COMODO
Creating Trust Online®

Comodo
Certificate Manager

Version 5.5

Introduction to Auto-Installer

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

Certificate Manager - Introduction to Auto-Installer

Comodo continuously updates its products and services with innovative technologies to provide the best to its partners and customers alike. This document is intended to introduce partners to the new Auto-Installer feature in Comodo **Certificate Manager** (CCM).

In brief:

- The new feature allows MRAO and RAO admins to automate the remote installation of any SSL certificate on to Apache Httpd, Apache Tomcat and IIS web-servers (more web-server types coming soon).
- The feature is enabled on a per-certificate basis by clicking the 'Add For Auto Install' button in the 'Certificate Management - SSL Certificates' area.
- There are two modes of implementation:

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

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

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

- Apache Tomcat
- IIS 5.0 to 8.0 (Server 2000 - 2008R2)

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

- If the admin chooses to install:
  - Windows IIS servers - the certificate will be activated immediately and the 'Server Software' state will be changed to 'Active' in CCM
  - Apache servers – the server will need to be restarted to finalize installation. The 'Server Software' state will be be changed to 'Restart Required' in CCM
- 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 CCM admin).

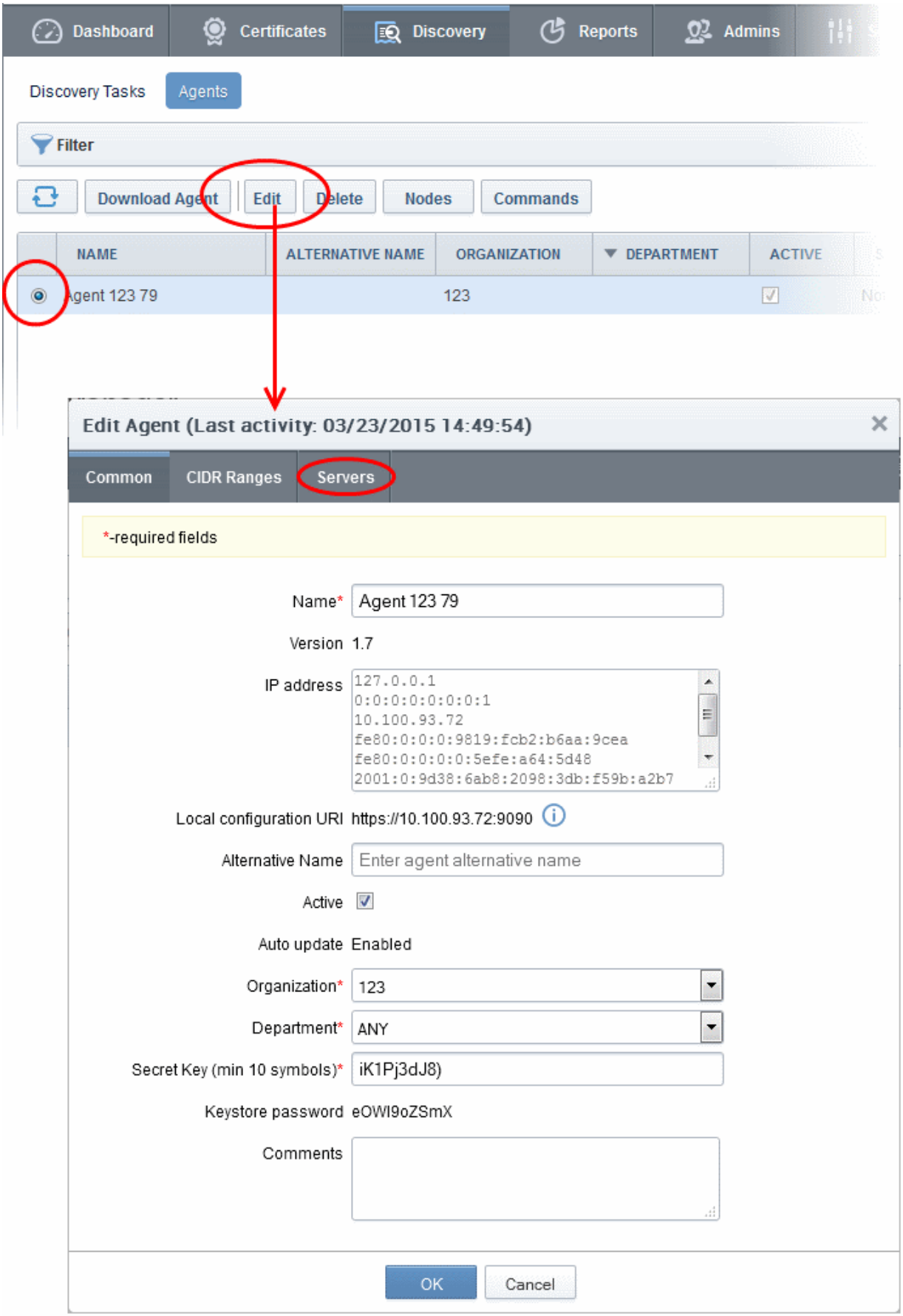
The remainder of this document is the portion of Administrator guide of Comodo Certificate Manager, that explains the process of application through installation of an SSL certificate using the new Auto-Installer feature.

Method 1 - Enterprise Controller Mode

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

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

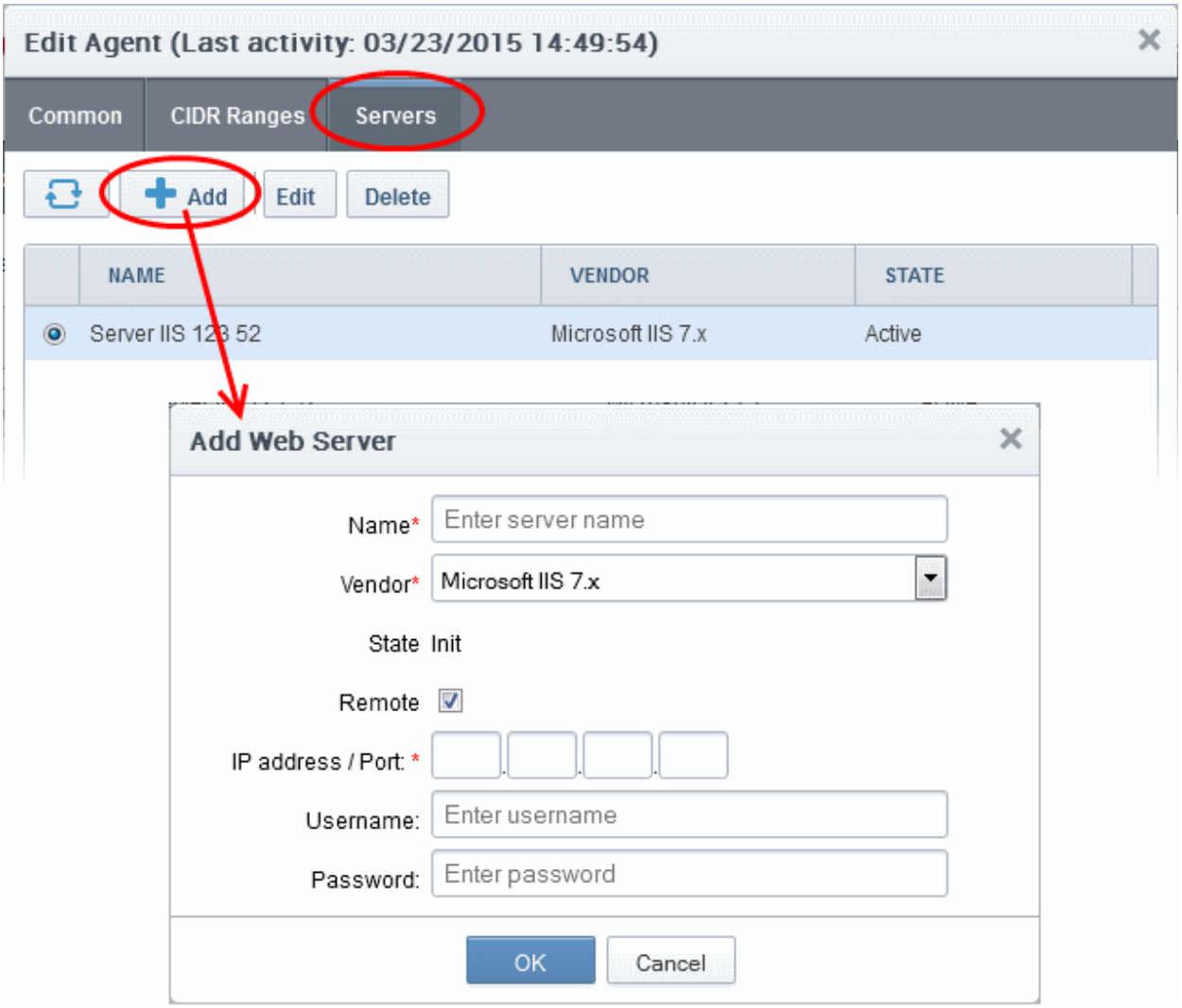
Note:The Certificate Controller software (also known as CD Extra Agent) should have been installed on the control server prior to the application for a certificate for a remote server. Refer to the section **5.1.2 Agents** in the Administrator Guide for more details on installing the controller and the section **Configuring the Certificate Controller Agent through Web Interface** for more details on configuring the controller to connect to Comodo CA through a proxy server (optional).



- Select the controller and click 'Edit' at the top to open the 'Edit Agent' dialog and choose the Servers tab 'Edit Agent' dialog .

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

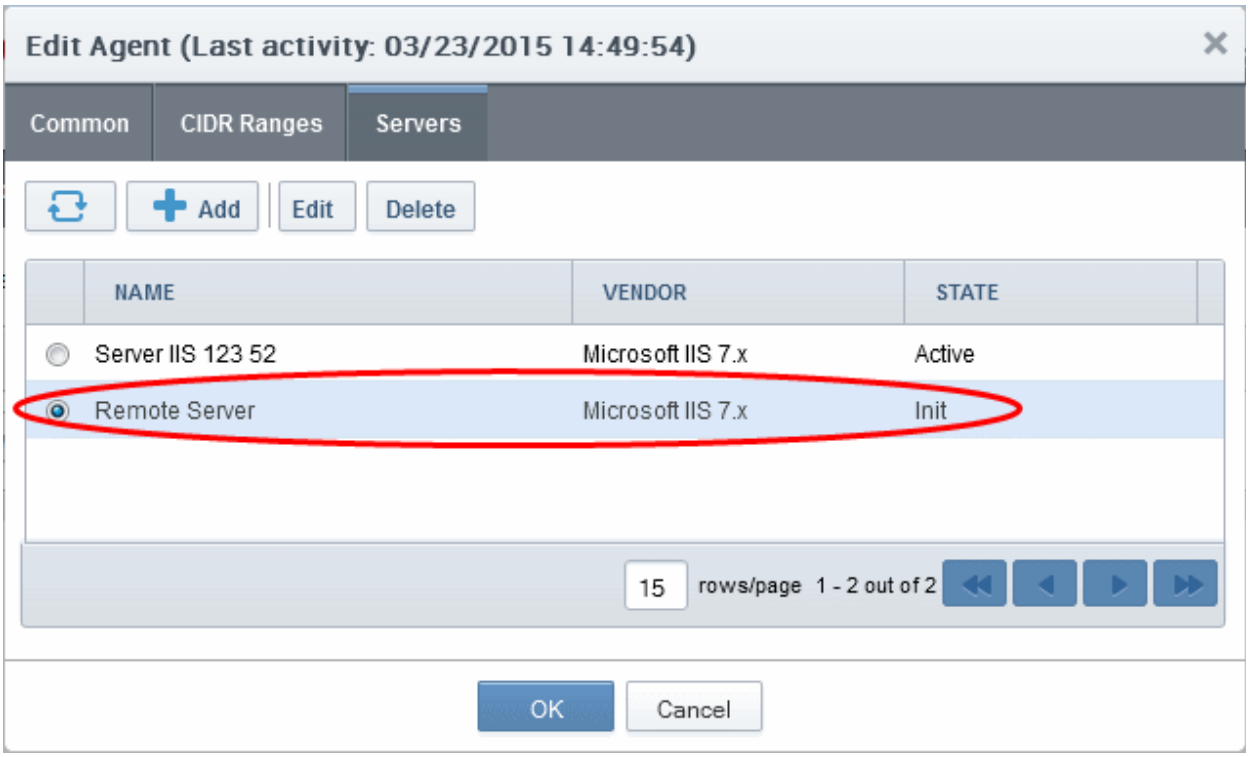
- Click 'Add' to associate a remote server to the controller. The 'Add Web Server' dialog will open.



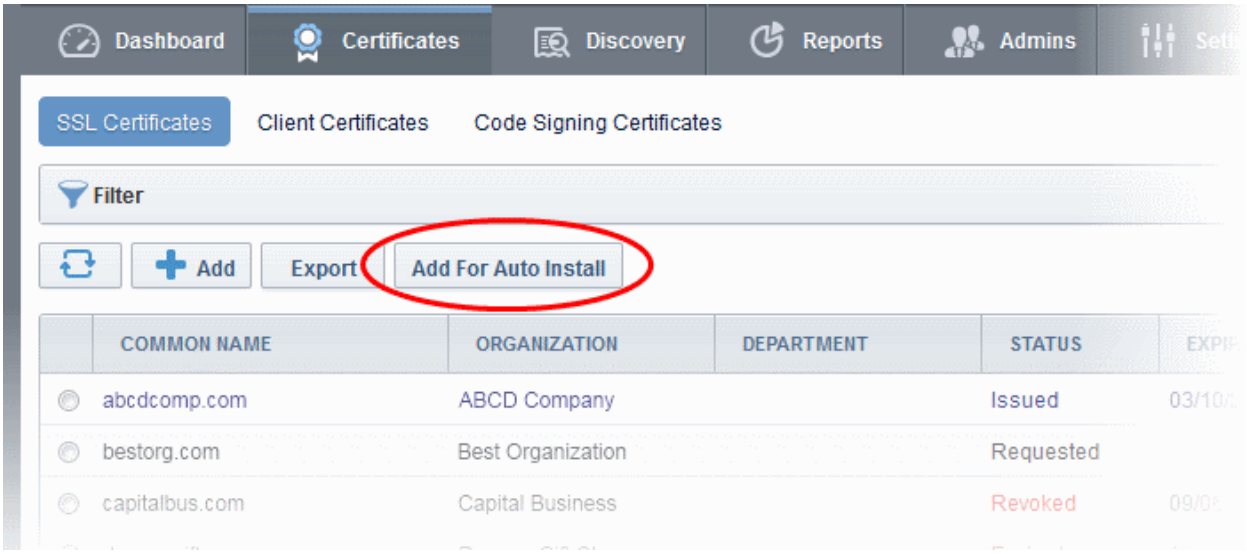
Add Web Server - Table of Parameters		
Field Name	**Type**	**Description**
Name	String	Enables the Administrator to enter the name of the server.
Vendor	Drop-down	Enables the Administrator to select the vendor of the server.
State		Indicates whether or not the server is initialized.
Path to web server	String	Enables the Administrator to specify the network path for the server. Required only for Apache 2.x and Apache Tomcat servers.
Remote	Checkbox	Enables the Administrator to specify whether the server is Remote or Local. While adding remote servers for agent-less automatic certificate installation, this checkbox should be selected.
IP Address / Port	String	Enables the Administrator to specify the IP address and connection port of the server for remote connection.

Add Web Server - Table of Parameters		
		Note: This field will be enabled only if 'Remote' is selected.
User Name	String	For IIS server - Enables the Administrator to specify the username of the administrator for logging-into the server. For Apache - Enables the Administrator to specify the private key file path to enable agent to access the server Note: This field will be enabled only if 'Remote' is selected.
Password	String	For IIS server - Enables the Administrator to specify the login password for the administrator account for logging into the server For Apache - Enables the Administrator to specify the passphrase of the private key file path Note: This field will be enabled only if 'Remote' is selected.

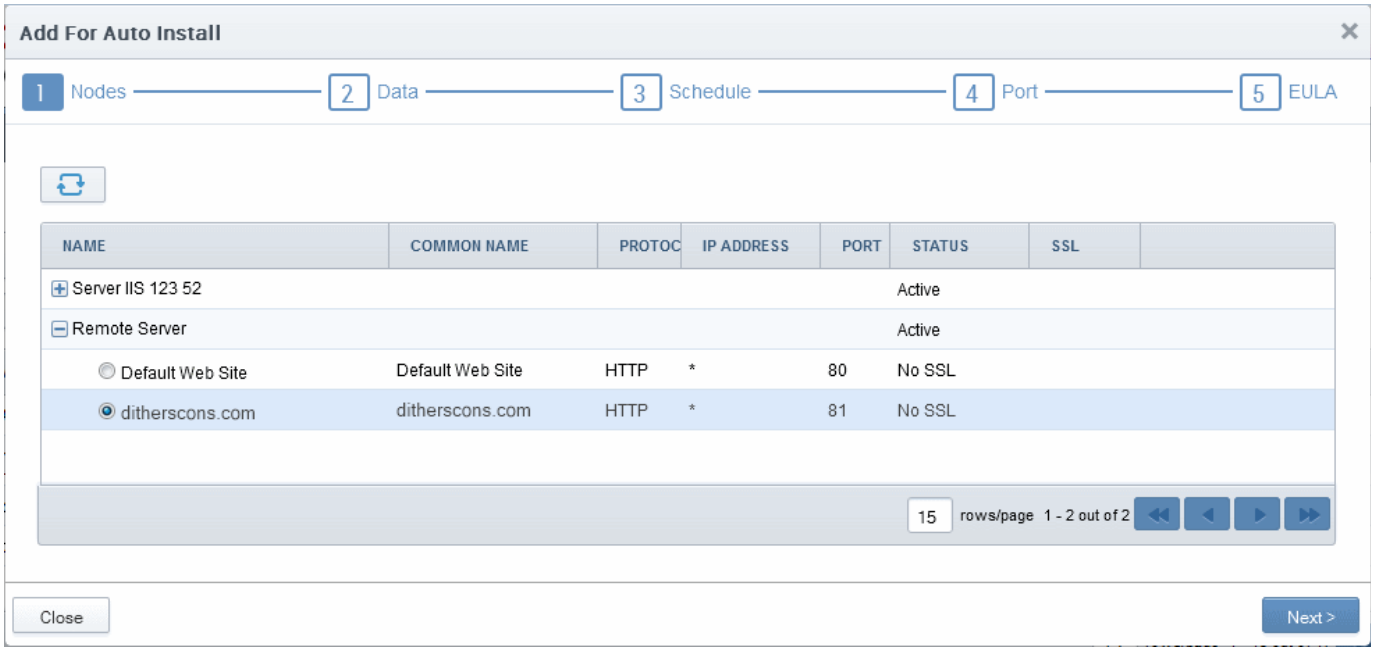
- Enter the parameters and click OK. The server will be added to the controller. It will take a few minutes for the server to become 'Active' state.



