InCommon Certificate Manager

Version 6.1

Quick Start Guide
Release Date: January 17th, 2018

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

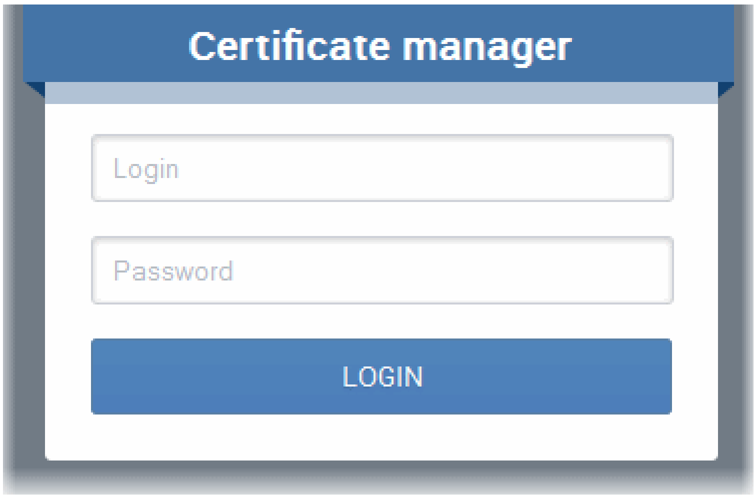
InCommon Certificate Manager - Quick Start Guide

This tutorial briefly explains how an administrator can setup InCommon Certificate Manager then issue and manage SSL, Client and Code Signing certificates.

The guide will take you through the following processes - click on any link to go straight to that section as per your current requirements.

Step 1 - Log in to InCommon CM

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



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

If you are not able to login, please raise a support ticket at the InCommon Partner Comodo Support portal by clicking the 'Support' link (requires account creation).

You may be prompted to change your password after logging in for the first time.

Tip: You can change your password at any time from the 'My Profile' dialog. You can access this dialog by clicking your username at the top-right of the interface.

Step 2 - Create Organizations and Departments

Any certificate ordered through InCommon CM must be assigned to an 'Organization'. Each organization can have multiple departments. Once created, you can assign domains and administrators to specific organizations or departments. Organizations are typically managed by a Registration Authority Officer (RAO) administrator while departments are typically managed by a Domain Registration Authority Officer (DRAO). A Master Registration Authority Officer (MRAO) manage all organizations and all departments.

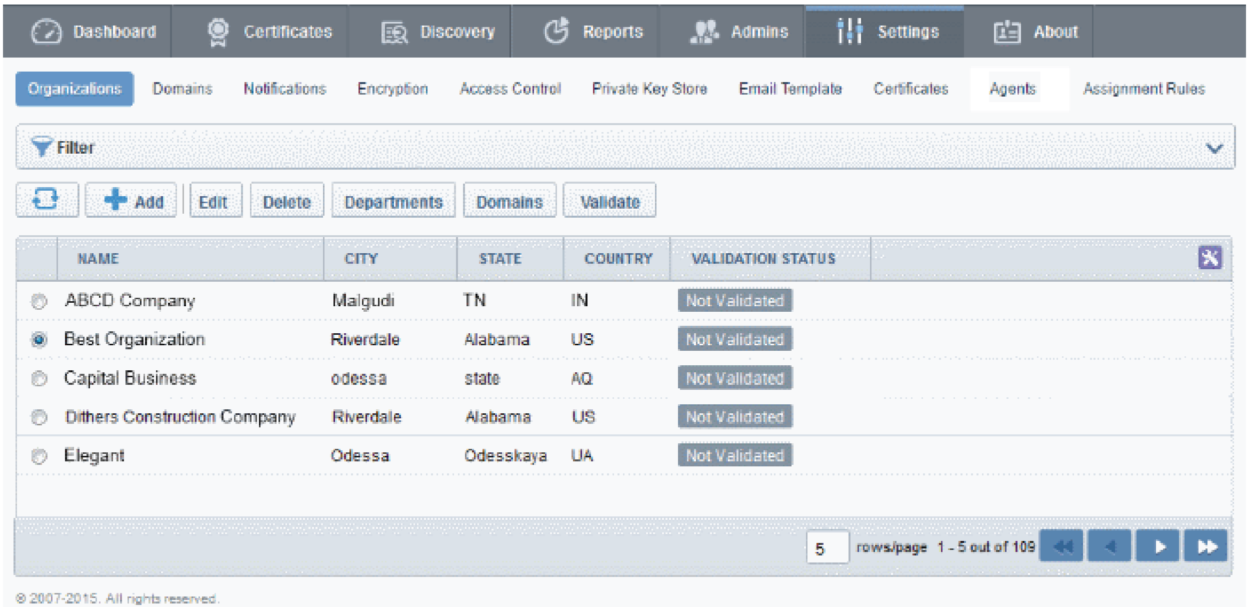
Once an organization or department has been created:

- Appropriately privileged officers can request and delegate domains to that Organization/Department
- Appropriately privileged officers can request, approve/decline requests and manage certificates on behalf of that Organization or Department.
- End-users can enroll into (or be assigned membership of) that Organization or Department and be provisioned with client certificates
- Administrators can run a certificate discovery scan on their networks. All discovered certificates will be assigned to the Organization you specify during scan configuration.

You are advised to plan the Organization/Department structure you'd like. All certificates that are newly applied or pre-installed in the network and identified by discovery scans are automatically assigned to an Organization or Department. These named entities will feature in the 'O' and 'OU' fields of your issued certificate. Once issued, you cannot 'reassign' a certificate to the auspices of another Organization in InCommon CM.

To create an Organization

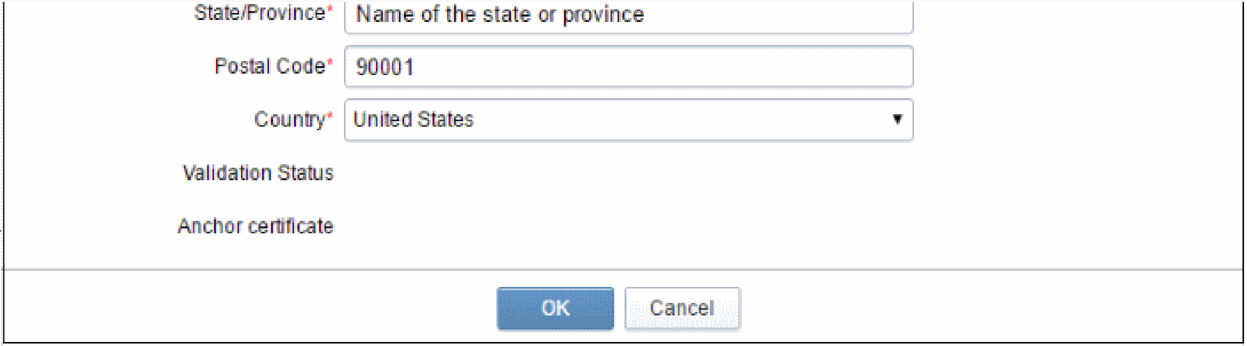
- Open the 'Organizations' management area by clicking the 'Settings' tab and then clicking 'Organizations' sub-tab.



	NAME	CITY	STATE	COUNTRY	VALIDATION STATUS
○	ABCD Company	Malgudi	TN	IN	Not Validated
●	Best Organization	Riverdale	Alabama	US	Not Validated
○	Capital Business	odessa	state	AQ	Not Validated
○	Dithers Construction Company	Riverdale	Alabama	US	Not Validated
○	Elegant	Odessa	Odesskaya	UA	Not Validated

5 rows/page 1 - 5 out of 109

© 2007-2015. All rights reserved.

- 

State/Province*	Name of the state or province
Postal Code*	90001
Country*	United States ▾
Validation Status	
Anchor certificate	

The 'Add New Organization' dialog contains six tabs. At this point you need only complete the 'General' tab to create the Organization - but should review the other tabs prior to requesting certificates.

- General - Allows you to configure high level details relating to the new Organization. (Mandatory)
- EV Details - Provide additional company details which are required for the validation of EV certificates for the Organization. (Optional)
- Client Certificate - Configure enrollment and term settings relating to S/MIME (email and client) certificates issued to end-users belonging to the Organization or Department (Optional)
- SSL Certificate - configure enrollment and term settings related to SSL certificates issued to the domains associated with the Organization (or Department of the Organization). (Optional)
- Code Signing Certificate- Allows you to enable or disable issuance of code signing certificates issued to end-users belonging to the Organization (or Department of the Organization) . (Optional)

This section explains the configuration parameters under the 'General' tab. The configuration of individual certificate settings for the Organization is optional. Refer to the section 'Organization Management' in the administrator guide for more details.

General Settings

Field Name	Description
Organization Name	The name of the Organization to be created.
Address 1	Organization's address (used for issuing SSL and S/MIME certificates)
Address 2	Organization's address (used for issuing SSL and S/MIME certificates)
Address 3	Organization's address (used for issuing SSL and S/MIME certificates
City	City where the Organization is located (used for issuing SSL and S/MIME certificates)
State/Province	State or province (used for issuing SSL and S/MIME certificates)
Postal Code	Postal code (used for issuing SSL and S/MIME certificates)
Country	Two characters country code (used for issuing SSL and S/MIME certificates)
Validation Status	Indicates the progress of Organizational Validation (OV) on the 'Organization' in question. States can be 'Not validated', 'Validated', 'Pending', 'Failed', 'Expired'. The Validation Status will be displayed only if OV certificates are enabled for your account.
Anchor Certificate	Indicates the status of Anchor certificate. The Anchor Certificate is issued after the Organization Validation is completed. This is used as a reference for Organization Validation status by

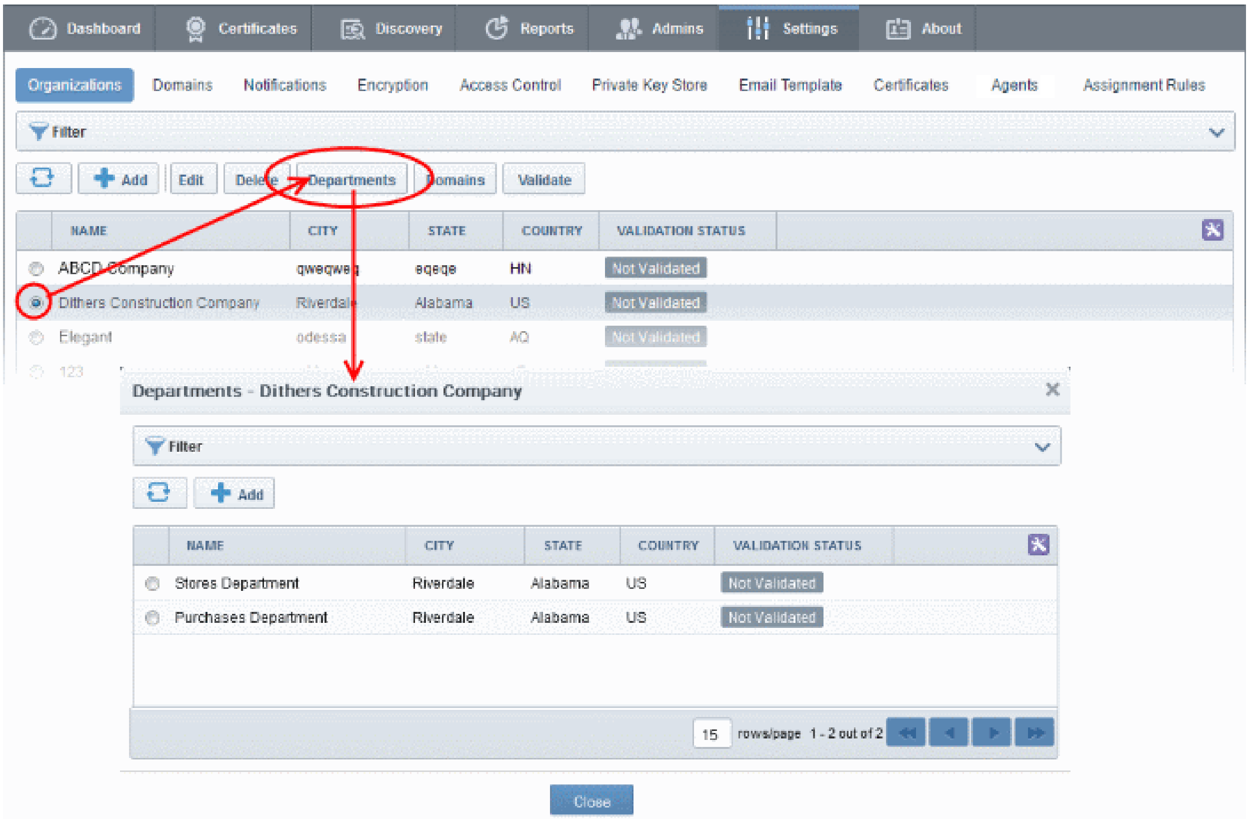
	InCommon CM whenever an OV SSL certificate is requested for the Organization or Departments under it. The Anchor Certificate field will be displayed only if OV certificates are enabled for your account.

- Enter the parameters as explained above and click 'OK'.

The Organization will be added to the list under the 'Organizations' sub-tab. You can repeat the process to add more Organizations'.

To add a Department under an Organization

- Open the 'Organizations' management area by clicking the 'Settings' tab then select the 'Organizations' sub-tab.
- Choose the Organization from the list and then click the 'Departments' button that appears at the top.

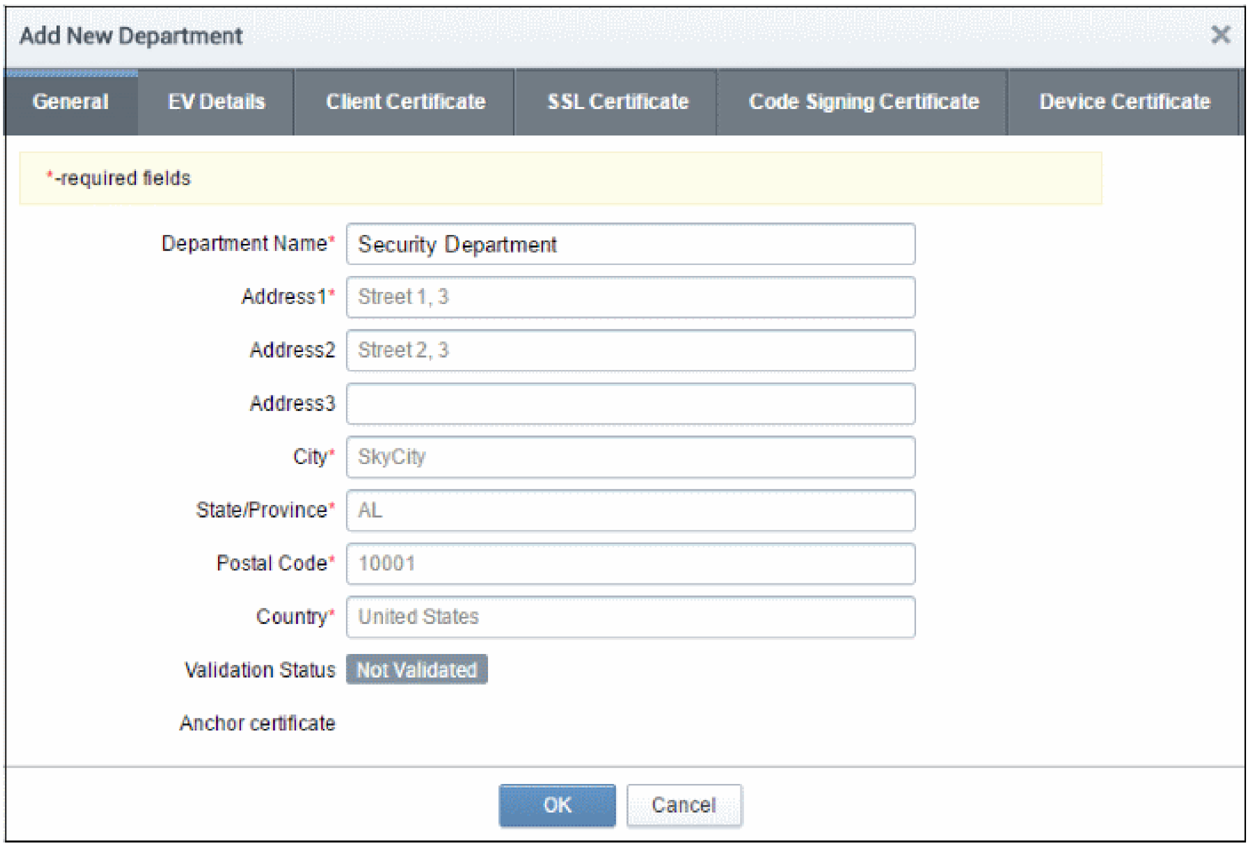


NAME	CITY	STATE	COUNTRY	VALIDATION STATUS
ABCD Company	qweqweq	eqeqe	HN	Not Validated
Dithers Construction Company	Riverdale	Alabama	US	Not Validated
Elegant	odessa	state	AQ	Not Validated
123				

Departments - Dithers Construction Company

NAME	CITY	STATE	COUNTRY	VALIDATION STATUS
Stores Department	Riverdale	Alabama	US	Not Validated
Purchases Department	Riverdale	Alabama	US	Not Validated

- Click the 'Add' button



Add New Department

*-required fields

Department Name*	Security Department
Address1*	Street 1, 3
Address2	Street 2, 3
Address3	
City*	SkyCity
State/Province*	AL
Postal Code*	10001
Country*	United States
Validation Status	Not Validated
Anchor certificate	

The 'Add New Department' dialog will open. This interface is similar to 'Add New Organization' dialog. The settings made here will apply only to the new Department. Repeat the process to add more Departments under the Organization.

Step 3 - Run a Discovery Scan for SSL certificates installed on Organization/Department network

A discovery scan will identify all existing certificates on your network and import them into InCommon CM for further management. Discovered certificates are given 'Unmanaged' status, which means they were not ordered through InCommon CM. Once imported, you can easily renew or replace discovered certificates with InCommon equivalents.

You are advised to create the Organization/Department structure you'd like before creating and running a discovery scan. On completion of a discovery scan, all identified certificates will be automatically assigned to the Organization/Department configured in the discovery task. The administrators in charge of the organization/department will then receive notifications relevant to the certificate (for example, certificate expiry reminders).

InCommon advises you run a scan at the earliest opportunity so that you gain a firm inventory of your company's certificate assets. Discovery scans are, however, optional at this stage and can be run at anytime. You can skip to step 4 if you wish to do this later.

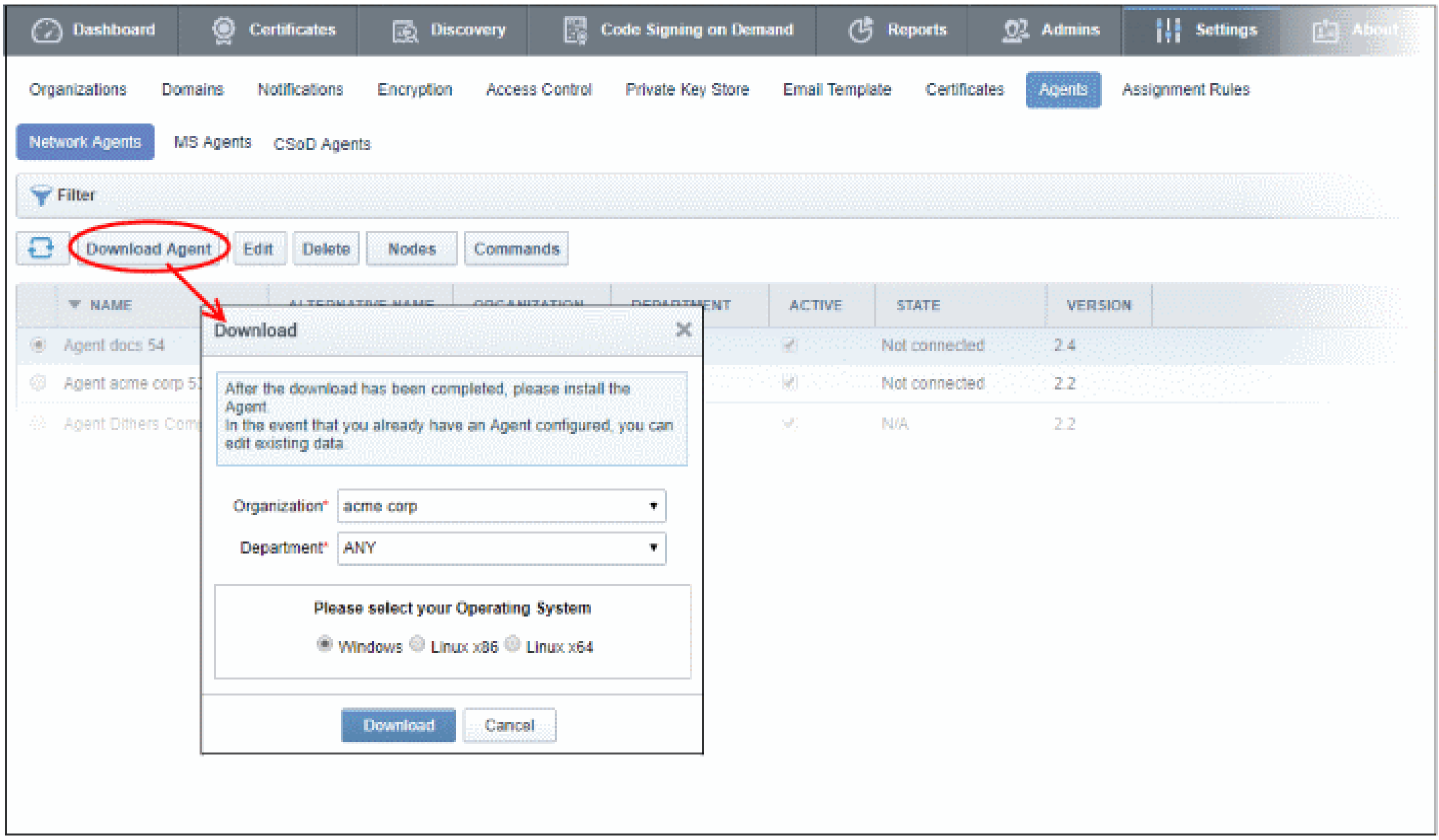
To run a discovery scan, you need to:

1. Install the certificate discovery agent on your network and configure it for certificate discovery. Once installed, this agent will also allow you to use InCommon CM's automatic certificate installation feature.
2. Create and run a 'Discovery Task' by specifying target IP ranges.

