

InCommon®



InCommon Certificate Manager

Introduction to Auto-Installer

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

InCommon Certificate Manager - Introduction to Auto-Installer

This document is intended to introduce the new certificate Auto-Installer feature in InCommon Certificate Manager.

In brief:

- The new feature allows MRAO and RAO admins to automate the remote installation of any SSL certificate on Apache Tomcat, Apache/ModSSL ApacheSSL, IIS and F5 BIG-IP web-servers (more web-server types coming soon).
- The feature is enabled on a per-certificate basis by selecting the 'Auto install initial certificate' option in the 'Request New SSL Certificate' form
- There are two modes of implementation:

Enterprise Controller Mode	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 coordinate automatic CSR generation and certificate installation. See Method 2 - CM Controller Mode

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. The controller is configured through a web-interface and can be set to communicate with InCommon CA infrastructure through a proxy server.
- 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.
- iii. The auto-installation/renewal is enabled for the following server types:
 - Apache/Mod SSL
 - Apache - SSL
 - Apache Tomcat
 - Microsoft IIS 1.x to 4.x (Server 2000 - 2008R2)
 - Microsoft IIS 5.x and above (Server 2000 - 2008R2)
 - F5 BIG-IP

See [Method 1 - Enterprise Controller Mode](#) for a tutorial on automatic installation of Certificates on remote web servers

2. 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.

iii. The auto-installation/renewal is available for the following server types:

- Apache/Mod SSL
- Apache - SSL
- Apache Tomcat
- Microsoft IIS 1.x to 4.x (Server 2000 - 2008R2)
- Microsoft IIS 5.x and above (Server 2000 - 2008R2)

See [Method 2 - CM Controller Mode](#) for a tutorial on automatic installation of Certificates on web servers.

- If the admin chooses to install:
 - Windows IIS, Tomcat and F5 BIG-IP servers - the certificate will be activated immediately and the 'Server Software' state will be changed to 'Active' in InCommon CM
 - Apache servers - the server will need to be restarted to finalize installation. The 'Server Software' state will be changed to 'Restart Required' in InCommon CM
- Once configured and running, the agent also helps automate the renewal of the certificate by, effectively, repeating this process close to expiry time (creating a new CSR and presenting it for approval by the InCommon CM admin).

The remainder of this document is the portion of Administrator guide of InCommon Certificate Manager, that explains the process of application through installation of an SSL certificate using the new Auto-Installer feature.

Method 1 - Enterprise Controller Mode

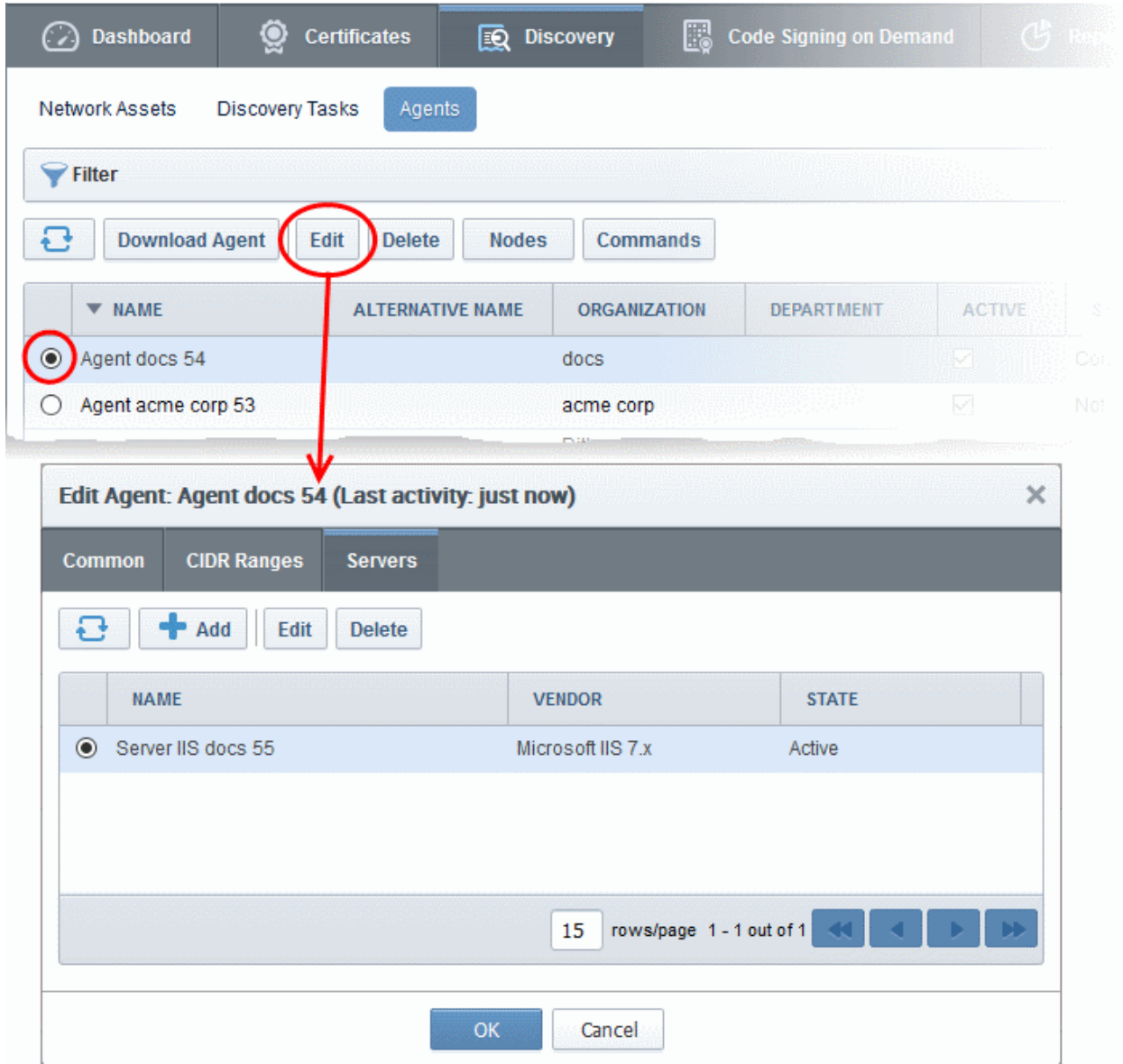
Enterprise Controller mode allows admins to automatically install certificates on any remote server on the network.

- Controller software first needs to be installed on a server in your network.
- You then need to add web-servers to the controller to enable certificate auto-installation. This is done in the 'Discovery' > 'Agents' interface.
- If a new certificate is requested for an associated server, the controller will coordinate with the host to generate a CSR, submit it to InCommon CA, collect the certificate and install it.

- The controller software is configured through a dedicated web-interface. If required, the controller can be set to communicate with InCommon CA through a proxy server. See [Configuring the Certificate Controller Agent through Web Interface](#) if you need help with this.

To add remote servers to the certificate controller

- Click 'Discovery' > 'Agents':



The screenshot shows the 'Agents' page in the InCommon Certificate Manager. The 'Edit' button for 'Agent docs 54' is circled in red, with an arrow pointing to the 'Edit Agent: Agent docs 54' dialog box. The dialog box has tabs for 'Common', 'CIDR Ranges', and 'Servers'. The 'Servers' tab is active, showing a table with one server entry: 'Server IIS docs 55' from 'Microsoft IIS 7.x' in an 'Active' state. The dialog also includes 'Add', 'Edit', and 'Delete' buttons, a table with columns 'NAME', 'VENDOR', and 'STATE', and 'OK' and 'Cancel' buttons at the bottom.

NAME	ALTERNATIVE NAME	ORGANIZATION	DEPARTMENT	ACTIVE	STATUS
Agent docs 54		docs		<input checked="" type="checkbox"/>	Con...
Agent acme corp 53		acme corp		<input checked="" type="checkbox"/>	No...

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

- Select the controller, click 'Edit' then open the 'Servers' tab

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

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

Edit Agent: Agent docs 54 (Last activity: just now) [X]

Common | CIDR Ranges | **Servers**

[Refresh] **+ Add** [Edit] [Delete]

	NAME	VENDOR	STATE
<input checked="" type="radio"/>	Server IIS docs 55	Microsoft IIS 7.x	Active

Add Web Server [X]

*-required fields

Name*

Vendor*

State

Remote

IP address / Port* . . . :

Use key

Username

Password

[OK] [Cancel]



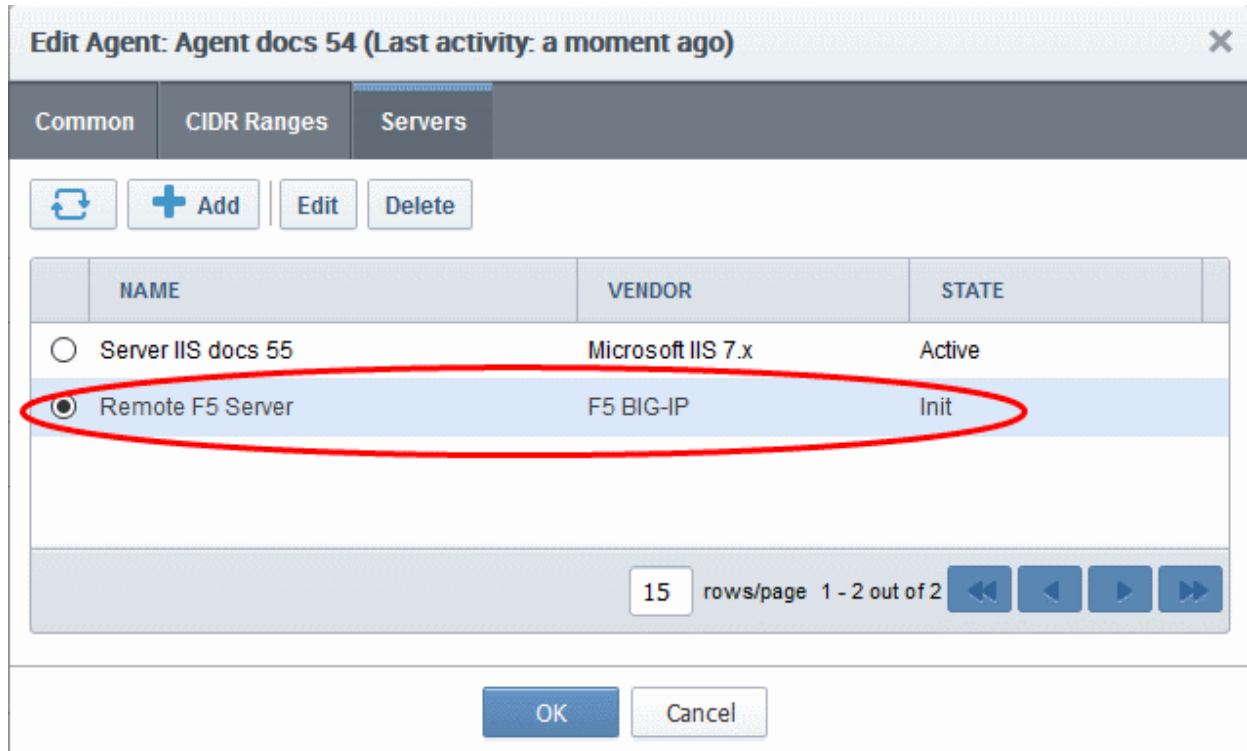
Add Web Servers - Table of Parameters

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: <ul style="list-style-type: none"> • Microsoft IIS 7.x • Apache, Tomcat 5.x, 6.x and 7.x • F5 BIG-IP <p>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).</p>
State		Indicates whether or not the server is connected. The connection will be initialized and 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.

Add Web Servers - Table of Parameters

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)

Common | CIDR Ranges | **Servers**

Refresh | **+ Add** | Edit | Delete

	NAME	VENDOR	STATE
<input type="radio"/>	Server IIS docs 55	Microsoft IIS 7.x	Active
<input checked="" type="radio"/>	Remote F5 Server	F5 BIG-IP	Init

15 rows/page 1 - 2 out of 2

OK Cancel

Once the remote server is added to the controller, administrators can apply for certificates for domains on the server in the 'Certificates Management' > 'SSL Certificates' area.

- Repeat the process to add more remote servers

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.



Request New SSL Certificate

*-required fields

Organization* ⓘ Refresh

Department*

[Click here to edit address details](#)

Certificate Type*

Certificate Term*

Server Software*

CSR

Signature Algorithm

Key Size

Certificate Parameters

Common Name*

Requester

External Requester ⓘ

Comments

Renewal & Installation

Auto renew days before expiration

Create new key pair

Auto install renewed certificate

Auto install initial certificate

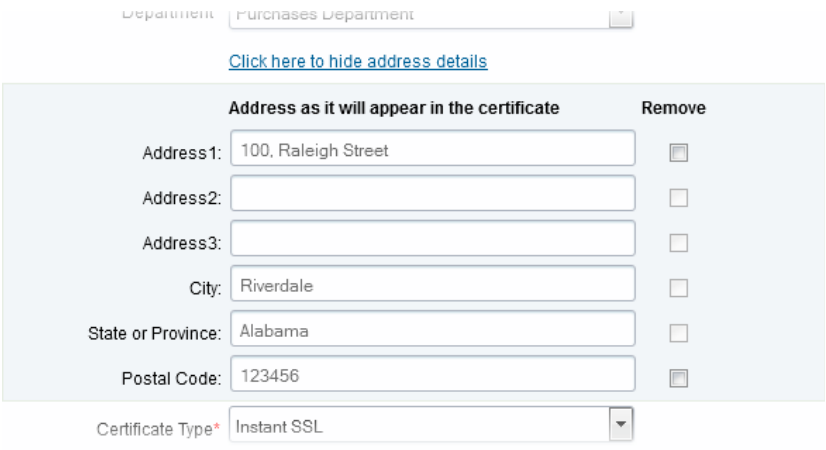
Subscriber Agreement

Print

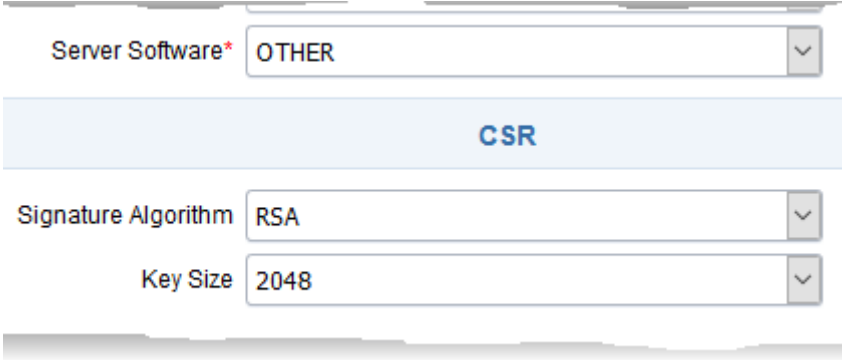
I agree.* Scroll to bottom of the agreement to activate check box.

OK Cancel



Form Element	Type	Description
Organization <i>(required)</i>	Drop-down list	Choose the Organization that the SSL certificate will belong to.
Department <i>(required)</i>	Drop-down list	Choose the Department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'.
Click here to edit address details	<i>Text Fields</i>	<p>Clicking this link will expand the address fields.</p>  <p>The address fields are auto-populated from the details of the Organization or Department on whose behalf this certificate request is being made.</p> <p>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.</p> <p>The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted".</p> <p>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.</p>
Certificate Type <i>(required)</i>	<i>Drop-down list</i>	<p>Choose the certificate type that you wish to add for auto-installation.</p> <p>Note: Currently InCommon CM supports auto-installation only for the 'Instant SSL' certificate type. Other certificate types will be enabled for auto-installation in the future versions.</p>
Certificate Term	<i>Drop-down list</i>	Choose the validity period of the certificate. For example, 1 year, 2



Form Element	Type	Description
(<i>required</i>)		years, 3 years.
Server Software (<i>required</i>)	<i>Drop-down list</i>	<p>Select the server software on which the certificate is to be installed. Auto-installation is supported only on the following server types:</p> <ul style="list-style-type: none"> • Apache/Mod SSL • Apache - SSL • Apache Tomcat • Microsoft IIS 1.x to 4.x • Microsoft IIS 5.x and above • F5 BIG-IP <p>Note: Choose 'OTHER' if you want to use F5 BIG-IP.</p>
CSR		
Provide CSR/Autogenerate CSR and Manage Private Key	Leave these fields blank.	After a successful application, the certificate controller will co-ordinate with the web server to create the CSR and submit it to InCommon CA.
CSR (<i>required</i>)	Once you choose 'Auto install initial certificate' under ' Renewal & Installation ' in this form, these fields will disappear.	
Get CN from CSR (<i>optional</i>)	You can choose the signature algorithm to be used by the public key of the certificate and the key size for the certificate under 'CSR'.	
Upload CSR (<i>optional</i>)		
Certificate Parameters		
Common Name (<i>required</i>)	<i>Text Field</i>	Type the domain that the certificate will be issued to.
Requester (<i>auto-populated</i>)	<i>Text Field</i>	The 'Requester' is field is auto-populated with the name of the administrator making the application.


