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 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

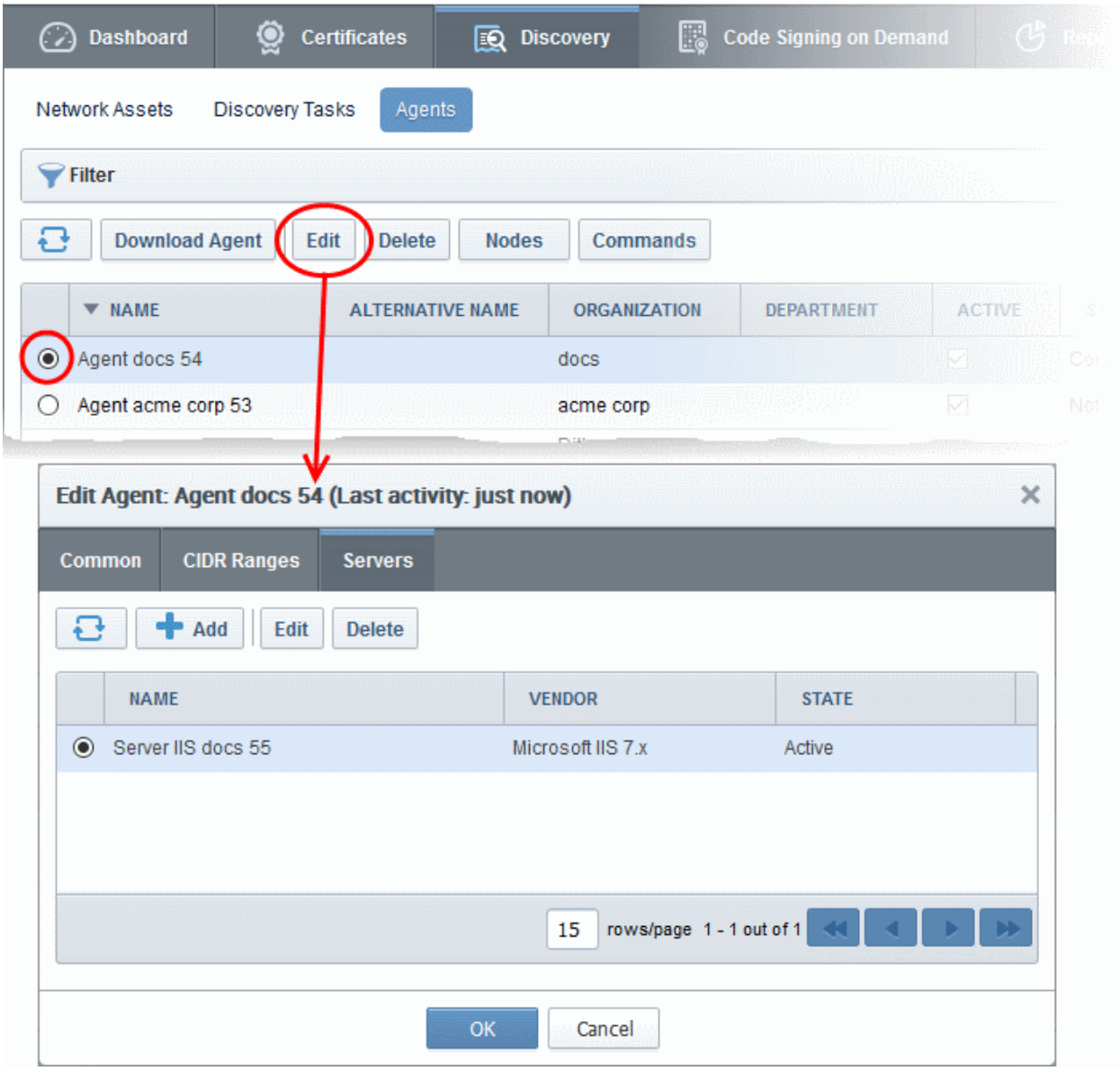
Enterprise Controller mode allows admins to automatically install certificates on any remote server on the network.

- 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

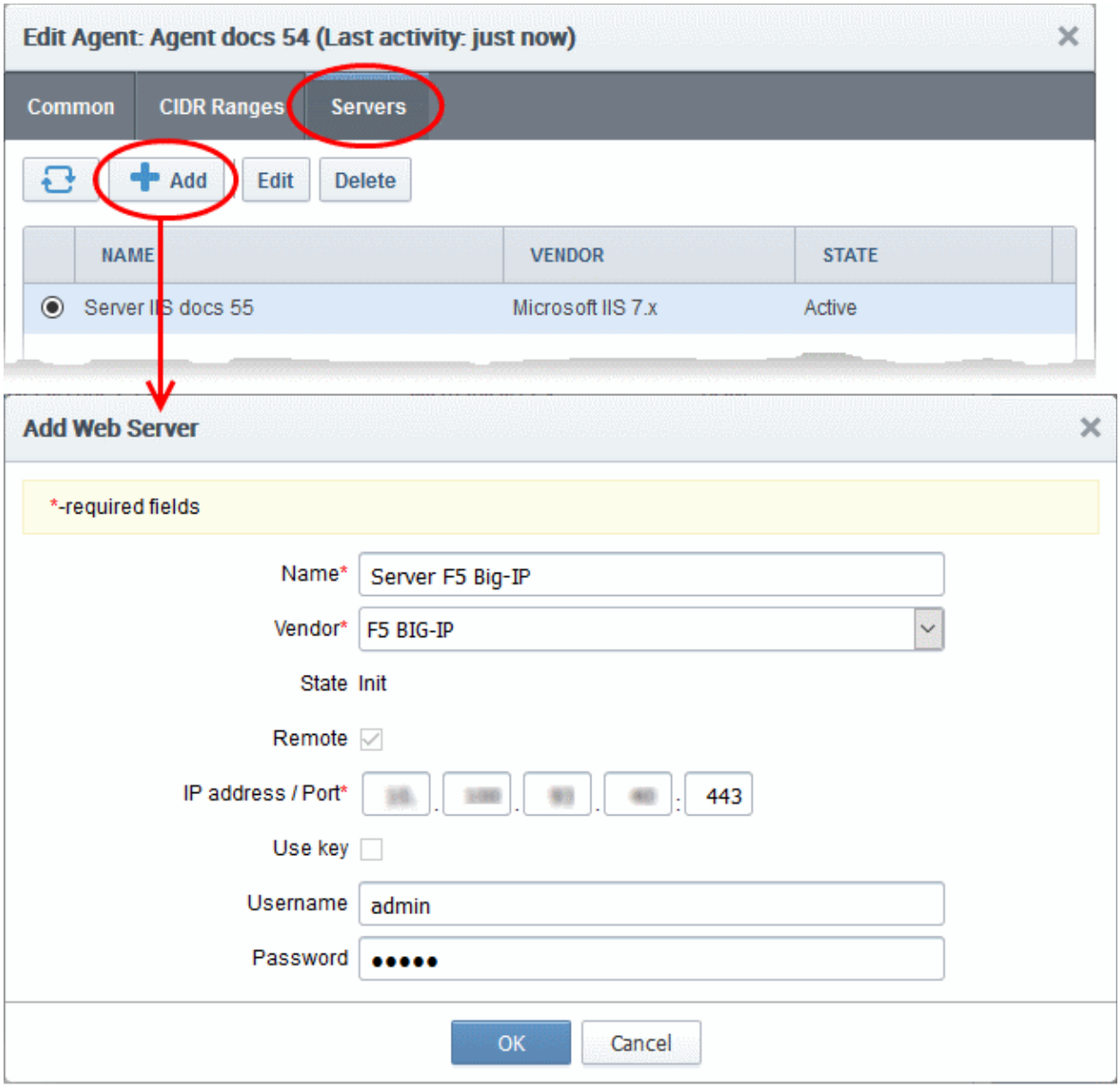
- Click 'Discovery' > 'Agents':



- 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.

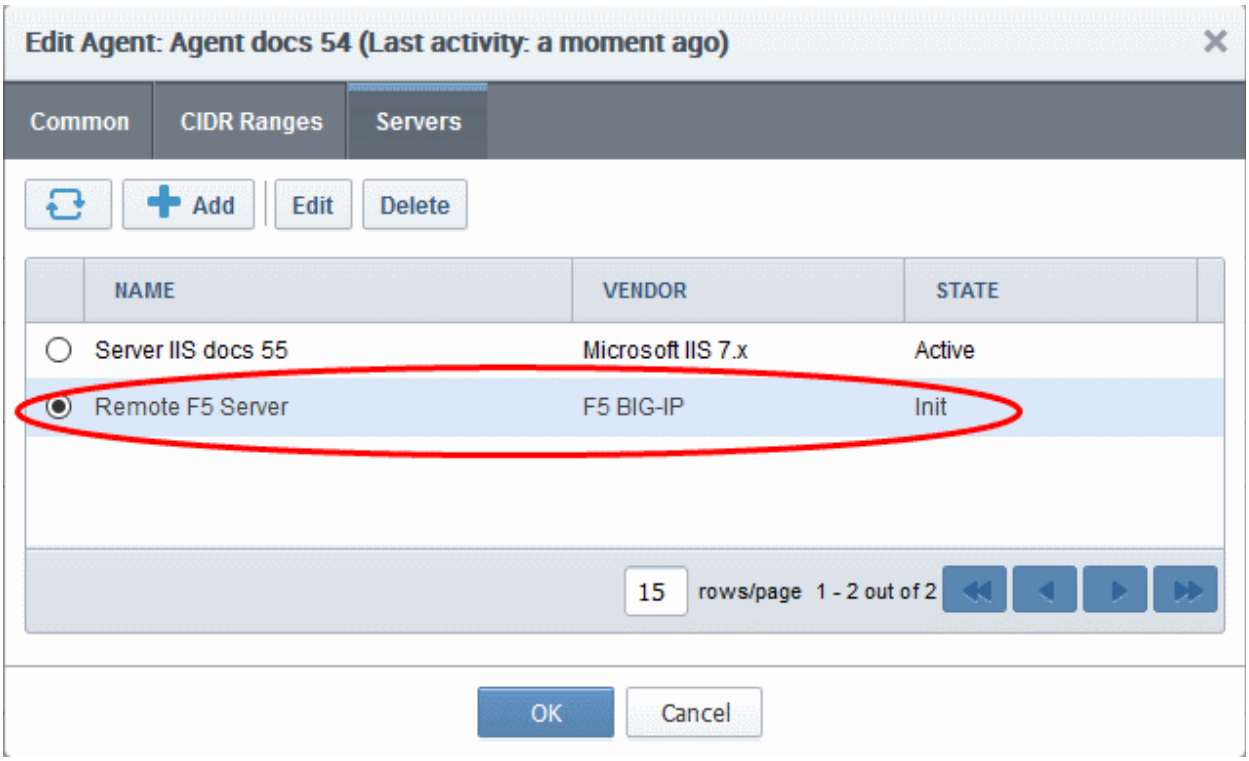
- Click 'Add' to associate a remote server with the controller. The 'Add Web Server' dialog will open.


Edit Agent: Agent docs 54 (Last activity: just now)
Common
CIDR Ranges
Servers
Add
Edit
Delete
NAME
VENDOR
STATE
Server IIS docs 55
Microsoft IIS 7.x
Active
Add Web Server
*-required fields
Name*
Server F5 Big-IP
Vendor*
F5 BIG-IP
State
Init
Remote
IP address / Port*
443
Use key
Username
admin
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: • Microsoft IIS 7.x • Apache, Tomcat 5.x, 6.x and 7.x • F5 BIG-IP **Note**: Agents installed on a Windows server will only support IIS and F5 BIG-IP web-server types. Agents installed on a Linux server support all types (Apache, Tomcat, IIS and F5).
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'.



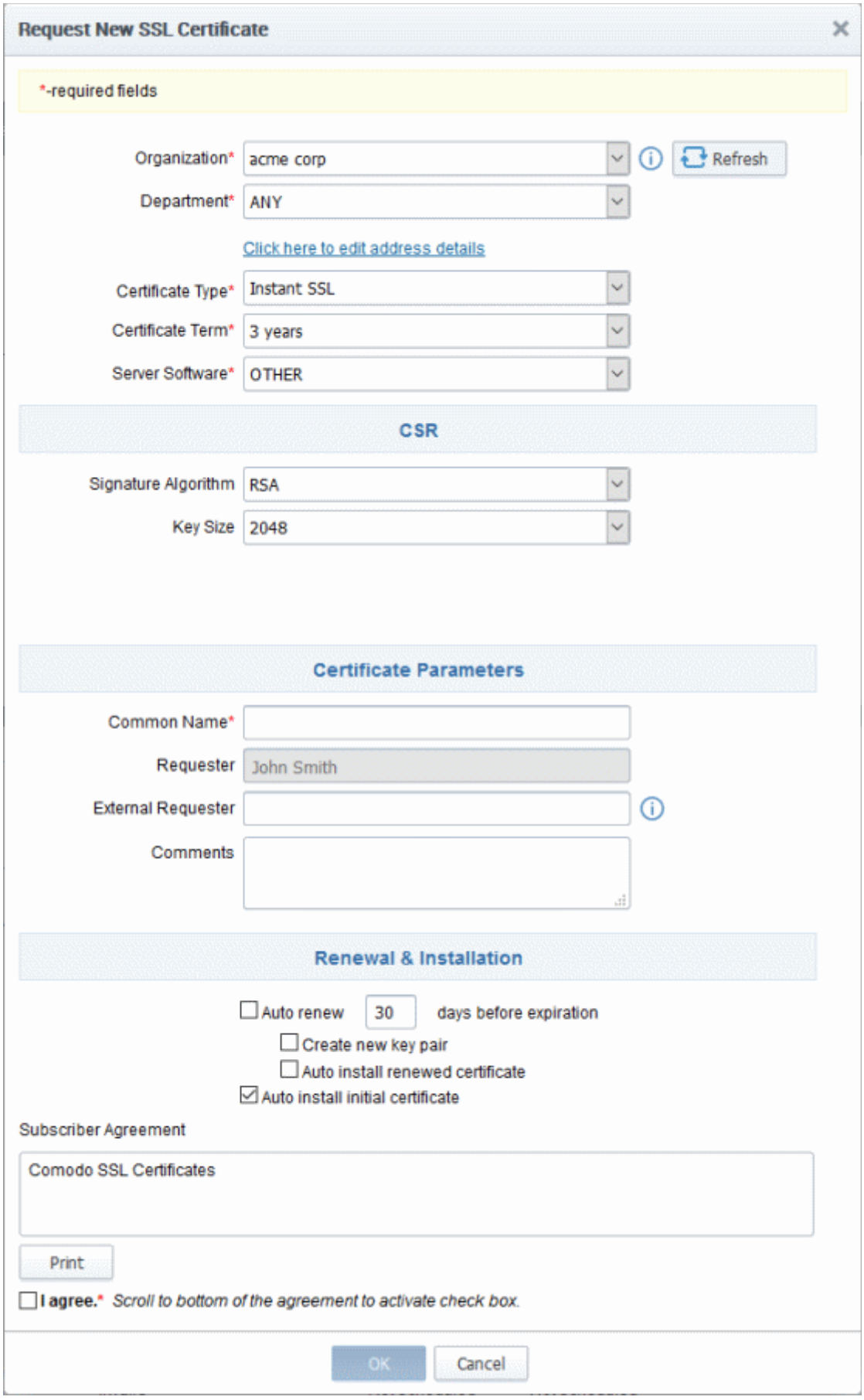
Once the remote server is added to the controller, administrators can apply for certificates for domains on the server in the 'Certificates Management' > 'SSL Certificates' area.

