InCommon®

InCommon Certificate Manager

Version 6.1

RAO Administrator Guide

Release Date: January 17th, 2018

InCommon
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor MI, 48104

Table of Contents

1 Introduction to InCommon Certificate Manager

InCommon Certificate Manager (CM) centralizes and streamlines the life-cycle management of web server, S/MIME and code signing certificates through a unified interface. The system features full integration with InCommon 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, CM 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 Incommon CM service.

- Section 1, Introduction to Incommon 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 an 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, Code Signing on Demand - Contains an overview of the area's main functionality and detailed explanations on how to enroll developers, issue code signing certificates for them and code signing executables and script files without the need for developer downloading their certificate. The feature is available only is enabled for your account. Contact your Master Administrator or Incommon Account manager if you wish to enable this feature for you.
- Section 5, Admin Management - Covers the creation and management of Certificate Service Manager administrators and the assigning of privileges and responsibilities to those administrators.
- Section 6, Settings - Contains overviews and tutorials pertaining to the functional areas housed under the 'Settings' tab, including guidance on how to edit an organization, manage organizations, add domains and associate them with an organization or department, set up Notifications, manage Encryption settings, and managing Assignment rules for auto-assignment of unmanaged certificates to required organizations and departments. Incommon CM Agents explains how to configure agents for certificate discovery and auto-installation. To view detailed information about each area, click on the links below:
  - Organizations
  - Departments
  - Domains
  - Encryption and Key Escrow
  - Notifications
  - Assignment Rules
  - InCommon CM Agents

- Section 7, Certificate Discovery and Agents - explains how to scan and monitor a network for all installed SSL certificates including certificates that may or may not have been issued using Incommon CM, 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 8, 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 9, Version and Feature information - explains how to view the version of Incommon CM and the features enabled for the subscription.
- Section 10, My Profile - explains how to changes the time format and the password.
- Section 11, Logging out of Incommon Certificate Manager explains the process for logging out.

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 Incommon 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 Department Registration Authority Officer (DRAO).

Once an organization or department has been created:

- Appropriately privileged administrators can request and delegate domains to that organization/department
- Appropriately privileged administrators 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

Incommon 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 2 classes of Administrator in InCommon Certificate Manager:

- **Registration Authority Officer (RAO)** - A role created by a Master Administrator to manage the certificates and end-users of specific Incommon CM organizations.
- RAOs have control over certificates that are ordered on behalf of their organization(s). They also have control over domains and users that have been delegated to their organization/dept.
- RAOs can create peer RAOs for their organizations. They can edit or remove RAOs of their organization if appropriate privileges have been assigned to them by a Master Administrator.
- **Department Registration Authority Officer (DRAO)** - Department Registration Authority Officers are created by, and subordinate to, the RAO class of administrator.
- DRAOs are assigned control over certificates, users and domains belonging to departments of organizations.
- DRAOs can create peer DRAOs for their departments. They can edit or remove DRAOs of their department if appropriate privileges have been assigned to them by an MRAO or RAO.

RAO and DRAO administrators are sub-divided into specific roles by certificate type:

- RAO SSL administrators
- RAO S/MIME administrators
- RAO Code Signing administrators
- DRAO SSL administrators
- DRAO S/MIME administrators
- DRAO Code Signing administrators

The privileges of any particular CM administrator are, therefore, 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)

CM 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.

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 for organizations that have delegated to them. They can approve or

Security Role / Type of Administrator	Definition
	decline requests for SSL certificates that have been made using the Self-Enrollment form for their organization(s) and sub-ordinate department(s). • RAO SSL admins can upload private keys of SSL certificates belonging to their organizations and their sub-ordinate departments for management by Private Key Store, configured in the local network. They can also download the private keys of the certificates. • 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. • RAO SSL admins cannot create new organizations. Neither can they edit the General settings of any organization - even those 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 the Master Administrator 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 have been delegated to them. • 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

Security Role / Type of Administrator	Definition
	with 'Allow DCV' privileges can be created only by the Master Administrator. • 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 Httpd, Apache Tomcat and IIS web servers. • RAO SSL Admins can view the network assets like certificates installed on various servers and endpoints and web servers with websites/domains hosted on them, as identified by manual or scheduled discovery scans configured for the networks belonging to their organizations (and their sub-ordinate departments). • RAO SSL Admins can assign unmanaged SSL certificates identified by discovery scans to their organizations and departments, in order to bring them under management through Incommon CM. • RAO SSL admins can view the SSL certificates Reports and Discovery Scan Log Reports for the Organization that they were assigned rights to. • RAO SSL admins cannot access or manage 'Settings' > 'Encryption' as this can only be managed by those with 'RAO S/MIME' role. • RAO SSL admins can view Activity Logs only for their organization(s). An 'at-a-glance' summary of Administrator security roles and access rights is available here.
RAO S/MIME ***(Registration Authority Officer - S/MIME Certificates)***	Administrators with the security role 'RAO S/MIME' have privileges to access, manage, request and approve the requests of Client Certificates for domains that have been delegated to their organization • RAO S/MIME admins have visibility and control over client certificates which belong to organizations that they control. • They have no permissions over the client certificates of organizations which they do not control. • RAO S/MIME admins can only manage S/MIME 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 S/MIME Administrator. • RAO S/MIME admins will see only those organizations that have been delegated to them in the 'Organizations' area. • RAO S/MIME admins cannot create new organizations. Neither can they edit the General settings of any organization - even those organizations of which they are S/MIME administrator. • RAOs can request the Master Administrator to add client

Security Role / Type of Administrator	Definition
	certificates with specific capabilities to their account. If the certificates are not available on the account then the Master Administrator can make a request to Incommon to get them added. • For example, 'Signing Only', 'Encryption Only', 'Dual Use' (Signing + Encryption), 'Smart Card Logon and Authentication' and more. • It is also possible to create custom client certificate types with combinations of capabilities. • RAOs can also restrict issuance of specific types of client certificates to end-users in their organization. • RAO S/MIME administrators can create departments only within organizations that have been delegated to them • RAO S/MIME admins cannot approve or request the creation of administrators that have more privileges than themselves. They can: • Request the creation of fellow RAO S/MIME admins only for organizations that have been delegated to them if the Master Administrator has enabled this feature for them • Request and approve the creation of DRAO S/MIME 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 S/MIME admins admins can delegate domains to sub-ordinate departments of organizations that have been delegated to them. • When creating a new department, an RAO S/MIME admin can: • Enable or disable the ability of RAO S/MIME admins (themselves) to recover the private keys of client certificates that belong to this department • Enable or disable the ability of DRAO S/MIME admins to recover the private keys of client certificates that belong to this department • All or any combination of the above • RAO S/MIME 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, S/MIME certificates - including those SSL/S/MIME certificates belonging to the organization of which they are Code Signing Certificate Administrator. • 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 Signing 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 organization that have been delegated to them if the Master Administrator 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 cannot access or manage 'Settings' > 'Encryption' as this can only be managed by those with 'RAO S/MIME' role. • RAO Code Signing admins can delegate domains to sub-ordinate

Security Role / Type of Administrator	Definition
	departments of organizations that have been delegated to them. • RAO Code Signing admins can create developers for Code Signing on Demand (CSoD) service and approve code signing requests generated by developers only for the organization(s) (and their sub-ordinate departments) that are delegated to them. (Applicable only if CSoD service is enabled for your account). • 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 • 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 S/MIME' , 'DRAO SSL' AND/OR '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

Security Role / Type of Administrator	Definition
	• 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) they administrate if they were given 'Allow DCV' privileges. • DRAO SSL admin with such privileges can be created only by Master Administrator 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 the network assets like certificates installed on various servers and endpoints and web servers with websites/domains hosted from them, as identified by manual or scheduled discovery scans run on networks belonging to their department. • DRAO SSL Admins can assign unmanaged SSL certificates identified from discovery scans to their department, to bring them under management through Incommon CM. • 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 'Settings' > 'Encryption' as this can only be managed by those with 'DRAO S/MIME' role. • DRAO SSL admins cannot view Activity Logs. • An 'at-a-glance' summary of Administrator security roles and access rights is available here.
DRAO S/MIME ***(Department Registration Authority Officer - S/MIME Certificates)***	Administrators with the security role 'DRAO S/MIME' have privileges to access, manage and request Client Certificates for domains that have been delegated to their department by an RAO • DRAO S/MIME admins have visibility over the client certificates belonging to End-Users of the department(s) which have been delegated to them.

Security Role / Type of Administrator	Definition
	- DRAOs cannot manage client certificates of end-users that do not belong to their department(s). - DRAOs will only see their own departments(s) listed in the 'Departments' area. The 'Organizations' area is not visible to DRAOs. - A DRAO S/MIME admin can only request S/MIME certificates for domains that have been delegated to their department. - DRAO S/MIME 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 S/MIME. - It is possible for an RAO to make the same individual a 'DRAO S/MIME' , 'DRAO SSL', and a 'DRAO Code Signing' for the same department during the Admin creation or editing process (See Admin Management, for more details). - DRAO S/MIME admins cannot request the creation of administrators that have more privileges than themselves. They can: - Request the creation of fellow DRAO S/MIME 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 S/MIME 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 S/MIME admin can recover the private keys of client certificates belonging to their Department. - 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 S/MIME 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 an organization that have been delegated to them by an RAO. - DRAO Code Signing admins have visibility of and can request Code Signing certificates for the department(s) that have been

Security Role / Type of Administrator	Definition
	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 S/MIME' , 'DRAO SSL', and a 'DRAO Code Signing' for the same 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 admins cannot access or manage 'Settings' > 'Encryption' as this can only be managed by those with 'DRAO S/MIME' role. • DRAO Code Signing admins can create developers for Code Signing on Demand (CSoD) service and approve code signing requests generated by developers only for the department(s) that are delegated to them. (Applicable only if CSoD service is enabled for your account)

Security Role / Type of Administrator	Definition
	• 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 Incommon CM 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 Incommon CM interface. They exist in Incommon CM 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 Incommon CM via: • Manually Adding End-Users; • The End-User ordering a Client Certificate using the Self Enrollment Form; • End-User is imported into Incommon CM 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 Incommon 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' section of IncommonCM interface.
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 Incommon CM as either End-Users or Administrators if they applied using use the self-enrollment/external application forms

Security Role / Type of Administrator	Definition
	Applicable only if 'Code Signing on Demand' feature is enabled for your account. A developer is the person that can use the 'Code Signing on Demand' service to sign the executables and script files. Incommon CM can store the code-signing certificate issued to them and use it for signing code files uploaded by the developer. The developer can then download the signed file from Incommon CM. • A new user can be added as a developer as a new user or an existing end-user can be assigned the 'Developer' role

1.2.4 Security Roles - Comparative Table

Administrator Management					
Action	Controls	RAO		DRAO	
Configure other Administrators	Add, View Delete, Edit	Create DRAOs of Subordinate Departments who are responsible for same Certificate Type Create RAOs of Delegated Organization who are responsible for same Certificate Type		Create DRAOs of Delegated Department who are responsible for the same certificate type if enabled by a RAO administrator or Master Administrator	
Approve/Reject Administrator Creation Requests	Approve, Reject	DRAOs of Subordinate Departments who are responsible for same Certificate Type		✗	
Activate/Deactivate Administrators	Check box	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	RAO		DRAO	
Directly submit Certificate Requests using the built-in application form	Add, Renew, Replace	Delegated Organizations Subordinate Departments Only those Certificate Types for which RAO is responsible		Delegated Departments Only those Certificate Types for which DRAO is responsible	
Directly submit Certificate Requests to the issuing Certificate Authority for Auto-Installation by	Add, Renew, Approve, Decline, Install	Delegated Organizations Subordinate Departments		Delegated Departments	
		RAO SSL	✓	RAO SSL	✓
		RAO S/MIME	✗	RAO S/MIME	✗

InCommon CM (IIS, Apache and Apache Tomcat only)		RAO Code Signing	✗	RAO Code Signing	✗
Approve/Decline Certificate Requests that have been made using the 3.1.2.3.1.Method 1 - Self Enrollment Form	Approve, Decline	Delegated Organizations Subordinate Departments Only those Certificate Types for which RAO is responsible		Delegated Departments Only those Certificate Types for which DRAO is responsible	
Download the Private Key of an SSL certificate Upload the Private Key of an SSL certificate		Delegated Organizations Subordinate Departments		Delegated Departments	
		RAO SSL	✓	DRAO SSL	✓
		RAO S/MIME	✗	DRAO S/MIME	✗
		RAO Code Signing	✗	DRAO Code Signing	✗
Manage Certificates	View, Edit, Revoke	Delegated Organizations Subordinate Departments Only those SSL certificates for which RAO is responsible		Delegated Department Only those SSL certificates for which DRAO is responsible	
Certificate Discovery	Add CIDR, Delete CIDR, Setup Certificate Discovery (CD) agent for internal scanning	RAO SSL	✓	DRAO SSL	✓
		RAO S/MIME	✗	DRAO S/MIME	✗
		RAO Code Signing	✗	DRAO Code Signing	✗
Request New Domains for...	Add	Delegated Organizations Subordinate Departments		Delegated Departments	
Approve / Reject New Domain Requests	Approve, Reject	✓ Subordinate Departments		✗	
Delegate Existing Domains to...	Delegate	Subordinate Departments RAOs can only delegate domains to the Departments belonging to the Organization that have been delegated to them but cannot re-delegate to remove a domain's delegation.		✗	
Activate/Deactivate Existing Domains	Check box	✗		✗	

Initiate DCV	Select method of DCV as applicable to the domain	RAO SSL	On Domains added to Delegated Organizations and Subordinate Departments	DRAO SSL	On Domains added to Delegated Department
		RAO S/MIME	✗	DRAO S/MIME	✗
		RAO Code Signing	✗	DRAO Code Signing	✗

Department Management

Action	Controls	RAO	DRAO
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	RAO S/MIME	DRAO S/MIME
Manage Encryption of client certificates	Initialize, Re-encrypt	Delegated Organizations Subordinate Departments	Delegated Departments
Recover private keys from escrow	Decrypt	Delegated Organizations Subordinate Departments	Delegated Departments
Can permit Administrators other than themselves to recover keys for a particular Organization or Department	Allow key recovery by.... *(checkbox)*	RAO S/MIME Admins DRAO S/MIME Admins	✗

Note: Escrow privileges are configured at the point of organization / department creation.

If granted escrow privileges , the RAO S/MIME 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 RAO S/MIME admin (themselves) should have the ability to recover the private keys of client certificates of that belonging to that department
2. Whether or not the DRAO S/MIME 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	RAO Administrator	DRAO Administrator

Configure access control settings	Add, Delete, Edit CIDR	✓	✓
View Notifications for...	Add, Delete, Edit	Delegated Organizations Subordinate Departments	Delegated Department
Create Notifications for...	Add, Delete, Edit	Delegated Organizations Subordinate Departments	Delegated Department
View Reports for...	See 'Reports - Security Role Access Table' section for details.	Delegated Organizations Subordinate Departments	Delegated Department
Modify Email Templates for..	Edit	Delegated Organizations Subordinate Departments	Delegated Department

1.2.5 Multiple Security Roles

Multiple security roles may be selected for any particular administrator. A RAO that has been granted administrative rights over multiple certificate types for a particular organization can assign similar, multi-role, privileges to a sub-ordinate DRAO administrator for a particular department.

1.2.6 Organizations and Departments

- Creating an organization and delegating domains to it is an important step towards the issuance and management of SSL, code signing an client certificates in Certificate Manager.
- Organizations and departments are created by administrators for the purpose of requesting, issuing and managing certificates for domains and employees. (See '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).

Once an Organization has been created:

- RAO administrators can create multiple departments within an organization (See 'Organizations / Section Overview ' for more details).
- RAO and DRAO administrators can directly request that certificates be issued to domains that have been delegated to their organization(s) and/or department. They can also approve/decline certificate requests from individuals that have applied using one of the external application forms.
- 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.

- 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 can be viewed and exported for that organization and/or specific department

1.2.7 Reports

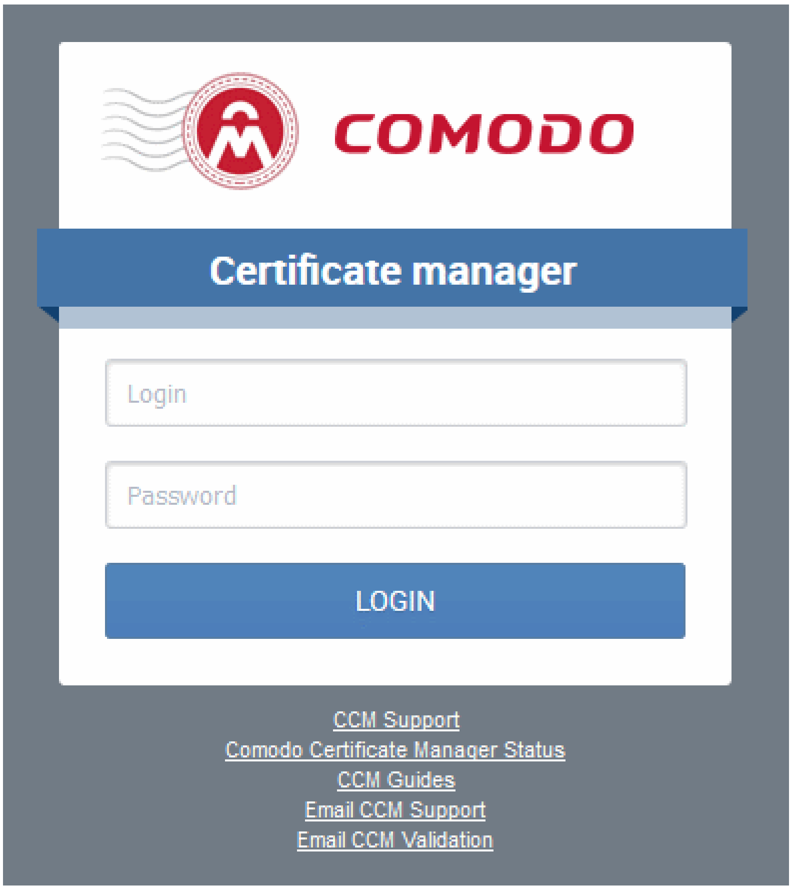
Certificate reports can be viewed and exported for an organization and/or department via the Report section. An appropriately privileged administrator is enabled to view different types of reports according their security roles. The following types of reports are available:

Type of Report	Description
SSL Certificates	Enables the administrator to monitor all statistics related to SSL certificates including usage, ownership, issuance, provisioning and status.
Client Certificates	Enables the administrator to monitor all statistics, related to client certificates including usage, ownership, issuance, provisioning and status.
Code Signing Certificates	Enables RAO/DRAO Code Signing administrators to monitor all statistics, related to code signing certificates including usage, ownership, issuance, provisioning and status.
Code Signing Requests	Enables the RAO/DRAO Code Signing administrators to view reports containing the Code Signing on Demand (CSoD) requests and their activities.
Discovery Scan Log	Enables the administrator to view the Discovery Scan Log. A Discovery Scan is an audit of all SSL certificates installed on your network.
DCV Report	Enables RAO/DRAO SSL administrators to generate a report containing details on all of their registered domains, with their DCV status and expiration dates.
Discovery Tasks	Enables RAO/DRAO SSL Administrators to generate reports on configured Discovery tasks. Reports are delivered in .csv format.

See 'Report', for detailed information.

1.3 Log into Your Account

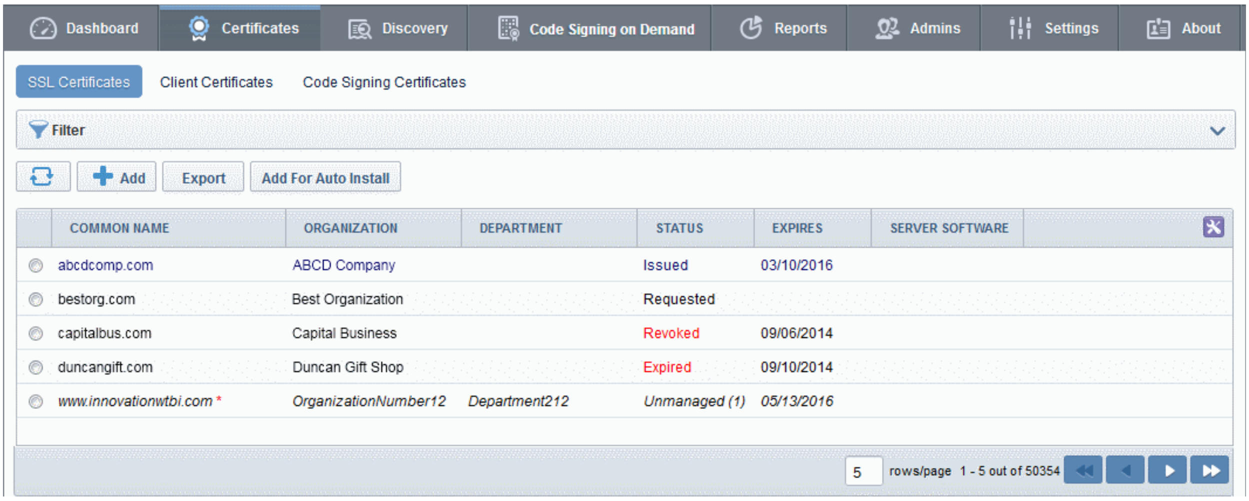
Once your organization has subscribed for an Comodo Certificate Manager account, Comodo will provide your account manager with a username, password and login URL for the Certificate Manager interface. By default, the format of this URL is: https://cert-manager.Comodo.com/customer/[REAL CUSTOMER URI].



- Please contact your Comodo account manager if you have not been supplied with your login details,
- If you are not able to login with your login details, you can raise a support ticket at the Comodo Support portal by clicking 'Incommon CM Support'. You can create an account for free and submit your ticket to get your login problems resolved.
- You may be prompted to change your password after first login if set by your administrator in access control settings.
- You may also change your password at any time in the 'My Profile' area.

1.4 The Main Interface - Summary of Areas

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

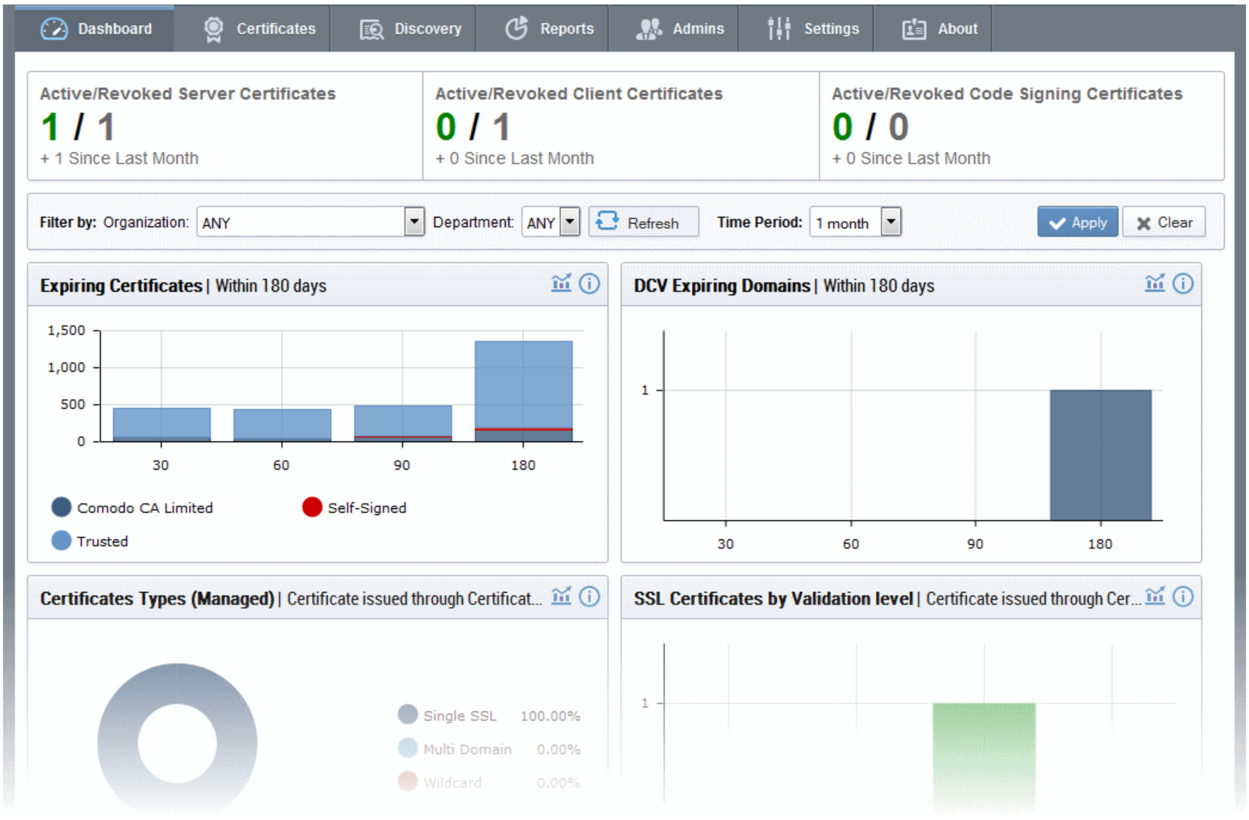


	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	SERVER SOFTWARE
○	abcdcomp.com	ABCD Company		Issued	03/10/2016	
○	bestorg.com	Best Organization		Requested		
○	capitalbus.com	Capital Business		Revoked	09/06/2014	
○	duncangift.com	Duncan Gift Shop		Expired	09/10/2014	
○	*www.innovationwtbi.com* *	*OrganizationNumber12*	*Department212*	*Unmanaged (1)*	*05/13/2016*	

5 rows/page 1 - 5 out of 50354

- There are (a maximum of) eight tabs that cover each of the main functional areas of the application. These are 'Dashboard', 'Certificates', 'Discovery', 'Code Signing on Demand', 'Reports', 'Admins', 'Settings' and 'About'.
- The 'Certificates' tab contains sub-sections for managing the certificate types that have been enabled for your company. There are a maximum of four certificate sections - 'SSL Certificates', 'Client Certificates', and 'Code Signing Certificates'.
- The 'Discovery' tab allows you to setup scans to discover existing certificates on your network. The sub-sections are Network Assets and Net Discovery Tasks. and.
- The 'Code Signing on Demand' tab is displayed only if the Code Signing on Demand (CSoD) feature is enabled for your account. The tab contains sub-sections for adding and managing developers and handling code signing requests from the developers. The sub-sections are Requests and Developers.
- The 'Settings' tab contains sub-sections for 'Organizations', 'Domains', 'Notifications' , 'Encryption', Agents and Assignment Rules.
- The remainder of this section contains a brief overview of each tab and the security role requirements for access to that area.

Dashboard: Contains graphs and charts about the certificates on your network, such as certificates approaching expiry, certificates issued/requested, DCV status, breakdown of certificates by types, issuers, and more.



Active/Revoked Server Certificates

1 / 1

+ 1 Since Last Month

Active/Revoked Client Certificates

0 / 1

+ 0 Since Last Month

Active/Revoked Code Signing Certificates

0 / 0

+ 0 Since Last Month

Filter by: Organization: ANY Department: ANY Refresh Time Period: 1 month Apply Clear

Expiring Certificates | Within 180 days

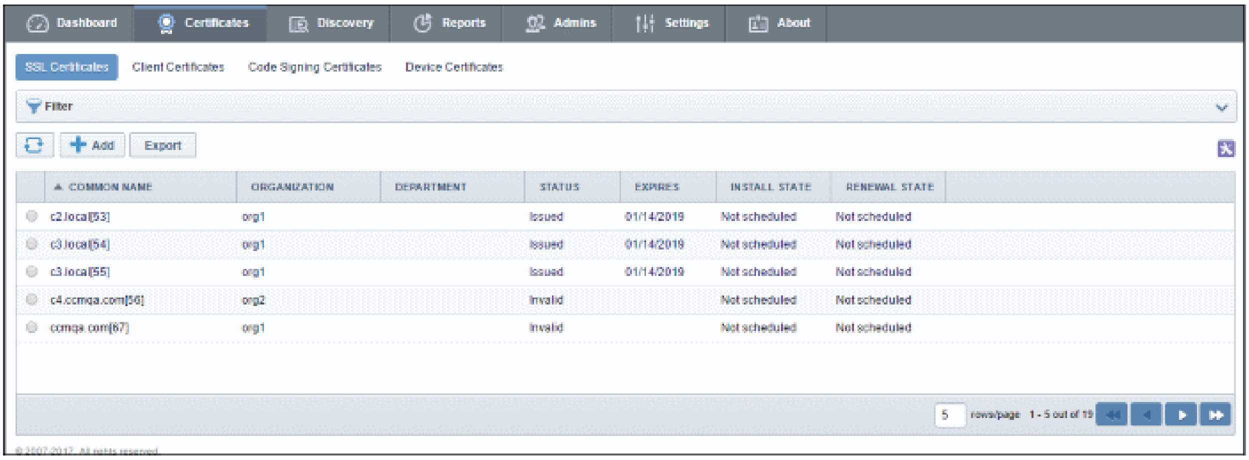
DCV Expiring Domains | Within 180 days

Certificates Types (Managed) | Certificate issued through Certificat...

SSL Certificates by Validation level | Certificate issued through Cer...

[Click here for more information about the Dashboard.]

[Certificates Management] Contains up to four sub-sections which allow you to manage SSL, client and code signing.



	▲ COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
○	c2.local[53]	org1		Issued	01/14/2019	Not scheduled	Not scheduled
○	c3.local[54]	org1		Issued	01/14/2019	Not scheduled	Not scheduled
○	c3.local[55]	org1		Issued	01/14/2019	Not scheduled	Not scheduled
○	c4.ccmqa.com[56]	org2		Invalid		Not scheduled	Not scheduled
○	ccmqa.com[67]	org1		Invalid		Not scheduled	Not scheduled

5 rows/page 1 - 5 out of 15

© 2007-2017. All rights reserved.

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

Security Role / Type of Administrator	Available Action
RAO SSL	Can access all areas and functionality of the SSL Certificates section; has visibility and control over SSL Certificates belonging to their delegated organization(s).

Security Role / Type of Administrator	Available Action
RAO S/MIME	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 S/MIME	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.

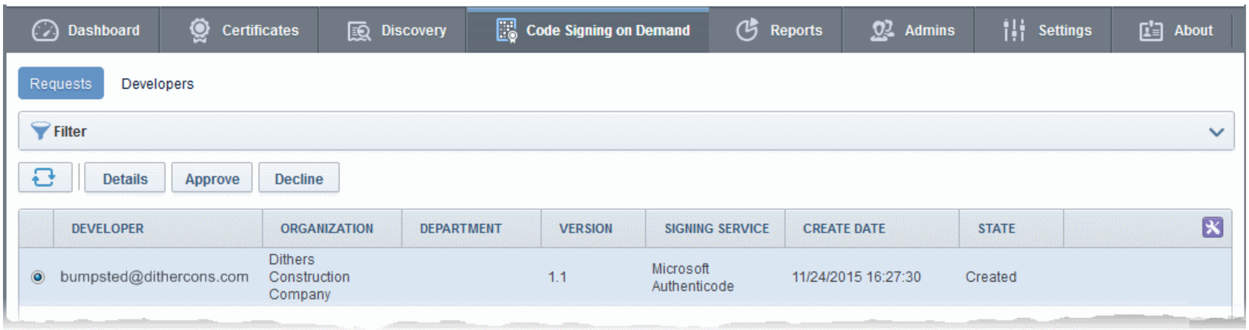
Code Signing on Demand - The 'Code Signing on Demand' tab is visible only if the feature is enabled for your account. If you wish to enable this feature, contact your Master Administrator or your InCommon account manager.

The CSoD service is available in two modes:

- **In-House Hosted mode** - Developers upload software to a local portal. The code signing process is handled by a locally installed controller. The controller will generate CSoD enabled code-signing certificates which developers can use to sign files. The certificates and their private keys are stored in encrypted form in a local database created by the controller.

  There are two deployment types available in hosted mode:

  - Standard deployment - The CSoD agent is installed on a single machine. Use of HSM is optional.
  - Clustered deployment - CSoD agents are installed on multiple servers for redundancy. Use of HSM and network file sharing is mandatory
- **Cloud Service Mode** - The signing service is hosted on InCommon's highly secure cloud servers. The service generates CSoD enabled code signing certificates for developers to sign files. The certificates and their private keys are generated and stored in encrypted format in InCommon's data-center for the lifetime of the certificate, tightly protected by InCommon's military grade security infrastructure.



	DEVELOPER	ORGANIZATION	DEPARTMENT	VERSION	SIGNING SERVICE	CREATE DATE	STATE
●	bumpsted@dithercons.com	Dithers Construction Company		1.1	Microsoft Authenticode	11/24/2015 16:27:30	Created

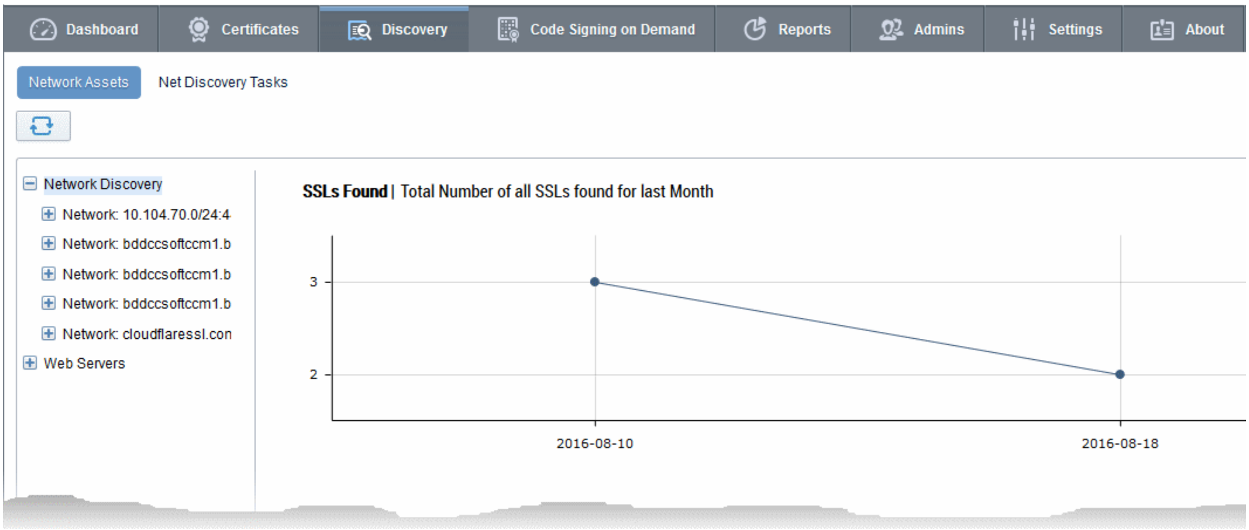
The 'Code Signing on Demand' area is accessible only by RAO Code Signing and DRAO Code Signing administrators.

Security Role / Type of Administrator	Available Action
RAO Code Signing	• Can add and manage developers for any organizations (and any sub-ordinate departments) that have been delegated to them. • Can approve code signing requests from developers pertaining to organizations (and any sub-ordinate departments) that have been delegated to them.
DRAO Code Signing	• Can add and manage developers only for the department(s) that have been delegated to them. • Can approve code signing requests only from developers pertaining to department(s) that have been delegated to them.

See 'Code Signing on Demand' for more details on Code Signing on Demand.

Certificate Discovery Tasks:

- Network Certificate discovery requires the installation of the certificate 'Controller' agent. This a small piece of software that identifies certificates on your network and auto-installs SSL Certificates
- The 'Discovery Tasks' area allows you to configure certificate controller agents for the network and to commence certificate discovery tasks.
- The 'MS AD Discovery Tasks' area allows you to scan for all types of certificates on objects in an active directory (AD) server.
- Discovery scan results are displayed in the 'Network Assets' area under the 'Discovery' tab.
- The results include 'Managed' certificates (those issued through IncommonCM) and 'Unmanaged' certificates (those acquired from other CAs, those Incommon certs not obtained through Incommon CM , and self-signed certificates).
- Administrators can assign unmanaged certificates to an 'Organization' or 'Department' to bring them under Incommon CM management.
- The 'Network Assets' area also displays web-servers and domains found on scanned networks. If Active Directory servers have been integrated with Incommon CM then the area will also shows all certificates found by scans run on AD servers.

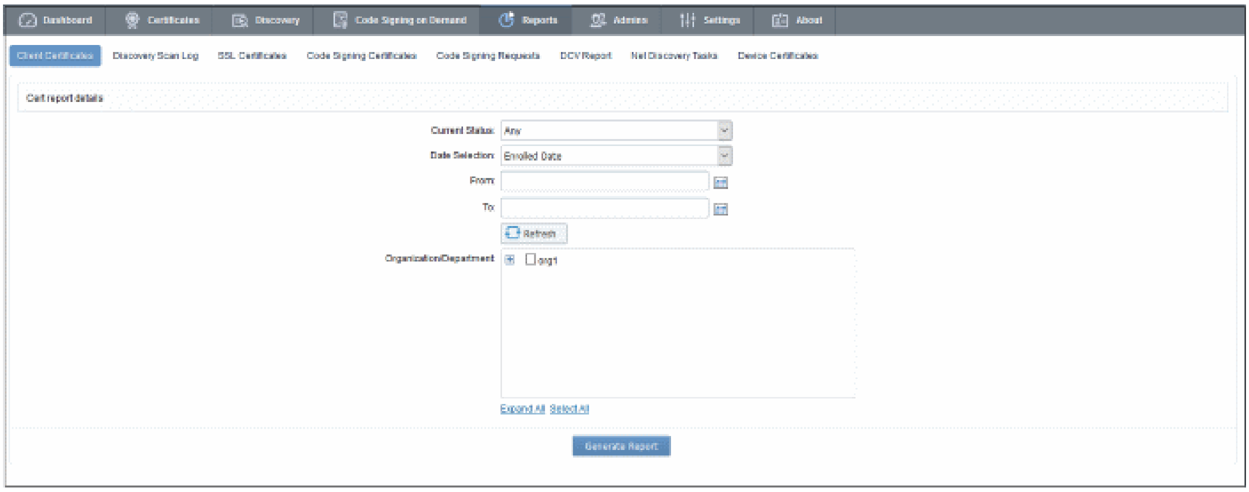


The 'Discovery' area is accessible only by RAO SSL and DRAO SSL administrators.

Security Role / Type of Administrator	Available Action
RAO SSL	Can set up agents and run certificate scans on organizations that have been delegated to them. Can also run scans on departments of those organizations.
DRAO SSL	Can set up agents and run certificate scans on departments that have been delegated to them.

Click here for more information about the Discovery section.

Reports: Enables administrators to view a range of reports depending on their privilege level. The 'Reports' interface is fully explained in Section 8. Reports.



Cert report details

Current Status: Any

Date Selection: Enrolled Date

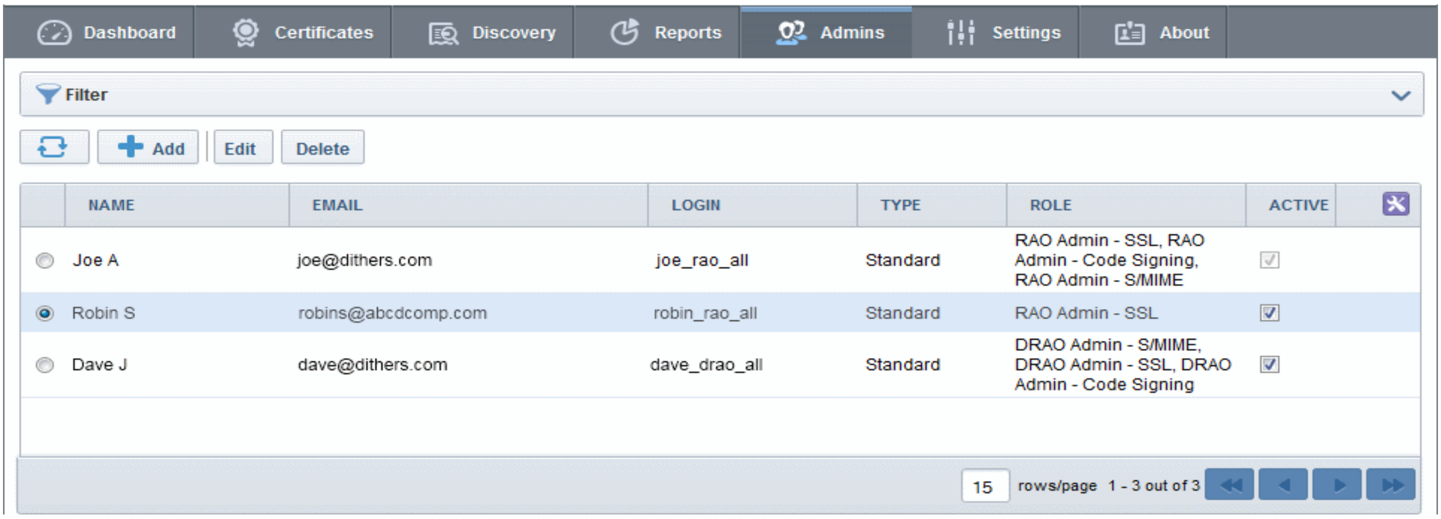
From:

To:

Organization/Department: ☐ org1

Available reports are 'Client Certificates', 'Discovery Scan Logs', 'SSL Certificates', 'Code Signing Certificates', 'Code Signing Requests' DCV Report and 'Discovery Tasks'. The types of report available to a particular administrator is dependent on their security role:

Security Role / Type of Administrator	Available Action
RAO SSL ***RAO S/MIME*** ***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 RAO SSL Admins) • 'SSL / S/MIME / Code Signing Certificate' report that is appropriate to their administrative type and for their organization(s) and department(s) only • DCV Report for their organization(s) and department(s) only (Only RAO SSL Admins)
DRAO SSL ***DRAO S/MIME*** ***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 / S/MIME / Code Signing Certificate' report that is appropriate to their administrative type and for their organization(s) and department(s) only • DCV Report for their Department(s) only (Only DRAO SSL Admins)



	NAME	EMAIL	LOGIN	TYPE	ROLE	ACTIVE
○	Joe A	joe@dithers.com	joe_rao_all	Standard	RAO Admin - SSL, RAO Admin - Code Signing, RAO Admin - S/MIME	☑
●	Robin S	robins@abcdcomp.com	robin_rao_all	Standard	RAO Admin - SSL	☑
○	Dave J	dave@dithers.com	dave_drao_all	Standard	DRAO Admin - S/MIME, DRAO Admin - SSL, DRAO Admin - Code Signing	☑

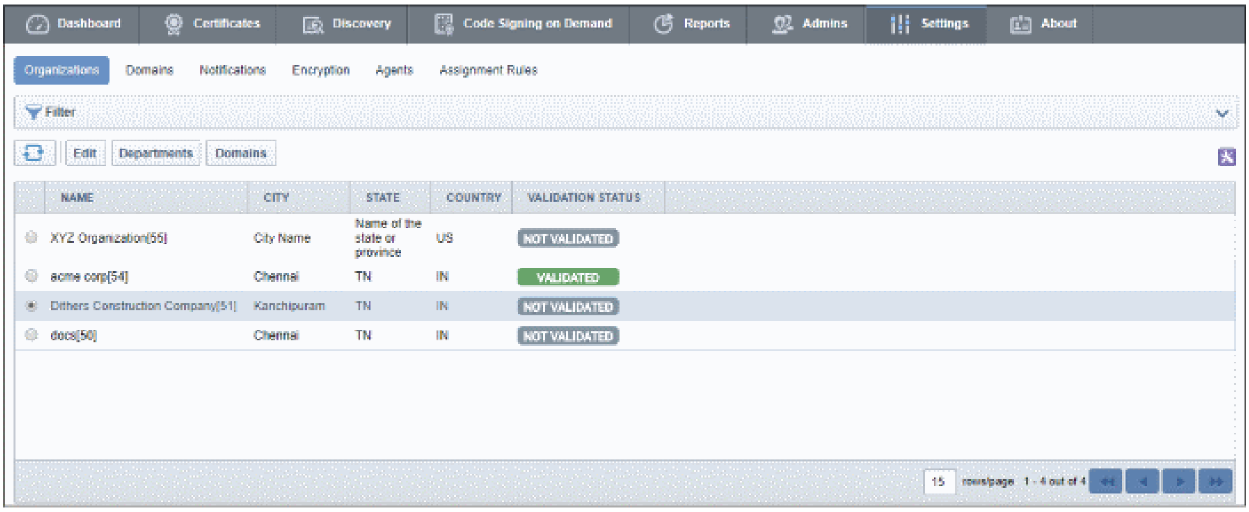
15 rows/page 1 - 3 out of 3

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
RAO SSL ***RAO S/MIME*** ***RAO Code Signing***	Can • 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 S/MIME*** ***DRAO Code Signing***	Can • 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 the CM. The number of tabs that are visible to a particular administrator is dependent on their security role (RAO or DRAO).



	NAME	CITY	STATE	COUNTRY	VALIDATION STATUS
○	XYZ Organization[55]	City Name	Name of the state or province	US	NOT VALIDATED
○	acme corp[54]	Chennai	TN	IN	VALIDATED
●	Dithers Construction Company[51]	Kanchipuram	TN	IN	NOT VALIDATED
○	docs[50]	Chennai	TN	IN	NOT VALIDATED

Click here for more information about the 'Settings' area.

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

(1) Organizations: Visible only to RAO class administrators. RAOs can view, edit, request new domains and add departments to organizations that have been delegated to them.

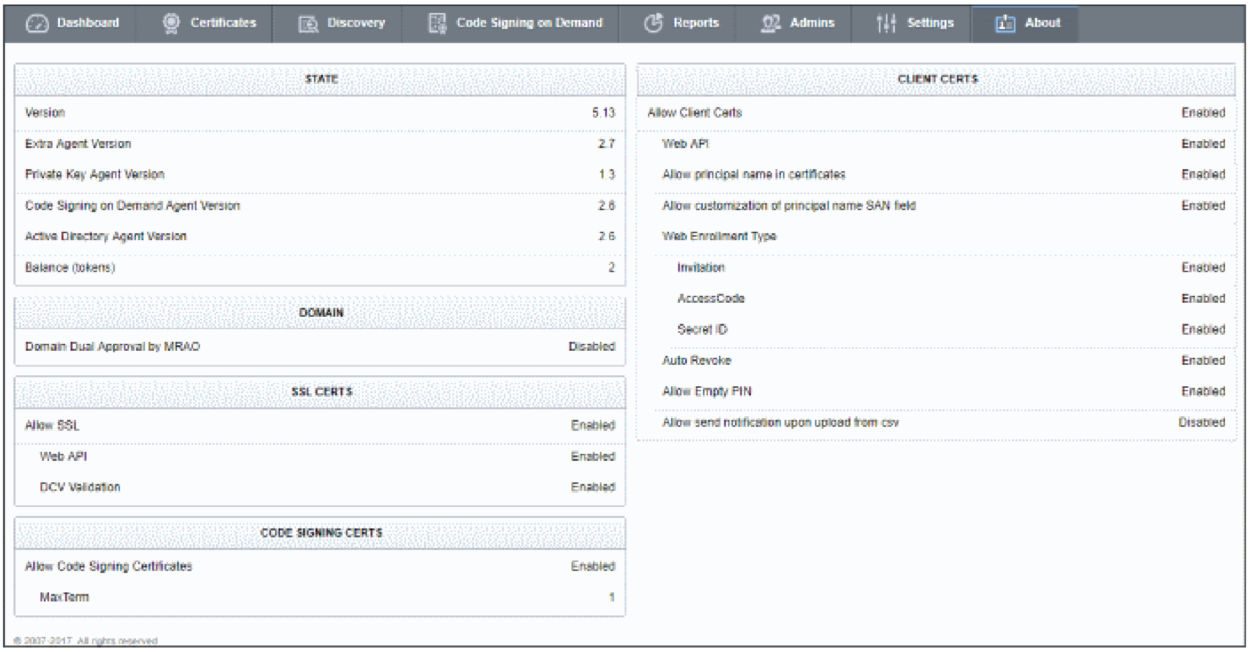
(2) Departments: Visible only to DRAO class administrators (DRAO's see a 'Departments' tab instead of the 'Organizations' tab). Allows DRAOs to view all departments that have been delegated to them and to request new domains for those departments.

(3) Domains: 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) Encryption: Allows RAO/DRAO S/MIME administrators to initialize a new master key pair or to re-encrypt the private keys of client certificates held in escrow.

(5) Incommon CM Agents - You need to install Incommon CM agents for the certificate discovery and auto-installation of SSL certificates.

(6) Assignment Rules - Enables RAO/DRAO administrators to define assignment rules for automatically assigning unmanaged certificates identified by discovery scans to required organizations and departments and apply the rules while configuring Discovery Scans.



STATE	
Version	5.13
Extra Agent Version	2.7
Private Key Agent Version	1.3
Code Signing on Demand Agent Version	2.6
Active Directory Agent Version	2.6
Balance (tokens)	2

DOMAIN	
Domain Dual Approval by MRAO	Disabled

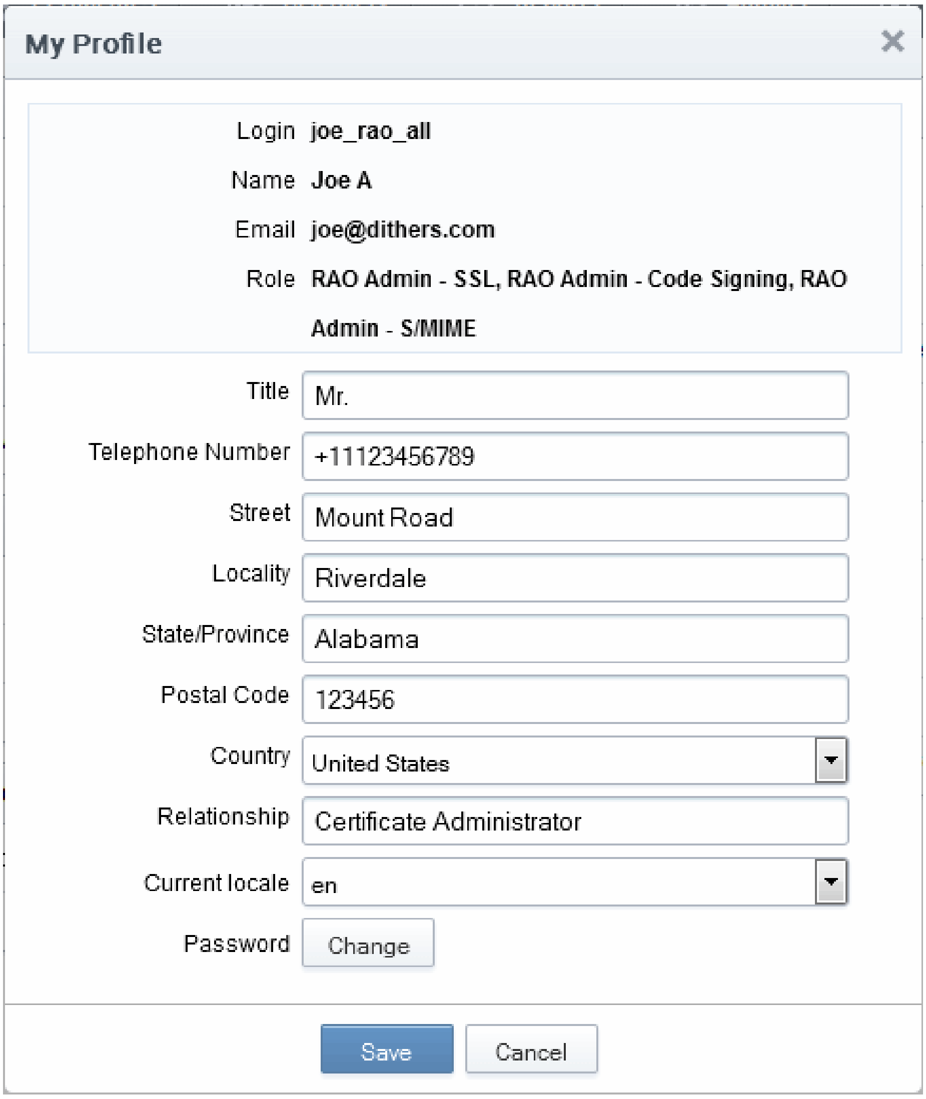
SSL CERTS	
Allow SSL	Enabled
Web API	Enabled
DCV Validation	Enabled

CODE SIGNING CERTS	
Allow Code Signing Certificates	Enabled
MaxTerm	1

CLIENT CERTS	
Allow Client Certs	Enabled
Web API	Enabled
Allow principal name in certificates	Enabled
Allow customization of principal name SAN field	Enabled
Web Enrollment Type	
Invitation	Enabled
AccessCode	Enabled
Secret ID	Enabled
Auto Revoke	Enabled
Allow Empty PIN	Enabled
Allow send notification upon upload from csv	Disabled

© 2007-2017. All rights reserved

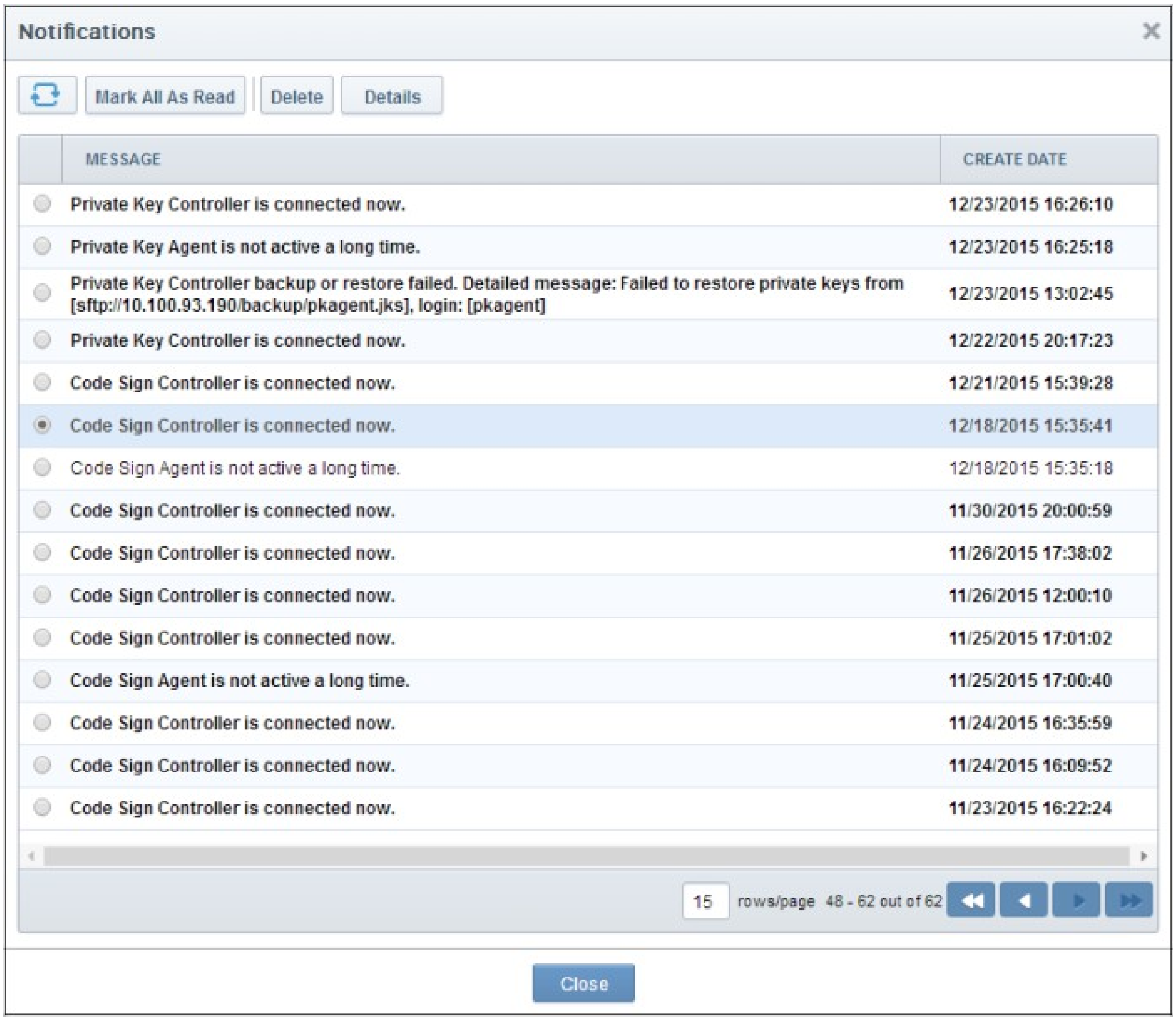
My Profile: Enables currently logged-in administrator to view/edit address details and change the password.



Login	joe_rao_all
Name	Joe A
Email	joe@dithers.com
Role	RAO Admin - SSL, RAO Admin - Code Signing, RAO Admin - S/MIME
Title	Mr.
Telephone Number	+11123456789
Street	Mount Road
Locality	Riverdale
State/Province	Alabama
Postal Code	123456
Country	United States
Relationship	Certificate Administrator
Current locale	en
Password	Change

Support - Clicking the help icon takes you to InCommon partner, Comodo's support page at https://support.comodo.com/, the Comodo support web page, an online knowledge-base and support ticketing system. The fastest way to get further assistance in case you find any problem using Incommon CM management console.

Notification - The notification icon at the top indicates the number of message that are yet be read. Click on the icon to view the messages. The types of messages displayed are related to validation, controller, agent and so on.



	MESSAGE	CREATE DATE
○	Private Key Controller is connected now.	12/23/2015 16:26:10
○	Private Key Agent is not active a long time.	12/23/2015 16:25:18
○	Private Key Controller backup or restore failed. Detailed message: Failed to restore private keys from [sftp://10.100.93.190/backup/pkagent.jks], login: [pkagent]	12/23/2015 13:02:45
○	Private Key Controller is connected now.	12/22/2015 20:17:23
○	Code Sign Controller is connected now.	12/21/2015 15:39:28
●	Code Sign Controller is connected now.	12/18/2015 15:35:41
○	Code Sign Agent is not active a long time.	12/18/2015 15:35:18
○	Code Sign Controller is connected now.	11/30/2015 20:00:59
○	Code Sign Controller is connected now.	11/26/2015 17:38:02
○	Code Sign Controller is connected now.	11/26/2015 12:00:10
○	Code Sign Controller is connected now.	11/25/2015 17:01:02
○	Code Sign Agent is not active a long time.	11/25/2015 17:00:40
○	Code Sign Controller is connected now.	11/24/2015 16:35:59
○	Code Sign Controller is connected now.	11/24/2015 16:09:52
○	Code Sign Controller is connected now.	11/23/2015 16:22:24

15 rows/page 48 - 62 out of 62

Logout: Click the icon to log out of InCommon Certificate Manager.

1.5 Release Notes

Version History	
Version Number	**List of Changes**
Version 6.0	• MS AD agent now supports issuance of device certificates from MS CA. • Auto-installation support now extended to multi-domain and wildcard certificate types. • New wizard for requesting for SSL certificates • Various bug fixes
Version 5.13	• The 'Code Signing on-Demand' controller now supports multi-instance deployments. Multi-instance deployments require a network HSM and Network File System. • New API methods to create, edit, delete and list custom fields. • Support for custom fields added to the 'Enroll SSL' API.
Version 5.12	• New RESTful API methods for the 4 types of domain control validation (email, http, https and cname) • Active Directory discovery scans have been merged with discovery tasks. You can now manage AD scans in Discovery > Discovery Tasks • Assignment rules can now be applied to Active Directory discovery scans • Support information and links have been added to customer login pages
Version 5.11	• Added auto-installer support for F5 BIG-IP web-servers. Version 5.11 supports now support auto-install/renewal on the following platforms: • Apache Web Server (Linux 32/64bit) • IIS 7/7.5/8 (Windows 32/64) • Apache Tomcat (Windows 32/64bit, Linux 32/64bit) • F5 Big-IP • Added hash-signing support to the Code Signing on Demand (CSoD) service. Instead of uploading an entire file, developers can upload a hash of their binaries for signing with their code-signing certificate. The signed hash and certificate can then be embedded with their binary.
Version 5.10	• Support for RESTful APIs for Discovery service • Added API method for renewal of SSL Certificates using renew ID • Added ability to group MS Agents installed on different AD servers to form clustered Agent for certificate discovery and issuance

Version History	
Version Number	**List of Changes**
Version 5.9	• Added API method for replacement of SSL Certificates • Added ability to edit device certificate approval email template • Improved certificate collection time • Various bug fixes
Version 5.8	• Support for RESTful APIs for Code Signing on Demand service • Added client certificate authentication support for SOAP APIs • Improved device cert reports with addition of status information • Added ability to edit device certificate collection email template • Added ability to resend device certificate collection emails • Improvements to SCEP configuration of device certificates
Version 5.7	• Added ability to integrate InCommonCM with a Hardware Security Module (HSM) to generate and store keys and code signing certificates enrolled for Code Signing on Demand (CSoD) • Added ability to enroll device certificates through Simple Certificate Enrollment Protocol (SCEP)
Version 5.6	• Improvements in auto-installation including scheduled auto-renew and enhanced scheduling abilities. • Added ability to map MS AD Certificate Templates to InCommon CM certificate types • Added ability for issuance of device certificates from Private Certificate Authorities using C InCommon CM certificate types • Added ability for self-enrollment of device certificates by applicants
Version 5.5	• Added the ability to issue Device Certificates for authentication of devices and endpoints, including BYOD devices connected to the networks. • Added ability to integrate AD servers by installing MS agents, for running discovery scans on the servers and issue device certificates to devices enrolled to them. • Added ability to define assignment rules for automatically assigning unmanaged certificates identified by discovery scans to required organizations and departments for bringing them under management. • Added Network Assets view to display the SSL certificates installed on various nodes, servers and endpoints, as identified by discovery scans, web-servers with details on websites/domains hosted on them and Active Directory objects with certificates installed on them as discovered by AD server scans. • Added new API for integration to Mobile Device Management (MDM) solutions, for issuance of Device Certificates. • Various Bug fixes.

Version History	
Version Number	**List of Changes**
Version 5.4	• Maintenance update addressing bug fixes and various back-end improvements • Added Identity Providers (IdP) feature, which allows admins to log into Incommon CM using credentials of his/her IdP. New admins can also be enrolled using the IdP method.
Version 5.3	• Added Bulk DCV feature that enables admins to validate multiple domains at once, as long as all domains share a common email listed on the WhoIs record.
Version 5.1	• Added Private Key Store feature that enables storage an management of private keys of managed SSL certificates at customers network. Certificates whose private keys are managed at the private key store can be imported in .p12 format for directly imported to any server(s) for installation.
Version 5.0	• Redesigned User Interface. • Improved Dashboard with drill-down statistical reports. • Support for issuance of certs to private domain names.
Version 4.6	• Added the new Dashboard feature with graphs and charts that allow the administrator to quickly gain an overview of all SSL, S/MIME and code-signing certificates on the network.
Version 4.5	• Added a new report type 'Notification log Statistics' to enable Master 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	• Various bug fixes

Version History	
Version Number	**List of Changes**
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, InCommon CM 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 interfaces 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 web server which will communicate with InCommon CM for certificate requests. If a request exists, the agent will generate a CSR and present it to the administrator for approval in the InCommon CM interface. • Various Bug fixes
Version 2.10	• 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

Version History	
Version Number	**List of Changes**
	- Added a column 'External Requester' to SSL report - Improvements to the notifications system **Bug Fixes**: - Fixed bug whereby Master Administrator is sent 'Discovery Scan Summary' notification even though the Notify Master Admin(s) check-box 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 Master Administrators - 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 Master Administrators. - Domain creation/delegation requests approved by Master Administrator with privilege 'Allowing domain validation without Dual Approval' are activated immediately without requiring approval by a second Master Administrator. - Domains created by DRAO Administrators are to be approved by RAO of the organization to which the department belongs prior to approval by Master Administrators . - 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) functionality to determine capabilities of Client

Version History	
Version Number	List of Changes
	Certificates of end-users belonging to an Organization. • Added functionality to display only required fields in the request forms for EVSSL certificates (both Built-in application form and the Self Enrollment form) • Subscriber's Agreements are made specific to the Certificate type selected while requesting for SSL Certificate and Code Signing Certificates. • Implemented Simple Certificate Enrollment Protocol (SCEP) support to Client Certificates in addition to SSL 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 • Master Administrator admin can add a new delegation for approved domain without dual MRAO approval. • Dual Master Administrator Approval check-boxes are selected by default while creating new domains.
Version 2.8.20	• Added Dual Master Administrator Approval for New Domains. When enabled, each new domain created by an RAO or a DRAO needs to be approved by two Master Administrators. The Domain will remain in 'Requested' status until both the Master Administrators have approved it; • Administrators that have privileges to 'Allow creation of admin users' privileges are now allowed to create peer level admins without needing approval from a higher level administrator; **Bug Fixes**: • 'Person upload' notification messages are now customizable; • Fixed bug whereby a Master Administrator could bypass 'dual domain auto approval' by using 'domain edit'; • Fixed bug that sometimes allowed domains created by a Master Administrator to be automatically sent forward for validation without requiring approval from second Master Administrator; • 'Active' checkbox in 'Settings/Domains' is now, by default, always enabled for Master Administrator; • 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;

Version History	
Version Number	List of Changes
	• Fixed occasional bug whereby an Master Administrator could modify their own privileges and/or those of a fellow Master Administrator; • 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 Master Administrator by changing admin role of another Master Administrator.

2 The Dashboard

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

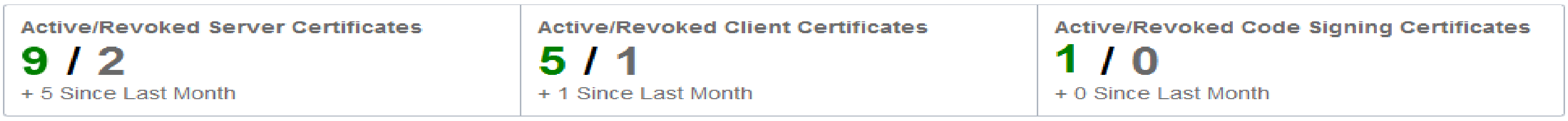
The charts and graphs in the dashboard provide an essential combination of key life-cycle information (such as certificates approaching expiry, certificates issued/requested and DCV status) as well as important technical insights like how many servers have support for perfect forward secrecy, renegotiation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

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

Security Roles:

- RAO SSL, RAO S/MIME 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 S/MIME 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 displays a real-time summary of Active/Revoked certificates:



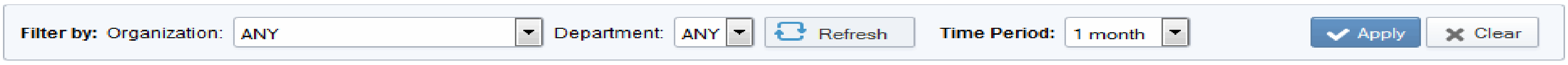
Active/Revoked Server Certificates
9 / 2
+ 5 Since Last Month

Active/Revoked Client Certificates
5 / 1
+ 1 Since Last Month

Active/Revoked Code Signing Certificates
1 / 0
+ 0 Since Last Month

Filtering Options:

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


Filter by: Organization: ANY Department: ANY Refresh Time Period: 1 month Apply Clear

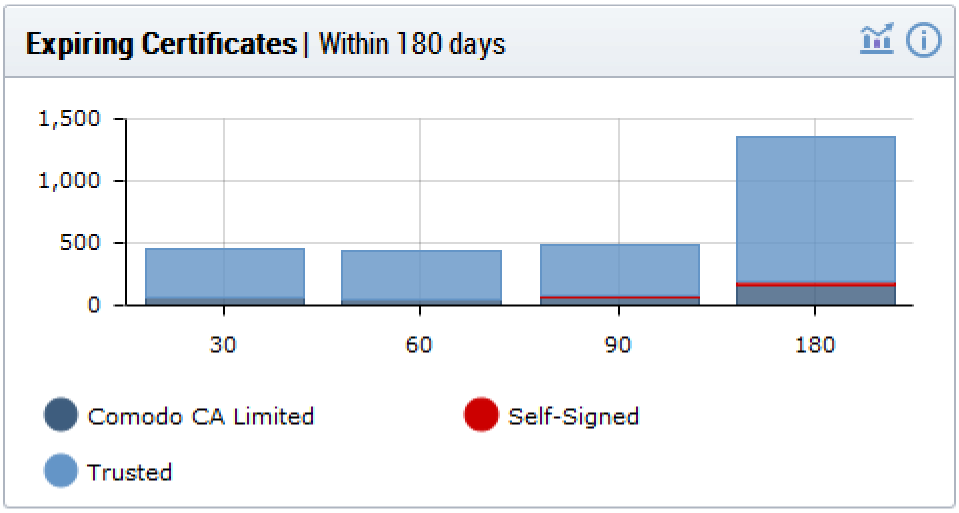
-
- To add a filter, select the type of the filter from the 'Add Filter' drop-down. The available options are:
  - Organization - Choose an organization / department from the respective drop-downs and click 'Apply'.
  - Time Period - Select the time period for which you wish to view statistics from the '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:

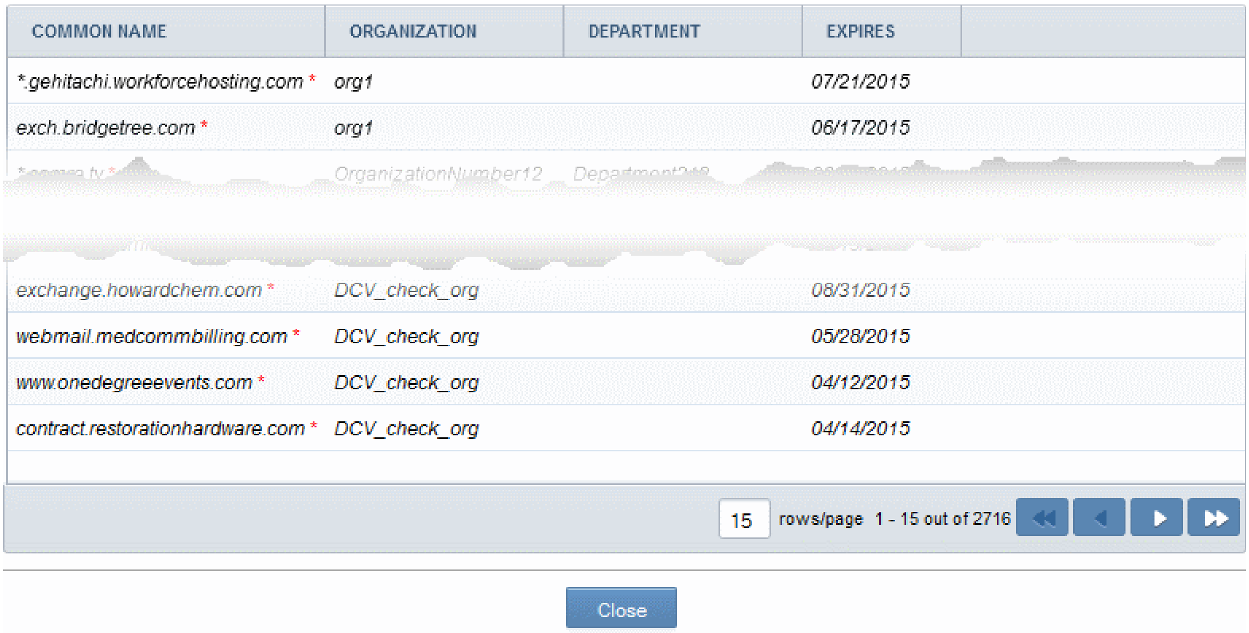
- Expiring Certificates by Issuer - InCommon, self-signed and 'Other Trusted' certificates expiring within 180 days
- DCV Expiring Domains - Domains for which Domain Control Validation will expire within 180 days
- Certificates Types (Managed) - Single Domain, Wildcard, Multi-Domain, UCC etc.
- Certificates by Validation Level - EV, DV, OV.
- SSL Certificate Types - Certificates issued through InCommon CM and broken down by brand names like Instant SSL, Premium SSL, EV SSL, AMT SSL certificate etc.
- Certificate Requests versus Certificates Issued
- Certificates by CA - Comodo, VeriSign, GoDaddy, Thawte, self-signed etc.
- Certificate Requests by Category of Certificate - SSL requests, S/MIME requests, Code signing requests
- Certificates By Duration - How many of your certificates are 1 year, 2 year, 3 year etc
- DCV Status - The current stage in the Domain Control Validation process held by your certificate-hosting domains
- 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 Signing Algorithm - Certificates by hashing and signing algorithms (e.g. SHA1withRSA)
- Certificates by Public Key Algorithm - Certificates broken down by encryption algorithm (RSA, DSA etc)
- CSoD Usage - Code signing requests broken down by total and signed requests
- CSoD Certificates Usage - Code signing requests broken down by certificates belonging to different developers

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 InCommon certificates in order to benefit from InCommon CM's management capabilities.



- Hovering the mouse cursor over a legend or graph displays the number of certificates in each category.
- Clicking on the information icon ⓘ displays a tool tip explaining the chart
- Clicking on the graph icon displays a report with the breakdown of statistics shown in the chart:



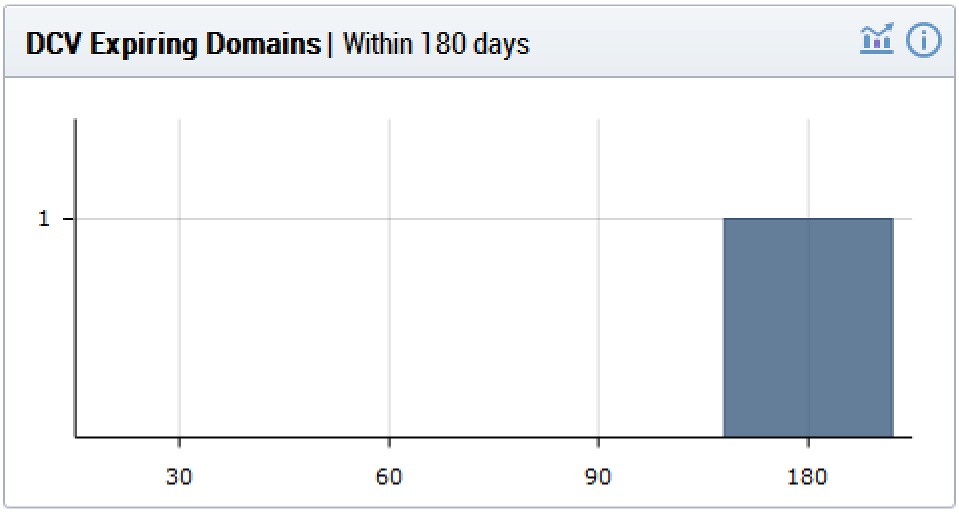
COMMON NAME	ORGANIZATION	DEPARTMENT	EXPIRES
*.gehitachi.workforcehosting.com *	org1		07/21/2015
exch.bridgetree.com *	org1		06/17/2015
exchange.howardchem.com *	DCV_check_org		08/31/2015
webmail.medcommbilling.com *	DCV_check_org		05/28/2015
www.onedegreeevents.com *	DCV_check_org		04/12/2015
contract.restorationhardware.com *	DCV_check_org		04/14/2015

'Expiring Certificates Report' Table - Column Descriptions	
Column Header	**Description**
Common Name	The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.
Organization	Name of the Organization that has been issued with the certificate.
Department	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.

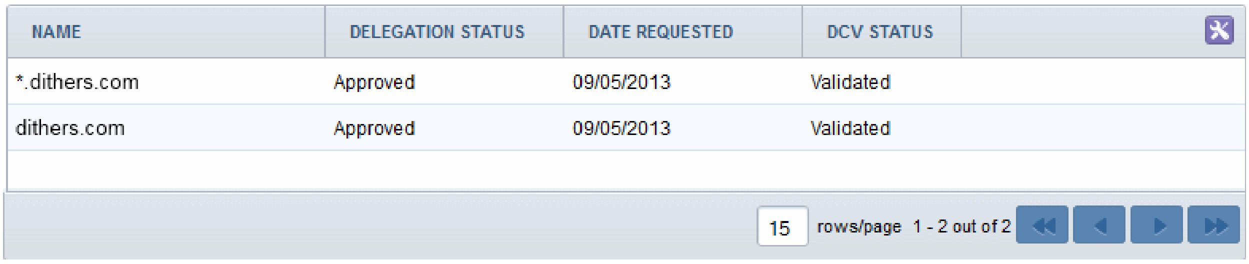
Expires	The expiration date of the certificate.

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.
- Clicking on the information icon ⓘ displays a tool tip explaining the chart
- Clicking on the graph icon 📊 displays a report with the breakdown of statistics shown in the chart:



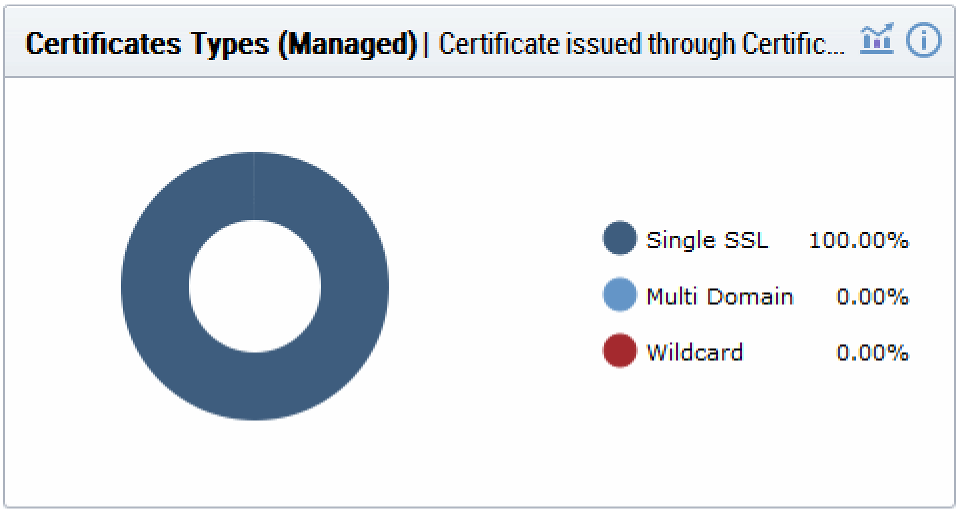
NAME	DELEGATION STATUS	DATE REQUESTED	DCV STATUS
*.dithers.com	Approved	09/05/2013	Validated
dithers.com	Approved	09/05/2013	Validated

'DCV Expiring Domains Report' Table - Column Descriptions	
Column Header	**Description**
Name	The name of the domain.
Delegation Status	Indicates whether domain is active or inactive
Date Requested	Indicates the date on which the domain was requested.

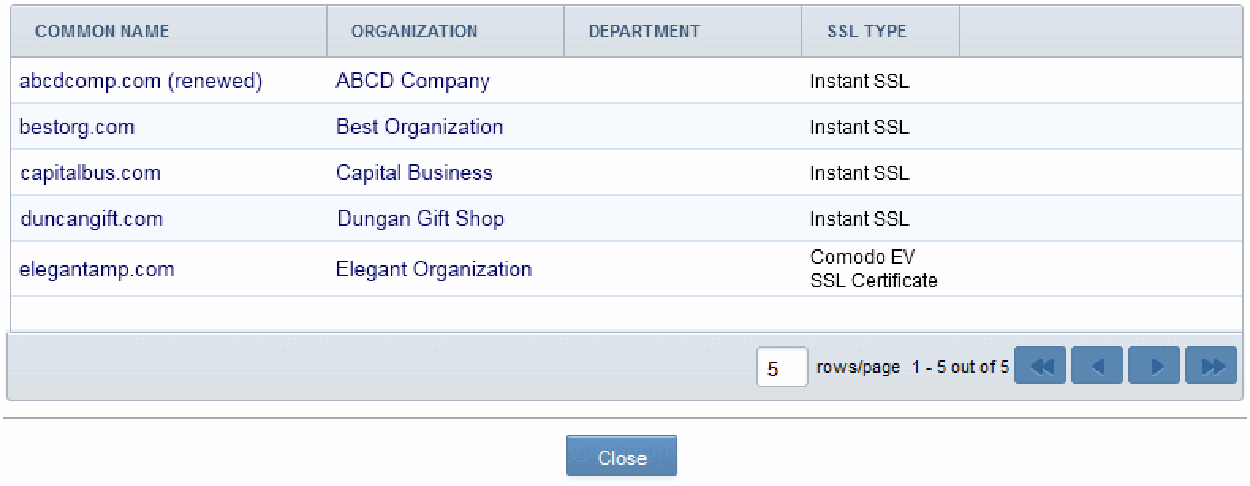
DCV Status	Indicates the request/approval status of the domain.

Certificate Types (Managed)

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 InCommon CM.



- Hovering your mouse cursor over a legend item or section displays additional details such as the actual quantity of certificates of that type.
- Clicking the information icon ⓘ displays a tool tip explaining the chart
- Clicking the graph icon displays a report with the breakdown of statistics shown in the chart:



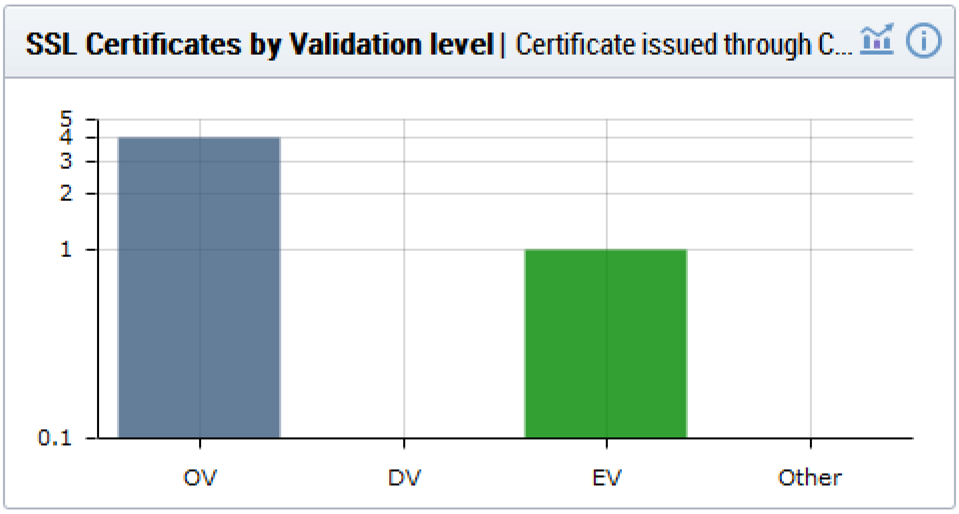
COMMON NAME	ORGANIZATION	DEPARTMENT	SSL TYPE
abcdcomp.com (renewed)	ABCD Company		Instant SSL
bestorg.com	Best Organization		Instant SSL
capitalbus.com	Capital Business		Instant SSL
duncangift.com	Dungan Gift Shop		Instant SSL
elegantamp.com	Elegant Organization		Comodo EV SSL Certificate

'Managed Certificate Types Report' Table - Column Descriptions	
Column Header	**Description**
Common Name	The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.

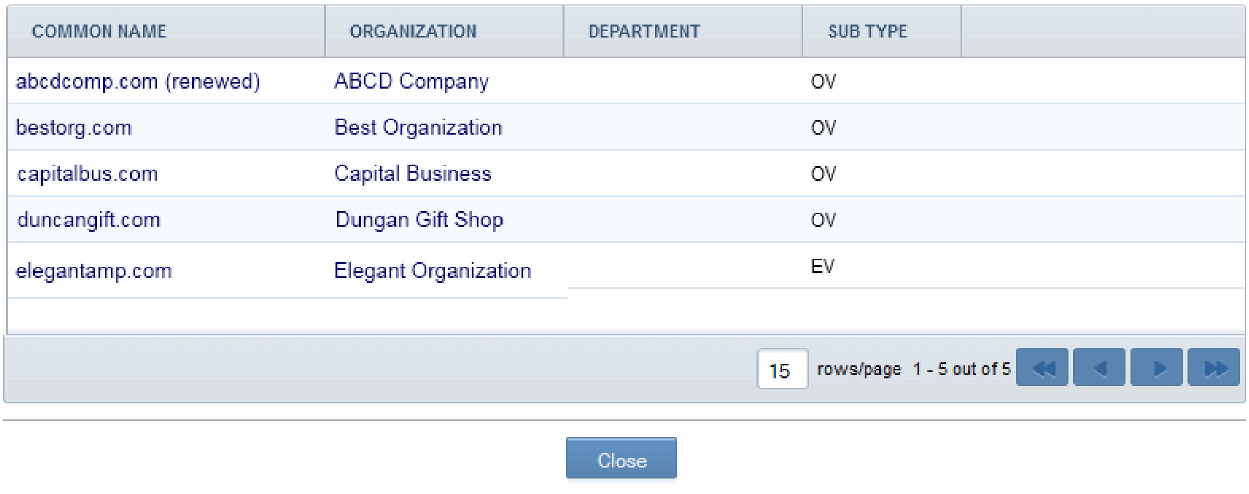
Organization	Name of the organization that has been issued with the certificate.
Department	The specific department of the organization that is associated with the certificate. This column will be blank if a department has not been delegated as the controlling entity.
SSL Type	Indicates type of the certificate with its brand name

Certificates by Validation Level

The chart 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.
- Clicking the information icon ⓘ displays a tool tip explaining the chart
- Clicking the graph icon displays a report with the breakdown of statistics shown in the chart:



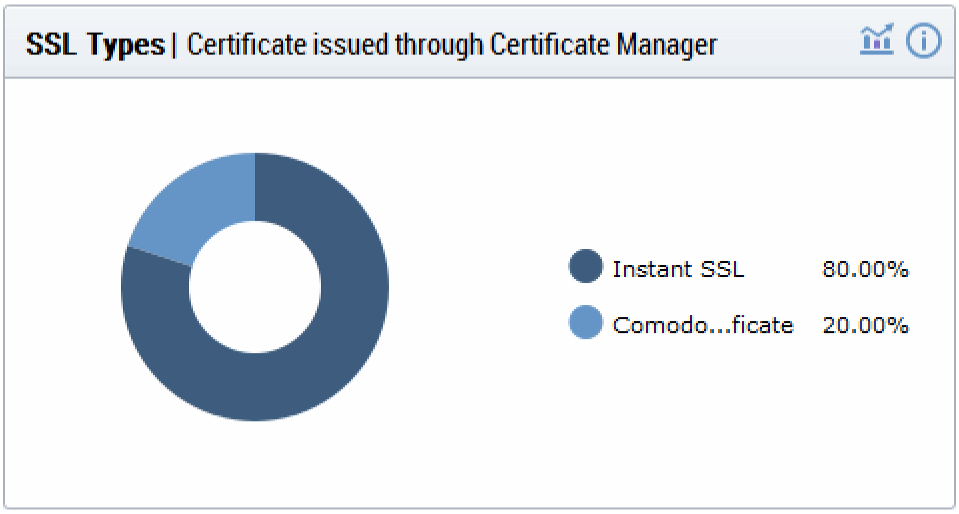
COMMON NAME	ORGANIZATION	DEPARTMENT	SUB TYPE
abcdcomp.com (renewed)	ABCD Company		OV
bestorg.com	Best Organization		OV
capitalbus.com	Capital Business		OV
duncangift.com	Dungan Gift Shop		OV
elegantamp.com	Elegant Organization		EV

'SSL Certificates by Validation Level Report' Table - Column Descriptions

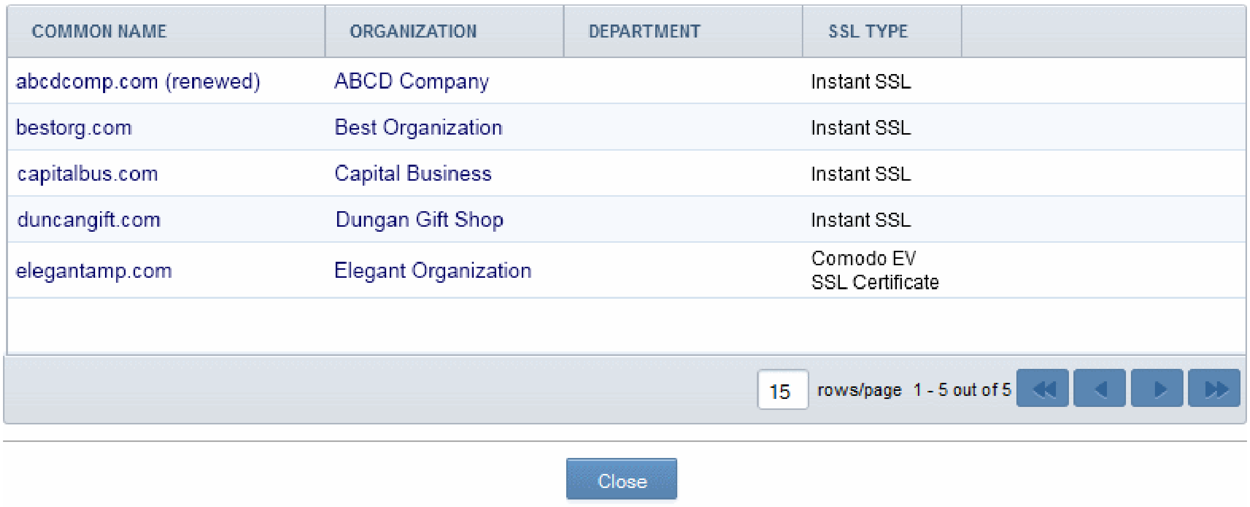
Column Header	Description
Common Name	The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.
Organization	Name of the Organization that has been issued with the certificate.
Department	The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity.
Sub Type	Indicates validation level of the certificate, like Domain Validated, Organization Validated and Extended Validation.

SSL Types

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



- Hovering your mouse over a legend or sector displays additional details.
- Clicking the information icon ⓘ displays a tool tip on the chart
- Clicking the graph icon 📊 displays a report with the breakdown of statistics shown in the chart



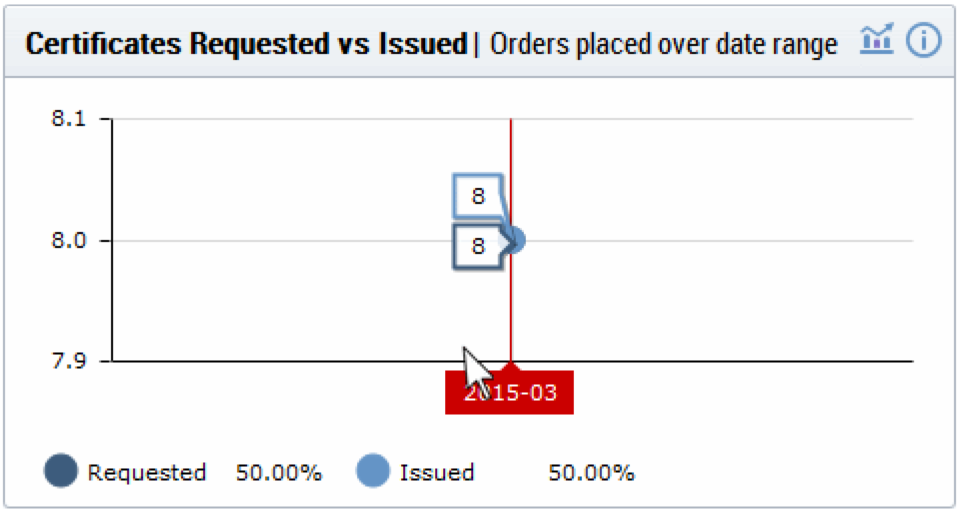
COMMON NAME	ORGANIZATION	DEPARTMENT	SSL TYPE
abcdcomp.com (renewed)	ABCD Company		Instant SSL
bestorg.com	Best Organization		Instant SSL
capitalbus.com	Capital Business		Instant SSL
duncangift.com	Dungan Gift Shop		Instant SSL
elegantamp.com	Elegant Organization		Comodo EV SSL Certificate

'SSL Types Report' Table - Column Descriptions	
Column Header	**Description**
Common Name	The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.
Organization	Name of the organization that has been issued with the certificate.
Department	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.
SSL Type	Indicates brand name of the certificate.

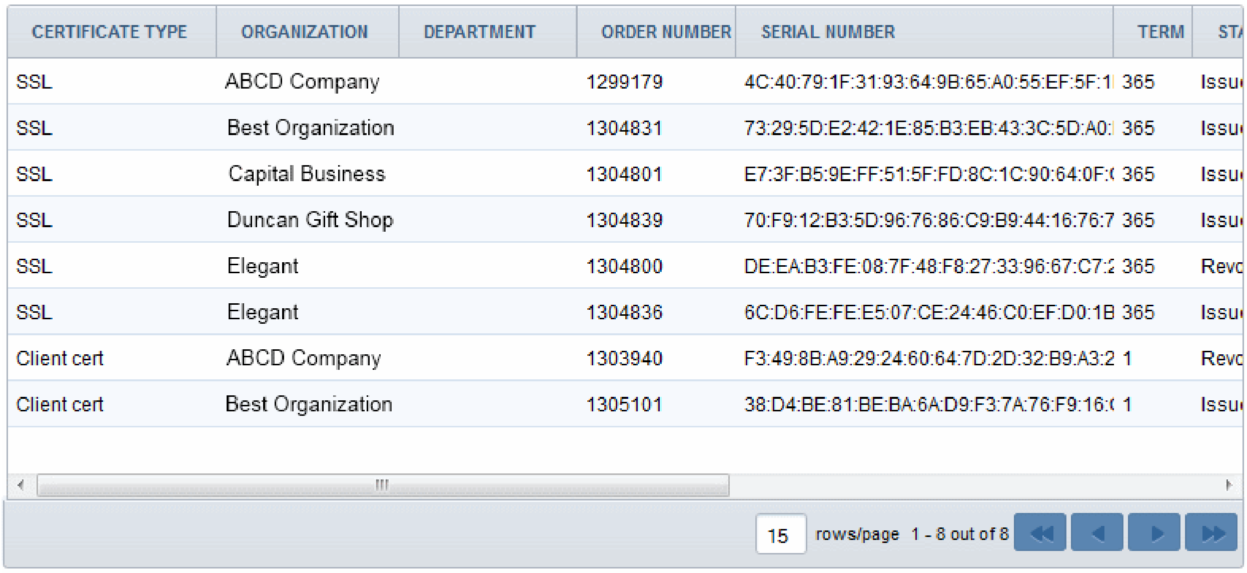
Note: Certificates with 'Issued' status are shown with blue text.

Certificates Requested vs Issued

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


Certificates Requested vs Issued | Orders placed over date range
8.1
8.0
7.9
8
8
2015-03
Requested 50.00%
Issued 50.00%

- Placing the mouse cursor over the graph nodes displays more details about the number of certificates that were requested and issued on that date.
- Clicking the information icon ⓘ displays a tool tip on the chart
- Clicking the details icon 📊 displays a report with the breakdown of statistics shown in the chart

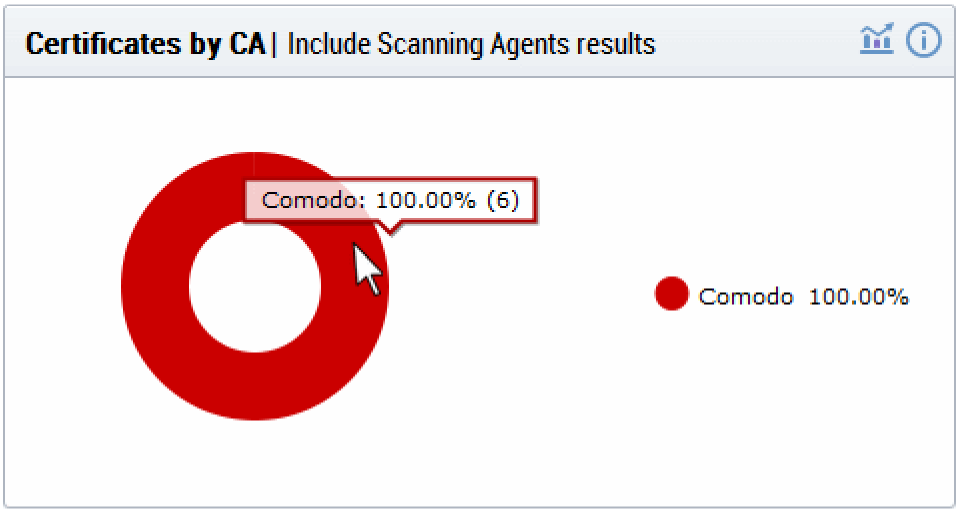


CERTIFICATE TYPE	ORGANIZATION	DEPARTMENT	ORDER NUMBER	SERIAL NUMBER	TERM	STA
SSL	ABCD Company		1299179	4C:40:79:1F:31:93:64:9B:65:A0:55:EF:5F:1	365	Issu
SSL	Best Organization		1304831	73:29:5D:E2:42:1E:85:B3:EB:43:3C:5D:A0:	365	Issu
SSL	Capital Business		1304801	E7:3F:B5:9E:FF:51:5F:FD:8C:1C:90:64:0F: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

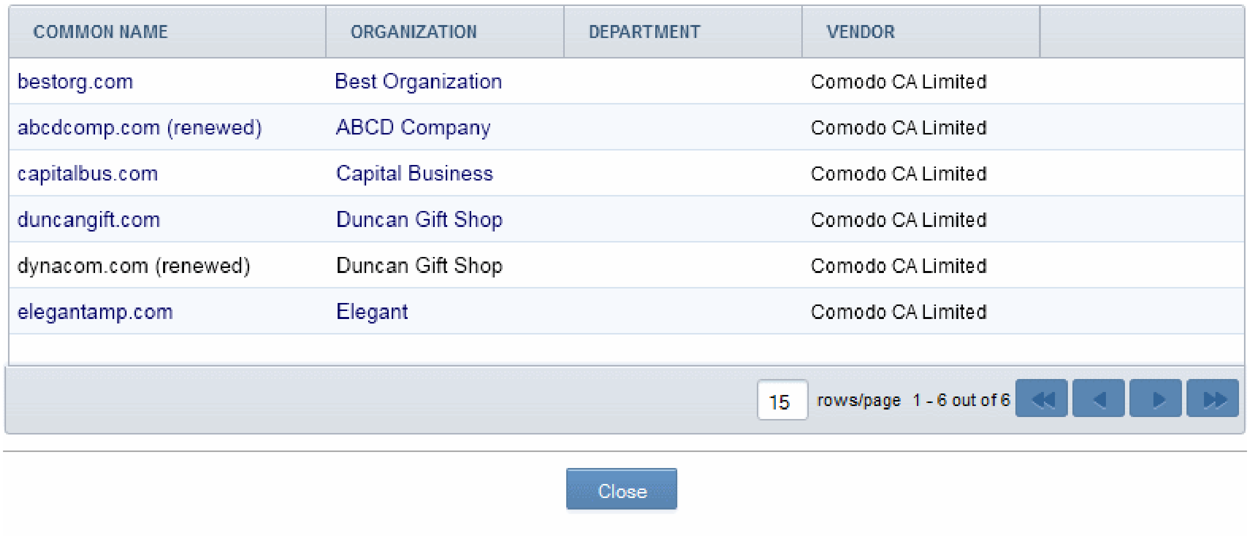
'Certificates Requested Vs Issued Report' Table - Column Descriptions	
Column Header	**Description**
Certificate Type	The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.
Organization	Name of the organization that has been issued with the certificate.
Department	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.
Order Number	Indicates the number assigned by the Certification Authority (CA) for the request.
Serial Number	Displays the serial number of the certificate that is unique and can be used to identify the certificate.
Term	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.
State	Indicates the current status of the certificate.
Requested	The date at which the certificate was requested by the end-user or the administrator
Collected	The date at which the certificate was collected by the end-user or the administrator
Expires	The date of expiry of the certificate

Certificates by CA

The 'Certificates by CA' chart allows you to determine what percentage (%) 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 InCommon equivalents in order to benefit from InCommon CM'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.
- Clicking the information icon ⓘ displays a tool tip on the chart
- Clicking the graph icon 📊 displays a report with the breakdown of statistics shown in the chart



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

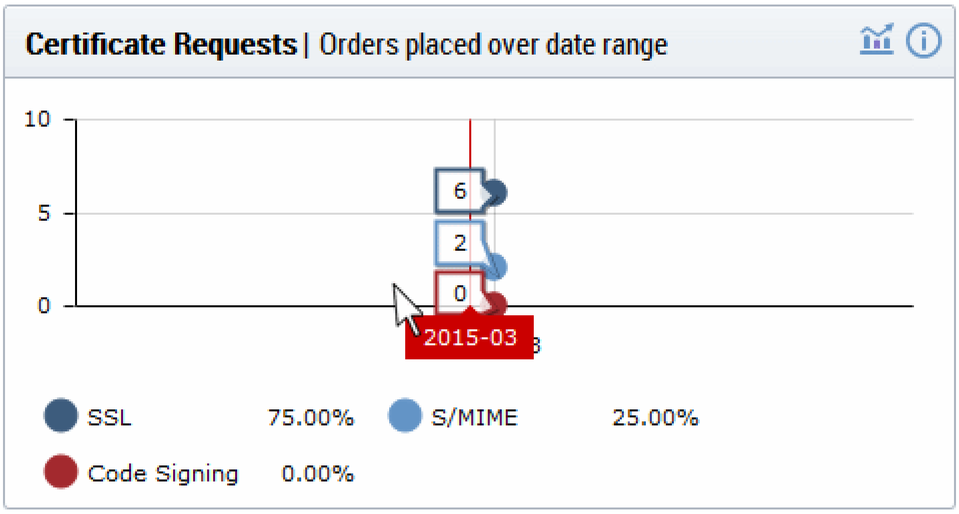
'Certificates by CA Report' Table - Column Descriptions	
Column Header	**Description**
Common Name	The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.
Organization	Name of the organization that has been issued with the certificate.

Department	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.
Vendor	Shows the vendor that has issued the certificate.

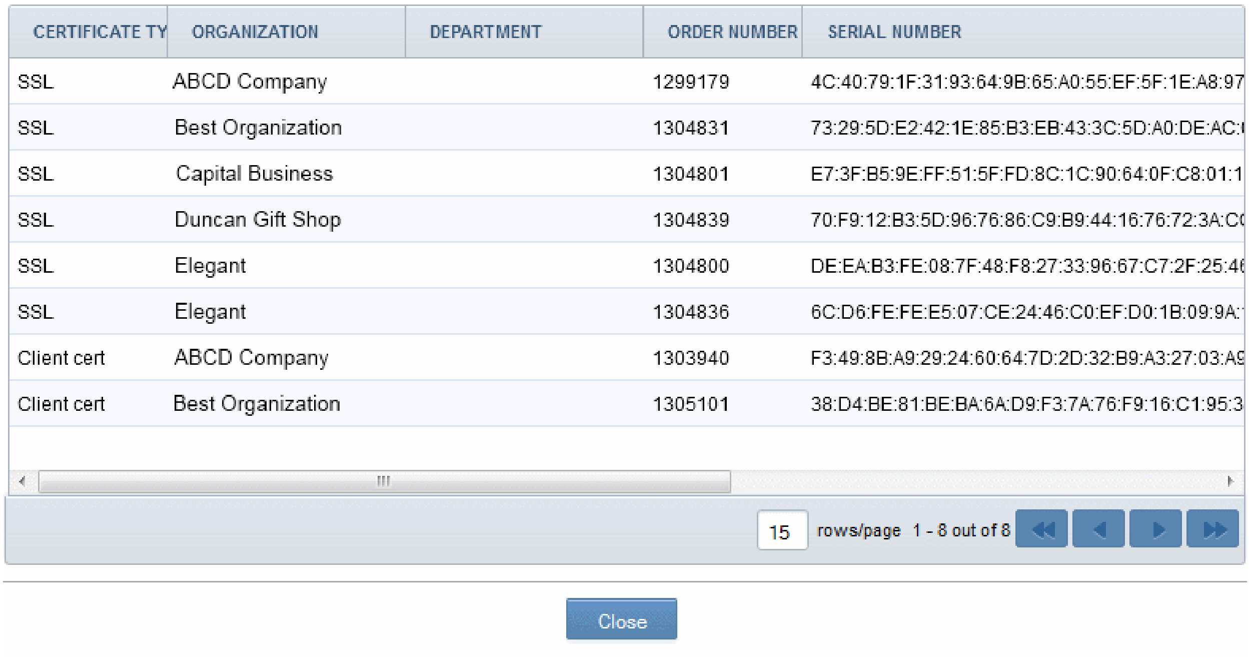
Note: Certificates with 'Issued' status are shown with blue text.

Certificate Requests

The 'Certificates Requests' graph displays the number of InCommon CM orders placed over time for SSL, S/MIME and Code Signing certificates.



- Hovering the mouse cursor over the nodes on the graph displays the exact number of certificates that were requested.
- Clicking the information icon ⓘ displays a tool tip on the chart
- Clicking the graph icon 📊 displays a report with the breakdown of statistics shown in the chart

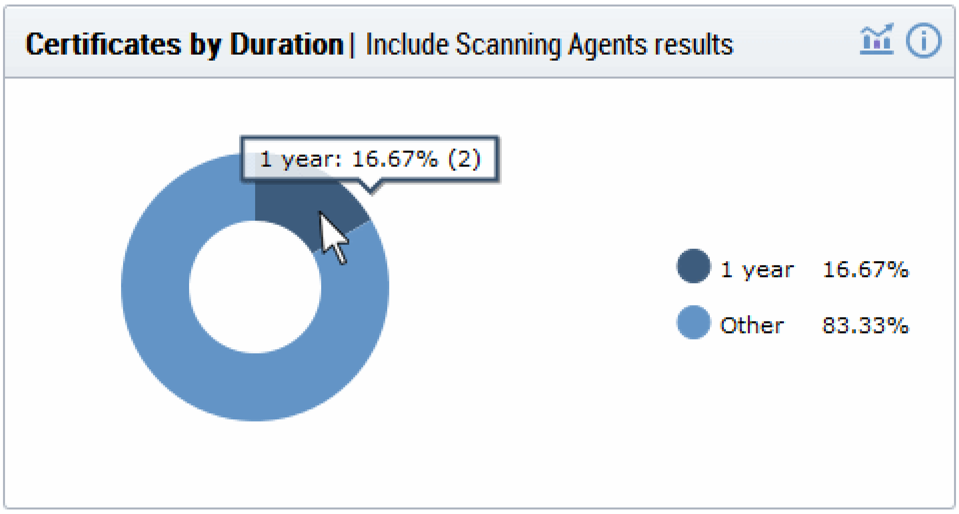


CERTIFICATE TY	ORGANIZATION	DEPARTMENT	ORDER NUMBER	SERIAL NUMBER
SSL	ABCD Company		1299179	4C:40:79:1F:31:93:64:9B:65:A0:55:EF:5F:1E:A8:97
SSL	Best Organization		1304831	73:29:5D:E2:42:1E:85:B3:EB:43:3C:5D:A0:DE:AC:
SSL	Capital Business		1304801	E7:3F:B5:9E:FF:51:5F:FD:8C:1C:90:64:0F:C8:01:1
SSL	Duncan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

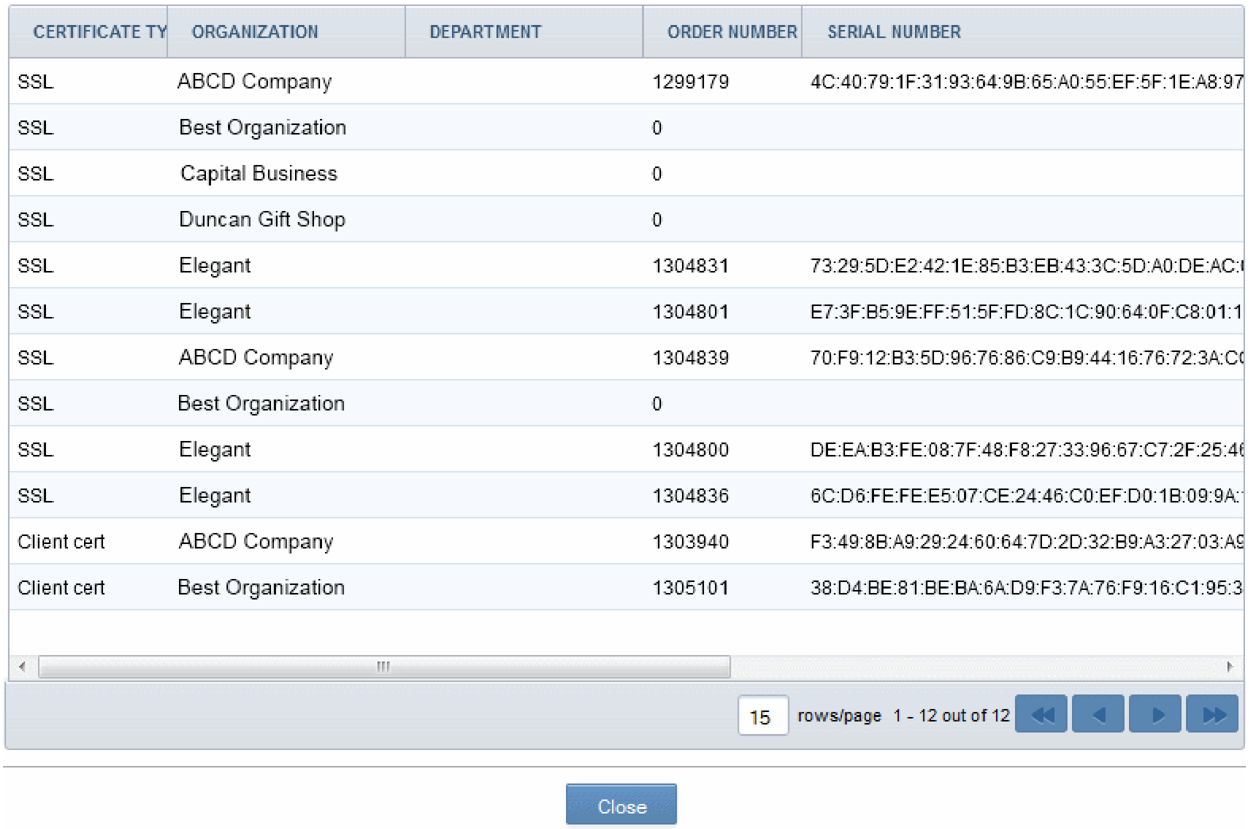
'Certificates Requests Report' Table - Column Descriptions	
Column Header	**Description**
Certificate Type	The domain for which the certificate was requested / issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.
Organization	Name of the organization that has been issued with the certificate.
Department	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.
Order Number	Indicates the number assigned by the Certification Authority (CA) for the request.
Serial Number	Displays the serial number of the certificate that is unique and can be used to identify the certificate.
Term	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.
State	Indicates the current status of the certificate.
Requested	The date at which the certificate was requested by the end-user or the administrator
Collected	The date at which the certificate was collected by the end-user or the administrator
Expires	The date of expiry of the certificate

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.
- Clicking the information icon ⓘ displays a tool tip on the chart
- Clicking the graph icon 📊 displays a report with the breakdown of statistics shown in the chart

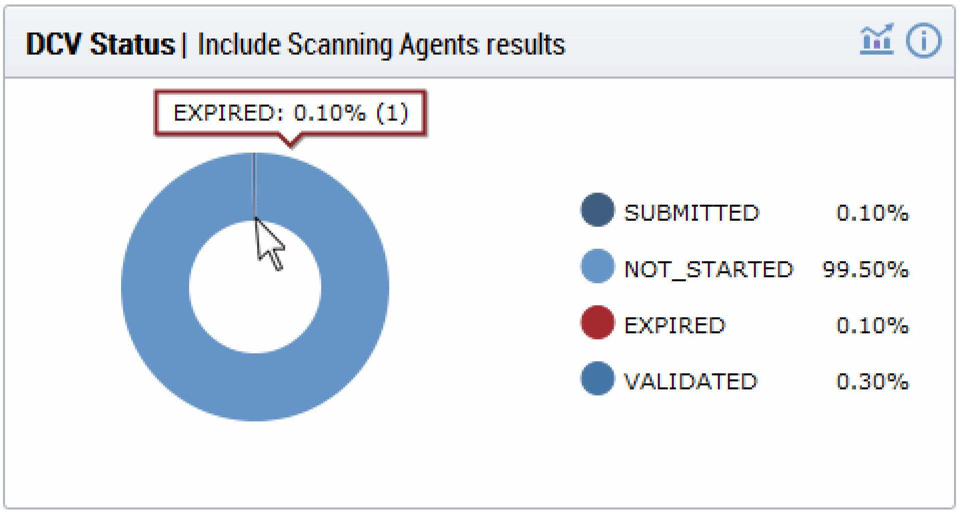


CERTIFICATE TY	ORGANIZATION	DEPARTMENT	ORDER NUMBER	SERIAL NUMBER
SSL	ABCD Company		1299179	4C:40:79:1F:31:93:64:9B:65:A0:55:EF:5F:1E:A8:97
SSL	Best Organization		0	
SSL	Capital Business		0	
SSL	Duncan Gift Shop		0	
SSL	Elegant		1304831	73:29:5D:E2:42:1E:85:B3:EB:43:3C:5D:A0:DE:AC:
SSL	Elegant		1304801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

'Certificates by Duration' Table - Column Descriptions	
Column Header	**Description**
Certificate Type	The domain for which the certificate was requested / issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.
Organization	Name of the organization that has been issued with the certificate.
Department	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.
Order Number	Indicates the number assigned by the Certification Authority (CA) for the request.
Serial Number	Displays the serial number of the certificate that is unique and can be used to identify the certificate.
Term	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.
State	Indicates the current status of the certificate.
Requested	The date at which the certificate was requested by the end-user or the administrator
Collected	The date at which the certificate was collected by the end-user or the administrator
Expires	The date of expiry of the certificate

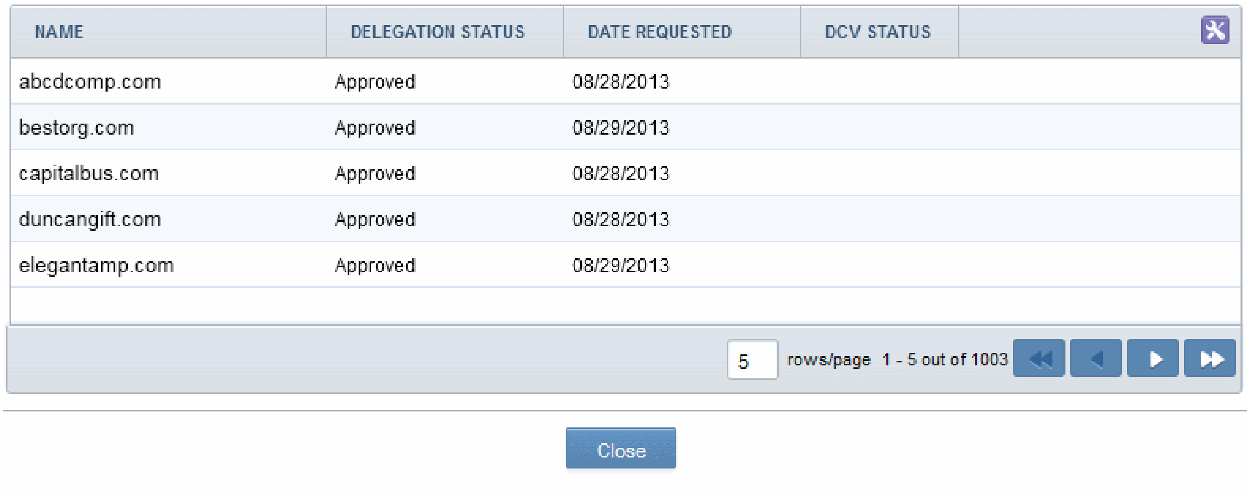
DCV Status

The chart shows a summary of Domain Control Validation (DCV) status of the domains registered with the CM. DCV is required in order for InCommon to issue certificates to your domains and sub-domains. We advise customers to first complete DCV on their registrable domain (e.g. domain.com). Once the domain has passed DCV, then future certificate applications will be faster, because all sub-domains, including wildcards, will also be considered complete.



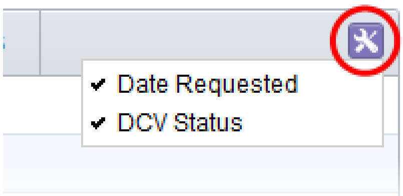
- Hovering your mouse cursor over a legend or section displays the quantity of domains with a particular status and their percentage of the total domains.

- Clicking the information icon ⓘ displays a tool tip on the chart
- Clicking the graph icon displays a report with the breakdown of statistics shown in the chart



NAME	DELEGATION STATUS	DATE REQUESTED	DCV STATUS
abcdcomp.com	Approved	08/28/2013	
bestorg.com	Approved	08/29/2013	
capitalbus.com	Approved	08/28/2013	
duncangift.com	Approved	08/28/2013	
elegantamp.com	Approved	08/29/2013	

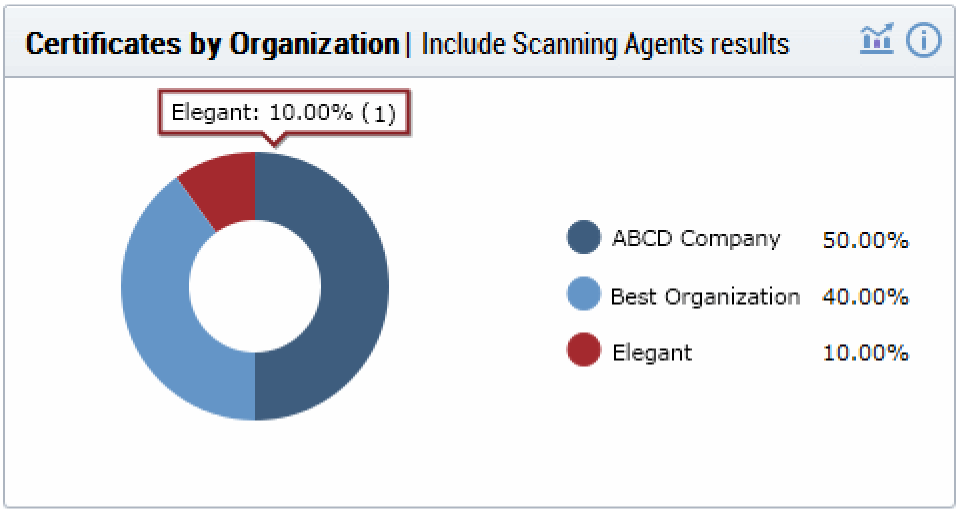
'DCV Status Report' Table - Column Descriptions	
Column Header	**Description**
Name	The name of the domain.
Delegation Status	Indicates the state of the domain within the CM. (Approved, Requested, etc.)
Date Requested	Indicates the date on which the domain was requested.
DCV Status	Indicates the request/approval status of the domain.



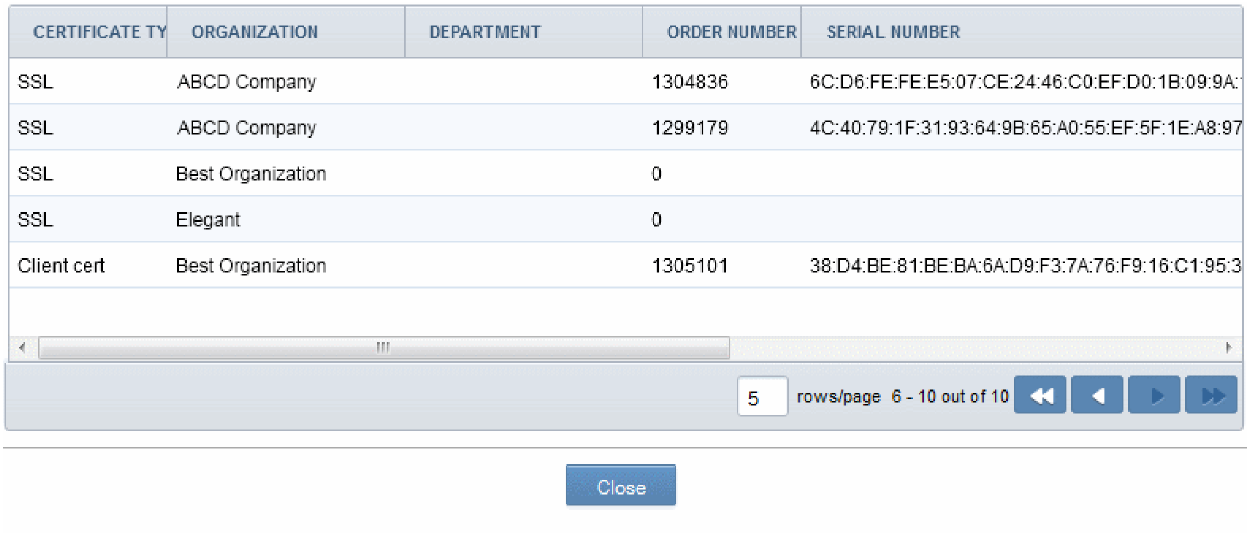
You can select the columns to be displayed by clicking the settings icon at the top right of the table and choosing the columns.

Certificates by Organization

The 'Certificates by Organization' chart shows how many certificates have been issued to each Organization in your InCommon CM 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.
- Clicking the information icon ⓘ displays a tool tip on the chart
- Clicking the graph icon displays a report with the breakdown of statistics shown in the chart



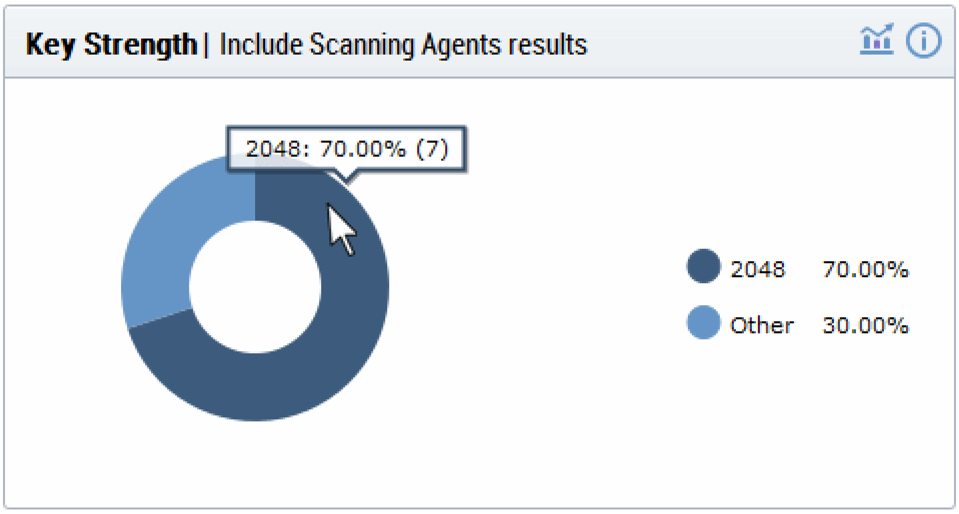
CERTIFICATE TY	ORGANIZATION	DEPARTMENT	ORDER NUMBER	SERIAL NUMBER
SSL	ABCD Company		1304836	6C:D6:FE:FE:E5:07:CE:24:46:C0:EF:D0:1B:09:9A:
SSL	ABCD Company		1299179	4C:40:79:1F:31:93:64:9B:65:A0:55:EF:5F:1E:A8:97
SSL	Best Organization		0	
SSL	Elegant		0	
Client cert	Best Organization		1305101	38:D4:BE:81:BE:BA:6A:D9:F3:7A:76:F9:16:C1:95:3

'Certificates by Organization' Table - Column Descriptions	
Column Header	**Description**
Certificate Type	The domain for which the certificate was requested / issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.
Organization	Name of the organization that has been issued with the certificate.
Department	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.
Order Number	Indicates the number assigned by the Certification Authority (CA) for the request.
Serial Number	Displays the serial number of the certificate that is unique and can be used to identify the

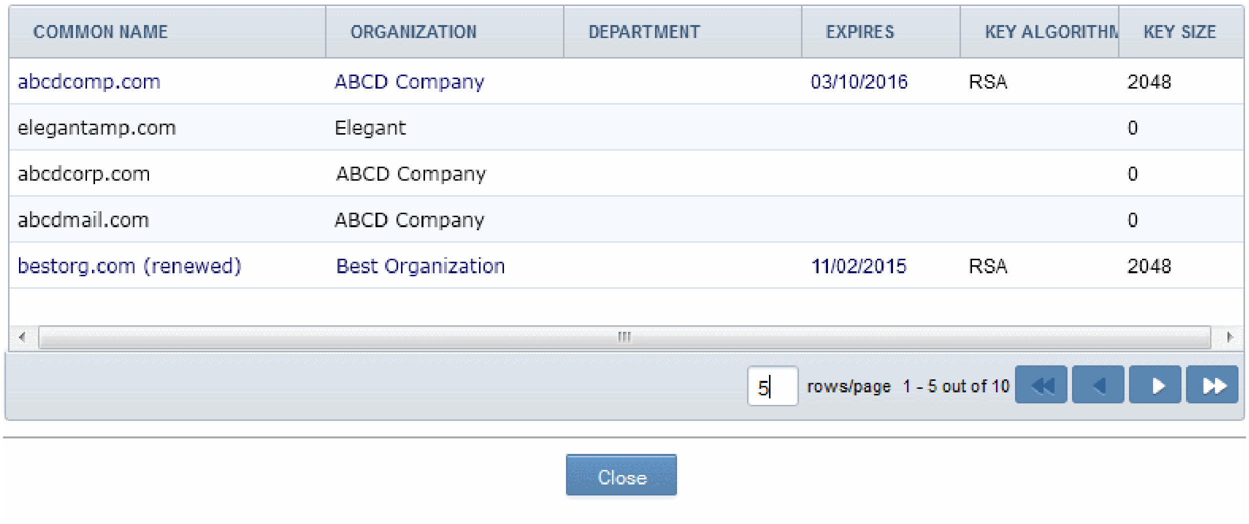
	certificate.
Term	The length of time the certificate is (or will be) valid for from the time of issuance. For certificates that have not yet been approved, this is the certificate lifetime that was requested during the application process.
State	Indicates the current status of the certificate.
Requested	The date at which the certificate was requested by the end-user or the administrator
Collected	The date at which the certificate was collected by the end-user or the administrator
Expires	The date of expiry of the certificate

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, using the RSA algorithm, issued after 1st January 2014 should be of at least 2048 bit in 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.
- Clicking the information icon ⓘ displays a tool tip on the chart
- Clicking the graph icon 📊 displays a report with the breakdown of statistics shown in the chart



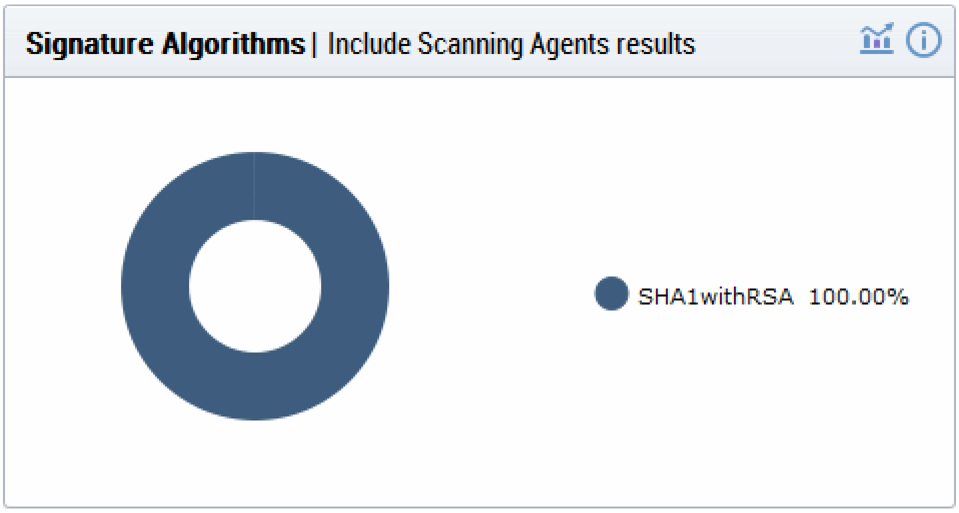
COMMON NAME	ORGANIZATION	DEPARTMENT	EXPIRES	KEY ALGORITHM	KEY SIZE
abcdcomp.com	ABCD Company		03/10/2016	RSA	2048
elegantamp.com	Elegant				0
abcdcorp.com	ABCD Company				0
abcdmail.com	ABCD Company				0
bestorg.com (renewed)	Best Organization		11/02/2015	RSA	2048

'Key Strength Report' Table - Column Descriptions	
Column Header	**Description**
Common Name	The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.
Organization	Name of the organization that has been issued with the certificate.
Department	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.
Expires	The date of expiry of the certificate
Key Algorithm	Displays the type of algorithm used, by the public and private keys, for encryption. (RSA, DSA, EC, etc.)
Key Size	Displays the key size used, on the public and private keys, for encryption. (1024, 2048, 4096, etc.)

Note: Certificates with 'Issued' status are shown with blue text.

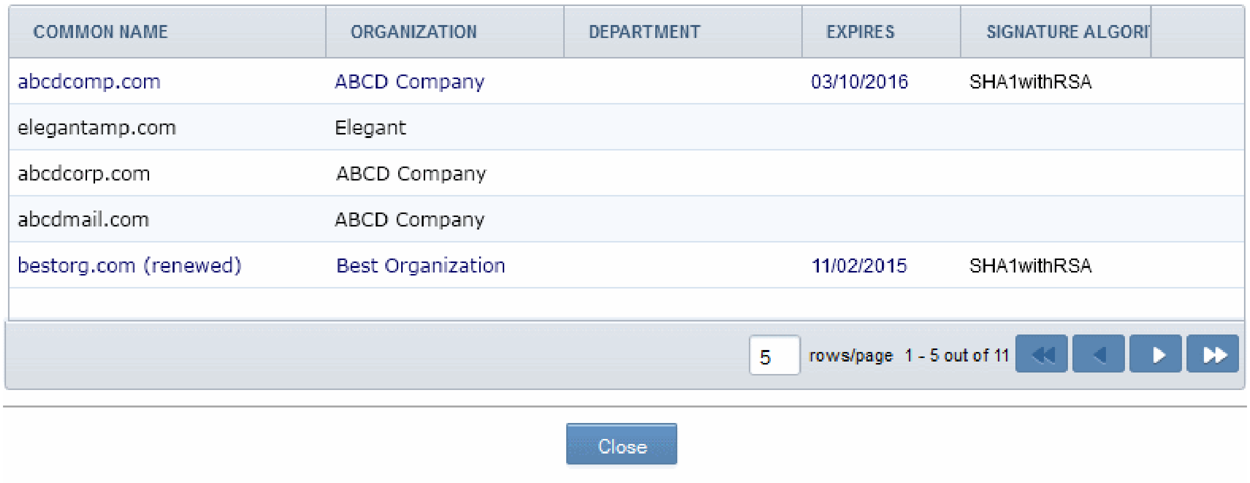
Signature Algorithm

The chart 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. InCommon 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

- 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.
- Clicking the information icon ⓘ displays a tool tip on the chart
- Clicking the graph icon displays a report with the breakdown of statistics shown in the chart



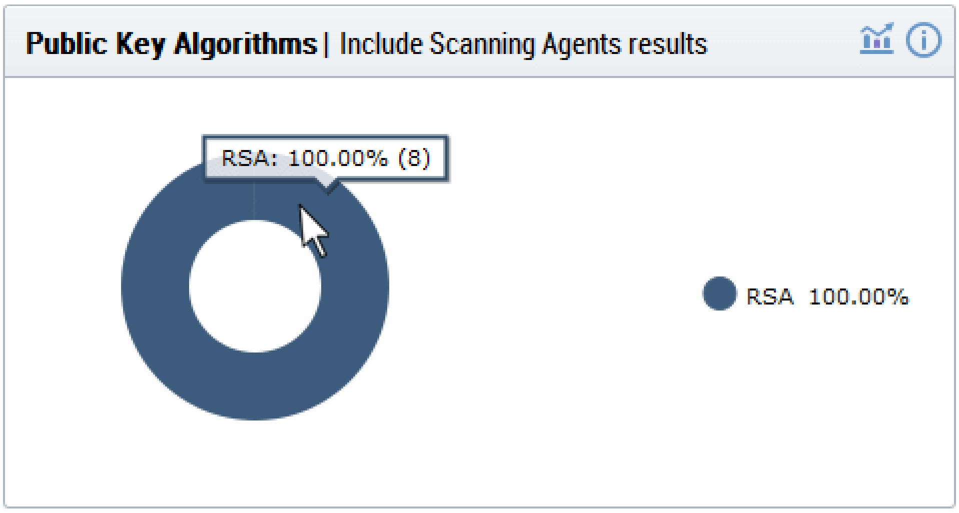
COMMON NAME	ORGANIZATION	DEPARTMENT	EXPIRES	SIGNATURE ALGORI
abcdcomp.com	ABCD Company		03/10/2016	SHA1withRSA
elegantamp.com	Elegant			
abcdcorp.com	ABCD Company			
abcdmail.com	ABCD Company			
bestorg.com (renewed)	Best Organization		11/02/2015	SHA1withRSA

'Signature Algorithm Report' Table - Column Descriptions	
Column Header	**Description**
Common Name	The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.
Organization	Name of the organization that has been issued with the certificate.
Department	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.
Expires	The date of expiry of the certificate
Signature Algorithm	Displays the type of signature algorithm used by the certificate. (SHA1 with RSA, SHA256

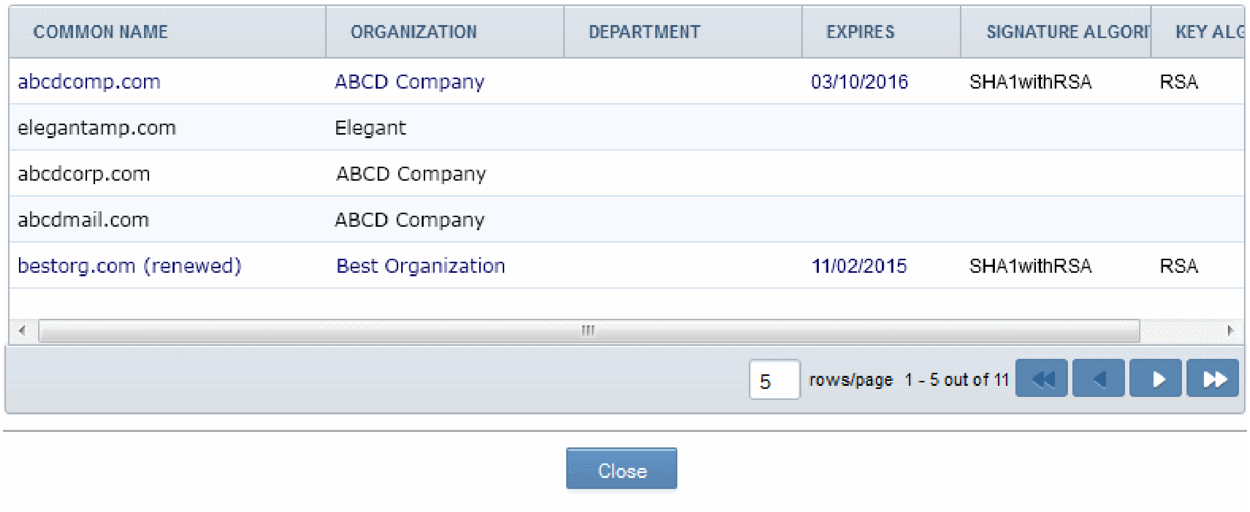
	with RSA,SHA384 with RSA, etc.)

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 public key algorithm and their percentage of the total certificates.
- Clicking the information icon ⓘ displays a tool tip on the chart
- Clicking the graph icon 📈 displays a report with the breakdown of statistics shown in the chart



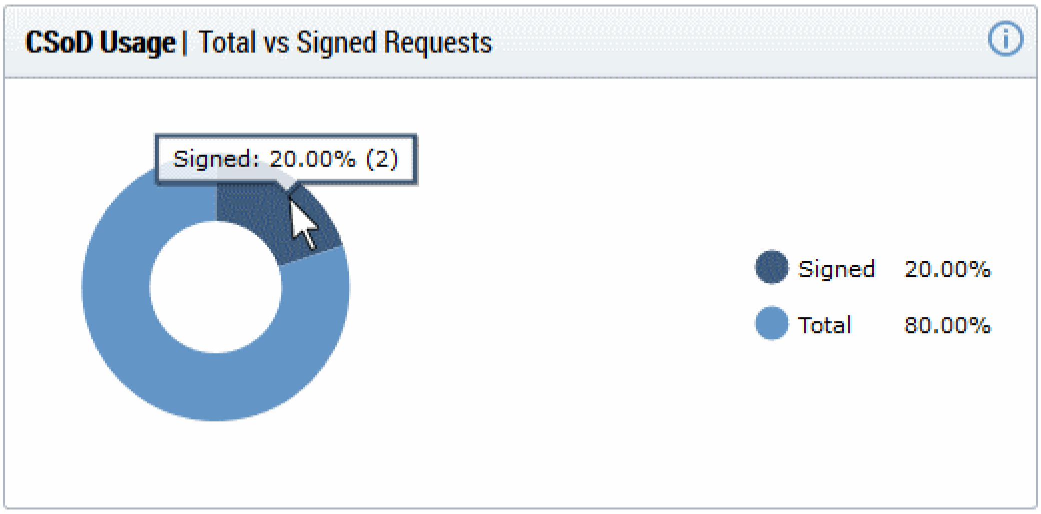
COMMON NAME	ORGANIZATION	DEPARTMENT	EXPIRES	SIGNATURE ALGORI	KEY ALG
abcdcomp.com	ABCD Company		03/10/2016	SHA1withRSA	RSA
elegantamp.com	Elegant				
abcdcorp.com	ABCD Company				
abcdmail.com	ABCD Company				
bestorg.com (renewed)	Best Organization		11/02/2015	SHA1withRSA	RSA

'Public Key Algorithm Report' Table - Column Descriptions	
Column Header	**Description**
Common Name	The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself.

Organization	Name of the organization that has been issued with the certificate.
Department	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.
Expires	The date of expiry of the certificate
Signature Algorithm	Displays the type of signature algorithm used by the certificate. (SHA1 with RSA, SHA256 with RSA, SHA384 with RSA, etc.)
Key Algorithm	Displays the type of algorithm used, by the public and private keys, for encryption. (RSA, DSA, EC, etc.)

CSoD Usage

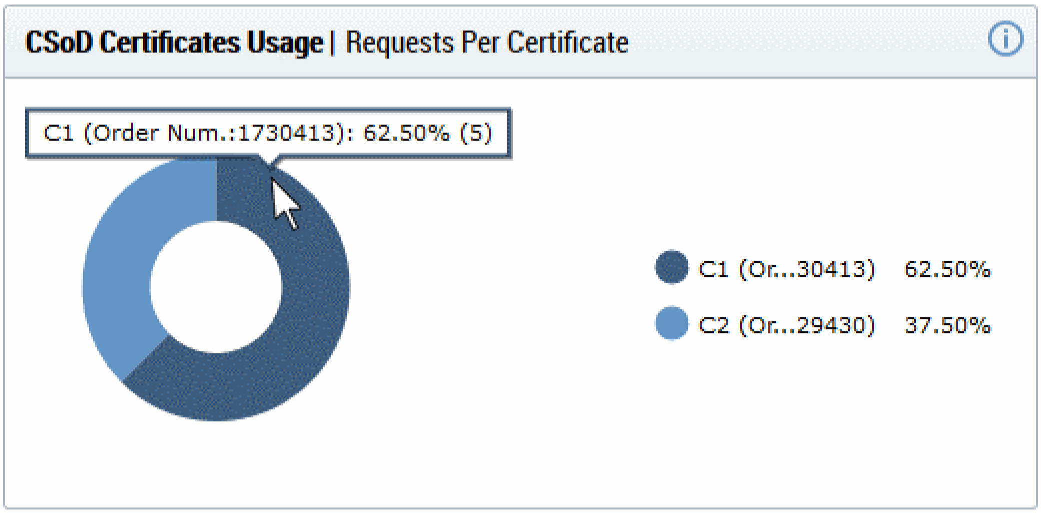
The number of CSoD requests received and the number of those that we eventually signed.



- Place your mouse cursor over a chart section to view the exact number of requests in that category.

CSoD Certificates Usage

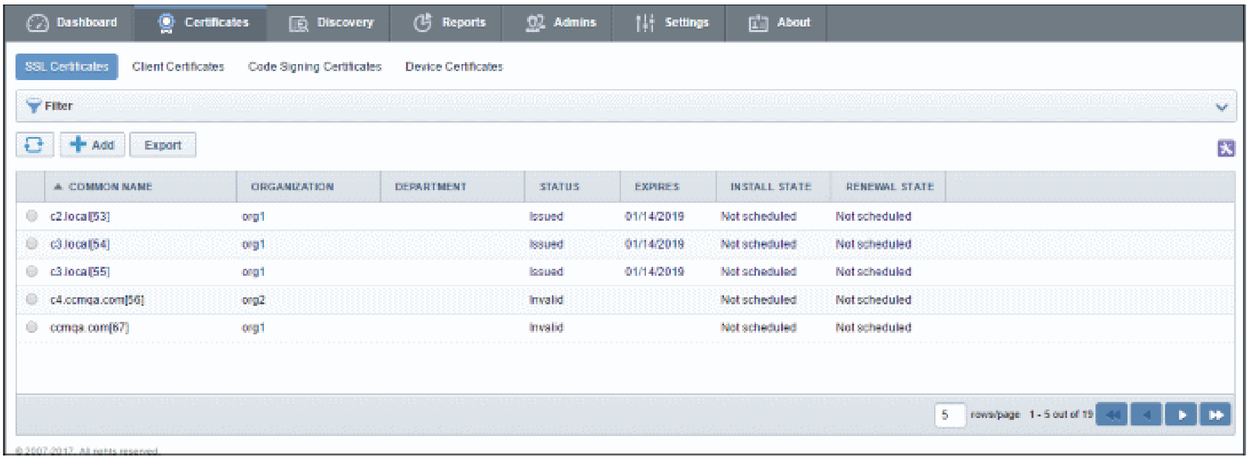
CSoD requests broken down by signing certificate.


CSoD Certificates Usage | Requests Per Certificate
C1 (Order Num.:1730413): 62.50% (5)
C1 (Or...30413) 62.50%
C2 (Or...29430) 37.50%

- Place your mouse cursor over a chart section to view the certificate order number and the exact number of requests signed with that certificate.

3 Certificates Management

- The 'Certificates' tab provides appropriately privileged administrators with the ability to request, collect, revoke and manage SSL and Client, Code Signing.
- It is divided into four main administrative areas, namely:
  - The SSL Certificates tab
  - The Client Certificates tab
  - The Code Signing Certificates tab



	▲ COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
○	c2.local[53]	org1		Issued	01/14/2019	Not scheduled	Not scheduled
○	c3.local[54]	org1		Issued	01/14/2019	Not scheduled	Not scheduled
○	c3.local[55]	org1		Issued	01/14/2019	Not scheduled	Not scheduled
○	c4.ccmqa.com[56]	org2		Invalid		Not scheduled	Not scheduled
○	ccmqa.com[67]	org1		Invalid		Not scheduled	Not scheduled

5 rows/page 1 - 5 out of 15
© 2007-2017. All rights reserved.

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.SSL Certificates Area- High level introduction to the SSL interface. Contains brief explanations of functionality and an overview of Incommon 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 Sign 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.

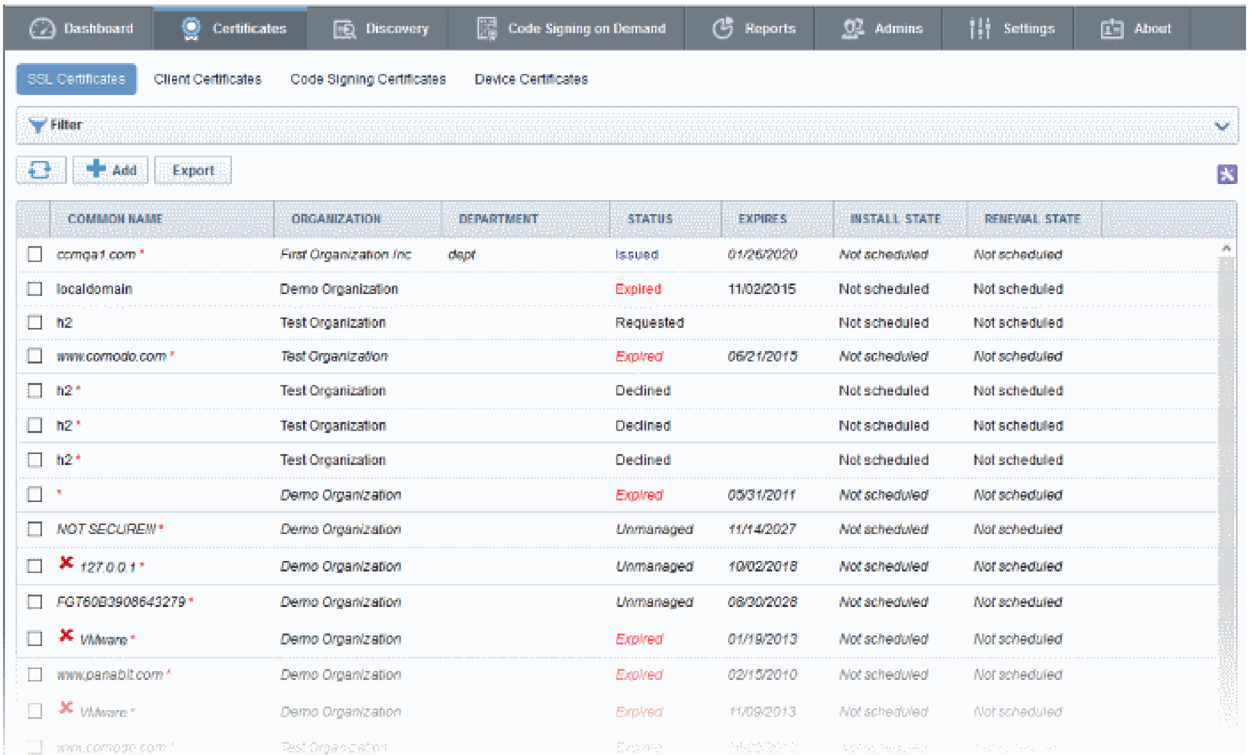
Note: Administrators can also run a 'Discovery Scan' on their servers which will audit and monitor their entire network for all installed SSL certificates (including certificates issued by other vendors). Once completed, all discovered certificates are automatically imported into the 'Certificates Management' 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 RAO / DRAO SSL administrators with the information and controls necessary to manage the life-cycle of SSL certificates for an organization.

- RAO SSL admins can request and manage certificates for their delegated organization(s). They can approve or decline certificate requests for their organization.
- DRAO SSL admins can request SSL certificates for domains belonging to their delegated department(s). They can approve or decline certificate requests for their department.



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
□	ccmqa1.com *	First Organization Inc	dept	Issued	01/26/2020	Not scheduled	Not scheduled
□	localdomain	Demo Organization		Expired	11/02/2015	Not scheduled	Not scheduled
□	h2	Test Organization		Requested		Not scheduled	Not scheduled
□	www.comodo.com *	Test Organization		Expired	06/21/2015	Not scheduled	Not scheduled
□	h2 *	Test Organization		Declined		Not scheduled	Not scheduled
□	h2 *	Test Organization		Declined		Not scheduled	Not scheduled
□	h2 *	Test Organization		Declined		Not scheduled	Not scheduled
□	*	Demo Organization		Expired	05/31/2011	Not scheduled	Not scheduled
□	NOT SECURE!!! *	Demo Organization		Unmanaged	11/14/2027	Not scheduled	Not scheduled
□	✗ 127.0.0.1 *	Demo Organization		Unmanaged	10/02/2018	Not scheduled	Not scheduled
□	FGT60B3908643279 *	Demo Organization		Unmanaged	08/30/2028	Not scheduled	Not scheduled
□	✗ VMware *	Demo Organization		Expired	01/19/2013	Not scheduled	Not scheduled
□	www.panabit.com *	Demo Organization		Expired	02/15/2010	Not scheduled	Not scheduled
□	✗ VMware *	Demo Organization		Expired	11/09/2013	Not scheduled	Not scheduled
□	www.comodo.com *	Test Organization		Expired	[illegible]	[illegible]	[illegible]

Note: The SSL Certificates area is visible only to RAO / DRAO SSL administrators.

SSL Certificates Sub-tab - Table of Parameters

Field Name		Description
Subject Alt Name		Displays the names of domain(s) for which the certificate is used for.
City		Name of the organization that requested or has been issued with the certificate listed in the 'Common Name' column.
State		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.
Country		Displays the name of the country entered while creating the Organization / Department.
	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 RAO SSL administrator- or organizations and departments of 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 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 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 email cmvalidation@comodo.com with the order number.
	Issued (number of found certificates)	• The certificate was issued by Comodo and collected by Certificate Manager. • A blue font color (Issued) means that the certificate was issued by CA but was not installed. • Place your mouse cursor over the '**Common Name**' to view the name of the vendor 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. • Place your mouse cursor over the 'State' column to display all the IP address / Port combinations that this certificate was found on.
	Expired	• The certificate is invalid because its term has expired. • Placing your 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 your 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 your 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 your 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 auto-installation feature or the Self Enrollment Form or the Built-in Enrollment Form has been rejected by one of the following: - 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 Incommon Certificate Manager (including any pre-existing Incommon 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 your 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 your mouse cursor over the '**State**' column will display all the IP address / Port combinations that this certificate was found on.
Signature Algorithm		Date when the certificate expires.
Key Algorithm		Displays the type of algorithm used for the encryption.
	Not Scheduled	The certificate is not scheduled for auto-installation.
	Scheduled	The certificate is scheduled for auto-installation.
	Started	Certificate installation on the remote server has started as per the schedule
	Successful	Certificate was successfully installed on the remote server at the scheduled time
	Failed	Certificate installation on the remote server failed
Key Size		Displays the key size used by certificate for the encryption.
	Not Scheduled	The certificate is not scheduled for auto-renewal
	Scheduled	A schedule has been set for auto-renewal of the certificate
	Started	The auto-renewal process has been started as per the schedule
	Successful	The certificate has been auto-renewed and installed successfully
	Failed	Auto-renewal of the certificate has failed

MD5 Hash Displays the MD5 hash (thumbprint/fingerprint) for the certificate.		
SHA1 Hash		Displays the SHA1 hash (thumbprint/fingerprint) for the certificate.
Private Key		Indicates whether the private key of the certificate is managed by Incommon CM
Key Usage		The cryptographic purpose(s) for which the certificate can be used. For example, key encipherment and signing.
Extended Key Usage		Higher level capabilities of the certificate. For example, web server authentication and client authentication.
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 Incommon CA (the issuing Certificate Authority). Once submitted, the certificate's state will change to 'Applied'. If the request is approved by Incommon CA, the certificate State changes to 'Issued'. If the request was declined by Incommon CA because of incorrect enrollment details (for example, a mistake in the CSR or other form value), then 'State' will be listed as 'Invalid'. If the request was declined by Incommon CA for legal reasons then the certificate will have a status of 'Rejected'. Certificate requests can be approved by: 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 Incommon 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. Set Auto Renewal & Installation Create a schedule for auto-renewing a certificate in advance of its expiry, and to configure auto-installation of the renewed certificate. See the section Scheduling Automatic Renewal and Installation for more details.

Requester		Displays the name of the Incommon CM 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.
State		Displays the name of the state/province entered while creating the organization / department.
Country		Displays the name of the country entered while creating the organization / department.
Signature Algorithm		Displays the signature algorithm used by the certificate.
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 (thumbprint/fingerprint) for the certificate.
SHA1 Hash		Displays the SHA1 hash (thumbprint/fingerprint) for the certificate.
Private Key		Indicates whether the private key of the certificate is managed by Incommon CM
Key Usage		The cryptographic purpose(s) for which the certificate can be used. For example, key encipherment and signing.
Extended Key Usage		Higher level capabilities of the certificate. For example, web server authentication and client authentication.
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 and sends the request for the certificate to Incommon CA (the issuing Certificate Authority). • Once submitted, the certificate 'State' will change to 'Applied'. • If the request is approved by Incommon CA, the certificate State changes to 'Issued'.

		• If the request was declined by Incommon CA because of incorrect enrollment details (for example, a mistake in the CSR or other form value), then 'State' will be listed as 'Invalid'. • If the request was declined by Incommon CA for legal reasons then the certificate will have a status of 'Rejected'. • Certificate requests can be approved by: • 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 Incommon Certificate Authority for processing.
	Edit	• Modify SSL certificate parameters. • This option is available only for certificates with a state of 'Requested', 'Rejected' or 'Invalid'.
	Renew	• Opens the 'Renew Certificate' dialog which will be pre-populated with the company and domain details of the existing certificate. • Click 'OK' to submit the certificate renewal request. • This control is available only for the certificates states of: Issued, Expired and Unmanaged.
	Set Auto Renewal & Installation	Create a schedule for auto-renewing a certificate in advance of its expiry, and to configure auto-installation of the renewed certificate. See the section Scheduling Automatic Renewal and Installation for more details.

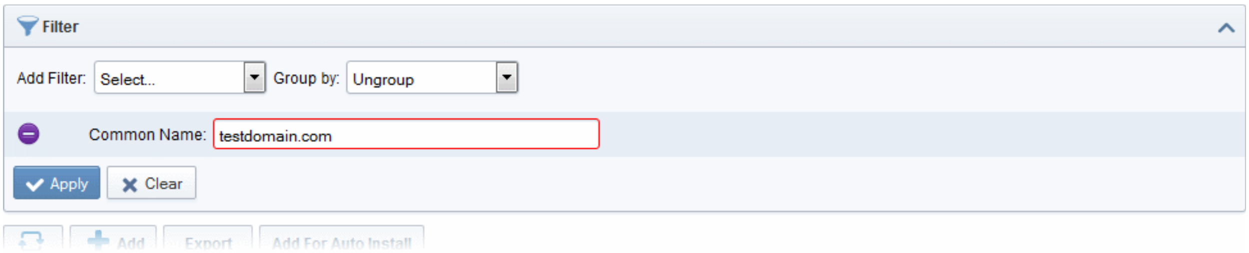
3.1.1.1 Sorting and Filtering Options

- Click a column header to sort items in order of the entries in the column.

- To apply filters, click on the down arrow at the right end of the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the results with other options that appears depending on the selection from the 'Add Filter' drop-down.

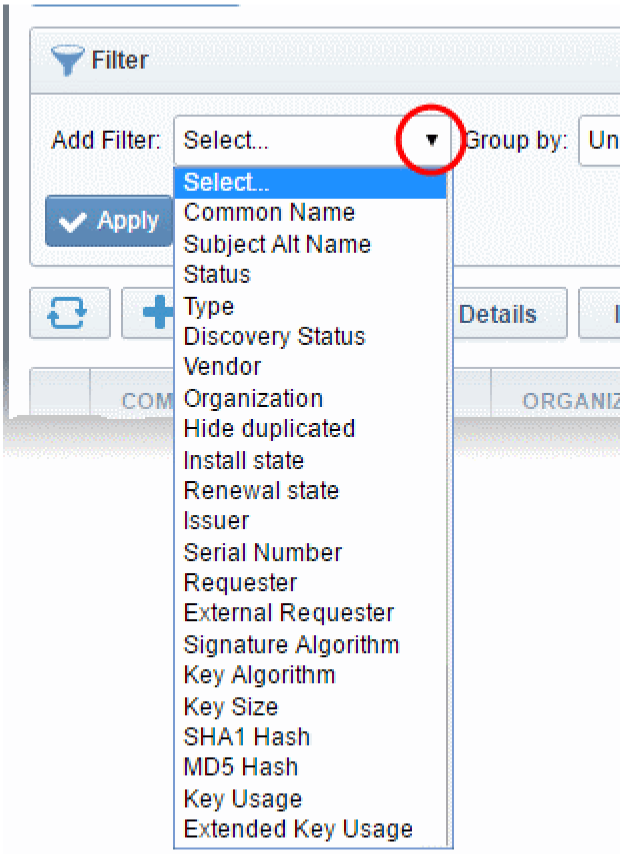
To add a filter

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



Common Name: testdomain.com

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



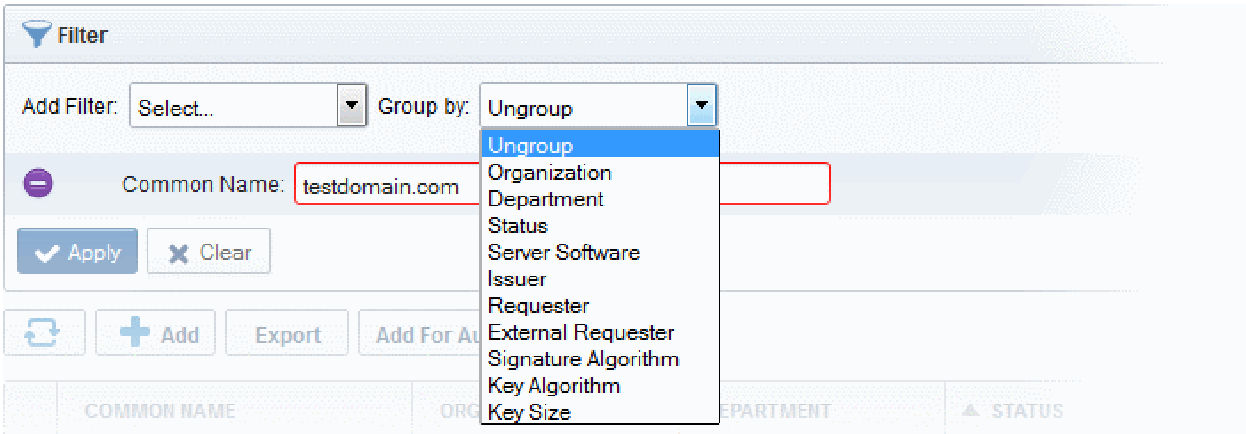
The available filter criteria and their filter parameters are given in the following table:

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 'State' 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 CM 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.
Key Algorithm	Enter the key algorithm of the certificate.
Key Size	Enter the key size in bits.
SHA1 Hash	Enter the SHA1 Hash (thumbprint/fingerprint) of the certificate
MD5 Hash	Enter the MD5 Hash (thumbprint/fingerprint) of the certificate
Key Usage	Filter certificates by cryptographic capabilities.
Extended Key Usage	Filter certificates by higher level purpose. E.g. web server authentication..

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

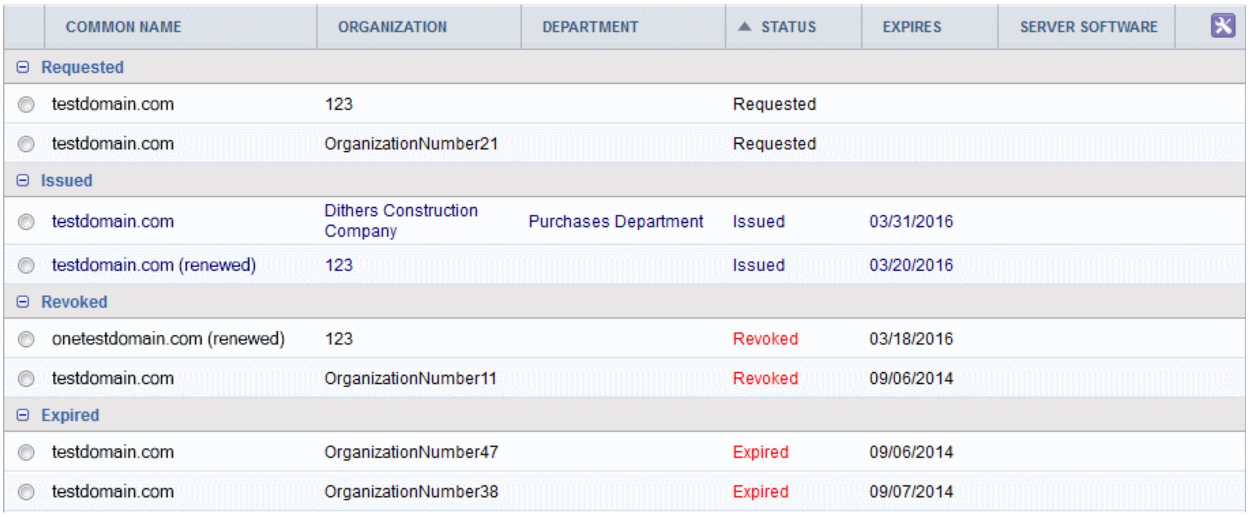


Add Filter: Select...

Group by: Ungroup

Common Name: testdomain.com

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



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

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

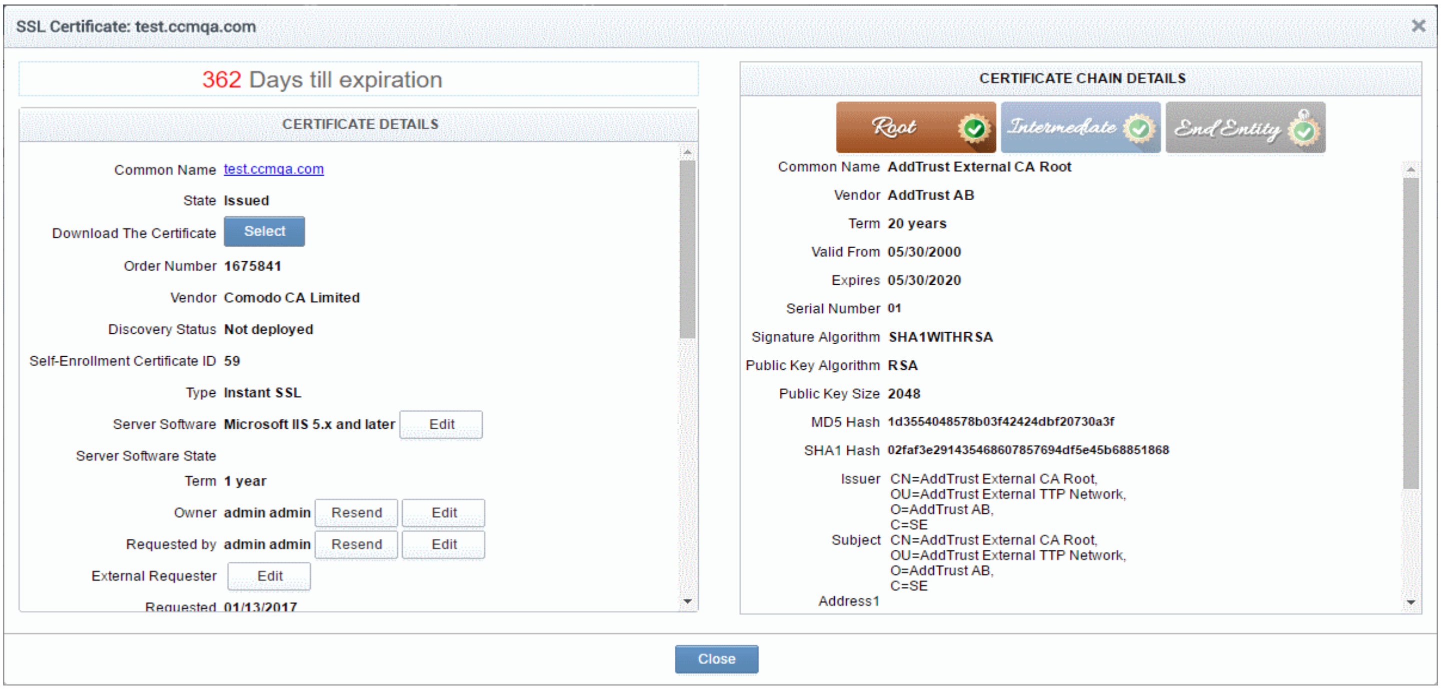
Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'SSL certificates' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear'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

3.1.1.2 SSL Certificate 'Details' Dialog

- Click 'Certificates' > 'SSL Certificates'
- Select a certificate in the list
- Click 'Details'

The SSL Certificate 'Details' dialog displays complete details about a cert and allows administrators to:

- Download the certificate in different formats for installation onto servers
- Upload the certificate's private key to Incommon CM's private key store
- Download the certificate's private key from the private key store
- View full certificate chain and installation details
- Resend the notification email to the requester of the issued certificate
- Restart Apache after auto-installation of the certificate
- Update auto-renewal status



362 Days till expiration

CERTIFICATE DETAILS

Common Name	test.ccmqa.com
State	Issued
Download The Certificate	Select
Order Number	1675841
Vendor	Comodo CA Limited
Discovery Status	Not deployed
Self-Enrollment Certificate ID	59
Type	Instant SSL
Server Software	Microsoft IIS 5.x and later
Server Software State	
Term	1 year
Owner	admin admin
Requested by	admin admin
External Requester	
Requested	01/13/2017

CERTIFICATE CHAIN DETAILS

Common Name	AddTrust External CA Root
Vendor	AddTrust AB
Term	20 years
Valid From	05/30/2000
Expires	05/30/2020
Serial Number	01
Signature Algorithm	SHA1WITHRSA
Public Key Algorithm	RSA
Public Key Size	2048
MD5 Hash	1d3554048578b03f42424dbf20730a3f
SHA1 Hash	02faf3e291435468607857694df5e45b68851868

Issuer	CN=AddTrust External CA Root,
	OU=AddTrust External TTP Network,
	O=AddTrust AB,
	C=SE

Subject	CN=AddTrust External CA Root,
	OU=AddTrust External TTP Network,
	O=AddTrust AB,
	C=SE

Address1	

The certificate details dialog contains two panes:

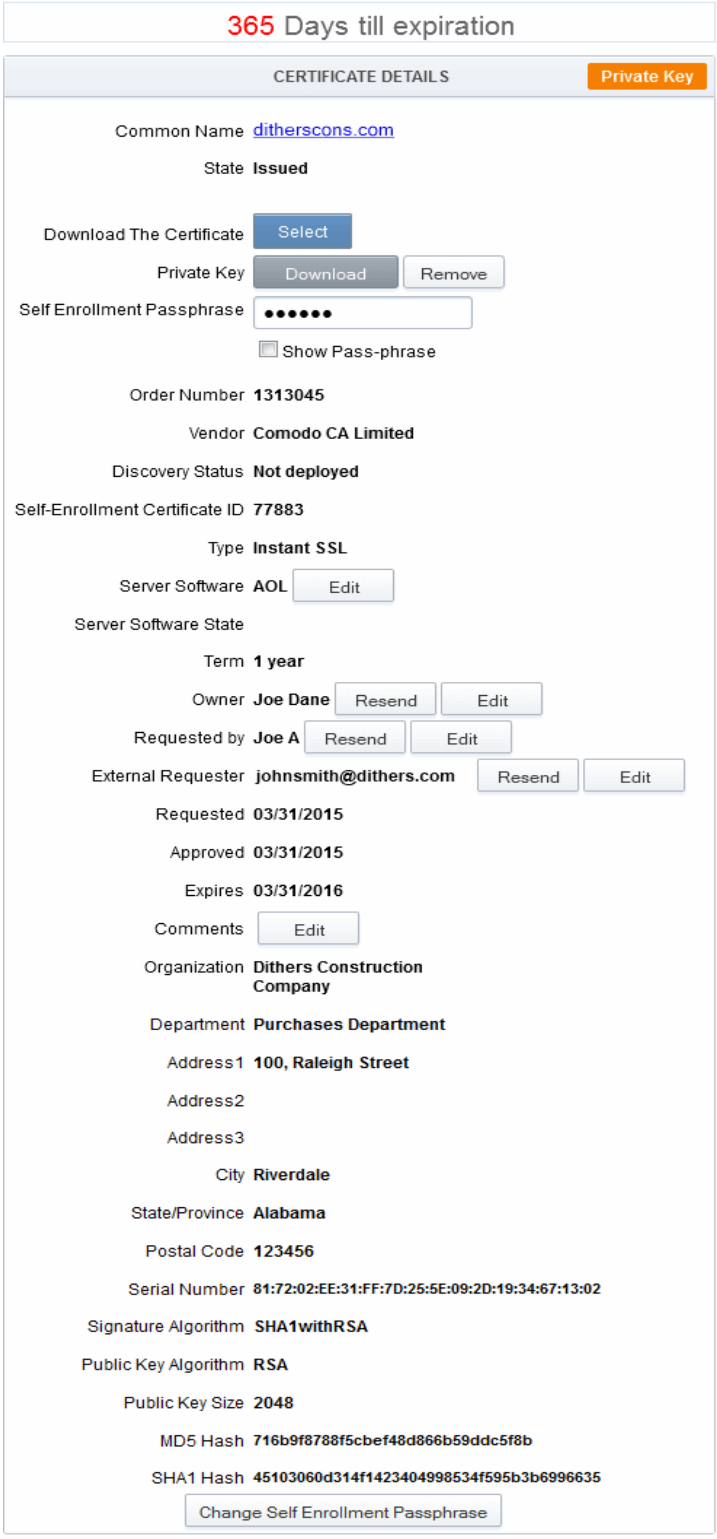
- Certificate Details
- Certificate Chain Details

Certificate Details

The top of the 'Certificate Details' pane displays the number of days remaining before the certificate expires. The lower section shows Incommon CM and server related information about the certificate and contains various other controls. The precise contents of the 'Certificate Details' pane is dependent on the current 'State' of the certificate:

SSL Certificate with 'Issued' state

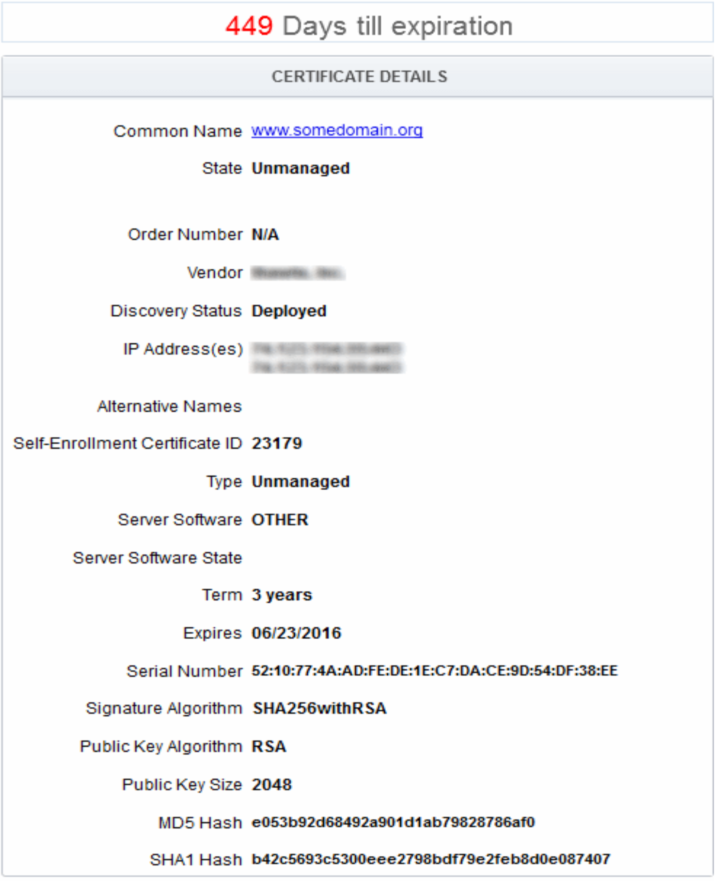
SSL Certificate with 'Unmanaged' state



365 Days till expiration

CERTIFICATE DETAILS

Common Name	ditherscons.com
State	Issued
Download The Certificate	Select
Private Key	Download Remove
Self Enrollment Passphrase	••••••
	□ Show Pass-phrase
Order Number	1313045
Vendor	Comodo CA Limited
Discovery Status	Not deployed
Self-Enrollment Certificate ID	77883
Type	Instant SSL
Server Software	AOL Edit
Server Software State	
Term	1 year
Owner	Joe Dane Resend Edit
Requested by	Joe A Resend Edit
External Requester	johnsmith@dithers.com Resend Edit
Requested	03/31/2015
Approved	03/31/2015
Expires	03/31/2016
Comments	Edit
Organization	Dithers Construction Company
Department	Purchases Department
Address1	100, Raleigh Street
Address2	
Address3	
City	Riverdale
State/Province	Alabama
Postal Code	123456
Serial Number	81:72:02:EE:31:FF:7D:25:5E:09:2D:19:34:67:13:02
Signature Algorithm	SHA1withRSA
Public Key Algorithm	RSA
Public Key Size	2048
MD5 Hash	716b9f8788f5cbef48d866b59ddc5f8b
SHA1 Hash	45103060d314f1423404998534f595b3b6996635



449 Days till expiration

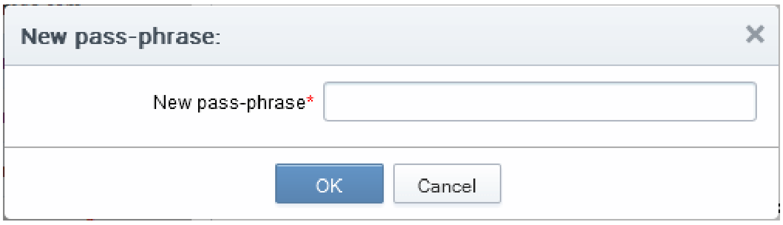
CERTIFICATE DETAILS

Common Name	www.somedomain.org
State	Unmanaged
Order Number	N/A
Vendor	[redacted]
Discovery Status	Deployed
IP Address(es)	[redacted]
Alternative Names	
Self-Enrollment Certificate ID	23179
Type	Unmanaged
Server Software	OTHER
Server Software State	
Term	3 years
Expires	06/23/2016
Serial Number	52:10:77:4A:AD:FE:DE:1E:C7:DA:CE:9D:54:DF:38:EE
Signature Algorithm	SHA256withRSA
Public Key Algorithm	RSA
Public Key Size	2048
MD5 Hash	e053b92d68492a901d1ab79828786af0
SHA1 Hash	b42c5693c5300eee2798bdf79e2feb8d0e087407

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).
Download	Control	Download the certificate in different formats.
Private Key	Control	For certificates enrolled by manually entering the CSR • Allows administrators to upload the certificate's private key to the private key store. For certificates requested via by Incommon CM and whose keys are managed by the private key store • Allows administrators to download the private key of the certificate in .key format. For more details, see: • Uploading private key of a certificate • Downloading the private key of a certificate **Note**: The Private Key field is displayed only if the Private Key Store feature is enabled for your account and a Private Key Store controller is installed on your local network and configured.
Pass Phrase	Text Field	The Pass Phrase of the certificates enrolled by auto-generation of CSR by InCommon CM and whose keys are managed by Private Key Store. The passphrase is displayed if 'Show Pass-phrase' checkbox is selected. This phrase is required to import the certificate on to any server, after downloading the certificate in .p12 format. **Note**: The Pass Phrase field is displayed only if the Private Key Store feature is enabled for your account and a Private Key Store controller is installed on your local network and configured.
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**. • **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	Displays the brand name of the certificate.
Server Software	Text Field	Indicates the server type on which the certificate was issued.

SSL Certificates 'Details' Dialog - Table of Parameters		
Field	**Type**	**Description**
		- Clicking 'View' allows you to view the installation status of the deployed certificate. Refer to the section Viewing the installation details of the certificate for more details. - Clicking 'Edit' allows you to change the Server Software for which the certificate is intended.
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.
External Requester	Text Field	The email address of the applicant on behalf of whom the administrator has applied for this certificate through the built-in application form in the CM interface, as an alternative to making an applicant to complete the 'Self Enrollment 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.