Form Element	Type	Description
External Requester (optional)	<i>Text Field</i>	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. This field is not required when requesting for EV SSL certificate and hence will be hidden.
Comments (<i>optional</i>)	<i>Text Field</i>	Enter your comments on the certificate. This is optional.
Renewal and Installation		
Auto Renew	<i>Checkbox and text field</i>	Enable to auto-renew the certificate when it is nearing expiry. You can also 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.
Create new key pair	<i>Checkbox</i>	Select this option if you want a new key pair is to be generated for the renewal certificate. Leaving it unselected means InCommon CM will re-use the existing key pair of the expiring certificate.
Auto install renewed certificate	<i>Checkbox</i>	Select this option if you want the renewed certificate be auto-installed.
Auto install initial certificate	<i>Checkbox</i>	Select this option to mark this certificate for auto-installation. After completing the form, the auto-installation wizard will allow you to select the nodes on which the certificate should be installed and to create an installation schedule.
Subscriber Agreement (<i>required</i>)	<i>Control</i>	You must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox.

- Click 'OK' to submit the application

The 'Set Auto Renewal & Installation' dialog will be displayed with the 'Nodes' interface opened. The 'Nodes' interface displays a tree structure of servers associated with the Certificate Controller and the domains hosted on them.

✕
Set Auto Renewal & Installation

1 Nodes
 2 Schedule
 3 Port
 4 EULA



NAME	COMMON NAME	PROTOCOL	IP ADDRESS	PORT	STATUS	SSL
					Active	
Remote F5 Server						
<input checked="" type="radio"/> ~Common-test-vs	~Common-test-vs	HTTP	192.168.200.87	80	No SSL	
<input type="radio"/> ~CCMQA~ccmq-cluster01_8459	~CCMQA~ccmq-cluster01_8459	HTTPS	200.200.200.8	8459	Installed	External
<input type="radio"/> ~Common-VS02_HTTP_8459	~Common-VS02_HTTP_8459	HTTPS	192.168.200.87	8459	Installed	External
<input type="radio"/> ~Common-test-vs_8449	~Common-test-vs_8449	HTTPS	192.168.200.87	8449	Installed	External
<input type="radio"/> ~CCMQA~ccmq-cluster01_8450	~CCMQA~ccmq-cluster01_8450	HTTPS	200.200.200.8	8450	Installed	External
<input type="radio"/> ~Common-test-vs_8447_8450	~Common-test-vs_8447_8450	HTTPS	192.168.200.87	8450	Installed	External
<input type="radio"/> ~Common-test-vs_8445	~Common-test-vs_8445	HTTPS	192.168.200.87	8445	Installed	External
<input type="radio"/> ~Common-test-vs_8447	~Common-test-vs_8447	HTTPS	192.168.200.87	8447	Installed	External
<input type="radio"/> ~Common-test-vs_8446	~Common-test-vs_8446	HTTPS	192.168.200.87	8446	Installed	External
<input type="radio"/> ~Common-VS02_HTTP_8455	~Common-VS02_HTTP_8455	HTTPS	192.168.200.87	8455	Installed	External
<input type="radio"/> ~Common-VS-20160912-233122_HTTPS_8454	~Common-VS-20160912-233122_HTTPS_8454	HTTPS	192.168.200.87	8454	Installed	External
<input type="radio"/> ~Common-vstest01_8454	~Common-vstest01_8454	HTTPS	192.168.200.87	8454	Installed	External
<input type="radio"/> ~Common-vstest01_8454_8456	~Common-vstest01_8454_8456	HTTPS	192.168.200.87	8456	Installed	External
<input type="radio"/> ~Common-VS05_HTTPS_9095	~Common-VS05_HTTPS_9095	HTTPS	192.168.200.87	443	Installed	External

15 rows/page 1 - 1 out of 1

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

The 'Schedule' interface will be displayed enabling you to choose whether you wish to manually install the certificate from the InCommon CM interface or set a schedule for auto-installation.

✕
Set Auto Renewal & Installation

1 Nodes
2 Schedule
3 Port
4 EULA

Manual
 Certificate installation must be started manually.

Schedule
 Certificate installation will be started during selected time period.

Time zone: UTC+00:00 - GMT, UCT, UTC, WET, EGST ▼

Start not earlier than: 01/18/2017

Time Of Day

Run Between: 00 : 19 00 : 19

Day of Week

Run Only: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Close
< Back
Next >

- If you want to manually install the certificate from the InCommon CM interface, select 'Manual'
- If you want to install the certificate at a scheduled time, select 'Schedule', select your time zone, and set a time period. The controller will generate the CSR and submit it to InCommon CA the next time it polls InCommon CM after the scheduled time.
- Click 'Next'.

The 'Port' interface will open.

✕
Set Auto Renewal & Installation

1 Nodes
2 Schedule
3 Port
4 EULA

~Common-test-vs 8460

i
 Default node port will be used. Virtual Server ~Common-test-vs:172.16.223.97:80 will be updated by port 8460

Close
< Back
Next >

- Specify the HTTPS port for installing the certificate, (**Default = 9443**)
- Click 'Next'. The EULA interface will open.

Set Auto Renewal & Installation ✕

1 Nodes
 2 Schedule
3 Port
4 EULA

Subscriber Agreement:

Predefined test SSL license text for test customer[2]...

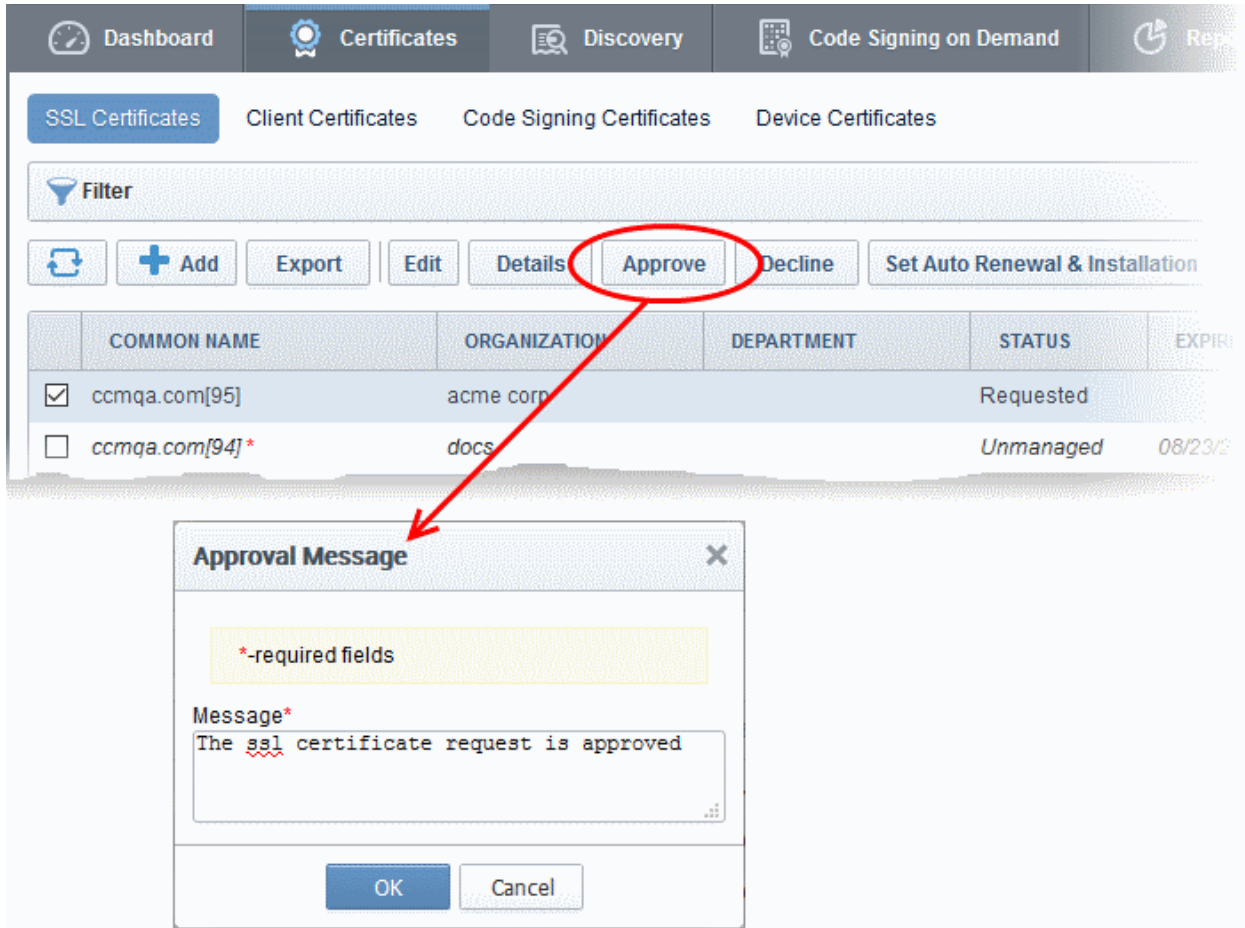
I agree.* *Scroll to bottom of the agreement to activate check box.*

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

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

Dashboard Certificates Discovery Code Signing on Demand Reports Admin						
SSL Certificates Client Certificates Code Signing Certificates Device Certificates						
Filter						
<input type="button" value="Refresh"/> <input type="button" value=" + Add"/> <input type="button" value=" Export"/> <input type="button" value=" Delete"/> <input type="button" value=" Details"/> <input type="button" value=" Revoke"/> <input type="button" value=" Set Auto Renewal & Installation"/>						
	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL ST
<input type="checkbox"/>	ccmqa.com[95] *	acme corp		Requested		Not schedule
<input checked="" type="checkbox"/>	ccmqa.com[94] *	docs		Unmanaged	08/23/2018	Not schedule
<input type="checkbox"/>	ccmqa.com[93] *	docs		Unmanaged	08/22/2018	Not schedule
<input type="checkbox"/>	ccmqa.com[92] *	docs		Unmanaged	07/14/2018	Not schedule

- 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:

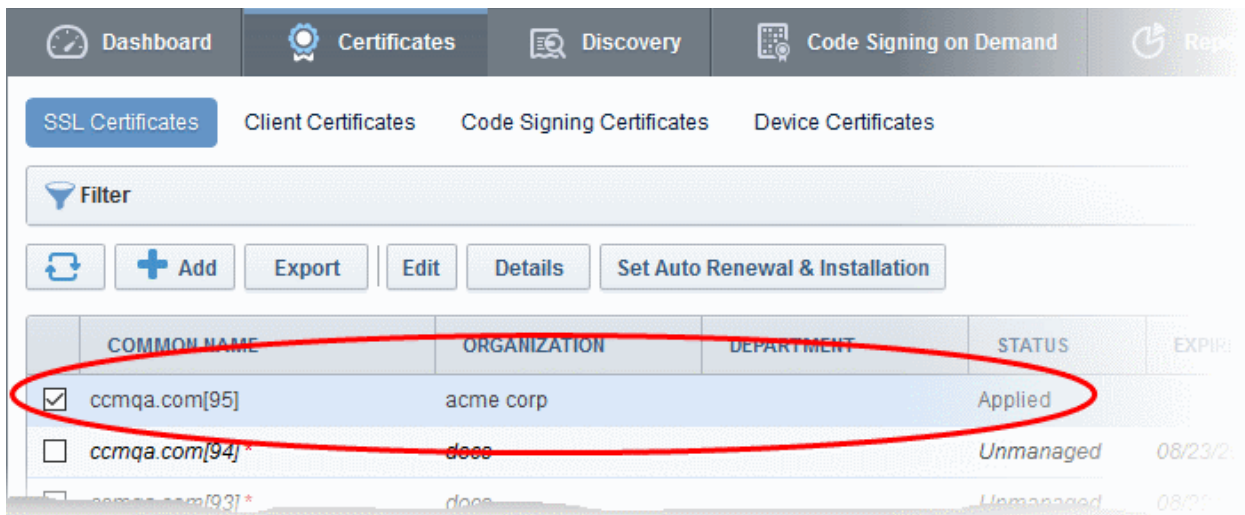


The screenshot shows the 'Certificates' section of the InCommon Certificate Manager. The 'Approve' button is circled in red. An 'Approval Message' dialog box is open, containing a text area with the message: 'The ssl certificate request is approved'. The dialog has 'OK' and 'Cancel' buttons.

	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES
<input checked="" type="checkbox"/>	ccmqa.com[95]	acme corp		Requested	
<input type="checkbox"/>	ccmqa.com[94] *	docs		Unmanaged	08/23/20

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

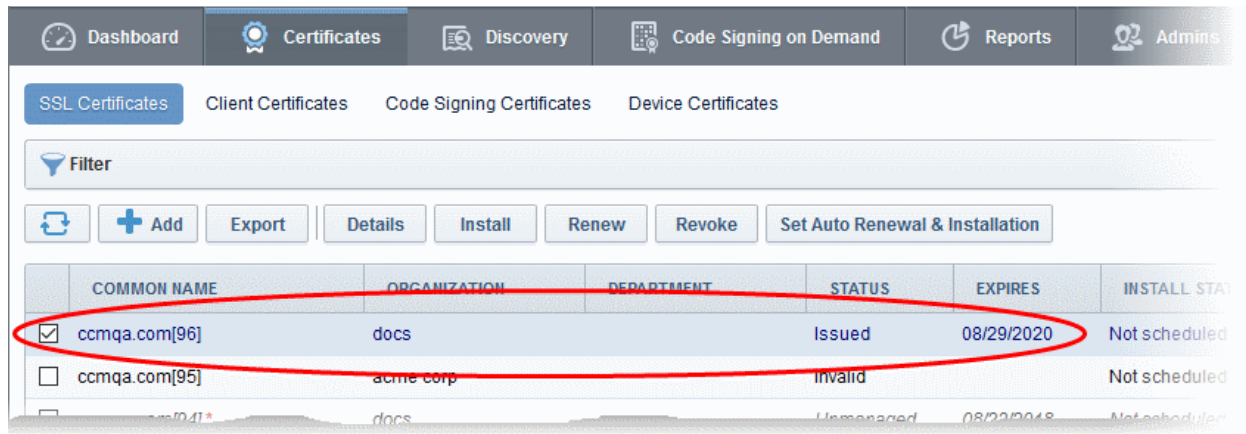
On approval, the CSR will be submitted to InCommon CA to apply for the certificate. The certificate status will change to 'Applied'.



The screenshot shows the same 'Certificates' section. The 'Approve' button is no longer visible. The first row in the table now has a status of 'Applied'.

	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES
<input checked="" type="checkbox"/>	ccmqa.com[95]	acme corp		Applied	
<input type="checkbox"/>	ccmqa.com[94] *	docs		Unmanaged	08/23/20
<input type="checkbox"/>	ccmqa.com[93] *	docs		Unmanaged	08/23/20

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

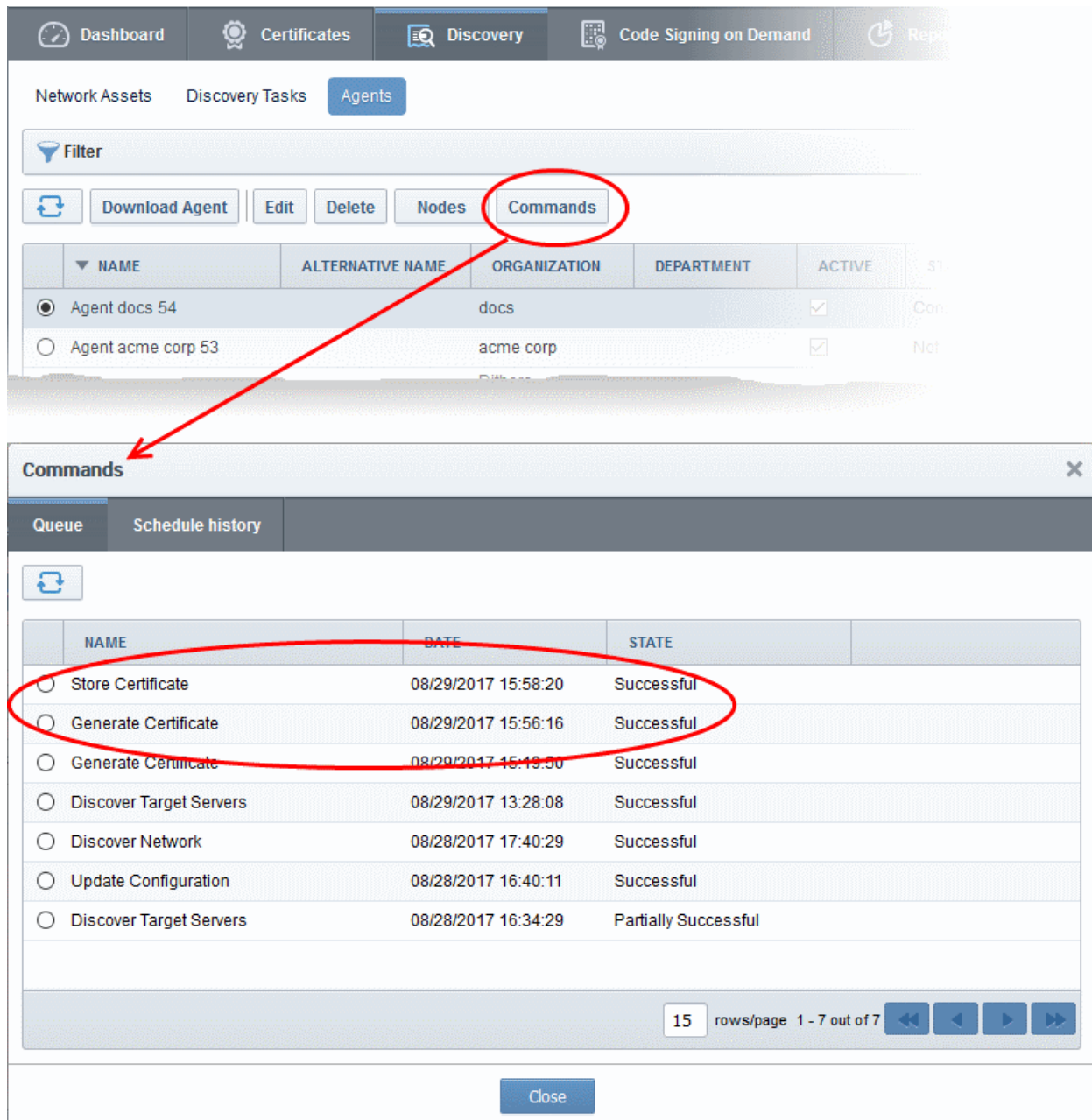


	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STA
<input checked="" type="checkbox"/>	ccmqa.com[96]	docs		Issued	08/29/2020	Not scheduled
<input type="checkbox"/>	ccmqa.com[95]	acme corp		Invalid		Not scheduled
<input type="checkbox"/>	ccmqa.com[94]	docs		Unmanaged	08/29/2018	Not scheduled

To check whether the Certificate Controller has stored the certificate

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

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



The screenshot shows the InCommon Certificate Manager interface. At the top, there are navigation tabs: Dashboard, Certificates, Discovery, Code Signing on Demand, and Reports. Below these, there are sub-tabs: Network Assets, Discovery Tasks, and Agents. A 'Filter' dropdown is visible. Below the filter, there are buttons for 'Download Agent', 'Edit', 'Delete', 'Nodes', and 'Commands'. The 'Commands' button is circled in red. Below these buttons is a table with columns: NAME, ALTERNATIVE NAME, ORGANIZATION, DEPARTMENT, ACTIVE, and STATE. Two rows are visible: 'Agent docs 54' and 'Agent acme corp 53'. A red arrow points from the 'Commands' button to a 'Commands' window that is open below. This window has tabs for 'Queue' and 'Schedule history'. The 'Queue' tab is active, showing a table with columns: NAME, DATE, and STATE. Two rows are circled in red: 'Store Certificate' and 'Generate Certificate'. At the bottom of the 'Commands' window, there is a 'Close' button.

