled this feature for them
	  • Cannot request the creation of any type of administrator for Departments that have not been delegated to them
	  • Cannot request creation of administrators of any other certificate type - even for those Departments that have been delegated to them
	• DRAO SMIME admins can request the addition of new Domains only for to Departments that have been delegated to them.
	• If enabled for their Department, a DRAO SMIME admin can recover the private keys of client certificates belonging to their Department
	• DRAO SMIME admins can view Reports, edit Access Control Lists and modify Email Templates for the Department that has been delegated to them.
	• DRAO SMIME admins cannot view Activity Logs.
	• An 'at-a-glance' summary of Administrator security roles and access rights is available **here**.

DRAO Code Signing **(Department Registration Authority Officer - Code Signing Certificates)**	Administrators with the security role 'DRAO Code Signing' have privileges to access, manage and request Code Signing certificates for Departments of a Organization that have been delegated to them by an RAO or MRAO.

Security Role / Type of Administrator	Definition

	• DRAO Code Signing admins have visibility of and can request Code Signing certificates for the Department(s) that have been delegated to them. They have no access to manage Code Signing certificates belonging to Departments for which have not been delegated to them. They will only see their own Departments(s) listed in the 'Departments' area. The 'Organizations' area is not visible to DRAOs.
	• A DRAO Code Signing admin can only request Code Signing certificates for domains that have been delegated to their Department.
	• DRAO Code Signing admins have no visibility of and cannot request certificates of any other type - including those other types of certificate that belong to the Department of which they are DRAO Code Signing.
	• It is possible for an RAO to make the same individual a 'DRAO SMIME' , 'DRAO SSL', 'DRAO Code Signing' for a single Department during the Admin creation or editing process (for more details, see section **Admin Management**).
	• DRAO Code Signing admins cannot approve or request the creation of administrators that have more privileges than themselves. They can:
	  • Request the creation of fellow DRAO Code Signing admins only for Departments that have been delegated to them if the RAO administrator has enabled this feature for them
	  • Cannot request the creation of any type of administrator for Departments that have not been delegated to them
	  • Cannot request creation of administrators of any other certificate type - even for those Departments that have been delegated to them
	• DRAO Code Signing admins can request the creation of new Domains only for Departments that have been delegated to them.
	• DRAO Code Signing admins can view Reports, edit Access Control Lists and modify Email Templates for the Department that has been delegated to them.
	• DRAO Code Signing Administrators cannot access or manage Encryption Settings.
	• DRAO Code Signing Administrators cannot view Activity Logs.
	• An 'at-a-glance' summary of Administrator security roles and access rights is available **here**.

End-User, Owner and Requester

Security Role / Type of Administrator	Definition
End-User	An End-User in CCM is a person that has been issued with or requested a Client Certificate or has made an application for an SSL certificate using the Self Enrollment form. • 'End-Users' have no access rights whatsoever to the CCM

Security Role / Type of Administrator	Definition

	interface. They exist in CCM 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 CCM via:
	  • **Manual creation by a Administrator in the 'Client Certificate' area**;
	  • **The End-User ordering a Client Certificate using the Self Enrollment Form**;
	  • **End-User is imported into CCM from .csv file**.
	• A new end-user will also be added via SSL certificate applications made through the **self enrollment form**. If the applicant does not already exist as an end-user then Comodo Certificate Manager will automatically add this applicant when the form is submitted. End-Users that are auto-created in this way will not (yet) have a Client Certificate.
	• All end-users and Client Certificates owned or requested by that end-user are listed in the 'Client Cert' sub-tab of the 'Certificates Management' section of CCM interface.
	• An 'at-a-glance' summary of Administrator security roles and access rights is available **here**.

Owner	The **Owner** of the certificate is the Administrator that first approved the request for the certificate. The privileges of the 'Owner' therefore depend on that Administrator's administrative role. (See the definitions above).
Requester	The Requester of the certificate is the person that created and successfully submitted the initial application for the certificate. • The 'Requester' can be any class of Administrator or End-User • SSL certificates and Client certificates can be requested by people that do not yet 'exist' in CCM as either End-Users or Administrators if they applied using use the self-enrollment/external application forms

1.2.4 Security Roles - Comparative Table

Organization and Department Management				
Action	**Controls**	**MRAO**	**RAO**	**DRAO**
Configure other Administrators	Add, View Delete, Edit	Any MRAO Any RAO of Any Certificate Type Any DRAO of Any Certificate Type	Create DRAOs of Subordinate Departments who are responsible for same Certificate Type Creation of RAOs of Delegated Organization	Creation of DRAOs of Delegated Department who are responsible for the same certificate type if enabled by a RAO administrator

			who are responsible for same Certificate Type	or a MRAO
Approve/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 same Certificate Type	✘
Activate/Deactivate Administrators	Checkbox	Any MRAO Any RAO of Any Certificate Type Any DRAO of Any Certificate Type	RAOs of Delegated Organization who are responsible for same Certificate Type DRAOs of Subordinate Departments who are responsible for same Certificate Type	✘

Certificate Management

Action	Controls	MRAO	RAO		DRAO	
Directly submit Certificate Requests to the issuing Certificate Authority for **Auto-Installation by CCM** (IIS , Apache and Apache Tomcat only)	Add, Renew, Approve, Decline, Install	Any Organization Any Department	Delegated Organizations Subordinate Departments		Delegated Departments	
			RAO SSL	✓	RAO SSL	✓
			RAO SMIME	✘	RAO SMIME	✘
			RAO Code Signing	✘	RAO Code Signing	✘
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 RAO is responsible		Delegated Departments Only those Certificate Types for which DRAO is responsible	
Approve/Decline Certificate Requests that have been made using the **Self-Enrollment form**	Approve, Decline	Any Organization Any Department Of any Certificate Type	Delegated Organizations Subordinate Departments Only those Certificate Types for which RAO is responsible		Delegated Departments Only those Certificate Types for which DRAO is responsible	
Manage Certificates	View, Edit, Revoke	Any Organization Any Department	Delegated Organizations		Delegated Department	

		Of any Certificate Type	Subordinate Departments Only those Certificate Types for which RAO is responsible		Only those Certificate Types for which DRAO is responsible	
Certificate Discovery	Add CIDR, Delete CIDR, Setup Certificate controller agent for internal scanning	✓	RAO SSL	✓	DRAO SSL	✓
			RAO SMIME	✗	DRAO SMIME	✗
			RAO Code Signing	✗	DRAO Code Signing	✗
Request Domains for...	Add	Any Organization Any Department	Delegated Organizations Subordinate Departments		Delegated Departments	
Approve / Reject Domain Requests for...	Approve, Reject	Any Organization Any Department	Subordinate Departments		✗	
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 but cannot re-delegate or remove a domain's delegation.		✗	
Activate/Deactivate Domains for...	Checkbox	Any Organization Any Department	✗		✗	
Initiate DCV	Select method of DCV as applicable to the domain	Any Organization Any Department	RAO SSL	On Domains added to Delegated Organizations and Subordinate Departments	DRAO SSL	On Domains added to Delegated Department
			RAO SMIME	✗	DRAO SMIME	✗
			RAO Code	✗	DRAO Code Signing	✗

			Signing			
Organization and Department Management						
Action	**Controls**	**MRAO Administrator**	**RAO**		**DRAO**	
Create and Manage Organizations	Add, Delete, Edit	✓	✗		✗	
Approve/Reject Organization Creation	Approve	✓	✗		✗	
Create and Manage Departments	Add, Delete, Edit	✓	Subordinate Departments of Delegated Organization		✗	
Approve Department Creation	Approve	✓	Subordinate Departments of Delegated Organization		✗	
Key Escrow						
Action	**Controls**	**MRAO**	**RAO SMIME**		**DRAO SMIME**	
Manage Encryption of client certificates	Initialize, Re-encrypt	Any delegated RAO Any delegated DRAO	Delegated Organizations Subordinate Departments		Delegated Organizations	
Recover private keys from escrow	Decrypt	Any Enabled Organization * Any Enabled Department *	Delegated Organizations Subordinate Departments		Delegated Organizations	
Can permit Administrators other than themselves to recover keys for a particular Organization or Department	Allow key recovery by.... (Checkbox)	MRAO admins RAO SMIME admins	MRAO Admins RAO SMIME Admins DRAO SMIME Admins		✗	

* Escrow privileges are configured at the point of Organization / Department creation.

When setting up an Organization, the MRAO can specify any, all or none of the following:

1. Whether or not the MRAO (themselves) should have the ability to recover the private keys of client certificates of that Organization
2. Whether or not the RAO SMIME admin of the Organization should have the ability to recover private keys of client certificates of that Organization

If granted escrow privileges above, the RAO SMIME admin will be subsequently be able to specify any, all or none of the following for any Departments they create:

1. Whether or not the MRAO should have the ability to recover the private keys of client certificates of that Department
2. Whether or not the RAO SMIME admin (themselves) should have the ability to recover the private keys of client certificates of that belonging to that Department
3. Whether or not the DRAO SMIME admin should have the ability to recover the private keys of client certificates belonging to that Department

See '**Encryption and Key Escrow**' for more details.

Notifications, Reports and Miscellaneous				
Action	**Controls**	**MRAO Administrator**	**RAO Administrator**	**DRAO Administrator**
Configure access control settings	Add, Delete, Edit CIDR	✓	✓	✓
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...	See **'Reports - Security Role Access Table'** section for details.	Any Organization Any Department	Delegated Organizations Subordinate Departments	Delegated DRAO
Manage SSL Type Availability	Type, Term	✓	✘	✘
Modify Email Templates for...	Edit	Any Organization Any Department	Delegated Organizations Subordinate Departments	Delegated Department

1.2.5 Multiple Security Roles

Multiple security roles may be selected for any particular administrator. An MRAO can assign SSL, SMIME and Code Signing administrative privileges to the same RAO for a particular organization. An RAO that has been granted administrative rights over multiple certificate types can assign similar, multi-role, privileges to a sub-ordinate DRAO administrator for a particular Department.

1.2.6 Organizations and Departments

The creation of an Organization and the delegation of a domain to that Organization is an important step towards the issuance and effective management of SSL, code signing or client certificates via the Certificate Manager interface.

Organizations and Departments are created by administrators for the purposes of requesting, issuing and managing certificates for domains and employees. Organizations can be sub-divided into Departments for the purposes of certificate and end-user

management. (See section **Creating a New Organization** for more details).

Each Organization can have multiple Departments. Organizations are typically managed by a Registration Authority Officer (RAO). Departments are typically managed by a Department Registration Authority Officer (DRAO). A Master RAO (MRAO) can manage all Organizations and all Departments.

Once an Organization has been created:

- MRAOs can create (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 them.
- MRAOs and RAOs can create multiple Departments within that Organization (See '**Organizations / Section Overview**' for more details).
- MRAOs can create (or assign existing) RAOs to manage individual Departments
- MRAOs can delegate domain(s) to the Organization or Department
- RAO and DRAO class administrators can directly request that certificates be issued to domains that have been delegated to their Department. They can also approve/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/Department.
- Administrators can manage the client certificates of end-users belonging to an Organization or Department via the 'Certificates Management - Client Certificates' interface and can manage SSL certificates for the Organization via the '**Certificate Managements - SSL Certificates**' area. Code Signing Certificates are managed from the 'Code Signing' area
- A wide range of Organization and Department specific email notifications can be set up to alert personnel to changes in certificate status, changes to domain status, Discovery Scan Summaries, Admin creation and more.
- MRAOs, RAOs and DRAOs can utilize the **Certificate Discovery** feature to audit 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/or specific Department.

1.2.7 Reports

Certificate reports and activity logs can be viewed and exported for an Organization and/or Department via the **Report** section. An appropriately privileged administrator is enabled to view different types of reports according their security roles. The following types of reports are available:

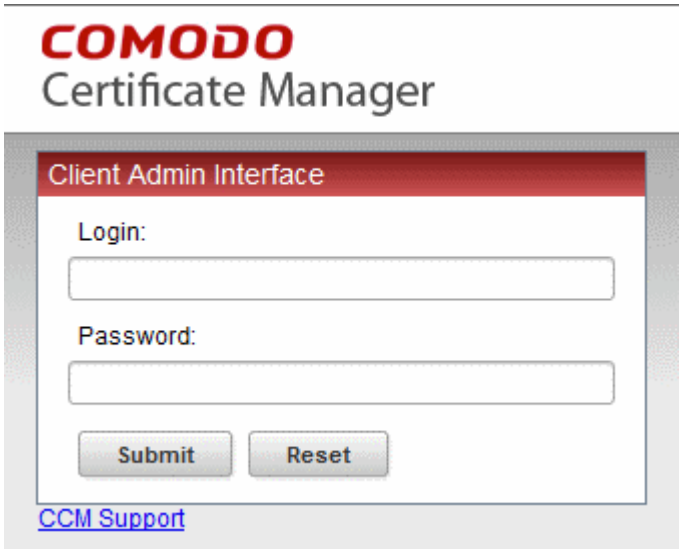
Type of Report	Description
Activity Log	Enables the MRAO to view all actions that have occurred within the interface within specific time periods.
SSL Certificates	Enables the MRAO and RAO/DRAO SSL administrators to monitor all statistics related to SSL certificates including usage, ownership, issuance, provisioning and status.
Discovery Scan Log	Enables the MRAO and RAO/DRAO SSL administrators to view the Discovery Scan Log. A Discovery Scan is an audit of all SSL certificates installed on your network.
Client Certificates	Enables the MRAO and RAO/DRAO SMIME administrators to monitor all statistics, related to client certificates including usage, ownership, issuance, provisioning and status.
Code Signing Certificates	Enables the MRAO and RAO/DRAO Code Signing administrators

Type of Report	Description
	to monitor all statistics, related to code signing certificates including usage, ownership, issuance, provisioning and status.
Admin	Enables the MRAO to generate and view reports providing the details of the enrolled Administrators of all privilege levels.
XML Data	Enables the MRAO to generate a report containing complete details of all the organizations, departments, their administrators and the all the certificates in XML format.
DCV Report	Enables the MRAO and RAO/DRAO SSL administrators to generate a report containing details on all of their registered domains, with their DCV status and expiration dates.
Notification Log Statistics Report	Enables the MRAO administrator to generate reports containing complete details of the notifications emails sent to RAO and DRAO administrators for various CCM events.

For more detailed information see the section '**Reports**' of the guide.

1.3 Logging into Your Account

Once your Organization has subscribed for a Comodo account, your Comodo account manager will provide you with a username, password and login URL for the Certificate Manager interface. By default, the format of this URL is: https://cert-manager.com/customer/[REAL CUSTOMER URI]/



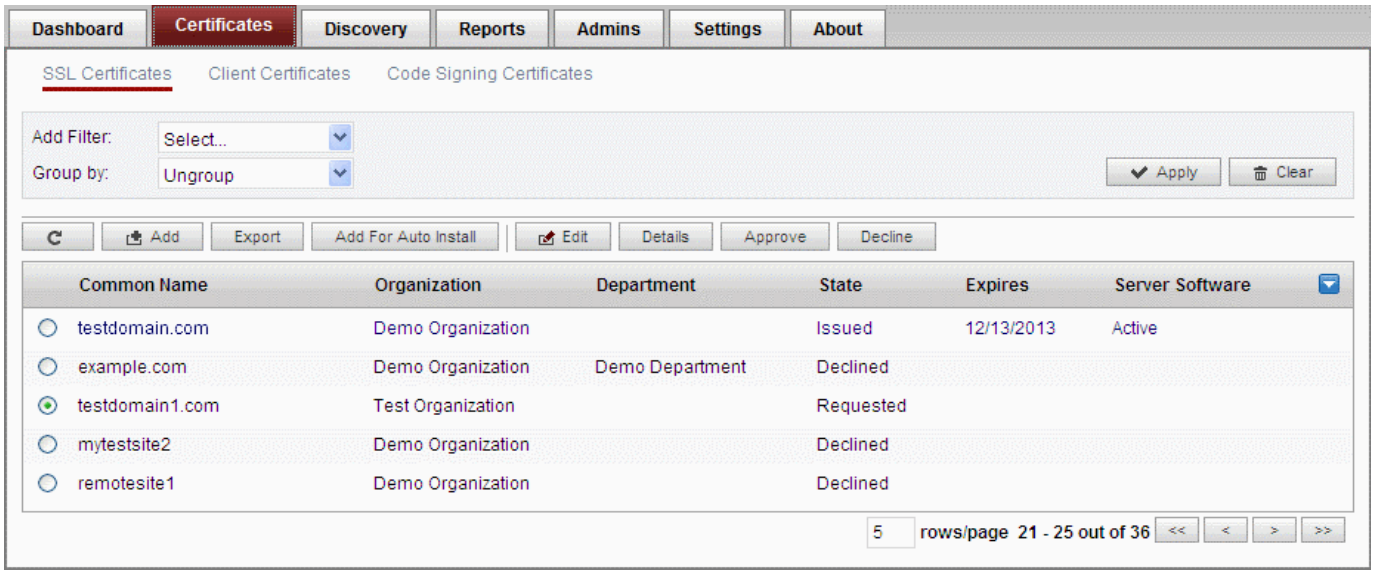
If you have not been supplied with your login details, please contact your Comodo account manager.

If you are not able to login with your login details, you can raise a support ticket at the Comodo Support portal by clicking 'Support link'. You can create an account for free and submit your ticket to get your login problems resolved.

Depending on the Access Control Settings specified by the administrator, you will be prompted to change your password after logging in for the first time. You may also change your password at any time via the '**My Profile**' area.

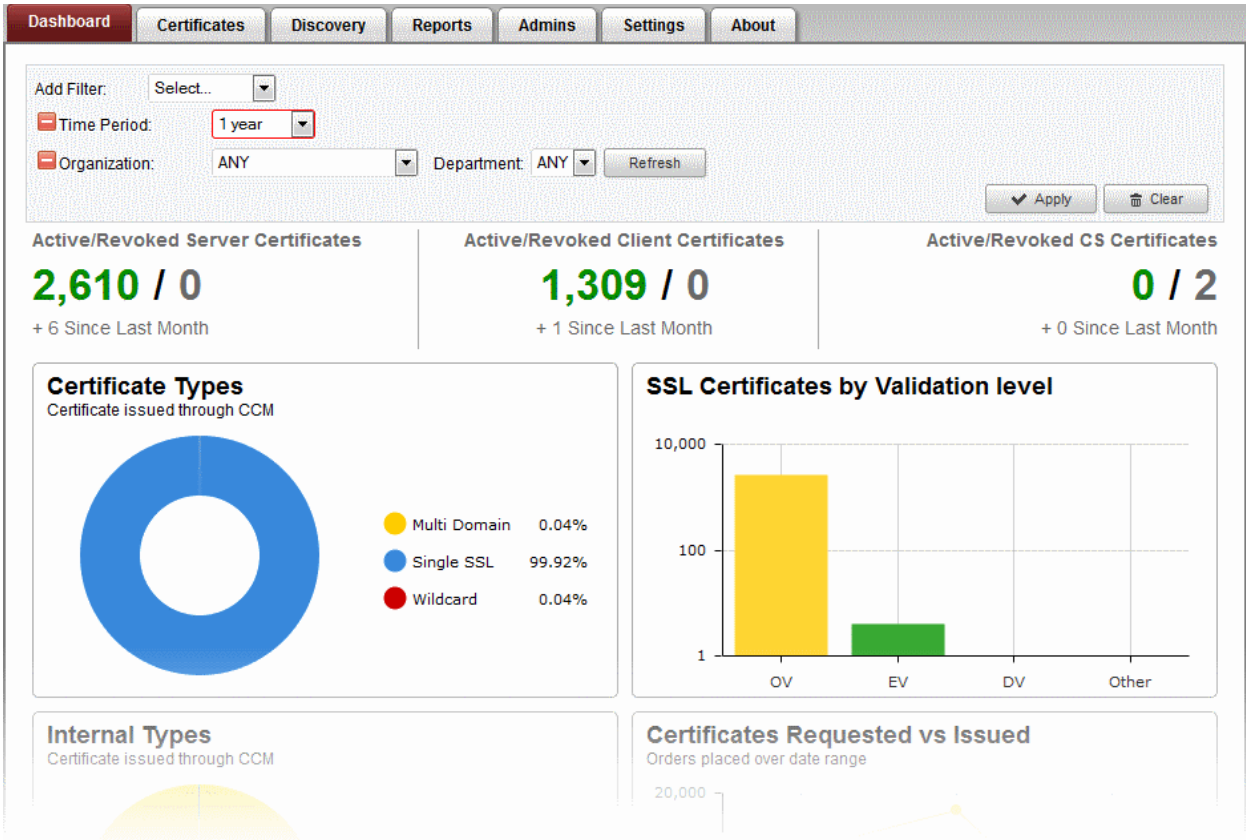
1.4 The Main Interface - Summary of Areas

Comodo Certificate Manager interface has a tab structure that facilitates access to all major settings.



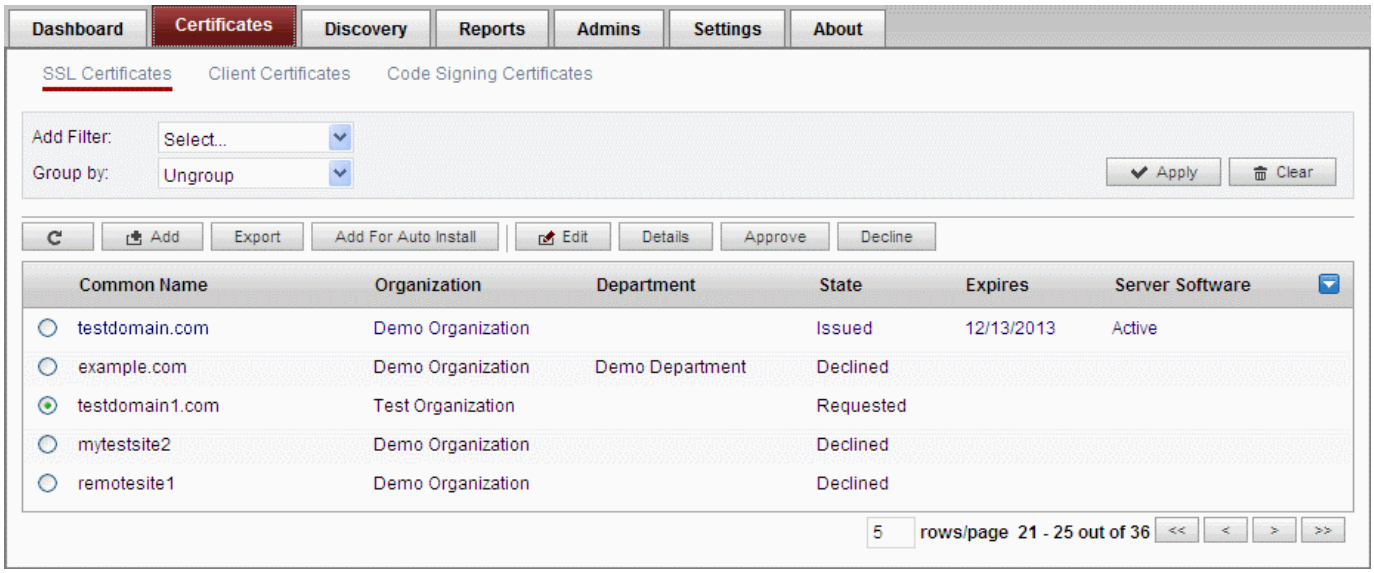
- There are (a maximum of) seven tabs that cover each of the main functional areas of the application. These are '**Dashboard**', '**Certificates Management**', '**Discovery**', '**Report**', '**Admin Management**', '**Settings**' and '**About**'.
- The '**Certificates Management**' tab contains sub-sections for managing the certificate types that have been enabled for your company. There is therefore a maximum of three sub-sections - '**SSL Certificates**', '**Client Certificates** and '**Code Signing Certificates**'.
- The '**Discovery**' tab contains sub-sections for scanning the network for installed certificates and for managing CD agents. The sub-sections are **Discovery Tasks** and **Agents**.
- The '**Settings**' tab contains sub-sections for '**Organizations**', '**Departments**', '**Domains**', '**Notifications**', '**Encryption**', '**Access Control**', '**Certificates**' and **Email Templates**.
- The remainder of this introduction contains an introduction to each tabbed area and the Security Role requirements for access to that area. Full details of the actual usage and functionality of the tabbed areas listed above are in sections **2. The Dashboard, 3. Certificates Management**, **4. Admin Management**, **5. Settings**, **6. Certificate Discovery and Agents, 7. Reports**, **8. Version and Feature Information**, **9. My Profile** and **10. Logging out of Comodo Certificate Manager**.

Dashboard: Contains graphs and charts that display snap-shot summaries of certificate key life-cycle information such as certificates approaching expiry, certificates issued/requested, DCV status, breakdown of certificates by types, issuers, and more.



Click here for more information about the Dashboard.

Certificates Management: Contains up to three sub-sections for the management of SSL, Client and Code Signing certificates.



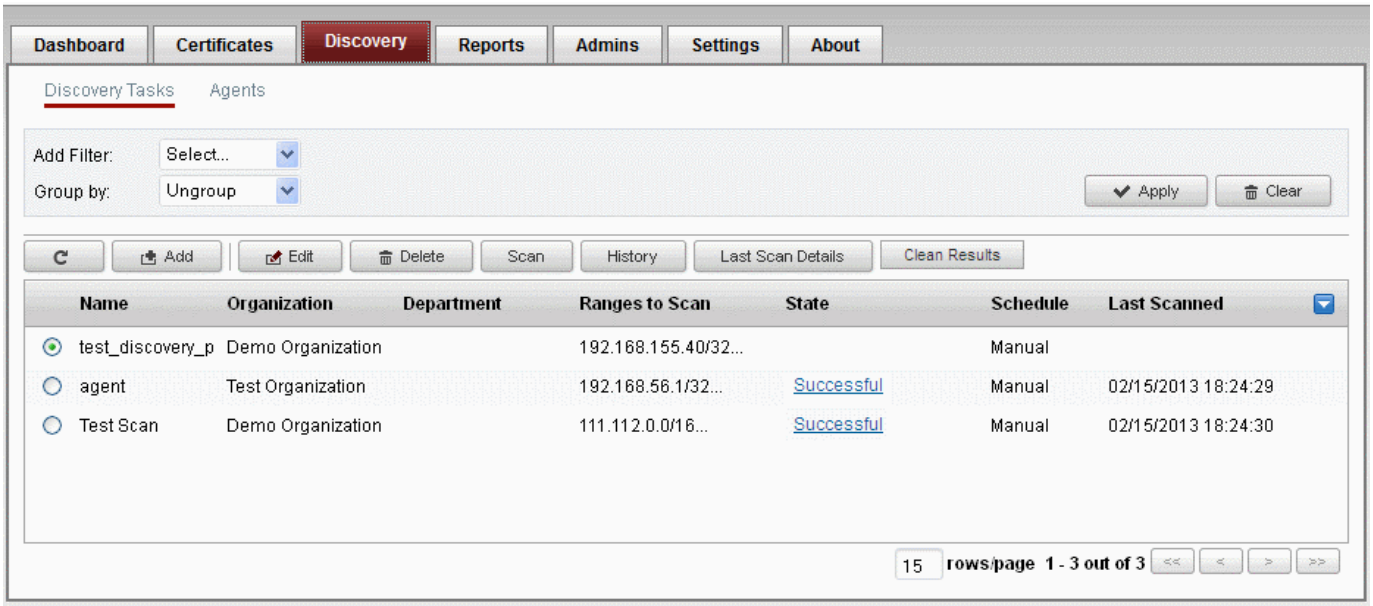
These sub-tabs are accessible according administrator security role privileges:

Security Role / Type of Administrator	Available Action
MRAO	Can access all areas and functionality of the section: has full visibility and control over all types of certificates.
RAO SSL	Can access all areas and functionality of the SSL Certificates section; has

Security Role / Type of Administrator	Available Action
	visibility and control over SSL Certificates belonging to their delegated Organization(s).
RAO SMIME	Can access all areas and functionality of the Client Certificates section; has visibility and control over client certificates and end-users belonging to their delegated Organization(s).
RAO Code Signing	Can access all areas and functionality of the Code Signing Certificates section; has visibility and control over Code Signing Certificates issued to end-users belonging to their delegated Organization(s).
DRAO SSL	Can access all areas and functionality of the SSL Certificates section; has visibility and control only over SSL Certificates belonging to belonging to their delegated Department(s).
DRAO SMIME	Can access all areas and functionality of the Client Certificates section; has visibility and control over client certificates and end-users belonging to their delegated Department(s).
DRAO Code Signing	Can access all areas and functionality of the Code Signing Certificates section; has visibility and control over Code Signing Certificates issued to end-users belonging to their delegated Department(s).

Click here for more information about the Certificates Management section.

Certificate Discovery and Agents: Comodo Certificate Manager uses Certificate Controller agent, a small piece of software that facilitates discovery of SSL certificates installed in the network and automatic request and installation of SSL certificates on remote servers. The Discovery area in the CCM interface enables the administrators to configure certificate controller agents for the network and to commence certificate discovery tasks. The scan results can be obtained from the Reports area.

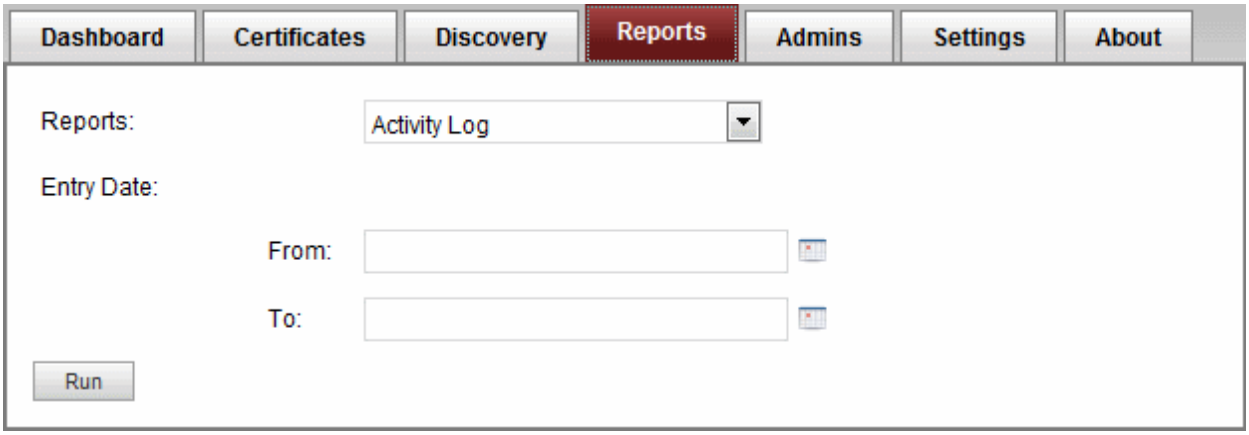


The 'Discovery' area is accessible only by MRAO, RAO SSL and RAO SSL administrators.

Security Role / Type of Administrator	Available Action
MRAO	Can set up agents for any organization and department and can scan for certificates requested, issued, expired, revoked and replaced for any Organization or Department.
RAO SSL	Can set up agents for and can scan for certificates requested, issued, expired, revoked and replaced for Organizations (and any sub-ordinate Departments) that have been delegated to them.
DRAO SSL	Can set up agents for and can scan for certificates requested, issued, expired, revoked and replaced only for the Department(s) that have been delegated to them.

Click here for more information about the Discovery section.

Report: Enables administrators to view a range of reports depending on their privilege level. The 'Reports' interface is fully explained in the Section '**Reports**'.

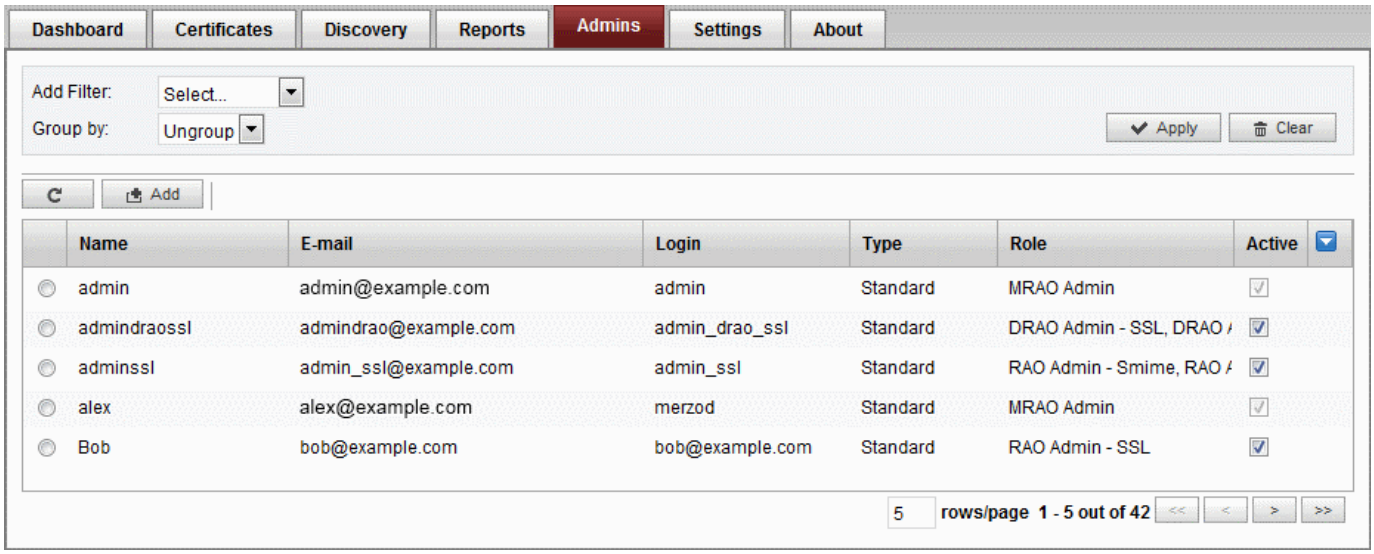


Available reports are 'Activity Log', 'Client Certificates', 'Discovery Scan Logs', 'SSL Certificates', 'Code Signing Certificates', 'Admins', XML Data, DCV Report and 'Notification Log Statistics'. The types of report available to a particular administrator is dependent on their security role:

Security Role / Type of Administrator	Available Action
MRAO	Can view all types of report for all Organizations and Departments • 'Activity' reports for any Organization and Department • 'Certificate Discovery' reports for any Organization and Department • Can view 'SSL', 'Client Certificates' and 'Code Signing Certificates' reports for any Organization and Department • 'Admin' reports for any Organization and Department • XML Data report for all the Organizations and Departments • 'DCV' report for any Organization and Department • 'Agent Log Events' for any Organization and Department
RAO SSL **RAO SMIME** **RAO Code Signing**	Can view: • 'Certificate Discovery' reports on scans that have been run on behalf of their delegated Organization(s) and Department(s) (Only

Security Role / Type of Administrator	Available Action
	RAO SSL Admins) • 'SSL / SMIME / Code Signing Certificate' report that is appropriate to their administrative type and for their Organization(s) and Department(s) only • 'DCV' report of their delegated Organization(s) and Department(s) (Only RAO SSL Admins)
DRAO SSL **DRAO SMIME** **DRAO Code Signing**	Can view: • 'Certificate Discovery' reports on scans that have been run on behalf of their delegated Department(s) (Only DRAO SSL Admins) • 'SSL / SMIME / Code Signing Certificate' report that is appropriate to their administrative type and for their Organization(s) and Department(s) only • 'DCV' report of their Department(s) (Only RAO SSL Admins)

Admin Management: Enables the currently logged-in administrator to view a list of administrative personnel. The 'Admin Management' interface is fully explained in Section **Admin Management**.



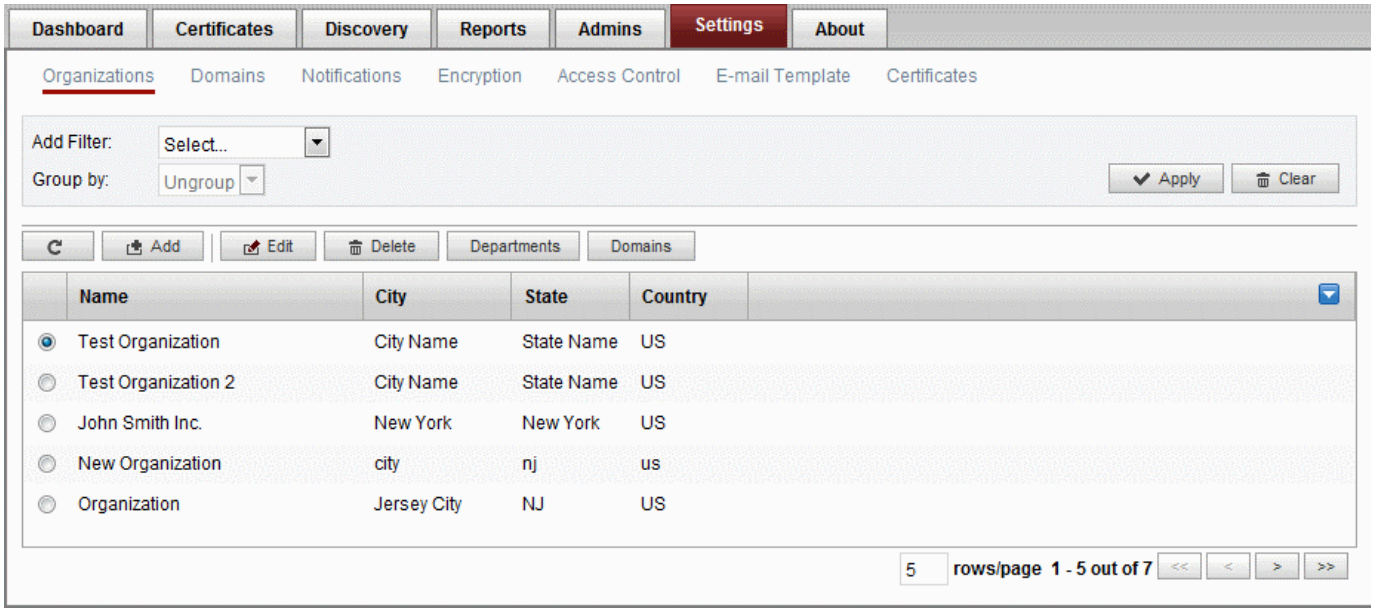
The visibility of other administrators and the availability of controls in this area is dependent on which type of administrator is currently logged in:

Security Role / Type of Administrator	Available Action
MRAO	Full visibility of all administrators across every Organization and Department. Can perform the following actions on administrators of any class or type: • View • Add/Delete • Edit • Approve/Reject

Security Role / Type of Administrator	Available Action
	• Activate/Deactivate
RAO SSL **RAO SMIME** **RAO Code Signing**	• View/Edit RAOs and DRAOs of their delegated Organization(s) and any subordinate Department(s) who are responsible for the same certificate type(s) as themselves • Request the creation of fellow RAOs who are responsible for the same certificate type(s) as themselves • Approve/Reject the creation of DRAOs who are responsible for the same certificate type(s) as themselves from.
DRAO SSL **DRAO SMIME** **DRAO Code Signing**	• View DRAOs of their delegated Department(s) who are responsible for the same certificate type(s) as themselves • Request the creation of fellow DRAOs who are responsible for the same certificate type(s) as themselves • Edit their own details

Click here for more information about Admin Management section.

Settings: The 'Settings' area contains several tabs relating to the overall configuration of CCM. The number of tabs that are visible to a particular administrator is dependent on their security role (MRAO, RAO or DRAO).



(1) **Organizations**: Visible only to MRAO and RAO class administrators. RAOs can view, edit, request new domains and add Departments to Organizations that have been delegated to them. MRAOs can view, edit, request new domains, create new Departments and delete any Organization or Department. MRAOs can initiate the process of validating organizations for the purpose of requesting and issuance of OV SSL certificates to organizations and departments under them.

(2) **Departments**: Visible only to DRAO class administrators. Allows DRAOs to view all Departments that have been delegated to them and to request new domains for those Departments.

(3) **Domains**: MRAOs can view all domains that have been requested or created; submit domain requests for validation, select the validation method, activate, deactivate, edit domains and delegate, a domain to any Organization or Department, delete a domain. 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.

(4) **Notifications**: Allows administrators to set up and manage email notifications to various personnel - including notifications triggered by SSL certificate status, notifications triggered by Client Certificate status and Discovery Scan Summaries.

(5) **Encryption**: Allows administrators to initialize a new master key pair or to re-encrypt the private keys of client certificates held in escrow.

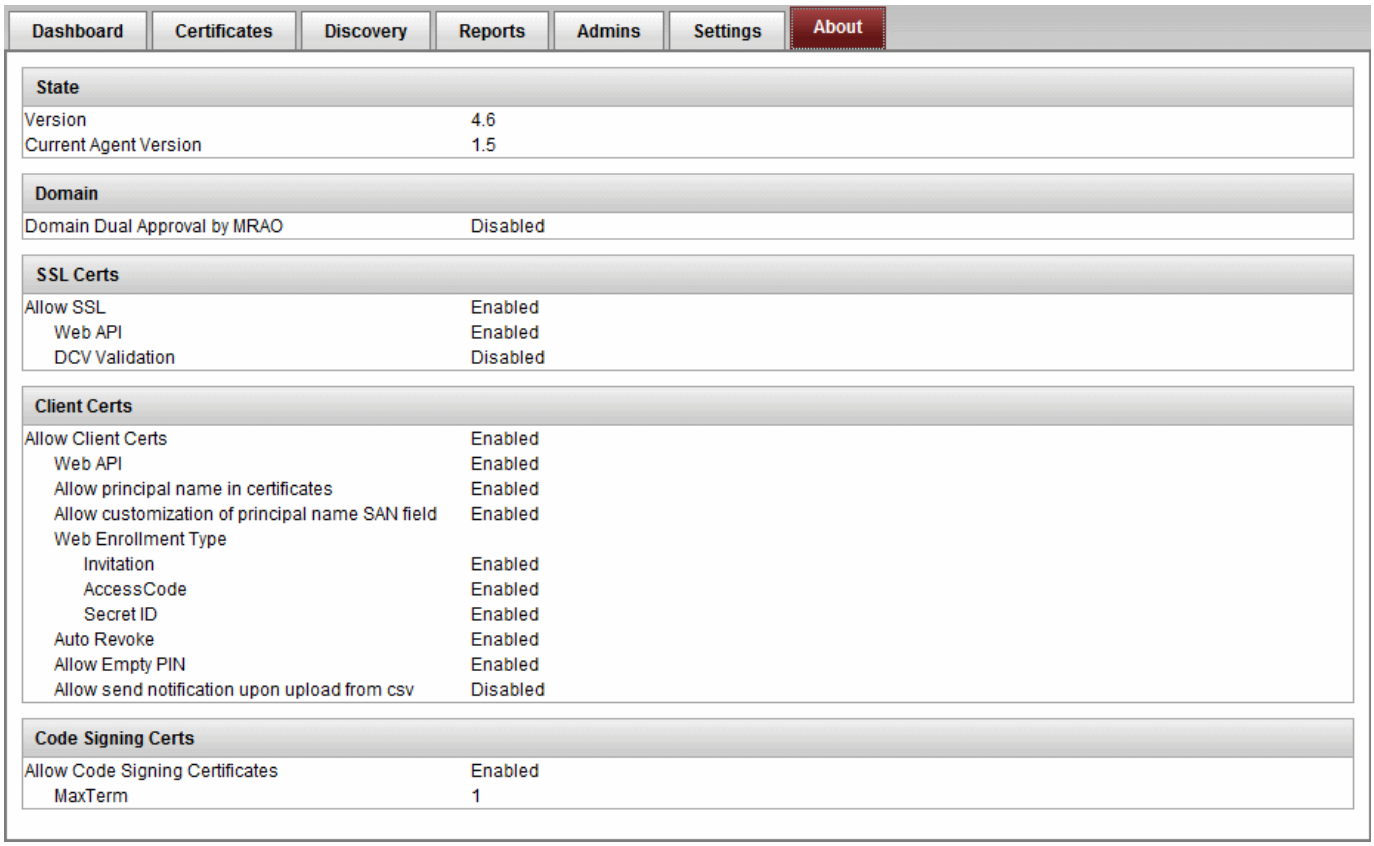
(6) **Access Control**: Allows the MRAO to grant access access to the CM login page only for specified IP range.

(7) **Certificates** - Allows MRAOs to customize the types and term lengths of SSL and Client certificates available through the Built-in application form and the Self Enrollment form. In addition to the standard fields that appear in the Built-in application form and the Self Enrollment form, MRAO admins can also configure to add additional custom fields in these forms.

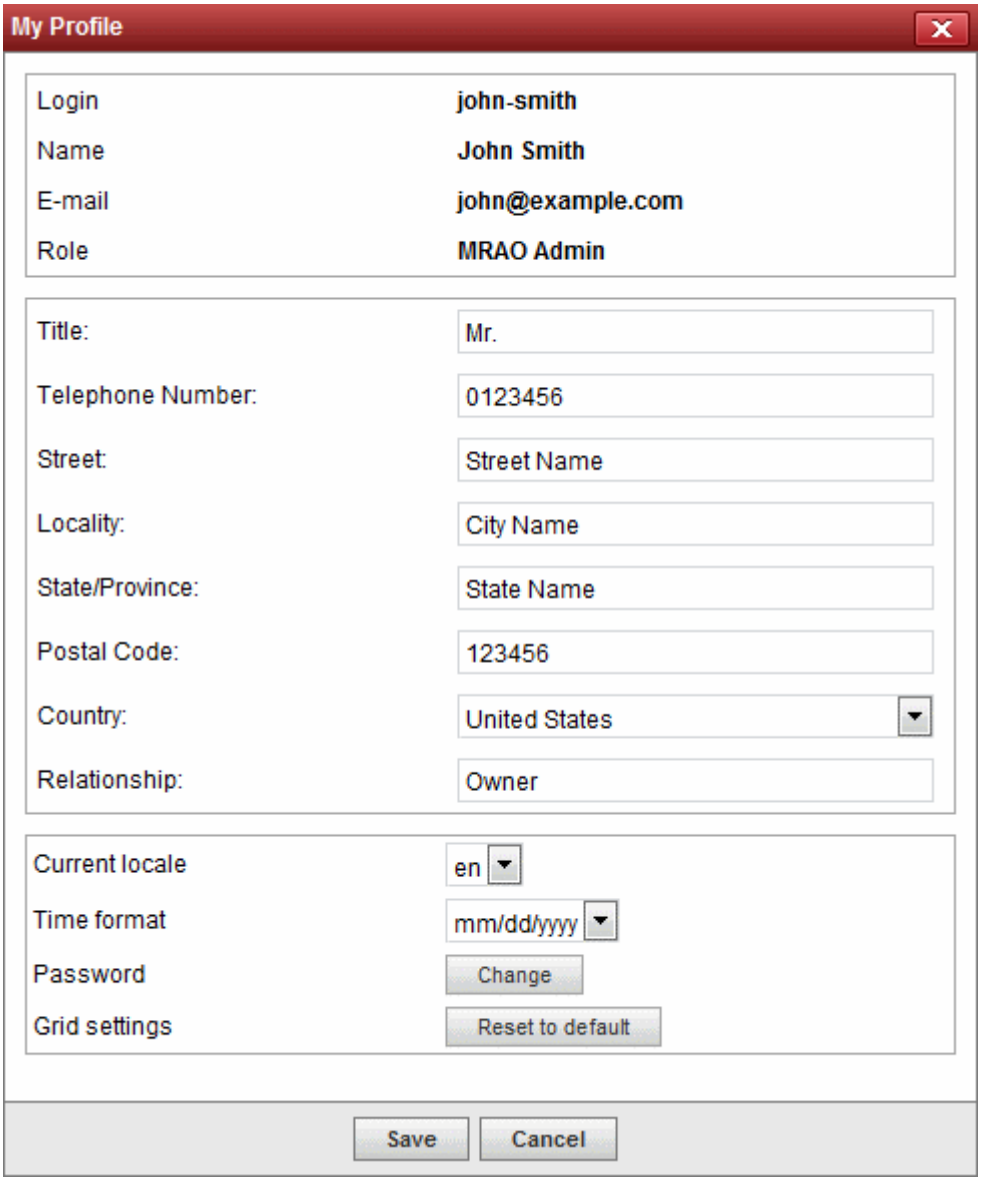
(8) **Email Templates**: Enables MRAO and RAO administrators to customize the content of templates for event-based email notifications. DRAO administrators can edit templates for their Department via the 'Edit Department' dialog (Settings > Departments > Edit)

Click here for more information about the 'Settings' area

About - Enables currently logged-in administrator to view the version of CCM and the features that are enabled and disabled for the account.



My Profile - Enables currently logged-in administrator to view/edit address details, change the interface language, time format and change password.



Logout: Logging out of Comodo Certificate Manager.

1.5 Release Notes

Version History	
Version Number	**List of Changes**
Version 4.6	• Added the new Dashboard feature with graphs and charts that allow the administrator to quickly gain an overview of all SSL, SMIME and code-signing certificates on the network.
Version 4.5	• Added a new report type 'Notification log Statistics' to enable MRAO administrators to generate and view logs of automated notification emails sent to other administrators during various events • Added ability to external applicants to renew their SSL certificates through

	self-renewal form, by entering their certificate ID and Pass Phrase. • Various bug fixes and UI improvements
Version 4.4	• Added new process of validating organizations for the issuance of OV SSL certificates • Improved the process of validating organizations for the quick issuance of EV SSL certificates. • Added ability to create domains without delegating them to organizations or departments. • Various bug fixes
Version 4.3	• Streamlined the DCV process for a faster validation. • Added ability to sort items in various interfaces by clicking the column headers • Added ability to search and filter certificates based on requester in SSL Certificates interface • Custom field data included for a certificate will continue on the renewal certificates too • Various bug fixes and several optimizations to improve the performance of the database and application server for improved stability
Version 4.2	• Added ability for MRAO administrators to add custom fields in the Built-in Application Form and Self-Enrollment Form for SSL and Client certificates requisition. • Various bug fixes

Version 4.1	• Introduced HTTPS method introduced in addition to HTTP.
	• Updated and improved SCEP support of iOS.
	• Enhanced the self-enrollment form, optimized to be used on iPhones. When a user wants to enroll and install a client certificate with the self-enrollment form, CCM presents an optimized page. After the enrollment process completes, the user can automatically install the certificate onto the iOS device.
	• Several UI improvements, including saving search filters. The filters configured for various iinterfaces will be saved and automatically applied when the same interface is opened again
	• Enabled auto installation feature for Apache Tomcat server. Version 4.1 supports auto-installation / auto-renewal for following platforms:
	  • Apache Web Server (Linux 32/64bit)
	  • IIS 7/7.5/8 (Windows 32/64)
	  • Apache Tomcat (Windows 32/64bit, Linux 32/64bit)
	• Various Bug Fixes

Version 4.0	• User Interface changes • Multiple certificate discovery tasks can be run at the same time • Agents will automatically check for newer versions and update itself

Version 2.11	• Added automatic installation and renewal of SSL certificates. This feature is enabled for accounts on a per-case basis. There are two available modes:
	  • Enterprise Controller Mode - Software installed on a local host will communicate directly with the CA issuance infrastructure to automatically apply for and install certificates on designated web-servers.
	  • Certificate Manager Controller mode - An agent is installed on each webserver which will communicate with CCM for certificate requests. If a request exists, the agent will generate a CSR and present it to the administrator for approval in the CCM interface.
	• Various Bug fixes

Version 2.10	• Added Auto-installation and Auto-renewal features for automatic SSL application, CSR generation, and certificate installation on IIS and Apache. • Various Bug fixes
Version 2.8.26	• Added functionality for scanning internal servers for installed certificates using Certificate Discovery (CD) Agent, installed in a local computer. • Various Bug Fixes
Version 2.8.25	• Added three methods EMAIL, HTTP file and DNS CNAME for Domain Control Validation (DCV) functionality to validate new and existing domains

Version 2.8.23	• Enhanced logging for system resources/usage statistics
	• Improved error handling/logging
	• Added a column 'External Requester' to SSL report
	• Improvements to the notifications system
	• **Bug Fixes:**
	  • Fixed bug whereby MRAO is sent 'Discovery Scan Summary' notification even though the Notify Master Admin(s) checkbox is not selected
	  • Fixed bug related to issue of SSL through Self-Enrollment Links for local hostnames
	  • Fixed bug whereby an administrator was not able to edit organization under certain circumstances
	  • RAO administrators can see only the client cert types that are allowed for them
	  • Fixed logo bug in IE 9.0 window
	  • Fixed bug related to invalid CSR common name
	  • Fixed issue related to mismatch of available notifications during Notification creation
	  • RAOs can set up a notification which notifies MRAOs
	  • Fixed bug related to incorrect timing of 'Your session has expired' messages
	  • Fixed bug whereby Domains are in a 'Suspended' state after an entry by RAO

Version 2.8.21.8	• The functionality Settings > Email Templates for editing templates of email messages corresponding to various events is restricted only to MRAO level Administrators
	• Domain creation/delegation requests approved by MRAO Administrators with privilege 'Allowing domain validation without Dual Approval' are activated immediately without requiring approval by a second MRAO.
	• Domains created by DRAO Administrators are to be approved by RAO of the Organization to which the department belongs prior to approval by MRAOs.
	• Added option to specify default Client Certificate Type(s) for all Organizations
	• Add 'Apply' button to Client Cert customization interfaces
	• **Bug Fixes:**
	  • All the server types are now available in the self-enrollment form for applying for SSL certificate.
	  • Administrators can now enroll for EV SSL Certificate manually
	  • Fixed issues related to Firefox version 4 Browser.
	  • Only the default Client Cert types customized for an organization are made visible in the self-enrollment forms.
	  • RAO and DRAO can send invitations for Client Certificates only for Certificate types allowed for their Organization
	  • SCEP Logs are improved

Version 2.8.21	• Added Key Usage Template (KUT) support to determine capabilities of Client Certificates of end-users belonging to an Organization.
	• Implemented Simple Certificate Enrollment Protocol (SCEP) support to Client Certificates in addition to SSL Certificates.
	• Subscriber's Agreements are made specific to the Certificate type selected while requesting for SSL Certificate and Code Signing Certificates.
	• **Bug Fixes:**
	  • Fixed bug whereby user can now enroll for Code Signing Certificates through Internet Explorer.
	  • Fixed bug whereby DRAO Administrators can request for SSL certificates from the management interface.
	  • Correct Subscriber Agreements are displayed on both built in application form and Self enrollment form according to Certificate type selected.
	  • Fixed bug to accept CSR of size less than 2048 bits for SSL Certificate replacement

Version 2.8.20	• 'Person upload' notification messages are now customizable; • 'Active' checkbox in 'Settings/Domains' is now, by default, always enabled for MRAO; • **Bug Fixes:** • Fixed bug whereby an MRAO could bypass 'dual domain auto approval' by using 'domain edit';

	• Fixed bug that sometimes allowed domains created by an MRAO to be automatically sent forward for validation without requiring approval from second MRAO; • Fixed bug where some notifications did not correspond to the modified E-mail Template; • Fixed bug that caused domain delegation requests to be displayed incorrectly; • Fixed occasional bug whereby an MRAO could modify their own privileges and/or those of a fellow MRAO; • Fixed occasional internal error that occurred when editing a deleted Administrator; • Fixed bug whereby an incorrect error would be displayed while importing from CSV; • Fixed Internal error that occurred when an RAO Admin tried to approve a Domain that had not yet been delegated by DRAO Admin; • Fixed bug that allowed Administrators to add and activate a domain for an Organization that has already been added to a Department; • Fixed bug whereby incorrect data was displayed in the domain details window; • Fixed bug whereby Client Certificate Administrators that were created in a certain manner were not made to follow password policy rules; • Fixed bug whereby variables could not be added via the 'Insert Variables' button while editing an email template in Internet Explorer; • Fixed bug whereby only active MRAO by changing admin role of another MRAO.

2 The Dashboard

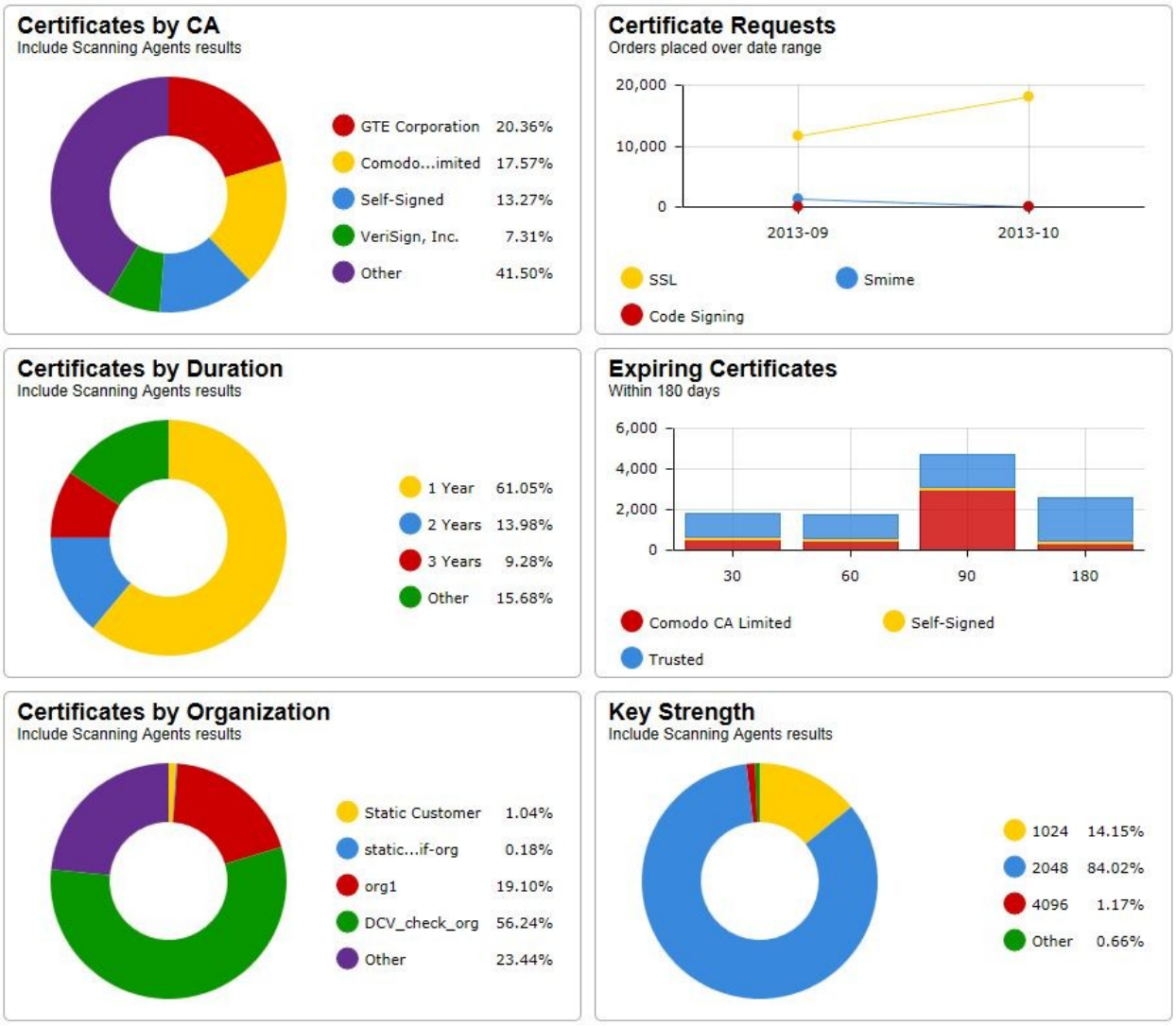
The CCM Dashboard will be displayed by default when an administrator first logs into the CCM interface. The dashboard provides a heads-up-display which allows you to quickly gain an overview of all SSL, SMIME and code-signing certificates on the network.

The charts and graphs in the dashboard provide an essential combination of key life-cycle information (such as certificates approaching expiry, certificates issued/requested and DCV status) as well as important technical insights like how many servers have support for perfect forward secrecy, renegotiation and RC4 suites.

Chart data is updated in real-time, so any modifications should be reflected in the dashboard near-instantly.

Security Roles:

- MRAO – can view charts for all certificate types, domains and web servers pertaining to all Organizations and Departments.
- RAO SSL, RAO SMIME and RAO Code Signing - can view charts relevant to the certificate types, domains and web servers of the Organizations (and any sub-ordinate Departments) that have been delegated to them.
- DRAO SSL, DRAO SMIME and DRAO Code Signing - can view the charts relevant to the certificate types, domains and web servers of the Departments that have been delegated to them.



The area at the top of the dashboard allows you to filter chart data and features a real-time summary of Active/Revoked certificates:

Filtering Options:

The statistics displayed in the dashboard can be filtered based on the time period and by Organization/Department:

- To add a filter, select the type of the filter from the 'Add Filter' drop-down. The available options are:
  - Organization – Choose an Organization / Department from the respective drop-downs and click 'Apply'.

- Time Period – Select the time period for which you wish to view statistics from the 'Time Period' drop-down and click 'Apply'.

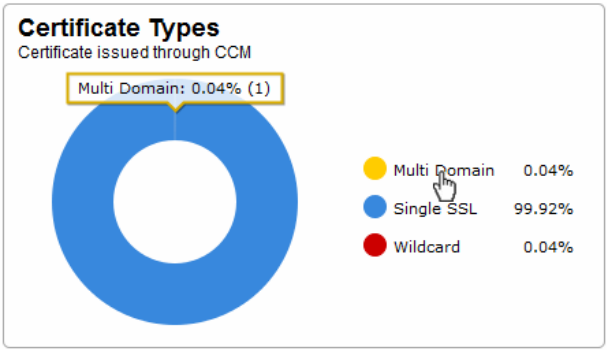
- To remove a filter, click the ' - ' button beside the filter.
- To reset the filters, click 'Clear'.

Charts available in first release. Click any link to view more details:

- **Certificates by Type** – Single Domain, Wildcard, Multi-Domain, UCC etc.
- **Certificates by Validation Level** – EV, DV, OV.
- **Certificates by Internal Type** – Certificates broken down by brand names like Instant SSL, Premium SSL etc.
- **Certificates by Issuer** – Comodo, VeriSign, GoDaddy, Thawte, self-signed etc.
- **Certificate Requests by Category of Certificate** – SSL requests, SMIME requests, Code signing requests
- **Certificate Requests versus Certificates Issued**
- **Certificates By Duration** – How many of your certificates are 1 year, 2 year, 3 year etc
- **Expiring Certificates by Issuer** – Comodo, self-signed and 'Other Trusted' certificates expiring within 180 days
- **DCV Status** – The current stage in the Domain Control Validation process held by your certificate-hosting domains
- **DCV Expiring Domains** – Domains for which Domain Control Validation will expire within 180 days
- **Certificates by Organization** - Certificates broken down by the Organizations they are issued to.
- **Certificates by Key Strength** - Certificates by the strength of key with which they were signed (1024 bit, 2048 bit etc)
- **Certificates by Public Key Algorithm** - Certificates broken down by encryption algorithm (RSA, DSA etc)
- **Certificates by Signing Algorithm** - Certificates by hashing and signing algorithms (e.g. SHA1withRSA)

Charts which are coming soon. Click any link to view more details:

- **EV Express Validation** – Organizations whose eligibility for accelerated EV validation will expire within 180 days.
- **Forward Secrecy** - The degree to which forward secrecy is supported on the web-servers hosting your certificates
- **Hosted by OS** - Details the server operating systems used to host your certificates (Windows, Linux etc)
- **RC4 Support -** The level of support for RC4 suites on the web-servers that host your certificates
- **Renegotiation Support** – The level of renegotiation support on the web-servers that host your certificates
- **Supported Protocols** – The types of encryption protocols supported by the web-servers that host your certificates
- **Certificates by port number** – The port numbers used for SSL traffic on the web-servers that host your certificates



Certificate Types

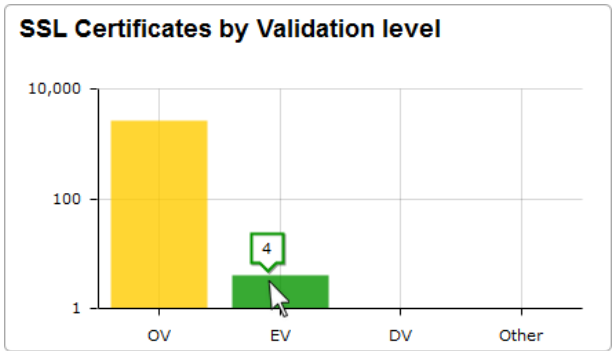
The 'Certificate Types' pie chart summarizes the different types of SSL certificates installed on servers in your network. (single domain, wildcard, multi-domain etc). This chart covers only 'managed' certificates issued through CCM.

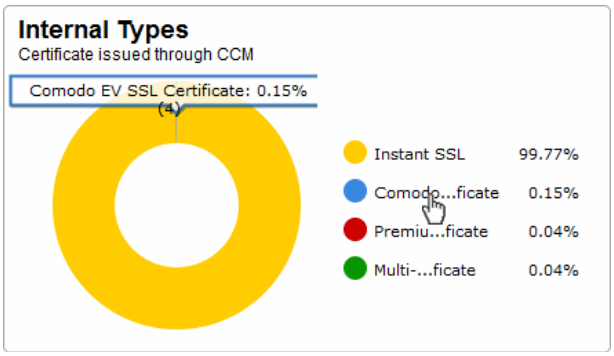
Hovering your mouse cursor over a legend item or section displays additional details such as the actual quantity of certificates of that type.

SSL Certificates by Validation level

Displays the composition of your certificate portfolio according to certificate validation level. This includes the number of Domain Validated, Organization Validated and Extended Validation certificates on your network.

Hovering the mouse cursor over a bar displays the exact number of certificates in that category.





Internal Types

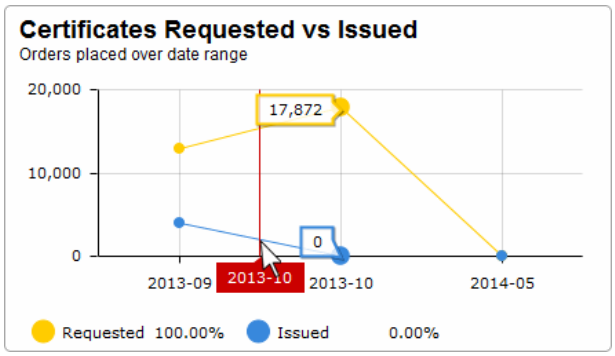
The 'Internal Types' chart details the quantities of SSL certificates issued by CCM according to certificate brand name.

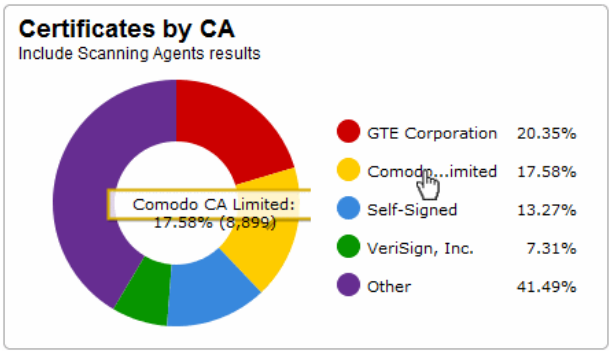
Hovering your mouse over a legend or sector displays additional details.

Certificates Requested Vs Issued

The 'Certificates Requested Vs Issued' graph allows you to view certificate issuance against certificate requests over time.

Placing the mouse cursor over the graph nodes displays more details about the number of certificates that were requested and issued on that date.





Certificates by CA

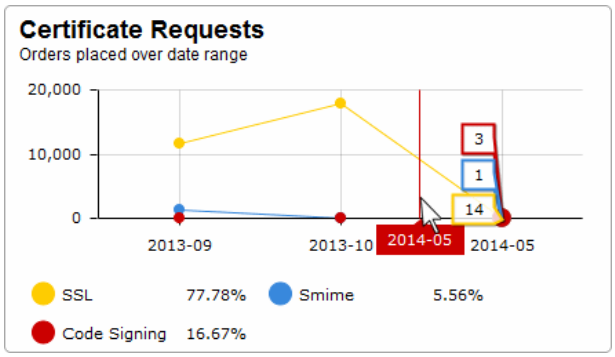
The 'Certificates by CA' chart allows you to determine what % of your certificates are publicly trusted by providing a break-down of certificates by signer. This includes all certificates signed by Certificate Authorities (CA) and those which are self-signed. It also highlights certificates from other CA's which you may want to replace with Comodo equivalents in order to benefit from CCM's management capabilities.

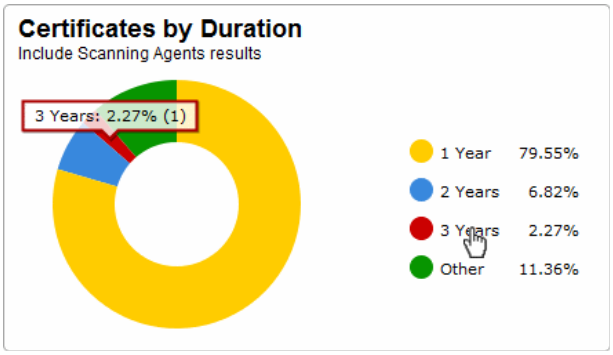
Placing your mouse cursor over a legend or sector displays the number of certificates by that signer and their % of the total certificates.

Certificate Requests

The 'Certificates Requests' graph displays the number of CCM orders placed over time for SSL, SMIME and Code Signing certificates.

Hovering the mouse cursor over the nodes on the graph displays the exact number of certificates that were requested.





Certificates by Duration

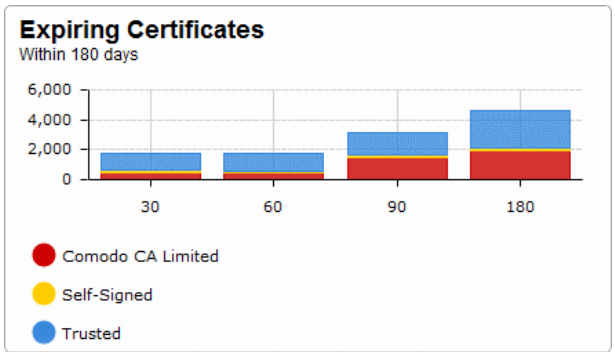
The 'Certificates by Duration' pie chart is a break-down of your certificates by term length.

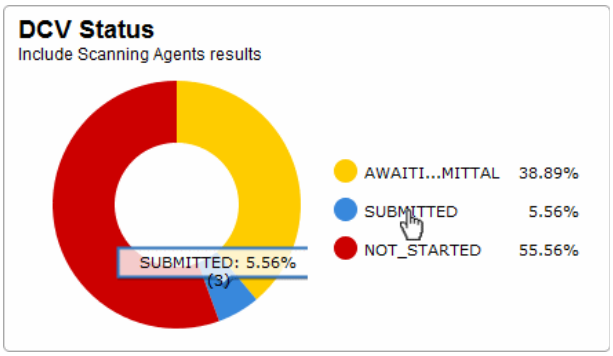
Hovering your mouse cursor over a legend or section displays the exact number of certificates with that term length and their percentage of the total.

Expiring Certificates

The 'Expiring Certificates' bar graph shows the number of certificates expiring within the next 30, 60, 90 and 180 days. Expiring certificates are further broken down according to signer. 'Trusted' certificates are those from other CAs which you may want to replace with Comodo certificates in order to benefit from CCM's management capabilities.

Hovering the mouse cursor over a legend or graph displays the number of certificates in each category.





DCV Status

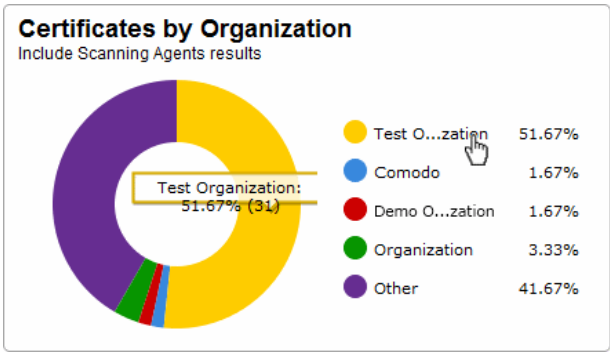
Summarizes the Domain Control Validation status of certificates on your network. DCV is required in order for Comodo to issue certificates to your domains and sub-domains. We advise customers to first pass DCV on their high level domain (e.g. domain.com). Once the HLD has passed DCV then future applications will be faster because all sub-domains, including wildcards, will be considered passed.

Hovering your mouse cursor over a legend or section displays the quantity of domains with a particular status and their percentage of the total domains.

DCV Expiring Domains

Indicates how many of your domains are within 30, 60, 90 and 180 days of DCV (domain control validation) expiry. DCV validity lasts for one year so It is possible DCV might be approaching expiry even though your certificate is not. If DCV is allowed to expire, it will not mean your certificate becomes invalid/stops functioning. However, your next application for that domain will need to pass DCV again.

Placing the mouse cursor over a legend or graph displays a tool-tip showing the number of domains within that time-frame.



Certificates by Organization

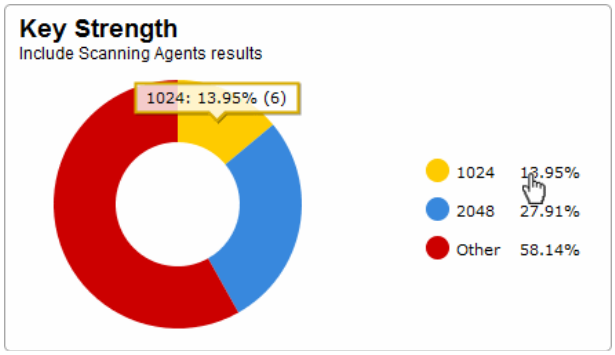
The 'Certificates by Organization' chart shows how many certificates have been issued to each Organization in your CCM account.

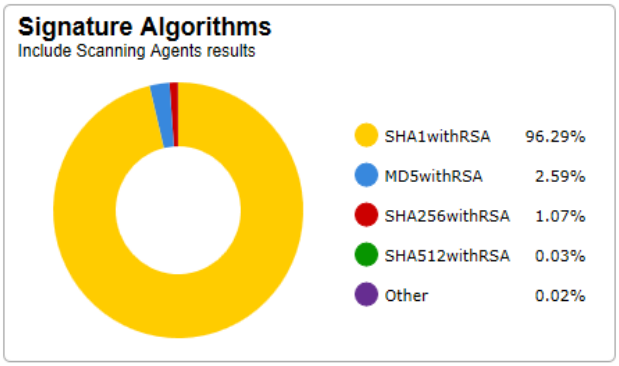
Hovering your mouse cursor over a legend or section displays the precise number and percentage of total certificates issued to to a particular Organization.

Key Strength

The 'Key Strength' chart shows the composition of your certificate portfolio based on the size of their signature. This can be useful for identifying certificates which need to replaced in order to be compliant with National Institute of Standards (NIST) recommendations. NIST has stated that all certificates issued after 1st January 2014 should be of at least 2048 bit key length

Placing your mouse cursor over a legend or sector displays the exact number of certificates with a particular signature size and their percentage of the total certificates.





Signature Algorithms

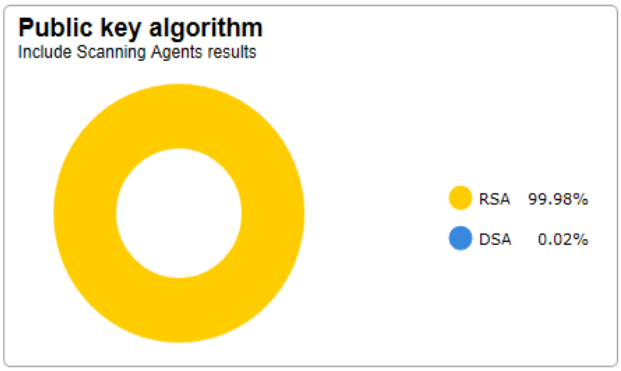
Provides an overview of the algorithms used by your certificates to hash and sign data. This chart can be useful for identifying certificates using weaker algorithms which may need to be replaced before their expiry dates. Comodo recommends SHA-256 and upwards. MD5 has been proven insecure and Microsoft has stated its products will stop trusting SHA-1 code-signing and SSL certificates in 2016 and 2017 respectively.

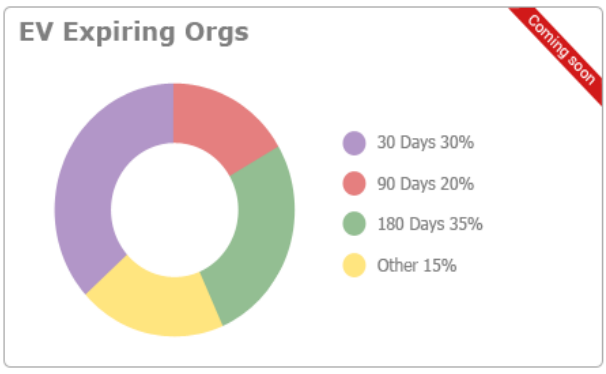
For more details, see **http://www.comodo.com/e-commerce/SHA-2-transition.php**

Public Key Algorithm

This chart provides an overview of the algorithms used to encrypt data by certificates on your network. Example algorithms include RSA, DSA and ECC.

Placing your mouse cursor over a legend or sector displays the exact number of certificates using a particular signature algorithm and their percentage of the total certificates.



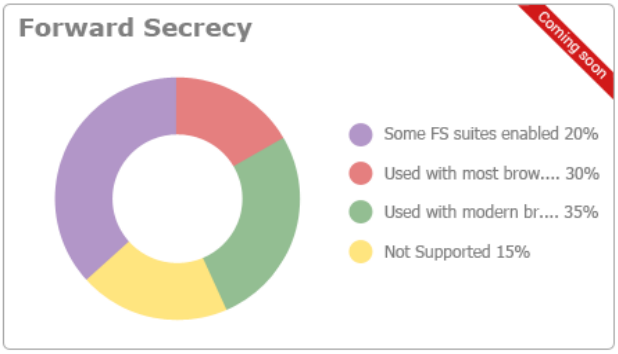


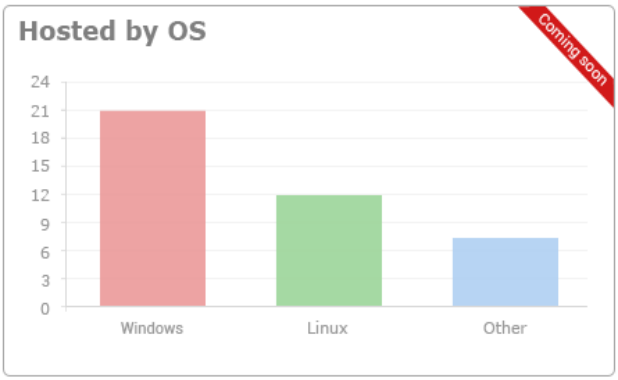
EV Express Validation – coming soon

Displays the percentage of Organizations for which accelerated validation of one or more EV certificates will expire within 30, 90 and 180 days. Once an EV certificate has been validated for the high level domain (e.g. domain.com) it qualifies for EV Express and subsequent EV applications for that domain and it's sub-domains will be issued much more quickly (assuming address and contact details are not changed). EV Express status lasts for 13 months before it must be renewed by re-validating the details of the certificate on the high level domain.

Forward Secrecy Enabled – coming soon

Displays the percentage of certificates which are hosted on web-servers which have perfect forward secrecy fully or partially enabled. Forward secrecy prevents encrypted data from previous sessions from being decrypted in the event that the private key of the certificate is compromised.



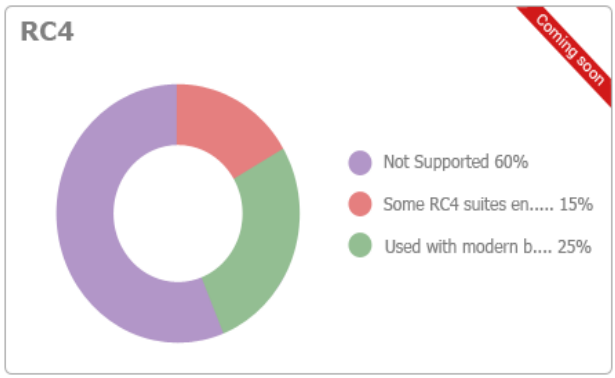


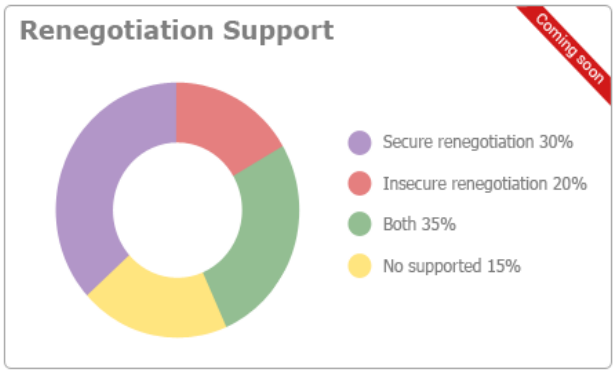
Hosted by OS – coming soon

Provides a visual break-down of the server operating systems used to host your certificates.

RC4 Support – coming soon

Indicates the degree to which the RC4 streaming cipher is supported by servers hosting your certificates. If your environment can operate without RC4, it is best practice to disable it.





Renegotiation Support – coming soon

Renegotiation is a feature that makes it possible to adjust the parameters of an SSL connection without disrupting the user experience by requiring an entirely new session. Take, for example, the case of an anonymous user browsing an e-commerce website who adds some products to the shopping cart then decides to login and purchase. Renegotiation allows the data from the 'anonymous' session to be transposed in a fluid and secure fashion. Unfortunately, security flaws were discovered in renegotiation in TLS 1 / SSL 3 which required a patch to fix. Unpatched web servers are shown here as 'Insecure renegotiation'.

Supported Protocols – coming soon

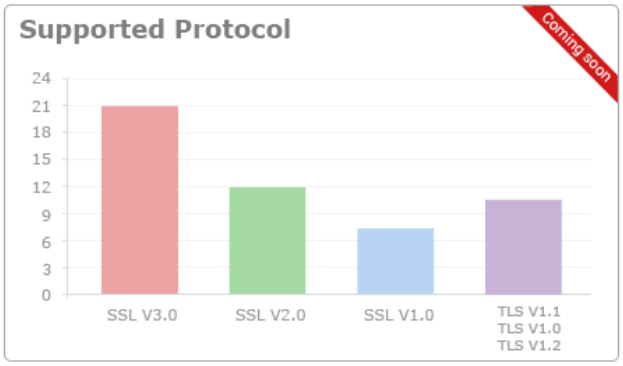
Shows the support for various cryptographic protocols on the web servers which are used to host your certificates. While we recommend each customer to investigate the precise impact of disabling a given protocol by analyzing the browsers used by their visitors, Comodo would recommend the following:

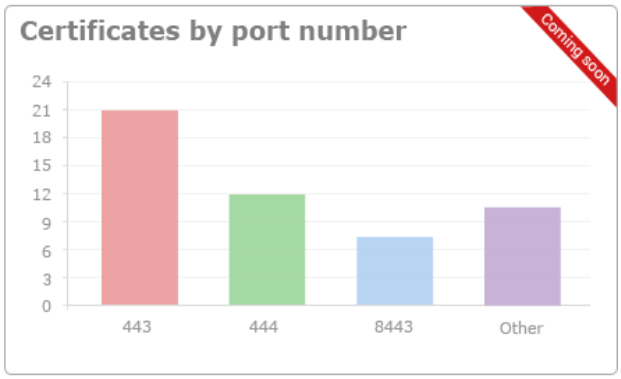
TLS 1.0, 1.1, 1.2 – Enable

SSL 3.0 – Discretionary. Disable preferred *

SSL 1.0. 2.0 – Disable

* SSL 3.0 is needed mainly for Windows XP / Internet Explorer 6.0 users. Microsoft have discontinued support for these systems and their use by the public has waned significantly. However, CCM customers *may* want to retain support in the short-medium term if widely supported by their user base.





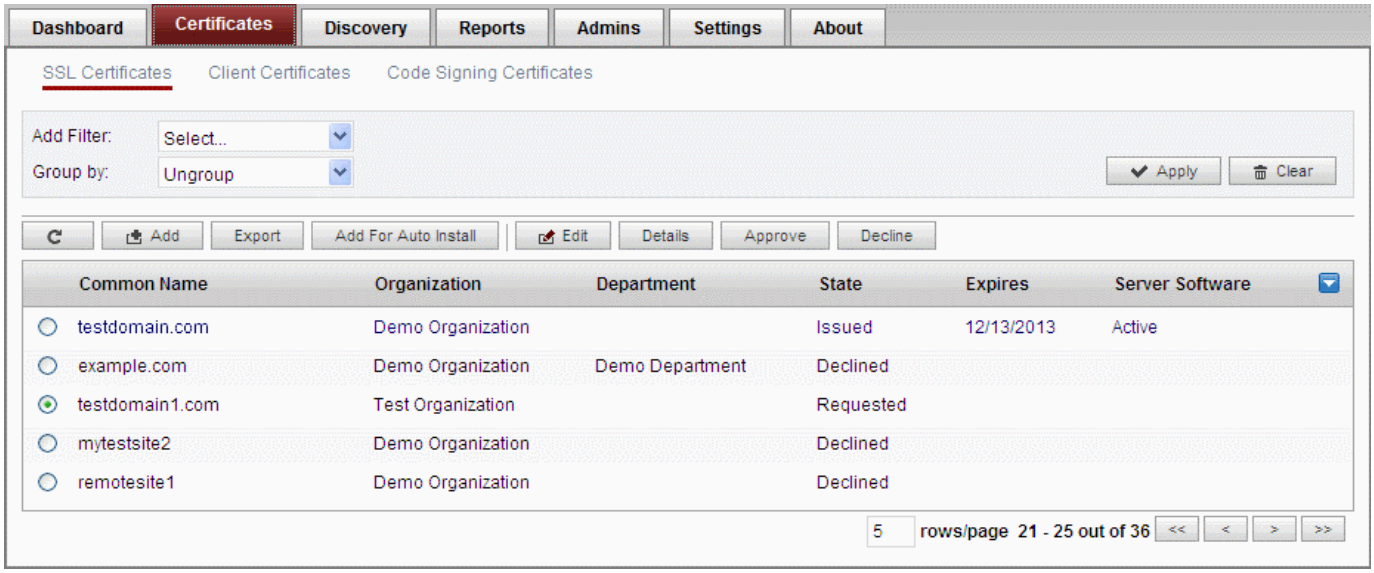
Certificates by port number – coming soon

Shows the port numbers that are used for secure connections on web-servers that host your certificates.

3 Certificates Management

The Certificates Management tab provides appropriately privileged administrators with the ability to request, collect, revoke and manage SSL, Client and Code Signing certificates.

It is divided into three main administrative areas, namely the SSL Certificates tab, the Client Certificates tab and the Code Signing Certificates tab.



This chapter provides guidance on the Certificates Management interface and explains the processes behind the administration and provisioning of SSL certificates, client certificates and code signing certificates. This chapter is divided into the following sections:

3.1 The SSL Certificates area - High level introduction to the SSL interface. Contains brief explanations of functionality and an

overview of Comodo SSL certificate types.

3.1.2 Request and Issuance of SSL Certificates to Web Servers and Hosts - Detailed explanations of the entire application, provisioning and life management of SSL web server certificates.

3.2 The Client Certificates area - Introduction to the Client Certificate interface that covers basic interface functionality and the creation, import and management of certificate end-users.

3.2.5 Request and Issuance of Client Certificates to Employees and End-Users - Detailed explanations of the initiation, application, provisioning, collection and management of Client Certificates.

3.3 The Code Signing Certificates area - Introduction to the Code Sign Certificate interface that covers basic interface functionality and the application, import and management of code signing certificates.

3.3.4 Request and Issuance of Code Signing Certificates - Explains the initiation, application, requisition, collection and management of Code Signing Certificates.

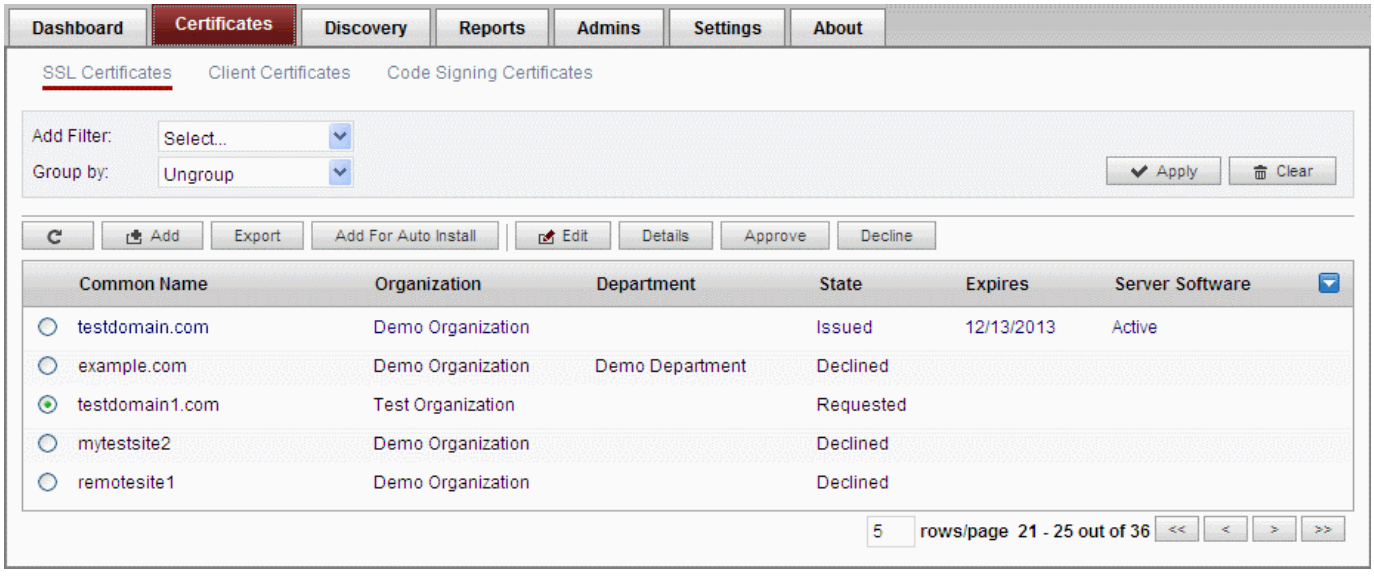
Note: Administrators can also run a 'Discovery Scan' on their servers which will audit and monitor their entire network for all installed SSL certificates (including certificates issued by other vendors). Once completed, all discovered certificates are automatically imported into the 'Certificates Management' area. This feature is covered in greater detail in the **Certificate Discovery** section of this guide.

3.1 SSL Certificates Area

3.1.1 Overview of the Interface

The SSL Certificates Area provides MRAOs and nominated RAO / DRAO SSL administrators with the information and controls necessary to manage the life-cycle of SSL certificates for an Organization.

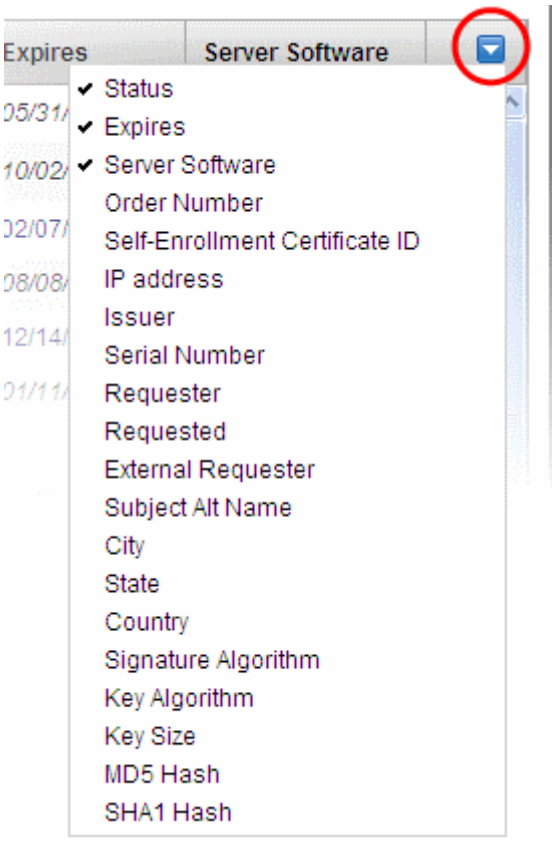
- MRAOs can request and manage SSL certificates for any Organization/Department. Can approve or decline certificate requests made for automatic installation and using the external application form for any Organization or Department.
- RAO SSL admins can request and manage certificates for their delegated Organization(s). Can approve or decline certificate requests made for automatic installation and using the external application form for their Organization.
- DRAO SSL admins can request SSL certificates for domains belonging to their delegated Department(s). Can approve or decline certificate requests made for automatic installation and using the external application form for their Organization.



Note: The SSL Certificates area is visible only to MRAO Administrators and RAO / DRAO SSL administrators. For more details refer to **1.2.3 Administrative Roles**.

SSL Certificates Sub-tab - Table of Parameters		
Column		**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.
Organization		Name of the Organization that requested or has been issued with the certificate listed in the 'Common Name' column.
Department		Indicates the specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity.
Status		Indicates the current status of the certificate.
	Requested	The 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, his/her request appears in the 'SSL Certificates' sub-tab with a 'Requested' state. The Administrator can "View", "Edit", "Approve" or "Decline" this request. A certificate can be requested by • An applicant using the **Self Enrollment Form**. • An MRAO - for any Organization or Department - using **Auto Installation feature**, **Self Enrollment Form** or the **Built In Application Form** • An RAO SSL administrator- for Organizations and Departments which they have been delegated control. Can use **Auto Installation feature**, **Self Enrollment Form** or the **Built In Application Form** • A DRAO SSL administrator - for Departments of an Organization which they have been delegated control. Can use **Auto Installation feature**, **Self Enrollment Form** or the **Built In Application Form**
	Approved	A certificate request that was made using the **Auto Installation feature** or the **Self Enrollment Form** has been approved by one of the following: • An MRAO • An RAO SSL administrator of the Organization on whose behalf the request was made. • A DRAO SSL administrator of the Department on whose behalf the request was made.
	Applied	The request has been sent to the Certificate Authority (CA) for validation. In order to accelerate the validation process, the administrator can request the domain control administrator to complete the domain control validation process, through out-of-band communication like email, if the response for DCV is not received for long time.
	Issued (number of found certificates)	The certificate was issued by CA and collected by Certificate Manager. A Blue font color (Issued) means that the certificate was issued by CA but was not installed. Placing the mouse cursor over the '**Common Name**' will display the name of the Vendor that is associated with this certificate. A number in parentheses to the right of the certificate's status indicates how many servers this specific certificate is installed upon. Placing the mouse cursor over the '**State**' column will display all the *IP address / Port* combinations that this certificate was found on.
	Expired	The certificate is invalid because its term has expired. Placing the mouse cursor over the '**Common Name**' will display the name of the Vendor that is associated with this certificate. A number in parentheses to the right of the certificate's status indicates how many servers this specific certificate is installed upon. Placing the mouse cursor over the '**State**' column will display all the *IP address / Port* combinations that this certificate was found on and will display a certificate expired warning.
	Revoked	The certificate is invalid because it has been revoked. Placing the mouse cursor over the

SSL Certificates Sub-tab - Table of Parameters		
Column		**Description**
		'**Common Name**' will display the name of the Vendor that is associated with this certificate. A number in parentheses to the right of the certificate's status indicates how many servers this specific certificate is installed upon. Placing the mouse cursor over the '**State**' column will display all the *IP address / Port* combinations that this certificate was found on and will display a certificate revoked warning.
	Declined	A certificate request that was made using the **Self Enrollment Form** or the **Built-in Application Form** has been rejected by one of the following: • An MRAO - can decline any certificate requests from any Organization or Department • An RAO SSL administrator can decline certificate requests for Organizations over which they have been delegated control. • An DRAO SSL administrator can decline certificate requests for Departments over which they have been delegated control.
	Invalid	The Certificate Authority did NOT process the certificate request because of an error the applicant made in the enrollment form (e.g. CSR contains incorrect details).
	Rejected	The Certificate Authority rejected the request after a validation check.
	Unmanaged (n - number of found certificates)	This state applies to certificates that were detected by a network **Discovery Scan** but were NOT ordered and issued through Comodo Certificate Manager (including any pre-existing Comodo certificates that may have been ordered from the website or partner API's). The red color *(Unmanaged)* indicates, that he certificate's term has expired. Placing the mouse cursor over the '**Common Name**' will display the name of the Vendor that is associated with this certificate. A number in parentheses to the right of the certificate's status indicates how many servers this specific certificate is installed upon. Placing the mouse cursor over the '**State**' column will display all the *IP address / Port* combinations that this certificate was found on.
Expires		Expiration term of the certificate.
Server Software		Indicates the current status of the server on which the certificate is auto- installed.
	Blank	The server is not configured for Auto-Installation and Auto-Renewal
	Active	The server is configured for Auto-Installation and Auto-Renewal
	Error	Indicates that errors generated during the server configuration or automatic certificate installation.
	Restart Required	Indicates that the server has to be restarted after automatic installation of a certificate by CCM. The installation will be active only on next restart of the server. **Note**: Restarting the server after automatic certificate installation is required only for Apache. The server can be restarted from the Certificate Details dialog. For more details please see the section **Restarting Apache after Auto-Installation of SSL Certificate**.
Note: The administrator can add more column headers from the drop-down button beside the last item in the column:		

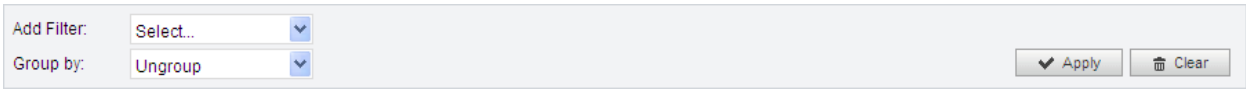
SSL Certificates Sub-tab - Table of Parameters		
Column		**Description**
		
Order Number		The order number of the certificate request as assigned by the Certificate Authority, when the request was made.
Self Enrollment Certificate ID		Displays the unique enrollment ID assigned to the certificate request, If the certificate was obtained by self enrollment by the domain administrator.
IP address		Displays all the IP address / Port combinations on which the certificate is installed.
Issuer		Displays the details of the Certificate Authority that issued the certificate and the name of the certificate.
Serial Number		Displays the serial number of the certificate that is unique and can be used to identify the certificate.
Requester		Displays the name of the CCM administrator that has requested the certificate through the auto-install feature or the built-in enrollment form, or e-mail of end-user that has requested the certificate through the self-enrollment form.
Requested		Displays the date of the certificate request.
External Requester		Displays the the email address of the external requester on behalf of whom the administrator has requested the certificate through the built-in enrollment form.
Subject Alt Name		Displays the names of domain(s) for which the certificate is used for.
City		Displays the name of the city entered while creating the Organization / Department.
Country		Displays the name of the country entered while creating the Organization / Department.

SSL Certificates Sub-tab - Table of Parameters		
Column		**Description**
Key Algorithm		Displays the type of algorithm used for the encryption.
Key Size		Displays the key size used by certificate for the encryption.
MD5 Hash		Displays the MD5 hash for the certificate
SHA1 Hash		Displays the SHA1 hash for the certificate
Control Buttons **Note:** The type of control buttons that are displayed above the column header depends on the state of the selected certificate	Details	Allows the administrator to view information about the certificate (see **SSL certificate 'Details' dialog** description).
	Revoke	Revokes the certificate.
	Install	Uses the auto-installer feature to install the certificate on the target web server. See the section **Automatic Installation and Renewal** for more details.
	Replace	Replaces the existing certificate with a new one. **Note:** You will be prompted to specify new CSR.
	Approve	Approves certificate requests that were made for Auto Installation and using the **auto-installation feature** or the **Self Enrollment Form** and sends the request for the certificate to Comodo CA (the issuing Certificate Authority). Once submitted, the certificate State will change to 'Applied'. If the request is approved by Comodo CA, the certificate State changes to 'Issued'. If the request was declined by Comodo CA because of incorrect enrollment details (for example, a mistake in the CSR or other form value), then 'State' will be listed 'Invalid'. If the request was declined by Comodo CA for legal reasons then the certificate will have a status of 'Rejected'. Certificate requests can be approved by: • An MRAO • An RAO SSL administrator of the Organization on whose behalf the request was made. • A DRAO SSL administrator of the Department on whose behalf the request was made
	Decline	Declines the certificate request. This request will not be sent to Comodo Certificate Authority for processing.
	Edit	Enables administrator to edit SSL certificate parameters. This option is available only for certificates with a state of 'Requested', 'Rejected' or 'Invalid'.
	Renew	Clicking the 'Renew' button will open the 'Renew Certificate' dialog which will be pre-populated with the company and domain details of the existing certificate. Clicking 'OK' will submit the certificate renewal request. This control is available only for the certificates states of: Issued, Expired and Unmanaged.

3.1.1.1 Sorting and Filtering Options

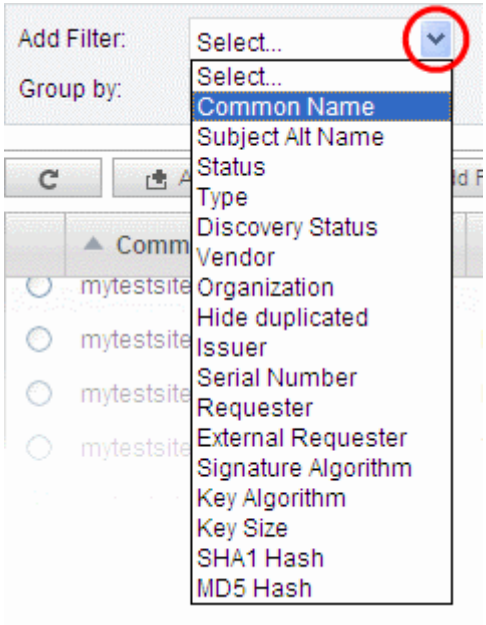
- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for particular SSL certificates by adding filters.

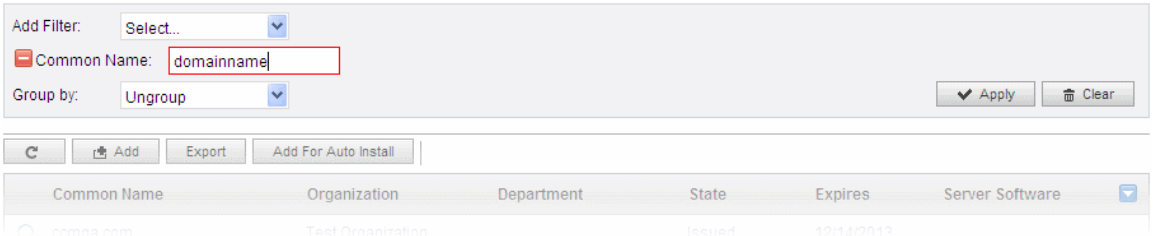


To add a filter

- Select a filter criteria from the 'Add Filter' drop-down



- Enter or select the filter parameter as per the selected criteria.



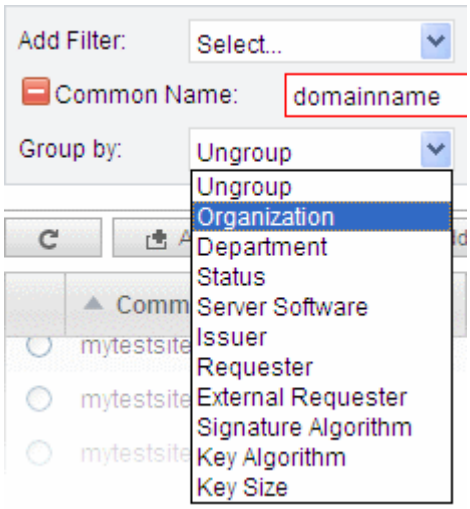
The available filter criteria and their filter parameters are given in the following table:

Filter Criteria	Filter Parameter
Common Name	Enter the common name or domain name for the certificate fully or in part
Subject Alt Name	Enter the subject alternative name for the certificate fully or in part
Status	Choose the state of the certificate from the 'Status' drop-down
Type	Choose the type of the certificate from the 'Type' drop-down
Discovery Status	Choose the status, that is whether the certificate is deployed or not from the 'Discovery Status' drop-down
Vendor	Select the vendor of the certificate (CA) from the Vendor drop-down.
Organization	Select the Organization and/or the department to which the certificate belongs, from the 'Organization' and 'Department' drop-downs.
Hide Duplicated	Choose Hide Duplicated if you want duplicate certificates are not to be listed and select the 'Hide duplicated' check box.
Issuer	Enter the name of the issuer of the certificate
Serial Number	Enter the serial number of the certificate in full or part.
Requester	Enter the name of the CCM administrator that has requested

	the certificate through the auto-install feature or the built-in enrollment form, or e-mail of end-user that has requested the certificate through the self-enrollment form, in full or part.
External Requester	Enter the email address of the external requester on behalf of whom the administrator has requested the certificate through the built-in enrollment form, in full or part.
Signature Algorithm	Enter the signature algorithm of the certificate
Key Algorithm	Enter the key algorithm of the certificate
Key Size	Enter the key size in bits
SHA1 Hash	Enter the SHA1 Hash of the certificate
MD5 Hash	Enter the MD5 Hash of the certificate

Tip: You can add more than one filter at a time to narrow down the filtering. To remove a filter criteria, click the '-' button to the left if it.

- Select the criteria by which the results are to be grouped from the 'Group by' drop-down and enter or select the grouping parameter



For example, if you want to filter the certificates with a specific Common Name starting with 'mytestsite' and group the results by their 'Status', then select 'Common Name' from the 'Add Filter' drop-down, enter mytestsite and select 'State' from the 'Group by' drop-down. The certificates, having 'mytestsite' in their common name will be displayed as a list, grouped based on their 'state'.

Common Name	Organization	Department	State	Expires	Server Software	SHA1 H
Requested						
mytestsite1	Demo Organization		Requested			
mytestsite2	Demo Organization		Requested			
mytestsite1	Test Organization		Requested			
mytestsite1	Test Organization		Requested			
mytestsite1	Demo Organization		Requested			
mytestsite1	Demo Organization		Requested			
mytestsite1	Test Organization		Requested			
Declined						
mytestsite2	Demo Organization		Declined			
Issued						
mytestsite1	Test Organization		Issued	02/05/2014		

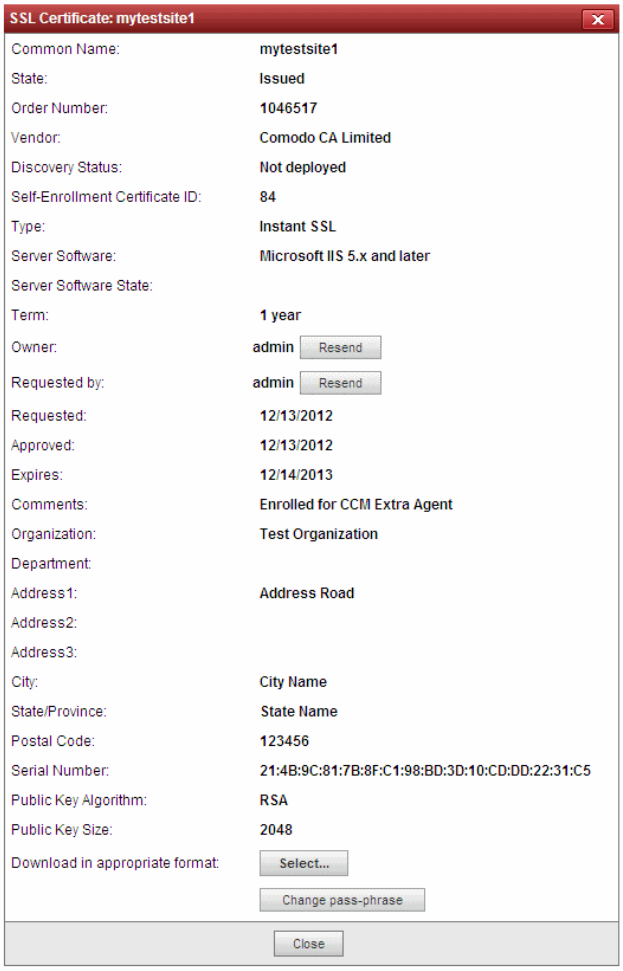
- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'SSL certificates' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

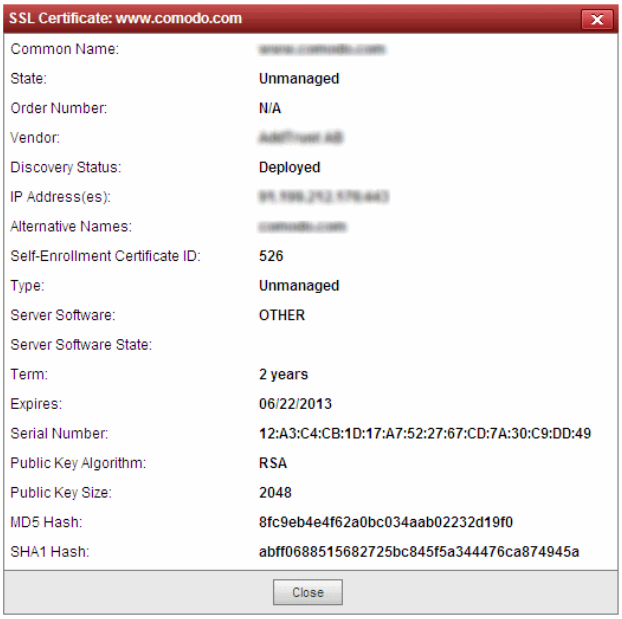
3.1.1.2 SSL Certificate 'Details' Dialog

Clicking the 'Details' button after selecting a certificate listed in the SSL Certificates tab will open a panel containing a summary of that certificate's details. The precise contents of the 'Details' dialog is dependent on the current 'State' of the certificate:

SSL Certificate with the state 'Issued'



SSL Certificate with the state 'Unmanaged'



SSL Certificates 'Details' Dialog - Table of Parameters		
Field	**Type**	**Description**
Common Name	Text Field	The domain name that was used during the SSL certificate request. This domain name refers to the 'Common Name' in the SSL certificate itself.
State	Text Field	State of the certificate (for the definitions see on the table **above**).
Order Number	Text Field	Order number of the certificate request.
Vendor	Text Field	A vendor that is associated with the certificate. The vendor for self-signed SSL certificates is '**Self-Signed**'.
Discovery Status	Text Field	There are two possible values: **Not Deployed** and **Deployed**.

SSL Certificates 'Details' Dialog - Table of Parameters		
Field	**Type**	**Description**
		• **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	Text Field	Displays the unique ID of the certificate.
Type	Text Field	Type of the certificate.
Server Software	Text Field	Indicates the server type to which the certificate was issued.
Server Software State	Text Field	Indicates the state of the server on which the certificate is installed. (For the definitions see on **the table above**).
Term	Text Field	The length of time the certificate is (or will be) valid for 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	Text Field	Name of the 'Owner' of the certificate. The Owner of the certificate is the Administrator that first approved the request for the certificate.
Requested by	Text Field	Displays either: • The email address of the end-user that requested this certificate using the Self Enrollment Application form or • The name of the administrator that requested this certificate using the auto-install feature or the Built-In Application form.
Requested	Text Field	Date that the certificate was requested.
Approved	Text Field	Date that the certificate was approved.
Expires	Text Field	Date that the certificate expires.
Comments ***(optional)***	Text Field	Information for administrator.
Organization	Text Field	Name of the Organization on behalf of which the certificate was requested
Department	Text Field	Name of the Department on behalf of which the certificate was requested
Address 1: Address 2: Address 3: City: State or Province: Postal Code:	Text Fields	Displays the address of the Organization as mentioned while requesting for the certificate. Only those address fields that were allowed to be displayed while applying for the certificate are shown here and the rest of the fields are displayed as "Details Omitted".
Serial Number	Text Field	Indicates the serial number of the certificate issued.
Public Key Algorithm	Text Field	Displays the encryption algorithm of the public key of the certificate
Public Key Size	Text Field	Displays the key length of the public key in bits
Revoked	Text Field	Date that the certificate was revoked (if applicable.)

SSL Certificates 'Details' Dialog - Table of Parameters		
Field	**Type**	**Description**
Download in appropriate format	Control	Allows the administrator to download the certificate in different formats.
Change Pass Phrase	Control	This phrase is required to revoke certificates should the situation arise
Close	Control	Closes the dialog.

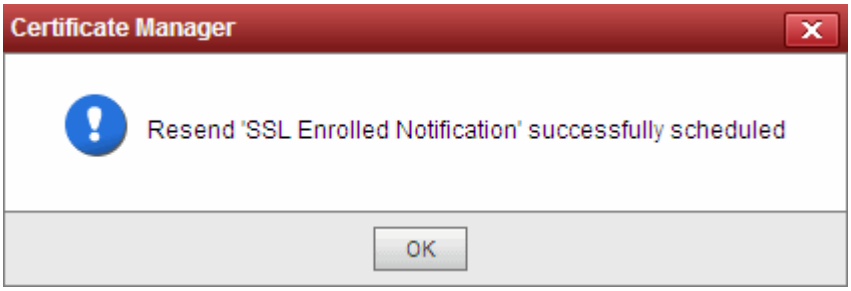
3.1.1.2.1 Resending Notification Email for Certs with 'Issued' State

The 'Details' dialog for SSL certificates with 'Issued' state allows the administrator to resend the 'Certificate Enrolled' notification to the domain control administrator.

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

- The 'Details' dialog for the SSL certificate with the Issued state, displays a 'Resend' button beside the Owner and Requested by: fields.

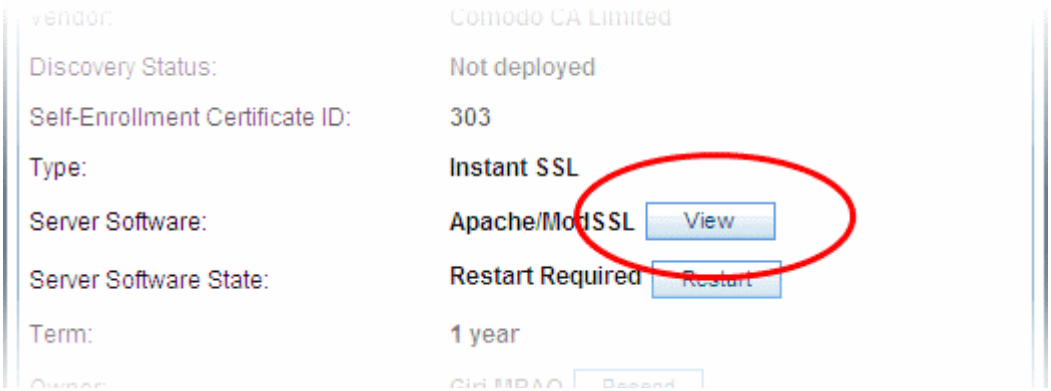
- Clicking the 'Resend' button will create a schedule for CCM to resend the notification email.



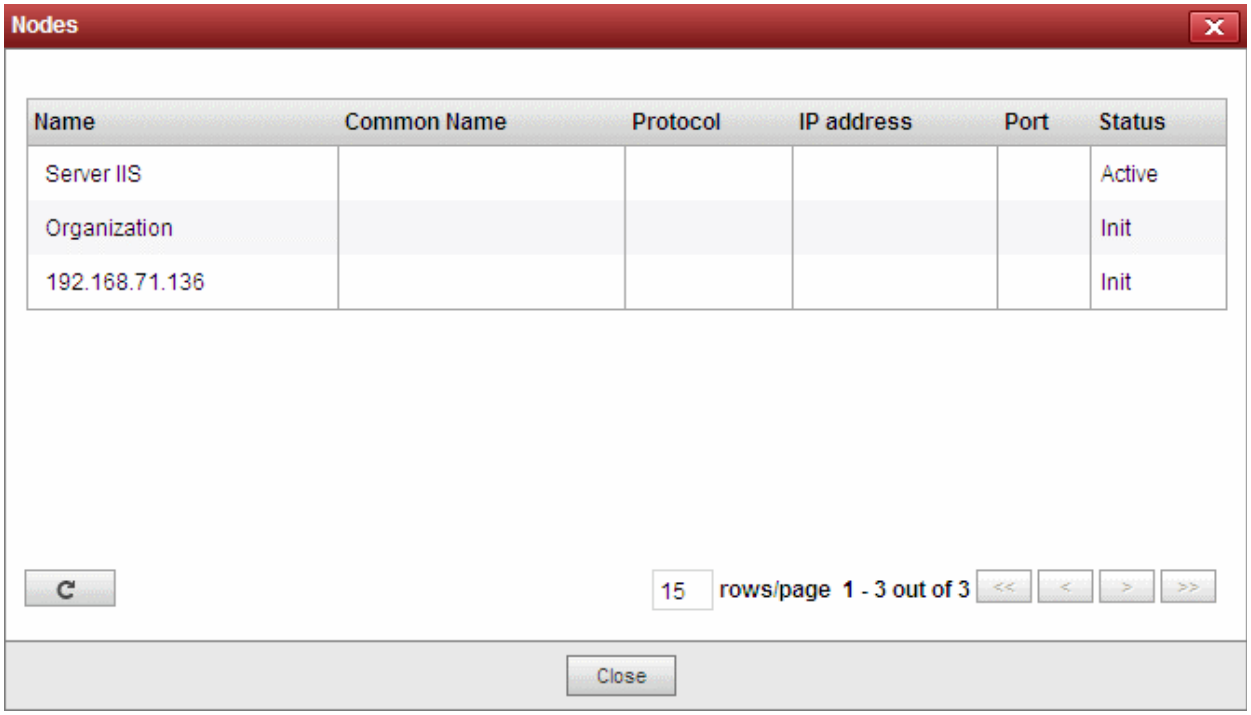
3.1.1.2.2 Viewing Installation Details of Certificates

The 'Details' dialog for SSL certificates added for auto installation to IIS or Apache, allows the administrator to view the installation state of the certificate.

- The 'Details' dialog for the SSL certificate added for auto installation, displays a 'View' button beside the 'Server Software' field.

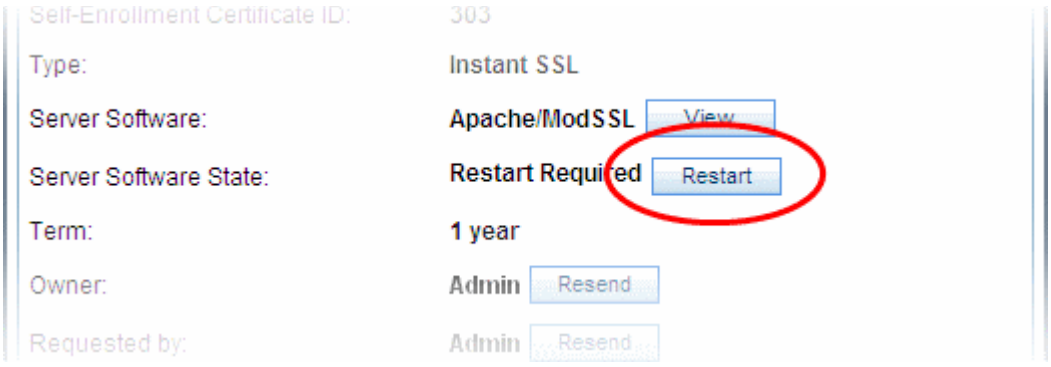


- Clicking the 'View' button will display a Nodes dialog that provides the details on the Agent responsible for auto-installation, the node server upon which the certificate is installed and the installation status.



3.1.1.2.3 Restarting Apache after Auto-Installation of SSL Certificate

The Apache will need to be restarted to finalize the installation of the SSL certificate. Administrators can do this remotely from the CCM interface by clicking the 'Restart' button on the certificate 'Details' dialog:



- Clicking 'Restart' will reboot the server. After rebooting, the 'Server Software State' will change to 'Active'.

3.1.1.3 Comodo SSL Certificates

3.1.1.3.1 Definition of Terms

Validation Levels

OV: Organization **V**alidated certificates include full business and company validation from a certificate authority using currently established and accepted manual vetting processes.

EV: Browsers with EV support display more information for EV certificates than for previous SSL certificates. Microsoft Internet Explorer 7, Mozilla Firefox 3, Safari 3.2, Opera 9.5, and Google Chrome all provide EV support.

Certificate Types

SDC: Single **D**omain **C**ertificates will secure a single fully qualified domain name.

WC: Wildcard **C**ertificates will secure the domain and unlimited sub-domains of that domain.

MDC: Multi-**D**omain **C**ertificates will secure up to 100 different domain names on a single certificate.

Certificate Name	Type	Validation Level	Description	Maximum Term Length
Comodo Trial SSL Certificate	SDC	OV	Secures a single domain	30 days
Comodo Intranet SSL Certificate	SDC	OV	Secures a single internal host	1 year - 3 years
Comodo InstantSSL Certificate	SDC	OV	Secures a single domain	1 year - 3 years
Comodo InstantSSL Pro Certificate	SDC	OV	Secures a single domain	1 year - 3 years
Comodo PremiumSSL Certificate	SDC	OV	Secures a single domain	1 year - 3 years
Comodo PremiumSSL Wildcard Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain	1 year - 3 years
Comodo PremiumSSL Legacy Certificate	SDC	OV	Secures a single domain	1 year - 3 years
Comodo PremiumSSL Legacy Wildcard Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain	1 year - 3 years
Comodo SGC SSL Certificate	SDC	OV	Secures a single domain	1 year - 3 years
Comodo SGC SSL Wildcard Certificate	WC	OV	Secures domain and unlimited sub-domains 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 sub-domains 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 sub-domains of that domain	1 year - 3 years
PlatinumSSL SGC Certificate	SDC	OV	Secures a single domain	1 year - 3 years

Certificate Name	Type	Validation Level	Description	Maximum Term Length
PlatinumSSL SGC Wildcard Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain	1 year - 3 years
Comodo Multi-Domain SSL Certificate	MDC	OV	Secure multiple Fully Qualified domains on a single certificate	1 year - 3 years
Comodo EV SSL Certificate	SDC	EV	Secures a single domain	1 year - 2 years
Comodo EV SGC SSL Certificate	SDC	EV	Secures a single domain	1 year - 2 years

3.1.2 Request and Issuance of SSL Certificates to Web Servers and Hosts

There are two broad methods an SSL administrator can use to request and install certificates:

- **Automatic installation** - Administrators can configure CCM to automatically create certificate requests for their domains and then automatically install the certificate on the web server. When a certificate is nearing expiry, a CSR is automatically generated and forwarded for administrative approval. Once issued by CA, the certificate will be collected and automatically installed on the web server. The auto-installation feature must be enabled for your account. Refer to the section **Automatic Installation and Renewal** for more details.
- **Manual Installation** - SSL administrators, or the applicants authorized by them, can also obtain certificates via CCM's applications forms. The applicant will then need to manually install the certificate on the target web server. Refer to the section **Request, Installation and Renewal using Application Forms** for more details.

Summary of steps for requesting and issuing an SSL certificate:

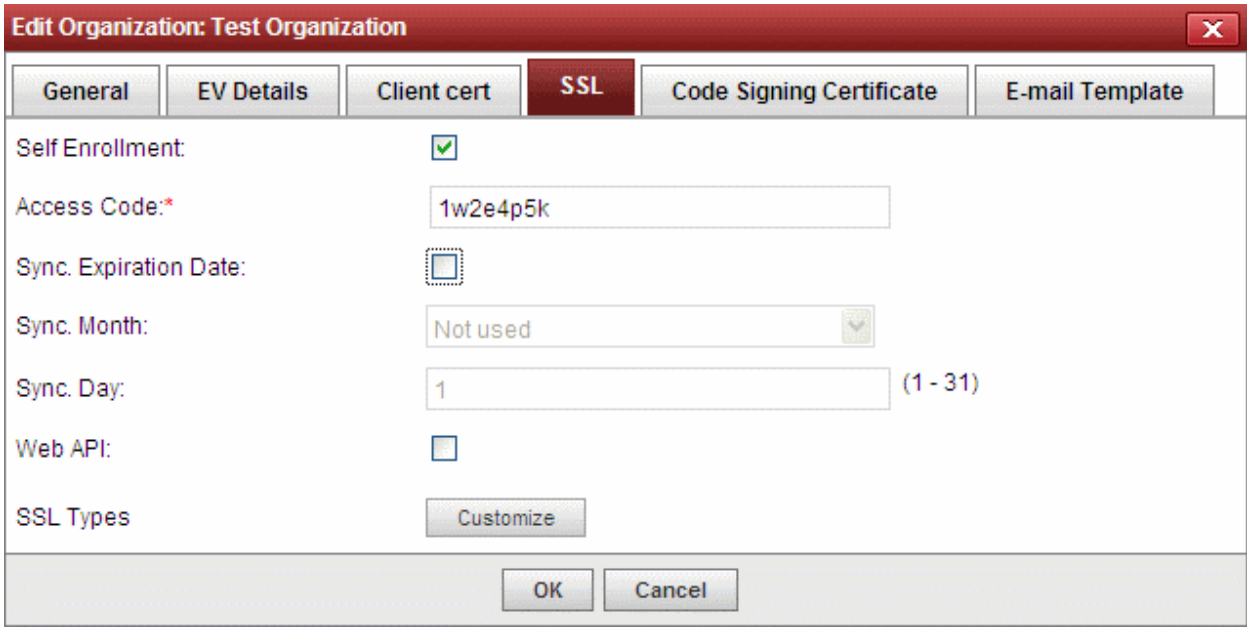
- Applicant confirms completion of the **prerequisites**;
- A certificate request is made via the certificate auto-installer or an application form as explained **above**.
- The certificate will appear in the 'SSL Certificates' area of Comodo Certificate Manager with the state 'Requested'. The MRAO, RAO SSL or DRAO SSL administrator (as applicable) will receive an email notification that a certificate request is awaiting approval.
- The certificate request will then need to be checked and approved or declined by appropriately privileged SSL Administrator. If it is approved then the request will be forwarded to Comodo CA for validation and issuance or rejection.
    - If the certificate is applied through CCM interface for automatic installation, the certificate will be issued and its state will be changed to 'Issued' in the 'Certificates Management' area. The administrator can choose to install the certificate remotely by clicking the 'Install' button in the CCM interface.
    - If the certificate is applied through the an application form, a collection mail will be sent to the applicant which contains a link to the certificate collection form (see section **Certificate Collection** for more details). The applicant can manually download and install the certificate.
- Once an administrator has 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 **Certificate Request Approval** for more details.
- The applicant will be designated as 'Requester' of the certificate. If the applicant does not exist then CCM will automatically add this applicant as a new 'End-user' at the time the certificate enrollment form is successfully submitted.

3.1.2.1 Prerequisites

- The domain for which the SSL certificate is to be issued has been enabled for SSL certificates, has been pre-validated by Comodo through **DCV** process and that the domain has been activated for account by your Comodo account manager. All certificate requests made on 'pre-validated' domains or sub-domains thereof are issued automatically. If

you request a certificate for a brand new domain, then this domain will first have to undergo validation by Comodo. Once validated, this new domain will be added to your list of pre-validated domains and future certificates will be issued immediately.

- For applications using Enterprise Controller mode, the administrator has installed the Certificate Controller on a control server and configured it to communicate with the remote hosts. (See the section **Agents** for more details.)
- For applications using CCM 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 it in the host. (See the section **Agents** for more details.)
- The administrator has created at least one Organization/Department that the domain will belong to. (See chapter '**Settings - Organizations**'- for more details.)
- If the administrator wishes to enable **external SSL applications**, that the administrator has checked the 'Self Enrollment' box in the **SSL tab** of the 'Create/Edit' Organizations dialog box (see screen-shot below)



- If the administrator wishes to enable external SSL application using the Self Enrollment Form, that the administrator has specified an **Access Code** in the **SSL tab** of the 'Create/Edit' Organizations dialog box (see screen-shot). Comodo recommends using a mixture of alpha and numeric characters that cannot not easily be guessed.
- For the Built-in and the Self Enrollment Forms, the applicant has already created the Certificate Signing Request (CSR) using their web server software prior to beginning the application. This helps avoid potential errors on the certificate application form by allowing the common name (CN) to be automatically drawn from the CSR. Please note that CSR must be 2048 bit and must contain the following fields:

  Common Name (Fully Qualified Domain Name)
  Organization
  Organization Unit
  Locality
  State/Province
  Country (2 character ISO code)
- **Optional**: The administrator has checked the '**Sync. Expiration Date**' box and specified the day of the month upon which the certificate will expire.

3.1.2.2 Automatic Installation and Renewal

Comodo Certificate Manager has the ability to automatically install SSL certificates on Apache, Apache Tomcat and IIS servers. There are two available modes:

Enterprise Controller Mode	CCM Controller Mode

Requires one-time installation of the certificate controller software on a central control server inside your network. The controller communicates with each remote host and co-ordinates automatic CSR generation and certificate installation. See **Method 1 - Enterprise Controller Mode**	Requires an agent to be installed on each individual web server. These agents communicate with CCM to co-ordinate automatic CSR generation and certificate installation. See **Method 2 - CCM Controller Mode**

1. Enterprise Controller Mode
   i. Certificate Controller software is installed on a host in your network. This controller will communicate with your remote web-hosts and will automatically apply for and install certificates on to them. The controller is configured through a web-interface and can be configured to communicate directly with Comodo CA infrastructure through a proxy server.
   ii. The controller periodically polls CCM for certificate requests for remote servers. If a request exists, it will automatically generate a CSR for the web server and present the application for administrator approval via the CCM interface. On approval, the agent will submit the CSR to Comodo CA and track the order number. Once the certificate is issued by CA, the controller will download the certificate and allow the administrator to install the certificate from the CCM interface.
   iii. The auto-installation/renewal is enabled for the following server types:
      - Apache2 (httpd)
      - Apache Tomcat
      - IIS 5.0 to 8.0 (Server 2000 - 2008R2)

   Refer to the section **Method 1 - Enterprise Control Mode** for a tutorial on automatic installation of Certificates on remote web servers
2. CCM Controller Mode
   i. This mode requires an agent to be installed on each of the web servers for which certificate auto-installation/renewal is required.
   ii. The agent periodically polls CCM for certificate requests for web servers enabled for automatic certificate installation. If a request exists, it will automatically generate a CSR for the web server and present the application for administrator approval via the CCM interface. On approval, the agent will submit the CSR to Comodo CA and track the order number. Once the certificate is issued by the CA, the agent will download the certificate and allow the administrator to install the certificate from the CCM interface.
   iii. The auto-installation/renewal is enabled for the following server types:
      - Apache2 (httpd)
      - Apache Tomcat
      - IIS 5.0 to 8.0 (Server 2000 - 2008R2)

   Refer to the section **Method 2 - CCM Controller Mode** for a tutorial on automatic installation of Certificates on web servers.

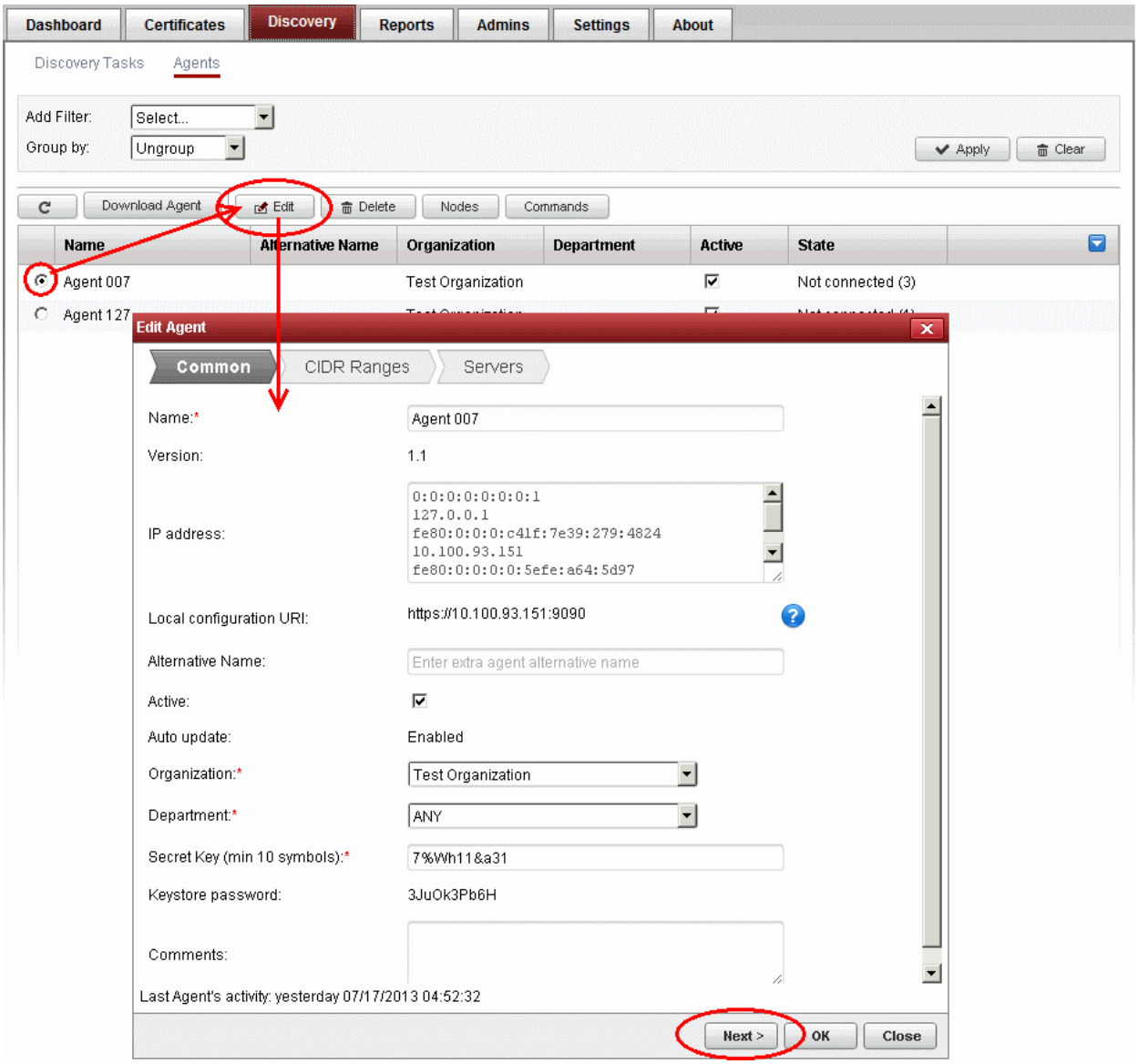
Background Note: It is possible for one Organization to have multiple certificates for different domain names. See the section **5.2.2.4.2 General Settings - Table of Parameters** if you would like to read more about this at this time.

3.1.2.2.1 Method 1 - Enterprise Controller Mode

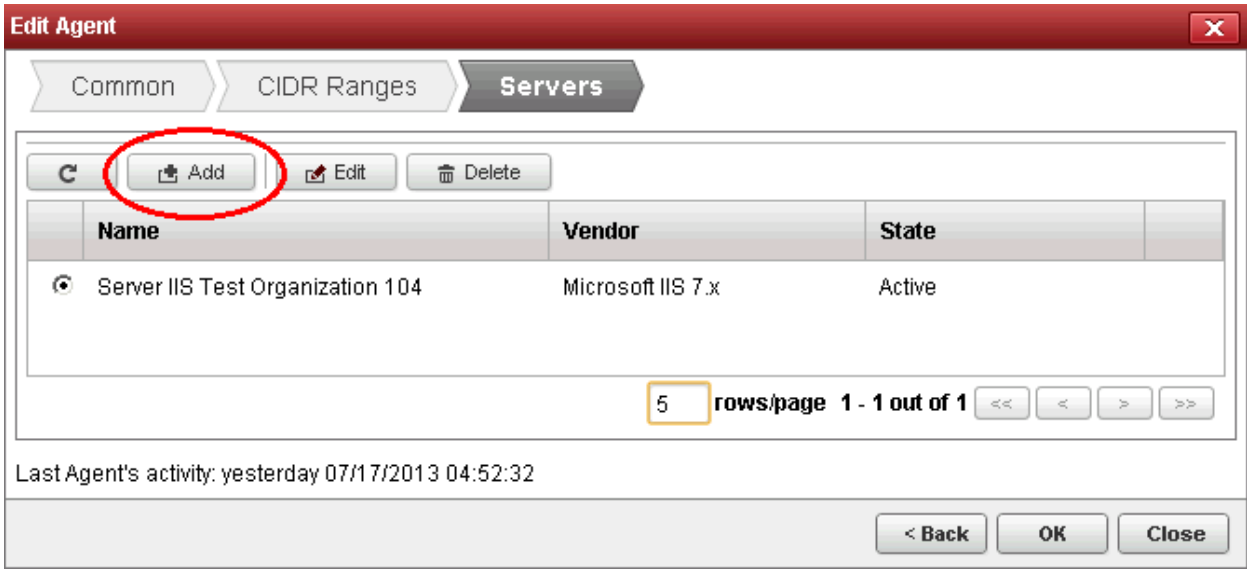
Enterprise Controller mode enables administrators to automatically install certificates on any remote server on the network. Certificate Controller software needs to be installed on a control server and this software will communicate with web-hosts on your network. If a new certificate is required, it will coordinate with the host to generate a CSR, submit it to Comodo CA, collect the certificate and install it. The certificate controller software is accessible through a dedicated web-interface and can be configured to communicate with Comodo CA through a company owned proxy server for additional security.

Certificate Manager Administrator can add remote servers for automatic installation of certificates through Discovery > Agents interface.

Note:The Certificate Controller software should have been installed on the control server prior to the application for a certificate for a remote server. Refer to the section **Agents** for more details on installing the controller and the section **Configuring the Certificate Controller Agent through Web Interface** for more details on configuring the controller to connect to Comodo CA through a proxy server (optional).