SSL Certificates 'Details' Dialog - Table of Parameters		
Field	**Type**	**Description**
Signature Algorithm	Text Field	Displays the signature algorithm of the public key of the certificate

SSL Certificates 'Details' Dialog - Table of Parameters		
Field	**Type**	**Description**
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.)
MD5 Hash	Text Field	Displays the MD5 Hash (thumbprint/fingerprint) value of the certificate
SHA1 Hash	Text Field	Displays the SHA1 Hash (thumbprint/fingerprint) value of the certificate
Key Usage	Text Field	The cryptographic purpose(s) for which the certificate can be used. For example, key encipherment and signing.
Extended Key Usage	Text Field	Higher level capabilities of the certificate. For example, web server authentication.
Change Pass Phrase	Control	Set or change the self-enrollment pass-phrase of the certificate. This phrase is required to revoke certificates should the situation arise.  New pass-phrase: New pass-phrase*
Auto-renewal	Control	Enable / Disable automatic renewal of the certificate

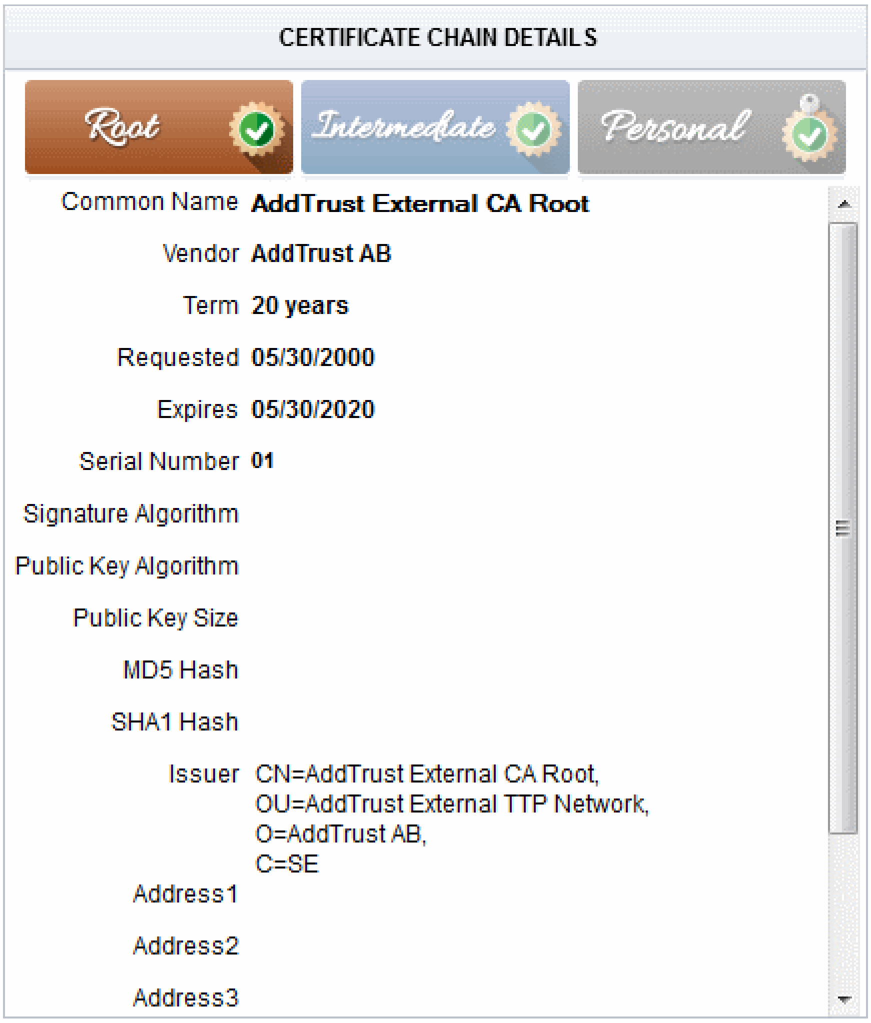
The following sections explain in detail on the tasks that can be accomplished from the 'Certificate Details' pane.

- Uploading private key of a certificate for storage and management by the Private Key Store
- Downloading private key of a certificate
- Resending Notification Email for Certs with 'Issued' State
- Viewing Installation Details of Certificates
- Restarting Apache after Auto-Installation of SSL Certificate
- Update auto-renewal status

Certificate Chain Details

The 'Certificate Chain Details' pane displays the details of the 'Root' and 'Intermediate' certificates linked to the SSL certificate chain.

- Clicking the 'Root', 'Intermediate' and the 'Personal' tabs, displays the certificate details of the Root, Intermediate and the self SSL certificate respectively.



Common Name	AddTrust External CA Root
Vendor	AddTrust AB
Term	20 years
Requested	05/30/2000
Expires	05/30/2020
Serial Number	01
Signature Algorithm	
Public Key Algorithm	
Public Key Size	
MD5 Hash	
SHA1 Hash	

Issuer	CN=AddTrust External CA Root,
	OU=AddTrust External TTP Network,
	O=AddTrust AB,
	C=SE

Address1	
Address2	
Address3	

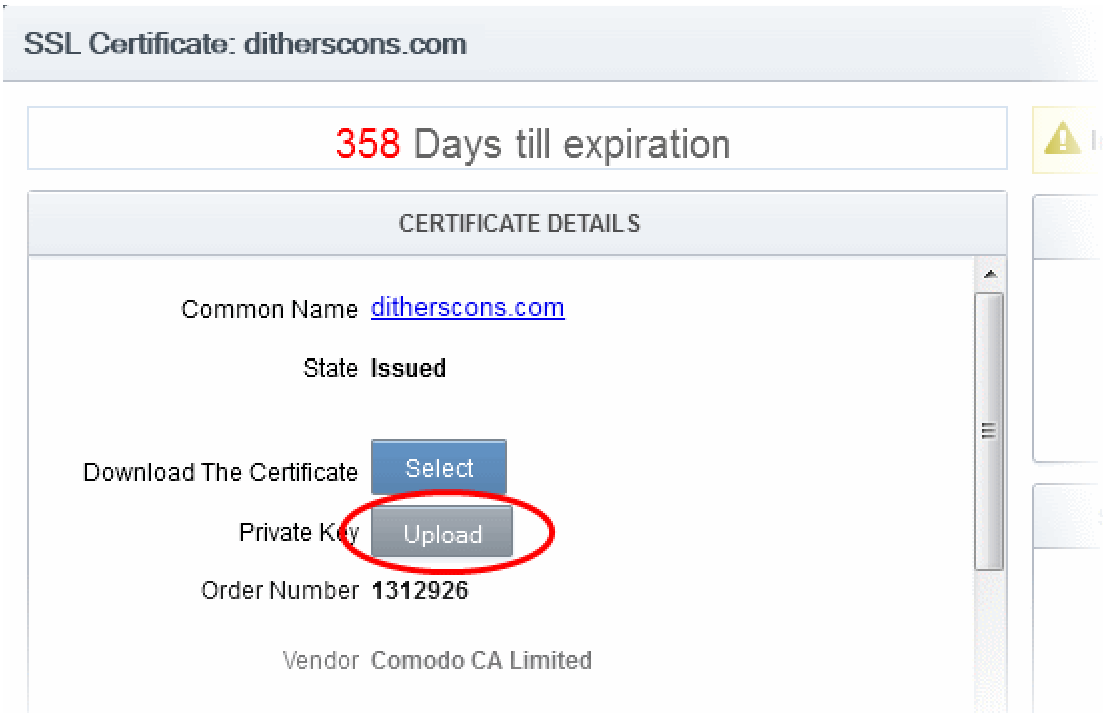
3.1.1.2.1 Uploading Private Key of a Certificate for Storage and Management by the Private Key Store

The 'Details' dialog for SSL certificates with 'Issued' state allows the administrator to upload the private key associated with it, for storage and management by the Private Key Store configured in their local network. Managing the private key in the key store facilitates:

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

Prerequisite - Your account should have been enabled for Private Key Store feature. The Private Key Store controller should have been installed on your local network and configured by the Master Administrator.

The 'Certificate Details' pane of the details dialog for the SSL certificate with the Issued state, displays a 'Upload' button beside the 'Private Key' field.



SSL Certificate: ditherscons.com

358 Days till expiration

CERTIFICATE DETAILS

Common Name ditherscons.com

State **Issued**

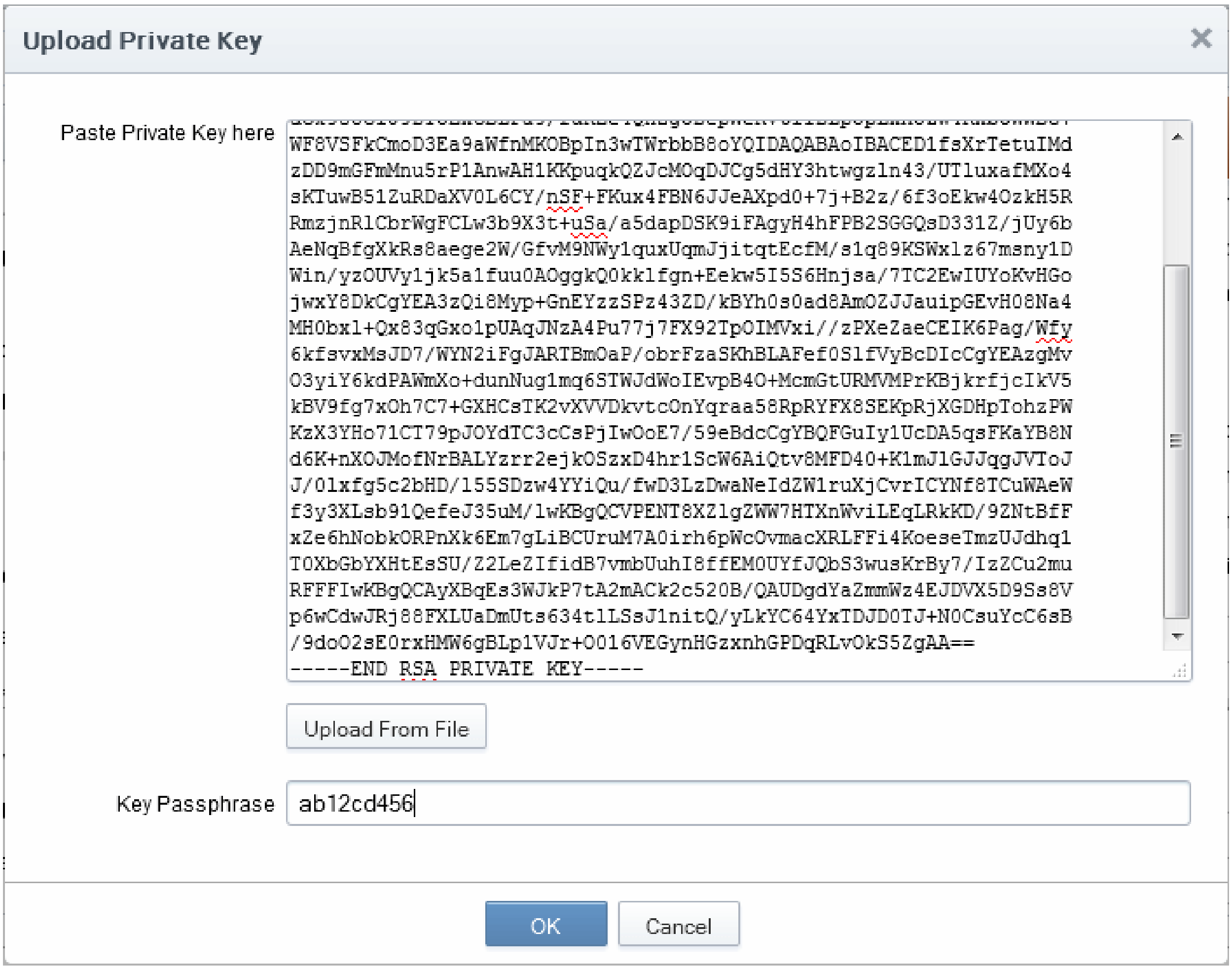
Download The Certificate

Private Key

Order Number **1312926**

Vendor Comodo CA Limited

- Clicking the 'Upload' button will open the 'Upload Private Key' dialog.



Upload Private Key

Paste Private Key here

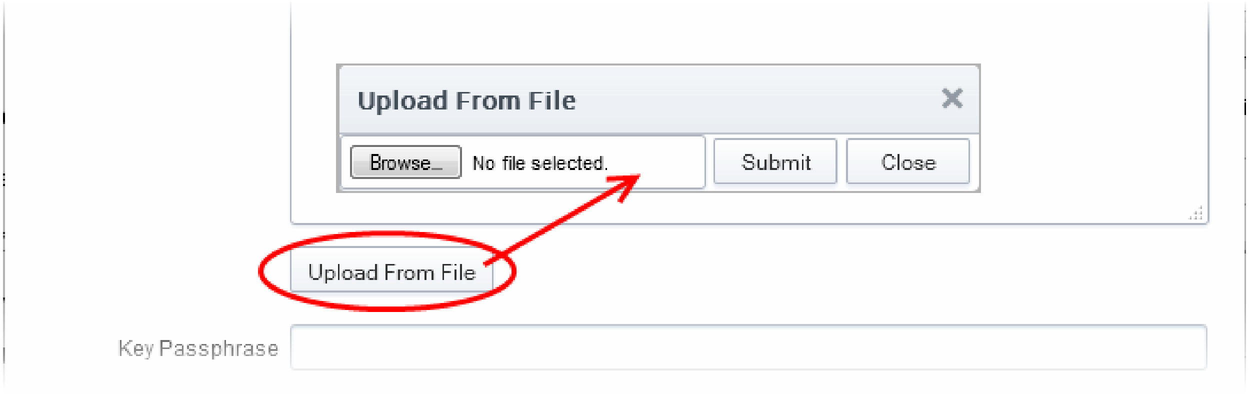
```
WF8VSFkCmoD3Ea9aWfnMKOBpIn3wTWrbbB8oYQIDAQABAoIBACED1fsXrTetuIMd
zDD9mGFmMnu5rP1AnwAH1KKpuqkQZJcMOqDJCg5dHY3htwgzln43/UTluxafMXo4
sKTuwB51ZuRDaXV0L6CY/nSF+FKux4FBN6JJeAXpd0+7j+B2z/6f3oEkw4OzkH5R
RmzjnRlCbrWgFCLw3b9X3t+uSa/a5dapDSK9iFAgyH4hFPB2SGGQsD331Z/jUy6b
AeNqBfgXkRs8aege2W/GfvM9NWy1quxUqmJjitqtEcfM/s1q89KSWxlz67msny1D
Win/yzOUVy1jk5a1fuu0AOggkQ0kklfgn+Eekw5I5S6Hnjsa/7TC2EwIUYoKvHGo
jwxY8DkCgYEA3zQi8Myp+GnEYzzSPz43ZD/kBYh0s0ad8AmOZJJauipGEvH08Na4
MH0bxl+Qx83qGxo1pUAqJNzA4Pu77j7FX92TpOIMVxi//zPXeZaeCEIK6Pag/Wfy
6kfsvxMsJD7/WYN2iFgJARTBmOaP/obrFzaSKhBLAFef0SlfVyBcDIcCgYEAzgMv
O3yiY6kdPAWmXo+dunNug1mq6STWJdWoIEvpB4O+McmGtURMVMPrKBjkrfjcIkV5
kBV9fg7xOh7C7+GXHCsTK2vXVVDkvtcOnYqraa58RpRYFX8SEKpRjXGDHpTohzPW
KzX3YHo71CT79pJOYdTC3cCsPjIwOoE7/59eBdcCgYBQFGuIy1UcDA5qsFKaYB8N
d6K+nXOJMofNrBALYzrr2ejkOSzxD4hr1ScW6AiQtv8MFD40+K1mJ1GJJqgJVToJ
J/01xfg5c2bHD/155SDzw4YYiQu/fwD3LzDwaNeIdZW1ruXjCvrICYNf8TCuWAeW
f3y3XLsb91QefeJ35uM/1wKBgQCVPENT8XZ1gZWW7HTXnWviLEqLRkKD/9ZNtBfF
xZe6hNobkORPnXk6Em7gLiBCUruM7A0irh6pWcOvmacXRLFFi4KoeseTmzUJdhq1
T0XbGbYXHtEsSU/Z2LeZIfidB7vmbUuhI8ffEM0UYfJQbS3wusKrBy7/IzZCu2mu
RFFFIwKBgQCAyXBqEs3WJkP7tA2mACk2c520B/QAUDgdYaZmmWz4EJDVX5D9Ss8V
p6wCdwJRj88FXLUaDmUts634tlLSsJ1nitQ/yLkYC64YxTDJD0TJ+N0CsuYcC6sB
/9doO2sE0rxHMW6gBLp1VJr+O016VEGynHGzxnhGPDqRLvOkS5ZgAA==
-----END RSA PRIVATE KEY-----
```

Key Passphrase ab12cd456

- Enter the Private Key of the certificate

You can enter the private key associated with the certificate in two ways:

1. Directly paste the private key in the 'Paste Private Key here' text box
2. Save the private key as a text file and upload the file by clicking the 'Upload From File' button

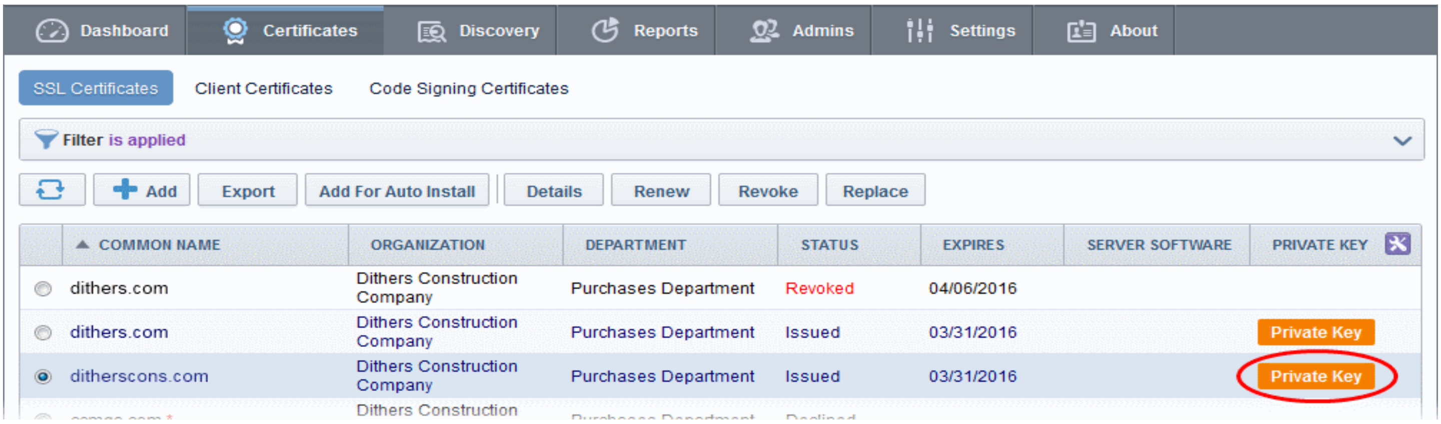


- Enter a passphrase for the key

This passphrase is required for importing the certificate with the key pair on to the server for installation.

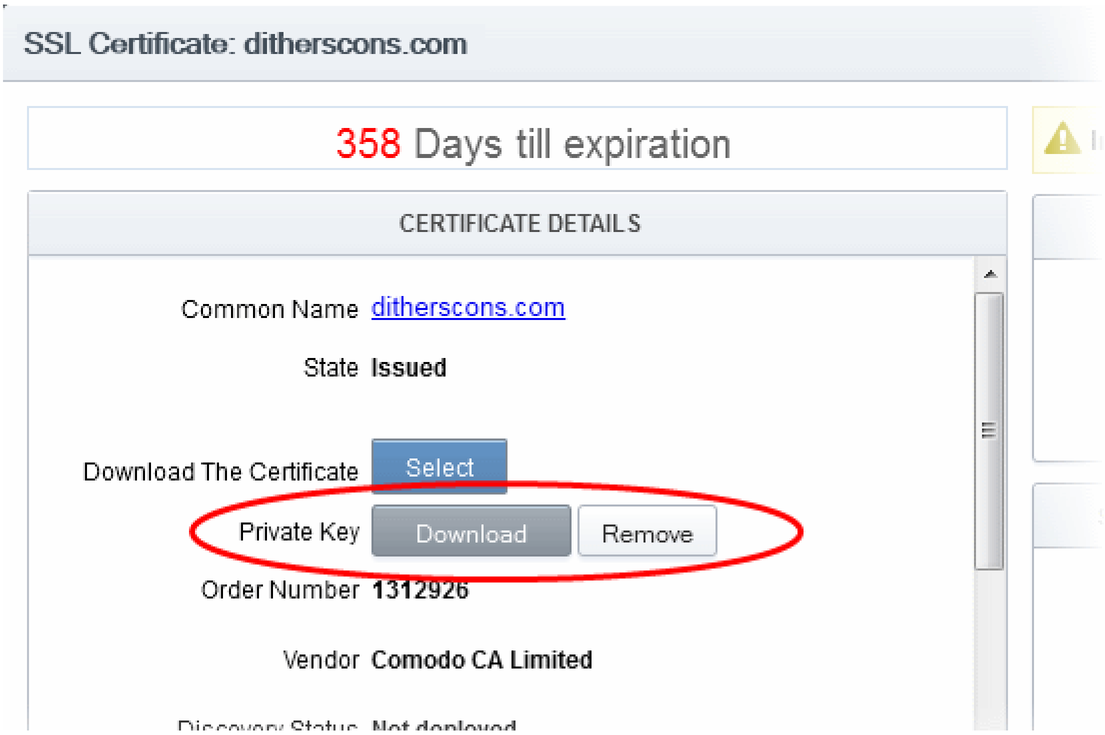
- Click 'OK'
- Close the 'Certificate Details' dialog

InCommon CM will send a command to the controller to store the Private Key. The private key is now stored and managed by the Private Key Store. It will be indicated under the Private Key column in the 'SSL Certificates' area.



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	SERVER SOFTWARE	PRIVATE KEY
○	dithers.com	Dithers Construction Company	Purchases Department	Revoked	04/06/2016		
○	dithers.com	Dithers Construction Company	Purchases Department	Issued	03/31/2016		Private Key
●	ditherscons.com	Dithers Construction Company	Purchases Department	Issued	03/31/2016		Private Key
○		Dithers Construction	Purchases Department	Declined			

Also, you can download the private key from the 'Certificate Details' dialog.



SSL Certificate: ditherscons.com

358 Days till expiration

CERTIFICATE DETAILS

Common Name ditherscons.com

State Issued

Download The Certificate Select

Private Key Download Remove

Order Number 1312926

Vendor Comodo CA Limited

Discovery Status Not deployed

3.1.1.2.2 Downloading private key of a certificate

The 'Details' dialog for SSL certificates with Private Keys stored at the Private Key Store allows the administrator to download the private key in .key format.

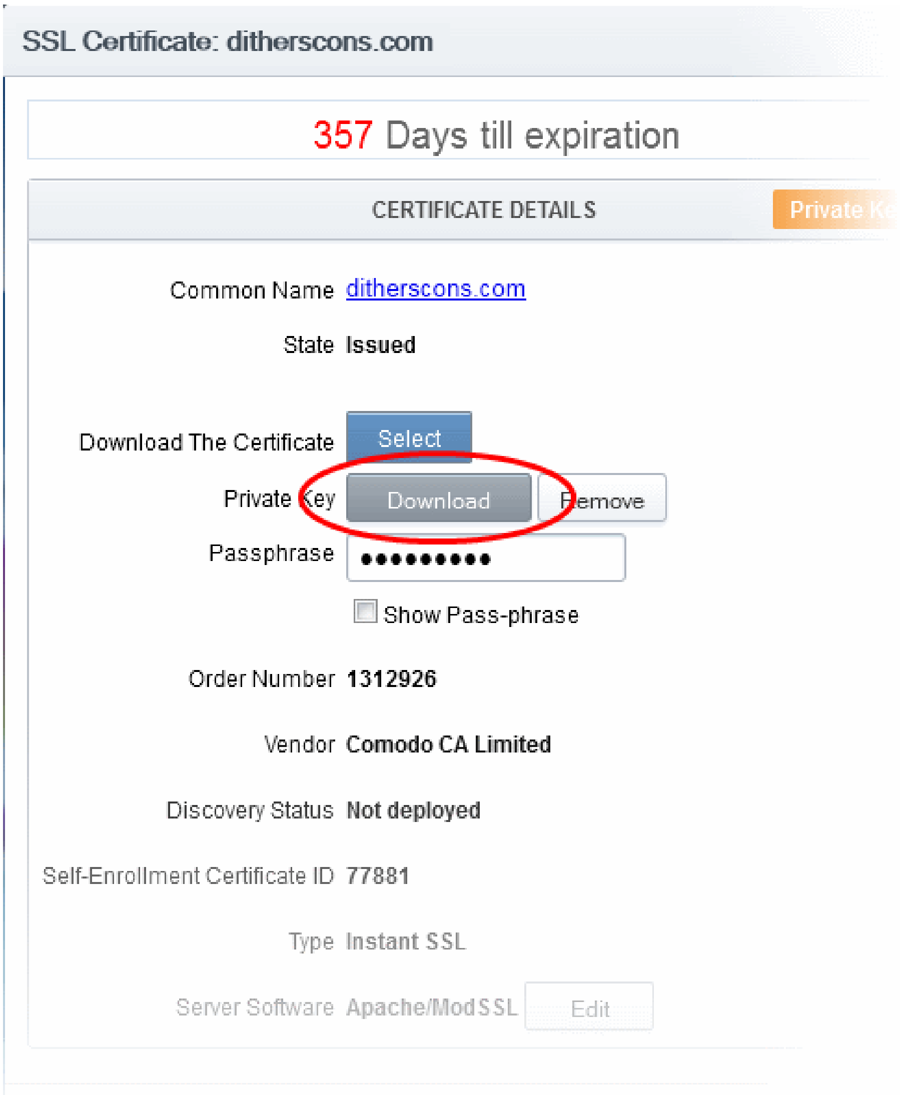
Limitations - The private key can be downloaded only for certificates whose private keys are managed by the private key store. This includes:

- Certificates applied using auto-CSR generation feature in Incommon CM. See Method 3 - Built-in Enrollment Form - Auto CSR Generation for more explanation on using the Auto-CSR generation feature.
- Certificates for which the private keys were manually uploaded to the Private Key Store. See Uploading Private Key of a Certificate for Storage and Management by the Private Key Store for more details.

- In order to download a private key, the administrator should have been logged-in to Incommon CM through a computer in the same local network on which the Private Key Store controller is installed and should have a personal authentication certificate installed on the computer.
- During the download process, Incommon CM sends a download command to the controller.
- The controller requests for authentication of the administrator and checks for authentication certificate.
- Once authenticated, the private key controller enables the administrator to download the private key in .key format directly from it, without uploading it to Incommon CM. This ensures that the private key does not leave your network though Incommon CM initiates the download.

The 'Certificate Details' pane of the details dialog for the SSL certificate with managed private key, displays a 'Download' button beside the 'Private Key' field.

The 'Certificate Details' pane of the details dialog for the SSL certificate with managed private key, displays a 'Download' button beside the 'Private Key' field.



SSL Certificate: ditherscons.com

357 Days till expiration

Common Name ditherscons.com

State Issued

Download The Certificate Select

Private Key Download Remove

Passphrase ●●●●●●●●●

□ Show Pass-phrase

Order Number 1312926

Vendor Comodo CA Limited

Discovery Status Not deployed

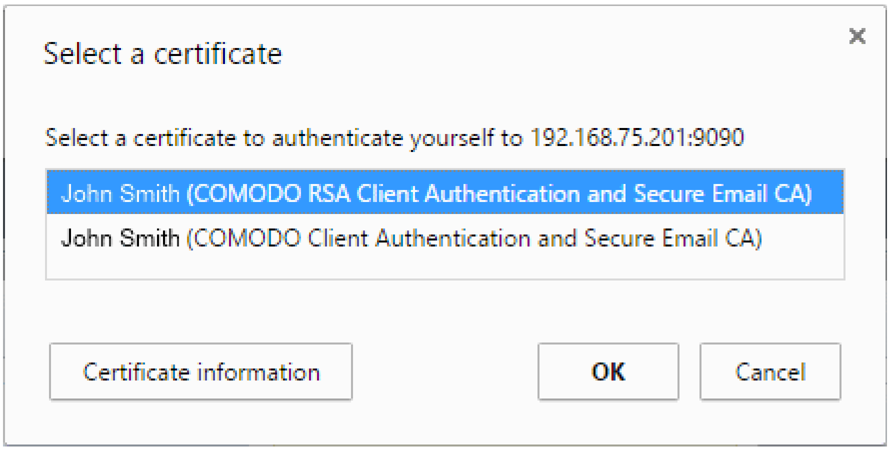
Self-Enrollment Certificate ID 77881

Type Instant SSL

Server Software Apache/ModSSL Edit

- Clicking the 'Download' button will send a command to the Private Key Store controller.

The private key storage controller will request for authentication and search for the personal authentication certificate of the administrator in the computer from which the administrator has logged-in. If more than one certificate is found, the Select Certificate dialog will be displayed for the administrator to choose the certificate.



Select a certificate

Select a certificate to authenticate yourself to 192.168.75.201:9090

John Smith (COMODO RSA Client Authentication and Secure Email CA)

John Smith (COMODO Client Authentication and Secure Email CA)

- Choose the certificate for authentication and click OK.

Upon authentication verification, the download dialog will be displayed, enabling the administrator to download the private key in .key format.

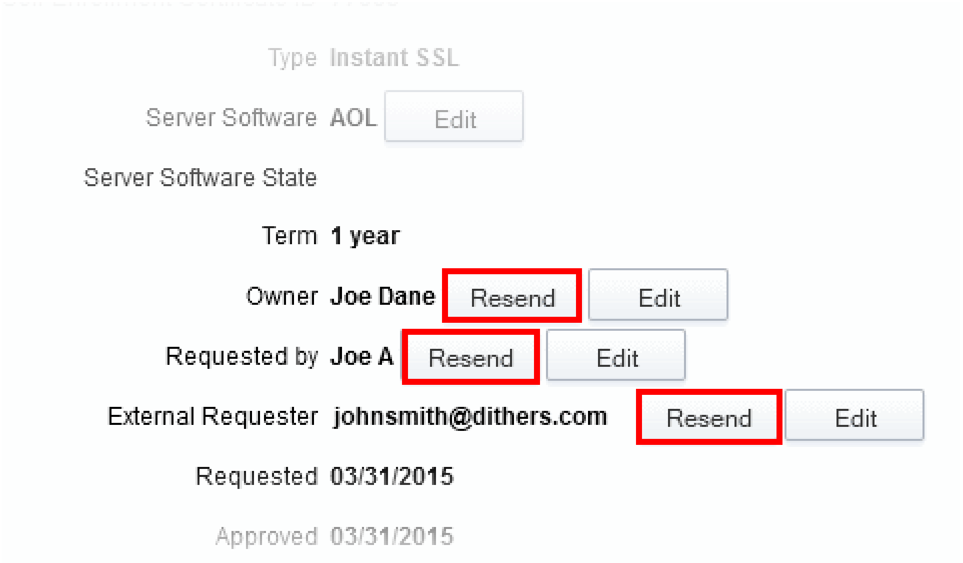
3.1.1.2.3 Resending Notification Email for Certs with 'Issued' State

The 'Details' dialog for SSL certificates with 'Issued' state allows the administrator to resend the 'Certificate Enrolled' notification to the domain control administrator. the applicant that applied for the certificate through the Self Enrollment Form and/or the applicant on behalf of whom the administrator has applied for the certificate through the Built-in Enrollment Form.

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

The 'Certificate Details' pane of the details dialog for the SSL certificate with the Issued state, displays a 'Resend' button beside the Owner and Requested by and External Requester (if applicable) fields.

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



Type Instant SSL

Server Software AOL

Server Software State

Term 1 year

Owner Joe Dane

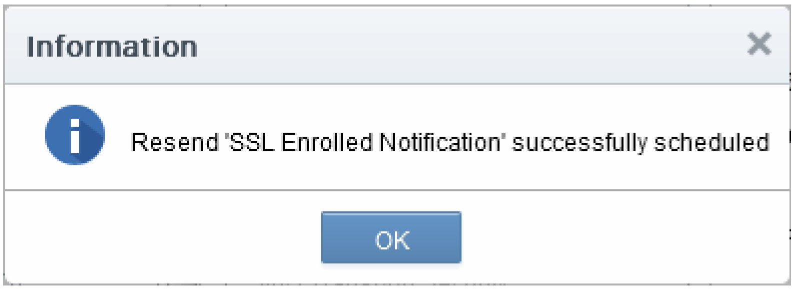
Requested by Joe A

External Requester johnsmith@dithers.com

Requested 03/31/2015

Approved 03/31/2015

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



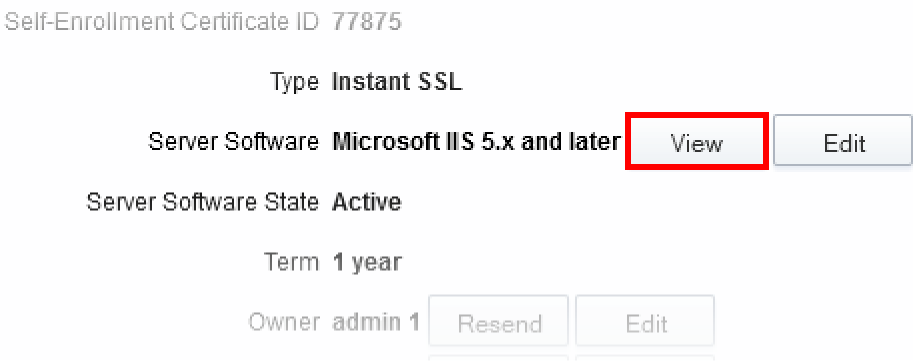
Information

Resend 'SSL Enrolled Notification' successfully scheduled

3.1.1.2.4 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 'Certificate Details' pane of the details dialog for the SSL certificate added for auto installation, displays a 'View' button beside the 'Server Software' field.



Self-Enrollment Certificate ID 77875

Type Instant SSL

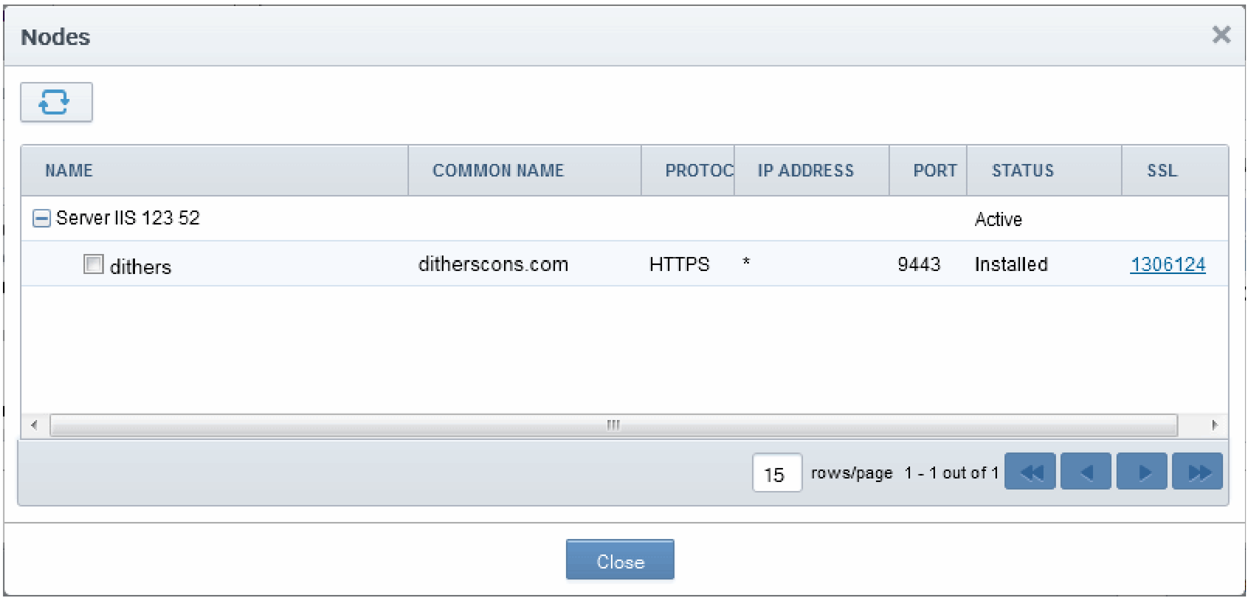
Server Software Microsoft IIS 5.x and later

Server Software State Active

Term 1 year

Owner admin 1

- 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.

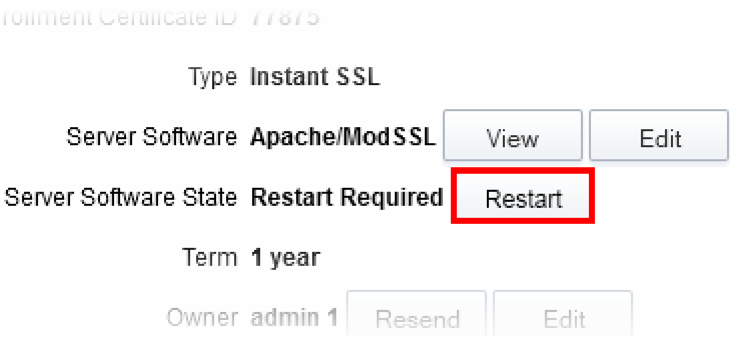


Nodes

NAME	COMMON NAME	PROTOC	IP ADDRESS	PORT	STATUS	SSL
⊟ Server IIS 123 52					Active	
□ dithers	ditherscons.com	HTTPS	*	9443	Installed	1306124

3.1.1.2.5 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 CM interface by clicking the 'Restart' button on the 'Certificate Details' pane of the details dialog.



rollment Certificate ID 77875

Type Instant SSL

Server Software Apache/ModSSL

Server Software State Restart Required

Term 1 year

Owner admin 1

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

3.1.1.2.6 Update Auto-Renewal Status

You can update the auto-renewal status of a certificate from its 'Details' screen.

- Click 'Certificates' > 'SSL Certificates' > select a certificate and click the 'Details' button.
- Scroll down the certificate details screen and click 'Edit' beside 'Auto-renewal'.
- Choose the number of days prior to expiry that you want to start the auto-renew process (default = 30 days out)
- On the scheduled day, the certificate controller will initiate a renewal request using the existing CSR and submit it to CA.

See 'Schedule Automatic Certificate Renewal' for more details.

3.1.1.3 InCommon SSL Certificates

3.1.1.3.1 Definition of Terms

Validation Levels

OV : **O**rganization **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 : **S**ingle **D**omain **C**ertificates will secure a single fully qualified domain name.

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

MDC : **M**ulti-**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
InCommon SSL Certificate	SDC	OV	Secures a single domain	1 year - 3 years
InCommon Wildcard SSL Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain	1 year - 3 years
InCommon Multi-Domain SSL Certificate (MDC)	MDC	OV	Secures multiple Fully Qualified domains on a single certificate	1 year - 3 years
InCommon Unified Communication Certificate (UCC)	MDC	OV	Secures multiple Fully Qualified domains on a single certificate. Specifically designed for use with Microsoft Exchange and Microsoft Office Communications servers	1 year - 3 years
InCommon Intranet SSL Certificate	SDC	OV	Secures a single internal host	1 year - 3

Certificate Name	Type	Validation Level	Description	Maximum Term Length
				years
Comodo Extended Validation (EV) SSL Certificate	SDC	EV	Secures a single domain	1 year - 2 years
Comodo EV Multi-Domain SSL Certificate (EVMDC)	MDC	EV	Secures multiple Fully Qualified domains on a single certificate	1 year - 2 years
InCommon AMT SSL Certificate	SDC	OV	Secures a single domain. Specifically designed for communication between Intel Setup and Configuration Software (SCS) at server and PCs using Active Management Technology (AMT), a feature of Intel® vPro™ platforms.	1 year - 3 years
InCommon AMT Wildcard SSL Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain. Specifically designed for communication between Intel Setup and Configuration Software (SCS) at server and PCs using Active Management Technology (AMT), a feature of Intel® vPro™ platforms.	1 year - 3 years
InCommon Multi-Domain AMT SSL Certificate	MDC	OV	Secures multiple Fully Qualified domains on a single certificate. Specifically designed for communication between Intel Setup and Configuration Software (SCS) at server and PCs using Active Management Technology (AMT), a feature of Intel® vPro™ platforms.	1 year - 3 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** - Admins can configure Incommon CM to automatically create certificate requests for their domains then automatically install the certificate on a web server. When a certificate is nearing expiry, a CSR is automatically generated and forwarded for admin 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. See Automatic Installation and Renewal for more details.
- **Manual Installation** - SSL administrators, or applicants authorized by them, can also obtain certificates via Incommon CM's enrollment wizard. The applicant will then need to manually install the certificate on the target web server. See Initiating SSL Enrollment Form and Built-in Wizard for more details.

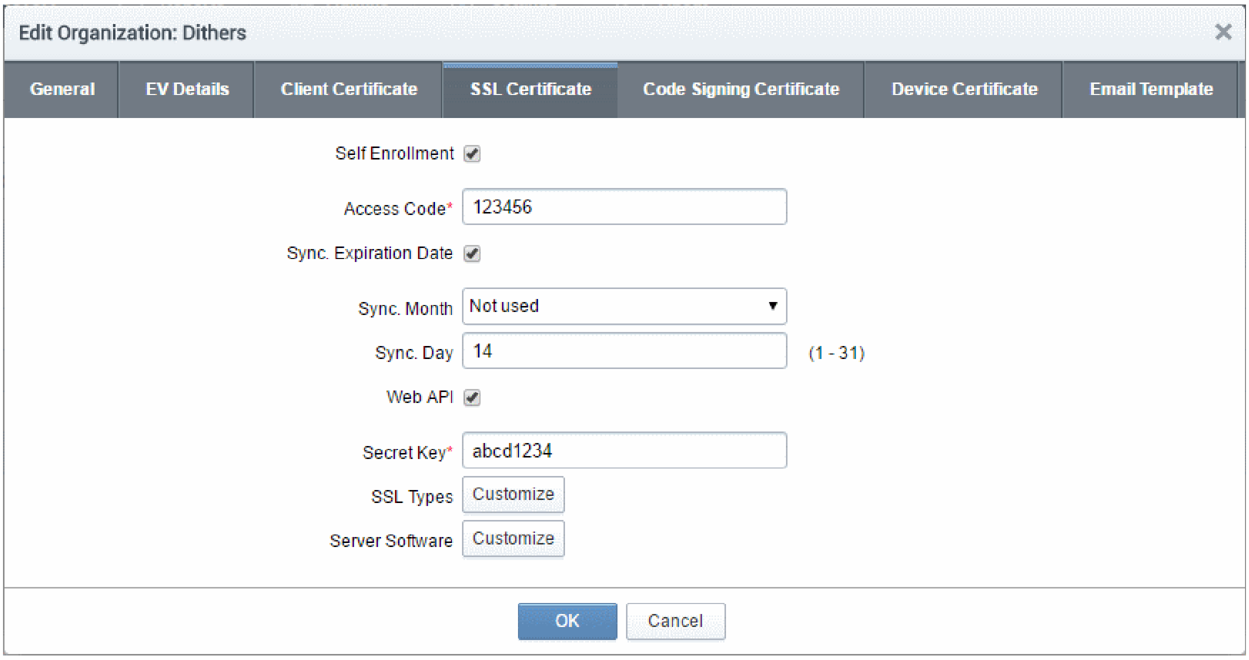
Summary of steps for requesting and issuing an SSL certificate:

- Applicant confirms completion of the prerequisites.

- A certificate request is made via the certificate auto-installer or via an application form/wizard as explained above.
- The certificate will appear in the 'SSL Certificates' area of Incommon Certificate Manager with the state 'Requested'. The 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 Incommon CA for validation and issuance or rejection.
    - If the certificate was applied for via the Incommon CM interface it will be issued and its state will change to 'Issued' in the 'Certificates' area. The admin can install the certificate remotely by clicking the 'Install' button in the Incommon CM interface.
- If the certificate was applied for via the self-enrollment application form or wizard, a collection mail will be sent to the applicant. This mail contains a link to the certificate collection form (see 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 the 'Requester' of the certificate. If the applicant does not exist then Incommon CM will add him/her as a new 'End-user' when the certificate application form is successfully submitted.

3.1.2.1 Prerequisites

- The domain for which the SSL certificate is intended has been enabled for SSL certificates. The domain should also have passed domain control validation (DCV) and should have been activated for your account by your account manager.
    - All certificate requests made on validated domains or sub-domains thereof are issued without further validation. If you request a certificate for a brand new domain, then this domain will first have to undergo validation by Incommon.
    - Once validated, this new domain will be added to your list of 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 Incommon CM 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).



Edit Organization: Dithers

Self Enrollment ☑

Access Code* 123456

Sync. Expiration Date ☑

Sync. Month Not used

Sync. Day 14 (1 - 31)

Web API ☑

Secret Key* abcd1234

SSL Types Customize

Server Software Customize

- 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). Incommon recommends using a mixture of alpha and numeric characters that cannot not easily be guessed.
- For the Built-in wizard and the Self Enrollment Form, 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 enrollment by allowing the common name (CN) to be automatically drawn from the CSR. Please note that CSR must be at least RSA-2048 bit and must contain at least the following fields:

  Common Name (Fully Qualified Domain Name)
  Organization
  Organization Unit
  Locality
  State/Province
  Country (2 character ISO code)
- For enrollment of through Built-in Wizard using the auto-CSR generation feature, the Master Administrator has setup a Private Key Store in their local network by installing the Private Key Store Controller and configured it to connect to Incommon CM.

Note: Contact your Master Administrator if the feature is not available for you and should you require it.

- **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

Incommon Certificate Manager has the ability to automatically install SSL certificates on servers. There are two possible methods, or 'modes', you can use to achieve this:

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

Auto-installation is available for all SSL certificate types (single domain, wildcard, multi-domain/UCC) and is supported on the following web-servers:

- Apache/ModSSL
- Tomcat
- Microsoft IIS
- F5 BIG IP

Please see the table below for details of supported configurations:

S.No	Supported server software type for auto-install (Vendor)	Host operating system on which the network agent is installed	
		Linux	Windows
1	Apache 2.X	C / E	N/A
2	Tomcat	C / E	C
3	Microsoft IIS	N / A	C / E
4	F5 BIG-IP	E	E

- C - Incommon CM Controller Mode (Local)
- E – Enterprise Controller Mode (Remote)

1. Enterprise Controller Mode

   i. Certificate controller software is installed on a host in your network. The controller will communicate with your remote web-hosts and will automatically apply for and install certificates on to them.

   ii. The controller periodically polls Incommon CM for certificate requests. If a request exists, it will automatically generate a CSR for the web server and present the application for approval via the Incommon CM interface. After approval, the agent will submit the CSR to Incommon CA and track the order number. After issuance, the controller will download the certificate and allow administrators to install it from the Incommon CM interface.

See Method 1 - Enterprise Controller Mode for a tutorial on automatic installation of Certificates on remote web servers

2. Incommon CM 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 polls Incommon CM for certificate requests for servers that have been enabled for automatic installation. If a request exists, it will automatically generate a CSR for the web server and present the application for administrator approval in the Incommon CM interface. After approval, the agent will submit the CSR to Incommon CA and track the order number. After issuance, the agent will download the certificate and allow administrators to install it from the Incommon CM interface.

See Method 2 - Incommon CM 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.

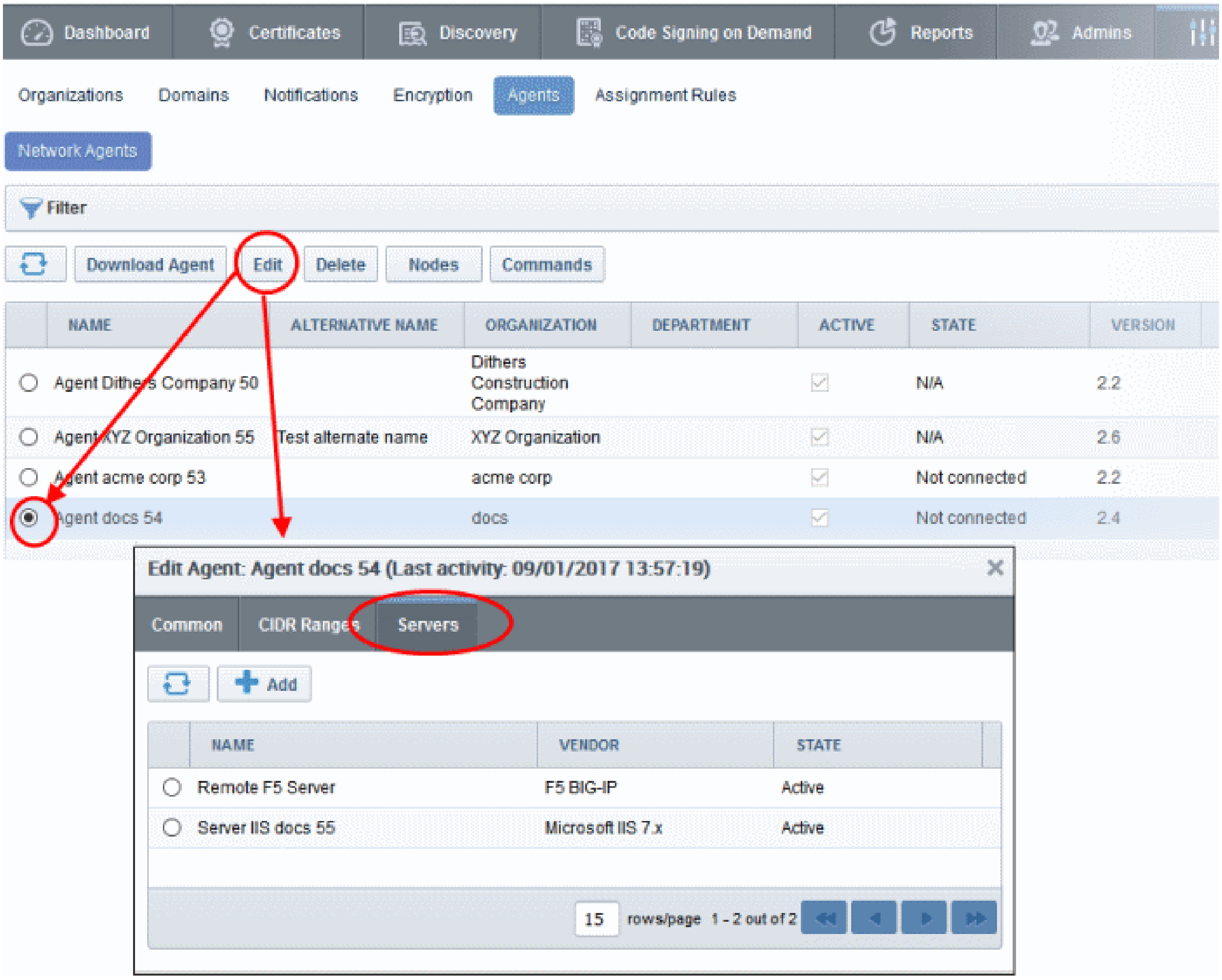
3.1.2.2.1 Method 1 - Enterprise Controller Mode

Enterprise Controller mode allows you to automatically install certificates on any remote server on the network.

- Controller software first needs to be installed on a server in your network. See Configure the Agents for Auto-Installation and Internal Scanning if you need help to install the controller.
- You then need to add web-servers to the controller to enable certificate auto-installation. This is done in the 'Settings' > 'Agents' > 'Network Agents' interface. See the explanation below.
- If a new certificate is requested for an enabled server, the controller will coordinate with the host to generate a CSR, submit it to Incommon CA, collect the certificate and install it.
  - You can install multiple controllers on different servers. If the controllers are all assigned to same organization/department, then a single controller can be used to auto-install certificates on servers (nodes) associated with another controller.

To add remote servers to the certificate controller

- Click 'Settings' > 'Agents' > 'Network Agents'
- Select the controller you want to work with
- Click 'Edit' then open the 'Servers' tab:



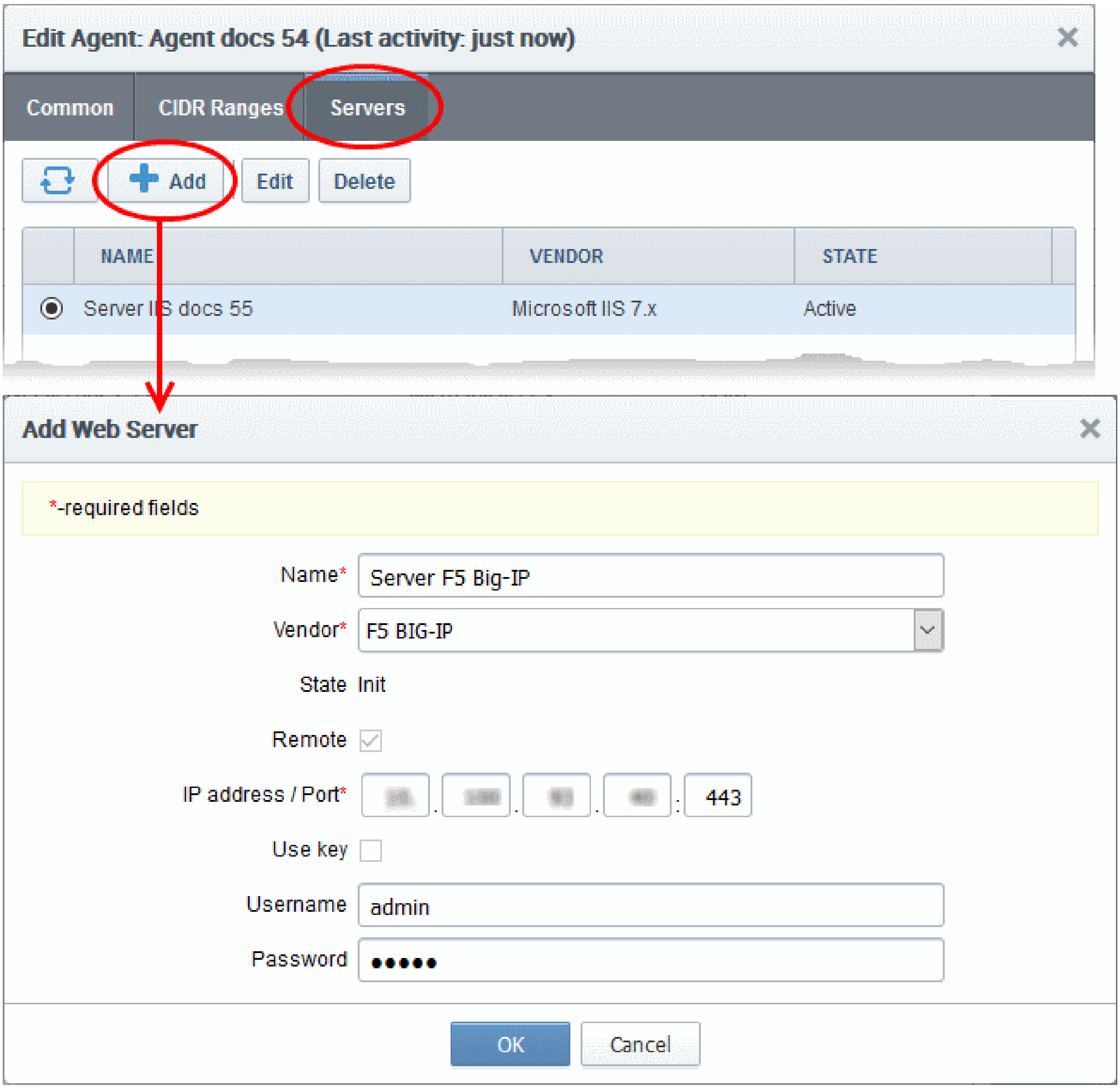
	NAME	ALTERNATIVE NAME	ORGANIZATION	DEPARTMENT	ACTIVE	STATE	VERSION
○	Agent Dithers Company 50		Dithers Construction Company		☑	N/A	2.2
○	Agent XYZ Organization 55	Test alternate name	XYZ Organization		☑	N/A	2.6
○	Agent acme corp 53		acme corp		☑	Not connected	2.2
●	Agent docs 54		docs		☑	Not connected	2.4

Edit Agent: Agent docs 54 (Last activity: 09/01/2017 13:57:19)

	NAME	VENDOR	STATE
○	Remote F5 Server	F5 BIG-IP	Active
○	Server IIS docs 55	Microsoft IIS 7.x	Active

- The server(s) on which the controller is installed will be shown.

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



Edit Agent: Agent docs 54 (Last activity: just now)

NAME	VENDOR	STATE
● Server IIS docs 55	Microsoft IIS 7.x	Active

Add Web Server

*-required fields

Name* Server F5 Big-IP

Vendor* F5 BIG-IP

State Init

Remote ☑

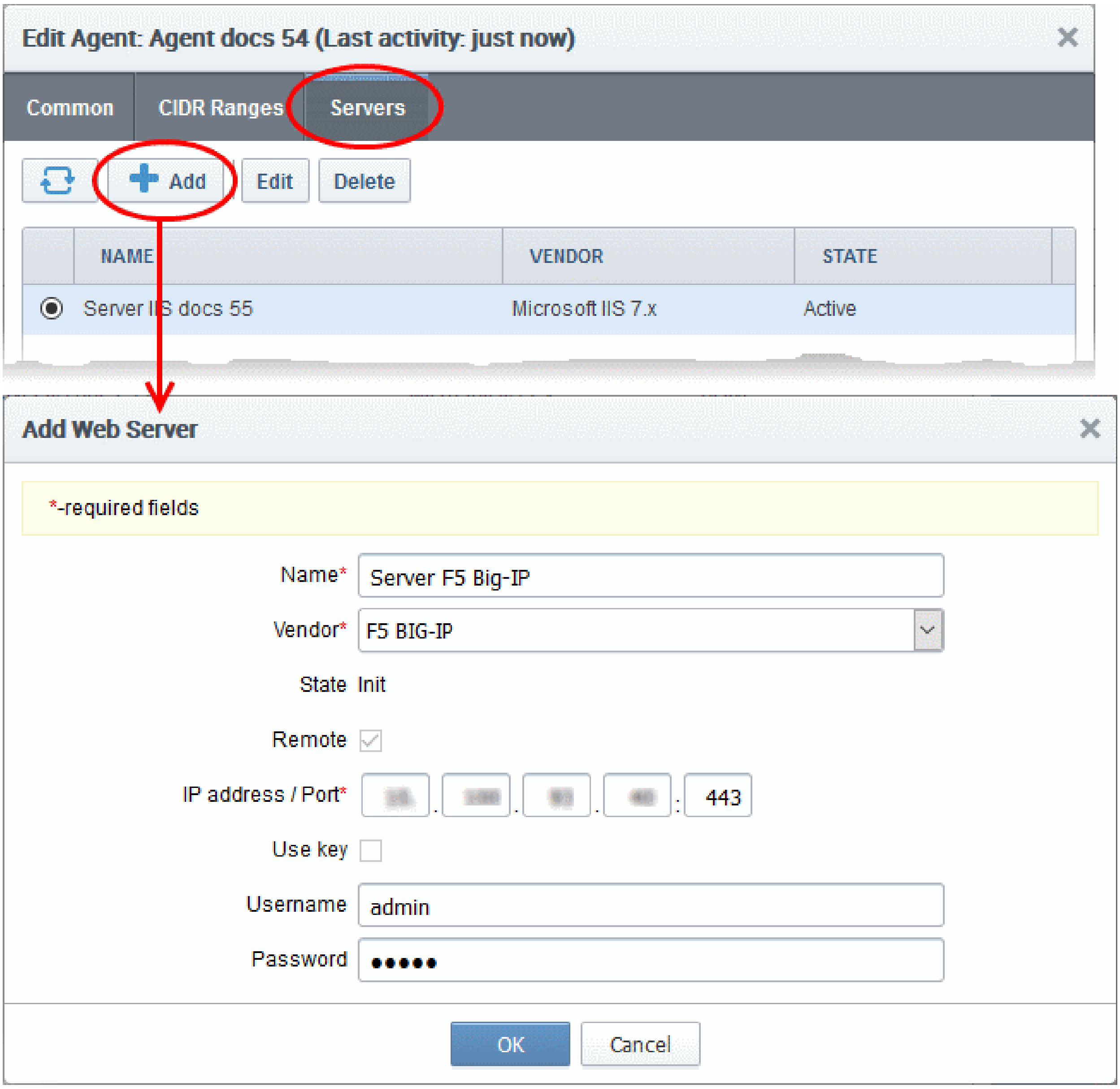
IP address / Port* [redacted] . [redacted] . [redacted] . [redacted] : 443

Use key □

Username admin

Password ●●●●●

- Enter the server name, address and login details:



Edit Agent: Agent docs 54 (Last activity: just now)

NAME	VENDOR	STATE
● Server IIS docs 55	Microsoft IIS 7.x	Active

Add Web Server

*-required fields

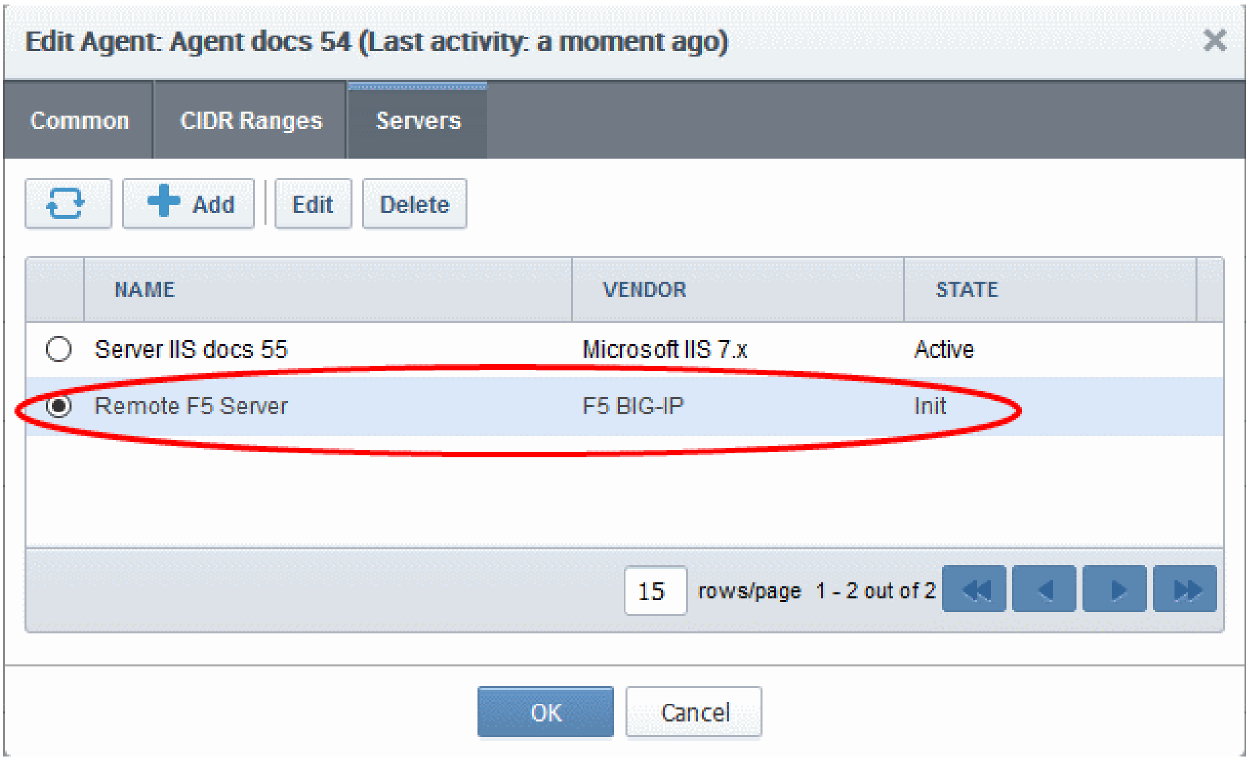
Name*	Server F5 Big-IP
Vendor*	F5 BIG-IP
State	Init
Remote	☑
IP address / Port*	[redacted] . [redacted] . [redacted] . [redacted] : 443
Use key	□
Username	admin
Password	●●●●●

- Enter the server name, address and login details:

Add Web Servers - Table of Parameters		
Field Name	**Type**	**Description**
Name	String	Enter the hostname of the server.
Vendor	Drop-down	Select the web-server type.
State		Indicates whether or not the server is connected. The connection will be initialized and active once the agent starts communicating with it.

Add Web Servers - Table of Parameters		
Path to web server	String	Specify the network path of the server. Only required for Tomcat under Linux.
Remote	Checkbox	Specify whether the server is remote or local. This checkbox should be selected when adding remote servers for agent-less automatic certificate installation.
IP Address / Port	String	Specify the IP address and connection port of the server for remote connection. Note: This field will be enabled only if 'Remote' is selected.
Use key	Checkbox	• Specify whether the agent should use SSH Key-Based Authentication to access the server. • Only applies to Apache and Tomcat web-servers installed on Linux.
User Name / Private Key File Path	String	• If 'Use key' is not selected, specify the admin username to log-into the server. • If 'Use key' is selected, specify the path to the SSH private key file to access the server Note: This field will be enabled only if 'Remote' is selected.
Password / Passphrase	String	• If 'Use key' is not selected, specify the admin password to log-into the server. • If 'Use key' is selected, specify the passphrase for the private key file. Note: This field will be enabled only if 'Remote' is selected.

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



Edit Agent: Agent docs 54 (Last activity: a moment ago)

	NAME	VENDOR	STATE
○	Server IIS docs 55	Microsoft IIS 7.x	Active
●	Remote F5 Server	F5 BIG-IP	Init

15 rows/page 1 - 2 out of 2

- Repeat the process to add more remote servers
- Once all servers have been successfully added to the controller, you can apply for certificates for domains on the server. Go to 'Certificates' > 'SSL Certificates' to apply for new certificates.

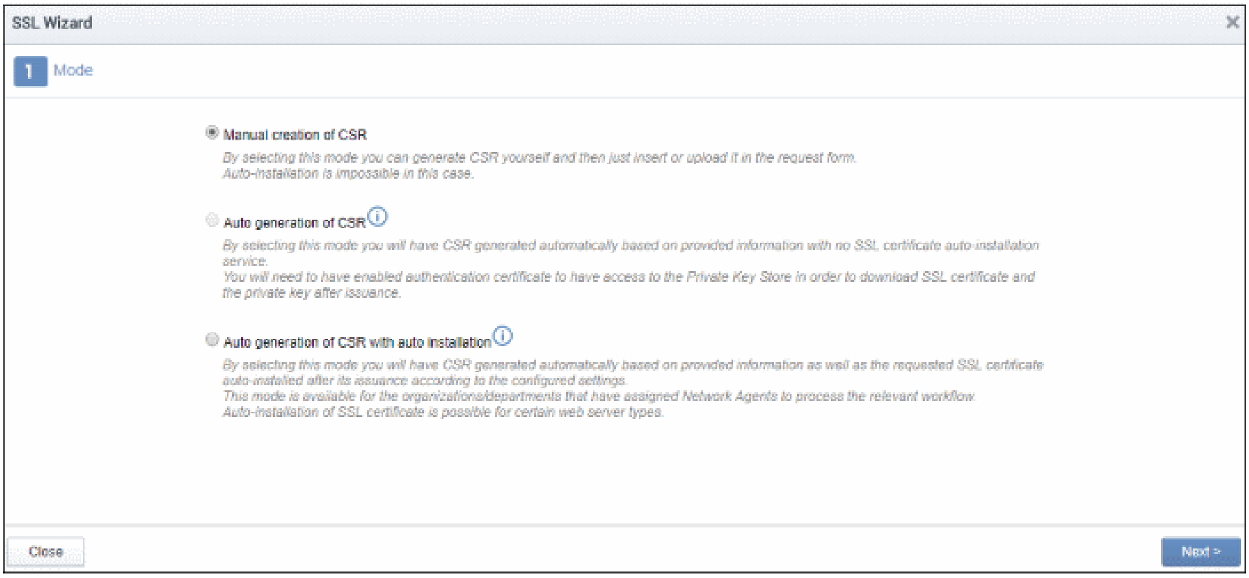
To enroll a certificate for auto-installation

- Click the 'Certificates' tab and choose the 'SSL Certificates' sub-tab
- Click the 'Add' button

The built-in application form for SSL Enrollment will appear.

To enroll a certificate for auto-installation

- Click the 'Certificates' tab and choose the 'SSL Certificates' sub-tab
- Click the 'Add' button
- This will start the SSL enrollment wizard:



● Manual creation of CSR

*By selecting this mode you can generate CSR yourself and then just insert or upload it in the request form.
Auto-installation is impossible in this case.*

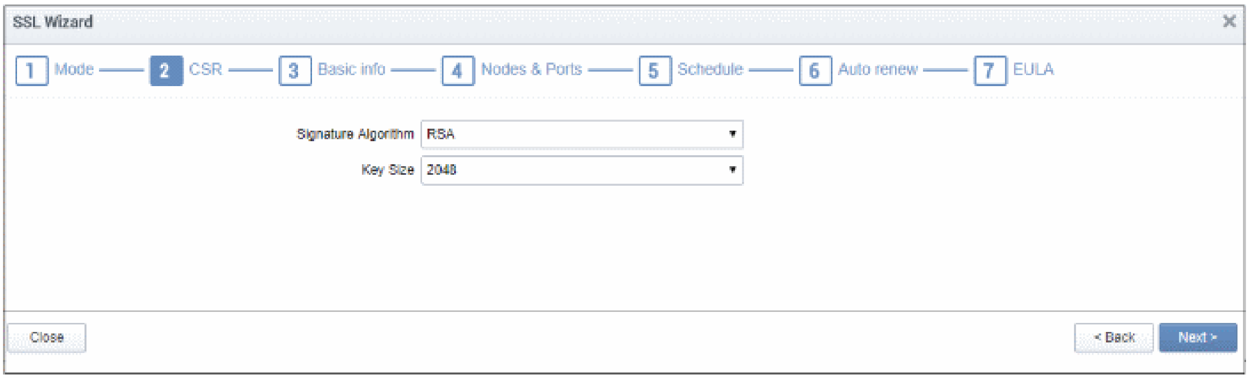
○ Auto generation of CSR

*By selecting this mode you will have CSR generated automatically based on provided information with no SSL certificate auto-installation service.
You will need to have enabled authentication certificate to have access to the Private Key Store in order to download SSL certificate and the private key after issuance.*

○ Auto generation of CSR with auto installation

*By selecting this mode you will have CSR generated automatically based on provided information as well as the requested SSL certificate auto-installed after its issuance according to the configured settings.
This mode is available for the organizations/departments that have assigned Network Agents to process the relevant workflow.
Auto-installation of SSL certificate is possible for certain web server types.*

- Select the third option, 'Auto generation of CSR with auto installation', and click 'Next'.



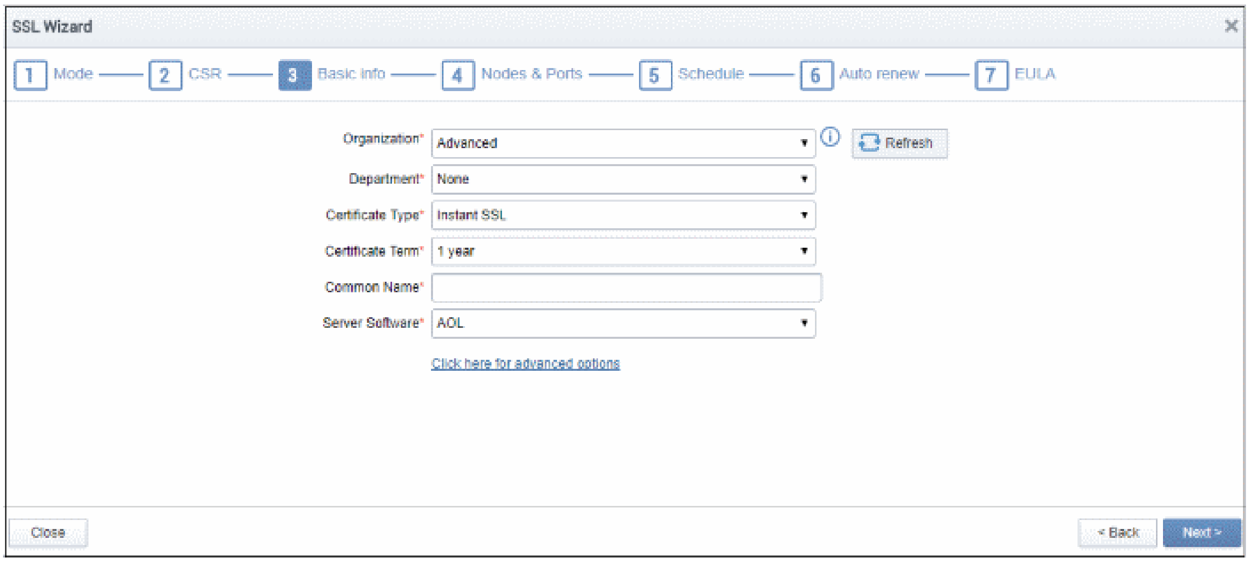
Signature Algorithm: RSA

Key Size: 2048

The next step is to provide the CSR parameters:

- Signature Algorithm – Select the digital signature algorithm you want to use in the certificate. Currently only RSA is supported.
- Key Size – Options available are 2048 and 4096. 2048 bit is the recommended industry standard and provides very high security for public-facing and internal hosts. 4096 is even more secure, but may lead to longer connection times due to the extra processing time needed to exchange keys during the SSL handshake.

- Click 'Next'



SSL Wizard

Organization* Advanced

Department* None

Certificate Type* Instant SSL

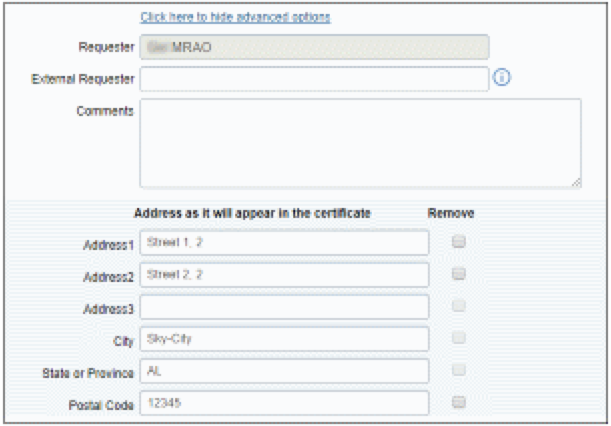
Certificate Term* 1 year

Common Name*

Server Software* AOL

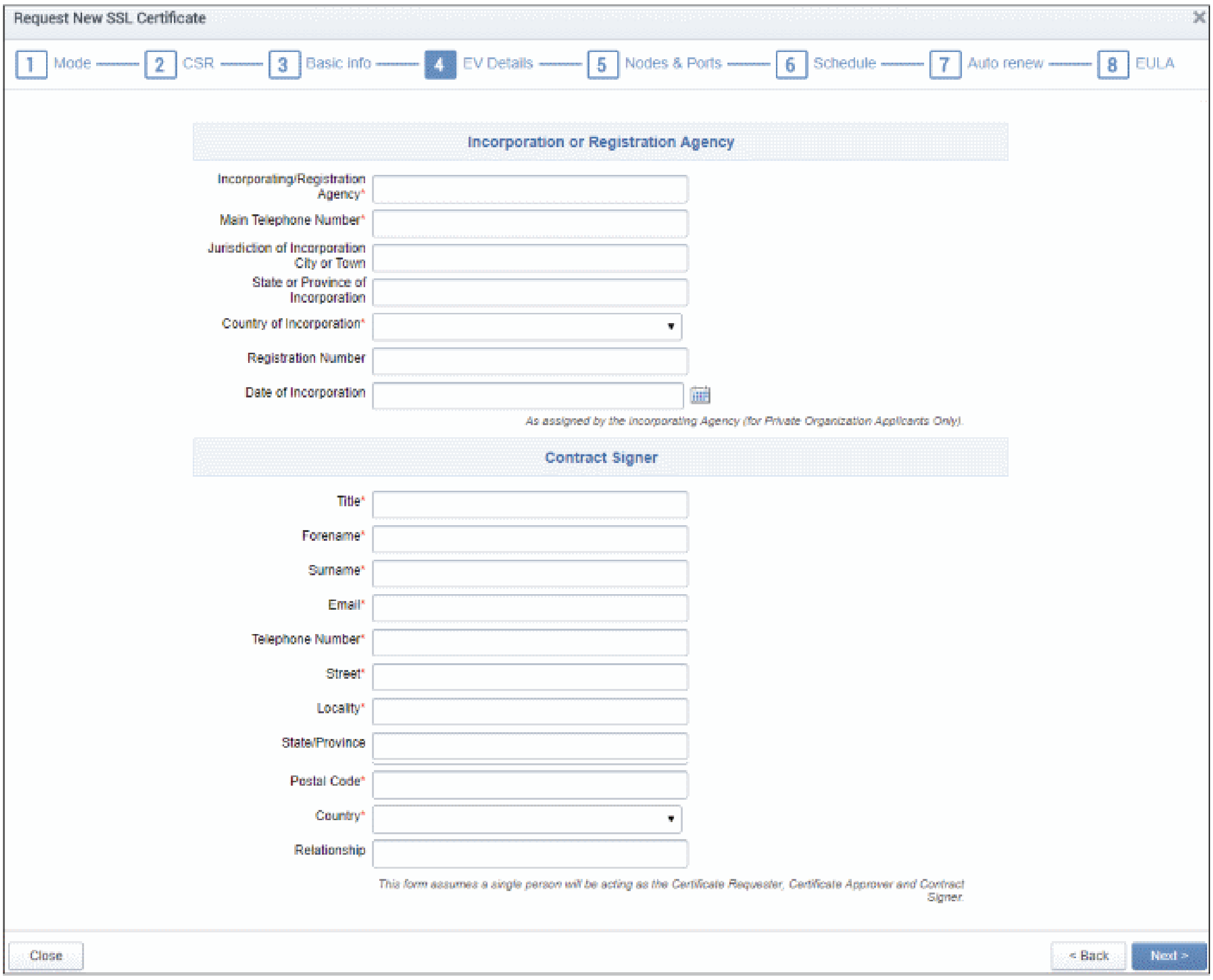
Click here for advanced options

Form Element	Type	Description
Organization (***required***)	Drop-down list	Choose the Organization that the SSL certificate will belong to.
Department (***required***)	Drop-down list	Choose the Department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'.
Certificate Type (***required***)	Drop-down list	Choose the certificate type that you wish to add for auto-installation. See Comodo SSL Certificates for a list of certificate types. The specific certificate types displayed in the drop-down list depends on the SSL Types allowed for the selected organization. See Editing a new Organization and Customize an Organization's SSL Certificate Types
Certificate Term (***required***)	Drop-down list	Choose the validity period of the certificate. For example, 1 year, 2 years, 3 years. See **Comodo SSL Certificates** for a list of certificate types and term lengths. The validity periods available for a particular Organization depends on its configuration. See Editing a new Organization and Customize an Organization's SSL Certificate Types.
Common Name (***required***)	Text Field	Type the domain that the certificate will be issued to.
Server Software (***required***)	Drop-down list	Select the server software on which the certificate is to be installed. **Note**: Choose 'OTHER' if you want to use F5 BIG-IP.
Subject Alternative Names (***optional***)	Text Field	This field appears only if a multi domain or UCC certificate type is selected. Specify the additional domain names. Each domain name should be separated by a comma.
Click here for advanced options	Text Fields	Clicking this link will expand the address fields.

Form Element	Type	Description
		• Requester – This field is auto-populated with the name of the administrator making the application. • External Requester (optional) - Enter the email address of an external requester on whose behalf the application is made.  Click here to hide advanced options Requester: [redacted] MRAO External Requester: Comments: Address as it will appear in the certificate — Remove Address1: Street 1, 2 □ Address2: Street 2, 2 □ Address3: □ City: Sky-City □ State or Province: AL □ Postal Code: 12345 □ **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. • Comments (optional) - Enter your comments on the certificate. **Address fields in the certificate** 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 of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and 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.

- Click 'Next'

The EV Details wizard will appear if you choose EV certificate type:



Request New SSL Certificate

Incorporation or Registration Agency

Incorporating/Registration Agency*

Main Telephone Number*

Jurisdiction of Incorporation City or Town

State or Province of Incorporation

Country of Incorporation*

Registration Number

Date of Incorporation

As assigned by the incorporating Agency (for Private Organization Applicants Only).

Contract Signer

Title*

Forename*

Surname*

Email*

Telephone Number*

Street*

Locality*

State/Province

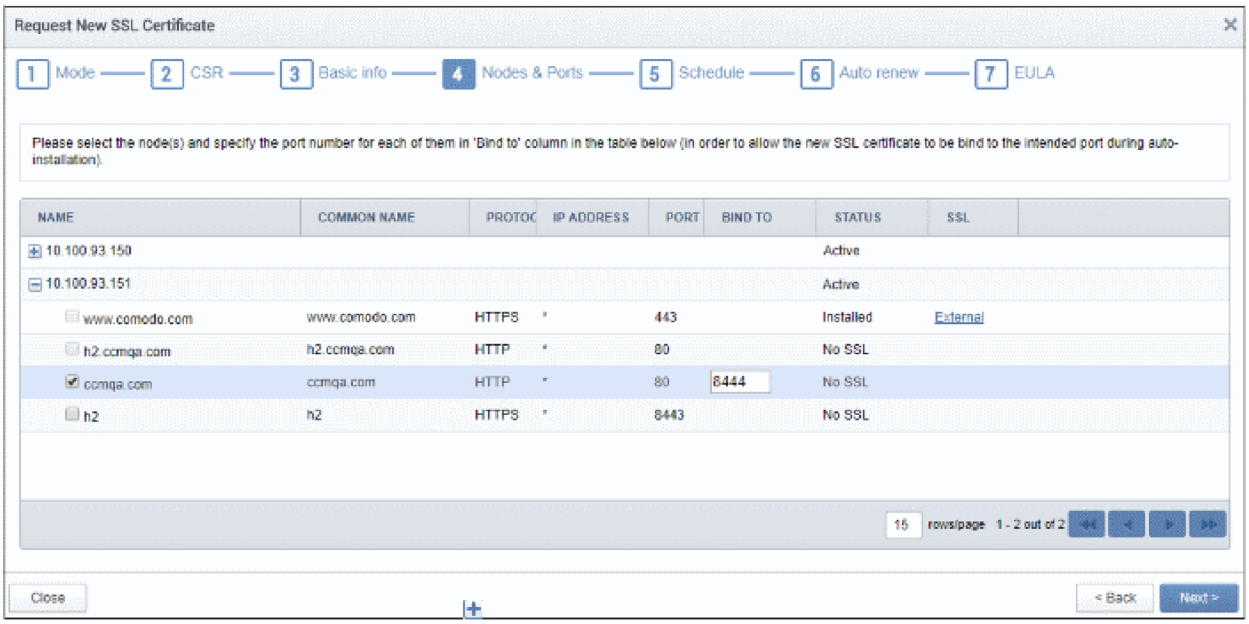
Postal Code*

Country*

Relationship

This form assumes a single person will be acting as the Certificate Requester, Certificate Approver and Contract Signer.

- The details you need to complete depends on the EV mode activated for your account.
- This is same information as provided in the EV details tab when adding a new organization. See 'EV Details Tab' for more info. If the EV type is 'RA' for your account, this will be auto-populated.
- Click 'Next' when all required fields are complete.



Request New SSL Certificate

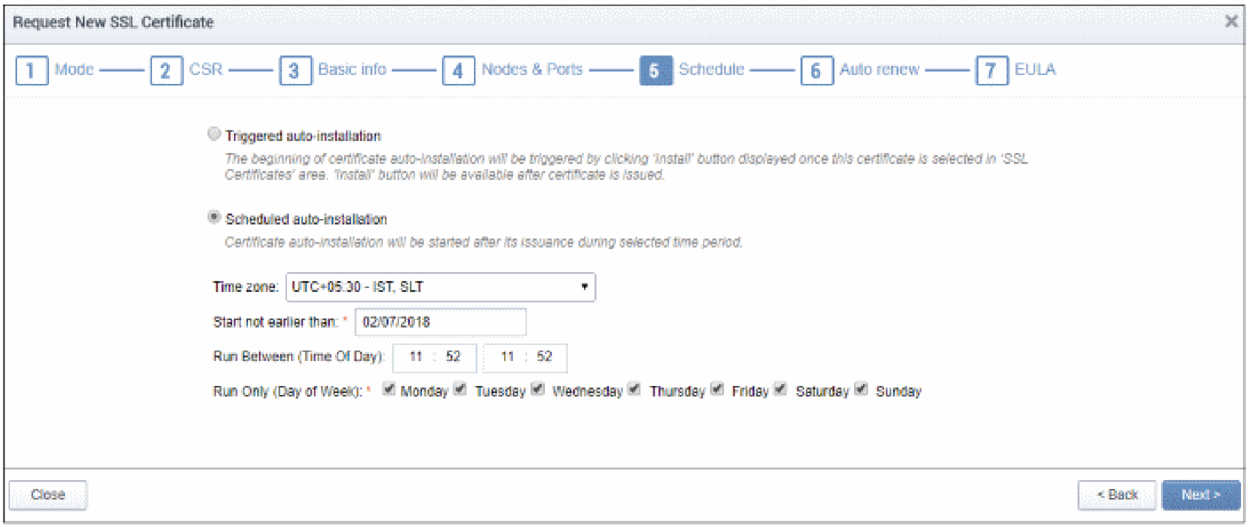
1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — 5 Schedule — 6 Auto renew — 7 EULA

Please select the node(s) and specify the port number for each of them in 'Bind to' column in the table below (in order to allow the new SSL certificate to be bind to the intended port during auto-installation).

NAME	COMMON NAME	PROTOC	IP ADDRESS	PORT	BIND TO	STATUS	SSL
⊞ 10.100.93.150						Active	
⊟ 10.100.93.151						Active	
□ www.comodo.com	www.comodo.com	HTTPS	*	443		Installed	External
□ h2.ccmqa.com	h2.ccmqa.com	HTTP	*	80		No SSL	
☑ ccmqa.com	ccmqa.com	HTTP	*	80	8444	No SSL	
□ h2	h2	HTTPS	*	8443		No SSL	

The 'Nodes & Ports' wizard displays the configured options.

- Select the server which hosts your target domain.
- Select the domain on which you want to install the certificate.
  - Bind To - Specify the port number to which the SSL certificate should be bind to after issuance. This is editable only for protocol with HTTP status.
- Click 'Next'



Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — 5 Schedule — 6 Auto renew — 7 EULA

○ Triggered auto-installation

The beginning of certificate auto-installation will be triggered by clicking 'Install' button displayed once this certificate is selected in 'SSL Certificates' area. 'Install' button will be available after certificate is issued.

● Scheduled auto-installation

Certificate auto-installation will be started after its issuance during selected time period.

Time zone: UTC+05:30 - IST, SLT

Start not earlier than: * 02/07/2018

Run Between (Time Of Day): 11 : 52 11 : 52

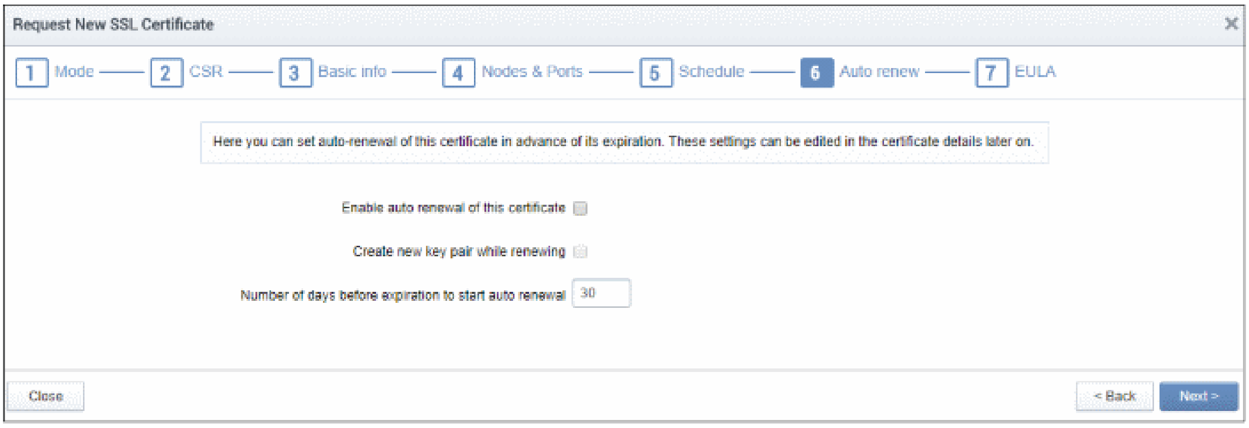
Run Only (Day of Week): * ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Schedule' - Choose whether you want to start auto-installation manually or schedule for a later time.

- 'Triggered auto-installation' – You need to start the auto-installation manually after completing the wizard. To do this, go to 'Certificates' > 'SSL Certificates' > select the certificate > Click 'Install'

- 'Scheduled auto-installation' – Specify a date and time to run the auto-installer. The controller will generate the CSR and submit it to Incommon the next time it polls Incommon CM after the scheduled time.

- Click 'Next'.



Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — 5 Schedule — 6 Auto renew — 7 EULA

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

Enable auto renewal of this certificate □

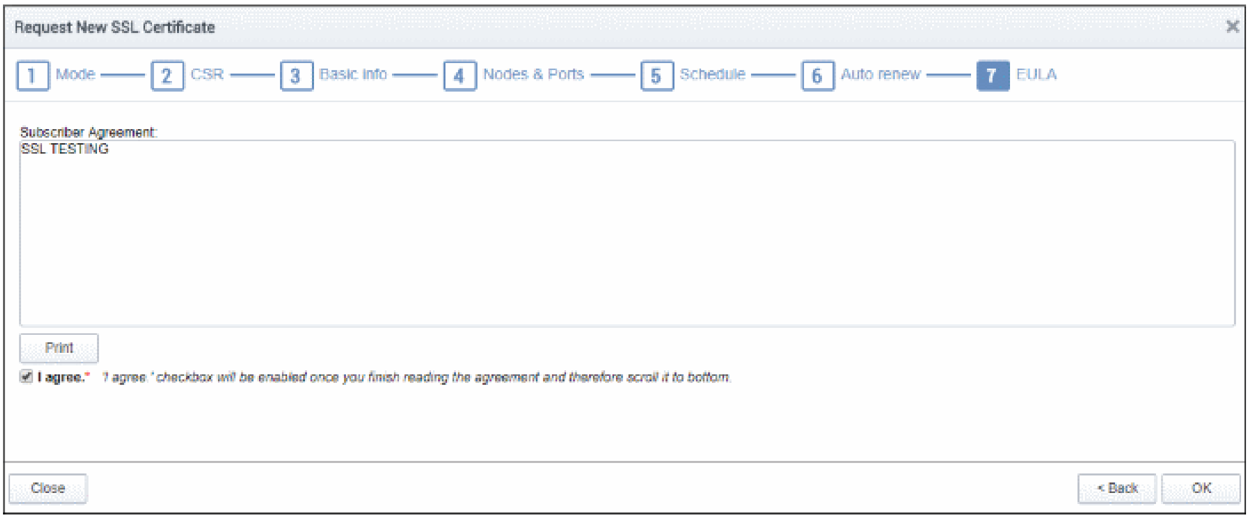
Create new key pair while renewing □

Number of days before expiration to start auto renewal 30

The next step is to configure the auto-renewal options.

- Enable auto renewal of this certificate – Select this to have Incommon CM apply for a new certificate when this one approaches expiry.
- Create new key pair while renewing – If the option above is selected, then choose whether or not you want a generate a new key pair for the renewed certificate. Leaving it disabled means Incommon CM will re-use the key pair of the old certificate.
- Number of days before expiration to start auto renewal - Choose the number of days in advance of expiry that the renewal process should start. On the scheduled day, the certificate controller will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.

- Click 'Next'



Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — 5 Schedule — 6 Auto renew — 7 EULA

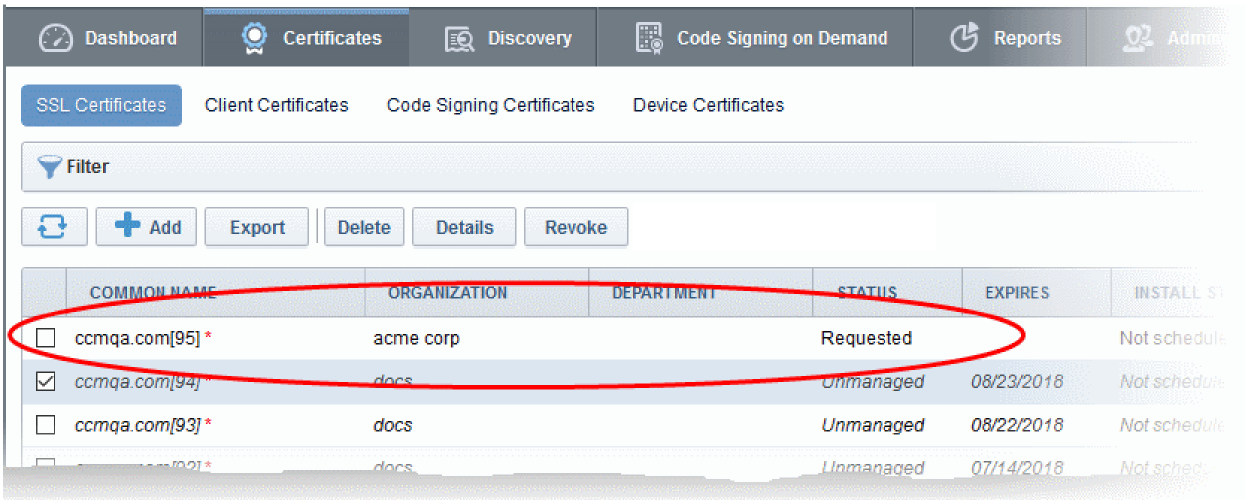
Subscriber Agreement:
SSL TESTING

☑ **I agree.**" 'I agree.' checkbox will be enabled once you finish reading the agreement and therefore scroll it to bottom.

The final stage is to agree to the EULA.

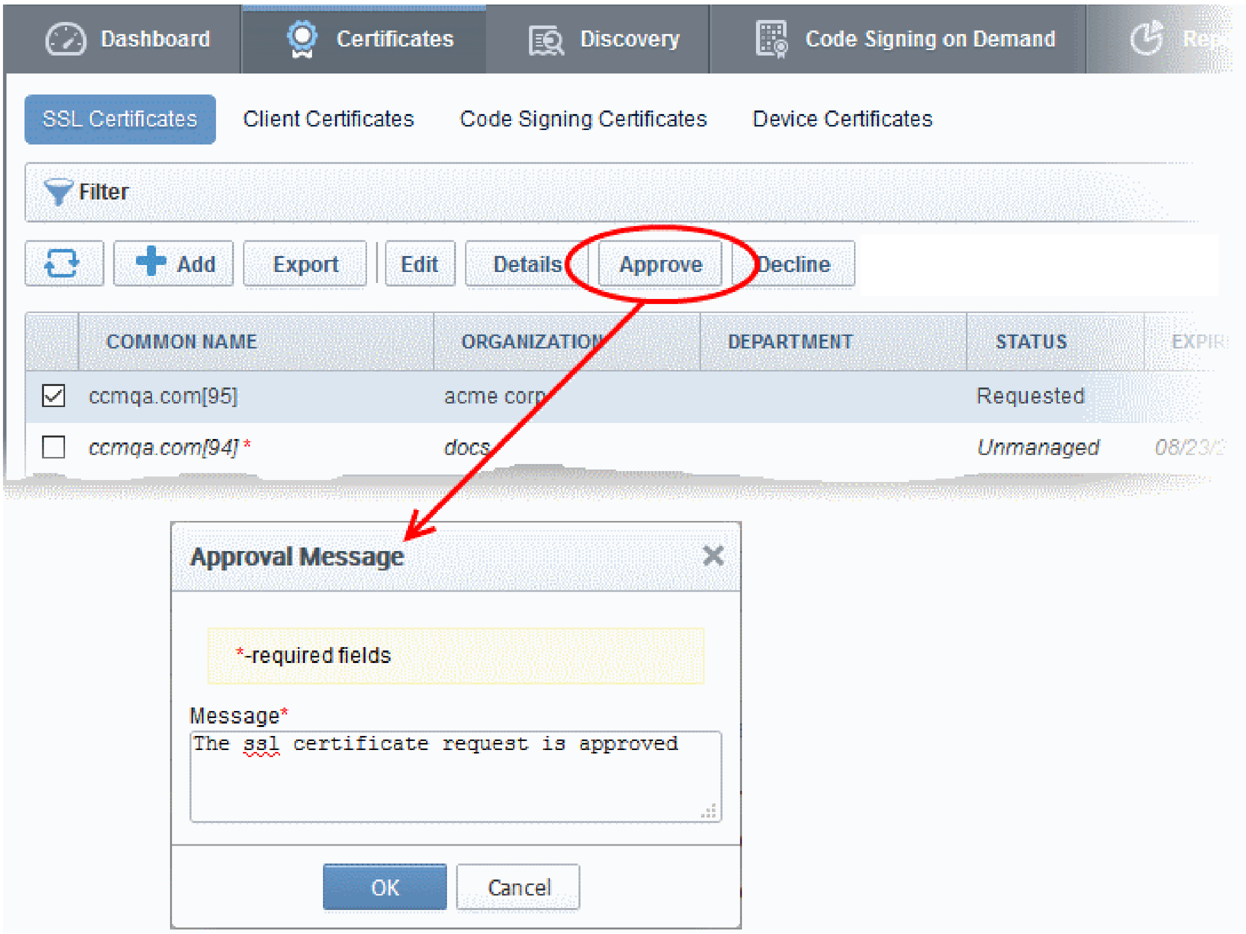
- Read the EULA fully and accept to by the selecting 'I Agree' checkbox.
- Click 'OK' to submit the application

The certificate will be added to the 'SSL Certificates' interface with a status of 'Requested'.



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL ST
□	ccmqa.com[95] *	acme corp		Requested		Not schedul
☑	ccmqa.com[94] *	docs		Unmanaged	08/23/2018	Not schedul
□	ccmqa.com[93] *	docs		Unmanaged	08/22/2018	Not schedul
□	ccmqa.com[92] *	docs		Unmanaged	07/14/2018	Not sched

- The CSR for the requested certificate will be generated automatically. After the CSR has been created, the 'Approve' button will appear at the top when you select the certificate in the list:

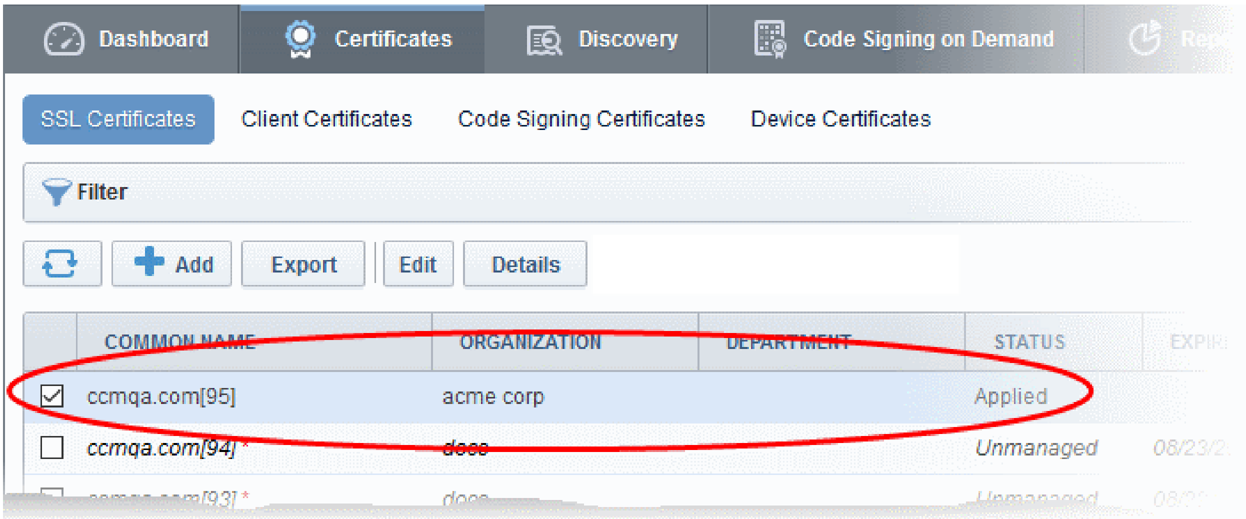


	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIR
☑	ccmqa.com[95]	acme corp		Requested	
□	*ccmqa.com[94]* *	*docs*		*Unmanaged*	*08/23/*

Message*
The ssl certificate request is approved

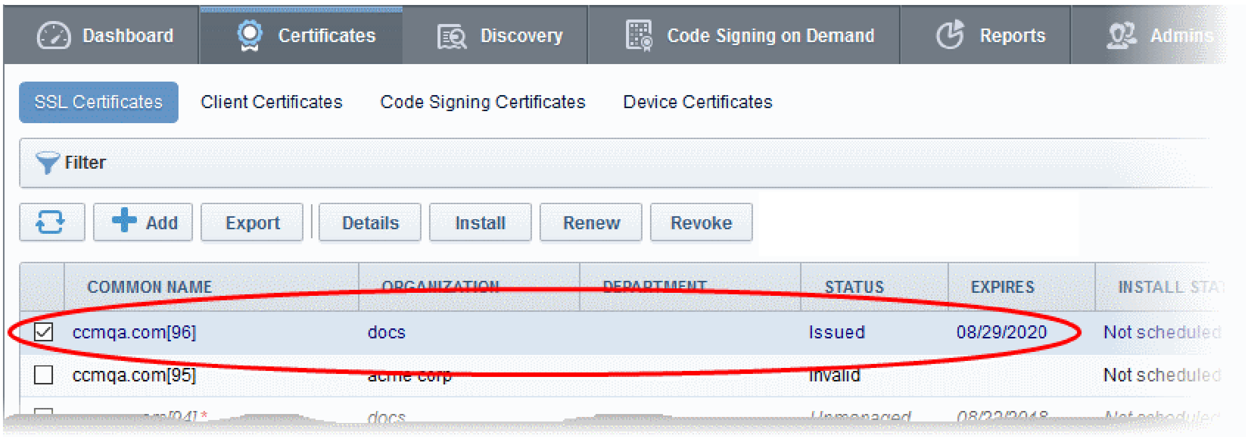
- Click the 'Approve' button to approve the request, enter an approval message and click 'OK'.

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



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIR
☑	ccmqa.com[95]	acme corp		Applied	
□	*ccmqa.com[94]* *	*docs*		*Unmanaged*	*08/23/2*
□	*ccmqa.com[93]* *	*docs*		*Unmanaged*	*08/*

The controller will track the order number and will download the certificate once it is issued. The certificate will stored and its status will change to 'Issued'.

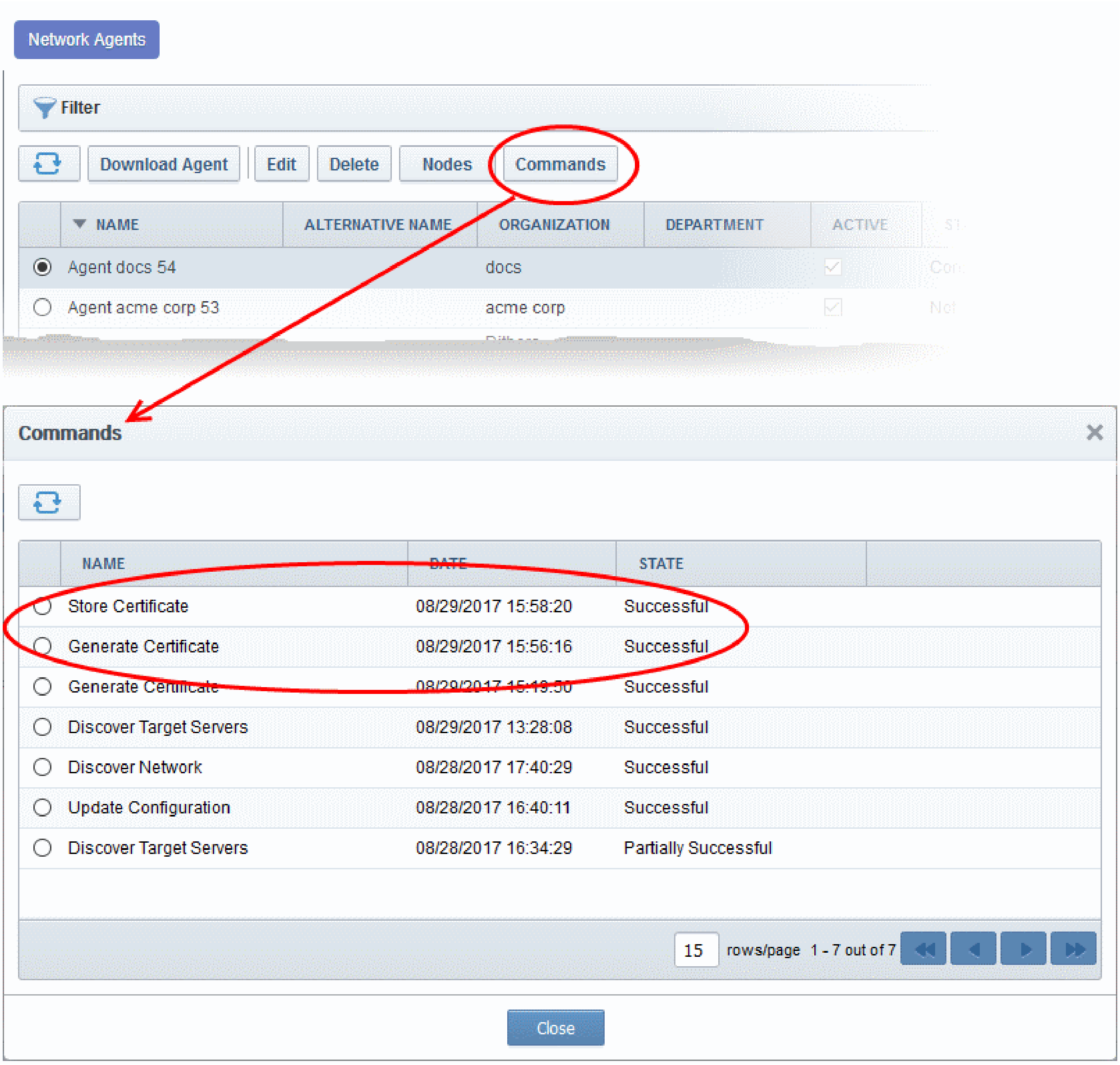


	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STAT
☑	ccmqa.com[96]	docs		Issued	08/29/2020	Not scheduled
□	ccmqa.com[95]	acme corp		Invalid		Not scheduled
□	m[94]*	docs		Unmanaged	08/22/2018	Not scheduled

To check whether the certificate controller has stored the certificate:

- Click 'Settings' > 'Agents' > 'Network Agents'
- Select the controller and click 'Commands' button

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



	NAME	ALTERNATIVE NAME	ORGANIZATION	DEPARTMENT	ACTIVE	ST
●	Agent docs 54		docs		✓	Con
○	Agent acme corp 53		acme corp		✓	Not

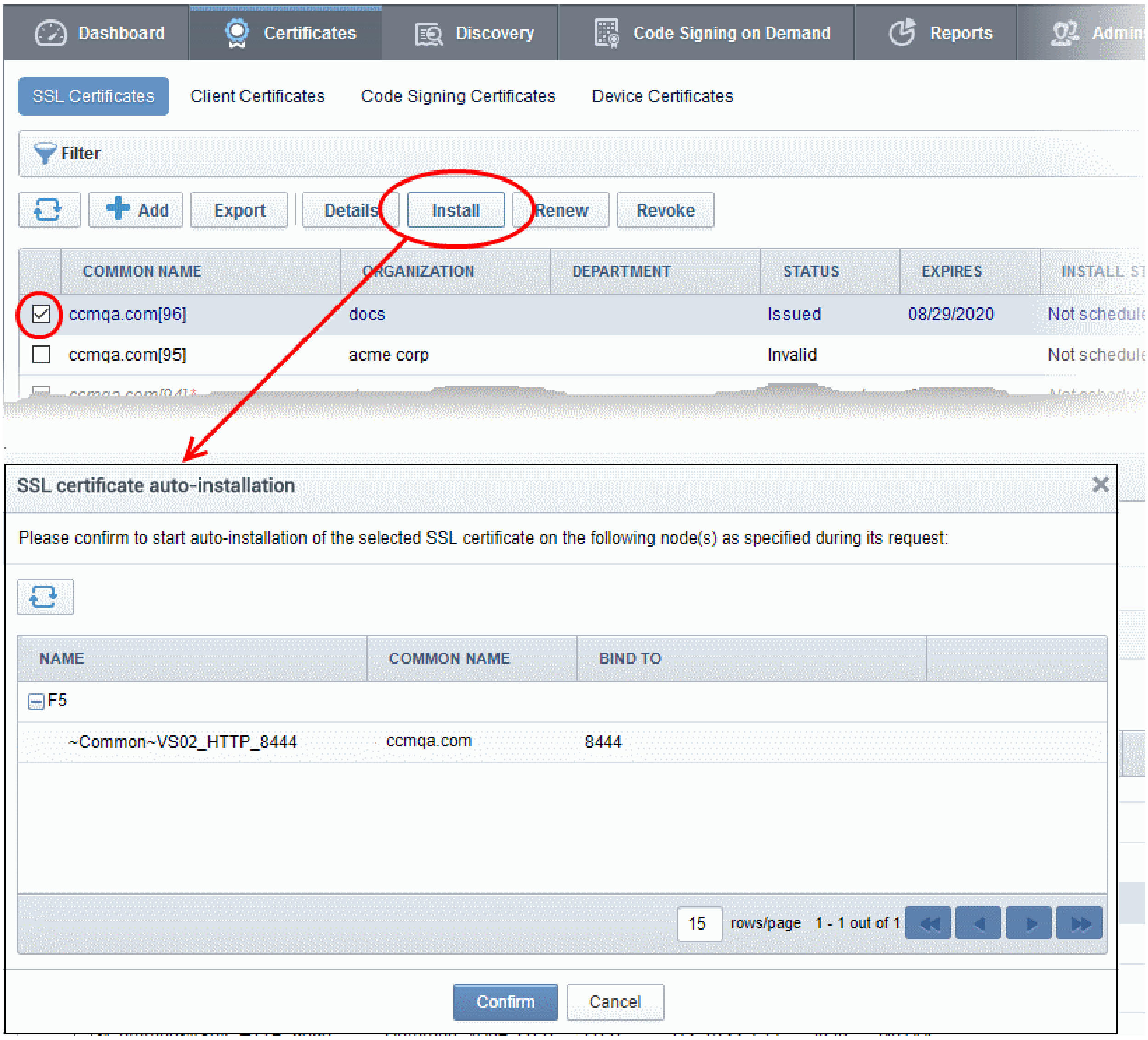
	NAME	DATE	STATE
○	Store Certificate	08/29/2017 15:58:20	Successful
○	Generate Certificate	08/29/2017 15:56:16	Successful
○	Generate Certificate	08/29/2017 15:19:30	Successful
○	Discover Target Servers	08/29/2017 13:28:08	Successful
○	Discover Network	08/28/2017 17:40:29	Successful
○	Update Configuration	08/28/2017 16:40:11	Successful
○	Discover Target Servers	08/28/2017 16:34:29	Partially Successful

The certificate is stored on the server by the agent.

- If you set a schedule for automatic installation, it will be installed automatically at the scheduled time.
- If you selected 'Triggered auto-installation' you can manually initiate the installation process or schedule for auto-installation, from the 'Certificates' > 'SSL Certificates' interface of the Incommon CM console.

To manually initiate auto-installation of a certificate

- Select the certificate from the 'Certificates' > 'SSL Certificates' interface and click 'Install'



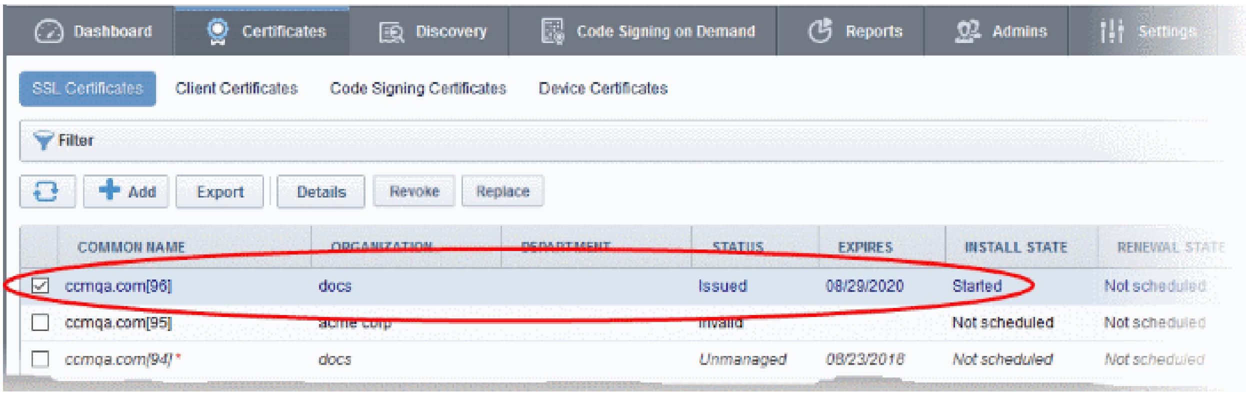
	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL ST
☑	ccmqa.com[96]	docs		Issued	08/29/2020	Not schedule
□	ccmqa.com[95]	acme corp		Invalid		Not schedule

SSL certificate auto-installation

Please confirm to start auto-installation of the selected SSL certificate on the following node(s) as specified during its request:

NAME	COMMON NAME	BIND TO
⊟F5		
~Common~VS02_HTTP_8444	ccmqa.com	8444

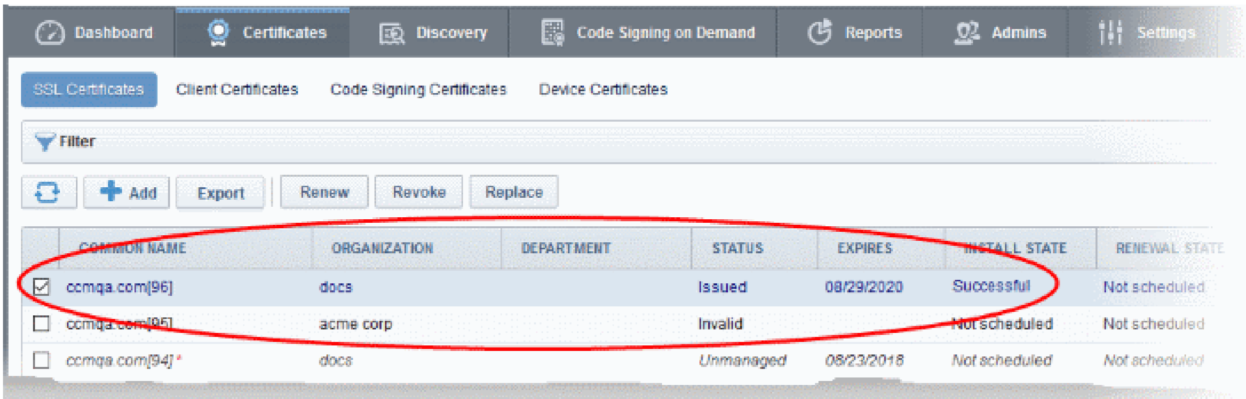
The certificate installation will begin instantly. Once the installation commences, the 'Install State' of the certificate will change to 'Started'.



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
☑	ccmqa.com[96]	docs		Issued	08/29/2020	Started	Not scheduled
☐	ccmqa.com[95]	acme corp		Invalid		Not scheduled	Not scheduled
☐	ccmqa.com[94]*	docs		Unmanaged	08/23/2018	Not scheduled	Not scheduled

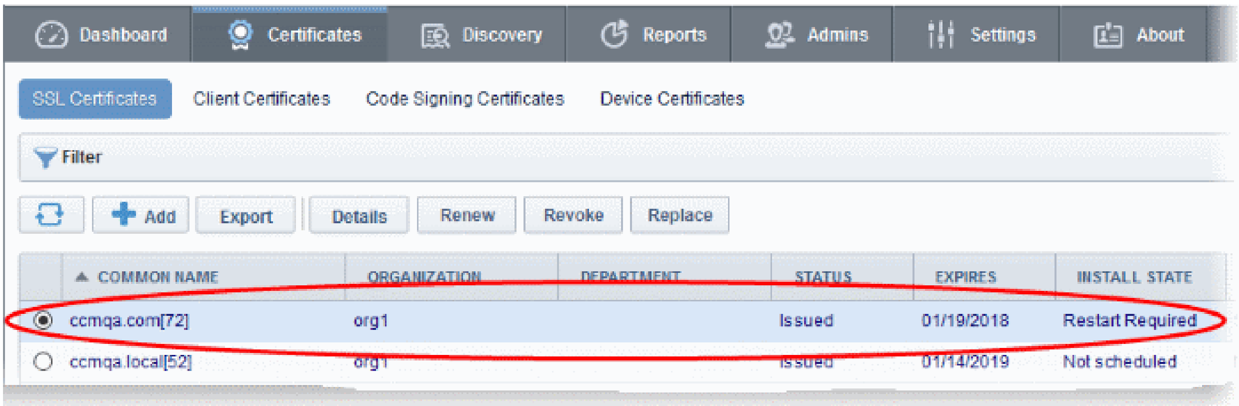
When installation is complete:

- **IIS servers**, **Tomcat** and **F5 BIG-IP** - The certificate will be activated immediately and the install state will change to 'Successful'.



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
☑	ccmqa.com[96]	docs		Issued	08/29/2020	Successful	Not scheduled
☐	ccmqa.com[95]	acme corp		Invalid		Not scheduled	Not scheduled
☐	ccmqa.com[94]*	docs		Unmanaged	08/23/2018	Not scheduled	Not scheduled

- **Apache** - The certificate will become active after the server is restarted. The install state will change to 'Restart Required'.



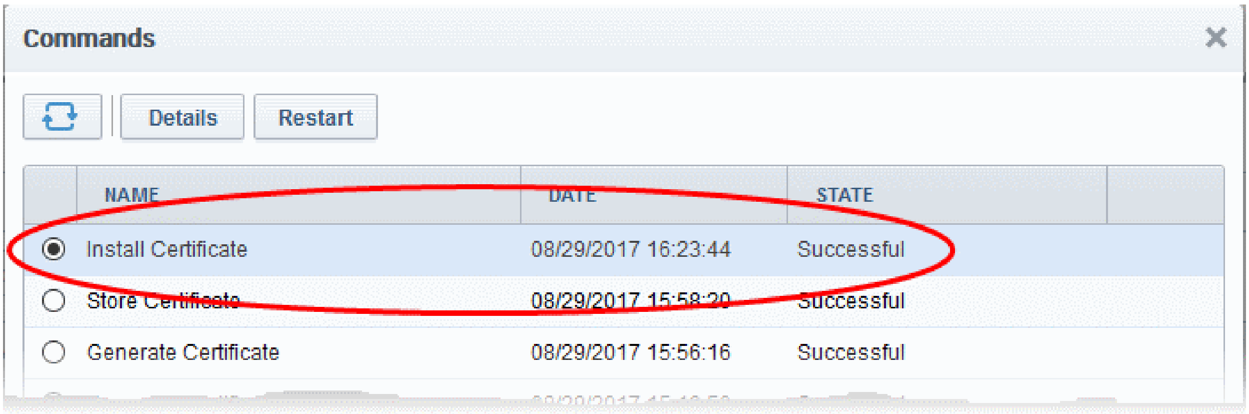
	▲ COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE
●	ccmqa.com[72]	org1		Issued	01/19/2018	Restart Required
○	ccmqa.local[52]	org1		Issued	01/14/2019	Not scheduled

Tip: The server can be restarted from Incommon CM through the Certificate Details dialog. See Restarting Apache after Auto-Installation of SSL Certificate, for more details.

After restarting the server, the certificate will activated and the 'Install State' will change to 'Successful'.

- To check whether the controller has installed the certificate, click Settings > Agents > Network Agents
- Select the controller and click the 'Commands' button

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



	NAME	DATE	STATE
●	Install Certificate	08/29/2017 16:23:44	Successful
○	Store Certificate	08/29/2017 15:58:20	Successful
○	Generate Certificate	08/29/2017 15:56:16	Successful

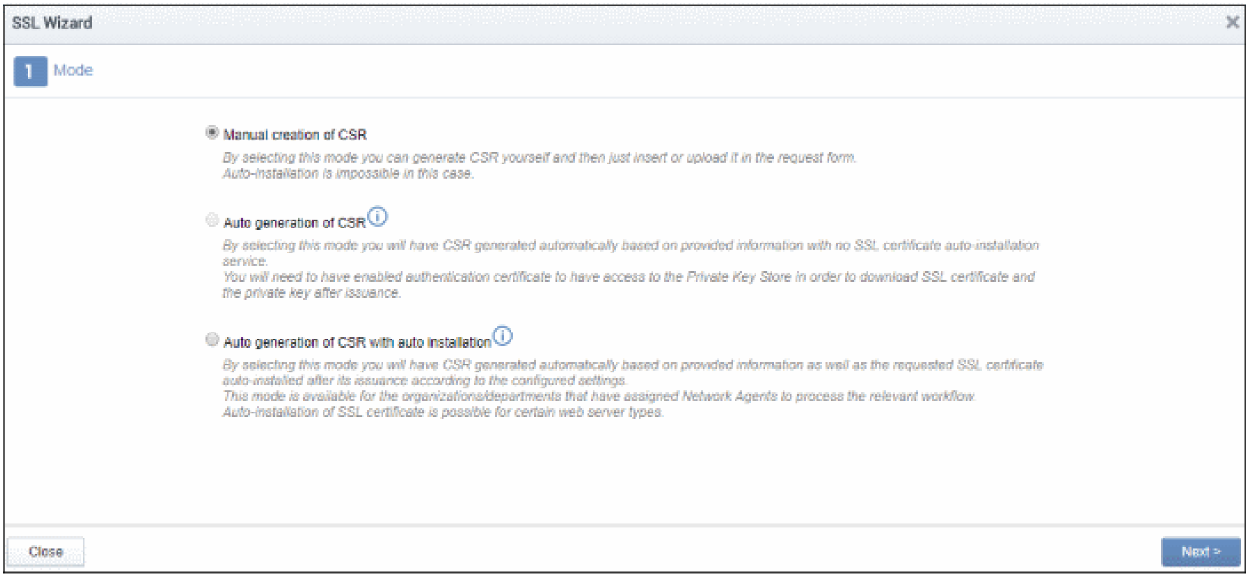
- To view command details, select the command and click the 'Details' button at the top.

3.1.2.2.2 Method 2 - CM Controller Mode

- Administrators can request and install new certificates for domains hosted on different web servers from the 'Certificate Management - SSL Certificates' area.
- 'Incommon CM Controller Mode' requires an agent to be installed on each web server upon which the certificates are to be auto-installed/renewed. See Agents for more details on installing the agent.

To enroll a certificate for auto-installation

- Click the 'Certificates' tab then open the 'SSL Certificates' tab
- Click the 'Add' button
- This will start the SSL enrollment wizard:



● Manual creation of CSR

By selecting this mode you can generate CSR yourself and then just insert or upload it in the request form.
Auto-installation is impossible in this case.

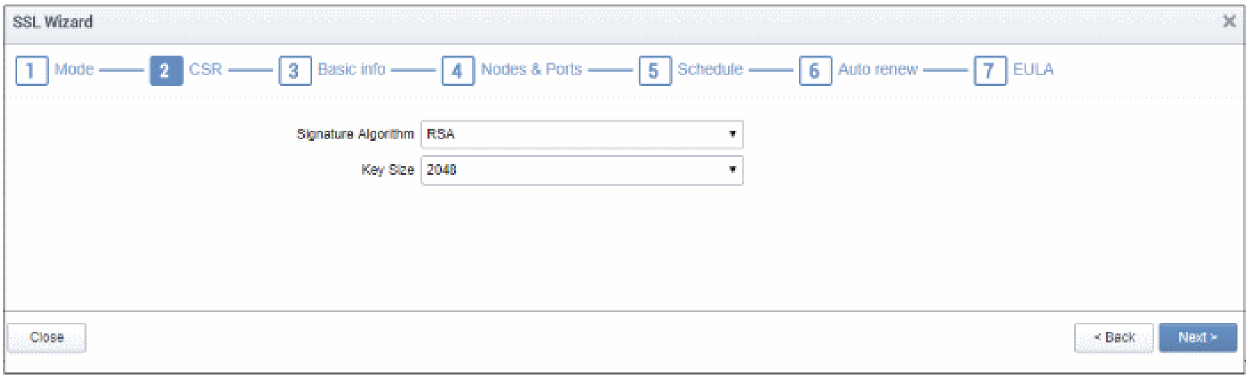
○ Auto generation of CSR

By selecting this mode you will have CSR generated automatically based on provided information with no SSL certificate auto-installation service.
You will need to have enabled authentication certificate to have access to the Private Key Store in order to download SSL certificate and the private key after issuance.

○ Auto generation of CSR with auto installation

By selecting this mode you will have CSR generated automatically based on provided information as well as the requested SSL certificate auto-installed after its issuance according to the configured settings.
This mode is available for the organizations/departments that have assigned Network Agents to process the relevant workflow.
Auto-installation of SSL certificate is possible for certain web server types.

- Select the third option, 'Auto generation of CSR with auto installation', and click 'Next'.

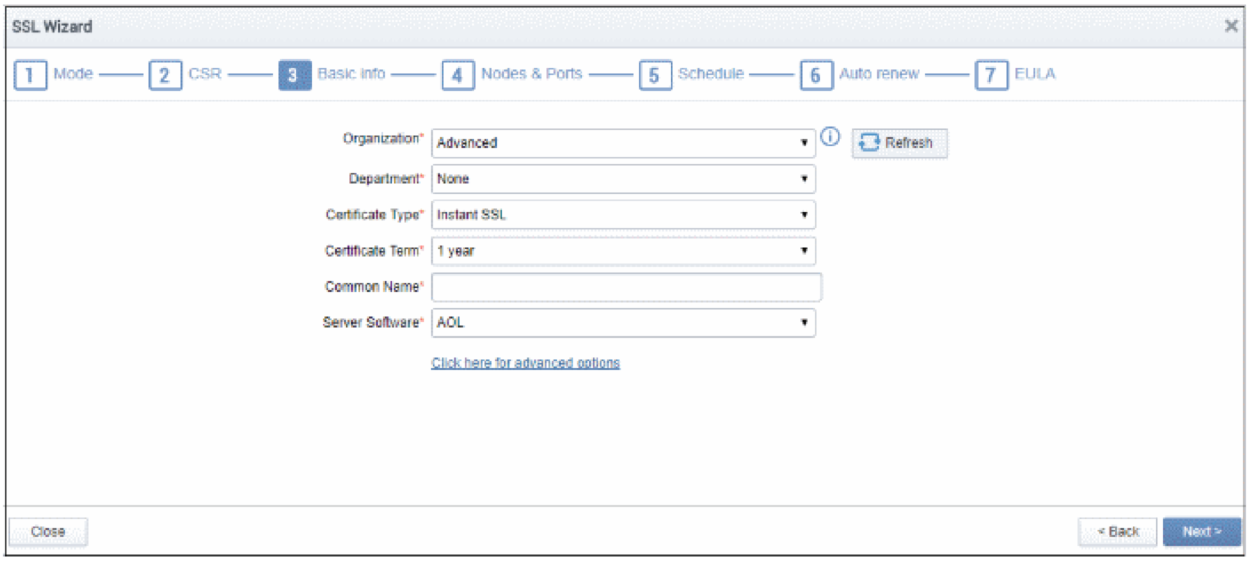


Signature Algorithm: RSA

Key Size: 2048

The next step is to provide the CSR parameters:

  - Signature Algorithm – Select the digital signature algorithm you want to use in the certificate. Currently only RSA is supported.
  - Key Size – Options available are 2048 and 4096. 2048 bit is the recommended industry standard and provides very high security for public-facing and internal hosts. 4096 is even more secure, but may lead to longer connection times due to the extra processing time during the SSL handshake.
- Click 'Next'



Organization*: Advanced

Department*: None

Certificate Type*: Instant SSL

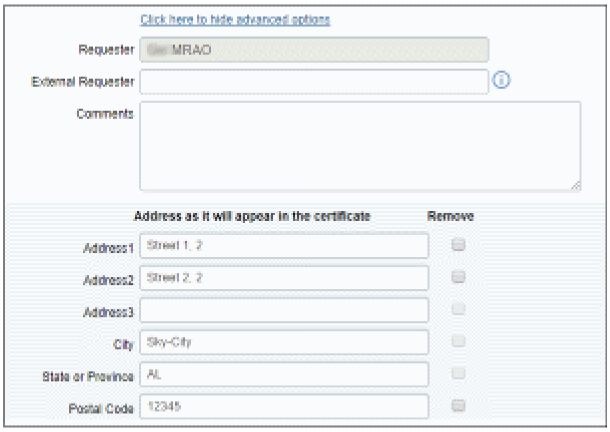
Certificate Term*: 1 year

Common Name*:

Server Software*: AOL

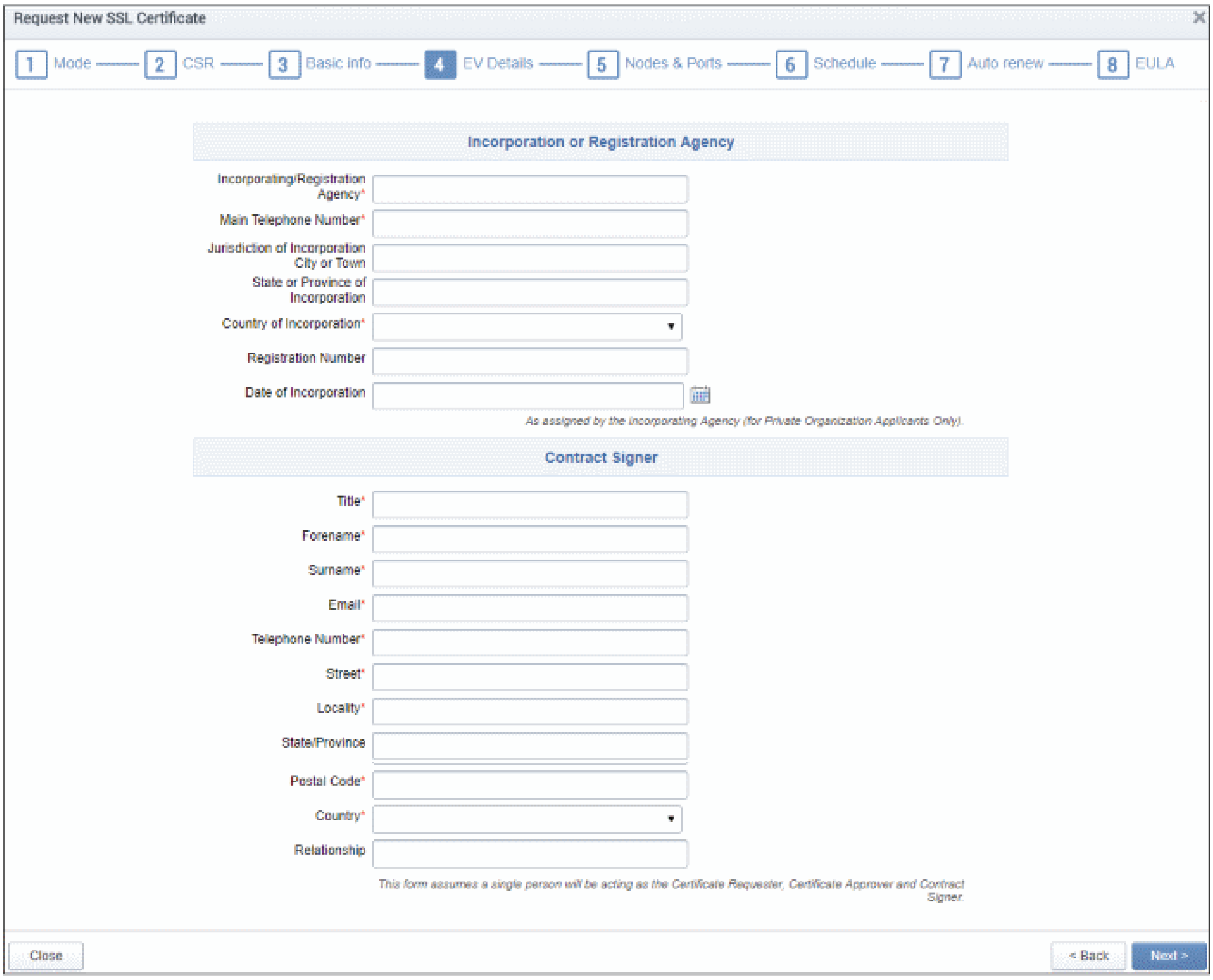
Click here for advanced options

Form Element	Type	Description
Organization (***required***)	Drop-down list	Choose the Organization that the SSL certificate will belong to.
Department (***required***)	Drop-down list	Choose the Department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'.
Certificate Type (***required***)	Drop-down list	Choose the certificate type that you wish to add for auto-installation. See Comodo SSL Certificates for a list of certificate types. The specific certificate types displayed in the drop-down list depends on the SSL Types allowed for the selected organization. See Editing a new Organization and Customize an Organization's SSL Certificate Types
Certificate Term (***required***)	Drop-down list	Choose the validity period of the certificate. For example, 1 year, 2 years, 3 years. See **Comodo SSL Certificates** for a list of certificate types and term lengths. The validity periods available for a particular Organization depends on its configuration. See Editing a new Organization and Customize an Organization's SSL Certificate Types.
Common Name (***required***)	Text Field	Type the domain that the certificate will be issued to.
Server Software (***required***)	Drop-down list	Select the server software on which the certificate is to be installed. Note: Choose 'OTHER' if you want to use F5 BIG-IP.
Subject Alternative Names (***optional***)	Text Field	This field appears only if a multi domain or UCC certificate type is selected. Specify the additional domain names. Each domain name should be separated by a comma.
Click here for advanced options	Text Fields	Clicking this link will expand the address fields.

Form Element	Type	Description
		 Click here to hide advanced options Requester: [redacted] MRAO External Requester: Comments: Address as it will appear in the certificate — Remove Address1: Street 1, 2 □ Address2: Street 2, 2 □ Address3: □ City: Sky-City □ State or Province: AL □ Postal Code: 12345 □ • Requester – This field is auto-populated with the name of the administrator making the application. • External Requester (optional) - Enter the email address of an external requester on whose behalf the application is made. **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. • Comments (optional) - Enter your comments on the certificate. **Address fields in the certificate** • 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 of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and 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.

- Click 'Next'

The EV Details wizard will appear if you choose EV certificate type:



Incorporation or Registration Agency

Incorporating/Registration Agency*

Main Telephone Number*

Jurisdiction of Incorporation City or Town

State or Province of Incorporation

Country of Incorporation*

Registration Number

Date of Incorporation

As assigned by the incorporating Agency (for Private Organization Applicants Only).

Contract Signer

Title*

Forename*

Surname*

Email*

Telephone Number*

Street*

Locality*

State/Province

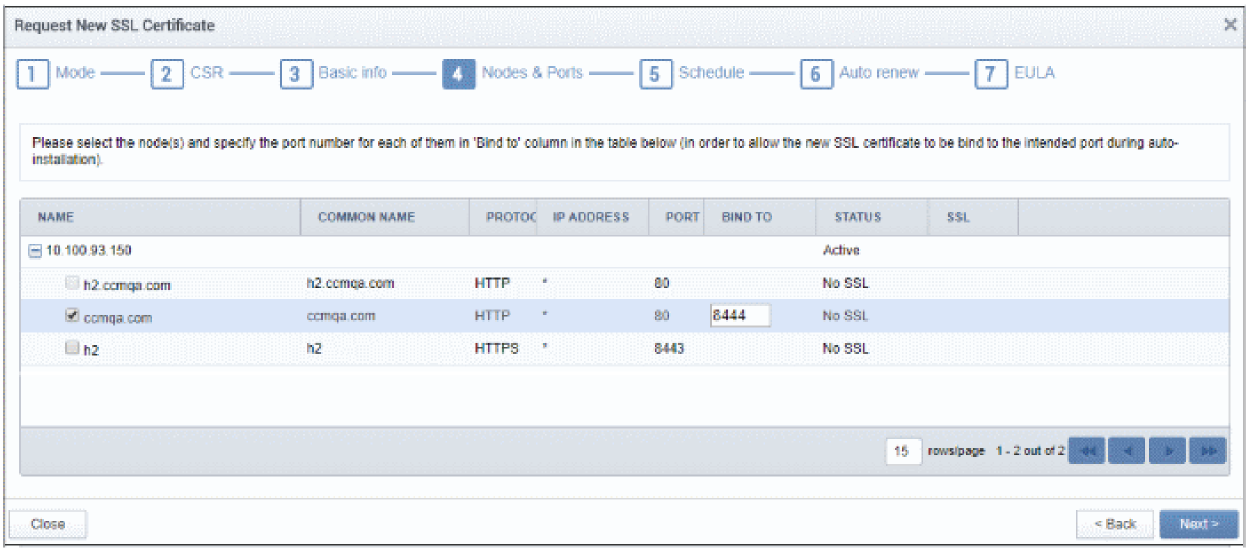
Postal Code*

Country*

Relationship

This form assumes a single person will be acting as the Certificate Requester, Certificate Approver and Contract Signer.

- The details you need to complete depends on the EV mode activated for your account.
- This is same information as provided in the EV details tab when adding a new organization. See 'EV Details Tab' for more info. If the EV type is 'RA' for your account, this will be auto-populated.
- Click 'Next' when all required fields are complete.



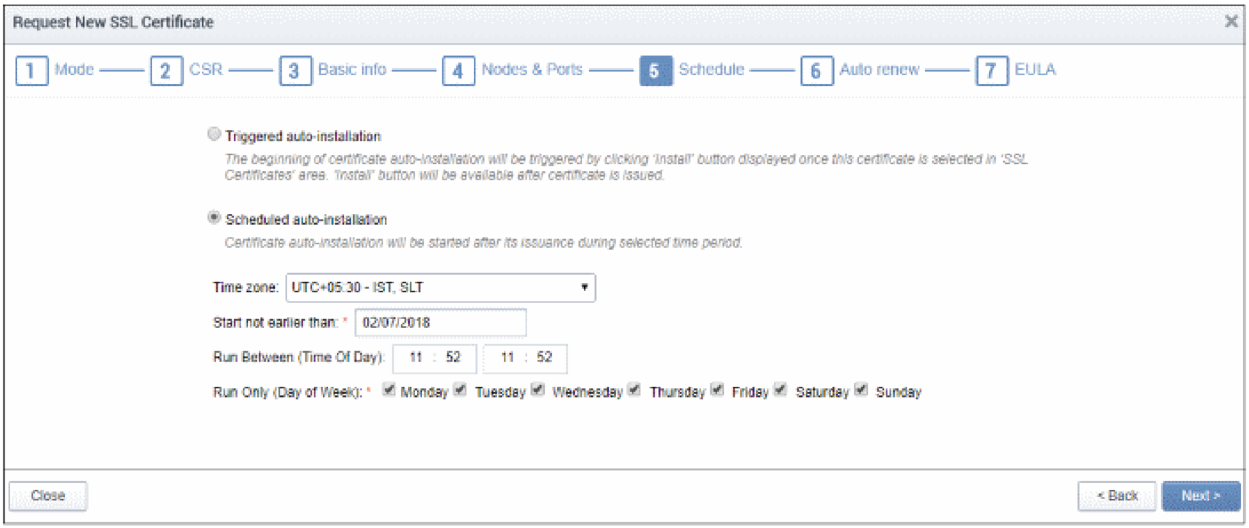
Please select the node(s) and specify the port number for each of them in 'Bind to' column in the table below (in order to allow the new SSL certificate to be bind to the intended port during auto-installation).

NAME	COMMON NAME	PROTOC	IP ADDRESS	PORT	BIND TO	STATUS	SSL
⊟ 10.100.93.150						Active	
□ h2.ccmqa.com	h2.ccmqa.com	HTTP	*	80		No SSL	
☑ ccmqa.com	ccmqa.com	HTTP	*	80	8444	No SSL	
□ h2	h2	HTTPS	*	8443		No SSL	

15 rows/page 1 - 2 out of 2

The 'Nodes & Ports' wizard displays the configured options.

- A list of server nodes is shown under each agent.
- Select the domain on which you want to install the certificate.
    - Bind To - Specify the port number to which the SSL certificate should be bind to after issuance. This is editable only for protocol with HTTP status.
- Click 'Next'



Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — 5 Schedule — 6 Auto renew — 7 EULA

○ Triggered auto-installation

The beginning of certificate auto-installation will be triggered by clicking 'Install' button displayed once this certificate is selected in 'SSL Certificates' area. 'Install' button will be available after certificate is issued.

● Scheduled auto-installation

Certificate auto-installation will be started after its issuance during selected time period.

Time zone: UTC+05:30 - IST, SLT

Start not earlier than: * 02/07/2018

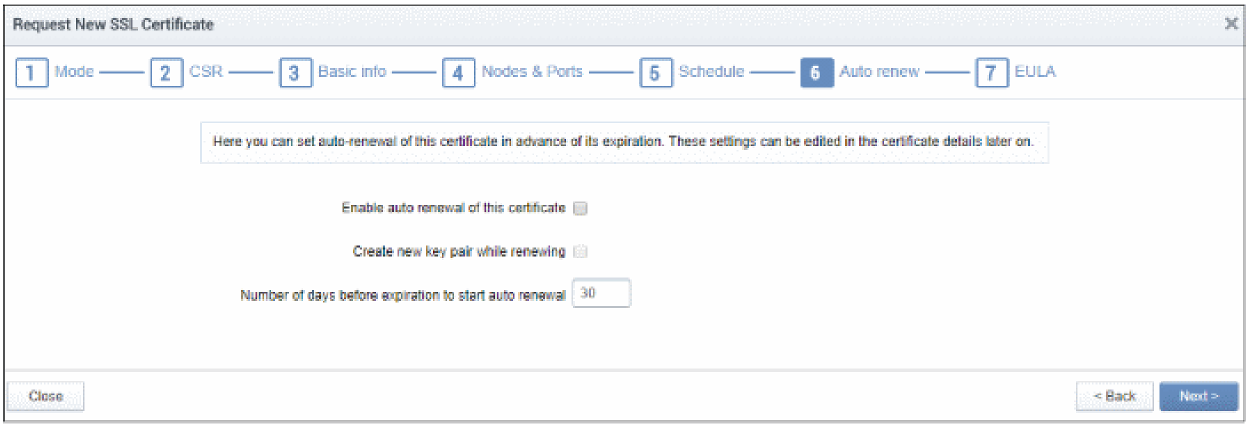
Run Between (Time Of Day): 11 : 52 11 : 52

Run Only (Day of Week): * ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Schedule - Choose whether you want to start auto-installation manually or schedule for a later time.

- 'Triggered auto-installation' – You need to start the auto-installation manually after completing the wizard. To do this, go to 'Certificates' > 'SSL Certificates' > select the certificate > Click 'Install'
- 'Scheduled auto-installation' – Specify a date and time to run the auto-installer. The controller will generate the CSR and submit it to Incommon the next time it polls Incommon CM after the scheduled time.

- Click 'Next'.



Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — 5 Schedule — 6 Auto renew — 7 EULA

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

Enable auto renewal of this certificate □

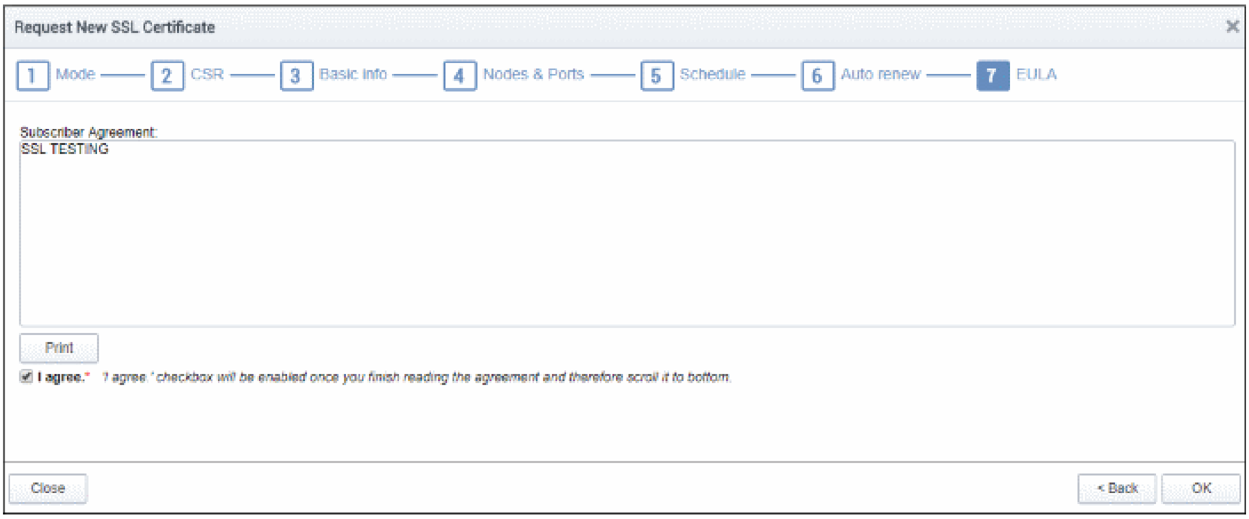
Create new key pair while renewing □

Number of days before expiration to start auto renewal 30

The next step is to configure the auto-renewal options.

- Enable auto renewal of this certificate – Select this to have Incommon CM apply for a new certificate when this one approaches expiry.
- Create new key pair while renewing – If the option above is selected, then choose whether or not you want a generate a new key pair for the renewed certificate. Leaving it disabled means Incommon CM will re-use the key pair of the old certificate.
- Number of days before expiration to start auto renewal - Choose the number of days in advance of expiry that the renewal process should start. On the scheduled day, the certificate controller will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.

- Click 'Next'



Request New SSL Certificate

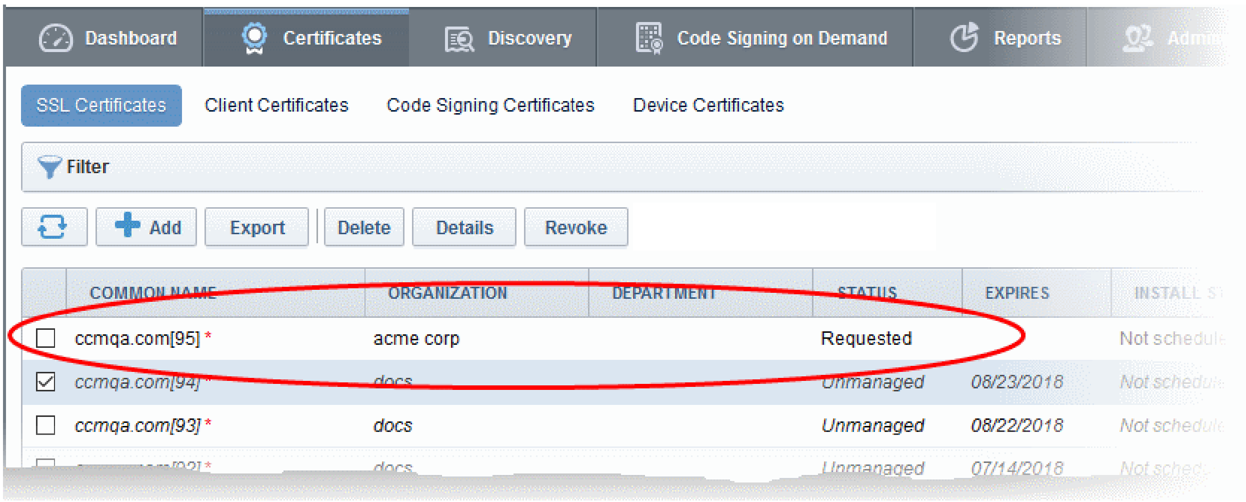
Subscriber Agreement:
SSL TESTING

☑ I agree.* 'I agree.' checkbox will be enabled once you finish reading the agreement and therefore scroll it to bottom.

The final stage is to agree to the EULA.

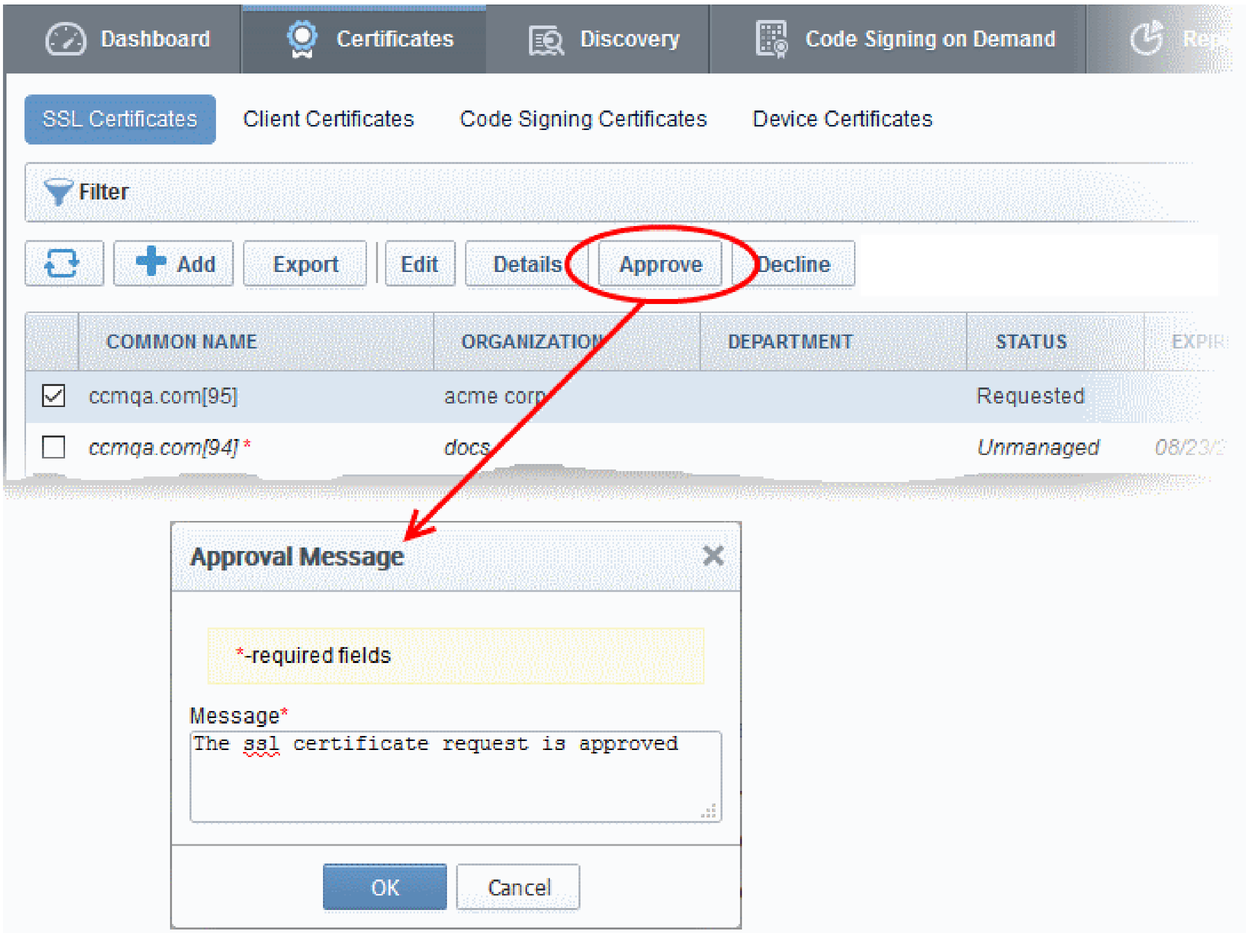
- Read the EULA fully and accept to by the selecting 'I Agree' checkbox.
- Click 'OK' to submit the application

The certificate will be added to the 'SSL Certificates' interface with a status of 'Requested'.



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL S
☐	ccmqa.com[95] *	acme corp		Requested		Not schedul
☑	ccmqa.com[94] *	docs		Unmanaged	08/23/2018	Not schedul
☐	ccmqa.com[93] *	docs		Unmanaged	08/22/2018	Not schedul
☐	ccmqa.com[92] *	docs		Unmanaged	07/14/2018	Not sched

- The CSR for the requested certificate will be generated automatically. After the CSR has been created, the 'Approve' button will appear at the top when you select the certificate in the list:



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIR
☑	ccmqa.com[95]	acme corp		Requested	
□	*ccmqa.com[94]* *	*docs*		*Unmanaged*	*08/23/*

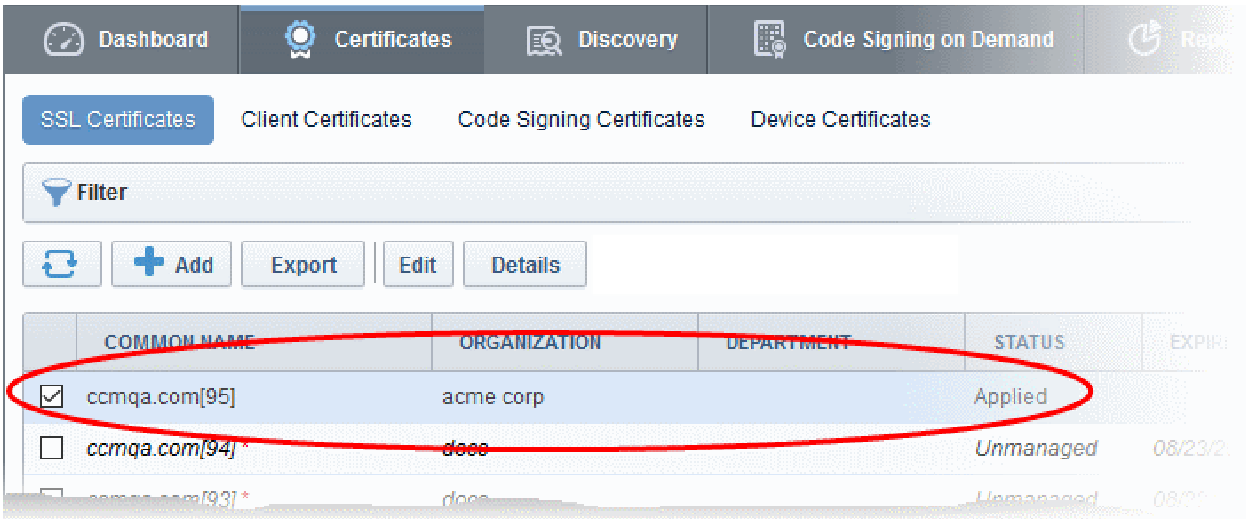
Approval Message

*-required fields

Message*

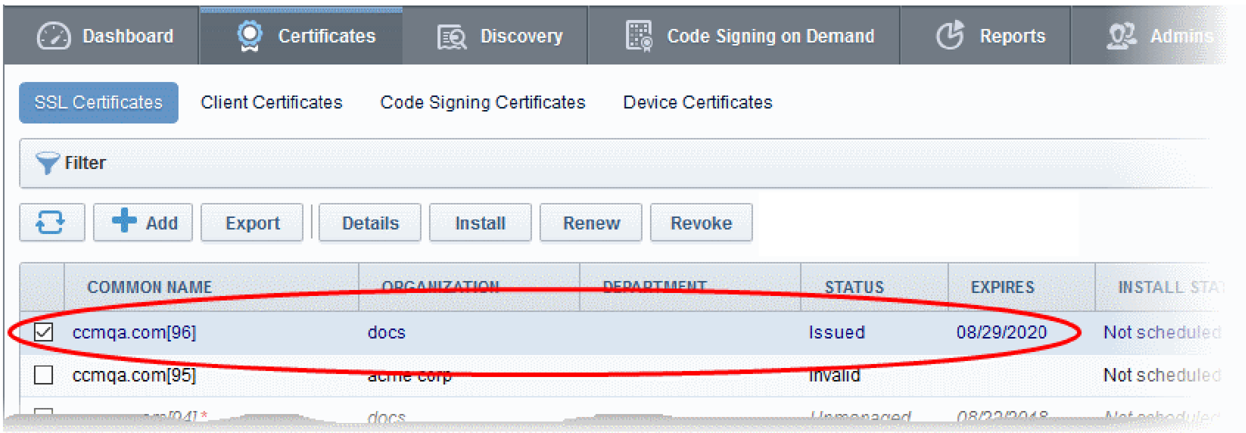
The ssl certificate request is approved

- Click the 'Approve' button to approve the request, enter an approval message and click 'OK'.
- On approval, the CSR will be submitted to Incommon CA to apply for the certificate. The certificate status will change to 'Applied'.



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIR
☑	ccmqa.com[95]	acme corp		Applied	
□	ccmqa.com[94] *	docs		Unmanaged	08/23/2
□	ccmqa.com[93] *	docs		Unmanaged	08/2

The controller will track the order number then collect and store the certificate once it is issued. The certificate status will change to 'Issued'.

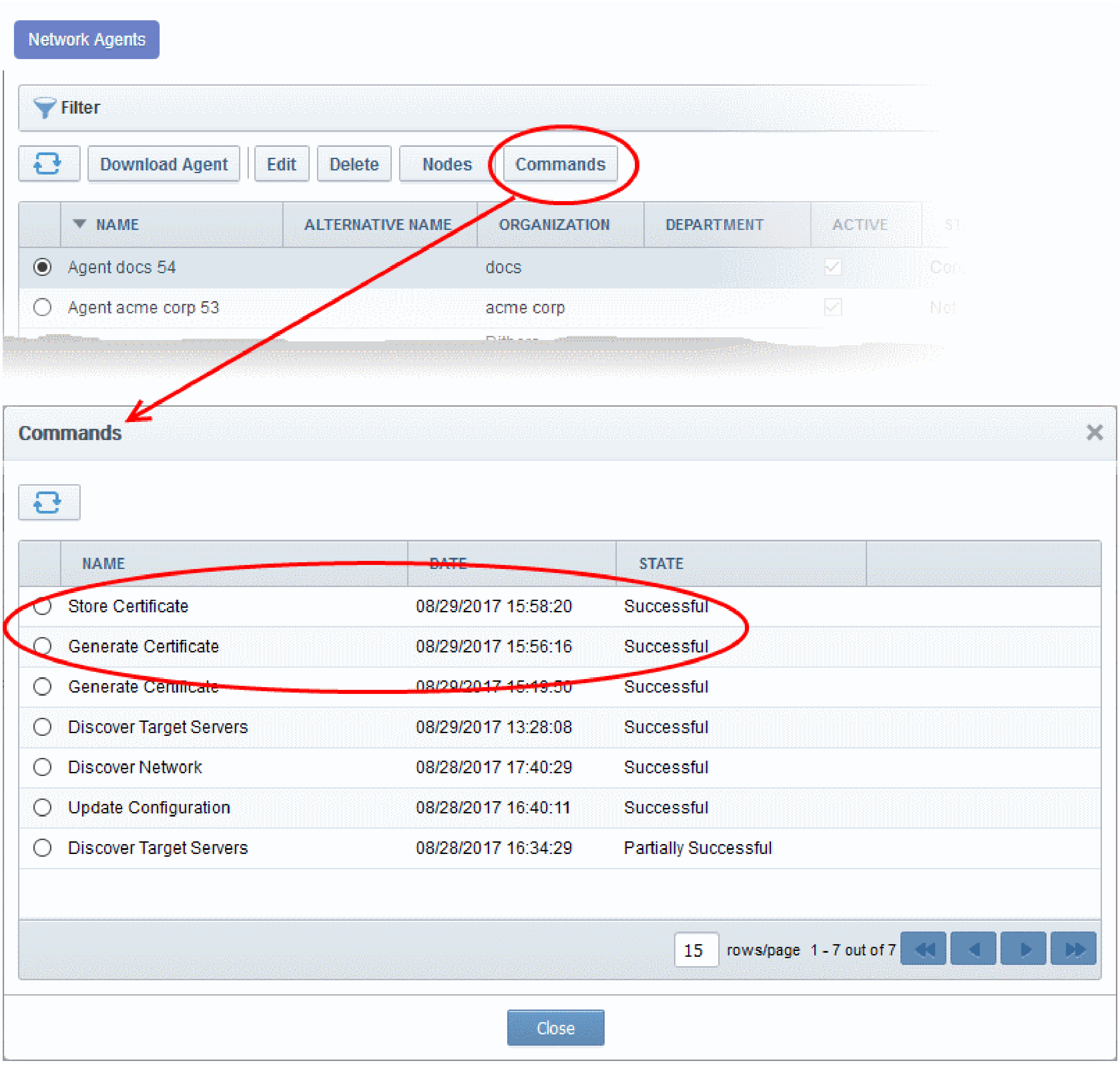


	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STA
☑	ccmqa.com[96]	docs		Issued	08/29/2020	Not scheduled
□	ccmqa.com[95]	acme corp		Invalid		Not scheduled
□	ccmqa.com[94] *	docs		Unmanaged	08/23/2018	Not scheduled

To check whether the certificate controller has stored the certificate:

- Click 'Settings' > 'Agents' > 'Network Agents'
- Select the controller and click the 'Commands' button

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



	NAME	ALTERNATIVE NAME	ORGANIZATION	DEPARTMENT	ACTIVE	ST
●	Agent docs 54		docs		☑	Con
○	Agent acme corp 53		acme corp		☑	Not

Commands

	NAME	DATE	STATE
○	Store Certificate	08/29/2017 15:58:20	Successful
○	Generate Certificate	08/29/2017 15:56:16	Successful
○	Generate Certificate	08/29/2017 15:19:50	Successful
○	Discover Target Servers	08/29/2017 13:28:08	Successful
○	Discover Network	08/28/2017 17:40:29	Successful
○	Update Configuration	08/28/2017 16:40:11	Successful
○	Discover Target Servers	08/28/2017 16:34:29	Partially Successful

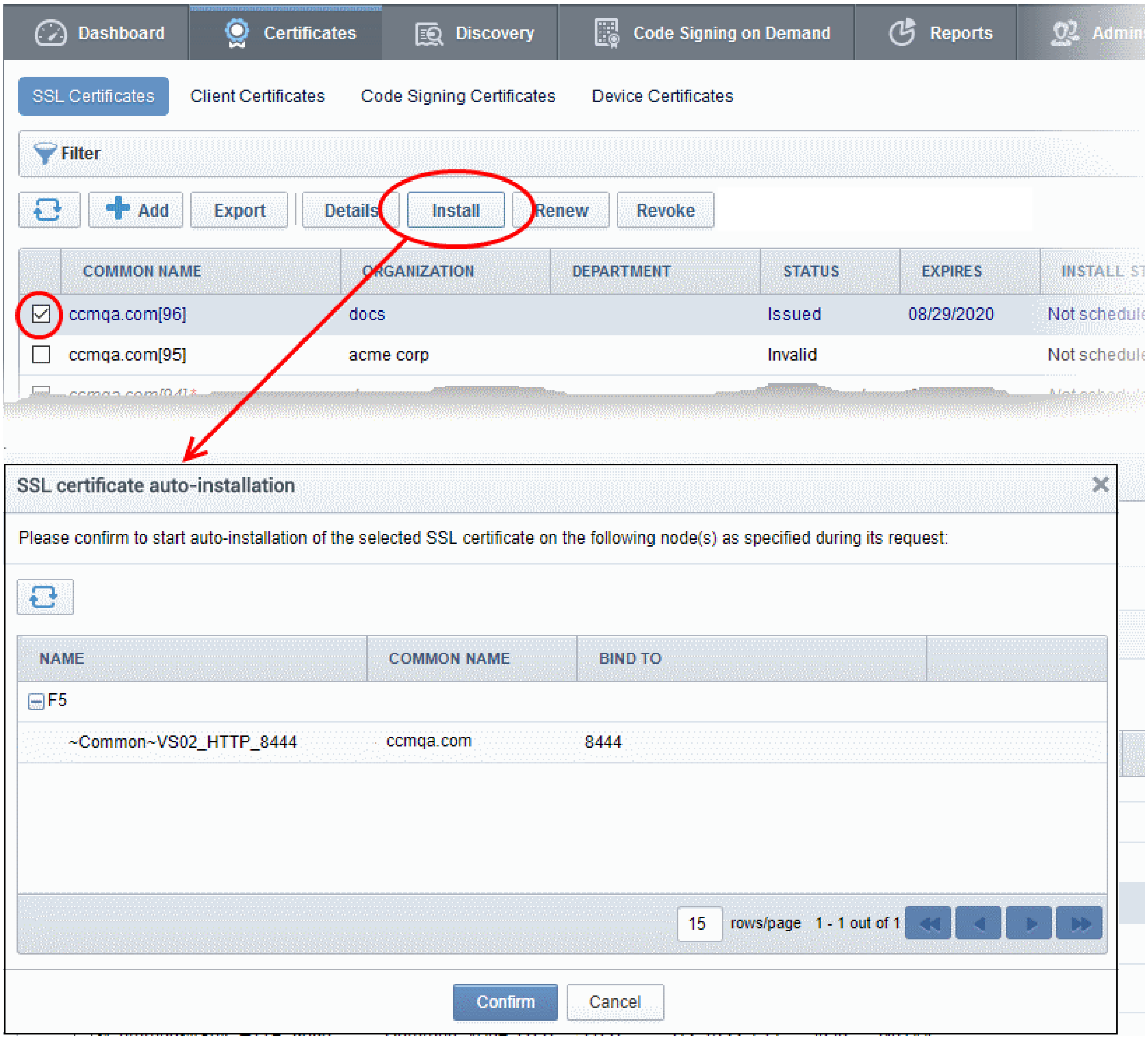
15 rows/page 1 - 7 out of 7

The certificate is stored on the server by the agent.

- If you set a schedule for automatic installation, it will be installed automatically at the scheduled time.
- If you selected 'Triggered auto-installation' you can manually initiate installation (or schedule auto-installation) from the 'Certificates' > 'SSL Certificates' interface:

To manually initiate auto-installation of a certificate

- Click 'Certificates' > 'SSL Certificates'
- Select the certificate from the list and click 'Install':



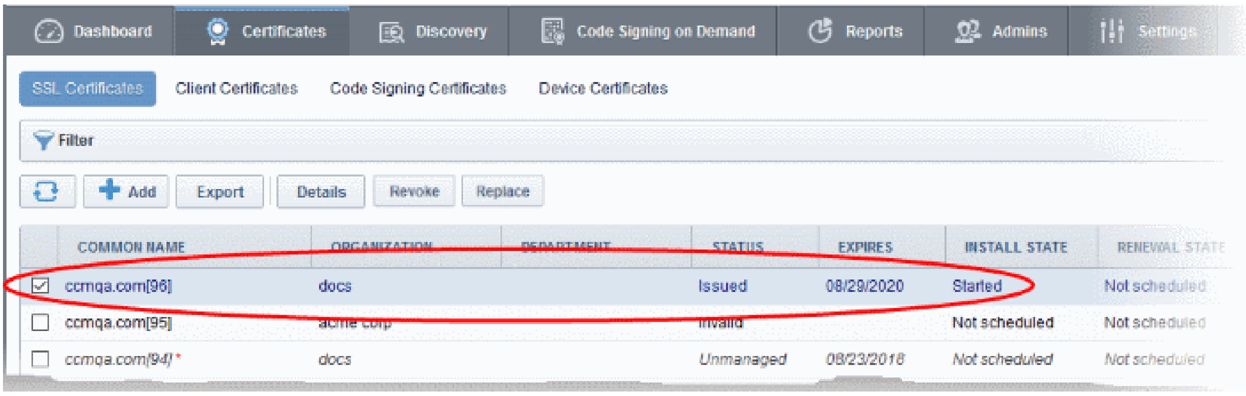
	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL ST
☑	ccmqa.com[96]	docs		Issued	08/29/2020	Not schedule
□	ccmqa.com[95]	acme corp		Invalid		Not schedule

SSL certificate auto-installation

Please confirm to start auto-installation of the selected SSL certificate on the following node(s) as specified during its request:

NAME	COMMON NAME	BIND TO	
⊟F5			
~Common~VS02_HTTP_8444	ccmqa.com	8444	

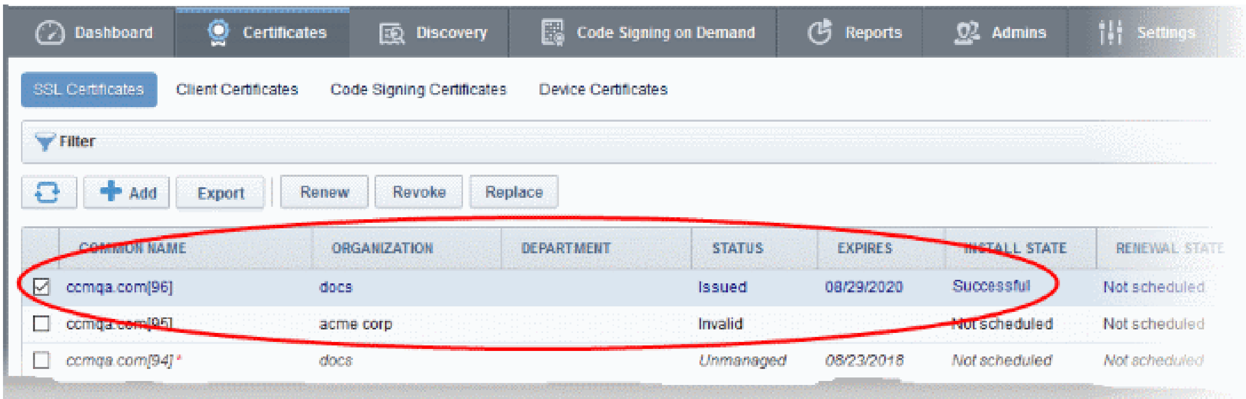
The installation will begin instantly. Once the installation commences, the 'Install State' of the certificate will change to 'Started'.



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
☑	ccmqa.com[96]	docs		Issued	08/29/2020	Started	Not scheduled
□	ccmqa.com[95]	acme corp		Invalid		Not scheduled	Not scheduled
□	ccmqa.com[94]*	docs		Unmanaged	08/23/2018	Not scheduled	Not scheduled

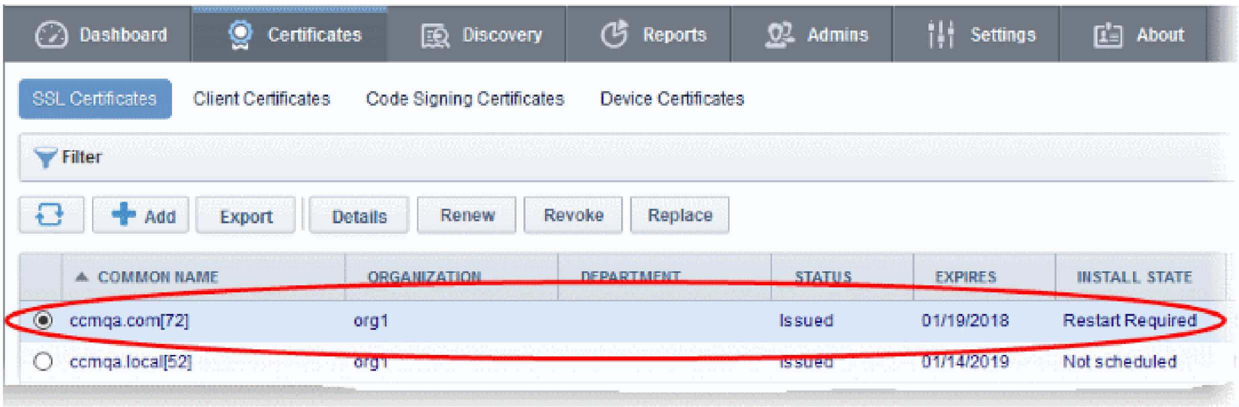
When installation is complete:

- IIS servers and Tomcat servers - The certificate will be activated immediately and the install state will change to 'Successful'.



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
☑	ccmqa.com[96]	docs		Issued	08/29/2020	Successful	Not scheduled
□	ccmqa.com[95]	acme corp		Invalid		Not scheduled	Not scheduled
□	ccmqa.com[94]*	docs		Unmanaged	08/23/2018	Not scheduled	Not scheduled

- Apache servers - The certificate will become active after the server is restarted. The install state will change to 'Restart Required'.



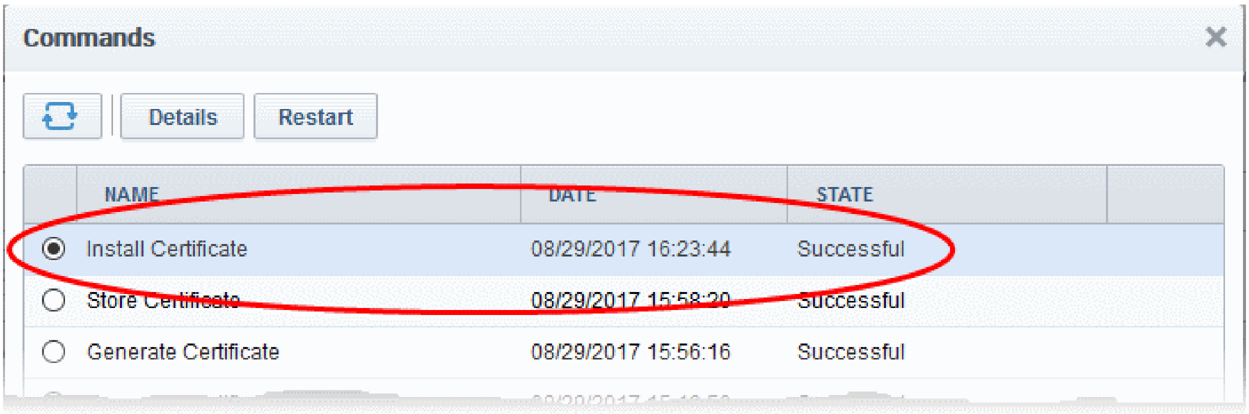
	▲ COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE
●	ccmqa.com[72]	org1		Issued	01/19/2018	Restart Required
○	ccmqa.local[52]	org1		Issued	01/14/2019	Not scheduled

Tip: The server can be restarted from Incommon CM through the SSL Certificate 'Details' Dialog dialog. See Restarting Apache after Auto-Installation of SSL Certificate, for more details.

After restarting the server, the certificate will activated and the 'Install State' will change to 'Successful'.

- To check whether the controller has installed the certificate, click Settings > Agents > Network Agents
- Select the controller and click the 'Commands' button

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



	NAME	DATE	STATE
●	Install Certificate	08/29/2017 16:23:44	Successful
○	Store Certificate	08/29/2017 15:58:20	Successful
○	Generate Certificate	08/29/2017 15:56:16	Successful

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

3.1.2.3 Initiating SSL Enrollment using Application Forms

SSL administrators, or applicants authorized by them, can request certificates by completing an application form. On successful submission and validation by Incommon 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 as planned.

Incommon CM offers two types of SSL application forms:

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.

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

The Enrollment Wizard- Admins can login and request SSL certificates using the wizard at 'Certificates Management' > 'SSL Certificates'. The wizard allows you to enroll for SSL certificates in two ways:

i. **Manual CSR Generation** - The administrator needs to generate the certificate signing request (CSR) at the server on which the certificate needs to be installed and enter the CSR in the wizard. See Method 2 - Built-in Enrollment Wizard - Manual CSR Generation for a tutorial on applying for and installing certificates.

ii. **Auto CSR Generation** - Incommon CM can generate the CSR for the domain name with the private key stored by the Private Key Store controller installed on a server at the customer premises. On completion of certificate issuance, the administrator can download the certificate with the public/private key pair from Incommon CM and import to the server(s) on which it needs to be installed. See Method 3 - Built-in Enrollment Wizard - Auto CSR Generation for a tutorial on applying for and installing certificates.

- After submitting the application form, the certificate will be added to 'Certificates Management' > 'SSL Certificates' with the status 'Requested'.