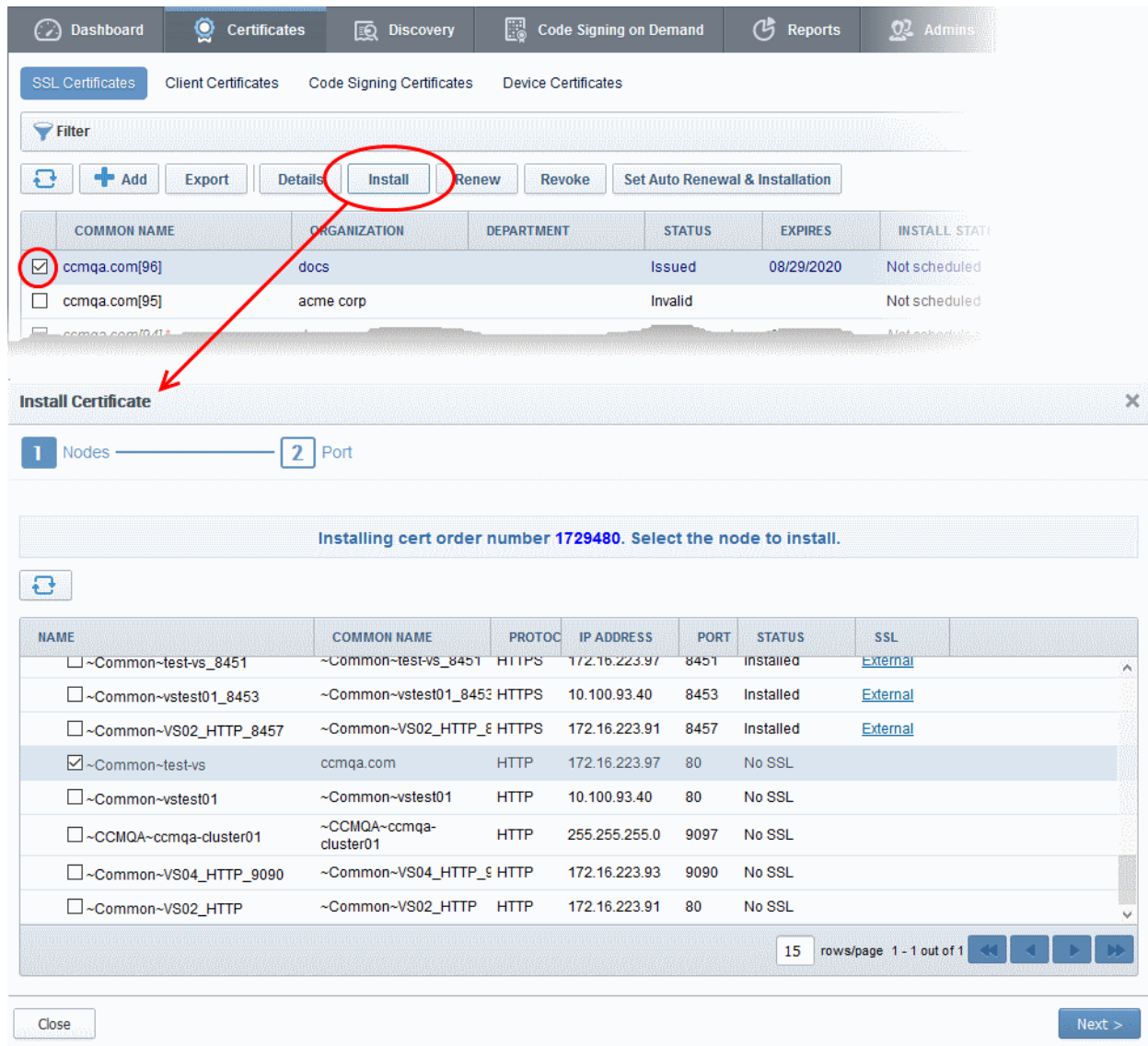
NAME	ALTERNATIVE NAME	ORGANIZATION	DEPARTMENT	ACTIVE	STATE
Agent docs 54		docs		<input checked="" type="checkbox"/>	Con...
Agent acme corp 53		acme corp		<input checked="" type="checkbox"/>	Net...

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

The certificate is stored on the server by the agent. If you have set a schedule for automatic installation in the Schedule step while applying for the certificate, it will be installed automatically at the scheduled time. If you have selected 'Manual' in the Schedule step, 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'



The screenshot shows the 'Install Certificate' wizard in the InCommon Certificate Manager. The main interface has a navigation bar with 'Certificates' selected. Below it, there are tabs for 'SSL Certificates', 'Client Certificates', 'Code Signing Certificates', and 'Device Certificates'. A 'Filter' box is present, and a row of action buttons includes 'Add', 'Export', 'Details', 'Install' (circled in red), 'Renew', 'Revoke', and 'Set Auto Renewal & Installation'. Below the buttons is a table of certificates:

COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE
<input checked="" type="checkbox"/> ccmqa.com[96]	docs		Issued	08/29/2020	Not scheduled
<input type="checkbox"/> ccmqa.com[95]	acme corp		Invalid		Not scheduled

The 'Install Certificate' dialog box is open, showing a progress indicator with '1 Nodes' and '2 Port'. The main instruction reads: 'Installing cert order number 1729480. Select the node to install.' Below this is a table of nodes:

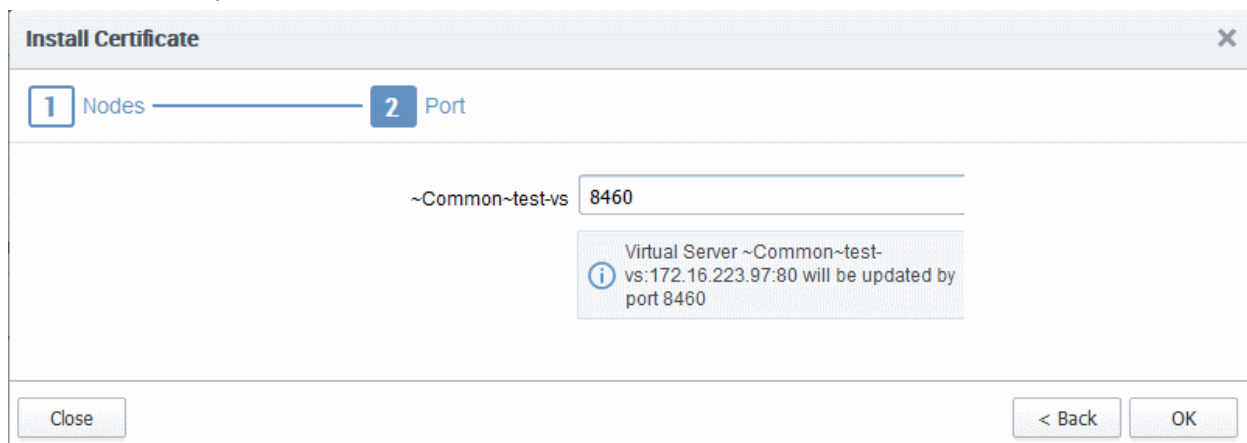
NAME	COMMON NAME	PROTOC	IP ADDRESS	PORT	STATUS	SSL
<input type="checkbox"/> ~Common~test-vs_8451	~Common~test-vs_8451	HTTPS	172.16.223.97	8451	Installed	External
<input type="checkbox"/> ~Common~vstest01_8453	~Common~vstest01_8453	HTTPS	10.100.93.40	8453	Installed	External
<input type="checkbox"/> ~Common~VS02_HTTP_8457	~Common~VS02_HTTP_8	HTTPS	172.16.223.91	8457	Installed	External
<input checked="" type="checkbox"/> ~Common~test-vs	ccmqa.com	HTTP	172.16.223.97	80	No SSL	
<input type="checkbox"/> ~Common~vstest01	~Common~vstest01	HTTP	10.100.93.40	80	No SSL	
<input type="checkbox"/> ~CCMQA~ccmqa-cluster01	~CCMQA~ccmqa-cluster01	HTTP	255.255.255.0	9097	No SSL	
<input type="checkbox"/> ~Common~VS04_HTTP_9090	~Common~VS04_HTTP_8	HTTP	172.16.223.93	9090	No SSL	
<input type="checkbox"/> ~Common~VS02_HTTP	~Common~VS02_HTTP	HTTP	172.16.223.91	80	No SSL	

The dialog also includes a 'Close' button and a 'Next >' button.

The 'Install Certificate' wizard will start with the 'Nodes' interface. The node upon which the certificate is to be installed is pre-selected.

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

The 'Ports' interface will open.



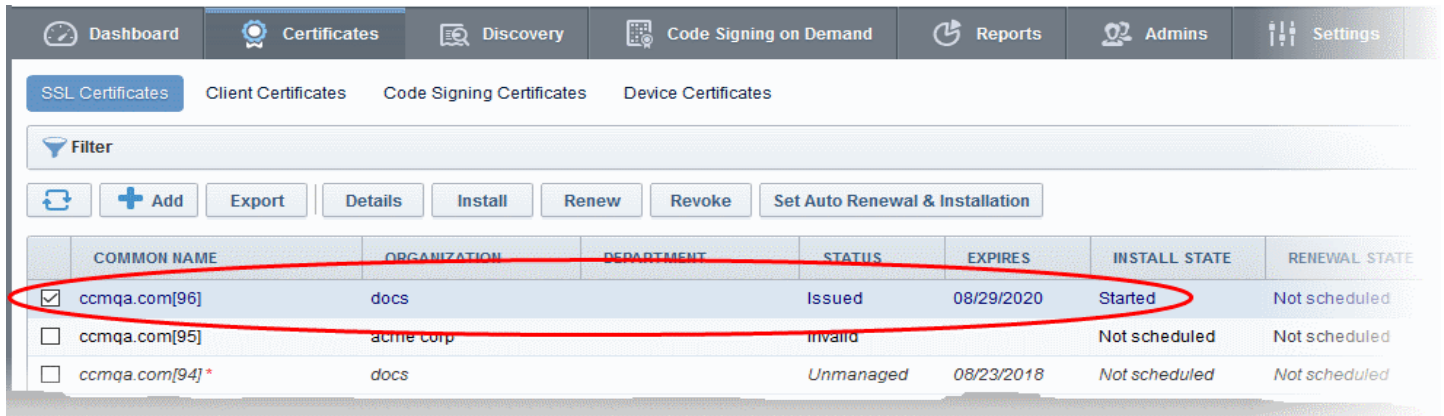
The 'Install Certificate' dialog box is shown at the 'Port' step. The progress indicator shows '1 Nodes' and '2 Port'. The selected node is '~Common~test-vs' and the port is '8460'. A tooltip provides additional information:

Virtual Server ~Common~test-vs:172.16.223.97:80 will be updated by port 8460

The dialog includes 'Close', '< Back', and 'OK' buttons.

- Specify the port and click 'OK'.

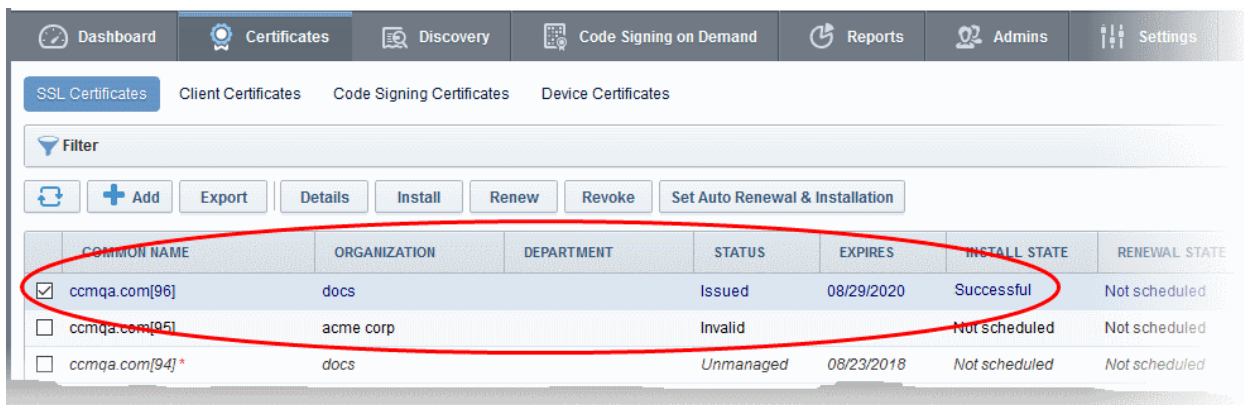
The certificate installation will begin instantly. Once the installation commences, the 'Install State' of the certificate will change to 'Started'.



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
<input checked="" type="checkbox"/>	ccmqa.com[96]	docs		Issued	08/29/2020	Started	Not scheduled
<input type="checkbox"/>	ccmqa.com[95]	acme corp		Invalid		Not scheduled	Not scheduled
<input type="checkbox"/>	ccmqa.com[94]*	docs		Unmanaged	08/23/2018	Not scheduled	Not scheduled

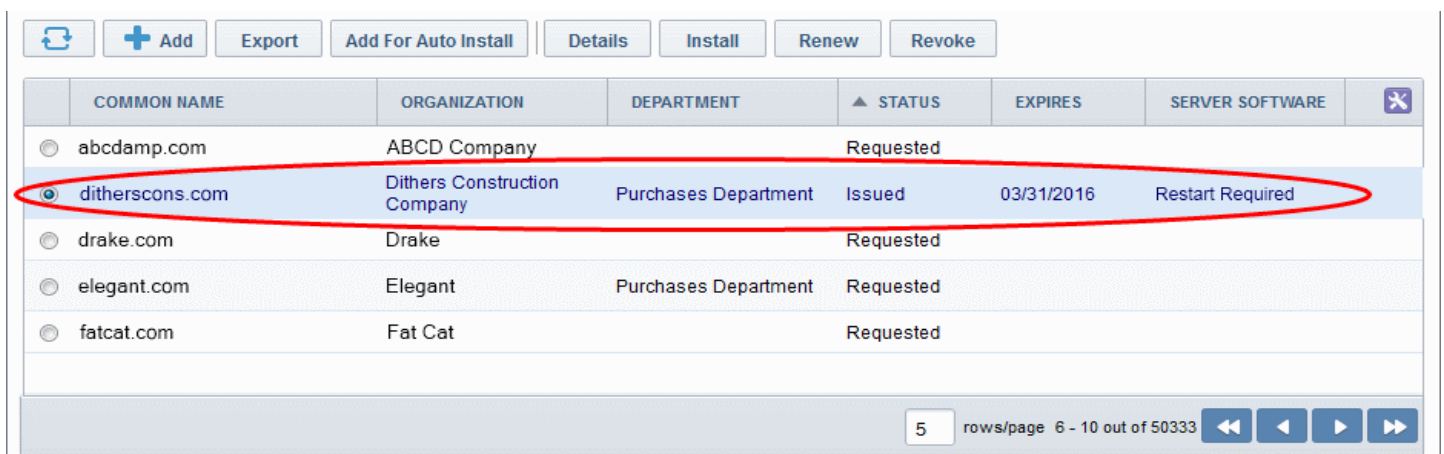
When installation is complete:

- **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
<input checked="" type="checkbox"/>	ccmqa.com[96]	docs		Issued	08/29/2020	Successful	Not scheduled
<input type="checkbox"/>	ccmqa.com[95]	acme corp		Invalid		Not scheduled	Not scheduled
<input type="checkbox"/>	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	SERVER SOFTWARE
<input type="radio"/>	abcdamp.com	ABCD Company		Requested		
<input checked="" type="radio"/>	ditherscons.com	Dithers Construction Company	Purchases Department	Issued	03/31/2016	Restart Required
<input type="radio"/>	drake.com	Drake		Requested		
<input type="radio"/>	elegant.com	Elegant	Purchases Department	Requested		
<input type="radio"/>	fatcat.com	Fat Cat		Requested		

Administrators can restart the server remotely from the InCommon CM interface by clicking the 'Details' button then 'Restart':

- Select the certificate and click the 'Details' button at the top. The 'Certificate Details' dialog will be displayed.
- Click 'Restart' beside the Server Software State field in the 'Details' dialog

Enrollment Certificate ID 77875

Type **Instant SSL**

Server Software **Apache/ModSSL** View Edit

Server Software State **Restart Required** Restart

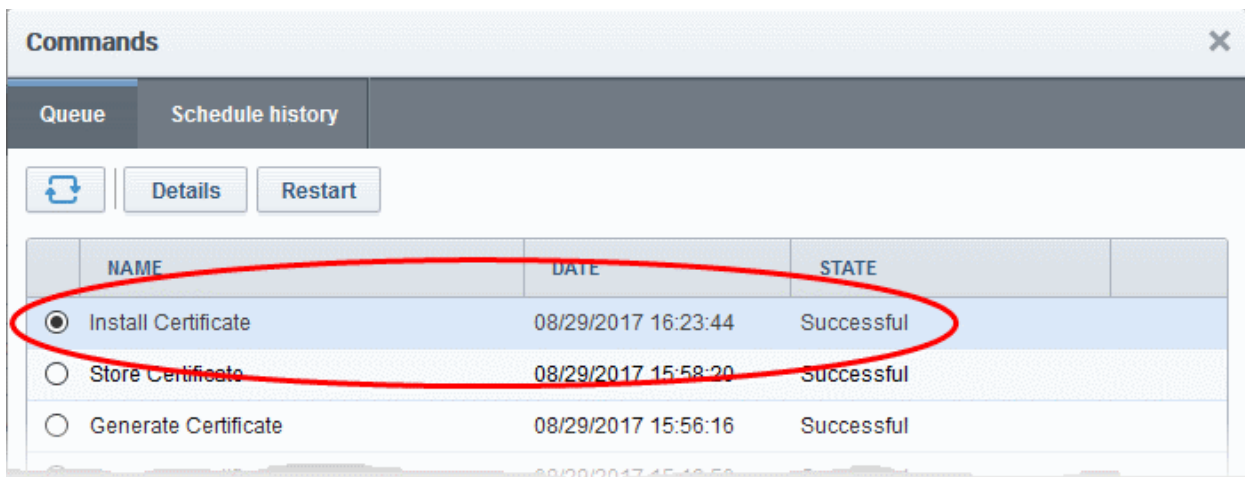
Term **1 year**

Owner admin 1 Resend Edit

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

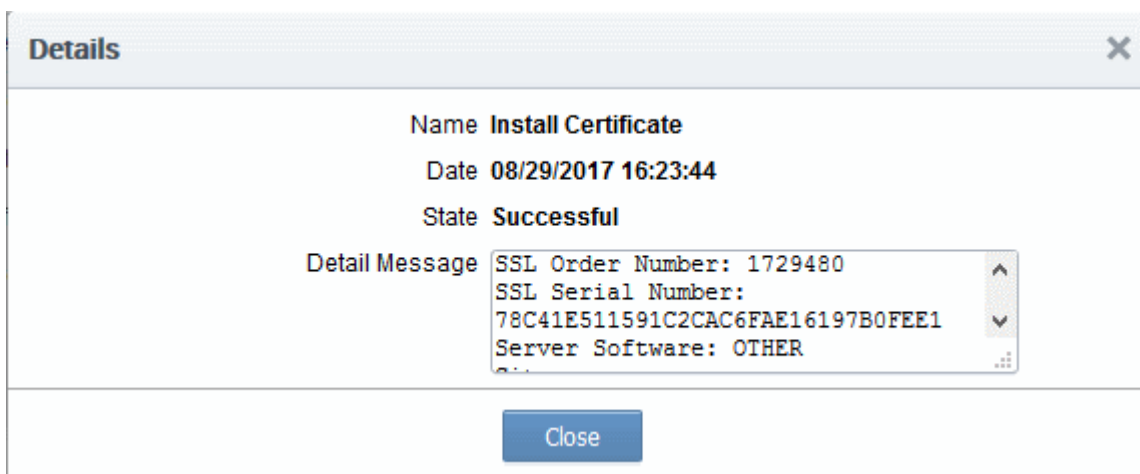
- To check whether the controller has installed the certificate, click Discovery > Agents
- Select the controller and click the 'Commands' button

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



	NAME	DATE	STATE
<input checked="" type="radio"/>	Install Certificate	08/29/2017 16:23:44	Successful
<input type="radio"/>	Store Certificate	08/29/2017 15:58:20	Successful
<input type="radio"/>	Generate Certificate	08/29/2017 15:56:16	Successful

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



Name Install Certificate

Date 08/29/2017 16:23:44

State Successful

Detail Message SSL Order Number: 1729480
 SSL Serial Number:
 78C41E511591C2CAC6FAE16197B0FEE1
 Server Software: OTHER

Close

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. 'CM Controller Mode' requires an agent to be installed on each web server upon which the certificates are to be auto-installed/renewed.

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.



Request New SSL Certificate

*-required fields

Organization*

Department*

[Click here to edit address details](#)

Certificate Type*

Certificate Term*

Server Software*

CSR

Provide CSR Autogenerate CSR and Manage Private Key

CSR*

Max CSR size is 32K

Certificate Parameters

Common Name*

Requester

External Requester

Comments

Renewal & Installation

Auto renew days before expiration

Create new key pair

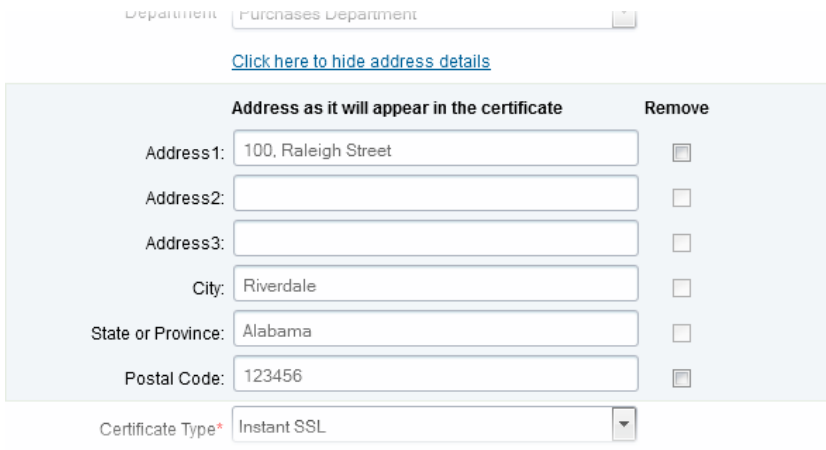
Auto install renewed certificate

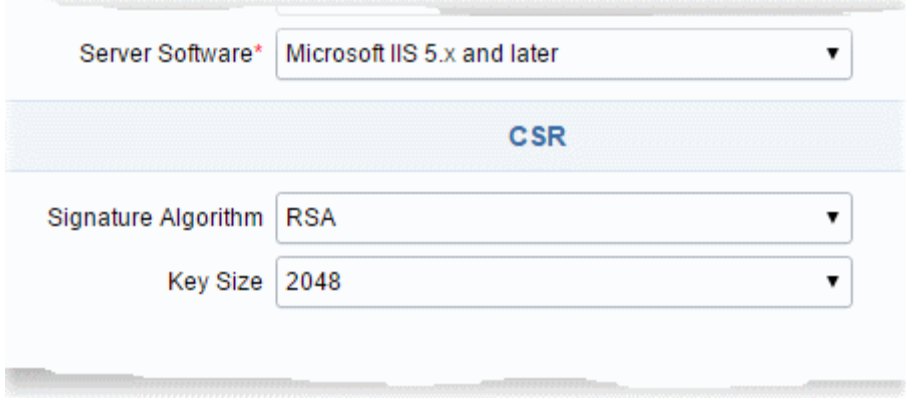
Auto install initial certificate

Subscriber Agreement

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



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'.
Click here to edit address details	Text Fields	<p>Clicking this link will expand the address fields.</p>  <p>The address fields are auto-populated from the details of the Organization or Department on whose behalf this certificate request is being made.</p> <p>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.</p> <p>The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted".</p> <p>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.</p>
Certificate Type (required)	Drop-down list	<p>Choose the certificate type that you wish to add for auto-installation.</p> <p>Note: Currently InCommon CM supports auto-installation only for the 'Instant SSL' certificate type. Other certificate types will be enabled for auto-installation in future versions.</p>
Certificate Term (required)	Drop-down list	Choose the validity period of the certificate. For example, 1 year, 2 years, 3 years.

Form Element	Type	Description
Server Software (required)	Drop-down list	Select the server software on which the certificate is to be installed. Auto-installation is supported only on the following server types: <ul style="list-style-type: none"> • Apache/Mod SSL • Apache - SSL • Apache Tomcat • Microsoft IIS 1.x to 4.x • Microsoft IIS 5.x and above
CSR		
Provide CSR/Autogenerate CSR and Manage Private Key		Leave these fields blank. After a successful application, the certificate controller will co-ordinate with the web server to create the CSR and submit it to InCommon CA.
CSR (required)		Once you choose 'Auto install initial certificate' under ' Renewal & Installation ' in this form, these fields will disappear.
Get CN from CSR (optional)		You can choose the signature algorithm to be used by the public key of the certificate and the key size for the certificate under 'CSR'.
Upload CSR (optional)		
Certificate Parameters		
Common Name (required)	Text Field	Type the domain that the certificate will be issued to.
Requester (auto-populated)	Text Field	The 'Requester' is 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.

Form Element	Type	Description
		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 (<i>optional</i>)	Text Field	Enter your comments on the certificate. This is optional.
Renewal and Installation		
Auto Renew	Checkbox and text field	Enable to auto-renew the certificate when it is nearing expiry. You can also 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.
Create new key pair	Checkbox	Select this option if you want a new key pair is to be generated for the renewal certificate. Leaving it unselected means InCommon CM will re-use the existing key pair of the expiring certificate.
Auto install renewed certificate	Checkbox	Select this option if you want the renewed certificate be auto-installed.
Auto install initial certificate	Checkbox	Select this option to mark this certificate for auto-installation. After completing the form, the auto-installation wizard will allow you to select the nodes on which the certificate should be installed and to create an installation schedule.
Subscriber Agreement (<i>required</i>)	Control	You must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox.

- Click 'OK' to submit the application

The 'Set Auto Renewal & Installation' dialog will be displayed with the 'Nodes' interface open. The 'Nodes' interface displays a list of agents installed on your servers for different Organizations and Departments. A list of server nodes is shown under each Agent.

✕
Set Auto Renewal & Installation

1 Nodes
2 Schedule
3 Port
4 EULA

✕
Server IIS org1 50
Active

NAME	COMMON NAME	PROTOCOL	IP ADDRESS	PORT	STATUS	SSL
<input type="radio"/> test.ccmqa.com	fortest.ccmqa.com	HTTPS	*	8444	Failed	1675873
<input type="radio"/> self.ccmqa.local	self.ccmqa.local	HTTP	*	8443	No SSL	
<input checked="" type="radio"/> ms1.ccmqa.com	ms1.ccmqa.com	HTTP	*	443	No SSL	
<input type="radio"/> Default Web Site	Default Web Site	HTTP	*	80	No SSL	

15 rows/page 1 - 1 out of 1

⏪
⏩

Close
Next >

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

The 'Schedule' interface will open, allowing you to install the certificate manually from the InCommon CM interface or to set a schedule for auto-installation.

✕
Set Auto Renewal & Installation

1 Nodes
2 Schedule
3 Port
4 EULA

Manual
 Certificate installation must be started manually.

Schedule
 Certificate installation will be started during selected time period.

Time zone: UTC+00:00 - GMT, UCT, UTC, WET, EGST

Start not earlier than: 01/18/2017

Time Of Day

Run Between: 00 : 19 00 : 19

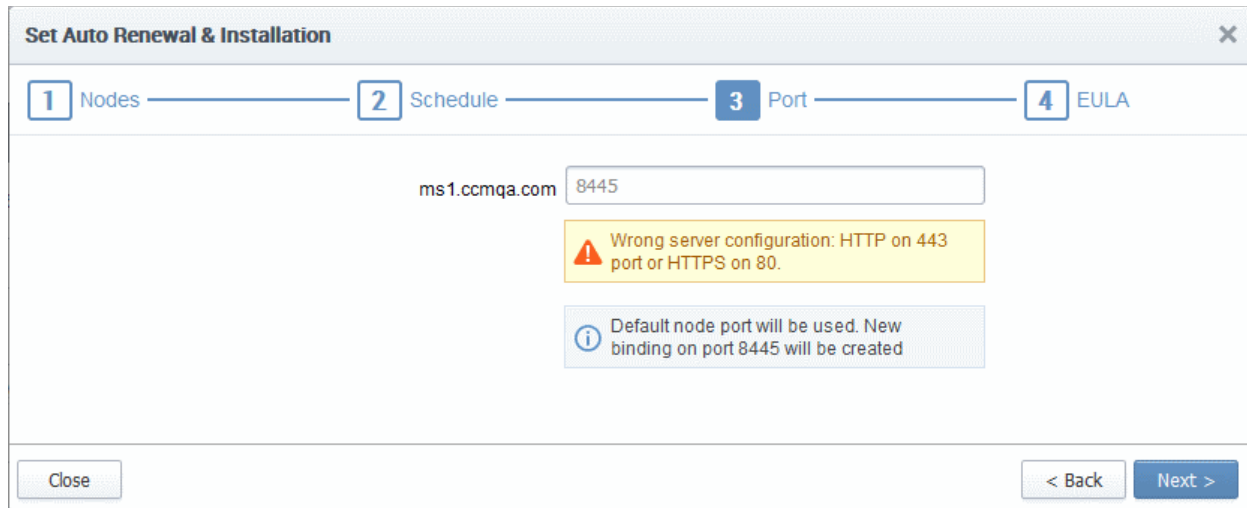
Day of Week

Run Only: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Close
< Back
Next >

- If you want to manually install the certificate from the InCommon CM interface, select 'Manual'
- If you want to install the certificate at a scheduled time, select 'Schedule' then select your time zone and a 'not earlier than' time. The controller will generate a CSR and submit it to InCommon CA the first time it polls InCommon CM after the 'not earlier than' time. Use the check-boxes at the bottom to limit which days of the week that the installation should run.
- Click 'Next'.

The 'Port' interface will open.



Set Auto Renewal & Installation

1 Nodes — 2 Schedule — **3 Port** — 4 EULA

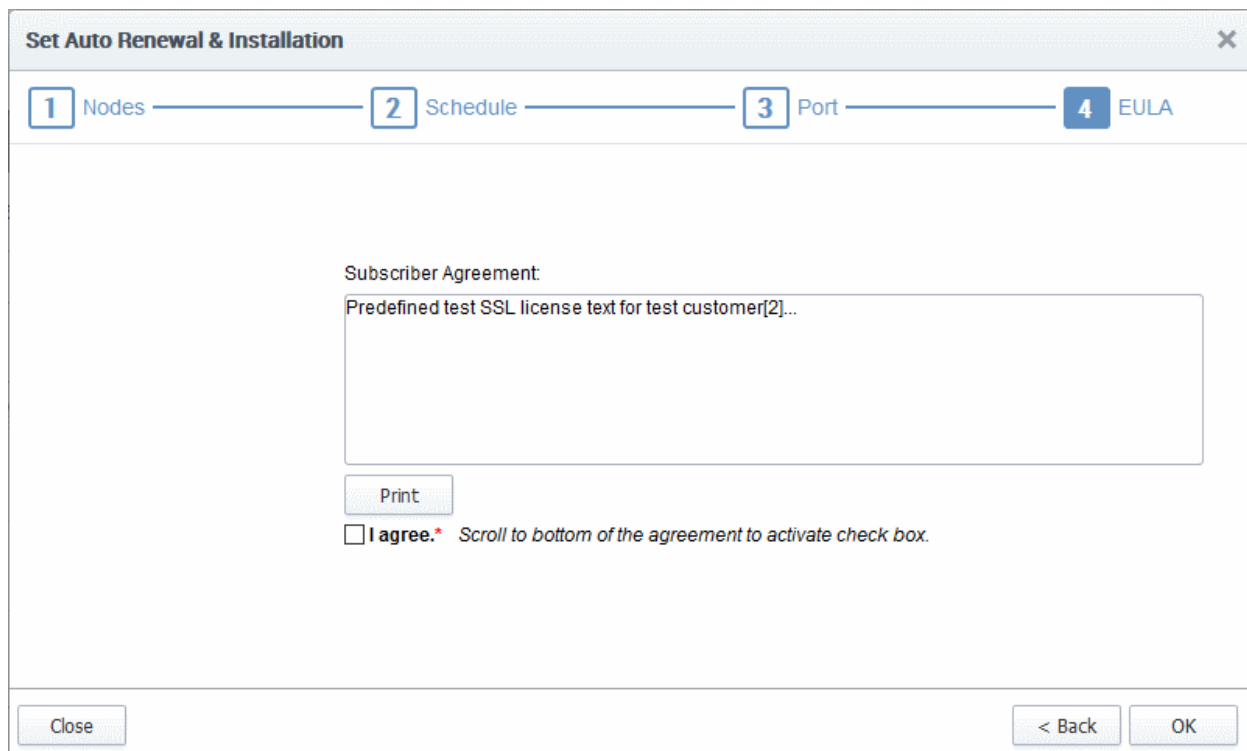
ms1.ccmqa.com

Warning: Wrong server configuration: HTTP on 443 port or HTTPS on 80.