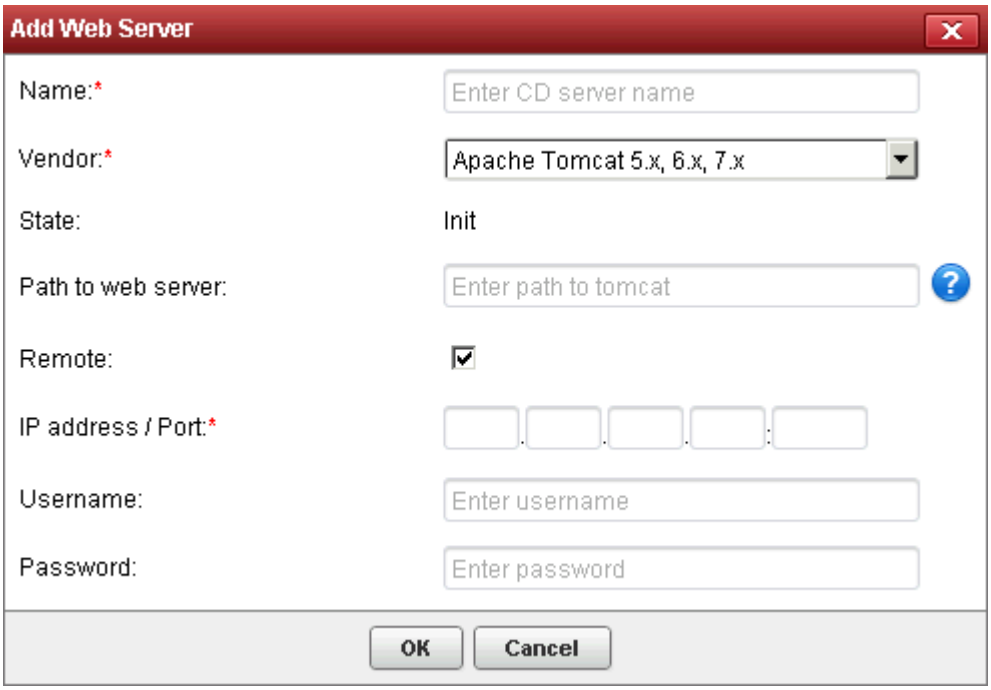


- Select the controller and click 'Edit' at the top to open the 'Edit Agent' dialog and click 'Next' button in it till the Server tab is opened.



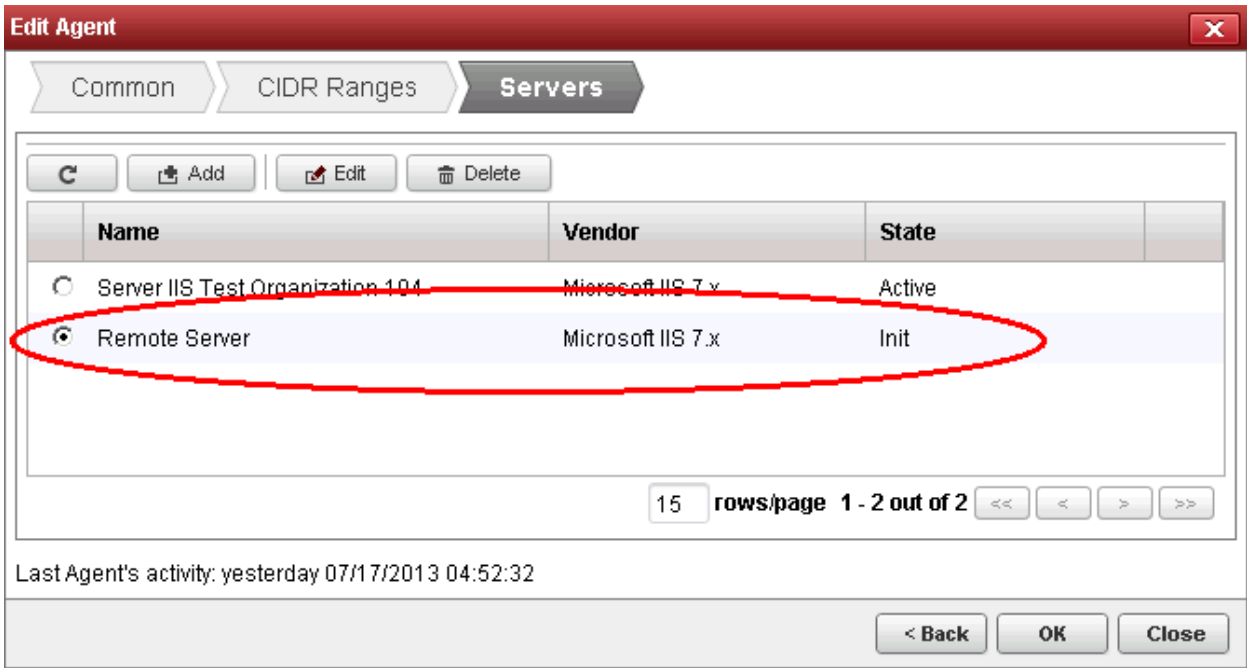
The server on which the controller is installed will be displayed in the list of servers.

- Click 'Add' to associate a remote server to the controller. The 'Add Web Server' dialog will open.

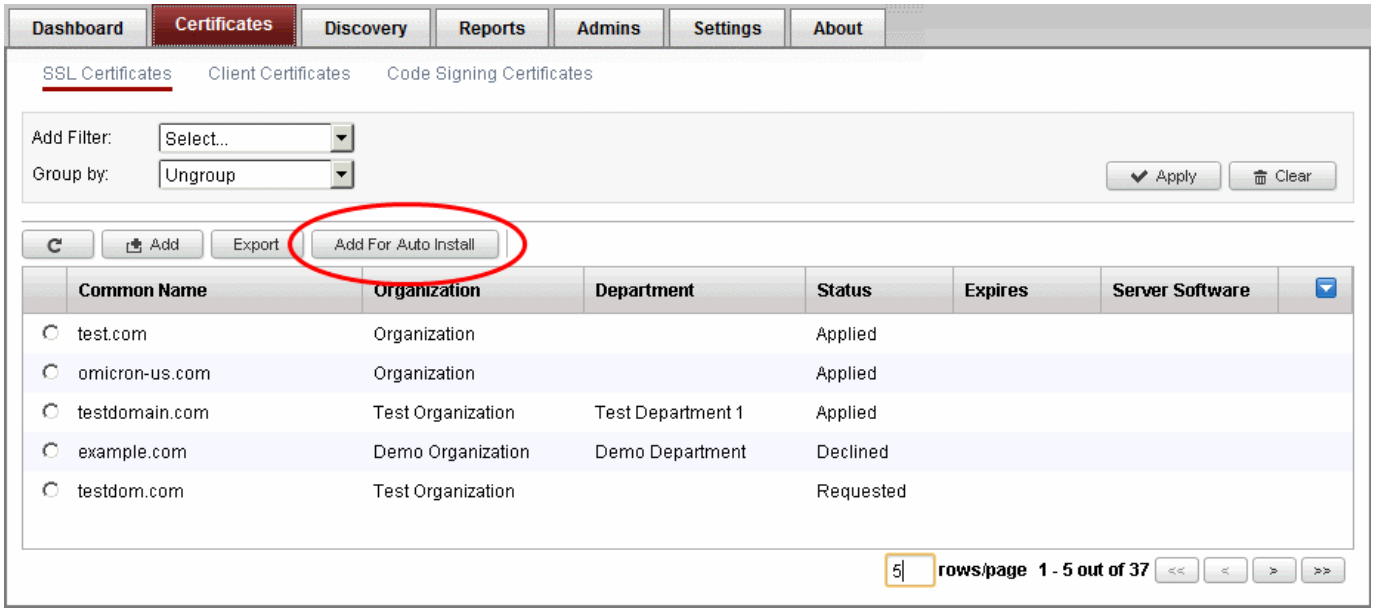


Add Web Server - Table of Parameters		
Field Name	**Type**	**Description**
Name	String	Enables the Administrator to enter the name of the server.
Vendor	drop-down	Enables the Administrator to select the vendor of the server.
State		Indicates whether or not the server is initialized.
Path to web server	String	Enables the Administrator to specify the network path for the server.
Remote	Checkbox	Enables the Administrator to specify whether the server is Remote or Local. While adding remote servers for agent-less automatic certificate installation, this checkbox should be selected.
IP Address / Port	String	Enables the Administrator to specify the IP address and connection port of the server for remote connection. Note: This field will be enabled only if 'Remote' is selected.
User Name	String	For IIS server - Enables the Administrator to specify the username of the administrator for logging-into the server. For Apache - Enables the Administrator to specify the private key file path to enable agent to access the server Note: This field will be enabled only if 'Remote' is selected.
Password	String	For IIS server - Enables the Administrator to specify the login password for the administrator account for logging into the server For Apache - Enables the Administrator to specify the passphrase of the private key file path Note: This field will be enabled only if 'Remote' is selected.

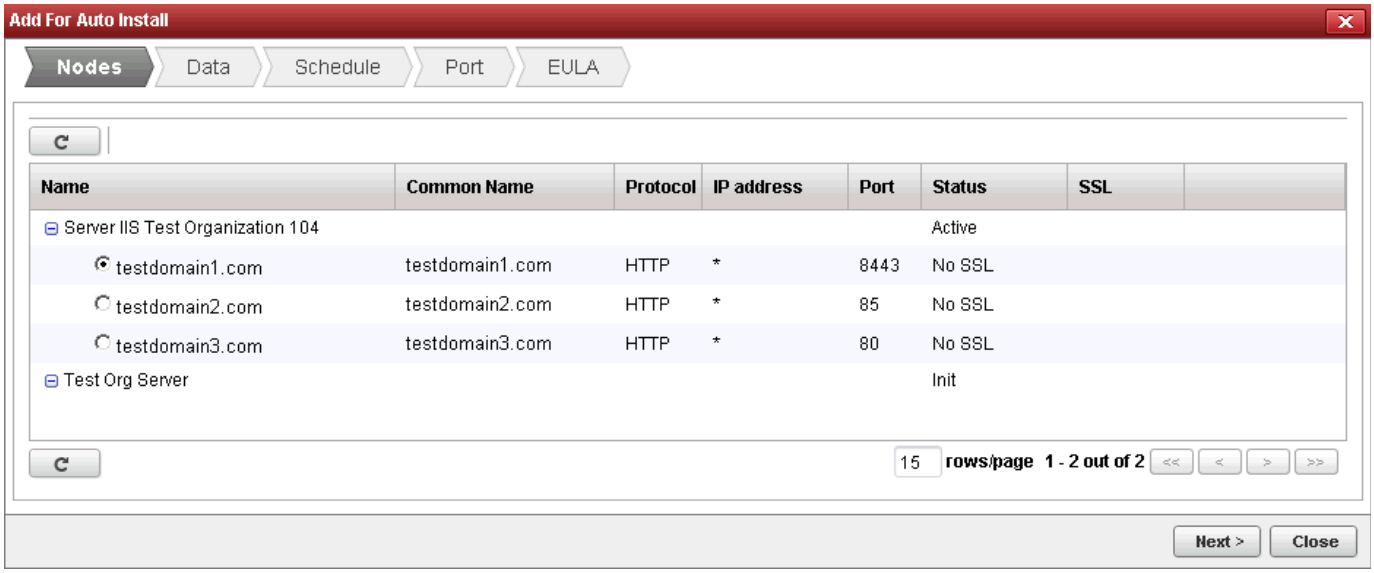
- Enter the parameters and click OK. The server will be added to the controller. It will take a few minutes for the server to become 'Active' state.



Once the remote server is added to the controller, the administrator can apply for the domains hosted from the server through the Certificates Management > SSL Certificates area of CCM interface by clicking the 'Add For Auto Install' button (as shown).

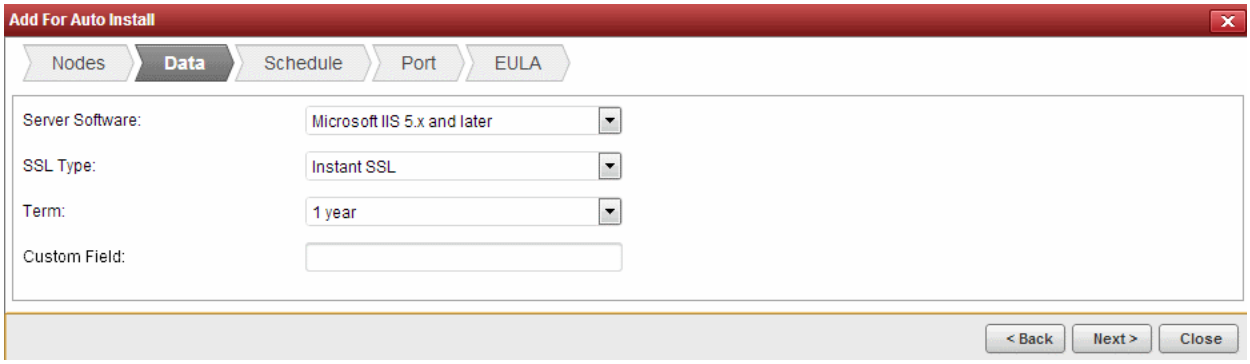


The 'Add for Auto Install' dialog will be displayed with the 'Nodes' interface opened. The 'Nodes' interface displays a tree structure of servers associated with the Certificate Controller and the domains hosted by them.

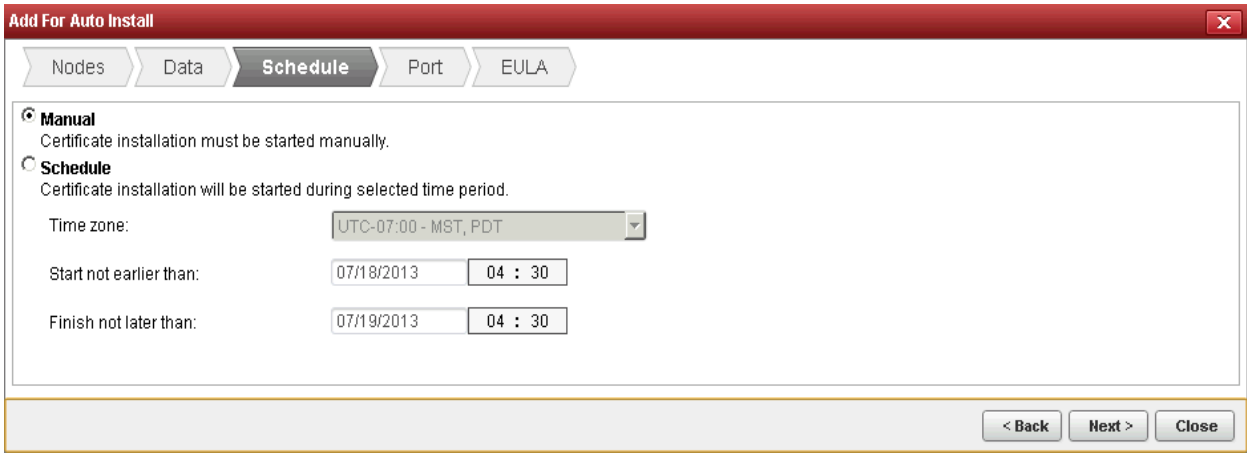


- Select the domain from the remote server for which you wish to install a SSL certificate and click 'Next'.

The Data interface will be displayed enabling you to select the server software and the SSL certificate type.

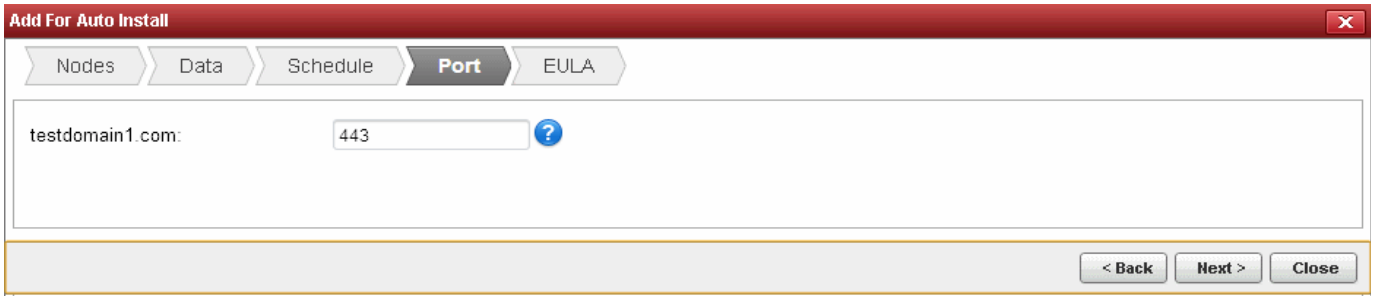


- Select the Server type from the Server Software drop-down.
- Select the SSL certificate type that you wish to order from the SSL Type drop-down. The drop-down will list only the certificate types that are enabled for the Organization. See section **Comodo SSL Certificates** for a list of certificate types.
- Select the term length of the certificate from the Term drop-down.
- Enter the parameter(s) for custom field(s) such as 'Employee Code, Telephone' (if any) added for the SSL enrollment forms. Refer to the section **Custom Fields** for more details.
- Click Next. The 'Schedule 'interface will be opened.

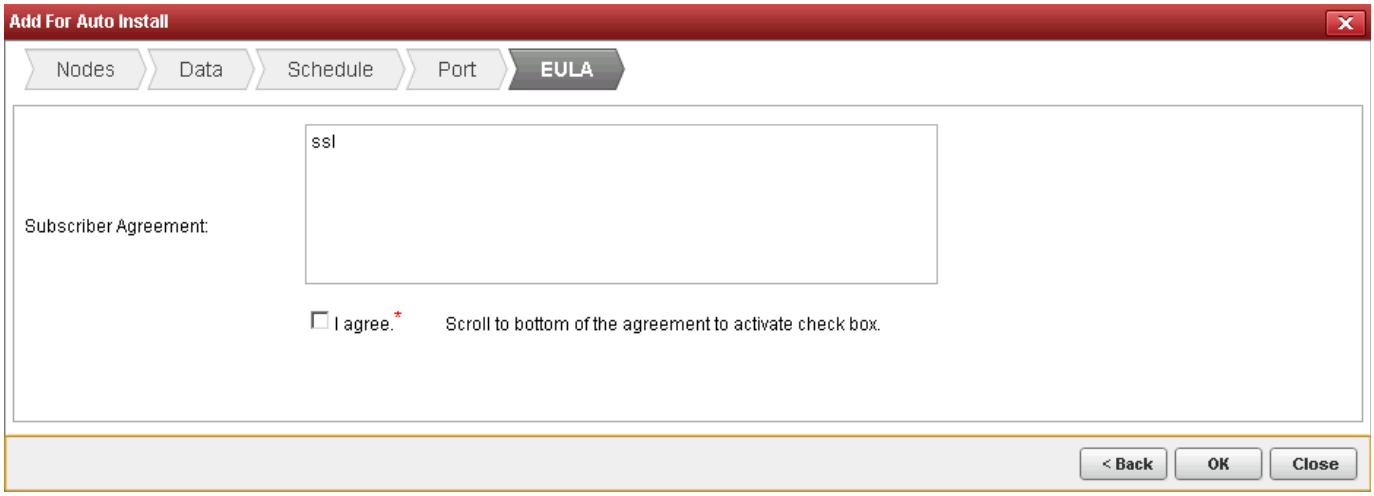


- If you want to manually install the certificate, select 'Manual'
- If you want to install the certificate at a scheduled time, select 'Schedule' and then select your time zone, and set a time period . The Certificate Controller will generate the CSR and submit to Comodo CA, when it polls the CCM for the first time, within the set time period.
- Click Next.

- If you are applying for a SSL certificate for a node with HTTP protocol, the Port interface will open. If you you have chosen a node with HTTPS protocol, this step will be skipped and the **EULA interface** will open.

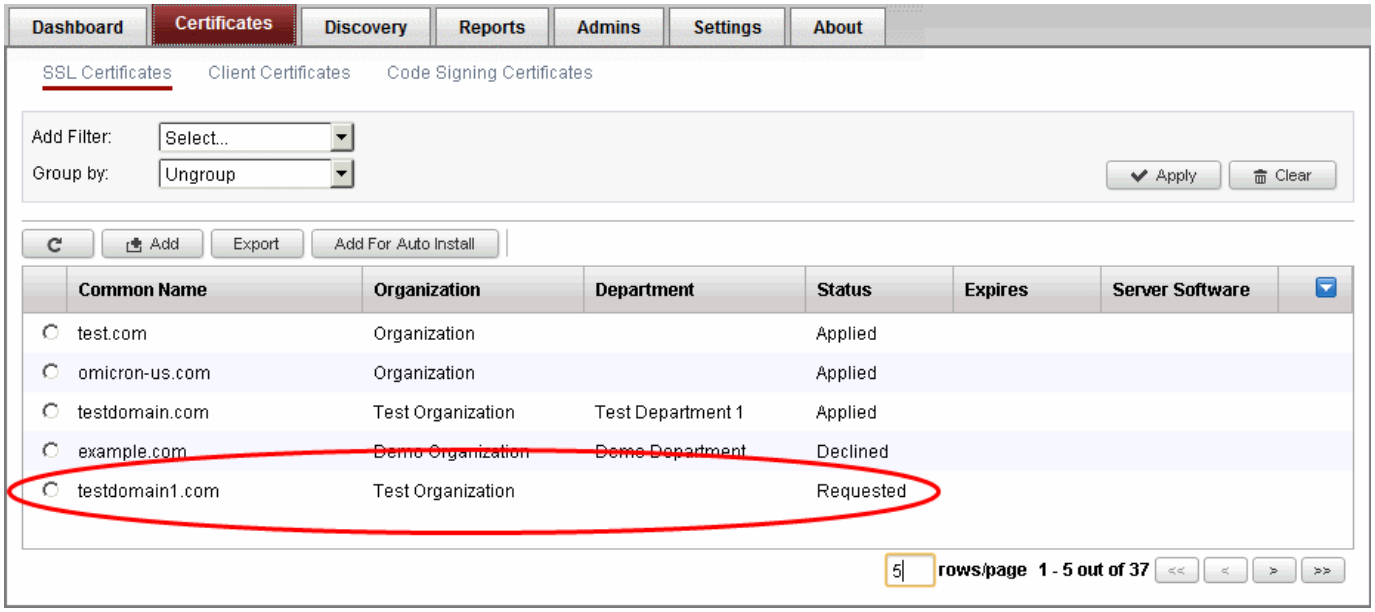


- Specify the HTTPS port for installing the certificate, (***Default = 443***)
- Click 'Next'. The EULA interface will open.

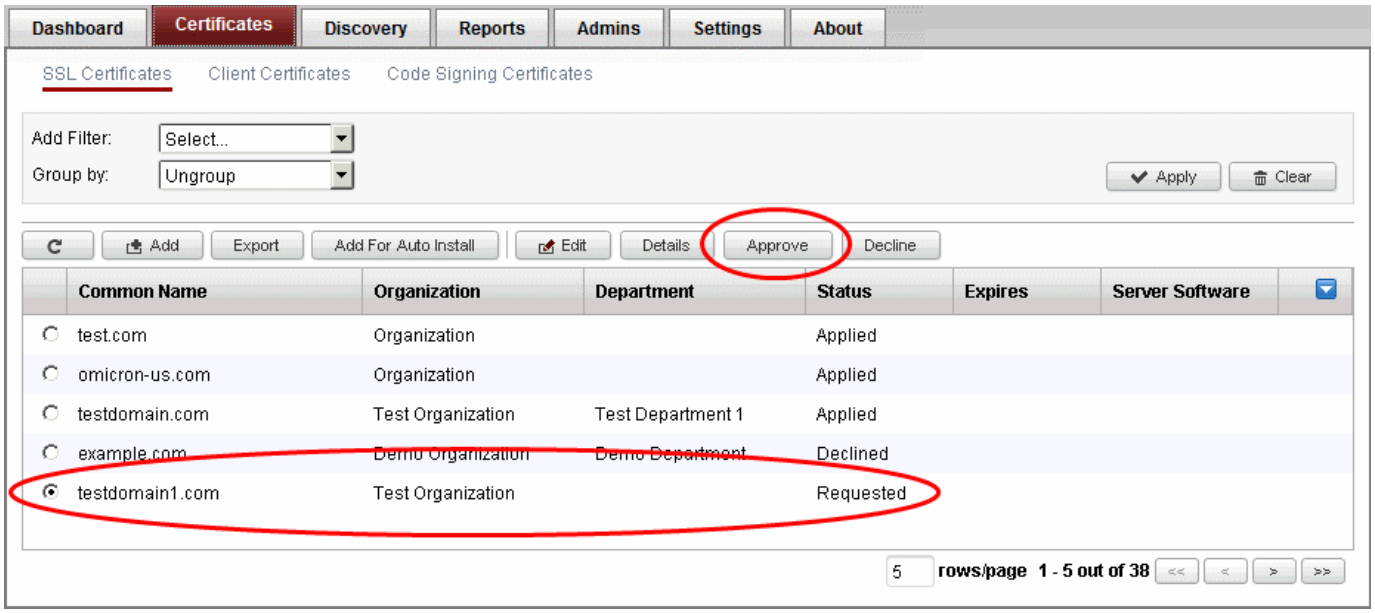


- Read the EULA fully and accept to it by selecting 'I Agree' checkbox.
- Click OK to save your application.

The certificate will be added to the SSL Certificates interface and its status will be displayed as 'Requested'.

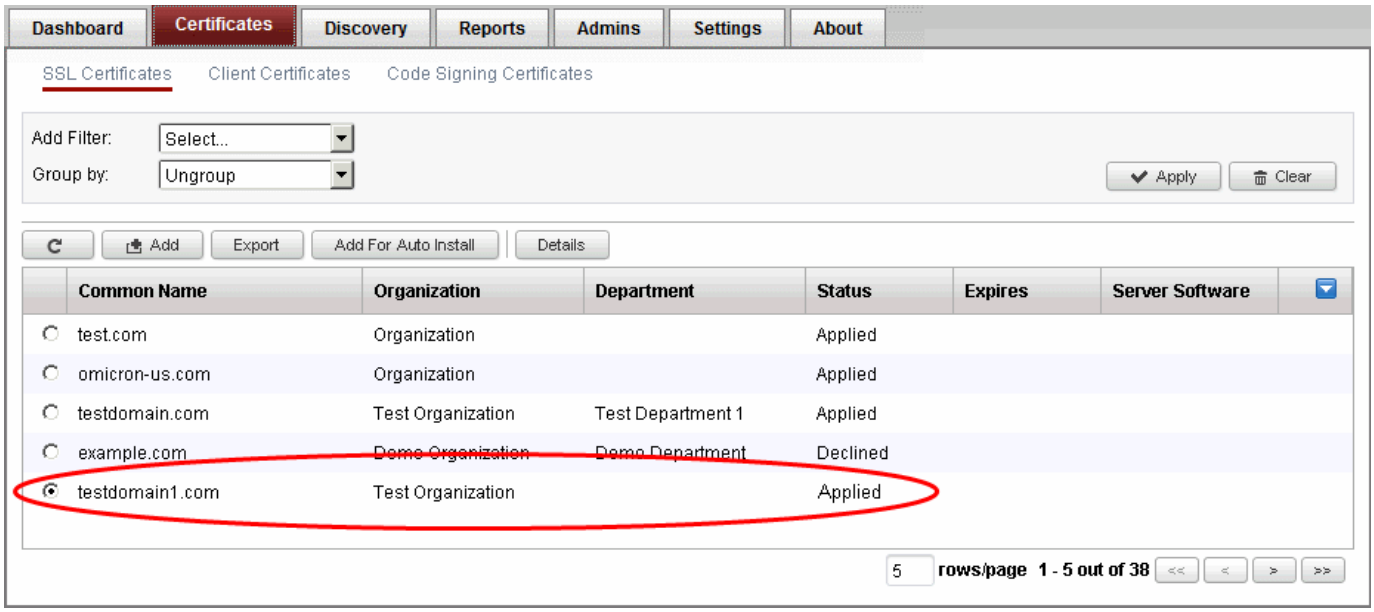


- The CSR for the requested certificate will be generated automatically. On successful creation of CSR, the 'Approve' button will appear at the top, on selecting the certificate.

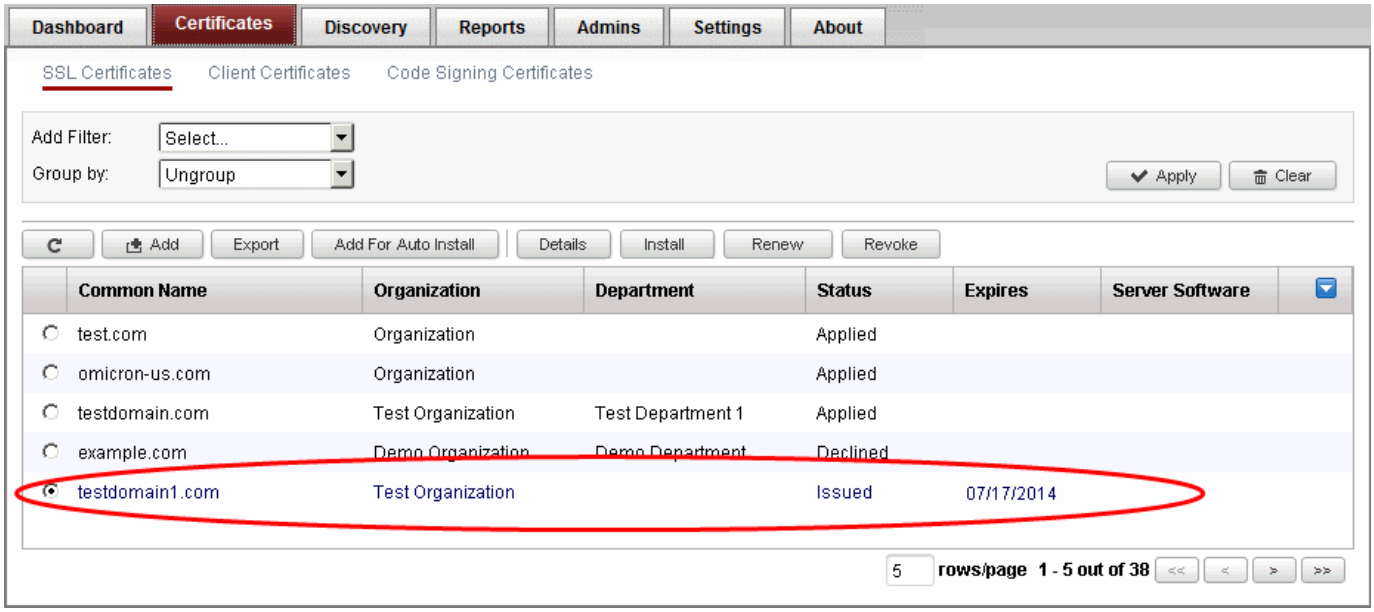


- Click the 'Approve' button to approve the request, enter the approval message in the 'Approval Message' dialog and click 'OK'.

On approval, the CSR will be submitted to Comodo CA to apply for the certificate. The certificate status will be changed to 'Applied'.

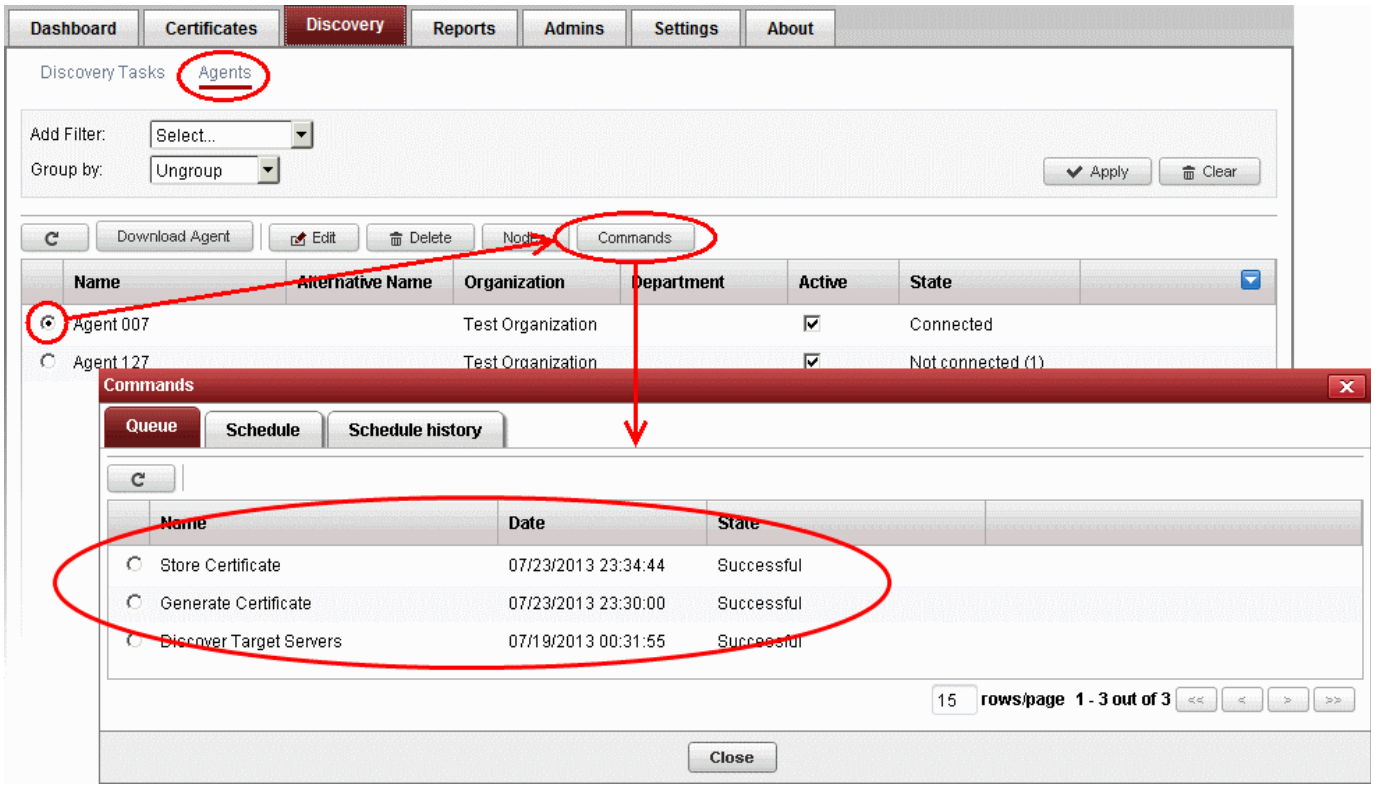


The Certificate Controller will track the order number and download the certificate from the CA, once it is issued and stores it. The certificate status will be changed to 'Issued'.

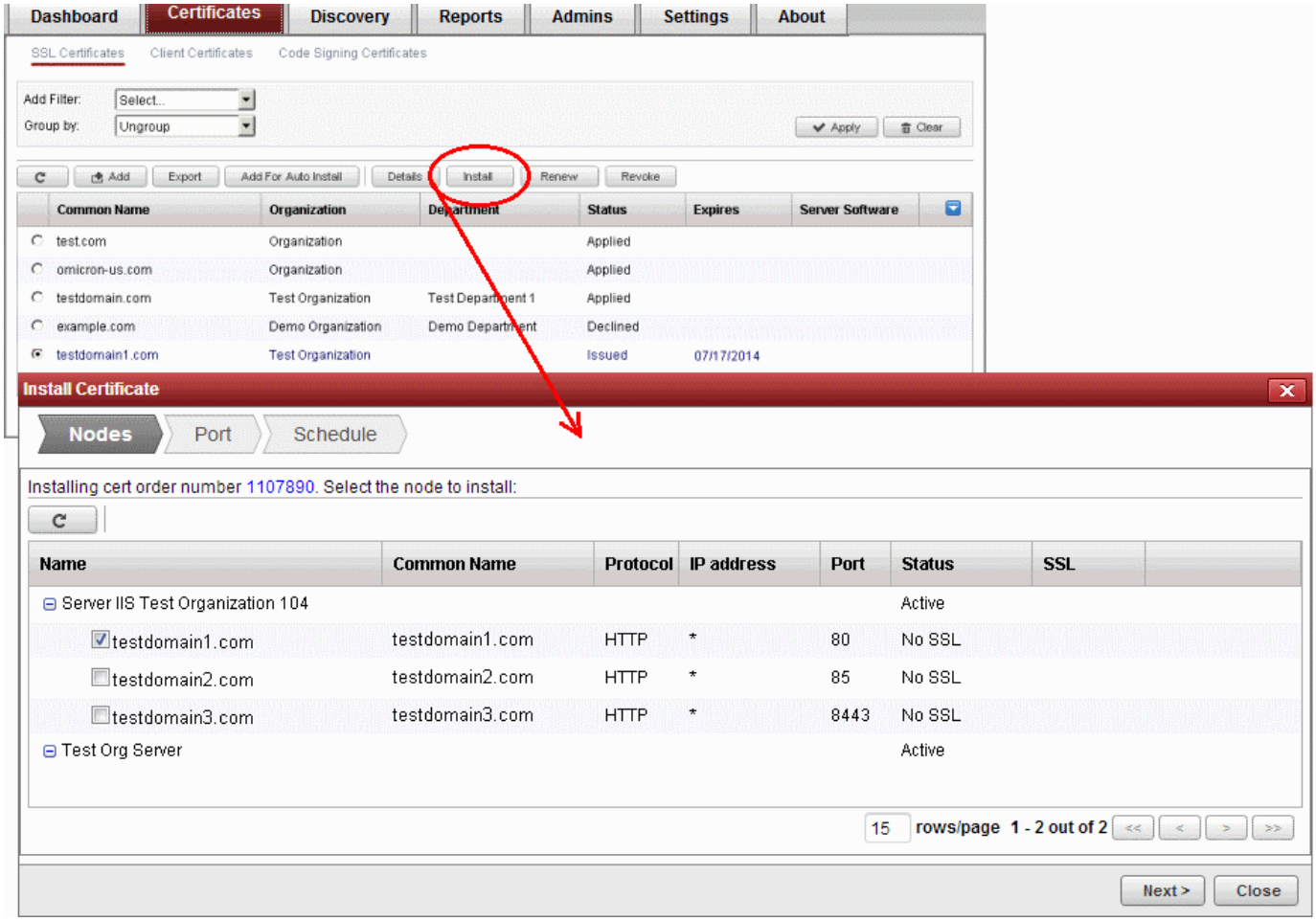


- To check whether the Certificate Controller has stored the certificate, click Settings > Discovery > Agents
- Select the controller and click 'Commands' button

You will see successful execution of 'Store Certificate' command.



- To install the certificate on to the remote server, select the certificate and click 'Install' from the 'Certificates Management' interface.

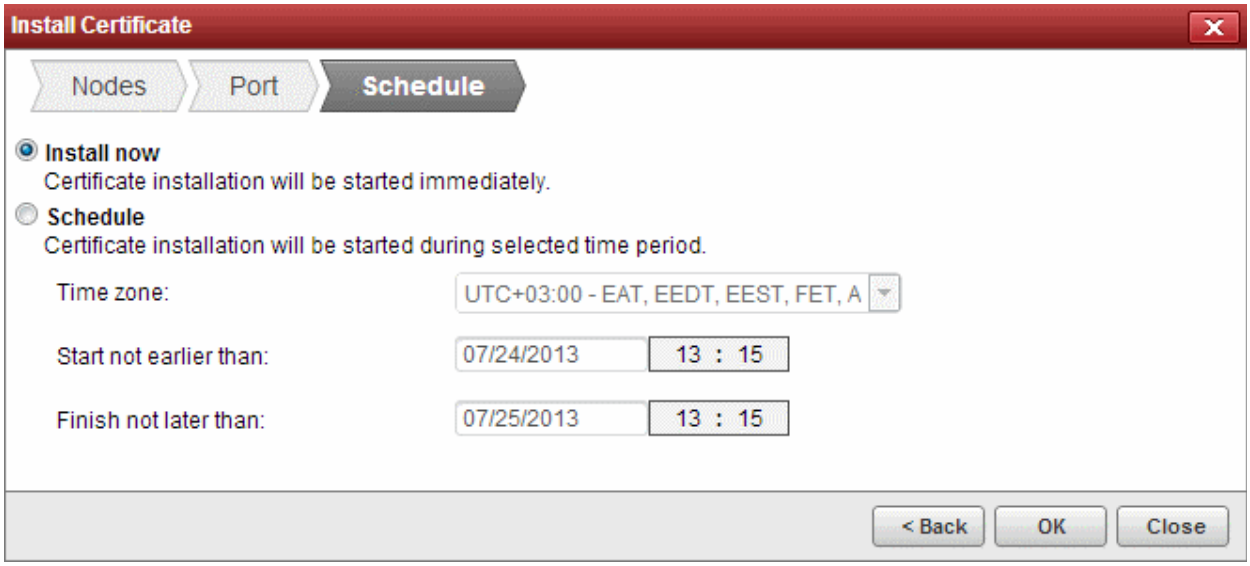


The 'Install Certificate' dialog will be displayed with the nodes interface opened. The node upon which the certificate is to be installed is pre-selected.

- If you want to install the same certificate to additional nodes or to a different node, select the node(s) as required
- Click 'Next'.

- If you have chosen to install the certificate on to a node with HTTP protocol, the 'Port' interface will open to specify the HTTPS port on to which the certificate has to be installed. If you have chosen a node with HTTPS protocol, this step will be skipped and the **Schedule interface** will open.

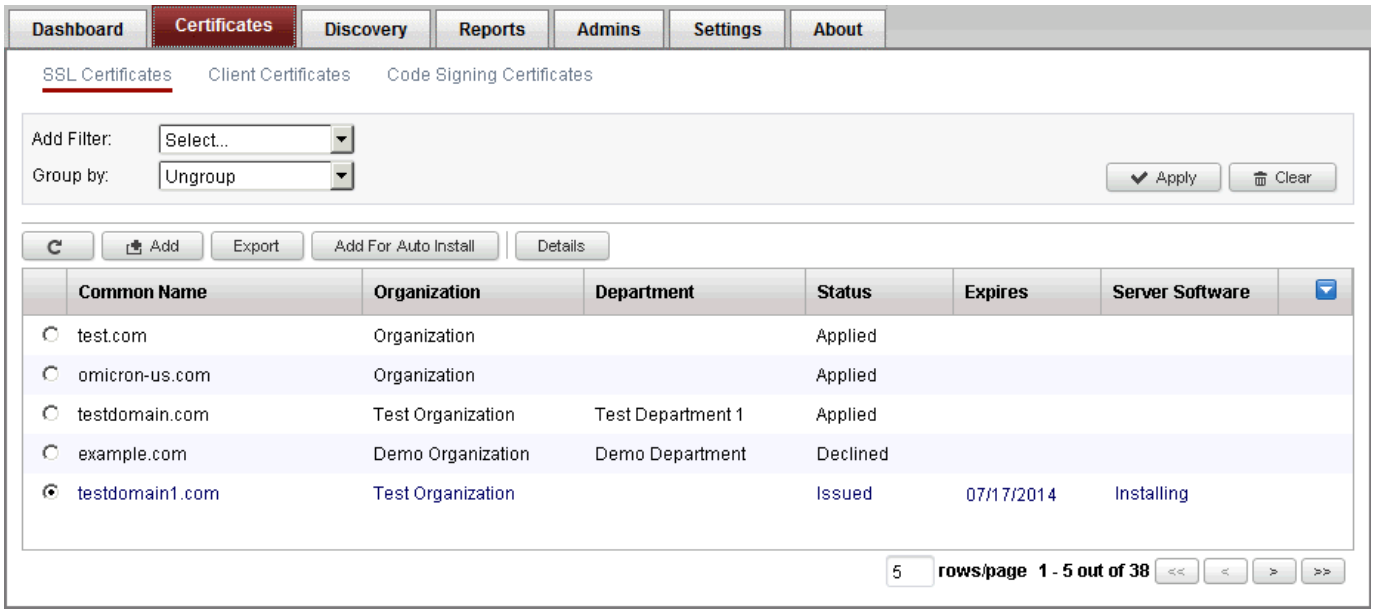
- Specify the port and click 'Next'. The 'Schedule' interface will open.



- If you want to instantly install the certificate, select 'Install now'
- If you want to install the certificate at a later time, select 'Schedule', then select your time zone, and set a time period. The certificate will be installed on the remote server when the certificate controller polls CCM for the first time, within the set time period.

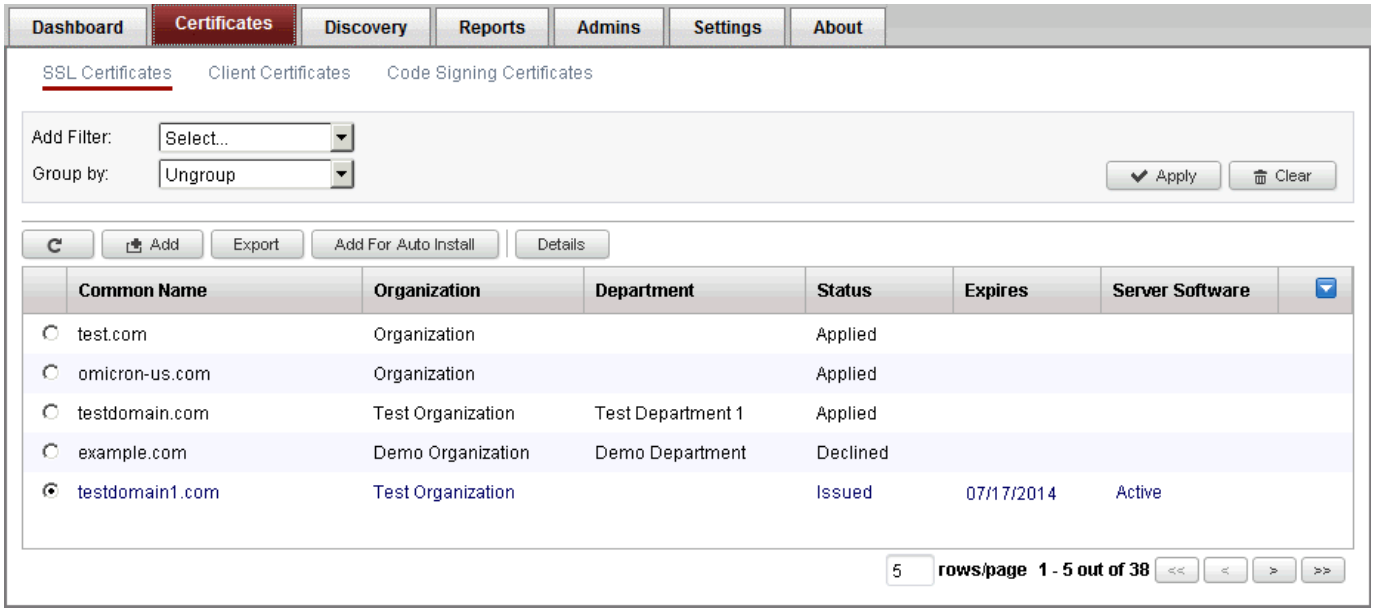
- Click OK

The certificate installation will begin instantly or at the scheduled time as set in the 'Schedule' interface and the Server Software state of the certificate will be displayed as 'Installing...'

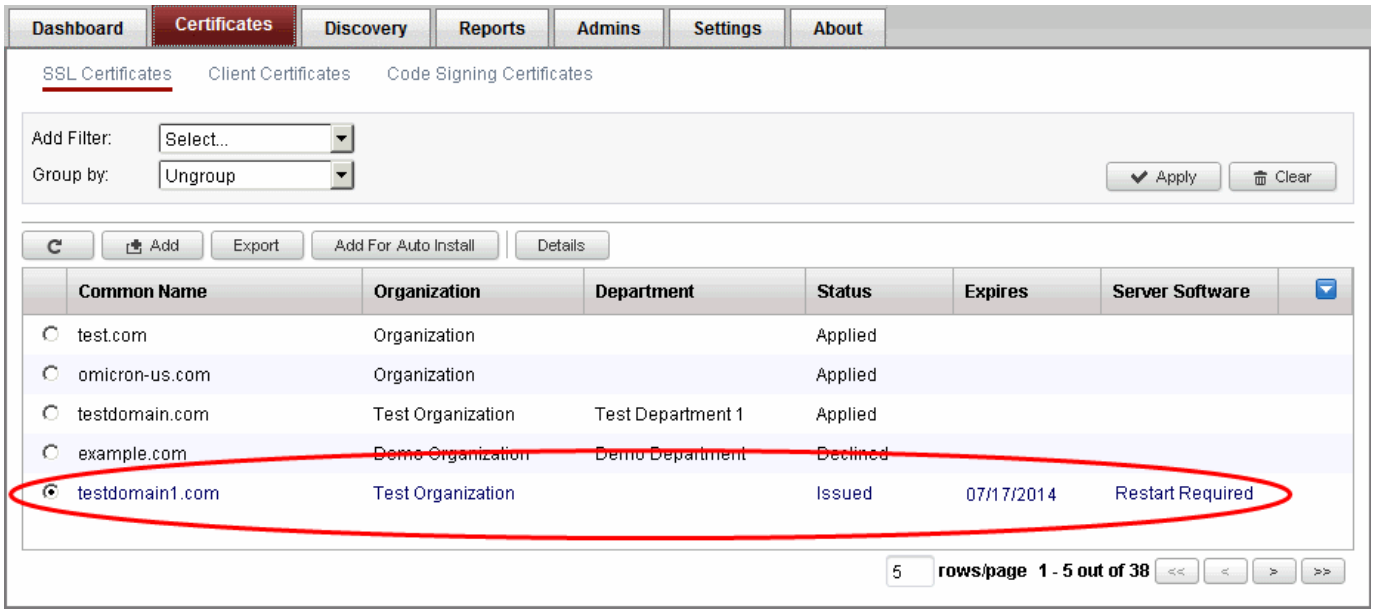


Upon completion of installation,

- For IIS servers and Tomcat servers: the certificate will be activated immediately and the Server Software state will be indicated as 'Active'.



- For Apache server: the certificate will be activated upon restart of the server. The Server Software state will be indicated as 'Restart Required'.

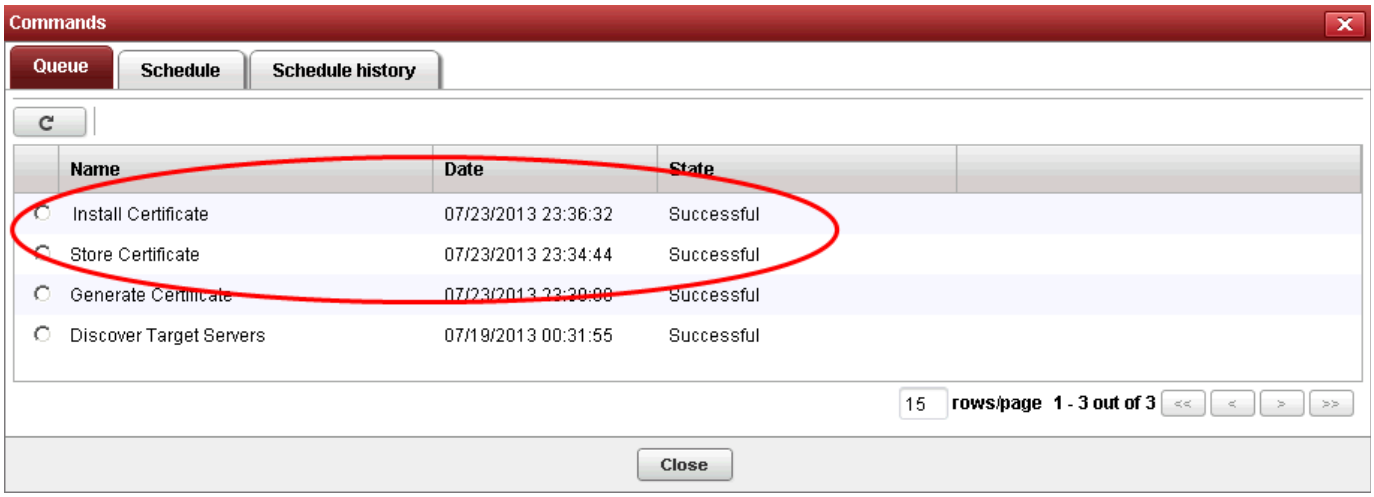


Tip: The server can be restarted from CCM through the **Certificate Details** dialog. For more details, refer to the section **Restarting Apache after Auto-Installation of SSL Certificate**.

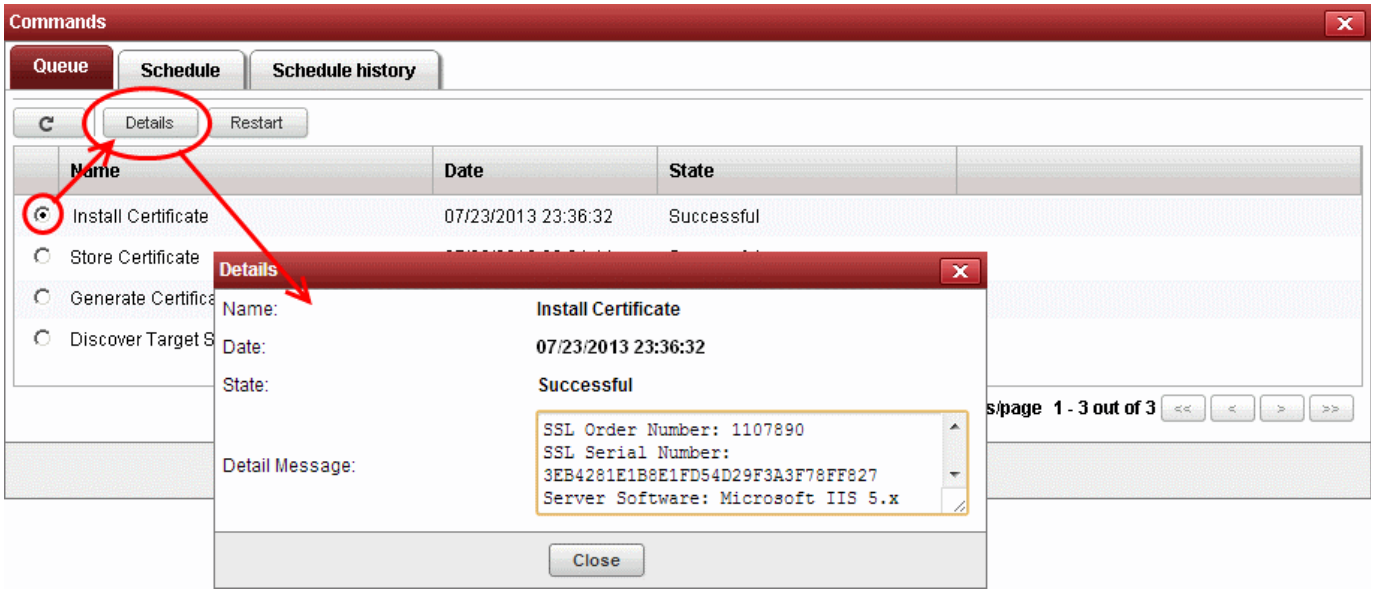
Upon restarting the server, the certificate will be activated and the Server Software state will be indicated as 'Active'.

- To check whether the Certificate Controller has installed the certificate, click Discovery > Agents
- Select the controller and click the 'Commands' button

You will see successful execution of 'Install Certificate' command.



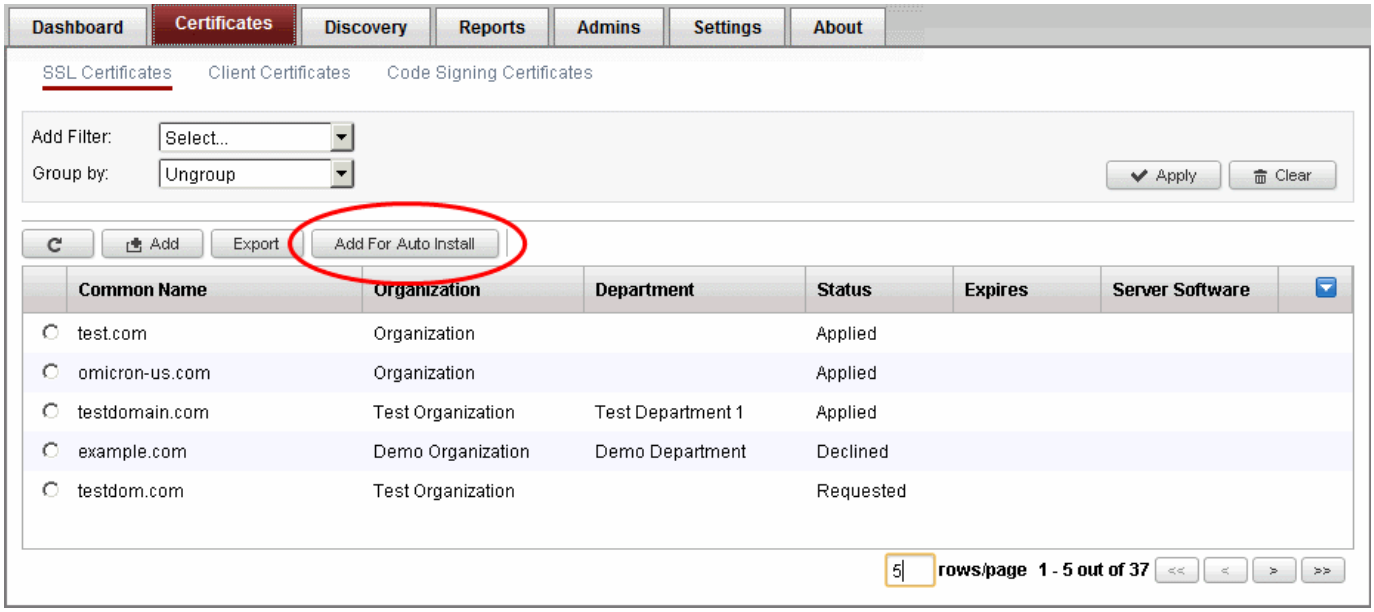
- To view the details of the command, select the command and click the 'Details' button from the top.



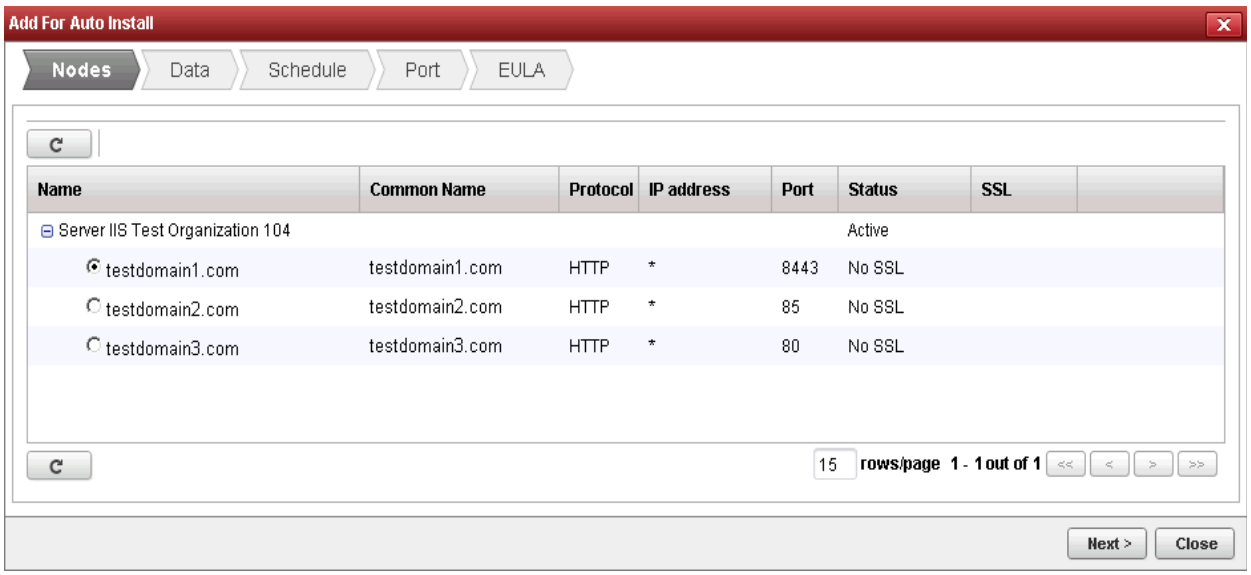
3.1.2.2.2 Method 2 - CCM Controller Mode

Certificate Manager administrators can apply for new certificates for domains hosted from different web servers, directly from the 'Certificate Management - SSL Certificates' area. The CCM Controller Mode requires an agent to be installed on each web server upon which the certificates are to be auto-installed/renewed. Refer to the section **Agents** for more details on installing the agent.

- To apply for a certificate click the 'Add For Auto Install' button (as shown).

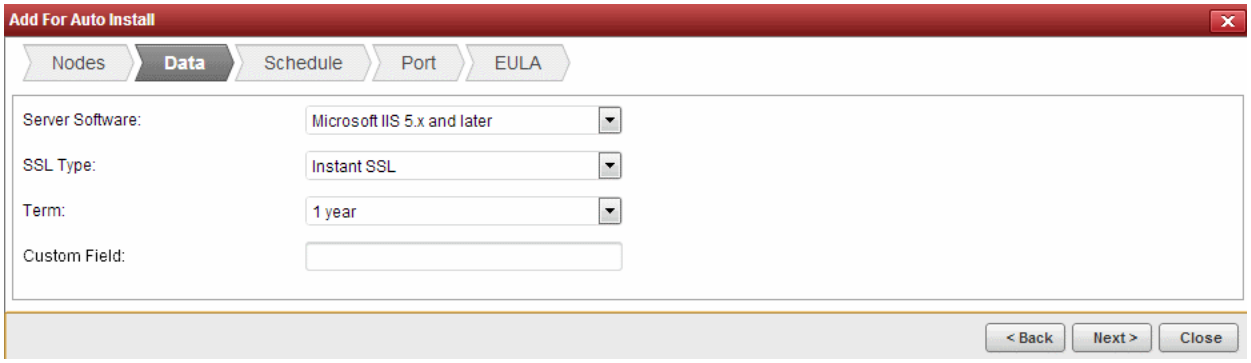


The 'Add for Auto Install' dialog will be displayed with the 'Nodes' interface opened. The 'Nodes' interface displays a list of Agents installed in your servers for different Organizations and Departments, with the list of server nodes under each Agent.



- Select the domain for which you wish to install a SSL certificate and click Next.

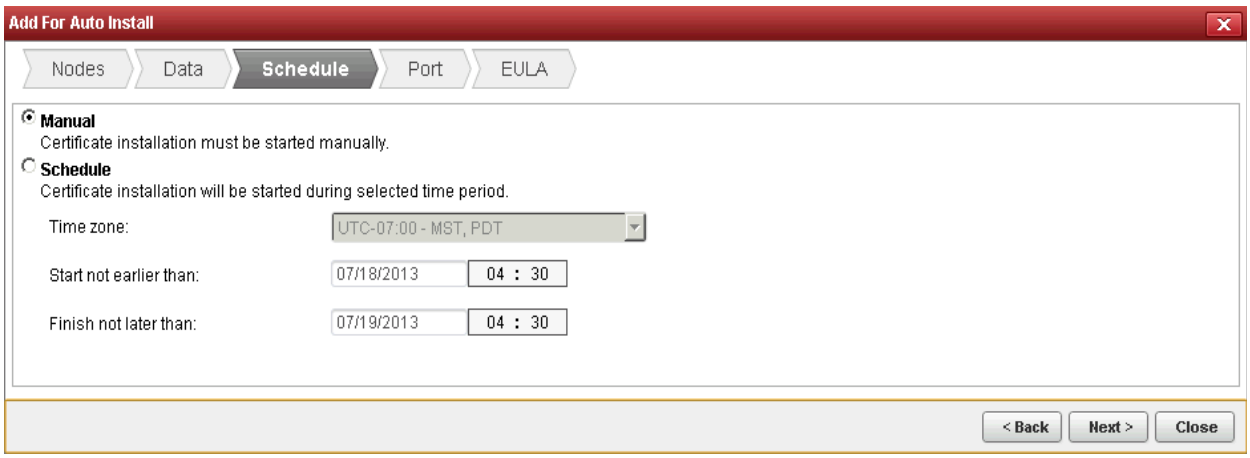
The Data interface will be displayed enabling you to select the server software and the SSL certificate type.



- Select the Server type from the Server Software drop-down.
- Select the SSL certificate type that you wish to order from the SSL Type drop-down. The drop-down will list only the

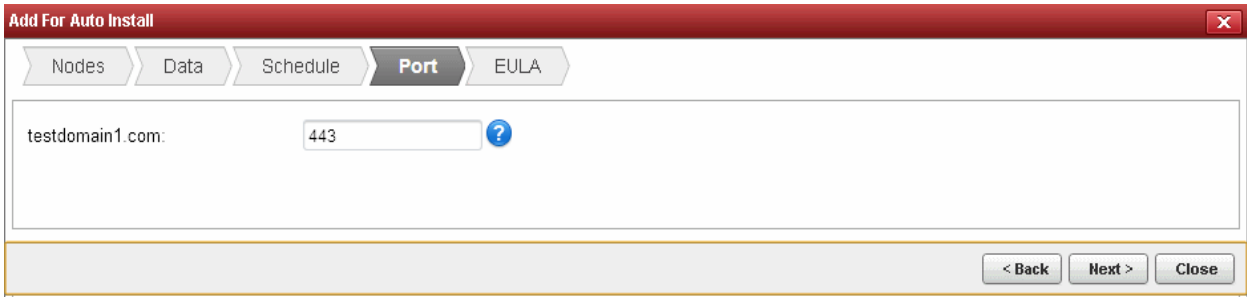
certificate types that are enabled for the Organization. See section **Comodo SSL Certificates** for a list of certificate types.

- Select the term length of the certificate from the Term drop-down.
- Enter the parameter(s) for custom field(s) such as 'Employee Code, Telephone' (if any) added for the SSL enrollment forms. Refer to the section **Custom Fields** for more details.
- Click Next. The 'Schedule' interface will be opened.

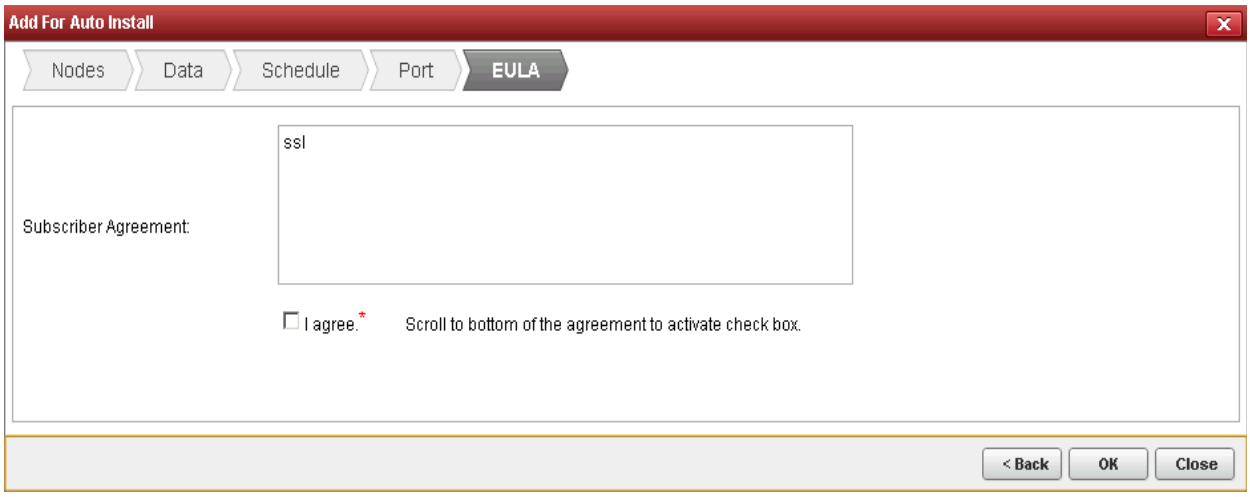


- If you want to manually install the certificate, select 'Manual'
- If you want to install the certificate at a scheduled time, select 'Schedule' and then select your time zone, and set a time period . The CSR will be generated and submitted to Comodo CA, during the first polling by the Agent, within the set time period.
- Click Next.

- If you are applying for a SSL certificate for a node with HTTP protocol, the Port interface will open. If you have chosen a node with HTTPS protocol, this step will be skipped and the **EULA interface** will open.

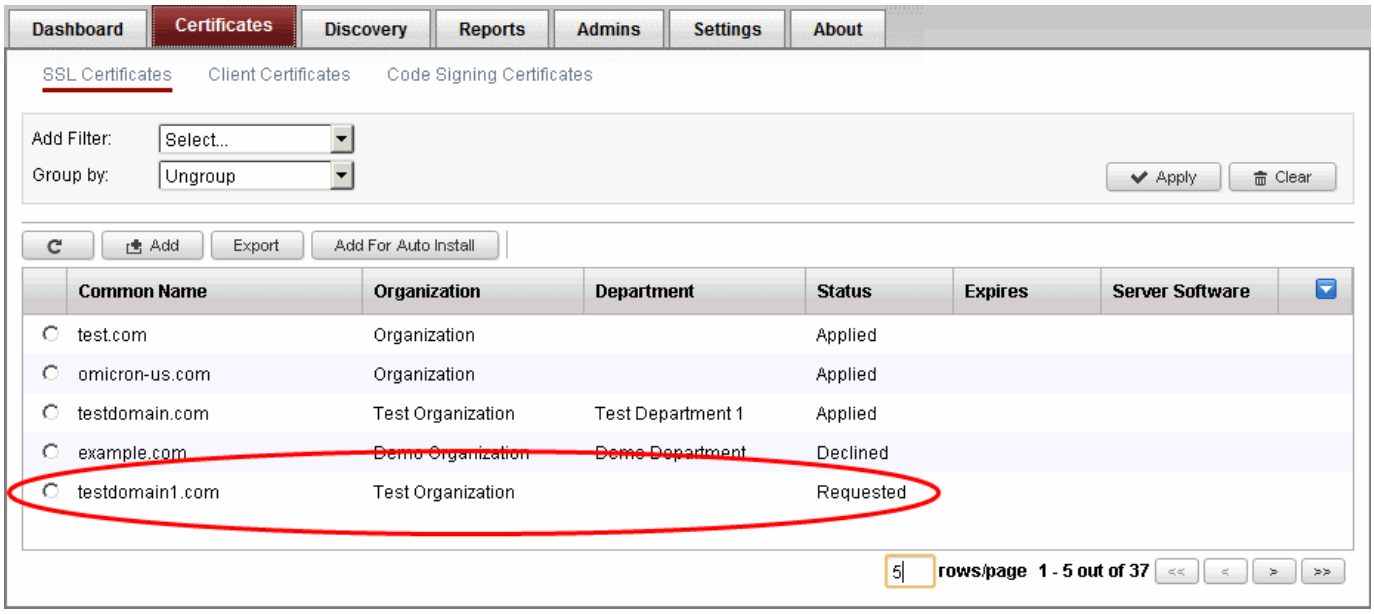


- Specify the HTTPS port for installing the certificate, (***Default = 443***)
- Click 'Next'. The EULA interface will open

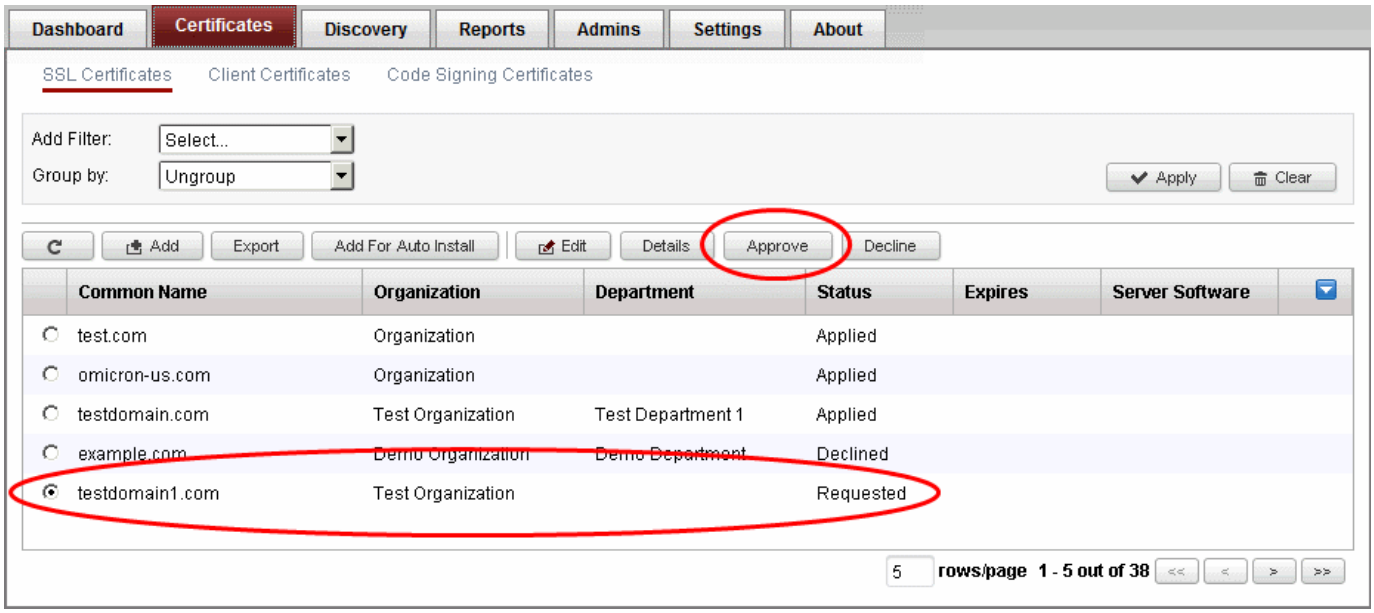


- Read the EULA fully and accept to it by selecting 'I Agree' checkbox.
- Click OK to save your application.

The certificate will be added to the SSL Certificates interface and its status will be displayed as 'Requested'.

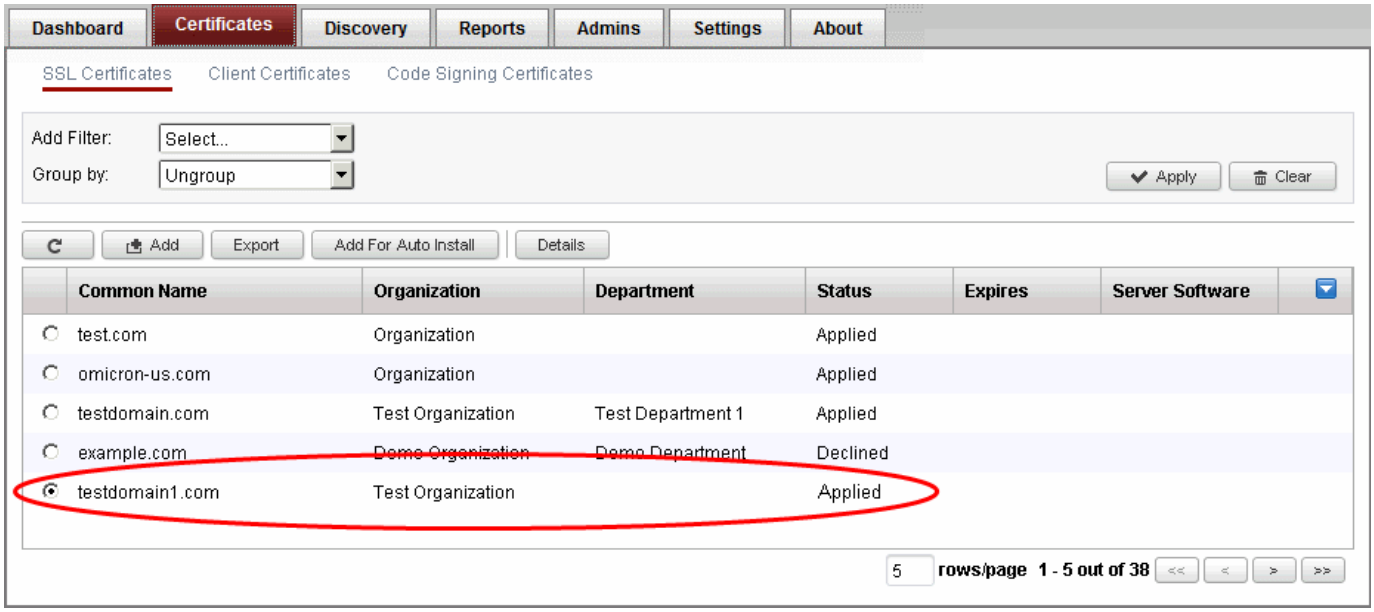


- The Agent will generate a CSR for the requested certificate automatically during its first polling cycle in the set schedule period. If you want to generate the CSR instantly, click 'Refresh'. On successful creation of CSR, the 'Approve' button will appear for the certificate.

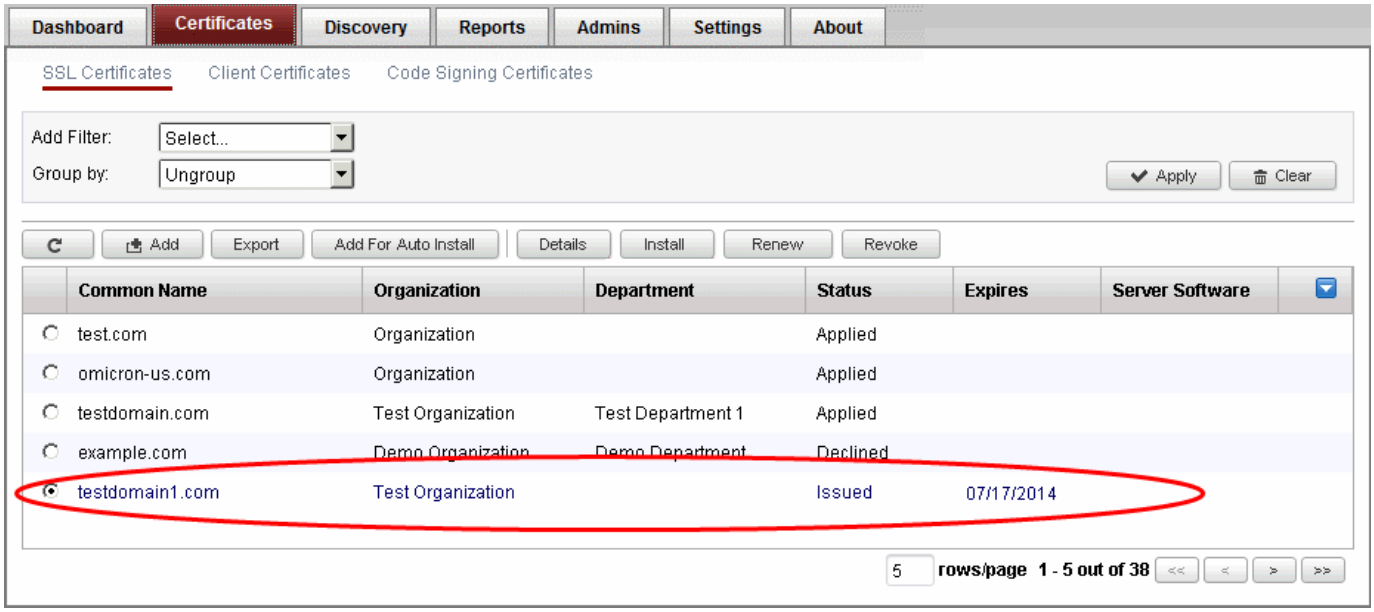


- Click the 'Approve' button to approve the request, enter the approval message in the 'Approval Message' dialog and click 'OK'.

On approval, the CSR will be submitted to Comodo CA to apply for the certificate. The certificate status will be changed to 'Applied'.

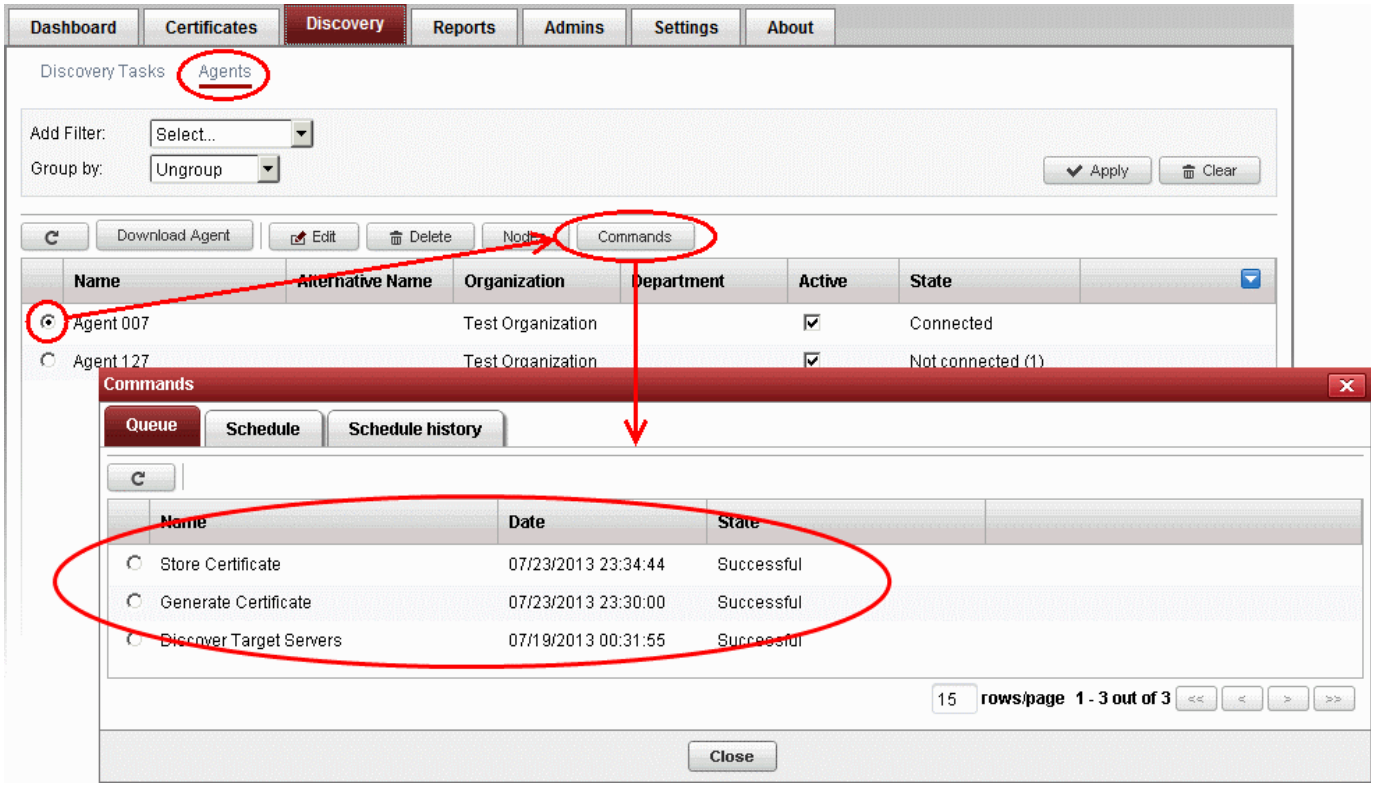


The Agent will track the order number and download the certificate from the CA, once it is issued and stores it. The certificate status will be changed to 'Issued'.

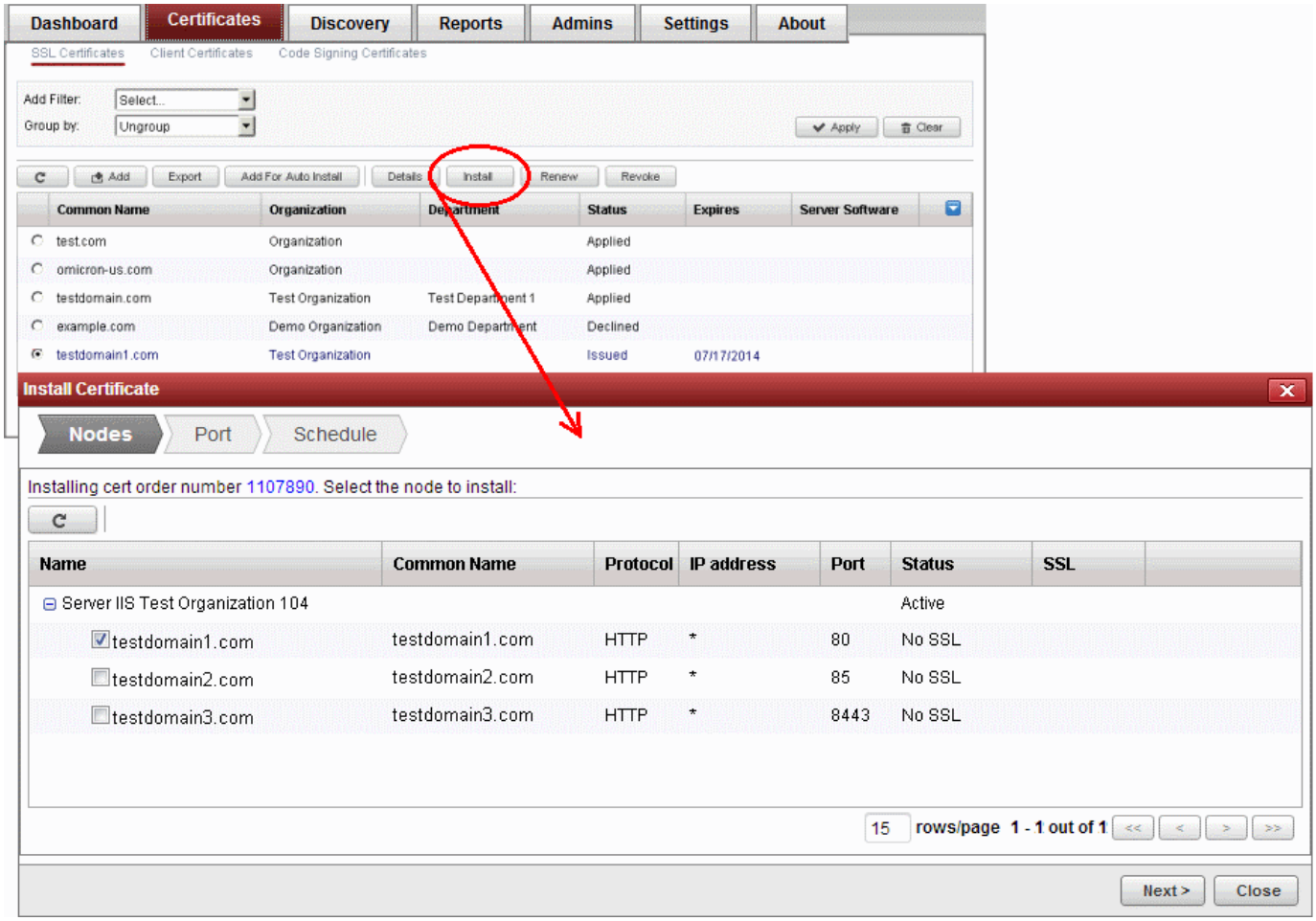


- To check whether the Agent has stored the certificate, click Discovery > Agents
- Select the Agent and click 'Commands' from the top

You will see successful execution of 'Store Certificate' command.



- To install the certificate, click 'Install' from the 'Certificates Management' interface.

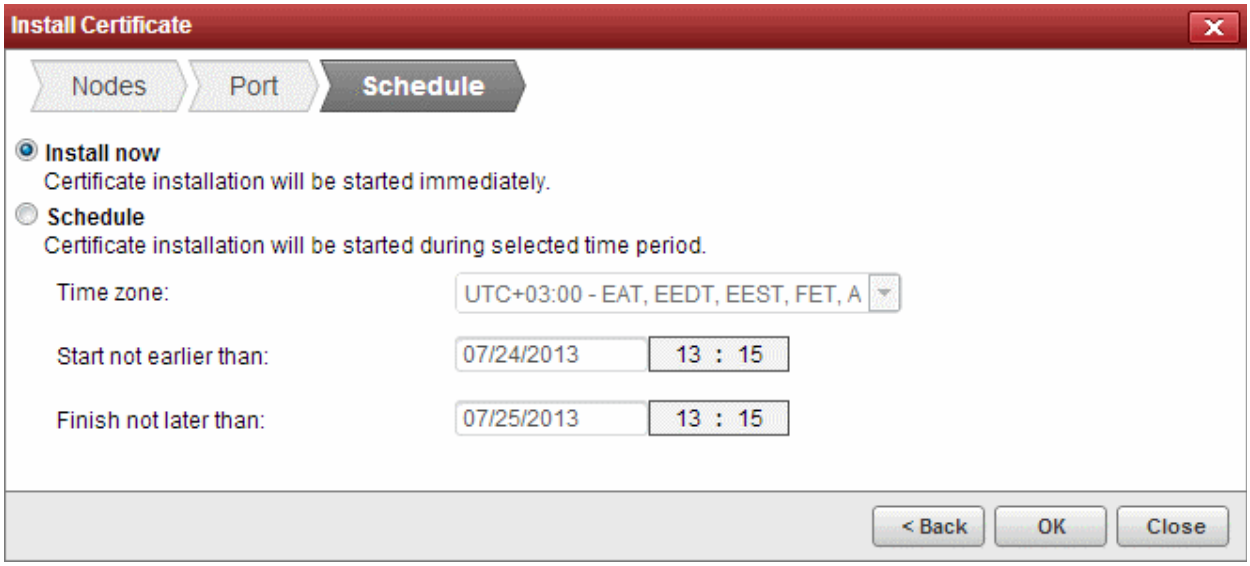


The 'Install Certificate' dialog will be displayed with the nodes interface opened. The node upon which the certificate is to be installed is pre-selected.

- If you want to install the same certificate to additional nodes or to a different node, select the node(s) as required
- Click 'Next'.

- If you have chosen to install the certificate on to a node with HTTP protocol, the 'Port' interface will open to specify the HTTPS port on to which the certificate has to be installed. If you have chosen a node with HTTPS protocol, this step will be skipped and the **Schedule interface** will open.

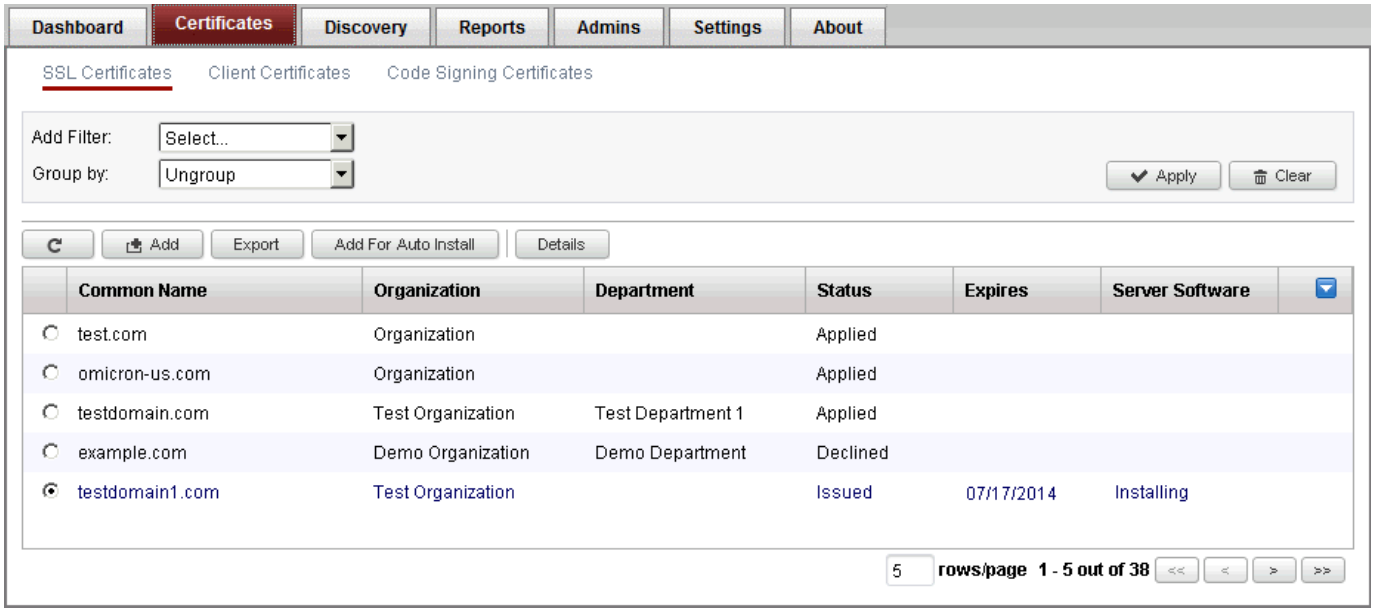
- Specify the port and click 'Next'. The 'Schedule' interface will open.



- If you want to instantly install the certificate, select 'Install now'
- If you want to install the certificate at a later time, select 'Schedule', then select your time zone, and set a time period. The Agent will install the certificate when it polls the CCM for the first time, within the set time period.

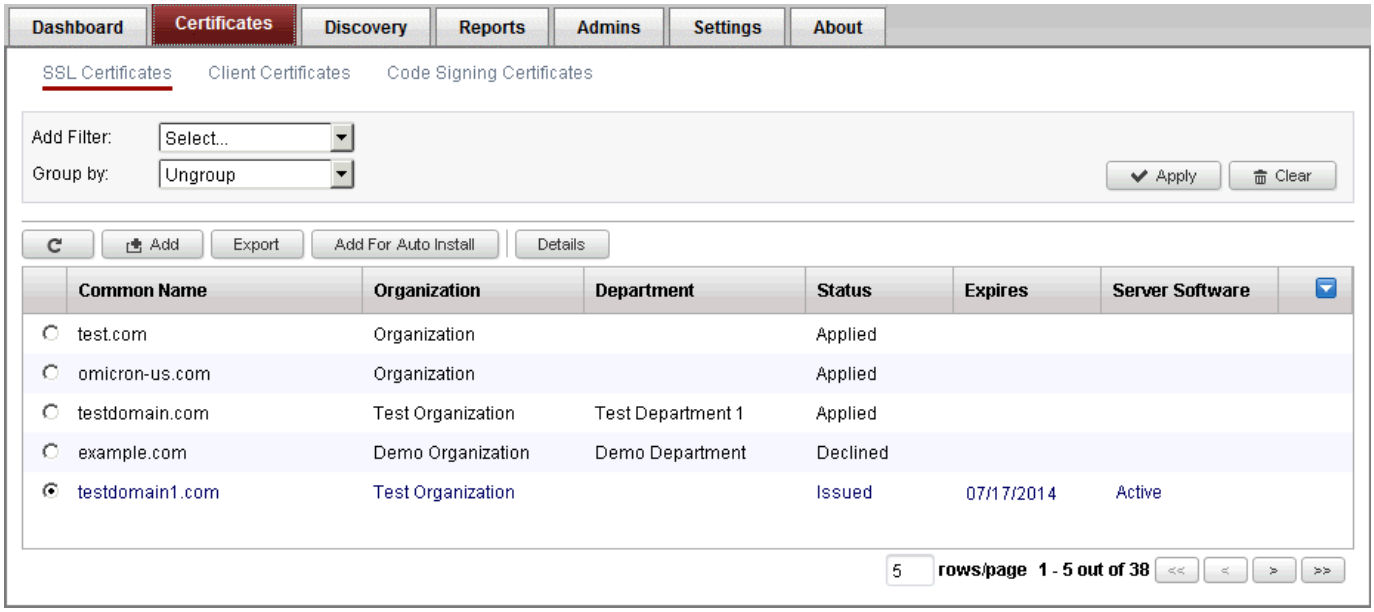
- Click OK

The certificate installation will begin instantly or at the scheduled time as set in the 'Schedule' interface and the Server Software state of the certificate will be displayed as 'Installing...'

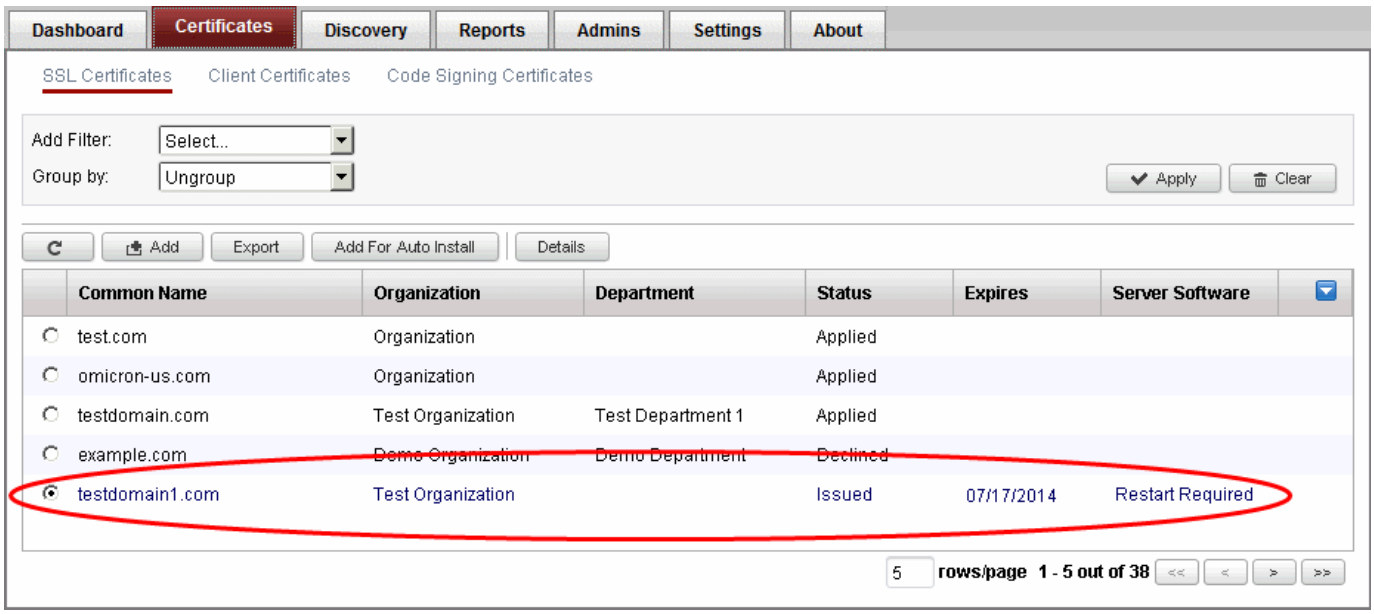


Upon completion of installation,

- For IIS servers and Tomcat servers: the certificate will be activated immediately and the Server Software state will be indicated as 'Active'.



- For Apache servers: the certificate will be activated upon restart of the server. The Server Software state will be indicated as 'Restart Required'.

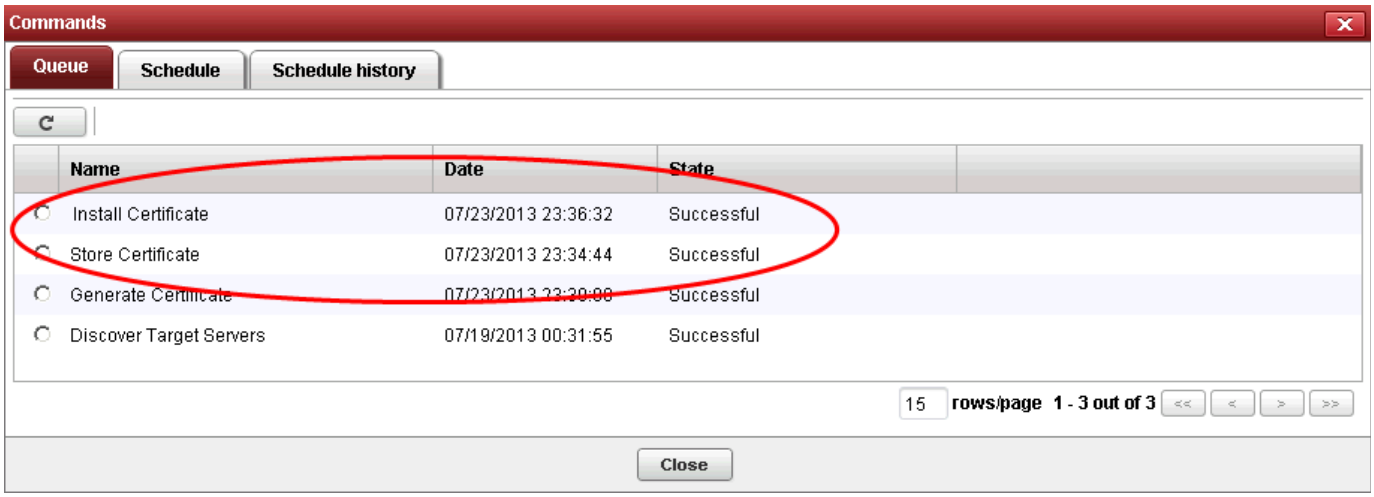


Tip: The server can be restarted from CCM through the **Certificate Details** dialog. For more details, refer to the section **Restarting Apache after Auto-Installation of SSL Certificate**

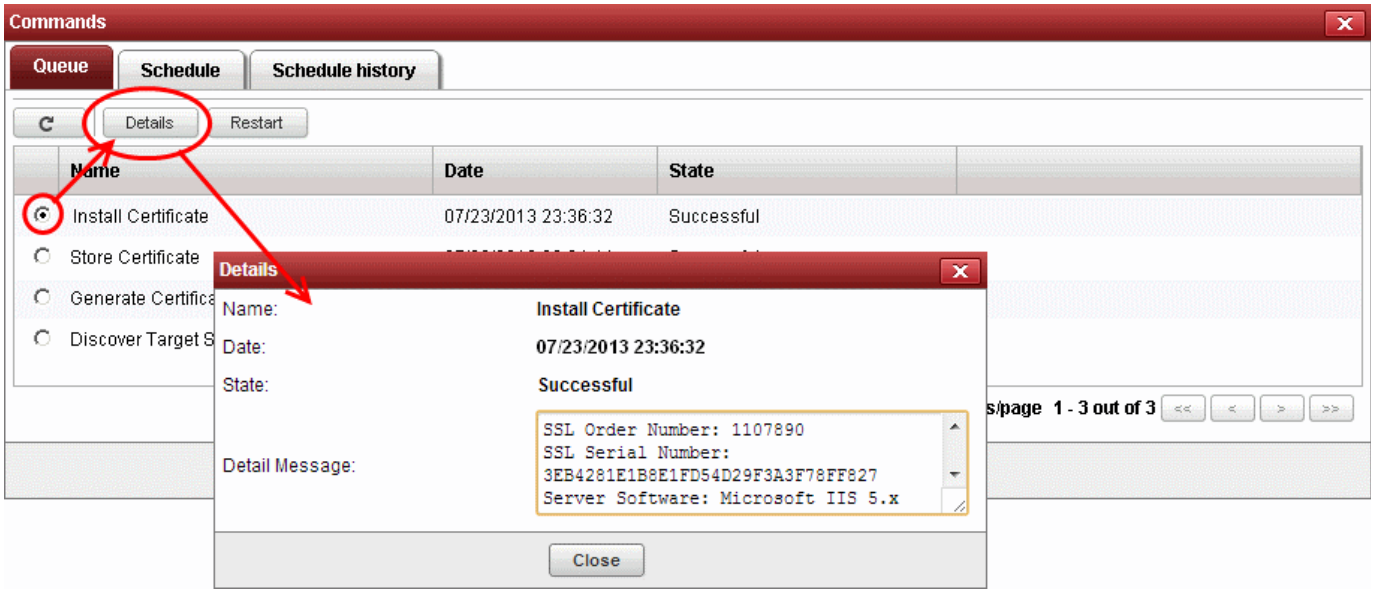
Upon restarting the server, the certificate will be activated and the Server Software state will be indicated as 'Active'.

- To check whether the Agent has installed the certificate, click Discovery > Agents
- Select the agent and click the 'Commands' button.

You will see successful execution of 'Install Certificate' command.



- To view the details of the command, select the command and click the 'Details' button from the top.



3.1.2.3 Initiating SSL Enrollment using Application Forms

The SSL Administrators or the applicants authorized by them can make request for certificates to be installed on to the web servers by submission of application forms. On successful submission and validation by Comodo CA, the certificate will be issued and a notification email will be sent to the applicant. The applicant can download the certificate and install it on to respective web server.

CCM offers two types of SSL application forms:

1. **The Self Enrollment Form** - Administrators can apply or direct applicants to the request form to order SSL certificates. Applicants using this method must validate their application to Certificate Manager by:

   i. Entering the appropriate **Access Code** for the Organization or Department. The Access Code is a mixture of alpha and numeric characters that the applicant needs to provide in order to authenticate the request to Certificate Manager.
   and

   ii. The email address they enter must be from the domain that the certificate application is for. This domain must have been assigned to the Organization or Department.

   Refer to the section **Method 1 - Self Enrollment Form** for a tutorial on applying for and installing certificates through the self-enrollment form.

2. **The Built-in Application** Form to make a request directly from the Certificate Manager Interface. Administrators can login and request SSL certificates using the built-in application form available at the Certificates Management > SSL

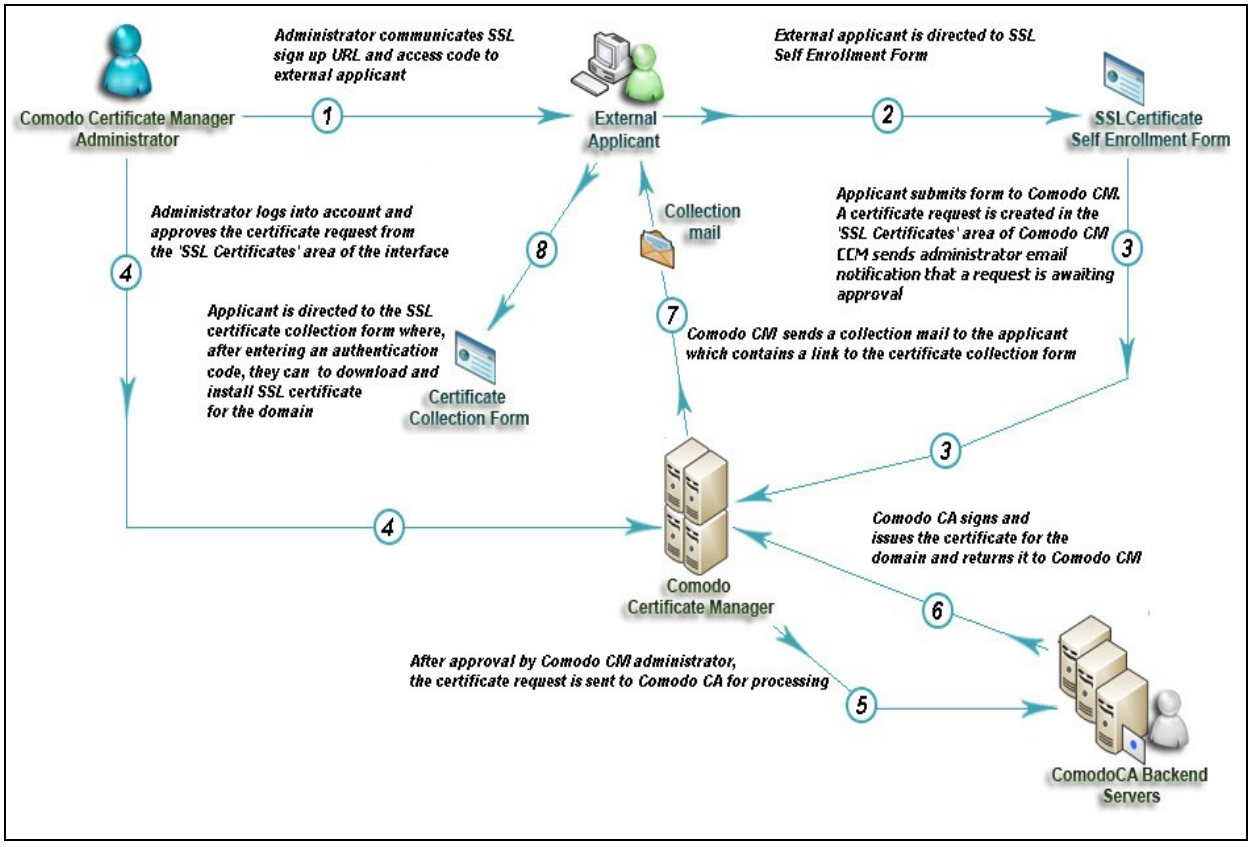
Certificates area.

Refer to the section **Method 2 - Built-in Enrollment Form** for a tutorial on applying for and installing certificates through the Built-in application form.

On successful completion of application submission, the certificate will be added to the Certificates Management > SSL Certificates area with the status 'Requested'. An appropriately privileged SSL administrator should **approve** the request. On approval, CCM will forward the application to Comodo CA. After validating the application, the CA will issue the certificate and the certificate status will be changes to Issued in the SSL certificates area of the CCM interface. A collection email will be sent to the administrator or the applicant. The applicant can collect, download and install the certificate in the respective web server. For more details on collection of the certificate, refer to the section **Certificate Collection**. For more details on downloading and installing the certificate, refer to the section **Downloading and Importing SSL Certificates**.

Background Note: It is possible for one Organization to have multiple certificates for different domain names. See **5.2.2.3.2 General Settings - Table of Parameters** if you would like to read more about this at this time.

3.1.2.3.1 Method 1 - Self Enrollment Form



3.1.2.3.1.1 Initiating the Self Enrollment Process

After completing the **prerequisite steps**, the administrator needs to communicate enrollment details to all and any end-users they wish to issue SSL certificates to (for example, via email). The communication must contain the following information:

1. A link to the Self Enrollment Form - https://cert-manager.com/customer/[REAL CUSTOMER URI]/ssl
2. The Access Code specified in the Organization or Department's **SSL settings tab**.

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

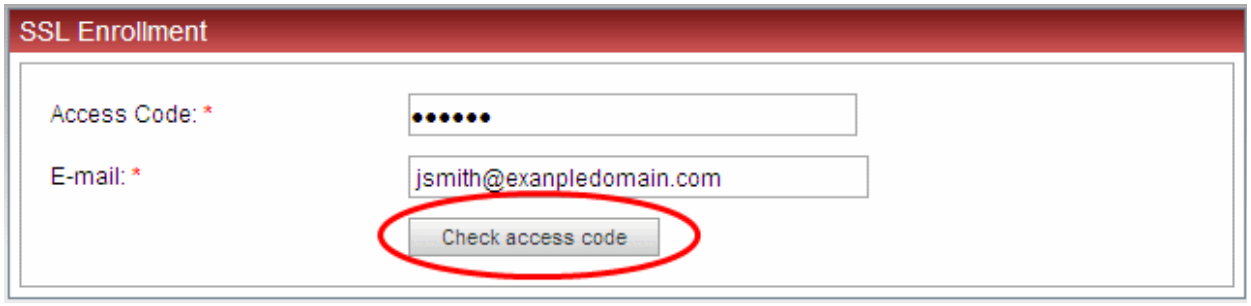
3.1.2.3.1.2 The Self Enrollment Form

The application form for SSL certificates is hosted, by default, at: https://cert-manager.com/customer/[REAL CUSTOMER

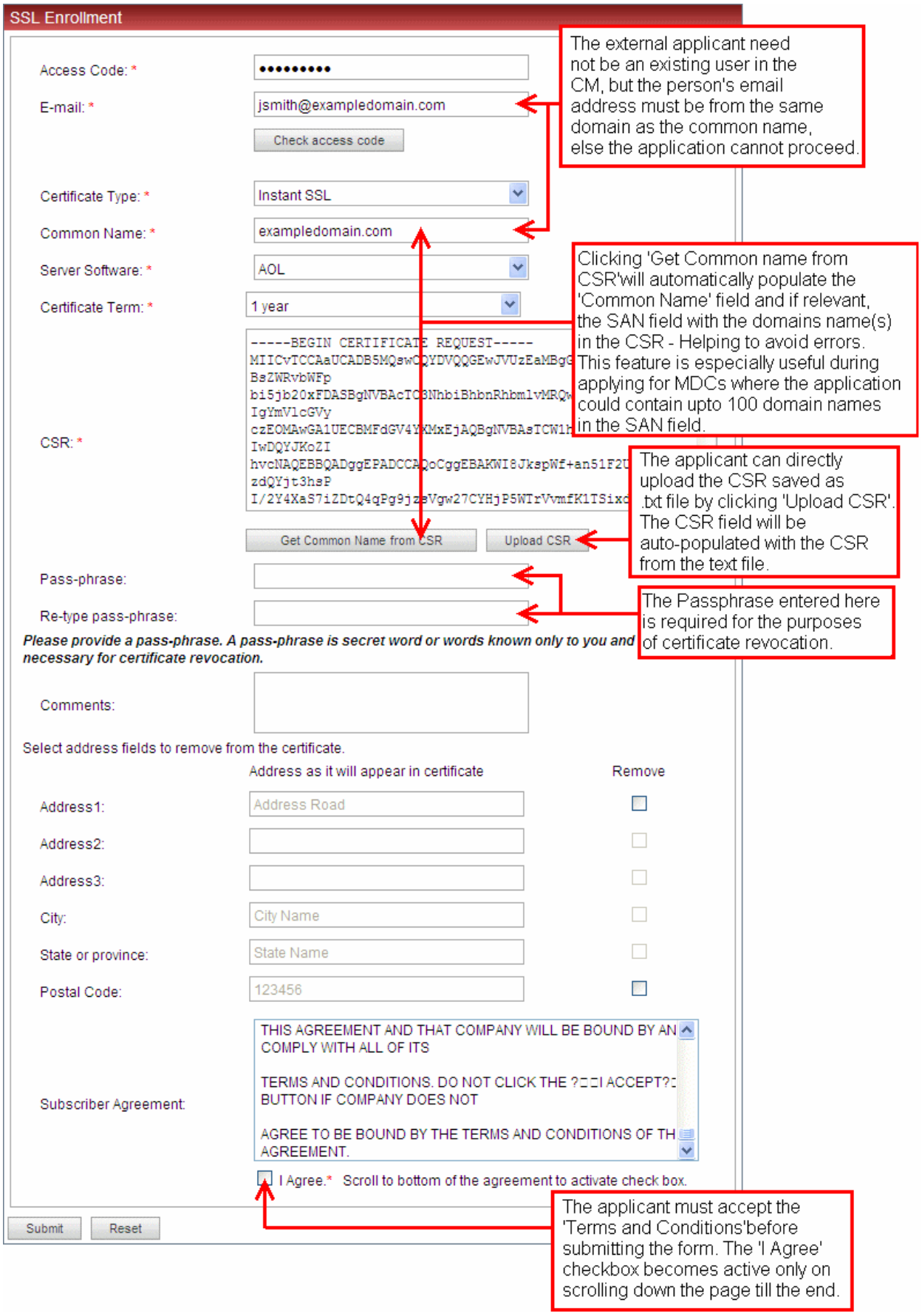
URI]/ssl

End-users should be directed to this page using the administrators preferred communication method. Please refer to the preceding section, **Initiating the Self Enrollment Process** for more details.

- Clicking the 'Certificate enrollment' link will open the self enrollment form



- Before proceeding to the full application form, the applicant has to authenticate the request by:
  - Entering the correct Access Code for the Organization or Department
  - Entering an email address from a domain that has been assigned to that Organization or Department.
- Clicking the 'Check Access Code' will contact CCM to authenticate that the applicant has the right to apply for a certificate
- If both Access Code and E-mail address are successfully verified then the applicant will move onto the full certificate application form:

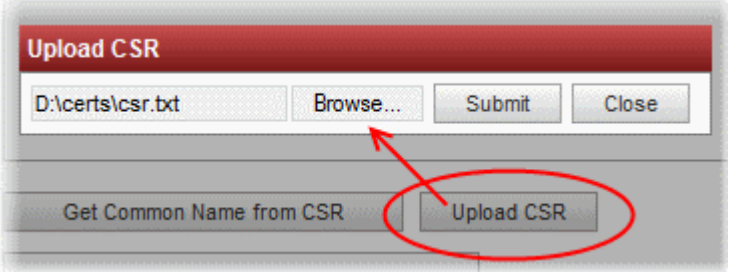


- The 'Access Code' and 'E-mail' address fields will be pre-populated.
- The domain that the user specifies in the 'CN' field must be the same domain as the applicant's E-mail address. The applicant MUST be able to receive emails at this address.

- Comodo provide a range of CSR generation documents designed to assist Administrators and external applicants through the CSR creation process. For a list of these documents, please visit: **https://support.Comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav=0** . (Select 'CSR generation' section and web server software).
- It is possible for Certificate Manager Account holders to use their own, custom form templates rather than the default form supplied by Comodo. Contact your account manager for more details on enabling this functionality and for submitting custom banners for application forms

3.1.2.3.1.3 Form Parameters

Form Element	Type	Description
Access Code ***(required)***	Text Field	An Access Code identifies a particular 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 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. Administrators should choose a complex Access Code containing a mixture of alpha and numeric characters that cannot easily be guessed. This code should be conveyed to the applicant(s) along with the URL of the sign up form. Applicants that request a certificate using the Self Enrollment Form will need to enter this code.
Email ***(required)***	Text Field	Applicant should enter their full email address. The email address must be for a domain that has been assigned to the Organization or Department.
Certificate Type ***(required)***	Drop-down list	Applicant should select certificate type. For a list of Comodo SSL certificate types, see the section **Comodo SSL Certificates.** The specific certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections **Creating a new Organization**, **Customize an Organization's SSL Certificate Types** and **SSL Types** for more details.
Common Name ***(required)***	Text Field	Applicants should enter the correct fully qualified domain name for the Organization or Department Single Domain certificates - enter domain name using the form: domain.com. Wildcard Certificates - enter domain name using the form: *.domain.com. Multi-Domain Certificates - enter the primary domain name using the form: domain.com.
Subject Alternative Names ***(required for Multi-Domain certificates)***	Text Field	If the certificate 'Type' is a Multi-Domain Certificate (MDC) then the applicant should list the 'Subj Alt Name' additional domains here. Each domain listed in this field should be separated by a comma.
Server Software ***(required)***	Drop-down list	Applicant should select the server software that is used to operate their web server (for example, Apache, IIS etc). Installation support documentation is available from the Comodo's support portal here: **https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav=0**
Certificate term ***(required)***	Drop-down list	Applicant should select the term length of the certificate. The term lengths of specific certificate types displayed in the drop-down list (and

Form Element	Type	Description
		therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections **Creating a new Organization** , **Customize an Organization's SSL Certificate Types** and **SSL Types** for more details.
CSR ***(required)***	Text Field	A Certificate Signing Request (CSR) is required to be entered into this field in order for Comodo CA to process your application and issue the certificate for the domain. The CSR can be entered in two ways: • Pasting the CSR directly into this field • Uploading the CSR saved as a .txt file by clicking the 'Upload CSR' button **Background:** In public key infrastructure systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority 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 chosen 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 certificate authority, and the certificate authority may contact the applicant for further information. Upon uploading or pasting the CSR, the form will automatically parse the CSR. Administrators that require assistance to generate a CSR should consult the Comodo knowledge article for their web server type here: **https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,1** **Special Note regarding MDC applications:** The CSR you generate only needs to be for the single 'Common Name' (aka 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 ***(optional)***	Control	Once the CSR has been entered correctly, clicking this button will auto-populate the Common Name (CN) field. Using this method helps to avoid human error by ensuring the domain name mentioned in the application form exactly match that in the CSR. If the domain name mentioned in this application form do not match that in the CSR, then Comodo CA will not be able to issue the certificate. **Special Note regarding MDC applications:** In order to successfully order a Multi-Domain Certificate, the applicant need 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 Subject Alternative Names. In this case, clicking the 'Get CN from CSR' button will also auto-populate the 'Subject Alternative Names' form fields as well as the 'Common Name' field.
Upload CSR ***(optional)***	Control	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 - helping to avoid errors. 

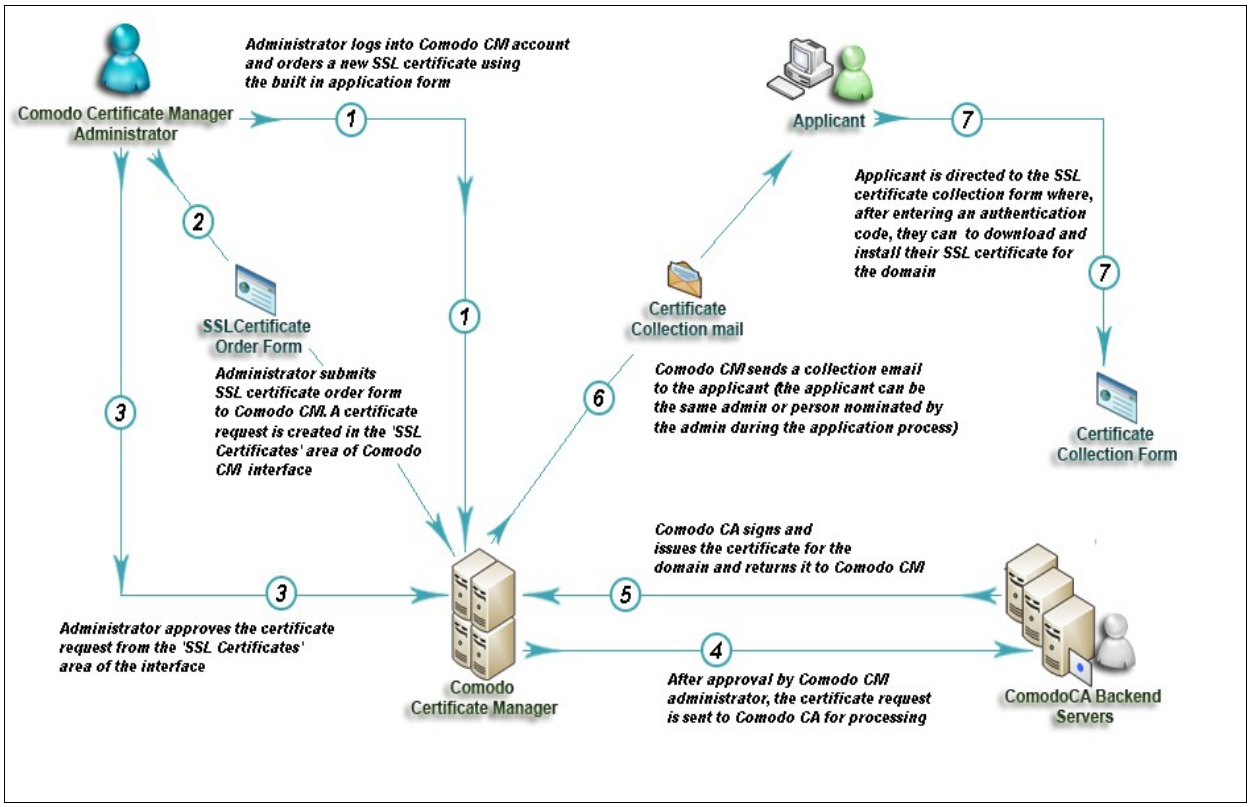
Form Element	Type	Description
Pass Phrase ***(optional)***	Text Field	This phrase is needed to revoke the certificate when using the external revocation page at: https://cert-manager.com/customer/real_customer_uri/ssl?action=revoke

Form Element	Type	Description
Re-Enter Pass Phrase ***(required if specified in the field above)***	Text Field	Confirmation of the above.

Form Element	Type	Description
Comments ***(optional)***	Text Field	Applicant can enter information for the administrator.
Address 1: Address 2: Address 3: City: State or Province: Postal Code: (all auto-populated)	Text Fields	The address fields are auto-populated from the details in the '**General Settings**' tab 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**, the applicant can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields. The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted". For **EV level certificates**, it is mandatory to include and display address details in the certificates. Therefore, the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down.
Subscriber Agreement	Checkbox	Applicant must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox. **Note**: The Subscriber Agreement will differ depending on the type of SSL certificate selected from the 'Certificate Type' drop-down. If Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate is selected, The 'I Agree' checkbox will not be shown and the agreement will be taken as accepted, when the user submits the application.
Submit	Control	Submits the application.
Reset	Control	Clears all data entered on the form.

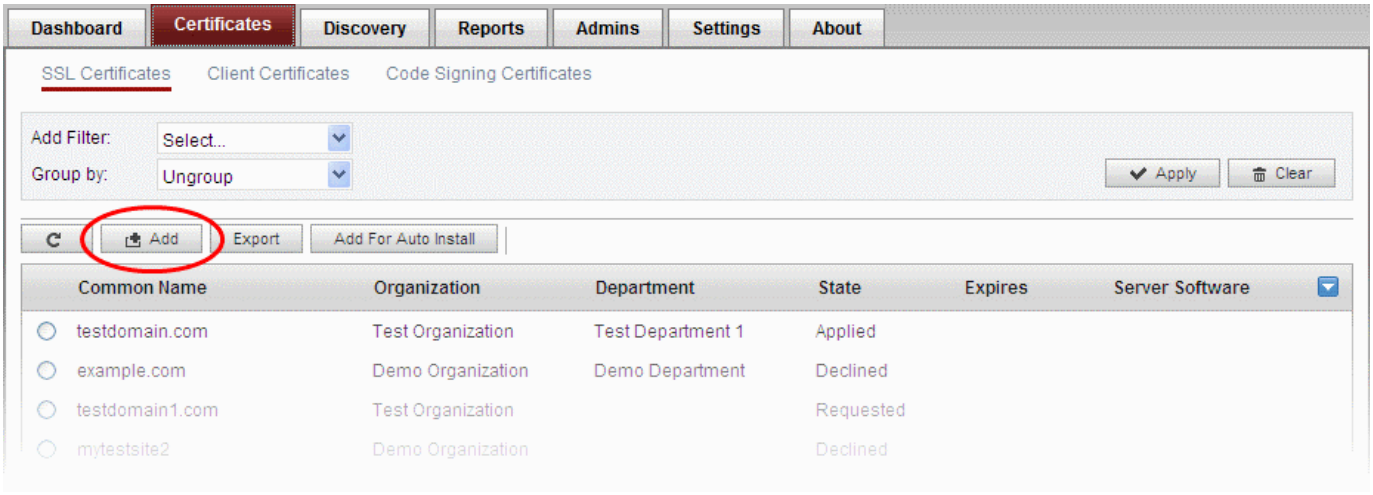
Note: In addition to the standard fields in the Self Enrollment form, custom fields such as 'Employee Code, Telephone' can be added by the MRAO Administrator. Refer to the section **Custom Fields** for more details.

3.1.2.3.2 Method 2 - Built-in Enrollment Form



3.1.2.3.2.1 Accessing the Built-in Application Form

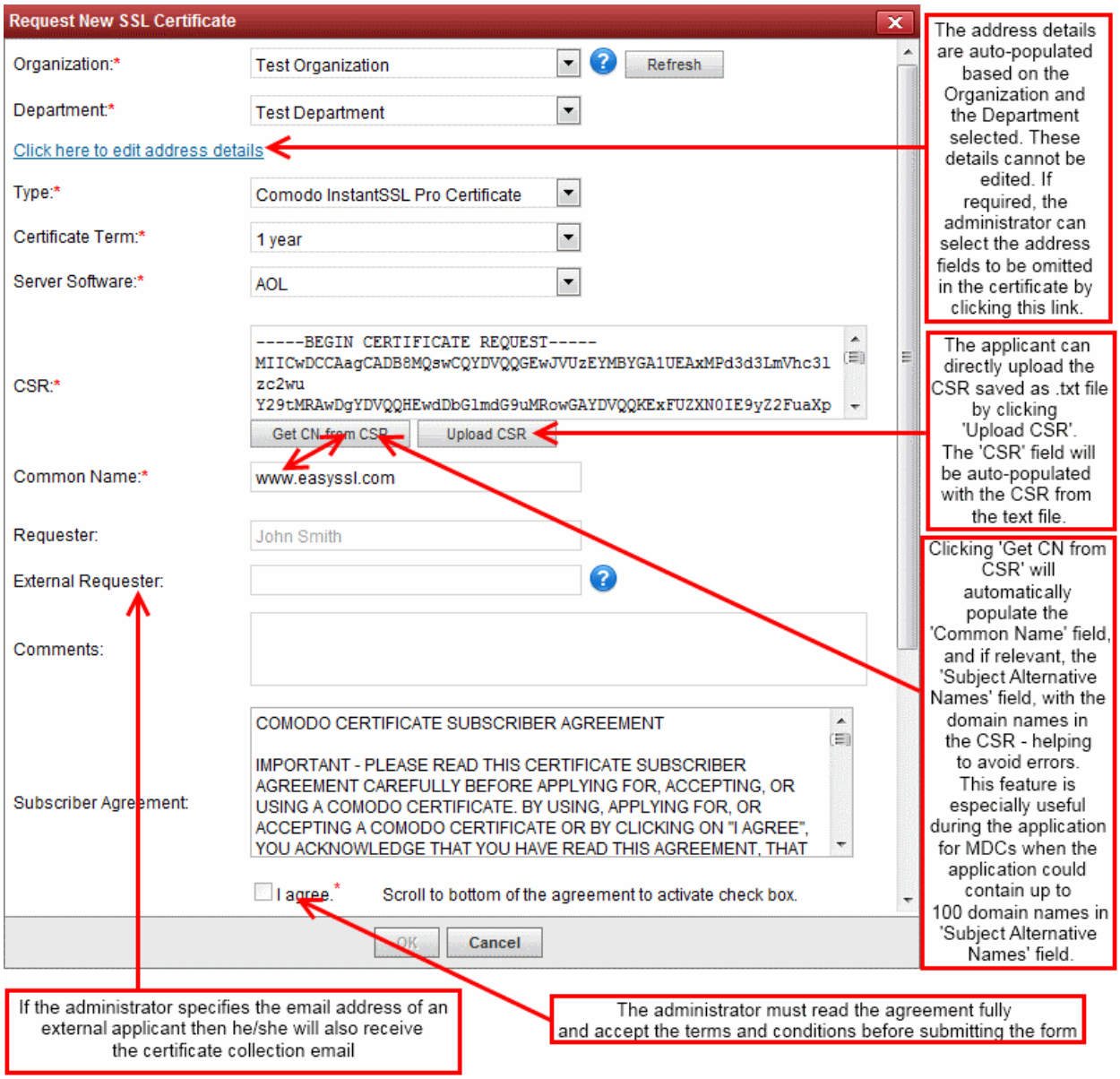
Certificate Manager administrators can apply for new certificates directly from the 'Certificate Management - SSL Certificates' area by clicking the 'Add' button (as shown).



Clicking the 'Add' button will open the built-in 'Request New SSL Certificate' form. The next sections of this guide will explain this form in more details.

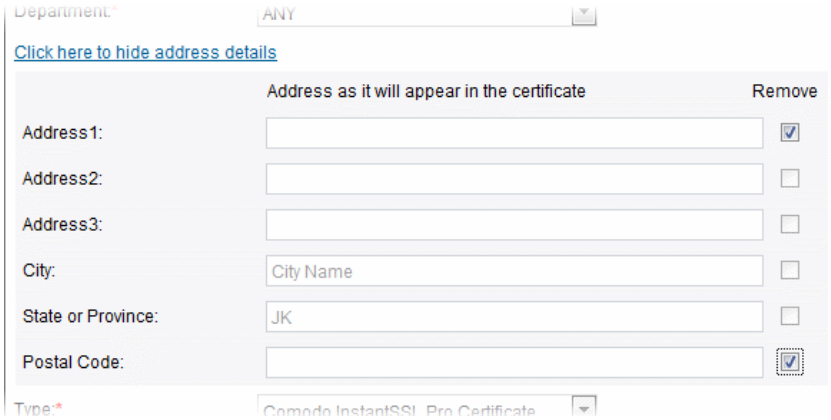
3.1.2.3.2.2 The Built-In Application Form

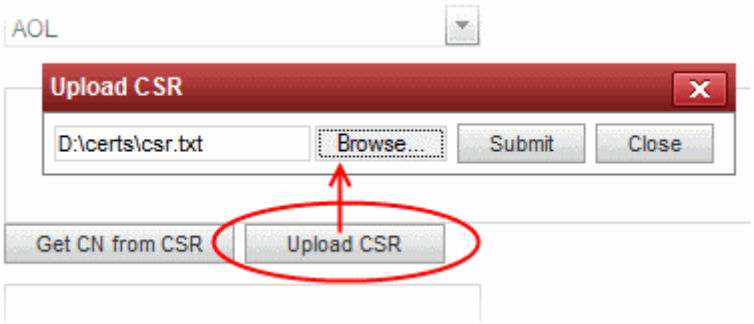
The built in SSL certificate application form is very similar to the Self Enrollment Form but does not require an Access Code:



Note: Each type of certificate has a slightly different form.

3.1.2.3.2.3 Form Parameters

Form Element	Type	Description
Organization (***required***)	*Drop-down list*	Administrators should choose the Organization that the SSL certificate will belong to.
Department (***required***)	*Drop-down list*	Administrators should choose the Department that the SSL certificate will belong to.
Click here to edit address details	*Text Fields*	Clicking this link will expand the address fields.  The address fields are auto-populated from the details in the '**General Properties**' tab 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, the administrator can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields. The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted". For **EV level certificates**, it is mandatory to include and display address details in the certificates. Therefore, the option to remove certain fields is not available on the built-in application form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Type' drop-down.
Type (***required***)	*Drop-down list*	Type of the certificate that the applicant wishes to order. See section **Comodo SSL Certificates** for a list of certificate types. The specific certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections **Creating a new Organization**, **Customize an Organization's SSL Certificate Types** and **SSL Type**s for more details.
Certificate Term (***required***)	*Drop-down list*	Administrators should select the term length of the certificate. See section **Comodo SSL Certificates** for a list of certificate types and term lengths. The term lengths of specific certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections **Creating a new Organization**, **Customize an Organization's SSL Certificate Types** and **SSL Types** for more details.
Server Software (***required***)	*Drop-down list*	Applicant should select the server software that is used to operate their web server (for example, Apache, IIS etc). Installation support documentation is available from Comodo support portal here: **https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav=0**
CSR (***required***)	*Text Field*	A Certificate Signing Request (CSR) is required to be entered into this field in order for Comodo CA to process your application and issue the certificate for the domain. The CSR can be entered in two ways: • Pasting the CSR directly into this field

Form Element	Type	Description
		• Uploading the CSR saved as a .txt file by clicking the 'Upload CSR' button **Background**: In public key infrastructure systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority 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 chosen 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 certificate authority, and the certificate authority may contact the applicant for further information. Upon uploading or pasting the CSR, the form will automatically parse the CSR. Administrators that require assistance to generate a CSR should consult the Comodo knowledgebase article for their web server type here: **https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,1** **Special Note regarding MDC applications**: The CSR you generate only needs to be for the single 'Common Name' (aka 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 (***optional***)	*Control*	Once the CSR has been pasted correctly, clicking this button will auto-populate the Common Name (CN) field. Using this method helps to avoid human error by ensuring the domain name mentioned in the application form exactly match that in the CSR. If the domain name mentioned in this application form do not match that in the CSR, then Comodo CA will not be able to issue the certificate. **Special Note regarding MDC applications**: In order to successfully order a Multi-Domain Certificate, the applicant need 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 Subject Alternative Names. In this case, clicking the 'Get CN from CSR' button will also auto-populate the 'Subject Alternative Names' form fields as well as the 'Common Name' field.
Upload CSR (***optional***)	*Control*	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 - helping to avoid errors. 
Common Name (***required***)	*Text Field*	Type the domain that the certificate will be issued to. Single Domain certificates - enter domain name using the form: domain.com. Wildcard Certificates - enter domain name using the form: *.domain.com. Multi-Domain Certificates: enter the primary domain name using the form: domain.com.
Subject Alternative Names (***required for Multi Domain certificates***)	*Text Field*	If the certificate 'Type' is a Multi-Domain Certificate (MDC) then the applicant should list the 'Subj Alt Name' additional domains here. Each domain should be separated by a comma.

Form Element	Type	Description
Requester (***auto-populated***)	*Text Field*	The 'Requester' is field is auto-populated with the name of the administrator making the application.
External Requester (***optional***)		As an alternative to making an applicant complete the **'Self Enrollment' form'**, the administrator can complete the application themselves using this built-in form and specify an 'External Requester'. Entering the email address of an external requester in this field will mean that person will also receive a certificate collection email. **Note**: The 'Requester' will still be the administrator that is completing this form (to view this, open the 'Certificates Management' area and click 'View' next to the certificate in question.) The email address of the 'External Requester' will be displayed as the 'External Requester' in the 'View' dialog of an issued certificate. This field is not required when requesting for EV SSL certificate and hence will be hidden.
Comments (***optional***)	*Text Field*	Enables administrator to add comments.
Subscriber Agreement (***required***)	*Control*	Applicant must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox. **Note**: The Subscriber Agreement will differ depending on the type of SSL certificate selected from the 'Certificate Type' drop-down. If Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate is selected, The 'I Agree' checkbox will not be shown and the agreement will be taken as accepted, when the user submits the application.
OK	*Control*	Submits the application to Certificate Manager for approval. If the form was completed correctly then the certificate will appear in the 'SSL' area with the state 'Requested'.
Cancel	*Control*	Cancels the application.

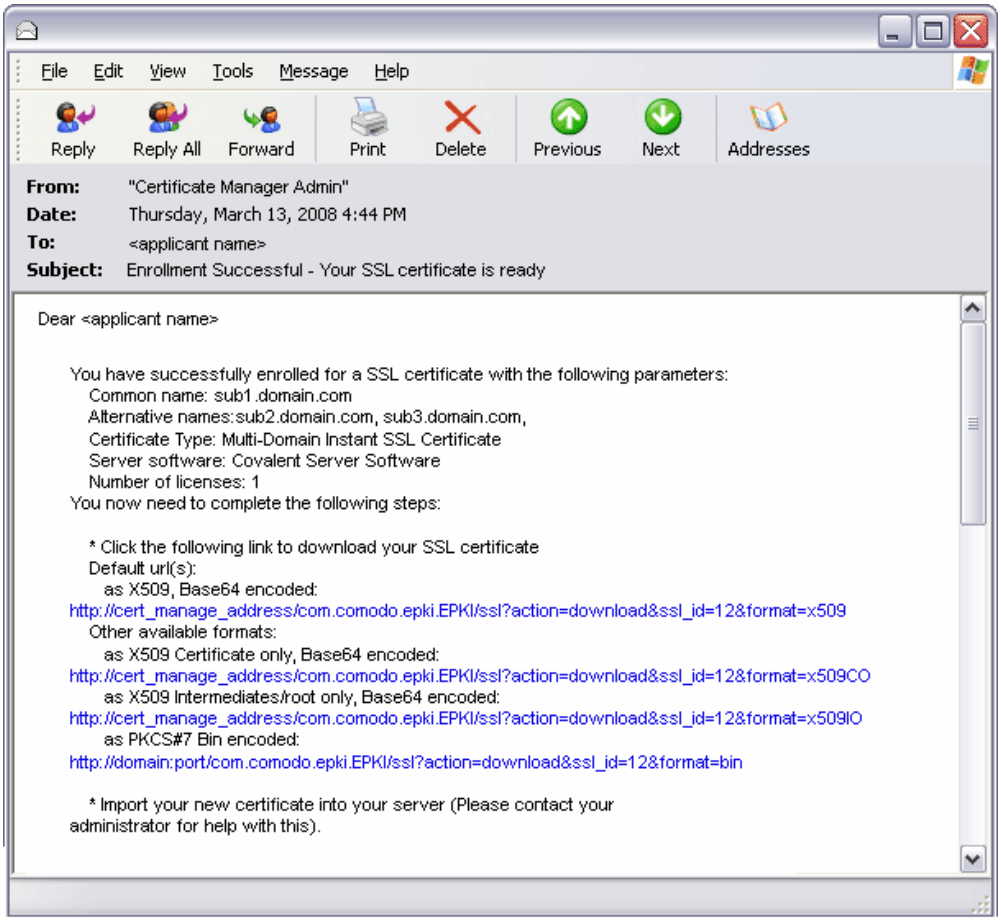
Note: In addition to the standard fields in the Enrollment form, custom fields such as 'Employee Code, Telephone' can be added by the MRAO Administrator. Refer to the section **Custom Fields** for more details.