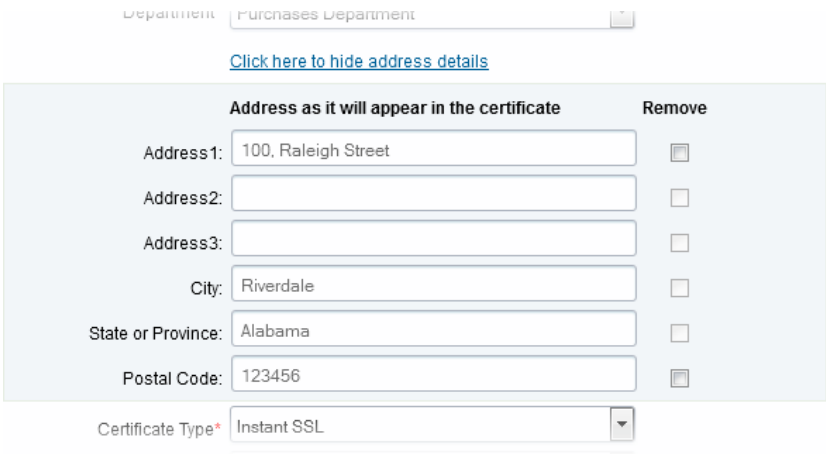
- Repeat the process to add more remote servers

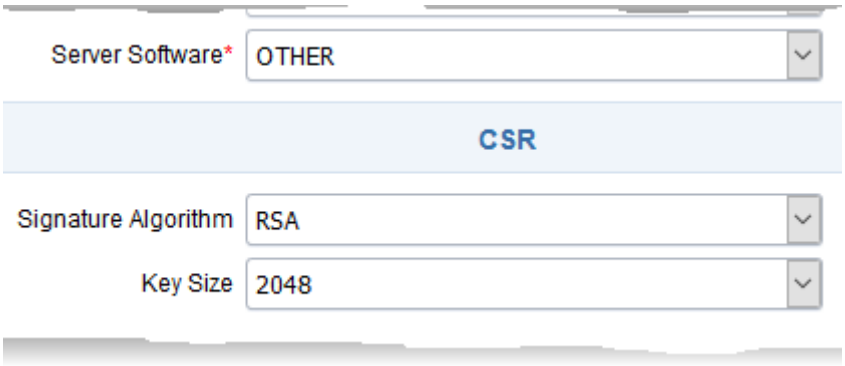
To enroll a certificate for auto-installation

- 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*
acme corp
Refresh
Department*
ANY
Click here to edit address details
Certificate Type*
Instant SSL
Certificate Term*
3 years
Server Software*
OTHER
CSR
Signature Algorithm
RSA
Key Size
2048
Certificate Parameters
Common Name*
Requester
John Smith
External Requester
Comments
Renewal & Installation
Auto renew
30
days before expiration
Create new key pair
Auto install renewed certificate
Auto install initial certificate
Subscriber Agreement
Comodo SSL Certificates
Print
I agree.* Scroll to bottom of the agreement to activate check box.
OK
Cancel

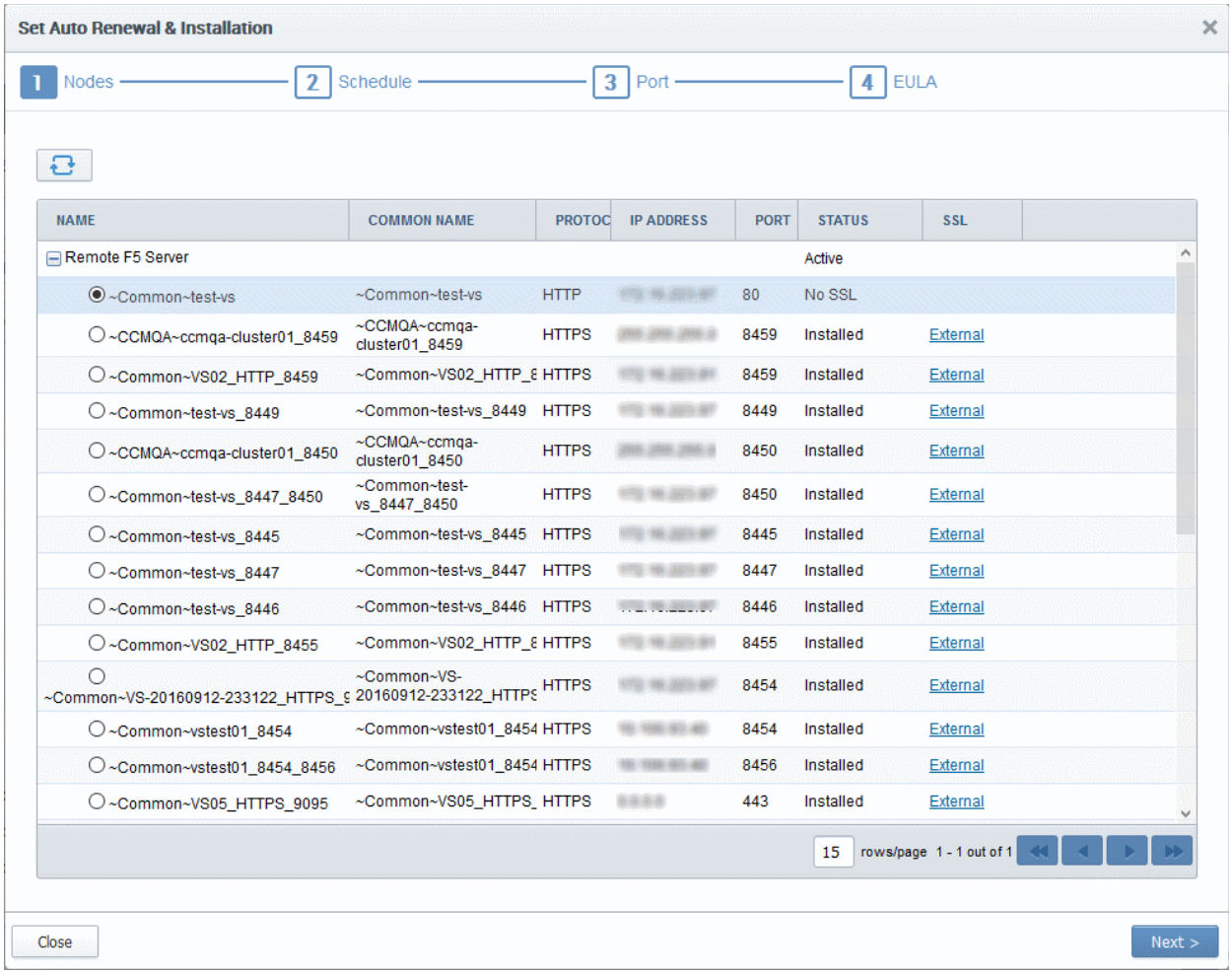
Form Element	Type	Description
Organization (***required***)	Drop-down list	Choose the Organization that the SSL certificate will belong to.
Department (***required***)	Drop-down list	Choose the Department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'.
Click here to edit address details	*Text Fields*	Clicking this link will expand the address fields.  The address fields are auto-populated from the details of the Organization or Department on whose behalf this certificate request is being made. These fields cannot be modified but, in the case of OV level certificates, the administrator can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields. The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted". For EV level certificates, it is mandatory to include and display address details of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down.
Certificate Type (***required***)	*Drop-down list*	Choose the certificate type that you wish to add for auto-installation. **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.
Certificate Term	*Drop-down list*	Choose the validity period of the certificate. For example, 1 year, 2

Form Element	Type	Description
(***required***)		years, 3 years.
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: • Apache/Mod SSL • Apache - SSL • Apache Tomcat • Microsoft IIS 1.x to 4.x • Microsoft IIS 5.x and above • F5 BIG-IP **Note**: Choose 'OTHER' if you want to use F5 BIG-IP.
CSR		
Provide CSR/Autogenerate CSR and Manage Private Key CSR (***required***) Get CN from CSR (***optional***) Upload CSR (***optional***)	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. Once you choose 'Auto install initial certificate' under 'Renewal & Installation' in this form, these fields will disappear. 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'. 	
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.

Form Element	Type	Description
External Requester (optional)	*Text Field*	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 (***optional***)	*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 (***required***)	*Control*	You must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox.

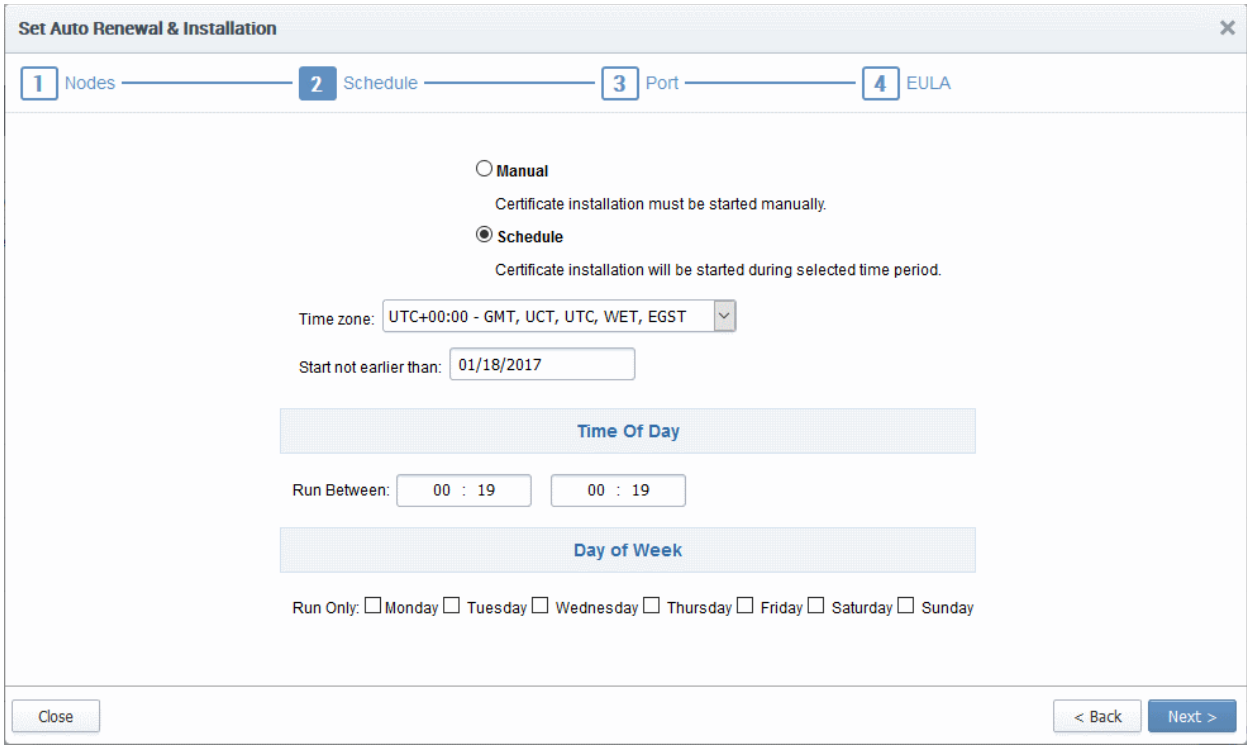
- Click 'OK' to submit the application

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



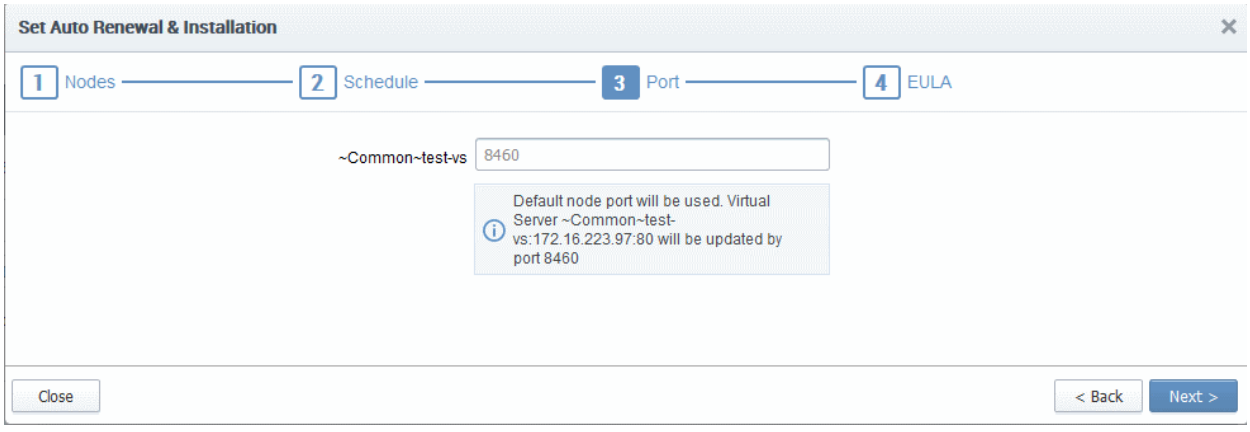
- Select the domain from the remote server for which you wish to install a SSL certificate and click 'Next'.

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.



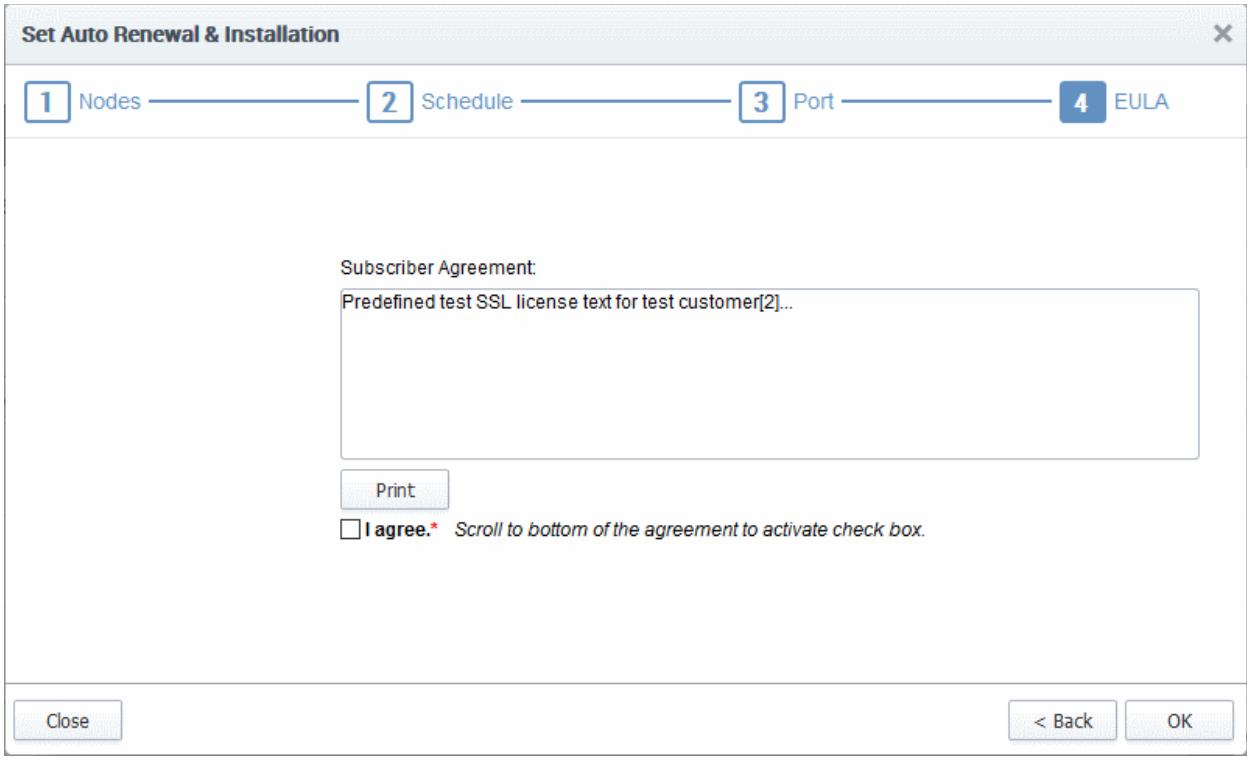
- If you want to manually install the certificate from the InCommon CM interafce, select 'Manual'
- If you want to install the certificate at a scheduled time, select 'Schedule', select your time zone, and set a time period. The controller will generate the CSR and submit it to InCommon CA the next time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

The 'Port' interface will open.



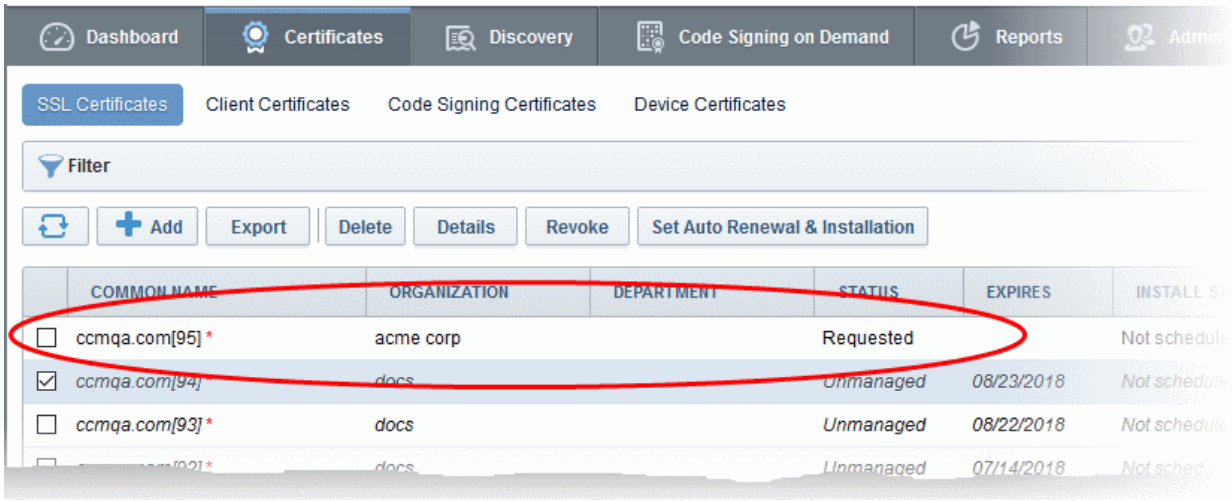
- Specify the HTTPS port for installing the certificate, (***Default = 9443***)

- Click 'Next'. The EULA interface will open.

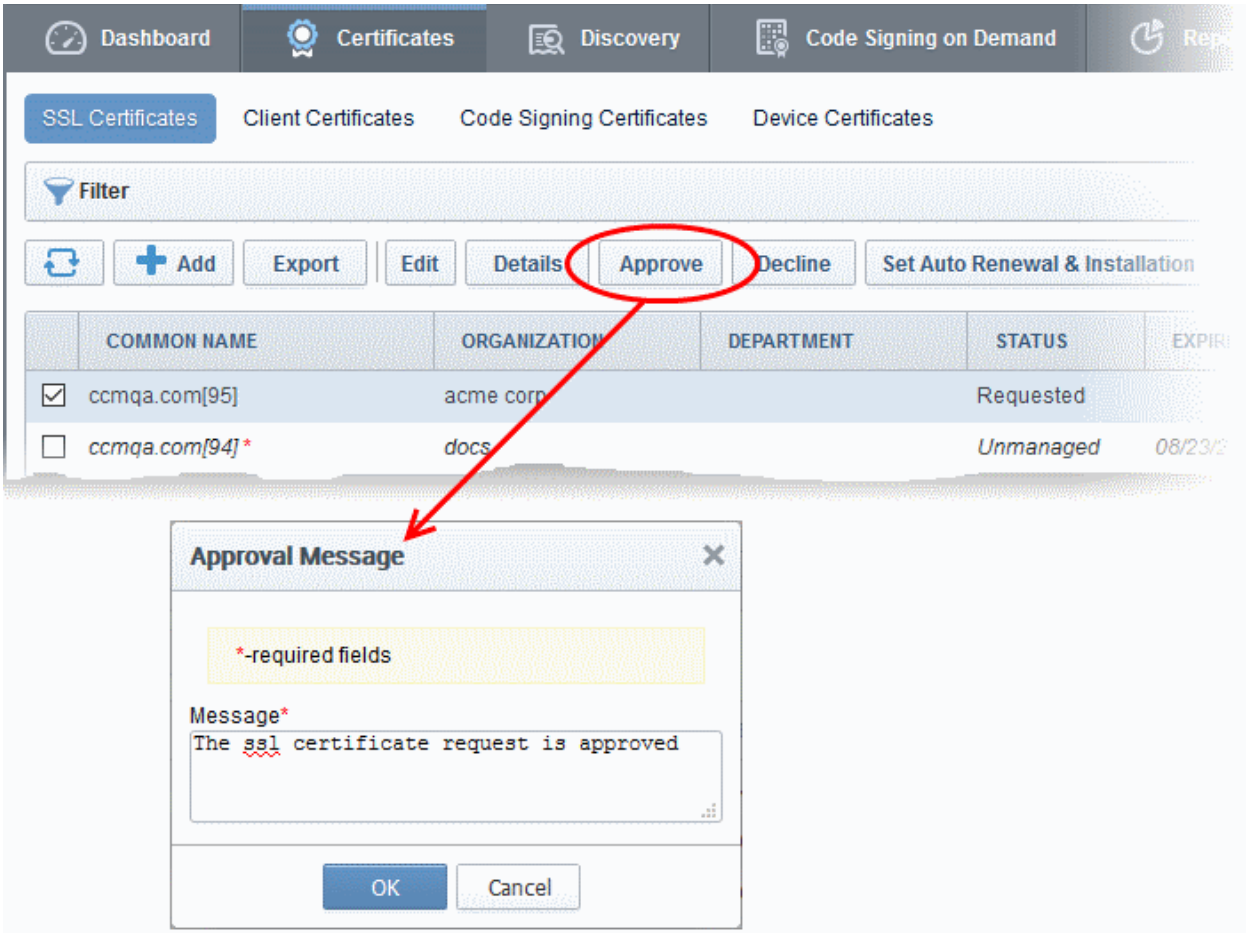


- Read the EULA fully and accept to by the selecting 'I Agree' checkbox.
- Click 'OK' to save your application.