Any certificates discovered by the scan will be displayed in the 'SSL Certificates' area of the 'Certificates' interface.

To install and configure the agent

- Click the 'Settings' tab then 'Agents' sub tab
- Select 'Network Agents' then click 'Download Agent'



NAME	ACTIVE	STATE	VERSION
Agent docs 54	✓	Not connected	2.4
Agent acme corp 57	✓	Not connected	2.2
Agent Dithers Com	✓	N/A	2.2

Download

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

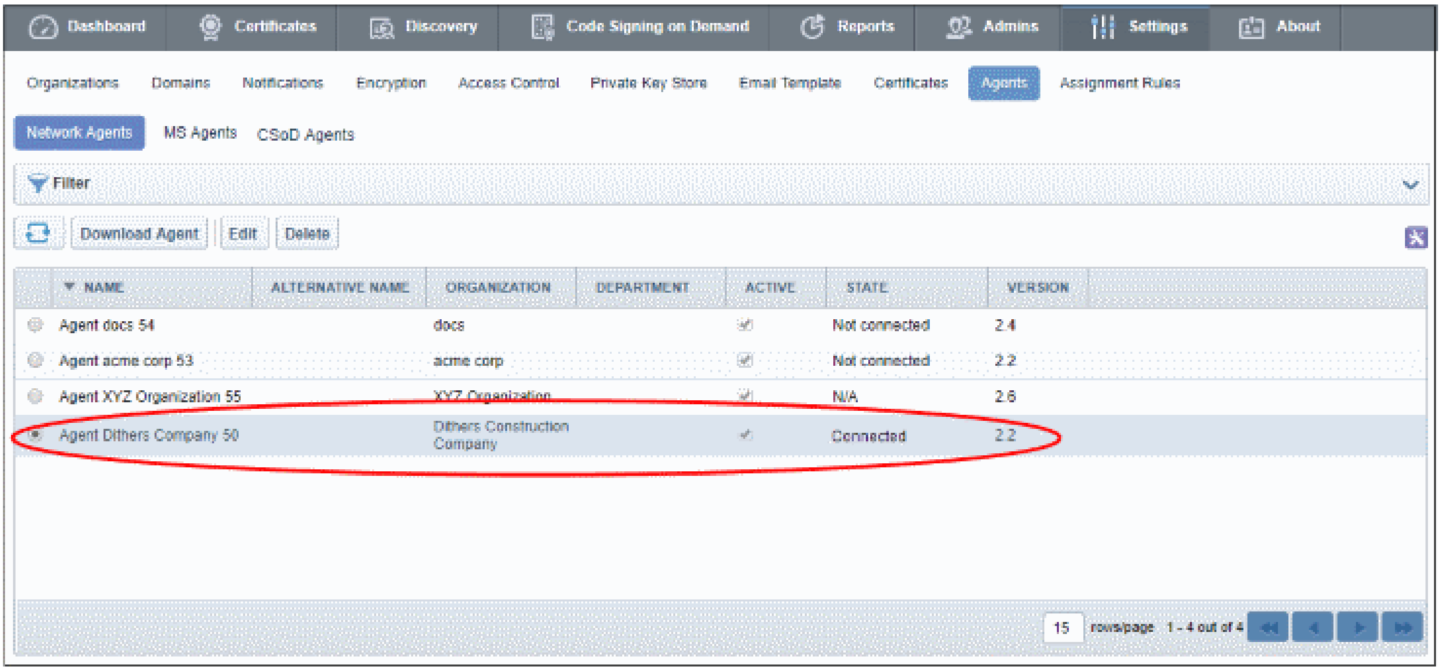
Please select your Operating System

● Windows ○ Linux x86 ○ Linux x64

- Select the Organization/Department on whose behalf you want to discover certificates. Next, choose the agent version appropriate for your server operating system.

- Click 'Download' and save the setup file.
- Install the agent on a machine in your network. To install the agent on Windows, right-click on the setup file and select 'Run as Administrator'. If you are installing the Linux version of the agent, run the installation from the command line.

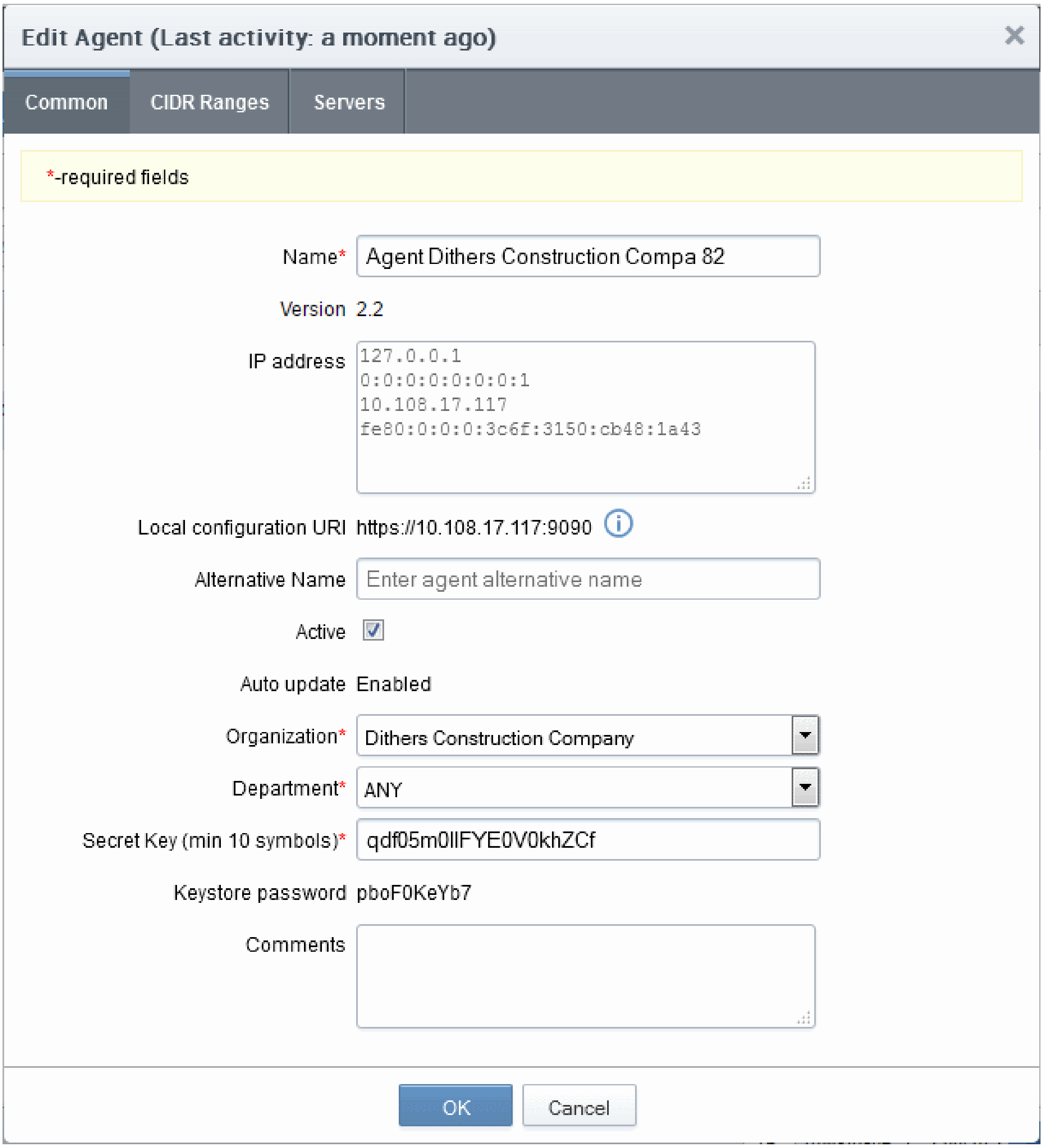
After installation, the agent will be listed in the InCommon CM interface:



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

The next step is to configure the agent to scan your internal network. You can do this by specifying the address of the network you wish to scan.

- Choose the agent from the 'Network Agents' interface and click 'Edit'.



Edit Agent (Last activity: a moment ago)

*-required fields

Name* Agent Dithers Construction Compa 82

Version 2.2

IP address
```
127.0.0.1
0:0:0:0:0:0:0:1
10.108.17.117
fe80:0:0:0:3c6f:3150:cb48:1a43
```

Local configuration URI https://10.108.17.117:9090

Alternative Name Enter agent alternative name

Active ☑

Auto update Enabled

Organization* Dithers Construction Company

Department* ANY

Secret Key (min 10 symbols)* qdf05m0llFYE0V0khZCf

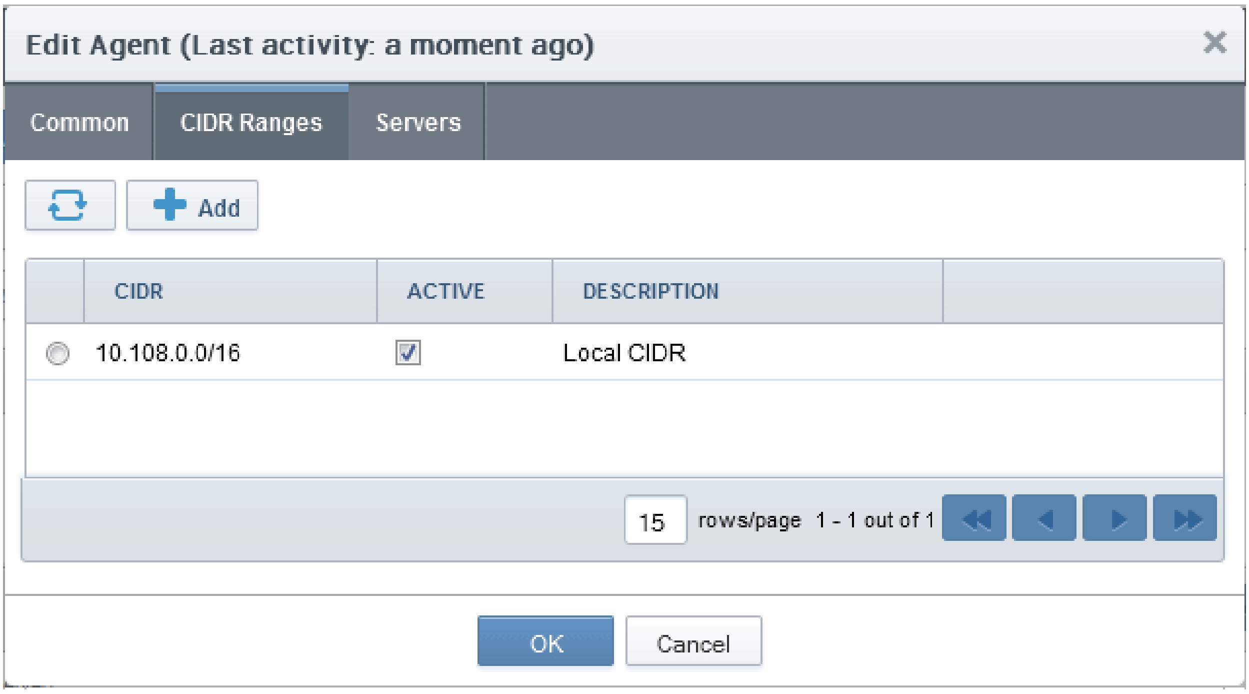
Keystore password pboF0KeYb7

Comments

Field Name	Description
Name	Create a name for the agent. The name should ideally describe the target network of the agent.
Version	Agent version.
IP Address	Displays the IPv6 loopback address, IPv4 loopback address, IPV6 address, IPv4 address and MAC address of the server on which the agent is installed.
Local Configuration URI	The URL used to access and configure the agent via a web browser. For more

	information, see 'Configuring the Certificate Controller Agent through the Web Interface in the admin guide.
Alternative Name	Specify an alternative name for the agent
Active	Switch the agent on or off
Auto update	Indicates whether or not agent updates should be automatically installed.
Organization	Select the organization that you want to associate with the agent.
Department	Select the department, if any, that you want to associate with the agent.
Secret Key	Key generated by the agent to authenticate itself to the InCommon CM server. The secret key must have 10 characters. Please keep a record of this key. If an agent needs to be be reinstalled on a particular server then the key is required to authenticate the agent to the InCommon CM server.
Keystore password	Displays the key store password generated by the Agent. You can copy and save the secret key store password in a safe location for use in a new agent, in case the agent has to be reinstalled in the same server.
Comments	Type a descriptive comment about the purpose of the agent

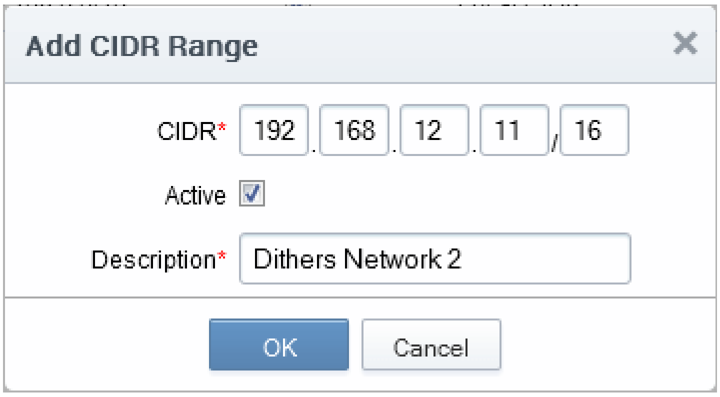
- Edit the values if required. To edit the CIDR ranges, click the 'CIDR Ranges' tab.



Edit Agent (Last activity: a moment ago)

	CIDR	ACTIVE	DESCRIPTION
○	10.108.0.0/16	☑	Local CIDR

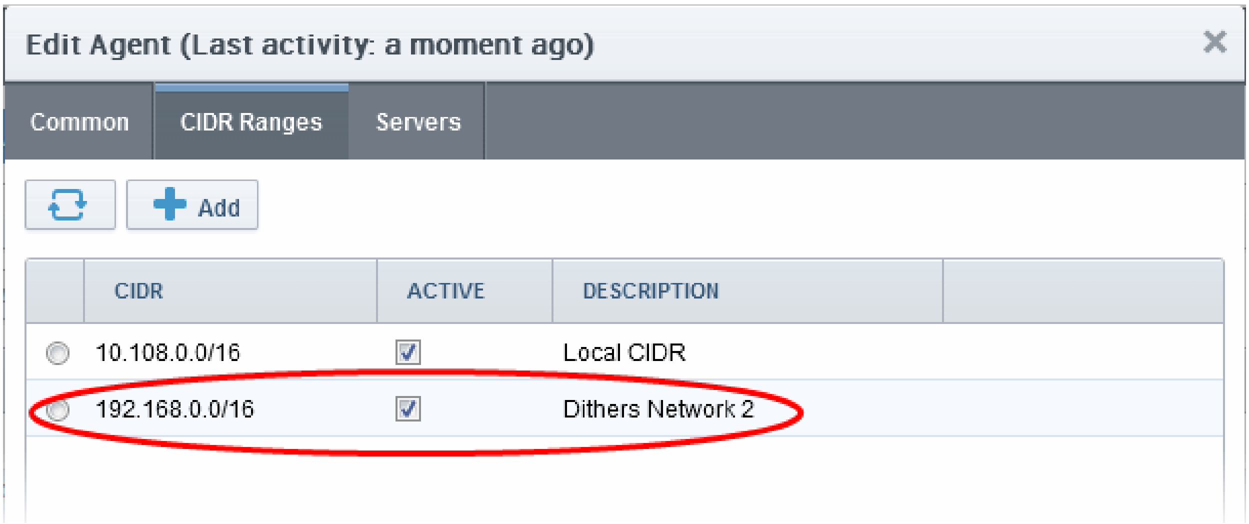
- To add a new CIDR range, click 'Add'. The 'Add CIDR Range' dialog will open.



Add CIDR Range

CIDR*	192 . 168 . 12 . 11 / 16
Active	☑
Description*	Dithers Network 2

- Enter the internal IP address range to be scanned, set whether the Agent is to be Active and type a description for the range in the dialog and click OK. The CIDR Range will be added in the 'CIDR Ranges' tab.



Edit Agent (Last activity: a moment ago)

	CIDR	ACTIVE	DESCRIPTION
○	10.108.0.0/16	☑	Local CIDR
○	192.168.0.0/16	☑	Dithers Network 2

You can add as many ranges as you want by repeating the same procedure.

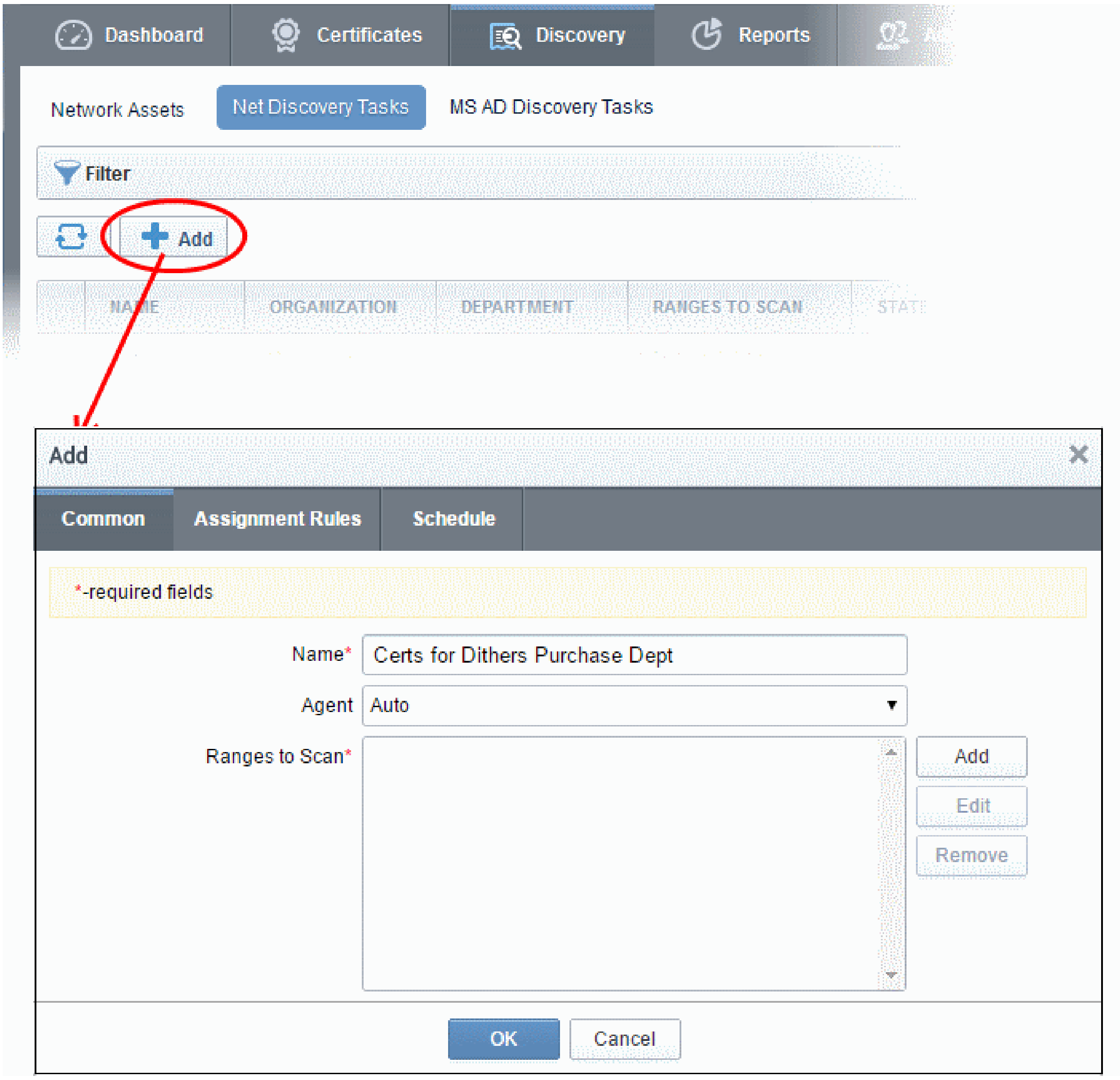
The Servers tab allows you to add local/remote servers for auto-installation of SSL certificates. You can add servers at a later time by editing the agent.

- Click 'OK' in the 'Edit Agent' interface

The agent is now configured to scan the servers covered by the specified CIDR range and can be used to run a discovery task on the network.

To create a Discovery Task

- Click the 'Discovery' tab then click 'Net Discovery Tasks'
- Click 'Add'



*-required fields

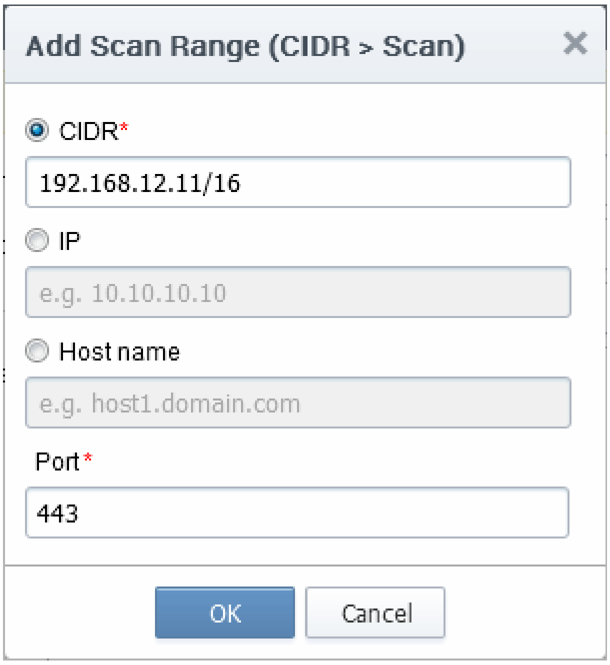
Name* Certs for Dithers Purchase Dept

Agent Auto

Ranges to Scan*

- Enter a name to identify the discovery task
- Leave 'Agent' at the default 'Auto' setting.
- Click 'Add' beside 'Ranges to Scan' to specify the networks/servers you wish to scan.