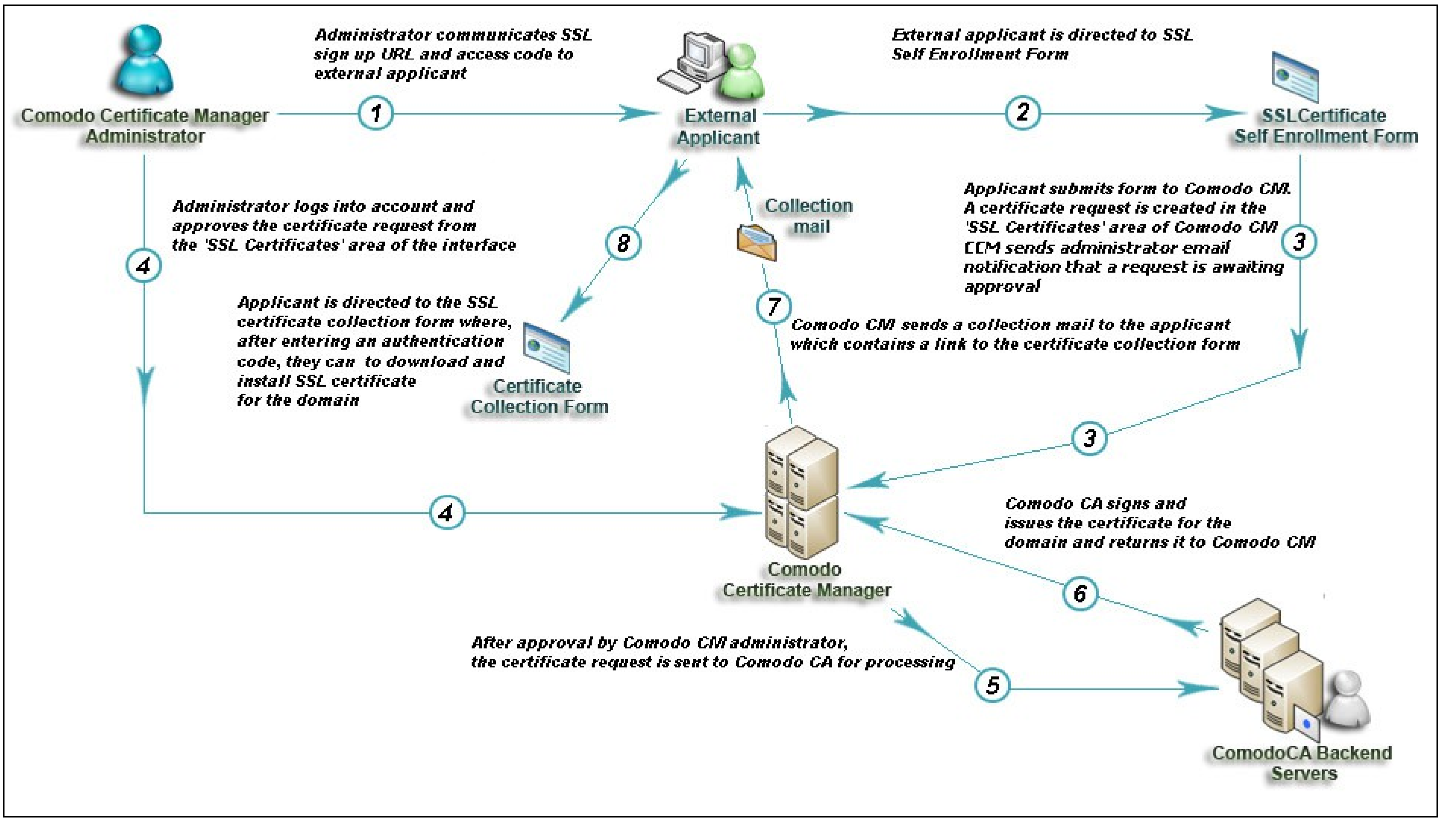
  An appropriately privileged SSL administrator should approve the request. On approval, Incommon CM will forward the application to Incommon CA.

- After validating the application, the CA will issue the certificate and the certificate status will change to 'Issued'. A collection email will be sent to the applicant.

- The applicant can collect, download and install the certificate on the respective web server.

  For more details on certificate collection, see Certificate Collection. For more details on downloading and installing the certificate, see Downloading and Importing SSL Certificates.

3.1.2.3.1 Method 1 - Self Enrollment Form


Comodo Certificate Manager Administrator
1
Administrator communicates SSL sign up URL and access code to external applicant
External Applicant
2
External applicant is directed to SSL Self Enrollment Form
SSLCertificate Self Enrollment Form
4
Administrator logs into account and approves the certificate request from the 'SSL Certificates' area of the interface
8
Collection mail
3
Applicant submits form to Comodo CM. A certificate request is created in the 'SSL Certificates' area of Comodo CM CCM sends administrator email notification that a request is awaiting approval
Applicant is directed to the SSL certificate collection form where, after entering an authentication code, they can to download and install SSL certificate for the domain
Certificate Collection Form
7
Comodo CM sends a collection mail to the applicant which contains a link to the certificate collection form
3
4
Comodo Certificate Manager
Comodo CA signs and issues the certificate for the domain and returns it to Comodo CM
6
After approval by Comodo CM administrator, the certificate request is sent to Comodo CA for processing
5
ComodoCA Backend Servers

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:

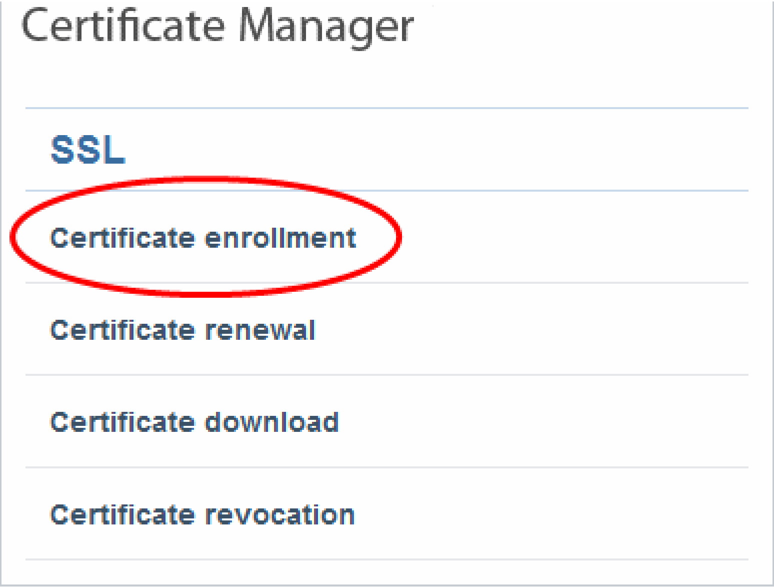
1. A link to the Self Enrollment Form - https://cert-manager.com/customer/InCommon/ssl?action=enroll
2. The Access Code specified in the organization or department's SSL Certificates tab.

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.

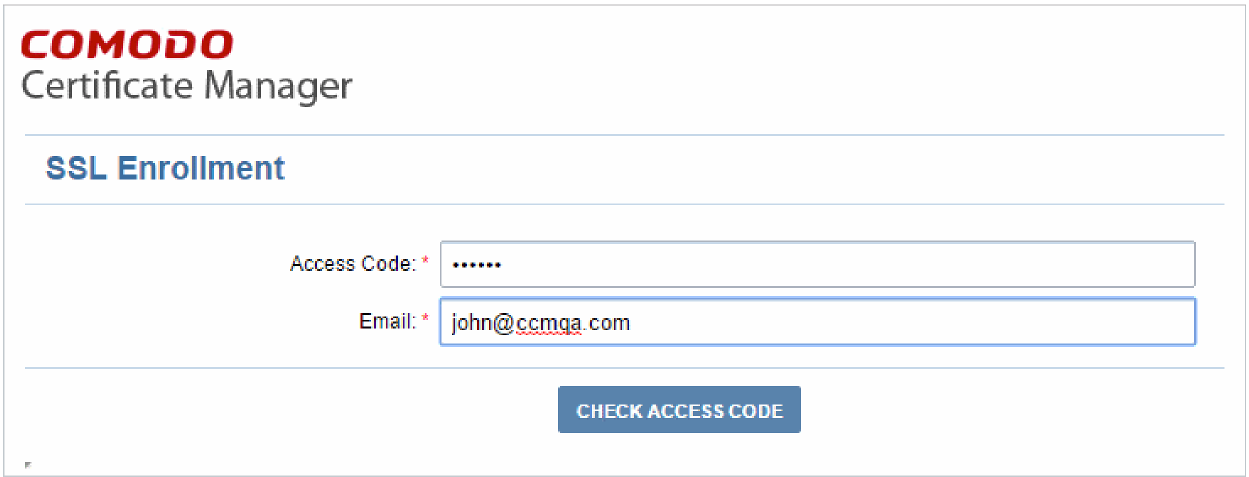
3.1.2.3.1.2 The Self Enrollment Form

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

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



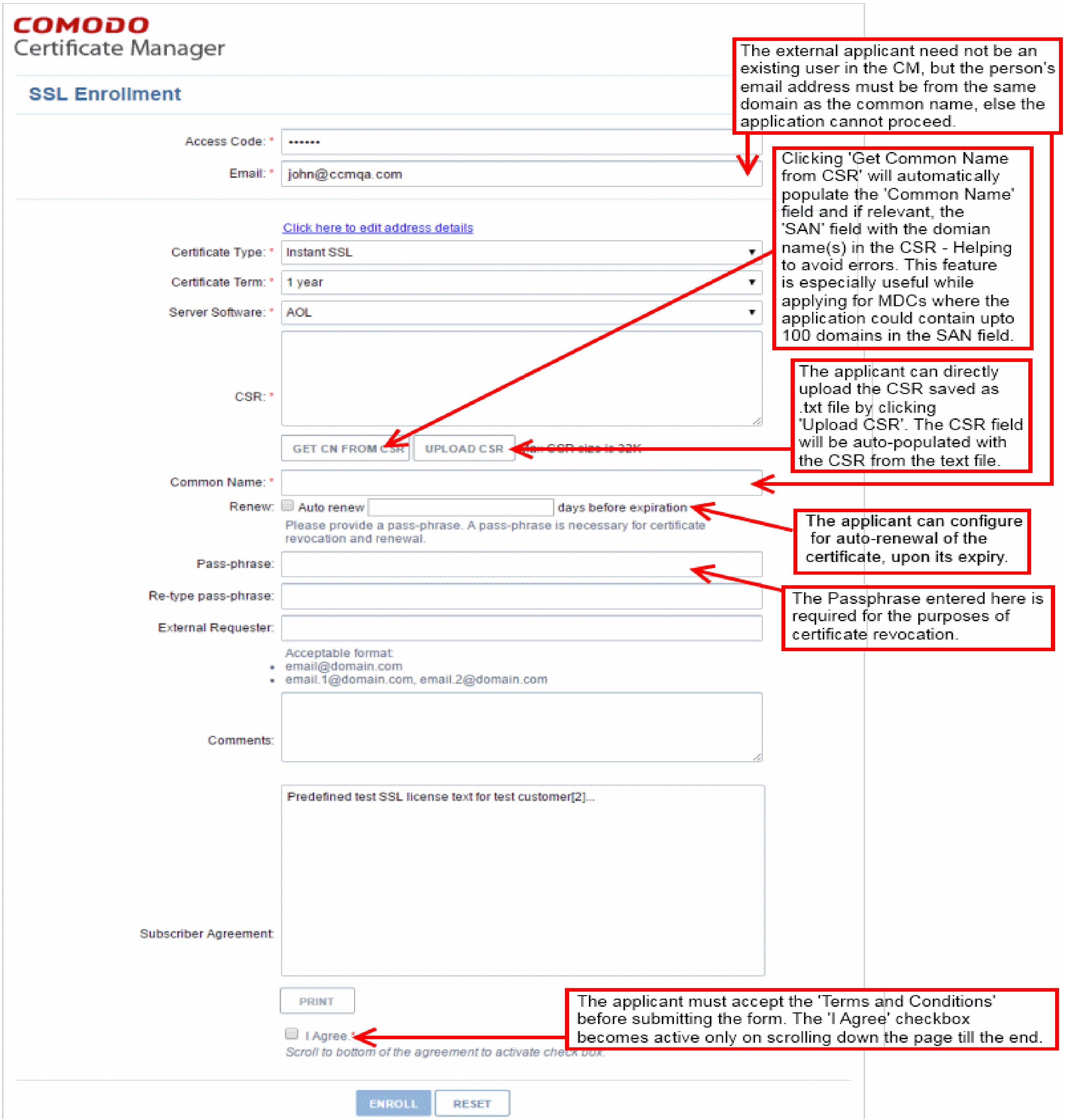
- Clicking the 'Certificate enrollment' link will open the self enrollment form



Access Code: * ••••••

Email: * john@ccmqa.com

- 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 'Check Access Code' will contact CM 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:



COMODO Certificate Manager

SSL Enrollment

Access Code: *	••••••
Email: *	john@ccmqa.com
	Click here to edit address details
Certificate Type: *	Instant SSL
Certificate Term: *	1 year
Server Software: *	AOL
CSR: *	
	GET CN FROM CSR · UPLOAD CSR · Max CSR size is 32K
Common Name: *	
Renew:	□ Auto renew ___ days before expiration
	Please provide a pass-phrase. A pass-phrase is necessary for certificate revocation and renewal.
Pass-phrase:	
Re-type pass-phrase:	
External Requester:	
	Acceptable format: • email@domain.com • email.1@domain.com, email.2@domain.com
Comments:	
Subscriber Agreement:	Predefined test SSL license text for test customer[2]...
	PRINT
	□ I Agree * *Scroll to bottom of the agreement to activate check box.*

The external applicant need not be an existing user in the CM, but the person's email address must be from the same domain as the common name, else the application cannot proceed.

Clicking 'Get Common Name from CSR' will automatically populate the 'Common Name' field and if relevant, the 'SAN' field with the domian name(s) in the CSR - Helping to avoid errors. This feature is especially useful while applying for MDCs where the application could contain upto 100 domains in the SAN field.

The applicant can directly upload the CSR saved as .txt file by clicking 'Upload CSR'. The CSR field will be auto-populated with the CSR from the text file.

The applicant can configure for auto-renewal of the certificate, upon its expiry.

The Passphrase entered here is required for the purposes of certificate revocation.

The applicant must accept the 'Terms and Conditions' before submitting the form. The 'I Agree' checkbox becomes active only on scrolling down the page till the end.

- 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.
- Applicants requesting Extended Validation (EV) SSL certificates need to follow the steps on the following InCommon EV SSL page https://www.incommon.org/cert/evcerts.html.

- It is possible for Certificate Manager Account holders to use their own, custom form templates rather than the default form supplied by InCommon. Contact your account manager for more details on enabling this functionality and for submitting custom banners for application forms

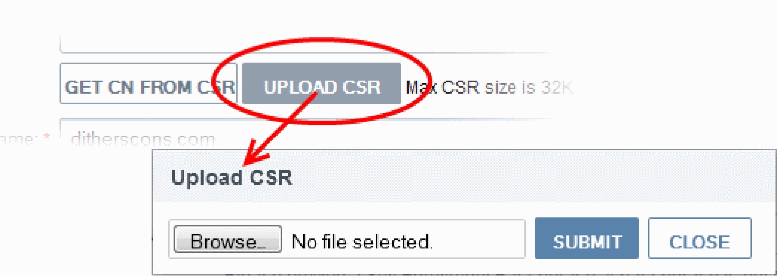
3.1.2.3.1.3 Form Parameters

- Comodo, an InCommon partner provides 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 (Select 'CSR generation' section and web server software).

Form Element	Type	Description
Access Code ***(required)***	Text Field	• Applicants that request a certificate using the self-enrollment form will need to enter the access code. • The code identifies a particular organization or department and is used to authenticate certificate requests made using the self-enrollment form. • Organizations and departments are uniquely identified by a combination of the organization's 'Access Code' and 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 which contains a mixture of alpha and numeric characters which cannot easily be guessed. This code needs to be communicated to the applicant(s) along with the URL of the sign up form.
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.
Address Details Displayed on clicking the Click here to edit address details link. Address 1: Address 2: Address 3: City: State or Province: Postal Code: (all auto-populated)	Text Fields	• Click 'Click here to edit address' to view and edit the address fields. • The address fields are auto-populated from the details in the 'General Settings' tab of the organization or department on whose behalf the 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 address details of the organization, Incorporating or Registration Agency, Certificate Requester and the Contract Signer. Therefore, these fields cannot be removed from the EV self-enrollment forms.

Form Element	Type	Description
Certificate Types ***(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. See Editing a new Organization and Customize an Organization's SSL Certificate Types for more details.
Certificate Term ***(required)***	Drop-down list	Applicant should select the life time of the certificate chosen from the 'Certificate Type ' drop-down. The available term lengths for different certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the organization. See Editing a new Organization and Customize an Organization's SSL Certificate 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 the Comodo's 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 • 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

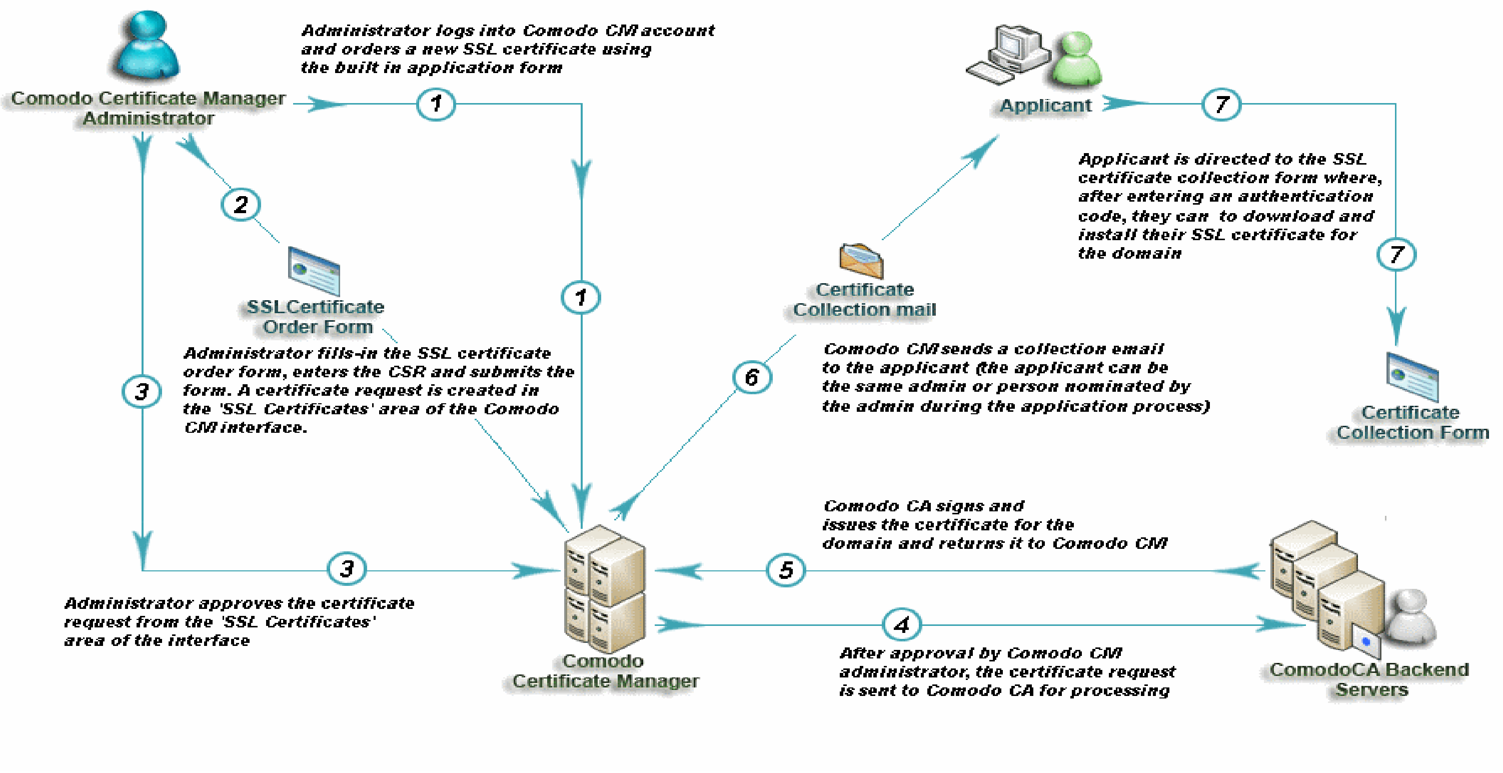
Form Element	Type	Description
		Comodo knowledgebase article for their web server type here: https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,1 **Special Note regarding MDC applications**: The CSR you generate only needs to be for the single 'Common Name' (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 entered correctly, clicking this button will auto-populate the Common Name (CN) field. • This method helps avoid human error by ensuring the domain name in the application form exactly matches the domain in the CSR. • If the domain name mentioned in the form does not match the one in the CSR, then Incommon 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.  GET CN FROM CSR UPLOAD CSR Max CSR size is 32K ame: * ditherscons.com Upload CSR Browse... No file selected. SUBMIT CLOSE
Common Name ***(required)***	Text Field	Applicants should enter the correct fully qualified domain name for the organization or department • Single Domain certificates – enter the domain name using the format: example.com • Wildcard Certificates - enter domain name using the format: *.example.com. • Multi-Domain Certificates - enter the primary domain name using the format: example.com.
Renew	Check box	Allows applicants to specify whether the certificate should be automatically

Form Element	Type	Description
		renewed when it is nearing expiry. Applicants can also choose the number of days in advance of expiry that the renewal process should start. On the scheduled day, Incommon CM will automatically submit the renewal application to the CA with a CSR generated using the same parameters as the existing certificate.

Form Element	Type	Description
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.
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
Re-type Pass Phrase ***(required if specified in the field above)***	Text Field	Confirmation of the above.
External Requester (***optional***)	Text Field	Applicants should enter the full email address of the user on behalf of whom the application is made. The email address must be from the same domain name for which the certificate is applied. The certificate collection email will be sent to this email address.
Comments ***(optional)***	Text Field	Applicant can enter information for the administrator.
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.
Enroll	Control	Submits the application and enrolls the new certificate request.
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 Master Administrator. Contact your Master Administrator if such custom fields are required.

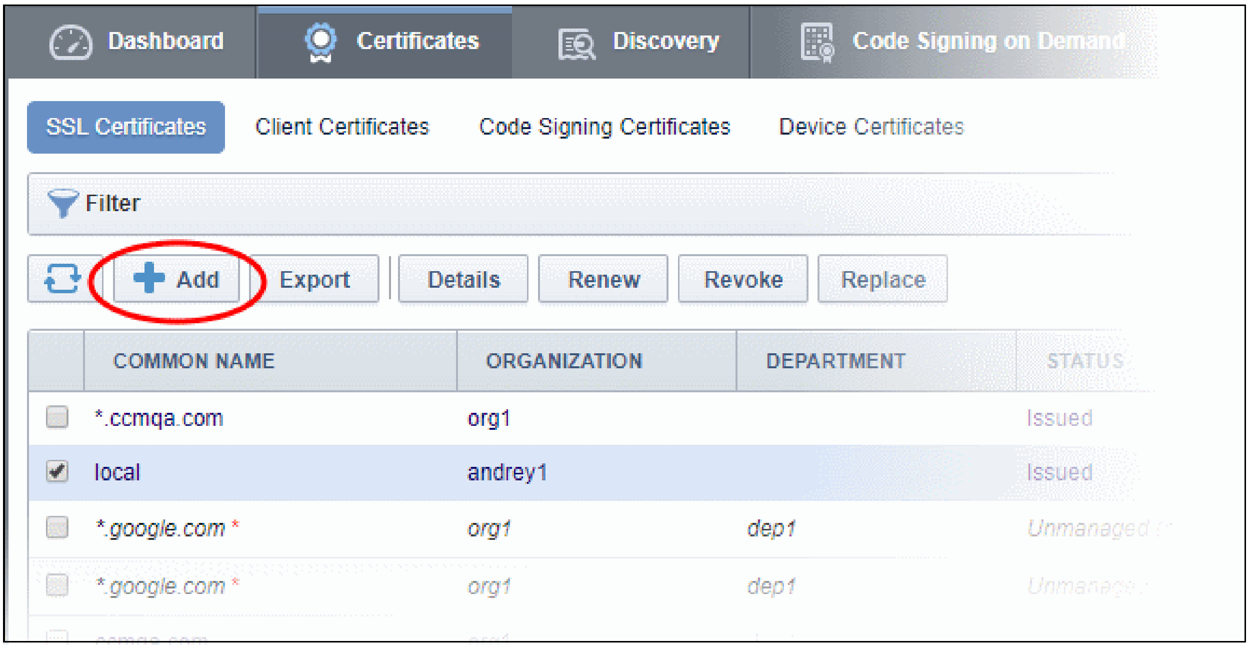
3.1.2.3.2 Method 2 - Built-in Enrollment Wizard - Manual CSR Generation


Comodo Certificate Manager Administrator
Administrator logs into Comodo CM account and orders a new SSL certificate using the built in application form
1
2
SSLCertificate Order Form
Administrator fills-in the SSL certificate order form, enters the CSR and submits the form. A certificate request is created in the 'SSL Certificates' area of the Comodo CM interface.
1
3
3
Administrator approves the certificate request from the 'SSL Certificates' area of the interface
Comodo Certificate Manager
Applicant
7
Applicant is directed to the SSL certificate collection form where, after entering an authentication code, they can to download and install their SSL certificate for the domain
7
Certificate Collection mail
6
Comodo CM sends a collection email to the applicant (the applicant can be the same admin or person nominated by the admin during the application process)
Certificate Collection Form
Comodo CA signs and issues the certificate for the domain and returns it to Comodo CM
5
4
After approval by Comodo CM administrator, the certificate request is sent to Comodo CA for processing
ComodoCA Backend Servers

3.1.2.3.2.1 SSL Certificate Enrollment – Manual CSR Generation

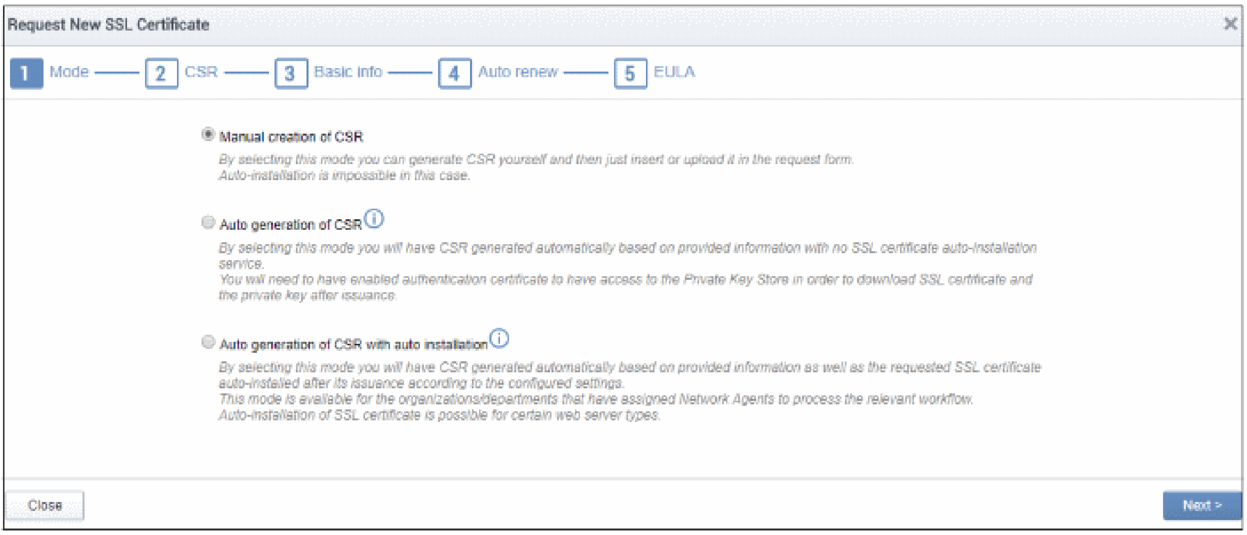
Administrators can manually apply for new certificates as follows:

- Click 'Certificate Management' > 'SSL Certificates' area
- Click the 'Add' button (as shown below):



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS
□	*.ccmqa.com	org1		Issued
☑	local	andrey1		Issued
□	*.google.com *	org1	dep1	Unmanaged
□	*.google.com *	org1	dep1	Unmanage

- This will open the 'Request New SSL Certificate' wizard:



Request New SSL Certificate

● Manual creation of CSR

By selecting this mode you can generate CSR yourself and then just insert or upload it in the request form. Auto-installation is impossible in this case.

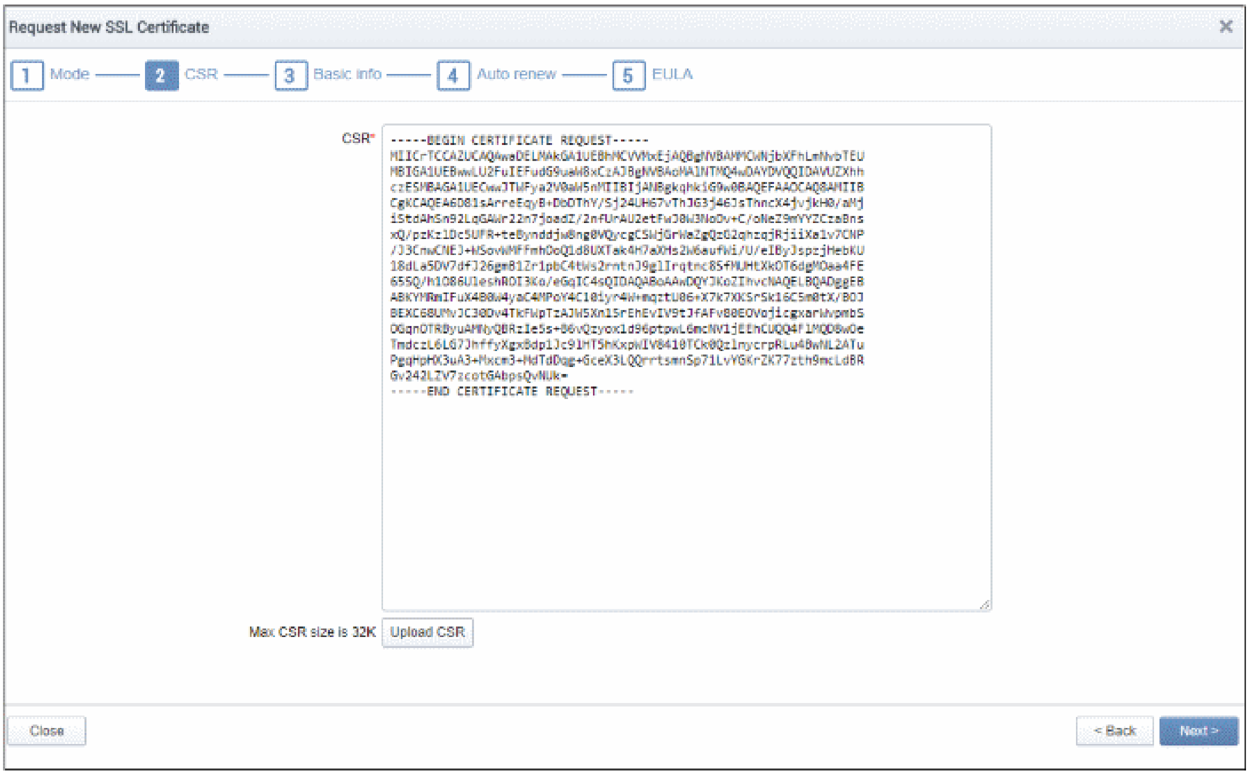
○ Auto generation of CSR

By selecting this mode you will have CSR generated automatically based on provided information with no SSL certificate auto-installation service. You will need to have enabled authentication certificate to have access to the Private Key Store in order to download SSL certificate and the private key after issuance.

○ Auto generation of CSR with auto installation

By selecting this mode you will have CSR generated automatically based on provided information as well as the requested SSL certificate auto-installed after its issuance according to the configured settings. This mode is available for the organizations/departments that have assigned Network Agents to process the relevant workflow. Auto-installation of SSL certificate is possible for certain web server types.

- Select the first option, 'Manual creation of CSR', and click 'Next'.



Request New SSL Certificate

CSR*

```
-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCA2UCAQAwaDELMAkGA1UEBhMCVVMxEjAQBgNVBAMMCWNjbXFhLmNvbTEU
MBIGA1UEBwwLU2FuIEFudG9uaW8xCzAJBgNVBAoMA1NTMQ4wDAYDVQQIDAVUZXhh
czESMBAGA1UECwwJTWFya2V0aW5nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6D81sArreEqyB+DbDThY/Sj24UH67vThJG3j46JsThncX4jvjkH0/aMj
iStdAhSn92LqGAWr22n7joadZ/2nfUrAU2etFwJ0W3NoDv+C/oNeZ9mYYZCzaBns
xQ/pzKz1Dc5UFR+teBynddjw8ng0VQycgCSWjGrWaZgQzG2qhzqjRjiiXa1v7CNP
/J3CnwCNEJ+WSovWMFFmhOoQ1d8UXTak4H7aXHs2W6aufWi/U/elByJspzjHebKU
18dLa5DV7dfJ26gm812r1pbC4tWs2rntnJ9g1Irqtnc85fMUHtXkOT6dgMOaa4FE
655Q/h1O86UleshROI3Ko/eGqIC4sQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEB
ABKYMRmIFuX4B0W4yaC4MPoY4C10iyr4W+mqztU06+X7k7XKSrSk16C5m0tX/BOJ
BEXC68UMvJC30Dv4TkFWpTzAJW5Xn15rEhEvIV9tJfAFv80EOVojicgxarWvpmbS
OGqnOTRByuAMNyQBRzIe5s+86vQzyox1d96ptpwL6mcNV1jEEhCUQQ4F1MQD0wOe
TmdczL6LG7JhffyXgx8dp1Jc91HT5hKxpWIV8410TCk0QzlnycrpRLu4BwNL2ATu
PgqHpHX3uA3+Mxcm3+MdTdDqg+GceX3LQQrrtsmnSp71LvYGKrZK77zth9mcLdBR
Gv242LZV7zcotGAbpsQvNUk=
-----END CERTIFICATE REQUEST-----
```

Max CSR size is 32K

Paste your 'Certificate Signing Request' (CSR) into this field in order for Incommon CA to process your application and issue the certificate for the domain.

The CSR can be entered in two ways:

- Paste the CSR directly into this field
- Upload the CSR as a .txt file by clicking the 'Upload CSR' button

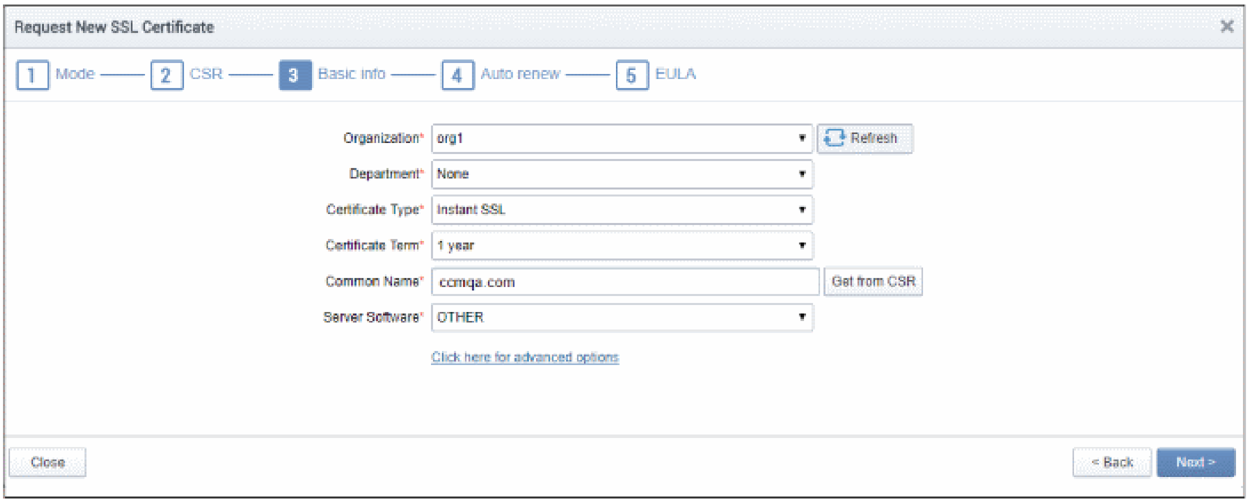
Background:

- 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 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 Incommon 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.

- Click 'Next'



Request New SSL Certificate

Organization*: org1

Department*: None

Certificate Type*: Instant SSL

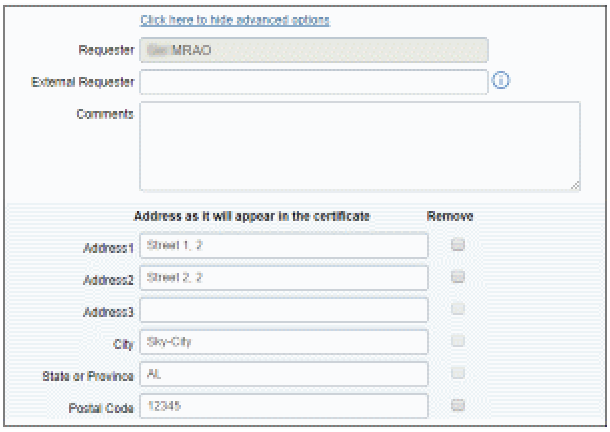
Certificate Term*: 1 year

Common Name*: ccmqa.com

Server Software*: OTHER

Click here for advanced options

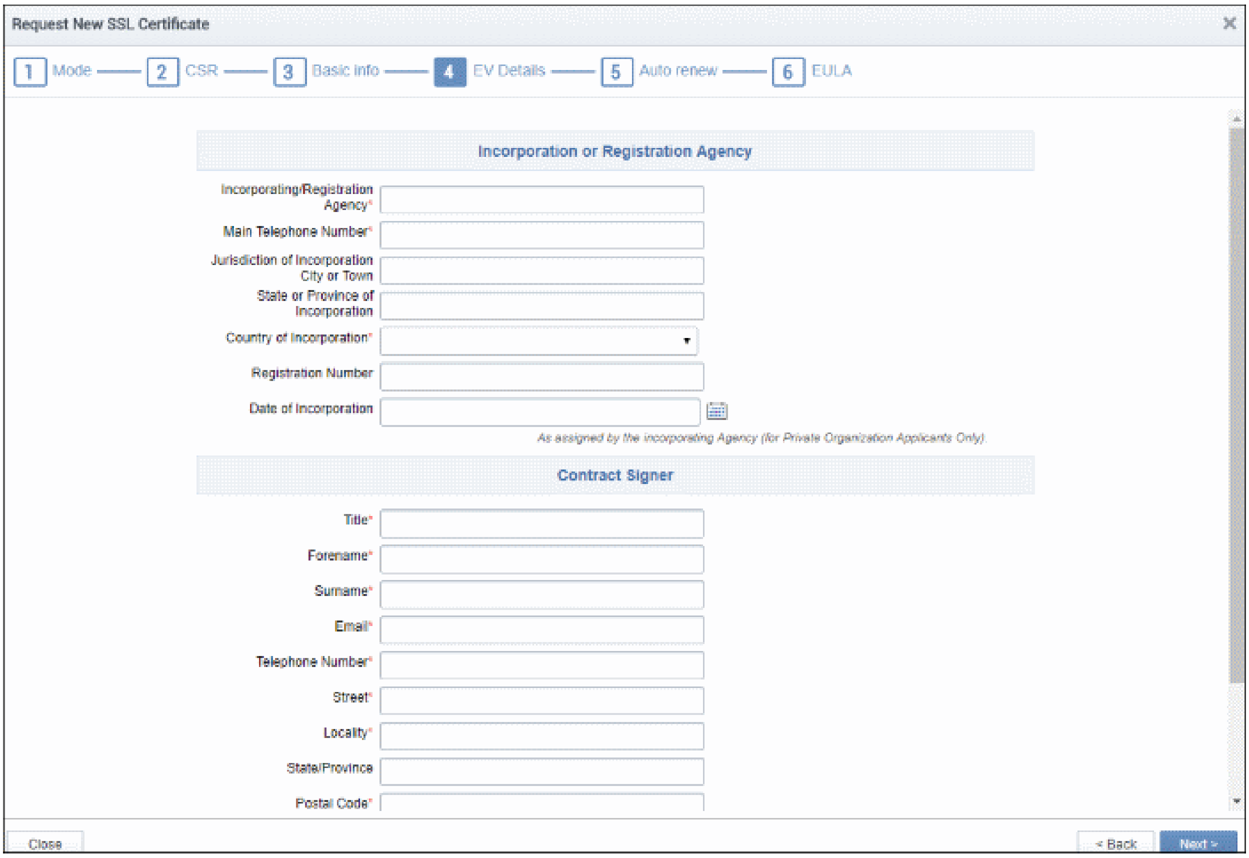
Form Element	Type	Description
Organization (***required***)	Drop-down list	Choose the Organization that the SSL certificate will belong to.
Department (***required***)	Drop-down list	Choose the Department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'.
Certificate Type (***required***)	Drop-down list	Choose the certificate type that you wish to enroll. See Comodo SSL Certificates for a list of certificate types. The specific certificate types displayed in the drop-down list depends on the SSL Types allowed for the selected Organization. See sections Editing a new Organization and Customize an Organization's SSL Certificate Types for more details.

Form Element	Type	Description
Certificate Term (***required***)	Drop-down list	Choose the validity period of the certificate. For example, 1 year, 2 years, 3 years. See Comodo SSL Certificates for a list of certificate types and term lengths. The validity periods available for a particular Organization depends on its configuration. See sections Editing a new Organization and Customize an Organization's SSL Certificate Types for more details.
Common Name (***required***)	Text Field	Type the domain that the certificate will be issued to.
Get CN from CSR (***optional***)	Control	• Once the CSR has been entered correctly, clicking this button will auto-populate the Common Name (CN) field. • This method helps avoid human error by ensuring the domain name in the application form exactly matches the domain in the CSR. • If the domain name mentioned in the form does not match the one in the CSR, then Incommon 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.
Server Software (***required***)	Drop-down list	Select the server software on which the certificate is to be installed. **Note**: Choose 'OTHER' if you want to use F5 BIG-IP.
Subject Alternative Names (***optional***)	Text Field	This field appears only if a multi domain or UCC certificate type is selected. Specify the additional domain names. Each domain name should be separated by a comma.
Click here for advanced options	Text Fields	Clicking this link will expand the advanced options:  Click here to hide advanced options Requester: [redacted] MRAO External Requester: Comments: Address as it will appear in the certificate — Remove Address1: Street 1, 2 □ Address2: Street 2, 2 □ Address3: □ City: Sky-City □ State or Province: AL □ Postal Code: 12345 □ • Requester – This field is auto-populated with the name of the administrator making the application. • External Requester (optional) - Enter the email address of an external requester on whose behalf the application is made. **Note**: The 'Requester' will still be the administrator that is completing this

Form Element	Type	Description
		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. • Comments (optional) - Enter your comments on the certificate. **Address fields in the certificate** 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 of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and 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.

- Click 'Next'

The EV details form is next if you choose EV certificate type:



Incorporation or Registration Agency

Incorporating/Registration Agency*

Main Telephone Number*

Jurisdiction of Incorporation City or Town

State or Province of Incorporation

Country of Incorporation*

Registration Number

Date of Incorporation

As assigned by the incorporating Agency (for Private Organization Applicants Only)

Contract Signer

Title*

Forename*

Surname*

Email*

Telephone Number*

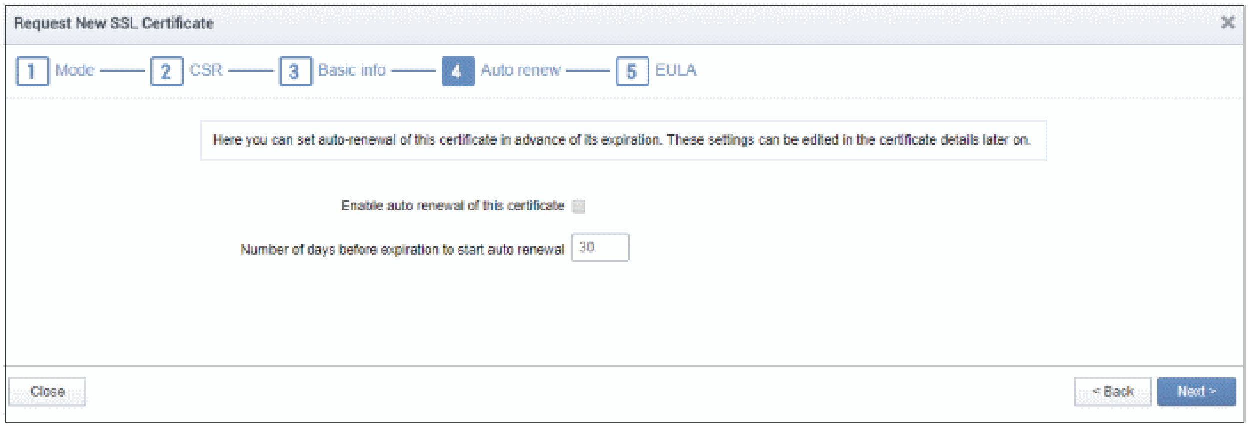
Street*

Locality*

State/Province

Postal Code*

- The details you need to complete depends on the EV mode activated for your account.
- This is same information as provided in the EV details tab when adding a new organization. See 'EV Details Tab' for more info. If the EV type is 'RA' for your account, this will be auto-populated.
- Click 'Next' when all required fields are complete.



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

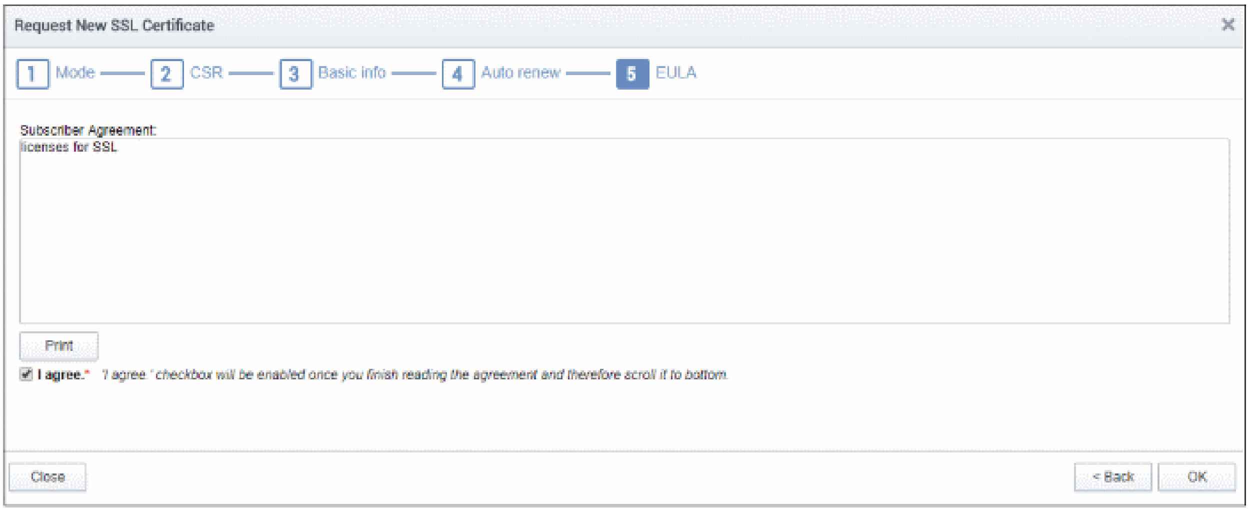
Enable auto renewal of this certificate □

Number of days before expiration to start auto renewal 30

The next step is to configure the auto-renewal options.

  - Enable auto renewal of this certificate – Select this to have Incommon CM apply for a new certificate when this one approaches expiry.
  - Number of days before expiration to start auto renewal - Choose the number of days in advance of expiry that the renewal process should start. On the scheduled day, the certificate controller will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.

- Click 'Next'



Subscriber Agreement:
licenses for SSL

☑ I agree.* 'I agree.' checkbox will be enabled once you finish reading the agreement and therefore scroll it to bottom.

The final stage is to agree to the EULA.

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

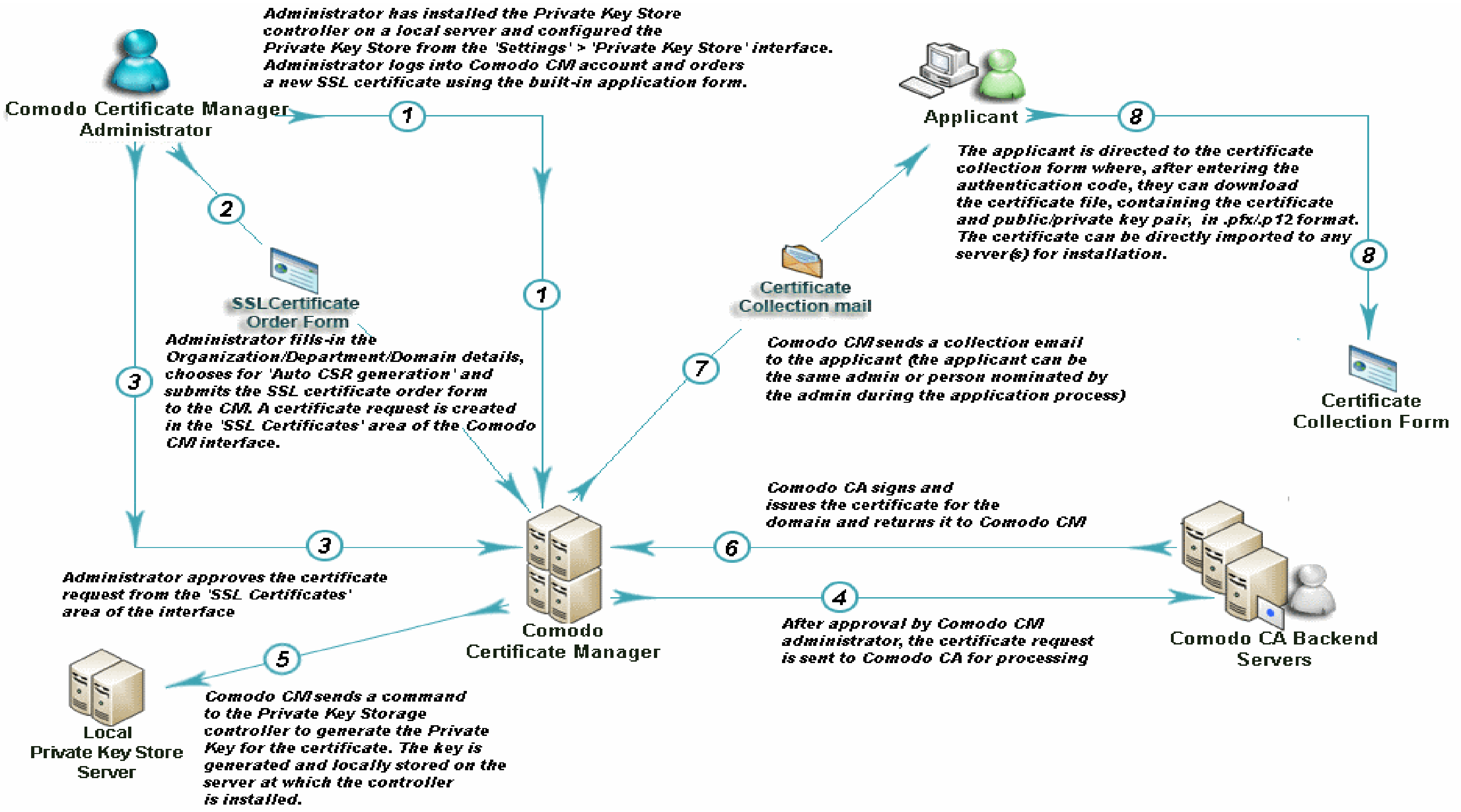
The certificate will be added to the 'SSL Certificates' interface with a status of 'Requested'. Next, the requested has to be approved. See the sections 'Certificate Requests – Approving, Declining, Viewing and Editing', 'Certificate Collection' for more information.

3.1.2.3.3 Method 3 - Built-in Enrollment Wizard - Auto CSR Generation

- As an alternative to manually creating a CSR, Incommon CM can automatically generate a CSR at the point of application. Incommon CM will generate a CSR using the details entered in the Organization/Department, Common name, and server software fields of the application.
- During the CSR generation process, Incommon CM sends a command to generate the private key for the certificate to the Private Key Store controller.
- This controller is installed on a local server in the customer network and can be configured by clicking 'Settings' > 'Private Key Store'. The private key is stored in a database created by the controller on the local server and does not leave your network. It is not uploaded to Incommon CM.
- Upon approval and issuance, the certificate can be collected by the administrator or the applicant from the 'Certificate Details' dialog or from the collection form.

- During collection, Incommon CM retrieves the private key from the key store over an encrypted channel and integrates it with the certificate. The certificate can then be downloaded in .pfx or .p12 format. The certificate can be imported to and installed on any server.

Prerequisite - The auto-CSR generation feature needs the Private Key Store controller installed on a local server and configured to connect to Incommon CM for receiving command and generate and store the private keys.



Administrator has installed the Private Key Store controller on a local server and configured the Private Key Store from the 'Settings' > 'Private Key Store' interface. Administrator logs into Comodo CM account and orders a new SSL certificate using the built-in application form.

The applicant is directed to the certificate collection form where, after entering the authentication code, they can download the certificate file, containing the certificate and public/private key pair, in .pfx/.p12 format. The certificate can be directly imported to any server(s) for installation.

Administrator fills-in the Organization/Department/Domain details, chooses for 'Auto CSR generation' and submits the SSL certificate order form to the CM. A certificate request is created in the 'SSL Certificates' area of the Comodo CM interface.

Comodo CM sends a collection email to the applicant (the applicant can be the same admin or person nominated by the admin during the application process)

Comodo CA signs and issues the certificate for the domain and returns it to Comodo CM

Administrator approves the certificate request from the 'SSL Certificates' area of the interface

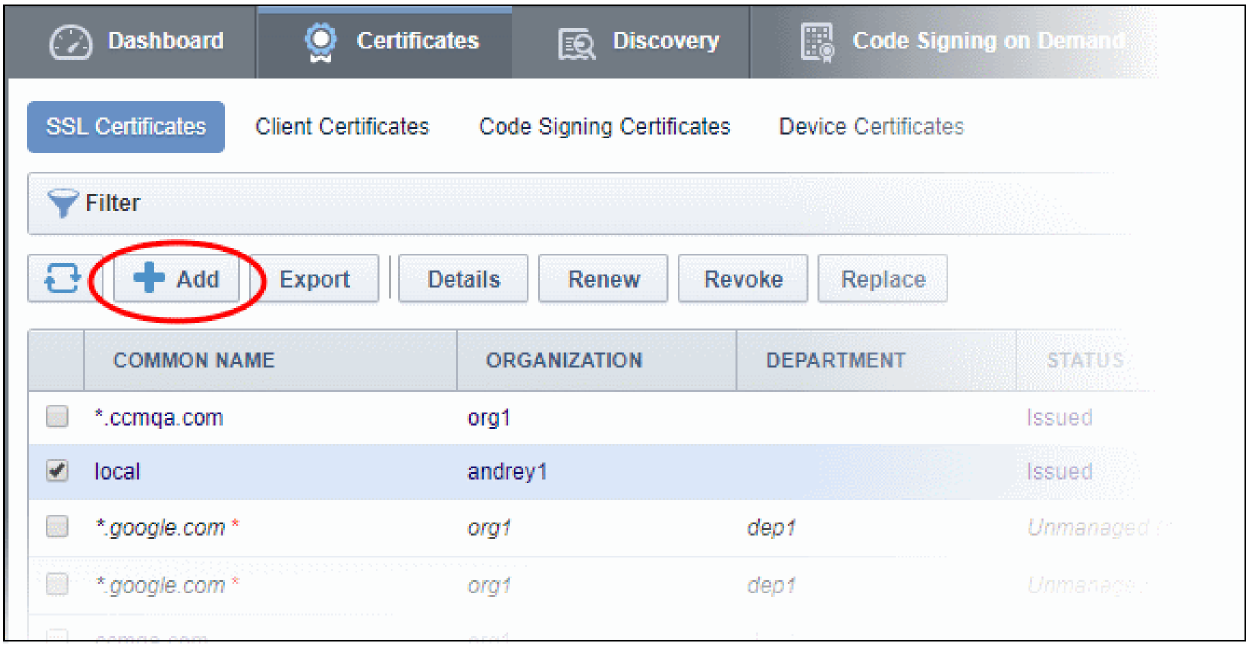
After approval by Comodo CM administrator, the certificate request is sent to Comodo CA for processing

Comodo CM sends a command to the Private Key Storage controller to generate the Private Key for the certificate. The key is generated and locally stored on the server at which the controller is installed.

Comodo Certificate Manager Administrator
1
Applicant
8
2
SSL Certificate Order Form
1
Certificate Collection mail
8
3
7
Certificate Collection Form
3
6
4
Comodo Certificate Manager
Comodo CA Backend Servers
5
Local Private Key Store Server

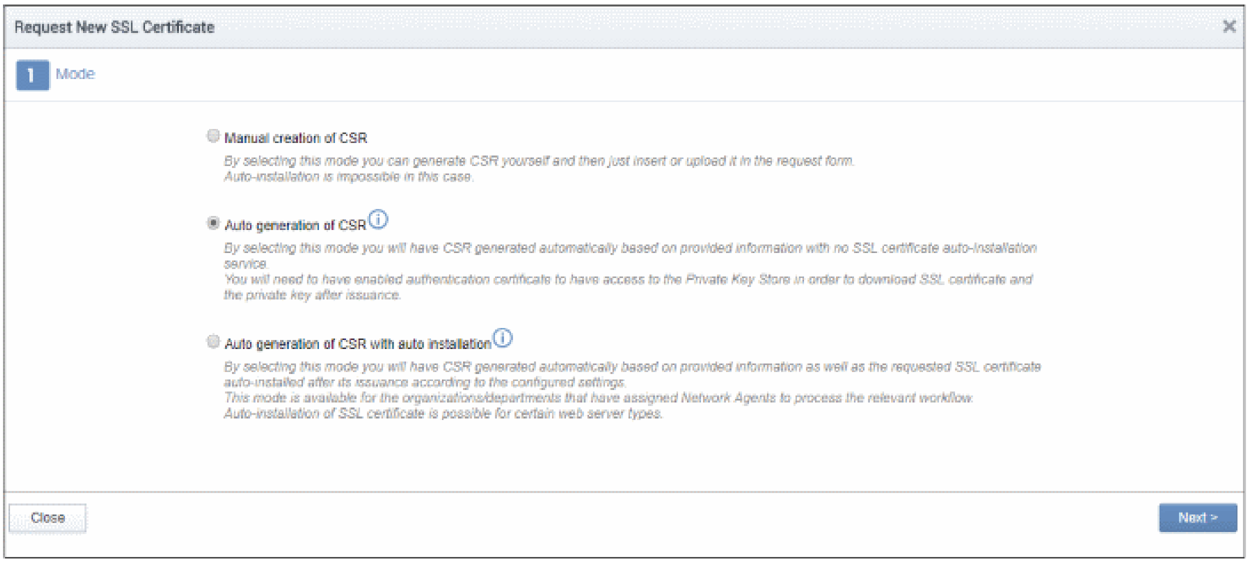
3.1.2.3.3.1 SSL Certificate Enrollment – Auto CSR Generation

- Click the 'Certificates' tab and choose 'SSL Certificates':



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS
□	*.ccmqa.com	org1		Issued
☑	local	andrey1		Issued
□	*.google.com *	org1	dep1	Unmanaged
□	*.google.com *	org1	dep1	Unmanage

- Click the 'Add' button to open the 'Request New SSL Certificate' wizard:



○ Manual creation of CSR

By selecting this mode you can generate CSR yourself and then just insert or upload it in the request form.
Auto-installation is impossible in this case.

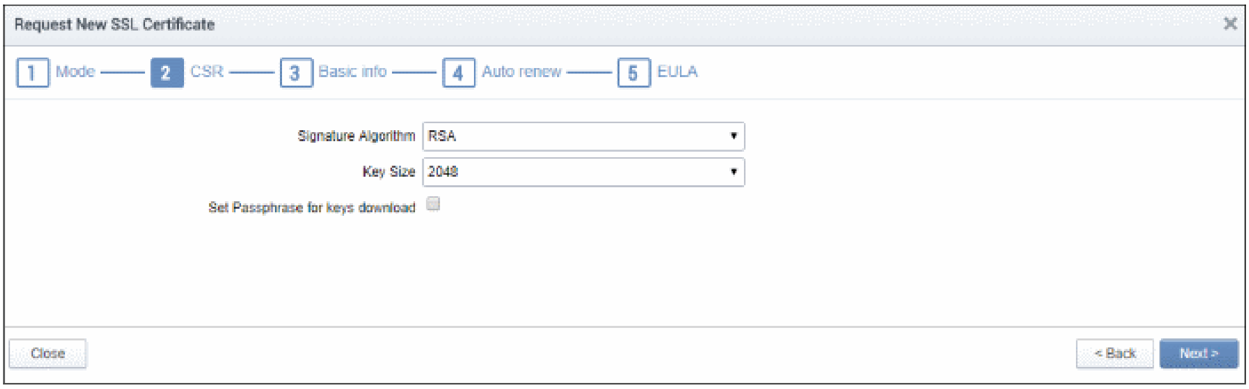
● Auto generation of CSR

By selecting this mode you will have CSR generated automatically based on provided information with no SSL certificate auto-installation service.
You will need to have enabled authentication certificate to have access to the Private Key Store in order to download SSL certificate and the private key after issuance.

○ Auto generation of CSR with auto installation

By selecting this mode you will have CSR generated automatically based on provided information as well as the requested SSL certificate auto-installed after its issuance according to the configured settings.
This mode is available for the organizations/departments that have assigned Network Agents to process the relevant workflow.
Auto-installation of SSL certificate is possible for certain web server types.

- Select the second option, 'Auto generation of CSR' then click 'Next'.



Request New SSL Certificate

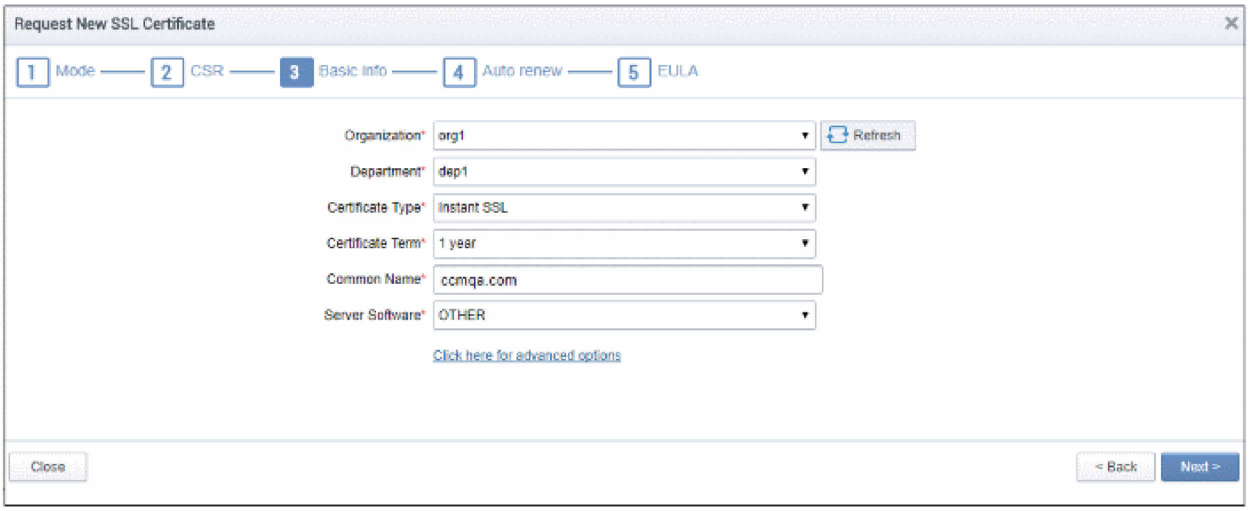
Signature Algorithm: RSA

Key Size: 2048

Set Passphrase for keys download □

The next step is to provide the CSR parameters:

- Signature Algorithm – Select the digital signature algorithm you want to use in the certificate. Currently only RSA is supported.
- Key Size – Options available are 2048 and 4096. 2048 bit is the recommended industry standard and provides very high security for public-facing and internal hosts. 4096 is even more secure, but may lead to longer connection times due to the extra processing time during the SSL handshake.
- Passphrase protection – Enable to protect the certificate with a password. The passphrase can be manually entered or auto-generated. Store this in a safe location.
  - For manual, enter the passphrase and confirm it in the next field.
  - Click 'Generate' to auto-generate a passphrase.
  - To view the passphrase, select 'Show Passphrase' checkbox.
- Click 'Next'



Request New SSL Certificate

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

Organization*: org1

Department*: dep1

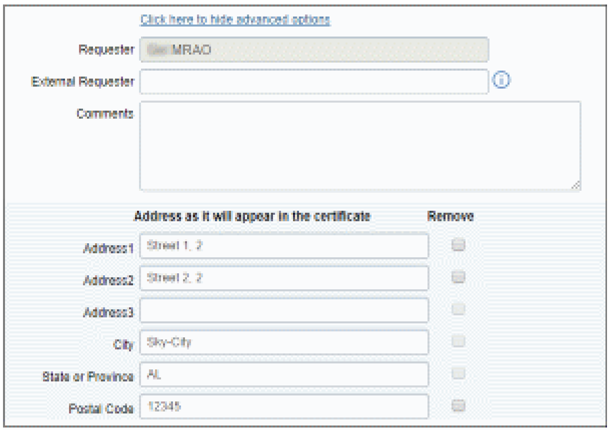
Certificate Type*: Instant SSL

Certificate Term*: 1 year

Common Name*: ccmqa.com

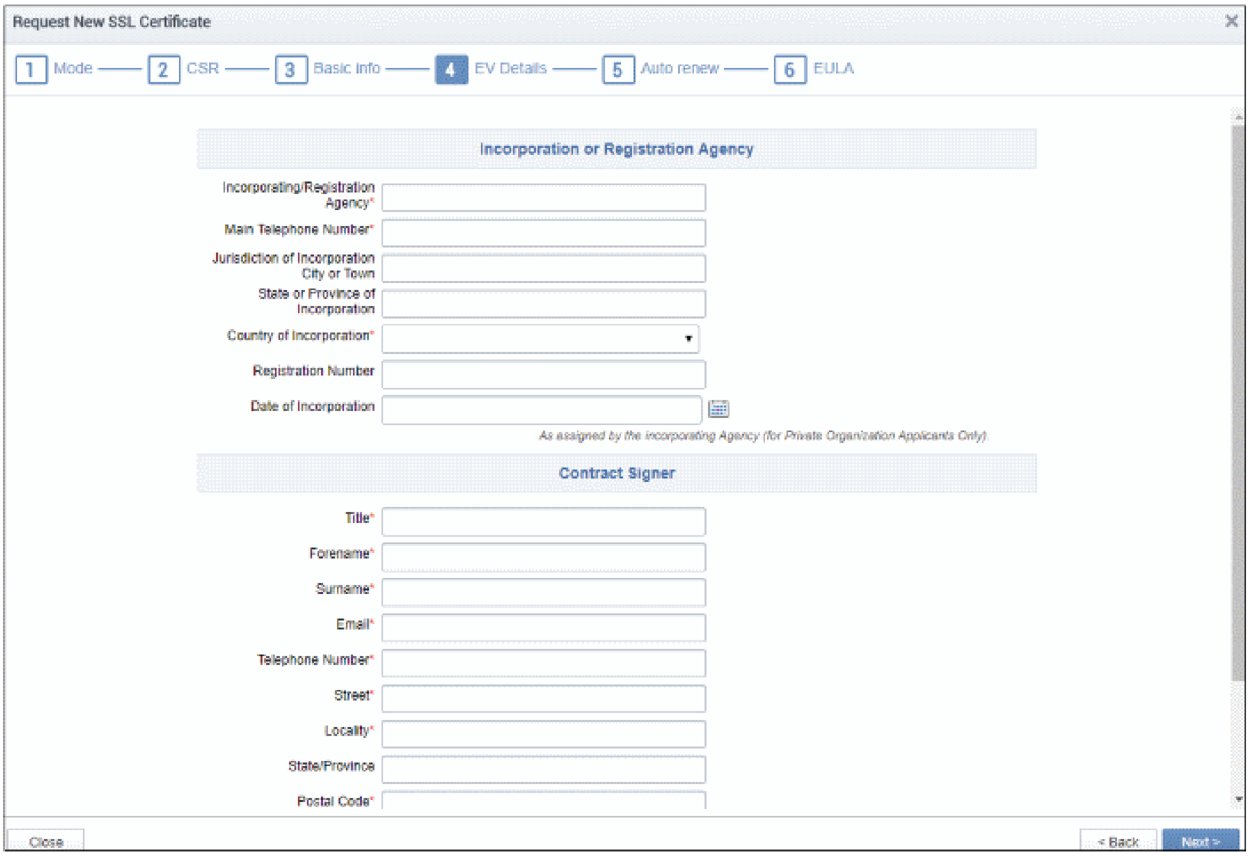
Server Software*: OTHER

Refresh
Click here for advanced options
Close
< Back
Next >

Form Element	Type	Description
Organization (***required***)	Drop-down list	Choose the Organization that the SSL certificate will belong to.
Department (***required***)	Drop-down list	Choose the Department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'.
Certificate Type (***required***)	Drop-down list	Choose the certificate type that you wish to enroll. See Comodo SSL Certificates for a list of certificate types. The specific certificate types displayed in the drop-down list depends on the SSL Types allowed for the selected Organization. See Editing a new Organization and Customize an Organization's SSL Certificate Types for more details.
Certificate Term (***required***)	Drop-down list	Choose the validity period of the certificate. For example, 1 year, 2 years, 3 years. See **Comodo SSL Certificates** for a list of certificate types and term lengths. The validity periods available for a particular Organization depends on its configuration. See Editing a new Organization and Customize an Organization's SSL Certificate Types for more details.
Common Name (***required***)	Text Field	Type the domain that the certificate will be issued to.
Server Software (***required***)	Drop-down list	Select the server software on which the certificate is to be installed. **Note**: Choose 'OTHER' if you want to use F5 BIG-IP.
Subject Alternative Names (***optional***)	Text Field	This field appears only if a multi domain or UCC certificate type is selected. Specify the additional domain names. Each domain name should be separated by a comma.
Click here for advanced options	Text Fields	Clicking this link will expand the advanced options:  Click here to hide advanced options Requester: [redacted] MRAO External Requester: Comments: Address as it will appear in the certificate — Remove Address1: Street 1, 2 □ Address2: Street 2, 2 □ Address3: □ City: Sky-City □ State or Province: AL □ Postal Code: 12345 □ - Requester – This field is auto-populated with the name of the administrator making the application. - External Requester (optional) - Enter the email address of an external requester on whose behalf the application is made. **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

Form Element	Type	Description
		'External Requester' will be displayed as the 'External Requester' in the 'View' dialog of an issued certificate. • Comments (optional) - Enter your comments on the certificate. **Address fields in the certificate** 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 of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and 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.

The EV Details form is next if you are applying for an EV certificate:



Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 EV Details — 5 Auto renew — 6 EULA

Incorporation or Registration Agency

Incorporating/Registration Agency*

Main Telephone Number*

Jurisdiction of Incorporation City or Town

State or Province of Incorporation

Country of Incorporation*

Registration Number

Date of Incorporation

As assigned by the incorporating Agency (for Private Organization Applicants Only)

Contract Signer

Title*

Forename*

Surname*

Email*

Telephone Number*

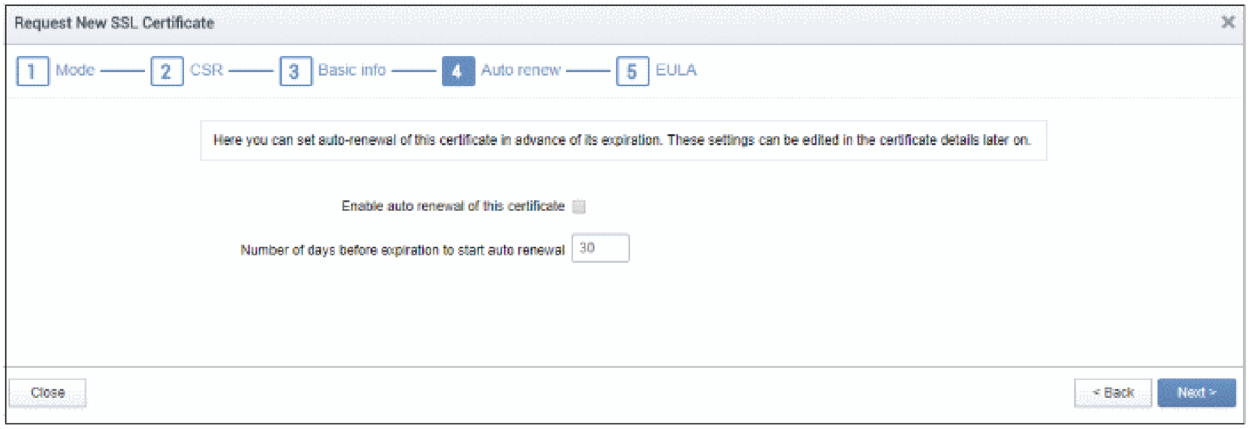
Street*

Locality*

State/Province

Postal Code*

- The details you need to complete depends on the EV mode activated for your account.
- This is same information as provided in the EV details tab when adding a new organization. See 'EV Details Tab' for more info. If the EV type is 'RA' for your account, this will be auto-populated.
- Click 'Next' when all required fields are complete.



Request New SSL Certificate

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

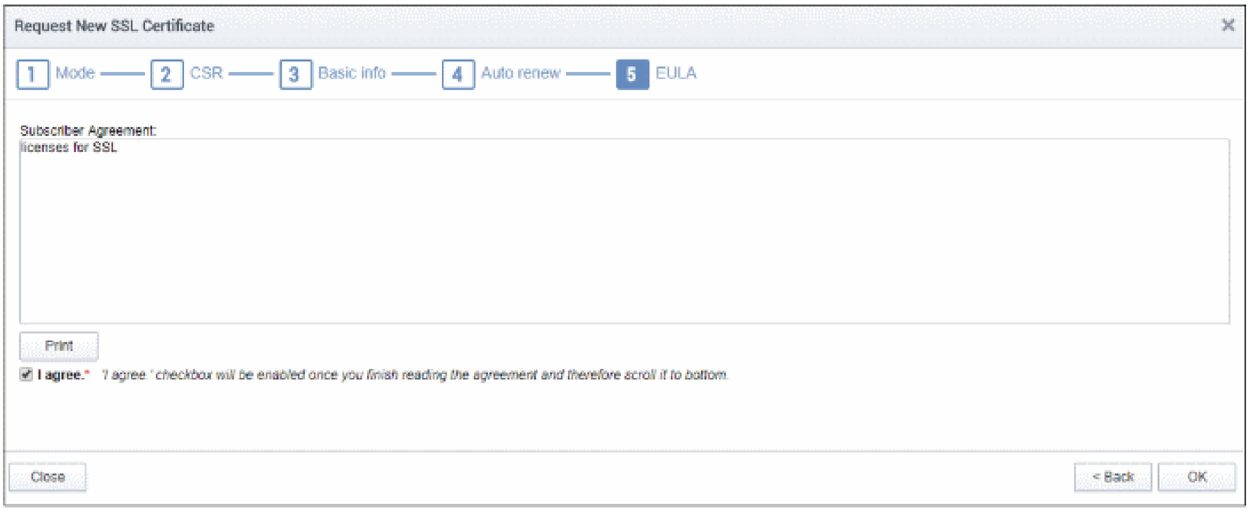
Enable auto renewal of this certificate □

Number of days before expiration to start auto renewal 30

The next step is to configure the auto-renewal options.

- Enable auto renewal of this certificate - Select this to have Incommon CM apply for a new certificate when this one approaches expiry.
- Number of days before expiration to start auto renewal - Choose the number of days in advance of expiry that the renewal process should start. On the scheduled day, the certificate controller will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.

- Click 'Next'



Subscriber Agreement:
licenses for SSL

☑ **I agree.*** *'I agree ' checkbox will be enabled once you finish reading the agreement and therefore scroll it to bottom.*

The final stage is to agree to the EULA.

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

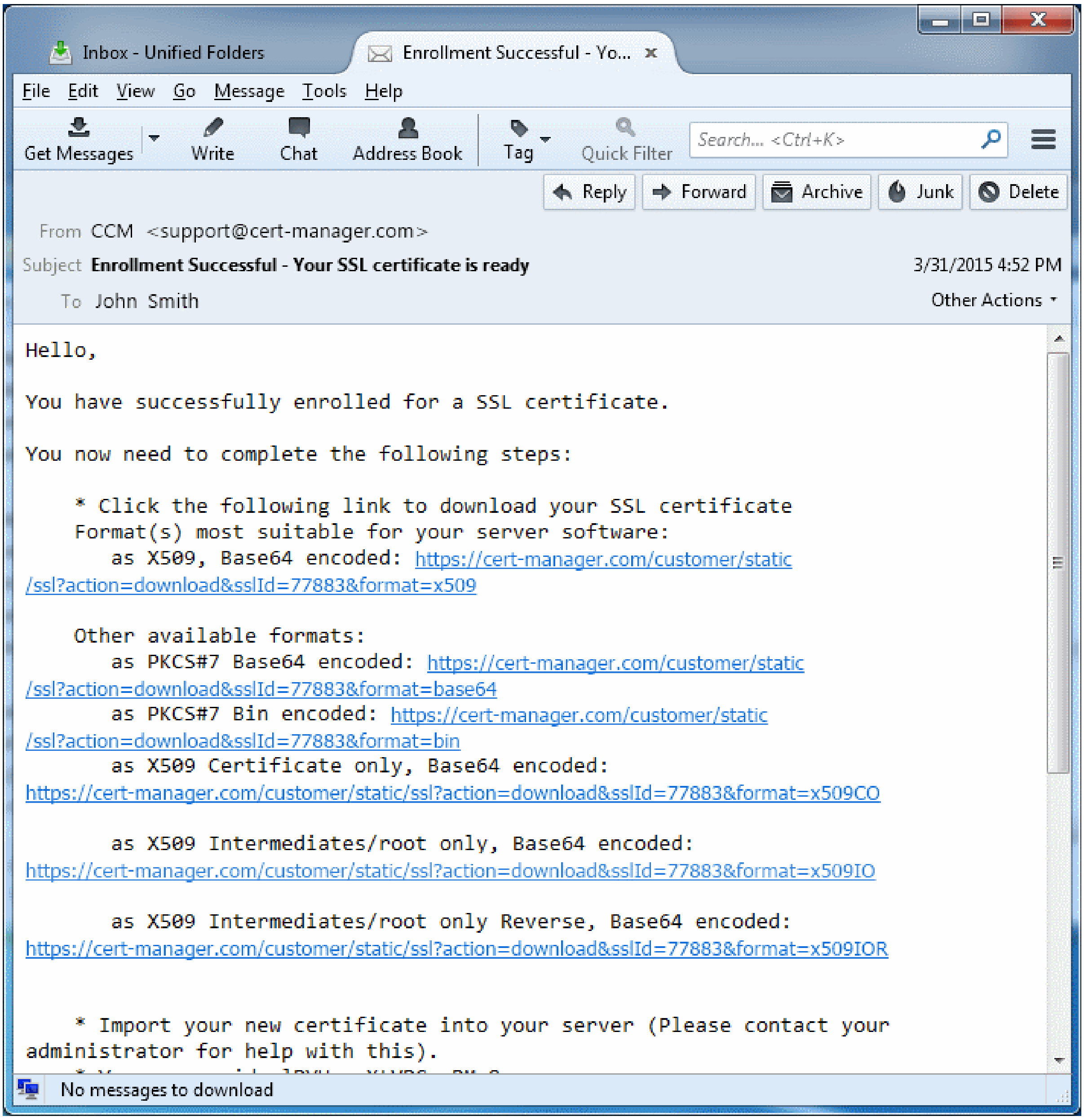
The certificate will be added to the 'SSL Certificates' interface with a status of 'Requested'. Next, the request has to be approved. See 'Certificate Requests – Approving, Declining, Viewing and Editing' and 'Certificate Collection' for more information.

3.1.2.3.4 Certificate Collection

- After Incommon 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, Incommon 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.

3.1.2.3.4.1 Collection of SSL Certificate Through Email

1. Once the certificate has been issued, Incommon 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 Incommon CM 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.



From CCM <support@cert-manager.com>

Subject **Enrollment Successful - Your SSL certificate is ready** 3/31/2015 4:52 PM

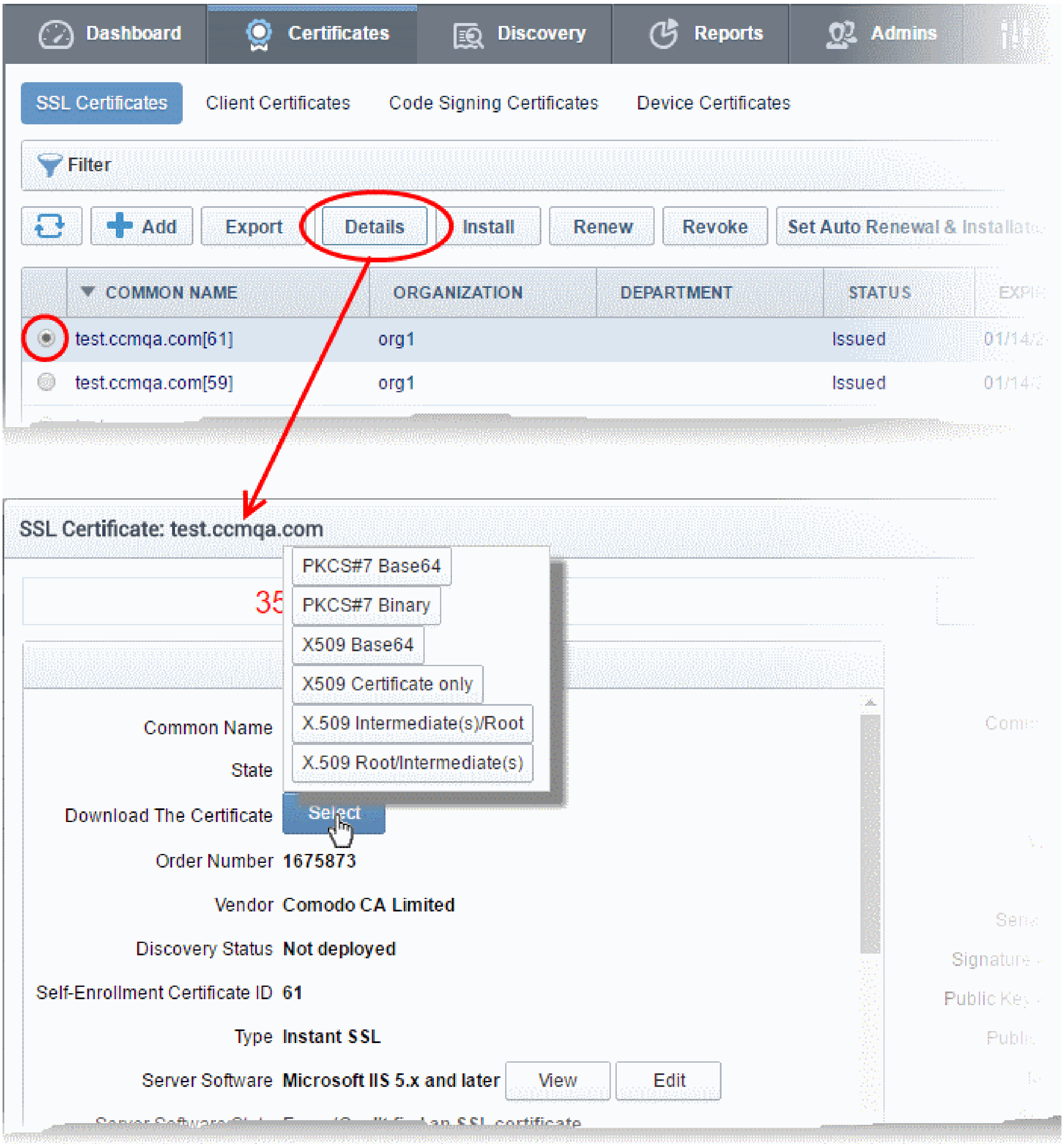
To John Smith

```
Hello,

You have successfully enrolled for a SSL certificate.

You now need to complete the following steps:

    * Click the following link to download your SSL certificate
    Format(s) most suitable for your server software:
       as X509, Base64 encoded: https://cert-manager.com/customer/static
/ssl?action=download&sslId=77883&format=x509

    Other available formats:
       as PKCS#7 Base64 encoded: https://cert-manager.com/customer/static
/ssl?action=download&sslId=77883&format=base64
       as PKCS#7 Bin encoded: https://cert-manager.com/customer/static
/ssl?action=download&sslId=77883&format=bin
       as X509 Certificate only, Base64 encoded:
https://cert-manager.com/customer/static/ssl?action=download&sslId=77883&format=x509CO

       as X509 Intermediates/root only, Base64 encoded:
https://cert-manager.com/customer/static/ssl?action=download&sslId=77883&format=x509IO

       as X509 Intermediates/root only Reverse, Base64 encoded:
https://cert-manager.com/customer/static/ssl?action=download&sslId=77883&format=x509IOR


    * Import your new certificate into your server (Please contact your
administrator for help with this).
```

2. Having clicked the link in the collection email, the end-user will be able to download the certificate file.

3.1.2.3.4.2 Collection of SSL Certificate by an Administrator

- Issued certificates can also be downloaded and provided to the applicant from the SSL Certificate Details dialog.
- Click 'Certificates' > 'SSL Certificates'
- Select the certificate you wish to collect from the list
- Click the 'Details' button:



Common Name	
State	
Download The Certificate	Select
Order Number	1675873
Vendor	Comodo CA Limited
Discovery Status	Not deployed
Self-Enrollment Certificate ID	61
Type	Instant SSL
Server Software	Microsoft IIS 5.x and later

The details dialog allows you to download the issued certificate in several formats.

- Click the 'Select' button
- Click the appropriate button to download the certificate in your preferred format.

If the private key of the certificate is managed by Incommon CM at the Private Key Store configured at the local network, the administrator then have the option to download certificates in .pfx/.p12 format containing the public/private key pair so, for example, it may be exported to another web server.

Certificates can only be download in .p12 format after an admin has authenticated themselves with a client certificate at the computer from which they are accessing Incommon CM.

3.1.2.3.5 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.

The precise installation process depends on the web server type and a range of installation guides are available at the Comodo support website at:

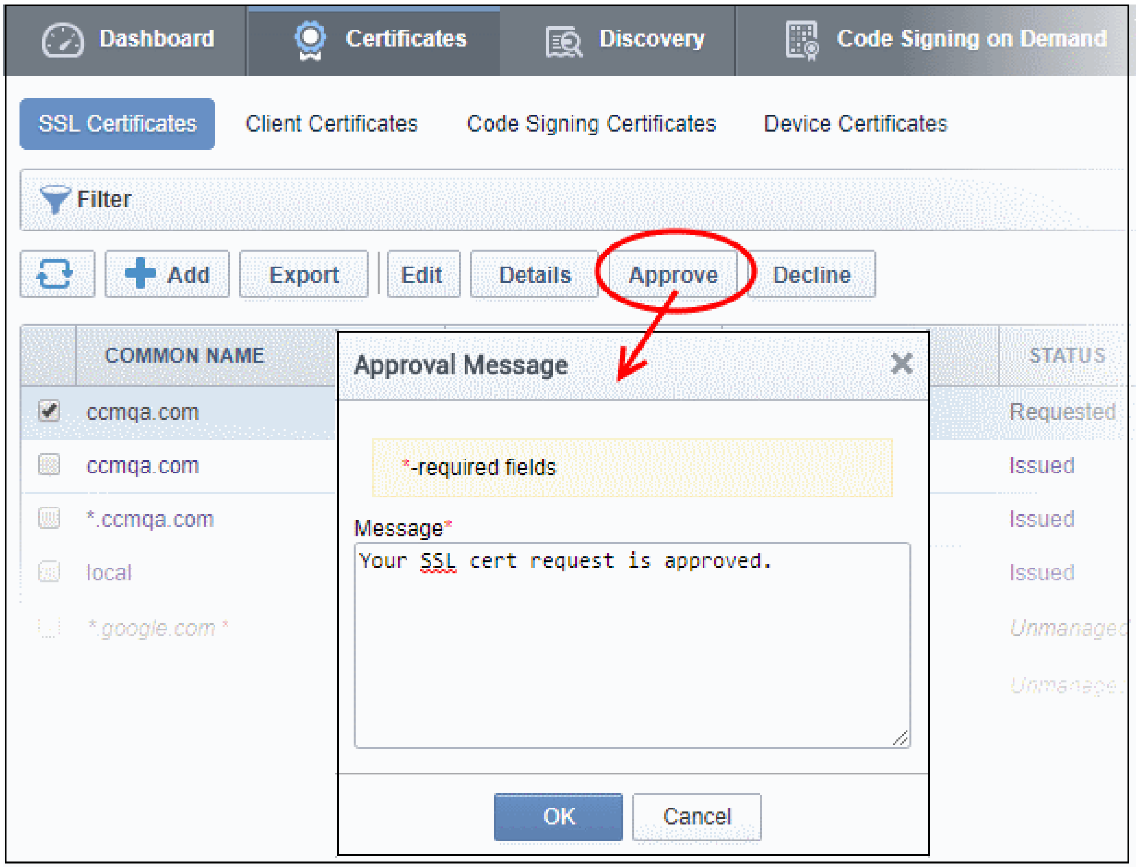
https://support.Comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav

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

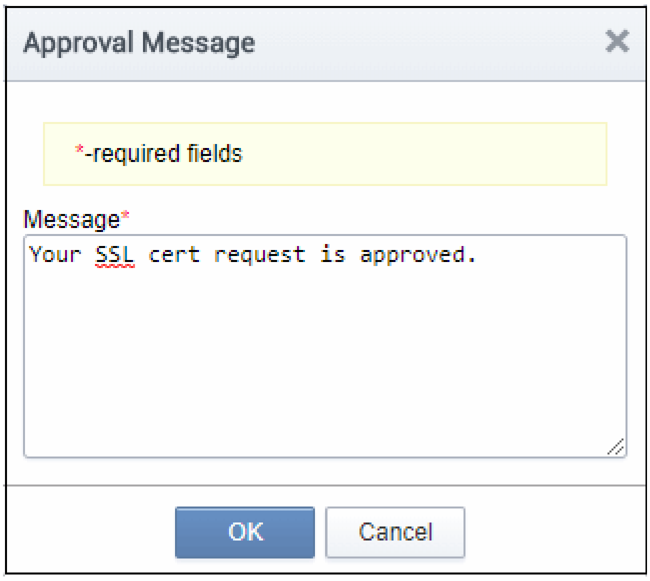
A certificate request will appear in the 'SSL Certificates' area after a success application using either the Auto Installer or SSL Enrollment Form and Built-in Wizard.

- Click 'Certificates' > 'SSL certificates'
- Use the filters to view all certificates with a 'Status' of 'Requested'
- Select the certificate that you want to approve, decline, view or edit



Your SSL cert request is approved.

- At this point, the certificate request has NOT been submitted to Incommon 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 you want to reject a request, click the 'Decline' button.
  - Declining a request will change the certificate status to 'Declined'. If an 'SSL Declined' notification has been set up then a mail will be sent to the applicant informing them that the request has been turned down.
  - Declined requests can still be approved at any time in the future by a 'RAO SSL' or 'DRAO SSL' admin.
- Select a certificate then click the 'Details' button to view info about the certificate fields, certificate type and more.
- Click the 'Edit' button if you wish to modify the application before submitting to Incommon CA for processing.
- Click 'Approve' to submit the application to Incommon CA for processing.
  - After clicking the 'Approve' button, a box will appear that allows you to send a message with the approval notification email.



Message*
Your SSL cert request is approved.

  - 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 request has been submitted to Incommon CA, the certificate state will change to 'Approved'. This will change to 'Applied' if accepted by Incommon (it can also can be rejected).
- Incommon will send a Certificate Collection email to the applicant when the certificate is issued. The 'State' of the certificate will change to 'Issued' in Incommon CM.

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

3.1.2.5 Certificate Renewal

SSL certificates can be renewed manually or automatically:

Manual

There are two broad ways to manually renew certificates via Incommon CM:

- SSL administrators can renew certificates from the SSL certificates interface. Jump to Certificate Renewal by Administrators for more details.
- External applicants can renew using the self-renewal form. Jump to Certificate Renewal by the End-User for more details.

Automatic

Administrators can configure automatic renewal of SSL certificates. Jump to Scheduling Automatic Renewal and Installation for more details.

3.1.2.5.1 Certificate Renewal by Administrators

- The SSL Certificates interface allows administrators to renew both managed and unmanaged certificates.
- A unmanaged certificate is any certificate that was not ordered using Incommon Certificate Manager. Typically these are found during a discovery scan.
- The processes for renewing managed and unmanaged certificates are different.

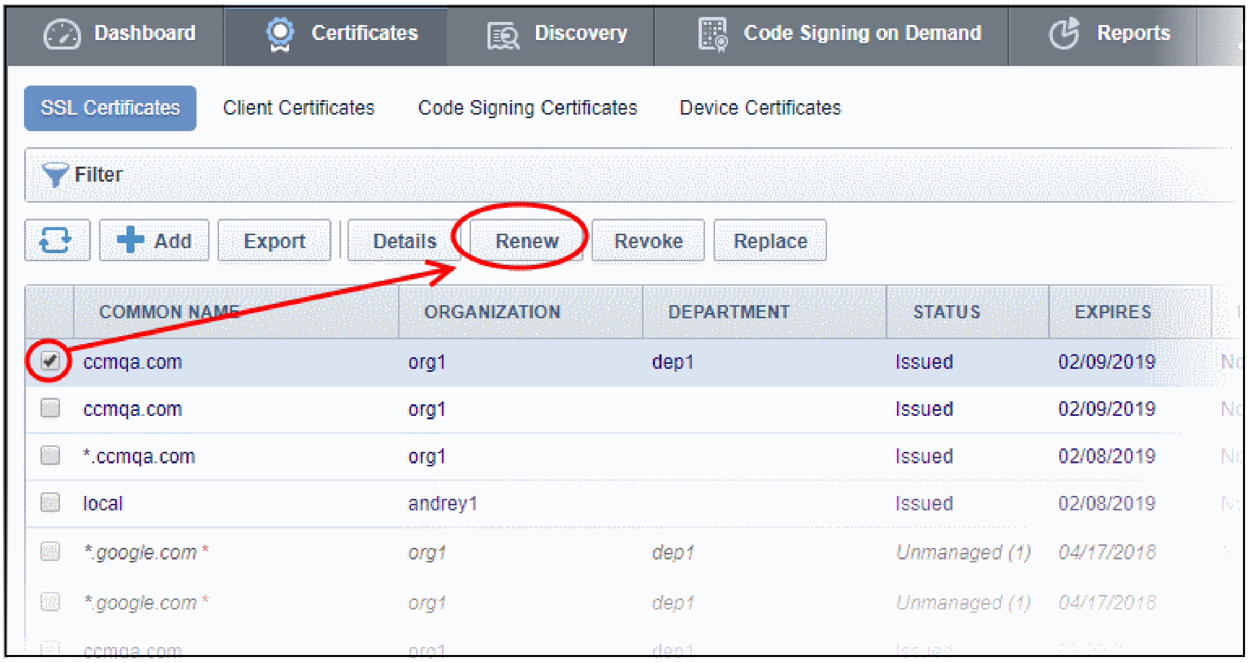
Managed Certificates	Unmanaged Certificates
• A 'managed certificate' is a certificate which has been issued via Incommon CM to a specific combination of domain and organization. • You will need to submit a CSR the first time you apply for a certificate for any such combination. After issuance, this certificate will become 'managed'. • 'Managed' certificates are those with Incommon CM statuses of 'Issued', 'Applied' or 'Requested' • For renewals of 'managed' certificates, you will typically not need to submit a CSR because Incommon CM shall re-use the existing CSR.	• An 'unmanaged certificate' is a certificate which was found during a discovery scan but was not issued via Incommon CM. • You will need to submit a new CSR during renewal of an 'Unmanaged' certificate because Incommon CM 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 an organization's address details, then you are effectively creating a new certificate application. You are not 'renewing' a certificate. In these circumstances, you will also have to submit a new CSR.

Renewing a 'Managed' Certificate

- Click 'Certificates' > 'SSL Certificates'
- Select the managed certificate you wish to renew from the list

- Click the 'Renew' button:



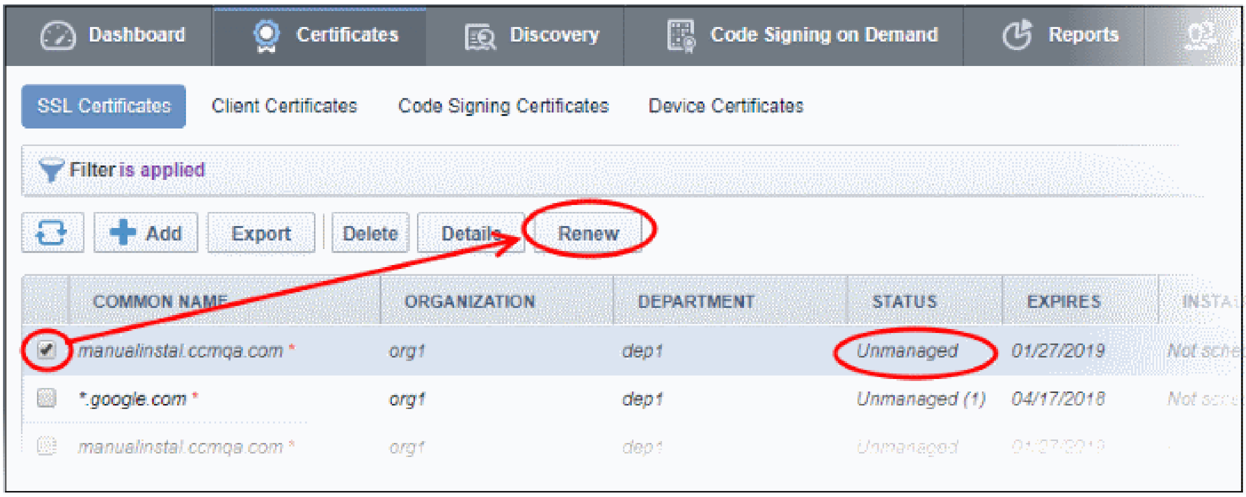
	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES
☑	ccmqa.com	org1	dep1	Issued	02/09/2019
□	ccmqa.com	org1		Issued	02/09/2019
□	*.ccmqa.com	org1		Issued	02/08/2019
□	local	andrey1		Issued	02/08/2019
□	*.google.com *	org1	dep1	Unmanaged (1)	04/17/2018
□	*.google.com *	org1	dep1	Unmanaged (1)	04/17/2018
□	ccmqa.com	org1	dep1	Issued	

- On clicking 'Renew', Incommon CM 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. See Certificate Collection for more details.

Renewing an 'Unmanaged' Certificate

Renewing an unmanaged certificate is similar to renewing a managed certificate, except you will need to complete full request details for the certificate.

- Click 'Certificates' > 'SSL Certificates'
- Select the unmanaged certificate you wish to renew from the list
- Click the 'Renew' button:



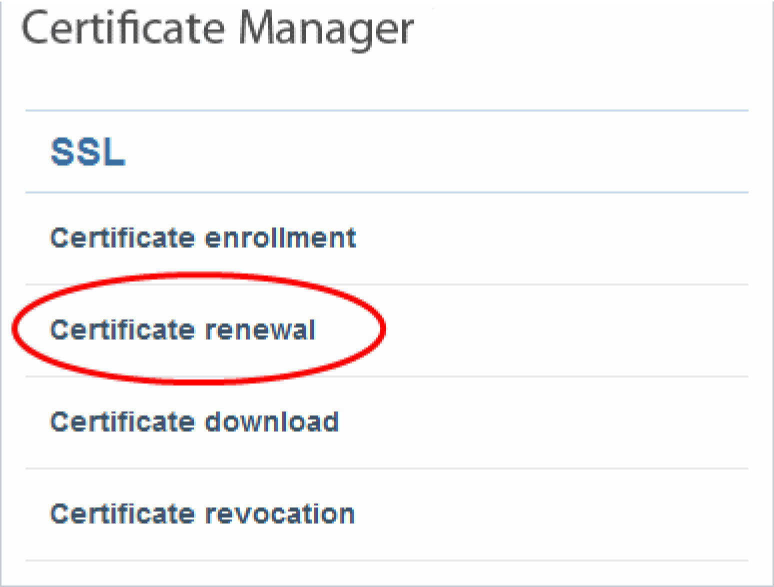
	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTA
☑	manualinstal.ccmqa.com *	org1	dep1	Unmanaged	01/27/2019	Not sche
□	*.google.com *	org1	dep1	Unmanaged (1)	04/17/2018	Not sc
□	manualinstal.ccmqa.com *	org1	dep1	Unmanaged	01/27/2019	

- Clicking the 'Renew' will open the 'Renew SSL Certificate' form. This form is similar to the Built-in Enrollment Wizard – Manual CSR Generation.
- Complete the wizard as explained in the section Built-in Enrollment Wizard – Manual CSR Generation.
- Incommon CM will place a request for the new certificate. The request needs to be approved before it is sent to Incommon CA for processing.
- Once issued, the renewed certificate can be collected and installed. See Certificate Collection for more details. After installation, the status of the certificate changes to 'Managed'.

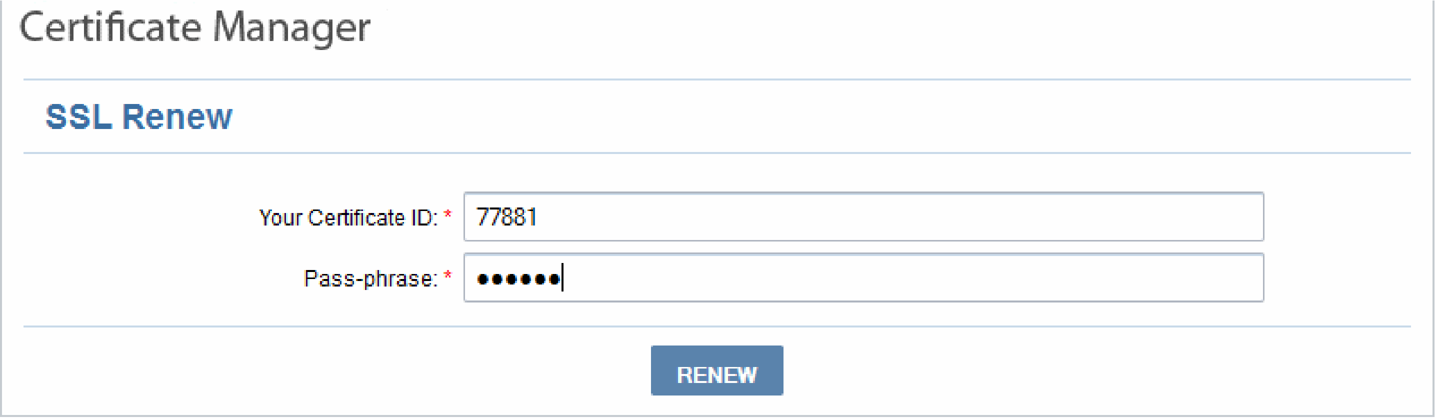
3.1.2.5.2 Certificate Renewal by the End-User

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/InCommon/ssl.



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


Certificate Manager

SSL Renew

Your Certificate ID: * 77881

Pass-phrase: * ••••••

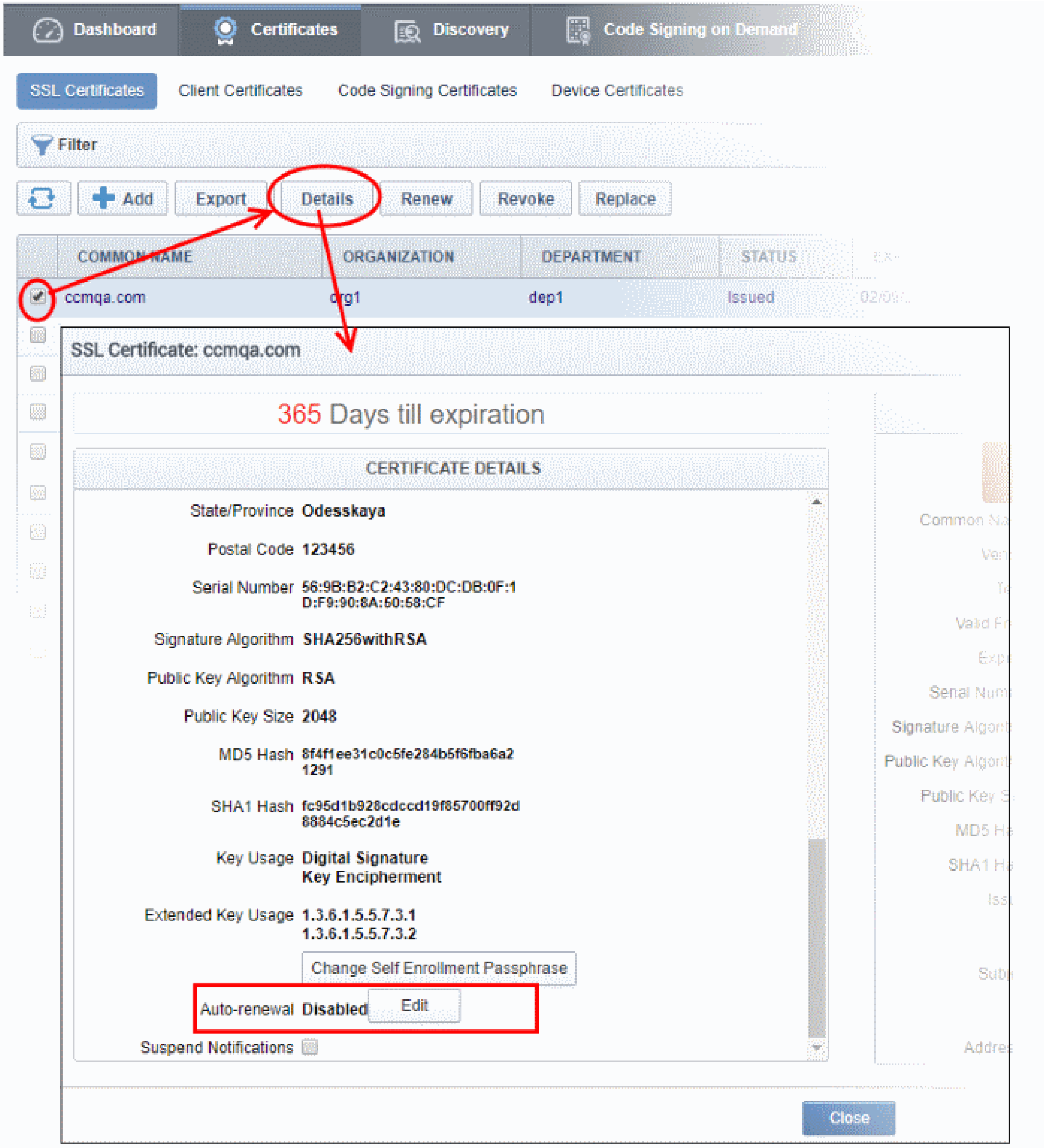
- Before proceeding to the full renewal application form, the user has to authenticate the request by:
  - Entering the correct certificate ID. The certificate ID is available from the certificate collection email and in the 'Certificates' > 'SSL' interface. Administrators may need to communicate the certificate ID to external applicants.
  - Entering the certificates renewal/revocation passphrase. This phrase was created during enrollment for the original 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.

3.1.2.5.3 Schedule Automatic Certificate Renewal

- You can schedule automatic renewal in the certificate details screen:
  - Click 'Certificates' > 'SSL Certificates' > select a certificate and click the 'Details' button.
  - Scroll down the certificate details screen and click 'Edit' beside 'Auto-renewal'

To configure auto-renewal of an SSL Certificate

- Click the 'Certificates' tab and choose 'SSL Certificates'
- Select the certificate you want to auto-renew and click the 'Details' button:



COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EX
☑ ccmqa.com	org1	dep1	Issued	02/09

SSL Certificate: ccmqa.com

365 Days till expiration

CERTIFICATE DETAILS

State/Province	Odesskaya
Postal Code	123456
Serial Number	56:9B:B2:C2:43:80:DC:DB:0F:1 D:F9:90:8A:50:58:CF
Signature Algorithm	SHA256withRSA
Public Key Algorithm	RSA
Public Key Size	2048
MD5 Hash	8f4f1ee31c0c5fe284b5f6fba6a2 1291
SHA1 Hash	fc95d1b928cdccd19f85700ff92d 8884c5ec2d1e
Key Usage	Digital Signature Key Encipherment
Extended Key Usage	1.3.6.1.5.5.7.3.1 1.3.6.1.5.5.7.3.2
Auto-renewal	Disabled
Suspend Notifications	□

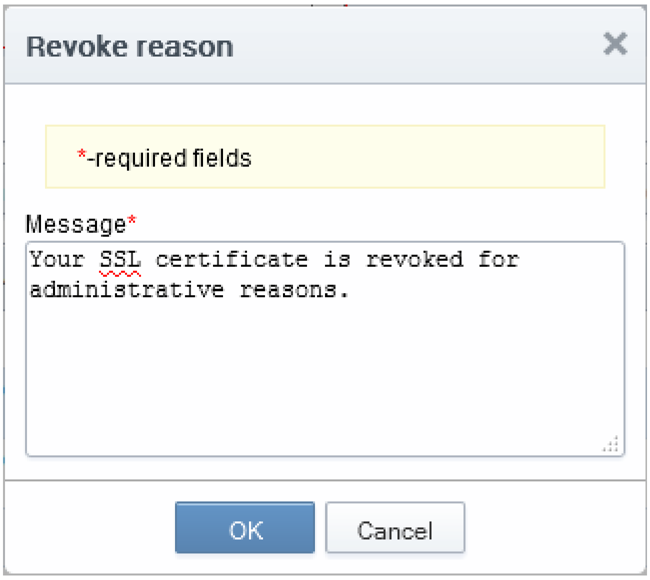
- Click the 'Edit' button beside 'Auto-renewal'
  - Enable auto renewal of this certificate – Select this to have Incommon CM apply for a new certificate when this one approaches expiry.
  - Create new key pair while renewing – Choose whether or not you want to generate a new key pair for the renewed certificate. Leaving it disabled means Incommon CM will re-use the key pair of the old certificate. Please note this option is available for certs with auto CSR generation and auto installation.
  - Number of days before expiration to start auto renewal - Choose the number of days in advance of expiry that the renewal process should start. On the scheduled day, the certificate controller will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.
- Click 'OK'

See 'SSL Certificate 'Details' Dialog' for other options in the SSL cert details screen.

3.1.2.6 Certificate Revocation, Replacement and Deletion

In the 'SSL Certificates' sub-tab of 'Certificates' interface 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.



Revoke reason

*-required fields

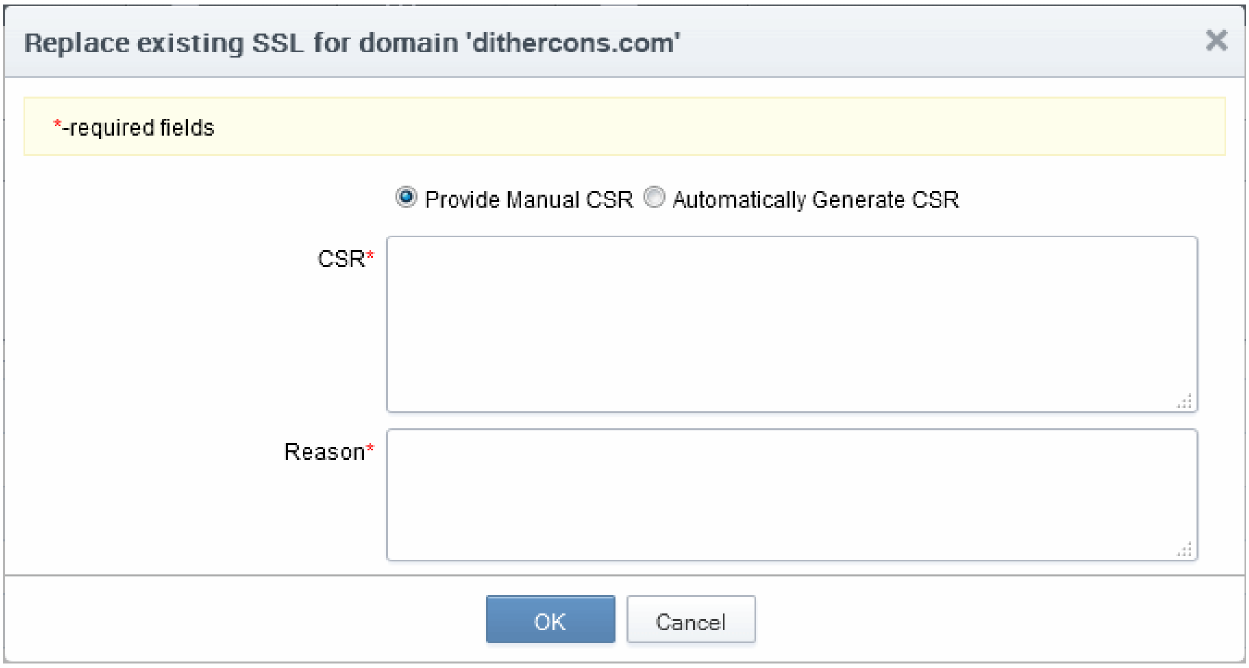
Message*

Your SSL certificate is revoked for administrative reasons.

- 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.



Replace existing SSL for domain 'dithercons.com'

*-required fields

● Provide Manual CSR ○ Automatically Generate CSR

CSR*

Reason*

- The administrator can choose to:
- Manually upload a new CSR for the new certificate. Refer to the section Method 2 - Built-in Enrollment Form - Manual CSR Generation for more details
- Instruct InCommon CM to generate a CSR and manage the private key associated with the new certificate at the Private Key Store configured at the local network. Refer to the section Method 3 - Built-in Enrollment Form - Auto CSR Generation for more details

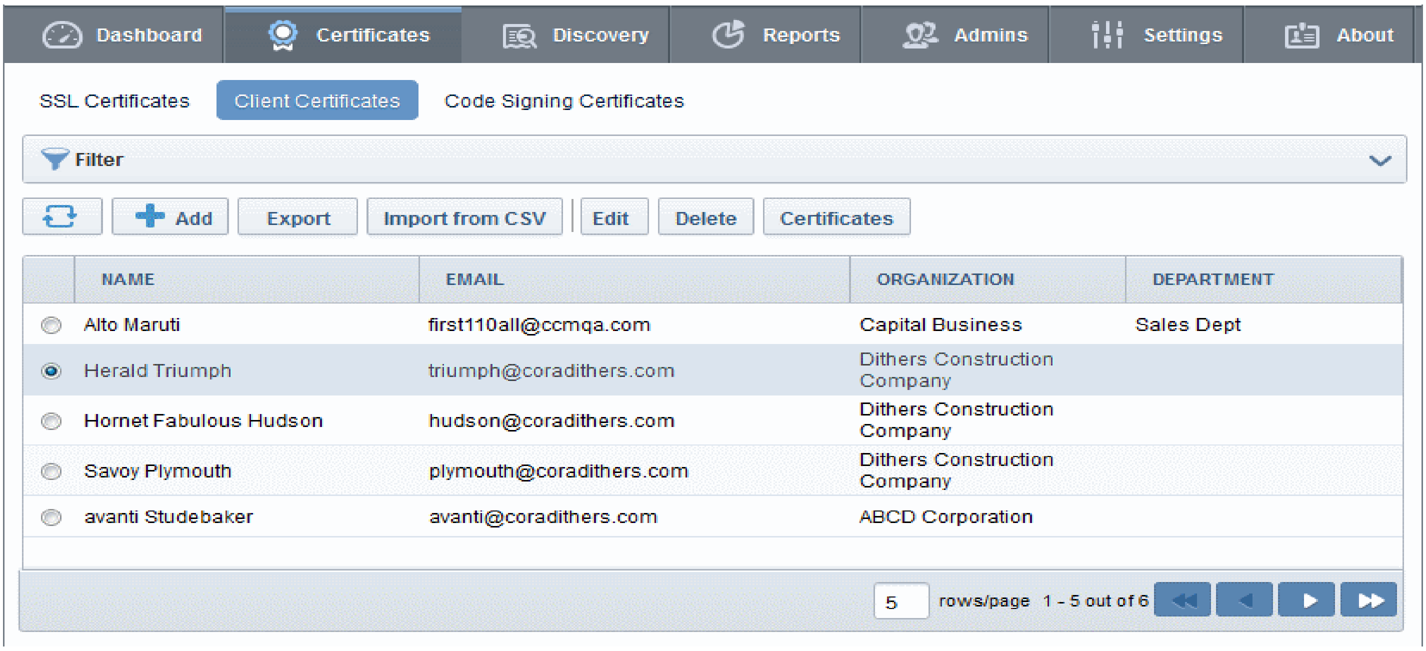
3.2 The Client Certificates area

3.2.1 Overview

The 'Client Certificates' area allows administrators to manage end-users client certificates and their owners' details.

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

- RAO S/MIME administrators - can view the client certificates and end-users of organizations (and any subordinate departments) that have been delegated to them.
- DRAO S/MIME administrators - can view the client certificates and end-users of departments that have delegated to them.



	NAME	EMAIL	ORGANIZATION	DEPARTMENT
○	Alto Maruti	first110all@ccmqa.com	Capital Business	Sales Dept
●	Herald Triumph	triumph@coradithers.com	Dithers Construction Company	
○	Hornet Fabulous Hudson	hudson@coradithers.com	Dithers Construction Company	
○	Savoy Plymouth	plymouth@coradithers.com	Dithers Construction Company	
○	avanti Studebaker	avanti@coradithers.com	ABCD Corporation	

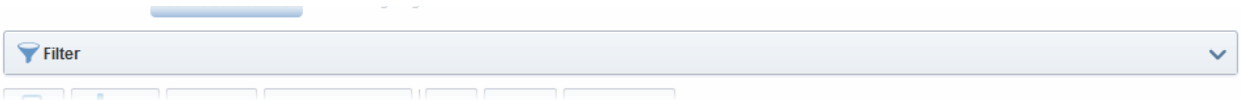
5 rows/page 1 - 5 out of 6

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
	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.

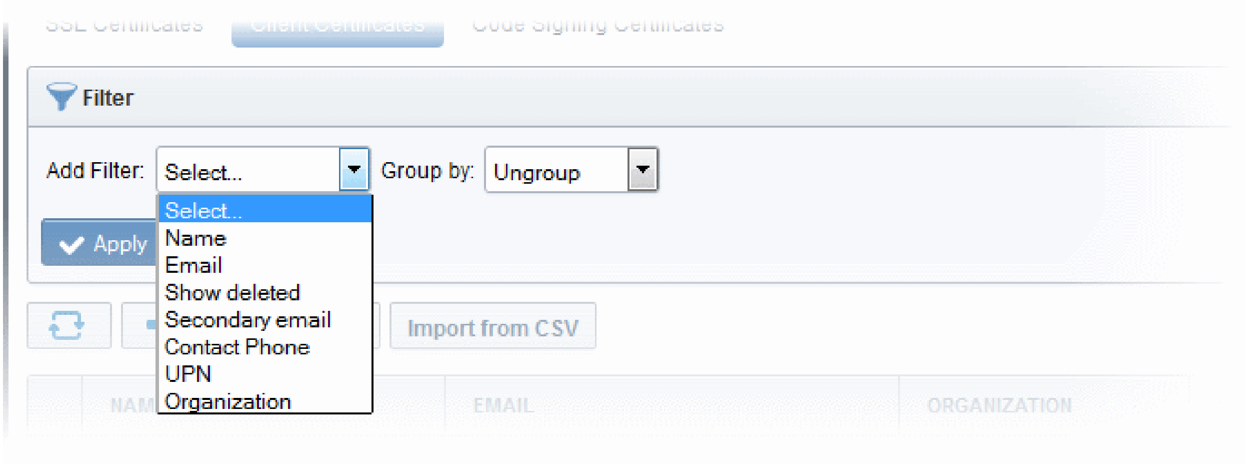
3.2.1.1 Sorting and Filtering Options

- Clicking 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.

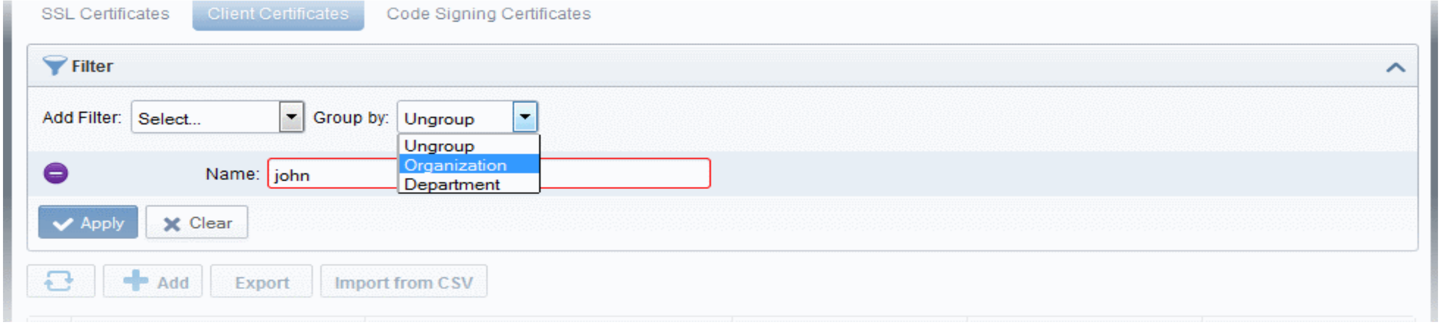


- To apply filters, click the down arrow on the right of the 'Filters' stripe. The filter options will be displayed.
- You can add filters by selecting from the options in the 'Add Filter' drop-down. You can group the results by various parameters.
- For example, you could filter certificates by 'Name' and group by 'Organization'



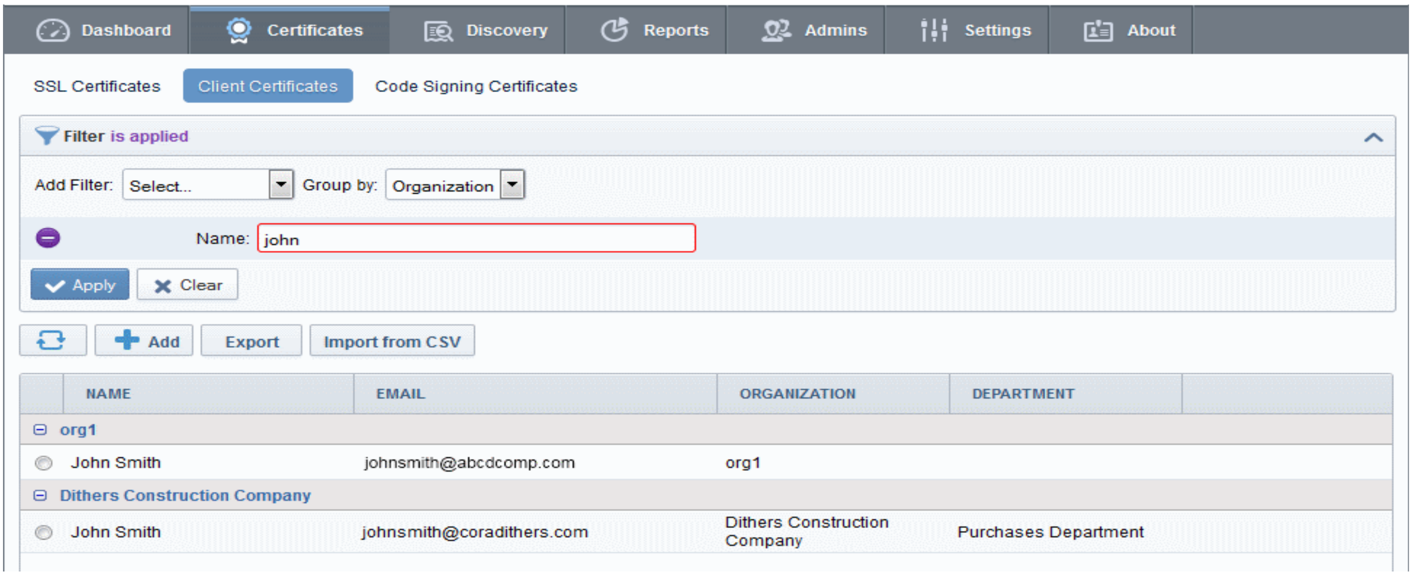
Tip: You can add more than one filter at a time to narrow down the filtering. To remove a filter criteria, click the '-' button to the left if it.

- 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:



Add Filter: Select... Group by: Organization

Name: john

NAME	EMAIL	ORGANIZATION	DEPARTMENT
⊟ org1			
○ John Smith	johnsmith@abcdcomp.com	org1	
⊟ Dithers Construction Company			
○ John Smith	johnsmith@coradithers.com	Dithers Construction Company	Purchases Department

- 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.

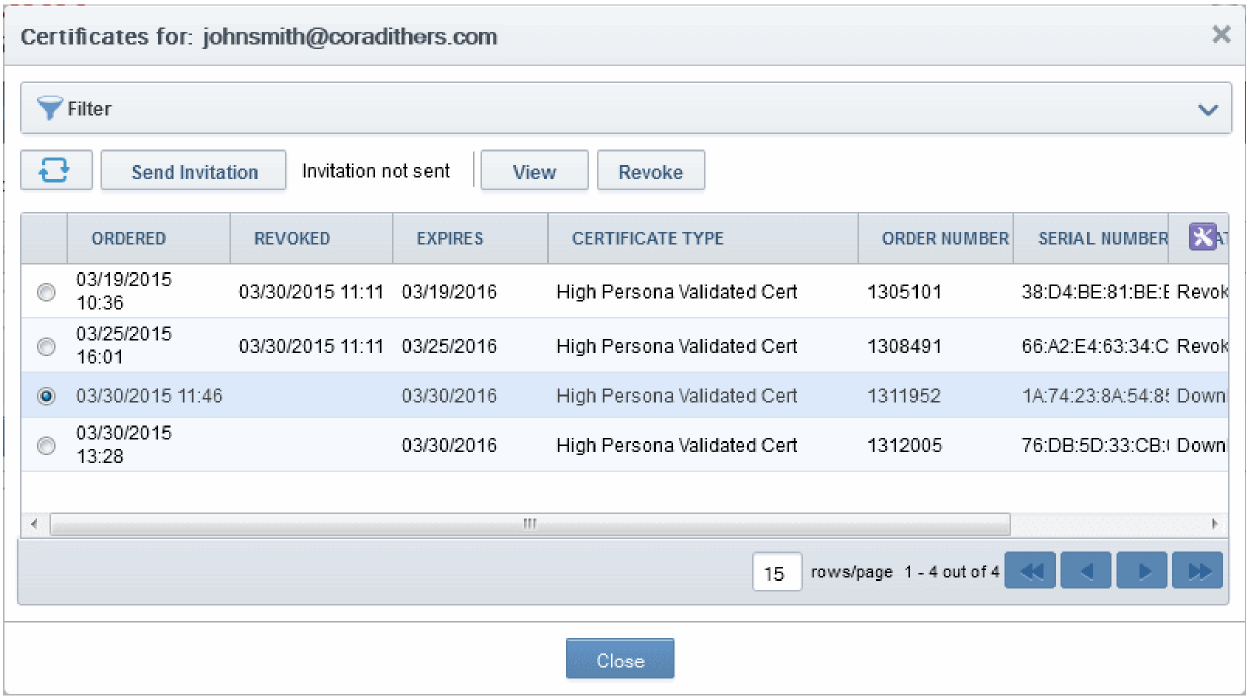
3.2.1.2 'Certificates' Dialog

To view all certificates that belong to a user:

- Click 'Certificates' > 'Client Certificates'
- Select a user from the list
- Click the 'Certificates' button

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.

The interface allows administrators to revoke, download, view and send a certificate invitation:



Certificates for: johnsmith@coradithers.com

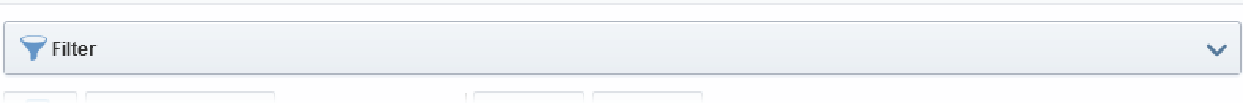
	ORDERED	REVOKED	EXPIRES	CERTIFICATE TYPE	ORDER NUMBER	SERIAL NUMBER	ST
○	03/19/2015 10:36	03/30/2015 11:11	03/19/2016	High Persona Validated Cert	1305101	38:D4:BE:81:BE:E	Revok
○	03/25/2015 16:01	03/30/2015 11:11	03/25/2016	High Persona Validated Cert	1308491	66:A2:E4:63:34:C	Revok
●	03/30/2015 11:46		03/30/2016	High Persona Validated Cert	1311952	1A:74:23:8A:54:8	Down
○	03/30/2015 13:28		03/30/2016	High Persona Validated Cert	1312005	76:DB:5D:33:CB:	Down

15 rows/page 1 - 4 out of 4

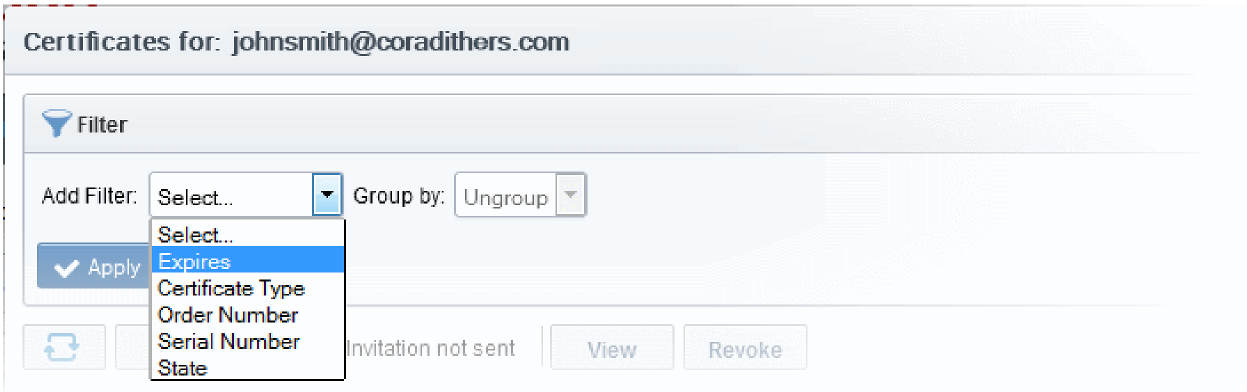
Sorting and Filtering Options

- Click a column header to sort items in alphabetical order of the entries in the respective column.

Administrators can search for a particular certificate by using filters.



To apply filters, click on the down arrow at the right end of the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down.



Certificates for: johnsmith@coradithers.com

The options available are:

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

  - State - Allows you to filter certificates based on their states

- Choose the filter and enter the parameters.
- 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		
Form Element	**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	Control	Reloads the list.

* InCommon 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:

i) 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;

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

InCommon 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 CM. 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 (PIN) to protect access to private key in .p12 file as well. The Administrator is able to bypass the PIN but should be aware that not all programs will subsequently allow the certificate to be imported if they do so. The following is a summary of browsers in which it is possible to import .p12 with empty password field.

Browser	Windows 8	Windows 7	Vista	XP	Mac
IE 6	-	-	-	✓	-
IE 7	-	-	✓	✓	-
IE 8 and above	✓	✓	✓	✓	-

FF 2	✓	✓	✓	✓	✓
FF 3 and above	✘	✘	✘	✘	✘
Opera 9	✓	✓	✓	✓	✓
Opera 10	✓	✓	✓	✓	✓
Google Chrome	✓	✓	✓	✓	✓
Safari	✓	✓	✓	✓	✓

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

3.2.2 Adding Cert End-Users

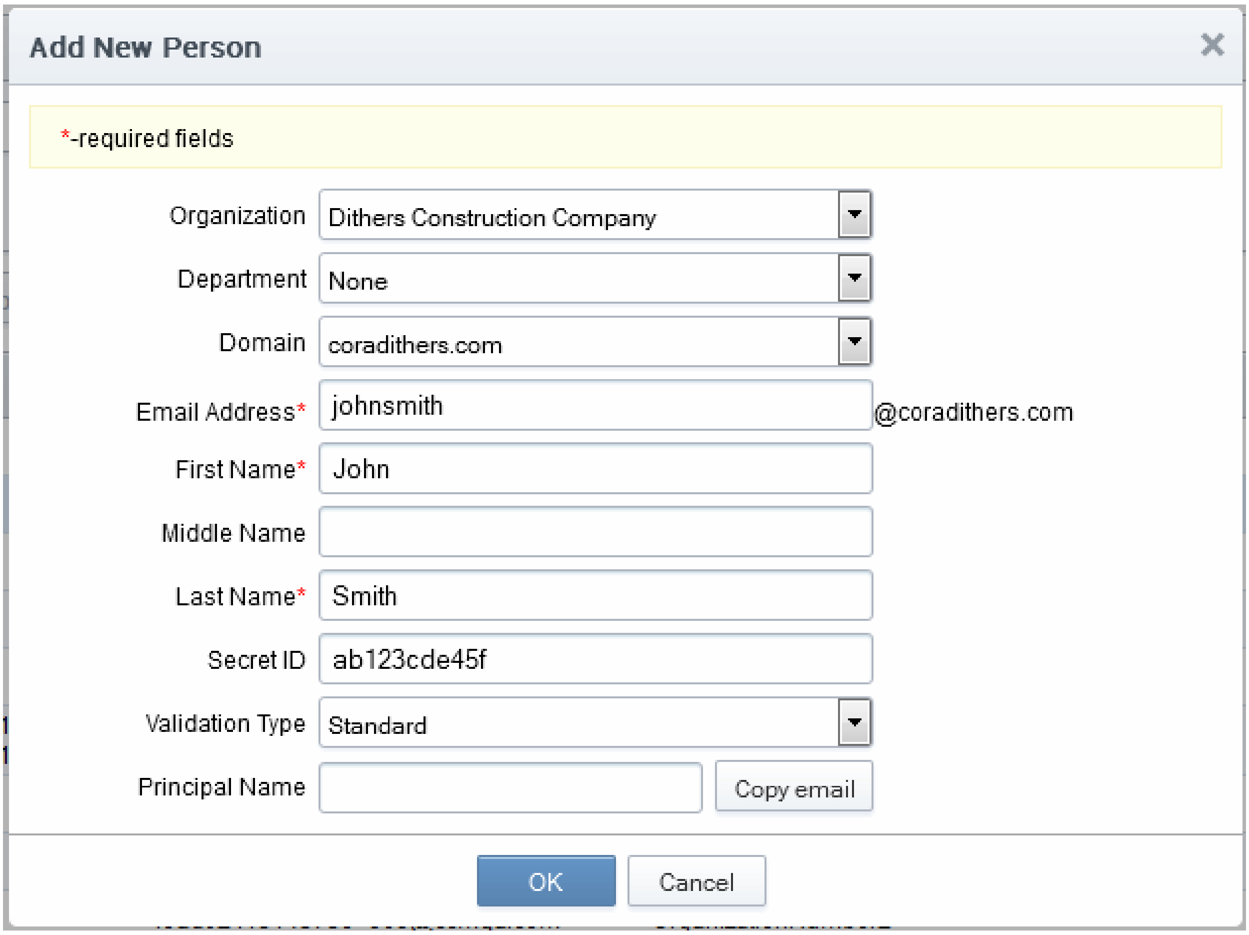
There are several methods of adding end-users to organizations in Certificate Manager.

- 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 when an SSL certificate application is made through the SSL Self Enrollment form. If the applicant does not already exist as an End-User when the form is submitted then a new End-User 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 Certificates' at the top left of the CM interface;



Add New Person

*-required fields

Organization	Dithers Construction Company
Department	None
Domain	coradithers.com
Email Address*	johnsmith @coradithers.com
First Name*	John
Middle Name	
Last Name*	Smith
Secret ID	ab123cde45f
Validation Type	Standard
Principal Name	

- Click the 'Add' button to open the 'Add New Person' form:
- Click 'OK' to add the end-user to Certificate Manager.
- An end-user's details can be modified at any time by selecting the user then clicking the 'Edit' button at the top of the interface.
    - 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.
    - Incommon CM maintains a username history. If a username is changed, you will still be able to search for client certificates using both the old and new names.
- 'Validation Type' drop down will only be visible if enabled by your InCommon 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

Form Element	Type	Description
		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 CM. 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 InCommon account manager. • Specify the type of client certificate that is issued to an applicant. • The two options are 'Standard' and 'High'. The difference between the two lies in the degree of user authentication is carried out prior to issuance. • 'Standard' certificates can be issued quickly and take advantage of the user authentication mechanisms that are built into Incommon CM. A user applying for a 'Standard' 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 validated as the owner of that domain • The user must know either a unique 'Access Code' or 'Secret ID' that should be entered at the certificate enrollment form. 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

Form Element	Type	Description
		Note: The additional validation steps must be completed PRIOR to the 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. • Contact your Master Administrator to check whether an organization or department is enabled for Principal Name support/customization. • 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 a department, this field will be auto populated with the email address entered in '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 Load Multiple End-Users from a Comma Separated Values (.csv) File

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

Note: Only RAO S/MIME and DRAO S/MIME admins can load end-users from a .csv file.

3.2.2.2.1 Procedure Overview

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

1. Admin generates a .csv file containing a list of end-users. .csv files can be created in programs such as Excel or Open Office Calc.

2. In Incommon CM, click 'Certificates Management' > 'Client Certificates' > 'Import from CSV' button

3. Browse to your .csv file and click 'Submit'

4. Incommon CM 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.

5. Click the end-user record. The “Certificate for end-user@exampledomain” dialog will be displayed.

6. Click 'Send Invitation'

7. End-users collect and install their certificates.

3.2.2.2.2 Requirements for .csv file

The fields per-user in the .csv differ depending on whether or not principal name support is enabled for the organization. Contact your Master Administrator to check whether an organization or department is enabled for Principal Name support/customization.

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' is mandatory if the administrator that is importing is a DRAO S/MIME.
  RAO S/MIME (and DRAO S/MIME administrators that are also RAO S/MIME 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 as specified below (including commas (,) and quotation marks (" ")).

- For the Organizations enabled with Principal Name support, the Principal Name field must be entered with the value. For the Organizations that are not enabled with Principal Name Support, the field must be included but should be left blank ("").

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/customization by contacting the Master Administrator.

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.

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 S/MIME.
RAO S/MIME (and DRAO S/MIME administrators that are also RAO S/MIME 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 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:

- Any mandatory field in 3.2.2.2.2.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
- 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
- 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:
  - RAO S/MIME administrators have permission to import for organizations (and any subordinate departments) that have been delegated to them. RAO S/MIME may leave the 'Department' field blank.
  - DRAO S/MIME administrators have permission to import for departments that have delegated to them. DRAO S/MIME administrators ***cannot*** leave the 'Department' field blank unless they are also an RAO S/MIME for the same Organization.

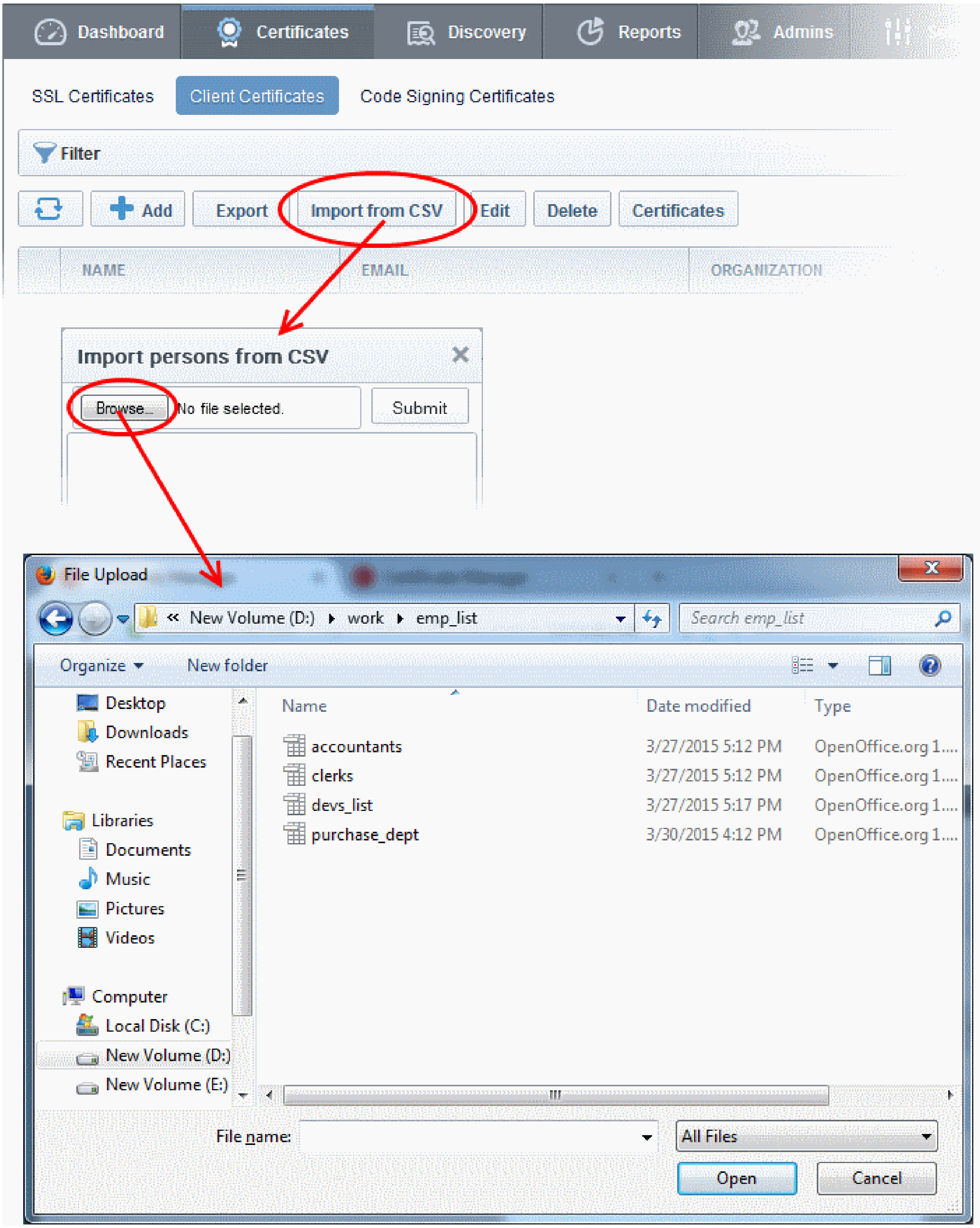
3.2.2.2.4 The Import Process

To load the .csv file

- Click 'Certificates Management' > 'Client Certificates' > 'Import from CSV'

The 'Import from CSV' dialog will appear.

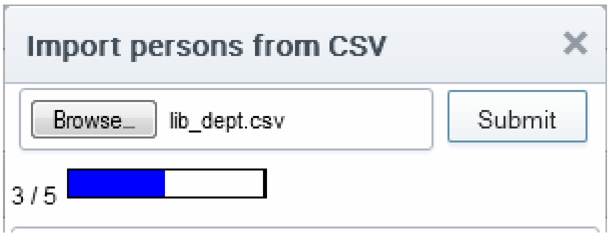
- Click the 'Browse' button and navigate to the .csv file



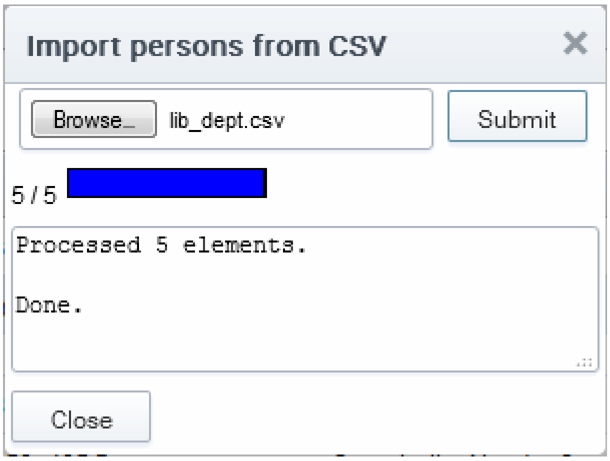
Name	Date modified	Type
accountants	3/27/2015 5:12 PM	OpenOffice.org 1....
clerks	3/27/2015 5:12 PM	OpenOffice.org 1....
devs_list	3/27/2015 5:17 PM	OpenOffice.org 1....
purchase_dept	3/30/2015 4:12 PM	OpenOffice.org 1....

- Click 'Submit'.

An import status dialog box is displayed. You will see a progress bar indicating that information is being uploaded:



CM will inform you when the process is finished:

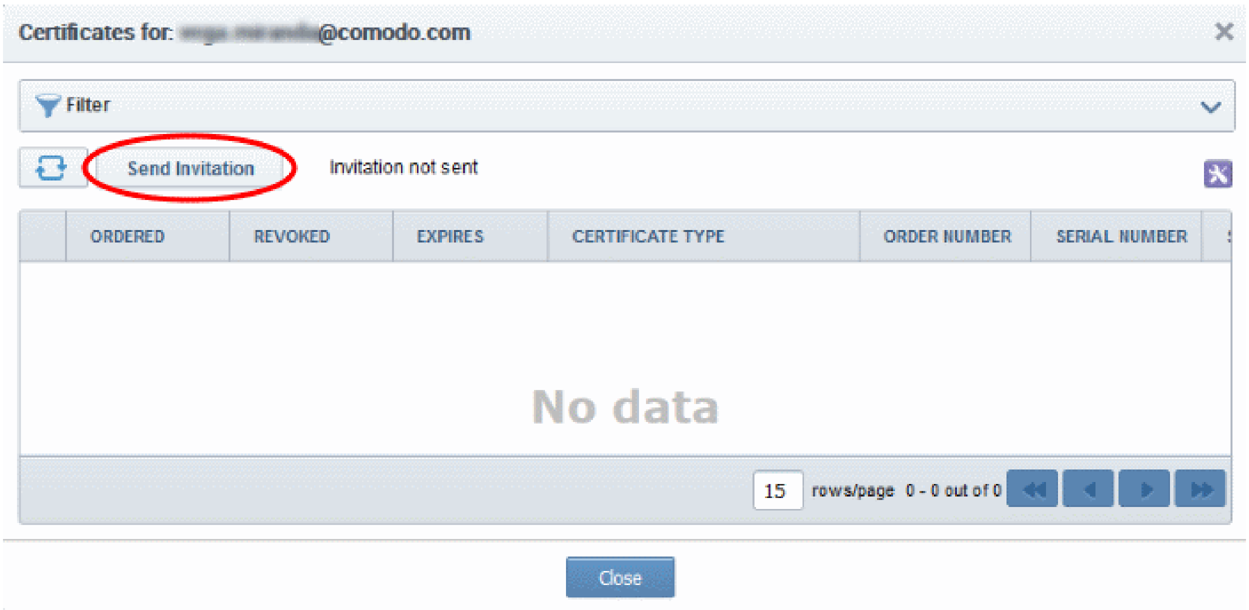


```
Processed 5 elements.

Done.
```

All imported users will appear in the 'Client Certificates' section. Notification emails containing a link to the Self-Enrollment form and the secret ID will also be sent to imported users. This notification email will be sent to the end-user after their record is created.

To manually send an invitation to a user:

- Click 'Certificates Management' > 'Client Certificates'
- Click the end-user record. The "Certificate for end-user@exampledomain" dialog will be displayed.
- Click "Send Invitation"


Certificates for: [redacted]@comodo.com

Invitation not sent

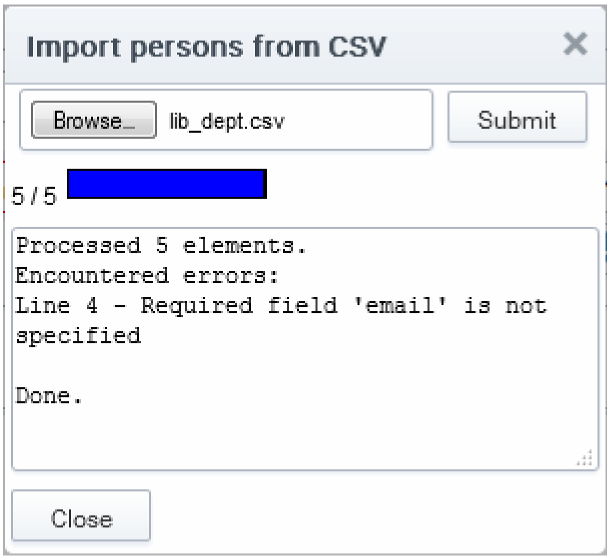
An email with a link to the user registration form will be sent to the applicant. The email will be sent to the account in the user's record in Incommon CM.

- Click the link in the notification email to open the self-enrollment form.
- Enter the fields required in the form and click 'Submit'.

The certificate will be downloaded.

3.2.2.2.5 Errors in .csv file

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



```
Processed 5 elements.
Encountered errors:
Line 4 - Required field 'email' is not
specified

Done.
```

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

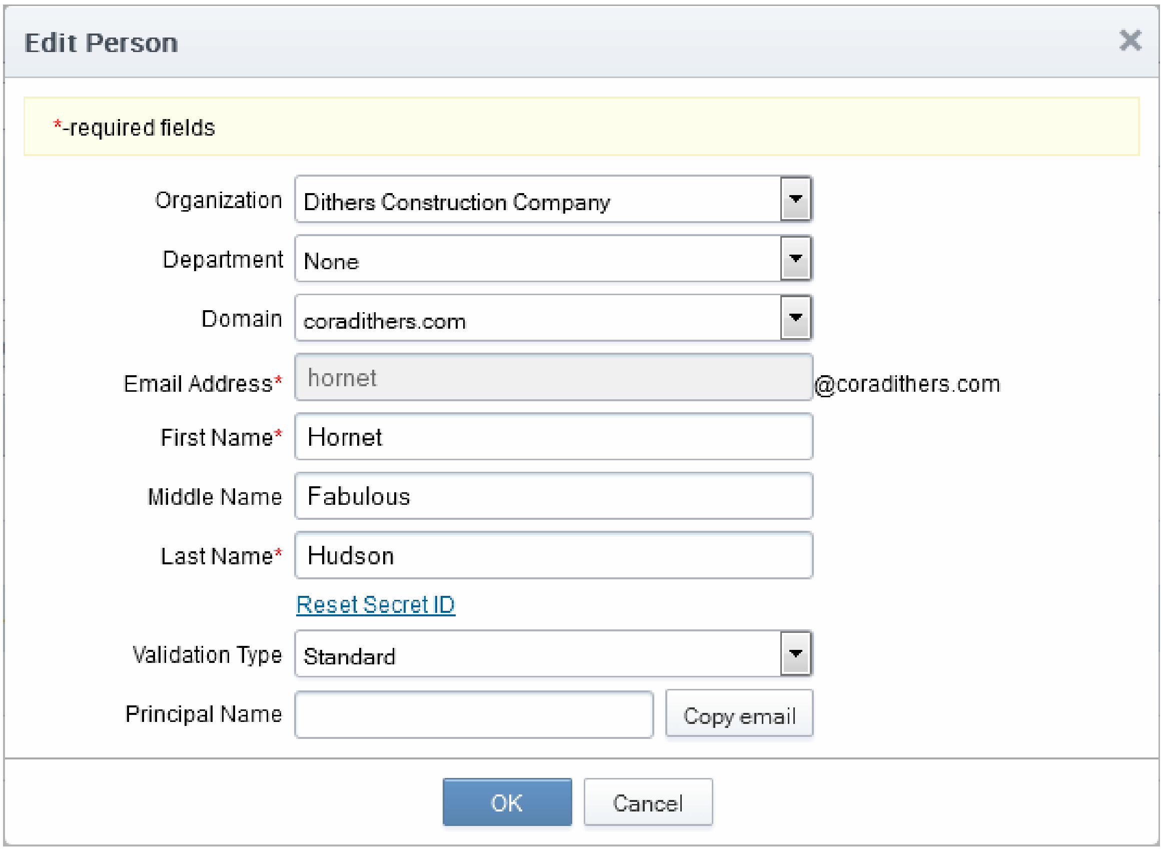
3.2.2.3 Auto Creation of End-Users via Certificate Self Enrollment Form

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.



Edit Person

*-required fields

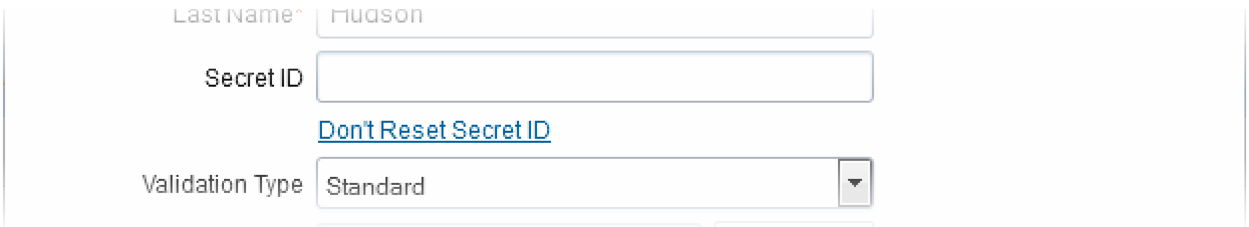
Organization	Dithers Construction Company
Department	None
Domain	coradithers.com
Email Address*	hornet @coradithers.com
First Name*	Hornet
Middle Name	Fabulous
Last Name*	Hudson
	Reset Secret ID
Validation Type	Standard
Principal Name	

Notes:

- 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.



Last Name*	Hudson
Secret ID	
	Don't Reset Secret ID
Validation Type	Standard

    - 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 InCommon account manager. For an explanation of validation types, see 'Validation Type' in the 'Add New Person' table of parameters.

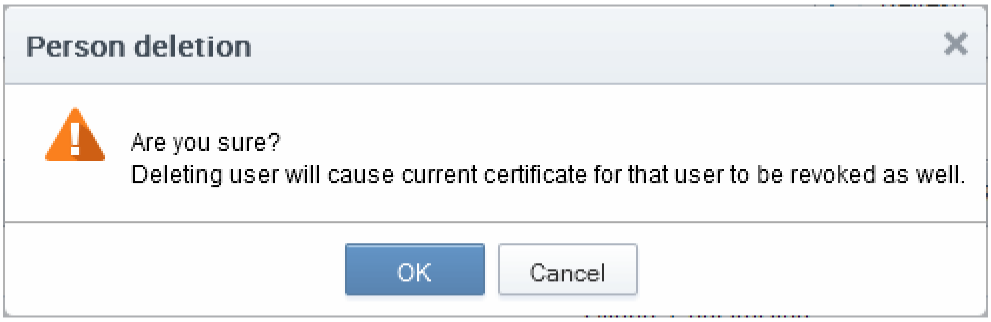
- Renaming an end-user does not affect the search and filtering actions in the Client Certificates Interface. CM allows the administrators to search for particular user or client certificates using both the old name and the new name in case a user name is changed.

- 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.



Person deletion

Are you sure?
Deleting user will cause current certificate for that user to be revoked as well.

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 CM. The Administrators can send the invitation mail from the CM 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.

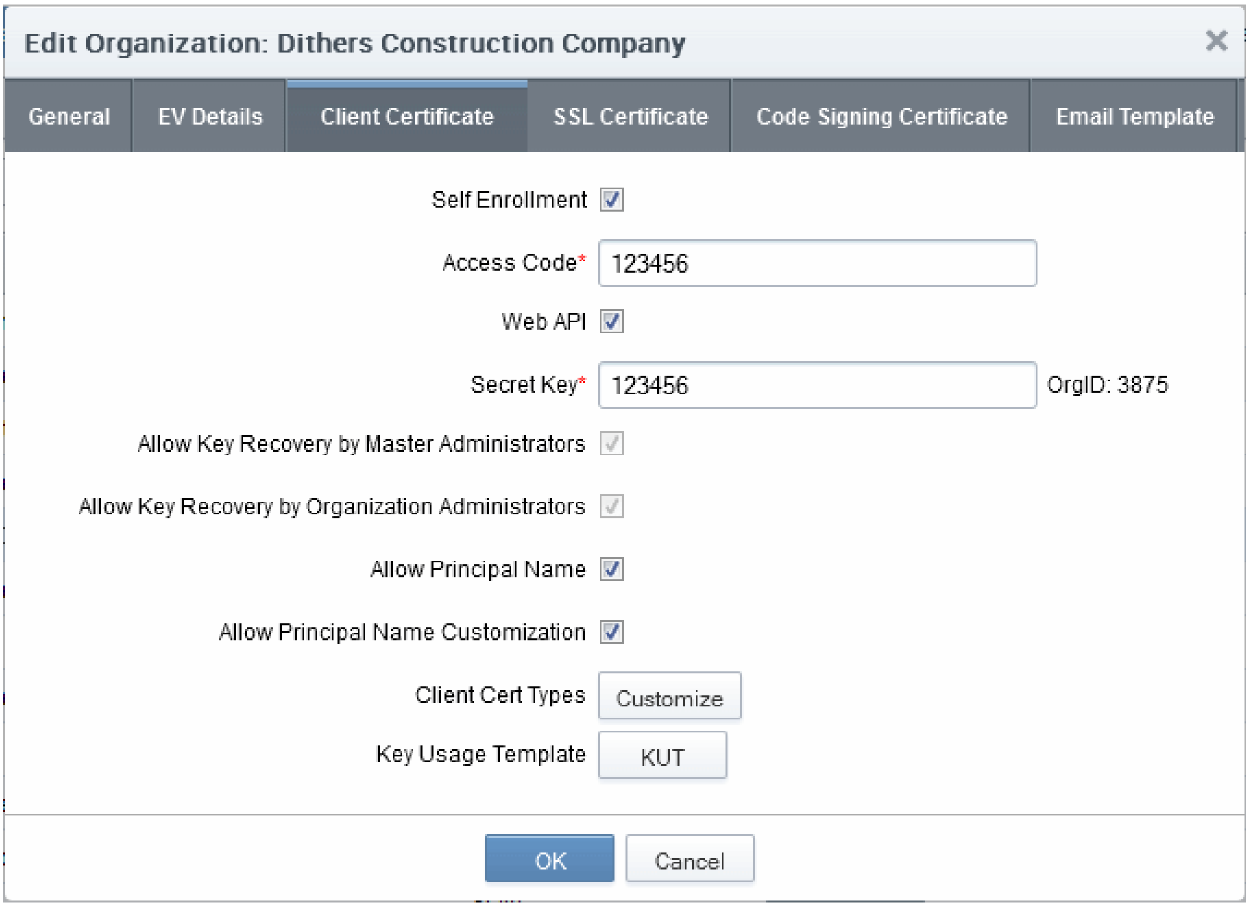
3.2.5.1 Self Enrollment by Access Code

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 S/MIME certificates, has been pre-validated by Incommon and that the domain has been activated by your Incommon account manager. (i.e. if you wish to issue client certificates to end-user@mycompany.com, then mycompany.com must have been pre-validated by Incommon).

  If you request a certificate for a brand new domain, then this domain will first have to undergo validation by Incommon. Once validated, the 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 an organization or department. See Editing an Existing Organization for more details on adding a domain to an organization.
- The RAO S/MIME or DRAO S/MIME 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.


Edit Organization: Dithers Construction Company

Self Enrollment ☑

Access Code* 123456

Web API ☑

Secret Key* 123456 OrgID: 3875

Allow Key Recovery by Master Administrators ☑

Allow Key Recovery by Organization Administrators ☑

Allow Principal Name ☑

Allow Principal Name Customization ☑

Client Cert Types Customize

Key Usage Template KUT

- 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.

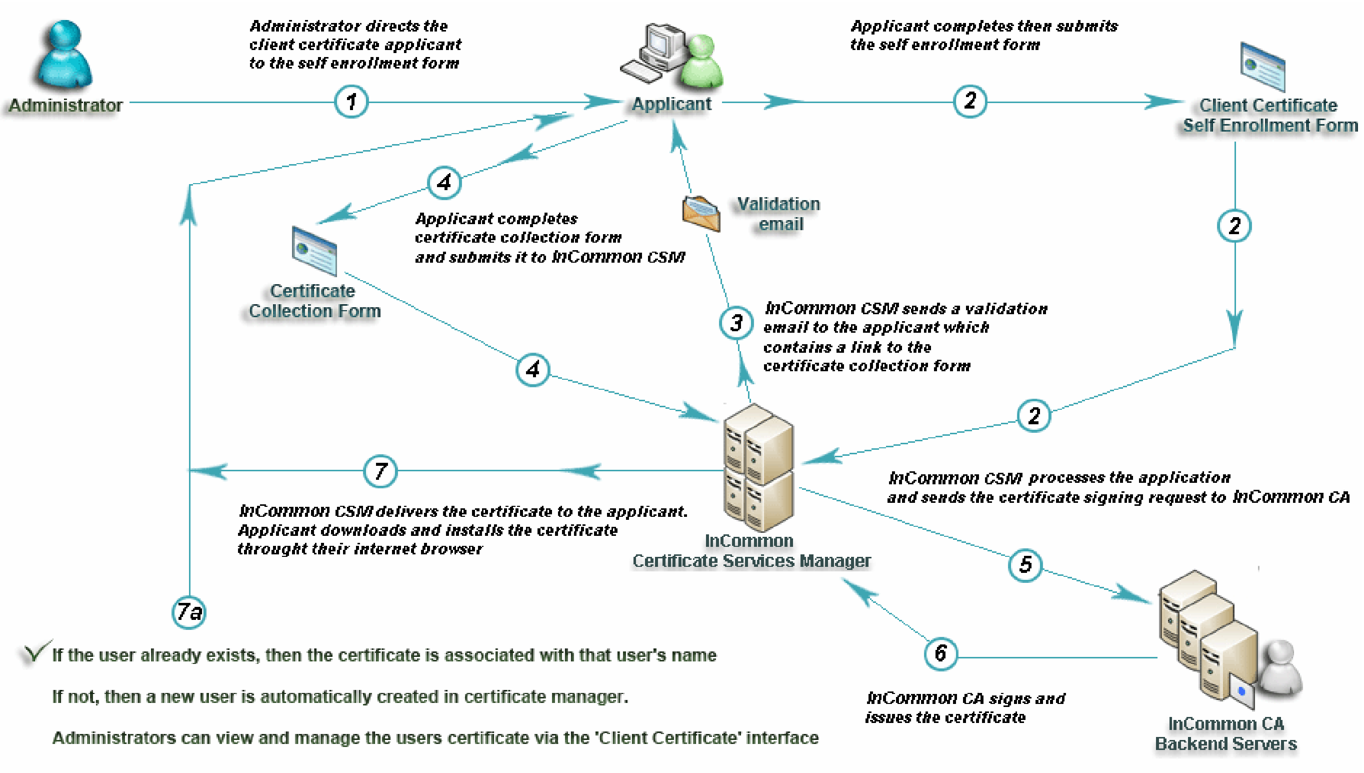
3. Administrator directs the personal certificate applicant to the 'Access Code' based Self Enrollment Form - making sure the application is done from the end-user's computer (see section Initiating the enrollment process).

4. Applicant completes then submits the Self Enrollment Form, specifying the correct Access Code for the Organization's domain. (See section The Self Enrollment Form)

5. CM 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)

6. Applicant completes the Account Validation form. The certificate request is sent to InCommon CA servers. If the application is successful, the applicant will be able to download and install their personal certificate. (See section Certificate Collection.)

7. 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 CM 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 CM will automatically add this applicant as a new 'End-user' to the 'Client Certificates' area'. (Click Here for further details)



Administrator
Administrator directs the client certificate applicant to the self enrollment form
1
Applicant
Applicant completes then submits the self enrollment form
2
Client Certificate Self Enrollment Form
2
4
Applicant completes certificate collection form and submits it to InCommon CSM
Validation email
Certificate Collection Form
3
InCommon CSM sends a validation email to the applicant which contains a link to the certificate collection form
4
2
InCommon CSM processes the application and sends the certificate signing request to InCommon CA
7
InCommon CSM delivers the certificate to the applicant. Applicant downloads and installs the certificate throught their internet browser
InCommon Certificate Services Manager
5
7a
✓ If the user already exists, then the certificate is associated with that user's name
If not, then a new user is automatically created in certificate manager.
Administrators can view and manage the users certificate via the 'Client Certificate' interface
6
InCommon CA signs and issues the certificate
InCommon CA Backend Servers

3.2.5.1.3 Initiating the Enrollment Process

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

1. A link to the Access Code based Self Enrollment Form - https://cert-manager.com/customer/Comodo/smime?action=enroll&swt=ac

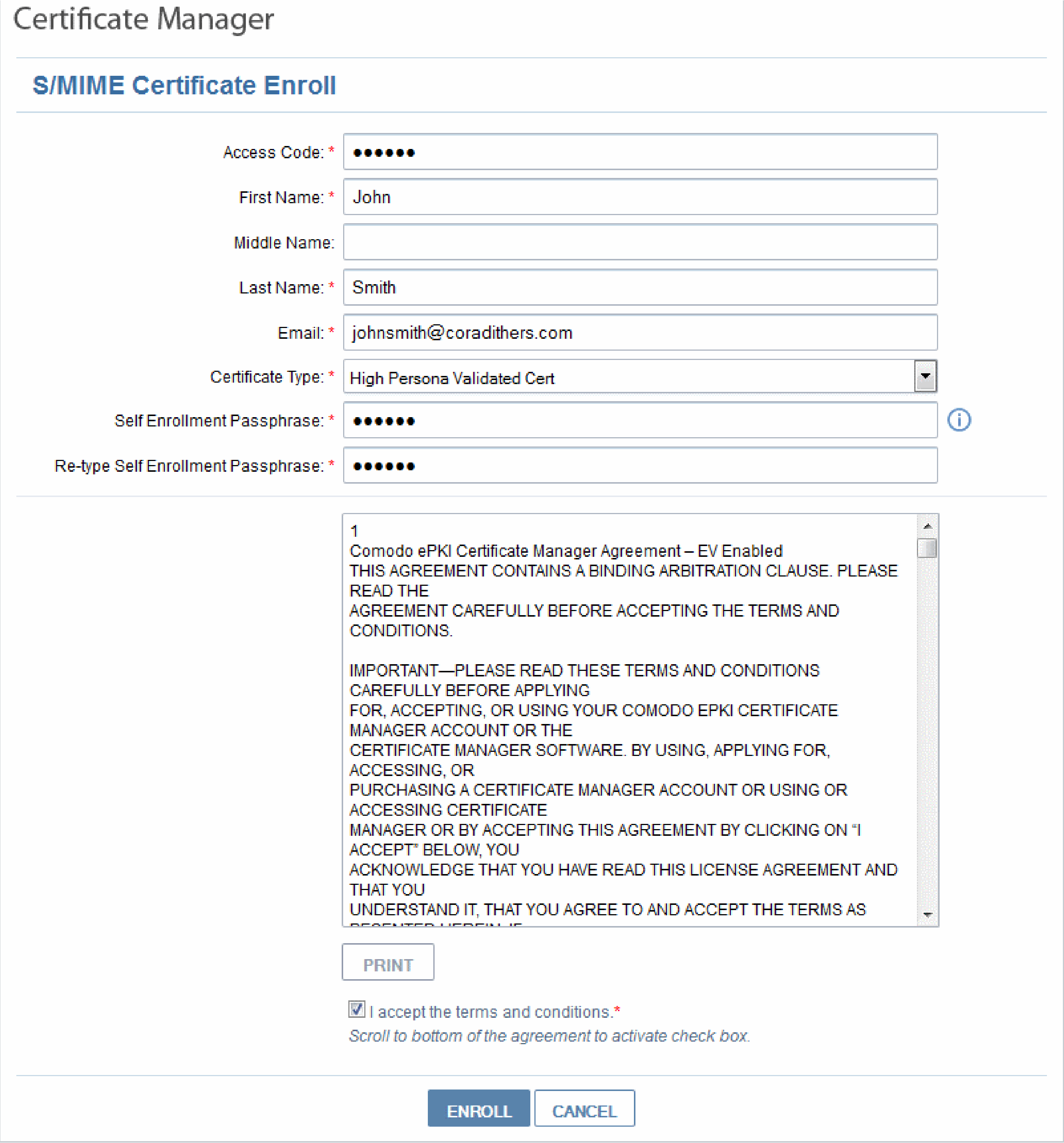
- The client access code specified in that organization's Client Cert settings tab..

These details can be sent to the applicant using an out-of-band communication method such as email.

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



Certificate Manager

S/MIME Certificate Enroll

Access Code: *	••••••
First Name: *	John
Middle Name:	
Last Name: *	Smith
Email: *	johnsmith@coradithers.com
Certificate Type: *	High Persona Validated Cert
Self Enrollment Passphrase: *	••••••
Re-type Self Enrollment Passphrase: *	••••••

1
Comodo ePKI Certificate Manager Agreement – EV Enabled
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE
AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.

IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING
FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE MANAGER ACCOUNT OR THE
CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR, ACCESSING, OR
PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR ACCESSING CERTIFICATE
MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU
ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND THAT YOU
UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS

☑ I accept the terms and conditions.*

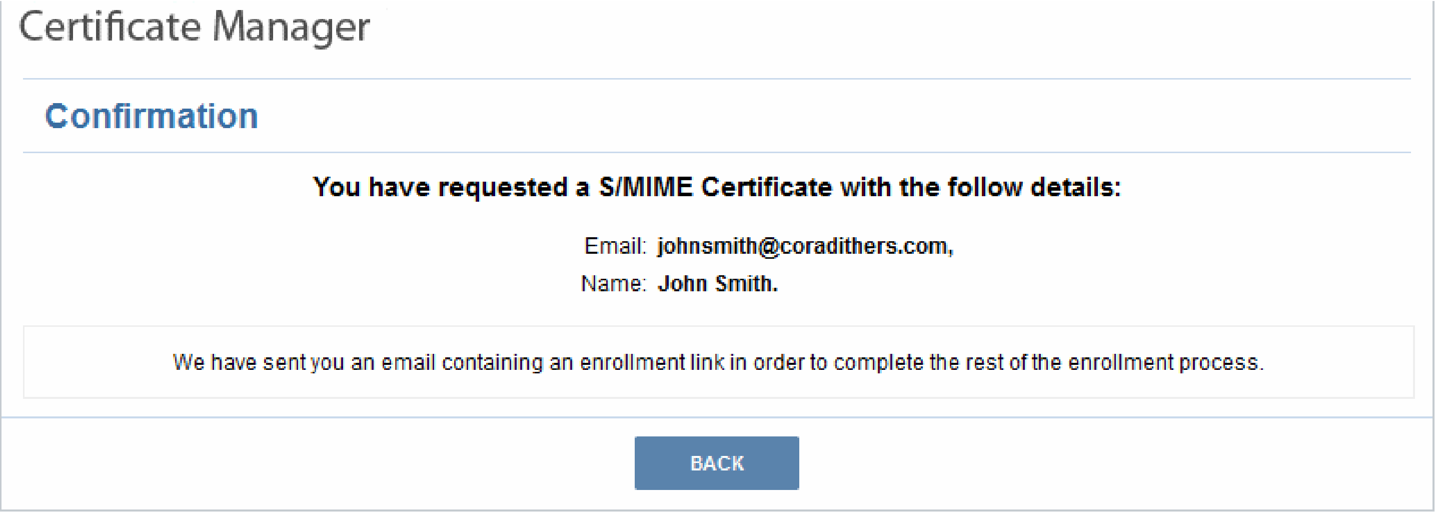
Scroll to bottom of the agreement to activate check box.

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)***	Check-box	Applicant must accept the terms and conditions before submitting the form.
Enroll	Control	Submits the application and enrolls the applicant for the client certificate.
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 Master Administrator. Contact your Master Administrator if such custom fields are required.

After completing the form and clicking the 'Enroll' button, a confirmation dialog will be displayed:



Certificate Manager

Confirmation

You have requested a S/MIME Certificate with the follow details:

Email: **johnsmith@coradithers.com,**

Name: **John Smith.**

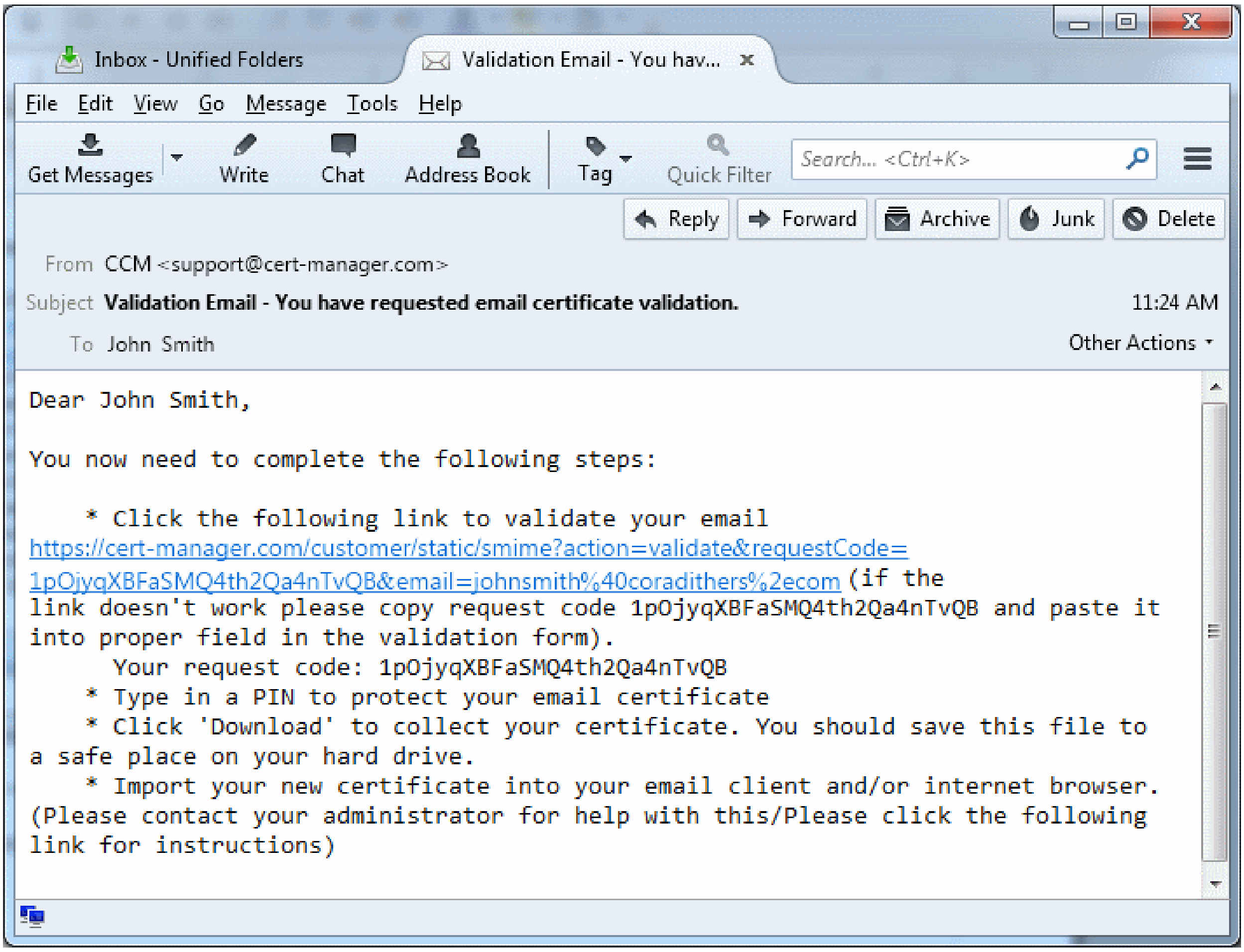
We have sent you an email containing an enrollment link in order to complete the rest of the enrollment process.