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

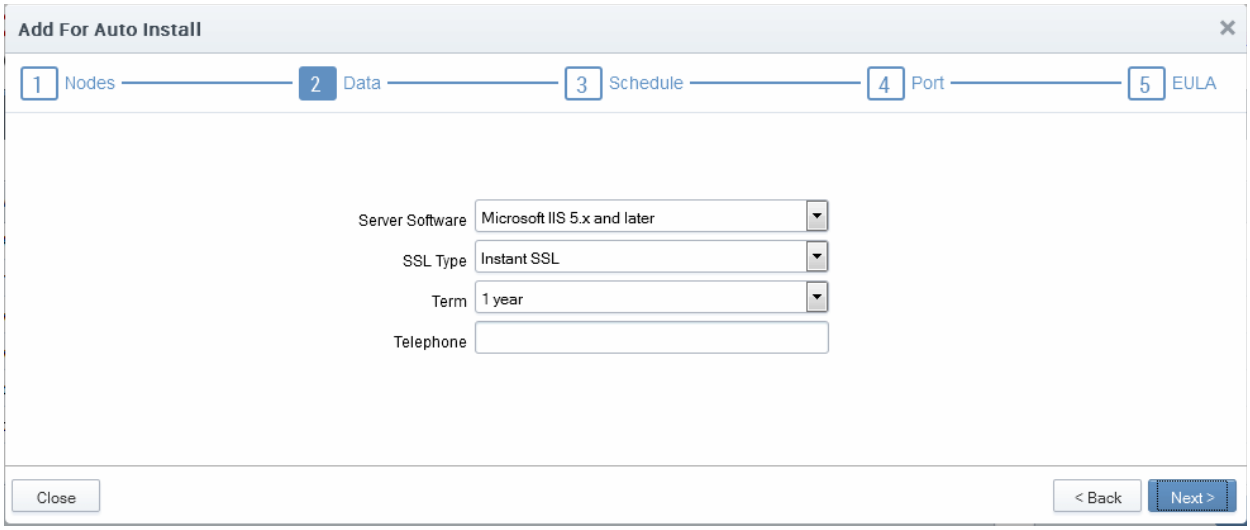


The 'Add for Auto Install' dialog will be displayed with the 'Nodes' interface opened. The 'Nodes' interface displays a tree structure of servers associated with the Certificate Controller and the domains hosted by them.

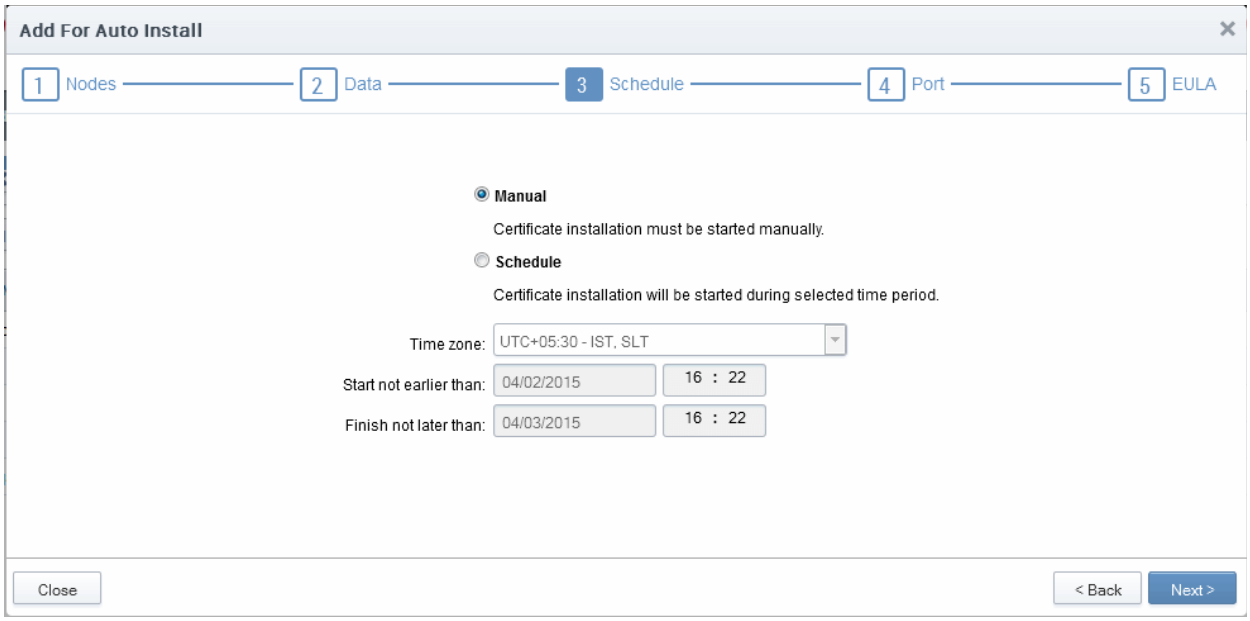


- Select the domain from the remote server for which you wish to install a SSL certificate and click 'Next'.

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

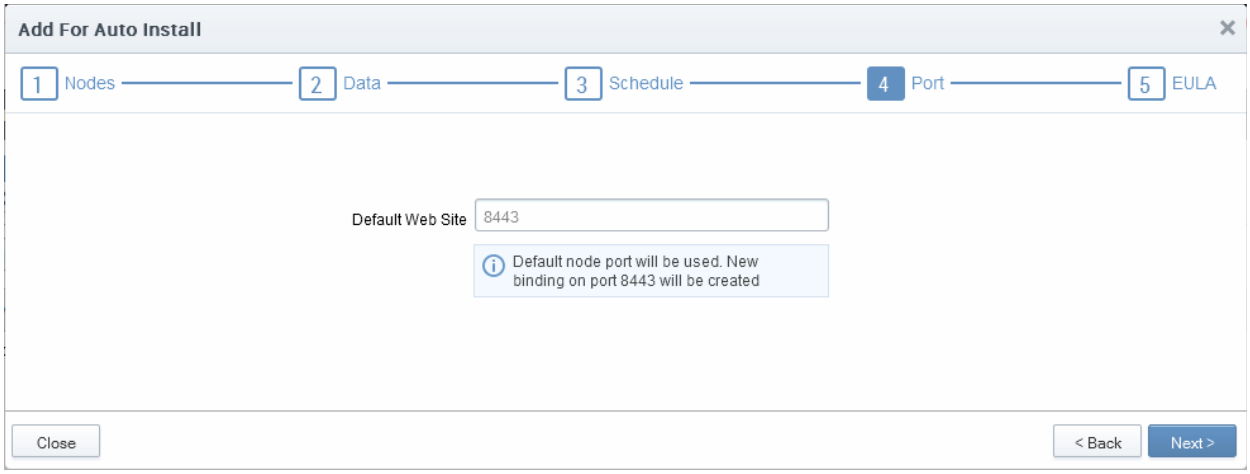


- Select the Server type from the 'Server Software' drop-down.
- Select the SSL certificate type that you wish to order from the 'SSL Type' drop-down. The drop-down will list only the certificate types that are enabled for the Organization.
- Select the term length of the certificate from the 'Term'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



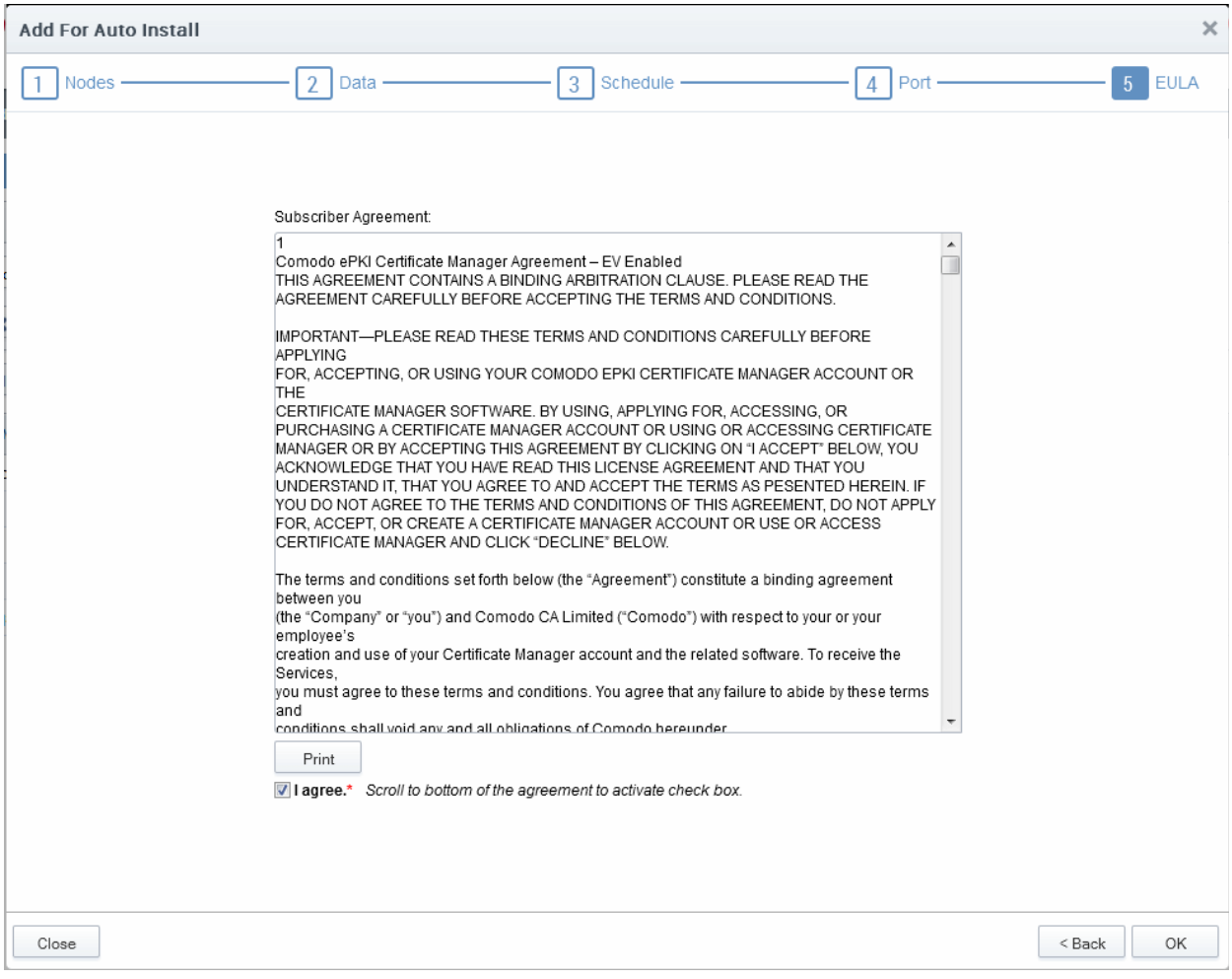
- If you want to manually install the certificate, select 'Manual'
- If you want to install the certificate at a scheduled time, select 'Schedule' and then select your time zone, and set a time period . The Certificate Controller will generate the CSR and submit to Comodo CA, when it polls the CCM for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

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



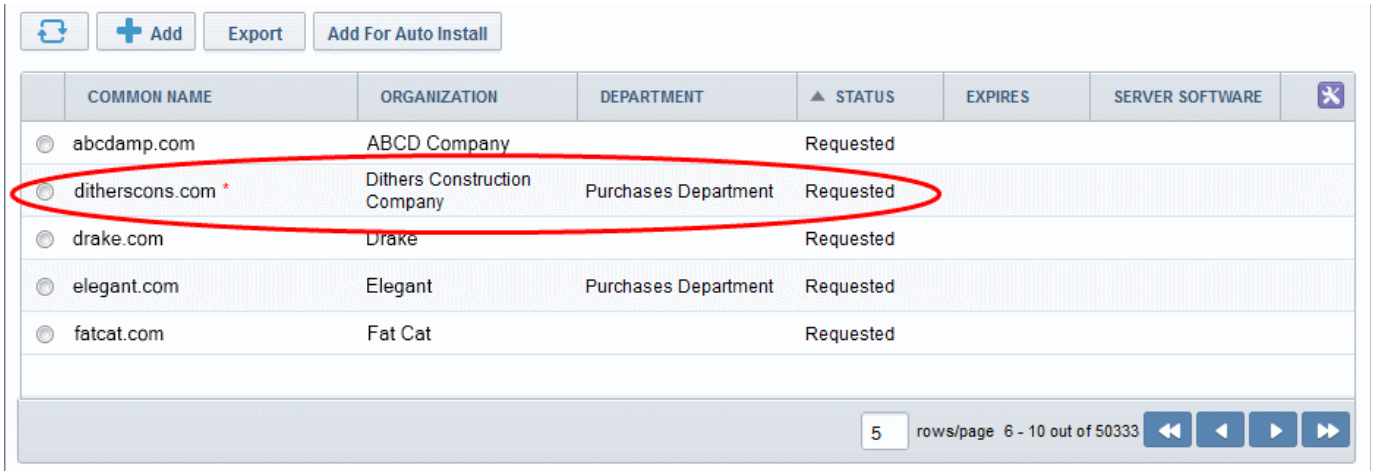
- Specify the HTTPS port for installing the certificate, (Default = 9443)
- Click 'Next'.

The EULA interface will open.

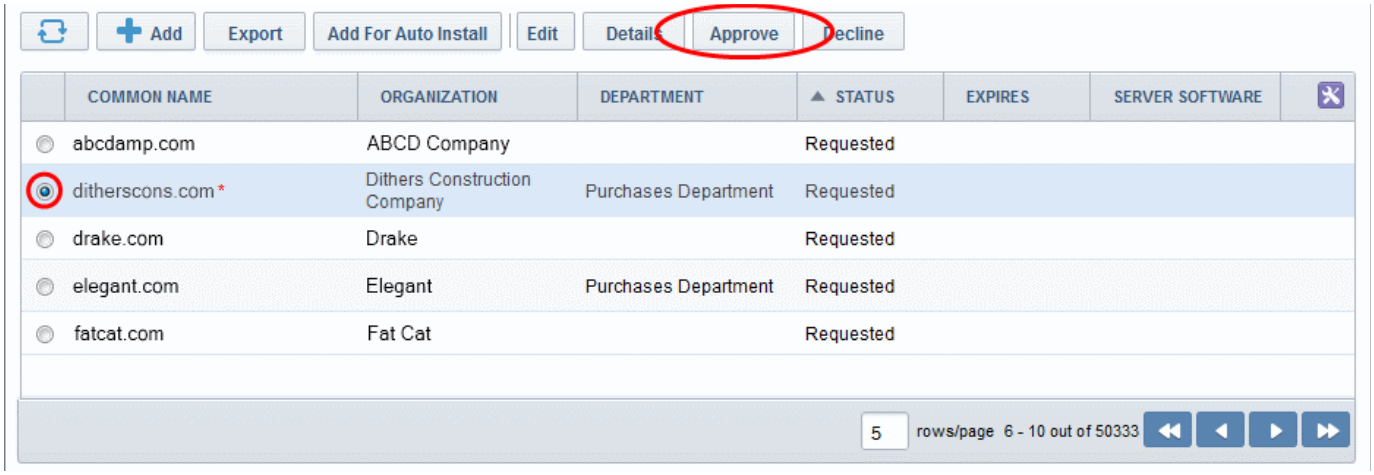


- Read the EULA fully and accept to it by selecting 'I Agree' checkbox.
- Click 'OK' to save your application.

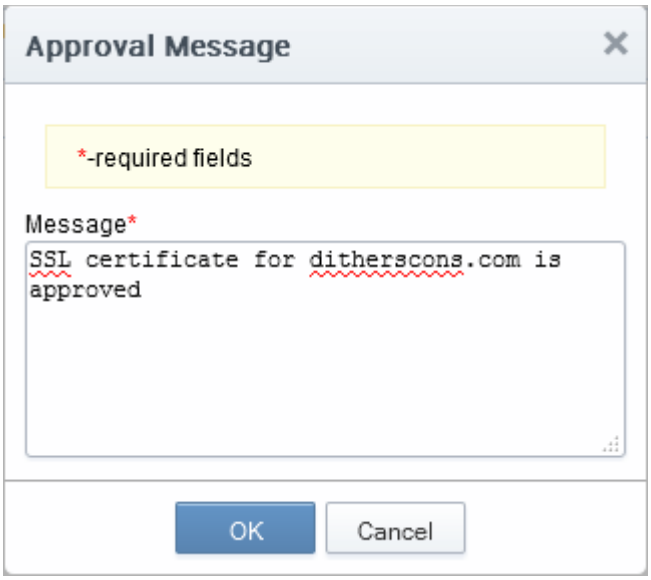
The certificate will be added to the SSL Certificates interface and its status will be displayed as 'Requested'.



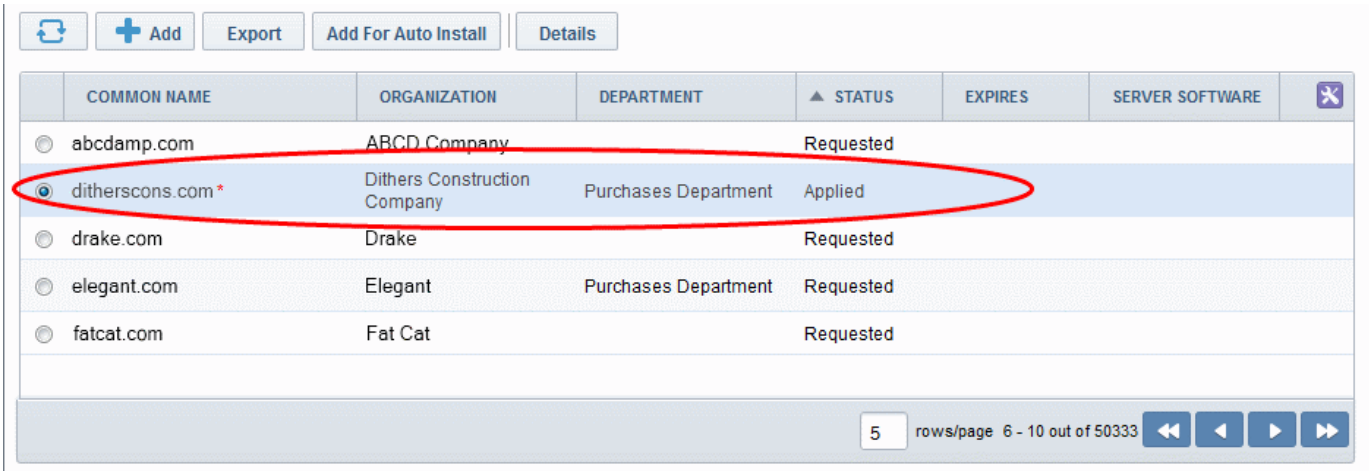
- The CSR for the requested certificate will be generated automatically. On successful creation of CSR, the 'Approve' button will appear at the top, on selecting the certificate.