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

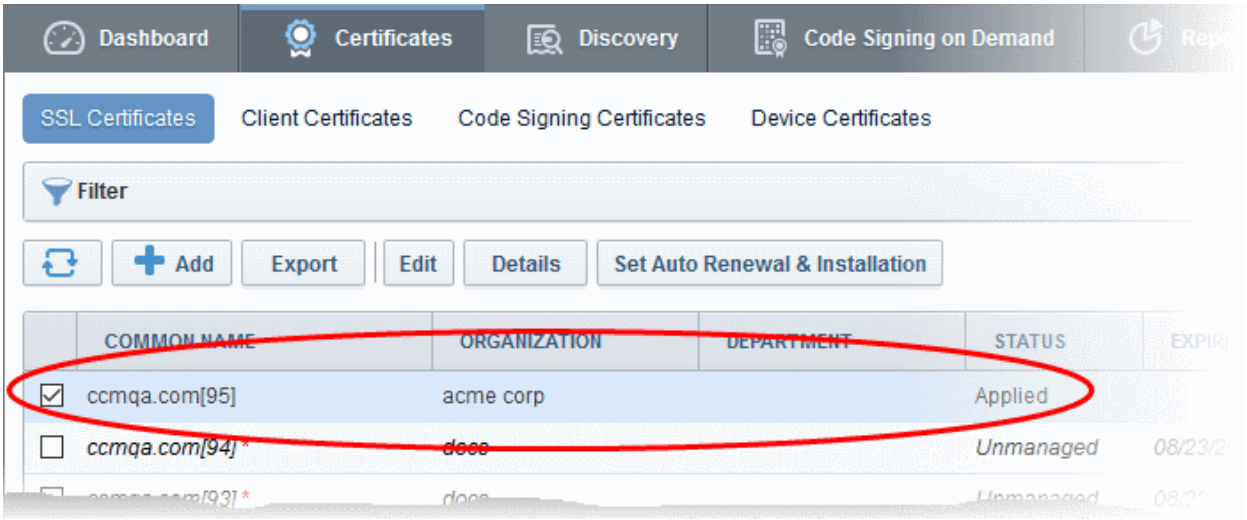


- The CSR for the requested certificate will be generated automatically. After the CSR has been created, the 'Approve' button will appear at the top when you select the certificate in the list:

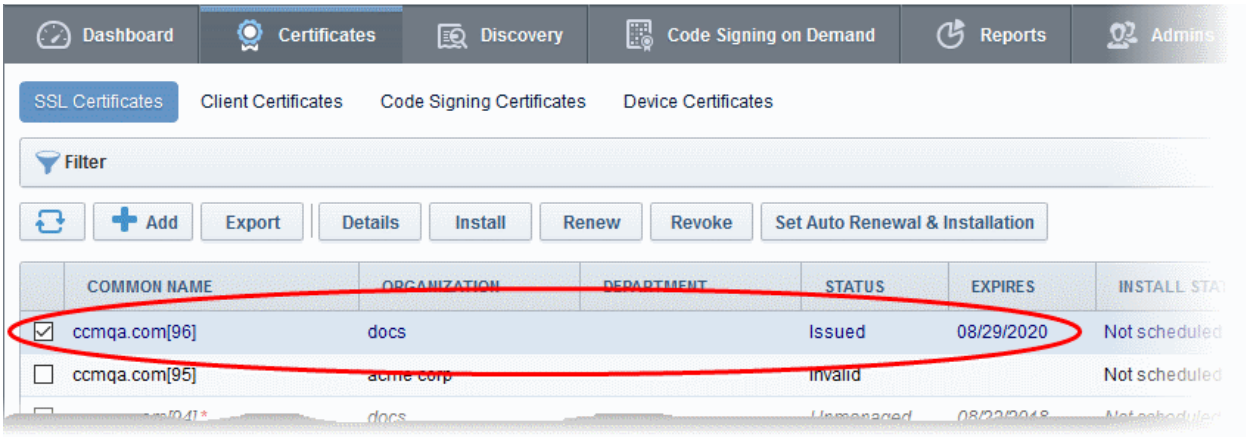


- Click the 'Approve' button to approve the request, enter an approval message and click 'OK'.

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



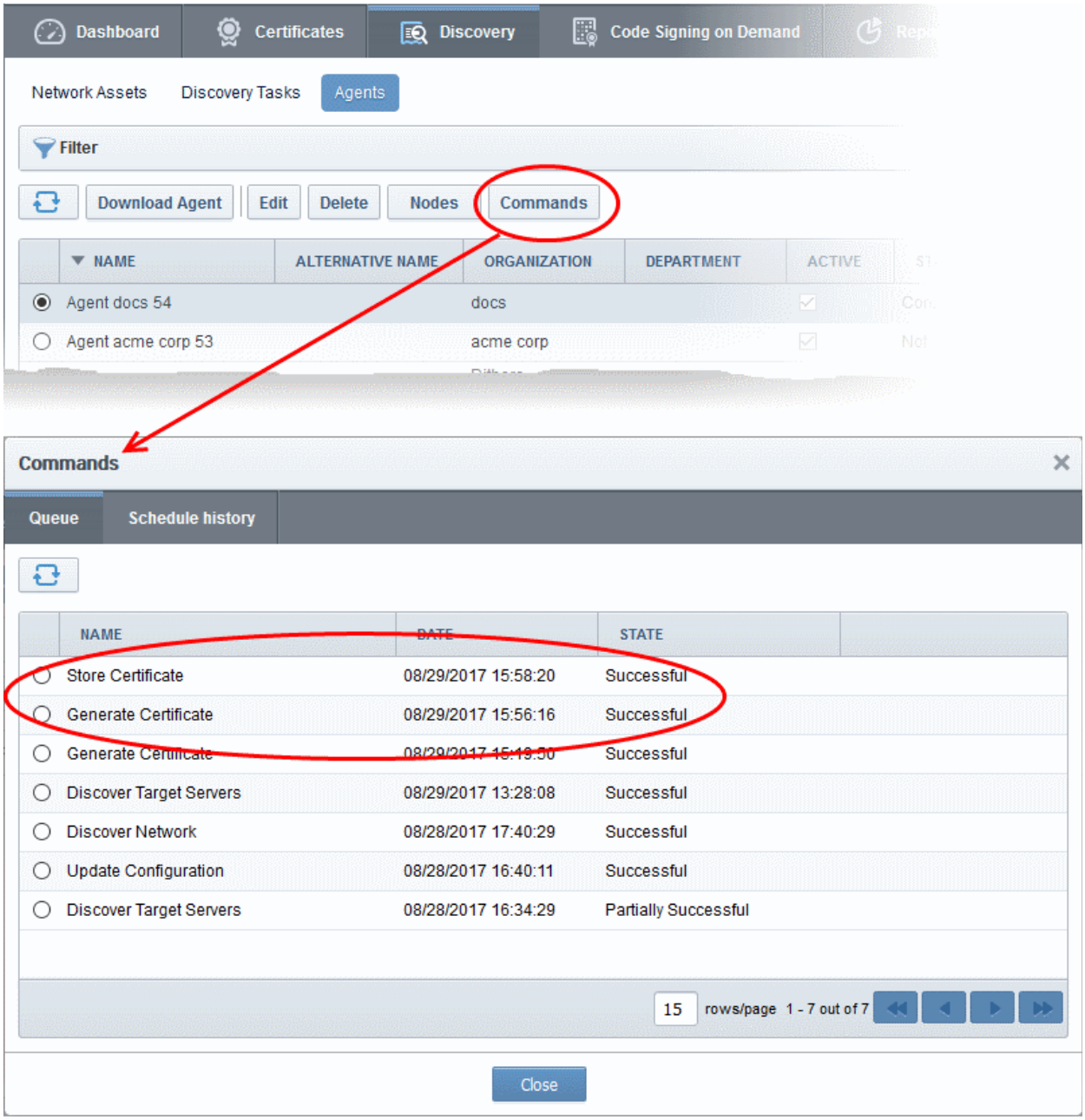
The controller will track the order number and will download the certificate once it is issued. The certificate will stored and its status will change to 'Issued'.



To check whether the Certificate Controller has stored the certificate

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

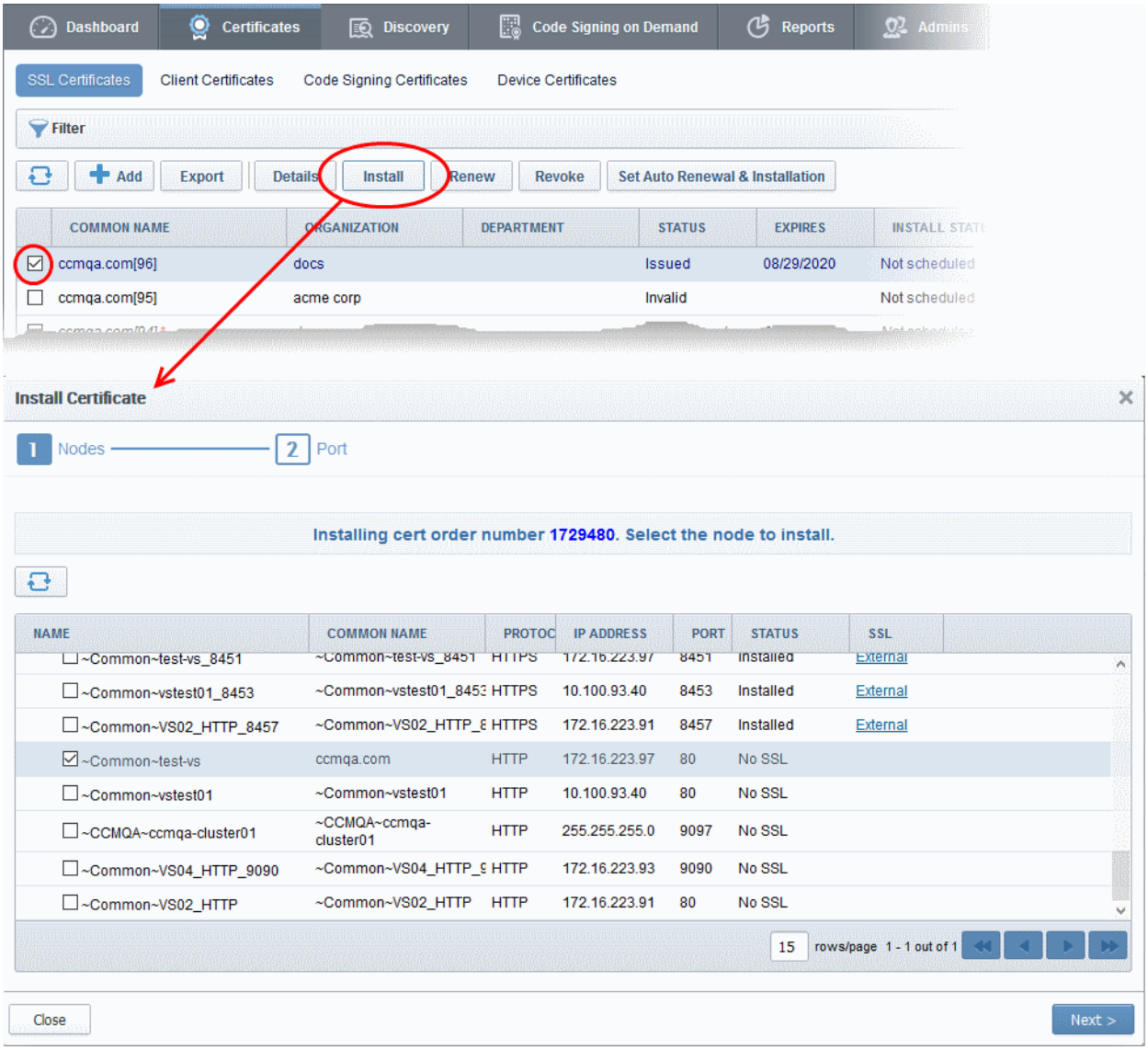
You will see successful execution of 'Store Certificate' command.



The 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

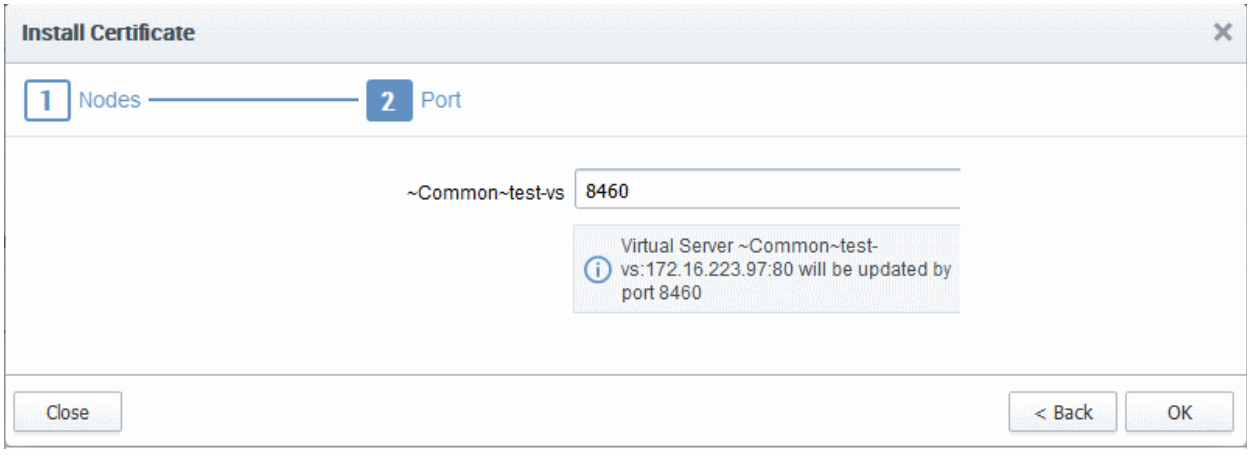
- Select the certificate from the 'Certificates' > 'SSL Certificates' interface and click 'Install'



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

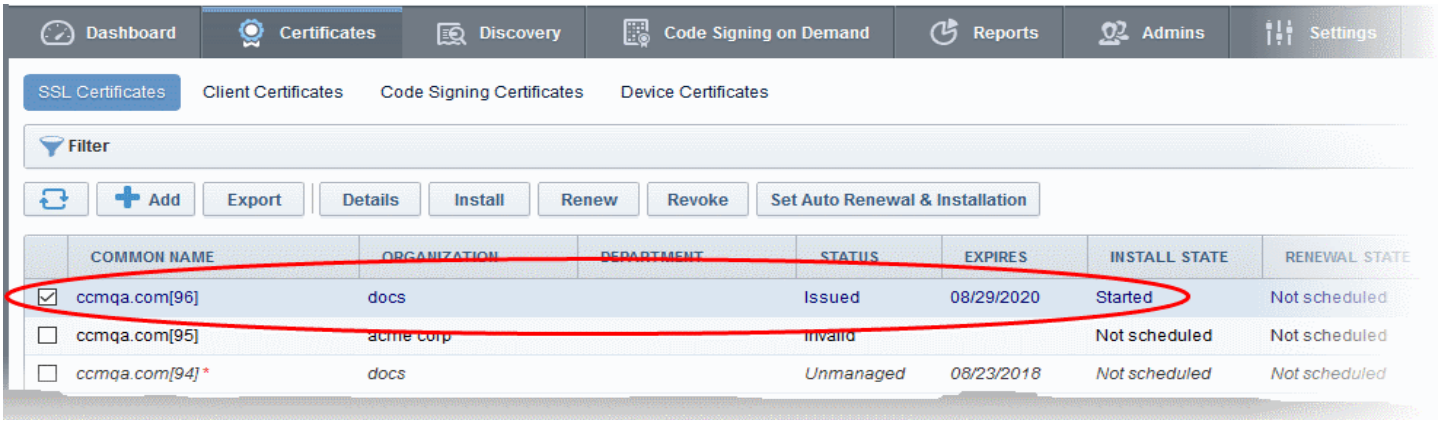
- If you want to install the same certificate to additional nodes or to a different node, select the node(s) as required
- Click 'Next'.

The 'Ports' interface will open.