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 Validation of the Application for more details. After completing the validation process, a certificate collection form will appear. This form allows the end-user to download and save the certificate. See 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 InCommon.

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 the link in the email will automatically populate the request 'Code' and 'Email' fields in the Account Validation form.



From CCM <support@cert-manager.com>

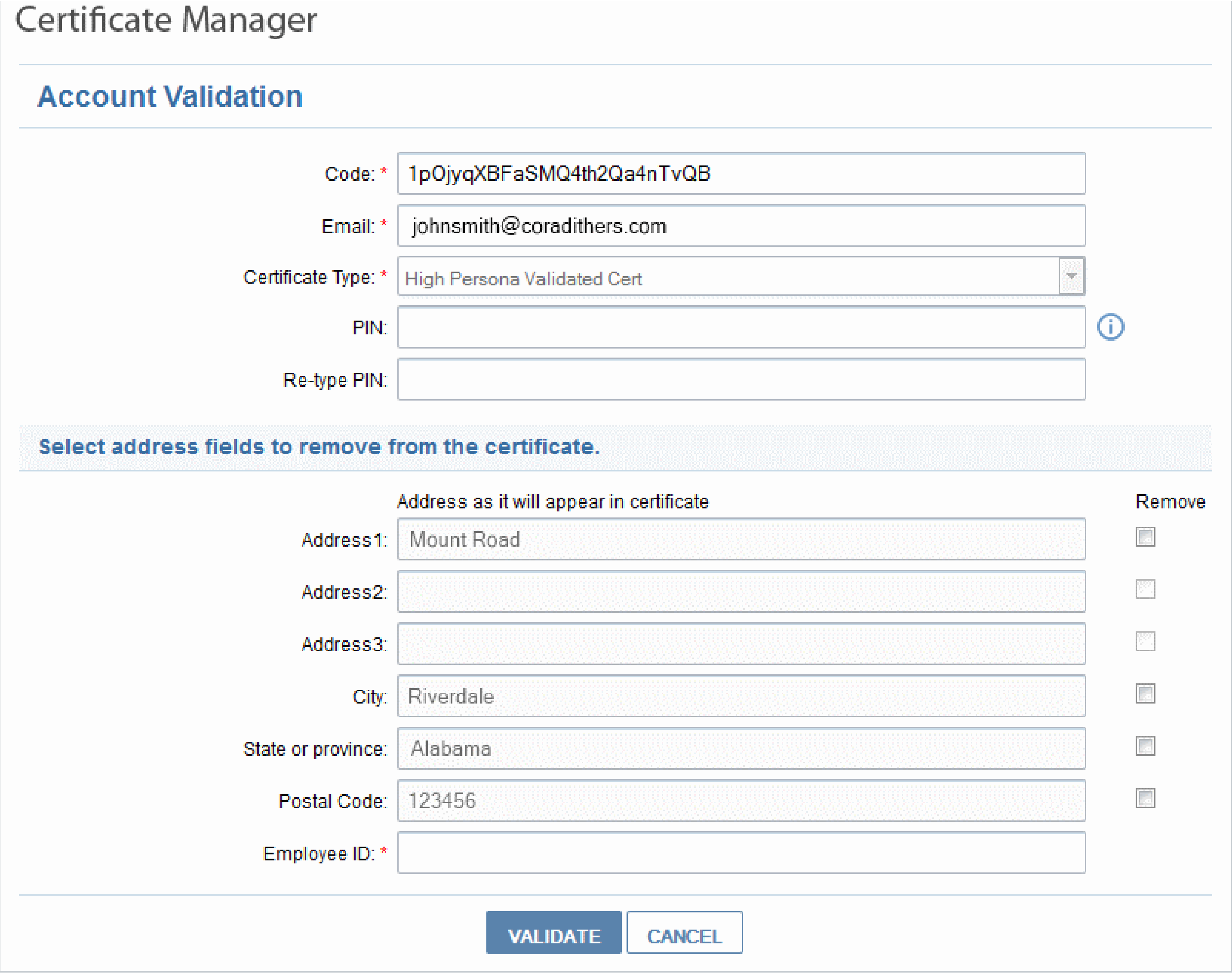
Subject **Validation Email - You have requested email certificate validation.** 11:24 AM

To John Smith

```
Dear John Smith,

You now need to complete the following steps:

    * Click the following link to validate your email
https://cert-manager.com/customer/static/smime?action=validate&requestCode=
1pOjyqXBFaSMQ4th2Qa4nTvQB&email=johnsmith%40coradithers%2ecom (if the
link doesn't work please copy request code 1pOjyqXBFaSMQ4th2Qa4nTvQB and paste it
into proper field in the validation form).
      Your request code: 1pOjyqXBFaSMQ4th2Qa4nTvQB
    * Type in a PIN to protect your email certificate
    * Click 'Download' to collect your certificate. You should save this file to
a safe place on your hard drive.
    * Import your new certificate into your email client and/or internet browser.
(Please contact your administrator for help with this/Please click the following
link for instructions)
```

Note: It is possible for administrators to modify the contents of these emails in the 'Email Templates' area under 'Organization' > 'Edit'.

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



Certificate Manager

Account Validation

Code: * 1pOjyqXBFaSMQ4th2Qa4nTvQB

Email: * johnsmith@coradithers.com

Certificate Type: * High Persona Validated Cert

PIN:

Re-type PIN:

Select address fields to remove from the certificate.

	Address as it will appear in certificate	Remove
Address1:	Mount Road	☐
Address2:		☐
Address3:		☐
City:	Riverdale	☐
State or province:	Alabama	☐
Postal Code:	123456	☐

Employee ID: *

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.
Email *(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	Check boxes	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' check boxes beside the required address fields. Click here for more details.
Validate	Control	Completes the validation process and enables the applicant to download the certificate
Cancel	Control	Clears all data entered on the form

Selecting Address Fields to be Removed from the Certificate

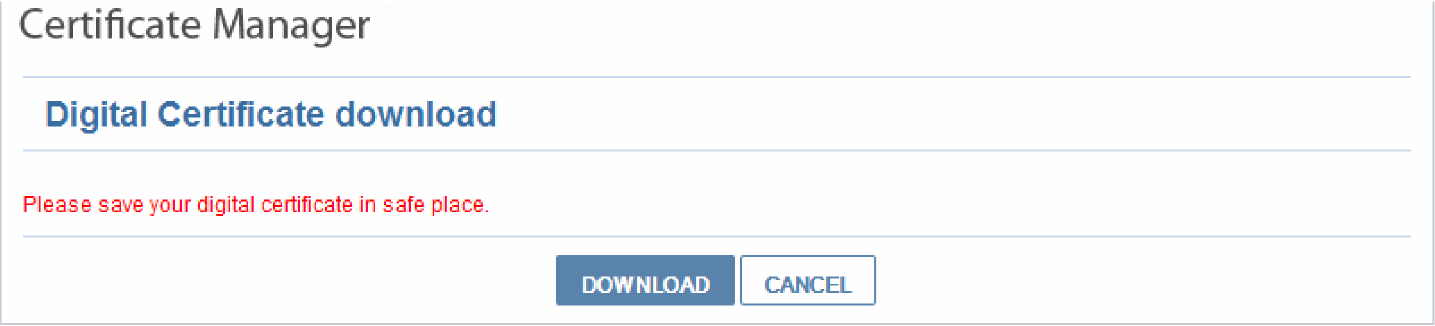
The following address fields...

- 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' check-boxes 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.

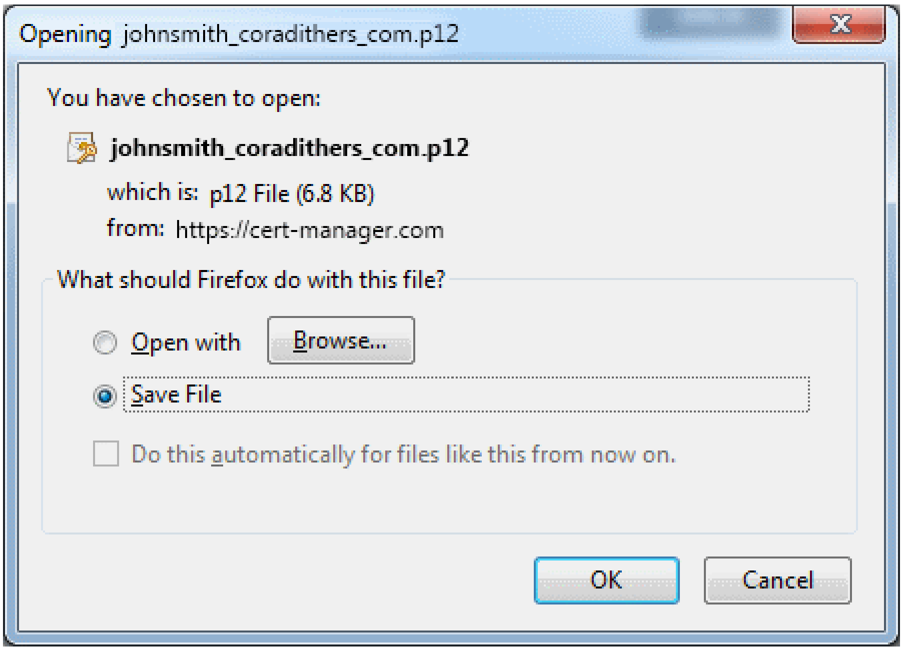


Certificate Manager

Digital Certificate download

Please save your digital certificate in safe place.

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



Opening johnsmith_coradithers_com.p12

You have chosen to open:

johnsmith_coradithers_com.p12

which is: p12 File (6.8 KB)

from: https://cert-manager.com

What should Firefox do with this file?

○ Open with [Browse...]

● Save File

□ Do this automatically for files like this from now on.

[OK] [Cancel]

CM 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.

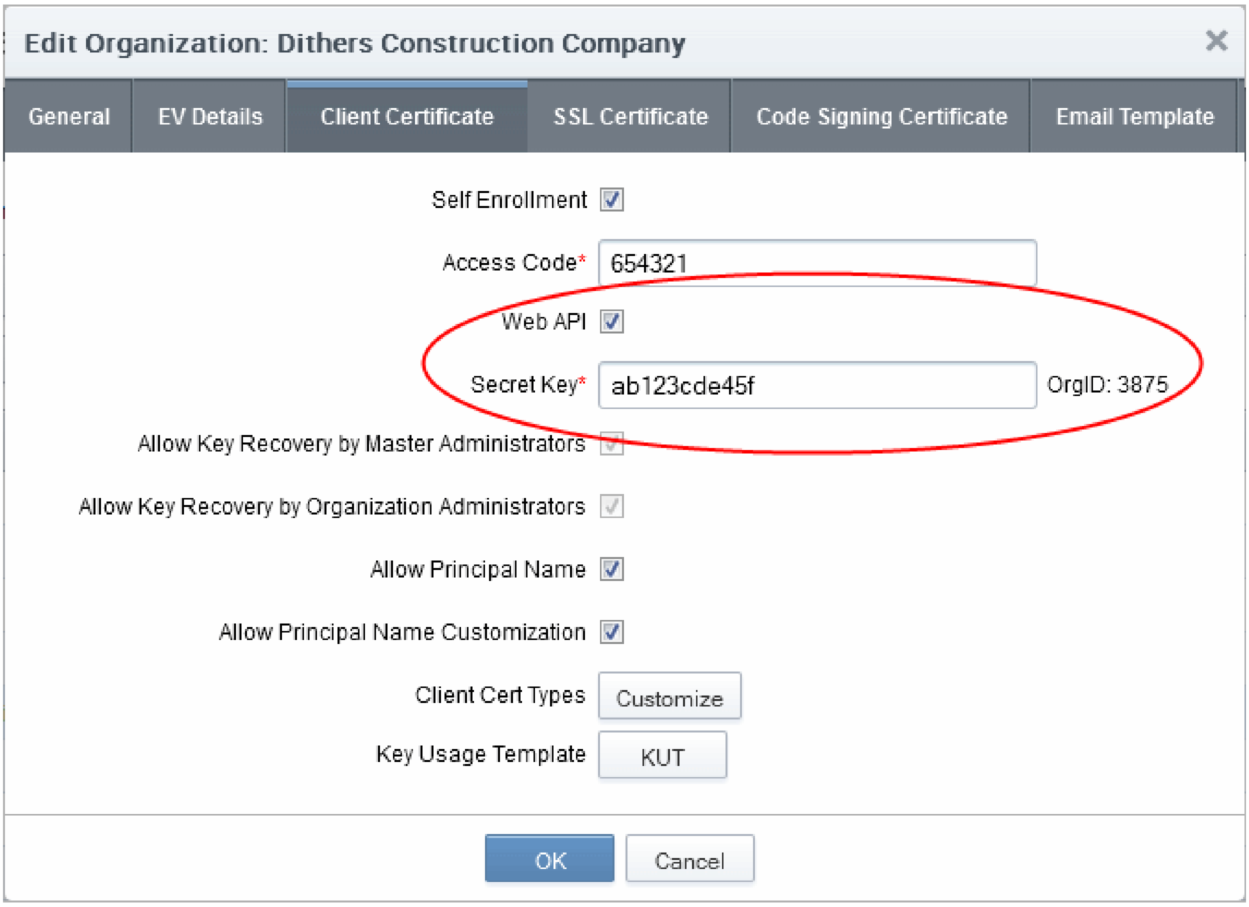
3.2.5.2 Self Enrollment by Secret Identifier

This section explains how to set up a self-enrollment form which uses an organization's secret identifier for authentication. After setup, end-users can use the form to apply for certificates.

3.2.5.2.1 Prerequisites

- The domain from which the client certificate is to be issued has been enabled for S/MIME certificates, has been pre-validated by InCommon and that the domain has been activated by your InCommon 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 InCommon).
  However, if you request a certificate for a brand new domain, then this domain will first have to undergo validation by InCommon. 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 Editing an Existing Organization for more details on adding a domain to an Organization.
- The RAO S/MIME or DRAO S/MIME 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.



Edit Organization: Dithers Construction Company

Self Enrollment ☑

Access Code* 654321

Web API ☑

Secret Key* ab123cde45f OrgID: 3875

Allow Key Recovery by Master Administrators ☑

Allow Key Recovery by Organization Administrators ☑

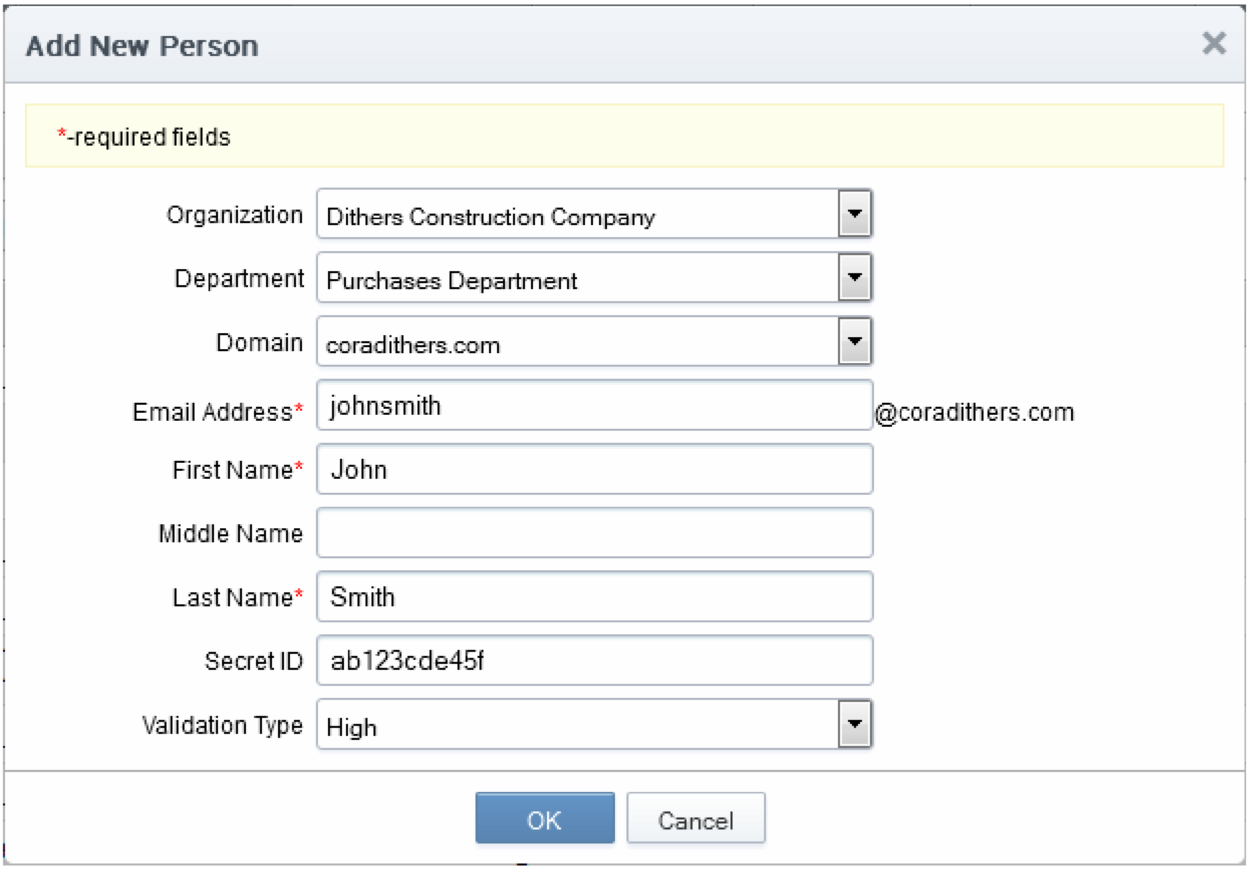
Allow Principal Name ☑

Allow Principal Name Customization ☑

Client Cert Types Customize

Key Usage Template KUT

- 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.



Add New Person

*-required fields

Organization	Dithers Construction Company
Department	Purchases Department
Domain	coradithers.com
Email Address*	johnsmith @coradithers.com
First Name*	John
Middle Name	
Last Name*	Smith
Secret ID	ab123cde45f
Validation Type	High

3.2.5.2.2 Procedure Overview

- Administrator confirms completion of the prerequisite steps.
- Administrator directs the personal certificate applicant to either the 'Secret Identifier' based Self Enrollment Form - makinInitiating the enrollment processg 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 InCommon 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/InCommon/smime?action=enroll&swt=si

2. The secret identifier specified for the end-user.

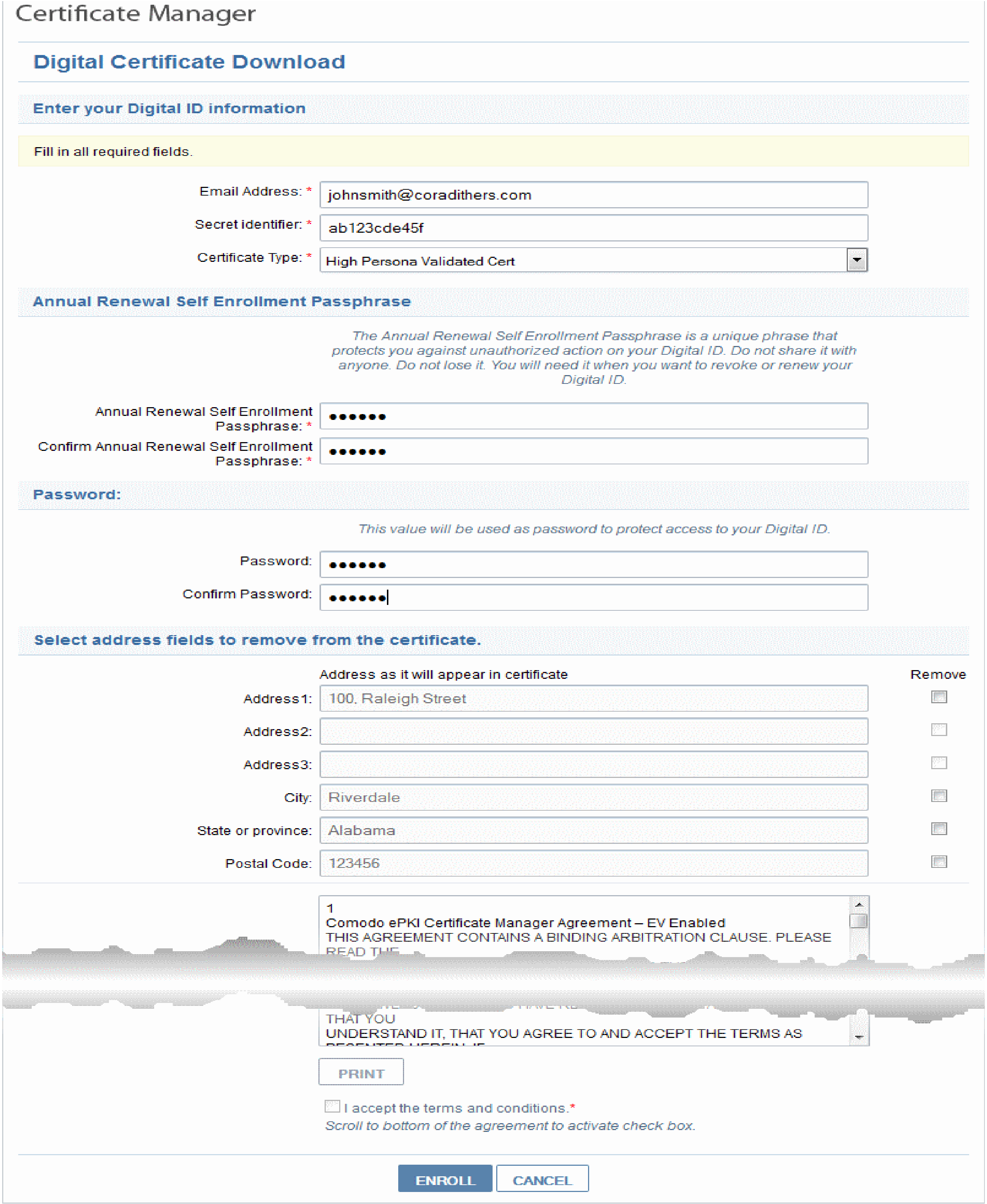
These details can be informed to the applicant by the any preferred out-of-band communication method like email. The end-user can access the form at the given url, fill-in with the necessary details and submit it.

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:



Certificate Manager

Digital Certificate Download

Enter your Digital ID information

Fill in all required fields.

Email Address: *	johnsmith@coradithers.com
Secret identifier: *	ab123cde45f
Certificate Type: *	High Persona Validated Cert ▾

Annual Renewal Self Enrollment Passphrase

The Annual Renewal Self Enrollment Passphrase 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 Self Enrollment Passphrase: *	••••••
Confirm Annual Renewal Self Enrollment Passphrase: *	••••••

Password:

This value will be used as password to protect access to your Digital ID.

Password:	••••••
Confirm Password:	••••••

Select address fields to remove from the certificate.

	Address as it will appear in certificate	Remove
Address1:	100, Raleigh Street	□
Address2:		□
Address3:		□
City:	Riverdale	□
State or province:	Alabama	□
Postal Code:	123456	□

1
Comodo ePKI Certificate Manager Agreement – EV Enabled
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE

THAT YOU
UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS

PRINT

□ I accept the terms and conditions.*
Scroll to bottom of the agreement to activate check box.

ENROLL CANCEL

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. The password should be of at least eight characters.
Select address fields to remove from the certificate	Check boxes	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' check boxes beside the required address fields. Click here for more details.
Eula Acceptance ***(required)***	Check-box	Applicant must accept the terms and conditions before submitting the form.
Enroll	Control	Submits the application and enrolls the applicant for the client certificate.
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 Master Administrator. Contact your Master Administrator if such custom fields are required.

Selecting Address Fields to be Removed from the Certificate

The following address fields...

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

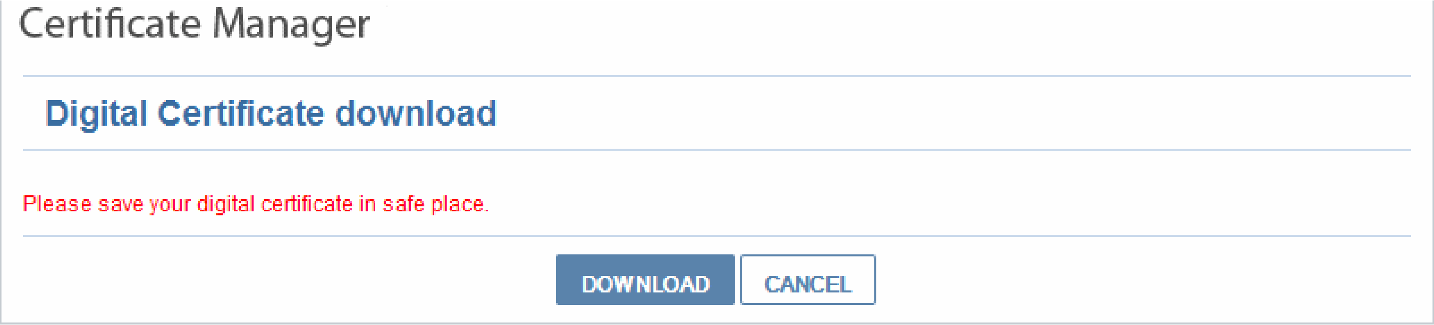
...are automatically populated with the address details of the Organization or Department that the user belongs to. The applicant can choose to remove these details from the client certificate by selecting the 'Remove' check-boxes below beside the corresponding field. The selected details will not be 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 Certificate Collection for more details.

Note: It is possible for CM Account holders to use their own, custom form templates rather than the default form supplied by InCommon. See your InCommon 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.

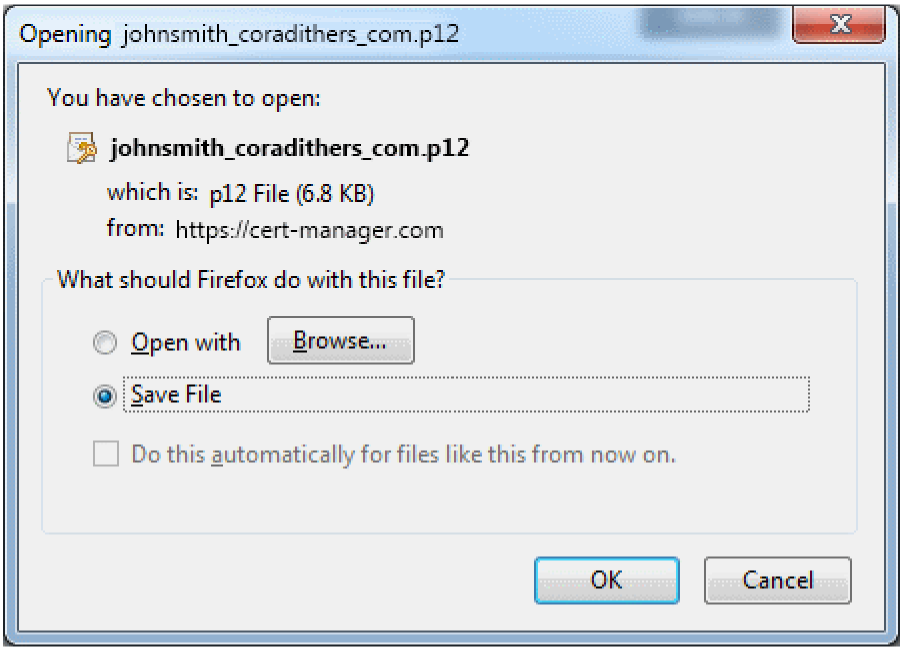


Certificate Manager

Digital Certificate download

Please save your digital certificate in safe place.

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



Opening johnsmith_coradithers_com.p12

You have chosen to open:

johnsmith_coradithers_com.p12

which is: p12 File (6.8 KB)

from: https://cert-manager.com

What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.

CM 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 CM interface and how the end-user can apply for, collect, download and install their certificate.

3.2.5.3.1 Prerequisites

- The domain to which the client certificate is to be issued has:

- Been enabled for S/MIME certificates
- Been validated by Incommon
- Been activated by your Incommon account manager.
  For example, if you wish to issue a client certificate to end-user@mycompany.com, then mycompany.com must have been validated by Incommon.
- If you request a certificate for a new domain, then this domain will have to undergo validation. Once validated, it will be added to your list of pre-validated domains and future certificates will be issued immediately.
- The domain has been delegated to the organization or department. See Editing an Existing Organization for more details on adding a domain to an Organization.
- The RAO S/MIME or DRAO S/MIME administrator has been delegated control of this of this organization or department
- The administrator has added the end-user(s) to the Certificates Management > Client Certificates area of Incommon CM.

3.2.5.3.2 Procedure Overview

Client certificates can be provisioned to employees after the employee has been enrolled into Incommon CM.

Overview of stages:

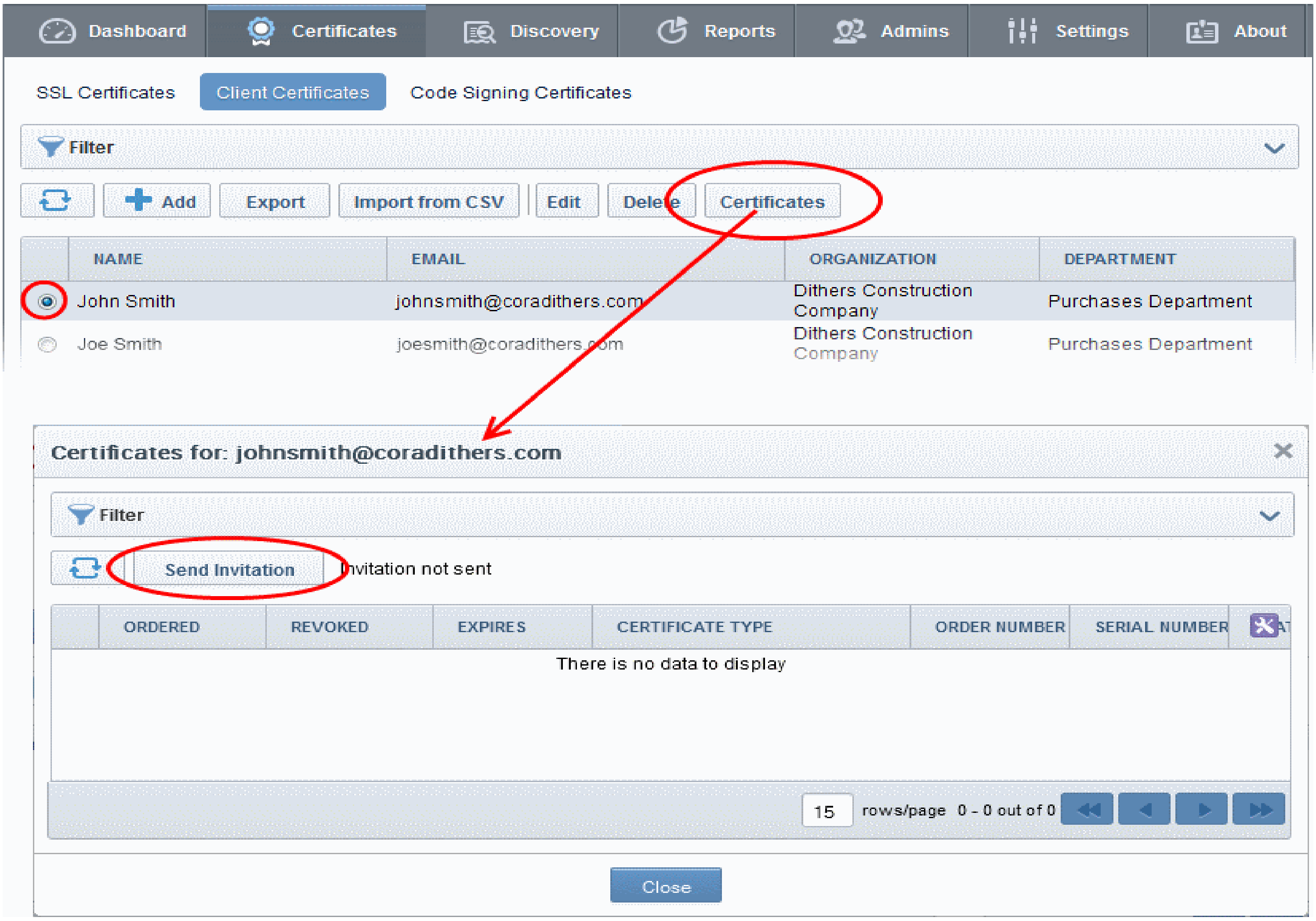
1. Administrator confirms completion of the prerequisite steps.
2. Administrator sends an enrollment invitation to end-users from the Incommon CM interface. See section Initiating the Enrollment Process.
3. The invitation mail contains a link to the user registration form. See Validation of the Email Address for more details.
4. The end-user completes the registration form. The certificate request is sent to Incommon CA servers. If the registration is successful, the end-user will be able to download and install their personal certificate. See Certificate Collection.

3.2.5.3.3 Initiate 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).



	NAME	EMAIL	ORGANIZATION	DEPARTMENT
●	John Smith	johnsmith@coradithers.com	Dithers Construction Company	Purchases Department
○	Joe Smith	joesmith@coradithers.com	Dithers Construction Company	Purchases Department

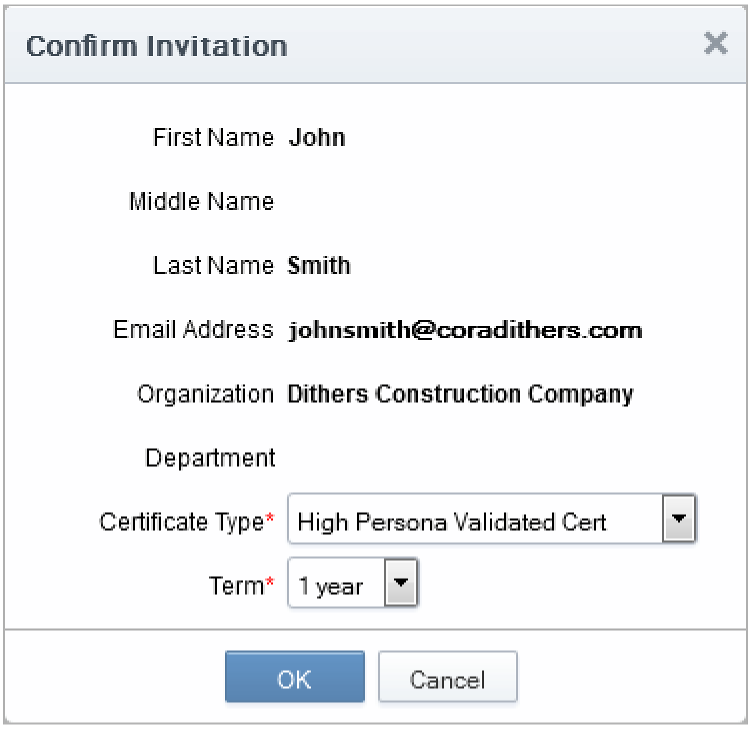
Certificates for: johnsmith@coradithers.com

Invitation not sent

ORDERED	REVOKED	EXPIRES	CERTIFICATE TYPE	ORDER NUMBER	SERIAL NUMBER

There is no data to display

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



Confirm Invitation

First Name John

Middle Name

Last Name Smith

Email Address johnsmith@coradithers.com

Organization Dithers Construction Company

Department

Certificate Type* High Persona Validated Cert

Term* 1 year

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.

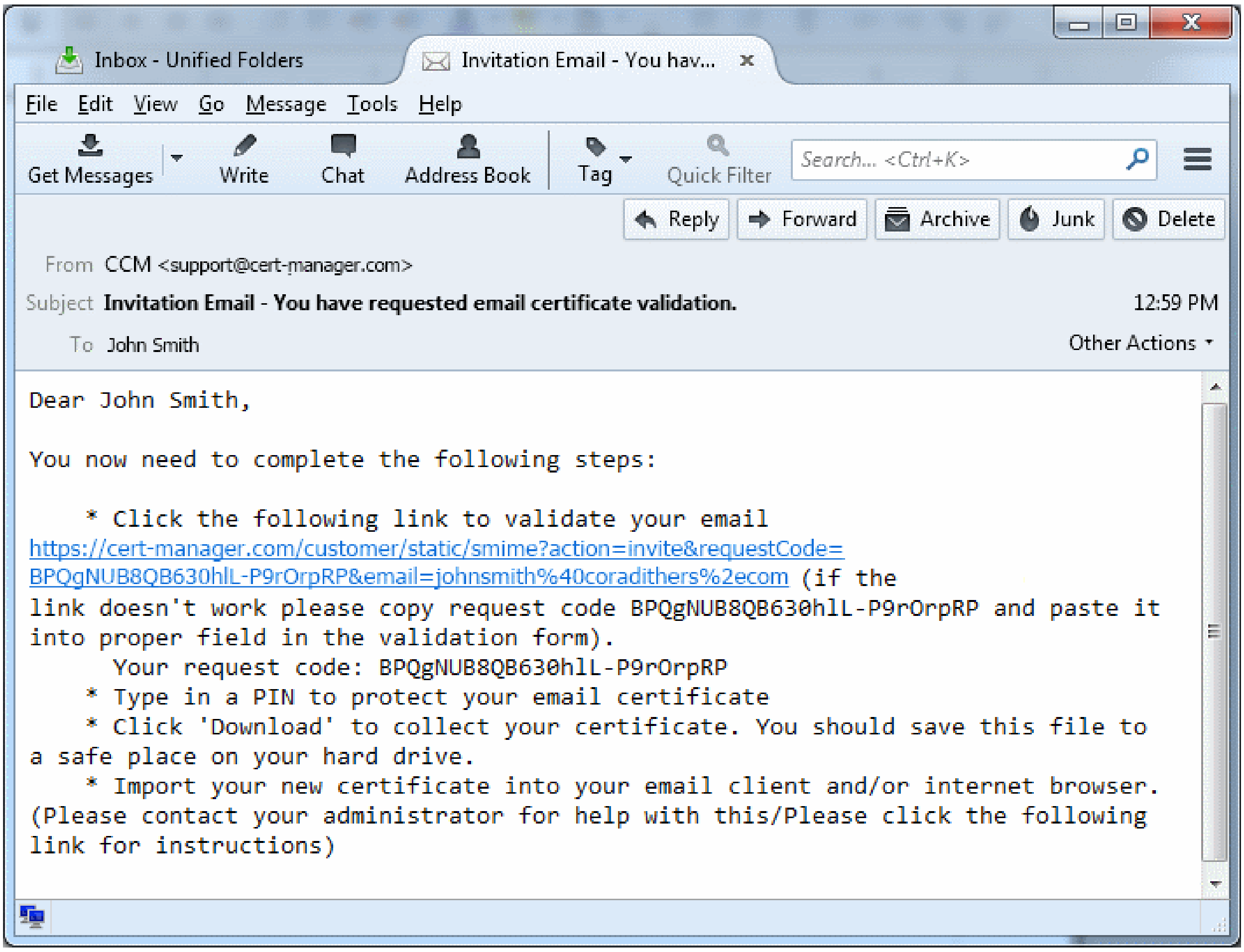
- Upon clicking 'OK', an invitation email will be sent to the end-user.

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 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.



From CCM <support@cert-manager.com>

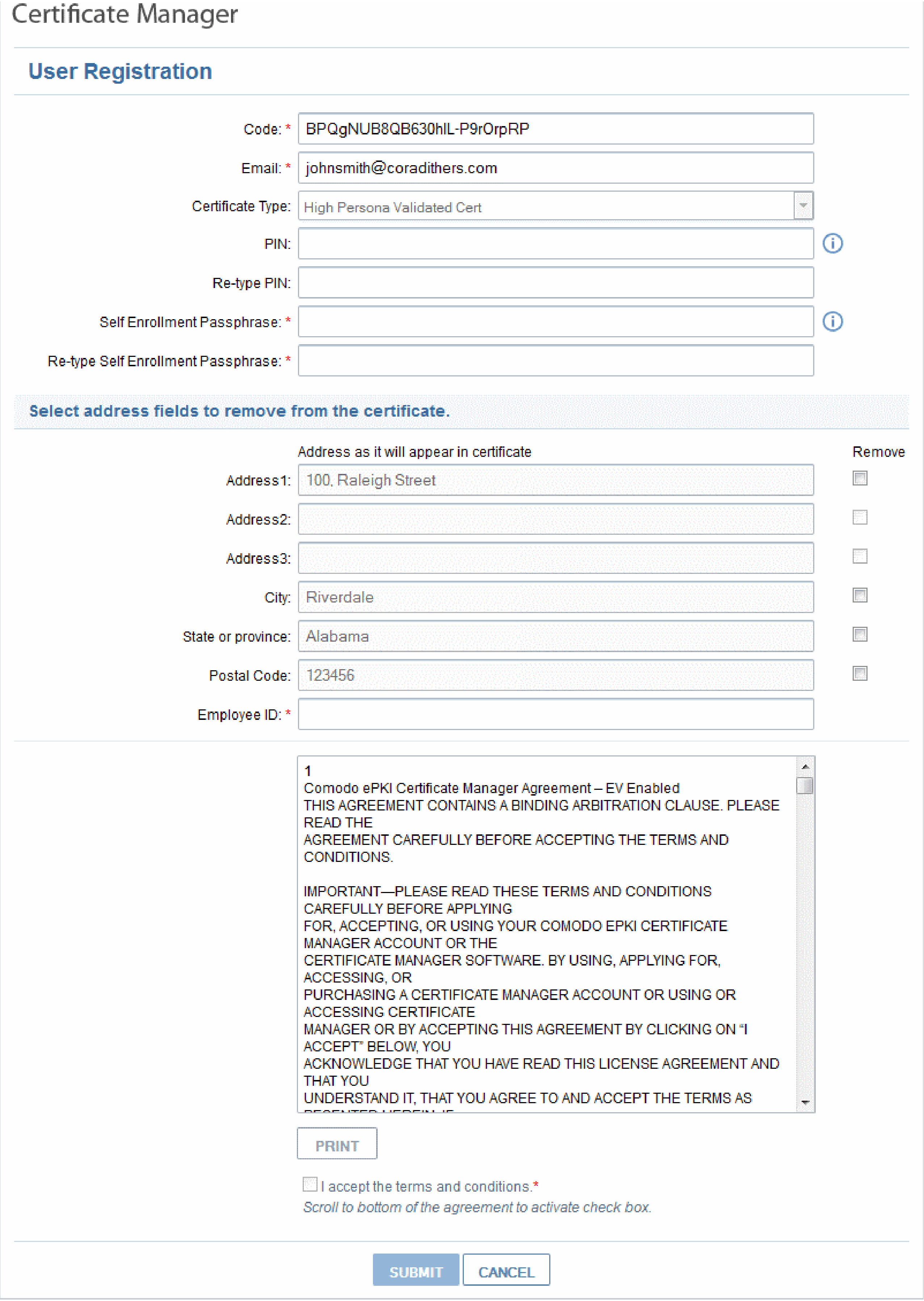
Subject **Invitation Email - You have requested email certificate validation.** 12:59 PM

To John Smith

```
Dear John Smith,

You now need to complete the following steps:

    * Click the following link to validate your email
https://cert-manager.com/customer/static/smime?action=invite&requestCode=
BPQgNUB8QB630hlL-P9rOrpRP&email=johnsmith%40coradithers%2ecom (if the
link doesn't work please copy request code BPQgNUB8QB630hlL-P9rOrpRP and paste it
into proper field in the validation form).
      Your request code: BPQgNUB8QB630hlL-P9rOrpRP
    * Type in a PIN to protect your email certificate
    * Click 'Download' to collect your certificate. You should save this file to
a safe place on your hard drive.
    * Import your new certificate into your email client and/or internet browser.
(Please contact your administrator for help with this/Please click the following
link for instructions)
```

Note: It is possible for administrators to modify the contents of these emails in the 'Email Templates area under Organizations > Edit.

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



Certificate Manager

User Registration

Code: * BPQgNUB8QB630hlL-P9rOrpRP

Email: * johnsmith@coradithers.com

Certificate Type: High Persona Validated Cert

PIN:

Re-type PIN:

Self Enrollment Passphrase: *

Re-type Self Enrollment Passphrase: *

Select address fields to remove from the certificate.

	Address as it will appear in certificate	Remove
Address1:	100, Raleigh Street	□
Address2:		□
Address3:		□
City:	Riverdale	□
State or province:	Alabama	□
Postal Code:	123456	□
Employee ID: *		

1
Comodo ePKI Certificate Manager Agreement – EV Enabled
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE
READ THE
AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND
CONDITIONS.

IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS
CAREFULLY BEFORE APPLYING
FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE
MANAGER ACCOUNT OR THE
CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR,
ACCESSING, OR
PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR
ACCESSING CERTIFICATE
MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I
ACCEPT" BELOW, YOU
ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND
THAT YOU
UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS

□ I accept the terms and conditions.*

Scroll to bottom of the agreement to activate check box.

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.
Email ***(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)***	Check boxes	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' check boxes beside the required address fields. Click here for more details.
EULA Acceptance ***(required)***	Check box	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

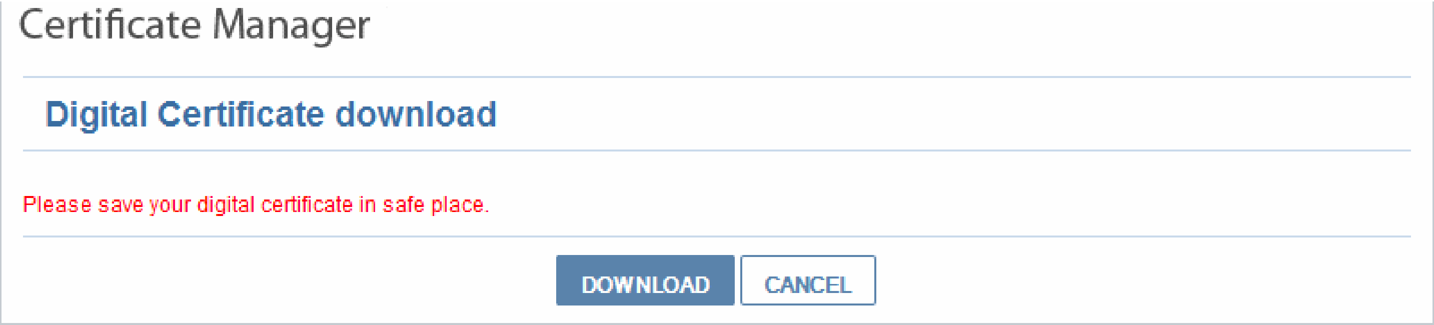
The following address fields:

- 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' check-boxes 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.

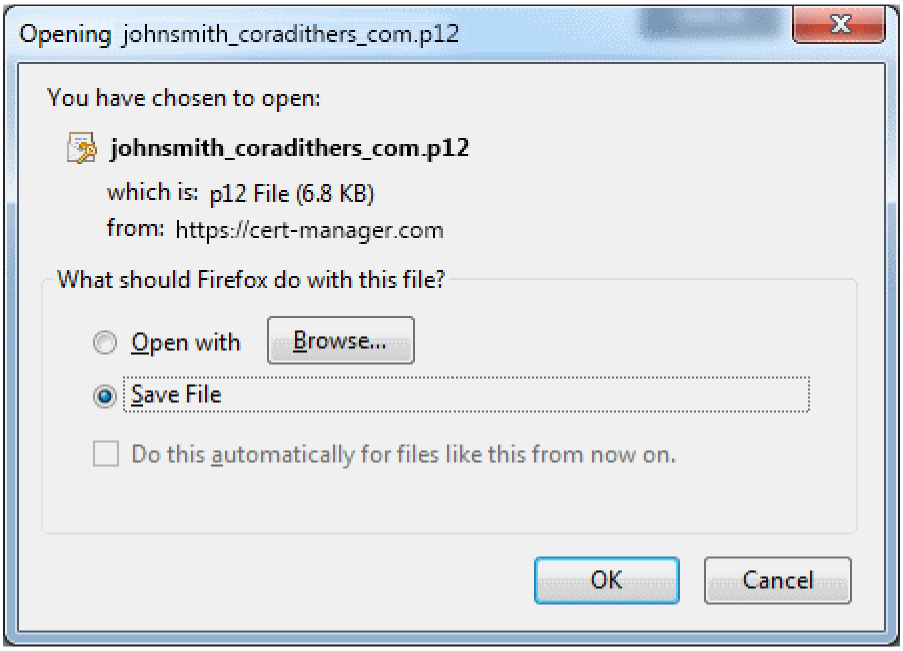


Certificate Manager

Digital Certificate download

Please save your digital certificate in safe place.

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



Opening johnsmith_coradithers_com.p12

You have chosen to open:

johnsmith_coradithers_com.p12

which is: p12 File (6.8 KB)

from: https://cert-manager.com

What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.

CM 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 in 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 'Certificates' Dialog for more details;
- The end-user can directly revoke their client certificate. See Revocation of Client Certificates by End-Users for more details.

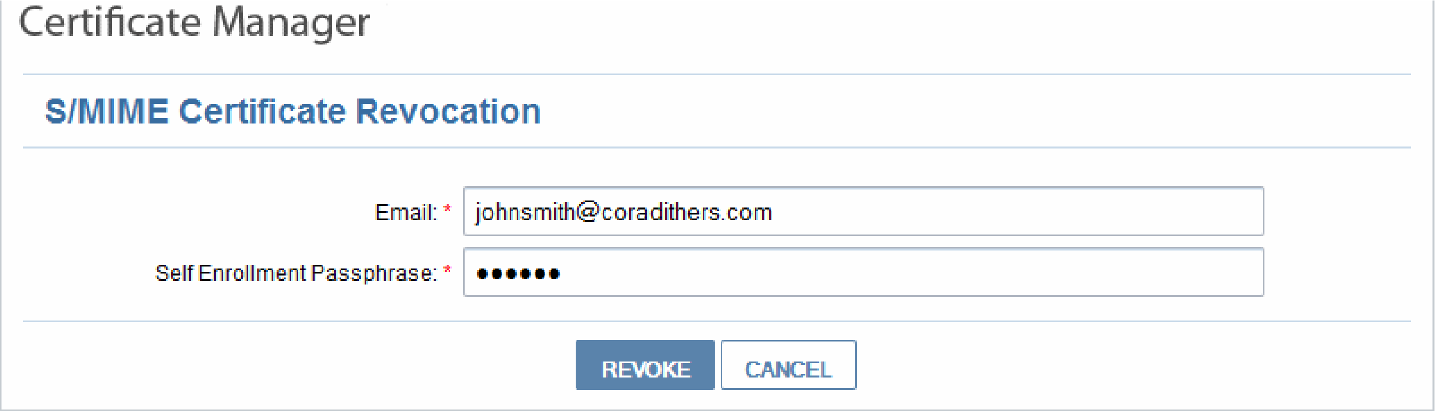
3.2.6.1 Revocation of Client Certificates by End Users

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/InCommon/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. Administrator directs the end-user to the revocation interface hosted at https://cert-manager.com/customer/Comodo/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



Certificate Manager

S/MIME Certificate Revocation

Email: * johnsmith@coradithers.com

Self Enrollment Passphrase: * ●●●●●●

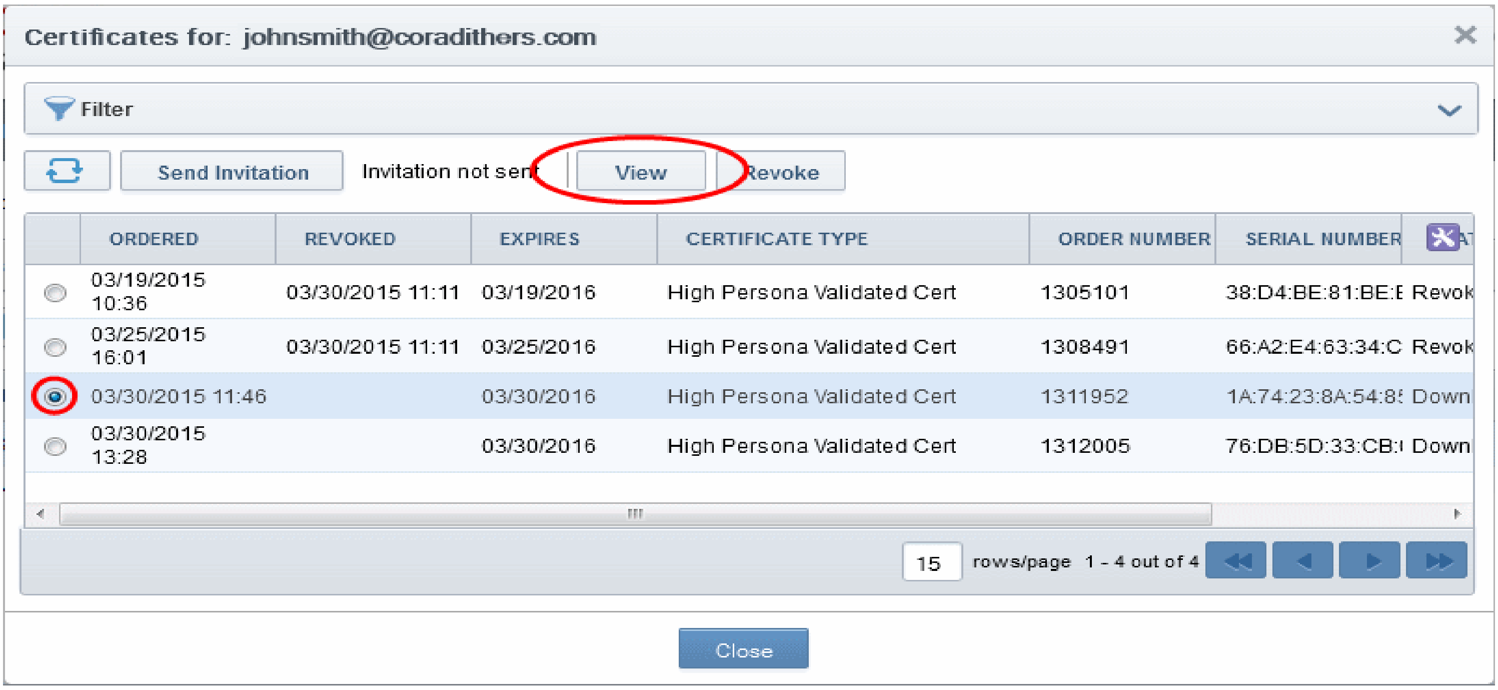
3.2.6.1.3 Form Parameters

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.
Revoke	Control	Revokes the certificate
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.

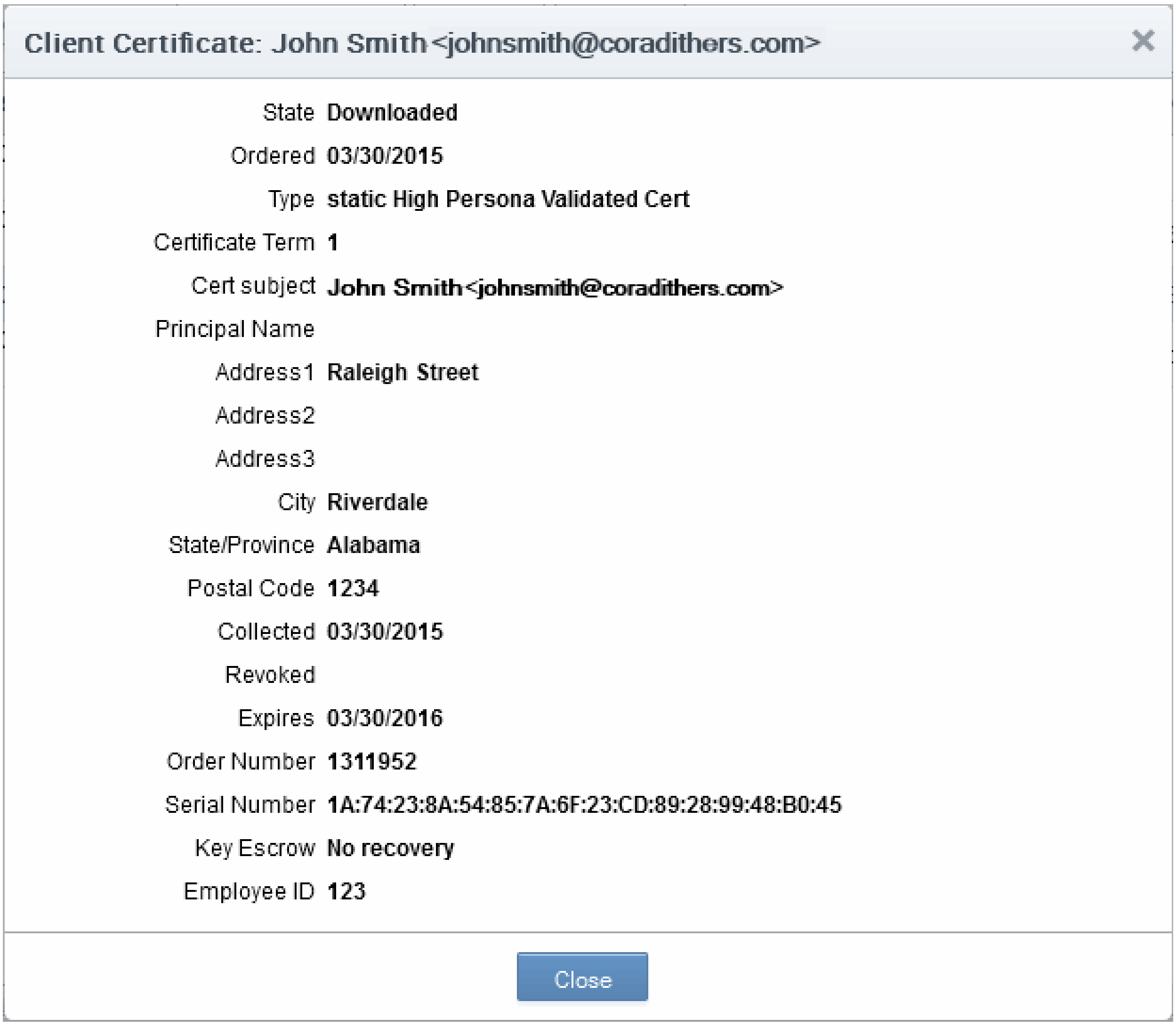
Selecting the person whose certificate is to be viewed and clicking the 'Certs' button at the top will open the 'Certificates for...' dialog.



Certificates for: johnsmith@coradithers.com

	ORDERED	REVOKED	EXPIRES	CERTIFICATE TYPE	ORDER NUMBER	SERIAL NUMBER	
○	03/19/2015 10:36	03/30/2015 11:11	03/19/2016	High Persona Validated Cert	1305101	38:D4:BE:81:BE:E	Revok
○	03/25/2015 16:01	03/30/2015 11:11	03/25/2016	High Persona Validated Cert	1308491	66:A2:E4:63:34:C	Revok
●	03/30/2015 11:46		03/30/2016	High Persona Validated Cert	1311952	1A:74:23:8A:54:8!	Down
○	03/30/2015 13:28		03/30/2016	High Persona Validated Cert	1312005	76:DB:5D:33:CB:!	Down

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



Client Certificate: John Smith <johnsmith@coradithers.com>

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

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 InCommon Certificate Manager to CA.
Type	Text Field	Type of the client certificate, prefixed with the customer name.
Certificate Term		The life term of the certificate
Cert subject		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 CM 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.

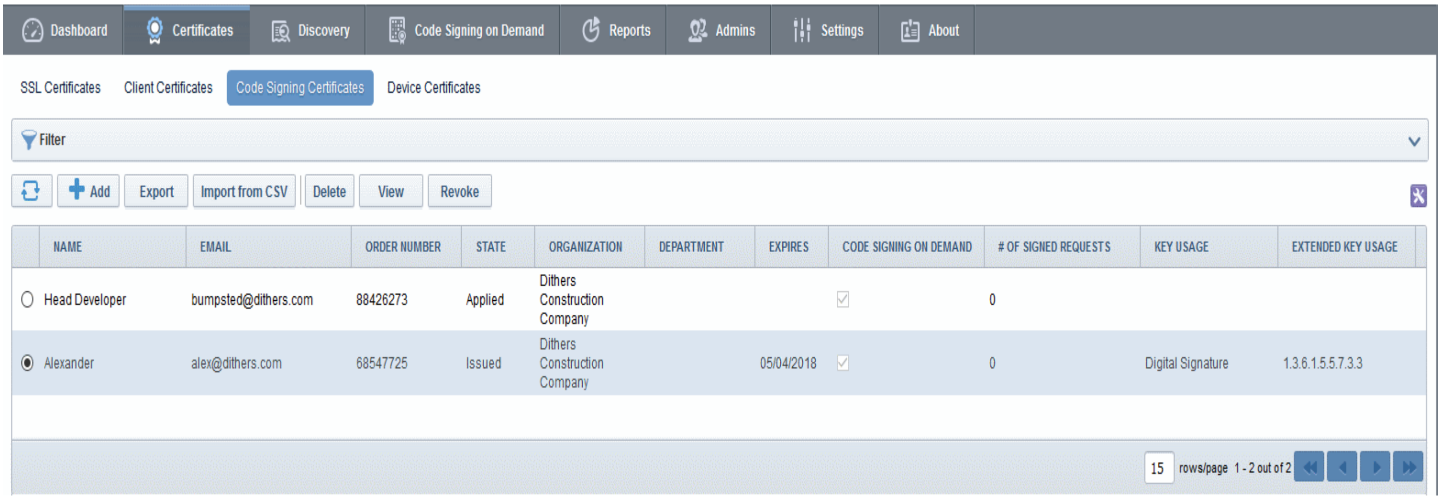
3.3 The Code Sign Certificates Area

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 or department.

Visibility of the 'Code Signing Certificates' area is restricted to:

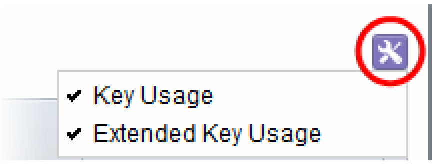
- RAO Code Signing administrators - can view the code signing certificates and their applicants of Organizations (and any subordinate Departments) that have been delegated to them.
- DRAO Code Signing administrators - can view the code signing certificates and their end-users of Departments that have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

Note: Incommon also offer the ability for companies to simplify the code signing process using our Code Signing on Demand service. The service, available in both hosted and cloud versions, can sign .EXE, .DLL, .CAB, .MSI, .JS, .VBS, .PS1, .OCX, .SYS, .WSF, .CAT, .MSP, .CPL, .EFI. formats. Please contact your Master Administrator/Incommon Account Manager if you wish to enable this feature.



	NAME	EMAIL	ORDER NUMBER	STATE	ORGANIZATION	DEPARTMENT	EXPIRES	CODE SIGNING ON DEMAND	# OF SIGNED REQUESTS	KEY USAGE	EXTENDED KEY USAGE
○	Head Developer	bumpsted@dithers.com	88426273	Applied	Dithers Construction Company			✓	0		
●	Alexander	alex@dithers.com	68547725	Issued	Dithers Construction Company		05/04/2018	✓	0	Digital Signature	1.3.6.1.5.5.7.3.3

Code Sign Certificates area - Table of Parameters		
Field Name		**Description**
Name		The name of the applicant.
Email		The email address of the applicant.
Order Number		Order number of the certificate request made to CA.

Code Sign Certificates area - Table of Parameters		
Field Name		**Description**
State		Which stage the certificate is at in the certificate issuance process.
	Init	Applies only to certificates added to the Code Signing on Demand (CSoD) service. Indicates that the certificate issuance process has been initiated by the agent.
	Invited	The applicant has been sent an invitation email by the administrator.
	Requested	A request for the certificate 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 the CA and collected by InCommon CM, but has not yet been downloaded by the applicant. For the certificates issued for CSoD, the agent will automatically download the certificate.
	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 its 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.
Code Signing on Demand		Indicates whether the certificate is enrolled for CSoD service or not. Note: This column is displayed only if Code Signing on Demand is enabled for your account.
# of Signed Requests		Number of files signed with the certificate. Only applies to certificates generated by the CSoD service.
Key Usage		Primary purposes of the certificate. Purposes include digital signing, encryption and more.
Extended Key Usage		Other purposes that the certificate can be used for.
Note: You can enable/disable columns by clicking the button on the right of the column headers:  ✔ Key Usage ✔ Extended Key Usage		
Control Buttons	Add	Apply for a new code signing certificate. You will need to specify a user for the certificate as part of the application.
	Export	Save the list of code signing certificates in CSV format

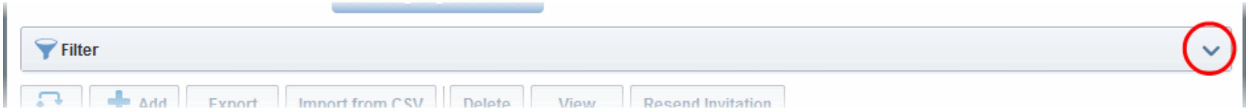
Code Sign Certificates area - Table of Parameters

Field Name		Description
	Import from CSV	Import a list of code signing certificates into InCommon 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 depend on the state of the selected certificate	View	View certificate details (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 allowing them to request their certificate)
	Revoke	Revokes the certificate.
	Delete	Removes the certificate

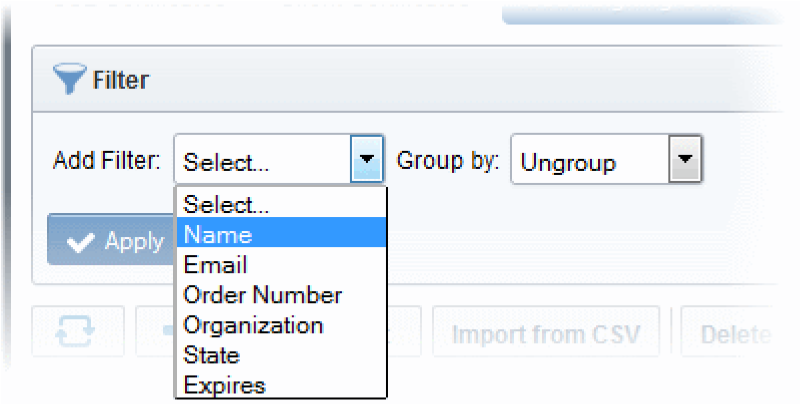
3.3.1 Sorting and Filtering Options

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

Administrators can search for particular code signing certificate by using filters.

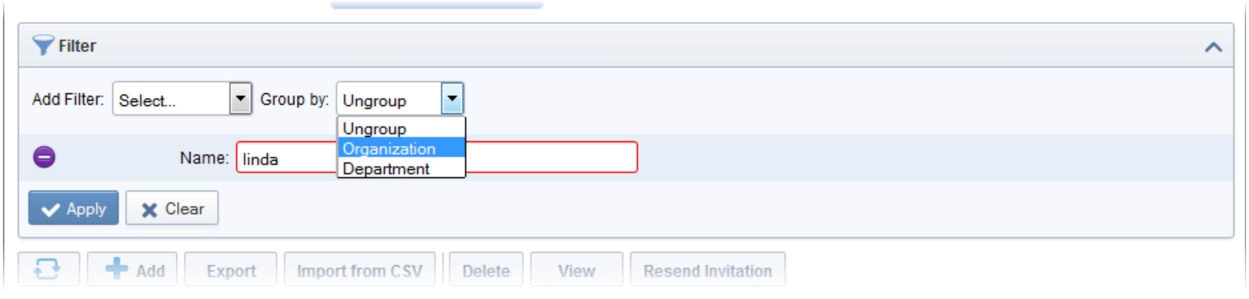


To apply filters, click on the down arrow at the right end of the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.



For example, if you want to 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.

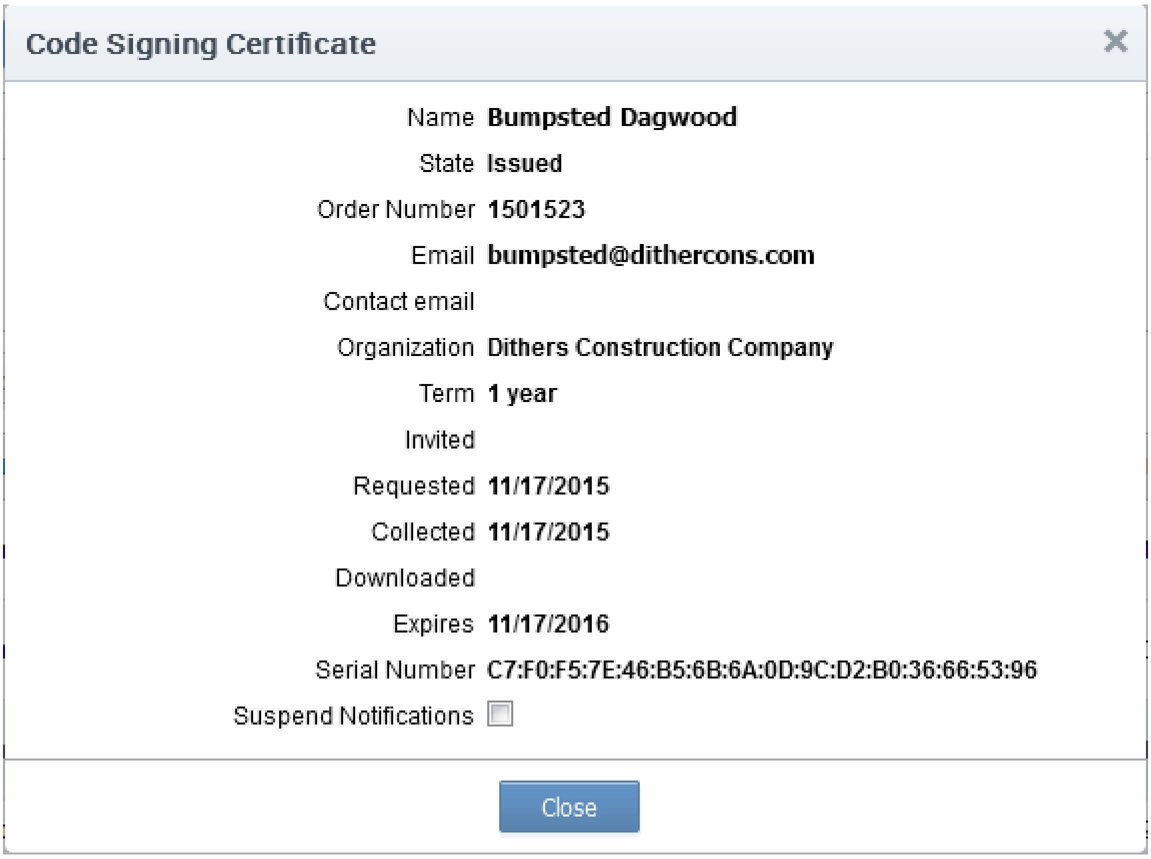
The filtered items based on the entered parameters will be displayed.

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

Select a code-signing certificate then click the 'View' button to view that certificate's details:



Code Signing Certificate

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

Code Sign Certificate 'View' Dialog - Table of Parameters		
Form Element	**Type**	**Description**
Name	Text Field	The 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 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.
Order Number	Numeric	Order number of the certificate request made to CA.
Email	Text Field	The email address of the applicant.

Code Sign Certificate 'View' Dialog - Table of Parameters		
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 applicant 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 InCommon CM to CA.
Collected	Numeric	Date of the collection of certificate by InCommon CM 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

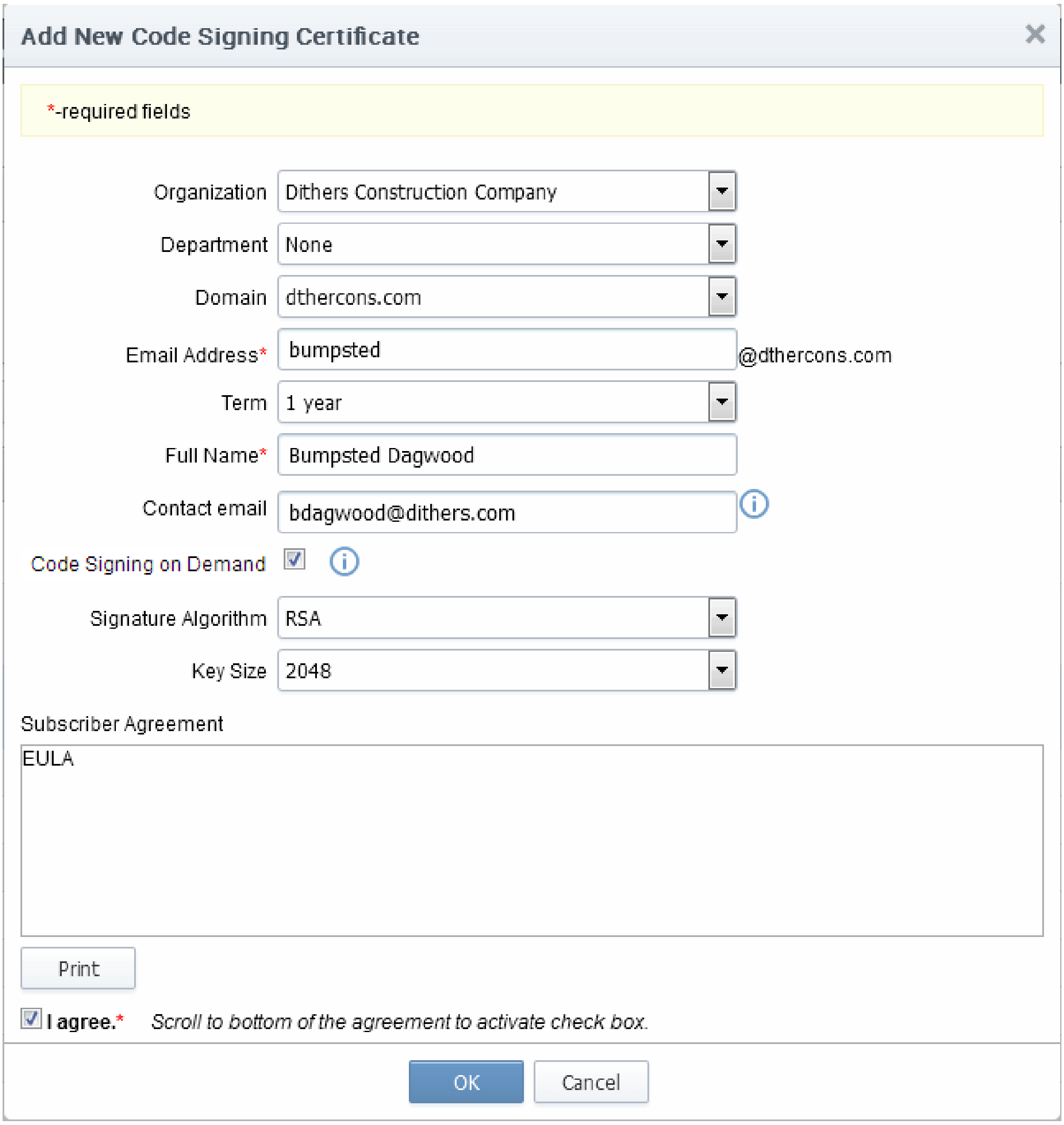
There are several methods of adding certificates to the Code Sign Certificates area of Certificate Manager.

- 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 Add Certificates

You can add code signing certificates for both 'Code Signing on Demand' (CSoD) and manual signing:

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



Add New Code Signing Certificate

*-required fields

Organization	Dithers Construction Company
Department	None
Domain	dthercons.com
Email Address*	bumpsted @dthercons.com
Term	1 year
Full Name*	Bumpsted Dagwood
Contact email	bdagwood@dithers.com
Code Signing on Demand	☑
Signature Algorithm	RSA
Key Size	2048

Subscriber Agreement

EULA

☑ I agree.* *Scroll to bottom of the agreement to activate check box.*

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.
Code Signing on Demand	Checkbox	The certificate will be issued to a developer for use in the 'Code Signing on Demand' service (CSoD). Prerequisites: • The code signing on demand service has been setup for your account. • You have added a 'Developer' role to Incommon CM. See Code Signing on Demand, for more details.
Signature Algorithm	Drop-down	• Appears only if 'Code Signing on Demand' is selected. • Choose the signature algorithm to be used by the certificate.
Keysize	Drop-down	• Appears only if 'Code Signing on Demand' is selected. • Choose the key-size (in bits) of the certificate.
Subscriber Agreement	Text field	• Appears only if 'Code Signing on Demand' is selected. • Displays the End-User License Agreement (EULA) for the certificate. Read through the EULA and accept to it by selecting the 'I agree' checkbox for the application to proceed.

- 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 CM. 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 Incommon 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 automatically to new users to initiate the self enrollment process. See 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 CM 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 CM, 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"

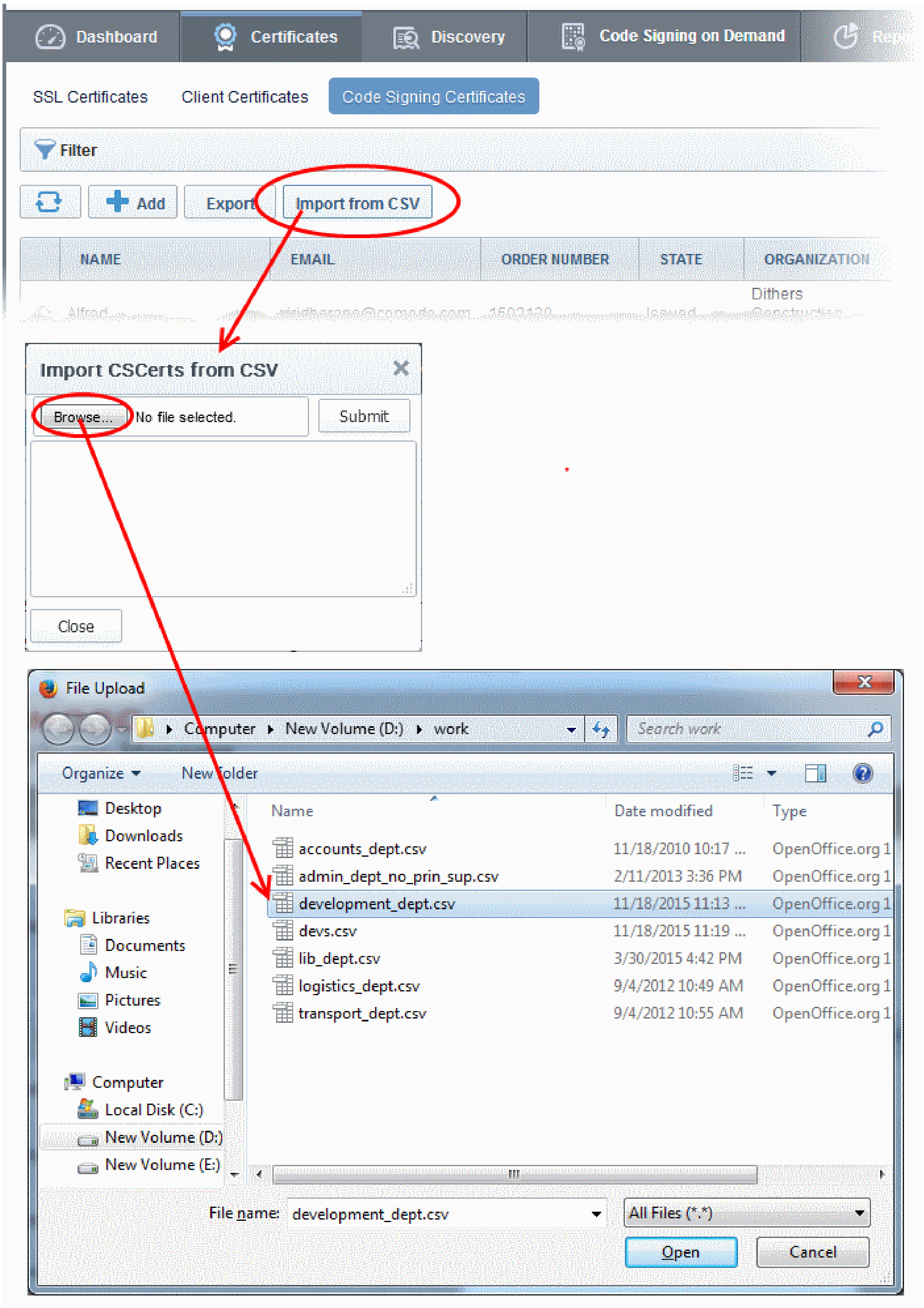
  The following table explains the requirements and formats of the values.

Values	Organization	Department	Term	E-Mail 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 year","john_s@example.com","JOHNSMITH","jsmith@alternativeemail.com"

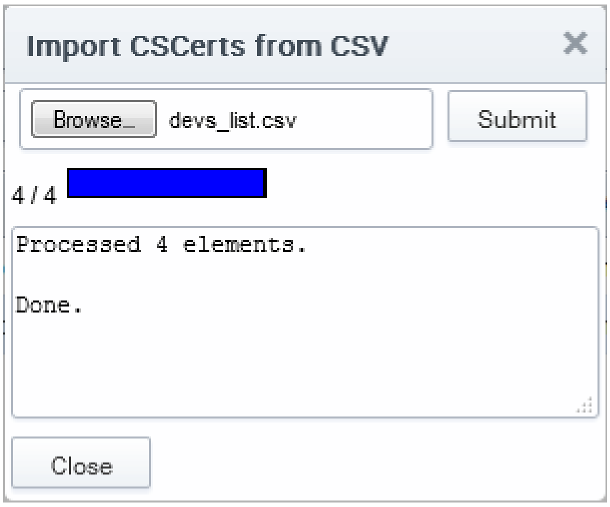
In order to do load the .csv file to CM, click on 'Import from CSV' in 'Certificates Management' > 'Code Sign Certificates' interface. A File Upload dialog will appear. Click the 'Browse' button, and navigate to the .csv file, and click on 'Submit'.



Name	Date modified	Type
accounts_dept.csv	11/18/2010 10:17 ...	OpenOffice.org 1
admin_dept_no_prin_sup.csv	2/11/2013 3:36 PM	OpenOffice.org 1
development_dept.csv	11/18/2015 11:13 ...	OpenOffice.org 1
devs.csv	11/18/2015 11:19 ...	OpenOffice.org 1
lib_dept.csv	3/30/2015 4:42 PM	OpenOffice.org 1
logistics_dept.csv	9/4/2012 10:49 AM	OpenOffice.org 1
transport_dept.csv	9/4/2012 10:55 AM	OpenOffice.org 1

File name: development_dept.csv

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.



devs_list.csv

4 / 4

```
Processed 4 elements.

Done.
```

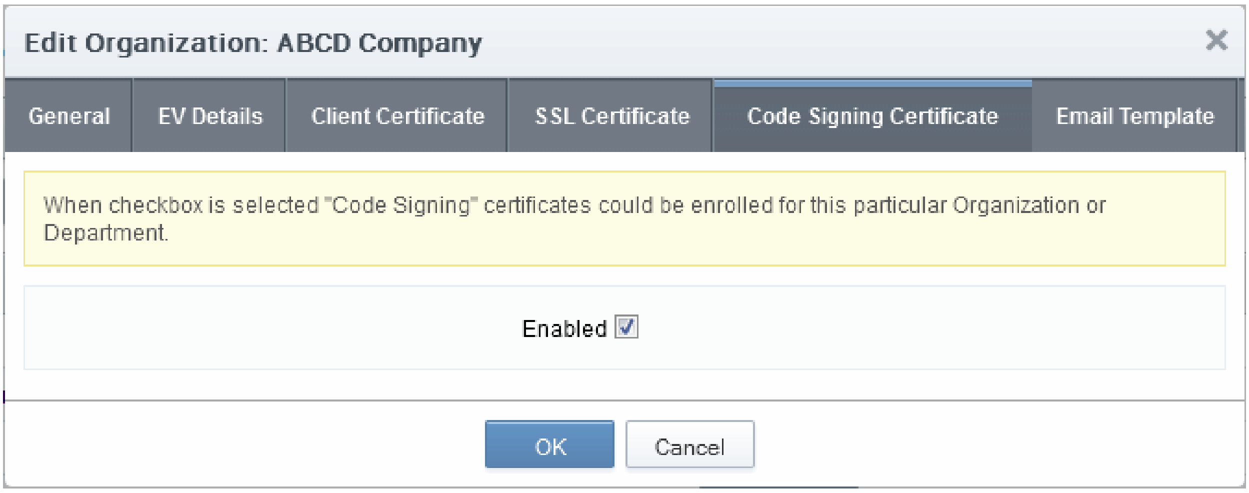
3.3.3.3 Auto Creation of End-Users by Initiating Self Enrollment

Certificates issued to end-users by the self enrollment process 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 InCommon CA and that the domain has been made activate by your InCommon 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 InCommon.) 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 InCommon CA. 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 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 delegated RAO administrator has **enabled Code Signing Certificates for the Organization** by selecting the 'Enabled' check box in the 'Code Signing tab' of the 'Add New/Edit' Organizations dialog box (see screen-shot below)



Edit Organization: ABCD Company

When checkbox is selected "Code Signing" certificates could be enrolled for this particular Organization or Department.

Enabled ☑

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

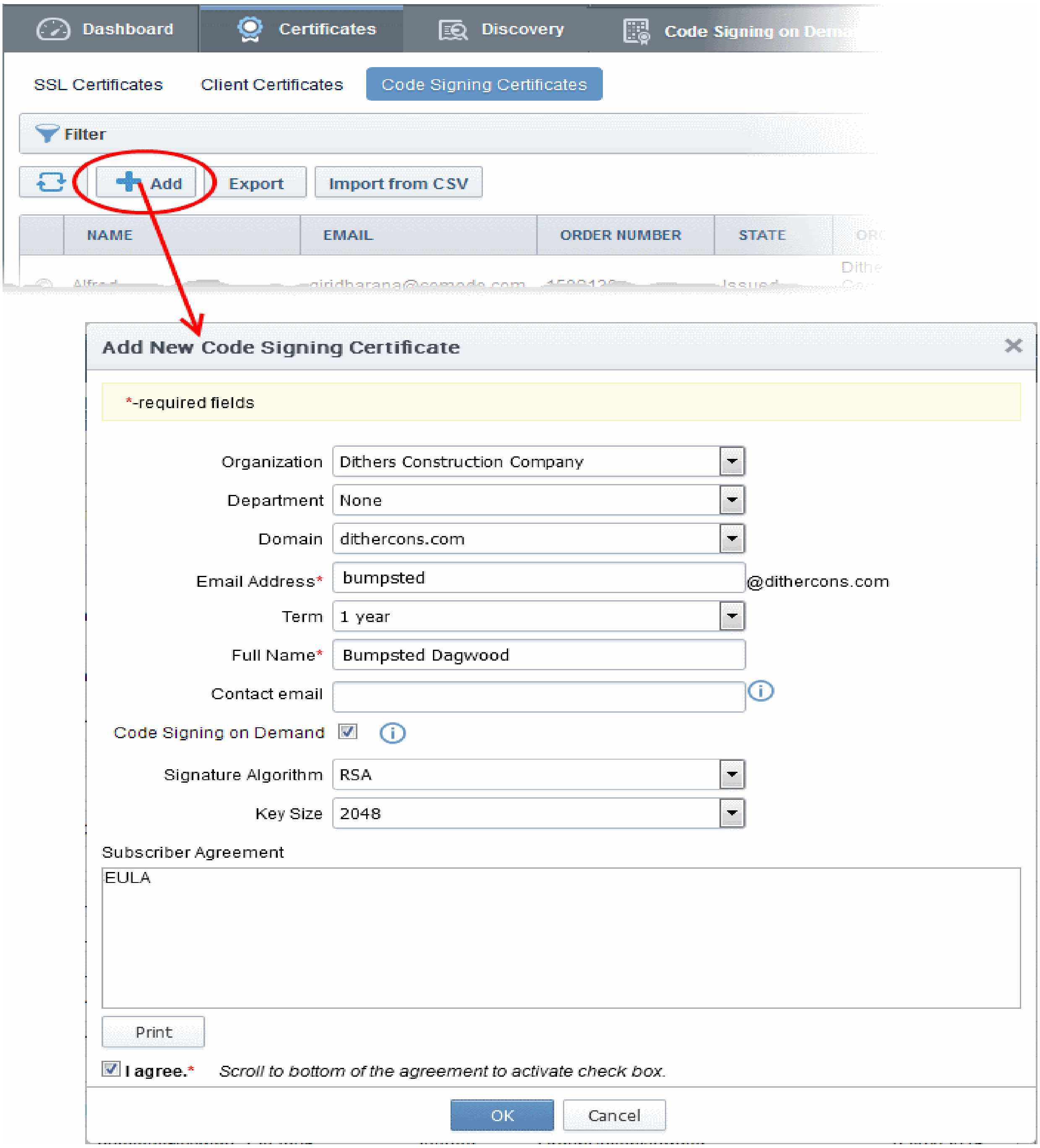
1. The delegated RAO or DRAO Administrator completes the prerequisite steps.
2. Administrator sends an invite email to the end-user which contains links to begin the enrollment process.
3. End-user validates their email address then completes the online application form for the certificate.
4. The certificate request is sent to InCommon CA servers by InCommon CM.
5. If the application is successful, InCommon CM sends an email with a certificate download link to the end-user
6. The certificate will be added to the end-user account in InCommon CM and can be managed from the 'Code Sign Certificates' area.

3.3.4.3 Initiating the Enrollment Process

After completing the prerequisite steps, the next step is to send an email to your end-users which allows them to start the certificate enrollment process.

To send the invitation mail:

- Open the 'Code Sign Certificates' area then click the 'Add' button.
- This will open 'Add New Code Signing Certificate' dialog:



Add New Code Signing Certificate

*-required fields

Organization	Dithers Construction Company
Department	None
Domain	dithercons.com
Email Address*	bumpsted @dithercons.com
Term	1 year
Full Name*	Bumpsted Dagwood
Contact email	
Code Signing on Demand	☑
Signature Algorithm	RSA
Key Size	2048

Subscriber Agreement

EULA

☑ I agree.* *Scroll to bottom of the agreement to activate check box.*

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.
Code Signing on Demand	Check-box	Allow the certificate to be used by the CSoD service. See Obtain a Code-Signing Certificate for CSoD for more details.

Fields marked with a * are mandatory.

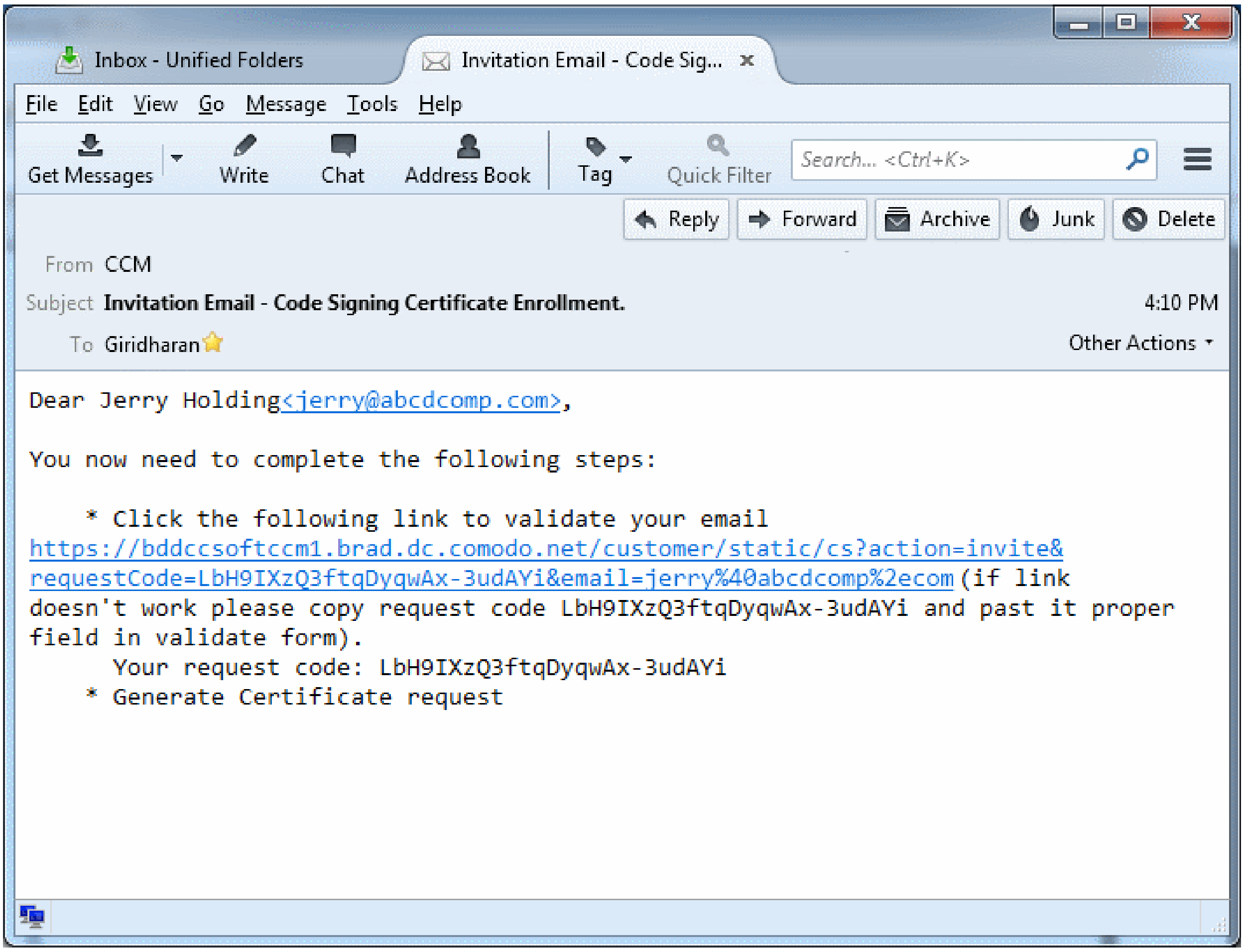
- Complete the necessary details and click 'OK'.

An invitation email will be automatically sent to the applicant. The certificate status will change to 'INVITED' in the 'Code Signing Certificates' area of CM.

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.

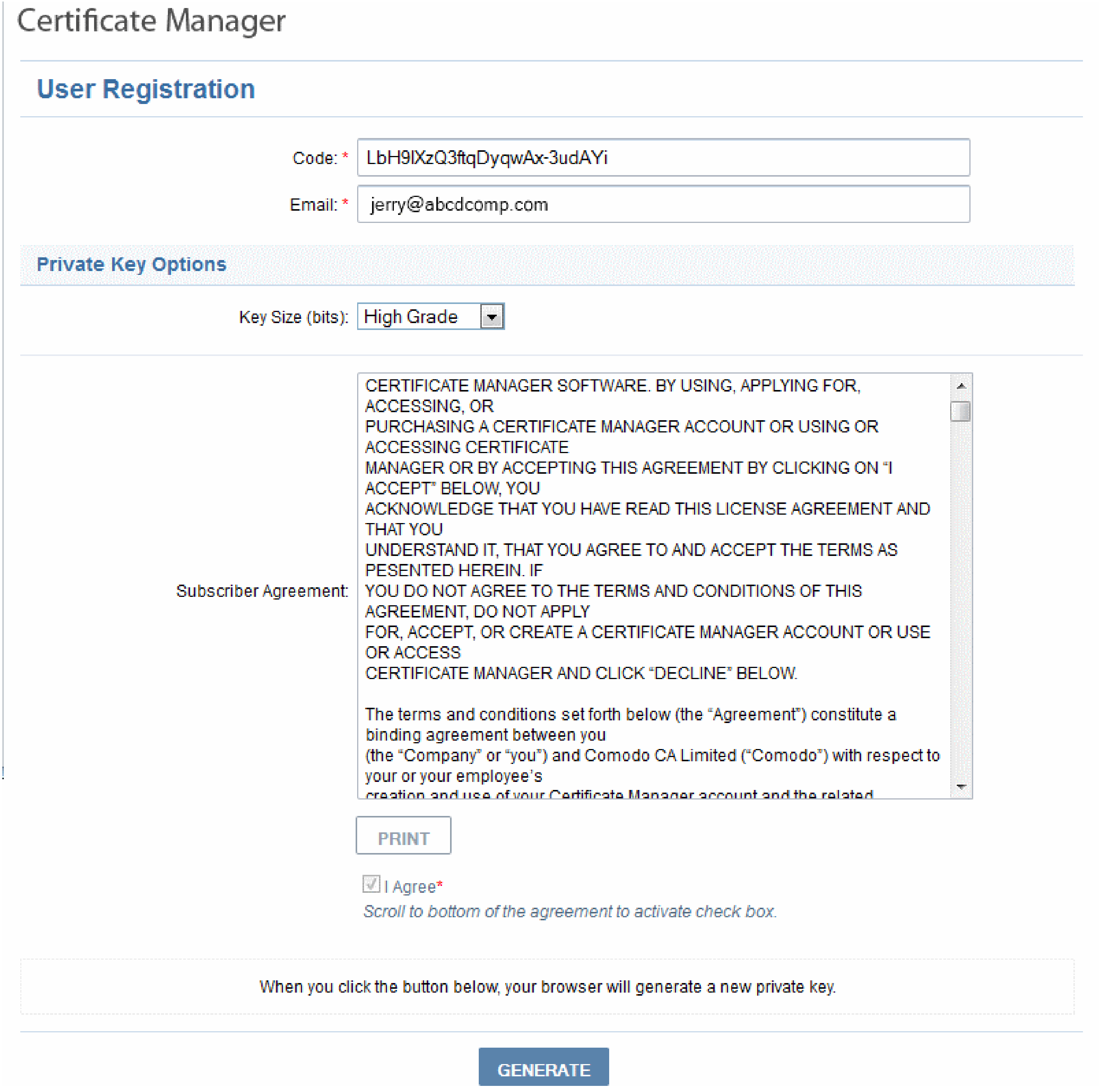


From CCM
Subject **Invitation Email - Code Signing Certificate Enrollment.** 4:10 PM
To Giridharan

```
Dear Jerry Holding<jerry@abcdcomp.com>,

You now need to complete the following steps:

    * Click the following link to validate your email
https://bddccsoftccm1.brad.dc.comodo.net/customer/static/cs?action=invite&
requestCode=LbH9IXzQ3ftqDyqwAx-3udAYi&email=jerry%40abcdcomp%2ecom (if link
doesn't work please copy request code LbH9IXzQ3ftqDyqwAx-3udAYi and past it proper
field in validate form).
      Your request code: LbH9IXzQ3ftqDyqwAx-3udAYi
    * Generate Certificate request
```

Note: It is possible for administrators to modify the contents of these emails in the 'Email Templates' area under Organization > Edit.

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



Certificate Manager

User Registration

Code: * LbH9lXzQ3ftqDyqwAx-3udAYi

Email: * jerry@abcdcomp.com

Private Key Options

Key Size (bits): High Grade

Subscriber Agreement:

CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR, ACCESSING, OR PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR ACCESSING CERTIFICATE MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND THAT YOU UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS PESENTED HEREIN. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR CREATE A CERTIFICATE MANAGER ACCOUNT OR USE OR ACCESS CERTIFICATE MANAGER AND CLICK "DECLINE" BELOW.

The terms and conditions set forth below (the "Agreement") constitute a binding agreement between you (the "Company" or "you") and Comodo CA Limited ("Comodo") with respect to your or your employee's creation and use of your Certificate Manager account and the related

☑ I Agree*

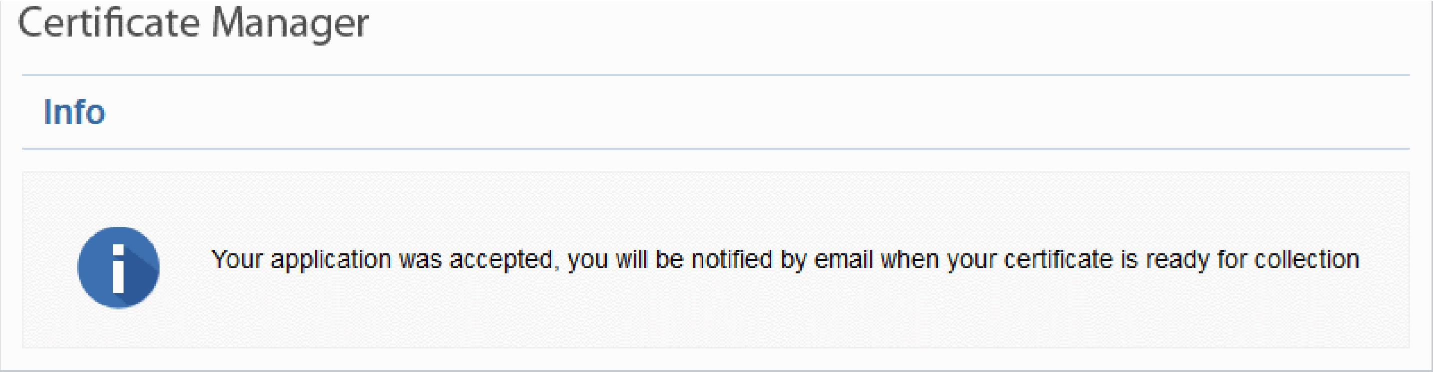
Scroll to bottom of the agreement to activate check box.

When you click the button below, your browser will generate a new private key.

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. InCommon 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 applicants are strongly advised to backup their 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 clicking the 'Generate' button. The certificate request will be automatically generated and a request will be sent to CM.



Certificate Manager

Info

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

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

3.3.4.5 Downloading and Installing the Certificate

The CM will collect the certificate from the server and send a notification mail to the end-user 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 CM. The certificate can be installed by the applicant and used to digitally sign the executables.

4 Code Signing on Demand

- Code Signing on Demand (CSoD) offers customers a faster, more intuitive and highly secure way to digitally sign their software. The service is available in both hosted and cloud versions and is capable of signing EXE .DLL .CAB .MSI .OCX .SY, WAR, JAVA JAR and Android application files.
- InCommon CM is also capable of hash signing, whereby developers upload a hash of their files for signing instead of the files themselves. The developer then needs to embed the hash with their files.

Code signing on demand is available in two deployment options:

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

Both modes require you to create a new 'Developer' role in Incommon CM. The developer will be responsible for uploading software and collecting the signed code (after administrator approval).

Note: The CSoD service is only available if enabled for your account. For In-house Hosted Mode, your Master Administrator should have setup and configured the CSoD service controller on your local network.

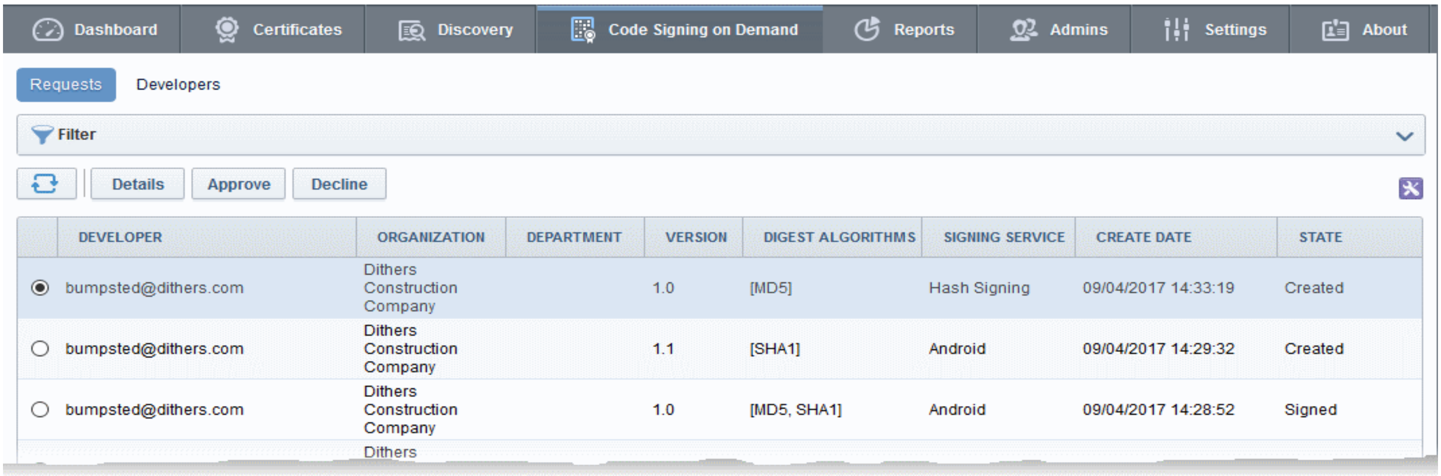
If you wish to add this service, please contact your Master Administrator/Incommon account manager.

The 'Code Signing on Demand' Interface

The 'Code Signing on Demand' area lets you manage 'Developers' and signing requests.

The interface is divided into two main sections:

- The 'Requests' tab - View and approve/decline code signing requests from developers
- The 'Developers' tab - Add and manage 'Developer' accounts in Incommon CM



	DEVELOPER	ORGANIZATION	DEPARTMENT	VERSION	DIGEST ALGORITHMS	SIGNING SERVICE	CREATE DATE	STATE
●	bumpsted@dithers.com	Dithers Construction Company		1.0	[MD5]	Hash Signing	09/04/2017 14:33:19	Created
○	bumpsted@dithers.com	Dithers Construction Company		1.1	[SHA1]	Android	09/04/2017 14:29:32	Created
○	bumpsted@dithers.com	Dithers Construction Company		1.0	[MD5, SHA1]	Android	09/04/2017 14:28:52	Signed
		Dithers						

Visibility of the 'Code Signing on Demand' area is restricted to:

- RAO Code Signing administrators - can add developers and manage code signing requests only for Organizations (and any subordinate Departments) that have been delegated to them.
- DRAO Code Signing administrators - can add developers and manage code signing requests only for Departments that have been delegated to them.

This chapter contains the following sections:

- Add Developers
- Obtain a Code Signing Certificate for CSoD
- How to sign code using CSoD

4.1 Add Developers

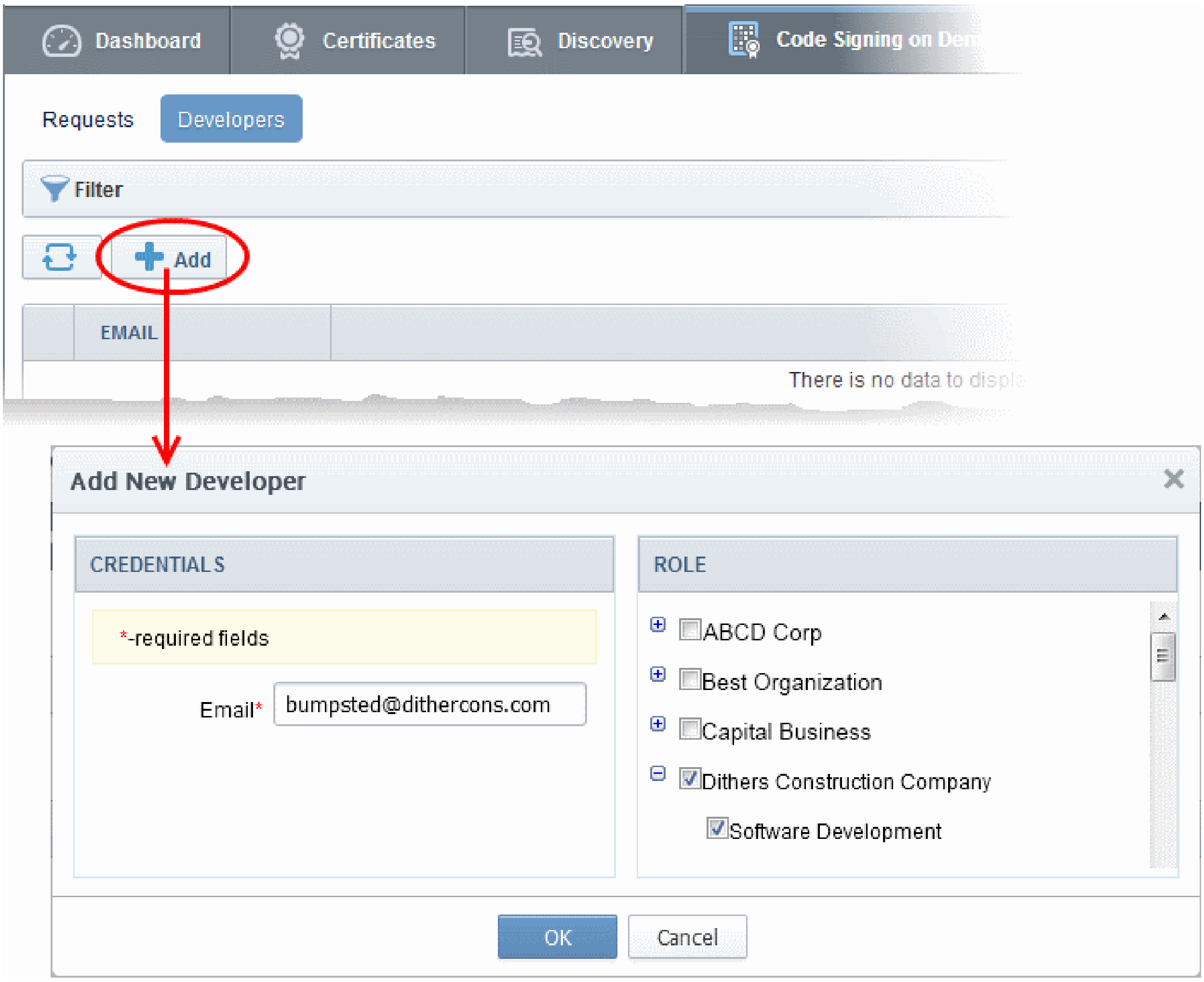
A 'Developer' is a role in Incommon CM with permission to:

- Login to CSoD Service
- Upload files or hashes for code-signing
- Download the signed file or signed hash

You can create a developer as a new user, or add developer privileges to an existing Incommon CM user. An RAO or DRAO administrator will need to approve the developer's actual signing requests, unless your Master Administrator has enabled auto-approval of the requests in the service configuration.

To add a developer

- Open the 'Developers' interface by clicking 'Code Signing on Demand' > 'Developers'
- Click the 'Add' button. This will open 'Add New Developer' dialog.



*-required fields

Email* bumpsted@dithercons.com

⊞ □ ABCD Corp

⊞ □ Best Organization

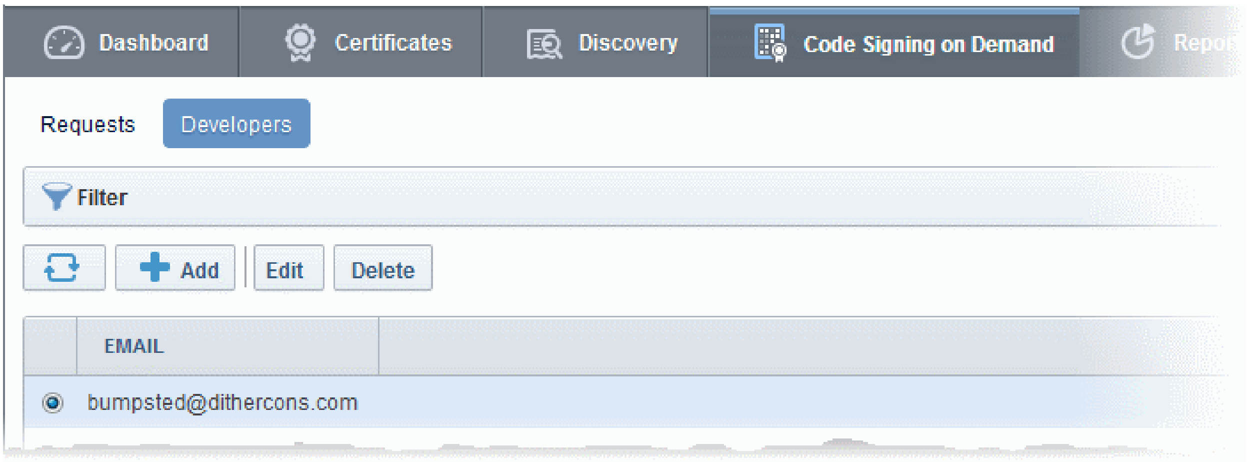
⊞ □ Capital Business

⊟ ☑ Dithers Construction Company

☑ Software Development

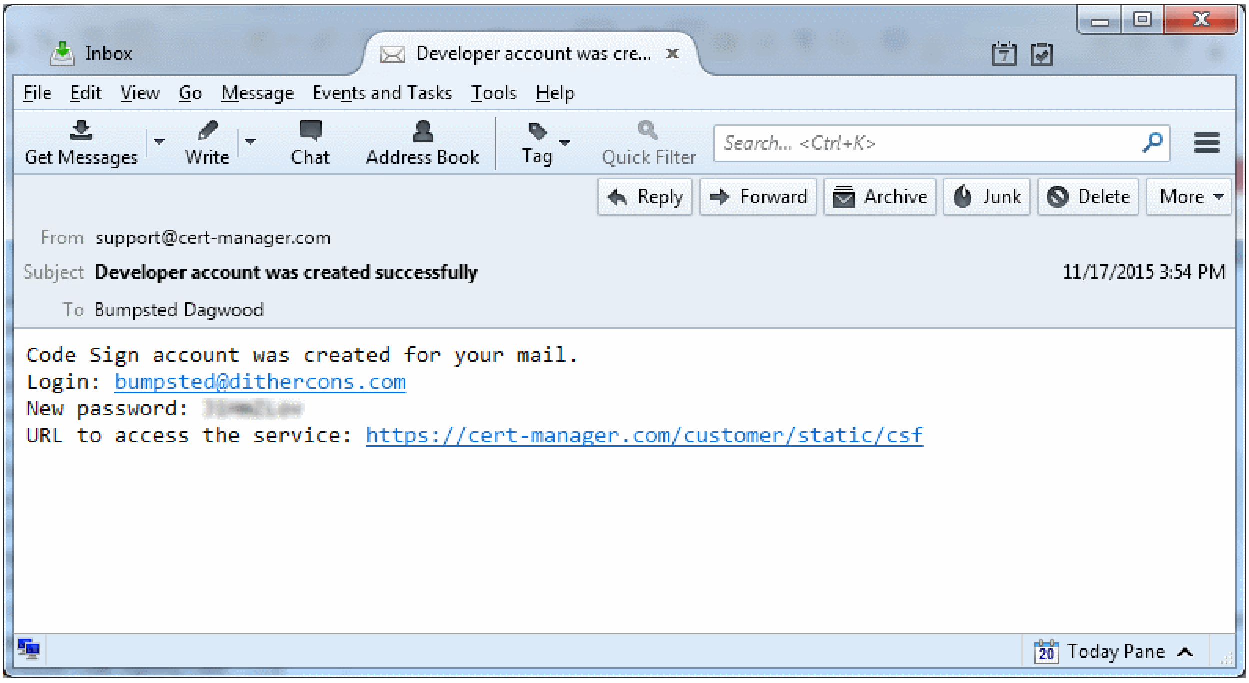
- Type the email address of the developer in the email field.
- Use the right-hand pane to select the Organization(s) / Department(s) to which the developer should belong.
- Click 'OK' to confirm your selection.

The developer will be added to the list. You can edit the user to change their Organization/Department, reset their password or to remove the developer.



● bumpsted@dithercons.com

A notification email will be sent to the developer with the credentials to access the CSoD service. An example is shown below:



From support@cert-manager.com

Subject **Developer account was created successfully** 11/17/2015 3:54 PM

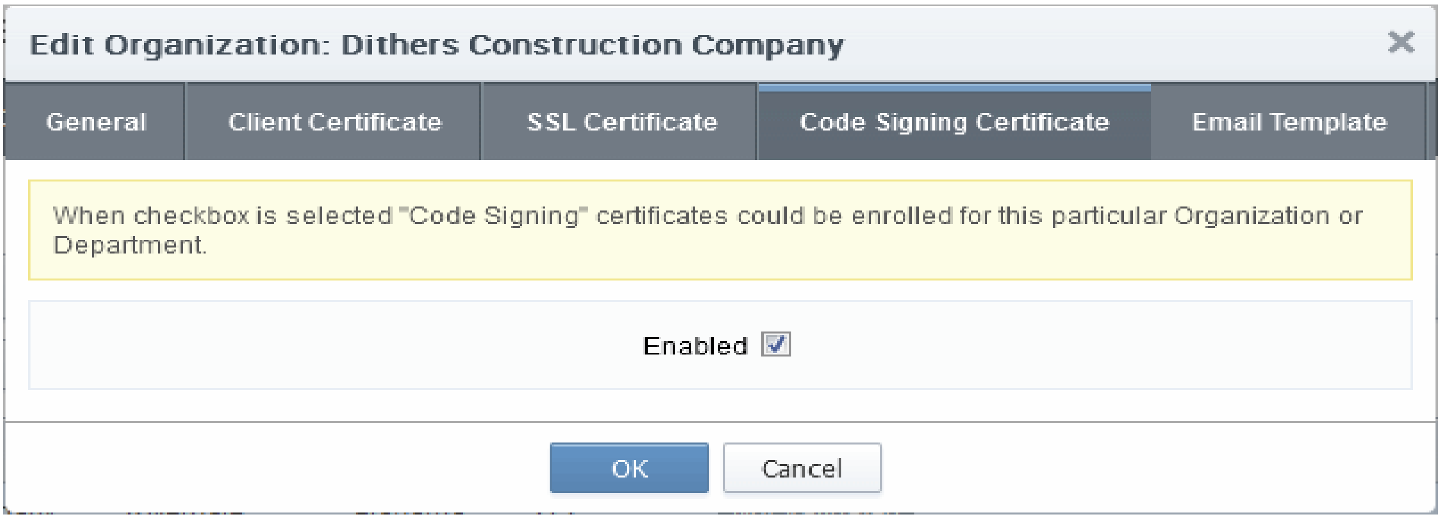
To Bumpsted Dagwood

```
Code Sign account was created for your mail.
Login: bumpsted@dithercons.com
New password: [redacted]
URL to access the service: https://cert-manager.com/customer/static/csf
```

4.2 Obtain a code-signing certificate for CSoD

Prerequisites:

- You have created a 'Developer' role as explained in the preceding section.
- The domain from which the certificate is to be issued has been enabled for code signing certificates. The domain has been activated by your Incommon account manager.
  - For example, if you wish to issue code signing certs to end-user@mycompany.com, then mycompany.com must have been validated by Incommon.
  - All certificate requests made on validated domains or sub-domains are issued automatically. Certificate requests for new domains will first have to undergo validation.
- The domain has been delegated to an organization or department. See Editing an Existing Organization if you need help with this.
- An 'RAO Code-Signing' or 'DRAO Code-Signing' admin has been delegated control of the organization/ dept.
- The admin has enabled code signing certificates for the organization in the 'Code Signing tab' of the organization's settings (see screen-shot below). 'Edit' an organization to access these settings.



Edit Organization: Dithers Construction Company

When checkbox is selected "Code Signing" certificates could be enrolled for this particular Organization or Department.

Enabled ☑

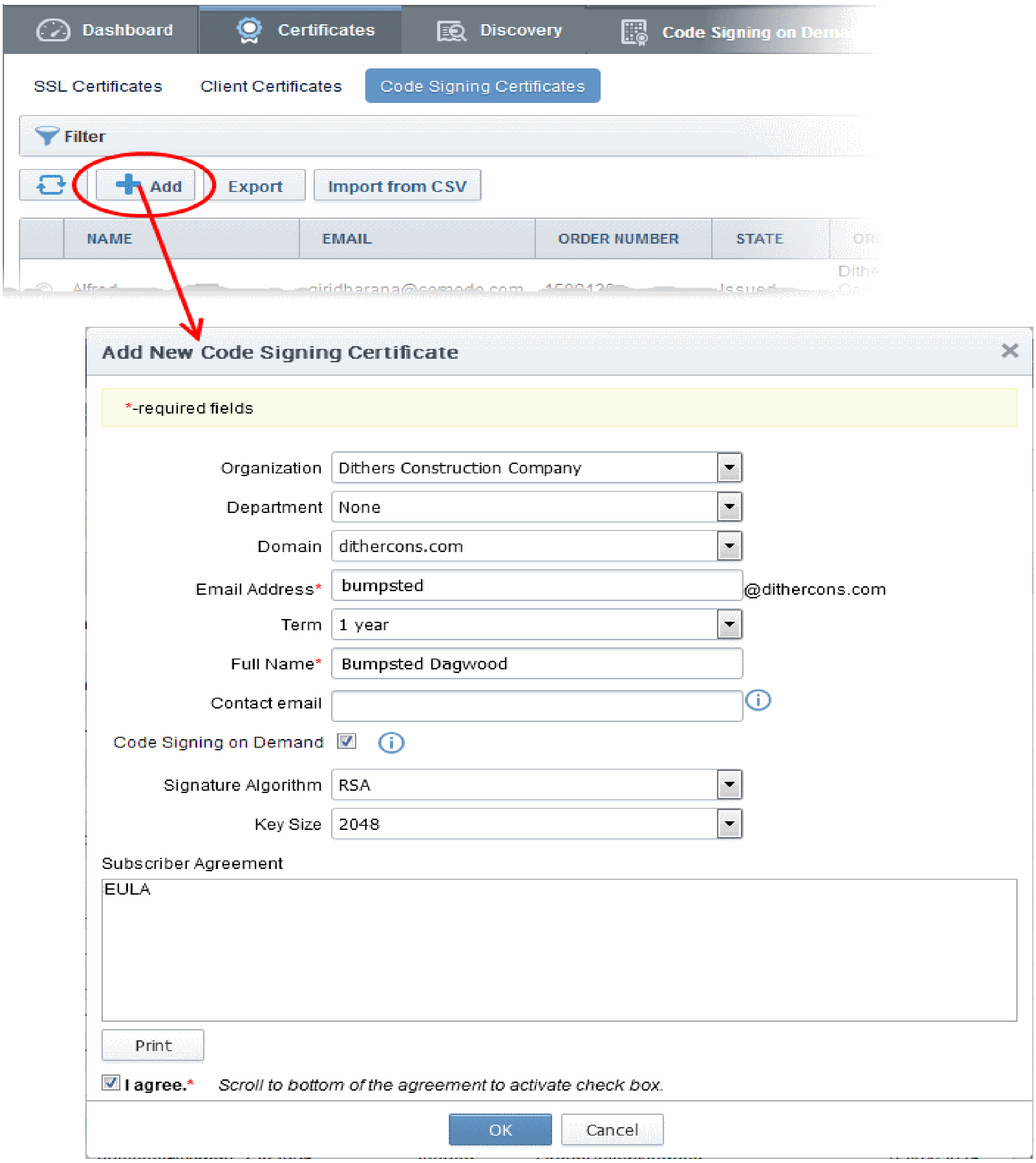
- Hosted mode - the CSoD service controller also needs to be installed on the local network and connected to InCommon CM.
- Cluster Mode - If the controllers are installed on multiple machines then they must be configured to generate and store keys on a HSM appliance. If you install the controller on a single machine then it is optional to use a HSM appliance to generate and store keys.
- Contact your Master Administrator for CSoD agent configuration on servers.

Procedure Overview:

1. The administrator confirms completion of the prerequisite steps.
2. The administrator adds a new code-signing certificate for the developer from the 'Certificates' > 'Code Signing Certificates' interface, with 'Code Signing on Demand' enabled for the certificate.
    - For Hosted Mode - The CSoD controller generates and stores the key pair locally and submits the CSR to Incommon CA. Once the certificate is issued, the CSoD controller automatically downloads the certificate and stores it in your local network. If a HSM appliance is used, the key pair is generated and stored on the HSM. On issuance of the certificate, the controller downloads the certificate and stores it on the HSM appliance.
    - For Cloud Mode - The CSoD cloud service generates and stores the key pair and submits the CSR to Incommon CA. Once the certificate is issued, the service automatically downloads the certificate and stores it on the cloud server. If the HSM service is used, the key pair is generated and stored on the HSM. The service will collect the certificate after it is issued and will store it on the HSM.

To add a code signing certificate for the developer

- Click 'Certificates' > 'Code Signing Certificates' to open the 'Code Signing Certificates' interface
- Click the 'Add' button to open the certificate application form.
- Complete all required fields on the form, making sure:
    - The correct developers email address is used.
    - The correct organization and department are specified for the developer.
    - The 'Code Signing on Demand' box is checked.



Add New Code Signing Certificate

*-required fields

Organization	Dithers Construction Company
Department	None
Domain	dithercons.com
Email Address*	bumpsted @dithercons.com
Term	1 year
Full Name*	Bumpsted Dagwood
Contact email	
Code Signing on Demand	☑
Signature Algorithm	RSA
Key Size	2048

Subscriber Agreement

EULA

☑ I agree.* *Scroll to bottom of the agreement to activate check box.*

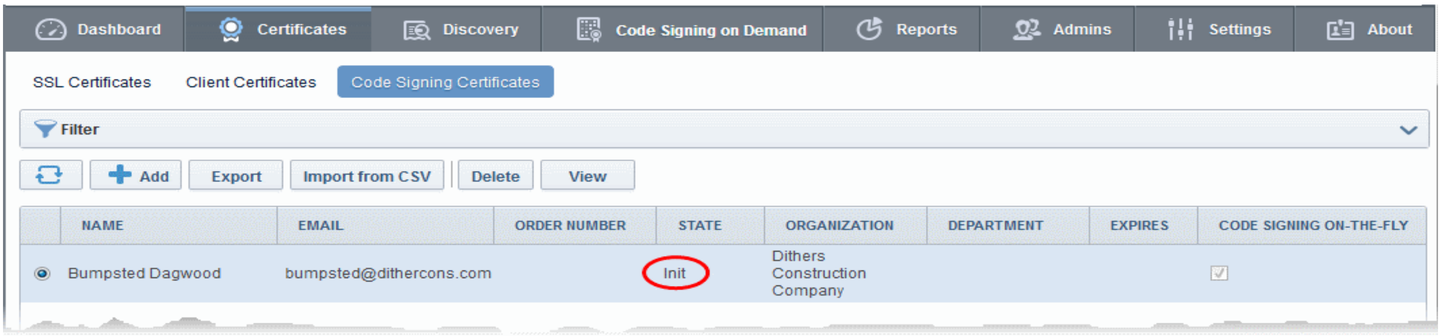
The following table explains the fields on the form:

Field	Description
Organization	Select the Organization to which the developer belongs.
Department	Select the Department to which the developer belongs.
Domain	Select the domain to which you want to issue the certificate. This will be a domain that is assigned to the organization/department
Term	Select the term of the certificate.
Email Address	Enter the email address of the developer.
Full Name	Full name of the applicant.

Field	Description
Contact Email	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.
Code Signing on Demand	Enable to allow the certificate to be used by the CSoD service.
Signature Algorithm	Choose the signature algorithm to be used by the certificate.
Keysize	Choose the key-size (in bits) by the certificate. Recommended = 2048 bit or higher.
Subscriber Agreement	Displays the End-User License Agreement (EULA) for the certificate. Read through the EULA and accept to it by selecting the 'I agree' checkbox for the application to proceed.

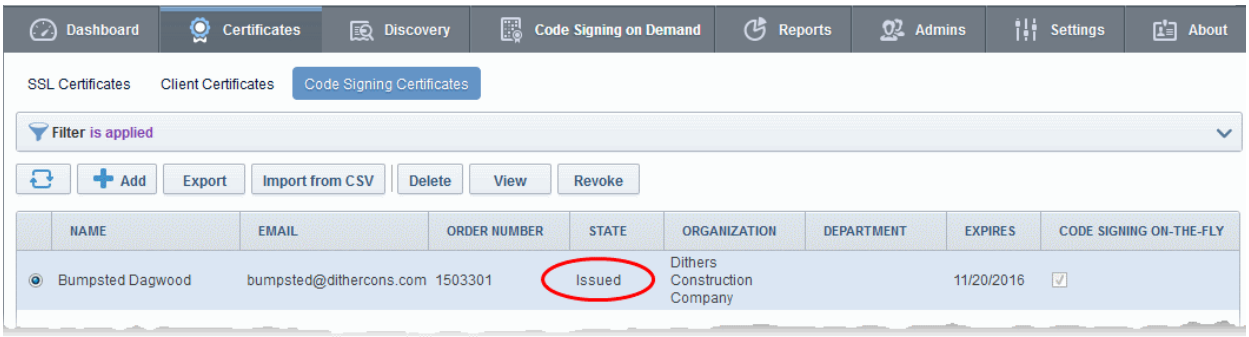
- Click 'OK' to submit the request.

The certificate will be added with the state 'init', indicating that the certificate enrollment has been initiated.



	NAME	EMAIL	ORDER NUMBER	STATE	ORGANIZATION	DEPARTMENT	EXPIRES	CODE SIGNING ON-THE-FLY
●	Bumpsted Dagwood	bumpsted@dithercons.com		Init	Dithers Construction Company			✓

Once issued, the state of the certificate will change to 'Issued':

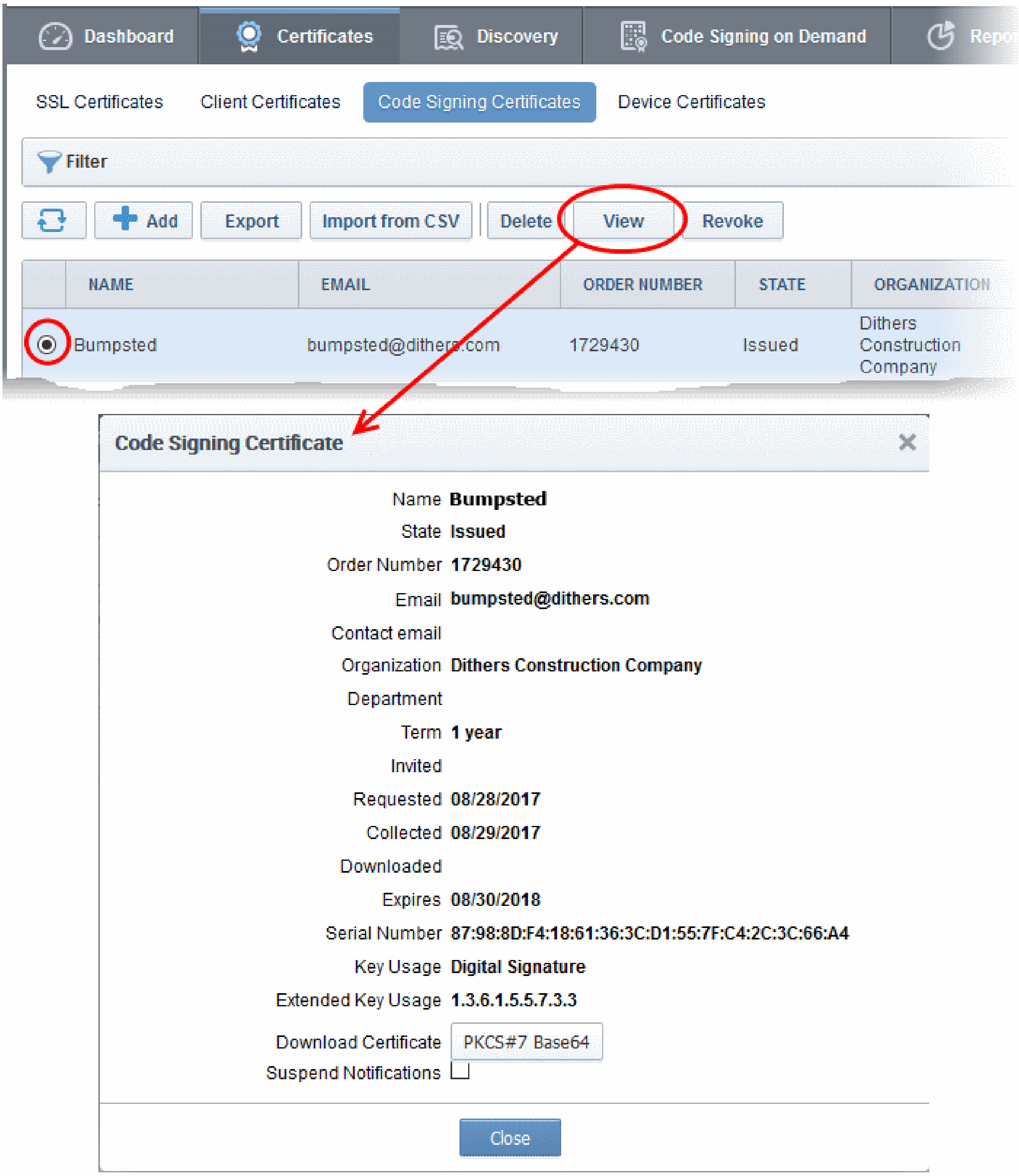


	NAME	EMAIL	ORDER NUMBER	STATE	ORGANIZATION	DEPARTMENT	EXPIRES	CODE SIGNING ON-THE-FLY
●	Bumpsted Dagwood	bumpsted@dithercons.com	1503301	Issued	Dithers Construction Company		11/20/2016	✓

The certificate can now be used to sign code submitted by your developer. Each signing action will, however, need to be approved by an administrator UNLESS auto-approval of code signing requests is enabled by your Master Administrator.

Viewing and Downloading the certificate

- Select the certificate and click 'View' to see certificate details:



	NAME	EMAIL	ORDER NUMBER	STATE	ORGANIZATION
●	Bumpsted	bumpsted@dithers.com	1729430	Issued	Dithers Construction Company

Code Signing Certificate

Name	Bumpsted
State	Issued
Order Number	1729430
Email	bumpsted@dithers.com
Contact email	
Organization	Dithers Construction Company
Department	
Term	1 year
Invited	
Requested	08/28/2017
Collected	08/29/2017
Downloaded	
Expires	08/30/2018
Serial Number	87:98:8D:F4:18:61:36:3C:D1:55:7F:C4:2C:3C:66:A4
Key Usage	Digital Signature
Extended Key Usage	1.3.6.1.5.5.7.3.3
Download Certificate	PKCS#7 Base64
Suspend Notifications	□

- Click the 'Download' button to download the certificate in PKCS#7 format.

4.3 How to Sign Code using CSoD

Once you have created a developer and obtained at least one CSoD enabled code-signing certificate, your developer is ready to upload files or hashes for signing.

- Code Signing - Developers can upload EXE .DLL .CAB .MSI .OCX .SY, JAVA JAR, WAR and Android application files.

- Hash Signing - Developers can upload a text file containing the SHA or MD5 hash value of their software which will be signed with their code signing certificate. Developers can embed the signed hash and certificate with their binary. This is useful if:
  - The source files are large and the developer wishes to avoid longer upload times
  - Company policy allows code signing of binaries to be performed only within a local system

  See Obtain a code-signing certificate for CSoD if you need help with getting a code-signing certificate.

Note: The 'Hash Signing' feature is only available if enabled for your account. Please contact your InCommon account manager if you wish to add this service.

Checklist:

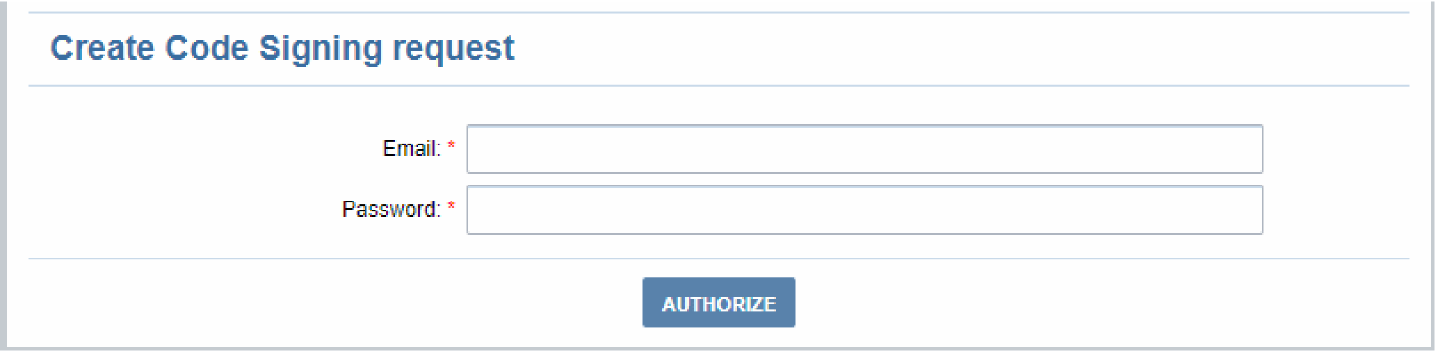
In-House Hosted Mode	Cloud Service Mode
• The 'Code Signing on Demand' (CSoD) service is enabled in 'Hosted Mode' for your account. • Your Master Administrator has installed the CSoD controller on your network and it is connected to InCommon CM. • Developer accounts have been created and issued with a CSoD Code Signing certificate.	• The 'Code Signing on Demand' (CSoD) service is enabled in 'Cloud Mode' for your account • Developer accounts have been created and issued with a CSoD Code Signing certificate.

Overview of steps:

- Step 1 - Upload the files to be Signed - The developer logs-in to the CSoD service portal, enters the details of the file(s) to be signed, selects the signing service and uploads their code or hash. This will create a request which can be viewed in the 'Code Signing on Demand' > 'Requests' interface.
- Step 2 - Approve the Code Signing Request (optional) - An administrator views the request, checks the files to be signed and approves the request from the 'Code Signing on Demand' > 'Requests' interface Note - this step will be skipped if 'Auto-Approval of Code Signing Requests' is enabled by your Master Administrator.
- Step 3 - Download Code-Signed files - After the signing process is complete, the status of the request will change to 'Signed'. A notification mail is sent to the developer with a URL to download the signed files.

Step 1 - Upload the files to be Signed

- Once a developer has been added, they will be able to login to InCommon CM using the link in their confirmation email.
- By default, the format of this URL is: https://cert-manager.com/customer/InCommon/csod.

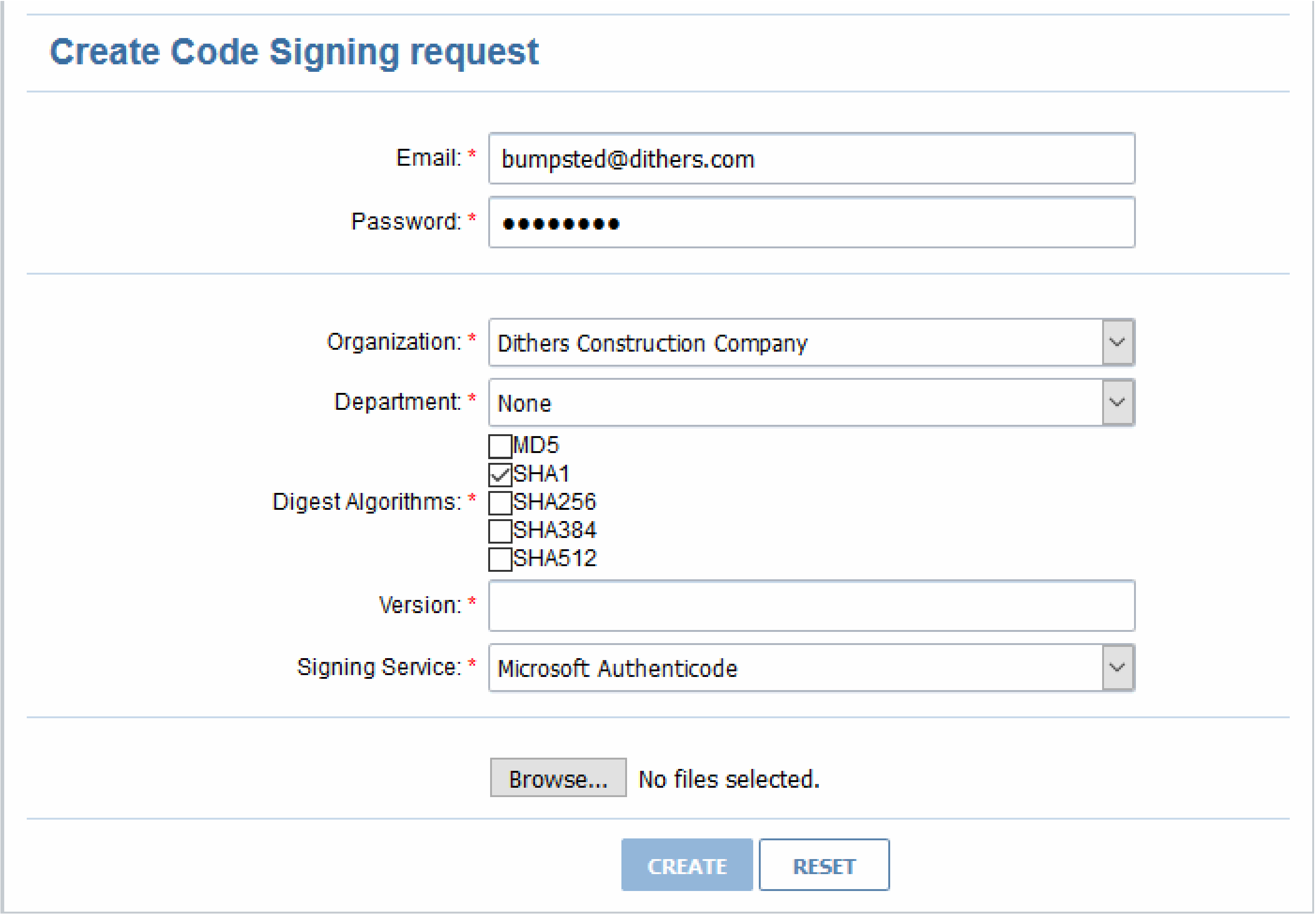


Create Code Signing request

Email: *

Password: *

- After logging in, developers can upload files using the following form:



Create Code Signing request

Email: * bumpsted@dithers.com

Password: * ••••••••

Organization: * Dithers Construction Company

Department: * None

Digest Algorithms: *
□ MD5
☑ SHA1
□ SHA256
□ SHA384
□ SHA512

Version: *

Signing Service: * Microsoft Authenticode

No files selected.

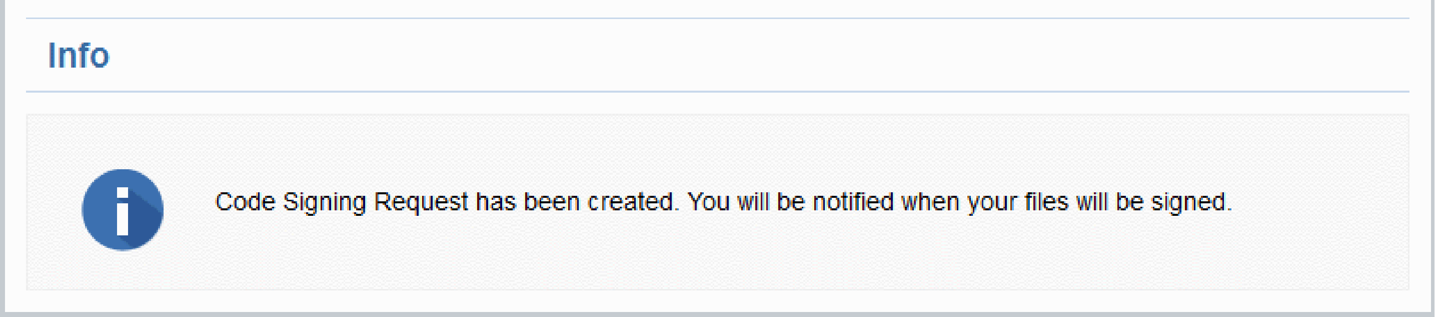
- **Organization** - The organization(s) to which the developer belongs. The organization selected here will be shown in the certificate as the publisher of the software.
- **Department** - Allows the developer to choose a department If departmental information is also required in the certificate.
- **Digest Algorithm** - Select the algorithm you wish to use to create the file hash-code (aka 'digest). The hash-code is used by client software to verify the integrity of your signed code. Recommended = SHA256 and upwards.

- **Version** - Developer should type the version number of the software they wish to sign
- **Signing Service** - Select the appropriate signing service for the type of file you want to sign:
  1. ***Files*** - Choose 'Microsoft Authenticode', 'Java' or 'Android' as the signing service
  2. ***Hash values*** - Choose 'Hash Signing' as the signing service. You need to generate a hash-code of your file with the SHA or MD5 algorithm (to generate a .sha or .md5 file). Alternatively, create a .txt file containing the hash value.

  Note: 'Hash Signing' is only available if the service is enabled for your account. Contact your account manager if you want to enable 'Hash Signing'.
- **Browse**... - Choose the files or hashes to upload for signing. Multiple files can be uploaded.

- The developer should complete the form and click the 'Create' button to submit the signing request to the CSoD service.

A confirmation dialog will be displayed:



Info

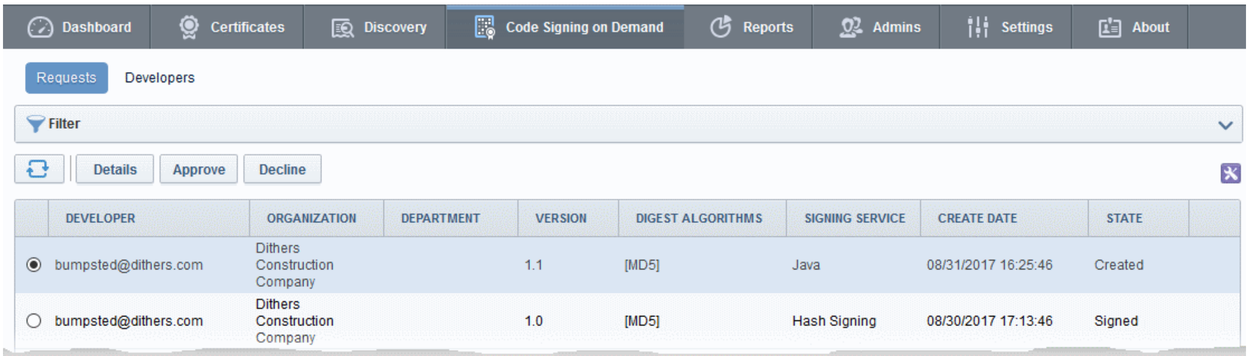
Code Signing Request has been created. You will be notified when your files will be signed.

- The code signing request can be seen in 'Code Signing on Demand' > 'Requests'.
- By default, the request needs to be approved by the appropriate RAO or DRAO administrator before the signing will take place.
- If 'Auto-Approval' of Code Signing Requests is enabled, the service will sign the code immediately. Contact your Master Administrator to enable this feature.

Step 2 - Approve the Code Signing Request

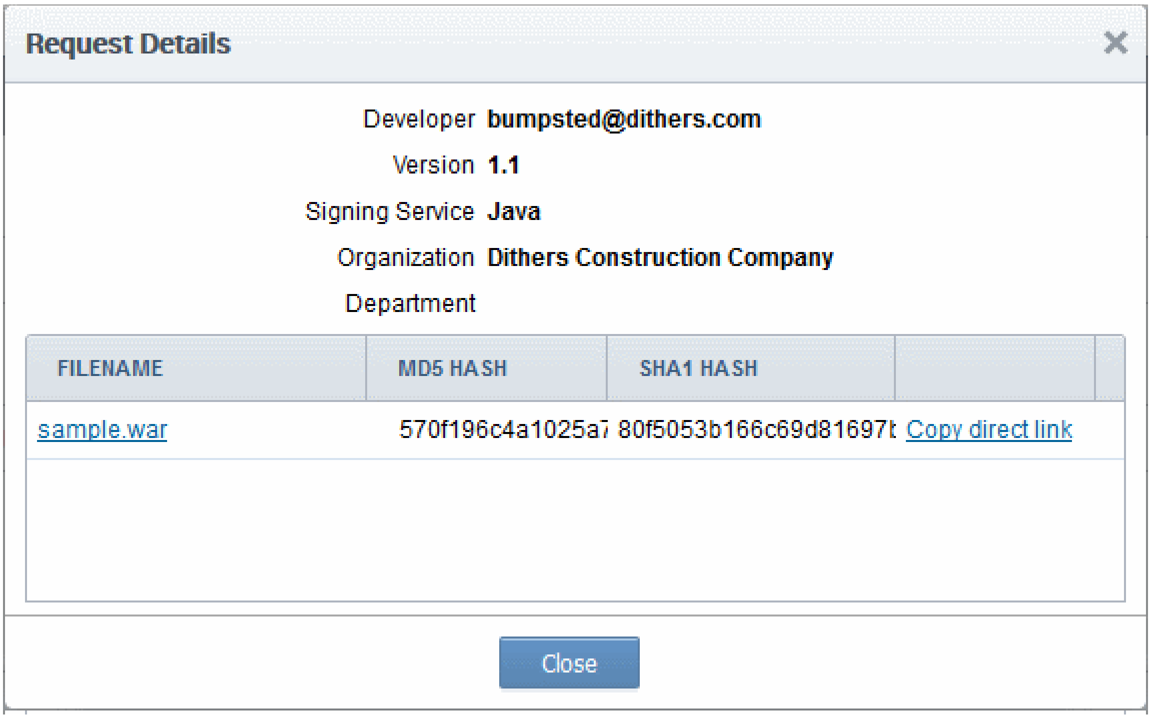
A code signing request will appear in 'Code Signing on Demand' > 'Requests' after a developer has uploaded files for signing. Under default settings, an administrator needs to review and approve the request before the service will actually sign the files.

- Click 'Code Signing on Demand' tab and choose the 'Requests' sub tab.
- A list of requests will be displayed.



	DEVELOPER	ORGANIZATION	DEPARTMENT	VERSION	DIGEST ALGORITHMS	SIGNING SERVICE	CREATE DATE	STATE
●	bumpsted@dithers.com	Dithers Construction Company		1.1	[MD5]	Java	08/31/2017 16:25:46	Created
○	bumpsted@dithers.com	Dithers Construction Company		1.0	[MD5]	Hash Signing	08/30/2017 17:13:46	Signed

- Click 'Details' to view the specifics of the request:



Developer **bumpsted@dithers.com**

Version **1.1**

Signing Service **Java**

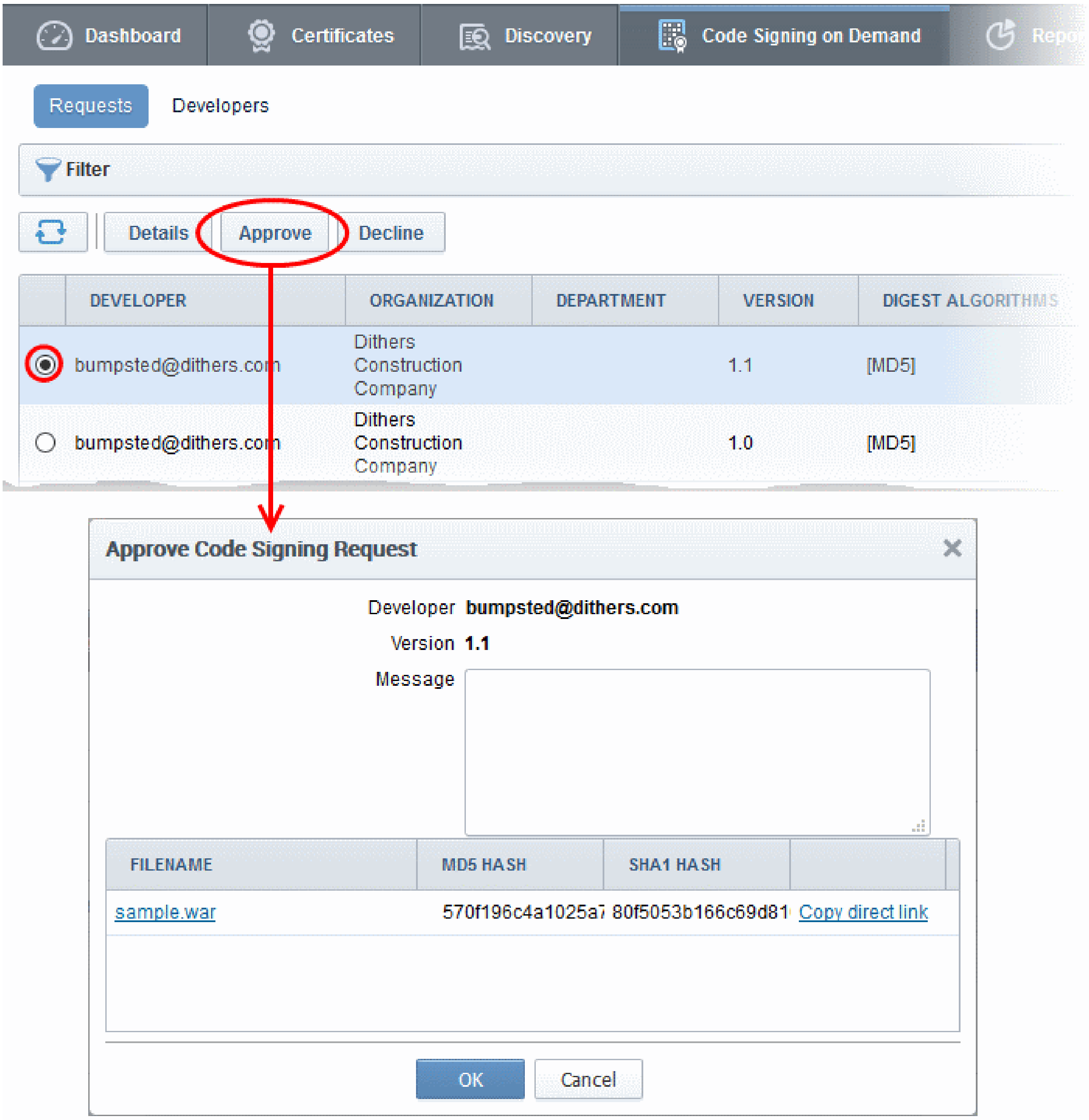
Organization **Dithers Construction Company**

Department

FILENAME	MD5 HASH	SHA1 HASH	
sample.war	570f196c4a1025a7	80f5053b166c69d81697t	Copy direct link

The details dialog shows the developer's name, file details, and the MD5 and SHA1 hash values of the files.

- Click the file name to download the file for examination
- Select the request and click 'Approve' to allow the signing process to go ahead



	DEVELOPER	ORGANIZATION	DEPARTMENT	VERSION	DIGEST ALGORITHMS
●	bumpsted@dithers.com	Dithers Construction Company		1.1	[MD5]
○	bumpsted@dithers.com	Dithers Construction Company		1.0	[MD5]

Approve Code Signing Request

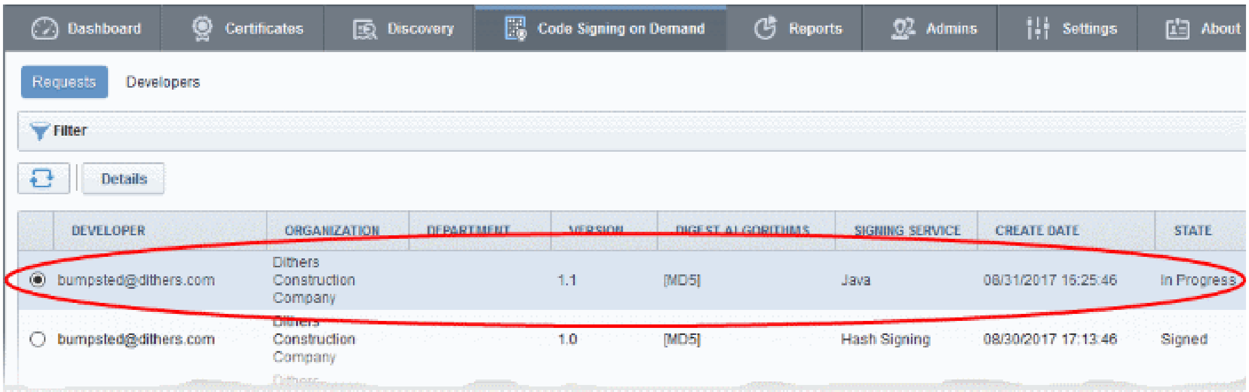
Developer **bumpsted@dithers.com**

Version **1.1**

Message

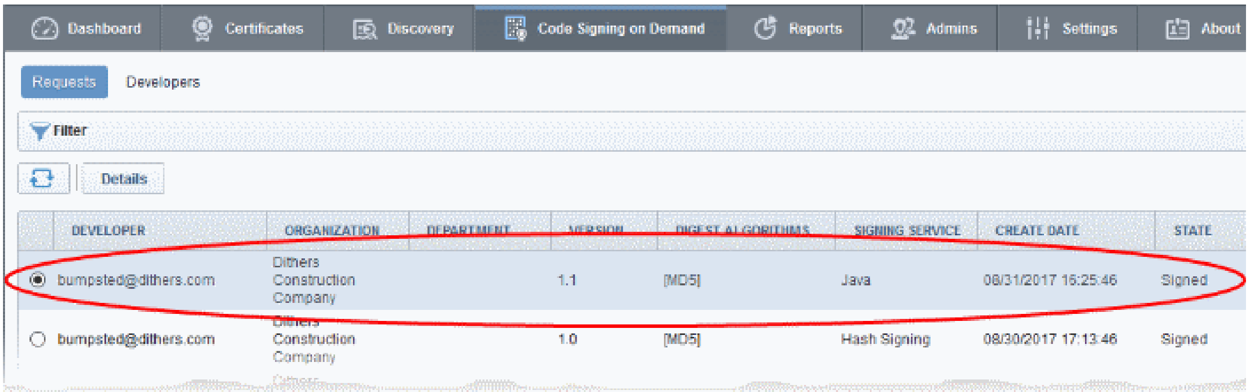
FILENAME	MD5 HASH	SHA1 HASH	
sample.war	570f196c4a1025a7	80f5053b166c69d81	Copy direct link

- Enter an approval message in the 'Message' field and click 'OK'
- The request will be approved and its state will change to 'In Progress':



	DEVELOPER	ORGANIZATION	DEPARTMENT	VERSION	DIGEST ALGORITHMS	SIGNING SERVICE	CREATE DATE	STATE
●	bumpsted@dithers.com	Dithers Construction Company		1.1	[MD5]	Java	08/31/2017 15:25:46	In Progress
○	bumpsted@dithers.com	Dithers Construction Company		1.0	[MD5]	Hash Signing	08/30/2017 17:13:46	Signed

- The request state will change to 'Signed' once the signing process is complete.
- A notification mail will be sent to the developer to download the signed file.
- The Developer must download the signed files within three days of the notification. The files will be removed from the database three days after signing.
- If required, you can resend the email by clicking 'Resend Signed Notification'

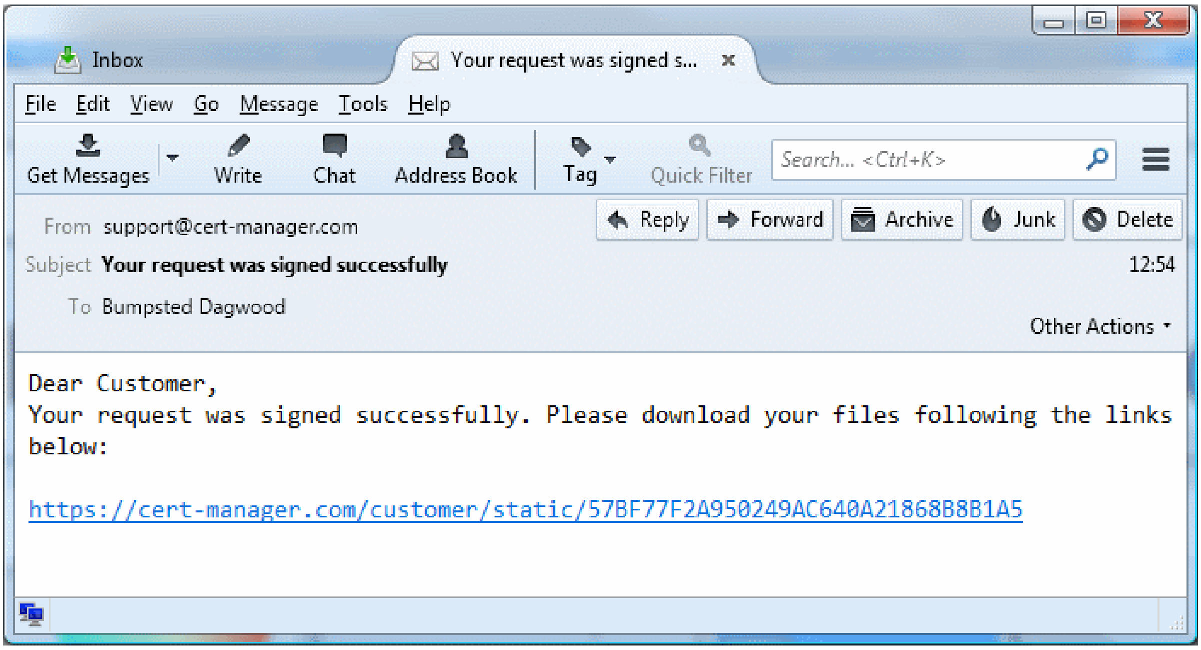


	DEVELOPER	ORGANIZATION	DEPARTMENT	VERSION	DIGEST ALGORITHMS	SIGNING SERVICE	CREATE DATE	STATE
●	bumpsted@dithers.com	Dithers Construction Company		1.1	[MD5]	Java	08/31/2017 15:25:46	Signed
○	bumpsted@dithers.com	Dithers Construction Company		1.0	[MD5]	Hash Signing	08/30/2017 17:13:46	Signed

Note. As mentioned earlier, if the Master Administrator has enabled Auto-Approval of Code Signing Requests in the CSoD service configuration, the code signing process is completed without the need of approval by the administrators.

Step 3 - Download Code-Signed files

After completing the signing process, the developer will receive an email with links to download each signed file. An example is shown below.



From support@cert-manager.com

Subject **Your request was signed successfully**

12:54

To Bumpsted Dagwood

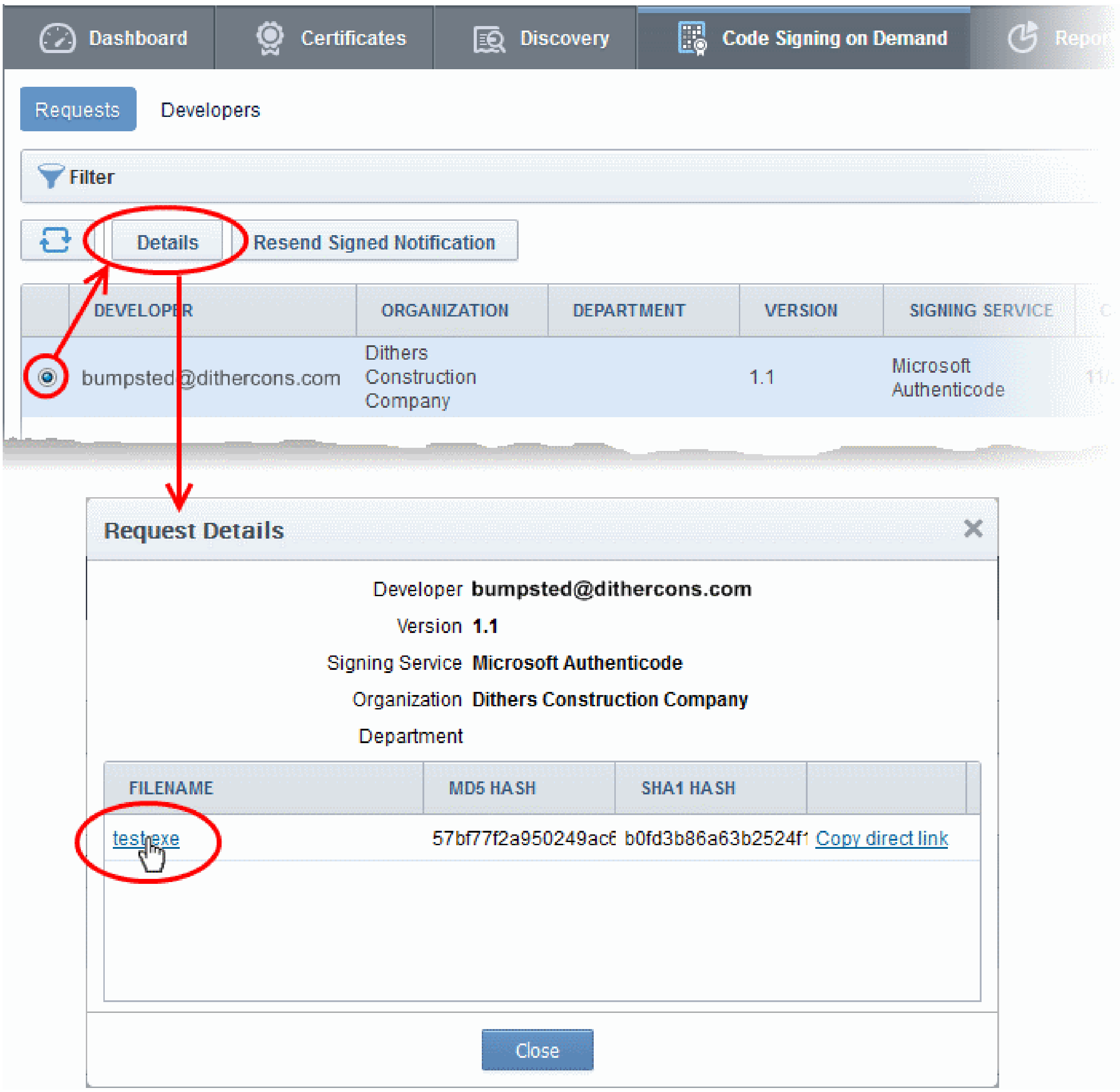
```
Dear Customer,
Your request was signed successfully. Please download your files following the links
below:

https://cert-manager.com/customer/static/57BF77F2A950249AC640A21868B8B1A5
```

If a hash was uploaded, the developer can download the signed hash and embed it into the binary to create a digitally signed file.

Note: The developer must download the signed files within three days of the notification. The files will be removed from the database three days after signing.

Administrators can also download signed files from the 'Details' dialog of the request.

- Choose the request from the 'Code Signing on Demand' > 'Requests' interface and click 'Details'



	DEVELOPER	ORGANIZATION	DEPARTMENT	VERSION	SIGNING SERVICE	C
●	bumpsted@dithercons.com	Dithers Construction Company		1.1	Microsoft Authenticode	11/

Request Details

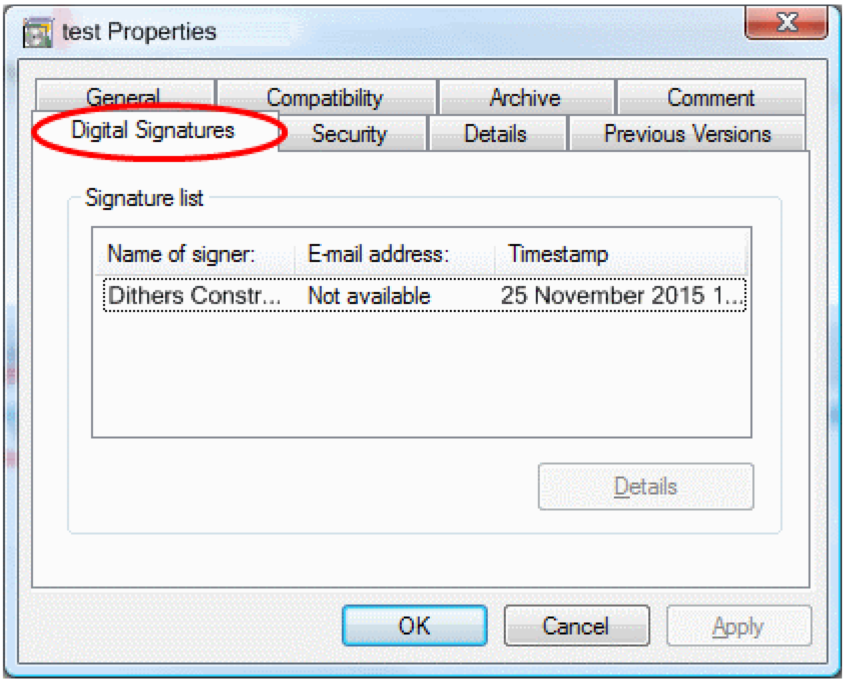
Developer **bumpsted@dithercons.com**
Version **1.1**
Signing Service **Microsoft Authenticode**
Organization **Dithers Construction Company**
Department

FILENAME	MD5 HASH	SHA1 HASH	
test.exe	57bf77f2a950249ac	b0fd3b86a63b2524f	Copy direct link

- Click the file name in the 'Request Details' dialog to download the signed file.

To check whether the file is signed

- Right click on the file and choose 'Properties'
- Choose the 'Digital Certificates' tab



Name of signer:	E-mail address:	Timestamp
Dithers Constr...	Not available	25 November 2015 1...

The details of the signer will be displayed.

5 Admin Management

5.1 Section Overview

The 'Admin Management' tab allows administrators to create, manage and edit permissions for new and existing administrators. There are 8 types of administrators:

- Registration Authority Officer (RAO) - SSL
- Registration Authority Officer (RAO) - S/MIME
- Registration Authority Officer (RAO) - Code Signing
- Department Registration Authority Officer (DRAO) - SSL
- Department Registration Authority Officer (DRAO) - S/MIME
- Department Registration Authority Officer (DRAO) - Code Signing

Administrative Roles:

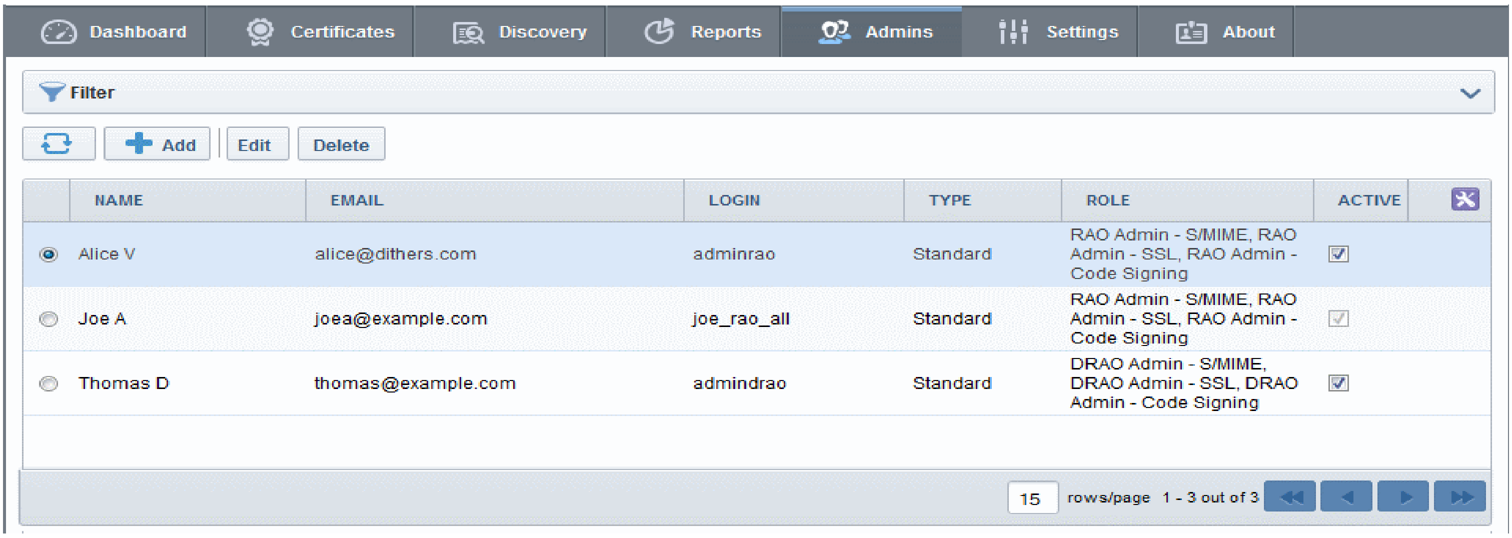
Registration Authority Officer (RAO)

- A Registration Authority Officer (RAO) is an administrative role created by a Master Administrator at InCommon CA or fellow RAO for the purposes of managing the certificates and end-users belonging to one or more CM 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 the Master Administrator at InCommon CA; 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 Master Administrator at InCommon CA.
- 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 have been delegated to them.
- 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.

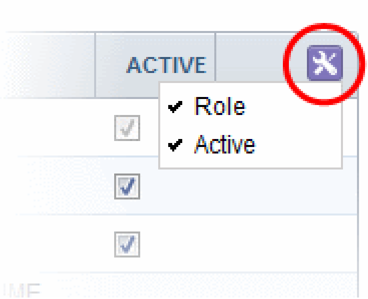
It is also possible to create an Administrator with more than one Admin privileges. Further details about the privileges and security roles of these administrator types can be found in section 1.2.1.Security Roles The remainder of this chapter contains detailed explanations of the controls available from the 'Admin Management' tab.



	NAME	EMAIL	LOGIN	TYPE	ROLE	ACTIVE
●	Alice V	alice@dithers.com	adminrao	Standard	RAO Admin - S/MIME, RAO Admin - SSL, RAO Admin - Code Signing	☑
○	Joe A	joea@example.com	joe_rao_all	Standard	RAO Admin - S/MIME, RAO Admin - SSL, RAO Admin - Code Signing	☑
○	Thomas D	thomas@example.com	admindrao	Standard	DRAO Admin - S/MIME, DRAO Admin - SSL, DRAO Admin - Code Signing	☑

15 rows/page 1 - 3 out of 3

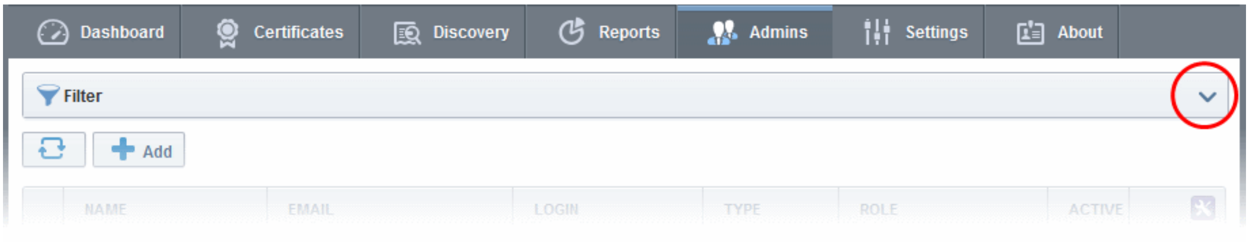
Admin Management Area - Table of Parameters		
Fields	**Values**	**Description**
Name	*String*	Administrator's full name.
Email address	*String*	Administrator's Email Address (it will be used for client certificate enrollment, notifications)
Login	*String*	The login username of the administrator.
Type		Shows the type of the administrators.
	Standard	Indicates that the administrator is a standard administrator.
	IdP Template	Indicates that the administrator is added as Identity Provider (IdP) template.
	IdP User	Indicates that the administrator is added as IdP user.
Role	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 S/MIME	RAO S/MIME 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 a RAO Admin. (More...)
	DRAO Admin S/MIME	DRAO S/MIME 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.

Admin Management Area - Table of Parameters		
Fields	**Values**	**Description**
		(More...)
Active	Checkbox	Indicates whether the administrator is active or not. Also allows 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 columns displayed in the table, from the drop-down at the right end of the table header: 		
Control Buttons	Add	Enables RAO Administrators to add new administrators.
	Edit	Enables 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.*
	Refresh	Refreshes the list.
Administrator Control Buttons **Note**: The availability of the control buttons depends on the chosen administrator.	Edit	Enables 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 admins to view the details of RAO/DRAO added by another RAO, pending approval.
	Approve	Enables admins to approve RAO/DRAO added by an RAO. The newly added administrator becomes active only on approval by the Master administrator.
	Reject	Enables MRAO admins to reject RAO/DRAO added by an RAO, pending approval.
	Reset Lockout	Enables Master admins to unlock the login screen that has been locked due to consecutive five wrong attempts to login.