Info: Default node port will be used. New binding on port 8445 will be created

Close < Back Next >

- Specify the HTTPS port for installing the certificate, (**Default = 9443**)
- Click 'Next'. The EULA interface will open.



Set Auto Renewal & Installation

1 Nodes — 2 Schedule — 3 Port — **4 EULA**

Subscriber Agreement:

Predefined test SSL license text for test customer[2]...

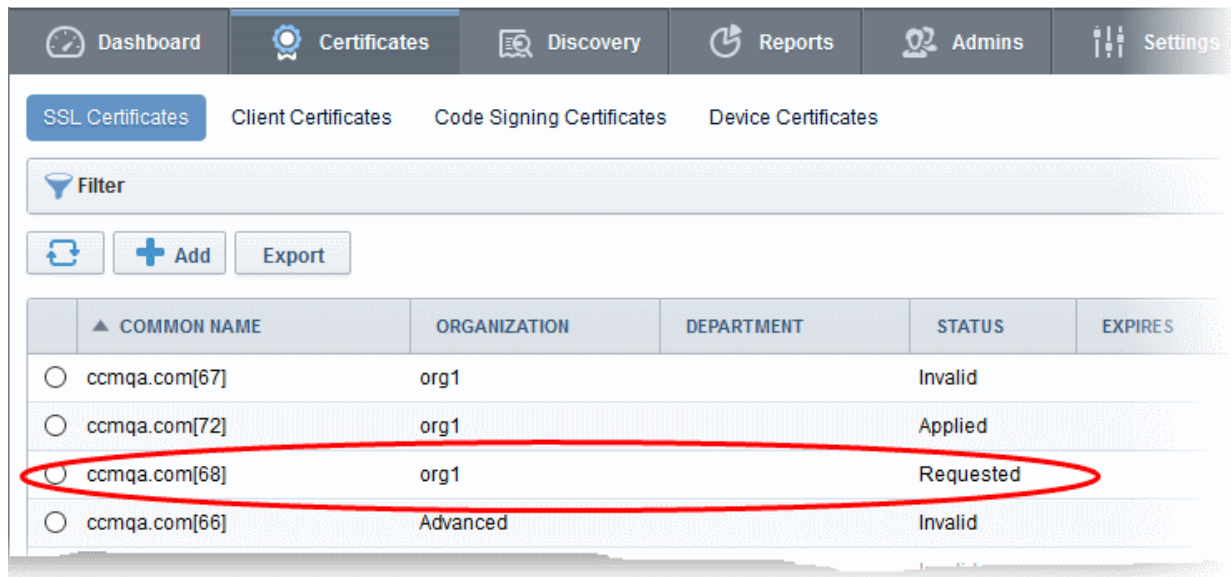
Print

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

Close < Back OK

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

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



Dashboard Certificates Discovery Reports Admins Settings

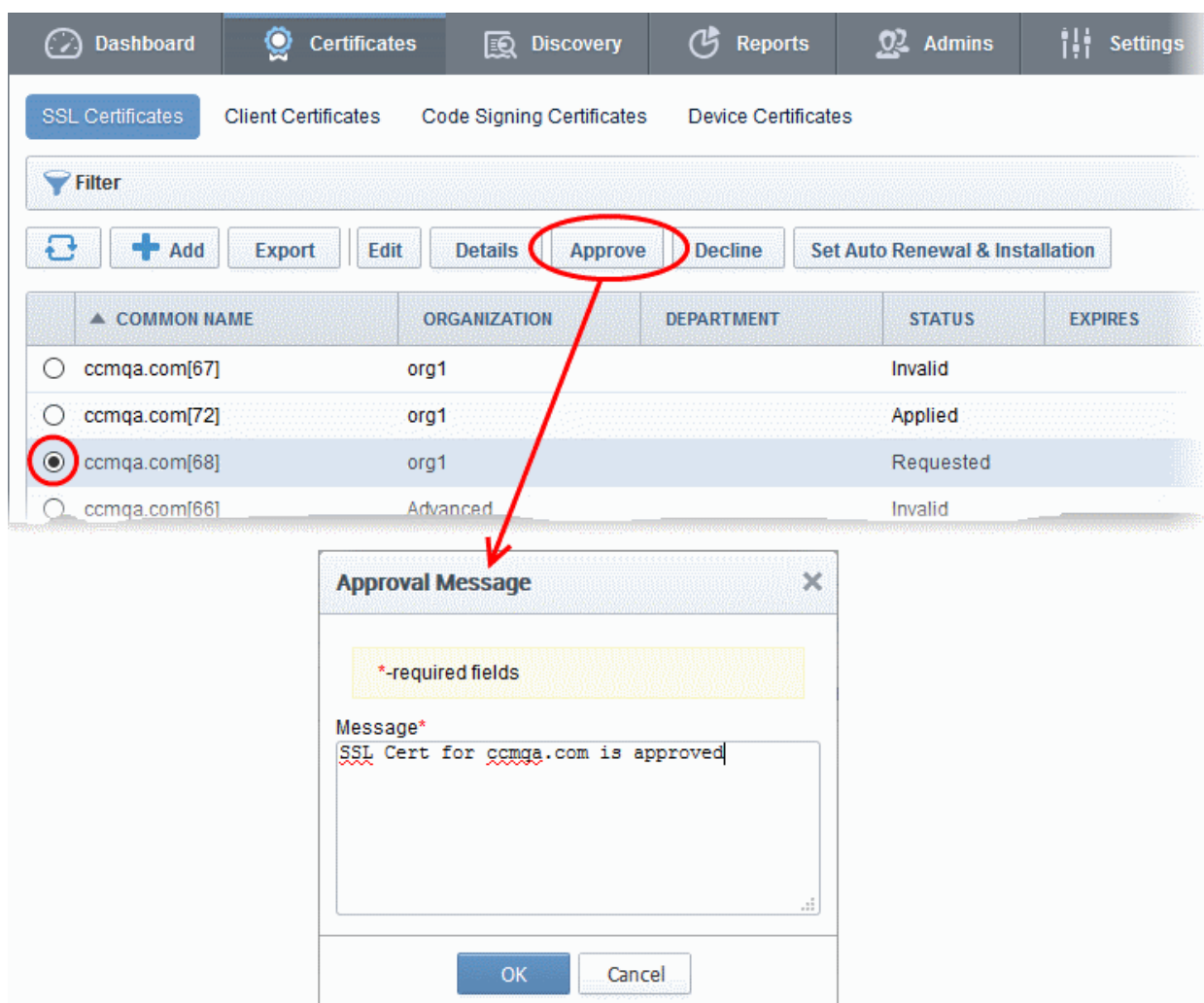
SSL Certificates Client Certificates Code Signing Certificates Device Certificates

Filter

Refresh Add Export

	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES
<input type="radio"/>	ccmqa.com[67]	org1		Invalid	
<input type="radio"/>	ccmqa.com[72]	org1		Applied	
<input checked="" type="radio"/>	ccmqa.com[68]	org1		Requested	
<input type="radio"/>	ccmqa.com[66]	Advanced		Invalid	

- The CSR for the requested certificate will be generated automatically. After the CSR is created, the approve button will appear at the top when you select the certificate in the list.



Dashboard Certificates Discovery Reports Admins Settings

SSL Certificates Client Certificates Code Signing Certificates Device Certificates

Filter

Refresh Add Export Edit Details Approve Decline Set Auto Renewal & Installation

	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES
<input type="radio"/>	ccmqa.com[67]	org1		Invalid	
<input type="radio"/>	ccmqa.com[72]	org1		Applied	
<input checked="" type="radio"/>	ccmqa.com[68]	org1		Requested	
<input type="radio"/>	ccmqa.com[66]	Advanced		Invalid	

Approval Message [X]

*-required fields

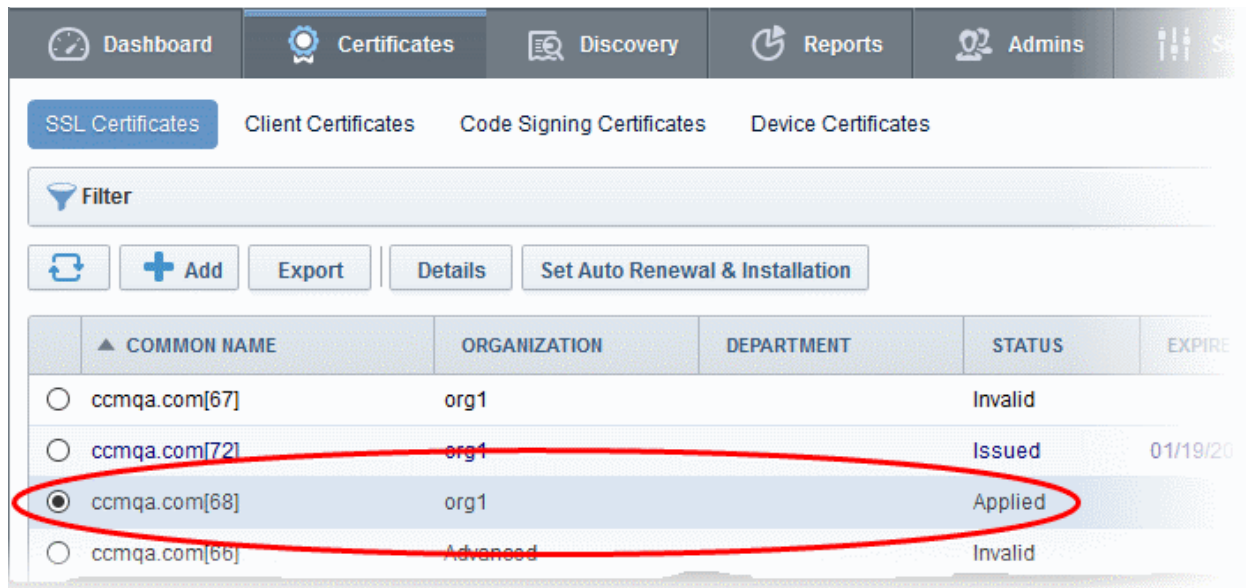
Message*

SSL Cert for ccmqa.com is approved

OK Cancel

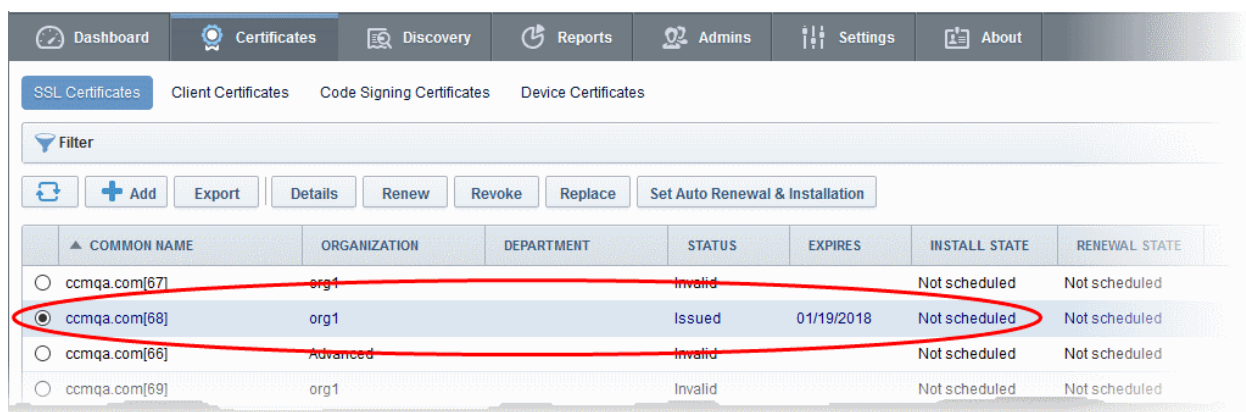
- Click the 'Approve' button to approve the request, enter the approval message in the 'Approval Message' dialog and click 'OK'.

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



	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES
<input type="radio"/>	ccmqa.com[67]	org1		Invalid	
<input type="radio"/>	ccmqa.com[72]	org1		Issued	01/19/2018
<input checked="" type="radio"/>	ccmqa.com[68]	org1		Applied	
<input type="radio"/>	ccmqa.com[66]	Advanced		Invalid	

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

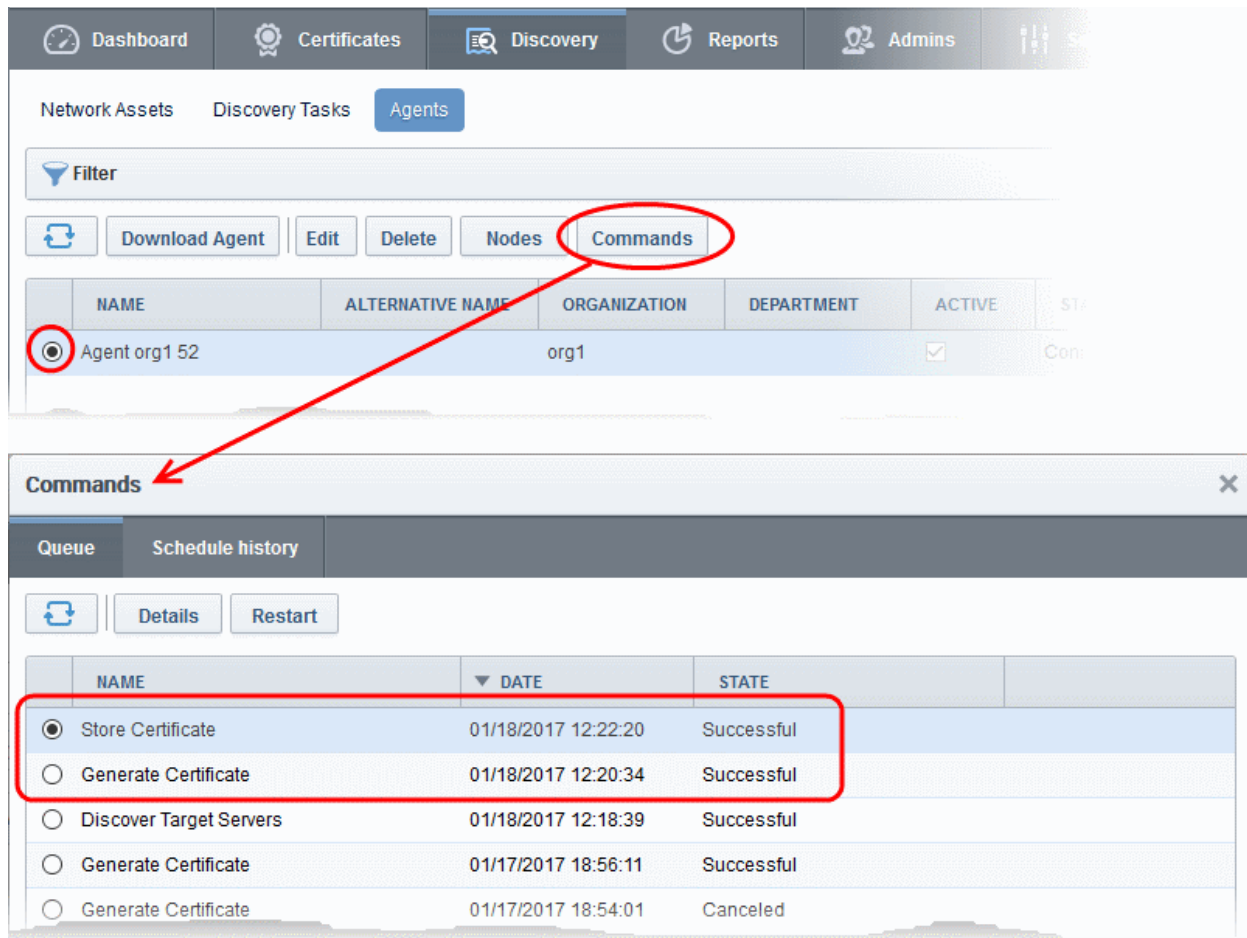


	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
<input type="radio"/>	ccmqa.com[67]	org1		Invalid		Not scheduled	Not scheduled
<input checked="" type="radio"/>	ccmqa.com[68]	org1		Issued	01/19/2018	Not scheduled	Not scheduled
<input type="radio"/>	ccmqa.com[66]	Advanced		Invalid		Not scheduled	Not scheduled
<input type="radio"/>	ccmqa.com[69]	org1		Invalid		Not scheduled	Not scheduled

To check whether the controller has stored the certificate:

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

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



The screenshot shows the 'Agents' section of the InCommon Certificate Manager. A table lists agents, with 'Agent org1 52' selected. A red circle highlights the 'Commands' button in the top navigation bar, and another red circle highlights the selected agent row. A red arrow points from the 'Commands' button to a modal window titled 'Commands'.