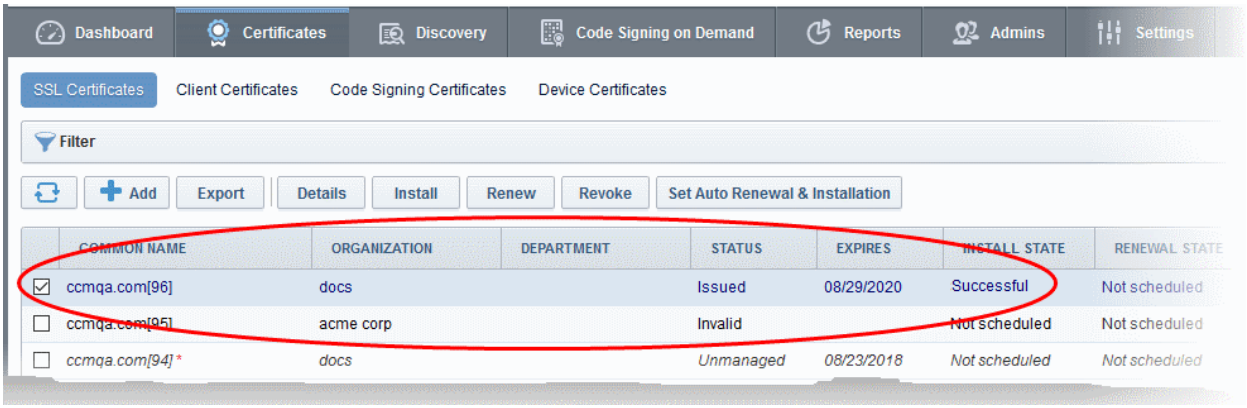
- Specify the port and click 'OK'.

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

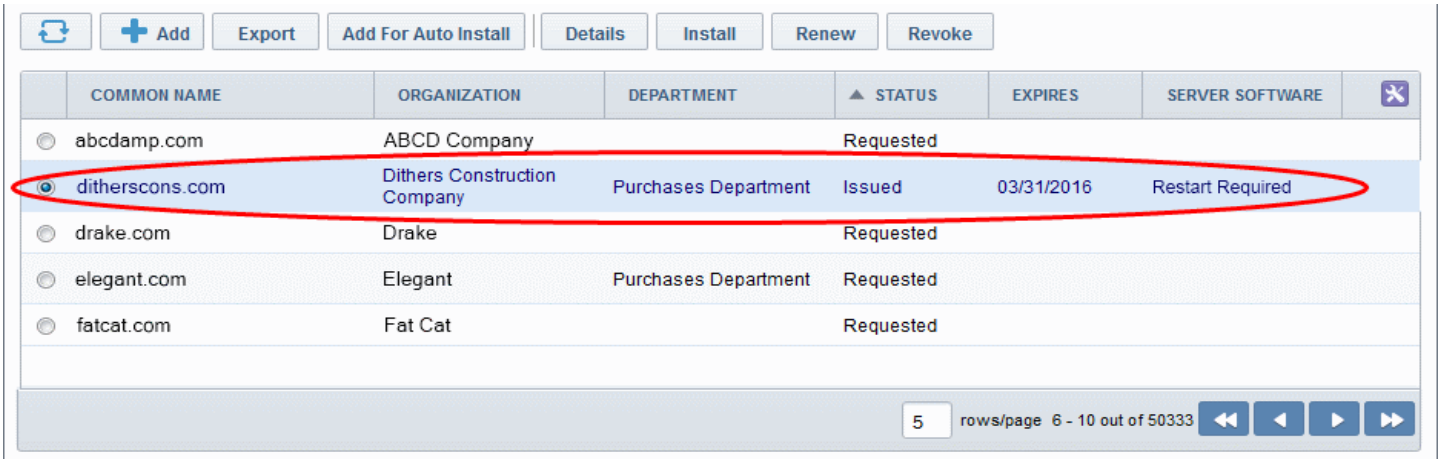


When installation is complete:

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

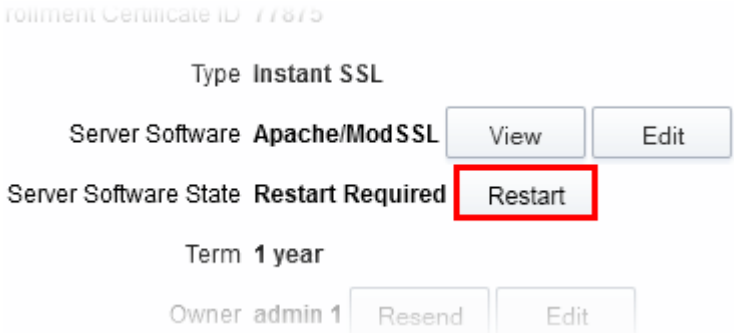


- **Apache** - The certificate will become active after the server is restarted. The install state will change to 'Restart Required'.



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

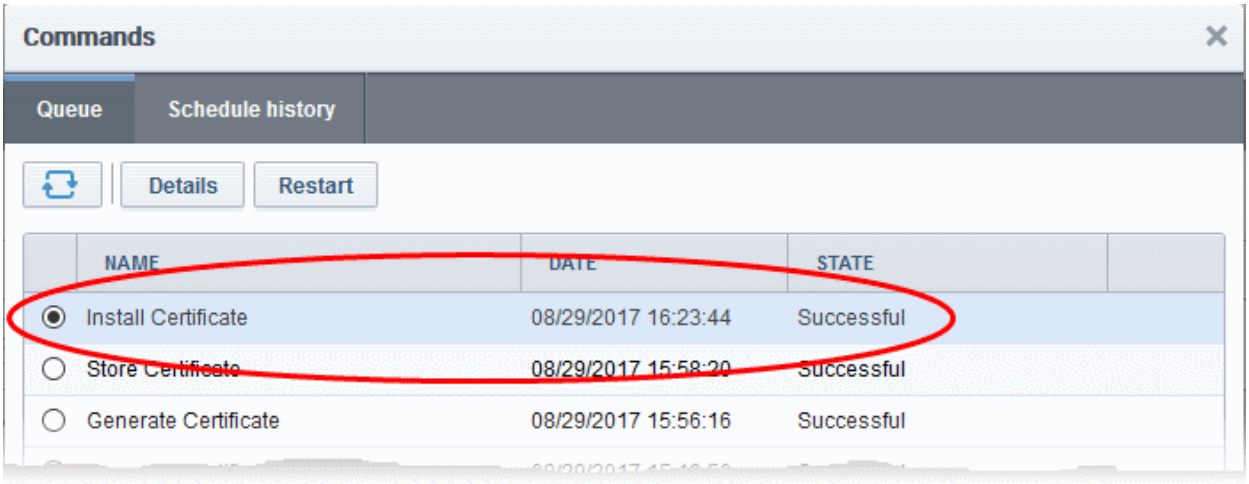
- Select the certificate and click the 'Details' button at the top. The 'Certificate Details' dialog will be displayed.
- Click 'Restart' beside the Server Software State field in the 'Details' dialog



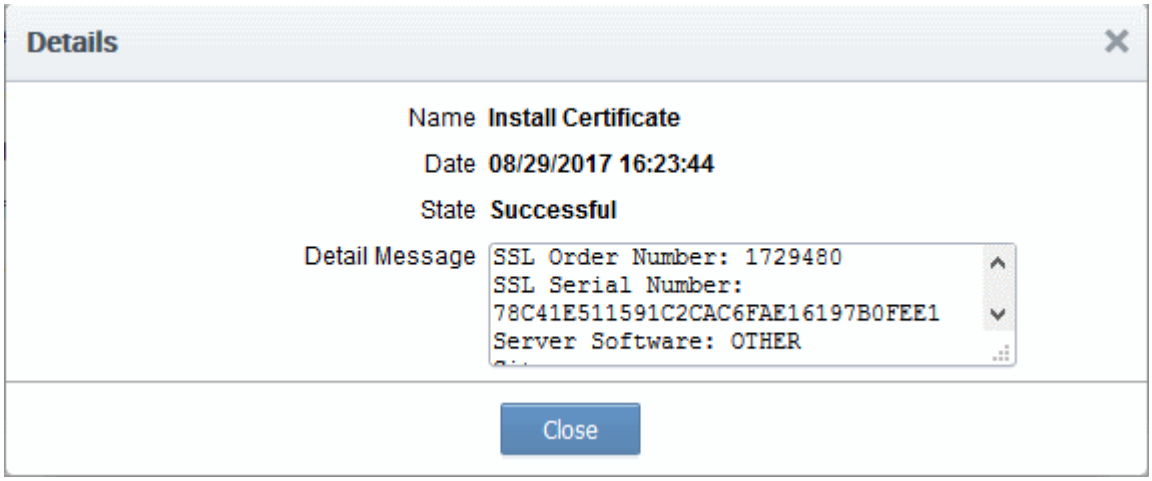
After restarting the server, the certificate will activated and the 'Install State' will change to 'Successful'.

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

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



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



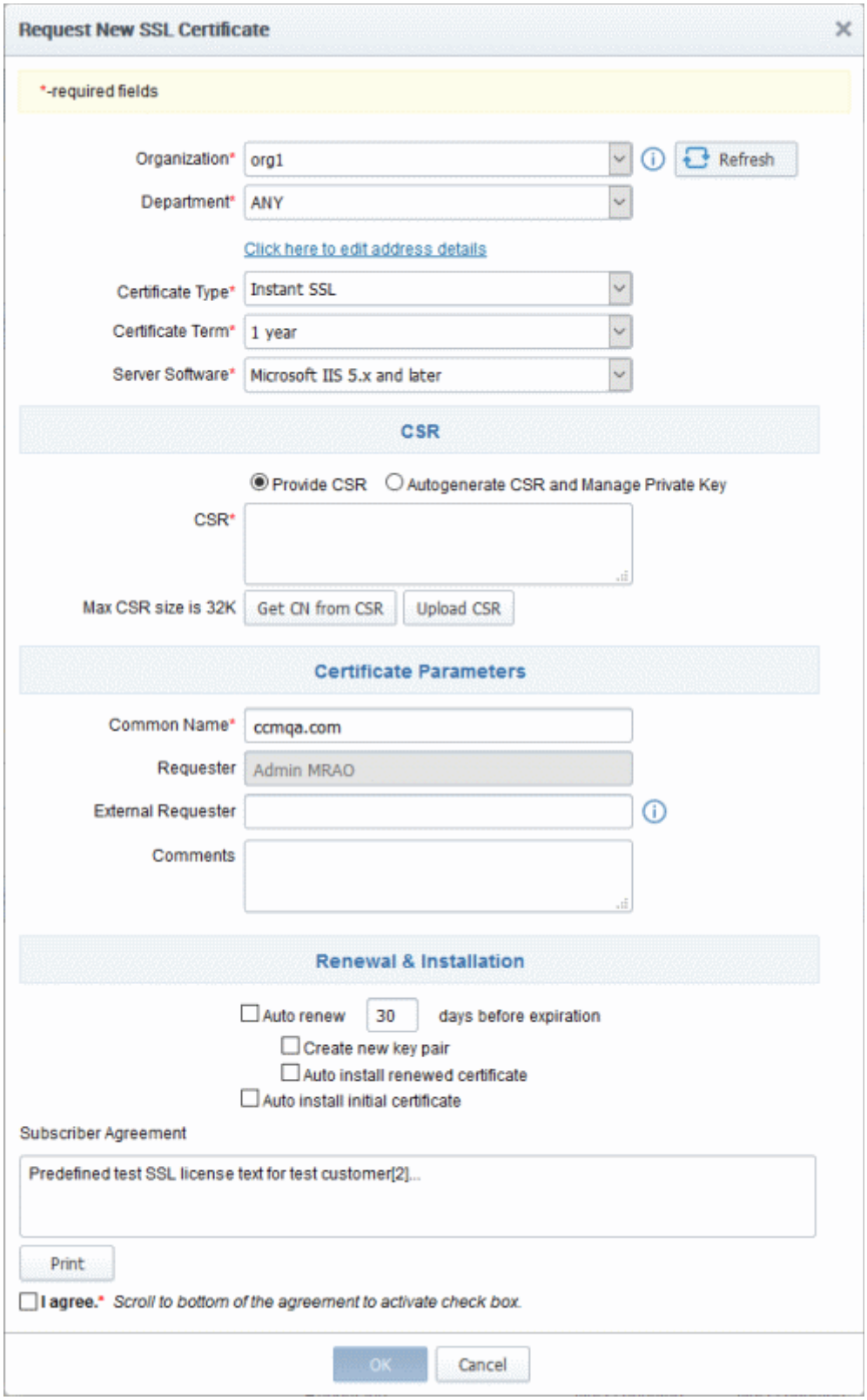
Method 2 - CM Controller Mode

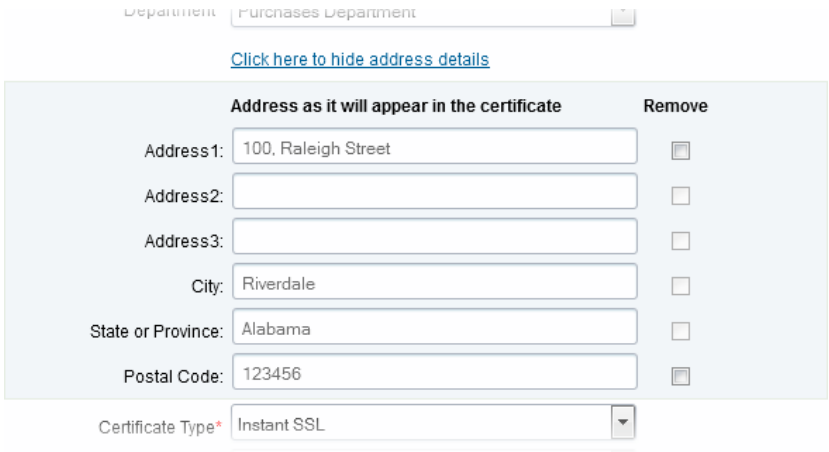
Administrators can request and install new certificates for domains hosted on different web servers from the 'Certificate Management - SSL Certificates' area. 'CM Controller Mode' requires an agent to be installed on each web server upon which the certificates are to be auto-installed/renewed.

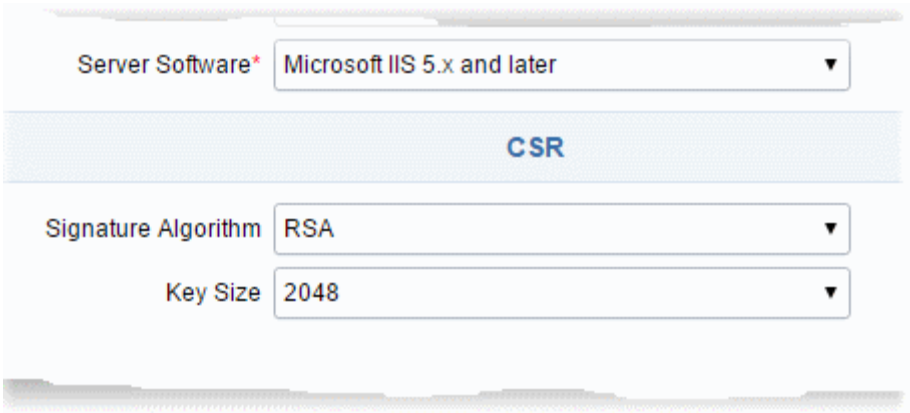
To enroll a certificate for auto-installation

- 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*
org1
Refresh
Department*
ANY
Click here to edit address details
Certificate Type*
Instant SSL
Certificate Term*
1 year
Server Software*
Microsoft IIS 5.x and later
CSR
Provide CSR
Autogenerate CSR and Manage Private Key
CSR*
Max CSR size is 32K
Get CN from CSR
Upload CSR
Certificate Parameters
Common Name*
ccmqa.com
Requester
Admin MRAO
External Requester
Comments
Renewal & Installation
Auto renew
30
days before expiration
Create new key pair
Auto install renewed certificate
Auto install initial certificate
Subscriber Agreement
Predefined test SSL license text for test customer[2]...
Print
I agree.*
Scroll to bottom of the agreement to activate check box.
OK
Cancel

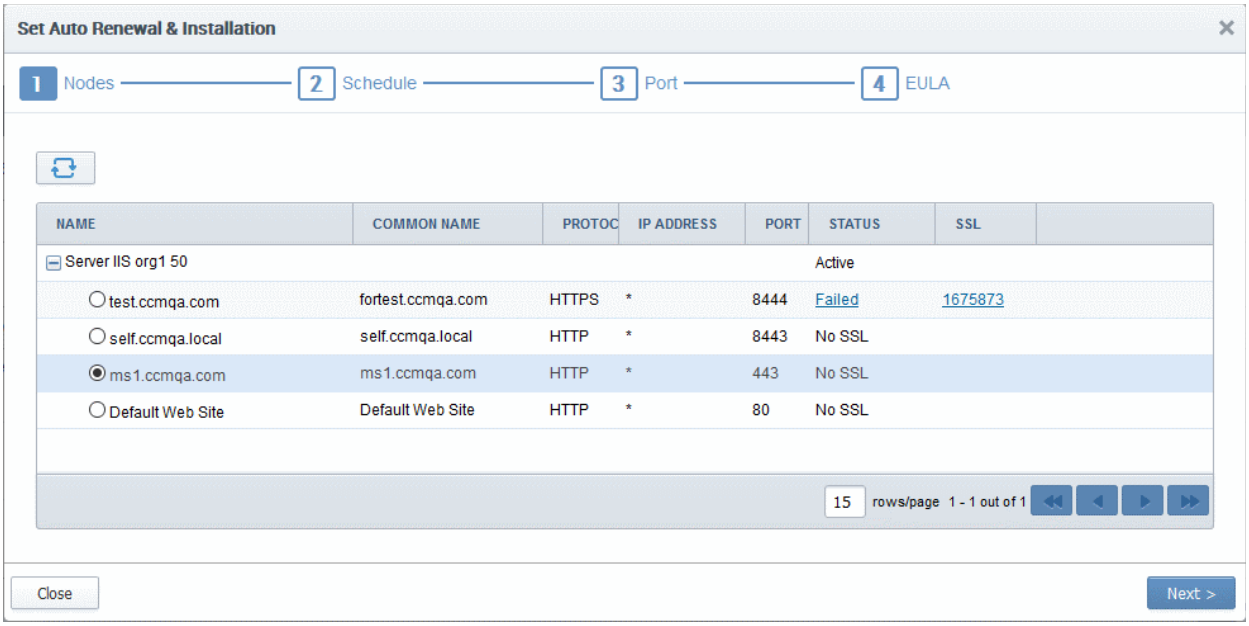
Form Element	Type	Description
Organization (***required***)	*Drop-down list*	Choose the Organization that the SSL certificate will belong to.
Department (***required***)	*Drop-down list*	Choose the Department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'.
Click here to edit address details	*Text Fields*	Clicking this link will expand the address fields.  The address fields are auto-populated from the details of the Organization or Department on whose behalf this certificate request is being made. These fields cannot be modified but, in the case of OV level certificates, the administrator can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields. The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted". For EV level certificates, it is mandatory to include and display address details of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down.
Certificate Type (***required***)	*Drop-down list*	Choose the certificate type that you wish to add for auto-installation. **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.
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: • 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. Once you choose 'Auto install initial certificate' under 'Renewal & Installation' in this form, these fields will disappear. 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'. 
CSR (***required***)		
Get CN from CSR (***optional***)		
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 (***optional***)	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 (***required***)	Control	You must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox.