3.1.2.3.3 Certificate Collection

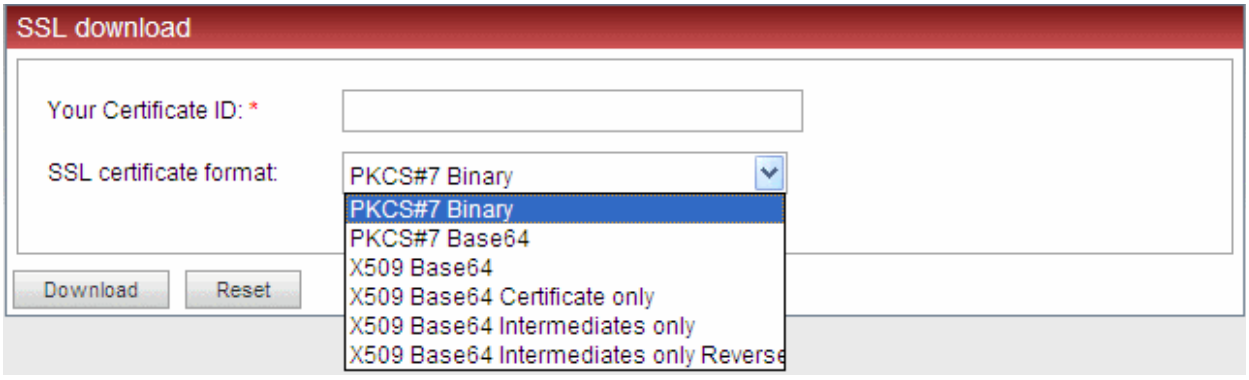
After Comodo CA has issued the certificate applied through the Built-in application form or the Self-enrollment form, the next stage of the provisioning process is for the applicant to download their certificate. Once the certificate has been issued, Comodo Certificate Manager will automatically send a collection email to the applicant. The certificate can be downloaded by the applicant by clicking the link in the email. Also, the issued SSL certificate can be downloaded by an MRAO, RAO SSL or DRAO SSL administrator from the **SSL Certificate Details dialog** accessed from the Certificates Management > SSL certificates tab

3.1.2.3.3.1 Collection of SSL Certificate Through Email

1. Once the certificate has been issued, Comodo Certificate Manager will automatically send a collection email to the applicant. This can be either an external applicant using the self enrollment method or a CCM administrator using the built-in application form.) The email will contain a summary of the certificate details, a link to the certificate collection form and a unique certificate ID that will be used for validation.



2. Having clicked the link in the collection email, the end-user will be taken to the certificate collection and download form:

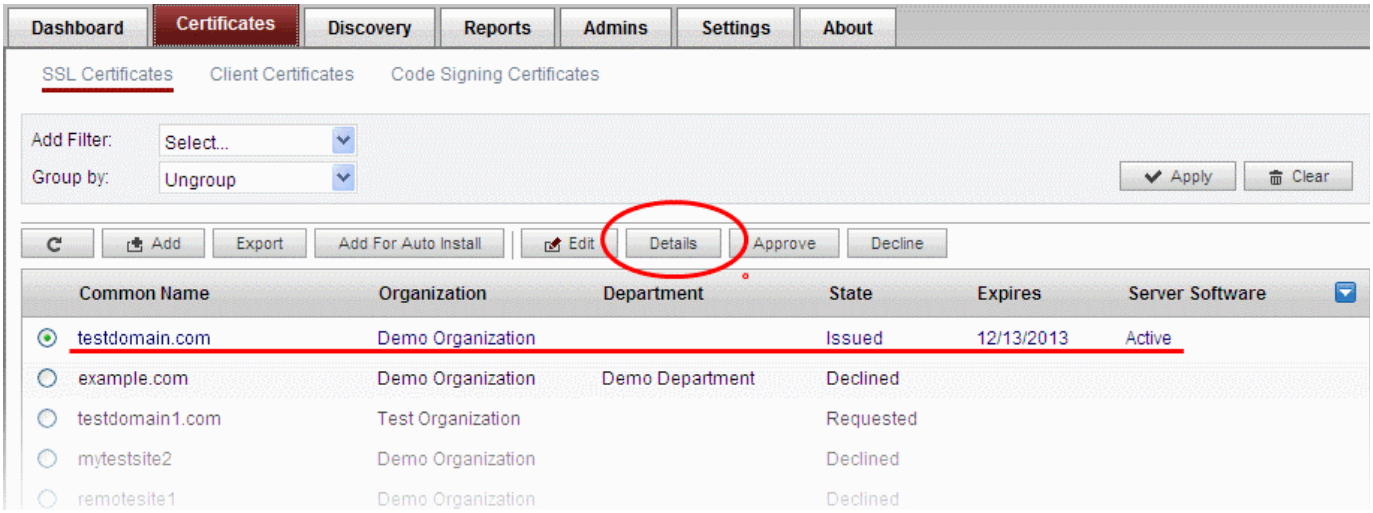


If the 'Certificate ID' is not already populated as a resulted of clicking on the link in the collection mail, then the applicant should copy and paste it in. The form also provides the opportunity to specify the format of the certificate. The applicant can now

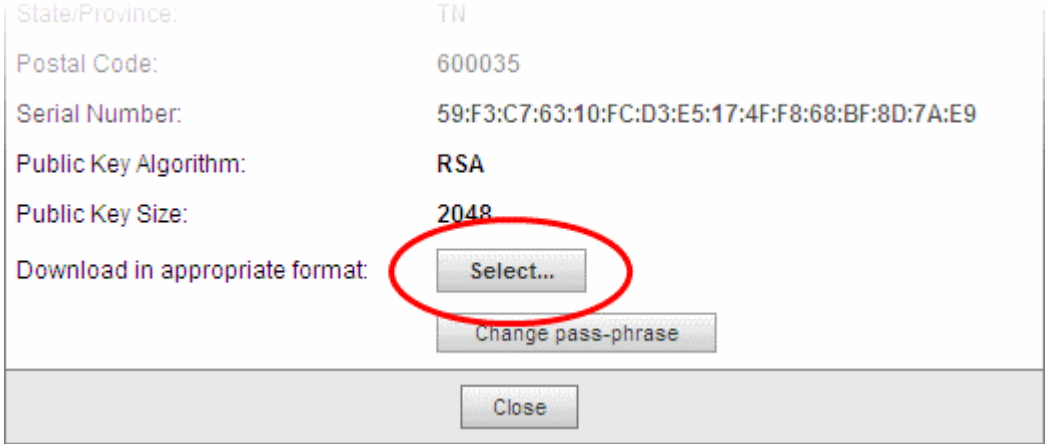
download, save and import the certificate.

3.1.2.3.3.2 Collection of SSL certificate by Administrator

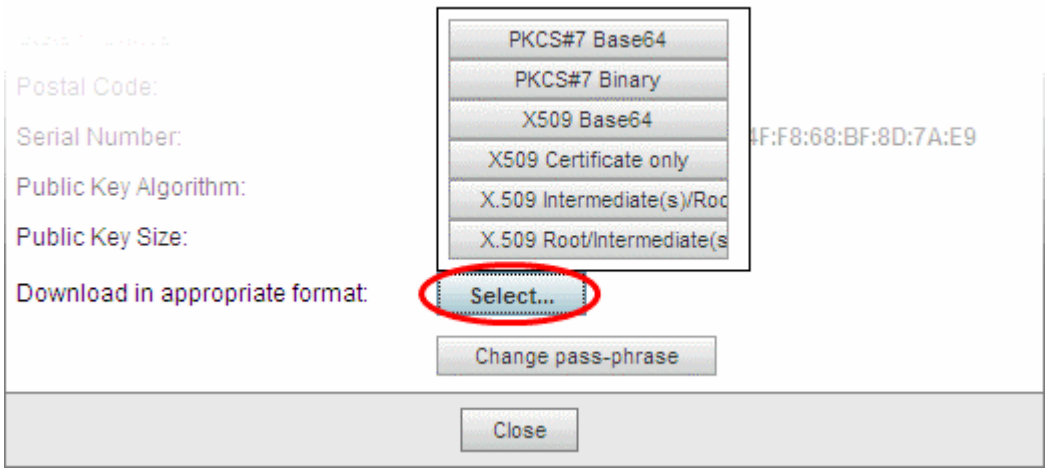
The issued certificate can also be downloaded and provided to the applicant from the **SSL Certificate Details dialog**. Click the 'Details' button at the top after selecting the issued certificate from the SSL Certificates tab of the Certificate management interface.



The resulting dialog contains options to download the issued certificate in several formats at its bottom:



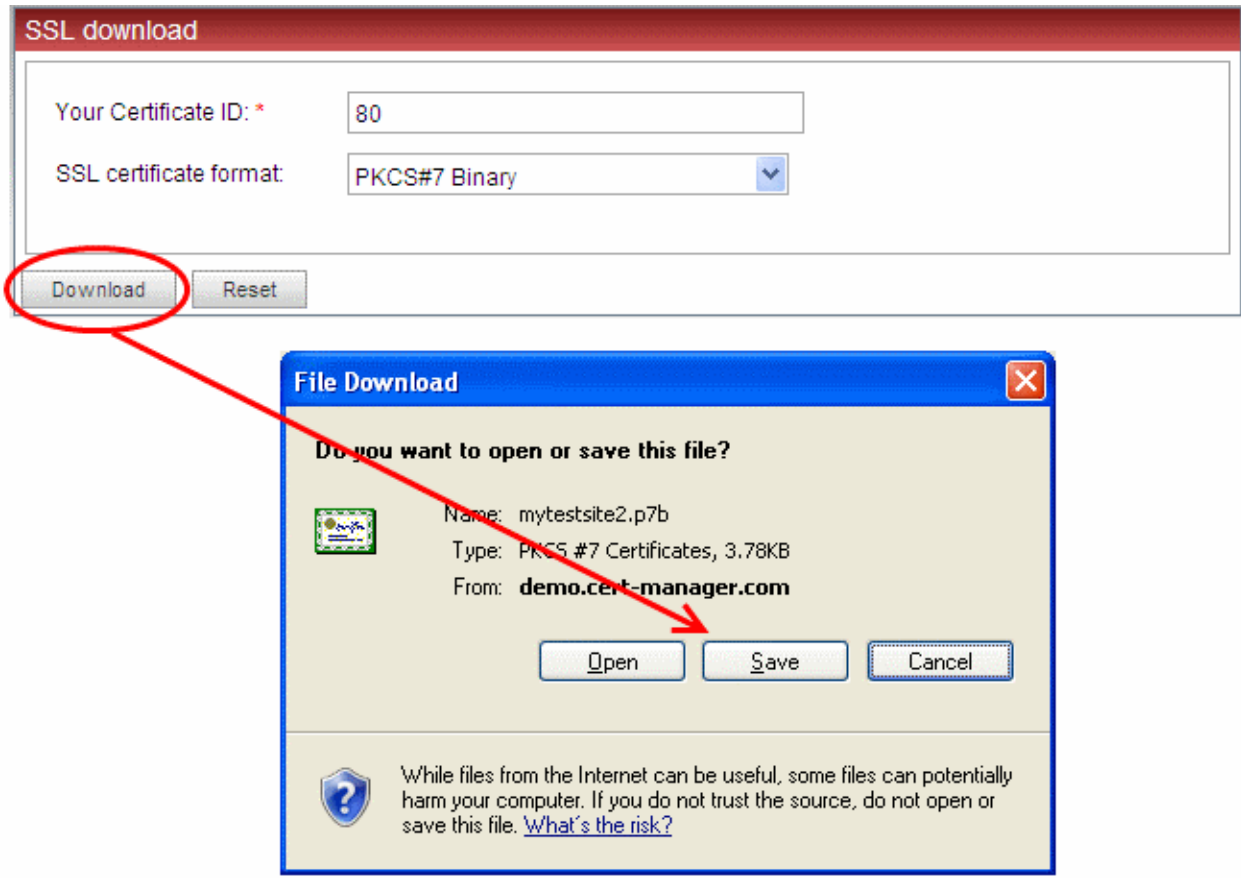
- Click the 'Select' button



- Click the appropriate button to download the certificate in desired format.

3.1.2.3.4 Downloading and Importing SSL Certificates

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



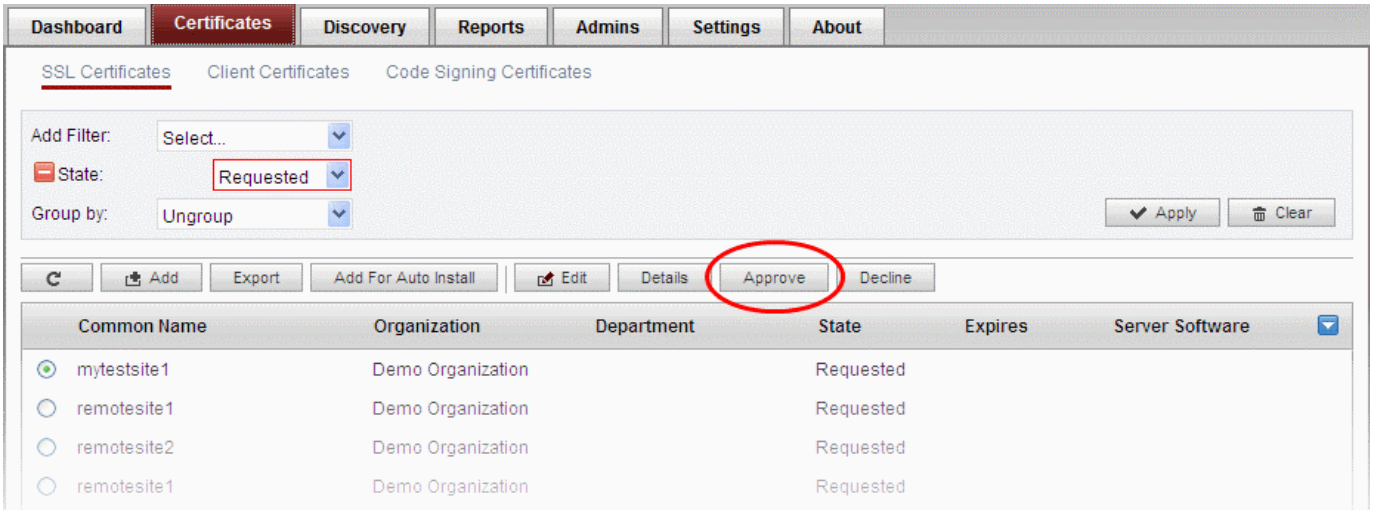
- Click 'Download' and save the certificate in your hard drive.

The precise installation process depends on the web server type and a range of installation guides are available at the Comodo support website at:
https://support.Comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav

First select the Comodo certificate type and then choose the appropriate web server software to view a detailed guide explaining the import process.

3.1.2.4 Certificate Requests - Approving, Declining, Viewing and Editing

A certificate request will appear in the 'SSL Certificates' area after the applicant has successfully applied for a certificate using either the **Auto Installer**, the **Self Enrollment Form** or the **Built-in application form**. Use the filter option to view all the certificates that are in 'Requested' state. Select the certificate that you want to approve, decline, view or edit.



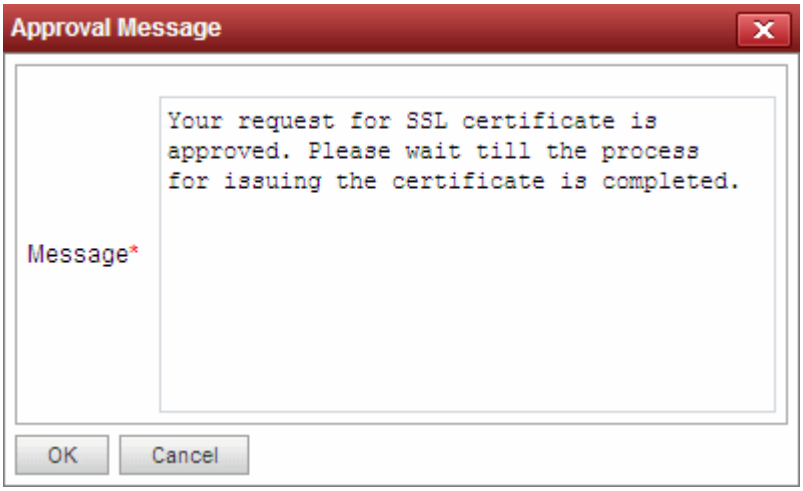
- At this point, the certificate request has NOT been submitted to Comodo CA and is pending approval from a Certificate Manager administrator. (If the application was made by an administrator, that administrator can, of course, approve their own request.)

If the administrator does not want to submit this request, they should click the 'Decline' button.

Note: Declining a certificate request will change the certificate status to 'Declined'. If an '**SSL Declined**' Notification has been set up then an email will be automatically sent to the requester informing them that the request has been declined.

However, this request can still be 'Approved' at any time in the future by a 'MRAO', 'RAO SSL' or 'DRAO SSL' administrator with appropriate privileges.

- If the administrator wishes to view the details of the request, they should click the 'Details' button at the top after selecting the checkbox next to the certificate name.
- If the administrator wishes to modify the request they should click the 'Edit' button. (for example, administrators may wish to correct certain request fields in the application before submitting to Comodo CA for processing).
- To approve the request and submit the application to Comodo CA for processing, administrators should click the 'Approve' button at the top.
    - After clicking the 'Approve' button, an 'Approval Message' box will be displayed. This allows the Administrator to type a message that will be sent along with the approval notification email.



    - Click 'OK' to add the message and send the approval email.

Note: The **SSL Approved Notification** should have been set up for the requester to receive the email notification.

- Once the Administrator has approved the request and submitted it to Comodo CA,the certificate state will be displayed as 'Approved'. If the request has applied by Comodo CA, the state of the certificate is changed to the proper value - 'Applied' (It also can be rejected by CA). Next, if validation is successful, then Comodo will send a **Certificate Collection** email to the certificate requester and the 'State' of the certificate will change to one of 'Issued'.

Please see the '**SSL Certificates**' chapter for full details of the options available in this area.

3.1.2.5 Certificate Renewal

There are two broad ways that SSL certificates can be renewed in CCM

- SSL administrators can renew certificates from the SSL certificates interface
- External applicants can renew using the self-renewal form

3.1.2.5.1 Certificate Renewal by Administrators

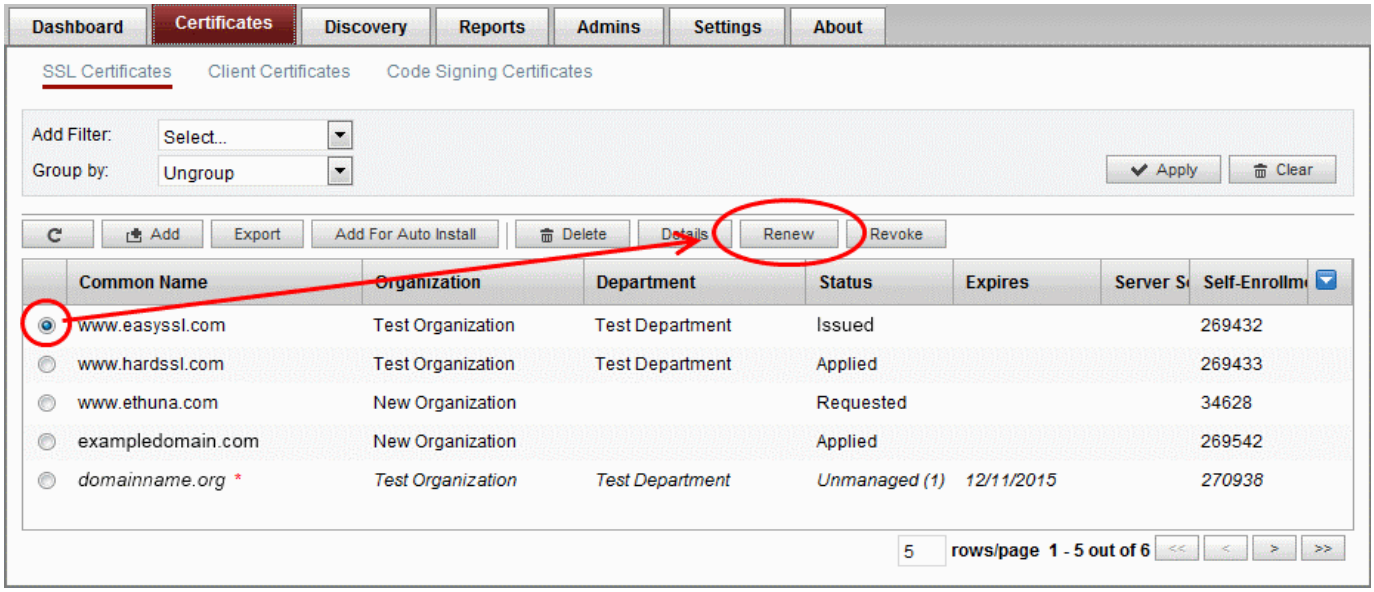
The SSL Certificates interface allows administrators to renew both managed certificates and unmanaged certificates. As the name suggests, unmanaged certificates are those are listed in CCM but are not currently managed by CCM. Usually these are certificates that were identified during discovery scans but were not originally ordered using CCM. The processes for renewing managed and unmanaged certificates are different.

Managed Certificates	Unmanaged Certificates
A 'managed certificate' is a certificate which has been issued, via CCM, to a specific combination of domain and organization. You will need to submit a CSR the first time you apply for a certificate for any such combination. After issuance, this certificate will become 'managed'. 'Managed' certificates are those with CCM statuses of 'Issued', 'Applied' or 'Requested' For renewals of 'managed' certificates, you will typically not need to submit a CSR because CCM shall re-use the existing CSR.	An 'unmanaged certificate' is a certificate which was found installed on servers during a discovery scan but was not issued via CCM. You will need to submit a new CSR during renewal of an 'Unmanaged' certificate because CCM does not have one on record. After issuance, this certificate will become 'managed'.

General note: If you moved a domain from one organization to another or modified the address details of an organization, then you are effectively creating a new certificate application, not 'renewing' a certificate. In these circumstances, you will also have to submit a new CSR.

Renewing a 'Managed' Certificate

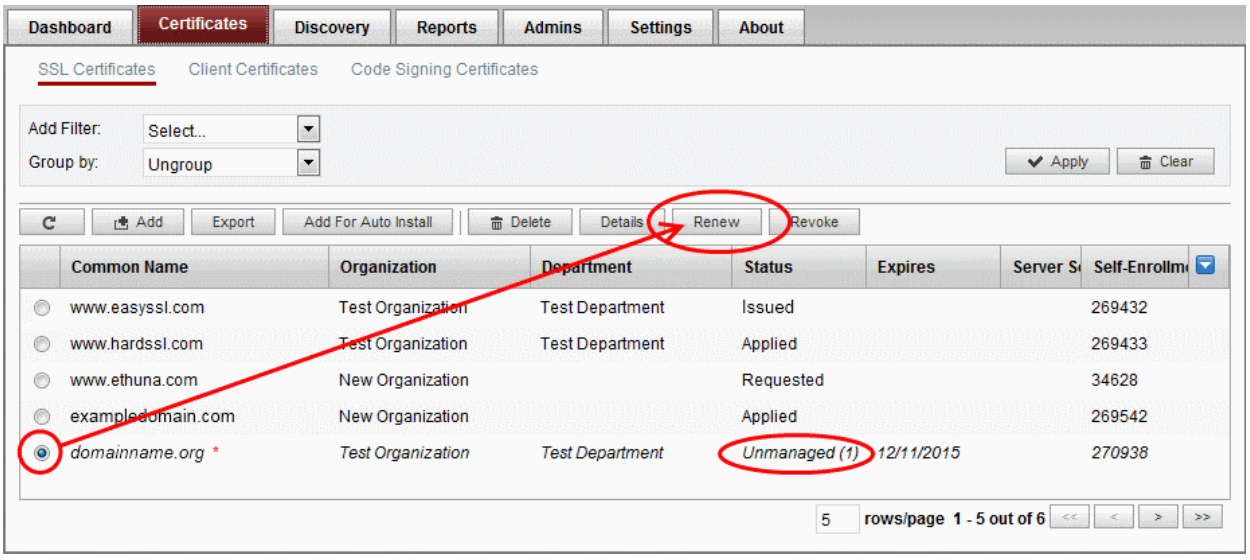
If the administrator wishes to renew a managed certificate, they should select the radio button beside it and click the 'Renew' button at the top.



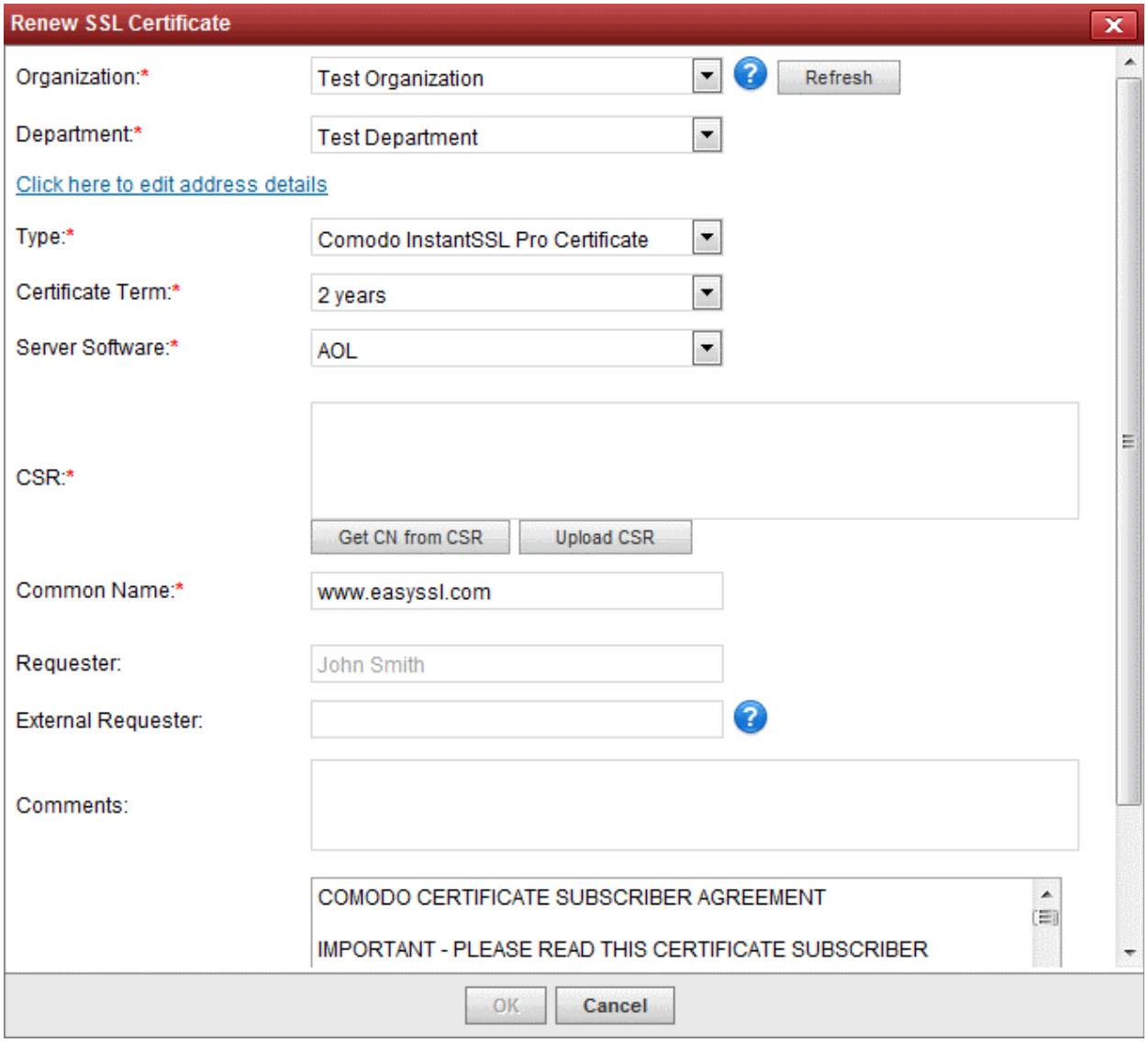
- On clicking 'Renew', CCM will automatically request a renewal with the same details as the existing certificate.
- Once issued, the renewed certificate will become available for collection and installation. Refer to the section **Certificate Collection** for more details.

Renewing an 'Unmanaged' Certificate

If the administrator wishes to renew an unmanaged certificate, they should select the radio button beside it and click the 'Renew' button at the top.



- Clicking the 'Renew' button will open the 'Renew SSL Certificate' form. This form is similar to the **Built-in Enrollment form** with the company and domain details pre-populated from the existing certificate. If needed, the administrator can select the new certificate type and edit the details.



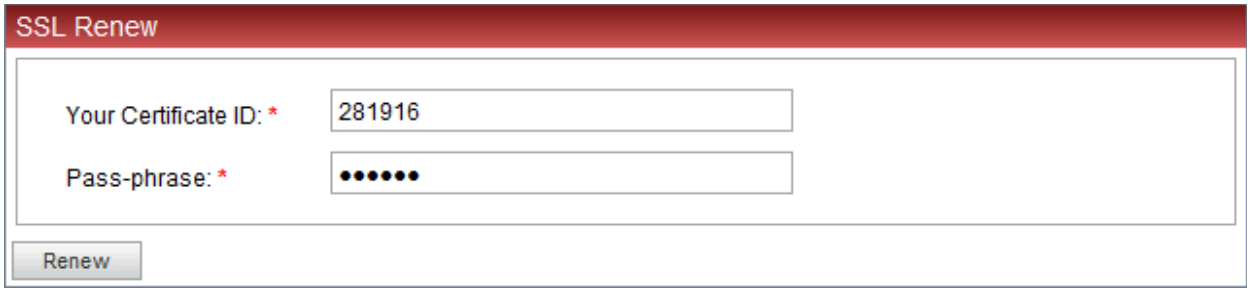
- The administrator should paste or upload a new CSR, accept to the Certificate Subscriber Agreement and click the OK button.
- CCM will place a request for the renewal certificate with the new CSR
- Once issued, the renewal certificate can be collected and installed. Refer to the section **Certificate Collection** for more details. After installation, the status of the certificate changes to 'Managed'.

3.1.2.5.2 Certificate Renewal by the End-User

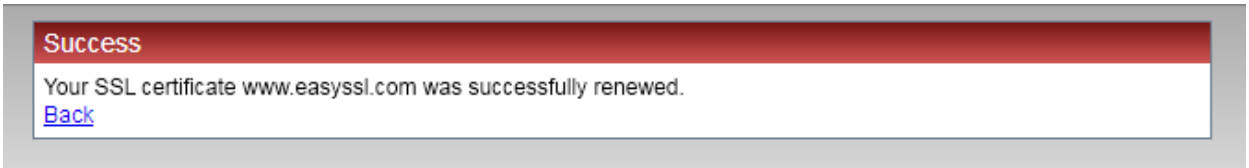
End-users can renew their certificates through the self renewal application form.

- The self renewal form is hosted by default at https://cert-manager.com/customer/[REAL CUSTOMER URI]/ssl.

- Clicking the Certificate renewal link will open the self renewal form



- Before proceeding to the full renewal application form, the user has to authenticate the request by:
  - Entering the correct self enrollment certificate ID. The certificate ID is available from certificate collection email received during enrollment. The Certificate ID is also available from the Certificates > SSL interface. If needed, the administrator can communicate the Self enrollment certificate ID to the user through any out of band communication method like email.
  - The renewal/revocation passphrase entered in the self-enrollment form, while enrolling for the certificate.
- Clicking 'Renew' will automatically renew the certificate with the same details as in the existing certificate.

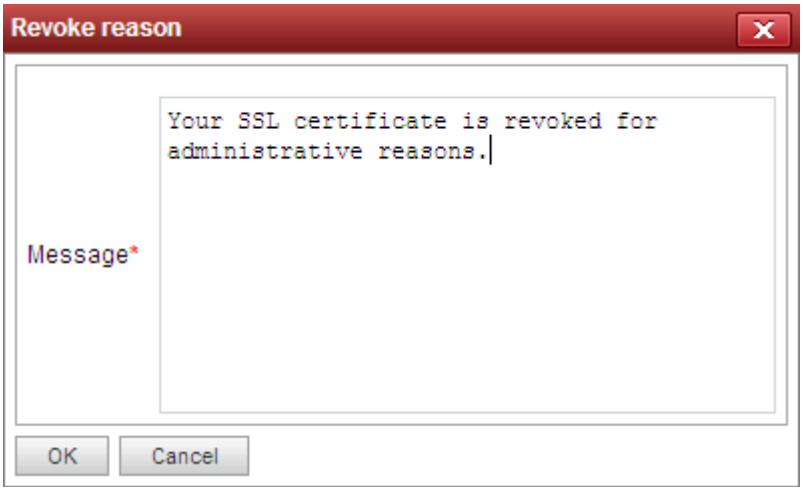


- Once issued, the renewal certificate can be collected and installed. Refer to the section **Certificate Collection** for more details.

3.1.2.6 Certificate Revocation, Replacement and Deletion

In the 'SSL Certificates' sub-tab of 'Certificates Management' section explained **above**, the administrator has also the option to revoke, renew, replace or delete a certificate.

- If the Administrator wishes to revoke a certificate, they should first select the certificate and click the 'Revoke' button at the top.
  - After clicking the 'Revoke' button, a 'Revoke reason' message box will be displayed. This allows the administrator to type a message that will be sent along with the revoke notification email.



- Click 'OK' to add the message and send the revoke email.

Note: The **SSL Revoked Notification** should have been set up for the requester to receive the email notification.

- If the administrator wishes to replace an existing certificate, they should select the checkbox beside it and click the 'Replace' button at the top. Clicking the 'Replace' button will open the 'Replace existing SSL' dialog which requires a new CSR and reason for replacing the certificate.
- If the administrator wishes to delete a certificate, they should should select the checkbox beside it and click the 'Delete' button at the top.

Please see the '**SSL Certificates**' chapter for full details of the options available in this area.

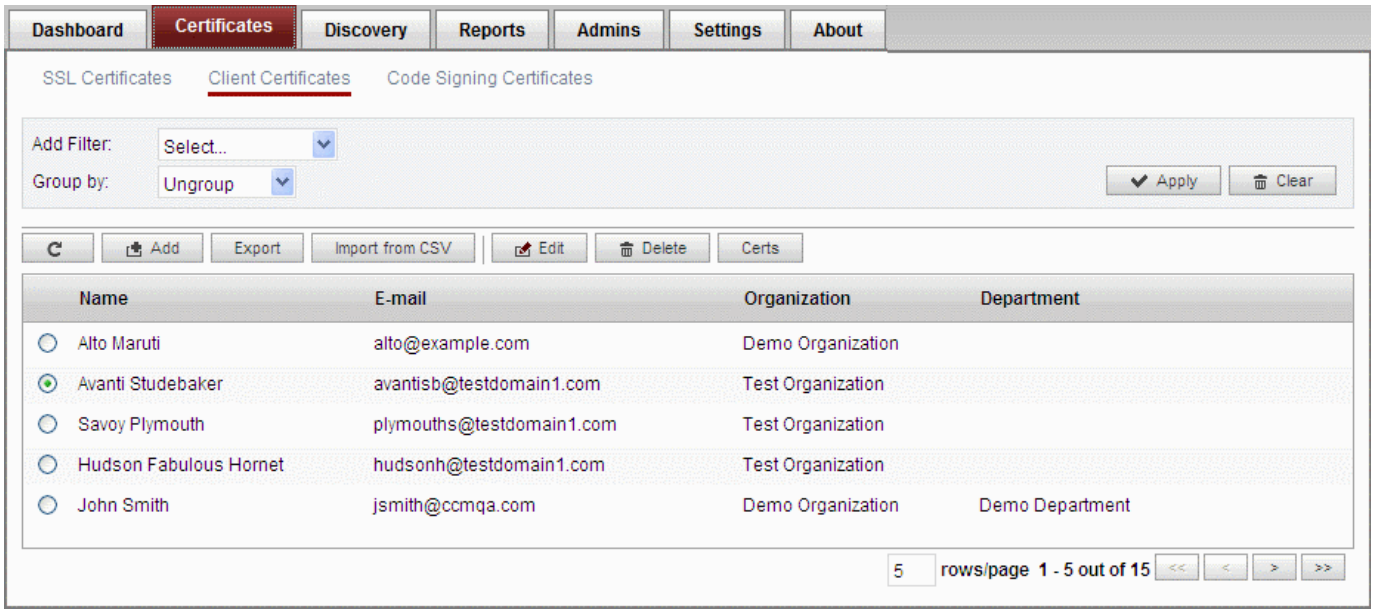
3.2 The Client Certificates Area

3.2.1 Overview

The Client Certificates area provides administrators with the ability to manage all end-users' certificates and their owners' details.

Visibility of the 'Client Certificates' area is restricted to:

- MRAO administrators - can view the client certificates and end-users of any Organization or Department.
- RAO SMIME administrators - can view the client certificates and end-users of Organizations (and any subordinate Departments) that have been delegated to them.
- DRAO SMIME administrators- can view the client certificates and end-users of Departments that have delegated to them.



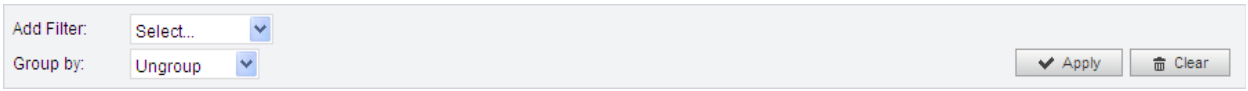
'Client Certificates' table		
Column Name		**Description**
Name		End-user's name.
Email		End-user's email address.
Organization		Name of the Organization that the end -user belongs to.
Department		Name of the Department that the end-user belongs to (if applicable)
Control Buttons	Add	Allows the administrator to add a new end-user and configure a client certificate for that user

'Client Certificates' table		
Column Name		**Description**
	Export	Export the currently displayed list to a spreadsheet in .csv format
	Import from CSV	Enables the administrator to import list of new end-users in .csv format into the Certificate Manager database.
	Refresh	Updates the currently displayed list of users. Will remove any users that have been recently deleted and add any that have been recently created. Will update details such as Organization, email etc if those details have recently changed.
Certificate Control Buttons **Note**: The types of certificate control buttons that are displayed in the table header depends on the state of the selected certificate	Edit	Enables the administrator to edit the end-user's details.
	Delete	Enables the administrator to delete the end-user.
	Certs	Enables the administrator to view/manage the end-user's Client certificates.

3.2.1.1 Sorting and Filtering Options

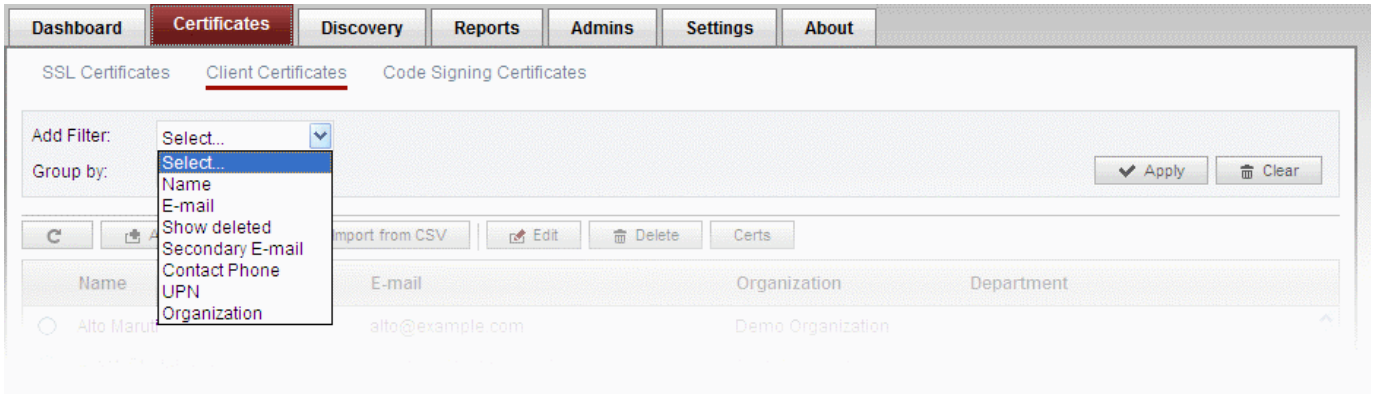
- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for particular client certificates by using filters under the sub-tab:



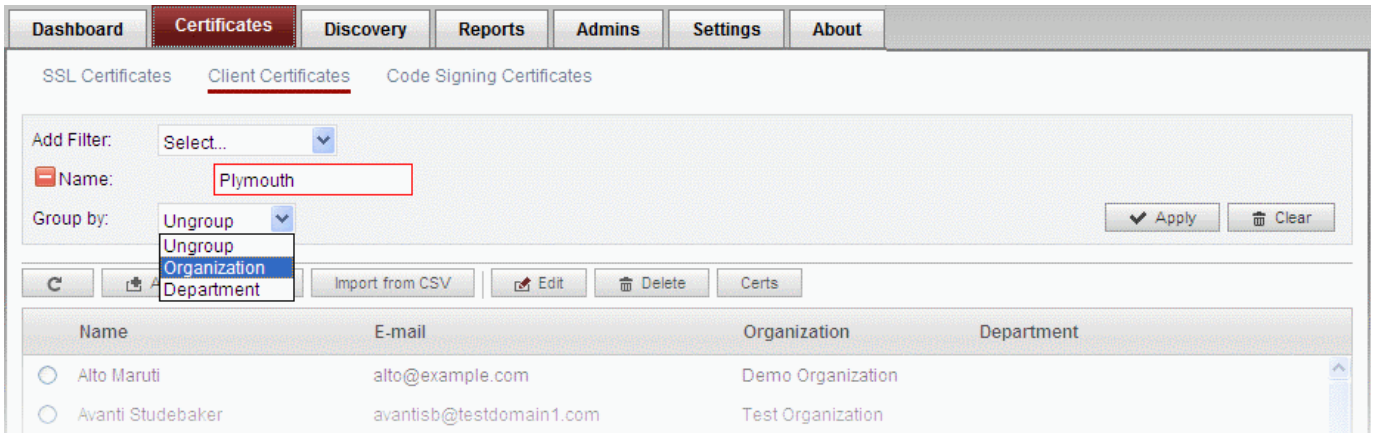
You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with another set of options available from the 'Group by' drop-down.

For example, if you want to filter the certificates with 'Name' and group with 'Organization', select 'Name' from the 'Add Filter' drop-down:



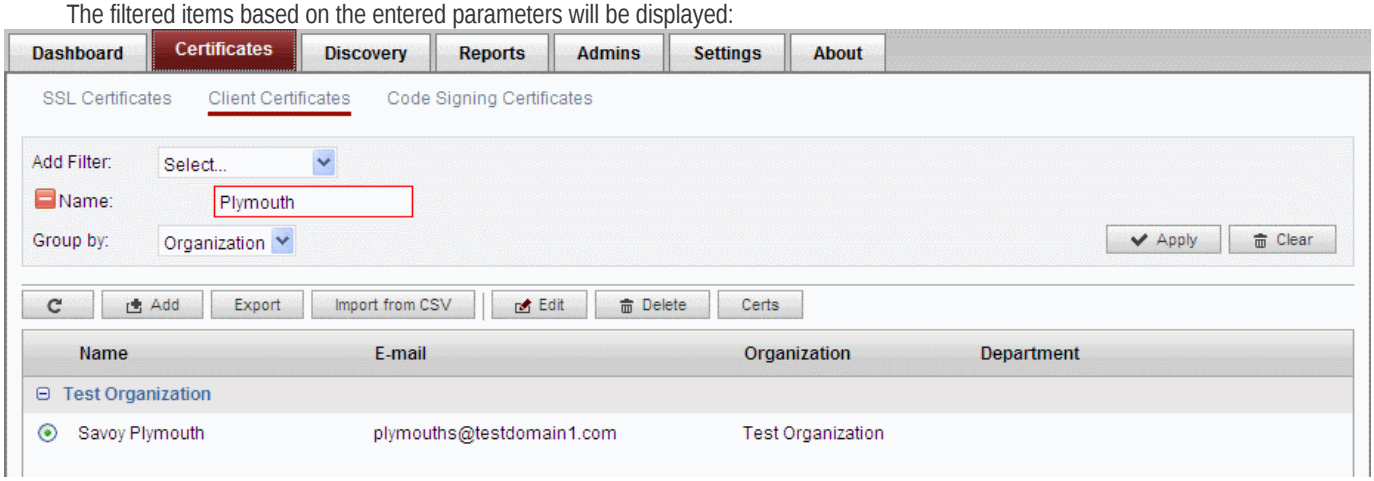
Tip: You can add more than one filter at a time to narrow down the filtering. To remove a filter criteria, click the '-' button to the left if it.

- Enter part or full name in the Name field.
- Select 'Organization' from the 'Group by' drop-down.



- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed:



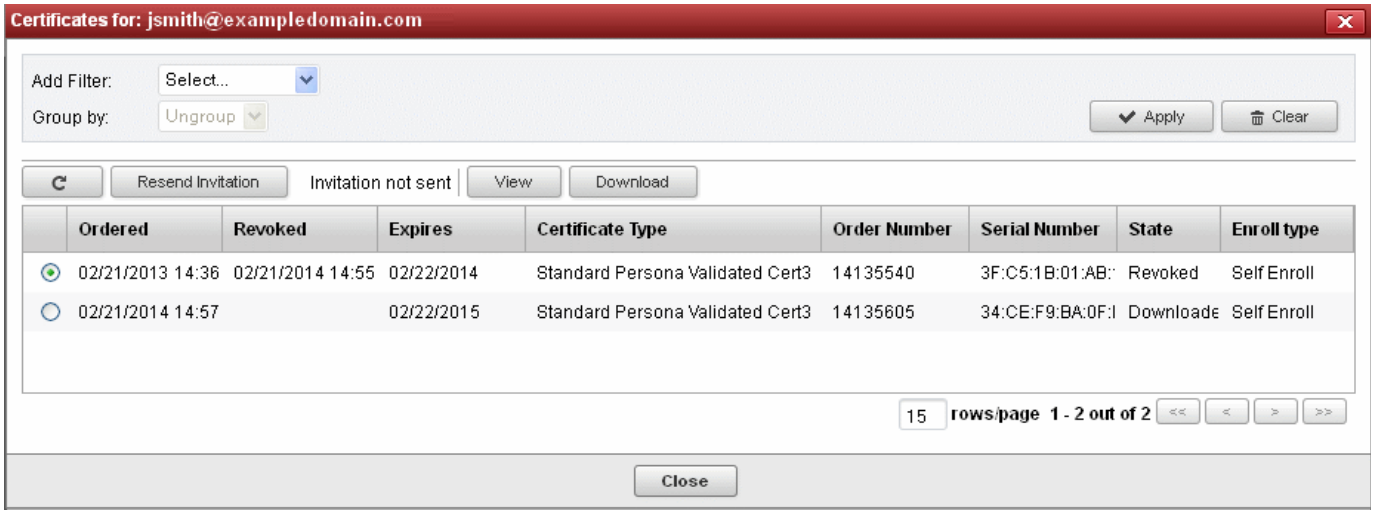
- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Client Certificates' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

3.2.1.2 'Certs' Dialog

Clicking the 'Certs' button at the top after selecting the check box next to a end-user's name will list all the client certificates belonging to that end-user. Certificates are listed in chronological order (newest first). If a certificate has been revoked, then the date of revocation is displayed in the 'Revoked' column.

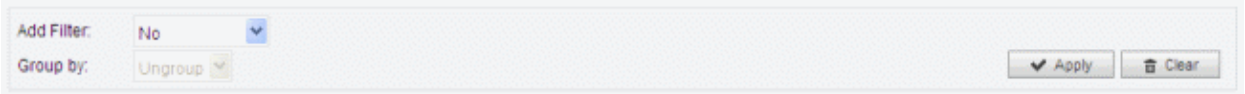
This interface allows the administrator to revoke, download, view and send invitation for that certificate. (See below).



Sorting and Filtering Options

- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for a particular certificate by using filters under the sub-tab:



You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down. The options available are:

- Type - Standard and High - Sorts the results based on the selected parameter.
- Serial Number - Sorts the results based on the serial number of the certificate entered
- Click the 'Apply' button. The results will displayed based on the filters selected / entered.
- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Certificates' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

Client Certificate 'Cert' Dialog - Table of Parameters		
Controls	**Type**	**Description**
View	Button	Allows administrators to view an end-user's certificate. See **Viewing End-User's certificate** for more details.
Revoke	Button	Allows administrators to revoke an end-user's certificate. Once revoked, the date and time of revocation is displayed in this column.
Download	Button	Allows administrators to download a copy of the end-user's certificate. *
Send Invitation	Button	Enables the administrator to send an email to the end-user with instructions on how to apply for/collect their client certificate. See '**Request and issuance of 'Client Certificates to Employees and End-Users**' for an explanation of the process from this point.
Refresh	Button	Reloads the list.

*Comodo Certificate Manager creates a copy of each end-user's certificate which it saves on the server. This duplicate certificate

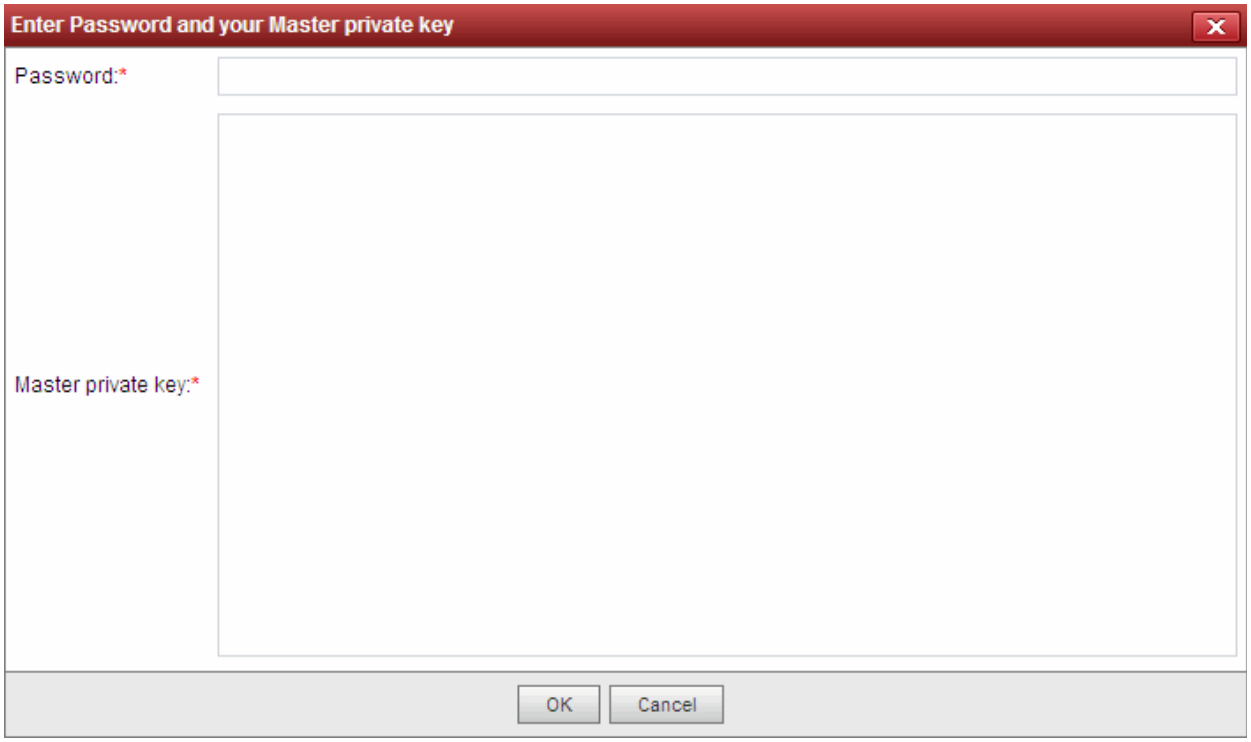
is protected in two ways:

The key pair of each end-user's certificate is encrypted by a master public key. See the '**Encryption and Key Escrow**' section for more details;

- Password protected with an administrator set password. The end-user will be asked for this password every time he wish to download a certificate.

Comodo Certificate Manager stores the individual private keys of end-user's client certificates so that they can be retrieved at a later date by the administrator or end-user. Due to the highly sensitive and confidential nature of this feature, all end-users' key pairs are stored in encrypted form so that they cannot be easily stolen or compromised. Each end-user's key pair is encrypted using a 'master' public key that is stored by CCM. In order to decrypt this end-user's key pair the administrator must paste the corresponding 'master' private key into the space provided. Admin can set a password to protect access to private key in .p12 file as well. The Administrator is able to bypass the password but should be aware that not but not all programs will subsequently allow the certificate to be imported if they do so. (PIN may be 7 characters maximum.) The following is a summary of browsers in which it is possible to import .p12 with empty password field.

Browser	Windows 7	Vista	XP	Mac
IE 6	-	-	✓	-
IE 7	-	✓	✓	-
IE 8	✓	✓	✓	-
FF 2	✓	✓	✓	✓
FF 3	✗	✗	✗	✗
Opera 9	✓	✓	✓	✓
Opera 10	✓	✓	✓	✓
Netscape9	✓	✓	✓	✓
Safari	✓	✓	✓	✓



WARNING! If an administrator downloads an end-user's certificate, this certificate will be revoked.

3.2.2 Adding Cert End-Users

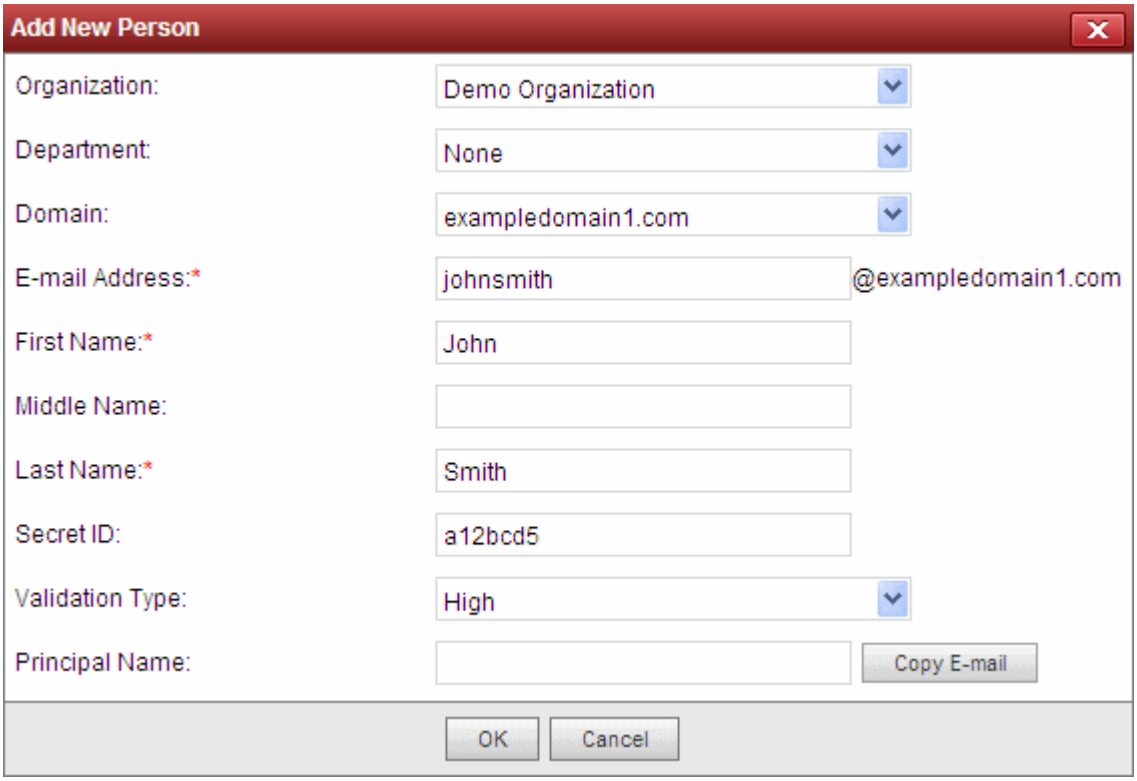
There are several methods of adding end-users to Organizations in Certificate Manager.

- **Manually adding end-users**
- **Loading multiple end-users from a comma separated values (.csv) file**
- **Auto Creation of end-users via certificate Self Enrollment Forms**

Note: A new end-user will also be created and added to this interface via SSL certificate applications 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 will be created with the name 'requesterSSL <DOMAIN.com>' (where DOMAIN.com = the domain name for which the application is being made) This End-User will automatically be assigned membership of the Organization that the SSL Certificate was ordered for but will not own a Client Certificate.

3.2.2.1 Manually Adding End-Users

- Click 'Certificates Management' - > 'Clients Cert' at the top left of the CCM interface;
- Click the 'Add' button to open the 'Add New Person' form:



- Click 'OK' to add the end-user to Comodo Certificate Manager.
- An end-user's details can be modified at any time by clicking the 'Edit' button at the top after selecting the checkbox next to their name in the main list of end-users. If any information in this dialog is changed, with the exception of Secret ID, any previously issued client certificates for this email address shall be automatically revoked. CCM maintains a username history. If the username is changed, the Administrator will still be able to search for the client certificates using both the old name and the new name.
- 'Validation Type' drop down will only be visible if enabled by your Comodo account manager.

3.2.2.1.1 'Add New Person' form - Table of Parameters

Form Element	Type	Description
Organization	Drop down menu	Administrator should select the Organization that they wish the new end-user to belong to.
Department	Drop down menu	If required, the administrator should specify the Department that the end-user is to belong to.
Domain	Drop down menu	Administrator should select the domain from which to issue from the drop down menu. This drop-down will only display domains that have been correctly delegated to the Organization/Department selected earlier.
Email Address	Text Field	Administrator should enter the email address of the end-user. The email address must be for the domain belonging to the Organization.
First Name	Text Field	Administrator should enter the first name of the end-user.
Middle Name	Text Field	If required, the administrator should enter the middle name of the end-user.
Last Name	Text Field	Administrator should enter the last name of the end-user. **Note**: The combined length of First Name and the Last name should not exceed 64 characters.
Secret ID	Text Field	A 'Secret ID' (or 'Secret Identifier'/SID) is used to identify the details of an existing end-user in CCM. Assigning SIDs to users will simplify the client certificate enrollment process for those users and therefore help eliminate errors. This is because, as the details of the user are already stored, the end-user need only specify the email address If the administrator wishes to allow enrollment by Secret ID then they must fill out this field.
Validation Type	Drop Down Menu	**Note**: The 'Validation Type' drop down will only be visible if enabled by your Comodo account manager. Allows the administrator to specify the type of client certificate that is issued to an applicant. The difference between the two lies in the degree of user authentication is carried out prior to issuance. The two options are 'Standard' and 'High'. 'Standard' certificates can be issued quickly and take advantage of the user authentication mechanisms that are built into CCM. A user applying for a 'Standard Personal Validation' certificate is authenticated using the following criteria: • User must apply for a certificate from an email address @ a domain that has been delegated to the issuing Organization • The Organization has been independently validated by an web-trust accredited Certificate Authority as the owner of that domain • 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 the administrator to the user via out-of-band communication. • 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 will contain a validation code that the user will need to enter at the certificate collection web page. 'High Personal Validation' certificates require that the user undergo the validation steps listed above AND • Face-to-Face meeting with the issuing Organization **Note**: The additional validation steps must be completed PRIOR to the

Form Element	Type	Description
		administrator selecting 'High Personal Validation' type.
Principal Name	Text Field	The Administrator can enter the email address that should appear as principal name in the certificate to be issued. **Note**: For the Organizations/departments enabled for Principal Name support, the client certificates issued to the end-users of the Organization/Department will include an additional name - Principal Name, in addition to the RFC822 name in the Subject Alternative Name(SAN) field. If included, the Principal Name will be 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/Department. The Administrator can check whether an Organization or department is enabled for Principal Name support from the Settings interface by clicking **Settings > Organizations > Edit button in the row of the respective Organization name > Client Cert tab** or **Settings > Organizations > Department button in the row of the respective Organization name > Edit button in the row of the respective Department > Client Cert tab**. This field will be 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 the Department belonging to the Organization, this field will be auto populated with the email address entered in the Email Address field.
Copy E-Mail	Button	Auto-fills the Principal Name field with the email address entered in the E-mail Address field.

3.2.2.2 Loading Multiple End-Users from a Comma Separated Values (.csv) File

Administrators can import list of end-users into CCM in comma separated values (.csv) format. After importing the list, your employees then only need to complete the self enrollment with their secret code.

Note: The ability to loading multiple end-users from a .csv file functionality is only available to MRAO, RAO SMIME and DRAO SMIME administrators.

3.2.2.2.1 Procedure Overview

Summary of required steps for adding end-users by loading a .csv file:

1. Administrator generates a .csv file using containing a list of end-users. .csv files can be exported directly from spreadsheet programs such as Excel or Open Office Calc.
2. Administrator loads the .csv file by clicking the 'Load from CSV' button in the 'Certificates Management' > 'Client Certificates' interface
3. CCM sends an email notification containing a link to the self-enrollment form and the secret identifier to each end-user included in the .csv file.

Note: For the CM to automatically send the notification emails to the end-users, the administrator should have configured for this by selecting the checkbox 'Send invitations on successful upload' in the Import persons from CSV dialog while loading the .csv file. If not configured, the administrator should manually send an email containing a link to the self-enrollment form and the secret identifier to each end-user. For more details refer to section **The Import Process**.

4. End-users collect and install their certificates.

3.2.2.2.2 Requirements for .csv file

The fields per user in the .csv differs for Organizations depending on whether or not the Principal Name Support is enabled for the Organization. For more details on the principal Name Support, refer to **Settings > Organisations > Creating a New Organisation > Client Cert Settings tab**.

3.2.2.2.2.1 For Organizations with Principal Name Support Enabled

There are 12 potential fields per user that can be imported via .csv. 6 are mandatory and there is one conditionally mandatory value. The 12 potential fields are as follows:

First Name
Middle Name
Last Name
Email Address (Primary)
Alternative Email Address(es)
Validation Type
Organization
Department
Secret Identifier
Phone
Country
Principal Name

- Each entry should have 12 fields. Even the optional fields without values must be included but should be left blank ("").
- 'Department' will be mandatory if the administrator that is importing is a DRAO SMIME.
  MRAO, RAO SMIME (and DRAO SMIME administrators that are also MRAO or RAO SMIME administrators) have the option to leave this field blank. See **3.2.2.2.3.General Rules** for more details.
- The 'Secret ID' value can be used to add a layer of authentication to the process. If specified, the user will need to type the identifier at the certificate enrollment form to complete the process.
- With the exception of the 'Secret ID' and 'Phone', make sure the fields are imported using characters as specified below. (including commas (,) and quotation marks (" ")).

The following table explains the requirements and formats of the values.

Values	First Name	Middle Name	Last Name	Email Address (primary)	Email Addresses (Alternative)	Validation Type	Organization	Department	Secret ID	Phone	Country	Principal Name
Required	Yes		Yes	Yes	Yes		Yes				Yes	
Min Length (characters)	1	0	1	3	3		1	0	0	0	2	1
Max Length (characters)	128	128	128	128	128		128	128	128	128	2	128
Format				Valid email address	Valid email address, separated by space						Valid two letter country code	
Characters allowed	A-Z, a-z, 0-9, '.', '-', ' '	A-Z, a-z, 0-9, '.', '-', ' '	A-Z, a-z, 0-9, '.', '-', ' '	A-Z, a-z, 0-9, '.', '-', '_'	A-Z, a-z, 0-9, '.', '-', '_'	'high', empty or 'standard'	ANY	ANY	ANY	ANY	A-Z, a-z	ANY

Example:

"First1","Middle1","Last1","User----1-al@abc.com","User----1-sec-al@abc.com","standard","System","sysdep,"Secret1",380487000001,"UA","User----1-al@abc.com"

Note: If an Organization is enabled for Principal Name support and a Department belonging to the Organization is not enabled for Principal Name support, when loading end-users of the Department, the Principal Name field must be included but should be left blank.

The Administrator can check whether an Organization or department is enabled for Principal Name support from the Settings interface by clicking **Settings > Organizations > Edit button in the row of the respective Organization name > Client Cert tab** or **Settings > Organizations > Department button in the row of the respective Organization name > Edit button in the row of the respective Department > Client Cert tab**..

3.2.2.2.2.2 For Organizations without Principal Name Support

There are 11 potential fields per user that can be imported via .csv. 6 are mandatory and there is one conditionally mandatory value. The 11 potential fields are as follows:

First Name

Middle Name

Last Name

Email Address (Primary)

Alternative Email Address(es)

Validation Type

Organization

Department

Secret Identifier

Phone

Country

- Each entry should have 11 fields. Even the optional fields without values must be included but should be left blank ("").
- 'Department' will be mandatory if the administrator that is importing is a DRAO SMIME.
  MRAO, RAO SMIME (and DRAO SMIME administrators that are also MRAO or RAO SMIME administrators) have the option to leave this field blank. See **3.2.2.2.3.General Rules** for more details.
- The 'Secret ID' value can be used to add a layer of authentication to the process. If specified, the user will need to type the identifier at the certificate enrollment form to complete the process.
- With the exception of the 'Secret ID' and 'Phone', make sure the fields are imported using characters as specified below. (including commas (,) and quotation marks (" ")).

The following table explains the requirements and formats of the values.

Values	First Name	Middle Name	Last Name	Email Address (primary)	Email Addresses (Alternative)	Validation Type	Organization	Department	Secret ID	Phone	Country
Required	Yes		Yes	Yes	Yes		Yes				Yes
Min Length (characters)	1	0	1	3	3		1	0	0	0	2
Max Length (characters	128	128	128	128	128		128	128	128	128	2

)											
Format				Valid email address	Valid email address, separated by space						Valid two letter country code
Characters allowed	A-Z, a-z, 0-9, '.', '-', ' '	A-Z, a-z, 0-9, '.', '-', ' '	A-Z, a-z, 0-9, '.', '-', ' '	A-Z, a-z, 0-9, '.', '-', '_'	A-Z, a-z, 0-9, '.', '-', '_'	'high', empty or 'standard'	ANY	ANY	ANY	ANY	A-Z, a-z

Example:

"First1","Middle1","Last1","User----1-al@abc.com","User----1-sec-al@abc.com","standard","System","sysdep,"Secret1",380487000001,"UA",

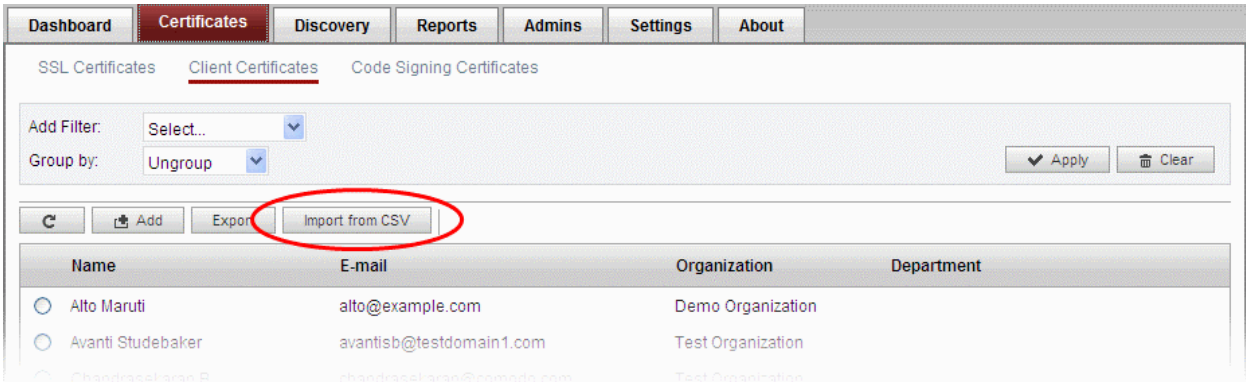
3.2.2.2.3 General Rules

The import will fail if:

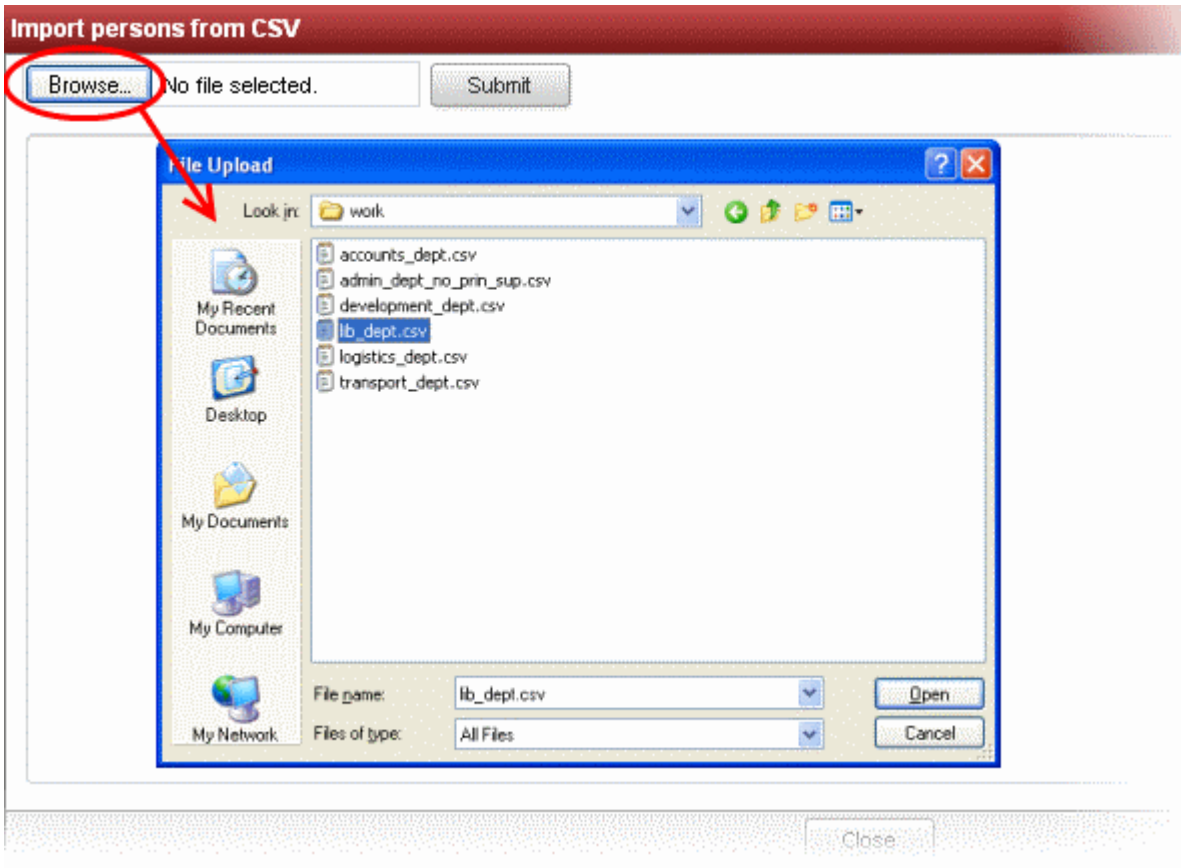
- All the lines are not having the 12/11 fields as required.
- Any mandatory field as explained in **2.2.2.2.2.Requirements for .csv file** is missing
- The Organization does not exist
- The Department, if present, does not exist
- The Department, if present, does not exist for the specified Organization
- The Primary Email Address 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 Secondary Email Address (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 and/or Department:
    - MRAO administrators have permission to import for any valid Organization or Department. MRAOs may leave the 'Department' field blank.
    - RAO SMIME administrators have permission to import for Organizations (and any subordinate Departments) that have been delegated to them. RAO SMIME may leave the 'Department' field blank.
    - DRAO SMIME administrators have permission to import for Departments that have delegated to them. DRAO SMIME administrators ***cannot*** leave the 'Department' field blank unless they are also an RAO SMIME for the same Organization.

3.2.2.2.4 The Import Process

To load the .csv file, click 'Import from CSV' in 'Certificates Management' > 'Client Certificates' interface:

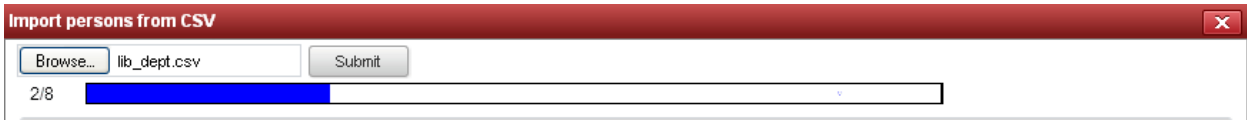


The 'Import from CSV' dialog appears.

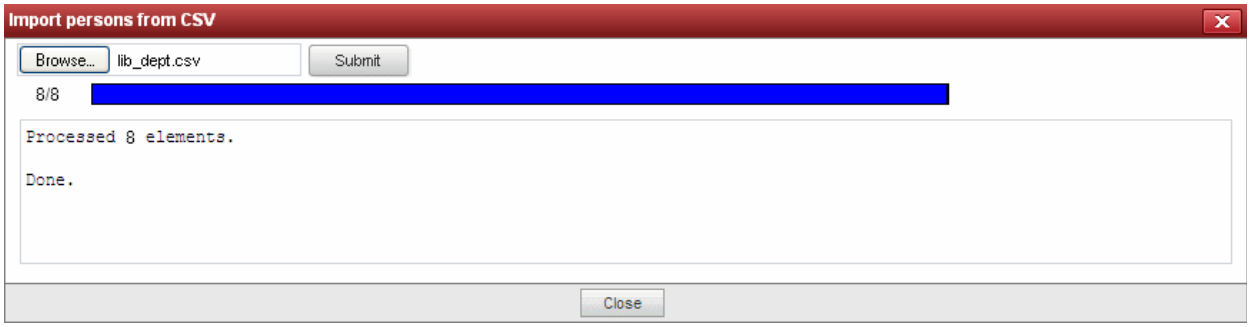


- Click the 'Browse' button, navigate to the .csv file
- Click 'Submit'.

The import status will be indicated. You will see a progress bar indicating that information is being uploaded:



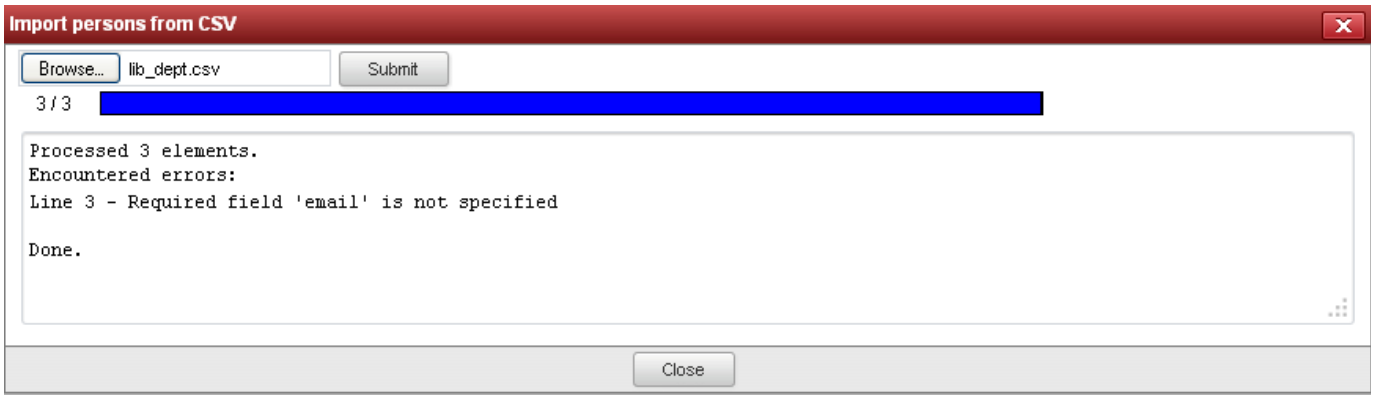
CCM will inform you when the process is finished:



All imported users appear in the list of end-users in the 'Client Certificates' section and notification emails containing a link to the **self-enrollment form** and the secret ID will be automatically sent to the imported end-users, if the checkbox 'Send invitations on successful upload' is selected.

3.2.2.2.5 Errors in .csv file

CCM will inform you if there is an error in the .csv file (mandatory fields are missing, for example).



Only the end-users included in the lines without errors will be loaded to CCM and the end-users included in the lines with errors will not be loaded.

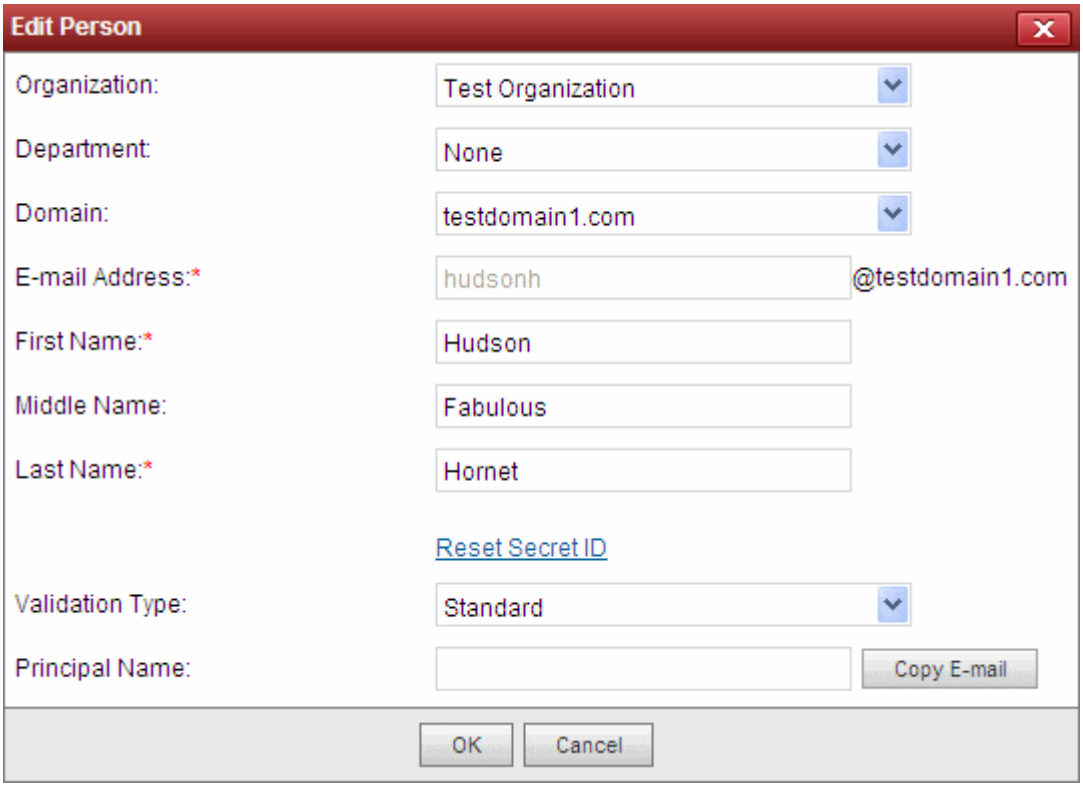
3.2.2.3 Auto Creation of End-Users via Certificate Self Enrollment Form

End-users applying via the SSL or Client Certificate enrollment form are automatically added to the 'Certificate Management - Client Certificates' area.

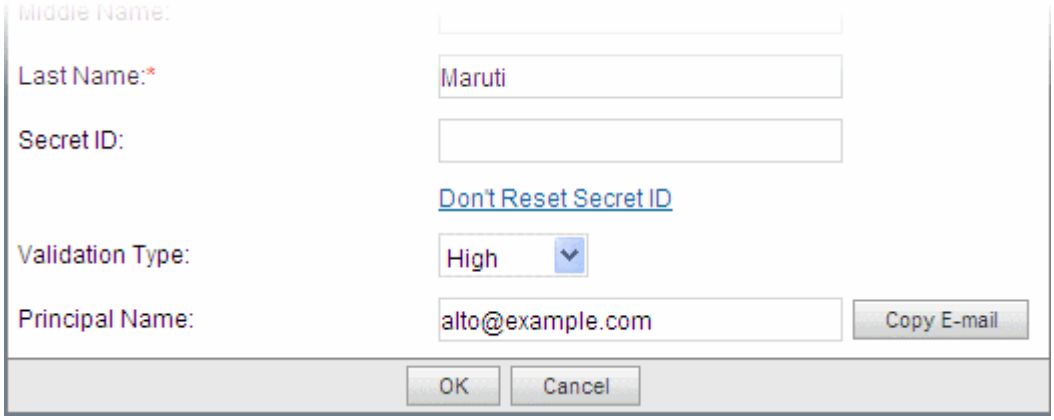
For more details see: **Request and issuance of client certificates to employees and end-users**

3.2.3 Editing End-Users

All end-user details can be modified at any time by clicking the 'Edit' button after selecting the end-user's name.



- If any information in this dialog is changed, with the exception of 'Secret ID', any previously issued client certificates for this email address shall be automatically revoked.
- For security reasons, the 'Secret ID' field is not displayed. If the SID needs to be changed, administrator can click the Reset Secret ID link.
    - On clicking the link, the Secret ID text box will be displayed, enabling the administrator to specify a new SID.



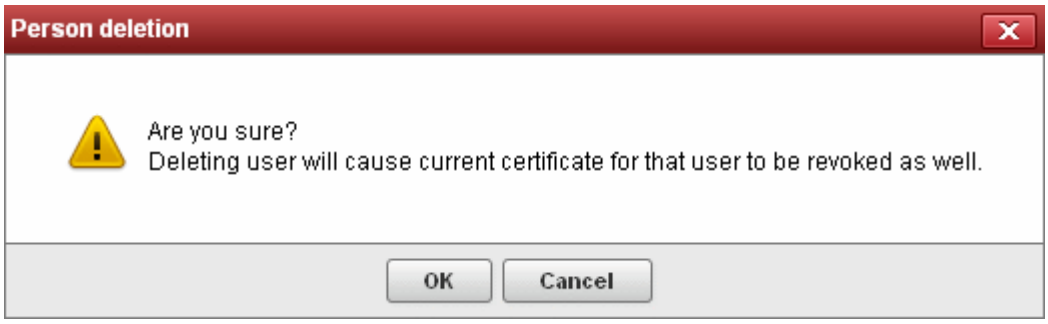
    - To change the SID, the administrator can type a new SID in this field.
    - To retain the existing SID, the administrator can click the Don't Reset Secret ID link.
- 'Validation Type' drop down will only be visible if enabled by your Comodo account manager. For an explanation of validation types, see 'Validation Type' in the '**Add New Person**' table of parameters.
- Renaming an end-user does not affect the search and filtering actions in the Client Certificates Interface. CCM allows the administrators to search for particular user or client certificates using both the old name and the new name in case a username is changed.
- To customize the Principal Name for the end-user, type the new Principal Name as it should appear in the in the Subject Alternative Name (SAN) field of the certificate in the Principal Name field. To revert the Principal Name to the email address of the end-user, click the 'Copy E-Mail' button. This button will be available only if this feature is enabled

for your account.

Full details of the fields available when editing an existing end-user are available in the section **'Add New Person' form - table of parameters**.

3.2.4 Deleting an End-User

An Administrator can delete any end-user by clicking 'Delete' button after selecting the end-user's name.



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

3.2.5 Request and Issuance of Client Certificates to Employees and End-Users

End-users can be enrolled for client certificates (a term which covers email certificates, end-user authentication certificates and dual-use certificates) in three ways:

- **Self Enrollment of End-Users by Access Code** - Involves directing the end-users to apply for their own client certificate by accessing the self enrollment form. The Administrator has 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 the section **Self Enrollment by Access Code** for more details.
- **Self Enrollment of End-Users by Secret Identifier** - Involves directing the end-users to apply for their own client certificate by accessing the self enrollment form. The Administrator has to inform the end-user of the URL at which the self-enrollment form is hosted and the Secret Identifier of the Organization to which the end-user belongs. This should be done by out-of-band communication such as email. See the section **Self Enrollment by Secret Identifier** for more details.
- **Enrollment by Administrator's Invitation**- Involves sending invitation mails to end-users previously added to CCM. The Administrators can send the invitation mail from the CCM interface itself. The invitation mail will contain a validation link and instructions for the end-users to download and install their certificates. See the section **Enrollment by Invitation** for more details.

3.2.5.1 Self Enrollment by Access Code

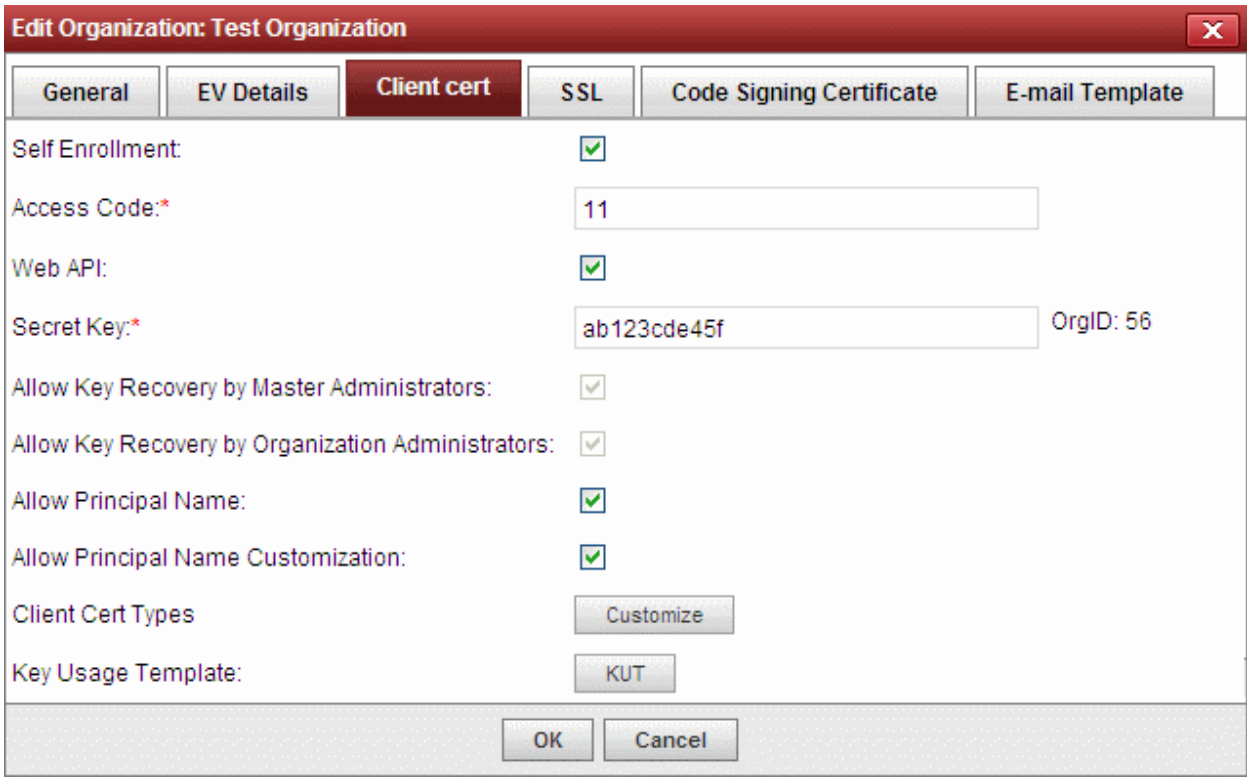
This section explains how the administrator can direct the end-user for self-enrollment using the access code specified for the Organization and how the end-user can apply for, collect, download and install their certificate.

3.2.5.1.1 Prerequisites

- The domain from which the client certificate is to be issued has been enabled for SMIME certificates, has been pre-validated by Comodo and that the domain has been activated by your Comodo account manager. (i.e. if you wish to issue client certs to end-user@mycompany.com, then mycompany.com must have been pre-validated by Comodo).

  However, if you request a certificate for a brand new domain, then this domain will first have to undergo validation by Comodo. Once validated, this new domain will be added to your list of pre-validated domains and future certificates will be issued immediately.
- The domain from which the client certificates are to be issued has been delegated to the Organization or Department. See **Creating a New Organization** and **Editing an Existing Organization** for more details on adding a domain to an Organization.

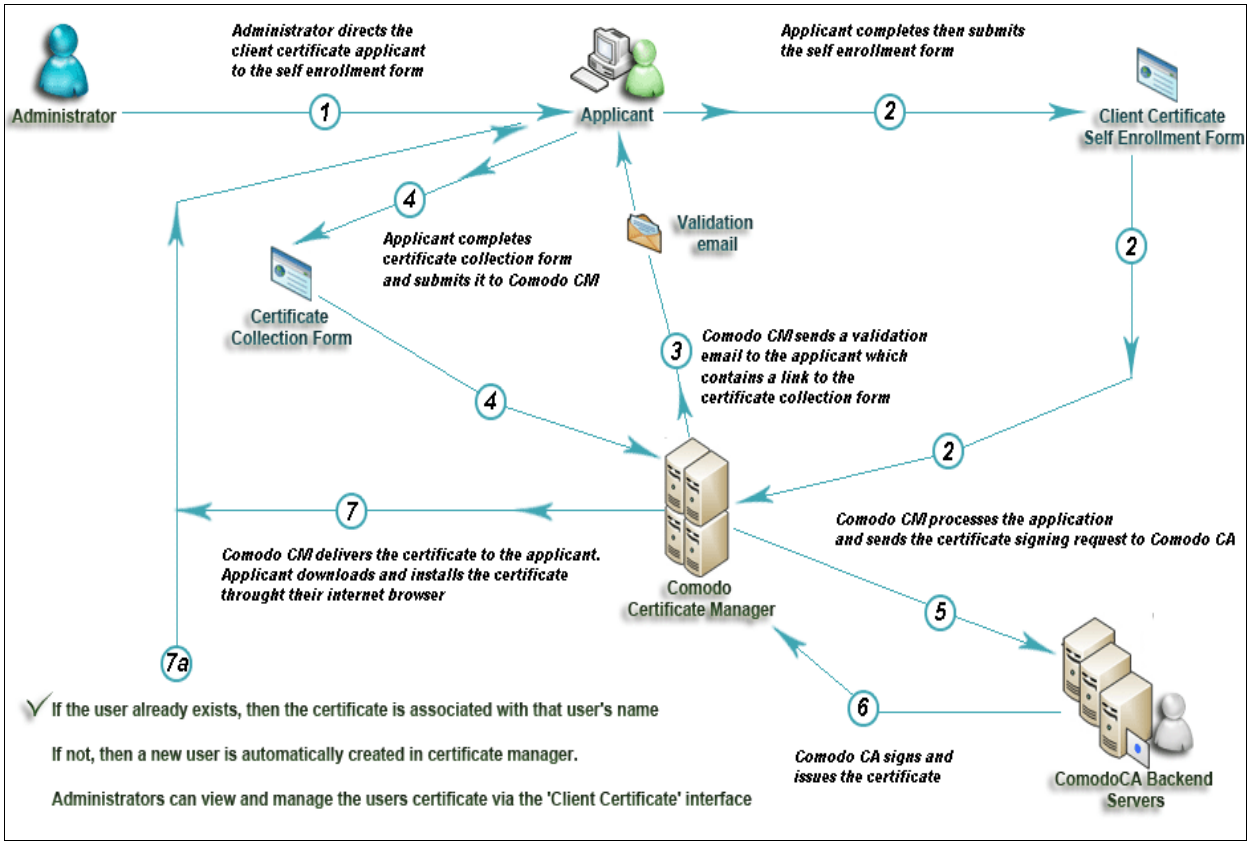
- The RAO SMIME or DRAO SMIME administrator has been delegated control of this Organization or Department
- The administrator has **checked** the 'Self Enrollment' box in the '**Client Cert' tab** of the 'Create/Edit' Organizations dialog box.



- The administrator has **specified an Access Code** in the ' **Client Cert' tab** of the 'Create/Edit' Organizations dialog box. This should be a mixture of alpha and numeric characters that cannot easily be guessed.

3.2.5.1.2 Procedure Overview

1. Administrator confirms completion of the **prerequisite steps**.
2. Administrator directs the personal certificate applicant to the 'Access Code' based Self Enrollment Form - making sure the application is done from the end-user's computer (see section **Initiating the enrollment process**).
3. Applicant completes then submits the Self Enrollment Form, specifying the correct Access Code for the Organization's domain. (See section **The Self Enrollment Form**)
4. CCM sends a validation mail to the applicant which contains a link to the Account Validation form and a request code. (See section **Validation of the Application** for more details)
5. Applicant completes the Account Validation form. The certificate request is sent to Comodo CA servers. If the application is successful, the applicant will be able to download and install their personal certificate. (See section **Certificate Collection..**)
6. If the applicant already exists as an 'End-User' (viewable in the '**Client Certificates**' area of 'Certificates Management' section) then the certificate will be added to their account. If the applicant does not exist as an 'End-User' then CCM will automatically add this applicant as a new 'End-user' at the point of certificate issuance. If the applicant already exists as an Administrator (visible in '**Admin Management**') but not as as a (client certificate) 'End-User' then CCM will automatically add this applicant as a new 'End-user' to the 'Client Certificates' area'. (**Click here** for further details)



3.2.5.1.3 Initiating the Enrollment Process

After completing the **prerequisite** steps, administrators need to communicate enrollment details to all and any end-users they wish to issue client certificates to. The communication must contain the following information:

1. A link to the Access Code based Self Enrollment Form - https://cert-manager.com/customer/[REAL CUSTOMER URI]//smime?action=enroll&swt=ac
2. The client access code specified in that Organization's **Client Cert settings tab**.

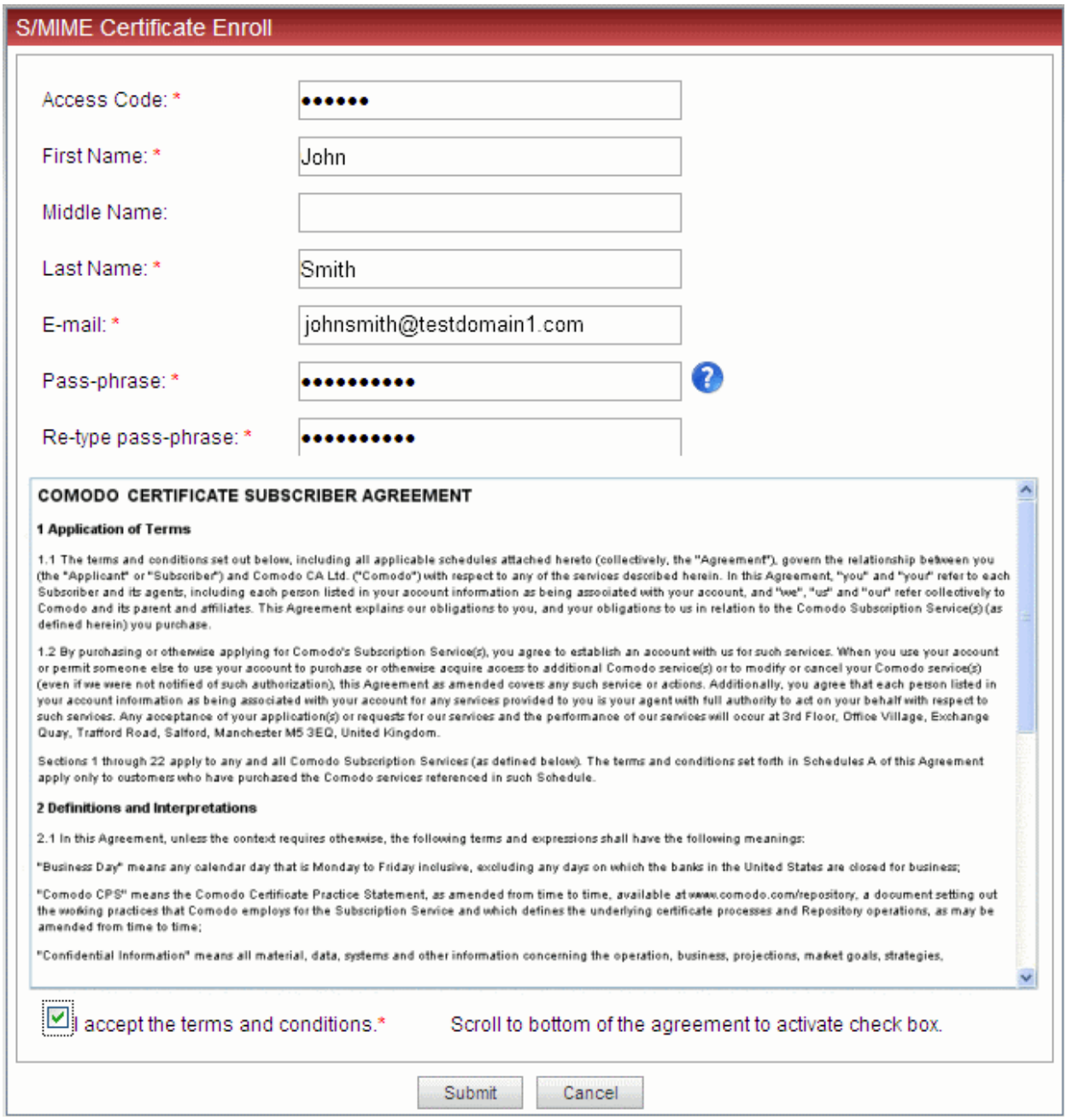
These details can be informed to the applicant by the any preferred out-of-band communication method like email. The end-user can access the form at the given url, fill-in with the necessary details and submit it.

Please Note:

The domain of the email address that the end-user specifies in the Self Enrollment Form MUST match a 'Common Name' (domain) associated with an **Organization or Department within an Organization**. 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 the administrator for that specific Organization.

3.2.5.1.3.1 The Access Code Based Self Enrollment Form



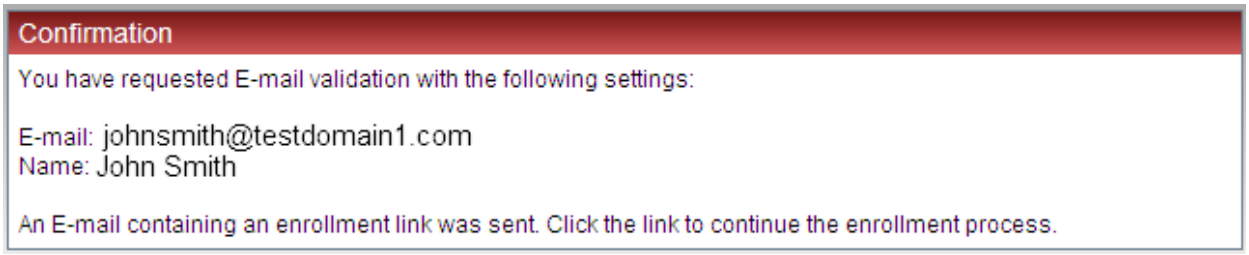
3.2.5.1.3.2 Form Parameters

Form Element	Type	Description
Access Code**(required)**	Text Field	This is the **Access Code** specified for the Organization or Department.
First Name **(required)**	Text Field	Applicant should enter their first name
Middle Name **(optional)**	Text Field	If required, the applicant should enter their middle name
Last Name **(required)**	Text Field	Applicant should enter their last name
Email **(required)**	Text Field	Applicant should enter their full email address. The Email address must be for the domain belonging to the Organization.
Pass-Phrase **(required)**	Text Field	This phrase is needed to renew or revoke the certificate should the situation arise.

Re-type Pass-Phrase **(required)**	Text Field	Confirmation of the above
Eula Acceptance **(required)**	Checkbox	Applicant must accept the terms and conditions before submitting the form.
Submit	Control	Submits the application.
Cancel	Control	Clears all data entered on the form

Note: In addition to the standard fields in the Enrollment form, custom fields such as 'Employee Code, Telephone' can be added by the MRAO Administrator. Refer to the section **Custom Fields** for more details.

After completing the form and clicking the 'Submit' button, a confirmation dialog will be displayed...

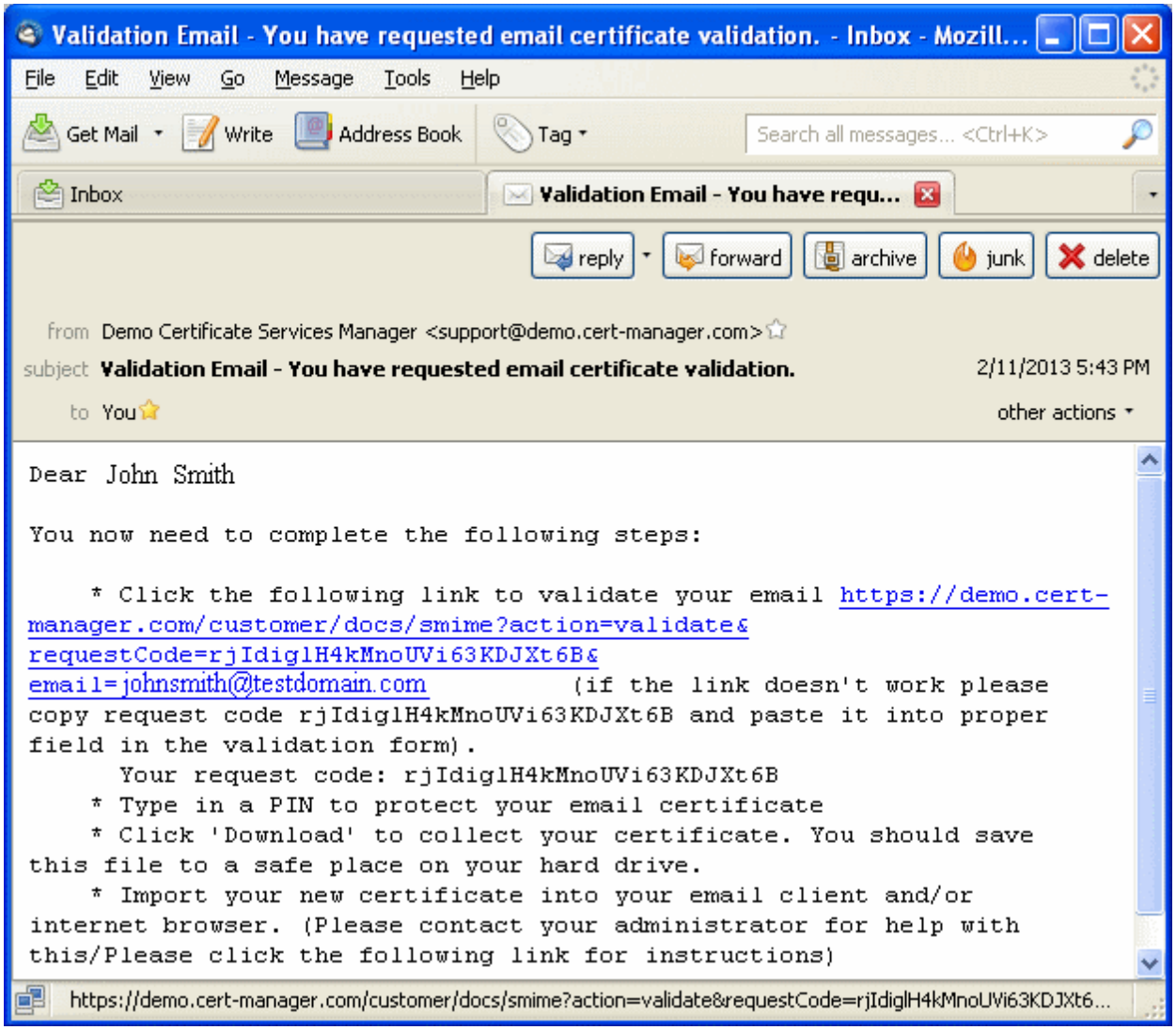


...and the applicant will receive an email containing a URL for validating the application, a request validation code and instructions for downloading the certificate. Upon clicking the link, the end-user will be taken to the Account Validation form. See the section **Validation of the Application** for more details. On completion of the validation process, a certificate collection form will appear, enabling the end-user to download and save the certificate. See the section **Certificate Collection** for more details.

3.2.5.1.4 Validation of the Application

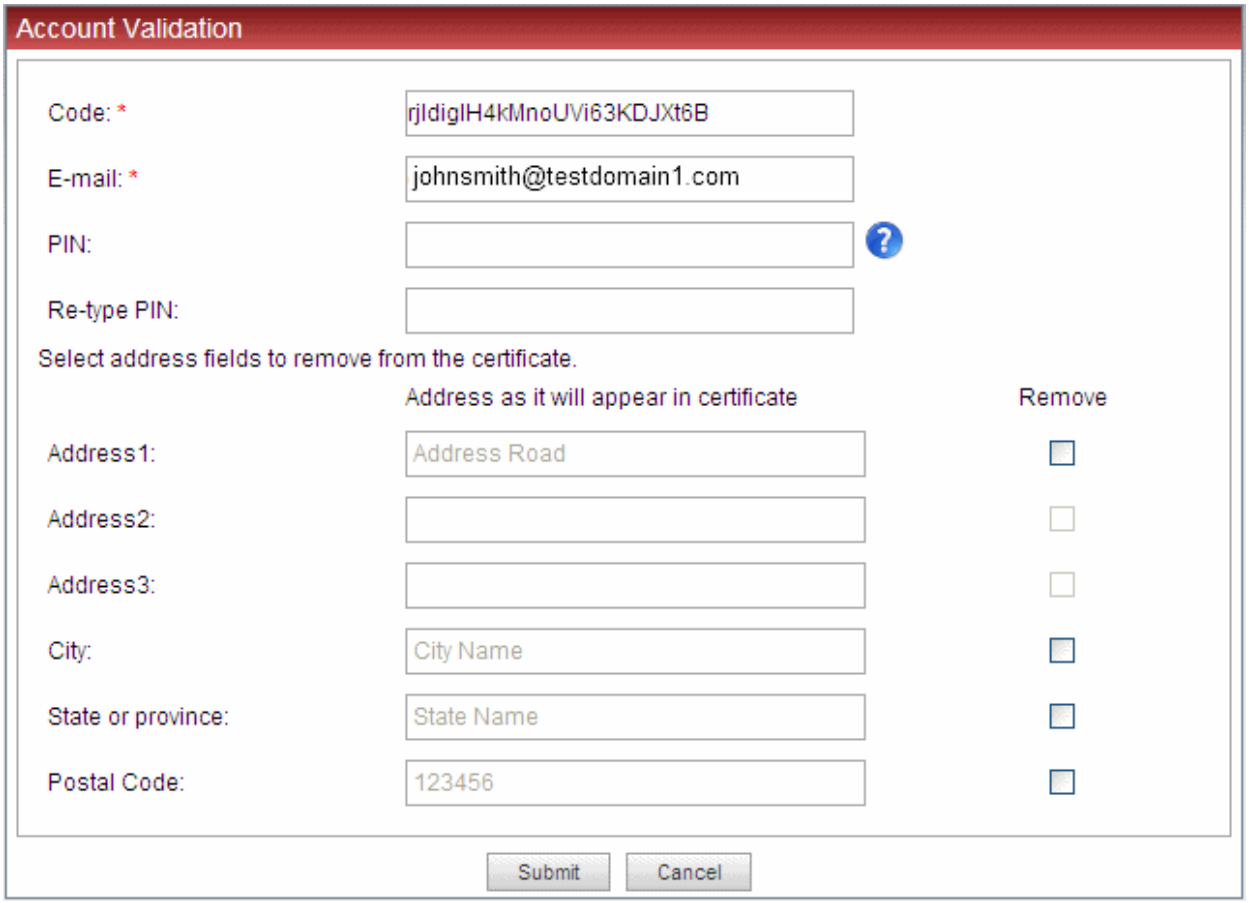
The applicant will receive a validation email on successful submission of the **Self Enrollment Form** and after being processed at Comodo.

The validation email will contain a link to the Account Validation form. The link will also contain a randomly generated 'Request Code' that the end-user will need in order to validate that they are the correct applicant. Simply clicking on the link in the email will automatically populate the request 'Code' and 'Email' fields in the Account Validation form.



Note: It is possible for administrators to modify the contents of these emails in the '**Email Templates**' area under the 'Settings' tab.

Upon clicking the link the applicant will be taken to the validation form.



Form Element	Type	Description
Code **(required)**	Text Field	The validation request code. This field is auto-populated when the applicant clicks the validation link contained in the email.
E-mail **(required)**	Text Field	Email address of the applicant. This field is auto-populated.
PIN **(required)**	Text Field	The applicant should specify a PIN for the certificate to protect the certificate.
Re-type PIN **(required)**		Confirmation of the above.
Select address fields to remove from the certificate **(optional)**	Checkboxes	By default, the address details are displayed in the View Certificate Details dialog. The applicant can hide these details selectively in the View Certificate Details dialog by selecting the 'Remove' checkboxes beside the required address fields. **Click here** for more details.
Submit	Control	Submits the application.
Cancel	Control	Clears all data entered on the form

Selecting Address Fields to be Removed from the Certificate

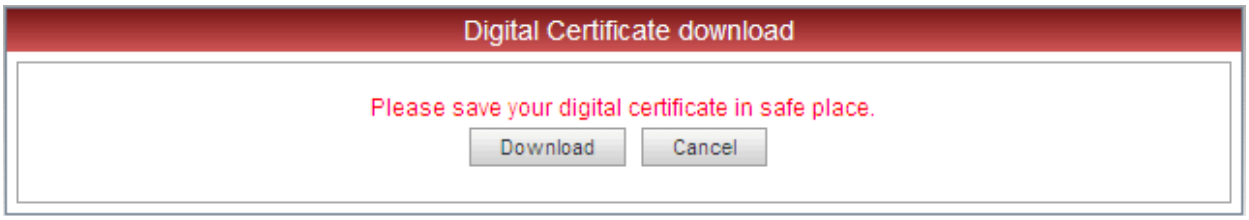
The following address fields...

- Address1;
- Address2;
- Address3:
- City;
- State/Province;
- Postal Code.

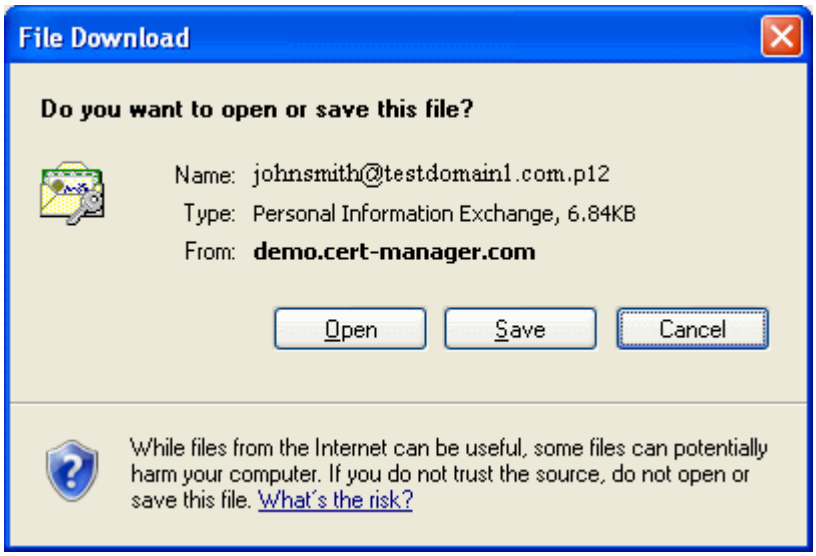
...are automatically populated with the address details of the Organization or Department that the user belongs to. The applicant can choose to remove these details from the client certificate by selecting the 'Remove' checkboxes below beside the corresponding field. The selected details will not be included in the certificate that is issued. The 'View Certificate Details' dialog will state 'Details Omitted' next to these fields.

3.2.5.1.5 Certificate Collection

Upon successful submission of the Account Validation form, a download dialog will be displayed enabling the applicant to download and save the certificate.



The applicant can collect the certificate by clicking 'Download' and save the file in a safe location in his/her computer.



CCM will deliver 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 will be asked for this PIN when he/she imports the certificate into the certificate store of their machine.

New end-users: If the end-user does not already exist in Certificate Manager (viewable in the 'Client Certificates' area of 'Certificates Management' section) then he/she will be automatically created and added as a new end-user belonging to the Organization for which the certificate was issued. This new end-user will now be viewable in the **Client Certificates Sub-tab** of the interface 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**: Name of the Organization to which this end-user belongs to.
- **Existing end-users**: If the end-user already exists, then the certificate will be associated with their end-user name.

See section '**The Client Certificates Area**' for more information regarding end-user and client certificate management.

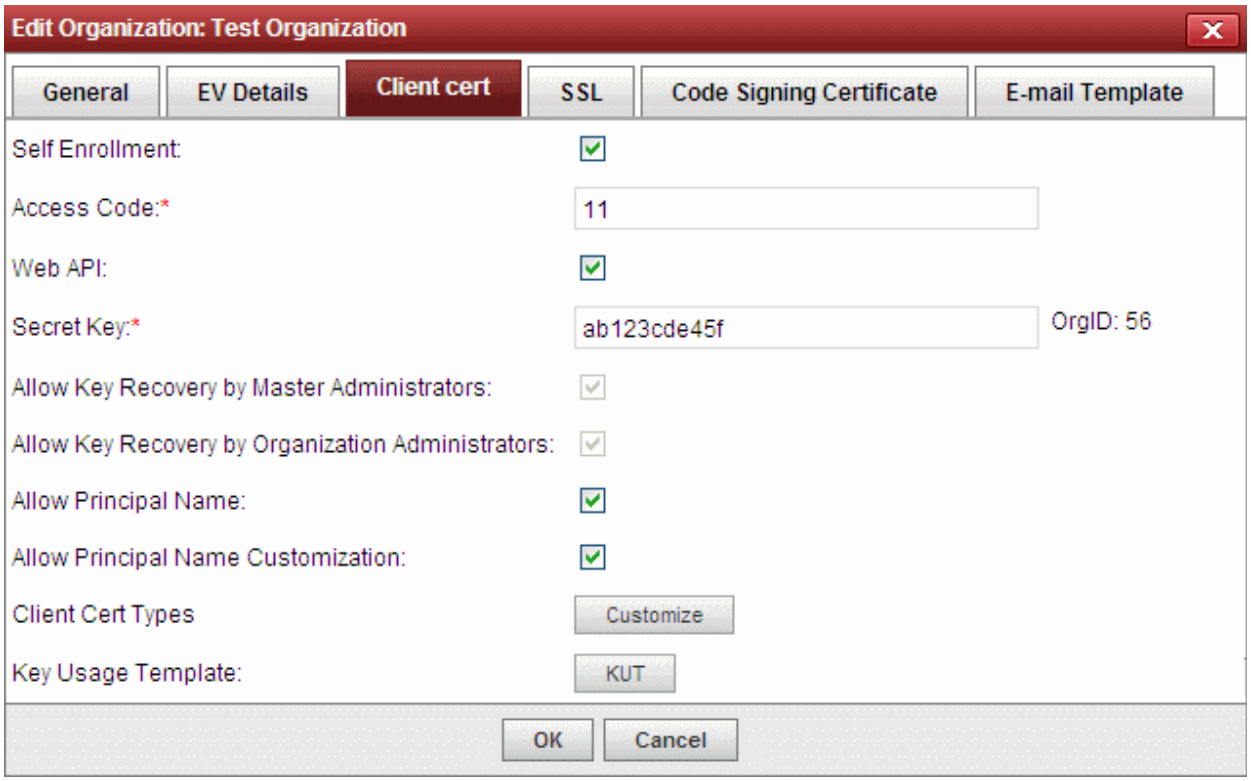
3.2.5.2 Self Enrollment by Secret Identifier

This section explains how the administrator can direct the end-user for self-enrollment using the Secret Identifier specified for the Organization and how the end-user can apply for, collect, download and install their certificate.

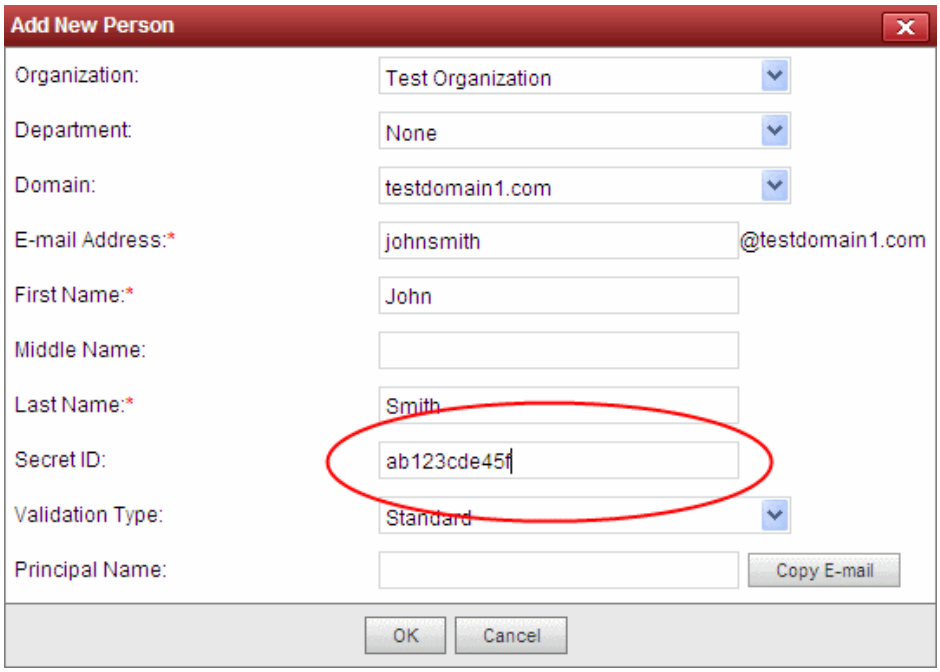
3.2.5.2.1 Prerequisites

- The domain from which the client certificate is to be issued has been enabled for SMIME certificates, has been pre-validated by Comodo and that the domain has been activated by your Comodo account manager. (i.e. if you wish to issue client certs to end-user@mycompany.com, then mycompany.com must have been pre-validated by Comodo).

  However, if you request a certificate for a brand new domain, then this domain will first have to undergo validation by Comodo. Once validated, this new domain will be added to your list of pre-validated domains and future certificates will be issued immediately.
- The domain from which the client certificates are to be issued has been delegated to the Organization or Department. See **Creating a New Organization** and **Editing an Existing Organization** for more details on adding a domain to an Organization.
- The RAO SMIME or DRAO SMIME administrator has been delegated control of this Organization or Department
- The administrator has **checked** the "Web API' box in the '**Client Cert' tab** of the 'Create/Edit' Organizations dialog box.



- The administrator has **specified a Secret ID** for the user using either the '**Add User**' or '**Edit User**' dialog boxes or when '**Importing from .csv**' .The secret code should be a mixture of alpha and numeric characters that cannot easily be guessed.



3.2.5.2.2 Procedure Overview

- Administrator confirms completion of the **prerequisite steps**.
- Administrator directs the personal certificate applicant to the 'Secret Identifier' based Self Enrollment Form - making sure the application is done from the end-user's computer (see section **Initiating the enrollment process**).
- Applicant completes then submits the Self Enrollment Form, specifying the correct Secret Identifier assigned to him/her. (See section **The Self Enrollment Form**)
- The certificate request is sent to Comodo CA servers. If the application is successful, the applicant will be able to download and install their personal certificate. (See the section **Certificate Collection**)

3.2.5.2.3 Initiating the Enrollment Process

After completing the **prerequisite steps**, administrators need to communicate enrollment details to each end-user, they wish to issue client certificates to. The communication must contain the following information:

1. A link to the Secret Identifier based Self Enrollment Form - https://cert-manager.com/customer/[REAL CUSTOMER URI]/smime?action=enroll&swt=si
2. The secret identifier specified for the end-user.

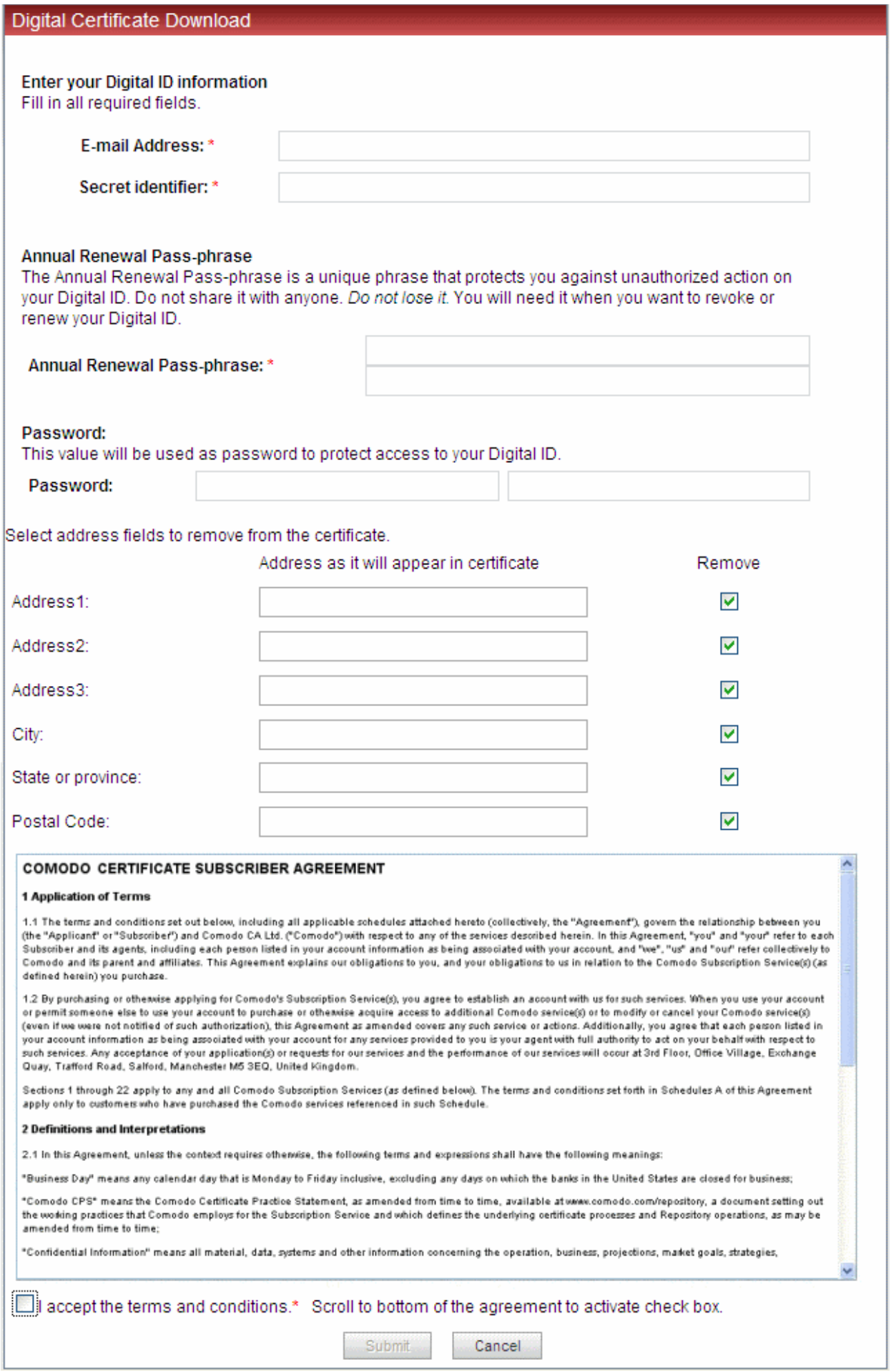
These details can be informed to the applicant by the any preferred out-of-band communication method like email. The end-user can access the form at the given url, fill-in with the necessary details and submit it.

Please Note: The domain of the email address that the end-user specifies in the Self Enrollment Form MUST match a 'Common Name' (domain) associated with an **Organization or Department within an Organization**. The applicant MUST be able to receive emails at this address.

The Secret Identifier the end-user enters at the Self Enrollment Form MUST match the identifier specified for him/her by the administrator.

3.2.5.2.3.1 Secret Identifier Based Self Enrollment Form

The applicant needs to fill the application form, shown below.


Digital Certificate Download
Enter your Digital ID information
Fill in all required fields.
E-mail 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: *
Password:
This value will be used as password to protect access to your Digital ID.
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:
COMODO CERTIFICATE SUBSCRIBER AGREEMENT
1 Application of Terms
1.1 The terms and conditions set out below, including all applicable schedules attached hereto (collectively, the "Agreement"), govern the relationship between you (the "Applicant" or "Subscriber") and Comodo CA Ltd. ("Comodo") with respect to any of the services described herein. In this Agreement, "you" and "your" refer to each Subscriber and its agents, including each person listed in your account information as being associated with your account, and "we", "us" and "our" refer collectively to Comodo and its parent and affiliates. This Agreement explains our obligations to you, and your obligations to us in relation to the Comodo Subscription Service(s) (as defined herein) you purchase.
1.2 By purchasing or otherwise applying for Comodo's Subscription Service(s), you agree to establish an account with us for such services. When you use your account or permit someone else to use your account to purchase or otherwise acquire access to additional Comodo service(s) or to modify or cancel your Comodo service(s) (even if we were not notified of such authorization), this Agreement as amended covers any such service or actions. Additionally, you agree that each person listed in your account information as being associated with your account for any services provided to you is your agent with full authority to act on your behalf with respect to such services. Any acceptance of your application(s) or requests for our services and the performance of our services will occur at 3rd Floor, Office Village, Exchange Quay, Trafford Road, Salford, Manchester M5 3EQ, United Kingdom.
Sections 1 through 22 apply to any and all Comodo Subscription Services (as defined below). The terms and conditions set forth in Schedules A of this Agreement apply only to customers who have purchased the Comodo services referenced in such Schedule.
2 Definitions and Interpretations
2.1 In this Agreement, unless the context requires otherwise, the following terms and expressions shall have the following meanings:
"Business Day" means any calendar day that is Monday to Friday inclusive, excluding any days on which the banks in the United States are closed for business;
"Comodo CPS" means the Comodo Certificate Practice Statement, as amended from time to time, available at www.comodo.com/repository, a document setting out the working practices that Comodo employs for the Subscription Service and which defines the underlying certificate processes and Repository operations, as may be amended from time to time;
"Confidential Information" means all material, data, systems and other information concerning the operation, business, projections, market goals, strategies,
I accept the terms and conditions.* Scroll to bottom of the agreement to activate check box.
Submit
Cancel

3.2.5.2.3.2 Form Parameters

Form Element	Type	Description
Email Address **(required)**	Text Field	Applicant should enter their full email address. The Email address must be for the domain belonging to the Organization.
Secret identifier **(required)**	Text Field	Applicant should enter the Secret ID specified for him/her. This should have been communicated to the applicant by the administrator.
Annual Renewal Pass-Phrase **(required)**	Text Field	This phrase is needed to renew or revoke the certificate should the situation arise.
Password **(required)**	Text Field	The applicant should specify a password for the certificate. This is needed for accessing the certificate e.g. 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 text box and reentered in the second text box for confirmation.
Select address fields to remove from the certificate **(optional)**	Checkboxes	By default, the address details are displayed in the View Certificate Details dialog. The applicant can hide these details selectively in the View Certificate Details dialog by selecting the 'Remove' checkboxes beside the required address fields. **Click here** for more details.
Eula Acceptance **(required)**	Checkbox	Applicant must accept the terms and conditions before submitting the form.
Submit	Control	Submits the application.
Cancel	Control	Clears all data entered on the form

Note: In addition to the standard fields in the Enrollment form, custom fields such as 'Employee Code, Telephone' can be added by the MRAO Administrator. Refer to the section **Custom Fields** for more details.

Selecting Address Fields to be Removed from the Certificate

The following address fields...

- Address1;
- Address2;
- City;
- State/Province;
- Postal Code.

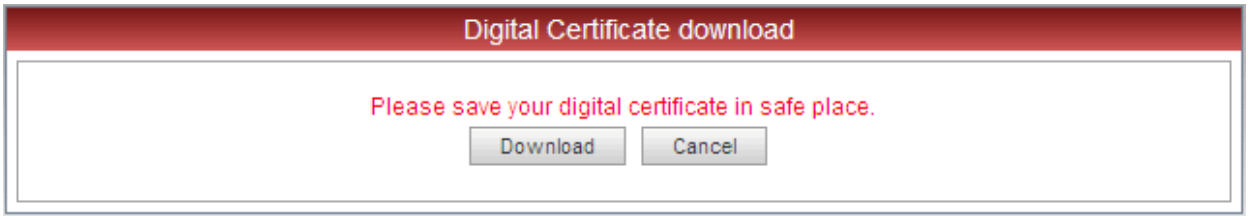
...are automatically populated with the address details of the Organization or Department that the user belongs to. The applicant can choose to remove these details from the client certificate by selecting the 'Remove' checkboxes below beside the corresponding field. The selected details will not be included in the certificate that is issued. The 'View Certificate Details' dialog will state 'Details Omitted' next to these fields.

After completing the form and clicking the 'Submit' button a certificate collection form will appear, enabling the end-user to download and save the certificate. See the section **Certificate Collection** for more details.

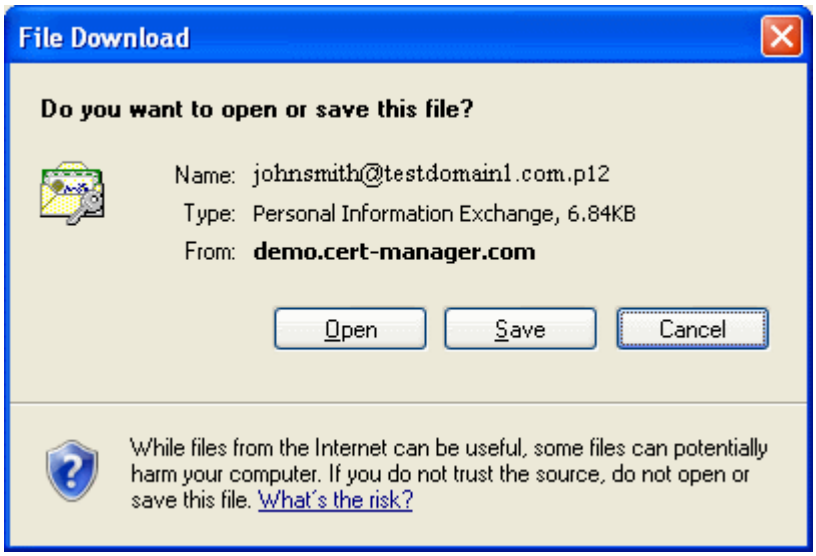
Note: It is possible for CCM Account holders to use their own, custom form templates rather than the default form supplied by Comodo. See your Comodo account manager for more details on enabling this functionality.

3.2.5.2.4 Certificate Collection

Once the enrollment form is submitted, a download dialog will be displayed enabling the applicant to download and save the certificate.



The applicant can collect the certificate by clicking 'Download' and save the file in a sale location in his/her computer.



CCM will deliver the certificate to the end-user in PKCS#12 file format (.p12 file). The PIN specified in the password fields is used to protect access to this .p12 file. The end-user will be asked for this PIN when he/she imports the certificate into the certificate store of their machine.

3.2.5.3 Enrollment by Invitation

This section explains how the administrator can invite the end-user for enrollment from the CCM interface and how the end-user can apply for, collect, download and install their certificate.

3.2.5.3.1 Prerequisites

- The domain from which the client certificate is to be issued has been enabled for SMIME certificates, has been pre-validated by Comodo and that the domain has been activated by your Comodo account manager. (i.e. if you wish to issue client certs to end-user@mycompany.com, then mycompany.com must have been pre-validated by Comodo).

  However, if you request a certificate for a brand new domain, then this domain will first have to undergo validation by Comodo. Once validated, this new domain will be added to your list of pre-validated domains and future certificates will be issued immediately.
- The domain from which the client certificates are to be issued has been delegated to the Organization or Department. See **Creating a New Organization** and **Editing an Existing Organization** for more details on adding a domain to an Organization.
- The RAO SMIME or DRAO SMIME administrator has been delegated control of this Organization or Department
- The administrator has added the end-user(s) to the Certificates Management > Client Certificates area of CCM.

3.2.5.3.2 Procedure Overview

Client certificates can be provisioned to the employees and end-users by inviting them for enrollment.

Overview of stages:

1. Administrator confirms completion of the **prerequisite steps**.

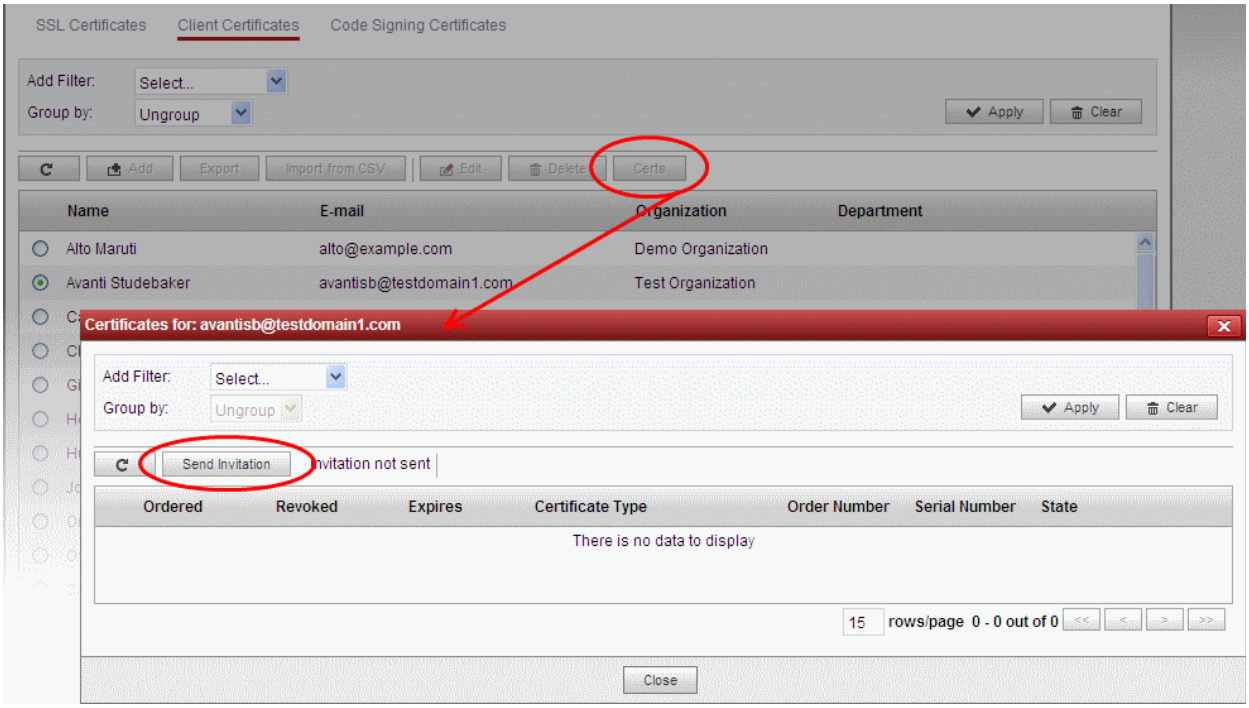
2. Administrator sends invitation for enrollment to the end-users from the Comodo CM interface. (see section **Initiating the Enrollment Process**)
3. CCM sends an Invitation mail to the end-user which contains a link to the User Registration Form. (See section **Validation of the Email Address** for more details)
4. The end-user completes the User Registration form. The certificate request is sent to Comodo CA servers. If the registration is successful, the end-user will be able to download and install their personal certificate. (See the section **Certificate Collection**)

3.2.5.3.3 Initiating the Enrollment Process

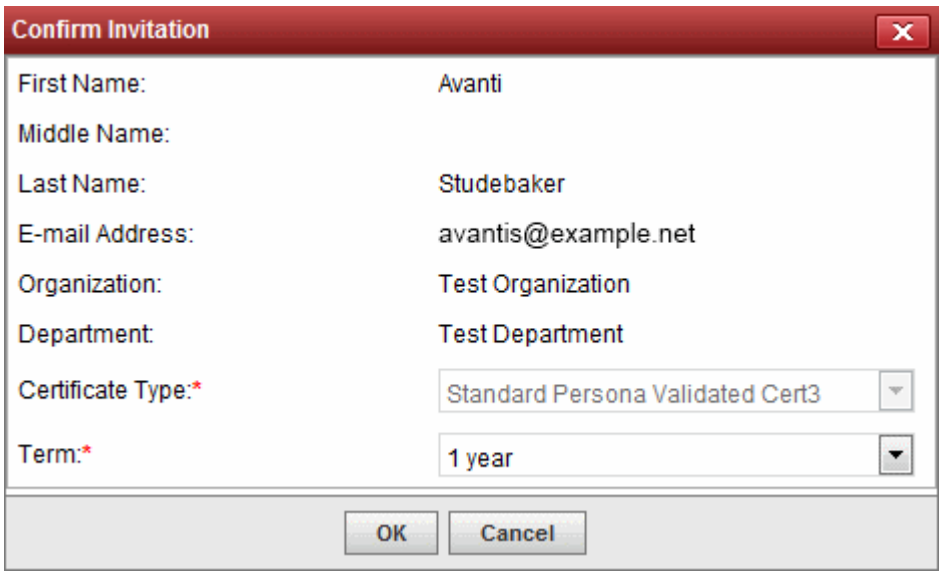
After completing the **prerequisite steps**, administrators need to send invitations to the end-users.

