COMODO
Creating Trust Online®

Comodo
Certificate Manager

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 Apache/ModSSL Tomcat, Microsoft 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' wizard.
- There are two modes of implementation:

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

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

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

Please see the table below for details of supported configurations:

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

- C - CCM Controller Mode (Local)
- E – Enterprise Controller Mode (Remote)

1. Enterprise Controller Mode
   i. Certificate controller software is installed on a host in your network. The controller will communicate with your remote web-hosts and will automatically apply for and install certificates on to them.
   ii. The controller periodically polls CCM 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 CCM interface. After approval, the agent will submit the CSR to Comodo CA and track the order number. After issuance, the controller will download the certificate and allow administrators to install it from the CCM interface.

   See 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 polls CCM 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 CCM interface. After approval, the agent will submit the CSR to Comodo CA and track the order number. After issuance, the agent will download the certificate and allow administrators to install it from the CCM interface.

   See Method 2 - CCM 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 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.

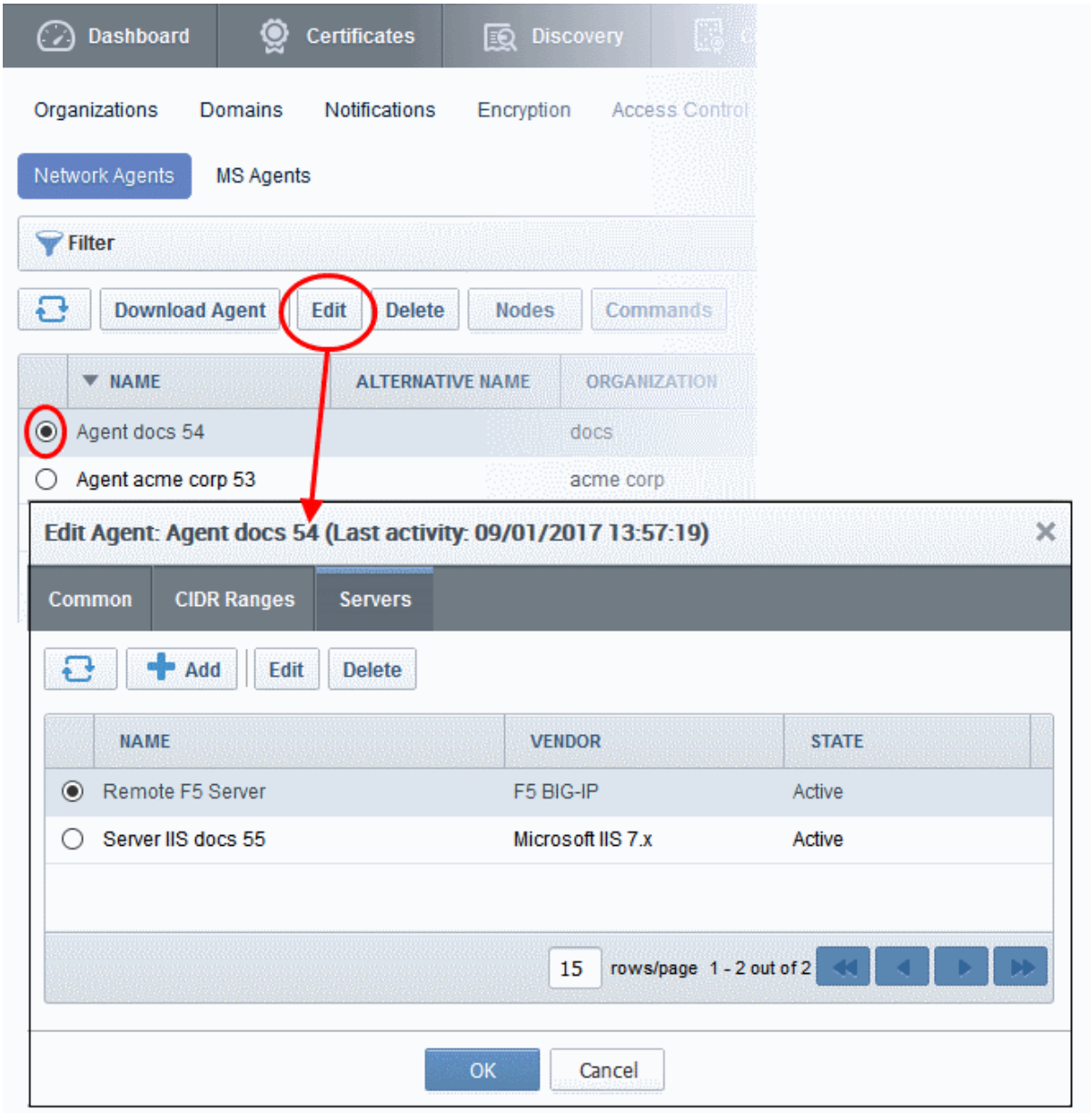
Method 1 - Enterprise Controller Mode

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

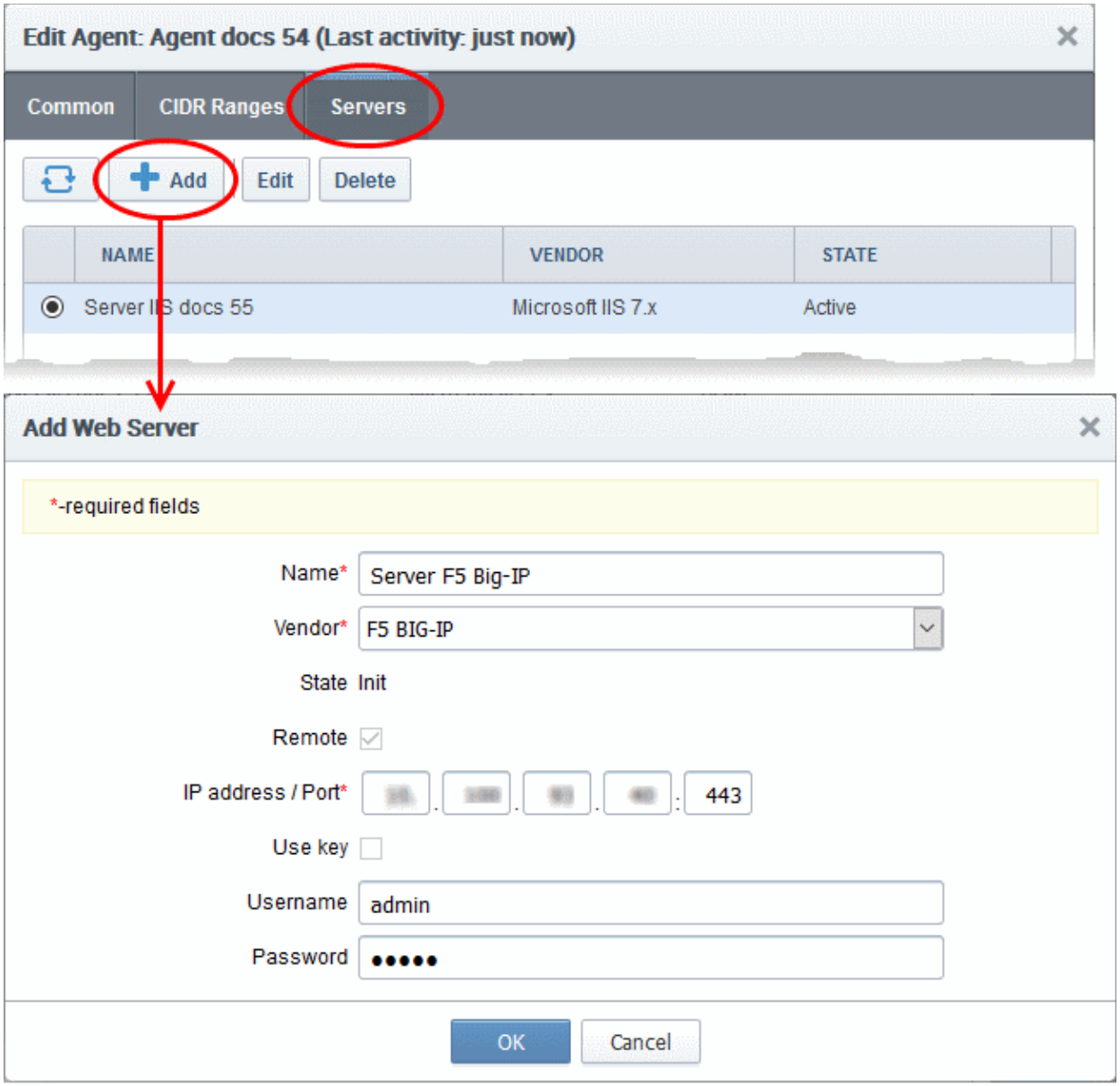
- Controller software first needs to be installed on a server in your network.
- You then need to add web-servers to the controller to enable certificate auto-installation. This is done in the 'Settings' > 'Agents' > 'Network Agents' interface. See the explanation below.
- If a new certificate is requested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

To add remote servers to the certificate controller

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



- The server(s) on which the controller is installed will be shown.
- Click 'Add' to associate a new remote server with the controller. The 'Add Web Server' dialog will open.

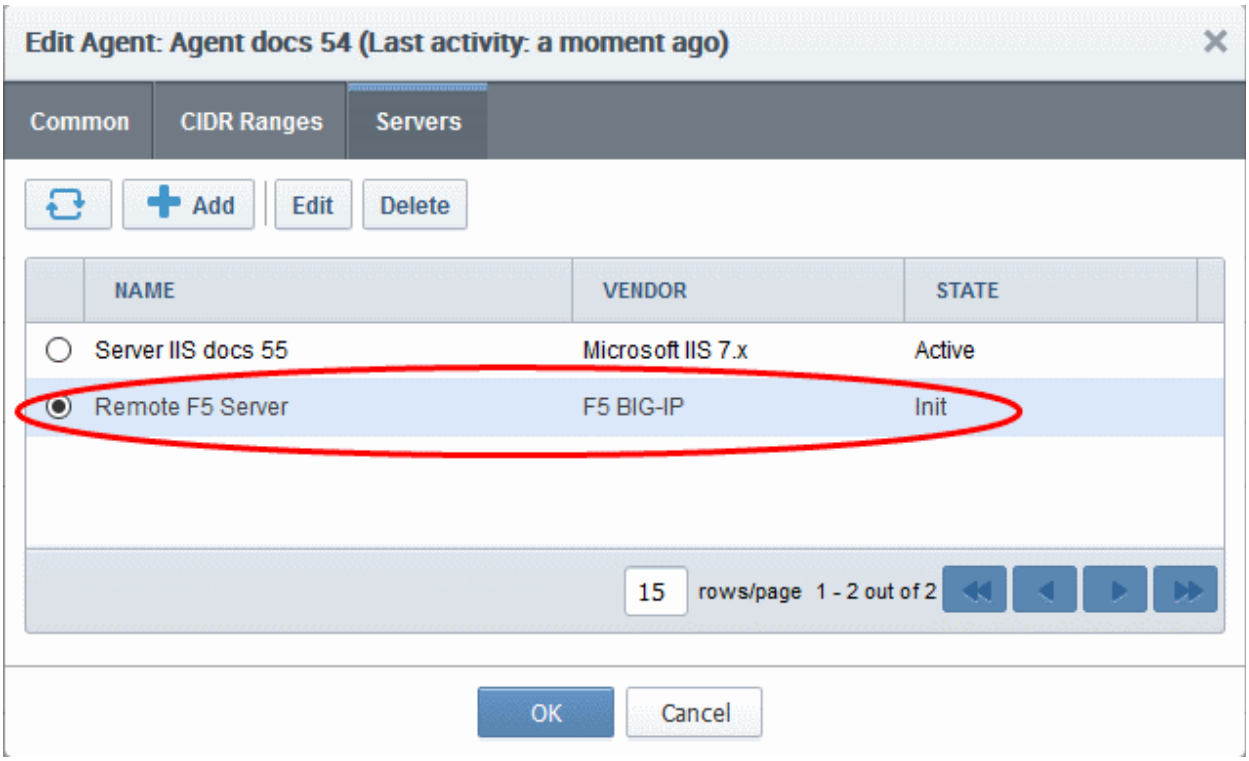


- Enter the server name, address and login details:

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.
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. Only required for Tomcat under Linux.
Remote	Checkbox	Specify whether the server is remote or local. This checkbox should be selected when adding remote servers for agent-less automatic certificate installation.

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

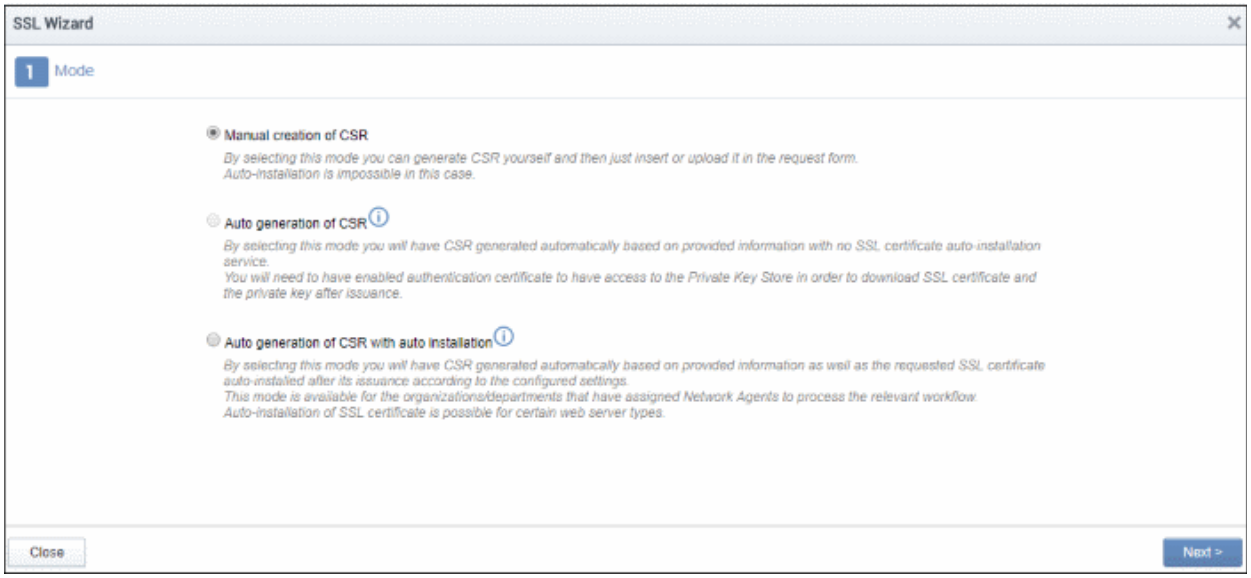
- Complete the form and click 'OK'. The server will be added to the controller. It will take a few minutes for the server to become 'Active'.