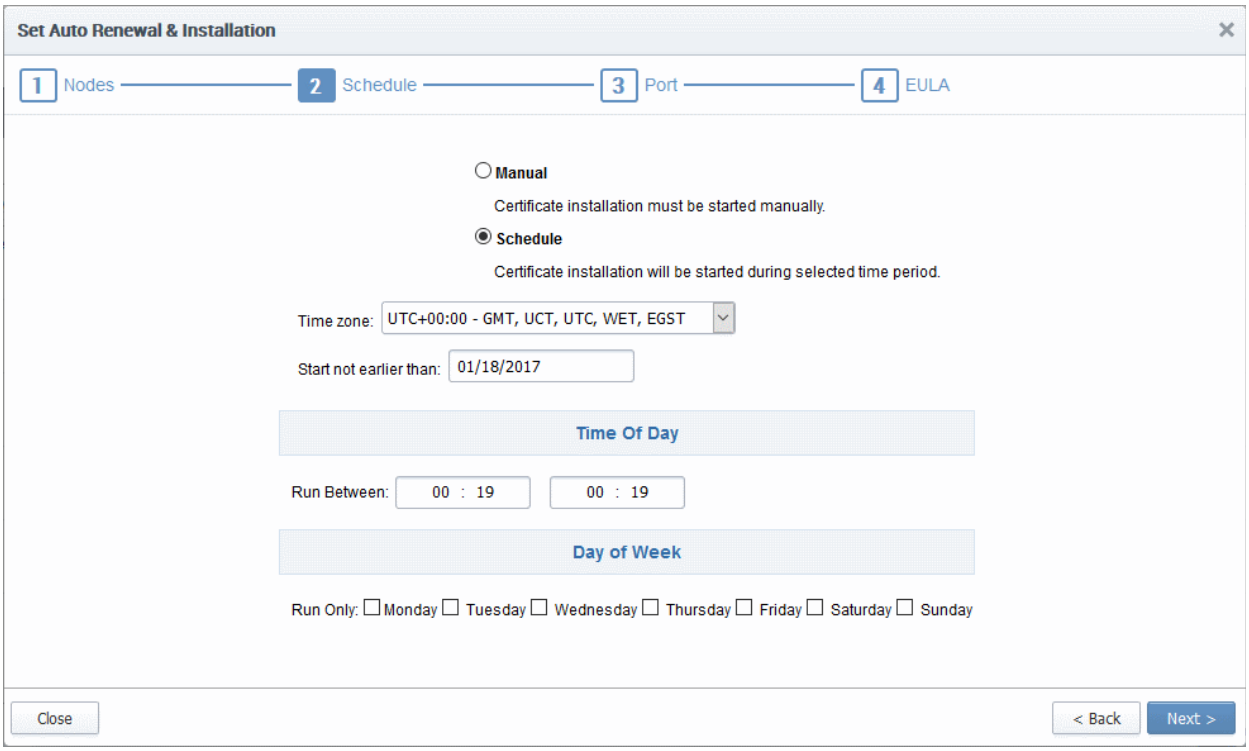
- Click 'OK' to submit the application

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.



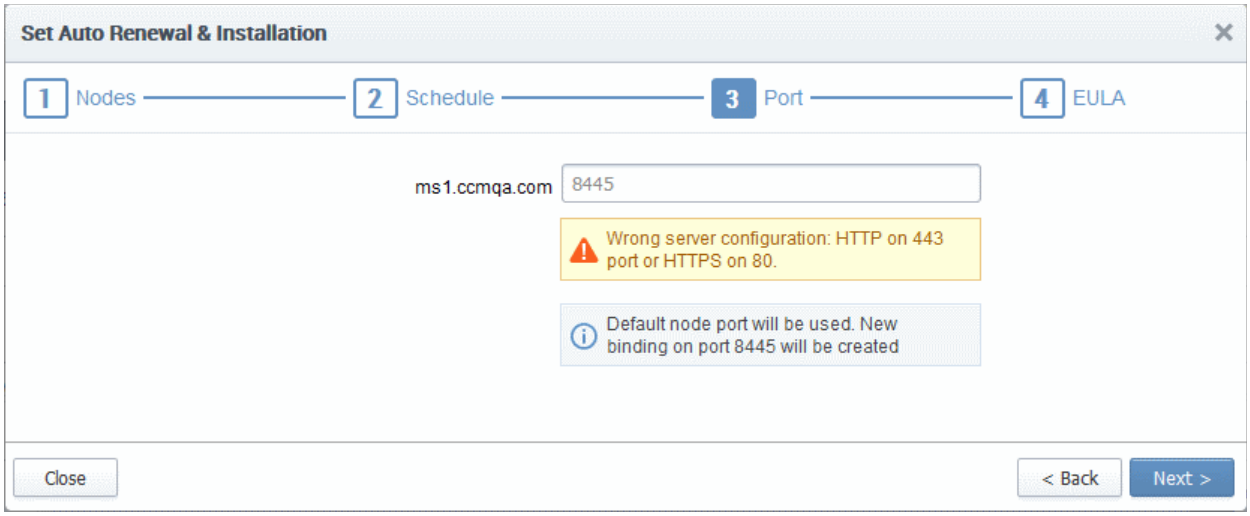
- Select the domain on which you wish to install a certificate and click Next.

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.



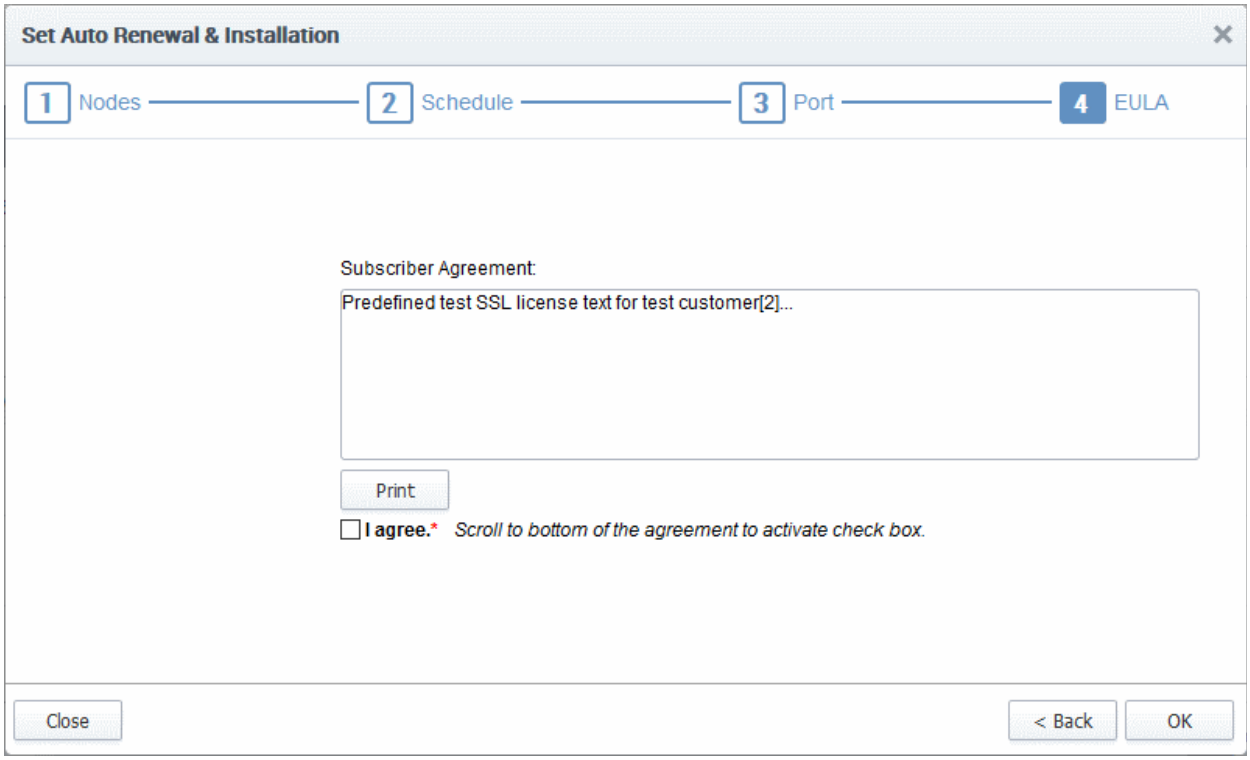
- If you want to manually install the certificate from the InCommon CM interface, select 'Manual'
- If you want to install the certificate at a scheduled time, select 'Schedule' then select your time zone and a 'not earlier than' time. The controller will generate a CSR and submit it to InCommon CA the 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.



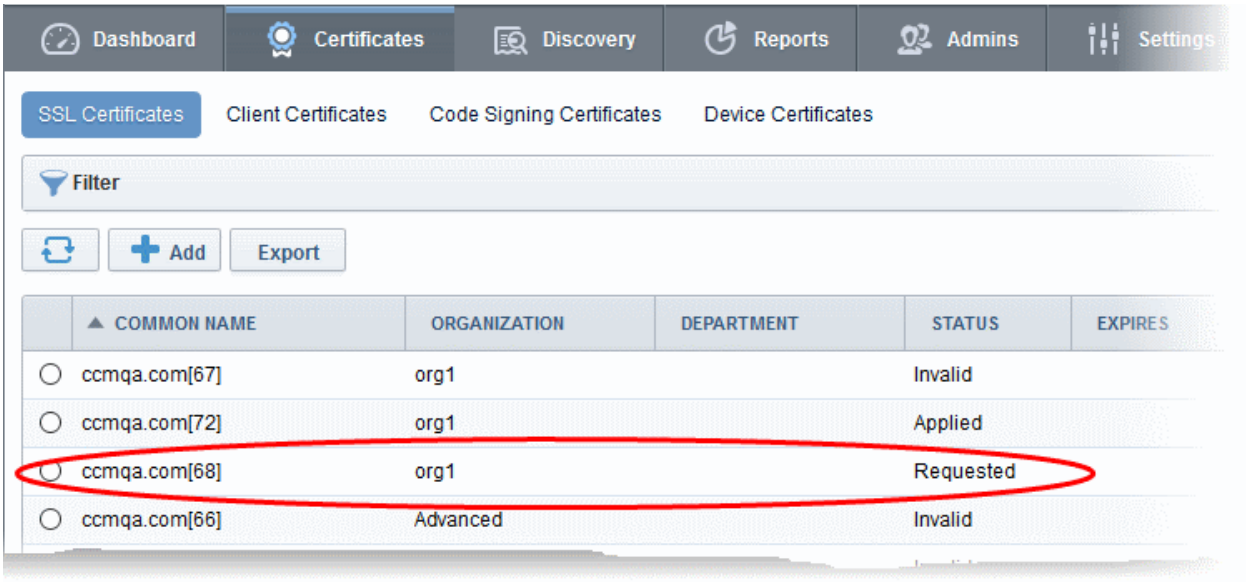
- Specify the HTTPS port for installing the certificate, (***Default = 9443***)

- Click 'Next'. The EULA interface will open.

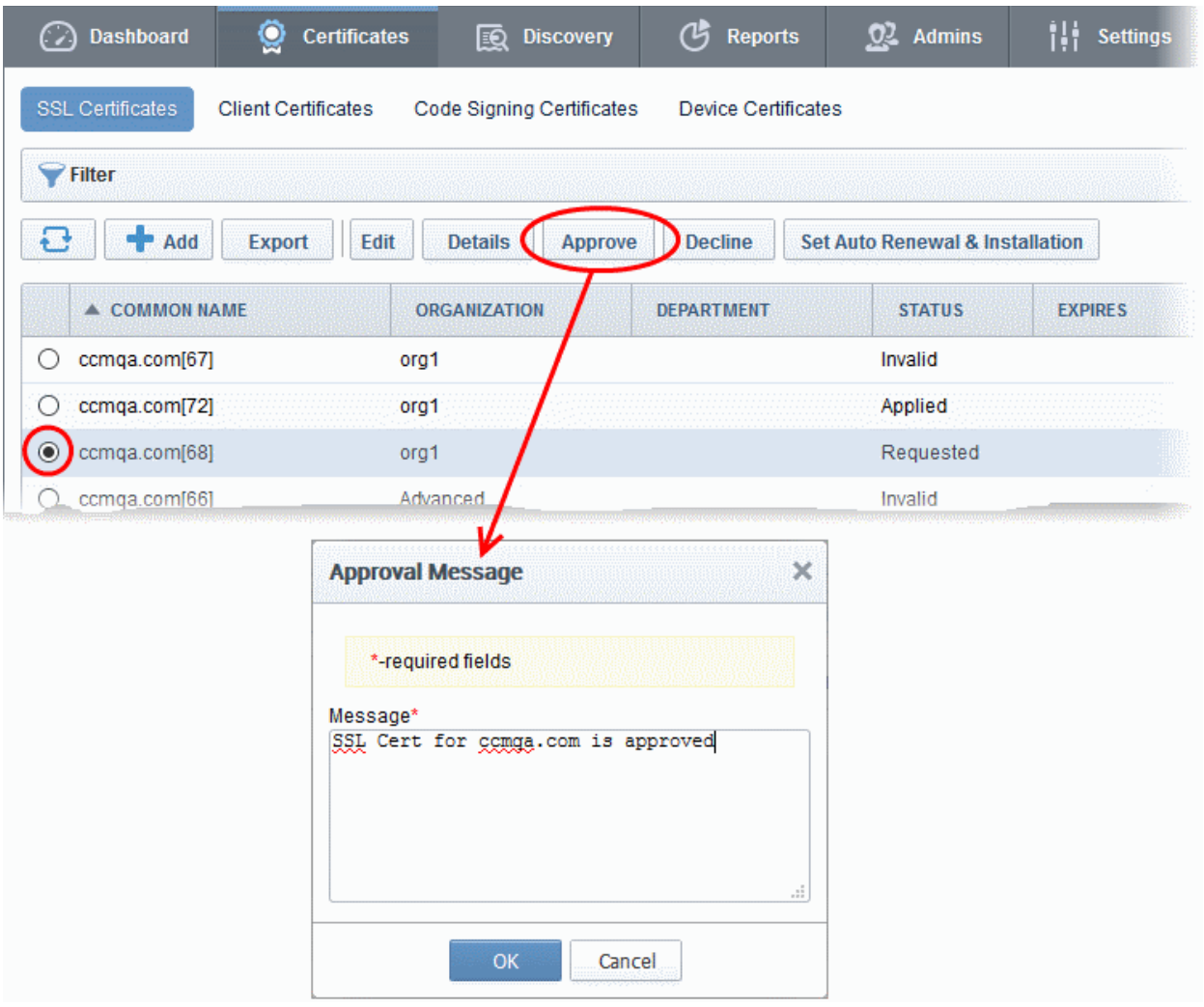


- Read the EULA fully and accept it by selecting the 'I Agree' checkbox.
- Click 'OK' to save your application.

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

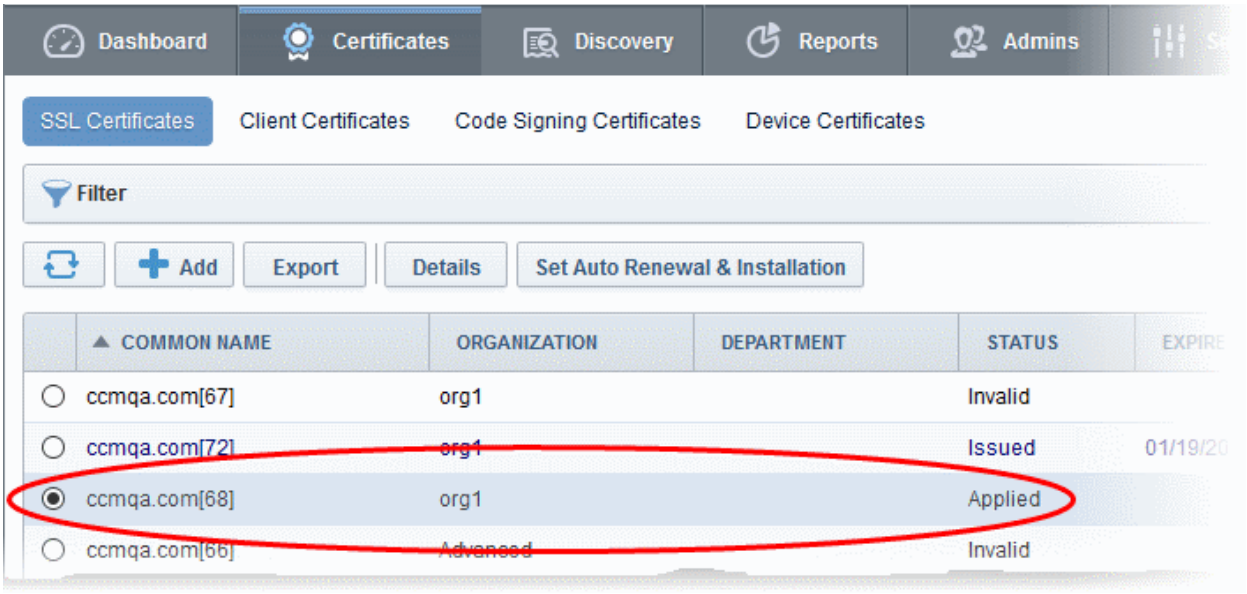


- The CSR for the requested certificate will be generated automatically. After the CSR is created, the approve button will appear at the top when you select the certificate in the list.