To send invitation administrator should:

- Click Certificate Management > Client Certificates. The list of end-users added previously will be displayed.
- Click 'Certs' button at the top after selecting the checkbox beside the end-user's name;
- In the dialog that appears press 'Send Invitation' button. (See screenshot below).



After clicking 'Send Invitation', the 'Confirm Invitation' dialog will be displayed:



The confirmation dialog displays the details of the user and allows the administrator to choose the client certificate type and the term.

Certificate Type - If your Organization's account has been enabled for High Personal Validated Certificates AND the administrator has specified a 'Validation Type' of 'High' * for this user THEN the 'Certificate Type' value will be a drop down menu rather than flat text. This menu will offer a choice between sending an invitation for a 'High Personal Validated' or a "Standard Personal Validated' certificate. The default choice is 'High Personal Validated'.

Certificate Term - You can choose the term length for the certificate to be issued to the end-user. The 'Term' drop-down displays the term options allowed for your Organization.

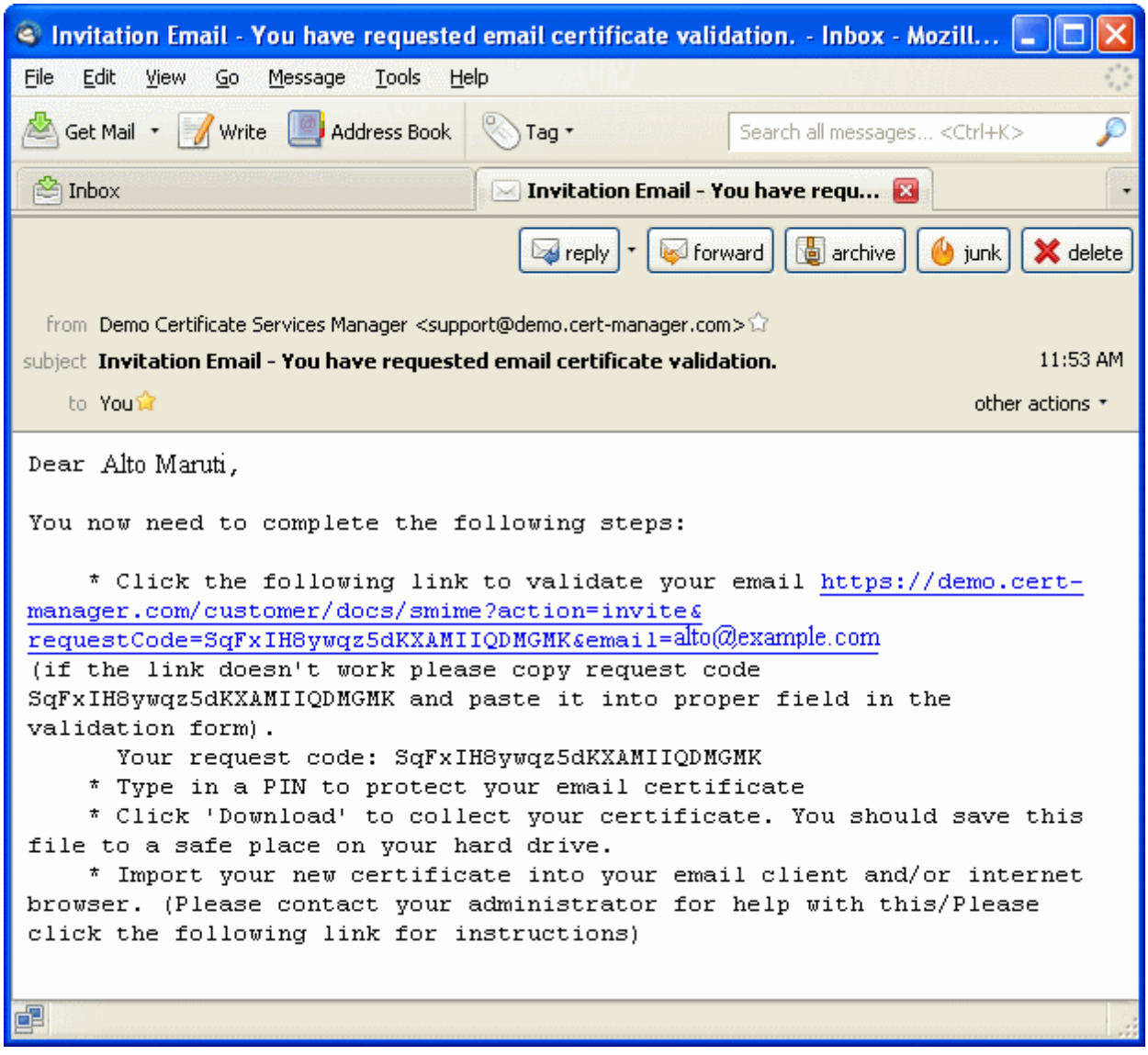
- Upon clicking 'OK', an invitation email will be sent to the end-user.

The email will contain the URL of the certificate validation form, a request validation code and instructions for downloading the certificate. The request code will be contained within the URL so that applicants can simply click the link or copy and paste the URL in their browser. See the section Validation of the Email Address for more details. On completion of the validation and user registration processes, a certificate collection form will appear, enabling the end-user to download and save the certificate. See the section **Certificate Collection** for more details.

3.2.5.3.4 Validation of the Email Address

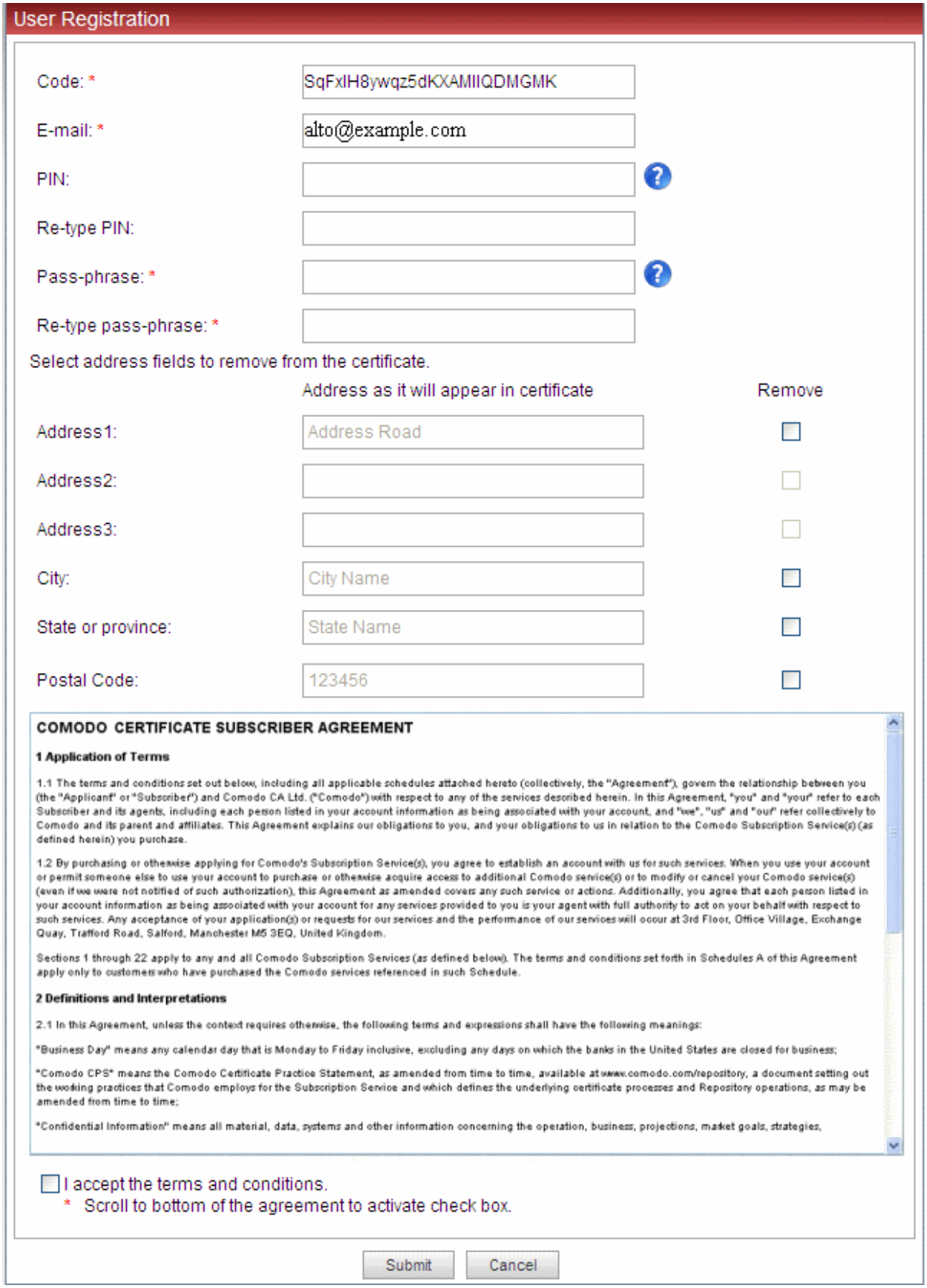
The end-user will receive an Invitation email on the administrator clicking the 'Send Invitation' button.

The invitation email will contain a link to the User Registration form. The link will also contain a randomly generated 'Request Code' that the end-user will need in order to validate that they are the correct applicant. Simply clicking on the link in the email will automatically populate the request 'Code' and 'Email' fields in the User Registration form.



Note: It is possible for administrators to modify the contents of these emails in the '**Email Templates**' area under the 'Settings' tab.

Upon clicking the link the applicant will be taken to the user registration form.



Form Element	Type	Description
Code **(required)**	Text Field	The validation request code. This field is auto-populated when the applicant clicks the validation link contained in the email.
E-mail **(required)**	Text Field	Email address of the applicant. This field is auto-populated.
PIN **(required)**	Text Field	The applicant should specify a PIN for the certificate to protect the certificate.
Re-type PIN **(required)**	Text Field	Confirmation of the above.
Pass-Phrase **(required)**	Text Field	The end-user needs to enter a pass-phrase for their certificate. This phrase is needed to revoke the certificate should the situation arise.
Select address fields to remove from the certificate **(optional)**	Checkboxes	By default, the address details are displayed in the View Certificate Details dialog. The applicant can hide these details selectively in the View Certificate Details dialog by selecting the 'Remove' checkboxes beside the required address fields. **Click here** for more details.
Eula Acceptance **(required)**	Checkbox	Applicant must accept the terms and conditions before submitting the form.
Submit	Control	Submits the application.
Cancel	Control	Clears all data entered on the form

Selecting Address Fields to be Removed from the Certificate

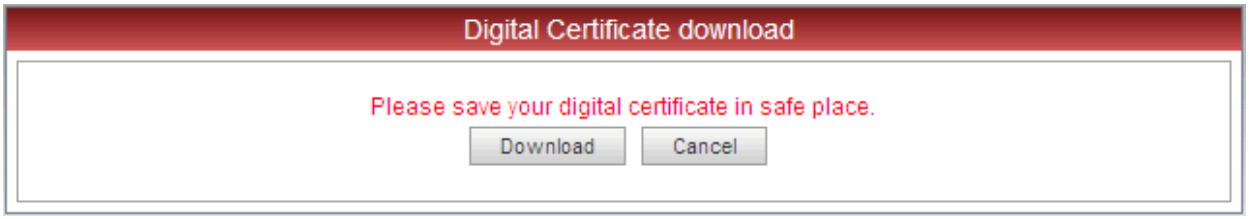
The following address fields...

- Address1;
- Address2;
- Address3:
- City;
- State/Province;
- Postal Code.

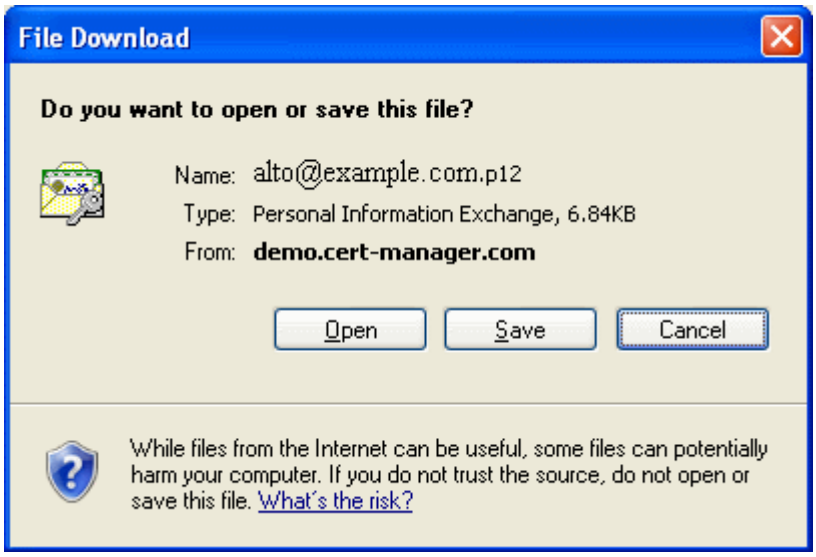
...are automatically populated with the address details of the Organization or Department that the user belongs to. The applicant can choose to remove these details from the client certificate by selecting the 'Remove' checkboxes below beside the corresponding field. The selected details will not be included in the certificate that is issued. The 'View Certificate Details' dialog will state 'Details Omitted' next to these fields.

3.2.5.3.5 Certificate Collection

Upon successful submission of the Account Validation form, a download dialog will be displayed enabling the applicant to download and save the certificate.



The applicant can collect the certificate by clicking 'Download' and save the file in a sale location in his/her computer.



CCM will deliver the certificate to the end-user in PKCS#12 file format (.p12 file). The pass-code specified in the PIN fields is used to protect access to this .p12 file. The end-user will be asked for this PIN when he/she imports the certificate into the certificate store of their machine.

See section '**The Client Certificates Area**' for more information regarding end-user and client certificate management.

3.2.6 Revocation of Client Certificates

The client certificates belonging to any end-user can be revoked by two ways:

- The Administrator can revoke the client certificate belonging to any end-user, from the Certs dialog accessible by clicking **Certificates Management** > **Client Certificates** > clicking **Certs** button at the top after selecting the checkbox beside the end-user's name. See the section '**Certs' Dialog** for more details;
- The end-user can directly revoke their client certificate. See the section **Revocation of Client Certificates by End-Users** for more details.

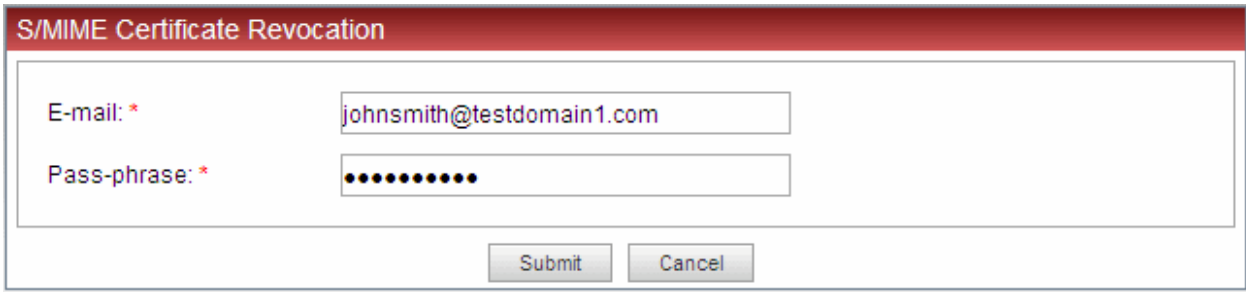
3.2.6.1 Revocation of Client Certificates by End-Users

End-users can revoke their client certificates on their own, when a necessity arises. On such an occasion, the end-user can request the administrator. The Administrator can direct the end-user to access the revocation interface hosted at **https://cert-manager.com/customer/Comodo/smime?action=revoke**. The pass-phrase set for the certificate is required for revoking the certificate by the end-user.

3.2.6.1.1 Procedure Overview

1. The end-user requests for access to the self revocation interface to the Administrator.
2. The Administrator directs the end-user to the revocation interface hosted at https://cert-manager.com/customer/[REAL CUSTOMER URI]/smime?action=revoke
3. The end-user accesses the revocation interface and fills the revocation form with the email address and the pass-phrase set by him/her during self-enrollment or User Registration and submits the form.
4. The client certificate is revoked.

3.2.6.1.2 Revocation form



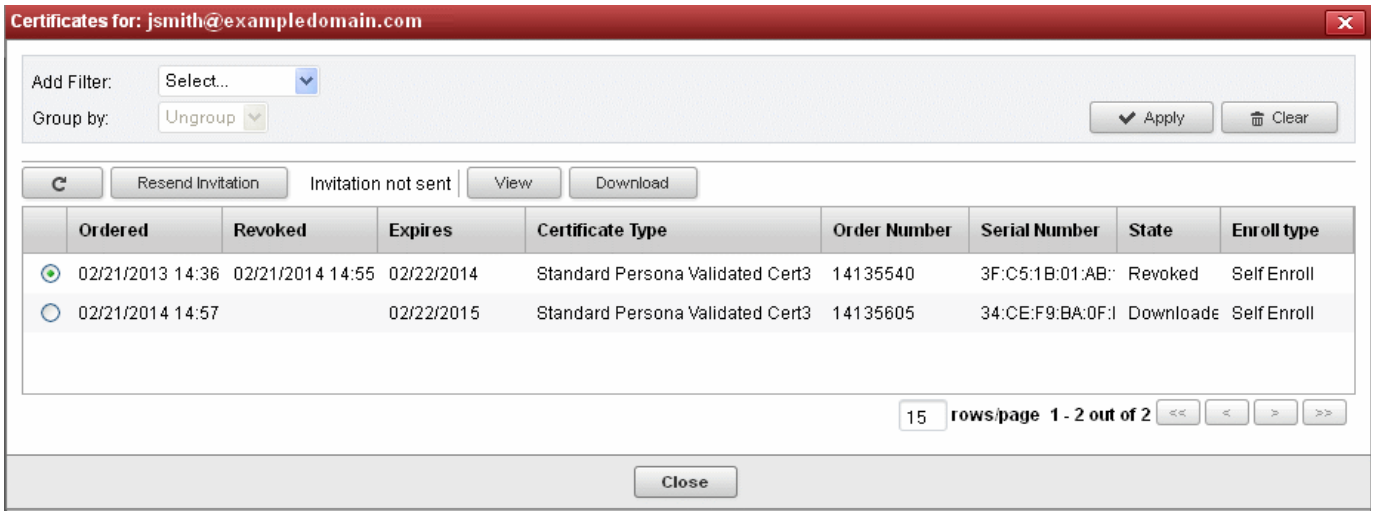
3.2.6.1.3 Form Parameters

Form Element	Type	Description
Email **(required)**	Text Field	The end-user should enter their full email address.
Pass Phrase **(required)**	Text Field	The end-user should enter the pass-phrase of the client certificate. This Pass-phrase must be the same as entered during **self enrollment** or in the **User Registration form**.
Submit	Control	Submits the application.
Cancel	Control	Cancels the process.

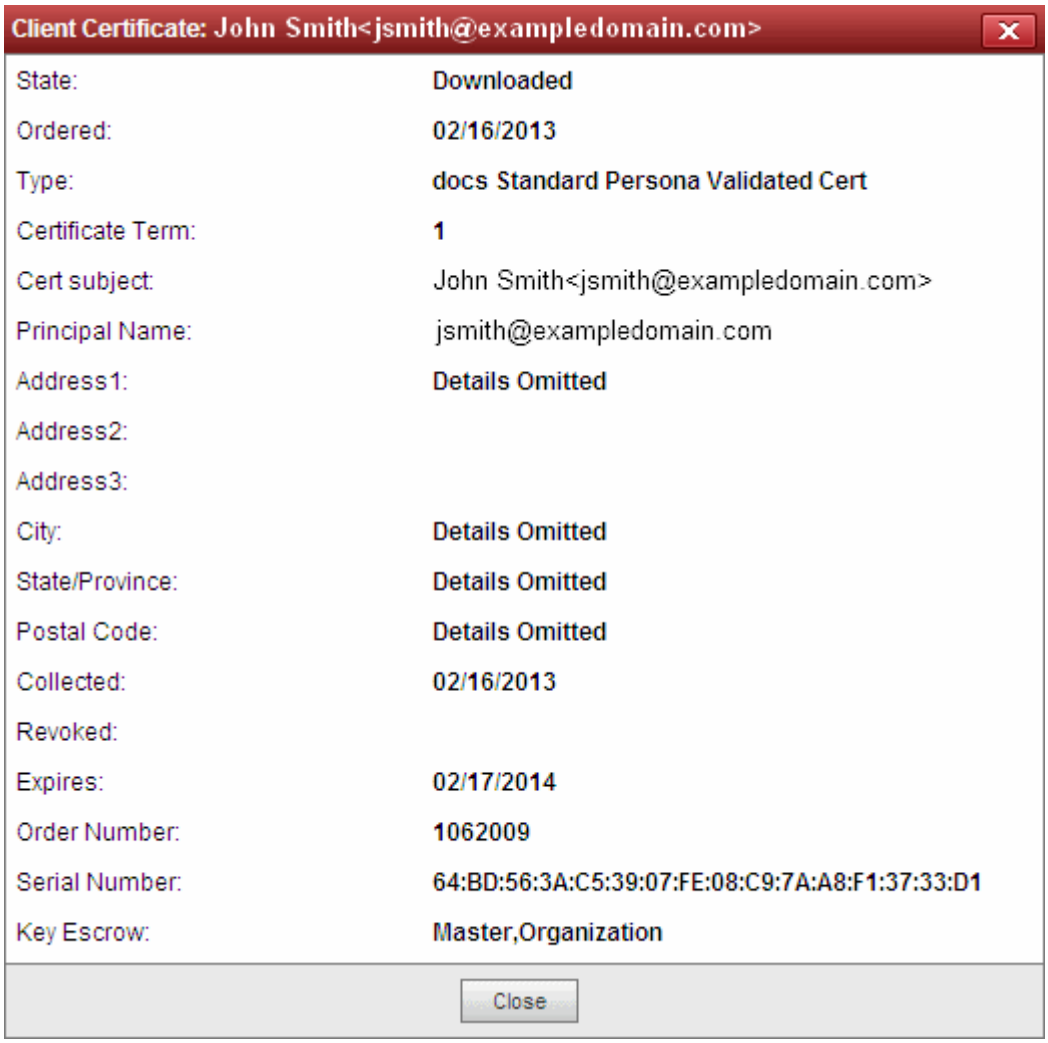
3.2.7 Viewing End-User's Certificate

Administrators can view the certificates applied for, downloaded by or issued to the end-users from the Client Certificates area.

Selecting the person whose certificate is to be viewed and clicking the 'Certs' button at the top will open the 'Certificates for...' dialog.



- Select the certificate that you want to view the details and click the 'View' button at the top.



Client Certificate 'View' Dialog - Table of Parameters		
Field	**Type**	**Description**
State		Indicates the current status of the certificate.
	Invited	The end-user has been sent an invitation email by the Administrator
	Requested	The request has been sent to the Certificate Authority (CA) for approval.
	Applied	The end-user has validated the email and applied for the certificate.
	Issued	The certificate was issued by CA and collected by Certificate Manager. A Blue font color (Issued) means that the certificate was issued by CA but was not installed.
	Downloaded	The end-user has downloaded the certificate.
	Revoked	The certificate in question is invalid because it was revoked .
	Expired	The certificate in question is invalid because it's term has expired.
	Rejected	CA rejected the request after validation check.
Ordered	Numeric	Date of the request made by CCM to CA
Type	Text Field	Type of the client certificate.
Certificate Term	Text Field	The life term of the certificate

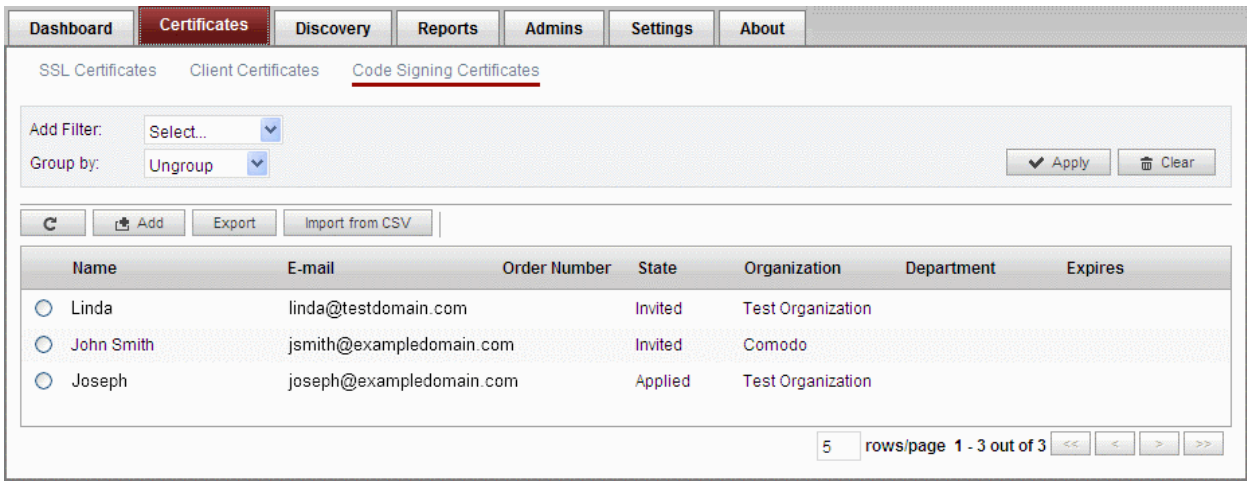
Client Certificate 'View' Dialog - Table of Parameters		
Field	**Type**	**Description**
Cert subject	Text Field	Name and email address of the end-user
Principal Name	Text Field	Principal name included in the certificate
Address 1: **Address 2:** **Address 3:** **City:** **State or Province:** **Postal Code:**	Text Fields	Displays the address of the Organization as mentioned while requesting for the certificate. Only those address fields that were allowed to be displayed while applying for the certificate are shown here and the rest of the fields are displayed as "Details Omitted".
Collected	Numeric	Date of the collection of certificate by CCM from CA
Revoked	Numeric	Date of the revocation of the certificate
Expires	Numeric	Expiry date of the certificate.
Order Number	Numeric	Order number of the certificate request made to CA.
Serial Number	Numeric	Serial number of the certificate.
Key Escrow		Indicates whether Key Escrow is available for certificate recovery by the administrator.

3.3 The Code Sign Certificates Area

The Code Sign Certificates area provides administrators with the information and controls necessary to manage the life-cycle of code signing certificates for their respective Organization/Department.

Visibility of the 'Client Certificates' area is restricted to:

- MRAO administrators - can view the code signing certificates and their end-users of any Organization or Department.
- RAO Code Signing administrators - can view the code signing certificates and their end-users of Organizations (and any subordinate Departments) that have been delegated to them.
- DRAO Code Signing administrators - can view the code signing certificates and their end-users of Departments that have been delegated to them.



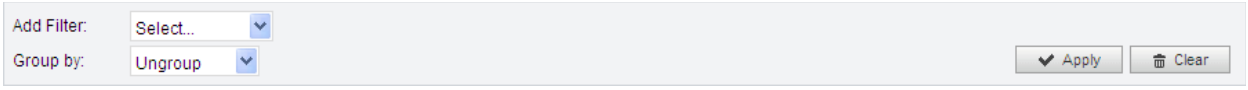
Code Sign Certificates area - Table of Parameters		
Field Name		**Description**
Name		Name of the applicant
Email		Email address of the applicant.
Order Number		Order number of the certificate request made to CA.
State		Indicates the current status of the certificate.
	Invited	The applicant has been sent an invitation email by the Administrator
	Requested	The request has been sent to the Certificate Authority (CA) for approval.
	Applied	The applicant has validated the email and applied for the certificate.
	Issued	The certificate was issued by CA and collected by Certificate Manager, but not downloaded by the applicant.
	Downloaded	The applicant has downloaded the certificate.
	Revoked	The certificate in question is invalid because it was revoked .
	Expired	The certificate in question is invalid because it's term has expired.
	Rejected	CA rejected the request after validation check.
Organization		Name of the Organization to which the applicant belongs.
Department		Name of the Department to which the applicant belongs.
Expires		Expiry date of the certificate.
Control Buttons	Add	Allows the administrator to add new end-user for the process of issuing code signing certificate
	Export	Allows administrators to save the list of code signing certificates in CSV format
	Import from CSV	Allows administrators to import a list of code signing certificates into Comodo CM in comma separated values (.csv) format.
	Refresh	Updates the currently displayed list of users. Will remove any users that have been recently deleted and add any that have been recently created. Will update details such as Organization, email etc if those details have recently changed.
Certificate Control Buttons **Note**: The types of certificate control buttons that are displayed in the table header depends on	View	Allows to view information about the certificate (see **Code Sign certificate "View' dialog** description)
	Resend Invitation	Re-sends the invitation email to the applicant (thus validating the applicant's email address and enabling them to request their certificate)
	Approve	Approves the certificate request from the applicants (end-users) and sends the request for the certificate to CA. If the request is approved by Comodo CA, the certificate State changes to 'Issued'. If the request was declined by Comodo CA because of incorrect enrollment details (for example, a mistake in the CSR or other form value), then 'State' changes to 'Invalid'. If the request was declined by Comodo CA for legal reasons then the state of the certificate changes to 'Rejected'.

Code Sign Certificates area - Table of Parameters		
Field Name		**Description**
the state of the selected certificate		Certificate requests can be approved by: • An MRAO • An RAO Code signing Administrator of the Organization on whose behalf the request was made. • A DRAO Code signing Administrator of the Department within the Organization on whose behalf the request was made.
	Decline	Declines the certificate request. This request will not be sent to Comodo CA for processing.
	Revoke	Revokes the certificate.
	Delete	Deletes the certificate

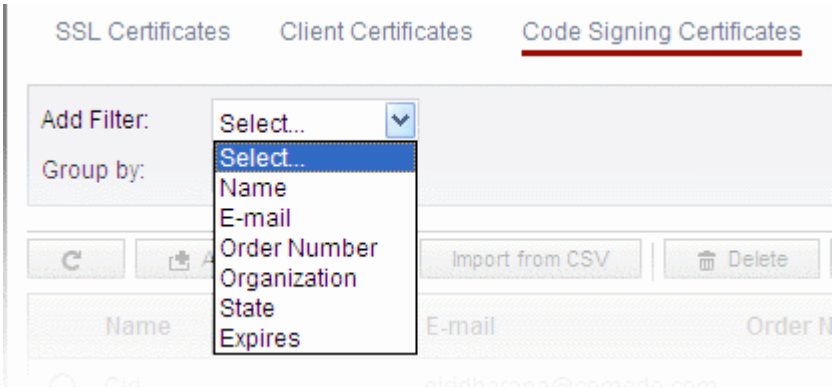
3.3.1 Sorting and Filtering Options

- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective column.

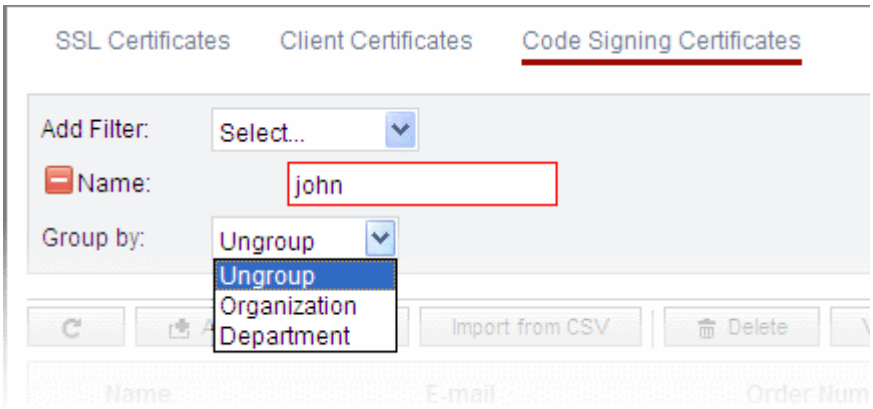
Administrators can search for particular code signing certificates by using filters under the sub-tab:



You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with another set of options available from the 'Group by' drop-down. For example, if you want to filter the certificates with 'Name' and group with 'Organization', select 'Name' from the 'Add Filter' drop-down:



- Enter part or full name in the Name field.
- Select 'Organization' from the 'Group by' drop-down.



- Click the 'Apply' button.

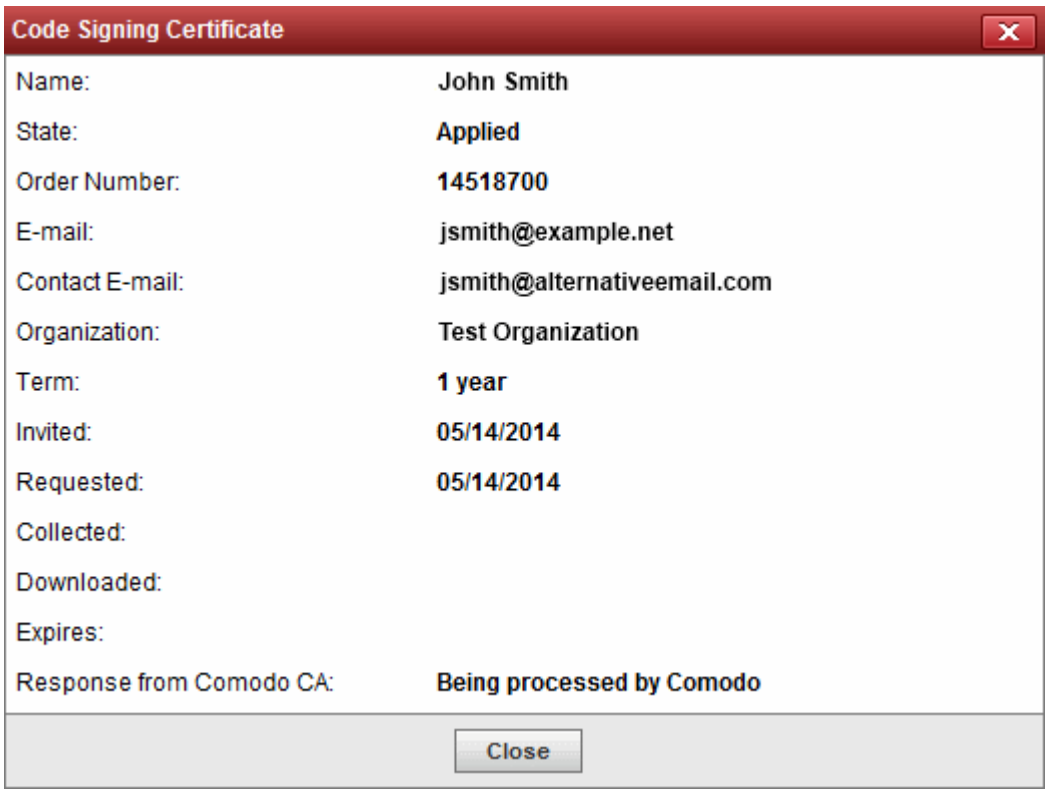
The filtered items based on the entered parameters will be displayed.

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Code Signing Certificates' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

3.3.2 Code Sign Certificates View Dialog

Clicking the 'View' button after selecting a certificate listed in the Code Sign Certificates tab will open a panel containing a summary of that certificate's details.



Code Sign Certificate 'View' Dialog - Table of Parameters		
Field Element	**Type**	**Description**
Name	Text Field	Name of the applicant.
State		Indicates the current status of the certificate.
	Invited	The applicant has been sent an invitation email by the Administrator
	Requested	The request has been sent to the Certificate Authority (CA) for approval.
	Applied	The applicant has validated the email and applied for the certificate.
	Issued	The certificate was issued by CA and collected by Certificate Manager, but not downloaded by the end-user.
	Downloaded	The end-user has downloaded the certificate.
	Revoked	The certificate in question is invalid because it was revoked .
	Expired	The certificate in question is invalid because it's term has expired.
	Rejected	CA rejected the request after validation check.
Order Number	Numeric	Order number of the certificate request made to CA.
Email	Text Field	End-user's email address.
Contact Email	Text Field	Contact email address or alternative email address of the applicant. The contact email address may be the customer facing email address like support@company.com, sales@company.com etc.
Organization	Text Field	Name of the Organization to which the end-user belongs.
Term	Numeric	The life term of the certificate
Invited	Numeric	Date at which invitation was sent to the end-user
Requested	Numeric	Date of the request made by CCM to CA
Collected	Numeric	Date of the collection of certificate by CCM from CA
Downloaded	Numeric	Date of download of certificate by the end-user
Expires	Numeric	Expiry date of the certificate.
Response from CA	Text Field	Comments, if any, from the CA

3.3.3 Adding Certificates to be Managed

There are several methods of adding certificates to the Code Sign Certificates area of Certificate Manager.

- **Manually adding certificates**
- **Loading multiple certificates from a comma separated values (.csv) file**
- **Auto Creation of end-users by initiating self enrollment**

3.3.3.1 Manually Adding Certificates

- Click Certificates Management > Code Signing Certificates
- Click the 'Add' button to open the 'Add New Code Signing Certificate' form.

Add New Code Signing Certificate dialog - Table of parameters		
Field	**Type**	**Description**
Organization	Drop-down	Select the Organization to which the applicant belongs.
Department	Drop-down	Select the Department to which the applicant belongs.
Domain	Drop-down	Select the domain pertaining to the Department
Term	Drop-down	Select the term of the certificate.
Email Address	Text field	Enter the email address of the applicant.
Full Name	Text field	Full name of the applicant.
Contact Email	Text field	Enter 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 like support@company.com, sales@company.com etc.

- Complete the 'Add New Code Signing Certificate' form.
- Click 'OK'.

If the applicant is an existing user, the corresponding certificate will be automatically added to CCM. If the applicant is a new user, an invitation mail will be sent to initiate self enrollment process. Refer to **Request and issuance of code signing certificates** for more details on self enrollment.

3.3.3.2 Loading Multiple Certificates from a Comma Separated Values (.csv) File

Administrators can import a list of code signing certificates into Comodo CM in comma separated values (.csv) format. After importing the list, the certificates belonging to existing users will be automatically added and invitation emails will be sent to new users automatically to initiate the self enrollment process, Refer to **Request and issuance of code signing certificates** for more details on self enrollment.

3.3.3.2.1 Procedure Overview

Summary of required steps for adding certificates by loading a .csv file:

1. Administrator generates a .csv file using containing a list of the certificates. .csv files can be exported directly from spreadsheet programs such as Excel or Open Office Calc.
2. Administrator loads the .csv file to CCM by clicking 'Load from CSV' in 'Certificates Management' > 'Code Sign Certificates' interface.

3.3.3.2.2 Requirements for .csv file

- There are 6 potential values per certificate that can be imported in CCM, but 4 are mandatory. As long as each user listed in the .csv file has at least these four elements then they can be added into the system.
- The 6 potential values are as follows. Mandatory values are highlighted in red. Make sure to export with the commas (,) and the quotation marks ("") as specified below

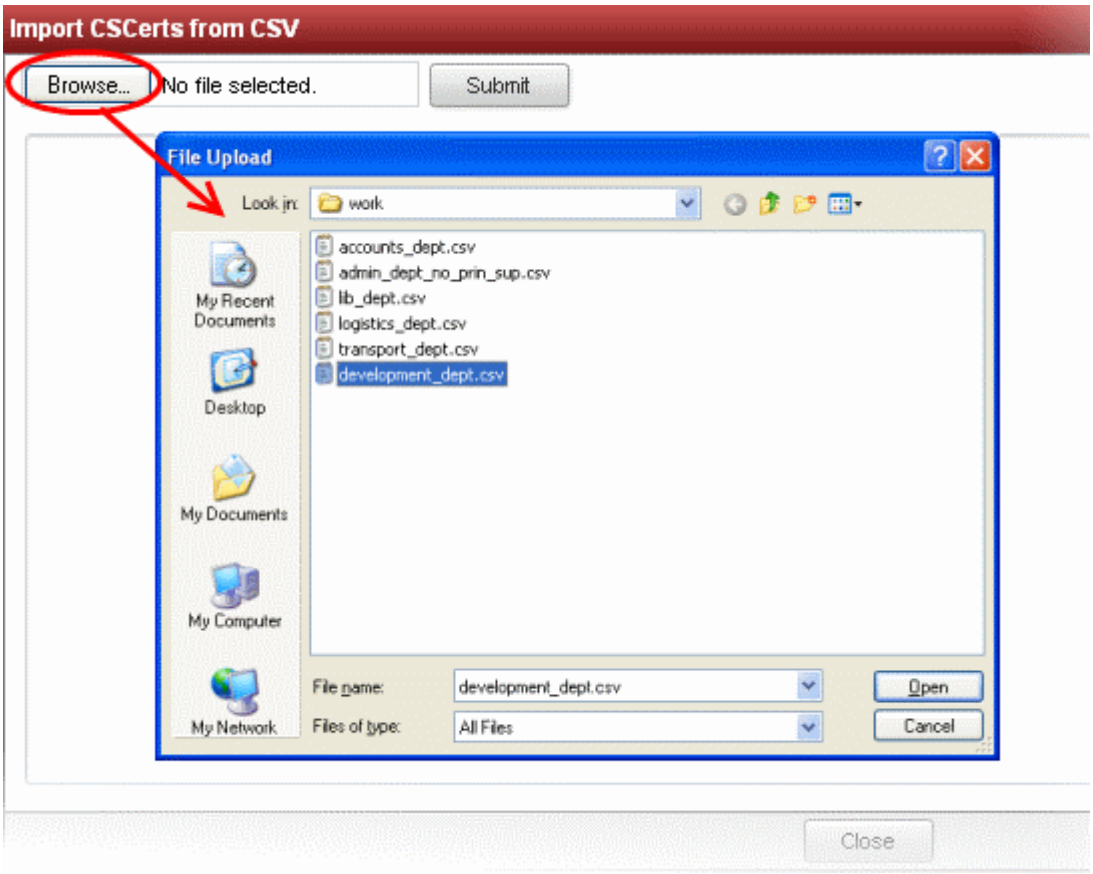
  "Organization","Department","Term","Email Address","Full Name","Contact Email Address"
- The following table explains the requirements and formats of the values.

Values	Organization	Department	Term	Email Address	Full Name	Contact Email Address
Required	Yes	No	Yes	Yes	Yes	No
Min Length (characters)	1	0	1	3	1	3
Max Length (characters)	128	128	1	128	64	128
Format			integer	Valid email address	Valid name	Valid email address
Characters allowed	ANY	ANY	01/05/10	A-Z, a-z, 0-9, '.', '-', '_' ,'@'	A-Z, a-z, 0-9, '.', '-', ' '	A-Z, a-z, 0-9, '.', '-', '_' , '@'

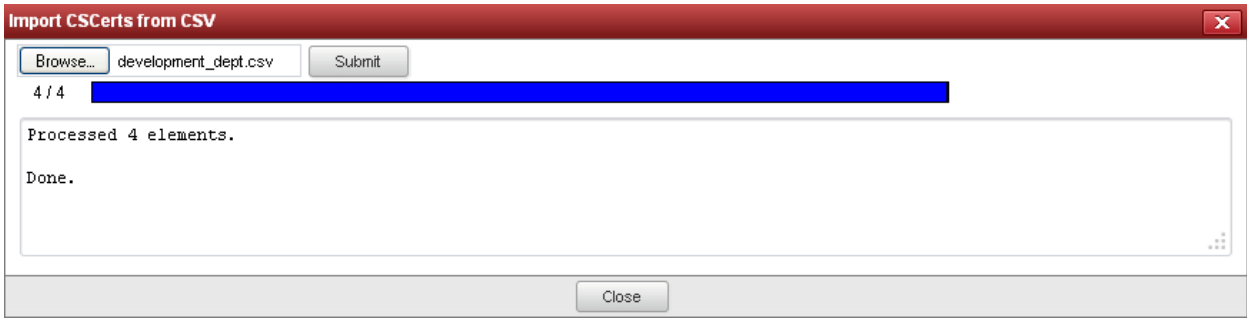
Example:

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

In order to do load the .csv file to CCM, click on 'Load from CSV' in 'Certificates Management' > 'Code Sign Certificates' interface. A File Upload dialog will appear. Click the 'Browse' button, and navigate to the in .csv file, and click on 'Submit'.



An import status dialog box is displayed. You will see a progress bar indicating that information is being uploaded. On successful completion, all the imported data will appear in the list of certificates in 'Code Sign Certificates' and 'Organization' areas.



3.3.3.3 Auto Creation of End-Users by Initiating Self Enrollment

Certificates issued to end-users by the self enrollment process initiated by an Administrator are automatically added to the 'Certificate Management - Code Sign Certificates' area. For more details see: **Request and issuance of code signing certificates**.

3.3.4 Request and Issuance of Code Signing Certificates

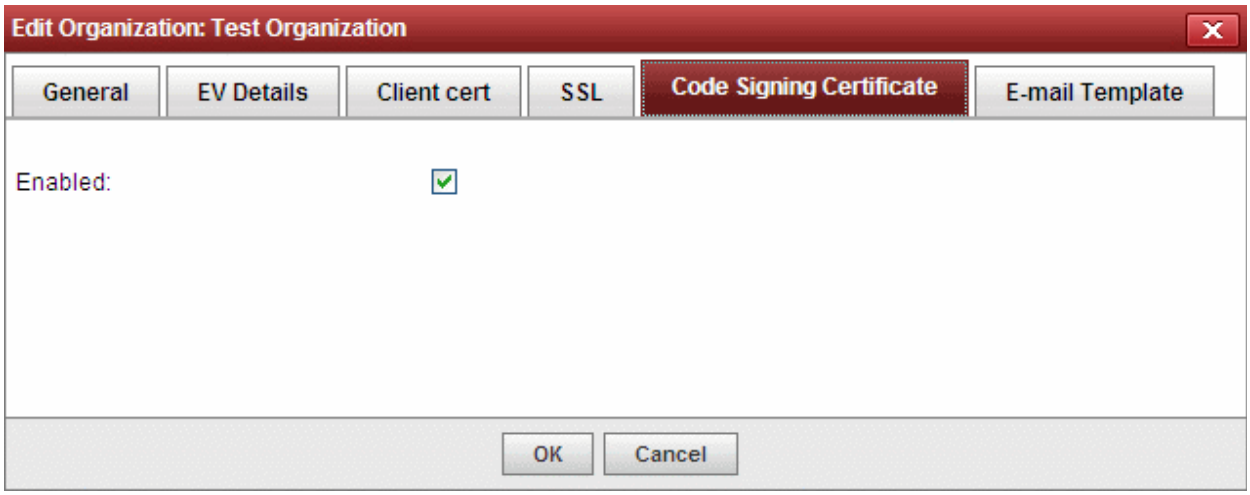
3.3.4.1 Prerequisites

- The domain for which the code signing certificate is to be issued has been enabled for Code Signing certificates, has been pre-validated by Comodo and that the domain has been made activate by your Comodo account manager. (i.e. if you wish to issue code signing certs to end-user@mycompany.com, then mycompany.com must have been pre-validated by Comodo.) All certificate requests made on 'pre-validated' domains or sub-domains thereof are issued automatically.

  However, if you request a certificate for a brand new domain, then this domain will first have to undergo validation by Comodo. Once validated, this new domain will be added to your list of pre-validated domains and future certificates

will be issued immediately.

- The domain from which the client certificates are to be issued has been delegated to the Organization or Department. See **Creating a New Organization** and **Editing an Existing Organization** for more details on adding a domain to an Organization.
- 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 the 'Enabled' checkbox in the '**Code Signing tab**' of the 'Add New/Edit' Organizations dialog box (see screen-shot below)



3.3.4.2 Procedure Overview

The Code Signing Certificates can be provisioned to the employees and end-users using a self-enrollment process.

Overview of stages:

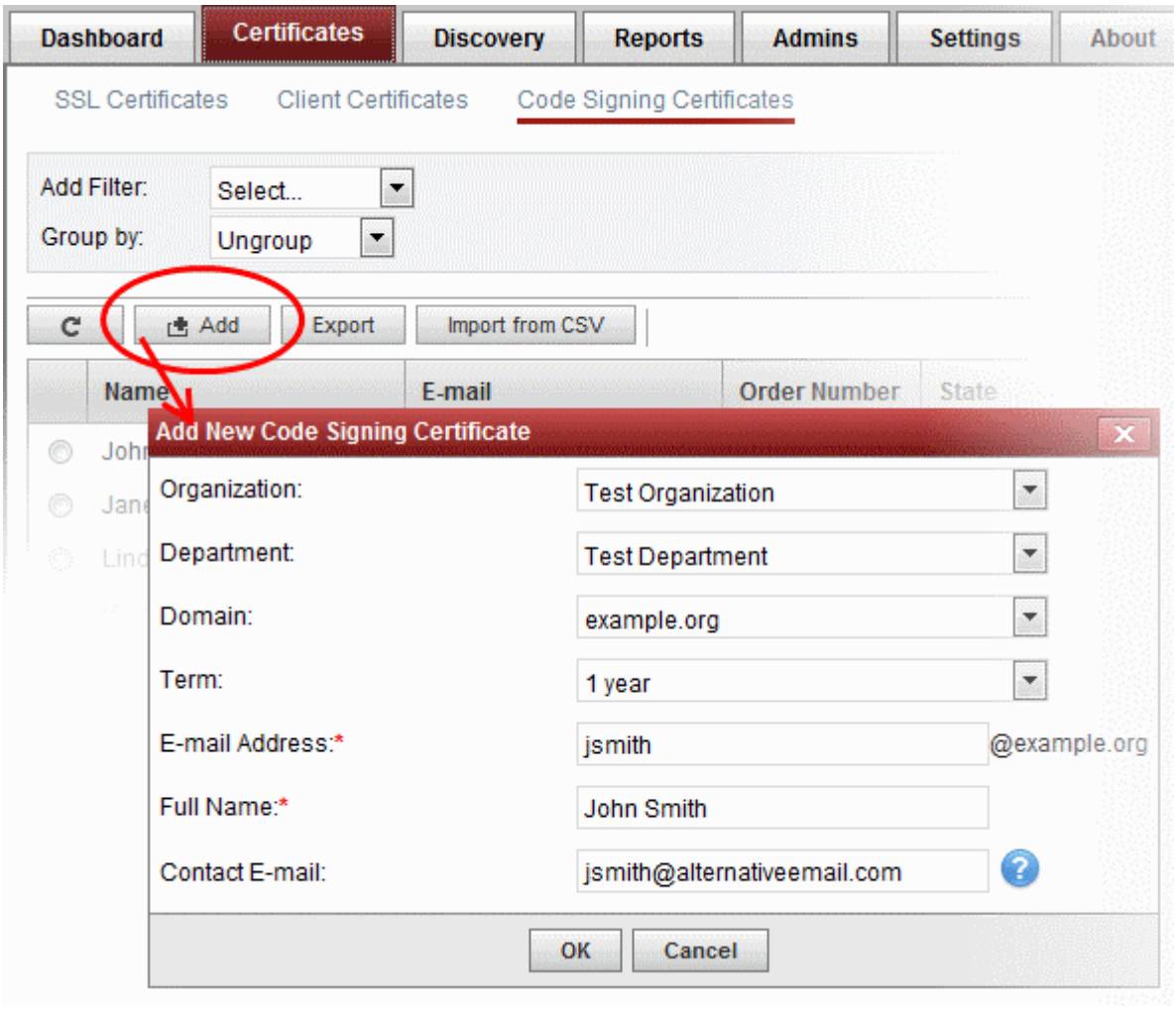
1. The administrator confirms the completion of the **prerequisite steps**.
2. The administrator sends an invitation email to the end-user for enrollment.
3. End-user validates the email address, completes the online form for auto-generation of CSR and requests for the certificate.
4. The certificate request is sent to Comodo CA servers by CCM.
5. If the application is successful, CCM sends an email with a download link to the end-user, enabling to download the certificate.
6. The certificate will be automatically added to the end-user account in CCM and will be manageable form the 'Code Sign Certificates' area.

3.3.4.3 Initiating the Enrollment Process

After completing the **prerequisite steps**, Administrators need to send an invitation to the end-user.

To send invitation and initiate the process

- Click the Add button from the 'Code Sign Certificates' area. This will open 'Add New Code Signing Certificate' dialog.



Add New Code Signing Certificate dialog - Table of parameters		
Field	**Type**	**Description**
Organization	Drop-down	Select the Organization to which the applicant belongs.
Department	Drop-down	Select the Department to which the applicant belongs.
Domain	Drop-down	Select the domain pertaining to the Department
Term	Drop-down	Select the term of the certificate.
Email Address*	Text field	Enter the email address of the applicant. The invitation message will be sent to this address. This will be validated before commencing the request process.
Full Name*	Text field	Enter the Full name of the applicant.
Contact Email	Text field	Enter 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 like support@company.com, sales@company.com etc.

Fields marked with* are mandatory.

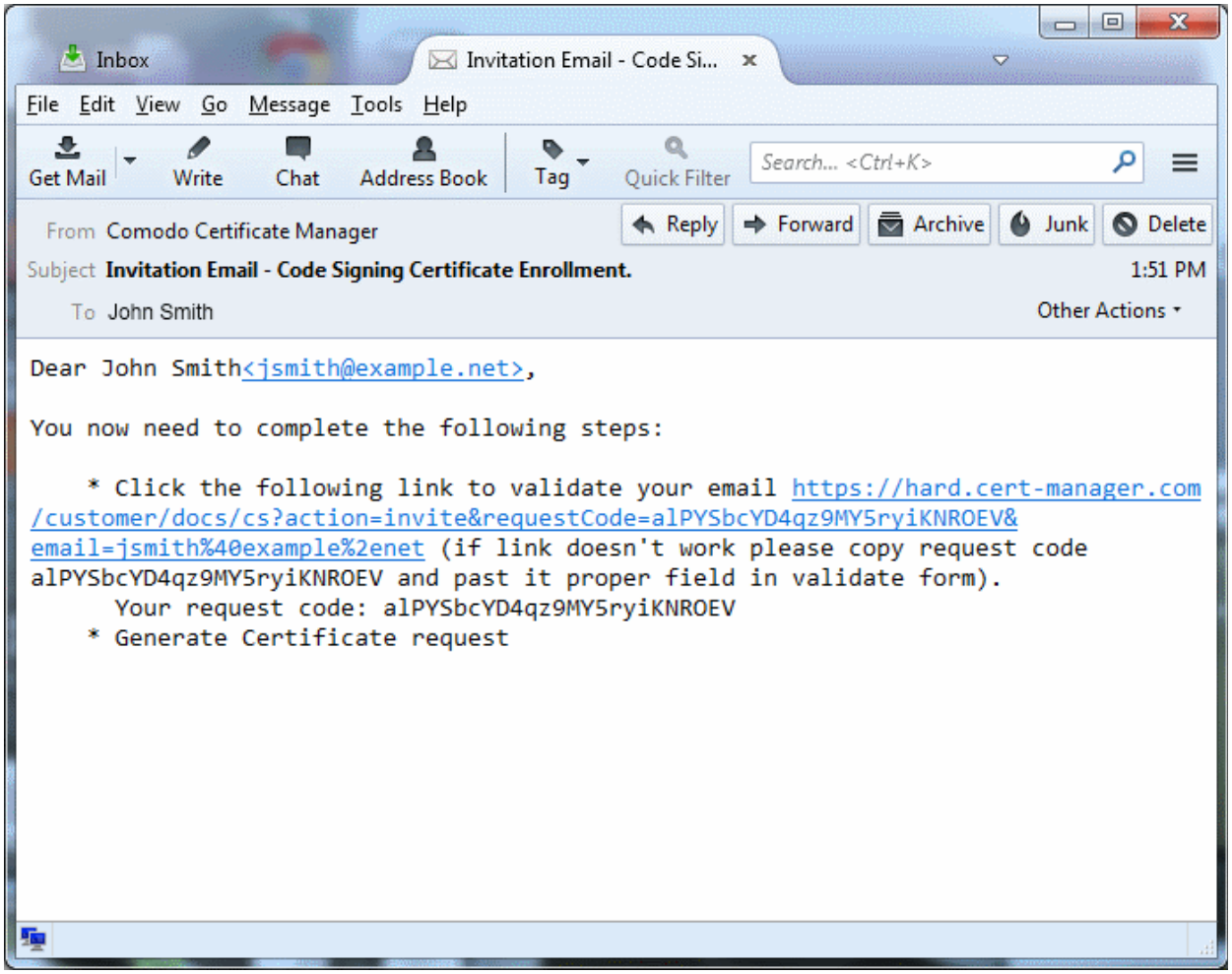
- Fill the necessary details and click 'OK'.

An invitation email will be automatically sent to the applicant. The certificate status will be set to 'INVITED' and added to 'Code Signing Certificates' area of CCM.

Note: For the new applicants added by **importing a .csv file**, the invitations will be sent automatically.

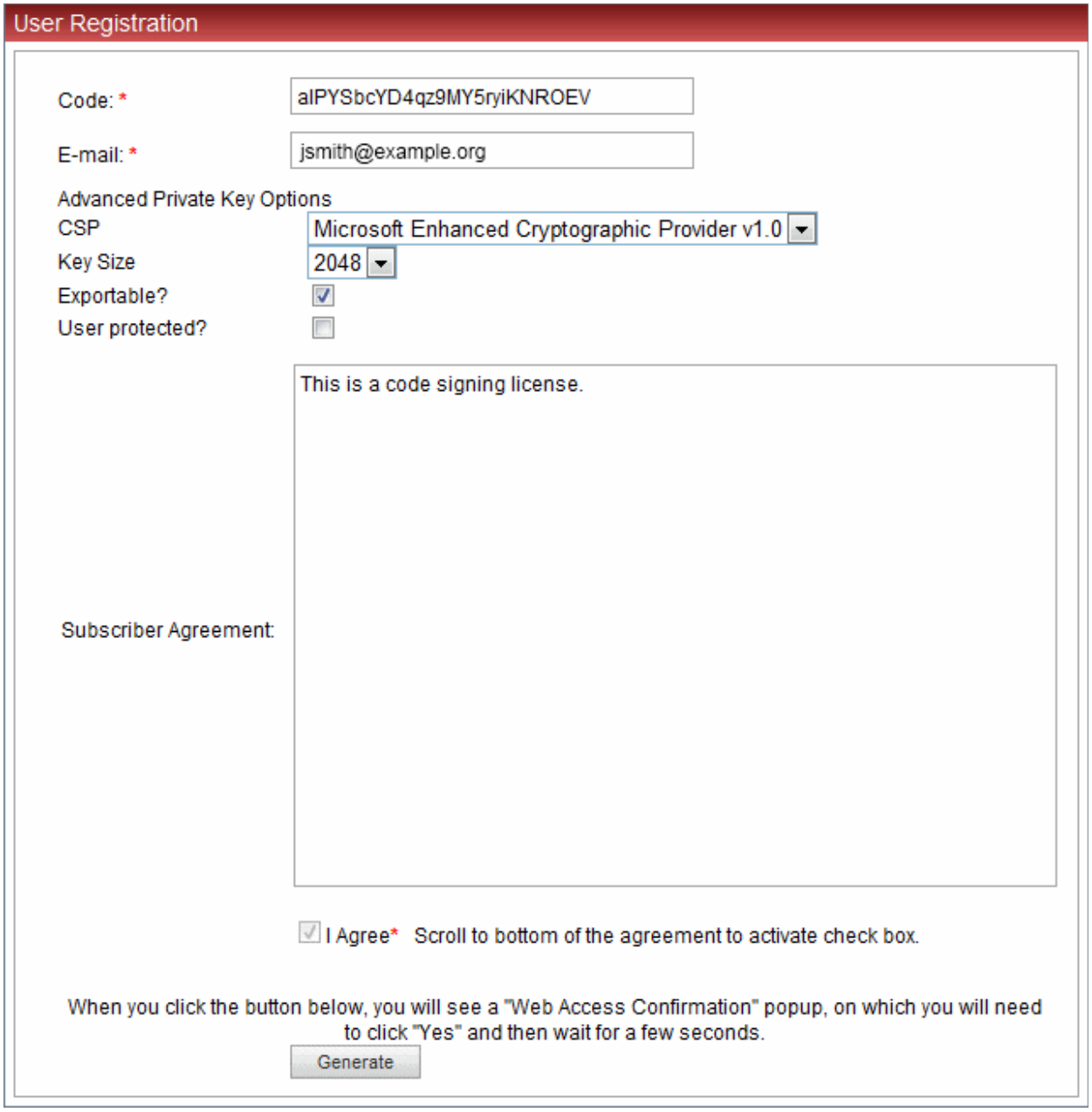
3.3.4.4 Validation of Email address and Requisition

The applicant will receive an invitation email with a link to validate his/her email address. An example is shown below.



Note: It is possible for administrators to modify the contents of these emails in the '**Email Templates**' area under the 'Settings' tab.

Upon clicking the link in the mail, the email address will be validated and the applicant will be taken to user registration page.



Form Parameters

Form Element		Type	Description
Code (***required***)		Text Field	The Code field will be 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 (***required***)		Text Field	The email address of the applicant. This field will be auto-populated.
Advanced Private Key Options	CSP	Drop Down	The applicant can select the cryptographic service provider for the certificate from the drop-down (Default = Microsoft Cryptographic Provider v1.0)
	Key Size	Drop Down	The applicant can select the key size for the private key of the certificate (Default = 2048 bit) Note: The private key is generated locally by the crypto module of the browser/ operating system. The key never leaves the computer and no copy is ever transmitted to the certificate issuer. Comodo 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

Form Element		Type	Description
			private key, during certificate installation process.
	Exportable	Checkbox	The applicant can choose whether or not the certificate is exportable.
	User Protected	Checkbox	If enabled, you will be asked to set password and security levels during the certificate collection process. Windows will prompt you for a password and/or your permission every time you access your certificate to code sign.
Subscriber Agreement (***required***)		Checkbox	Applicant must accept the terms and conditions before submitting the form.
Generate		Control	Starts the certificate generation process.

The applicant needs to fill-in the form, accept to the subscriber agreement by reading it and selecting the checkbox 'I Agree' and click the 'Generate' button. The certificate request will be automatically generated and a request will be sent to CCM.

Info

Your application was accepted, you will be notified by E-mail when your certificate is ready for collection

The certificate status will be set to 'REQUESTED' in the Code Sign Certificates area. CCM will process the request and send a certificate request to Comodo CA Server. The certificate status will be set to 'APPLIED'

3.3.4.5 Downloading and Installing the Certificate

The CCM will collect the certificate from the server and send a notification mail to the applicant with a link to download the certificate. The certificate status will be changed to 'ISSUED' in Code Sign Certificates area. The applicant can follow the link and download the certificate. The certificate status will be changed to 'DOWNLOADED' in CCM. The certificate can be installed by the user and used to digitally sign the executables.

4 Admin Management

4.1 Section Overview

The 'Admin Management' tab allows administrators to create, manage and edit permissions for new and existing administrators. There are 7 types of administrator:

- Master Registration Authority Officer (MRAO)
- Registration Authority Officer (RAO) - SSL
- Registration Authority Officer (RAO) - SMIME
- Registration Authority Officer (RAO) - Code Signing
- Department Registration Authority Officer (DRAO) - SSL
- Department Registration Authority Officer (DRAO) - SMIME
- Department Registration Authority Officer (DRAO) - Code Signing

Administrative Roles:

Master Registration Authority Officer (MRAO)

- The MRAO is the top level administrator and can access all areas and functionality of the CCM interface.
- MRAO admins are visible only to other MRAO Admins in the 'Admin Management' area of the CCM interface.
- The MRAO can delegate control over the certificates, domains and notifications of any Organization or Department.

- The MRAO also has full rights over the creation and privileges of Registration Authority Officers (RAOs), Department Registration Authority Officers (DRAOs) and end-users of any Organization or Department. **Click here for more details**.

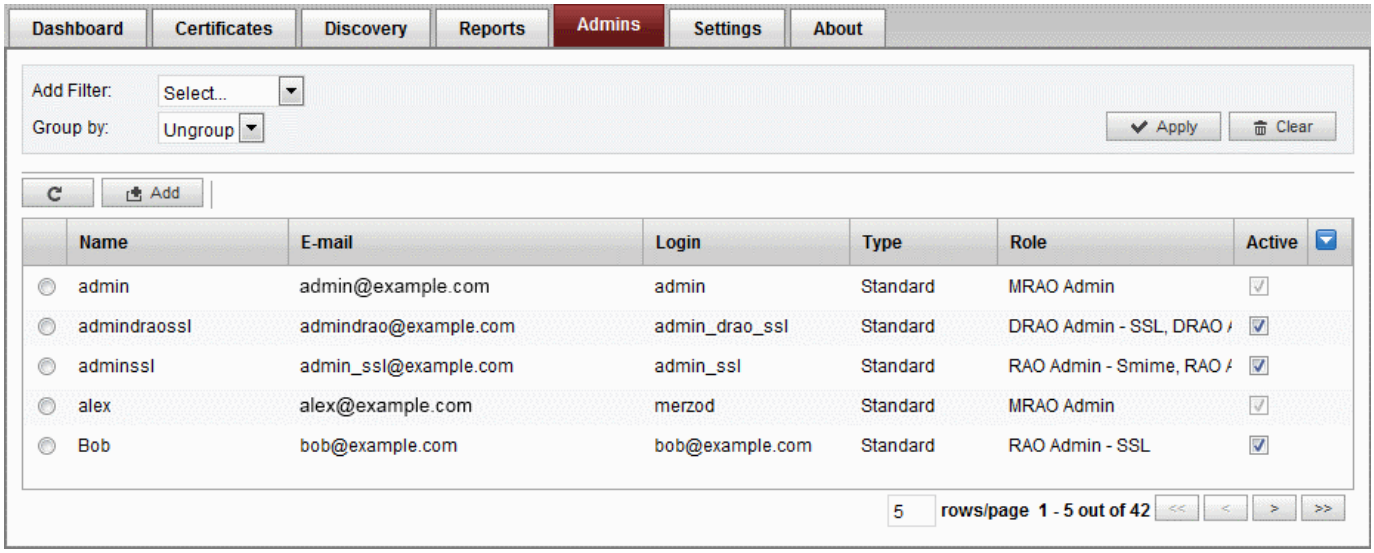
Registration Authority Officer (RAO)

- A Registration Authority Officer (RAO) is an administrative role created by an MRAO or fellow RAO for the purposes of managing the certificates and end-users belonging to one or more CCM Organizations.
- They have control over the certificates that are ordered on behalf of their Organization(s); over Domains that have been delegated to their Organization/Dept by an MRAO; over any Departments of their Organization and over that Organization's end-user membership.
- The RAOs can create Departments and DRAO Administrators within their own Organization, but they should be approved by the MRAO.
- RAO Administrators cannot create a new Organization or edit the General settings of any Organization - even those Organizations to which they have been delegated control. **Click here for more details**.

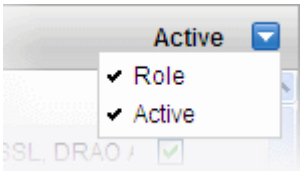
Department Registration Authority Officer (DRAO)

- Department Registration Authority Officers are created by, and subordinate to, the RAO class of Administrator.
- They are assigned control over the certificates, users and domains belonging to a Department(s) of an Organization.
- DRAOs have privileges to access, manage and request certificates for Departments of a Organization that have been delegated to them by a RAO.
- DRAOs have no Admin creation rights. They can edit only self or fellow DRAO administrators of the Department(s) that they administrate.
- DRAOs have visibility of and can request certificates only for the Department(s) that have been delegated to them. They have no access to manage certificates belonging to Organizations or Departments for which they have not been granted permissions. **Click here for more details**.

It is also possible to create an Administrator with more than one Admin privileges. Further details about the privileges and security roles of these administrator types can be found in section **1.2.3. Administrative Roles**. The remainder of this chapter contains detailed explanations of the controls available from the 'Admin Management' tab.



Admin Management Area - Table of Parameters		
Fields	**Values**	**Description**
Name	String	Administrator's full name.
Email	String	Administrator's Email Address (it will be used for client certificate enrollment, notifications)
Login	String	The login username of the administrator.

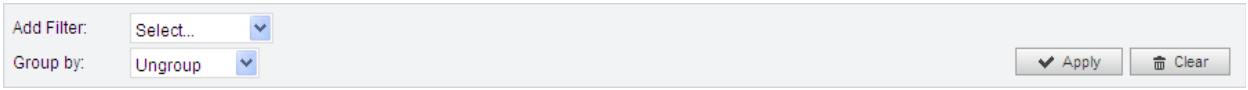
Admin Management Area - Table of Parameters		
Fields	**Values**	**Description**
Type		Shows the type of the administrators
	Standard	Indicates that the administrator is created in CCM
	IdP Template	Indicates that the administrator is added via Identity Provider (IdP) template
	IdP User	Indicates that the administrator is added in CCM and was authenticated by IdP
Role	MRAO Admin	The MRAO is the top level administrator and can access all areas and functionality of the Certificate Manager interface. (**More...**)
	RAO Admin SSL	RAO SSL administrators have privileges to access, manage, request and approve the requests of SSL certificates for Departments/domains belonging to their Organization. (**More...**)
	RAO Admin SMIME	RAO SMIME administrators have privileges to access, manage, request and approve the requests of Client Certificates for Departments/domains that have been delegated to their Organization. (**More...**)
	RAO Admin Code Signing	RAO Code Signing administrators have privileges to access, manage, request and issue the Code signing Certificates for end-users belonging to their Organization. (**More...**)
	DRAO Admin SSL	DRAO SSL administrators have privileges to access, manage and request SSL certificates for Departments of a Organization that have been delegated to them by MRAO or a RAO Admin. **(More...)**
	DRAO Admin SMIME	DRAO SMIME administrators have privileges to access, manage, request Client Certificates for domains that have been delegated to their Department. **(More...)**
	DRAO Admin Code Signing	DRAO Code Signing administrators have privileges to access, manage, request and issue the Code signing Certificates for end-users belonging to their Department. **(More...)**
Active	Checkbox	Indicates whether the administrator is active or not. Also allows the MRAO and delegated RAO admins to switch other admins between active and inactive states according to their privilege levels.
Note: An administrator can enable or disable the column from the drop-down button beside the last item in the column: 		
Control Buttons	Add	Enables MRAO and RAO administrators to add new administrators.
	Refresh	Refreshes the list
Certificate Control Buttons **Note**: The types of certificate control buttons depend on the state of the selected certificate	Edit	Enables MRAO and RAO administrators to modify the details of the selected administrator.
	Delete	Deletes the administrator. ***Note:*** *If an Administrator is deleted, the details of that Administrator can be viewed but they will no longer be editable.*
	View	Enables MRAO admins to view the details of RAO/DRAO added by another RAO, pending approval.

Admin Management Area - Table of Parameters		
Fields	**Values**	**Description**
	Approve	Enables MRAO admins to approve RAO/DRAO added by an RAO. The newly added administrator becomes active only on approval by the MRAO.
	Reject	Enables MRAO admins to reject RAO/DRAO added by an RAO, pending approval.
	Reset Lockout	Enables MRAOs to unlock the login screen that has been locked due to consecutive five wrong attempts to login.

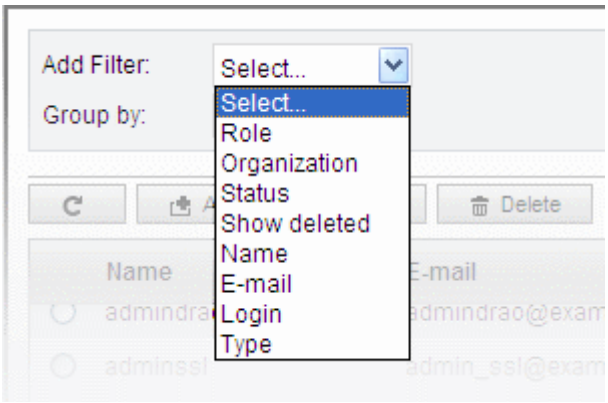
4.1.1 Sorting and Filtering Options

- Clicking on the column header 'Name', 'Email' or Type sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for particular administrator by using filters under the sub-tab:



You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.

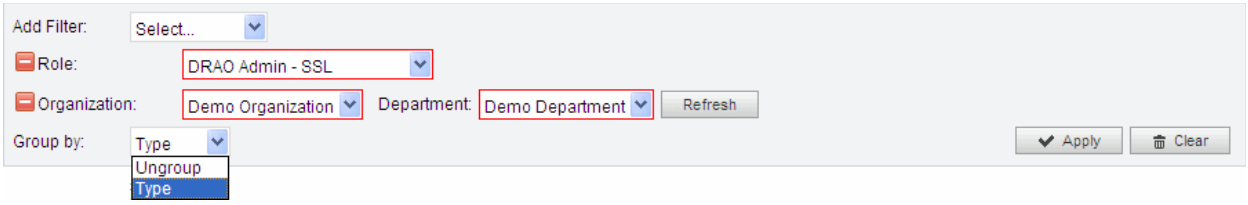


For example if you want to search for DRAO SSL administrators belonging to Demo Organization and Demo Department and group them based on their types:

- Select Role in the 'Add Filter' drop-down
- Select Organization in the 'Add Filter' drop-down

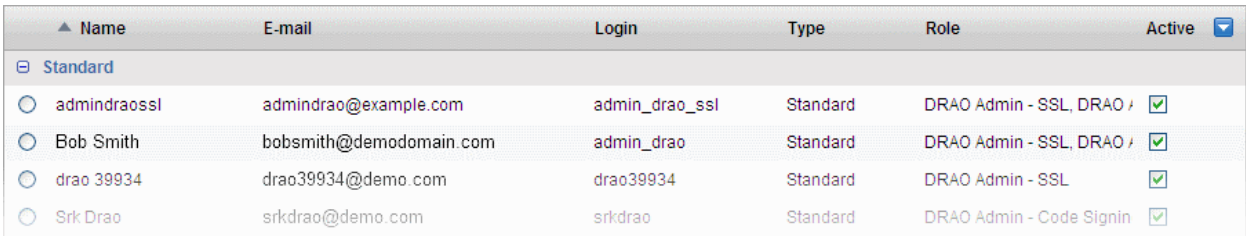
The Organization and Department filters will be displayed.

- Select Demo Organization and Demo Department in the Organization and Department in the drop-downs respectively
- Select 'Type' from the 'Group by' drop-down



- Click the 'Apply' button.

The filtered items based on the entered and selected parameters will be displayed:



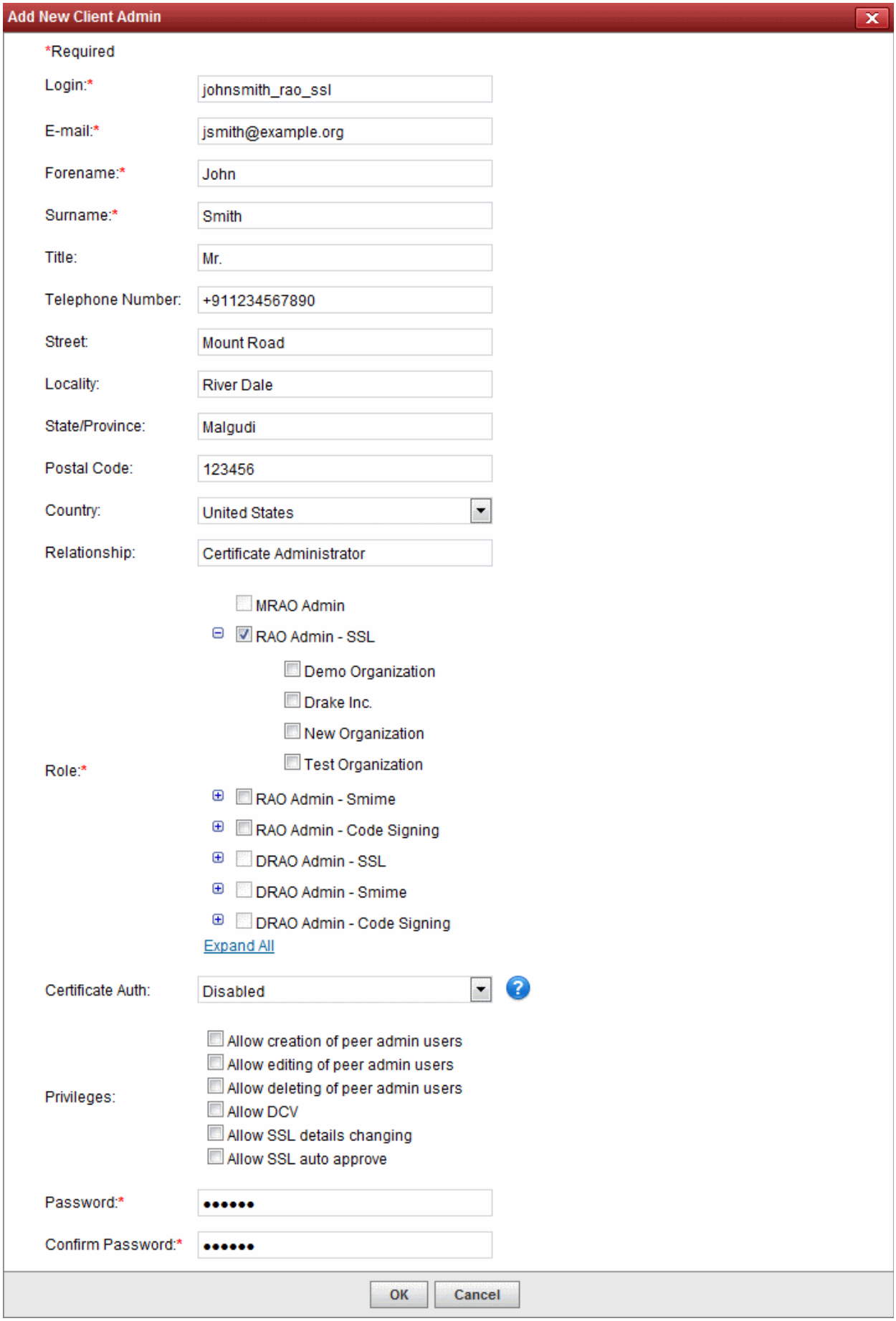
Name	E-mail	Login	Type	Role	Active
Standard					
admindraossl	admindrao@example.com	admin_drao_ssl	Standard	DRAO Admin - SSL, DRAO A	☑
Bob Smith	bobsmith@demodomain.com	admin_drao	Standard	DRAO Admin - SSL, DRAO A	☑
drao 39934	drao39934@demo.com	drao39934	Standard	DRAO Admin - SSL	☑
Srk Drao	srkdrao@demo.com	srkdrao	Standard	DRAO Admin - Code Signin	☑

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Admins' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

4.2 Adding Administrators

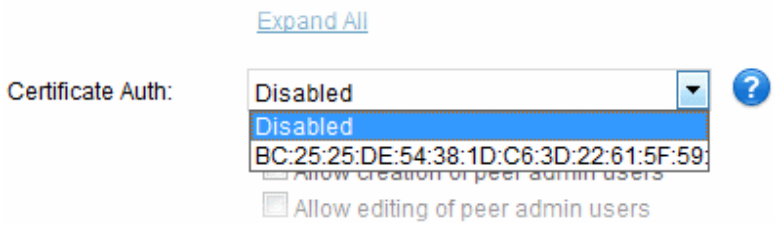
1. Click the 'Admin Management' tab at the top left of the Certificate Manager interface
2. Click the 'Add' button to open the 'Add new Client Admin' form.
3. Complete the 'Add New Client Admin' form.


Add New Client Admin
*Required
Login:*
johnsmith_rao_ssl
E-mail:*
jsmith@example.org
Forename:*
John
Surname:*
Smith
Title:
Mr.
Telephone Number:
+911234567890
Street:
Mount Road
Locality:
River Dale
State/Province:
Malgudi
Postal Code:
123456
Country:
United States
Relationship:
Certificate Administrator
Role:*
MRAO Admin
RAO Admin - SSL
Demo Organization
Drake Inc.
New Organization
Test Organization
RAO Admin - Smime
RAO Admin - Code Signing
DRAO Admin - SSL
DRAO Admin - Smime
DRAO Admin - Code Signing
Expand All
Certificate Auth:
Disabled
Privileges:
Allow creation of peer admin users
Allow editing of peer admin users
Allow deleting of peer admin users
Allow DCV
Allow SSL details changing
Allow SSL auto approve
Password:*
Confirm Password:*
OK
Cancel

4. Click 'OK' to add the administrator to the Certificate Manager.

4.2.1 'Add New Client Admin' form - Table of Parameters

Form Element	Type	Description
Login*	Text Field	Enter login username for the new administrator.
Email *	Text Field	Enter full email address of the new administrator.
Forename*	Text Field	Enter first name of the new administrator.
Surname*	Text Field	Enter surname of the new administrator.
Title	Text Field	Enter the title for the new administrator.
Telephone Number	Text Field	Enter the contact phone number for the new administrator.
Street Locality State/Province Postal Code Country	Text Field Text Field Text Field Text Field Drop-down	Enter the address details of the new administrator.
Relationship	Text Field	The role of the new administrator, for example, RAO SSL Administrator.
Role*	Checkboxes	A new administrator can have one or more of the following roles: • MRAO Admin • RAO Admin SSL • RAO Admin SMIME • RAO Admin Code Signing • DRAO Admin SSL • DRAO Admin SMIME • DRAO Admin Code Signing The new Administrator can be assigned to a particular Organization/Department by selecting the appropriate Organization/Department from the list that appears after selecting a role. 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. Clicking on 'Expand All' expands the tree structure to display all the Departments under each Organization. Clicking on 'Collapse All' in the expanded view collapses the tree structure of all the Organizations and hides the Departments under each Organization.
Certificate Auth	Drop-down	Enables the administrator to specify whether the new administrator must authenticate themselves to Certificate Manager with his/her client certificate over a https: connection prior to being granted login rights. The drop-down is auto-populated with the client certificate(s) issued by CCM for the new administrator, based on his/her email address in the 'Email' field.

Form Element	Type	Description
		 If authentication is needed, the administrator can select the certificate from the drop-down. The new administrator can login to CCM, only if the specified certificate is installed on the computer from which he/she attempts to login. If authentication is not needed, the administrator can select 'Disabled' from the drop-down.
Privileges	Checkboxes	Administrator can assign admin management privileges to the new administrator. The new administrator will be able to add, edit or remove other administrators of their own level or of lower level in the hierarchy, depending on the options selected here. • Allow creation of peer admin users - Enables the new administrator to add new administrators from their management interface. • Allow editing of peer admin users - Enables the new administrator to edit roles of existing administrators from their management interface • Allow deleting of peer admin users - Enables the new administrator to remove existing administrators from their management interface **Note**: The new administrator can create, edit or delete the other administrators of their own tier and administrators of the lower tier. Refer to the descriptions under **Administrative Roles** in the section **4.1 Section Overview** for more details. • Allow domain validation without Dual Approval - The new administrator will be privileged so that the domain creation/delegation approved by the administrator will be activated immediately, without the requirement of approval by a second MRAO. This checkbox will be active only for Administrators with MRAO role. Refer to the section **Domains** for more details. • Allow DCV - Enables the new administrator to initiate Domain Control Validation (DCV) process for newly created domains. The privilege is available only for MRAO and RAO/DRAO SSL Administrators. • Allow SSL Details changing - Enables the new MRAO or RAO/DRAO SSL administrator to change the details of SSL certificates from the Certificates > SSL Certificates interface. • Allow SSL auto approve - The SSL certificates requested by the MRAO administrator is automatically approved and those by RAO/DRAO SSL administrators are automatically approved by the administrator of same level and await approval from higher level administrator. **Note**: 'Allow domain validation without Dual Approval' and 'Allow DCV' fields will only be visible if the features are enabled for your account.
Password*	Text Field	Password to access the Certificate Manager interface.

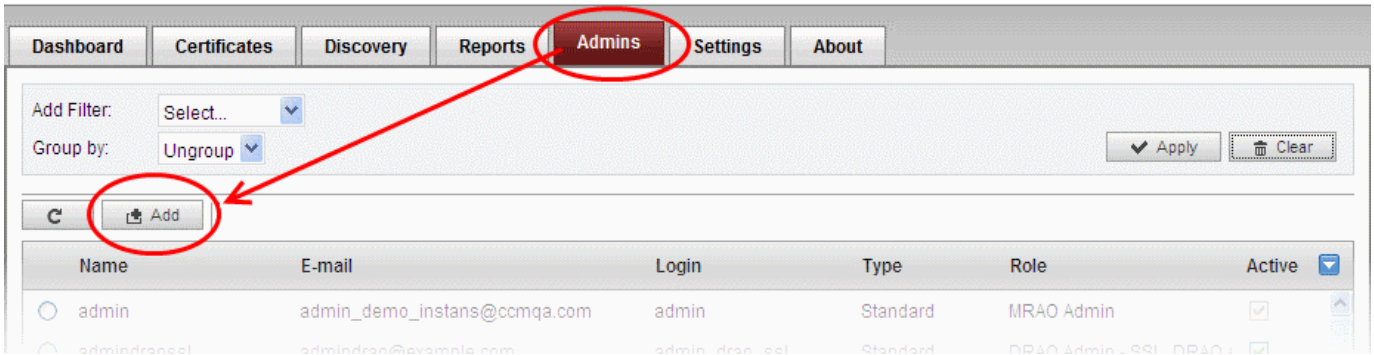
Note: Fields marked with * are mandatory.

Important Note: The administrators created by the MRAOs and RAOs with the Admin Creation Privileges are immediately added to the CCM. But the administrators created by other RAOs will await approval from the MRAO. The new administrators will be added to CCM only if the MRAO approves them by selecting the administrator and clicking the 'Approve' button at the top in the Admin Management area of the CCM interface.

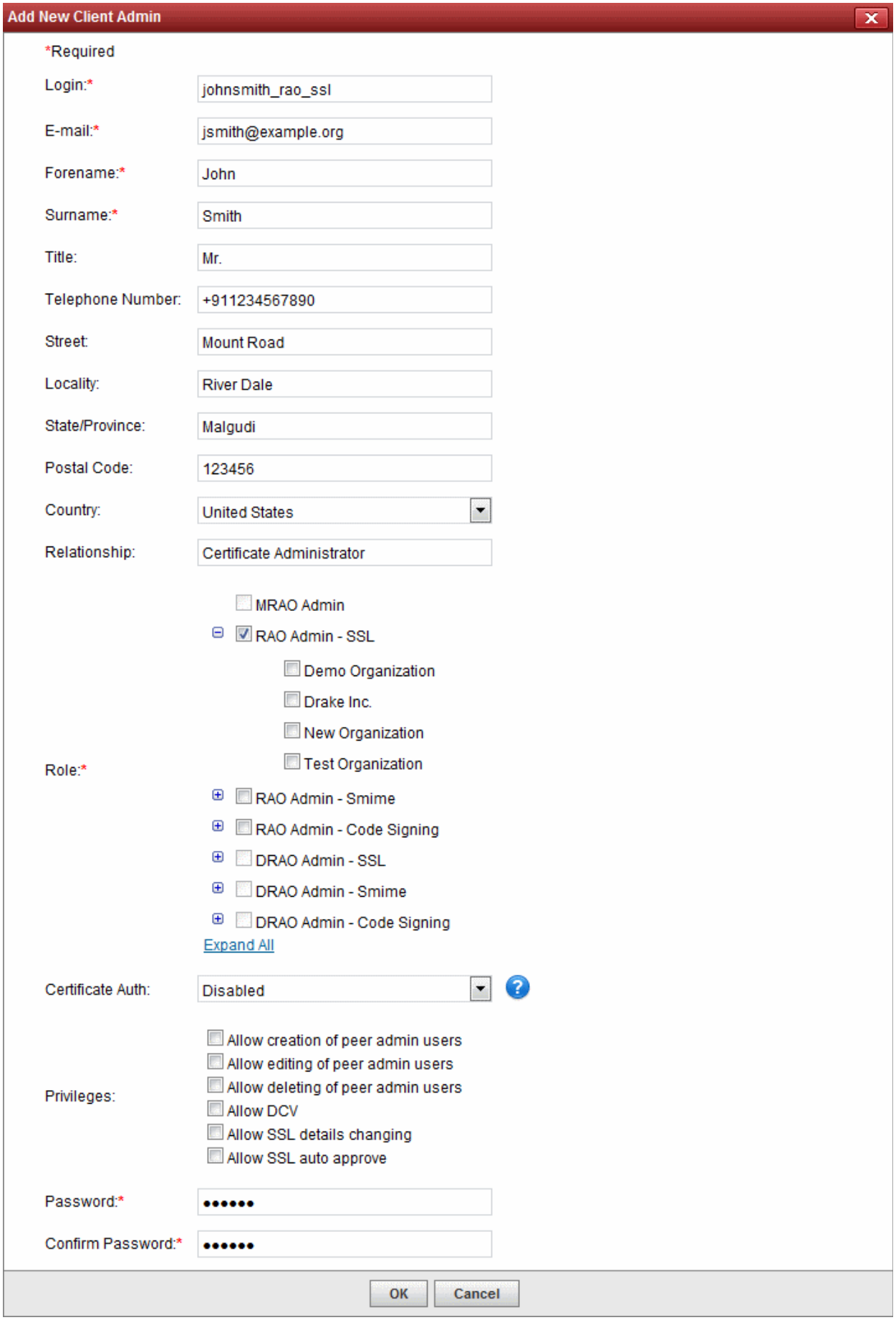
The details of the new administrator created by an MRAO can be modified at any time by selecting the administrator and clicking the 'Edit' button at the top. The details of the new administrator created by an RAO can be edited at any time after the new administrator has been approved by the MRAO.

4.2.2 Example: Adding a New Administrator with multiple privileges

1. Click the 'Admin Management' tab at the top left of the Certificate Manager interface.
2. Click the 'Add' button to open the 'Add new Client Admin' form (as shown below).



3. Complete the 'Add New Client Admin' form.


Add New Client Admin
*Required
Login:*
johnsmith_rao_ssl
E-mail:*
jsmith@example.org
Forename:*
John
Surname:*
Smith
Title:
Mr.
Telephone Number:
+911234567890
Street:
Mount Road
Locality:
River Dale
State/Province:
Malgudi
Postal Code:
123456
Country:
United States
Relationship:
Certificate Administrator
Role:*
MRAO Admin
RAO Admin - SSL
Demo Organization
Drake Inc.
New Organization
Test Organization
RAO Admin - Smime
RAO Admin - Code Signing
DRAO Admin - SSL
DRAO Admin - Smime
DRAO Admin - Code Signing
Expand All
Certificate Auth:
Disabled
Privileges:
Allow creation of peer admin users
Allow editing of peer admin users
Allow deleting of peer admin users
Allow DCV
Allow SSL details changing
Allow SSL auto approve
Password:*
Confirm Password:*
OK
Cancel

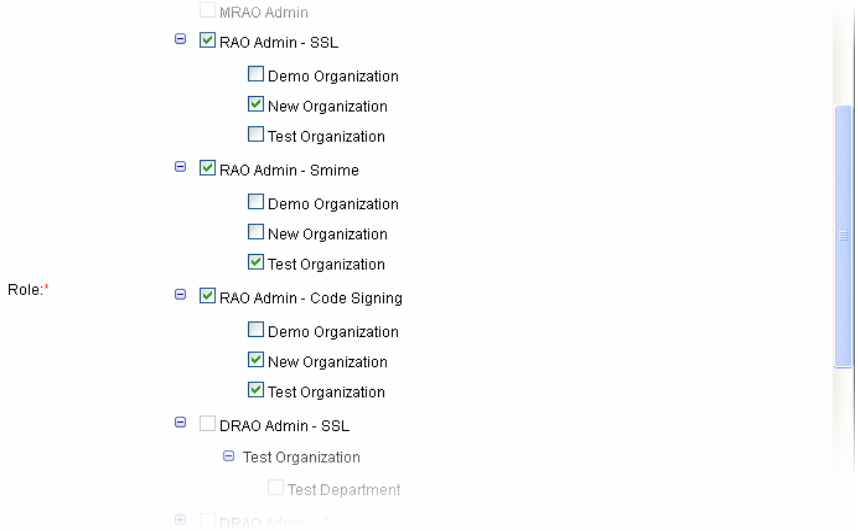
4. Fill out the contact and login details that should apply to the new administrator :
5. Next, you should specify the new administrator's security role:

A new administrator can be:

- MRAO Admin - Will be able to manage ALL certificates for ALL listed Organizations, (this is disables the Organization selection checkboxes.)
- RAO Admin SSL - Will be able to manage ONLY SSL certificates and ONLY for selected Organization(s).
- RAO Admin SMIME - Will be able to manage ONLY client certificates and ONLY for selected Organization(s).
- RAO Admin Code Signing - Will be able to manage ONLY the code signing certificates issued to end-users belonging to the selected Organization(s).
- DRAO Admin SSL - Will be able to manage ONLY SSL certificates and ONLY for selected Departments(s).
- DRAO Admin SMIME - Will be able to manage ONLY client certificates and ONLY for selected Departments(s).
- DRAO Admin Code Signing - Will be able to manage ONLY the code signing certificates issued to end-users belonging to the selected Department(s).

The same RAO can be assigned as RAO SSL, RAO SMIME and RAO Code Signing as required. Similarly, same DRAO can be assigned as RAO SSL, RAO SMIME and RAO Code Signing as required. Further details about the privileges and security roles of these administrator types can be found in section **1.2.3. Administrative Roles**

6. Select the Organization/Department to which the new administrator will have access.



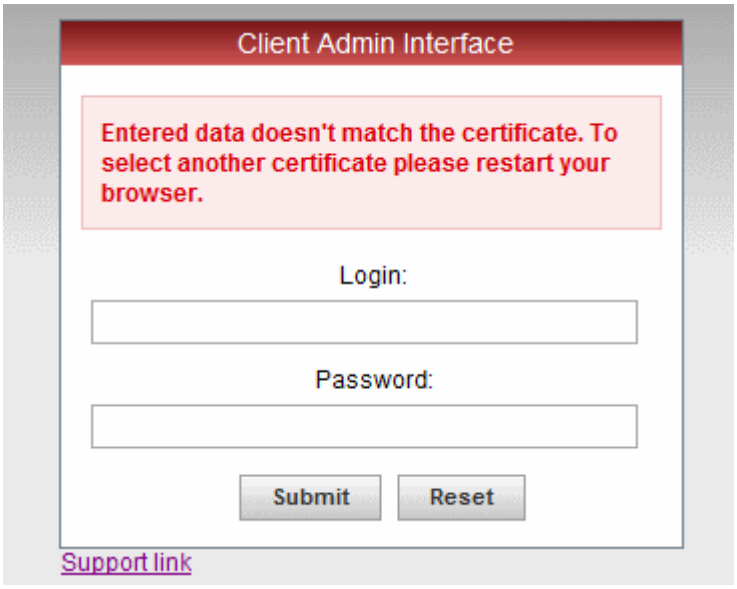
If the single RAO is chosen as RAO SSL, RAO SMIME and/or RAO Code Signing, he or she can have the multiple privileges only for a particular Organization. Similarly, If the single DRAO is chosen as DRAO SSL, DRAO SMIME and/or DRAO Code Signing, he or she can have the multiple privileges only for a particular Department.

7. Set the access password for the new administrator. You can also select the 'Certificate Auth' checkbox.
8. Click 'OK' to save all changes and finish the process.

4.2.2.1 The 'Certificate auth' Field

If enabled, the administrators currently being created will only be able to login to Certificate Manager after authenticating themselves with an certificate. This means, that the Certificate Manager Server will request the certificate specified during creation of the administrator in addition to their login and password details.

If Certificate Manager does not detect the authentication certificate specified during adding an admin, an error will be displayed and the administrator will not be able to login.

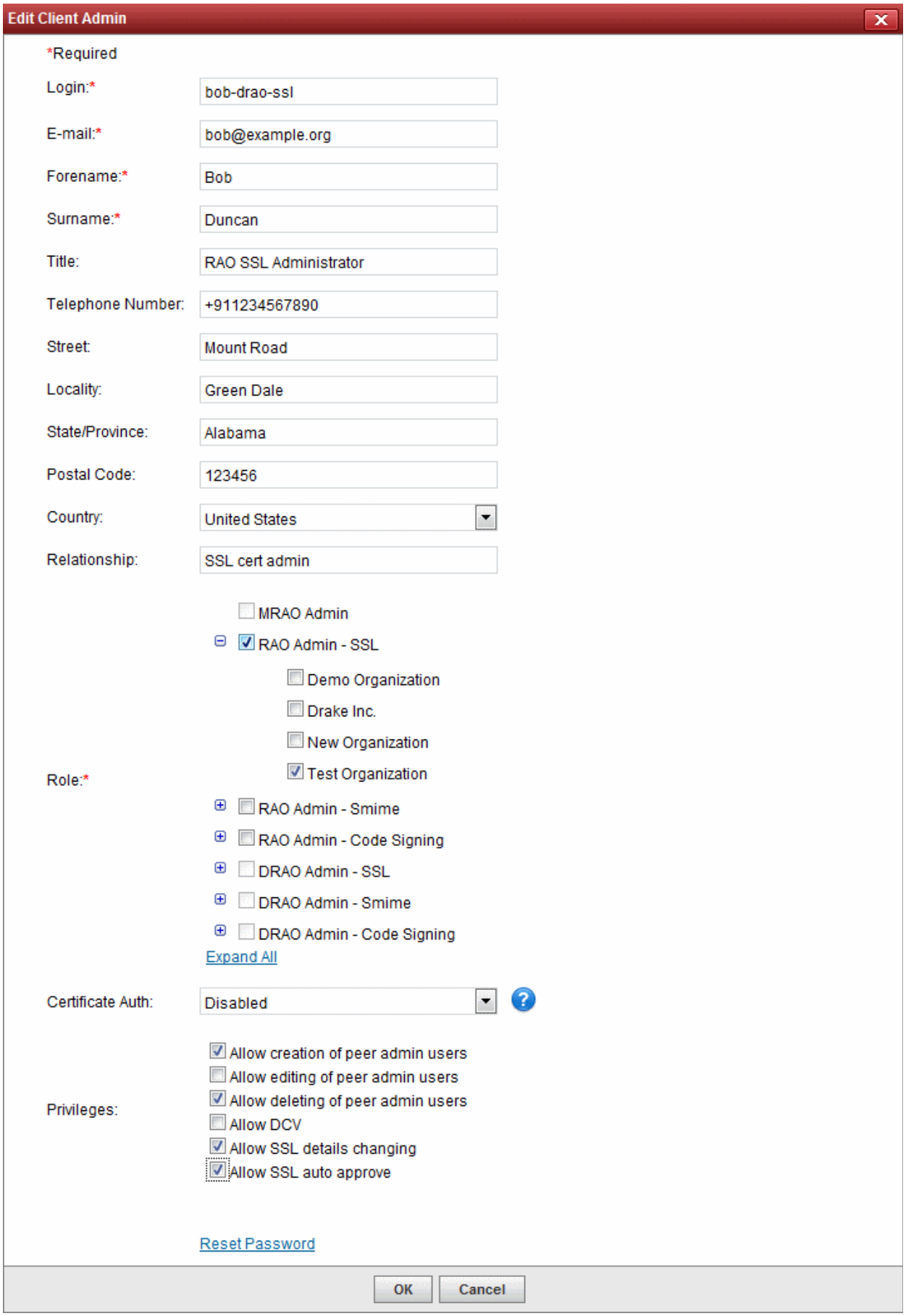


Note: In the event that an administrator has replaced their certificate used for 'Certificate Auth', Certificate Manager needs to re-sync their certificate information. You will need to re-select the appropriate certificate. To do this:

- Open the Admins interface by clicking the 'Admins' tab
- Click 'Edit' button at the top after selecting the radio button next to the administrator's name to re-open the administrator configuration dialog
- Select the new authentication certificate from the 'Certificate Auth' drop down.
- Save by clicking 'OK'.

4.3 Editing Administrators

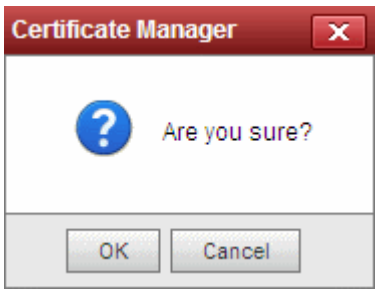
All parameters of any administrator can be modified at any time by selecting the administrator and clicking the 'Edit' button at the top.



Full details of the options available when editing an existing administrator are available in the section '**Add New Client Admin' form - table of parameters**'.

4.4 Deleting an Administrator

Master administrator can delete any administrator by selecting the administrator and clicking the 'Delete' button at the top.



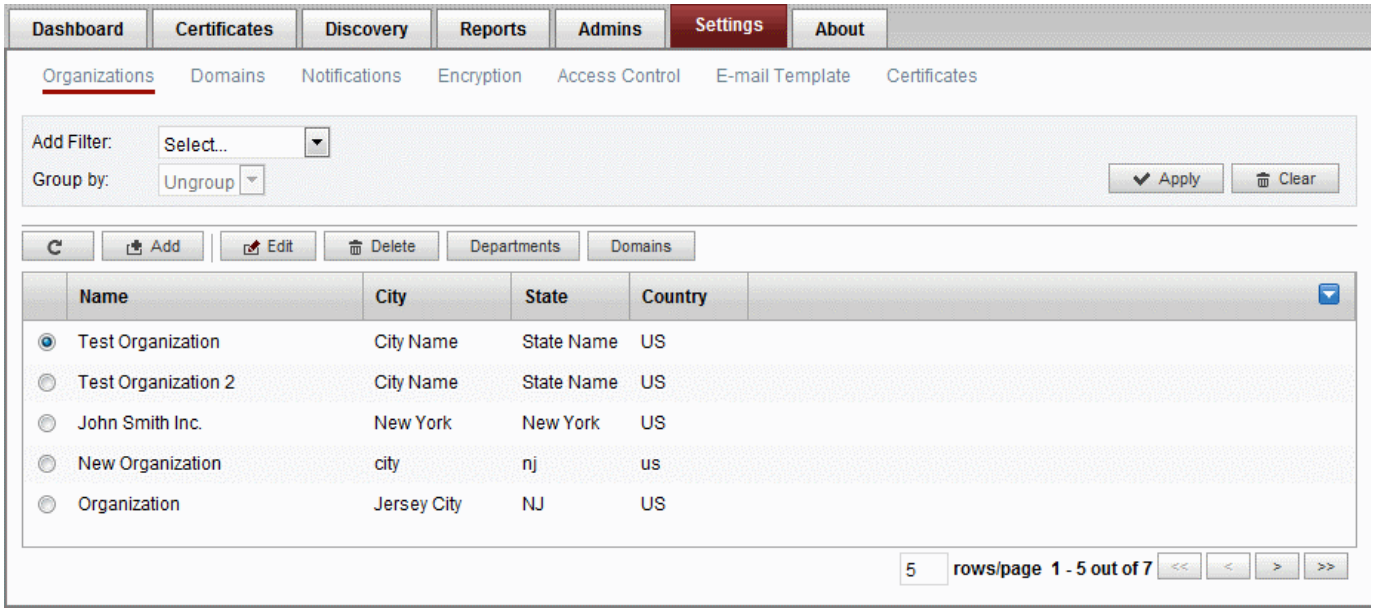
- Click OK to delete the Administrator.

Note: There must always be at least one MRAO Administrator. It is not possible to delete the 'last' Master Administrator.

5 Settings

5.1 Overview

The 'Settings' tab contains a maximum of seven sub-tabs. These tabs are visible selectively depending on the privilege level of the currently logged Administrator.



- **Organizations** - Enables MRAO and RAO administrators to view the list of Organizations, add/edit/delete Organizations and assign Departments and Domains to the Organizations. MRAOs can initiate the process of validating organizations for the purpose of requesting and issuance of OV SSL certificates to organizations and departments under them.
- **Departments** - Enables DRAO administrators to view the list of Departments and assign Domains to the Departments
- **Domains** - Contains a list of all domains that have been created in CCM. This interface allows administrators to add new domains, edit domain details, activate or deactivate a domain, delegate the domain to a particular Organization or Department of an Organization, select the validation type and to filter viewed domains using a range of parameters.
- **Notifications** - Allows administrators to precisely define email notifications to various personnel based on a range of parameters - including notifications triggered by SSL certificate status, notifications triggered by Client Certificate status and notifications triggered by Discovery Scan Summaries.

- **Encryption and Key Escrow** - Overview of key escrow processes.

Note: MRAO and RAO/DRAO SMIME Administrators are strongly advised to familiarize themselves with the information in this section before creating their first Organization or Department. Once key escrow options have been set they cannot be reversed.

- **Access Control** - Enables administrator to grant access only for specified IP range.
- **Email Template** - Allows MRAO and RAO administrators to directly edit the content of the automated notification emails issued by CCM. DRAO administrators can edit templates for their Department via the 'Edit Department' dialog (Settings > Departments > Edit)
- **Certificates** - Enables the MRAO admins to select the types and term lengths of SSL and Client certificates which will be available for new certificate applications through either the Built-in application form or the Self Enrollment form. In addition to the standard fields that appear in the Built-in application form and the Self Enrollment form, MRAO admins can also configure to add additional custom fields in these forms. **Note:** The custom fields can be added only if this feature is enabled for your account. Please contact your Comodo account manager for enabling these feature.

5.2 Organizations

5.2.1 Section Overview

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 and SMIME certificates via the CCM interface.

- Organizations are umbrella entities created by administrators for the purposes of requesting, issuing and managing certificates for domains and employees.
- Organizations can be sub-divided 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 Admins) and Department level administrators (DRAO Admins).
- Organization level administrators can manage any and all certificates, domains and users belonging to their Organization *and* any of its sub-Departments. They are also able to create new Departments and appoint Department administrators.
- Department level administrators can view and manage only those certificates, domains and users belonging to the Department for which they have been delegated responsibility.

Comodo Certificate Manager uses the following naming conventions for Organizations and Administrators:

CCM Entity	Administrator Types
Organization	RAO - SSL Admin RAO - SMIME Admin RAO - Code Signing Admin
Department	DRAO - SSL Admin DRAO - SMIME Admin DRAO - Code Signing Admin
Master Registration Authority Officers (MRAOs) have complete visibility of and control over all Organizations and Departments.	

Although we strongly advise Administrators to plan any Organizational and administrative structure beforehand, it is, of course, possible to rearrange and tweak it later. Organizations, Departments, Domains and Administrators are each created and configured as independent entities in CCM. 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. If you would like further advice on setting up an Organizational structure and administrative chains-of-command then please contact your Comodo account manager. Our representatives have years of experience in PKI management infrastructures and will be pleased to help you find the correct deployment strategy for your company.

5.2.1.1 Example Scenarios

In order to maximize the effectiveness of your CCM implementation, it is important that you first decide the structure of your Organizational and administrative hierarchy. CCM's flexibility allows you to create and delegate hierarchies that are as simple or sophisticated as you require.

The examples listed below are merely workable suggestions for reasonably straightforward situations. Administrators should, of course, follow their own policies when determining how to setup and manage domains between Organizations and Departments. Each example outlines a hypothetical issuance scenario followed by two or three alternative solutions that are possible through CCM:

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
- No Departments
- Delegate all the domain and the sub-domains 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
- No Departments
- Delegate each domain to a separate Organization
- Create three RAO SSL Admins
- Delegate one RAO SSL Admin 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 Admin
- Delegate the RAO SSL to control the Organization (and therefore also its Departments)
- Create three DRAO SSL Admins
- Delegate one DRAO SSL Admin 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 SMIME certificates. Your company operates 2 distinct websites, each with it's own unique first level domain name and two sub-domains.

Solution 1 - Very Simple:

- Create a single Organization
- No Departments
- Delegate both first level domains and all sub-domains to this single Organization
- The MRAO manages all SSL certificates and all SMIME 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 it's sub domains to each of the three Departments in an Organization
- Create one RAO Admin. Assign this single RAO with SSL and SMIME Administrative roles
- Delegate the RAO to control both Organizations (and therefore all Departments, domains and sub-domains)
- Create three DRAO SSL Admins
- Create six DRAO SMIME Admins
- Delegate one DRAO Admin per certificate type to each of the three Departments

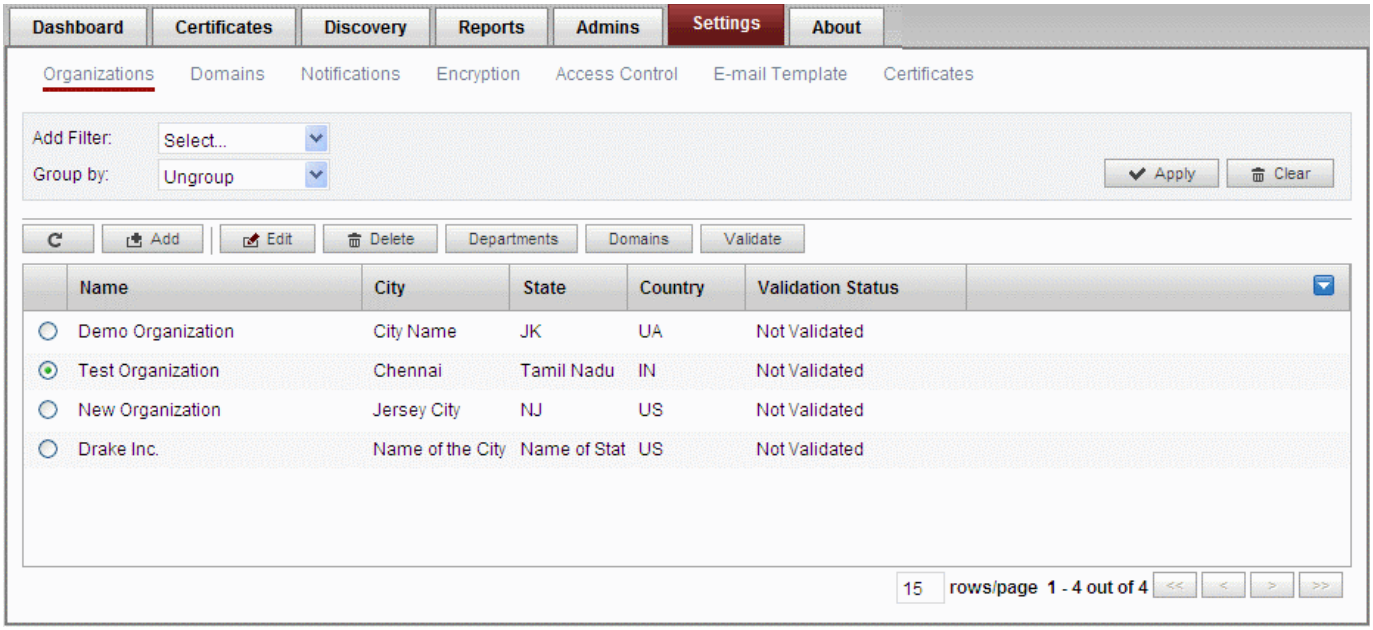
This means that you will have 2 Organizations, each with three Departments. Each of these Departments is associated with a distinct first level domain or sub-domain. Each Department has *two* Departmental Administrators - each responsible for a particular certificate type. All of these Department Administrators (DRAOs) are sub-ordinate to the Organization Admin (RAO) who is, in turn, sub-ordinate 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 SMIME ADMIN 1	http://website_1.com
	Organization 1 - Department 2	DRAO SSL ADMIN 2	http://payments.website_1.com
		DRAO SMIME ADMIN 2	http://payments.website_1.com
	Organization 1 - Department 3	DRAO SSL ADMIN 3	http://mail.website_1.com
		DRAO SMIME ADMIN 3	http://mail.website_1.com
Organization 2	Organization 2 - Department 1	DRAO SSL ADMIN 1	http://website_2.com
		DRAO SMIME ADMIN 4	http://website_2.com
	Organization 2 - Department 2	DRAO SSL ADMIN 2	http://payments.website_2.com
		DRAO SMIME ADMIN 5	http://payments.website_2.com
	Organization 2 - Department 3	DRAO SSL ADMIN 3	http://mail.website_2.com
		DRAO SMIME ADMIN 6	http://mail.website_2.com

5.2.2 Organization Management

5.2.2.1 Organizations Area Overview

Click the 'Organizations' sub-tab of the 'Settings' tab to open the Organization management area. The 'Organizations' tab is not visible to a DRAO (they see the 'Departments' tab instead).



This area :

- Lists all Organizations available to an Administrator as per their privilege level
- Facilitates the creation and deletion of Organizations and Departments
- Facilitates the modification of settings for any existing Organization or Department

- Allows Administrators to delegate Domains to an Organization or Department
- Allows administrators to initiate the organization validation process
- Allows Administrators to search and filter Organizations by Name and Department.

Administrative Roles:

- MRAO Administrators - can see a list of all the Organizations and their Departments in the Organizations area. They 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.
- RAO Administrators - can only see their own Organization(s) in the 'Organizations' area. They cannot create new Organizations but can manage and create Departments for the Organization(s) that has/have been delegated to them.
- DRAO Administrators cannot view the 'Organizations' area. They have visibility only of the 'Departments' tab. They have the rights to manage only the Department(s) that has/have been delegated to them.

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 • Any Department	• Can Manage the Delegated Organization • Can create and manage Subordinate Department(s)	Can manage Delegated Department (s) (via the 'Departments' sub-tab)

5.2.2.2 Summary of Fields and Controls

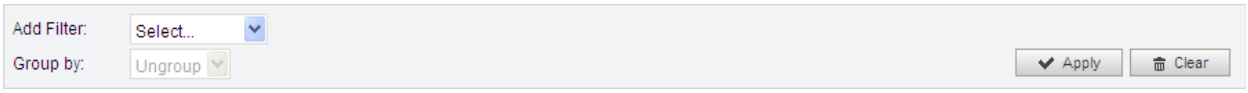
Organizations Area - Table of Parameters		
Fields	**Values**	**Description**
Name	String	Name of the Organization
City	String	Name of the City where the Organization is located
State	String	Name of the State or province
Country	String	Two character country code
Postal Code	Numeric	The postal code or zip code of the city
Validation Status	String	Displays whether the Organization is validated for the request and issuance of OV SSL certificates. For more details refer to the section **Validating an Organization**.
Note: An administrator can enable or disable the columns from the drop-down button beside the last item in the table header: 		
Control Buttons	Add	Enables MRAO Administrators to create a new Organization for the purposes of issuing certificates to end-users and domains. The button is not visible to RAO and DRAO Admins.

Organizations Area - Table of Parameters		
Fields	**Values**	**Description**
	Refresh	Refreshes the list
Organization Control Buttons **Note**: The Organization control buttons appear only on selecting an Organization	Edit	Enables administrators to modify General, Client, SSL and Code Signing Certificate settings pertaining to an existing Organization.
	Delete	Deletes the Organization. The button is not visible to RAO and DRAO Administrators.
	Departments	Enables administrators to view and manage Departments that belong to that Organization.
	Domains	Enables administrators to view, edit and delegate domains to the Organization and the Departments within the Organization.
	Validate	Enables administrators to initiate the organization validation process.

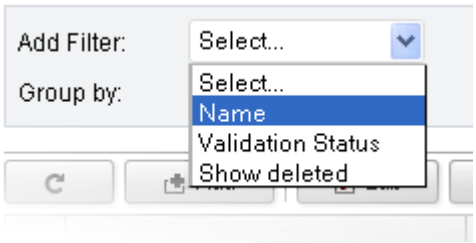
5.2.2.3 Sorting and Filtering Options

- Clicking on the column header 'Name' sorts the items in the alphabetical order of the names of the organizations.

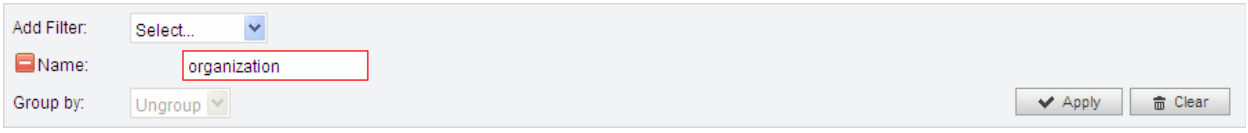
Administrators can search for particular organization by using filters under the sub-tab:



You can add filters by selecting from the options in the 'Add Filter' drop-down. For example, if you want to filter the organization with 'Name':

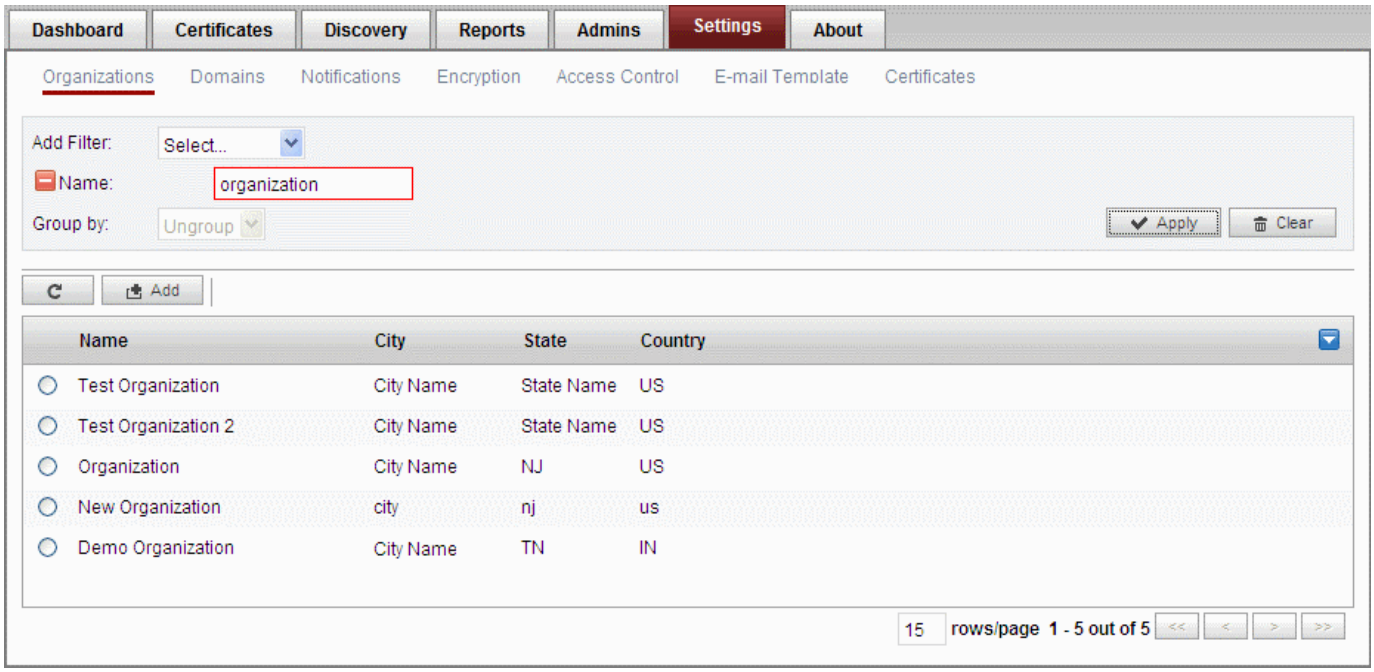


- Enter part or full name in the Name field.



- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed:



- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Organizations' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

5.2.2.4 Creating a New Organization

In order to provide certificates to employees, for websites or for code signing, the MRAO should first create an 'Organization'. Organizations are uniquely identified by combination of the Organization's 'Access Code' and the Common Name specified in 'General' properties. More than one Organization can share either the same Access Code or the same Common Name but no two Organizations can share both.

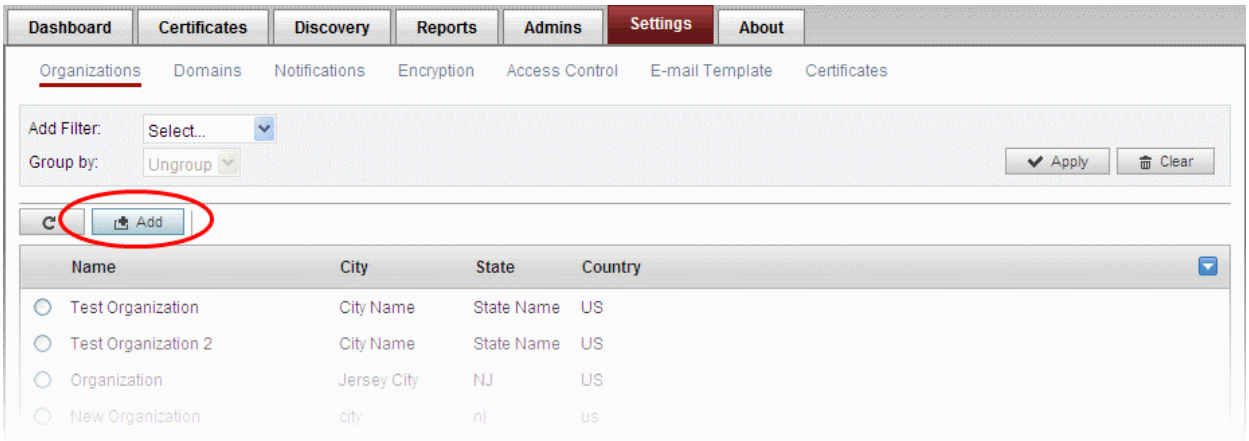
If OV certificates are enabled for the CCM account, the Organizations for which OV certificates are requested, need to be validated by Comodo. For more details on Organization Validation please refer to the section **Validating an Organization**.

Once an Organization is created, an appropriately privileged Administrator can:

- Request SSL certificates using the CCM interface for the domain that is associated with that Organization and can approve or reject certificate requests
- Create multiple Departments within an Organization and associate each Department with a distinct domain(s). (See '**Organizations / Section Overview**' for more details)
- 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. (List of end-users is viewable in the 'Client Certificates' area of 'Certificates Management' section)
- Manage the client certificates of end-users belonging to that Organization via the 'Client Certificates' sub-tab of CCM interface
- Manage SSL certificates for the Organization via the 'SSL certificates' area
- Manage Code Signing certificates for the Organization via the 'Code Signing' area
- Edit the General, Client Certificate and SSL Certificate parameters that apply to that Organization by clicking the 'Edit' button at the top after selecting the checkbox next to its name in the 'Organizations' sub area of 'Settings'
- Utilize the **Certificate Discovery** feature to audit, then monitor all certificates on the network
- Configure a wide range of email notifications for that Organization
- View, filter and export a variety of reports and activity logs for that Organization

The MRAO admin can add a new Organization at any time by clicking the 'Add' button located at the top of the 'Organizations'

area:



This will open the 'Add New Organization' dialog.

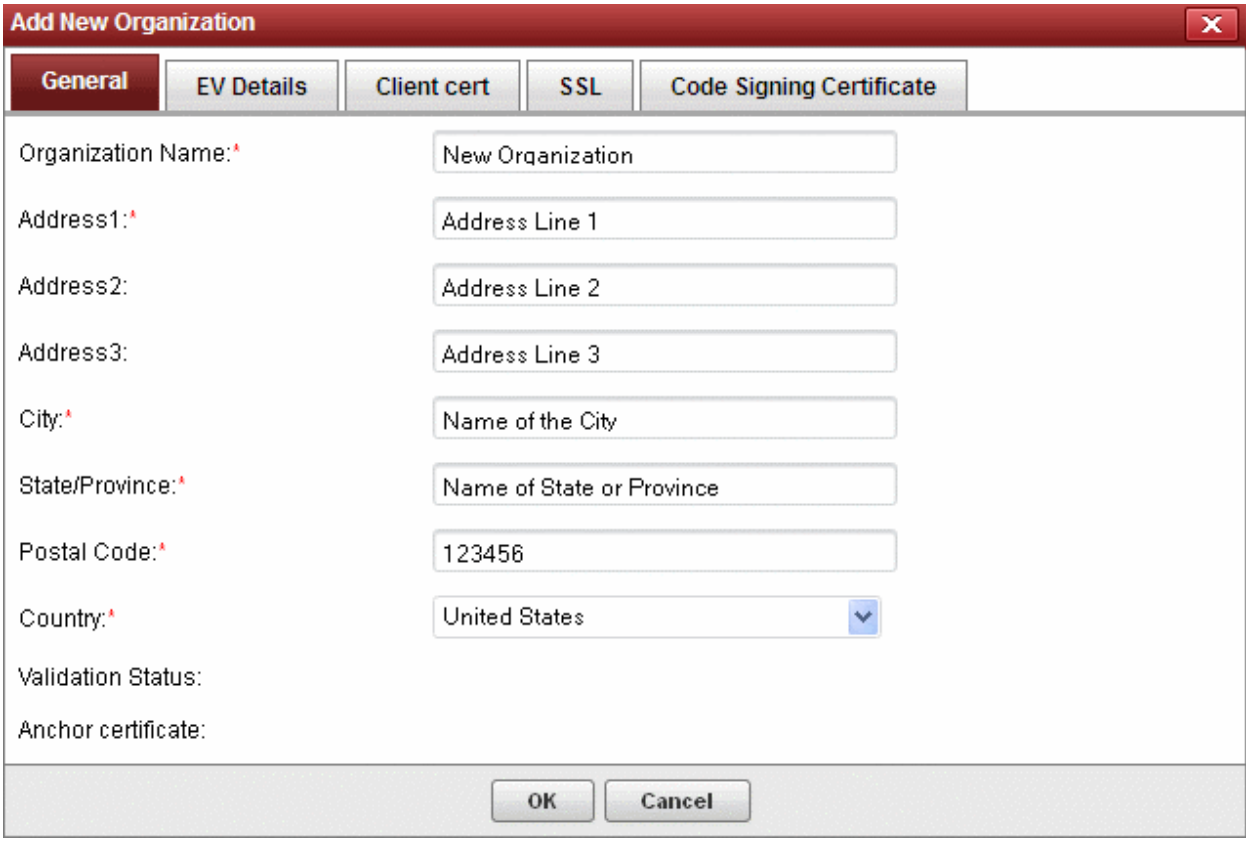
The dialog contains five tabs:

- **General**
- **EV Details**
- **Client Cert**
- **SSL**
- **Code Signing**

The next five sections of this guide will explain these tabs in more detail.

5.2.2.4.1 General Settings

'General' settings allows the MRAO to configure high level details relating to the new Organization:



- The 'Organization Name' and 'Address' information specified for an Organization will be used to populate the 'Subject' field of any SSL certificates requested and issued for this Organization.
- It is important that Administrators make sure that the details above match those used when generating their CSR.
- Fields marked with '*' are mandatory and an Organization cannot be created without filling them out.
- 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 Organization Validated SSL certificates for Organizations and Departments under them your CCM should have been enabled for OV certificates and the Organization should be validated by Comodo. The validation process for newly created organizations can be initiated by MRAOs and when the process is completed successfully, the Validation Status will display as Validated. The Anchor Certificate will display as ON and this will be used for OV reference by CCM whenever an Organization Validated SSL certificate is requested for an Organization or Departments under it.

  The various stages of validation status are:

  Not Validated - The validation process not started.
  Validated - The organization is validated and anchor certificate issued.
  Pending - Validation process started and not completed.
  Failed - The validation process failed for the organization.
  Expired - The validation period of 36 months is expired for the organization.

  For more details on Organization Validation, refer to the section **Validating an Organization**.
- Client and SSL certificates may only be automatically issued to common names of domains (and sub-domains) delegated to the Organization which Comodo CA has pre-validated that you have the right to use. If you apply for certificates on a new domain, then Comodo CA will first need to validate your ownership of the domain before the certificate can be issued for it. See **Delegating Domains to Organizations** for more details.
- For more details on these fields, see '**General Settings' - table of parameters**'
- For background information on Organizations and Departments, see '**Organizations / Section Overview**'

5.2.2.4.2 General Settings - Table of Parameters

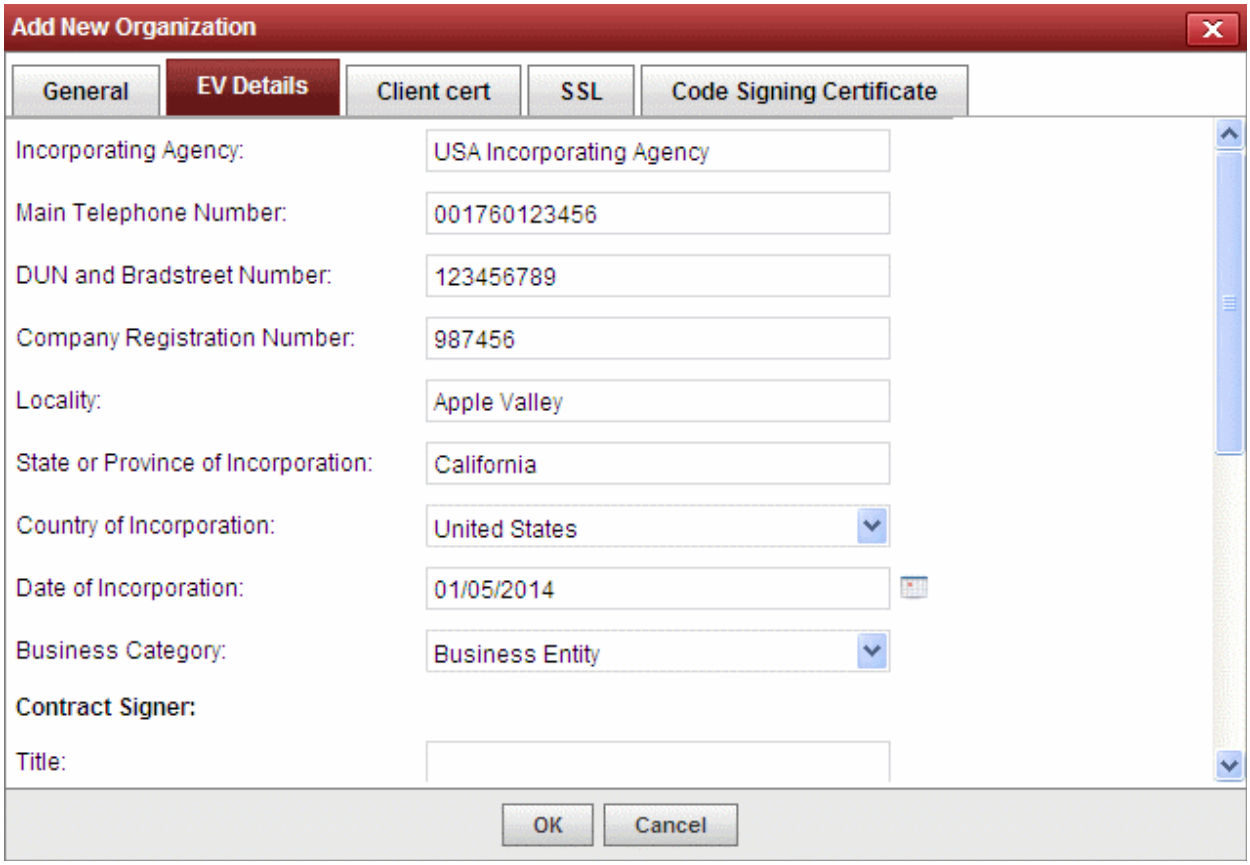
Field Name	Values	Description
Organization Name	*Textbox* ***(required)***	The name of the Organization to be created.
Address 1	*Textbox* ***(required)***	Organization's address (used for issuing SSL and SMIME certificates)
Address 2	*Textbox*	Organization's address (used for issuing SSL and SMIME certificates)
Address 3	*Textbox*	Organization's address (used for issuing SSL and SMIME certificates)
City	*Textbox* ***(required)***	City where the Organization is located (used for issuing SSL and SMIME certificates)
State/Province	*Textbox* ***(required)***	State or province (used for issuing SSL and SMIME certificates)
Postal Code	*Textbox* ***(required)***	Postal code (used for issuing SSL and SMIME certificates)
Country	*Textbox* ***(required)***	Two characters country code (used for issuing SSL and SMIME certificates)
Validation Status		Indicates the progress of organizational validation (OV) on the CCM 'Organization' in question. States can be 'Not validated', 'Validated', 'Pending', 'Failed', 'Expired'. The Validation Status will be displayed only if OV certificates are enabled for the CCM account.
Anchor Certificate		Issued after the organization validation is completed. Indicates the status of Anchor certificate. This is used as a reference for organization validation status by CCM whenever an Organization Validated SSL certificate is requested for an Organization or Departments under it.

Field Name	Values	Description
		The Anchor Certificate field will be displayed only if OV certificates are enabled for the CCM account.

5.2.2.4.3 EV Details Tab

The EV Details tab 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 / or departments under it. The details provided in these fields will be auto populated in the EV SSL certificate request form. The administrator can also leave these fields blank and the details will be fetched from the EV SSL certificate request form and automatically filled when the request is submitted.

Note: The EV details tab is displayed only if Extended Validation Registration Authority (EVRA) feature is enabled for your CCM account. Contact your CCM account manager for enabling this feature.



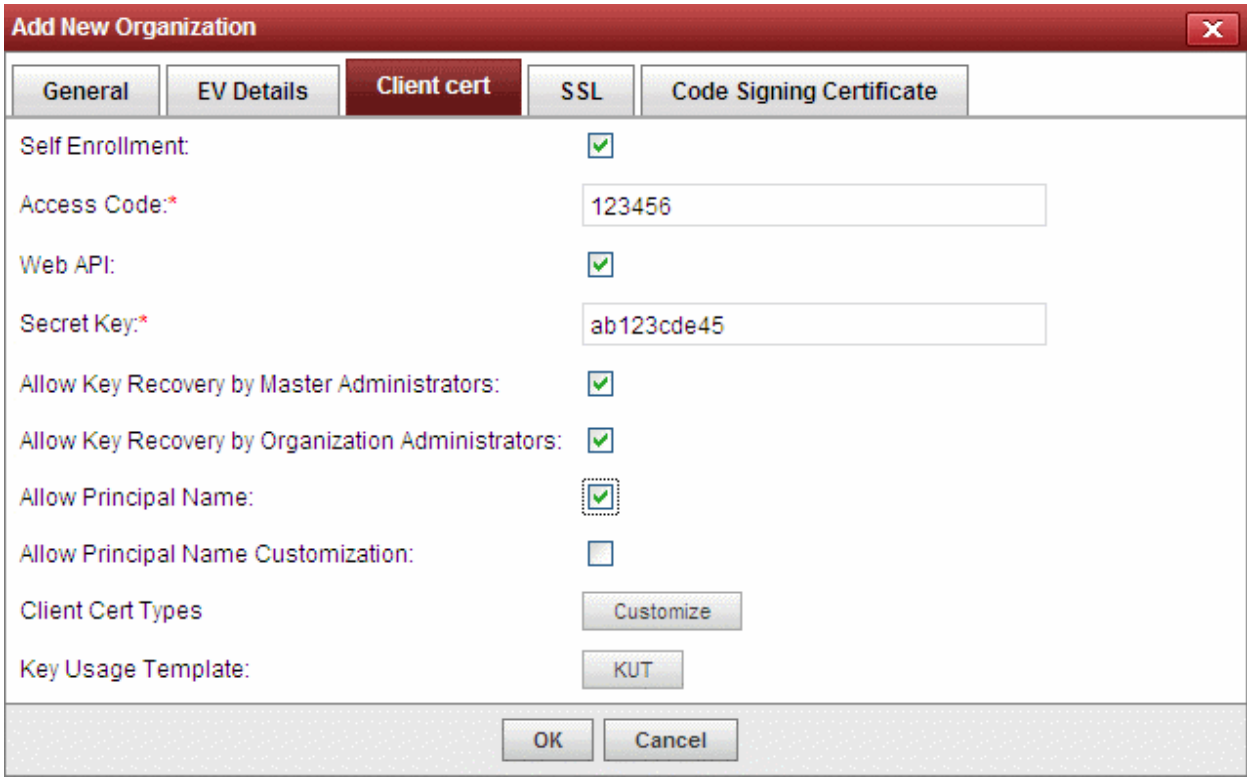
5.2.2.4.4 EV Details - Table of Parameters

Field Name	Type	Description
Incorporating Agency	Textbox	Name of the Incorporating Agency in whose records the name of the organization exists as a legal entity.
Main Telephone Number	Textbox	The primary telephone number of the Incorporating Agency.
DUN and Bradstreet Number	Textbox	The nine digit number issued by D&B to the organization.
Company Registration Number	Textbox	The registration number issued to the organization.

Field Name	Type	Description
Locality	Textbox	The locality where the organization is established.
State or Province of Incorporation	Textbox	The State or Province where the organization is located.
Country of Incorporation	Drop-downs	The country where the organization is established.
Date of Incorporation	Selection	The date on which the organization was registered.
Business Category	Drop-down	The business category of the organization. The options are: • Private Organization • Government Entity • Business Entity • Non-Commercial Entity
Contract Signer - The person representing the organization that has signed the EV SSL contract with Comodo.		
Title	Textbox	Title of the contract signer
Forename	Textbox	First name of the contract signer
Surname	Textbox	Last name of the contract signer
Email	Textbox	Email address of the contract signer
Telephone	Textbox	Primary telephone number of the contract signer
Street	Textbox	Name of the street where the contract signer is located.
Locality	Textbox	Name of the locality where the contract signer is located.
State/Province	Textbox	Name of the state or province where the contract signer is located.
Postal Code	Textbox	Postal code of the area where the contract signer is located.
Country	Drop-downs	Name of the country where the contract signer is located.
Relationship	Textbox	The relationship of the contract signer with the organization.

5.2.2.4.5 Client Cert Settings Tab

The Client Cert tab allows appropriately privileged administrators to configure enrollment and term settings relating to SMIME (email and client) certificates issued to end-users. The settings chosen in this section relate only to those client certificates issued to the domain associated with the currently selected Organization.



5.2.2.4.6 Client Cert Settings - Table of Parameters

Field Name	Type	Description
Self Enrollment	Checkbox Default state - not checked	Checking this box will allow the end-users that belong to the Organization to apply for a personal certificate using the enrollment form hosted (by default) at: https://CCM/customer/customer_uri/smime. The Administrator can communicate the self-enrollment URL 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 will also be automatically created as a new 'End-User' in this Organization/Department if they do not already exist. (List of end-users is viewable in the 'Client Certificates' area of 'Certificates Management' section). • It is possible for Certificate Manager Account holders to use their own custom form templates rather than the default form supplied by Comodo. See your account manager for more details on enabling this functionality.
Access Code (Appears only if the 'Self Enrollment' checkbox is selected)	Textbox (required)	An Access Code identifies a particular 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 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.