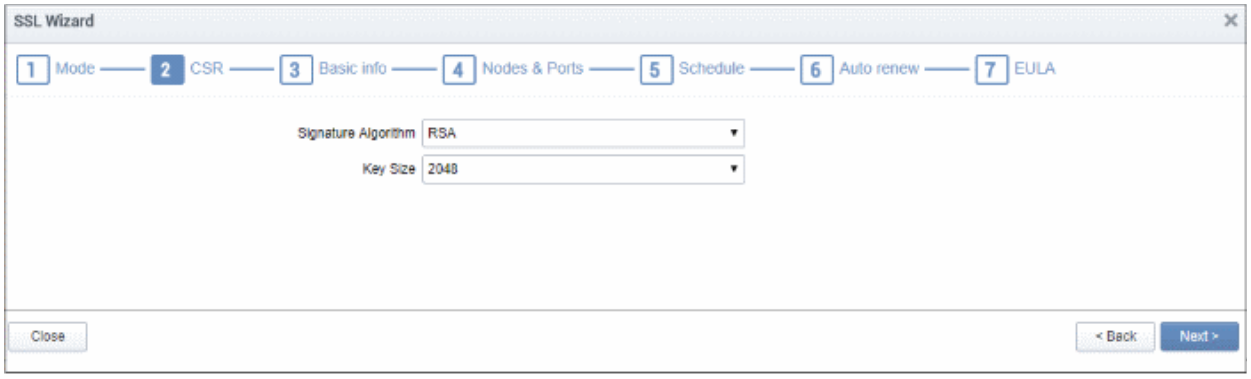
- Repeat the process to add more remote servers
- Once all servers have been successfully added to the controller, you can apply for certificates for domains on the server. Go to 'Certificates' > 'SSL Certificates' to apply for new certificates.

To enroll a certificate for auto-installation

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

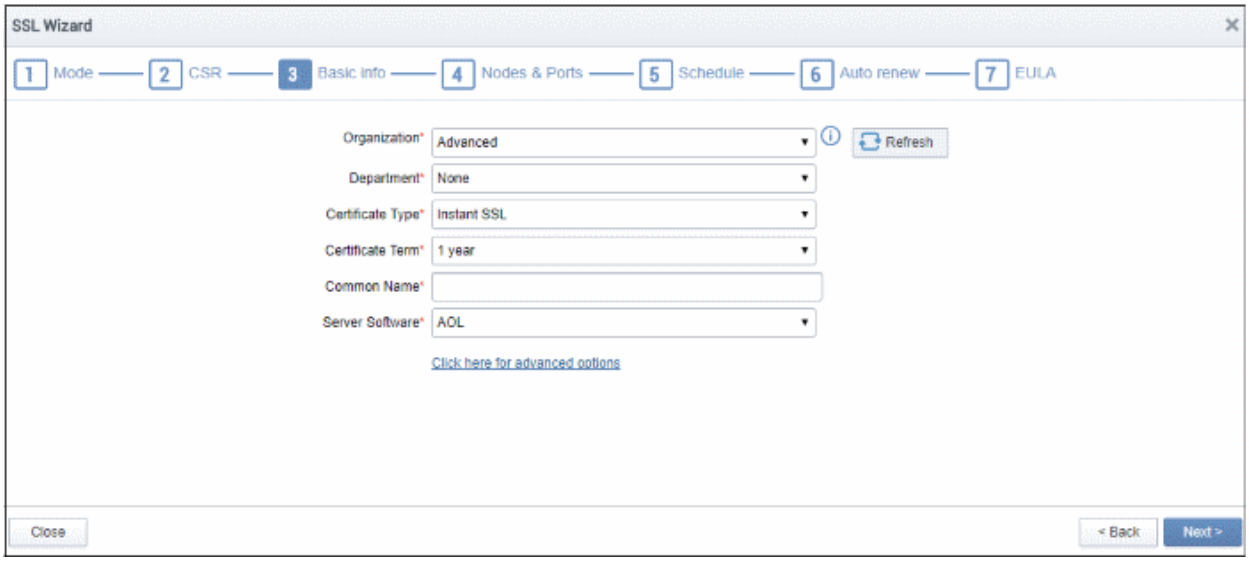


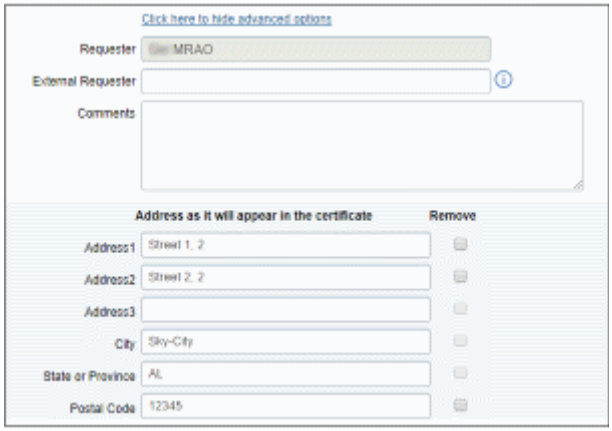
- Select the third option, 'Auto generation of CSR with auto installation', and click 'Next'.



The next step is to provide the CSR parameters:

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

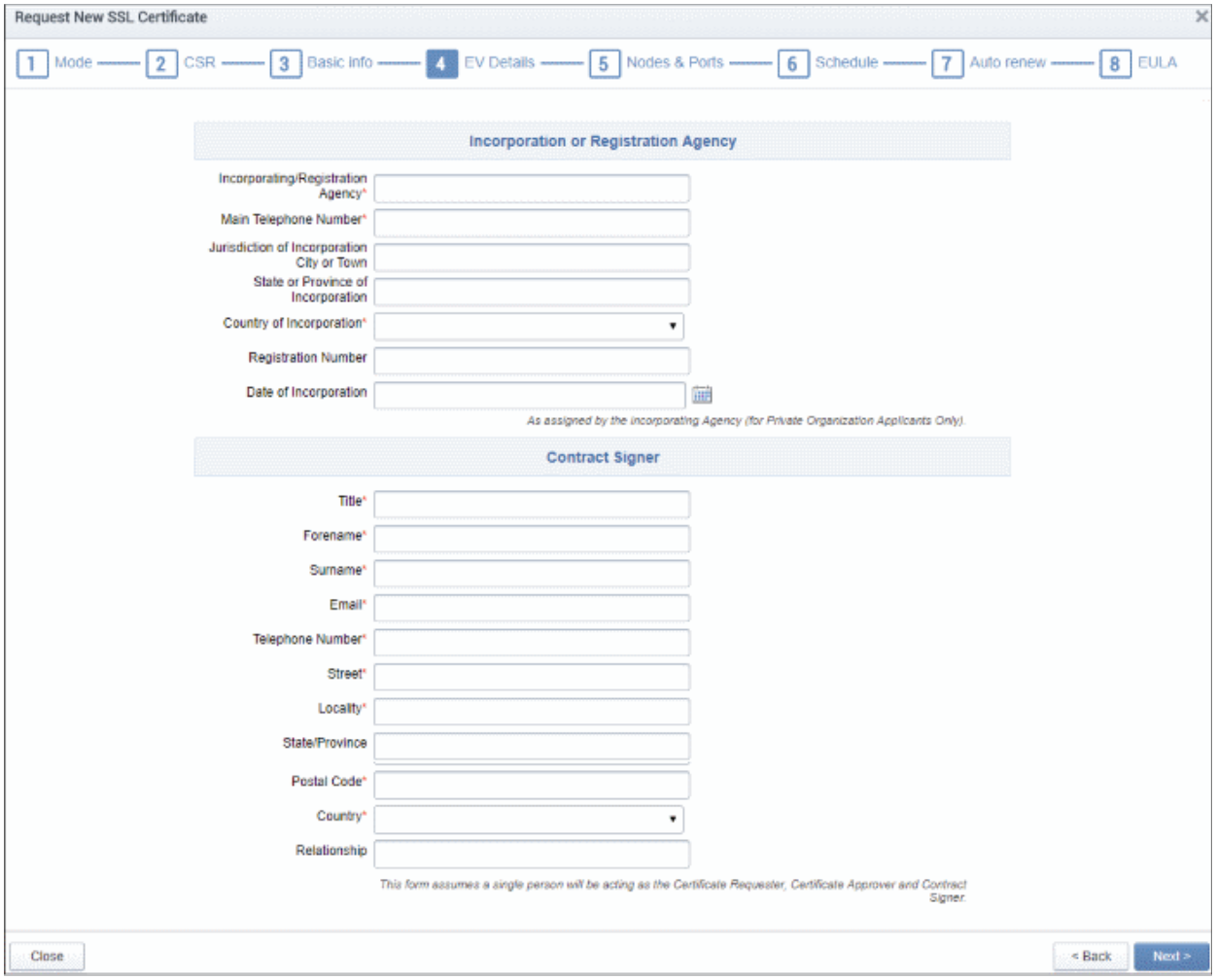


Form Element	Type	Description
Organization (*required*)	Drop-down list	Choose the organization that the SSL certificate will belong to.
Department (*required*)	Drop-down list	Choose the department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'.
Certificate Type (*required*)	Drop-down list	Choose the certificate type that you wish to add for auto-installation.
Certificate Term (*required*)	Drop-down list	Choose the validity period of the certificate. For example, 1 year, 2 years, 3 years.
Common Name (*required*)	Text Field	Type the domain that the certificate will be issued to.
Server Software (*required*)	Drop-down list	Select the server software on which the certificate is to be installed. **Note**: Choose 'OTHER' if you want to use F5 BIG-IP.
Subject Alternative Names (*optional*)	Text Field	This field appears only if a multi domain or UCC certificate type is selected. Specify the additional domain names. Each domain name should be separated by a comma.
Click here for advanced options	Text Fields	Clicking this link will expand the advanced options: 

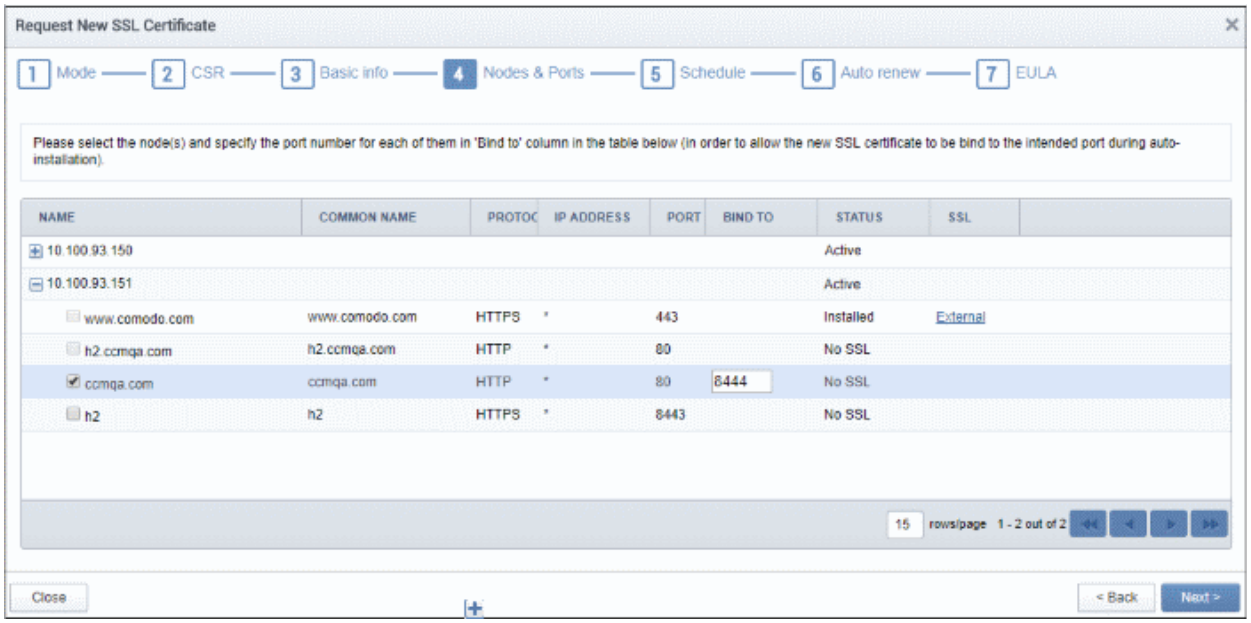
Form Element	Type	Description
		• Requester – This field is auto-populated with the name of the administrator making the application. • External Requester (optional) - Enter the email address of an external requester on whose behalf the application is made. Note: The 'Requester' will still be the administrator that is completing this form (to view this, open the 'Certificates Management' area and click 'View' next to the certificate in question). The email address of the 'External Requester' will be displayed as the 'External Requester' in the 'View' dialog of an issued certificate. • Comments (optional) - Enter your comments on the certificate. **Address fields in the certificate** • The address fields are auto-populated from the details of the Organization or Department on whose behalf this certificate request is being made. • These fields cannot be modified but, in the case of OV level certificates, the administrator can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields. • The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted". For EV level certificates, it is mandatory to include and display address details of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down.

