



Comodo Certificate Manager

Active Directory - Certificate Template Settings for Enrollment
from MS CA

Certificate template settings for 'Enroll-On-Behalf' feature

The following settings are for user and computer-based templates for the CCM 'Enroll-On-Behalf' feature.

Setting templates:

1. Open the Windows command prompt (cmd).
2. Run the following command: certtmpl.msc
3. Duplicate the desired template for the 'enroll-on-behalf' feature.
4. Customize the template properties as explained below:
 - a) 'Template display name': Any name is allowed, but note the restrictions on the number of significant characters in Windows identifiers. For example: WWW

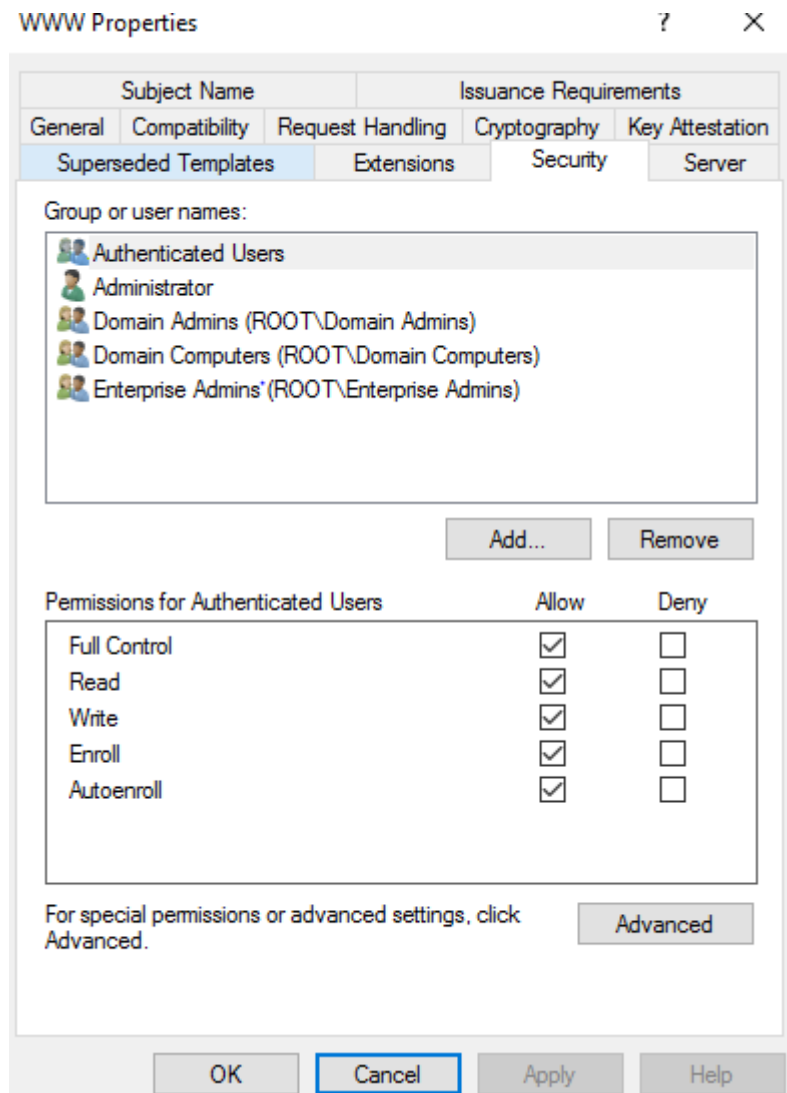
The screenshot shows the 'WWW Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a question mark and a close button. The main area is divided into several sections: 'Subject Name' and 'Issuance Requirements' at the top; 'Superseded Templates', 'Extensions', 'Security', and 'Server' below that; and 'General', 'Compatibility', 'Request Handling', 'Cryptography', and 'Key Attestation' at the bottom. The 'General' tab is active, showing 'Template display name:' and 'Template name:' both set to 'WWW'. Below these are 'Validity period:' set to '1 years' and 'Renewal period:' set to '6 weeks'. At the bottom, there are two checkboxes: 'Publish certificate in Active Directory' (unchecked) and 'Do not automatically reenroll if a duplicate certificate exists in Active Directory' (unchecked). The 'Cancel' button is highlighted with a blue border.

- b) Configure the 'Compatibility' tab as shown below :

The screenshot shows the 'WWW Properties' dialog box with the 'Compatibility' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are two main sections: 'Subject Name' and 'Issuance Requirements'. Under 'Issuance Requirements', there are four sub-sections: 'Superseded Templates', 'Extensions', 'Security', and 'Server'. The 'Compatibility' tab is active, showing a message: 'The template options available are based on the earliest operating system versions set in Compatibility Settings.' Below this message is a checked checkbox labeled 'Show resulting changes'. A 'Compatibility Settings' box contains two dropdown menus: 'Certification Authority' set to 'Windows Server 2016' and 'Certificate recipient' set to 'Windows 10 / Windows Server 2016'. At the bottom of the dialog, there are four buttons: 'OK', 'Cancel' (highlighted with a blue border), 'Apply', and 'Help'. A note at the bottom of the dialog states: 'These settings may not prevent earlier operating systems from using this template.'