Field Name	Type	Description
		Administrators should choose a complex Access Code containing a mixture of alpha and numeric characters that cannot easily be guessed. This code should be conveyed to the applicant(s) along with the URL of the sign up form. Applicants that request a certificate using the Self Enrollment Form will need to enter this code.
Web API	Checkbox Default state - not checked	• Checking this box allows applicants to enroll for certificates through the Web Service API. This requires special agreement with Comodo CA. For detailed instructions please refer to Web API documentation.
Secret Key (Appears only if the 'Web API' checkbox is selected)	String	Secret key is a phrase that is unique for all Organizations. This phrase restricts access for enrolling certificates for that Organization. • Used in pair with 'Organization ID' (visible only for already created Organizations).
Allow Key Recovery by Master Administrators	Checkbox Default state - checked	If selected, the MRAO will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the MRAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificate UNTIL the MRAO has initialized their master key pair in the **Encryption** tab. See '**Encryption and Key Escrow**' for a more complete explanation of key recovery processes.
Allow Key Recovery by Organization Administrators	Checkbox Default state - checked	If selected, the RAO will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the RAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificate UNTIL the RAO has initialized their master key pair in the **Encryption** tab. See '**Encryption and Key Escrow**' for a more complete explanation of key recovery processes.
Allow Principal Name	Checkbox Default state - not checked	Checking this box enables Principal Name support to the Organization. If enabled, the client certificates issued to the end-users of the Organization will include an additional name - Principal Name, in addition to the RFC822 name in the Subject Alternative Name(SAN) field. If included, the Principal Name will be 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/Department.
Allow Principal Name Customization	Checkbox Activated only on selecting 'Allow Principal Name' checkbox	Checking this box enables customization of the Principal Names by the Administrator.
Client Cert Types	Button 'customize'	The Client Cert types customization options allow the administrator to specify the Client Certificate types and term lengths that will be available for this Organization through the Self Enrollment Forms. Refer to the section **Customize an Organization's Client Certificate** Types for more details. • Clicking the 'customize' button will open the 'Bind Client Cert Types' interface. • All choices made in the 'Bind Client Cert Types' interface will apply only to this specific Organization. • The more powerful '**Client Cert Types**' area contains a very similar interface that allows MRAO Administrators to determine universal

Field Name	Type	Description
		certificate type and term lengths that apply to ALL Organizations • If a particular certificate type or term is not visible in the 'Bind Client Cert Types' area then it may need enabling in the '**Client Cert Types**' area.
Key Usage Template	Button 'KUT'	The Key Usage Template (KUT) options allow administrators to specify the scope of key usage in client certificates at an Organization and/or Departmental level. It is possible for a key to be capable of (1) Digitally signing (2) Encrypting (3) Both signing and encrypting. Please refer to the section 'Defining Key Usage Template for an Organization's Client Certificates' for more details. • Clicking the 'KUT' button will open the '**Key Usage Template**' interface. From here you will be able to specify the usage scope of the keys of a particular organization. • The KUT defined through the 'Key Usage Template' interface will apply only to this specific Organization. **Important Note:** The Key Usage Template (KUT) feature will not be available by default. If required, the MRAO Administrator can contact Comodo and request for it. The KUT button will be visible to the MRAO Administrators only if it is enabled by Comodo.

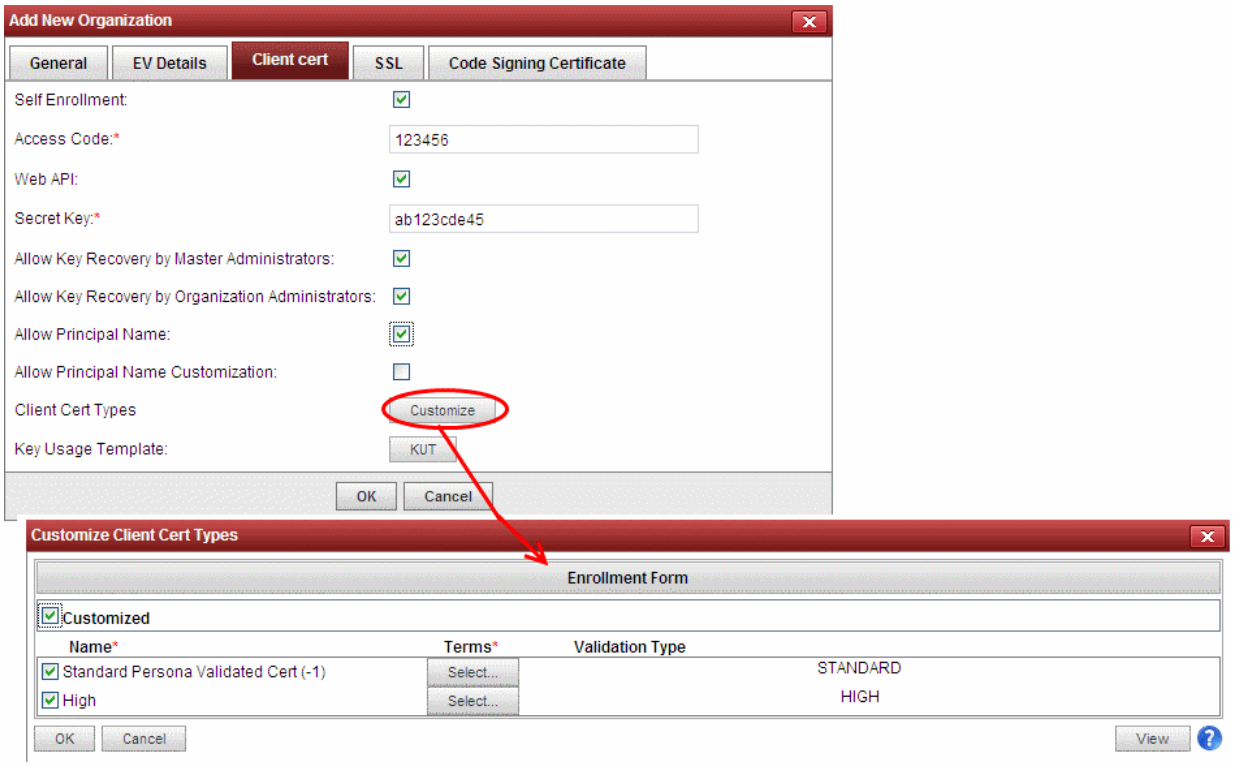
5.2.2.4.6.1 Customize an Organization's Client Certificate Types

Security Roles:

- MRAO - can customize client certificate type availability for all Organizations and Departments
- RAO SMIME - can customize client certificate type availability only for the Organizations and Departments belonging to the Organizations that are delegated to them.
- DRAO SMIME - cannot customize client certificate type availability.

The types and term lengths of client certificates that are available to any particular Organization can be customized using the 'Bind Client Cert Types' interface. Creating a targeted 'certificate roster' simplifies the certificate selection procedure at the application forms and helps avoid applications for certificates which are inappropriate for that Organization.

To access the 'Customize Client Cert Types' interface, click the 'Customize' button under the 'Client Cert' tab of the Add New/Edit Organization interface:



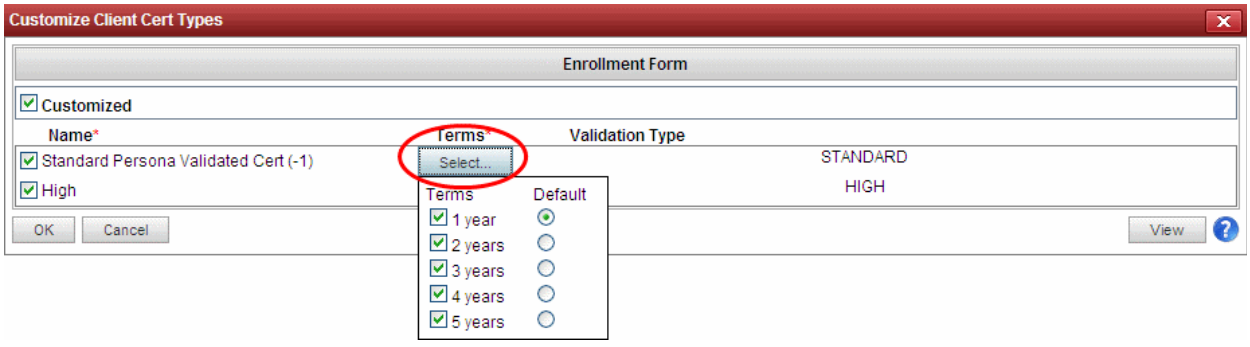
This will open the 'Customize Client Cert Types' interface for that Organization, that enables to restrict the Client Cert types that will be available to applicants using the **Self Enrollment Form** for that Organization.

By default, the 'Customized' option is left unchecked so that all the certificate types are available through the self enrollment forms (both Access Code and Secret ID based application forms).

Prior to customization, MRAO Administrators can also view the Client Cert Type customization as imposed by the RAO Administrator of an Organization and can modify the same. Refer to **Viewing Pre-imposed Client Certificate Type Customization for an Organization** for more details.

To restrict the Client Cert types and their term lengths:

1. Select the 'Customized' checkbox.
2. Check the names of the certificates you wish to be available for the Organization leave the others unchecked.
3. Click the 'Select' button next to the certificate name to choose which terms will be available. If you want to set the selected term as default term for the selected certificate type, select Default radio button.



4. Select the Validation type from the drop-down.

The two options available are 'Standard' and 'High' validation types.

'Standard' certificates can be issued quickly and take advantage of the user authentication mechanisms that are built into CCM.

A user applying for a 'Standard Personal Validation' certificate is authenticated using the following criteria:

- User must apply for a certificate from an email address @ a domain that has been delegated to the issuing Organization
- The Organization has been independently validated by an web-trust accredited Certificate Authority as the owner of that domain
- 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 the administrator to the user via out-of-band communication.
- 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 will contain a validation code that the user will need to enter at the certificate collection web page.
- 'High Personal Validation' certificates require that the user undergo the validation steps listed above AND
- Face-to-Face meeting with the issuing Organization

Note: The additional validation steps must be completed PRIOR to the administrator selecting 'High Personal Validation' type.

5. Click 'OK'.

The administrator needs to log out then back in again for the customization options to take effect.

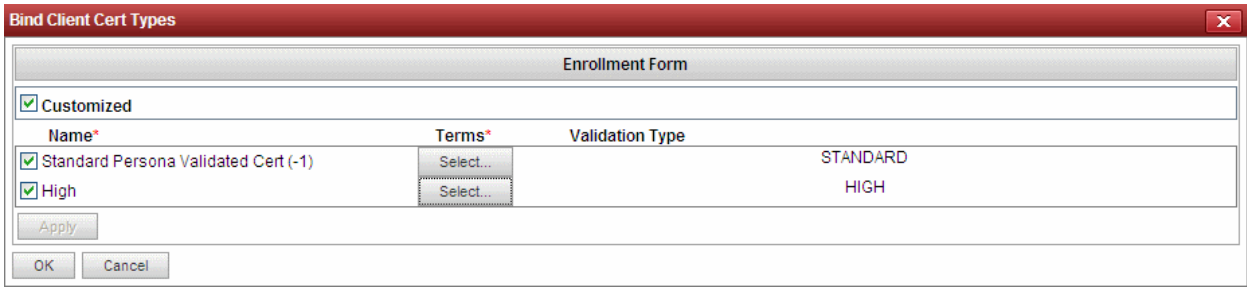
Only the types and terms of client certificates that are selected in the 'Bind Client Cert Types' interface will now be available in the 'Type' drop-down field of the Self Enrollment form.

Viewing Pre-imposed Client Certificate Type Customization for an Organization

While editing an existing Organization, MRAO Administrators can view the Client Cert Type customization imposed by the RAO Administrator of the Organization, before imposing his/her own customization, by clicking the 'View' button at the bottom right of the 'Bind Client Cert Types' interface.

Note: The 'View' button will be active only when the 'Customized' checkbox is not selected in the 'Customize Client Cert Types' interface.

Clicking the 'View' button will display the 'Bind Client Cert Types' dialog as displayed to the RAO Administrator of the respective Organization.



This interface also allows the MRAO Administrator to modify the customization of client certificate type availability for the Organization by the RAO Administrator.

Notes:

- All choices made in the 'Bind Client Cert Types' interface will apply only to this specific Organization.
- The more powerful '**Client Cert Types**' area contains a very similar interface that allows MRAO to determine universal certificate type and term lengths that apply to ALL Organizations.

5.2.2.4.6.2 Defining Key Usage Template for an Organization's Client Certificates

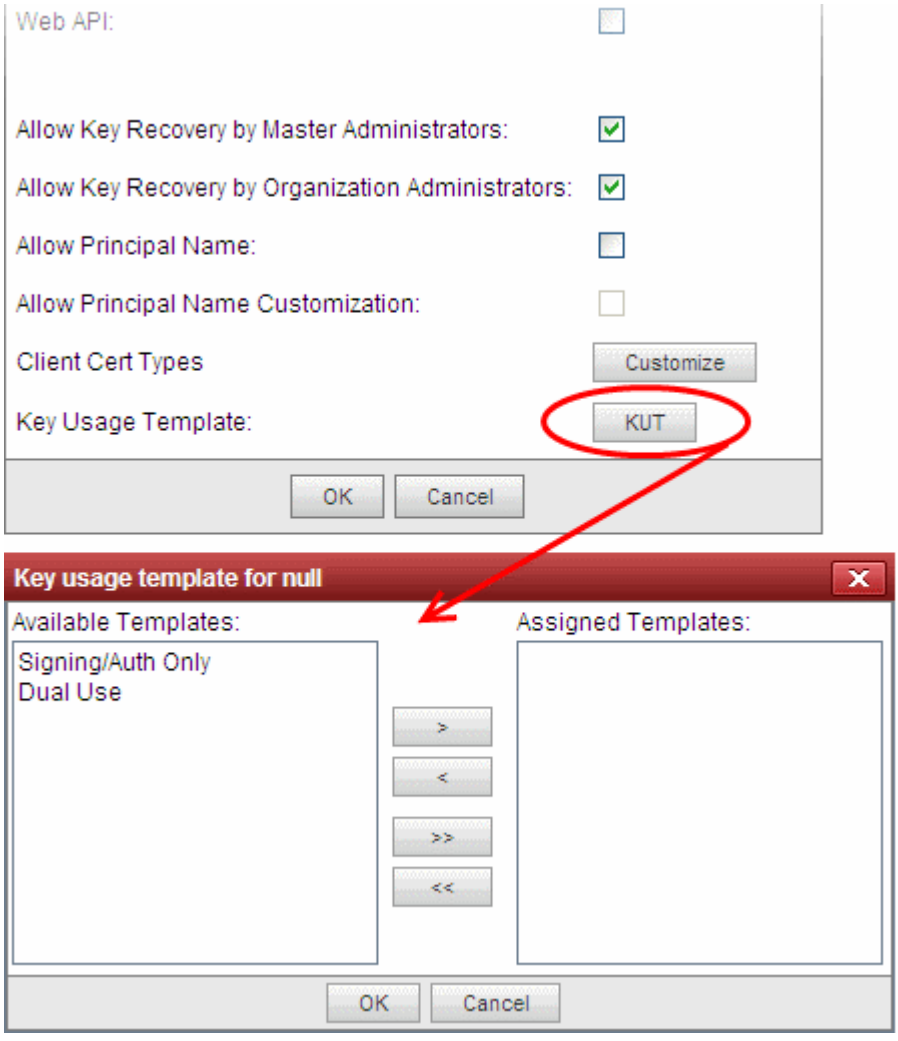
Important Note: The Key Usage Template (KUT) feature will not be available by default. If required, the MRAO Administrator can contact Comodo and request for it. The KUT button will be visible to the MRAO Administrators only if it is enabled by Comodo.

Security Roles:

- MRAO - Can define Key Usage Template (KUT) for all Organizations.
- RAO SMIME - Can define KUT for Organization(s) delegated to them and the Departments belonging to those Organizations. The KUT options available for an Organization depend on the templates defined for the Organization by the MRAO.
- DRAO SMIME - cannot view or change the KUTs.

The KUT for the Client Certificates of the end-users belonging to any particular Organization can be defined through 'Key Usage Template' interface. Defining the templates restrict the usage of the client certificates to the purposes of digital signing, encryption or both depending on the nature of the Organization and limits the inappropriate usage by the end-users.

To access the 'Key Usage Templates' interface, click the 'KUT' button under the 'Client Cert' tab of the Add New/Edit Organization interface:



This will open the 'Key Usage Templates' for that Organization, that enables to restrict the capabilities of the Client Certificates of the end-users within that Organization.

The KUTs available are displayed as a list in the left hand side pane and the KUTs assigned to the Client Certificates of the Organization are displayed in the right hand side pane. By default, no templates are assigned to the Organization.

To define the KUTs

- Select the template from the LHS pane and move it to RHS pane by clicking the right arrow button. Repeat the process for defining more than one template. To assign all the templates, just click the right double arrow button.
- To remove the assigned templates, select the template from the RHS pane and click left arrow button to move to LHS

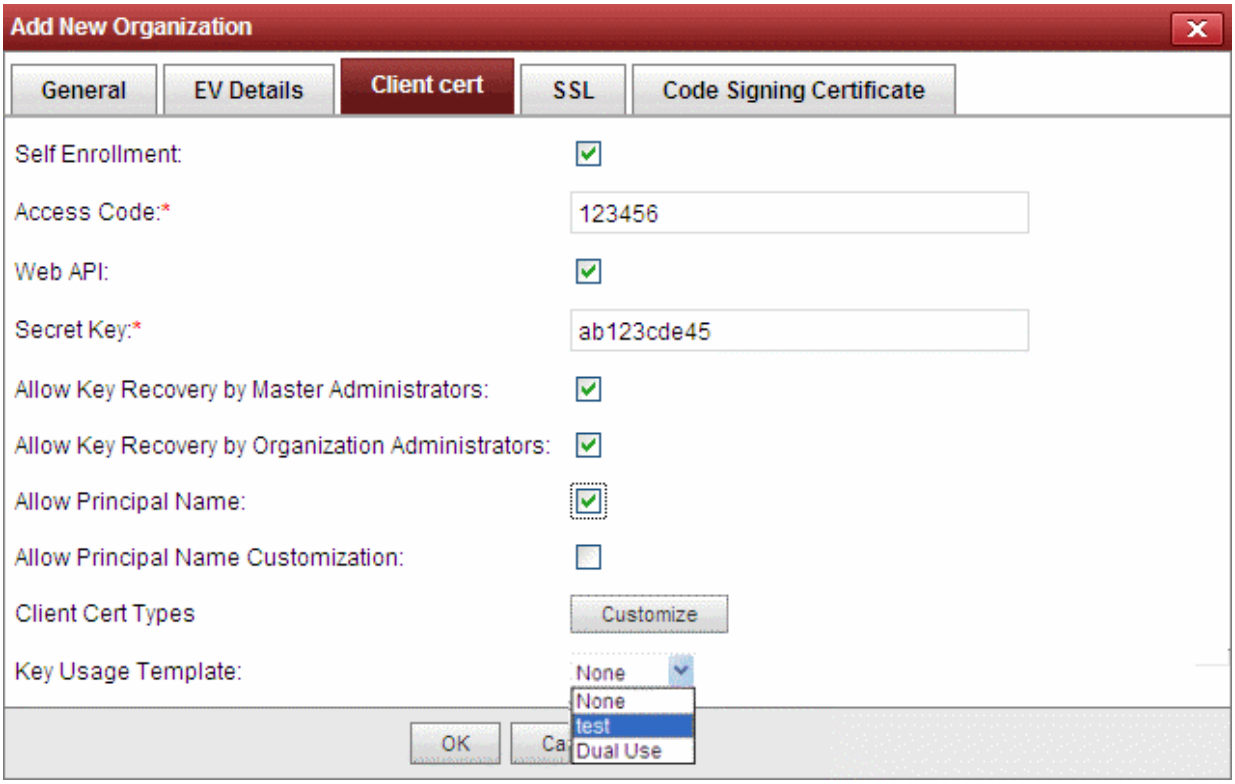
pane. To remove all the templates, just click left double arrow button.

- Click OK.

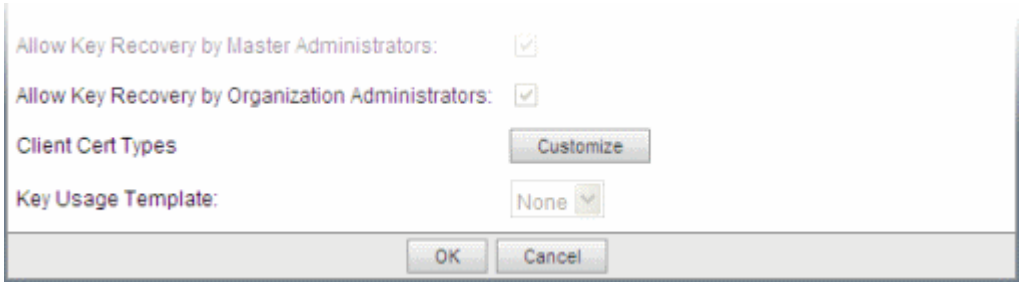
The end-users belonging to the Organization can use their Client Certificate only for the purposes as dictated by the assigned templates.

Notes:

- The KUTs defined in the 'Key Usage Template' interface will apply only to this specific Organization.
- The Key Usage Template interface is accessible only by MRAO administrators. RAO administrators will see only a drop-down with the template options assigned by the MRAO for the Organization while editing the Organization or the Departments of the Organization.

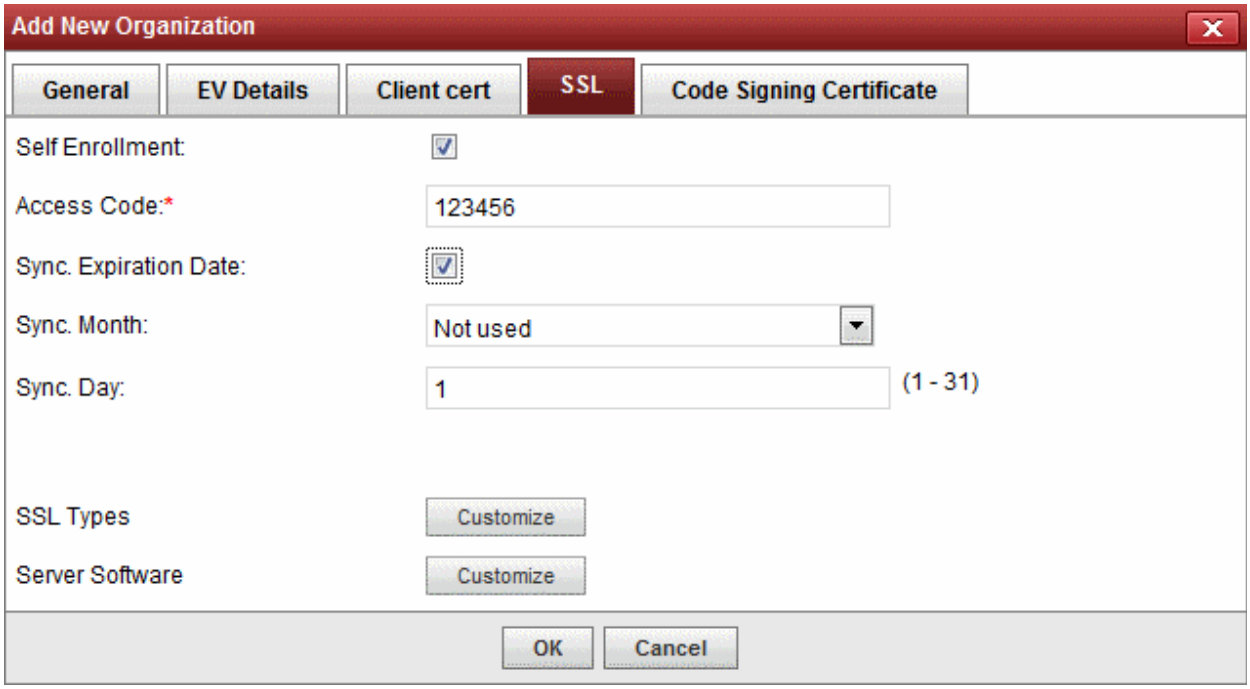


- If the MRAO administrator has not assigned any templates, the option will not be available.



5.2.2.4.7 SSL Certificates Settings Tab

The 'SSL' tab allows the MRAO to specify Self Enrollment, certificate types and term lengths, Web API capabilities and expiry synchronization settings relating to the SSL certificates issued to the domain associated with the Organization (or Department of the Organization). The settings chosen in this section relate only to those certificates issued to the domain associated with the currently selected Organization.



5.2.2.4.8 SSL Certificates - Table of Parameters

Field Name	Type	Description
Self Enrollment	*Checkbox* *Default state - not checked*	Checking this box will enable external requests for SSL certificates to be made by using the Self Enrollment Form hosted (by default) at: https://CCM/customer/customer_uri/ssl • Certificates requested using the Self Enrollment Form will appear in the 'SSL Certificates' sub-tab of 'Certificates Management' section of Comodo Certificate Manager **before** they are submitted to Comodo CA for validation. It is the responsibility of the administrator to review then approve or decline the request. If the request is approved it will then be forwarded to Comodo CA for processing. If the application is made for a domain that has been pre-validated for your account then certificate will be issued immediately. If the application is made for a new domain, then Comodo will first need to validate your company's ownership of that domain prior to issuing the certificate. After successful validation, the new domain will be added to your list of 'pre-validated' domains and future certificates will be processed immediately. • To successfully complete the SSL request, the applicant must supply the correct Access Code for the Organization at the Self Enrollment Form. This Access Code should be communicated to the applicant using out-of-bands methods. • Provided that the Access Code matches the Organization being applied for AND the email address that the applicant entered at the enrollment form is from the same domain as that Organization's 'Common Name' then SSL certificates can be requested by individuals that do not yet exist in Comodo Certificate Manager. In such circumstances, a new end-user will be automatically created under the 'SSL Certificates' sub-tab of CCM interface with the end-user name 'requesterSSL <DOMAIN.com>' (where DOMAIN.com = the domain name for which the application is being made). This End-User will automatically be assigned membership of the Organization that the SSL Certificate was ordered for but will not own a Client Certificate.

Field Name	Type	Description
Access Code (Appears only if the 'Self Enrollment' checkbox is selected)	*String*	• An Access Code identifies a particular 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 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. • Administrators should choose a complex Access Code containing a mixture of alpha and numeric characters that cannot easily be guessed. This code should be conveyed to the applicant(s) along with the URL of the sign up form. • Applicants that request a certificate using the Self Enrollment Form will need to enter this code.
Sync. Expiration Date	*Checkbox*	Checking this box will enable the ability to modify and synchronize the expiration month and day of all certificates issued to the Organization. • It is possible to select only a specific day of the month for expiry (simply select 'Not Used' for 'Sync. Month') • It is possible to select both a specific day and a specific month for expiry. • It is not possible to specify just a month of expiry.
Sync. Month:	*Drop-down Selection*	Allows Administrators to choose a specific month of the year during which all certificates issued to the Organization will expire. Administrators will also need to choose a specific day of expiration.
Sync. Day:	*String* *Numeric character.* *Between 1-31 if no specific month is chosen.* *Between 1-31 ; 1-30 or 1-28 if a specific month is also chosen.*	The Organization's Administrators can specify the day of the month on which certificates issued to the domain will expire. Specifying a certain day of the month for expiry for all SSL certificates issued to an Organization(s) can greatly simplify the certificate management process - especially in enterprises with large volumes of certificates. ***Note 1**: Certificate terms cannot exceed the duration selected at the SSL certificate application form. This means:* • *If a specific Month is ALSO selected at the 'Sync. Month' drop down THEN the certificate will expire on the occurrence of that precise date that is closest to the certificate term selected on the* SSL Certificates **Self Enrollment Form** *or the* ***Built In Application Form*** • If a specific Month is NOT selected at the 'Sync. Month' drop down THEN the certificate will expire on the numbered day of the month that is nearest to the certificate term *selected on the* **SSL Certificates Self Enrollment Form** *or the* ***Built In Application Form*** ***Example***: Ordinarily, a 2 year certificate issued on the 12th of August 2008 would expire 730 days later on the 12th August 2010. However: • If the administrator has ONLY specified day 16 as the 'sync expiry day' then the certificate will expire on the 16th of July 2010 • If the administrator has ONLY specified day 5 as the 'sync expiry day', then the certificate will expire on the 5th August 2010 • If the administrator has specified 14th of June as the sync expiry 'day' and 'month', then the certificate will expire on the 14th June 2010 • If the administrator has specified 14th of August as the sync expiry

Field Name	Type	Description
		'day' and 'month', then the certificate will expire on the 14th August 2009 ***Note 2**: Specifying a sync expiry day only affects certificates issued from that point forward. The expiry date of certificates that have already been issued will not change. The sync expiry day will, however, apply to all renewals of existing certificates.*
Web API	*Checkbox* *Default state - not checked*	Checking this box allows to open access for enrolling certificates through Web Service API. This requires special agreement with Comodo CA. For detailed instructions please refer to Web API documentation.
Secret Key (Appears only if the 'Web API' checkbox is selected)	*String* •	The Secret key is a phrase that is unique for all Organizations. This phrase restricts access for enrolling certificates for that Organization. Used in pair with 'Organization ID' (visible only for already created Organizations).
SSL Types	*Button* *'Customize'*	The SSL types customization options allow the administrator to specify the SSL Certificate types and term lengths that will be available for this Organization for new certificate applications. • Clicking the 'Customize' button will open the 'Bind SSL Types' interface. • All choices made in the 'Bind SSL Types' interface will apply only to this specific Organization. • It is possible to make different certificate types and terms available to the applicant depending on whether the application is made using the Built-in application form (Admin UI) or the (Self) Enrollment form. See section **Customize an Organization's SSL Certificate Types** for more details on this and the other options available through the 'Bind SSL Types' interface. • The more powerful '**SSL Types**' area contains a very similar interface that allows Master Administrators to determine universal certificate type and term lengths that apply to ALL Organizations • If a particular certificate type or term is not visible in the '**Bind SSL Types**' area then it may need enabling in the 'SSL Types' area. SSL Administrators should seek the advice of the Master Administrator.
Server Software	Button *'Customize'*	The Server Software customization options allow the administrator to specify the types of server software that are allowed for this Organization. • Clicking the 'Customize' button will open the 'Server Software' interface, with a list of server software • The administrator can select the server software that can be used for the Organization • All choices made in the ' Server Software' interface will apply only to this specific Organization. • The server software selected in this field will be available in the 'Server Software' drop-down of both the Built-in application form (Admin UI) or the (Self) Enrollment form. See section **Customize an Organization's Server Software Types** for more details on this.

5.2.2.4.8.1 Customize an Organization's SSL Certificate Types

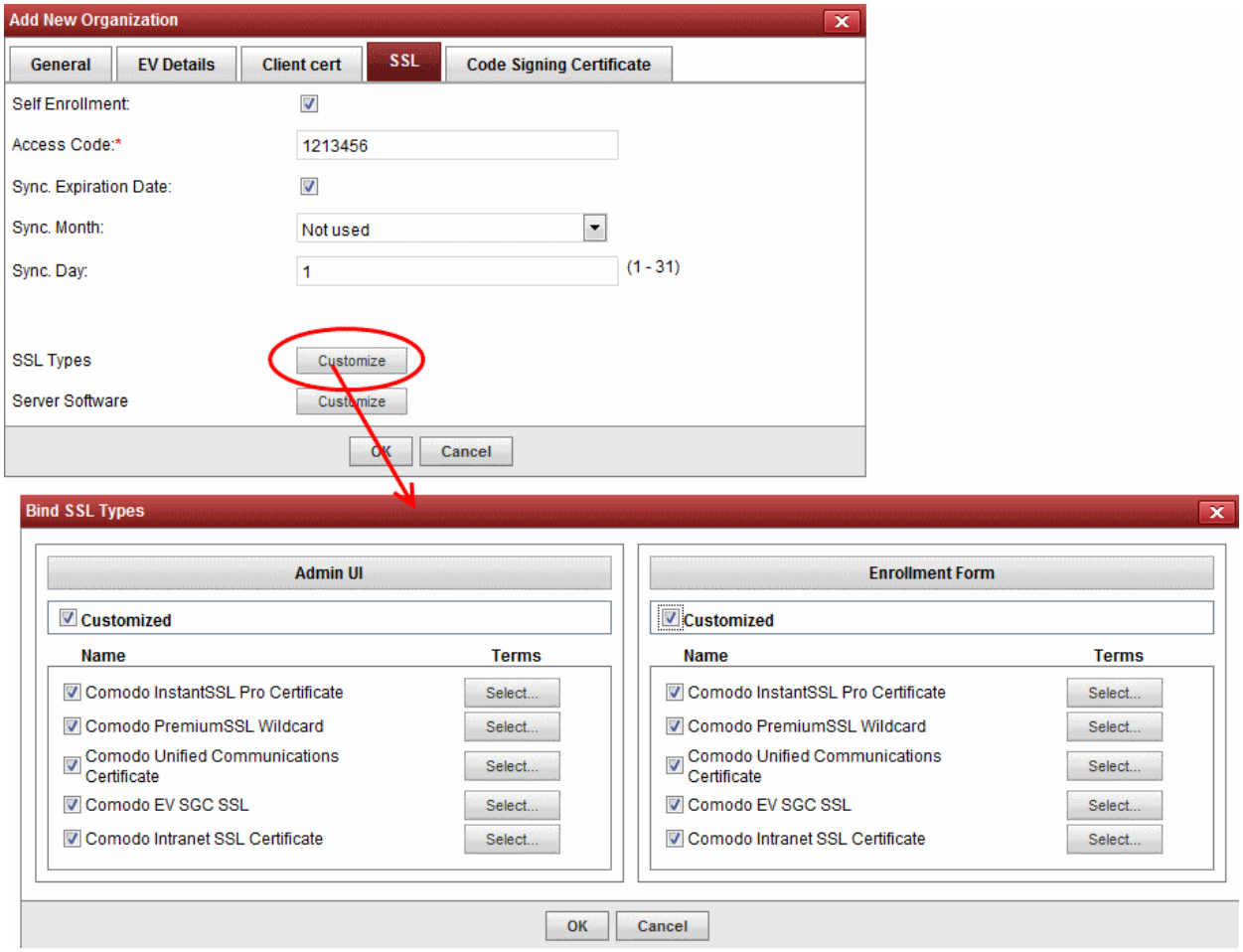
Security Roles:

- MRAO - can customize SSL certificate type availability for all Organizations and Departments
- RAO SSL - can customize SSL certificate type availability only for Organizations (and any subordinate Departments) that are delegated to them.
- DRAO - cannot customize SSL certificate type availability.

(i.e. RAO/DRAO SSL Admins cannot change which SSL certificates are available to Organizations or Departments that they control).

The types and term lengths of SSL certificates that are available to any particular Organization can be customized using the 'Bind SSL Types' interface. Creating a targeted 'certificate roster' simplifies the certificate selection procedure at the application forms and helps avoid applications for certificates which are inappropriate for that Organization.

To access the 'Bind SSL Types' interface, click the 'Customize' button beside SSL Types under the SSL tab of the Add New/Edit Organization interface. This will open the 'Bind SSL Types' for that Organization.



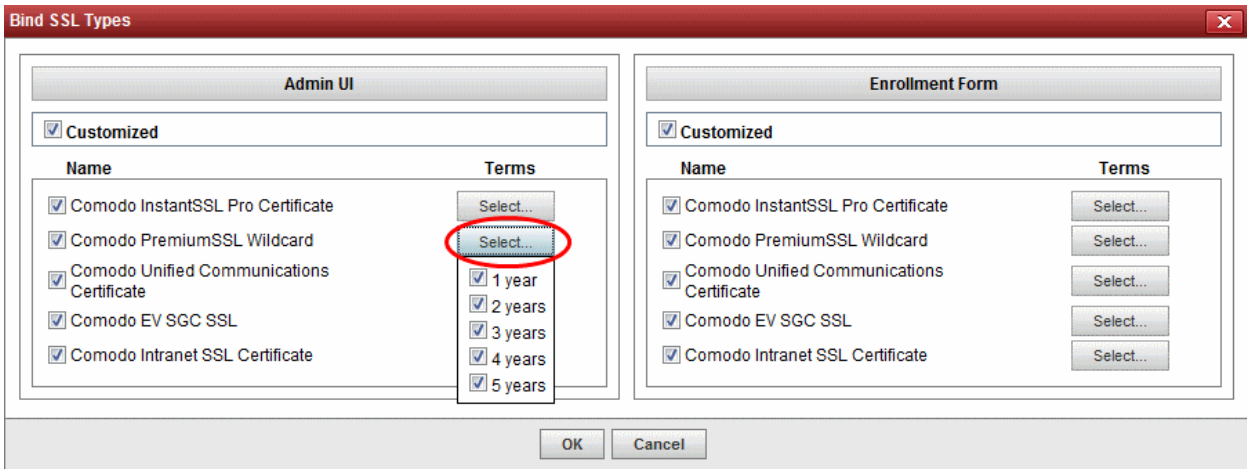
- **Admin UI** - Determines the SSL certificate types that will be available to applicants using the **Built-In Application form** for that Organization.
- **Enrollment Form** - Determines the SSL certificate types that will be available to applicants using the **Self Enrollment Form** for that Organization.
- It is therefore possible to choose a different selection of certificate availabilities for an Organization depending on whether the Built-in or Self-Enrollment form is to be used.

By default, the 'Customized' option is left unchecked so that all the certificate types are available through both types of application form.

To restrict the SSL types and their terms

1. Select the 'Customized' option below either or both 'Admin UI' or 'Enrollment Form'.
2. Check the names of the certificates you wish to be available to that Organization and leave the others unchecked.

3. Click the 'Select' button next to the certificate name to choose which terms will be available.



4. Click OK.

The MRAO needs to log out then back in again for the customization options to take effect.

The types and terms of SSL certificates that are selected in the 'Bind SSL Types' interface will now be available in the 'Type' and 'Term' drop-down fields of this Organization's application forms.

Notes:

- All choices made in the 'Bind SSL Types' interface will apply only to this specific Organization.
- The more powerful '**SSL Types**' area contains a very similar interface that allows MRAO to determine universal certificate type and term lengths that apply to ALL Organizations.

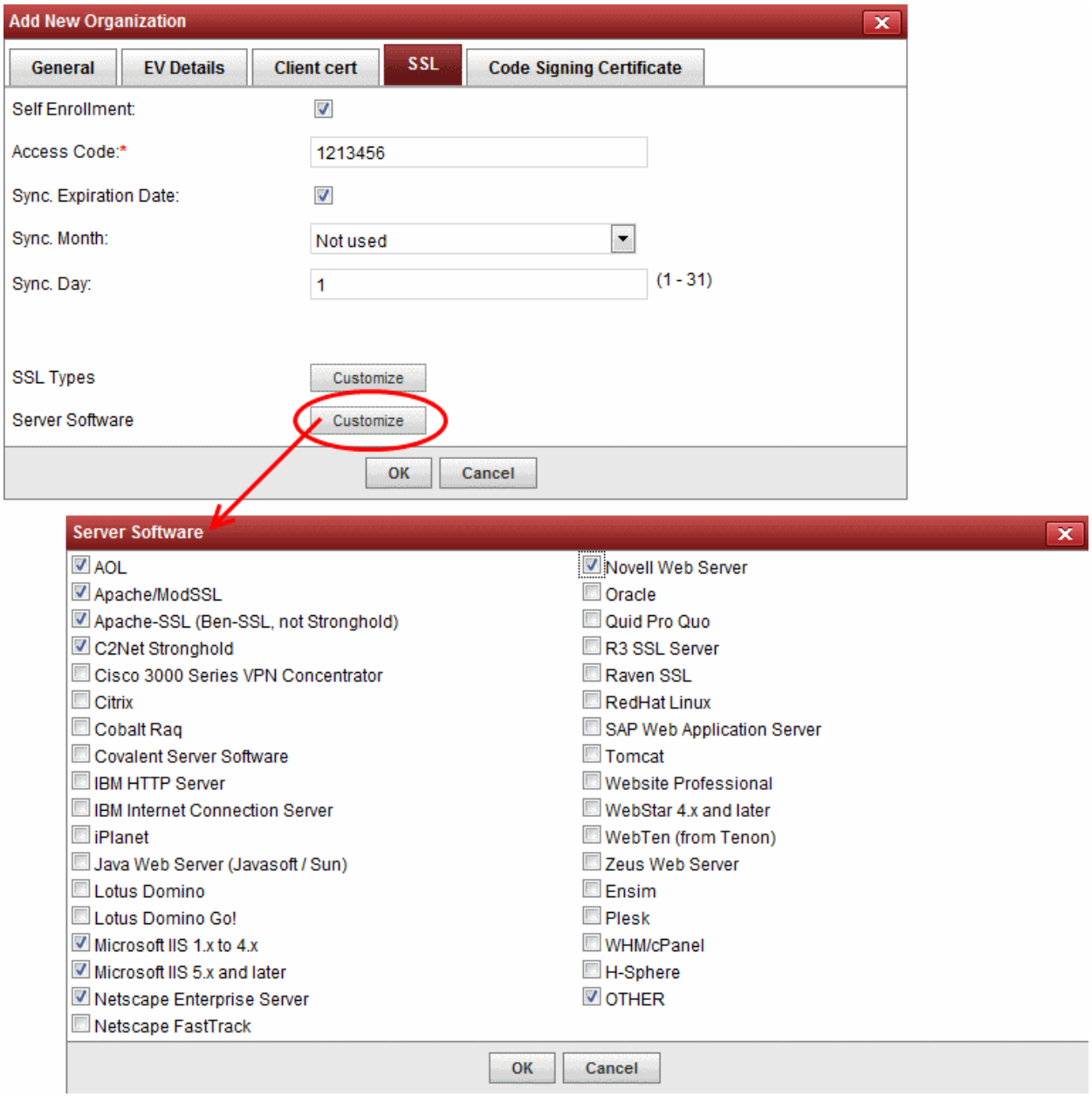
5.2.2.4.8.2 Customize an Organization's Server Software Types

Security Roles:

- MRAO - can customize server software types that can be used for all Organizations and Departments
- RAO SSL - can customize server software types that can be used for only for Organizations (and any subordinate Departments) that are delegated to them.
- DRAO - cannot customize server software types.

The types of server software that can be used to any particular Organization can be customized using the 'Server Software' interface. Only those allowed server software will be listed in the Server Software drop down of both the **Self Enrollment** and the **Built-in Application** forms for adding new SSL certificate for that Organization.

To access the 'Server Software' interface, click the 'Customize' button beside 'Server Software', under the SSL tab of the Add New/Edit Organization interface. This will open the 'Server Software' for that Organization.



By default, no server software will be selected.

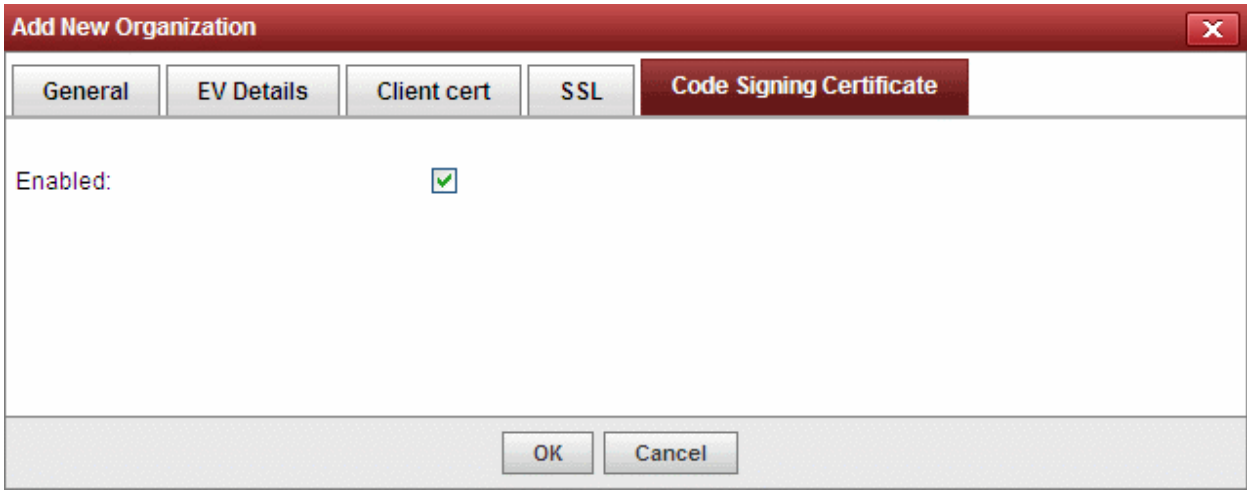
- To restrict the Server Software types select the names of the server software you wish to allow for that Organization and leave the others unchecked. Click OK to save the selection.

The MRAO needs to log out then back in again for the customization options to take effect.

Note: All choices made in the 'Server Software' interface will apply only to this specific Organization.

5.2.2.4.9 'Code Signing Certificates' Settings tab

The 'Code Signing' tab allows the Administrators to enable request/issuance of Code Signing Certificates for the Organization. The setting in this section relate only to those certificates issued to the domain associated with the currently selected Organization.

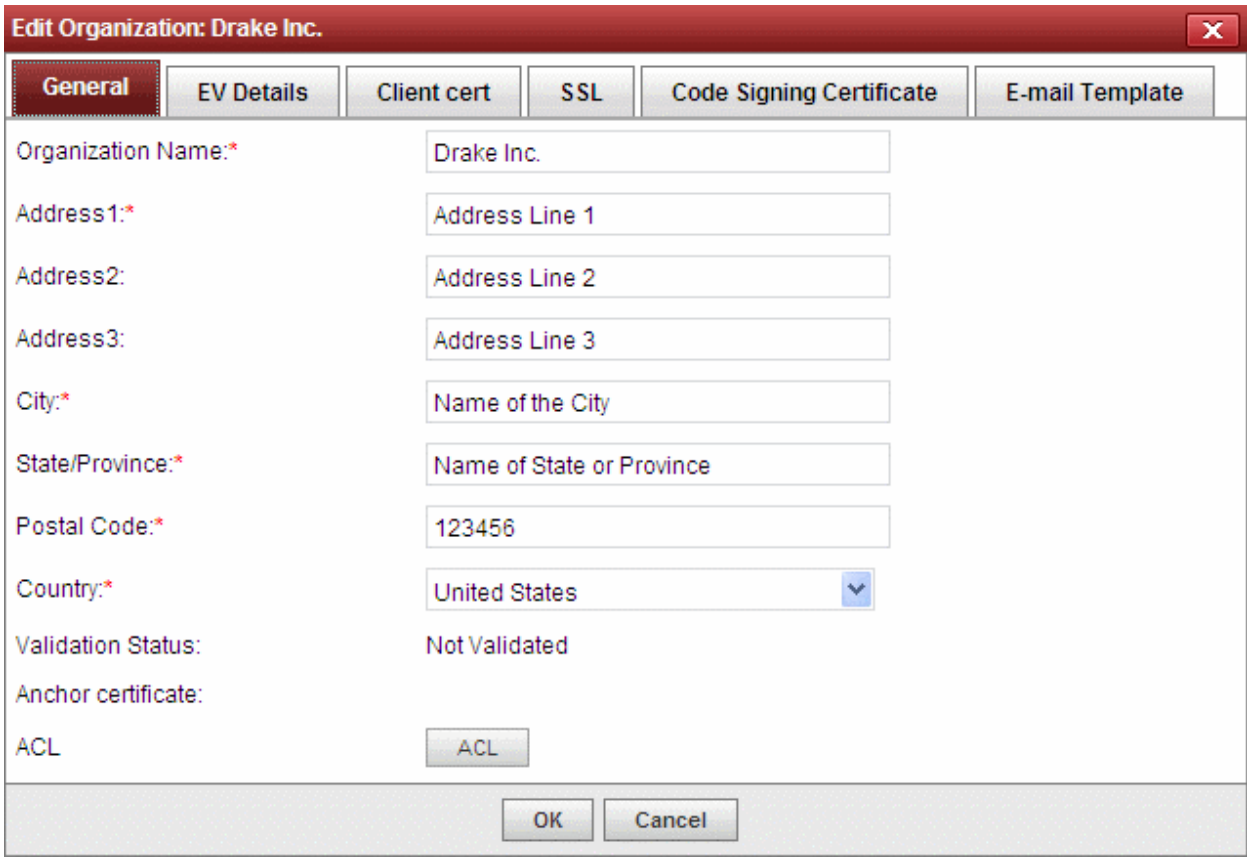


5.2.2.4.10 Code signing Certificates - Table of Parameters

Field Name	Type	Description
Enabled	Checkbox Default state - not checked	Checking this box will enable the request and issuance of Code Signing Certificates to end-users that are members of this Organization.

5.2.2.5 Editing an Existing Organization

Selecting an Organization and clicking the 'Edit' button at the top will open the Edit Organization dialog.



The Edit Organization dialog enables administrators to view/modify the 'General', 'EV Details', 'Client Cert' , 'SSL' and Code Signing Certificate details pertaining to an existing Organization at any time.

- MRAO Administrators - can view and edit details under all the tabs
- RAO Administrators - can view and edit details under all the tabs except 'General Settings' . The details under General Settings tab are visible to the RAO but cannot be edited.

Full details of the options available when editing an existing Organization are available in the previous section, '**Creating a new Organization**'. Additionally the 'Email Template' tab allows the Administrator to directly edit the content of the automated notification emails as set by him/her in the Notifications area. For more details, refer to the **Email Templates** section of this guide.

General Settings

The General Settings area under Edit Organization dialog is similar to that in the '**Create New Organization**' dialog except for an additional Access Control button ACL.

- **ACL**: Enables the administrator to configure and limit incoming access to the CCM interface to certain IP addresses and ranges. This is very useful if they want to grant access only to certain IP addresses and so prevent unauthorized or unsecured access to the CCM interface. After specifying one or more IP addresses or ranges in CIDR notation, only administrators attempting to login from these specified addresses will be allowed access.
- The MRAO can access a more powerful **Access Control** area by clicking Settings > Access Control, which has a similar interface and allows to limit incoming access to the CCM interface. The Access Control settings made by the MRAO through Settings > Access Control will over-rule any settings made through 'Edit Organization' area. Also RAO/DRAO can restrict access only to IP ranges that fall within the range that the MRAO has set in the 'Settings > Access Control' area.

5.2.2.5.1 Imposing Access Restrictions to CCM interface

Security Roles:

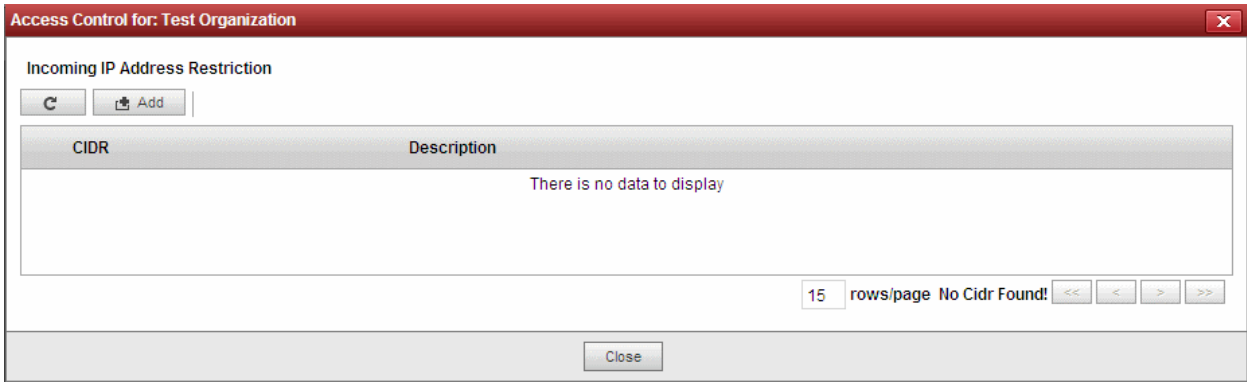
- MRAO - Access restrictions imposed by MRAO will apply for the management of the certificates, administrators, end-users and settings for all the Organizations and Departments.
- RAO - Access restrictions imposed by RAOs will apply for the management of the certificates, administrators, end-

users and settings for the Organizations (and any subordinate Departments) that have been delegated to them.

- DRAO - Access restrictions imposed by DRAOs will apply for the management of the certificates, end-users and settings for the Departments that have been delegated to them.

To limit incoming access to the CCM interface

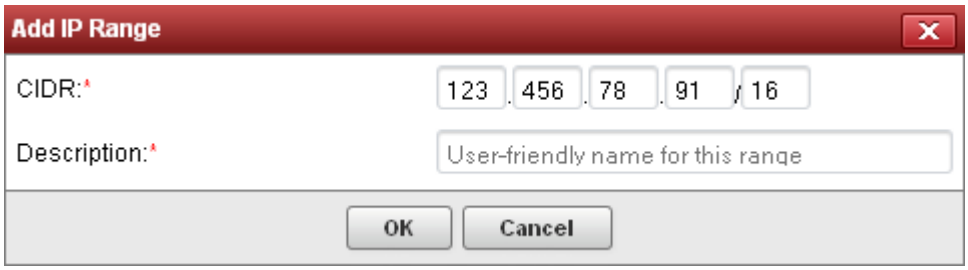
- Click the ACL button from the Settings > Organizations > 'Edit Organization' dialog. The 'Access Control' dialog will appear.



Column Display	Description
CIDR	Short for Classless Internet DOMAIN Routing. Administrator should specify IP range: it should be IP address followed by network prefix, e.g. 123.456.78.91/16.
Description	Contains a short description for the IP range as entered by the administrator while creating the CIDR.
Control Buttons	**Description**
Edit	Enables administrator to edit CIDR's details.
Delete	Enables administrator to delete the CIDR.
Add	Opens 'Add IP Range' dialog.
Refresh	Updates the list of IP ranges

To add a new IP Range

- Click 'Add'. The 'Add IP Range' dialog will appear.



- Enter the IP range, followed by network prefix, e.g. 123.456.78.91/16.
- Enter a short description for the IP range
- Click OK.

The IP range will be added as a new CIDR and the access to CCM from the new IP range will be allowed.

- For details on other options in the General Settings Area, see **5.2.2.4.1.General Settings**
- For details on the EV Details tab, see **5.2.2.4.3 EV Details Tab**

- For details on the Client certs tab, see **5.2.2.4.5.Client Cert Settings Tab**
- For details on the SSL certs tab, see **5.2.2.4.7.SSL Certificates Settings Tab**

Note: Any changes you make to the settings of an existing Organization will NOT affect certificates that have already been issued to domains belonging to that Organization.

5.2.2.6 Validating an Organization

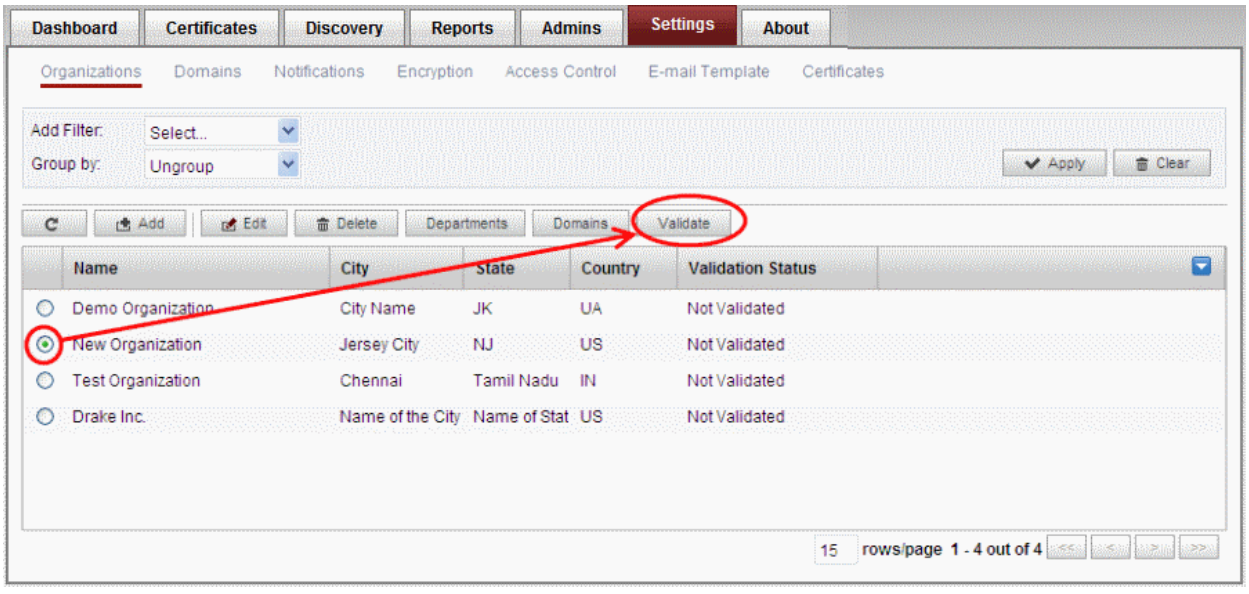
Before you can issue Organization Validated (OV) SSL certificates for an Organization (or Department), the Organization must first be validated by Comodo.

Note: The request and issuance of OV certificates for Organizations or Departments require OV certificates enabled for your CCM account. If not enabled previously, contact your CCM account manager for enabling this feature.

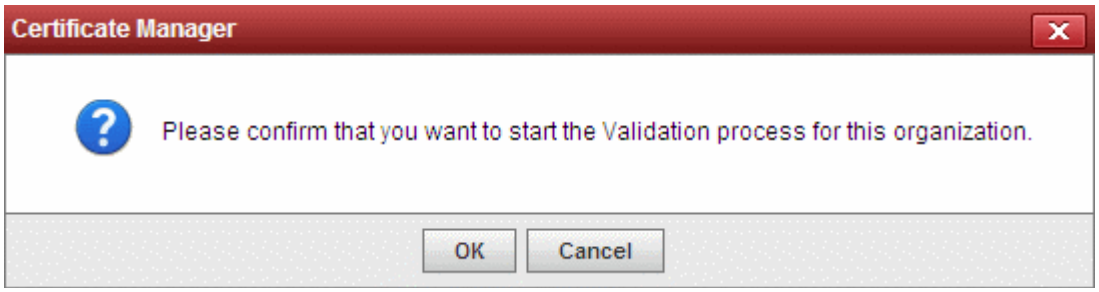
The 'Validation Status' of new Organizations will initially be 'Not Validated' and the 'Anchor Certificate' field will be blank. Validation Status will change to 'Validated' after successful validation and the 'Anchor Certificate' status will be 'ON'. MRAOs can initiate the validation process by selecting the Organization and clicking the 'Validate' button. This certificate will be used as a reference by CCM whenever an OV SSL certificate is requested for the Organization or any Department under it. Address details entered in the 'General' tab of 'Add or Edit Organization' are used for the validation process and they cannot be edited while the validation status is 'Pending'. Details can be edited again only when the validation status is 'Validated', 'Expired' or 'Failed'.

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

To validate an Organization, select it and click the 'Validate' button:



- Click 'OK' to confirm starting the validation process.



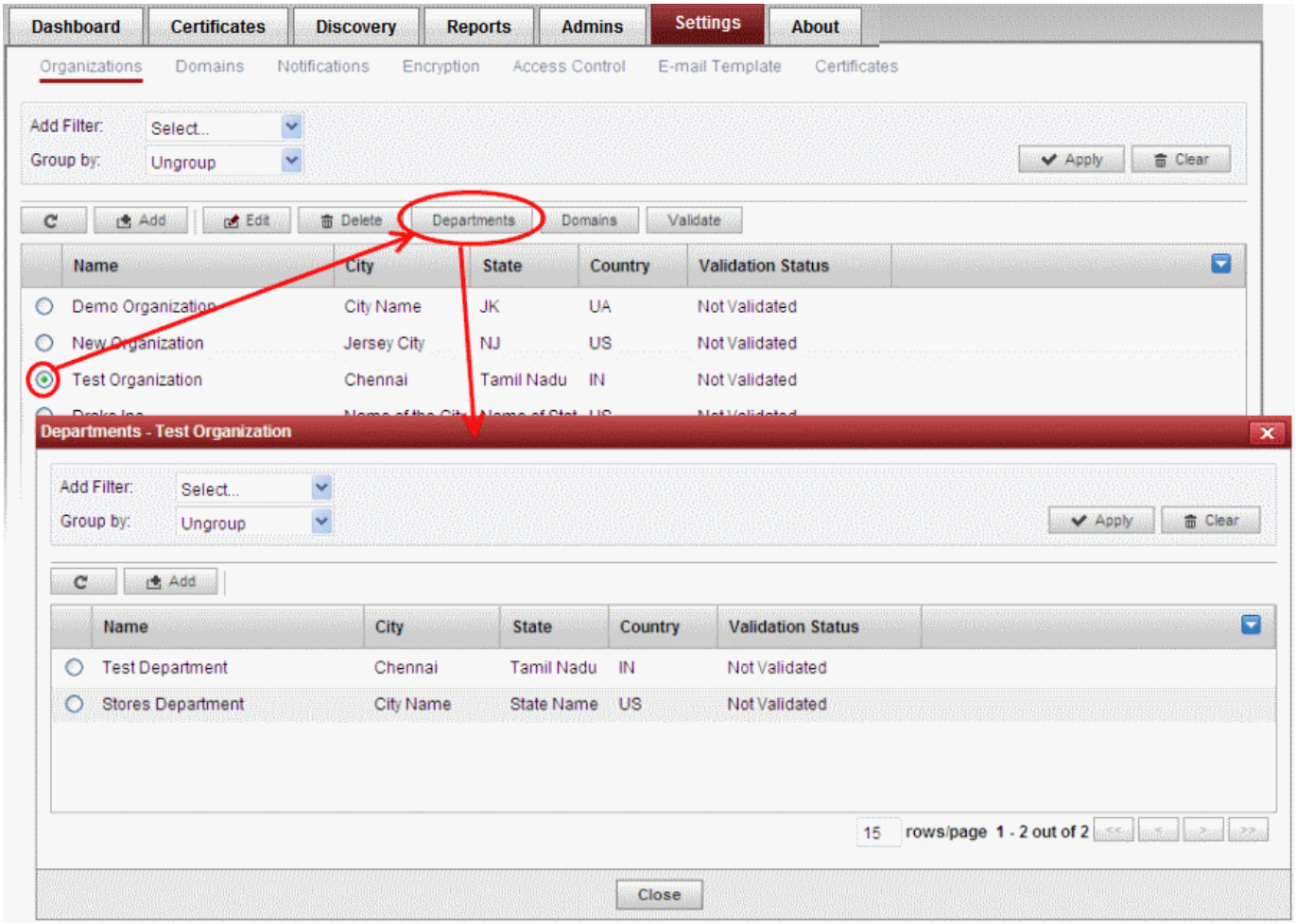
The validation process will begin and when completed successfully, Validation Status will display as 'Validated' in the Edit > General tab of the organization.

The various stages of validation status are:

- **Not Validated** - The validation process not started. MRAOs can start the process of validation by selecting an organization and clicking the 'Validate' button at the top.
- **Validated** - The organization is validated and anchor certificate issued. The organization and departments under it can request for OV SSL certificates.
- **Pending** - Validation process started and not completed. The address details of the organization in the General tab is locked and non-editable.
- **Failed** - The validation process failed for the organization. MRAOs can initiate the validation process again by clicking the 'Validate' button.
- **Expired** - The validation period of 36 months is expired for the organization. MRAOs can initiate the validation process by clicking the 'Validate' button.

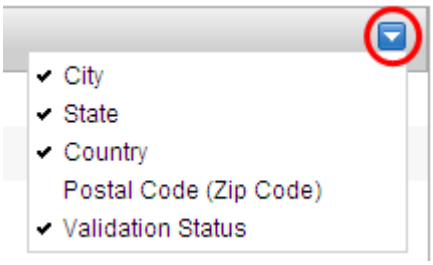
5.2.2.7 Managing the Departments of an Organization

MRAO and RAO Administrators can view and edit Departments belonging to an Organization by selecting it and clicking the 'Departments' button at the top. This will open a dialog that lists all Departments belonging to the Organization and controls to Edit, Delete, Add and manage Domains.



5.2.2.7.1 Departments Dialog - Table of Parameters

Column Display	Description
Name	A list of all Departments that have been delegated to the Administrator that is currently logged in.
City	Displays the name of the city entered at the time of creating the department
State	Displays the name of the State entered at the time of creating the department
Country	Displays the name of the Country entered at the time of creating the department
Postal Code (Zip Code)	Displays the postal code entered at the time of creating the department
Validation Status	Displays whether the department is validated for the request and issuance of OV SSL certificates. For more details refer to the section **Validating an Organization**.
Note: An administrator can enable or disable the columns from the drop-down button beside the last item in the table header:	

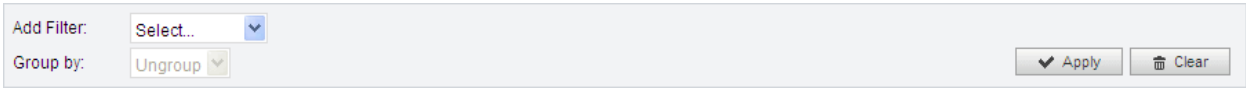


Controls Buttons	Add	Enables Administrators to modify General, Client, SSL and Code Signing Certificate settings pertaining to an existing Department.
	Refresh	Updates the list of Departments.
Department Control Buttons **Note**: The Department control buttons appear only on selecting a Department	Edit	Enables Administrators to modify General, Client, SSL, Code Signing Certificate and E-mail Template settings pertaining to an existing Department.
	Delete	Deletes the Department. The Control is not visible to DRAO Administrators.
	Domains	Enables Administrators to view, edit and delegate domains to the Departments.

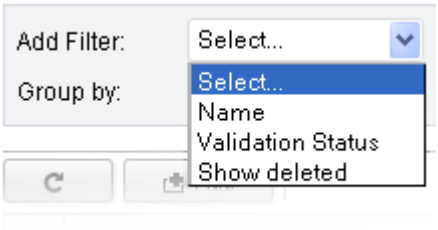
5.2.2.7.2 Sorting and Filtering Options

- Clicking on the column header 'Name' sorts the items in the alphabetical order of the names of the departments.

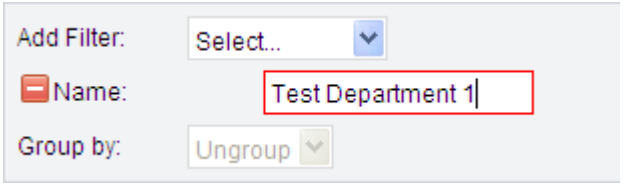
Administrators can search for particular department by using filters under the sub-tab:



You can add filters by selecting from the options in the 'Add Filter' drop-down. For example, if you want to filter the Department with 'Name':

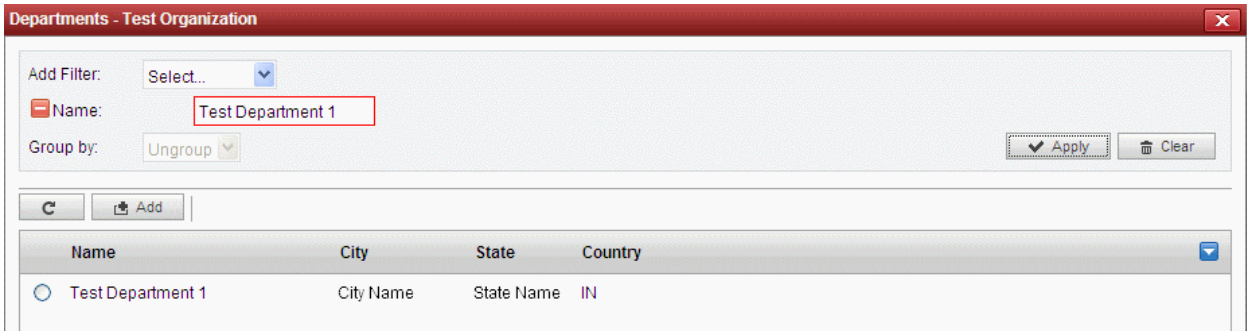


- Enter part or full name in the Name field.



- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed:



- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Departments' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

5.2.2.7.3 Creating Departments

An Organization may consist of sub-ordinate Departments, managed by DRAO Administrators. In order to provide certificates to the employees, end-users or websites pertaining to the Departments, the MRAO or the RAO Administrators can should first create the Departments under the Organization and associate domains to the Departments.

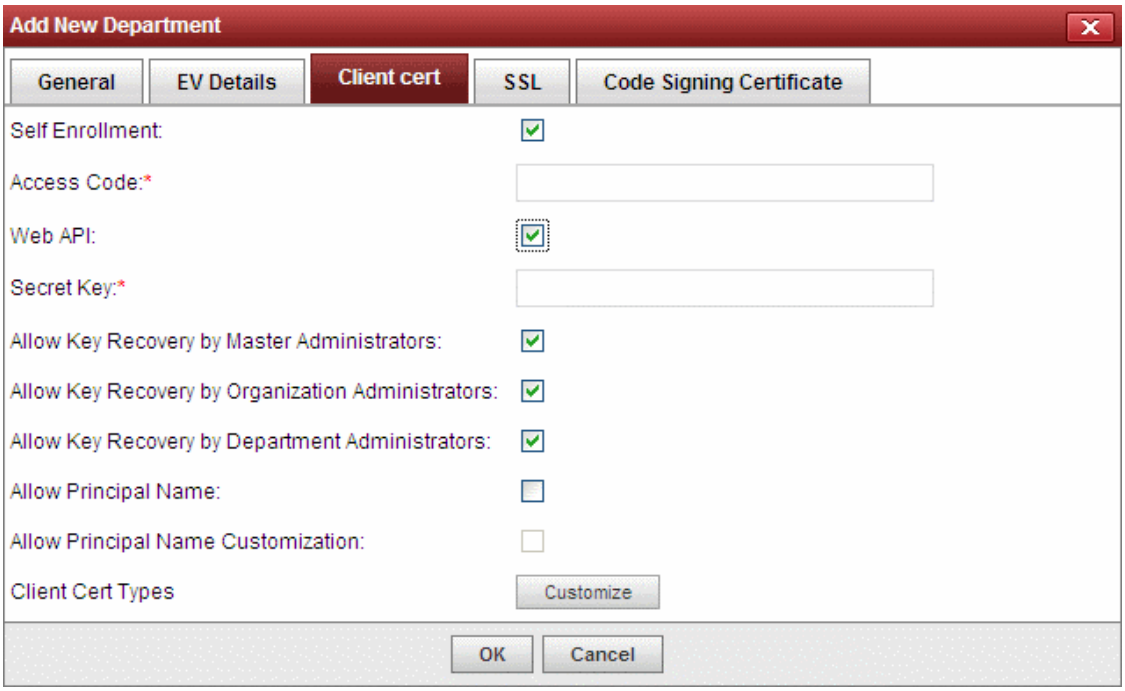
MRAO and RAO Administrators can add a new Department at any time by clicking the 'Add' button located at the top of the 'Departments' dialog:

The dialog contains five tabs - General, EV Details, Client Cert, SSL and Code Signing. Apart from 'Client Certificates', these tabs are the same as those in the 'Add New Organization' dialog. If the parent organization is already validated by Comodo for the request and issuance of OV SSL certificates, the address details except the Department Name will be auto populated with the parent organization's address. Refer to the section **Validating an Organization** for more details.

- The 'General' tab - see **5.2.2.4.1 General Settings** for more details
- The 'EV Details' tab - see **5.2.2.4.3 EV Details Tab** for more details.
- The 'SSL Certificate' tab - see **5.2.2.4.7 SSL Certificate Settings tab** for more details
- The 'Code Signing' tab - see **5.2.2.4.9 Code Signing Certificates Settings tab** for more details

Client Certs tab

The Client Certificate tab is the same as that explained in **5.2.2.4.5.Client Certificate Settings Tab** but contains an additional setting related to key recovery:



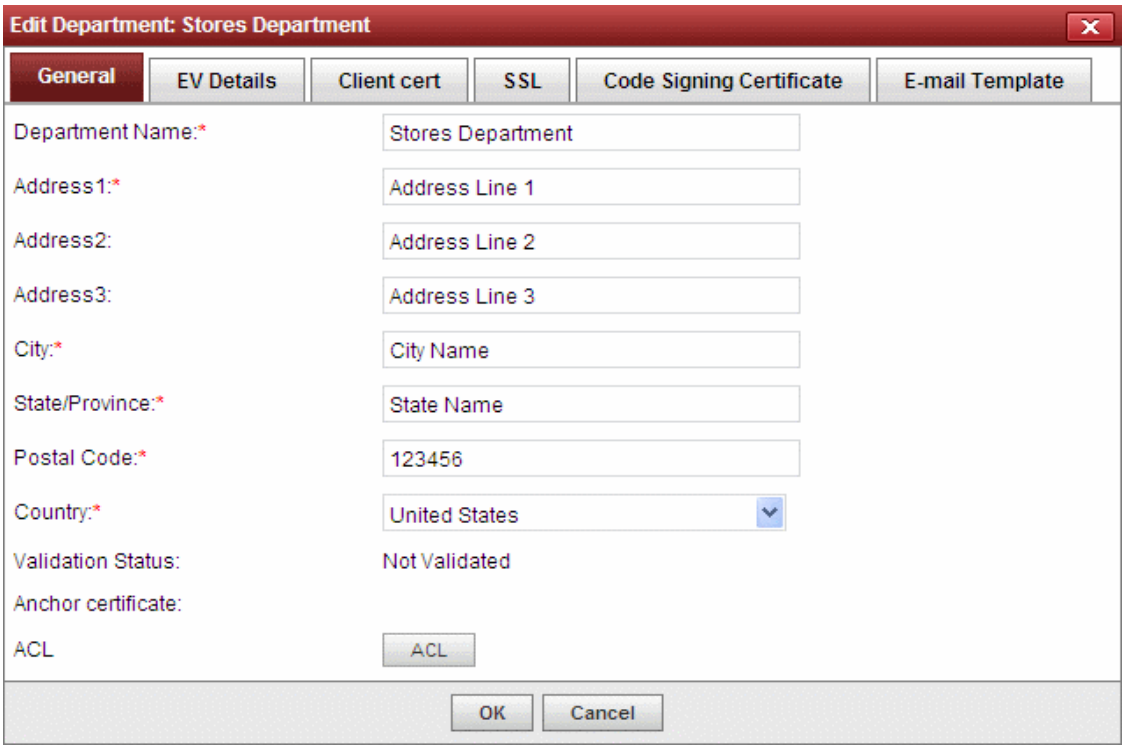
Allow Key Recovery by Master Administrators	Checkbox Default state - checked if pre-enabled by MRAO*	If selected, the MRAO Administrator will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the MRAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificates UNTIL the MRAO has initialized their master key pair in the '**Encryption**' tab. See '**Encryption and Key Escrow**' for a more complete explanation of key recovery processes.
Allow Key Recovery by Organization Administrators	Checkbox Default state - checked if pre-enabled by MRAO*	If selected, the RAO Administrator will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the RAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificate UNTIL the RAO has initialized their master key pair in the 'Encryption' tab. See '**Encryption and Key Escrow**' for a more complete explanation of key recovery processes.
Allow Key Recovery by Department administrators	Checkbox Default state - checked if pre-enabled by MRAO*	If selected, the DRAO Administrator will have the ability to recover the private keys of client certificates issued by this Department. At the point of creation, each client certificate will be encrypted with the DRAOs master public key before being placed into escrow. If this box is selected then the Department will not be able to issue client certificate UNTIL the DRAO has initialized their master key pair in the 'Encryption' tab. See '**Encryption and Key Escrow**' for a more complete explanation of key recovery processes.

- The settings outlined above will be active ONLY IF the MRAO has enabled the appropriate key recovery options when **configuring Client Certificate options** for the Organization.

5.2.2.7.4 Editing Departments belonging to an Organization

The existing Departments under any Organization can be edited by the appropriately privileged administrator at any time by selecting the Department and clicking the Edit button at the top in the 'Departments' interface.

The Edit Department dialog will appear.



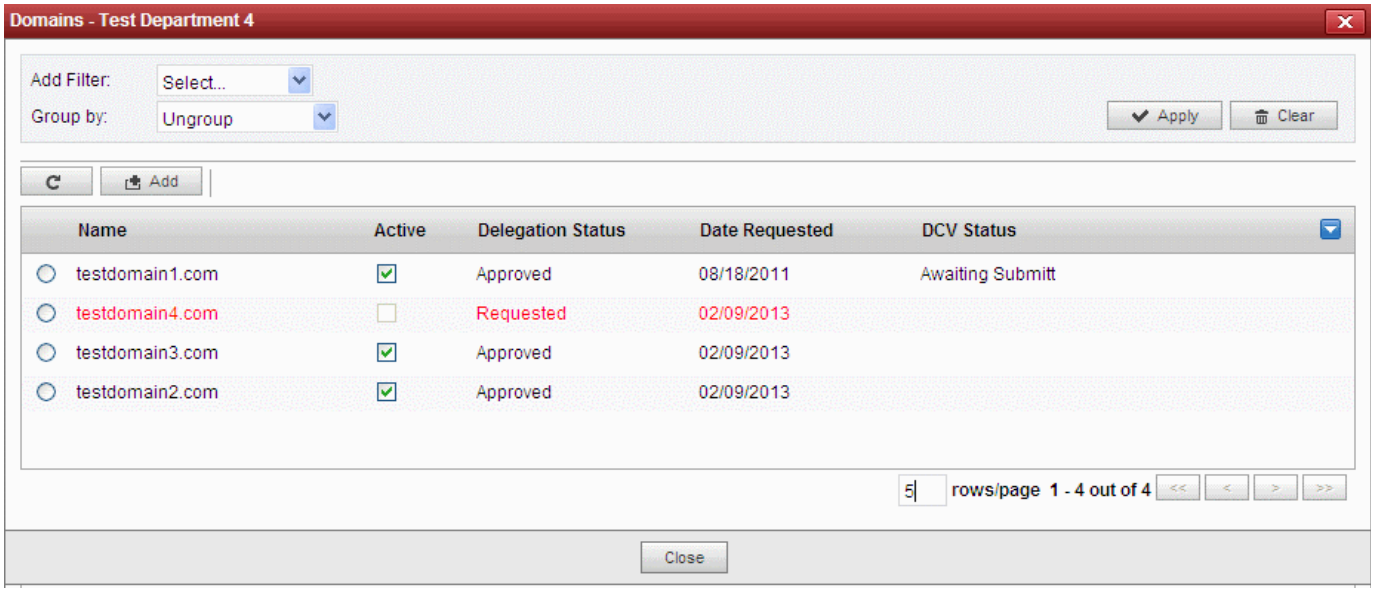
General Tab

The General settings area is similar to the General settings area in **Create New Department** dialog except for an additional option ACL.

- For details on other options, - see **5.2.2.4.2.General Settings - Table of Parameters**
- For more details on ACL - see **Imposing Access Restrictions to CCM interface**
- For more details on 'EV Details' tab - see **5.2.2.4.3 EV Details Tab**
- For more details on 'Client Certs' tab, - see **Client Certs tab** under **5.2.2.6.3.Creating Departments**
- For more details on 'SSL Certificate' tab - see **5.2.2.4.7 SSL Certificate Settings tab**
- For more details on 'Code Signing Certificate' tab - see **5.2.2.4.9 Code Signing Certificates Settings tab**

5.2.2.7.5 Managing Domains Belonging to a Department

The domains delegated to a Department can be viewed and managed by selecting the Department and clicking the 'Domains' button from the top. The 'Domains' dialog enables appropriately privileged Administrators to view, edit and delegate any Domains attached to the Department.

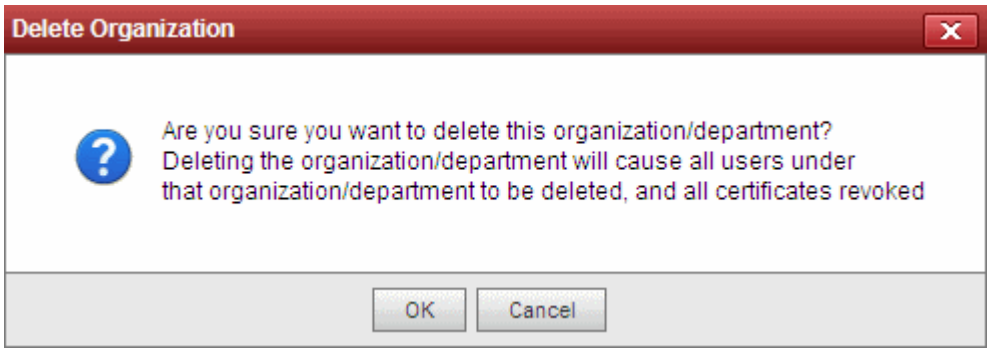


A detailed explanation on this area is available in section: **5.4.2.1 Domains Area Overview**

5.2.2.7.6 Deleting an Existing Department

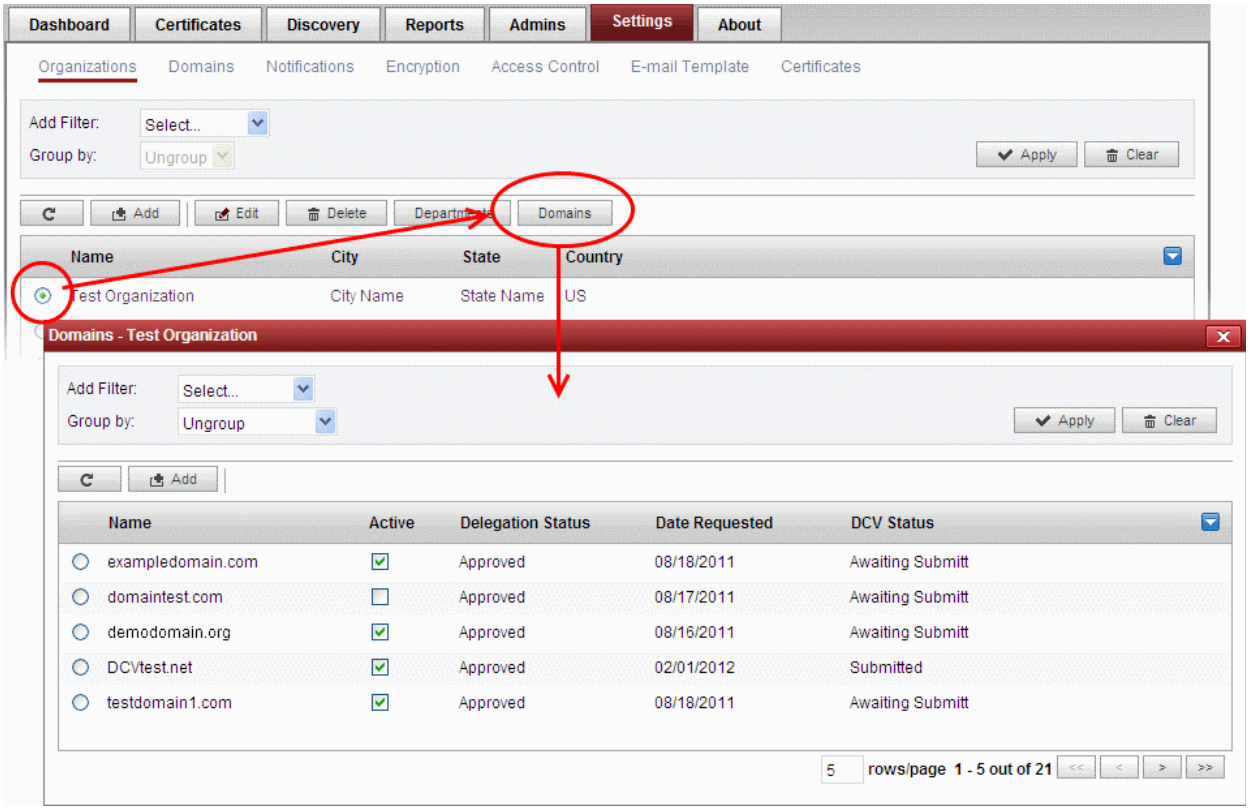
The Administrator can remove a Department if he/she no longer wishes to issue certificates from it, by selecting it and clicking the 'Delete' button from the top.

Note: Deleting an Organization will automatically revoke any certificates issued to that Department and will delete any end-users that are members of it. For this reason, Comodo Certificate Manager will prompt for confirmation:



5.2.2.8 Managing the Domains of an Organization

The Administrators can view an manage the domains delegated to an Organization by selecting it and clicking the 'Domains' button at the top. The 'Domains' dialog displays a list of Domains attached to the Organization and the Departments under that Organization.

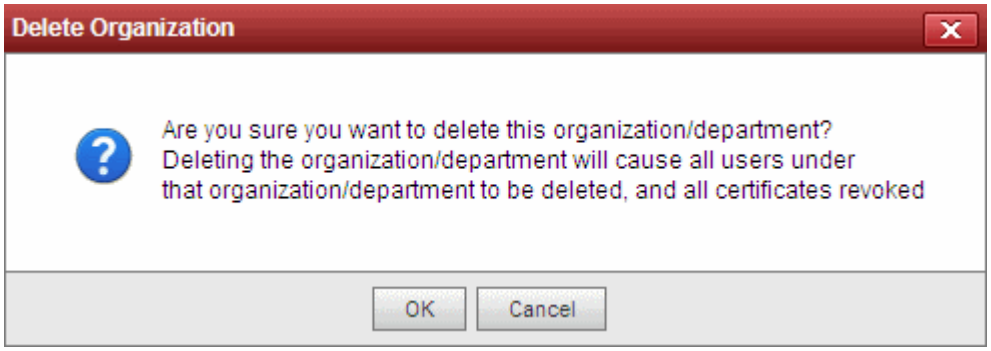


A detailed explanation of the controls available in this area is available in section **5.4.Domains**

5.2.2.9 Deleting an Existing Organization

The Administrator can remove an Organization, if he/she no longer wishes to issue certificates from it, by selecting it and clicking the 'Delete' button from the top.

Note: Deleting an Organization will automatically revoke any certificates issued to that Organization and will delete any end-users that are members of it. For this reason, CCM will prompt for confirmation:

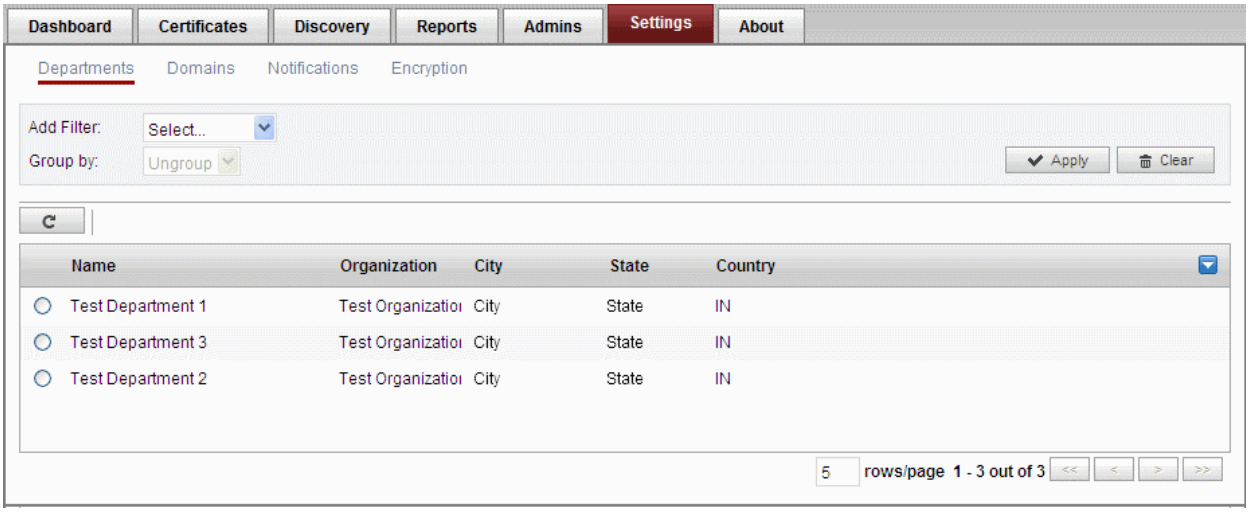


Note: The Delete control will not be visible for RAOs and DRAOs.

5.3 Departments

The Departments tab allows DRAO Administrators to manage existing domains and add new domains to the Departments that are delegated to them. Clicking the 'Edit' button at the top after selecting a Department will allow the DRAO Administrator to alter the general and email template settings for the Department for which they have been delegated control.

Important Note: The 'Departments' area is visible only to DRAO Administrators. MRAOs and RAOs will instead see the 'Organizations' tab and can manage the Departments associated with any specific Organization (for which they are assigned rights to) by clicking the Departments button after selecting it beside the Organization name from the Organizations interface. Refer to **5.2.2.7 Managing Departments of an Organization** for more details. The 'Departments' area is, in effect, a limited view of the information available in 'Organizations' area - containing data and controls relating to the Department that the DRAO is responsible for.



The 'Departments' area is similar to the 'Departments' dialog that appears on clicking the Departments button for a selected Organization from the 'Organizations' interface. Detailed explanations on the options and controls in this area are available at **4.2.2.7 Managing Departments of an Organization**.

5.4 Domains

5.4.1 Section Overview

The 'Domains' tab allows Administrators to view the list of domains associated with the Organizations that are enrolled with CCM and the Departments within the Organizations. The Administrators can also create new domains, initiate Domain Control Validation (DCV) and delegate/re-delegate existing domains to the required Organizations/Departments and restrict the certificate types that can be offered for the domains, depending on the purpose(s) for which its use is authorized, from this interface.

- MRAO Administrator - can create, edit and delegate a domain to any Organization or Department. They can also request, approve and manage certificates for any domain. The domains created by MRAO are automatically approved.
- RAO Administrator - can create, edit and delegate domains to Organizations (and any subordinate Departments) that have been delegated to them. Can also initiate DCV, request, approve and manage certificates for such domains. The domains created or approved by RAO are to be validated and 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 just a single MRAO'.
- DRAO Administrator - can create, edit and delegate domains to the Department that have been delegated to them. 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. If 'Allow domain validation without Dual Approval' was selected during the MRAO creation process, then requests can be approved by just a single MRAO. The 'Domain Awaiting Approval' notification will be sent to MRAO only after the domain created by DRAO is first approved by RAO.

Note: Dual MRAO Approval for created Domains and Domain Control Validation (DCV) options will be visible only if the respective features are enabled for your account.

The following table provides a summary of the ability of Administrator types to manage Domains:

Action	MRAO Administrator	RAO Administrator	DRAO Administrator
Creating Domains	✓	✓	✓
Initiate Domain Control Validation (DCV)	✓	✓	✓
Delegating Domains	Can delegate domains to any Organization/Department	Can delegate domains only to those Organizations/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	✓	✓ Can approve domains created by DRAO Administrators of the Departments under the Organization, prior to approval by the MRAO.	✗

Note: A single domain can be delegated to more than one Organization/Department as per requirements.

5.4.1.1 Wildcard Domains

When a wildcard domain is created and delegated to an organization or a department, and is validated by MRAO, then the primary domain and all the sub-domains belonging to it are automatically validated only for the same organization or the department. For example, if *.example.com is delegated and validated for a specific organization 'Test Organization', then all the sub-domains such as anything.example.com and something.example.com are automatically validated and approved for the 'Test Organization'.

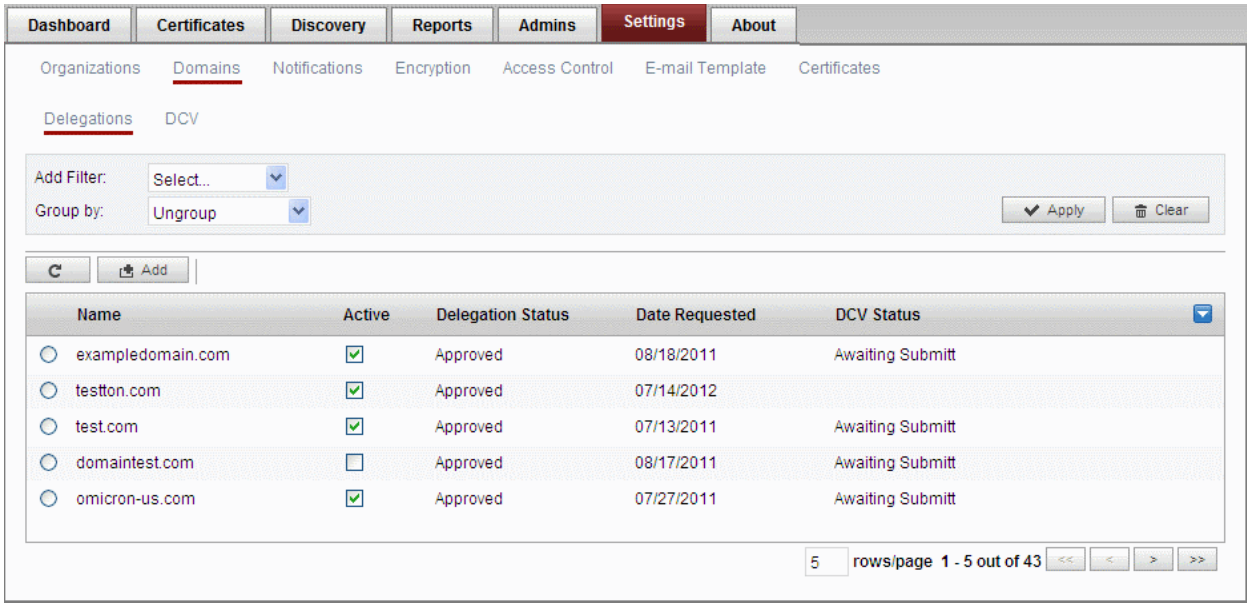
If the sub-domains of a primary domain delegated to an organization or department are to be delegated to other organizations or departments, they need to be validated and approved by the MRAO. For example, if *.example.com is delegated and validated for a specific organization 'Test Organization' and:

- If an RAO wants to re-delegate the sub-domain(s) such as anything.example.com and something.example.com to other organization 'Demo Organization' then the re-delegation needs to be validated and approved by the MRAO.
- If a DRAO wants to re-delegate the sub domain(s) such as anything.example.com and something.example.com to a department 'Test Department' (a department that belongs to the same organization) then the re-delegation needs to be validated and approved by the RAO.

5.4.2 Domain Management

5.4.2.1 The Domains Area

Click the 'Domains' sub-tab of the 'Settings' tab to open the Domain management area:



The Domain management area is divided into two areas accessible by clicking the respective tabs at the top left:

- **Delegations** - Displays a list of all enrolled domains with their delegation status and controls to approve delegate/re-delegate them.
- **DCV** - Displays list of enrolled domains as a tree structure with their Domain Control Validation (DCV) status and controls to initiate the DCV process.

Note: Domain Control Validation (DCV) tab will be visible only if the DCV feature is enabled for your account.

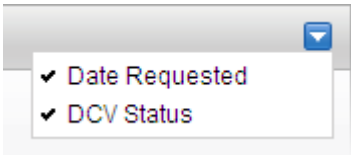
5.4.2.1.1 Domain Delegations

The Domain Delegations area is displayed by default under Domains > Settings and displays a list of requested and approved domains.

- MRAO Administrator - can add new domains, view all the requested and approved domains with their delegation and DCV status. The MRAO Administrator can also view the full details of a domain, delegate/re-delegate domains to required Organizations/Departments, Approve domains requested by RAO and DRAO Administrators. Domains added by MRAO Administrators are automatically approved. MRAO administrators can also view domains without delegation that were added by RAO and DRAO administrators and delegate to required organizations/departments.
- RAO Administrator - can add new domains to the Organizations that have been delegated to them, view the requested and approved domains delegated to their Organizations with their delegation and DCV status. The RAO Administrator can also view the full details of a domain, delegate/re-delegate domains to their Organizations/Departments, Approve domains requested by DRAO Administrators. The domains created or approved by RAO are 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 just a single MRAO'.
- DRAO Administrator - can add new domains to the Departments that have been delegated to them, view the requested and approved domains delegated to their Departments with their delegation and DCV status. The DRAO Administrator can also view the full details of a domain, delegate/re-delegate domains to their Departments. 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. If 'Allow domain validation without Dual Approval' was selected during the MRAO creation process, then requests can be approved by just a single MRAO'. The 'Domain Awaiting Approval' notification will be sent to MRAO only after the domain created by DRAO is first approved by RAO.

5.4.2.1.1.1 Summary of Fields and Controls

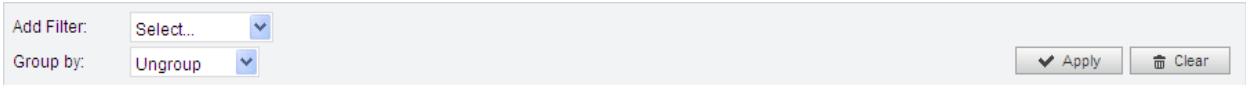
Column Display		Description

Name		A list of all available Domains created for this account. List is displayed in ascending alphabetical order. The domains which are awaiting approval are displayed in red.
Active		The checkbox allows the administrator to toggle the domain between the active and inactive states. If this is made inactive, the status of the domain will be shown as suspended.
Delegation Status		Indicates the request/approval status of the domain.
Date Requested		Indicates the date on which the domain was requested.
DCV Status		Indicates the validation status of the domain. **Note:** DCV Status column will be visible only if the respective feature is enabled for your account.
Note: An administrator can enable or disable the columns from the drop-down button beside the last item in the table header: 		
Controls		Contains controls that allow MRAO and RAO administrators to add new domains, delegate any existing domain to an Organization/Department and MRAO Administrators to validate and approve the newly created Domains. DRAO Administrators can only create Domains and associate it to the Departments that have been delegated to them.
	Add	Enables administrators to create a new Domains to be associated with the existing Organizations and Departments, for the purposes of issuing certificates to end-users
	Refresh	Updates the list of displayed Domains.
Domain Control Buttons **Note**: The Domain control buttons are visible only on selecting a domain	View	Enables administrators 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 administrators to associate or delegate an existing domain to Organizations and Departments as required. **Note**: This control is not visible to DRAO Administrators.
	Delete	Deletes the domain. This control is available only for domains yet to be approved.

5.4.2.1.1.2 Sorting and Filtering Options

- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective column

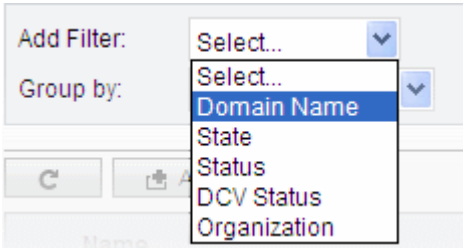
Administrators can search for particular domain by using filters:



Filter Options	Description
Domain Name	Enables Administrators to filter the list of Domains by name.
State	Enables Administrators to filter the list of Domains based on their active state: ANY - Displays the list of all the domains; Active - Displays the list of Domains which are currently active, as set by the administrator. Inactive - Displays the list of Domains which are currently inactive, as set by the administrator.
Status	Enables Administrators to filter the list of Domains based on their status:

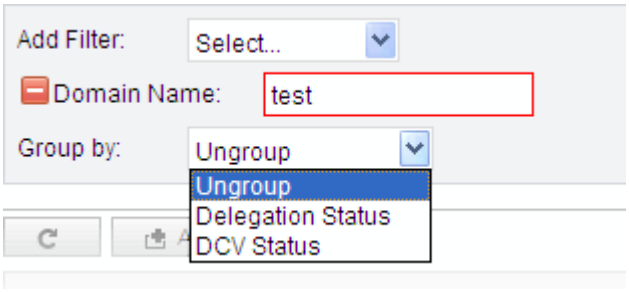
	ANY - Displays the list of all the domains; Requested - Displays the list the domains which are requested and awaiting for approval by MRAO. Approved - Displays the list of Domains which are already approved by the MRAO.
Organization	Enables to filter only the domains associated with the Organization selected from the drop-down menu. **Note**: This Field is not visible to RAO and DRAO Administrators.

You can add filters by selecting from the options in the 'Add Filter' drop-down. For example, if you want to filter the domain with the domain name, select 'Domain Name':



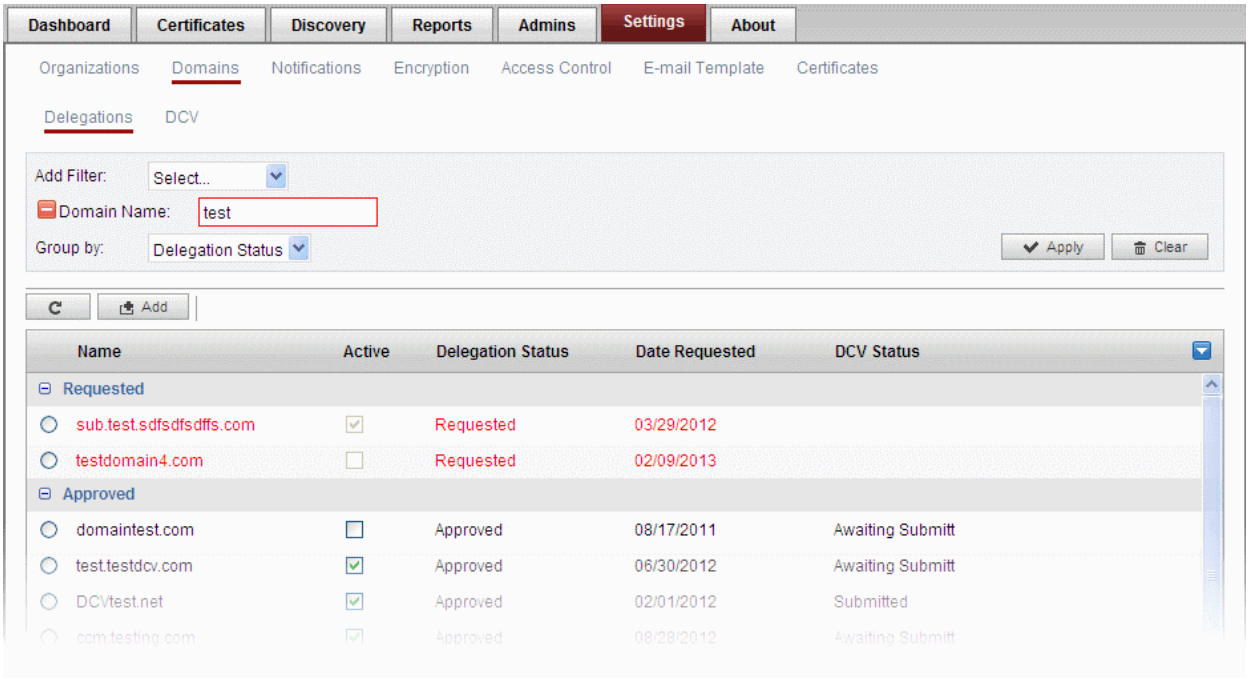
- Enter part or full name in the Name field.

- If you want to group the results based on their delegation status or their DCV status, select the option from the 'Group by' drop-down.



- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed:

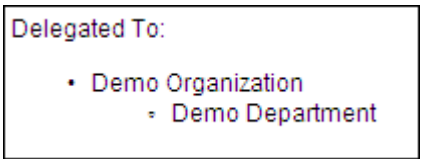


- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Domains' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

5.4.2.1.1.3 Tool Tip

On pointing the mouse cursor over a domain, the Organizations/Departments to which the domain is delegated is displayed as a tool tip. Also if the domain is re-delegated to another Organization/Department, and awaits approval from the MRAO, the awaiting status is also displayed.



5.4.2.1.2 DCV

The DCV area of the Domains interface displays a list of registered domains along with their DCV status and expiration dates. From this interface, MRAOs can initiate the DCV process on any domain. Domains enrolled by RAO/DRAO SSL Administrators are to be approved by MRAO Administrators before being subject to validation.

- MRAO Administrator - can initiate DCV process for all registered Domains.
- RAO Administrator - can initiate DCV process for the domains delegated to the Organizations that are administrated by them.
- DRAO Administrator - can initiate DCV process for domains delegated to the Departments that are administrated by them.

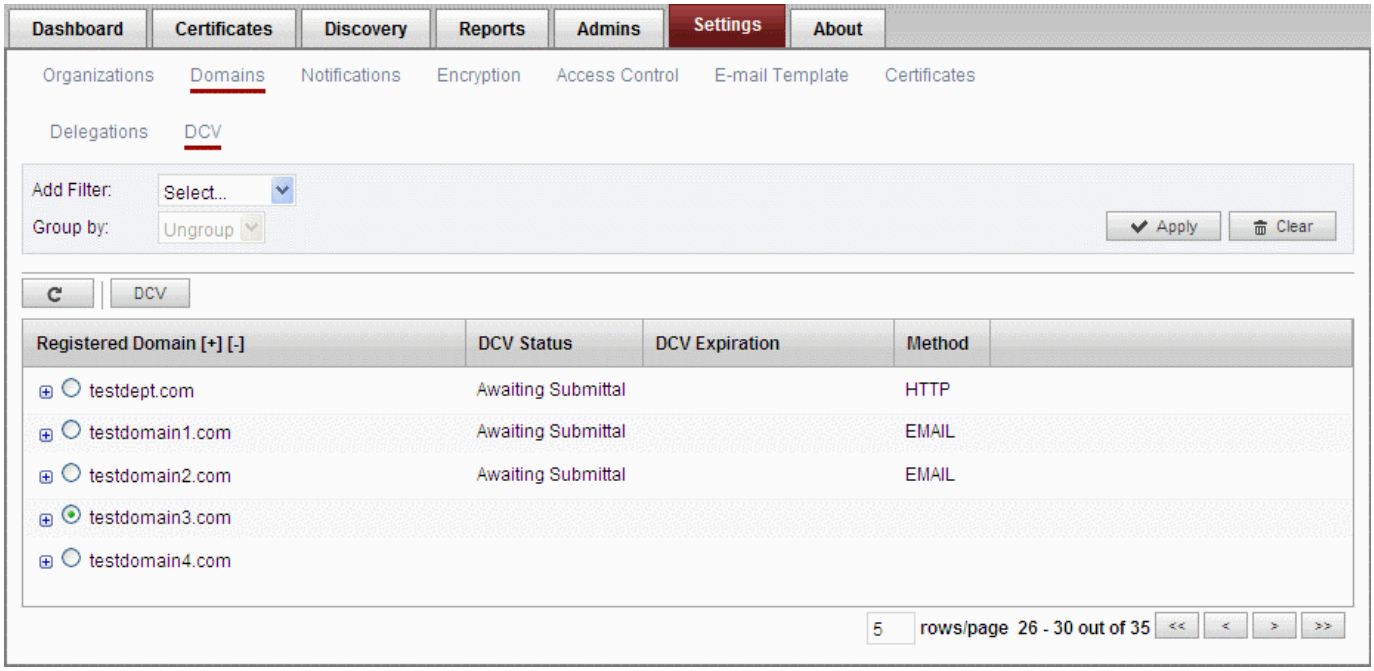
The Administrator can choose anyone from the three methods to initiate DCV process for a domain:

- Email - CCM will send an automated email with a validation link to the email address of the domain administrator. The domain will be validated on the domain administrator visiting the validation link in the mail.
- DNS CNAME - CCM will send a hash value that must be entered as DNC CNAME for the domain. CCM will validate by checking the DNS CNAME of the domain
- HTTP/HTTPS File - CCM will send a .txt file which is to be placed at the root of the web server. CCM will validate the domain based on the presence of the sent file

If a wildcard domain is created and delegated to an Organization or a Department, CCM will validate only the registered High

Level Domain (HLD). If the HLD is successfully validated, all the sub domains within the name space of the HLD will be considered validated.

For more details on initiating DCV process, refer to the section **Validating the Domain**.



5.4.2.1.2.1 Summary of Fields and Controls

Column Display	Description
Registered Domain	A list of all available Domains created for this account. Clicking the '+' beside a domain name displays the sub-domains of the registered domain.

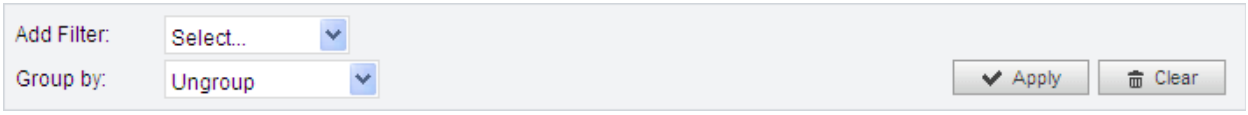
DCV Status	Indicates the validation status of the domain. The status can be one of the following:
	• Not Started - The DCV process has not been initiated for the registered high level domain (HLD).
	• Awaiting Submittal - The DCV process has been initiated but the request has not yet been submitted to the Domain Administrator. This status will be available only for the following DCV methods:
	  • HTTP / HTTPS
	  • CNAME
	• Submitted - The DCV request has been submitted to the domain administrator.
	• Validated - The registered high level domain (HLD) has been successfully validated
	• Expired - The DCV request has expired for the HLD.

DCV Expiration	Indicates the expiry date of the DCV request.
Method	Indicates the DCV method chosen by the administrator for validating the domain.
DCV Control Button **Note**: The DCV Control button appears only on selecting a domain.	Enables the MRAO and RAO/DRAO SSL Administrators to initiate or restart the DCV process for the selected Domain.

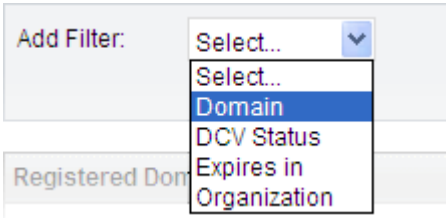
5.4.2.1.2.2 Sorting and Filtering Options

- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective column

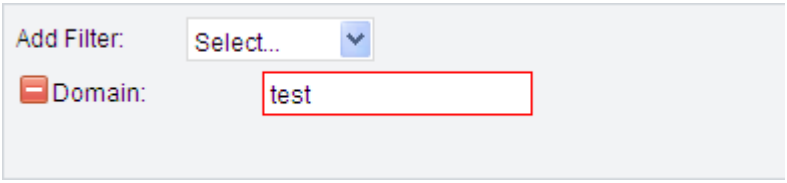
Administrators can search for particular domain by using filters:



You can add filters by selecting from the options in the 'Add Filter' drop-down. For example, if you want to filter the domain with the domain name, select 'Domain':



- Enter part or full name in the Name field.

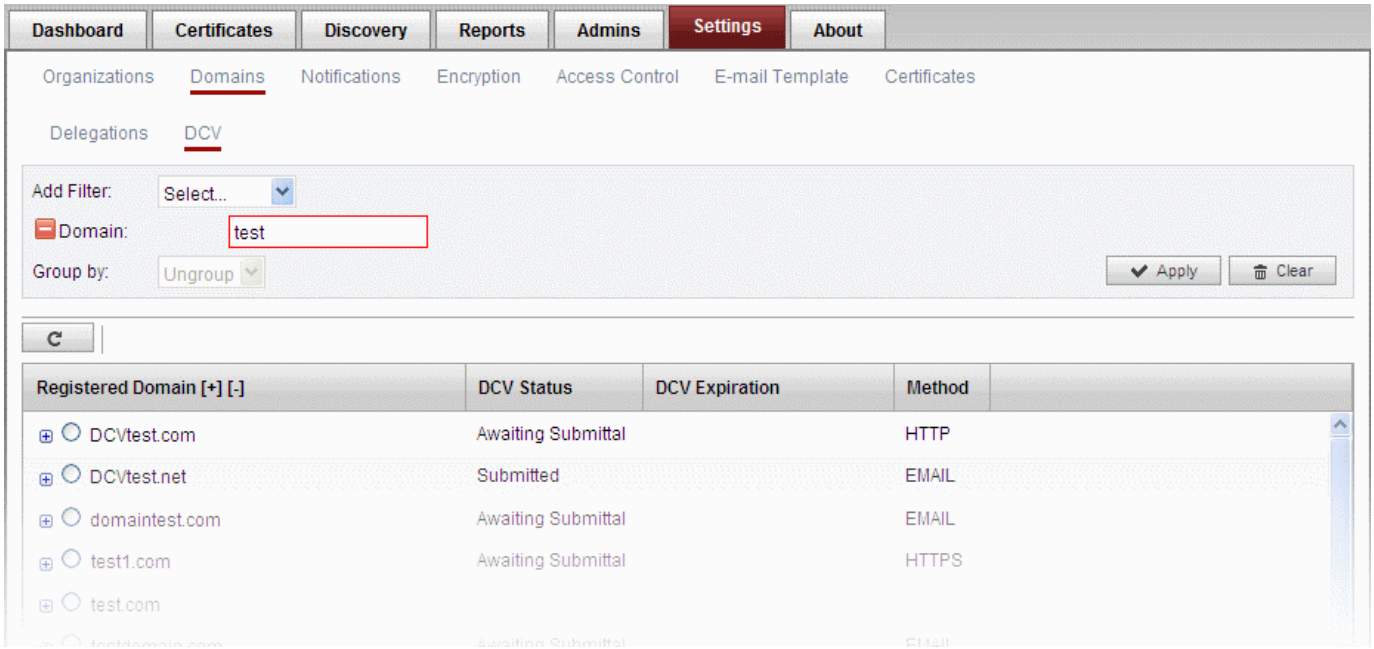


The available filter criteria and their filter parameters are given in the following table:

Filter Options	Description
Domain	Enables Administrators to filter the list of Domains by name.
DCV Status	Enables Administrators to filter the list of Domains based on their DCV status: • ANY - Displays the list of all the domains; • Not Started - Displays only the Domains for which the. DCV process has not yet been started. • Awaiting Submittal - Displays only the Domains for which the DCV process has started but the request has not yet been submitted to the Domain Administrator. • Submitted - Displays only the Domains for which the DCV request has been submitted to the domain administrator. • Validated - Displays only the Domains for which the validation has been successfully completed • Expired - Displays only the domains for which the DCV request has expired
Expires in	Enables Administrators to filter the list of Domains based on the remaining days for their DCV expiry. The administrator can choose the domains to be listed, whose DCV request expires in: • Any • Next 3 days • Next 7 days • Next 14 days • Next 30 days • Next 60 days • Next 90 days
Organization	Enables to filter only the domains associated with the Organization selected from the drop-down menu. **Note**: This Field is not visible to RAO and DRAO Administrators.

- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed:



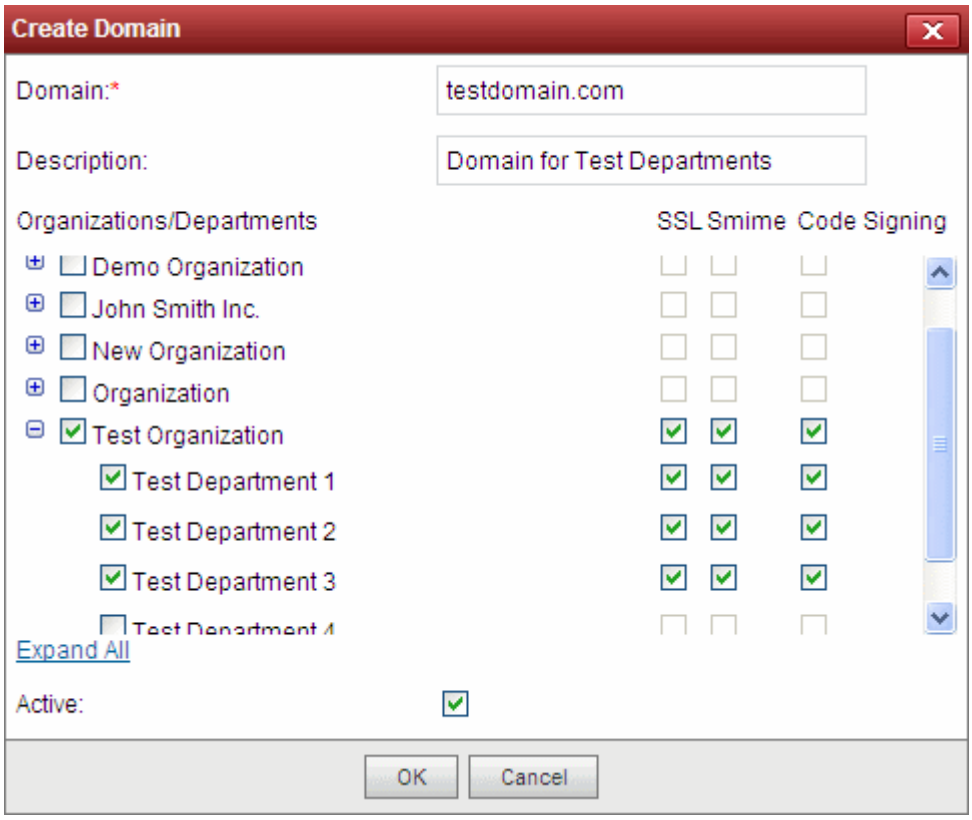
- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Domains' > 'DCV' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

5.4.2.2 Creating a New Domain

In order to request, approve and manage all the company's certificates, the administrator should first create domains corresponding to different Organizations/Departments of the company. These domains are to be delegated to respective Departments and/or Organizations delegated to them. The delegated domains are to be validated through Domain Control Validation process, which is to be initiated by MRAO or an RAO/DRAO SSL with the 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. The administrator 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 click the 'Add' button located at the top of the 'Domains' area. This will open the 'Create domain' dialog.



5.4.2.2.1 Create Domain - Table of Parameters

Field Name	Values	Description
Domain	String (required)	The name of the Domain
Description	String	A short description of the domain.
Organizations/Departments	Checkboxes	Enables the administrator to delegate the currently created domain to an Organization/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 to the Organization(s) and/or the Department(s) by selecting the respective checkbox(es). A single domain can be delegated to more than one Organization/Department. Clicking on 'Expand All' expands the tree structure to display all the Departments under each Organization. Clicking on 'Collapse All' in the expanded view collapses the tree structure of all the Organizations and hides the Departments under each Organization.
SSL, Smime, Code Signing	Checkboxes	Enables the administrator to allow or restrict the types of certificates that can be requested for the created domain, by checking or unchecking the respective checkboxes. The certificate types can be restricted according to the purpose of the domain created.
Active	Checkbox	Enables the administrator to toggle the status of the domain between active and inactive states. Default = Active state.

5.4.2.2.2 Validating the Domain

Upon creation of a new domain, it must be approved and subjected to Domain Control Validation (DCV) process by an appropriately privileged administrator.

- MRAO Administrator - can initiate DCV process for all registered Domains.
- RAO Administrator - can initiate DCV process for the domains delegated to the Organizations that are administrated by them.
- DRAO Administrator - can initiate DCV process for domains delegated to the Departments that are administrated by them.

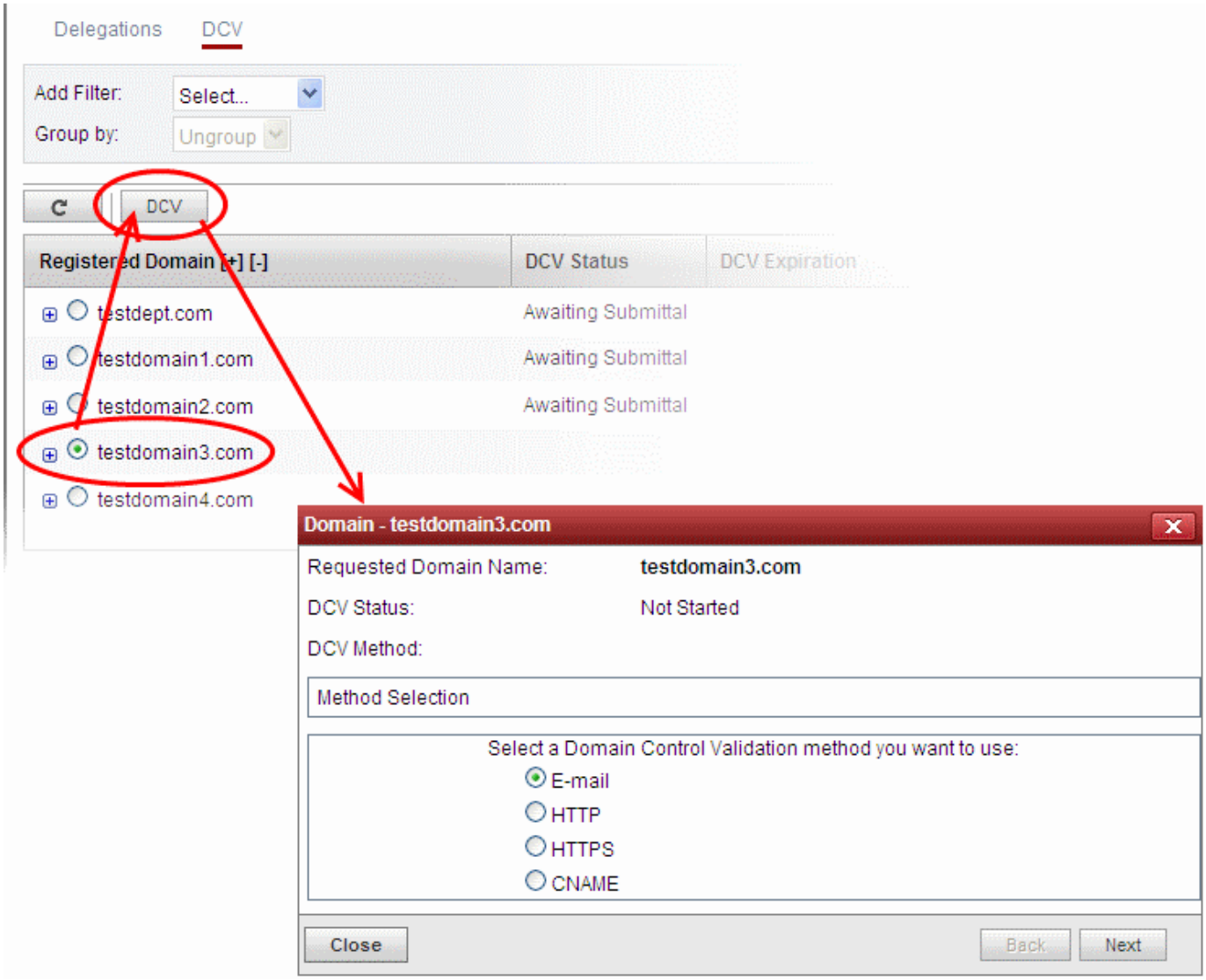
CCM enables the Administrator to initiate DCV process by three methods:

- Email - CCM will send an automated email with a validation link to the selected email address of the domain administrator. The domain will be validated on the domain administrator visiting the validation url in the mail.
- DNS CNAME - CCM will send a hash value that must be entered as DNC CNAME for the domain. CCM will validate by checking the DNS CNAME of the domain
- HTTP/HTTPS File - CCM will send a .txt file which is to be placed at the root of the web server. CCM will validate the domain based on the presence of the sent file

If a wildcard domain is created and delegated to an Organization or a Department, CCM will validate only the registered High Level Domain (HLD). If the HLD is successfully validated, all the sub domains within the name space of the HLD will be considered validated.

To initiate DCV for a Domain

1. Open the DCV interface by clicking Settings > Domains > DCV.
2. Next, initiate DCV by selecting the domain and clicking the 'DCV' button that appears at the top. This will open the DCV wizard:



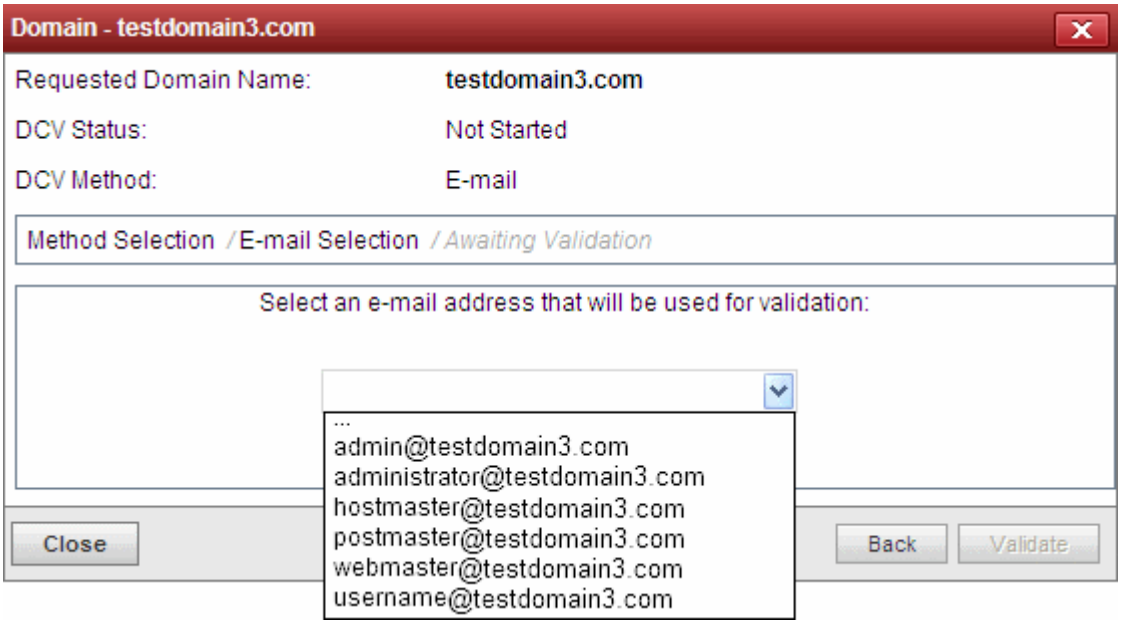
Select the DCV method from:

- **Email**
- **HTTP/HTTPS**
- **CNAME**

... and click 'Next'

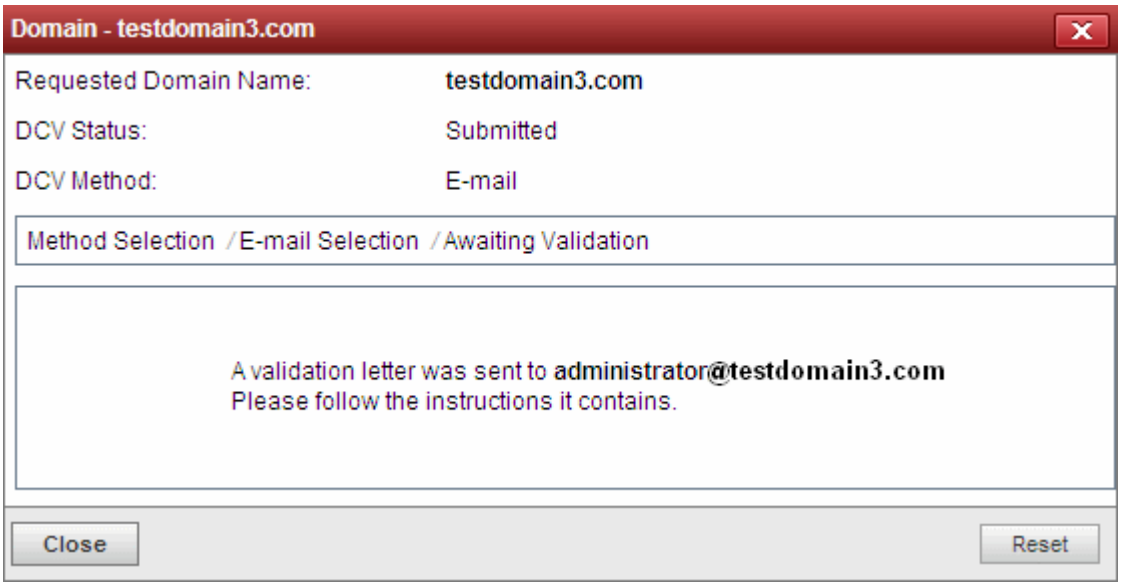
Email

On selection of EMAIL method, the next step allows you to select the email address of the Domain Administrator for sending the validation email.



3. Select the email address of the administrator who can receive and respond to the validation mail from the drop-down and click 'Validate'.

An automated email will be sent to the selected Domain Administrator email address. The DCV status of the Domain will change to 'Submitted'.

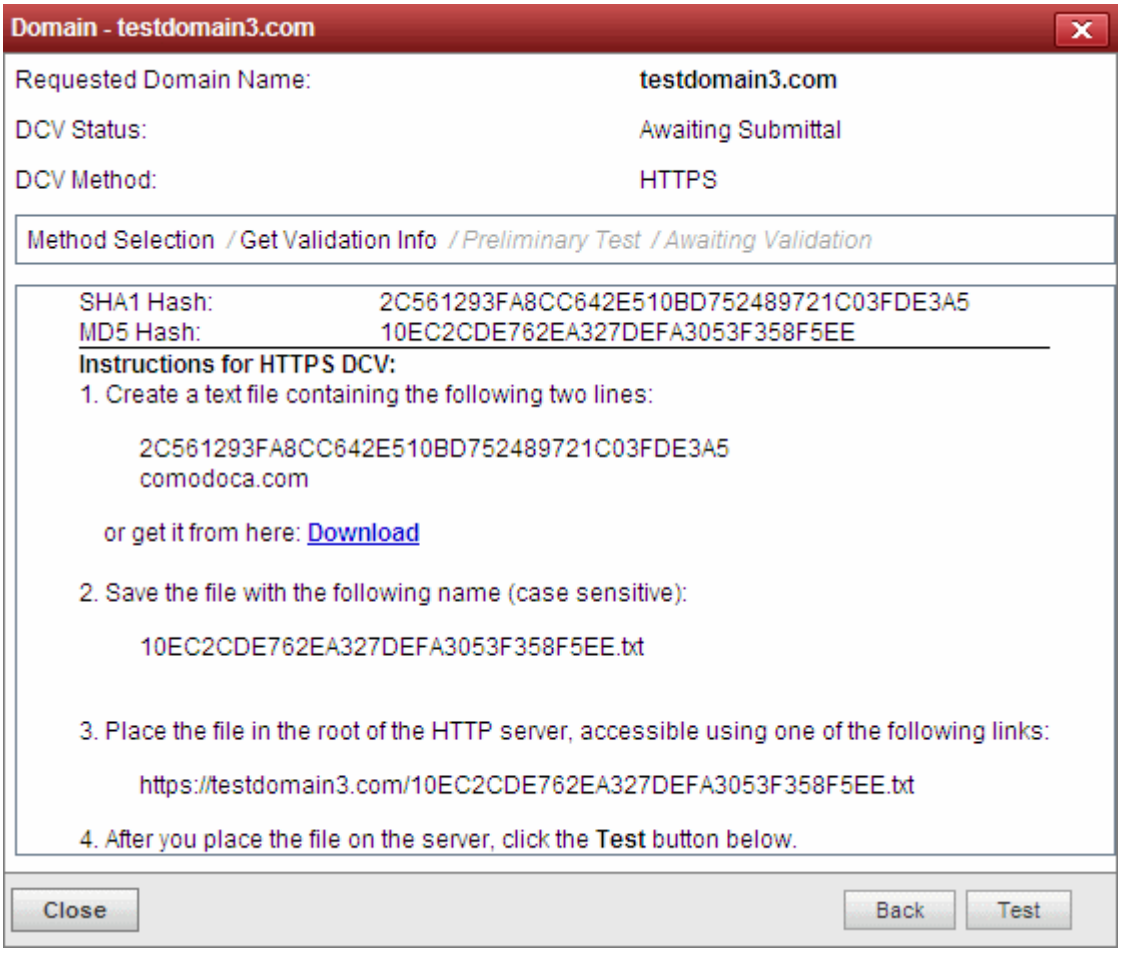


On receiving the email, the domain administrator should click the validation link in it and enter the validation code in the

validation from that appears on clicking the validation link in order to complete the validation process. Once completed, the DCV status of the Domain will change to 'Validated'

HTTP/HTTPS

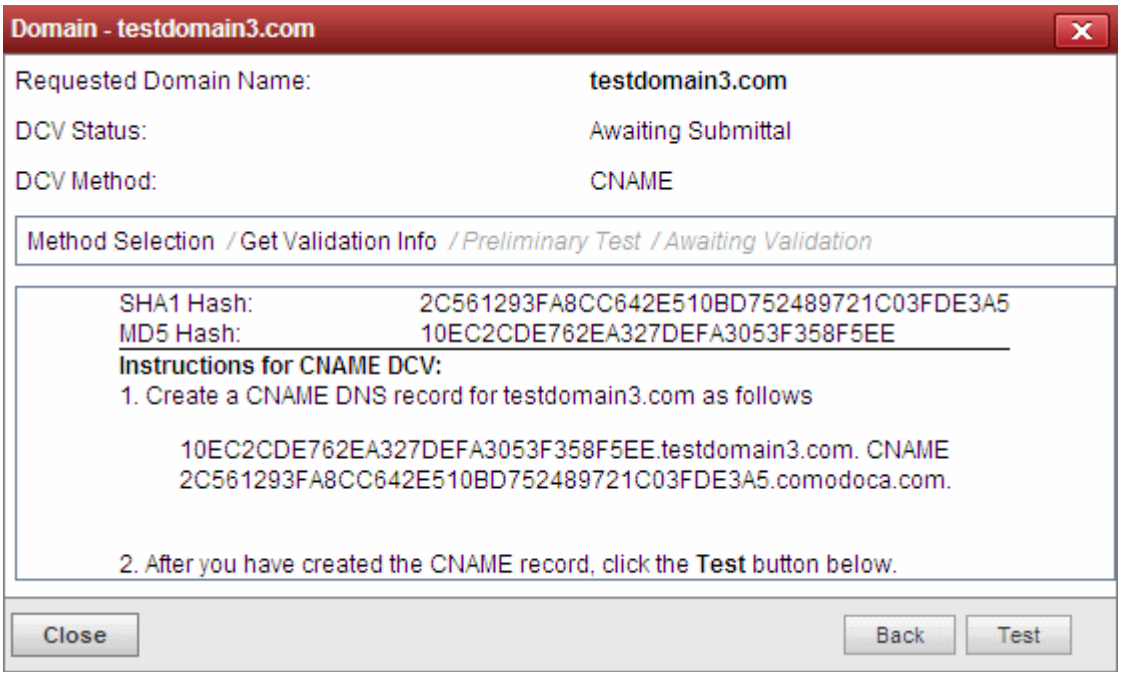
On selection of HTTP or HTTPS method, the next step allows you to download the .txt file for sending to the Domain Administrator. CCM creates a Hash value for the .txt file and stores it for future reference on validating the domain. The DCV status of the Domain will be changed to 'Awaiting Submittal'.



3. Click 'Download' and save the .txt file or create a new notepad file, copy and paste the string given in item 1 and save the file with the name given in item 2.
4. Click Close. CCM will save the hash value generated for future comparison
5. Send the .txt file to the Domain Administrator through any out-of-band communication method like email and request the domain administrator to place the file in the root of the HTTP/HTTPS server, so that the file is accessible by one of the paths specified in item 3.
6. Once the Domain Administrator has placed the .txt file on the HTTP HTTPS server, open the DCV interface by clicking Settings > Domains > DCV tab
7. Resume the DCV process by clicking the DCV button in the row of the Domain
8. Click 'Test' to check whether the file has been placed in the web server root. If the file is present, the DCV Submission dialog will appear. Click 'Submit'. The DCV status of the domain will change to 'Submitted'
9. CCM will validate the Domain on successful submission and the DCV status of the domain will change to 'Validated'.

DNS CName

On selection of CNAME method, CCM creates a DNS CNAME record for the requested domain and stores its hash value for future reference. The next step allows you to get the DNS CNAME record for the requested domain. The DCV status of the Domain will be changed to 'Awaiting Submittal'.



3. Copy the CNAME DNS record given in item no. 1 and pass it to the domain administrator through out-of-band communication method like email and request the domain administrator to create the record for the domain.
4. Click Close. CCM will save the hash value generated for future comparison
5. After the Domain Administrator has created the record, open the DCV interface by clicking Settings > Domains > DCV tab
6. Resume the DCV process by clicking the DCV button in the row of the Domain
7. Click 'Test' to check whether the record has been created. If it is created, the DCV Submission dialog will appear. Click 'Submit'. The DCV status of the domain will change to 'Submitted'
8. CCM will validate the Domain on successful submission and the DCV status of the domain will change to 'Validated'.

5.4.2.2.1 Changing DCV method for Validation Pending Domains

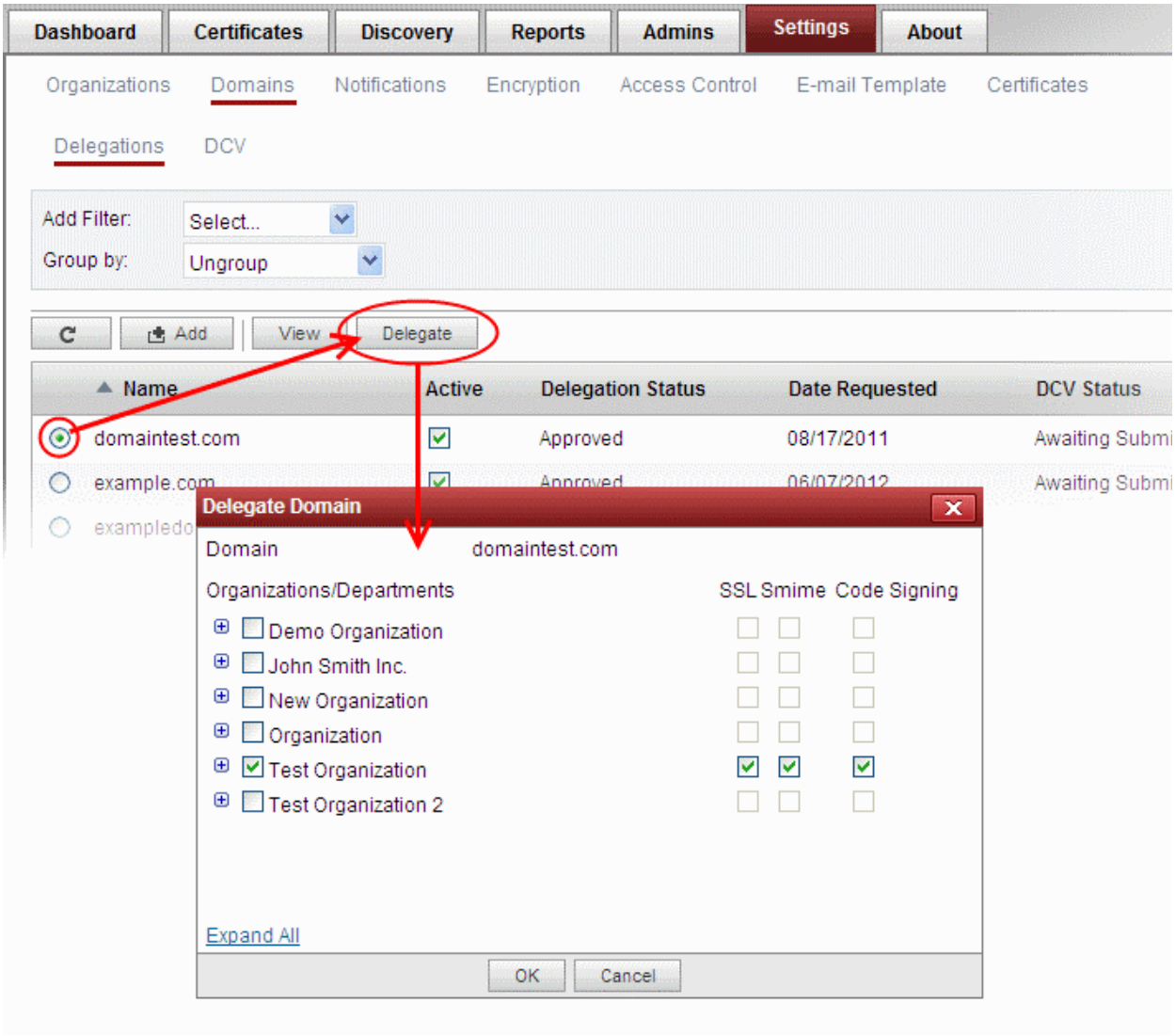
The MRAO or RAO/DRAO SSL Administrator with appropriate privileges can change the DCV method for the domains whose validation is pending, from the DCV interface.