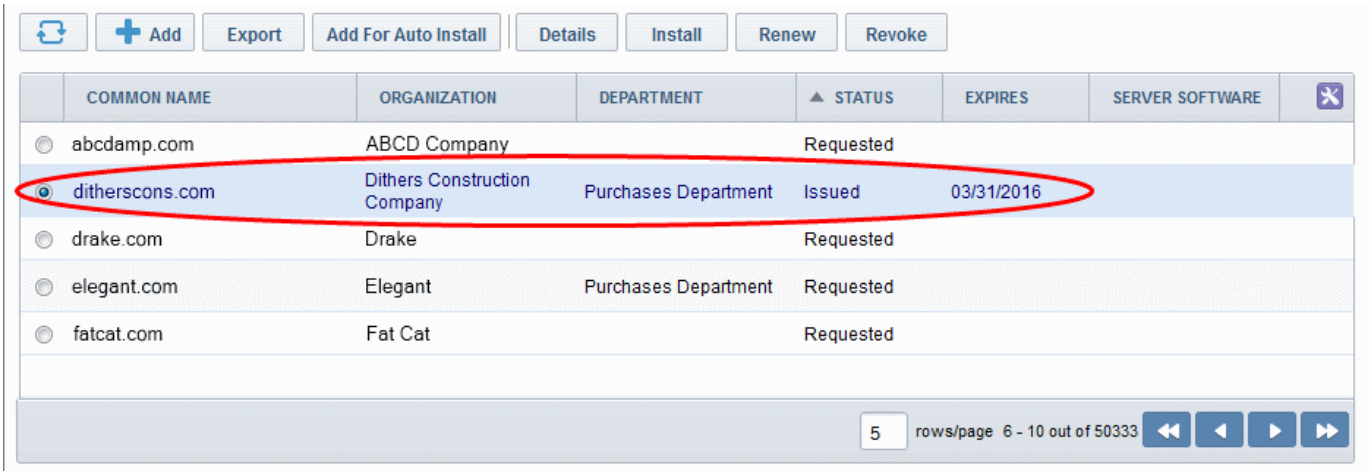
- Click the 'Approve' button to approve the request, enter the approval message in the 'Approval Message' dialog and click 'OK'.



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

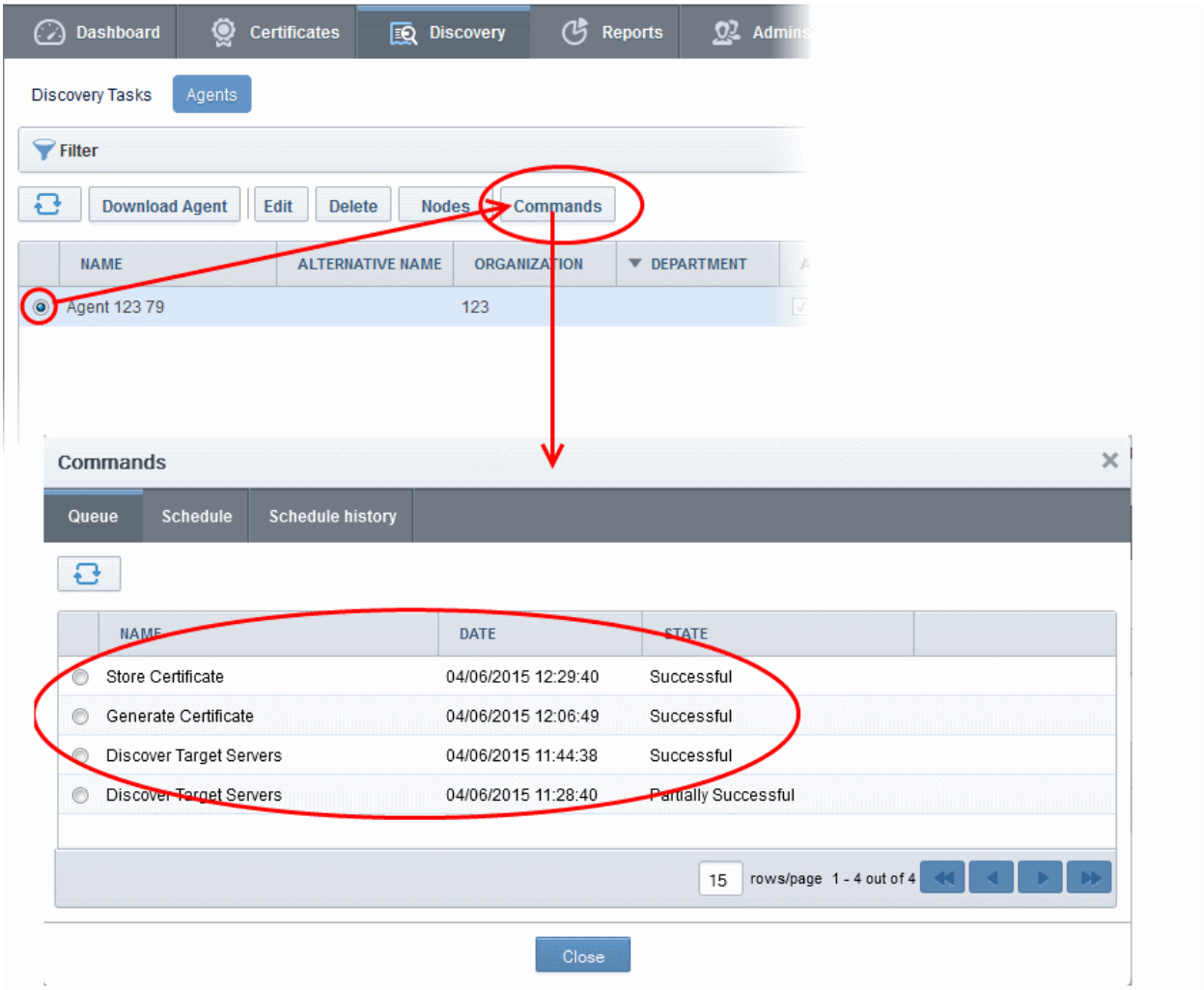


The Certificate Controller will track the order number and download the certificate from the CA, once it is issued and stores it. The certificate status will be changed to 'Issued'.

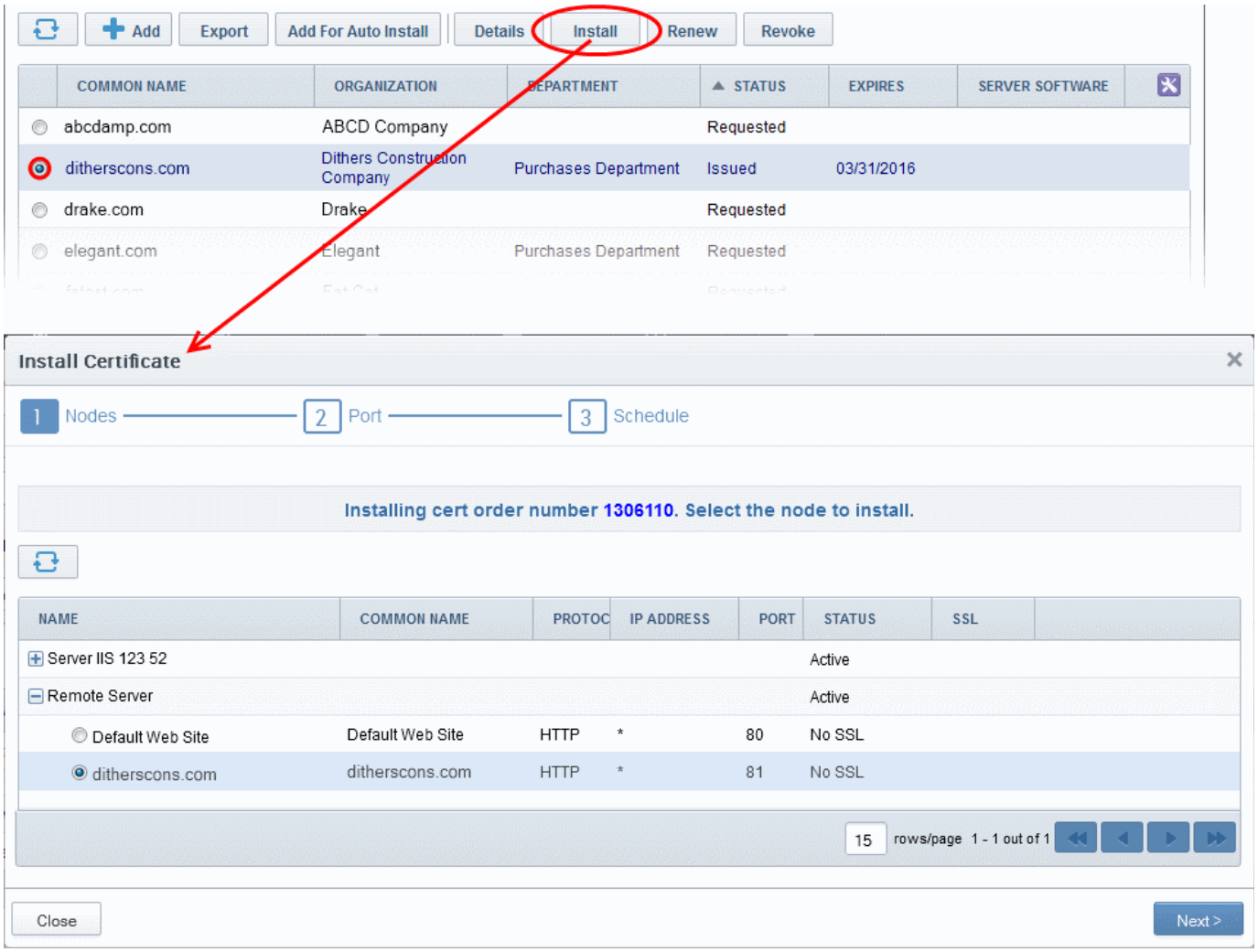


- To check whether the Certificate Controller has stored the certificate, click 'Settings' > 'Discovery' > 'Agents'.
- Select the controller and click 'Commands' button

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



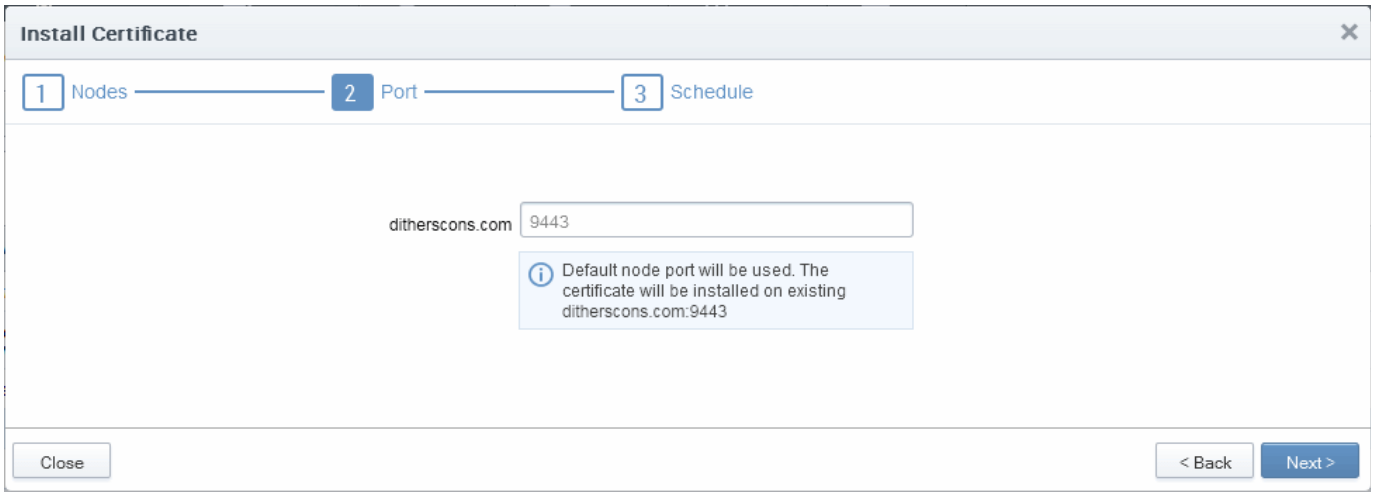
- To install the certificate on to the remote server, select the certificate and click 'Install' from the 'Certificates' interface.



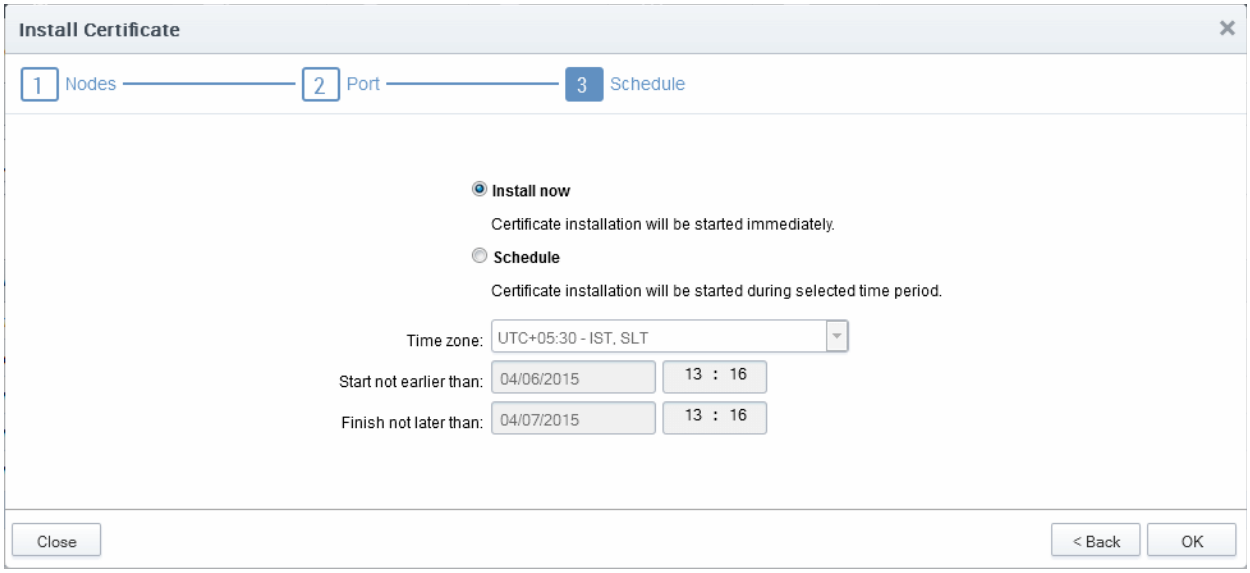
The 'Install Certificate' dialog will be displayed with the nodes interface opened. The node upon which the certificate is to be installed is pre-selected.

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

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



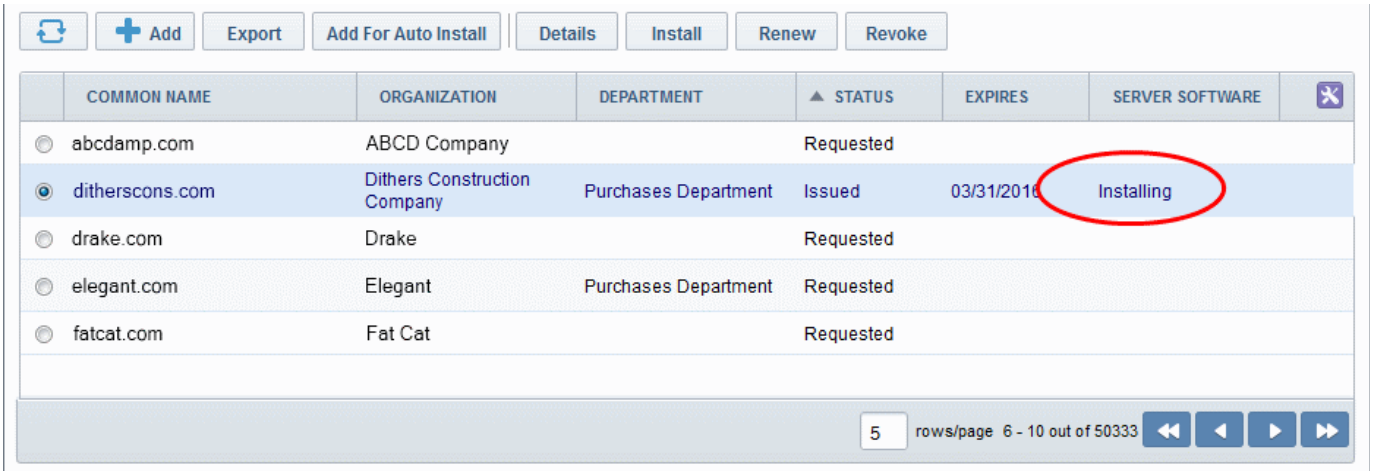
- Specify the port and click 'Next'. The 'Schedule' interface will open.