You can specify scan ranges in CIDR notation, by IP address or by hostname.



Add Scan Range (CIDR > Scan)

● CIDR*

192.168.12.11/16

○ IP

e.g. 10.10.10.10

○ Host name

e.g. host1.domain.com

Port*

443

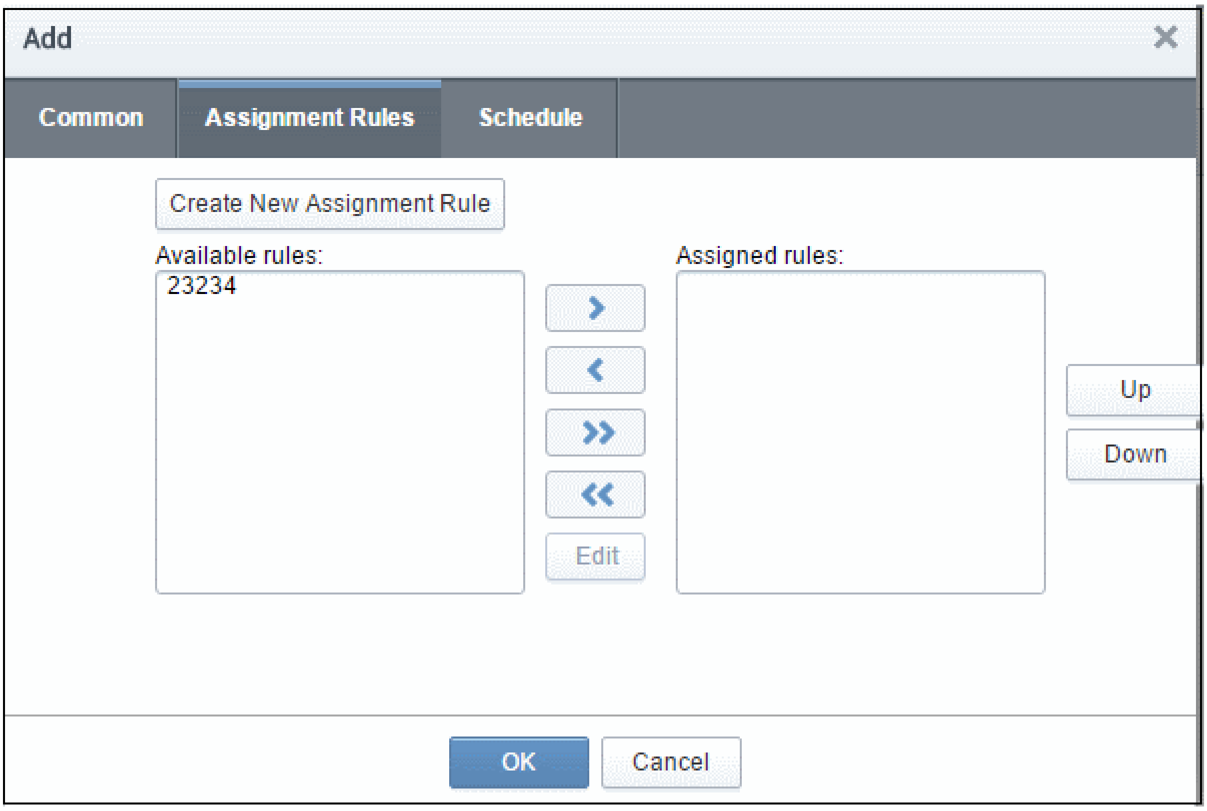
Form Element	Description
CIDR	Short for 'Classless Internet DOMAIN Routing'. Type the IP address you wish to scan followed by network prefix, e.g. 123.456.78.91/16 Enter the same CIDR value specified for the agent.
IP	Type the IP address you wish to scan
Host name	Enter the host name you wish to scan
Ports ***(required)***	The port number(s) through which the agent can access your targets

- Click 'OK' when you have specified your targets.

The range will be added to the 'Ranges to Scan' field

- Click 'OK' in the 'Add' dialog.

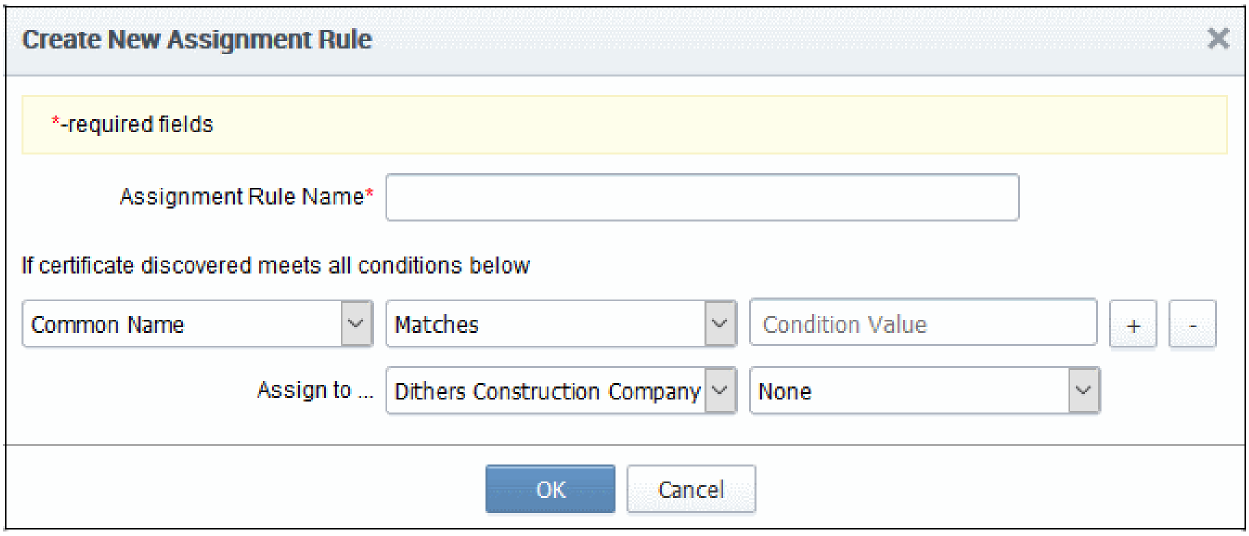
The 'Assignment Rules' tab lets you add rules which will assign discovered certificates to a specific organization/department based on criteria you define.



Available rules:
23234

Assigned rules:

- Existing rules can be added to the task by clicking the right-arrow button.
- Click the 'Create New Assignment Rule' button to set up a new rule:



*-required fields

Assignment Rule Name*

If certificate discovered meets all conditions below

Common Name | Matches | Condition Value

Assign to ... Dithers Construction Company | None

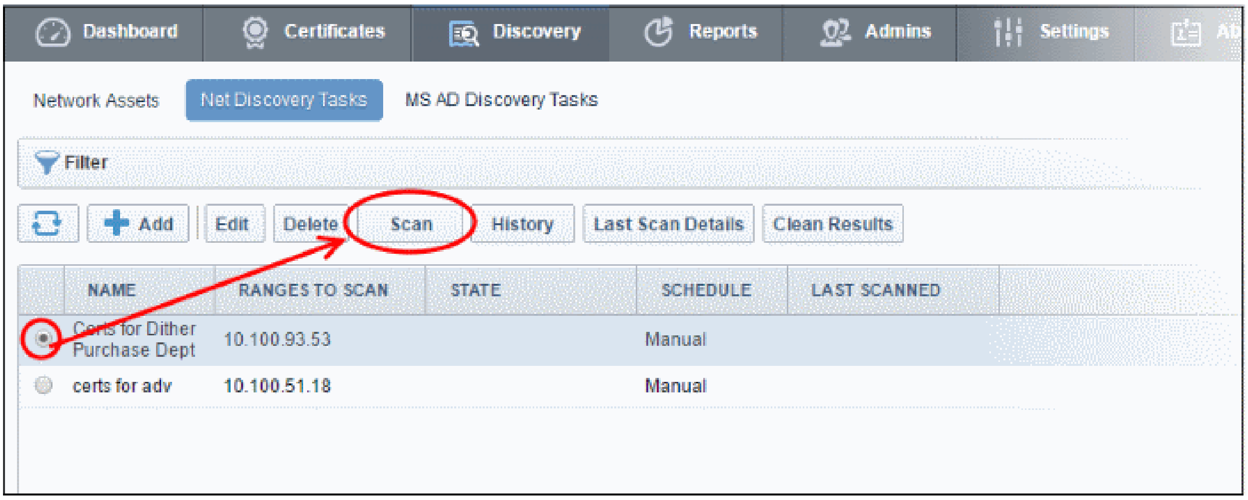
- Enter a name for the new rule in the first text field. Each individual rule allows you to assign certificates to a single organization or department based on one or more conditions.
- Set the rule conditions by modifying the parameters under 'If certificate is discovered meets all conditions below'. For example, you could assign all certificates that contain 'example.com' in the common name to a specific organization.

- Use the '+' button to add more conditions. For example, you may also want to assign all certificates that contain 'mycompany.com' to the same organization/department.
- Select the target Organization/Department in the 'Assign to...' area.
- Click 'OK' to save the rule. You can create multiple rules per task to assign different types of certificate to different organizations.

The new discovery task will be added to the list. You can now launch scans using this task.

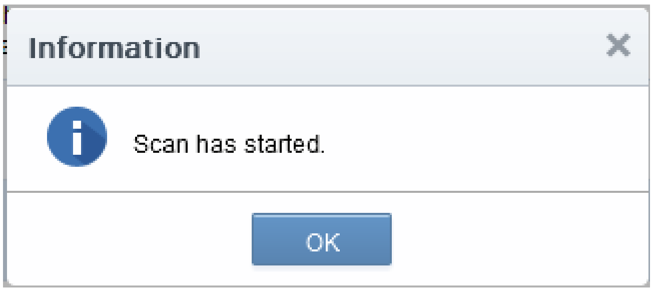
To start a scan

- Click the 'Discovery' tab then click 'Net Discovery Tasks'
- Select the task you wish to execute then click 'Scan':



NAME	RANGES TO SCAN	STATE	SCHEDULE	LAST SCANNED
Certs for Dither Purchase Dept	10.100.93.53		Manual	
certs for adv	10.100.51.18		Manual	

- The scan will begin immediately:

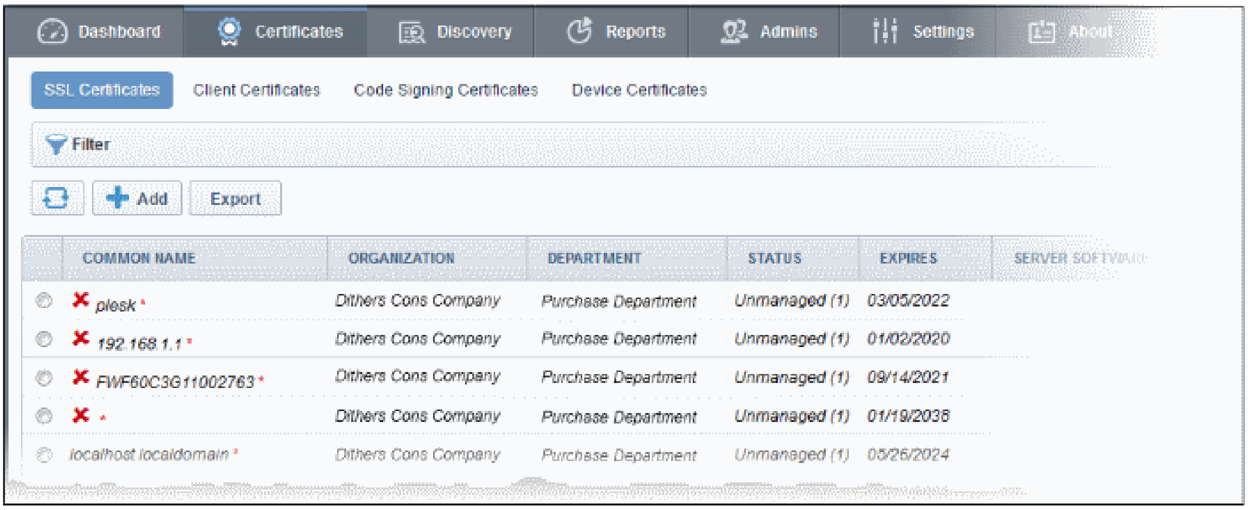


Scan has started.

- All certificates discovered by the scan will be assigned to the chosen organization/department
- Click 'Certificates' > 'SSL Certificates' to view discovered certificates

To view the results

- Click 'Certificates' > 'SSL Certificates' to open the certificates management area:



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	SERVER SOFTWARE
○	✗ plesk *	Dithers Cons Company	Purchase Department	Unmanaged (1)	03/05/2022	
○	✗ 192.168.1.1 *	Dithers Cons Company	Purchase Department	Unmanaged (1)	01/02/2020	
○	✗ FWF60C3G11002763 *	Dithers Cons Company	Purchase Department	Unmanaged (1)	09/14/2021	
○	✗ *	Dithers Cons Company	Purchase Department	Unmanaged (1)	01/19/2038	
○	localhost.localdomain *	Dithers Cons Company	Purchase Department	Unmanaged (1)	05/26/2024	

All discovered certificates will be listed in the interface along with details such as the org/dept to which they are assigned.

To re-assign *unmanaged* certificates to a different org/dept:

- Renew/replace the '*unmanaged'* certificate with a InCommon equivalent through InCommon CM. Certificates issued by InCommon CM automatically have a status of '*managed*'. You need to specify a new organization/department during the renewal/application process.

  OR

- Identify the IP addresses of the servers on which the certificate/are installed. Then run a new discovery task on these IPs which assigns discovered certificates to your desired organization/department.
  - Select the certificate from the 'Certificates' > 'SSL Certificates' interface.
  - Click the 'Details' button at the top to view the 'Certificate Details'
  - Identify the IP addresses on which the certificate is installed
  - Create a new discovery task which scans just those IP addresses. Specify your new organization/department during scan configuration.
  - After running the scan, discovered certificates will be re-assigned to the new organization/department.

Step 4 - Add Administrators

Once you have created organizations and departments you can add and assign administrators to them. Administrators are able to procure and manage certificates for InCommon CM organizations and departments.

There are 7 types of administrators:

- Master Registration Authority Officer (MRAO)
- 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:

Master Registration Authority Officer (MRAO)

- The MRAO is the top level administrator and can access all areas and functionality of the InCommon CM. They have control over the certificates, domains and notifications of all organizations and departments.
- The MRAO can also create and set the permissions of Registration Authority Officers (RAOs), Department Registration Authority Officers (DRAOs) and end-users of any organization or department.

Registration Authority Officer (RAO)

- An RAO is a role created by an MRAO or fellow RAO for the purpose of managing the certificates/end-users of an organization or department.
- RAOs can create departments and DRAO administrators for their own organization. These must be approved by the MRAO.
- RAOs cannot create a new organization or edit the general settings of an organization – even of those organizations of which they have been delegated control.

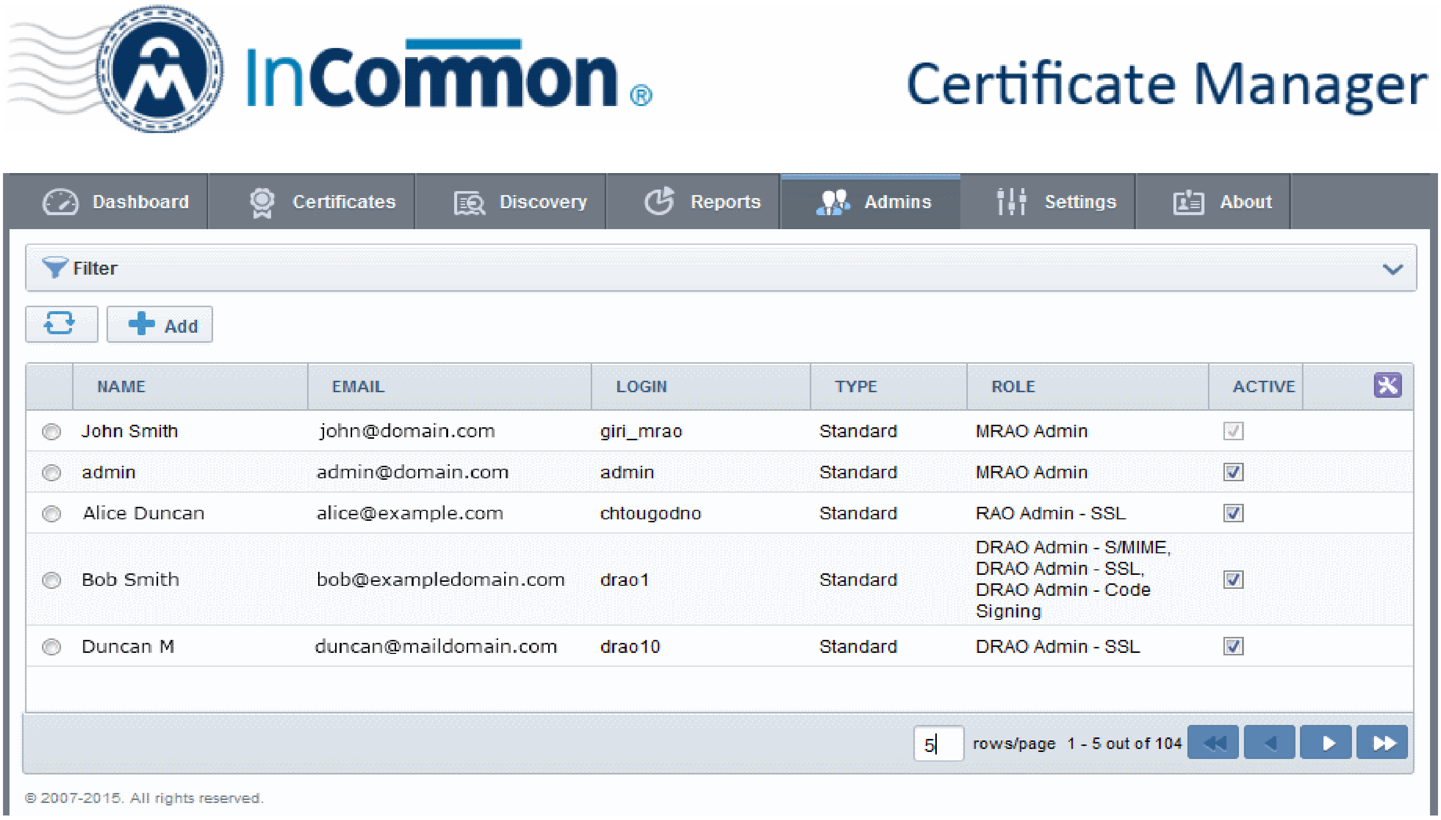
Department Registration Authority Officer (DRAO)

- DRAOs are created by, and subordinate to, the RAO class of administrator. They are assigned control over the certificates, users and domains belonging to department(s) of an organization.
- DRAOs have visibility of, and can only request certificates for, the department(s) that have been delegated to them. They have no ability to manage certificates belonging to organizations or departments over which they haven't been granted permissions.

It is also possible to award the same person multiple administrative roles. For example, the same person could be an RAO SSL, an RAO SMIME and a DRAO Code Signing. See 'Administrative Roles' in the admin guide if you'd like more details about security roles.

To add an administrator

- Click the 'Admins' tab to open the 'Administrators' management area:

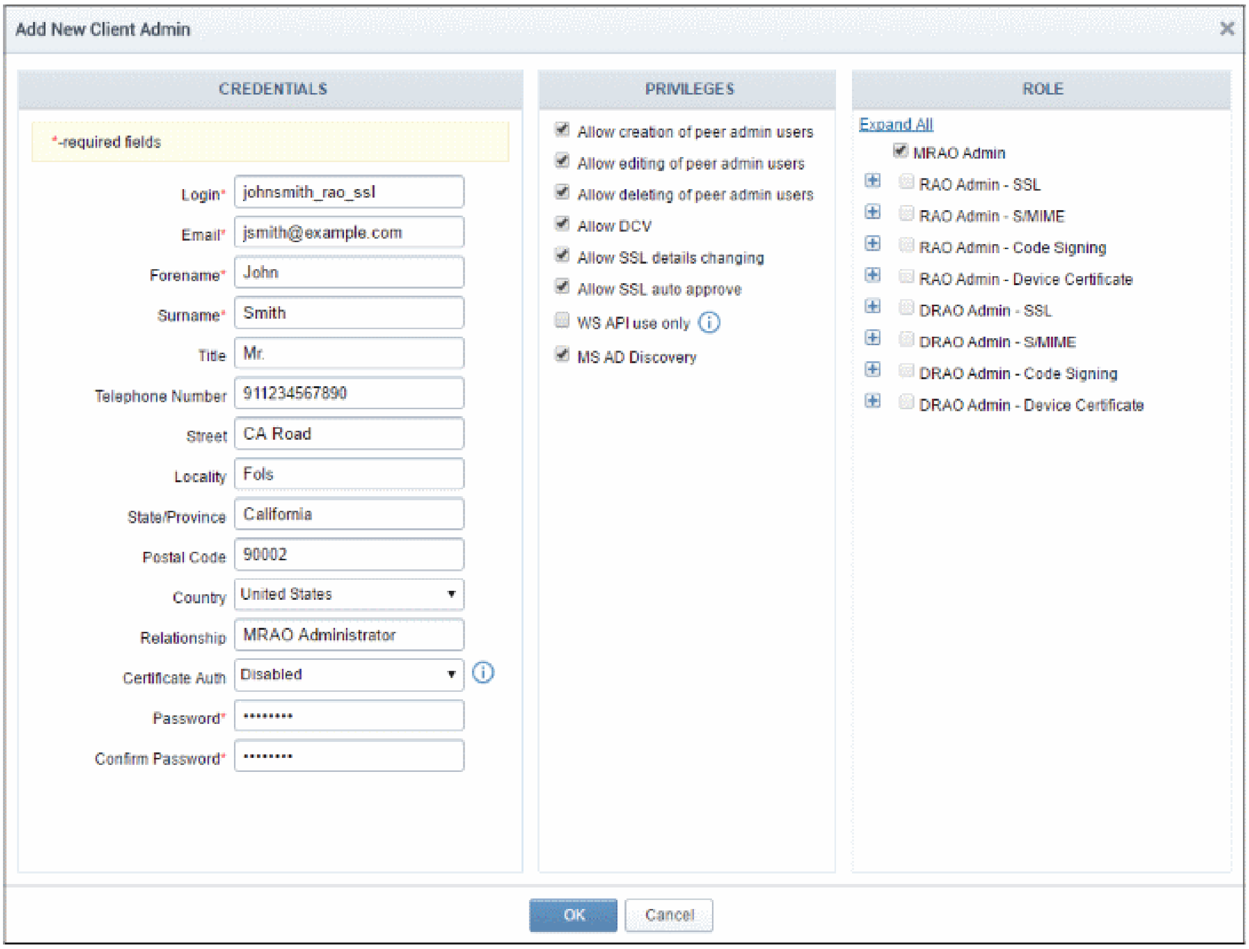


	NAME	EMAIL	LOGIN	TYPE	ROLE	ACTIVE
○	John Smith	john@domain.com	giri_mrao	Standard	MRAO Admin	☑
○	admin	admin@domain.com	admin	Standard	MRAO Admin	☑
○	Alice Duncan	alice@example.com	chtougodno	Standard	RAO Admin - SSL	☑
○	Bob Smith	bob@exampledomain.com	drao1	Standard	DRAO Admin - S/MIME, DRAO Admin - SSL, DRAO Admin - Code Signing	☑
○	Duncan M	duncan@maildomain.com	drao10	Standard	DRAO Admin - SSL	☑

5 rows/page 1 - 5 out of 104

© 2007-2015. All rights reserved.

