

**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.<br>See <b>Method 1 - Enterprise Controller Mode</b> | Requires an agent to be installed on each individual web server. The agents communicate with CCM to coordinate automatic CSR generation and certificate installation.<br>See <b>Method 2 - CCM Controller Mode</b> |

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       |
| <ul style="list-style-type: none"> <li>• C - CCM Controller Mode (Local)</li> <li>• E – Enterprise Controller Mode (Remote)</li> </ul> |  |   |         |

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 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:

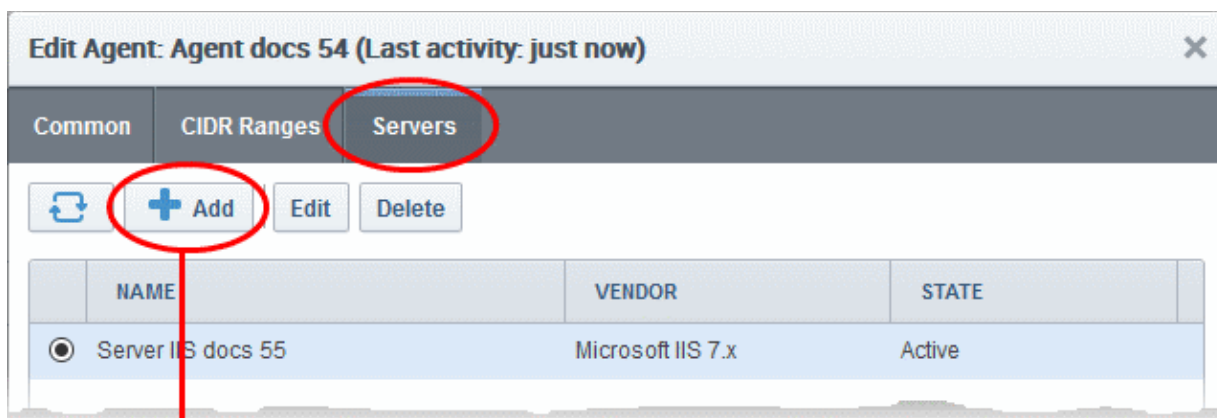
The screenshot shows the Comodo Certificate Manager interface. The top navigation bar includes 'Dashboard', 'Certificates', 'Discovery', and 'Tools'. Below this, there are tabs for 'Organizations', 'Domains', 'Notifications', 'Encryption', and 'Access Control'. The main area is divided into 'Network Agents' and 'MS Agents'. A 'Filter' section is present, followed by buttons for 'Download Agent', 'Edit', 'Delete', 'Nodes', and 'Commands'. A table lists agents with columns for 'NAME', 'ALTERNATIVE NAME', and 'ORGANIZATION'. The 'Edit Agent: Agent docs 54 (Last activity: 09/01/2017 13:57:19)' dialog is open, showing tabs for 'Common', 'CIDR Ranges', and 'Servers'. The 'Servers' tab is active, displaying a table with columns for 'NAME', 'VENDOR', and 'STATE'. The table contains two entries: 'Remote F5 Server' (F5 BIG-IP, Active) and 'Server IIS docs 55' (Microsoft IIS 7.x, Active). The dialog also includes 'Add', 'Edit', and 'Delete' buttons, a pagination control showing '15 rows/page 1 - 2 out of 2', and 'OK' and 'Cancel' buttons at the bottom.

| NAME   | ALTERNATIVE NAME | ORGANIZATION |
|--|------------------|--------------|
| <input checked="" type="radio"/> Agent docs 54 |                  | docs         |
| <input type="radio"/> Agent acme corp 53       |                  | acme corp    |

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

- 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.



**Add Web Server** ✕

\*-required fields

Name\*

Vendor\*  ▾

State

Remote

IP address / Port\*  .  .  .  :

Use key

Username

Password

- 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.<br>Note: This field will be enabled only if 'Remote' is selected.  |
| Use key                               | Checkbox | <ul style="list-style-type: none"> <li>Specify whether the agent should use SSH Key-Based Authentication to access the server.</li> <li>Only applies to Apache and Tomcat web-servers installed on Linux.</li> </ul>   |
| User Name / Private Key File Path     | String   | <ul style="list-style-type: none"> <li>If 'Use key' is not selected, specify the admin username to log into the server.</li> <li>If 'Use key' is selected, specify the path to the SSH private key file to access the server</li> </ul> Note: This field will be enabled only if 'Remote' is selected. |
| Password / Passphrase                 | String   | <ul style="list-style-type: none"> <li>If 'Use key' is not selected, specify the admin password to log into the server.</li> <li>If 'Use key' is selected, specify the passphrase for the private key file.</li> </ul> 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'.

The screenshot shows a window titled "Edit Agent: Agent docs 54 (Last activity: a moment ago)". It has three tabs: "Common", "CIDR Ranges", and "Servers". Below the tabs are buttons for "Refresh", "+ Add", "Edit", and "Delete". A table lists the servers:

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

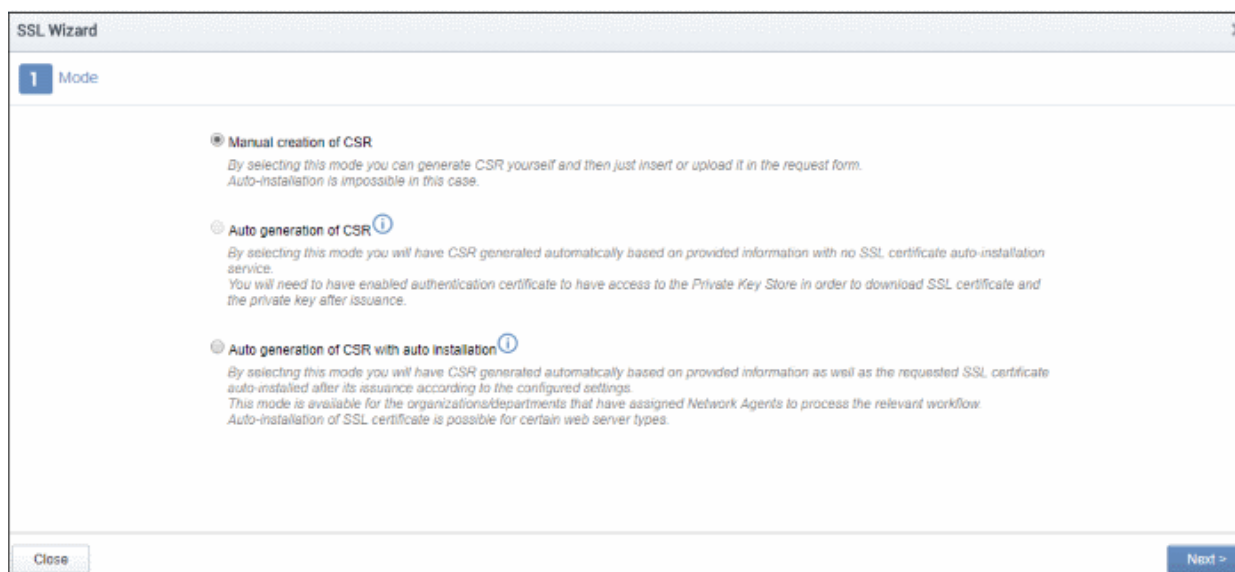
At the bottom of the table, there is a pagination control showing "15 rows/page 1 - 2 out of 2" with navigation arrows. Below the table are "OK" and "Cancel" buttons.