To change the validation method

1. Open the DCV interface by clicking Settings > Domains > DCV.
2. Click the 'DCV' button in the row of the domain with DCV status is 'Awaiting Submittal' or 'Submitted'. The DCV wizard will start.
3. Click 'Back' The wizard will move to the previous step of selecting the DCV method
4. Select the new DCV method and continue the process as explained in the section **Validating the Domain**.

5.4.2.3 Delegating/Re-delegating an Existing Domain

The administrator can delegate or re-delegate the domain to Organizations/Departments according to the requirement from the 'Domains' > 'Delegate' area. Selecting the domain and clicking 'Delegate' button from the top opens the 'Delegate Domain' interface that allows the administrator to delegate or re-delegate the domain. The screen also displays domains that were added by RAO and DRAO administrators without delegating them to any organizations/departments. The administrator can delegate these domains to the required organizations/departments. The administrator can also select the certificates to be made available for the domain on delegation to the specific Organization/Department based on purpose of delegating the domain to the Organization/Department.



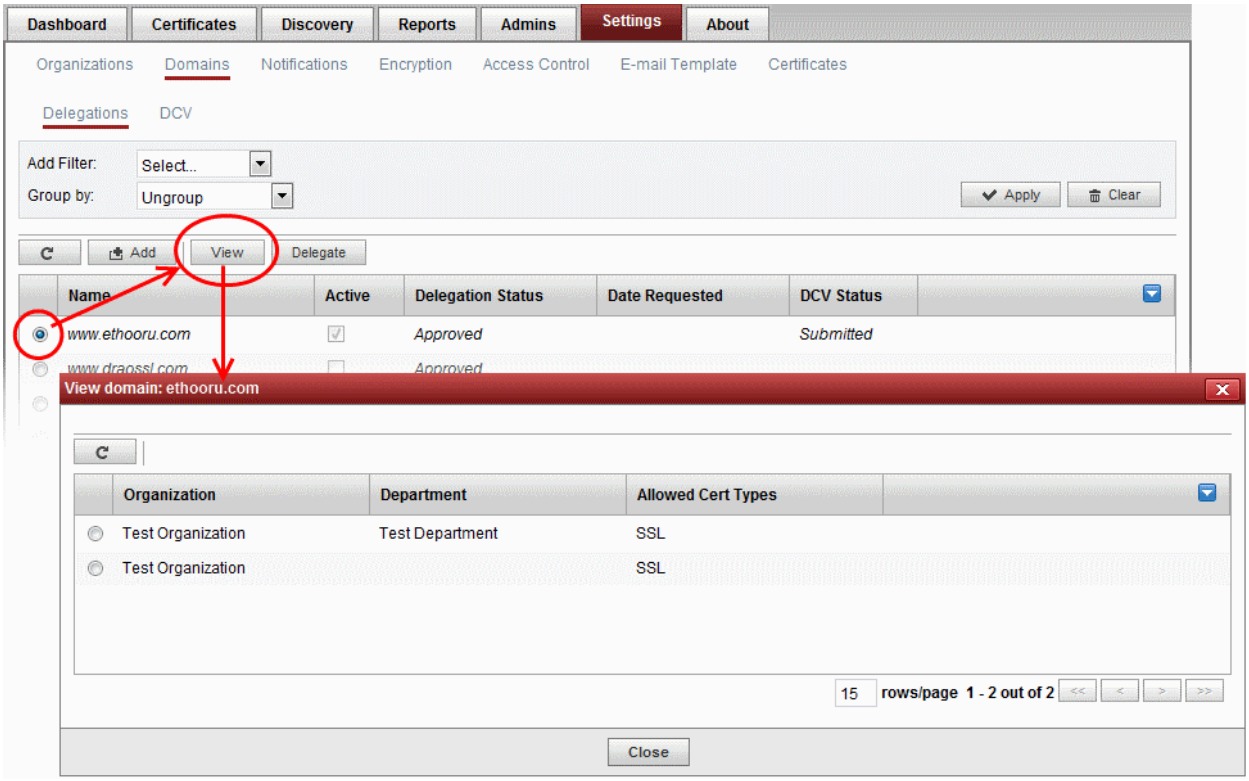
Also the administrator can validate the domain before delegating/re-delegating it specific Organization/Department by clicking the 'Validate' link. Clicking the link enables the administrator to send an automated email to the domain control administrator to check the domain control authority. See **Validating the Domain** for more details.

The domains delegated/re-delegated by the MRAO is activated immediately, but the domains delegated by other administrators are to be approved by the MRAO to become active.

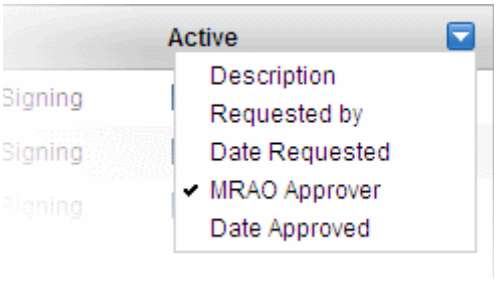
Full details on delegating a domain are available in the previous section, '**Create Domain - Table of Parameters**'

5.4.2.4 Viewing, Validating and Approving Newly Created Domains

The list of the Organization(s) and Department(s) to which a domain has been delegated and the certificate types enabled for them can be viewed by the appropriately privileged administrator by selecting the domain and clicking the 'View' button from the top. The view dialog also enables the administrators 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 enables for request and issuance of SSL certificates, Client certificates and Code Signing certificates.



5.4.2.4.1 View Domain - Summary of Fields and Controls

Column Display	Description
Organization	The Organization(s) to which the domain has been delegated. The delegations which are pending approval by the MRAO are displayed in red.
Department	The Department(s) to which the domain has been delegated. The delegations which are pending approval by the MRAO are displayed in red.
Description	Provides a short description of the domain as entered during creation of the domain by the administrator.
Requested by	Displays the name of the administrator who has created the domain.
Date Requested	The date at which the domain was added to CCM.
MRAO Approver	Displays the name of the MRAO administrator who has approved the creation/delegation of the domain.
Date Approved	The date at which the domain was approved by MRAO.
Allowed Cert Types	The Certificate types that are enabled and available for the domain
Note: The administrator can enable or disable the columns from the drop-down button beside the last item in the table header: 	

Controls	Refresh	Updates the list of displayed Organizations and Departments and their details.
Delegation Control Buttons **Note**: The Delegation control buttons are visible only on selecting a domain	Details	Enables the administrator to **view the requisition details** of the domain.
	Approve	Enables MRAO administrator to **approve the creation and delegation of the domain** by RAO and DRAO administrators. **Note**: This control button is visible only for Domains with 'Requested' status and only to MRAO and RAO administrators.
	Reject	Enables MRAO administrator to **decline the creation and delegation of the domain** by RAO and DRAO administrators. **Note**: This control button is visible only for Domains with 'Requested' status and only to MRAO and RAO administrators.

5.4.2.4.2 Approval of Creation and Delegation of Domains

Domains that are created and delegated by:

- MRAO Administrators are automatically validated and approved;
- RAO Administrators are to validated by the MRAO to become active;
- DRAO Administrators are to be first validated and approved by the RAO Administrator of the Organization to which the Department delegated with the domain and then by the MRAO to become active.

Domains which are awaiting approval are displayed in red color in the Domains area of the CCM interface.

The MRAO and RAO Administrator can check the validity of the Domain and approve/reject the request for the Domain.

To approve or reject a domain delegations

- Open the 'View Domain' dialog
- Select the Organization/Department for which the domain delegation has been requested
- Click 'Approve' or 'Reject' button from the top

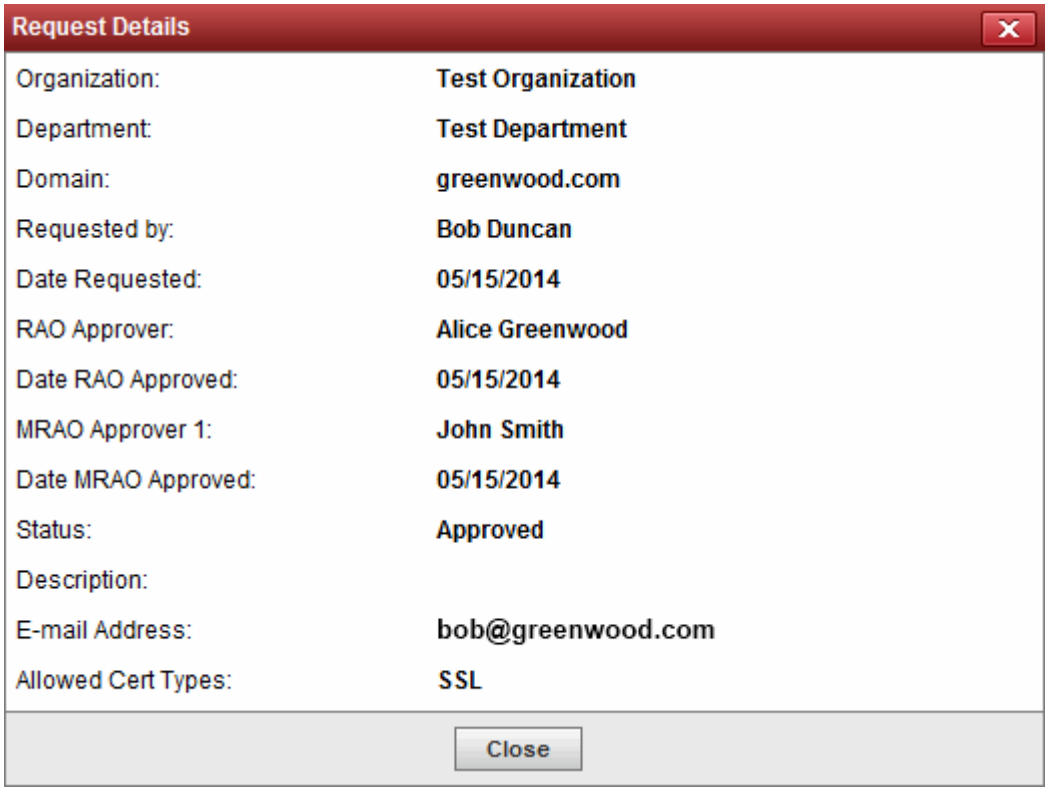
If a domain is created/delegated by a DRAO Administrator, it will be displayed in red only to the RAO Administrator of the Organization to which the Department belongs, indicating it is awaiting approval, in the Domains area of the CCM interface. Once it is validated and approved by the RAO Administrator, it becomes visible to the MRAOs for validation/approval.

If a domain is created by an RAO Administrator, it will be displayed in red to the MRAO Administrators indicating that it is awaiting validation/approval.

Once a requested domain is validated and approved by the MRAO a domain approval notification will be sent and the domain will be enabled for request and issuance of SSL certificates, client certificates and Code Signing certificates.

5.4.2.4.3 Viewing Requisition and Approval Details of a Domain

The administrator can view the request and approval details of the domain delegation by selecting an Organization or a Department and clicking the 'Details' button from the 'View Domain' interface.



5.4.2.4.4 Request Details - Table of Parameters

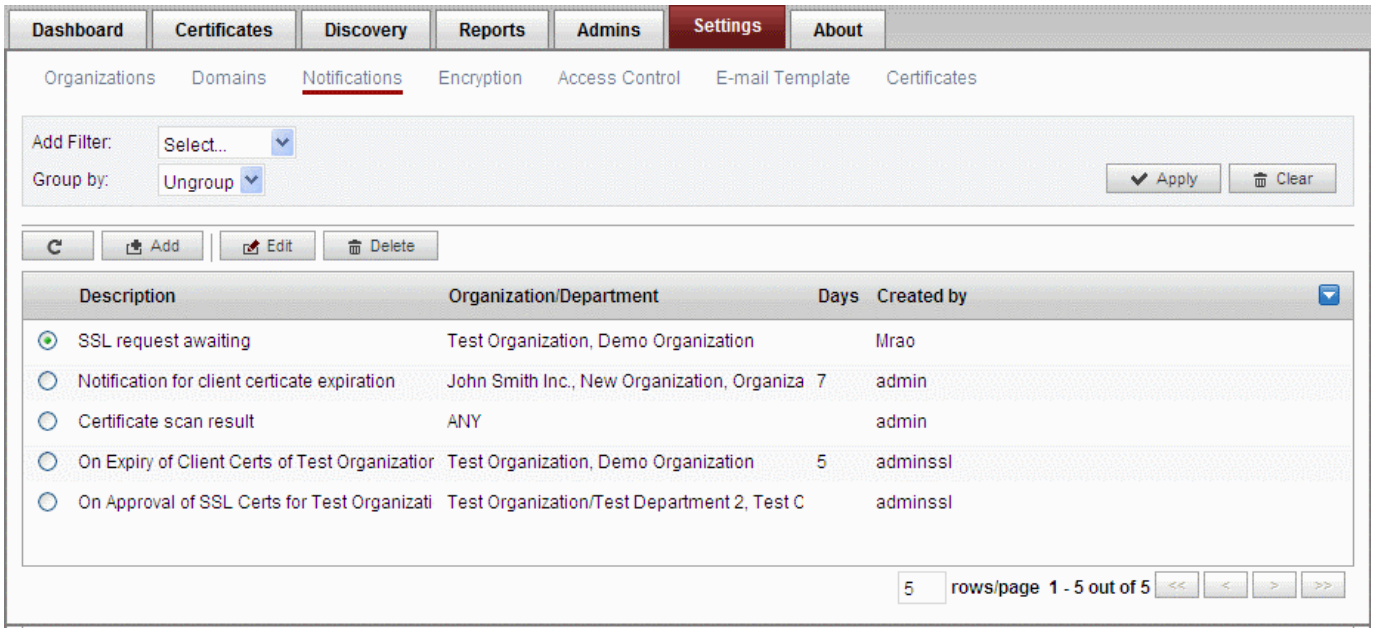
Field	Description
Organization	Indicates the name of the Organization to which the domain is delegated.
Department	Indicates the name of the Department to which the domain is delegated.
Domain	Indicates the name of the selected Domain.
Requested by	The name of the Administrator who has requested for the approval of the delegation of the domain to the Organization/Department .
Date Requested	Date of requisition for delegation.
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 on which the domain was approved by the RAO SSL administrator.
MRAO Approver	The name of the MRAO administrator who approved the domain.
Date MRAO Approved	The date on which 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 it.
E-mail Address	Email address of the administrator who has requested for the delegation of the domain.
Allowed Cert Types	Indicates the Certificate types which could be requested/issued for the domain.

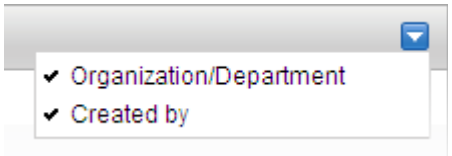
5.5 Notifications

Notifications enable MRAO, RAO and DRAO Administrators to set up and manage email notifications to various personnel - including notifications triggered by SSL certificate status, notifications triggered by Client Certificate status and Discovery Scan Summaries. CCM also enables the Administrators to customize the email templates of the notifications as required. Refer to **Email Templates** for more details.

Administrative Roles:

- MRAO - can see a list of all the notification types set by them, RAO Administrators and DRAO Administrators. They can create new notification types and can edit settings for notification for any Organization and any Department.
- RAO - can only see the notification types set up by them for the users belonging the Organizations (and any subordinate Departments) that have been delegated to them. They can create new notifications and edit settings for notifications only for the notification types on which they have authority AND only for the Organization (and any subordinate Departments) that have been delegated to them.
- DRAO - can only see their own Department(s) in the 'Departments' column. The 'Organizations' area is not visible to DRAOs. They can create new notifications and edit settings for notifications only for the notification types on which they have authority AND only for the Departments that have been delegated to them.



Notifications - Summary of Fields and Controls	
Column Display	**Description**
Description	Provides a short description for the notification, as entered by the administrator during creation.
Organization/Department	The Organization(s)/Department(s) for which the notification was created. The notification mails will be sent to the only to Administrators of these Organization(s)/Department(s).
Days	Number of days in advance of the event, the notification will be sent to the Administrators.
Created by	Displays the name of the administrator who has created the notification.
Note: An administrator can enable or disable the columns from the drop-down button beside the last item in the table header: 	

Control Buttons		
	Add	Enables the Administrator to add a new notification.
	Refresh	Updates the list of displayed Notifications.
Notification Control Buttons **Note**: The Notification control buttons are visible only on selecting a Notification		
	Edit	Enables the administrator to edit the notification. See note below.
	Delete	Enables the Administrator to delete the notification. See note below.

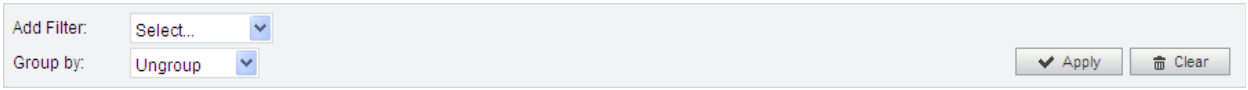
Important Notes:

- An administrator can either edit or delete an existing notification when all the following conditions are true:
- The administrator has authority for all of the organizations and departments contained within the scope of the notification.
- The administrator has authority for the notification type.
- The notification was created at the same or lower level than that of the administrator.

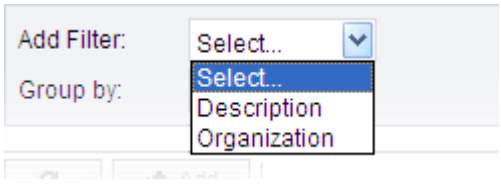
Sorting and Filtering Options

- Clicking on a column headers 'Description' and 'Days' sorts the items in the alphabetical order of the entries in the respective column.

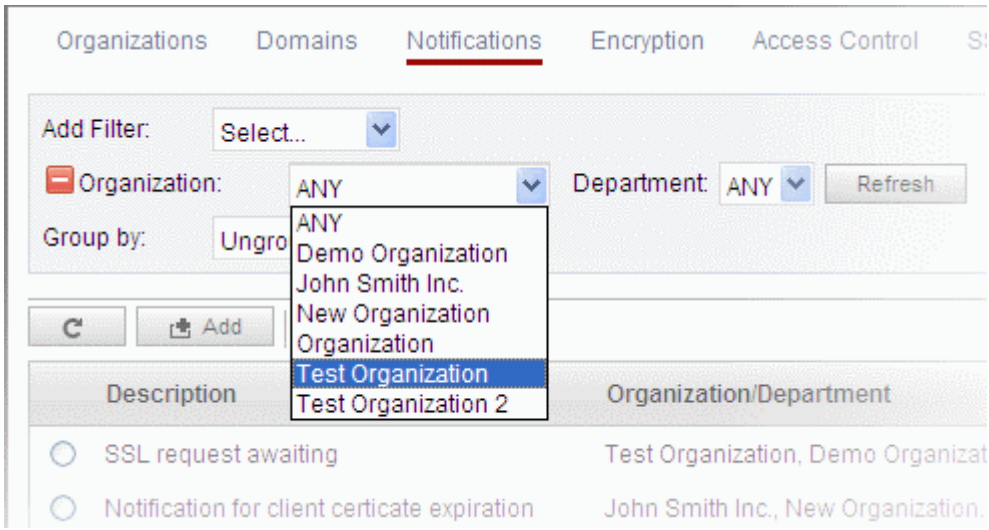
Administrators can search for a particular notification from the list by using filters under the sub-tab:



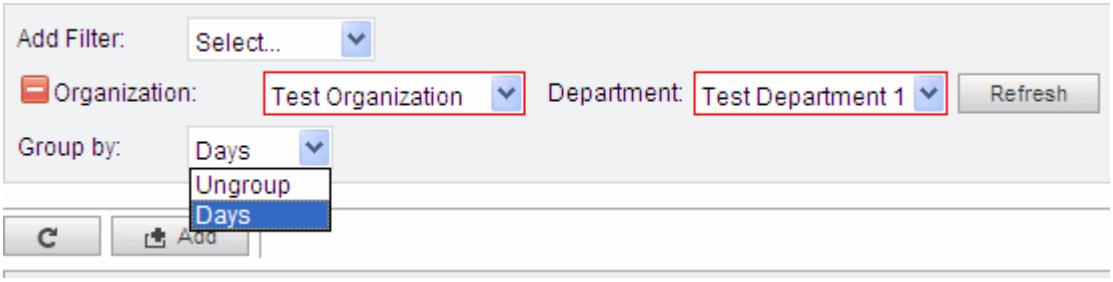
You can add filters by selecting from the options in the 'Add Filter' drop-down and refine the search much further by selecting from the Organization and Department drop-downs. For example, if you want to filter the notification type set for a department, select 'Organization' from the 'Add Filter' drop-down:



- Select the organization and the department from the 'Organization' and 'Department' drop-downs.

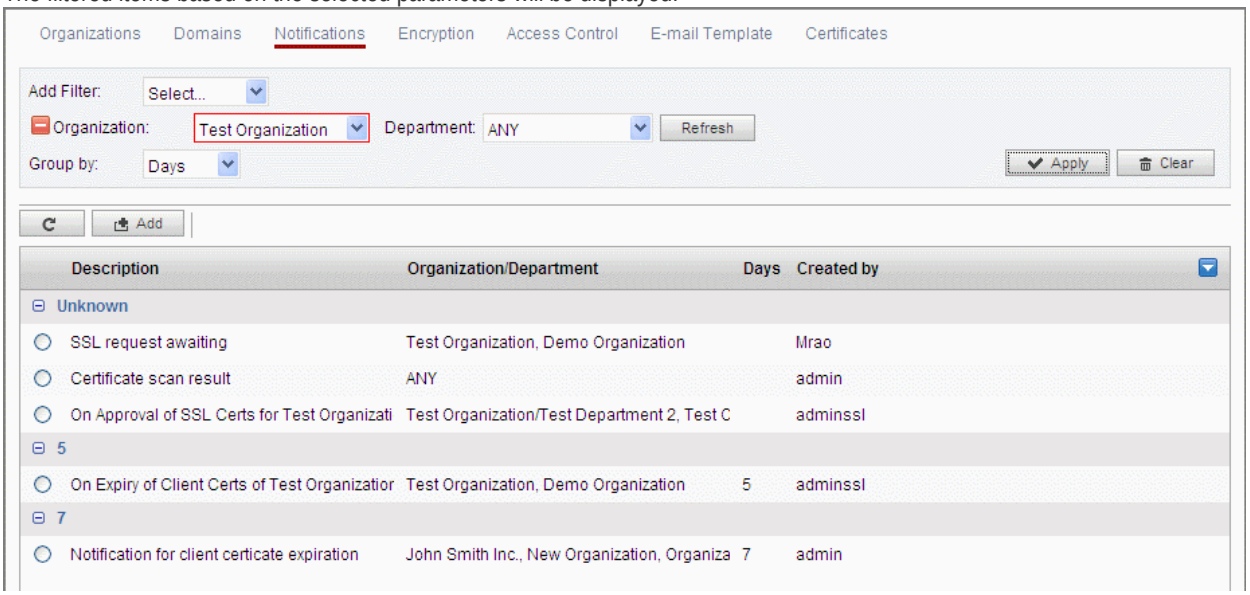


To group the results based on the days parameter, select 'Days' from the 'Group by' drop-down.



- Click the 'Apply' button.

The filtered items based on the selected parameters will be displayed:

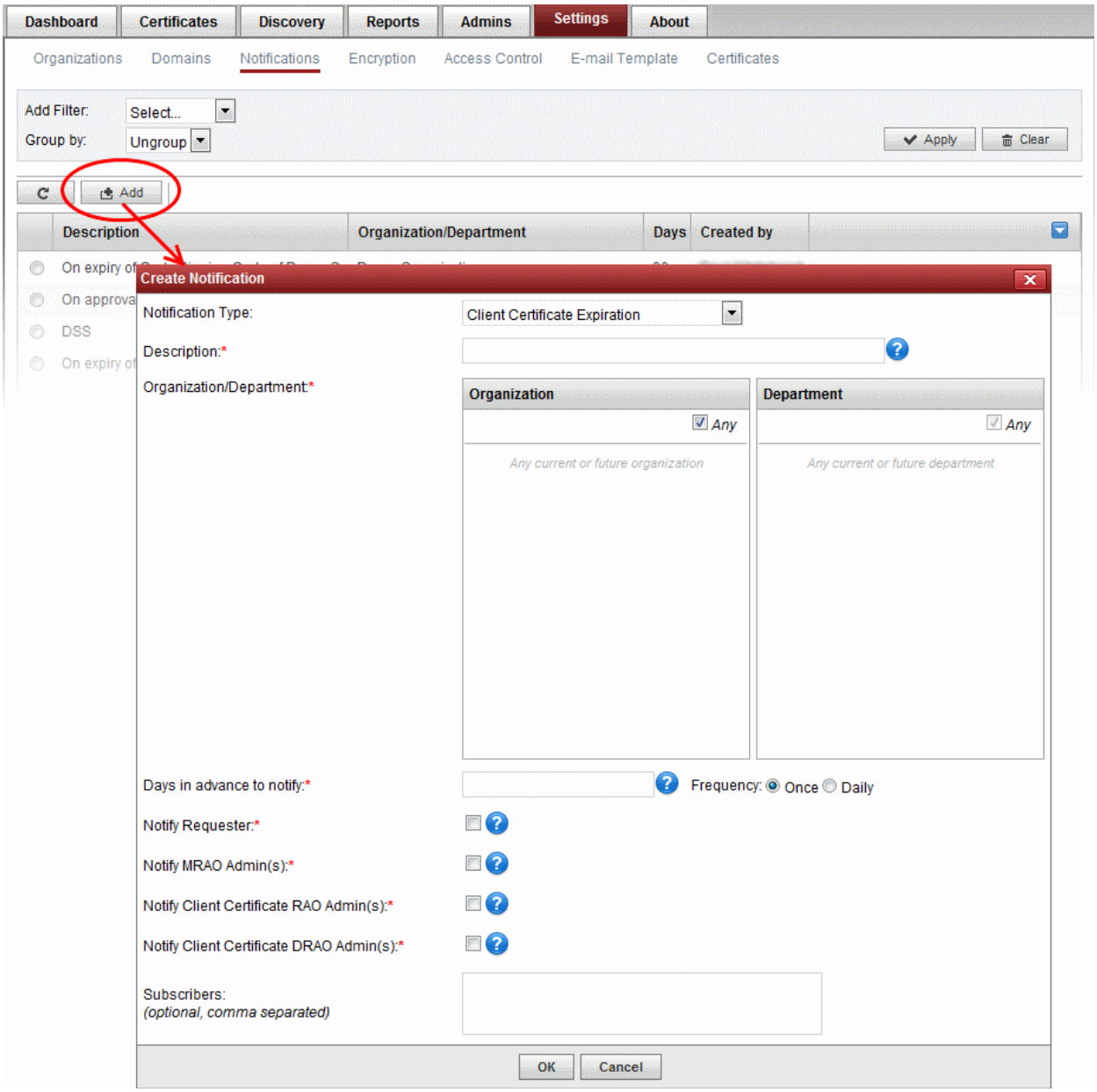


- To remove the filters, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Notifications' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

5.5.1 Adding a Notification

The administrator can add a new notification by clicking the 'Add' button at the bottom of Notifications sub-tab and filling out the form that appears.

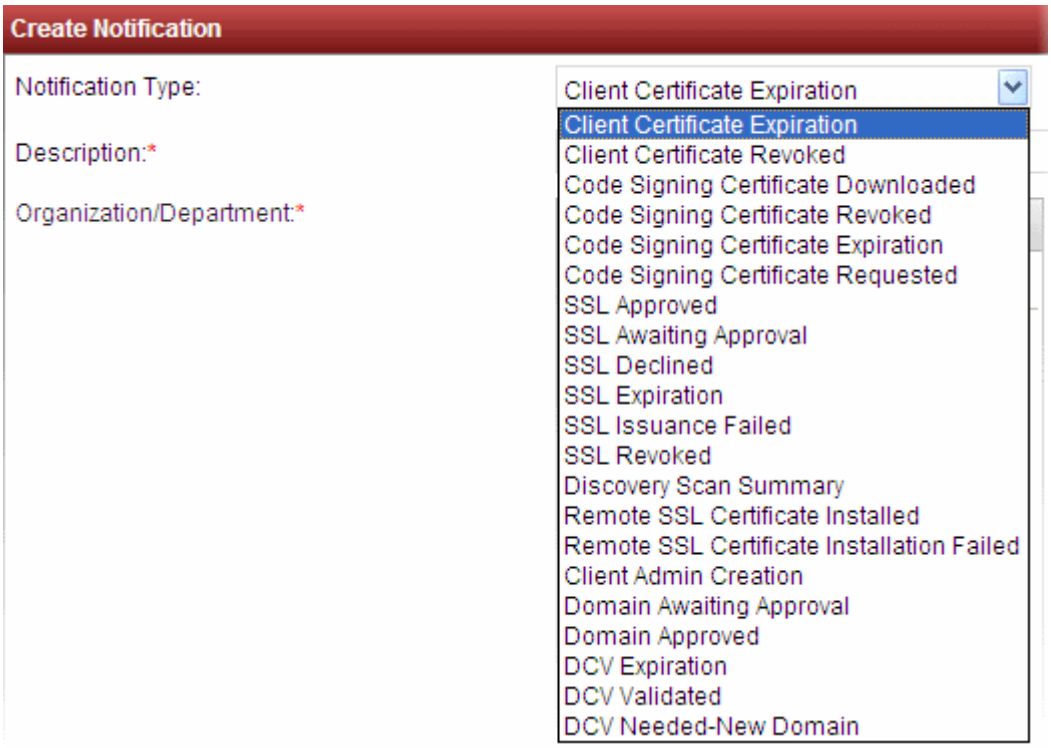


When adding a notification administrator should first select a Notification Type.

There are several types of notifications available for selection. The list of notification types in the drop-down is dependent on the role of the administrator. For example, RAO SSL and DRAO SSL administrators will see the options corresponding to only SSL certificates and so on.

An administrator can create notifications when he/she has authority for *all* of the organizations and departments contained within the scope of the notification *and* the administrator has authority for the notification type.

Similarly, an administrator can view existing notifications when he/she has authority for *any* of the organizations or departments contained within scope of the notification *and* the administrator has authority for the notification type.



The following table explains the notifications that are available for administrators according to their administrative roles.

Notification	Notification Type	Administrator Type
Client Certificate Expiration	Client Certificate	MRAO, RAO SMIME admins, DRAO SMIME admins.
Client Certificate Revoked	Client Certificate	MRAO, RAO SMIME admins, DRAO SMIME admins.
Code Signing Certificate Downloaded	Code Signing Certificate	MRAO, RAO Code Signing admins, MRAO Code Signing admins.
Code Signing Certificate Revoked	Code Signing Certificate	MRAO, RAO Code Signing admins, MRAO Code Signing admins.
Code Signing Certificate Expiration	Code Signing Certificate	MRAO, RAO Code Signing admins, MRAO Code Signing admins.
Code Signing Certificate Requested	Code Signing Certificate	MRAO, RAO Code Signing admins, MRAO Code Signing admins.
SSL Approved	SSL Certificate	MRAO, RAO SSL admin, DRAO SSL admin.
SSL Awaiting Approval	SSL Certificate	MRAO, RAO SSL admin, DRAO SSL admin.
SSL Declined	SSL Certificate	MRAO, RAO SSL admin, DRAO SSL admin.
SSL Expiration	SSL Certificate	MRAO, RAO SSL admin, DRAO SSL admin.

Notification	Notification Type	Administrator Type
SSL Issuance Failed	SSL Certificate	MRAO, RAO SSL admin, DRAO SSL admin.
SSL Revoked	SSL Certificate	MRAO, RAO SSL admin, DRAO SSL admin.
Discovery Scan Summary	Other	All administrators.
Remote SSL Certificate Installed	SSL Certificate	MRAO, RAO SSL admin, DRAO SSL admin
Remote SSL Certificate Installation Failed	SSL Certificate	MRAO, RAO SSL admin, DRAO SSL admin
Client Admin Creation	Other	All administrators.
Domain Awaiting Approval	Other	All administrators.
Domain Approved	Other	All administrators.
DCV Expiration	Domain Control Validation	MRAO, RAO SSL admin, DRAO SSL admin
DCV Validated	Domain Control Validation	MRAO, RAO SSL admin, DRAO SSL admin
DCV Needed-New Domain	Domain Control Validation	MRAO, RAO SSL admin, DRAO SSL admin

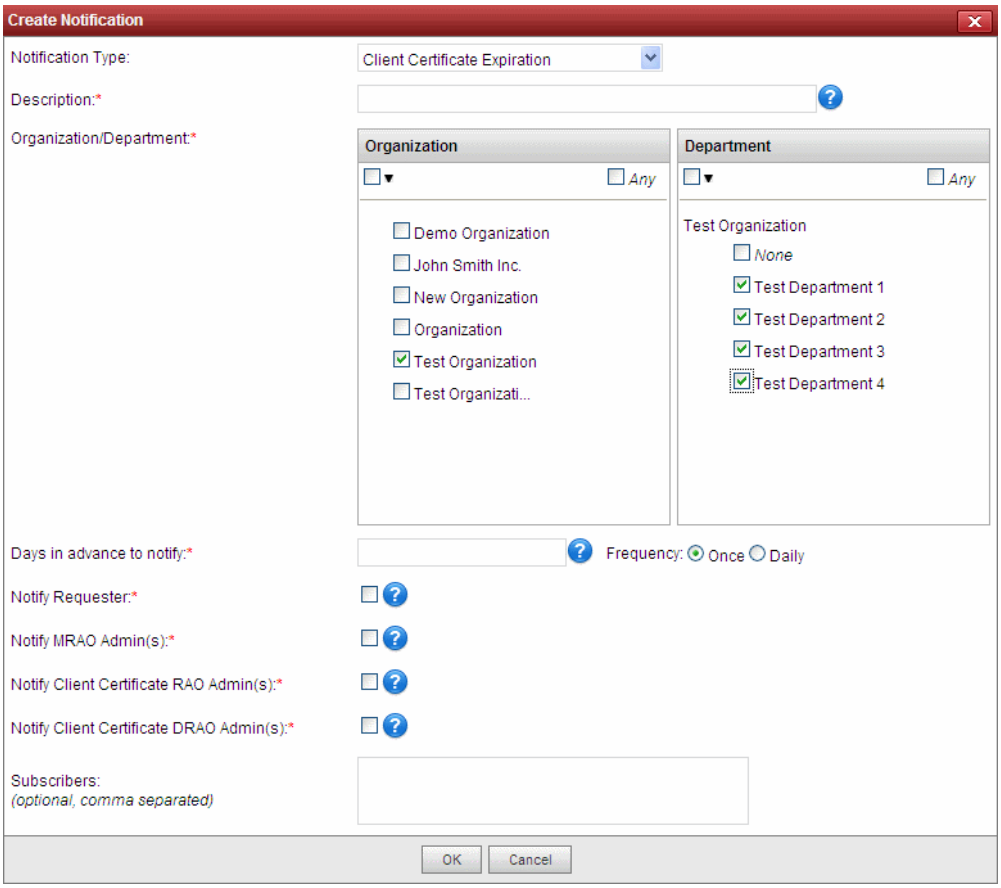
Note: The Notification Types related to DCV will be available only if the DCV feature is enabled for your account.

Detailed description of each type of form is given below. The 'Create Notification' form varies pursuant to the selected 'Notification Type'.

5.5.2 Notification Types

5.5.2.1 'Client Certificate Expiration' Create Notification Form

Enables administrator to set notification about terms of expiration of client certificates.



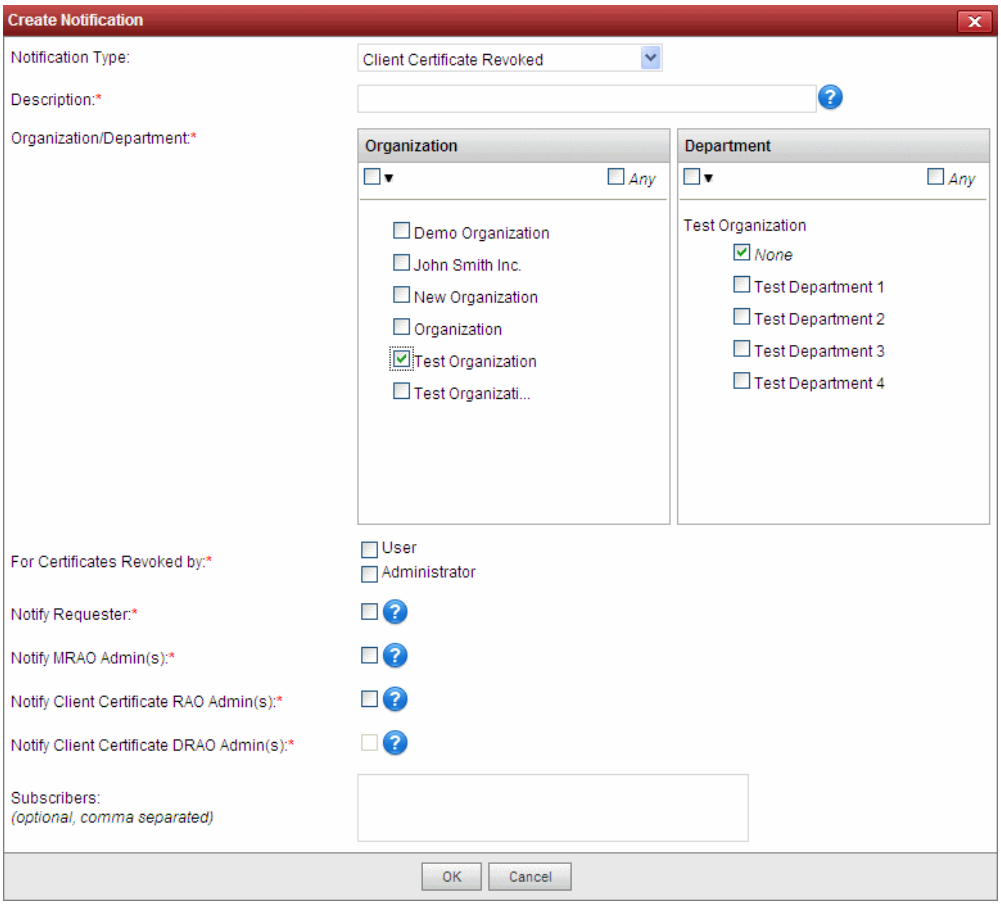
5.5.2.1.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator can select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Days in advance to notify ***(required)***	Text Field	Enables the administrator to set number of days the end-user will be informed about expiration of the certificate before the event. Administrator can also specify whether the notification has to be sent to the member(s) only once or daily till the expiration date by selecting the respective radio button.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for person that requested the certificate.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify Client Certificate RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SMIME Admin(s) of the Organization(s) which members use client certificates.
Notify Client Certificate DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO SMIME Admin(s) of the Departments(s) which members use client certificates.
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications

Form Element	Type	Description
		will be sent.

5.5.2.2 'Client Certificate Revoked' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel upon revocation of a client certificate.



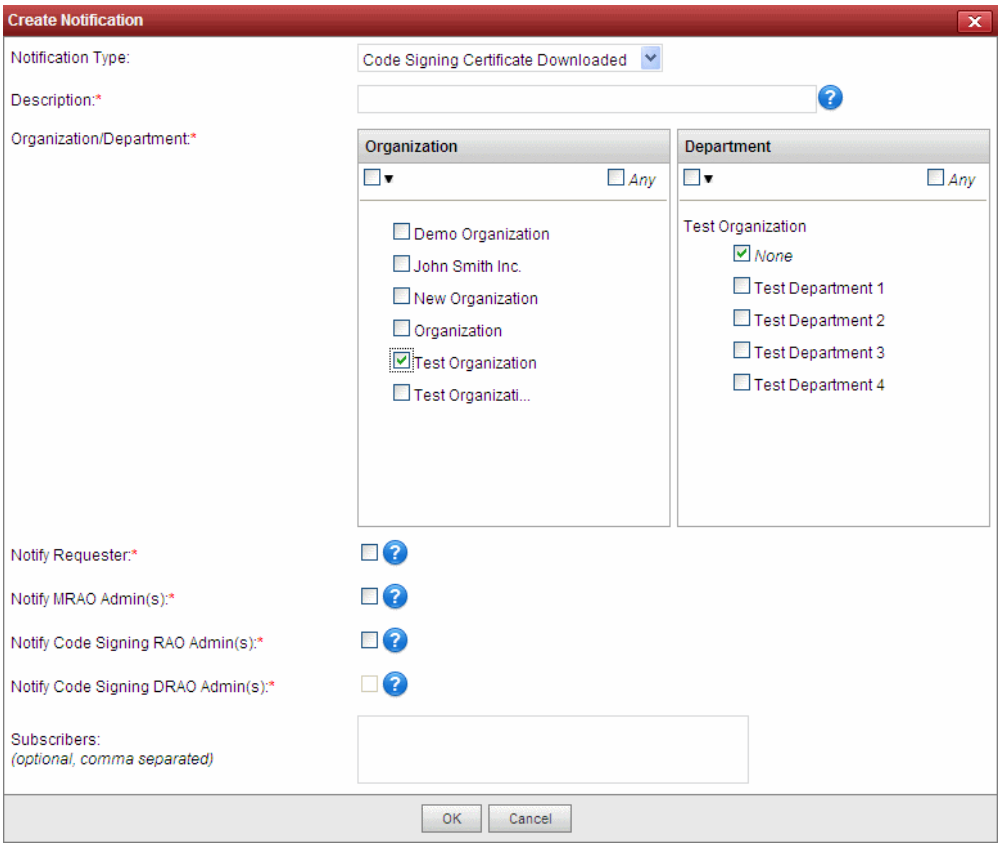
5.5.2.2.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
For Certificates Revoked by: ***(required)***	Checkbox	Administrator should select a person (administrator or user) after whose revoke action, the notification will be send.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for person, who requested the certificate.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).

Notify Client Certificate RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SMIME Admin(s) of the Organization(s) which members use client certificates.
Notify Client Certificate DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO SMIME Admin(s) of the Departments(s) which members use client certificates.
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.3 'Code Signing Certificate Downloaded' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose Code Signing Certificate was downloaded by the Administrator.



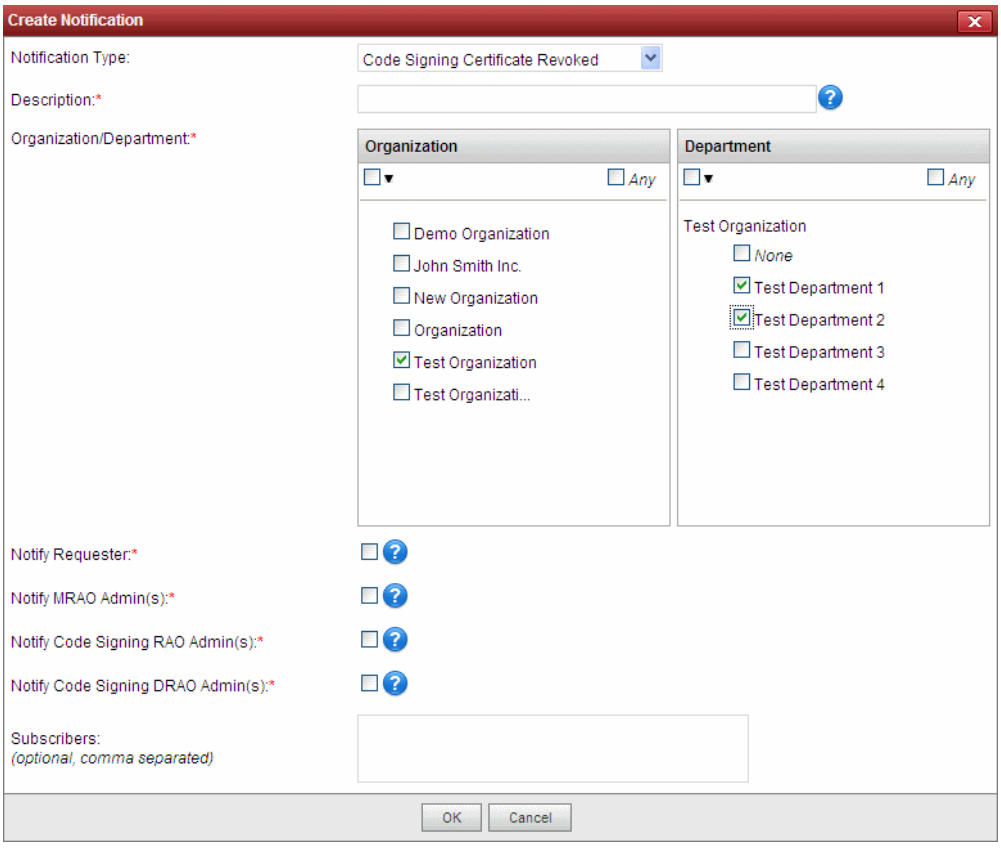
5.5.2.3.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for person, who requested the certificate.
Notify MRAO Admin(s)	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).

(required)		
Notify Code Signing RAO Admins(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO Code Signing Admin(s) of the selected Organization(s)/Department(s).
Notify Code Signing DRAO Admins(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO Code Signing Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.4 'Code Signing Certificate Revoked' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose Code Signing Certificate was revoked.



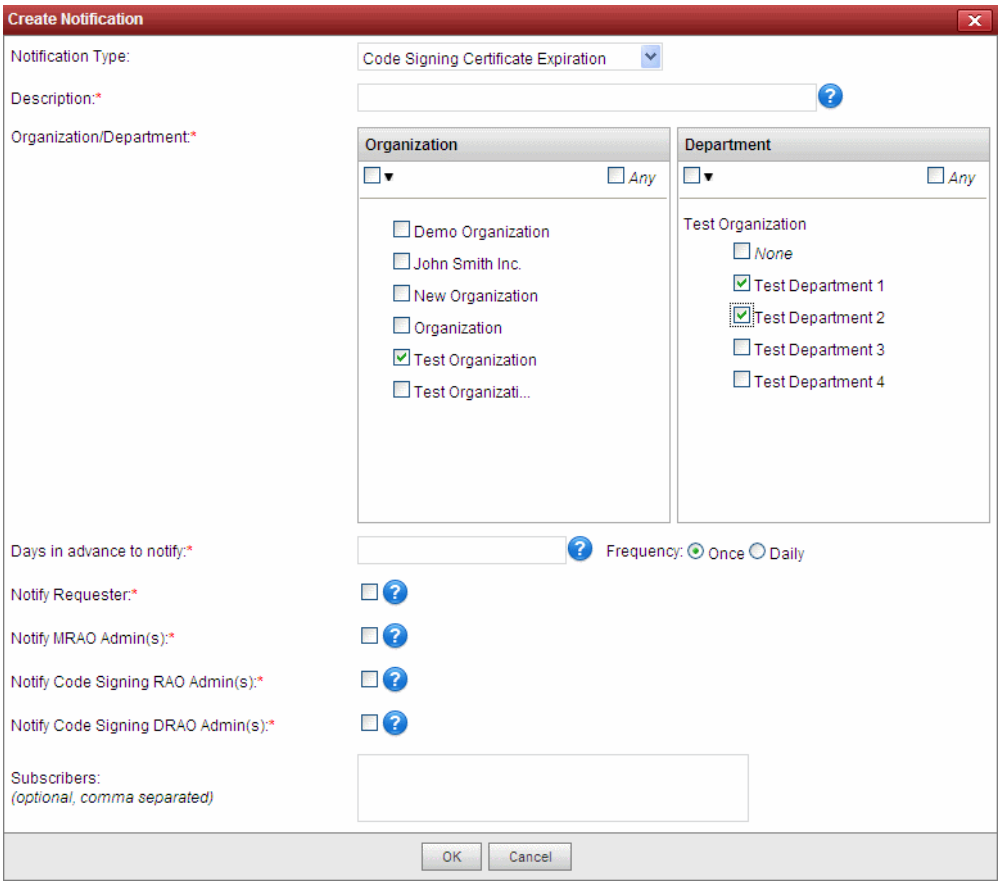
5.5.2.4.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for person, who requested the certificate.

Form Element	Type	Description
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify Code Signing RAO Admins(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO Code Signing Admin(s) of the selected Organization(s)/Department(s).
Notify Code Signing DRAO Admins(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO Code Signing Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.5 'Code Signing Certificate Expiration' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose Code Signing Certificate is due to expire.



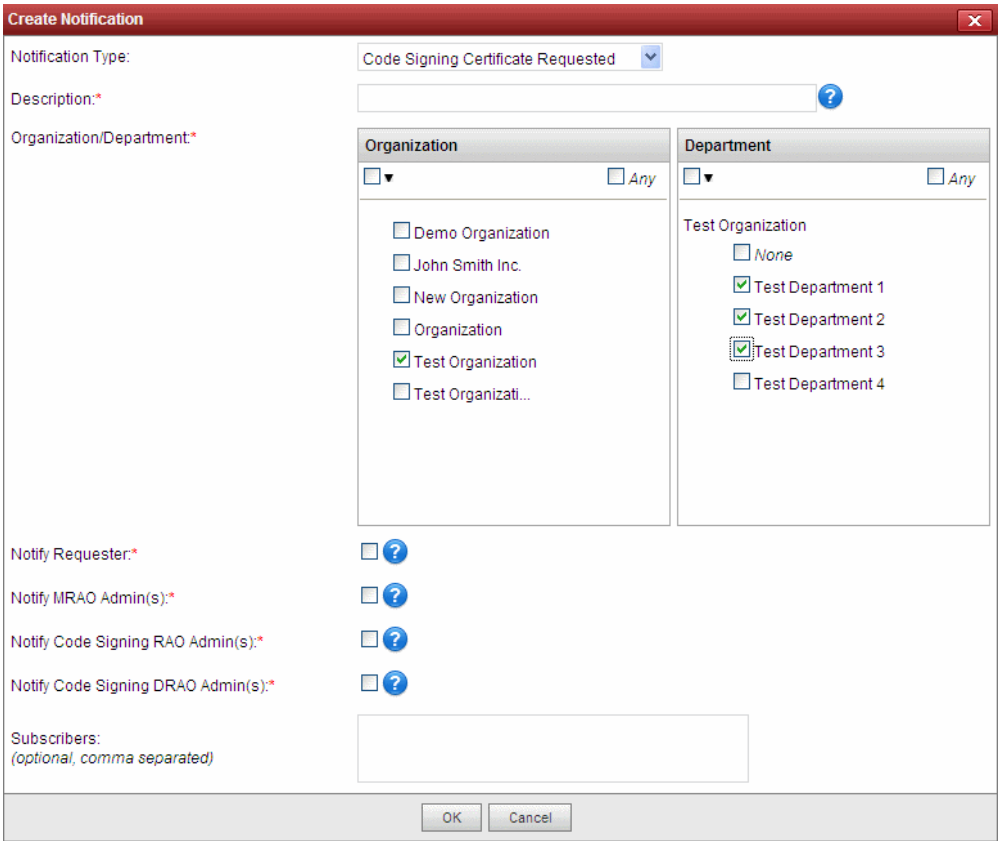
5.5.2.5.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.

Form Element	Type	Description
Days in advance to notify ***(required)***	Text Field	Enables the administrator to set number of days the end-user will be informed about expiration of the certificate before the event. Administrator can also specify whether the notification has to be sent to the member(s) only once or daily till the expiration date by selecting the respective radio button.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for person, who requested the certificate.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify Code Signing RAO Admins(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO Code Signing Admin(s) of the selected Organization(s)/Department(s).
Notify Code Signing DRAO Admins(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO Code Signing Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.6 'Code Signing Certificate Requested' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose Code Signing Certificate is been requested by the Administrator to the CA.



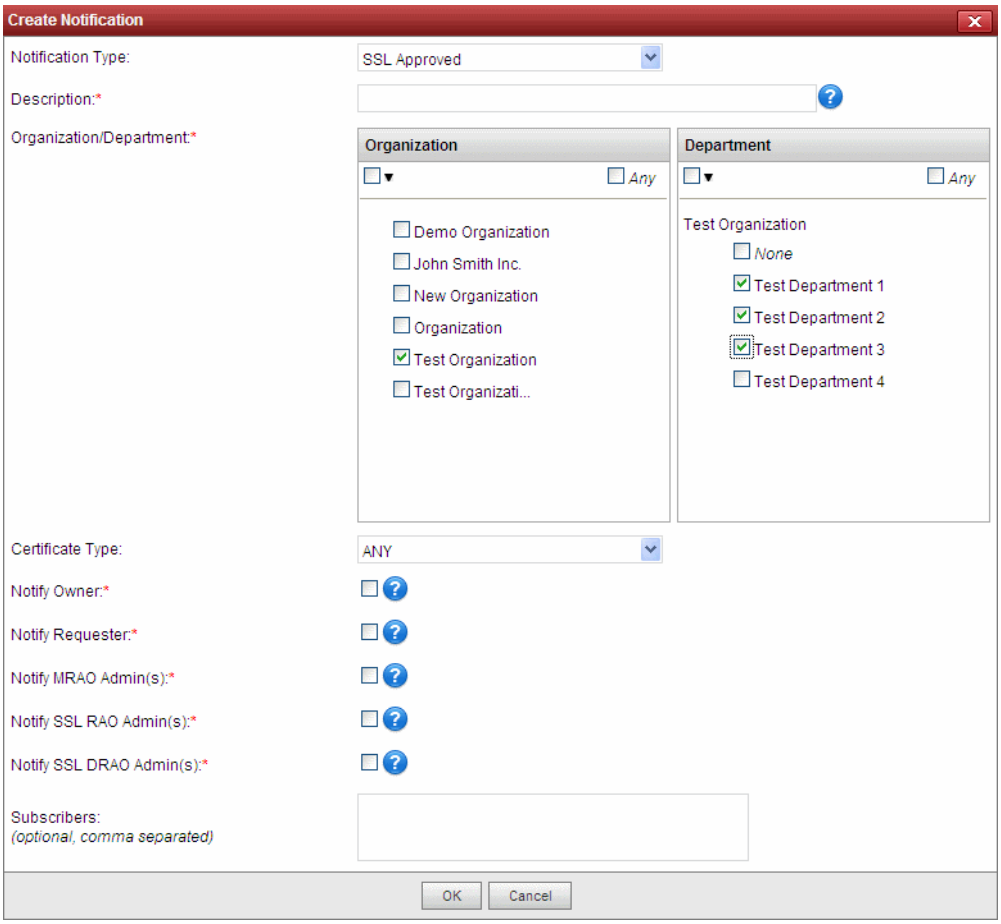
5.5.2.6.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.

Form Element	Type	Description
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for person, who requested the certificate.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify Code Signing RAO Admins(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO Code Signing Admin(s) of the selected Organization(s)/Department(s).
Notify Code Signing DRAO Admins(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO Code Signing Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.7 'SSL Approved' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel upon Approval of an SSL certificate request by an Administrator.

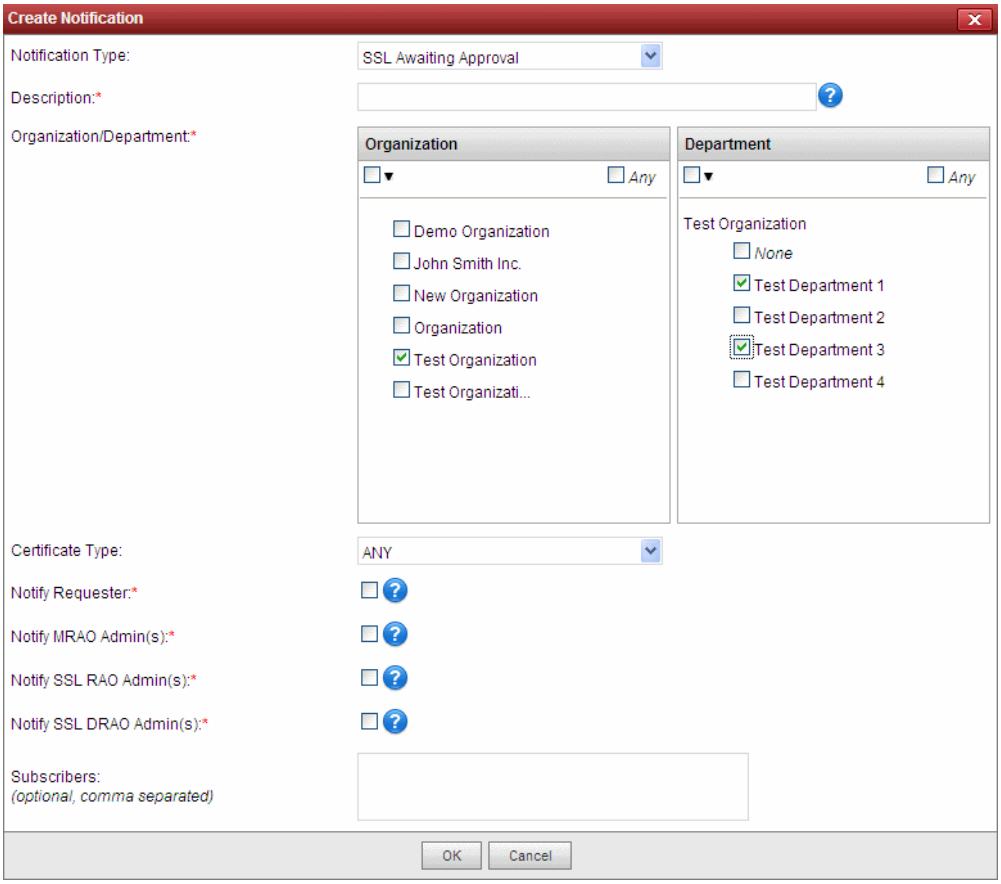


5.5.2.7.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Certificates Type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification is to be be set.
Notify Owner ***(required)***	Checkbox	Enables the administrator to set the notification for the Owner of the certificate. The Owner of the certificate is the Administrator that first approved the request for the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for person, who requested the certificate.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SSL Admin(s) of the Organization(s)/Department(s).
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.8 'SSL Awaiting Approval' Create Notification Form

Enables the administrator to set a notification about an SSL certificate state after the certificate was requested. An SSL certificate request must be approved by the administrator. Before the request is approved, its state is 'Awaiting Approval'.

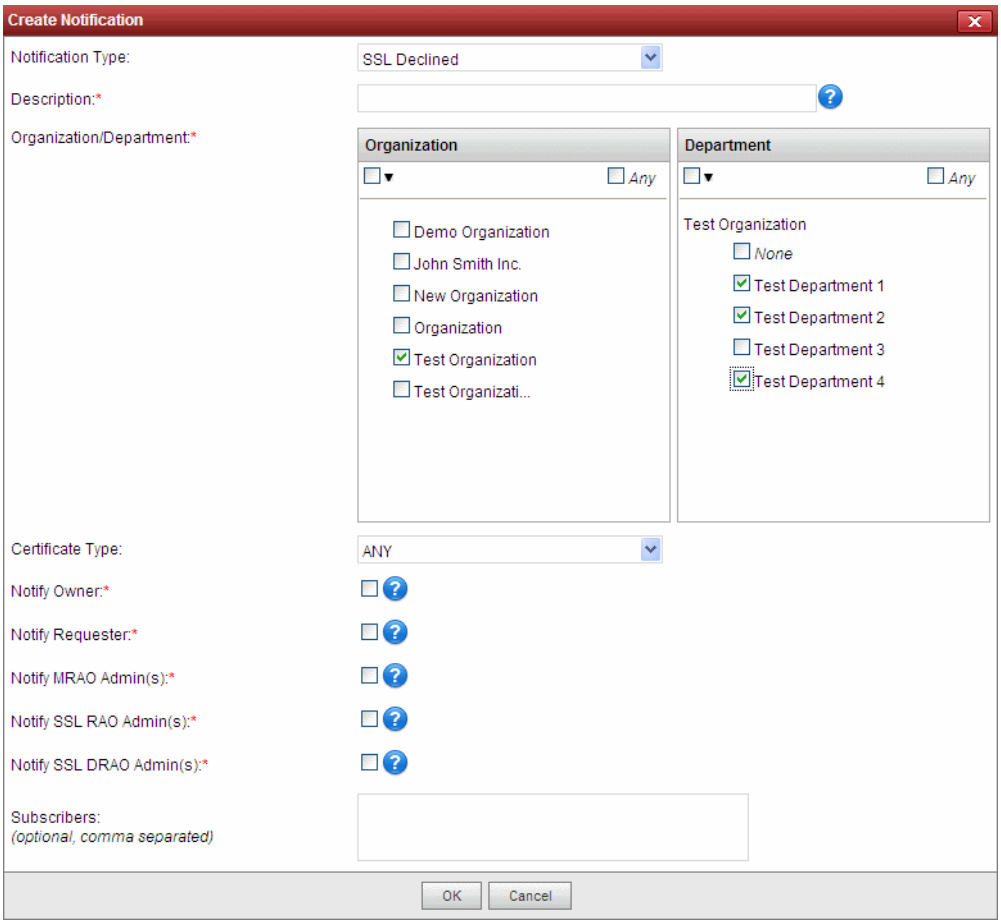


5.5.2.8.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Certificates type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification is to be be set.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for person, who requested the certificate.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SSL Admin(s) of the Organization(s)/Department(s).
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.9 'SSL Declined' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose SSL Certificate request was declined by the Administrator.

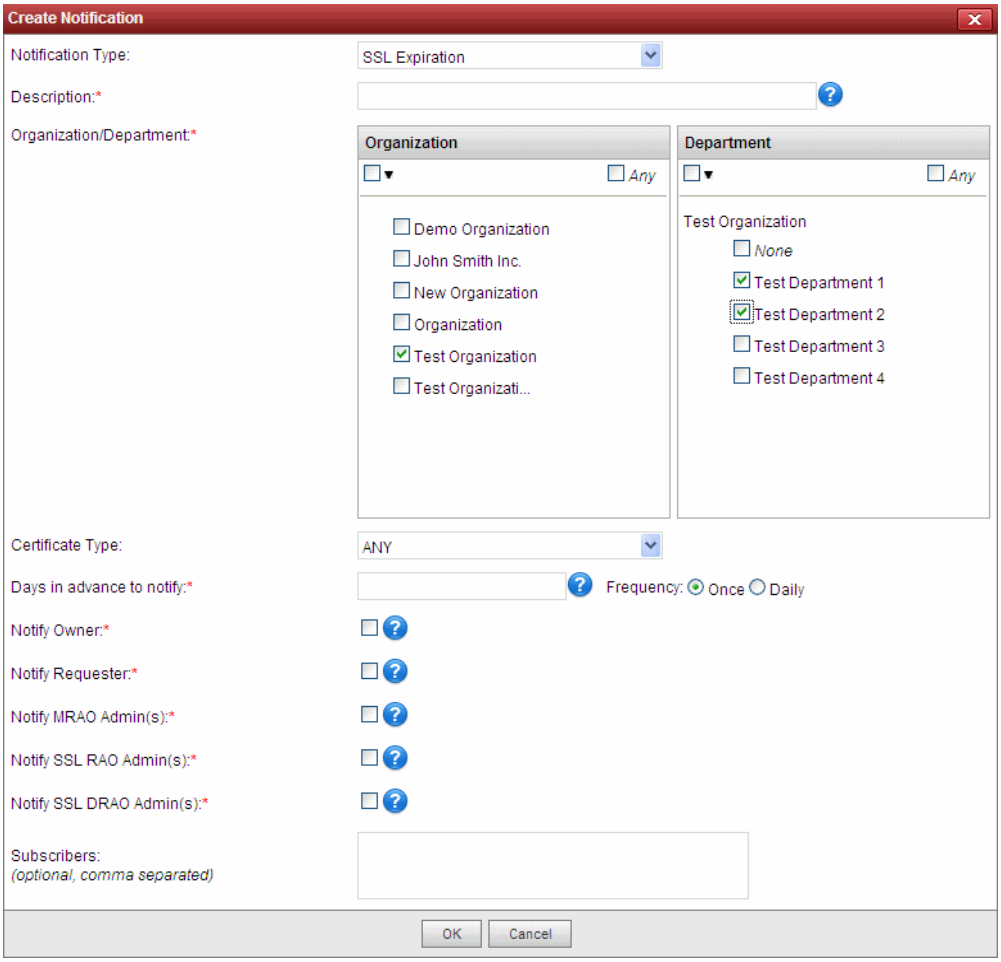


5.5.2.9.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Certificates Type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification will be set.
Notify Owner ***(required)***	Checkbox	Enables the administrator to set the notification for the Owner of the certificate. The Owner of the certificate is the Administrator that first approved the request for the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for a person, who requested the certificate.
Notify Master Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SSL Admin(s) of the Organization(s)/Department(s).
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO SSL Admin(s) of the Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.10 'SSL Expiration' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose SSL Certificates are due to expire, in advance.



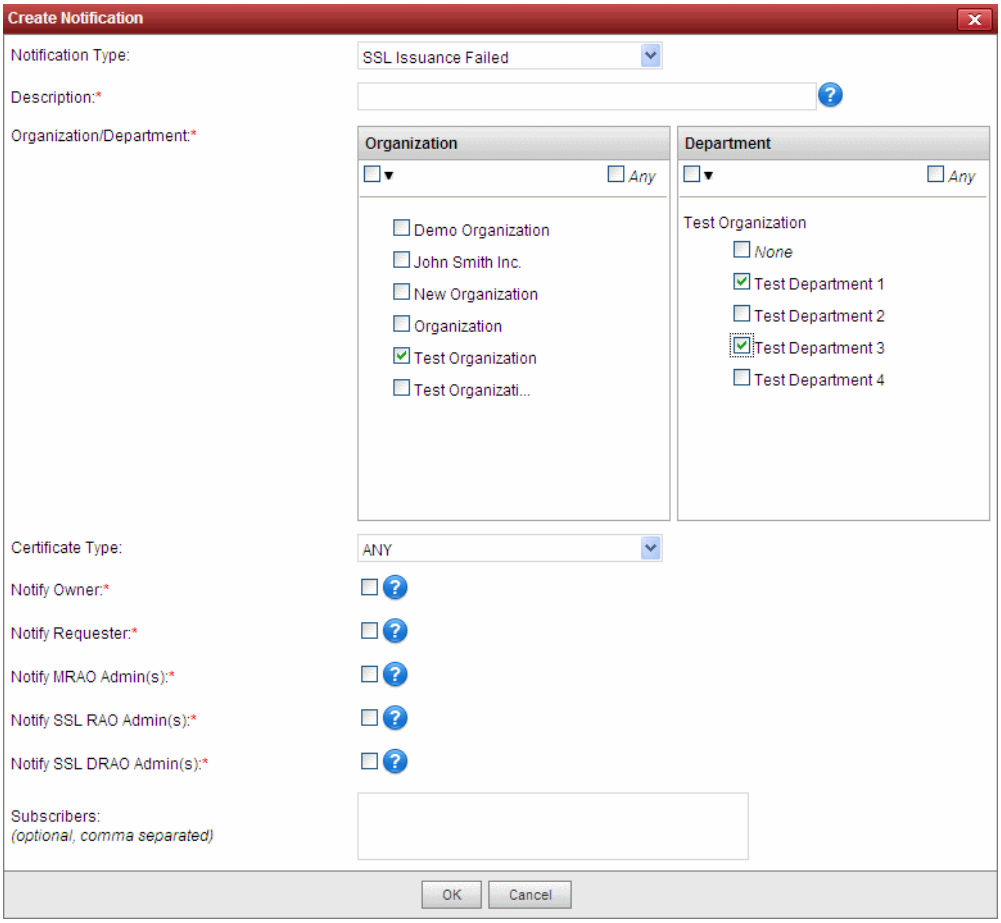
5.5.2.10.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Certificates type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification will be set.
Days in advance to notify ***(required)***	Text Field	Enables the administrator to set number of days the notification will be sent about expiration of the certificate before the event. Administrator can also specify whether the notification has to be sent only once or daily till the expiration date by selecting the respective radio button.
Notify Owner ***(required)***	Checkbox	Enables the administrator to set the notification for a person, who owns the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for a person, who requested the certificate.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).

Form Element	Type	Description
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SSL Admin(s) of the Organization(s)/Department(s).
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SSL Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.11 'SSL Issuance Failed' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel for whom the SSL Certificate issuance has failed.



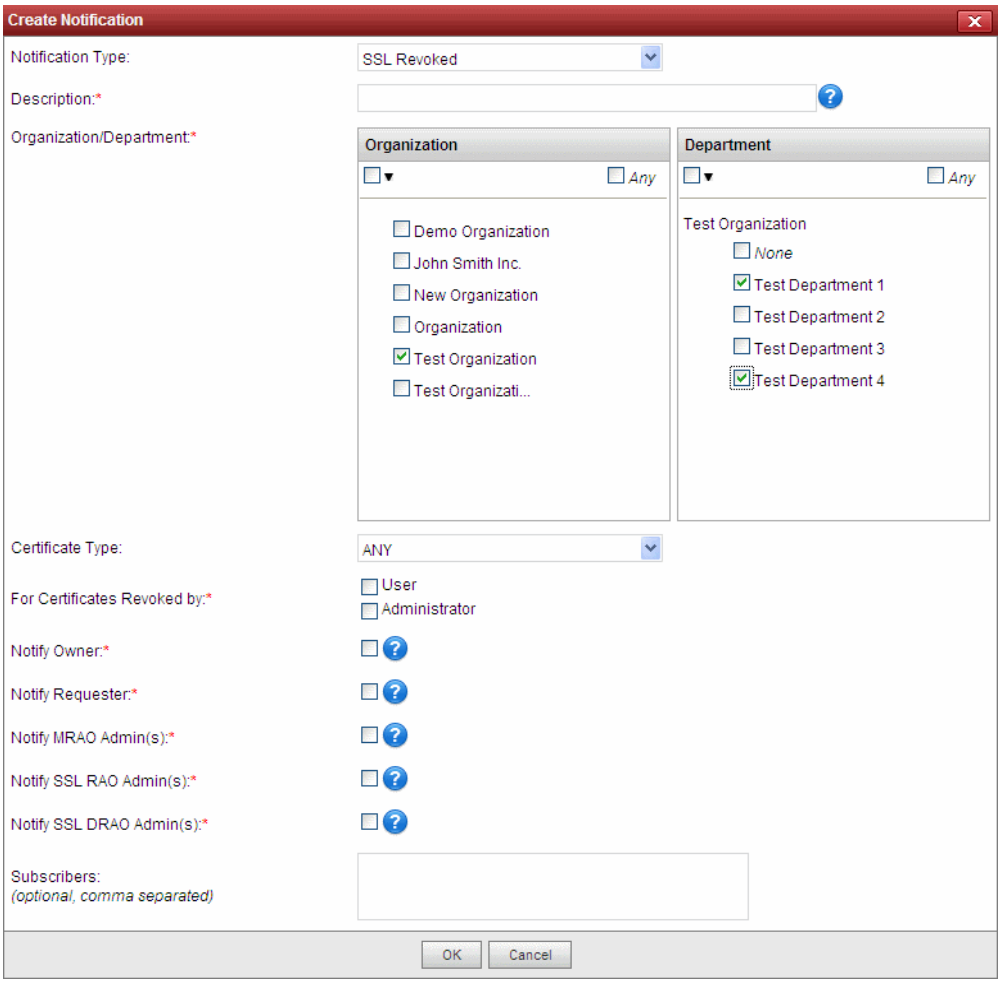
5.5.2.11.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.

Form Element	Type	Description
Certificates Type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification will be set.
Notify Owner ***(required)***	Checkbox	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for a person, who requested the certificate.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SSL Admin(s) of the Organization(s)/Department(s).
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.12 'SSL Revoked' Create Notification Form

Enables the administrator to set the notification about SSL certificates 'Revoke' action (the certificate could be revoked by the administrator or by the end-user).

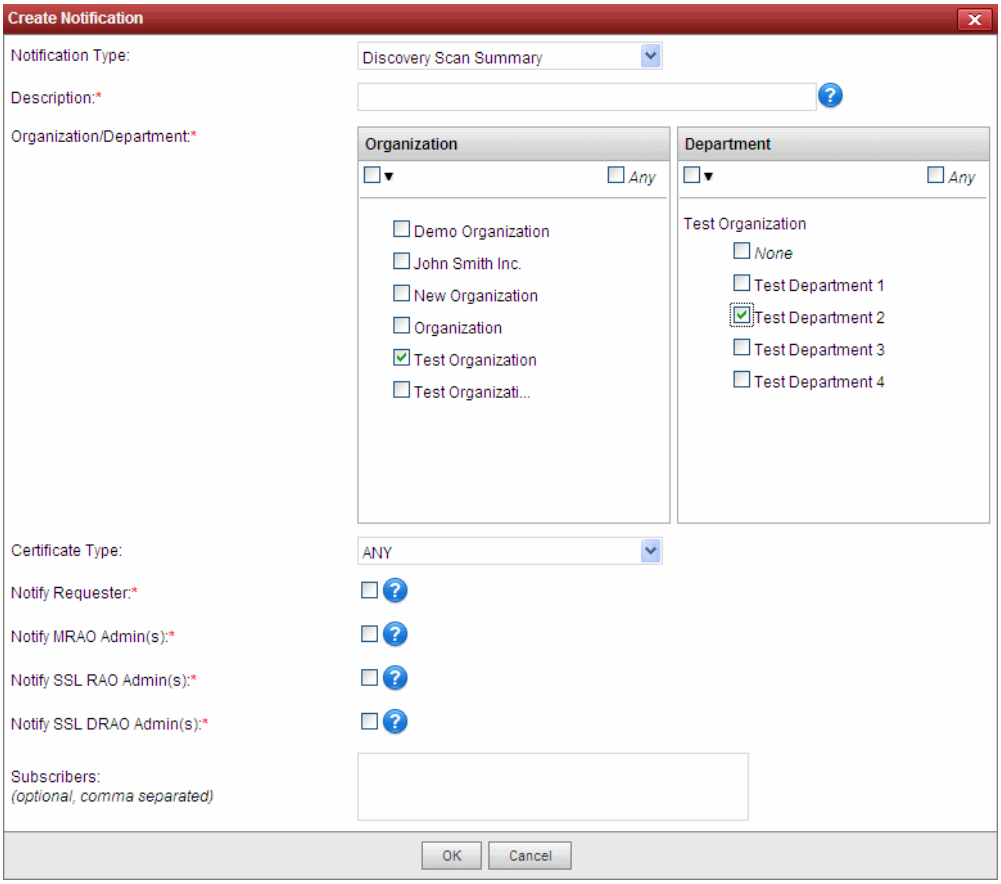


5.5.2.12.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Certificates Type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification will be set.
For Certificates Revoked by: ***(required)***	Checkbox	Administrator should select a person (administrator or user) after whose revocation action, the notification is to be sent.
Notify Owner ***(required)***	Checkbox	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification for a person, who requested the certificate.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SSL Admin(s) of the Organization(s)/Department(s).
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.13 'Discovery Scan Summary' Create Notification Form

Enables the Administrator to create a notification with a summary of certificate discovery scan results, for sending to selected personnel.

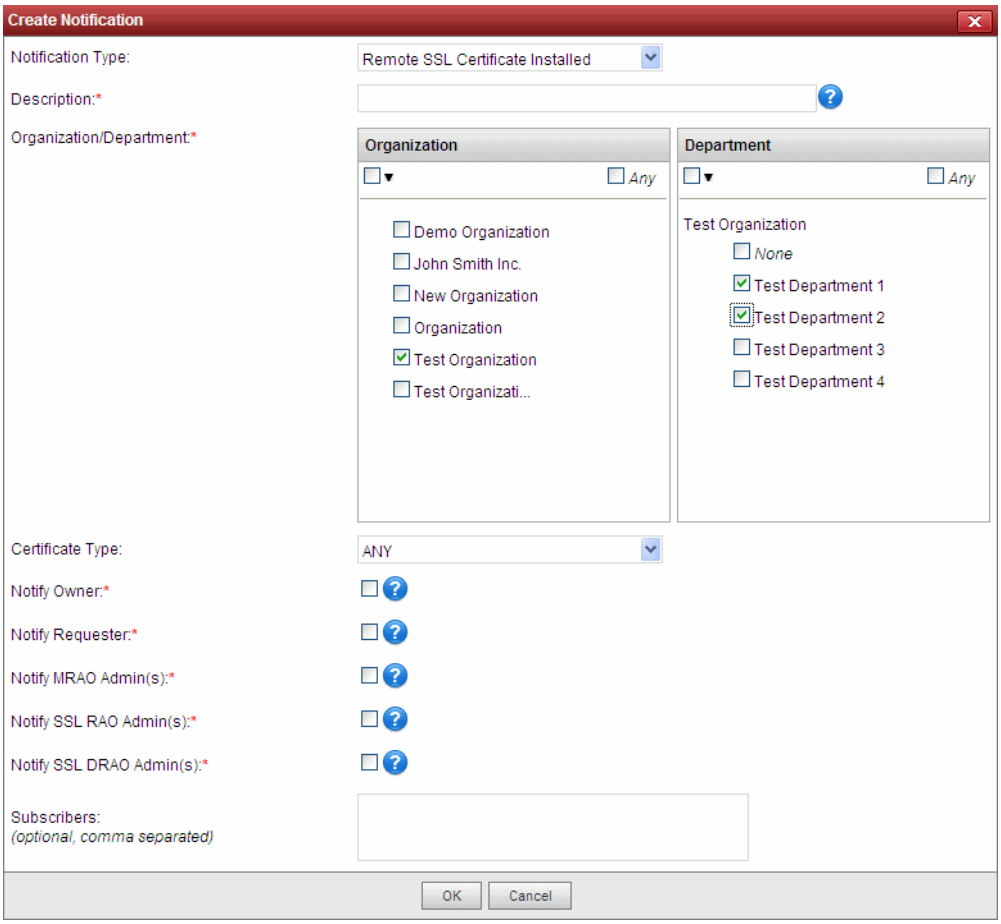


5.5.2.13.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Certificates Type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the discovery scan summary notification will be set.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SSL Admin(s) of the selected Organization(s)/Department(s).
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.14 'Remote SSL Certificate Installed ' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose SSL Certificate was remotely installed by the Administrator.



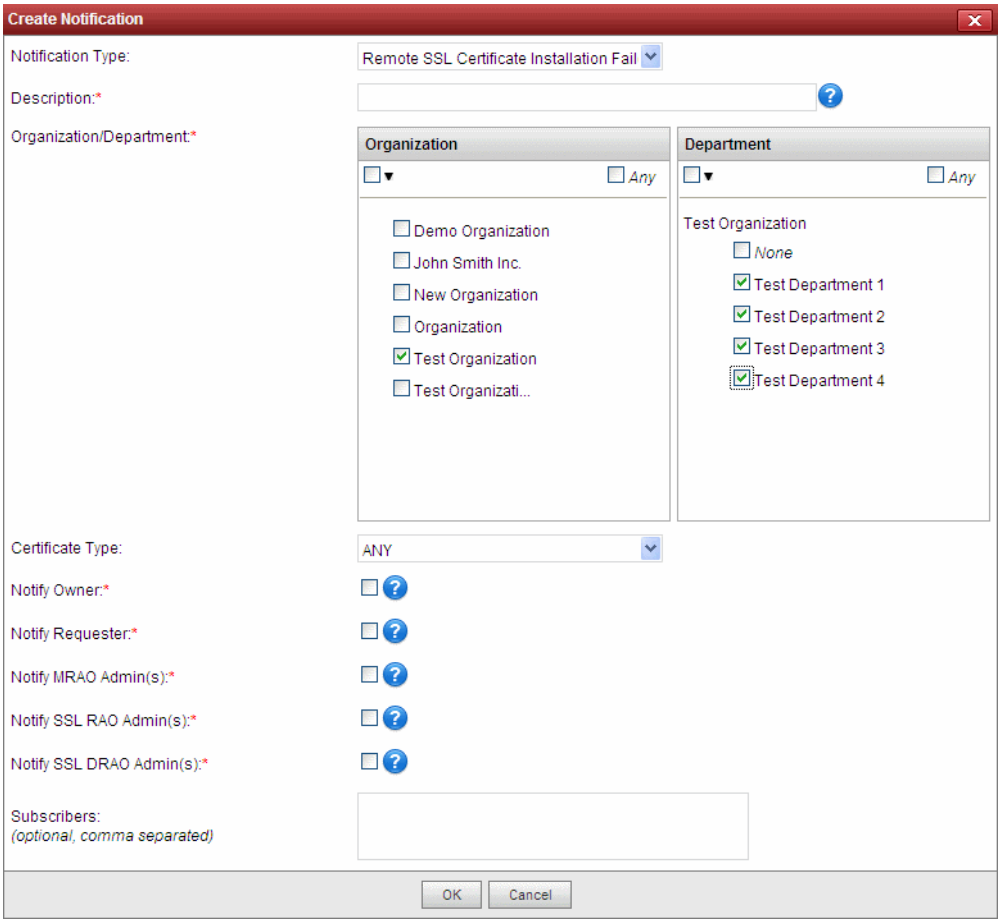
5.5.2.14.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Certificates Type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the SSL certificate was installed remotely notification will be set.
Notify Owner ***(required)***	Checkbox	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification to the person who requested the Admin status.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SSL Admin(s) of the selected Organization(s)/Department(s).

Form Element	Type	Description
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.15 'Remote SSL Certificate Installation Failed ' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose remote SSL Certificate installation failed.



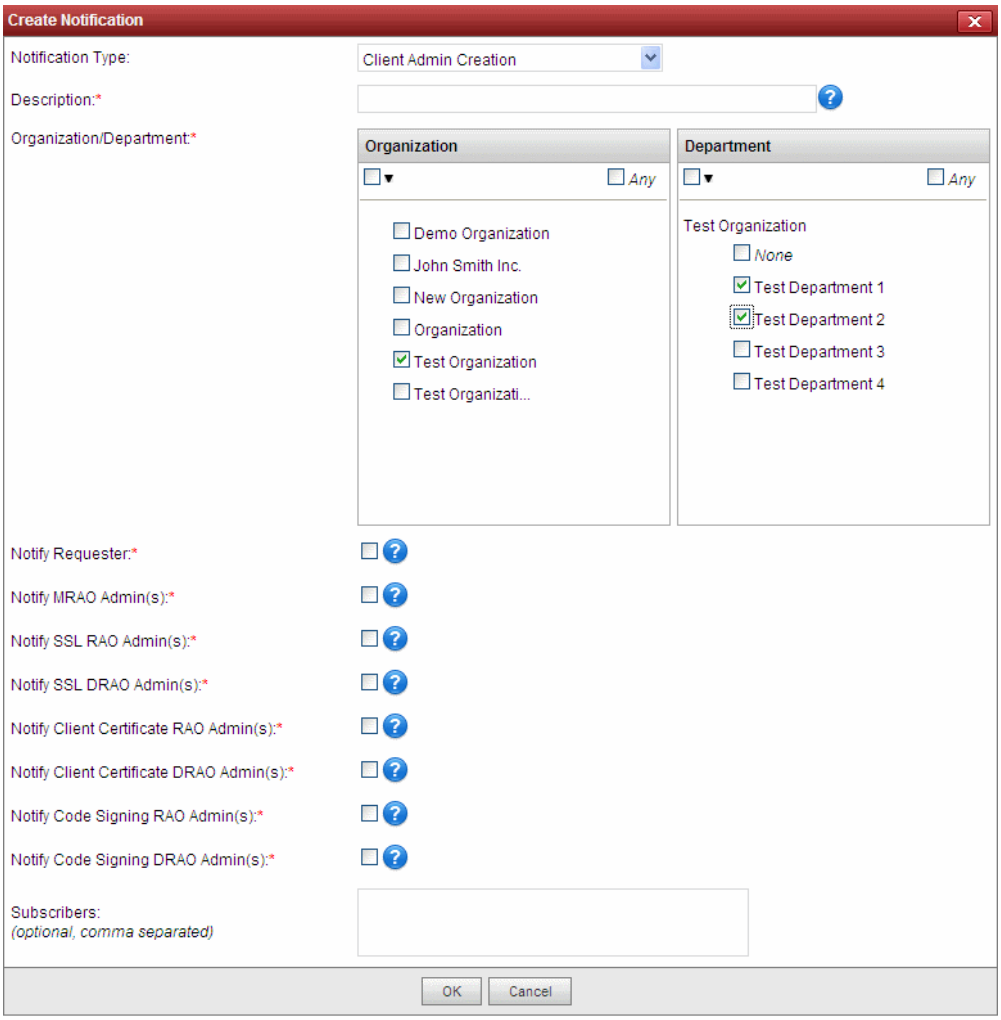
5.5.2.15.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Certificates Type: ***(required)***	Drop-down	Administrator should select the type of SSL certificate for which the remote installation failed notification will be sent.

Form Element	Type	Description
Notify Owner ***(required)***	Checkbox	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification to the person who requested the Admin status.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for RAO SSL Admin(s) of the selected Organization(s)/Department(s).
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected Department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.16 'Client Admin Creation' Create Notification Form

Enables the Administrator to create a notification to selected personnel upon creation of new Client Cert Administrators (RAO Admin SMIME and DRAO Admin SMIME).

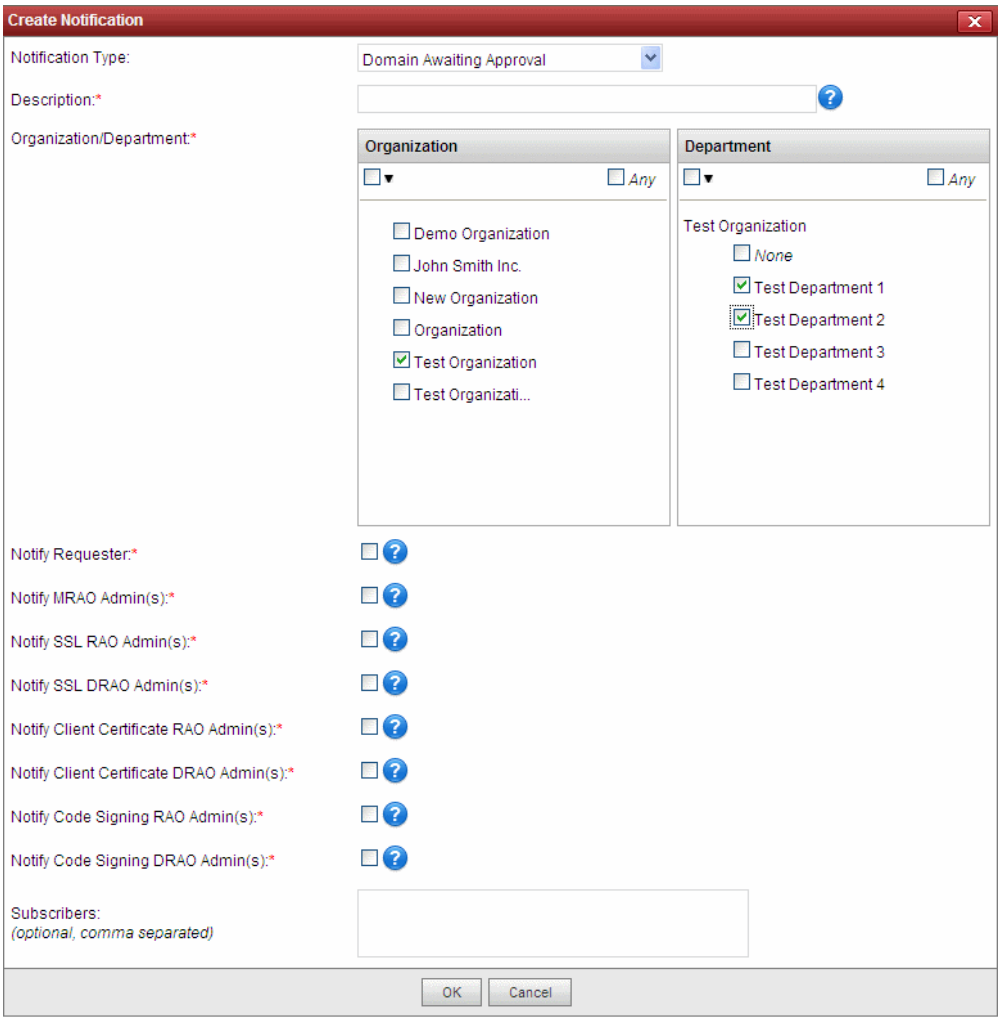


5.5.2.16.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification to the person who requested the Admin status.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments.
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the DRAO SSL Admin(s) of the selected Departments.
Notify Client Certificate RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO SMIME Admin(s) of the selected Organization(s)/Departments.
Notify Client Certificate DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the DRAO SMIME Admin(s) of the selected Departments.
Notify Code Signing RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO Code Signing Admin(s) of the selected Organization(s)/Departments.
Notify Code Signing DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the DRAO Code Signing Admin(s) of the selected Departments.
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.17 'Domain Awaiting Approval' Create Notification Form

Enables the administrator to set a notification about a request of a domain delegation to an Organization/Department. The Domain delegation request must be approved by the MRAO/RAO Administrator. Before the request is approved, its state is 'Awaiting Approval'.



5.5.2.17.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification to the person who requested the delegation of a created domain to an Organization/Department.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments.
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the DRAO SSL Admin(s) of the selected Departments.
Notify Client Certificate RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO SMIME Admin(s) of the selected Organization(s)/Departments.

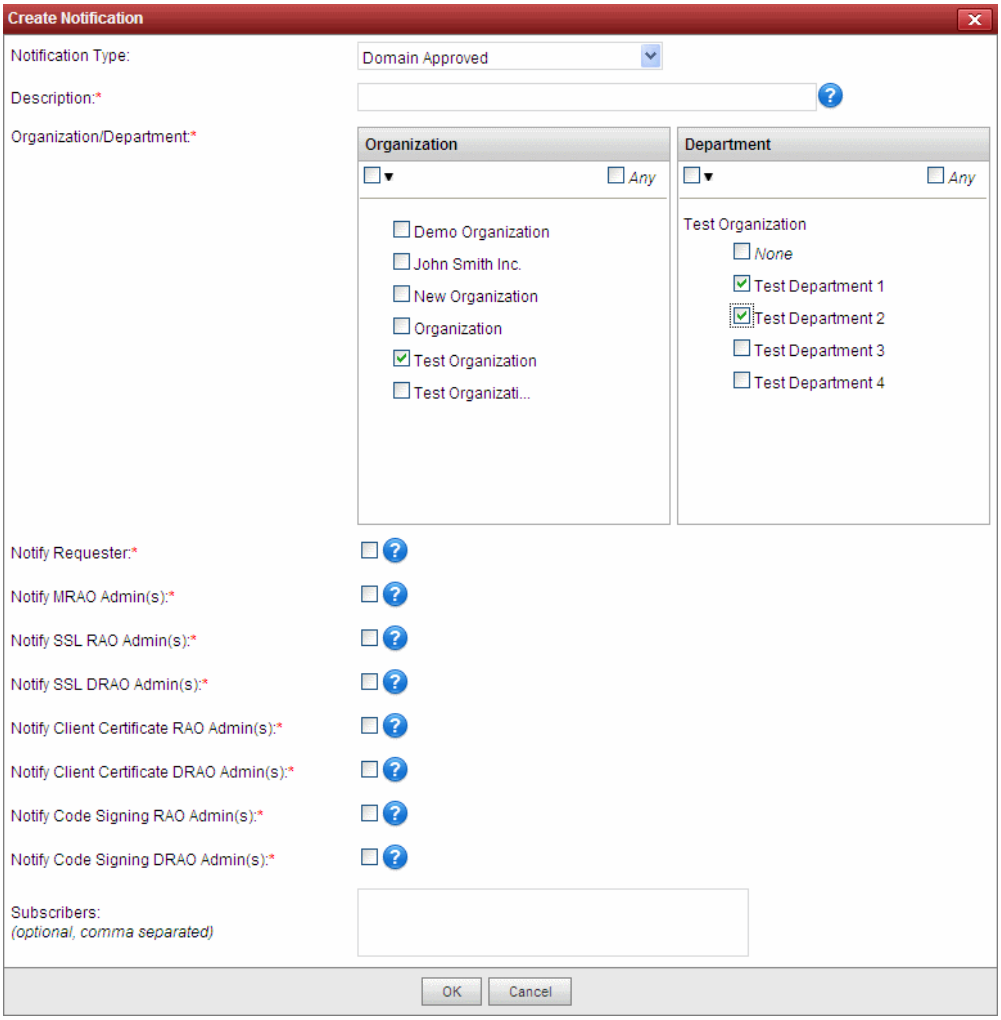
Form Element	Type	Description
Notify Client Certificate DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the DRAO SMIME Admin(s) of the selected Departments.
Notify Code Signing RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO Code Signing Admin(s) of the selected Organization(s)/Departments.
Notify Code Signing RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the DRAO Code Signing Admin(s) of the selected Departments.
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

Important Note: The 'Domain Awaiting Approval' notification will be sent to MRAO only after the requested domain is approved by RAO.

5.5.2.18 'Domain Approved' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel upon Approval of creation and delegation of a domain to an Organization/Department.

Important Note: The 'Domain Approved' notification will be sent only after the request has been 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 just a single MRAO'

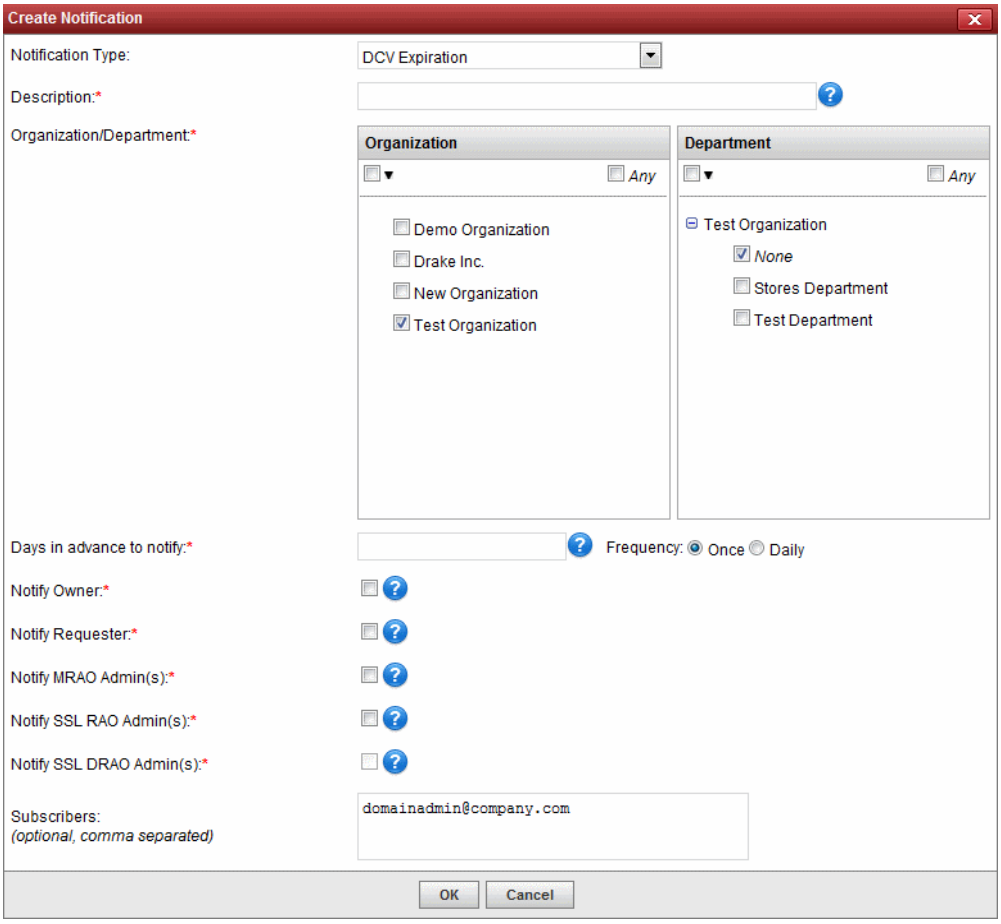


5.5.2.18.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification to the person who requested the delegation of a created domain to an Organization/Department.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments.
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the DRAO SSL Admin(s) of the selected Departments.
Notify Client Certificate RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO SMIME Admin(s) of the selected Organization(s)/Departments.
Notify Client Certificate DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the DRAO SMIME Admin(s) of the selected Departments.
Notify Code Signing RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO Code Signing Admin(s) of the selected Organization(s)/Departments.
Notify Code Signing DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the DRAO Code Signing Admin(s) of the selected Departments.
Subscribers ***(optional)***	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.19 'DCV Expiration' Create Notification Form

Enables administrator to set notification about expiration of domain control validation if it is due to expire.



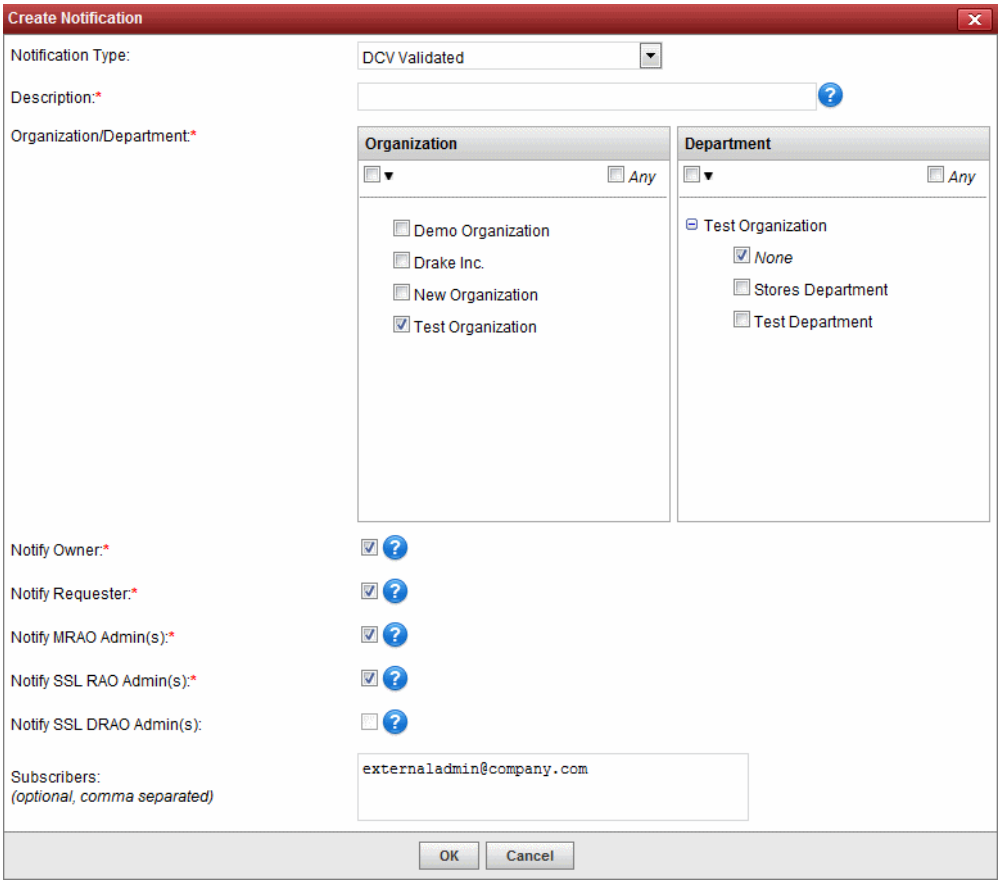
5.5.2.19.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Days in advance to notify ***(required)***	Text Field	Enables the administrator to set number of days the end-user will be informed about expiration of the certificate before the event. Administrator can also specify whether the notification has to be sent to the member(s) only once or daily till the expiration date by selecting the respective radio button.
Notify Owner ***(required)***	Checkbox	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification to the person who requested the delegation of a created domain to an Organization/Department.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments.
Notify SSL DRAO Admin(s)	Checkbox	Enables the administrator to set the notification all the DRAO SSL Admin(s) of

(required)		the selected Departments.
Subscribers (***optional***)	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.20 'DCV Validated' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel on successful completion of Domain Control Validation (DCV).



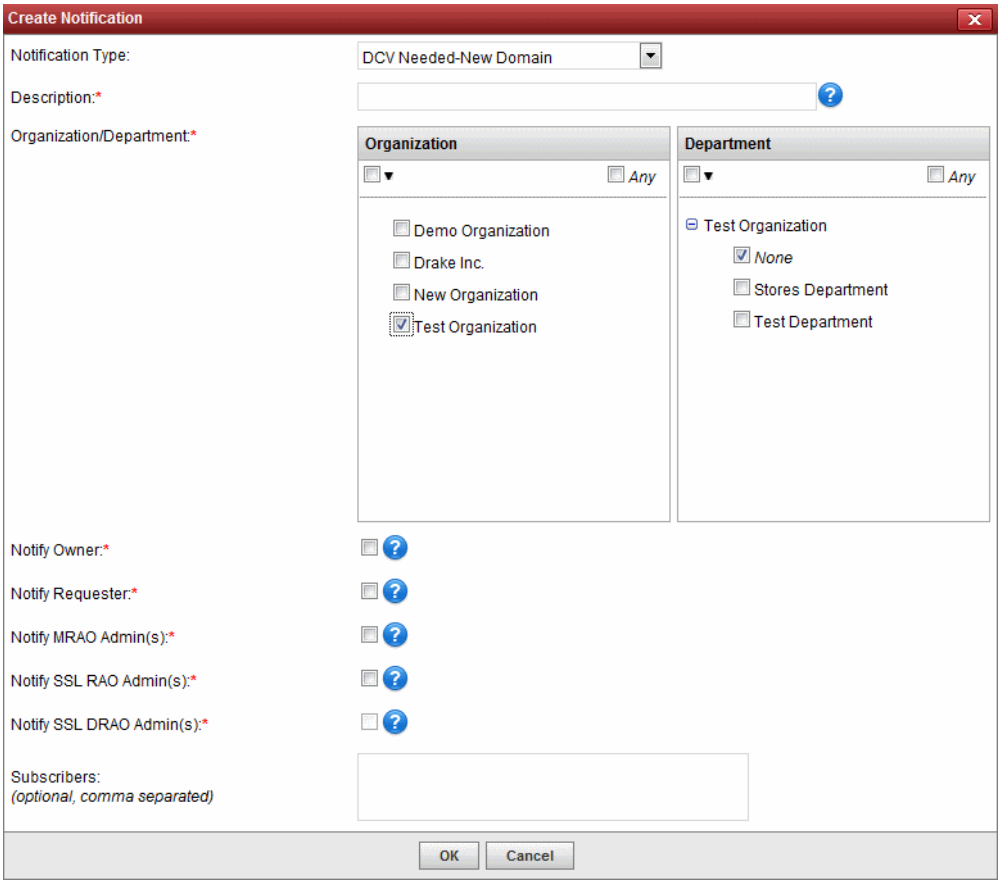
5.5.2.20.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.
Notify Owner ***(required)***	Checkbox	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification to the person who requested the delegation of a created domain to an Organization/Department.

Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments.
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the DRAO SSL Admin(s) of the selected Departments.
Subscribers (***optional***)	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.5.2.21 'DCV Needed-New Domain' Create Notification Form

Enables the Administrator to create a notification that will be sent to those personnel selected when a new domain is created and awaiting validation.



5.5.2.21.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Administrator should enter text of the notification in this field.
Organization/Department ***(required)***	Checkboxes	Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and departments will be displayed. Choose the Organizations/Departments from the tree structure.

Notify Owner ***(required)***	Checkbox	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification to the person who requested the delegation of a created domain to an Organization/Department.
Notify MRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the MRAO Admin(s).
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments.
Notify SSL DRAO Admin(s) ***(required)***	Checkbox	Enables the administrator to set the notification all the DRAO SSL Admin(s) of the selected Departments.
Subscribers (***optional***)	Text Field	Administrator can specify additional email address to which the notifications will be sent.

5.6 Encryption and Key Escrow

5.6.1 Introduction and basic concepts

Comodo Certificate Manager can store the individual private keys of end-user's client certificates so that they can be recovered at a later date by appropriately privileged Administrators. Due to the highly sensitive and confidential nature of this feature, all end-user client certificates are stored in encrypted form so that they cannot be easily stolen or compromised.

- It is possible to specify that keys in escrow be independently retrieved by any of the three levels of Administrator - MRAO and/or RAO SMIME and/or DRAO SMIME Administrators.
- Therefore, it is possible for CCM to store up to 2 encrypted versions of the private keys of client certificates of an Organization and up to 3 versions for a Department. Each version will be separately encrypted by three different 'master' public keys - the MRAO master key, the Organization master Key and the Departmental master key.
- These master public keys are stored by CCM. The corresponding master private keys are not stored in CCM (the master 'private' key is required for decryption/retrieval). These keys must be saved in a secure location by the Administrator that is creating the Organization/Department.
- There is one master key pair per Organizational tier and these are generated (if required) during the creation of that Organizational tier (e.g. during Organization creation or during Department creation). Therefore, one master key pair will be used by all RAO SMIME Administrators of a particular Organization - the Organization Master Key. Similarly, if key retrieval is required at the Departmental level then one pair of master keys will be used by all DRAO SMIME Admins of a particular Department - the Department Master Key.
- IF 'Allow key recovery by MRAO/RAO/DRAO' is enabled at the point of Organization/Department creation 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 '**Master Keys Required Prior to Client Cert Issuance**' for more details.
- Retrieving the private key of a user's client certificate from escrow will cause 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 is retrieved from escrow by clicking the 'Download' button next to the chosen certificate. See **Recovering a User's Private Key from Escrow** for more details.

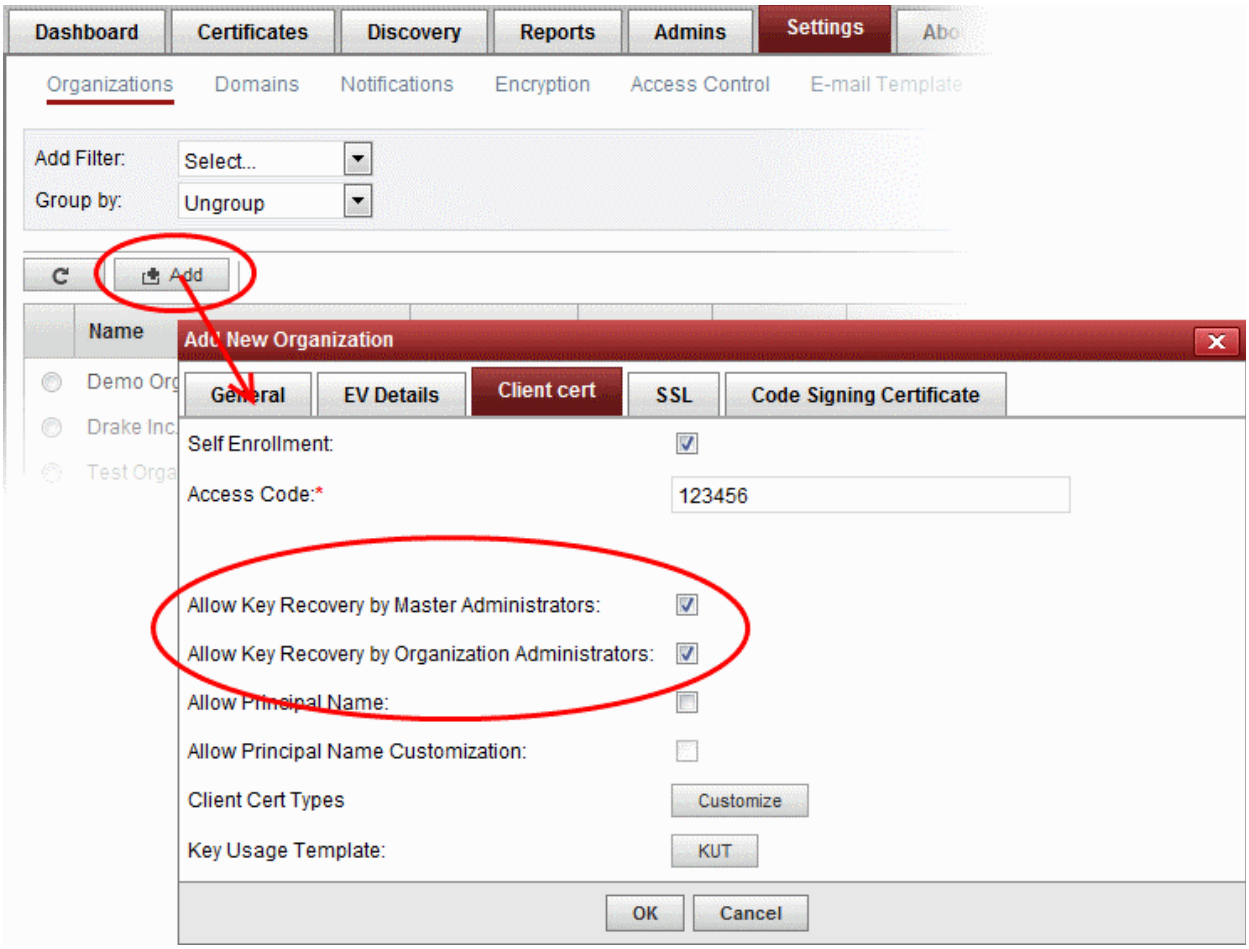
5.6.2 Setting up Key Escrow for an Organization

- Key recovery options are chosen during the creation of an Organization. Once chosen, these settings cannot be reversed.
- This section will deal purely with the key recovery elements of Organization creation. The key recovery settings are just one part of the overall Organization creation process. Administrators are therefore advised to treat this section as an information gathering exercise on key escrow prior to creating a new Organization. For a full outline of all steps and options involved in the creation an Organization, please see **Creating a New Organization**.

- Only an MRAO Administrator is able to specify key recovery settings for an Organization. This is because only an MRAO is able to create an Organization.

To set key recovery options:

- Select 'Settings' > 'Organizations' > 'Add'. This will open the 'Add New Organization' dialog box.
- Click the 'Client Cert' tab to view and configure key recovery options:



Allow Key Recovery by Master Administrators	*Checkbox* *Default state - checked*	If selected, the MRAO will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the MRAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificate UNTIL the MRAO has initialized their master key pair in the **Encryption** tab.
Allow Key Recovery by Organization Administrators	*Checkbox* *Default state - checked*	If selected, the RAO will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the RAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificate UNTIL the RAO has initialized their master key pair in the **Encryption** tab.
Allow Principal Name	*Checkbox* *Default state - unchecked*	Checking this box enables Principal Name support to the Organization. If enabled, the client certificates issued to the end-users of the Organization will include an additional name - Principal Name, in addition to the RFC822 name in the Subject Alternative Name(SAN) field. If included, the Principal Name will be 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/Department.

Allow Principal Name Customization	*Checkbox* *Default state - unchecked*	Checking this box enables customization of the Principal Names by the Administrator.
Key Usage Template	*Button*	The Key Usage Template (KUT) options allow administrators to specify the scope of key usage in client certificates at an Organization and/or Departmental level. It is possible for a key to be capable of (1) Digitally signing (2) Encrypting (3) Both signing and encrypting. Please refer to the section 'Defining Key Usage Template for an Organization's Client Certificates' for more details. • Clicking the 'KUT' button will open the '**Key Usage Template**' interface. From here you will be able to specify the usage scope of the keys of a particular organization. • The KUT defined through the 'Key Usage Template' interface will apply only to this specific Organization. **Important Note:** The Key Usage Template (KUT) feature will not be available by default. If required, the MRAO Administrator can contact Comodo and request for it. The KUT button will be visible to the MRAO Administrators only if it is enabled by Comodo.
The other settings in the 'Client Cert' tab are explained **here**.		

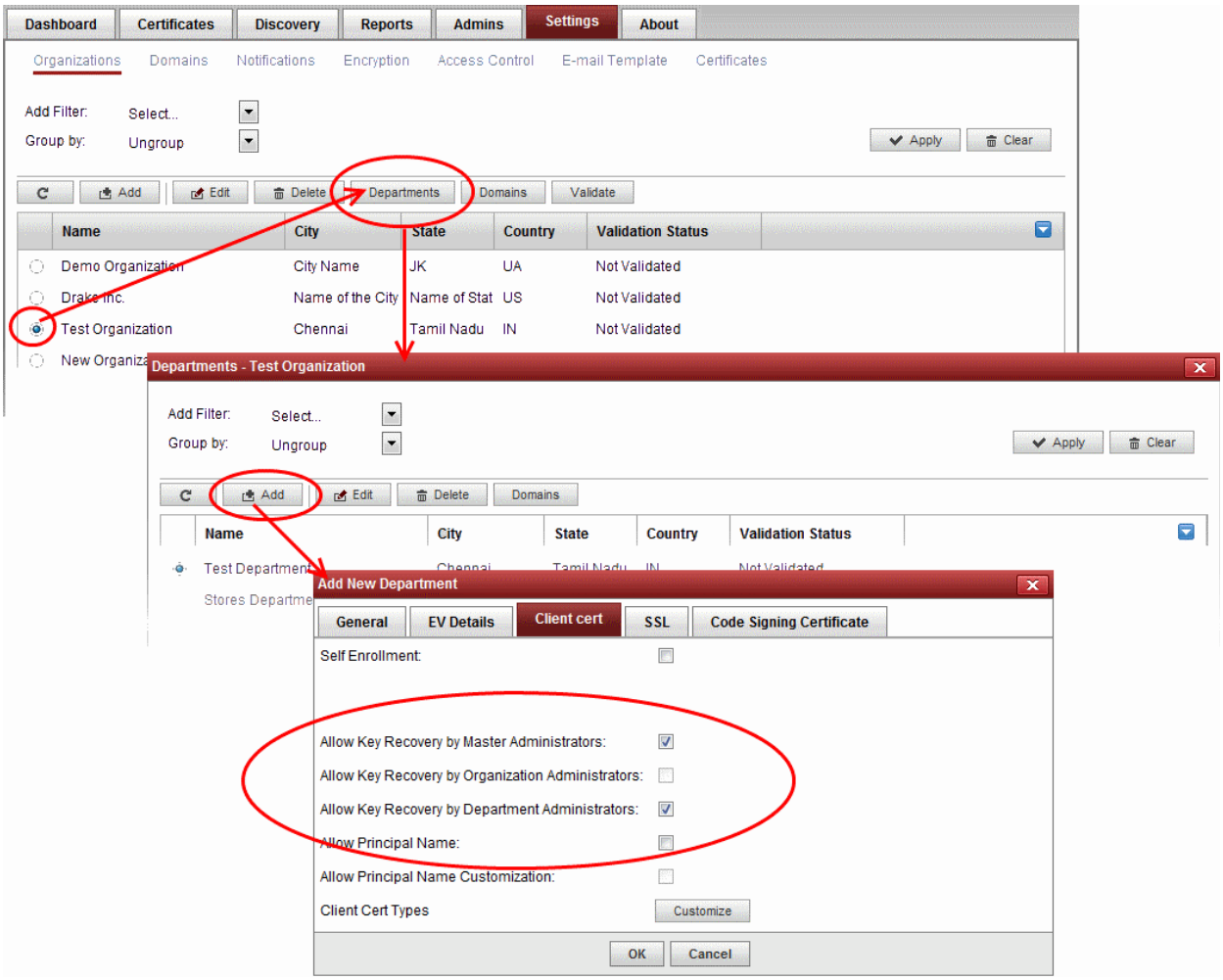
- Fill out the 'General Information' tab (and optionally the 'SSL' / 'Code Signing Certificate' tabs if those cert types are required). See **Creating a New Organization** for full details concerning the creation of a new Organization.
- Once you are satisfied with all settings, click 'OK' to add the Organization

5.6.3 Setting up Key Escrow for a Department

- Key recovery options are chosen during the creation of a Department. Once chosen, these settings cannot be reversed.
- This section will deal purely with the key recovery elements of Department creation. The key recovery settings are just one part of the overall Departmental creation process. Administrators are therefore advised to treat this section as an information gathering exercise on key escrow prior to creating a new Department. For a full outline of all steps and options involved in the creation a Department, please see **Managing the Departments of an Organization**
- Only MRAO Administrators and RAO SMIME Administrators are able to specify key recovery settings for an Organization. This is because only those types of Administrator are able to create a Department.

To set key recovery options:

- Select 'Settings' > 'Organizations'.
- Select the 'Organization' and click 'Departments' from the top to open the 'Departments' interface
- Click 'Add' from the 'Departments' interface to open Add New Department interface
- Click the 'Client Cert' tab to view and configure key recovery options:



Allow Key Recovery by Master Administrators	Checkbox Default state - checked if pre-enabled by MRAO*	If selected, the MRAO will have the ability to recover the private keys of client certificates issued by this Department. At the point of creation, each client certificate will be encrypted with the MRAOs master public key before being placed into escrow. If this box is selected then the Department will not be able to issue client certificate UNTIL the MRAO has initialized their master key pair in the **Encryption** tab
Allow Key Recovery by Organization Administrators	Checkbox Default state - checked if pre-enabled by MRAO*	If selected, the RAO will have the ability to recover the private keys of client certificates issued by this Department. At the point of creation, each client certificate will be encrypted with the RAOs master public key before being placed into escrow. If this box is selected then the Department will not be able to issue client certificate UNTIL the RAO has initialized their master key pair in the **Encryption** tab.
Allow Key Recovery by Department Administrators	Checkbox Default state - checked if pre-enabled by MRAO*	If selected, the DRAO SMIME Administrator will have the ability to recover the private keys of client certificates issued by this Department. At the point of creation, each client certificate will be encrypted with the DRAOs master public key before being placed into escrow. If this box is selected then the Department will not be able to issue client certificates UNTIL the DRAO has initialized their master key pair in the **Encryption** tab.
Allow Principal Name	Checkbox Default state - unchecked if pre-enabled by MRAO*	Checking this box enables Principal Name support to the Department. If enabled, the client certificates issued to the end-users of the Department will include an additional name - Principal Name, in addition to the RFC822 name in the Subject Alternative Name(SAN) field. If included, the Principal Name will be 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

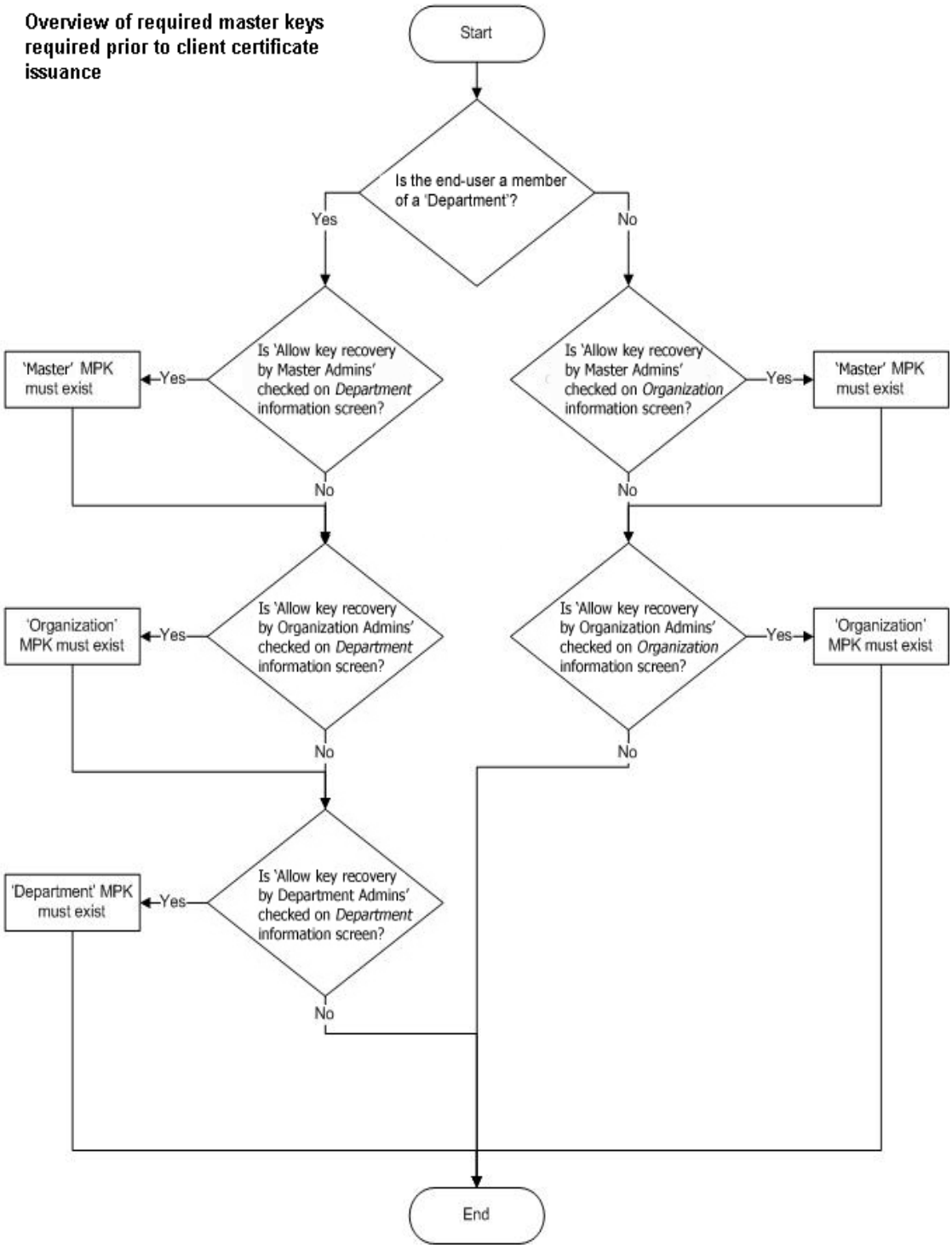
		Organization/Department.
Allow Principal Name Customization	Checkbox Default state - unchecked if pre-enabled by MRAO*	Checking this box enables customization of the Principal Names by the Administrator.
** The checkboxes will only be active IF the MRAO has enabled the appropriate key recovery options when **configuring client certificate options** for the Organization.* The other settings in the 'Client Cert' tab are explained **here**.		

- Fill out the 'General Information' tab (and optionally the 'SSL' / 'Code Signing Certificate' tabs if those cert types are required). See **Creating a New Organization** for full details concerning the creation of a new Organization.
- Once you are satisfied with all settings, click 'OK' to add the Department

5.6.4 Master Keys Required Prior to Client Cert Issuance

The diagram below is an overview of the master keys necessary per recovery requirements for the successful issuance of client certificates:

Overview of required master keys required prior to client certificate issuance



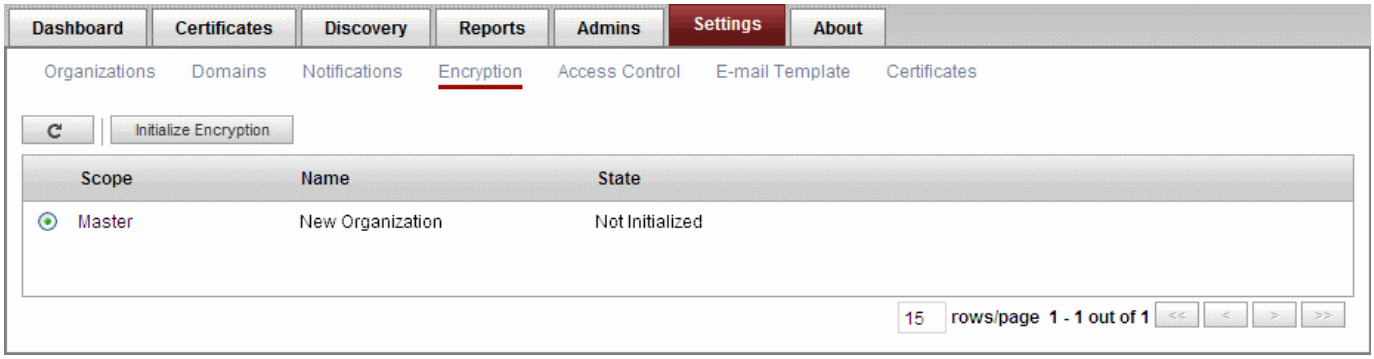
Notes:

- Administrators can find out whether recovery is checked for an Organization by clicking 'Settings > Organizations', clicking the 'Edit' button of the Organization in question then selecting the 'Client Cert' tab.
- MRAO and RAO SMIME Administrators can find whether recovery is checked for a Department by clicking 'Settings > Organizations', then clicking the 'Departments' button of the Organization in question. Next, select the Department in question and click 'Edit' button, then select the 'Client Cert' tab.
- 'MPK must exist' means that the key must have been initialized. If the key has not been initialized then the Organization or Department in question will not be able to issue client certificates. If key escrow is required through all tiers (MRAO + Organization + Department) then this means that 3 master private keys will need to be initialized. To check initialization status, the currently logged in administrator should click the 'Encryption' tab

5.6.5 Encryption

This area allows administrators to encrypt the private keys of user's client certificates. If key recovery was specified during the creation of an Organization or Department, then this step is *essential.* No client certificates can be issued until the master key pairs have been initialized.

Note: This area is visible and accessible by the MRAO and by RAO/DRAO SMIME Admins if key recovery has been enabled for their specific Organization/Department.



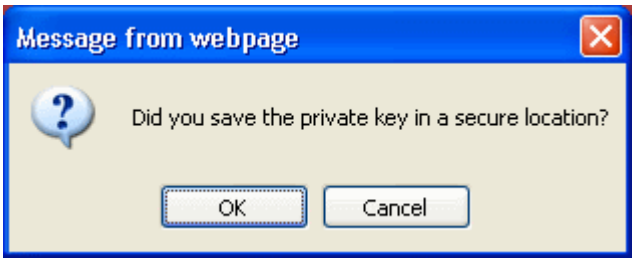
5.6.5.1 Summary of Fields and Controls

Column Display		Description
Scope		The Hierarchy level of the Organization/Department. It can be the Master, Organization or Department.
Name		The name of the Organization/Department.
State		Indicates the status of private key encryption.
Controls		
	Refresh	Reloads the list.
Encryption Controls **Note**: The Encryption control buttons will appear only on selecting the scope and depending on the state of private key encryption		
	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.
	Reencrypt	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.

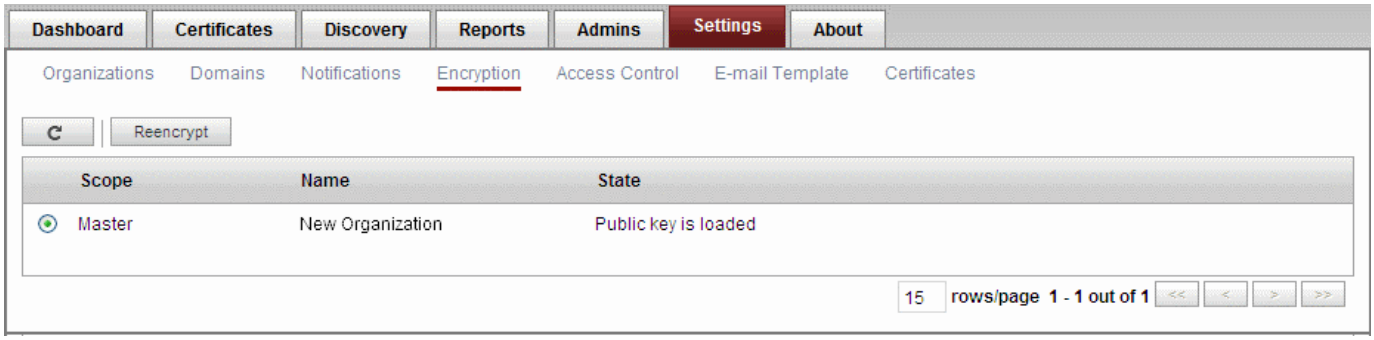
5.6.6 Encrypting the Private Keys

To use this feature the administrator needs to initialize private key encryption by clicking 'Initialize Encryption' button. The process will be started and a master private key will be generated. The administrators need to copy the private key and paste it in a .txt file and store in a secure location.

Note: This 'master' private key is not stored within Comodo Certificate Manager. We advise administrators to save the private key in a secure, password protected, location. It will be required should the administrator wish to either re-encrypt the keys or download a user's client certificate.



On clicking 'Done', the state is changed to 'Public key is loaded'.



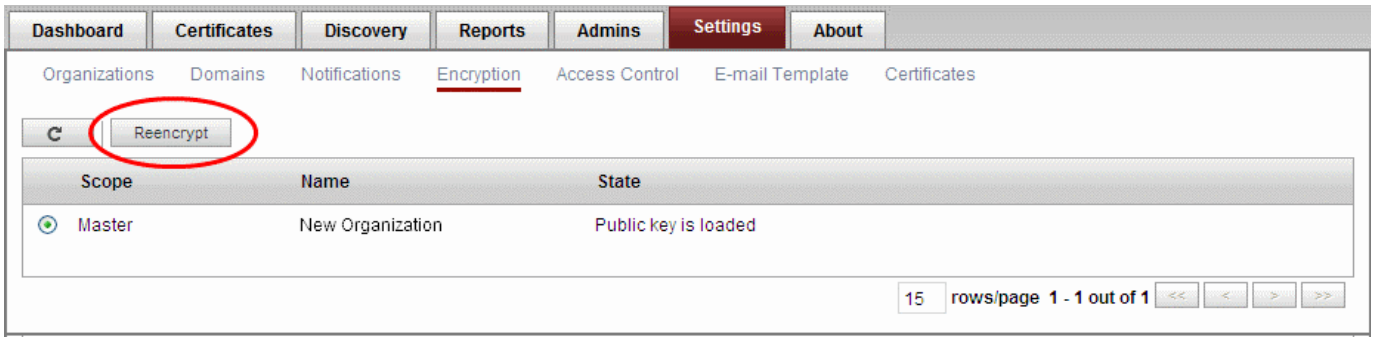
All the private keys of user client certificates are now encrypted using the master public key of the administrator that began this process. Decryption will require the private key that was saved earlier.

5.6.7 Re-encryption

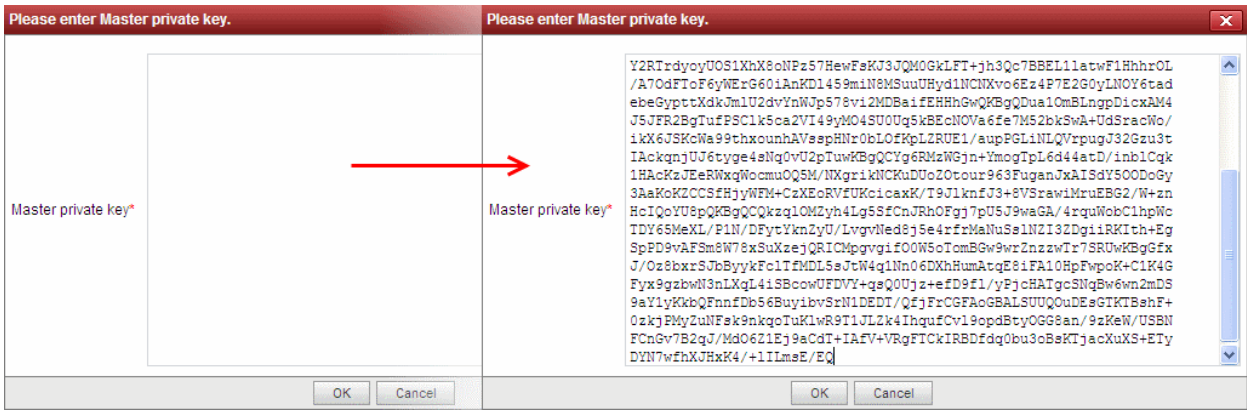
The re-encryption functionality allows MRAO, RAO SMIME and DRAO SMIME Administrators to change the master key pair and then automatically re-encrypt existing end-users key pairs with the new master public key. This may be necessary if the original private key becomes compromised or administrative personnel leave the company.

To start the Re-encryption process

- Select the scope and click the 'Reencrypt' button alongside the Organization/Department in the Controls column.

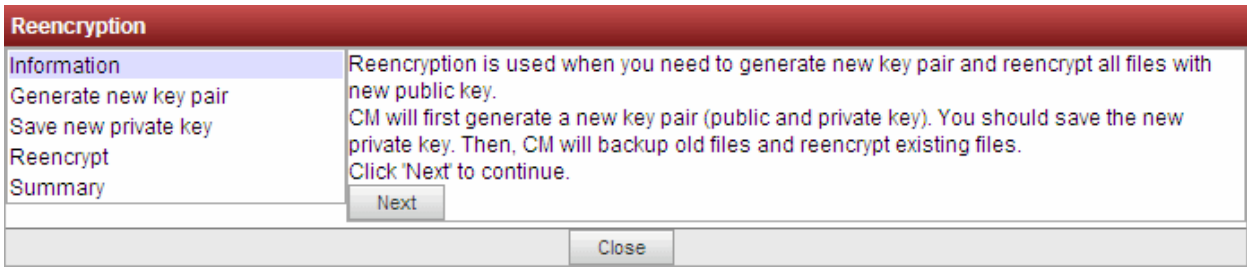


The Administrator will be prompted to paste the existing master private key to start the process:

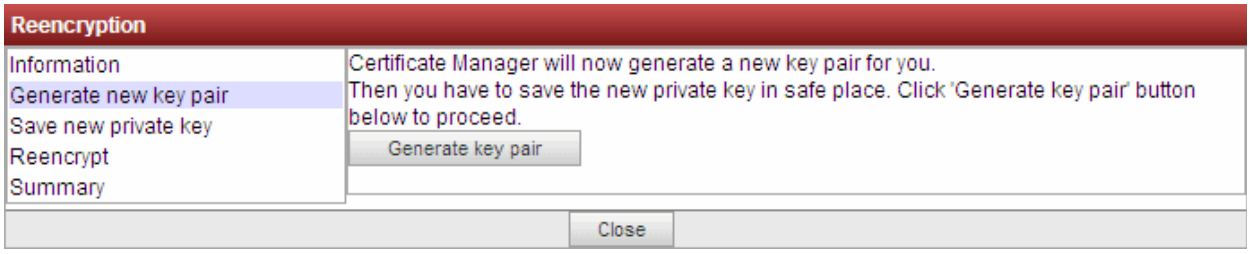


- Paste the Master key and click OK.

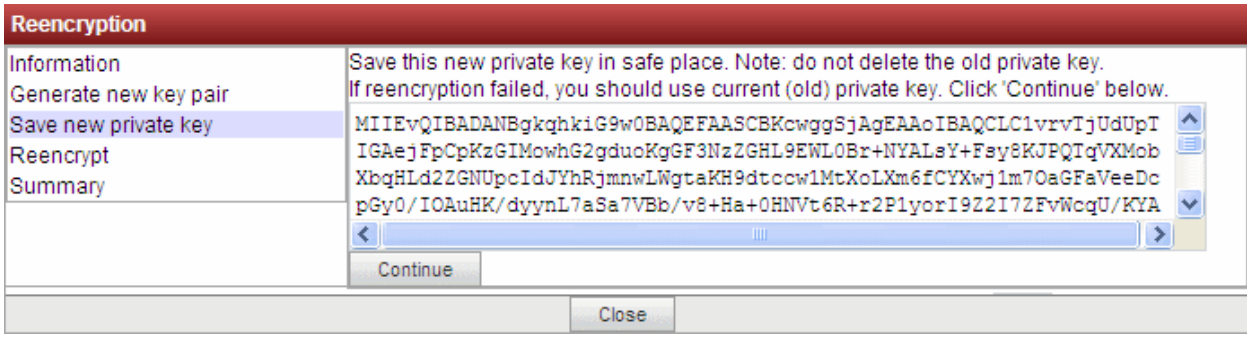
The re-encryption dialog will appear. This will provide a brief summary of the forthcoming process.



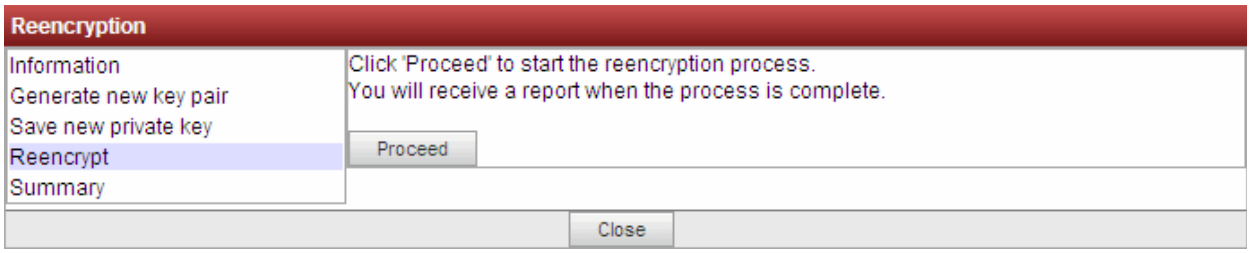
- Click 'Next' to continue:



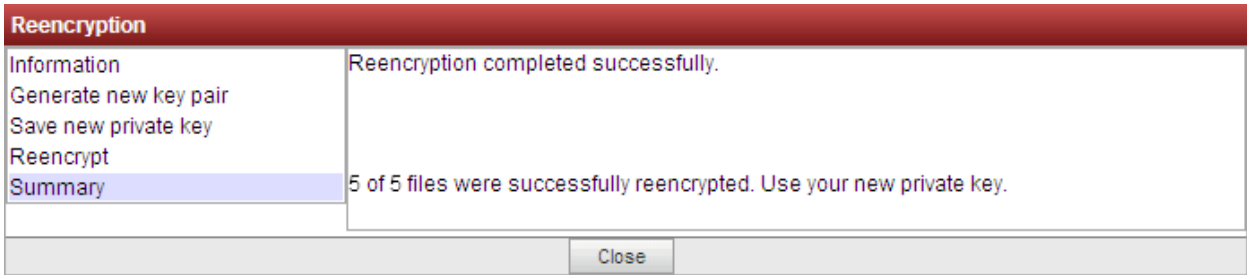
- Click the 'Generate Key Pair' to generate the new keys:



- Copy and paste the private key into a .txt file then save it in a secure, password protected location. Click 'Continue'. The re-encryption of the private keys will be started.