- Click the 'Add' button to open the 'Add new Client Admin' form:



*-required fields

Login*	johnsmith_rao_ssl
Email*	jsmith@example.com
Forename*	John
Surname*	Smith
Title	Mr.
Telephone Number	911234567890
Street	CA Road
Locality	Fols
State/Province	California
Postal Code	90002
Country	United States
Relationship	MRAO Administrator
Certificate Auth	Disabled
Password*	••••••••
Confirm Password*	••••••••

☑ 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

Expand All
☑ MRAO Admin
□ RAO Admin - SSL
□ RAO Admin - S/MIME
□ RAO Admin - Code Signing
□ RAO Admin - Device Certificate
□ DRAO Admin - SSL
□ DRAO Admin - S/MIME
□ DRAO Admin - Code Signing
□ DRAO Admin - Device Certificate

- Complete the 'Add New Client Admin' form and click 'OK'.

You can communicate the login URL for InCommon CM, the username and password to the new administrator through any out-of-band communication like email, enabling them to login to the CM console. Upon their first login, they will be prompted to change their password.

- Repeat the process to add more administrators.

Step 5 - Add Domains and delegate them to Organizations/Departments

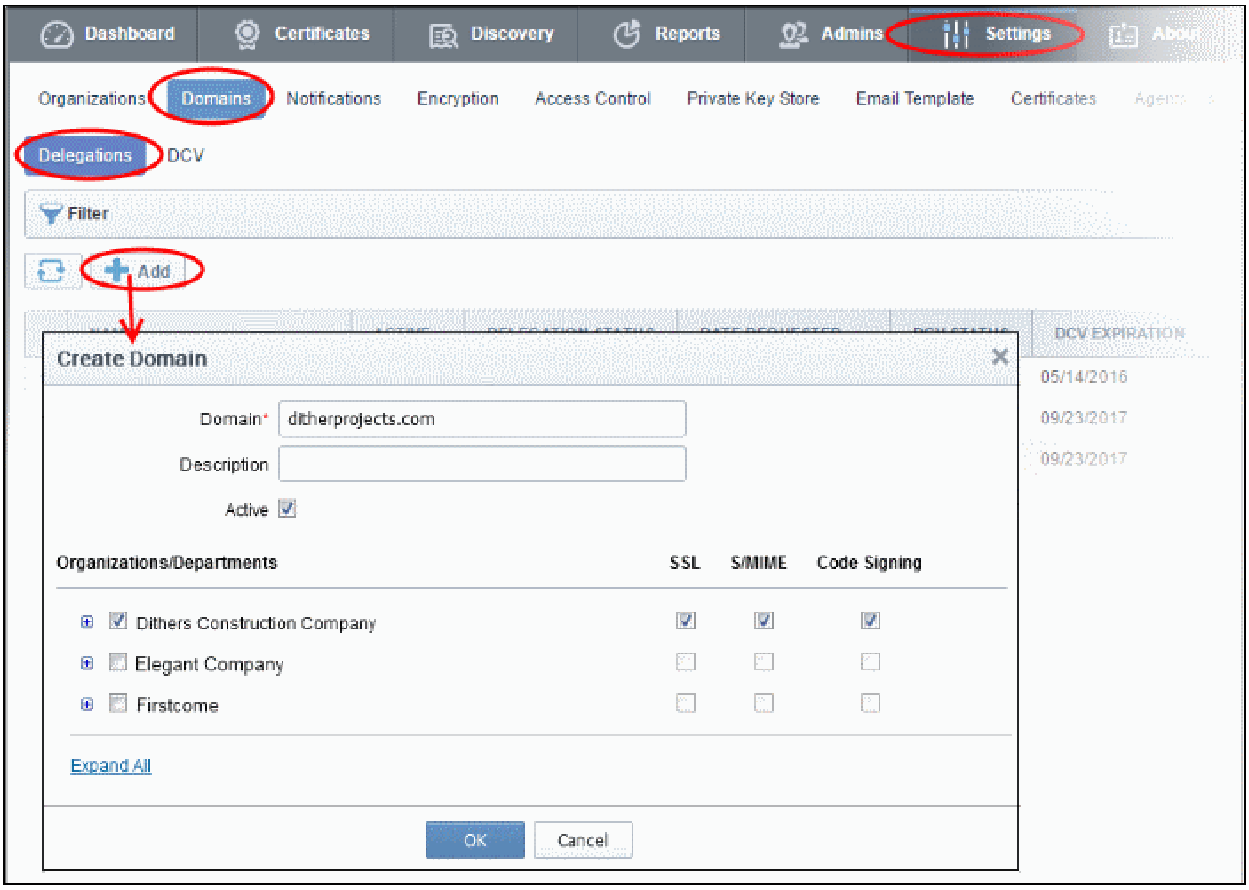
- The next step is to add the domains to which you want to issue certificates, and to delegate them to organizations or departments.
- Domains added by RAOs and DRAOs must be approved by an admin higher authority level.
- Each domain must pass domain control validation (DCV) before certificates can be issued to it.

The domain approval structure is as follows:

- MRAOs can add and manage domains for any organization/department. New domains are auto-approved .
- RAOs can add and manage domains for organizations that have been delegated to them (and any departments of those organizations). Any domains they add must be approved by two MRAOs with appropriate privileges, or by one MRAO with the 'Domain validation without Dual Approval' privilege.
- RAOs can add and manage domains for departments that have been delegated to them. Any domains they add must first be approved by the RAO admin of the organization to which the department belongs. Next, they must be approved by two MRAOs with appropriate privileges or by one MRAO with the 'Domain validation without Dual Approval' privilege.

To add and delegate a new domain

- Open the 'Domain Delegations' interface by clicking the 'Settings' > 'Domains' and then clicking 'Delegations'.
- Click the 'Add' button at the top left of the 'Domain Delegations' interface. This will open the 'Create domain' dialog.



Create Domain

Domain* ditherprojects.com

Description

Active ☑

Organizations/Departments	SSL	S/MIME	Code Signing
⊕ ☑ Dithers Construction Company	☑	☑	☑
⊕ □ Elegant Company	□	□	□
⊕ □ Firstcome	□	□	□

Expand All

OK Cancel

Field Name	Description
Domain	The domain name
Description	A short description of the domain.
Organizations/Departments	Choose the organization/department to which the domain should be delegated. All organizations are listed by default. Click the '+' button beside an organization to view its departments. A single domain can be delegated to more than one Organization/Department. If required, you can re-delegate the domain to a different Organization/Department at a later time.
SSL, S/MIME, Code Signing	Specify the types of certificates that can be requested for the domain.
Active	Activate or deactivate the domain. You cannot order certificates for inactive domains. Default = Active.

- Enter the details as shown above and click 'OK'.

The domain will be added to the CM and delegated to the selected Organization/Department with the delegation status 'Approved', if added by an MRAO admin or 'Requested' if added by a RAO or DRAO admin. Once approved, you can start the DCV process.

- MRAO admins can initiate DCV process for all registered Domains.
- RAO admins can initiate DCV process for the domains delegated to the Organizations that are administrated by them.
- DRAO admins can initiate DCV process for domains delegated to the Departments that are administrated by them.

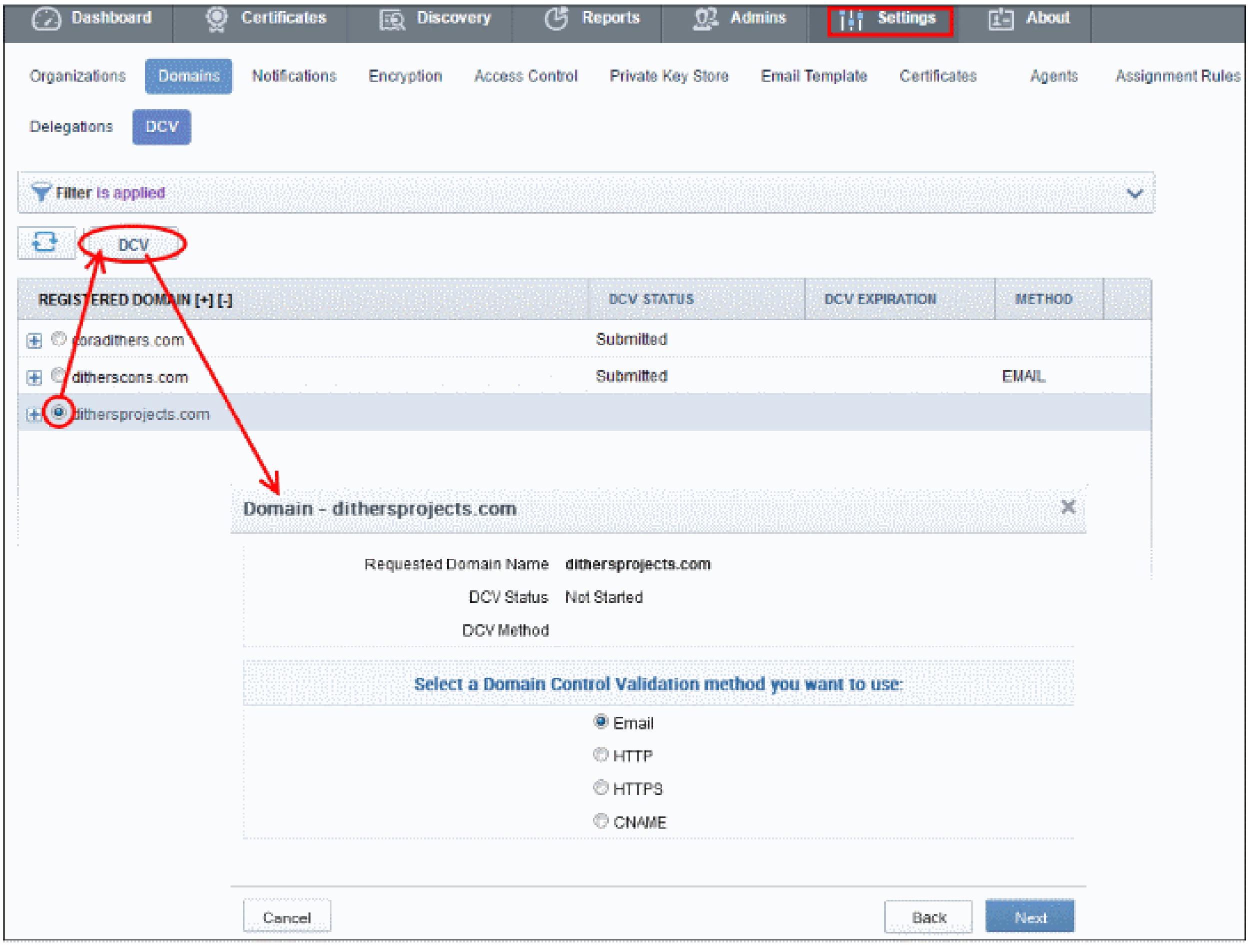
DCV can be carried out in three ways:

- Email - An activation email will be sent to the domain administrator. The domain will be validated on clicking the validation link in the email by the domain administrator.
- HTTP/HTTPS - InCommon CM generates a text file to be placed in the root of the web server. You can download and forward the .txt file to the domain administrator and instruct them to place the file in the web server. The CM can validate the domain by the presence of the text file in the server.
- CNAME - InCommon CM creates a DNS CNAME record for the domain. You can forward the record to the domain administrator and instruct them to create a DNS record using the same. The CM can validate the domain through its DNS record.

This section explains the simple Email method of DCV to start with. If you require details on HTTPS/HTTP and CNAME methods, please refer to the section 'Validating the Domain' in the Administrator guide.

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 [+] [-]	DCV STATUS	DCV EXPIRATION	METHOD
○ coradithers.com	Submitted		
○ ditherscons.com	Submitted		EMAIL
● dithersprojects.com			

Domain - dithersprojects.com

Requested Domain Name dithersprojects.com

DCV Status Not Started

DCV Method

Select a Domain Control Validation method you want to use:

● Email

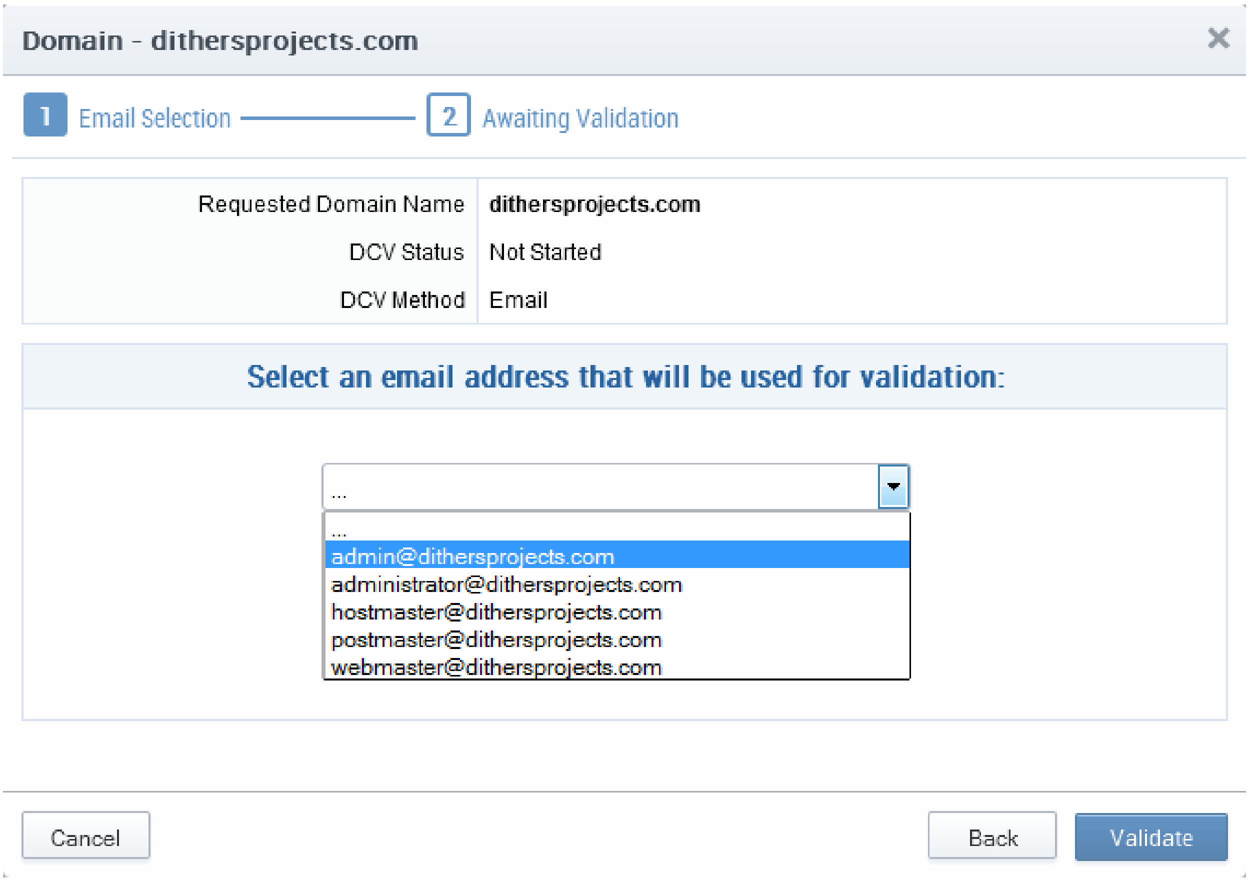
○ HTTP

○ HTTPS

○ CNAME

- Select the Email from as the 'DCV method and click 'Next'

On selection of EMAIL method, the next step allows you to select the email address of the Domain Administrator for sending the validation email.



Domain - dithersprojects.com

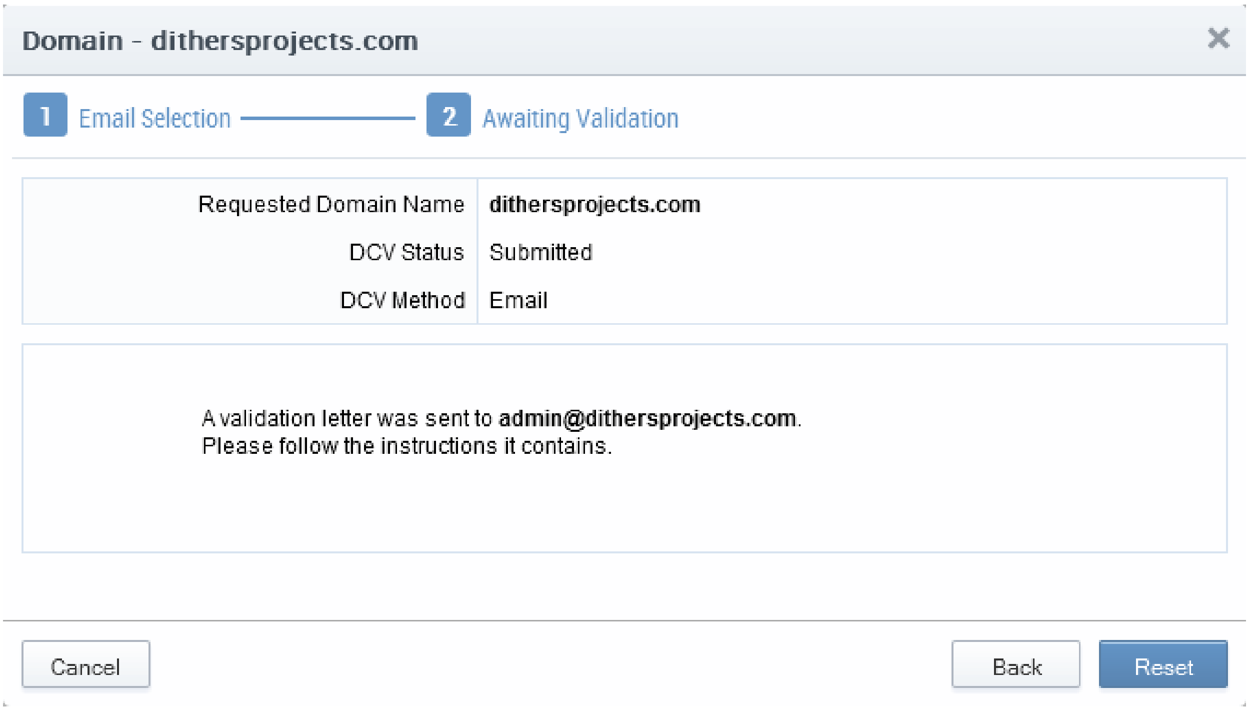
Requested Domain Name	dithersprojects.com
DCV Status	Not Started
DCV Method	Email

Select an email address that will be used for validation:

...
admin@dithersprojects.com
administrator@dithersprojects.com
hostmaster@dithersprojects.com
postmaster@dithersprojects.com
webmaster@dithersprojects.com

3. Select the email address of the administrator who can receive and respond to the validation mail from the drop-down and click 'Validate'.

An automated email will be sent to the selected Domain Administrator email address. The DCV status of the Domain will change to 'Submitted'.



Domain - dithersprojects.com

Requested Domain Name	dithersprojects.com
DCV Status	Submitted
DCV Method	Email

A validation letter was sent to **admin@dithersprojects.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 status of the Domain will change to 'Validated'.

You can now request and approve certificates for the domain.

Step 6 - Manage Certificates

You can begin requesting certificates for a domain after it has been delegated to an org/dept and has passed domain control validation (DCV). The following sections explain more about each type of certificate:

- Request and Issuance of SSL Certificates
- Request and Issuance of Client Certificates
- Request and Issuance of Code Signing Certificates

Request and Issuance of SSL Certificates

InCommon CM allows you to apply for SSL certificates for DCV validated domains in the following ways:

- **Automatic enrollment, request and installation** - You can configure InCommon CM to create certificate requests for enrolled domains then automatically install the certificate on the web server. Agents installed on a server in the network can automatically generate a CSR and forward it to InCommon CM to create a certificate request for admin approval. Once approved and issued, the agent will collect the certificate and install on the target server. The agent can also renew an expiring certificate in the same manner.
- **Self-enrollment by external applicant** - You can direct applicants to the request form to order SSL certificates for their domains. Applicants using this method must validate their application to Certificate Manager by:
    - Entering the appropriate Access Code specified for their Organization or Department. The Access Code is a mixture of alpha and numeric characters specified for the Organization/Department when it was created.