- 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.

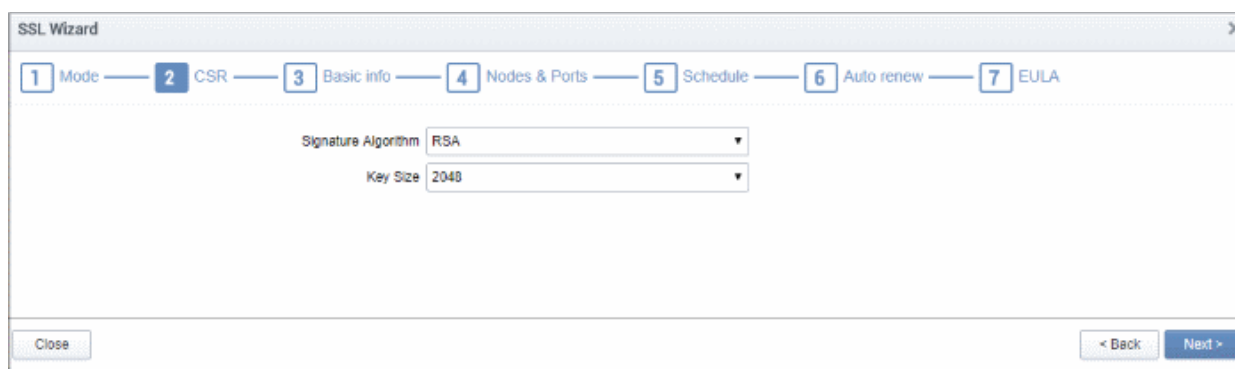
### To enroll a certificate for auto-installation



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

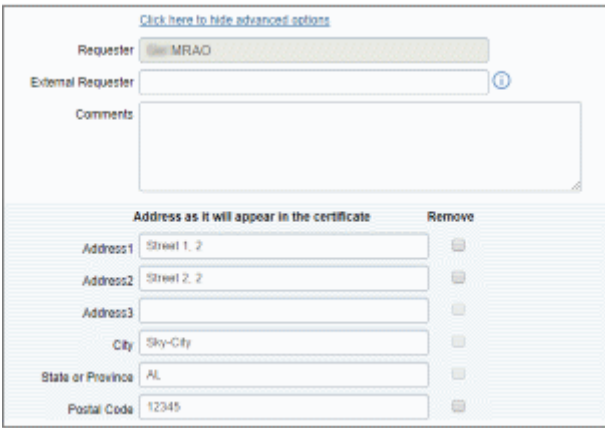


- Select the third option, 'Auto generation of CSR with auto installation', and click 'Next'.



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 ( <i>required</i> )              | Drop-down list | Choose the organization that the SSL certificate will belong to.   |
| Department ( <i>required</i> )                | Drop-down list | Choose the department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'.                                   |
| Certificate Type ( <i>required</i> )          | Drop-down list | Choose the certificate type that you wish to add for auto-installation.  |
| Certificate Term ( <i>required</i> )          | Drop-down list | Choose the validity period of the certificate. For example, 1 year, 2 years, 3 years.  |
| Common Name ( <i>required</i> )               | Text Field     | Type the domain that the certificate will be issued to.  |
| Server Software ( <i>required</i> )           | Drop-down list | Select the server software on which the certificate is to be installed.<br><b>Note:</b> Choose 'OTHER' if you want to use F5 BIG-IP.                                 |
| Subject Alternative Names ( <i>optional</i> ) | 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:<br>                         |



| Form Element | Type | Description  |
|--------------|------|--|
|              |      | <ul style="list-style-type: none"> <li>Requester – This field is auto-populated with the name of the administrator making the application.</li> <li>External Requester (optional) - Enter the email address of an external requester on whose behalf the application is made.</li> </ul> <p><b>Note:</b> 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.</p> <ul style="list-style-type: none"> <li>Comments (optional) - Enter your comments on the certificate.</li> </ul> <p><b>Address fields in the certificate</b></p> <ul style="list-style-type: none"> <li>The address fields are auto-populated from the details of the Organization or Department on whose behalf this certificate request is being made.</li> <li>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.</li> <li>The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted".</li> </ul> <p>For EV level certificates, it is mandatory to include and display address details of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down.</p> |

- Click 'Next'

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

Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic Info — 4 EV Details — 5 Nodes & Ports — 6 Schedule — 7 Auto renew — 8 EULA

### Incorporation or Registration Agency

Incorporating/Registration Agency\*

Main Telephone Number\*

Jurisdiction of Incorporation  
City or Town

State or Province of Incorporation

Country of Incorporation\*

Registration Number

Date of Incorporation

As assigned by the incorporating Agency (for Private Organization Applicants Only)

### Contract Signer

Title\*

Forename\*

Surname\*

Email\*

Telephone Number\*

Street\*

Locality\*

State/Province

Postal Code\*

Country\*

Relationship

This form assumes a single person will be acting as the Certificate Requester, Certificate Approver and Contract Signer

Close < Back Next >

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

Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — 5 Schedule — 6 Auto renew — 7 EULA

Please select the node(s) and specify the port number for each of them in 'Bind to' column in the table below (in order to allow the new SSL certificate to be bind to the intended port during auto-installation).

| NAME  | COMMON NAME    | PROTOC | IP ADDRESS | PORT | BIND TO | STATUS    | SSL      |
|---|----------------|--------|------------|------|---------|-----------|----------|
| <input type="checkbox"/> 10.100.93.150        |                |        |            |      |         | Active    |          |
| <input type="checkbox"/> 10.100.93.151        |                |        |            |      |         | Active    |          |
| <input type="checkbox"/> www.comodo.com       | www.comodo.com | HTTPS  | *          | 443  |         | Installed | External |
| <input type="checkbox"/> h2.ccmqa.com         | h2.ccmqa.com   | HTTP   | *          | 80   |         | No SSL    |          |
| <input checked="" type="checkbox"/> ccmqa.com | ccmqa.com      | HTTP   | *          | 80   | 8444    | No SSL    |          |
| <input type="checkbox"/> h2                   | h2             | HTTPS  | *          | 8443 |         | No SSL    |          |

15 rows/page 1 - 2 out of 2 < >

Close < Back Next >

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'

**Request New SSL Certificate**

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — **5 Schedule** — 6 Auto renew — 7 EULA

Triggered auto-installation  
The beginning of certificate auto-installation will be triggered by clicking 'Install' button displayed once this certificate is selected in 'SSL Certificates' area. 'Install' button will be available after certificate is issued.

Scheduled auto-installation  
Certificate auto-installation will be started after its issuance during selected time period.

Time zone: UTC+05:30 - IST, SLT

Start not earlier than: 02/07/2018

Run Between (Time Of Day): 11 : 52 — 11 : 52

Run Only (Day of Week):  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

Close < Back 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'.