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

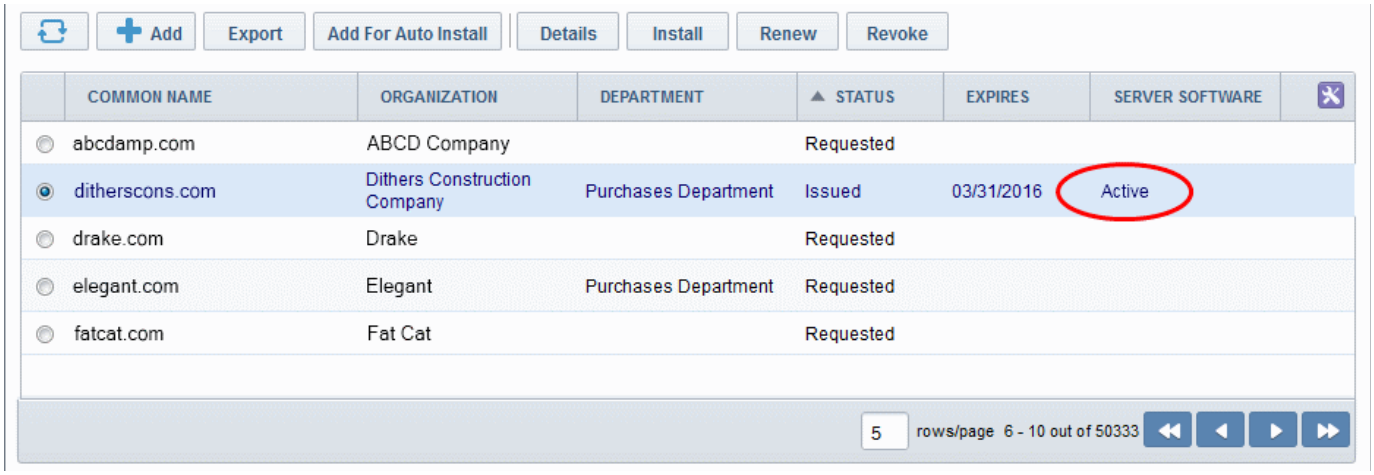
- Click 'OK'

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

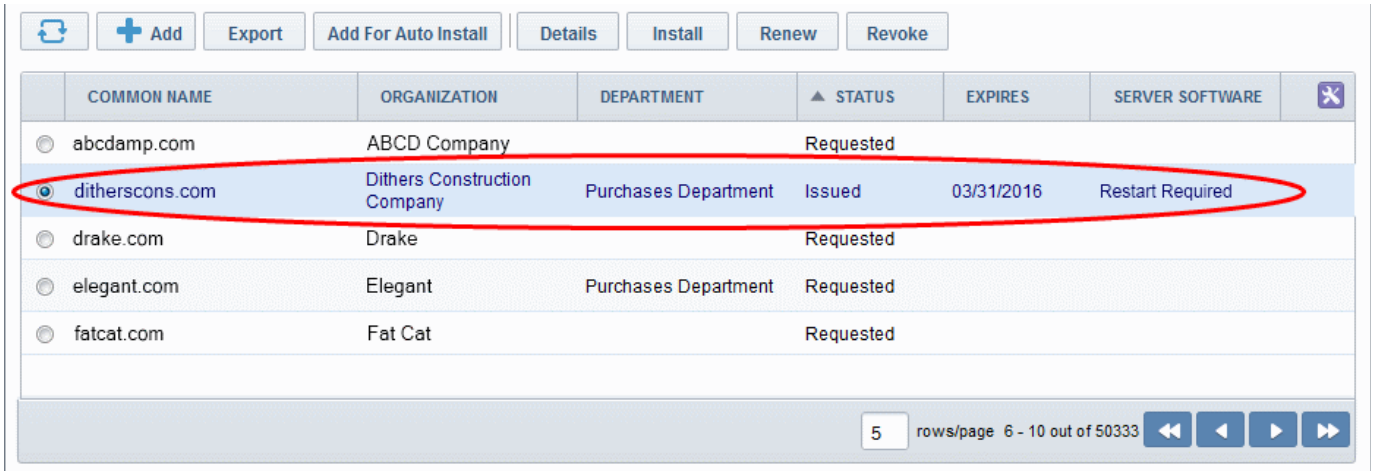


Upon completion of installation,

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

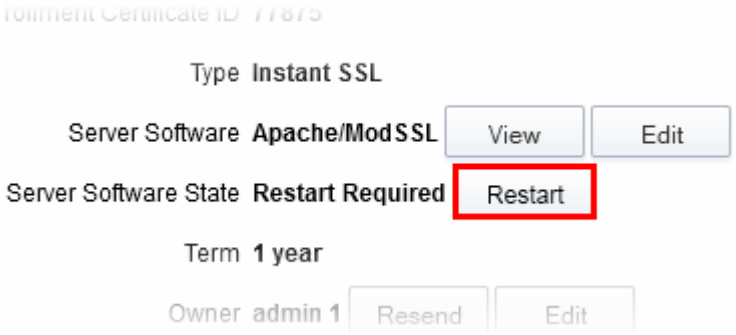


- For Apache Httpd/Apache Tomcat server: the certificate will be activated upon restart of the server. The Server Software state will be indicated as 'Restart Required'.



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

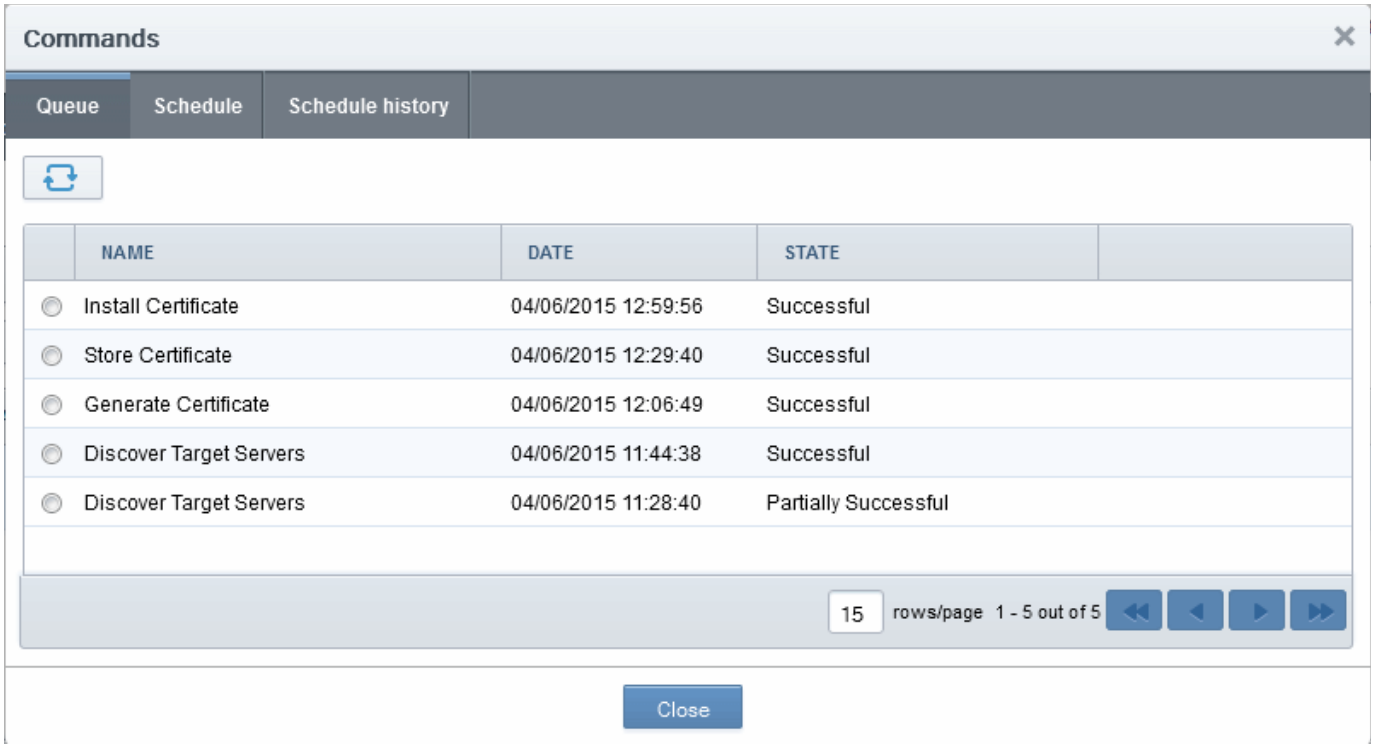
- Select the certificate and click the 'Details' button at the top. The 'Certificate Details' dialog will be displayed.
- Click 'Restart' beside the Server Software State field in the 'Details' dialog



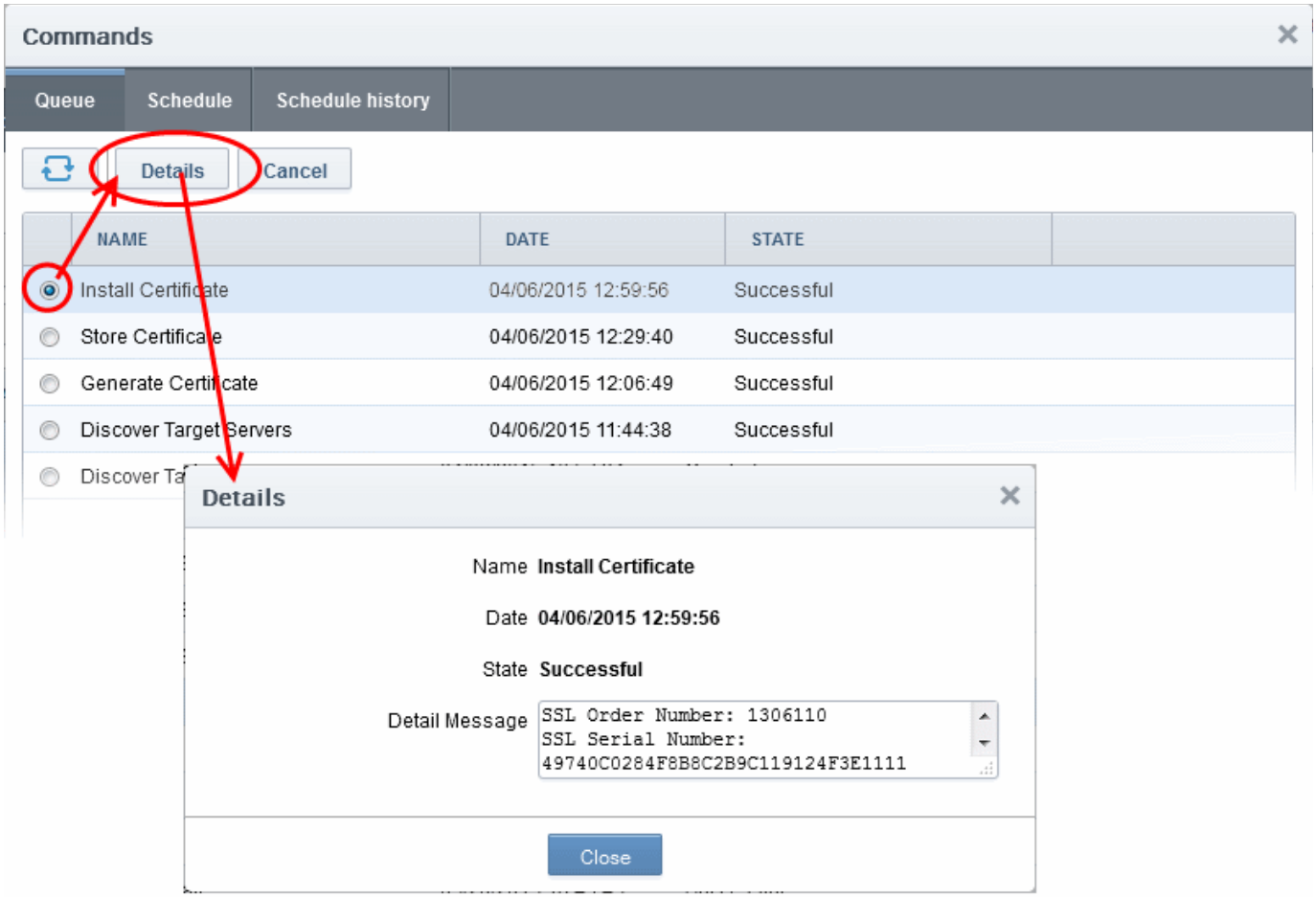
Upon restarting the server, the certificate will be activated and the Server Software state will be indicated as 'Active'.

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

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



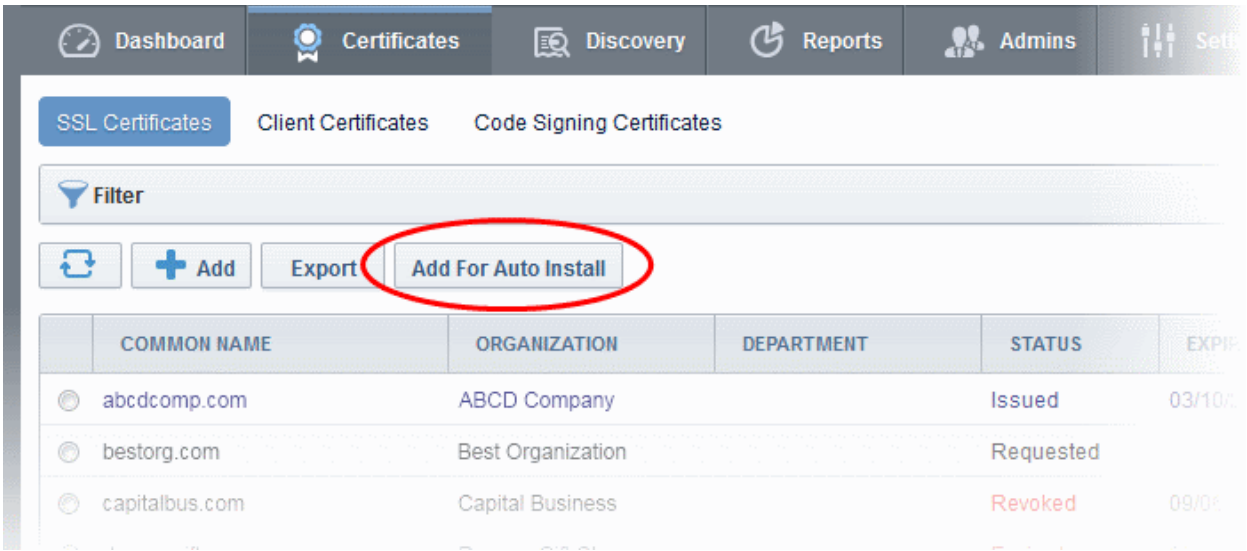
- To view the details of the command, select the command and click the 'Details' button from the top.



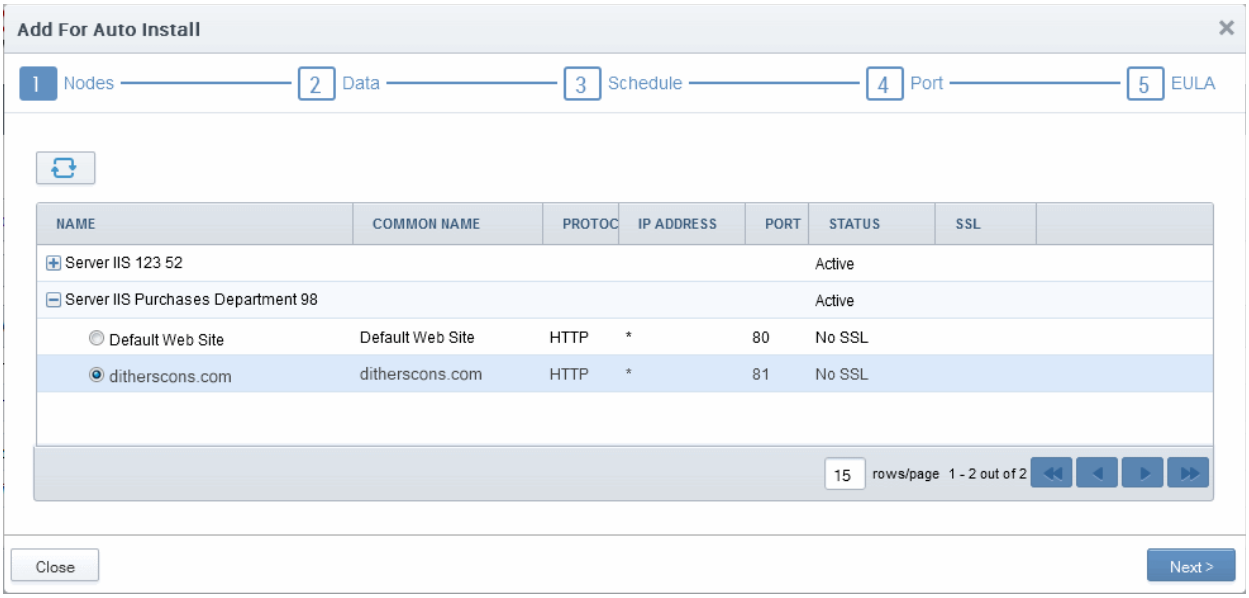
Method 2 - CCM Controller Mode

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

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

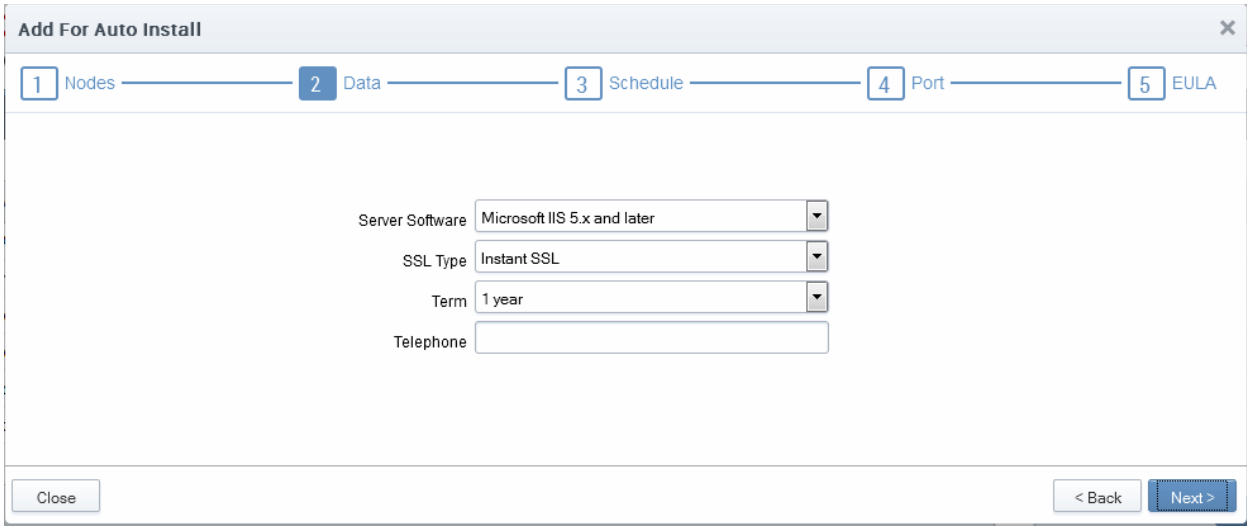


The 'Add for Auto Install' dialog will be displayed with the 'Nodes' interface opened. The 'Nodes' interface displays a list of Agents installed in your servers for different Organizations and Departments, with the list of server nodes under each Agent.

