COMODO
Creating Trust Online®

Comodo
Certificate Manager

Comodo Certificate Authority Proxy Server Installation Guide (For Windows Server 2008 / 2008 R2)

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

Table of Contents

1. Prerequisites ... 3
1.1.Server Requirement ... 3
1.2.Client Requirement ... 3
2. Active Directory Certificate Services (AD CS) Installation ... 3
3. Comodo CA Proxy Service Installation ... 4
4. Configure Certificate Enrollment Policy ... 11
5. Deploy Trusted Root Certificates ... 15
6. Configure Templates at Active Directory ... 18
7. Map Templates to CCM Certificate Types ... 28
8. Configure Active Directory Users ... 30
9. Enrollment and Auto-Enrollment ... 33
10.Configure MS Agents for Certificate Discovery and Issuance ... 38
10.1.Configure Stand-Alone MS Agents ... 40
10.2.Configuring Clustered MS Agent ... 42
10.3.Configure Active Directory Discovery Tasks ... 46
10.3.1.1.Prerequisites ... 48
10.3.1.2.Overview of Process ... 48
10.3.1.3.Add Domains and Start Scanning ... 48
10.3.1.4.Editing an AD Discovery Task ... 52
10.3.1.5.Deleting an AD Discovery Task ... 53
10.3.1.6.View History of AD Discovery Task ... 54
10.3.1.7.View Results of AD Discovery Scan Tasks ... 58
11.Troubleshooting ... 60
11.1.Enrollment Failure ... 60
11.2.Unsupported Editions of Windows 2008/R2 ... 60
About Comodo CA ... 61

1. Prerequisites

1.1. Server Requirement

- Windows Server 2008 /2008 R2 (Standard/Enterprise/Datacenter)
  - Active Directory Domain Services
  - Active Directory Certificate Services (AD CS), installed as enterprise root Certificate Authority (CA)

Certificate Manager Server (CCM) running under JRE 1.6., must be accessible from Active Directory Certificate Services host. CCM Server's URLs must be assigned to Trusted Zone.

Remark: Server platform can be 32 or 64 bit, both of them are supported. AD CS must be installed before Comodo CA Proxy. Additional components such as Web Enrollment Services and Network Device Enrollment Services are not included in Standard edition of Windows Server 2008.

Following features are available on servers running Windows Server 2008 that have been configured as CAs.

AD CS features	Standard	Enterprise	Datacenter
Version 2 and version 3 certificate templates	No	Yes	Yes
Key archival	No	Yes	Yes
Role separation	No	Yes	Yes
Certificate Manager restrictions	No	Yes	Yes
Delegated enrollment agent restrictions	No	Yes	Yes

Basically, Certificate Authority component can not be installed on Windows Server 2008 Web-edition, so there is no corresponding column in this table.

1.2. Client Requirement

- Windows 7 (32/64 bit) workstation as domain member
- Domain user account

2. Active Directory Certificate Services (AD CS) Installation

We recommend that you install the Comodo AD agent on a server without AD CS role pre-installed. It is the easiest way to get the correct AD CS role configuration for integration with CCM. To continue with this approach, please skip to section 3. However, if you decide to configure AC CS role independently, please refer to "Active Directory Certificate Services Role installation guide".

If the Comodo AD Agent finds that the AD CS role is already installed it will use existing configuration of AD CS.

3. Comodo CA Proxy Service Installation

Prerequisite: The Comodo CA Proxy Service can be installed only if AD integration is enabled for your CCM account. Please contact your Comodo account manager to ensure that AD support is enabled.

The service requires agent software to be installed on the server. The agent can be downloaded only by an MRAO administrator who has the 'MS AD Discovery' privilege. Please ensure that your MRAO admin has that privilege so they can provide the agent to you.

1. Make sure that you are logged on to the server as a domain administrator.
2. Click 'Start', point to 'Administrative Tools' then click 'Server Manager' (or click the 'Server Manager' button on the task bar).
3. If AD CS role is pre-installed, then the Microsoft AD CA service should be stopped to continue the installation of Comodo CA Proxy Service. To do this, Select 'Roles', expand it and then select and expand the 'Active Directory Certificate Services' node. Select the previously installed Microsoft AD CA service and click the 'Stop' button on the 'Server Manager' page. See the Figure 3.1 for details.

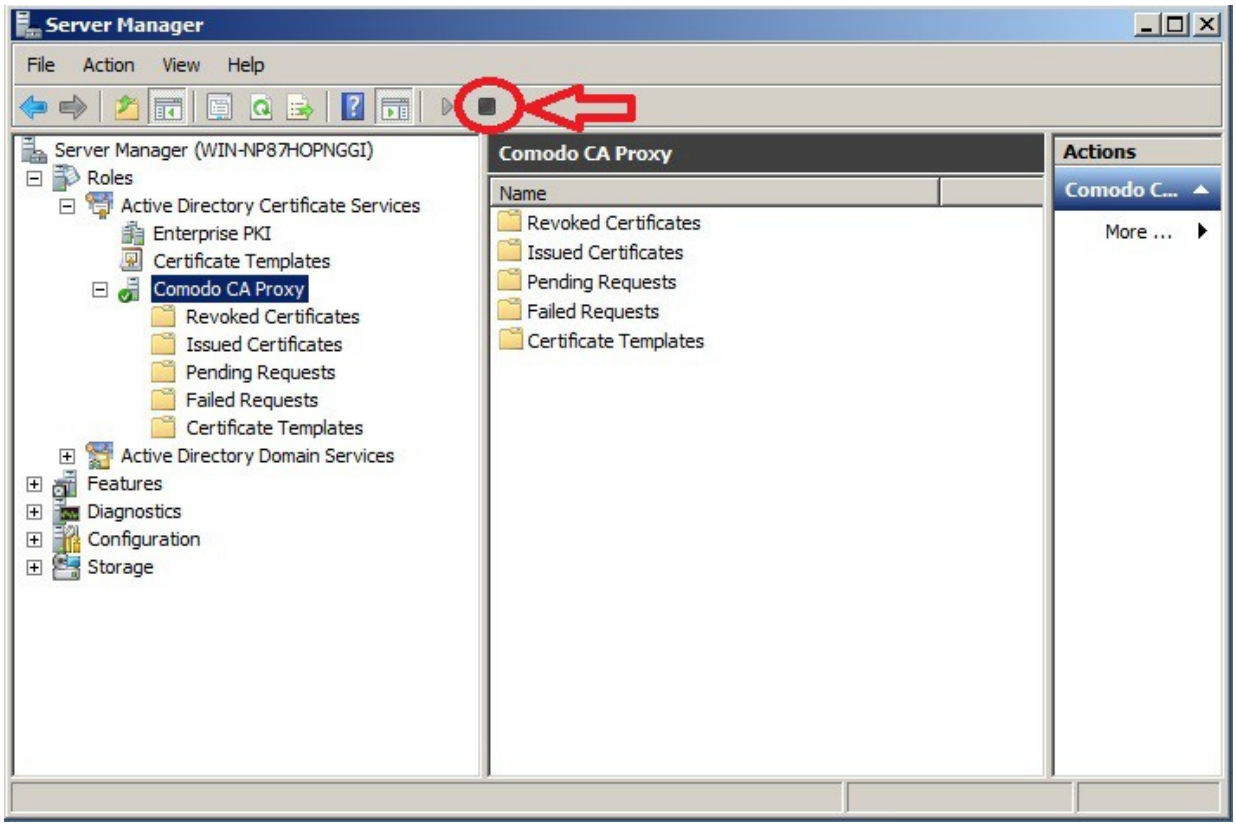
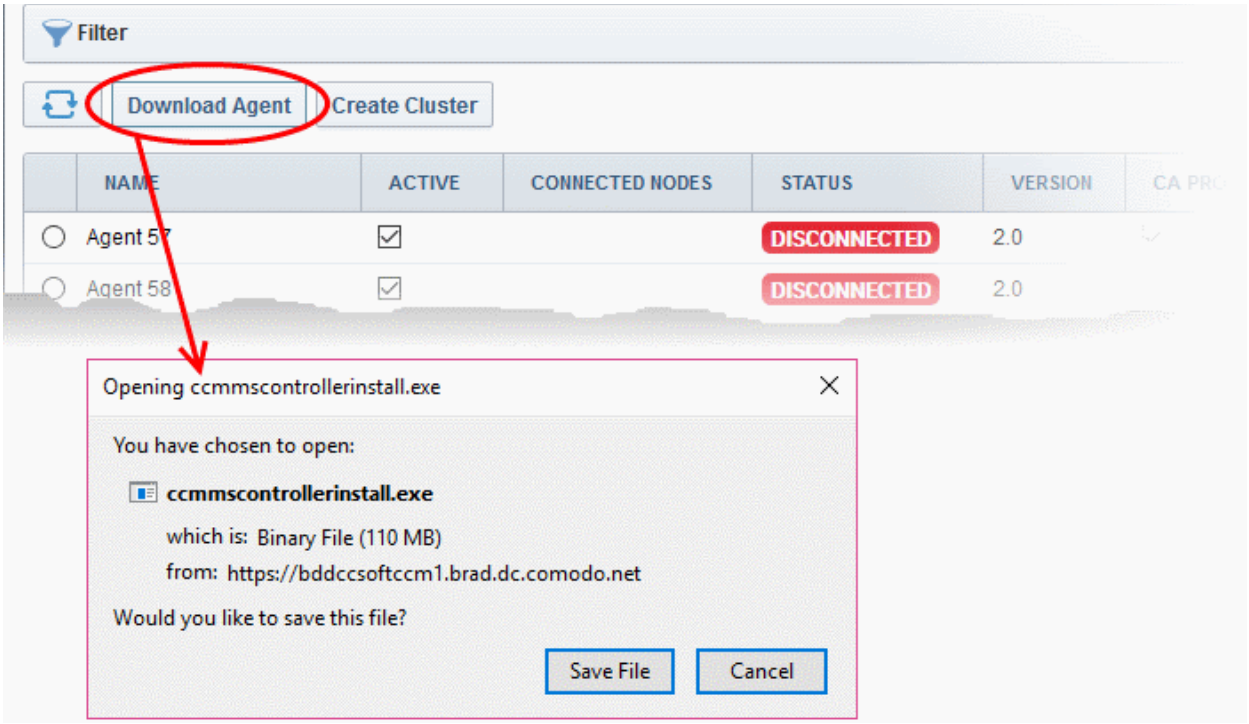


Figure 3.1

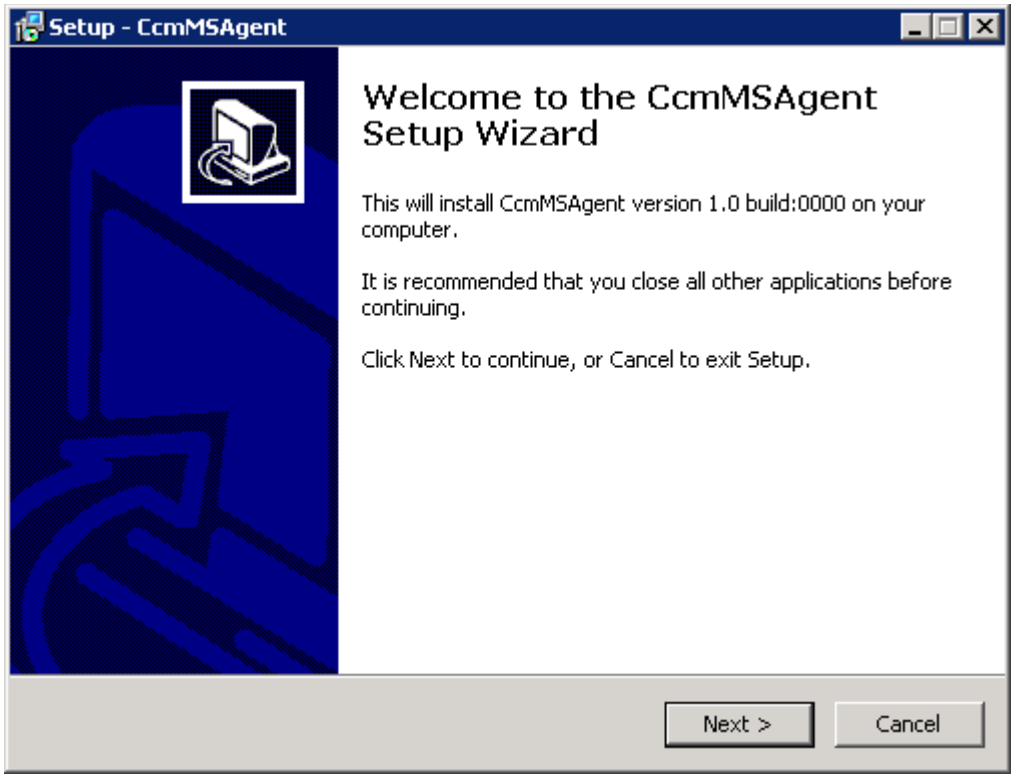
4. Download and install the MS Agent. To do this:
    - Login to CCM using as MRAO administrator with MS AD Discovery privileges



- Select the 'Settings' tab then 'Agents' >' 'MS Agents' then click 'Download Agent'.
- Save the agent setup file, 'ccmmscontrollerinstall.exe'

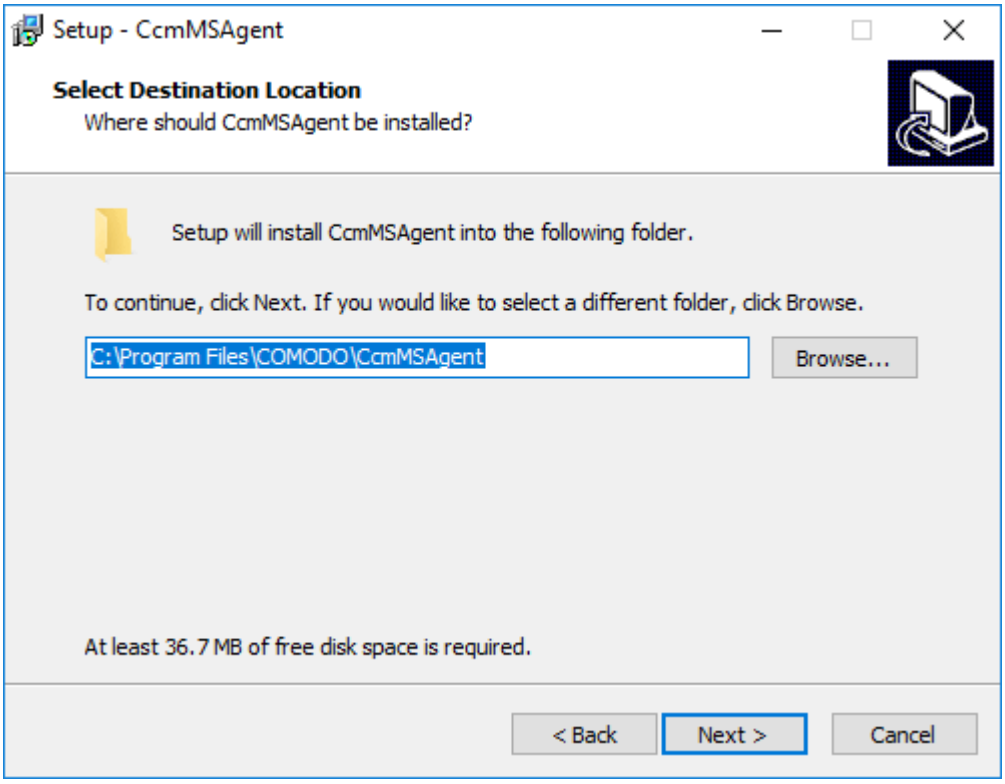
5. Start 'ccmmscontrollerinstaller.exe' from the command line or explorer

Note: The agent setup process will uninstall any previous versions of the agent.

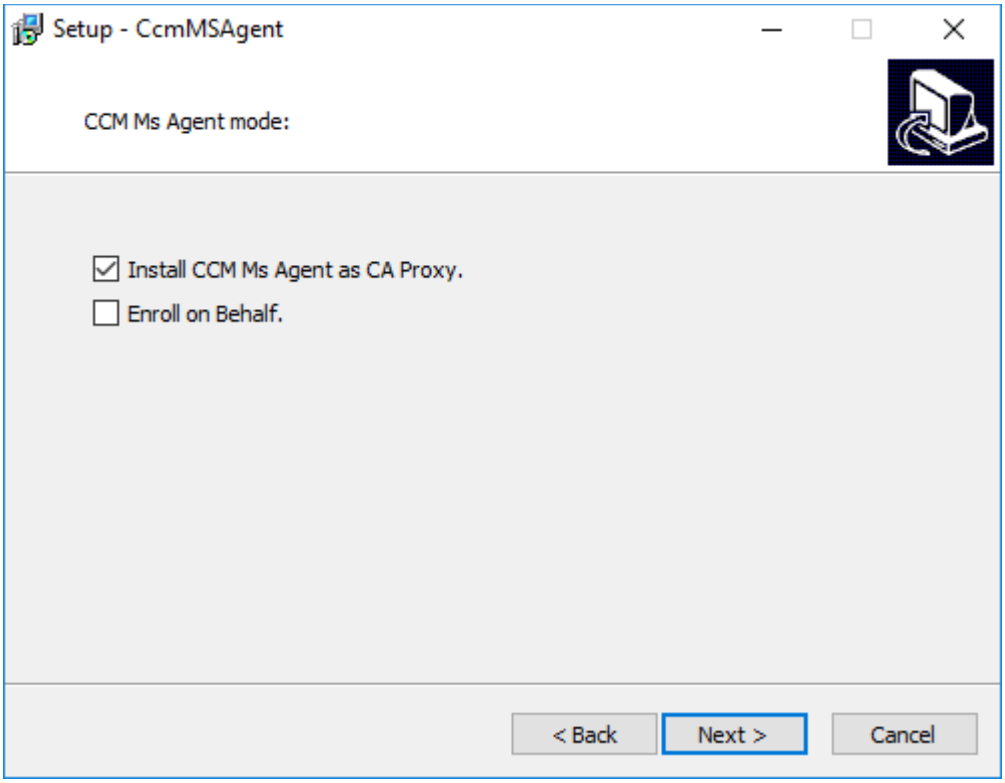


6. Click 'Next'

7. Read the end-user license agreement (EULA) and accept to it to continue the installation. The next step allows you to specify the installation location for the agent.



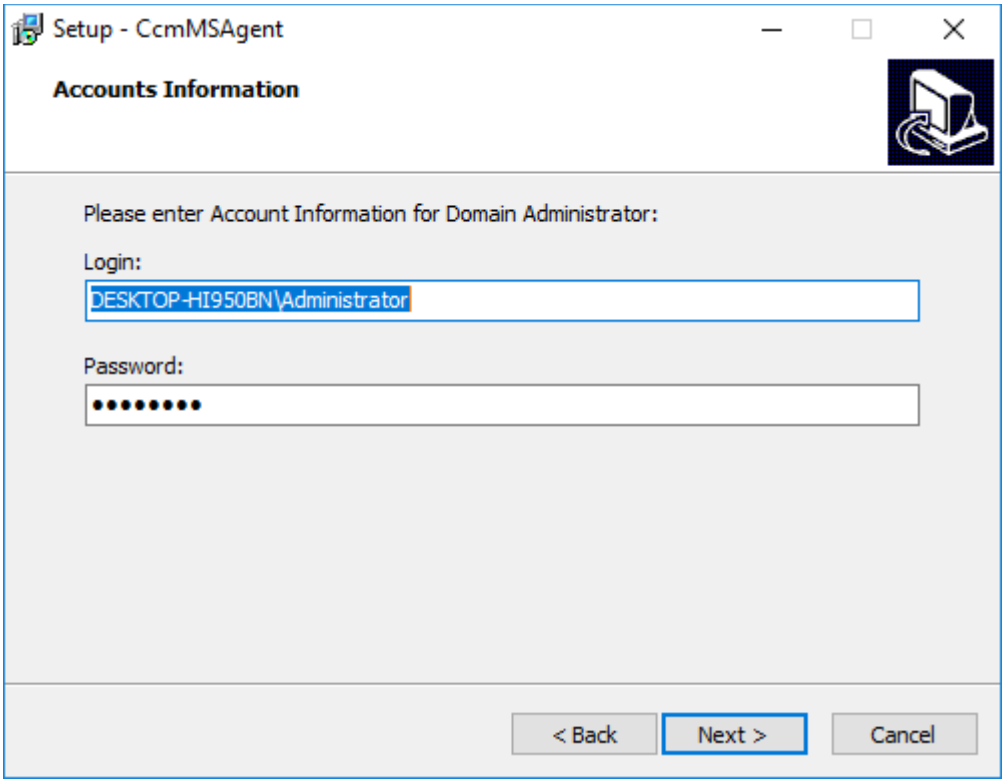
8. The default installation folder is C:\Program Files\COMODO\CcmMSAgent\ You can change this by clicking the 'Browse...' button:
9. Click 'Next'



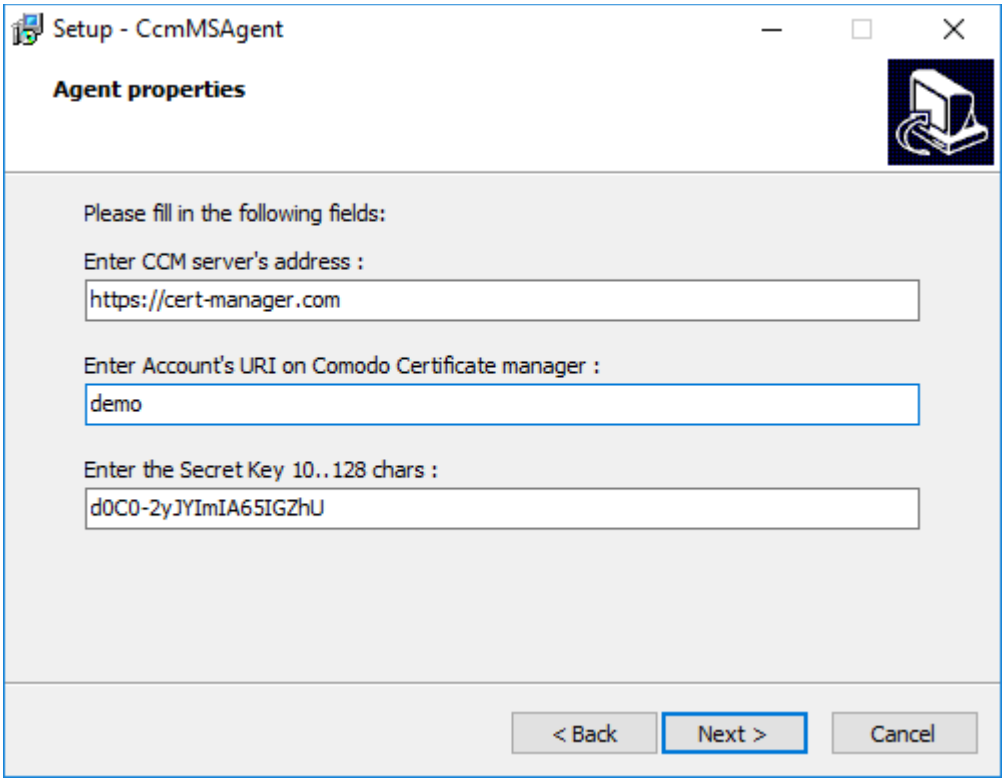
Agent installation preferences

- **Install CCM MS Agent as CA Proxy (*default*)** - Device certificates will be generated through NDES. Will also enable the discovery of AD objects.
- **Enroll on Behalf** – Device certificates will be generated through MS CA. Will also enable the discovery of AD objects.
- Please note if you prefer both options then install the agent on a server without MS CA that you plan to use.

10. Click 'Next'. The 'Accounts Information' step will be displayed if you opt for 'Enroll on Behalf'.



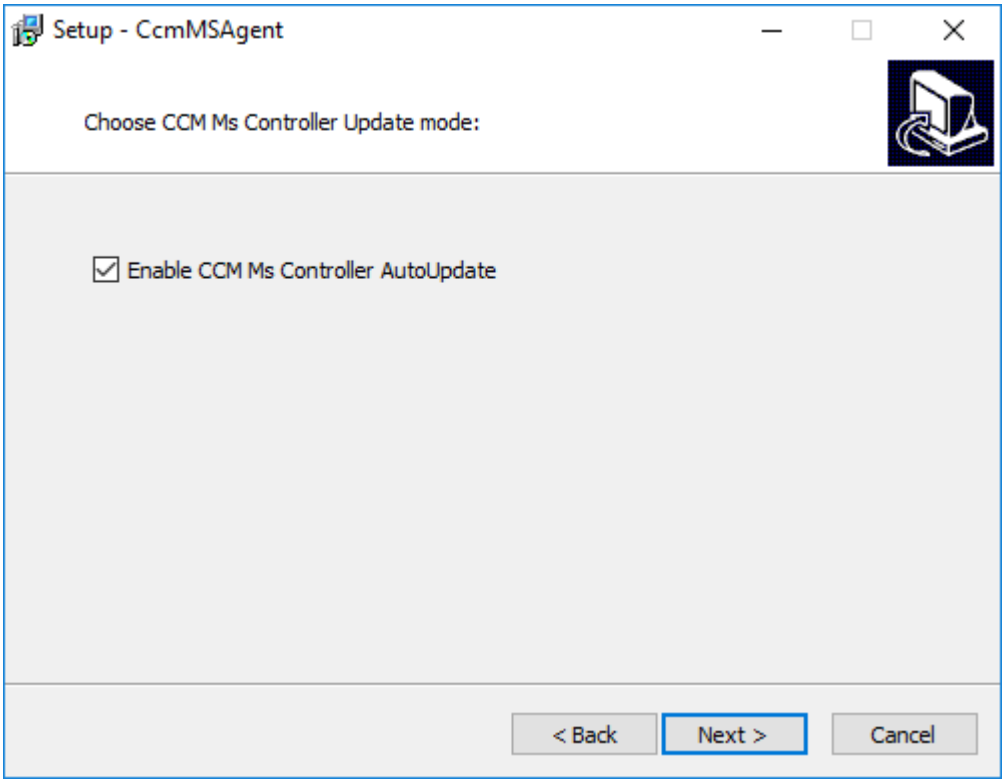
11. Enter the domain admin credentials and click 'Next'



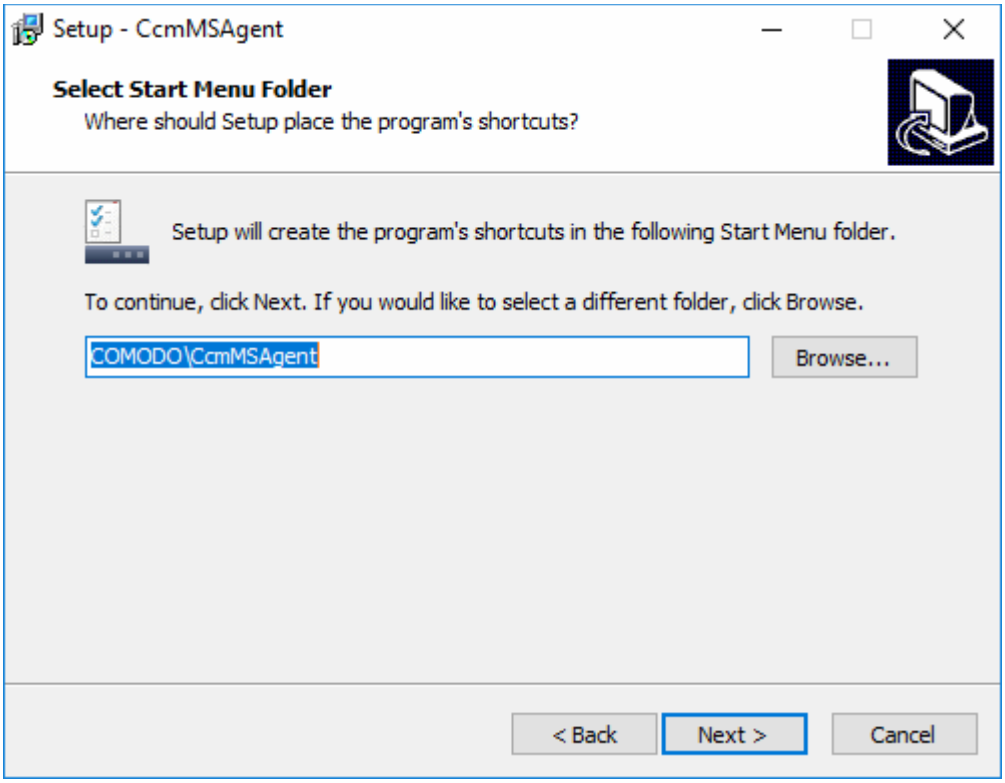
12. The fields are auto-generated:

- **Enter CCM server's address** – The URL of your CCM instance. Don't alter this.
- **Enter Account's URI on Comodo Certificate manager** – The URI for your account configured by CCM. Don't alter this. The URI of your CCM account is displayed at the end of your CCM instance URL. For example if the URL is https://demo.cert-manager.com/customer/demo, the last part after 'customer' is the URI.
- **Enter the Secret Key** – This is an authentication key auto-generated for the purpose of connecting to CCM. You can enter a pre-configured key here if required. After downloading the agent, it will be displayed in the CCM interface with status as 'N/A'.
- Go to Settings > Agents, then click ' MS Agents'. Select it and click 'Edit' at the top. In the 'Secret Key' field, change it to your preferred key, copy it and store. Click 'OK' to save your settings. Enter the copied key in this field.