**Request New SSL Certificate**

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — 5 Schedule — **6 Auto renew** — 7 EULA

Here you can set auto-renewal of this certificate in advance of its expiration. These settings can be edited in the certificate details later on.

Enable auto renewal of this certificate

Create new key pair while renewing

Number of days before expiration to start auto renewal 30

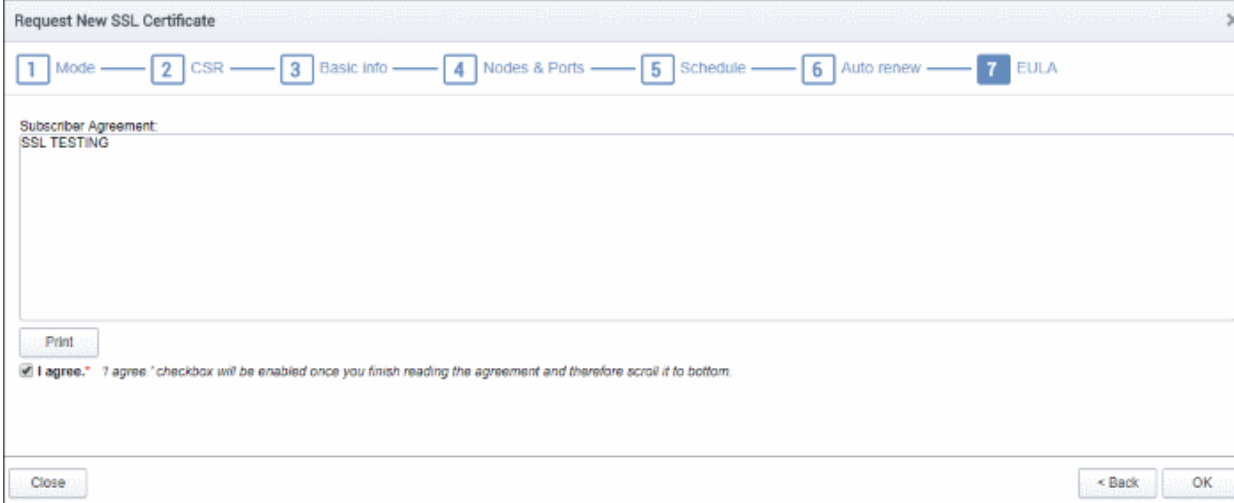
Close < Back Next >

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'



Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — 5 Schedule — 6 Auto renew — 7 EULA

Subscriber Agreement  
SSL TESTING

Print

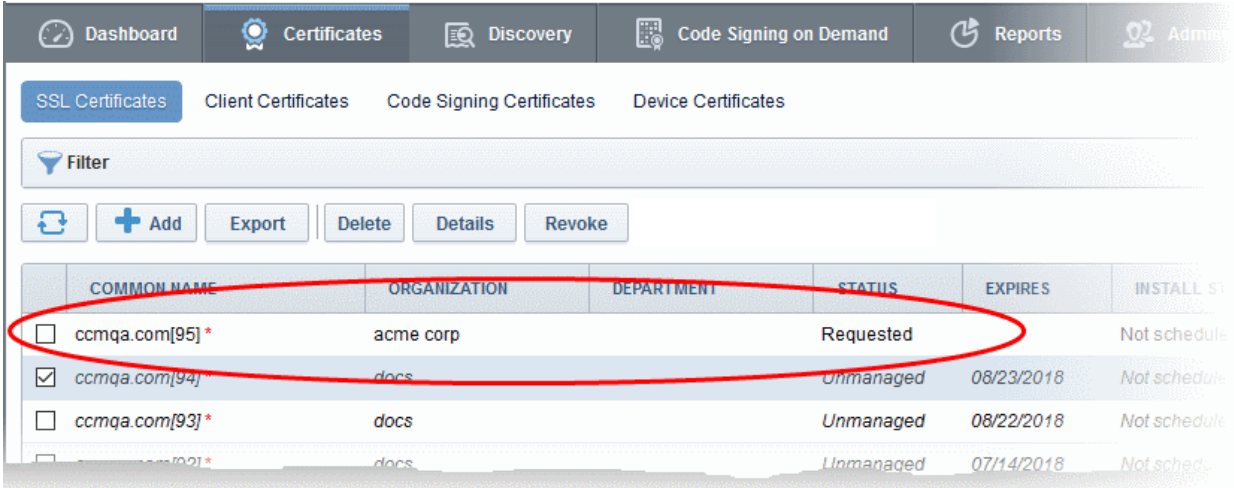
I agree. \* I agree. \*checkbox will be enabled once you finish reading the agreement and therefore scroll it to bottom.

Close < Back OK

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'.



|                                     | COMMON NAME     | ORGANIZATION | DEPARTMENT | STATUS    | EXPIRES    | INSTALL ST   |
|-------------------------------------|-----------------|--------------|------------|-----------|------------|--------------|
| <input type="checkbox"/>            | ccmqa.com[95] * | acme corp    |            | Requested |            | Not schedule |
| <input checked="" type="checkbox"/> | ccmqa.com[94]   | docs         |            | Unmanaged | 08/23/2018 | Not schedule |
| <input type="checkbox"/>            | ccmqa.com[93] * | docs         |            | Unmanaged | 08/22/2018 | Not schedule |
| <input type="checkbox"/>            | ccmqa.com[92] * | docs         |            | Unmanaged | 07/14/2018 | Not schedule |

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

The screenshot shows the 'Certificates' section of the Comodo Certificate Manager. The 'SSL Certificates' tab is active. A table lists certificate requests with columns for 'COMMON NAME', 'ORGANIZATION', 'DEPARTMENT', 'STATUS', and 'EXPIRES'. The first row, 'ccmqa.com[95]', has a status of 'Requested'. The 'Approve' button in the toolbar is circled in red. A red arrow points from this button to an 'Approval Message' dialog box. The dialog box contains a text area with the message: 'The ssl certificate request is approved'. There are 'OK' and 'Cancel' buttons at the bottom of the dialog.

|                                     | COMMON NAME    | ORGANIZATION | DEPARTMENT | STATUS    | EXPIRES    |
|-------------------------------------|----------------|--------------|------------|-----------|------------|
| <input checked="" type="checkbox"/> | ccmqa.com[95]  | acme corp    |            | Requested |            |
| <input type="checkbox"/>            | ccmqa.com[94]* | docs         |            | Unmanaged | 08/23/2017 |