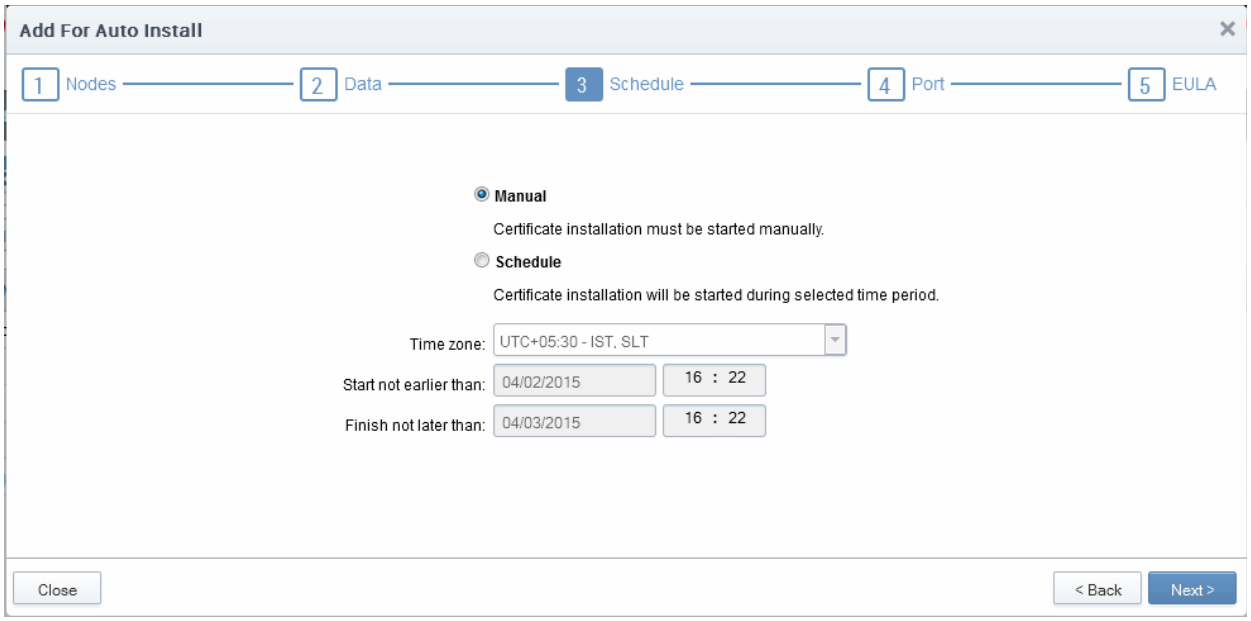


- Select the domain for which you wish to install a SSL certificate and click Next.

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

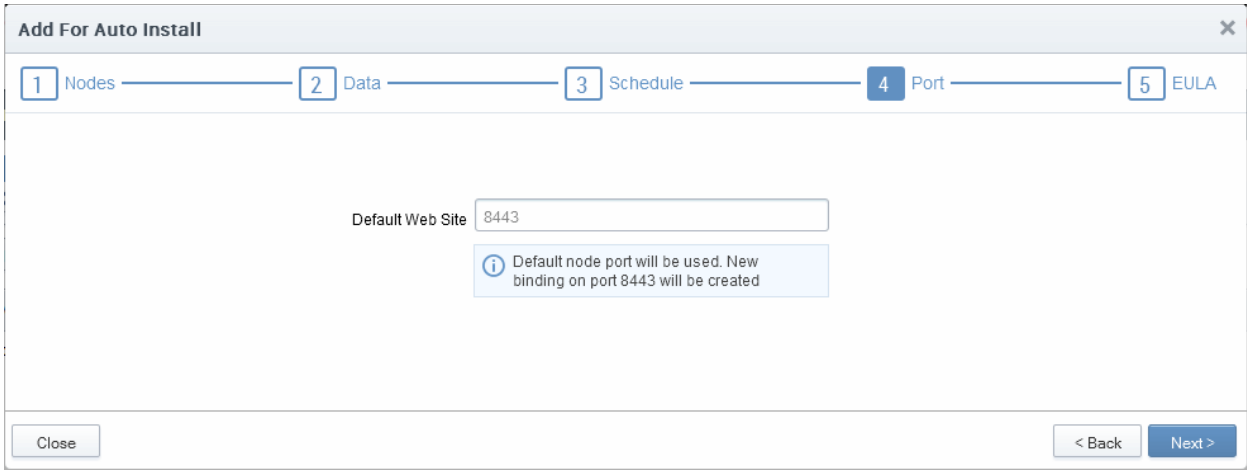


- Select the Server type from the 'Server Software' drop-down.
- Select the SSL certificate type that you wish to order from the 'SSL Type' drop-down. The drop-down will list only the certificate types that are enabled for the Organization.
- Select the term length of the certificate from the 'Term'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

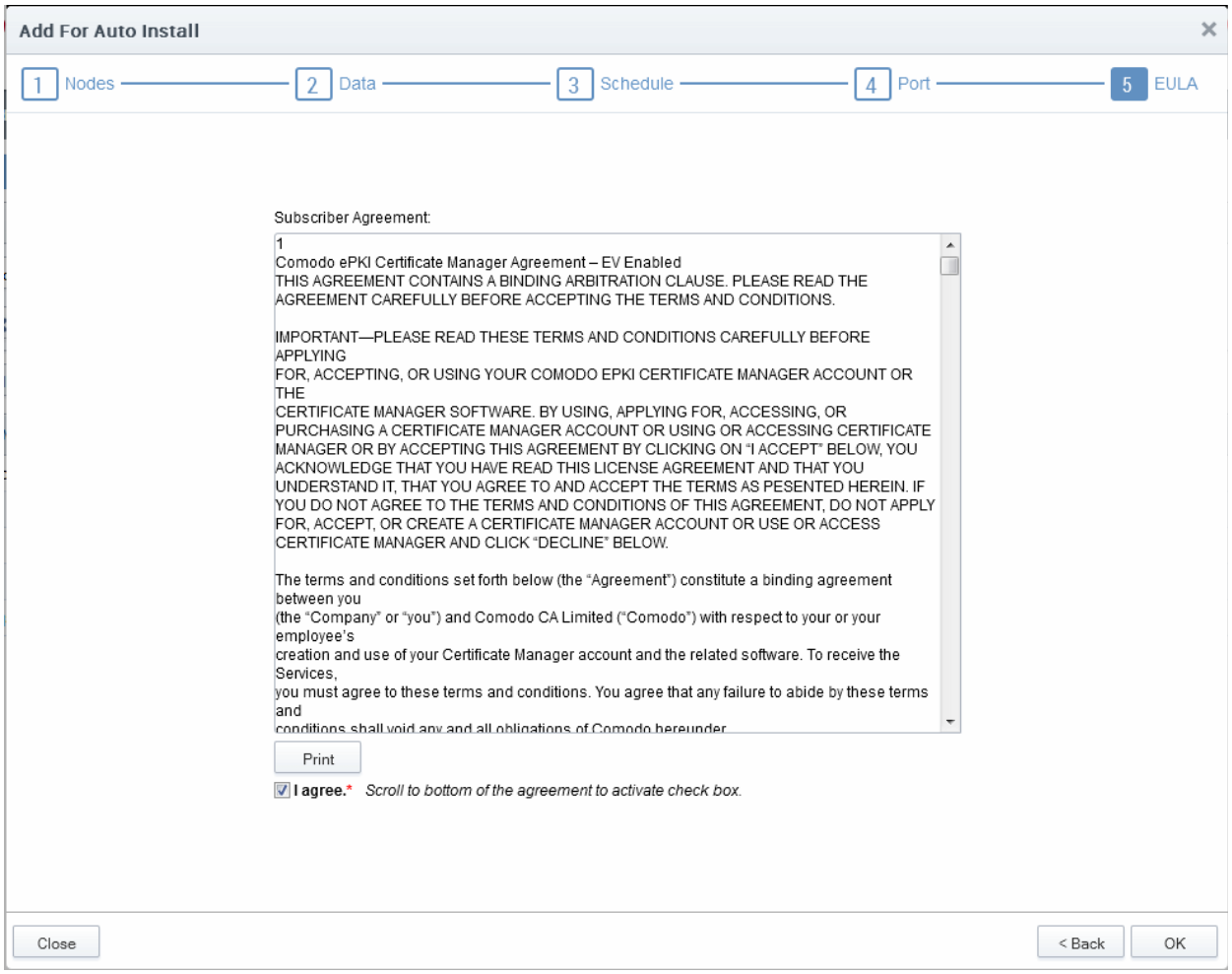


- If you want to manually install the certificate, select 'Manual'
- If you want to install the certificate at a scheduled time, select 'Schedule' and then select your time zone, and set a time period . The CSR will be generated and submitted to Comodo CA, during the first polling by the Agent, within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

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

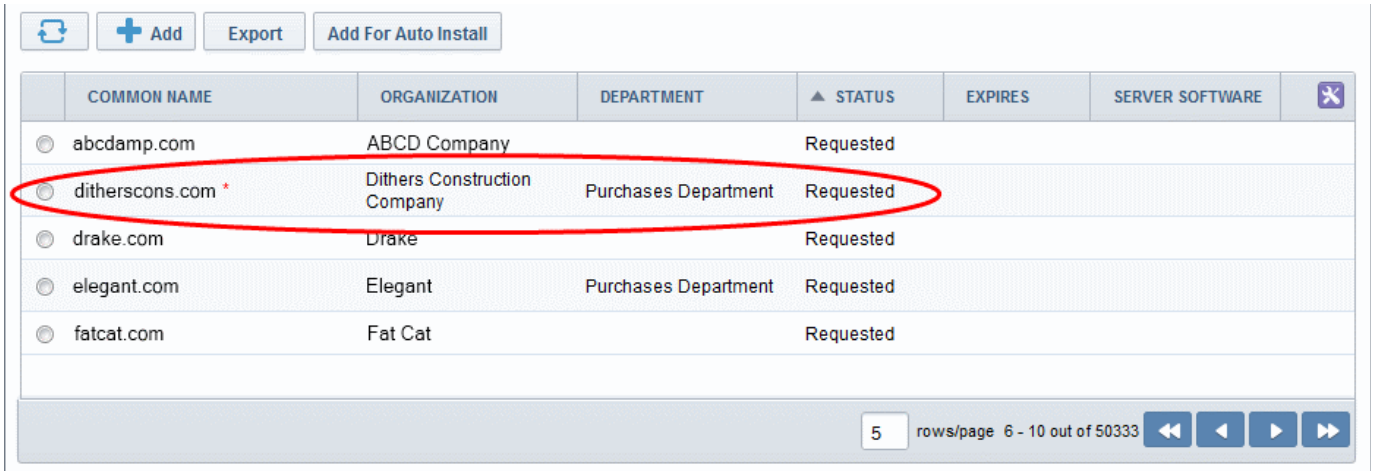


- Specify the HTTPS port for installing the certificate, (Default = 8443)
- Click 'Next'. The EULA interface will open

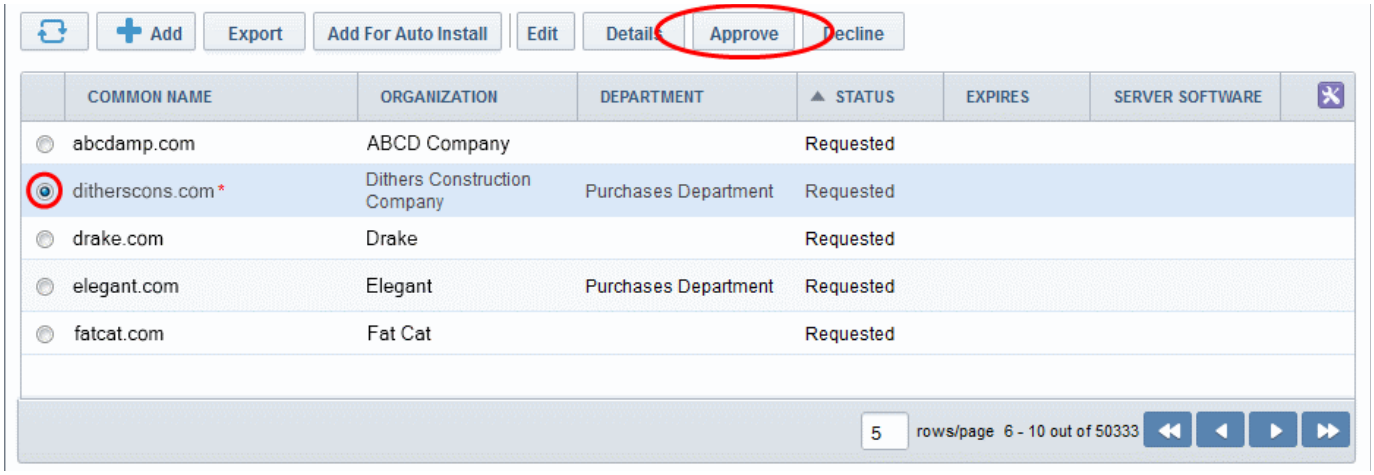


- Read the EULA fully and accept to it by selecting 'I Agree' checkbox.
- Click 'OK' to save your application.

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

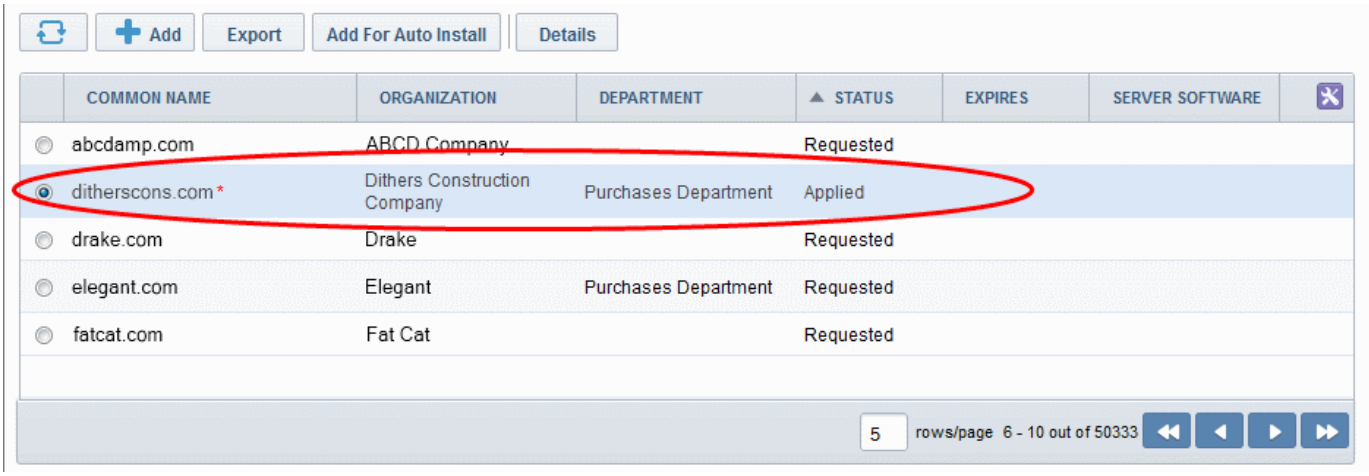


- The Agent will generate a CSR for the requested certificate automatically during its first polling cycle in the set schedule period. If you want to generate the CSR instantly, click 'Refresh'. On successful creation of CSR, the 'Approve' button will appear for the certificate.

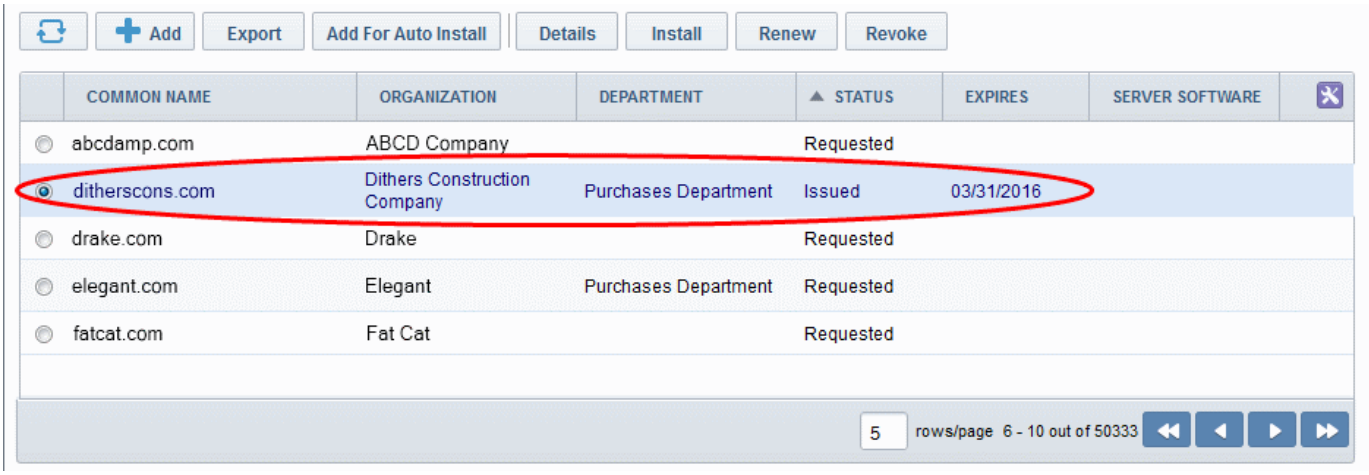


- Click the 'Approve' button to approve the request, enter the approval message in the 'Approval Message' dialog and click 'OK'.