- Click 'Next'

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

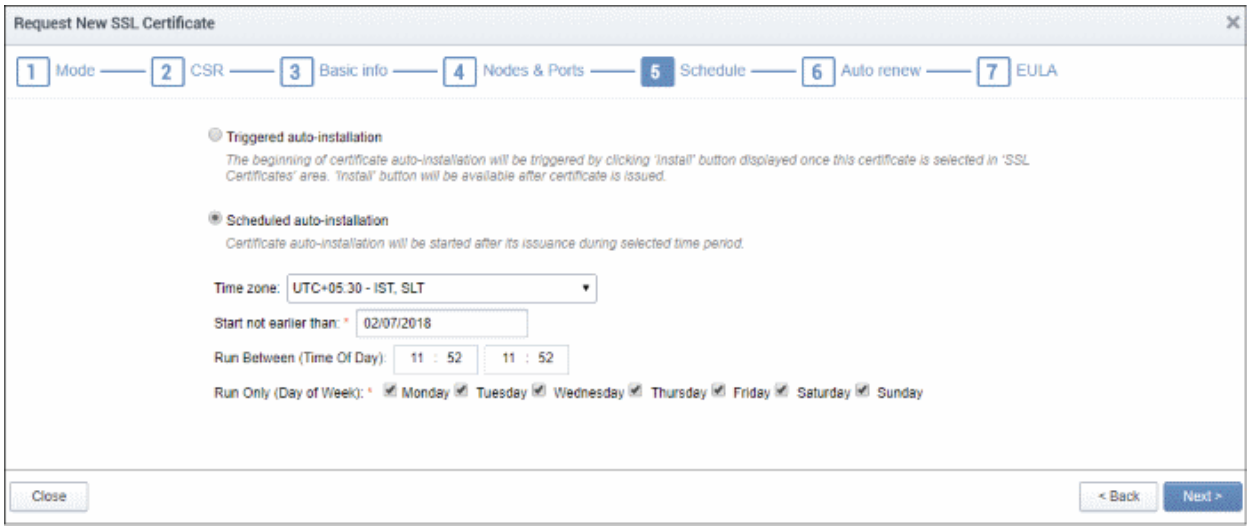


- The details you need to complete depends on the EV mode activated for your account.
- This is same information as provided in the EV details tab when adding a new organization. If the EV type is 'RA' for your account, this will be auto-populated.
- Click 'Next' when all required fields are complete.



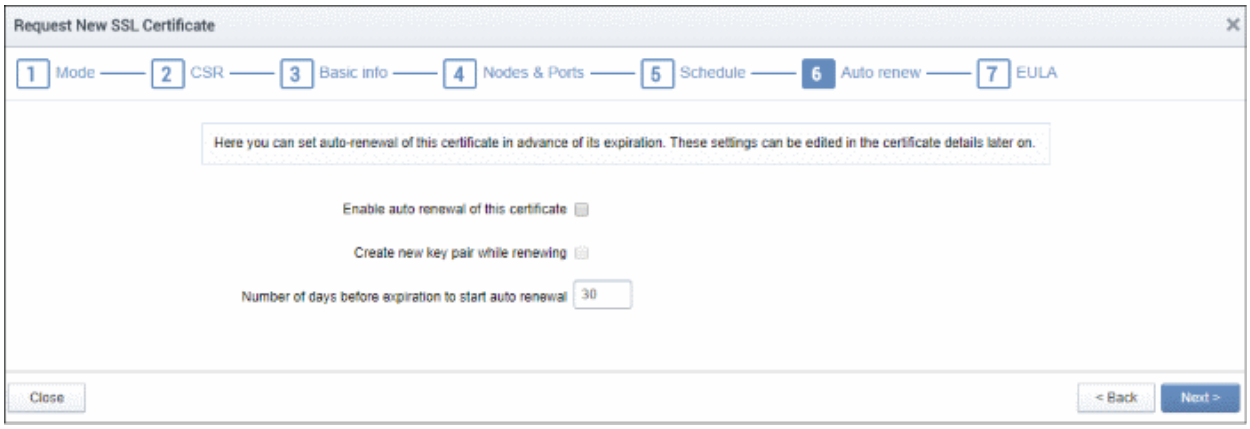
The 'Nodes & Ports' wizard displays the configured options.

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



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

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

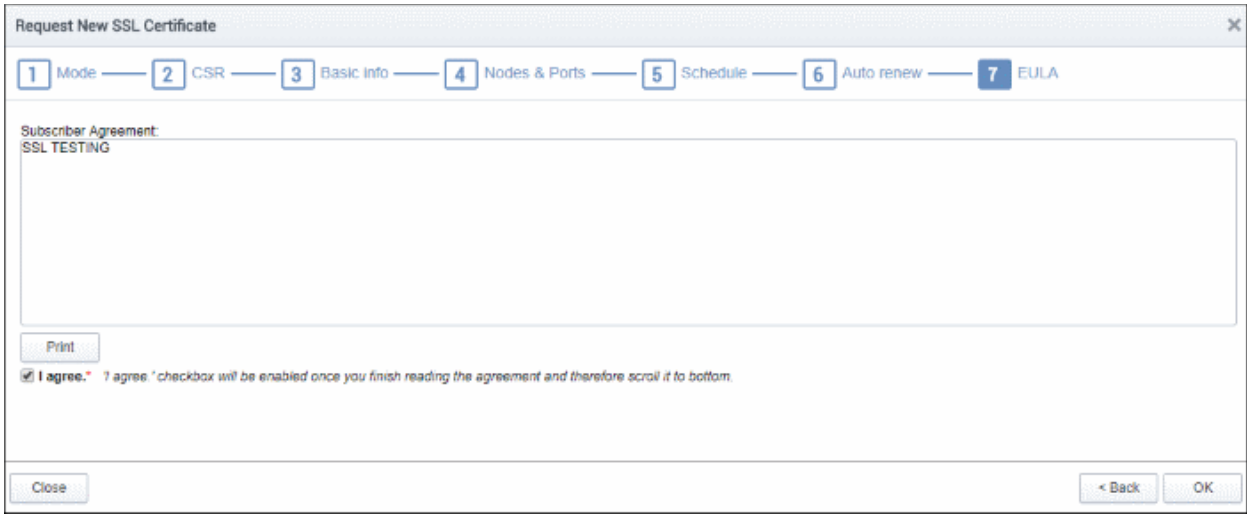


The next step is to configure the auto-renewal options.

- **Enable auto renewal of this certificate** – Select this to have CCM apply for a new certificate when this one approaches expiry.
- **Create new key pair while renewing** – If the option above is selected, then choose whether or not you want a generate a new key pair for the renewed certificate. Leaving it disabled means CCM will re-use the key pair of the old certificate.
- **Number of days before expiration to start auto renewal** - Choose the number of days in advance of

expiry that the renewal process should start. On the scheduled day, the certificate controller will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.

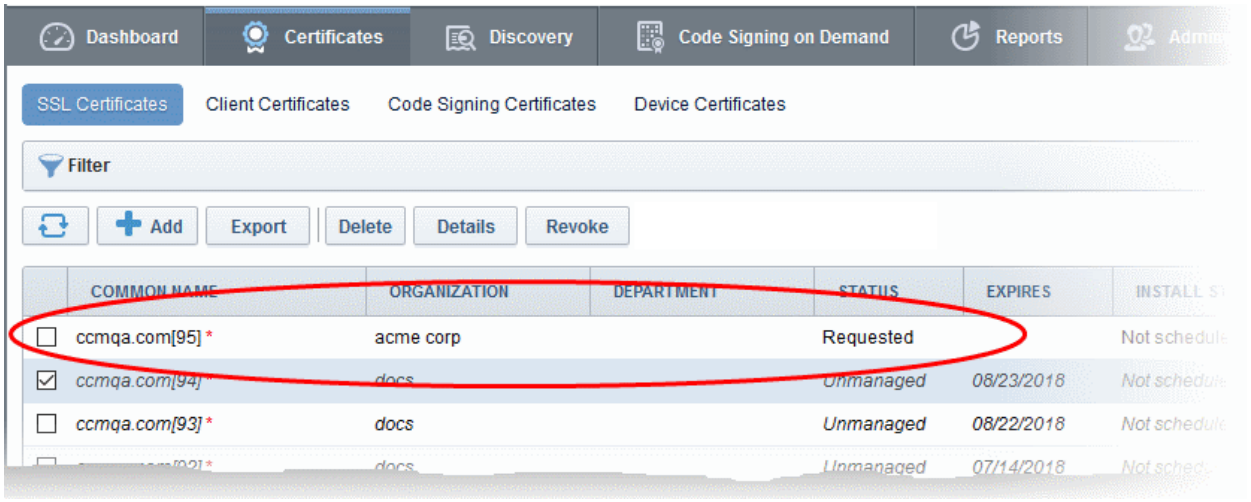
- Click 'Next'



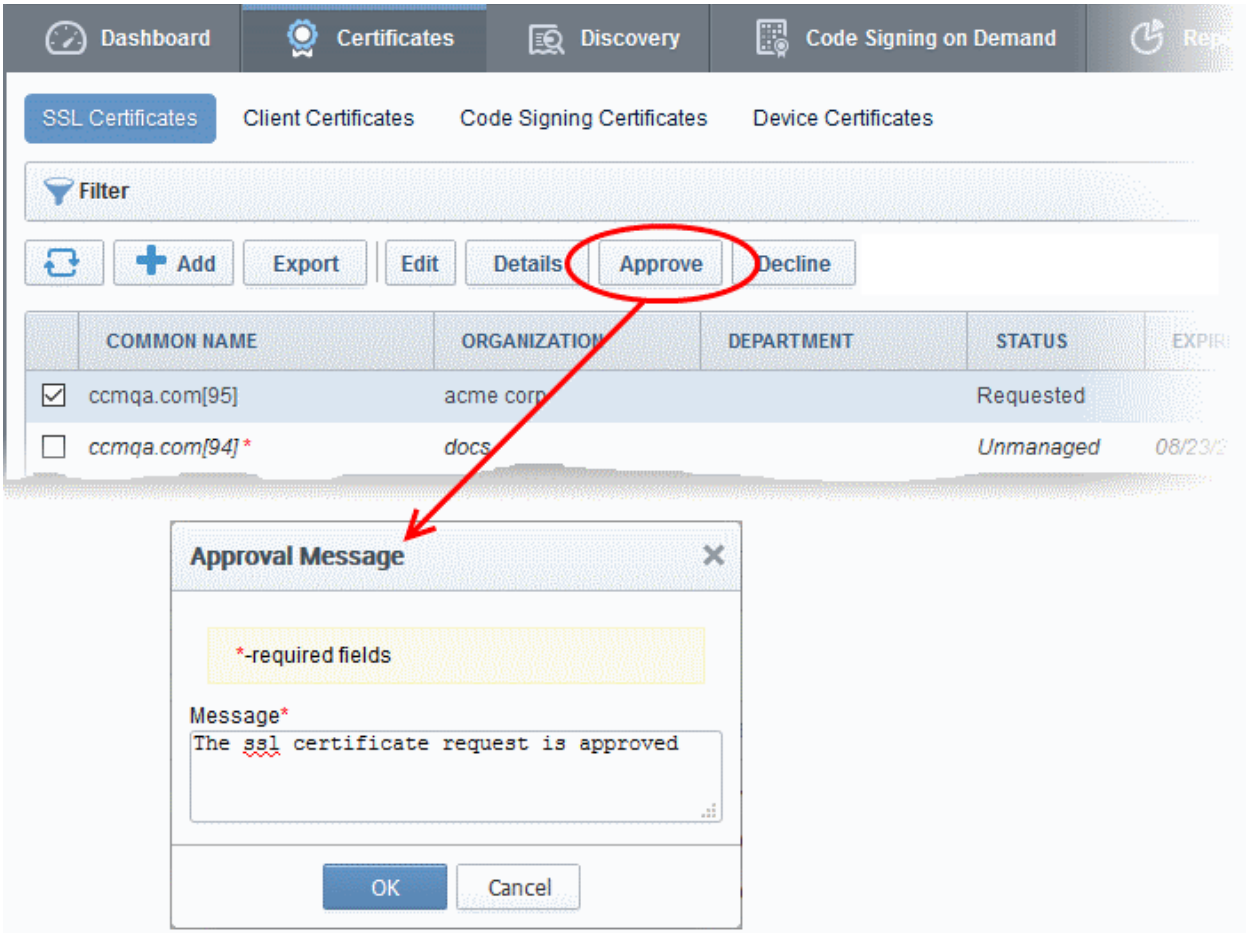
The final stage is to agree to the EULA.