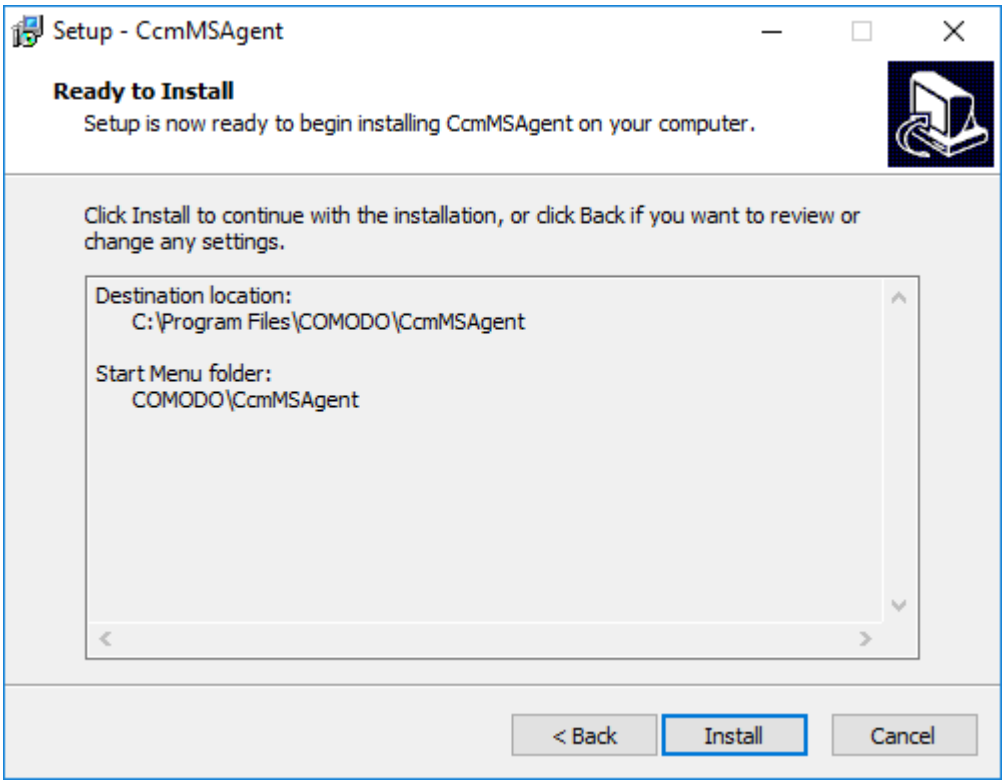
13. Enable CCM Ms Controller AutoUpdate - If selected, the MS Agent will be automatically updated to available new versions.



14. Click 'Next'. The next step allows you to select the start menu folder for the agent. The default location is COMODO/CcmMSAgent.



15. Change the location if required and 'click Next'



16. Review CcmMSAgent settings and click 'Install' to continue the installation

Check the agent is installed properly and ready to enroll certificates through Comodo CA:

- Navigate to 'Start Menu' > 'Administrator Tools'> 'Services'> 'Active Directory Certificate Services'
  - In the 'General' tab > Service name: CertSvc
  - Path to executable: C:\\Programs File\COMODO\CcmMSAgent\bin\ccm_ca.exe/w

17. Click 'Start', point to 'Administrative Tools', and then click 'Server Manager'. Or click the corresponding button on the task bar. Select the 'Roles Summary' section, expand it and then select and expand the 'Active Directory Certificate Services node'. Locate Comodo CA Proxy service. Make sure that the service is started. **Figure 3.1** shows running state of this service.

    Otherwise, try to start this service manually.

Note: To enable device certificates enrollment, NDES service is to be installed under AD CS role. For guidance on this, please refer to the online guide at:

http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx

4. Configure Certificate Enrollment Policy

1. Make sure, that you are logged on to the appropriate server as a domain administrator.
2. If the window with server manager is not open, click 'Start', point to 'Administrative Tools' and then click 'Server Manager' (or click the 'Server Manager' button on task bar).

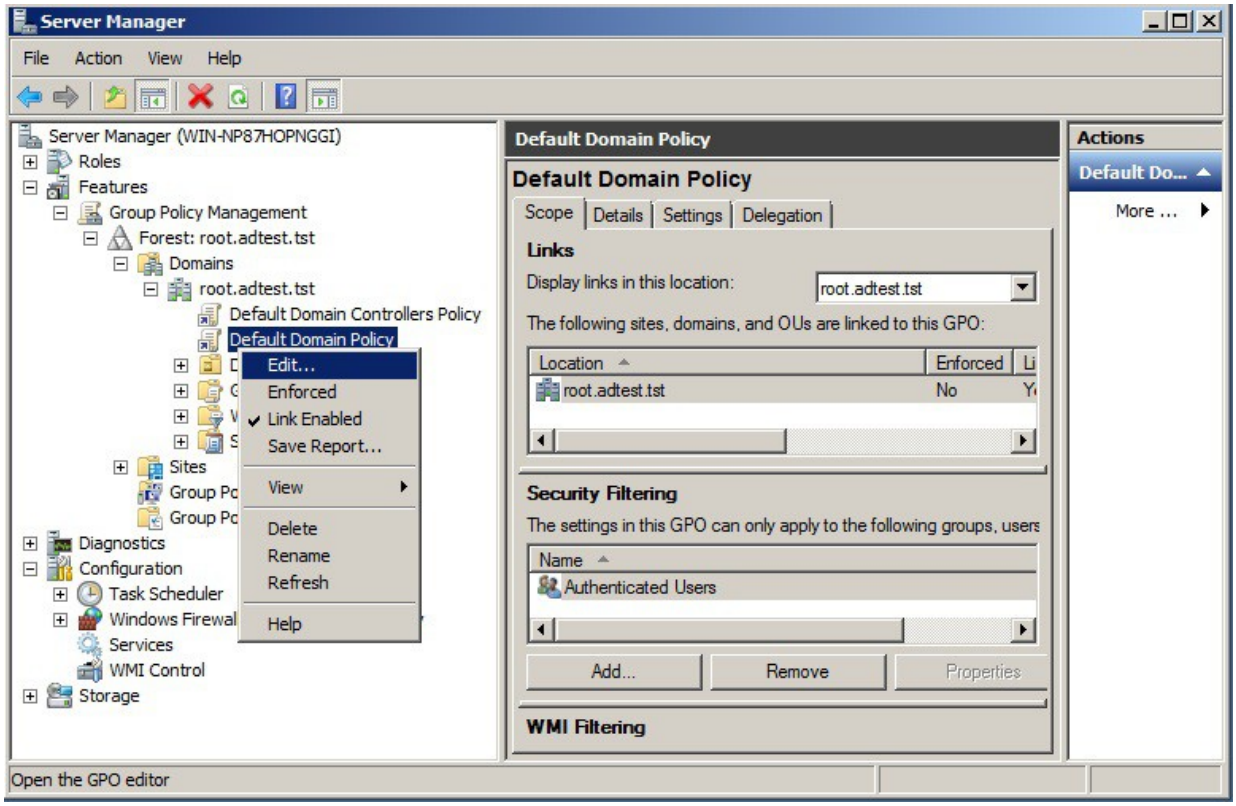


Figure 4.1

3. Select the 'Features' node, expand it according to Figure 4.1. Right-click and select 'Edit...' on 'Default Domain Policy. The Group Policy Management Editor will be displayed.

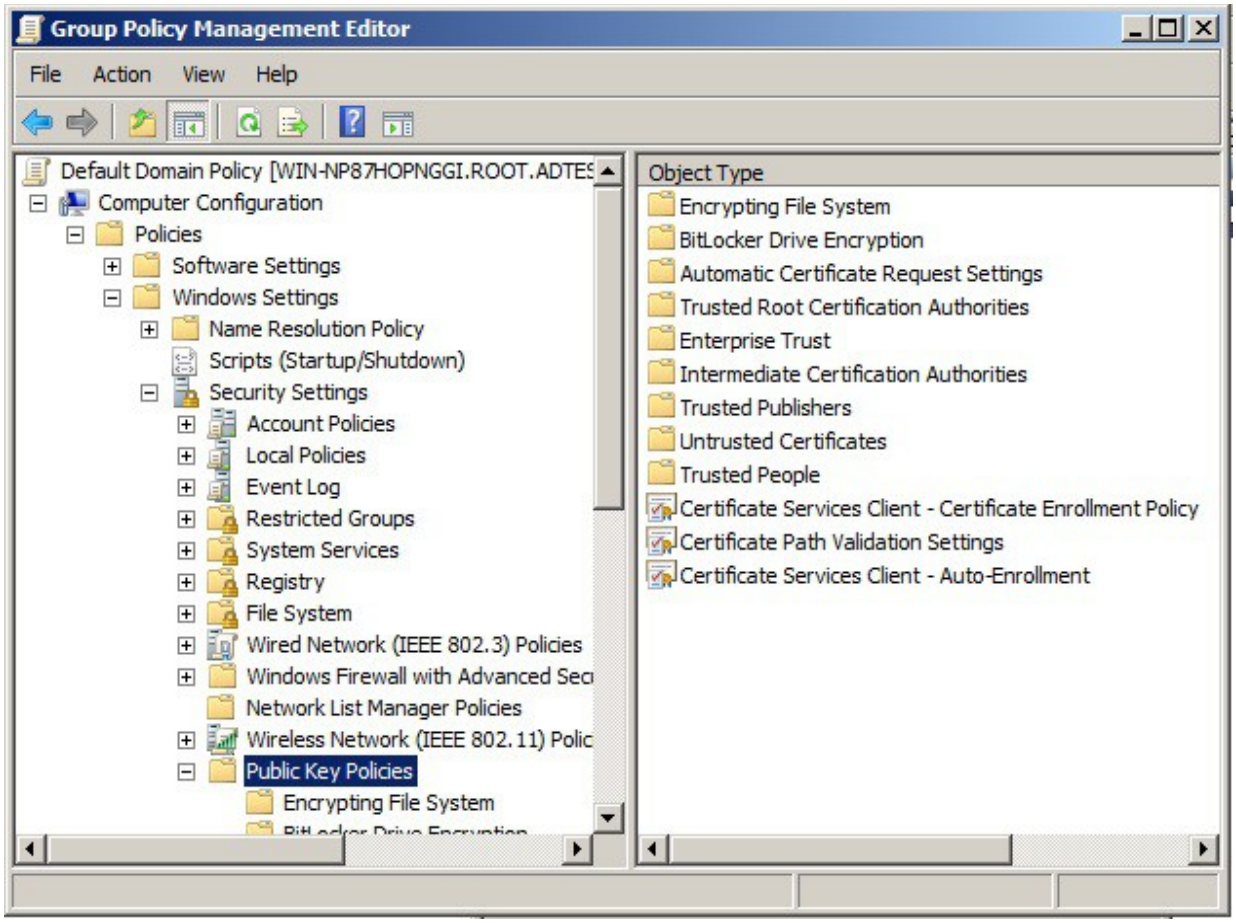


Figure 4.2

4. Select Computer configuration-->Policies-->Windows settings->Security Settings-->Public key policies.
5. In the 'Object Type' list, double-click on the Certificate Services Client - Certificate Enrollment Policy. Switch the configuration model to 'Enabled'. Make sure that this Active Directory Enrollment Policy is used as default. The 'Default' check box must be selected. The 'Automatic Enrollment' column must contain the value 'Enabled'. Otherwise, enable this policy in the next step.

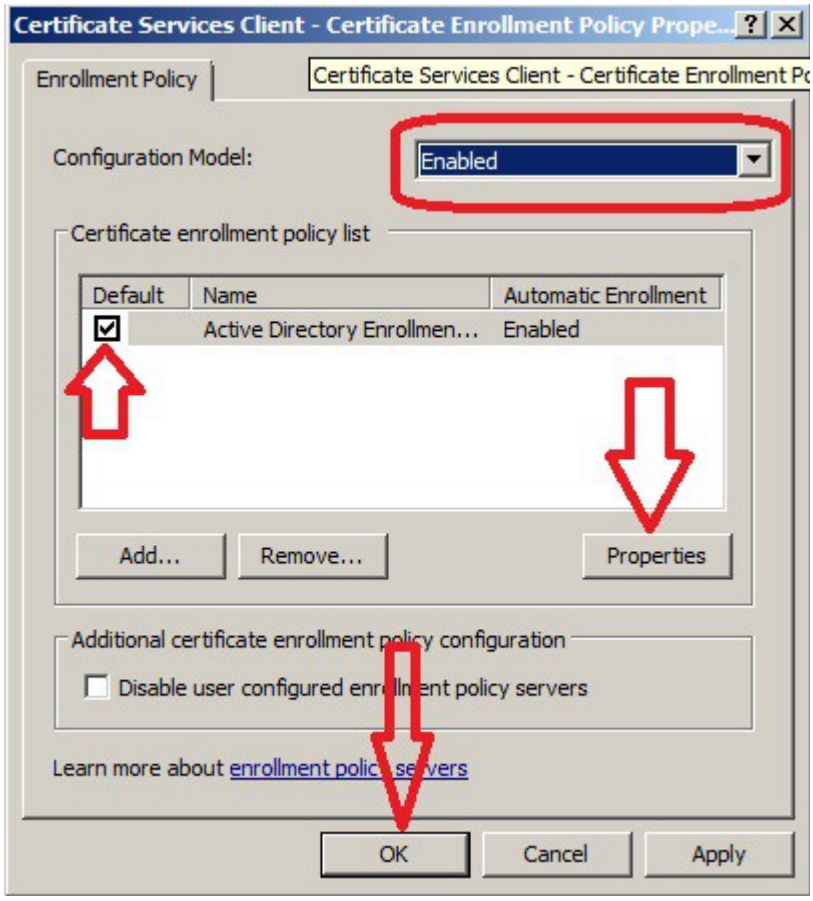


Figure 4.3

6. Press the 'Properties' button. Make sure, that all options in the 'Enrollment Configurations' group box are selected. 'Enrollment policy servers' list must contain a record with “LDAP” as Server URI and “Windows Integrated” as Authentication type. Such configuration is displayed at Figure 4.4

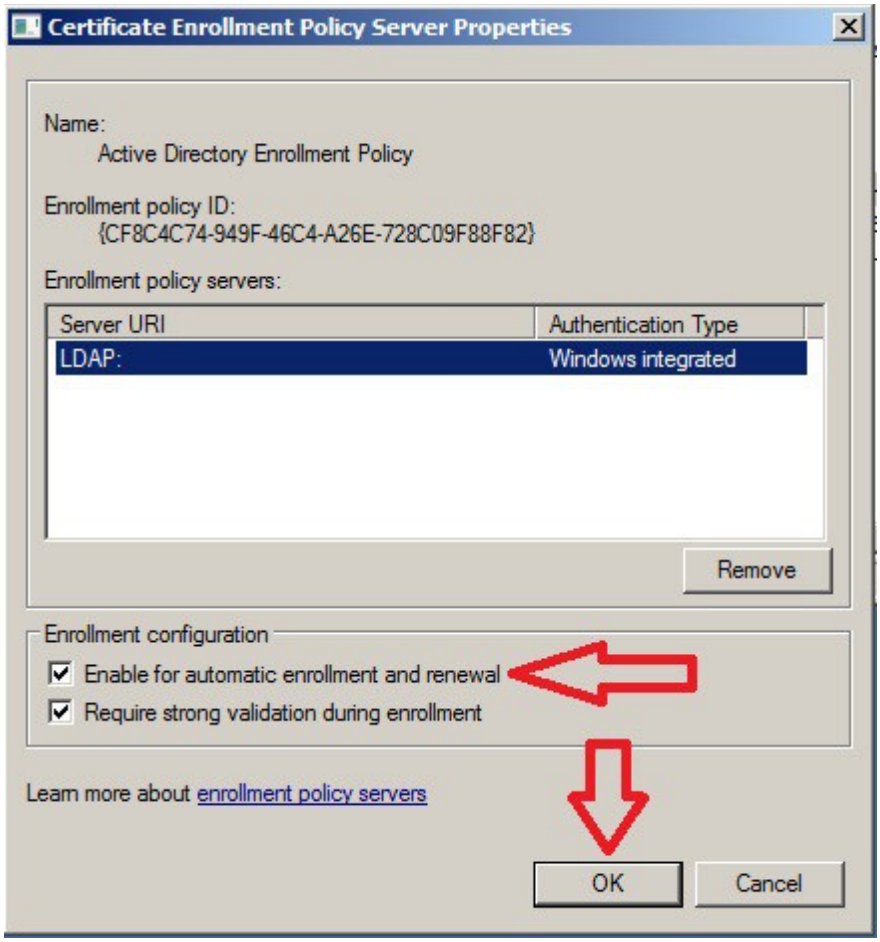


Figure 4.4

7. Click the 'OK' button to apply changes and close this window. Click the 'OK' button on the 'Certificate Services Client - Certificate Enrollment Policy Properties' form to apply changes and close this window.

Remark: This section is about the minimal configuration of Certificate Enrollment Policy. Basically, it is required for enrollment and auto-enrollment functionality for domain-joined users. But if you need to use extended features, such as web-enrollment services, you must add other enrollment policy.

8. In the **Object Type** list (**Fig**ure 4.2) double click on the Certificate Service Client - Certificate Auto-enrollment. Switch configuration model to 'Enabled'. It is recommended to activate the options which allow renew expired certificates, update pending certificates, renew revoked certificates and update certificates, that use certificate templates.

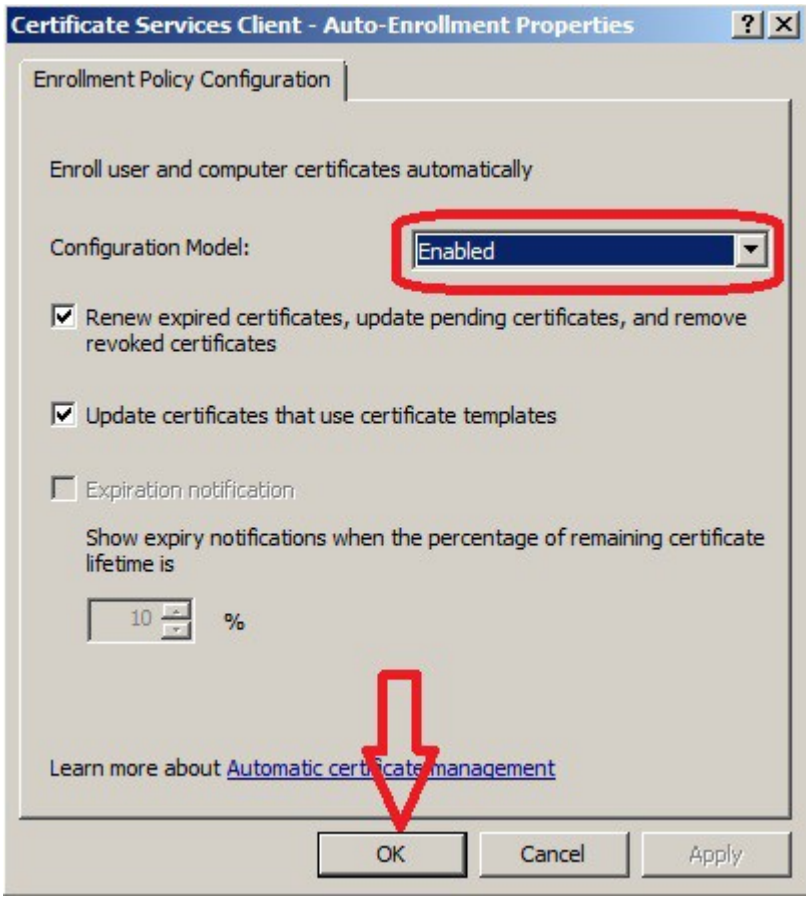


Figure 4.5

9. Press the 'OK' button to apply changes and close this window.

5. Deploy Trusted Root Certificates

1. Import Comodo CA's root and intermediate certificates to Group Policy. Open Group Policy Object Editor, go to Computer Configuration->Windows Settings-> Security Settings->Public Key Policies->Trusted Root Certificate Authorities (In Windows Server 2008 navigate to Computer Configuration->Policies->Windows Settings->Security Settings->Public Key Policies->Trusted Root Certificate Authorities)

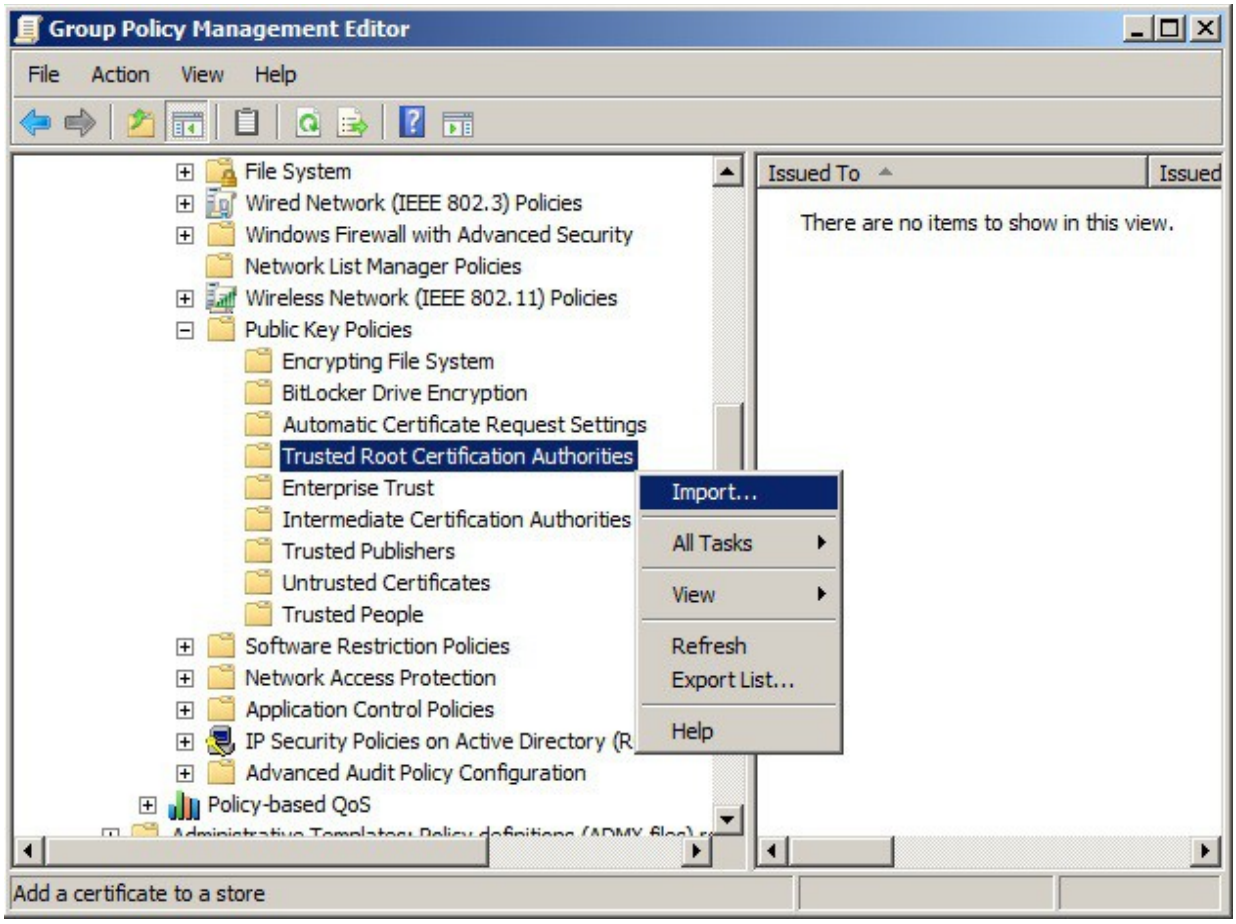


Figure 5.1

2. Click 'Import...' option from popup menu, then click the 'Next' button and input location of file with certificates. Basically, trusted cerficicates are located at \Trusted sub-folder of destination folder, that was entered to installer program at section 3, step 6. By default it is C:\Program Files \COMODO\CcmMSAgent\Trusted\