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

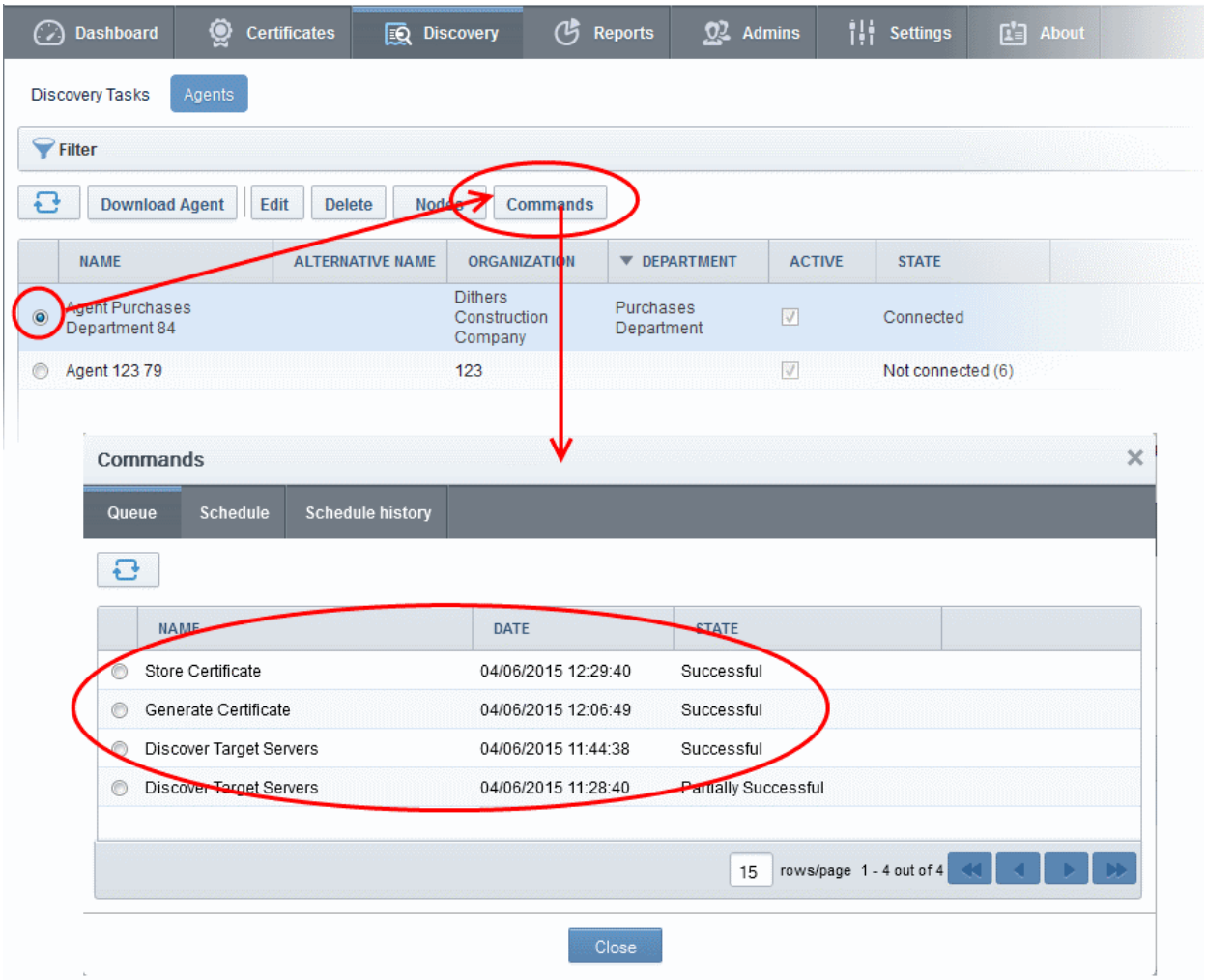


The Agent will track the order number and download the certificate from the CA, once it is issued and stores it. The certificate status will be changed to 'Issued'.

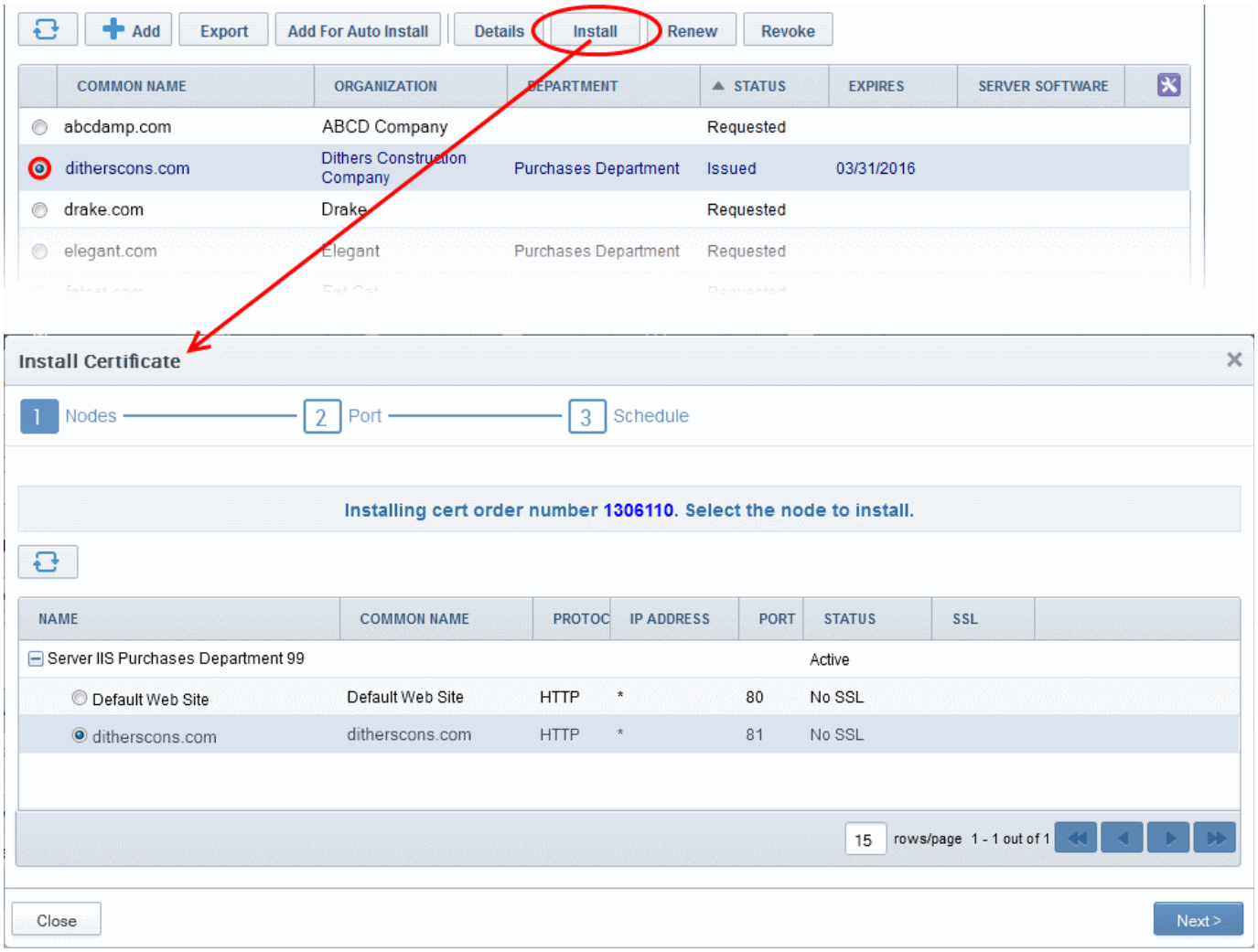


- To check whether the Agent has stored the certificate, click 'Discovery' > 'Agents'.
- Select the Agent and click 'Commands' from the top

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



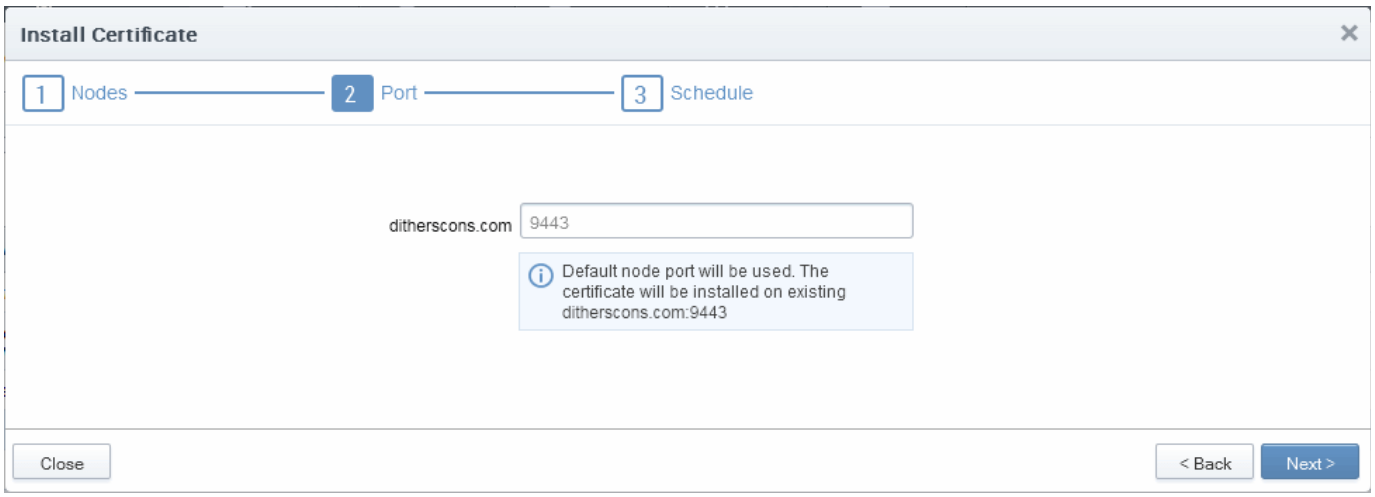
- To install the certificate, click 'Install' from the 'Certificates' interface.



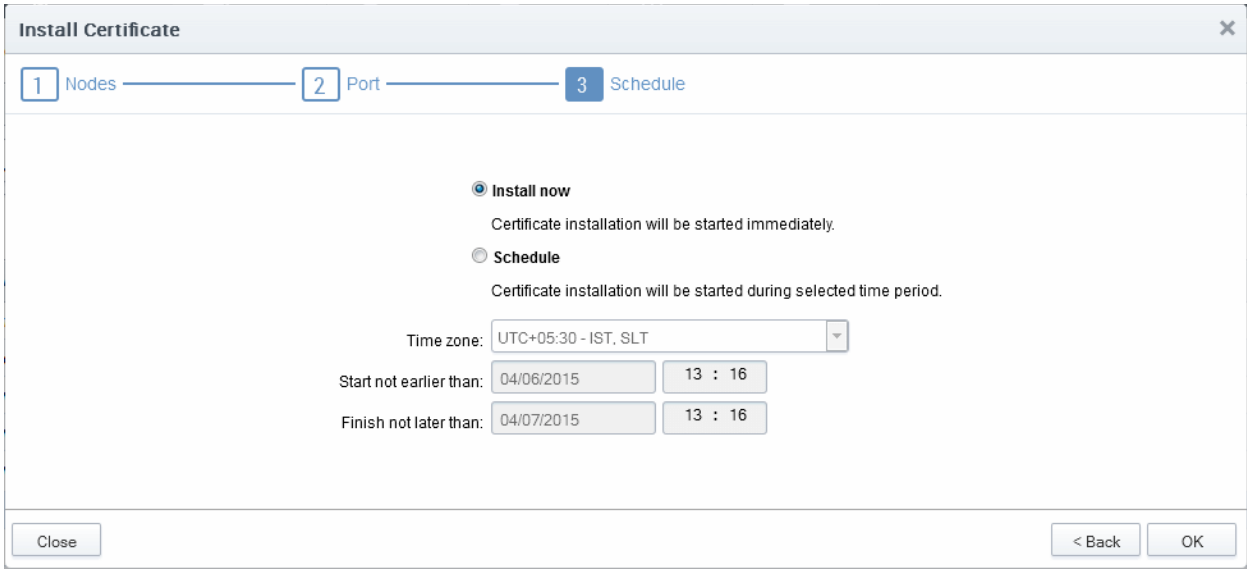
The 'Install Certificate' dialog will be displayed with the nodes interface opened. The node upon which the certificate is to be installed is pre-selected.

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

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



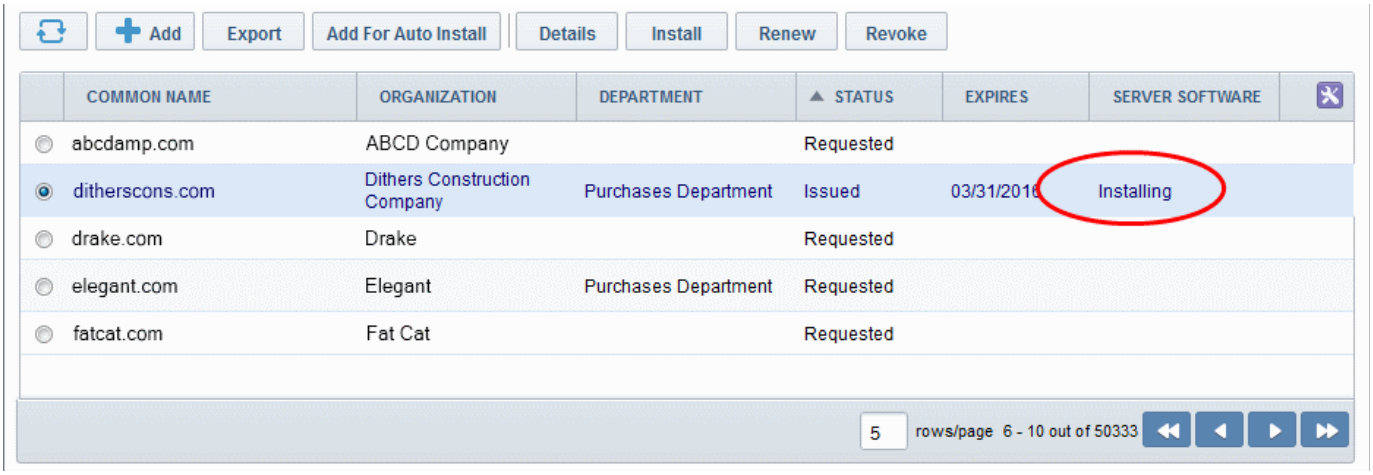
- Specify the port and click 'Next'. The 'Schedule' interface will open.



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

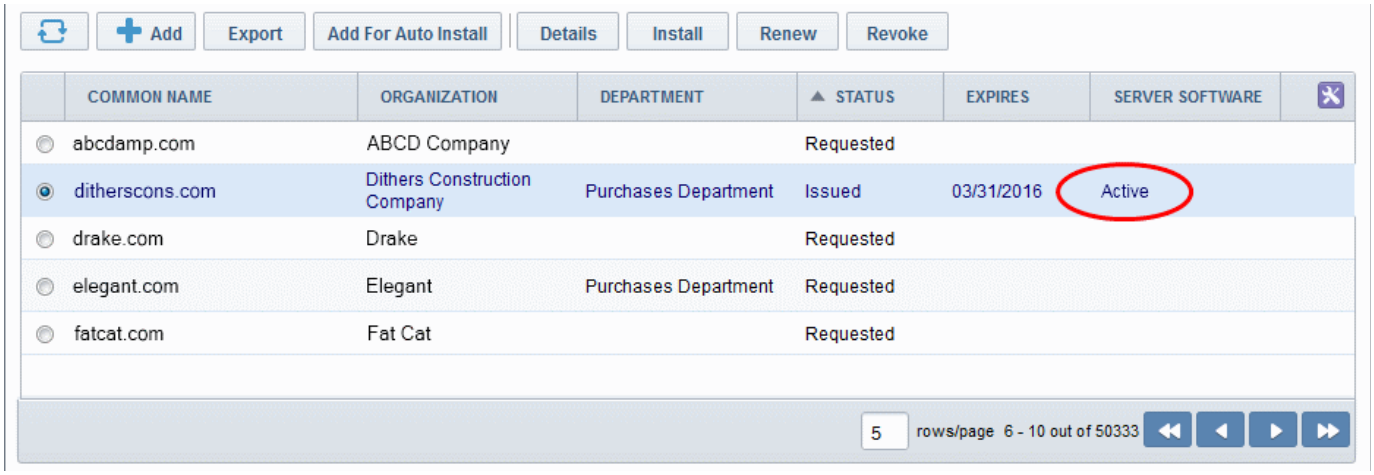
- Click 'OK'

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

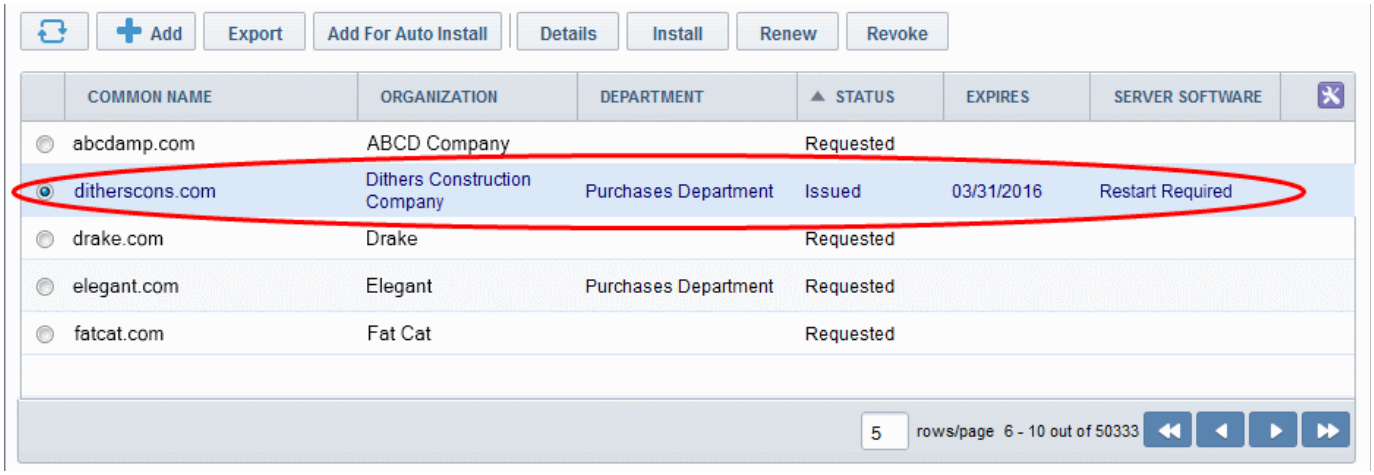


Upon completion of installation,

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

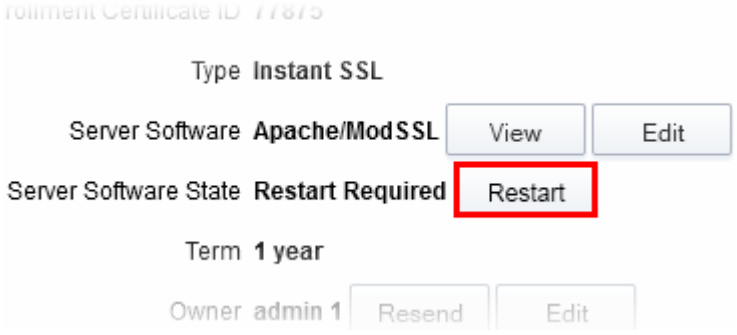


- For Apache servers: the certificate will be activated upon restart of the server. The Server Software state will be indicated as 'Restart Required'.