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

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

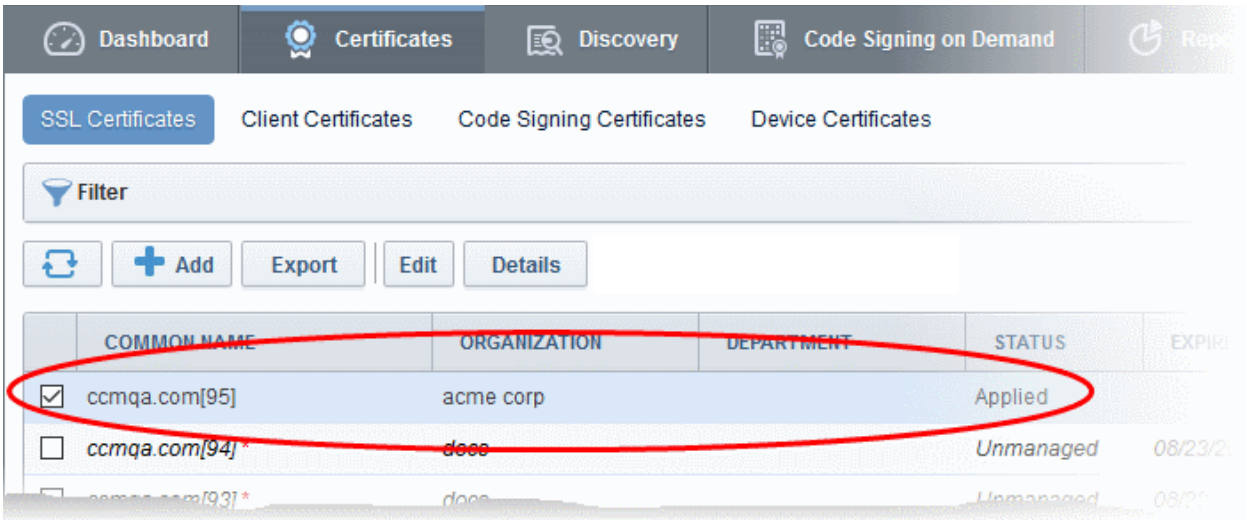


- The CSR for the requested certificate will be generated automatically. After the CSR has been created, the 'Approve' button will appear at the top when you select the certificate in the list:

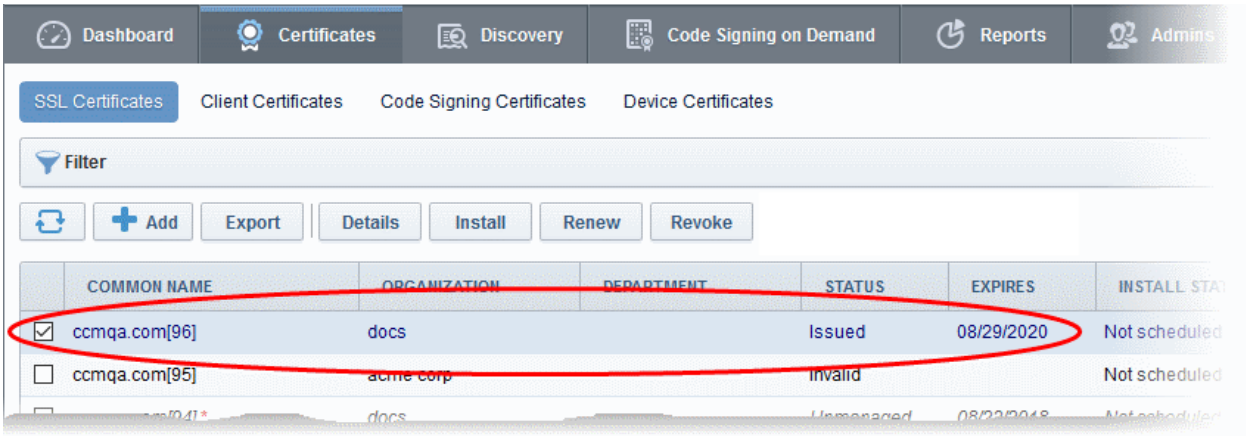


- Click the 'Approve' button to approve the request, enter an approval message and click 'OK'.

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



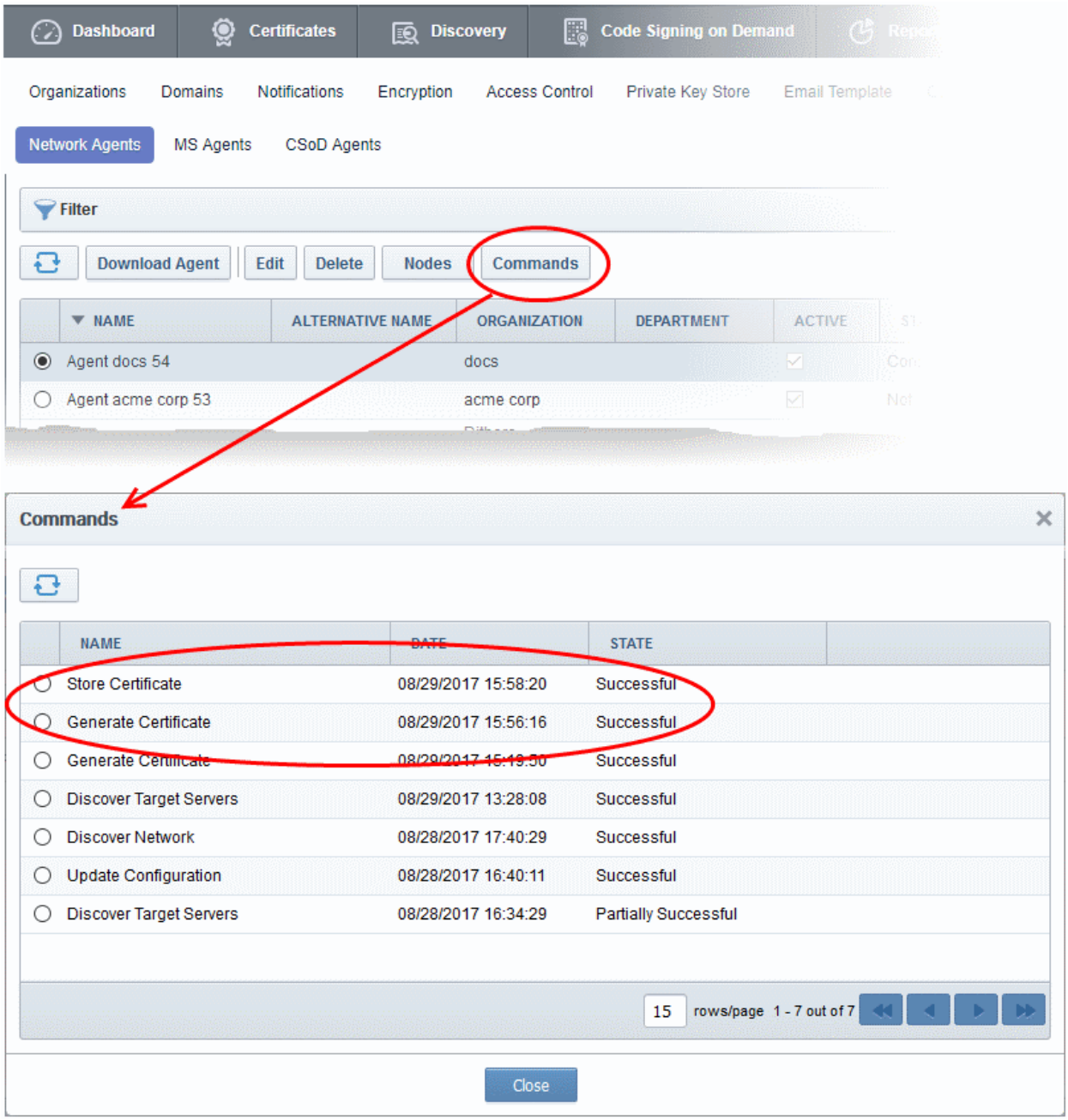
The controller will track the order number and will download the certificate once it is issued. The certificate will stored and its status will change to 'Issued'.



To check whether the certificate controller has stored the certificate:

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

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

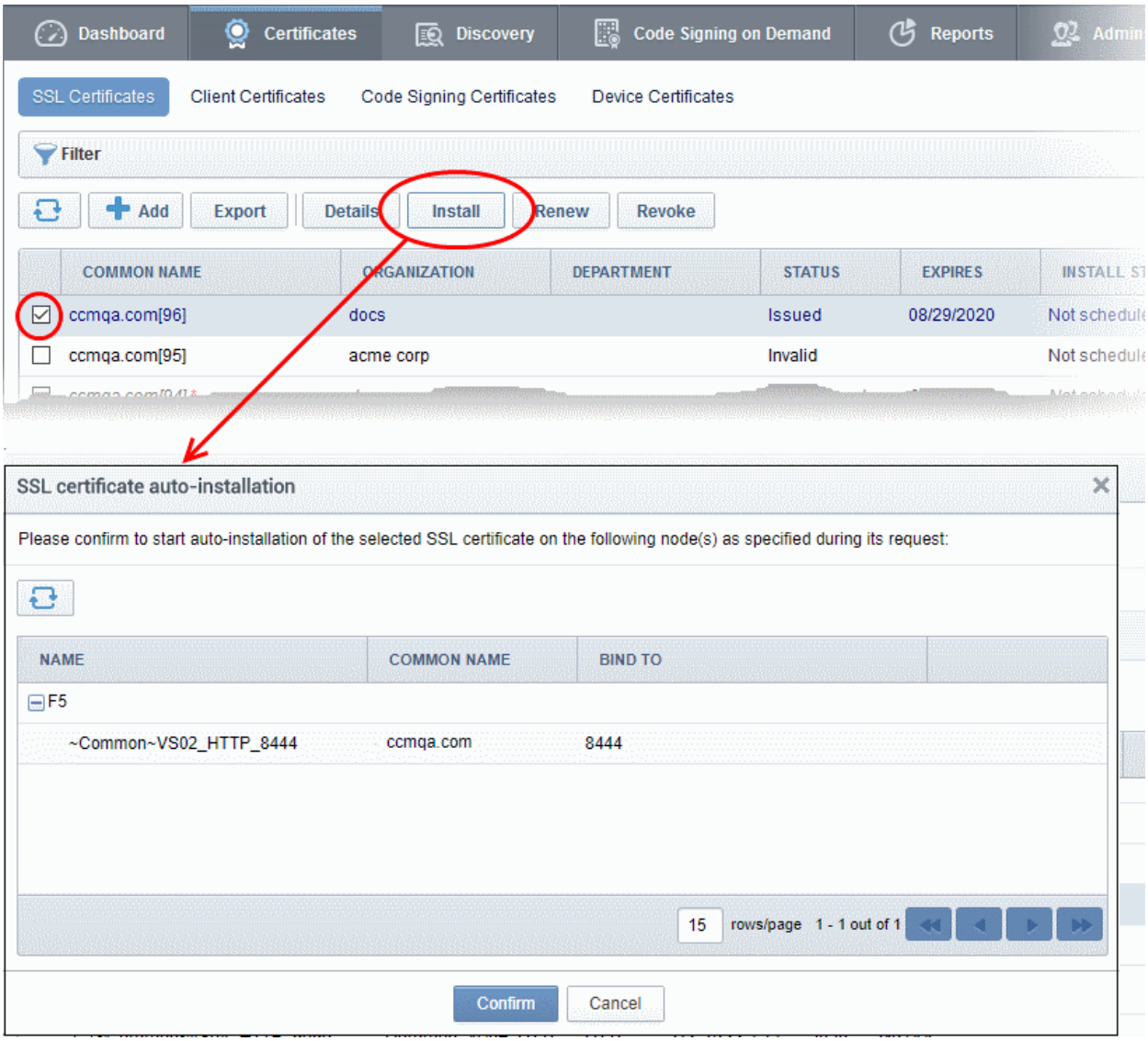


The certificate is stored on the server by the agent.

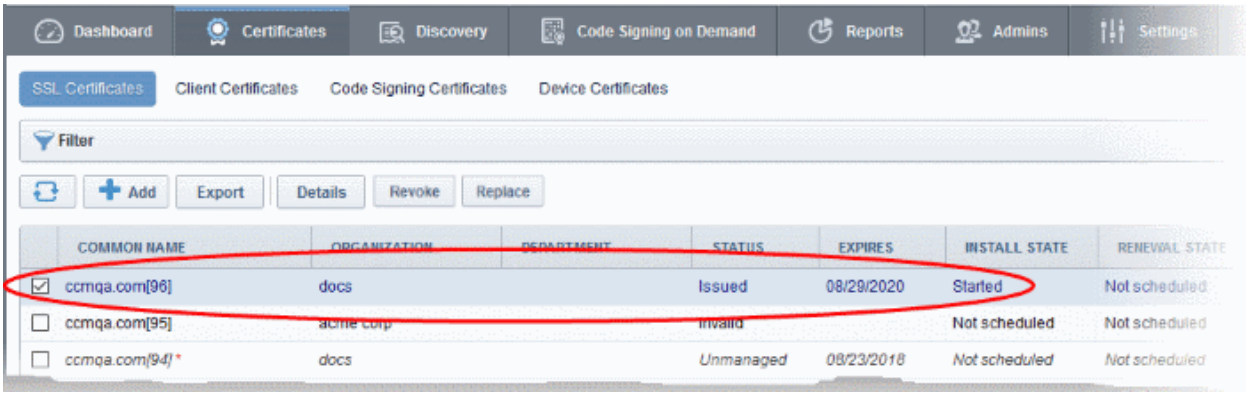
- If you set a schedule for automatic installation, it will be installed automatically at the scheduled time.
- If you selected 'Triggered auto-installation' you can manually initiate the installation process or schedule for auto-installation, from the 'Certificates' > 'SSL Certificates' interface of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

To manually initiate auto-installation of a certificate

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

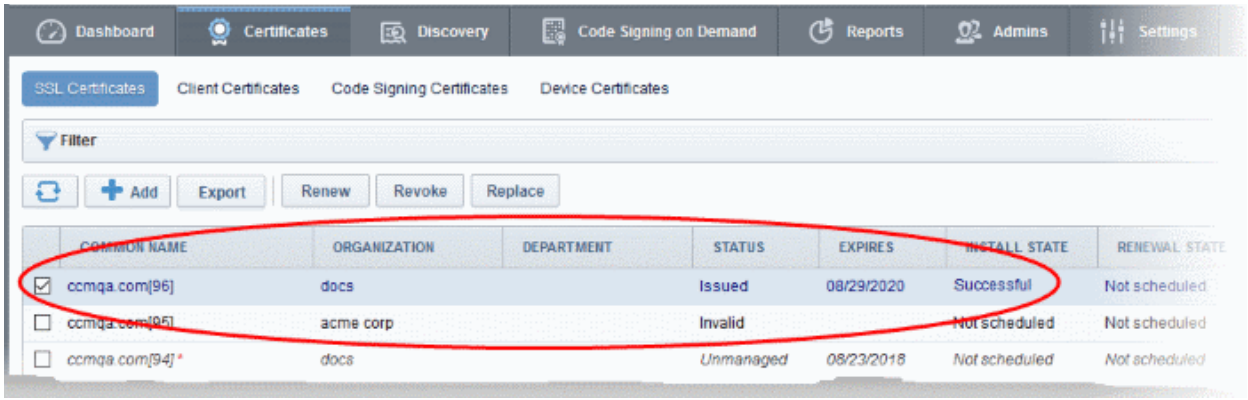


The certificate installation will begin instantly. Once the installation commences, the 'Install State' of the certificate will change to 'Started'.