- Click 'Proceed' to begin re-encrypting the private keys of client certificates. Upon successful re-encryption, a summary screen will be displayed.

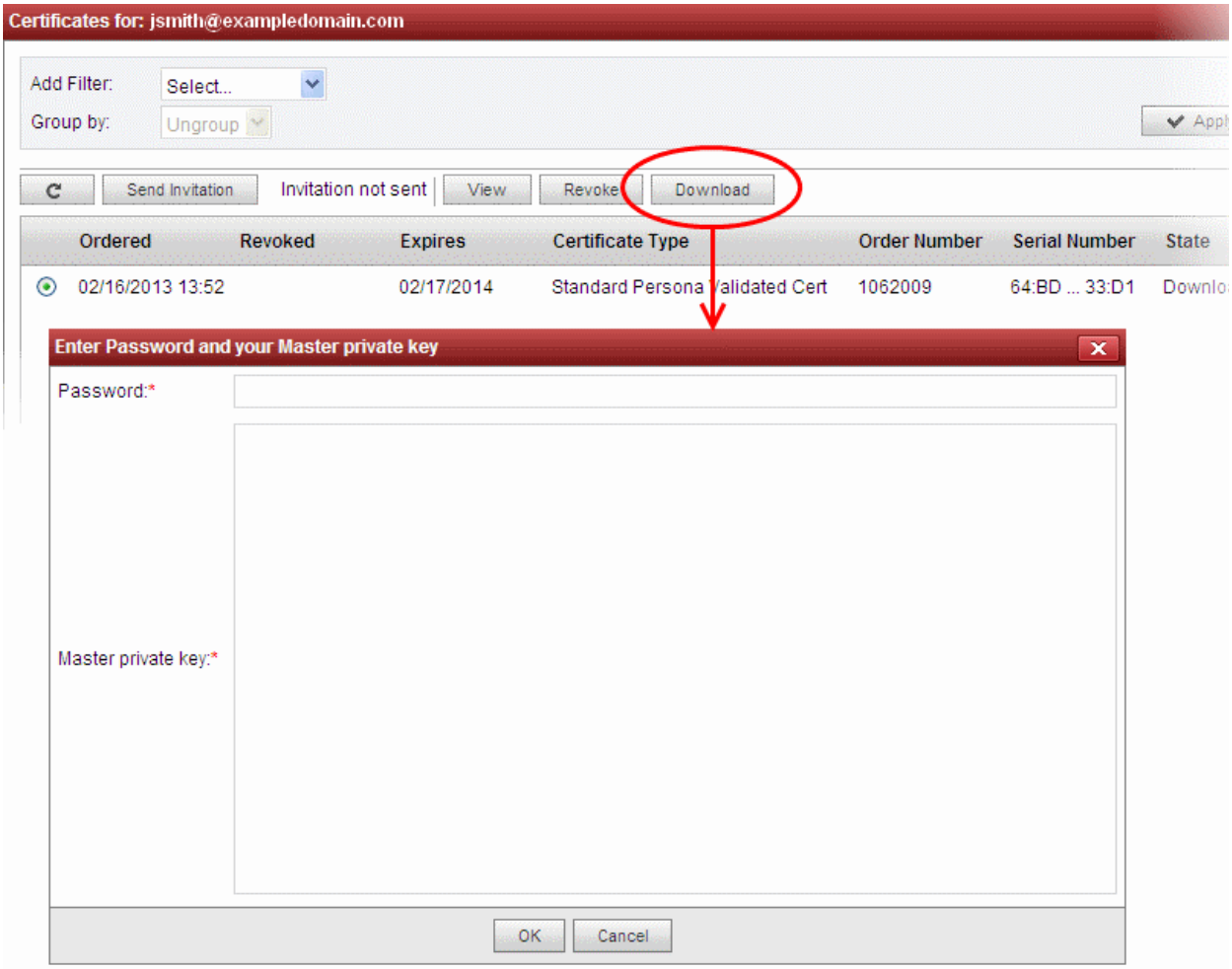


5.6.8 Recovering a User's Private Key from Escrow

The administrator may need to recover a users private key in order to decrypt data if, for example, the original client certificate belonging to and-user was lost or if the user left the company. The end-user's private key can be downloaded from the 'Certificates' > 'Client Certificates' interface.

- Open the 'Client Certificates' interface by clicking 'Certificates' > 'Client Certificates'.
- Select the end-user and click the 'Certs' button from the top. The 'Certificates for' interface will open with the list of all the certificates belonging to the end-user in chronological order (newest first).
- Select the certificate and click 'Download'

Note: Administrators should have their master private key ready - it will be required to complete this process.



In order to decrypt this end-user's key pair the administrator must paste the corresponding 'master' private key into the space provided in order to download any end-user's client certificates. The administrator can also set a password to protect access to private key in .p12 file as well.

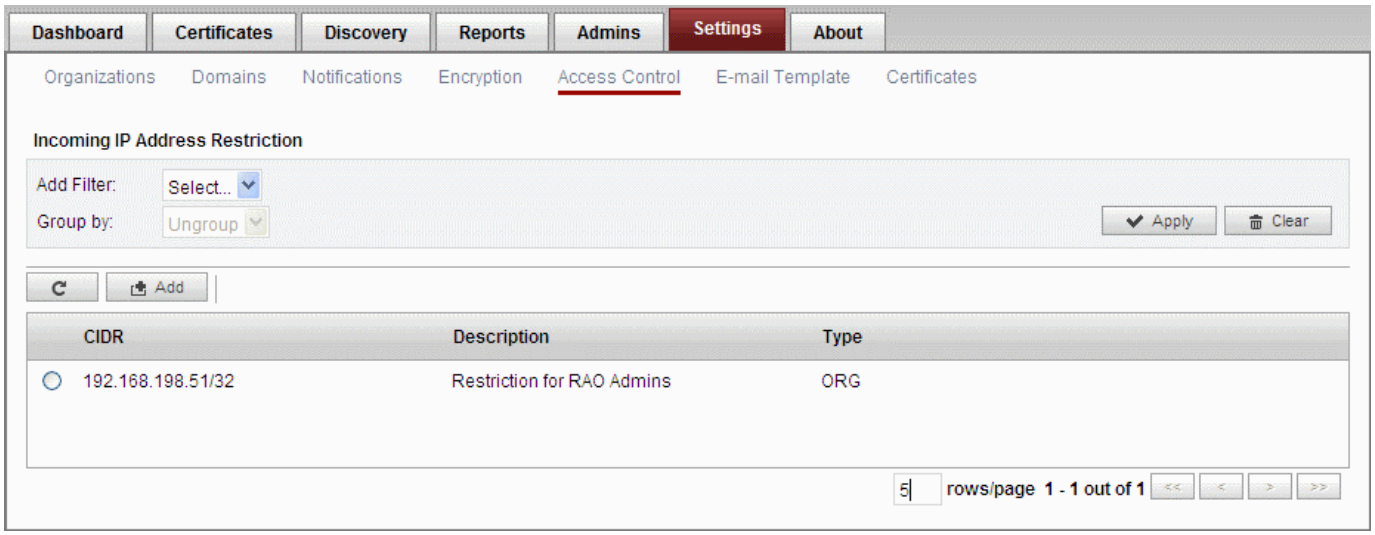
Note: Successfully downloading the private key of a client certificate will revoke that certificate.

5.7 Access Control

5.7.1 Overview

The 'Access Control' area is visible only to the MRAO. The MRAO can configure and limit incoming access to the CCM interface to certain IP addresses and ranges. This is very useful if they want to grant access only to certain IP addresses and so prevent unauthorized or unsecured access to the CCM interface.

- After specifying one or more IP addresses or ranges in CIDR notation, only administrators attempting to login from these specified addresses will be allowed access.
- Any user who is blocked from accessing CCM interface because of restriction will be provided a generic '403 Access Denied' error.
- The Access Restrictions can be applied for all the administrators, or selectively for MRAO administrator only or to RAO/DRAO administrators only.

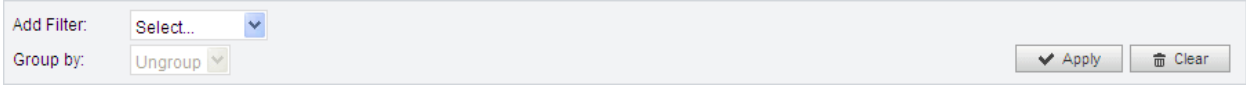


5.7.1.1 Access Control Options - Table of Parameters

Form Element		Description
CIDR		Short for Classless Internet DOMAIN Routing. Administrator should specify IP range: it should be IP address followed by network prefix, e.g. 123.456.78.91/16.
Description		Contains additional information.
Type		Displays the administrative role, like All, MRAO and RAO for which the CIDR is defined
Control Buttons	Add	Opens 'Add IP Range' dialog.
	Refresh	Updates the list of IP ranges.
CIDR Control Buttons **Note**: The CIDR control buttons are visible only on selecting a CIDR entry	Edit	Enables administrator to edit CIDR's details.
	Delete	Enables administrator to delete the CIDR.

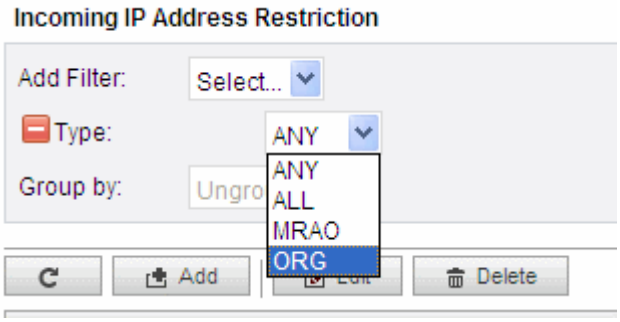
5.7.1.2 Filtering Options

Administrators can search for CIDR entries by using filters:



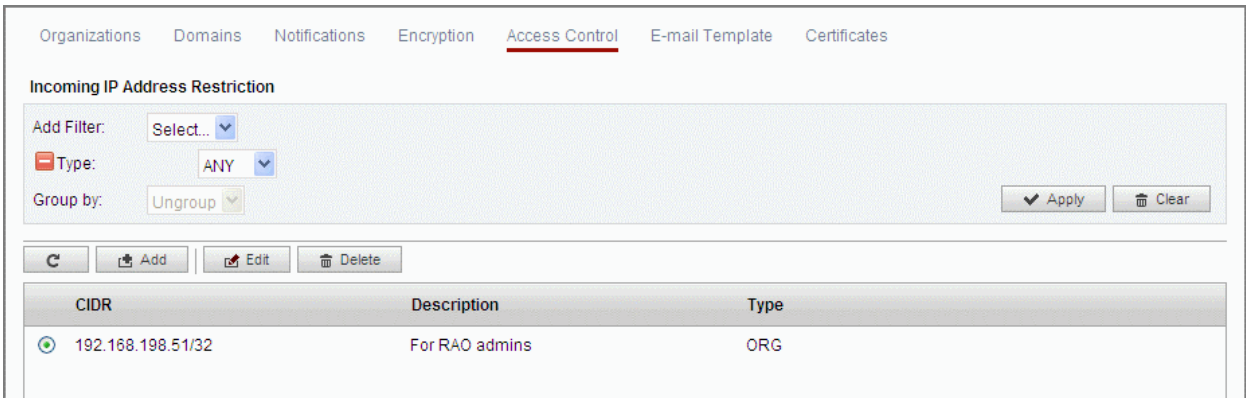
Filter Options	Description
Type	Enables the administrator to filter the CIDR details based on administrative roles: • All • MRAO • ORG

You can add filters by selecting from the options in the 'Add Filter' drop-down. For example, if you want to filter the CIDR entries based on a specific type, select 'Type' from the 'Add Filter' drop-down and the type of administrative role from the 'Type' drop-down:



- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed:

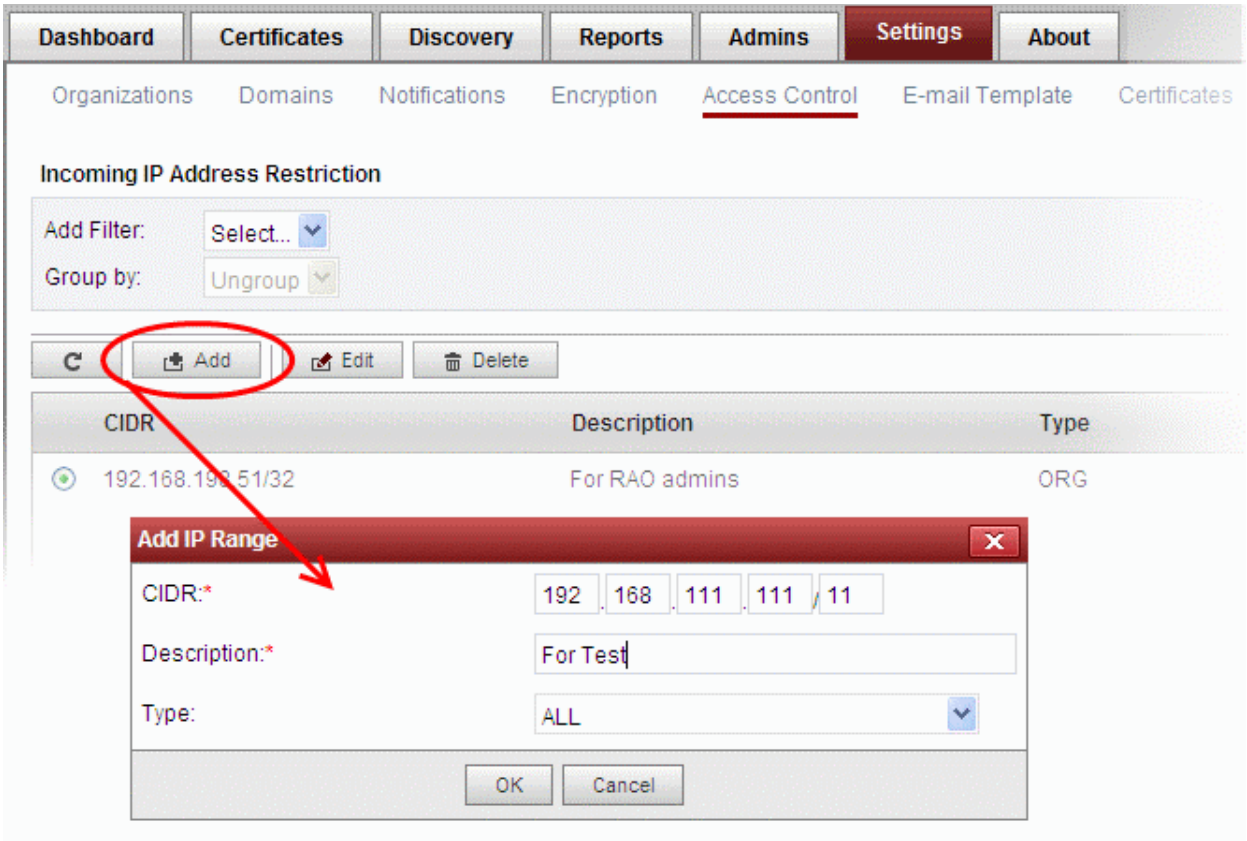


- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Access Control' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

5.7.2 Adding a New IP Range

New IP range can be added by clicking on 'Add' button in the interface the as shown below:



5.7.2.1 Add IP Range - Table of Parameters

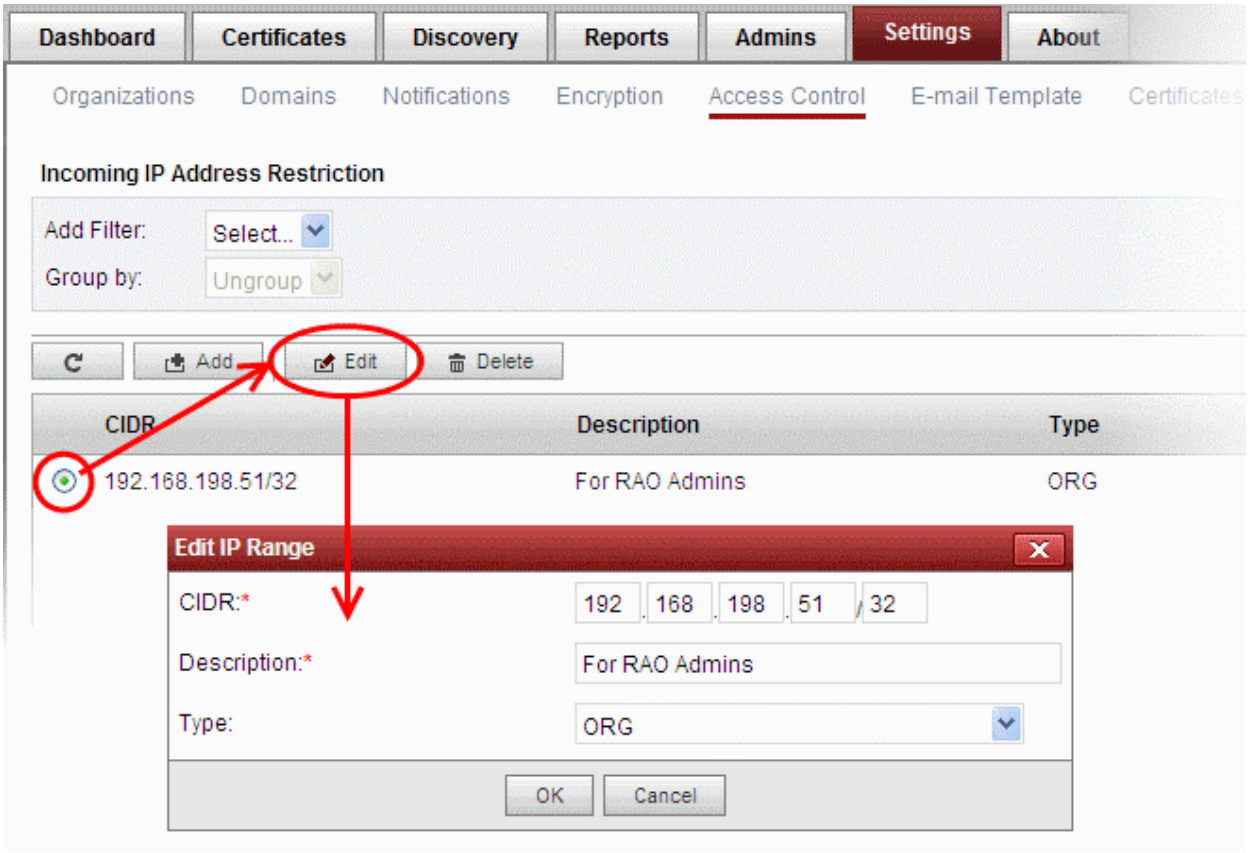
Field Name	Values	Description
CIDR (Required)	Numeric	The administrator should type the incoming IP ranges followed by network prefix, from which the access to the CCM interface has to be granted. All other IP addresses will be blocked. If no IP range is specified in Access Control then the default setting is to allow access from any IP:
Description (Required)	String	A short description of the IP range added.
Type	drop-down	Enables the administrator to select on whether the IP address restriction has to be imposed to all the administrators, MRAO administrator or the RAO administrators. All - The IP address based access restriction is imposed for all the administrators including the MRAO administrator. MRAO - The IP address based access restriction is imposed only for the MRAO administrator. ORG - The IP address based access restriction is imposed only all the RAO/DRAO administrators and not the MRAO administrator.

Additions and changes to the access control list will not take effect for the administrator's current session, they will take effect only on the administrator's next login.

Tip: The administrator can also configure and limit incoming access to the CCM interface to certain IP addresses and ranges for the Organizations individually. Refer to the section **Editing an Existing Organization** for more details.

5.7.3 Editing an IP Range

An existing IP range can be edited by selecting the entry and clicking the 'Edit' button the as shown below:



The administrator can edit the values and click OK for the changes to be saved. The changes to the access control list will not take effect for the administrator's current session, they will take effect only on the administrator's next login.

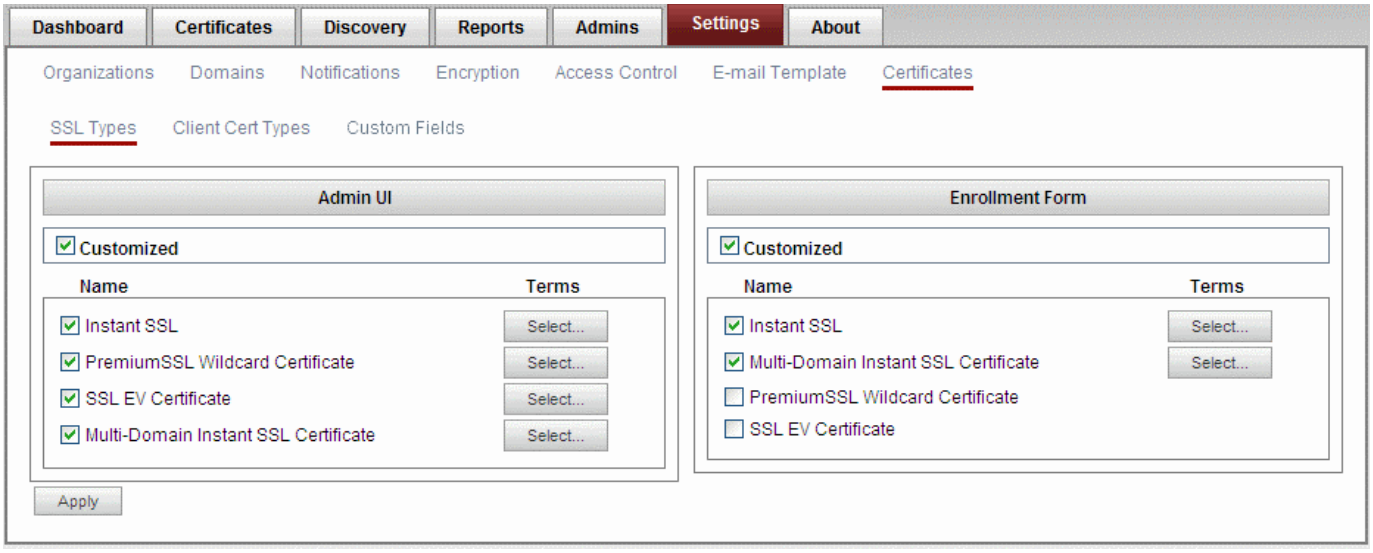
- To remove a CIDR entry, select it and click 'Delete' from the top.

5.8 Certificates

5.8.1 Section Overview

The 'Certificates' tab allows the MRAO Administrators to customize the types of SSL and Client certificates and their term lengths that are available for the new applications to all the new applications to all Organizations through the Built-in application form and the Self Enrollment form. The Custom Field tab in this area allow MRAO Administrators to configure to add fields in the **Built-In Application form** and the **Self Enrollment Form** for SSL and Client certificate requisition.

Note: The Custom Field tab will be available only if this feature is enabled for your account. If this is not available and want to add this option, please contact your Comodo account manager.

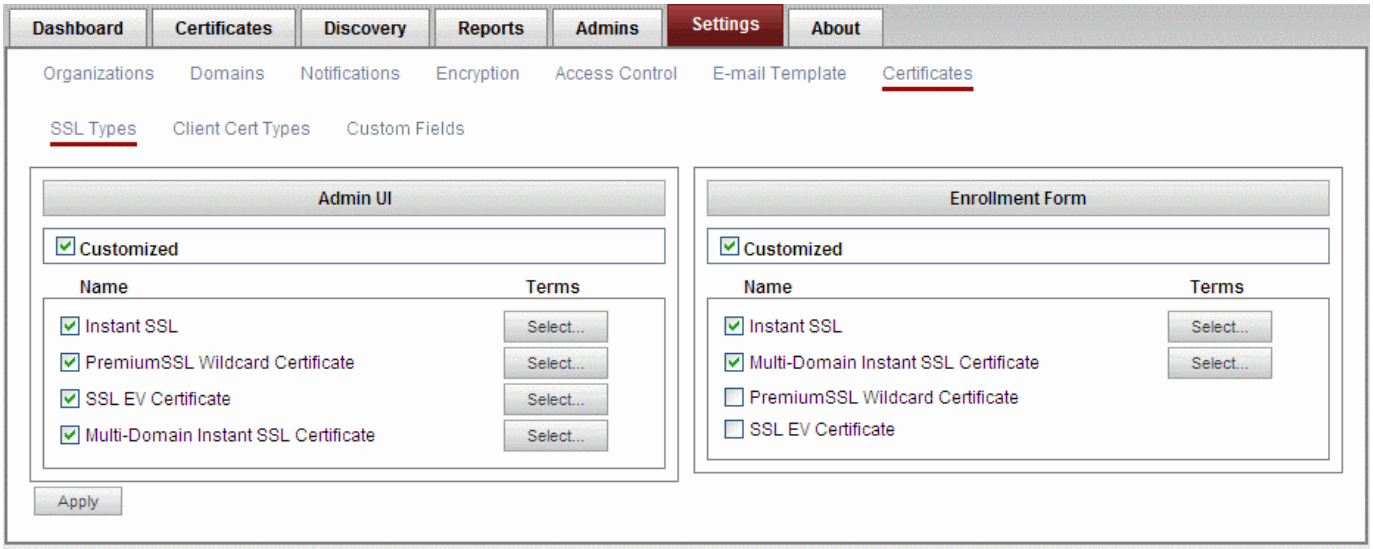


Note: The Certificates area is visible to and accessible only by MRAO Administrators.

5.8.2 SSL Types

The SSL Types tab allows the MRAO Administrators to customize the types of SSL certificates and their term lengths that are available for the new applications to all Organizations through the Built-in application form and the Self Enrollment form. It can be useful to create a such a targeted 'certificate roster' as it simplifies the certificate selection procedure at the application forms and helps avoid applications for certificates which are inappropriate.

Note: The SSL Types area is visible to and accessible only by MRAO Administrators.



- **Admin UI** - Determines the SSL certificate types that will be available to applicants using the **Built-In Application form**
- **Enrollment Form** - Determines the SSL certificate types that will be available to applicants using the **Self Enrollment Form.**
- It is therefore possible to choose a different selection of certificate availabilities depending on whether the Built-in or Self-Enrollment form is to be used.

SSL Types - Table of Parameters		
Field Name	**Type**	**Description**

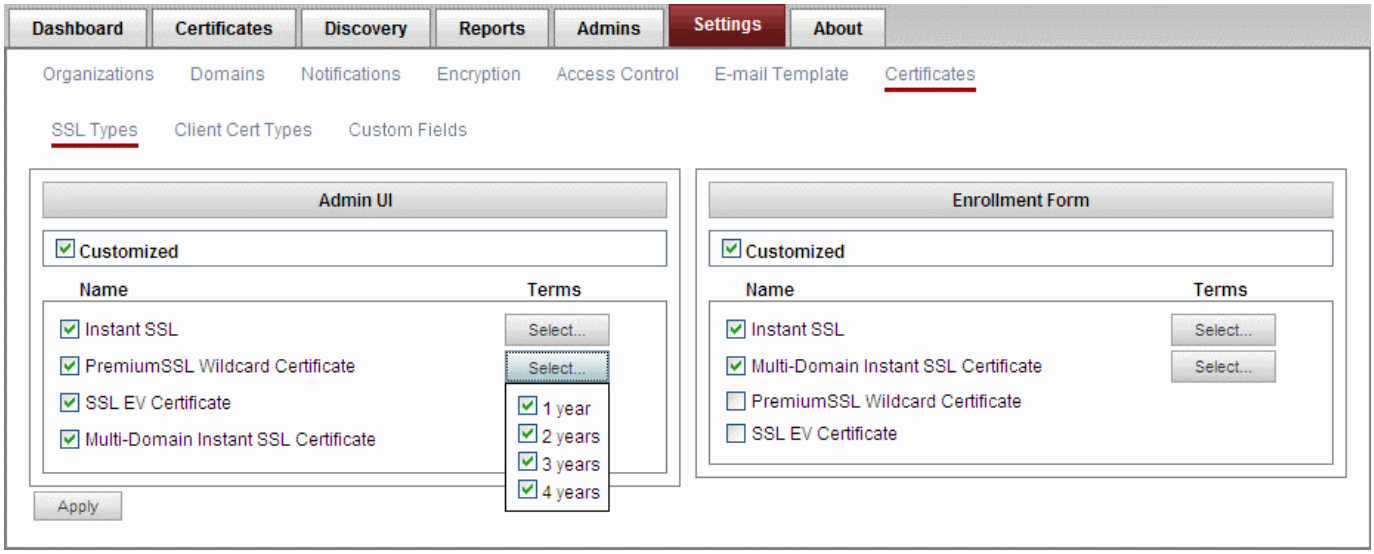
Customized	Checkbox	Checking this box enables customization of the SSL types. Leaving this unchecked means all the certificate types are available through both the Built-in Application form and the Self Enrollment form.
Name	List of Certificate types with checkboxes	Lists the SSL types that are assigned available for your account by your account Manager. For more details on Comodo SSL certificates refer **Comodo SSL Certificates.** **Note:** If a certificate or certificate term is not present here, administrators should contact their account manager to have it added.
Terms	Drop-down options	Clicking the Select button opens a drop-down box displaying the Term lengths available for the Certificate type.

By default, the 'Customized' option is left unchecked so that all the certificate types are available through both types of application form.

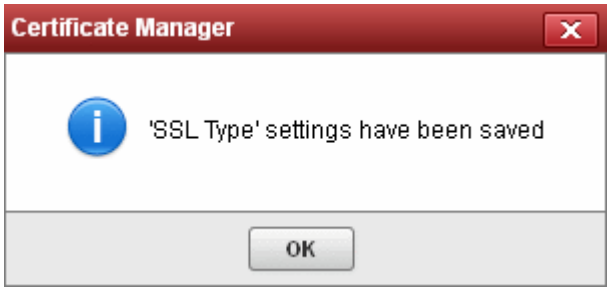
5.8.2.1 Customize SSL Certificate Types

To restrict the SSL types and their durations

1. Select the 'Customized' option below either or both 'Admin UI' and 'Enrollment Form'.
2. Check the names of the certificates you wish to be available on the whole and leave the others unchecked.
3. Click the 'Select' button next to the certificate name to choose which terms will be available.

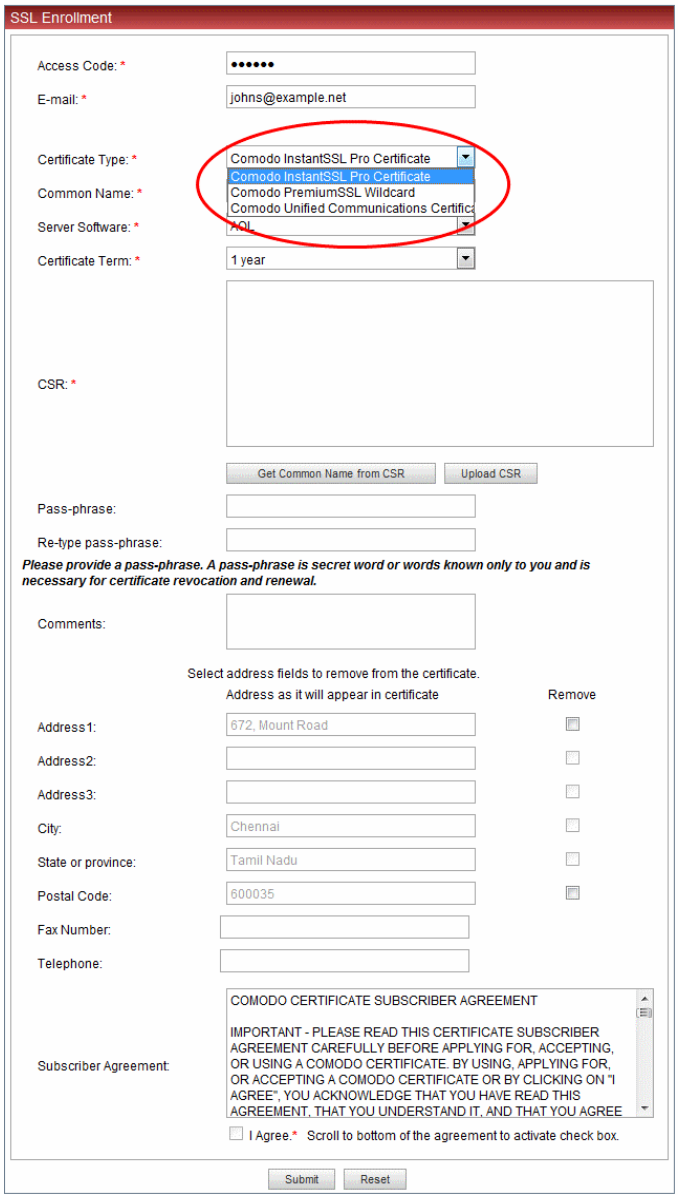


4. Click Apply. The confirmation dialog on saving your settings appears.

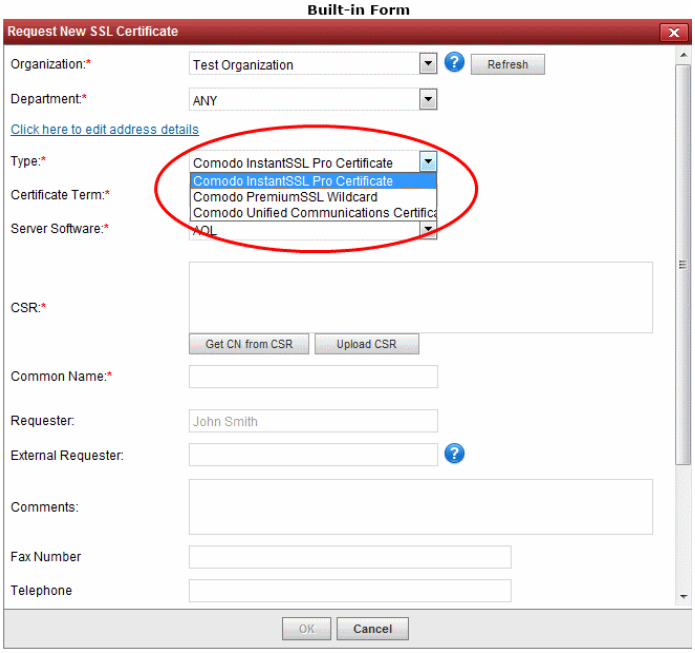


Only the types and terms of SSL certificates that are selected in the 'SSL Types' interface will now be available in the 'Type' and 'Term' drop-down fields of the Built-in Application form and the Self Enrollment form.

Self Enrollment Form



Built-in Form



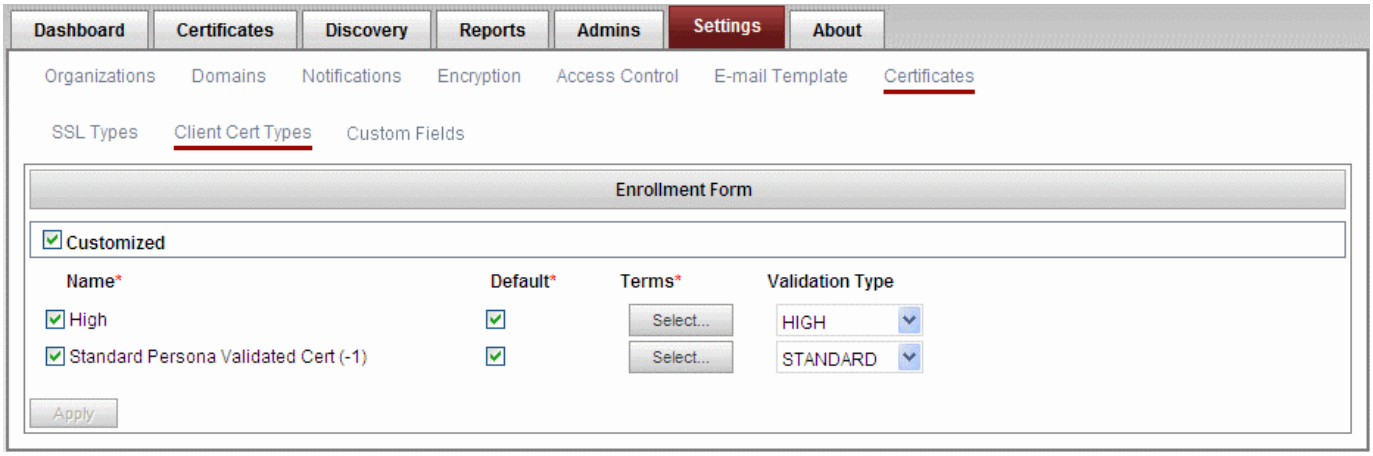
Notes:

- The SSL Types tab can be accessed only by the MRAO administrators and is not visible to RAO and DRAO Administrators.
- The selection of SSL Types and their Term lengths apply to all Organizations. For restricting SSL types available for a specific Organization, refer **Customize an Organization's SSL Certificate Types.**
- The certificate types or terms that are disabled through the SSL Types tab will not be available even in the **'Bind SSL Types' interface.** To add a specific certificate type/term for a particular Organization, the RAO SSL Administrators should seek the advice of the MRAO Administrator.

5.8.3 Client Cert Types

The Client Cert Types tab allows the MRAO Administrators to customize the types of client certificates and their term lengths that are available for the end-users for the all Organizations/Departments through self enrollment form (both Access Code based and Secret ID based). It can be useful to create a such a targeted 'certificate roster' as it simplifies the certificate selection procedure at the application forms and helps avoid applications for certificates which are inappropriate.

Note: The Client Cert Types area is visible to and accessible only by MRAO Administrators.



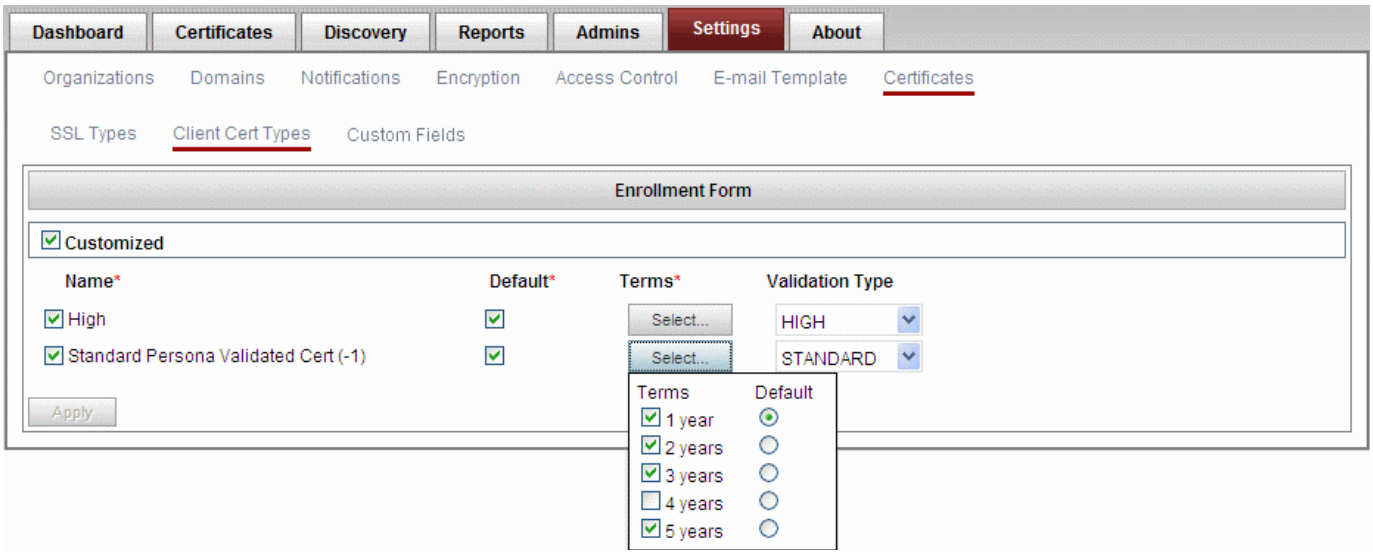
Client Cert Types - Table of Parameters		
Field Name	**Type**	**Description**
Customized	Checkbox	Checking this box enables customization of the Client Cert types. Leaving this unchecked means all the certificate types are available to the end-users.
Name	List of Certificate types with checkboxes	Lists the Client Certificate types that are assigned available for your account by your account Manager. **Note:** If a certificate or certificate term is not present here, administrators should contact their account manager to have it added.
Default	Checkbox	Allows the Administrator to set the certificate type as Default type for the Organizations. The client certificate type(s) for which the default checkbox is selected, will stand as default option(s) in the Self Enrollment forms for applying for Client Cert by end-users. **Note**: At least one certificate type has to be selected as default type.
Terms	Drop-down options	Clicking the Select button opens a drop-down box displaying the Term lengths available for the Certificate type.
Validation Type	Drop-down options	Allows the administrator to specify the type of client certificate that is issued to an applicant. The difference between the two lies in the degree of user authentication is carried out prior to issuance. The two options available are 'Standard' and 'High' validation types. 'Standard' certificates can be issued quickly and take advantage of the user authentication mechanisms that are built into CCM. A user applying for a 'Standard Personal Validation' certificate is authenticated using the following criteria: • User must apply for a certificate from an email address @ a domain that has been delegated to the issuing Organization • The Organization has been independently validated by an web-trust accredited Certificate Authority as the owner of that domain • 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 the administrator to the user via out-of-band communication. • 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 will contain a validation code that the user will need to enter at the certificate collection web page.

		'High Personal Validation' certificates require that the user undergo the validation steps listed above AND • Face-to-Face meeting with the issuing Organization **Note**: The additional validation steps must be completed PRIOR to the administrator selecting 'High Personal Validation' type.

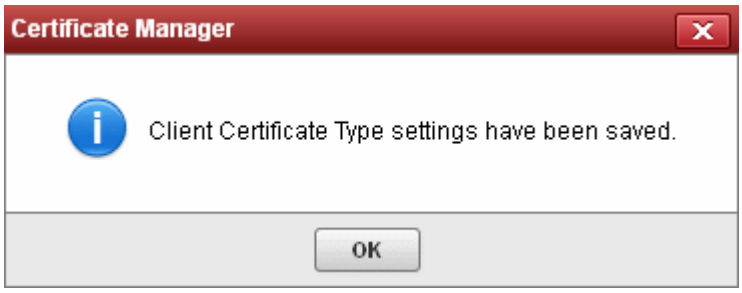
5.8.3.1 Customize Client Certificate Types

To restrict the SSL types and their durations

1. Select the 'customized' checkbox.
2. Check the names of the certificates you wish to be available on the whole and leave the others unchecked.
3. Select the 'Default' checkbox, if you wish this certificate type(s) has to be shown as default selected option in both access code based and secret ID based self-enrollment forms.
4. Click the 'Select' button next to the certificate name to choose which terms will be available. If you want to set the selected term as default term for the selected certificate type, select Default radio button.



5. Select the Validation type from the drop-down. For more information on the validation types, refer the **table** in the section **Overview**.
6. Click Apply. The confirmation dialog on saving your settings will appear.



Only the types and terms of client certificates that are selected in the 'Client Cert Types' interface will now be available in the 'Type' drop-down field of the Self Enrollment form.

Notes:

- The Client Cert Types tab can be accessed only by the MRAO administrators and is not visible to RAO and DRAO Administrators.
- The selection of Client Certificate Types and their Term lengths apply to all Organizations. For restricting client certificate types available for a specific Organization, refer **Customize an Organization's SSL Certificate Types.**
- The certificate types or terms that are disabled through the Client Cert Types Types tab will not be available even in the '**Bind Client Cert Types**' interface. To add a specific certificate type/term for a particular Organization, the RAO SSL Administrators should seek the advice of the MRAO Administrator.

5.8.4 Custom Fields

An SSL or a Client certificate has standard fields that contain information about the owner, domain, organization, department, address and so on. Some businesses may wish track additional information such as 'Employee Code' or 'Telephone Number'. Comodo Certificate Manager offers businesses the flexibility to track any information associated with the certificate by specifying custom fields that certificate requesters can fill in.

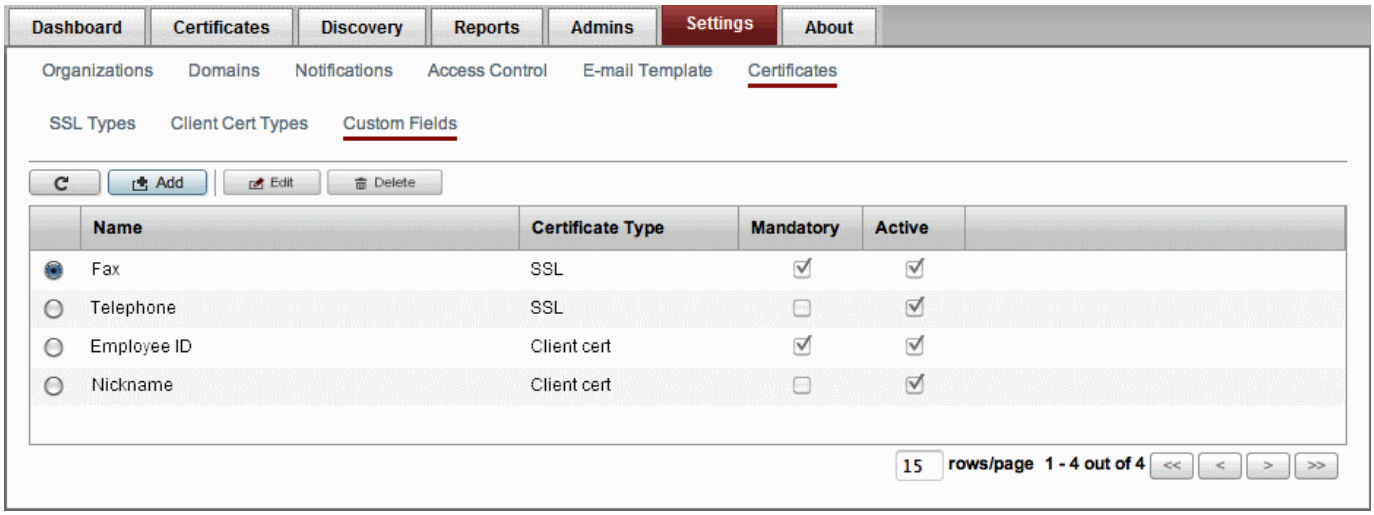
The Master Registration Authority Officer (MRAO) administrator can add additional fields to enrollment forms for both SSL and Client certificates. They can also specify whether the new fields should be mandatory or optional.

Note: The Custom Field tab will be available only if this feature is enabled for your account. If this is not available and you want to add this option, please contact your Comodo account manager.

In brief:

- Custom fields are not enabled by default. If you require the custom fields feature, please contact your account manager.
- Once enabled, custom fields can be configured by clicking Settings > Certificates > Custom Fields
- MRAO administrators can configure the name of the field, the certificate type to which it should apply (SSL or client certificates), whether or not the field should be mandatory and whether or not the custom field should be active.
- Custom fields can be edited at any time. Deactivating a custom field will remove it from the enrollment forms but all associated data will be retained. However, deleting a field will delete all data associated with the field.
- Once added, the custom fields will appear on the enrollment and renewal forms for your certificates.

Note: The Custom Fields area is visible to and accessible only by MRAO Administrators.



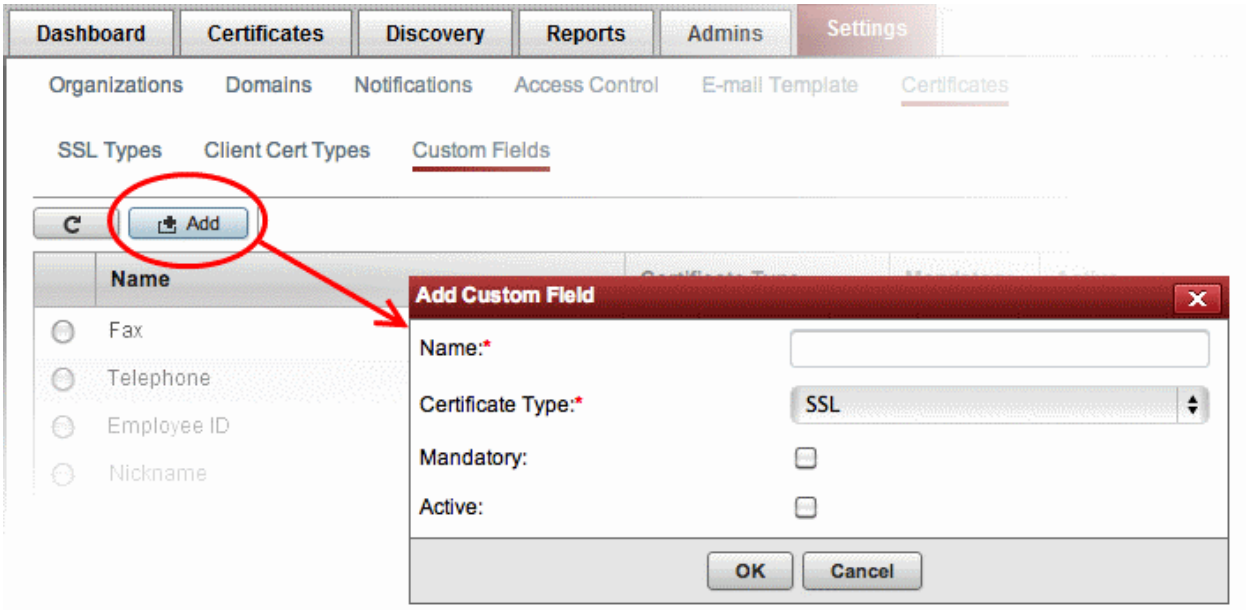
'Custom Fields' - Descriptions of Columns		
Column Name		**Description**
Name		Name of the custom field.
Certificate Type		The type of the certificate to which the custom field is applicable. Can be either 'SSL' or 'Client Cert'.
Mandatory		Allows administrators to toggle between mandatory and optional states. If a field is made mandatory then the form cannot be submitted without completing the field. Mandatory fields will be marked with an asterisk* on the form.
Active		Toggle the custom field between active and inactive states. If a field is made inactive, it will be hidden in the future application forms. However, existing data for this field will be retained in the database.
Control Buttons	Add	Allows the administrator to add a new custom field.
	Refresh	Updates the currently displayed list of custom fields.
Custom Field Control Buttons **Note**: Control buttons will appear only after selecting a particular custom field	Edit	Allows the administrator to edit the parameters of a particular custom field.
	Delete	Deletes the custom field. Unlike deactivation, deleting a field will also delete all data associated with this field.

5.8.4.1 Adding a new Custom Field

An MRAO administrator can add custom fields for both SSL and Client certificate types. The new fields will be displayed in the self-enrollment and built-in application forms of the chosen certificate type.

To add a new custom field

- Click 'Add' located at the top of the interface. The 'Add Custom' Field dialog will appear.



dd Custom Field - Table of Parameters		
Field Name	**Values**	**Description**
Name	String (required)	The name of the field to be added. (Max 256 characters). This will be the label of the field that is seen on the enrollment form.
Certificate Type	Drop-down (required)	Enables the administrator select the certificate type to which the new field is to be applied
Mandatory	Check-box	Enables the administrator to specify whether the field is mandatory or optional.
Active	Check-box	Enables the administrator to specify whether the field is to be active or inactive.

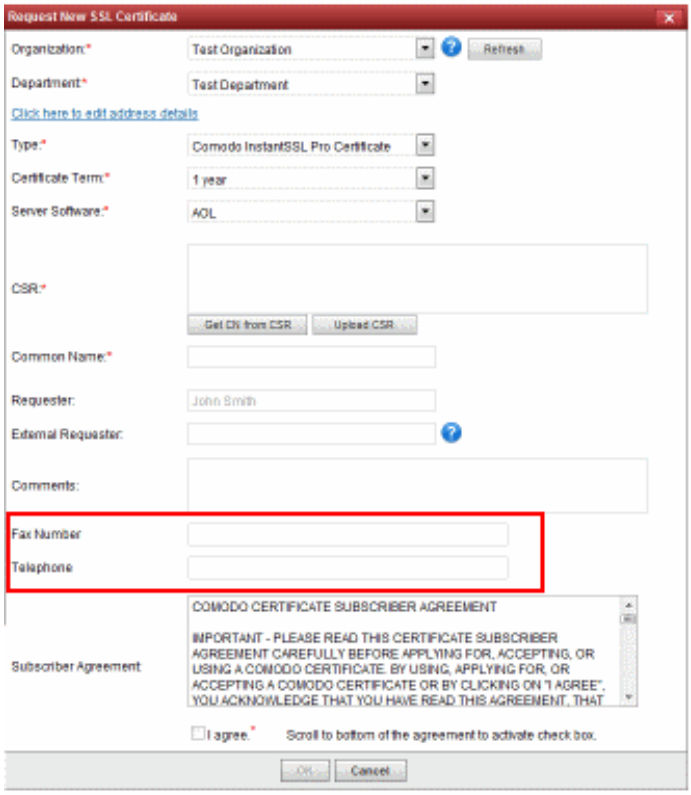
- After completing the 'Add Custom Field' dialog, click 'OK'. If you selected 'Active', the new field will be added to the application forms for the certificate type selected.

The total number of custom fields that you can add is specified by your Comodo account manager. If you reach the maximum permitted, the 'Add' button will not be displayed in the interface. Please contact your Comodo Account Manager, if you wish to have more fields added to your account.

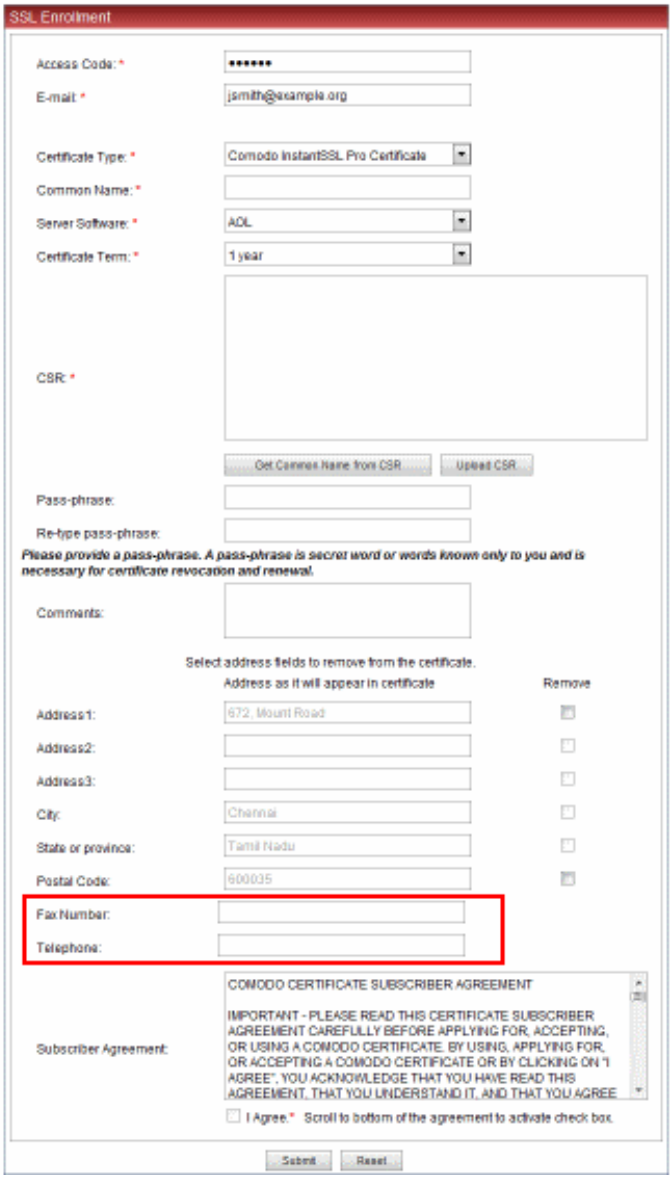
Once a custom field is added, the field appears in both the self-enrollment form and the built-in application form for the selected certificate type.

As an example, the 'Built-in' and 'Self-enrollment' application forms for an SSL certificate are shown below. Both examples show two custom fields - 'Fax Number' and 'Telephone'.

Built-in Enrollment Form



Self-Enrollment Form

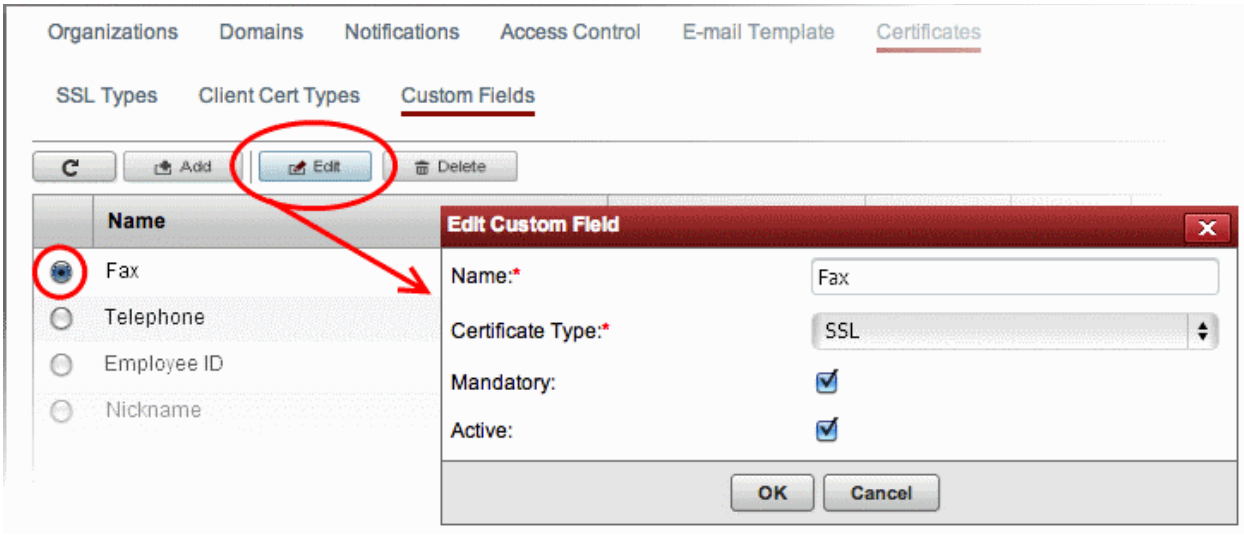


Note: The added custom fields will be available in the Built-in and Self Enrollment forms for both SSL and Client certificate types and will not be available for enrollment of certificates through Web API.

5.8.4.2 Editing an Existing Custom Field

- Select the field and click the 'Edit' button located at the top of the interface

The 'Edit Custom' Field dialog will appear.



The Edit Custom Field dialog will appear. The dialog is similar to **Add Custom Field** dialog.

5.8.4.3 Removing an Existing Custom Field

If an existing custom field turns to be unnecessary, the administrator can remove the field in two ways:

- **Disabling the field**
- **Deleting the field**

In general, Comodo recommends disabling rather than deleting a custom field. That way, all associated data will be retained and you can always re-insert the field at a later date 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. However, this is easily overcome by contacting your Comodo account manager and requesting more fields are added to your account.

Disabling the field

MRAO Administrators can deselect the 'Active' box to disable a field. If a field is made inactive, it will not be displayed in future application forms but the existing data relevant to the field will be retained in the database. The administrator cannot add a new custom field to replace the inactive field if the maximum number of fields has been reached. Disabling a field allows administrators to re-insert the field at a later date.

To disable a field

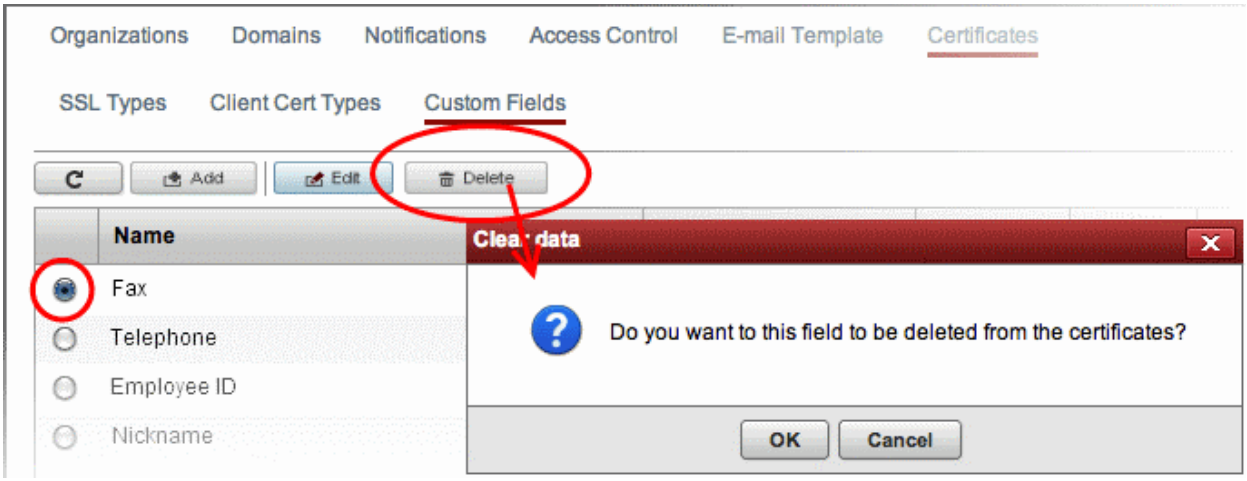
- Open the **Edit Custom Field** dialog
- Deselect the 'Active' check box and click OK.

Deleting the field

MRAO Administrators can delete a field if it is not going to be used in future. All previously stored data associated to the deleted field will be removed from the database. If a field is deleted, administrators can replace it with a new custom field.

To delete a field

- Click 'Settings' > 'Certificates' > 'Custom Fields' to open the Custom Fields interface.
- Select the field and click the 'Delete' button located at the top of the interface



- Click 'OK' to confirm.

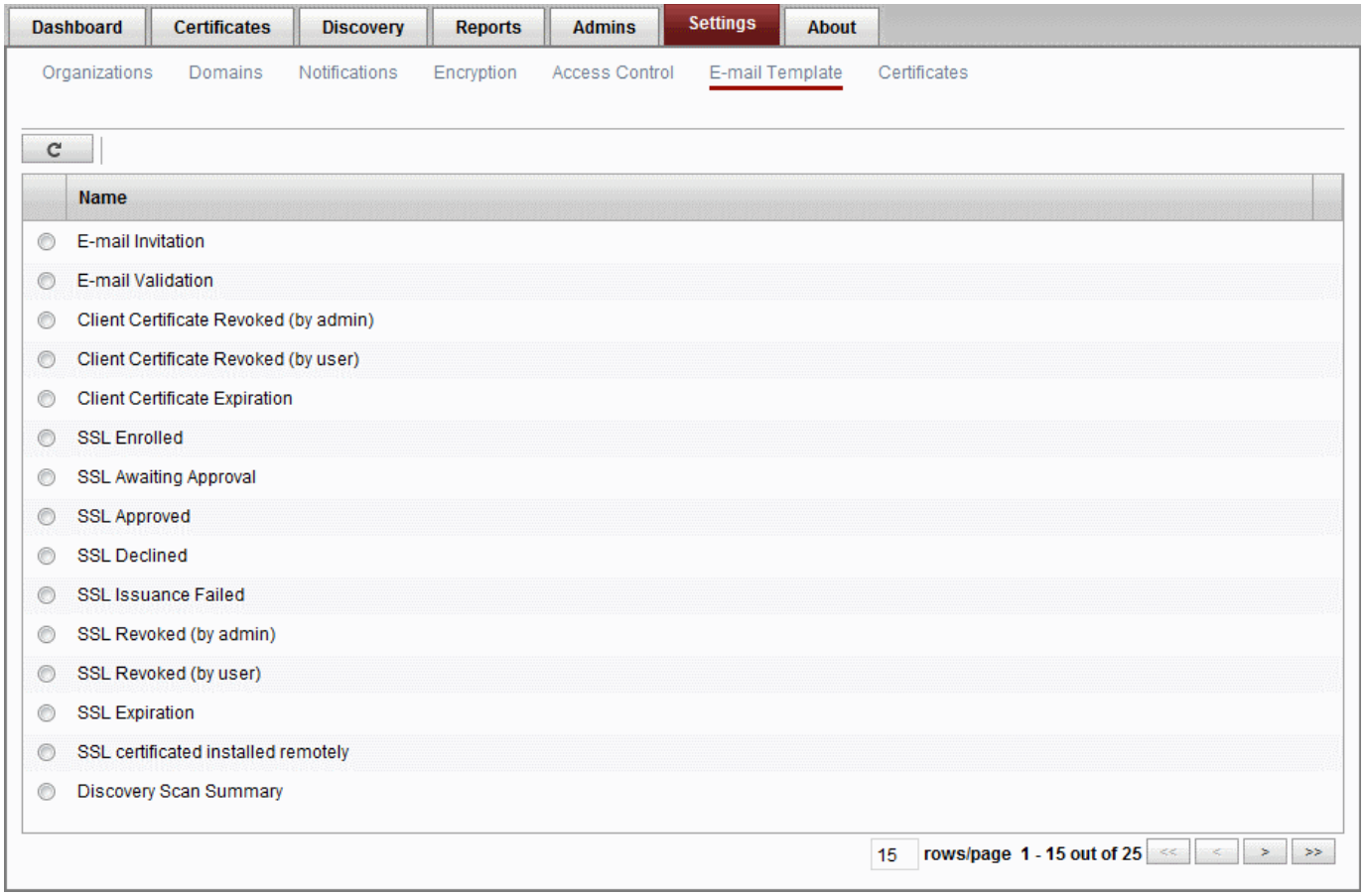
The field will be removed.

5.9 Email Templates

CCM can be configured to send automated email notifications to applicants, administrators and end-users of all types of certificates upon events such as the certificate status updates, approvals, certificate collection, revocation etc. These are set by the respective administrators in the **Notifications** area. The Email Templates area of CCM allows the currently logged in MRAO Administrators to customize the content of these email templates.

Security Roles:

- MRAO - Can view and edit any email notification templates for any certificate type for any Organization or Department.
- RAO Administrators - Cannot view the Email Templates area. They can, instead, edit email templates for their Organization by clicking the 'Edit' button in the Organizations area (Settings > Organizations > Edit)
- DRAO Administrators - Cannot view the Email Templates area. They can, instead, edit email templates for their Department by clicking the 'Edit' button in the Departments area (Settings > Departments > Edit)



The name column lists the types of automated email notifications sent on different stages.

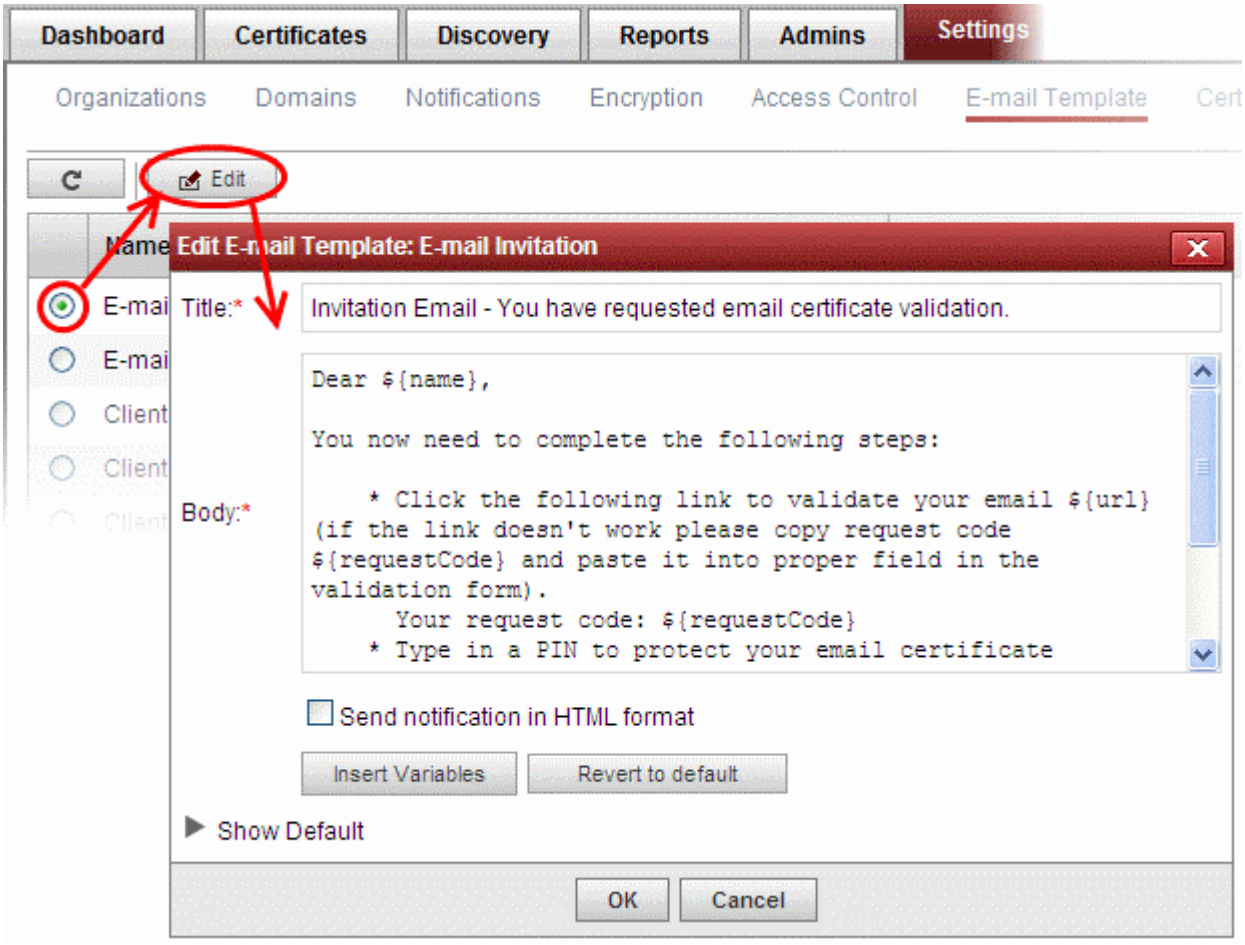
5.9.1 Viewing and Editing the Email Templates

The administrator can view and edit the email template messages from the 'Edit Email Template' dialog.

To view and edit email template message

- Select the email template
- Click the 'Edit' button from the top

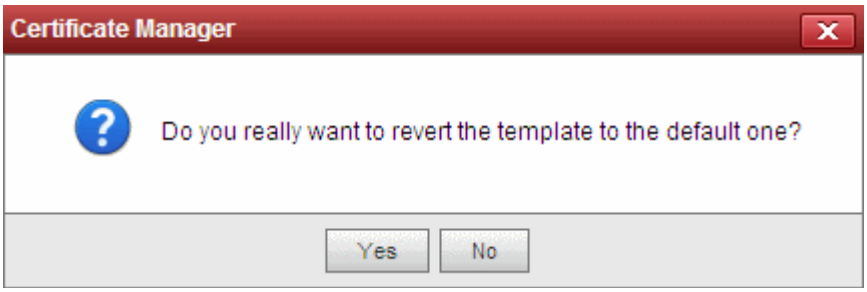
The 'Edit Email Template' dialog will open. An example is shown below.



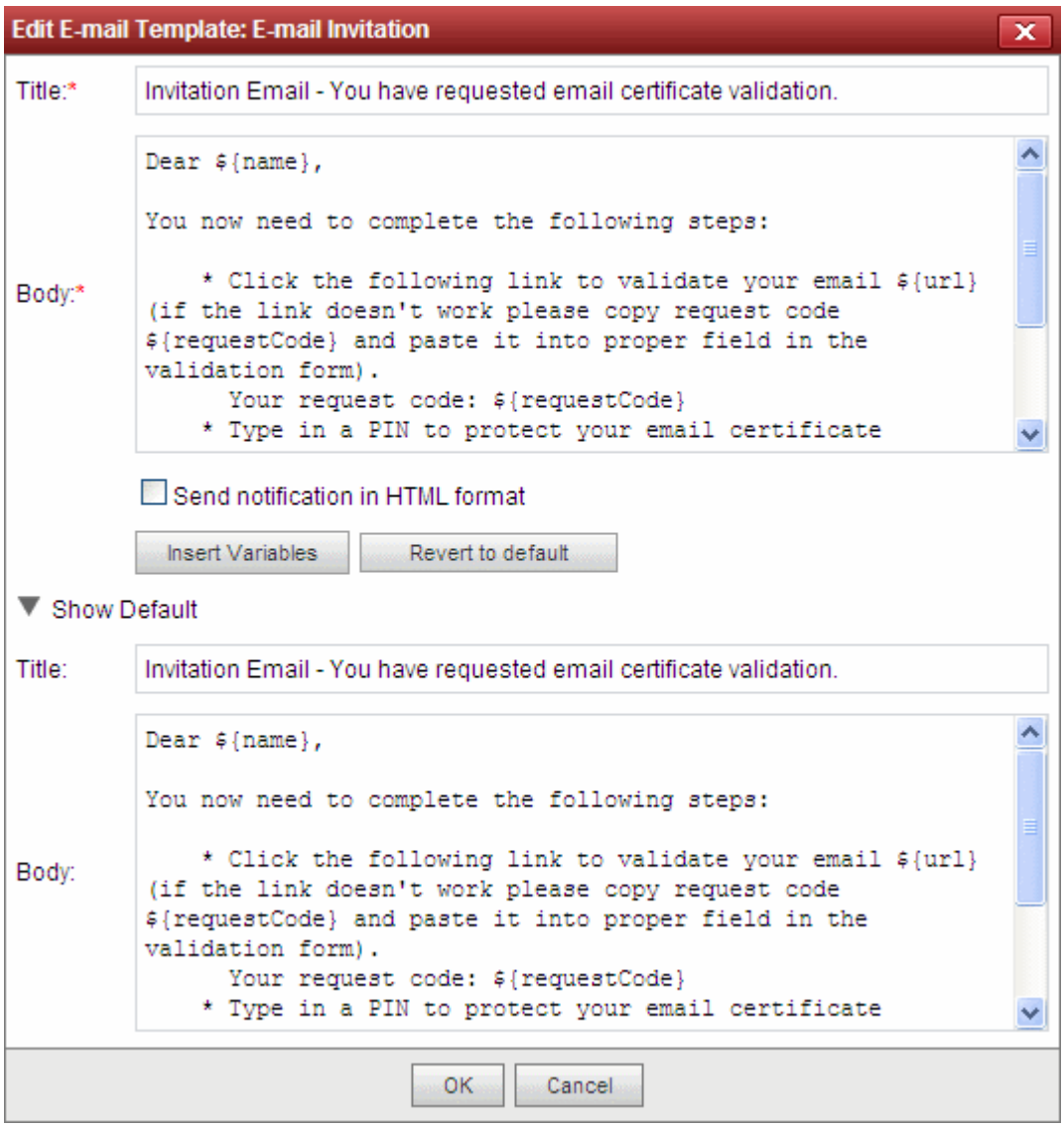
The Title field displays the subject line of the email to be sent. The 'Body' field contains the body content of the email message. The body content contains the text portions and the variables which will be replaced with the exact values from the details of the corresponding certificate/domain while sending the email automatically. The dialog allows the administrator to directly customize the content and add or remove the variables according to the need.

- Selecting the checkbox 'Send notification in HTML format' will send automated email notifications to administrators, applicants and end-users in HTML format.
- Clicking 'Insert Variables' will display a list of the variables used in the specific template. The administrator can select the variable to be inserted into the content from the list. This is useful if the administrator has accidentally deleted variable(s) which are essentially required in the template.

- Clicking 'Revert to default' enables the administrator to reset to the default content as shipped with CCM.



- Clicking 'Show Default' will display the default content for administrator to refer.



6 Certificate Discovery and Agents

CCM allows administrators to scan for SSL certificates installed in a network including certificates issued by third party vendors and self-signed certificates. Agents installed in the network facilitate this discovery process. In addition, the agents are also used for automatic installation of SSL certificates on Apache, Apache Tomcat and IIS 7, 7.5, and 8. Refer to the following sections for more detailed explanation on each area.

- **Certificate Discovery**
- **Agents**

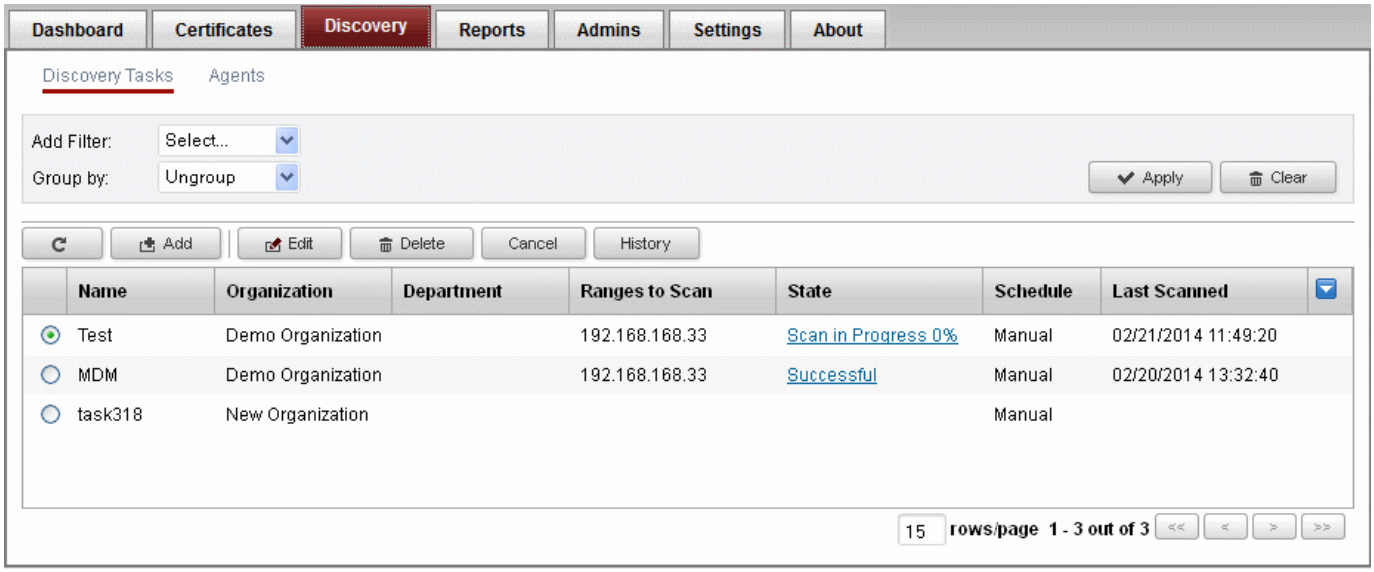
6.1 Certificate Discovery Area

6.1.1 Discovery Tasks

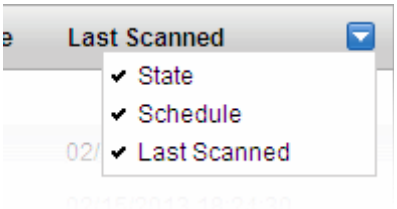
The Certificate Discovery option is a very convenient tool for scanning and monitoring a network for all installed SSL certificates (including Comodo Certificates that may or may not have been issued using Comodo Certificate Manager, any 3rd party vendor certificates and any self-signed certificates.)

Security Roles:

- MRAO - can scan for certificates requested, issued, expired, revoked and replaced for any Organization or Department.
- RAO - can scan for certificates requested, issued, expired, revoked and replaced for Organizations (and any sub-ordinate Departments) that have been delegated to them.
- DRAO - can scan for certificates requested, issued, expired, revoked and replaced only for the Department that have been delegated to them.



Discovery Tasks area - Table of Parameters		
Field Element	**Values**	**Description**
Name	String	Name of the certificate discovery task
Organization	String	Name of the organization selected for the discovery task
Department	String	Name of the department selected for the discovery task
Ranges to Scan	String	Displays the IP ranges that will be scanned during this task
State	String	Displays the status of the scan, that is, whether it is successful, failed, in progress or canceled. Clicking on the state displays respective result. For example, clicking on 'Successful' will display the number of certificates discovered.
Schedule	String	Displays whether the scan is to be run manually or scheduled
Last Scanned	String	Displays the date and time of the last scan performed
Note: The administrator can enable or disable the columns from the drop-down button beside the last item in the table header:		

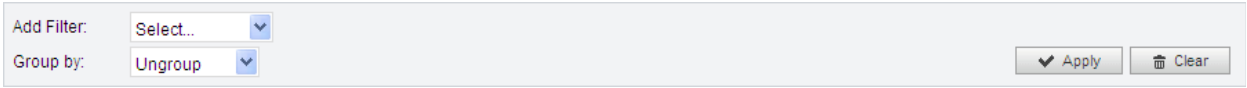


Control Buttons		
	Add	Enables administrator to add a new certificate discovery task
	Refresh	Updates the list of displayed discovery tasks
Discovery Task control Buttons **Note**: The Discovery Task control buttons are visible only on selecting a domain	Edit	Enables administrator to edit the selected discovery task such as change the IP range and more
	Delete	Enables administrator to delete a discovery task from the list
	Scan	Enables administrator to start a new scan for the selected discovery task
	Cancel	Enables administrator to cancel a discovery scan. This button will appear after starting a new scan
	History	Displays the details of past scans performed for the selected discovery task and allows administrators 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 tab

6.1.1.1 Sorting and Filtering Options

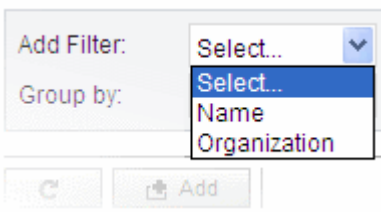
- Clicking on a column headers 'Name', 'Organization', 'Department', 'Schedule' or 'Last Scanned' sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for particular SSL certificates by adding filters.

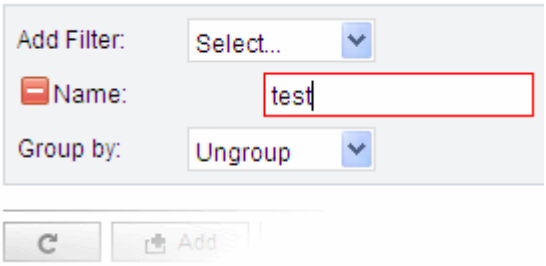


To add a filter

- Select a filter criteria from the 'Add Filter' drop-down



- Enter or select the filter parameter as per the selected criteria.



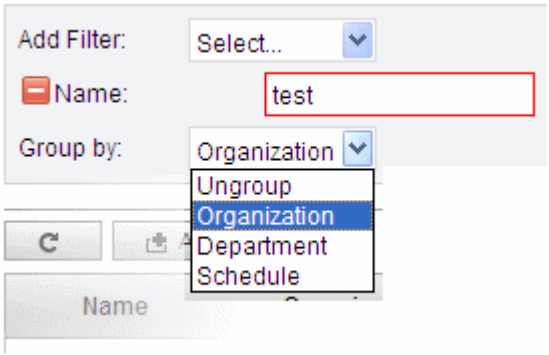
The available filter criteria and their filter parameters are given in the following table:

Filter Criteria	Filter Parameter
Name	Enter the name of the discovery task fully or in part
Organization	Select the Organization and/or the department to which the certificate belongs, from the 'Organization' and 'Department' drop-downs.

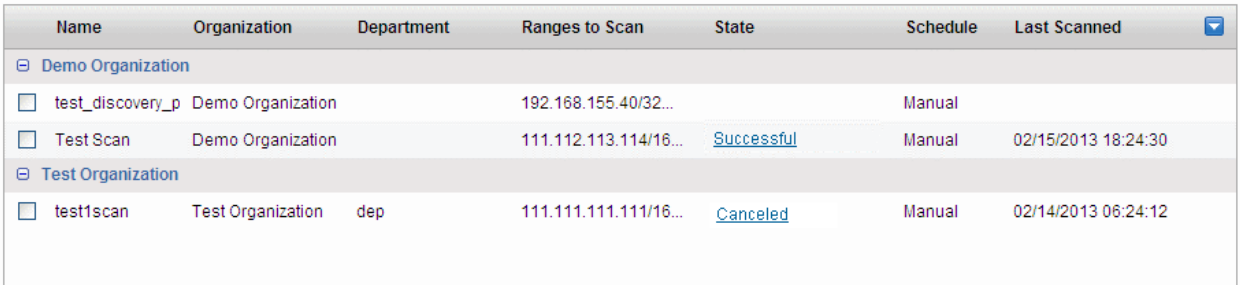
Tip: You can use more than one filter at a time. To remove a filter criteria, click the '-' button to the left if it.

- Select the criteria by which the results are to be grouped from the 'Group by' drop-down and enter or select the grouping parameter

For example, if you want to filter the discovery tasks with a specific Common Name starting with 'test' and group the results by 'Organizations/Departments', then select 'Name' from the 'Add Filter' drop-down, enter 'test' and select 'Organization/Department' from the 'Group by' drop-down. The tasks, having 'test' in their name will be displayed as a list.



The filtered items based on the entered parameters will be displayed:



- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Discovery Tasks' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want

the filters to be saved, click the 'Clear' button.

6.1.1.2 Prerequisites

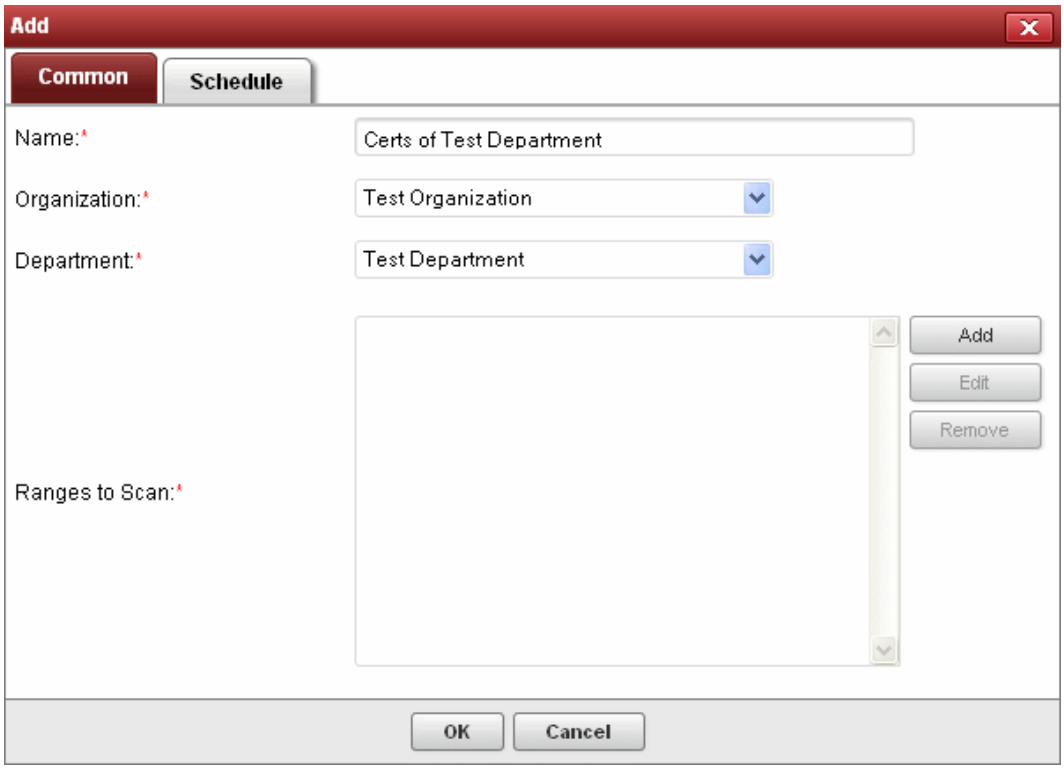
The administrator has installed the certificate controller agent and has configured it.

6.1.1.3 Overview of Process

1. Run a scan of networks in order to find all deployed SSL certificates.
2. CCM will automatically integrate all newly discovered certificates into the 'SSL Certificates' area (Certificates Management > SSL Certificates).
3. CCM will update the status of existing certificates that were issued using CCM (if necessary)
4. 'Unmanaged' certificates can become 'Managed' by renewing the particular certificate
5. The compiled results of the scan can be viewed in the '**Discovery Scan Log**'

6.1.1.4 Adding IP Range and Start Scanning

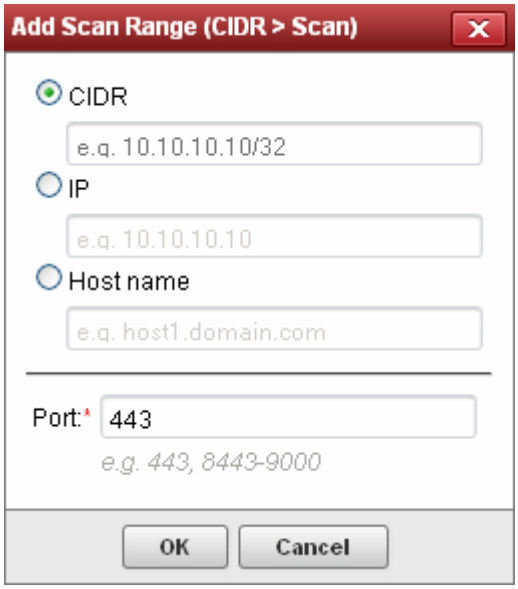
1. To begin a discovery scan, click 'Discovery' > Discovery' Tasks'> 'Add' to open the scan configuration form



Form Element	Element Type	Description
Name	Text Field	Type the name of the discovery task
Organization	Drop-down	Select an organization to which discovered certificates will be assigned
Department	Drop-down	Choose a specific department of the selected organization to be assigned discovered certificates
Add	Control Button	Opens 'Add Scan Range' dialog for specifying the scan ranges
Edit	Control Button	Enables the administrator to edit the selected scan range

Remove	Control Button	Enables the administrator to delete the selected scan range
OK	Control Button	Enables the administrators to add the discovery task to the list
Cancel	Control Button	Cancel the process of creating the discovery task
Schedule	Tab	Allows the administrator to schedule the scan

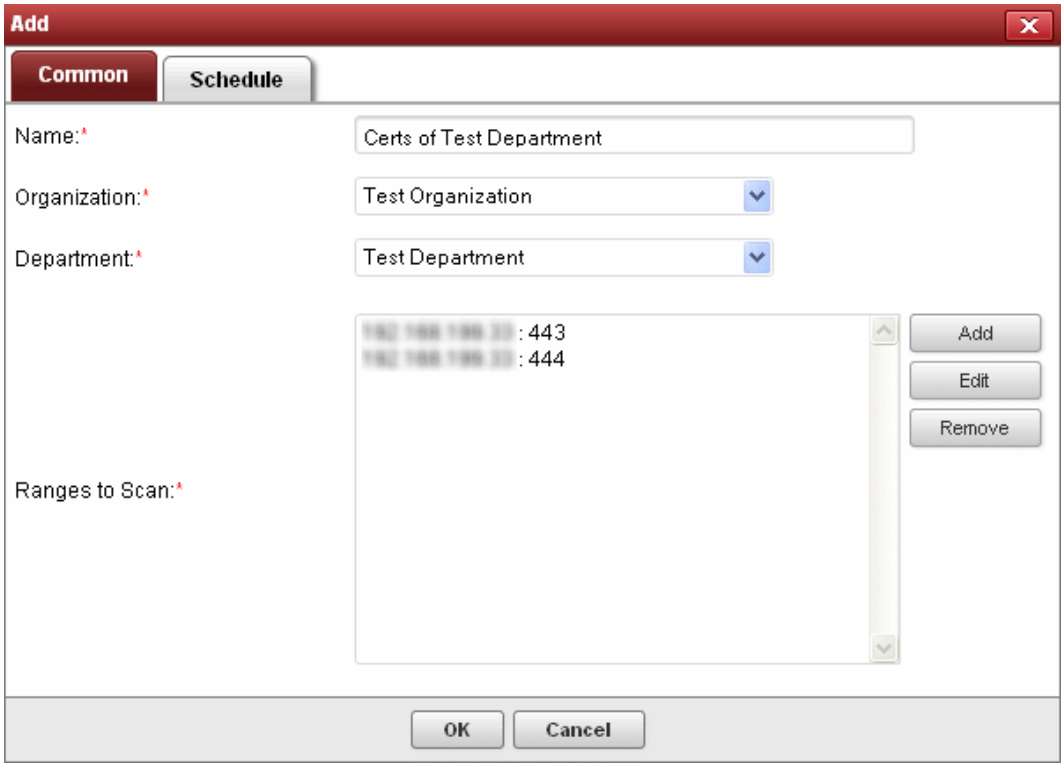
2. Click the 'Add' button to add the CIDR, IP or the host name in the Add Scan Range dialog.



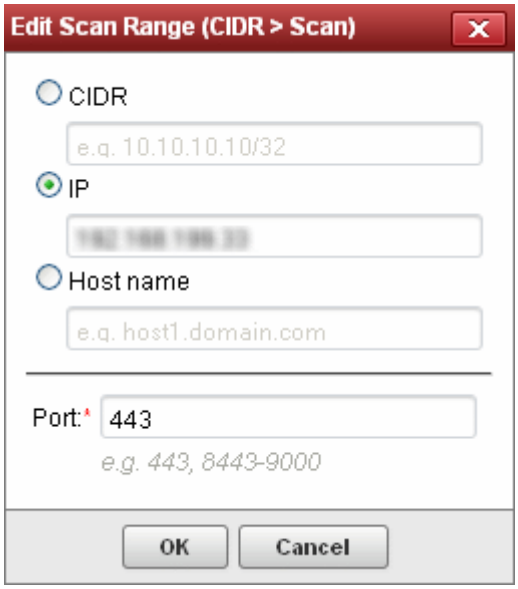
Form Element	Element Type	Description
CIDR	Text Field	Short for 'Classless Internet DOMAIN Routing'. Type the IP address you wish to scan followed by network prefix, e.g. 123.456.78.91/16 should be specified here.
IP	Text Field	Type the IP address you wish to scan
Host name	Text Field	Enter the host name you wish to scan
Ports to Scan ***(required)***	Text Field	The port number(s) for IP range.
OK	Control	Enables the administrator to add specified data into the scan list.
Cancel	Control	Enables the administrator to add cancel the process

3. Click OK after selecting and entering the appropriate details.

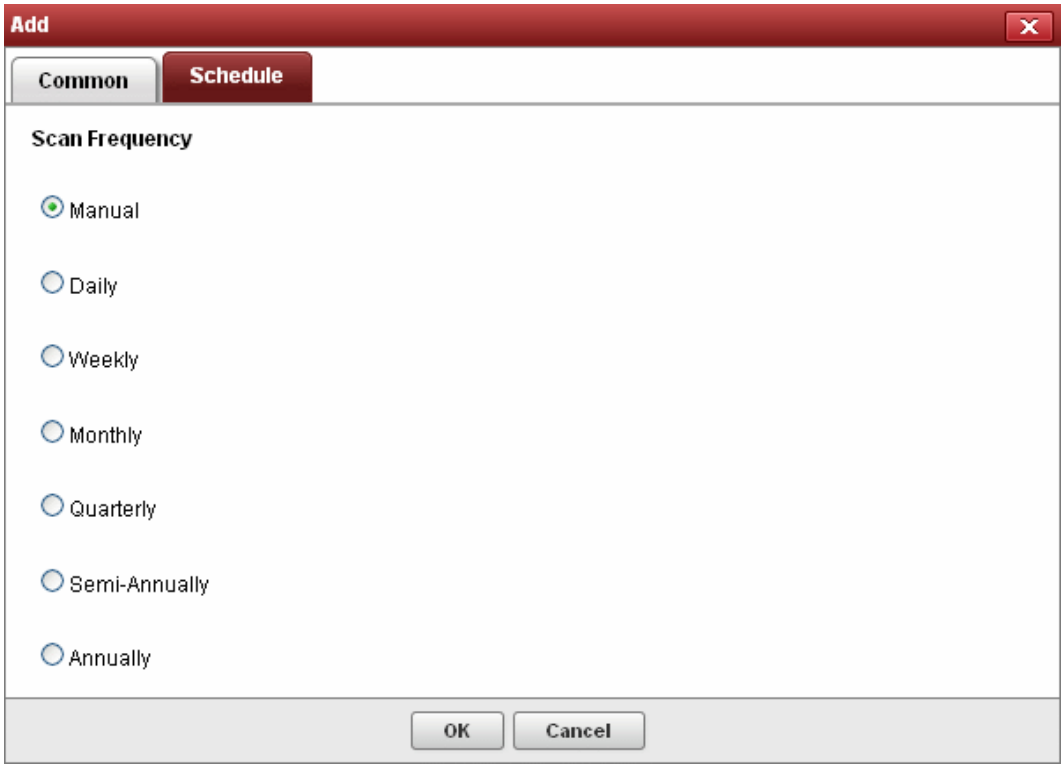
The administrator can add more scan ranges for the same discovery task. Repeat the process as explained above.



The entered scan ranges will be displayed. The administrator can edit or remove the scan range after selecting it.



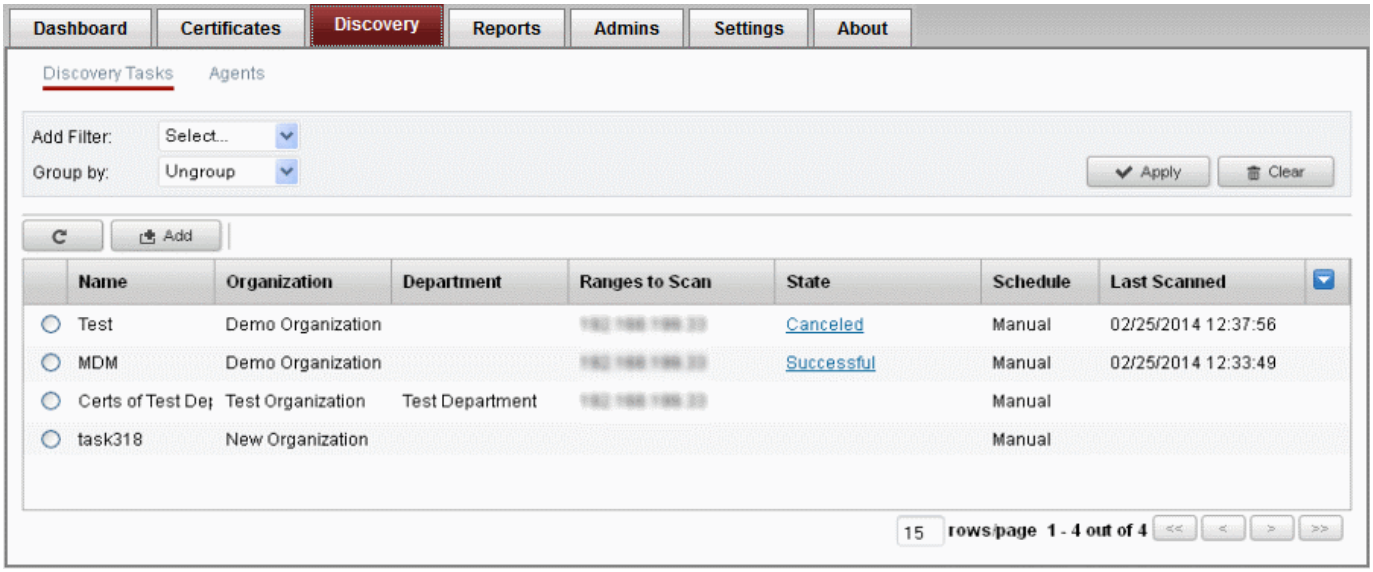
4. Click the 'Schedule' tab to set the scan frequency for the discovery task.



Scan frequency that could be set for the discovery task are: Manual (on demand), Daily, Weekly, Monthly, Quarterly, Semi-Annually and Annually.

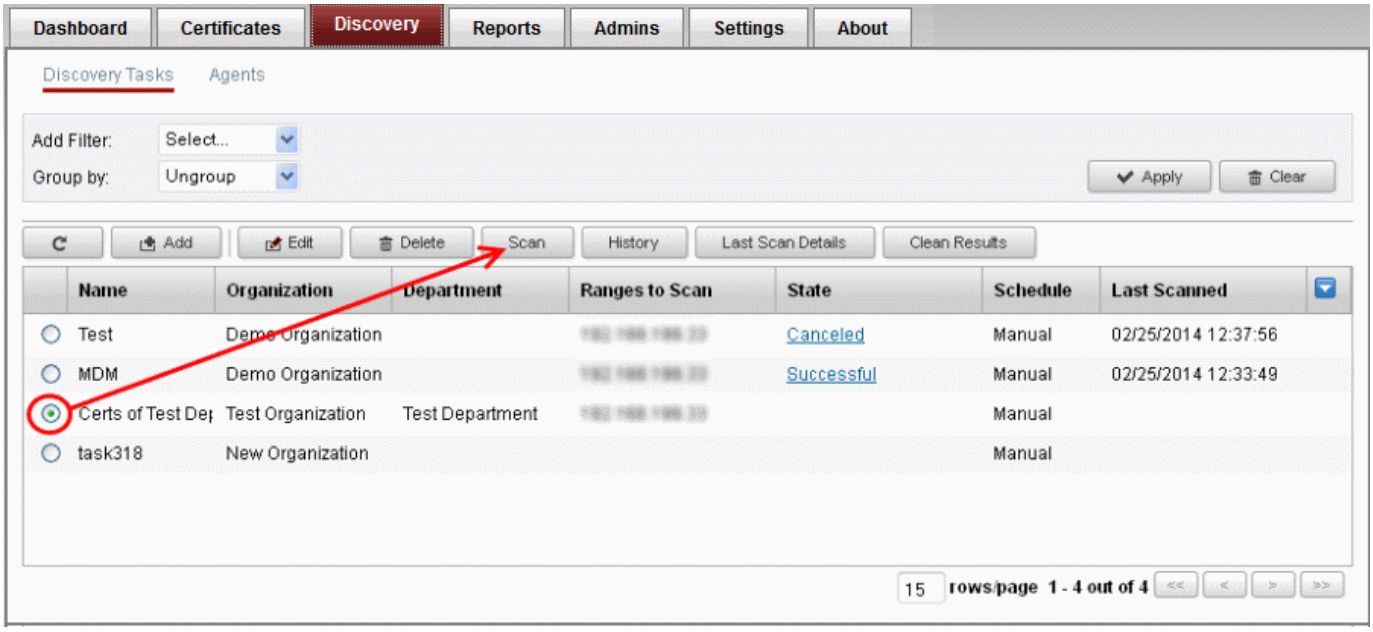
5. Click 'OK'.

The newly created discovery task will be displayed in the list.

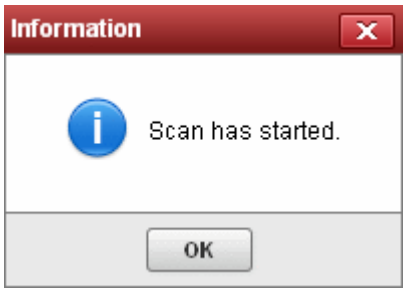


6. Select the discovery task to run the certificate discovery scan.

The control buttons for managing the task will be displayed at the top.



7. Click the 'Scan' button to commence the discovery scan for the selected task.



CCM allows administrators to run multiple discovery tasks at a time. After a scan has started, select another task and click the scan button at the top.

Discovery scanning uses a 2 second timeout for each IP/Port combination with 10 threads running at once. This information can be used to approximate how long a scan will take.

((# IP Addresses) * (# ports per address)) / 300 = Number of minutes for scan.

Note: The timeout interval and number of threads per minute may be subject to minor fluctuation. Admins are advised to treat these figures as a 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.

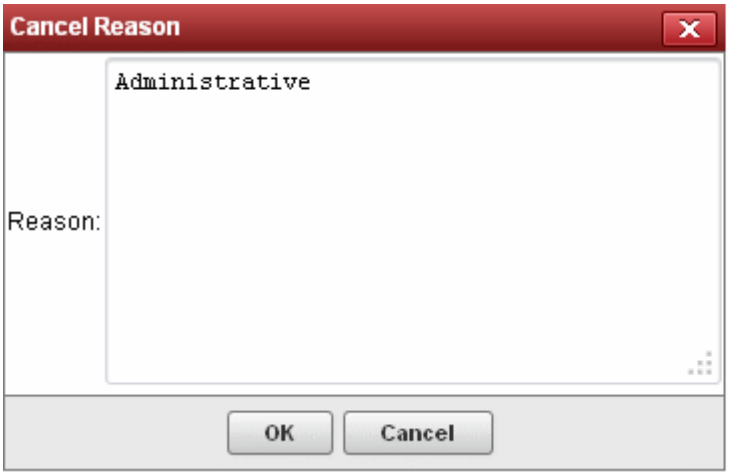
((65536)(1))/300 = approx 218 minutes.

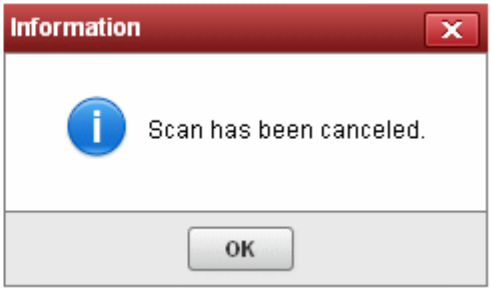
The progress of the scan can be viewed in the row of the selected discovery task under the 'State' column.

8. Click the 'Cancel' button if you want to cancel the scanning process.

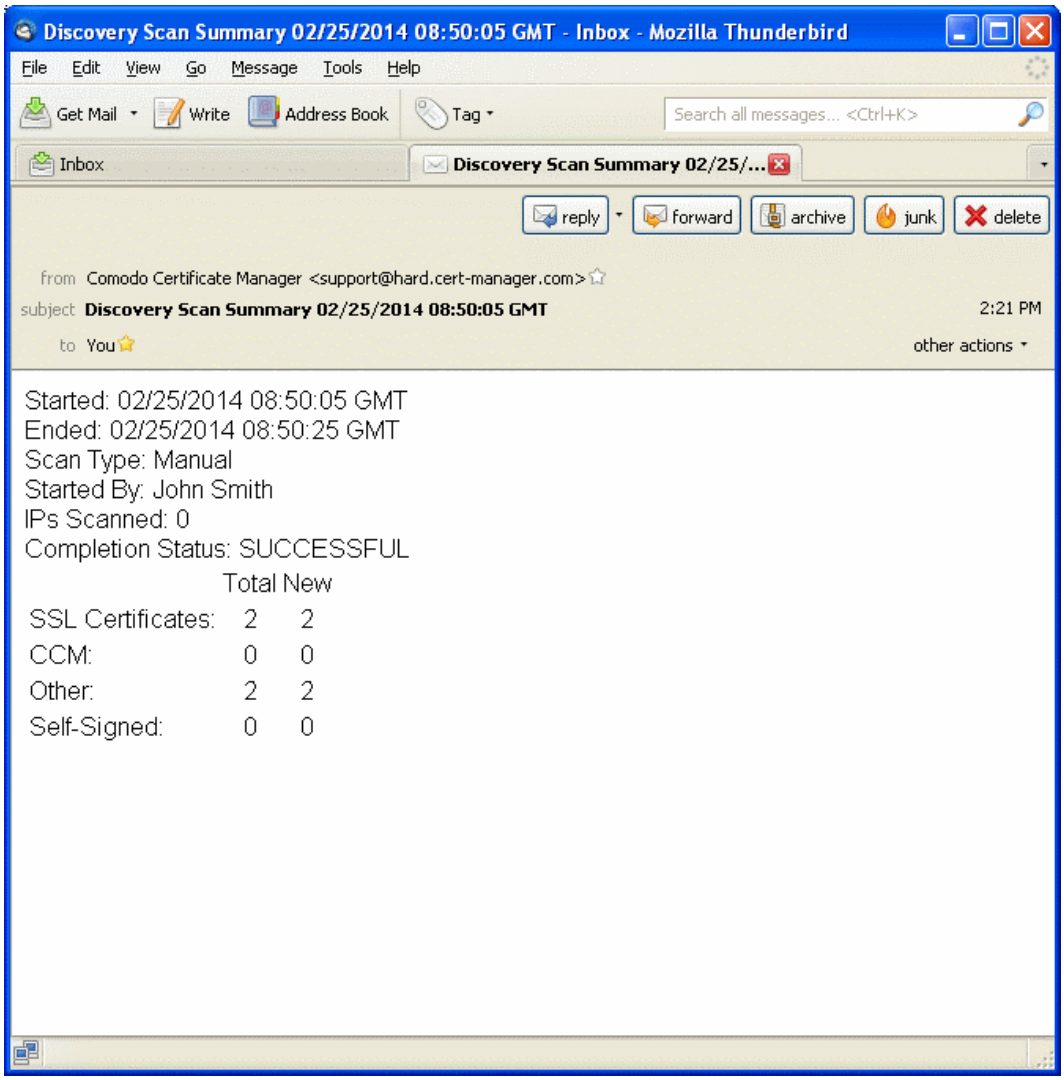
If you cancel the scanning process, the entire system will revert to the state that existed before the scan was started (i.e., any data collected during scanning will not be applied until the scanning process is completed).

If you cancel the scanning, you should specify the reason for in the 'Cancel Reason' dialog and click OK.





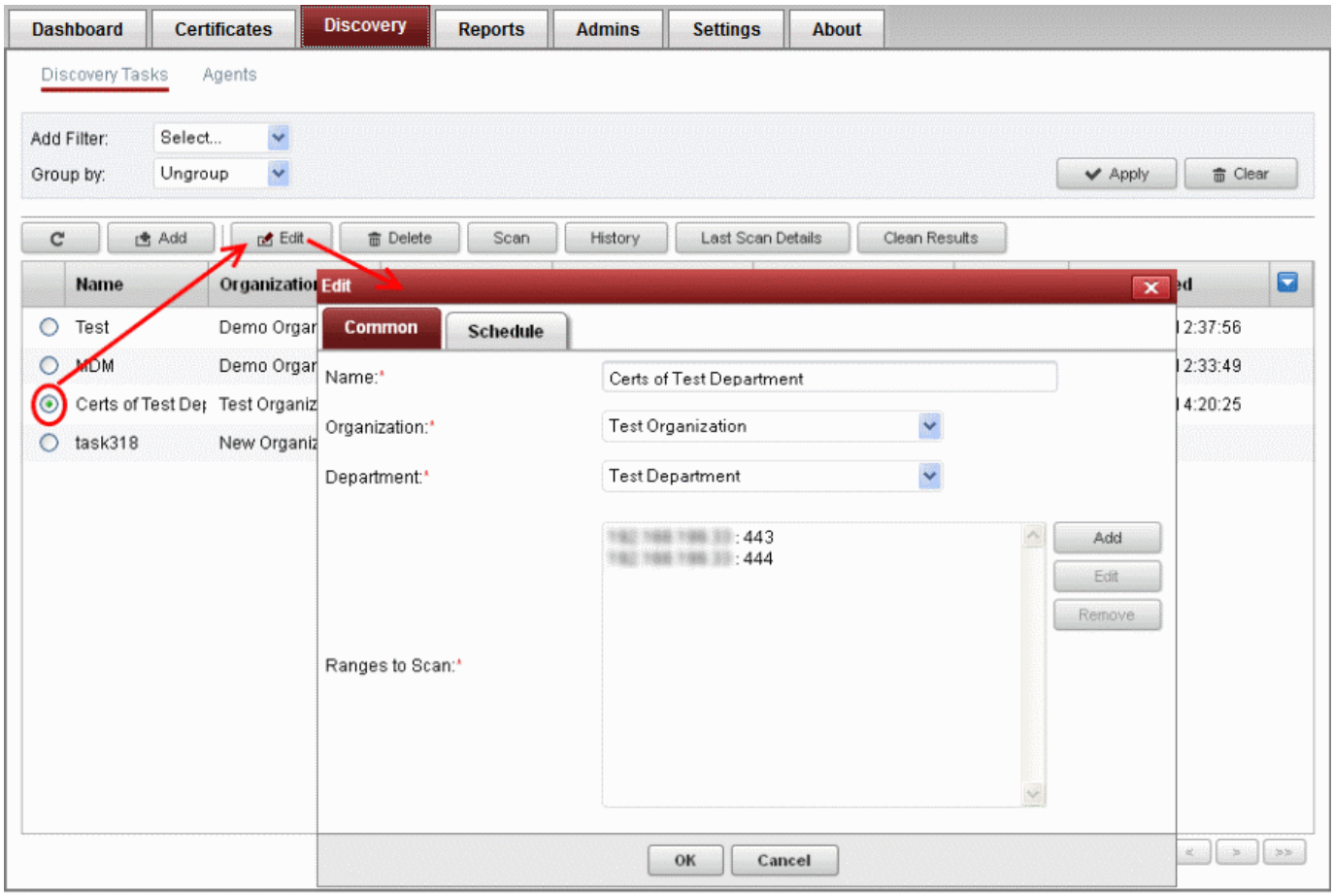
After the scan is complete, administrators will be notified of the result via email. Please note the email notification should have been configured in the **Discovery Scan Summary** notifications area.



The results of the scan can be viewed at '**SSL certificates**' sub-tab of the '**Certificate Management**' section and the '**Reports**' section.

6.1.1.5 Editing a Discovery Task

Administrators can edit an existing discovery task from the list such as change the task name, organization, department and the schedule for the scan. To edit a task, select it and click the edit button at the top.

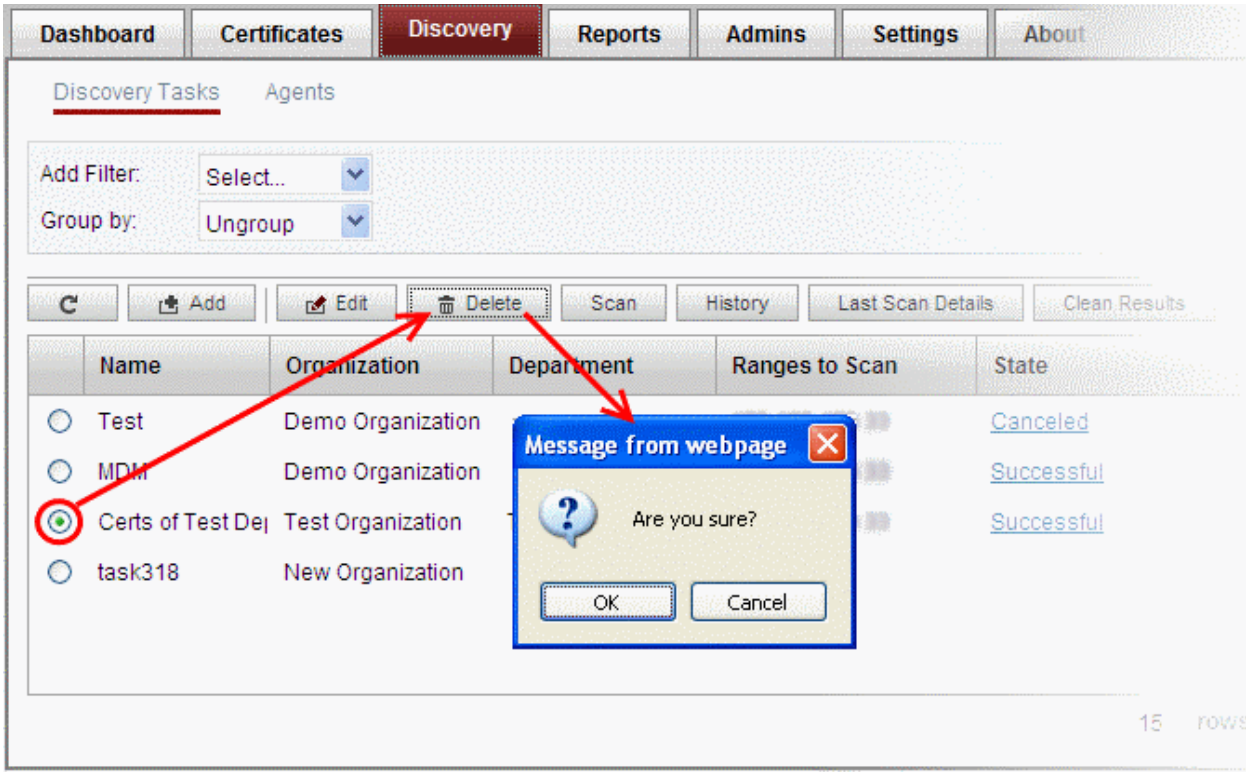


The Edit task interface will open.

The interface allows the administrator to change the task name, select another organization and department, add new scan range, edit existing scan ranges or remove it. In the schedule tab, the scan frequency can be edited. For more details refer to section **Adding IP Range and Start Scanning**.

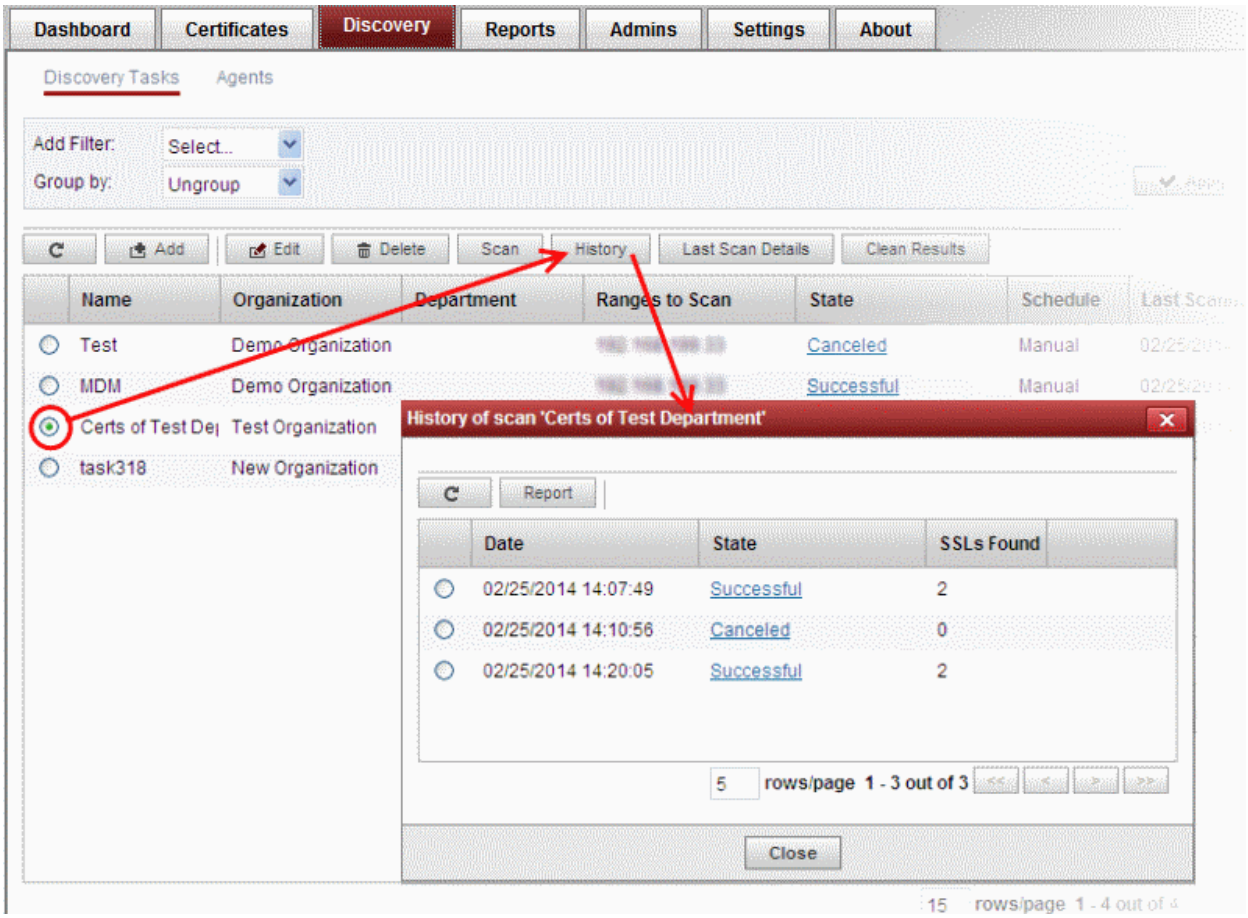
6.1.1.6 Deleting a Discovery Task

To delete a discovery task from the list, select it and click the 'Delete' button at the top.



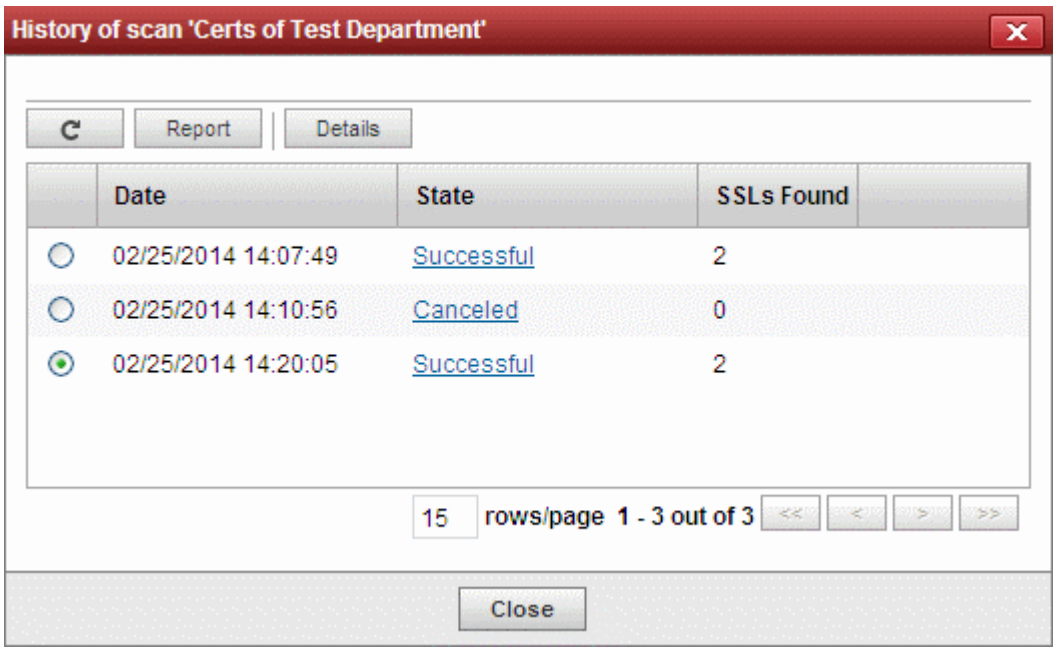
6.1.1.7 Viewing History of Discovery Tasks

CCM allows administrators to view the history of up to last five scan results of each discovery task, view details of each task and download the report from the interface. To view the history of a discovery task, select it and click the 'History' button at the top.



The 'History of scan..." dialog will be displayed.

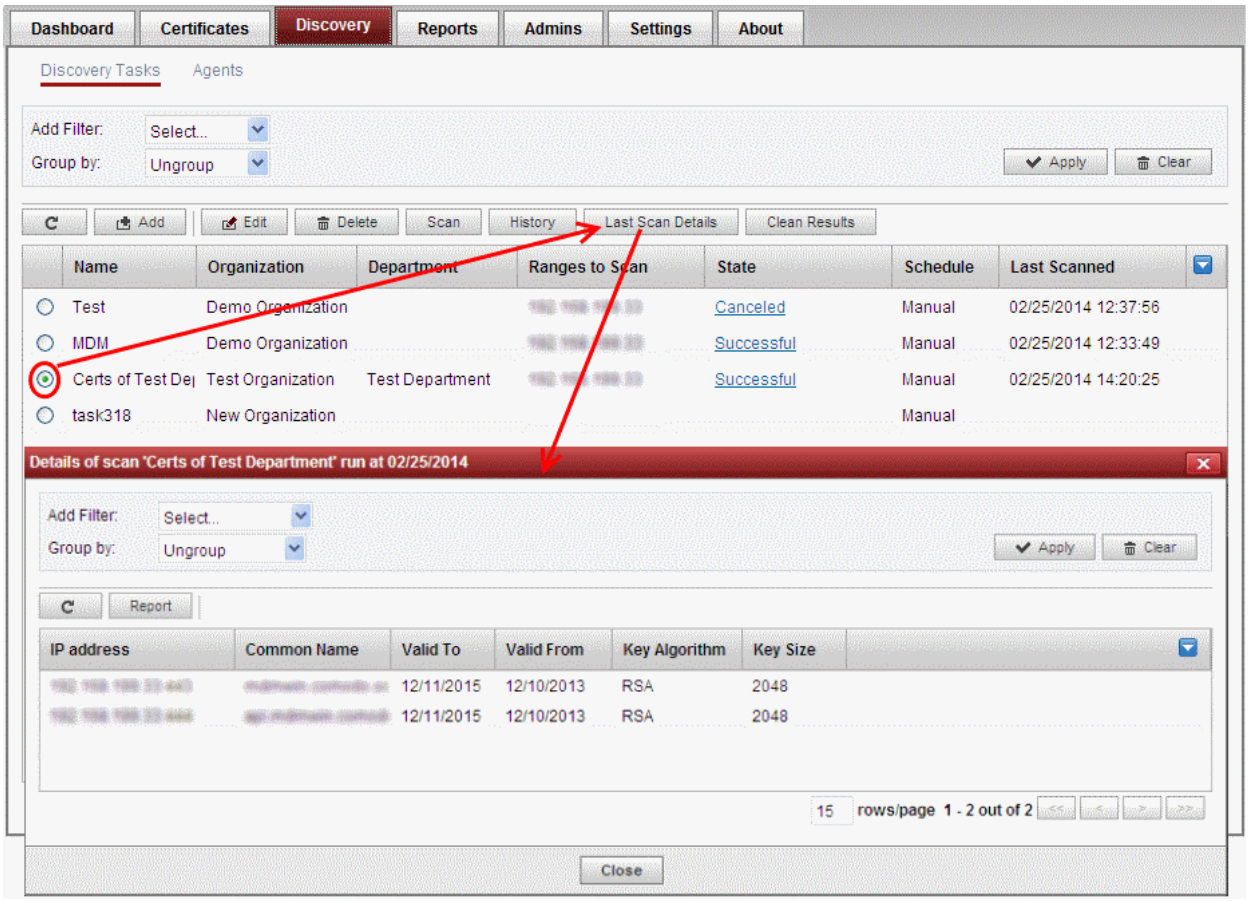
- Click the 'Report' button to download all the discovery scan reports, which is in the form .csv file.
- Select a scan result. The 'Details' button will be displayed at the top.



- Click the 'Details' button to view the details of discovered certificates for the selected scan.

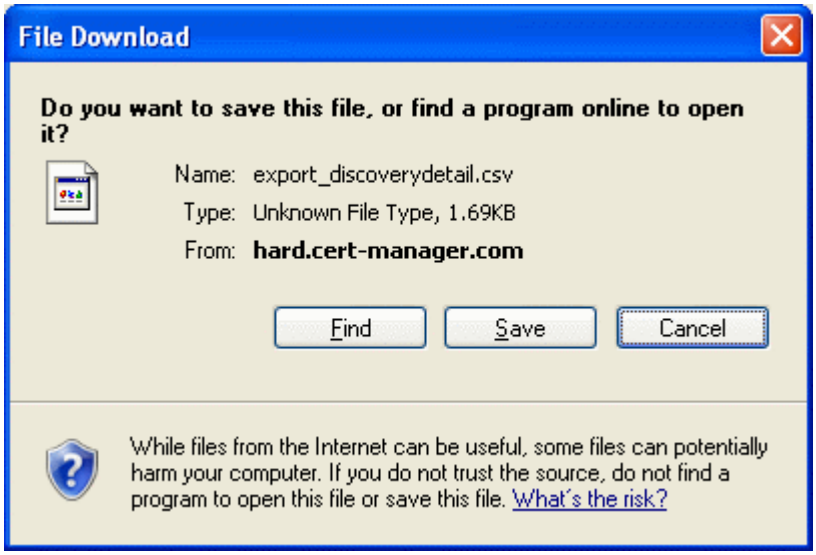
- Click the 'Report' button to download all the reports for the discovered certificates, which is in the form .csv file.

To view the details of latest result of certificates discovered for a discovery task, select it and click the 'Last Scan Details' button at the top.



The details of certificates discovered during the the last scan for the selected task will be displayed.

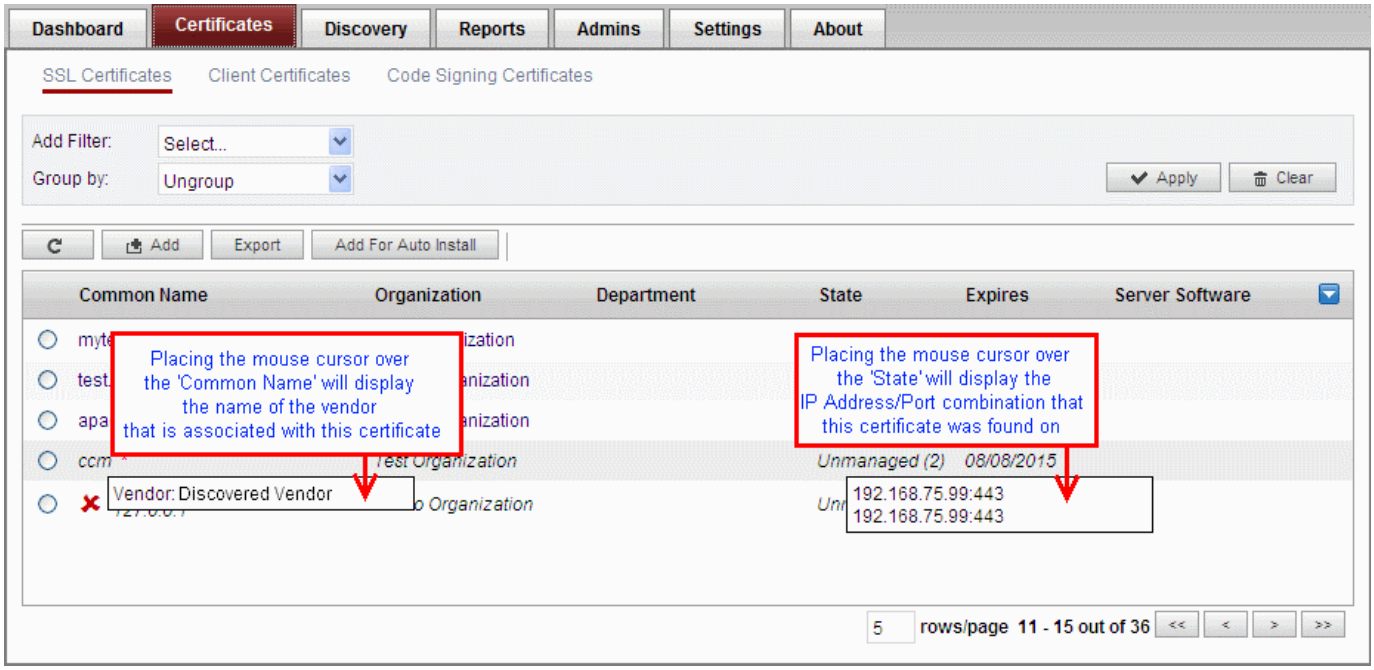
- Click the 'Report' button to download the report, which is in the form .csv file.



6.1.1.8 View Scan Results

Upon completion of the Discovery Scan, Comodo Certificate Manager will automatically update the '**SSL Certificates**' area with the results of the scan. It will add any newly discovered (unmanaged) certificates and update the status of any existing certificates. There are, therefore, two types of SSL certificates that could be discovered.

- **Certificates issued by Comodo Certificate Manager (also known as 'Managed' certificates).** Comodo Certificate Manager will simply update that certificates existing entry with any status changes that may have occurred. These certificates will stay assigned to the Organizations that they are currently assigned to.
- **Certificates that were not issued by Comodo Certificate Manager (also known as 'Unmanaged certificates)** If the certificate was NOT issued by CCM, they will be retained with '*Unmanaged*' status. This category covers:
  - Self-signed certificates
  - Certificates issued by Comodo CA but not via Comodo Certificate Manager
  - Certificates issued by 3rd party vendors / other certificate authorities



To bring an 'Unmanaged' certificate under the control of Comodo Certificate Manager you have to 'Renew' that certificate (to be more precise you will be effectively 'replacing' that certificate with an equivalent Comodo certificate). Clicking the 'Renew' button will begin the ordering process for new Comodo SSL certificate with the same parameters.

Certificate Type		View in the SSL Certificates Sub-Tab	
		State	View
Certificates, issued by CCM		One of the SSL certificates state listed **here**.	testdomain.com Test Organization Test Department 1 Applied example.com Demo Organization Demo Department Declined www.senthil Test Organization Expired 08/16/2012
Certificates, not issued by CCM	*Self-signed certificates*	*Unmanaged*	landfill.addons.allizom.org * Demo Organization Unmanaged (1) 02/15/2021 Self-signed certificates are marked with red cross alongside their common name. (Background - 'Self Signed' means that the certificate was not signed (issued) by a Trusted Certificate Authority. As such, these certificates will not be recognized by popular Internet browsers such as IE, Firefox, Opera. Konqueror, Safari and Chrome.)
	Issued by Comodo CA but not via	*Unmanaged*	test2.ccmqa.com Demo Organization Unmanaged 01/03/2014

Certificate Type		View in the SSL Certificates Sub-Tab	
		State	View
Certificates, issued by CCM		One of the SSL certificates state listed **here**.	testdomain.com Test Organization Test Department 1 Applied example.com Demo Organization Demo Department Declined www.senthil Test Organization Expired 08/16/2012
	CCM		
	Issued by 3rd party vendor	*Unmanaged*	*example.com Test Organization Unmanaged (1) 08/08/2015*

You can download the compiled scan results in .csv format in **Discovery Scan Log** report under the **Reports** tab.

The **Discovery Scan Log** report contains information concerning to overall scan options and discovered SSL certificates information.

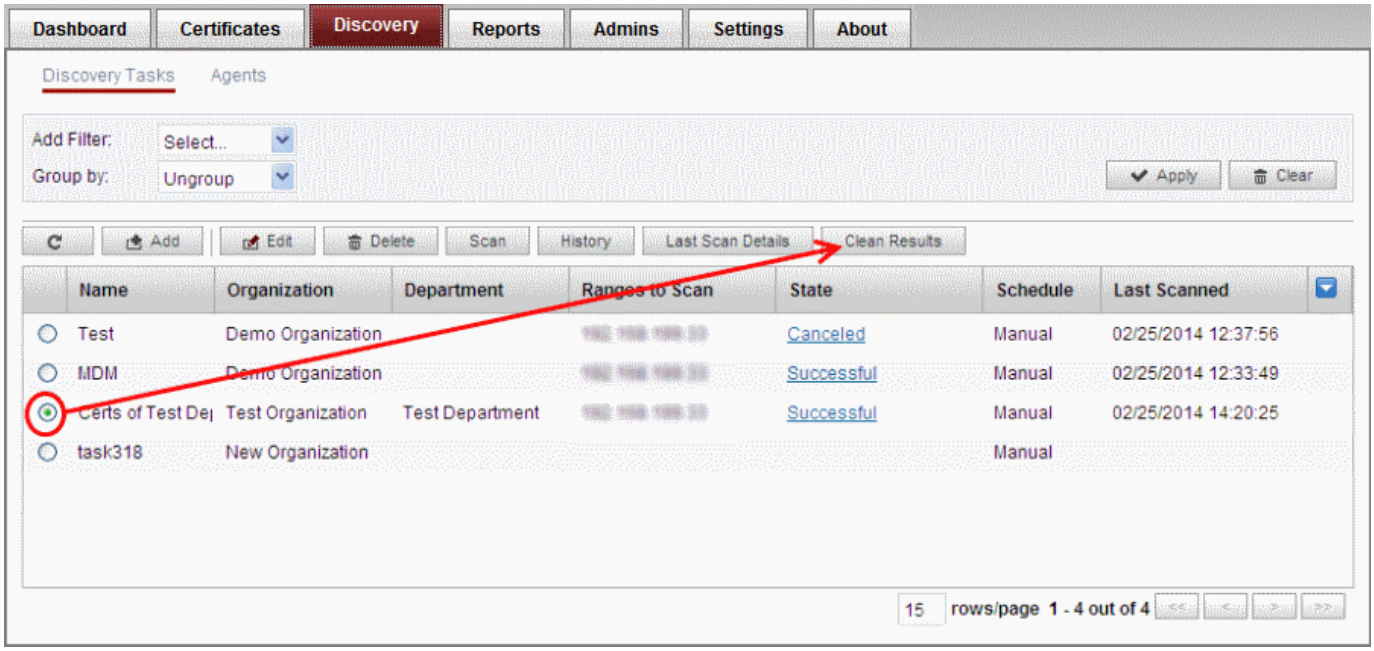
Comodo advises administrator to:

i. Schedule regular discovery scans as a matter of course;

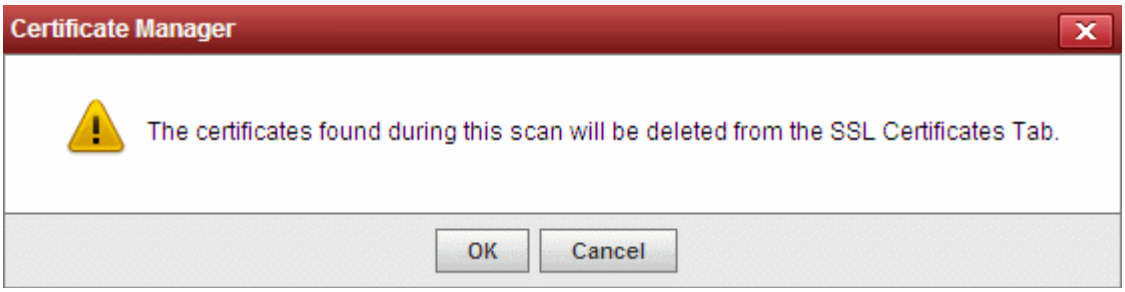
ii. Run a manual scan after every change to SSL certificate configuration. Otherwise, it is possible that the 'SSL Certificates' area will show inaccurate information. (e.g. you may have uploaded a certificate to your website but in CCM the certificate will have a state of 'Issued' and a discovery status of '**Not deployed**' if you haven't re-run the scan).

iii. Run a manual scan after any change to the network in general.