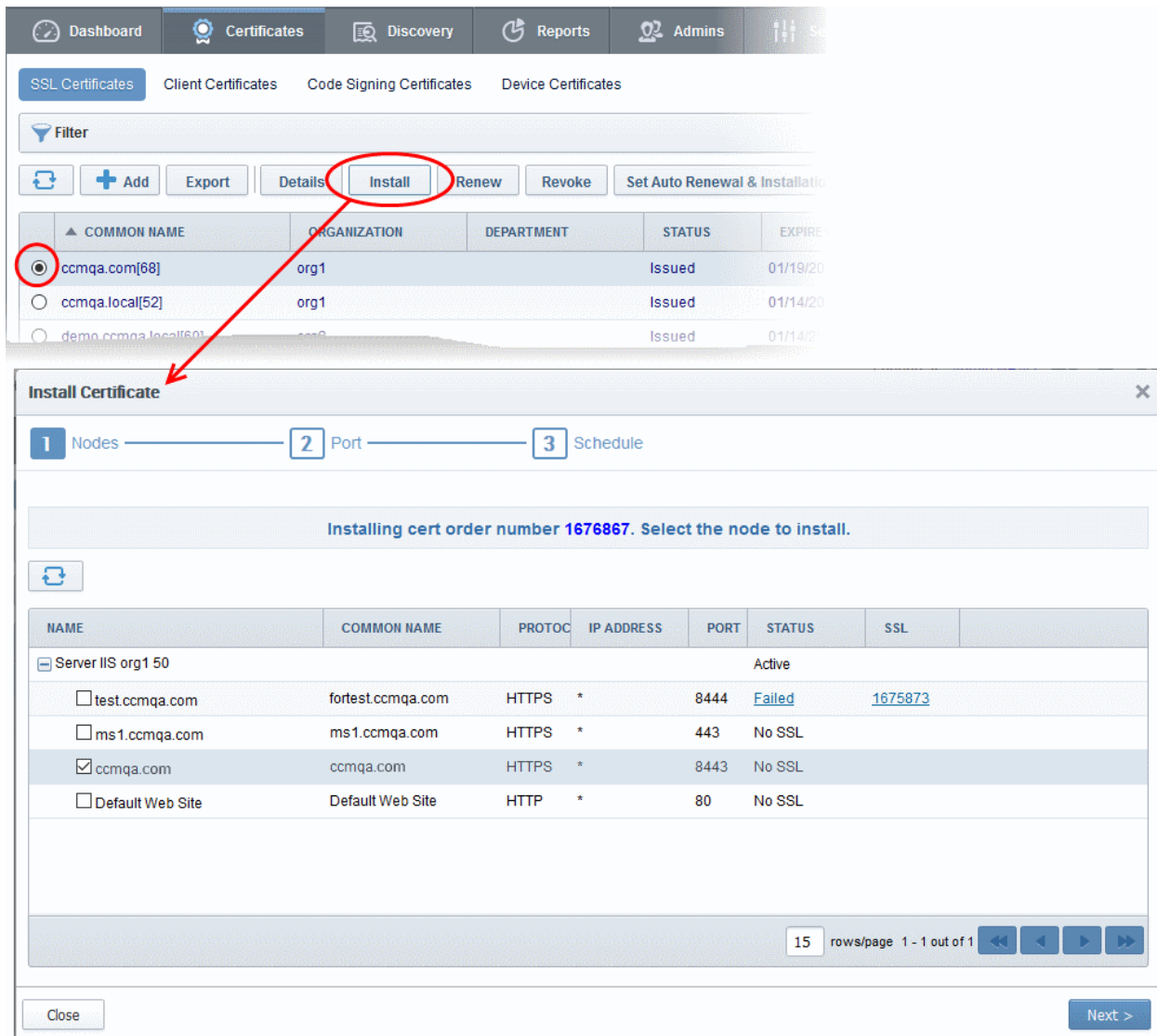
The 'Commands' modal window has tabs for 'Queue' and 'Schedule history'. The 'Queue' tab is active, showing a table of commands:

	NAME	DATE	STATE
<input checked="" type="radio"/>	Store Certificate	01/18/2017 12:22:20	Successful
<input type="radio"/>	Generate Certificate	01/18/2017 12:20:34	Successful
<input type="radio"/>	Discover Target Servers	01/18/2017 12:18:39	Successful
<input type="radio"/>	Generate Certificate	01/17/2017 18:56:11	Successful
<input type="radio"/>	Generate Certificate	01/17/2017 18:54:01	Canceled

The certificate is stored on the server by the agent. If you created a schedule for automatic installation in the Schedule step, it will be installed automatically at the scheduled time. If you selected 'Manual', you can initiate the auto-installation process from the 'Certificates' > 'SSL Certificates' interface:

To manually initiate auto-installation of a certificate

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



The screenshot shows the 'Install Certificate' wizard in the InCommon Certificate Manager. The wizard is currently on the 'Nodes' step (Step 1 of 3). The 'Nodes' table lists the following nodes:

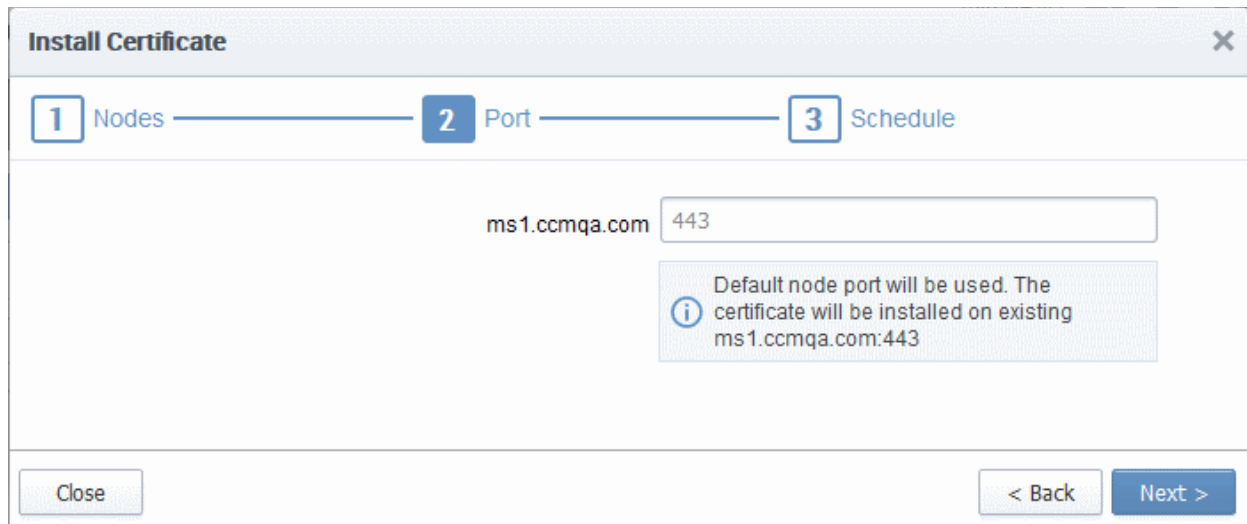
NAME	COMMON NAME	PROTOCOL	IP ADDRESS	PORT	STATUS	SSL
Server IIS org1 50 Active						
<input type="checkbox"/> test.ccmqa.com	fortest.ccmqa.com	HTTPS	*	8444	Failed	1675873
<input type="checkbox"/> ms1.ccmqa.com	ms1.ccmqa.com	HTTPS	*	443	No SSL	
<input checked="" type="checkbox"/> ccmqa.com	ccmqa.com	HTTPS	*	8443	No SSL	
<input type="checkbox"/> Default Web Site	Default Web Site	HTTP	*	80	No SSL	

The 'Nodes' step is pre-selected, and the 'Next >' button is visible at the bottom right of the wizard.

The 'Install Certificate' wizard will start with the 'Nodes' interface. The node upon which the certificate is to be installed is pre-selected.

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

The 'Ports' interface will open.



Install Certificate

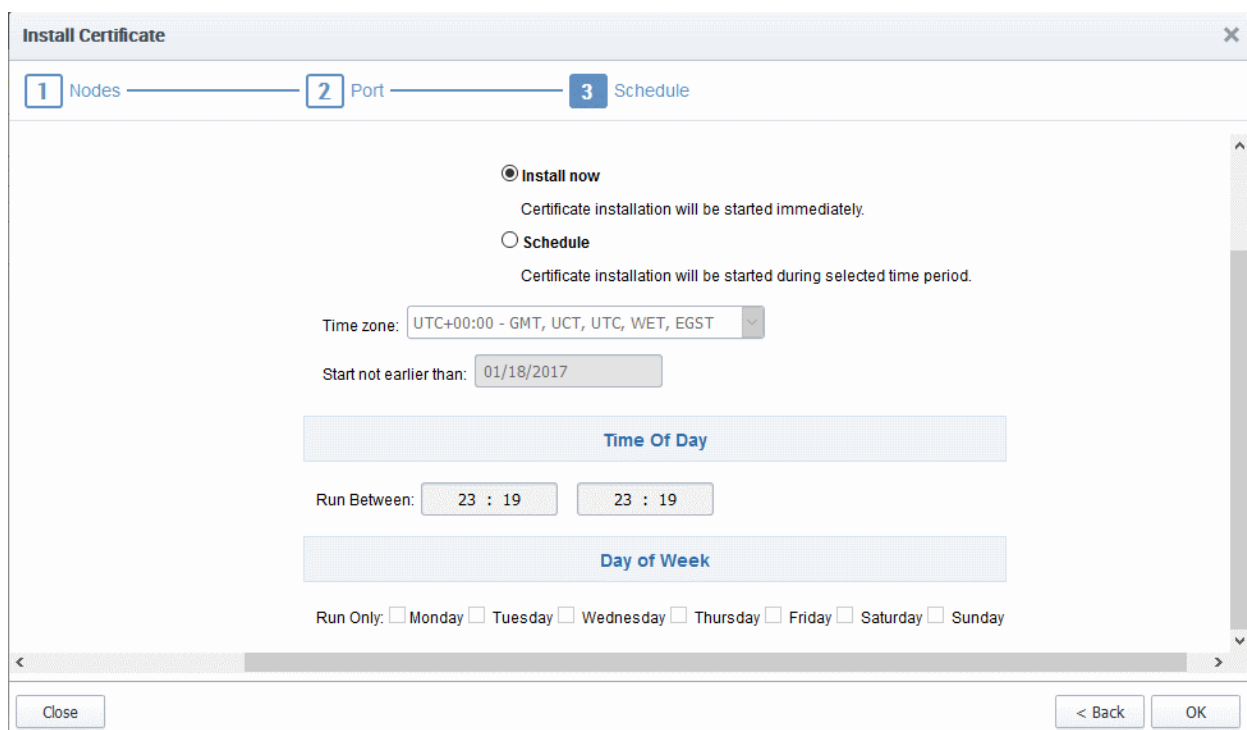
1 Nodes — 2 Port — 3 Schedule

ms1.ccmqa.com 443

Default node port will be used. The certificate will be installed on existing ms1.ccmqa.com:443

Close < Back Next >

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



Install Certificate

1 Nodes — 2 Port — 3 Schedule

Install now
Certificate installation will be started immediately.

Schedule
Certificate installation will be started during selected time period.

Time zone: UTC+00:00 - GMT, UCT, UTC, WET, EGST

Start not earlier than: 01/18/2017

Time Of Day

Run Between: 23 : 19 23 : 19

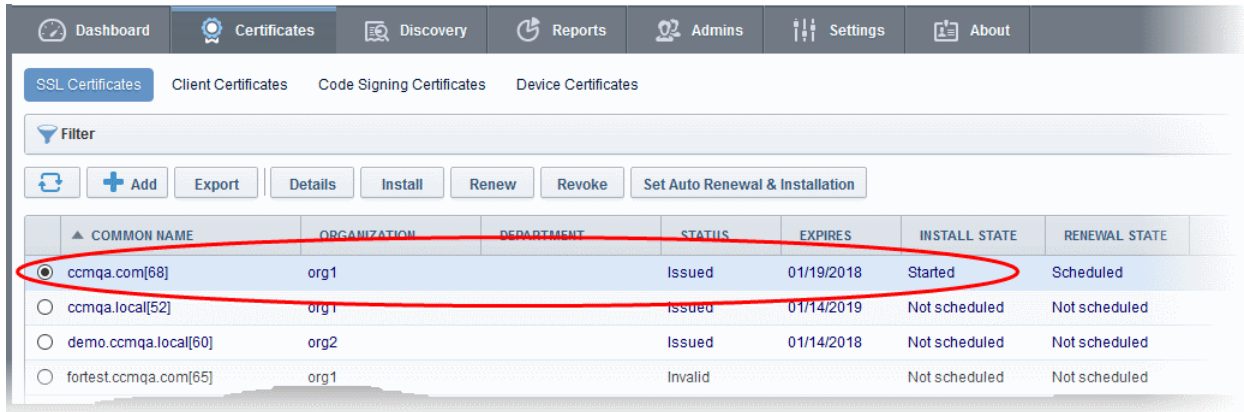
Day of Week

Run Only: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Close < Back OK

- If you want to instantly install the certificate, select 'Install now'
- If you want to install the certificate at a later time, select 'Schedule', then select your time zone, and set a 'not earlier than' date. The certificate will be installed on the server when the controller polls InCommon CM for the first time after the 'Not earlier than' date.
- Click 'OK'

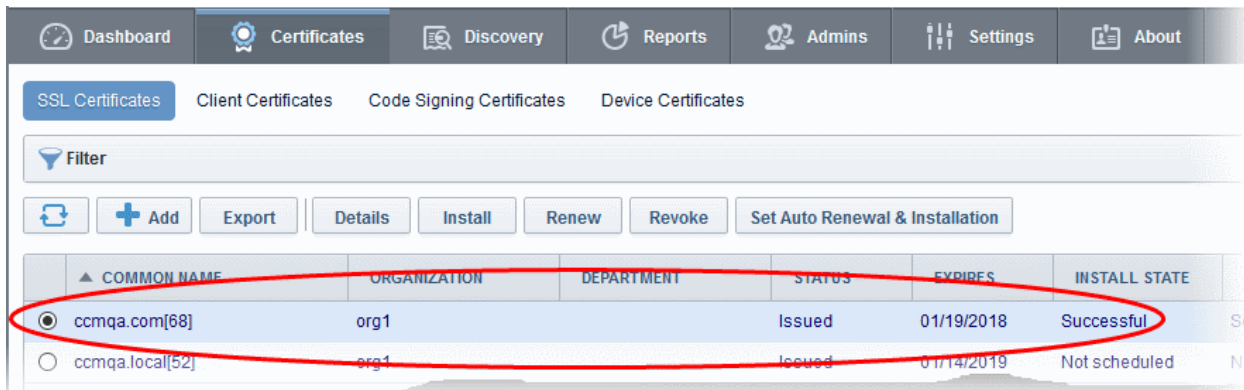
Once installation commences, the 'Install State' of the certificate will change to 'Started':



COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
<input checked="" type="radio"/> ccmqa.com[68]	org1		Issued	01/19/2018	Started	Scheduled
<input type="radio"/> ccmqa.local[52]	org1		Issued	01/14/2019	Not scheduled	Not scheduled
<input type="radio"/> demo.ccmqa.local[60]	org2		Issued	01/14/2018	Not scheduled	Not scheduled
<input type="radio"/> fortest.ccmqa.com[65]	org1		Invalid		Not scheduled	Not scheduled

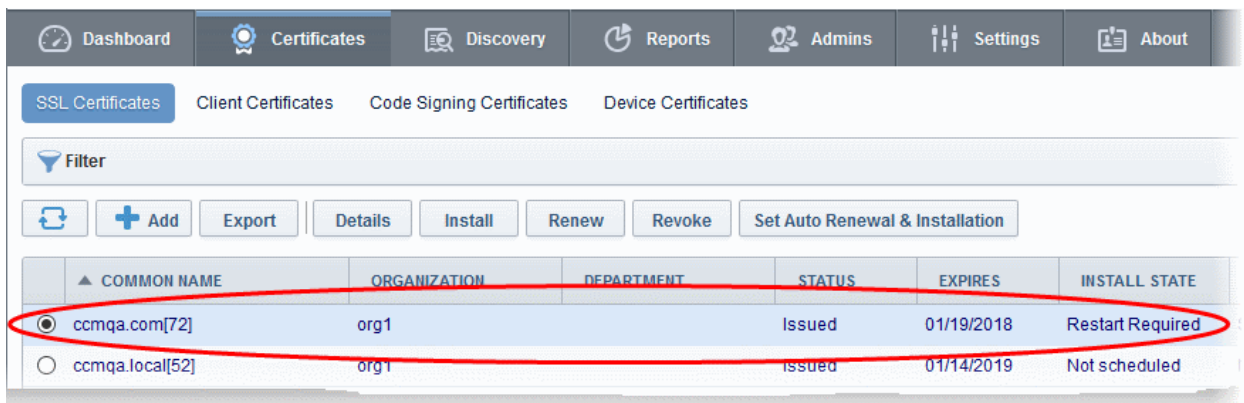
When installation is complete:

- 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
<input checked="" type="radio"/> ccmqa.com[68]	org1		Issued	01/19/2018	Successful
<input type="radio"/> ccmqa.local[52]	org1		Issued	01/14/2019	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
<input checked="" type="radio"/> ccmqa.com[72]	org1		Issued	01/19/2018	Restart Required
<input type="radio"/> ccmqa.local[52]	org1		Issued	01/14/2019	Not scheduled

Administrators can restart the server remotely from the InCommon CM interface by clicking the 'Details' button then 'Restart':