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

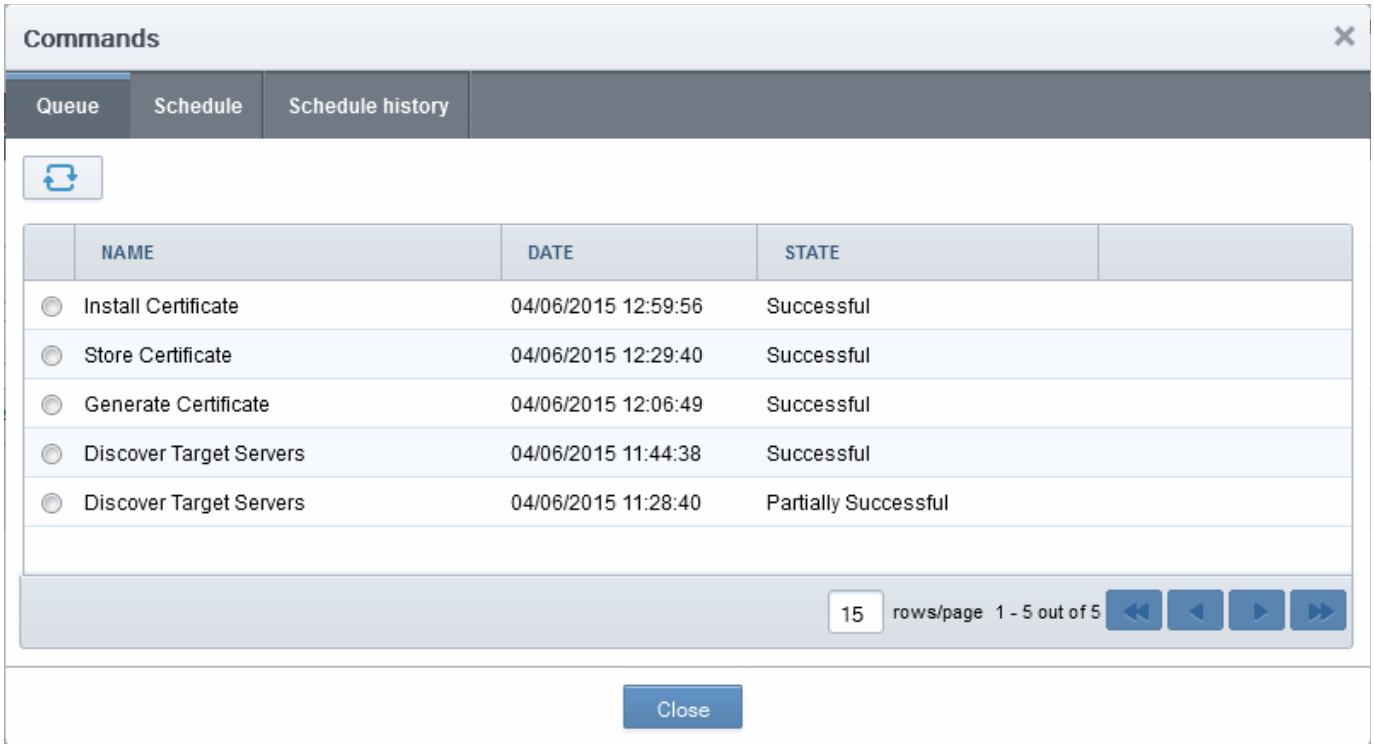
- Select the certificate and click the 'Details' button at the top. The 'Certificate Details' dialog will be displayed.
- Click Restart beside the Server Software State field in the 'Details' dialog



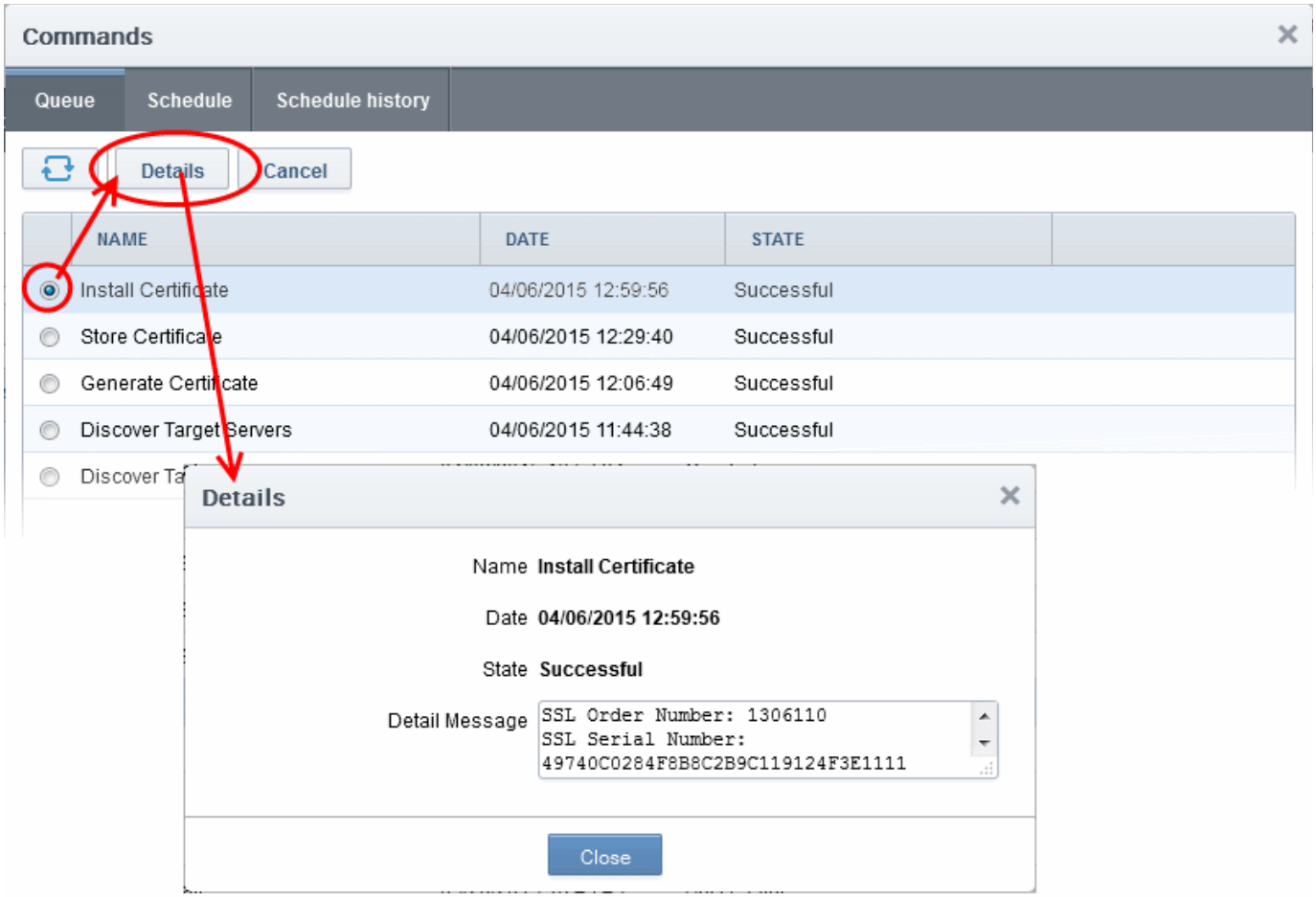
Upon restarting the server, the certificate will be activated and the Server Software state will be indicated as 'Active'.

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

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



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



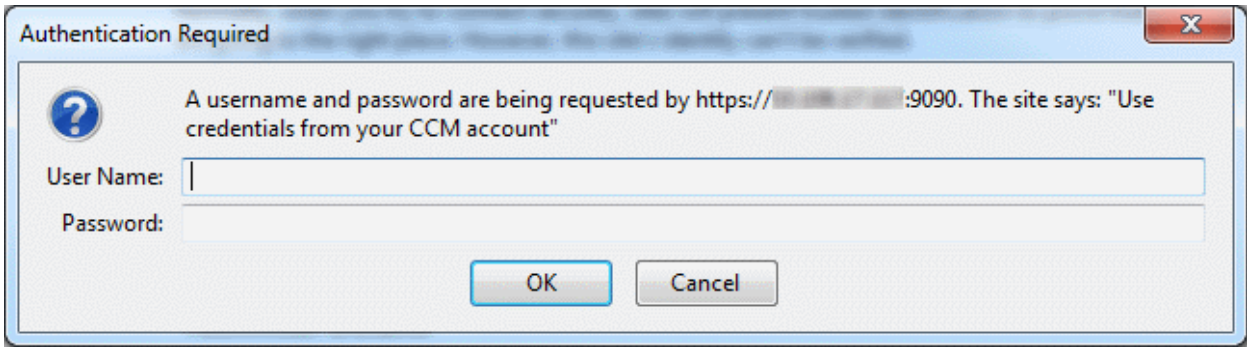
Configuring the Certificate Controller Agent through Web Interface

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

To access the Agent configuration web interface

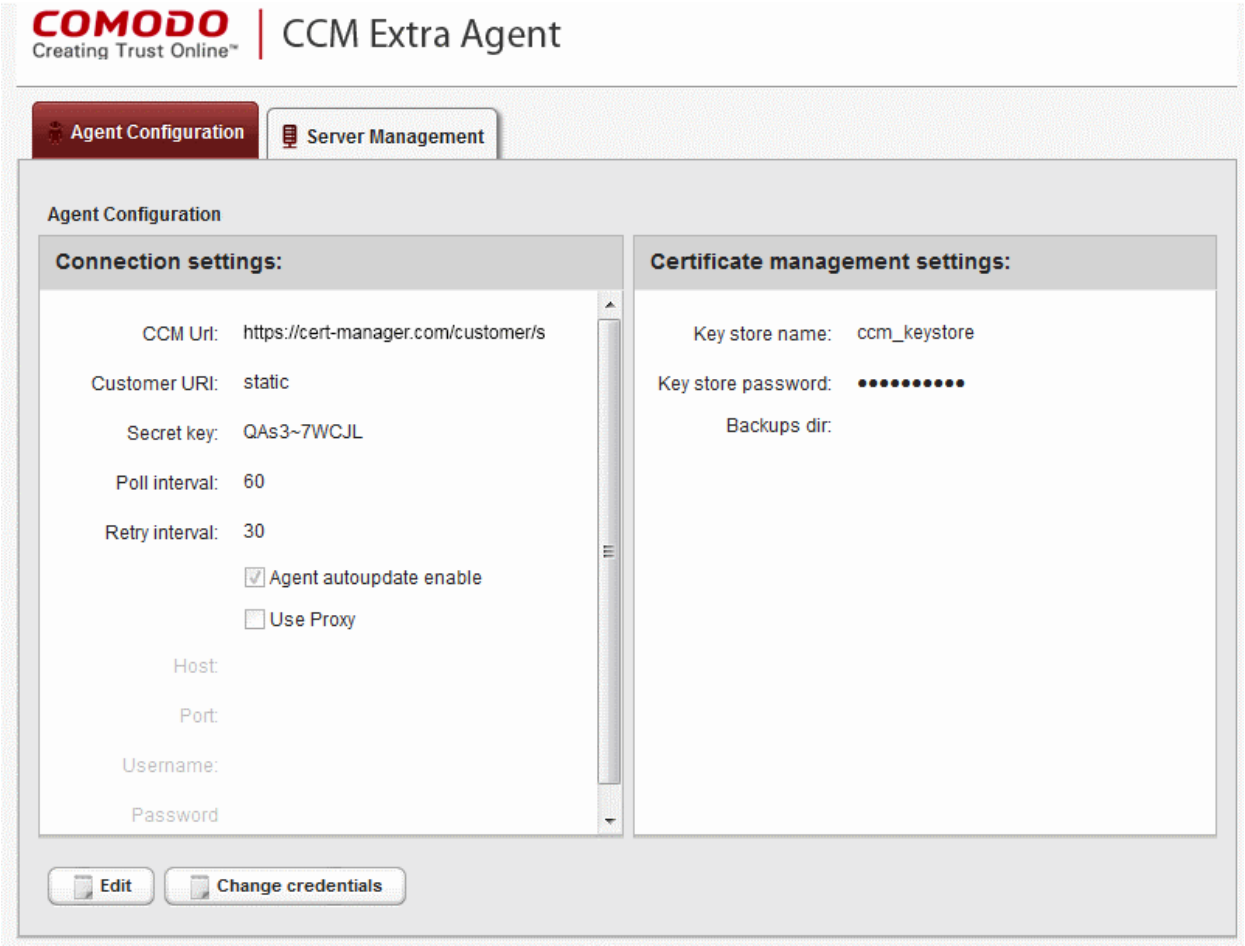
- Type http://<IP Address/host name of the server on which the agent is installed>:9090 in the address of your browser.

The login dialog will appear:



- Enter your CCM username and password.

The Agent configuration interface will open.



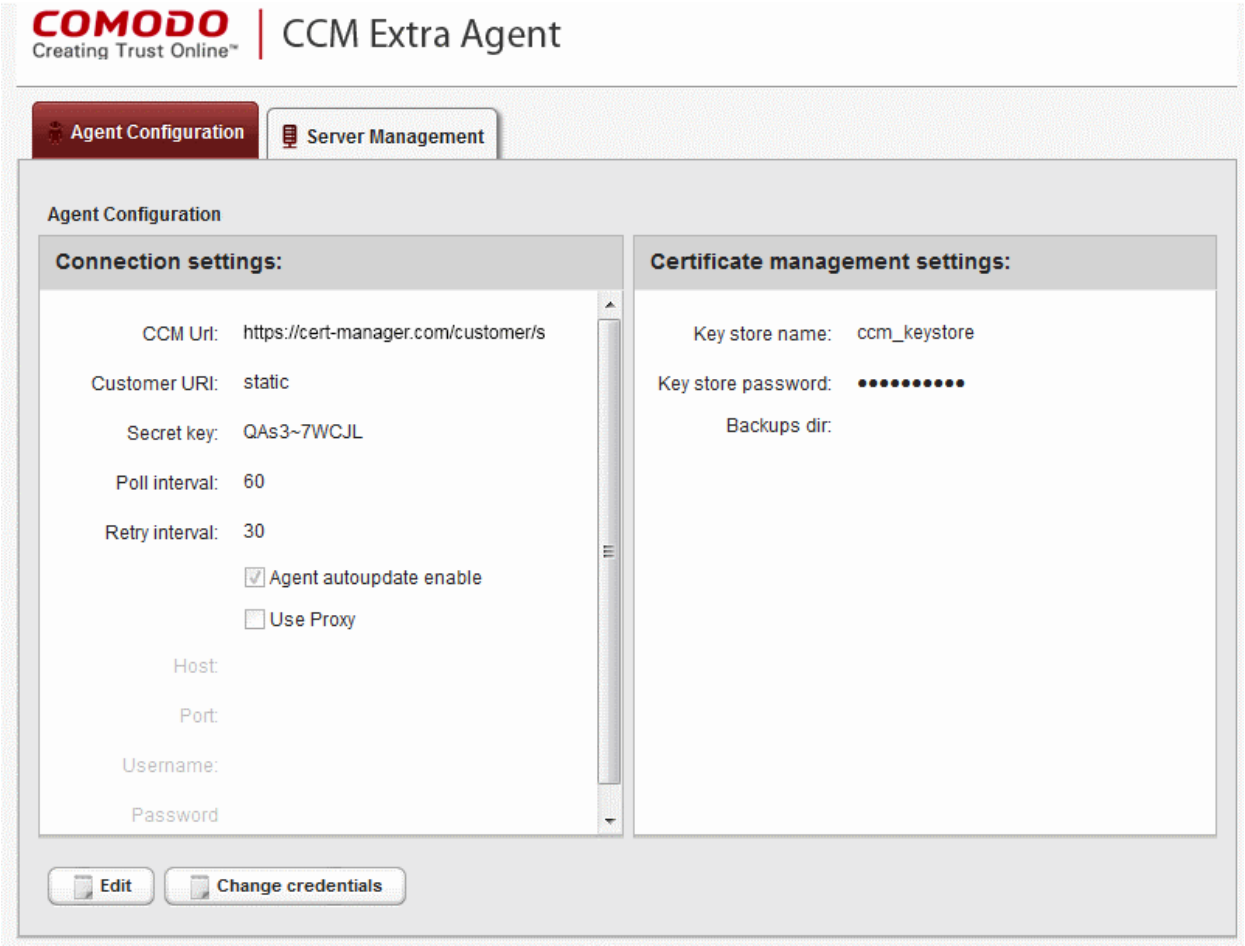
It has two tabs:

- **Agent Configuration**

- **Server Management**

Agent Configuration

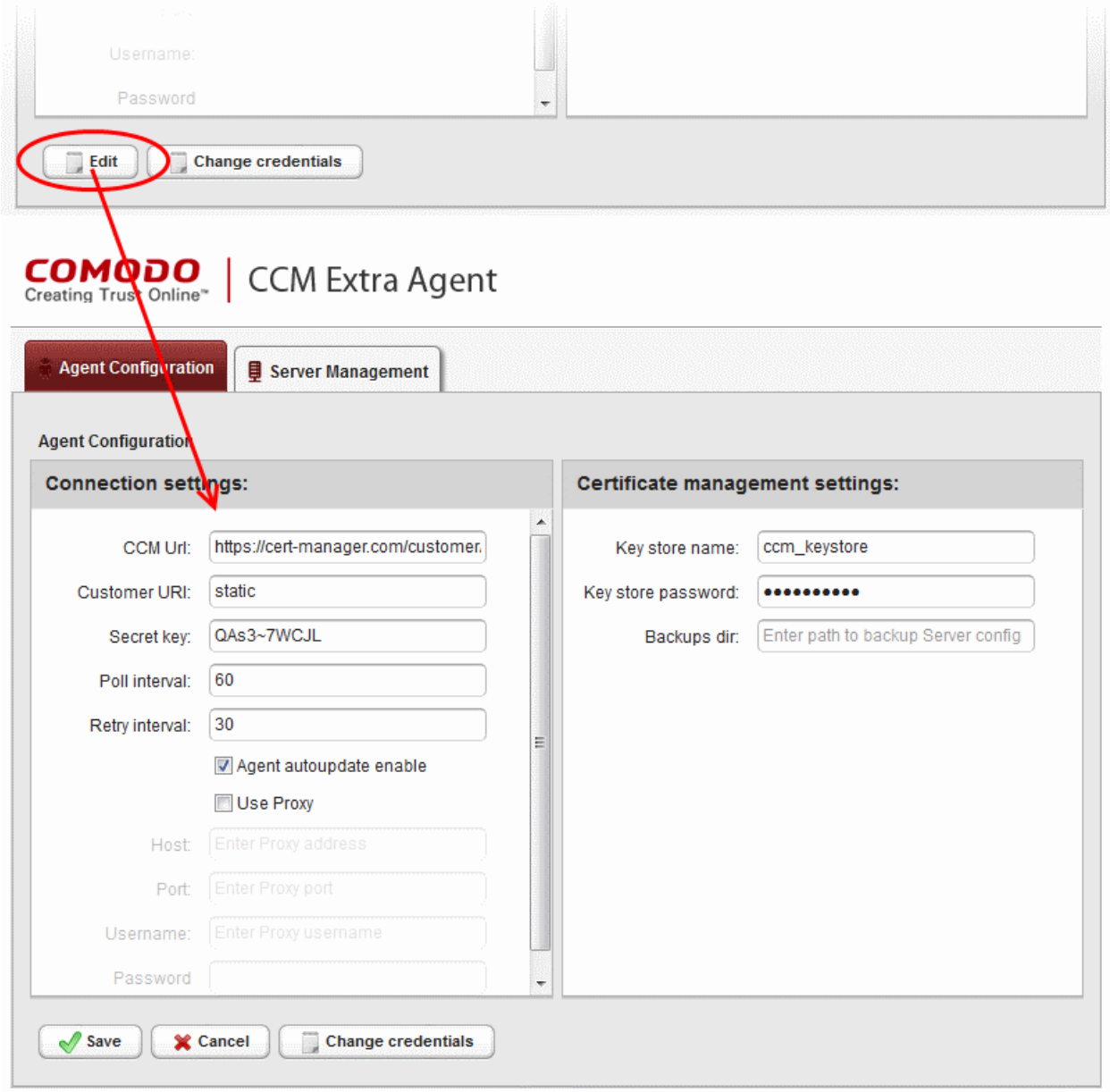
The Agent Configuration tab displays the connection management settings and certificate management settings of the agent and enables the administrator to edit them, if required.