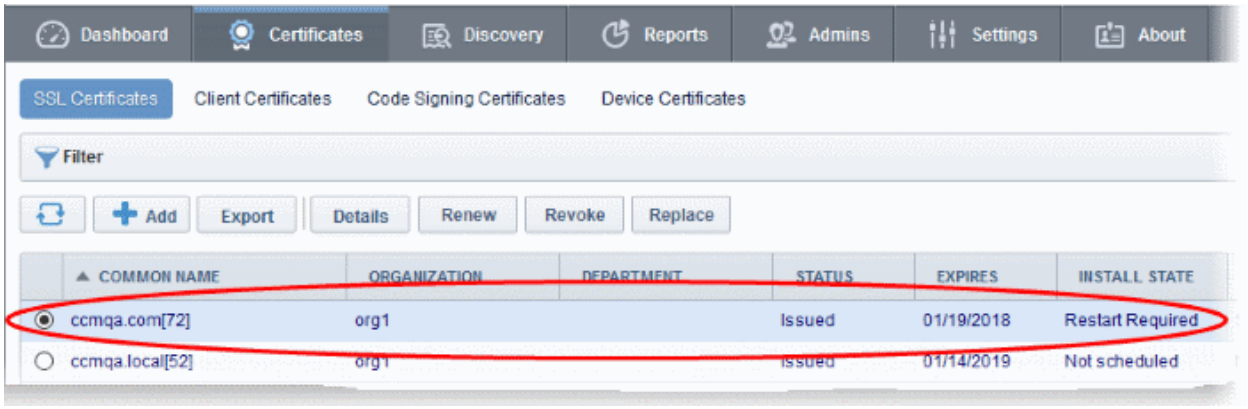


When installation is complete:

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

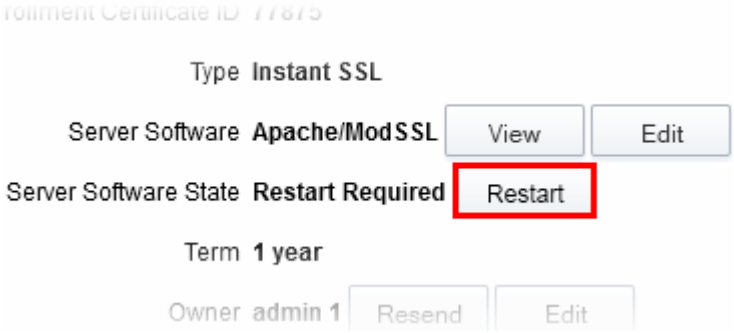


- **Apache** - The certificate will become active after the server is restarted. The install state will change to 'Restart Required'.



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

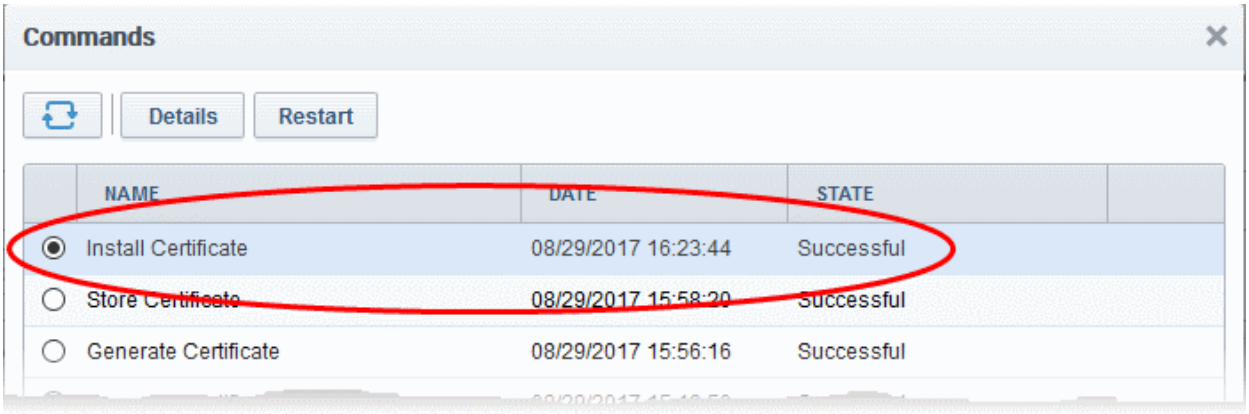
- Select the certificate and click the 'Details' button at the top. The 'Certificate Details' dialog will be displayed.
- Click 'Restart' beside the Server Software State field in the 'Details' dialog



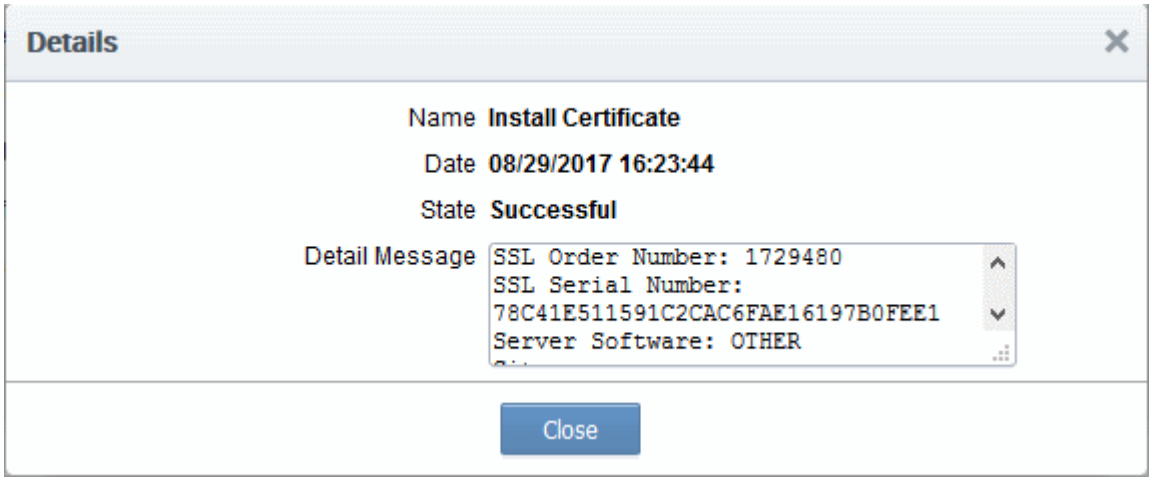
After restarting the server, the certificate will activated and the 'Install State' will change to 'Successful'.

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

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



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

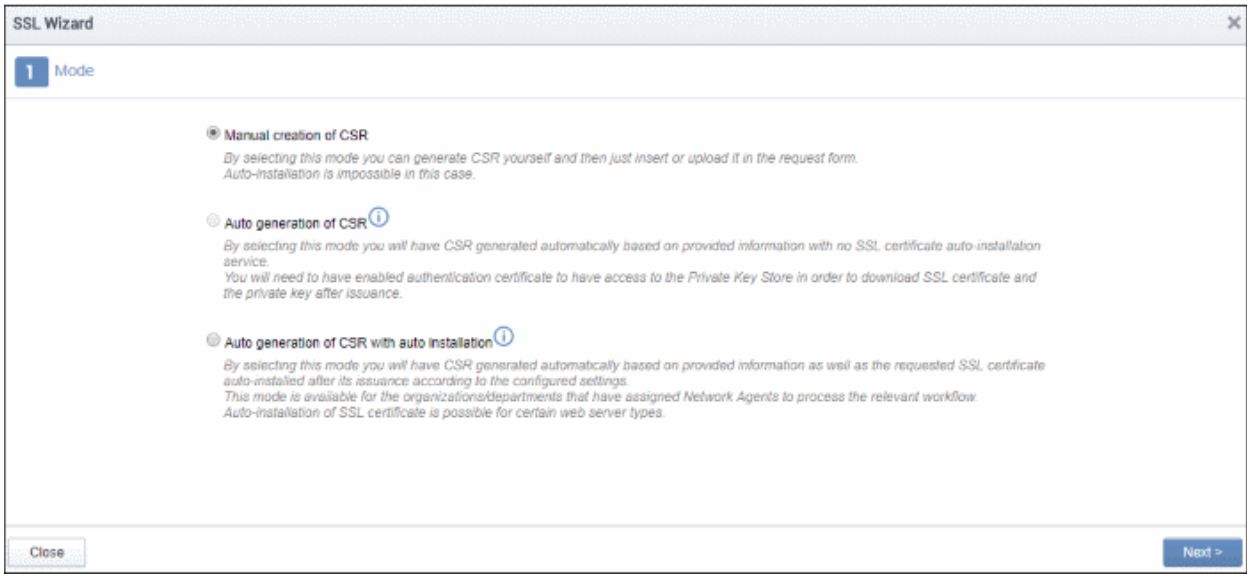


Method 2 - CCM Controller Mode

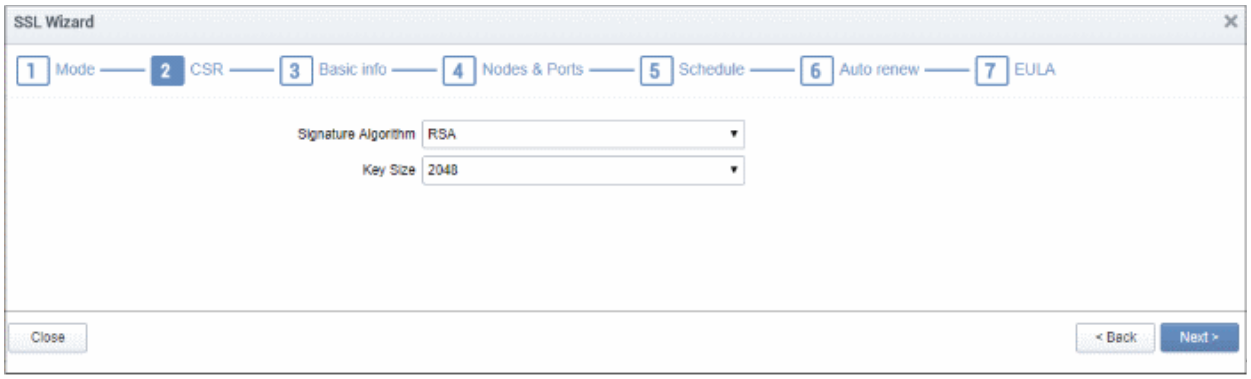
- Administrators can request and install new certificates for domains hosted on different web servers from the 'Certificate Management - SSL Certificates' area.
- 'CCM Controller Mode' requires an agent to be installed on each web server upon which the certificates are to be auto-installed/renewed.

To enroll a certificate for auto-installation

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

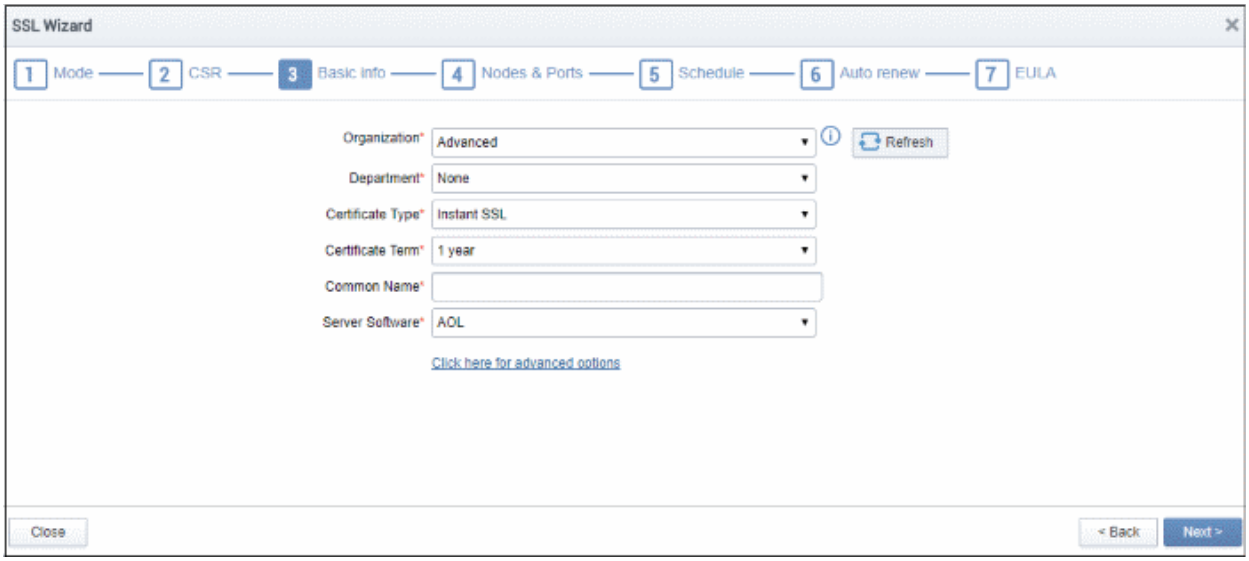


- Select the third option, 'Auto generation of CSR with auto installation', and click 'Next'.