- Select the certificate and click the 'Details' button at the top. The 'Certificate Details' dialog will be displayed.
- Click Restart beside the Server Software State field in the 'Details' dialog

rollment Certificate ID 77875

Type **Instant SSL**

Server Software **Apache/ModSSL**

View

Edit

Server Software State **Restart Required**

Restart

Term **1 year**

Owner **admin 1**

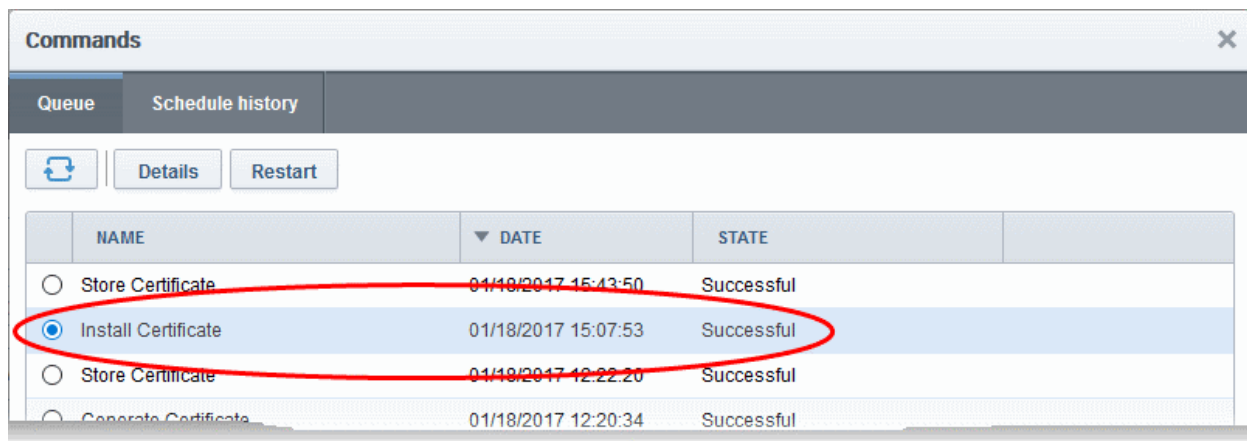
Resend

Edit

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

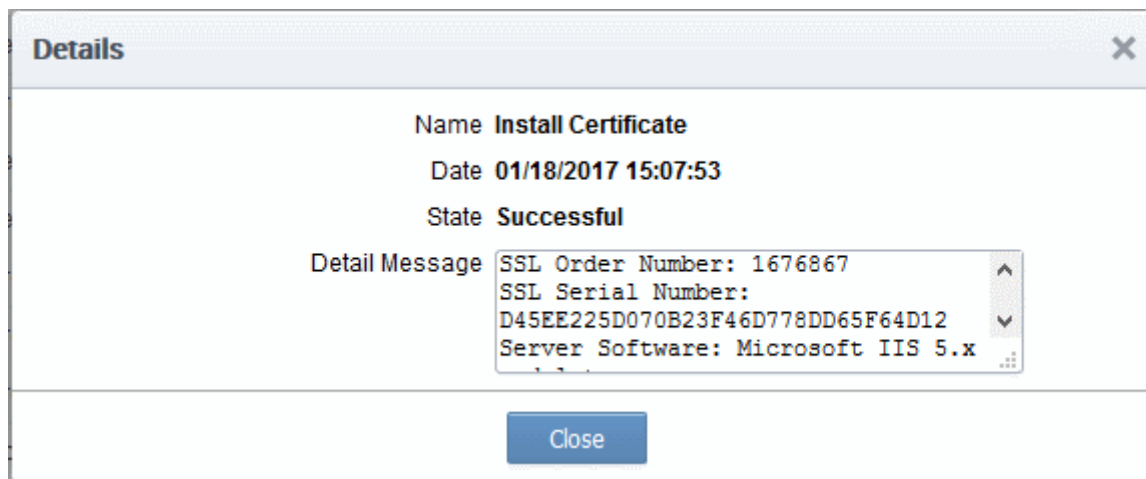
- To check whether the controller has installed the certificate, click Discovery > Agents
- Select the controller and click the 'Commands' button

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



	NAME	DATE	STATE
<input type="radio"/>	Store Certificate	01/18/2017 15:43:50	Successful
<input checked="" type="radio"/>	Install Certificate	01/18/2017 15:07:53	Successful
<input type="radio"/>	Store Certificate	01/18/2017 12:22:20	Successful
<input type="radio"/>	Generate Certificate	01/18/2017 12:20:34	Successful

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



Name Install Certificate

Date 01/18/2017 15:07:53

State Successful

Detail Message

```
SSL Order Number: 1676867
SSL Serial Number:
D45EE225D070B23F46D778DD65F64D12
Server Software: Microsoft IIS 5.x
```

Close

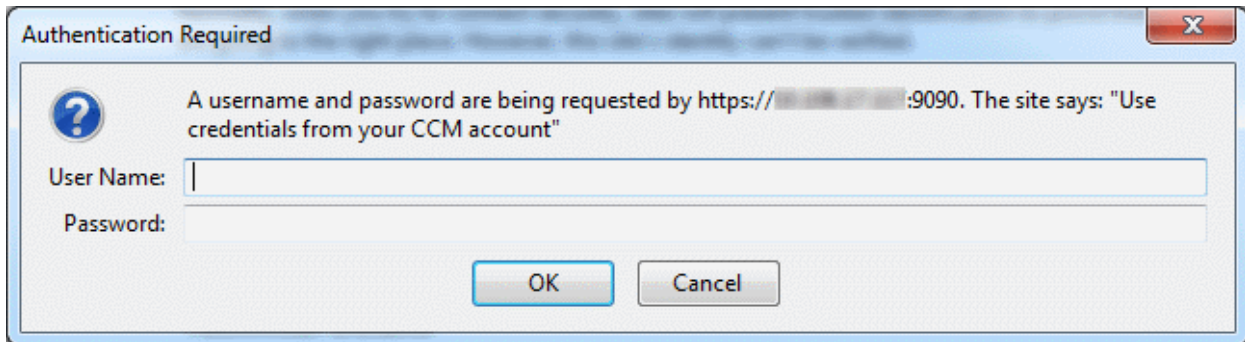
Configuring the Certificate Controller Agent through Web Interface

The Certificate Controller Agent can be configured by logging-in to its web-interface.

To access the Agent configuration web interface

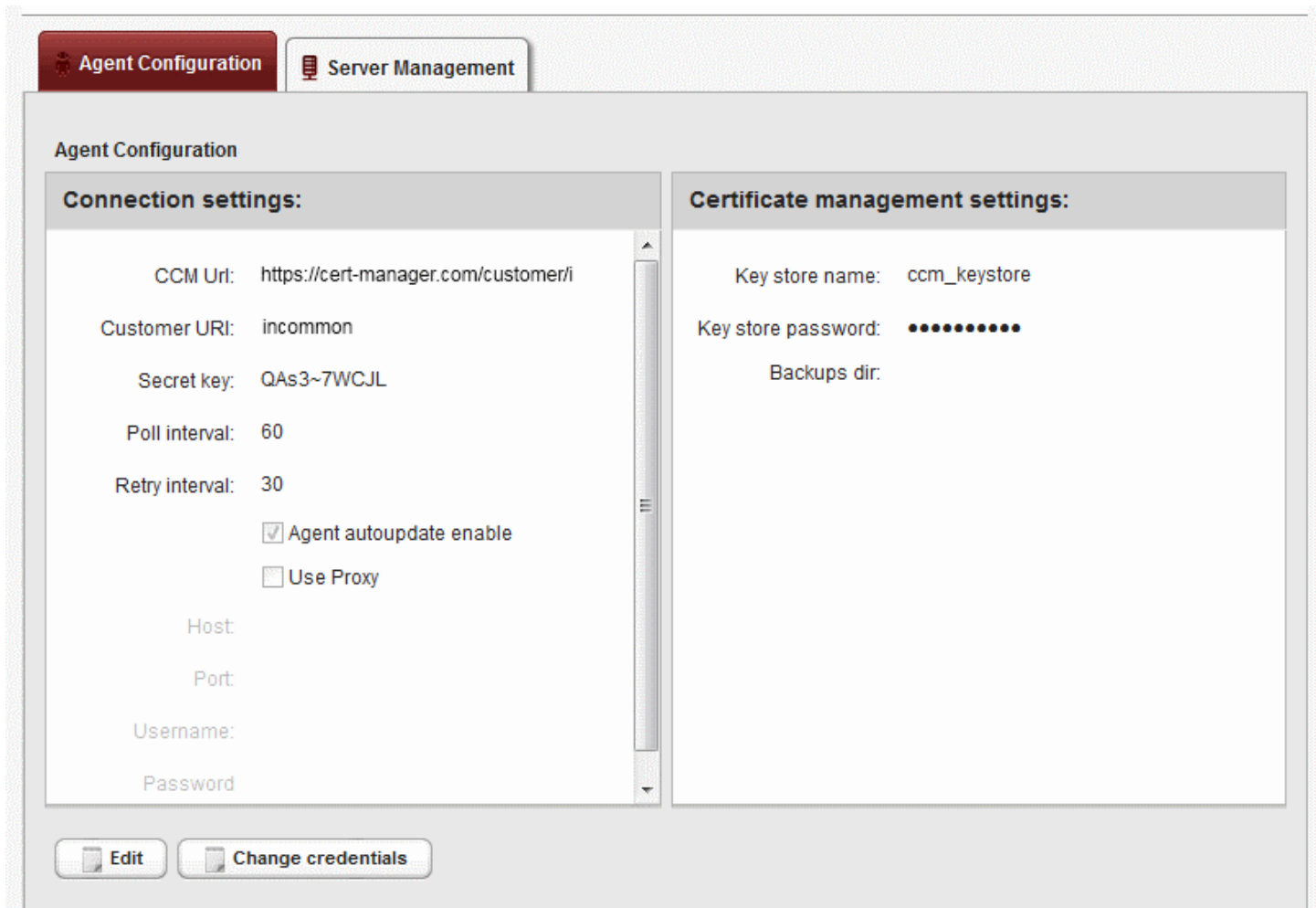
- Type `http://<IP Address/host name of the server on which the agent is installed>:9090` in the address of your browser.

The login dialog will appear:



- Enter your InCommon CM username and password.

The Agent configuration interface will open.

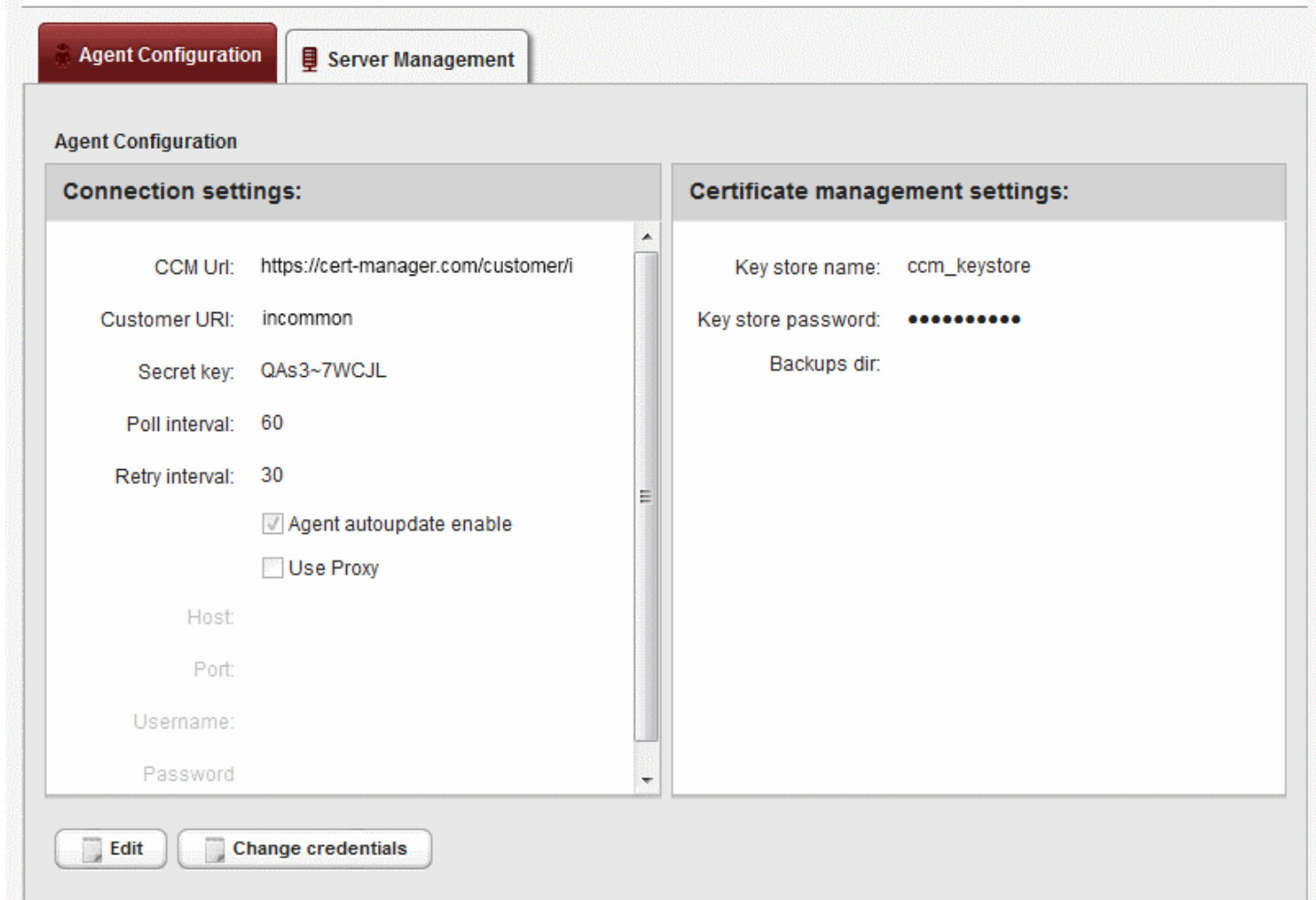


It has two tabs:

- [Agent Configuration](#)
- [Server Management](#)

Agent Configuration

The Agent Configuration tab displays the connection management settings and certificate management settings of the agent and enables the administrator to edit them, if required.



Agent Configuration

Connection settings:

CCM Uri:

Customer URI:

Secret key:

Poll interval:

Retry interval:

Agent autoupdate enable

Use Proxy

Host:

Port:

Username:

Password:

Certificate management settings:

Key store name:

Key store password:

Backups dir:

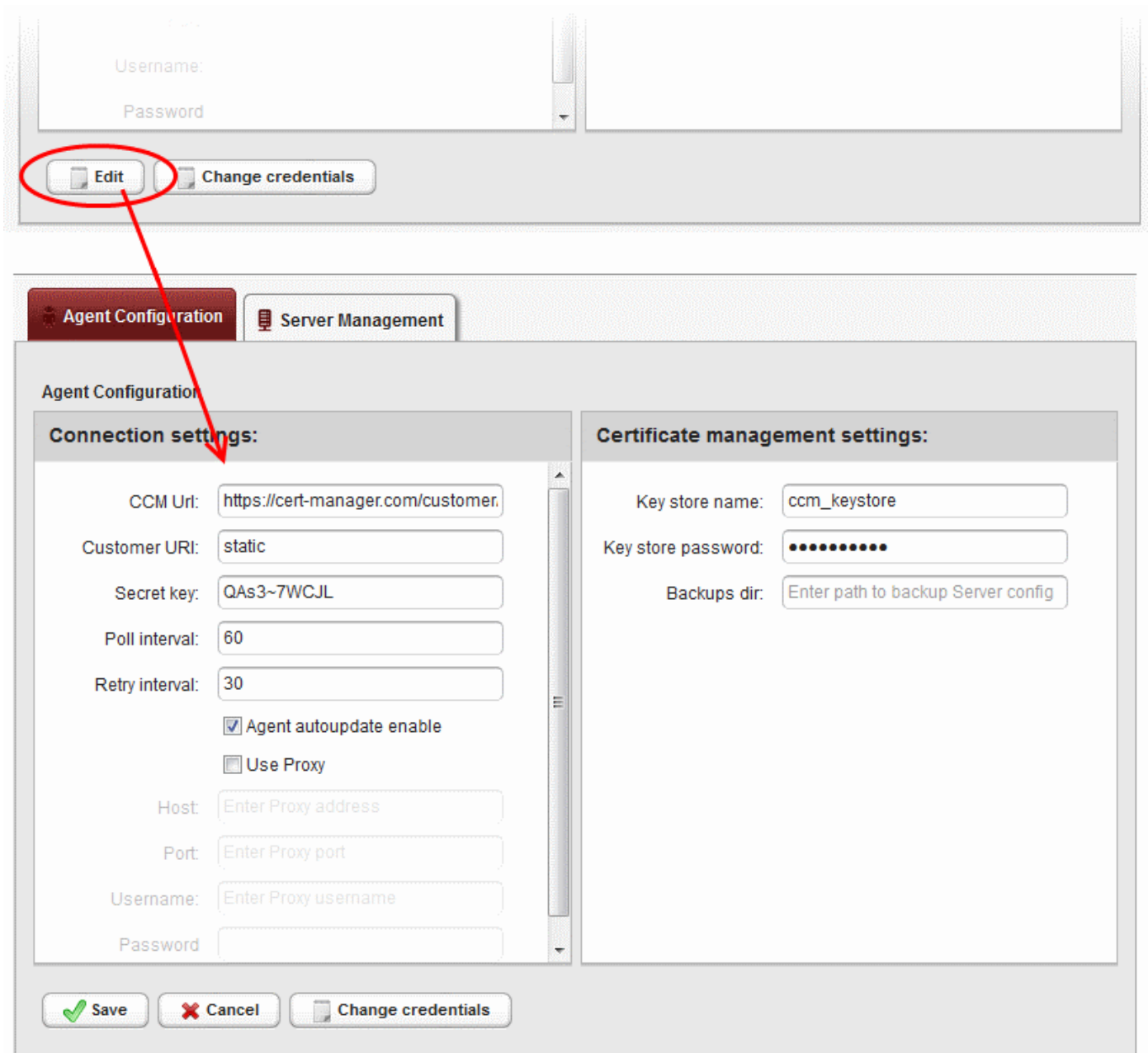
Agent Configuration - Table of Parameters