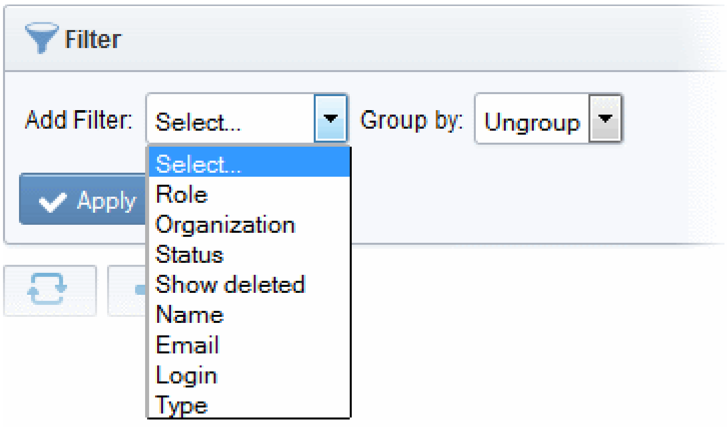
5.1.1 Sorting and Filtering Options

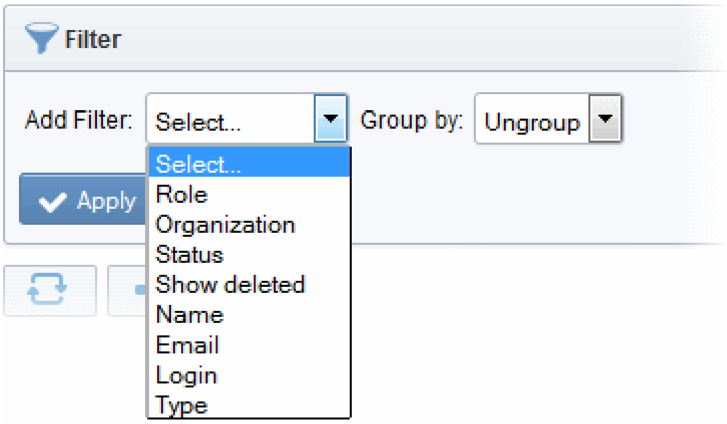
- Clicking the column header 'Name', 'Email' or Type sorts the items in the alphabetical order of the entries in the respective column.

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.



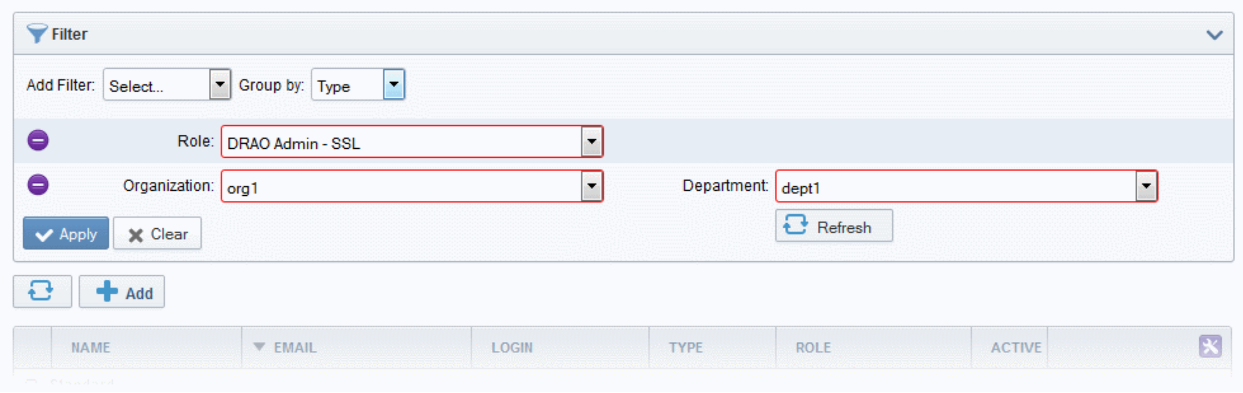


For example if you want to search for DRAO SSL administrators belonging to 'org1' organization and 'dept1' department and group them based on their types:

- Choose 'Role' from the 'Add Filter' drop-down
- Choose 'Organization' from the 'Add Filter' drop-down

The organization and department filters will be displayed.

- Choose 'org1' Organization and 'dept1' Department from the 'Organization' and 'Department' drop-downs respectively
- Choose 'Type' from the 'Group by' drop-down



Filter

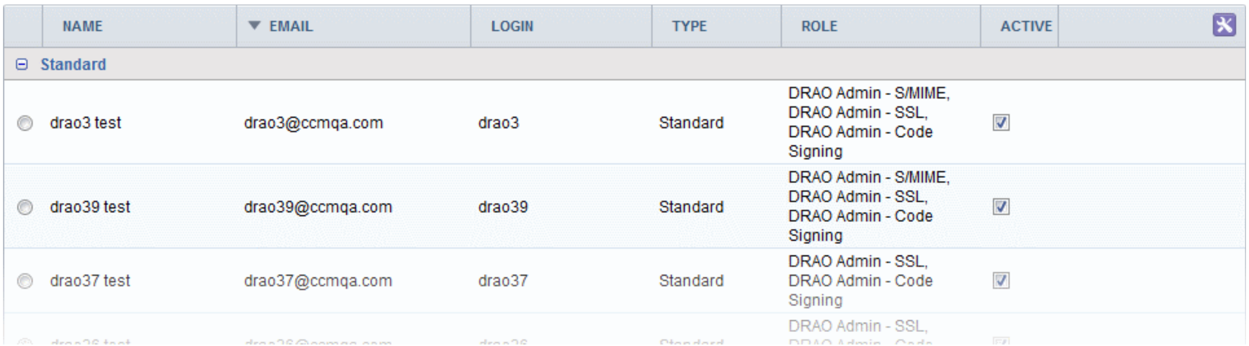
Add Filter: Select... Group by: Type

Role: DRAO Admin - SSL

Organization: org1 Department: dept1

- Click the 'Apply' button.

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



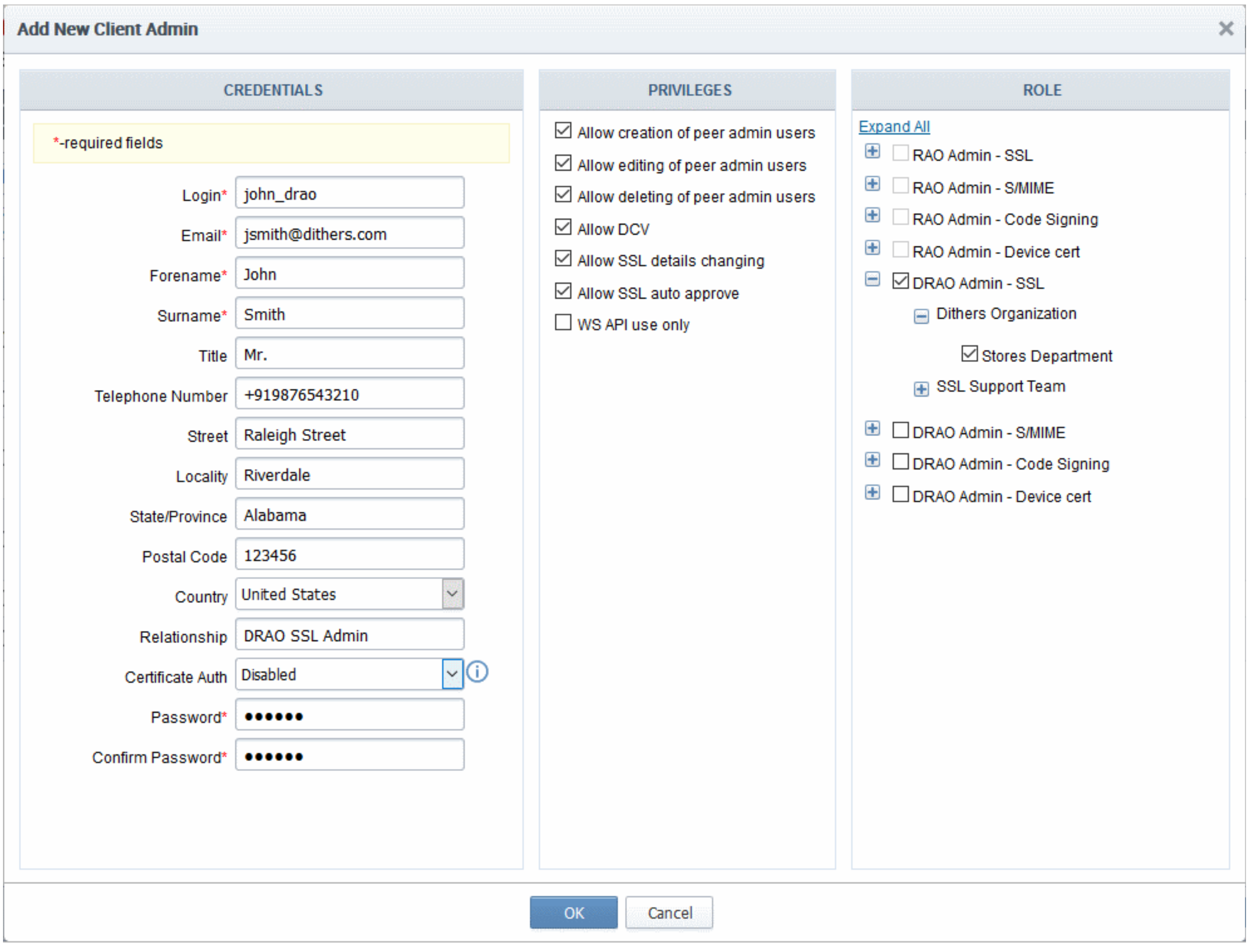
	NAME	EMAIL	LOGIN	TYPE	ROLE	ACTIVE
⊟	Standard					
○	drao3 test	drao3@ccmqa.com	drao3	Standard	DRAO Admin - S/MIME, DRAO Admin - SSL, DRAO Admin - Code Signing	☑
○	drao39 test	drao39@ccmqa.com	drao39	Standard	DRAO Admin - S/MIME, DRAO Admin - SSL, DRAO Admin - Code Signing	☑
○	drao37 test	drao37@ccmqa.com	drao37	Standard	DRAO Admin - SSL, DRAO Admin - Code Signing	☑
○	drao36 test	drao36@ccmqa.com	drao36	Standard	DRAO Admin - SSL, DRAO Admin - Code	☑

- 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.

5.2 Adding Administrators

1. Click the 'Admins' tab at the top 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 ✕

CREDENTIALS

*-required fields

Login*	john_drao
Email*	jsmith@dithers.com
Forename*	John
Surname*	Smith
Title	Mr.
Telephone Number	+919876543210
Street	Raleigh Street
Locality	Riverdale
State/Province	Alabama
Postal Code	123456
Country	United States
Relationship	DRAO SSL Admin
Certificate Auth	Disabled
Password*	••••••
Confirm Password*	••••••

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
- ☐ WS API use only

ROLE

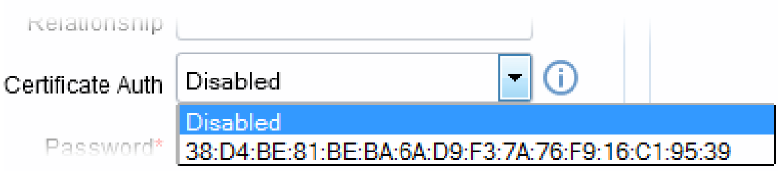
Expand All

- ⊞ ☐ RAO Admin - SSL
- ⊞ ☐ RAO Admin - S/MIME
- ⊞ ☐ RAO Admin - Code Signing
- ⊞ ☐ RAO Admin - Device cert
- ⊟ ☑ DRAO Admin - SSL
  - ⊟ Dithers Organization
    - ☑ Stores Department
  - ⊞ SSL Support Team
- ⊞ ☐ DRAO Admin - S/MIME
- ⊞ ☐ DRAO Admin - Code Signing
- ⊞ ☐ DRAO Admin - Device cert

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

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

Form Element	Type	Description
		Credentials
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	Text Field Text Field Text Field Text Field	Enter the address details of the new administrator.

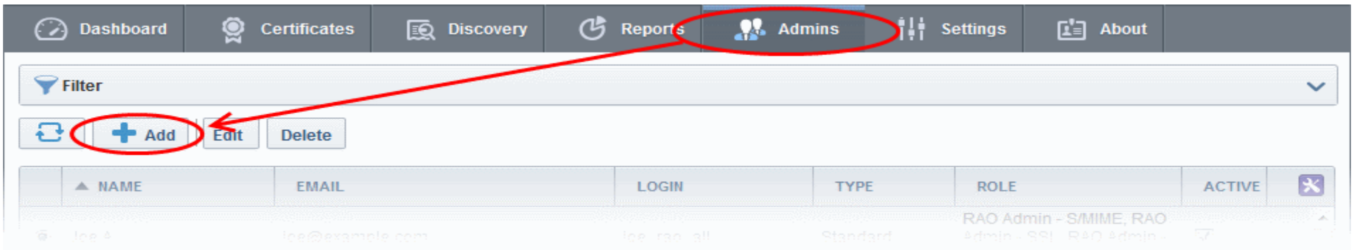
Form Element	Type	Description
Country	Drop-down	
Relationship	Text Field	The role of the new administrator, for example, RAO SSL Administrator.
Certificate Auth	Drop-down	- Enables the administrator to specify whether the new administrator must authenticate themselves to Certificate Manager with his/her 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 Incommon CM for the new administrator, based on his/her email address in the 'Email' field.  Relationship Certificate Auth: Disabled Password* Disabled 38:D4:BE:81:BE:BA:6A:D9:F3:7A:76:F9:16:C1:95:39 - If authentication is needed, the administrator can select the certificate from the drop-down. The new administrator can login to Incommon CM, 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.
Password* Confirm Password*	Text Field Text Field	Enter the password for the new administrator to access the CM interface and reenter the same for confirmation. The new administrator will need to change the password upon his/her first login.
Privileges		
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	Checkbox	Enables the new administrator to add new administrators from their management interface.
Allow editing of peer admin users	Checkbox	Enables the new administrator to edit roles of existing administrators from their management interface.
Allow deleting of peer admin users	Checkbox	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. See descriptions under Administrative Roles in the section Section Overview for more details.		
Allow domain validation without Dual Approval	Checkbox	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

Form Element	Type	Description
		checkbox will be active only for Administrators with MRAO role. See Domains for more details.
Allow DCV	Checkbox	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	Checkbox	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	Checkbox	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.
WS API use only	Checkbox	The administrator account can only be used for API integration. Incommon CM GUI access will not be allowed for this account.
Note: 'Allow domain validation without Dual Approval' and 'Allow DCV' fields will only be visible if the features are enabled for your account.		
Role		
Administrator can assign the role to the new administrator. For more details on the roles, refer to the section Administrative Roles.		
• RAO Admin SSL • RAO Admin S/MIME • RAO Admin Code Signing • DRAO Admin SSL • DRAO Admin S/MIME • DRAO Admin Code Signing	Checkboxes	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 'Expand All' expands the tree structure to display all the Departments under each organization. • Clicking 'Collapse All' in the expanded view collapses the tree structure of all the organizations and hides the departments under each organization.

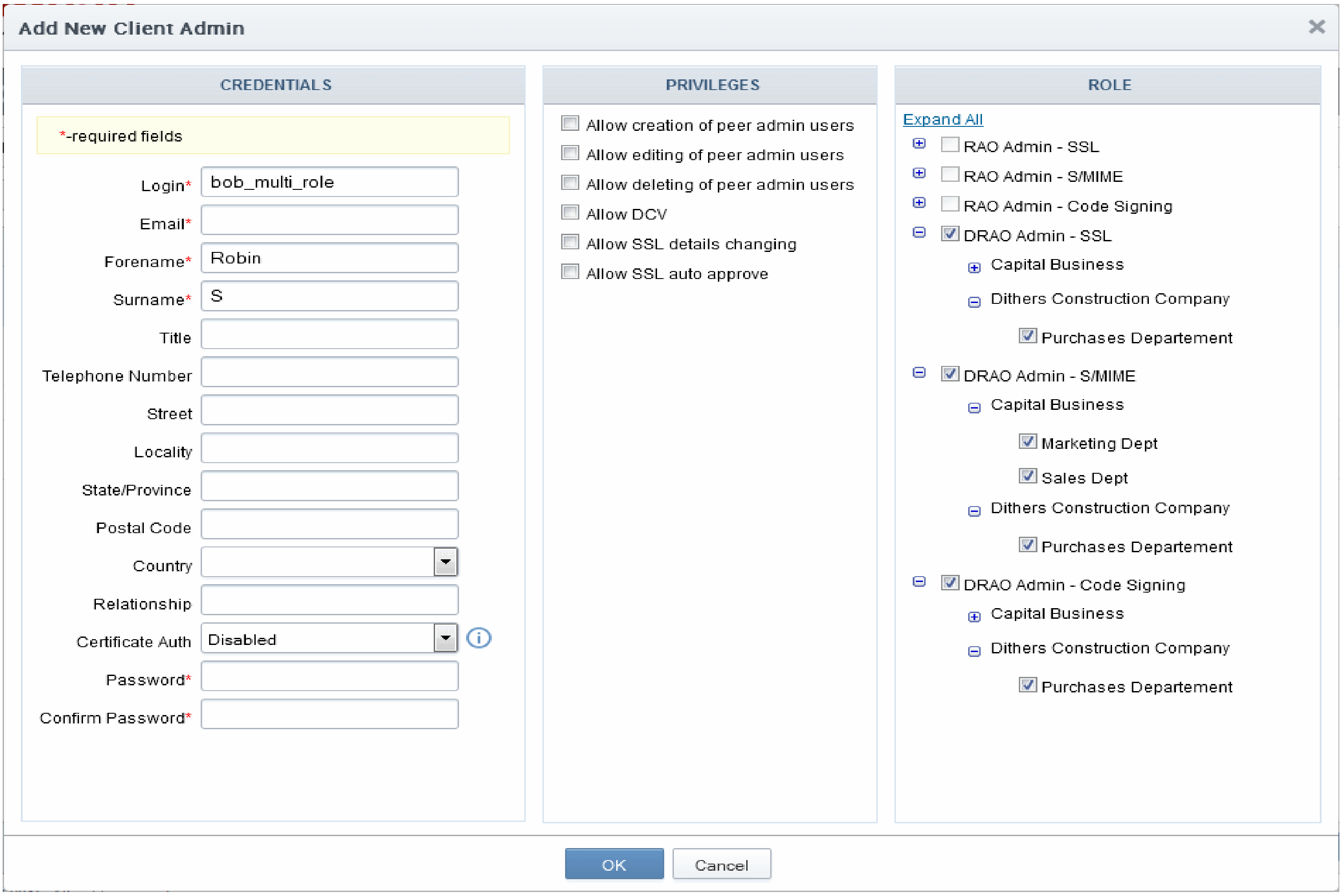
Note: Fields marked with * are mandatory.

5.2.2 Example: Adding a New Administrator with Multiple Security Roles

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

CREDENTIALS

*-required fields

Login*	bob_multi_role
Email*	
Forename*	Robin
Surname*	S
Title	
Telephone Number	
Street	
Locality	
State/Province	
Postal Code	
Country	
Relationship	
Certificate Auth	Disabled
Password*	
Confirm Password*	

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

ROLE

Expand All

- □ RAO Admin - SSL
- □ RAO Admin - S/MIME
- □ RAO Admin - Code Signing
- ☑ DRAO Admin - SSL
  - Capital Business
  - Dithers Construction Company
    - ☑ Purchases Departement
- ☑ DRAO Admin - S/MIME
  - Capital Business
    - ☑ Marketing Dept
    - ☑ Sales Dept
  - Dithers Construction Company
    - ☑ Purchases Departement
- ☑ DRAO Admin - Code Signing
  - Capital Business
  - Dithers Construction Company
    - ☑ Purchases Departement

i. Fill out the contact, login details and password and select the privileges that should apply to the new administrator

ii. Next, you should specify the new administrator's security role:

A new administrator can be:

- RAO Admin SSL - Will be able to manage ONLY SSL certificates and ONLY for selected Organization(s).
- RAO Admin S/MIME - 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 S/MIME - 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).

- DRAO Admin SSL - Will be able to manage ONLY SSL certificates and ONLY for selected Departments(s).
- DRAO Admin S/MIME - 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 S/MIME and RAO Code Signing as required. Similarly, same DRAO can be assigned as RAO SSL, RAO S/MIME 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

iii. Select the Organization/Department to which the new administrator will have access as shown above.

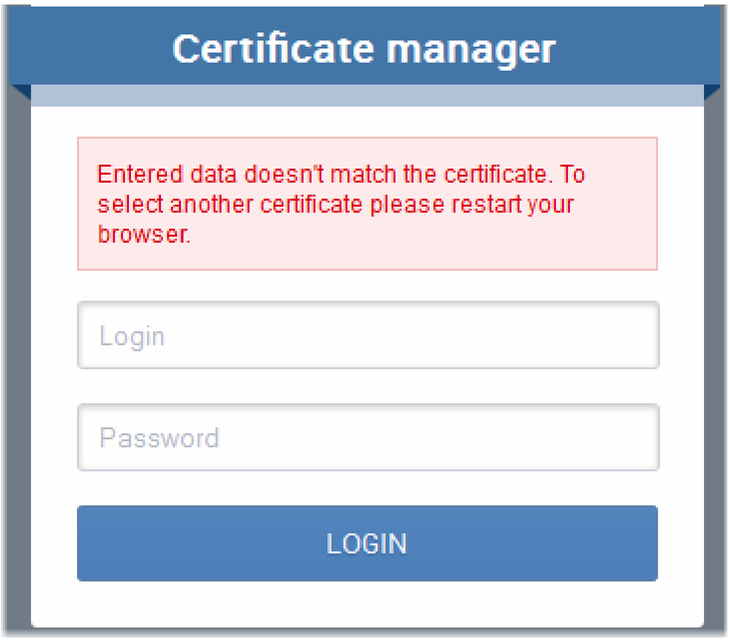
If the single RAO is chosen as RAO SSL, RAO S/MIME and/or RAO Code Signing, he or she can have the multiple privileges only for a particular Organization. Similarly, If the single DRAO is chosen as DRAO SSL, DRAO S/MIME and/or DRAO Code Signing, he or she can have the multiple privileges only for a particular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

iv. Click 'OK' to save all changes and finish the process.

5.2.3 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.


Certificate manager

Entered data doesn't match the certificate. To select another certificate please restart your browser.

If Certificate Manager does not detect the correct authentication certificate during login, an error stating that data doesn't match.

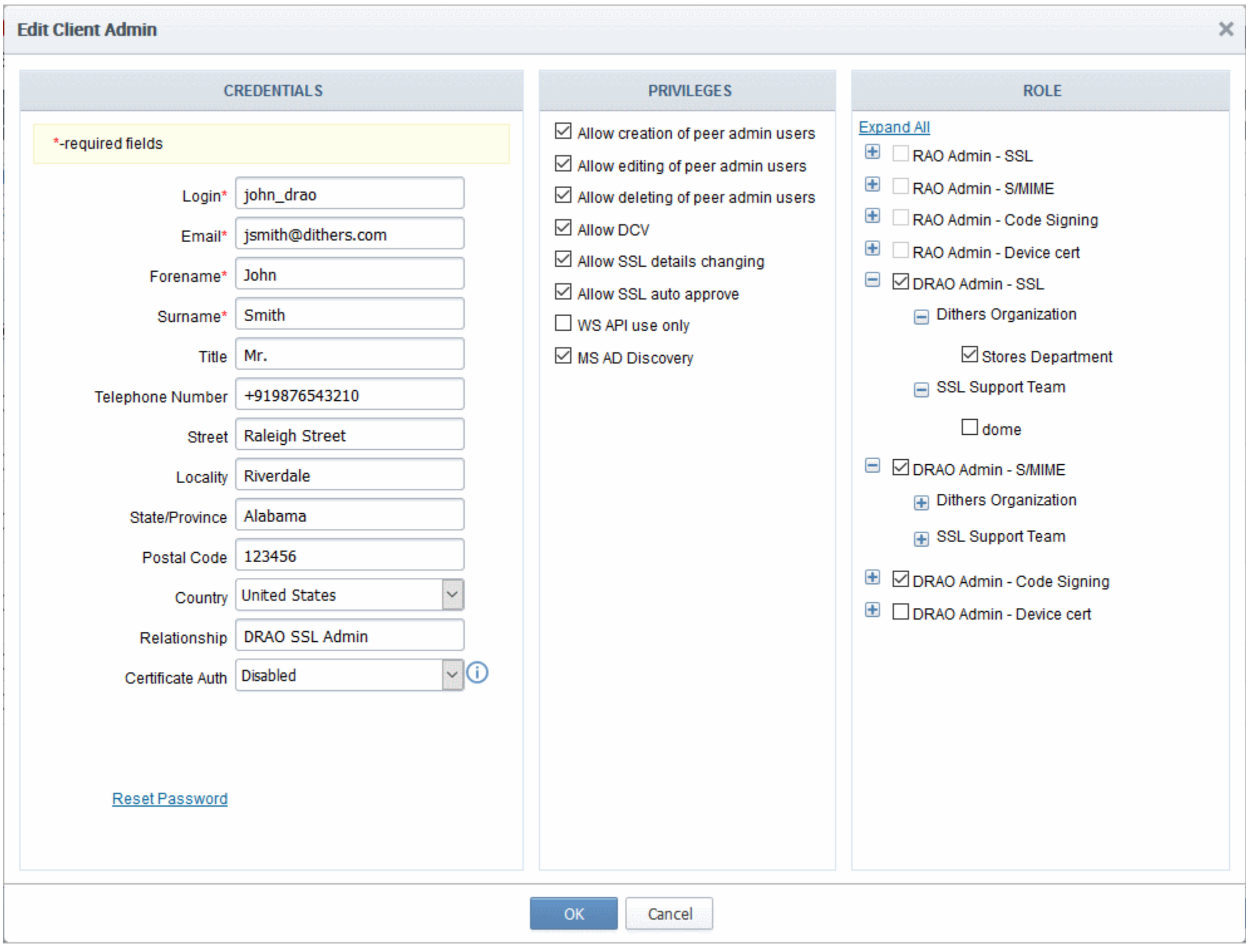
The administrator should restart the browser and select the correct digital certificate when requested at the login page. If the correct certificate is not detected or is not present on the administrator's system then they will not be able to access the Certificate Manager interface.

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'.

5.3 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.



Edit Client Admin

CREDENTIALS

*-required fields

Login*	john_drao
Email*	jsmith@dithers.com
Forename*	John
Surname*	Smith
Title	Mr.
Telephone Number	+919876543210
Street	Raleigh Street
Locality	Riverdale
State/Province	Alabama
Postal Code	123456
Country	United States
Relationship	DRAO SSL Admin
Certificate Auth	Disabled

Reset Password

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
- ☐ WS API use only
- ☑ MS AD Discovery

ROLE

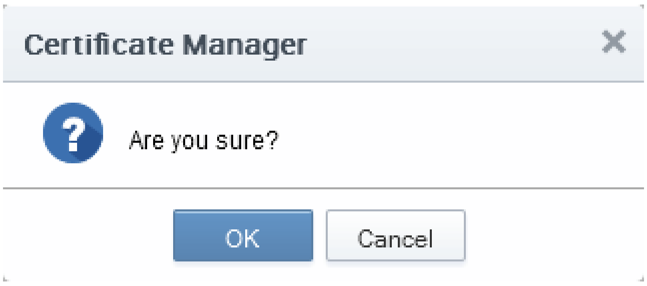
Expand All

- ☐ RAO Admin - SSL
- ☐ RAO Admin - S/MIME
- ☐ RAO Admin - Code Signing
- ☐ RAO Admin - Device cert
- ☑ DRAO Admin - SSL
  - Dithers Organization
    - ☑ Stores Department
  - SSL Support Team
    - ☐ dome
- ☑ DRAO Admin - S/MIME
  - Dithers Organization
  - SSL Support Team
- ☑ DRAO Admin - Code Signing
- ☐ DRAO Admin - Device cert

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

5.4 Deleting an Administrator

Appropriately privileged administrators can delete peer administrators or administrators of next hierarchy level by selecting them and clicking the 'Delete' button at the top.

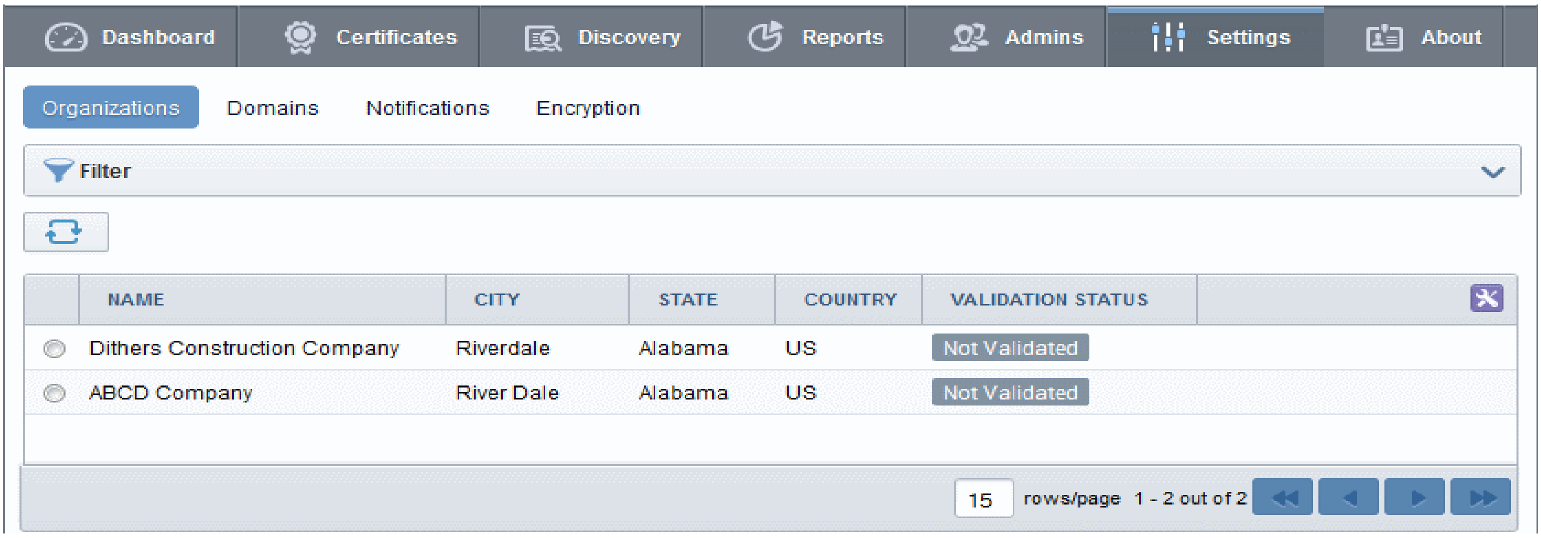


- Click 'OK' to delete the Administrator.

6 Settings

6.1 Overview

The 'Settings' area contains several tabs relating to the overall configuration of CM. The number of tabs that are visible to a particular administrator is dependent on their security role.



	NAME	CITY	STATE	COUNTRY	VALIDATION STATUS
○	Dithers Construction Company	Riverdale	Alabama	US	Not Validated
○	ABCD Company	River Dale	Alabama	US	Not Validated

- **Organizations** - Visible only to RAO class administrators. RAOs can view, edit, request new domains and add Departments to Organizations that have been delegated to them.
- **Departments** - Visible only to DRAO class administrators (DRAO's see a 'Departments' tab instead of the 'Organizations' tab). Allows DRAOs to view all departments that have been delegated to them and to request new domains for those departments.

- **Domains** - RAO class administrators can view the domains belonging to their organization; can delegate domains to departments and can request new domains for their organization. DRAOs can view existing domains and request the addition of new ones.
- **Notifications** - Define email notifications to specific personnel based on a range of criteria and triggers.
- **Encryption** - Visible only to RAO/DRAO S/MIME administrators. Allows administrators to initialize a new master key pair or to re-encrypt the private keys of client certificates held in escrow. **Note:** S/MIME administrators are strongly advised to familiarize themselves with the information in this section.
- **InCommon CM Agents** - Enables admins to download Network agents, view existing agents, modify agent settings and auto-install SSL certificates. Once installed, network agents can discover SSL certificates and auto-install certificates.
- **Assignment Rules** - Allows RAO/DRAO admins to create rules which will assign certificates found during a discovery scan to a specific organization or department.

6.2 Organizations

6.2.1 Section Overview

The 'Organizations' area allows RAO class administrators to view and manage their delegated Organizations and any Departments of that Organization. From here, RAOs can:

- Edit the way their Organization issues certificates
- Modify the content of email notifications that are issued on behalf of their Organization
- Create, Edit or Delete Departments of that Organization
- Request the addition of new Domains for their Organization
- Delegate existing Domains to any Organization or Department that they control

'Organizations' and 'Departments' and the delegation of domains to these entities is crucial to the issuance and effective management of SSL, code signing and S/MIME certificates via the Certificate Manager interface. Each Organization can have multiple Departments. 'Organizations' can only be managed by an RAO administrators whereas 'Departments' can be managed by a dedicated DRAO administrator or by the RAO.

Note: DRAO class administrators cannot view or access the 'Organizations' area - they see the 'Departments' area instead.

Summary:

- Organizations are umbrella entities for the purposes of requesting, issuing and managing certificates for domains and employees.
- Each Organization can have multiple Departments. Furthermore, each Organization and each Department can have multiple domains delegated to it.
- RAO class administrators can manage all certificates (of the type that they have privileges for), domains and users belonging to their Organization and any of its sub-Departments. They are also able to create new Departments and appoint DRAO administrators.
- RAO class administrators can request that certificates be issued to domains that have been delegated to their Organization. They can also approve/decline certificate requests from individuals using the external application form.

  - RAO SSL administrators can manage SSL certificates for their Organization/Departments via the 'Certificate Managements - SSL Certificates' area.
  - RAO Code Signing administrators can manage Code Signing Certificates for their Organization/Departments from the 'Code Signing' area.
  - RAO S/MIME administrators can manage the client certificates of end-users belonging to their Organization/Departments via the 'Certificates Management - Client Certificates' area.
- 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.
- 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.
- RAO and DRAO SSL administrators can utilize the Certificate Discovery feature to audit a network for the presence of SSL certificates then assign any unmanaged certificates to their Organization or Department.
- Reports can be run, viewed and exported for an Organization or Department

CM Entity	Administrator Types
Organization	RAO Administrator - SSL RAO Administrator - S/MIME RAO Administrator - Code Signing Certificates
Department	RAO Administrator - SSL RAO Administrator - S/MIME RAO Administrator - Code Signing Certificates DRAO Administrator - SSL DRAO Administrator - S/MIME DRAO Administrator - Code Signing Certificates

Although we strongly advise administrators to carefully plan any Organizational and administrative structure beforehand, it is, of course, possible to rearrange and tweak your structure at a later date. Organizations, Departments, Domains and Administrators are each created and configured as independent entities in CM. 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 InCommon account manager.

6.2.1.1 Example Scenarios

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

- You can delegate the same domain to multiple departments
- You can delegate multiple admins to a single department
- You cannot delegate domains directly to admins

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 CM:

Example 1:

Scenario: You wish to issue only SSL certificates for a single first level domain and two sub-domains.

Solution 1 - Simple: Certificates for all domains are delegated to the organization and managed by a single RAO SSL admin

- Request the creation of an RAO SSL admin if one does not already exist
- Do not create any DRAO SSL admins
- Do not create any departments
- Delegate the domain and all sub-domains your organization

Organization Name	Organization Admin(s)	Department Name / Department Admin	Domains
Your Organization	RAO SSL	-	http://website_1.com
			http://secure.website_1.com
			http://mail.website_1.com

Solution 2 - Simple: Create three departments and delegate a domain to each one. Create a single DRAO SSL admin to manage all departments.

- Request the creation of an RAO SSL admin if one does not already exist
- Create and approve a DRAO SSL admin
- Create three departments
- Delegate each domain to a separate department

Delegate the DRAO SSL to manage all three departments

Organization Name	Organization Admin(s)	Department Name / Department Admin		Domains
Your Organization	RAO SSL	Department 1	DRAO SSL	http://website_1.com
		Department 2		http://secure.website_1.com
		Department 3		http://mail.website_1.com

Solution 3 - Intermediate: Create three departments and delegate a domain to each one. Create three DRAO SSL admins to manage each of the departments.

- Request the creation of an RAO SSL admin if one does not already exist
- Create and approve three DRAO SSL Admins
- Create three departments
- Delegate each domain to one of these departments
- Delegate one DRAO SSL Admin to each of the departments

Organization Name	Organization Admin(s)	Department Name / Department Admin	Domains
Your Organization	RAO SSL	Department 1 / DRAO SSL 1	http://website_1.com
		Department 2 / DRAO SSL 2	http://secure.website_1.com
		Department 3 / DRAO SSL 3	http://mail.website_1.com

Example 2:

Scenario: Your company issues both SSL certificates and S/MIME certificates. Your company operates 2 distinct websites, each with it's own unique first level domain name and two sub-domains.

Solution 1 - Simple:

- Request the creation of one RAO SSL admin and one RAO S/MIME admin if they do not already exist
- Do not create any DRAO class admins
- Do not create any Departments
- Delegate both first level domains and all sub-domains to your organization
- The RAO SSL admin manages all SSL certificates for all domains
- The RAO S/MIME admin manages all Client Certificates for all domains

Organization Name	Organization Admin(s)	Department Name / Department Admin	Domains
Your Organization	RAO SSL RAO S/MIME	-	http://website_1.com
			http://secure.website_1.com
			http://mail.website_1.com
			http://website_2.com
			http://secure.website_2.com
			http://mail.website_2.com

Solution 2 - More sophisticated:

- Request the creation of one RAO SSL admin and one RAO S/MIME admin if they do not already exist
- Create four Departments

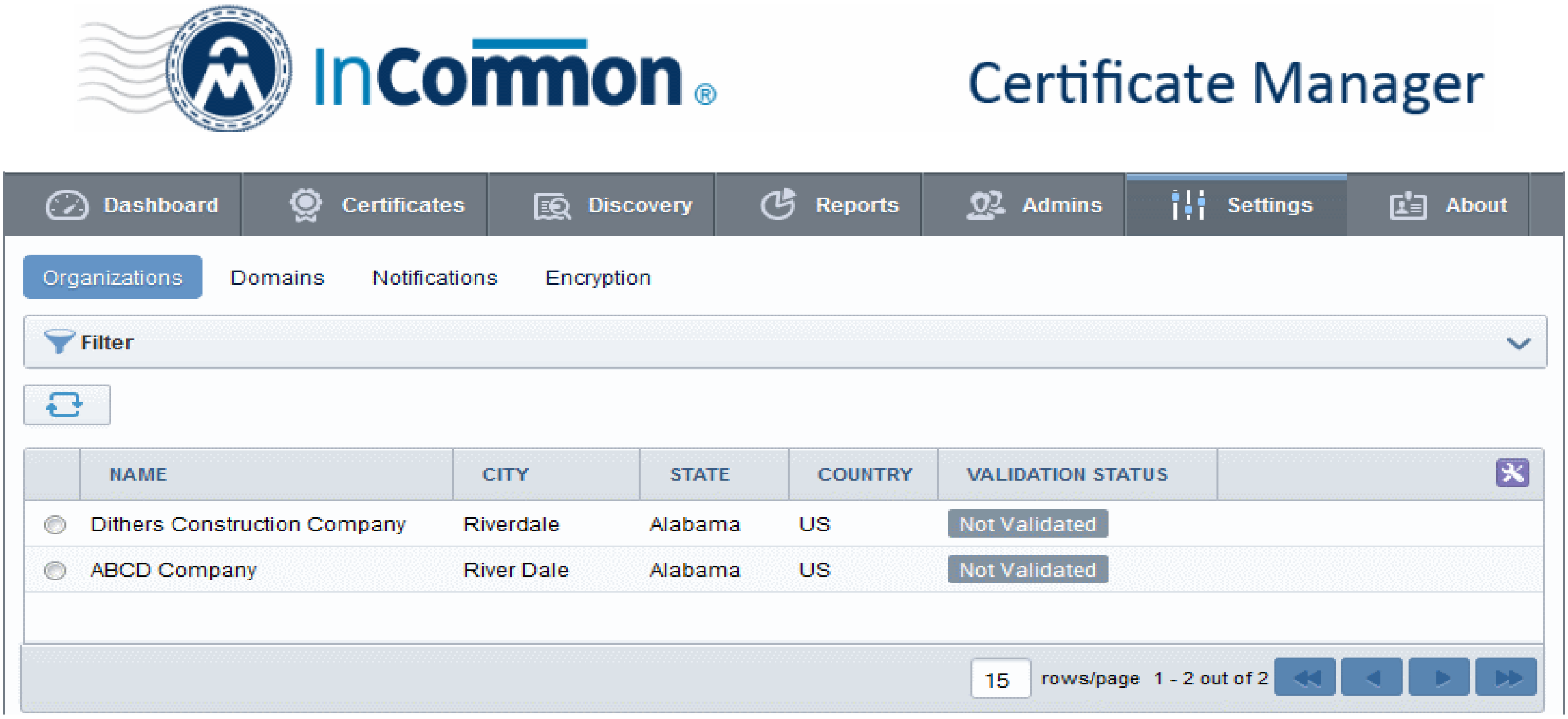
- Create four DRAO SSL admins
- Create two DRAO S/MIME admins
- Delegate the top level Domain and the two sub-domains of website #1 each to a separate Department. Assign a DRAO SSL admin to each of these departments.
- Delegate the top level Domain and the two sub-domains of website #2 all to Department 4. Assign the remaining DRAO SSL admin to this fourth department.
- Delegate one DRAO S/MIME as administrator of Departments 1,2 and 3. Delegate the other DRAO S/MIME as admin of department 4

Organization Name	Organization Admin(s)	Department Name / Department Administrator		Domains
Your Organization	RAO SSL	Department 1	DRAO SSL 1	http://website_1.com
		Department 2	DRAO SSL 2	http://secure.website_1.com
		Department 3	DRAO SSL 3	http://mail.website_1.com
		Department 4	DRAO SSL 4	http://website_2.com http://secure.website_2.com http://mail.website_2.com
	RAO S/MIME	Department 1	DRAO S/MIME 1	http://website_1.com
		Department 2		http://secure.website_1.com
		Department 3		http://mail.website_1.com
		Department 4	DRAO S/MIME 2	http://website_2.com http://secure.website_2.com http://mail.website_2.com

6.2.2 Organization Management

6.2.2.1 Organizations Area Overview

To open the 'Organizations' management area, click the 'Organizations' sub-tab under the 'Settings' tab. The 'Organizations' tab is not visible to a DRAO (they see the 'Departments' tab instead).



	NAME	CITY	STATE	COUNTRY	VALIDATION STATUS
○	Dithers Construction Company	Riverdale	Alabama	US	Not Validated
○	ABCD Company	River Dale	Alabama	US	Not Validated

15 rows/page 1 - 2 out of 2

This area:

- Lists all Organizations available to an RAO admin
- Allows RAO and DRAO admins to modify certificate settings and email templates for their organization and/or Department
- Allows RAO admins to request new and delegate existing domains to an organization or department
- Allows RAO admins to search and filter organizations by Name and Department.

Administrative Roles:

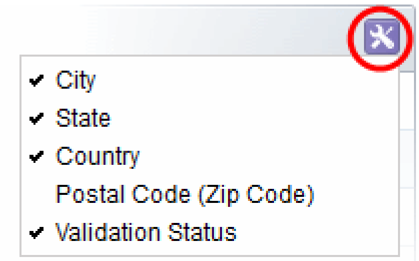
- RAO Administrators - Can only see their own Organization(s) in the 'Organizations' area. They cannot create new organizations but can manage and create departments for the organization(s) that has/have been delegated to them.
- DRAO Administrators cannot view the 'Organizations' area. They have visibility 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:

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

6.2.2.2 Summary of Fields and Controls

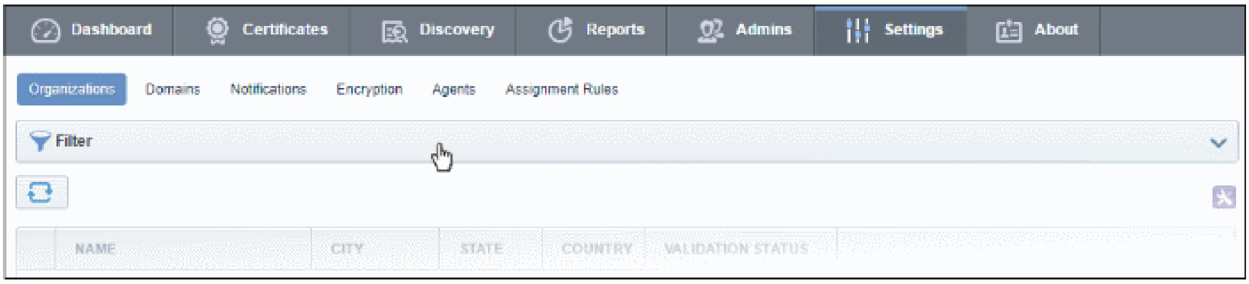
Column Display	Description	
Name	String	Name of the organization
City	String	Name of the City where the organization is located

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	Indicates whether the Organization has been validated by the [Master Administrator]().
Note: An administrator can enable or disable the columns from the drop-down button beside the last item in the column:  ✓ City ✓ State ✓ Country Postal Code (Zip Code) ✓ Validation Status		
Control Buttons	Refresh	Updates the list of displayed organizations.
Organization Control Buttons **Note**: The Organization control buttons appear only on selecting an Organization	Edit	Enables administrators to modify Client, SSL and Code Signing Certificate settings pertaining to an existing organization.
	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.

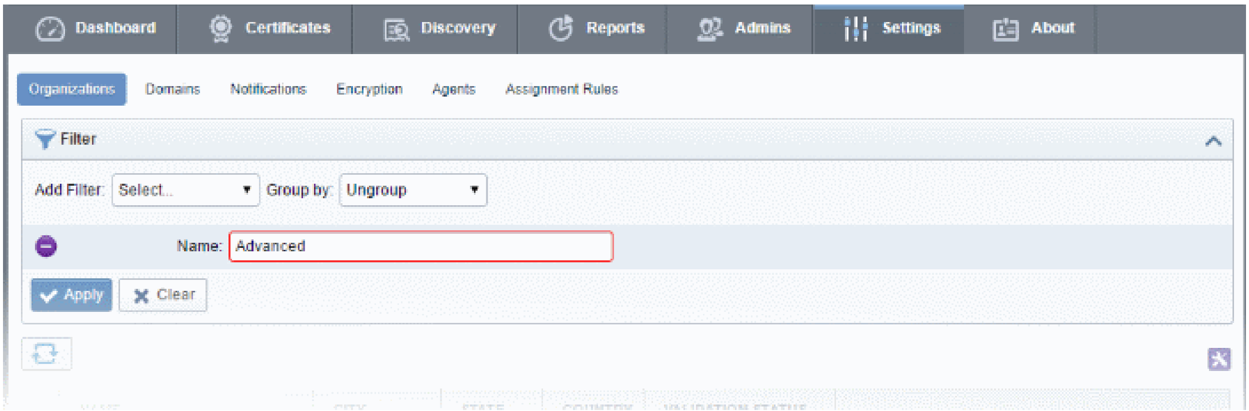
6.2.2.3 Sorting and Filtering Options

- Clicking 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 the filters.



- To apply filters, anywhere on the 'Filters' stripe. The filter options will be displayed.
- 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.



Add Filter: Select... Group by: Ungroup

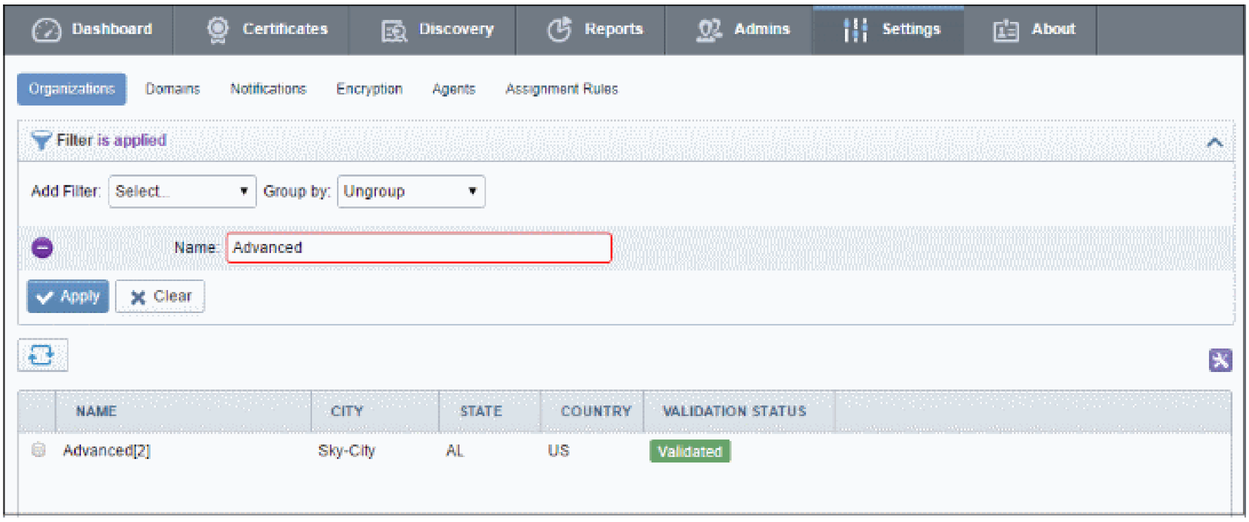
Name: Advanced

- Enter part of or full name in the 'Name' field and 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.



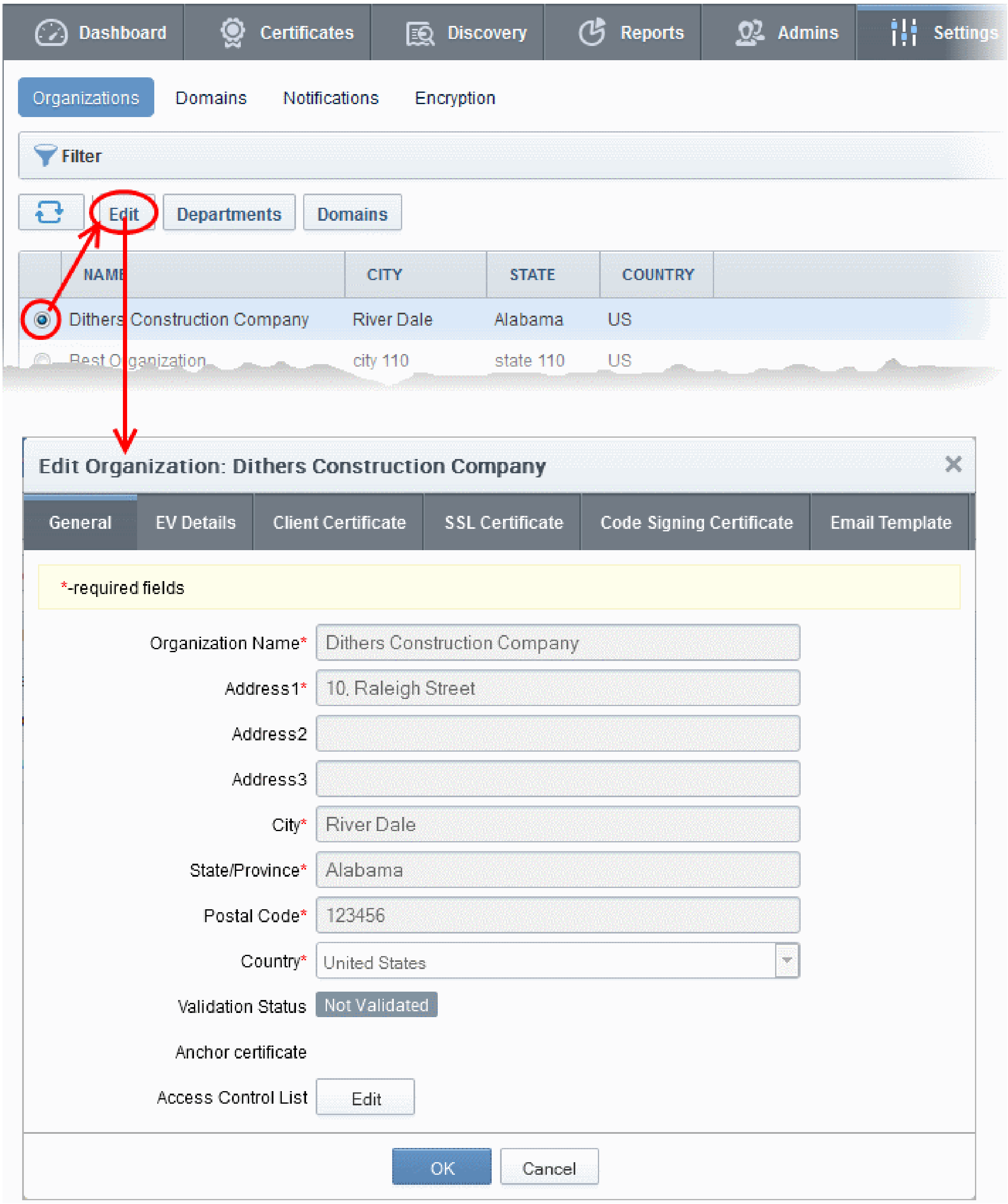
Add Filter: Select... Group by: Ungroup

Name: Advanced

NAME	CITY	STATE	COUNTRY	VALIDATION STATUS
Advanced[2]	Sky-City	AL	US	Validated

6.2.2.4 Editing an Organization

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



NAME	CITY	STATE	COUNTRY
● Dithers Construction Company	River Dale	Alabama	US
○ Best Organization	city 110	state 110	US

Edit Organization: Dithers Construction Company

*-required fields

Organization Name*	Dithers Construction Company
Address1*	10, Raleigh Street
Address2	
Address3	
City*	River Dale
State/Province*	Alabama
Postal Code*	123456
Country*	United States
Validation Status	Not Validated
Anchor certificate	
Access Control List	Edit

The dialog enables the RAO and DRAO Administrators to modify certificate and email settings for their organization or department. The precise functionality available in this dialog depends on the type of RAO administrator that is logged in:

- RAO S/MIME admins see 'General Settings', 'Client Cert' and 'E-mail Template' tabs
- RAO SSL admins see 'General Settings'', 'SSL' and 'E-mail Template' tabs

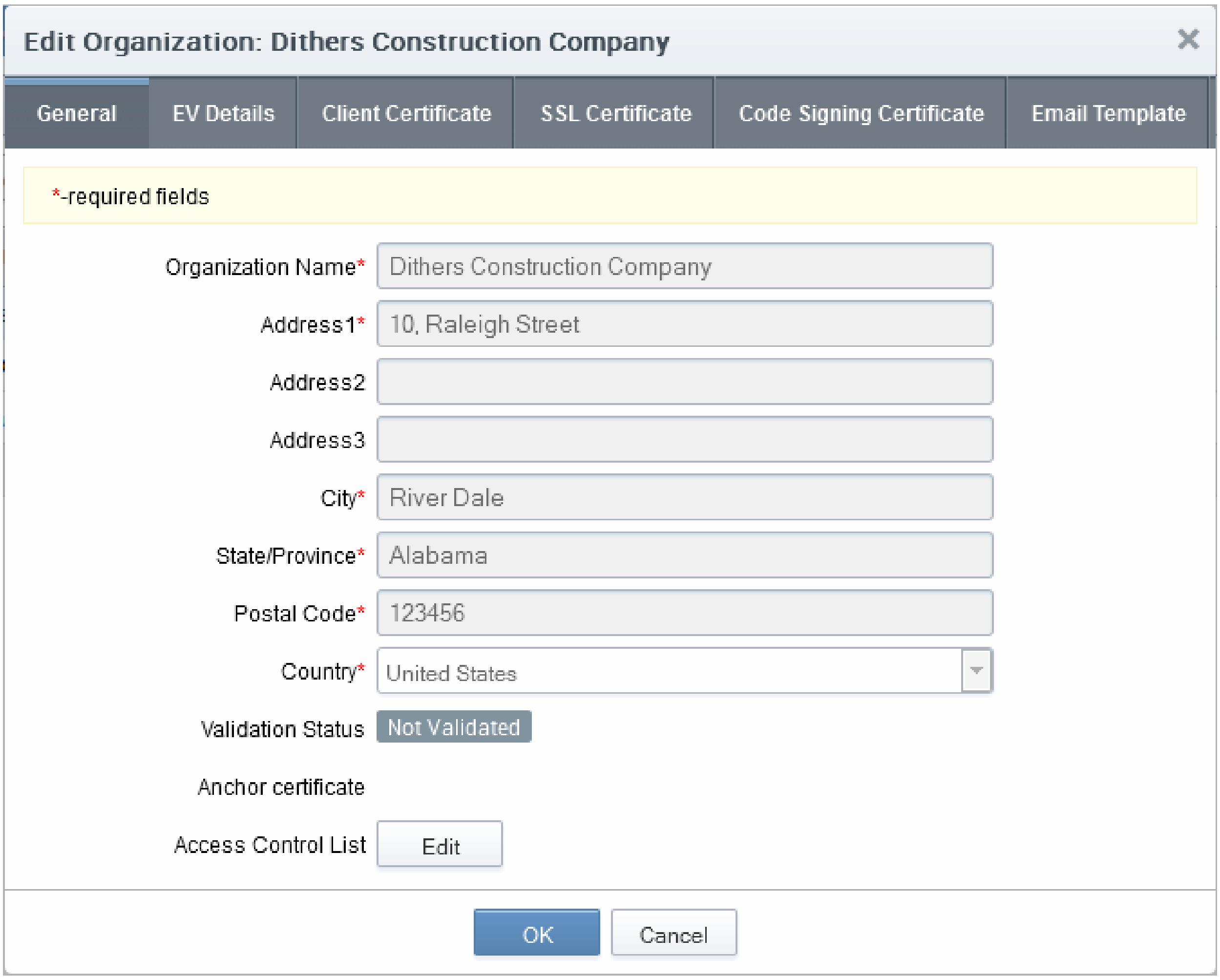
- RAO Code Signing admins see 'General Settings', 'Code Signing Certificate' and 'E-mail Template' tabs

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

6.2.2.4.1 General Settings

RAO and DRAO Administrators cannot edit the name and address details in the 'General' settings relating to an organization/department. Please contact the Master Administrator at InCommon CA should your company wish these details to be altered.

Note: The Master Administrator at InCommon is the person responsible for approving requests made by RAO and DRAO administrators. This includes approving requests for creating new domains; delegating domains to organizations and requests for new SSL and Code Signing Certificates. The Master Administrator also initiates the process for validating an organization and departments under it for the request and issuance of OV SSL certificates.



Edit Organization: Dithers Construction Company

*-required fields

Organization Name*	Dithers Construction Company
Address1*	10, Raleigh Street
Address2	
Address3	
City*	River Dale
State/Province*	Alabama
Postal Code*	123456
Country*	United States
Validation Status	Not Validated
Anchor certificate	
Access Control List	Edit

- **ACL**: Enables the administrator to configure and limit incoming access to the CM 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 CM 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.

6.2.2.4.1.1 Imposing Access Restrictions to CM interface

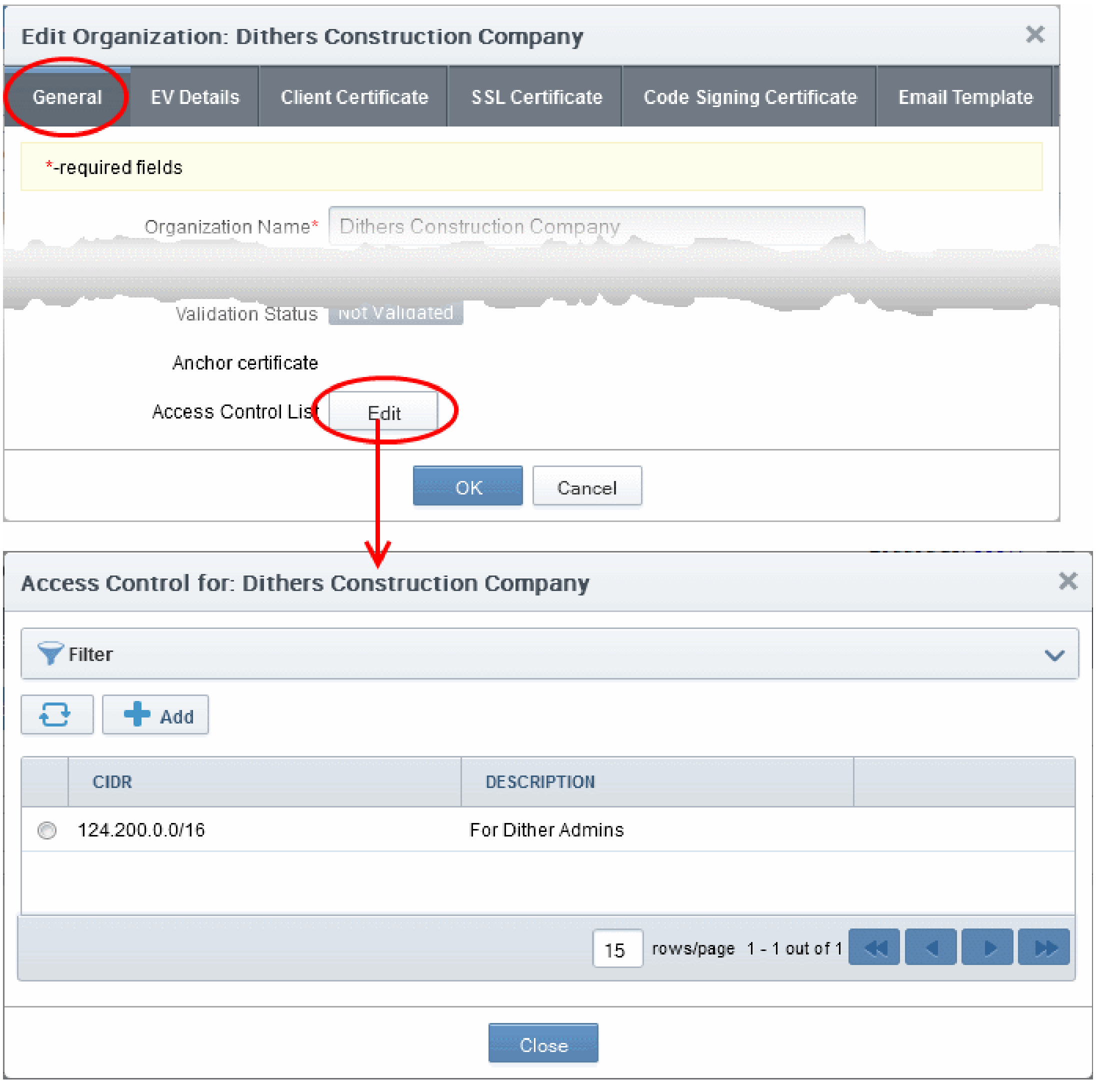
Security Roles:

- RAO - can impose access restrictions to CM 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 - can impose access restrictions to CM 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 CM interface

- Click the 'Edit' beside 'Access Control List' under the 'General' tab of the 'Edit Organization' dialog.

The 'Access Control for...' dialog will appear.



Edit Organization: Dithers Construction Company

*-required fields

Organization Name* Dithers Construction Company

Validation Status Not Validated

Anchor certificate

Access Control List Edit

Access Control for: Dithers Construction Company

	CIDR	DESCRIPTION	
○	124.200.0.0/16	For Dither Admins	

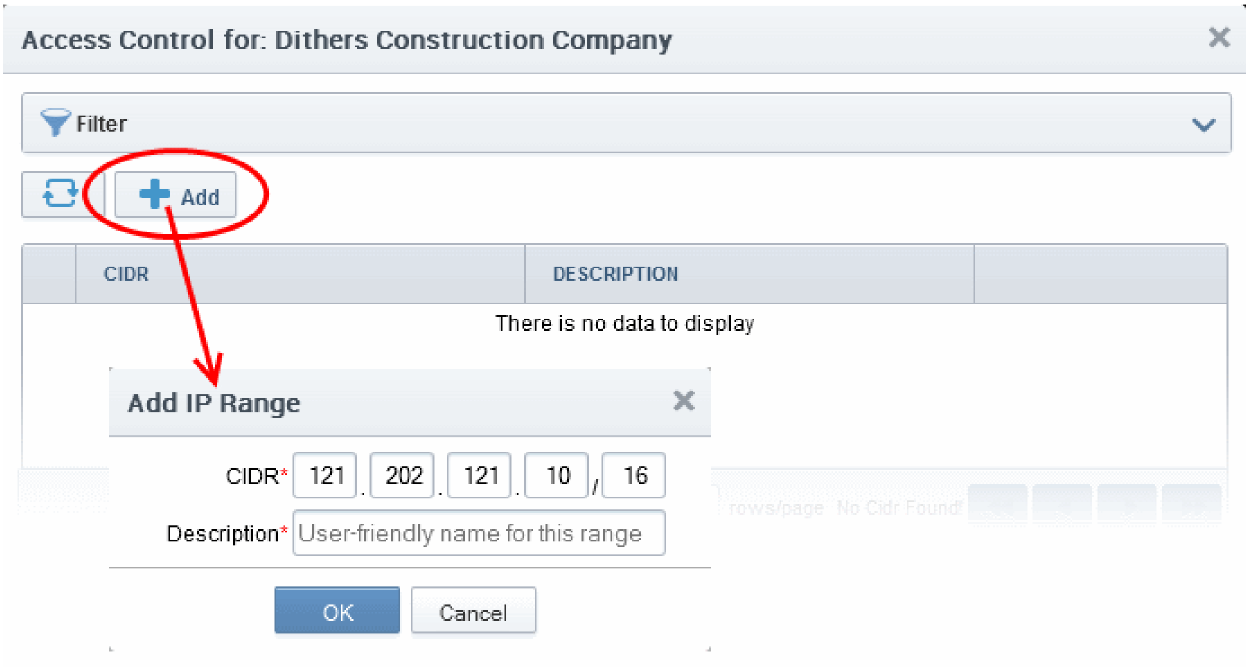
15 rows/page 1 - 1 out of 1

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.

Controls	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.



Access Control for: Dithers Construction Company

Add IP Range

CIDR* 121 . 202 . 121 . 10 / 16

Description* User-friendly name for this range

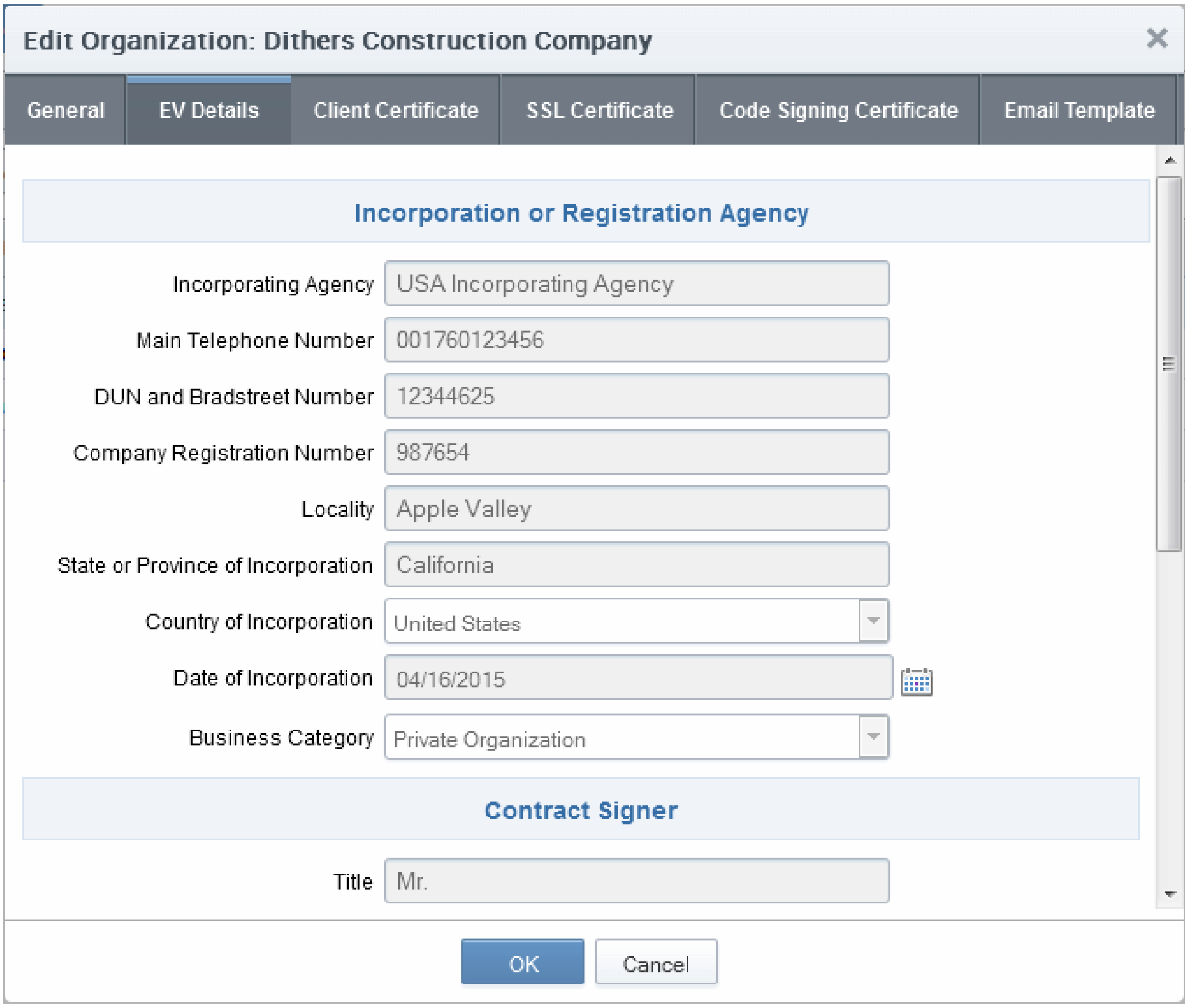
- Enter the IP range, followed by network prefix, e.g. 123.456.78.91/16.
- Enter a short description for the IP range
- Click OK.

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

6.2.2.4.2 EV Details Tab

RAO and DRAO Administrators cannot edit the details in the 'EV Details' tab relating to an organization/department. Please contact the Master Administrator at InCommon should your company wish these details to be altered.

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



Edit Organization: Dithers Construction Company

Incorporation or Registration Agency

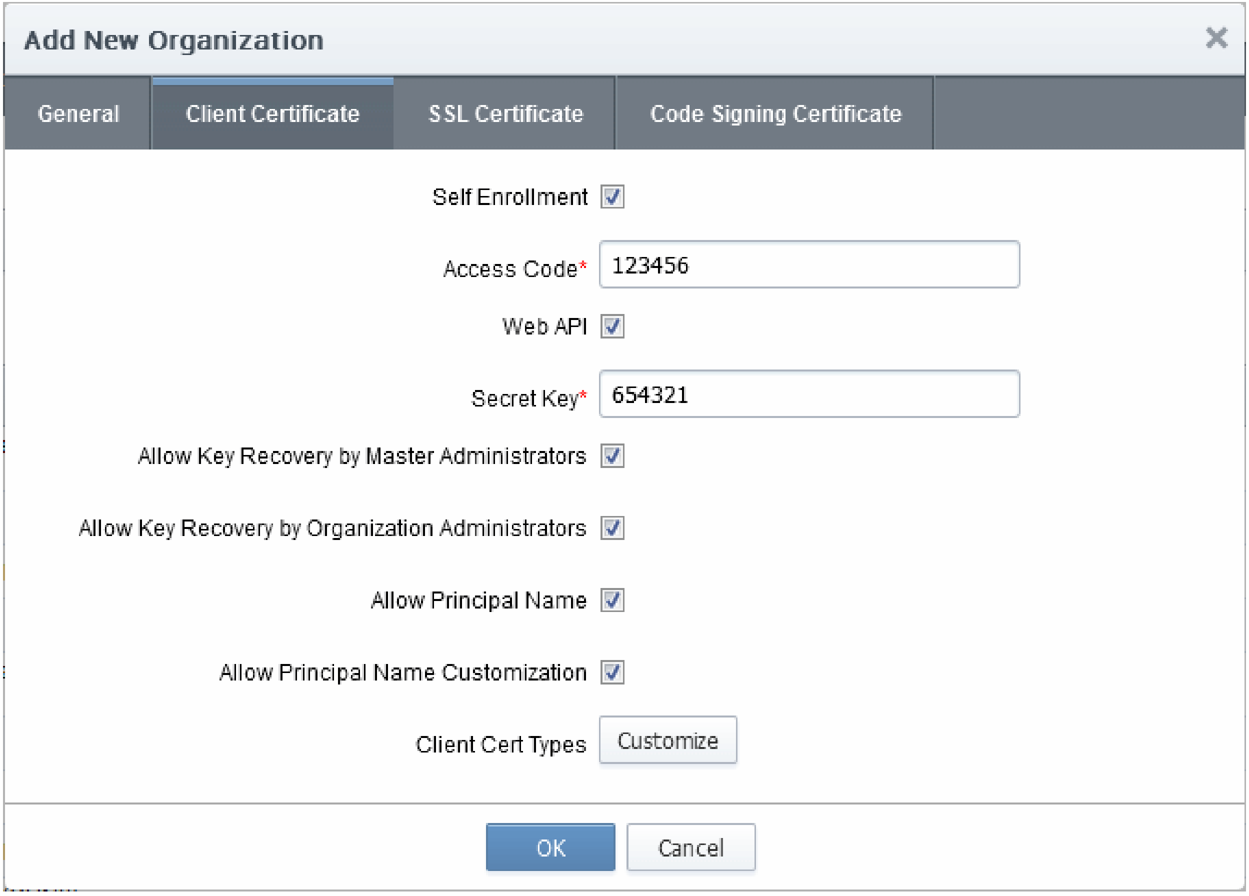
Incorporating Agency	USA Incorporating Agency
Main Telephone Number	001760123456
DUN and Bradstreet Number	12344625
Company Registration Number	987654
Locality	Apple Valley
State or Province of Incorporation	California
Country of Incorporation	United States
Date of Incorporation	04/16/2015
Business Category	Private Organization

Contract Signer

Title	Mr.

6.2.2.4.3 Client Cert Settings Tab

The 'Client Cert' tab allows RAO S/MIME administrators to configure enrollment and term settings relating to 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.



Self Enrollment ☑

Access Code* 123456

Web API ☑

Secret Key* 654321

Allow Key Recovery by Master Administrators ☑

Allow Key Recovery by Organization Administrators ☑

Allow Principal Name ☑

Allow Principal Name Customization ☑

Client Cert Types

6.2.2.4.4 Client Cert Settings - Table of Parameters

Field Name	Type	Description
Self Enrollment	*Check-box* *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://cert-manager.com/customer/InCommon/smime?action=enroll&swt=ac . 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 forms 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).
Access Code (Appears only if the 'Self Enrollment' check-box is selected)	*String* ***(Required)***	**Access Code** - To authenticate the certificate application, applicants are required to provide an access code at the Client Certificate Self Enrollment Form. The RAO administrators can modify the Access Code set by the Master Administrator while creating the organization and should choose a complex access code containing a mixture of alpha and numeric characters that cannot be easily guessed. This access code should be conveyed to the applicant(s) along with the URL of the sign up form.

Field Name	Type	Description
Web API	*Check-box* • *Default state - not checked*	Checking this box enables certificate enrollment through the WebService API. This requires a special agreement with InCommon. For detailed instructions please refer to Web API documentation.
Secret Key (Appears only if the 'Web API' check-box is selected)	*String*	The Secret key is a phrase that is unique to the organization. This phrase restricts access for enrolling certificates for that organization.
Allow Key Recovery by Master Administrator	*Check-box* *Default state - checked* •	If selected, the Master 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 Master Administrator's 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 Master Administrator 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	*Check-box* *Default state - checked* *Not modifiable*	• 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.
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. See 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.. • 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. RAO S/MIME and DRAO S/MIME Administrators should seek the advice of the Master Administrator.

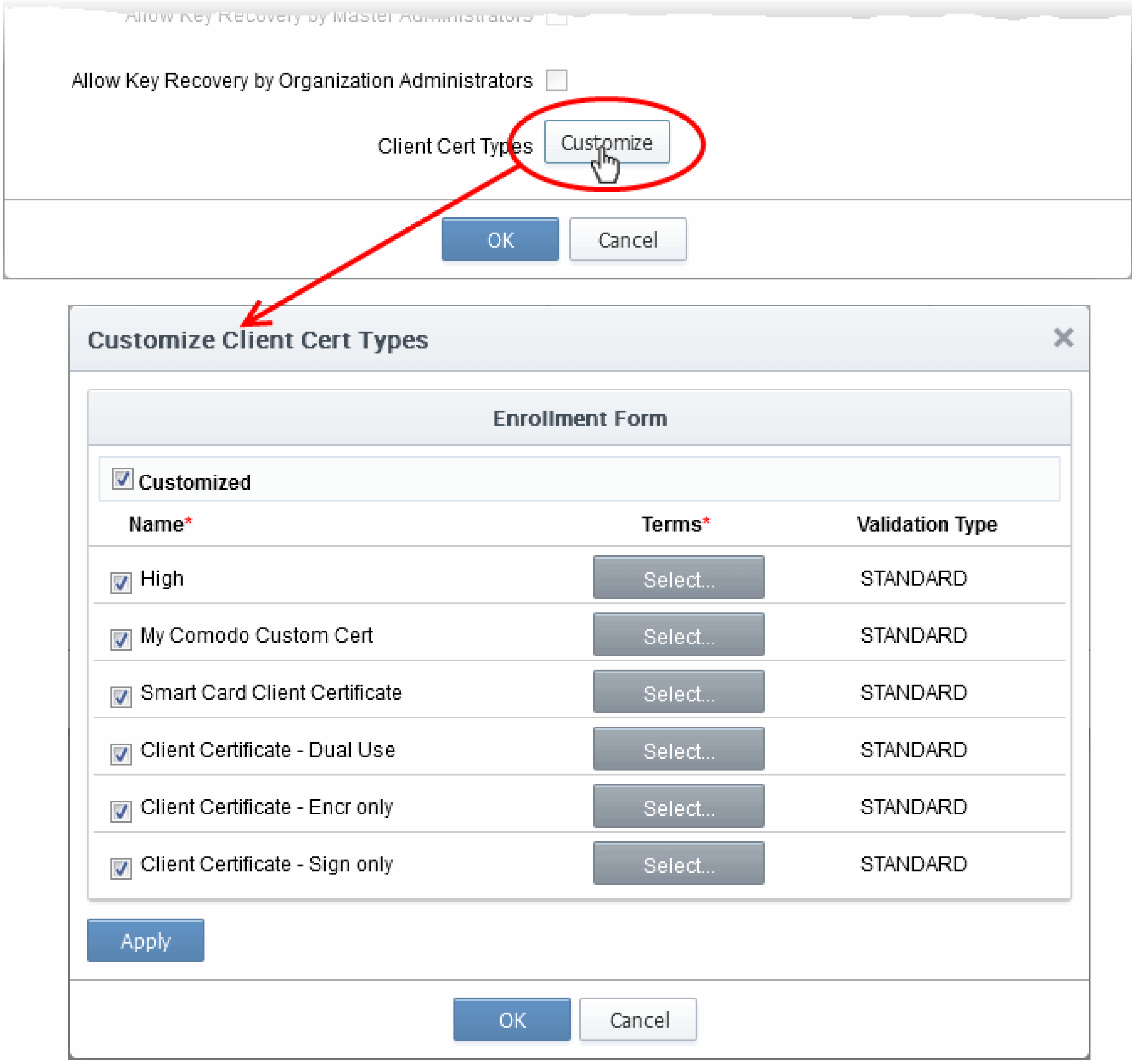
6.2.2.4.4.1 Customize an Organization's Client Certificate Types

Security Roles:

- RAO S/MIME - Can customize client certificate type availability only for the organizations and the departments belonging to the organizations that are delegated to them.
- DRAO S/MIME - 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 'Customize 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 an organization.

- Comodo offers different types of Client certificates for different purposes. For example, 'Signing Only', 'Encryption Only', 'Dual Use' (Signing + Encryption), 'Smart Card Logon and Authentication' and more.
- Contact your Master Administrator for details about the types of client certificates enabled for your account.
- It also possible to create custom client certificate types with combinations of capabilities depending on the requirements of your organization. To do so, click 'Settings' > 'Organizations' > select an organization in the list > Click the 'Edit' button > 'Client Certificates' tab > Click the 'Customize' button:



Allow Key Recovery by Master Administrators □

Allow Key Recovery by Organization Administrators □

Client Cert Types Customize

Customize Client Cert Types

Enrollment Form

☑ Customized

Name*	Terms*	Validation Type
☑ High	Select...	STANDARD
☑ My Comodo Custom Cert	Select...	STANDARD
☑ Smart Card Client Certificate	Select...	STANDARD
☑ Client Certificate - Dual Use	Select...	STANDARD
☑ Client Certificate - Encr only	Select...	STANDARD
☑ Client Certificate - Sign only	Select...	STANDARD

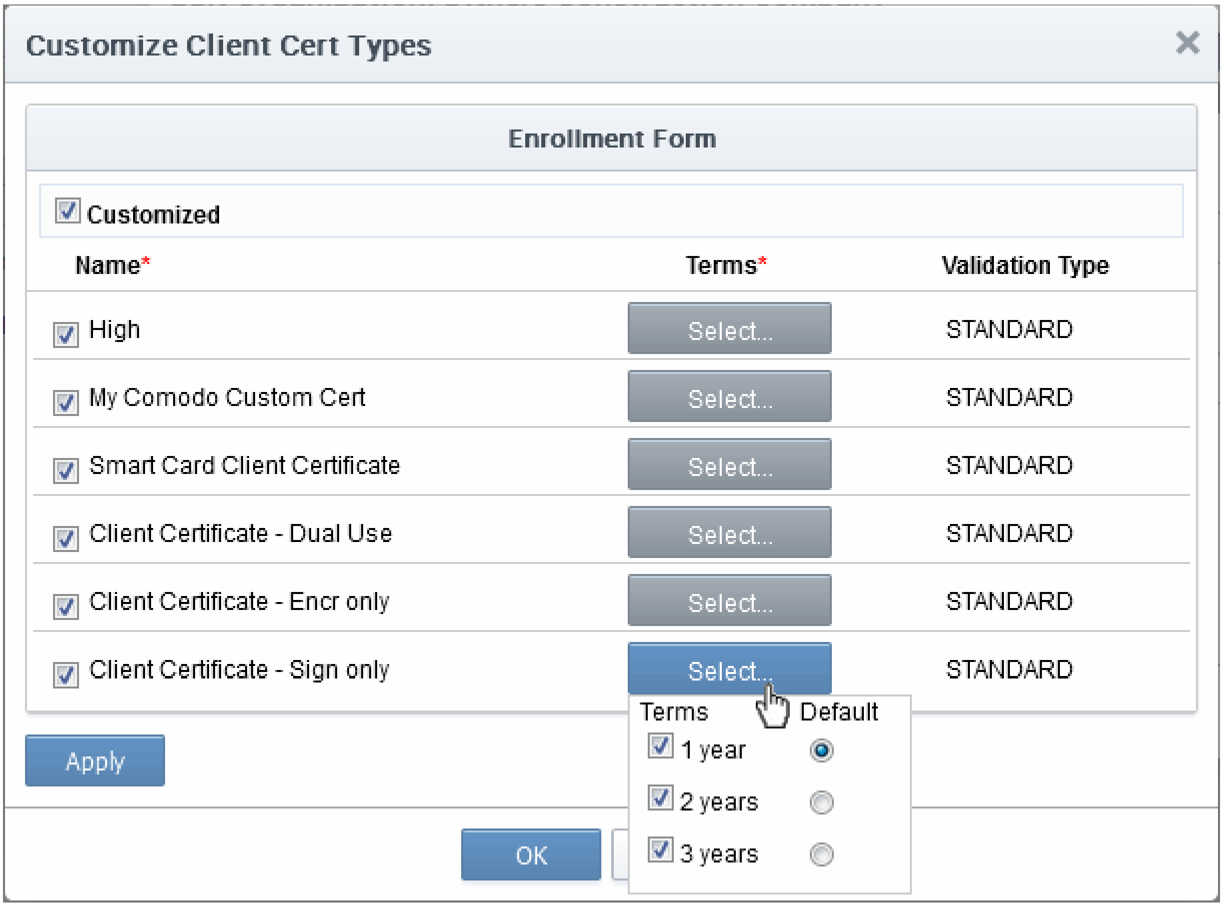
This will open the 'Customize Client Cert Types' for that Organization, that enables to restrict the Client Cert types that will be available to applicants using the Self Enrollment Form for that organization.

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).

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.

The Validation types for each cert type are shown in the 'Validation Type' column. The two types of validation are 'Standard' and 'High'.



Customize Client Cert Types

Enrollment Form

☑ Customized

Name*	Terms*	Validation Type
☑ High	Select...	STANDARD
☑ My Comodo Custom Cert	Select...	STANDARD
☑ Smart Card Client Certificate	Select...	STANDARD
☑ Client Certificate - Dual Use	Select...	STANDARD
☑ Client Certificate - Encr only	Select...	STANDARD
☑ Client Certificate - Sign only	Select...	STANDARD

Terms	Default
☑ 1 year	●
☑ 2 years	○
☑ 3 years	○

''Standard' validation type can be issued quickly and takes advantage of the user authentication mechanisms that are built into Incommon CM.

Under 'Standard Personal Validation' type, the user 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' type requires 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.

4. Click OK.

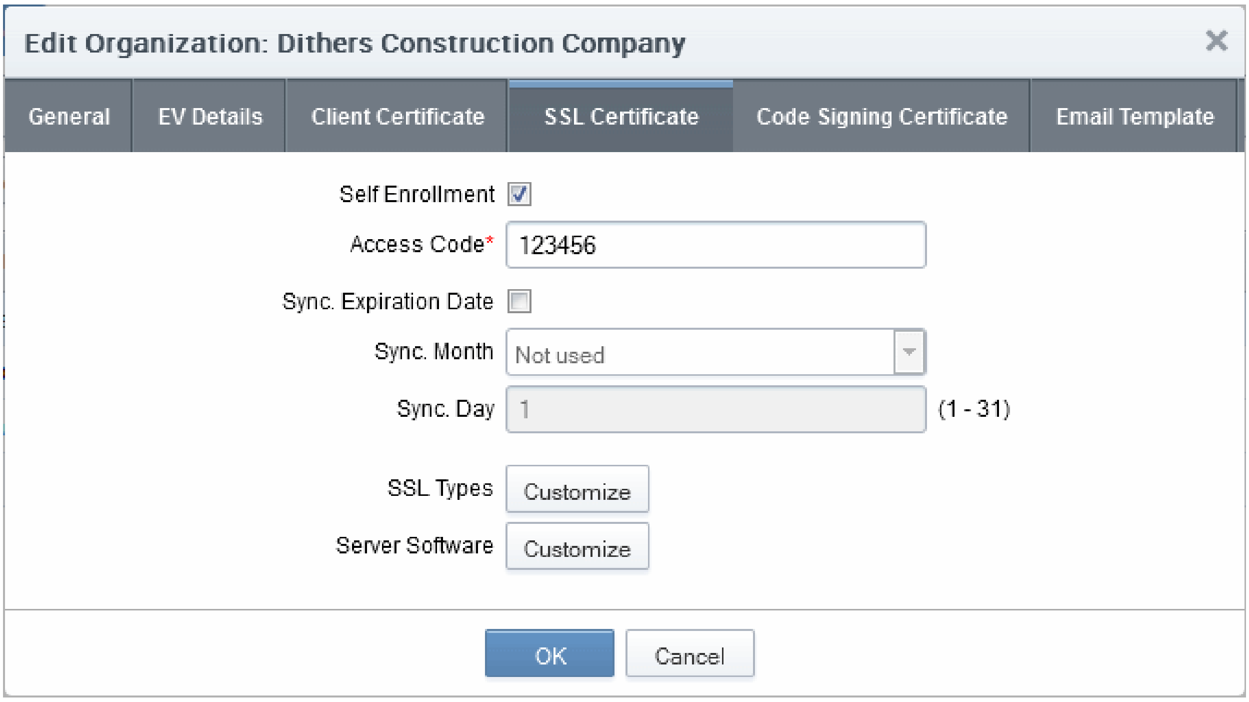
The administrator needs to log out then back in again for the customization options to take effect.

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

6.2.2.4.5 SSL Certificates Settings Tab

The 'SSL' tab allows RAO SSL administrators to:

- Enable or disable certificate self-enrollment for the organization. This determines whether or not users can apply for certificates using the external application forms.
- Which certificate types and term lengths are available to the organization.
- Web API capabilities and expiry synchronization settings relating to SSL certificates issued to the organization's domains.



Edit Organization: Dithers Construction Company

Self Enrollment ☑

Access Code* 123456

Sync. Expiration Date □

Sync. Month Not used

Sync. Day 1 (1 - 31)

6.2.2.4.6 SSL Certificates - Table of Parameters

Field Name	Type	Description
Self Enrollment	*Check-box* *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://cert-manager.com/customer/customer_uri/ssl?action=enroll • Certificates requested using the self-enrollment form will appear in the 'SSL Certificates' sub-tab of the 'Certificates Management' section before they are submitted to Incommon CA for validation. • RAOs must review and approve or decline the request. Approved requests will forwarded to Incommon CA for processing.

Field Name	Type	Description
		• 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 Incommon 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 request, the applicant must provide the correct 'Access Code' for the organization. Admins should communicate this code to the applicant using any out-of-bands methods like email. • Certificates can be requested by individuals that do not yet exist in Incommon CM IF: • The access code entered on the form is correct, AND • The email address entered on the form is from the same domain as that organization's 'Common Name'. In such circumstances, a new end-user will be automatically created 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 for which the SSL Certificate was ordered. The user will not, however, be issued with a client certificate.
Access Code (Appears only if the 'Self Enrollment' check-box 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 a 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 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	*Check-box*	Checking this box will enable the ability to modify and synchronize the

Field Name	Type	Description
Date		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 Wizard. • 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 Wizard. Example: Ordinarily, a 2 year certificate issued on the 12th of August 2014 would expire 730 days later on the 12th August 2016. However: • If the administrator has ONLY specified day 16 as the 'sync expiry day' then the certificate will expire on the 16th of July 2016. • If the administrator has ONLY specified day 5 as the 'sync expiry day', then the certificate will expire on the 5th August 2016. • If the administrator has specified 14th of June as the sync expiry 'day' and 'month', then the certificate will expire on the 14th June 2016. • If the administrator has specified 14th of August as the sync expiry 'day' and 'month', then the certificate will expire on the 14th August 2015. **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	*Check-box*	Checking this box enables certificate enrollment through the WebService

Field Name	Type	Description
	Default state - not checked	API. This requires a special agreement with Incommon. See Web API documentation, for detailed instructions.
Secret Key (Appears only if the 'Web API' check-box 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. • This is used in tandem with 'Organization ID' (visible only for already created organizations).
SSL Types	*Button* *'Customize'*	Allows you to specify the certificate types and term lengths that will be available for this organization. • Click the 'Customize' button to 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 wizard (Admin UI) or the (Self) Enrollment form. • 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 wizard (Admin UI) or the (Self) Enrollment form. See section Customize an Organization's Server Software Types for more details on this.

6.2.2.4.6.1 Customize an Organization's SSL Certificate Types

A streamlined 'certificate roster' can simplify the certificate selection procedure on application forms and avoid requests for inappropriate certificates

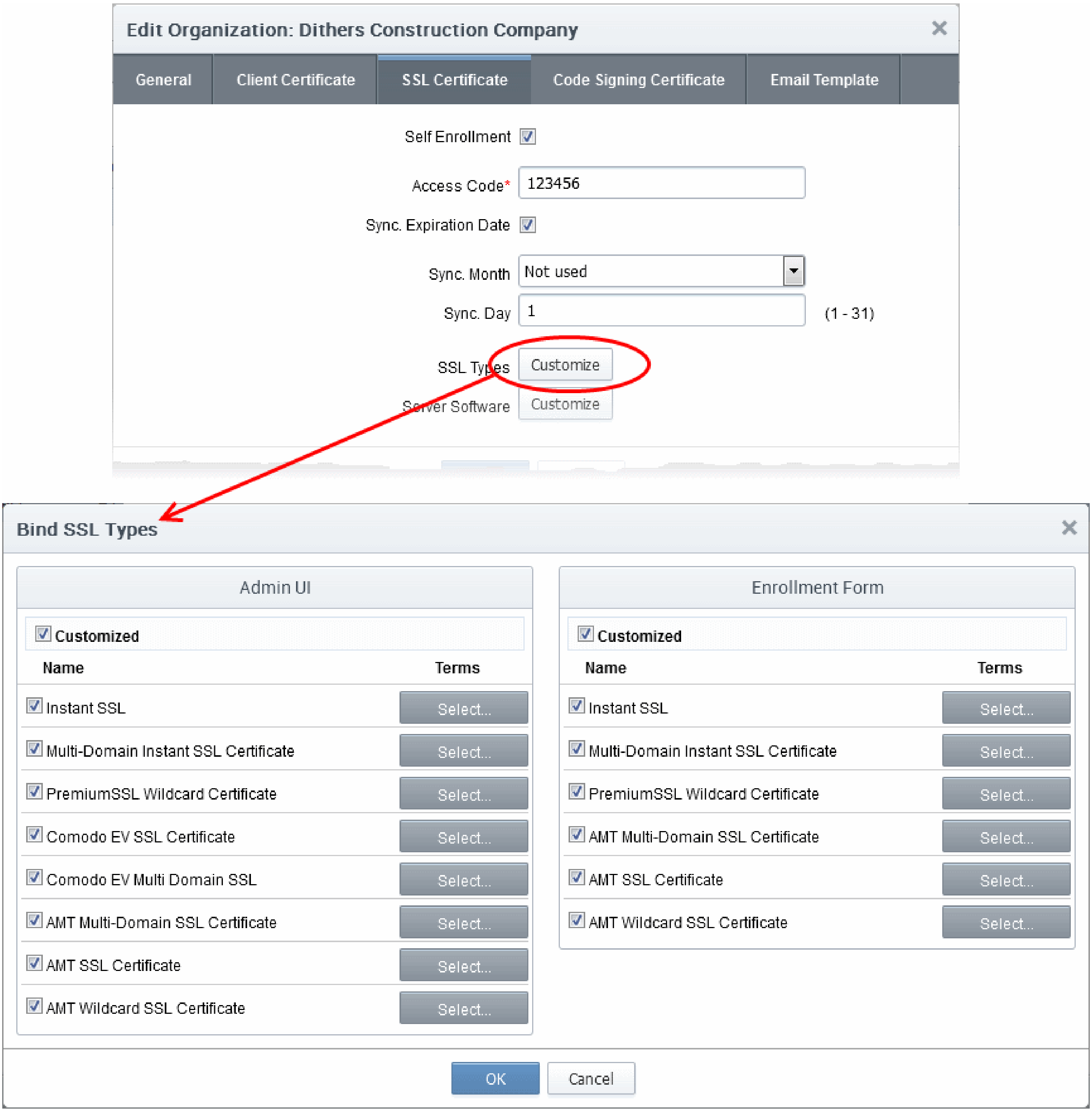
Security Roles:

- 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.

In other words, Master Administrator set the master certificate availability for organizations. RAOs can then enable or disable certificates within this list for orgs/depts that they control.

- The 'Bind SSL Types' interface lets you configure the types and terms of certificates available to an organization.
- Click 'Settings' > 'Organizations' > select an organization in the list > Click 'Edit' > 'SSL Certificate' > 'Customize' SSL types:

To access the 'Bind SSL Types' interface, click the 'Customize' button under the SSL tab of the 'Edit Organization' interface:



Self Enrollment ☑

Access Code* 123456

Sync. Expiration Date ☑

Sync. Month Not used

Sync. Day 1 (1 - 31)

SSL Types Customize

Server Software Customize

Admin UI

☑ Customized

Name	Terms
☑ Instant SSL	Select...
☑ Multi-Domain Instant SSL Certificate	Select...
☑ PremiumSSL Wildcard Certificate	Select...
☑ Comodo EV SSL Certificate	Select...
☑ Comodo EV Multi Domain SSL	Select...
☑ AMT Multi-Domain SSL Certificate	Select...
☑ AMT SSL Certificate	Select...
☑ AMT Wildcard SSL Certificate	Select...

Enrollment Form

☑ Customized

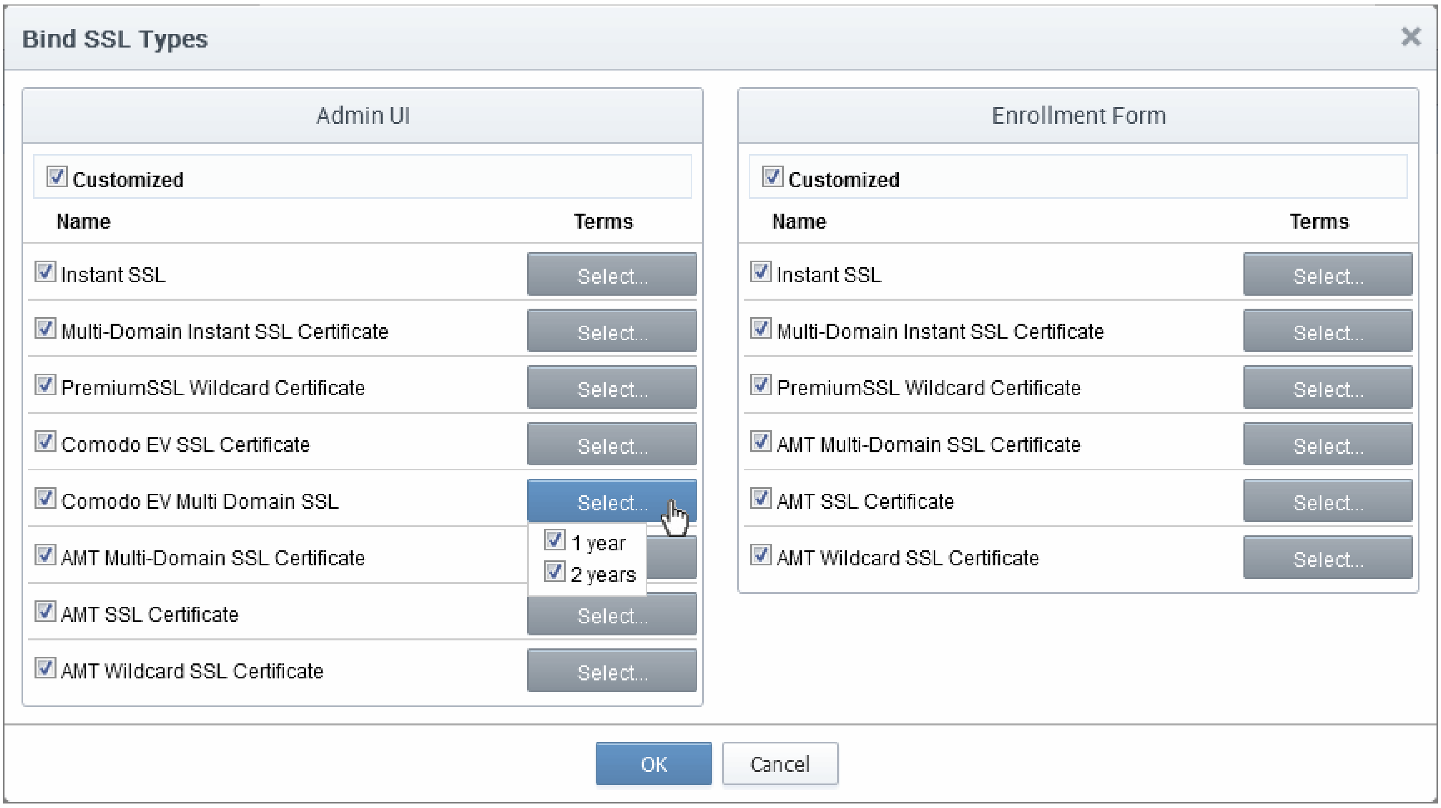
Name	Terms
☑ Instant SSL	Select...
☑ Multi-Domain Instant SSL Certificate	Select...
☑ PremiumSSL Wildcard Certificate	Select...
☑ AMT Multi-Domain SSL Certificate	Select...
☑ AMT SSL Certificate	Select...
☑ AMT Wildcard SSL Certificate	Select...

- **Admin UI** - Determines the SSL certificate types that will be available to applicants using the Built In Wiizard 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 certificates for the built-in wizard than is available in the self-enrollment form.

The 'Customized' option is unchecked by default, so all certificate types are available through both types of application form.

To restrict the SSL types and their durations

1. Enable the 'Customized' checkbox in the 'Admin UI' or 'Enrollment Form' pane.
2. Use the check-boxes on the left to choose the certificate types you wish to allow for the organization
3. Click the 'Select' button next to an enabled certificate to choose which terms will be available.



Bind SSL Types

Admin UI

☑ Customized

Name	Terms
☑ Instant SSL	Select...
☑ Multi-Domain Instant SSL Certificate	Select...
☑ PremiumSSL Wildcard Certificate	Select...
☑ Comodo EV SSL Certificate	Select...
☑ Comodo EV Multi Domain SSL	Select... ☑ 1 year ☑ 2 years
☑ AMT Multi-Domain SSL Certificate	
☑ AMT SSL Certificate	Select...
☑ AMT Wildcard SSL Certificate	Select...

Enrollment Form

☑ Customized

Name	Terms
☑ Instant SSL	Select...
☑ Multi-Domain Instant SSL Certificate	Select...
☑ PremiumSSL Wildcard Certificate	Select...
☑ AMT Multi-Domain SSL Certificate	Select...
☑ AMT SSL Certificate	Select...
☑ AMT Wildcard SSL Certificate	Select...

4. Click 'OK'.

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

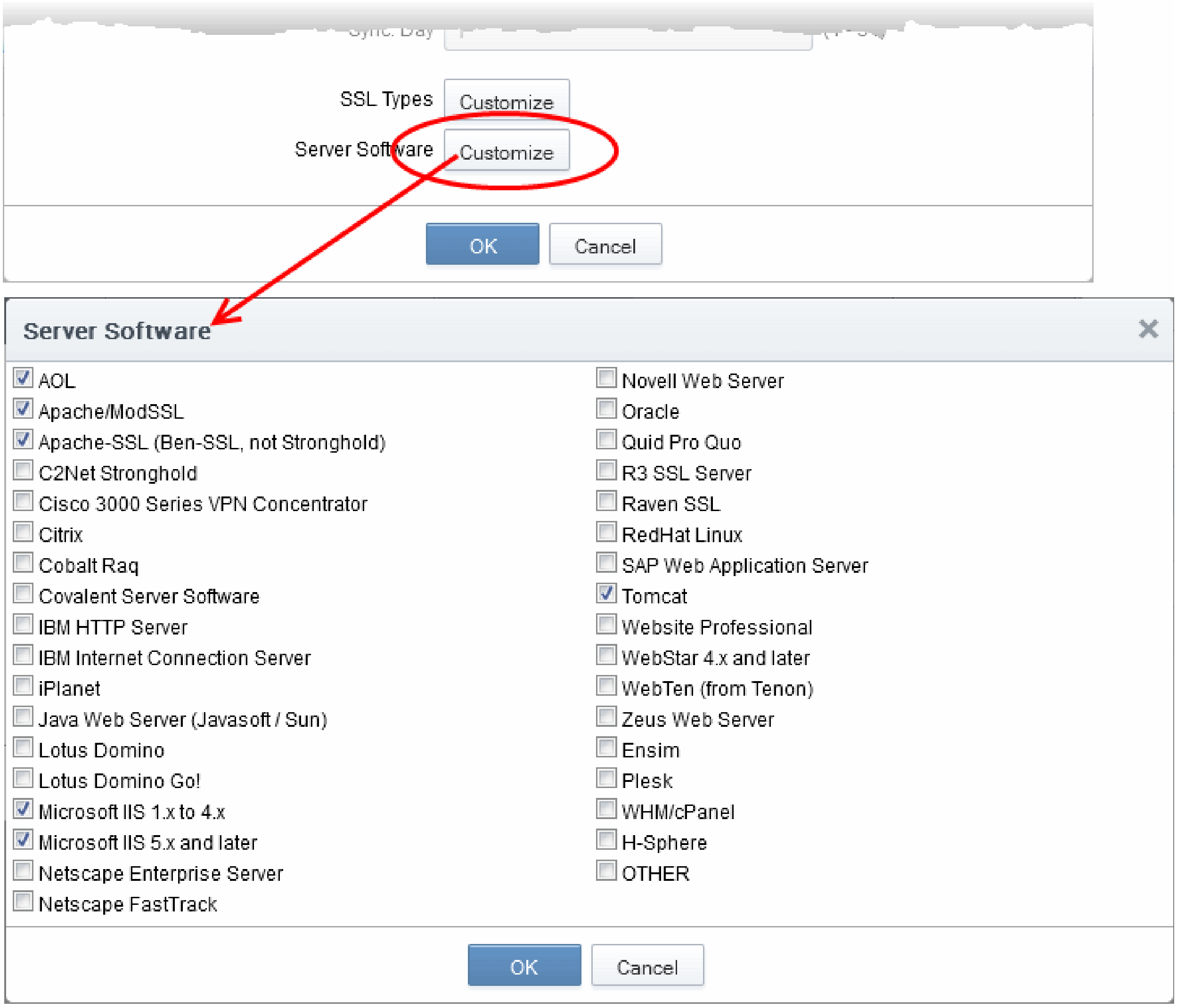
The types and terms of SSL certificates that are selected in the 'Bind SSL Types' interface will now be available in the 'Type' and 'Term' drop-down fields of this organization's application forms.

6.2.2.4.6.2 Customize an Organization's Server Software Types

Security Roles:

- 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 Form and the Built In Wiizard 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 Edit Organization interface. This will open the 'Server Software' for that organization.



☑ AOL
☑ Apache/ModSSL
☑ Apache-SSL (Ben-SSL, not Stronghold)
□ C2Net Stronghold
□ Cisco 3000 Series VPN Concentrator
□ Citrix
□ Cobalt Raq
□ Covalent Server Software
□ IBM HTTP Server
□ IBM Internet Connection Server
□ iPlanet
□ Java Web Server (Javasoft / Sun)
□ Lotus Domino
□ Lotus Domino Go!
☑ Microsoft IIS 1.x to 4.x
☑ Microsoft IIS 5.x and later
□ Netscape Enterprise Server
□ Netscape FastTrack
□ Novell Web Server
□ Oracle
□ Quid Pro Quo
□ R3 SSL Server
□ Raven SSL
□ RedHat Linux
□ SAP Web Application Server
☑ Tomcat
□ Website Professional
□ WebStar 4.x and later
□ WebTen (from Tenon)
□ Zeus Web Server
□ Ensim
□ Plesk
□ WHM/cPanel
□ H-Sphere
□ OTHER

By default, no server software will be selected.

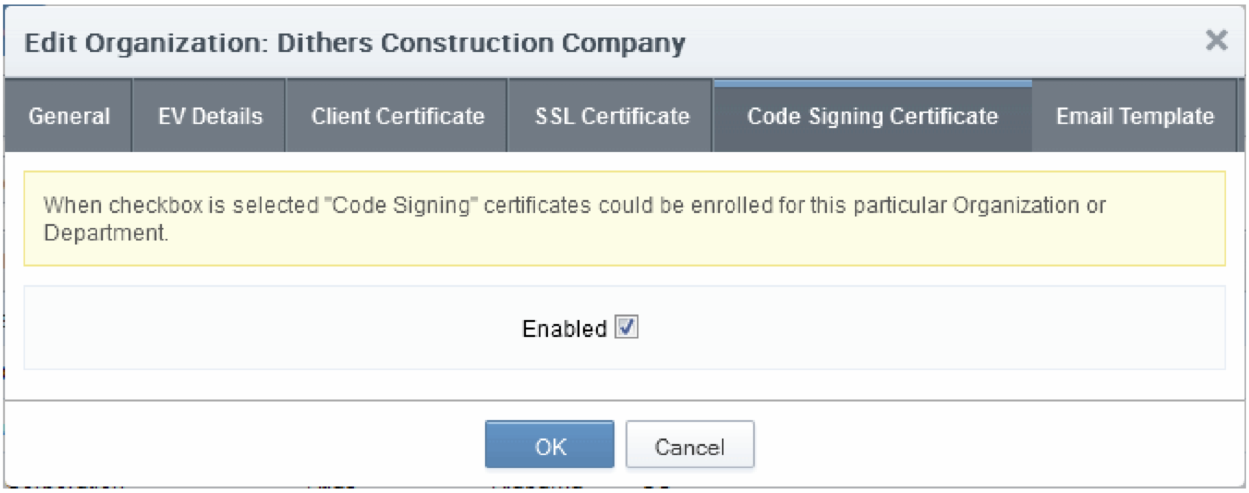
- To restrict the Server Software types select the names of the server software you wish to allow for that organization and leave the others unchecked. Click 'OK' to save the selection.

The administrator 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.

6.2.2.4.7 'Code Signing Certificate' 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.



When checkbox is selected "Code Signing" certificates could be enrolled for this particular Organization or Department.

Enabled ☑

6.2.2.4.7.1 Code Signing Certificates - Table of Parameters

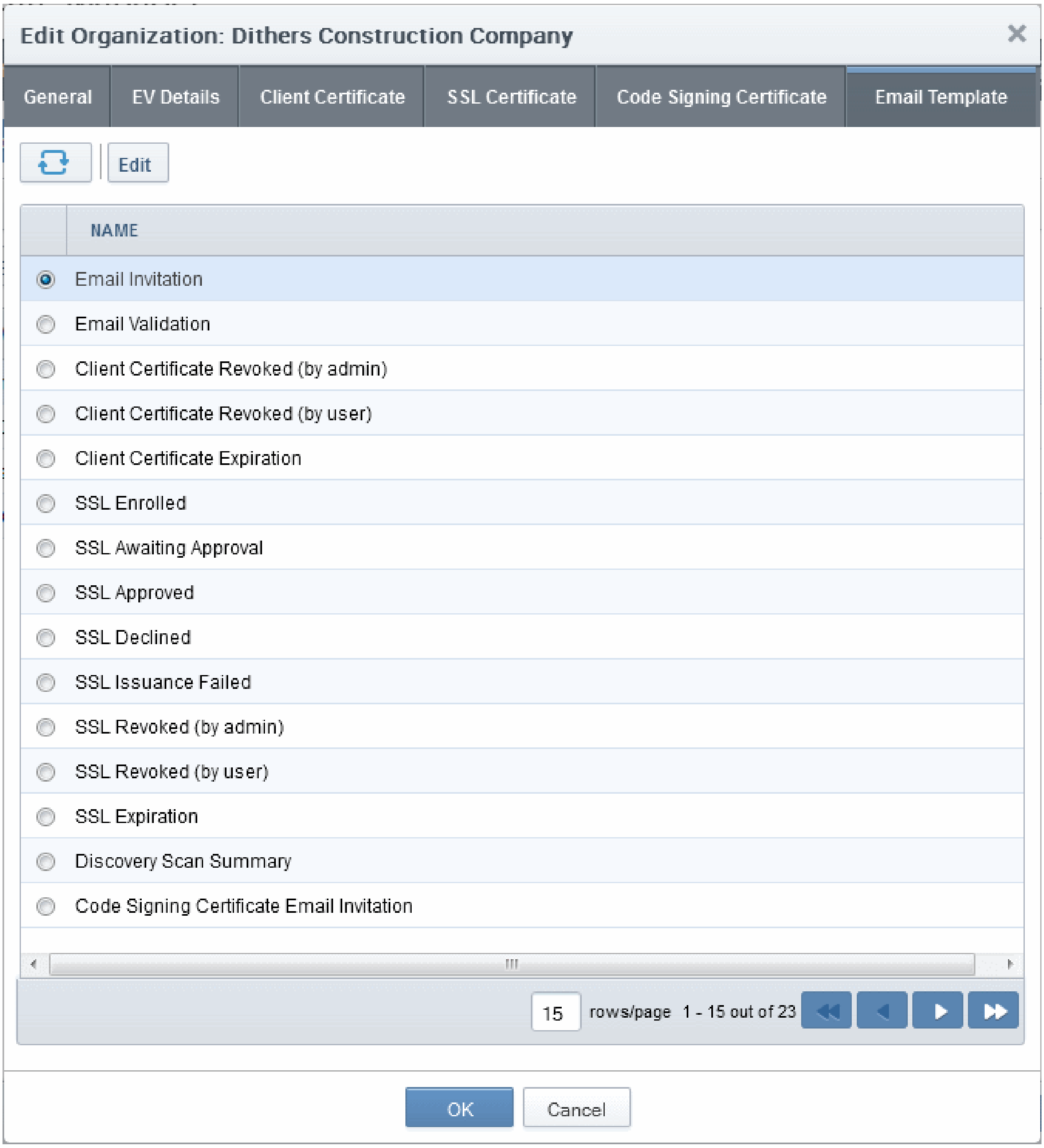
Field Name	Type	Description
Enabled	*Check-box* *Default state - not checked*	Checking this box will enable the request and issuance of Code Signing Certificates to end-users that are members of this organization.

6.2.2.4.8 'Email Template' tab

CM sends 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 Template' tab in the 'Edit Organization' dialog allows the Administrator to directly edit/customize the content of the automated notification emails as set by him/her in the Notifications area.

CM is shipped with several types of email templates corresponding to various notifications, related to different types of certificates and events. But the email templates displayed in the list and can be edited are dependent on the role of the administrator. For example, RAO SSL and DRAO SSL administrators will see the email templates of notifications corresponding to only SSL certificates and so on.



Edit Organization: Dithers Construction Company

	NAME
●	Email Invitation
○	Email Validation
○	Client Certificate Revoked (by admin)
○	Client Certificate Revoked (by user)
○	Client Certificate Expiration
○	SSL Enrolled
○	SSL Awaiting Approval
○	SSL Approved
○	SSL Declined
○	SSL Issuance Failed
○	SSL Revoked (by admin)
○	SSL Revoked (by user)
○	SSL Expiration
○	Discovery Scan Summary
○	Code Signing Certificate Email Invitation

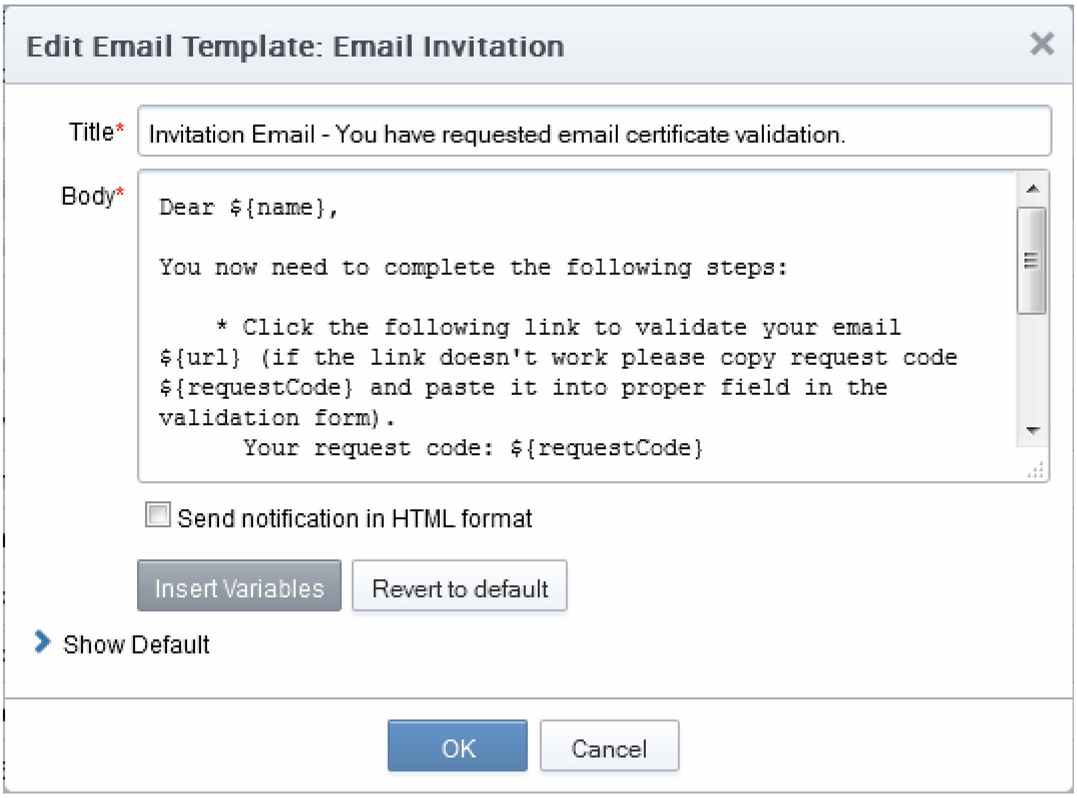
15 rows/page 1 - 15 out of 23

6.2.2.4.8.1 Viewing and Editing the Email Templates

Administrators can view and edit the email template messages from the 'Edit Email Template' dialog.

- Select the email template
- Click the 'Edit' button from the top

The 'Edit Email Template' dialog will open. An example is shown below.



Edit Email Template: Email Invitation

Title* Invitation Email - You have requested email certificate validation.

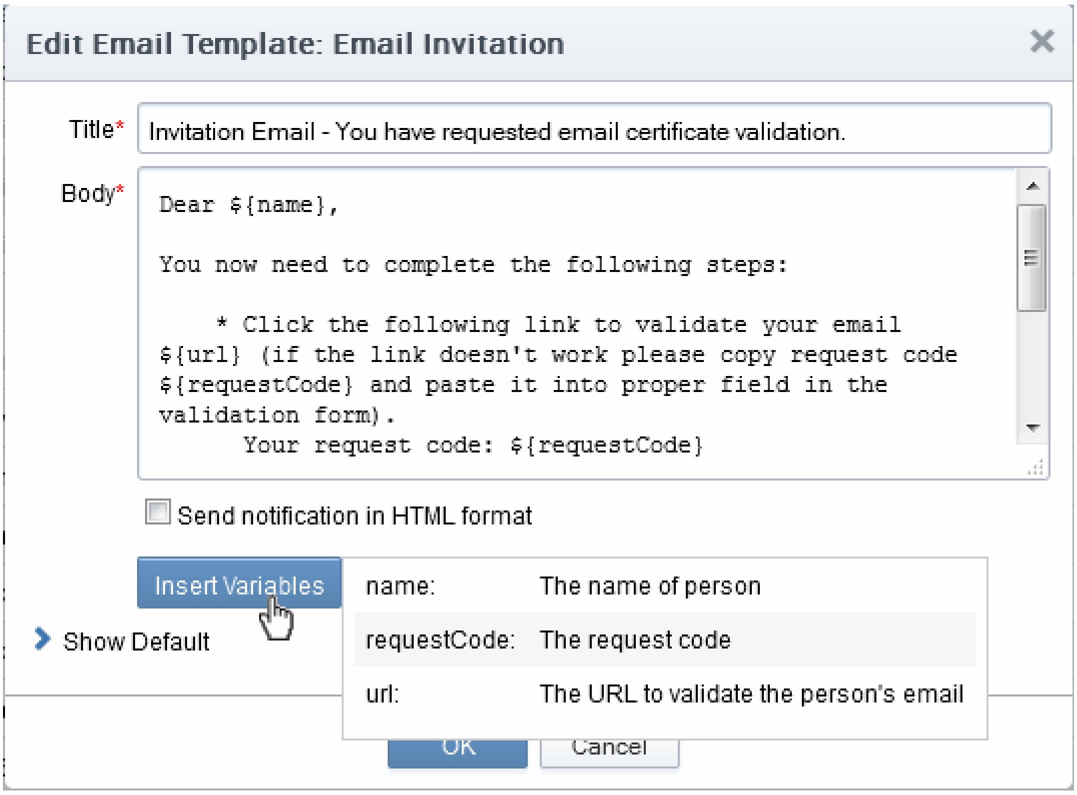
Body*

```
Dear ${name},

You now need to complete the following steps:

    * Click the following link to validate your email
${url} (if the link doesn't work please copy request code
${requestCode} and paste it into proper field in the
validation form).
      Your request code: ${requestCode}
```

□ Send notification in HTML format

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.



Edit Email Template: Email Invitation

Title* Invitation Email - You have requested email certificate validation.

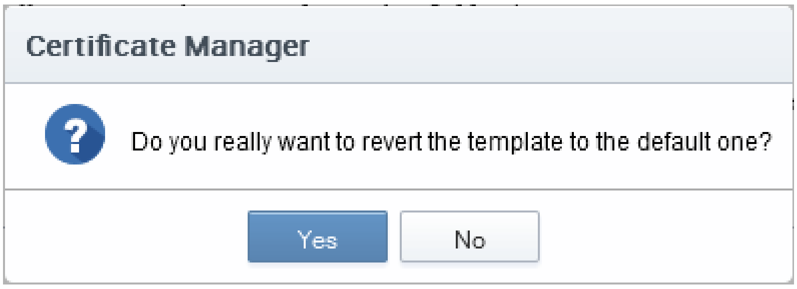
Body*

```
Dear ${name},

You now need to complete the following steps:

    * Click the following link to validate your email
${url} (if the link doesn't work please copy request code
${requestCode} and paste it into proper field in the
validation form).
      Your request code: ${requestCode}
```

□ Send notification in HTML format

name:	The name of person
requestCode:	The request code
url:	The URL to validate the person's email

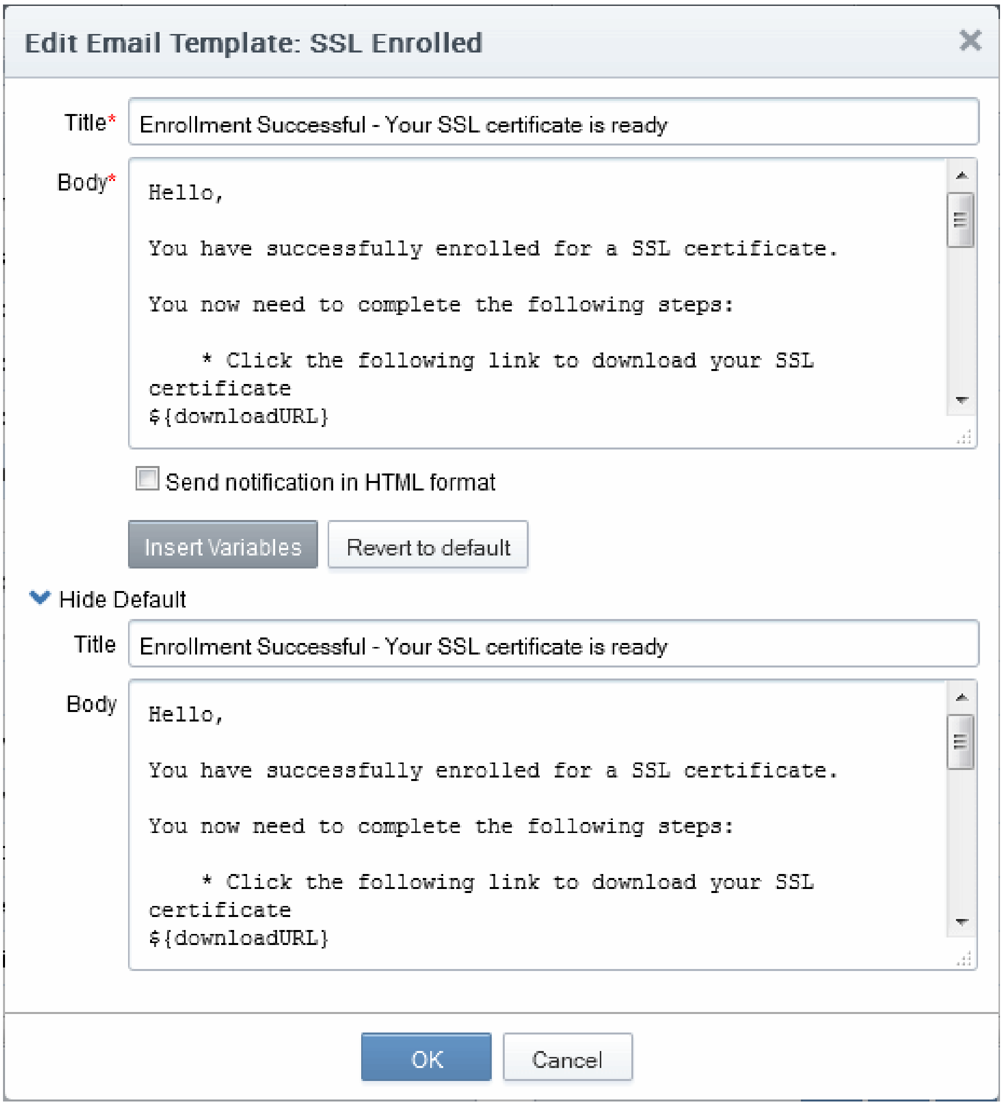
- Clicking 'Revert to default' enables the administrator to reset to the default content as shipped with CSM.



Certificate Manager

Do you really want to revert the template to the default one?

- Clicking 'Show Default' will display the default content for administrator to refer.



Edit Email Template: SSL Enrolled

Title* Enrollment Successful - Your SSL certificate is ready

Body*

```
Hello,

You have successfully enrolled for a SSL certificate.

You now need to complete the following steps:

    * Click the following link to download your SSL
certificate
${downloadURL}
```

□ Send notification in HTML format

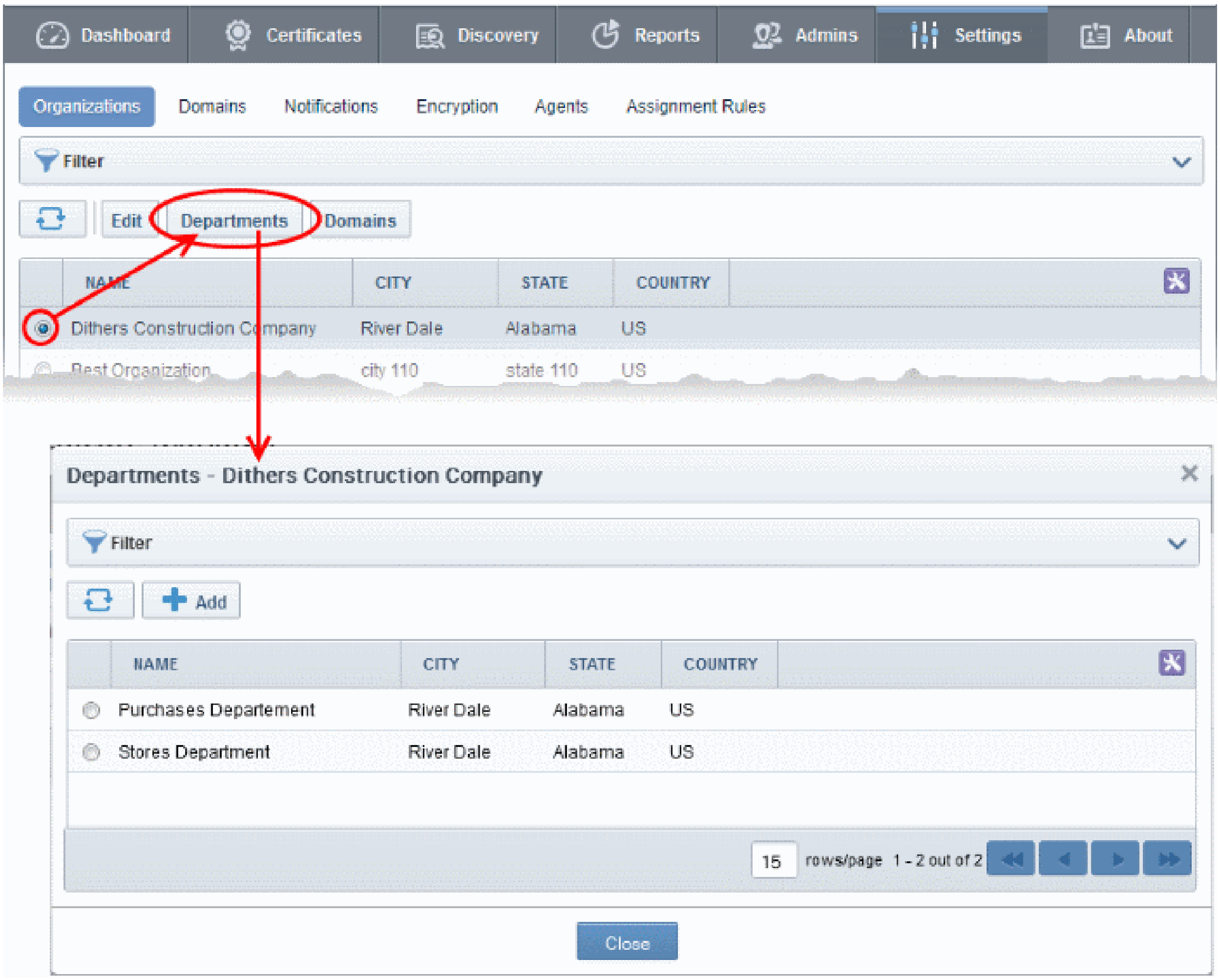
Title Enrollment Successful - Your SSL certificate is ready

Body

```
Hello,

You have successfully enrolled for a SSL certificate.

You now need to complete the following steps:

    * Click the following link to download your SSL
certificate
${downloadURL}
```

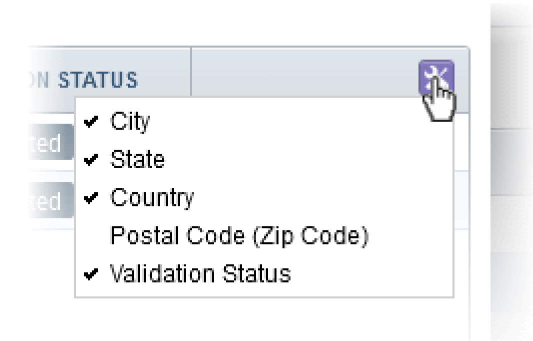
6.2.2.5 Managing the Departments of an Organization

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.



6.2.2.5.1 Departments Dialog - Table of Parameters

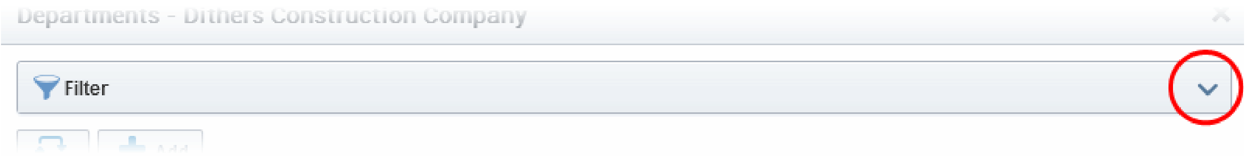
Column Display	Description
Name	A list of all departments that have been delegated to the administrator that is currently logged in. The list is displayed in ascending alphabetical order.
City	Displays the name of the city entered at the time of creating the department.
State	Displays the name of the 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 by the Master Administrator.
Note: An administrator can add more column headers from the drop-down button beside the last item in the column:	

 N STATUS ✔ City ✔ State ✔ Country Postal Code (Zip Code) ✔ Validation Status		
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 a 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.

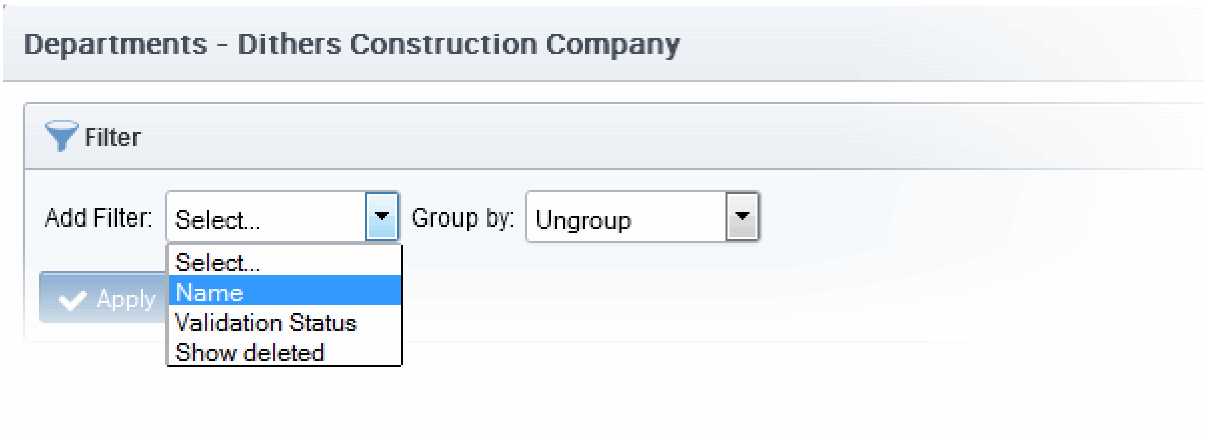
6.2.2.5.2 Sorting and Filtering Options

- Clicking 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:



- To apply filters, click on the down arrow at the right end of the 'Filters' stripe.
- The filter options will be displayed. 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 filter the department by 'Name':



Departments - Dithers Construction Company

- Enter the name of the department in part or full 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.

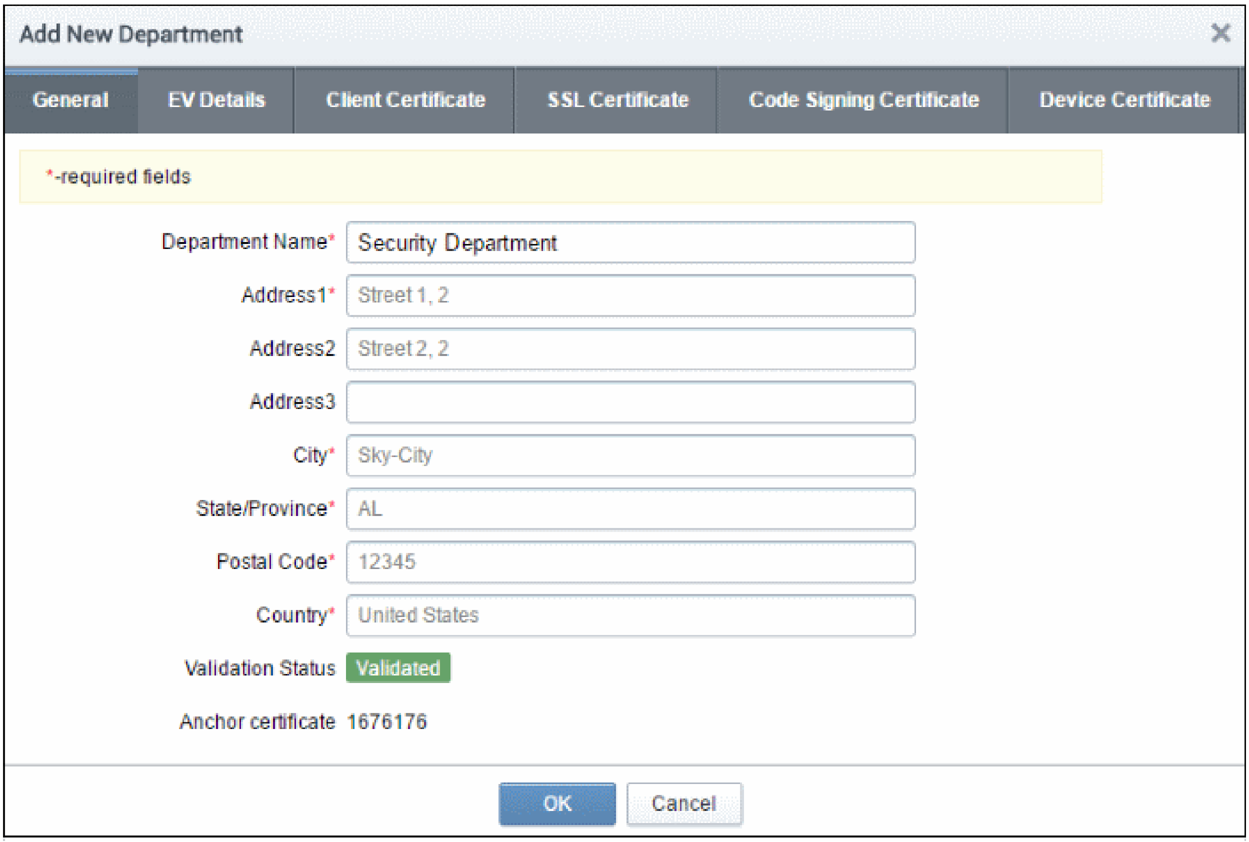
Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Departments' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear'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

6.2.2.5.3 Create New Departments

- An organization can also have sub-ordinate departments which are managed by a DRAO admin.
- A RAO administrator needs to create the department under the organization and assign domains to it. This will allow you to provide certificates to end-users and websites of the department.

To create a new department:

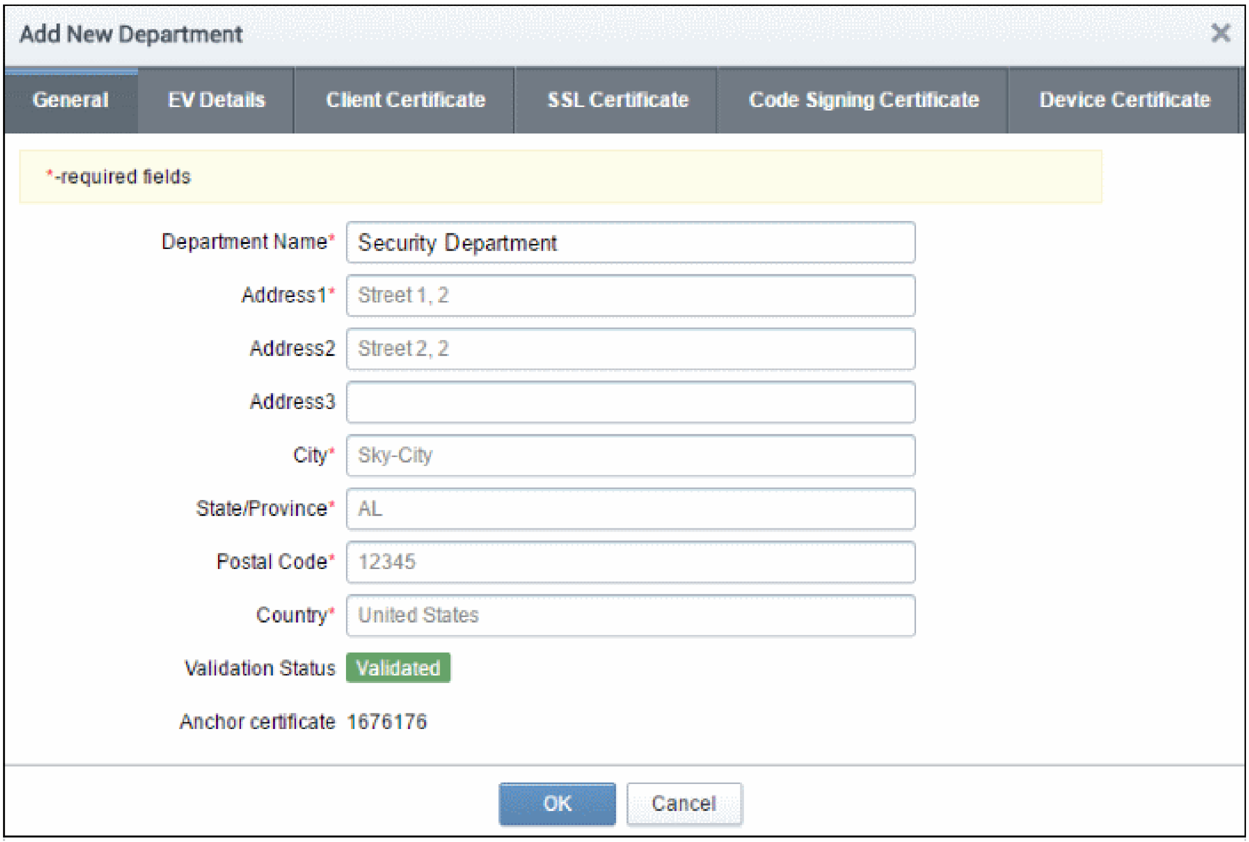
- Click 'Settings' > 'Organizations'
- Select the organization under which you want to create the new department from the list
- Click the 'Departments' button.
- Click the 'Add' button at the top of the 'Departments' dialog
- This will open the department configuration screen:



Add New Department

*-required fields

Department Name*	Security Department
Address1*	Street 1, 2
Address2	Street 2, 2
Address3	
City*	Sky-City
State/Province*	AL
Postal Code*	12345
Country*	United States
Validation Status	Validated
Anchor certificate	1676176



Add New Department

*-required fields

Department Name*	Security Department
Address1*	Street 1, 2
Address2	Street 2, 2
Address3	
City*	Sky-City
State/Province*	AL
Postal Code*	12345
Country*	United States
Validation Status	Validated
Anchor certificate	1676176

- The screen contains six 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 Incommon, the address details will be auto populated with the parent organization's address. You will need to give the dept. a name, though.

General Tab:

'General' settings allows the RAO administrator to configure high level details relating to the new department if the parent organization has not been validated. These details will be replaced with those in the anchor certificate issued for the parent organization the next time an OV certificate is ordered for the department. If the parent organization is already validated by Incommon 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. The administrator must fill the department name field, which will display as 'Organizational Unit' (OU) in the final certificate.

- The details in the 'General' section are used for Client, SSL and Code Signing Certificates requested on behalf of that department.
- Client and SSL certificates may only be automatically issued to common names of domains (and sub-domains) delegated to the department, which Incommon CA has pre-validated that you have the right to use. If you apply for certificates on a new domain, then Incommon CA will first need to validate your ownership of the domain before the certificate can be issued for it. See Delegating Domains for more details.
- For more details on these fields, see 'General Settings' - Table of Parameters'

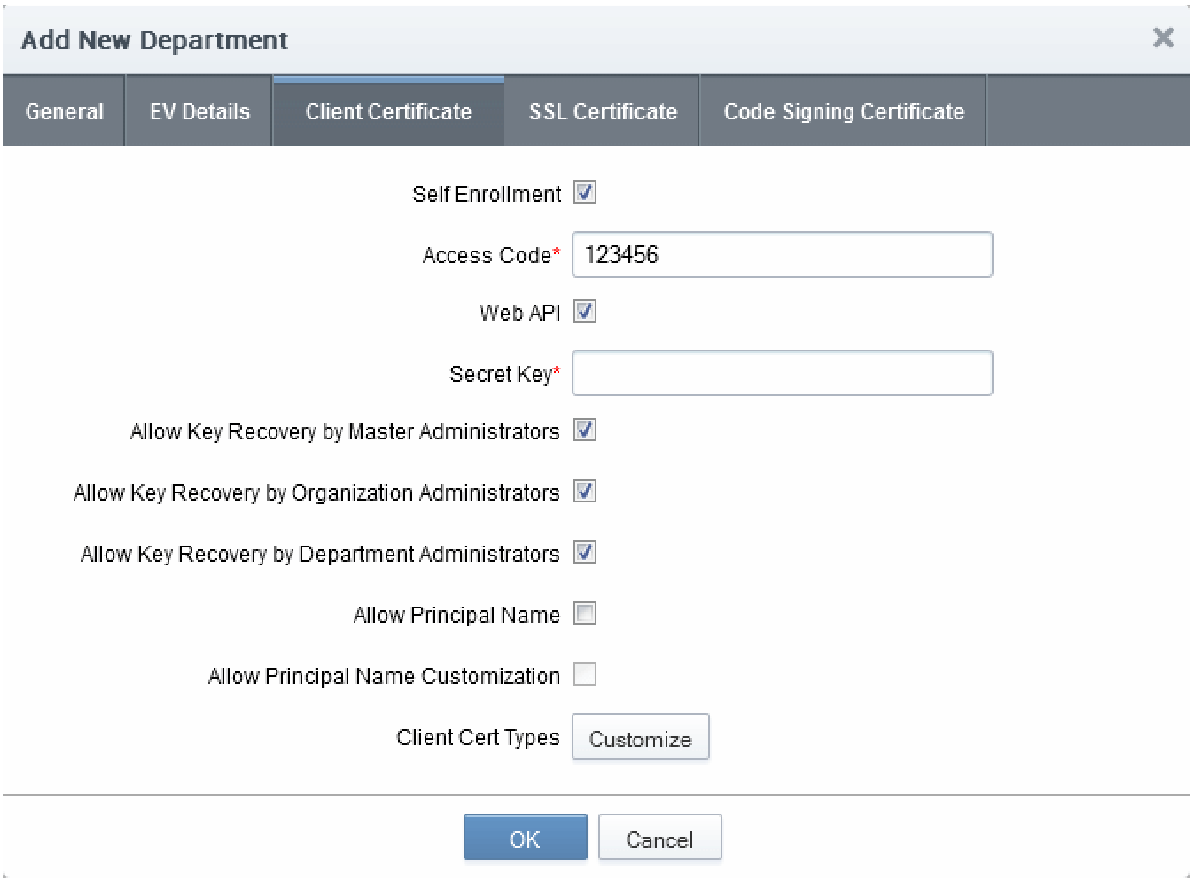
6.2.2.5.4 General Settings - Table of Parameters

Field Name	Values	Description
Department Name	*String **(required)***	The name of the Department to be created which will display as "Organizational Unit' (OU) in the final OV SSL certificate.
Address 1	*String **(required)***	If the parent organization is already validated by Incommon 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 and non-editable. If the parent organization is not validated, then the administrator can fill these details, but will be replaced with those in the anchor certificate issued for the parent organization after validation the next time an OV certificate is ordered for the department.
Address 2	*String*	
Address 3	*String*	
City	*String*	
State/Province	*String*	
Postal Code	*String*	
Country	*String*	
Validation Status		Indicates the progress of Organizational validation (OV) on the Incommon CM parent 'Organization' in question. States can be 'Not validated', 'Validated', 'Pending', 'Failed', 'Expired'.
Anchor Certificate		Issued after the organization validation is completed for the parent organization of the department. Indicates the status of Anchor certificate. This is used as a reference for organization validation status by Incommon CM whenever an Organization Validated SSL certificate is requested for an organization or departments under it.

- The 'EV Details' Tab - see 5.2.2.4.2 EV Details tab for more details
- The 'SSL Certificate' tab - see 5.2.2.4.5 SSL Certificate Settings tab for more details
- The 'Code Signing' tab - see 5.2.2.4.7 Code Signing Certificates Settings tab for more details

Client Cert Tab

The Client Certificate tab is the same as that explained in 5.2.2.4.3.Client Certificate Settings Tab but contains an additional setting related to key recovery:



Self Enrollment ☑

Access Code* 123456

Web API ☑

Secret Key*

Allow Key Recovery by Master Administrators ☑

Allow Key Recovery by Organization Administrators ☑

Allow Key Recovery by Department Administrators ☑

Allow Principal Name □

Allow Principal Name Customization □

Client Cert Types Customize

Allow Key Recovery by Master Administrator	*Check-box* *Default state - checked if pre-enabled by Master Administrator*	• If selected, the Master 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 Master Administrator 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 Master Administrator 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 RAO	*Check-box* *Default state - checked if pre-enabled by Master Administrator*	• 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 DRAO	*Check-box* *Default state - checked*	• 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.

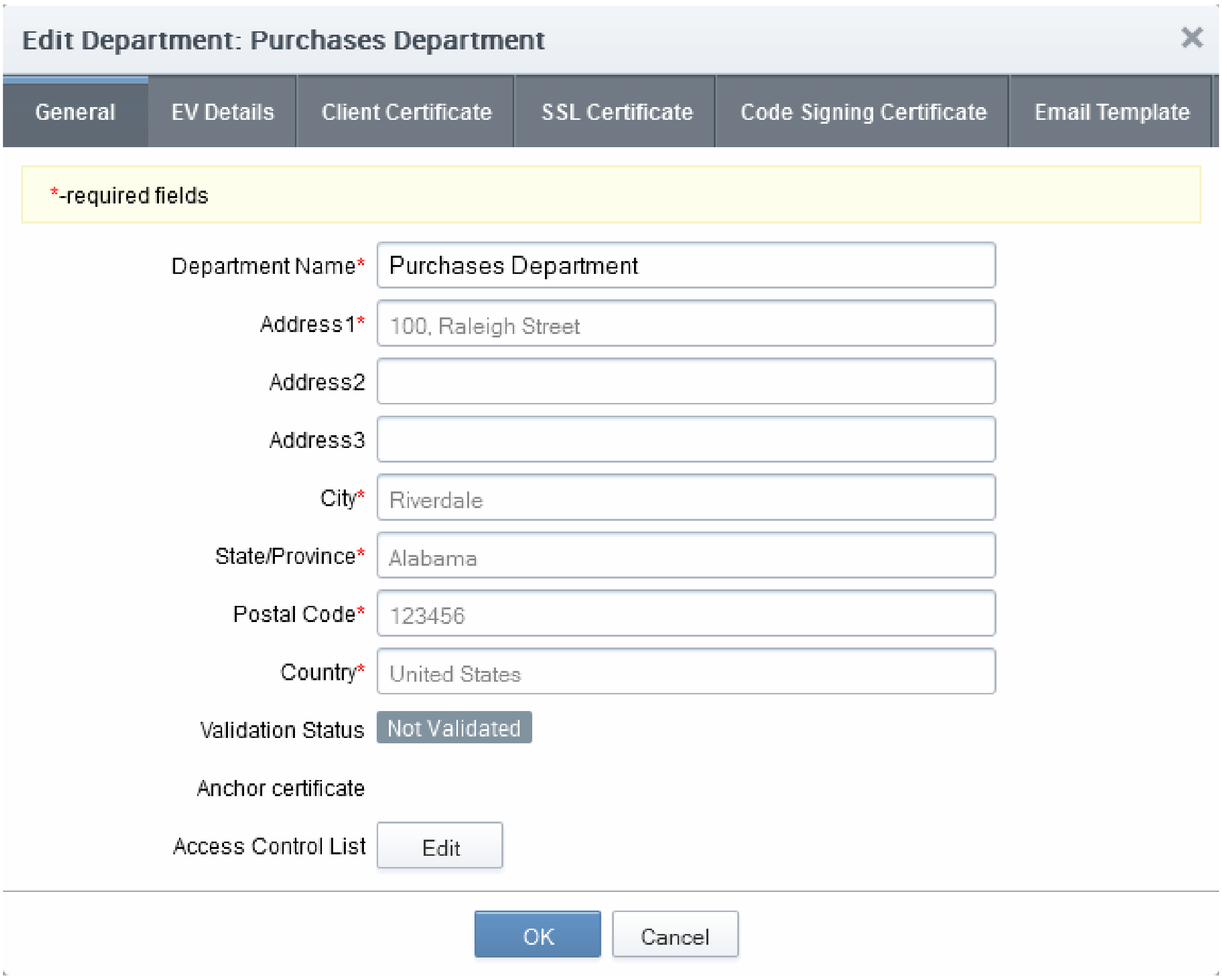
* The settings outlined above will be active ONLY IF they have been enabled for your organization.

6.2.2.5.5 Editing Departments belonging to an Organization

Appropriately privileged administrators can edit the departments of any organization at any time.

To do this:

- Click 'Settings' > 'Organizations'
- Select the organization whose department you want to edit
- Click the 'Departments' button
- Select the department you want to edit
- Click the 'Edit' button
- This will open the department configuration screen:



*-required fields

Department Name*: Purchases Department

Address1*: 100, Raleigh Street

Address2:

Address3:

City*: Riverdale

State/Province*: Alabama

Postal Code*: 123456

Country*: United States

Validation Status: Not Validated

Anchor certificate

Access Control List

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 5.2.2.5.4.General Settings - Table of Parameters
- For more details on ACL - see Imposing Access Restrictions to CM interface
- For more details on Client Certs tab - see Client Certs tab under 5.2.2.5.3.Creating Departments
- For more details on 'SSL Certificate' tab - see 5.2.2.4.5 'SSL Certificate' Settings tab
- For more details on 'Code Signing Certificate' tab - see 5.2.2.4.7 'Code Signing Certificate' Settings tab
- For more details on 'Email Template' tab - see 5.2.2.4.8 'Email Template' tab

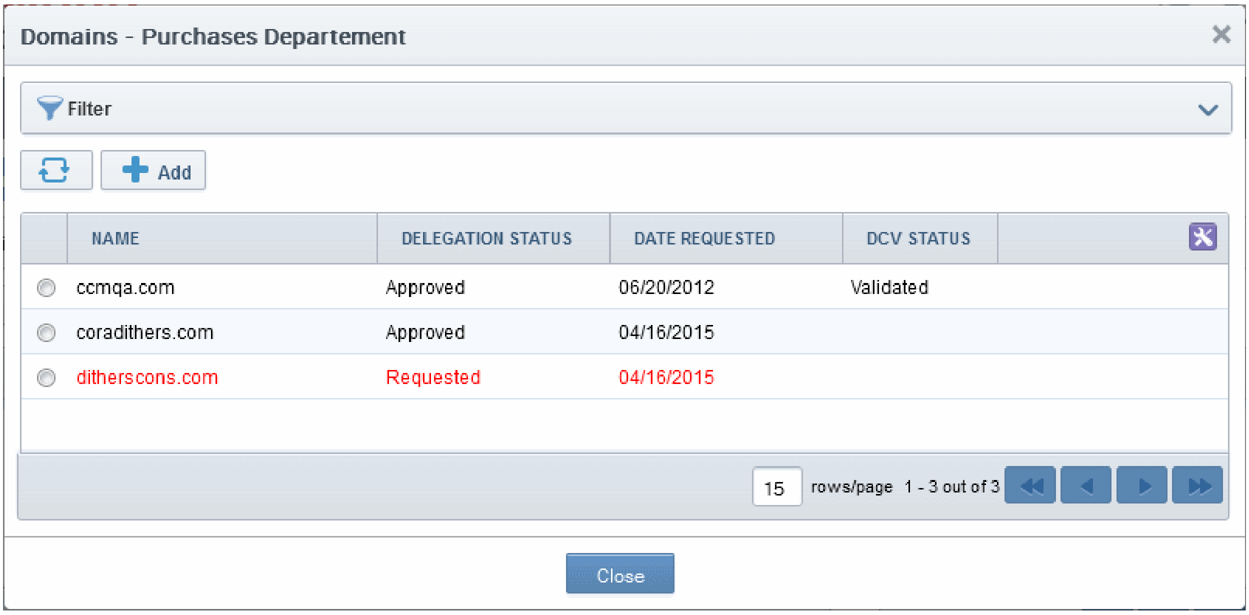
6.2.2.5.6 Manage Domains belonging to a Department

Administrators can view and manage domains delegated to a department.

To do this:

- Select the department
- Click 'Domains' from the top

The 'Domains' dialog enables appropriately privileged Administrators to view, edit and delegate any domains attached to the department.



NAME	DELEGATION STATUS	DATE REQUESTED	DCV STATUS
○ ccmqa.com	Approved	06/20/2012	Validated
○ coradithers.com	Approved	04/16/2015	
○ ditherscons.com	Requested	04/16/2015	

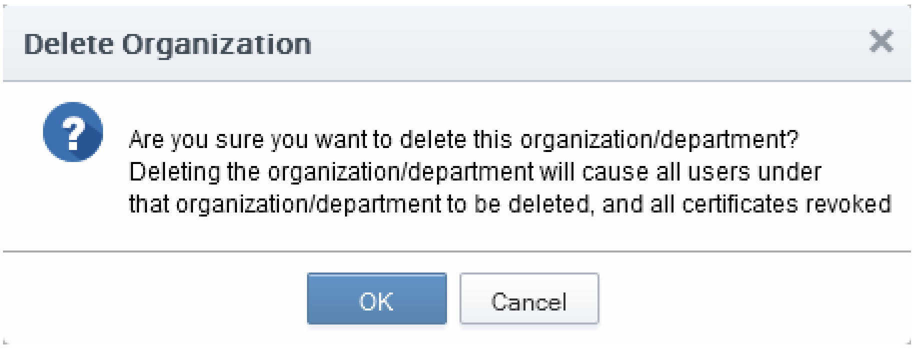
A detailed explanation on this area is available in section: 5.4.2.1 Domains Area Overview

6.2.2.5.7 Delete an Existing Department

Admins can remove a department if he/she no longer wishes to issue certificates from it.

To do this:

- Select a department
- Click 'Delete' button from the top



Delete Organization

Are you sure you want to delete this organization/department? Deleting the organization/department will cause all users under that organization/department to be deleted, and all certificates revoked

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, the CM will prompt for confirmation:

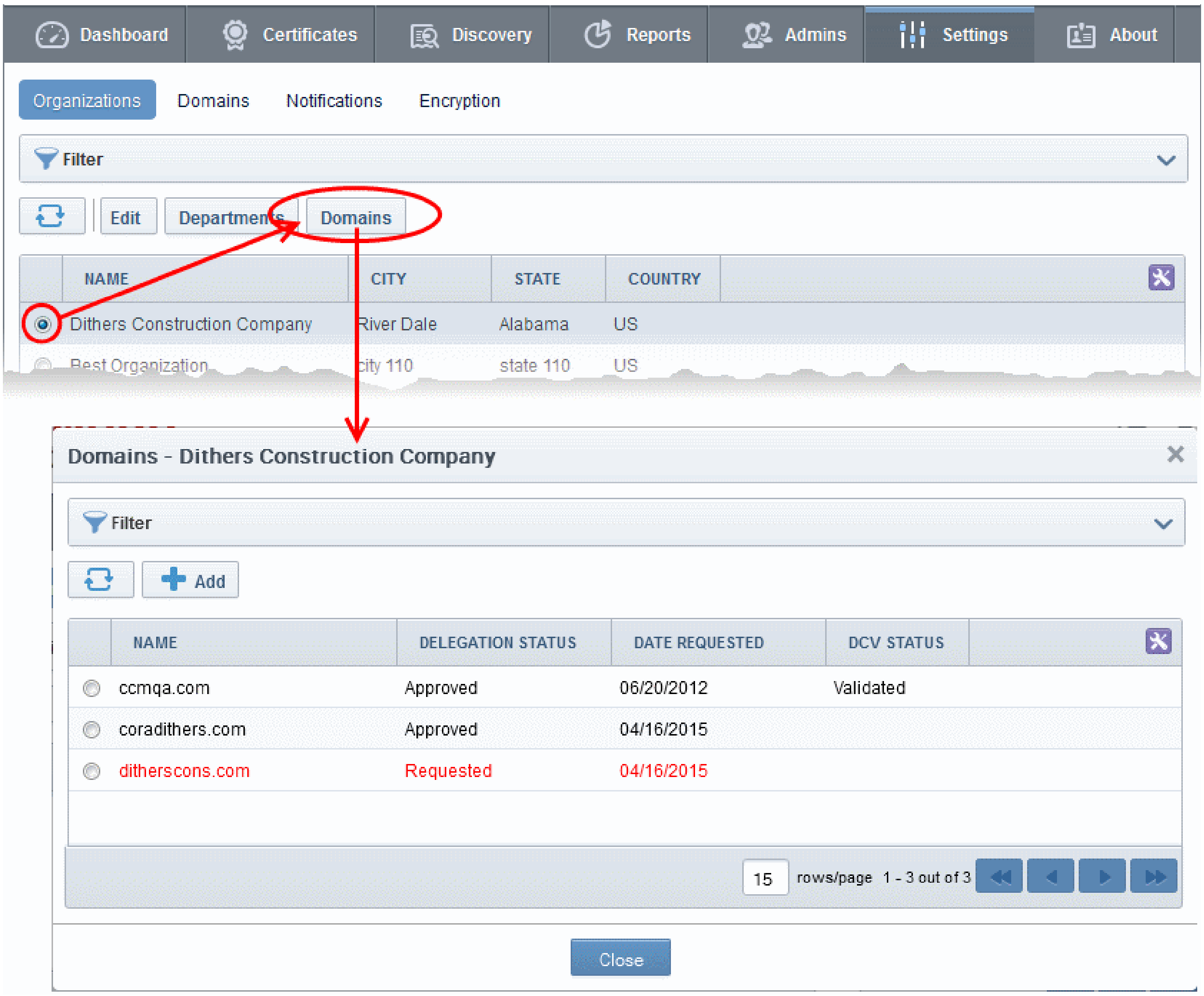
6.2.2.6 Managing the Domains of an Organization

Admins can view and manage the domains delegated to an organization.

To do this:

- Click 'Settings' > 'Organizations'
- Select the organization whose domains you wish to manage
- Click the 'Domains' button.
- This will open the domain configuration screen

The screen lists all domains assigned to the organization and its departments:



	NAME	CITY	STATE	COUNTRY
●	Dithers Construction Company	River Dale	Alabama	US
○	Best Organization	city 110	state 110	US

Domains - Dithers Construction Company

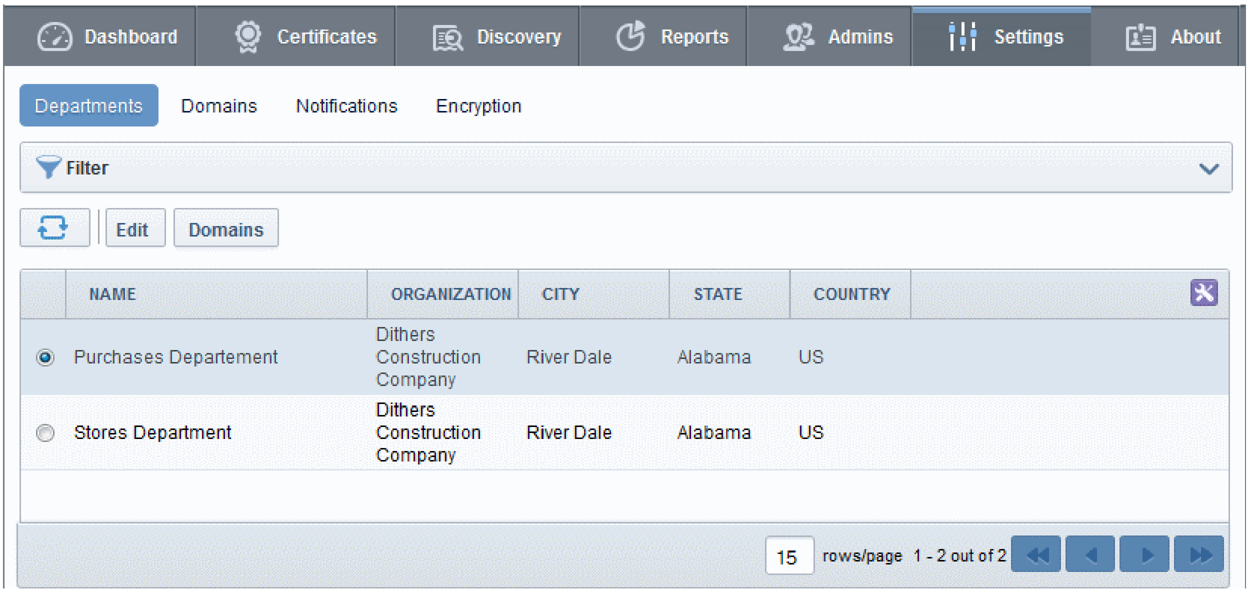
	NAME	DELEGATION STATUS	DATE REQUESTED	DCV STATUS
○	ccmqa.com	Approved	06/20/2012	Validated
○	coradithers.com	Approved	04/16/2015	
○	ditherscons.com	Requested	04/16/2015	

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

6.3 Departments

The Departments tab allows DRAO Administrators to manage existing domains and add new domains to the Departments that have been delegated to them. Clicking the 'Edit' button at the top after selecting the checkbox next to a listed Department will allow the DRAO Administrator to manage the certificates issued by the Department.

Important Note: The 'Departments' area is visible only to DRAO Administrators. 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 5.2.2.5 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.



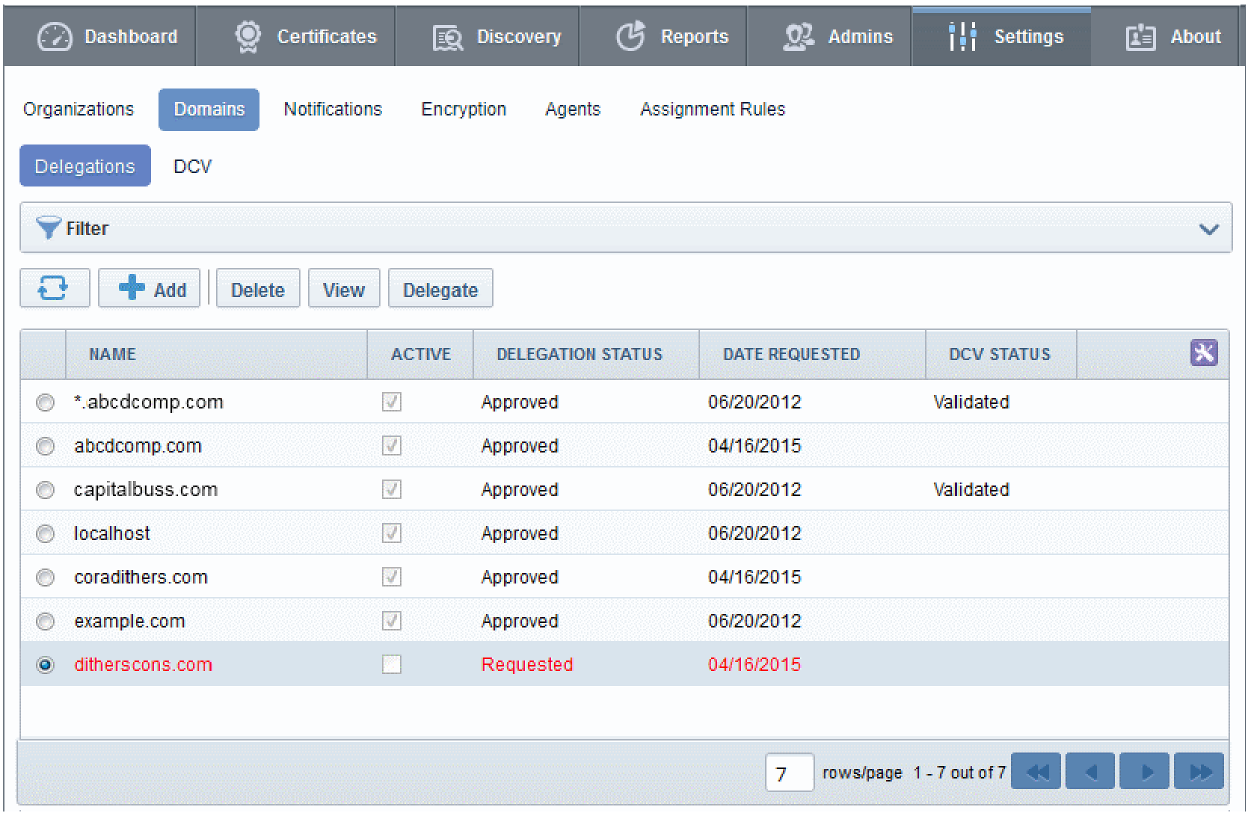
	NAME	ORGANIZATION	CITY	STATE	COUNTRY
●	Purchases Departement	Dithers Construction Company	River Dale	Alabama	US
○	Stores Department	Dithers Construction Company	River Dale	Alabama	US

The 'Departments' area similar to the 'Departments' dialog appearing on clicking the Departments button after selecting the checkbox beside an organization name from the 'Organizations' interface. Detailed explanations on the options and controls in this area are available at 5.2.2.5 Managing Departments of an Organization.

6.4 Domains

6.4.1 Section Overview

- The 'Domains' tab allows administrators to view all domains associated with organizations and departments.
- Admins can also create new domains, initiate domain control validation (DCV) and delegate domains to organizations/departments
- Admins can also restrict the certificate types that can be issued to specific domains



	NAME	ACTIVE	DELEGATION STATUS	DATE REQUESTED	DCV STATUS
○	*.abcdcomp.com	☑	Approved	06/20/2012	Validated
○	abcdcomp.com	☑	Approved	04/16/2015	
○	capitalbuss.com	☑	Approved	06/20/2012	Validated
○	localhost	☑	Approved	06/20/2012	
○	coradithers.com	☑	Approved	04/16/2015	
○	example.com	☑	Approved	06/20/2012	
●	ditherscons.com	□	Requested	04/16/2015	

- RAO admins:
  - RAOs can create, edit and assign domains to organizations and departments that have been delegated to them.
  - RAOs 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 Master Administrator(s).
- DRAO admins:
  - DRAOs can create, edit and assign domains to departments that have been delegated to them.
  - DRAOs 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 Master Administrator(s).
  - The 'Domain Awaiting Approval' notification will be sent to the Master Administrator only after the domain created by DRAO is first approved by RAO.

The following table provides a summary of the ability of administrators to manage domains:

Action	RAO Administrator	DRAO Administrator
Request New Domains for..	Delegated organizations Subordinate departments	Delegated departments
Approve/Reject New Domain Requests	✗ *(Responsibility of InCommon)*	✗ *(Responsibility of InCommon)*
Initiate Domain Control Validation (DCV)	✓	✓

Delegate Existing Domains to...	Subordinate Departments	✗
Activate/Deactivate Domains	✗ *(Responsibility of InCommon)*	✗ *(Responsibility of InCommon)*
Validating and Approving created Domains	✓ Can approve domains created by DRAO Administrators of the Departments under the Organization, prior to approval by the Master Administrator.	✗

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

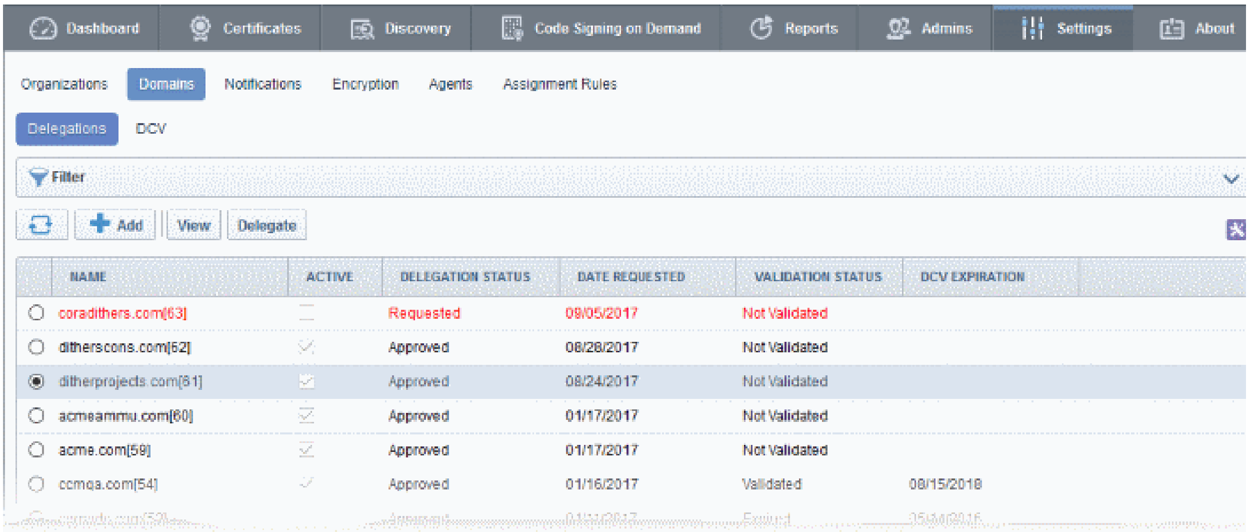
6.4.1.1 Wildcard Domains

- When a wildcard domain is validated by Master Administrator, 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 Master Administrator. For example, if *.example.com is delegated and validated for a specific organization 'Test Organization' and:
  - If an RAO wants to re-delegate the subdomain(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 Master Administrator.
  - If a DRAO wants to re-delegate the subdomain(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.

6.4.2 Domain Management

6.4.2.1 The Domains area

- Click 'Settings' > 'Domains' to open the domain management area:



	NAME	ACTIVE	DELEGATION STATUS	DATE REQUESTED	VALIDATION STATUS	DCV EXPIRATION
○	coradithers.com[63]	□	Requested	09/05/2017	Not Validated	
○	ditherscons.com[62]	✓	Approved	08/28/2017	Not Validated	
●	ditherprojects.com[61]	✓	Approved	08/24/2017	Not Validated	
○	acmeammu.com[60]	✓	Approved	01/17/2017	Not Validated	
○	acme.com[59]	✓	Approved	01/17/2017	Not Validated	
○	ccmqa.com[54]	✓	Approved	01/16/2017	Validated	08/15/2018

The domain management area has two tabs:

- Delegations - Delegation means whether or not the domain has been assigned to an organization or department. Incommon CM cannot issue certificates to adomain unless it has been delegated to an org/dep.
  This interface shows all enrolled domains along with their delegation status.

  A single domain can be delegated to any number of orgs/deps. You can add new domains and delegate them from this interface. You can also approve domain delegations made by other administrators.
- DCV - Domain Control Validation (DCV) status of all enrolled domains. You can initiate the DCV process from this screen.

6.4.2.1.1 Domain Delegations

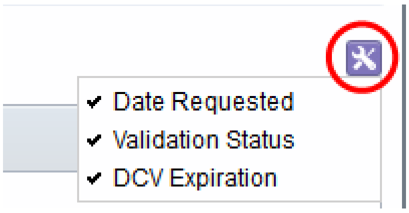
- Click 'Settings' > 'Domains' > 'Delegations' to view the domain delegations area.

The area shows a list of requested and approved domains.

- RAO Administrator:
  - RAOs can view and add new domains to organizations that have been delegated to them.
  - RAOs can delegate domains to their organizations/departments and approve domain requests from DRAOs.
  - Domains created or approved by an RAO need to be approved by Master Administrator(s) with appropriate privileges.
  - The RAO administrator can also create domains without delegating to them any organizations/departments.
  - Only the Master Administrator can view these undelegated domains and delegate to them required organizations/departments.
- DRAO Administrator:
  - DRAOs can view and add new domains to departments that have been delegated to them.
  - DRAOs can delegate domains to their departments. Domains requested a DRAO need to be approved by the organization RAO and then by two Master Administrators or a single Master Administrator with appropriate privileges.

- Domains created by DRAOs are to be validated and approved first by the RAO of the organization to which the department belongs and then by two Master Administrators or a single Master Administrator with appropriate privileges.
- The DRAO administrator can also create domains without delegating to them any organizations/departments.
- Only the Master Administrator can view these undelegated domains and delegate to them required organizations/departments.

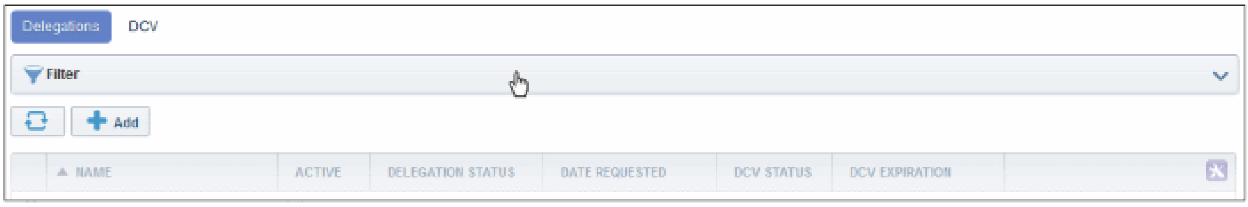
6.4.2.1.1.1 Summary of Fields and Controls

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.
Validation Status		Indicates the Domain Control Validation (DCV) status of the domain.
DCV Expiration		Indicates the date on which the DCV for the domain will expire.
Note: An administrator can enable or disable the columns from the drop-down button beside the last item in the table header:  		
Controls		Request a new domain for an existing organization or department.
	Add	Updates the list of displayed domains.
	Refresh	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.
Domain Control Buttons **Note**: The Domain control buttons are visible only on selecting a domain	View	Enables administrators to associate or delegate an existing domain to organizations and departments as required. **Note**: This control is not visible to DRAO Administrators.
	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.