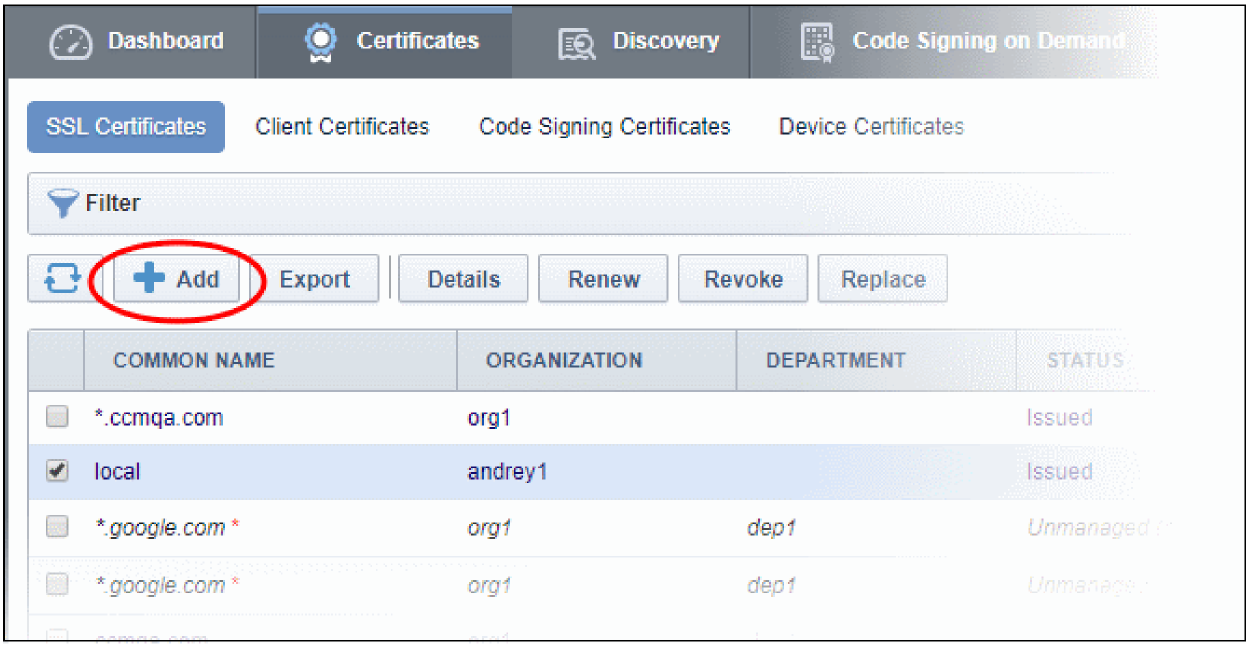
and

-
    - The email address they enter on the form must be from the domain that the certificate application is for. This domain must belong to the same Organization or Department.
- **Using Built-in application Wizard** - Admins can login and request SSL certificates using the built-in wizard available in the InCommon CM console. After the form is submitted and the request approved, InCommon CM will send a collection email to you (or to you and an external applicant if required). You or the external applicant can download the certificate and install it on the target server.

The reminder of this section explains request and issuance of the certificate using the built-in wizard (manual CSR generation). For detailed explanations and tutorials on the other methods, refer to the section 'Request and Issuance of SSL Certificates' in the Administrative guide.

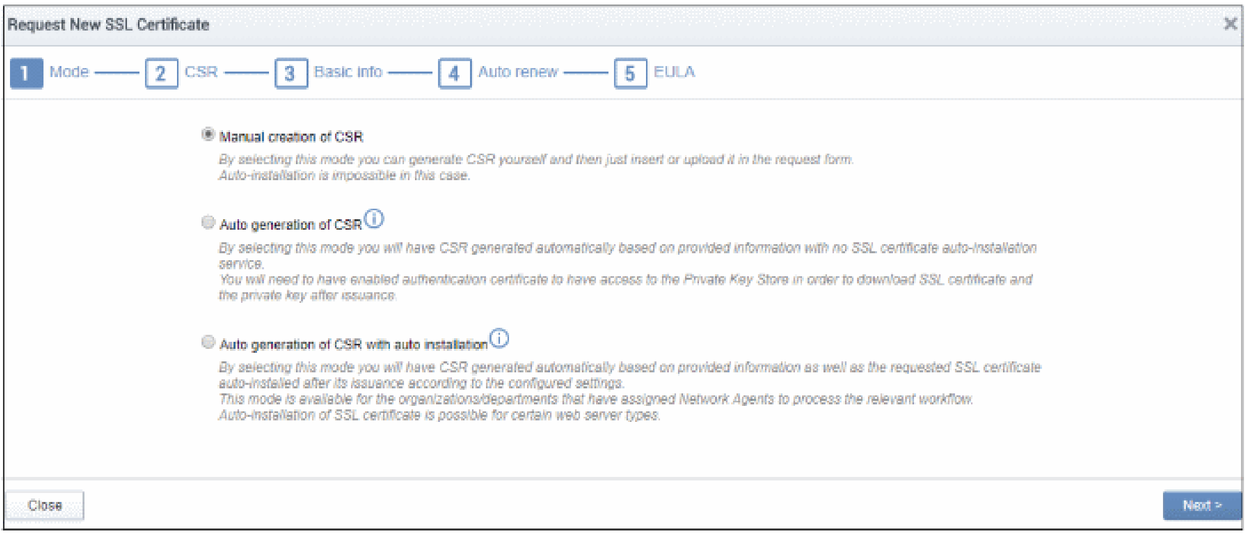
To apply for a SSL certificate

- Open the SSL Certificates management area by clicking the 'Certificates' tab and then clicking 'SSL Certificates'.
- 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	Unmanaged

- This will 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.

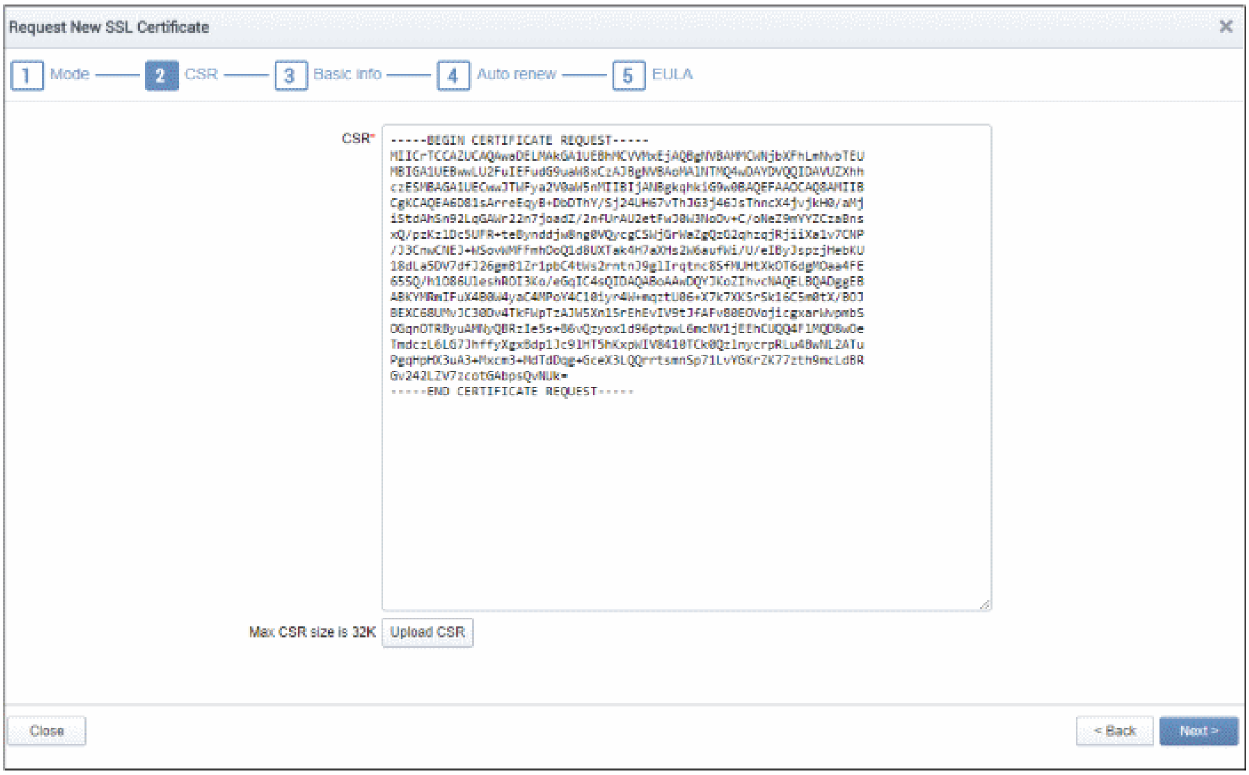
○ Auto generation of CSR

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



```
-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwaDELMAkGA1UEBhMCVVMxEjAQBgNVBAMMCWNjbXFhLmNvbTEU
MBIGA1UEBwwLU2FuIEFudG9uaW8xCzAJBgNVBAoMAlNTMQ4wDAYDVQQIDAVUZXhh
czESMBAGA1UECwwJTWFya2V0aW5nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6D81sArreEqyB+DbDThY/Sj24UH67vThJG3j46JsThncX4jvjkH0/aMj
iStdAhSn92LqGAWr22n7joadZ/2nfUrAU2etFwJ8W3NoDv+C/oNeZ9mYYZCzaBns
xQ/pzKz1Dc5UFR+teBynddjw8ng0VQycgCSWjGrWaZgQzG2qhzqjRjiiXa1v7CNP
/J3CnwCNEJ+WSovWMFfmhOoQ1d8UXTak4H7aXHs2W6aufWi/U/elByJspzjHebKU
18dLa5DV7dfJ26gm81Zr1pbC4tWs2rntnJ9g1Irqtnc85fMUHtXkOT6dgMOaa4FE
655Q/h1O86UleshRDI3Ko/eGqIC4sQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEB
ABKYMRmIFuX4B0W4yaC4MPoY4C10iyr4W+mqztU06+X7k7XKSrSk16C5m0tX/BOJ
BEXC68UMvJC30Dv4TkFWpTzAJW5Xn15rEhEvIV9tJfAFv80EOVojicgxarWvpmbS
OGqnOTRByuAMNyQBRz1e5s+06vQzyox1d96ptpwL6mcNV1jEEhCUQQ4F1MQD0wOe
TmdczL6LG7JhffyXgx8dp1Jc91HT5hKxpWIV8410TCk0Qz1nycrpRLu4BwNL2ATu
PgqHpHX3uA3+Mxcm3+MdTdDqg+GceX3LQQrrtsmnSp71LvYGKrZK77zth9mcLdBR
Gv242LZV7zcotGAbpsQvNUk=
-----END CERTIFICATE REQUEST-----
```

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

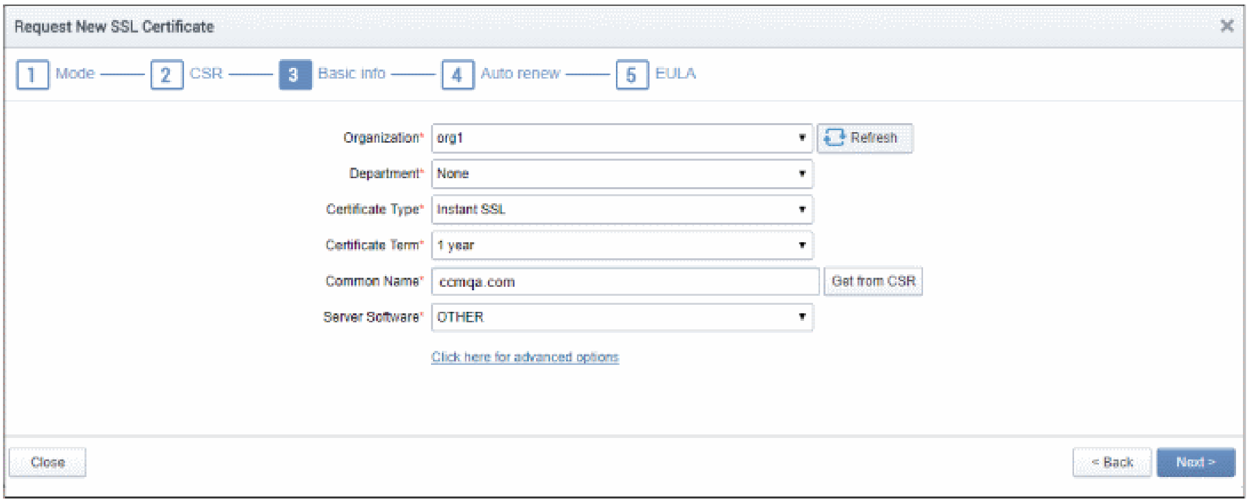
Background:

- 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

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

Organization*: org1

Department*: None

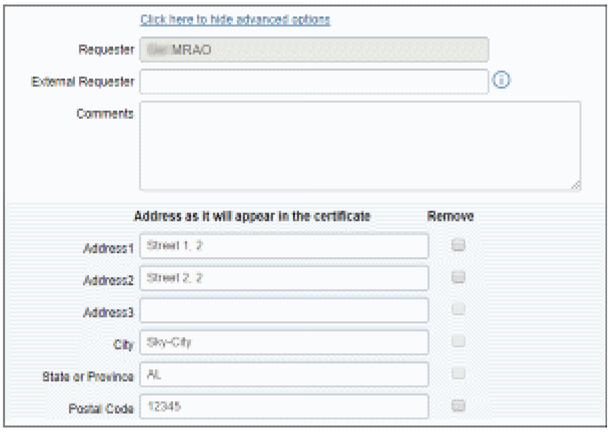
Certificate Type*: Instant SSL

Certificate Term*: 1 year

Common Name*: ccmqa.com

Server Software*: OTHER

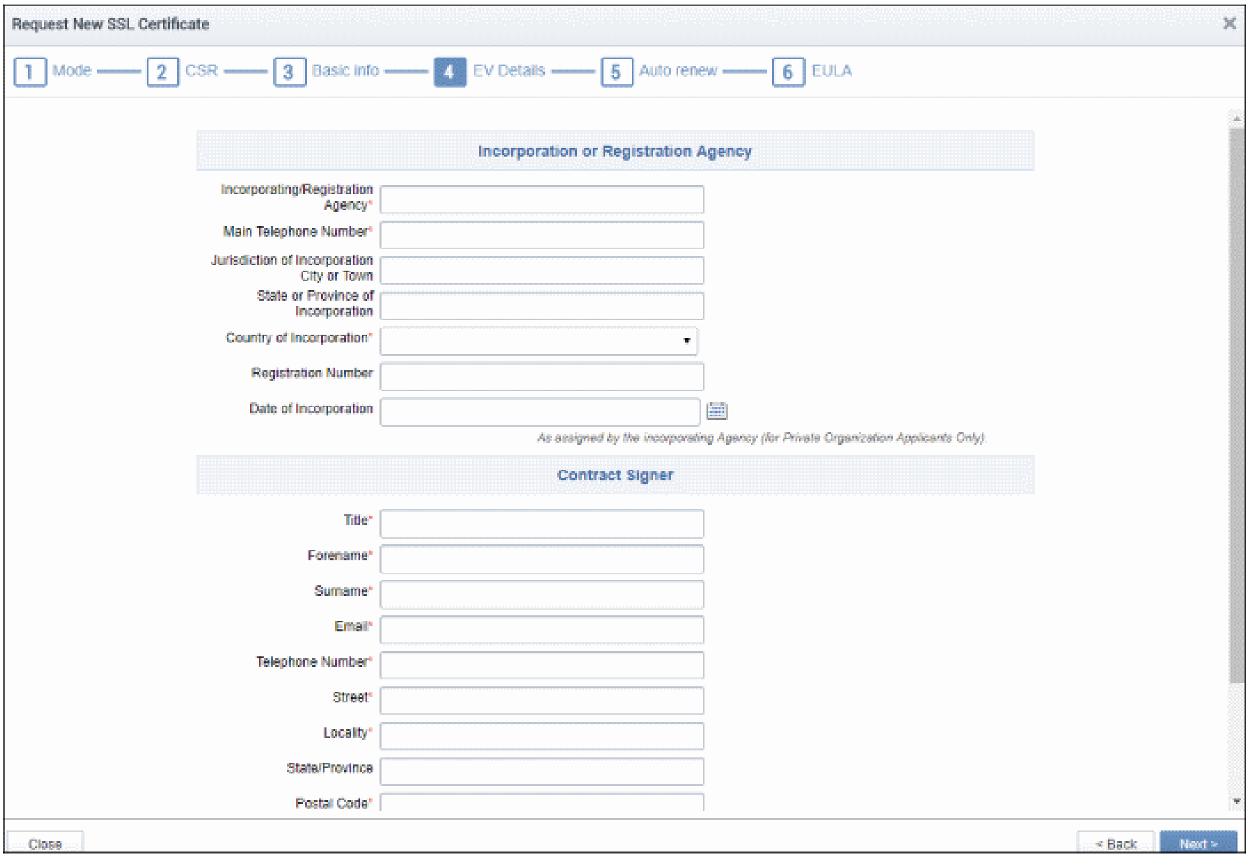
Form Element	Type	Description
Organization (***required***)	Drop-down list	Choose the organization that the SSL certificate will belong to.
Department (***required***)	Drop-down list	Choose the Department that the SSL certificate will belong to.
Certificate Type (***required***)	Drop-down list	Choose Type of the certificate that the applicant wishes to order. See Appendix - Comodo SSL Certificates for a list of certificate types.
Certificate Term (***required***)	Drop-down list	Select the term length of the certificate.
Common Name (***required***)	Text Field	Type the domain that the certificate will be issued to. • Single Domain certificates - enter domain name using the form: domain.com. • Wildcard Certificates - enter domain name using the form: *.domain.com. • Multi-Domain Certificates - enter the primary domain name using the form: domain.com.

Form Element	Type	Description
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 that is used to operate their web server (for example, Apache, IIS etc). Installation support documentation is available from Comodo support portal here: https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav=0
Subject Alternative Names (***required for Multi Domain certificates***)	Text Field	If the certificate 'Type' is a Multi-Domain Certificate (MDC) then the applicant should list the 'Subj Alt Name' additional domains here. Each domain should be separated by a comma.
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) - If the application is made on behalf of an external applicant enter the email address of the external requester in

Form Element	Type	Description
		this field, The applicant will also receive a certificate collection email. **Note**: The 'Requester' will still be the administrator that is completing this form (to view this, open the 'Certificates Management' area and click 'View' next to the certificate in question.) The email address of the 'External Requester' will be displayed as the 'External Requester' in the 'View' dialog of an issued certificate. This field is not required when requesting for EV SSL certificate and hence will be hidden. • Comments (optional) - 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 organization name, address, incorporating or registration agency, certificate requester and contract signer. It is not possible to remove these fields from the Comodo EV or Comodo EV MDC forms.

- Click 'Next'

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



Request New SSL Certificate

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

Incorporation or Registration Agency

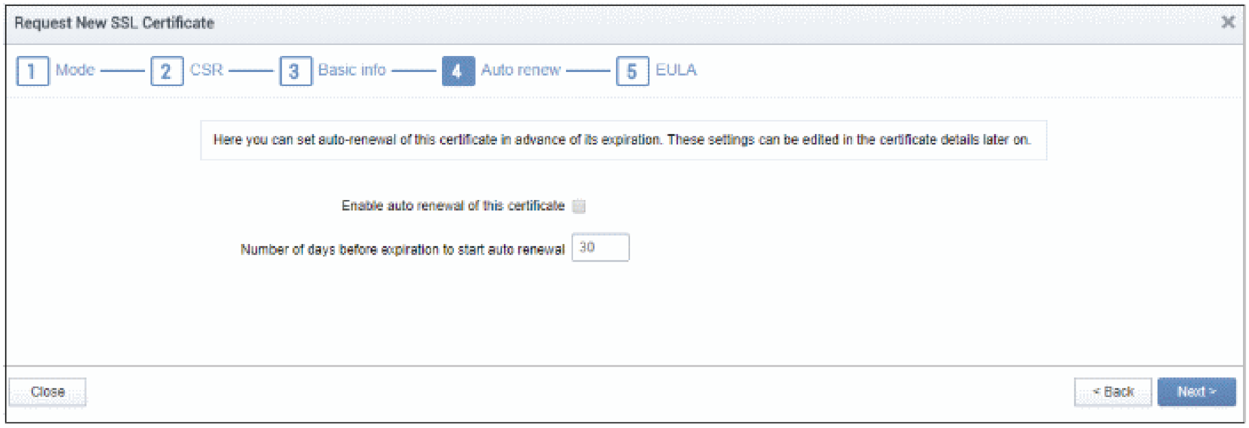
Incorporating/Registration Agency*	
Main Telephone Number*	
Jurisdiction of Incorporation City or Town	
State or Province of Incorporation	
Country of Incorporation*	▾
Registration Number	
Date of Incorporation	

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. 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.