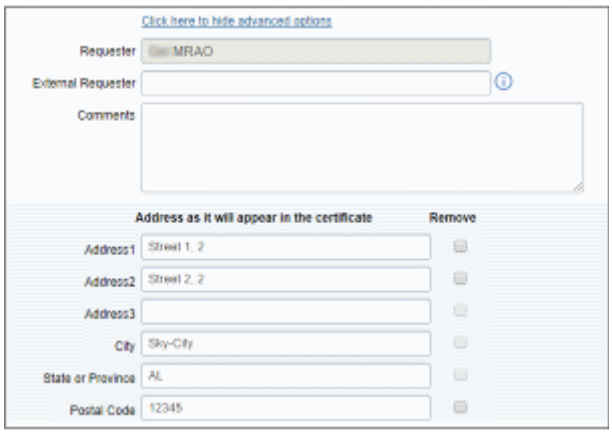


The next step is to provide the CSR parameters:

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

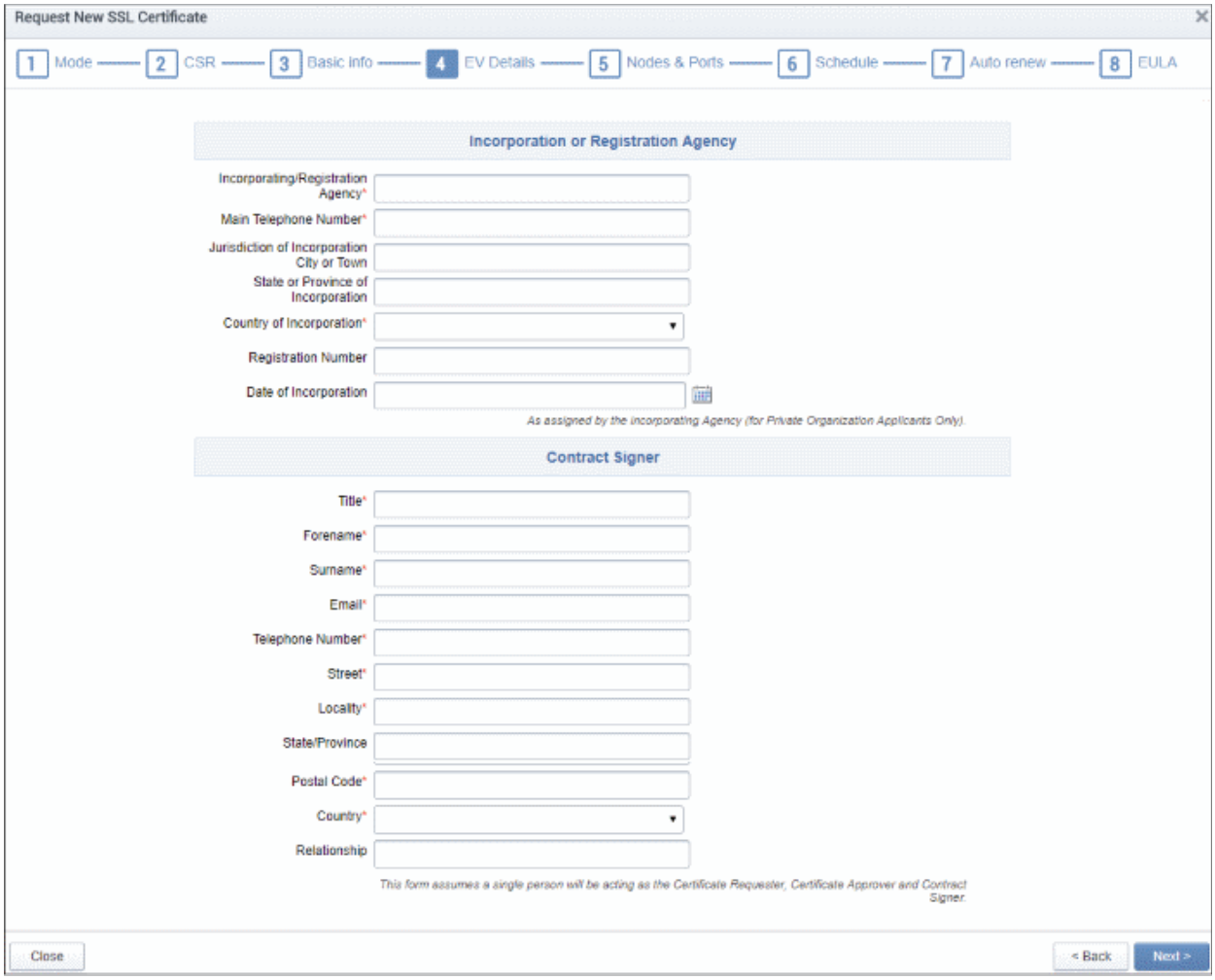


Form Element	Type	Description
Organization (*required*)	Drop-down list	Choose the organization that the SSL certificate will belong to.
Department (*required*)	Drop-down list	Choose the department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'.
Certificate Type (*required*)	Drop-down list	Choose the certificate type that you want to auto-install. The certificate types shown in the drop-down depend on the 'SSL Types' allowed for the organization.
Certificate Term (*required*)	Drop-down list	Choose the validity period of the certificate. For example, 1 year, 2 years, 3 years.
Common Name (*required*)	Text Field	Type the domain that the certificate will be issued to.
Server Software (*required*)	Drop-down list	Select the server software on which the certificate is to be installed. Note: Choose 'OTHER' if you want to use F5 BIG-IP.
Subject Alternative Names (*optional*)	Text Field	This field appears only if a multi domain or UCC certificate type is selected. Specify the additional domain names. Each domain name should be separated by a comma.
Click here for advanced options	Text Fields	Clicking this link will expand the advanced options:

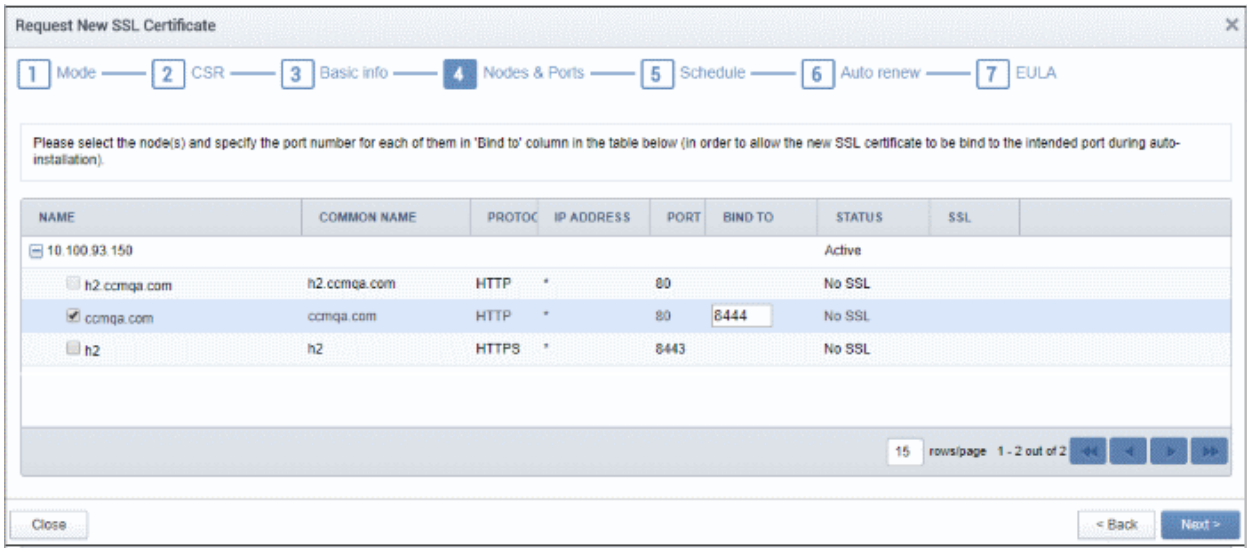
Form Element	Type	Description
		 • Requester – This field is auto-populated with the name of the administrator making the application. • External Requester (optional) - Enter the email address of an external requester on whose behalf the application is made. Note: The 'Requester' will still be the administrator that is completing this form (to view this, open the 'Certificates Management' area and click 'View' next to the certificate in question). The email address of the 'External Requester' will be displayed as the 'External Requester' in the 'View' dialog of an issued certificate. This field is not required when requesting for EV SSL certificate and hence will be hidden. • Comments (optional) - Enter your comments on the certificate. **Address fields in the certificate** • The address fields are auto-populated from the details in the 'General Properties' tab of the organization or department on whose behalf this certificate request is being made. • These fields cannot be modified but, in the case of OV level certificates, the administrator can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields. • The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted". For EV level certificates, it is mandatory to include and display address details of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down.

- Click 'Next'

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



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



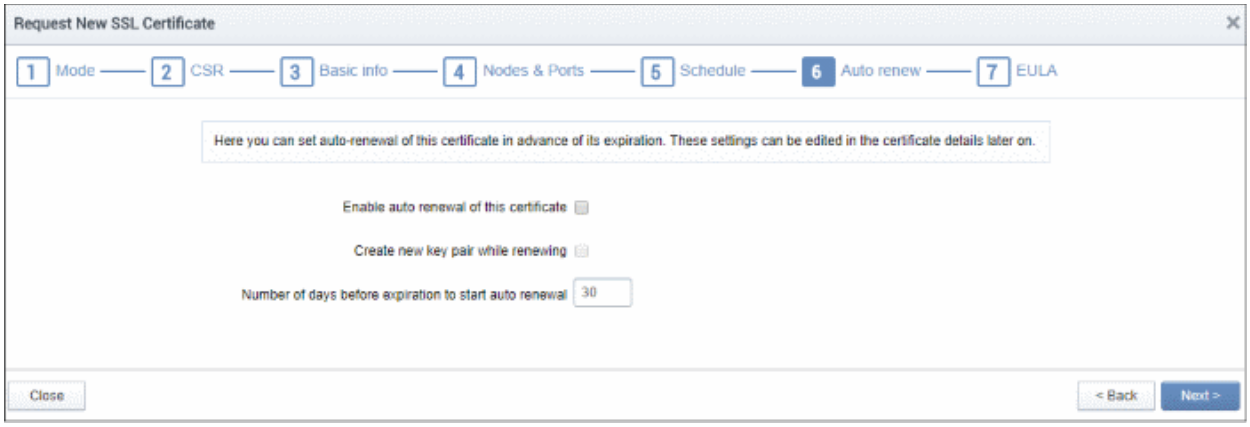
The 'Nodes & Ports' wizard displays the configured options.

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

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

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

- Click 'Next'.

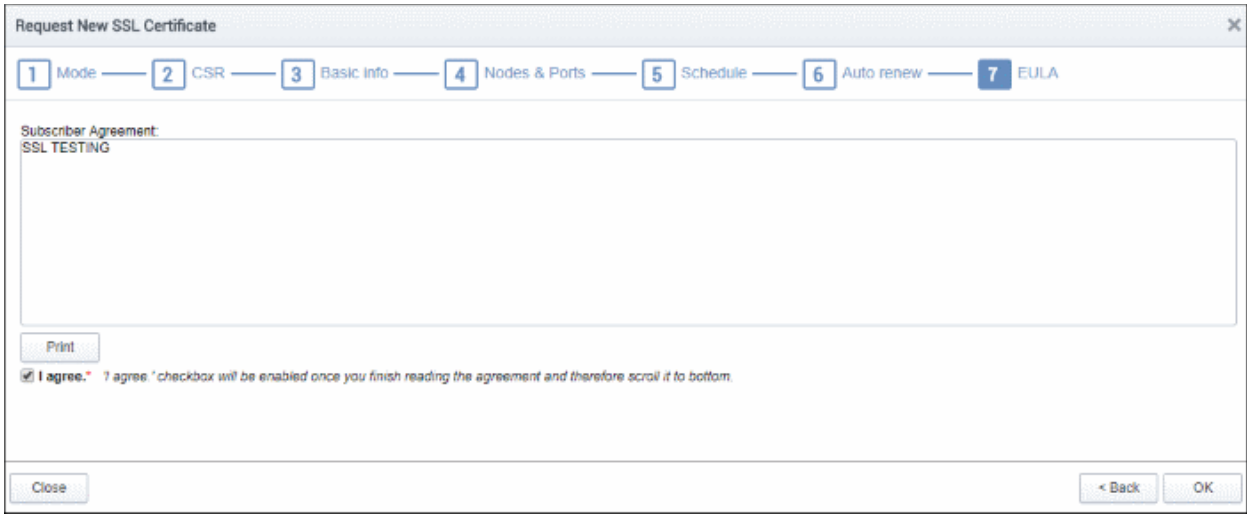


The next step is to configure the auto-renewal options.

- **Enable auto renewal of this certificate** – Select this to have CCM apply for a new certificate when this one approaches expiry.
- **Create new key pair while renewing** – If the option above is selected, then choose whether or not you want a generate a new key pair for the renewed certificate. Leaving it disabled means CCM will re-use the key pair of the old certificate.
- **Number of days before expiration to start auto renewal** - Choose the number of days in advance of

expiry that the renewal process should start. On the scheduled day, the certificate controller will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.