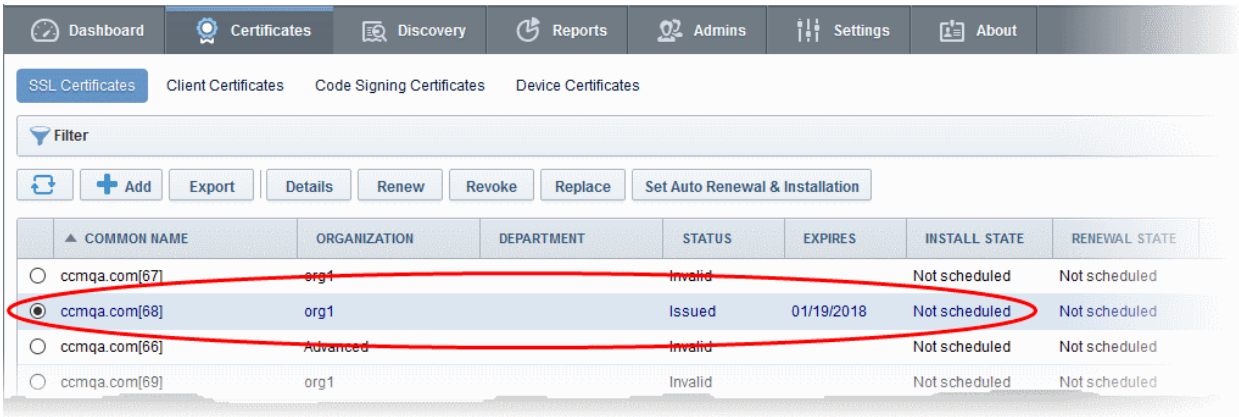


- Click the 'Approve' button to approve the request, enter the approval message in the 'Approval Message' dialog and click 'OK'.

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



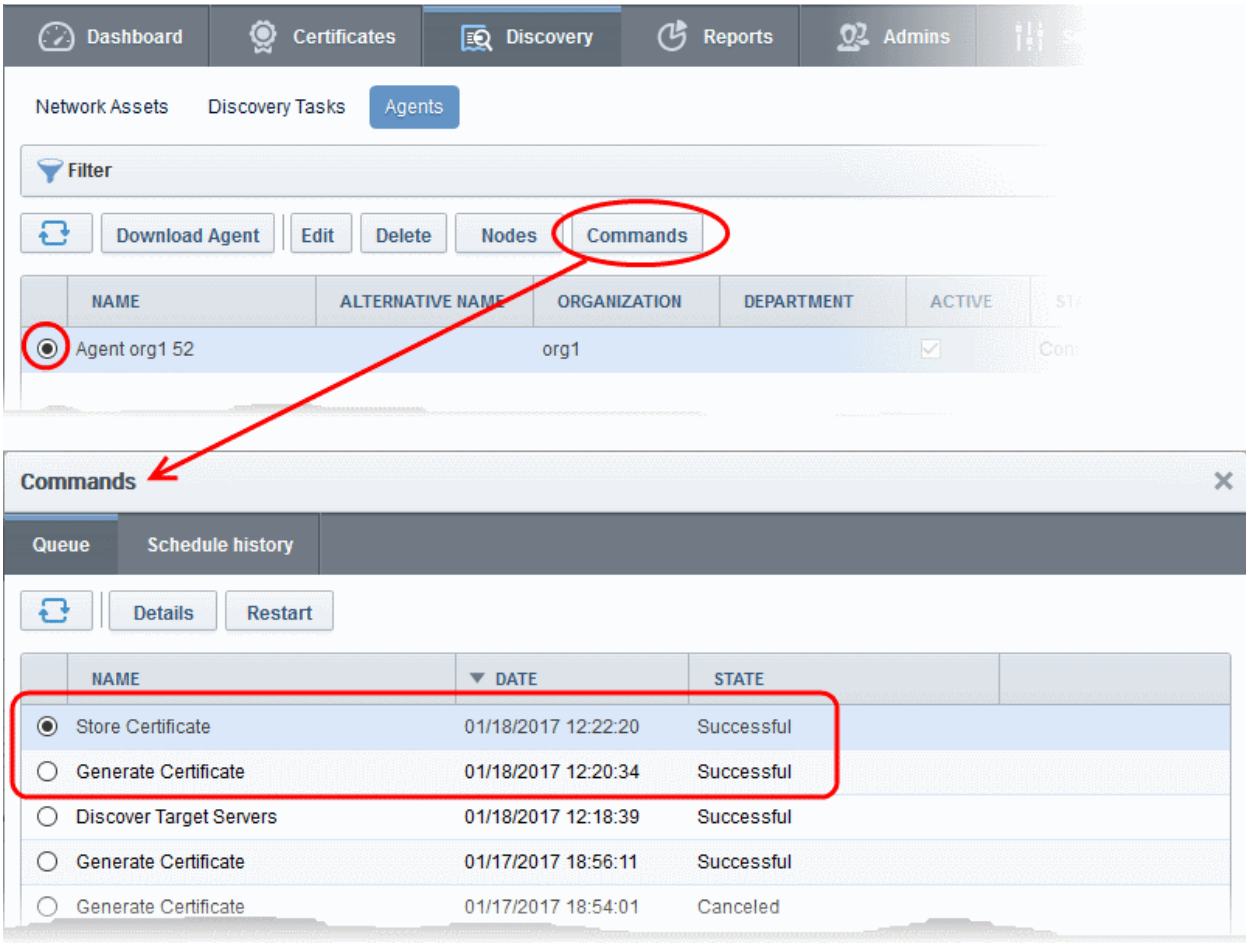
The controller will track the order number then collect and store the certificate once it is issued. The certificate status will change to 'Issued'.



To check whether the controller has stored the certificate:

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

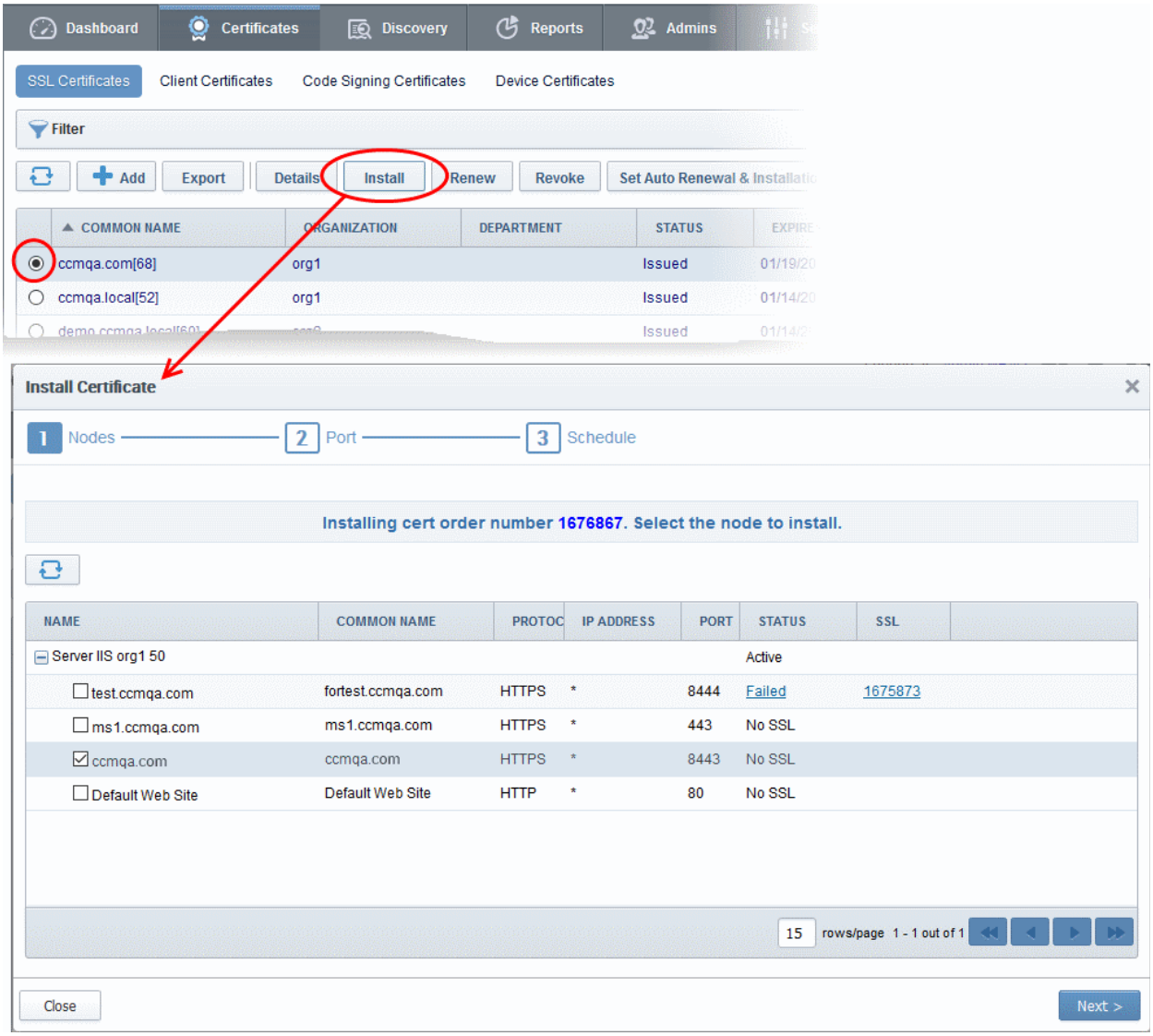
You will see successful execution of 'Store Certificate' command.



The 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

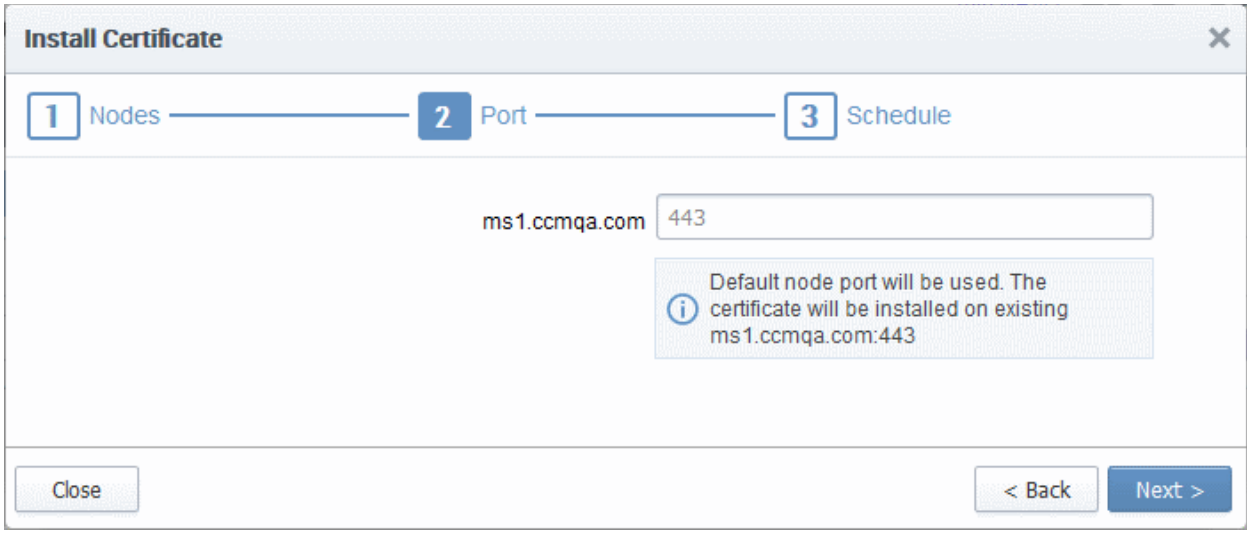
- Select the certificate from the 'Certificates' > 'SSL Certificates' interface and click 'Install'



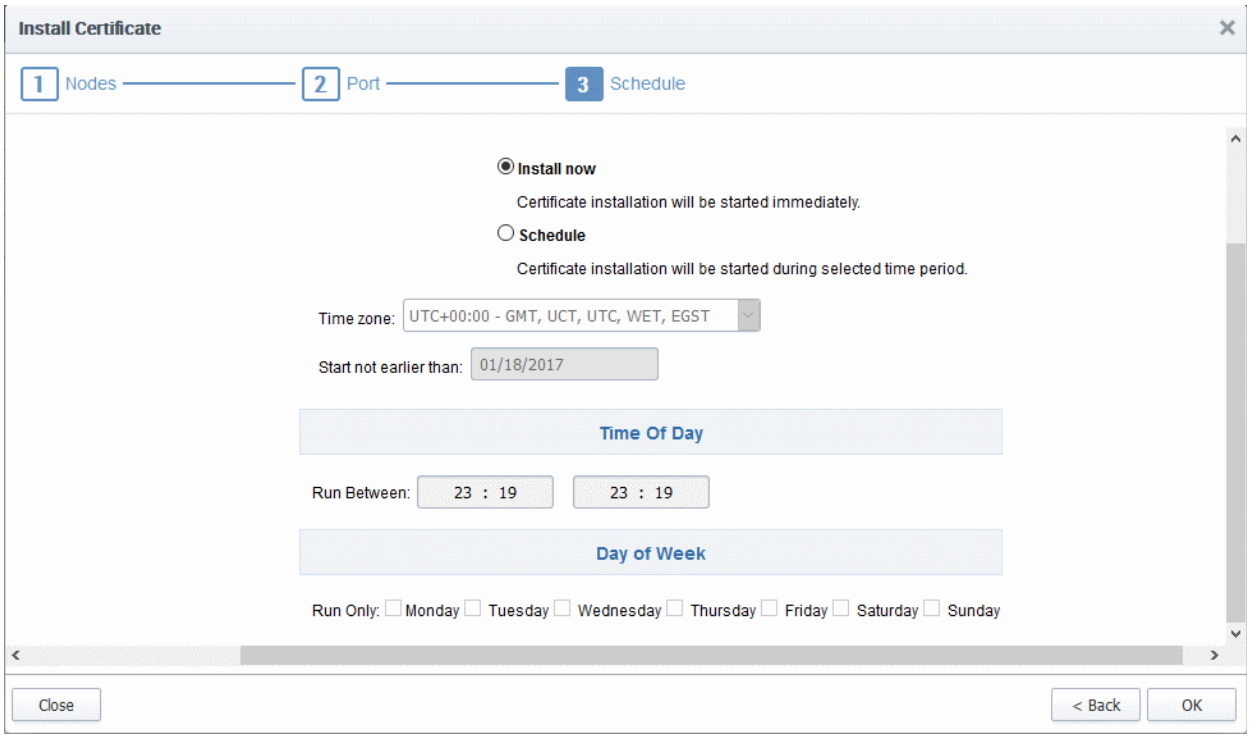
The 'Install Certificate' wizard will start with the 'Nodes' interface. The node upon which the certificate is to be installed is pre-selected.

- 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.

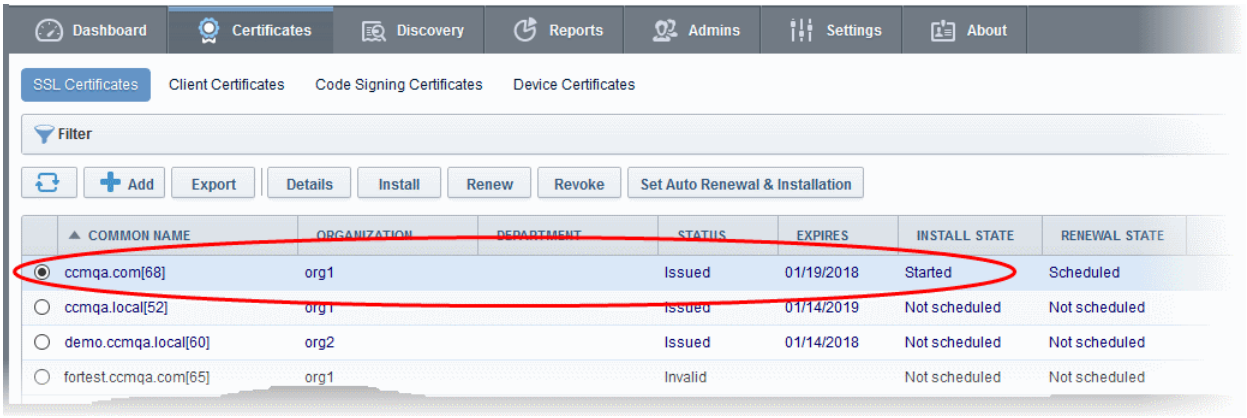


- Specify the port and click 'Next'. The 'Schedule' interface will open.