To remove the discovered certificates from the SSL Certificates screen for a particular discovery scan, navigate to Discovery > Discovery Tasks, select the discovery task and click the 'Clean Results' button.



In the confirmation dialog, click 'OK' to confirm removal of the certificates in the SSL Certificates interface.



6.1.2 Agents

Comodo Certificate Manager uses agents for:

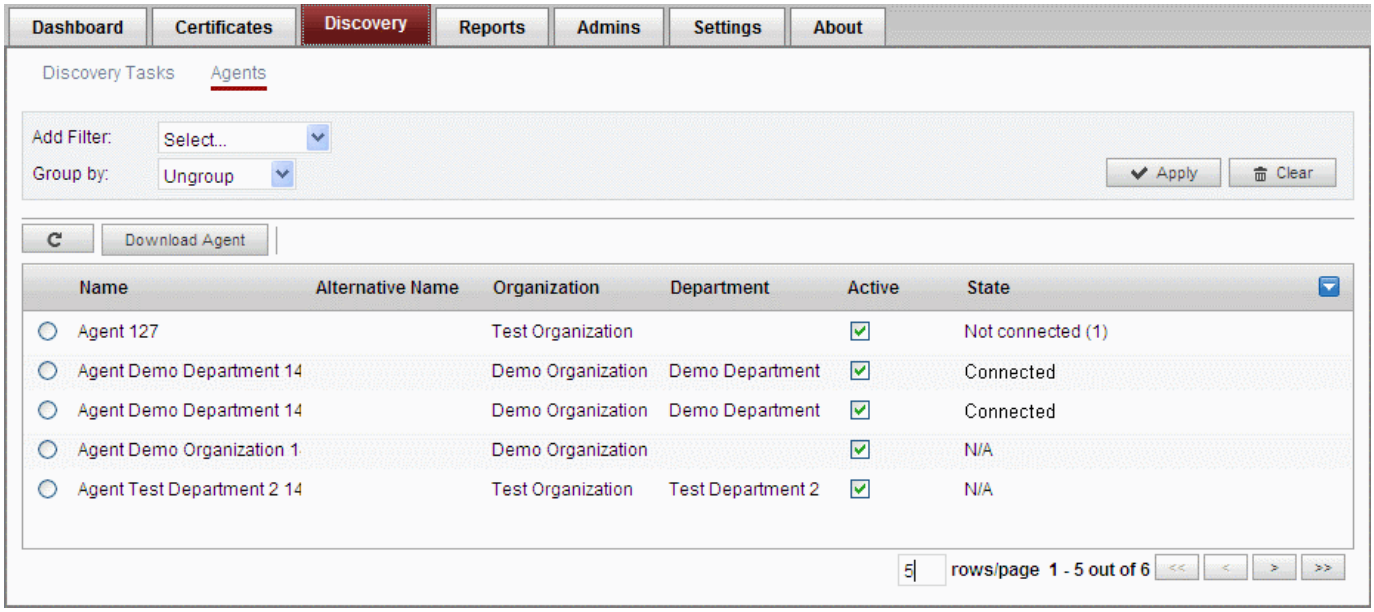
- **Automatic installation of certificates (on Apache, Apache Tomcat and IIS 7. 7.5and 8 only)** - The controller/agent installed on the web server, will periodically poll CCM for requests for certificates that have been enabled for auto-installation. If a request exists, it will automatically generate a CSR on the web server and present the application for administrator approval via the CCM interface. On approval, the agent submits the CSR to Comodo CA and tracks the order number. Once the certificate is issued by the CA, the agent downloads the certificate and allows the administrator to install the certificate from the CCM interface. The controller installed on one server can be configured to communicate with the other remote servers in the network. Once configured, it enables automatic installation of certificates on the remote servers without the need of installing the agent on them.
- **Discovery of SSL certificates installed on internal servers** - The agent installed on the web server or any local machine in the network, will scan and monitor internal servers for all installed SSL certificates. It is possible for administrators to configure Comodo CM to scan externally facing IP addresses directly from the 'Discovery Tasks' area (as explained in **Discovery Tasks**). However, Comodo CM can only scan internal hosts IF an agent which is configured to communicate with the Comodo CM servers is installed on the local network. After scanning the local network, the agent will send a report back to the Comodo CM console.

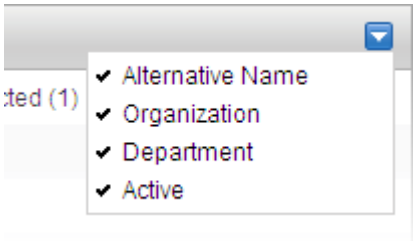
Note: Only if auto-installer feature is enabled for your account, the CCM agent will serve both the purposes of automatic installation of certificates and discovery of SSL certificates installed on your internal servers. If this feature is not enabled, the agent will act as certificate discovery agent and will only scan for SSL certificates installed in your servers.

Security Roles:

- MRAO - can set up Certificate Controller Agent for installing certificates and scanning internal servers of any Organization or Department, for certificates requested, issued, expired, revoked and replaced.
- RAO - can set up Certificate Controller agent for installing certificates and scanning internal servers of Organizations (and any sub-ordinate Departments) that have been delegated to them, for certificates requested, issued, expired, revoked and replaced.
- DRAO - can set up Certificate Controller agent for installing certificates and scanning internal servers of Department that have been delegated to them for certificates requested, issued, expired, revoked and replaced.

The Agents Interface:



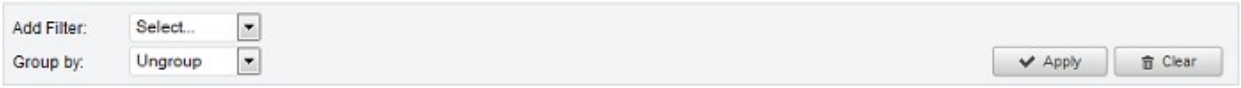
Column Display	Description
Name	Displays the name specified for the Certificate Controller Agent.
Alternative Name	Displays the alternative name specified for the Certificate Controller Agent.
Organization	Displays the Organization to which the Certificate Controller Agent is associated.
Department	Displays the Department to which the Certificate Controller Agent is associated.
Active	The checkbox displays whether the agent is active or inactive and allows the administrator to change the state if required.
State	Displays whether or not the agent is connected to CCM.
Note: The administrator can enable or disable the columns from the drop-down button beside the last item in the table header: 	
Controls	
	Download Agent — Starts downloading the Certificate Controller Agent setup file of the selected agent.
	Refresh — Updates the list of displayed Agents.
Agent Controls	
	Edit — Enables administrators to modify the Agent configuration settings.
	Delete — Removes the Agent.
	Nodes — Enables administrators to view and edit the server nodes for which the Agent is configured.
	Commands — Enables administrators to view the details of the commands like generation of CSR, scanning

		internal servers, executed by the Agent.

6.1.2.1 Sorting and Filtering Options

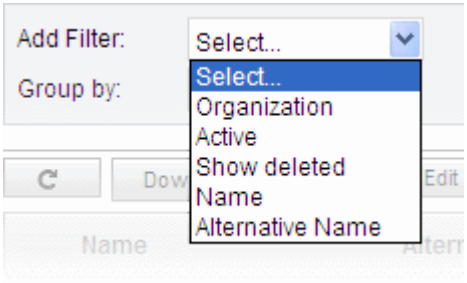
- Clicking on the column headers 'Name', 'Alternative Name', 'Organization', or 'Department' sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for a particular agent by using filters under the sub-tab:



Filter Options	Description
Organization	Enables Administrators to filter the list of Agents by Organization.
Active	Enables Administrators to filter only the active agents.
Show deleted	Enables Administrators to include the deleted agents in the list.
Name	Enables to filter the agents by entering the name fully and partially.
Alternative Name	Enables to filter the agents by entering the alternative name fully and partially.

You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.



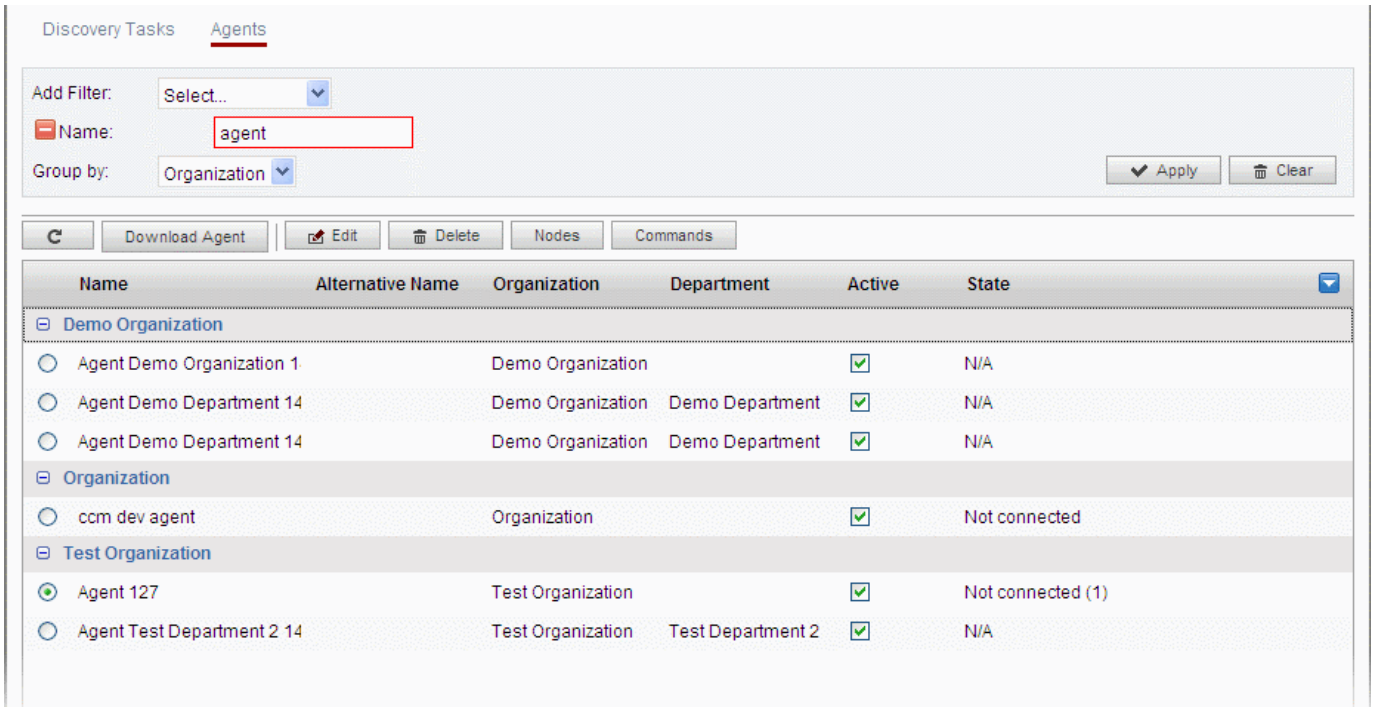
For example if you want to search for an agent by the name filter and belonging to a particular organization and department:

- Select 'Name' in the 'Add Filter' drop-down

Enter the name of the agent partly or fully in the 'Name' field.

- Select 'Organization' or 'Department' in the 'Group by:' drop-down.
- Click the 'Apply' button.

The filtered items based on the entered and selected parameters will be displayed:



- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Agents' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

6.1.2.2 Configuring the Agent for Auto-Installation and Internal Scanning - Overview of the Process

This section is a brief summary of the steps needed to set up a certificate controller/agent for automatic installation and renewal of SSL certificates and run an internal scan. Click any of the bullet points below to go to a more detailed explanation of that stage:

1. **Add a new IP range for Internal Scanning by creating a new CIDR in the Discovery Tasks tab.**
2. **Download and Install the agent on a server**
3. **Configure the Agent for adding CIDR ranges for certificate discovery and specifying local and remote servers on to which the certificates are to be auto-installed.**
4. **Return to the 'Discovery Tasks' tab and click 'Scan'.**
5. **The results can be viewed by selecting the 'Discovery Scan Log' under the 'Reports' tab. Newly discovered certificates will be added to the 'SSL Certificates' area of 'Certificates Management' and assigned to the Organization that has been set for that agent.**

6.1.2.3 Prerequisites

The administrator has defined at least one Organization. The Organization will be designated as the owner of certificates discovered by the agent during the agent configuration and installation process.

6.1.2.4 Configuring the Agent for Auto-Installation and Internal Scanning - Detailed Explanation of the Process

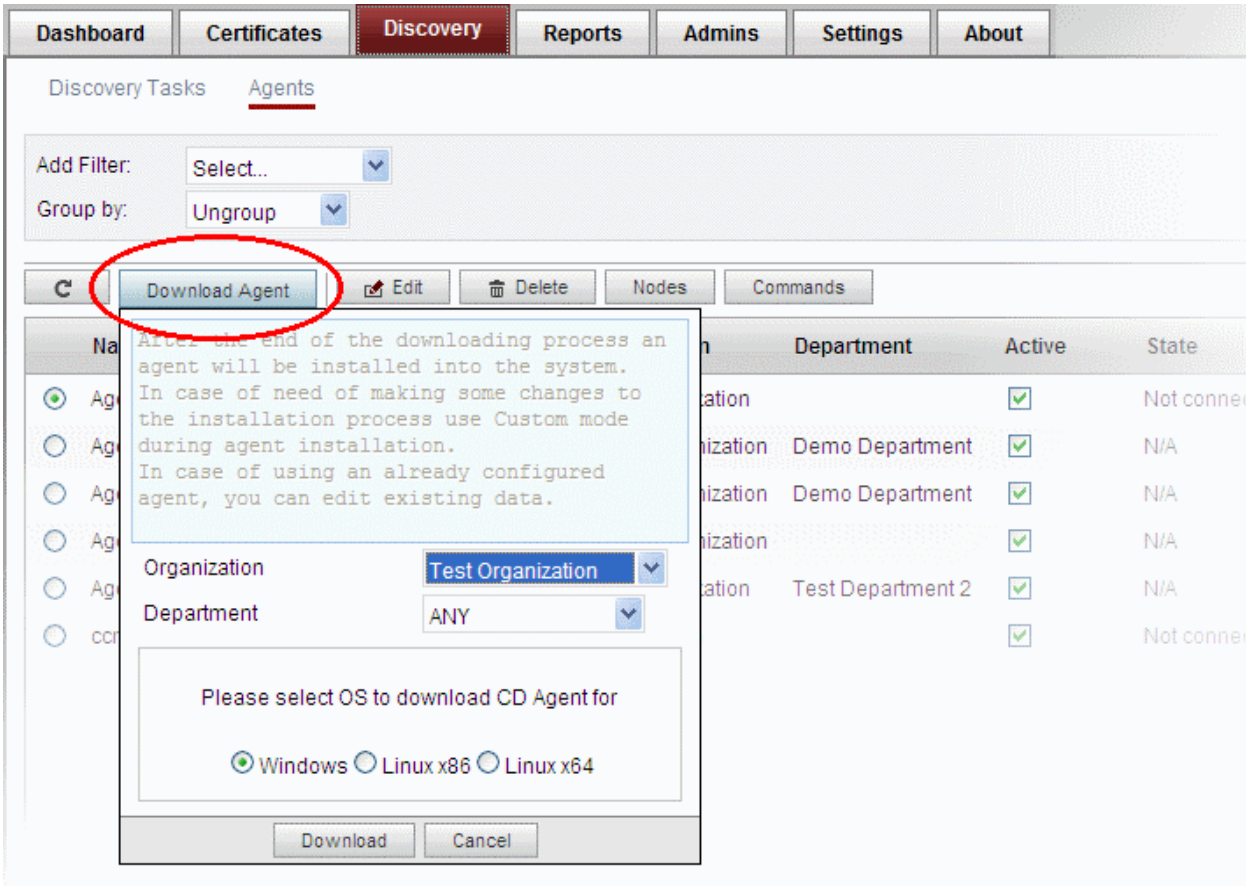
1. Add a new IP range for Internal Scanning by creating a new CIDR in the 'Discovery Tasks' tab and specify the ports to be scanned. The IPs you enter here should, naturally, be internal addresses. Once added, you will be able to initiate internal scans from this interface by clicking the 'Scan Now' button. See **Adding IP range and Start Scanning** for further reading.

Note: CCM is capable of scanning for installed certificates in external servers via Internet. If there is no agent installed in the server to be scanned, CCM will request the user to install the agent.

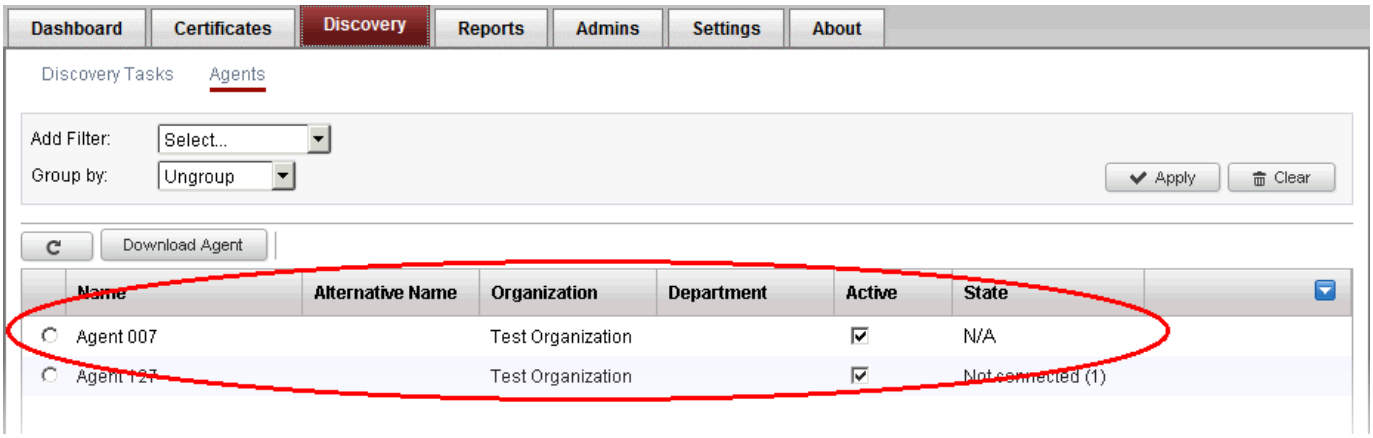
2. Download and Install the agent on a server in the network.

Note: The Agent is also responsible for automatic application and installation of SSL certificates. The Agent installed on one of the servers can be configured to communicate with the other web servers in the network without the need of any additional software, hence is capable of installing certificates on to the remote servers automatically. The important aspect is that the all the servers should be able to connect to CCM.

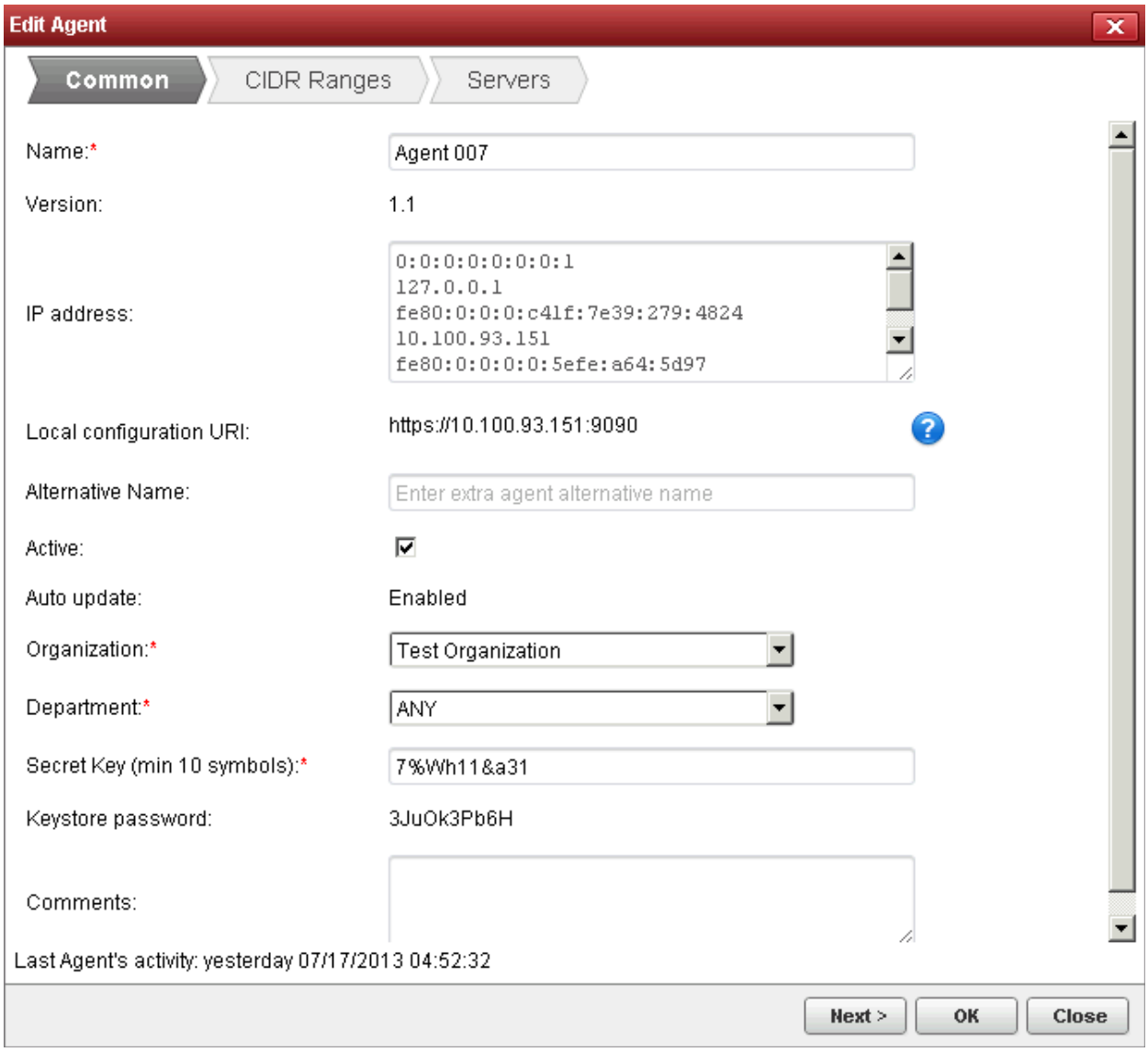
- To download the Certificate Controller Agent setup file, click 'Download Agent' from the Agents interface.



- Select the Organization/Department(s) for which you want to use the Certificate Controller Agent for auto-installation and discovery of certificates and choose Windows version or Linux version of the Agent setup file depending on the Operating system of the server.
- Click 'Download' and browse to the location where you want to save the setup file.
- The certificate controller / agent needs administrative privileges for installation. To install the Agent, right click on the setup file and select 'Run as Administrator' and follow the setup instructions in the wizard. If you are installing the Linux version of the Agent, run the installation from the command line.
- On completion of installation, the Agent will be added to the CCM interface.



- The next step is to configure the Agent to:
  - apply for and install SSL certificates on the local server
  - apply for and install SSL certificates on the remote servers in the network
  - scan the internal network by linking it to the CIDR created under the Certificate Discovery tab for internal scanning, by specifying the IP Range of the internal network
- To Edit the Agent Properties, click the 'Edit' button at the top after selecting the Agent

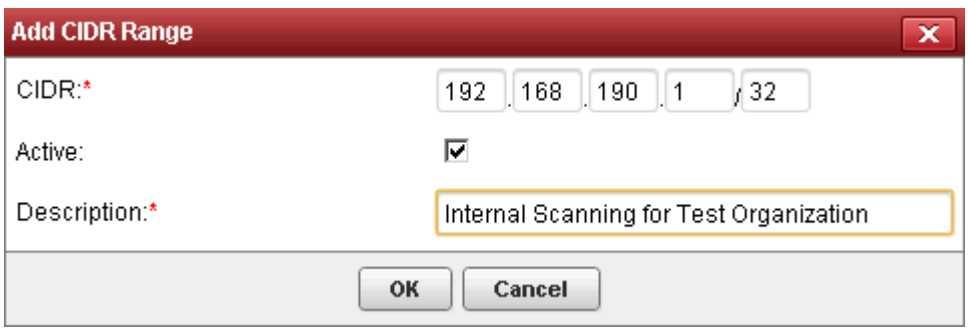


Edit Agent > Common Tab - Table of Parameters		
Field Name	**Type**	**Description**
Name	*String*	Enables the Administrator to edit the name of the Certificate Controller Agent.
Version		Specifies the version of the Agent
IP Address		Displays the IPv6 Loopback address, IPv4 loopback address, IPV6 IP Address IPv4 IP Address physical address of the server on which the agent is installed
Local Configuration URL		Displays the IP of the server in which the agent is installed. This URL is used to access the agent via a web browser for managing. Refer to the section **Configuring the Certificate Controller Agent through Web Interface** for more details.
Alternative Name	*String*	Enables the Administrator to specify an alternative name for the Agent
Active	*Checkbox*	Enables the Administrator to set the Agent in active state or inactive state.
Auto update	*String*	Indicates whether the agent is enabled for auto update

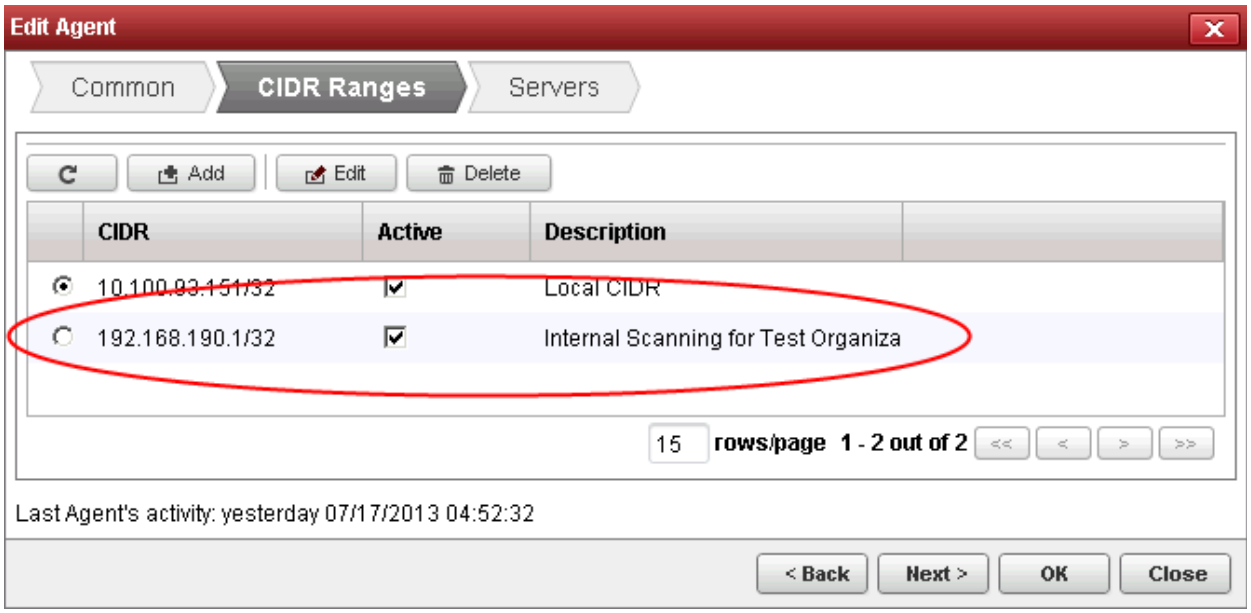
Edit Agent > Common Tab - Table of Parameters		
Organization	*Drop-down list*	Enables the Administrator to change the organization to be associated with the Agent.
Department	*Drop-down list*	Enables the Administrator to change the department to be associated with the Agent.
Secret Key	*String*	Displays the secret key generated by the Agent to authenticate itself to Remote Comodo CM server. The secret key must have 10 characters. The administrator 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 CCM server for scanning the same internal network.
Keystore password	*String*	Displays the key store password generated by the Agent. The administrator can copy and save the secret key store password in a safe location for use in a new agent, in case the agent has to be reinstalled in the same server.
Comments	*String*	Enables the Administrator to type a descriptive comment on the purpose of the Agent

- Edit the values if required, and click Next. The CIDR Ranges tab will be opened.

- To add a new CIDR range, click 'Add'. The 'Add CIDR Range' dialog will open.

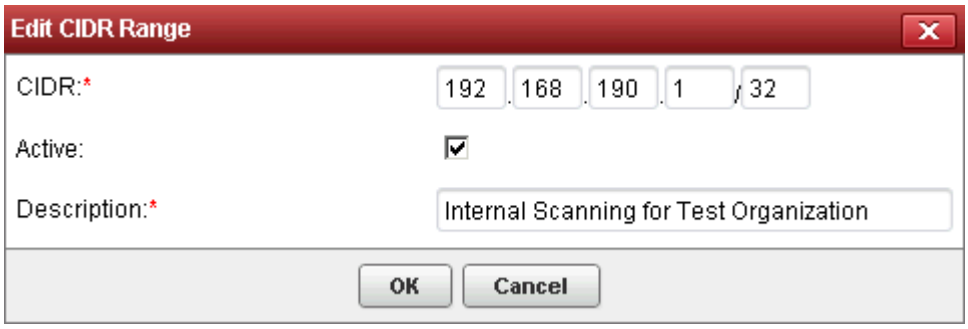


- Enter the internal IP address range to be scanned, set whether the Agent is to be Active and type a description for the range in the dialog and click OK. The CIDR Range will be added in the 'CIDR Ranges' tab.



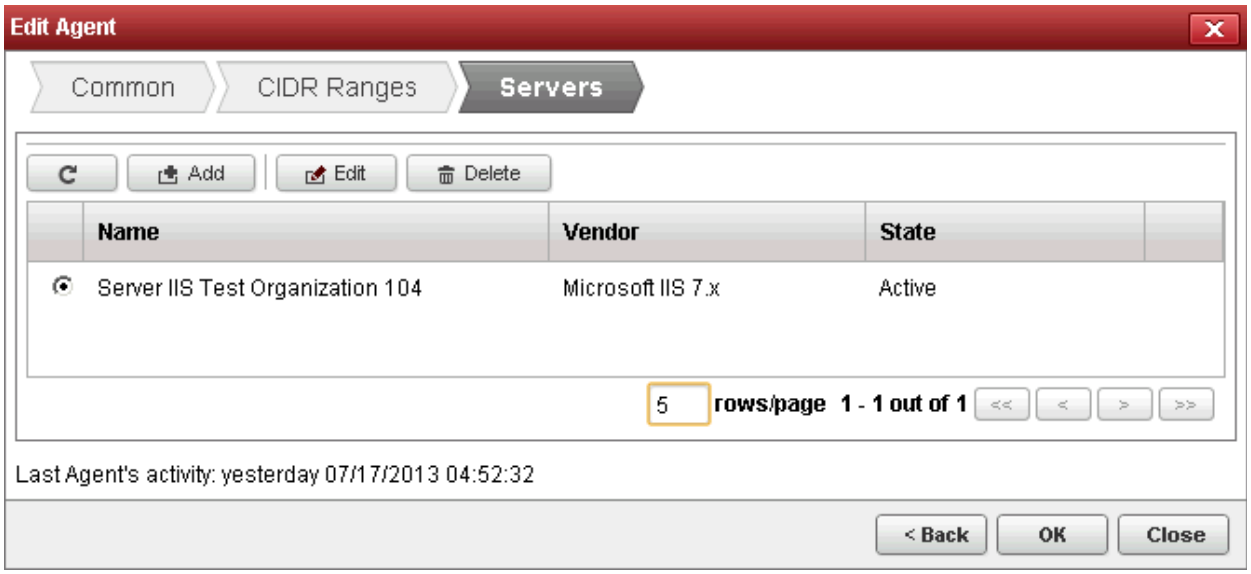
You can add as many ranges as you want by repeating the same procedure.

- To edit an existing CIDR range, select it and click 'Edit' from the top. The Edit CIDR Range dialog will open.



- To delete an existing CIDR range, select it and click 'Delete'. The confirmation dialog will open.

- Click 'Next'. The 'Servers' tab will be opened.



The Servers tab displays the list of Servers for which the agent is configured for auto-installation of certificates. On installation, the agent discovers the server upon which it is installed and adds it to the list automatically, enabling auto-installation of certificates on it.

You can edit the properties of the server by selecting it and clicking the Edit button from the top.

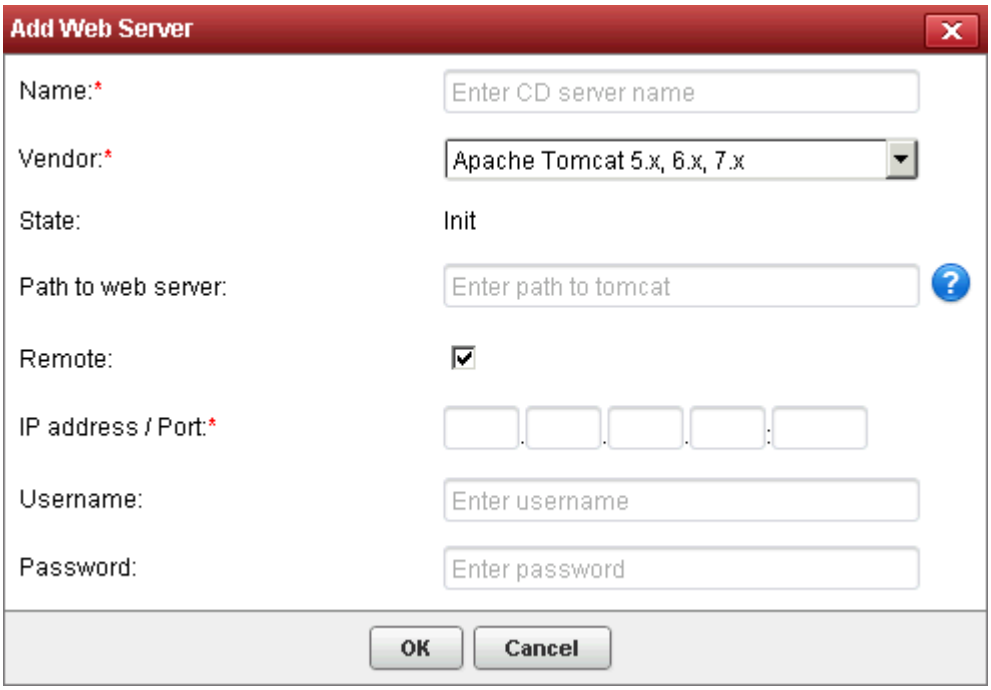
Edit Web Server - Table of Parameters		
Field Name	**Type**	**Description**
Name	*String*	Enables the Administrator to edit the name of the Server.
Vendor	*Drop-down list*	Enables the Administrator to select the vendor of the server.
Path to web server	*String*	Enables the Administrator to specify the network path for Apache. This is required only if Apache server is not accessible from the CCM console.
State		Indicates whether or not the server is connected.
Remote	*Checkbox*	Enables the Administrator to specify whether the server is local or remote. For the server in which the agent is installed, the checkbox should remain un-selected.

Configuring the Certificate Controller for Automatic Certificate Installation on Remote Servers

You can add other remote servers in the network to enable the agent to communicate with them. The agent polls CCM periodically for certificate requests for the added remote servers. If a request exists, it will automatically generate a CSR on the web server and present the application for administrator approval via the CCM interface. On approval, the agent will submit the CSR to Comodo CA and track the order number. Once the certificate is issued by the CA, the agent will download the certificate and allow the administrator to install the certificate from the CCM interface.

To add a remote server to the agent

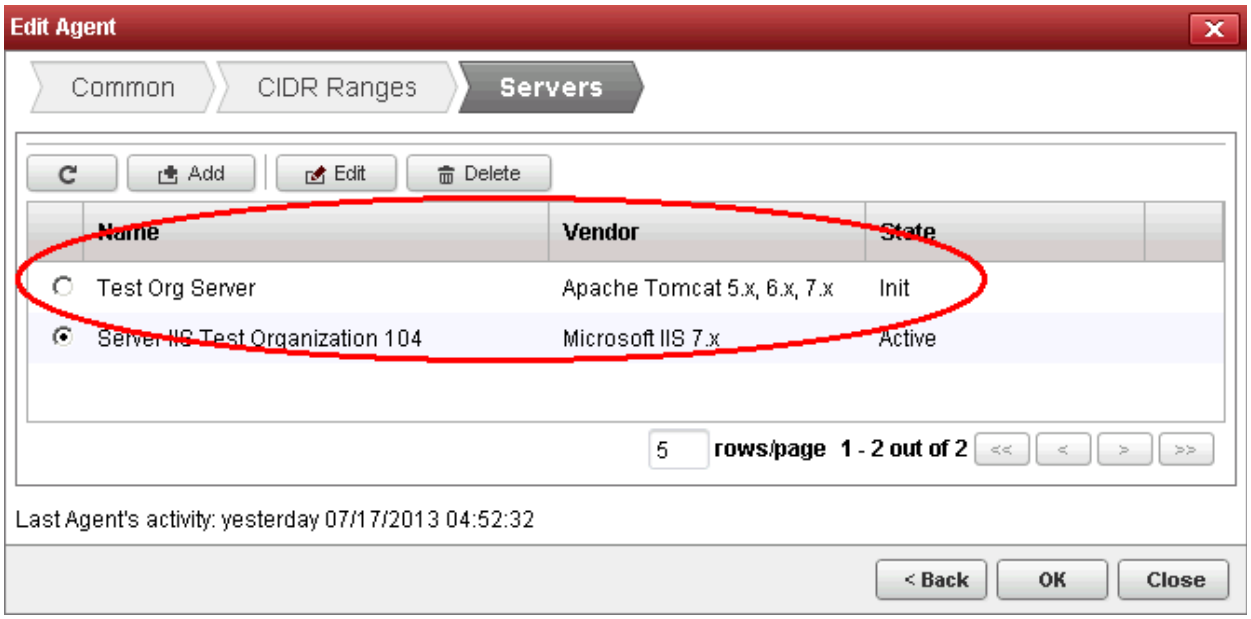
- Select the agent and click the 'Edit' but at the top and move to the Servers tab by clicking 'Next' two times in the Edit Agents dialog
- Click 'Add' under the Servers tab in the Edit Agent dialog



Add Web Servers - Table of Parameters		
Field Name	**Type**	**Description**
Name	*String*	Enables the Administrator to enter the name of the server.
Vendor	*drop-down*	Enables the Administrator to select the vendor of the server.
State	*String*	Indicates whether or not the server is initialized.
Path to Web Server	*String*	Enables the Administrator to specify the network path for Apache. This is required only if Apache server is not accessible from the CCM console.
Remote	*Checkbox*	Enables the Administrator to specify whether the server is Remote or Local. While adding remote servers for agent-less automatic certificate installation, this checkbox should be selected.
IP Address / Port	*String*	Enables the Administrator to specify the IP address and connection port of the server for remote connection. Note: This field will be enabled only if 'Remote' is selected.
User Name / Private key file	*String*	For IIS - Enables the Administrator to specify the username of the administrator for logging-into the server.

Add Web Servers - Table of Parameters		
path		For Apache - Enables the Administrator to specify the private key file path to enable agent to access the server Note: This field will be enabled only if 'Remote' is selected.
Password / Pass-Phrase	*String*	For IIS - Enables the Administrator to specify the log-in password for the administrator account for logging-into the server For Apache - Enables the Administrator to specify the passphrase of the private key file path Note: This field will be enabled only if 'Remote' is selected.

- Enter the parameters and click OK.



The remote server will be added with the state 'Initialized'.

- Click OK in the Edit Agents dialog to save your changes.

The agent will discover the newly added server and connect to it within a few minutes and the state will be changed to 'Connected'.

The Agent, is now configured to auto-install the certificates in the remote server and to scan the internal network. The Agent authenticates itself to remote Comodo CM server via combination of the secret key and awaits further instructions. The Agent polls CCM every 1 minute to find out whether there are any instructions such as an instruction to 'Scan Now'. When the 'Scan Now' button is clicked, CCM will tell the agent which CIDRs to scan. The agent performs this scan and sends the results back.

The Agent properties can be configured through the Agent's web interface accessible by typing http://<IP Address/host name of the server on which the agent is installed>:9090 in the browser address bar. The administrator can change the connection settings, polling interval, certificate management settings and server settings from the web interface. Refer to the section **Configuring the Certificate Controller Agent through Web Interface** for more details.

3. Go back to 'Certificates Discovery' tab and click 'Scan Now'. You can also schedule the scans to run periodically to discover the SSL certificates installed in the internal servers. See **Adding IP range and Start Scanning** for more details.
4. Certificate discovery results can be viewed by selecting the 'Discovery Scan Log' under the 'Reports' tab. Newly discovered certificates will be added to the 'SSL Certificates' area of 'Certificates Management'. All certificates will be assigned to the Organization that was specified for the agent in **Step 2**.
    - See the section, **View Scan Results**, for a more detailed account of scan reports and managing newly discovered certificates. Administrators that have not already done so may also want to familiarize themselves with the information in section **The SSL Certificates Area**.

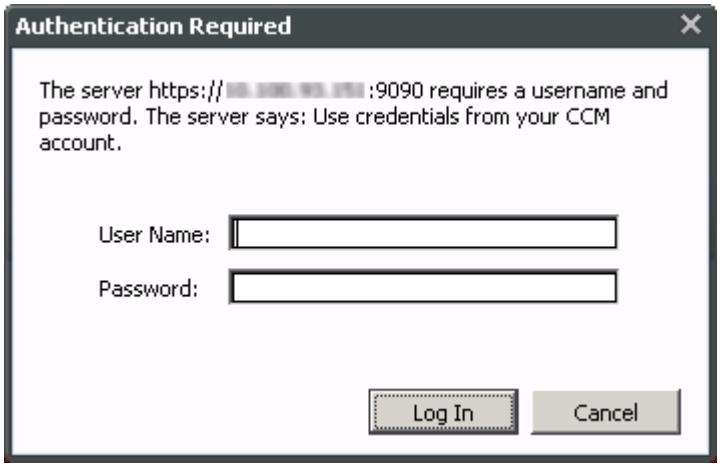
6.1.2.5 Configuring the Certificate Controller Agent through Web Interface

The Certificate Controller Agent can be configured by logging-in to its web-interface.

To access the Agent configuration web interface

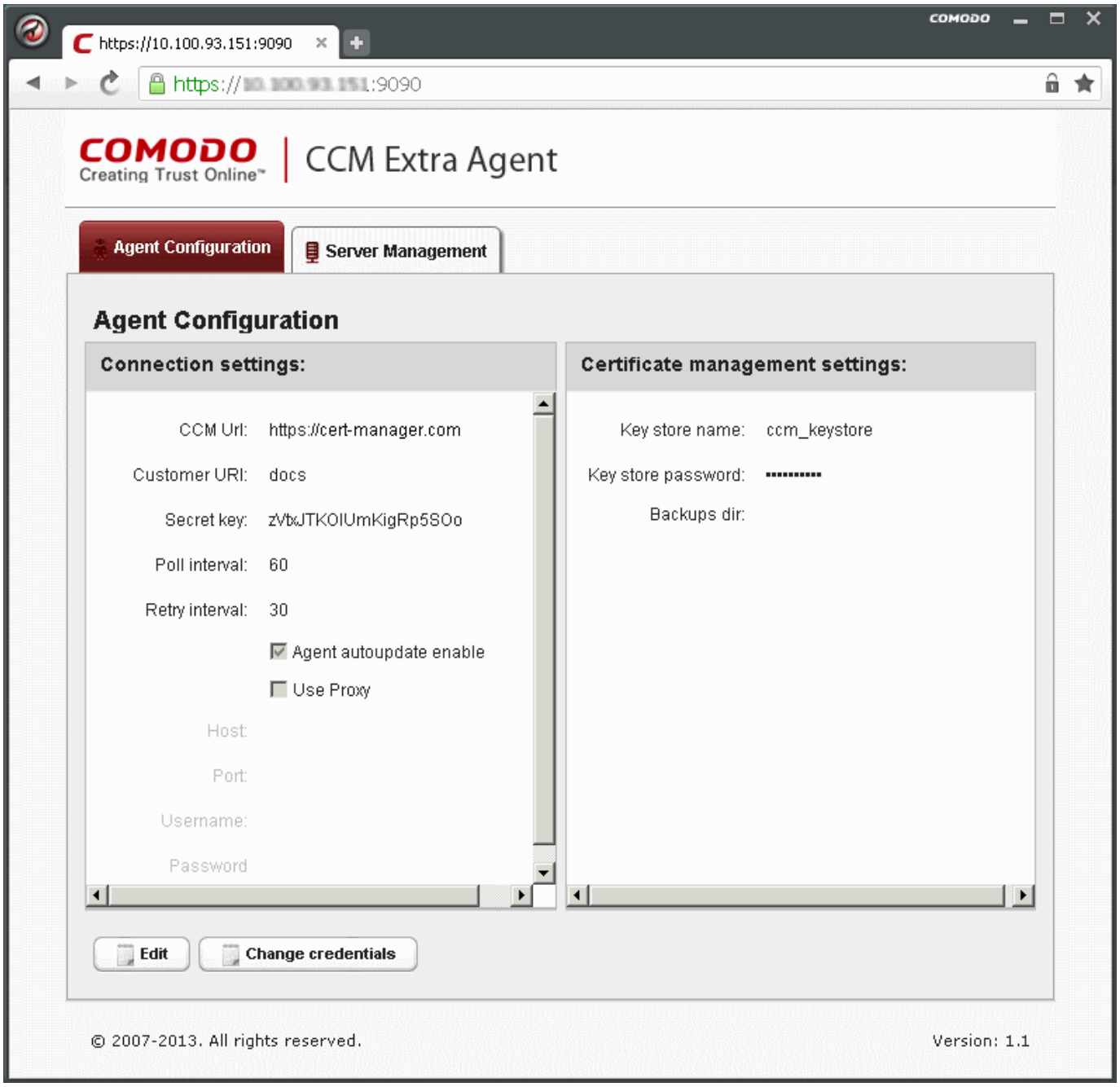
- Type http://<IP Address/host name of the server on which the agent is installed>:9090 in the address of your browser.

The login dialog will appear:



- Enter your CCM username and password.

The Agent configuration interface will open.

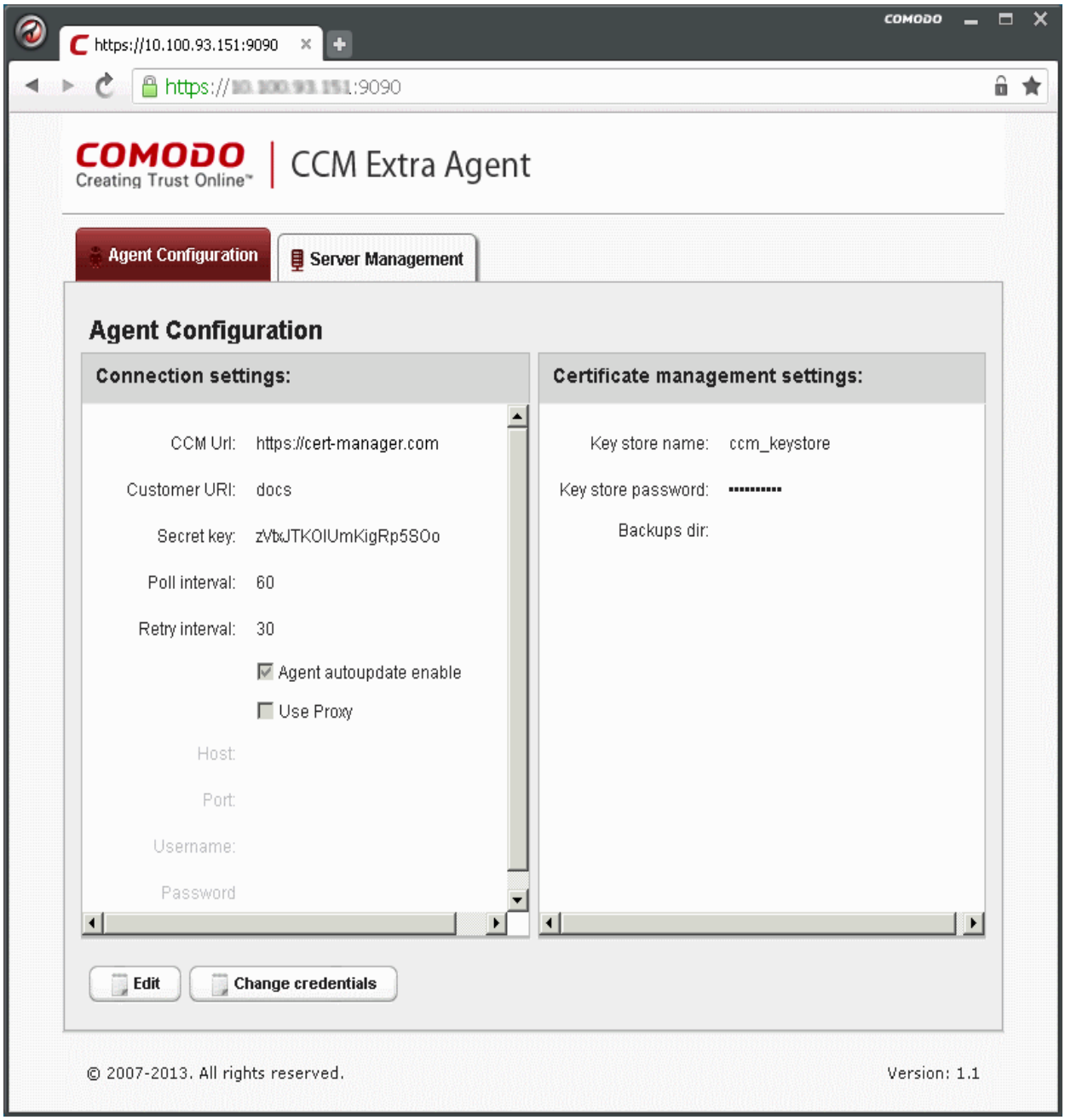


It has two tabs:

- **Agent Configuration**
- **Server Management**

6.1.2.5.1 Agent Configuration

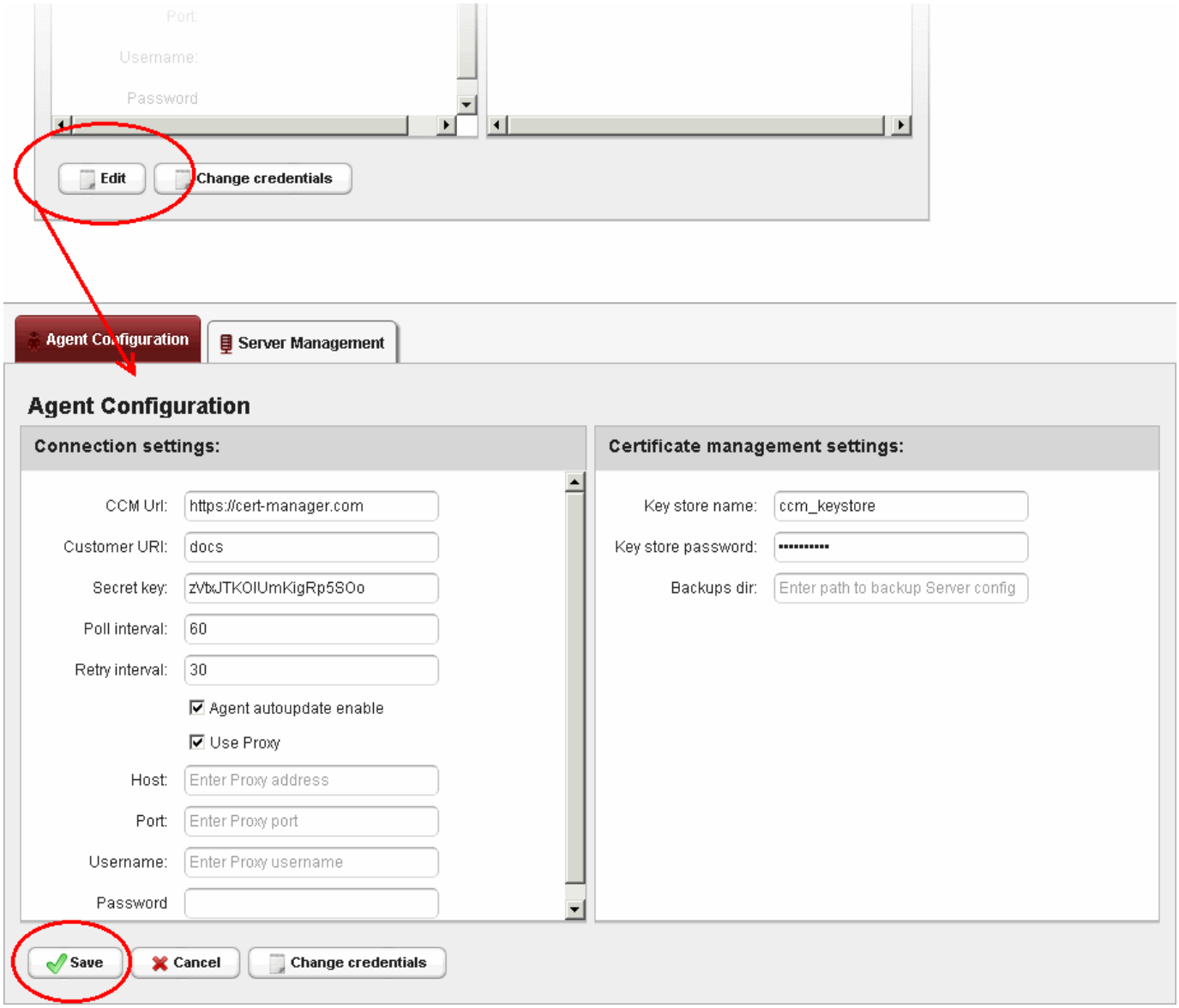
The Agent Configuration tab displays the connection management settings and certificate management settings of the agent and enables the administrator to edit them, if required.



Agent Configuration - Table of Parameters		
Field	**Type**	**Description**
Connection Settings		
CCM url	*Text field*	Displays the url of CCM server
Customer url	*Text field*	Displays the uniform resource identifier (URI) of the customer
Secret key	*Text field*	Displays the secret key unique to the agent, which it uses to identify it to CCM. This value should not be altered
Poll Interval	*Text field*	Displays the time interval at which the agent polls the CCM for new certificate requests (in seconds) and enables the administrator to edit it in edit mode.
Retry interval	*Text field*	Displays the time interval set for retrying polling on CCM server if polling fails (in seconds) and enables the administrator to edit it in edit mode.

Agent autoupdate enable	*Checkbox*	Indicates whether the agent is enabled for auto-update. The checkbox enables the administrator to switch the auto-update on/off in edit mode.
Use Proxy	*Checkbox*	Indicates whether the agent is configured to use a proxy server. The checkbox and the text fields below it enable the Administrator to instruct the agent to use proxy server and to specify the proxy server details, if required.
Host	*Text field*	Displays the IP/Host name of the proxy server and enables the Administrator to specify it in edit mode
Port	*Text field*	Displays the port of the proxy server for the agent to connect and enables the Administrator to specify it in edit mode
Username	*Text field*	Displays the username of the administrator account to login to the proxy server and enables the Administrator to specify it in edit mode
Password	*Text field*	Displays the password of the administrator account to login to the proxy server and enables the Administrator to specify it in edit mode
Server Settings		
Key store name	*Text field*	The name of the CCM keystore file, pertaining to the agent. By default, it will be 'ccm_keystore'. The Administrator can edit it in the edit mode
Keystore password	*Text field*	The password to access the CCM keystore file. The Administrator can edit it in the edit mode
Backup dir	*Text field*	Displays the folder path for backup of keystore file. The Administrator can edit it in the edit mode.

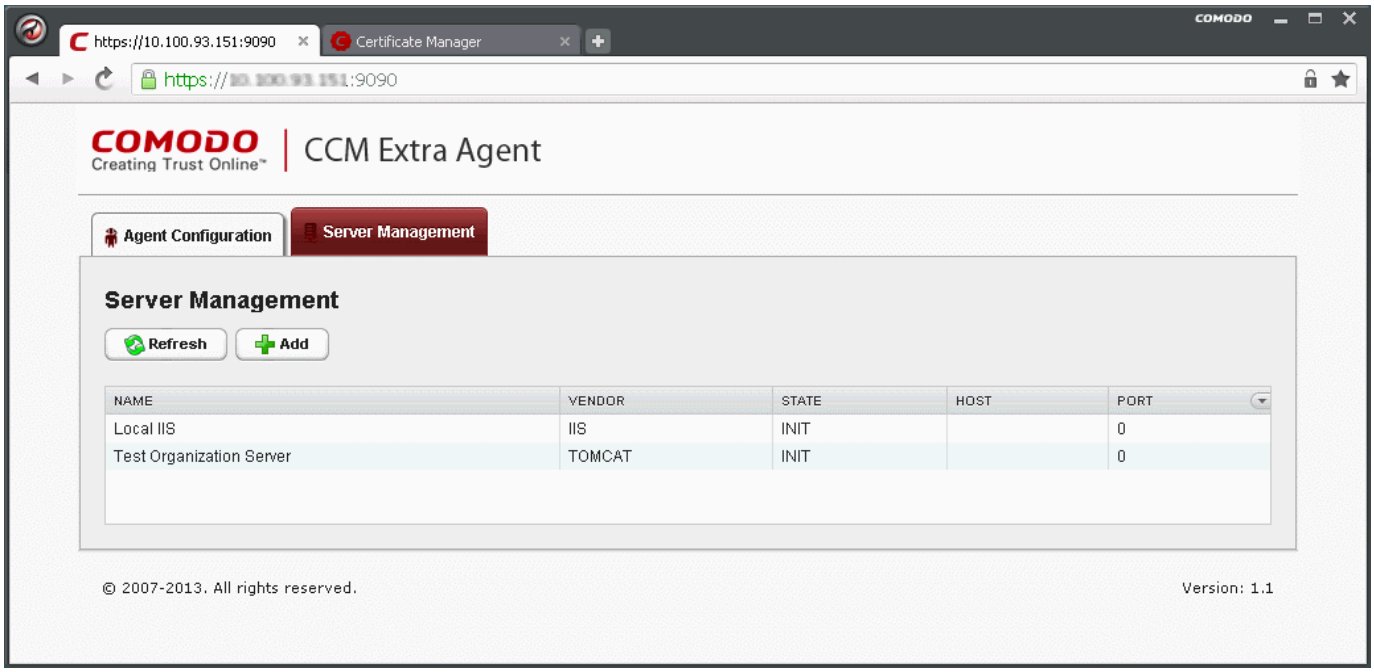
- To edit the agent configuration settings, click the 'Edit' button at the bottom left. The Agent Configuration page will open in edit mode.



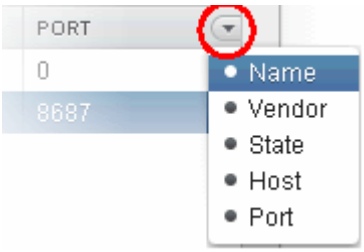
- Edit the required fields and click 'Save' for your changes to take effect.

6.1.2.5.2 Server Management

The Server Management tab enables the administrator to view, add and edit the servers for which the agent is configured.



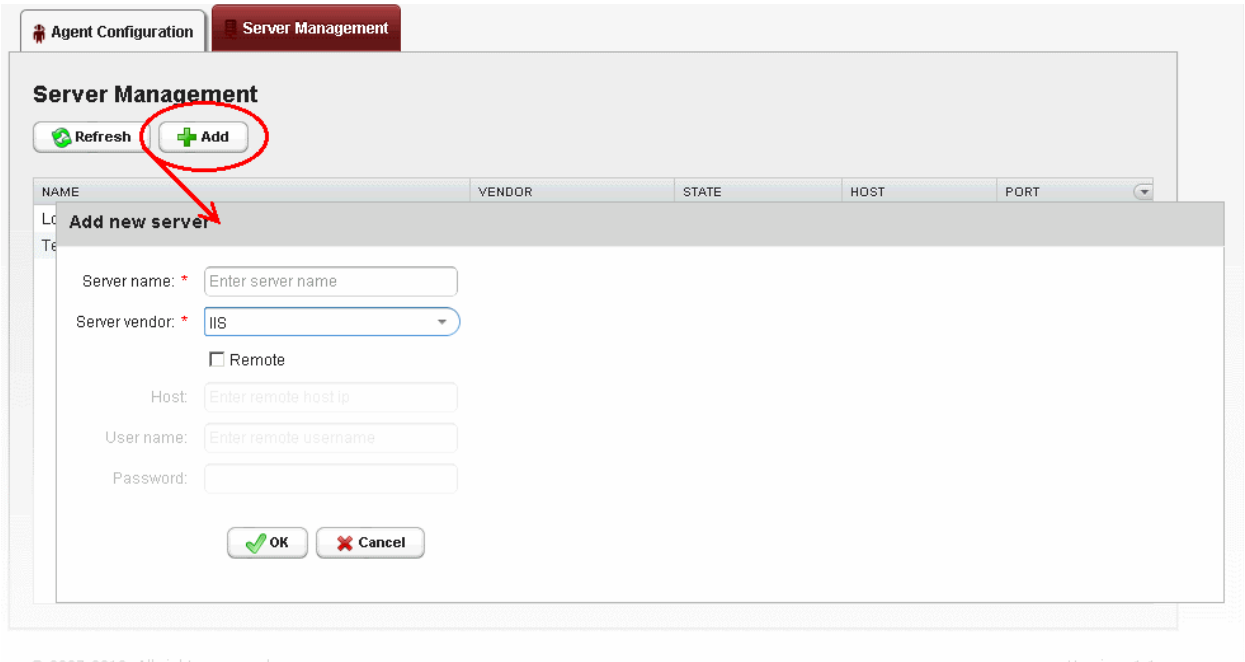
The Server Management tab displays the list of servers added to the agent with the vendor and activation status details. The administrator can add new servers and edit the details like the login username and password for the existing servers through this interface.

Column Display		Description
Name		Displays the name of the server.
Vendor		Displays the vendor of the server.
State		Indicates whether or not the server is initialized.
Host		Displays the IP address or the host name of the server for remote connection
Port		Displays the connection port of the server for remote connection.
Note: The administrator can enable or disable the columns from the drop-down button beside the last item in the table header: 		
Controls		
	Add	Enables the Administrator to add a new server to the agent
	Refresh	Updates the list of displayed servers.
Server Controls **Note**: The Server control buttons will appear only on selecting a		
	Edit	Enables administrators to modify the Server configuration settings.
	Delete	Removes the Server.

server.		

To add a server

- Click 'Add' from the top left. The 'Add new server' dialog will appear.



Add new server - Table of Parameters		
Field Name	**Type**	**Description**
Server name	*String*	Enables the Administrator to enter the name of the server.
Server vendor	*drop-down*	Enables the Administrator to select the vendor of the server.
State	*String*	Indicates whether or not the server is initialized.
Path	*String*	Enables the Administrator to specify the network path for the Tomcat server. This is required only if the Tomcat server is not accessible from the CCM console. Note: This field will be appear only of Tomcat server is selected in the Server vendor drop-down.
Remote	*Checkbox*	Enables the Administrator to specify whether the server is Remote or Local. While adding remote servers for agent-less automatic certificate installation, this checkbox should be selected.
Host	*String*	Enables the Administrator to specify the IP address or host name of the server for remote connection. Note: This field will be enabled only if 'Remote' is selected.
Port	*String*	Enables the Administrator to specify the connection port of the server for remote connection. Note: This field will be enabled only if 'Remote' is selected.
User Name	*String*	For IIS - Enables the Administrator to specify the username of the administrator for loggin-into the server.

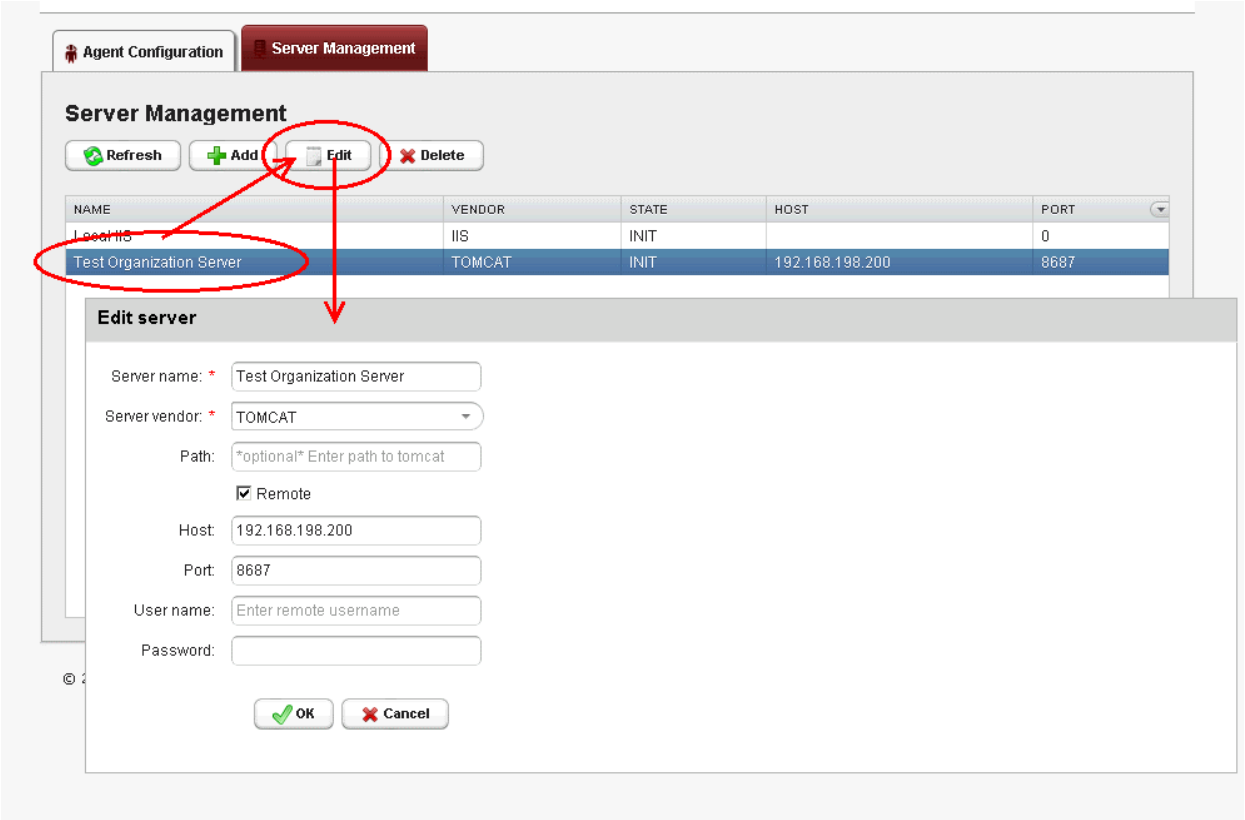
Add new server - Table of Parameters		
		For Apache - Enables the Administrator to specify the private key file path to enable agent to access the server Note: This field will be enabled only if 'Remote' is selected.
Password	*String*	For IIS - Enables the Administrator to specify the log-in password for the administrator account for logging-into the server For Apache - Enables the Administrator to specify the passphrase of the private key file path Note: This field will be enabled only if 'Remote' is selected.

- Enter the parameters and click OK.

The new server will be added and enabled for automatic installation of SSL certificates.

To edit a server

- Select the server and click the 'Edit' button that appears on top.



The Edit server dialog will open. The interface is similar to **Add new server** interface.

- Edit the required fields and click 'OK' for your changes to take effect.

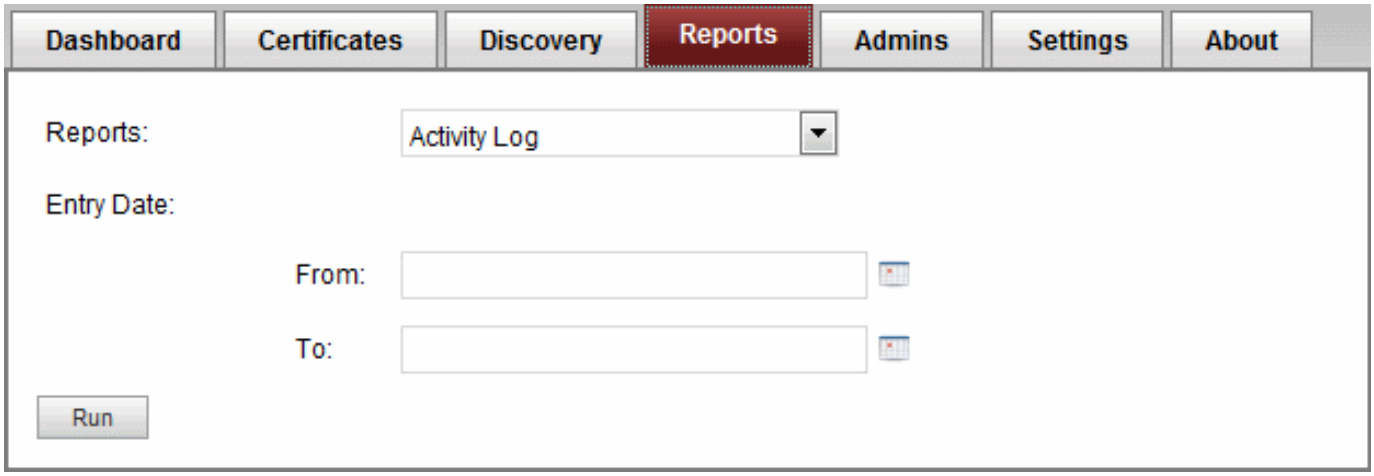
7 Reports

7.1 Overview

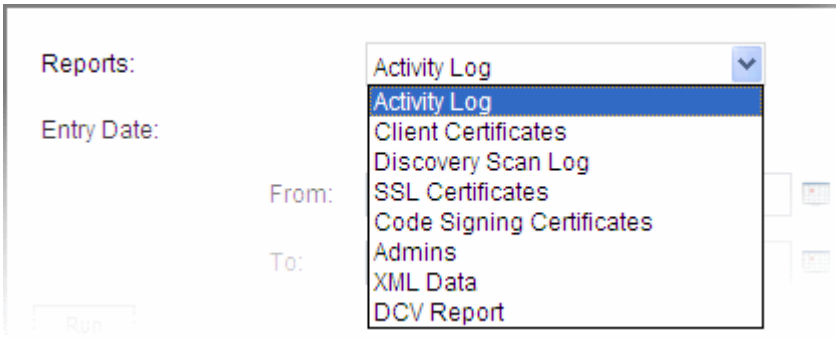
The 'Report' tab enables the administrator to generate and view reports that reflect an activity and other statistics related to usage, provisioning and monitoring of SSL and Client and Code Signing Certificates. There are nine main types of reports

available: Activity Log report, Client Certificates report, Discovery Scan Log , SSL Certificates report, Code Signing Certificates report, Admin report, XML Data report and DCV report.

- The **Activity Log report** enables the MRAO administrator to view history of all events concerning all the types of certificates: Client, SSL and Code Signing.
- The **Client Certificates reports** enable the administrator to view history of all events that concern to client certificates.
- The **Discovery Scan Log** reports enables the administrator to view information concerning to overall scan options and discovered SSL certificates information.
- The **SSL Certificates repor**t enable the administrator to view history of all events that concern to SSL certificates.
- The **Code Signing Certificates** reports enable the administrator to view history of all events that concern to code signing certificates.
- The **Admins report** enables the MRAO administrator to view the list of all the administrators and their privilege levels.
- The **XML Data report** enables the MRAO administrator to download a report containing complete details of the Organizations, Departments, their administrators and the all the certificates in XML format.
- The **DCV Report** enables the MRAO administrator and RAO/DRAO SSL Administrators to download a report containing complete details of registered domains and their Domain Control Validation (DCV) status.
- The **Notification Log Statistics Report** enables the MRAO administrator to download reports containing complete details of the notifications emails, statistics of notification types and overall notification logs.
- Administrators will find the Report functionality especially useful when troubleshooting any issues relating to the provisioning, installation and management of client or SSL certificates.
- The Report section is a permanent archive of all actions that took place with all certificates that were issued and managed via Comodo Certificate Manager.



Select the type of report you wish to view from drop-down menu:



Report Type	Description
Activity log	Selecting this type of report enables the MRAO to generate and view reports providing a highly detailed log of ALL actions recorded by Comodo Certificate Manager for the selected period of time. (for

Report Type	Description
	example - Admin Login times, Modifications to users, certificate requests, changes in certificate statuses etc)
Client Certificates	Selecting this type of report enables administrators to generate and view reports regarding Client Certificate Activity. Reports are delivered in .csv format and can be filtered to show only certificates with a specific current status, namely: • Any *(all certificates of any status)* • Enrolled - Downloaded • Enrolled - Pending Download • Revoked • Expired • Not Enrolled The reports can be further sorted by Organization/Department, (status specific) Date and by Time Interval.
Discovery Scan Log	Selecting this type of report enables administrators to generate and view log reports from the scanning processes. Reports are delivered in .csv format. The reports can be further sorted by Organization/Department.
SSL Certificates	Selecting this type of report enables administrators to generate and view reports regarding SSL Certificate Activity. Reports are delivered in .csv format and can be filtered to show only certificates with a specific current status, namely: • Any (*all certificates of any status*) • Requested • Issued • Revoked • Expired The reports can be further sorted by Organization/Department, (status specific) Date and by Time Interval.
Code Signing Certificates	Selecting this type of report enables administrators to generate and view reports regarding Code Signing Certificate Activity. Reports are delivered in .csv format and can be filtered to show only certificates with a specific current status, namely: • Any (*all certificates of any status*) • Enrolled - Downloaded • Enrolled - Pending Download • Revoked • Expired The reports can be further sorted by Organization/Department, (status specific) Date and by Time Interval.
Admin	Selecting this type of report enables the MRAO to generate and view reports providing the details of the enrolled Administrators of all privilege levels.
XML Data	Selecting this type of report enables the MRAO to generate a report containing complete details of all the Organizations, Departments, their administrators and the all the certificates in XML format.
DCV Report	Selecting this type of report enables the MRAO and RAO/DRAO SSL administrators to generate and view a report on registered domains with their Domain Control Validation (DCV) status. Reports are delivered in .csv format and can be filtered to show only certificates with a specific current status,

Report Type	Description
	namely: • Any *(all certificates of any status)* • Not Started • Awaiting Submittal • Submitted • Validated • Validated Renewing • Expired The reports can be further sorted by Organization/Department, (status specific) Date and by Time Interval. **Note**: DCV Report will be available only if DCV feature has been enabled for your account.
Notification Log Statistics Report	Selecting this type of report enables the MRAO to generate reports containing complete details of all notification emails sent to other administrators. Reports are delivered in .csv format.

7.2 Reports - Security Roles Access Table

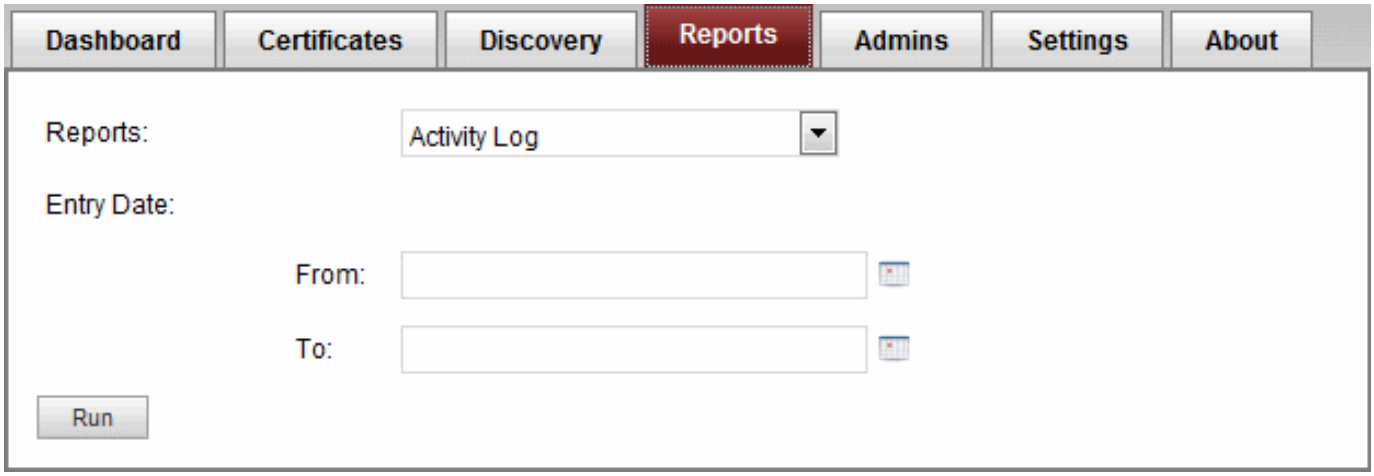
The following table provides a summary of the ability of the administrators to generate different types of reports.

Report Type/Organization	MRAO Administrator	RAO Administrator			DRAO Administrator		
		SSL	SMIME	Code Signing	SSL	SMIME	Code Signing
Report Type							
Activity Log	✓	✗	✗	✗	✗	✗	✗
Client Certificates	✓	✗	✓	✗	✗	✓	✗
Discovery Scan Log	✓	✓	✗	✗	✓	✗	✗
SSL Certificates	✓	✓	✗	✗	✓	✗	✗
Code Signing Certificates	✓	✗	✗	✓	✗	✗	✓
Admins	✓	✗	✗	✗	✗	✗	✗
XML Data	✓	✗	✗	✗	✗	✗	✗
DCV Report	✓	✓	✗	✗	✓	✗	✗
Notification Log Statistics Report	✓	✗	✗	✗	✗	✗	✗
Organizations/ Departments							
	All Organizations	Only the Organizations (and any sub-ordinate Departments) that have been			Only the Departments that have been		

	are available for selection.	delegated to them are available for selection.	delegated to them are available for selection.

7.3 Activity Log Report

The 'Activity Log' option enables the MRAO to generate and view reports that reflect ALL the activities (for example - Admin Login times, Modifications to users, certificate requests, changes in certificate statuses etc) recorded by the CCM for a selected period of time. Once the 'Activity Log' type of reports is selected the following form appears:



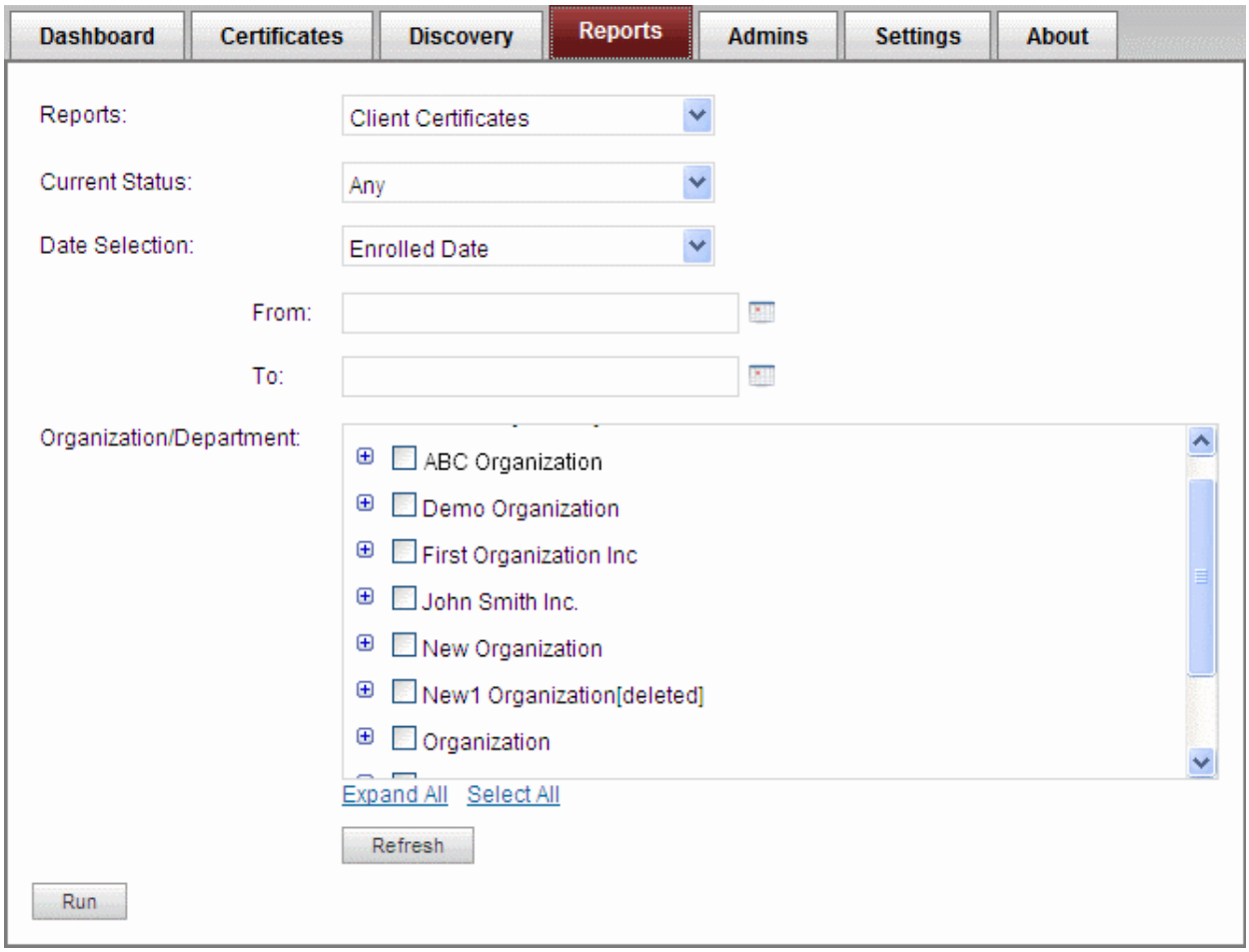
7.3.1 Report Type: Activity Log - Table of Parameters

Form Element	Control	Description
Entry Date	Calendar Buttons to select the date range	Enables administrator to generate a report in .csv format for Activity Log for a specified period of time. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the log entries, regardless of the entry date.
Run	Control	Starts the report generation.

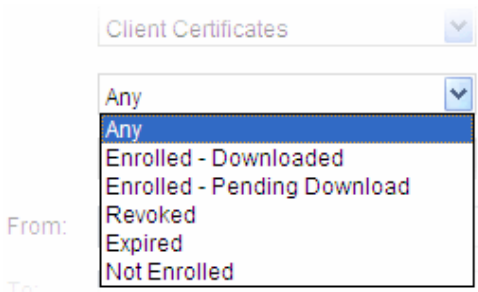
7.4 Client Certificates Reports

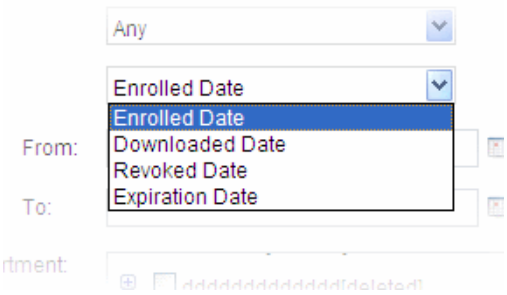
The 'Client Certificates' option enables the MRAO and RAO/DRAO SMIME administrators to generate and view reports that reflect an activity and other statistics related to usage, provisioning and monitoring of client certificates. The administrator is able to filter the reports by certificate status. The 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.

Once the 'Client Certificates' type of reports is selected the following form appears:



7.4.1 Report Type: Client Certificates - Table of Parameters

Form Element	Control	Description
Current Status	Drop-down list 	Enables administrator to generate a report in .csv format for Client Certificates with a specific current status: ***Any*** - Generates a report for ALL client certificates regardless of their current status. Does not display any SSL certificates. ***Enrolled - Downloaded*** - Generates a report of those client certificates that have been successfully enrolled for by the end-user and subsequently downloaded. ***Enrolled - Pending Download*** - Generates a report of those client certificates that have been successfully enrolled for 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 only for those end-users that belong to an Organization and are listed in the Client Certificates tab as a client certificate user but haven't enrolled for their client certificate.

Form Element	Control	Description
Date Selection	Drop-down list 	Enables administrator to set a 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 displayed on this drop-down menu is dependent on the status chosen in the 'Current Status' drop down. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the scans, regardless of the dates.
Organization/ Department	Checkboxes	Enables the administrator to generate reports for specific Organizations/Departments. If multiple Organizations/Departments are selected then the administrator will receive a single report that covers those selected Organizations/Departments. Each Organization will be displayed on a separate row in the 'Organizations' column and each Department will be displayed in a separate row in the 'Departments' column. Clicking on Expand All expands the tree structure to display all the Departments under each Organization. Clicking Select All will generate a report for ALL Organizations that were assigned to that administrator. If NO Organization/Department is selected, the report will be generated for all the Organizations/Departments, delegated to the specific administrator.
Refresh	Control	Enables the administrator to update the information in the form.
Run	Control	Starts the report generation.

7.5 Discovery Scan Log Reports

The 'Discovery Scan Log' option enables the MRAO and RAO/DRAO SSL administrators to generate and view log reports from the scanning processes.

The administrator is able to select any one of the following two types of the Discovery Scan Log Reports:

- **Summary**
- **Detail**

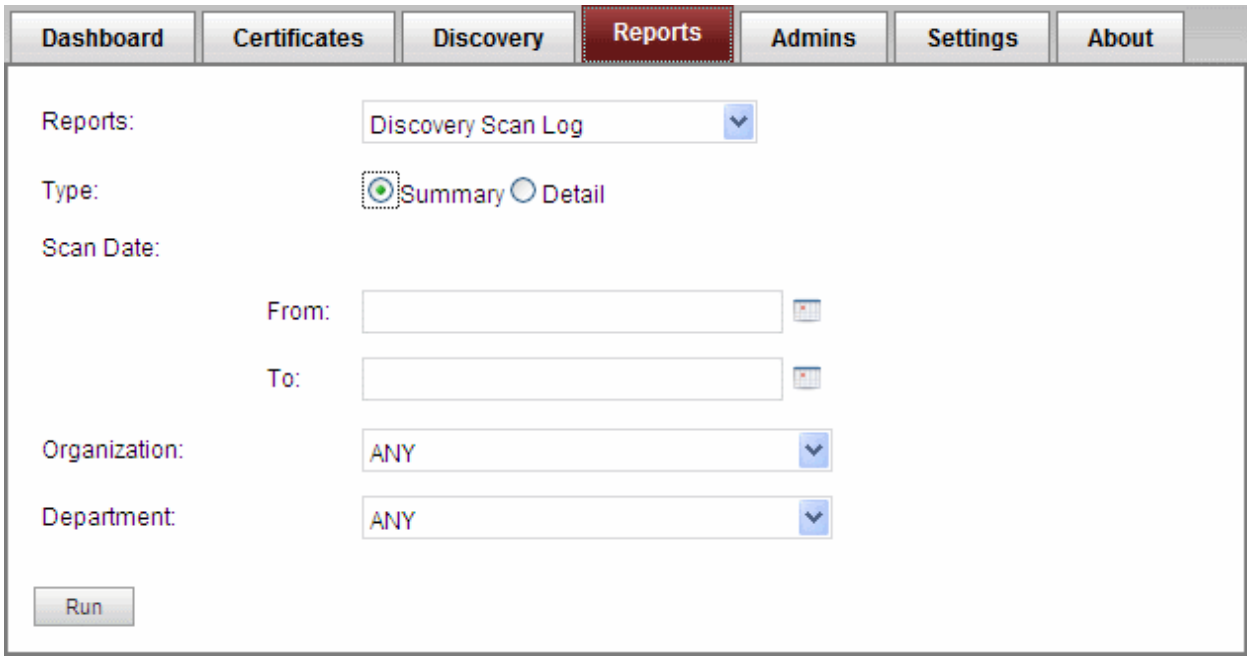
7.5.1 Discovery Scan Log Report: Summary type

The Summary type discovery scan log report is generated for a specified time period. The .csv format report generated will have 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;
- Comodo certificates Found;
- New Comodo 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 (if the scan is failed - the fail reason) | Scan Canceled by User);
- Reason for failure (in case of 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 etc).

On selecting the Summary type, the following form appears.



7.5.1.1 Report Type: Discovery Scan Log :Summary - Table of Parameters

Form Element	Control	Description
Type	Radio buttons	Enables administrators to choose between a detailed report or a summary report. Both types are generated in .csv format.

Scan Date	Calendar buttons	Enables the administrator to generate a report in .csv format for Discovery Scan Log for a specified time period. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the scans, regardless of the dates.
Organization	Drop-down	Enables the administrator to specify an Organization for which the discovery scan log has to be generated. Selecting 'Any' will generate a report for the Organizations that have been delegated to the specific administrator. This option is not visible to DRAO administrator.
Department	Drop-down	Enables the administrator to specify a Department belonging to the selected Organization for which the discovery scan log has to be generated. Selecting 'Any' will generate a report for the Departments belonging to the selected Organization. For DRAO admins, selecting 'Any' will generate a report for all the Departments that are delegated to him/her.
Run	Control	Starts the report generation

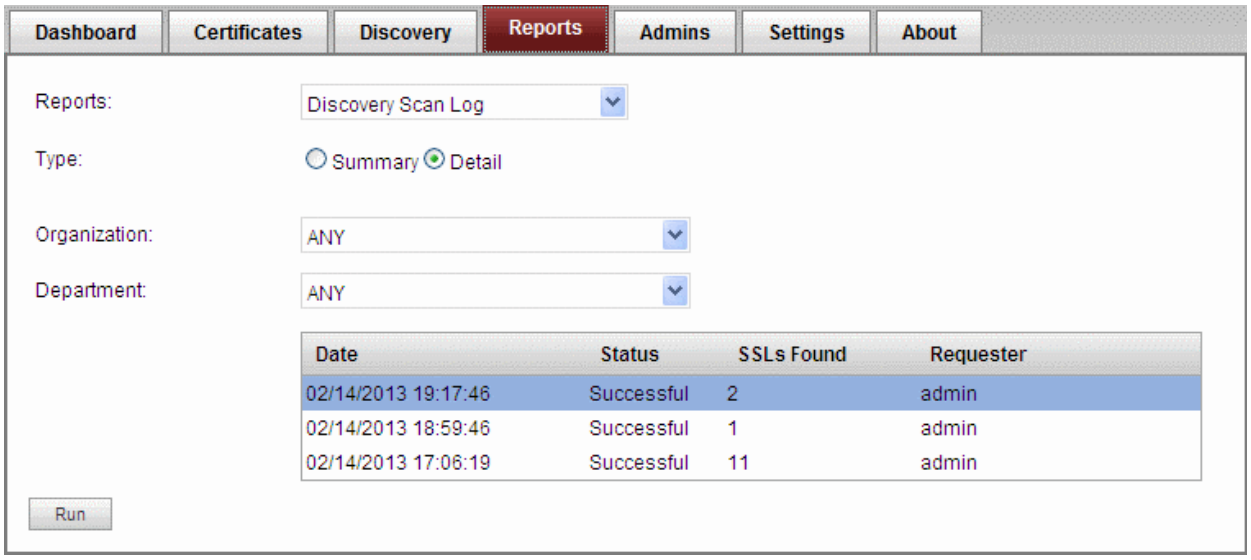
7.5.2 Discovery Scan Log Report: Detail type

The Detail type discovery scan log report is generated for a specific manual or scheduled scan and will contain in-depth details of the certificates found during the selected scan. The report generated in .csv format will contain 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.

On selecting the Detail type, a list of previously run manual/scheduled scans (up to last 10 scans with the most recent on top)

are displayed. The administrator can select a scan by clicking on it to generate a detailed discovery scan log report.

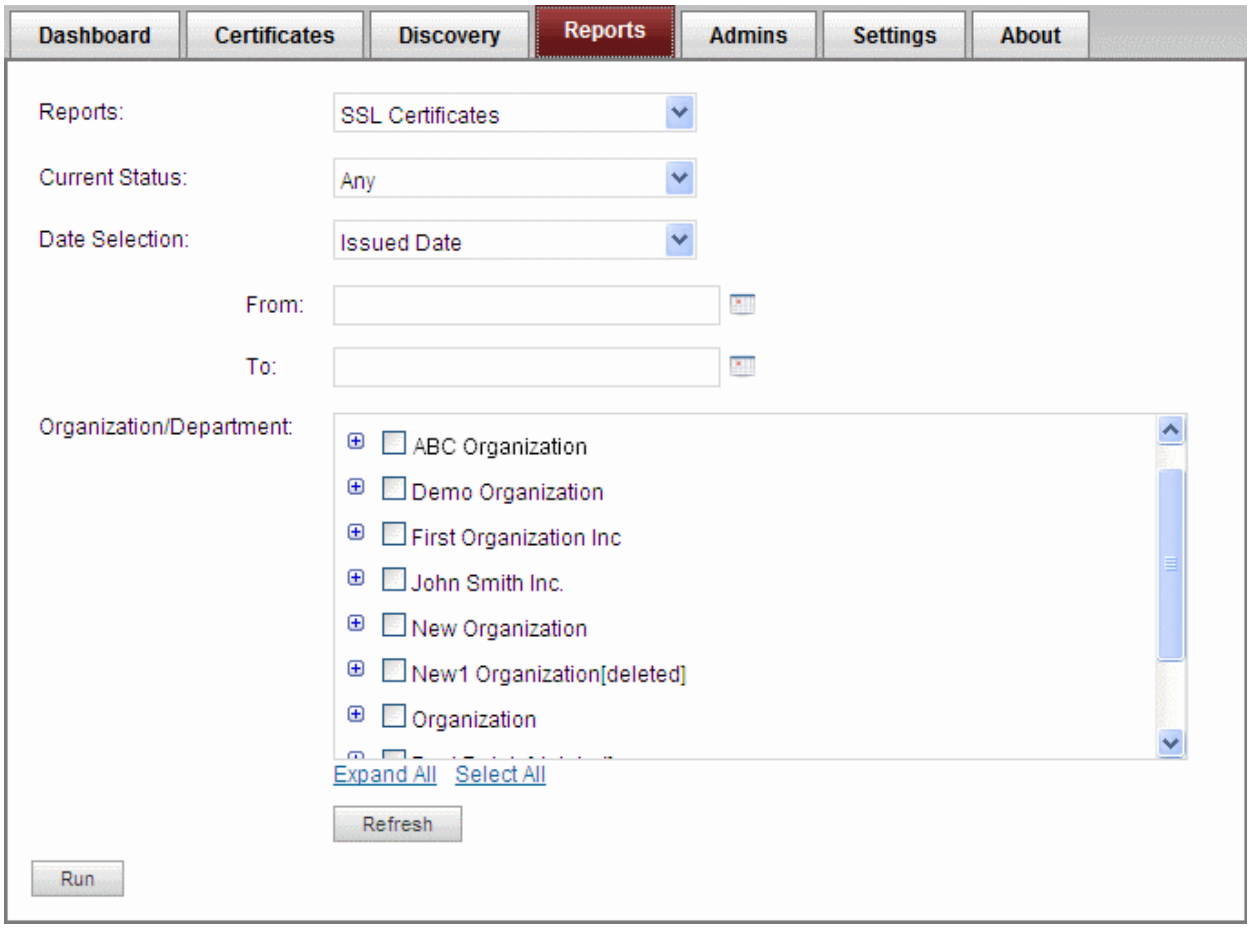


7.5.2.1 Report Type: Discovery Scan Log :Detail - Table of Parameters

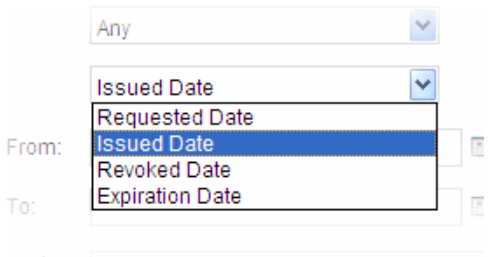
Form Element	Control	Description
Type	Radio buttons	Enables administrators to choose between a detailed report or a summary report. Both types are generated in .csv format.
Organization	Drop-down	Enables the administrator to specify an Organization for which the discovery scan log has to be generated. Selecting 'Any' will generate a report for the Organizations that have been delegated to the specific administrator. This option is not visible to DRAO administrator.
Department	Drop-down	Enables the administrator to specify a Department belonging to the selected Organization for which the discovery scan log has to be generated. Selecting 'Any' will generate a report for the Departments belonging to the selected Organization. For DRAO admins, selecting 'Any' will generate a report for all the Departments that are delegated to him/her.
List of most recent scans		Enables the administrator to select a scan for which the detailed discovery scan report has to be generated. After selecting an entry from the list, click the 'Run' button to generate the detailed report (.csv format). Date / Status / SSLs Found / Requester 02/14/2013 19:17:46 Successful 2 admin 02/14/2013 18:59:46 Successful 1 admin 02/14/2013 17:06:19 Successful 11 admin
Run	Control	Starts the report generation.

7.6 SSL Certificates Reports

The 'SSL Certificates' option enables the MRAO and RAO/DRAO SSL administrators to generate and view reports that reflect an activity and other statistics related to usage, provisioning and monitoring of SSL certificates. The administrator is able to generate the following types of reports: Requested, Issued, Revoked and Expired SSL certificates. Additionally, there is an ability to filter the certificates by date of request, issuance, revocation or expiration. Once the 'SSL Certificates' type of reports is selected the following form appears:



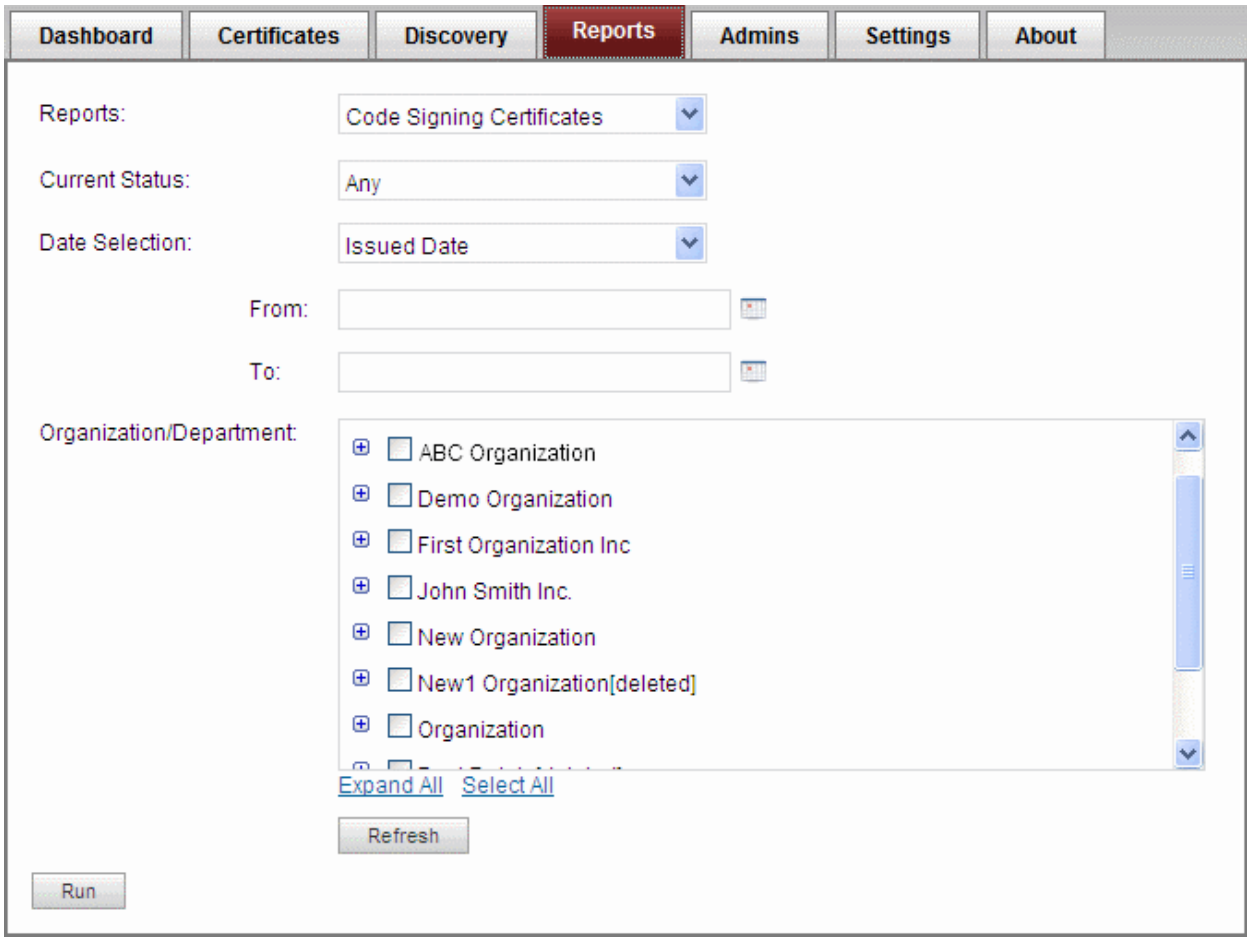
7.6.1 Report Type: SSL Certificates - Table of Parameters

Form Element	Control	Description
Current Status	Drop-down list 	Enables the administrator to generate a report in .csv format for SSL certificate with a specific current status: **Any** - Generates a report for ALL SSL certificate types regardless of their current status. **Requested** - Generates a report only for SSL certificate types that have been requested. **Issued** - Generates a report of those SSL certificates that have been issued successfully. **Revoked** - Generates a report only for SSL certificates that have been revoked. **Expired** - Generates a report only for SSL certificate types that have expired and are due for renewal.
Date Selection	Drop-down list 	Enables the administrator to set a specific date parameter for the report. The parameters are Issued Date, Requested Date, Revoked Date and Expiration Date. The choices displayed on this drop-down menu is dependent on the status chosen in the 'Current Status' drop down. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated.

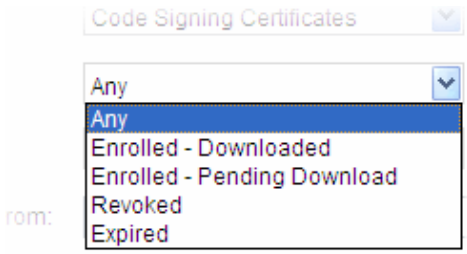
		If no dates are specified, the report will be generated for all the scans, regardless of the dates.
Organization/Department	Checkboxes	Enables the administrator to specify reports containing SSL certificates belonging to particular Organizations/Departments. If multiple Organizations/Departments are selected then the administrator will receive a single report that covers those selected Organizations/Departments. Each Organization will be displayed on a separate row in the 'Organizations' column and each Department will be displayed in a separate row in the 'Departments' column. Clicking on Expand All expands the tree structure to display all the Departments under each Organization. Clicking on Select All will generate a report for ALL Organizations that were assigned to that administrator. If NO Organization/Department is selected, the report will be generated for all the Organizations/Departments, delegated to the specific administrator.
Refresh	Control	Enables administrator to update the information in the form.
Run	Control	Starts the report generation.

7.7 Code Signing Certificates Report

The 'Code Signing Certificates' option enables the MRAO and RAO/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. The administrator is able to filter the reports by certificate status. The certificate statuses can be Any, Enrolled - Downloaded, Enrolled - Pending Download, Revoked and Expired. Reports can also be filtered by Organization, status specific dates and time interval. Once the 'Code Signing Certificates' type of reports is selected the following form appears:



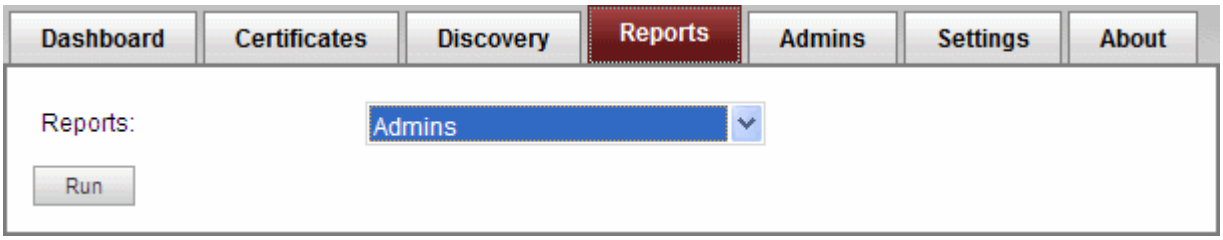
7.7.1 Report Type: Code Signing Certificates - Table of Parameters

Form Element	Control	Description
Current Status	Drop-down list  	Enables administrator to generate a report in .csv format for Client Certificates with a specific current status: **Any** - Generates a report for ALL code signing certificates regardless of their current status. Does not display any SSL certificates. **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 code signing certificates that have been successfully enrolled for by the end-user but have not yet been downloaded. **Revoked** - Generates a report for client certificates that

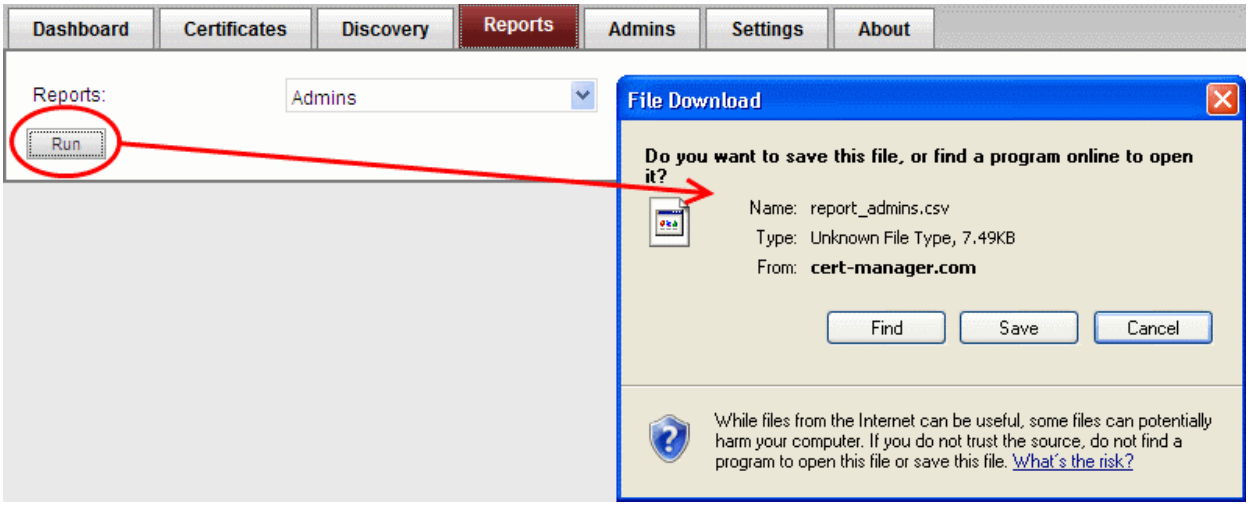
Form Element	Control	Description
		have been revoked. **Expired** - Generates a report only for client certificates that have expired and are due for renewal.
Date Selection	Drop-down list 	Enables administrator to set a specific date for collecting a report. It can be date of sending invitation by the administrator, certificate enrollment, date of certificate request, date of certificate issuance, download, date of certificate revocation or expiration. The choices displayed on this drop-down menu is dependent on the status chosen in the 'Current Status' drop down. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the scans, regardless of the dates.
Organization/Department	Checkboxes	Enables the administrator to generate reports for specific Organizations/Departments. If multiple Organizations/Departments are selected then the administrator will receive a single report that covers those selected Organizations/Departments. Each Organization will be displayed on a separate row in the 'Organizations' column and each Department will be displayed in a separate row in the 'Departments' column. Clicking on Expand All expands the tree structure to display all the Departments under each Organization. Clicking Select All will generate a report for ALL Organizations that were assigned to that administrator. If NO Organization/Department is selected, the report will be generated for all the Organizations/Departments, delegated to the specific administrator.
Refresh	Control	Enables the administrator to update the information in the form.
Run	Control	Starts the report generation.

7.8 Admins Report

The 'Admins' option enables the MRAO to generate and view reports providing details on all the enrolled administrators, their roles and the Organizations/Departments delegated to them. Once the 'Admins' type of reports is selected the following dialog appears:



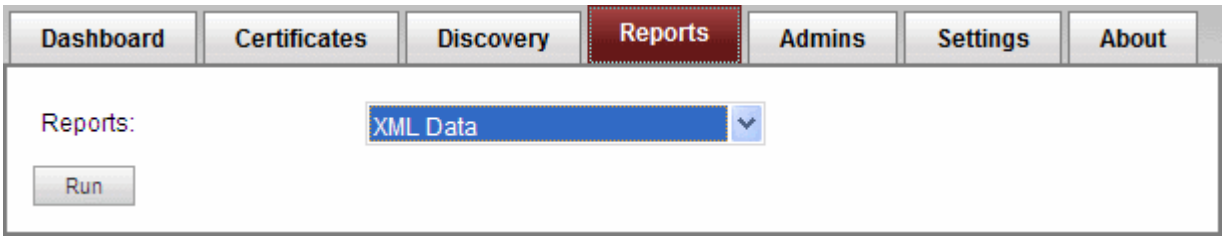
Clicking on 'Run' starts generating the report in .csv format.



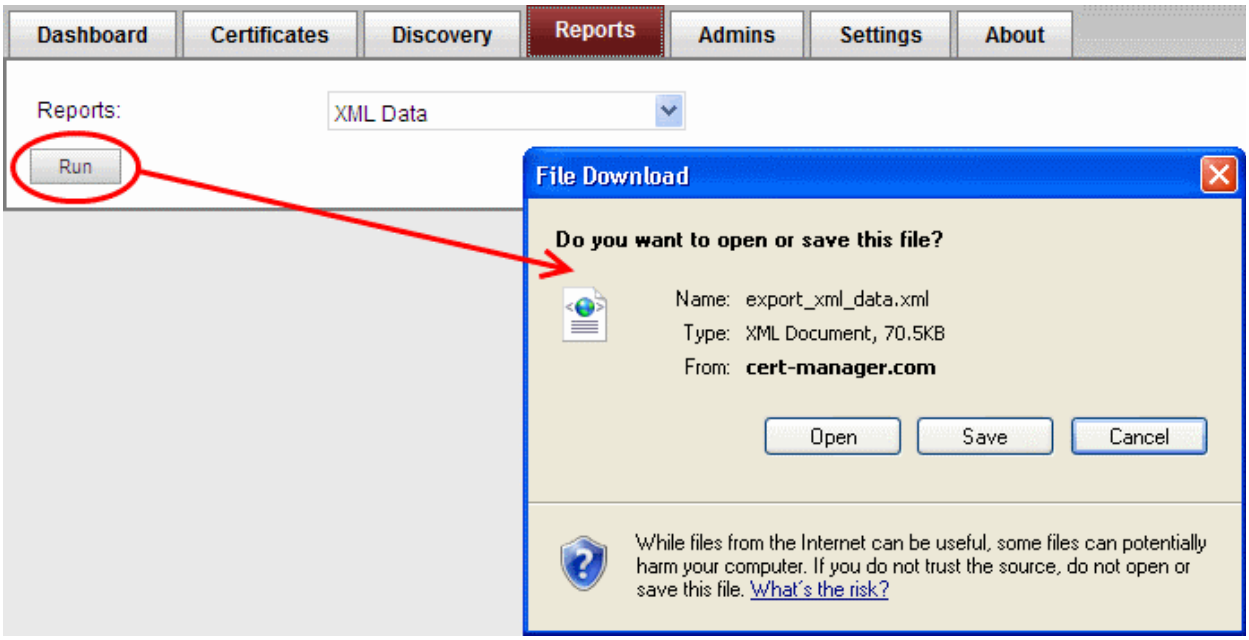
The report provides the details of the Name, Login, Email and Role of each of the administrators and the Organizations.

7.9 XML Data Report

The 'XML Data' option enables the MRAO to generate and view reports containing complete details of the Organizations, Departments, their administrators and the all the certificates in XML format. Once the 'XML Data' type of reports is selected the following dialog appears:



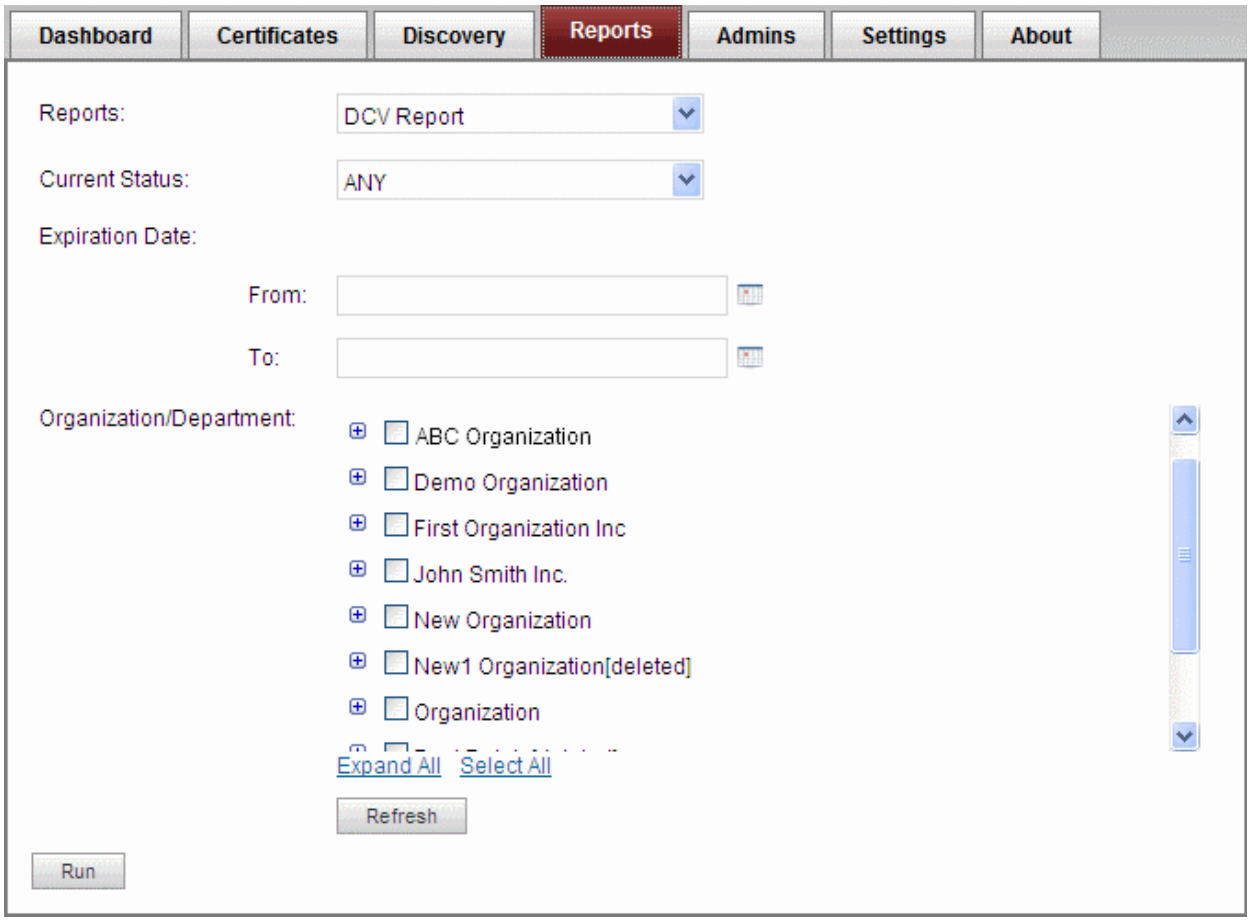
Clicking on 'Run' starts generating the report in .xml format.



The XML file enables the administrator to maintain a local database of all the details such as Departments, Administrators delegated, Certificates issued, Certificate settings etc. for each Organization. The XML file can also be imported into a database for collecting any data for any organization at any time by raising queries.

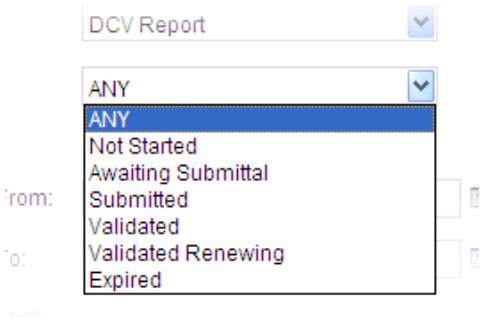
7.10 DCV Report

The 'DCV Report' option enables the MRAO and RAO/DRAO SSL administrators to generate and view reports that contain a list of all domains with their validation status and expiration of the DCV process. The administrator is able to filter the reports based on the DCV status. The DCV status can be Any, Awaiting Submittal, Submitted, Validated, Validated Renewing and Expired. Reports can also be filtered by Organization/Department, specific dates and time interval. Once the 'DCV Report' type of reports is selected the following form appears:



Note: DCV Report will be available only if DCV feature has been enabled for your account.

7.10.1 Report Type: DCV Report - Table of Parameters

Form Element	Control	Description
Current Status	Drop-down list 	Enables the administrator to generate a report of domains with a specific current DCV status **Any** - Generates a report for Domains regardless of their current status. **Not Started** - Generates a report on domains that have been added to CCM but have not yet started the DCV process. **Awaiting Submittal** - Generates a report only for Domains that are being waiting for submission of DCV request to the Domain administrator. **Submitted** - Generates a report only for Domains for which DCV request has been submitted. **Validated** - Generates a report on domains that have been successfully validated. **Validated Renewing** - Generates a report only for Domains that require renewal of Validation. **Expired** - Generates a report only for Domains for which the DCV request has expired.
Expiration Date		Enables the administrator to set an expiration date range for DCV request to generate a report on Domains whose DCV request is expiring within the date range. Clicking on the calendar buttons beside From: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all Domain Control Validated domains, regardless of the dates.
Organization/Department	Checkboxes	Enables the administrator to select Organizations/Departments to generate report on Domains of specific Organizations/Departments. If multiple Organizations/Departments are selected then the administrator will receive a single report that covers those selected Organizations / Departments. Each Organization will be displayed on a separate row in the 'Organizations' column and each Department will be displayed in a separate row in the 'Departments' column. Clicking on Expand All expands the tree structure to display all the Departments under each Organization. Clicking on Select All will generate a report for ALL Organizations that were assigned to that administrator. If NO Organization/Department is selected, the report will be generated for all the Organizations/Departments, delegated to the specific administrator.
Refresh	Control	Enables administrator to update the information in the form.
Run	Control	Starts the report generation.

7.11 Notification Log Statistics Report

The 'Notification Log Statistics Report' option enables the MRAO administrator to generate and view log reports on the notification emails sent to other RAO and DRAO administrators for various events, as configured in the **Settings > Notifications** area.

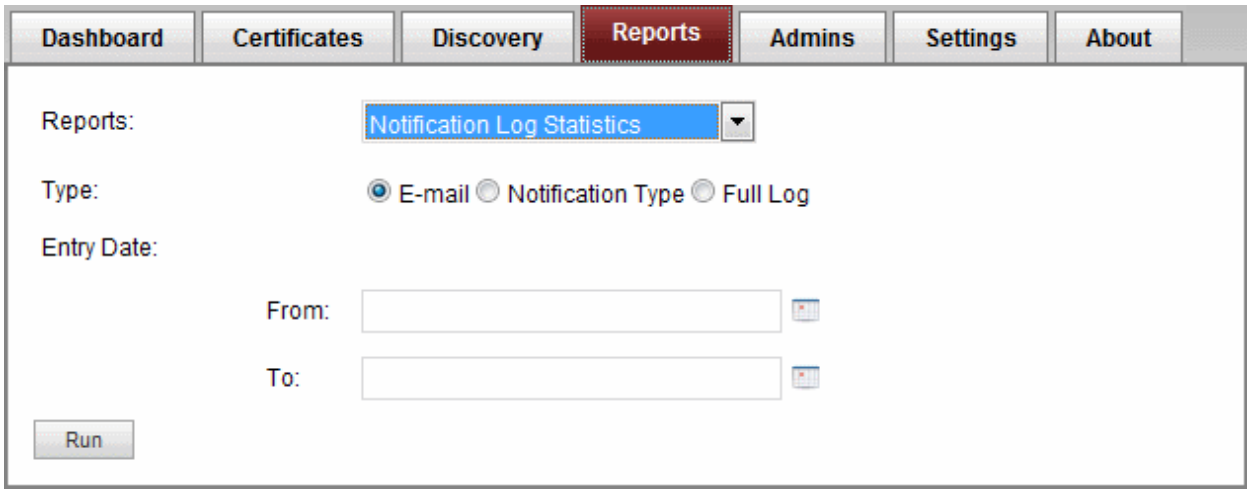
The administrator is able to select any one of the following three types of the Notification Log Statistics Reports:

- **E-Mail**
- **Notification Type**
- **Full Log**

7.11.1 Notification Log Statistics - Email

The Email log report can be generated for a specified time period. The .csv format report generated will show the number of notification emails sent to each RAO and DRAO administrator during the specified period.

On selecting the Email type, the following form appears.



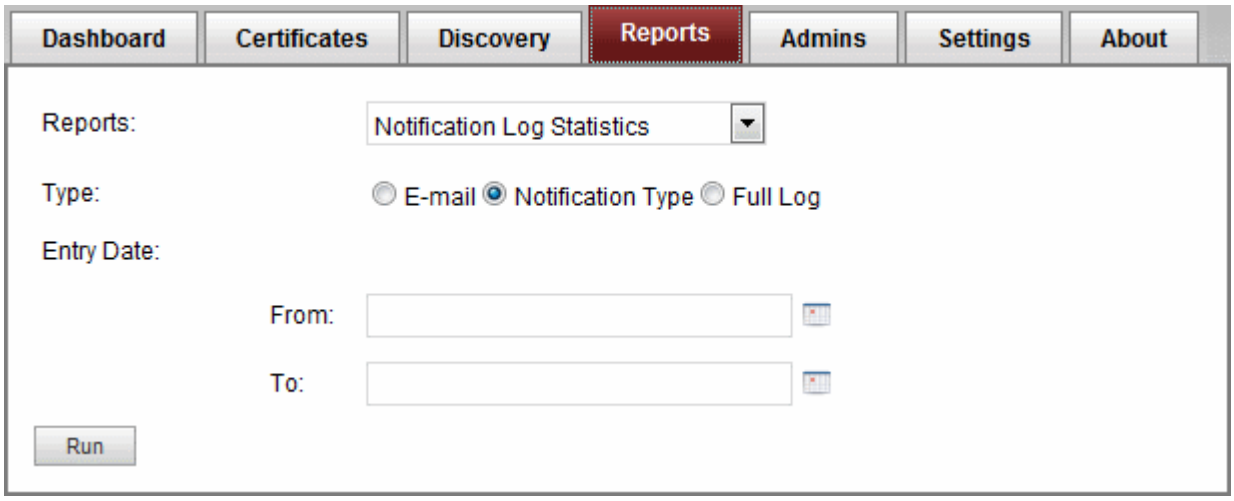
7.11.1.1 Report Type: Notification Log Statistics :Emails - Table of Parameters

Form Element	Control	Description
Type	Radio buttons	Enables administrators to choose between email report, notification type report or a full log report.
Entry Date	Calendar buttons	Enables the administrator to generate a report in .csv format for the notification emails sent within a specified time period. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the notification emails, regardless of the dates.
Run	Control	Starts the report generation

7.11.2 Notification Log Statistics - Notification Type

The Notification type log report can be generated for a specified time period. The .csv format report generated will show the number of notification emails sent for each notification type as configured in **Settings > Notifications** area to all the RAO and DRAO administrators during the specified period.

On selecting 'Notification Type', the following form appears.



7.11.2.1 Report Type: Notification Log Statistics :Notification Type - Table of Parameters

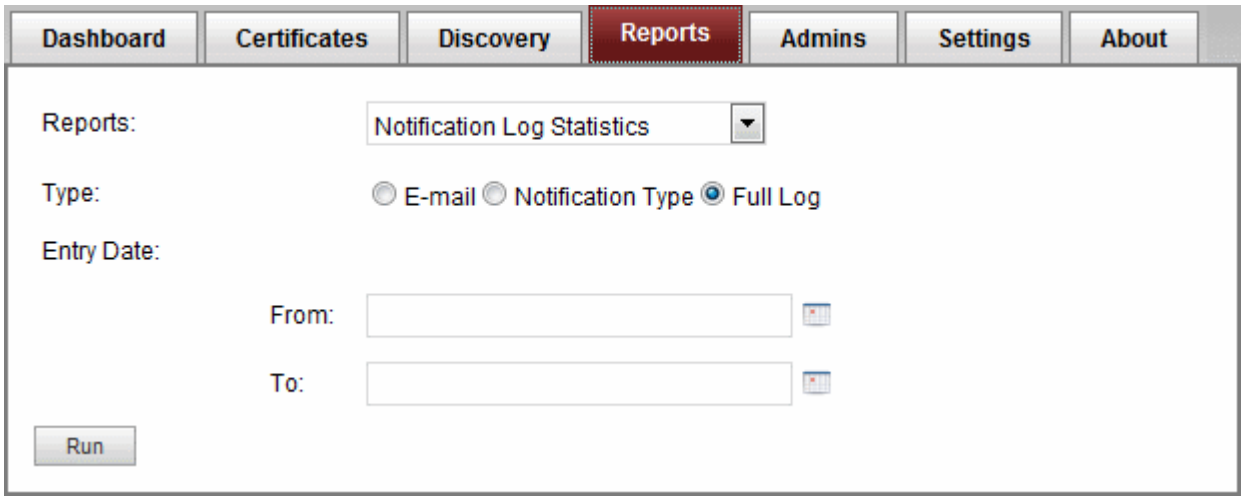
Form Element	Control	Description
Type	Radio buttons	Enables administrators to choose between email report, notification type report or a full log report.
Entry Date	Calendar buttons	Enables the administrator to generate a report in .csv format for the number of emails sent for different notification types within a specified time period. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the notifications, regardless of the dates.
Run	Control	Starts the report generation

7.11.3 Notification Log Statistics - Full Log

The full log report for notification emails can be generated for a specified time period. The report generated will show the list of emails sent for various notification types to different RAO and DRAO administrators, for each notification type as configured in **Settings > Notifications** area during the specified period. The report generated in .csv format will contain 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 at which the email as sent

On selecting the 'Full Log' type, the following form appears.



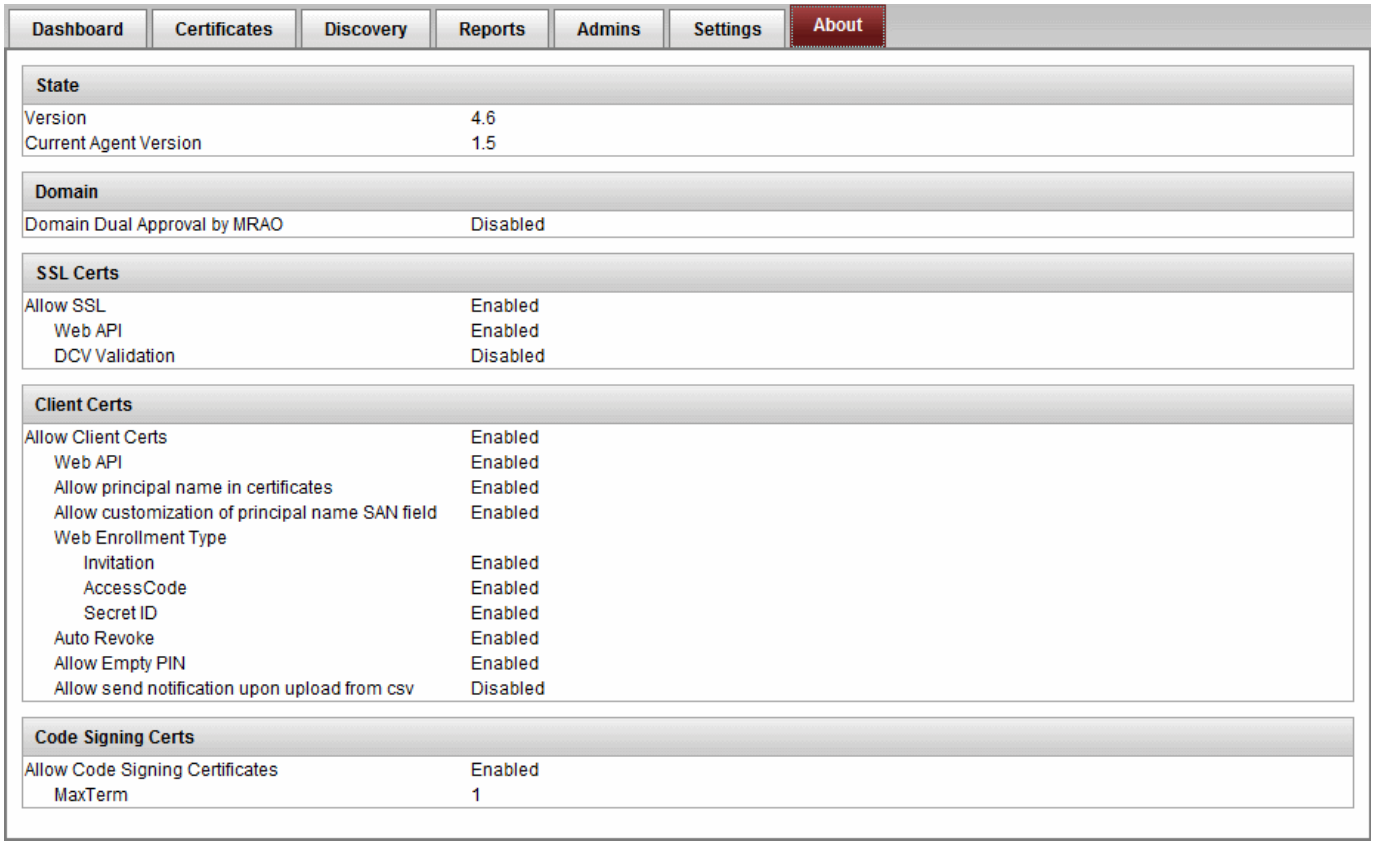
7.11.3.1 Report Type: Notification Log Statistics :Full Log - Table of Parameters

Form Element	Control	Description
Type	Radio buttons	Enables administrators to choose between email report, notification type report or a full log report.
Entry Date	Calendar buttons	Enables the administrator to generate a report in .csv format for the full log of notification emails within a specified time period. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the notifications, regardless of the dates.
Run	Control	Starts the report generation

8 Version and Feature Information

The 'About' tab enables the administrator to view the CCM version and the features that are enabled for the subscription.

- MRAO - can see a list of all the features.
- RAO - can only see a list of features related to SSL, Client Certificate and/or Code Signing Certificate according to their administrative role.
- DRAO - can only see a list of features related to SSL, Client Certificate and/or Code Signing Certificate according to their administrative role.

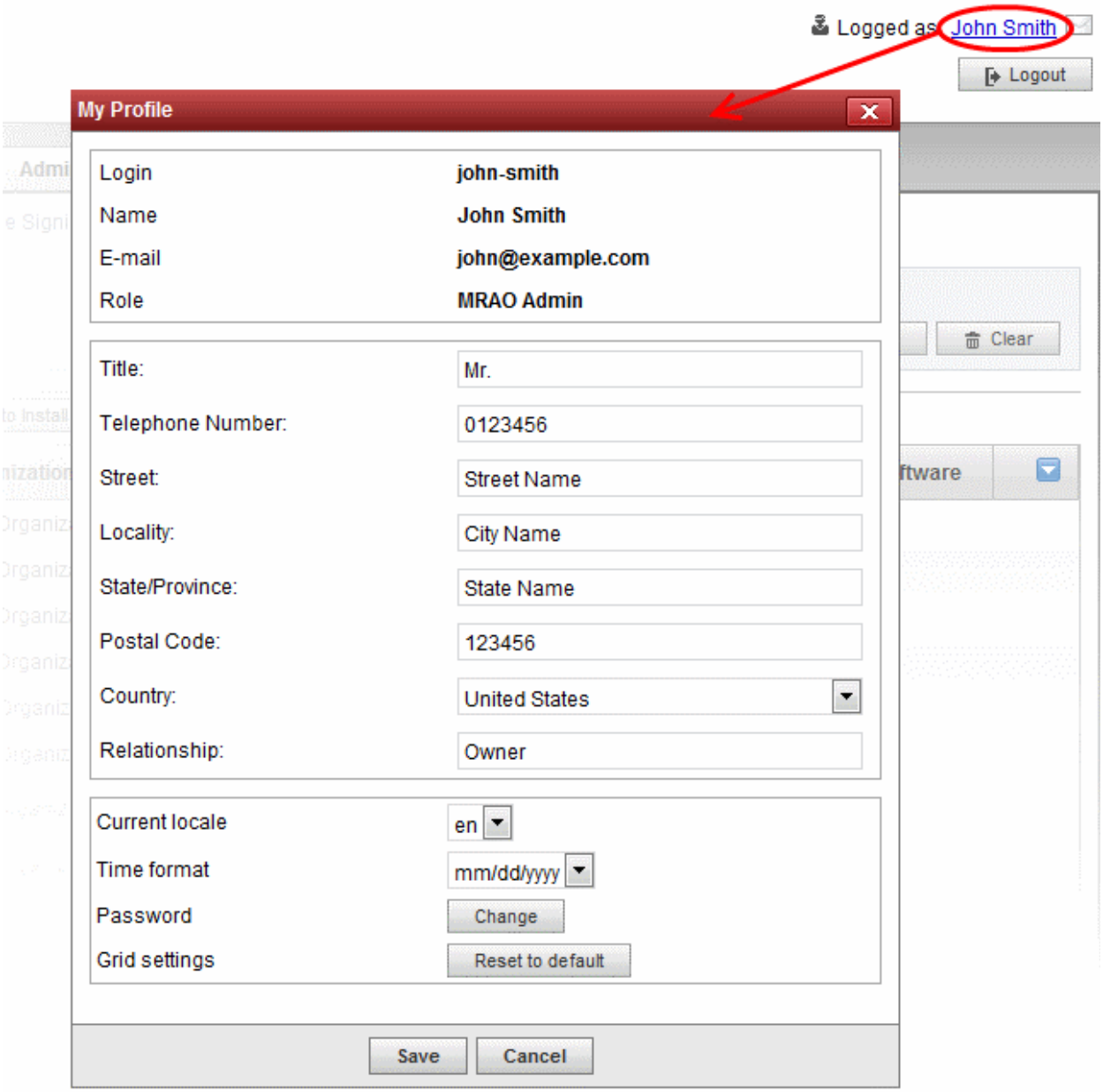


If any of the features are to be enabled or disabled, the MRAO Administrator can contact Comodo and request for them.

9 My Profile

The 'My Profile' area contains a details summary for the Administrator that is currently logged into the system. Administrators can view their login name, their full name, the email address that is associated with their account and their administrative role. The administrator can also view and edit the address details, and preferences.

To access this interface, click the username text link beside the 'Logged as' label at the top right side of the interface.



This area also allows the the Administrator to edit the following details:

Address Details:

- Title
- Telephone Number
- Street
- Locality
- State/ Province
- Postal Code
- Country
- Relationship

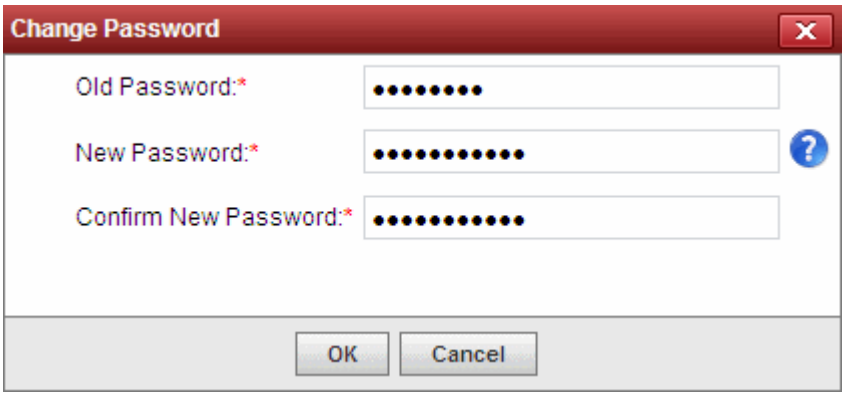
Preferences:

- Interface Language - CCM interface is available in multiple languages. The 'Current locale' drop-down menu enables the administrators to change the interface language according to their preferences. The settings will take effect only on clicking the 'Save' button.

- Time Format - Choices available are 'mm/dd/yyyy' or 'dd/mm/yyyy'.

Note: This only affects the way dates are represented in the CCM interface (for example, the 'Expires' column of the 'SSL Certificates sub-tab' in 'Certificates Management'. It does not affect the way that dates are displayed in the certificates themselves (this is not modifiable and is set in the format 'MM/dd/yy'). The settings will take effect only on clicking the 'Save' button.

- Password - To change the administrators password, click the 'Change' button next to 'Password' label.

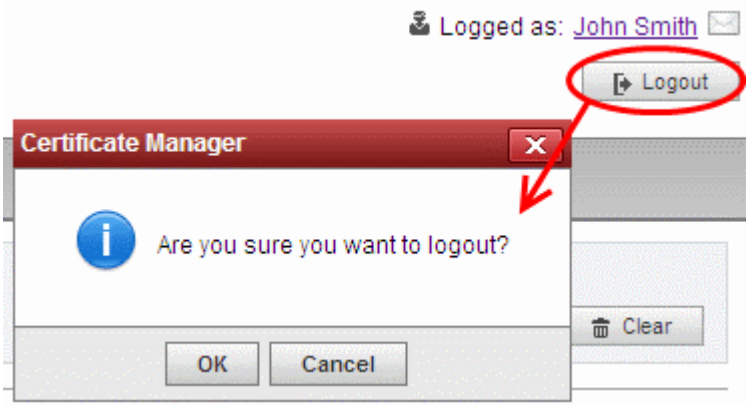


Hover the mouse cursor on the help button to view the password policy and change the password accordingly.

- Grid Settings - Click Reset to default to adjust the column widths and sorting preferences customized in various interfaces of CCM to default values.

10 Logging Out of Comodo Certificate Manager

Administrator can log out from the interface by clicking on the 'Logout' button located at the top right side of the interface.



Appendix 1 - Your responsibilities when 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. It is your responsibility to ensure 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 the contract you signed with Comodo and your Certificate Manager Account and could be a breach of the Certificate Manager Subscriber Agreement.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road,

Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

Email: **EnterpriseSolutions@Comodo.com**

For additional information on Comodo - visit **http://www.comodo.com/**