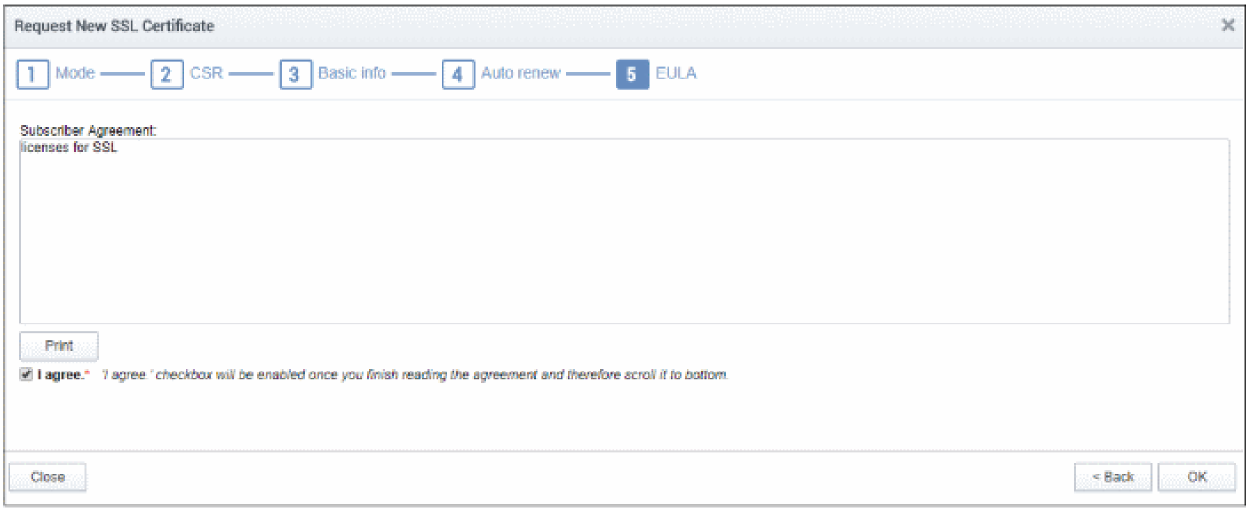
Enable auto renewal of this certificate □

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 CCM 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'



Request New SSL Certificate

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.

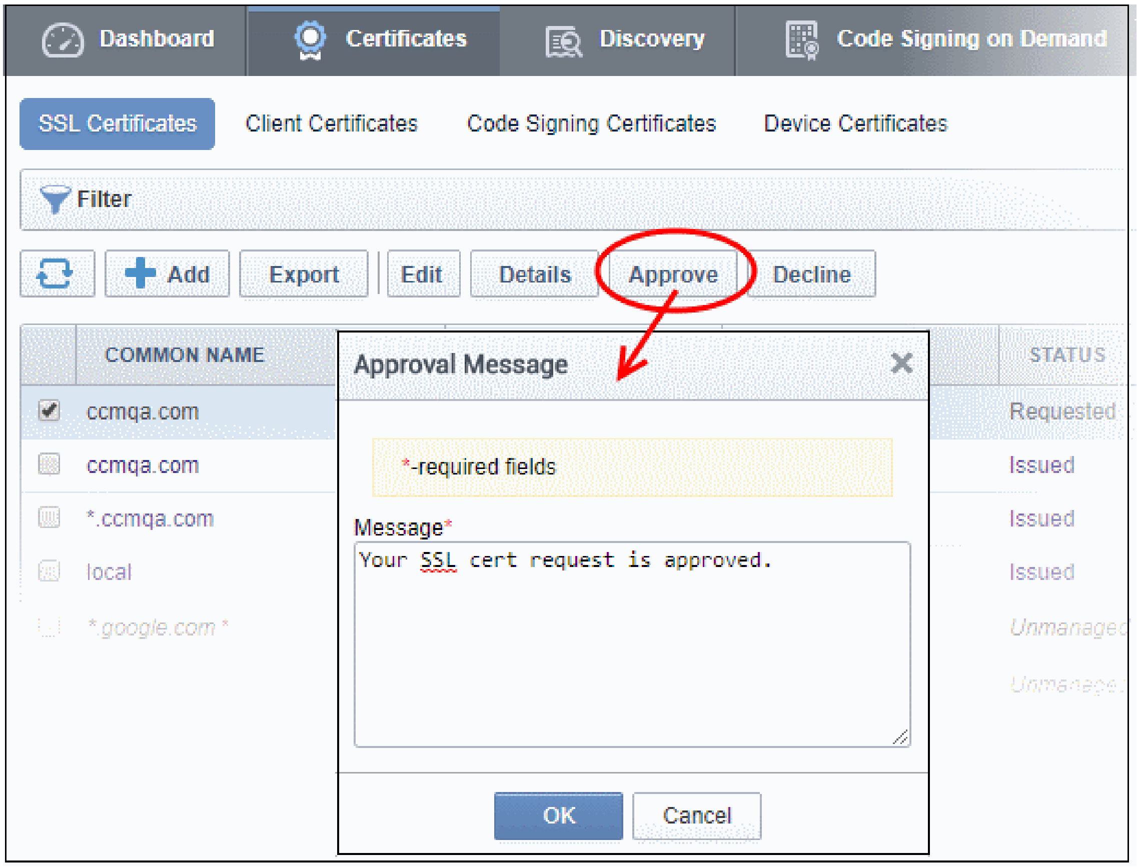
- Read the EULA fully and accept to by the selecting 'I Agree' checkbox.
- Click 'OK' to submit the application

The certificate will be added to the list in the 'Certificates' > 'SSL Certificates' interface, with the status 'Requested'.

The next step is to approve the request.

To approve the certificate request

- Choose the certificate from the 'Certificates' > 'SSL Certificates' interface and click 'Approve'.



Your SSL cert request is approved.

- Enter a message that will be sent along with the approval notification email.

- Click 'OK'.

Once an administrator has approved the request, the certificate status will change to 'Approved'. CCM will forward the application to Incommon CA and the status will change to 'Applied'. Incommon will issue the certificate if validation is successful. CCM will send a Certificate Collection email to the certificate requester and the 'Status' of the certificate will change to 'Issued'.

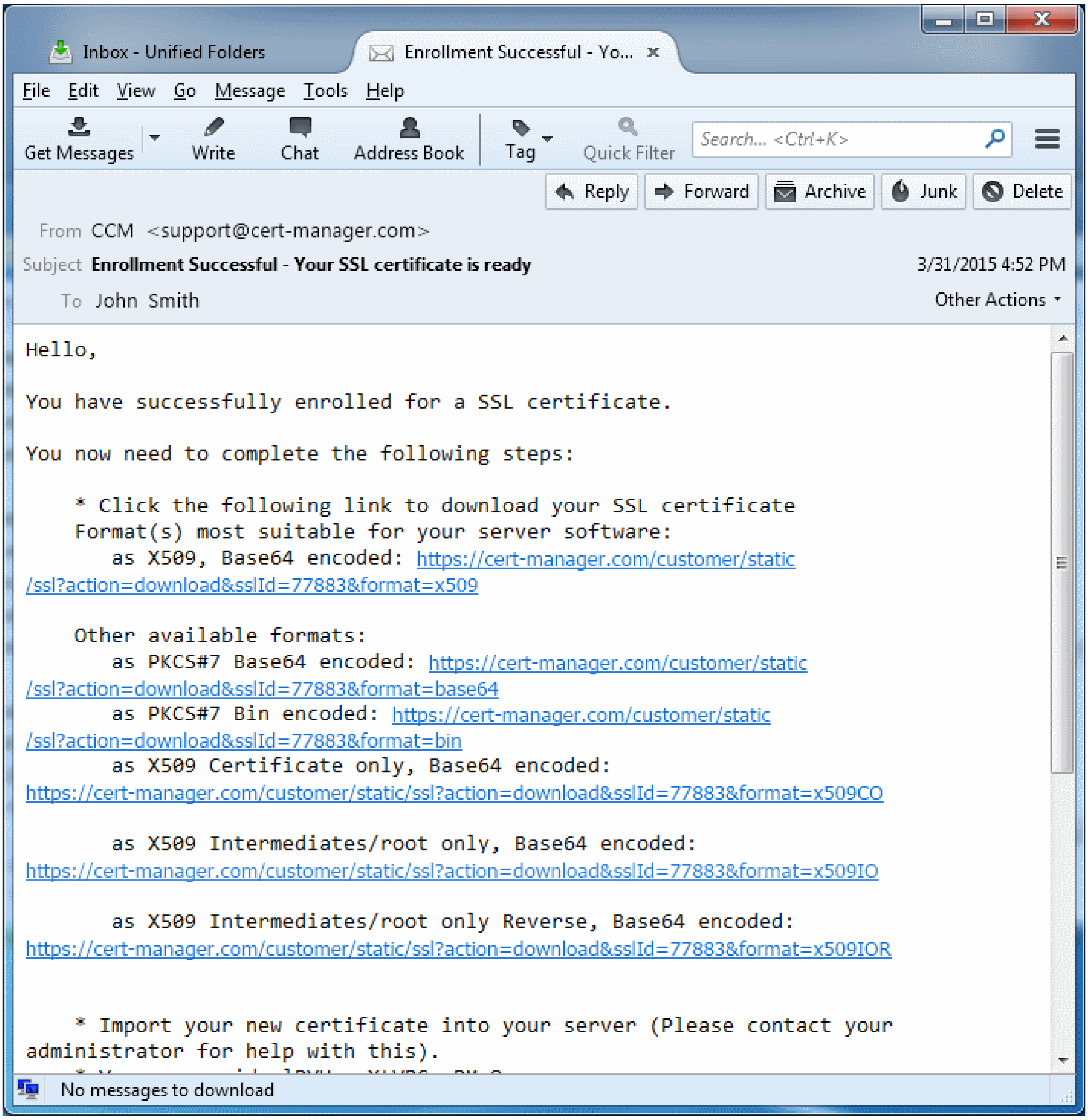
The next step is to collect the certificate. This can be done is two ways:

- Through Certificate Collection Email

- From the InCommon CM interface

Collection of SSL Certificate Through Email

Once the certificate has been issued, CCM will automatically send a collection email to you and the external applicant. 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).
```

- By clicking the link in the collection email, you/external applicant will be able to download the certificate file.

The certificate can now be installed on the server.

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

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

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

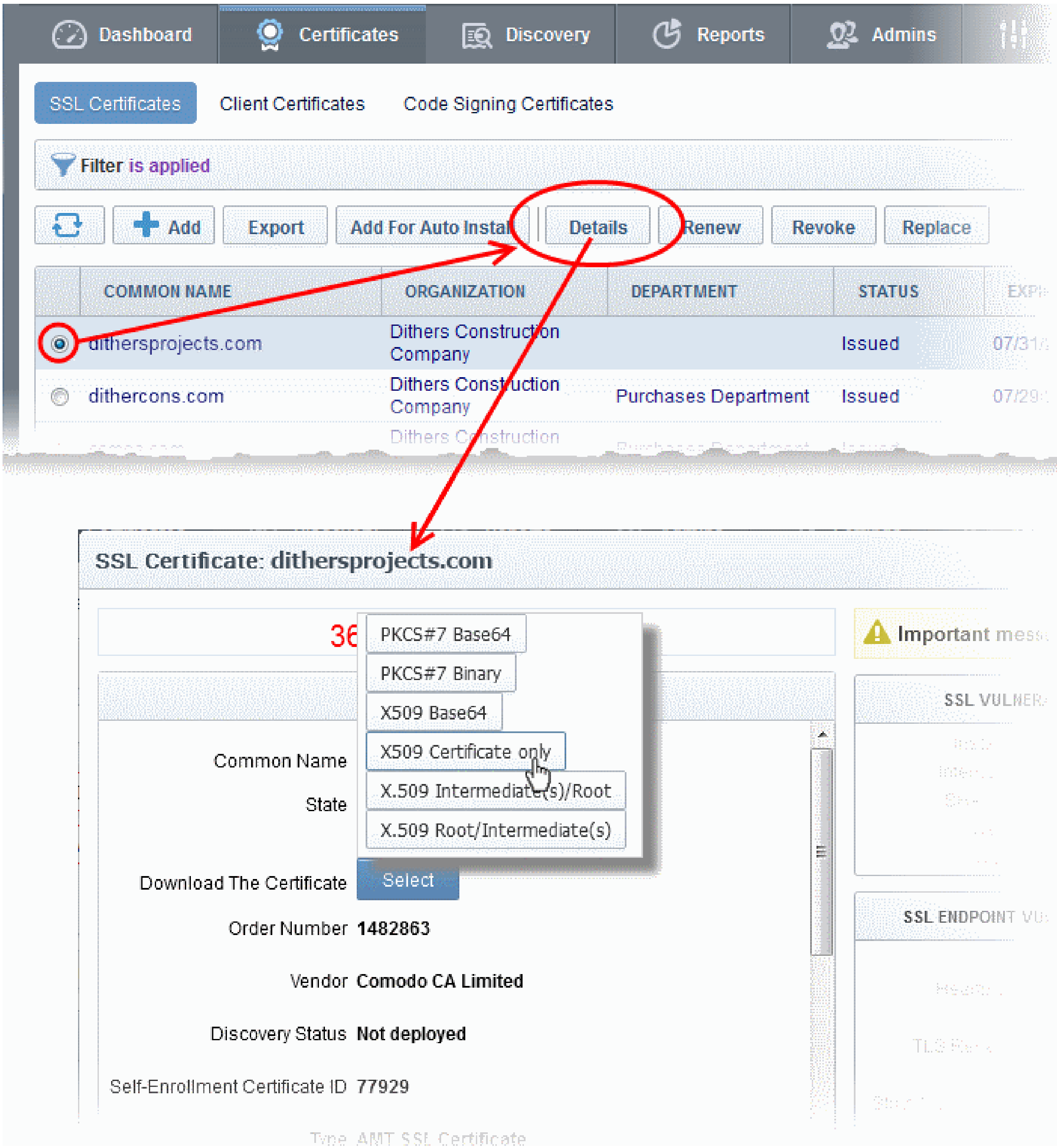
Collection of SSL certificate from the InCommon CM interface

You can download the certificate from the SSL Certificates management area of the InCommon CM console.

To download the certificate

- Open the SSL Certificates management area by clicking the 'Certificates' tab and then clicking 'SSL Certificates'.
- Choose the certificate and click the 'Details' button from the top.

The certificate details dialog will appear.



COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPI
● dithersprojects.com	Dithers Construction Company		Issued	07/31/
○ dithercons.com	Dithers Construction Company	Purchases Department	Issued	07/29/

Common Name

State

Download The Certificate Select

Order Number 1482863

Vendor Comodo CA Limited

Discovery Status Not deployed

Self-Enrollment Certificate ID 77929

Type AMT SSL Certificate

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

The certificate can now be installed on the server.

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

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

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

Request and Issuance of Client Certificates

InCommon CM allows you to issue client certificates to end-users for enrolled domains. Client certificates can only be issued for domains which have been delegated to an organization or department.

Client certificates can be requested/issued in two ways:

- **Adding End-users to InCommon CM** - You can add end-users to InCommon CM by entering their details manually or by importing a list of end-users from a CSV file. You can then initiate the issuance process by sending end-users an invitation mail from the InCommon CM console. On clicking the validation link in the email, the user will be presented with a certificate registration form which they need to complete and submit. After issuance, InCommon CM will send a collection email to the user so they can download and install the certificate.
- **Auto-creation of end-users by self-enrollment** - End-users can enroll themselves to InCommon CM by completing the self-enrollment form. Users must enter the 'Access Code' or 'Secret code' specific to the organization to which the domain belongs. The Access Code and the Secret code are specified under the 'Client Certificates' tab in the Create/Edit Organization/Department dialog. Upon successful validation of the application, the end-user will be automatically added to InCommon CM and will receive a collection email to download and install the certificate.

The reminder of this section explains the method of manually adding the end-users and provisioning them with client certificates. For detailed explanations on directing end-users to self enrollment, refer to the section 'Request and Issuance of Client Certificates' in the Administrator guide.

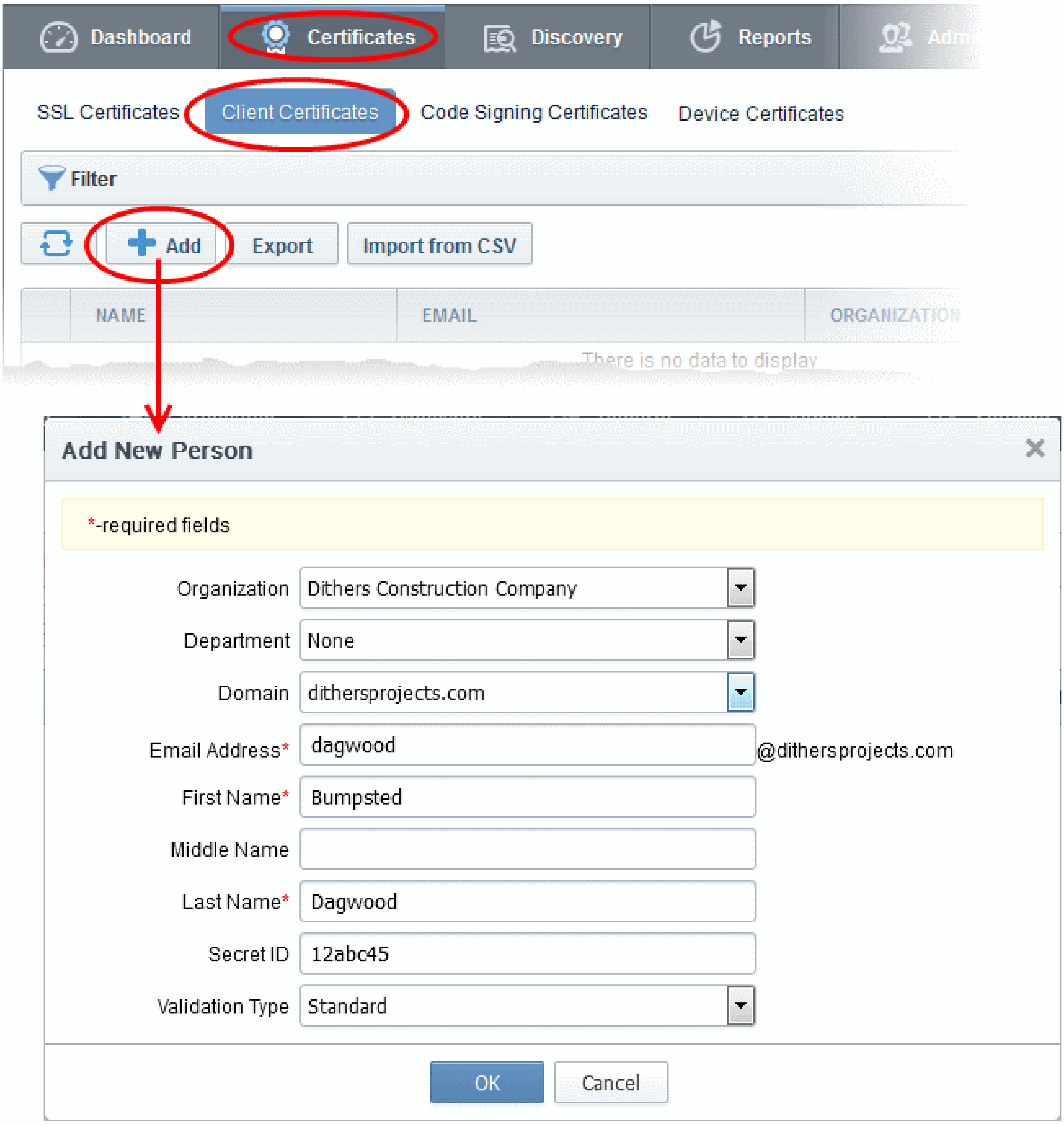
You can add client certificate end-users to InCommon CM in the following ways:

- **Manually enter the details of each end-user** - You need to enter the details of each user manually in the 'Add New Person' form to add the user to InCommon CM. The 'Add New Person' form is accessible from the 'Client Certificates' area under the 'Certificates' tab in the InCommon CM console.
- **Import a list of users from a CSV file** - You can create a .csv file containing a list of users with details like user name, email address, Organization, Department and so on. Each entry should have six mandatory and six optional fields for the details, in a specified order. You can upload the .csv file to the 'Client Certificates' area under the Certificates tab in the InCommon CM console to add the users in the list to InCommon CM.
- **Auto-enroll users through Active Directory (AD) Integration** - You can integrate your AD server with InCommon CM by installing the InCommon CM AD agent. You can then automatically import end-users and provision client certificates to them. For more details, contact your InCommon Account Manager.

This section explains the process of manually adding the end-users. For explanations and tutorials on importing users from a .csv file, refer to the section 'Request and Issuance of Client Certificates' in the Administrator guide.

To add an end-user

- Open the 'Client Certificates' management area by clicking the 'Certificates' tab and then clicking 'Client Certificates'.
- Click the 'Add' button to open the 'Add New Person' form:



Add New Person

*-required fields

Organization	Dithers Construction Company
Department	None
Domain	dithersprojects.com
Email Address*	dagwood @dithersprojects.com
First Name*	Bumpsted
Middle Name	
Last Name*	Dagwood
Secret ID	12abc45
Validation Type	Standard

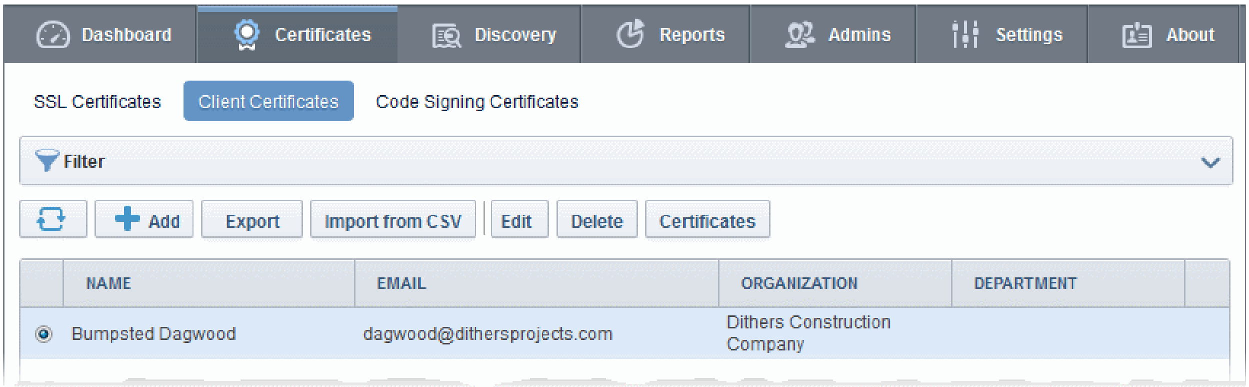
Form Element	Description
Organization	Select the Organization that they wish the new end-user belongs to.
Department	If required, choose the Department that the end-user belongs to.
Domain	The drop-down lists the domains delegated to the selected organization/department. Choose the domain to which the user is belongs. The domain must have passed DCV and the email address of the user should be from the same domain.
Email Address	Enter the username part of the email address of the user. The domain part is automatically entered as the domain chosen.
First Name	Enter the first name of the end-user.
Middle Name	If required, enter the middle name of the end-user.
Last Name	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	A 'Secret ID' (or 'Secret Identifier'/SID) is used to identify the details of an existing end-user in the 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 needs only to specify the email address If you wish to allow enrollment by Secret ID then fill this field with a alpha-numeric string.
Validation Type	**Note**: The 'Validation Type' drop-down will only be visible if enabled by your account manager. Allows you to specify the type of client certificate that is issued to an applicant. The difference between the two lies in the degree of user authentication carried out prior to issuance. The two options are 'Standard' and 'High'. 'Standard' certificates can be issued quickly and take advantage of the user authentication mechanisms that are built into InCommon CM. A user applying for a 'Standard Personal Validation' certificate is authenticated using the following criteria: • User must apply for a certificate from an email address @ a domain that has been delegated to the issuing Organization • The Organization has been independently validated by an web-trust accredited

Form Element	Description
	Certificate Authority as the owner of that domain • User must know either a unique Access Code or Secret ID that should be entered at the certificate enrollment form. These will have been communicated by the administrator to the user via out-of-band communication. • User must be able to receive an automated confirmation email sent to the email address of the certificate that they are applying for. The email will contain a validation code that the user will need to enter at the certificate collection web page. 'High Personal Validation' certificates require that the user undergo the validation steps listed above AND • Face-to-Face meeting with the issuing Organization **Note**: The additional validation steps must be completed PRIOR to the administrator selecting 'High Personal Validation' type.
Principal Name	**Note**: The 'Principle Name' field will only be visible if 'Principal Name Support' is enabled by your InCommon account manager. You 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. Administrators can check whether an Organization or Department is enabled for Principal Name support from the 'Settings' interface. Click 'Settings' > 'Organizations', select an organization in the list, click the 'Edit button' and open the 'Client Cert' tab. This field will be not available for organizations that do not have Principal Name support enabled. If Principal Name support is enabled for an organization but not for the department, this field will not be displayed in the form, but the principal name field in the issued certificate will be auto populated with the email address entered in the Email Address field.
Copy E-Mail	Auto-fills the Principal Name field with the email address entered in the E-mail Address field. This button will be available only if the 'Principal Name Customization' is enabled for the organization/department.

- Enter the details of the end-user as explained above and click 'OK'.

The end-user's details can be modified at any time by clicking the 'Edit' button at the top after selecting the checkbox next to their name in the main list of end-users. If any information in this dialog is changed, with the exception of Secret ID, any previously issued client certificates for this email address shall be automatically revoked. InCommon CM maintains a username history. If the username is changed, the Administrator will still be able to search for the client certificates using both the old name and the new name.

The user will be added to the list of users in the Client Certificates interface.

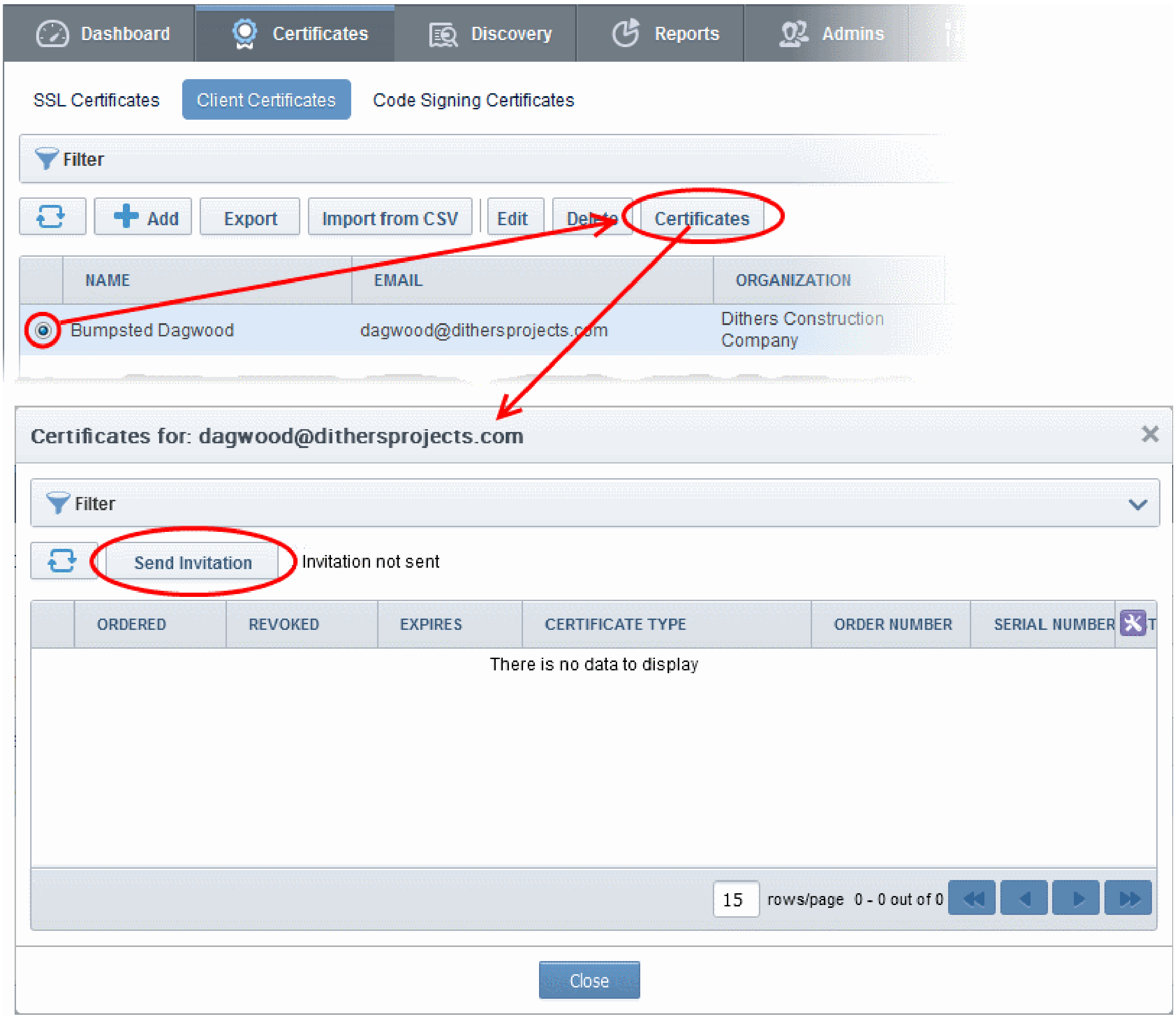


	NAME	EMAIL	ORGANIZATION	DEPARTMENT
●	Bumpsted Dagwood	dagwood@dithersprojects.com	Dithers Construction Company	

- Repeat the process to add more number of users.

To initiate enrollment for the end-user for client certificate

- Open the 'Client Certificates' management area by clicking the 'Certificates' tab and then clicking 'Client Certificates'.
- Select the user and click 'Certificates' from the options at the top.



NAME	EMAIL	ORGANIZATION
Bumpsted Dagwood	dagwood@dithersprojects.com	Dithers Construction Company

Certificates for: dagwood@dithersprojects.com

Invitation not sent

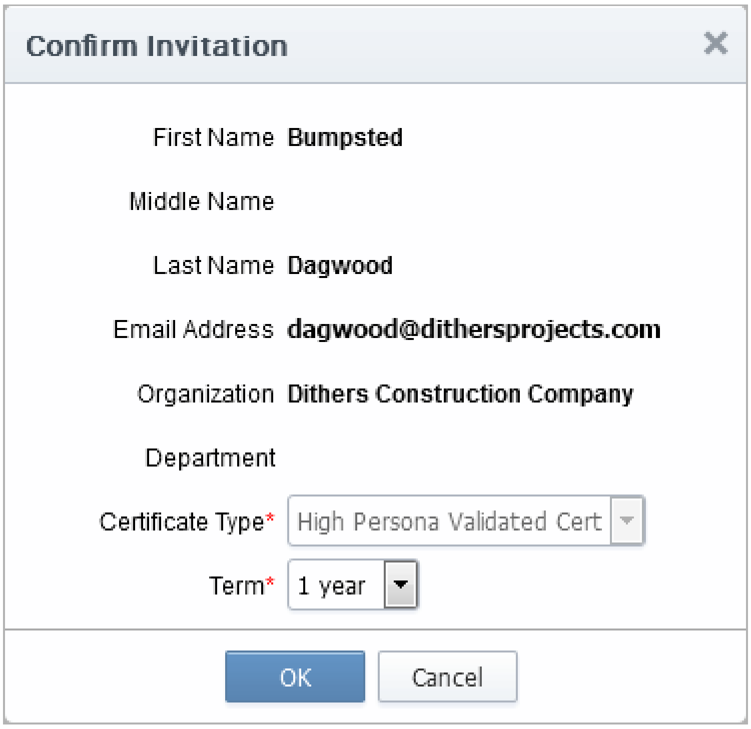
ORDERED	REVOKED	EXPIRES	CERTIFICATE TYPE	ORDER NUMBER	SERIAL NUMBER

There is no data to display

15 rows/page 0 - 0 out of 0

- Click 'Send Invitation'.

A confirmation dialog will appear.



Confirm Invitation

First Name	Bumpsted
Middle Name	
Last Name	Dagwood
Email Address	dagwood@dithersprojects.com
Organization	Dithers Construction Company
Department	
Certificate Type*	High Persona Validated Cert
Term*	1 year

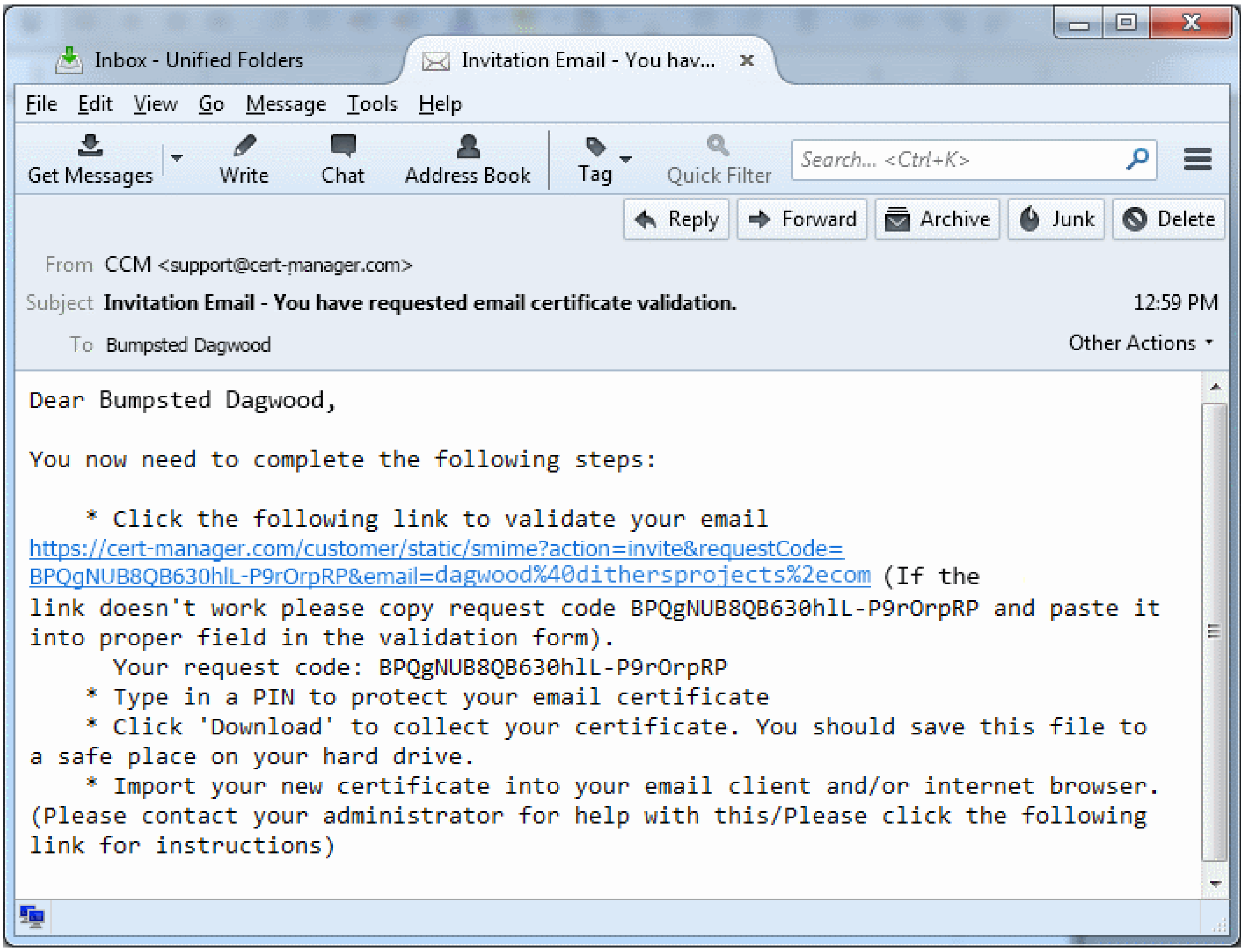
- Certificate Type - If your Organization's account has been enabled for High Personal Validated Certificates AND the administrator has specified a 'Validation Type' of 'High' * for this user THEN the 'Certificate Type' value will be a drop down menu rather than flat text. This menu will offer a choice 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.

- Click 'OK'.

An invitation email will be sent to the end-user.

- Repeat the process to enroll more users.

The invitation 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. 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. An example mail is shown below.



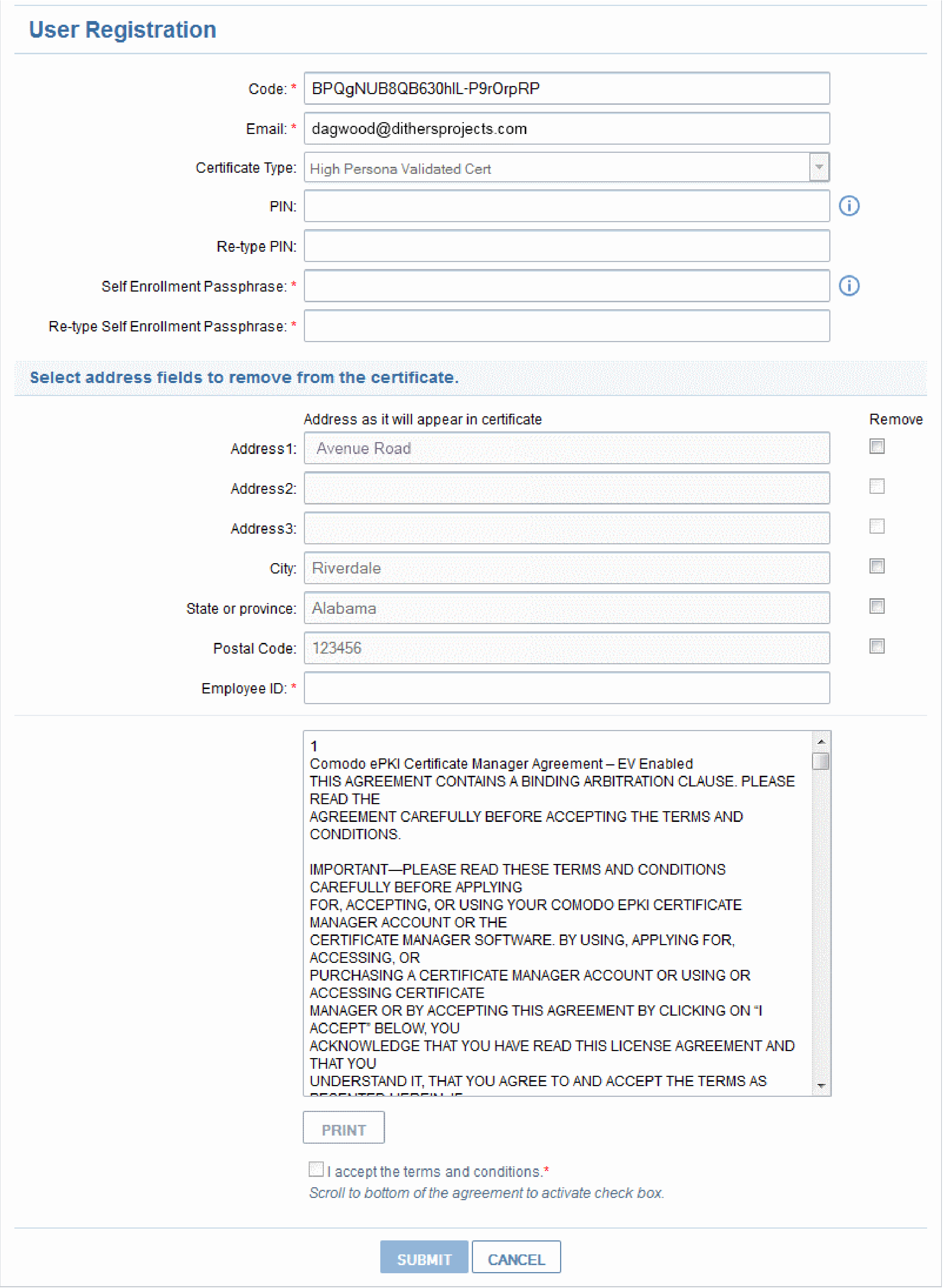
From CCM <support@cert-manager.com>

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

To Bumpsted Dagwood