Agent Configuration - Table of Parameters		
Field	**Type**	**Description**
Connection Settings		
CCM url	*Text field*	Displays the URL of CCM server
Customer 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 CCM. This value should not be altered
Poll Interval	*Text field*	Displays the time interval at which the agent polls the CCM for new certificate requests (in seconds) and enables the administrator to edit it in edit mode.
Retry interval	*Text field*	Displays the time interval set for retrying polling on CCM server if polling fails (in seconds) and enables the administrator to edit it in edit mode.

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

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



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

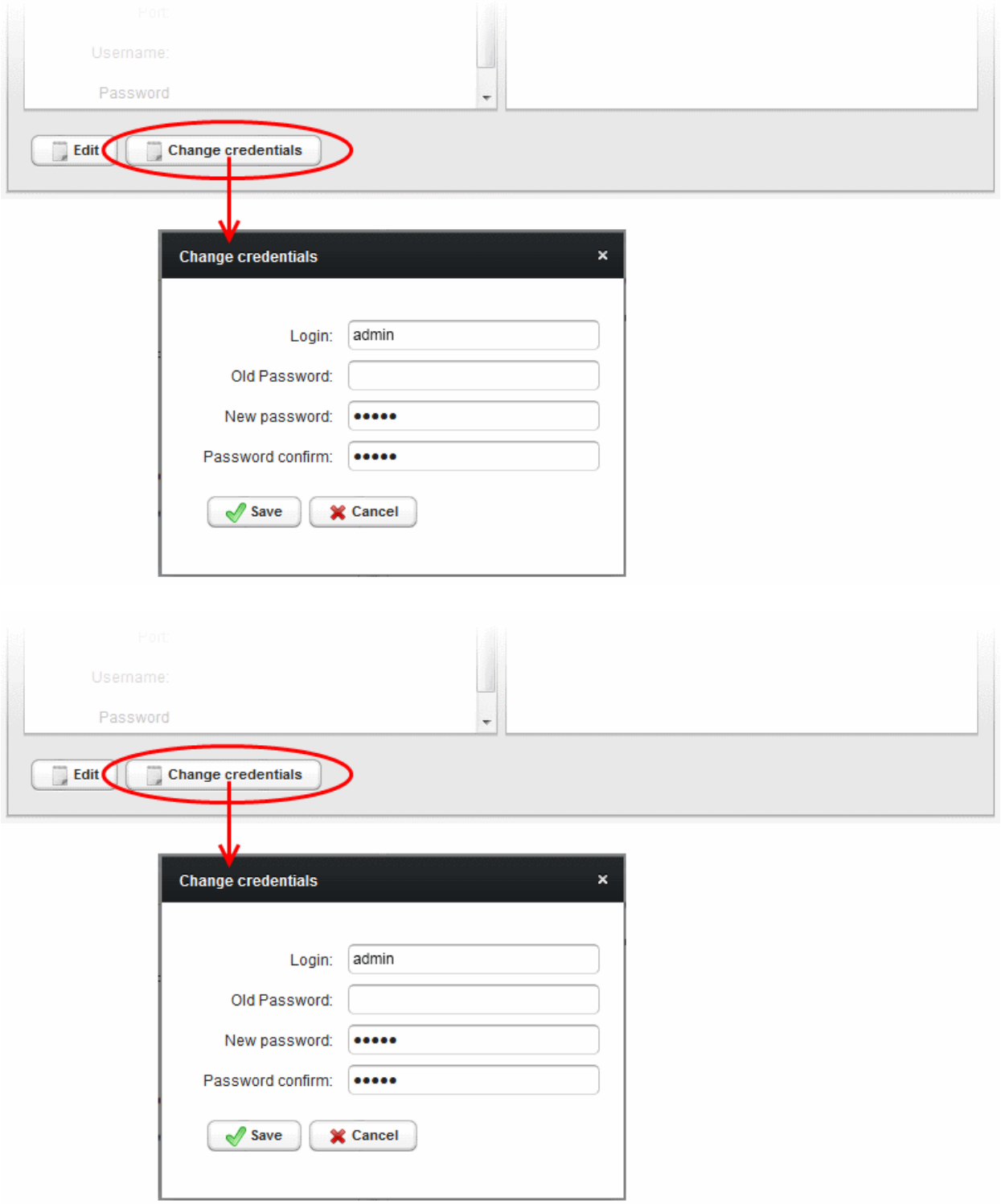
Changing Login Credentials for the Agents Configuration Console

By default, the administrator can use the username and password of their CCM 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.

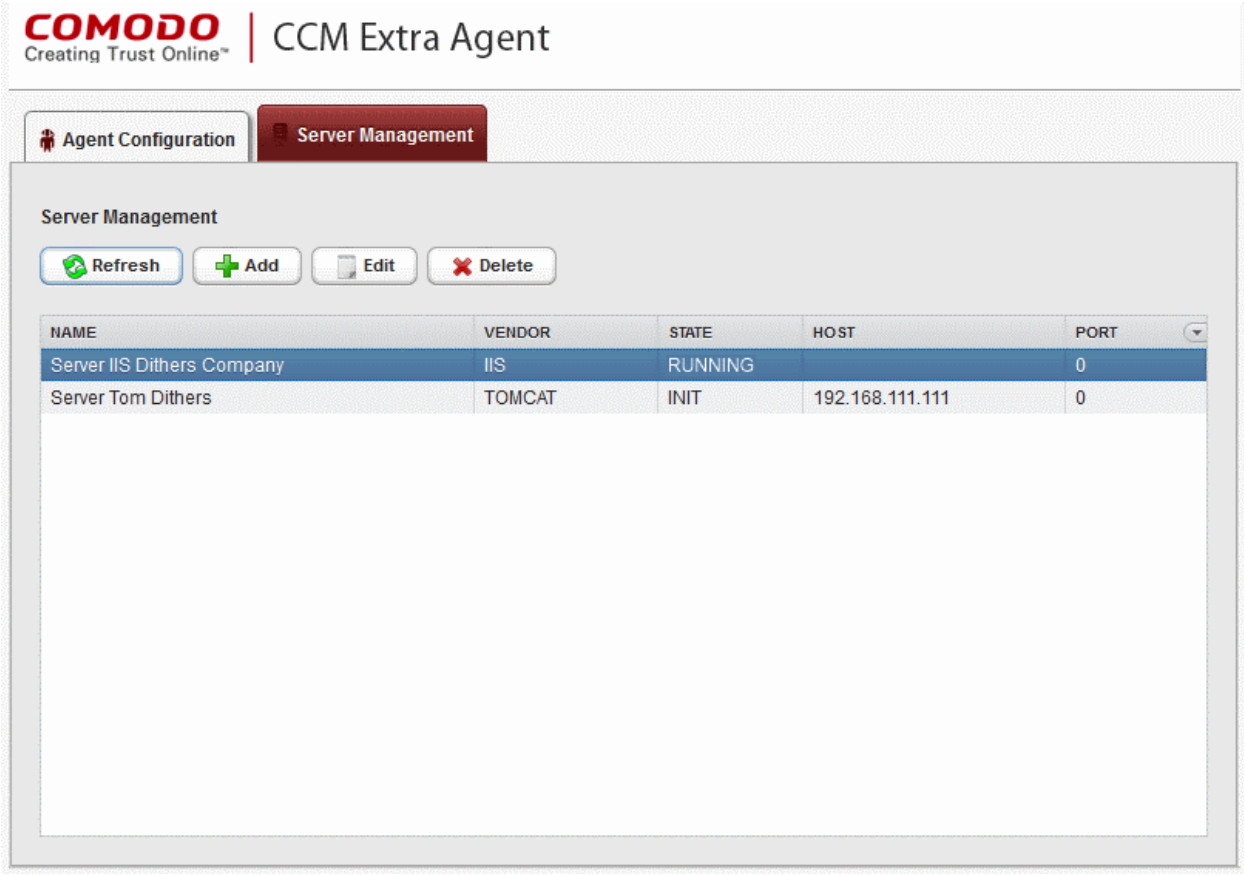


- To change your username, directly edit the Login field
- Enter your existing password in the 'Old Password' field
- Enter your new password in the New password field and reenter it for confirmation in the Password Confirmation field
- Click 'Save'

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

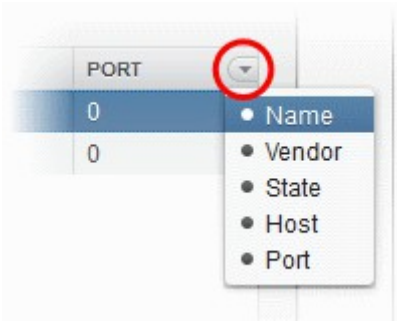
Server Management

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.

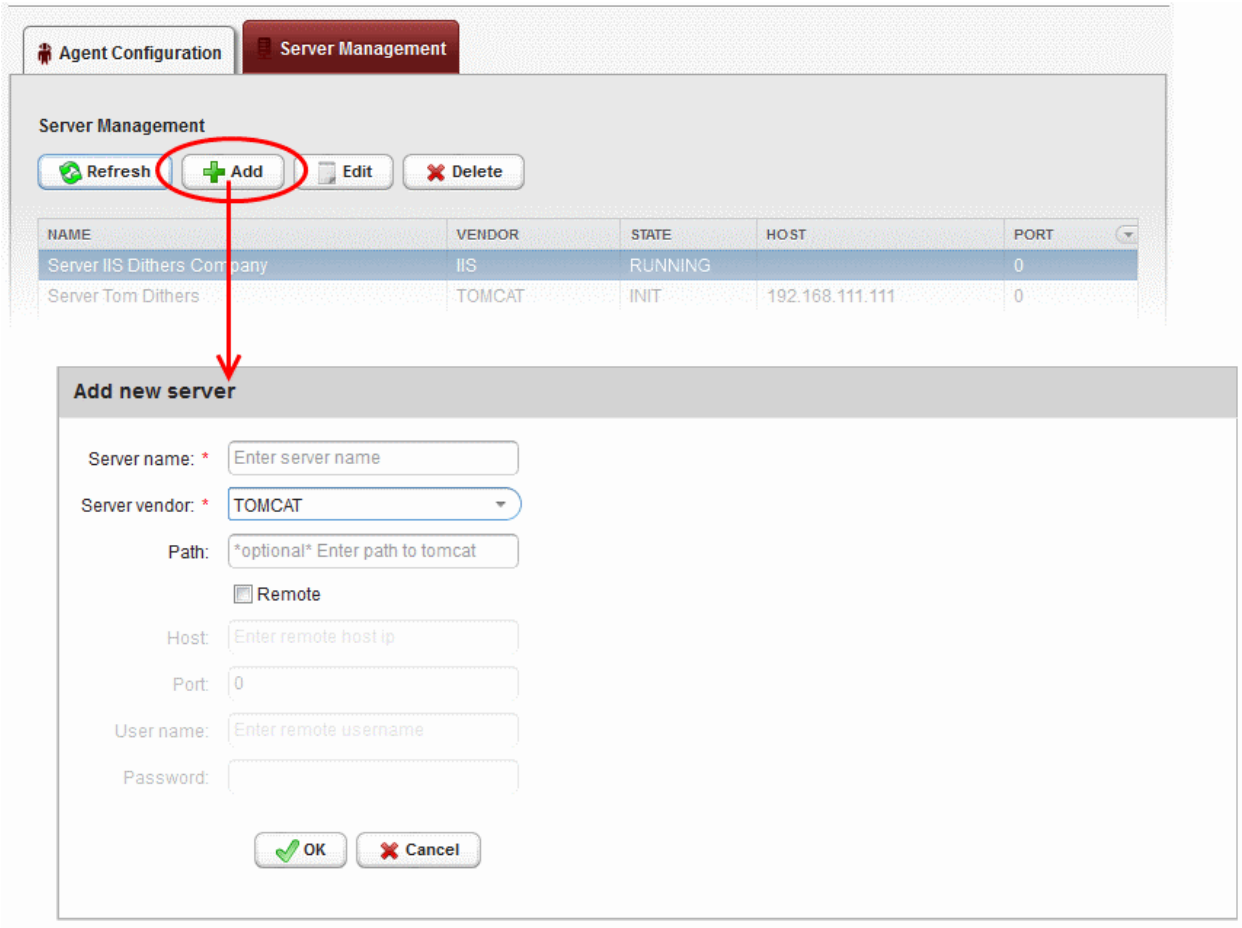
Column Display	Description
Name	Displays the name of the server.
Vendor	Displays the vendor of the server.
State	Indicates whether or not the server is initialized.
Host	Displays the IP address or the host name of the server for remote connection
Port	Displays the connection port of the server for remote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



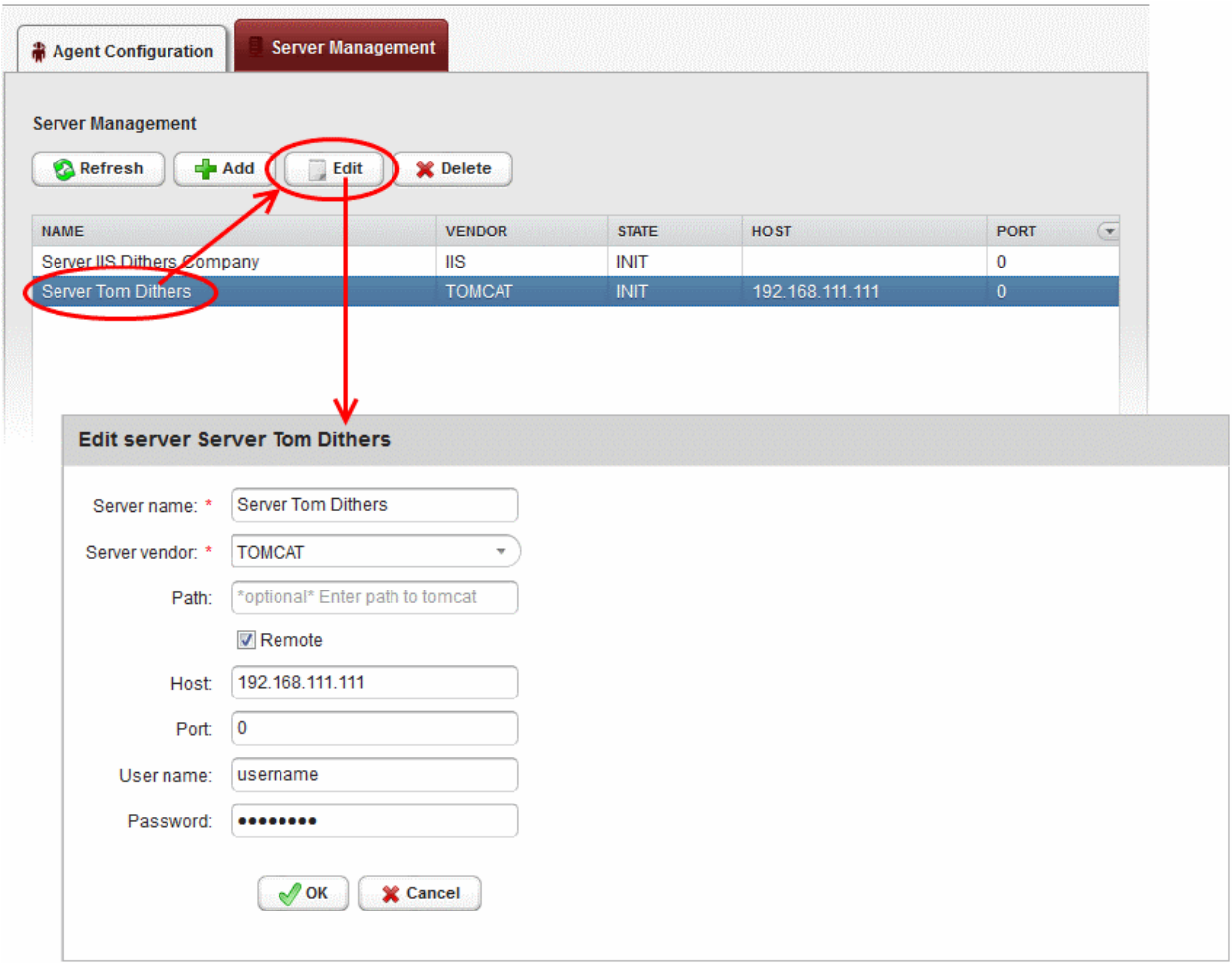
Add new server - Table of Parameters		
Field Name	**Type**	**Description**
Server name	*String*	Enter the name of the server.
Server vendor	*drop-down*	Choose the vendor of the server from the drop-down.
Path	*String*	Specify the network path for the Tomcat server. This is required only if the Tomcat server is not accessible from the CCM 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. **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.

Next Steps:

To discuss the auto-installer further and/or set up a test environment, please contact Comodo.

Email: **EnterpriseSolutions@comodo.com**

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

Email: **EnterpriseSolutions@Comodo.com**

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton,

NJ 07013

United States

Tel: +1.877.712.1309

Tel: +1.888.256.2608

For additional information on Comodo - visit **http://www.comodo.com/**