Field	Type	Description
Connection Settings		
CCM url	<i>Text field</i>	Displays the URL of Certificate Manager server
Customer URI	<i>Text field</i>	Displays the uniform resource identifier (URI) of the customer
Secret key	<i>Text field</i>	Displays the secret key unique to the agent, which it uses to identify it to CM. This value should not be altered



Poll Interval	<i>Text field</i>	Displays the time interval at which the agent polls the CM for new certificate requests (in seconds) and enables the administrator to edit it in edit mode.
Retry interval	<i>Text field</i>	Displays the time interval set for retrying polling on CM server if polling fails (in seconds) and enables the administrator to edit it in edit mode.
Agent autoupdate enable	<i>Checkbox</i>	Indicates whether the agent is enabled for auto-update. The checkbox enables the administrator to switch the auto-update on/off in edit mode.
Use Proxy	<i>Checkbox</i>	Indicates whether the agent is configured to use a proxy server. The checkbox and the text fields below it enable the Administrator to instruct the agent to use proxy server and to specify the proxy server details, if required.
Host	<i>Text field</i>	Displays the IP/Host name of the proxy server and enables the Administrator to specify it in edit mode
Port	<i>Text field</i>	Displays the port of the proxy server for the agent to connect and enables the Administrator to specify it in edit mode
Username	<i>Text field</i>	Displays the username of the administrator account to login to the proxy server and enables the Administrator to specify it in edit mode
Password	<i>Text field</i>	Displays the password of the administrator account to login to the proxy server and enables the Administrator to specify it in edit mode
Certificate Management Settings		
Key store name	<i>Text field</i>	The name of the CM keystore file, pertaining to the agent. By default, it will be 'ccm_keystore'. The Administrator can edit it in the edit mode
Keystore password	<i>Text field</i>	The password to access the CM keystore file. The Administrator can edit it in the edit mode
Backup dir	<i>Text field</i>	Displays the folder path for backup of keystore file. The Administrator can edit it in the edit mode.

- To edit the agent configuration settings, click the 'Edit' button at the bottom left. The Agent Configuration page will open in edit mode.



Username: _____
Password: _____

Edit **Change credentials**

Agent Configuration **Server Management**

Agent Configuration

Connection settings:

CCM Uri:

Customer Uri:

Secret key:

Poll interval:

Retry interval:

Agent autoupdate enable

Use Proxy

Host:

Port:

Username:

Password:

Certificate management settings:

Key store name:

Key store password:

Backups dir:

Save **Cancel** **Change credentials**

- Edit the required fields and click 'Save' for your changes to take effect.

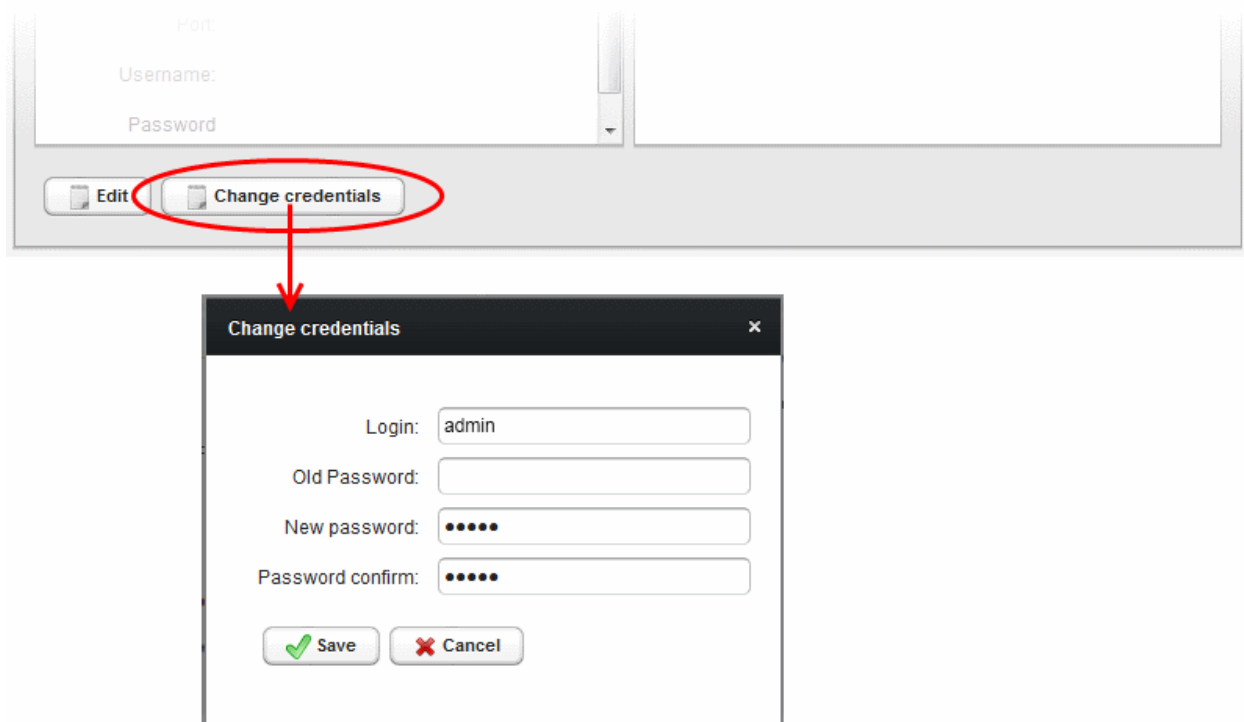
Changing Login Credentials for the Agents Configuration Console

By default, the administrator can use the username and password of their CM account to login to the agent configuration. If needed, the administrator can change their username and password for the agent configuration console at any time.

To change the username and password

- Click 'Change credentials' from the agent configuration interface.

The 'Change Credentials' dialog will appear.



- To change your username, directly edit the Login field
- Enter your existing password in the 'Old Password' field
- Enter your new password in the New password field and reenter it for confirmation in the Password Confirmation field
- Click 'Save'

From the next login to the agent configuration console, you need to use the new username and password.

Server Management

The Server Management tab enables the administrator to view, add and edit the servers for which the agent is configured.

Agent Configuration
Server Management

Server Management

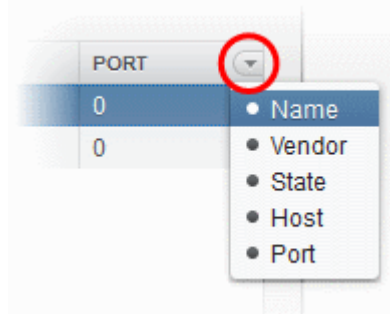
Refresh
+ Add
Edit
X Delete

NAME	VENDOR	STATE	HOST	PORT
Server IIS Dithers Company	IIS	RUNNING		0
Server Tom Dithers	TOMCAT	INIT	192.168.111.111	0

The 'Server Management' tab displays the list of servers added to the agent with the vendor and activation status details. The administrator can add new servers and edit the details like the login username and password for the existing servers through this interface.

Column Display	Description
Name	Displays the name of the server.
Vendor	Displays the vendor of the server.
State	Indicates whether or not the server is initialized.
Host	Displays the IP address or the host name of the server for remote connection
Port	Displays the connection port of the server for remote connection.

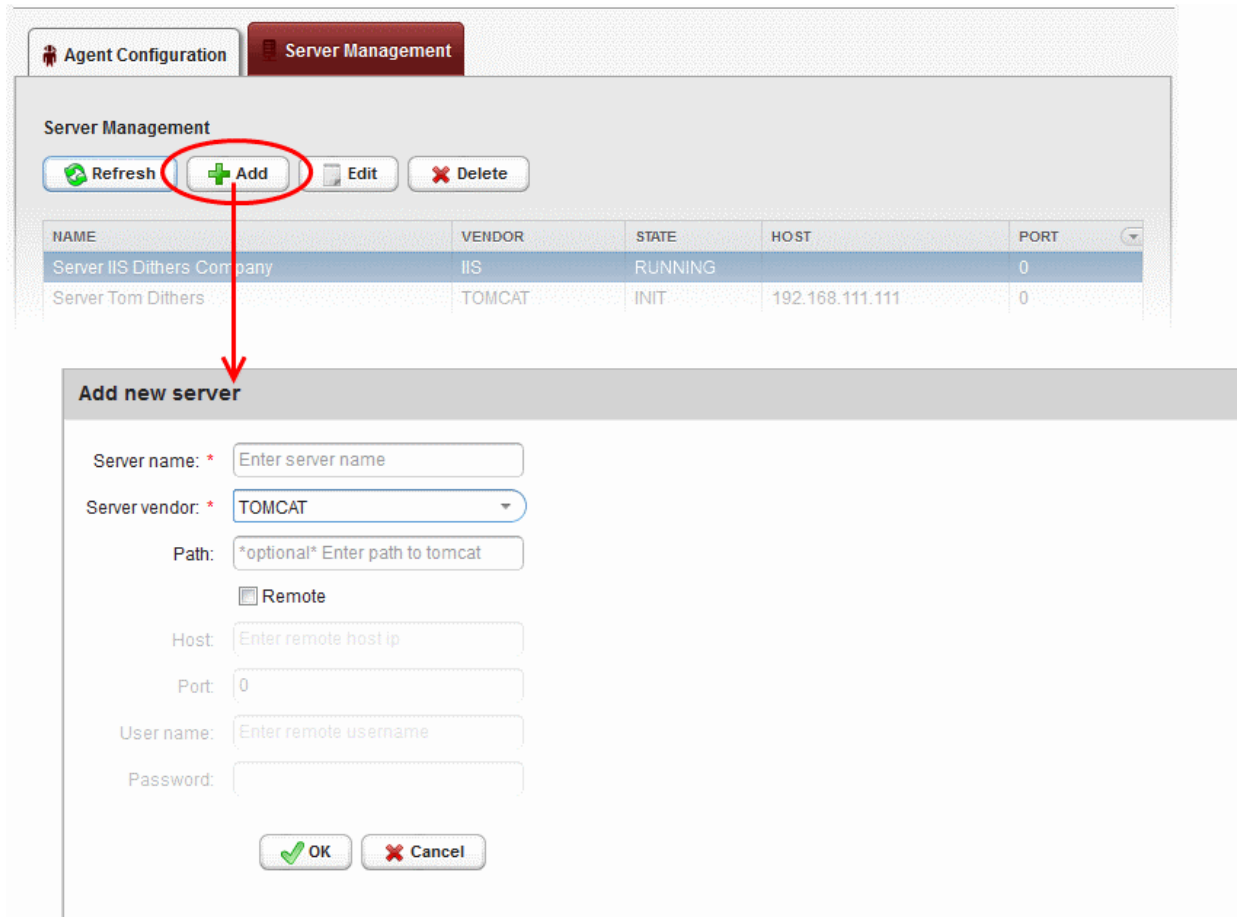
Note: The administrator can enable or disable desired columns from the drop-down at the right end of the table header:



Controls		
	Add	Enables the Administrator to add a new server to the agent
	Refresh	Updates the list of displayed servers.
Server Controls		
	Edit	Enables administrators to modify the Server configuration settings.
Note: The Server control buttons will appear only on selecting a server.	Delete	Removes the Server.

To add a server

- Click 'Add' from the top left. The 'Add new server' dialog will appear.



The screenshot shows the 'Server Management' section of the Certificate Manager. At the top, there are tabs for 'Agent Configuration' and 'Server Management'. Below the tabs, there are buttons for 'Refresh', 'Add', 'Edit', and 'Delete'. The 'Add' button is circled in red, and a red arrow points from it to a dialog box titled 'Add new server'. The dialog box contains the following fields:

- Server name: * Enter server name
- Server vendor: * TOMCAT
- Path: *optional* Enter path to tomcat
- Remote
- Host: Enter remote host ip
- Port: 0
- User name: Enter remote username
- Password:

At the bottom of the dialog box, there are 'OK' and 'Cancel' buttons.

Add new server - Table of Parameters

Field Name	Type	Description
Server name	String	Enter the name of the server.
Server vendor	drop-down	Choose the vendor of the server from the drop-down.
Path	String	Specify the network path for the Tomcat server. This is required only if the Tomcat server is not accessible from the CM console. Note: This field will appear only of Tomcat server is selected in the Server vendor drop-down.
Remote	Checkbox	Specify whether the server is Remote or Local. While adding remote servers for agent-less automatic certificate installation, this checkbox should be selected and the login credentials for an administrative account on the server are to be provided.
Host	String	Specify the IP address or host name of the server for remote connection.

Add new server - Table of Parameters

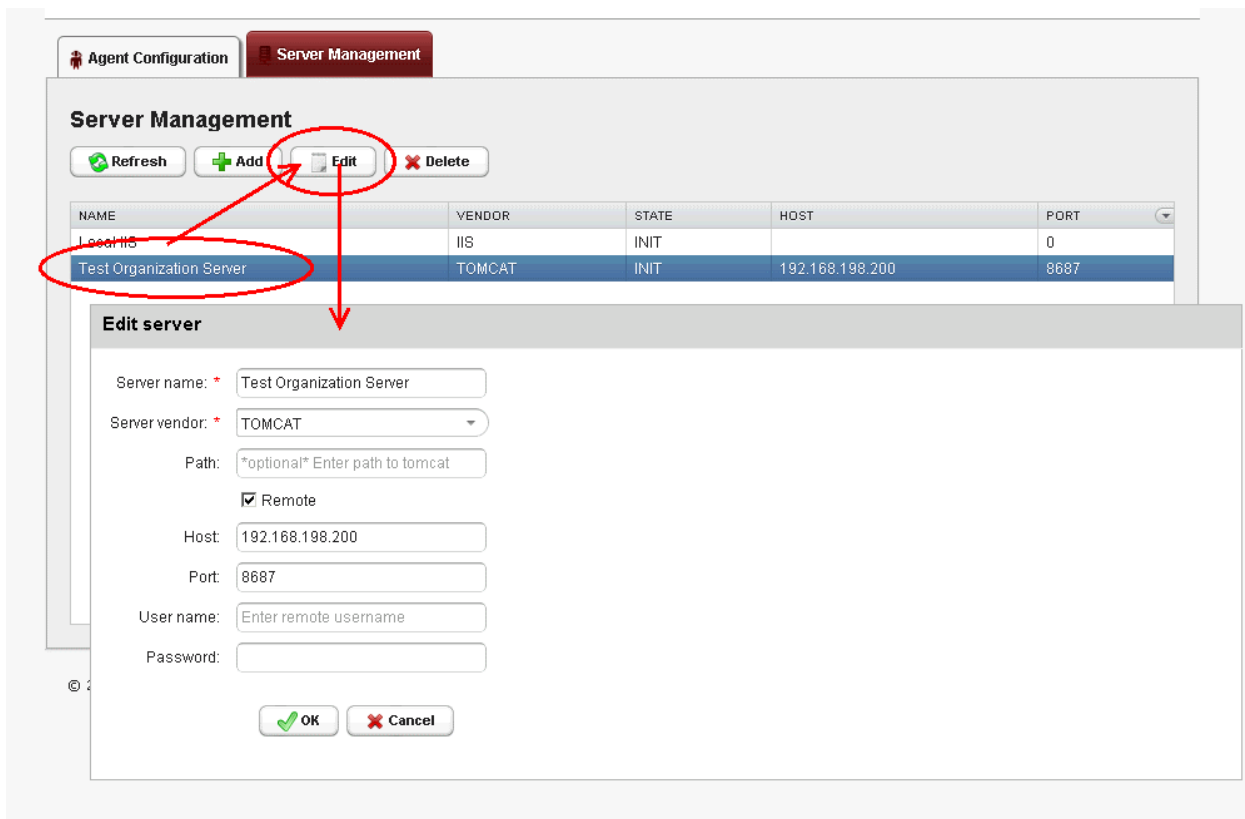
		Note: This field will be enabled only if 'Remote' is selected.
Port	<i>String</i>	Specify the connection port of the server for remote connection. Note: This field will be enabled only for remote 'Tomcat' server.
User Name	<i>String</i>	Enter the username of the administrator for loggin-into the server. Note: This field will be enabled only if 'Remote' is selected.
Password	<i>String</i>	Enter the log-in password for the administrator account for logging-into the server. Note: This field will be enabled only if 'Remote' is selected.

- Enter the parameters and click 'OK'.

The new server will be added and enabled for automatic installation of SSL certificates and to run scans for certificate discovery.

To edit a server

- Select the server and click the 'Edit' button that appears on top.



The Edit server dialog will open. The interface is similar to [Add new server](#) interface.

- Edit the required fields and click 'OK' for your changes to take effect.