6.4.2.1.1.2 Sorting and Filtering Options

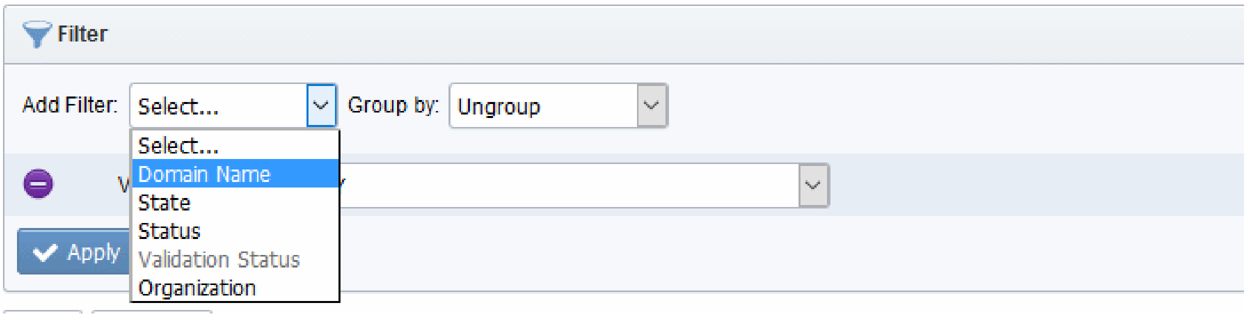
- Click a column header to sort items in order of the entries in the column

Administrators can search for particular domain by using filters:

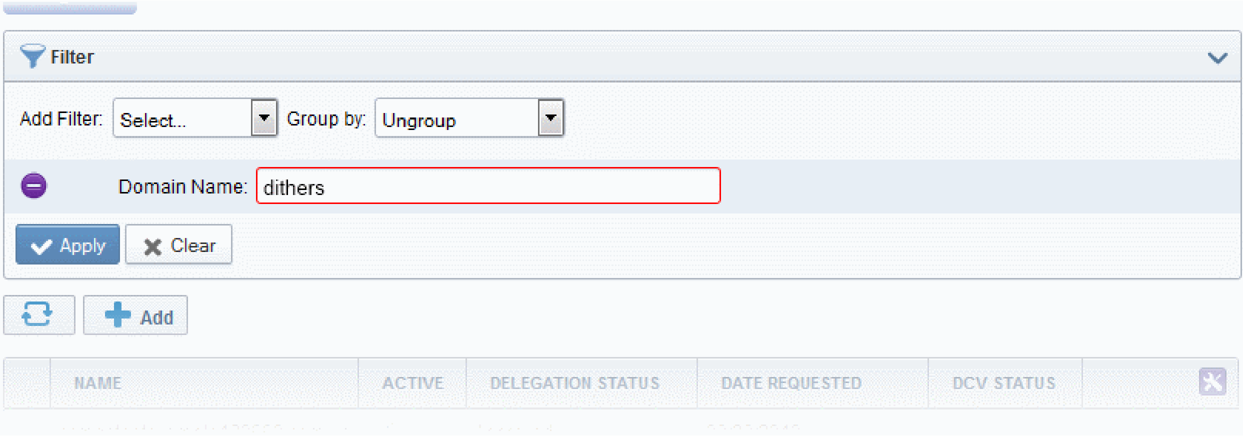


Filter Options	Description
Domain Name	Type a domain name to search for a particular domain.
State	• Active - Domains which have been enabled for certificate issuance. • Inactive - Domains which have been not been enabled for certificate issuance. • ANY - Shows both active and inactive domains.
Status	Filter by approval status: • Requested – Domains requested by RAOs and DRAOs which are awaiting approval by Master Administrator. • Approved - Domains which have been approved by Master Administrator. Certificates can be issued to approved domains providing they have also passed domain control validation. • ANY – Shows both requested and approved domains.
Validation Status	Filter by domain control validation status. • Not Validated - Displays the list of domains for which the validation process is not started or is in progress. • Validated - Displays the list of domains for which the domain control is validated. • Expired - Displays the list of domains for which DCV is expired. • ANY - Displays the list of all domains

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':



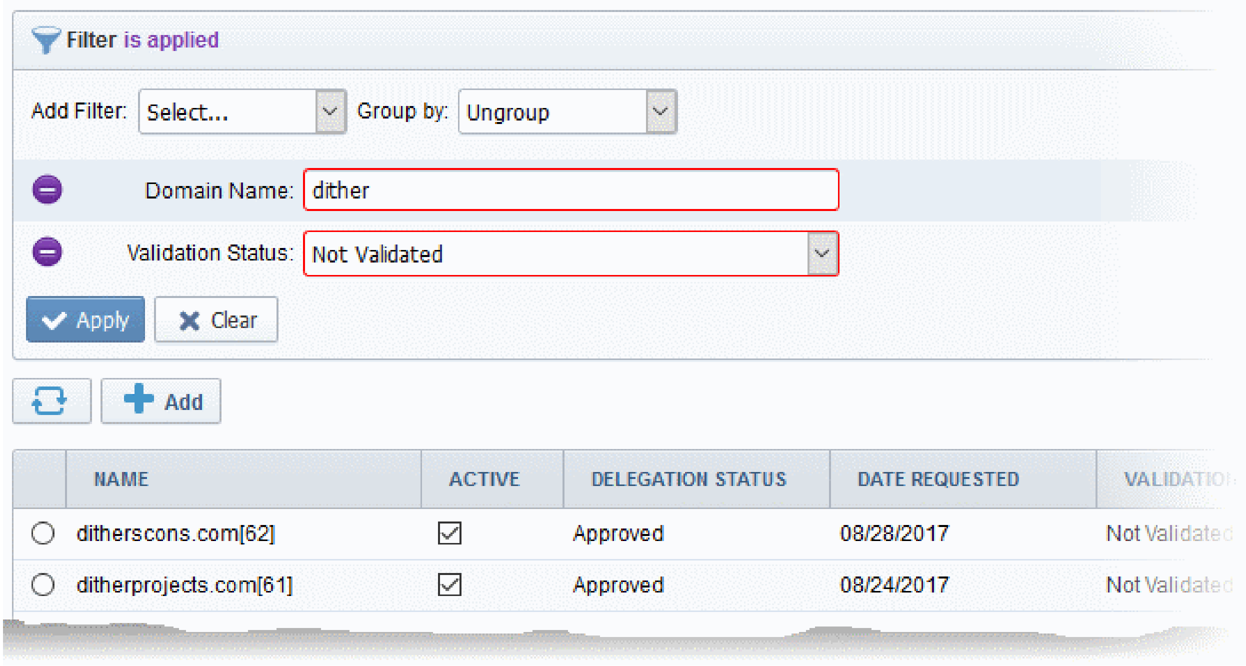
- Enter the domain name in part or full in the 'Name' field.



Domain Name: dithers

- 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:



Domain Name: dither

Validation Status: Not Validated

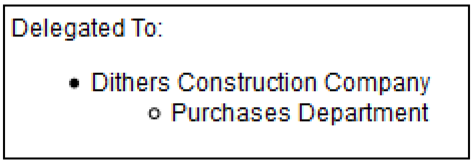
	NAME	ACTIVE	DELEGATION STATUS	DATE REQUESTED	VALIDATIO
○	ditherscons.com[62]	☑	Approved	08/28/2017	Not Validated
○	ditherprojects.com[61]	☑	Approved	08/24/2017	Not Validated

- 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.

6.4.2.1.1.3 Tool Tip

Place your mouse cursor over a domain to quickly view which organizations/departments it has been delegated to. The tool-tip also tells you if the domain is awaiting approval.

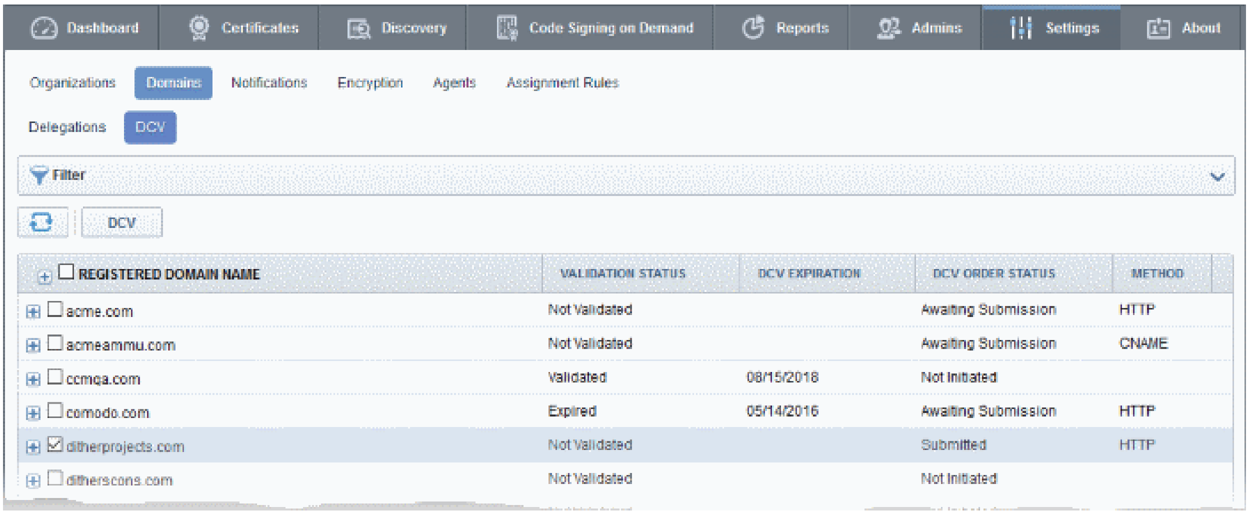


Delegated To:

- Dithers Construction Company
  - Purchases Department

6.4.2.1.2 DCV

- Click 'Settings' > 'Domains' > 'DCV' to open the domain control validation (DCV) area.



□ REGISTERED DOMAIN NAME	VALIDATION STATUS	DCV EXPIRATION	DCV ORDER STATUS	METHOD
□ acme.com	Not Validated		Awaiting Submission	HTTP
□ acmeammu.com	Not Validated		Awaiting Submission	CNAME
□ ccmqa.com	Validated	08/15/2018	Not Initiated	
□ comodo.com	Expired	05/14/2016	Awaiting Submission	HTTP
☑ ditherprojects.com	Not Validated		Submitted	HTTP
□ ditherscons.com	Not Validated		Not Initiated	

- The DCV area shows registered domains along with their DCV status and the date when DCV expires.
- Admins can initiate DCV on domains from here. A domain must pass DCV before Incommon can issue a certificate to it.
- DCV expires after 1 year and must be renewed. Existing certificates for the domain will remain valid even if DCV expires. However, you will need to pass DCV again in order to obtain new certificates for the domain.

Admin privileges:

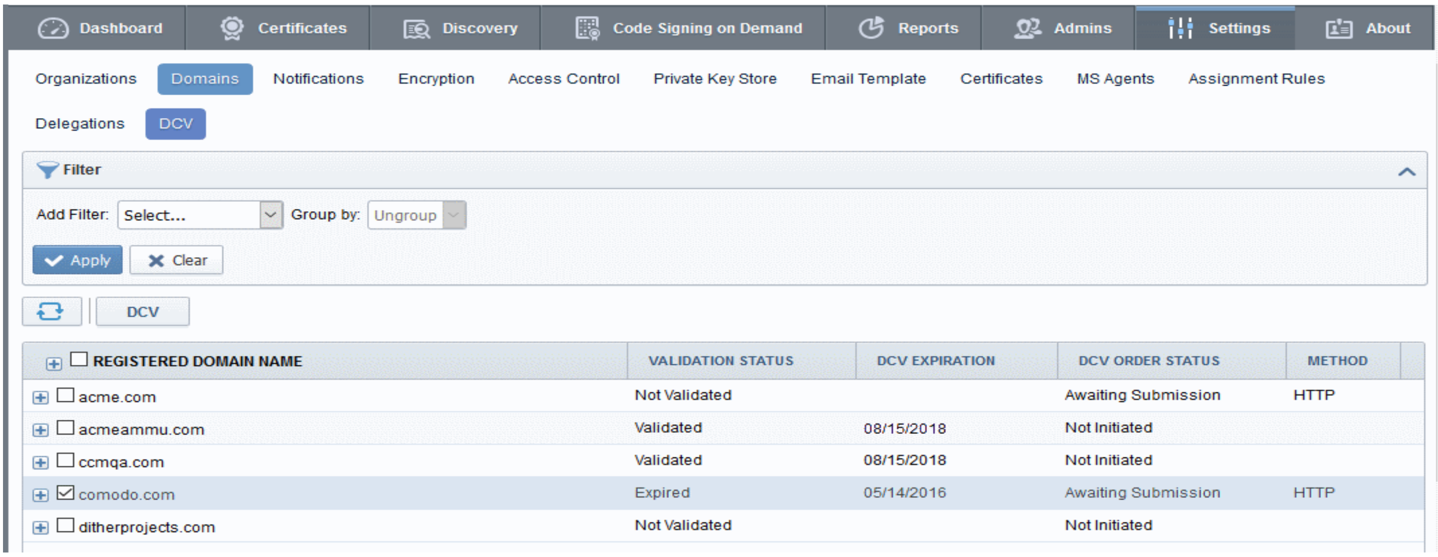
- MRAO Administrator - Can initiate DCV on any registered domain.
- RAO SSL Administrator - Can initiate DCV on domains which have been delegated to the RAO's organizations. DCV requests from an RAO must be approved by an MRAO.
- DRAO SSL Administrator - Can initiate DCV on domains which have been delegated to the DRAO's departments. DCV requests from a DRAO must be approved by an MRAO.

Administrators can choose from the following DCV methods:

- Email - InCommon CM will send an automated email with a validation link to the email address of the domain administrator holding control over the domain hosted on the company's web server. The domain will be validated on the domain administrator visiting the validation link in the mail.
- DNS CNAME - InCommon CM will send a hash value that must be entered as DNS CNAME for the domain. InCommon CM will validate by checking the DNS CNAME of the domain
- HTTP/HTTPS File - InCommon CM will send a .txt file which is to be placed at the root of the web server. InCommon CM 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, Incommon CM 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.

See Validating the Domain for more details on initiating DCV process.



☐ REGISTERED DOMAIN NAME	VALIDATION STATUS	DCV EXPIRATION	DCV ORDER STATUS	METHOD
☐ acme.com	Not Validated		Awaiting Submission	HTTP
☐ acmeammu.com	Validated	08/15/2018	Not Initiated	
☐ ccmqa.com	Validated	08/15/2018	Not Initiated	
☑ comodo.com	Expired	05/14/2016	Awaiting Submission	HTTP
☐ ditherprojects.com	Not Validated		Not Initiated	

6.4.2.1.2.1 Summary of Fields and Controls

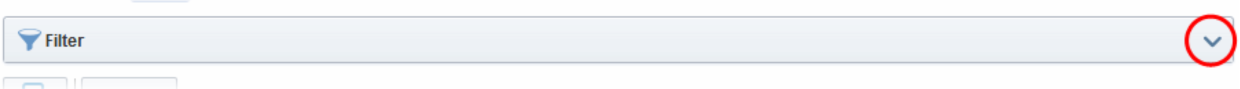
Column Display	Description
Registered Domain	A list of all available Domains created for this account. Clicking the '+' beside a domain name displays the sub-domains of the registered domain.
Validation Status	Whether the domain has passed DCV or not. Status can be one of the following: • Not Validated - DCV has not been initiated or is in-progress for the registered high level domain (HLD). • Validated - The registered high level domain has passed DCV • Expired - DCV on the domain has expired and has to be renewed. The DCV process has to be restarted for the domain
DCV Expiration	Indicates the date when Domain Control Validation for the domain expires. The DCV has to be done again after the expiry period.

Column Display	Description
DCV Order Status	Progress of validation on the domain. Status can be one of the following: • Not Initiated - DCV has not been started for the registered high level domain (HLD). • Awaiting Submittal - DCV has been initiated but the request has not yet been sent to the domain administrator (the admin who has control of the web server on which the domain is hosted). The 'Awaiting...' status is only available for the following DCV methods: • HTTP / HTTPS • CNAME • Submitted - The DCV request has been sent to the domain administrator for implementation. • Validated - The registered high level domain (HLD) has passed DCV. • Expired - DCV has expired on the domain. The DCV process has to be restarted for the domain .
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 RAO/DRAO SSL Administrators to initiate or restart the DCV process for the selected Domain.

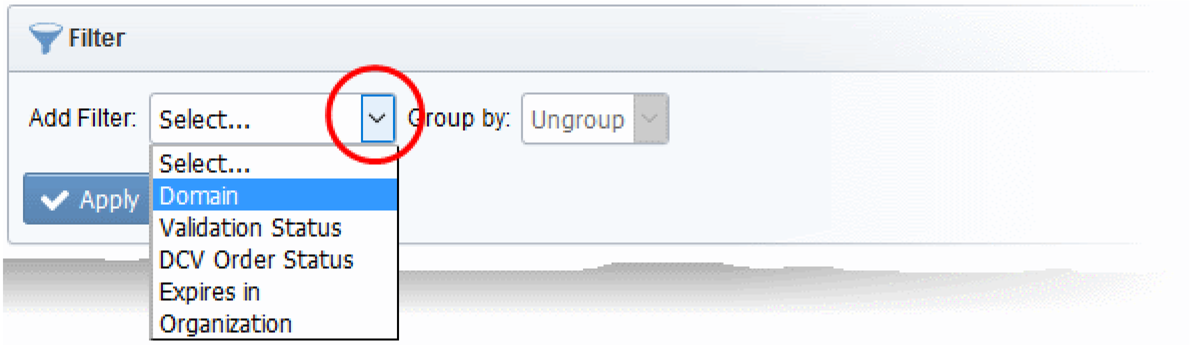
6.4.2.1.2.2 Sorting and Filtering Options

- Click a column header to sort items in order of the entries in the column

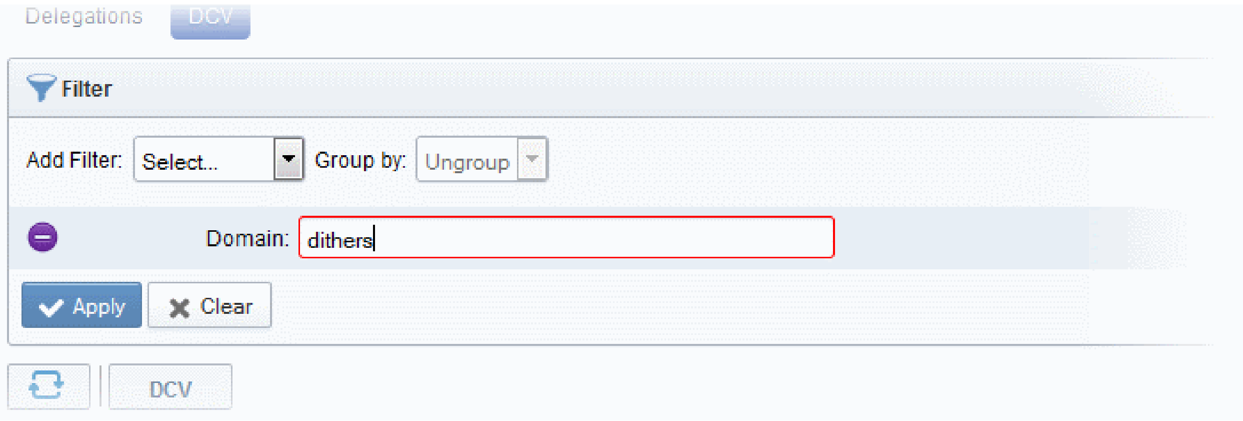
Administrators can search for particular domain by using filters:



To apply filters, click on the down arrow at the right end of the 'Filters' stripe. The filter options will be displayed. 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.



- Enter name of the domain in part or full in the Name field.



Domain: dithers

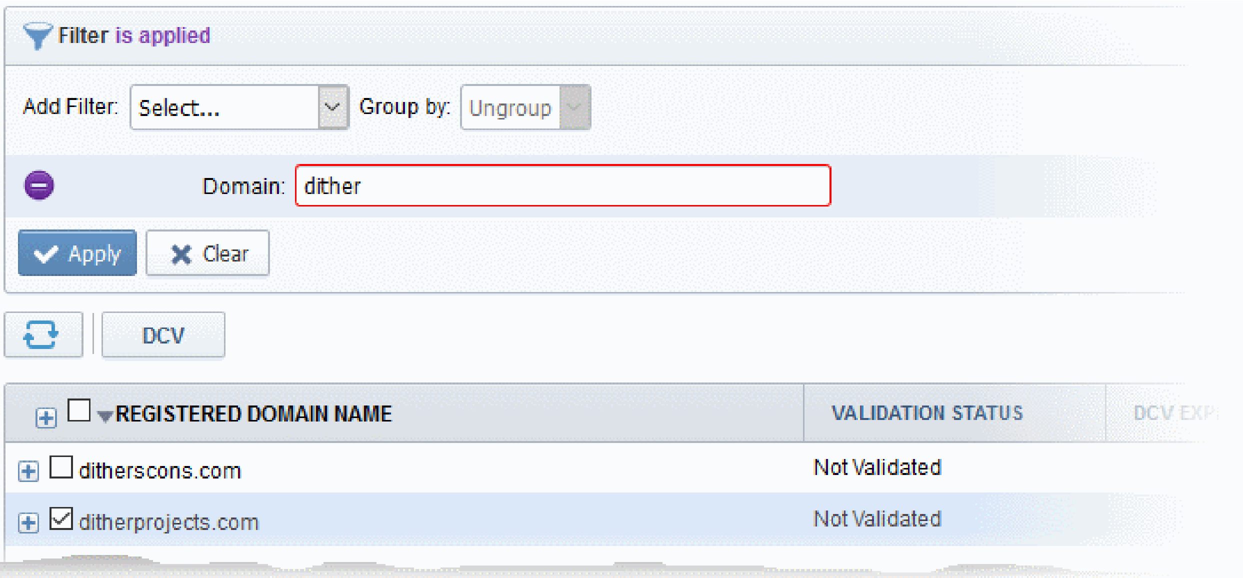
The available filter criteria and their filter parameters are given in the following table:

Filter Options	Description
Domain	Filter the list of domains by name.
Validation Status	Filter domains based on their validation status: • ANY - Will show all domains. No filters are applied. • Not Validated – Shows domains which have not yet pass Domain Control Validation (DCV). A domain must pass DCV before Incommon can issue certificates to it. Admins should initiate the DCV process on required domains. • Validated - Domains which have successfully passed Domain Control Validation (DCV). • Expired - Domains on which DCV has expired. DCV lasts for one before it must be renewed. Existing certificates will remain valid, but you must pass DCV on the domain again before you can order new certificates for it.
DCV Order Status	Filter domains based on their DCV Order status: • ANY - Displays the list of all the domains • Not Started – Domains for which the DCV process has not yet been started • Awaiting Submittal - Domains for which the DCV process was initiated but the request has not yet been submitted for approval by the domain administrator. • Submitted - Domains for which DCV has been submitted to domain administrator for approval. • Validated - Displays only domains which have passed DCV. • Expired - Displays a list of domains on which DCV has expired.
Expires in	Enables Administrators to filter the list of domains based on the remaining days for their

Filter Options	Description
	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

- Click the 'Apply' button.

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



Domain: dither

REGISTERED DOMAIN NAME	VALIDATION STATUS
□ ditherscons.com	Not Validated
☑ ditherprojects.com	Not Validated

- 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.

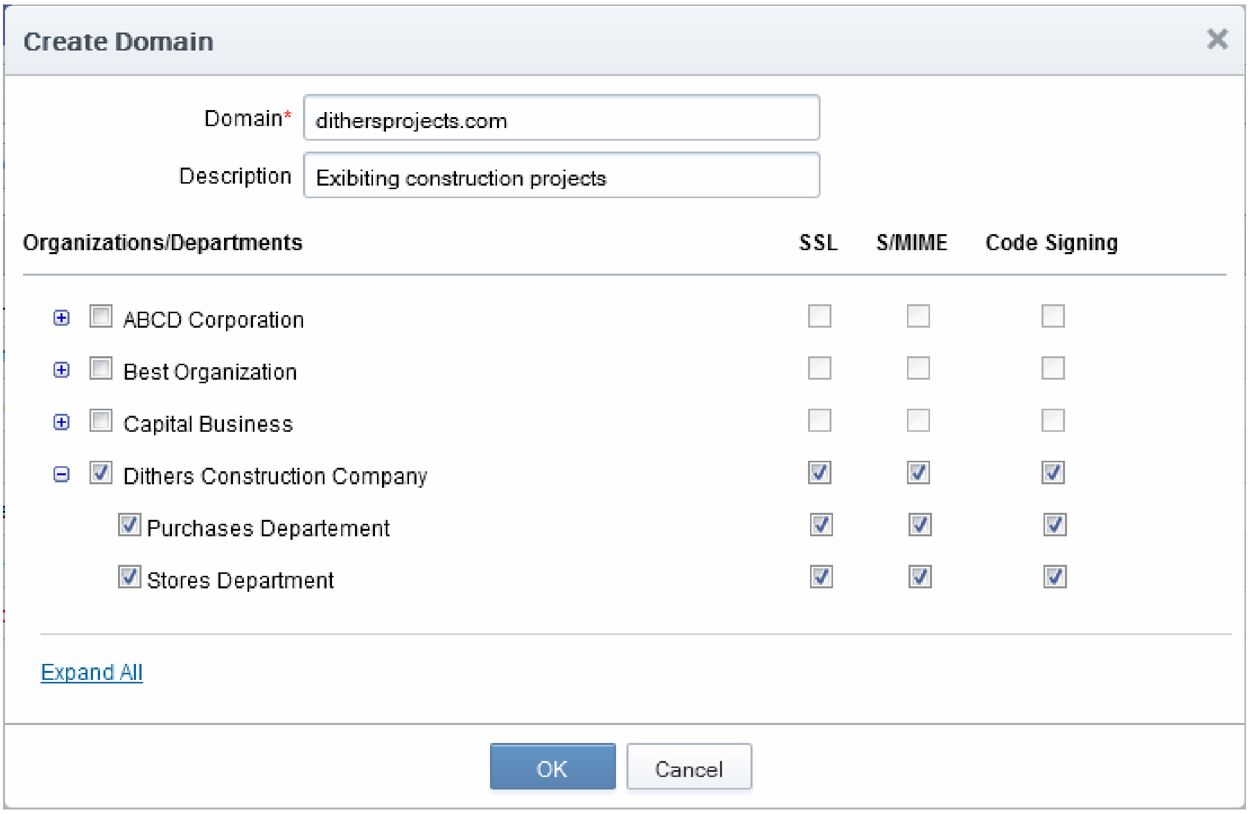
6.4.2.2 Create a New Domain

- Before you can request certificates, you first need to create domains then delegate them to organizations/departments.

- Delegated domains must pass Domain Control Validation (DCV). DCV must be initiated by RAO/DRAO SSL with sufficient privileges.
- Only approved and validated domains are facilitated for the request and approval of the SSL certificates and the issuance of client certificates to the end-users falling within the domain.
- 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.

Note: The administrator can select the certificate type for the domain depending on the privilege levels. E.g. A RAO SSL administrator can allow or restrict the availability of only SSL certificates for the created domain.

To create a new domain click the 'Add' button located at the top of the 'Domains' area. This will open the 'Create domain' dialog.



Create Domain

Domain* dithersprojects.com

Description Exibiting construction projects

Organizations/Departments	SSL	S/MIME	Code Signing
⊞ □ ABCD Corporation	□	□	□
⊞ □ Best Organization	□	□	□
⊞ □ Capital Business	□	□	□
⊟ ☑ Dithers Construction Company	☑	☑	☑
☑ Purchases Departement	☑	☑	☑
☑ Stores Department	☑	☑	☑

6.4.2.2.1 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	*Check-boxes*	• Enables the administrator to delegate the currently created domain to

Field Name	Values	Description
		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 'Expand All' expands the tree structure to display all the departments under each organization. • Clicking 'Collapse All' in the expanded view collapses the tree structure of all the organizations and hides the departments under each organization.
SSL, Smime, Code Signing	*Check-boxes*	• 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.

6.4.2.2.2 Validating Domains

- Any domain added to InCommon CM must pass Domain Control Validation (DCV) before InCommon can issue certificates to it.
- DCV requires your company to prove it has control of the domain.
- The domain administrator can confirm control via email validation, or by placing a .txt file in a publicly accessible location, or by making a DNS CNAME entry.
- InCommon CM Administrators can initiate DCV on an individual basis or, if all domains share a common 'WhoIs' email record, may initiate DCV on multiple domains at once.

Admin privileges

- RAO SSL Administrator - Can initiate DCV on domains which have been delegated to the RAO's organizations. DCV requests from an RAO must be approved by a master administrator
- DRAO SSL Administrator - Can initiate DCV on domains which have been delegated to the DRAO's departments. DCV requests from a DRAO must be approved by a master administrator.

There are three possible methods of completing DCV:

- Email - InCommon CM will send a challenge-response email to a mail address on the domain. You can choose the email address during setup. The email will contain a link to validate your ownership of the domain. The email method can be used for both validating a single domain and multiple domains at a time.
- DNS CNAME - InCommon CM will generate a hash value that must be entered as DNS CNAME for the domain. InCommon CM will validate by checking the DNS CNAME of the domain.
- HTTP/HTTPS File - InCommon CM will generate a .txt file which is to be placed on the root of the web server. InCommon CM will check for the presence of the file.

If a wildcard domain is created and delegated to an Organization or a Department, InCommon CM 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.

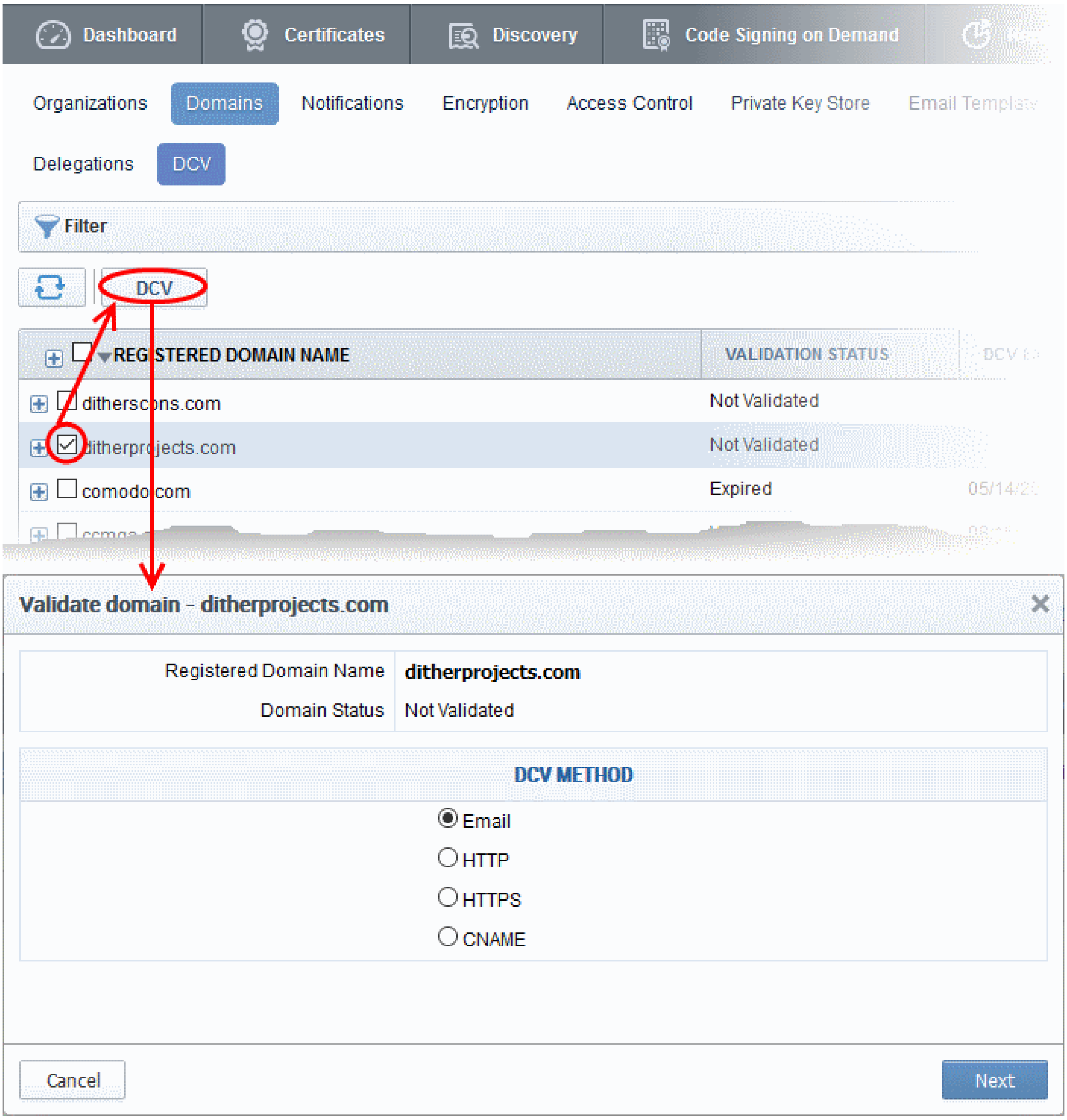
The following sections explain on:

- Validating a single domain
- Validating multiple domains at a time

Validating a Single Domain

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:



REGISTERED DOMAIN NAME	VALIDATION STATUS	DCV E
□ ditherscons.com	Not Validated	
☑ ditherprojects.com	Not Validated	
□ comodo.com	Expired	05/14/2
□ ccmqa		08/

Validate domain - ditherprojects.com

Registered Domain Name	ditherprojects.com
Domain Status	Not Validated

DCV METHOD

● Email
○ HTTP
○ HTTPS
○ CNAME

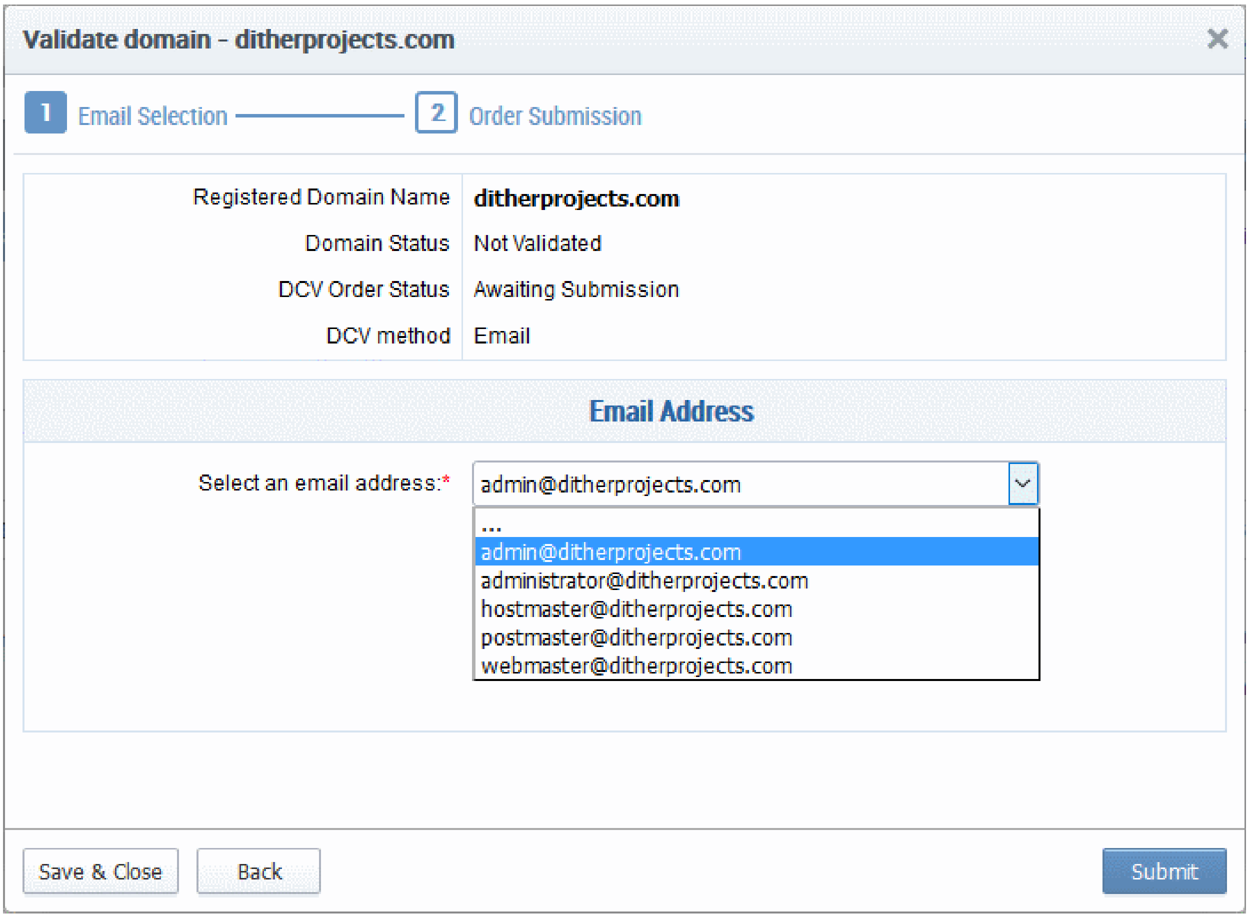
Select the DCV method from:

- 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.



Validate domain - ditherprojects.com

×
1 Email Selection
2 Order Submission

Registered Domain Name	**ditherprojects.com**
Domain Status	Not Validated
DCV Order Status	Awaiting Submission
DCV method	Email

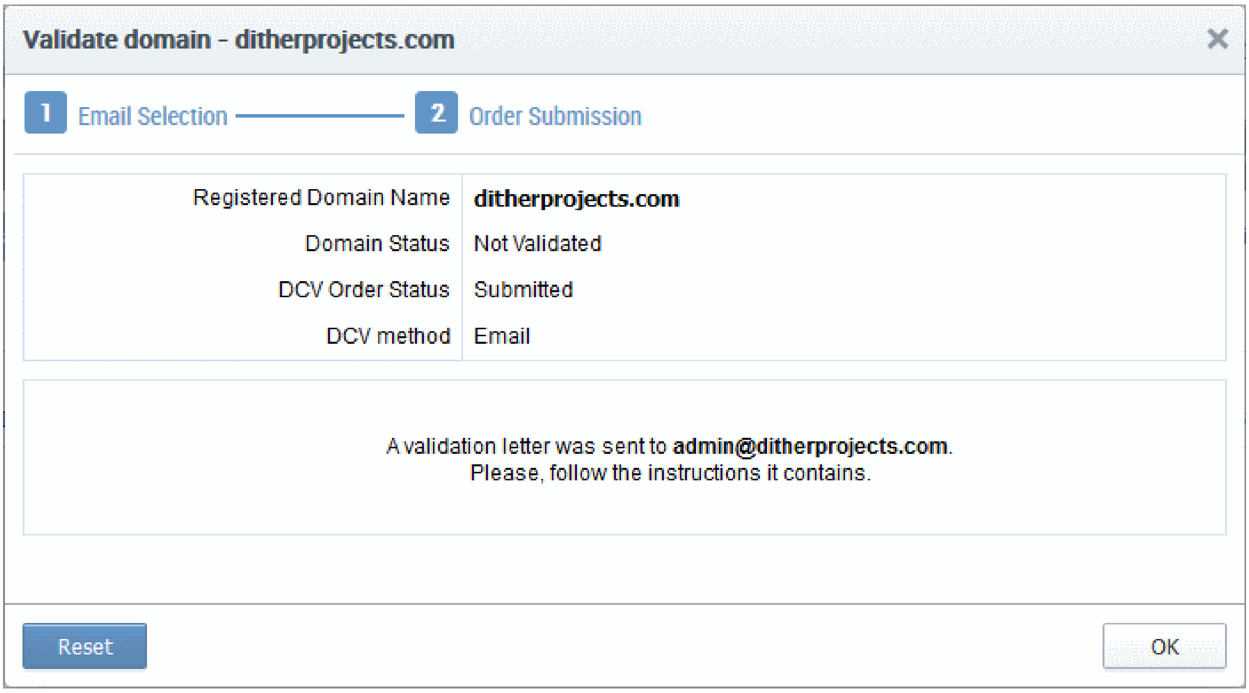
Email Address

Select an email address:* admin@ditherprojects.com

...
admin@ditherprojects.com
administrator@ditherprojects.com
hostmaster@ditherprojects.com
postmaster@ditherprojects.com
webmaster@ditherprojects.com
Save & Close
Back
Submit

3. Select the email address of the administrator who can receive and respond to the validation mail from the drop-down and click 'Submit'.
4. To send the validation email at a later time, click 'Save & Close'. On restarting the DCV process for the domain, the administrator email will be auto-selected.

An automated email will be sent to the selected Domain Administrator email address. The DCV Order status of the Domain will change to 'Submitted'.



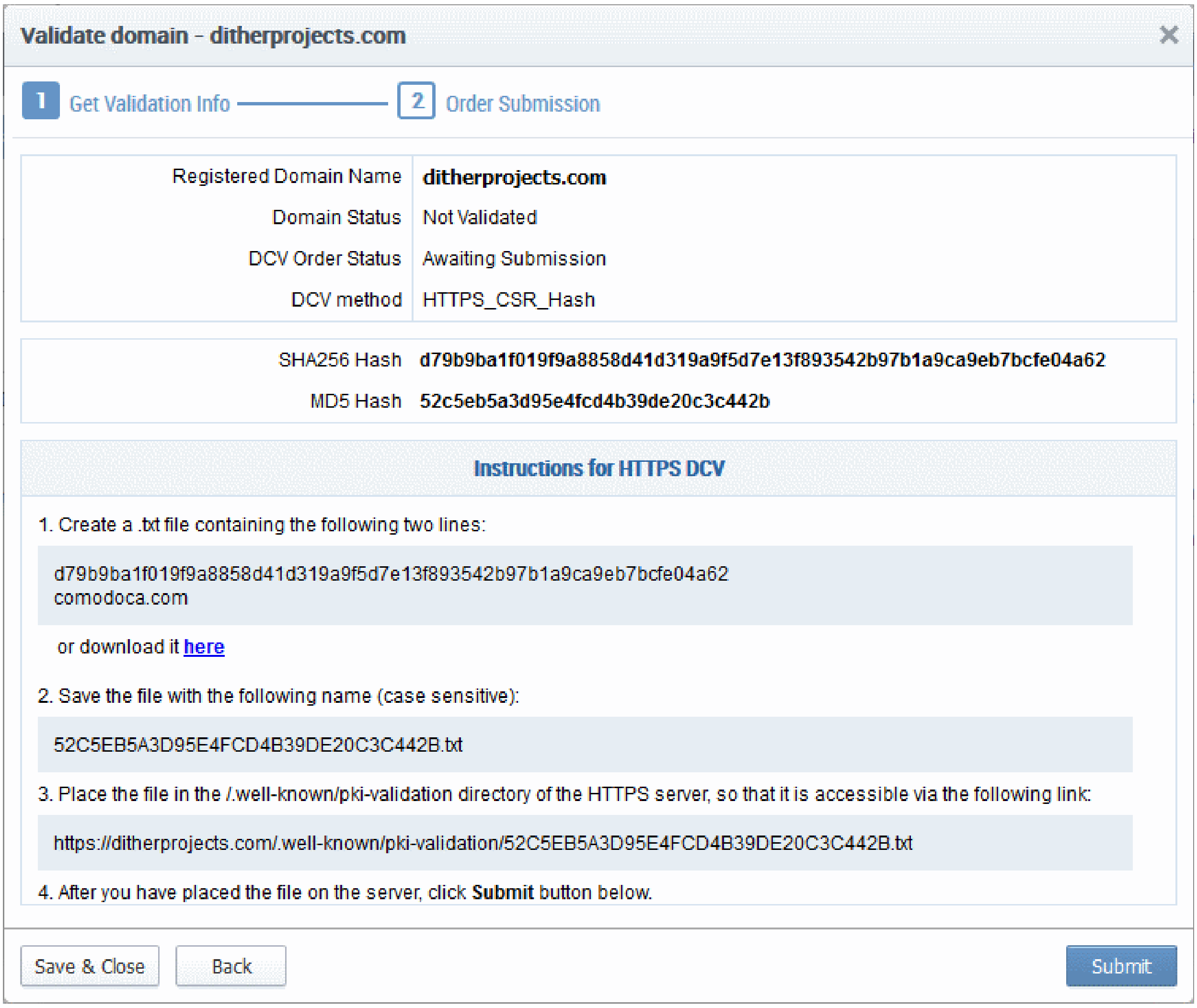
Registered Domain Name	**ditherprojects.com**
Domain Status	Not Validated
DCV Order Status	Submitted
DCV method	Email

A validation letter was sent to **admin@ditherprojects.com**.
Please, follow the instructions it contains.

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 Order 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. InCommon CM 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'.



Validate domain - ditherprojects.com

Registered Domain Name	**ditherprojects.com**
Domain Status	Not Validated
DCV Order Status	Awaiting Submission
DCV method	HTTPS_CSR_Hash

SHA256 Hash	**d79b9ba1f019f9a8858d41d319a9f5d7e13f893542b97b1a9ca9eb7bcfe04a62**
MD5 Hash	**52c5eb5a3d95e4fcd4b39de20c3c442b**

Instructions for HTTPS DCV

1. Create a .txt file containing the following two lines:

```
d79b9ba1f019f9a8858d41d319a9f5d7e13f893542b97b1a9ca9eb7bcfe04a62
comodoca.com
```

or download it here

2. Save the file with the following name (case sensitive):

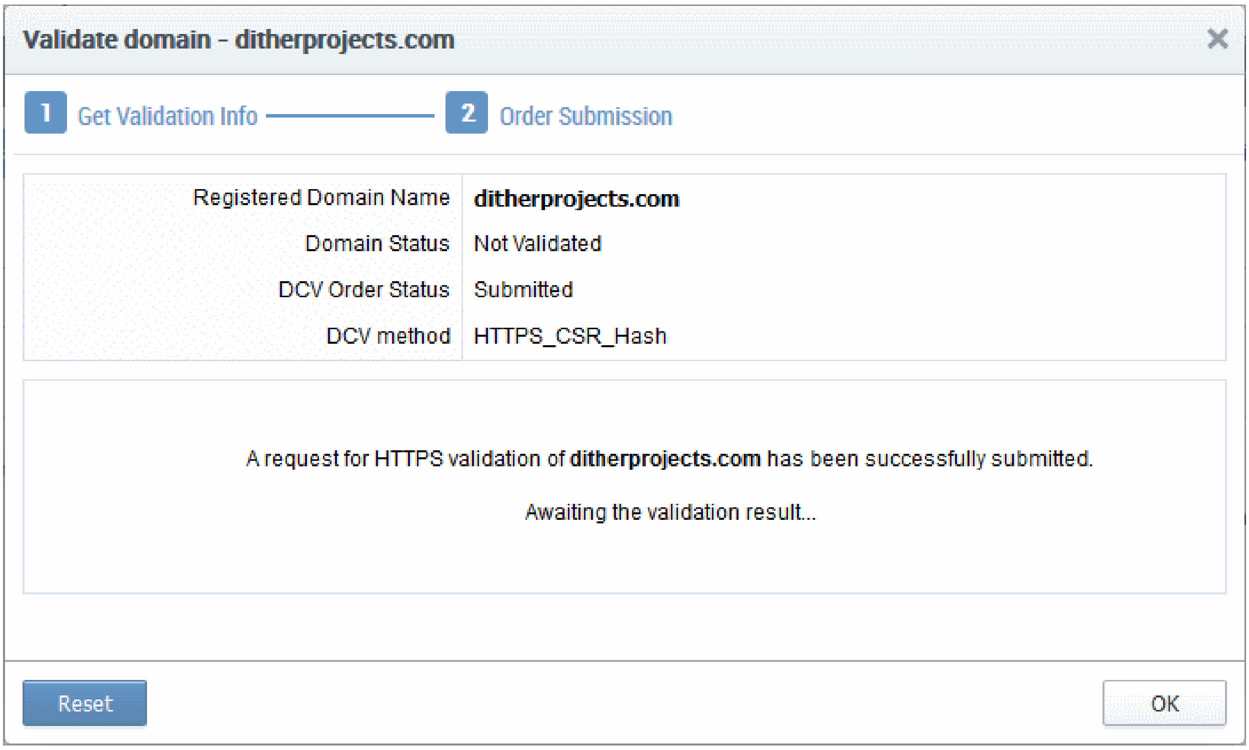
```
52C5EB5A3D95E4FCD4B39DE20C3C442B.txt
```

3. Place the file in the /.well-known/pki-validation directory of the HTTPS server, so that it is accessible via the following link:

```
https://ditherprojects.com/.well-known/pki-validation/52C5EB5A3D95E4FCD4B39DE20C3C442B.txt
```

4. After you have placed the file on the server, click **Submit** button below.

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 'Save & Close'. InCommon CM 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 selecting the domain and clicking the 'DCV' button
8. Click 'Submit'. The DCV Order status of the domain will change to 'Submitted'.



Validate domain - ditherprojects.com

Registered Domain Name	**ditherprojects.com**
Domain Status	Not Validated
DCV Order Status	Submitted
DCV method	HTTPS_CSR_Hash

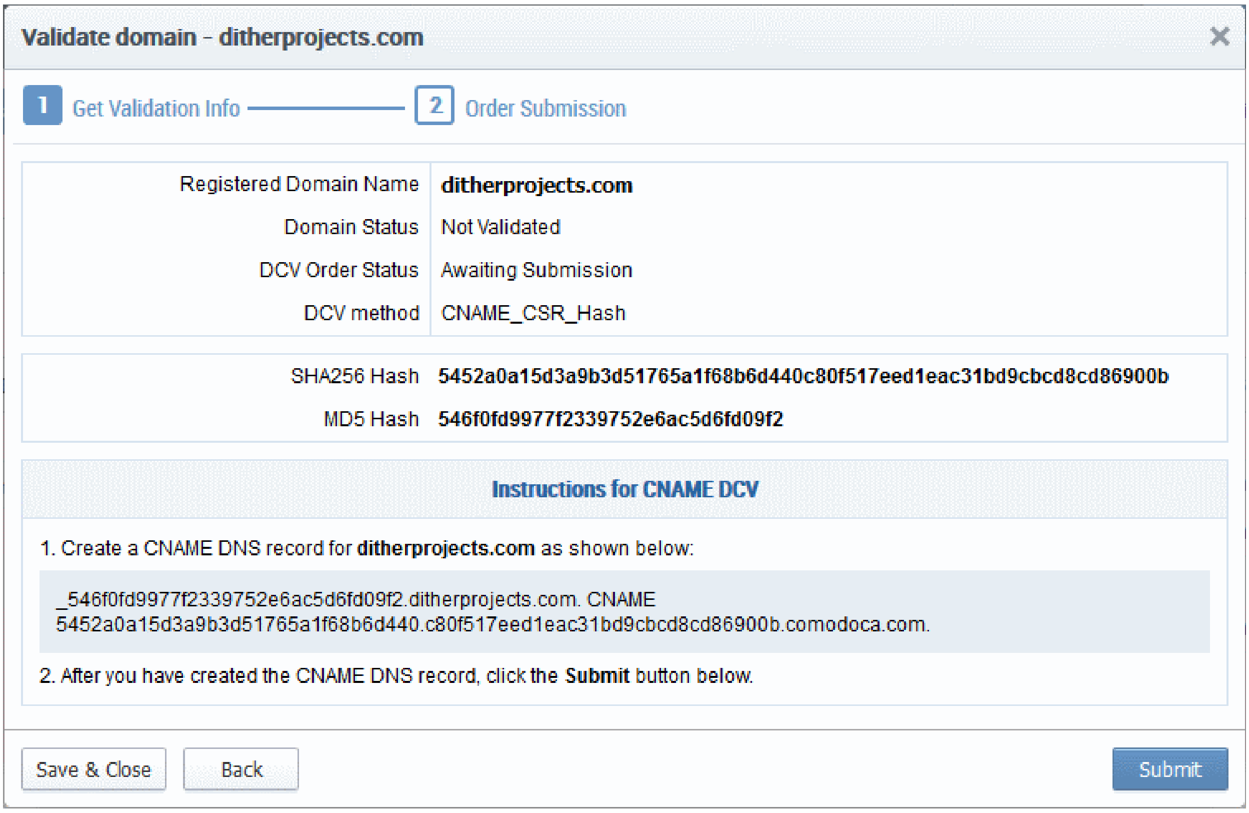
A request for HTTPS validation of **ditherprojects.com** has been successfully submitted.

Awaiting the validation result...

9. InCommon CM will check whether the file has been placed in the web server root and validate the domain. On successful validation, the DCV Order status of the domain will change to 'Validated'.

DNS CName

On selection of CNAME method, InCommon CM 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'.



Validate domain - ditherprojects.com

Registered Domain Name	**ditherprojects.com**
Domain Status	Not Validated
DCV Order Status	Awaiting Submission
DCV method	CNAME_CSR_Hash

SHA256 Hash	**5452a0a15d3a9b3d51765a1f68b6d440c80f517eed1eac31bd9cbcd8cd86900b**
MD5 Hash	**546f0fd9977f2339752e6ac5d6fd09f2**

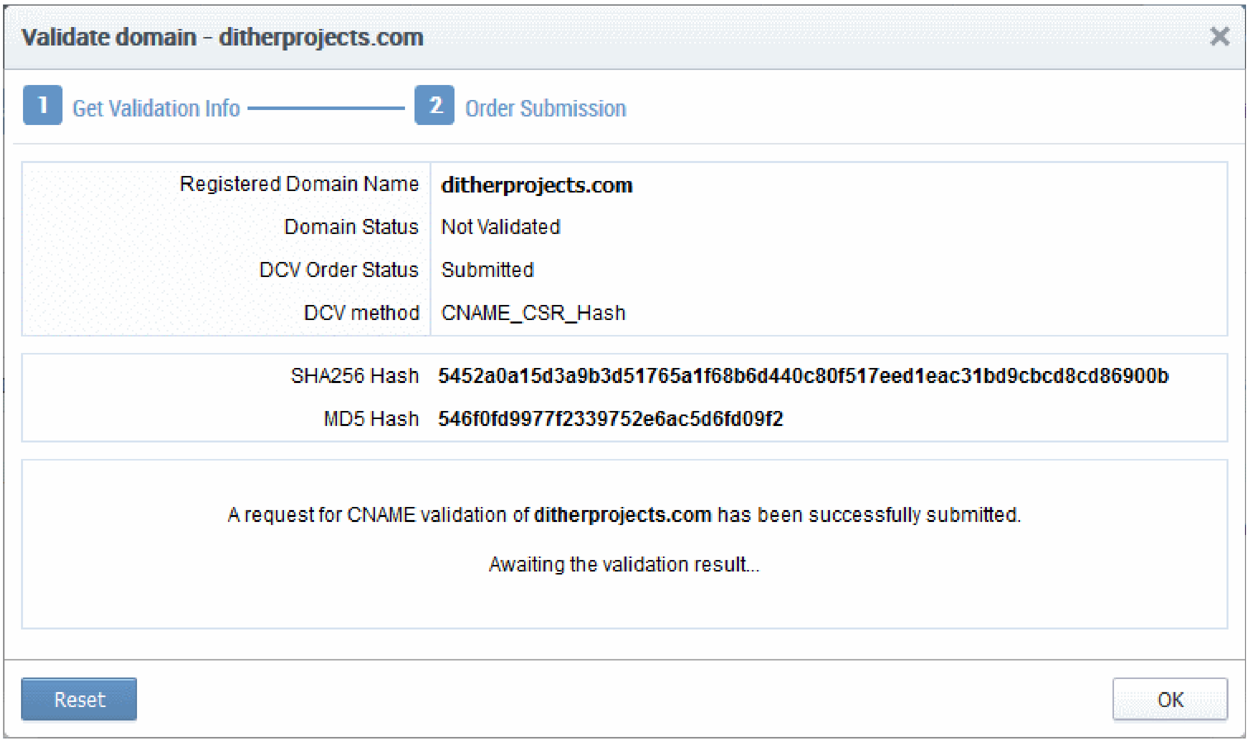
Instructions for CNAME DCV

1. Create a CNAME DNS record for **ditherprojects.com** as shown below:

```
_546f0fd9977f2339752e6ac5d6fd09f2.ditherprojects.com. CNAME
5452a0a15d3a9b3d51765a1f68b6d440.c80f517eed1eac31bd9cbcd8cd86900b.comodoca.com.
```

2. After you have created the CNAME DNS record, click the **Submit** button below.

3. Copy the CNAME DNS record given in item no. 1 and pass it to the domain administrator through any out-of-band communication method like email and request the domain administrator to create the record for the domain.
4. Click 'Save & Close'. InCommon CM 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 selecting the domain and clicking the 'DCV' button.
7. Click 'Submit'.The DCV Order status of the domain will change to 'Submitted'.



Validate domain - ditherprojects.com

Registered Domain Name	**ditherprojects.com**
Domain Status	Not Validated
DCV Order Status	Submitted
DCV method	CNAME_CSR_Hash

SHA256 Hash	**5452a0a15d3a9b3d51765a1f68b6d440c80f517eed1eac31bd9cbcd8cd86900b**
MD5 Hash	**546f0fd9977f2339752e6ac5d6fd09f2**

A request for CNAME validation of **ditherprojects.com** has been successfully submitted.

Awaiting the validation result...

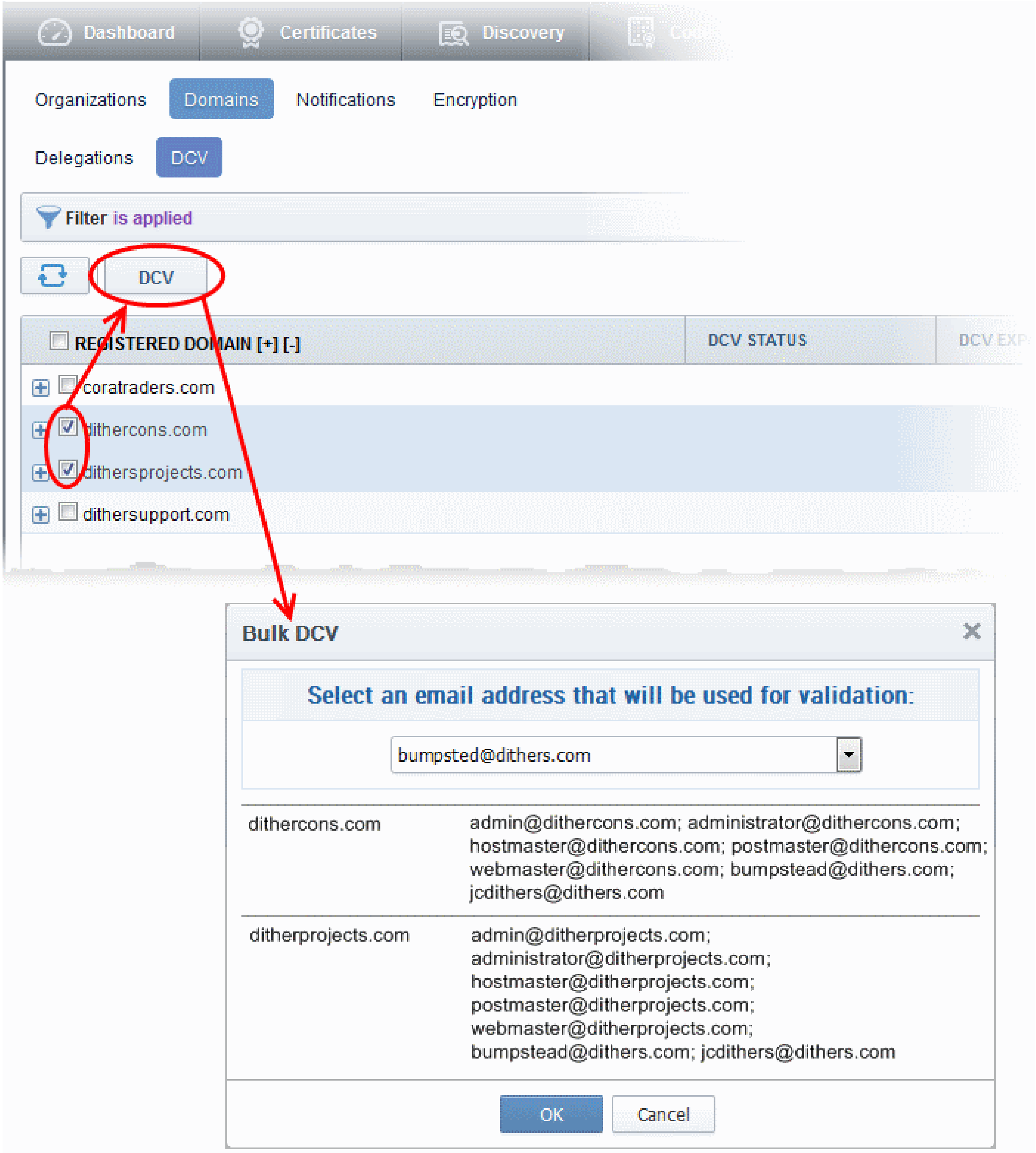
8. InCommon CM will check whether the record has been created. If it is found created, the DCV Order status of the domain will change to 'Validated'.

Validating Multiple Domains at a time

Domain Control Validation (DCV) can be initiated for multiple domains that share a common domain administrative email account in the WhoIs database, at once.

To initiate Bulk DCV for multiple domains

1. Open the DCV interface by clicking 'Settings' > 'Domains' > 'DCV'.
2. Select the domains that share common domain administrator email address
3. Click the 'DCV' button

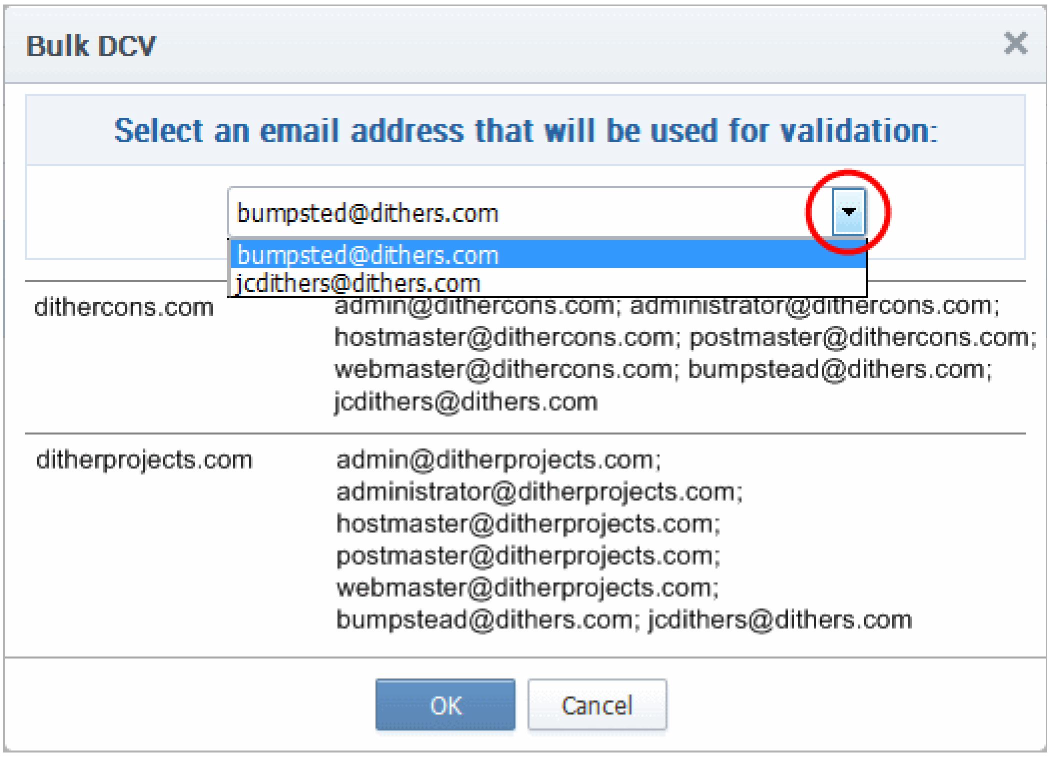


Select an email address that will be used for validation:

bumpsted@dithers.com

dithercons.com	admin@dithercons.com; administrator@dithercons.com; hostmaster@dithercons.com; postmaster@dithercons.com; webmaster@dithercons.com; bumpstead@dithers.com; jcdithers@dithers.com
ditherprojects.com	admin@ditherprojects.com; administrator@ditherprojects.com; hostmaster@ditherprojects.com; postmaster@ditherprojects.com; webmaster@ditherprojects.com; bumpstead@dithers.com; jcdithers@dithers.com

The Bulk DCV dialog will open. The dialog contains lists of possible domain administrator email addresses and the email addresses fetched from the WhoIs database for each domain. Common email addresses identified from the lists are displayed in the drop-down at the top.



Bulk DCV

Select an email address that will be used for validation:

bumpsted@dithers.com

bumpsted@dithers.com
jcdithers@dithers.com

dithercons.com	admin@dithercons.com; administrator@dithercons.com; hostmaster@dithercons.com; postmaster@dithercons.com; webmaster@dithercons.com; bumpstead@dithers.com; jcdithers@dithers.com
ditherprojects.com	admin@ditherprojects.com; administrator@ditherprojects.com; hostmaster@ditherprojects.com; postmaster@ditherprojects.com; webmaster@ditherprojects.com; bumpstead@dithers.com; jcdithers@dithers.com

4. Select the email address of the administrator who can receive and respond to the validation mail from the drop-down and click 'OK'.

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 to open the validation form and enter the validation code contained in the email, in order to complete the validation process. Once completed, the DCV status of the Domains will change to 'Validated'.

6.4.2.2.2.1 Changing DCV method for Validation Pending Domains

The RAO/DRAO SSL Administrator with appropriate privileges can change the DCV method for the domains whose validation is pending, from the DCV interface.

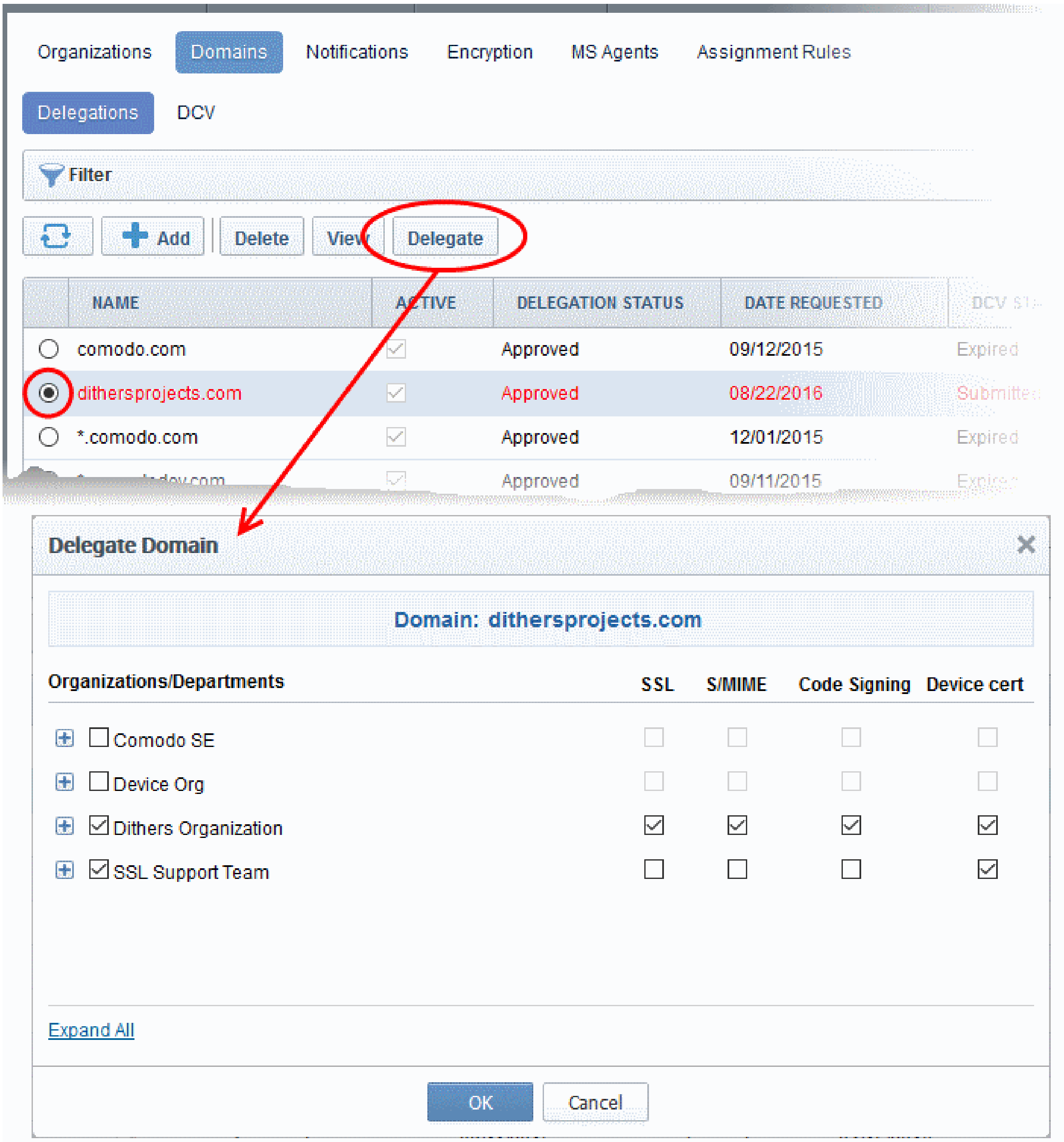
To change the validation method

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.

6.4.2.3 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.



	NAME	ACTIVE	DELEGATION STATUS	DATE REQUESTED	DCV ST...
○	comodo.com	☑	Approved	09/12/2015	Expired
●	dithersprojects.com	☑	Approved	08/22/2016	Submitte...
○	*.comodo.com	☑	Approved	12/01/2015	Expired
	*.[illegible]dev.com	☑	Approved	09/11/2015	Expire...

Delegate Domain ✕

Domain: dithersprojects.com

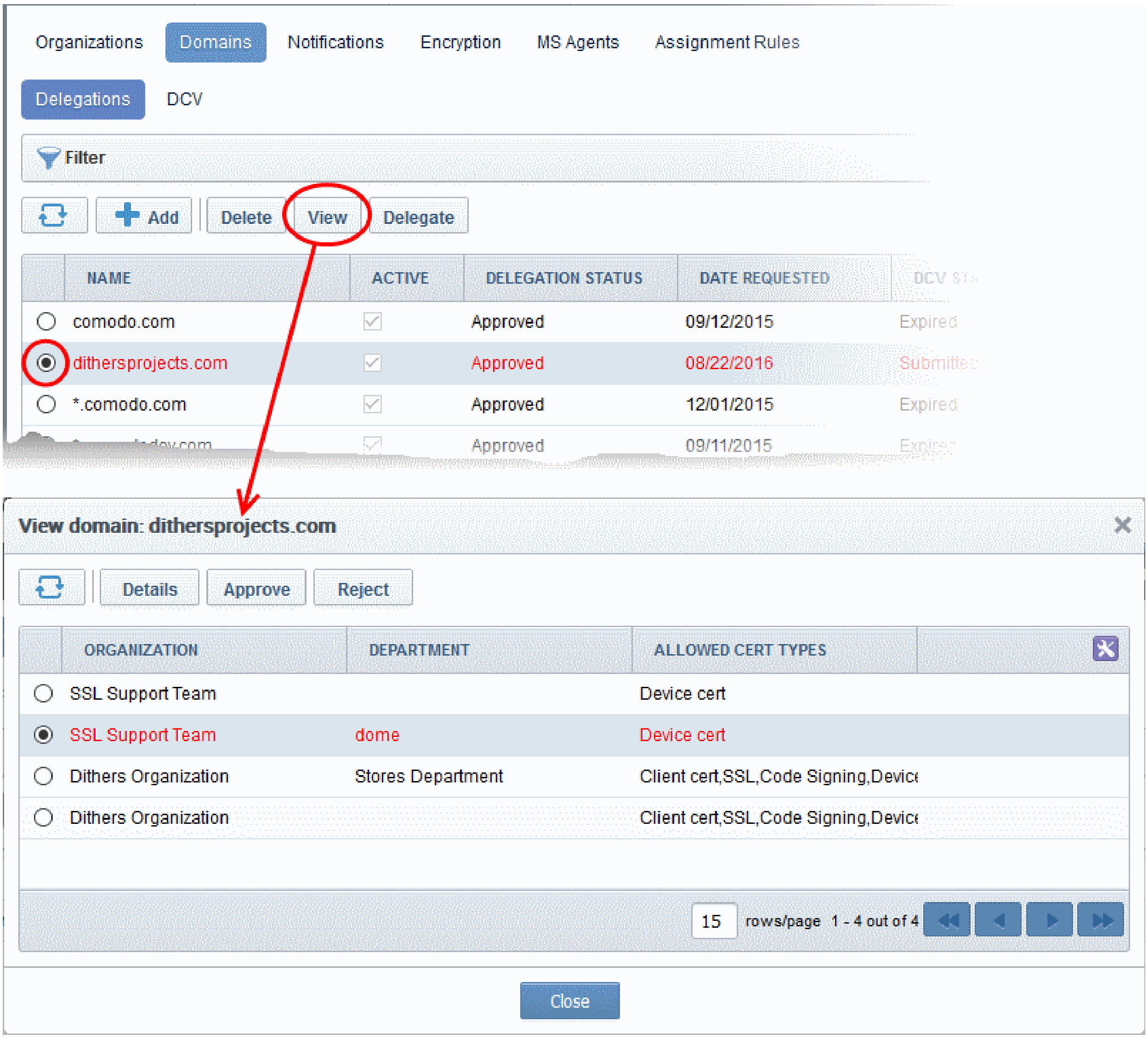
Organizations/Departments	SSL	S/MIME	Code Signing	Device cert
⊞ □ Comodo SE	□	□	□	□
⊞ □ Device Org	□	□	□	□
⊞ ☑ Dithers Organization	☑	☑	☑	☑
⊞ ☑ SSL Support Team	□	□	□	☑

- 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 by other administrators are to be approved by the Master Administrator at Incommon CA.
- Full details on delegating a domain are available in the previous section, 'Create Domain - Table of Parameters'.

6.4.2.4 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.
    - To do this, administrators should select the domain and click the 'View' button from the top.
- The view dialog also enables the administrators to view the requisition details of the domain and Master Administrator to validate and approve the domains created by other administrators.
- The domain becomes active only after the Master Administrator approves it and only then it enables for request and issuance of SSL certificates, Client certificates and Code Signing certificates.



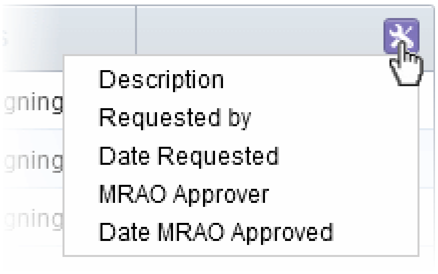
	NAME	ACTIVE	DELEGATION STATUS	DATE REQUESTED	DCV S
○	comodo.com	✓	Approved	09/12/2015	Expired
●	dithersprojects.com	✓	Approved	08/22/2016	Submittec
○	*.comodo.com	✓	Approved	12/01/2015	Expired
	*.[illegible]ladev.com	✓	Approved	09/11/2015	Expir

View domain: dithersprojects.com

	ORGANIZATION	DEPARTMENT	ALLOWED CERT TYPES
○	SSL Support Team		Device cert
●	SSL Support Team	dome	Device cert
○	Dithers Organization	Stores Department	Client cert,SSL,Code Signing,Device
○	Dithers Organization		Client cert,SSL,Code Signing,Device

15 rows/page 1 - 4 out of 4

6.4.2.4.1 View Domain - Summary of Fields and Controls

<table>
<tr><th>Column Display</th><th colspan="2">Description</th></tr>
<tr><td>Organization</td><td colspan="2">Displays the list of all Organizations delegated to the selected domain. List is displayed in ascending alphabetical order.</td></tr>
<tr><td>Department</td><td colspan="2">Displays the list of Department that is delegated the domain.</td></tr>
<tr><td>Description</td><td colspan="2">Short description of the domain</td></tr>
<tr><td>Requested by</td><td colspan="2">Displays the name of the administrator who has created the domain.</td></tr>
<tr><td>Date Requested</td><td colspan="2">The date at which the domain was added to the CM.</td></tr>
<tr><td>Date Approved</td><td colspan="2">The date at which the domain was added approved.</td></tr>
<tr><td>Allowed Cert Types</td><td colspan="2">The Certificate types that are enabled and available for the domain.</td></tr>
<tr><td colspan="3">Note: An administrator can enable or disable the columns from the drop-down button beside the last item in the table header:
 </td></tr>
<tr><td>Controls</td><td>Refresh</td><td>Updates the list of displayed Organizations and Departments and their details.</td></tr>
<tr><td rowspan="3">Delegation Control Buttons
Note: The Delegation control buttons are visible only on selecting a domain</td><td>Details</td><td>Enables the administrator to view the requisition details of the domain.</td></tr>
<tr><td>Approve</td><td>Enables Master administrator to approve the creation and delegation of the domain by RAO and DRAO administrators.
<b>Note</b>: This control button is visible only for Domains with 'Requested' status and only to RAO administrator.</td></tr>
<tr><td>Reject</td><td>Enables Master administrator to decline the creation and delegation of the domain by RAO and DRAO administrators.
<b>Note</b>: This control button is visible only for Domains with 'Requested' status and only to RAO administrator.</td></tr>
</table>

6.4.2.4.2 Approval of Creation and Delegation of Domains

Domains that are created and delegated by:

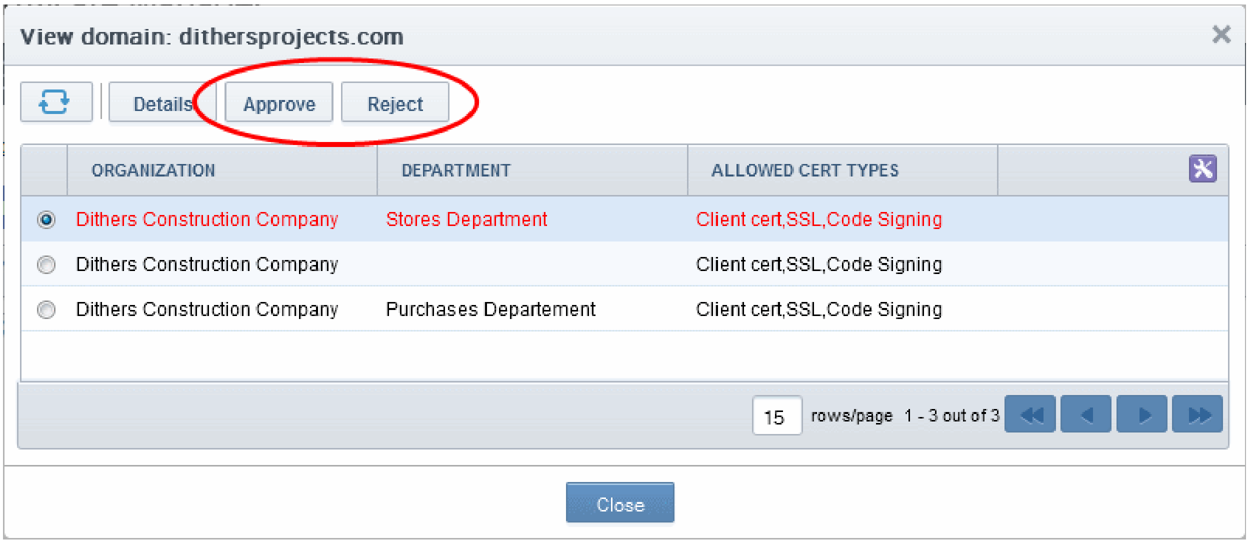
- RAO Administrators are to validated by Master Administrator(s) to become active;
- DRAO Administrators are to be first validated and approved by the RAO Administrator of the Organization to which the Department delegated with the domain and then by Master Administrator(s) to become active.

Domains which are awaiting approval are displayed in red color in the Domains area of the CM interface.

The RAO Administrator can check the validity of the Domain and approve/reject the request for the Domain.

To approve or reject a domain delegation

- 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.

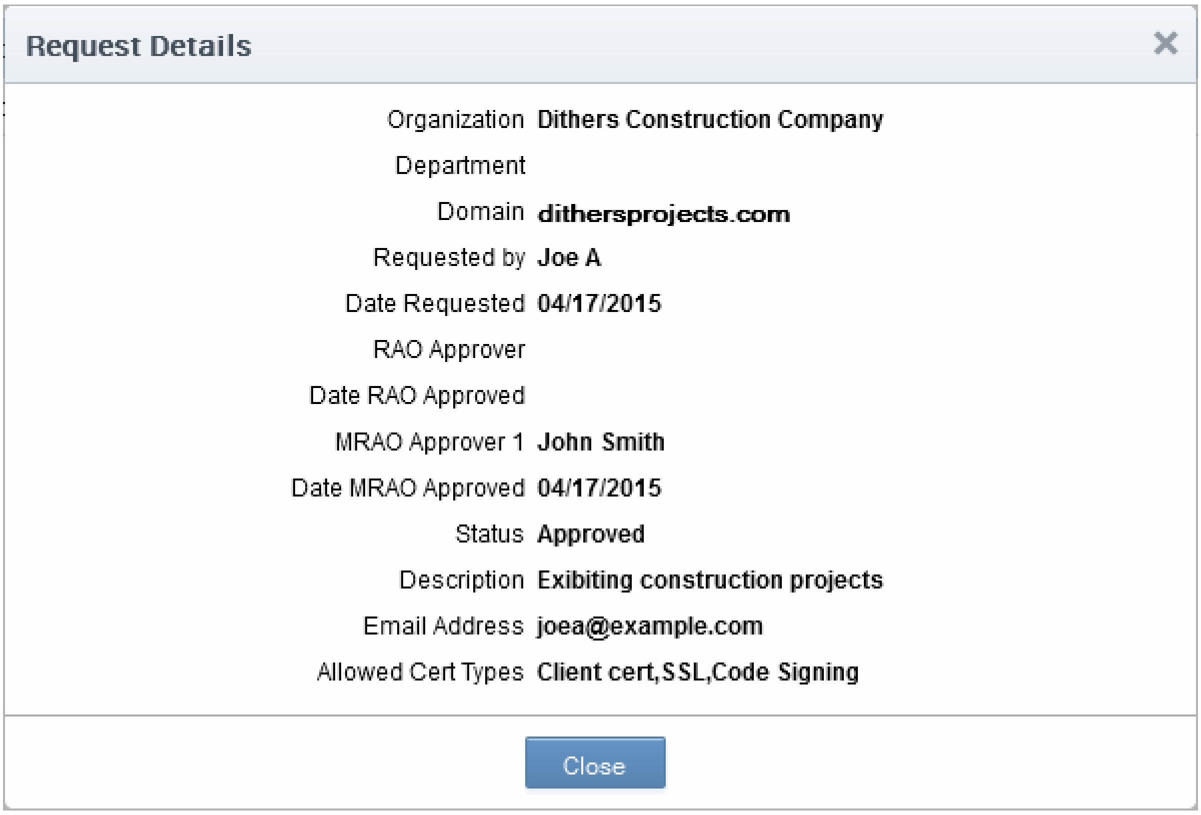


ORGANIZATION	DEPARTMENT	ALLOWED CERT TYPES
● Dithers Construction Company	Stores Department	Client cert,SSL,Code Signing
○ Dithers Construction Company		Client cert,SSL,Code Signing
○ Dithers Construction Company	Purchases Departement	Client cert,SSL,Code Signing

- 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 CSM interface.
- Once it is validated and approved by the RAO Administrator, it becomes visible to the Master Administrators for validation/approval.
- If a domain is created by an RAO Administrator, it will be displayed in red to the Master Administrators indicating that it is awaiting validation/approval.
- Once a requested domain is validated and approved by the Master Administrator, 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.

6.4.2.4.3 Viewing Requisition Details of a Domain

The administrator can view the request details of the domain delegation by selecting an organization or a department and clicking the 'Details' button from the 'View Domain' interface.



Request Details

Organization	Dithers Construction Company
Department	
Domain	dithersprojects.com
Requested by	Joe A
Date Requested	04/17/2015
RAO Approver	
Date RAO Approved	
MRAO Approver 1	John Smith
Date MRAO Approved	04/17/2015
Status	Approved
Description	Exibiting construction projects
Email Address	joea@example.com
Allowed Cert Types	Client cert,SSL,Code Signing

6.4.2.4.4 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 of the domain.
RAO Approver	The RAO administrator who approved the domain delegation
Date RAO Approved	The date on which the request was approved by the RAO administrator.
MRAO Approver	The Master administrator who approved the domain delegation
Date MRAO Approved	The date on which the request was approved by the master administrator.
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.
Email Address	Email address of the administrator who requested for the delegation of the domain.

Allowed Cert Types	Indicates the Certificate types which could be requested/issued for the domain.

6.5 Encryption and Key Escrow

6.5.1 Introduction and basic concepts

Incommon 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.

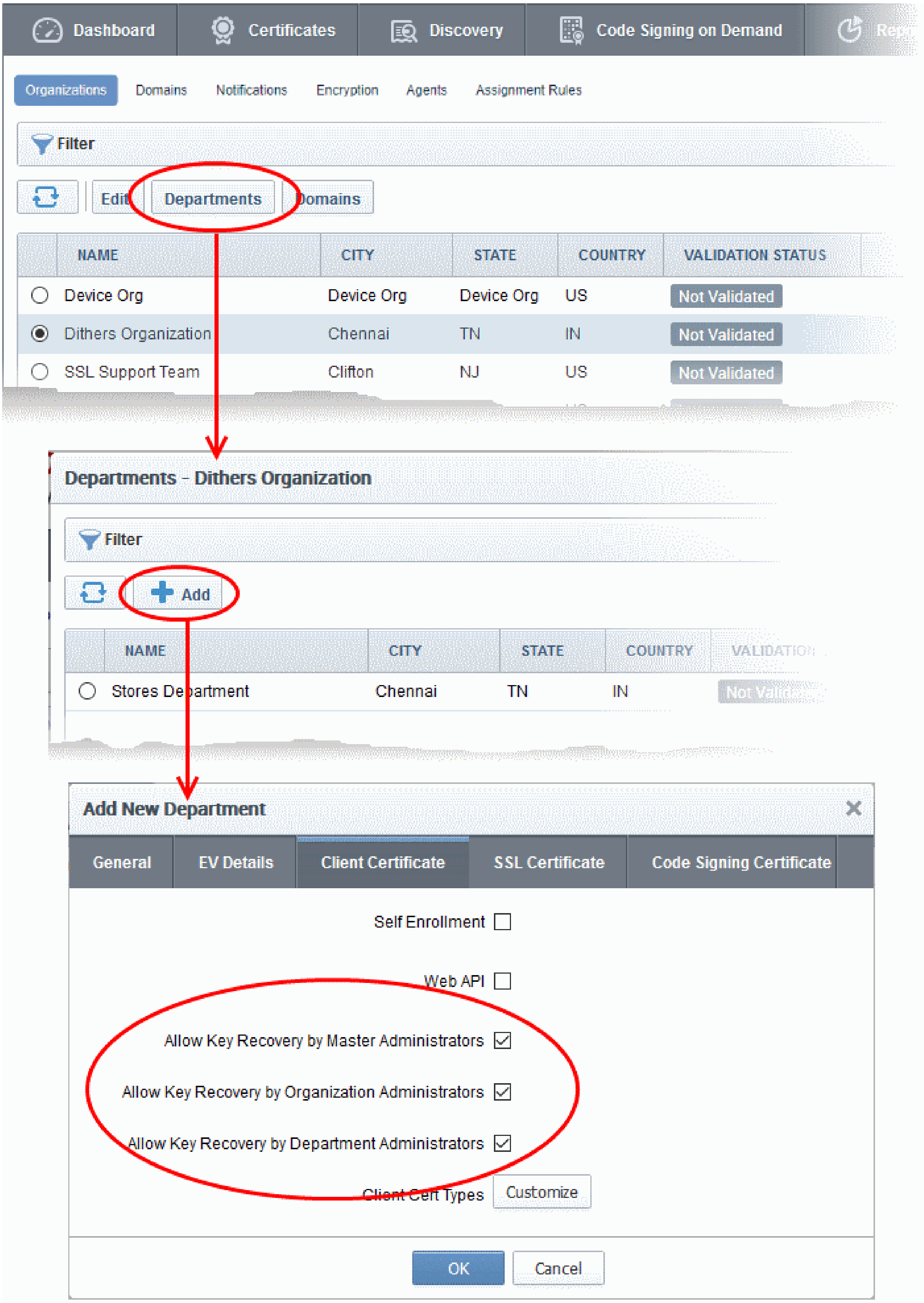
- It is possible to specify that keys in escrow be independently retrieved by three types of administrator - RAO S/MIME, DRAO S/MIME and the Master Administrator (at Incommon CA).
- Therefore, it is possible for Incommon CM to store up to 2 encrypted versions of the private keys of client certificates of an organization and up to 3 versions for a department. Each version will be separately encrypted by three different 'master' public keys - the Master Administrator master key, the organization master key and the departmental master key.
- These master public keys are stored by Certificate Manager. The corresponding master private keys are not stored in Certificate Manager (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 S/MIME 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 S/MIME Admins of a particular department - the Department Master Key.
- If 'Allow key recovery by 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.

6.5.2 Set 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 RAO S/MIME 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:



	NAME	CITY	STATE	COUNTRY	VALIDATION STATUS
○	Device Org	Device Org	Device Org	US	Not Validated
●	Dithers Organization	Chennai	TN	IN	Not Validated
○	SSL Support Team	Clifton	NJ	US	Not Validated

Departments - Dithers Organization

	NAME	CITY	STATE	COUNTRY	VALIDATION
○	Stores Department	Chennai	TN	IN	Not Valida

Add New Department

Self Enrollment □

Web API □

Allow Key Recovery by Master Administrators ☑

Allow Key Recovery by Organization Administrators ☑

Allow Key Recovery by Department Administrators ☑

Client Cert Types Customize

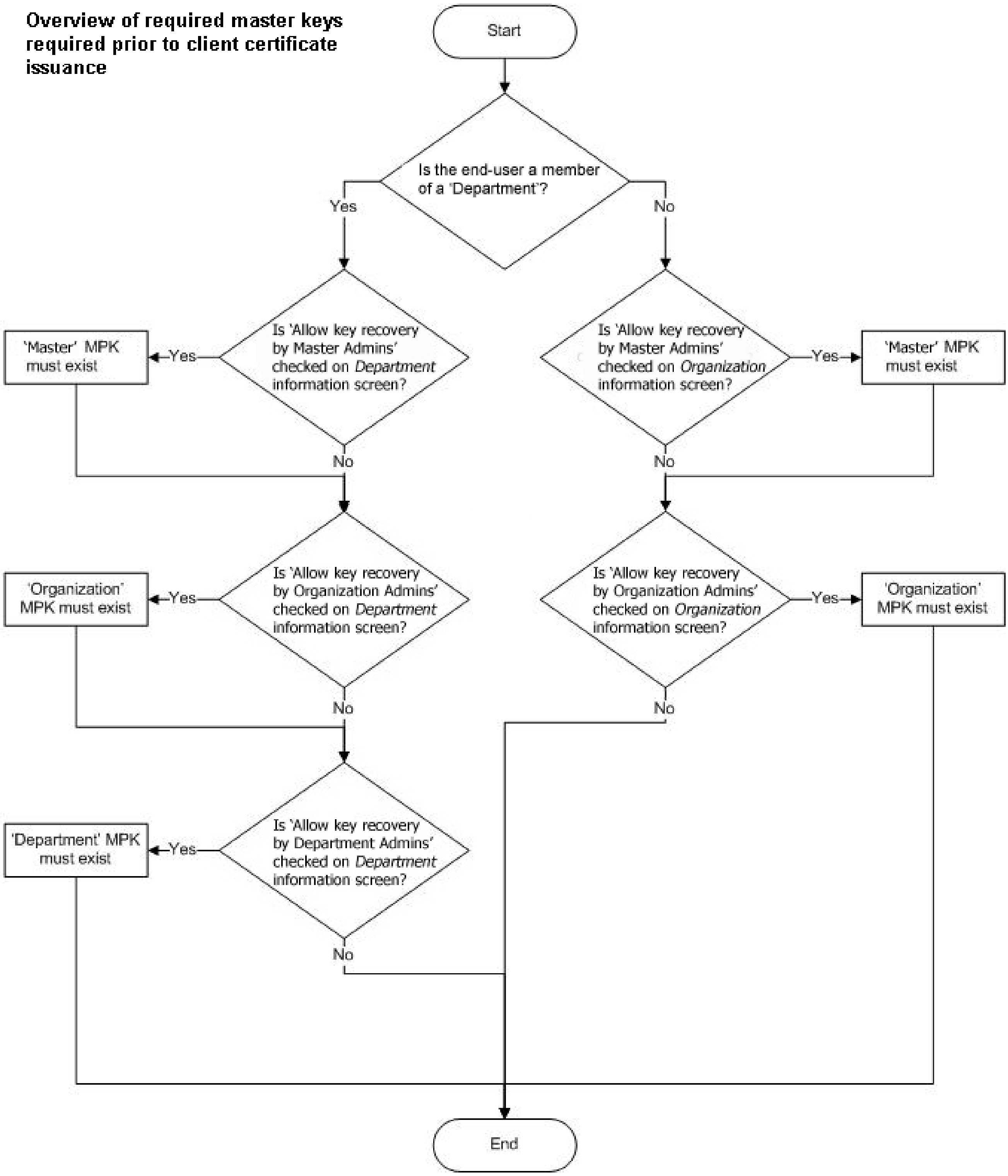
Allow Key Recovery by Master Administrators	Checkbox Default state - checked if pre-enabled by *Master Administrator*	- If selected, the Master Administrator will have the ability to recover the private keys of client certificates issued by this Department. - At the point of creation, each client certificate will be encrypted with the Master Administrator's 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 Master Administrator has initialized their master key pair in the Encryption tab
Allow Key Recovery by Organization Administrators	*Check-box* *Default state - checked if pre-enabled by Master Administrator*	- 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 S/MIME admin has initialized their master key pair in the Encryption tab.
Allow Key Recovery by Department Administrators	*Check-box* *Default state - checked if pre-enabled by Master Administrator*	- If selected, the DRAO S/MIME 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.

- Fill out the 'General Information' tab (and optionally the 'SSL' / 'Code Signing Certificate' tabs if those cert types are required). See Creating Departments for full details concerning the creation of a new Department.
- Once you are satisfied with all settings, click 'OK' to add the Department

6.5.3 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


Start
Is the end-user a member of a 'Department'?
Yes
No
Is 'Allow key recovery by Master Admins' checked on *Department* information screen?
Yes
'Master' MPK must exist
No
Is 'Allow key recovery by Master Admins' checked on *Organization* information screen?
Yes
'Master' MPK must exist
No
Is 'Allow key recovery by Organization Admins' checked on *Department* information screen?
Yes
'Organization' MPK must exist
No
Is 'Allow key recovery by Organization Admins' checked on *Organization* information screen?
Yes
'Organization' MPK must exist
No
Is 'Allow key recovery by Department Admins' checked on *Department* information screen?
Yes
'Department' MPK must exist
No
End

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.

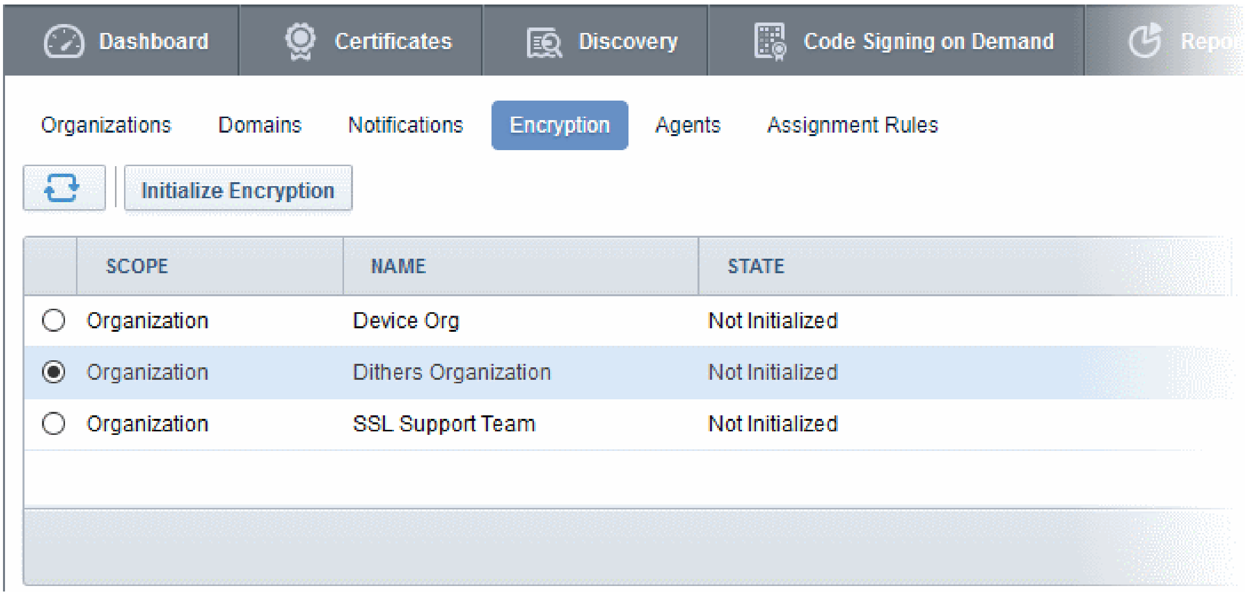
- RAO S/MIME Administrators can find whether recovery is checked for a department by clicking 'Settings' > 'Organizations', then clicking the 'Departments' button of the organization in question. Next, select the department in question and click 'Edit' button, then select the 'Client Cert' tab.
- '*MPK 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 (Organization + Department) then this means that 2 master private keys will need to be initialized. To check initialization status, the currently logged in administrator should click the 'Encryption' tab

6.5.4 Encryption

This area allows administrators to encrypt the private keys of users' client certificates. If key recovery was specified during the creation of a 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 RAO/DRAO S/MIME Administrators if key recovery has been enabled for their specific organization/department.

To use this feature the administrator needs to initialize private key encryption by clicking 'Initialize Encryption' button.



	SCOPE	NAME	STATE
○	Organization	Device Org	Not Initialized
●	Organization	Dithers Organization	Not Initialized
○	Organization	SSL Support Team	Not Initialized

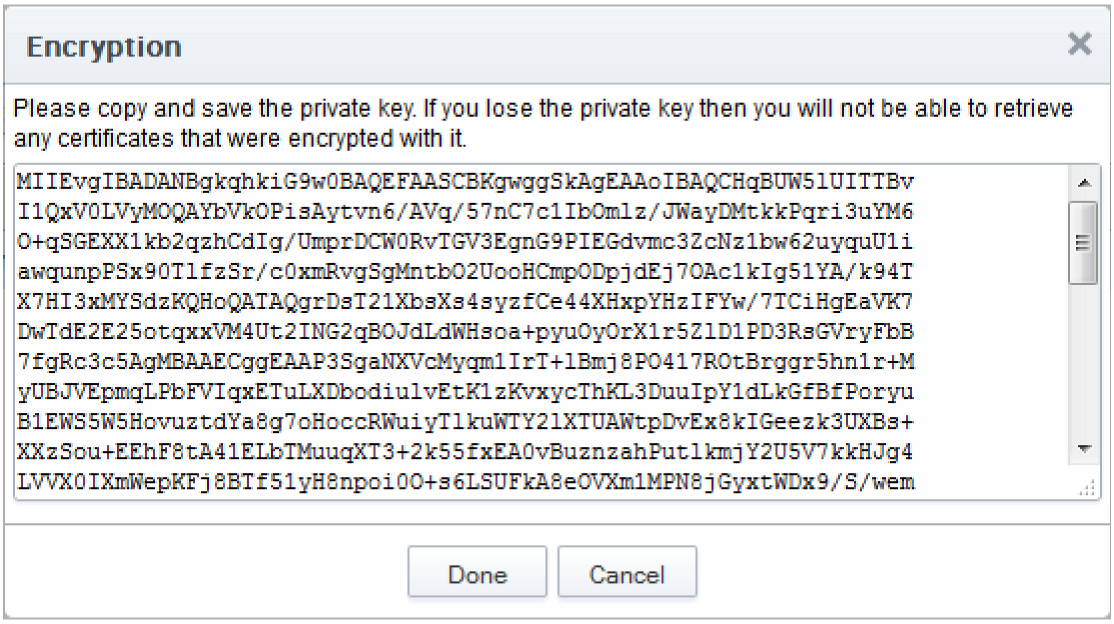
6.5.4.1 Summary of Fields and Controls

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	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.
	Re-encrypt	Starts the re-encryption process of the private keys of the certificates of the end-users of belonging to an organization/department. This

private key encryption		control is available only if the private keys are already encrypted.

6.5.5 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.



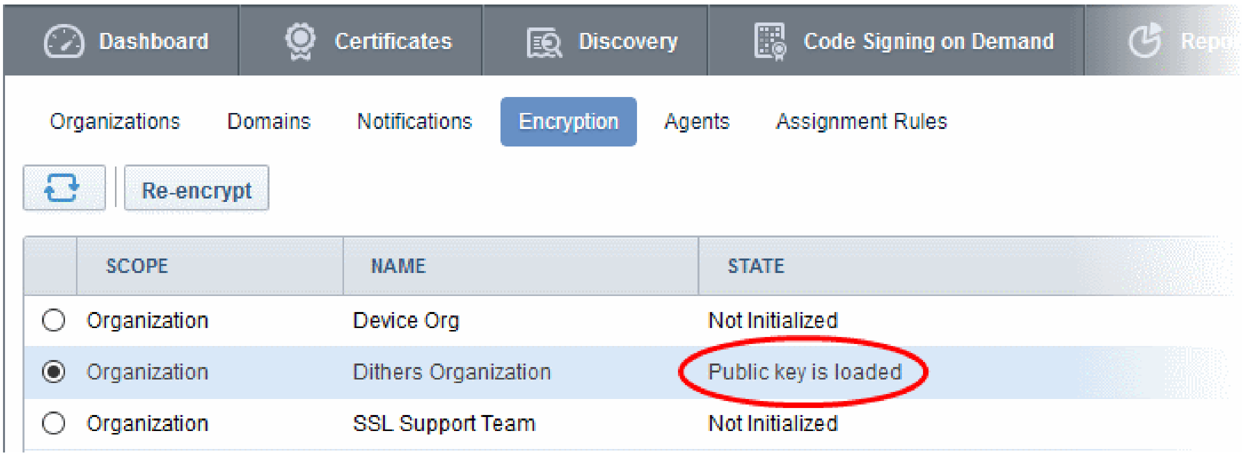
Encryption

Please copy and save the private key. If you lose the private key then you will not be able to retrieve any certificates that were encrypted with it.

```
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCHqBUW5lUITTBv
I1QxV0LVyMOQAYbVkOPisAytvn6/AVq/57nC7c1IbOmlz/JWayDMtkkPqri3uYM6
O+qSGEXX1kb2qzhCdIg/UmprDCW0RvTGV3EgnG9PIEGdvmc3ZcNz1bw62uyquU1i
awqunpPSx90TlfzSr/c0xmRvgSgMntbO2UooHCmpODpjdEj7OAc1kIg51YA/k94T
X7HI3xMYSdzKQHoQATAQgrDsT21XbsXs4syzfCe44XHxpYHzIFYw/7TCiHgEaVK7
DwTdE2E25otqxxVM4Ut2ING2qBOJdLdWHsoa+pyuOyOrX1r5Z1D1PD3RsGVryFbB
7fgRc3c5AgMBAAECggEAAP3SgaNXVcMyqm1IrT+1Bmj8PO417ROtBrggr5hn1r+M
yUBJVEpmqLPbFVIqxETuLXDbodiulvEtK1zKvxycThKL3DuuIpY1dLkGfBfPoryu
B1EWS5W5HovuztdYa8g7oHoccRWuiyTlkuWTY21XTUAWtpDvEx8kIGeezk3UXBs+
XXzSou+EEhF8tA41ELbTMuuqXT3+2k55fxEA0vBuznzahPutlkmjY2U5V7kkHJg4
LVVX0IXmWepKFj8BTf51yH8npoi0O+s6LSUFkA8eOVXm1MPN8jGyxtWDx9/S/wem
```

Note: This 'master' *private* key is not stored within InCommon 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'.



	SCOPE	NAME	STATE
○	Organization	Device Org	Not Initialized
●	Organization	Dithers Organization	Public key is loaded
○	Organization	SSL Support Team	Not Initialized

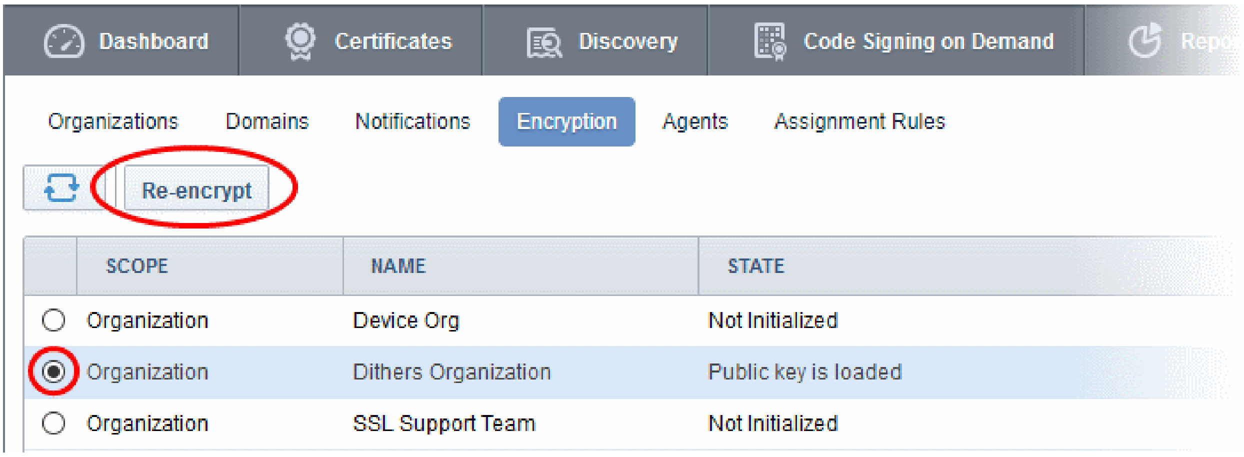
All the private keys of user client certificates are now encrypted using the master public key of the administrator that began this process. Decryption will require the private key that was saved earlier.

6.5.6 Re-encryption

The re-encryption area allows RAO S/MIME and DRAO S/MIME administrators to change their master key pair 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.

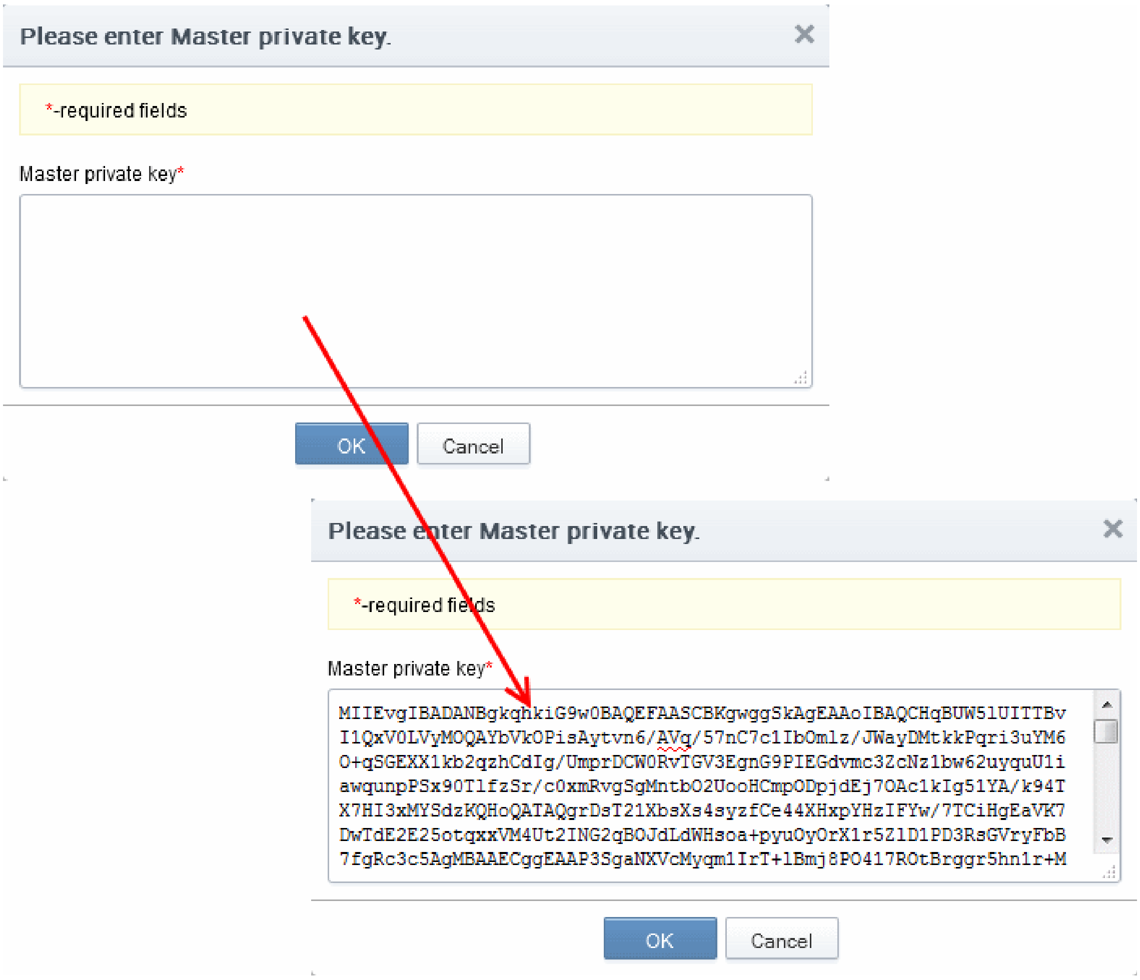
To start the Re-encryption process

- Click the 'Reencrypt' button to launch the process:



	SCOPE	NAME	STATE
○	Organization	Device Org	Not Initialized
●	Organization	Dithers Organization	Public key is loaded
○	Organization	SSL Support Team	Not Initialized

The Administrator will be prompted to paste the existing master private key to start the process:


Please enter Master private key.

*-required fields

Master private key*

Please enter Master private key.

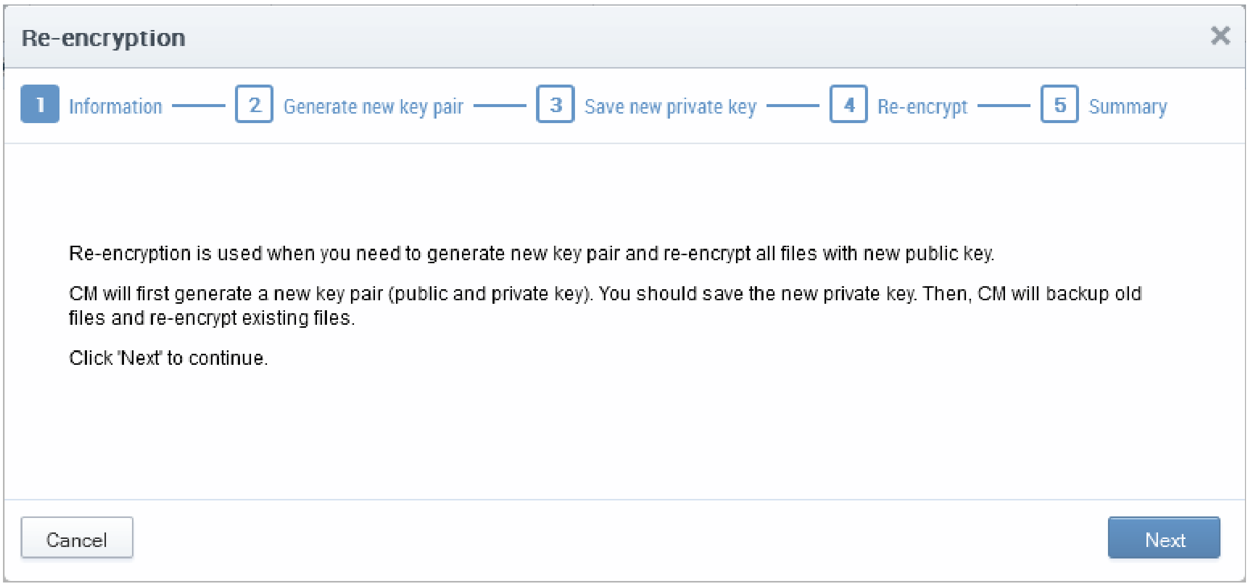
*-required fields

Master private key*

MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCHqBUW5lUITTBv
I1QxV0LVyMOQAYbVkOPisAytvn6/AVq/57nC7c1IbOmlz/JWayDMtkkPqri3uYM6
O+qSGEXX1kb2qzhCdIg/UmprDCW0RvTGV3EgnG9PIEGdvmc3ZcNz1bw62uyquU1i
awqunpPSx90TlfzSr/c0xmRvgSgMntbO2UooHCmpODpjdEj7OAc1kIg51YA/k94T
X7HI3xMYSdzKQHoQATAQgrDsT21XbsXs4syzfCe44XHxpYHzIFYw/7TCiHgEaVK7
DwTdE2E25otqxxVM4Ut2ING2qBOJdLdWHsoa+pyuOyOrX1r5Z1D1PD3RsGVryFbB
7fgRc3c5AgMBAAECggEAAP3SgaNXVcMyqm1IrT+1Bmj8PO417ROtBrggr5hn1r+M

- Paste the Master key and click 'OK'.

The re-encryption dialog will appear. This will provide a brief summary of the forthcoming process.



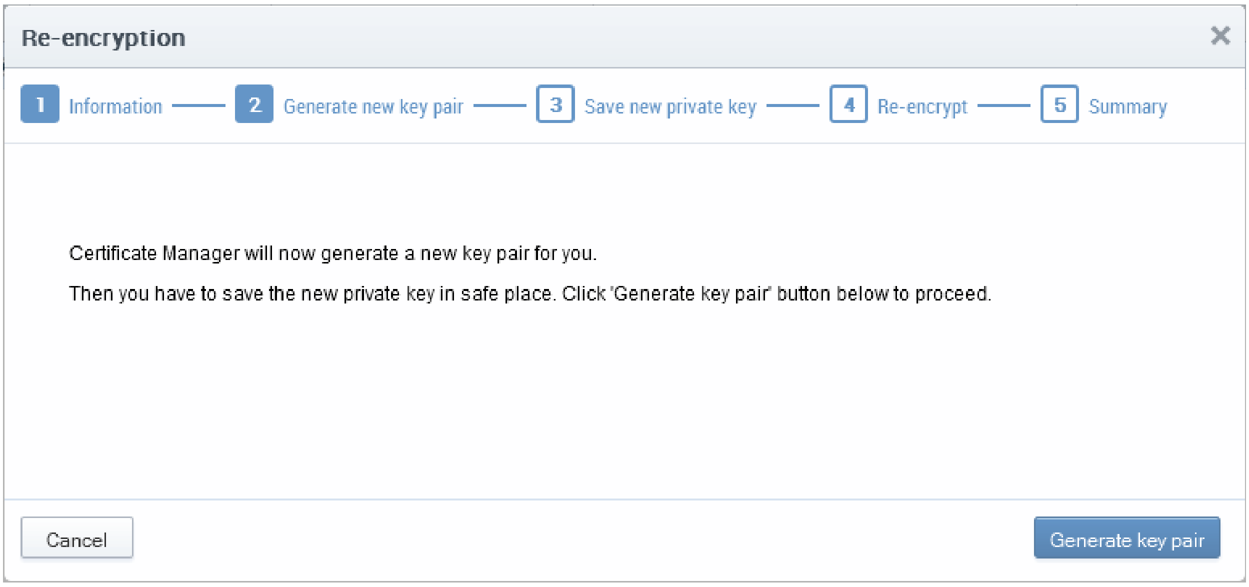
Re-encryption
1 Information — 2 Generate new key pair — 3 Save new private key — 4 Re-encrypt — 5 Summary

Re-encryption is used when you need to generate new key pair and re-encrypt all files with new public key.

CM will first generate a new key pair (public and private key). You should save the new private key. Then, CM will backup old files and re-encrypt existing files.

Click 'Next' to continue.

- Click 'Next' to continue:

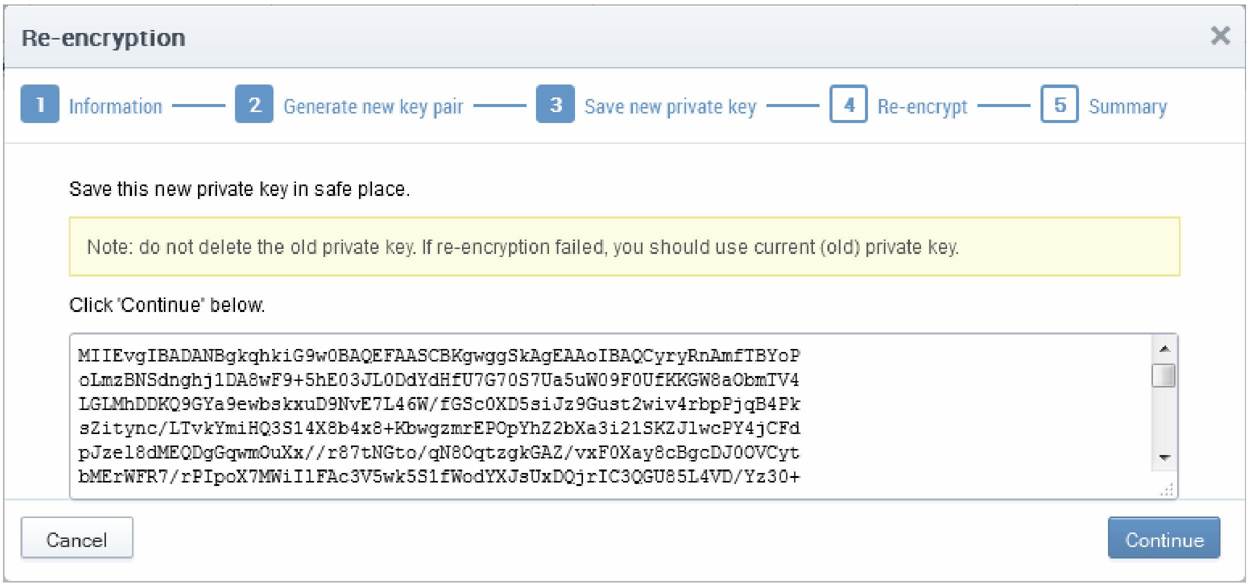


Re-encryption
1 Information — 2 Generate new key pair — 3 Save new private key — 4 Re-encrypt — 5 Summary

Certificate Manager will now generate a new key pair for you.

Then you have to save the new private key in safe place. Click 'Generate key pair' button below to proceed.

- Click the 'Generate Key Pair' to generate the new keys:



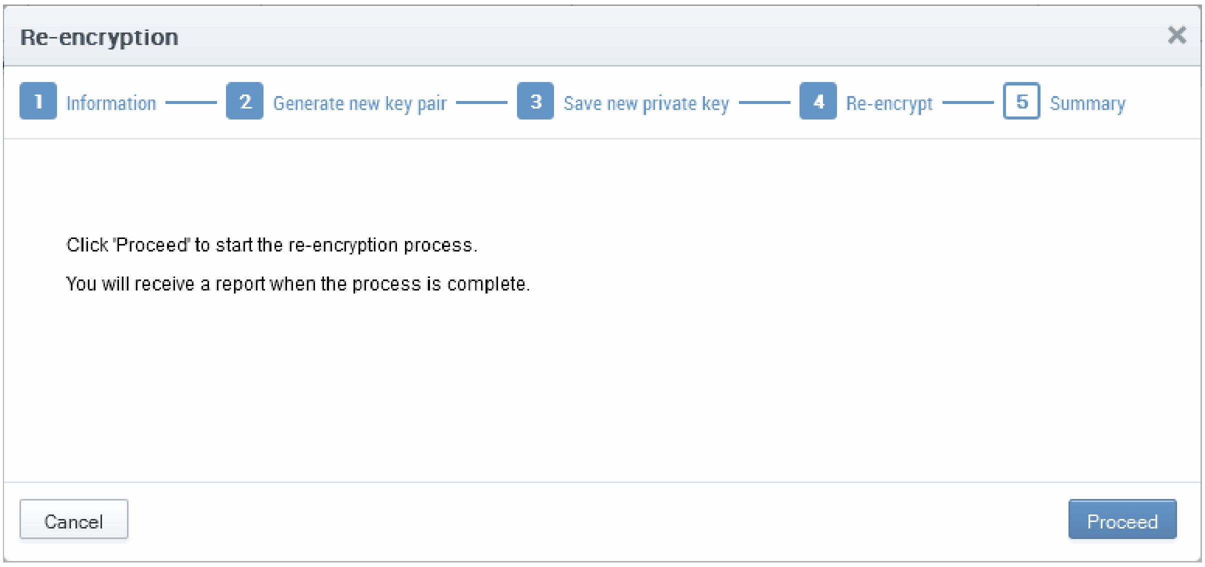
Save this new private key in safe place.

Note: do not delete the old private key. If re-encryption failed, you should use current (old) private key.

Click 'Continue' below.

```
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCyryRnAmfTBYoP
oLmzBNSdnghj1DA8wF9+5hE03JL0DdYdHfU7G70S7Ua5uW09F0UfKKGW8aObmTV4
LGLMhDDKQ9GYa9ewbskxuD9NvE7L46W/fGSc0XD5siJz9Gust2wiv4rbpPjqB4Pk
sZitync/LTvkYmiHQ3S14X8b4x8+KbwgzmrEPOpYhZ2bXa3i21SKZJlwcPY4jCFd
pJzel8dMEQDgGqwmOuXx//r87tNGto/qN8OqtzgkGAZ/vxF0Xay8cBgcDJ0OVCyt
bMErWFR7/rPIpoX7MWiIlFAc3V5wk5S1fWodYXJsUxDQjrIC3QGU85L4VD/Yz30+
```

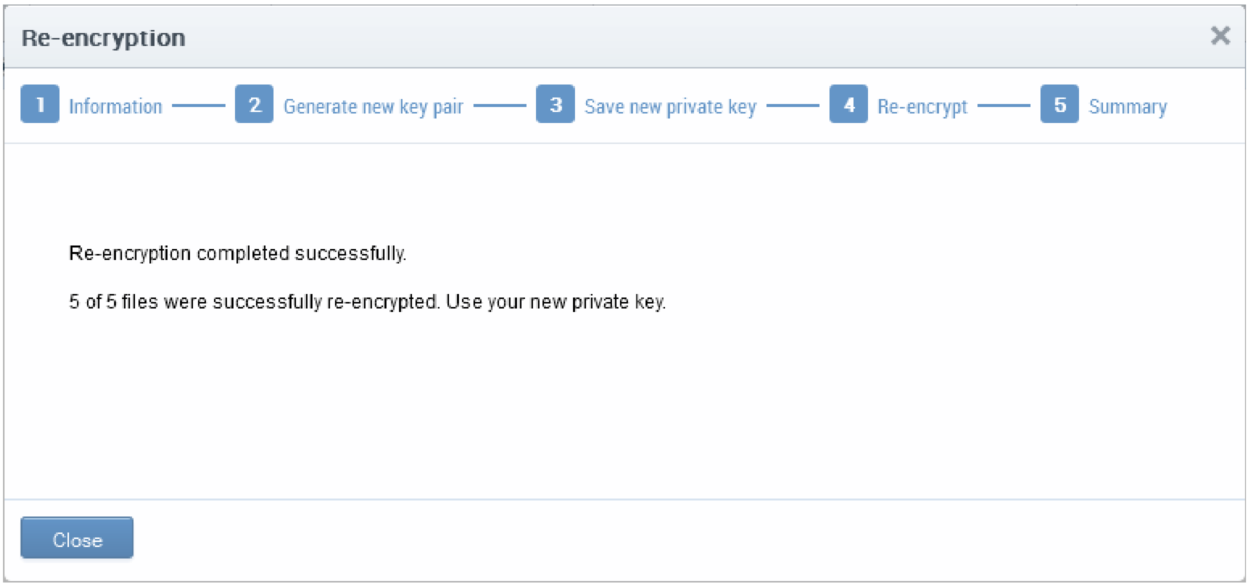
- Copy and paste the private key into a .txt file then save it in a secure, password protected location. Click continue. The re-encryption of the private keys will be started.



Click 'Proceed' to start the re-encryption process.

You will receive a report when the process is complete.

- Click 'Proceed' to begin re-encrypting the private keys of client certificates. Upon successful re-encryption, a summary screen will be displayed.



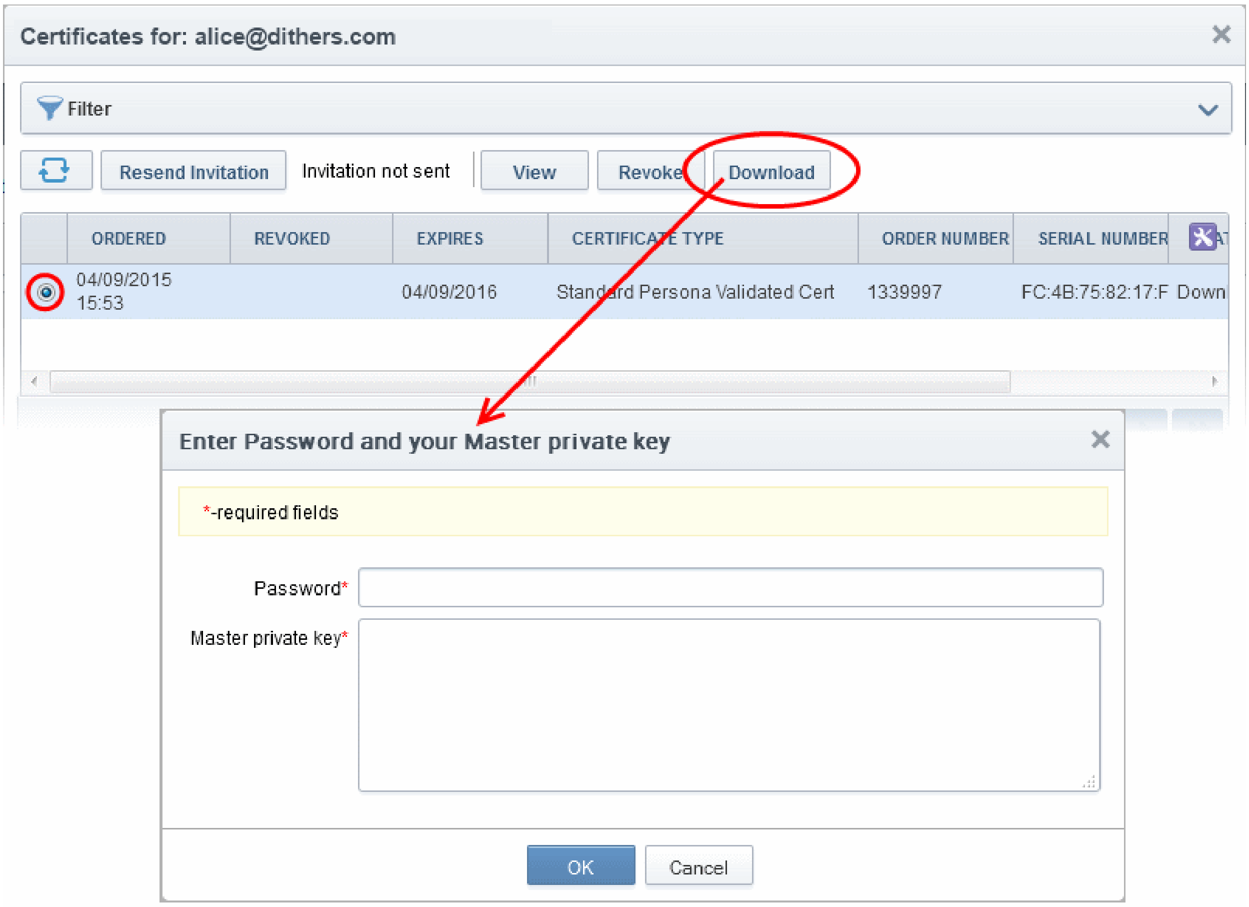
Re-encryption completed successfully.

5 of 5 files were successfully re-encrypted. Use your new private key.

6.5.7 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 an end-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. **Note** - administrators should have their master private key ready - it will be required to complete this process.

- 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'.



Certificates for: alice@dithers.com

Invitation not sent

ORDERED	REVOKED	EXPIRES	CERTIFICATE TYPE	ORDER NUMBER	SERIAL NUMBER	ST
04/09/2015 15:53		04/09/2016	Standard Persona Validated Cert	1339997	FC:4B:75:82:17:F	Down

Enter Password and your Master private key

*-required fields

Password*

Master private key*

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. Admin can set a password (**PIN)** 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.

6.6 Notifications

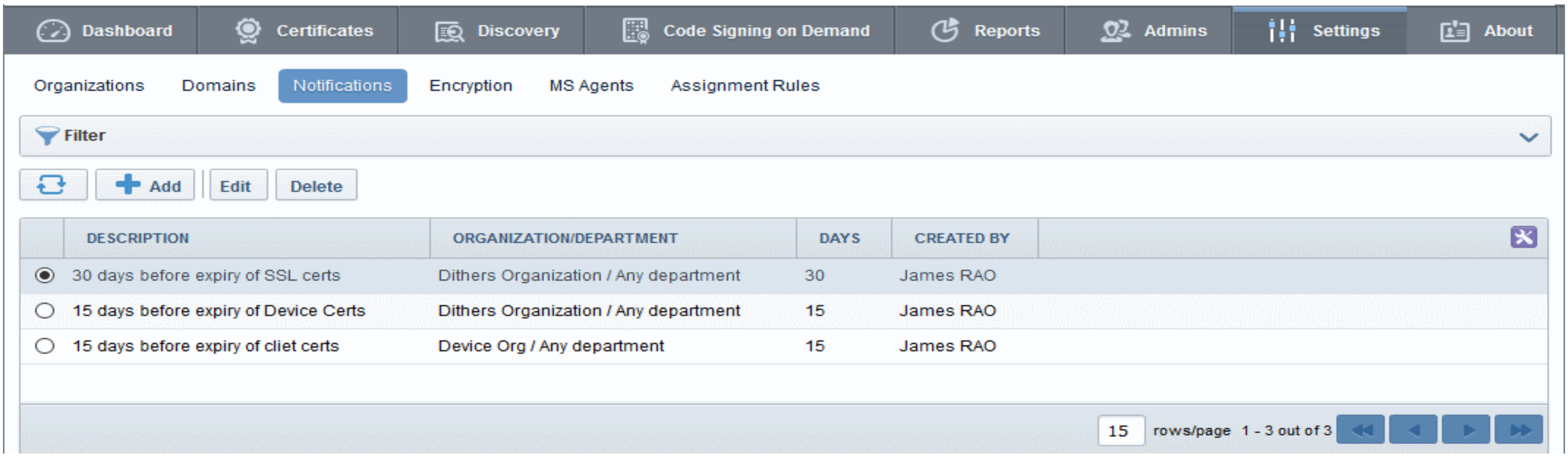
- Click 'Settings' > 'Notifications' to open the notifications area.

The 'Notifications' interface enables RAO and DRAO Administrators to set up and manage to set up and manage email notifications to various personnel - including notifications triggered by events like requisition, issuance, download, installation, expiry of certificates, requisition, approval and validation of domains and their delegations, creation of administrators, certificate discovery scan reports and more.

Tip: InCommon CM also enables the Administrators to customize the email templates of the notifications as required. Refer to Viewing and Editing Email Templates for more details.

Administrative Roles:

- RAO - Can only view the notification set by them for the users belonging the organizations (and any subordinate departments) that have been delegated to them. They can create and manage 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 view the notifications setup for the users belonging to department(s) delegated to them. They can create and manage notifications only for the notification types on which they have authority AND only for the departments that have been delegated to them.



Dashboard | Certificates | Discovery | Code Signing on Demand | Reports | Admins | Settings | About

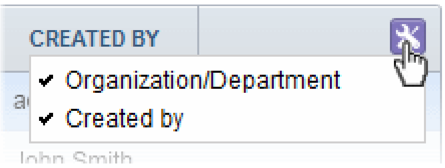
Organizations | Domains | Notifications | Encryption | MS Agents | Assignment Rules

Filter

Add | Edit | Delete

	DESCRIPTION	ORGANIZATION/DEPARTMENT	DAYS	CREATED BY
●	30 days before expiry of SSL certs	Dithers Organization / Any department	30	James RAO
○	15 days before expiry of Device Certs	Dithers Organization / Any department	15	James RAO
○	15 days before expiry of cliet certs	Device Org / Any department	15	James RAO

15 rows/page 1 - 3 out of 3

<table>
<tr><th colspan="3">Notifications - Summary of Fields and Controls</th></tr>
<tr><th>Column Display</th><th colspan="2">Description</th></tr>
<tr><td>Description</td><td colspan="2">Provides a short description for the notification, as entered by the administrator during creation.</td></tr>
<tr><td>Organization/Department</td><td colspan="2">The organization(s)/department(s) for which the notification was created. The notification mails will be sent to the only to Administrators/Users of these organization(s)/department(s).</td></tr>
<tr><td>Days</td><td colspan="2">Number of days in advance of the event, the notification will be sent.</td></tr>
<tr><td>Created by</td><td colspan="2">Displays the name of the administrator who has created the notification.</td></tr>
<tr><td colspan="3"><b>Note</b>: An administrator can enable or disable the columns from the drop-down button beside the last item in the table header:

CREATED BY
✔ Organization/Department
✔ Created by
John Smith</td></tr>
<tr><td rowspan="2">Control Buttons</td><td>Add</td><td>Enables the ddministrator to add a new notification.</td></tr>
<tr><td>Refresh</td><td>Updates the list of displayed notifications.</td></tr>
<tr><td rowspan="2">Notification Control Buttons
<b>Note</b>: The Notification control buttons are visible only on selecting a Notification</td><td>Edit</td><td>Enables the administrator to edit the notification. See the note below this table.</td></tr>
<tr><td>Delete</td><td>Enables the administrator to delete the notification. See the note below this table.</td></tr>
</table>

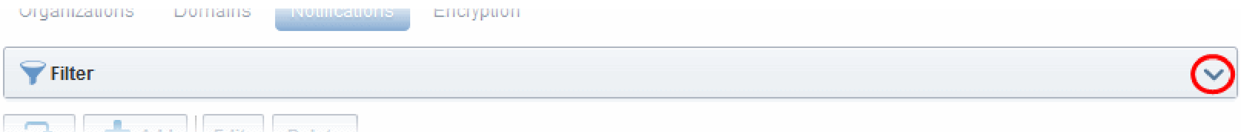
Important Note: An administrator can either edit or delete an existing notification when *all* the following conditions are true:

- 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 creator of the notification is of the same or lower administrative level than that of the administrator.

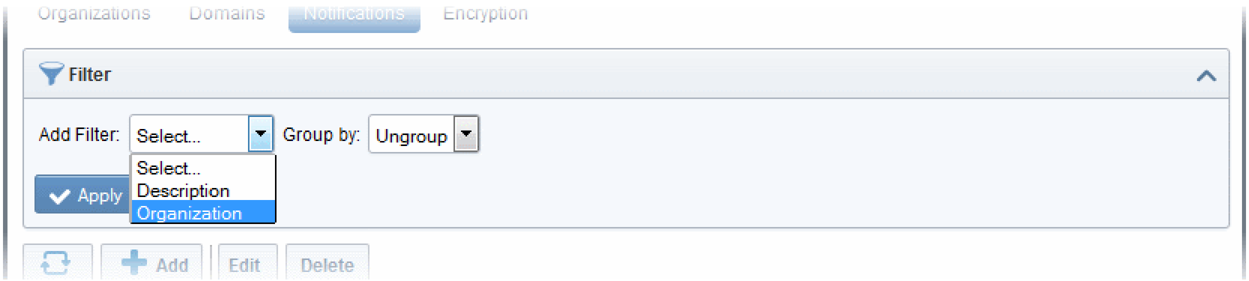
Sorting and Filtering Options

- Clicking on a column headers 'Description' and 'Days' sorts the items in the alphabetical order of the entries in the respective column.

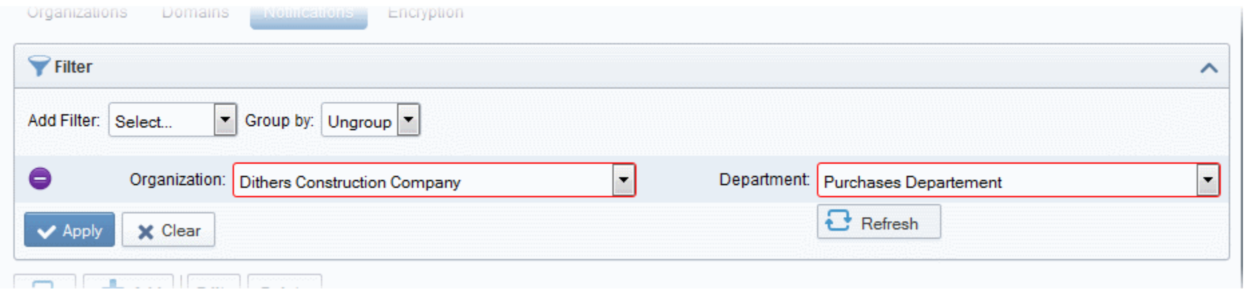
Administrators can search for a particular notification from the list by using filters under the sub-tab:



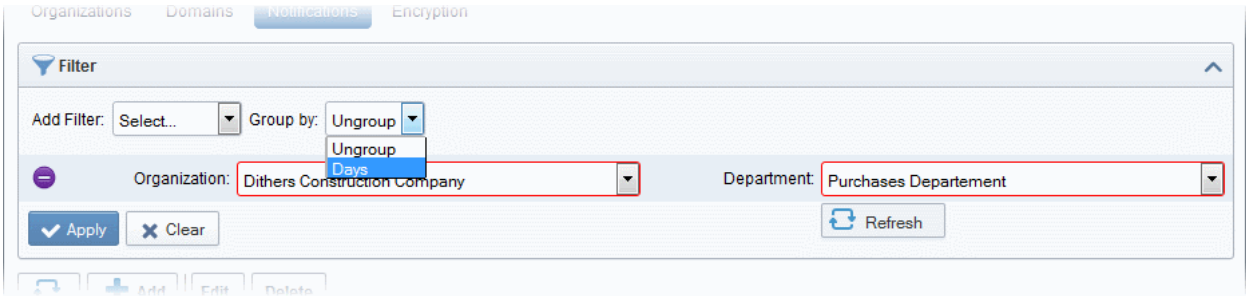
- To apply filters, click anywhere on the 'Filters' stripe.
- The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.
- For example, if you want to filter the notification type set for an organization/department, select 'Organization' from the 'Add Filter' drop-down:



- Select the organization to which the department belongs from the 'Organization' drop-down.

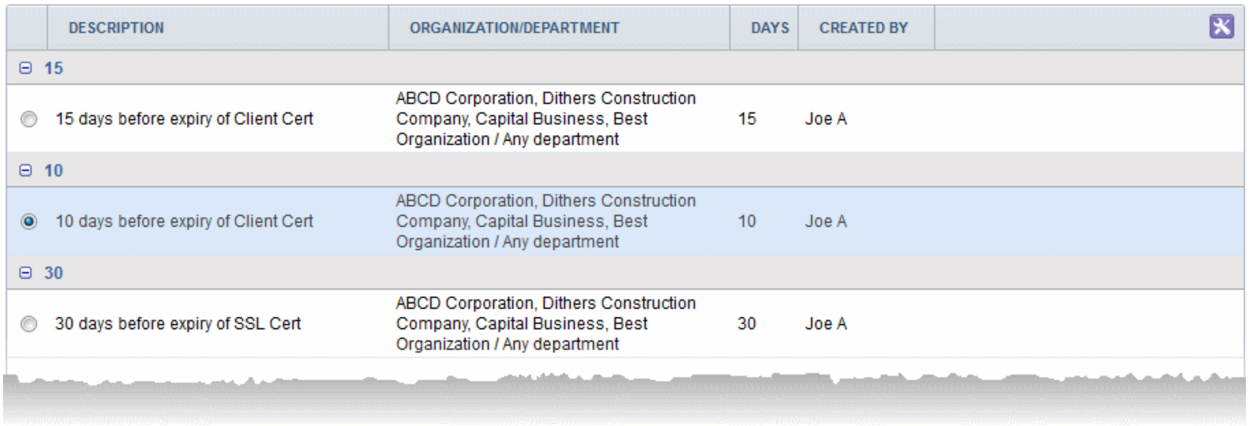

Add Filter: Select...
Group by: Ungroup
Organization: Dithers Construction Company
Department: Purchases Departement

- Select the department from the 'Department' drop-down.
- To group the results based on the days parameter, select 'Days' from the 'Group by' drop-down.


Add Filter: Select...
Group by: Ungroup
Organization: Dithers Construction Company
Department: Purchases Departement

- Click the 'Apply' button.

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



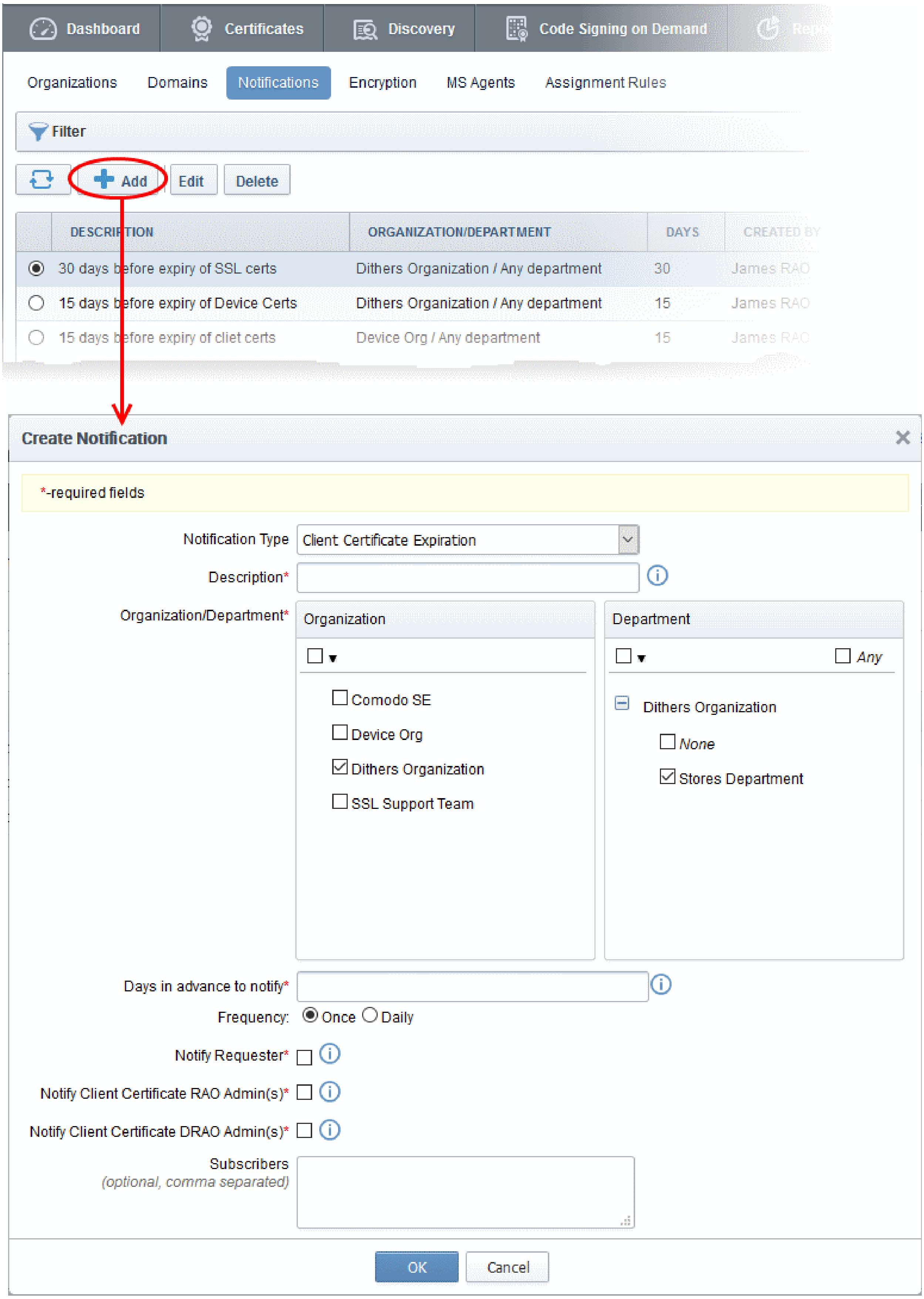
	DESCRIPTION	ORGANIZATION/DEPARTMENT	DAYS	CREATED BY
⊟ 15				
○	15 days before expiry of Client Cert	ABCD Corporation, Dithers Construction Company, Capital Business, Best Organization / Any department	15	Joe A
⊟ 10				
●	10 days before expiry of Client Cert	ABCD Corporation, Dithers Construction Company, Capital Business, Best Organization / Any department	10	Joe A
⊟ 30				
○	30 days before expiry of SSL Cert	ABCD Corporation, Dithers Construction Company, Capital Business, Best Organization / Any department	30	Joe A

- 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.

6.6.1 Adding a Notification

The administrator can add a new notification by clicking the 'Add' button under the 'Notifications' sub-tab and filling out the form that appears.



	DESCRIPTION	ORGANIZATION/DEPARTMENT	DAYS	CREATED BY
●	30 days before expiry of SSL certs	Dithers Organization / Any department	30	James RAO
○	15 days before expiry of Device Certs	Dithers Organization / Any department	15	James RAO
○	15 days before expiry of cliet certs	Device Org / Any department	15	James RAO

Create Notification

*-required fields

Notification Type: Client Certificate Expiration

Description*:

Organization/Department*:

Organization:
- □ Comodo SE
- □ Device Org
- ☑ Dithers Organization
- □ SSL Support Team

Department: □ *Any*
- Dithers Organization
  - □ *None*
  - ☑ Stores Department

Days in advance to notify*:

Frequency: ● Once ○ Daily

Notify Requester* □

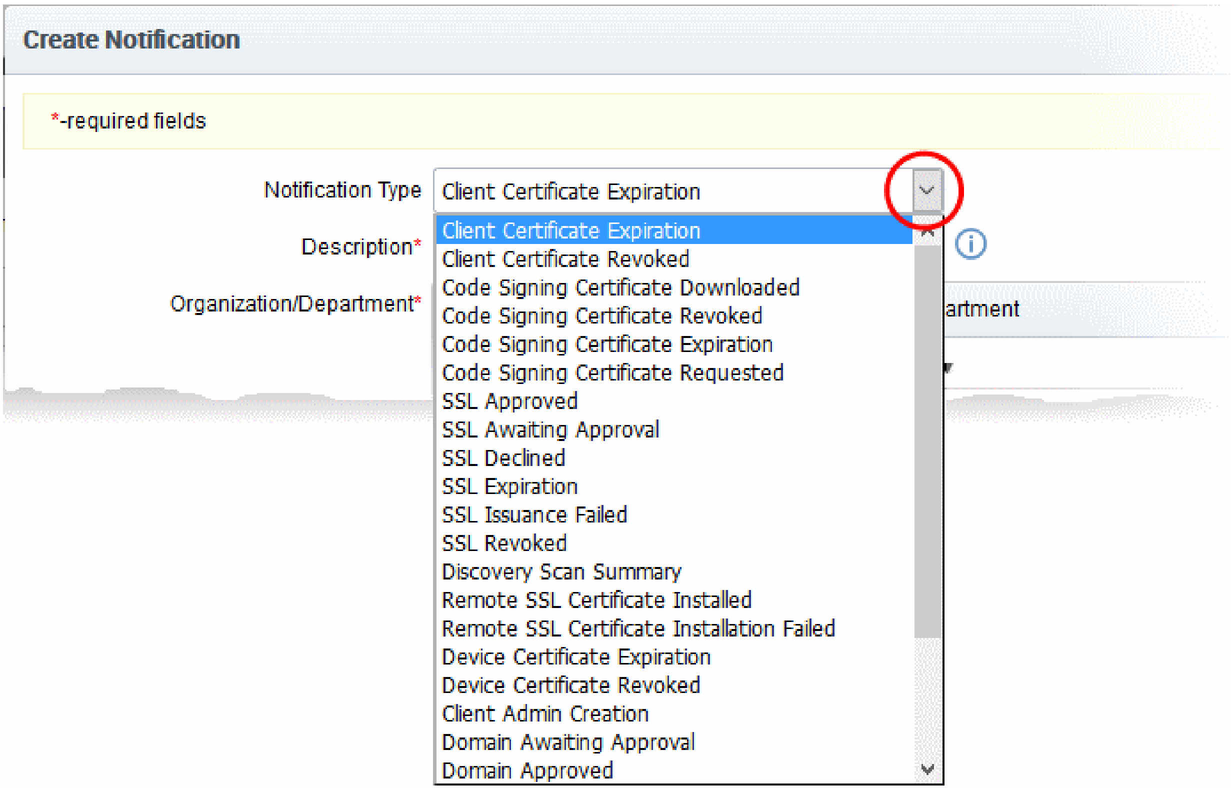
Notify Client Certificate RAO Admin(s)* □

Notify Client Certificate DRAO Admin(s)* □

Subscribers *(optional, comma separated)*

- 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 only to 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.



Create Notification

*-required fields

Notification Type: Client Certificate Expiration

Description*

Organization/Department*

Client Certificate Expiration
Client Certificate Revoked
Code Signing Certificate Downloaded
Code Signing Certificate Revoked
Code Signing Certificate Expiration
Code Signing Certificate Requested
SSL Approved
SSL Awaiting Approval
SSL Declined
SSL Expiration
SSL Issuance Failed
SSL Revoked
Discovery Scan Summary
Remote SSL Certificate Installed
Remote SSL Certificate Installation Failed
Device Certificate Expiration
Device Certificate Revoked
Client Admin Creation
Domain Awaiting Approval
Domain Approved
artment

The following table explains the notification types that are available for administrators according to their administrative roles.

Notification	Notification Type	Administrator Type
Client Certificate Expiration	Client Certificate	RAO S/MIME admins, DRAO S/MIME admins.
Client Certificate Revoked	Client Certificate	RAO S/MIME admins, DRAO S/MIME admins.
Code Signing Certificate Downloaded	Code Signing Certificate	RAO Code Signing admins, DRAO Code Signing admins.
Code Signing Certificate Revoked	Code Signing Certificate	RAO Code Signing admins, DRAO Code Signing admins.
Code Signing Certificate Expiration	Code Signing Certificate	RAO Code Signing admins, DRAO Code Signing admins.
Code Signing Certificate Requested	Code Signing Certificate	RAO Code Signing admins, DRAO Code Signing admins.

Notification	Notification Type	Administrator Type
SSL Approved	SSL Certificate	RAO SSL admin, DRAO SSL admin.
SSL Awaiting Approval	SSL Certificate	RAO SSL admin, DRAO SSL admin.
SSL Declined	SSL Certificate	RAO SSL admin, DRAO SSL admin.
SSL Expiration	SSL Certificate	RAO SSL admin, DRAO SSL admin.
SSL Issuance Failed	SSL Certificate	RAO SSL admin, DRAO SSL admin.
SSL Revoked	SSL Certificate	RAO SSL admin, DRAO SSL admin.
Discovery Scan Summary	Other	All administrators.
Remote SSL Certificate Installed	SSL Certificate	RAO SSL admin, DRAO SSL admin
Remote SSL Certificate Installation Failed	SSL Certificate	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	RAO SSL admin, DRAO SSL admin
DCV Expired	Domain Control Validation	RAO SSL admin, DRAO SSL admin
DCV Validated	Domain Control Validation	RAO SSL admin, DRAO SSL admin
DCV Needed-New Domain	Domain Control Validation	RAO SSL admin, DRAO SSL admin

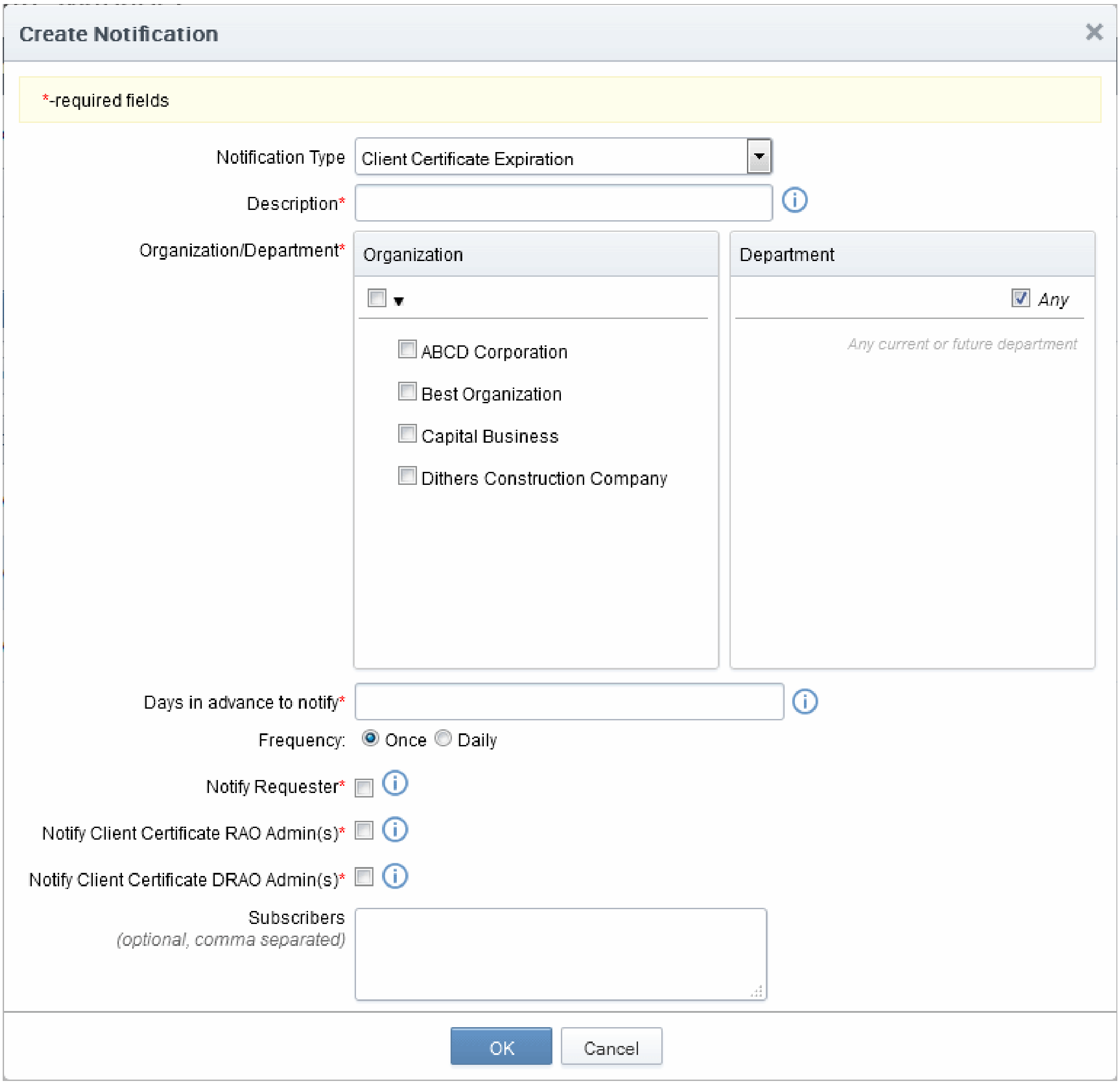
Notification	Notification Type	Administrator Type

Detailed description of each type of form is given below. The 'Create Notification' form varies pursuant to the selected 'Notification Type'.

6.6.2 Notification Types

6.6.2.1 'Client Certificate Expiration' Create Notification Form

Enables administrator to set notification about terms of expiration of client certificates.



Create Notification ✕

*-required fields

Notification Type: Client Certificate Expiration

Description*:

Organization/Department*:

Organization	Department
□ ▾	☑ Any
□ ABCD Corporation □ Best Organization □ Capital Business □ Dithers Construction Company	Any current or future department

Days in advance to notify*:

Frequency: ● Once ○ Daily

Notify Requester* □

Notify Client Certificate RAO Admin(s)* □

Notify Client Certificate DRAO Admin(s)* □

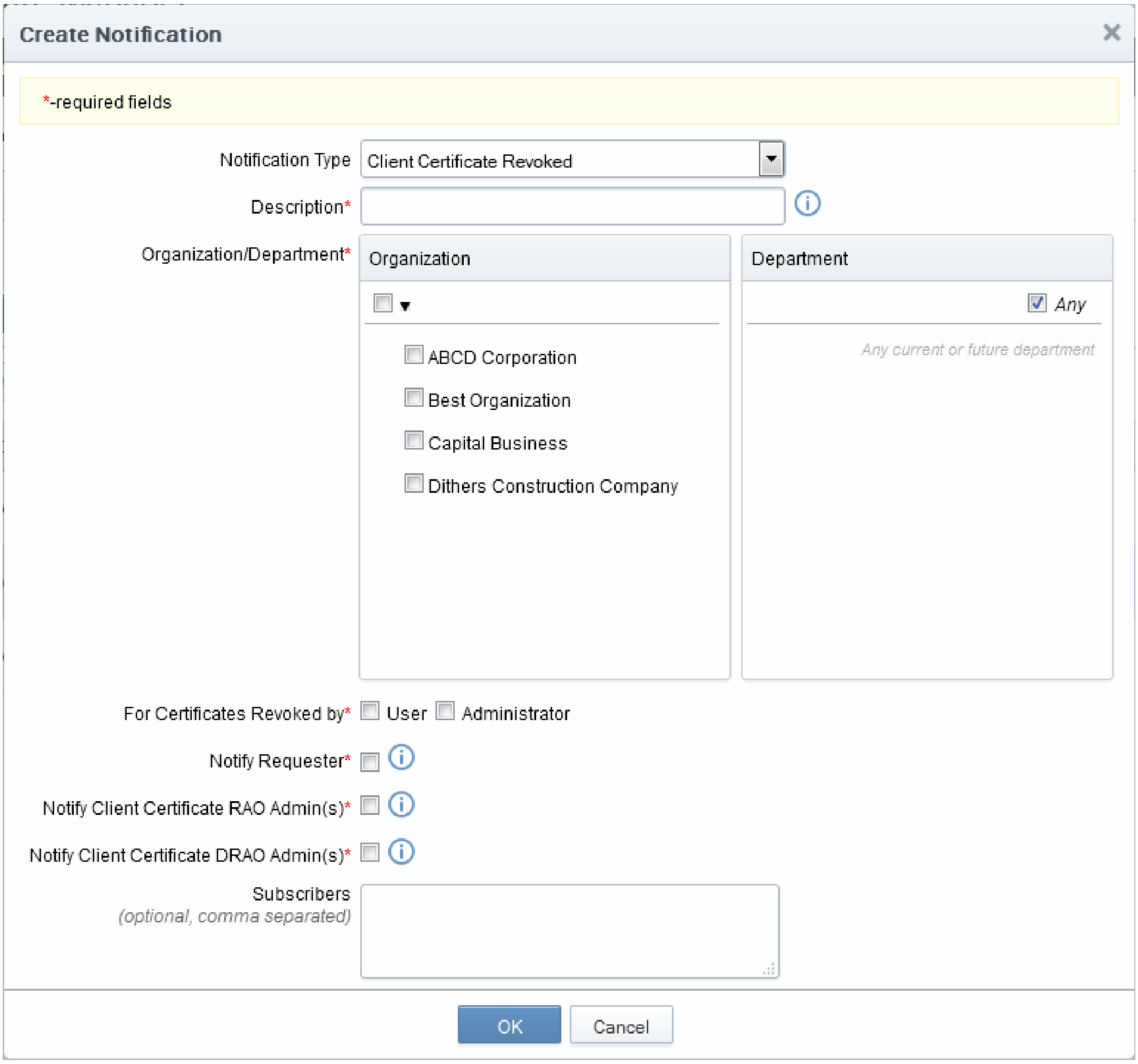
Subscribers (optional, comma separated):

6.6.2.1.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check Boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Days in advance to notify ***(required)***	Text Field	• Enables the administrator to send 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)***	Check-box	Enables the administrator to set the notification for person that requested the certificate.
Notify Client Certificate RAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification for RAO S/MIME Admin(s) of the selected organization(s).
Notify Client Certificate DRAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification for DRAO S/MIME Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.2 '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.



Create Notification

*-required fields

Notification Type: Client Certificate Revoked

Description*:

Organization/Department*:

Organization	Department
□ ▾	☑ Any
□ ABCD Corporation □ Best Organization □ Capital Business □ Dithers Construction Company	Any current or future department

For Certificates Revoked by* □ User □ Administrator

Notify Requester* □

Notify Client Certificate RAO Admin(s)* □

Notify Client Certificate DRAO Admin(s)* □

Subscribers (optional, comma separated)

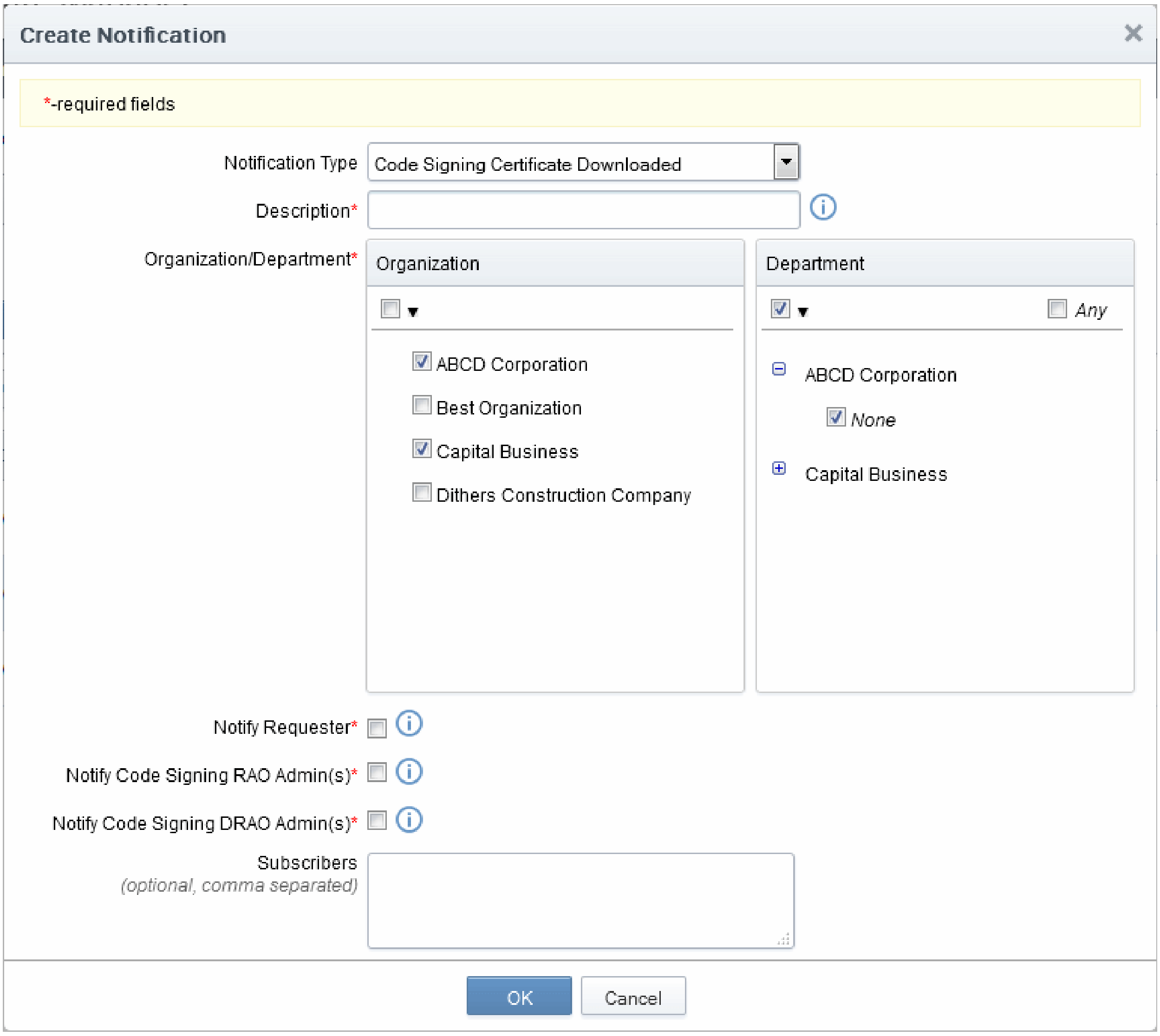
6.6.2.2.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check Boxes	- Choose the organizations/departments which should receive the notification. - Select the check-box above the list to enable for all current organizations/departments. - Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
For Certificates Revoked by: ***(required)***	Check-box	Administrator should select a person (administrator or user) after whose revoke action, the notification will be send.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification for person, who requested the certificate.

Notify Client Certificate RAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification for RAO S/MIME Admin(s) of the selected organization(s).
Notify Client Certificate DRAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification for DRAO S/MIME Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.3 '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.



Create Notification

*-required fields

Notification Type: Code Signing Certificate Downloaded

Description*:

Organization/Department*:

Organization
- ☑ ABCD Corporation
- □ Best Organization
- ☑ Capital Business
- □ Dithers Construction Company

Department ☑ □ Any
- ⊟ ABCD Corporation
  - ☑ *None*
- ⊞ Capital Business

Notify Requester* □

Notify Code Signing RAO Admin(s)* □

Notify Code Signing DRAO Admin(s)* □

Subscribers *(optional, comma separated)*

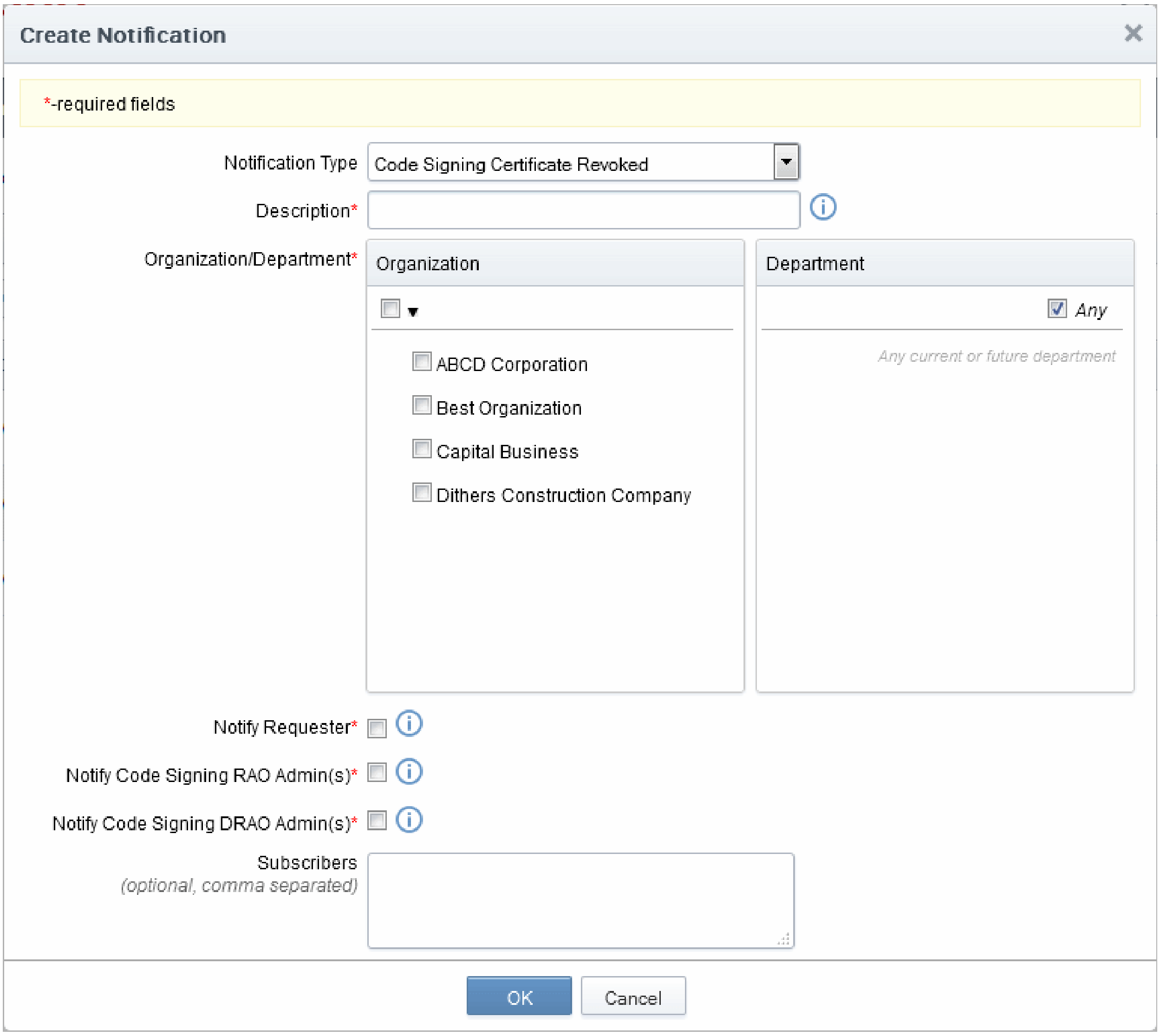
6.6.2.3.1 Table of Parameters

Form Element	Type	Descriptions

Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check Boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification for person, who requested the certificate.
Notify Code Signing RAO Admins(s) ***(required)***	Check-box	Enables the administrator to set the notification for RAO Code Signing Certificate Admin(s) of the selected organization(s)/department(s).
Notify Code Signing DRAO Admins(s) ***(required)***	Check-box	Enables the administrator to set the notification for DRAO Code Signing Certificate Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.4 '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.



Create Notification

*-required fields

Notification Type: Code Signing Certificate Revoked

Description*

Organization/Department*

Organization

□

□ ABCD Corporation
□ Best Organization
□ Capital Business
□ Dithers Construction Company

Department

☑ Any

Any current or future department

Notify Requester* □

Notify Code Signing RAO Admin(s)* □

Notify Code Signing DRAO Admin(s)* □

Subscribers
(optional, comma separated)

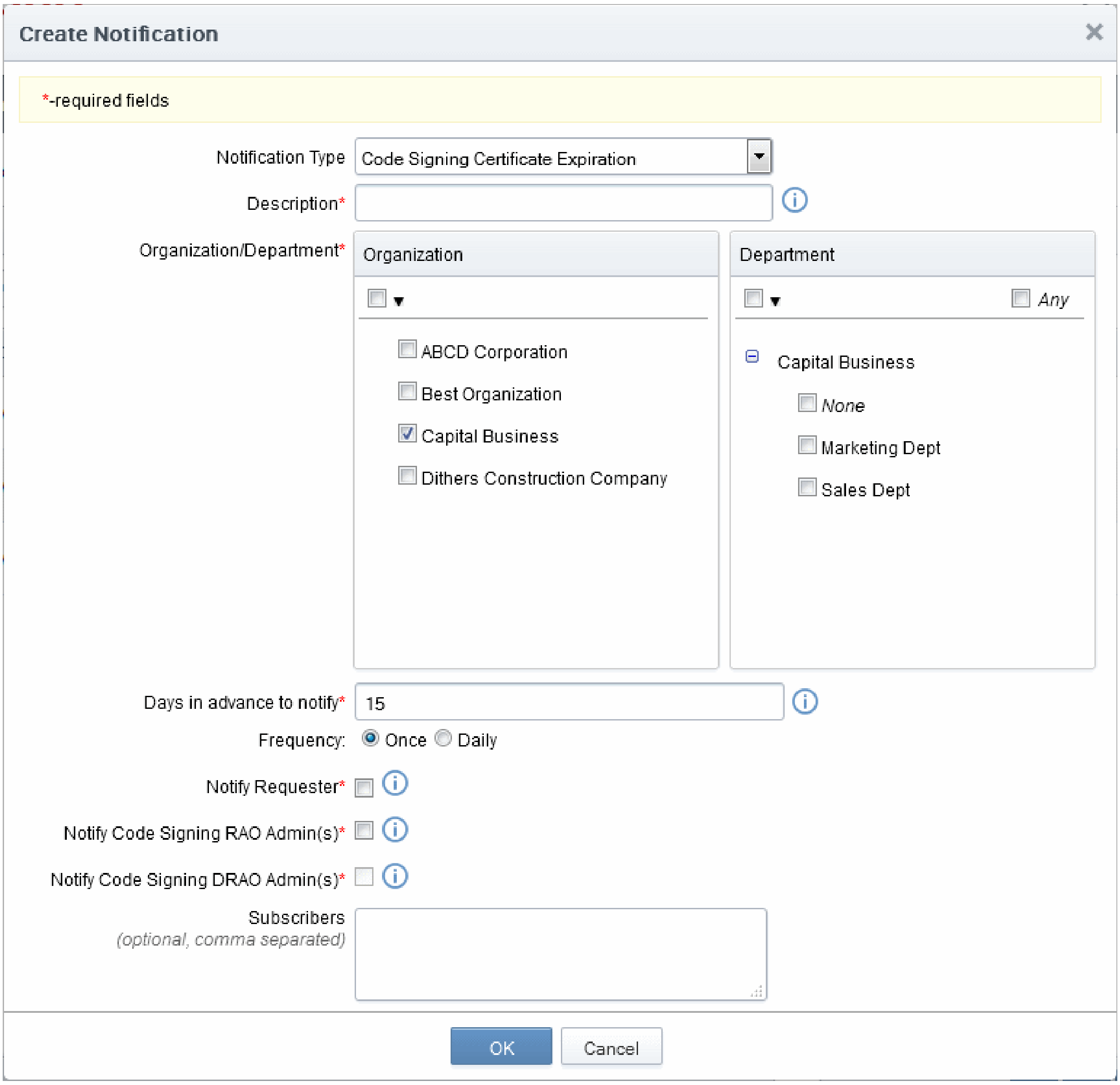
6.6.2.4.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check Boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification for person, who requested the certificate.
Notify Code Signing RAO Admins(s) ***(required)***	Check-box	Enables the administrator to set the notification for RAO Code Signing Certificate Admin(s) of the selected organization(s)/department(s).

Form Element	Type	Description
Notify Code Signing DRAO Admins(s) ***(required)***	Check-box	Enables the administrator to set the notification for DRAO Code Signing Certificate Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.5 '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.