Figure 5.2 Certificate Import Wizard

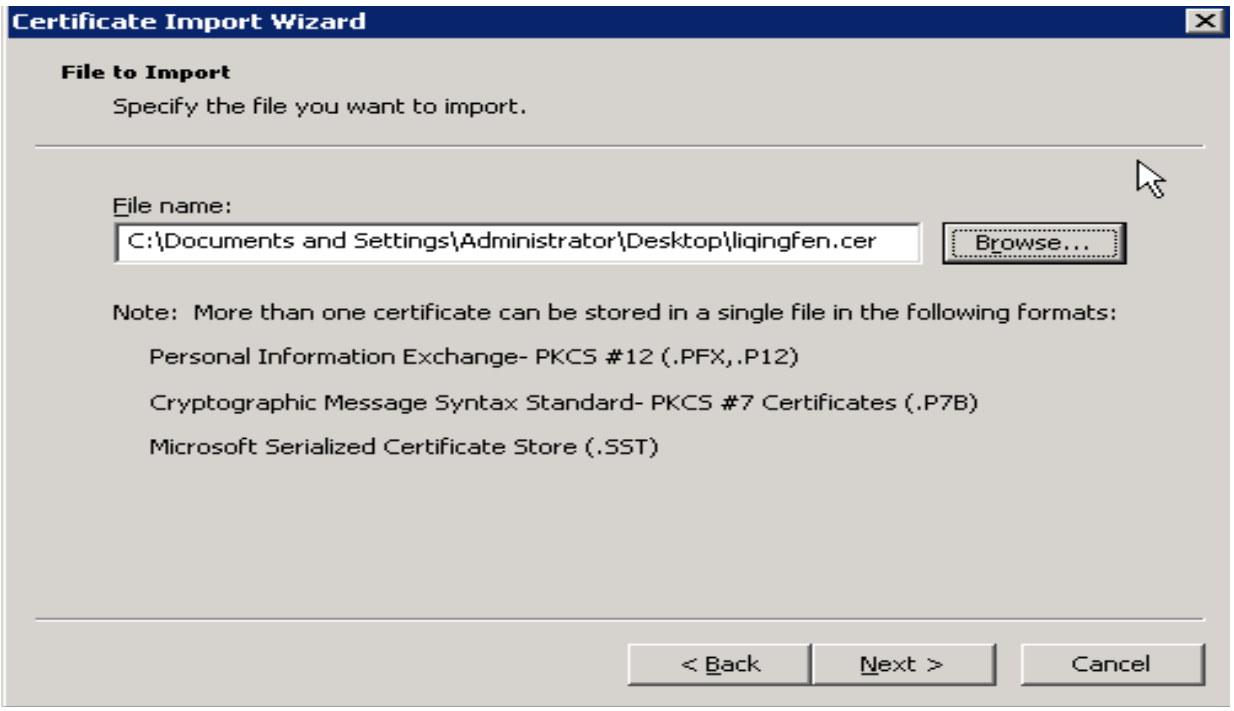


Figure 5.3

3. Select certificate to import

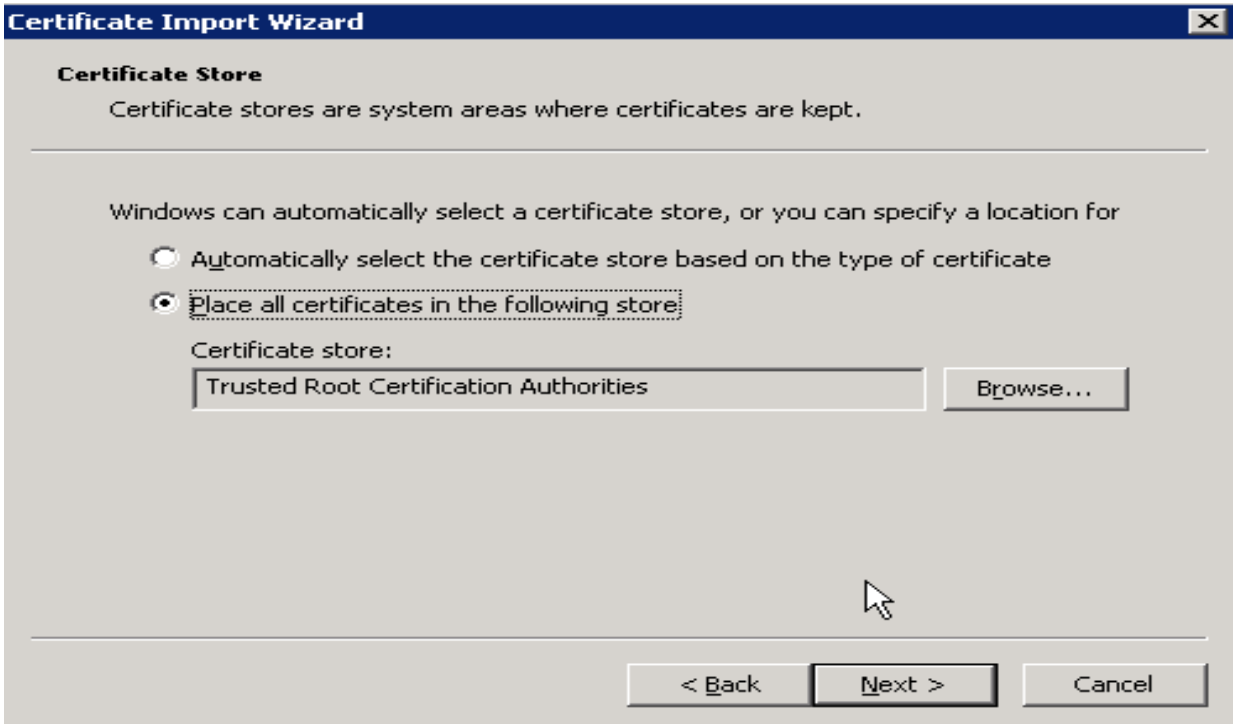


Figure 5.4

4. Select certificate store

Figure 5.5 Import complete

5. Press 'Finish' to close wizard. After importing, you should see certificates in Group Policy. You should do this action for each file with trusted certificates.

6. Configure Templates at Active Directory

CCM can issue private certificates with custom parameters by mapping CCM private certificate types to custom Active Directory certificate templates. Custom parameters include key usage, extended key usages, key sizes,

validity period and so on. This section explains how to create custom certificate templates for mapping to CCM private certificate types.

1. Log on to the appropriate server as a domain administrator.
2. Click 'Start', point to 'Administrative Tools', and then click 'Server Manager', or click corresponding button on task bar.
3. Select 'Roles' > 'Active Directory Certificate Services' > 'Certificate templates'
4. Right-click on a suitable template and choose 'Duplicate Template' from the right click options

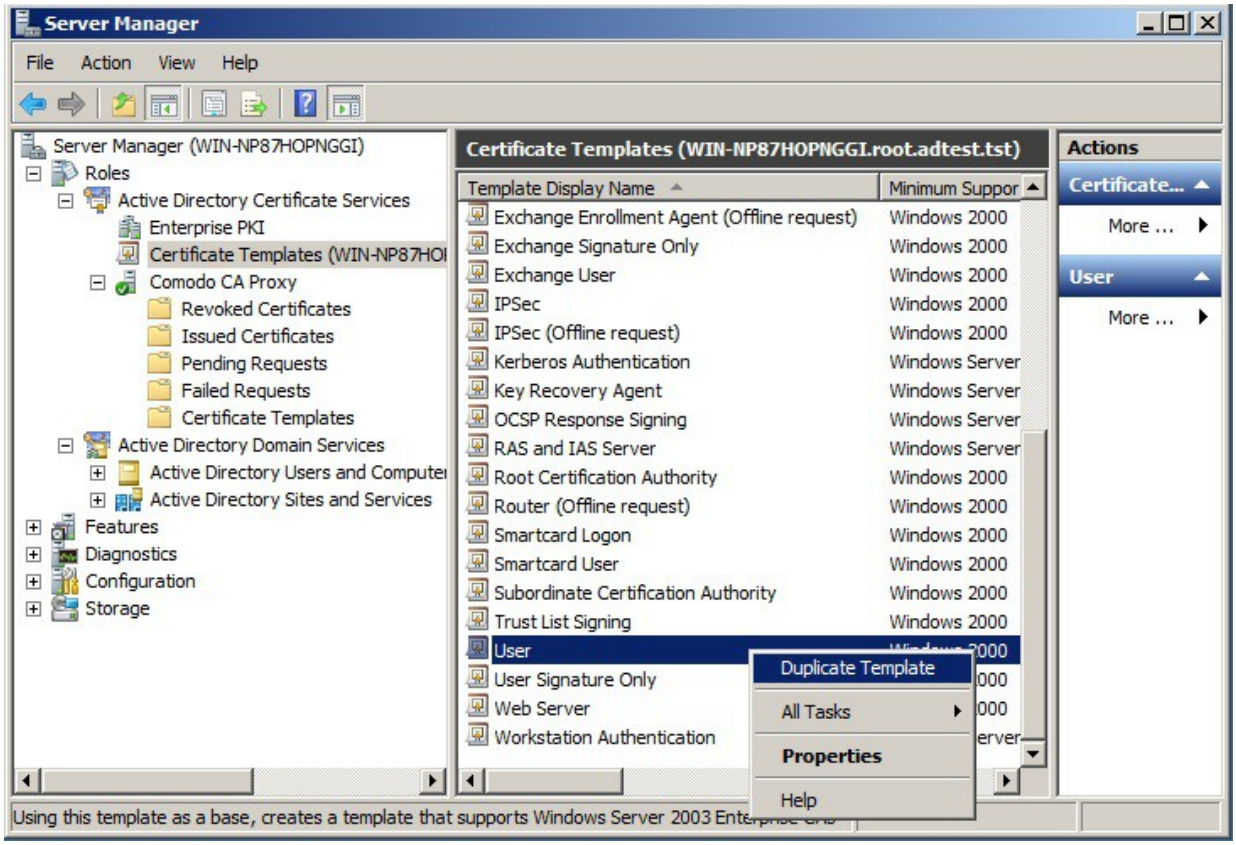


Figure 6.1

5. Choose the compatibility of the new template. It is recommended to choose it according to the OS versions on the CA Proxy server and workstations. Click 'OK' to save your choice.

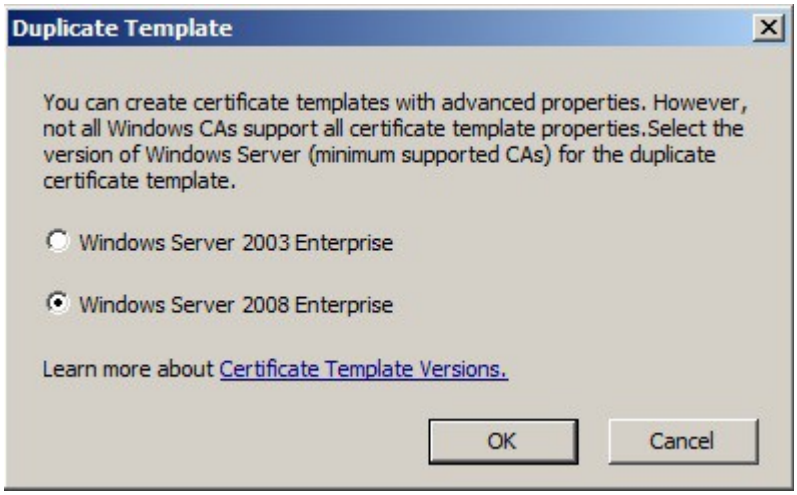


Figure 6.2

6. Enter 'Template Display Name' and 'Template Name'.

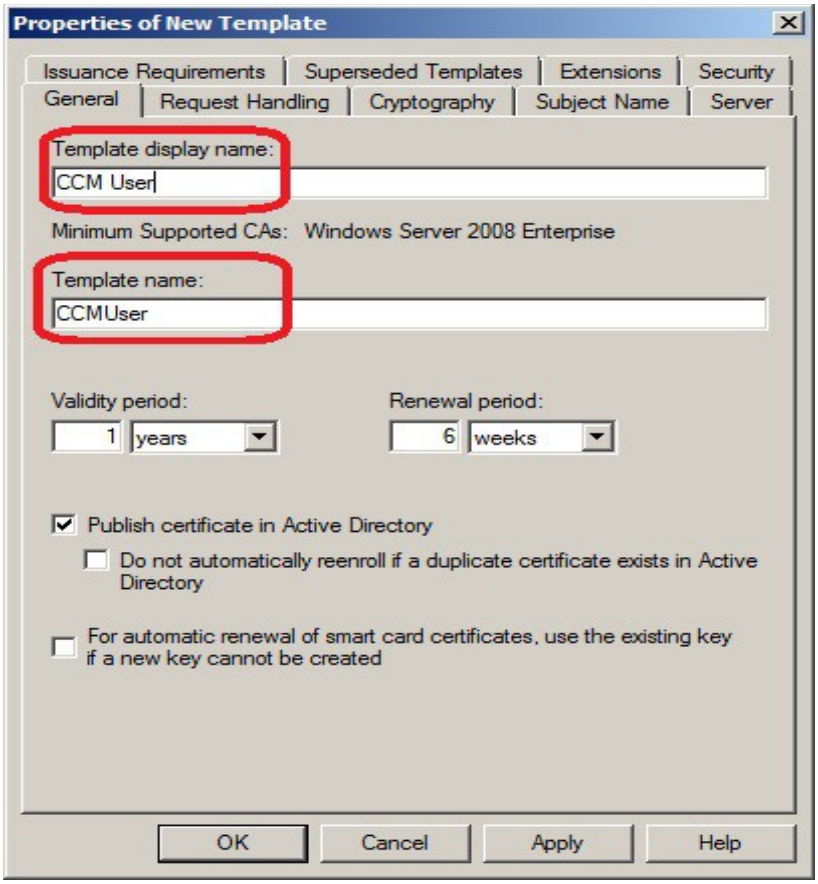


Figure 6.3

7. Set the necessary permissions to this template. Switch to 'Security' tab. For users that enroll for certificates using this template, you should set 'Read', 'Enroll' and 'Autoenroll' permissions.

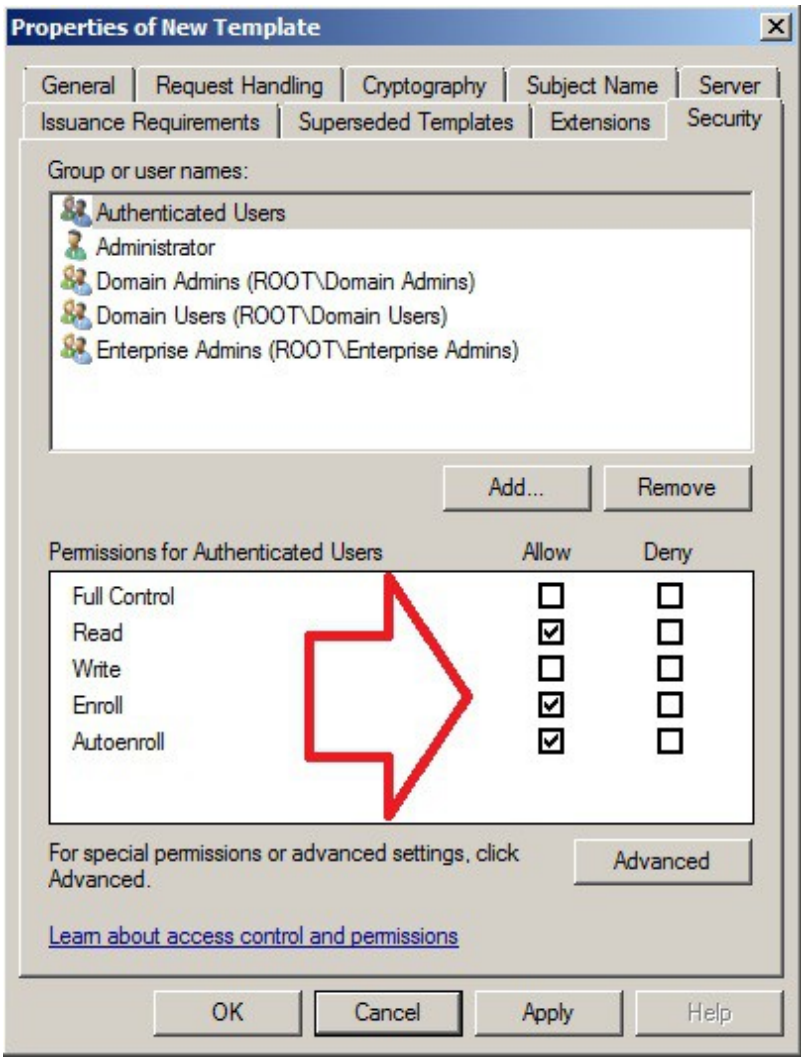


Figure 6.4

Note: 'Write' permission allows users to modify the properties of the template, so it is not recommended to set this permission for all users.

8. Click 'Apply' to commit your changes.
9. Open the 'Extension' tab and select 'Application Policies'. Click 'Edit...'

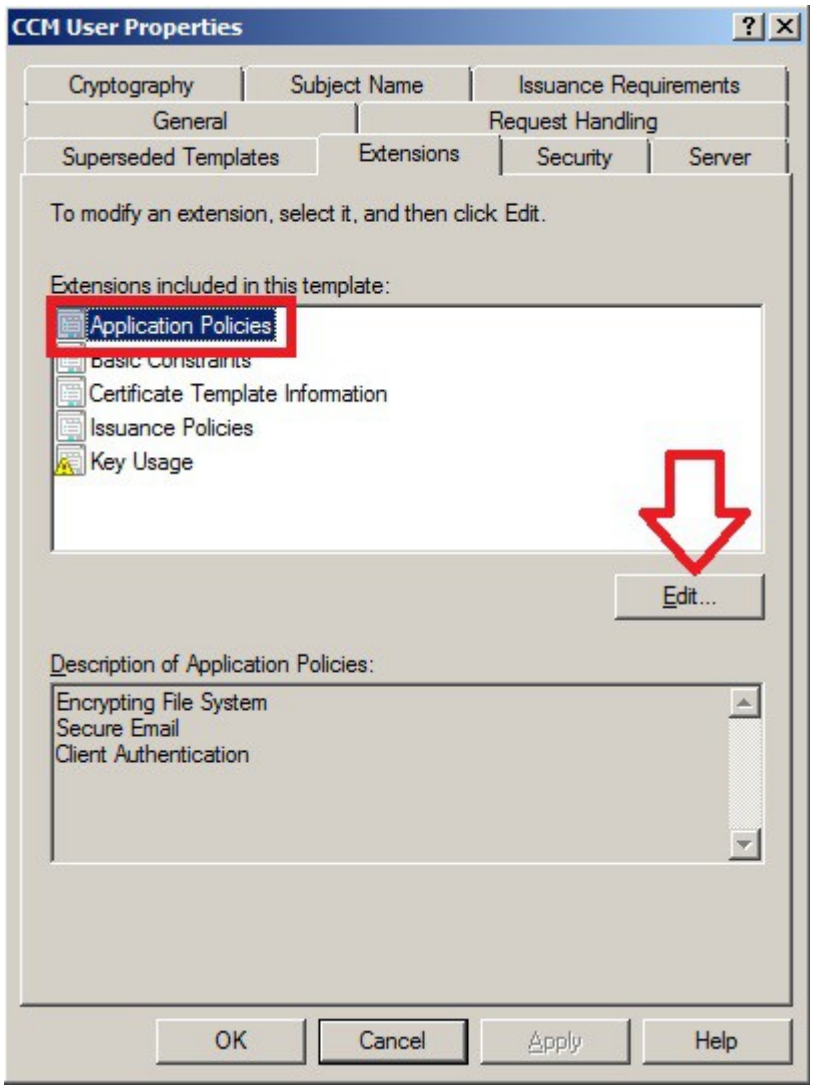


Figure 6.5

Now you will be able to add, edit or remove application policies for this template from the set of application policies.

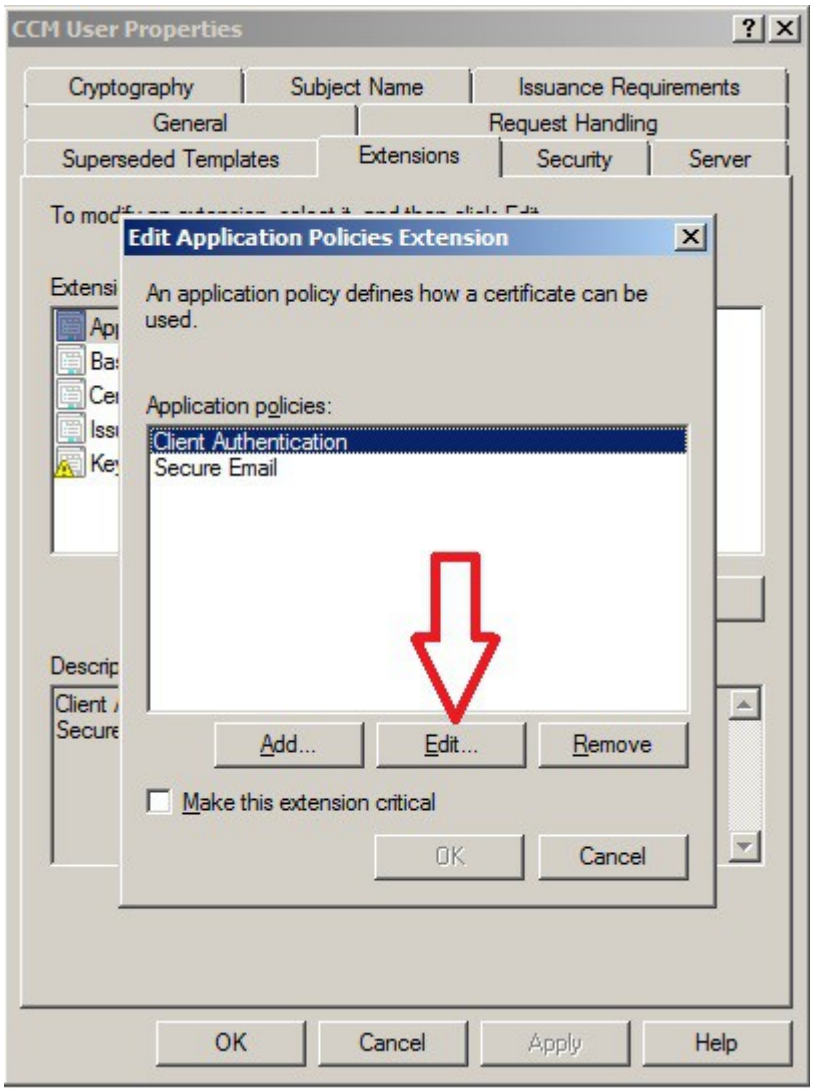


Figure 6.6

10. To view or edit the OID of a selected application policy, click Edit...

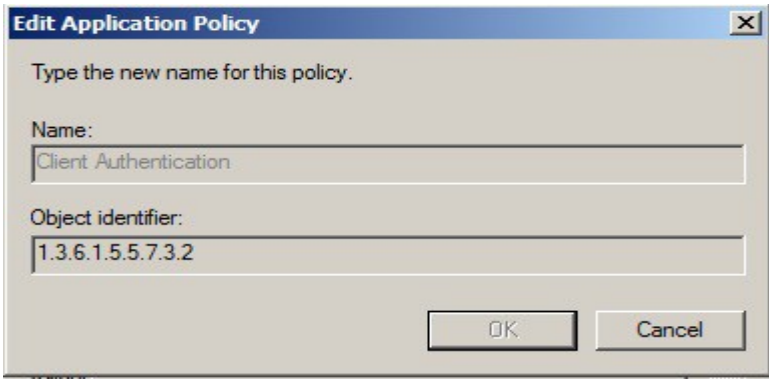


Figure 6.7

Note: You can add an application policy by clicking the 'Add' button.

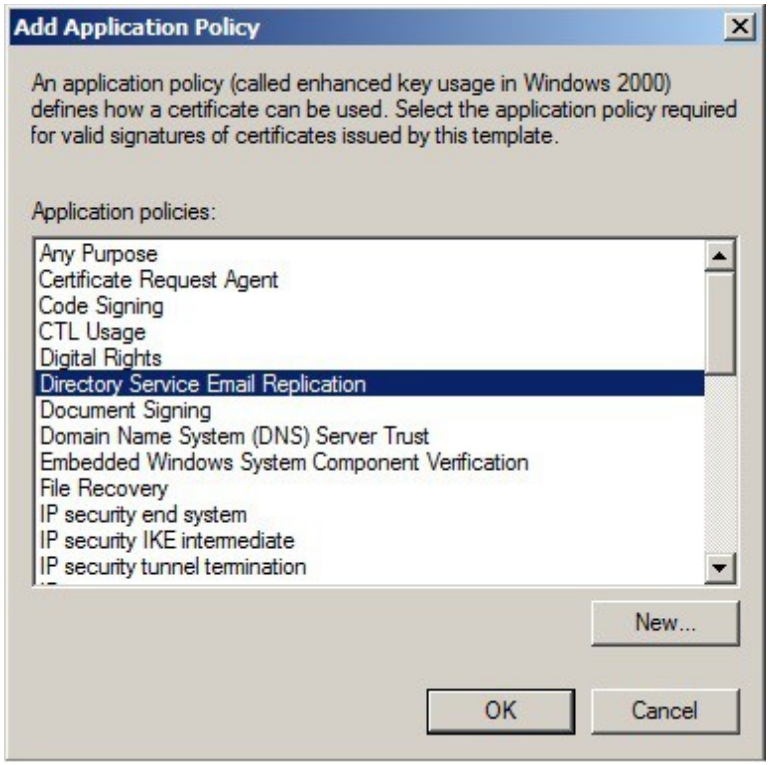


Figure 6.8

If you need a policy which is not in this list, click **New...** then enter the name and OID of the new policy and click **OK**.

You can use only OIDs, that are supported by current version of CCM. Please view OIDs list at CCM side. Section 6 explains how to view this list.

11. Select Key Usage item at 'Extensions' tab (Figure 6.5), then click 'Edit...' button. Select suitable options for Key Usage extension (Figure 6.9) of this template, then click 'OK' button. If you don't need any changes, press the 'Cancel' button.