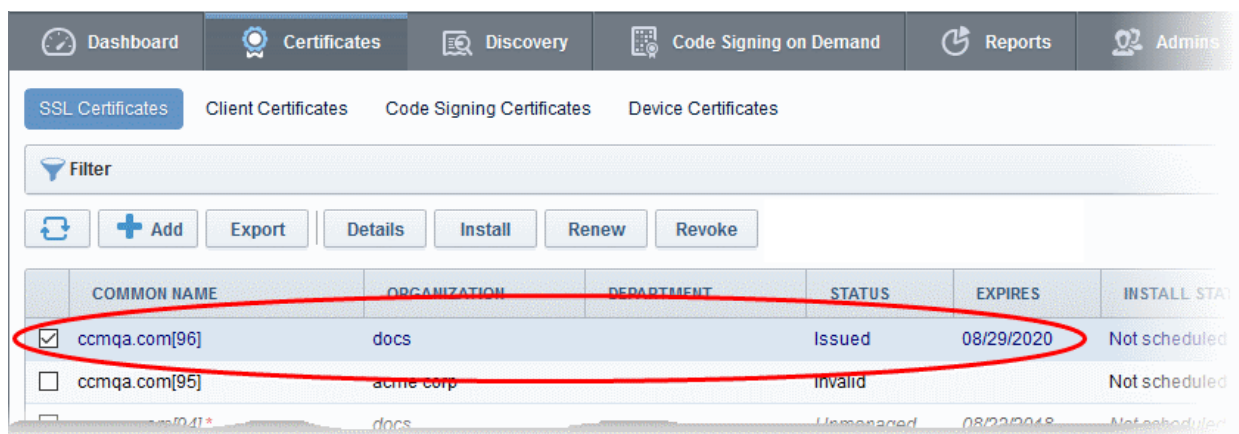
- Click the 'Approve' button to approve the request, enter an approval message and click 'OK'.

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

The screenshot shows the same 'Certificates' section as before. The 'SSL Certificates' tab is active. The table now shows the first row, 'ccmqa.com[95]', with a status of 'Applied'. This row is circled in red. The 'Approve' button is no longer visible in the toolbar.

|                                     | COMMON NAME    | ORGANIZATION | DEPARTMENT | STATUS    | EXPIRES    |
|-------------------------------------|----------------|--------------|------------|-----------|------------|
| <input checked="" type="checkbox"/> | ccmqa.com[95]  | acme corp    |            | Applied   |            |
| <input type="checkbox"/>            | ccmqa.com[94]* | docs         |            | Unmanaged | 08/23/2017 |
| <input type="checkbox"/>            | ccmqa.com[93]* | docs         |            | Unmanaged | 08/23/2017 |

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



The screenshot shows the 'Certificates' section of the Comodo Certificate Manager. It features a navigation bar with 'Dashboard', 'Certificates', 'Discovery', 'Code Signing on Demand', 'Reports', and 'Admins'. Below this, there are tabs for 'SSL Certificates', 'Client Certificates', 'Code Signing Certificates', and 'Device Certificates'. A 'Filter' dropdown is present, followed by action buttons: 'Refresh', '+ Add', 'Export', 'Details', 'Install', 'Renew', and 'Revoke'. The main area contains a table with the following columns: 'COMMON NAME', 'ORGANIZATION', 'DEPARTMENT', 'STATUS', 'EXPIRES', and 'INSTALL STATUS'. The first row is highlighted and circled in red, showing a certificate for 'ccmqa.com[96]' with organization 'docs', status 'Issued', and expiration date '08/29/2020'. The second row shows a certificate for 'ccmqa.com[95]' with status 'Invalid'. A third row is partially visible with 'ccmqa.com[94]' and status 'Unmanaged'.

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

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 screenshot shows the Comodo Certificate Manager interface. At the top, there are navigation tabs: Dashboard, Certificates, Discovery, Code Signing on Demand, and Reports. Below these are sub-tabs: Organizations, Domains, Notifications, Encryption, Access Control, Private Key Store, Email Template, and Certificates. Under the Certificates tab, there are sub-tabs for Network Agents, MS Agents, and CSoD Agents. A 'Filter' dropdown is visible. Below the filter are buttons for Download Agent, Edit, Delete, Nodes, and Commands. The Commands button is circled in red. A red arrow points from the Commands button to a modal window titled 'Commands'. The modal window contains a table with the following data:

|                       | NAME                    | DATE                | STATE                |
|-----------------------|-------------------------|---------------------|----------------------|
| <input type="radio"/> | Store Certificate       | 08/29/2017 15:58:20 | Successful           |
| <input type="radio"/> | Generate Certificate    | 08/29/2017 15:56:16 | Successful           |
| <input type="radio"/> | Generate Certificate    | 08/29/2017 15:19:50 | Successful           |
| <input type="radio"/> | Discover Target Servers | 08/29/2017 13:28:08 | Successful           |
| <input type="radio"/> | Discover Network        | 08/28/2017 17:40:29 | Successful           |
| <input type="radio"/> | Update Configuration    | 08/28/2017 16:40:11 | Successful           |
| <input type="radio"/> | Discover Target Servers | 08/28/2017 16:34:29 | Partially Successful |

At the bottom of the modal window, there is a pagination control showing '15 rows/page 1 - 7 out of 7' and navigation buttons. A 'Close' button is located at the bottom center of the modal window.

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 screenshot shows the 'Certificates' section of the Comodo Certificate Manager. The 'Install' button is circled in red. A modal window titled 'SSL certificate auto-installation' is open, showing a table of nodes for installation. The table has columns for NAME, COMMON NAME, and BIND TO. The first row is expanded to show details for node 'F5'.

| NAME                   | COMMON NAME | BIND TO |
|------------------------|-------------|---------|
| F5                     |             |         |
| -Common-VS02_HTTP_8444 | ccmqa.com   | 8444    |

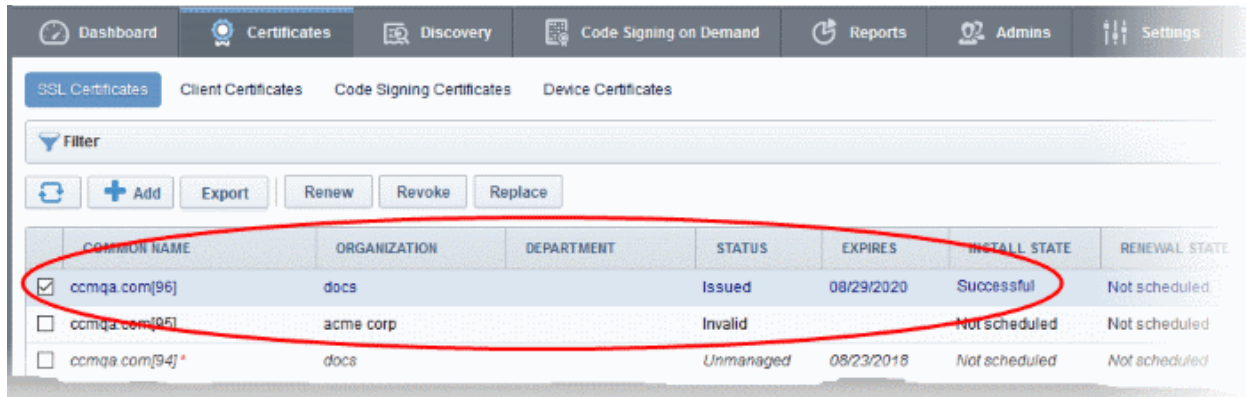
The certificate installation will begin instantly. Once the installation commences, the 'Install State' of the certificate will change to 'Started'.

The screenshot shows the 'Certificates' section after installation. The 'Install State' for the certificate 'ccmqa.com[96]' is now 'Started', which is circled in red. The table below shows the updated status of the certificates.