Create Notification ✕

*-required fields

Notification Type: Code Signing Certificate Expiration

Description*:

Organization/Department*:

Organization	Department
□ ▾	□ ▾ □ *Any*
□ ABCD Corporation	⊟ Capital Business
□ Best Organization	□ *None*
☑ Capital Business	□ Marketing Dept
□ Dithers Construction Company	□ Sales Dept

Days in advance to notify*: 15

Frequency: ● Once ○ Daily

Notify Requester* □

Notify Code Signing RAO Admin(s)* □

Notify Code Signing DRAO Admin(s)* □

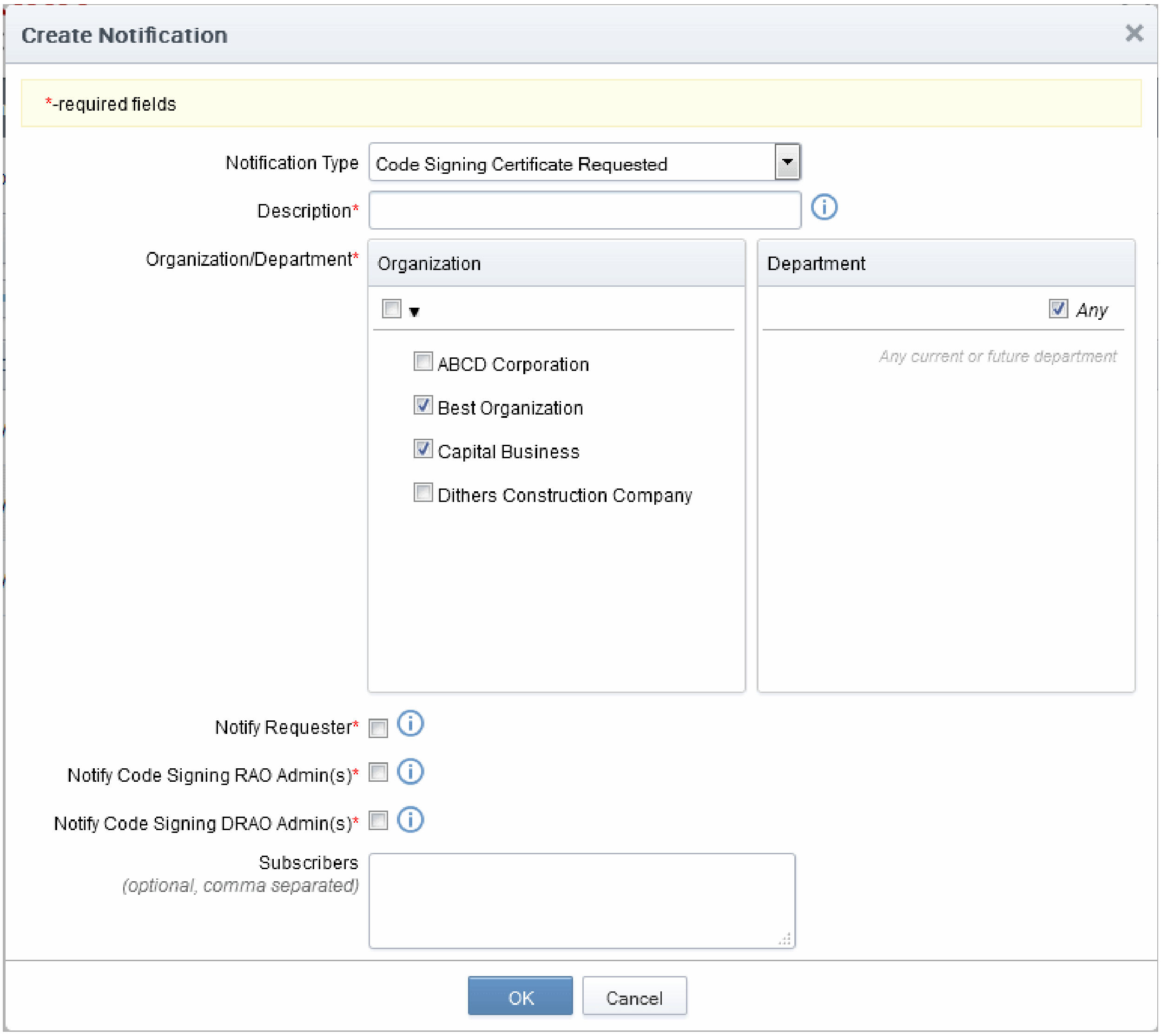
Subscribers *(optional, comma separated)*

6.6.2.5.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check Boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
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)***	Check-box	Enables the administrator to set the notification for person, who requested the certificate.
Notify Code Signing RAO Admins(s) ***(required)***	Check-box	Enables the administrator to set the notification for RAO Code Signing Certificate Admin(s) of the selected organization(s)/department(s).
Notify Code Signing DRAO Admins(s) ***(required)***	Check-box	Enables the administrator to set the notification for DRAO Code Signing Certificate Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.6 '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.



Create Notification

*-required fields

Notification Type: Code Signing Certificate Requested

Description*

Organization/Department*

Organization	Department
□ ▾	☑ Any
□ ABCD Corporation ☑ Best Organization ☑ Capital Business □ Dithers Construction Company	Any current or future department

Notify Requester* □

Notify Code Signing RAO Admin(s)* □

Notify Code Signing DRAO Admin(s)* □

Subscribers (optional, comma separated)

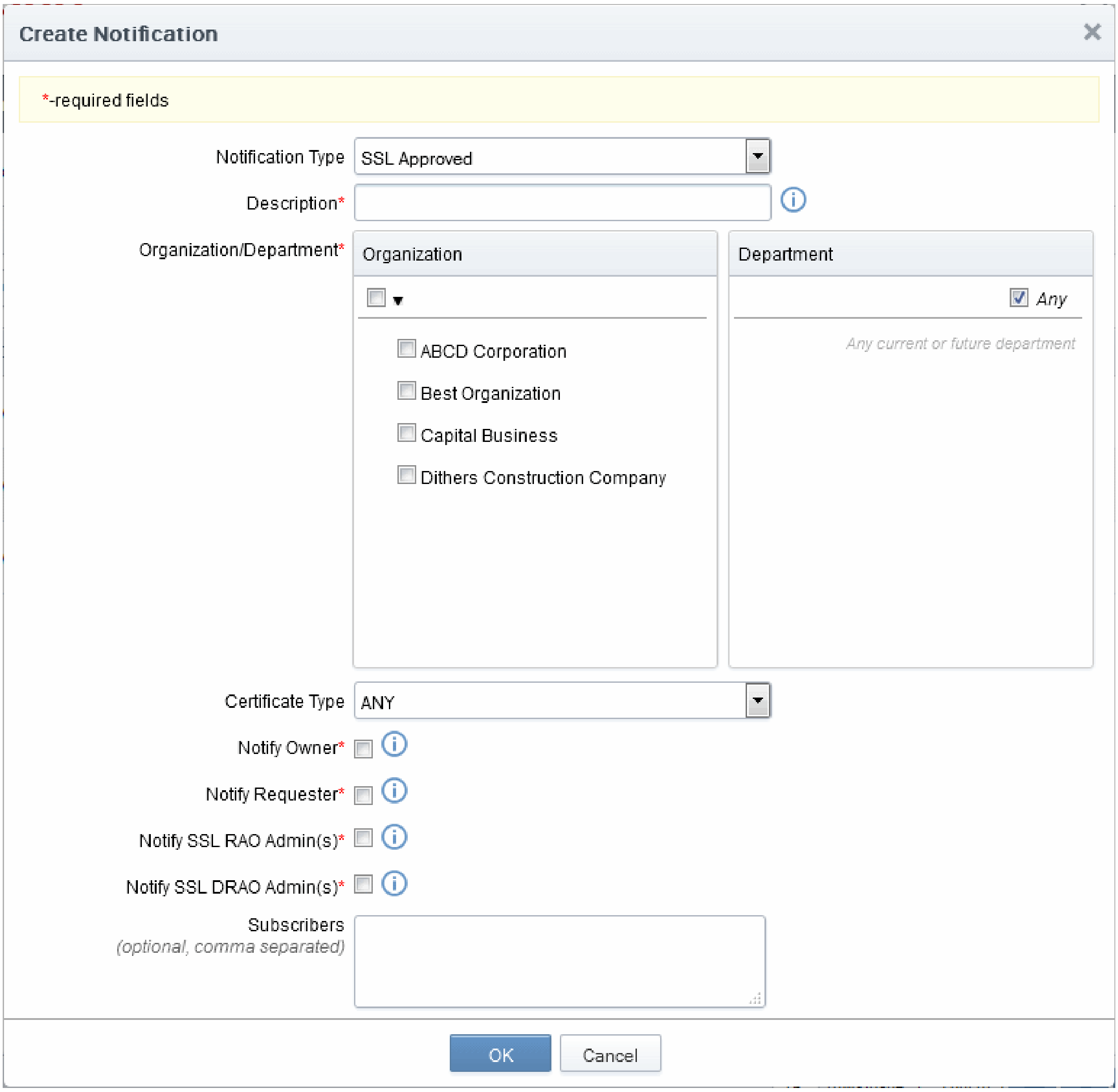
6.6.2.6.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check Boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification for person, who requested the certificate.
Notify Code Signing RAO Admins(s) ***(required)***	Check-box	Enables the administrator to set the notification for RAO Code Signing Certificate Admin(s) of the selected organization(s)/department(s).

Form Element	Type	Description
Notify Code Signing DRAO Admins(s) ***(required)***	Check-box	Enables the administrator to set the notification for DRAO Code Signing Certificate Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.7 '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.



Create Notification

*-required fields

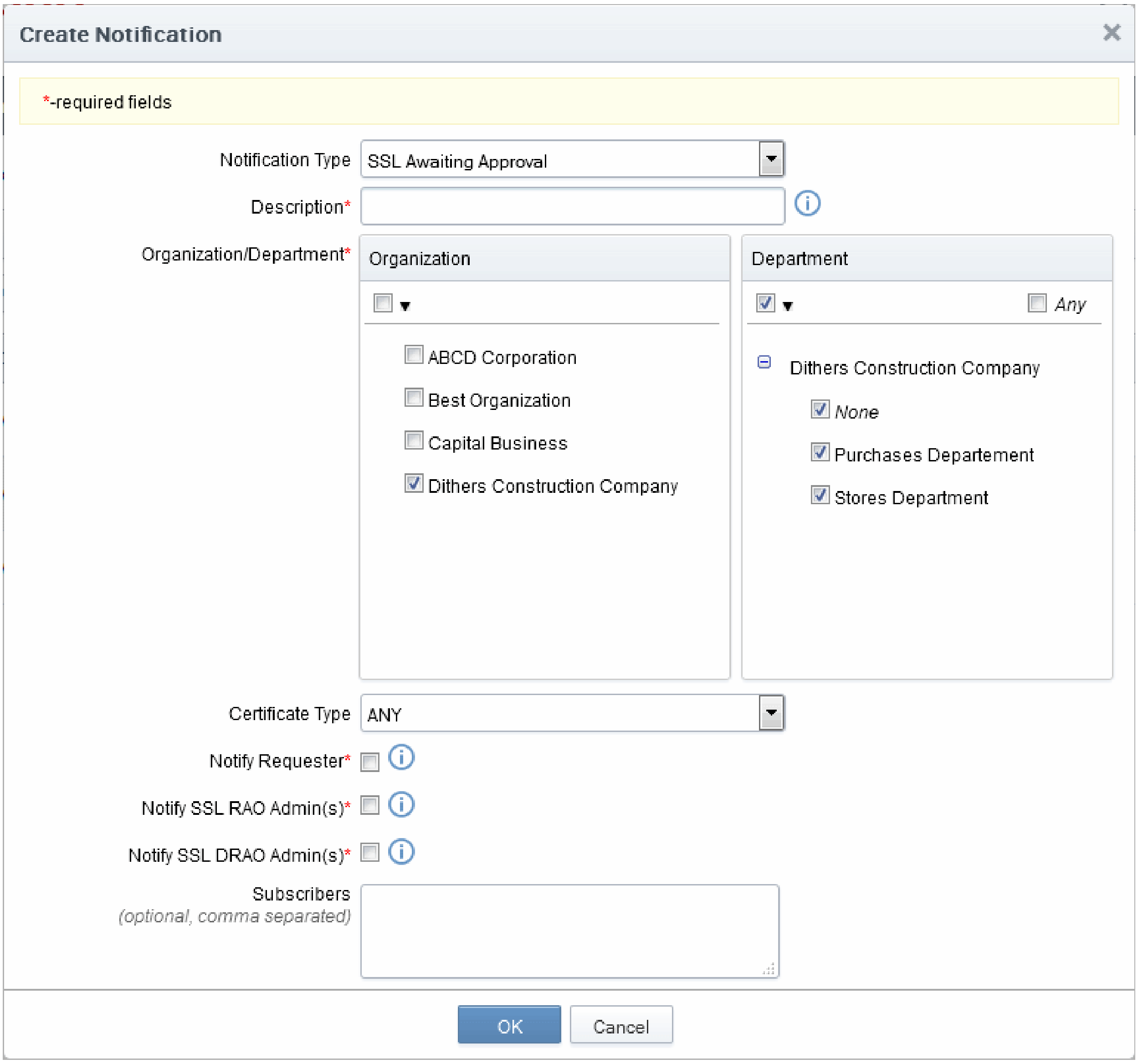
Notification Type	SSL Approved
Description*	
Organization/Department*	Organization: □ ABCD Corporation, □ Best Organization, □ Capital Business, □ Dithers Construction Company Department: ☑ *Any* — *Any current or future department*
Certificate Type	ANY
Notify Owner*	□
Notify Requester*	□
Notify SSL RAO Admin(s)*	□
Notify SSL DRAO Admin(s)*	□
Subscribers *(optional, comma separated)*	

6.6.2.7.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check Boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Certificate type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification is to be set.
Notify owner ***(required)***	Check-box	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)***	Check-box	Enables the administrator to set the notification for person, who requested the certificate.
Notify SSL RAO Admin(s) ***(required)***	Check-box	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)***	Check-box	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.8 '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'.



Create Notification

*-required fields

Notification Type	SSL Awaiting Approval
Description*	
Organization/Department*	Organization: □ ABCD Corporation; □ Best Organization; □ Capital Business; ☑ Dithers Construction Company Department: □ Any; Dithers Construction Company: ☑ None; ☑ Purchases Departement; ☑ Stores Department
Certificate Type	ANY
Notify Requester*	□
Notify SSL RAO Admin(s)*	□
Notify SSL DRAO Admin(s)*	□
Subscribers (optional, comma separated)	

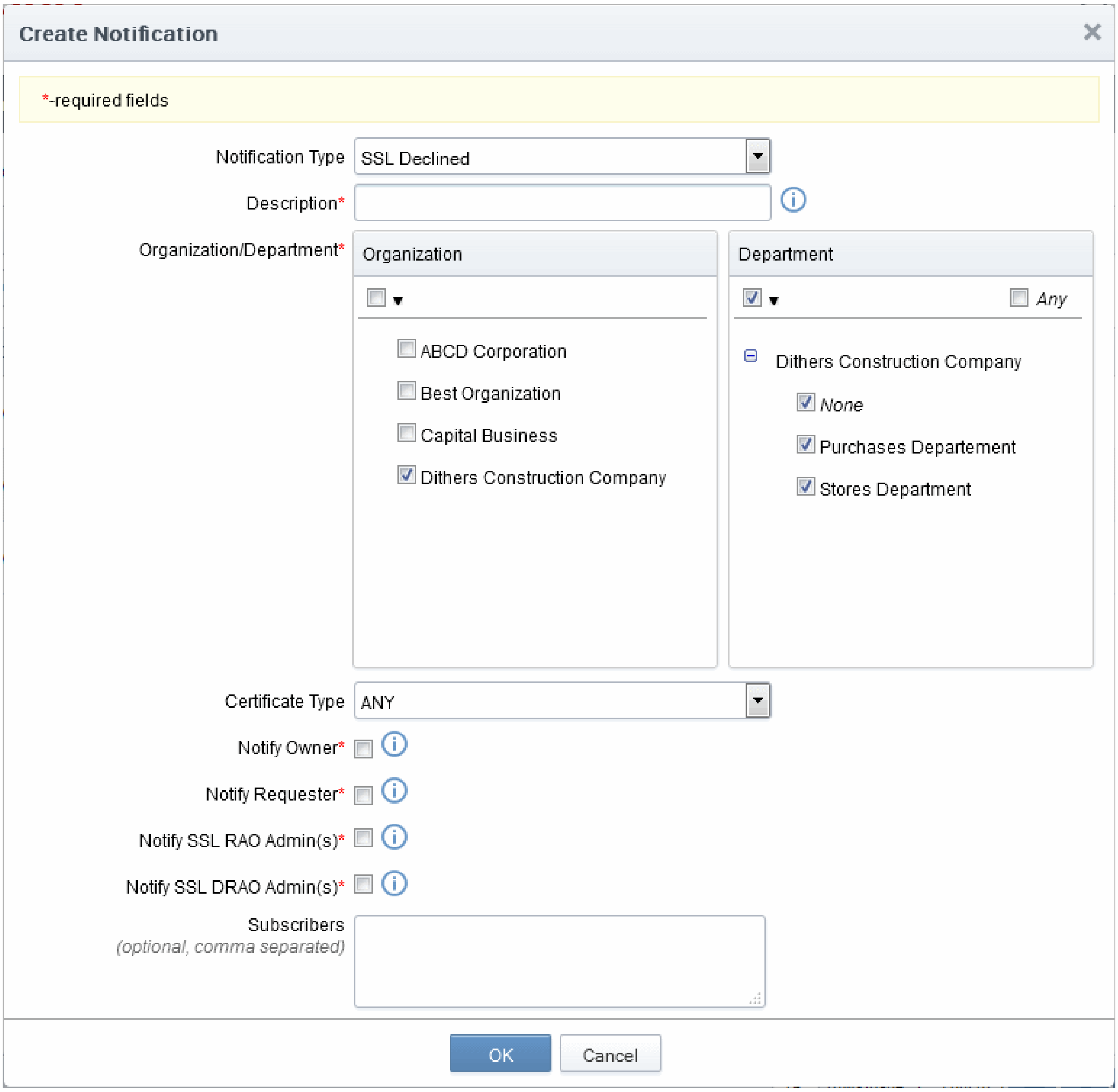
6.6.2.8.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check Boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Certificate type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification is to be set.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification for person, who requested the certificate.

Form Element	Type	Description
Notify SSL RAO Admin(s) ***(required)***	Check-box	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)***	Check-box	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.9 '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.



Create Notification

*-required fields

Notification Type: SSL Declined

Description*:

Organization/Department*

Organization: □ ABCD Corporation, □ Best Organization, □ Capital Business, ☑ Dithers Construction Company

Department: □ *Any*; Dithers Construction Company: ☑ *None*, ☑ Purchases Departement, ☑ Stores Department

Certificate Type: ANY

Notify Owner*: □

Notify Requester*: □

Notify SSL RAO Admin(s)*: □

Notify SSL DRAO Admin(s)*: □

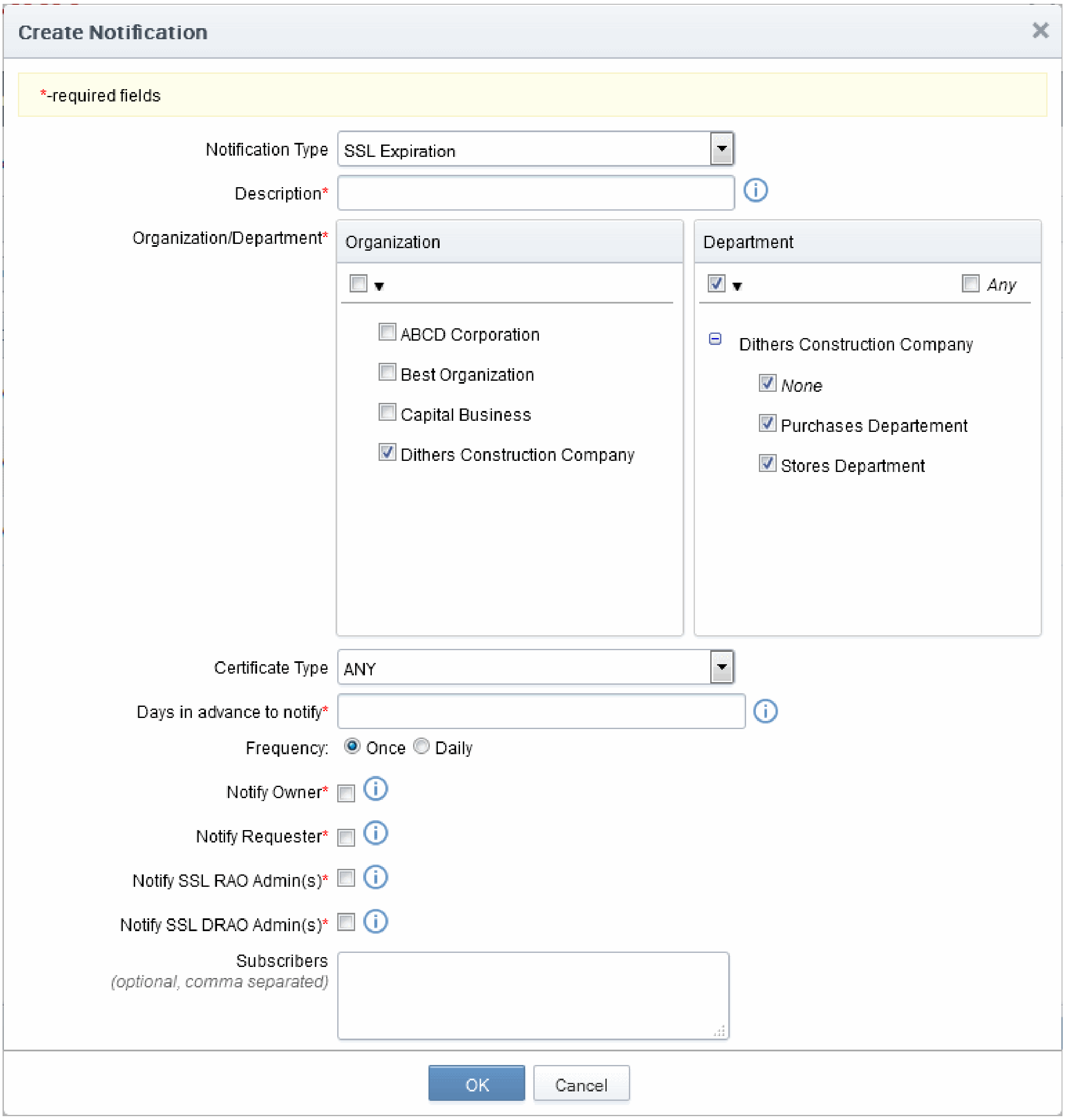
Subscribers *(optional, comma separated)*:

6.6.2.9.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check Boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Certificate type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification should be set.
Notify Owner ***(required)***	Check-box	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)***	Check-box	Enables the administrator to set the notification for a person, who requested the certificate.
Notify SSL RAO Admin(s) ***(required)***	Check-box	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)***	Check-box	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.10 '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.



Create Notification

*-required fields

Notification Type	SSL Expiration
Description*	
Organization/Department*	

Organization

□ ▾

□ ABCD Corporation

□ Best Organization

□ Capital Business

☑ Dithers Construction Company

Department

☑ ▾ □ *Any*

⊟ Dithers Construction Company

☑ *None*

☑ Purchases Departement

☑ Stores Department

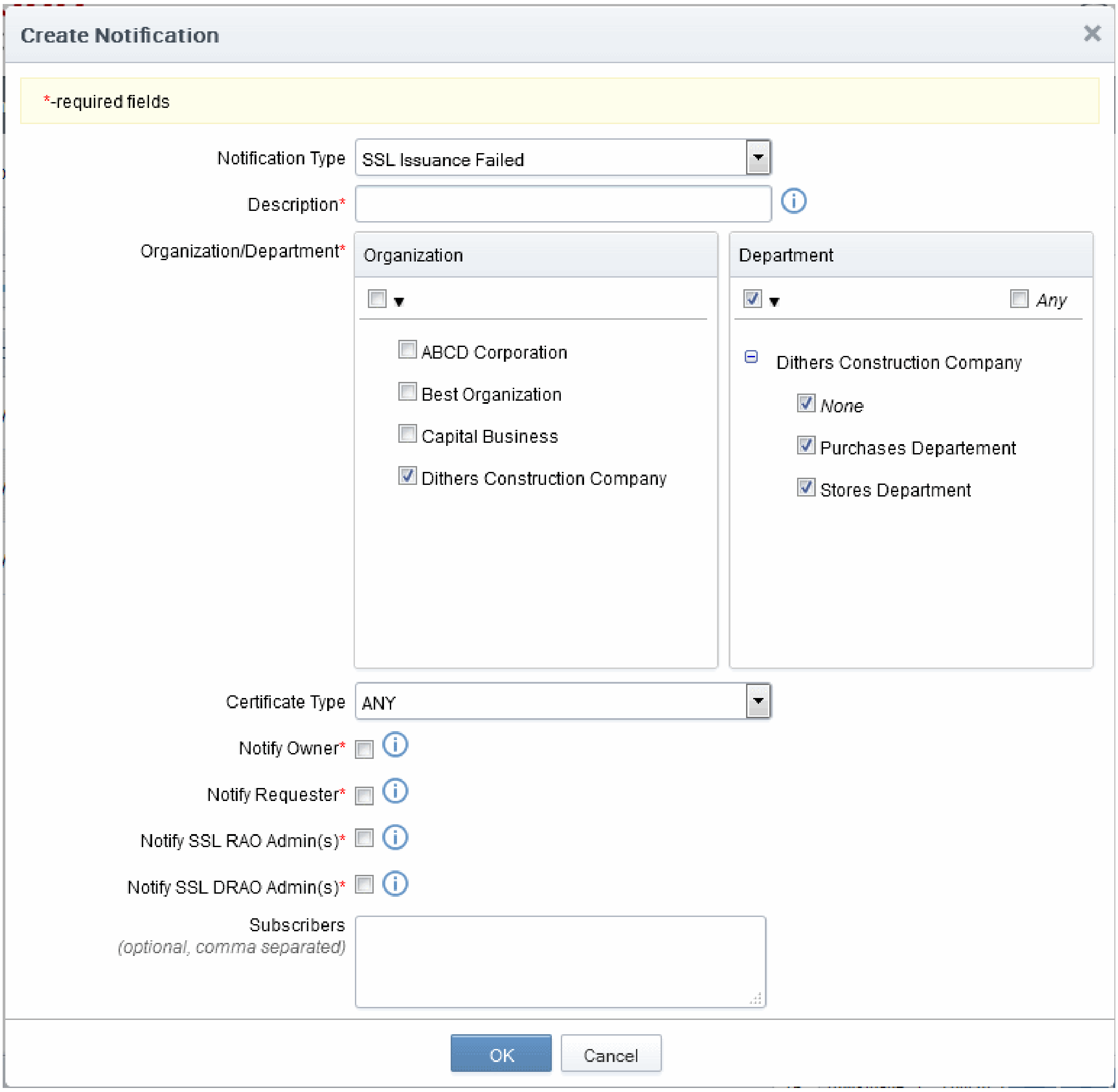
Certificate Type	ANY
Days in advance to notify*	
Frequency:	● Once ○ Daily
Notify Owner*	□
Notify Requester*	□
Notify SSL RAO Admin(s)*	□
Notify SSL DRAO Admin(s)*	□
Subscribers *(optional, comma separated)*	

6.6.2.10.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check Boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Certificate type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification is to 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)***	Check-box	Enables the administrator to set the notification for a person, who owns the certificate.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification for a person, who requested the certificate.
Notify SSL RAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification for RAO SSL Admin(s) of the selected organization(s)/departments.
Notify SSL DRAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification for DRAO SSL Admin(s) of the department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.11 '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.



Create Notification

*-required fields

Notification Type: SSL Issuance Failed

Description*

Organization/Department*

Organization

☐ ABCD Corporation

☐ Best Organization

☐ Capital Business

☑ Dithers Construction Company

Department

☑ ☐ Any

Dithers Construction Company

☑ None

☑ Purchases Departement

☑ Stores Department

Certificate Type: ANY

Notify Owner* ☐

Notify Requester* ☐

Notify SSL RAO Admin(s)* ☐

Notify SSL DRAO Admin(s)* ☐

Subscribers (optional, comma separated)

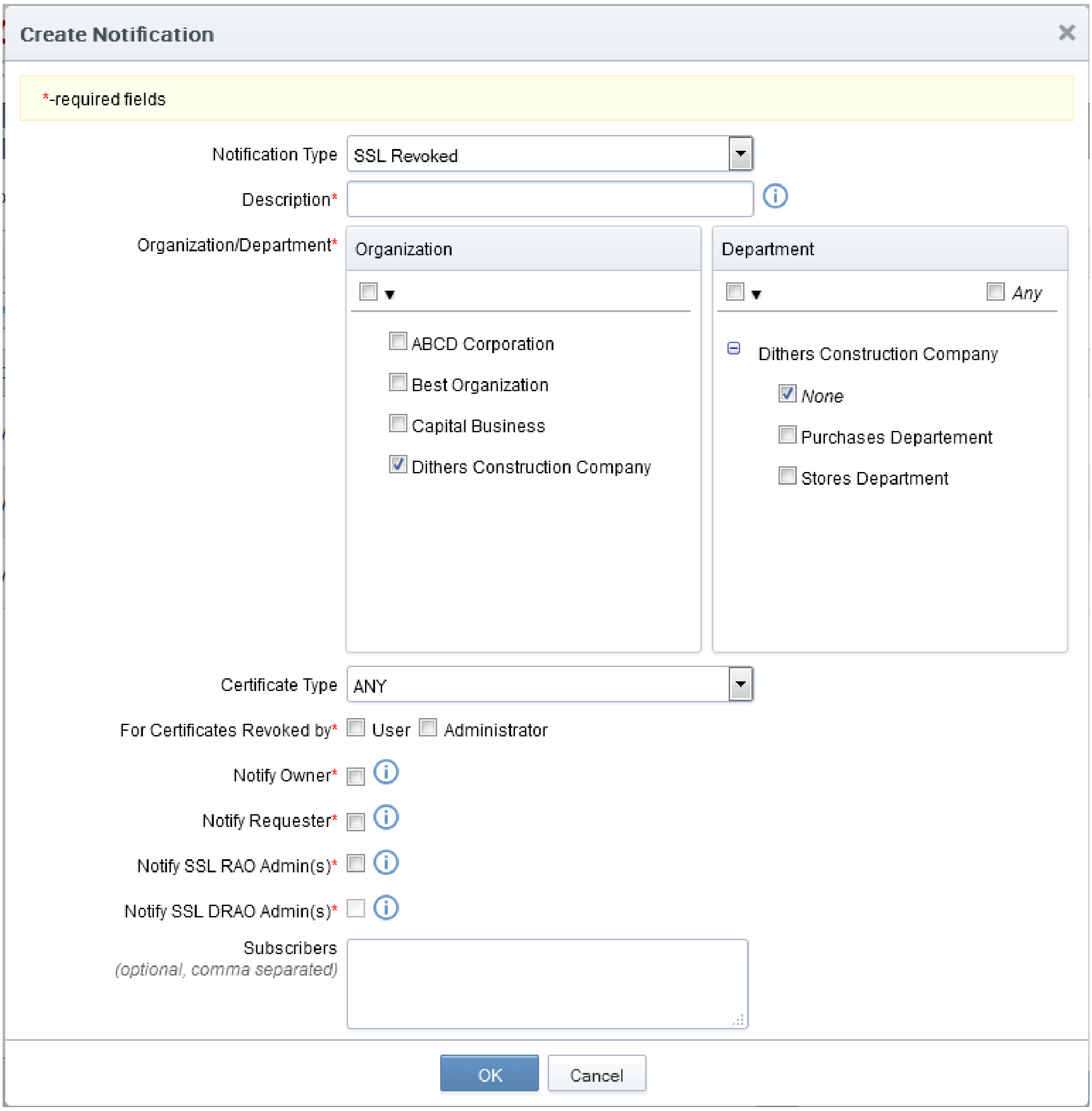
6.6.2.11.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Certificate type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification is to be set.

Form Element	Type	Description
Notify owner ***(required)***	Check-box	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification for a person, who requested the certificate.
Notify SSL RAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification for RAO SSL Admin(s) of the selected organization(s).
Notify SSL DRAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification for DRAO SSL Admin(s) of selected the department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.12 '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).



Create Notification

*-required fields

Notification Type: SSL Revoked

Description*:

Organization/Department*

Organization

□

- □ ABCD Corporation
- □ Best Organization
- □ Capital Business
- ☑ Dithers Construction Company

Department

□ □ *Any*

Dithers Construction Company

- ☑ *None*
- □ Purchases Departement
- □ Stores Department

Certificate Type: ANY

For Certificates Revoked by*: □ User □ Administrator

Notify Owner*: □

Notify Requester*: □

Notify SSL RAO Admin(s)*: □

Notify SSL DRAO Admin(s)*: □

Subscribers *(optional, comma separated)*:

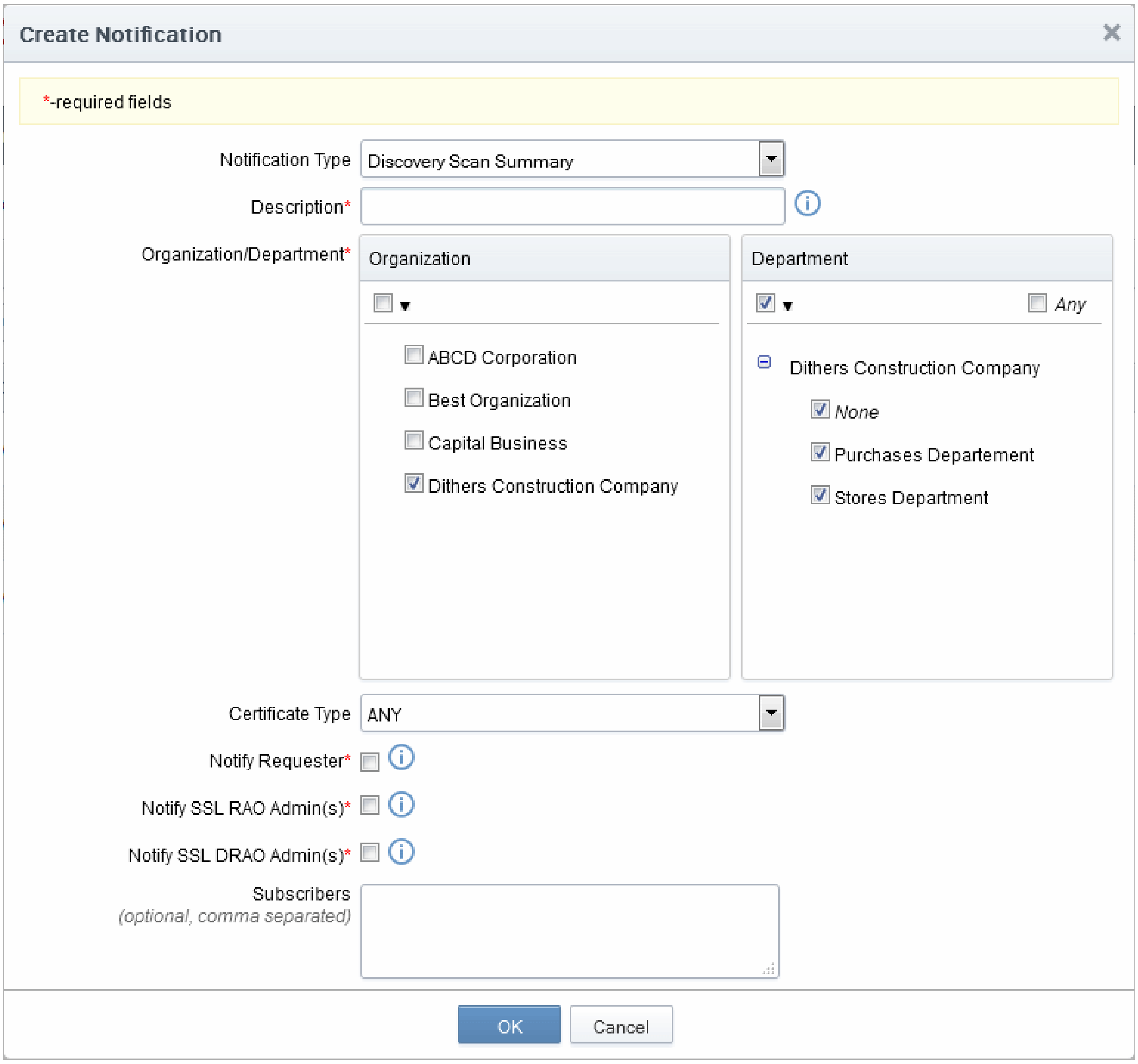
6.6.2.12.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Certificate type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the notification

Form Element	Type	Description
		is to be set.
For Certificates Revoked by: ***(required)***	Check-box	Administrator should select a person (administrator or user) after whose revocation action, the notification is to be sent.
Notify Owner ***(required)***	Check-box	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification for a person, who requested the certificate.
Notify SSL RAO Admin(s) ***(required)***	Check-box	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)***	Check-box	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.13 '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.



Create Notification

*-required fields

Notification Type: Discovery Scan Summary

Description*:

Organization/Department*:

Organization	Department
□	☑ □ Any
□ ABCD Corporation	⊟ Dithers Construction Company
□ Best Organization	☑ *None*
□ Capital Business	☑ Purchases Departement
☑ Dithers Construction Company	☑ Stores Department

Certificate Type: ANY

Notify Requester* □

Notify SSL RAO Admin(s)* □

Notify SSL DRAO Admin(s)* □

Subscribers *(optional, comma separated)*

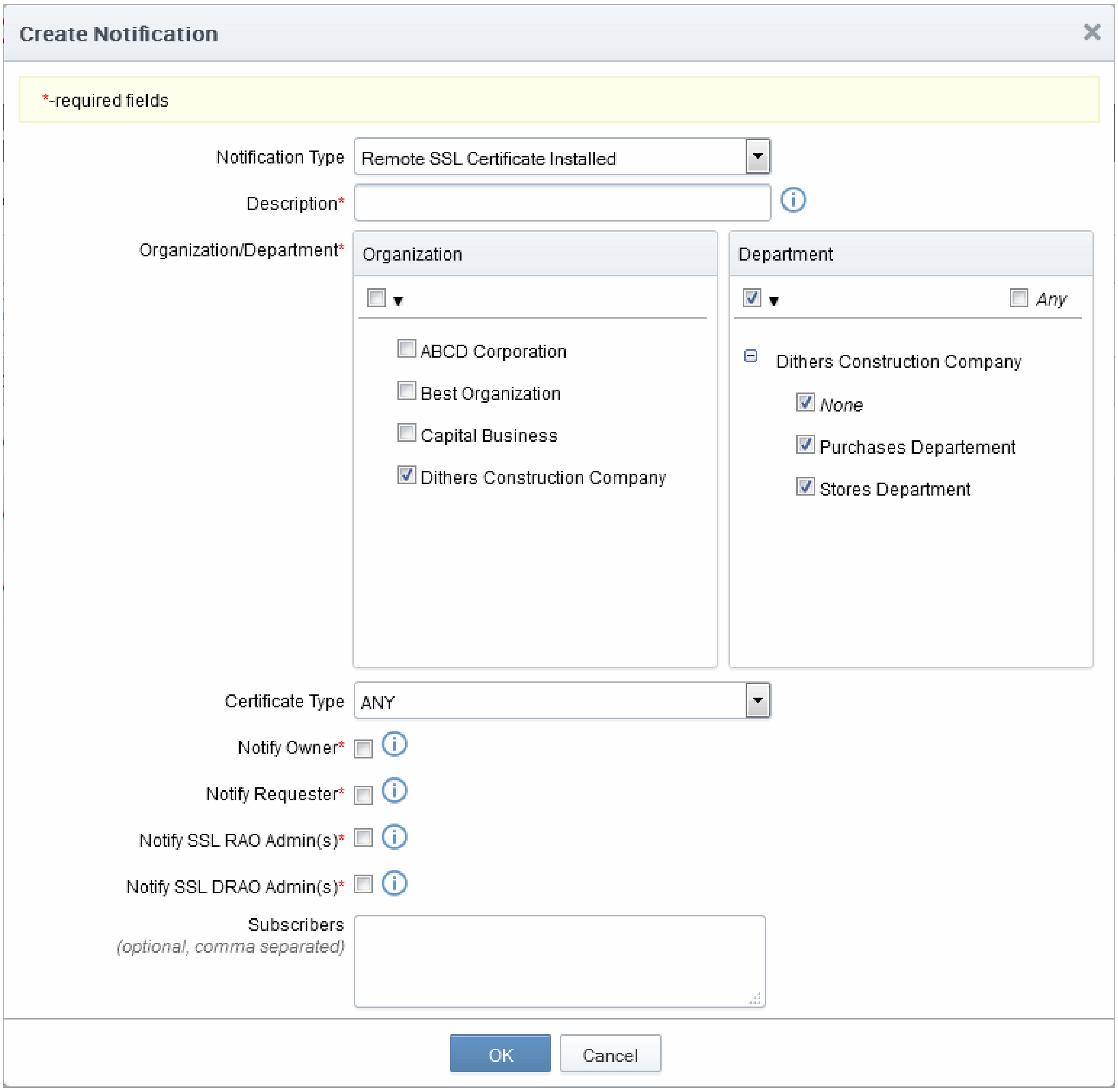
6.6.2.13.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Certificates type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the discovery scan summary notification will be set.
Notify SSL RAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification for RAO SSL Admin(s) of

Form Element	Type	Description
		the selected organization(s)/department(s).
Notify SSL DRAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification for DRAO SSL Admin(s) of the selected organization(s)/department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.14 '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.



Create Notification

*-required fields

Notification Type: Remote SSL Certificate Installed

Description*:

Organization/Department*:

Organization: □ ▾
- □ ABCD Corporation
- □ Best Organization
- □ Capital Business
- ☑ Dithers Construction Company

Department: ☑ ▾ □ *Any*
- ⊟ Dithers Construction Company
  - ☑ *None*
  - ☑ Purchases Departement
  - ☑ Stores Department

Certificate Type: ANY

Notify Owner* □

Notify Requester* □

Notify SSL RAO Admin(s)* □

Notify SSL DRAO Admin(s)* □

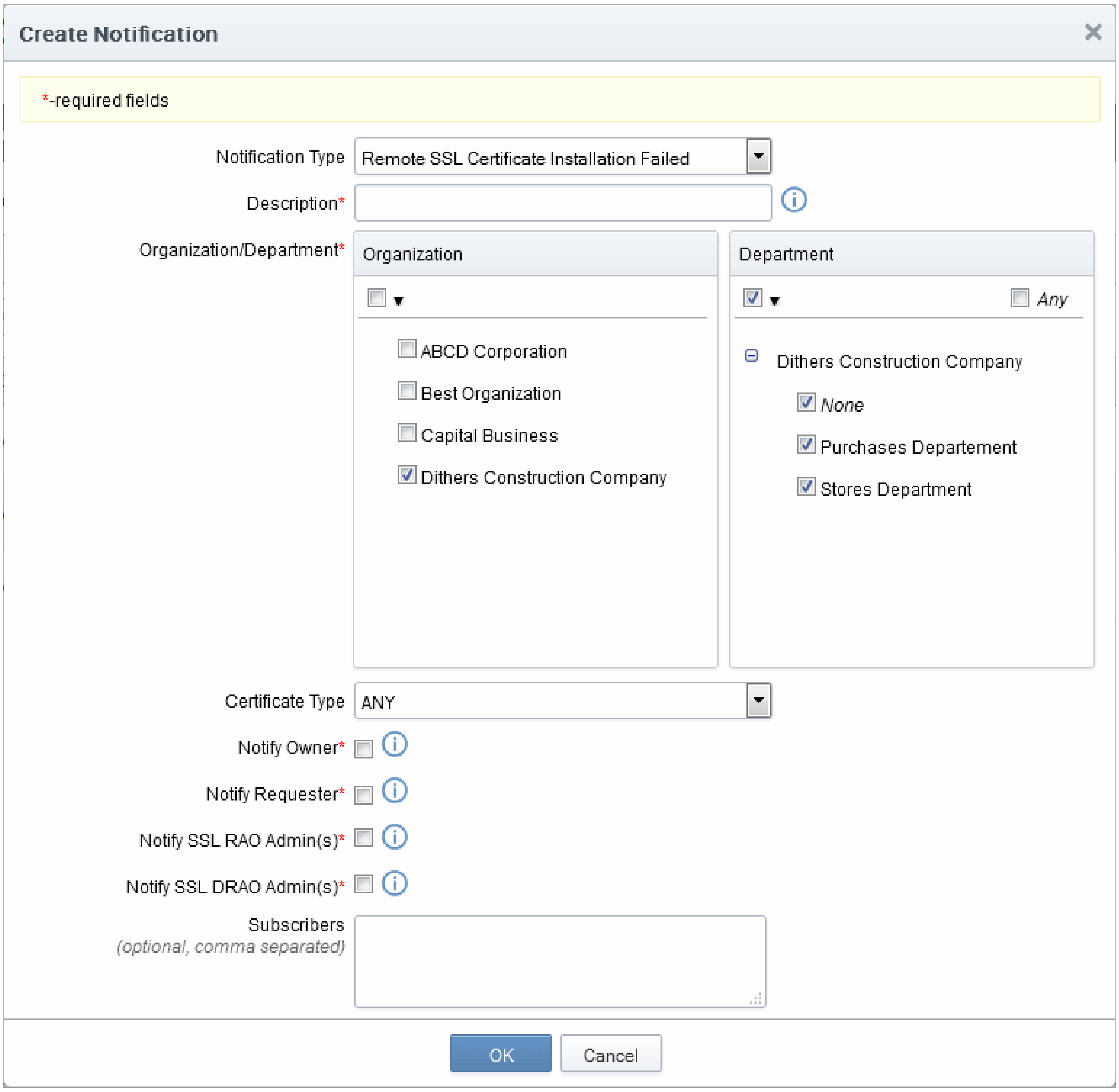
Subscribers *(optional, comma separated)*:

6.6.2.14.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Checkboxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Certificate Type: ***(required)***	Drop-down	Administrator should select type of SSL certificate for which the 'SSL certificate was installed remotely' notification is to 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 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 email address(es) of other people to whom the notifications are to be sent.

6.6.2.15 '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.



Create Notification

*-required fields

Notification Type: Remote SSL Certificate Installation Failed

Description*:

Organization/Department*:

Organization	Department
□	☑ □ Any
□ ABCD Corporation	⊟ Dithers Construction Company
□ Best Organization	☑ None
□ Capital Business	☑ Purchases Departement
☑ Dithers Construction Company	☑ Stores Department

Certificate Type: ANY

Notify Owner* □

Notify Requester* □

Notify SSL RAO Admin(s)* □

Notify SSL DRAO Admin(s)* □

Subscribers (optional, comma separated):

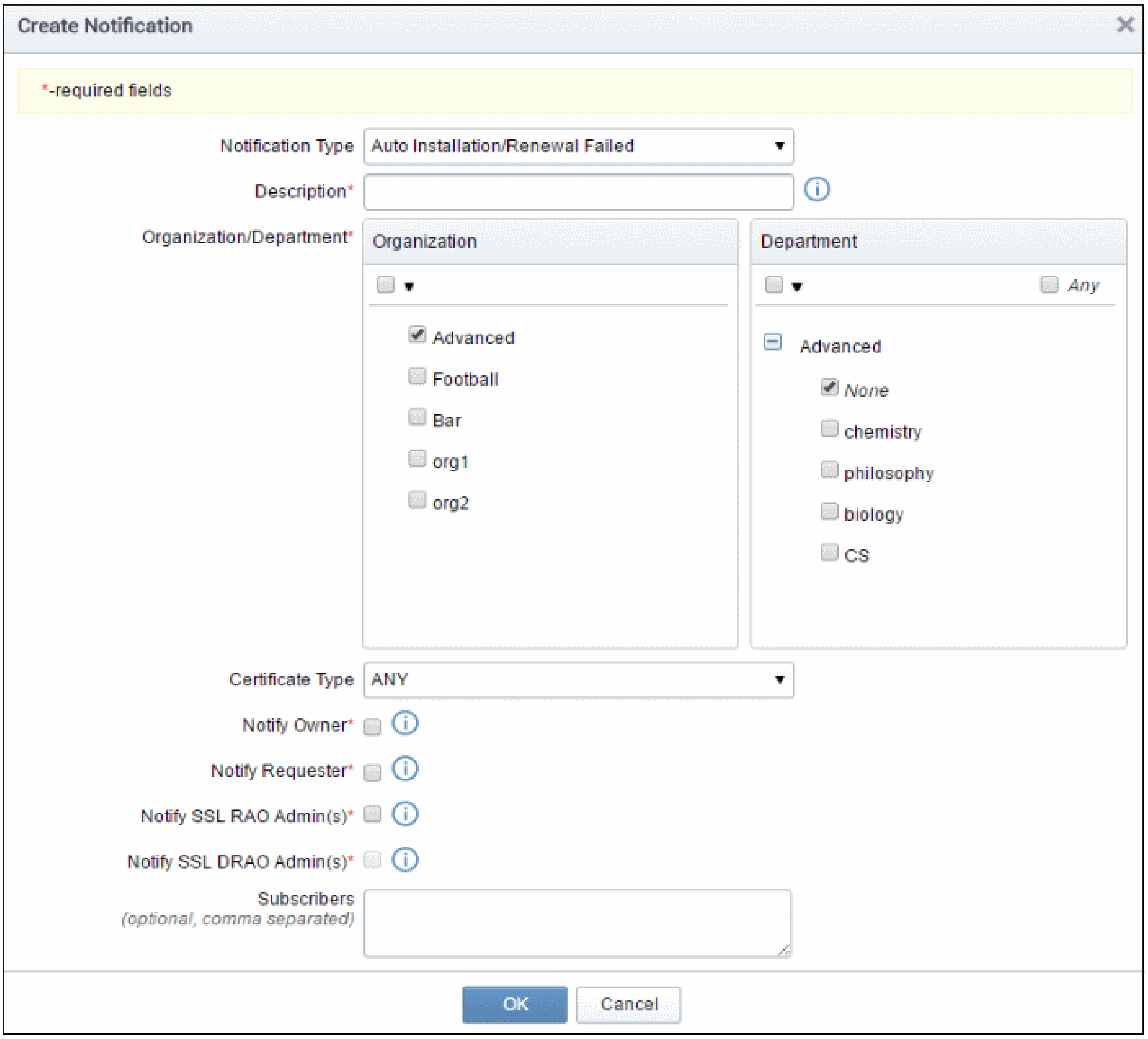
6.6.2.15.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Checkboxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Certificate Type: ***(required)***	Drop-down	Administrator should select the type of SSL certificate for which the 'Remote installation failed' notification is to be sent.
Notify Owner ***(required)***	Checkbox	Enables the administrator to set the notification for the Owner of the

Form Element	Type	Description
		certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to set the notification to the person who requested the Admin status.
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 email address(es) of other people to whom the notifications are to be sent.

6.6.2.16 'Auto Installation/Renewal Failed' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel for whom auto installation/renewal has failed.



Create Notification

*-required fields

Notification Type: Auto Installation/Renewal Failed

Description*:

Organization/Department*:

Organization	Department
☑ Advanced	Advanced: ☑ *None*, □ chemistry, □ philosophy, □ biology, □ CS
□ Football	
□ Bar	
□ org1	
□ org2	

Certificate Type: ANY

Notify Owner* □

Notify Requester* □

Notify SSL RAO Admin(s)* □

Notify SSL DRAO Admin(s)* □

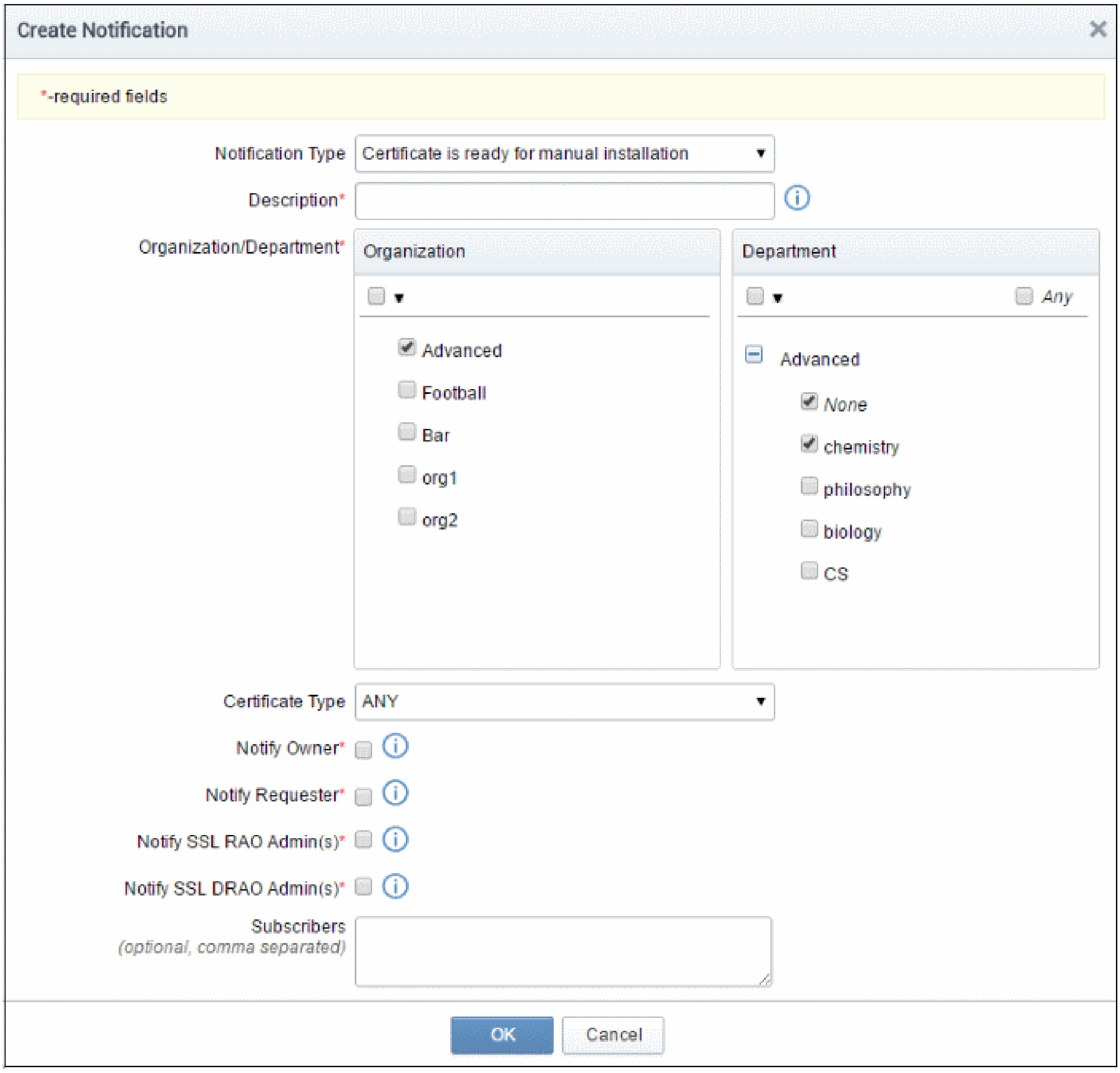
Subscribers *(optional, comma separated)*:

6.6.2.16.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Checkboxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Certificate Type: (required)	Drop-down	Administrator should choose the type of SSL certificate for which the remote installation failed notification will be sent.
Notify Owner ***(required)***	Checkbox	Enables the administrator to send the notification for the Owner of the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to send the notification to the person who requested the Admin status.
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to send 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 send the notification for DRAO SSL Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.17 'Certificate Ready for Manual Installation' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel for whom certificate is ready for manual installation.



Create Notification

*-required fields

Notification Type: Certificate is ready for manual installation

Description*:

Organization/Department*

Organization
- ☑ Advanced
- □ Football
- □ Bar
- □ org1
- □ org2

Department — □ *Any*
- ⊟ Advanced
  - ☑ *None*
  - ☑ chemistry
  - □ philosophy
  - □ biology
  - □ CS

Certificate Type: ANY

Notify Owner* □

Notify Requester* □

Notify SSL RAO Admin(s)* □

Notify SSL DRAO Admin(s)* □

Subscribers *(optional, comma separated)*:

6.6.2.17.1 Table of Parameters

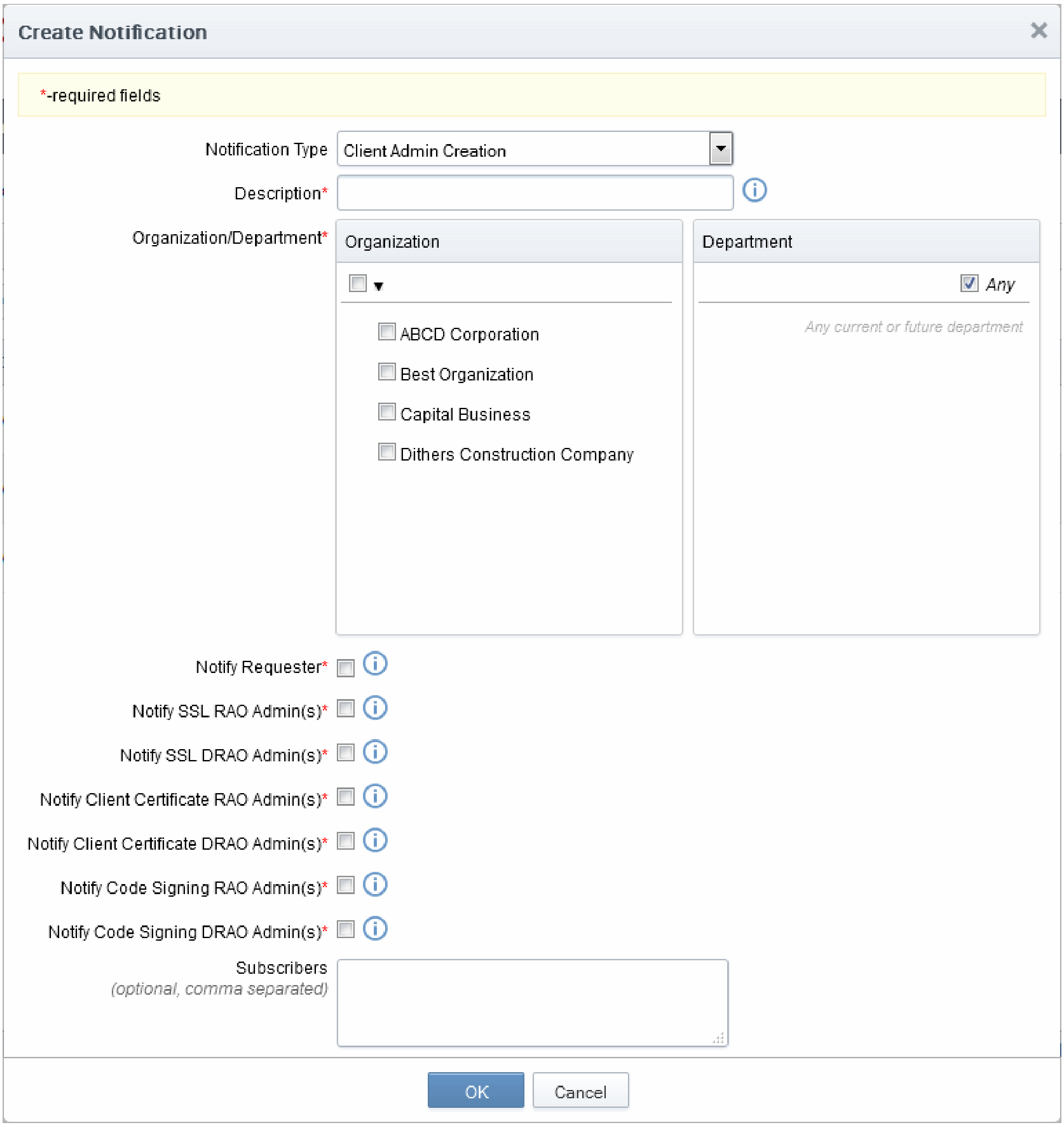
Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Checkboxes	- Choose the organizations/departments which should receive the notification.

Form Element	Type	Description
		- Select the check-box above the list to enable for all current organizations/departments. - Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.

Form Element	Type	Description
Certificate Type: (required)	Drop-down	Administrator should choose the type of SSL certificate for which the remote installation failed notification will be sent.
Notify Owner ***(required)***	Checkbox	Enables the administrator to send the notification for the Owner of the certificate.
Notify Requester ***(required)***	Checkbox	Enables the administrator to send the notification to the person who requested the Admin status.
Notify SSL RAO Admin(s) ***(required)***	Checkbox	Enables the administrator to send 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 send the notification for DRAO SSL Admin(s) of the selected department(s).
Subscribers ***(optional)***	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.18 'Client Admin Creation' Create Notification Form

Enables the Administrator to create a notification to selected personnel upon creation of new RAO or DRAO Administrators.



Create Notification

*-required fields

Notification Type	Client Admin Creation
Description*	
Organization/Department*	Organization: □ ABCD Corporation □ Best Organization □ Capital Business □ Dithers Construction Company Department: ☑ Any Any current or future department
Notify Requester*	□
Notify SSL RAO Admin(s)*	□
Notify SSL DRAO Admin(s)*	□
Notify Client Certificate RAO Admin(s)*	□
Notify Client Certificate DRAO Admin(s)*	□
Notify Code Signing RAO Admin(s)*	□
Notify Code Signing DRAO Admin(s)*	□
Subscribers (optional, comma separated)	

6.6.2.18.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments.

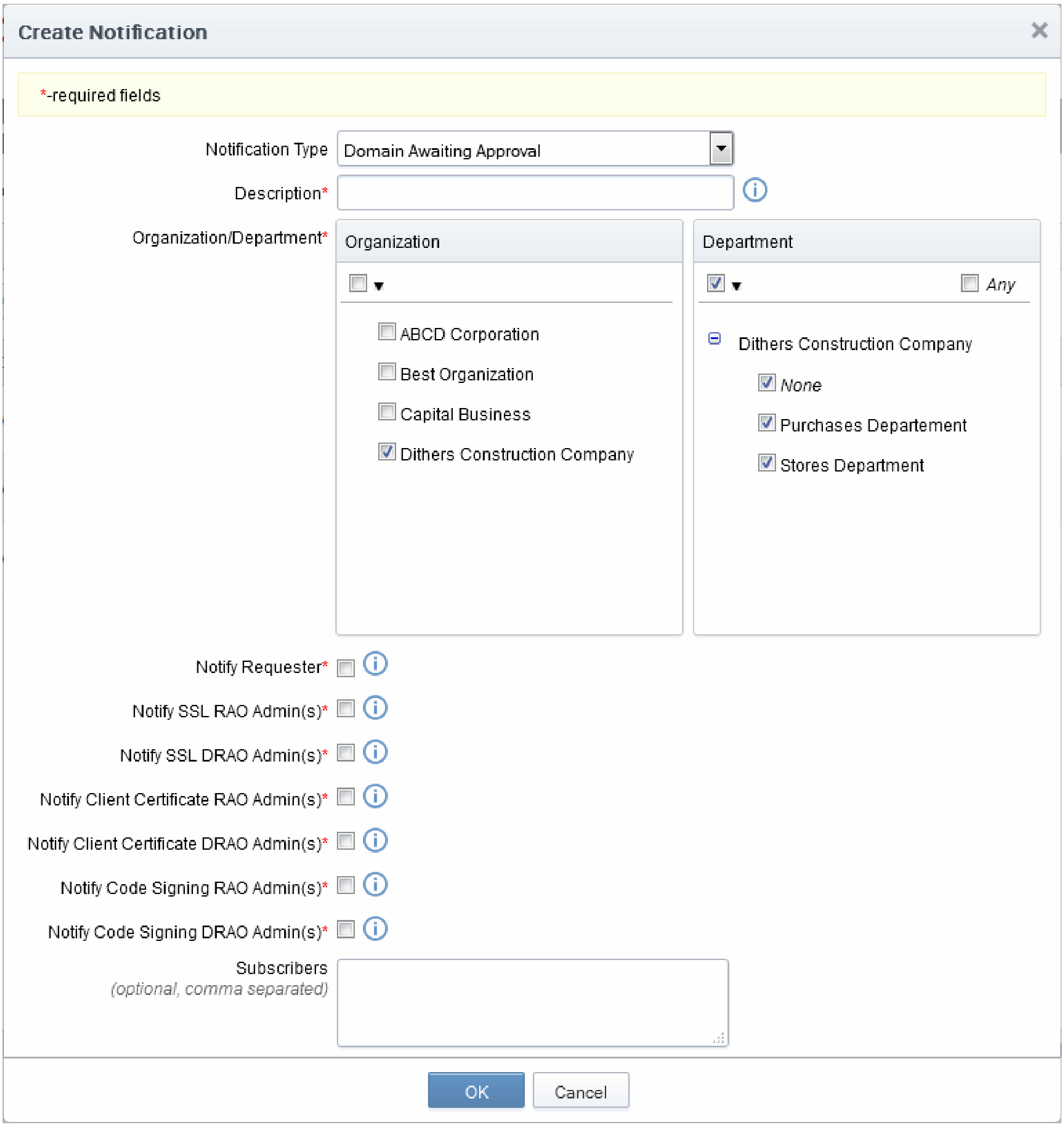
Form Element	Type	Description
		- Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.

Form Element	Type	Description
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification to the person who requested the Admin status.

Form Element	Type	Description
Notify SSL RAO Admin(s) ***(required)***	Check-box	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)***	Check-box	Enables the administrator to set the notification all the DRAO SSL Admin(s) of the selected departments.
Notify Client Certificate RAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification all the RAO S/MIME Admin(s) of the selected organization(s)/departments.
Notify Client Certificate DRAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification all the DRAO S/MIME Admin(s) of the selected departments.
Notify Code Signing RAO Admin(s) ***(required)***	Check-box	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)***	Check-box	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 email address(es) of other people to whom the notifications are to be sent.

6.6.2.19 '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 RAO Administrator. Before the request is approved, its state is 'Awaiting Approval'.



Create Notification

*-required fields

Notification Type: Domain Awaiting Approval

Description*:

Organization/Department*

Organization

□ ▾

□ ABCD Corporation

□ Best Organization

□ Capital Business

☑ Dithers Construction Company

Department

☑ ▾ □ *Any*

⊟ Dithers Construction Company

☑ *None*

☑ Purchases Departement

☑ Stores Department

Notify Requester* □

Notify SSL RAO Admin(s)* □

Notify SSL DRAO Admin(s)* □

Notify Client Certificate RAO Admin(s)* □

Notify Client Certificate DRAO Admin(s)* □

Notify Code Signing RAO Admin(s)* □

Notify Code Signing DRAO Admin(s)* □

Subscribers *(optional, comma separated)*

6.6.2.19.1 Table of Parameters

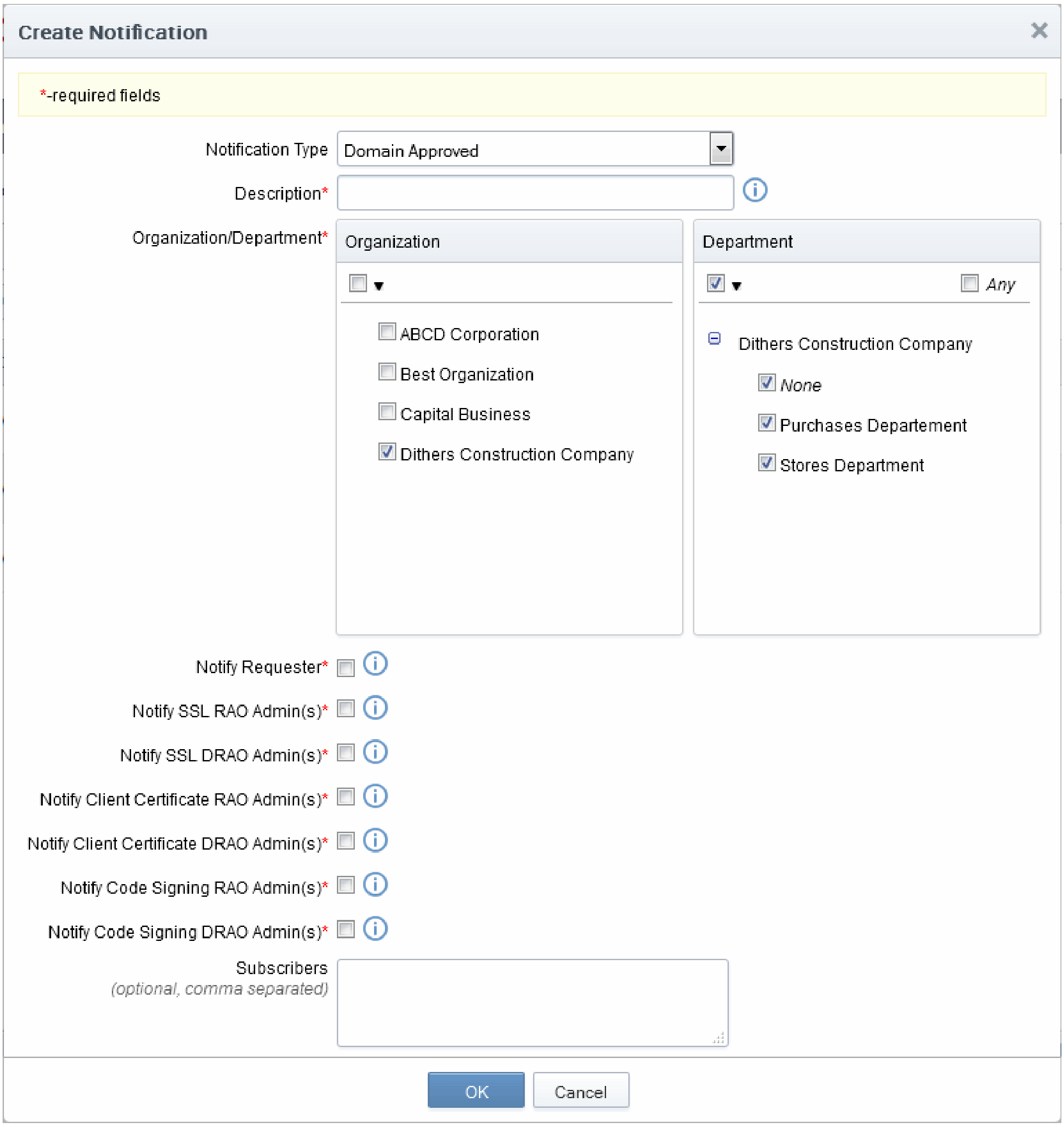
Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification to the person who requested the delegation of a created domain to an organization/department.
Notify SSL RAO Admin(s) ***(required)***	Check-box	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)***	Check-box	Enables the administrator to set the notification all the DRAO SSL Admin(s) of the selected departments.
Notify Client Certificate RAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification all the RAO S/MIME Admin(s) of the selected organization(s)/departments.
Notify Client Certificate DRAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification all the DRAO S/MIME Admin(s) of the selected departments.
Notify Code Signing RAO Admin(s) ***(required)***	Check-box	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)***	Check-box	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 email address(es) of other people to whom the notifications are to be sent.

Important Note: The 'Domain Awaiting Approval' notification will be sent to Master Administrator only after the requested domain is approved by RAO.

6.6.2.20 '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 on final approval of a requested domain by Master Administrator(s).



Create Notification ✕

*-required fields

Notification Type	Domain Approved ▾
Description*	ⓘ
Organization/Department*	

Organization	Department
□ ▾	☑ ▾ □ *Any*
□ ABCD Corporation	⊟ Dithers Construction Company
□ Best Organization	☑ *None*
□ Capital Business	☑ Purchases Departement
☑ Dithers Construction Company	☑ Stores Department

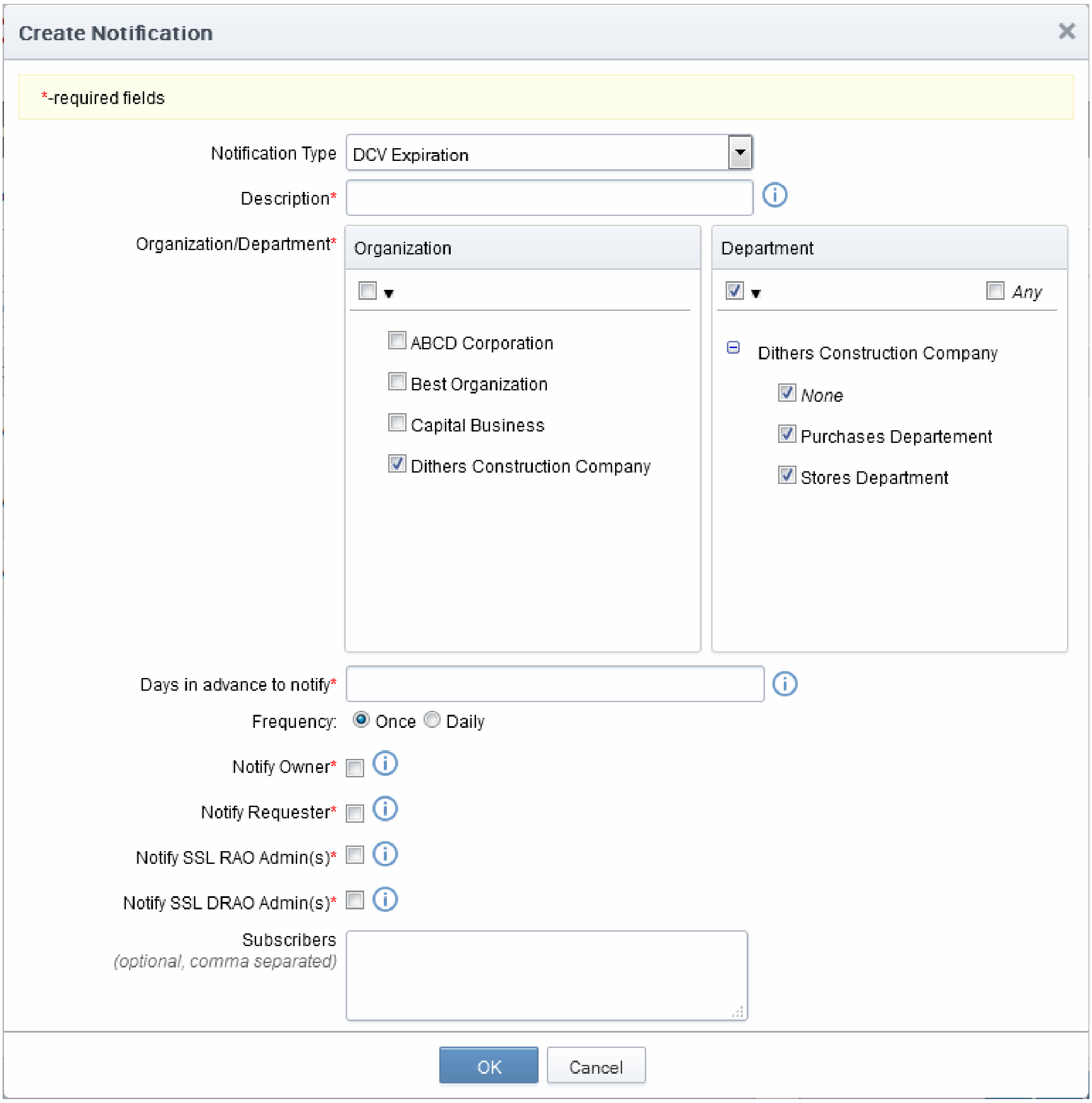
Notify Requester*	□ ⓘ
Notify SSL RAO Admin(s)*	□ ⓘ
Notify SSL DRAO Admin(s)*	□ ⓘ
Notify Client Certificate RAO Admin(s)*	□ ⓘ
Notify Client Certificate DRAO Admin(s)*	□ ⓘ
Notify Code Signing RAO Admin(s)*	□ ⓘ
Notify Code Signing DRAO Admin(s)*	□ ⓘ
Subscribers *(optional, comma separated)*	

6.6.2.20.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification to the person who requested the delegation of a created domain to an organization/department.
Notify SSL RAO Admin(s) ***(required)***	Check-box	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)***	Check-box	Enables the administrator to set the notification all the DRAO SSL Admin(s) of the selected departments.
Notify Client Certificate RAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification all the RAO S/MIME Admin(s) of the selected organization(s)/departments.
Notify Client Certificate DRAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification all the DRAO S/MIME Admin(s) of the selected departments.
Notify Code Signing RAO Admin(s) ***(required)***	Check-box	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)***	Check-box	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 email address(es) of other people to whom the notifications are to be sent.

6.6.2.21 'DCV Expiration' Create Notification Form

Enables administrator to set notification about expiration of domain control validation if it is due to expire.



Create Notification ✕

*-required fields

Notification Type: DCV Expiration

Description*:

Organization/Department*:

Organization	Department
□ ▾	☑ ▾ □ *Any*
□ ABCD Corporation	⊟ Dithers Construction Company
□ Best Organization	☑ *None*
□ Capital Business	☑ Purchases Departement
☑ Dithers Construction Company	☑ Stores Department

Days in advance to notify*:

Frequency: ● Once ○ Daily

Notify Owner* □

Notify Requester* □

Notify SSL RAO Admin(s)* □

Notify SSL DRAO Admin(s)* □

Subscribers *(optional, comma separated)*:

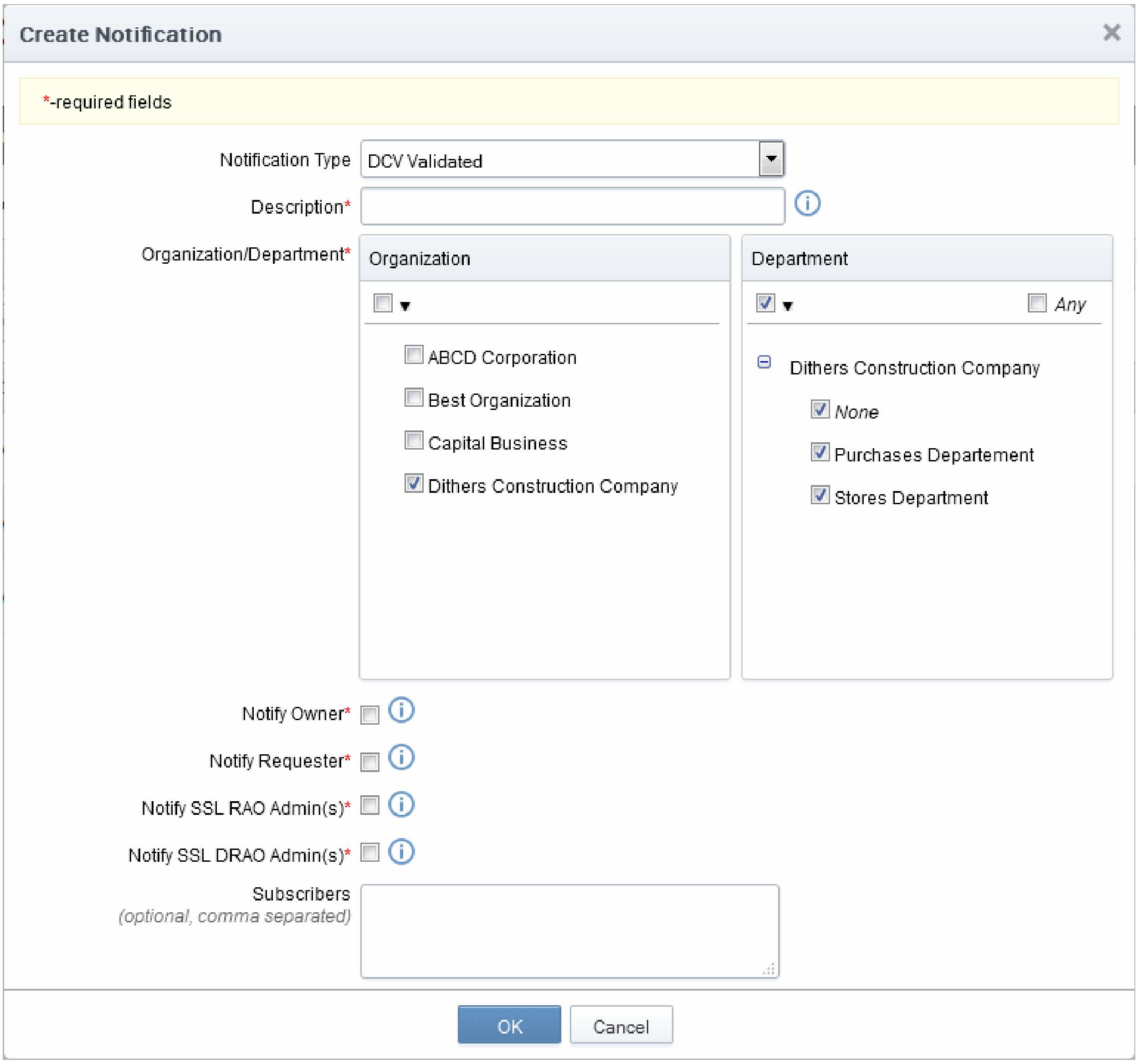
6.6.2.21.1 Table of Parameters

Form Element	Type	Description
Description *(required)*	Text Field	Provide a short description for the notification
Organization/Department *(required)*	Check boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
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)***	Check-box	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification to the person who requested the delegation of a created domain to an Organization/Department.
Notify SSL RAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification all the RAO Code Signing Admin(s) of the selected organization(s)/departments.
Notify SSL DRAO Admin(s) ***(required)***	Check-box	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 email address(es) of other people to whom the notifications are to be sent.

6.6.2.22 '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).



Create Notification

*-required fields

Notification Type: DCV Validated

Description*:

Organization/Department*:

Organization	Department
□ ▾	☑ ▾ □ *Any*
□ ABCD Corporation	⊟ Dithers Construction Company
□ Best Organization	☑ *None*
□ Capital Business	☑ Purchases Departement
☑ Dithers Construction Company	☑ Stores Department

Notify Owner* □

Notify Requester* □

Notify SSL RAO Admin(s)* □

Notify SSL DRAO Admin(s)* □

Subscribers *(optional, comma separated)*

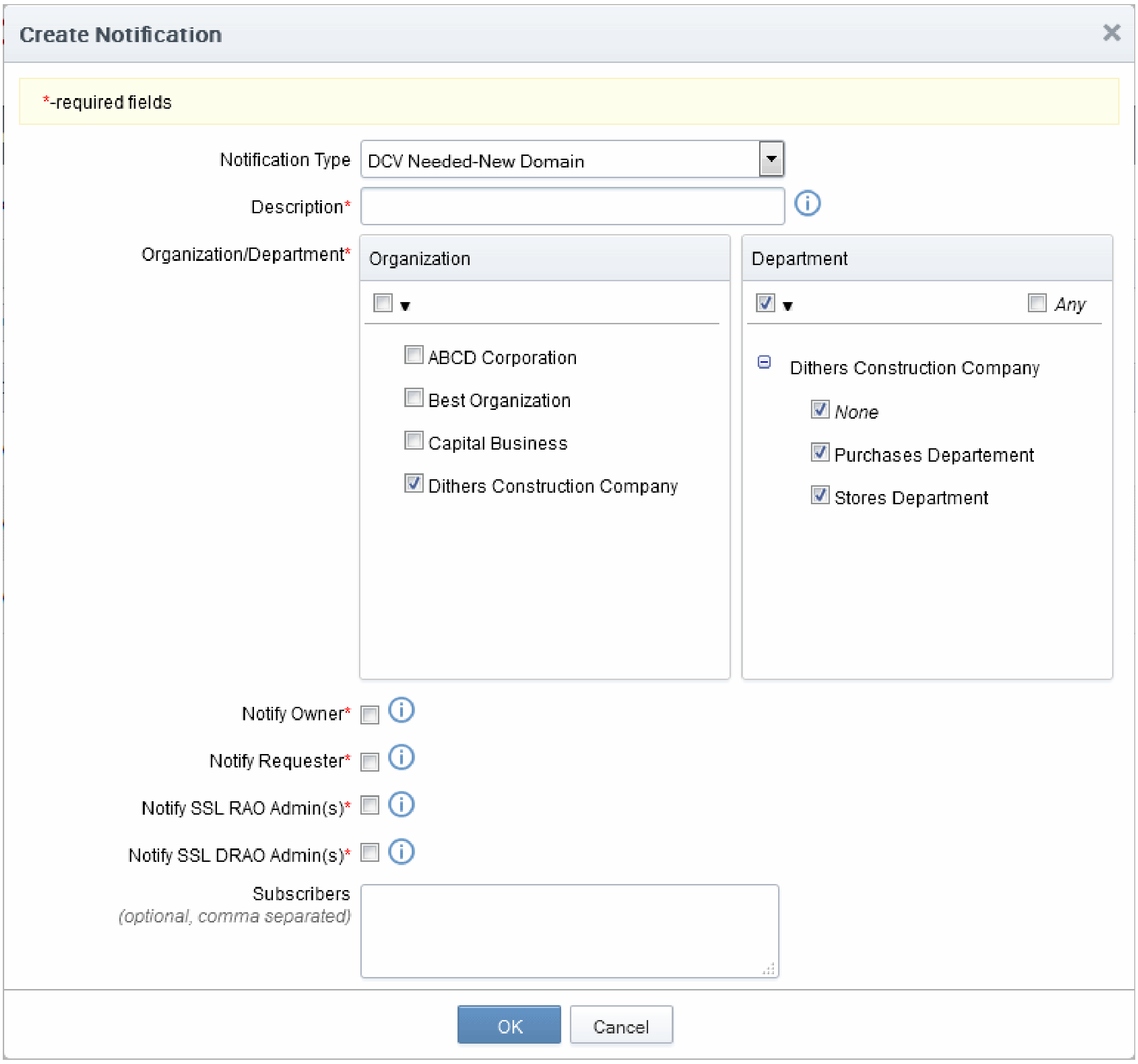
6.6.2.22.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Notify Owner ***(required)***	Check-box	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification to the person who

		requested the delegation of a created domain to an Organization/Department.
Notify SSL RAO Admin(s) ***(required)***	Check-box	Enables the administrator to set the notification all the RAO Code Signing Admin(s) of the selected organization(s)/departments.
Notify SSL DRAO Admin(s) ***(required)***	Check-box	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 email address(es) of other people to whom the notifications are to be sent.

6.6.2.23 '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.



Create Notification

*-required fields

Notification Type: DCV Needed-New Domain

Description*:

Organization/Department*:

Organization
- □ ABCD Corporation
- □ Best Organization
- □ Capital Business
- ☑ Dithers Construction Company

Department ☑ □ Any
- Dithers Construction Company
  - ☑ None
  - ☑ Purchases Departement
  - ☑ Stores Department

Notify Owner* □

Notify Requester* □

Notify SSL RAO Admin(s)* □

Notify SSL DRAO Admin(s)* □

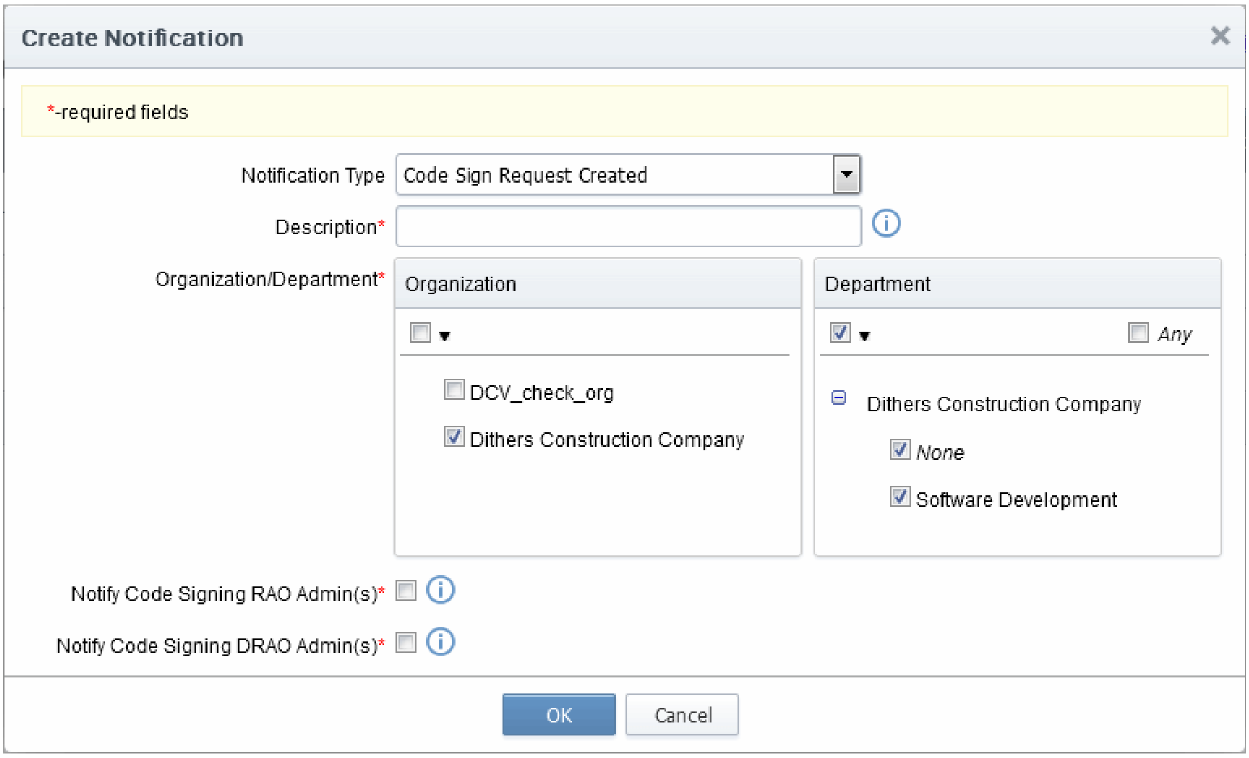
Subscribers (optional, comma separated):

6.6.2.23.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Check boxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
Notify Owner ***(required)***	Check-box	Enables the administrator to set the notification for the Owner of the certificate.
Notify Requester ***(required)***	Check-box	Enables the administrator to set the notification to the person who requested the delegation of a created domain to an Organization/Department.
Notify SSL RAO Admin(s) ***(required)***	Check-box	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)***	Check-box	Enables the administrator to set the notification all the DRAO SSL Admin(s) of the selected Departments.
Subscribers (***optional***)	Text Field	Administrator can specify email address(es) of other people to whom the notifications are to be sent.

6.6.2.24 'Code Sign Request Created' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel when a 'Code Signing on Demand' request has been created by a developer for a software.



Create Notification

*-required fields

Notification Type: Code Sign Request Created

Description*

Organization/Department*

Organization	Department
□ ▾	☑ ▾ □ *Any*
□ DCV_check_org	⊟ Dithers Construction Company
☑ Dithers Construction Company	☑ *None*
	☑ Software Development

Notify Code Signing RAO Admin(s)* □

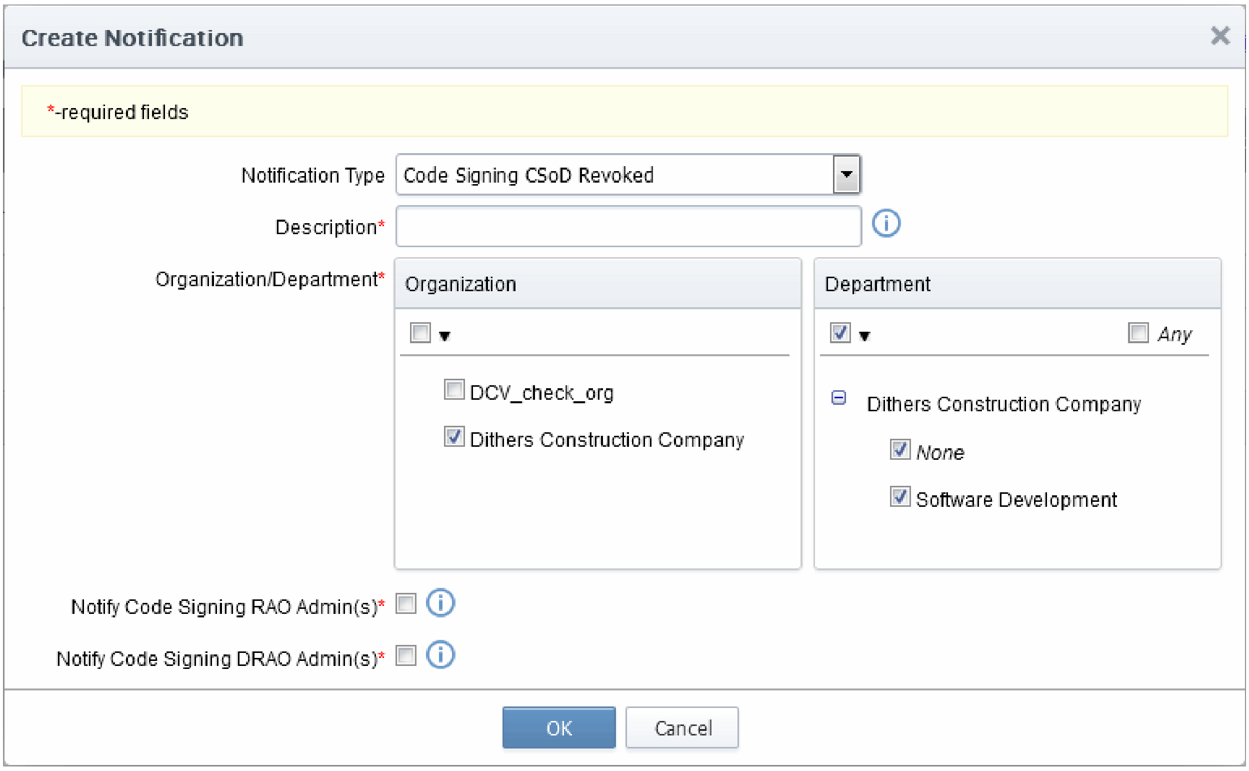
Notify Code Signing DRAO Admin(s)* □

6.6.2.24.1 Table of Parameters

Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Checkboxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
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.

6.6.2.25 Code Signing CSoD Revoked Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel when a 'Code Signing on Demand' request has been revoked by an administrator.



Create Notification

*-required fields

Notification Type: Code Signing CSoD Revoked

Description*:

Organization/Department*:

Organization	Department
□ ▾	☑ ▾ □ *Any*
□ DCV_check_org	⊟ Dithers Construction Company
☑ Dithers Construction Company	☑ *None*
	☑ Software Development

Notify Code Signing RAO Admin(s)* □

Notify Code Signing DRAO Admin(s)* □

6.6.2.25.1 Table of Parameters

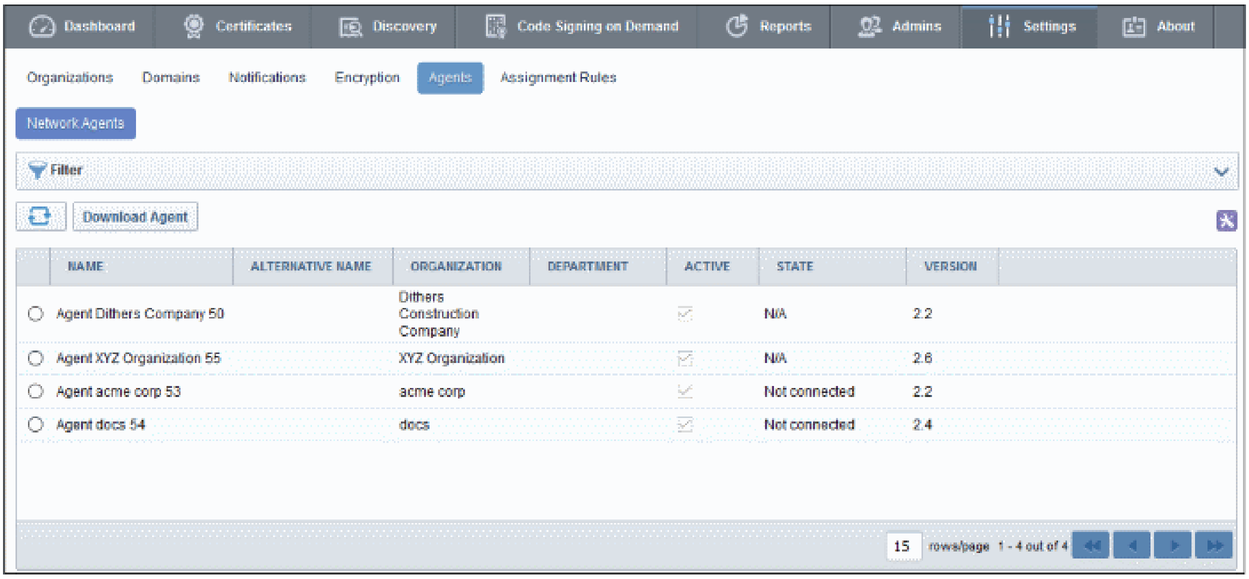
Form Element	Type	Description
Description ***(required)***	Text Field	Provide a short description for the notification
Organization/Department ***(required)***	Checkboxes	• Choose the organizations/departments which should receive the notification. • Select the check-box above the list to enable for all current organizations/departments. • Select the 'Any' check-box to enable the notification for all current organizations/departments and any that get added in the future.
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.

6.7 Incommon CM Agents

Incommon CM network agents allow you to automate various processes such as certificate discovery and certificate installation. The Network Agent (a.k.a Certificate Controller) does the following tasks:

- Certificate discovery on networks (only SSL web-server certs)
- Auto-request and installation of SSL certificates. There are two way to do this:
  - Enterprise Controller Mode – The 'Network agent' is installed on a single host which will communicate with your web-servers and will automatically request and install certificates on them.
  - Incommon CM Controller Mode – The 'Network agent' is installed on each web server for which certificate auto-nstallation and renewal is required.

To open the 'Agents' interface, click 'Settings' > 'Agents'



	NAME	ALTERNATIVE NAME	ORGANIZATION	DEPARTMENT	ACTIVE	STATE	VERSION
○	Agent Dithers Company 50		Dithers Construction Company		☑	N/A	2.2
○	Agent XYZ Organization 55		XYZ Organization		☑	N/A	2.6
○	Agent acme corp 53		acme corp		☑	Not connected	2.2
○	Agent docs 54		docs		☑	Not connected	2.4

Click the link below to find out more about:

- Network Agents for Certificate Discovery and Auto-Installation

6.7.1 Network Agents for Certificate Discovery and Auto-Installation

Incommon CM uses network agents for:

- **Automatic installation of certificates (on Apache Httpd, Apache, Tomcat and IIS 7. 7.5 and 8 and F5 BIG-IP only)** - An agent installed on a web server will periodically contact Incommon CM 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 Incommon CM interface. On approval, the agent submits the CSR to Incommon 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. A controller installed on a single server can be configured to communicate with, and install certificates on, other remote servers in the network.
- **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 Incommon CM to scan externally facing IP addresses directly from the 'Discovery Tasks' area (as explained in Discovery Tasks). However, Incommon CM can only scan internal hosts IF an agent which is configured to communicate with the Incommon CM servers is installed on the local network. After scanning the local network, the agent will send a report back to the Incommon CM console.

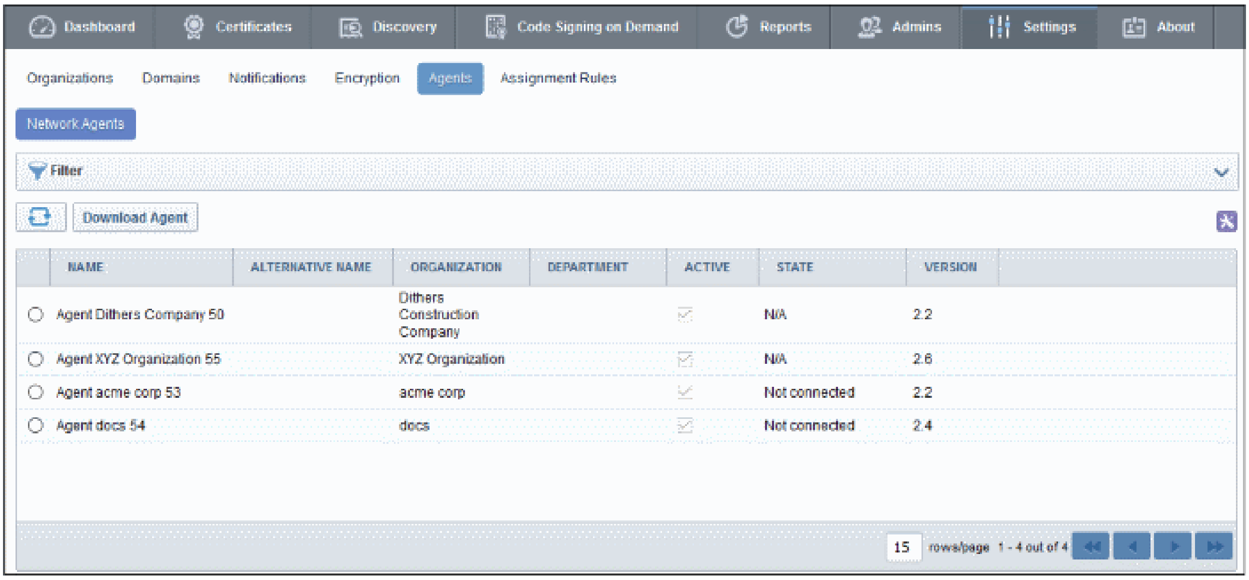
Note: The 'auto-installer' feature must be enabled for your account in order for it to execute certificate installation tasks.

If this feature is not enabled then the agent will only be capable of certificate discovery. Please contact your account manager if you require auto-installation to be enabled.

Security Roles:

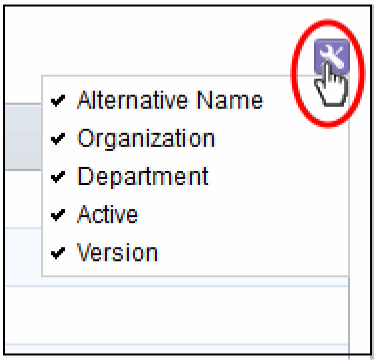
- RAO - Can set up Certificate Controller agent for installing certificates and scanning internal servers of Organizations (and any sub-ordinate departments) that have been delegated to them, for certificates requested, issued, expired, revoked and replaced.
- DRAO - Can set up Certificate Controller 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 Network Agents Interface:



	NAME	ALTERNATIVE NAME	ORGANIZATION	DEPARTMENT	ACTIVE	STATE	VERSION
○	Agent Dithers Company 50		Dithers Construction Company		✓	N/A	2.2
○	Agent XYZ Organization 55		XYZ Organization		✓	N/A	2.6
○	Agent acme corp 53		acme corp		✓	Not connected	2.2
○	Agent docs 54		docs		✓	Not connected	2.4

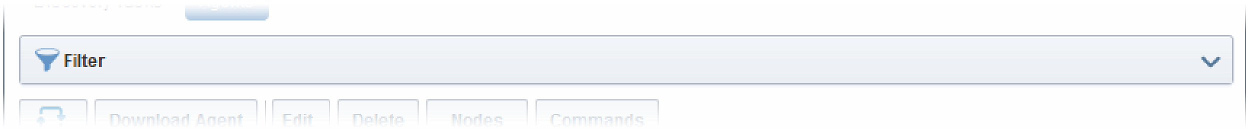
Column Display	Description
Name	Displays the name specified for the Certificate Controller agent.
Alternative Name	Displays the alternative name specified for the Certificate Controller agent.
Organization	Displays the Organization to which the Certificate Controller Agent is associated.
Department	Displays 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 Incommon CM.
Version	Displays the version number of the Certificate Controller agent.
Note: The administrator can enable or disable the columns as desired, from the drop-down button at the right end of the table header.	

 ✔ Alternative Name ✔ Organization ✔ Department ✔ Active ✔ Version		
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.

6.7.1.1 Sorting and Filtering Options

- Click the column headers to sort items in alphabetical order of the entries in the column.

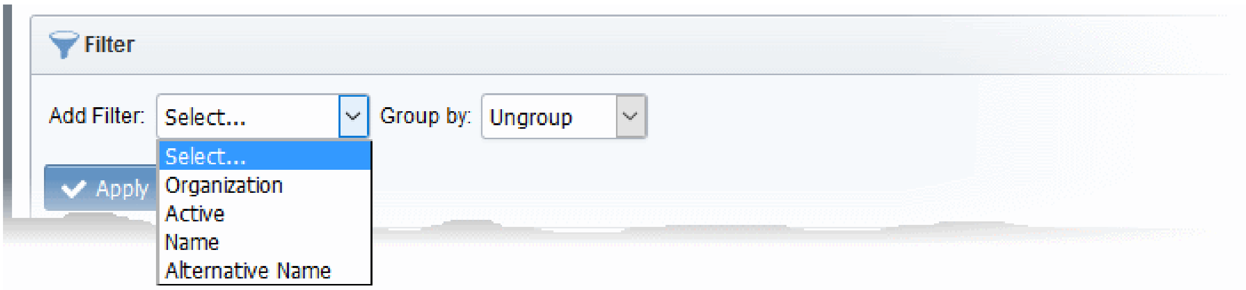
Administrators can search for a particular agent by using the filter.



You can apply filters and select grouping options using the drop-down menus above the table.

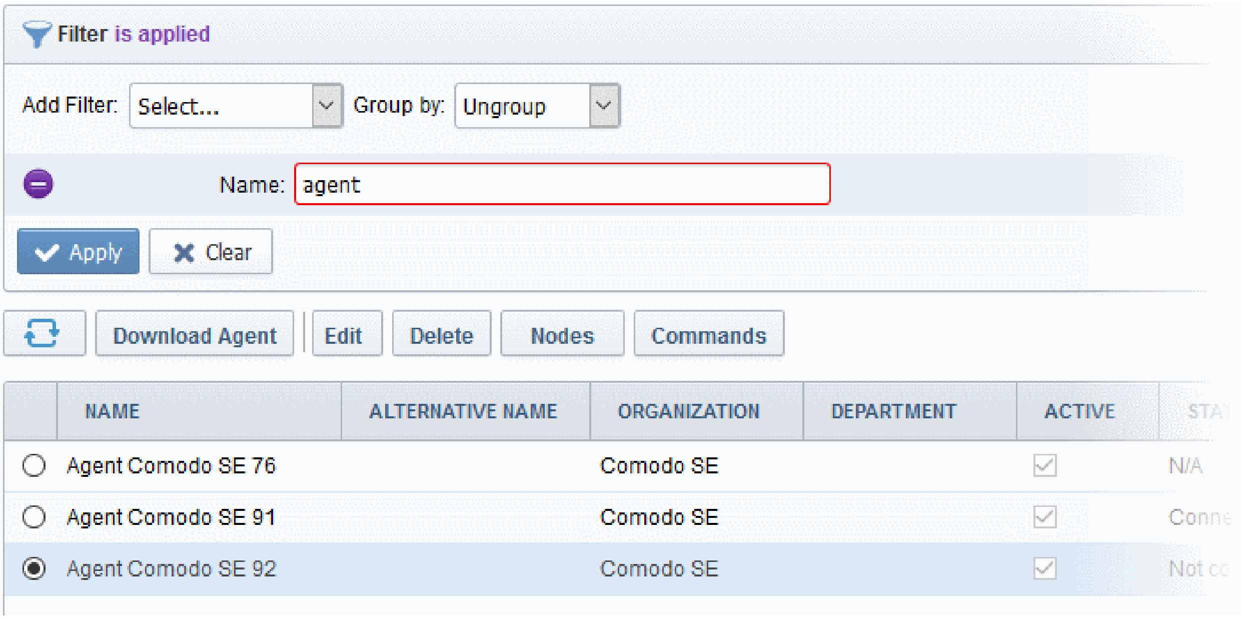
Filter Options	Description
Organization	Filter the list of agents by organization.
Active	View only active agents.
Name	Type the name of the agent you wish to locate.
Alternative Name	Filter agents by alternative name.

For example if you want to search for an agent by the name filter and belonging to a particular organization and Department:



- Choose 'Name' from the 'Add Filter' drop-down and enter the name of the agent in full or part.
- 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:



Name: agent

	NAME	ALTERNATIVE NAME	ORGANIZATION	DEPARTMENT	ACTIVE	STA
○	Agent Comodo SE 76		Comodo SE		☑	N/A
○	Agent Comodo SE 91		Comodo SE		☑	Conne
●	Agent Comodo SE 92		Comodo SE		☑	Not cc

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

Note: Search filters are automatically saved. The filters will still be in place when you reopen the 'Agents' interface in future. Click the 'Clear' button if you do not want the filters to be saved.

6.7.1.2 Configure the Agent for Auto-Installation and Internal Scanning - Overview of the Process

The following is a summary of the steps needed to set up a controller/agent for automatic certificate installation and for internal scanning.

Click any bullet to go to a more detailed explanation of that stage:

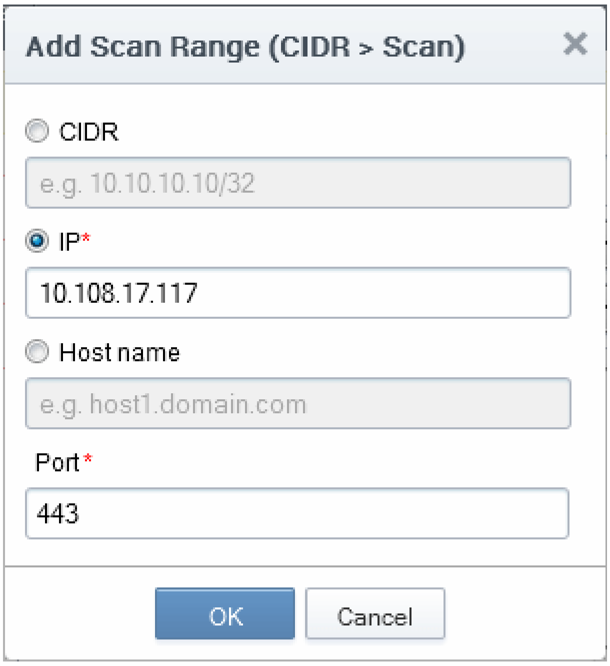
1. Add a new IP range for internal scans by creating a CIDR in the Net Discovery Tasks tab.
2. Download and install the agent on a server
3. Add CIDR ranges to the agent for certificate discovery and specify target servers for SSL auto-installation.
4. Return to the 'Net Discovery Tasks' tab and click 'Scan'.
5. **Results can be viewed by selecting 'Discovery Scan Log' under the 'Reports' tab. New certificates will be added to 'Certificates Management' > 'SSL Certificates'. They will be assigned to the organization that has been set for that agent.**

6.7.1.3 Prerequisites

The administrator has defined at least one 'Organization'. During setup, an organization needs to be designated as the owner of certificates discovered by the agent.

6.7.1.4 Configure 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 'Net 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.



Add Scan Range (CIDR > Scan)

○ CIDR

e.g. 10.10.10.10/32

● IP*

10.108.17.117

○ Host name

e.g. host1.domain.com

Port*

443

Note: Incommon CM is capable of scanning for installed certificates in external servers via Internet. If there is no agent installed in the server to be scanned, Incommon CM will request the user to install the agent.

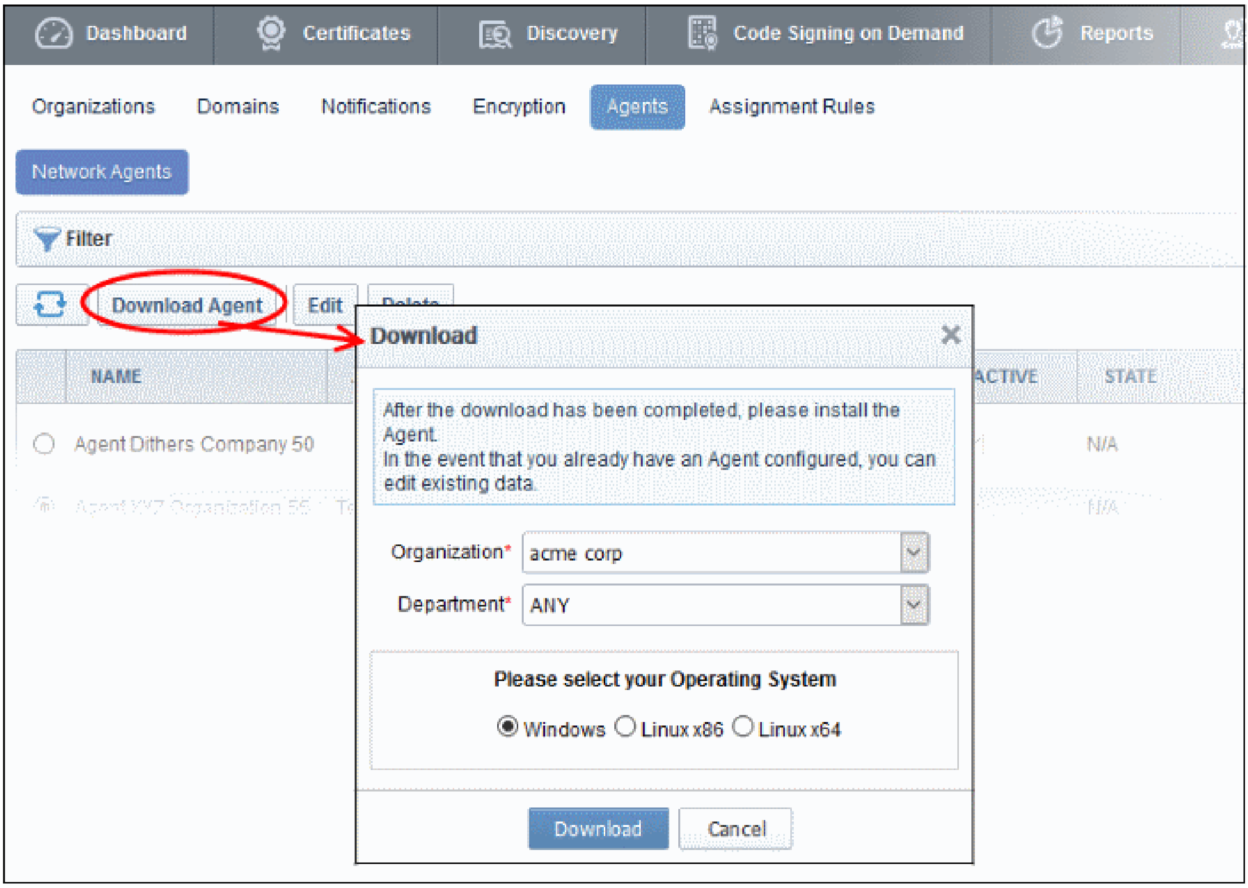
2. Download and Install the agent on a server in the network.

Note:

- The 'Network Agent' is also responsible for automatic application and installation of SSL certificates.
- An agent installed on one server can be configured to install certificates on other web servers in the network.
- The important aspect is that the all the servers should be able to connect to Incommon CM.

To download the agent setup file:

- Click 'Settings' >'Agents' > 'Network Agents' then 'Download Agent':



After the download has been completed, please install the Agent.
In the event that you already have an Agent configured, you can edit existing data.

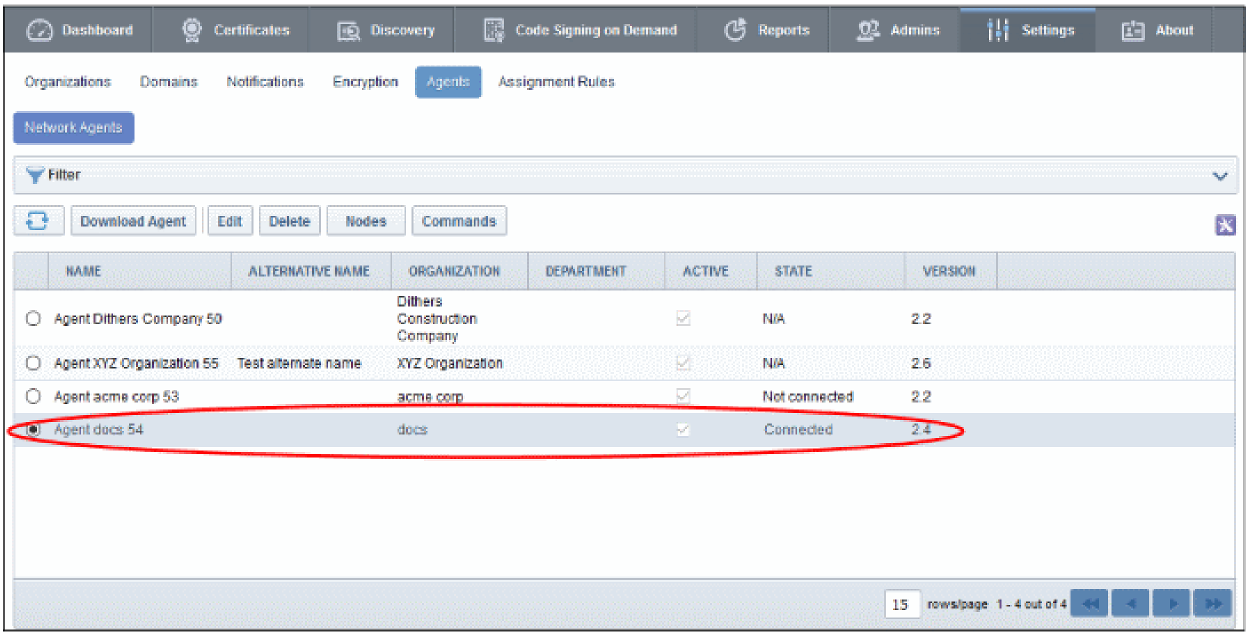
Organization* acme corp

Department* ANY

Please select your Operating System

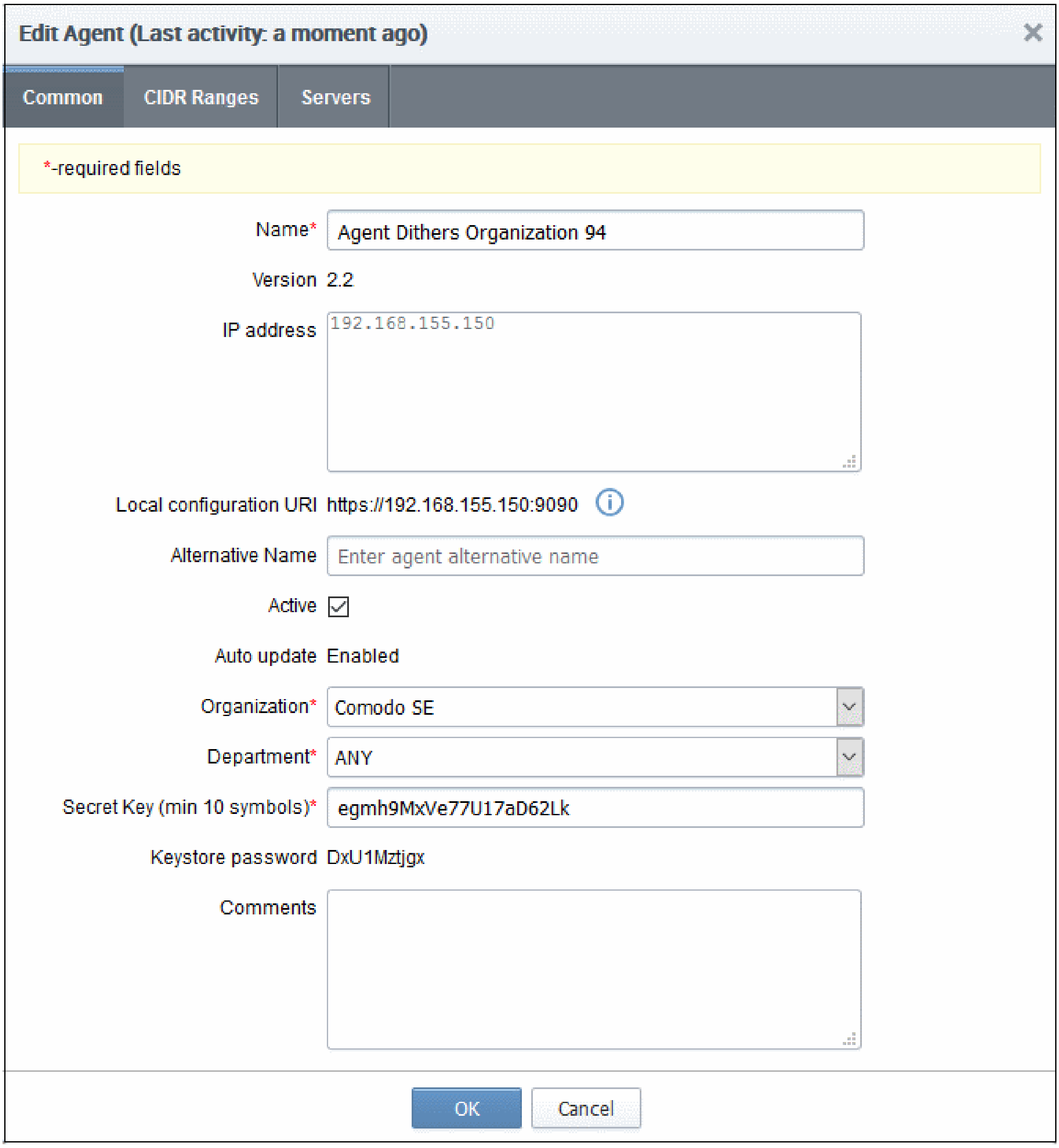
● Windows ○ Linux x86 ○ Linux x64

- Select the organization/department to which you want to assign certificates discovered by the agent.
- Choose the version of the agent appropriate for your server's operating system.
- Click 'Download' and 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' then follow the setup instructions. If you are installing the Linux version of the agent, run the installation from the command line.
- The agent will be added to the Incommon CM interface when installation is complete:



	NAME	ALTERNATIVE NAME	ORGANIZATION	DEPARTMENT	ACTIVE	STATE	VERSION
○	Agent Dithers Company 50		Dithers Construction Company		✓	N/A	2.2
○	Agent XYZ Organization 55	Test alternate name	XYZ Organization		✓	N/A	2.6
○	Agent acme corp 53		acme corp		✓	Not connected	2.2
●	Agent docs 54		docs		✓	Connected	2.4

- The next step is to configure the agent to:
  - Apply for and install SSL certificates on local servers
  - Apply for and install SSL certificates on remote servers
  - Scan internal networks. This is done by linking the agent to the CIDR created in the 'Discovery' tab.
- Select an agent then click the 'Edit' button to modify agent properties:



Edit Agent (Last activity: a moment ago)

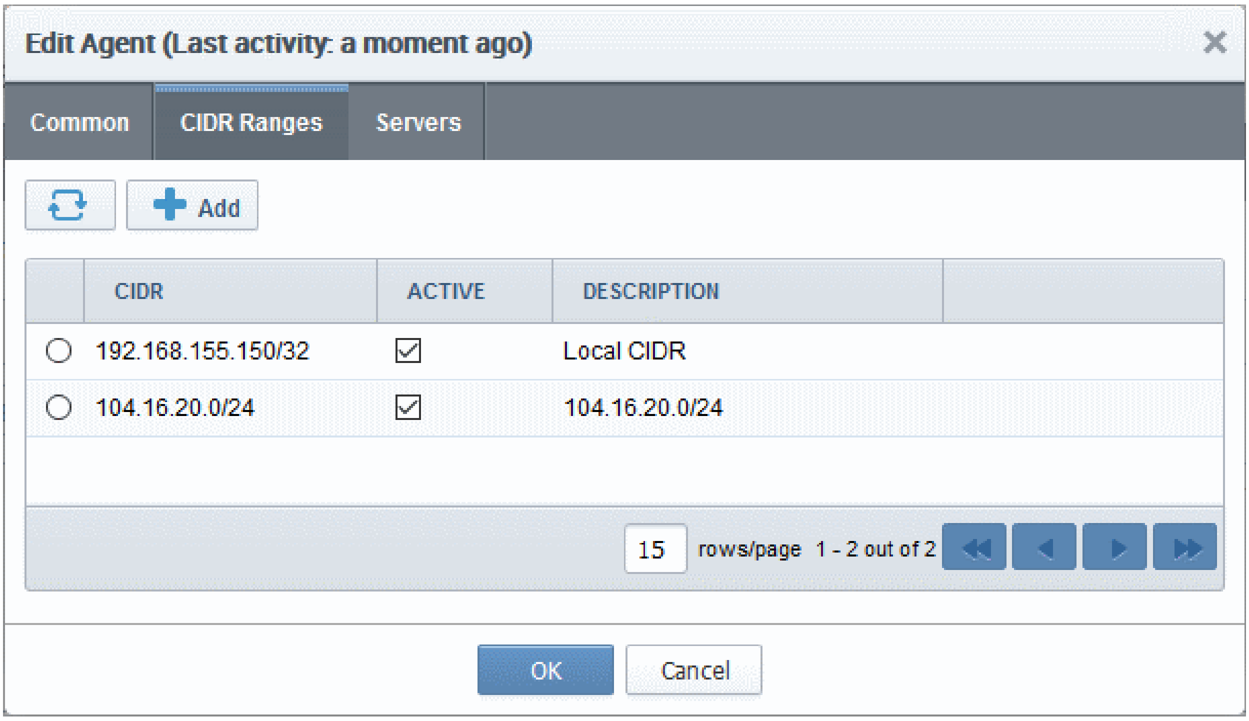
*-required fields

Name*	Agent Dithers Organization 94
Version	2.2
IP address	192.168.155.150
Local configuration URI	https://192.168.155.150:9090
Alternative Name	Enter agent alternative name
Active	☑
Auto update	Enabled
Organization*	Comodo SE
Department*	ANY
Secret Key (min 10 symbols)*	egmh9MxVe77U17aD62Lk
Keystore password	DxU1Mztjgx
Comments	

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		Displays the version number of the Agent.
IP Address		Displays the IPv6 Loopback address, IPv4 loopback address, IPV6 IP Address, IPv4 IP Address or the physical address of the server on which the agent is installed

Local Configuration URI		• Displays the IP of the server on which the agent is installed. • This URL is used to access the agent via a web browser for managing. See Configuring the Certificate Controller Agent through Web Interface for more details.
Alternative Name	String	Provide a brief description of the agent.
Active	Checkbox	Enable or disable the agent
Auto update	String	Indicates whether the agent is enabled for auto update
Organization	Drop-down list	Enables the Administrator to change the organization associated the agent.
Department	Drop-down list	Enables the Administrator to change the department associated with the agent.
Secret Key	String	• A unique identifier to authenticate the agent to Incommon CM. The secret key must have 10 characters or more. • Please save the secret key in a safe location. The key is required if you need to reinstall the agent.
Keystore password	String	• Password to access keys stored by this agent in the private key store. • The network agent stores the certificates and private keys in a JKS file (java keystore) on the agent. This password allows you to extract the certificates and private keys from the keystore if required.
Comments	String	Type any notes about the agent.

- Edit the values as required. To edit the CIDR ranges, click the 'CIDR Ranges' tab. The CIDR Ranges tab will open.

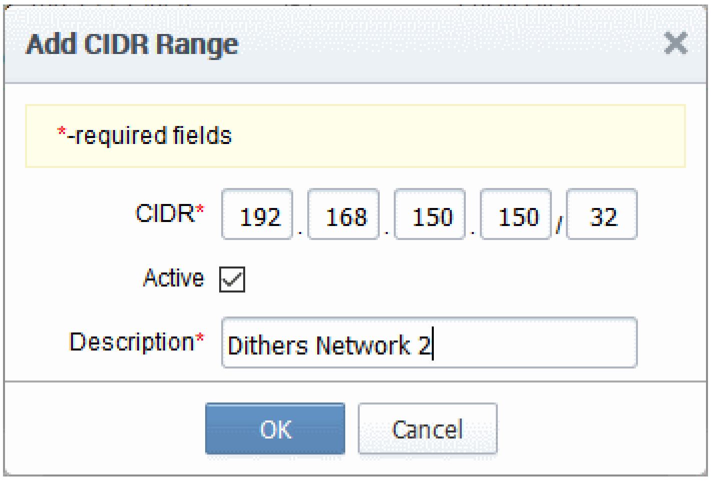


Edit Agent (Last activity: a moment ago)

	CIDR	ACTIVE	DESCRIPTION
○	192.168.155.150/32	☑	Local CIDR
○	104.16.20.0/24	☑	104.16.20.0/24

15 rows/page 1 - 2 out of 2

3. To add a new CIDR range, click 'Add'. The 'Add CIDR Range' dialog will open.



Add CIDR Range

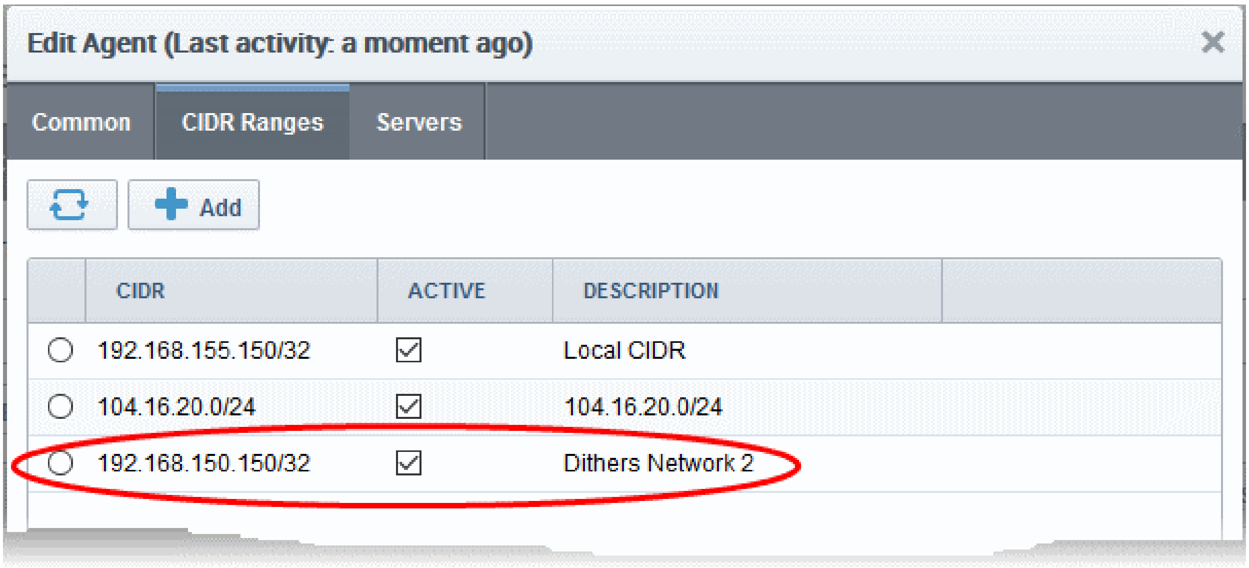
*-required fields

CIDR* 192 . 168 . 150 . 150 / 32

Active ☑

Description* Dithers Network 2

- Enter the internal IP address range you want to scan and type a description for the range. The agent must be 'Active' in order to run scans. The new CIDR Range will be added to the 'CIDR Ranges' area:

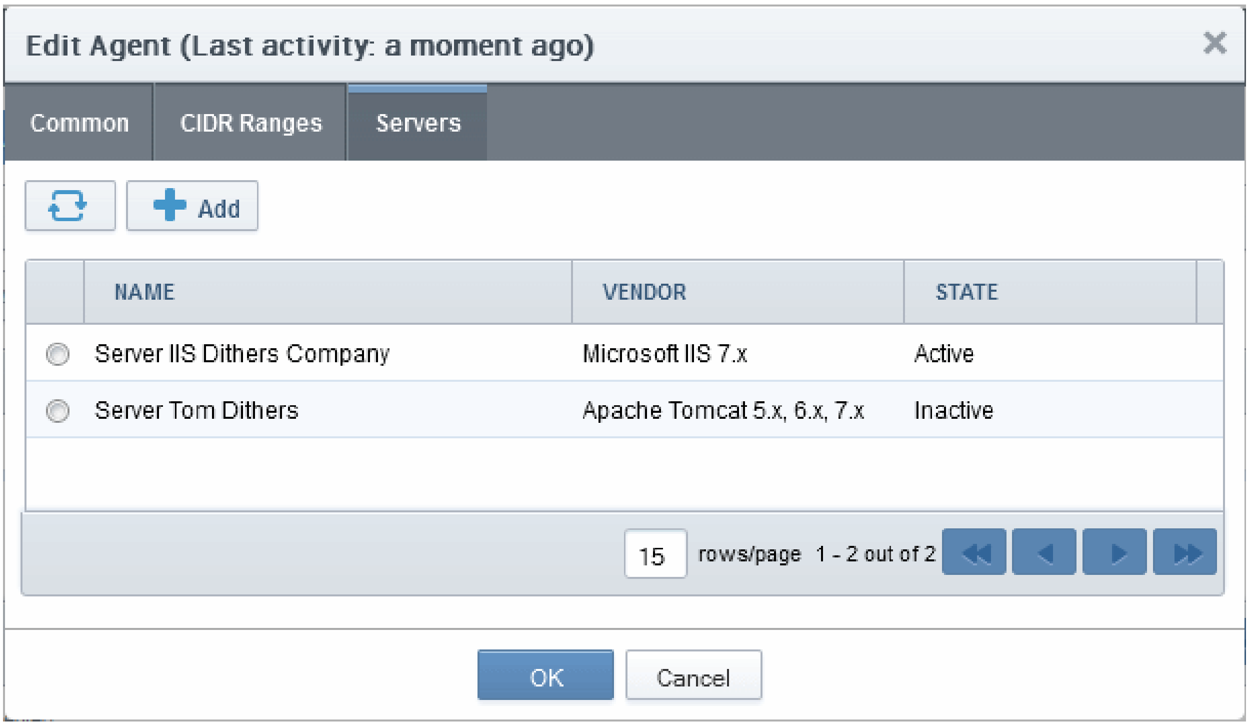


Edit Agent (Last activity: a moment ago)

	CIDR	ACTIVE	DESCRIPTION
○	192.168.155.150/32	☑	Local CIDR
○	104.16.20.0/24	☑	104.16.20.0/24
○	192.168.150.150/32	☑	Dithers Network 2

You can add as many ranges as you want by repeating the same procedure.

- To edit a range, select it and click the 'Edit' button. The Edit CIDR Range dialog will open.
- To delete a range, select it and click the 'Delete' button.
- Click the 'Servers' tab to configure servers for certificate auto-installation and scans.



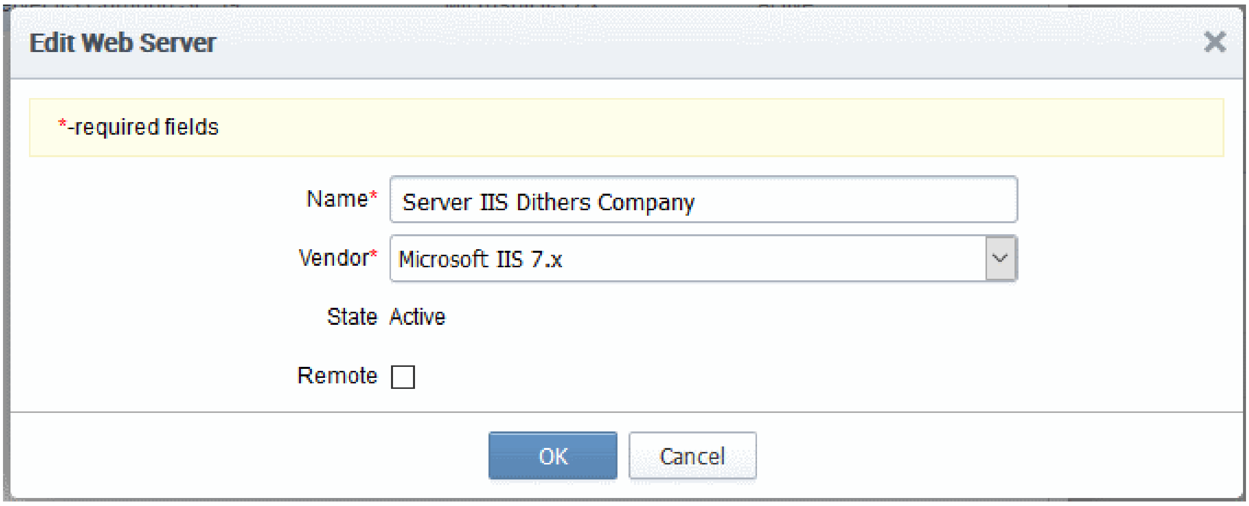
Edit Agent (Last activity: a moment ago)

	NAME	VENDOR	STATE
○	Server IIS Dithers Company	Microsoft IIS 7.x	Active
○	Server Tom Dithers	Apache Tomcat 5.x, 6.x, 7.x	Inactive

15 rows/page 1 - 2 out of 2

The 'Servers' tab shows all servers configured for certificate auto-installation using this agent. The agent automatically adds the server upon which it is installed to this list.

You can edit the properties of the server by selecting it and clicking the Edit button from the top.



Edit Web Server

*-required fields

Name* Server IIS Dithers Company

Vendor* Microsoft IIS 7.x

State Active

Remote □

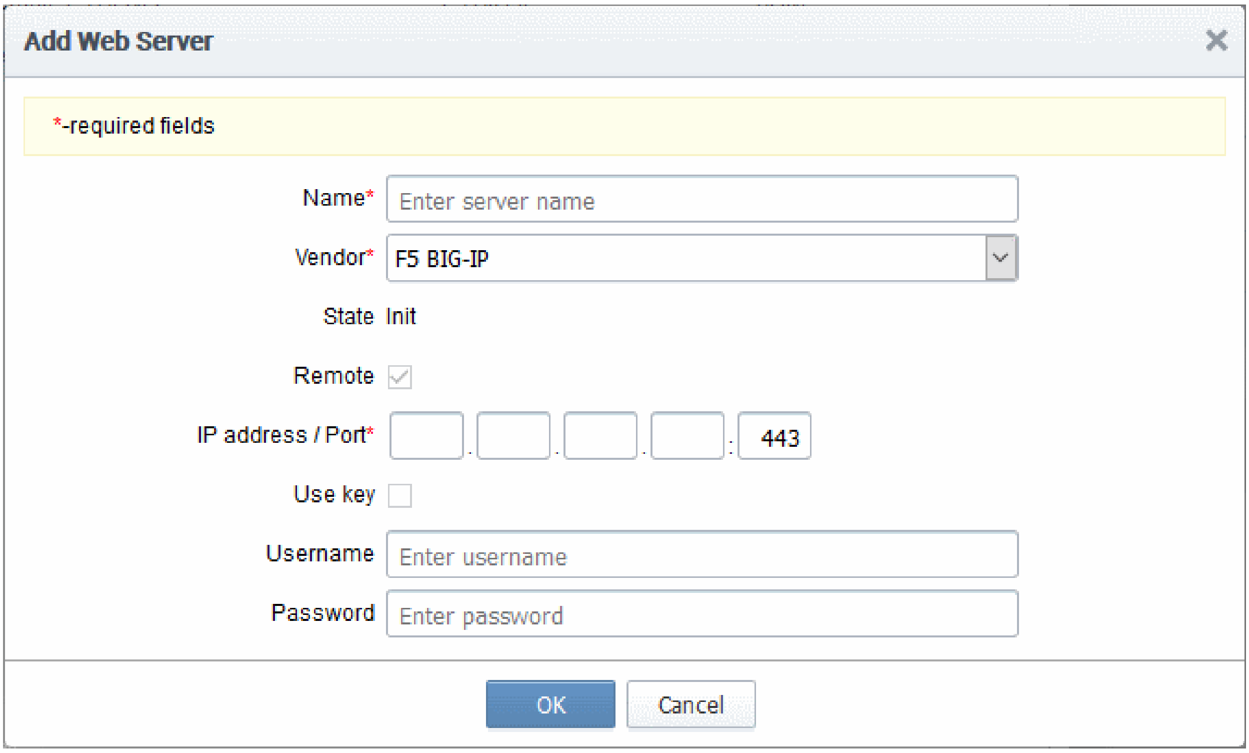
Edit Web Server - Table of Parameters		
Field Name	**Type**	**Description**
Name	String	Enables the Administrator to edit the name of the Server.
Vendor	Drop-down list	Enables the Administrator to select the vendor of the server.
Path to web server	String	Enables the Administrator to specify the network path for Apache. This is required only if Apache server is not accessible from the Incommon CM console.
State		Indicates whether or not the server is connected to Incommon CM.
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.

Configure 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 Incommon CM 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 Incommon CM interface. On approval, the agent will submit the CSR to Incommon 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 Incommon CM interface.

To add a remote server to the agent

- Select the agent then click the 'Edit' button. 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 Server

*-required fields

Name* Enter server name

Vendor* F5 BIG-IP

State Init

Remote ☑

IP address / Port* . . . : 443

Use key □

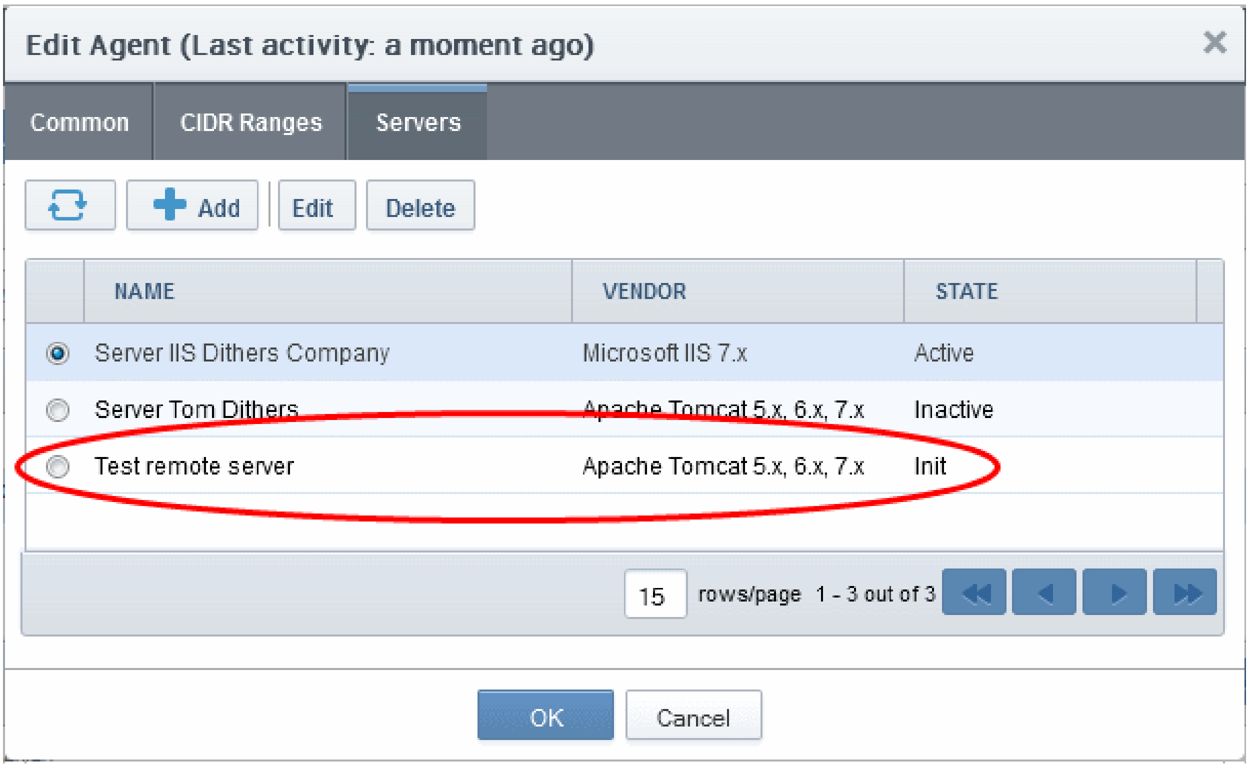
Username Enter username

Password Enter password

Add Web Servers - Table of Parameters		
Field Name	**Type**	**Description**
Name	String	Enter the host name of the server.
Vendor	Drop-down	Select the web-server type. Supported server types are: • Microsoft IIS • Apache 2.x • Tomcat • F5 BIG-IP **Note**: Agents installed on a Windows server will only support IIS and F5 BIG-IP web-server types. Agents installed on a Linux server support all types (Apache, Tomcat, IIS and F5). Click here for more details.
State		Indicates whether or not the server is connected. The connection will be automatically initialized and become active, once the agent starts communicating with it.
Path to web server	String	Specify the network path of the server. Required only for Tomcat under Linux.
Remote	Checkbox	Specify whether the server is remote or local. This checkbox should be selected when adding remote servers for agent-less automatic certificate installation.
IP Address / Port	String	Specify the IP address and connection port of the server for remote

		connection. Note: This field will be enabled only if 'Remote' is selected.
Use key	Checkbox	Specify whether the agent should use SSH Key-Based Authentication to access the server. Applicable only for Apache and Tomcat server types installed on Linux platform.
User Name / Private Key File Path	String	• If 'Use key' is not selected, specify the admin username to log-into the server, in the 'Username' field. • If 'Use key' is selected, specify the path to the SSH private key file to access the server Note: This field will be enabled only if 'Remote' is selected.
Password / Passphrase	String	If 'Use key' is not selected, specify the admin password to log-into the server, in the 'Password' field. If 'Use key' is selected, specify the passphrase for the private key file. Note: This field will be enabled only if 'Remote' is selected.

- Enter the parameters and click OK.



Edit Agent (Last activity: a moment ago)

	NAME	VENDOR	STATE
●	Server IIS Dithers Company	Microsoft IIS 7.x	Active
○	Server Tom Dithers	Apache Tomcat 5.x, 6.x, 7.x	Inactive
○	Test remote server	Apache Tomcat 5.x, 6.x, 7.x	Init

15 rows/page 1 - 3 out of 3

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 change to 'Connected'.
- The agent is now configured to auto-install the certificates on the remote server and to scan the internal network.
- The agent authenticates itself to remote Incommon CM server via the secret key and awaits commands.
- The agent polls Incommon CM every minute for new instructions. For example, a 'Scan Now' instruction. When the 'Scan Now' button is clicked, Incommon CM will tell the agent which CIDRs to scan. The agent performs the 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. See Configuring the Certificate Controller Agent through Web Interface for more details.

- Go back to 'Discovery' tab > 'Net Discovery Tasks' and click 'Scan'. 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.
- 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' as per the assignment rules defined for the discovery task. If no assignment rule apply then all unmanaged certificates will be assigned to the organization/department 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.

6.8 Auto-Assignment Rules for Unmanaged Certificates

- Administrators can create rules to automatically assign 'Unmanaged' certificates found after a discovery scan to a specific organization or department.
- Assignment Rules will assign certificates to a particular entity based on one or more conditions set by the administrator.
- The rules can be applied while configuring Net Discovery Tasks, so that each Unmanaged certificate found by a Discovery Scan and satisfying conditions in any of the rules applied to the scan, will be automatically assigned to the respective organization(s)/department(s). See Certificate Discovery Tasks, for more details on configuring Discovery Scans.
- The 'Assignment Rules' interface allows the Administrators to create rules for use in Discovery Scans.

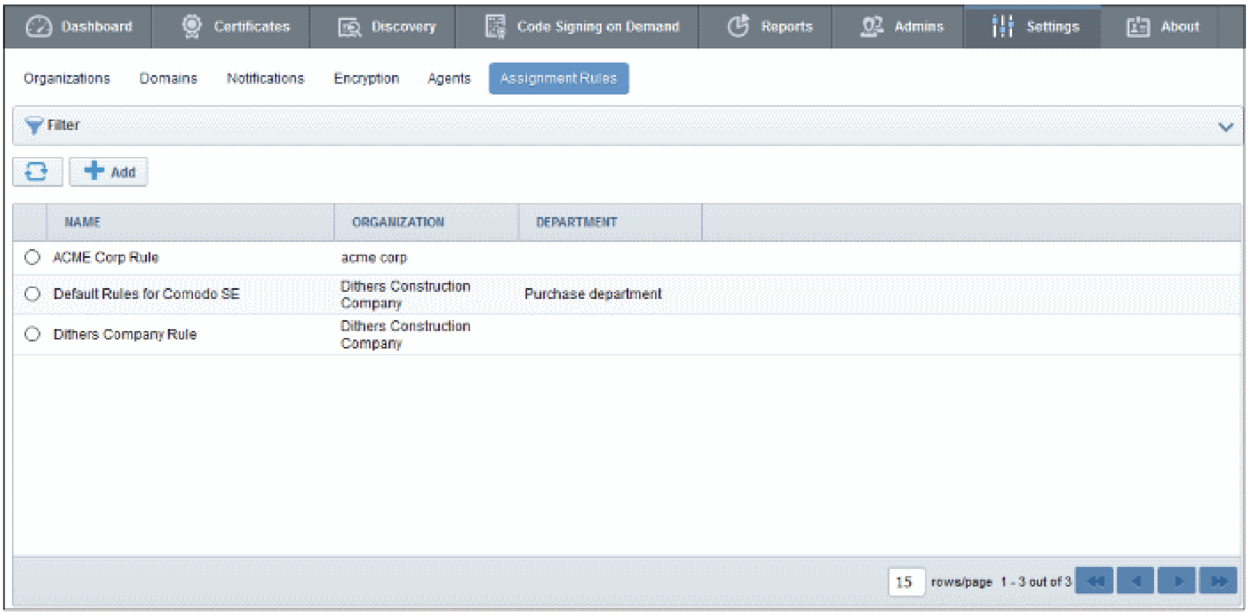
To open the 'Assignment Rules' interface:

- Click 'Settings' > 'Assignment Rules'

Security Roles:

- RAO - can create and manage rules to assign certificates discovered on their networks to organizations and sub-departments which have been delegated to them.
- DRAO - can create and manage rules to assign certificates discovered on their networks to Departments which have been delegated to them.

The 'Assignment Rules' interface displays a list of the available rules, allows administrators to create new rules and manage existing rules.



NAME	ORGANIZATION	DEPARTMENT
○ ACME Corp Rule	acme corp	
○ Default Rules for Comodo SE	Dithers Construction Company	Purchase department
○ Dithers Company Rule	Dithers Construction Company	

15 rows/page 1 - 3 out of 3

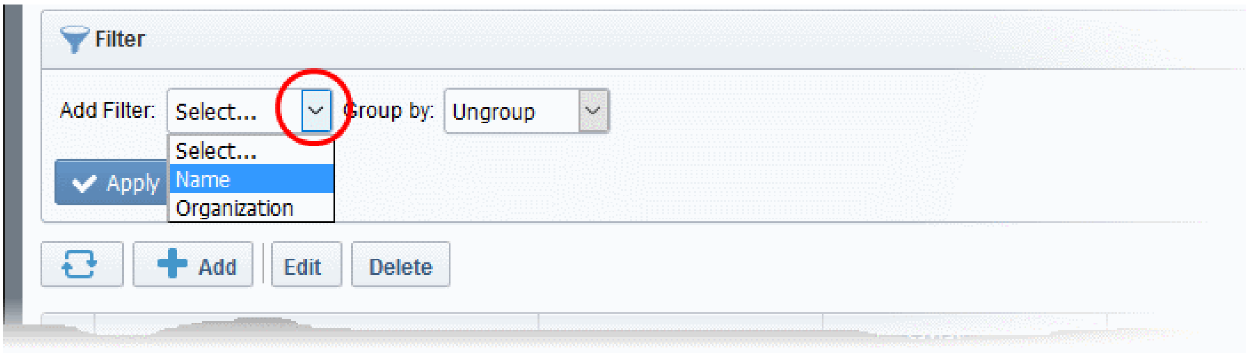
Assignment Rules - Table of Column Descriptions	
Column Header	**Description**
Name	Name of the unmanaged certificate assignment rule
Organization	Name of the organization to which the certificates matching the criteria specified in the rule will be auto-assigned.
Department	Name of the department to which the certificates matching the criteria specified in the rule will be auto-assigned.

Sorting and Filtering Options

- Clicking on a column headers 'Name', 'Organization' and 'Department' sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for a particular discovery task by using filter.

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.



Filter Criteria	Filter Parameter
Name	Enter the name of the rule in full or part
Organization	Select the organization and/or the department to which the certificate will be assigned as per the rule, from the 'Organization' and 'Department' drop-downs.

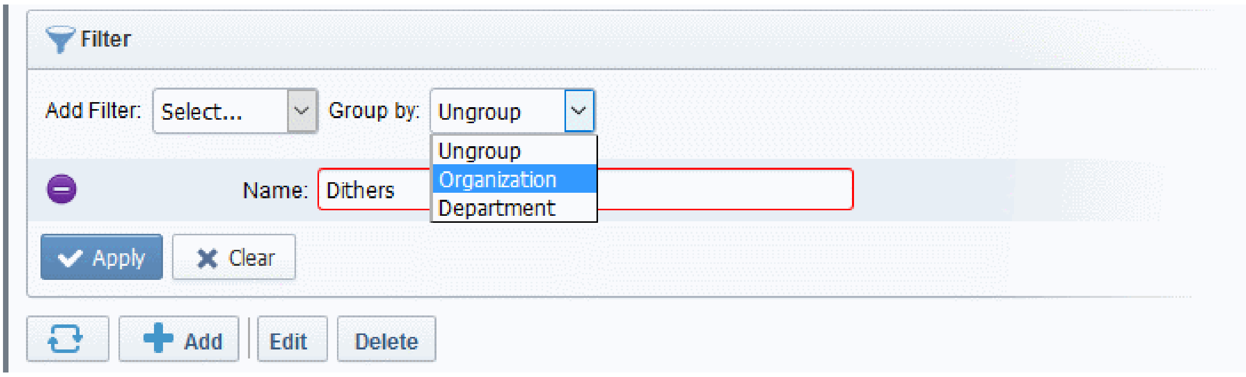
To add a filter

- Select a filter criteria from the 'Add Filter' drop-down
- Enter or select the filter parameter as per the selected criteria.

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 rules with a specific Common Name starting with 'Dithers' and group the results by 'Organizations/Departments', then select 'Name' from the 'Add Filter' drop-down, enter 'Dithers' 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.

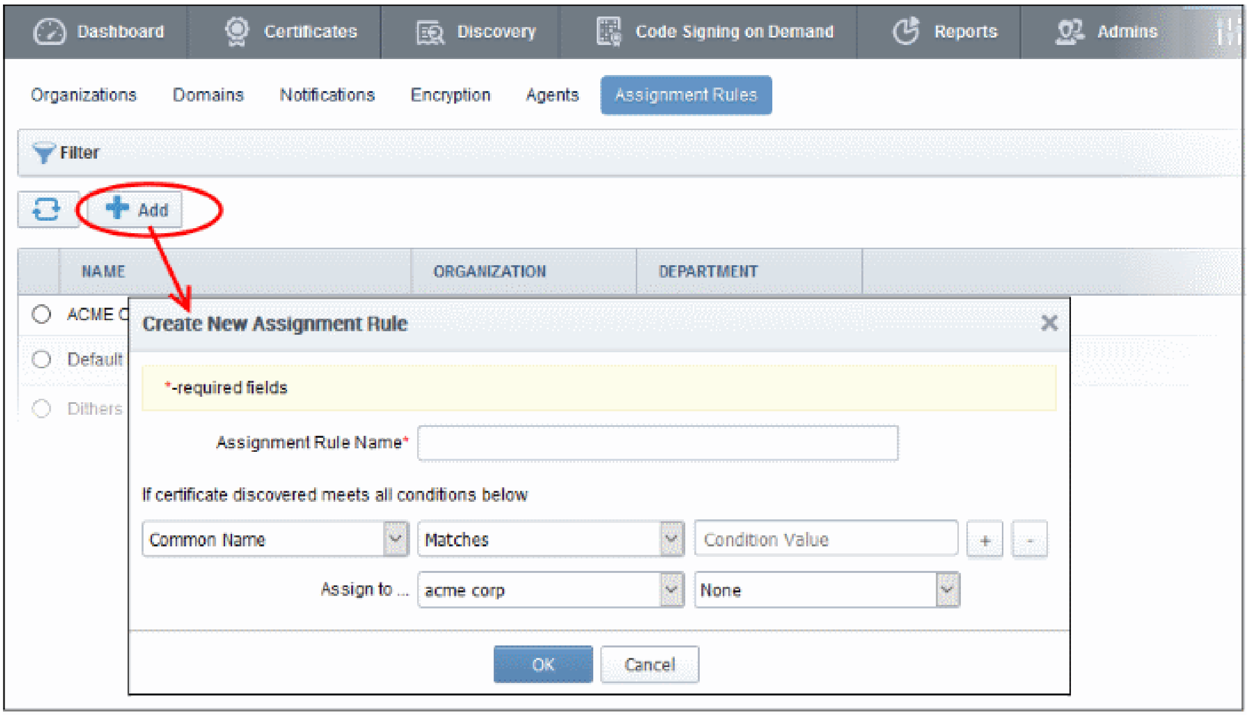
Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Assignment Rules' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear'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

Following sections explain in details about:

- Creating a new certificate assignment rule
- Editing an assignment rule

To create a new rule

- Click 'Add' from the 'Assignments Rules' interface



Create New Assignment Rule

*-required fields

Assignment Rule Name*

If certificate discovered meets all conditions below

Common Name | Matches | Condition Value

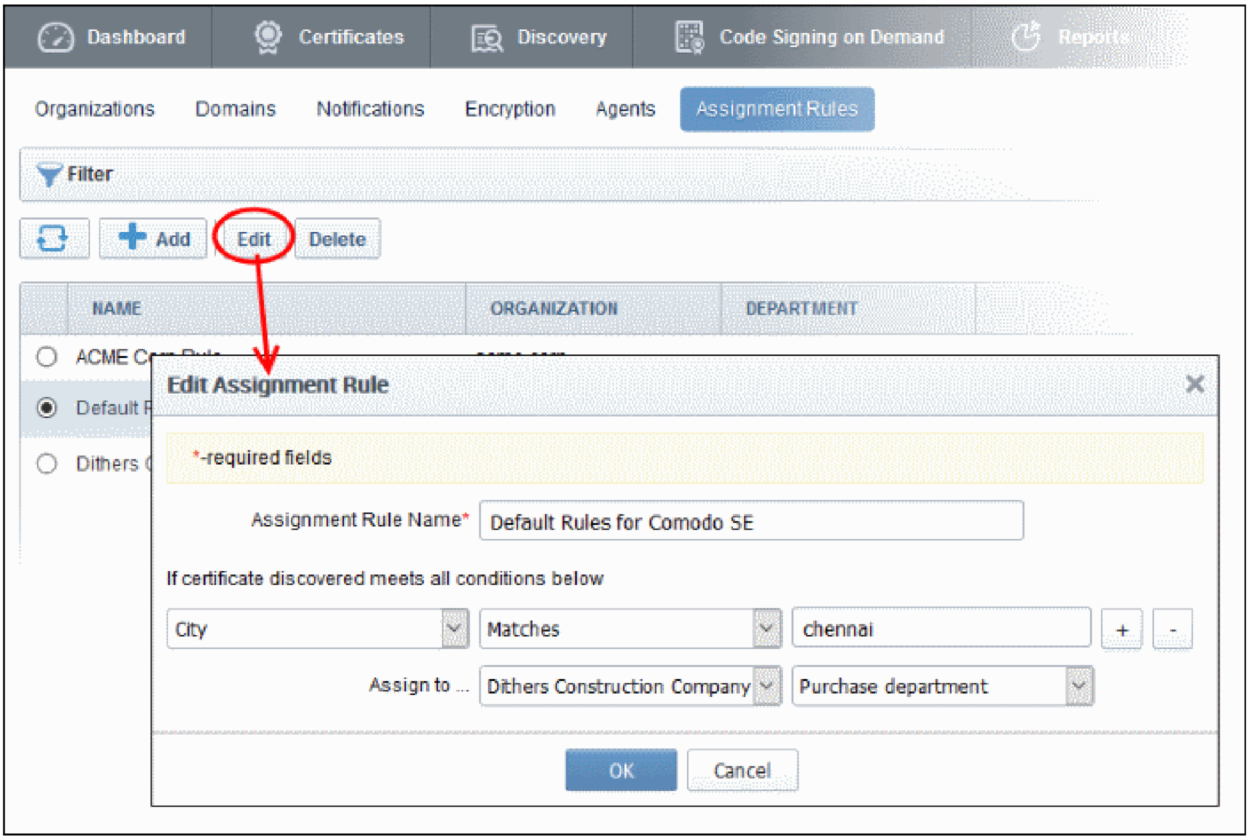
Assign to ... acme corp | None

- Enter a name shortly describing the rule in the Assignment Rule Name text box.
- Set the condition for identifying the certificate to be auto-assigned as per the rule.
  - Select the field of the certificate to be searched from the first drop-down
  - Select the relationship between the field value and the condition value from the second drop-down
  - Enter the condition value in the text field.
- For example, if you want to auto-assign certificates with common name dithers.com, then choose 'Common Name' from the first drop-down, select 'Matches' from the second drop-down and enter dithers.com in the text field.
- Choose the Organization and/or Department to which the certificates meeting the conditions to be auto-assigned, from the respective 'Assign to' drop-downs.
- Click OK.
- The Rule will be added to the list. The rule will be available for selection while configuring a Discovery Task. For more details on configuring Discovery Scans, refer to the section Network Discovery Tasks.

- Repeat the process to add more rules.

To edit a rule

- Select the rule and click the 'Edit' button



Edit Assignment Rule

*-required fields

Assignment Rule Name*: Default Rules for Comodo SE

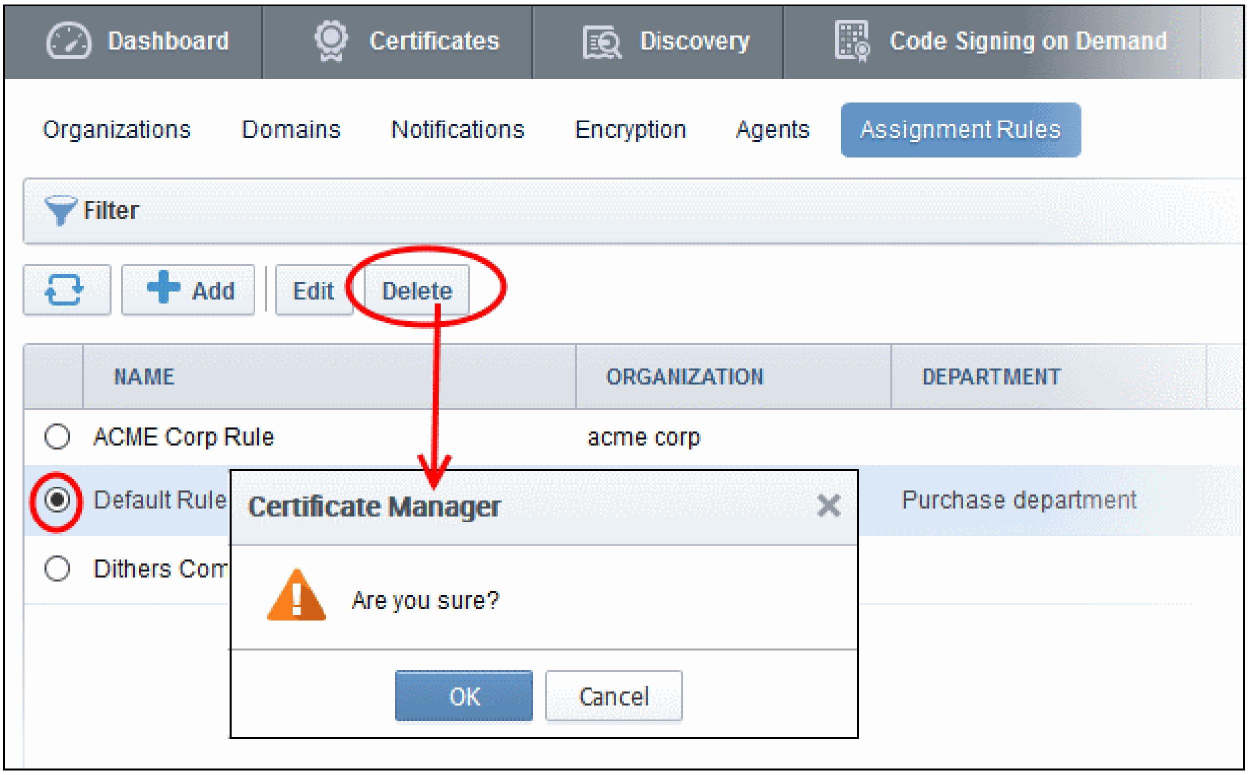
If certificate discovered meets all conditions below

City | Matches | chennai

Assign to ...: Dithers Construction Company | Purchase department

The 'Edit Assignment Rule' dialog will open. The dialog is similar to' Add Assignment Rule' dialog. For description of the parameters, refer to the explanation of adding a new rule

- Edit the parameters and click 'OK'
- To remove a rule, select the rule and click 'Delete'



NAME	ORGANIZATION	DEPARTMENT
○ ACME Corp Rule	acme corp	
● Default Rule		Purchase department
○ Dithers Com		

Certificate Manager

Are you sure?

A confirmation dialog will appear.

- Click 'OK' in the confirmation dialog.

7 Certificate Discovery Tasks

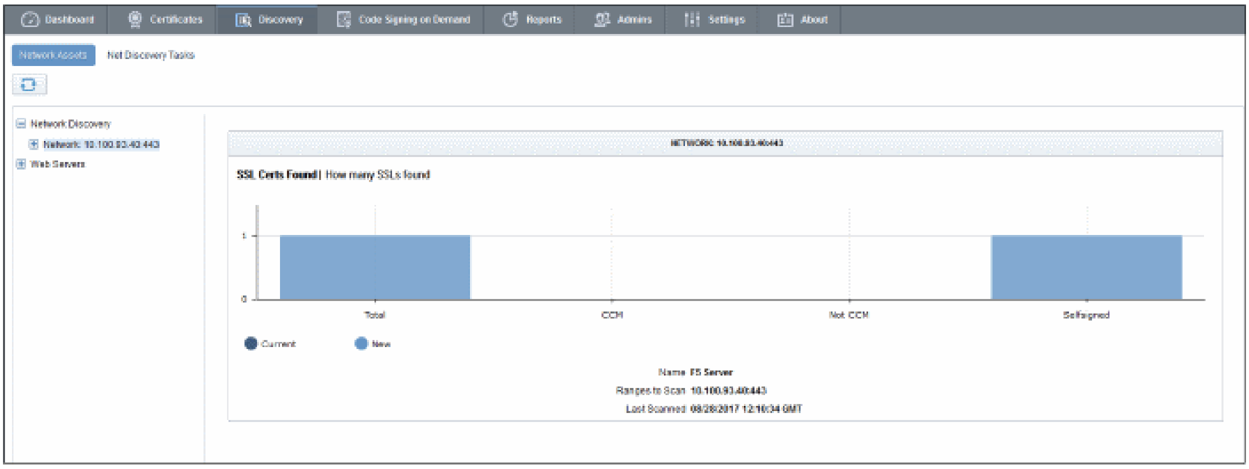
Incommon CM allows RAO administrators to scan networks and to identify:

- SSL certificates installed on your network servers. This includes certificates issued to domains, certificates issued by third party vendors and self-signed certificates.

Network Agents

- Network agents (a.k.a Certificate Controller) installed on network servers facilitate the discovery process in networks. In addition, the agents are also used for automatic installation of SSL certificates on Apache httpd, Apache Tomcat, IIS 7, 7.5, and 8. and F5 BIG IP servers. See Network Agents for Certificate Discovery and Auto-Installation for more details on network agents.

The 'Discovery' interface lets administrators configure and run network discovery scans and to view certificates identified by the scans.



Name: F5 Server

Ranges to Scan: 10.100.93.40:443

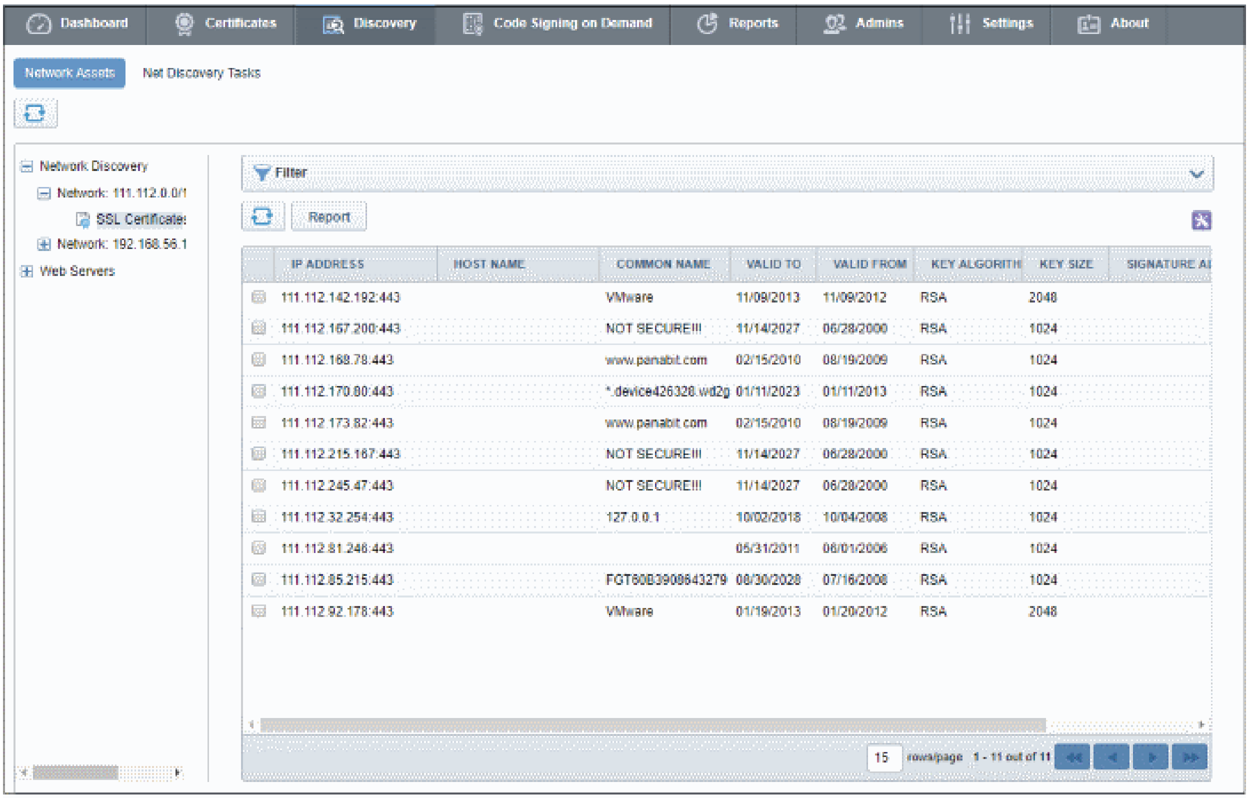
Last Scanned: 08/28/2017 12:10:34 GMT

The interface contains the following tabs:

- Network Assets - Allows you to view the results from scans. The results include certificates and web-servers discovered the network. See Network Assets for more details
- Net Discovery Tasks - Allows you to add, schedule and run discovery tasks on networks. See Network Discovery Tasks for guidance on configuring and running network discovery tasks.

7.1 Network Assets

- The 'Network Assets' area shows discovered SSL certificates installed on servers connected to the network. It also displays a list of web-servers identified on the network and any domains hosted on them.
- Network Assets are displayed as tree structure on the left.
- Select a tree node/device on the left to view installed certificates in the right pane.



IP ADDRESS	HOST NAME	COMMON NAME	VALID TO	VALID FROM	KEY ALGORITH	KEY SIZE	SIGNATURE AI
111.112.142.192:443		VMware	11/09/2013	11/09/2012	RSA	2048	
111.112.167.200:443		NOT SECURE!!!	11/14/2027	06/28/2000	RSA	1024	
111.112.168.78:443		www.panabit.com	02/15/2010	08/19/2009	RSA	1024	
111.112.170.80:443		*.device426328.wd2g	01/11/2023	01/11/2013	RSA	1024	
111.112.173.82:443		www.panabit.com	02/15/2010	08/19/2009	RSA	1024	
111.112.215.167:443		NOT SECURE!!!	11/14/2027	06/28/2000	RSA	1024	
111.112.245.47:443		NOT SECURE!!!	11/14/2027	06/28/2000	RSA	1024	
111.112.32.254:443		127.0.0.1	10/02/2018	10/04/2008	RSA	1024	
111.112.81.246:443			05/31/2011	06/01/2006	RSA	1024	
111.112.85.215:443		FGT60B3908643279	08/30/2028	07/16/2008	RSA	1024	
111.112.92.178:443		VMware	01/19/2013	01/20/2012	RSA	2048	

See the following sections for more detailed explanation on each category of Network Assets.

- Network Discovery
- Web Servers

7.1.1 Network Discovery

The 'Network Discovery' category view allows administrators to view a summary of all certificates installed on every network scanned and a history of previous scans. Administrators can also generate reports on discovered certificates and assign unmanaged certificates identified by discovery scans to respective organizations.

Note: An 'Unmanaged' certificate is one that was not obtained via Incommon Certificate Manager. This includes, for example, certificates from other CA's, self-signed certificates, and certificates issued by Incommon CA but not obtained via Incommon CM. Incommon CM identifies all certificates installed on a scanned network including 'Unmanaged' certificates and allows the administrator to assign them to respective organization/department for which the certificates were enrolled.

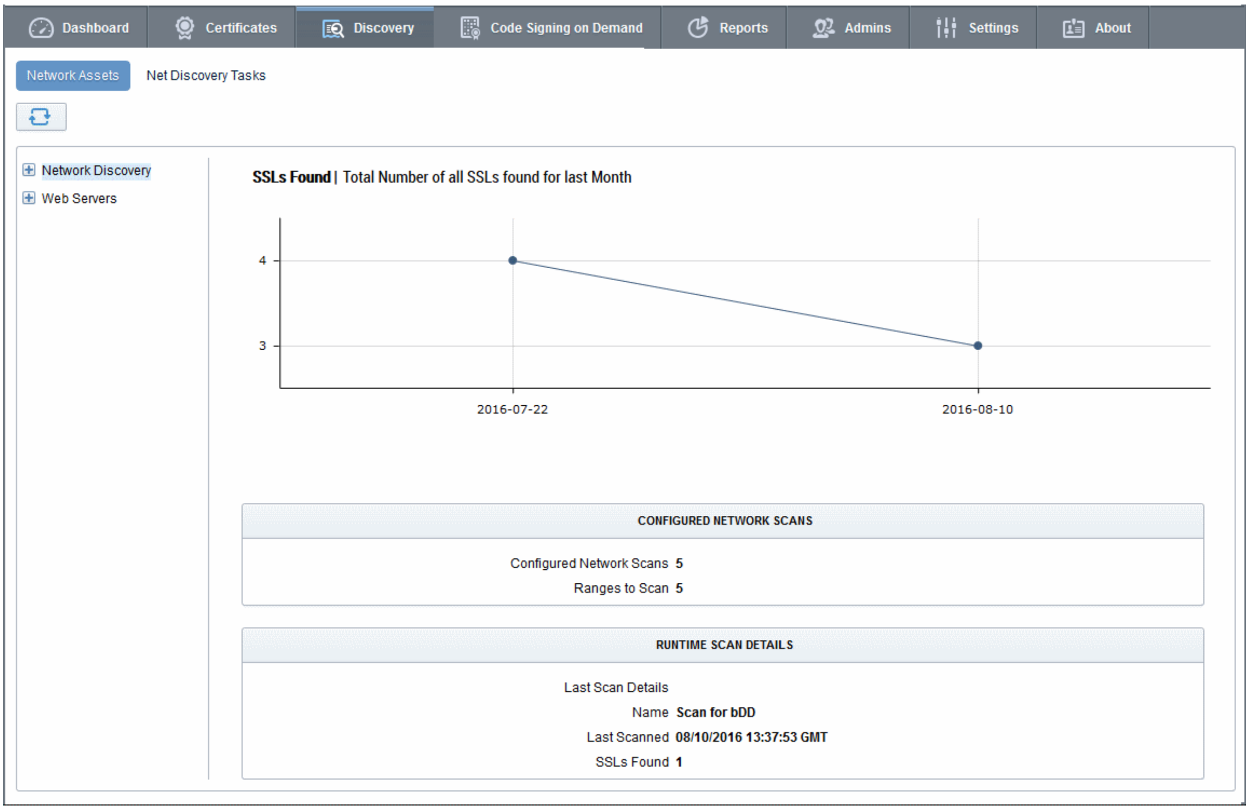
See Network Discovery Tasks for more details on configuring discovery scans.

Security Roles:

- RAO SSL Administrators - can view the certificates installed on networks of organizations (and any sub-ordinate Departments) that have been delegated to them.
- DRAO SSL Administrators - can view the certificates installed on networks of department(s) that have been delegated to them.

To view an over all statistical summary of SSL certificates installed on all scanned networks

- Click 'Discovery' tab and choose 'Network Assets' from the left.
- Choose 'Network Discovery' category from the left



SSLs Found | Total Number of all SSLs found for last Month

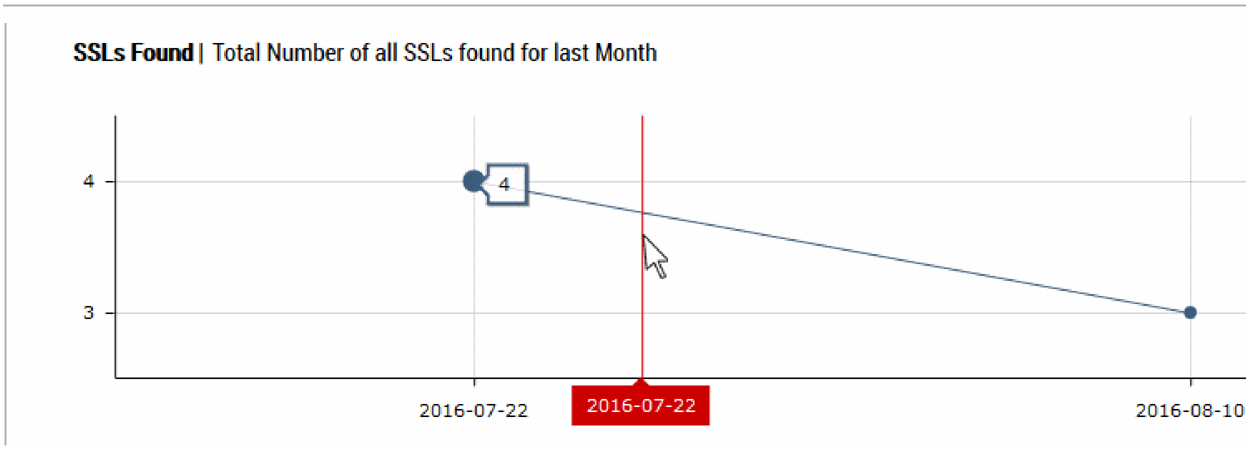
CONFIGURED NETWORK SCANS

Configured Network Scans 5
Ranges to Scan 5

RUNTIME SCAN DETAILS

Last Scan Details
Name Scan for bDD
Last Scanned 08/10/2016 13:37:53 GMT
SSLs Found 1

The right pane shows a time graph of number of SSL certificates and details of discovery scans run on the networks. Hovering the mouse over a date/month displays the number of SSL certificates identified on that date/month.