```
Dear Bumpsted Dagwood,

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=dagwood%40dithersprojects%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)
```

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



User Registration

Code: *	BPQgNUB8QB630hlL-P9rOrpRP	
Email: *	dagwood@dithersprojects.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:	Avenue Road	□
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

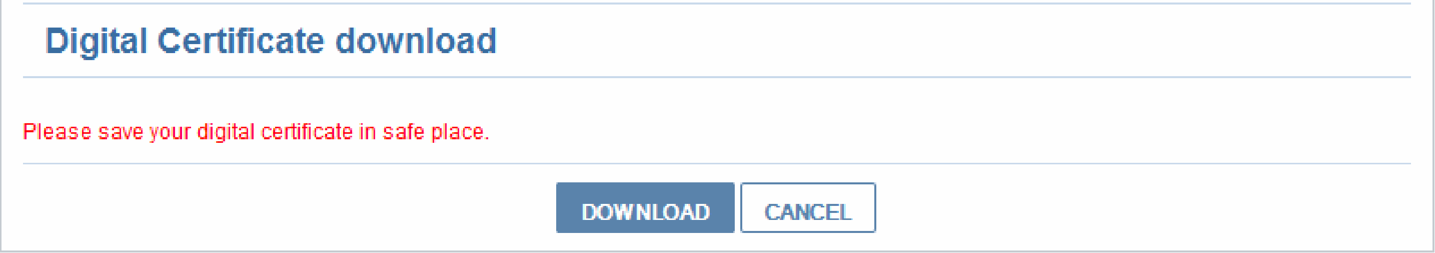
□ I accept the terms and conditions.*

Scroll to bottom of the agreement to activate check box.

Form Element	Description
Code **(required)**	The validation request code. This field is auto-populated when the applicant clicks the validation link contained in the email.
Email **(required)**	Email address of the applicant. This field is auto-populated.
PIN **(required)**	The applicant should specify a PIN for the certificate to protect the certificate.
Re-type PIN **(required)**	Confirmation of the above.
Pass-Phrase **(required)**	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)**	By default, the address details are displayed in the 'Certificate Details' dialog. The applicant can hide these details selectively by selecting the 'Remove' checkboxes beside the required address fields.
EULA Acceptance **(required)**	Applicant must accept the terms and conditions before submitting the form.

The user needs to fill-in the information as explained above, accept to the 'End User License Agreement' and click 'Submit'.

Upon successful submission of the 'User Registration' form, a download dialog will be displayed enabling the end-user to download and save the certificate.



Digital Certificate download

Please save your digital certificate in safe place.

InCommon 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.

Request and Issuance of Code Signing Certificates

- You can issue code-signing certificates to users with email addresses at domains you have added to CM
- Each domain should have been delegated to an InCommon CM organization/ department and should have passed DCV.

You can add code signing certificate end-users to the certificate manager in two ways:

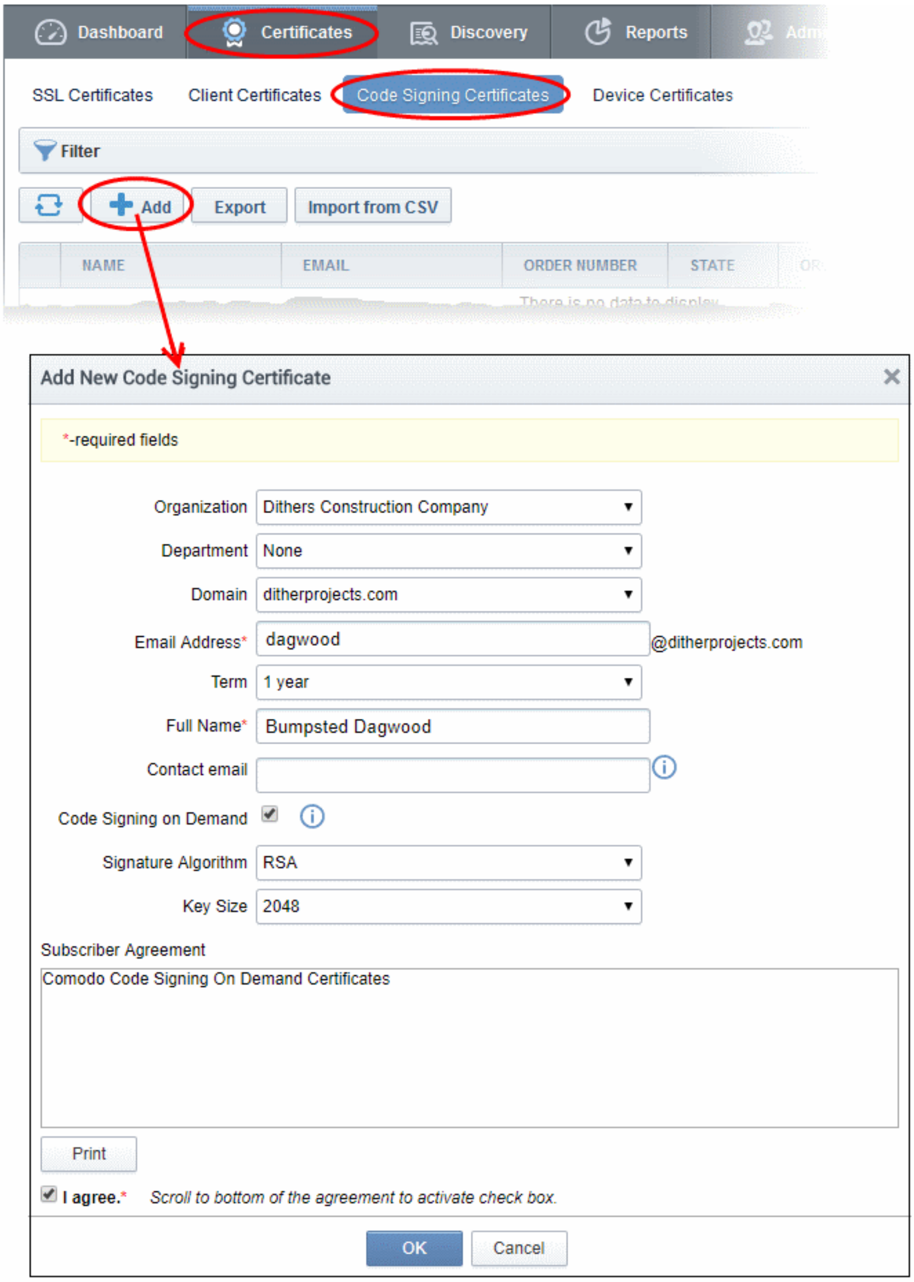
- **Manually entering the details of each end-user** - You need to enter the details of each user manually in the 'Add New Code Signing Certificate' form to add the user to the CM. The form is accessible from the 'Code Signing Certificates' area under the 'Certificates' tab in the InCommon CM console.
- **Importing list of users from a CSV file** - You can create a .csv file containing a list of users with details like user name, email address, Organization, Department and so on. Each entry should have four mandatory and two optional fields for the details, in a specified order. You can upload the .csv file to the 'Code Signing Certificates' area under the 'Certificates' tab in the InCommon CM console.

Once the users are added, InCommon CM will automatically send invitation mails to them. On clicking the validation link in the email, the end-user will be presented with a 'User Registration' form. The end-user needs to fill-in and submit the form. InCommon CM will send a collection email to the end-user in order for them to download and install the certificate.

This section explains the process of manually adding the end-users. For explanations and tutorials on importing users from a .csv file, refer to the section 'Request and Issuance of Code Signing Certificates' in the Administrator guide.

To add an end-user

- Open the 'Code Signing Certificates' area by clicking the 'Certificates' > 'Code Signing Certificates'.
- 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	ditherprojects.com
Email Address*	dagwood @ditherprojects.com
Term	1 year
Full Name*	Bumpsted Dagwood
Contact email	
Code Signing on Demand	☑
Signature Algorithm	RSA
Key Size	2048

Subscriber Agreement

Comodo Code Signing On Demand Certificates

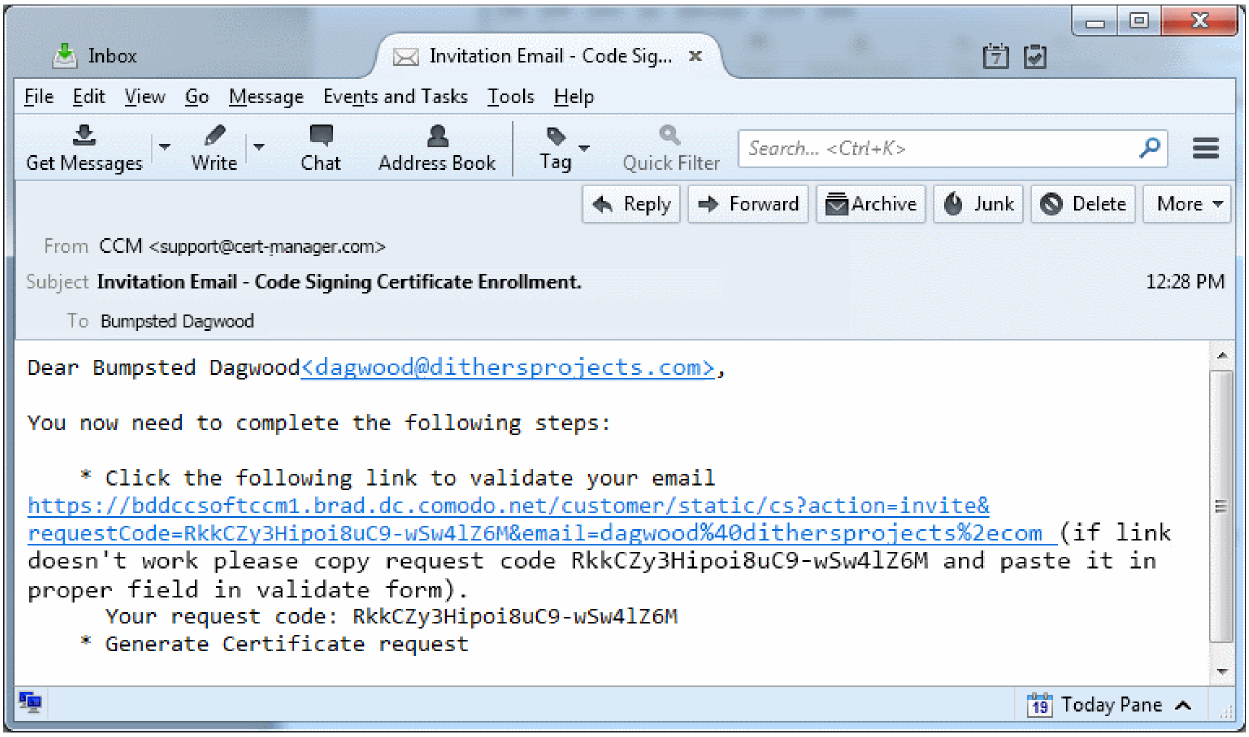
☑ **I agree.*** *Scroll to bottom of the agreement to activate check box.*

Add New Code Signing Certificate dialog - Table of parameters	
Field	**Description**
Organization	Select the Organization to which the end-user belongs.
Department	Select the Department to which the end-user 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.

Add New Code Signing Certificate dialog - Table of parameters	
Field	**Description**
Email Address	Enter the username part of the email address of the user. The domain part is automatically entered as the domain chosen.
Full Name	Full name of the applicant.
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	Allow the certificate to be used by the CSoD service. Note: If this option is selected, the issued certificate will be downloaded and stored by the CSoD controller. Click here for more details.
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.

- Complete the 'Add New Code Signing Certificate' form.
- Click 'OK'.
- Repeat the process to add more users.

If the end-user is an existing user, the corresponding certificate will be automatically added to the CM and a certificate collection email will be sent to the end-user. If the end-user is a new user, an invitation mail will be sent to initiate self enrollment process. The invitation email will contain the URL of the user registration 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. 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. An example mail is shown below.



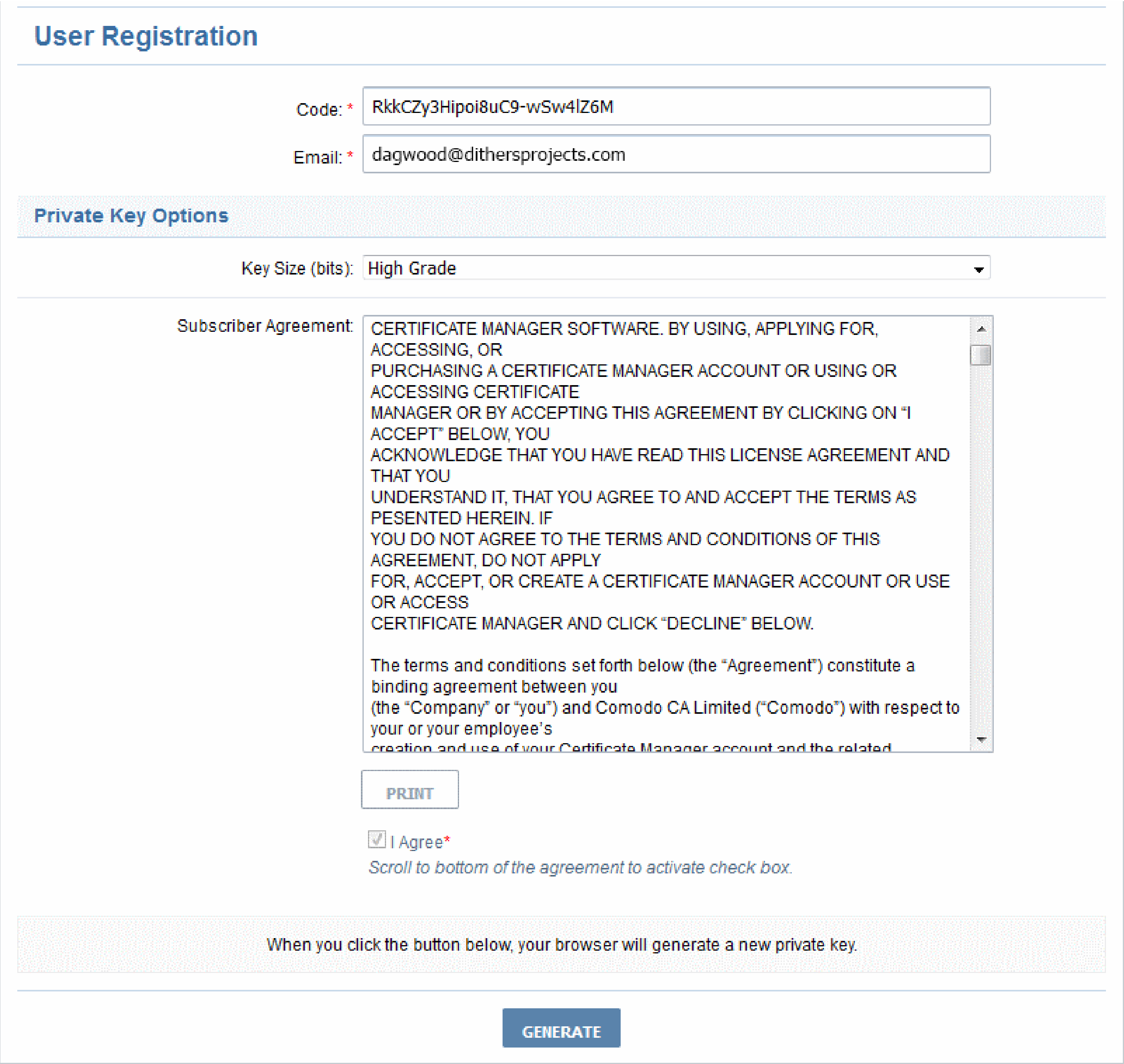
From CCM <support@cert-manager.com>

Subject **Invitation Email - Code Signing Certificate Enrollment.** 12:28 PM

To Bumpsted Dagwood

```
Dear Bumpsted Dagwood<dagwood@dithersprojects.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=RkkCZy3Hipoi8uC9-wSw4lZ6M&email=dagwood%40dithersprojects%2ecom (if link
doesn't work please copy request code RkkCZy3Hipoi8uC9-wSw4lZ6M and paste it in
proper field in validate form).
      Your request code: RkkCZy3Hipoi8uC9-wSw4lZ6M
    * Generate Certificate request
```

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



User Registration

Code: * RkkCZy3Hipoi8uC9-wSw4lZ6M

Email: * dagwood@dithersprojects.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*

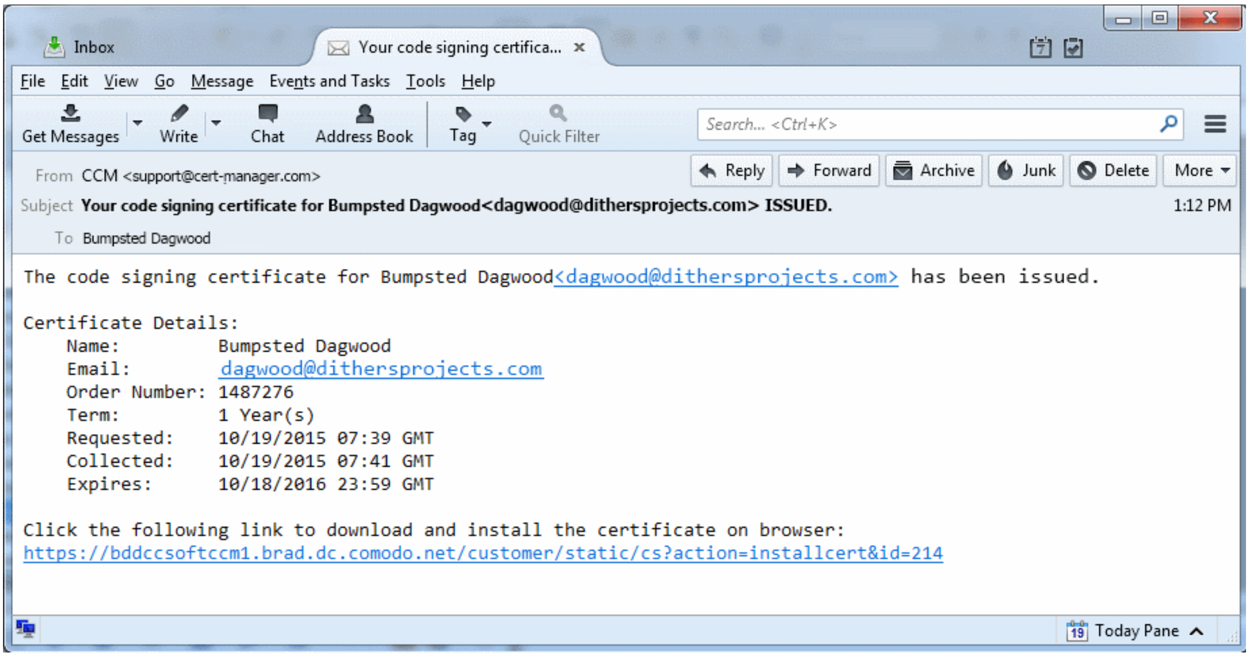
Scroll to bottom of the agreement to activate check box.

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

Form Element		Description
Code (***required***)		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***)		The email address of the applicant. This field will be auto-populated.
Advanced Private Key Options	Key Size	The applicant can select the key size for the private key of the certificate (Default = 2048 bit)

Form Element	Description
	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 end-users are strongly advised to backup their private key, during certificate installation process.
Subscriber Agreement (***required***)	Applicant must accept the terms and conditions before submitting the form by reading the agreement and selecting the 'I Agree' checkbox.
Generate	Starts the certificate generation process.

Once the end-user submits the form, the certificate request will be automatically generated and a request will be sent to InCommon CM. The CM will process the request and send a certificate request to InCommon CA Server. Once the certificate is issued the CM collects the certificate and sends a notification email to the end-user. The end-user can follow the link to download and install the certificate can use it for digitally signing the executables.



From CCM <support@cert-manager.com>

Subject **Your code signing certificate for Bumpsted Dagwood<dagwood@dithersprojects.com> ISSUED.** 1:12 PM

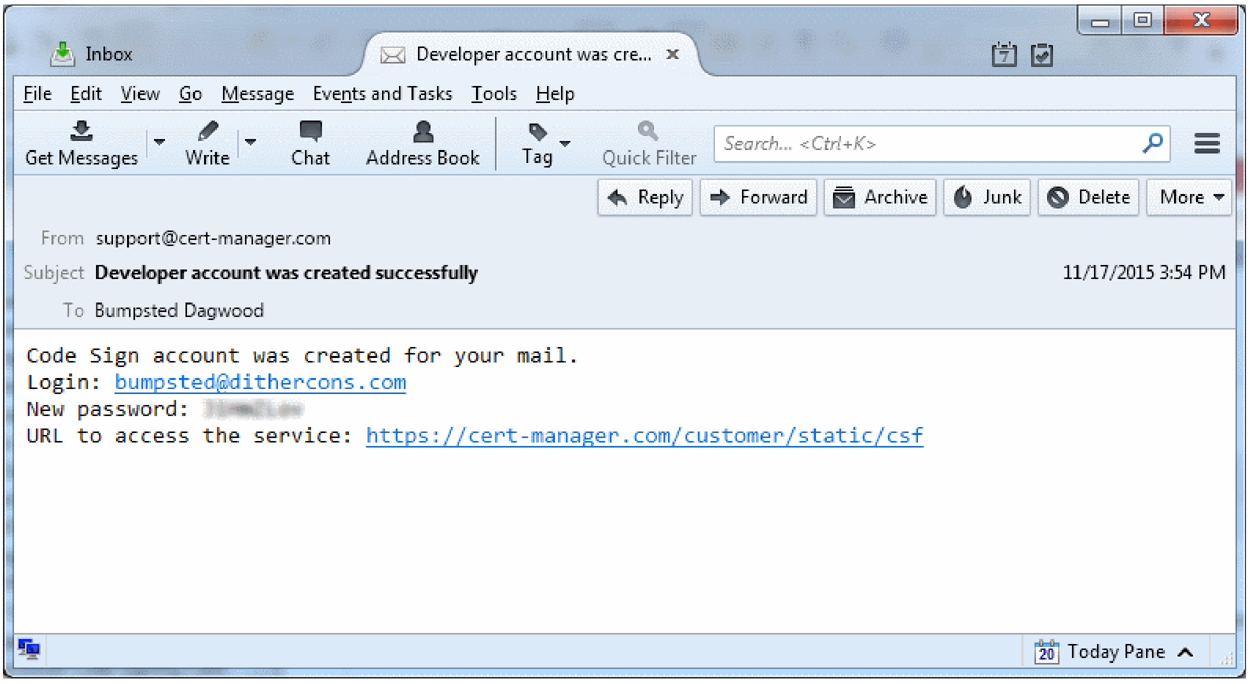
To Bumpsted Dagwood

```
The code signing certificate for Bumpsted Dagwood<dagwood@dithersprojects.com> has been issued.

Certificate Details:
    Name:          Bumpsted Dagwood
    Email:         dagwood@dithersprojects.com
    Order Number:  1487276
    Term:          1 Year(s)
    Requested:     10/19/2015 07:39 GMT
    Collected:     10/19/2015 07:41 GMT
    Expires:       10/18/2016 23:59 GMT

Click the following link to download and install the certificate on browser:
https://bddccsoftccm1.brad.dc.comodo.net/customer/static/cs?action=installcert&id=214
```

Code Signing on Demand Service option selected

- If the CSoD option is selected, no notification email will be sent to the end user.
- The certificate application will be tracked by the CSoD controller configured for the domain.
- After the certificate is issued, the controller will automatically download the certificate and store it.
- Admins can add developers in the 'Code Signing on Demand' > 'Developers' interface. A 'Developer' will upload the code or hash for signing, and will collect the items once signed.

- Developers will receive a notification email which tells them how to access the CSoD portal. An example mail 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
```

The developer can log in to the CSoD service portal in order to submit the files for signing. The CSoD enabled certificate can be downloaded by the administrator for the developer, if required.

Step 7 - Generate Reports

You can generate and view reports that reflect an activity and other statistics related to usage, provisioning and monitoring of SSL and Client and Code Signing Certificates. There are 14 main types of reports available: Activity Log report, Client Certificates report, Discovery Scan Log , SSL Certificates report, Code Signing Certificates report, Admin report, XML Data report, DCV report, Agent Log Events report, Notification Log Statistics report and Net Discovery Tasks.

- The **Activity Log report** – A report which covers all events concerning all types of certificates
- The **Client Certificates reports** - A report which covers all events concerning client certificates.
- The **Discovery Scan Log reports** - A report which covers all events related to discovery scans and discovered SSL certificates.
- The **SSL Certificates report** - A report which covers all events concerning SSL certificates
- The **Code Signing Certificates report** - A report which covers all events concerning code signing certificates.
- The **Code Signing Requests report** - A report which covers all requests made for Code Signing on Demand (CSoD) by developers.
- The **Admins report** – View a list of all administrators and their privilege levels.
- The **XML Data report** – An XML report containing details about Organizations, Departments, their administrators and their certificates.
- The **DCV Report** A report which details the Domain Control Validation (DCV) status for all registered domains.
- The **Agent Log Events report** A report which covers all scan and certificate installation activities by certificate controller agents.

- The **Notification Log Statistics Report** - A report which details about notifications emails, notification types and overall notification logs.
- The **Private Key Controller Activity Log report** - A report which covers all activity by the Private Key Controller.
- The **Net Discovery Tasks report** - A report on any discovery tasks, configured for organization(s) and department(s).

Please refer to the chapter 'Reports' in the Administrator's Guide for detailed explanations on each type of the report and tutorials on generating them.

Appendix - Certificate Types

If you do not know which type of certificate to choose then we recommend that you first contact your SSL admin who should be able to advise you. This appendix is provided only to give applicants an understanding of the different types of certificate that are available but does not cover pricing or warranty levels. The appendix opens with a definition of terms that should provide an insight into SSL terminology and concludes with a table listing all certificates offered by InCommon CA. Note - this is a *complete* list of InCommon certificates. You might not see all of these certificate types if your administrator hasn't made them available.

Validation Levels

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

EV: Extended **V**alidation certificates provide the highest levels of trust and reassure web site visitors that it is safe to trade by turning the address bar green during https sessions. EV's are generally more expensive than OV level certificates and require a more in-depth validation process prior to issuance. However, because the green bar has become a hallmark of security seen on the Internet's largest and most prestigious websites, placing an EV on your website can often lead to increased customer conversion.

Certificate Types

SDC: Single **D**omain **C**ertificates - will secure a single fully qualified domain name such as www.company.com

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

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

Additional Technologies

SGC: **S**erver **G**ated **C**ryptography. SGC technology upgrades the encryption capabilities of older browsers to modern day standards

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	1 year - 3 years

Certificate Name	Type	Validation Level	Description	Maximum Term Length
			Office Communications servers	
InCommon Intranet SSL Certificate	SDC	OV	Secures a single internal host	1 year - 3 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