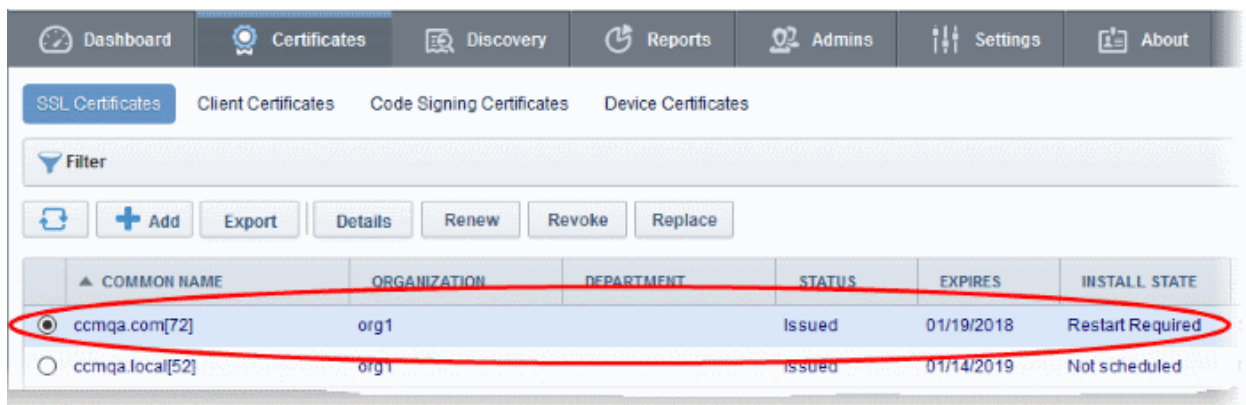
| COMMON NAME                                       | ORGANIZATION | DEPARTMENT | STATUS    | EXPIRES    | INSTALL STATE | RENEWAL STATE |
|---|--------------|------------|-----------|------------|---------------|---------------|
| <input checked="" type="checkbox"/> ccmqa.com[96] | docs         |  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

When installation is complete:

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

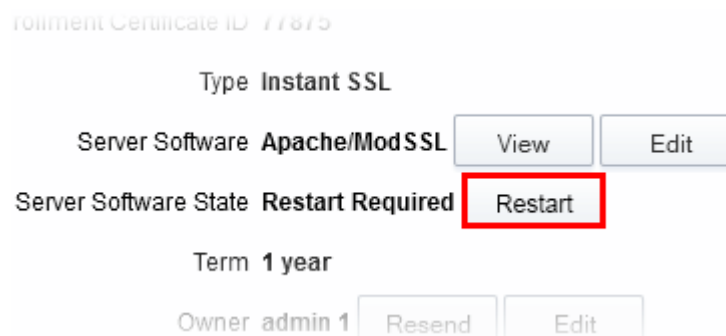


- **Apache** - The certificate will become active after the server is restarted. The install state will change to 'Restart Required'.



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 be 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.

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

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

**Details**

Name **Install Certificate**

Date **08/29/2017 16:23:44**

State **Successful**

Detail Message

```
SSL Order Number: 1729480
SSL Serial Number:
78C41E511591C2CAC6FAE16197B0FEE1
Server Software: OTHER
```

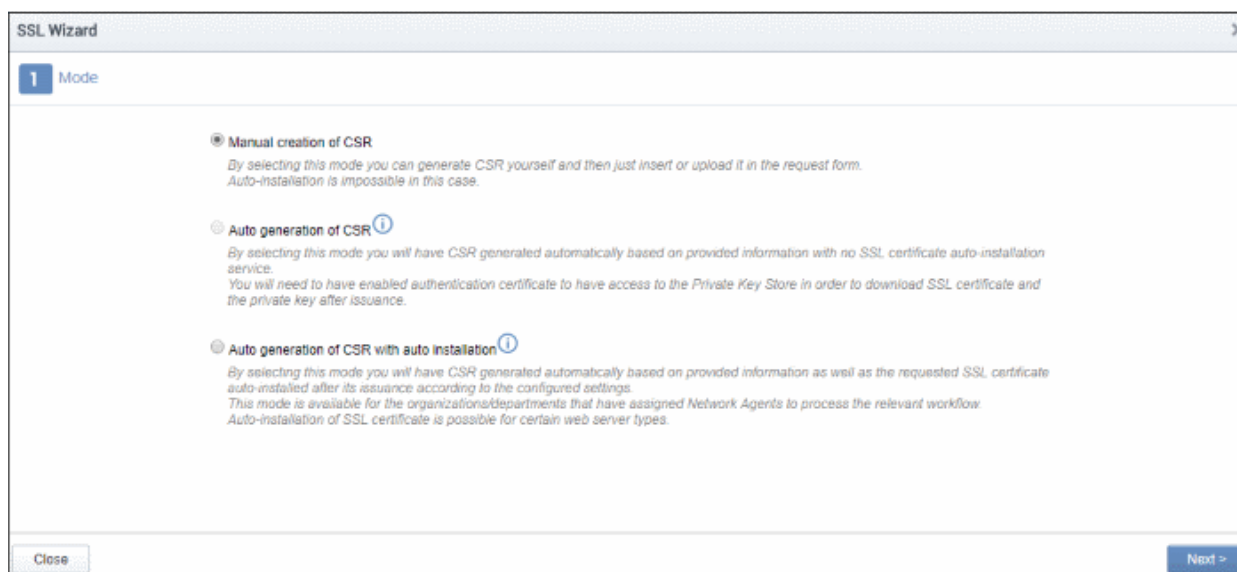
Close

## Method 2 - CCM Controller Mode

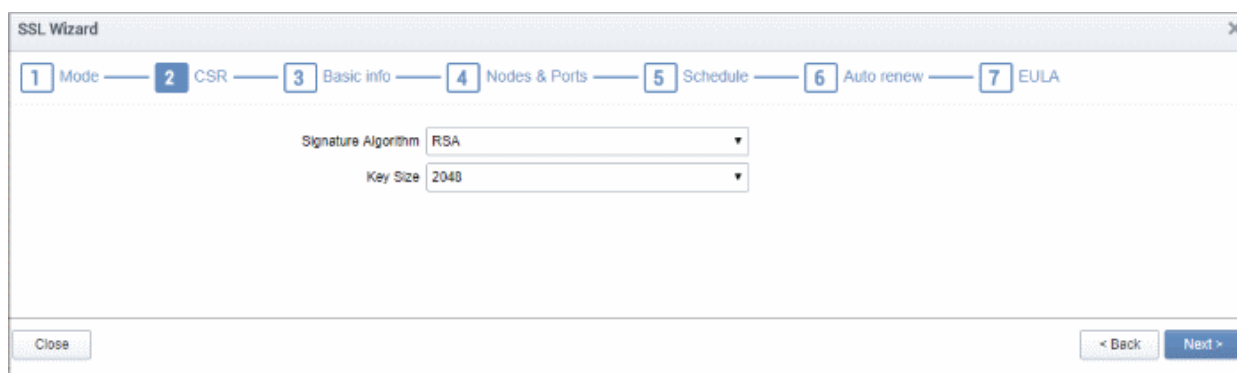
- Administrators can request and install new certificates for domains hosted on different web servers from the 'Certificate Management - SSL Certificates' area.
- 'CCM Controller Mode' requires an agent to be installed on each web server upon which the certificates are to be auto-installed/renewed.