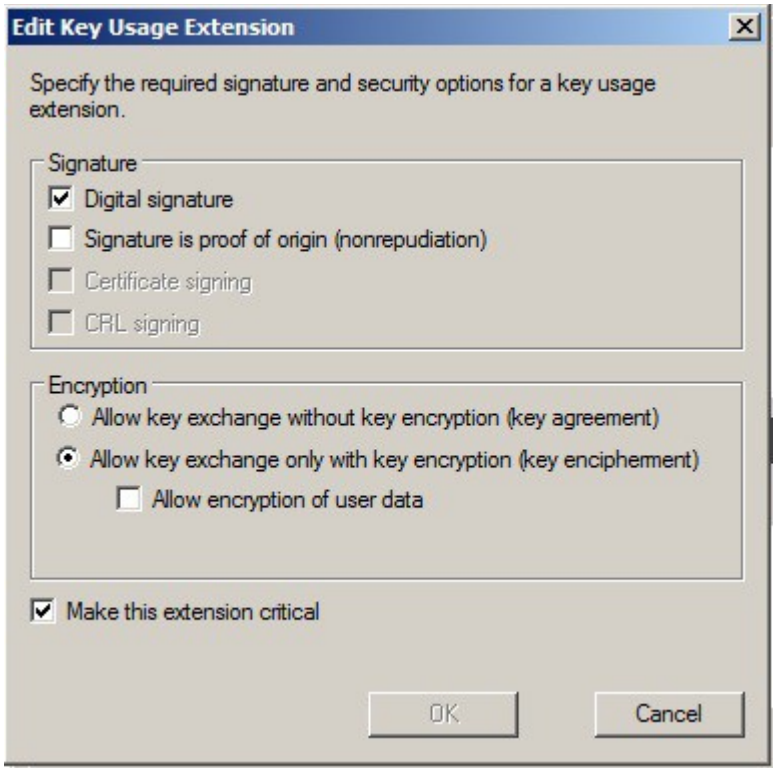


Figure 6.9

12. Select Cryptography tab of current template property editor (Figure 6.10). Enter algorithm name, key size and hash algorithm, then click the 'OK' button.

Note: This tab is available only for version 3 certificate templates. These settings apply to the certificate request only, not the certificate issued from this template.

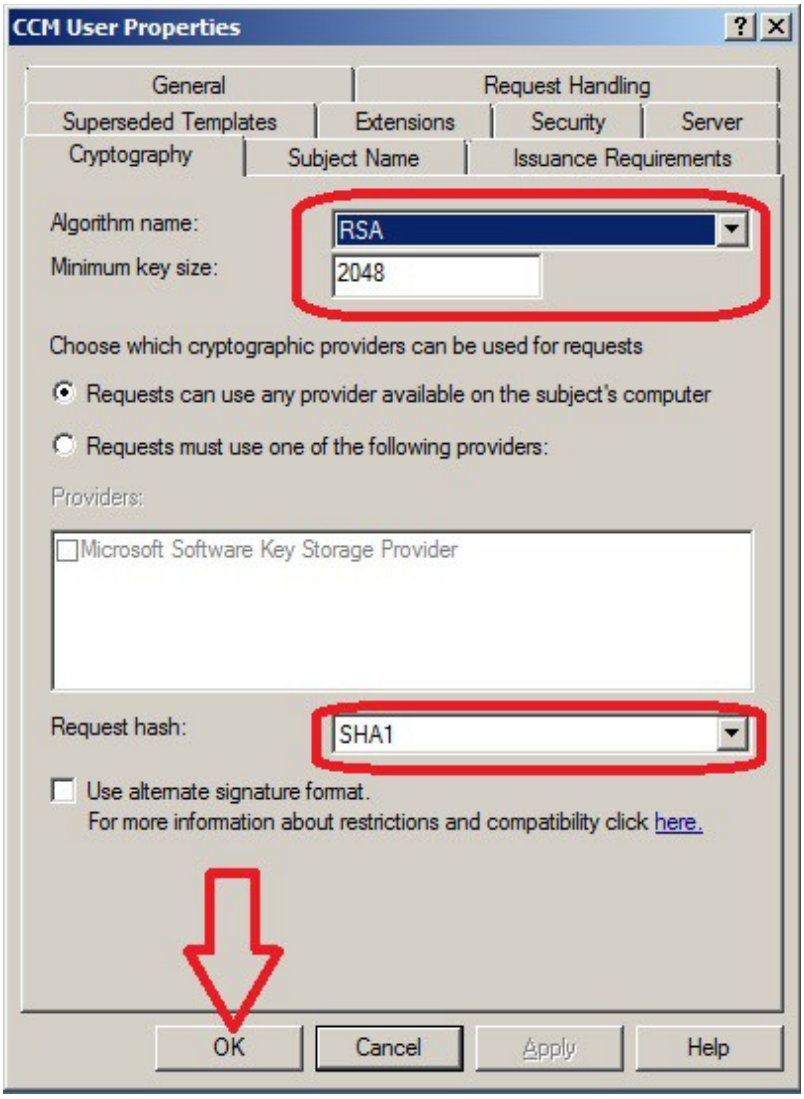


Figure 6.10

13. Complete the different template properties tabs according to the purposes of this template.
14. To associate the new template with Comodo CA Proxy, open Server Manager, select node 'Roles' > 'Active Directory Certificate Services' > 'Comodo CA Proxy' > 'Certificate Templates', then right click on 'Certificate Template' sub-node and select 'New' > 'Certificate Template to Issue', or choose main menu 'Actions' > 'New' > 'Certificate Template to Issue'.

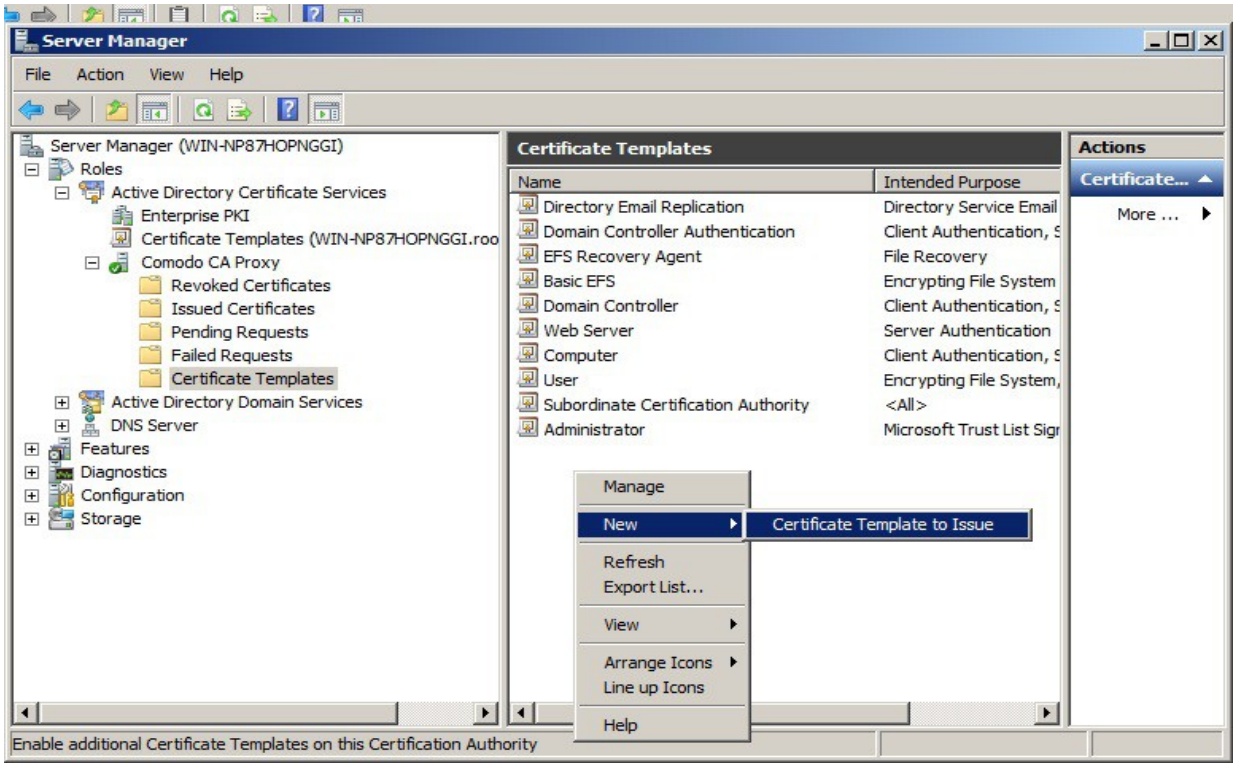


Figure 6.11

15. Select your template and click 'OK' to save changes and close the window

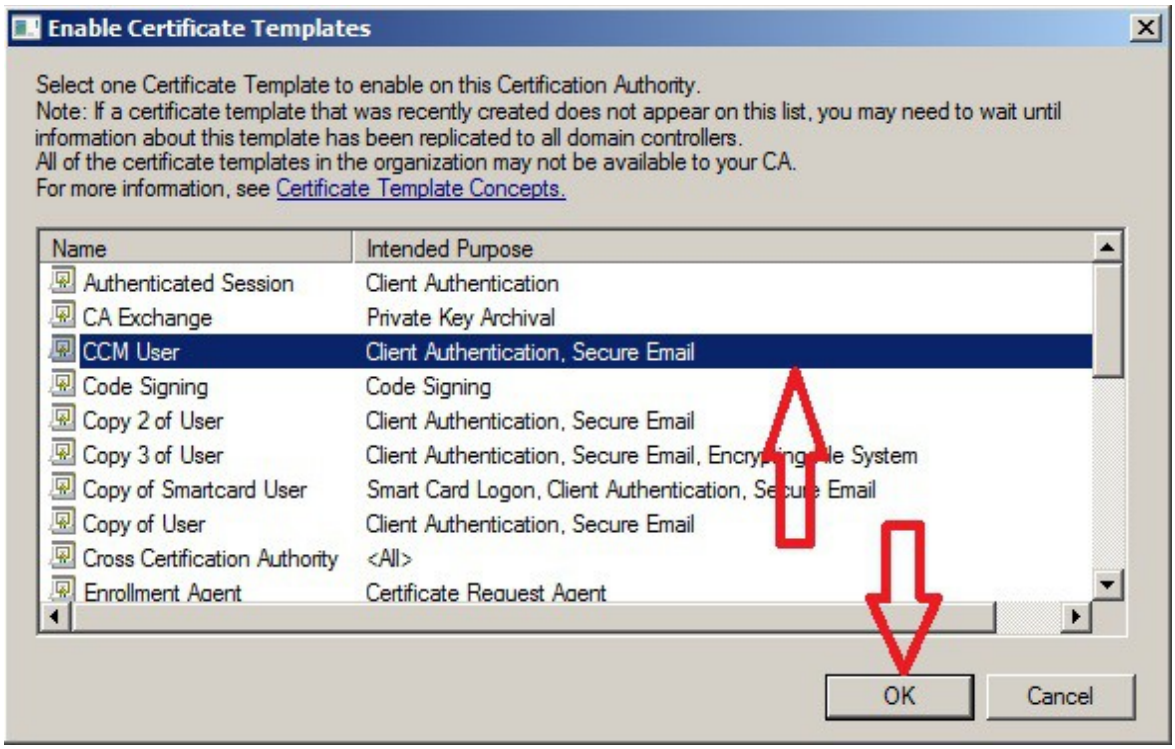


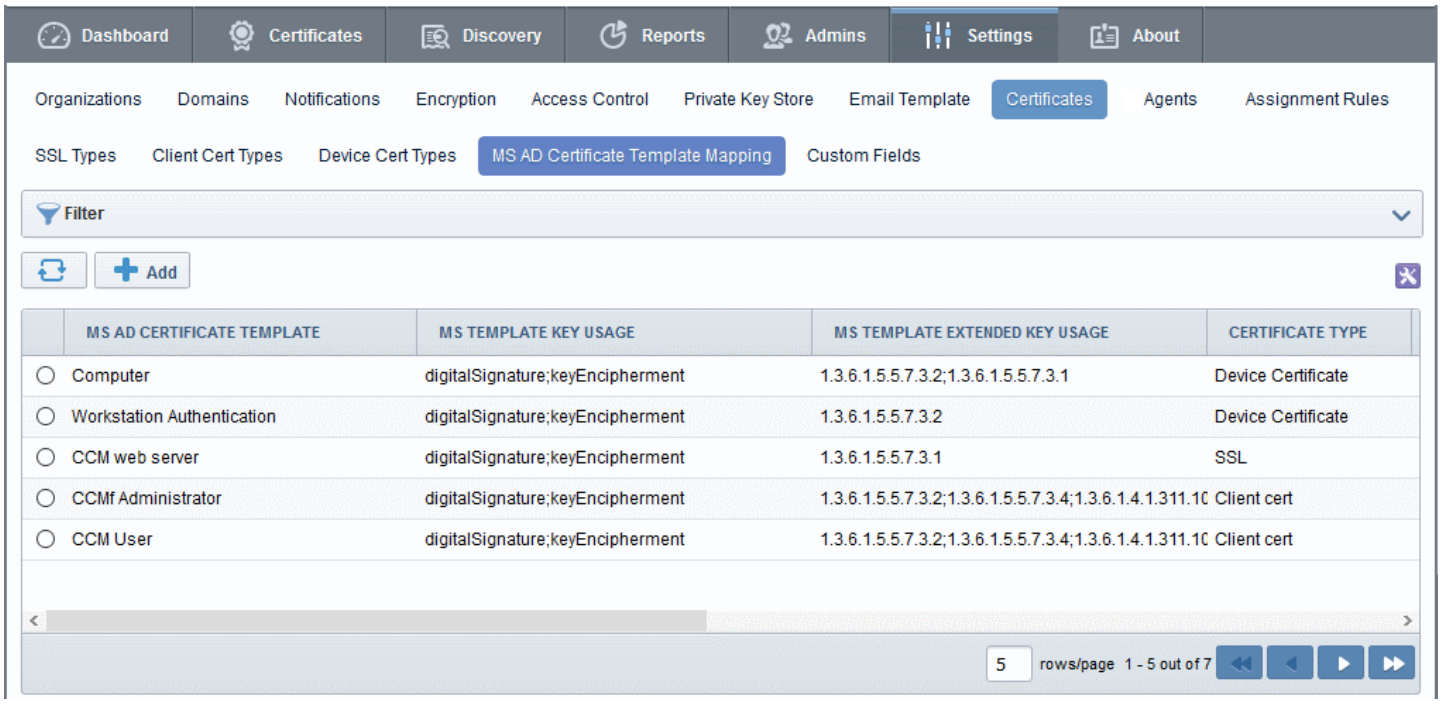
Figure 6.12

7. Map Templates to CCM Certificate Types

CCM allows you to map custom certificate templates created on a AD server to CCM private certificate types. After selecting a custom template and enrolling for a certificate using the Comodo CA Proxy service, CCM will issue a private CA certificate according to the parameters in the template.

The 'MS AD Certificate Template Mapping' interface in CCM allows admins to map templates to private CA certificate types. To get started:

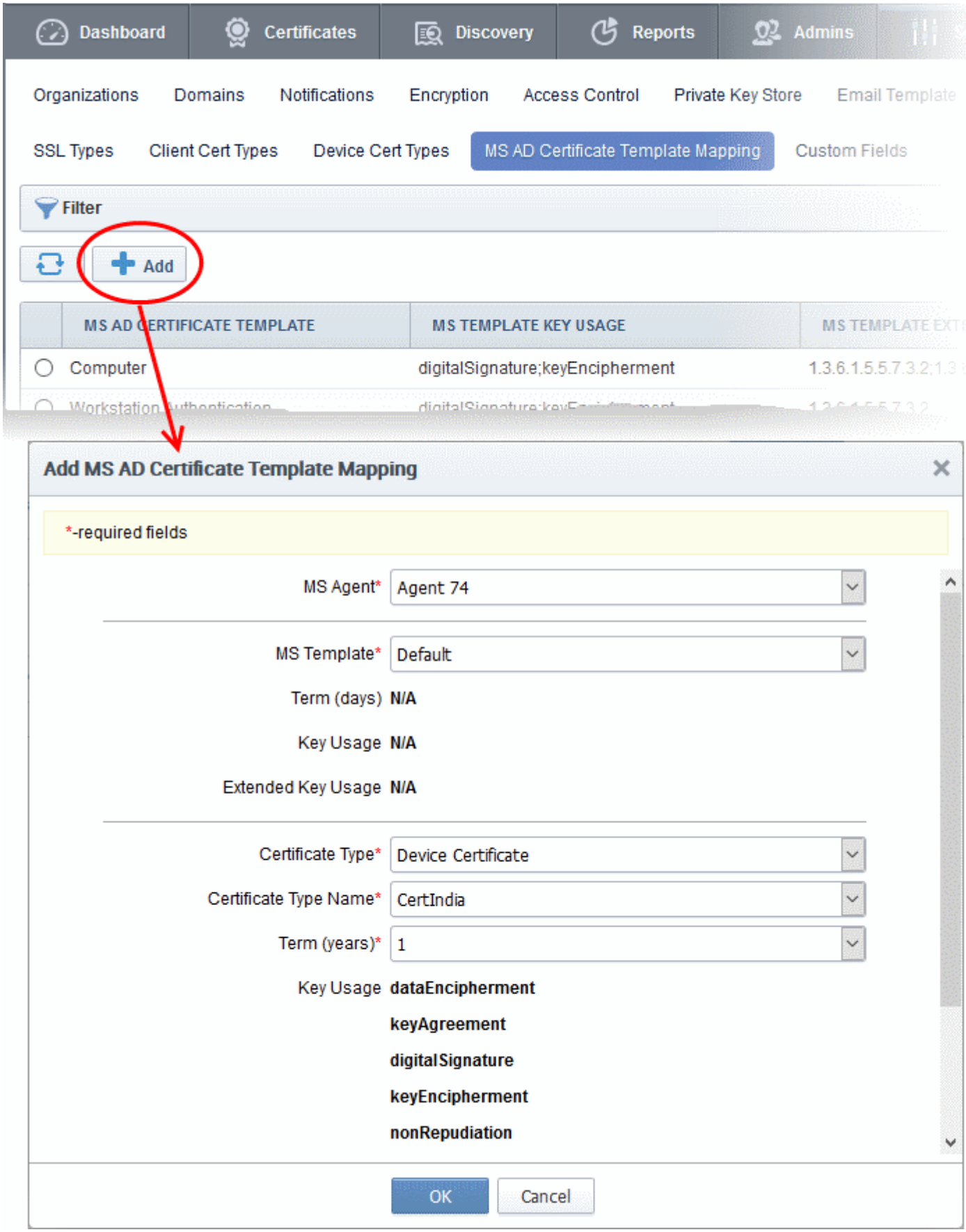
- Login to CCM as an MRAO administrator
- Open the mapping interface by clicking 'Settings' > 'Certificates' > 'MS AD Certificate Template Mapping'



Notes:

- The MS Agent should have been installed on the AD server of the Organization/Department from which the templates are to be mapped. The agent should have been configured to act as CA Proxy. Refer to the section **Comodo CA Proxy Service Installation** for more about installing and configuring the MS agent.
- Private certificates should be enabled for your account in order to map them to MS AD templates. Please contact your account manager to enable private certificates for your account.
- Certificate types with mapped templates can only be enrolled for through an AD server using the certificate enrollment service or a group enrollment policy.
- For SSL Certificates - CCM currently only supports MS AD template mapping for the 'Private UCC SSL' certificate type. Other private CA certificate types will be enabled for template mapping in future versions.
- For Device Certificates - Administrators can request their account manager to add private CA's to their account and create device certificate types as required from 'Settings' > 'Certificates' > 'Device Certificate Types'. These device certificate types can be mapped to MS AD certificate templates.

- To add a certificate template mapping to CCM. click the 'Add' button.



Form Element	Type	Description
MS Agent *(required)*	Drop-down list	The drop-down lists MS agents found on AD servers. Select the agent that you want to map with CCM for the template.
MS Template *(required)*	Drop-down list	The drop-down lists certificate templates found on the AD server. Select the template that you have configured as explained in the section 'Configure Templates at Active Directory'.
Term	Text Field	The validity period of the certificate as defined in the selected template.
Key Usage	Text Field	Details of key usage defined in the selected template
Extended Key Usage	Text Field	Details of extended key usage defined in the selected template
Certificate Type	Drop-down list	Available certificate categories are SSL, Client and Device. The certificate types are as configured on CCM . • SSL - Currently only Private UCC is available. Other private CA certificate types will be enabled for template mapping in future versions. • Client Cert - All client cert types available for your account. • Device Cert - All private device cert types added to your account. You can add private device cert types by associating them to private CA's added to your account and selecting Key Usage (KU) and Extended Key Usage (EKU) parameters. Contact your account manager for adding private CAs for adding Private CA's of your choice to your account.
Certificate Type Name	Drop-down list	Certificate sub-type. The certificates available in this drop-down are determined by the 'Certificate Type' chosen in the field above.
Term	Drop-down list	The terms configured for the selected sub-type in CCM.
Key Usage	Text Field	The key usage of the certificate sub-type as defined in CCM
Extended Key Usage	Text Field	The extended key usage of the certificate as defined in CCM

- Click 'OK' after configuring the certificate type for the selected template.

8. Configure Active Directory Users

First, check that the following attributes are correct for user accounts in Active Directory:

- First Name
- Last Name
- E-mail
- Company
- Department (optional)

To check this:

1. Make sure, that you are logged on to the appropriate server as a domain administrator.
2. If the window with Server Manager is not opened, click **'Start'**, point to **'Administrative Tools'**, and then click

'Server Manager', or click corresponding button on task bar. Select node **'Roles' > 'Active Directory Domain Services' > 'Active Directory Users and Computers',** then expand the node with your domain name. Find your user and double click it. Check this user according to following figures in this section.