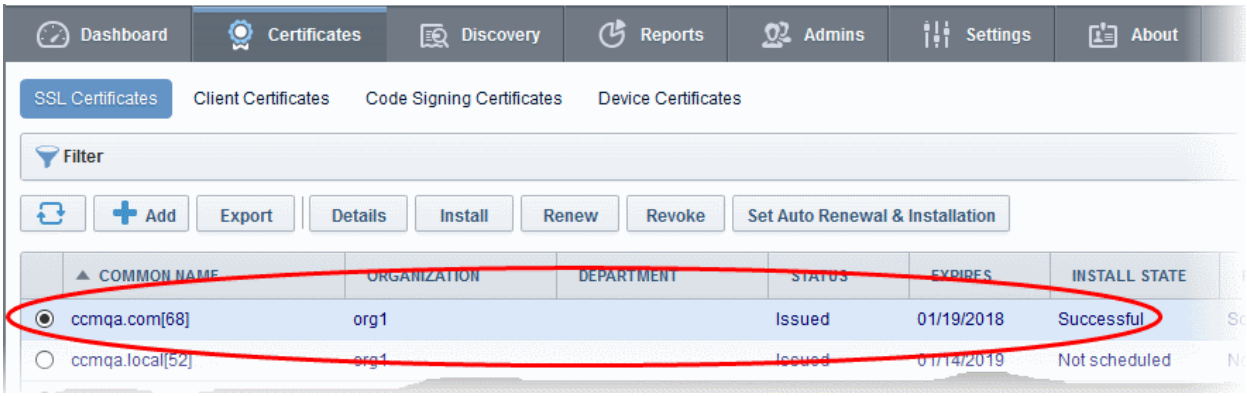
  - If you want to instantly install the certificate, select 'Install now'
  - If you want to install the certificate at a later time, select 'Schedule', then select your time zone, and set a 'not earlier than' date. The certificate will be installed on the server when the controller polls InCommon CM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

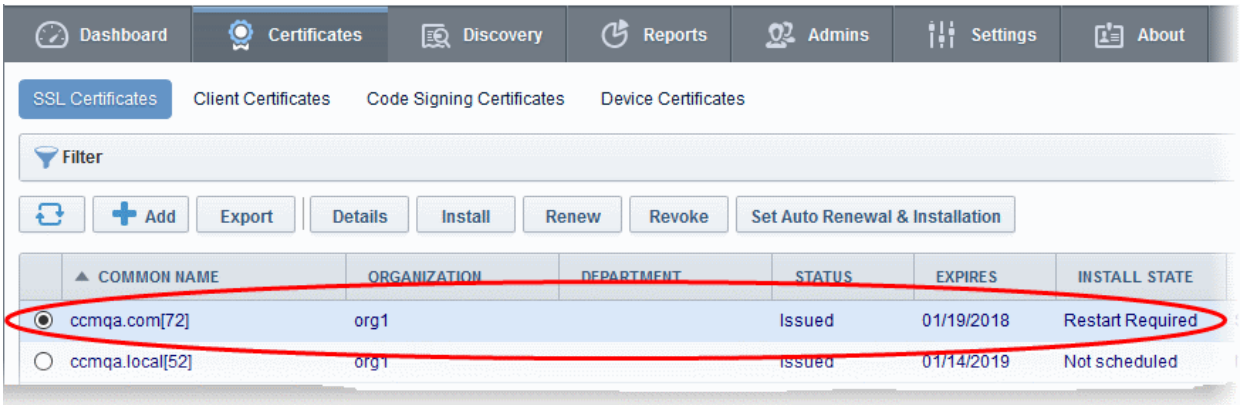


When installation is complete:

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

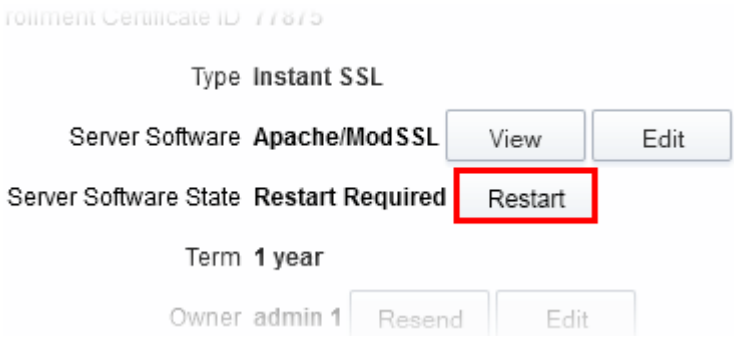


- Apache servers - The certificate will become active after the server is restarted. The install state will change to 'Restart Required'.



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

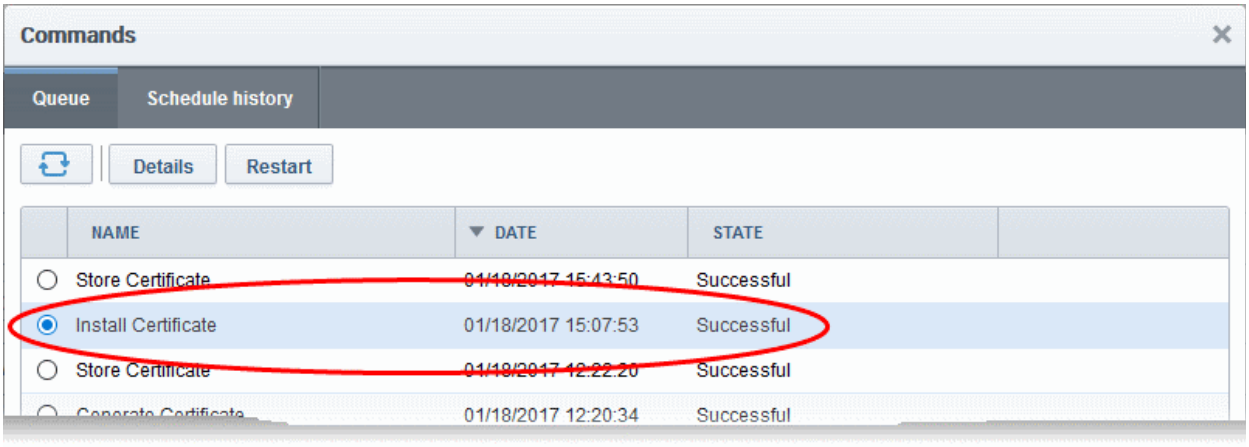
- Select the certificate and click the 'Details' button at the top. The 'Certificate Details' dialog will be displayed.
- Click Restart beside the Server Software State field in the 'Details' dialog



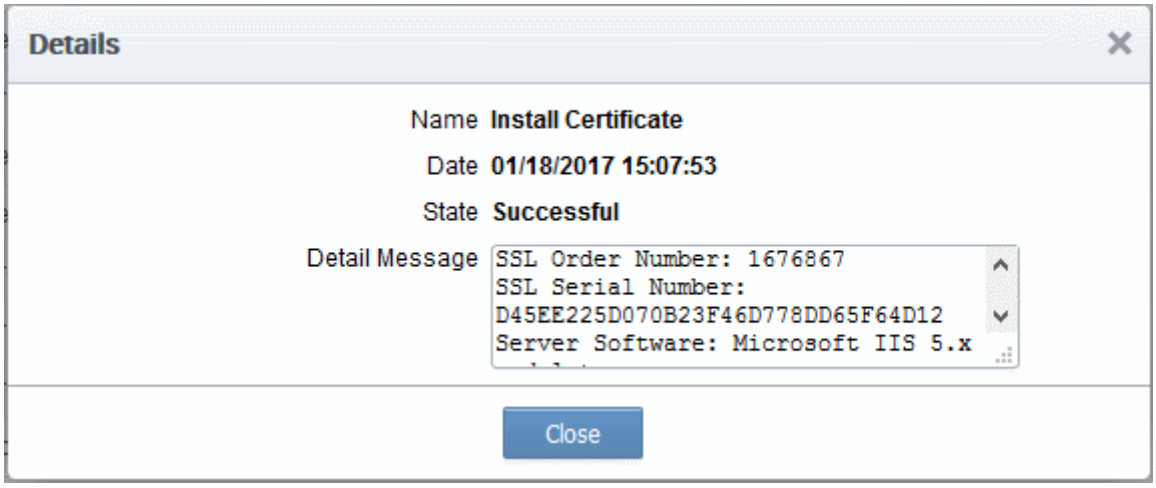
After restarting the server, the certificate will activated and the 'Install State' will change to 'Successful'.

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

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



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



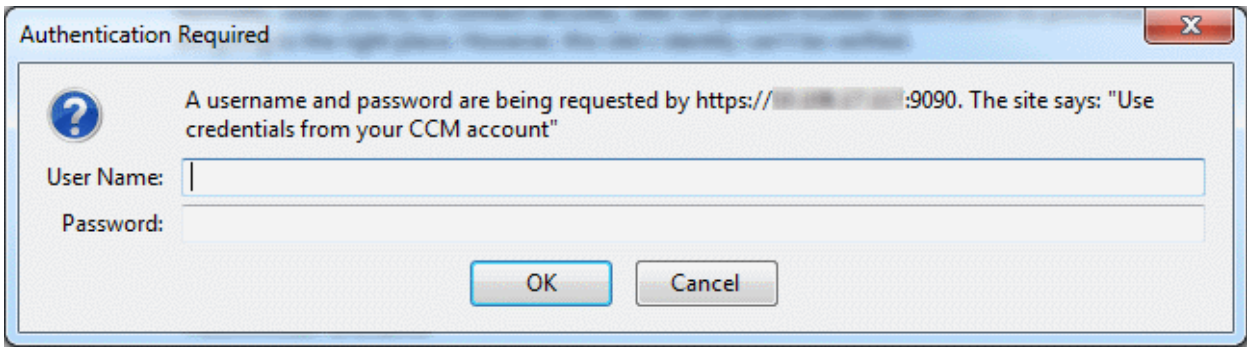
Configuring the Certificate Controller Agent through Web Interface

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

To access the Agent configuration web interface

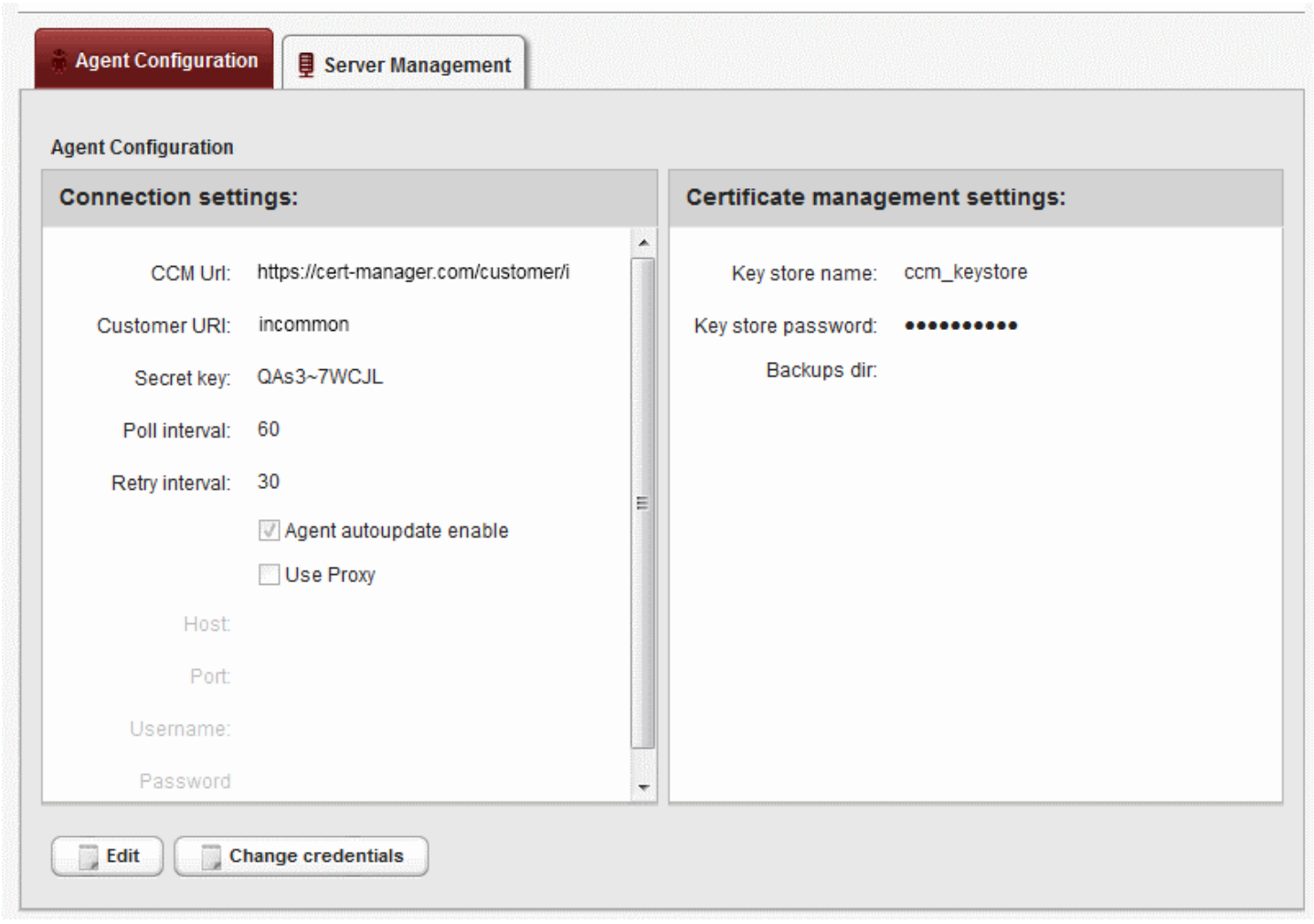
- Type http://<IP Address/host name of the server on which the agent is installed>:9090 in the address of your browser.

The login dialog will appear:



- Enter your InCommon CM username and password.

The Agent configuration interface will open.

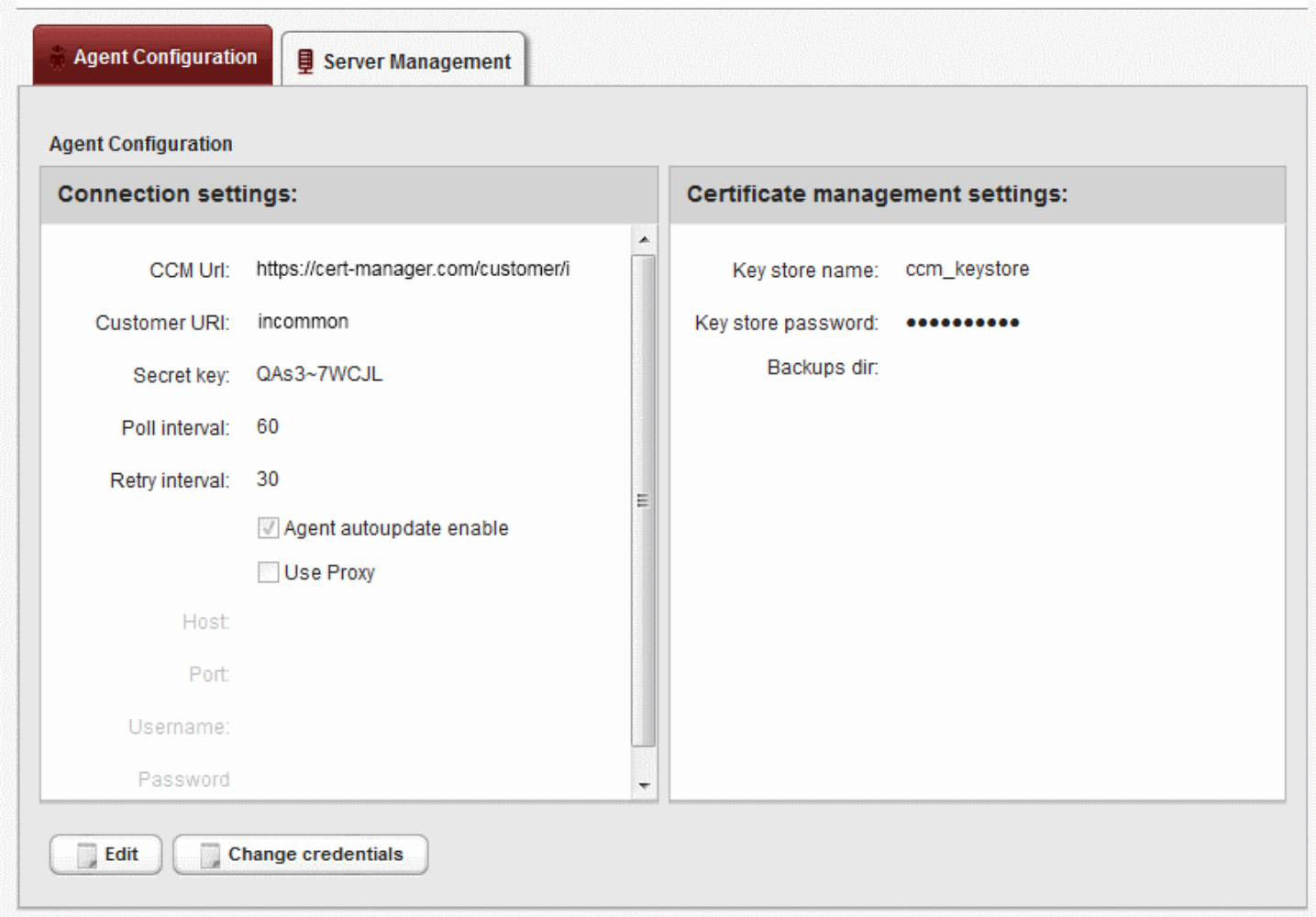


It has two tabs:

- Agent Configuration
- Server Management

Agent Configuration

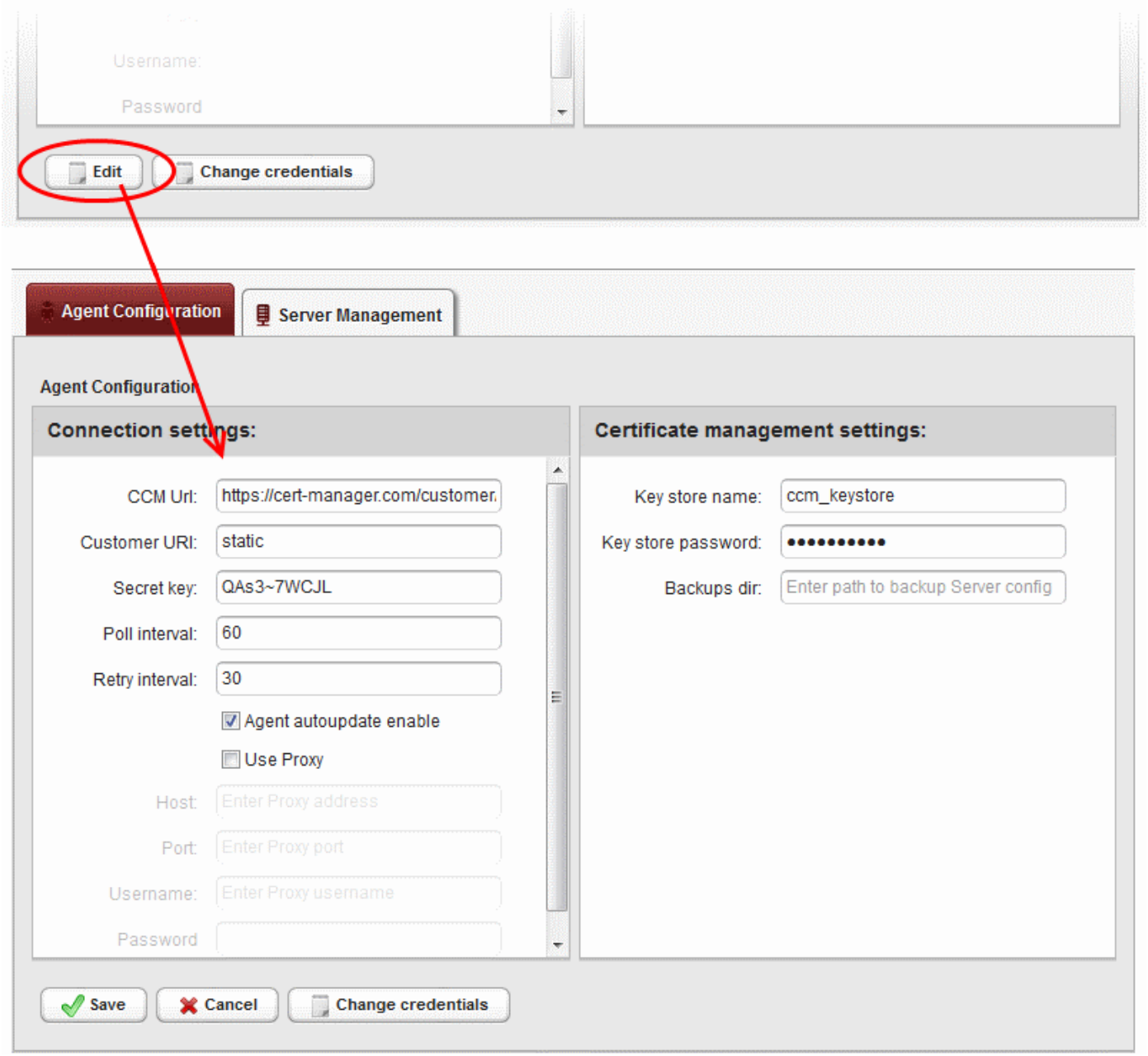
The Agent Configuration tab displays the connection management settings and certificate management settings of the agent and enables the administrator to edit them, if required.