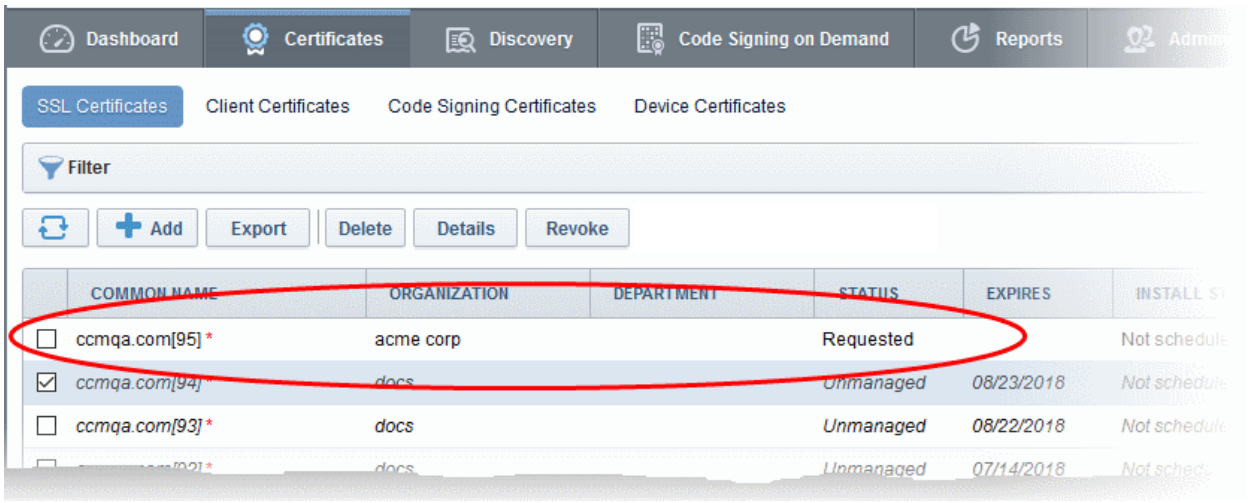
- Click 'Next'



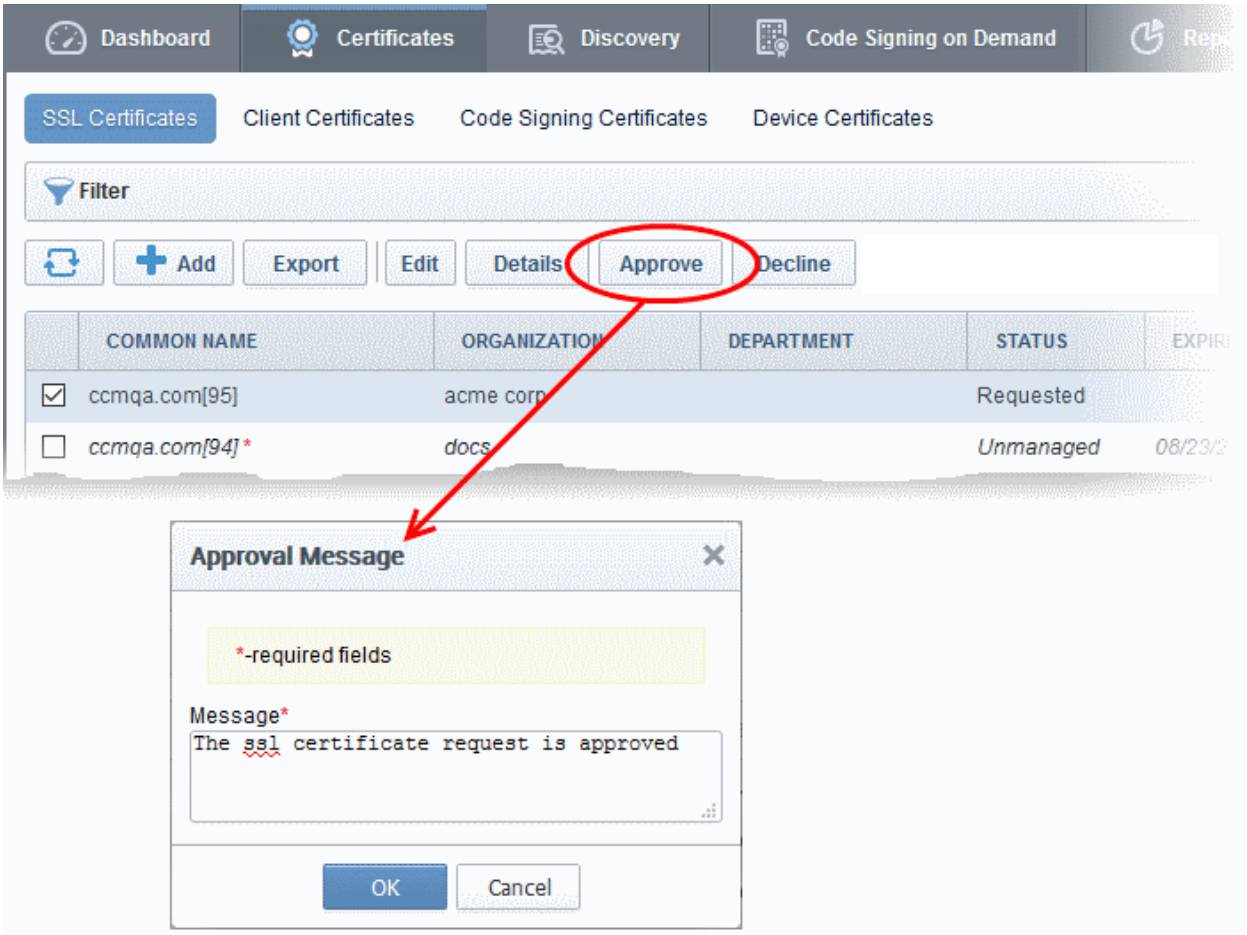
The final stage is to agree to the EULA.

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

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

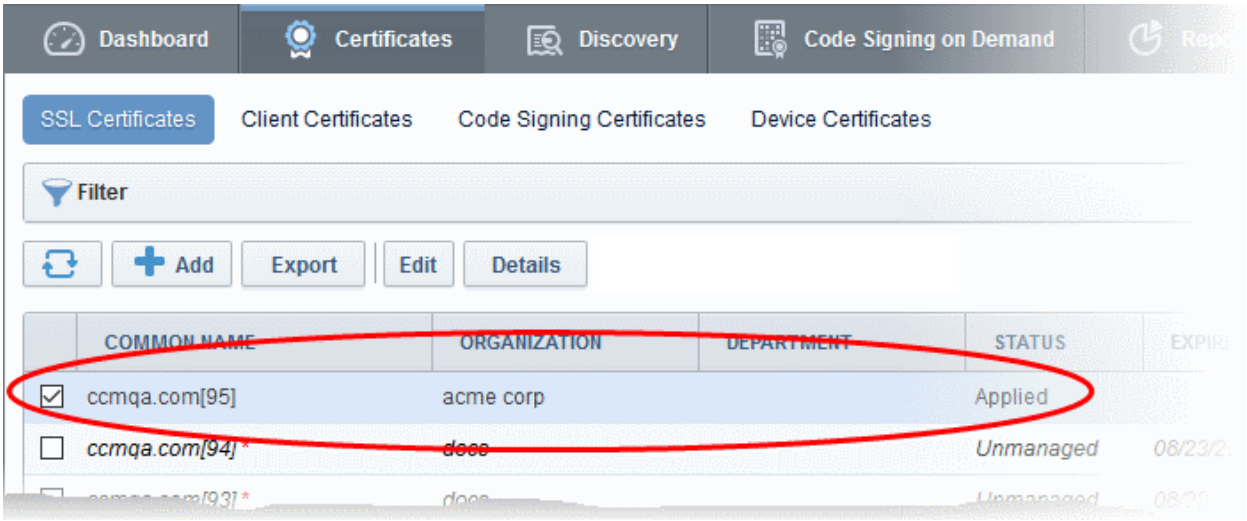


- The CSR for the requested certificate will be generated automatically. After the CSR has been created, the 'Approve' button will appear at the top when you select the certificate in the list:

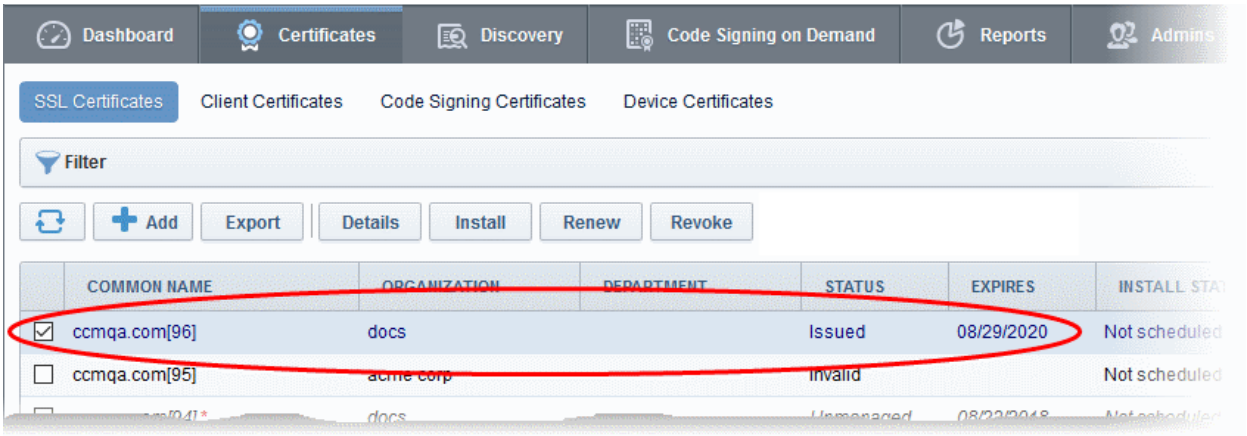


- Click the 'Approve' button to approve the request, enter an approval message and click 'OK'.

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



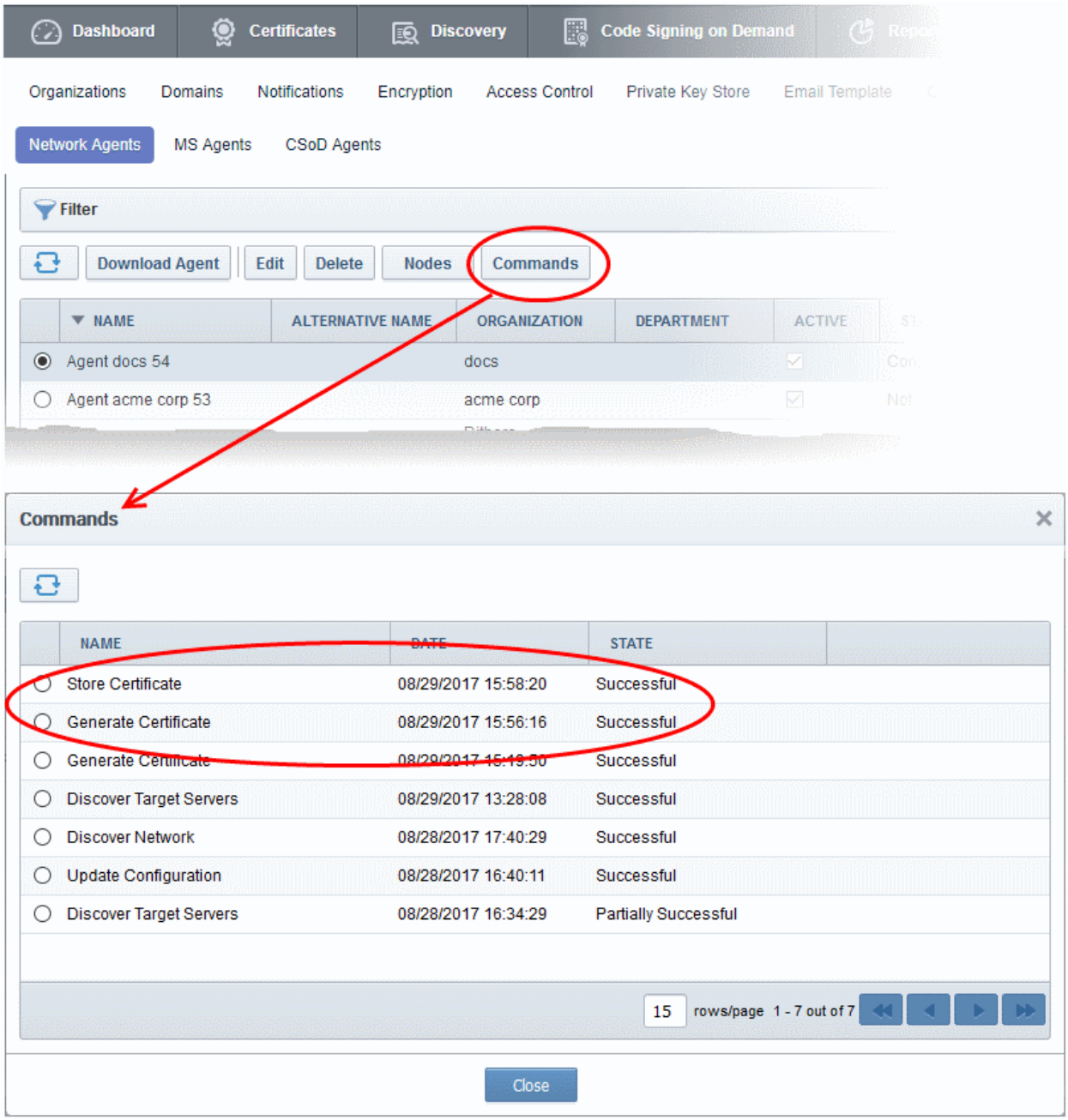
The controller will track the order number then collect and store the certificate once it is issued. The certificate status will change to 'Issued'.