### 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 ( <i>required</i> )              | Drop-down list | Choose the organization that the SSL certificate will belong to.   |
| Department ( <i>required</i> )                | Drop-down list | Choose the department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'.                                   |
| Certificate Type ( <i>required</i> )          | Drop-down list | Choose the certificate type that you want to auto-install.<br>The certificate types shown in the drop-down depend on the 'SSL Types' allowed for the organization.   |
| Certificate Term ( <i>required</i> )          | Drop-down list | Choose the validity period of the certificate. For example, 1 year, 2 years, 3 years.  |
| Common Name ( <i>required</i> )               | Text Field     | Type the domain that the certificate will be issued to.  |
| Server Software ( <i>required</i> )           | Drop-down list | Select the server software on which the certificate is to be installed.<br><b>Note:</b> Choose 'OTHER' if you want to use F5 BIG-IP.                                 |
| Subject Alternative Names ( <i>optional</i> ) | 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   |  |                          |  |                          |  |                          |   |                          |  |                          |   |                          |
|--|--------------------------|---|--|--------------------------|--|--------------------------|--|--------------------------|---|--------------------------|--|--------------------------|---|--------------------------|
|  |                          | <div data-bbox="730 257 1337 683" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p style="text-align: center; color: #00aaff; font-size: small;"><a href="#">Click here to hide advanced options</a></p> <p>Requester <input type="text" value="MRAO"/></p> <p>External Requester <input type="text"/></p> <p>Comments <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div></p> <hr/> <p style="text-align: center; font-size: small;"><b>Address as it will appear in the certificate</b> <span style="float: right;">Remove</span></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%;"><small>Address1</small> <input type="text" value="Street 1, 2"/></td> <td style="width: 20%; text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><small>Address2</small> <input type="text" value="Street 2, 2"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><small>Address3</small> <input type="text"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><small>City</small> <input type="text" value="Sky-City"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><small>State or Province</small> <input type="text" value="AL"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><small>Postal Code</small> <input type="text" value="12345"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> </table> </div> <ul style="list-style-type: none"> <li>Requester – This field is auto-populated with the name of the administrator making the application.</li> <li>External Requester (optional) - Enter the email address of an external requester on whose behalf the application is made.</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>Comments (optional) - Enter your comments on the certificate.</li> </ul> <p><b>Address fields in the certificate</b></p> <ul style="list-style-type: none"> <li>The address fields are auto-populated from the details in the <b>'General Properties'</b> tab of the organization or department on whose behalf this certificate request is being made.</li> <li>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.</li> <li>The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted".</li> </ul> <p>For EV level certificates, it is mandatory to include and display address details of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering these address details will be displayed and the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down.</p> | <small>Address1</small> <input type="text" value="Street 1, 2"/> | <input type="checkbox"/> | <small>Address2</small> <input type="text" value="Street 2, 2"/> | <input type="checkbox"/> | <small>Address3</small> <input type="text"/> | <input type="checkbox"/> | <small>City</small> <input type="text" value="Sky-City"/> | <input type="checkbox"/> | <small>State or Province</small> <input type="text" value="AL"/> | <input type="checkbox"/> | <small>Postal Code</small> <input type="text" value="12345"/> | <input type="checkbox"/> |
| <small>Address1</small> <input type="text" value="Street 1, 2"/> | <input type="checkbox"/> |   |  |                          |  |                          |  |                          |   |                          |  |                          |   |                          |
| <small>Address2</small> <input type="text" value="Street 2, 2"/> | <input type="checkbox"/> |   |  |                          |  |                          |  |                          |   |                          |  |                          |   |                          |
| <small>Address3</small> <input type="text"/>                     | <input type="checkbox"/> |   |  |                          |  |                          |  |                          |   |                          |  |                          |   |                          |
| <small>City</small> <input type="text" value="Sky-City"/>        | <input type="checkbox"/> |   |  |                          |  |                          |  |                          |   |                          |  |                          |   |                          |
| <small>State or Province</small> <input type="text" value="AL"/> | <input type="checkbox"/> |   |  |                          |  |                          |  |                          |   |                          |  |                          |   |                          |
| <small>Postal Code</small> <input type="text" value="12345"/>    | <input type="checkbox"/> |   |  |                          |  |                          |  |                          |   |                          |  |                          |   |                          |

- Click 'Next'

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

Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic Info — **4 EV Details** — 5 Nodes & Ports — 6 Schedule — 7 Auto renew — 8 EULA

### Incorporation or Registration Agency

Incorporating/Registration Agency\*

Main Telephone Number\*

Jurisdiction of Incorporation  
City or Town

State or Province of Incorporation

Country of Incorporation\*

Registration Number

Date of Incorporation

As assigned by the incorporating Agency (for Private Organization Applicants Only)

### Contract Signer

Title\*

Forename\*

Surname\*

Email\*

Telephone Number\*

Street\*

Locality\*

State/Province

Postal Code\*

Country\*

Relationship

This form assumes a single person will be acting as the Certificate Requester, Certificate Approver and Contract Signer

Close < Back Next >

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

Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — **4 Nodes & Ports** — 5 Schedule — 6 Auto renew — 7 EULA

Please select the node(s) and specify the port number for each of them in 'Bind to' column in the table below (in order to allow the new SSL certificate to be bind to the intended port during auto-installation).

| NAME  | COMMON NAME  | PROTOC | IP ADDRESS | PORT | BIND TO | STATUS | SSL |
|---|--------------|--------|------------|------|---------|--------|-----|
| <input checked="" type="checkbox"/> 10.100.93.150 |              |        |            |      |         | Active |     |
| <input type="checkbox"/> h2.ccmqa.com             | h2.ccmqa.com | HTTP   | *          | 80   |         | No SSL |     |
| <input checked="" type="checkbox"/> ccmqa.com     | ccmqa.com    | HTTP   | *          | 80   | 8444    | No SSL |     |
| <input type="checkbox"/> h2                       | h2           | HTTPS  | *          | 8443 |         | No SSL |     |

15 rows/page 1 - 2 out of 2 << < > >>

Close < Back Next >

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'

**Request New SSL Certificate**

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — **5 Schedule** — 6 Auto renew — 7 EULA

Triggered auto-installation  
The beginning of certificate auto-installation will be triggered by clicking 'Install' button displayed once this certificate is selected in 'SSL Certificates' area. 'Install' button will be available after certificate is issued.

Scheduled auto-installation  
Certificate auto-installation will be started after its issuance during selected time period.

Time zone: UTC+05:30 - IST, SLT

Start not earlier than: 02/07/2018

Run Between (Time Of Day): 11 : 52 — 11 : 52

Run Only (Day of Week):  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

Close < Back 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'.

**Request New SSL Certificate**

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — 5 Schedule — **6 Auto renew** — 7 EULA

Here you can set auto-renewal of this certificate in advance of its expiration. These settings can be edited in the certificate details later on.