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

Poll Interval	*Text field*	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	*Text field*	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	*Checkbox*	Indicates whether the agent is enabled for auto-update. The checkbox enables the administrator to switch the auto-update on/off in edit mode.
Use Proxy	*Checkbox*	Indicates whether the agent is configured to use a proxy server. The checkbox and the text fields below it enable the Administrator to instruct the agent to use proxy server and to specify the proxy server details, if required.
Host	*Text field*	Displays the IP/Host name of the proxy server and enables the Administrator to specify it in edit mode
Port	*Text field*	Displays the port of the proxy server for the agent to connect and enables the Administrator to specify it in edit mode
Username	*Text field*	Displays the username of the administrator account to login to the proxy server and enables the Administrator to specify it in edit mode
Password	*Text field*	Displays the password of the administrator account to login to the proxy server and enables the Administrator to specify it in edit mode
Certificate Management Settings		
Key store name	*Text field*	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	*Text field*	The password to access the CM keystore file. The Administrator can edit it in the edit mode
Backup dir	*Text field*	Displays the folder path for backup of keystore file. The Administrator can edit it in the edit mode.

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



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

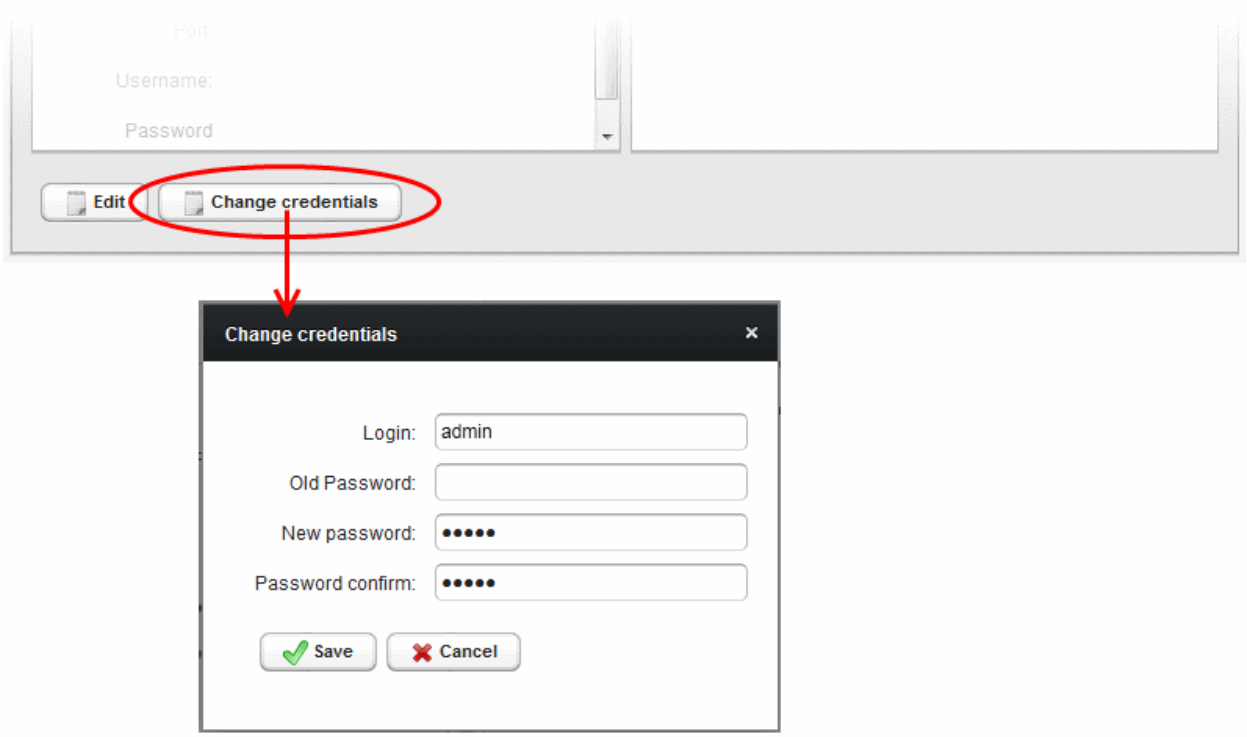
Changing Login Credentials for the Agents Configuration Console

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.

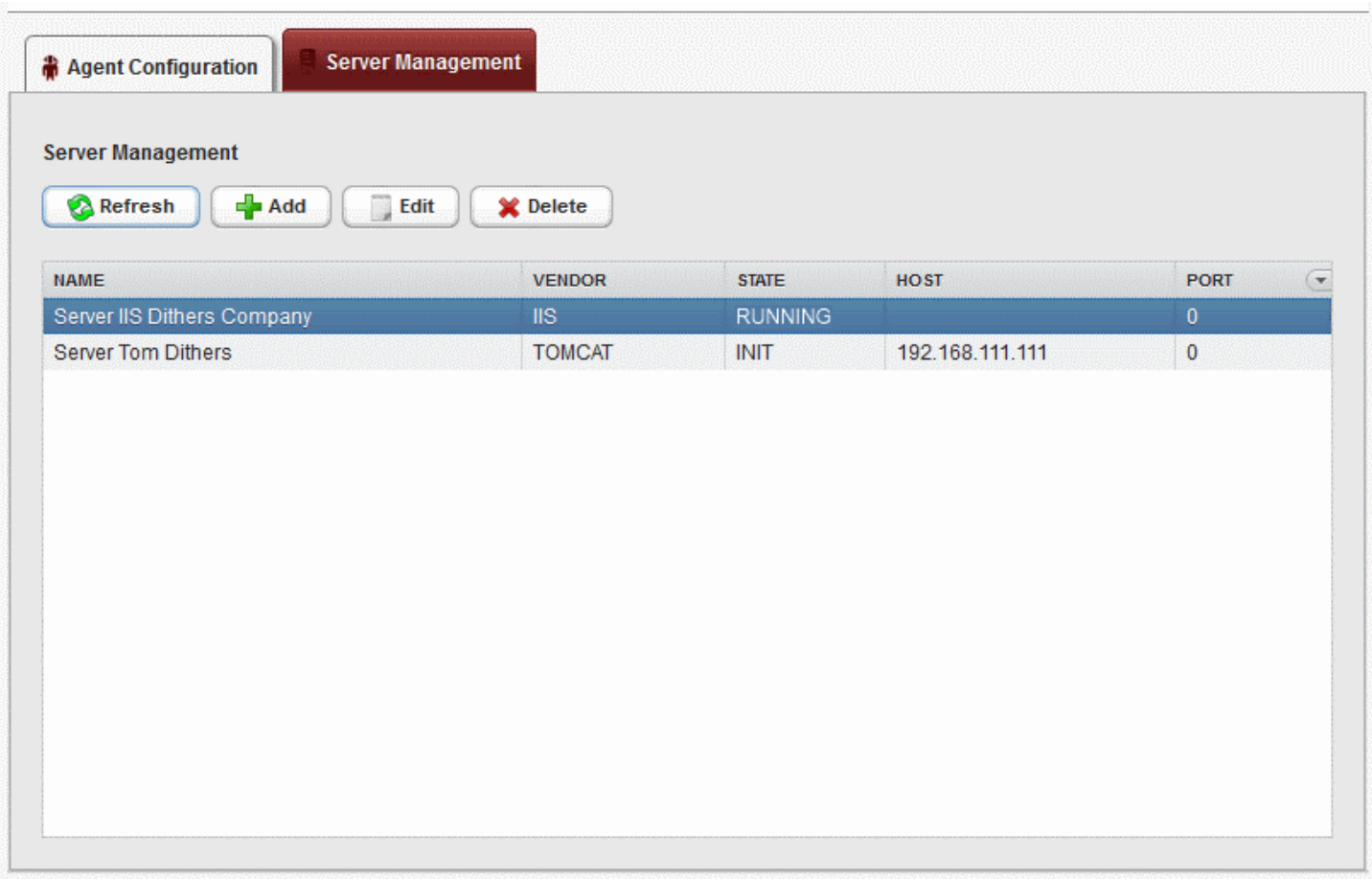


- To change your username, directly edit the Login field
- Enter your existing password in the 'Old Password' field
- Enter your new password in the New password field and reenter it for confirmation in the Password Confirmation field
- Click 'Save'

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

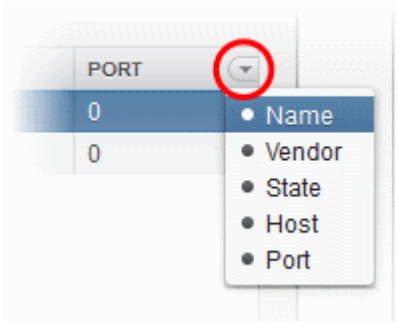
Server Management

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



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.

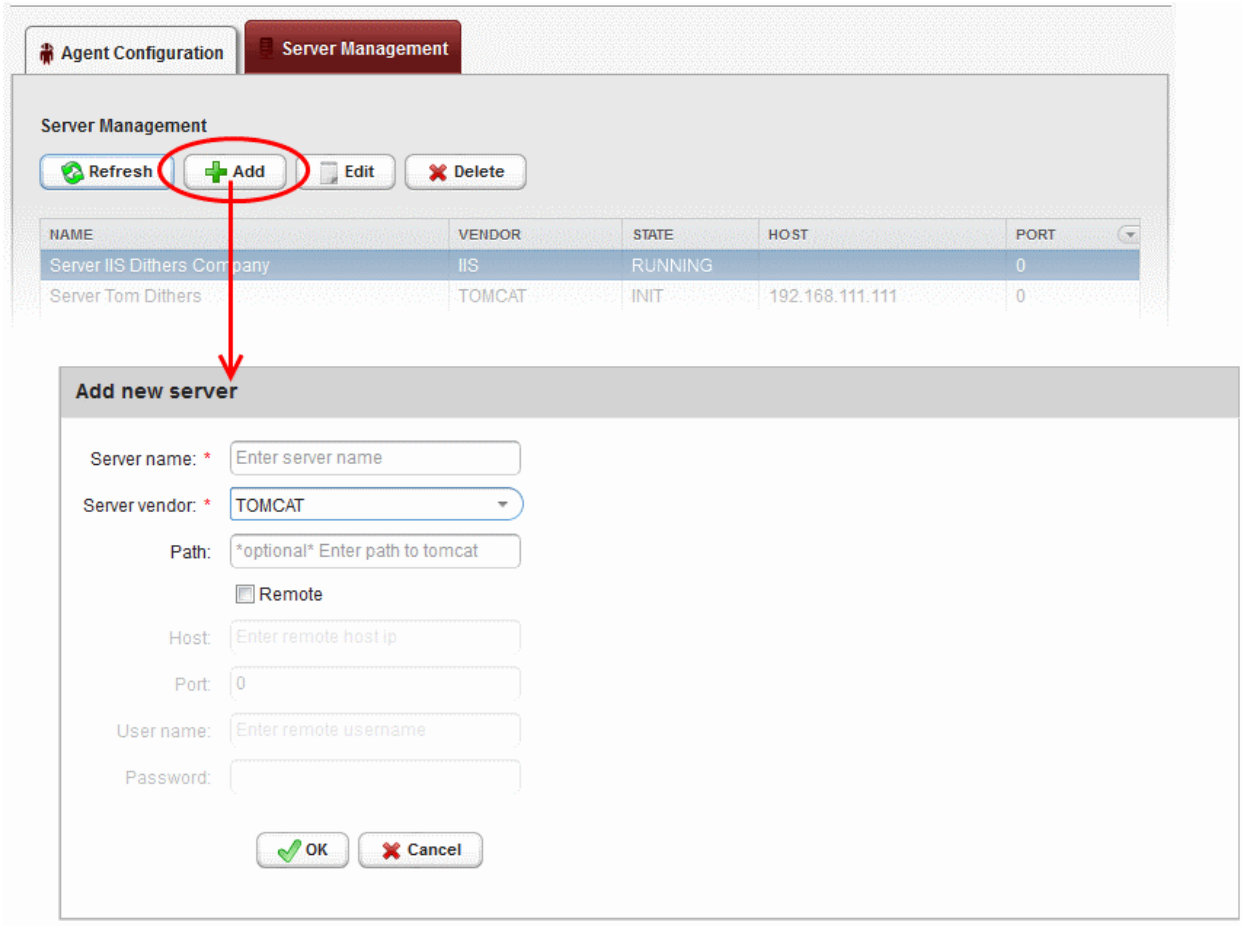
Column Display	Description
Name	Displays the name of the server.
Vendor	Displays the vendor of the server.
State	Indicates whether or not the server is initialized.
Host	Displays the IP address or the host name of the server for remote connection
Port	Displays the connection port of the server for remote 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 **Note**: The Server control buttons will appear only on selecting a server.		
	Edit	Enables administrators to modify the Server configuration settings.
	Delete	Removes the Server.

To add a server

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



Add new server - Table of Parameters		
Field Name	**Type**	**Description**
Server name	*String*	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.

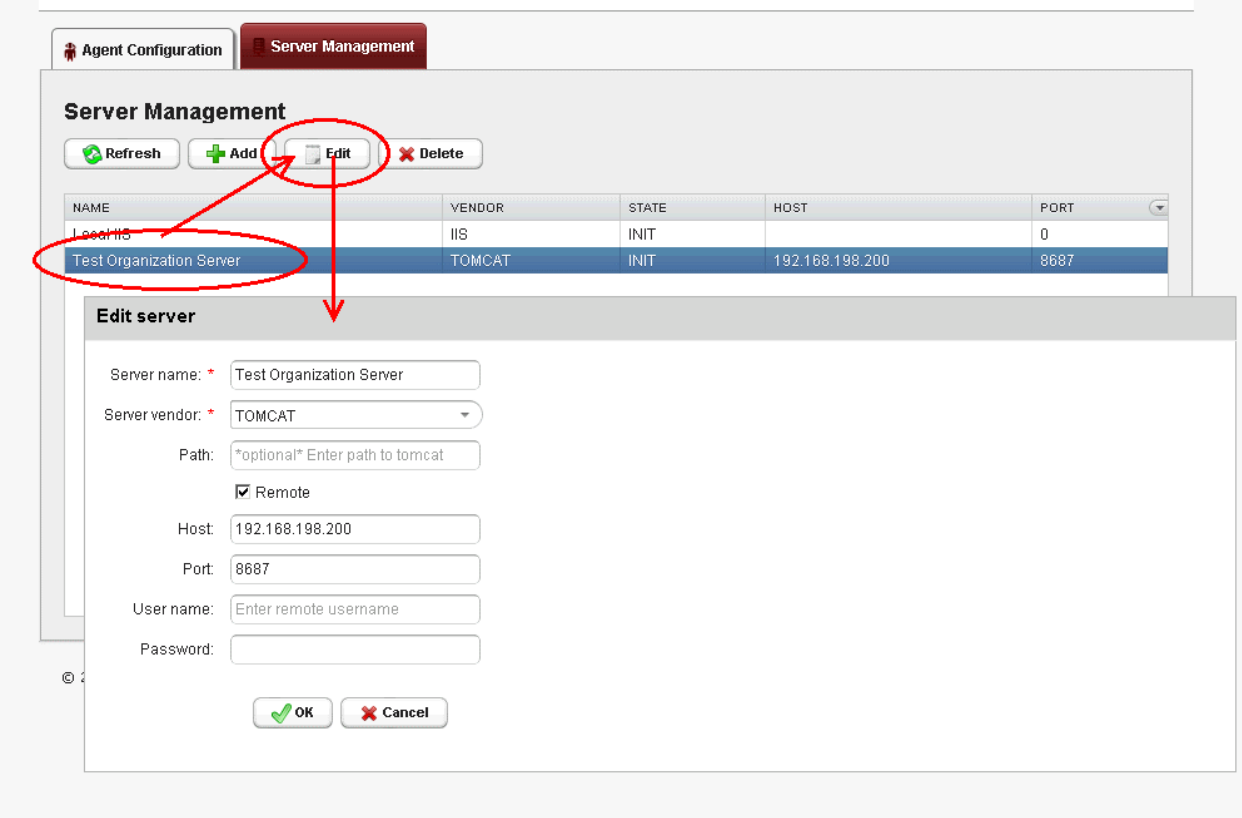
Add new server - Table of Parameters		
		Note: This field will be enabled only if 'Remote' is selected.
Port	*String*	Specify the connection port of the server for remote connection. **Note**: This field will be enabled only for remote 'Tomcat' server.
User Name	*String*	Enter the username of the administrator for loggin-into the server. **Note**: This field will be enabled only if 'Remote' is selected.
Password	*String*	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.