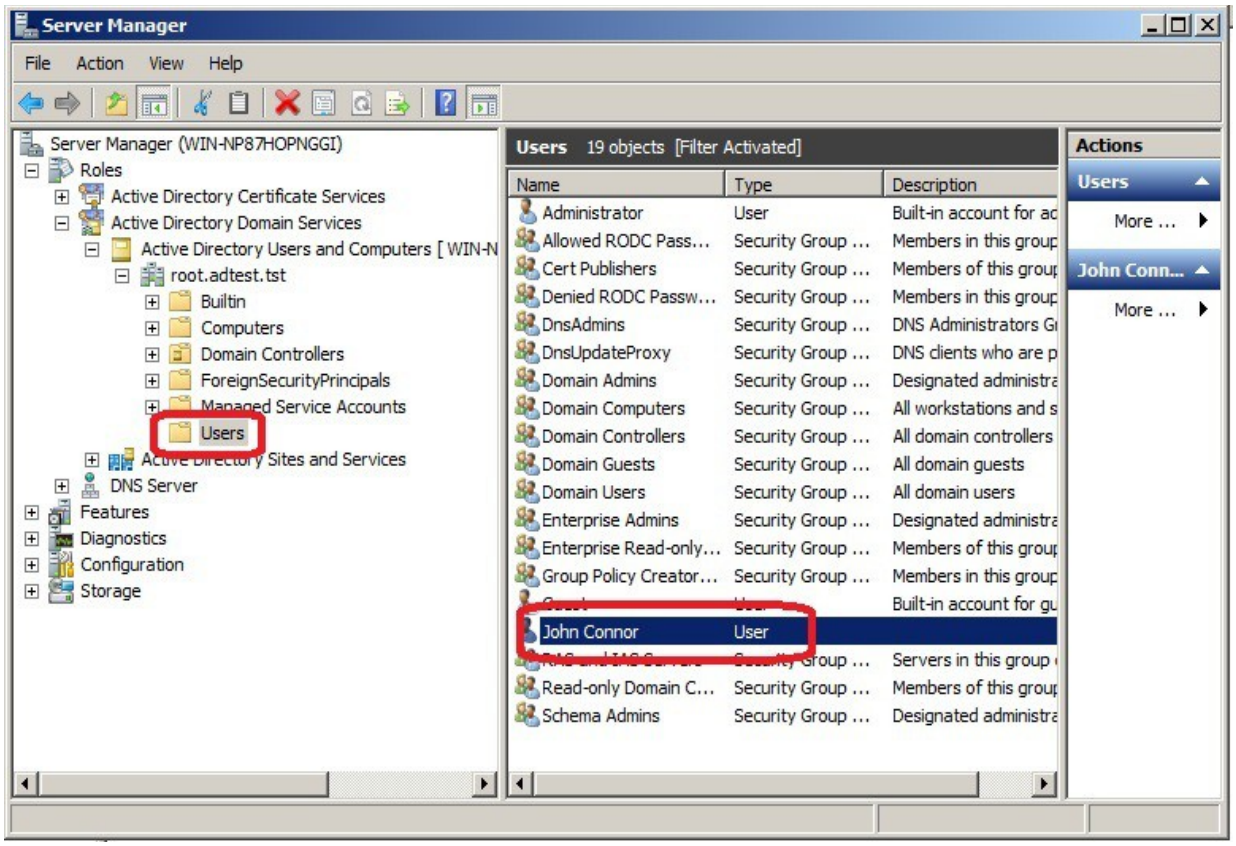


Figure 8.1

3. Double click on selected user.

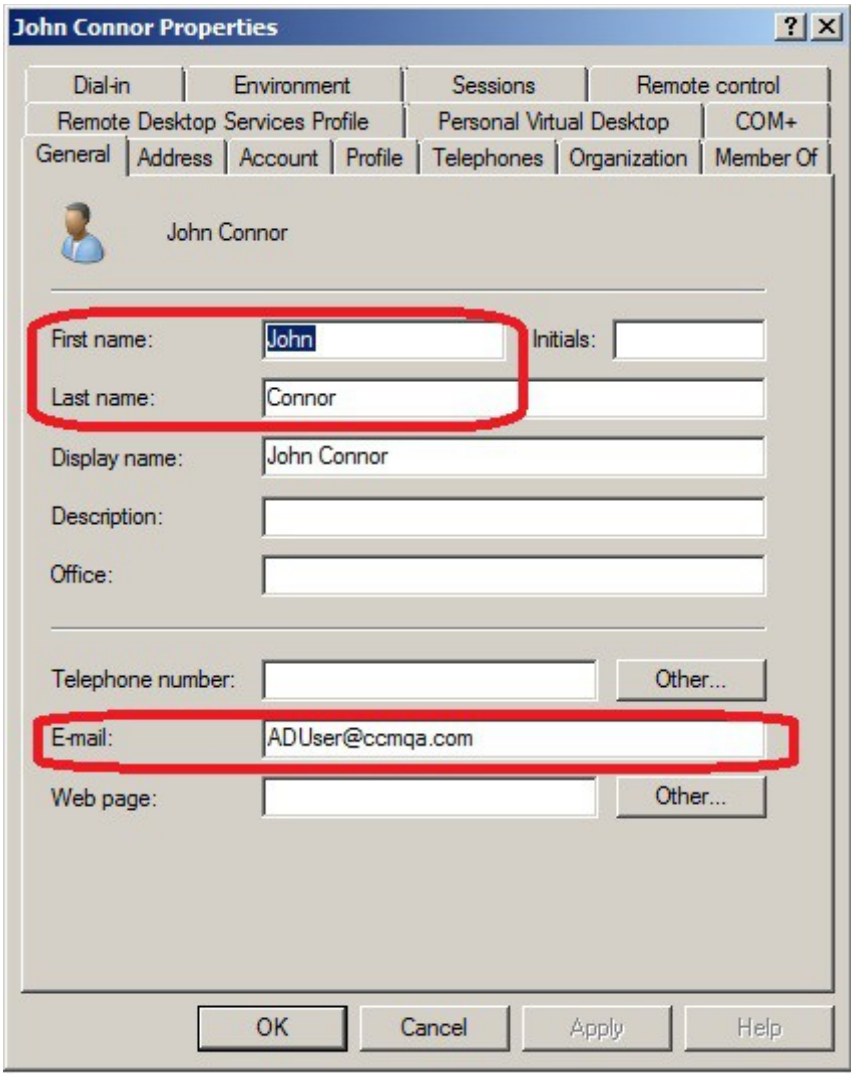


Figure 8.2

4. Check First name, Last Name, E-mail

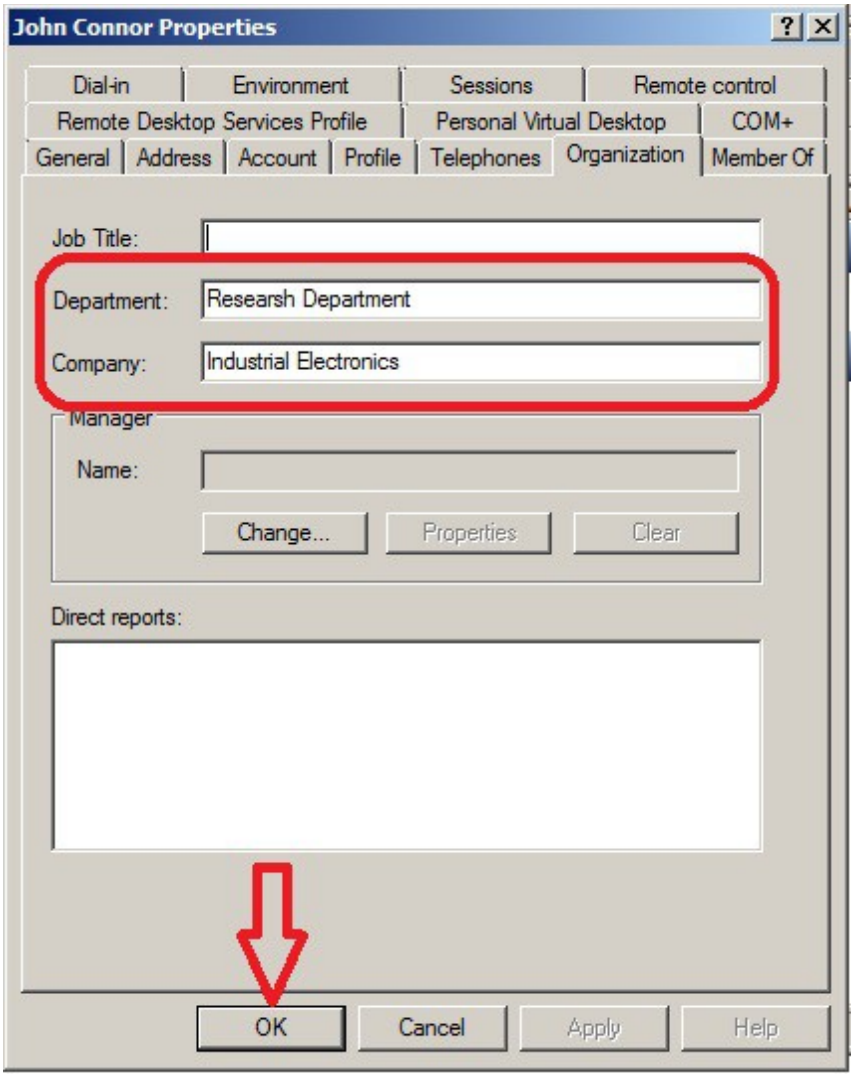


Figure 8.3

5. Check Department and Company
6. Click 'OK' button to apply changes and close this window

9. Enrollment and Auto-Enrollment

1. Log on to the user's workstation as domain-joined user. Auto-enrollment must be initiated by the system automatically. For details, see Microsoft's technical documentation related to certificate auto-enrollment.
2. Run certmgr.msc. Select node 'Certificates - Current User=>Personal'. If the 'Certificates' sub-node is present, select it and try to view the list of certificates. Otherwise, the auto-enrollment is in progress, or is not started.
3. To start manual enrollment, select the menu option 'Task' > 'Request New Certificate...'

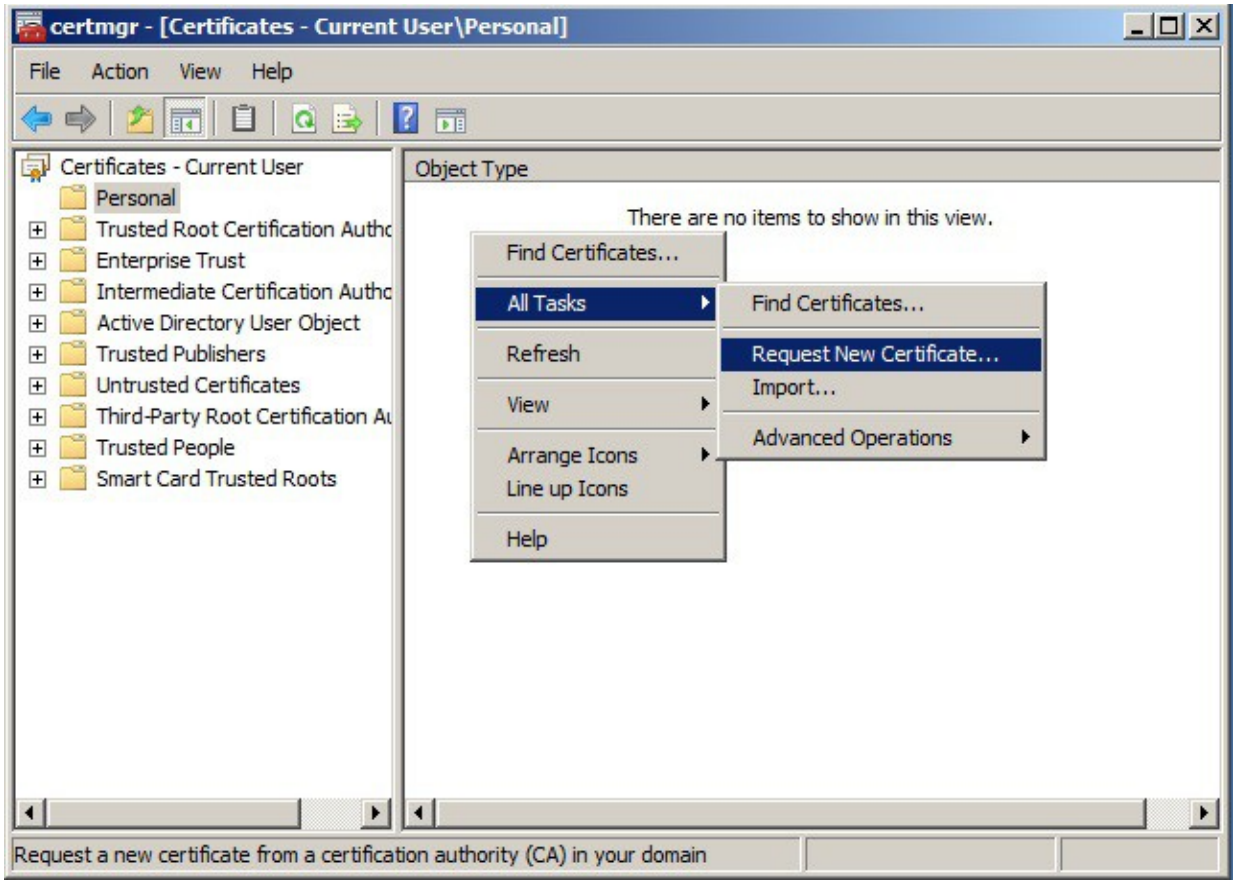


Figure 9.1

4. Read the 'Before you begin...' information and click the 'Next' button:

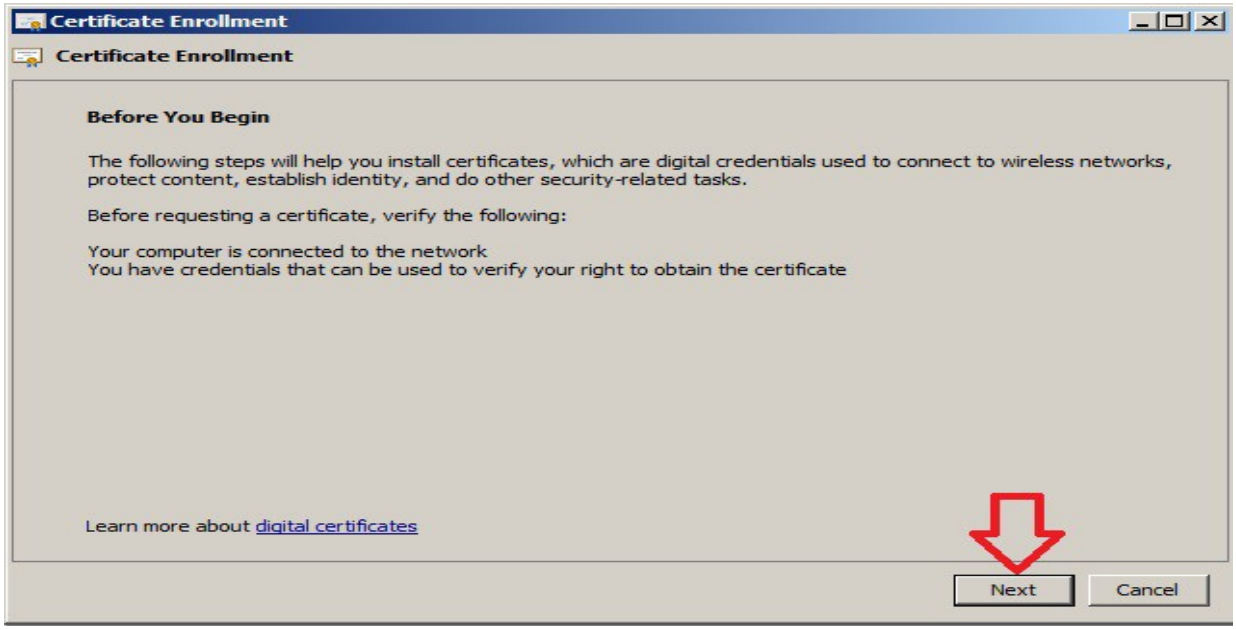


Figure 9.2

5. Select 'Active' Directory Enrollment Policy' and click the 'Next' button

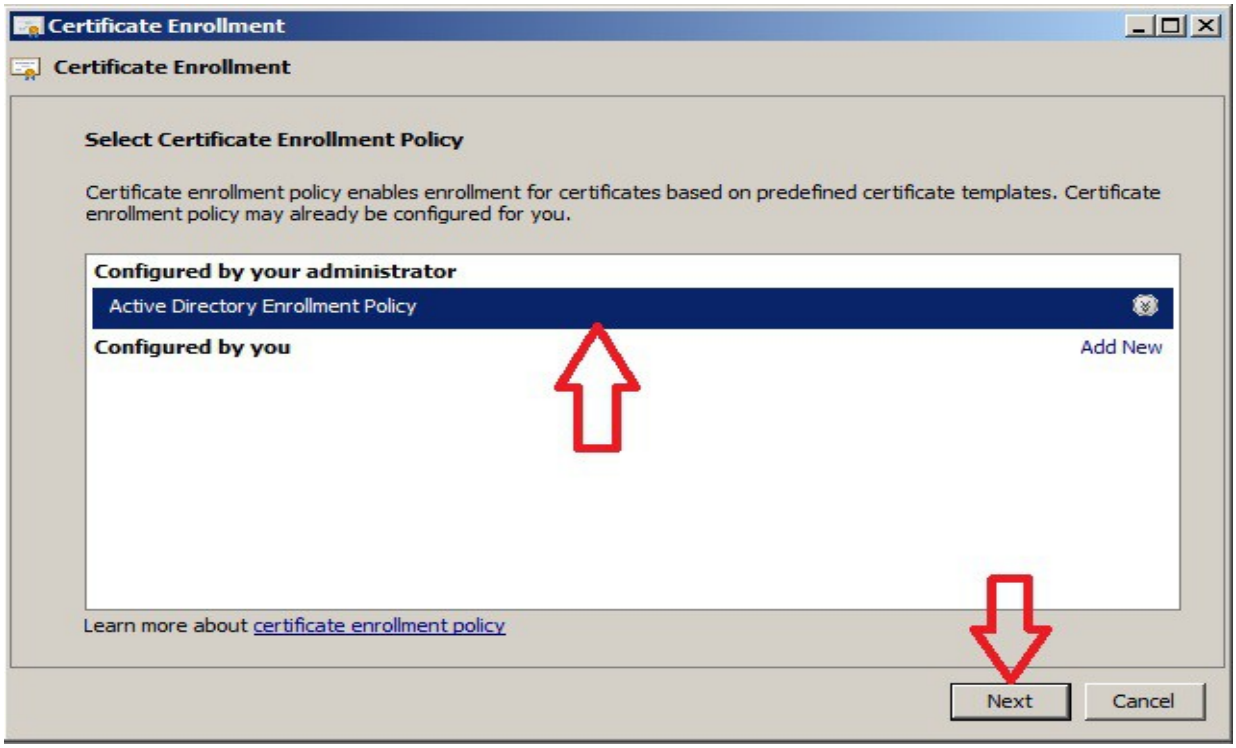


Figure 9.3

6. Select the certificate template you wish to use and click the 'Enroll' button

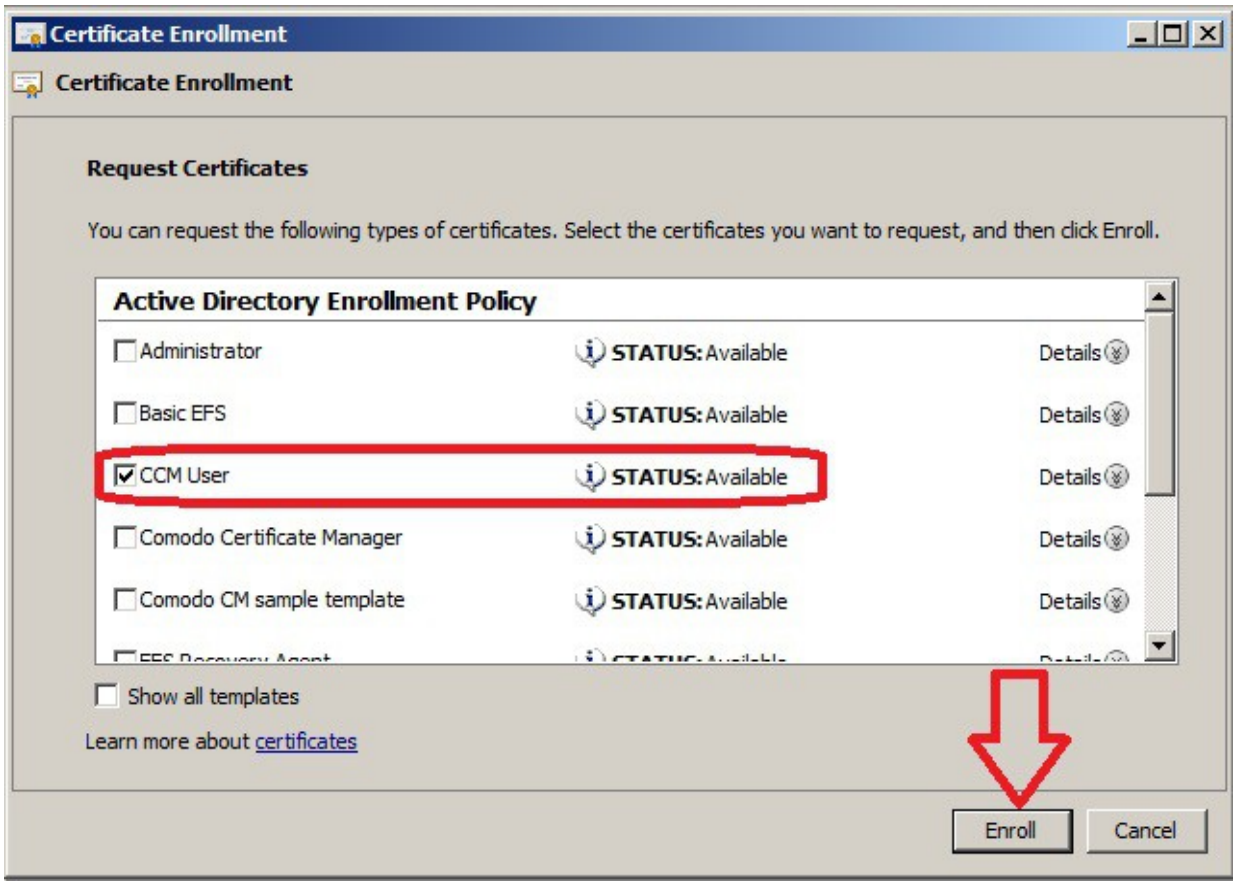


Figure 9.4

7. Make sure the enrollment operation finishes successfully then click the 'Finish' button:

Note: You can view detailed information about enrolled certificates by clicking the 'View Certificate' button See Figure 9.5.

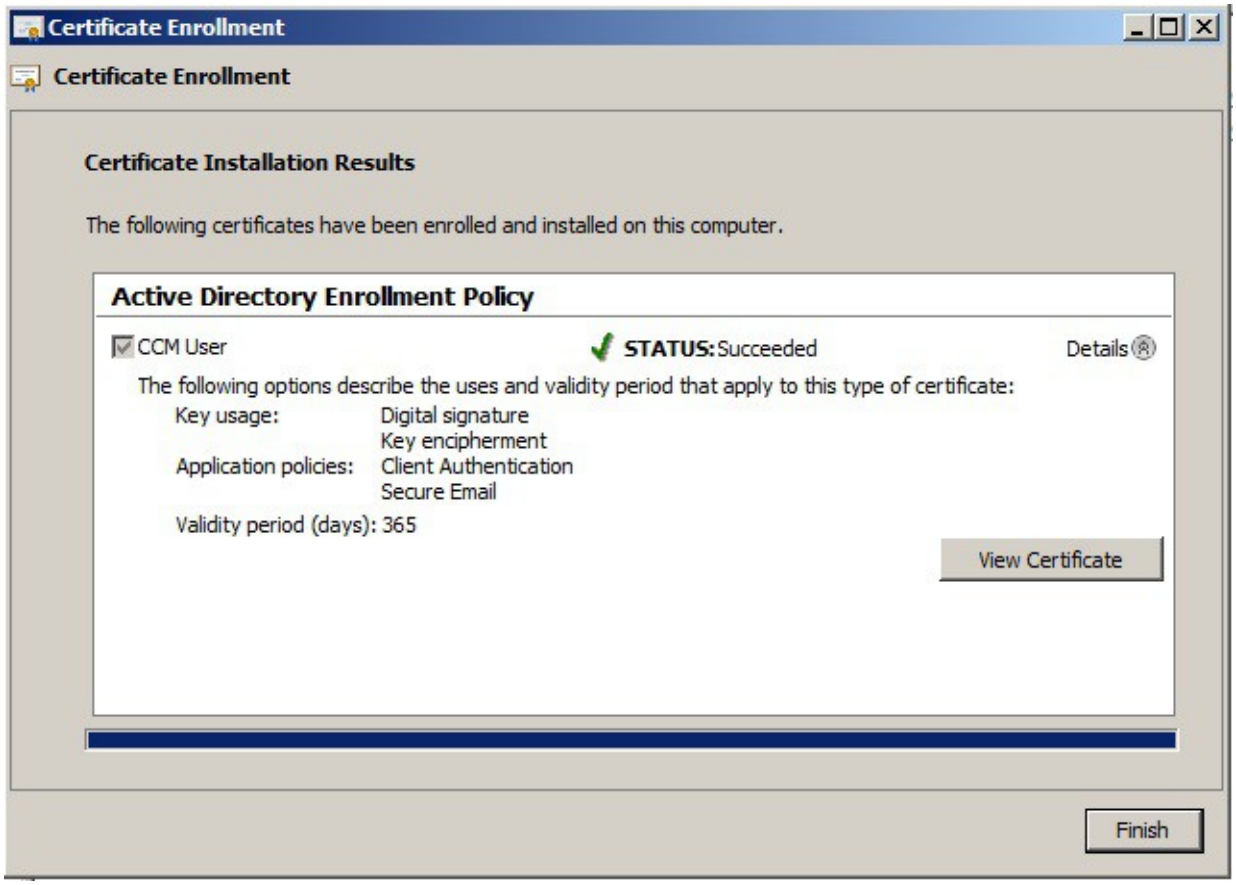


Figure 9.5

8. The 'Details' tab contains all certificate properties:

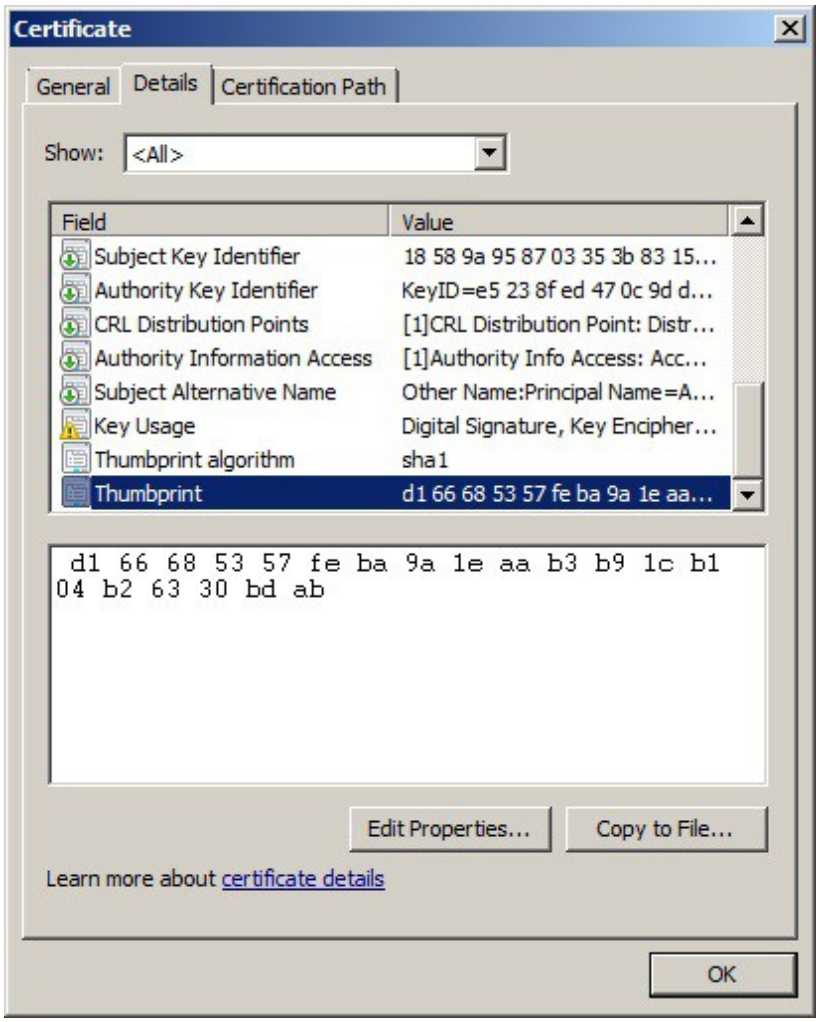


Figure 9.6

9. On the Comodo CA Server console you also can see this certificate under the **Issued certificates** node. To view it's details, double click it in the list. The result is same as from client certificates console and is displayed at Figure 9.6

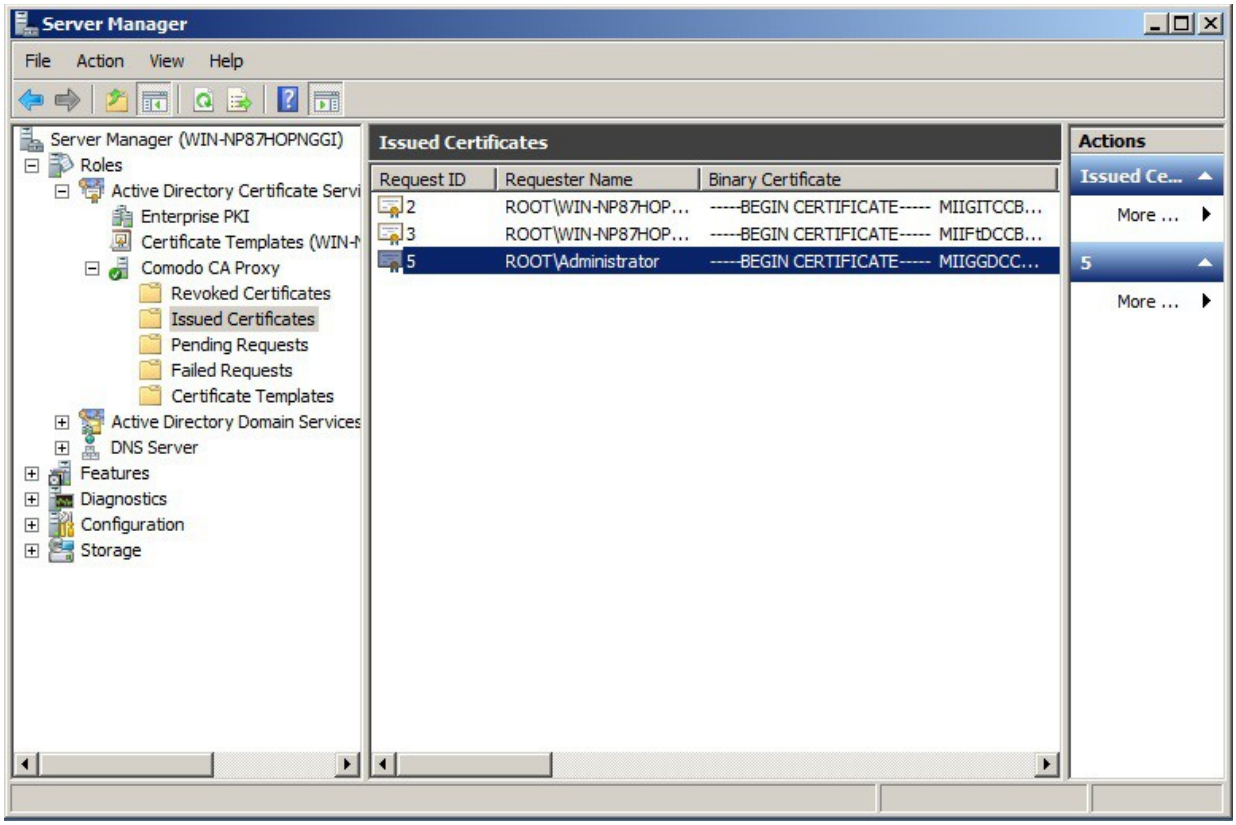


Figure 9.7

10. Configure MS Agents for Certificate Discovery and Issuance

Comodo Certificate Manager uses an agent for certificate discovery and for provisioning device certificates through the AD server:

- **Certificate Discovery** - Once configured, the agent periodically scans the server, fetches the network/object structure and passes information about detected certificates to CCM. The results can be viewed from the 'Discovery' > 'Network Assets' interface of CCM.
- **Provisioning of Device Authentication Certificates** - MS agents installed on AD servers also act as a CA proxy. The agent will receive certificate requests from the NDES server and forward them to CCM. The agent will track all orders and, after the device certificate has been issued, will fetch the certificates and forward them to the NDES server. The NDES server, in turn, will forward the certificates to the devices.