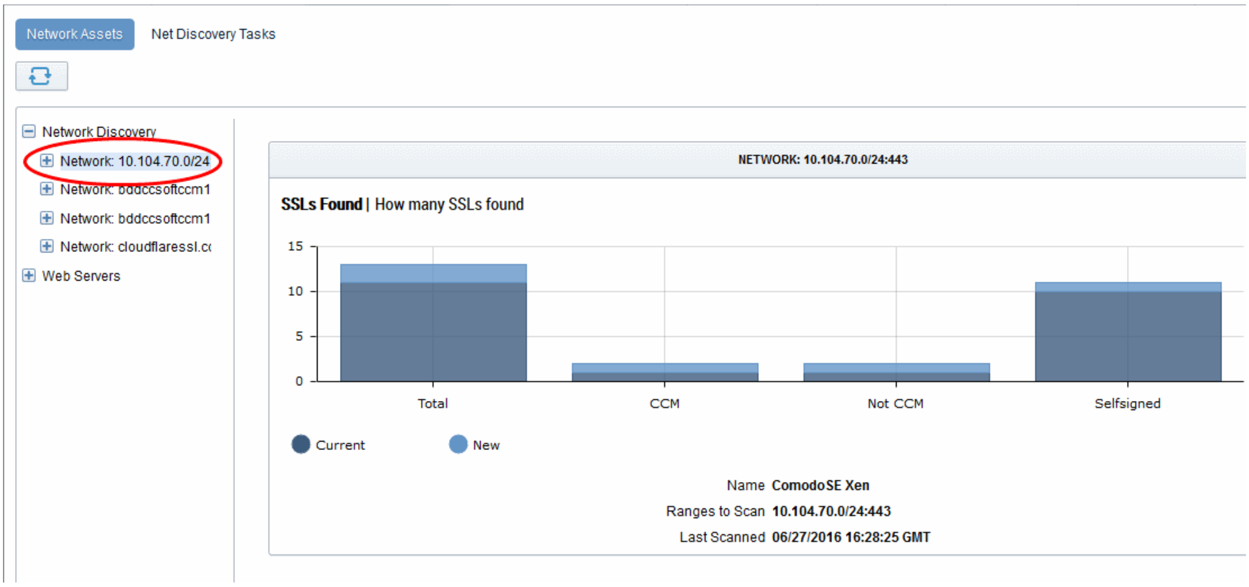


See Network Discovery Tasks for more details on configuring discovery scans.

To view the statistical summary of SSL certificates installed on a selected network

- Click 'Discovery' tab and choose 'Network Assets' from the left.

- Expand the 'Network Discovery' category and choose the network

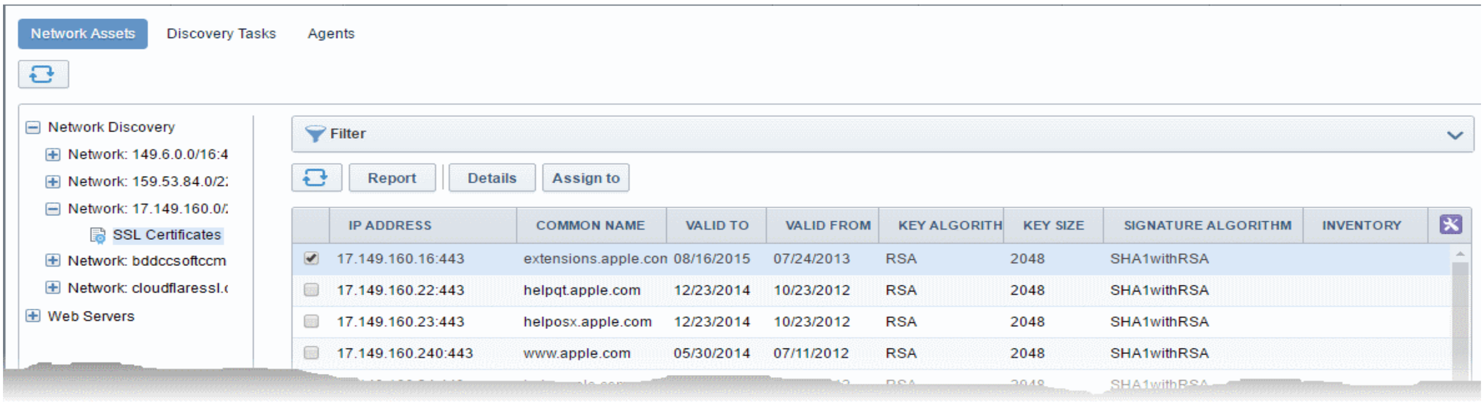


Name ComodoSE Xen
Ranges to Scan 10.104.70.0/24:443
Last Scanned 06/27/2016 16:28:25 GMT

The right pane displays a comparison graph of total number of SSL certificates with numbers of certificates that are managed by Incommon CM, unmanaged certificates and self-signed certificates installed on the network. The details of the discovery scan task name, network and IP ranges scanned and date/time of last run scan are displayed below the graph.

To view the list of SSL certificates installed on a selected network

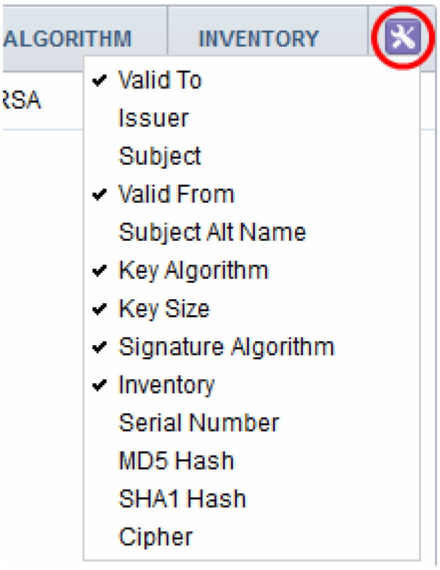
- Click 'Discovery' tab and choose 'Network Assets' sub-tab.
- Expand the 'Network Discovery' category to view the networks on which discovery scans were run.
- Expand the selected network and choose 'SSL certificates'.



	IP ADDRESS	COMMON NAME	VALID TO	VALID FROM	KEY ALGORITH	KEY SIZE	SIGNATURE ALGORITHM	INVENTORY
☑	17.149.160.16:443	extensions.apple.con	08/16/2015	07/24/2013	RSA	2048	SHA1withRSA	
□	17.149.160.22:443	helpqt.apple.com	12/23/2014	10/23/2012	RSA	2048	SHA1withRSA	
□	17.149.160.23:443	helposx.apple.com	12/23/2014	10/23/2012	RSA	2048	SHA1withRSA	
□	17.149.160.240:443	www.apple.com	05/30/2014	07/11/2012	RSA	2048	SHA1withRSA	

The list of certificates detected from the network during the last scan is displayed with their details as a table. Selecting a certificate allows displays options for viewing its details and to manually assign Unmanaged certificates to required organization/department.

The interface also allows you to create a report on the discovered certificates.

<table>
<tr><th colspan="2">List of Discovered Certificates - Column Descriptions</th></tr>
<tr><th>Column Header</th><th>Description</th></tr>
<tr><td>IP Address</td><td>The IP address of the server on which the certificate was discovered.</td></tr>
<tr><td>Host Name</td><td>The name of the server on which the certificate was discovered.</td></tr>
<tr><td>Valid to</td><td>Displays the expiry date of the certificate.</td></tr>
<tr><td>Valid From</td><td>The issuance date of the certificate.</td></tr>
<tr><td>Key Algorithm</td><td>Displays the type of algorithm used for the encryption.</td></tr>
<tr><td>Key Size</td><td>Displays the key size used by certificate for the encryption.</td></tr>
<tr><td>Signature Algorithm</td><td>Displays the type of algorithm used for the signing the certificate.</td></tr>
<tr><td>Inventory</td><td>Indicates whether the certificate is 'Managed' or 'Unmanaged'.
• Clicking the 'Managed' link opens the 'Certificate Details' screen of the certificate. See explanation under 'Viewing Details of a Certificate' for more details. You can open the certificate details dialog by selecting the certificate and clicking the 'Details' button at the top.
• Selecting an 'Unmanaged' certificate displays the option for assigning it to required organization/department. See explanation under Manually Assigning a Certificate to an Organization/Department for more details.
• **Tip –** Incommon CM also allows you to can configure for automatic assignment of Unmanaged certificates identified by a discovery scan to respective organizations and departments. See Overview of Process under Network Discovery Tasks for more details.</td></tr>
<tr><td colspan="2">**Note:** The administrator can add more columns from the drop-down button beside the last item in the column:


ALGORITHM
INVENTORY
RSA
✔ Valid To
Issuer
Subject
✔ Valid From
Subject Alt Name
✔ Key Algorithm
✔ Key Size
✔ Signature Algorithm
✔ Inventory
Serial Number
MD5 Hash
SHA1 Hash
Cipher

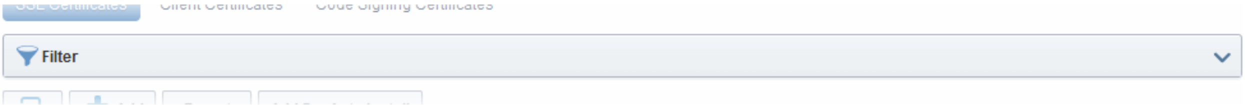
</td></tr>
<tr><td>Issuer</td><td>Displays the details of the Certificate Authority that issued the certificate and the name of the certificate.</td></tr>
<tr><td>Subject</td><td>Displays the details of the common name, organizational unit , organization and more,</td></tr>
</table>

	contained in the 'Subject' field of the certificate.
Subject Alt Name	Displays the names of domain(s) for which the certificate is used for.
Serial Number	Displays the serial number of the certificate that is unique and can be used to identify the certificate.
MD5 Hash	Displays the MD5 hash (thumbprint/fingerprint) for the certificate.
SHA1 Hash	Displays the SHA1 hash (thumbprint/fingerprint) for the certificate.
Cipher	The cipher suite used for encryption.
Key Usage	The cryptographic purpose(s) for which the certificate can be used. For example, key encipherment and signing.
Extended Key Usage	Higher level capabilities of the certificate. For example, web server authentication and client authentication.

Sorting and Filtering Options

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

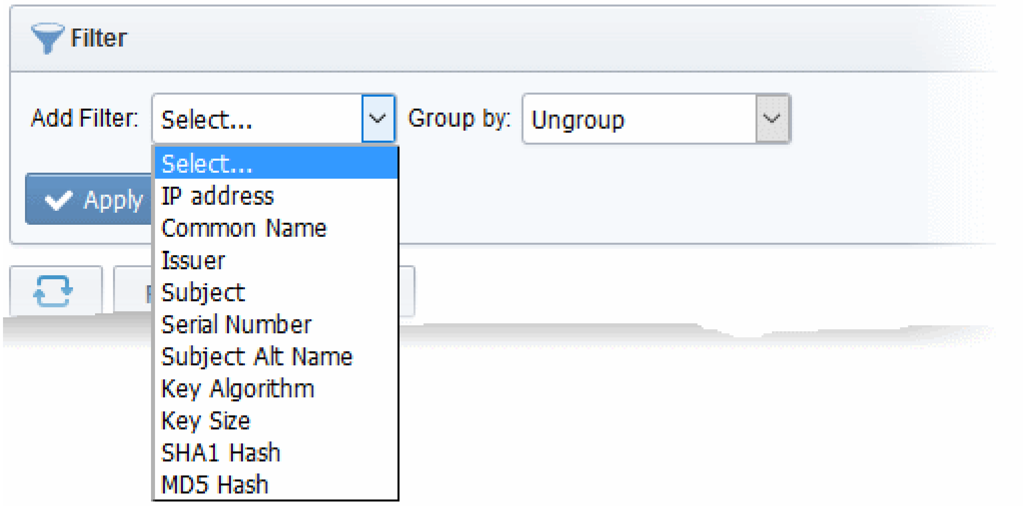
Administrators can search for particular SSL certificates using filters.



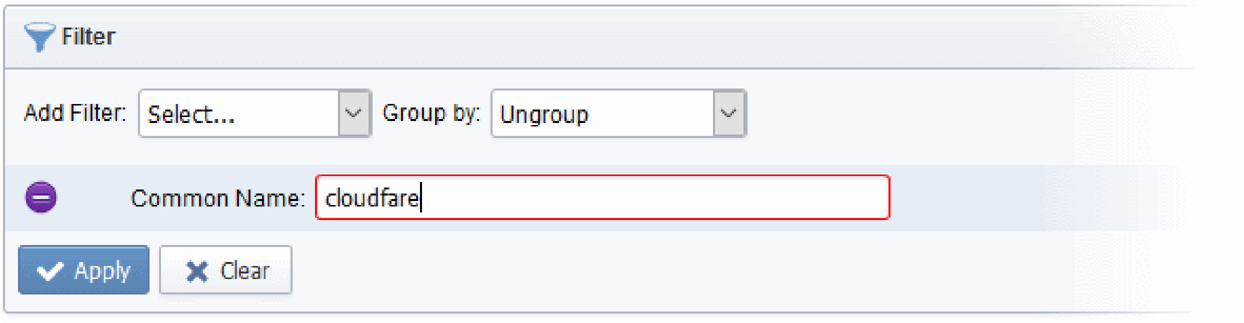
- To apply filters, click on the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the results with other options that appears depending on the selection from the 'Add Filter' drop-down.

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.



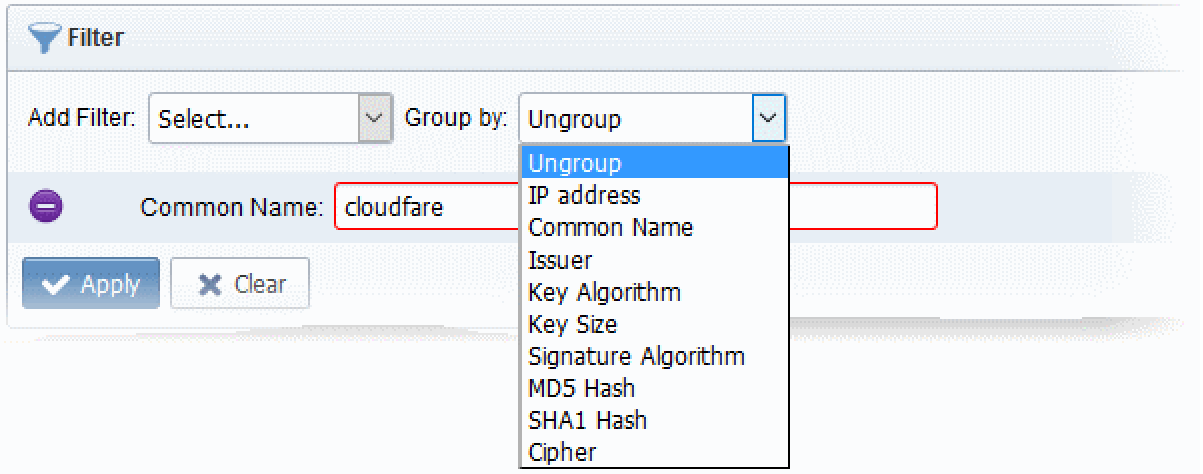
Common Name: cloudfare

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

Filter Criteria	Filter Parameter
IP Address	Enter the IP address from which the certificate was discovered
Host Name	Enter the name of the server on which the certificate is installed
Issuer	Enter the name of the issuer of the certificate
Subject	Enter the details in the Subject field of the certificate in full or part.
Serial Number	Enter the serial number of the certificate in full or part.
Subject Alt Name	Enter the subject alternative name for the certificate fully or in part
Key Algorithm	Enter the key algorithm of the certificate
Key Size	Enter the key size in bits
SHA1 Hash	Enter the SHA1 Hash (thumbprint/fingerprint) of the certificate
MD5 Hash	Enter the MD5 Hash (thumbprint/fingerprint) of the certificate
Key Usage	Filter certificates by cryptographic capabilities.
Extended Key Usage	Filter certificates by higher level purpose. E.g. web server authentication, client authentication.

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 'cloudfare.com' and group the results by their 'Issuer', then select 'Common Name' from the 'Add Filter' drop-down, enter 'cloudfare.com' and select 'Issuer' from the 'Group by' drop-down. The certificates, having 'cloudfare.com' in their common name will be displayed as a list, grouped based on their issuers.

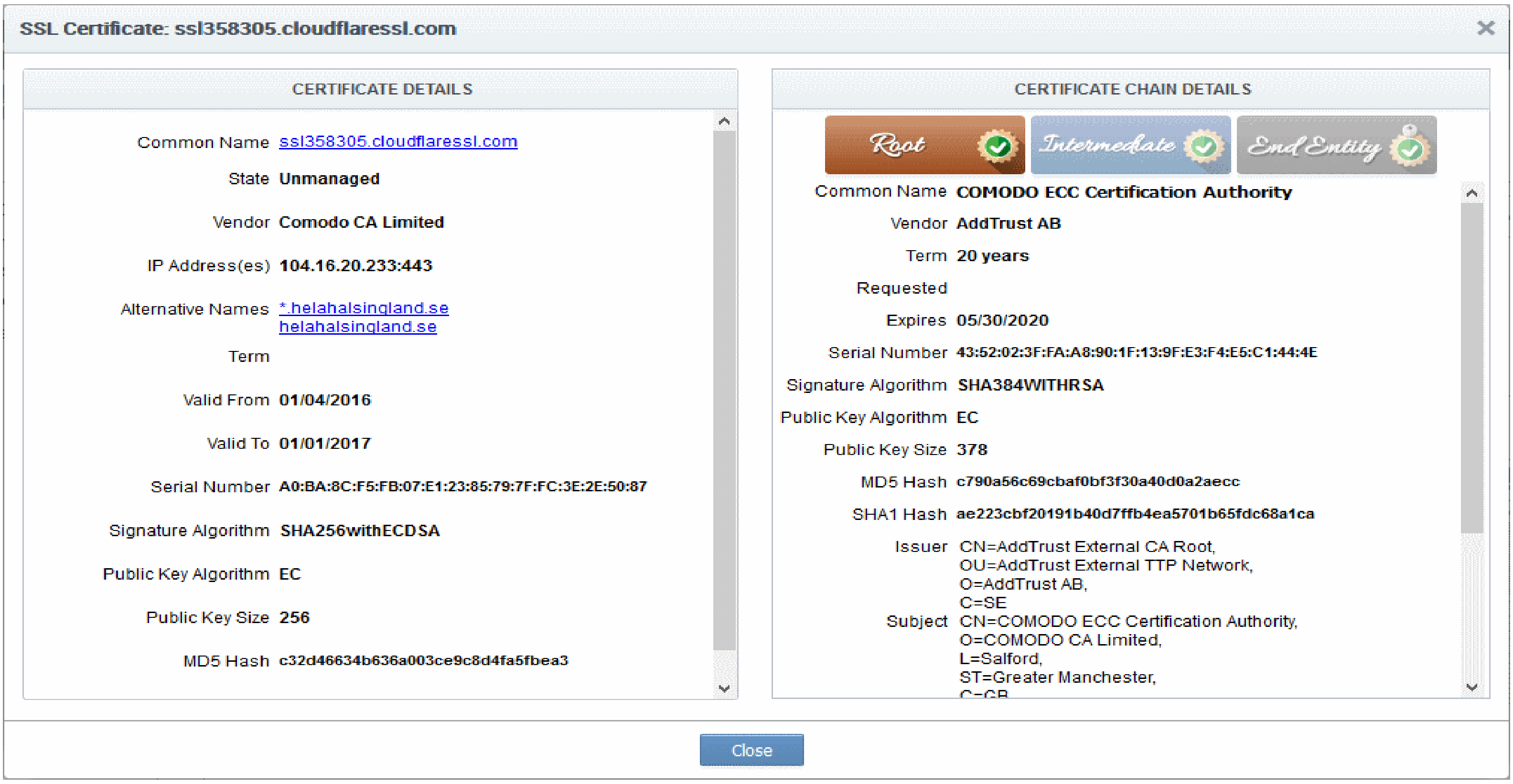
- To remove the filter options, click the 'Clear' button.

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.

Viewing Details of a Certificate

The 'Certificate Details' dialog displays the complete details of the selected SSL certificate with its certificate chain details.

- To view the SSL certificate details dialog, select the certificate from the list and click the 'Details' button at the top.
- Alternatively, click the 'Managed' link in the Inventory column



SSL Certificate: ssl358305.cloudflaressl.com

CERTIFICATE DETAILS

Common Name	ssl358305.cloudflaressl.com
State	Unmanaged
Vendor	Comodo CA Limited
IP Address(es)	104.16.20.233:443
Alternative Names	*.helahalsingland.se helahalsingland.se
Term	
Valid From	01/04/2016
Valid To	01/01/2017
Serial Number	A0:BA:8C:F5:FB:07:E1:23:85:79:7F:FC:3E:2E:50:87
Signature Algorithm	SHA256withECDSA
Public Key Algorithm	EC
Public Key Size	256
MD5 Hash	c32d46634b636a003ce9c8d4fa5fbea3

CERTIFICATE CHAIN DETAILS

Common Name	COMODO ECC Certification Authority
Vendor	AddTrust AB
Term	20 years
Requested	
Expires	05/30/2020
Serial Number	43:52:02:3F:FA:A8:90:1F:13:9F:E3:F4:E5:C1:44:4E
Signature Algorithm	SHA384WITHRSA
Public Key Algorithm	EC
Public Key Size	378
MD5 Hash	c790a56c69cbaf0bf3f30a40d0a2aecc
SHA1 Hash	ae223cbf20191b40d7ffb4ea5701b65fdc68a1ca

Issuer	CN=AddTrust External CA Root,
	OU=AddTrust External TTP Network,
	O=AddTrust AB,
	C=SE

Subject	CN=COMODO ECC Certification Authority,
	O=COMODO CA Limited,
	L=Salford,
	ST=Greater Manchester,
	C=GB

See Certificate 'Details' Dialog for more details on the information displayed in the Certificate Details dialog.

Manually Assigning a Certificate to an Organization/Department

The certificates that are issued through Incommon CM, otherwise called 'Managed' certificates are pre-assigned to their respective organizations or departments, specified during their enrollment process. But the certificates that are not obtained via Incommon CM and found installed on the network by discovery scans are classified as 'Unmanaged' certificates. These certificates are not pre-assigned to any organization or department by default.

You can assign certificates to required organizations/departments from the list of certificates displayed under 'Network Assets'.

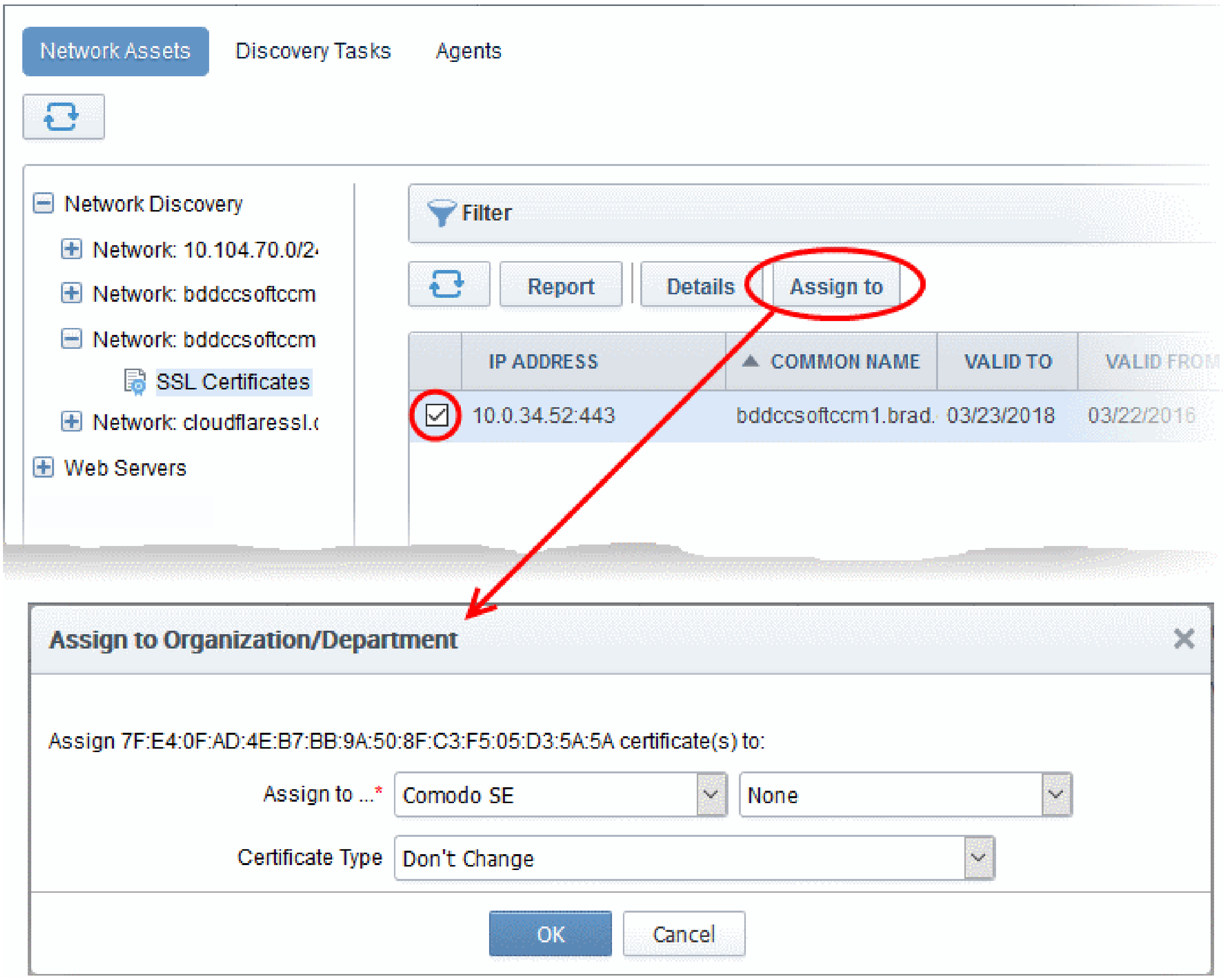
Tip: You can configure a discovery scan to automatically assign the unmanaged certificates identified by it to respective organizations and department by specifying Auto-Assignment Rules.

- See Adding IP Range and Start Scanning under Network Discovery Tasks for more details on configuring a discovery scan.
- See Auto-Assignment Rules for Unmanaged Certificates, for more details on configuring Auto Assignment Rules.

To manually assign certificates

- Click 'Discovery' tab and choose 'Network Assets' sub-tab.
- Expand the 'Network Discovery' category to view the list of scanned networks
- Expand the selected network and choose 'SSL certificates'. The list of SSL certificates found installed on the network will be displayed.

- Select the umnanaged certificate from the list and click 'Assign To'



Assign 7F:E4:0F:AD:4E:B7:BB:9A:50:8F:C3:F5:05:D3:5A:5A certificate(s) to:

Assign to ...*: Comodo SE | None

Certificate Type: Don't Change

The 'Assign to Organization/Department' dialog will appear.

Assign to Organization/Department dialog - Table of parameters	
Form Element	**Description**
Assign to	Select the Organization and Department (optional) from the respective drop-downs to which the certificate has to be assigned.

- Click OK.

The certificate will be assigned to the chosen organization or department.

Generating Report on Discovered Certificates

You can generate a report on the list of certificates discovered on selected network from the Network Assets interface.

To generate a report

- Click 'Discovery' tab and choose 'Network Assets' sub-tab.
- Expand the 'Network Discovery' category to view the list of scanned networks

- Expand the selected network and choose 'SSL certificates'. The list of SSL certificates found installed on the network will be displayed.
- Click the Report button at the top of the list.

The report will be generated as a spreadsheet file containing the list of certificate with their details. You can download the report in .xls format, which can be opened in spreadsheet software like Microsoft Excel or OpenOffice Calc.

7.1.2 Web Servers

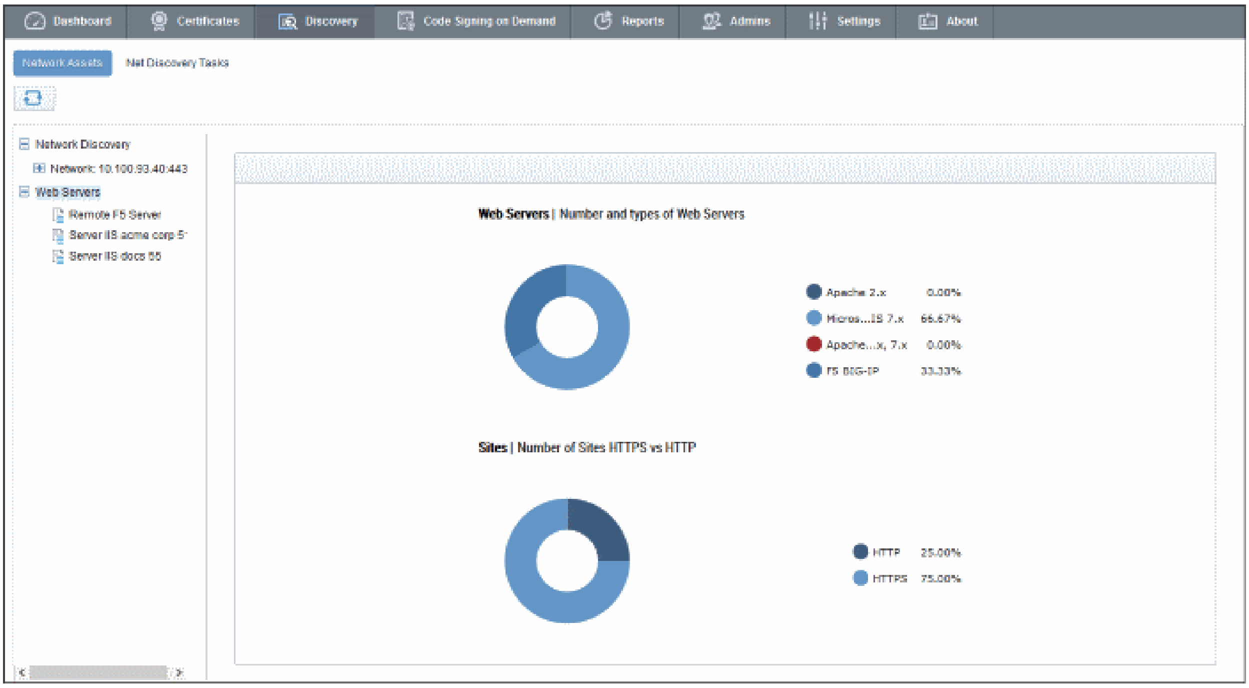
The 'Web Servers' category lets you view a summary of all web-servers identified on every network scanned. The results also show all domains hosted on each server.

Security Roles:

- RAO SSL Administrators - can view details of web servers pertaining to organizations (and any sub-ordinate Departments) that have been delegated to them.
- DRAO SSL Administrators - can view details of web servers pertaining to department(s) that have been delegated to them.

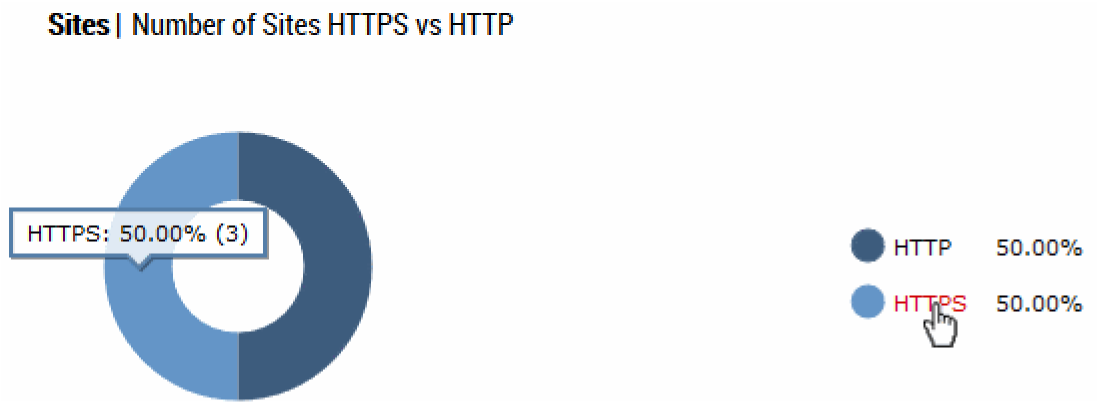
To view a dashboard summary of web servers identified on all scanned networks

- Click the 'Discovery' tab and choose the 'Network Assets' sub-tab.
- Choose 'Web Servers' on the left



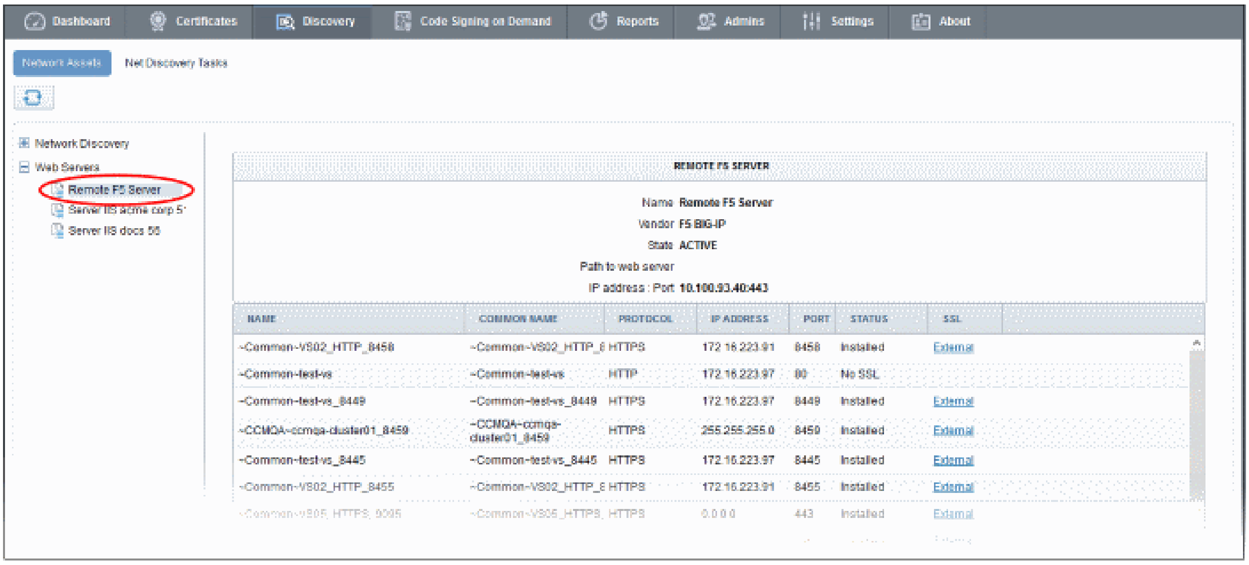
The pie-charts on the right show the percentage of scanned web-servers using different operating systems and the percentage of those servers using HTTPS versus HTTP.

- Placing your mouse over a chart segment or legend item displays additional details such as the exact number of servers/number of sites in that category.



To view details of websites/domains hosted on each server in scanned networks

- Click the 'Discovery' tab and choose the 'Network Assets' sub-tab.
- Expand the 'Web Servers' category to view the list of identified web servers
- Choose the server whose details you want to view



Name Remote F5 Server
Vendor F5 BIG-IP
State ACTIVE
Path to web server
IP address : Port 10.100.93.40:443

NAME	COMMON NAME	PROTOCOL	IP ADDRESS	PORT	STATUS	SSL
~Common~VS02_HTTP_8458	~Common~VS02_HTTP_8	HTTPS	172.16.223.91	8458	Installed	External
~Common~test-vs	~Common~test-vs	HTTP	172.16.223.97	80	No SSL	
~Common~test-vs_8449	~Common~test-vs_8449	HTTPS	172.16.223.97	8449	Installed	External
~CCMQA~ccmqa-cluster01_8459	~CCMQA~ccmqa-cluster01_8459	HTTPS	255.255.255.0	8459	Installed	External
~Common~test-vs_8445	~Common~test-vs_8445	HTTPS	172.16.223.97	8445	Installed	External
~Common~VS02_HTTP_8455	~Common~VS02_HTTP_8	HTTPS	172.16.223.91	8455	Installed	External
~Common~VS05_HTTPS_9095	~Common~VS05_HTTPS_	HTTPS	0.0.0.0	443	Installed	External

The right hand pane displays general server details and a list of websites/domains hosted on the server:

List of Discovered Websites - Column Descriptions	
Column Header	**Description**
Name	The name of the website/domain.
Common Name	The registered domain name for website/domain.
Protocol	Displays the data transfer protocol used by the website.
IP Address	The address where the site is hosted.
Port	The server port number through which the site is served
Status	Indicates whether the site is secured with SSL/TLS.

SSL	For HTTPS sites, indicates whether the certificate used by the site is managed by InCommon CM or not. Clicking the entry opens the 'Certificate Details' screen. For more details on the information shown in this screen, refer to Certificate 'Details' Dialog

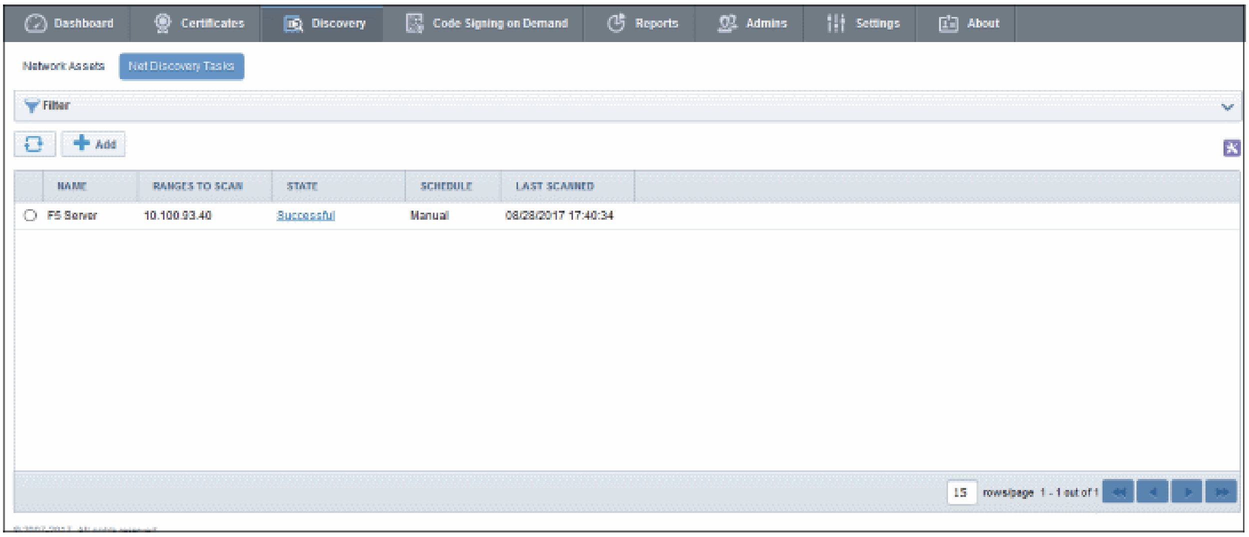
7.2 Network Discovery Tasks

- The Network Discovery option is a very convenient tool for scanning and monitoring a network for all installed SSL certificates (including Incommon Certificates that may or may not have been issued using Incommon Certificate Manager, any 3rd party vendor certificates and any self-signed certificates).
- Administrators can configure Discovery Tasks for different networks to be scanned and can optionally set a schedule for them for periodical scanning.
- Each discovery task can also be added with auto-assignment rules so that unmanaged certificates identified from that discovery scan will be assigned to the respective organizations/departments and added to the 'Certificates' > 'SSL Certificates' interface.

Security Roles:

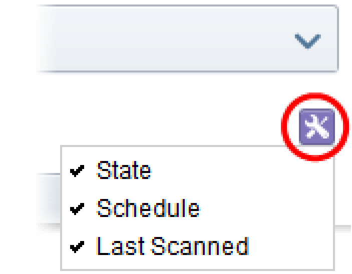
- RAO - can scan for certificates installed on networks pertaining to organizations (and any sub-ordinate Departments) that have been delegated to them.
- DRAO - can scan for certificates installed on networks pertaining to the department that have been delegated to them.

The 'Discovery Tasks' interface displays the list of tasks added to Incommon CM and allows Administrators to create new Discovery Tasks and edit existing tasks.



	NAME	RANGES TO SCAN	STATE	SCHEDULE	LAST SCANNED
○	F5 Server	10.100.93.40	Successful	Manual	08/28/2017 17:40:34

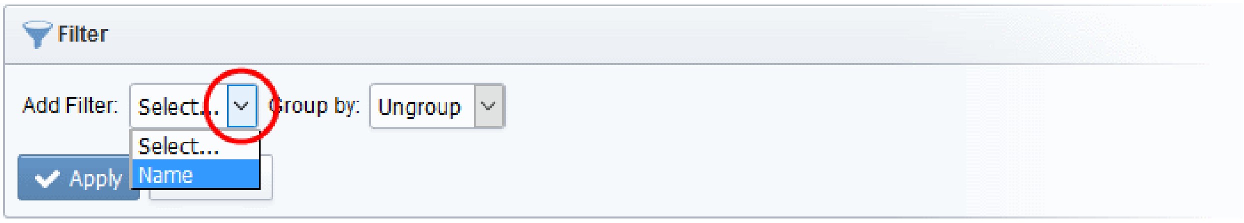
Discovery Tasks area - Table of Parameters		
Field Element	**Values**	**Description**
Name	String	Name of the certificate discovery task.
Ranges to Scan	String	Displays the IP ranges that will be scanned during this task.
State	String	Displays the status of the scan, that is, whether it is successful, failed,

		in progress or canceled. Clicking the state displays respective result. For example, clicking '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 desired columns from the drop-down at the right end of 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.

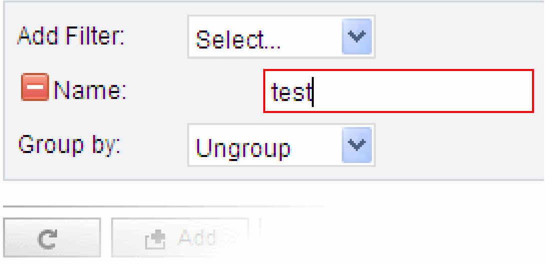
7.2.1 Sorting and Filtering Options

- Clicking the 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 a particular discovery task by using filter.



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.

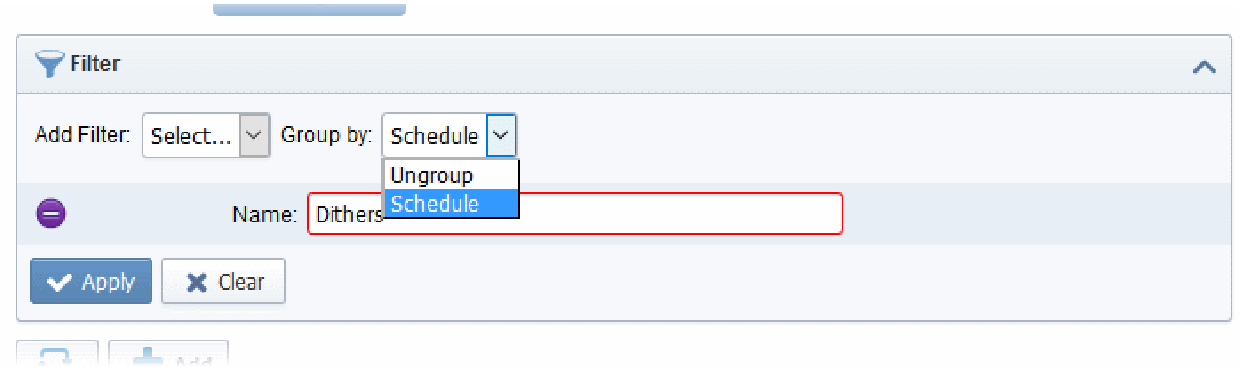


Filter Criteria	Filter Parameter
Name	Enter the name of the discovery task fully or in part

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.
- 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 'Dithers' and group the results by 'Scheduled', then select 'Name' from the 'Add Filter' drop-down, enter 'Dithers' and select 'Schedule' 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.

7.2.2 Prerequisites

The administrator has defined a default organization/department and has installed the discovery agent. All unmanaged certificates found during the certificate discovery scanning process will be assigned to the default organization/department. A discovery scan cannot be performed until the agent is installed and a default organization is defined.

7.2.3 Overview of Process

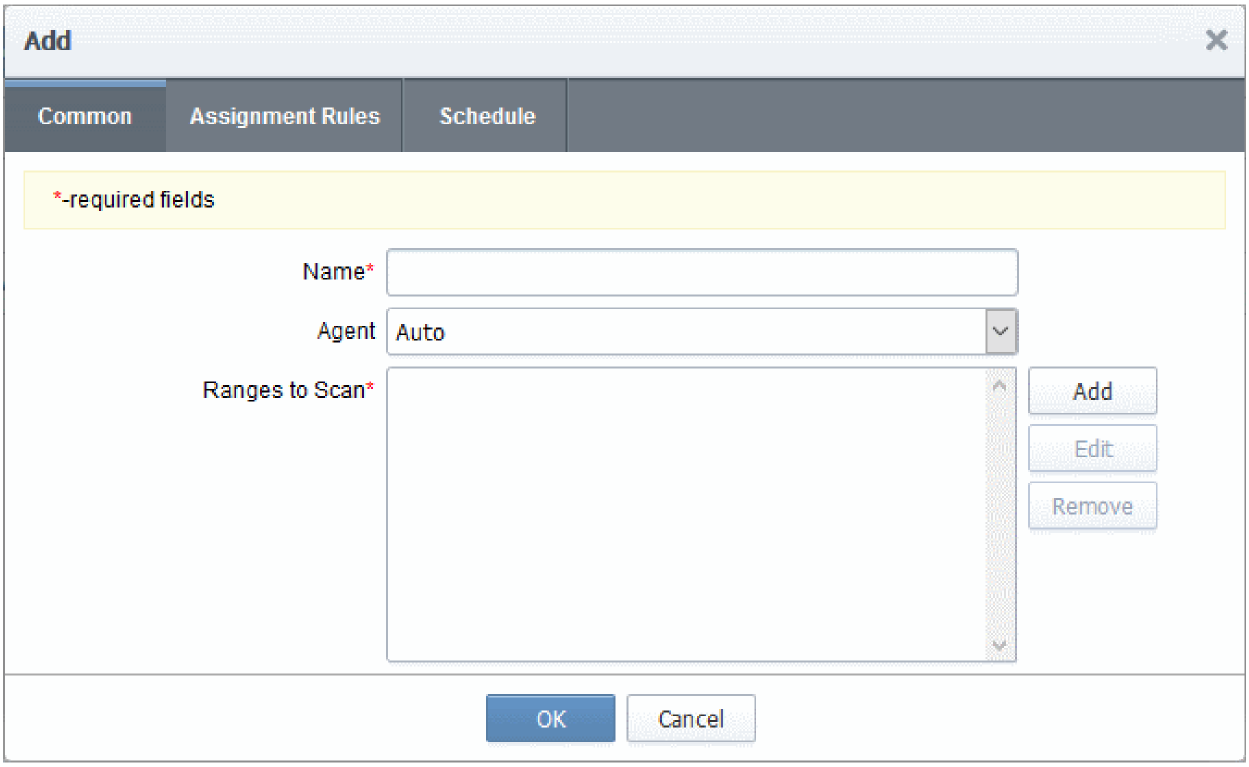
1. Run a scan of networks in order to find all deployed SSL certificates.
2. Incommon CM will automatically integrate all newly discovered certificates and add:
   - Certificates with Managed status and certificates with 'Unmanaged' status but auto-assigned to respective organizations/departments based on Assignment Rules applied to the discovery task, to 'SSL Certificates' area ('Certificates' > 'SSL' Certificates)
   - All certificates to the lists of certificates, including 'Unmanaged' certificates that are not assigned to any Organization/Department, under respective networks in the the 'Network Assets' area. Administrators can assign manually assign 'Unmanaged' certificates to organizations/departments to which they pertain, to bring them under management through the SSL Certificates area. See Network Discovery for more details.
3. InCommon CM will assign certificates that were not issued using the CM to the default organization with the status 'Unmanaged'.
4. InCommon CM will update the status of existing certificates that were issued using the CM (if necessary).
5. 'Unmanaged' certificates can become 'Managed' by renewing the particular certificate.
6. The compiled results of the scan can be viewed in the 'Discovery Scan Log'.

7.2.4 Adding IP Range and Start Scanning

1. To add a discovery scan task, click 'Discovery' > 'Discovery Tasks'> 'Add' to open the scan configuration form

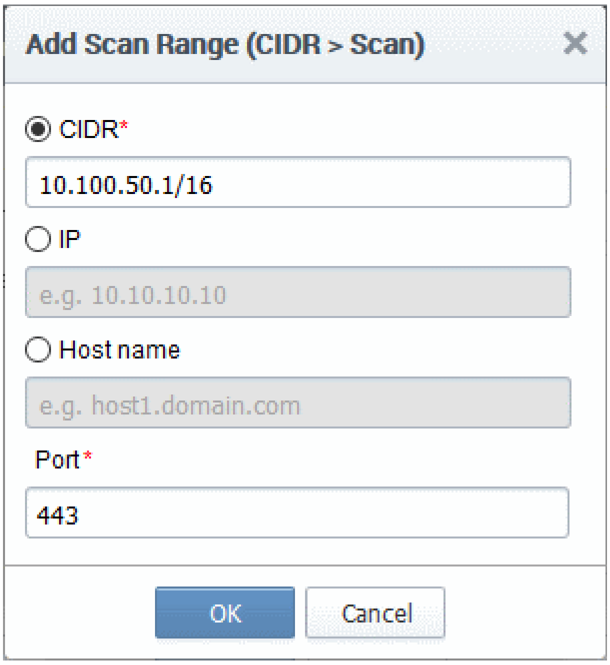
   The form has three tabs. The first to configure scan settings, the second to apply auto-assignment rules and the third to schedule the scan.

2. First, complete the 'Common' tab:



Form Element	Description
Name	Enter a name to describe the discovery task.
Agent	Select the Incommon CM controller agent to be used for scanning. Incommon CM uses agents installed on internal servers to scan for certificates. See Agents for more details.
Ranges to Scan	IP address ranges of servers to be scanned.
Add	Add IP ranges for scanning.
Edit	Edit the selected scan range .
Remove	Delete the selected scan range.
OK	Add the discovery task to the list.
Cancel	Cancel the task.

3. Click the 'Add' button to add the CIDR, IP or the host name in the 'Add Scan Range' dialog.



Add Scan Range (CIDR > Scan)

● CIDR*

10.100.50.1/16

○ IP

e.g. 10.10.10.10

○ Host name

e.g. host1.domain.com

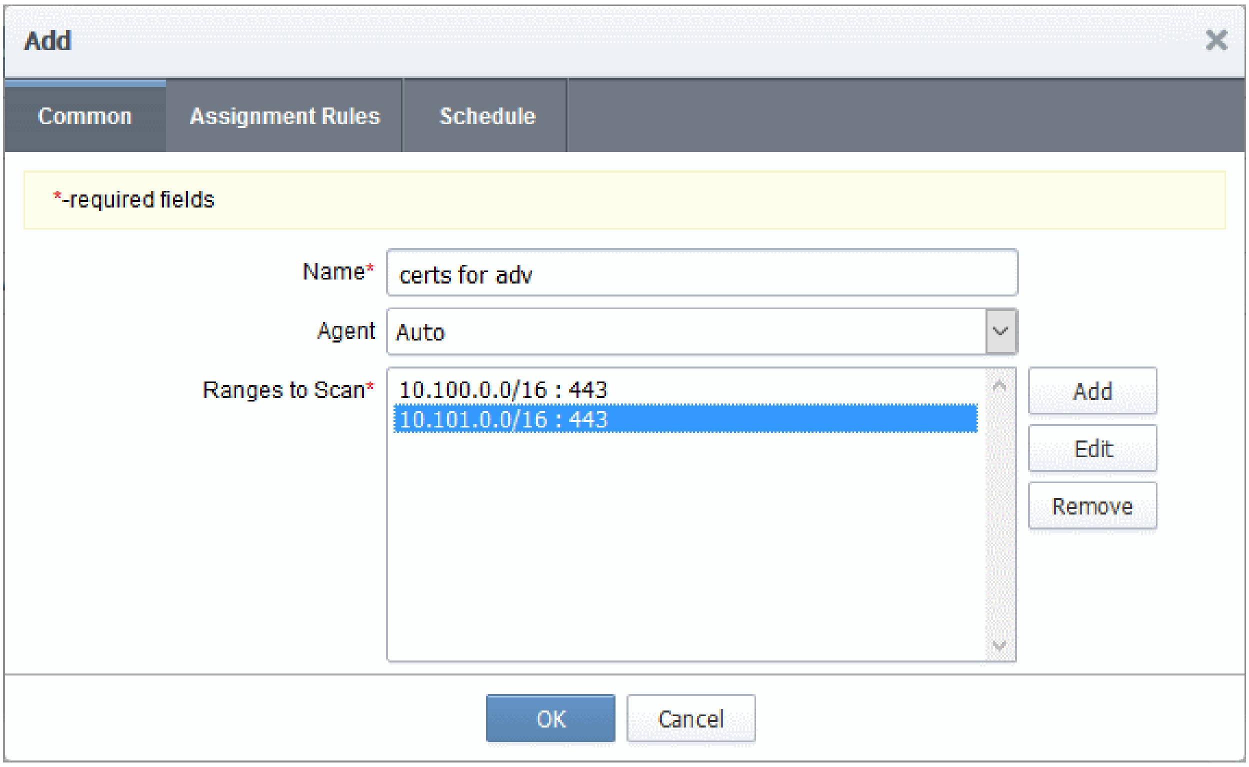
Port*

443

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.

4. Click OK after selecting and entering the appropriate details.

Administrators can add more scan ranges for the same discovery task. Repeat the process as explained above.



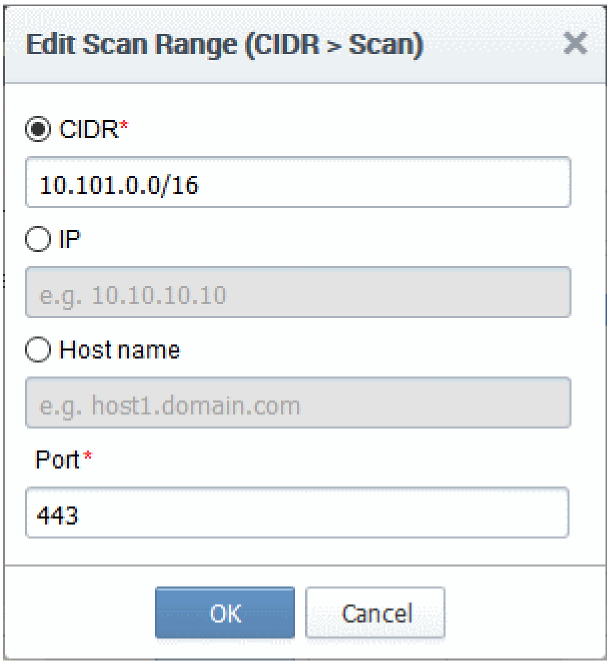
*-required fields

Name* certs for adv

Agent Auto

Ranges to Scan* 10.100.0.0/16 : 443
10.101.0.0/16 : 443

The entered scan ranges will be displayed. Administrators can edit or remove the scan range after selecting it and clicking 'Edit' or 'Remove'.



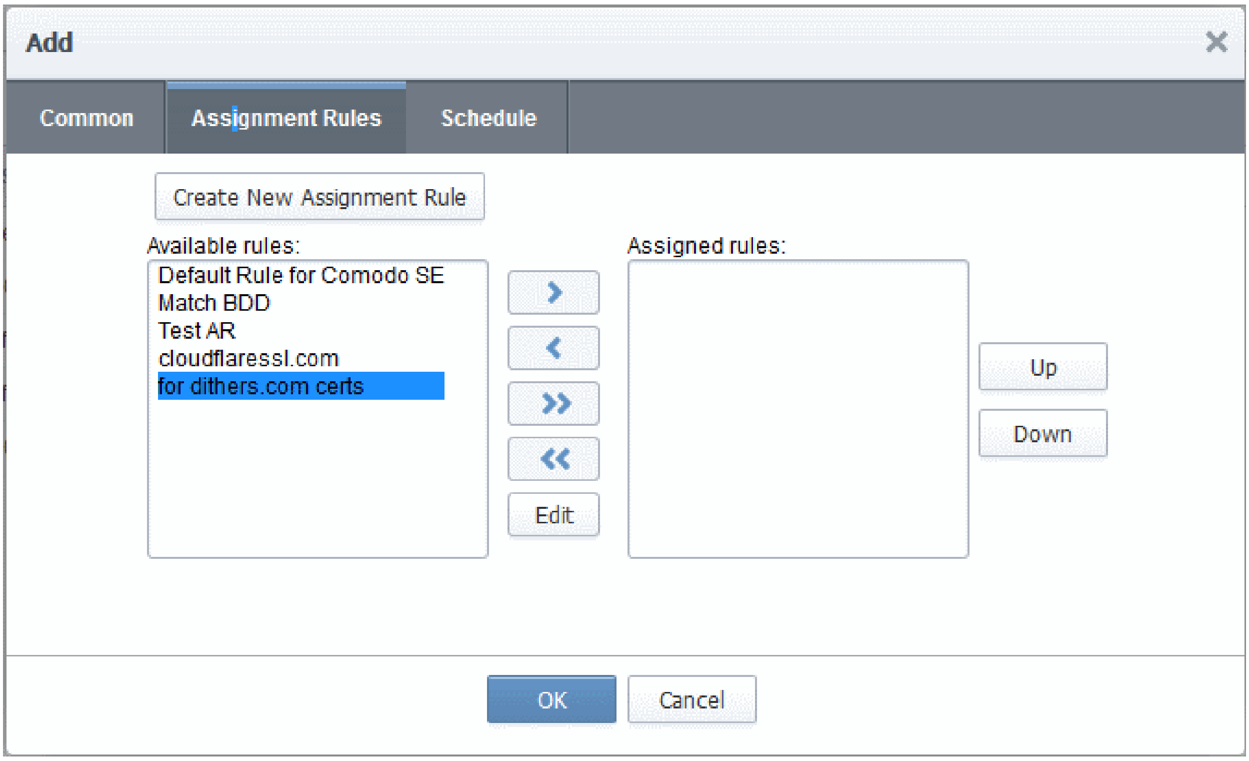
● CIDR* 10.101.0.0/16

○ IP e.g. 10.10.10.10

○ Host name e.g. host1.domain.com

Port* 443

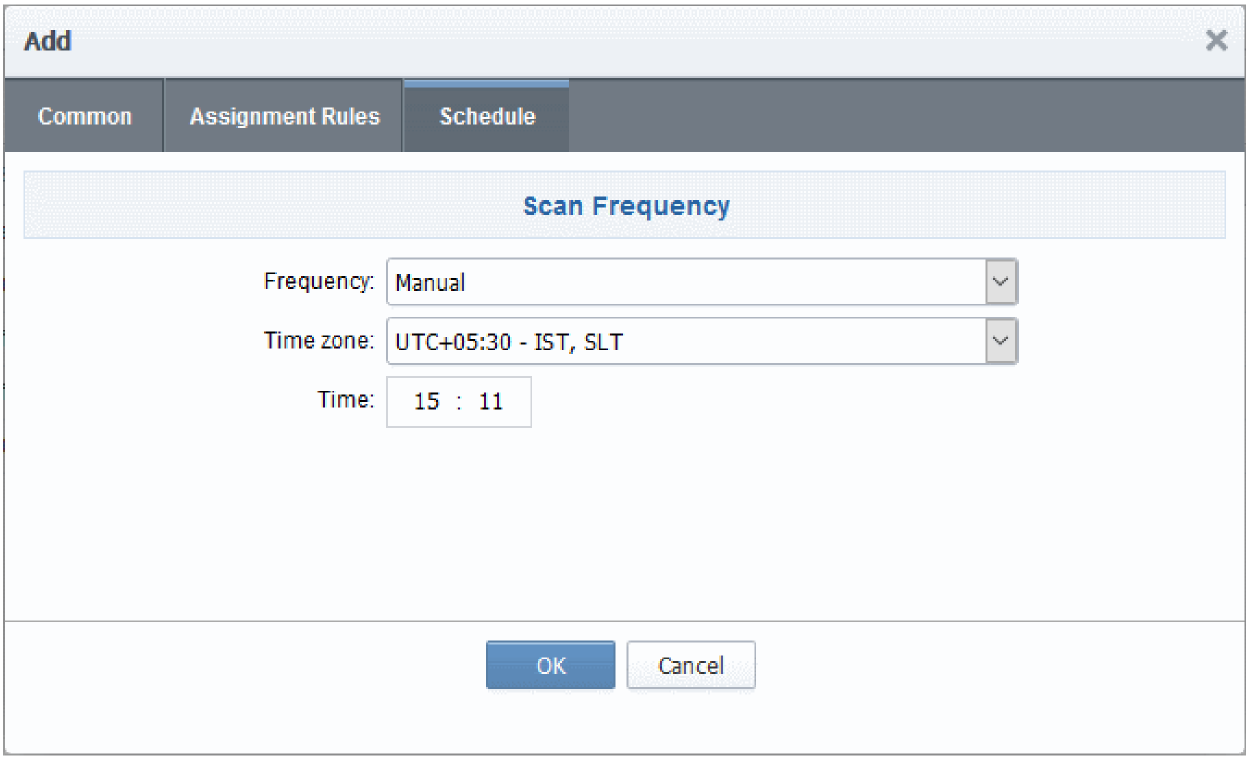
5. Click the 'Assignment Rules' tab to add rules based on which the unmanaged certificates identified by the scans are to be assigned to their respective organizations/departments.



All available rules are shown on the left. Use the arrow buttons to add rules to the discovery task. Rules can be configured in the 'Settings' > 'Assignment Rules' interface. For more details on managing auto-assignment rules, refer to Auto-Assignment Rules for Unmanaged Certificates.

- To create a new rule, click the 'Create New Assignment Rule' button. See Creating a new certificate assignment rule in Auto-Assignment Rules for Unmanaged Certificates for more guidance. The rule will be added to the list of Available Rules. Select it and move to the 'Assigned rules' list.
- To edit a rule, select it and click the Edit button. See Editing an assignment rule in the section Auto-Assignment Rules for Unmanaged Certificates for more guidance.

6. Click the 'Schedule' tab to set the scan frequency for the discovery task.



Frequency: Manual

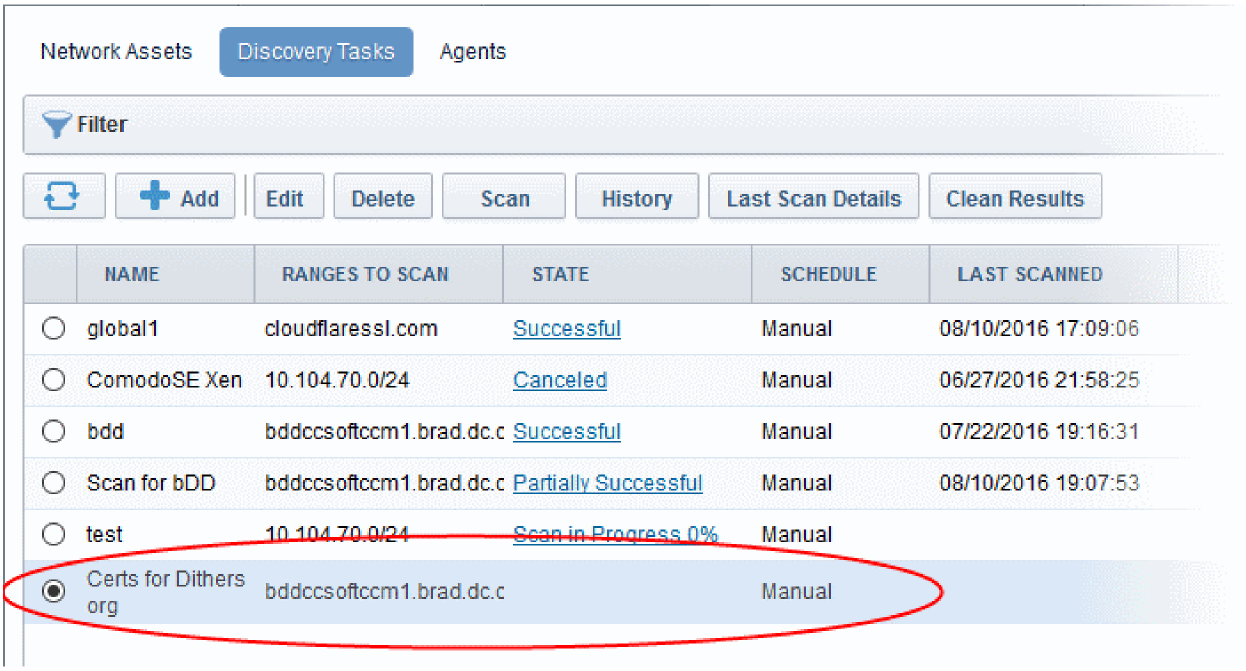
Time zone: UTC+05:30 - IST, SLT

Time: 15 : 11

Scan frequency that could be set for the discovery task are: Manual (on demand), Daily, Weekly, Monthly, Quarterly, Semi-Annually and Annually. You can set the date/day and time at which the scans are to be periodically run from the options, as per the chosen frequency.

7. Click 'OK'.

The newly created discovery task will be displayed in the list.



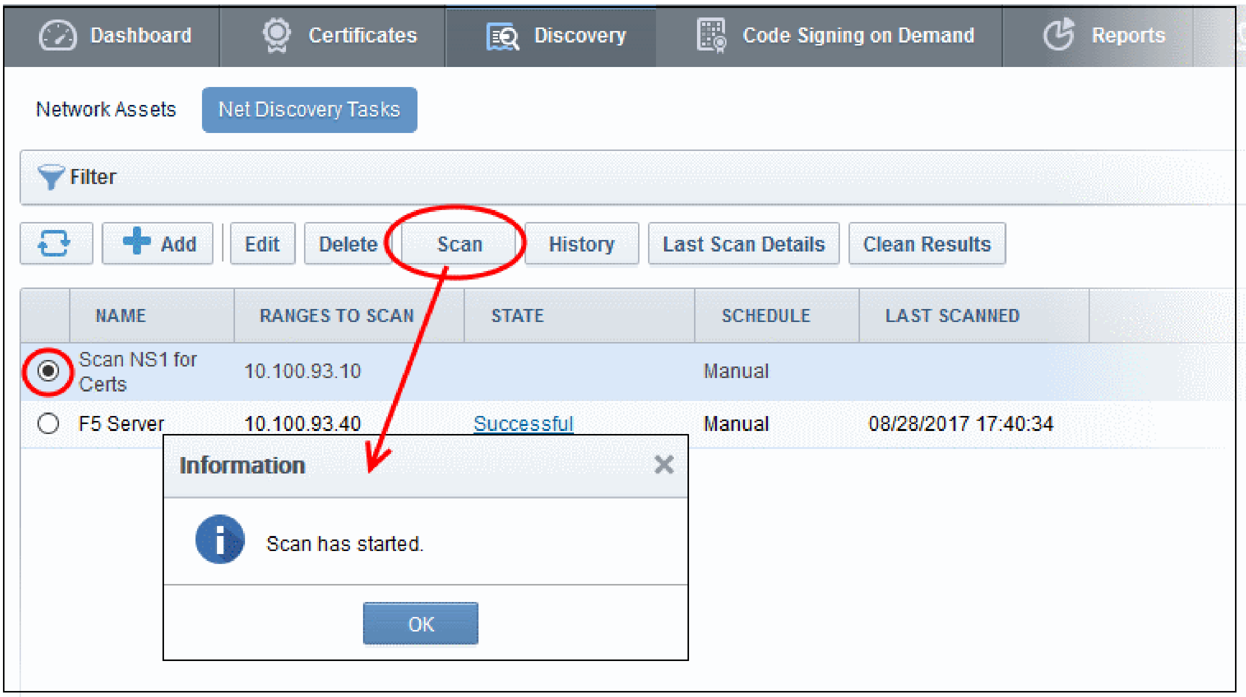
	NAME	RANGES TO SCAN	STATE	SCHEDULE	LAST SCANNED
○	global1	cloudflaressl.com	Successful	Manual	08/10/2016 17:09:06
○	ComodoSE Xen	10.104.70.0/24	Canceled	Manual	06/27/2016 21:58:25
○	bdd	bddccsoftccm1.brad.dc.c	Successful	Manual	07/22/2016 19:16:31
○	Scan for bDD	bddccsoftccm1.brad.dc.c	Partially Successful	Manual	08/10/2016 19:07:53
○	test	10.104.70.0/24	Scan in Progress 0%	Manual	
●	Certs for Dithers org	bddccsoftccm1.brad.dc.c		Manual	

Repeat the process to add more Network Discovery Tasks.

8. To run a scan, select it select the respective 'Discovery Task' from the list

The control buttons for managing the task will be displayed at the top.

9. Click the 'Scan' button to commence the discovery scan for the selected task.



	NAME	RANGES TO SCAN	STATE	SCHEDULE	LAST SCANNED
●	Scan NS1 for Certs	10.100.93.10		Manual	
○	F5 Server	10.100.93.40	Successful	Manual	08/28/2017 17:40:34

Information

Scan has started.

OK

InCommon CM 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.

2.((# 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 an approximate calculation of scanning times.

Example:

Scanning a single range xxx.xxx.0.0/16 for a single port (443) equals 65,536 IP addresses.

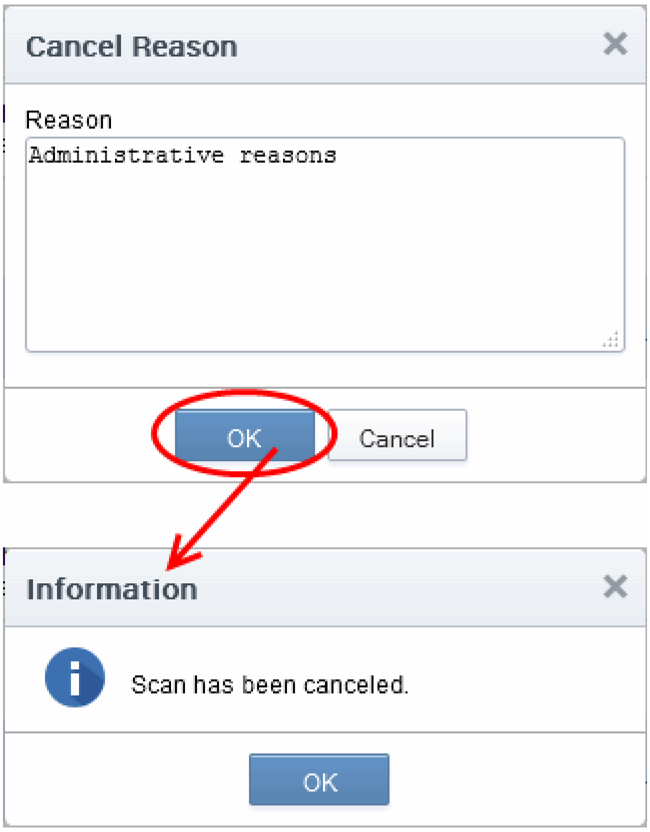
((65536)(1))/300 = approx 218 minutes.

The progress of the scan can be viewed in the row of the selected discovery task under the 'State' column.

10. 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.



Cancel Reason

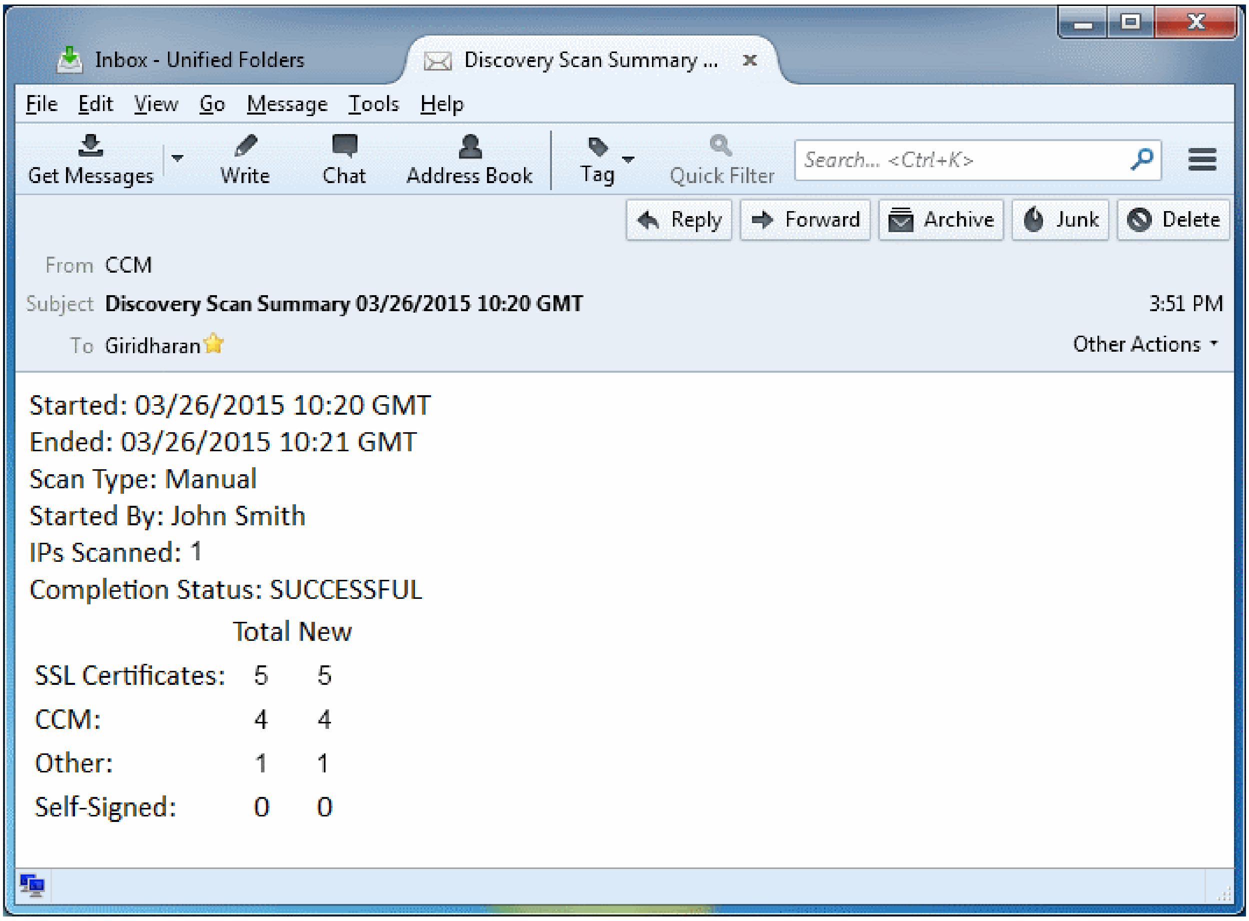
Reason

Administrative reasons

Information

Scan has been canceled.

After the scan is complete, administrators will be notified of the result via email. Please note the email notification should should have been configured in the Discovery Scan Summary notifications area.



From CCM

Subject **Discovery Scan Summary 03/26/2015 10:20 GMT** 3:51 PM

To Giridharan

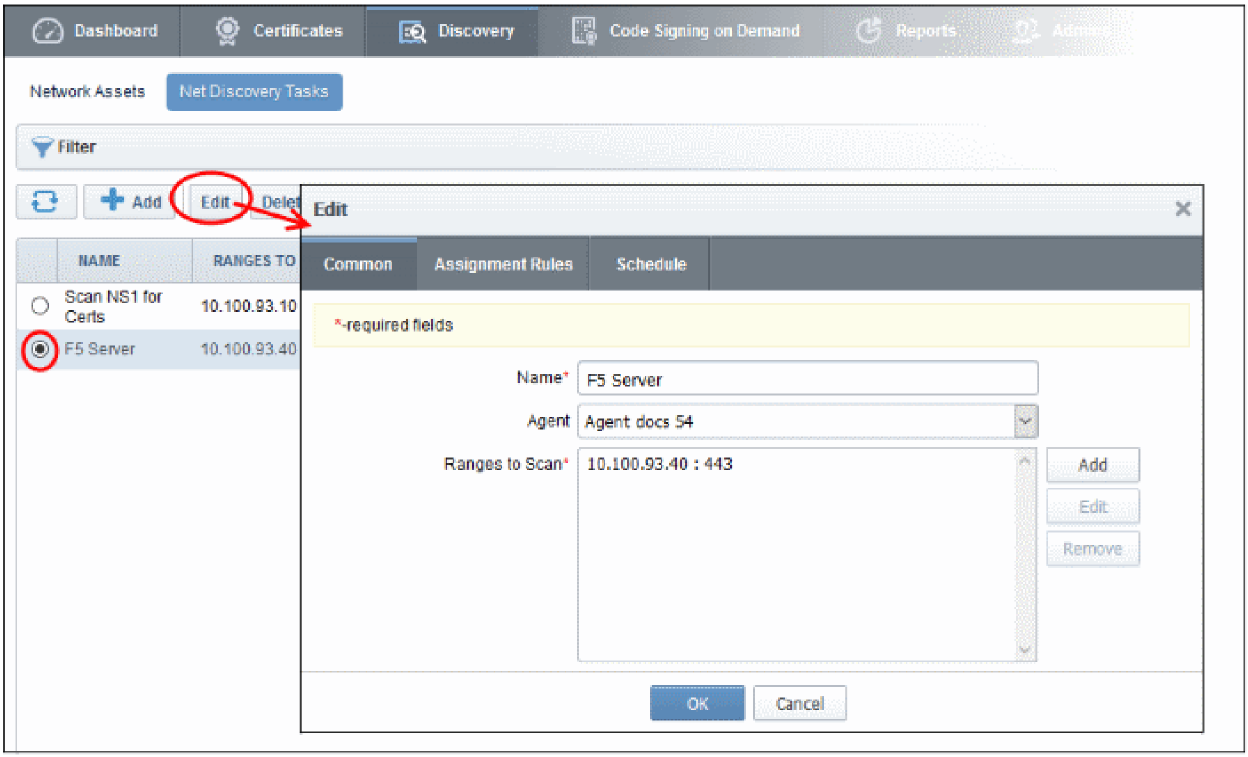
Started: 03/26/2015 10:20 GMT
Ended: 03/26/2015 10:21 GMT
Scan Type: Manual
Started By: John Smith
IPs Scanned: 1
Completion Status: SUCCESSFUL

	Total	New
SSL Certificates:	5	5
CCM:	4	4
Other:	1	1
Self-Signed:	0	0

The results of the scan can be viewed at 'SSL certificates' sub-tab of the 'Certificate Management' section and the 'Reports' section.

7.2.5 Editing a Network Discovery Task

Administrators can edit an existing discovery task by select ingit in the list and clicking the 'Edit' button at the top.



NAME	RANGES TO
○ Scan NS1 for Certs	10.100.93.10
● F5 Server	10.100.93.40

*-required fields

Name* F5 Server

Agent Agent docs 54

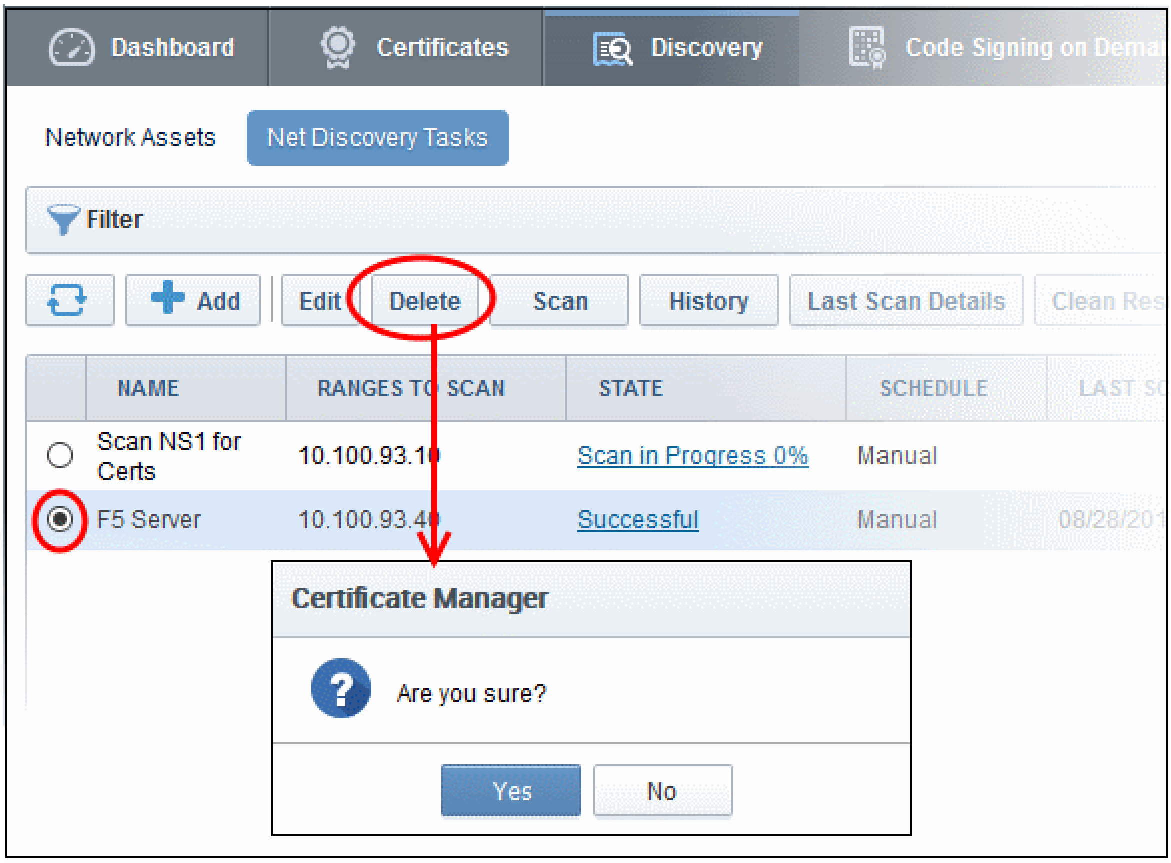
Ranges to Scan* 10.100.93.40 : 443

The 'Edit' interface will open.

The interface allows administrators to change the task name, select another agent, add a new scan range, edit existing scan ranges or remove it. In the schedule tab, the scan frequency can be edited. See Adding IP Range and Start Scanning for more details.

7.2.6 Deleting a Network Discovery Task

- To delete a discovery task from the list, select it and click the 'Delete' button at the top.



	NAME	RANGES TO SCAN	STATE	SCHEDULE	LAST SC
○	Scan NS1 for Certs	10.100.93.10	Scan in Progress 0%	Manual	
●	F5 Server	10.100.93.40	Successful	Manual	08/28/201

Certificate Manager

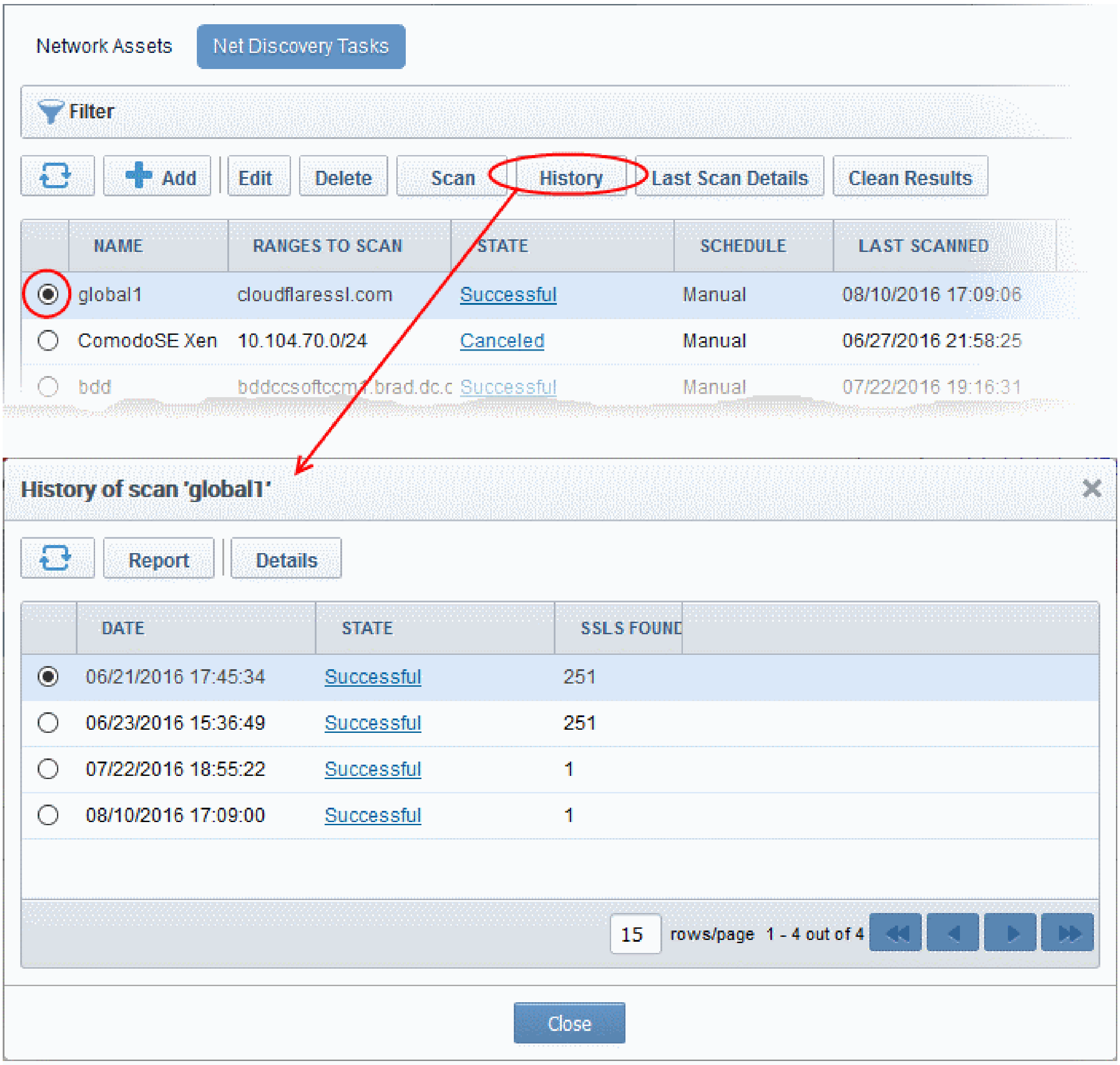
Are you sure?

- Confirm the deletion in the dialog that appears.

7.2.7 Viewing History of Network Discovery Tasks

Incommon CM allows administrators to view the previous five scan results of each discovery task. You can also download a report on each task and can assign unmanaged, discovered certificates to an organization or department.

- To view the history of a discovery task, select it and click the 'History' button at the top.



	NAME	RANGES TO SCAN	STATE	SCHEDULE	LAST SCANNED
●	global1	cloudflaressl.com	Successful	Manual	08/10/2016 17:09:06
○	ComodoSE Xen	10.104.70.0/24	Canceled	Manual	06/27/2016 21:58:25
○	bdd	bddccsoftccm1.brad.dc.c	Successful	Manual	07/22/2016 19:16:31

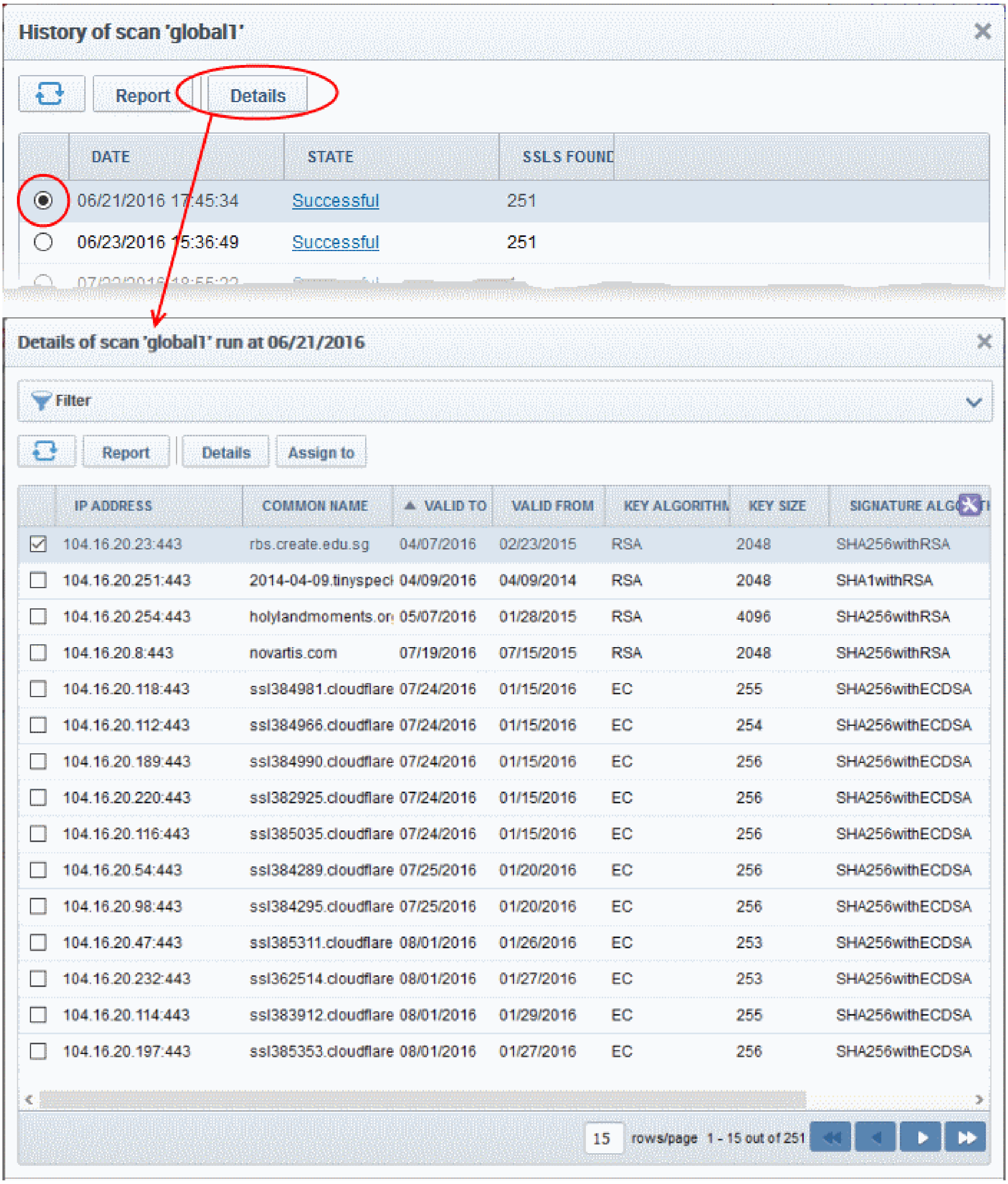
History of scan 'global1'

	DATE	STATE	SSLS FOUND
●	06/21/2016 17:45:34	Successful	251
○	06/23/2016 15:36:49	Successful	251
○	07/22/2016 18:55:22	Successful	1
○	08/10/2016 17:09:00	Successful	1

15 rows/page 1 - 4 out of 4

The 'History of scan...' dialog will be displayed.

- Click the 'Report' button to download all discovery scan reports as a .csv file.
- To view the list of certificates discovered during a scan, choose the scan and click the 'Details' button that appears at the top.



History of scan 'global1'

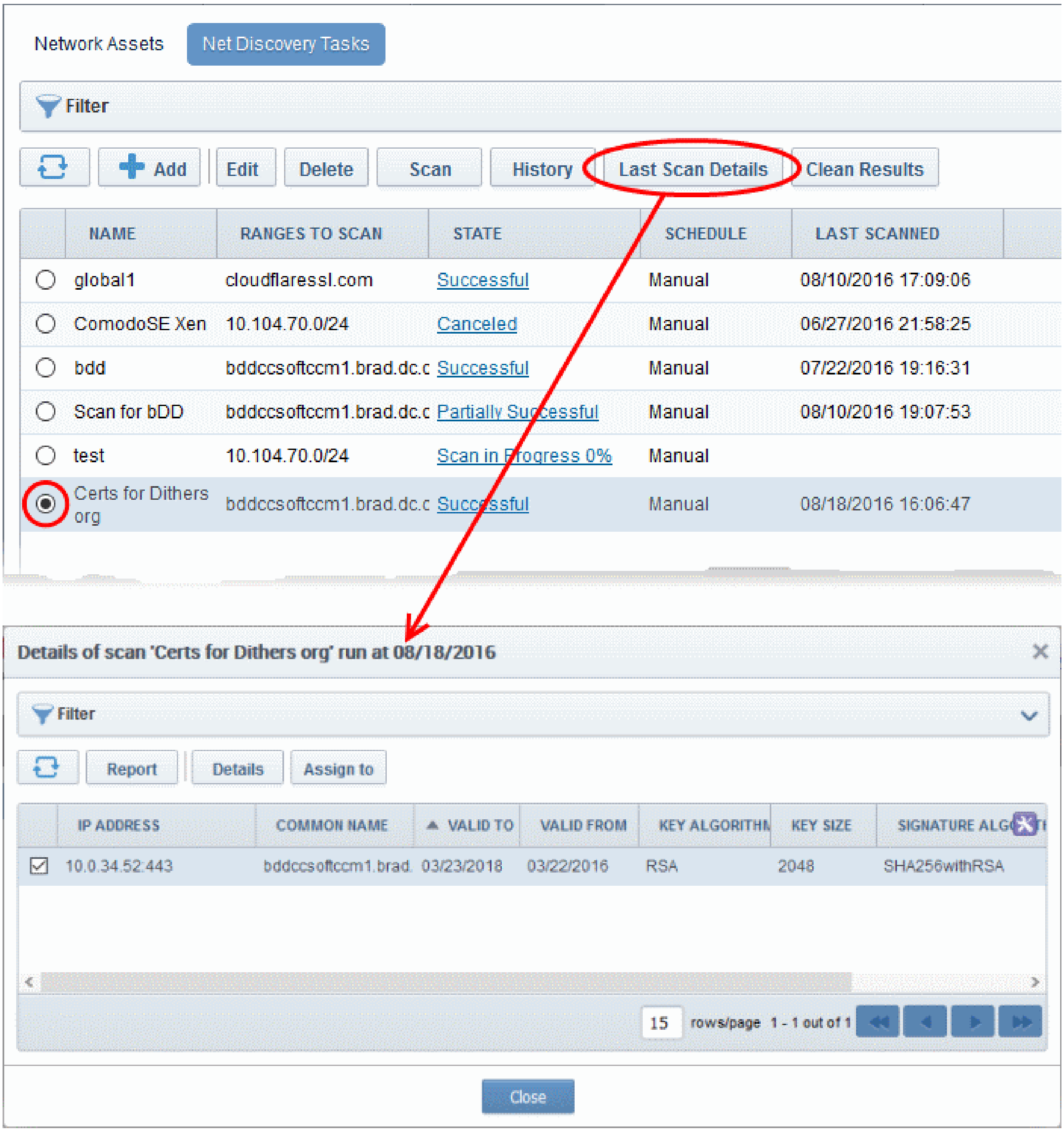
	DATE	STATE	SSLS FOUND
●	06/21/2016 17:45:34	Successful	251
○	06/23/2016 15:36:49	Successful	251

Details of scan 'global1' run at 06/21/2016

	IP ADDRESS	COMMON NAME	▲ VALID TO	VALID FROM	KEY ALGORITHM	KEY SIZE	SIGNATURE ALGO
☑	104.16.20.23:443	rbs.create.edu.sg	04/07/2016	02/23/2015	RSA	2048	SHA256withRSA
□	104.16.20.251:443	2014-04-09.tinyspeci	04/09/2016	04/09/2014	RSA	2048	SHA1withRSA
□	104.16.20.254:443	holylandmoments.or	05/07/2016	01/28/2015	RSA	4096	SHA256withRSA
□	104.16.20.8:443	novartis.com	07/19/2016	07/15/2015	RSA	2048	SHA256withRSA
□	104.16.20.118:443	ssl384981.cloudflare	07/24/2016	01/15/2016	EC	255	SHA256withECDSA
□	104.16.20.112:443	ssl384966.cloudflare	07/24/2016	01/15/2016	EC	254	SHA256withECDSA
□	104.16.20.189:443	ssl384990.cloudflare	07/24/2016	01/15/2016	EC	256	SHA256withECDSA
□	104.16.20.220:443	ssl382925.cloudflare	07/24/2016	01/15/2016	EC	256	SHA256withECDSA
□	104.16.20.116:443	ssl385035.cloudflare	07/24/2016	01/15/2016	EC	256	SHA256withECDSA
□	104.16.20.54:443	ssl384289.cloudflare	07/25/2016	01/20/2016	EC	256	SHA256withECDSA
□	104.16.20.98:443	ssl384295.cloudflare	07/25/2016	01/20/2016	EC	256	SHA256withECDSA
□	104.16.20.47:443	ssl385311.cloudflare	08/01/2016	01/26/2016	EC	253	SHA256withECDSA
□	104.16.20.232:443	ssl362514.cloudflare	08/01/2016	01/27/2016	EC	253	SHA256withECDSA
□	104.16.20.114:443	ssl383912.cloudflare	08/01/2016	01/29/2016	EC	255	SHA256withECDSA
□	104.16.20.197:443	ssl385353.cloudflare	08/01/2016	01/27/2016	EC	256	SHA256withECDSA

  - Click the 'Details' button to view full certificate information. See SSL Certificate 'Details' Dialog for more on the certificates details panel.
  - To manually assign unmanaged certificate(s) to an organization or department, select the certificate(s) and click the 'Assign to' button. For more on this, refer to Manually Assigning a Certificate to an Organization/Department in the section Network Discovery.
- Click the 'Last Scan Details' button to view the latest certificates discovered by a discovery task

The details of certificates discovered during the the last scan ran for the selected task will be displayed.



	NAME	RANGES TO SCAN	STATE	SCHEDULE	LAST SCANNED
○	global1	cloudflaressl.com	Successful	Manual	08/10/2016 17:09:06
○	ComodoSE Xen	10.104.70.0/24	Canceled	Manual	06/27/2016 21:58:25
○	bdd	bddccsoftccm1.brad.dc.c	Successful	Manual	07/22/2016 19:16:31
○	Scan for bDD	bddccsoftccm1.brad.dc.c	Partially Successful	Manual	08/10/2016 19:07:53
○	test	10.104.70.0/24	Scan in Progress 0%	Manual	
●	Certs for Dithers org	bddccsoftccm1.brad.dc.c	Successful	Manual	08/18/2016 16:06:47

Details of scan 'Certs for Dithers org' run at 08/18/2016

	IP ADDRESS	COMMON NAME	VALID TO	VALID FROM	KEY ALGORITHM	KEY SIZE	SIGNATURE ALGORITHM
☑	10.0.34.52:443	bddccsoftccm1.brad.	03/23/2018	03/22/2016	RSA	2048	SHA256withRSA

7.2.8 View Scan Results

After each discovery scan, Incommon Certificate Manager updates the lists of certificates in the Network Assets area and the 'SSL Certificates' area ('Certificates' > 'SSL' Certificates).

Certificates are assigned to these two areas as follows:

SSL Certificates interface

- Managed Certs
- Unmanaged certs which are assigned to an org/dep.

Network Assets interface

- Managed certs

- Unmanaged certs which are assigned to an org/dep.

- Unmanaged certs which are not assigned to an org/dep.

Network Assets Area:

The Network Assets area displays certificates discovered from all nodes of every scanned network, including web servers, domains and certificates discovered from AD servers integrated to InCommon CM.

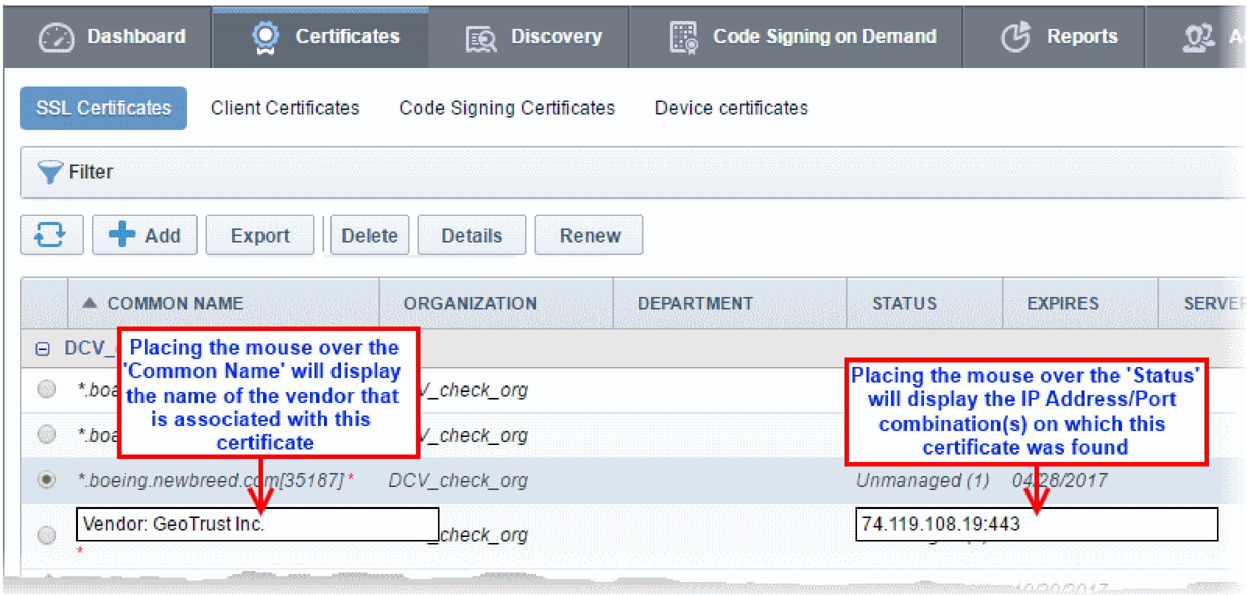
- **Network Discovery** - Displays a tree structure of scanned networks. Selecting a node displays all certificates identified on it, including managed certificates, unmanaged certificates that have been assigned to an organization/department by a rule, and unmanaged certificates that have not been assigned to a organization/department. You can view details of each certificate and manually assign unmanaged certificates to an organization or department. Doing so will grant them 'Managed' status and thus make them visible in the 'SSL Certificates' interface. See Network Discovery for more details.
- **Web Servers** - Displays a summary of all web-servers identified from every network scanned and a list of websites/domains hosted on each identified server. See Web Servers for more details.

SSL Certificates Area:

After a discovery scan, InCommon CM will add newly discovered 'unmanaged' certificates which have been assigned to an Org/Dep to the SSL certificates area. It will also update the status of any existing certificates. There are, therefore, two types of SSL certificates that could be discovered:

- **Certificates issued by InCommon Certificate Manager (also known as 'Managed' certificates).** InCommon Certificate Manager will simply update the certificate's 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 InCommon Certificate Manager (also known as 'Unmanaged certificates)** If the certificate was NOT issued by InCommon CM, they will be assigned '*Unmanaged'* status. The 'Unmanaged' category covers:
    - Self-signed certificates
    - Certificates issued by InCommon CA but not via InCommon Certificate Manager
    - Certificates issued by 3rd party vendors / other certificate authorities

Note: Only those 'Unmanaged' certificates that are assigned to an org/dep (either manually or by an assignment rule) will be added to the 'SSL Certificates' area at the end of a Discovery Scan. Discovered certificates which are not assigned to any organization or department will not be added to the SSL Certificates area. They can be viewed in the Network Assets interface.

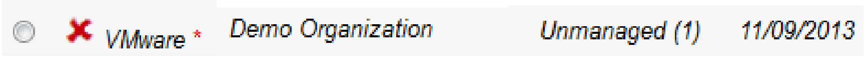
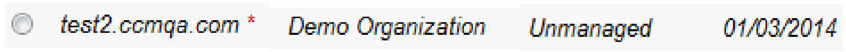


COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES
DCV_				
*.boa	_check_org			
*.boa	_check_org			
.boeing.newbreed.com[35187]	DCV_check_org		Unmanaged (1)	04/28/2017
Vendor: GeoTrust Inc.	_check_org		74.119.108.19:443	

Placing the mouse over the 'Common Name' will display the name of the vendor that is associated with this certificate

Placing the mouse over the 'Status' will display the IP Address/Port combination(s) on which this certificate was found

To bring an 'Unmanaged' certificate under the control of InCommon Certificate Manager you have to 'Renew' that certificate (to be more precise you will be effectively 'replacing' that certificate with an equivalent InCommon certificate). Clicking the 'Renew' button will begin the ordering process for new InCommon SSL certificate with the same parameters.

Certificate Type		View in the SSL Certificates Sub-Tab	
		State	View
Certificates, issued by CM		state listed here.	
Certificates, not issued by CM	*Self-signed certificates*	*Unmanaged*	 VMware * Demo Organization Unmanaged (1) 11/09/2013 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.) From the 'SSL Certificates' interface, you can: • View details of these certificates • 'Renew' these certificates by replacing them InCommon equivalents
	Issued by InCommon CA but not via CM	*Unmanaged*	 test2.ccmqa.com * Demo Organization Unmanaged 01/03/2014 From the 'SSL Certificates' interface, you can: • View details of these certificates • Revoke these certificates • 'Renew' these certificates
	Issued by 3rd party vendor	*Unmanaged*	 example.com Test Organization Unmanaged (1) 08/08/2015 From the 'SSL Certificates' interface, you can: • View details of these certificates • 'Renew' these certificates by replacing them InCommon equivalents

You can download the results of a discovery scan in .csv format in a Discovery Scan Log report from the Reports interface.

The Discovery Scan Log report contains information concerning overall scan options and discovered SSL certificates information.

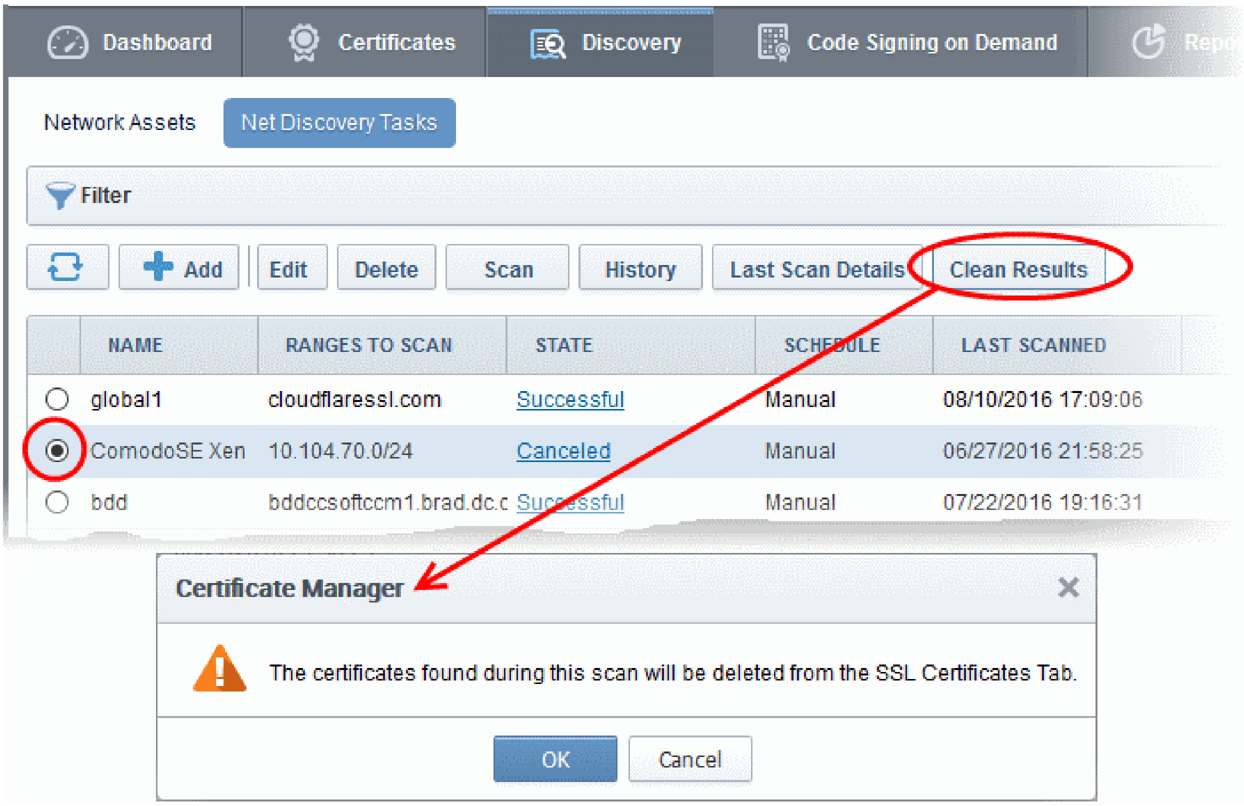
Incommon advises administrator to:

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 CM 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.



	NAME	RANGES TO SCAN	STATE	SCHEDULE	LAST SCANNED
○	global1	cloudflaressl.com	Successful	Manual	08/10/2016 17:09:06
●	ComodoSE Xen	10.104.70.0/24	Canceled	Manual	06/27/2016 21:58:25
○	bdd	bddccsoftccm1.brad.dc.c	Successful	Manual	07/22/2016 19:16:31

The certificates found during this scan will be deleted from the SSL Certificates Tab.

- Click 'OK' to confirm removal of the certificates in the SSL Certificates interface.

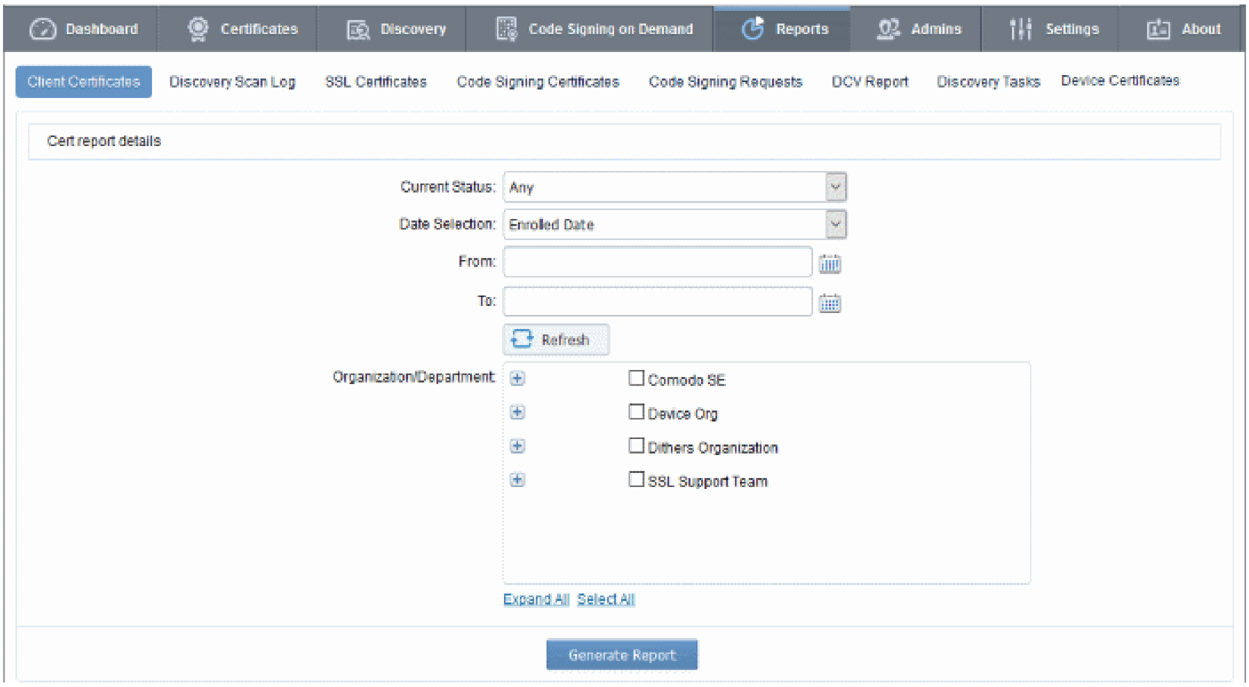
8 Reports

8.1 Overview

The 'Reports' interface lets you generate and view reports about the usage, provisioning and monitoring of all types of certificates. The following reports are available:

- The Client Certificates report - View a history of all events related to client certificates.
- The Discovery Scan Log - View information about scan options and discovered SSL certificates

- The [SSL Certificates] - View a history of all events related to SSL certificates.
- The Code Signing Certificates Report - View a history of all events related to code signing certificates.
- The Code Signing Request - View Code Signing on Demand (CSoD) requests and related activities.
- The DCV Report - MRAO and RAO/DRAO SSL admins can download a report on registered domains and their domain control validation (DCV) status.
- The Network Discovery Tasks - Report which allows MRAO and RAO/DRAO SSL administrators to view details of configured Net Discovery Tasks
- Administrators will find the reports especially useful when troubleshooting any issues related to the provisioning, installation and management of certificates.



Cert report details

Current Status: Any

Date Selection: Enrolled Date

From:

To:

Refresh

Organization/Department:
□ Comodo SE
□ Device Org
□ Dithers Organization
□ SSL Support Team

Expand All Select All

Generate Report

Note: The options available in the drop-down depend on the privilege level of the administrator that is logged in:

- RAO/DRAO SSL admins - can see Discovery Scan Log and SSL Certificates Logs, DCV Logs;
- RAO/DRAO S/MIME admins - can see only Client Certificates Logs;
- RAO/DRAO Code Signing admins - can see only Code Signing Certificates Logs.

Report Type	Description
Client Certificates	Enables RAO/DRAO S/MIME 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	Enables RAO/DRAO SSL administrators to view reports on the discovery scanning process. You can choose between a detailed or a summary report. Reports are delivered in .csv format. The reports can be further sorted by organization/department.
SSL Certificates	Enables RAO/DRAO SSL 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	Enables RAO/DRAO Code Signing 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.
Code Signing Requests	Enables RAO/DRAO Code Signing Administrators to view reports contianing the details of Code Signing on Demand (CSoD) requests and their activities. Reports are delivered in .csv format and can be filtered to show only certificates with a specific current status, namely: • Any (*all requests of any status*) • Created • In Progress • Declined • Signed • Expired • Failed The reports can be further sorted by organization/department, (status specific) Date and by Time Interval.

DCV Report	Enables 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, 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.
Net Discovery Tasks	Enables the RAO/DRAO SSL Administrators to generate reports on configured Discovery tasks. Reports are delivered in .csv format.

8.2 Reports - Security Roles Access Table

The following table provides a summary of the ability of the administrators to generate different types of reports.

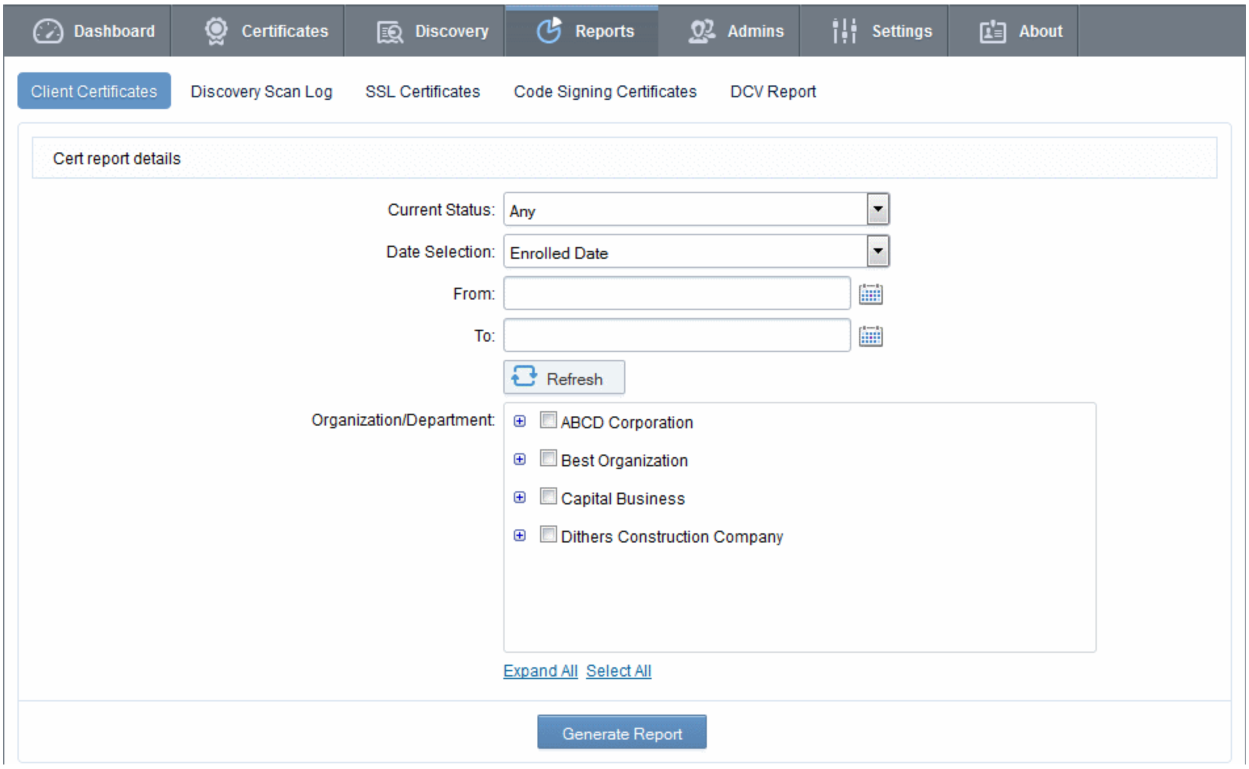
Report Type/Organization	RAO Administrator			DRAO Administrator		
	SSL	S/MIME	Code Signing	SSL	S/MIME	Code Signing
Report Type						
Client Certificates	✗	✓	✗	✗	✓	✗
Discovery Scan Log	✓	✗	✗	✓	✗	✗
SSL Certificates	✓	✗	✗	✓	✗	✗
Code Signing Certificates	✗	✗	✓	✗	✗	✓
Code Signing Requests	✗	✗	✓	✗	✗	✗
DCV Report	✓	✗	✗	✗	✗	✗
Net Discovery Tasks	✓	✗	✗		✗	✗
Scope	Can view reports for organizations (and any sub-			Can view reports for department that have been		

	ordinate departments) that have been delegated to them	delegated to them

8.3 Client Certificates Reports

'Client Certificates' reports allow RAO/DRAO S/MIME administrators to generate and view reports related to the usage, provisioning and monitoring of client certificates. Administrators are able to filter reports by certificate status.

Once the 'Client Certificates' type of reports is selected the following form appears:



Current Status: Any

Date Selection: Enrolled Date

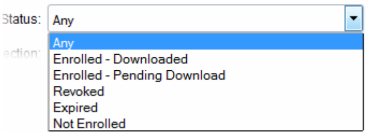
From:

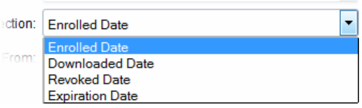
To:

Organization/Department:

- □ ABCD Corporation
- □ Best Organization
- □ Capital Business
- □ Dithers Construction Company

8.3.1 Report Type: Client Certificates - Table of Parameters

Form Element	Control	Description
Current Status	Drop-down list  Status: Any Any Enrolled - Downloaded Enrolled - Pending Download Revoked Expired Not Enrolled	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. • ***Enrolled*** - ***Downloaded*** - Generates a report of only those client certificates that have been successfully enrolled for by the end-user and subsequently downloaded. • ***Enrolled*** - Pending Download - Generates a report of only 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

Form Element	Control	Description
		have expired and are due for renewal. - ***Not Enrolled*** - Generates a report containing only those end-users that belong to an Organization and are listed in the 'Client Certificates' tab as a client certificate user but haven't enrolled for their client certificate.
Date Selection	Drop-down list  ction: Enrolled Date From: Enrolled Date Downloaded Date Revoked Date Expiration Date	- 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 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	Check-boxes	- 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 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.
Generate Report	Control	Starts the report generation.

8.4 Discovery Scan Log Reports

The 'Discovery Scan Log' option allows RAO/DRAO SSL administrators to generate and view log reports from discovery scans.

The administrator is able to select any one of the following two types of the Discovery Scan Log Reports:

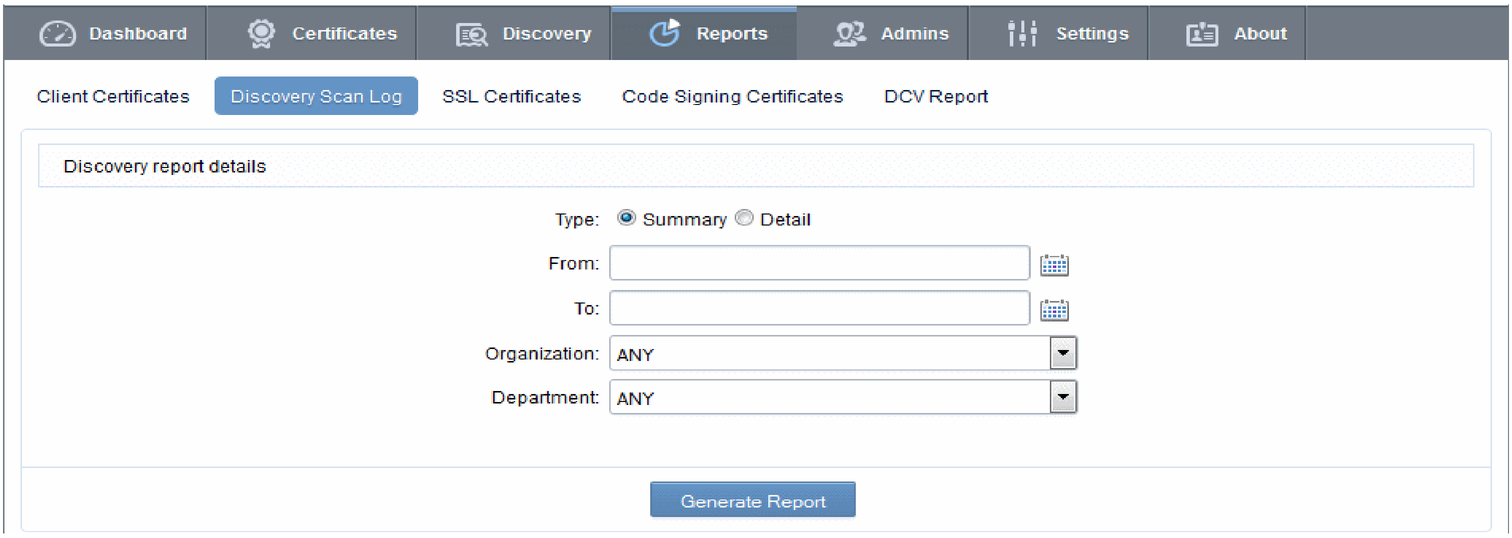
- Summary
- Detail

8.4.1 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;
- InCommon certificates Found;
- New InCommon 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.



Discovery report details

Type: ● Summary ○ Detail

From:

To:

Organization: ANY

Department: ANY

8.4.1.1 Report Type: Discovery Scan Log :Summary - Table of Parameters

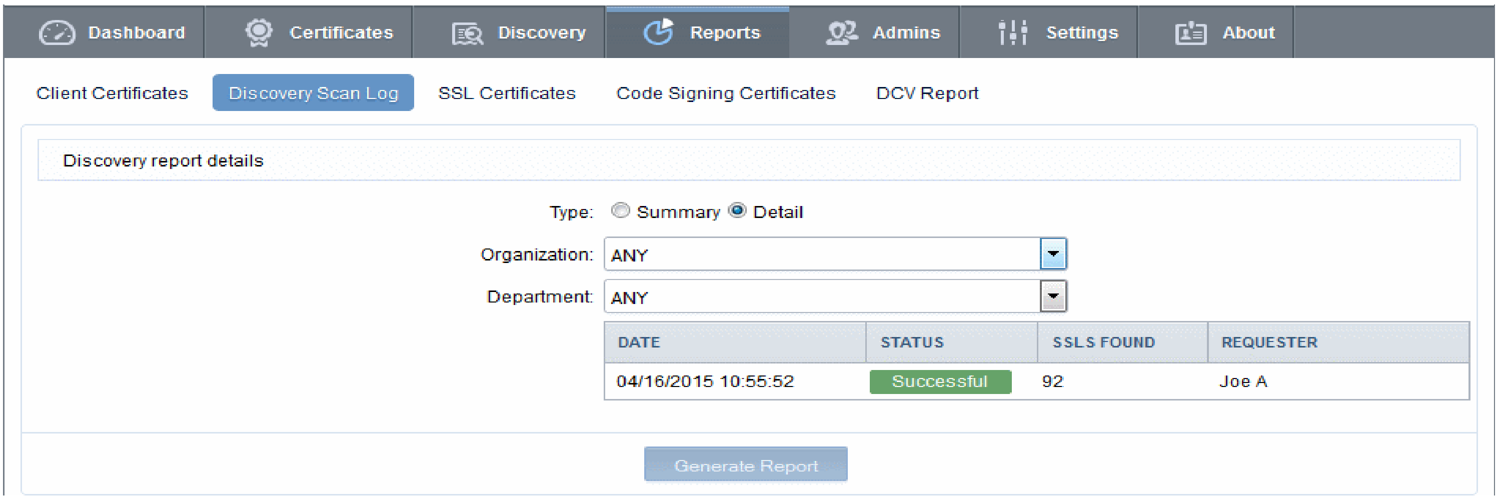
Form Element	Control	Description
Type	Radio buttons	Enables administrators to choose between a detailed report or a summary report. Both types are generated in .csv format.
Scan Date	Calendar buttons	• Enables the administrator to generate a report in .csv format for Discovery Scan Log for a specified time period. • Clicking 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.
Generate Report	Control	Starts the report generation

8.4.2 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.



Discovery report details

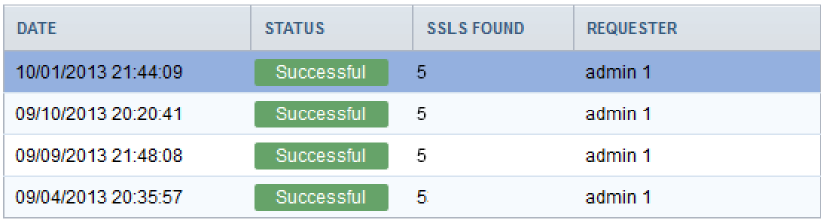
Type: ○ Summary ● Detail

Organization: ANY

Department: ANY

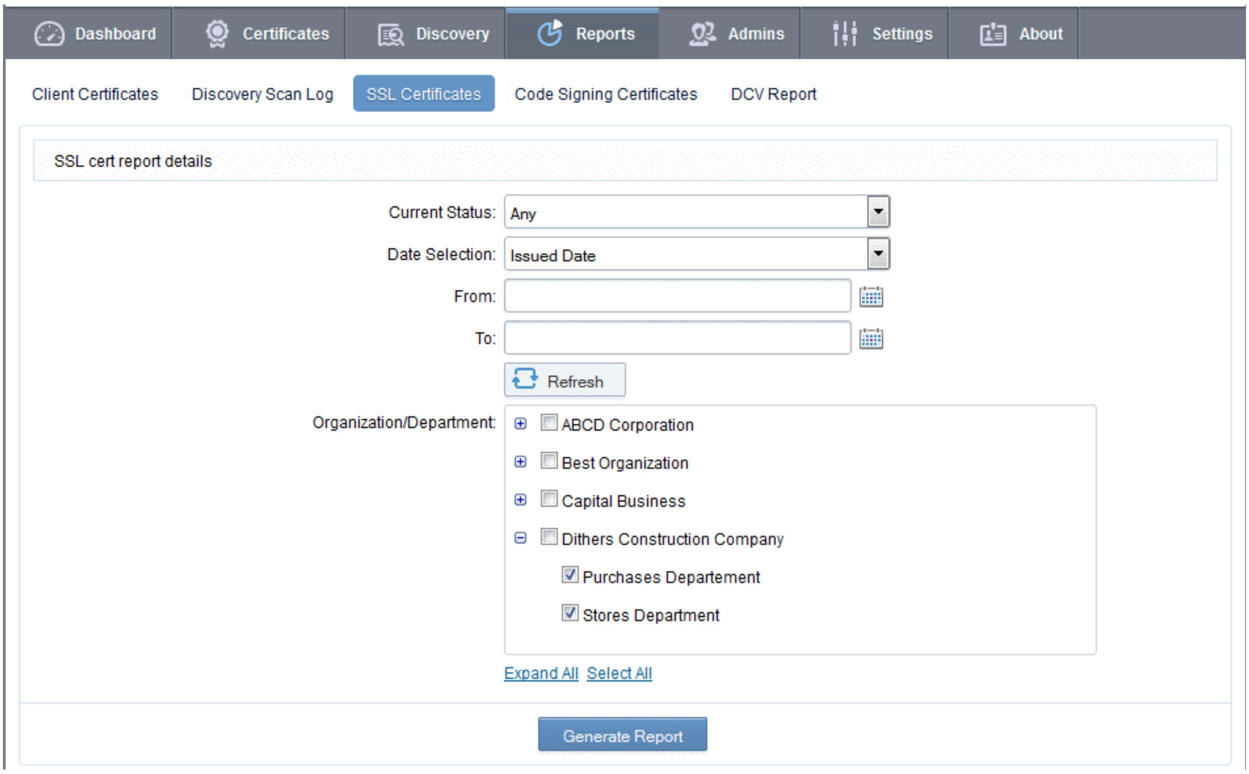
DATE	STATUS	SSLS FOUND	REQUESTER
04/16/2015 10:55:52	Successful	92	Joe A

8.4.2.1 Report Type: Discovery Scan Log :Detail - Table of Parameters

<table>
<tr><th>Form Element</th><th>Control</th><th>Description</th></tr>
<tr><td>Type</td><td>Radio buttons</td><td>Enables administrators to choose between a detailed report or a summary report. Both types are generated in .csv format.</td></tr>
<tr><td>Organization</td><td>Drop-down</td><td>• 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.</td></tr>
<tr><td>Department</td><td>Drop-down</td><td>• 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.</td></tr>
<tr><td>List of most recent scans</td><td></td><td>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 'Generate Report' button to generate the detailed report (.csv format).

<table>
<tr><th>DATE</th><th>STATUS</th><th>SSLS FOUND</th><th>REQUESTER</th></tr>
<tr><td>10/01/2013 21:44:09</td><td>Successful</td><td>5</td><td>admin 1</td></tr>
<tr><td>09/10/2013 20:20:41</td><td>Successful</td><td>5</td><td>admin 1</td></tr>
<tr><td>09/09/2013 21:48:08</td><td>Successful</td><td>5</td><td>admin 1</td></tr>
<tr><td>09/04/2013 20:35:57</td><td>Successful</td><td>5</td><td>admin 1</td></tr>
</table></td></tr>
<tr><td>Generate Report</td><td>Control</td><td>Starts the report generation.</td></tr>
</table>

8.5 SSL Certificates Reports

The 'SSL Certificates' option enables the 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:



SSL cert report details

Current Status: Any

Date Selection: Issued Date

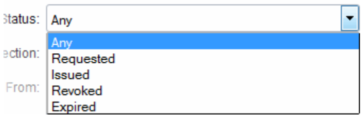
From:

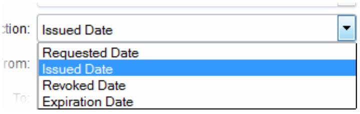
To:

Organization/Department:

- □ ABCD Corporation
- □ Best Organization
- □ Capital Business
- □ Dithers Construction Company
  - ☑ Purchases Departement
  - ☑ Stores Department

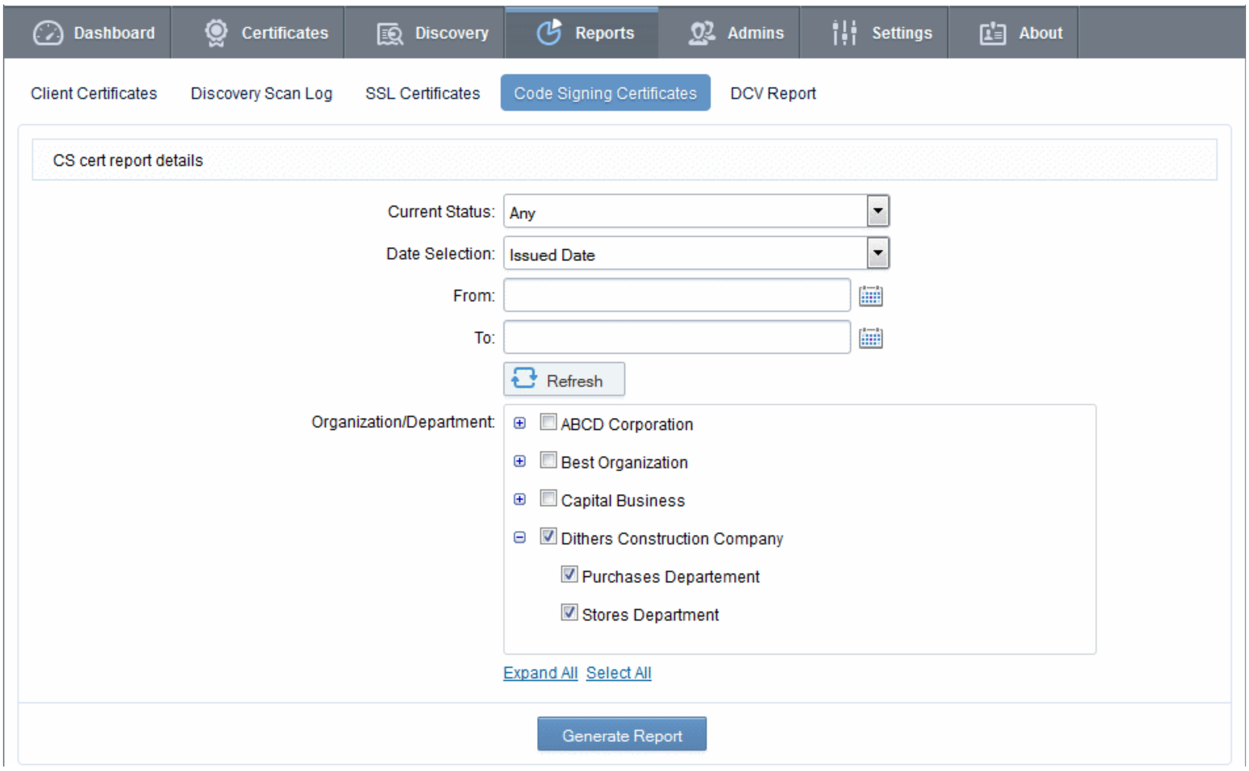
8.5.1 Report Type: SSL Certificates - Table of Parameters

Form Element	Control	Description
Current Status	Drop-down list  Status: Any Any Requested Issued Revoked Expired	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 certificates 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

Form Element	Control	Description
		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  tion: Issued Date rom: To: Requested Date Issued Date Revoked Date Expiration Date	- 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 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	Check-boxes	- 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 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 administrator to update the information in the form.
Generate Report	Control	Starts the report generation.

8.6 Code Signing Certificates Report

The 'Code Signing Certificates' option enables the 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:



CS cert report details

Current Status: Any

Date Selection: Issued Date

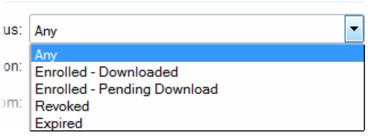
From:

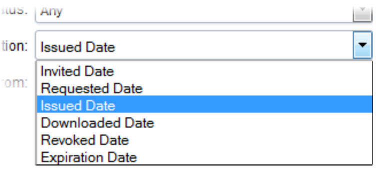
To:

Organization/Department:

- ⊞ □ ABCD Corporation
- ⊞ □ Best Organization
- ⊞ □ Capital Business
- ⊟ ☑ Dithers Construction Company
  - ☑ Purchases Departement
  - ☑ Stores Department

8.6.1 Report Type: Code Signing Certificates - Table of Parameters

Form Element	Control	Description
Current Status	Drop-down list  us: Any on: om: Any Enrolled - Downloaded Enrolled - Pending Download Revoked Expired	Enables administrator to generate a report in .csv format for Code Signing 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 Code Signing Certificates

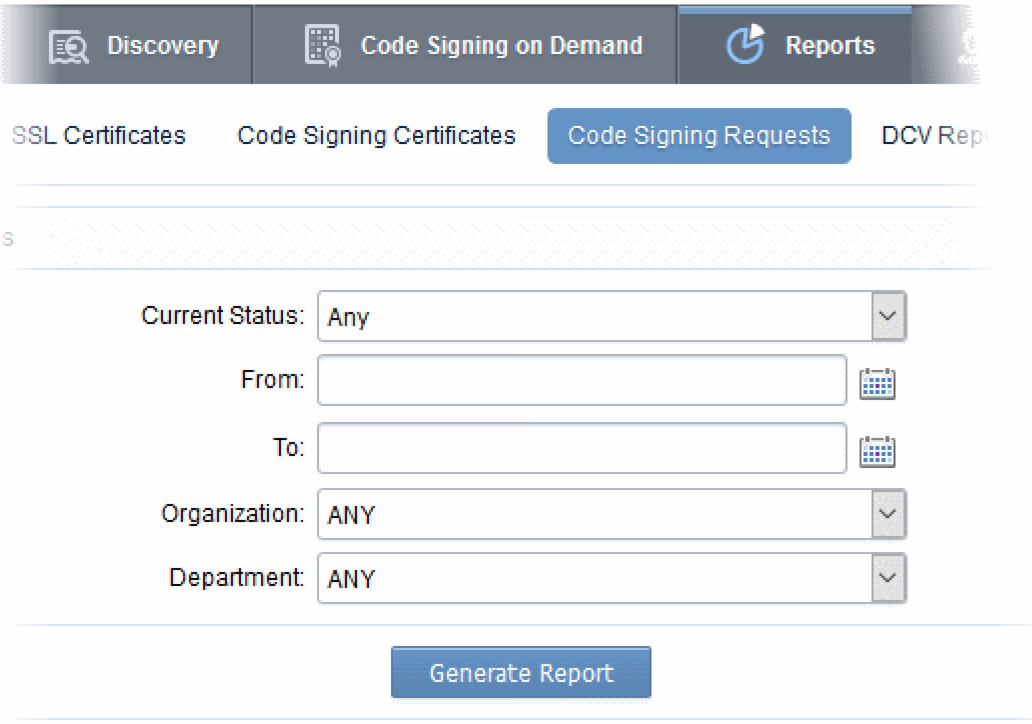
Form Element	Control	Description
		that have been revoked. • **Expired** - Generates a report only for Code Signing Certificates that have expired and are due for renewal.
Date Selection	Drop-down list  tus: Any tion: Issued Date om: Invited Date Requested Date Issued Date Downloaded Date Revoked Date Expiration Date	• 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 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	Check-boxes	• 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 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.
Generate Report	Control	Starts the report generation.

8.7 Code Signing Requests Report

The 'Code Signing Requests' tab enables the RAO/DRAO Code Signing administrators to generate and view reports that reflect an activity and other statistics related to requests made for Code Signing on Demand (CSoD) by developers enrolled for their Organizations/Departments. The administrator is able to filter the reports by the request status. The statuses can be Any, Created, In progress, Declined, Signed, Expired and Failed. Reports can also be filtered by Organization, status specific dates and time interval.

Note: The Code Signing Requests reports tab will be available only if CSoD feature is enabled for your account.

Once the 'Code Signing Requests' type of reports is selected the following form appears:



Current Status: Any

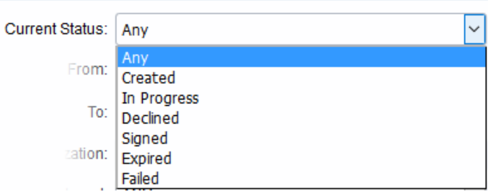
From:

To:

Organization: ANY

Department: ANY

8.7.1 Report Type: Code Signing Requests - Table of Parameters

Form Element	Control	Description
Current Status	Drop-down list  Current Status: Any Any Created In Progress Declined Signed Expired Failed	Enables administrator to generate a report in .csv format for Code Signing 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. • **Created** - Generates a report of those Code Signing Requests that are with 'Created' status. • **In progress** - Generates a report of those Code Signing Requests that are in progress status. • **Declined** - Generates a report of those Code Signing Requests that were declined by MRAO or RAO/DRAO Code Signing admins status.

Form Element	Control	Description
		• **Signed** - Generates a report of those Code Signing Requests that were declined by MRAO or RAO/DRAO Code Signing admins status. • **Expired** - Generates a report of those Code Signing Requests that were expired. • **Failed** - Generates a report of those Code Signing Requests that were failed.
Date Selection	Drop-down list	• Enables administrator to set a period for report generation. • Clicking 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.
Organization /Department	Drop-downs	• Enables the administrator to generate reports for specific organizations/departments. • If NO organization/department is selected, the report will be generated for all the organizations/departments, delegated to the specific administrator.
Generate Report	Control	Starts the report generation.

8.8 DCV Report

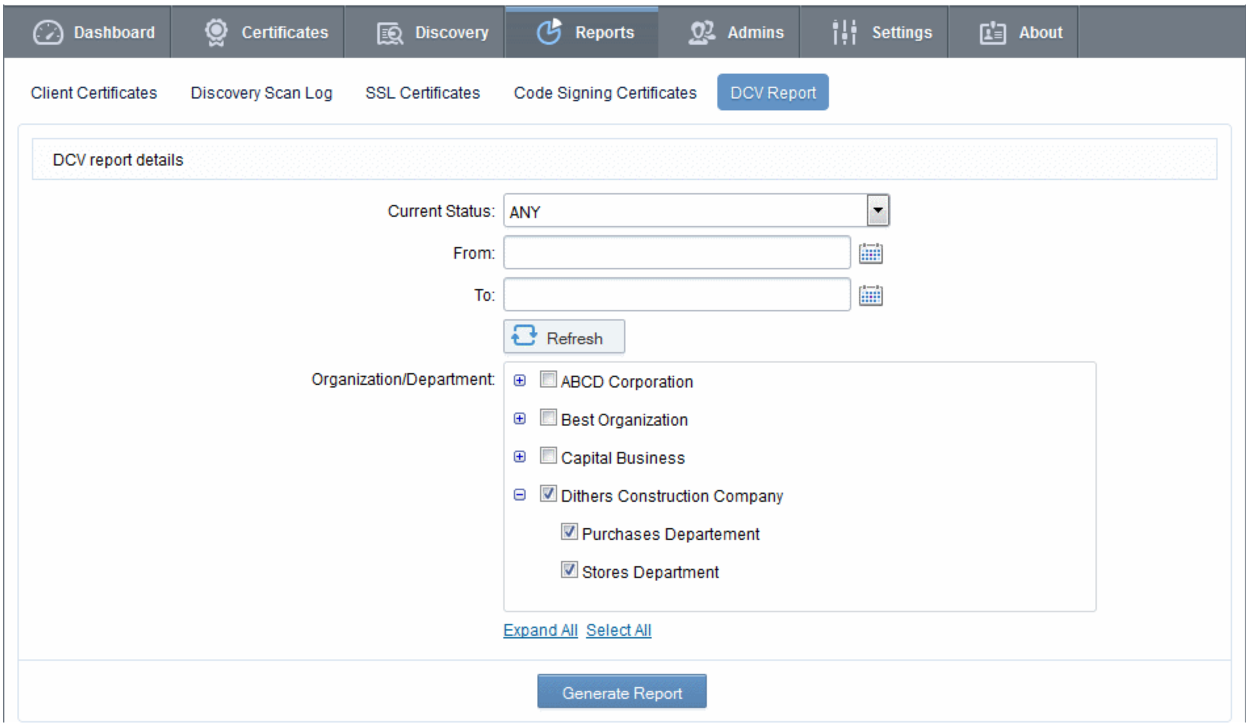
- The 'DCV Report' tab allows RAO/DRAO SSL admins to generate and view reports on the validation status of all domains. DCV = Domain Control Validation.

- DCV status can be 'Not Validated', 'Validated' and 'Expired'.

- DCV reports can be generated only for high-level domains if required.

- Reports can be filtered by validation status, organization/department and date.

- The following form appears if you select the 'DCV Report' type:



DCV report details

Current Status: ANY

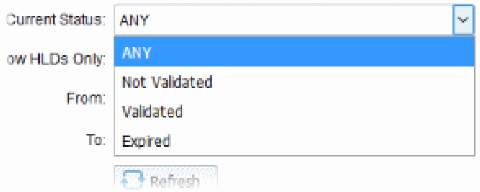
From:

To:

Organization/Department:

- □ ABCD Corporation
- □ Best Organization
- □ Capital Business
- ☑ Dithers Construction Company
  - ☑ Purchases Departement
  - ☑ Stores Department

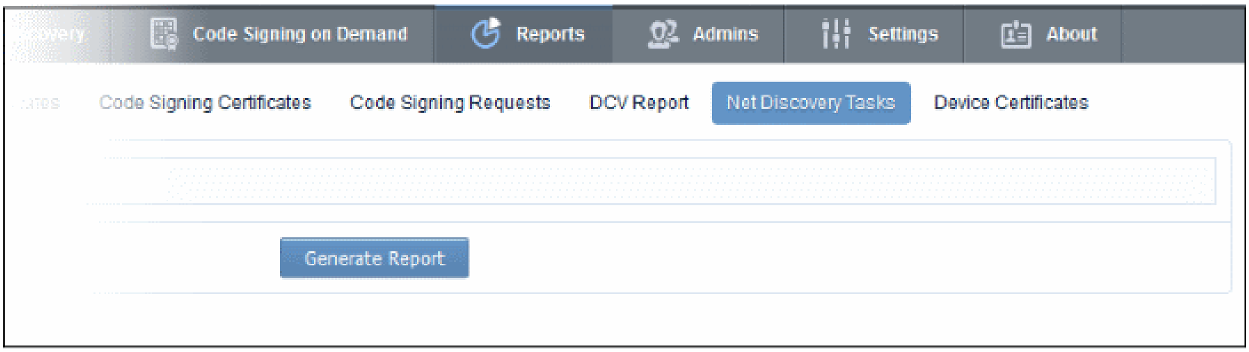
8.8.1 Report Type: DCV Report - Table of Parameters

Form Element	Control	Description
Current Status	Drop-down list  Current Status: ANY ow HLDs Only: From: To: ANY Not Validated Validated Expired Refresh	Generate a report on domains with a specific current DCV status: • **Any** – Creates a report on the validation status of every domain. • **Not Validated** - Report covers domains that have been added to Incommon CM but domain control validation has not been completed. • **Validated** - Report includes domains that have passed DCV, and for which DCV has not expired. New certificates can be ordered for these domains. • **Expired** - Report on domains where DCV has expired and needs to be renewed. DCV lasts for 1 year before it has to be renewed (re-run). All existing certificates issued to the domain will remain valid for their original terms. However, you will not be able to obtain new certificates for the domain until it passes DCV again.
Expiration Date		• The report will list the status of top level domains only. • For example, the report will cover example.com but will not cover subdomain.example.com • Note: If the high level domain has passed DCV then all sub-domains are also considered as validated.
Organization/Depa rtment	Check-boxes	• Generate a report on certificates for which DCV will expire within a specific time-frame. • Use the calendar buttons to select a date range.
Refresh	Control	• Generate a DCV report on domains which belong to a specific organization or department. • If multiple entities are selected then you will receive a single report that covers all selected organizations / departments. • Click Expand All to view the departments in an organization. • Click Select All to generate a report for ALL

		organizations that were assigned to that administrator. • If no selection is made here, the report will be generated for all orgs/depts delegated to the administrator.
Run	Control	Update the information in the form.
Generate Report	Control	Starts the report generation.

8.9 Discovery Tasks Report

- Click 'Reports' > 'Net Discovery Tasks' to open this interface
- The 'Net Discovery Tasks' tab allows admins to generate reports on discovery tasks.
  - RAO/DRAO admins can generate reports on discovery tasks configured for their org/dept.
- Click 'Generate Report' to create a discovery scan report. Reports are exported in .csv format

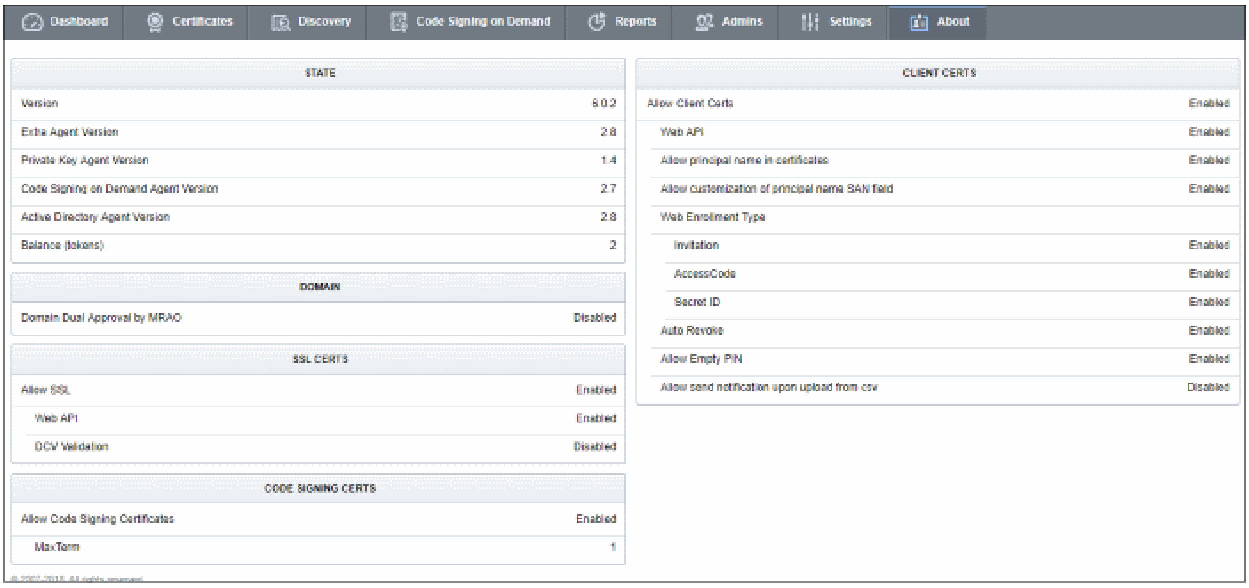


- Click 'Generate Report' to download the report in .csv format.

9 Version and Feature Information

The 'About' tab enables the administrator to view the Incommon CM version and the features that are enabled for the subscription.

- RAO admins - Can see features of the certificate types over which they have admin rights (RAO SSL, RAO Code Signing etc)
- DRAO admins - Can see features of the certificate types over which they have admin rights (DRAO SSL, DRAO Code Signing etc)



STATE	
Version	6.0.2
Extra Agent Version	2.8
Private Key Agent Version	1.4
Code Signing on Demand Agent Version	2.7
Active Directory Agent Version	2.8
Balance (tokens)	2

DOMAIN	
Domain Dual Approval by MRAO	Disabled

SSL CERTS	
Allow SSL	Enabled
Web API	Enabled
DCV Validation	Disabled

CODE SIGNING CERTS	
Allow Code Signing Certificates	Enabled
MaxTerm	1

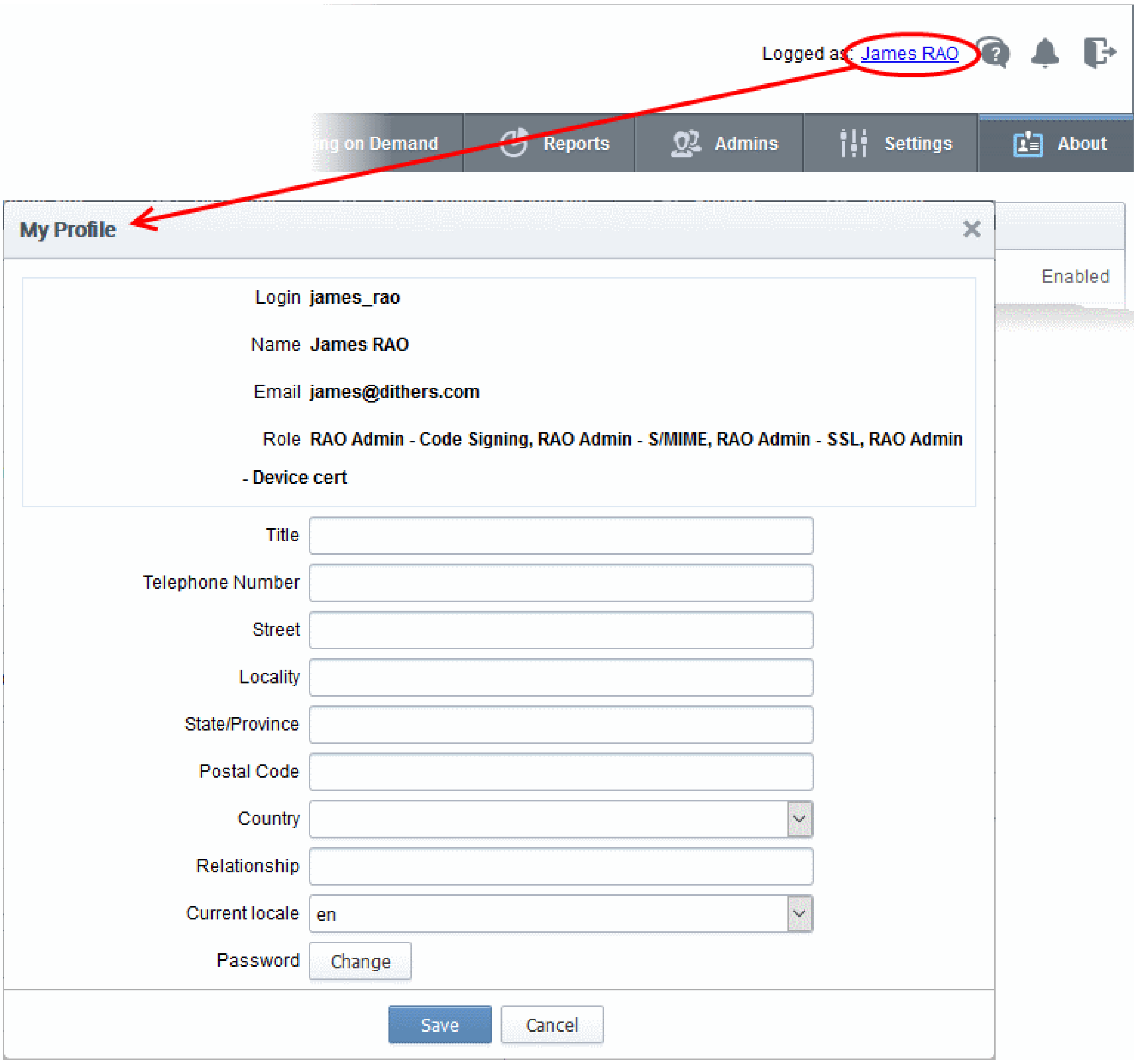
CLIENT CERTS	
Allow Client Certs	Enabled
Web API	Enabled
Allow principal name in certificates	Enabled
Allow customization of principal name SAN field	Enabled
Web Enrollment Type	
Invitation	Enabled
AccessCode	Enabled
Secret ID	Enabled
Auto Revoke	Enabled
Allow Empty PIN	Enabled
Allow send notification upon upload from csv	Disabled

© 2007-2018. All rights reserved

10 My Profile

The 'My Profile' area contains a details summary for the Administrator that is currently logged into InCommon Certificate Manager. 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 change the interface language and their password from this interface.

To access this interface, click the username text link beside the 'Logged as' label at the top right side of the interface.



My Profile

Login	james_rao
Name	James RAO
Email	james@dithers.com
Role	RAO Admin - Code Signing, RAO Admin - S/MIME, RAO Admin - SSL, RAO Admin - Device cert
Title	
Telephone Number	
Street	
Locality	
State/Province	
Postal Code	
Country	
Relationship	
Current locale	en
Password	Change

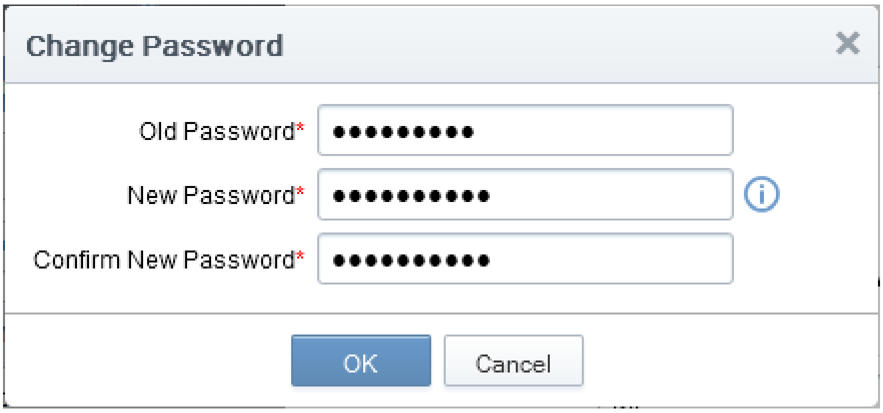
This area also allows the Administrator to edit the following details:

Address Details:

- Title
- Telephone Number
- Street
- Locality
- State/ Province
- Postal Code
- Country
- Relationship

Preferences:

- Interface Language - InCommon CM 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.
- Password - To change the administrators password, click the 'Change' button next to 'Password' label.

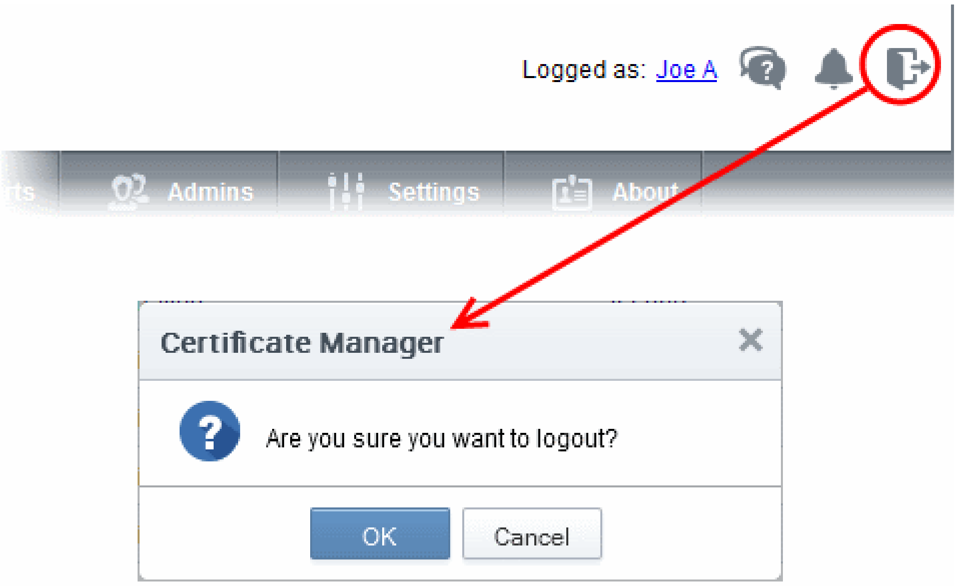


Hover the mouse cursor on the help button to view the password policy and change the password accordingly.

- Grid Settings - Click Reset to default to adjust the column widths and sorting preferences customized in various interfaces of InCommon CM to default values.

11 Logging out of InCommon Certificate Manager

Administrator can log out from the interface by clicking on the 'Logout' button located at the top right side of the interface.



Are you sure you want to logout?

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 InCommon and your Certificate Manager Account and could be a breach of the Certificate Manager Subscriber Agreement.

Appendix 2 - Simple Certificate Enrollment Protocol

Introduction

The Simple Certificate Enrollment Protocol (SCEP) is a mechanism for automating the requests of digital certificates. An administrator, by using SCEP, can automatically re-enroll and retrieve new digital certificates for the ones that are due to expire or expired. It was developed originally by Cisco Systems for use in network devices such as routers, but its use has expanded to other hardware and software devices.

A recent example of a SCEP-capable system would be Apple's iOS platform and the devices that run it (iPhone, iPad, iPod Touch).

InCommon CM supports SCEP and is integrated with a fully-compliant SCEP server. This document describes the settings required to access and use InCommon CM as a SCEP server to enroll certificates.

Note: SCEP can only be used by third-party software that requests certificates using the SCEP protocol. If you are considering creating a custom certificate application, the InCommon CM APIs may be a better choice, as they are easier to use and support additional functionality not available through SCEP.

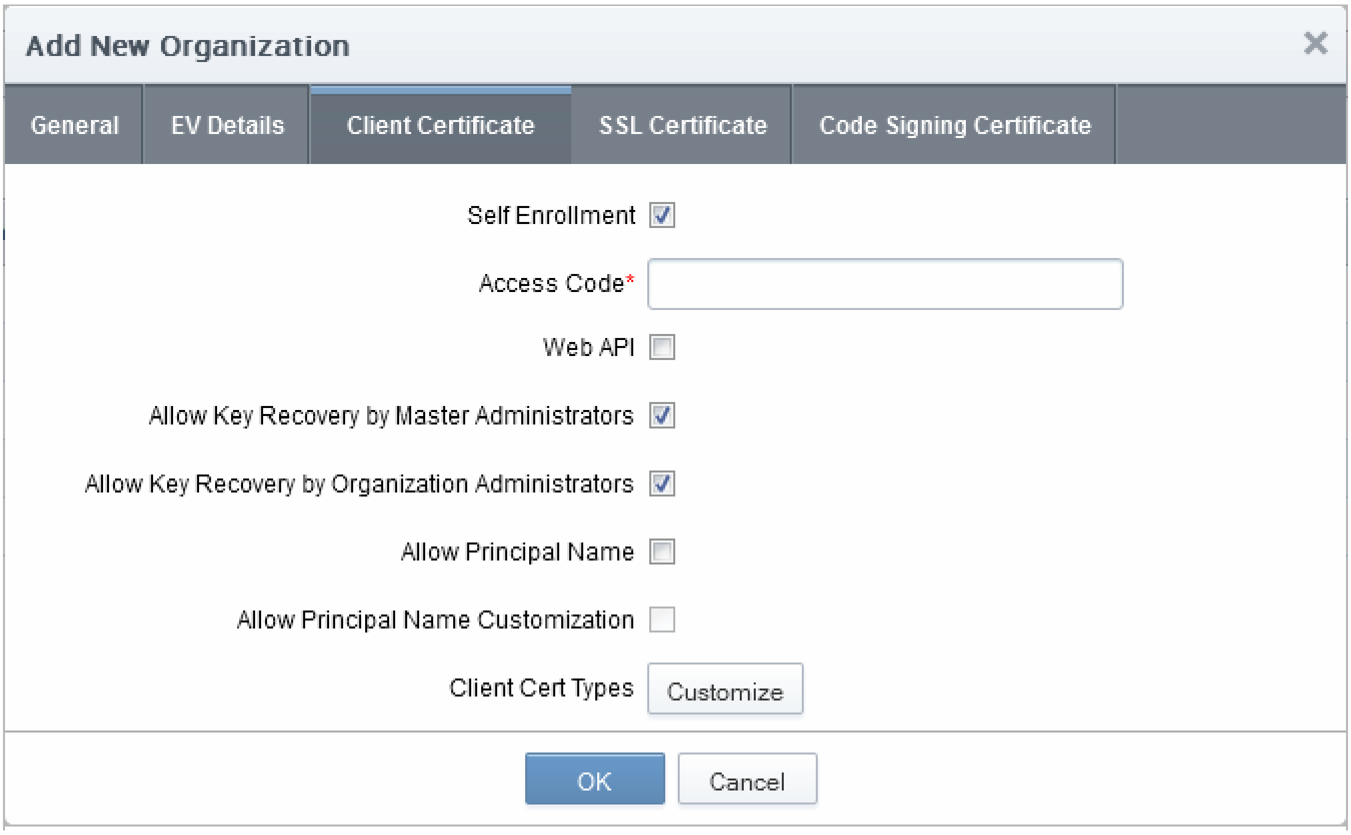
Settings

1. Enabling Self-Enrollment and Setting Access Code

Users can download certificates through SCEP only if Self-Enrollment is enabled and access code set in InCommon CM. This can be done while adding a new Organization/Department or editing Organization/Department by the Master Administrator or the RAO Administrator.

To enable self-enrollment and set access code for Organizations:

- In the 'Organizations' screen, click the 'Add' button or the 'Edit' button beside an existing Organization.
- In the 'Add New Organization' or 'Edit Organization' dialog, click the 'Client cert' tab.



Self Enrollment ☑

Access Code*

Web API □

Allow Key Recovery by Master Administrators ☑

Allow Key Recovery by Organization Administrators ☑

Allow Principal Name □

Allow Principal Name Customization □

Client Cert Types Customize

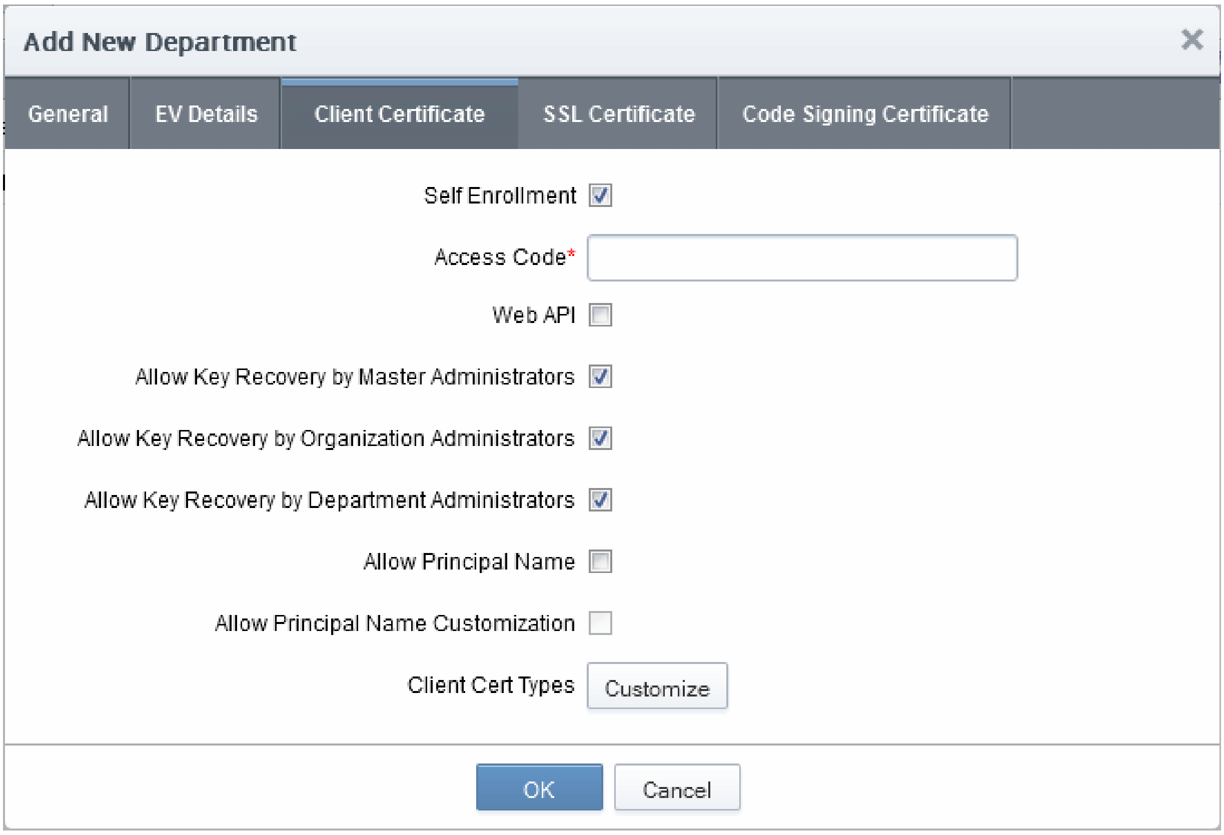
- Select the Self Enrollment checkbox.

The Access Code field will appear.

- Enter the access code in the field. This should be a mixture of alpha and numeric characters that cannot easily be guessed.
- Click 'OK'.

To enable self-enrollment and set access code for Departments:

- In the 'Organizations' screen, click the respective 'Department' button beside an Organization for which you want to enable self-enrollment and set access code.
- In the 'Departments' dialog, click the 'Add' button or the 'Edit' button beside an existing Department.
- In the 'Add New Department' or 'Edit Department' dialog, click the 'Client cert' tab.



Self Enrollment ☑

Access Code*

Web API □

Allow Key Recovery by Master Administrators ☑

Allow Key Recovery by Organization Administrators ☑

Allow Key Recovery by Department Administrators ☑

Allow Principal Name □

Allow Principal Name Customization □

Client Cert Types Customize

- Select the Self Enrollment checkbox.

The Access Code field will appear.

- Enter the access code in the field. This should be a mixture of alpha and numeric characters that cannot easily be guessed.
- Click 'OK'.

To view the access code that is already set for Organizations/Departments, click the 'Edit' button beside the respective Organization/Department. You can view the access code under the 'Client cert' tab. DRAO administrator cannot set and view access codes and must consult RAO administrator to find access code.

Note: The same access code should be entered in the 'challengePassword' field during the process of creating Certificate Signing Request. See section Certificate Signing Request for more details.

2. **URL of the SCEP server**

For S/MIME certificate:

http://cert-manager.com/customer/InCommon/scep/smime/pkiclient.exe

For SSL certificate:

http://cert-manager.com/customer/InCommon/scep/ssl/pkiclient.exe

The URL of the SCEP server must be entered into the user's SCEP client software - not typed into a browser. It tells the client software where to send the SCEP requests. Properly formatted SCEP request are sent to this URL.

Note 1: The URI protocol should be 'http' and not 'https', since the SCEP protocol relies on signed messages during a transaction and so operates over 'http'.

Note 2: Private keys for certificates obtained using SCEP cannot be escrowed as the private key is never sent to CM.

3. Certificate Signing Request

The Certificate Signing Request (CSR) requires the following:

- Key size - A minimum of 2048 bit.
- Subject information - Client certs need a minimum of CN and emailAddress.
- The subject CN (server certificates) must be an allowed domain, or the emailAddress (client certificates) must lie in an allowed domain for that Organization or Department.
- The CSR **requires** a 'challengePassword' to be set. This should be set to the 'Access Code' from within InCommon CM for the Organization or Department the certificate is being enrolled into. See section Enabling Self-Enrollment and Setting Access Code for more details on setting access code.

Tips for using SCEP in InCommon CM for iOS devices:

On some older versions of iOS (4.x), setting the RSA Key Size in the mobileconfig file at 4096 may be required, as it appears iOS will sometimes generate 2047 bit keys (when 2048 bit is chosen), which will not be accepted by InCommon CM or the CA.

In the nested-arrays for the Subject information in the mobileconfig, it may be necessary to use the OID for the 'emailAddress' field - 1.2.840.113549.1.9.1.

The 'challengePassword' can be set using the 'Challenge' key/value pair in the mobileconfig.

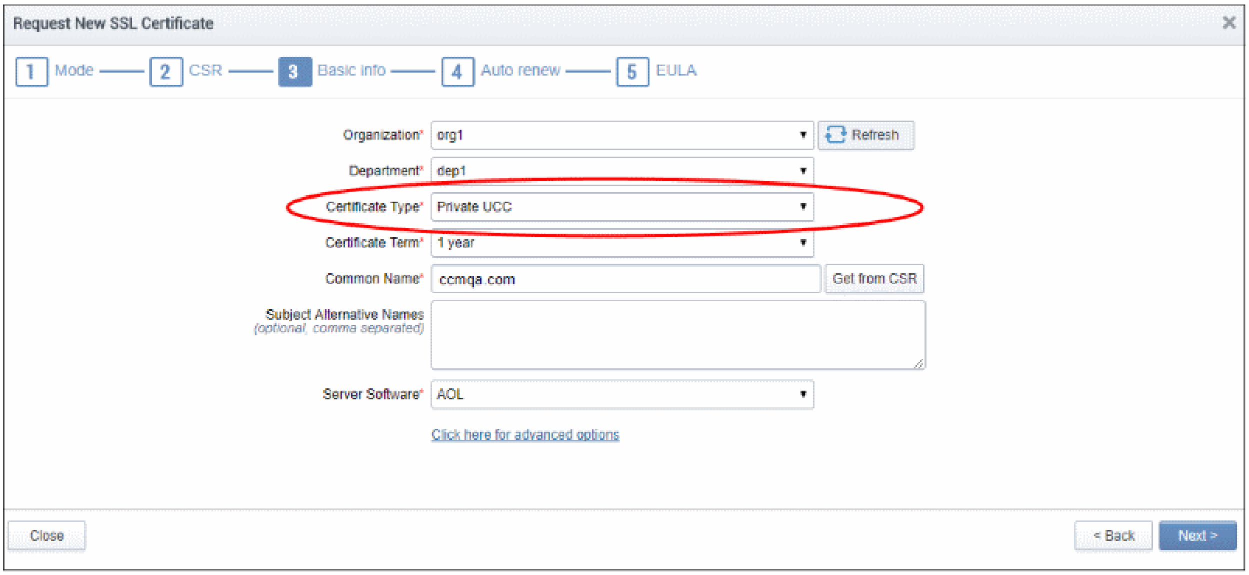
Appendix 3 - Private Certificates for Internal Hosts

Many companies use publicly trusted SSL certificates from a certificate authority (CA) to secure internal hosts, reserved IP addresses and intranets. However, after November 1st 2015 CA's are no longer able to issue publicly trusted certificates that contain internal names. By November 1st 2016, all such certificates must be revoked. Companies that rely on these publicly trusted certificates for internal services risk service disruption, error messages, user confusion and loss of security.

Private SSL certificates offer continuity by allowing businesses to continue using internal certificates with non-registered names. Under our Private CA system, InCommon will help you create your own private root certificate which is capable of signing end-entity certificate for all your internal servers and users. Once enabled, Private Certificates can be ordered by choosing 'Private UCC' when requesting a new certificate:

Private certificates use the same key sizes, signing algorithms, validity periods and CA protections as public certificates. After issuance, they can be managed, tracked and installed via InCommon CM just like any other certificate type.

Features in brief:



Request New SSL Certificate

Organization*	org1
Department*	dep1
Certificate Type*	Private UCC
Certificate Term*	1 year
Common Name*	ccmqa.com
Subject Alternative Names (optional, comma separated)	
Server Software*	AOL

- Create a private root for your company which is used to sign all internal server certificates
- Avoid the complexity, expense and risk involved with setting up an internal CA
- InCommon CM discovers all internal certificates on company networks and allows you to seamlessly replace them
- InCommon expertly supports your deployment and makes sure your certificates are always in compliance with future regulations