To check whether the certificate controller has stored the certificate:

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

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

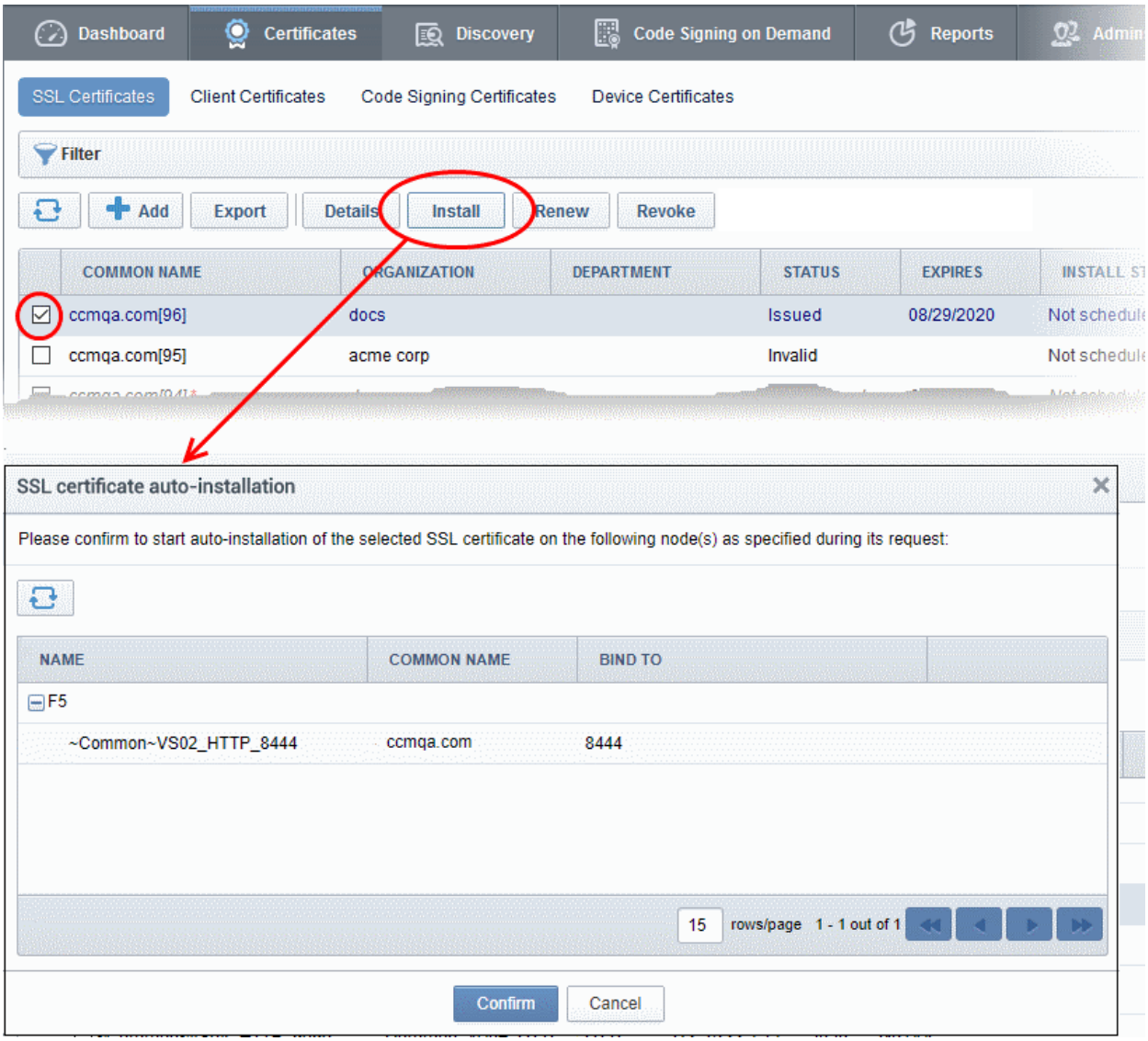


The certificate is stored on the server by the agent.

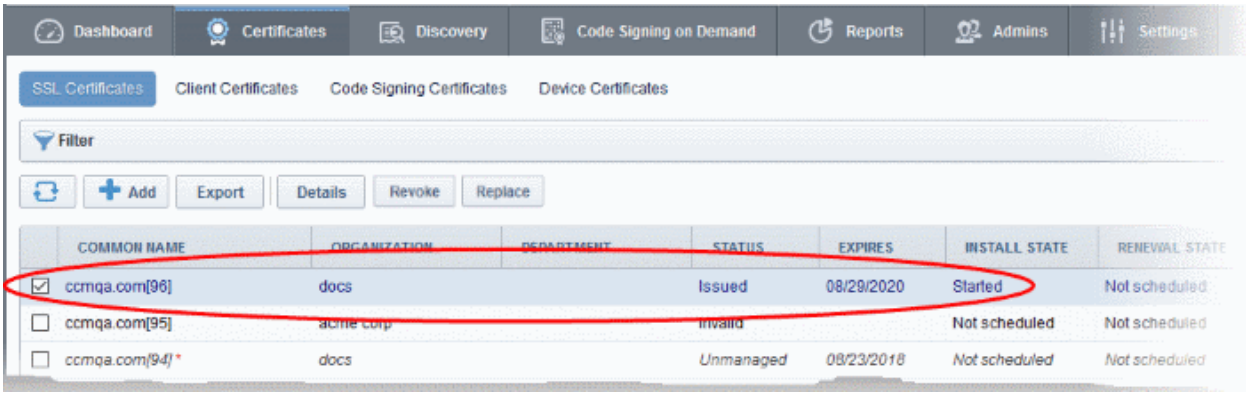
- If you set a schedule for automatic installation, it will be installed automatically at the scheduled time.
- If you selected 'Triggered auto-installation' you can manually initiate installation (or schedule auto-installation) from the 'Certificates' > 'SSL Certificates' interface:

To manually initiate auto-installation of a certificate

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

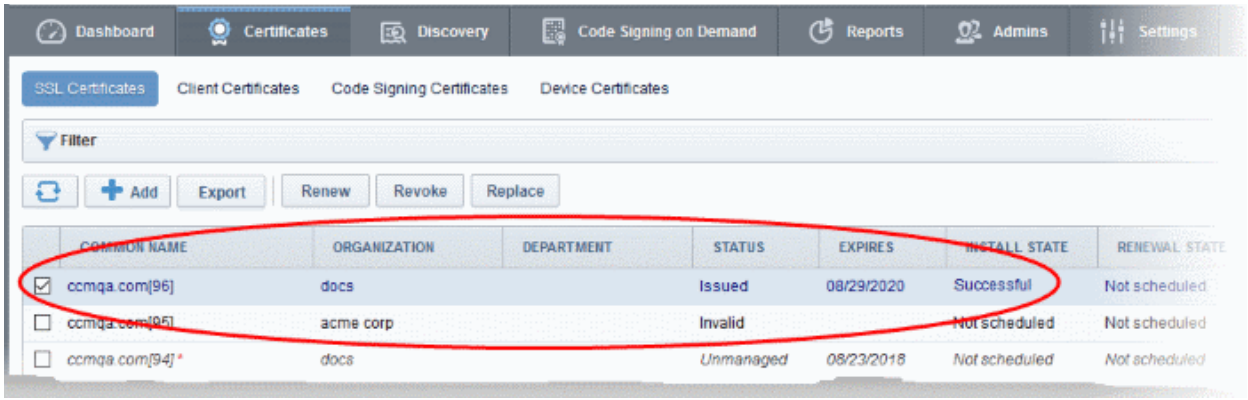


The installation will begin instantly. Once the installation commences, the 'Install State' of the certificate will change to 'Started'.

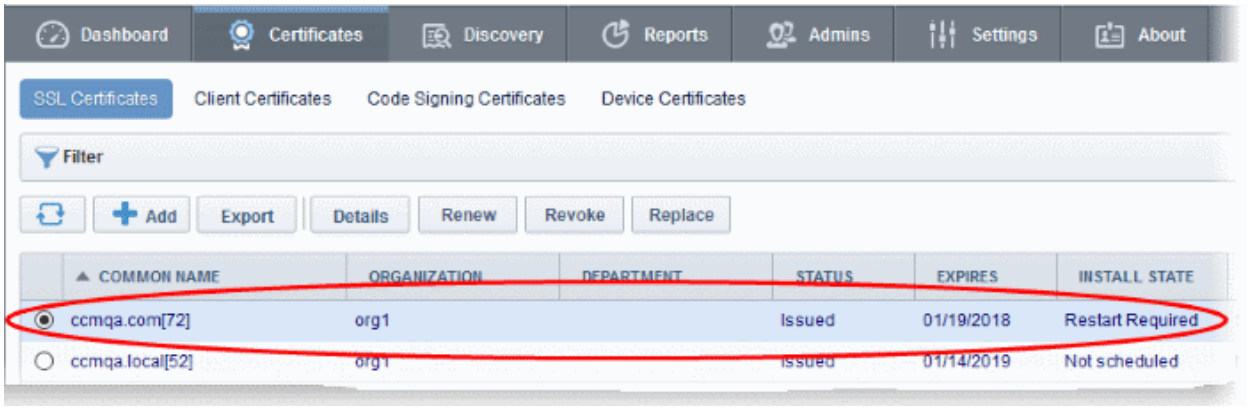


When installation is complete:

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

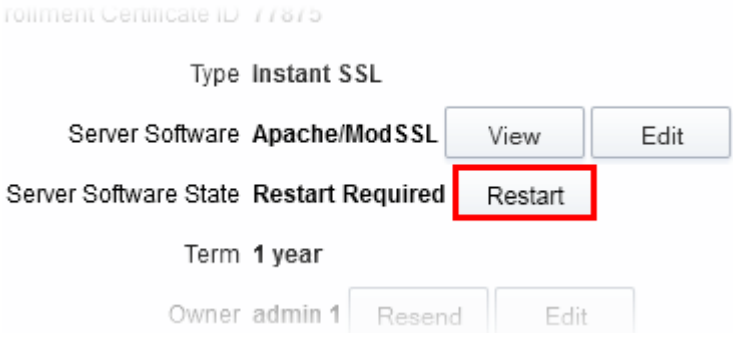


- Apache servers - The certificate will become active after the server is restarted. The install state will change to 'Restart Required'.



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

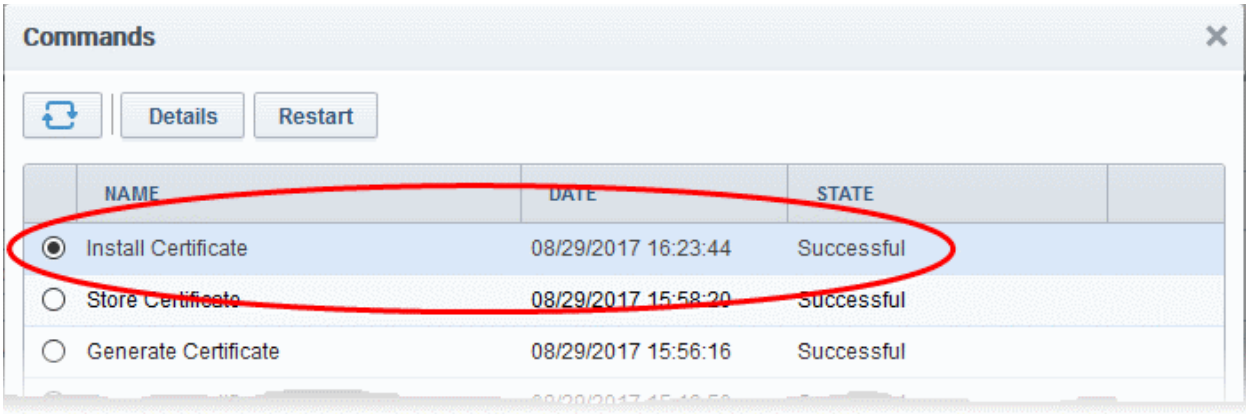
- Select the certificate and click the 'Details' button at the top. The 'Certificate Details' dialog will be displayed.
- Click Restart beside the Server Software State field in the 'Details' dialog



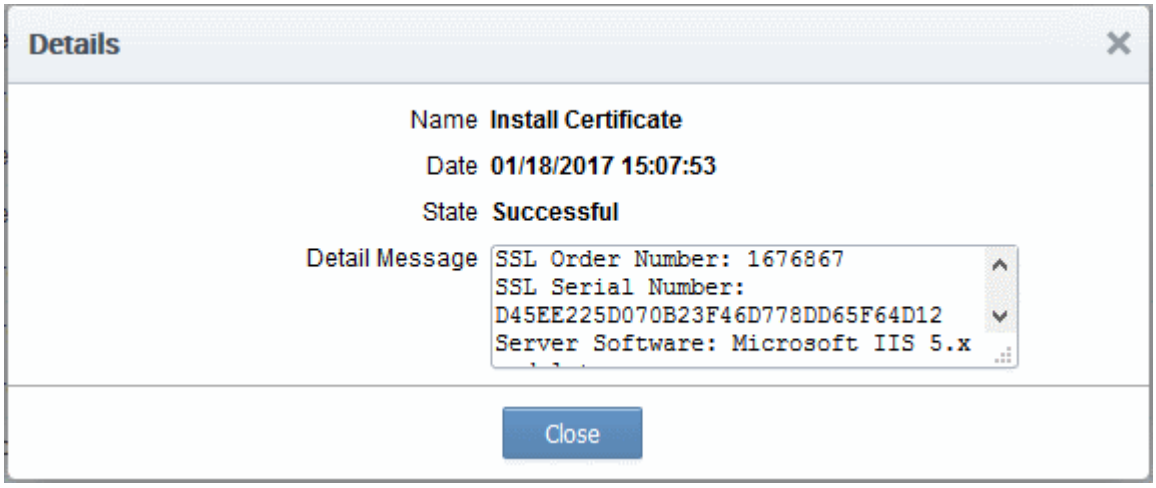
After restarting the server, the certificate will activated and the 'Install State' will change to 'Successful'.

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

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



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



About Comodo CA

Comodo Certificate Authority is one of the world's largest providers of SSL certificates by volume having issued over 91 million certificates and serving over 200,000 customers across 150 countries. The company provides a full suite of certificate products spanning all validation levels for website certificates, certificates for code-signing and email-signing, and the Comodo Certificate Manager (CCM) platform. Comodo CA has its US headquarters in New Jersey and international offices in the United Kingdom, Ukraine and India.

Comodo CA Limited

3rd floor, Office Village Exchange Quay

Trafford Road, Manchester, M5 3EQ

United Kingdom

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767