Note: To provision device authentication certificates, the AD server must have:

- A Network Device Enrollment Service (NDES) server integrated
- A Group Policy which will enroll device certificates for devices

For guidance on this, please refer to the online guide at:
http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx

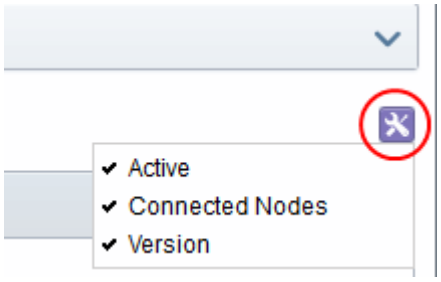
- **Mapping MS AD Certificate Templates to CCM Certificate Types** -
  - MS agents on AD servers allow templates on the server to be mapped with CCM certificate types, enabling CCM to act as a Private CA for an Organization/Department.
  - Domain admins can create custom certificate templates on their server as required and request

CCM admins to map these templates to private certificate types.

- Domain administrators can enroll for certificates from the AD server by selecting the correct template. See Map Templates to CCM Certificate Types for more details.

- CCM also allows you to create clusters of MS Agents installed on different AD servers to act as a single agent. If any agent fails, the other agents in the cluster will seamlessly continue the functions of certificate discovery and provisioning. This ensures that users do not suffer delays or data loss when requesting certificates.
- The 'MS Agents' interface shows a list of agents installed on different AD servers and allows admins to configure them for certificate discovery and issuance.
- Login to CCM as an MRAO administrator
- Click 'Settings' > 'Agents' > 'MS Agents':

Column Header	Description
Name	Name of the MS Agent.
Active	Indicates whether or not the agent is active. Administrators can change the state if required.
Connected Nodes	The number of nodes currently connected to CCM out of all nodes.
Status	The current connection status of stand-alone and clustered agents. The possible states are: CONNECTED - Stand-alone agent - The agent is connected to CCM Clustered Agent - All node agents in the cluster are connected to CCM. DISCONNECTED - Stand-alone agent - The agent is not connected to CCM Clustered Agent - None of the nodes agents in the cluster are connected to CCM. WARNING - Clustered Agent - One or more of the node agents in the cluster is not connected to CCM N/A - Stand-alone agent - The agent has never established connection to CCM. Clustered Agent - No node agents are added to the clustered

		agent.
Version		Displays the version number of the MS Agent.
CA Proxy Enabled		Indicates whether the MS agent is enabled as a CA proxy to receive device certificate requests from the NDES server.
Note: Administrators can enable or disable the columns as desired using the drop-down on the right. 		
Controls	Download Agent	Download and create a new MS Agent for installation on to an AD server that you wish to integrate.
	Create Cluster	Create an agent cluster by grouping a set of stand-alone agents. See Configuring Clustered MS Agent for more details.
	Refresh	Updates the list of agents.
Agent Controls	Edit	Stand-alone Agent - Enables administrators to modify the agent configuration settings Clustered Agent - Enables administrators to edit general settings, add or remove node agents and edit scan configuration settings.
	Delete	Removes the agent.
	Commands	View commands executed by the agent. Commands are available for configuration updates, scanning the AD server and more.
	Restore	Allows admins to download the agent setup file for pre-configured agents. This is useful if you if you have already configured, downloaded and installed the agent on a server but want to re-install the agent for some reason. The new agent setup file will be configured with the same parameters (agent name, secret key, CA proxy, update settings, scan schedule etc). Applicable only for the agents that are active.

The following sections explain more about:

- Configure stand-alone MS Agents
- Configure MS Agent Clusters
- Configure Active Directory Discovery Tasks

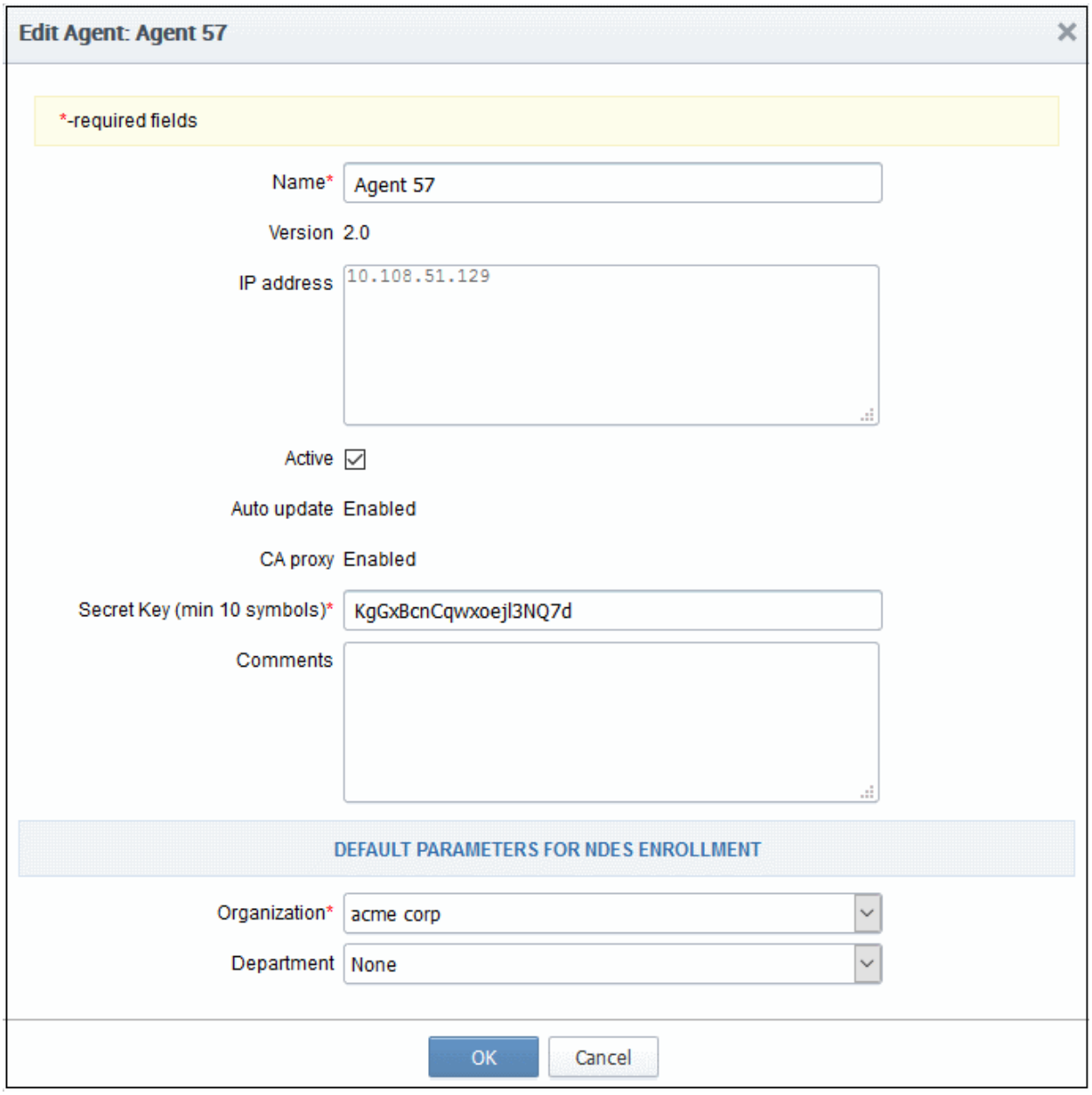
10.1. Configure Stand-Alone MS Agents

You can configure a schedule for MS Agents to specify when they should scan your servers and forward the results to CCM.

To configure an agent

- Login to CCM as an MRAO administrator

- Open the 'MS Agents' interface by clicking 'Settings' > 'Agents' > 'MS Agents'.
- Select the agent and click the 'Edit' button



Edit Agent - Table of Parameters		
Field Name	**Type**	**Description**
Name	*String*	The name of the agent. Administrators can edit the name of the MS agent.
Version		The version number of the agent.
IP Address	*Text box*	Shows the IPV4/IPV6 address, or loop-back address, or the physical address of the server on which the agent is installed.
Active	*Checkbox*	Enables admins to enable or disable the agent

Edit Agent - Table of Parameters		
Auto update	*String*	Shows whether or not the agent is configured for auto update
CA proxy	*String*	Whether or not the agent is enabled as a CA Proxy to forward device certificate requests from the NDES server to CCM.
Secret Key	*String*	Displays the secret key generated by the agent to authenticate itself to the Comodo CM server. Administrators can copy and save the secret key in a safe location for use in a new agent. This can be useful if the agent has to be reinstalled to the same server for scanning the same internal network.
Comments	*String*	Enables admins to leave internal notes about the agent
Default Parameters for NDES Enrollment		
Organization	*Drop-down list*	Select the organization you want to associate with the agent for issuance of certificates through NDES.
Department	*Drop-down list*	Select the department you want to associate with the agent for issuance of certificates through NDES.

- Edit the values if required. To set a scan schedule for the agent, click the 'Scan Configuration' tab.
- Click 'OK' in the 'Edit Agent' dialog for your configuration to take effect.
- Once MS Agent is installed on a AD server, you can configure AD discovery scan tasks. See section Configure Active Directory Discovery Tasks for more details about scan configurations.

10.2. Configuring Clustered MS Agent

CCM allows you to create agent clusters by grouping stand-alone MS Agents which are installed on different servers. Once clustered, the stand-alone agents will act as a single agent. This provides redundancy, so if an agent goes down, its certificate discovery and issuance functions will be taken over by another agent in the cluster. This prevents delays and data loss during issuance and discovery operations.

Any number of agents can be included in a cluster.

Prerequisites:

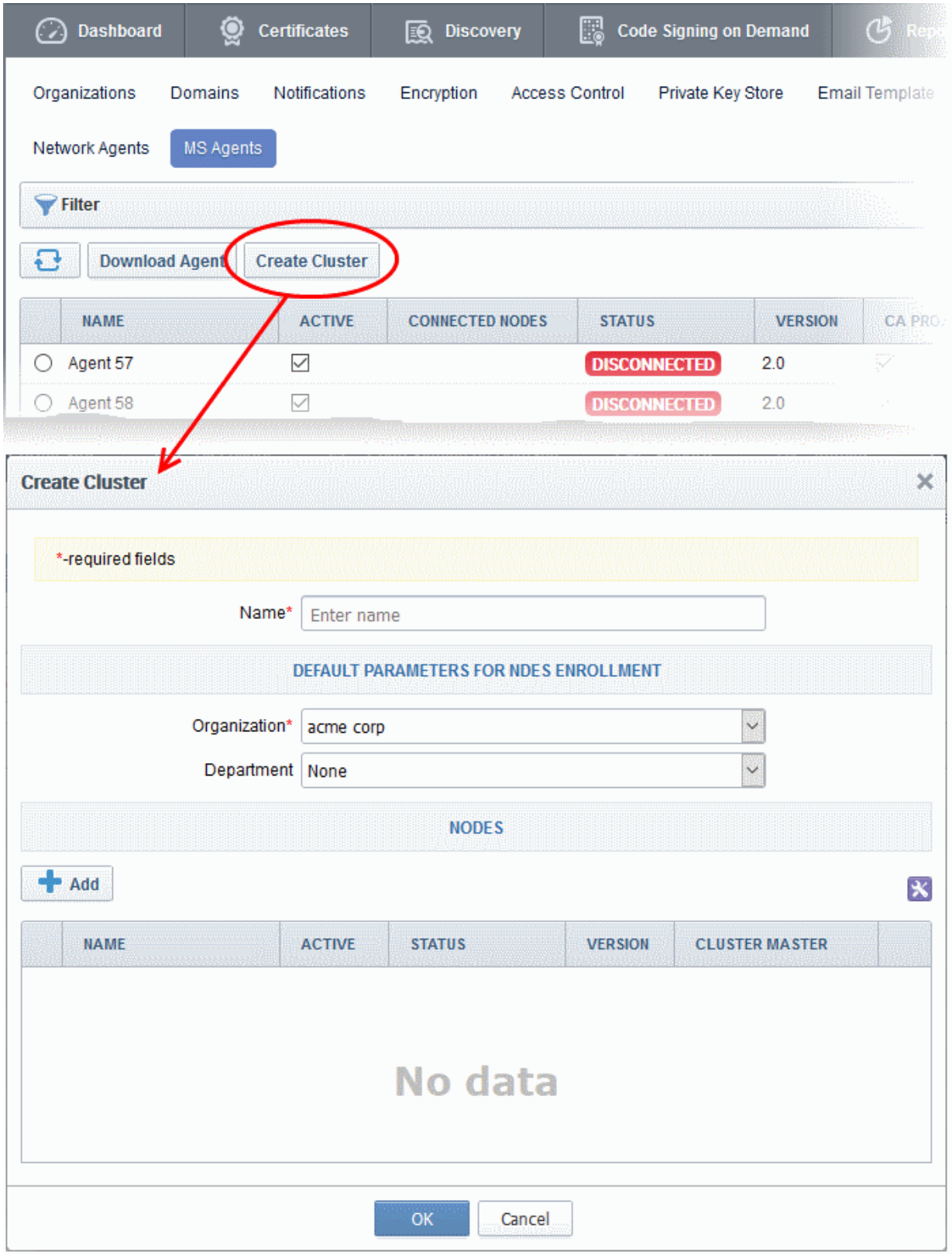
The MS agents to be included in the cluster are installed on AD servers, connected to CCM and configured with the following parameters enabled:

- CA Proxy
- Active
- Auto Update

See the section Comodo CA Proxy Service Installation for guidance on downloading and installing stand-alone MS Agents.

To create a clustered agent

- Login to CCM as an MRAO administrator
- Open the 'MS Agents' interface by clicking 'Settings' > Agents' > 'MS Agents'
- Click the 'Create Cluster' button



Create Cluster - General Tab - Table of Parameters		
Field Name	**Type**	**Description**
Name	*String*	Enter a name for the clustered agent.

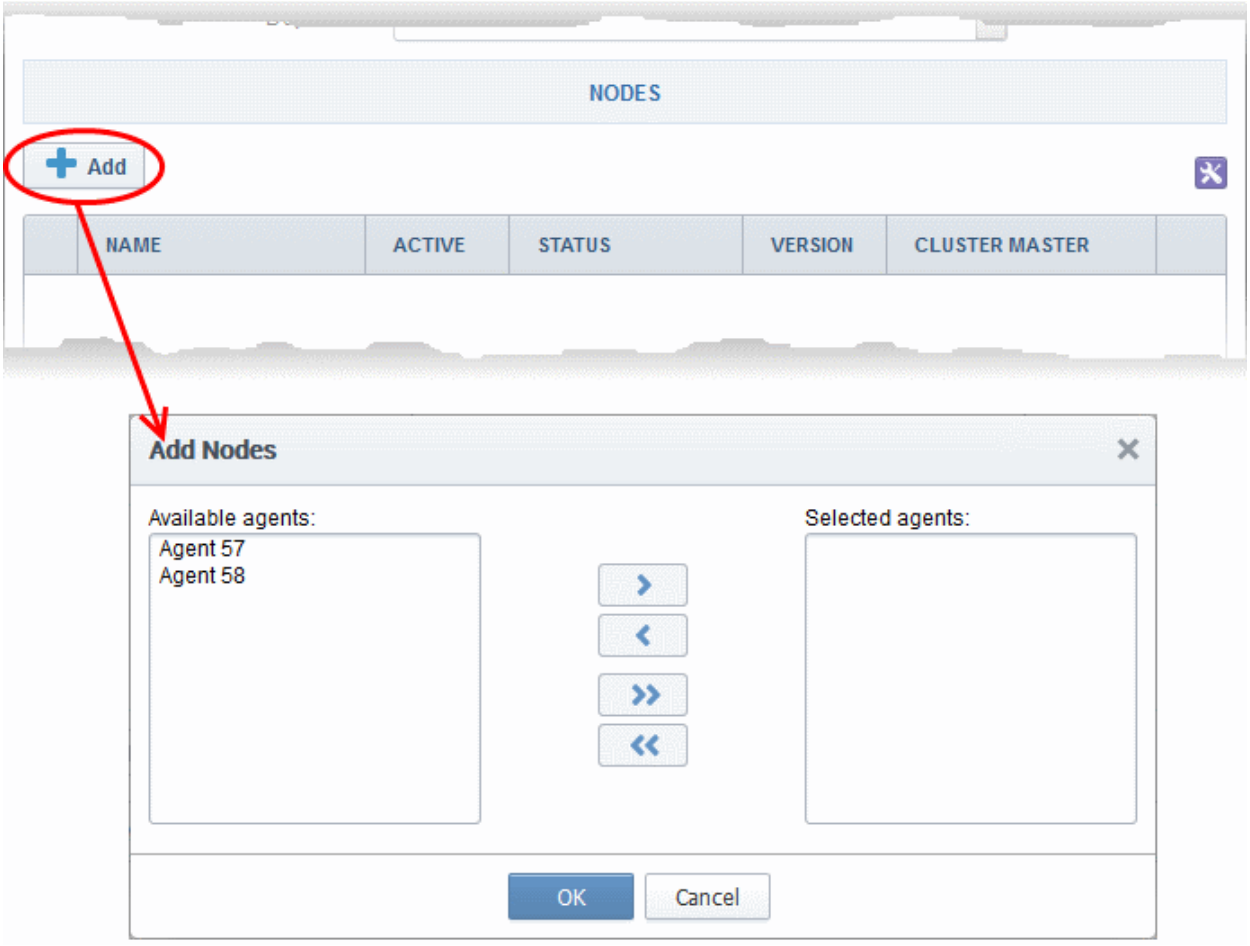
Create Cluster - General Tab - Table of Parameters		
Default Parameters for NDES Enrollment		
Organization	*Drop-down list*	Select the organization you want to assign to the cluster for issuing certificates through NDES.
Department	*Drop-down list*	Select the department you want to assign to the cluster for issuing certificates through NDES.
Nodes		
Add	*Control button*	Allows you to add stand-alone agents to the cluster. See the explanation of Adding Node Agents to the Cluster for more details.

Adding Node Agents to the Cluster

You can add pre-configured stand-alone MS Agents to a cluster. Please ensure the agents are the latest version, are active, and are connected to CCM.

To add agents to a cluster

- Click 'Add' in the 'Create Cluster' > 'General' tab dialog
- The 'Add Nodes' dialog will open

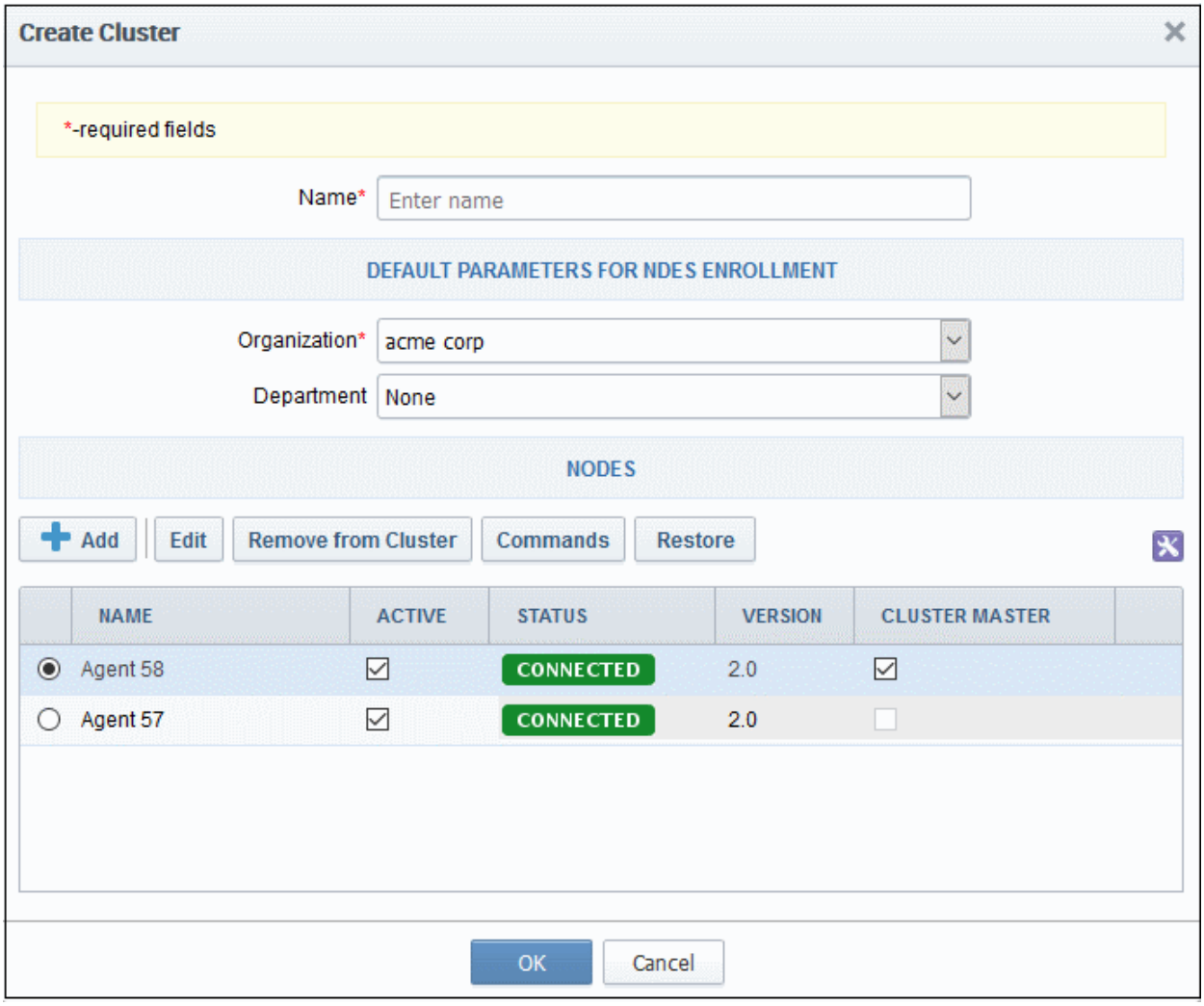


A list of available stand-alone agents will be shown in the left pane.

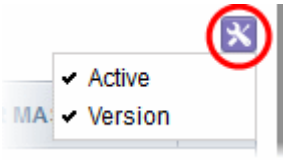
- Use the arrow buttons to add the stand-alone agents to the cluster

- Select the agents to be added and move them to right pane by clicking right arrow button or simply drag and drop the agent(s) to the right pane
- To add all agents at once click the button
- To remove agent(s) added by mistake, select the agent from the right pane and click the left arrow or simply drag and drop the agent to the left pane
- To remove all agents at once click the button.

The agents will be added to the cluster and shown as a list.



Nodes in a Clustered Agent - Table of column Descriptions	
Column Header	**Description**
Name	Name of the MS Agent.
Active	Indicates whether or not the agent is active. Administrators can change the state if required.
Status	The current connection status of the agent. The possible states are: CONNECTED - The agent is connected to CCM DISCONNECTED - The agent is not connected to CCM

	N/A - The agent has never established connection to CCM.	
Version	Displays the version number of the MS Agent.	
Cluster master	Indicates whether the node is set as the master agent in the cluster. Note: CCM automatically assigns one of the agents in the cluster as master agent in order to receive the commands for discovery scans and certificate issuance. The cluster master is selected depending on the order of connection and the current connection status. If connection to the cluster master is lost, the next agent is set as the cluster master.	
Note: Administrators can enable or disable the columns as desired, from the drop-down button at the right end. 		
Controls	Add	Allows you add nodes to the cluster
Agent Controls	Edit	Allows you to view the general settings and scan configuration of the agent and edit the name of the agent.
	Remove from Cluster	Releases the agent from the cluster. The released agent is added to CCM as a stand-alone agent.
	Commands	Enables administrators to view commands executed by the agent. Commands include configuration updates and scanning the AD server.
	Restore	Allows admins to download the agent setup file for pre-configured agents. This is useful if you if you have already configured, downloaded and installed the agent on a server but want to re-install the agent for some reason. The new agent setup file will be configured with the same parameters (agent name, secret key, CA proxy, update settings, scan schedule etc). Applicable only for agents that are active.

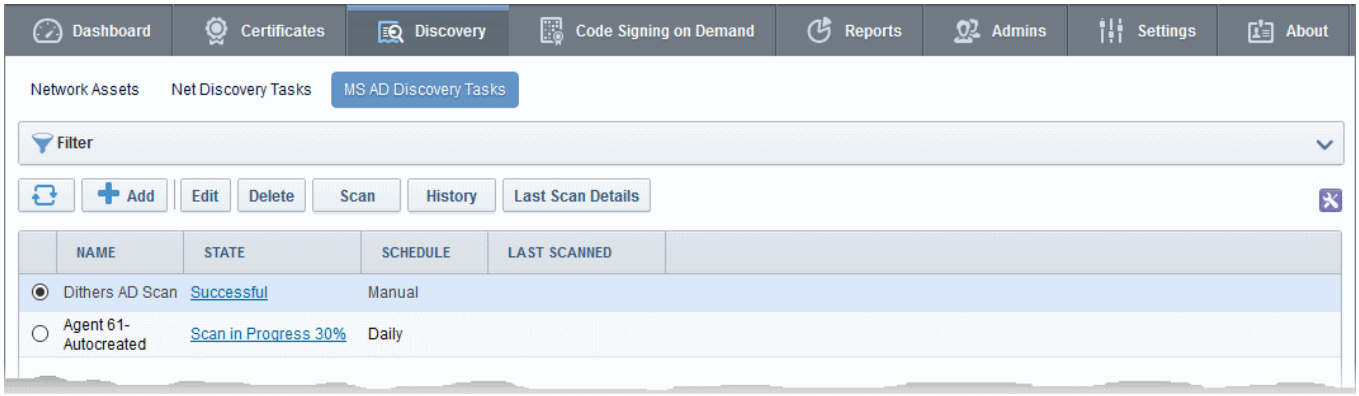
- Click 'OK' in the 'Create Cluster' dialog for your configuration to take effect.