Enable auto renewal of this certificate

Create new key pair while renewing

Number of days before expiration to start auto renewal 30

Close < Back 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'



Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Nodes & Ports — 5 Schedule — 6 Auto renew — 7 EULA

Subscriber Agreement  
SSL TESTING

Print

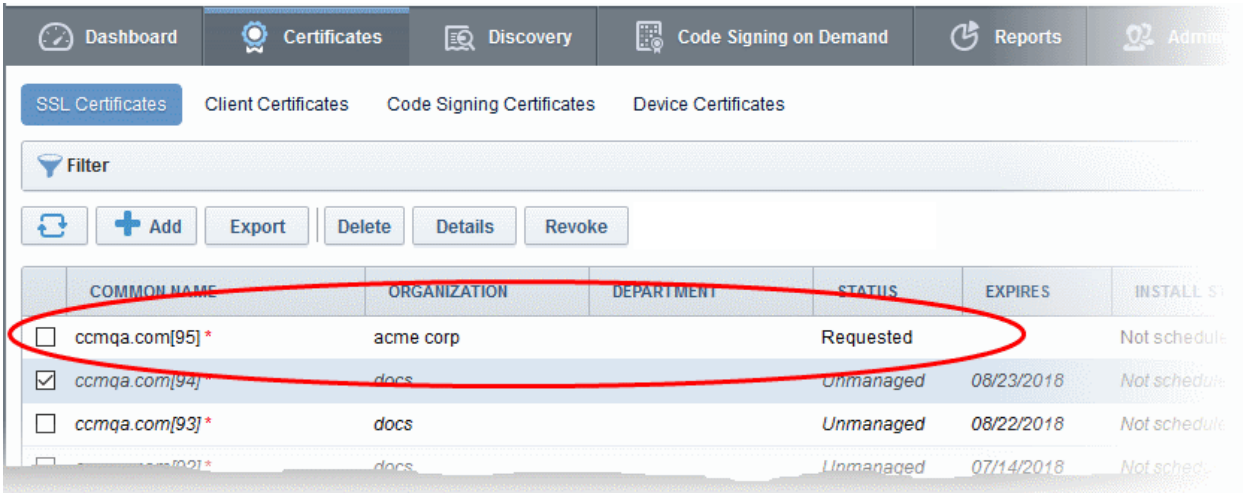
I agree. \* I agree. \*checkbox will be enabled once you finish reading the agreement and therefore scroll it to bottom.

Close < Back OK

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'.



Dashboard Certificates Discovery Code Signing on Demand Reports Admin

SSL Certificates Client Certificates Code Signing Certificates Device Certificates

Filter

Refresh Add Export Delete Details Revoke

|                                     | COMMON NAME     | ORGANIZATION | DEPARTMENT | STATUS    | EXPIRES    | INSTALL S    |
|-------------------------------------|-----------------|--------------|------------|-----------|------------|--------------|
| <input type="checkbox"/>            | ccmqa.com[95] * | acme corp    |            | Requested |            | Not schedule |
| <input checked="" type="checkbox"/> | ccmqa.com[94]   | docs         |            | Unmanaged | 08/23/2018 | Not schedule |
| <input type="checkbox"/>            | ccmqa.com[93] * | docs         |            | Unmanaged | 08/22/2018 | Not schedule |
| <input type="checkbox"/>            | ccmqa.com[92] * | docs         |            | Unmanaged | 07/14/2018 | Not schedule |

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

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

|                                     | COMMON NAME    | ORGANIZATION | DEPARTMENT | STATUS    | EXPIRES    |
|-------------------------------------|----------------|--------------|------------|-----------|------------|
| <input checked="" type="checkbox"/> | ccmqa.com[95]  | acme corp    |            | Requested |            |
| <input type="checkbox"/>            | ccmqa.com[94]* | docs         |            | Unmanaged | 08/23/2017 |

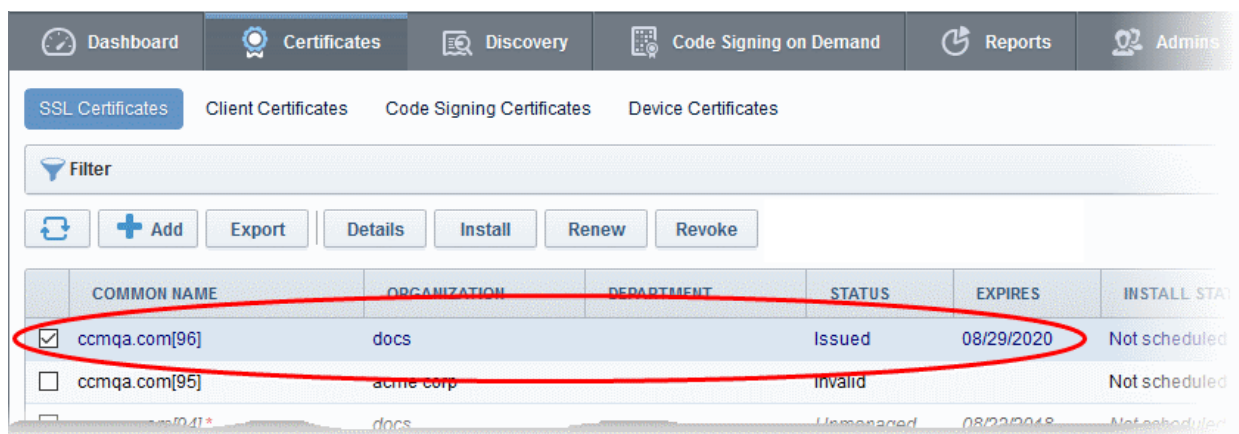
- Click the 'Approve' button to approve the request, enter an approval message and click 'OK'.

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

The screenshot shows the 'Certificates' section of the Comodo Certificate Manager. The certificate 'ccmqa.com[95]' now has a status of 'Applied'. The row for this certificate is circled in red.

|                                     | COMMON NAME    | ORGANIZATION | DEPARTMENT | STATUS    | EXPIRES    |
|-------------------------------------|----------------|--------------|------------|-----------|------------|
| <input checked="" type="checkbox"/> | ccmqa.com[95]  | acme corp    |            | Applied   |            |
| <input type="checkbox"/>            | ccmqa.com[94]* | docs         |            | Unmanaged | 08/23/2017 |
| <input type="checkbox"/>            | ccmqa.com[93]* | docs         |            | Unmanaged | 08/23/2017 |

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



The screenshot shows the 'Certificates' section of the Comodo Certificate Manager. It features a navigation bar with 'Dashboard', 'Certificates', 'Discovery', 'Code Signing on Demand', 'Reports', and 'Admins'. Below this, there are tabs for 'SSL Certificates', 'Client Certificates', 'Code Signing Certificates', and 'Device Certificates'. A 'Filter' dropdown is present, followed by action buttons: 'Refresh', '+ Add', 'Export', 'Details', 'Install', 'Renew', and 'Revoke'. The main area contains a table of certificates with the following data:

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

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 screenshot shows the Comodo Certificate Manager interface. The top navigation bar includes 'Dashboard', 'Certificates', 'Discovery', 'Code Signing on Demand', and 'Reports'. Below this, there are tabs for 'Network Agents', 'MS Agents', and 'CSoD Agents'. The main content area shows a list of agents with columns for 'NAME', 'ALTERNATIVE NAME', 'ORGANIZATION', 'DEPARTMENT', 'ACTIVE', and 'STATUS'. The 'Commands' button is circled in red. A red arrow points from this button to a 'Commands' window that is open. This window contains a table with columns for 'NAME', 'DATE', and 'STATE'. The first two rows of the table are circled in red.

| NAME  | DATE                | STATE                |
|---|---------------------|----------------------|
| <input type="radio"/> Store Certificate       | 08/29/2017 15:58:20 | Successful           |
| <input type="radio"/> Generate Certificate    | 08/29/2017 15:56:16 | Successful           |
| <input type="radio"/> Generate Certificate    | 08/29/2017 15:19:50 | Successful           |
| <input type="radio"/> Discover Target Servers | 08/29/2017 13:28:08 | Successful           |
| <input type="radio"/> Discover Network        | 08/28/2017 17:40:29 | Successful           |
| <input type="radio"/> Update Configuration    | 08/28/2017 16:40:11 | Successful           |
| <input type="radio"/> Discover Target Servers | 08/28/2017 16:34:29 | Partially Successful |

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 screenshot shows the 'Certificates' section of the Comodo Certificate Manager. The 'Install' button is circled in red. A red arrow points from this button to a modal window titled 'SSL certificate auto-installation'. The modal window contains a table with the following data:

| NAME                   | COMMON NAME | BIND TO |
|------------------------|-------------|---------|
| F5                     |             |         |
| -Common-VS02_HTTP_8444 | ccmqa.com   | 8444    |

At the bottom of the modal window, there are 'Confirm' and 'Cancel' buttons.

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

The screenshot shows the 'Certificates' section of the Comodo Certificate Manager. The 'Install State' of the certificate 'ccmqa.com[96]' is now 'Started', which is circled in red. The table below shows the updated status of the certificates:

| COMMON NAME    | ORGANIZATION | DEPARTMENT | STATUS    | EXPIRES    | INSTALL STATE | RENEWAL STATE |
|----------------|--------------|------------|-----------|------------|---------------|---------------|
| ccmqa.com[96]  | docs         |            | Issued    | 08/29/2020 | Started       | Not scheduled |
| ccmqa.com[95]  | acme corp    |            | Invalid   |            | Not scheduled | Not scheduled |
| ccmqa.com[94]* | docs         |            | Unmanaged | 08/23/2018 | Not scheduled | Not scheduled |

When installation is complete:

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

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

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

| COMMON NAME                                    | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES    | INSTALL STATE    |
|--|--------------|------------|--------|------------|------------------|
| <input checked="" type="radio"/> ccmqa.com[72] | org1         |            | Issued | 01/19/2018 | Restart Required |
| <input type="radio"/> ccmqa.local[52]          | org1         |            | Issued | 01/14/2019 | Not scheduled    |

Administrators can restart the server remotely from the 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

Enrollment Certificate ID 77875

Type **Instant SSL**

Server Software **Apache/ModSSL** View Edit

Server Software State **Restart Required** Restart

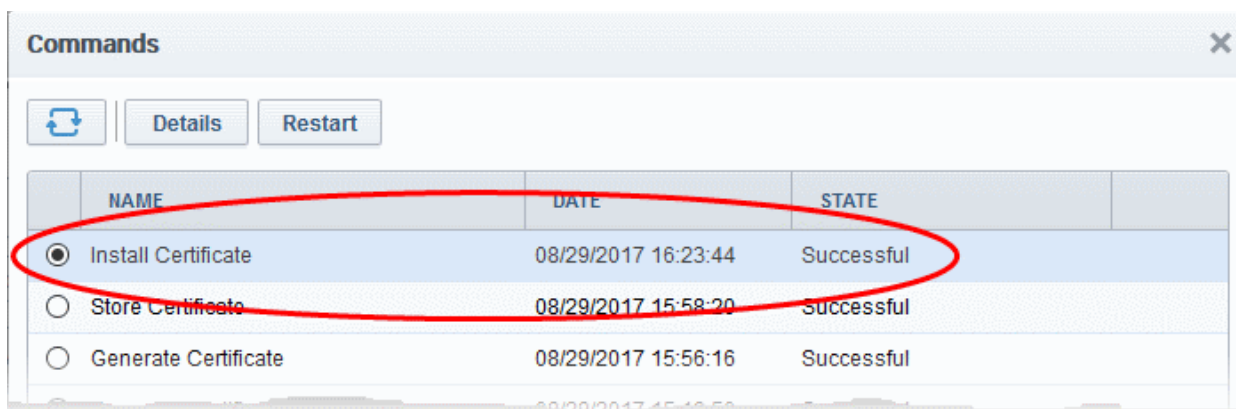
Term **1 year**

Owner admin 1 Resend Edit

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

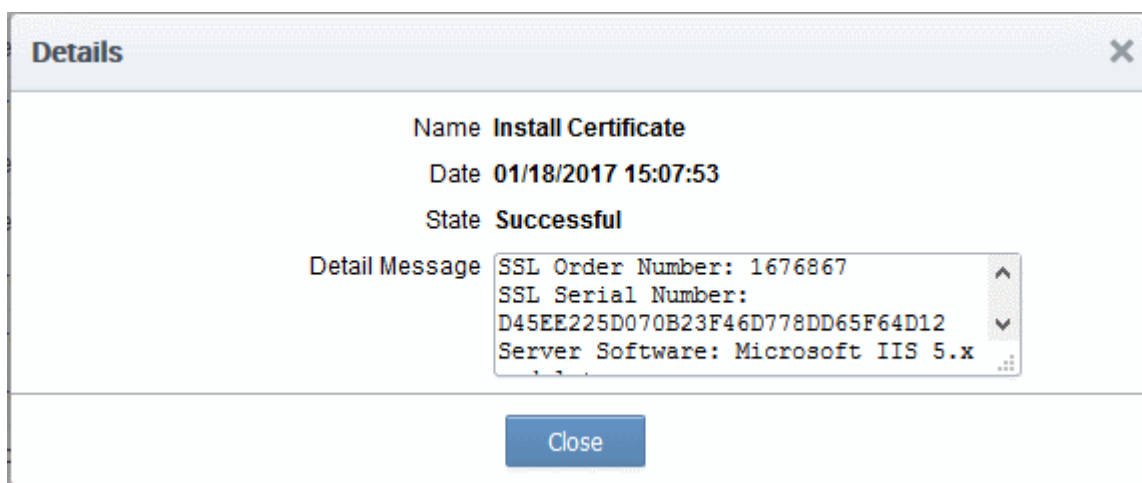
- To check whether the controller has installed the certificate, click Settings > Agents > Network Agents
- Select the controller and click the 'Commands' button

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



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

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



**Details**

Name **Install Certificate**  
Date **01/18/2017 15:07:53**  
State **Successful**

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

Close

## 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**

3<sup>rd</sup> floor, Office Village Exchange Quay

Trafford Road, Manchester, M5 3EQ

United Kingdom

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767