Once the general settings are configured and the agents are added, the next step is to configure the scan settings. See section Configure Active Directory Discovery Tasks for more details about scan configurations.

10.3. Configure Active Directory Discovery Tasks

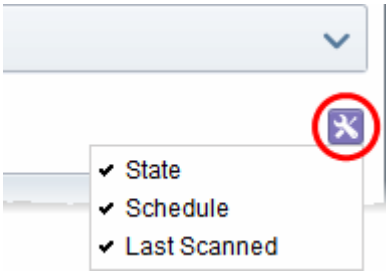
- The 'Active Directory Discovery Tasks' interface lets you configure scans on AD servers which have been integrated with CCM. Scan results can be viewed in the 'Network Assets' tab.
- Active Directory (AD) scans will locate all certificates installed on servers, devices and endpoints on active directory domains.
- Each scan will identify the network/object structure and locate all types of certificates - including SSL, client certs, code signing certs and device authentication certs.
- You can add auto-assignment rules to scans so unmanaged certificates will be assigned to a specific organization or department.
- You need to install the MS AD agent on your active directory server and integrate it with CCM in order to run the scans. See Comodo CA Proxy Service Installation if you haven't yet done this.

Click the 'Discovery' tab then choose 'MS AD Discovery Tasks' to open the interface:



Click the following links to learn more about Active Directory scans:

- Prerequisites
- Overview of process
- Add domains and start scanning
- Edit an AD discovery task
- Delete an AD discovery task
- View a history of AD scan tasks
- View AD scan results

MS AD Discovery Tasks area - Table of Parameters		
Column Header	**Values**	**Description**
Name	String	Name of the certificate discovery task
State	String	Displays the status of the scan, that is, whether it is successful, failed, in progress or canceled. Clicking on the state displays respective result. For example, clicking on 'Successful' will display the number of certificates discovered.
Schedule	String	Displays whether the scan is to be run manually or scheduled
Last Scanned	String	Displays the date and time of the last scan performed
Note: Administrators can enable or disable columns by clicking the button on the right: 		
Control Buttons		
	Add	Enables administrator to add a new AD discovery task
	Refresh	Updates the list of displayed tasks

Discovery Task control Buttons Note: The Discovery Task control buttons are visible only on selecting a domain	Edit	Enables administrator to edit the selected discovery task such as change the scan name, domains to be scanned, assignment rules and schedule
	Delete	Enables administrator to delete a AD discovery task from the list
	Scan	Enables administrator to start a new scan for the selected discovery task
	Cancel	Enables administrator to stop a running discovery scan. This button will appear after starting a new scan for a discovery task.
	History	Displays the details of past scans performed for the selected discovery task and allows administrators to download scan reports
	Last Scan Details	Displays the results of the last scan for the selected discovery task
	Clean Results	Removes all the discovered certificates from the SSL certificates tab

10.3.1.1. Prerequisites

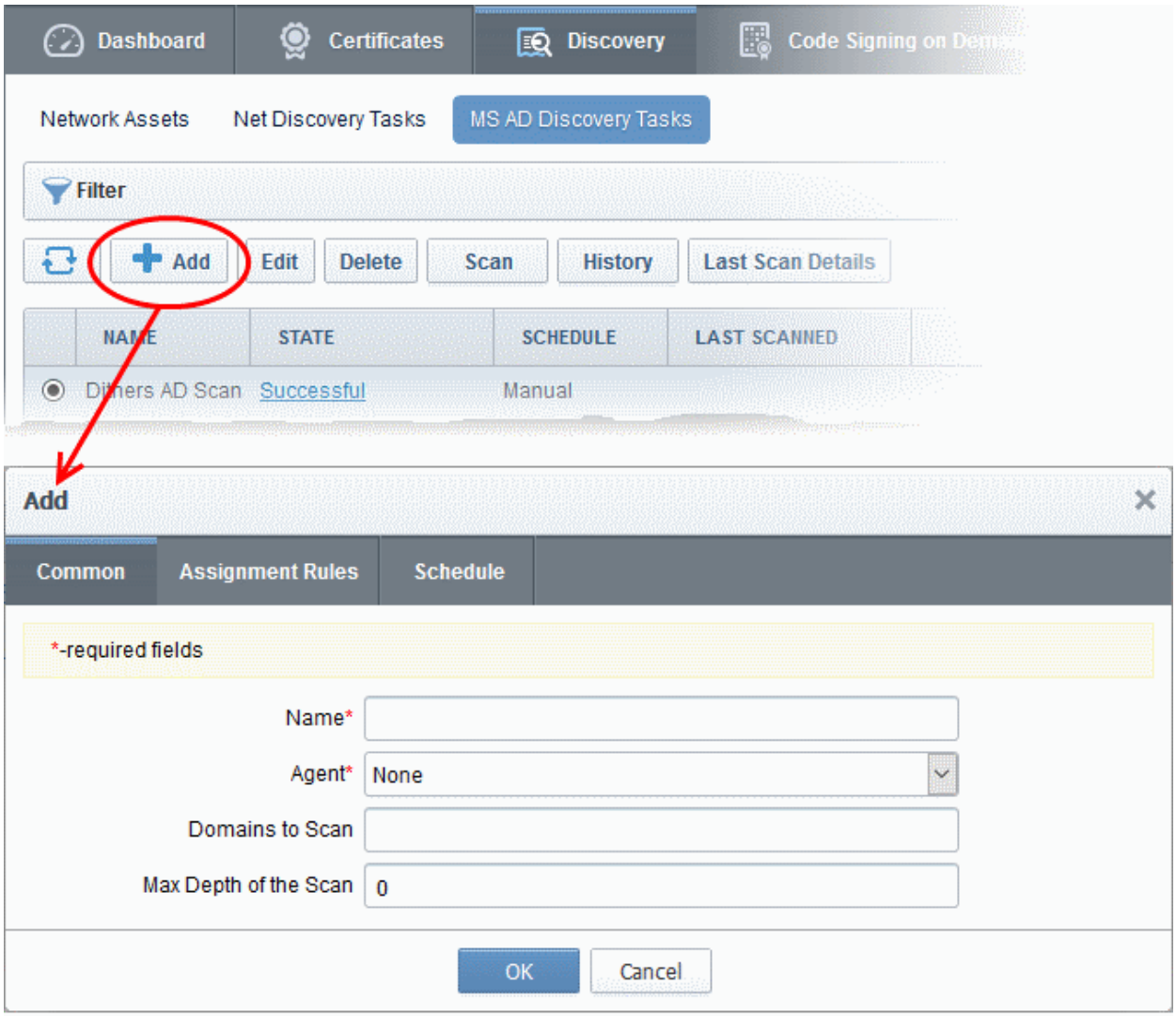
The administrator has installed the MS Agent on required AD server and has integrated the server to CCM. See Comodo CA Proxy Service Installation for more details.

10.3.1.2. Overview of Process

1. Run a scan on an AD domain in order to find the network object structure, endpoints, user accounts and all deployed certificates.
2. Discovered items will be shown in the CCM interface as follows:
   - All discovered certificates will be listed under respective certificate types in the Certificates area of the CCM interface. ('Certificates' > 'SSL Certificates', 'Certificates' > 'Client Certificates', 'Certificates' > 'Code Signing Certificates', 'Certificates' > 'Device Certificates').
   - All items discovered on the AD domain will be shown in the 'Network Assets' interface. See View Results of AD Discovery Scan Tasks for more details. This includes certificates and items like devices, user accounts, and endpoints.
3. CCM will update the status of existing certificates that were issued using CCM (if necessary)
4. 'Unmanaged' certificates can become 'Managed' by renewing the particular certificate

10.3.1.3. Add Domains and Start Scanning

1. To add a new MS AD discovery scan task, click 'Discovery' > 'MS AD Discovery Tasks'> 'Add' to open the scan configuration form

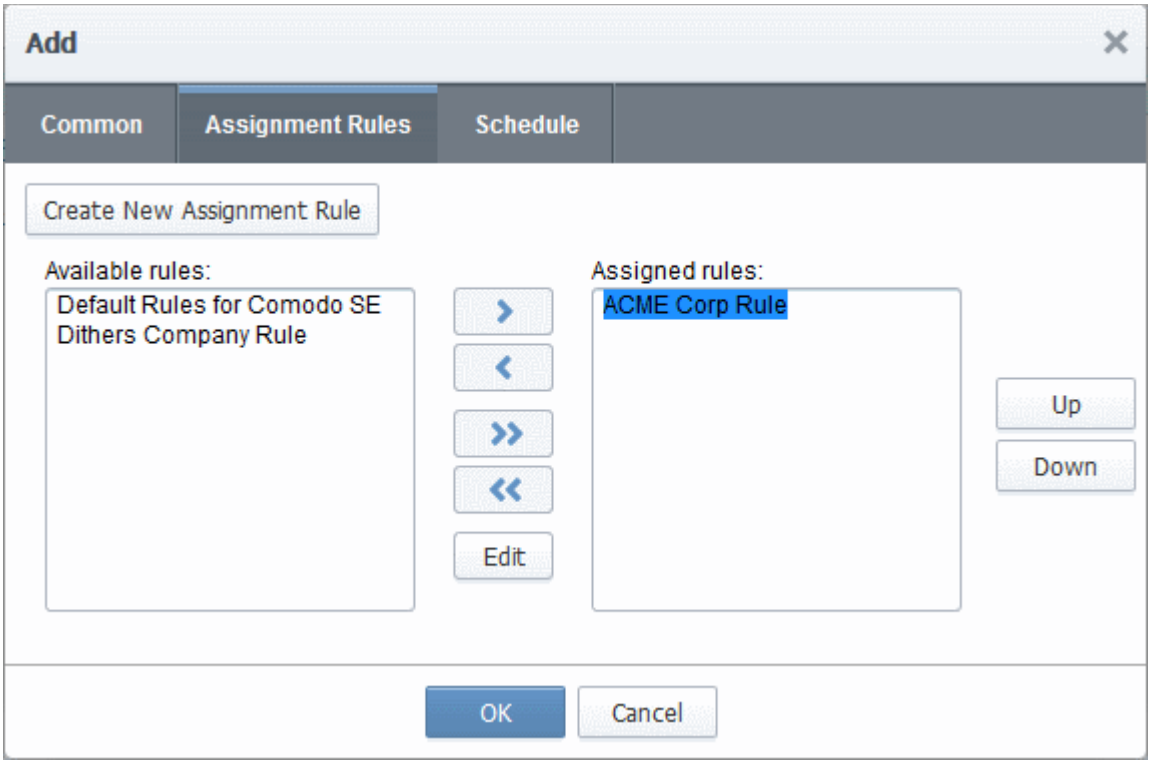


The form has three tabs. The first to configure scan settings, the second to apply auto-assignment rules and the third to schedule the scan.

2. First, complete the 'Common' tab:

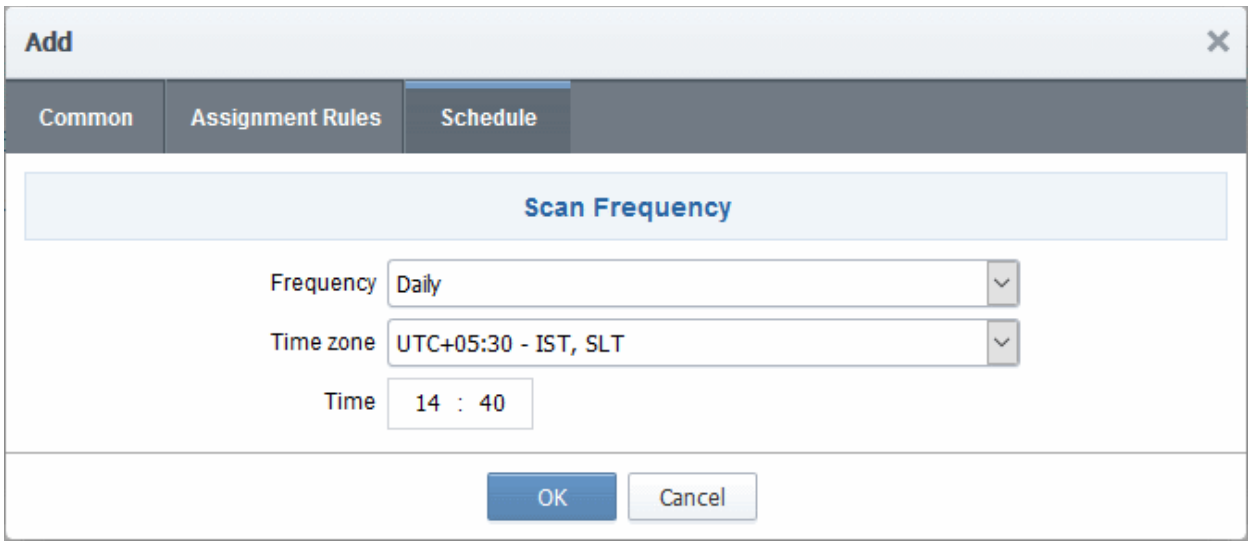
Form Element	Description
Name	Enter a name to describe the AD discovery task
Agent	Select the MS AD Agent or AD Agent Cluster to be used for scanning. For more details on MS Agents and clusters,
Domains to Scan	Enter the Active Directory domains you wish to scan.
Max Depth of the Scan	Select the number of network hierarchy levels to be scanned. The depth of the scan should cover all required endpoints/users and other AD objects in the network. 0 = Unlimited

3. Click the 'Assignment Rules' tab to add rules which will assign unmanaged certificates identified by the scan to an organization or department.



- Administrators can create and manage rules which automatically assign discovered certificates to specific organizations/departments.
- The rules can be configured in 'Settings' > 'Assignment Rules'. For more details on managing auto-assignment rules, see Auto-Assignment Rules for Unmanaged Certificates.in the CCM MRAO Administrator Guide
    - All auto-assignment rules configured on your CCM account are shown on the left.
    - Use the arrow buttons to add rules to the discovery task.
    - To create a new rule, click the 'Create New Assignment Rule' button.
    - To edit a rule, select it and click the Edit button.

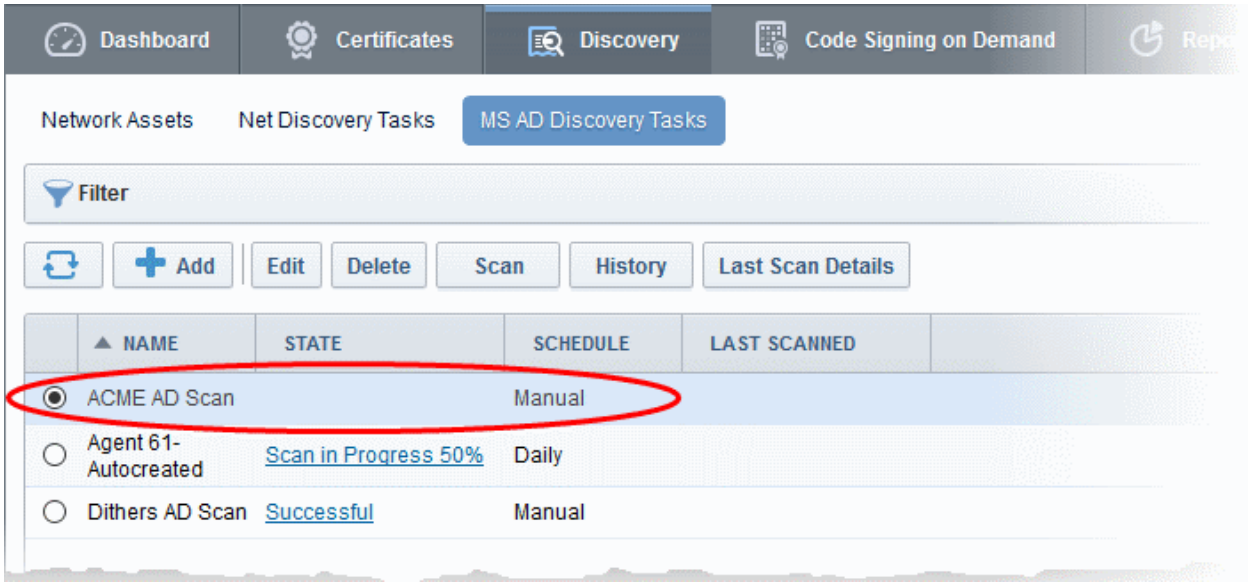
4. Click the 'Schedule' tab to set the scan day, date and start time, and the frequency of the scans according to the task:



Available scan frequencies are: Manual (on demand), Daily, Weekly, Monthly, Quarterly, Semi-Annually and Annually.

5. Click 'OK'.

The newly created discovery task will be displayed in the list.

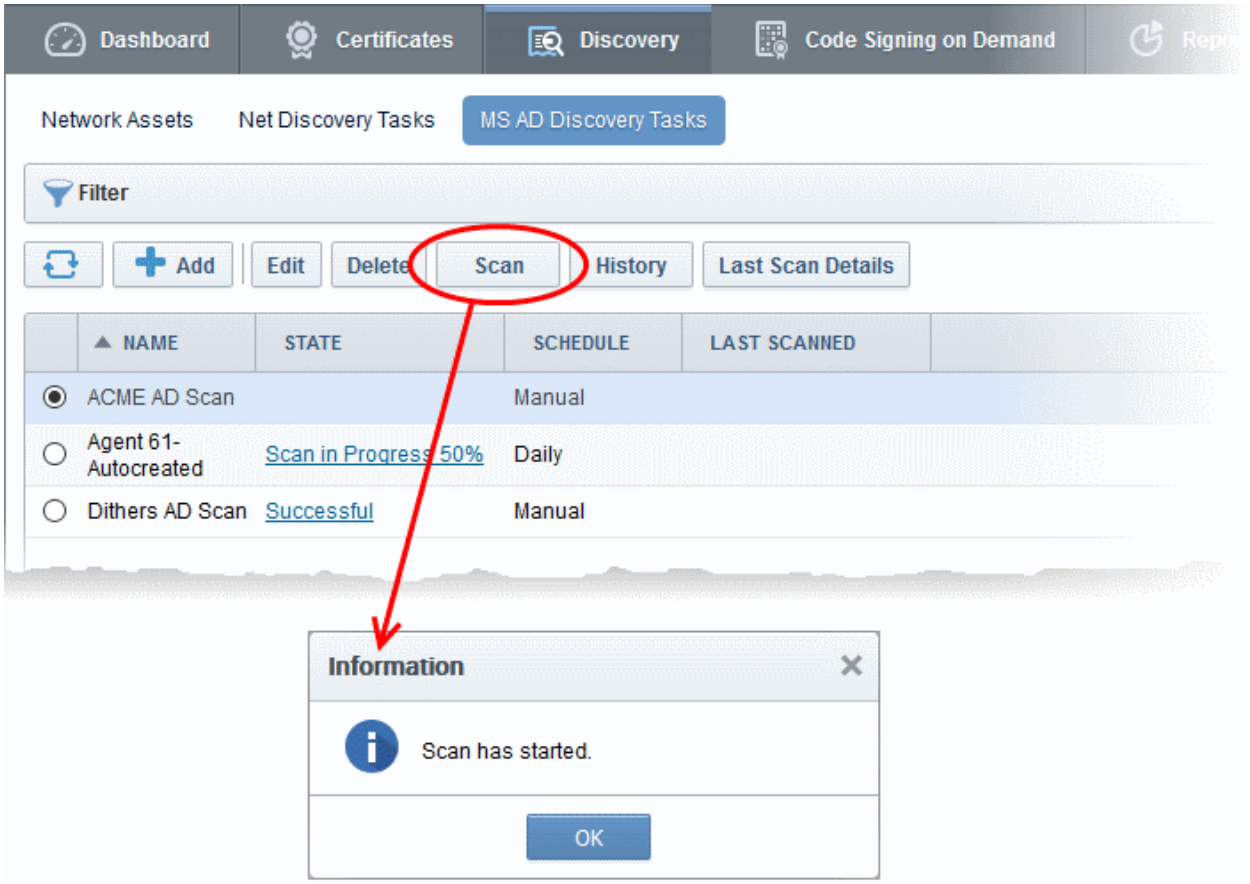


Repeat the process to add more MS AD Discovery Tasks.

6. To run a scan, select the respective 'Discovery Task' from the list

The control buttons for managing the task will appear at the top.

7. Click the 'Scan' button to commence the discovery scan for the selected task.

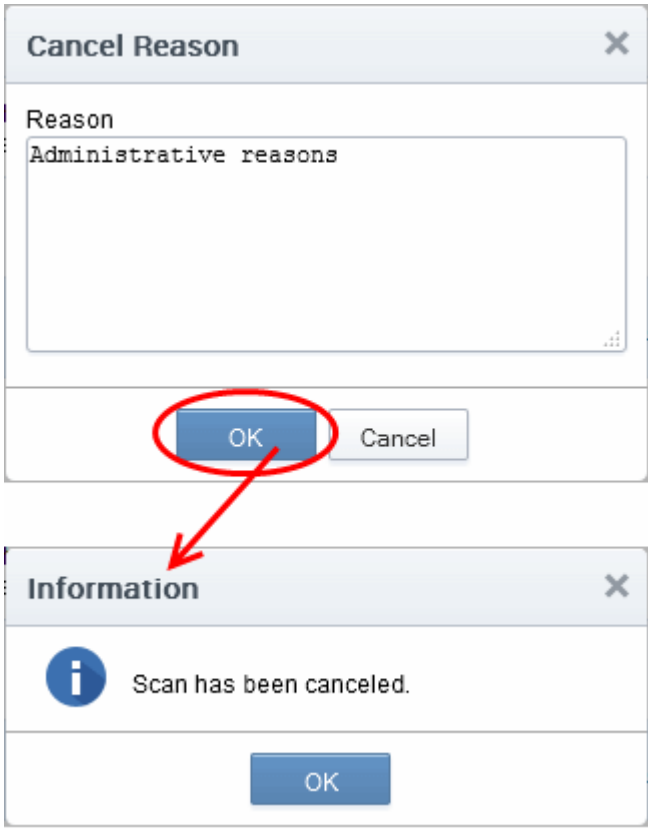


Note: You can manually initiate a scan only for the tasks with schedule 'Manual'. Other scan will automatically run as per the schedule set for respective the task.

CCM allows administrators to run multiple discovery tasks at a time. After a scan has started, select another task and click the scan button at the top.

If you cancel the scanning process, the entire system will revert to the state that existed before the scan was started (i.e., any data collected during scanning will not be applied until the scanning process is completed).

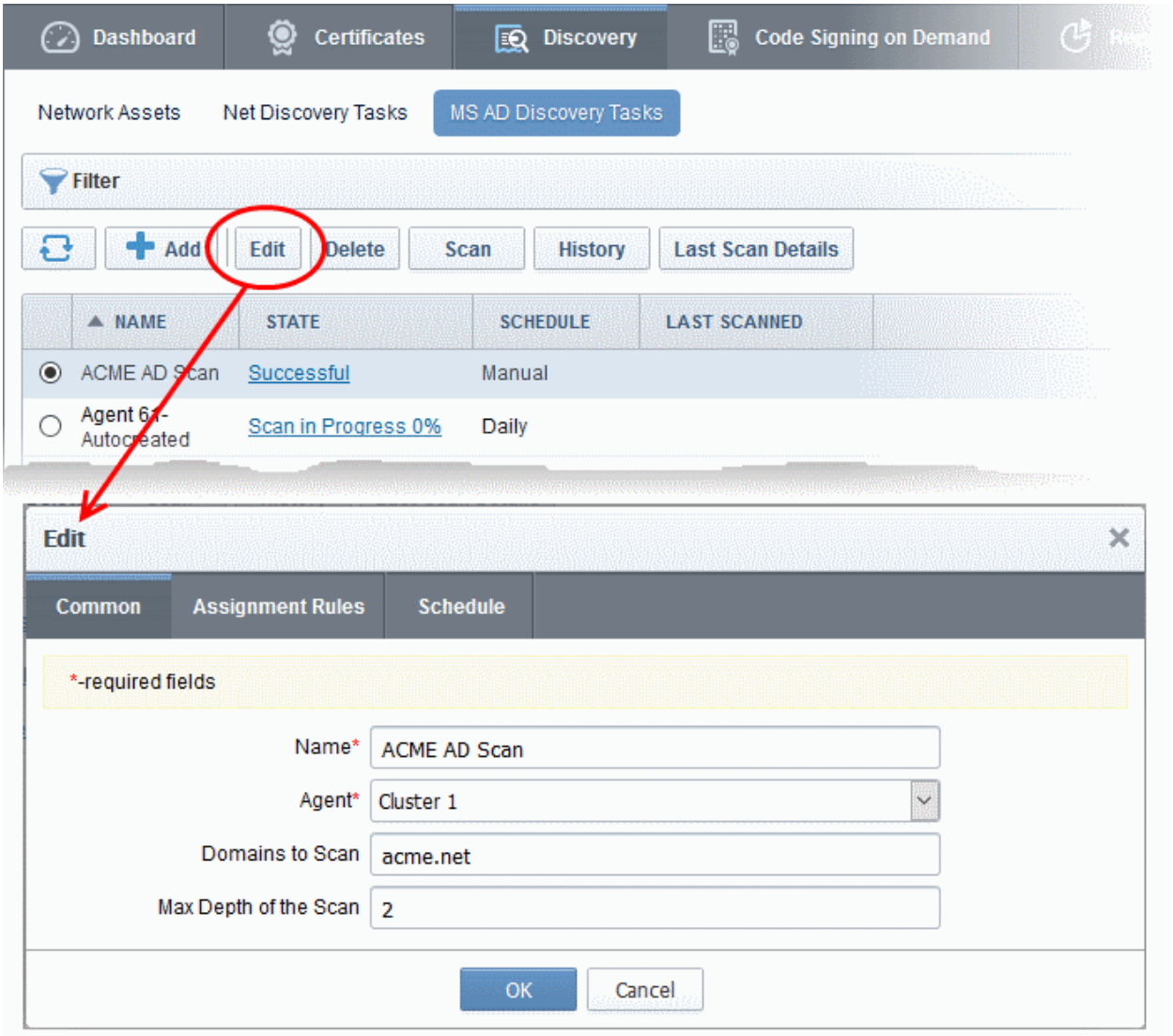
If you cancel the scanning, you should specify the reason for in the 'Cancel Reason' dialog and click OK.



After the scan is complete, the results will be shown under 'Active Directory' in the 'Discovery' > 'Network Assets' area of the CCM interface.

10.3.1.4. Editing an AD Discovery Task

Administrators can reconfigure an existing AD discovery task by selecting it in the list and clicking the 'Edit' button at the top.

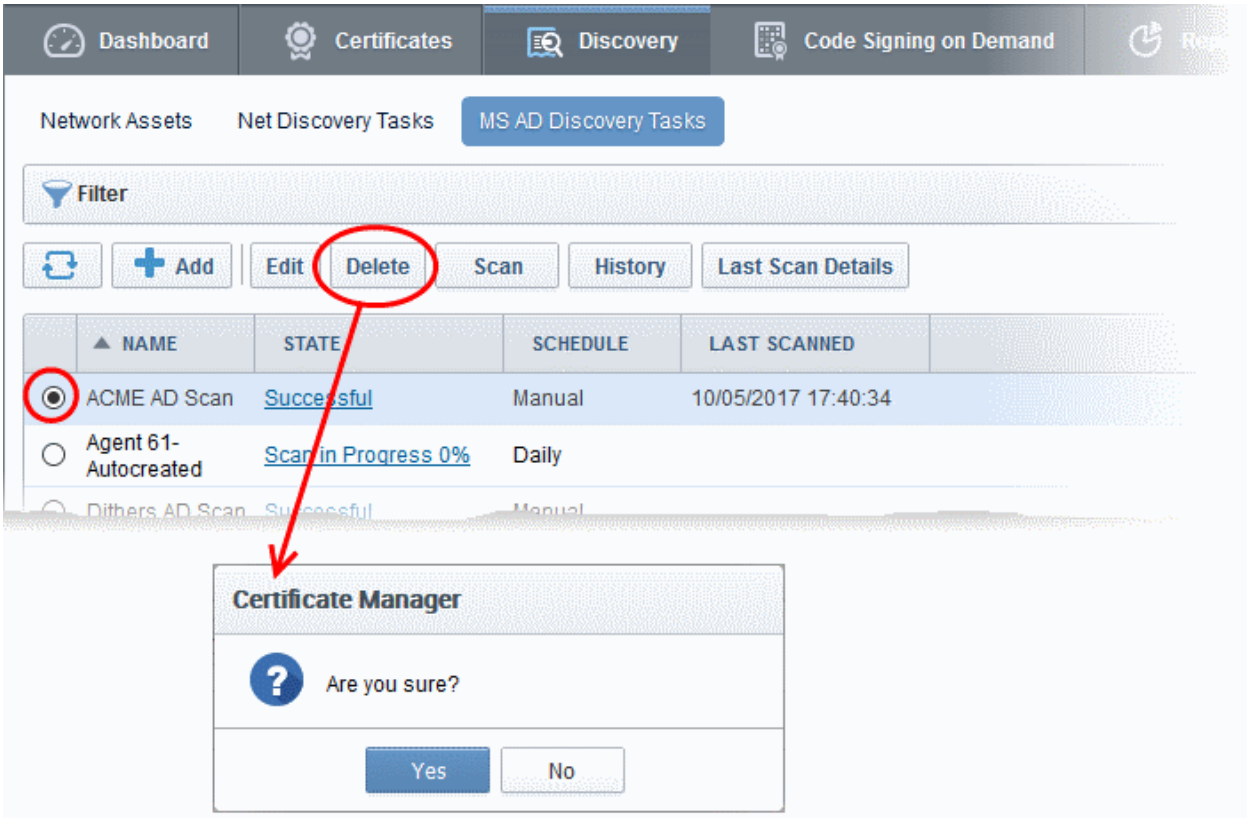


The 'Edit' interface will open.

The interface is similar to the from for adding a new discovery task and allows administrators to change the task name, select a another agent, choose a different domain, add or remove assignment rules, change the schedule and more. For more details see Add Domains and Start Scanning.

10.3.1.5. Deleting an AD Discovery Task

To remove an AD discovery task from the list, select it and click the 'Delete' button at the top.

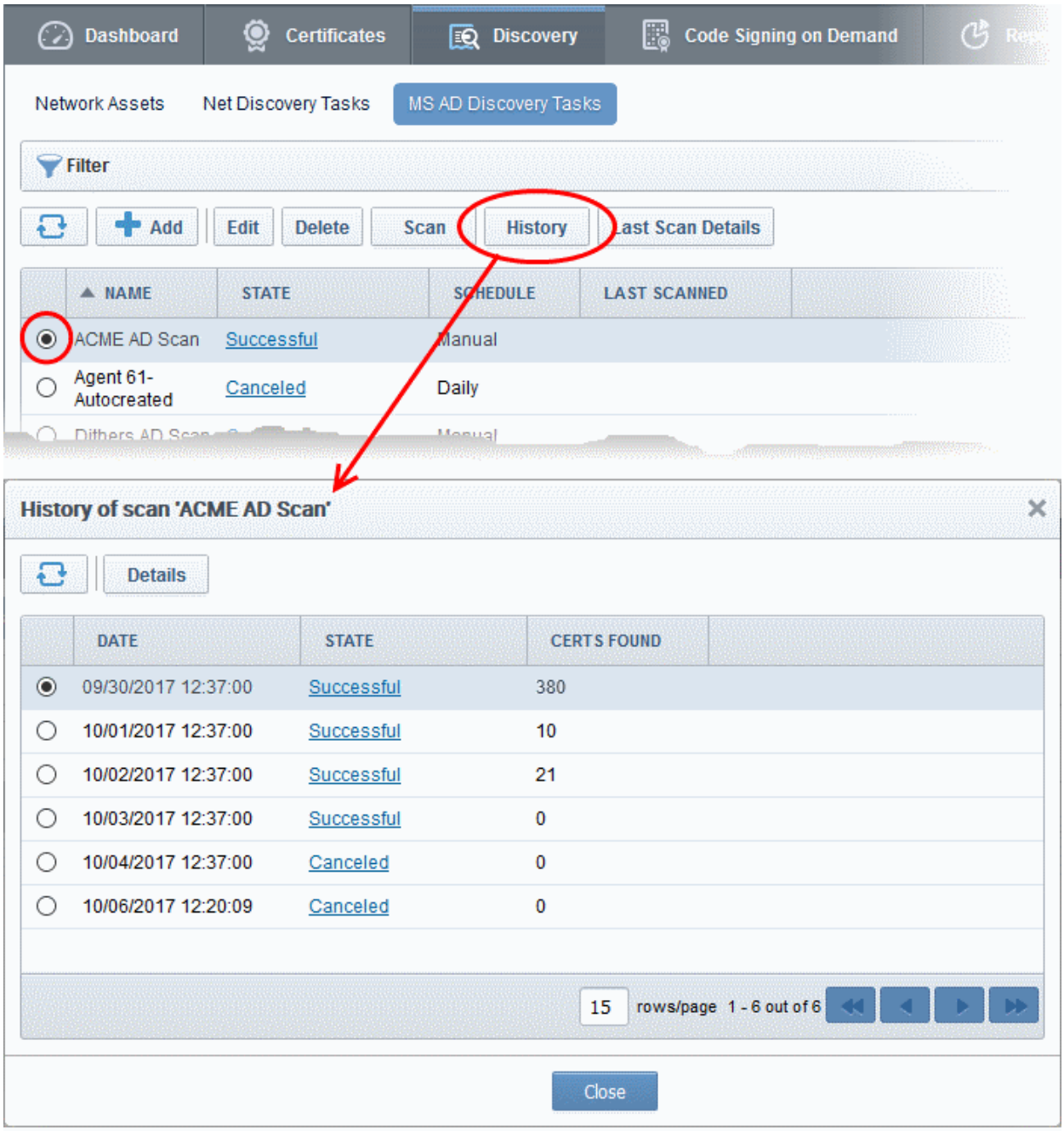


10.3.1.6. View History of AD Discovery Task

Administrators can view the results of previous scans for each AD discovery task. You can also view details of certificates identified by each scan and can assign unmanaged certificates to an organization or department.

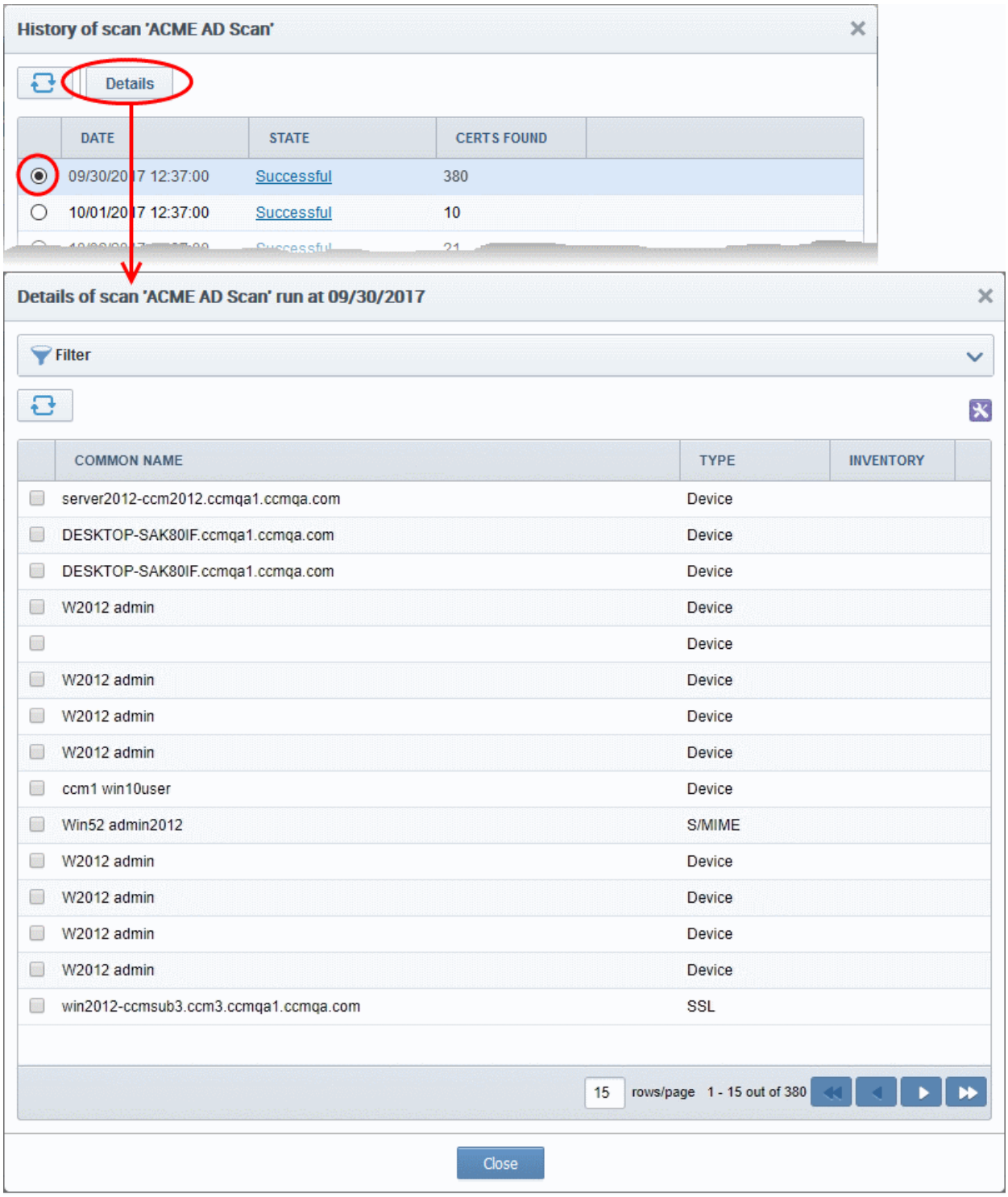
To view task history:

- Click 'Discovery' > 'MS AD Discovery Tasks'
- Select a task from the list
- Click the 'History' button above the table
- All previous scans run under the task will be listed in a new window:

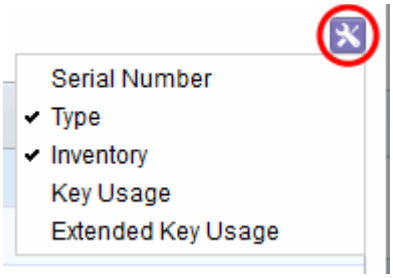


History of Scan - Column Descriptions	
Column Header	**Description**
Date	Precise date and time at which the scan was run
State	Whether the scan succeeded, failed, or was canceled.
Certs Found	The total number of certificates identified by the scan. This includes SSL certificates, client certificates, code signing certificates and device certificates.

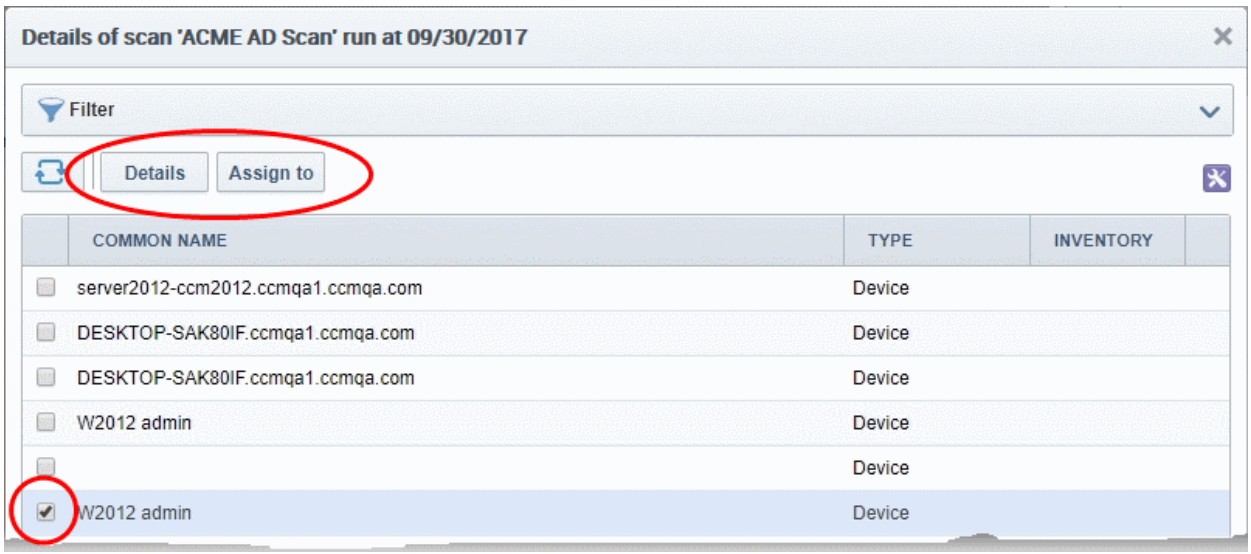
- Click the 'Details' button to view all certificates discovered during a scan:



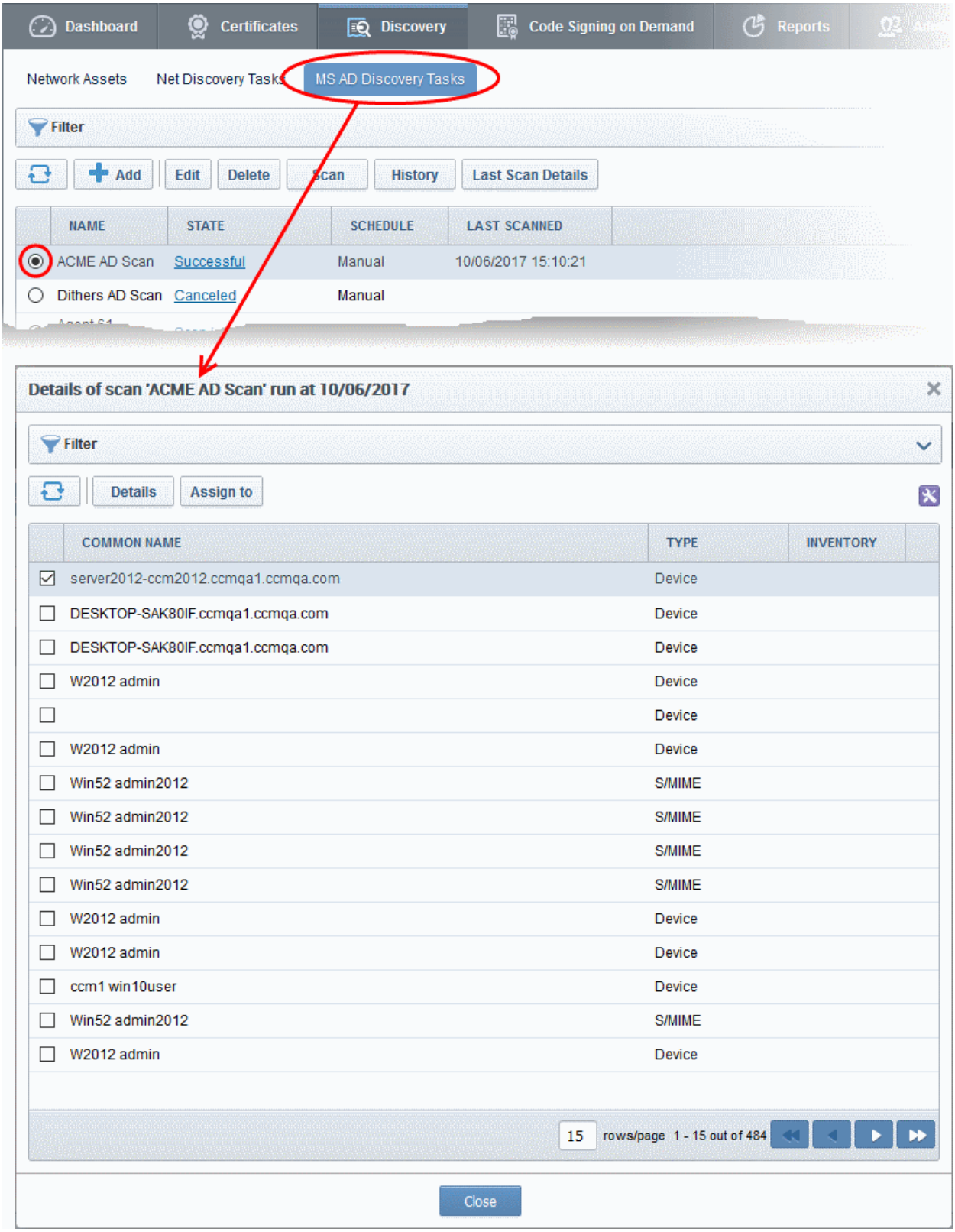
Details of AD Scan - Column Descriptions	
Column Header	**Description**
Common Name	The value in the 'Common Name' field of the certificate. This will vary according to certificate type. SSL certificates will usually show a domain name. S/MIME certificates may show an email address or host name, and device certificates usually show the host name of the device.
Type	Indicates whether the certificate is SSL (web server), SMIME (email certificates, client certificates), code signing, or device certificate.

Inventory	Indicates whether the certificate is 'Managed' or 'Unmanaged'. • **Managed** - The certificate was requested and issued using Comodo Certificate Manager. Click a 'Managed' link to view certificate details. You can also open certificate details dialog by selecting the certificate and clicking the 'Details' button. • **Unmanaged** - The certificate was not requested/issued using CCM. This category includes 3rd party certificates, self-signed certificates and Comodo certificates issued by other platforms. Select an 'Unmanaged' certificate and click the 'Assign to...' button to delegate it to an organization or department Tip - CCM allows you to configure AD discovery scans to automatically assign unmanaged certificates to an specific organization or department. See Overview of Process under Active Directory Discovery Tasks for more details.
Note: Administrators can enable or disable columns by clicking the button on the right: 	
Serial Number	The unique serial number of the certificate. This can be used to identify the certificate.
Key Usage	The cryptographic purpose(s) for which the certificate can be used. For example, key encipherment and signing.
Extended Key Usage	Higher level capabilities of the certificate. For example, web server authentication and client authentication.

- Click the 'Assign to' button to manually delegate an unmanaged certificate(s) to an organization or department.



- Click the 'Last Scan Details' button to view certificates discovered by the most recent scan:

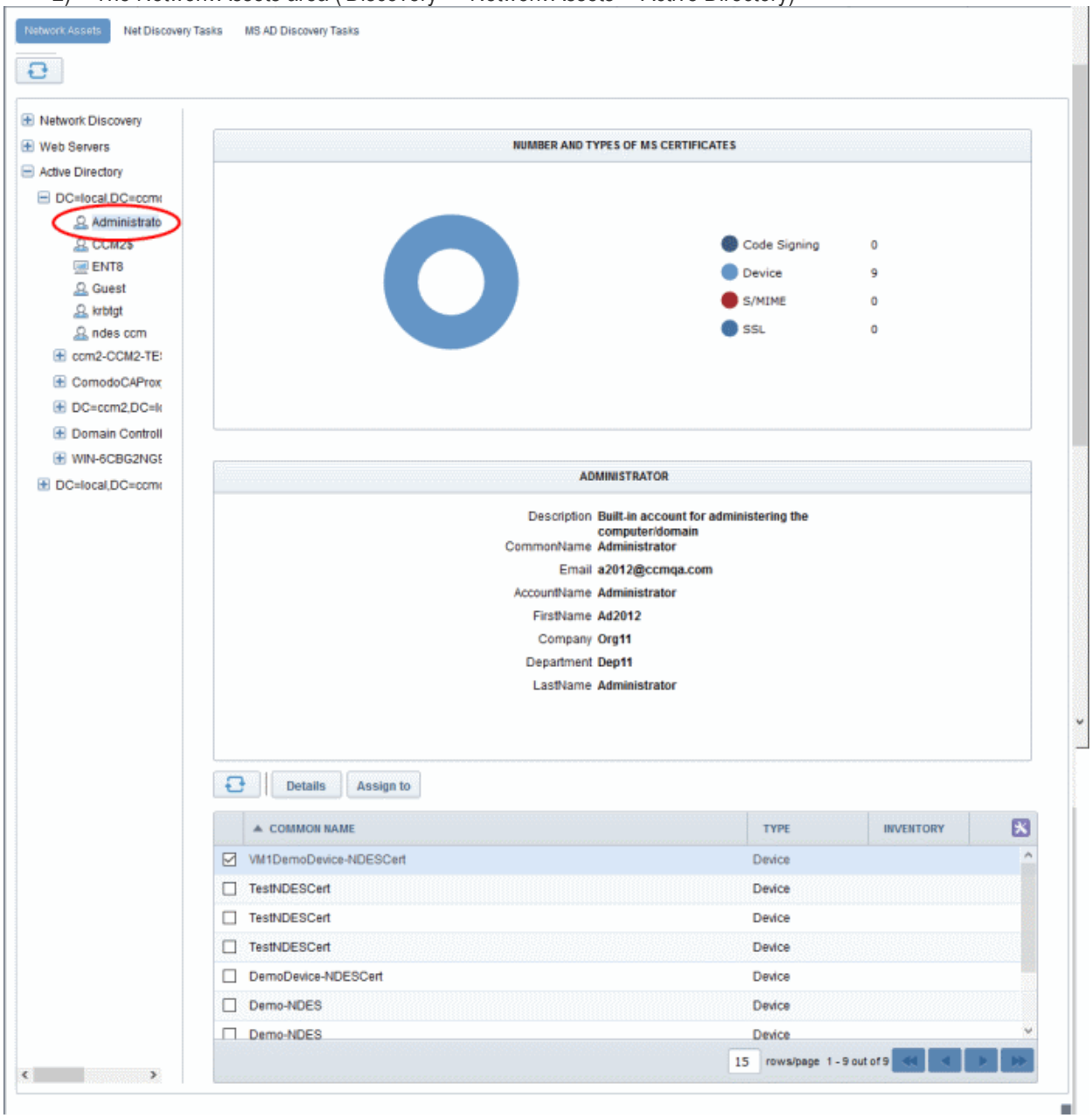


10.3.1.7. View Results of AD Discovery Scan Tasks

After each Active Directory discovery scan, Comodo Certificate Manager updates the lists of certificates in the following areas of the CCM interface:

1) The 'Certificates' area ('Certificates' > 'SSL Certificates', 'Client Certificates', 'Code Signing Certificates' and 'Device Certificates').

2) The Network Assets area ('Discovery' > 'Network Assets' > Active Directory)



The Active Directory section of 'Network Assets' contains:

- Managed certs
- Unmanaged certs which are assigned to an Org/Dep.
- Unmanaged certs which are **not** assigned to an Org/Dep.
- Network objects including domains, users and devices enrolled to the AD domain

- The Active Directory area shows AD domains that have been integrated to CCM by installing the MS agent.
- Each AD tree shows objects found on the domain (including user accounts, devices and endpoints) and all certificates associated with that object.
- You can view details of each certificate and manually assign unmanaged certificates to organizations or departments. Doing so will make them available in the SSL certificates interface.

Comodo advises administrator to:

i. Schedule regular discovery scans as a matter of course;

ii. Run a manual scan after every change to certificate configuration. Otherwise, it is possible that the 'SSL Certificates' area will show inaccurate information. (e.g. you may have uploaded a certificate to your website but in CCM the certificate will have a state of 'Issued' and a discovery status of '**Not deployed**' if you haven't re-run the scan).

iii. Run a manual scan after any change to the network in general.

11. Troubleshooting

11.1. Enrollment Failure

See *.log files under \Log sub-folder for error logs. Logs can be opened with any text viewer or editor.

In case of enrollment failure, please make sure that the following is completed:

1) Names of the organization and the department in user's properties at Active Directory side matches the corresponding settings on the CCM side.
2) The email address in user properties at the Active Directory side is valid.
3) The selected domain is delegated to appropriate organization and department in CCM.
4) Active Directory certificate template has Read, Enroll, Autoenroll permissions for appropriate users and/or groups. Also enrollment and auto-enrollment is allowed by Public Key Policies of the domain.
5) ccm_ca32.exe is trusted for domain network and allowed by Windows Firewall

11.2. Unsupported Editions of Windows 2008/R2

Some editions of Windows Server 2008/R2 are not supported.

- Web Edition - has limited functionality, ADCS role cannot be installed
- Itanium Edition - has limited functionality, ADCS role cannot be installed.

Also the Comodo CA Proxy is built for IA-32 and x64 (x86-64) architectures. It is incompatible with Itanium (IA-64) architecture.

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