Note: Admin should not necessarily use Server 2016. They need to use the highest/latest values of compatibility available to them.

c) Open the 'Security' tab and provide the necessary permissions for the requester:



Note: Make sure to have 'Domain Admins' in 'Group or user names' section with at least "Read" and "Enroll" permissions assigned.

d) Open the 'Request Handling' tab and enable 'Allow private key to be exported' (if disabled):

WWW Properties ? X

Subject Name		Issuance Requirements		
Superseded Templates		Extensions	Security	Server
General	Compatibility	Request Handling	Cryptography	Key Attestation

Purpose: ▾

Delete revoked or expired certificates (do not archive)

Include symmetric algorithms allowed by the subject

Archive subject's encryption private key

Authorize additional service accounts to access the private key (*)

Allow private key to be exported

Renew with the same key

For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

Enroll subject without requiring any user input

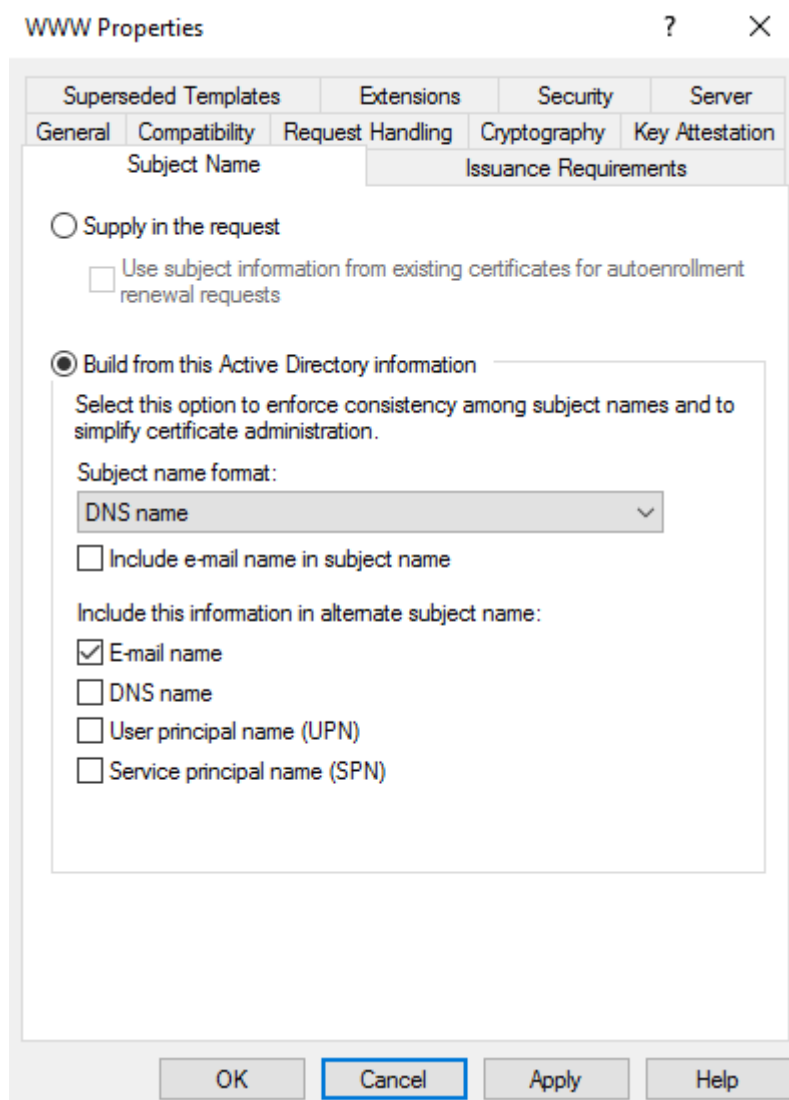
Prompt the user during enrollment

Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to [compatibility settings](#).

e) If it is a user-based template for the 'enroll-on-behalf' feature, click 'OK' and go to '**Setting the Certificate Authority (CA) properties for the 'Enroll-on-behalf' feature**'. Or if it is a computer-based template proceed with template settings configuration as explained below:

- Open the 'Subject Name' tab to create the correct subject for the template. Select 'Build from this Active Directory information'. Choose 'DNS name' as the format and 'Email name' as information to include in the alternate subject name:



- Open the 'Issuance Requirements' tab. Set the following properties for the 'Enroll-On-Behalf' feature to work with computer-based templates:
 - i. Set a minimum of 1 authorized signatures
 - ii. Set the following:
 - 'Policy type required in signature:' - 'Application Policy'
 - 'Application Policy:' - 'Certificate Request Agent'
- Click 'OK' button and proceed as follows below.

Setting the Certificate Authority (CA) properties for the 'Enroll-on-behalf' feature :

1. Return to the Windows command prompt (cmd).
2. Run the following command: `certsrv.msc`
3. Customize the CA properties as explained below:
 - a) Right-click the CA name > 'Properties' > "Enrollment Agents" tab > Add the following properties and click 'OK' button:

WWW Properties ? X

Superseded Templates	Extensions	Security	Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation

Subject Name Issuance Requirements

Require the following for enrollment:

CA certificate manager approval

This number of authorized signatures:

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:
Application policy

Application policy:
Certificate Request Agent

Issuance policies:

Require the following for reenrollment:

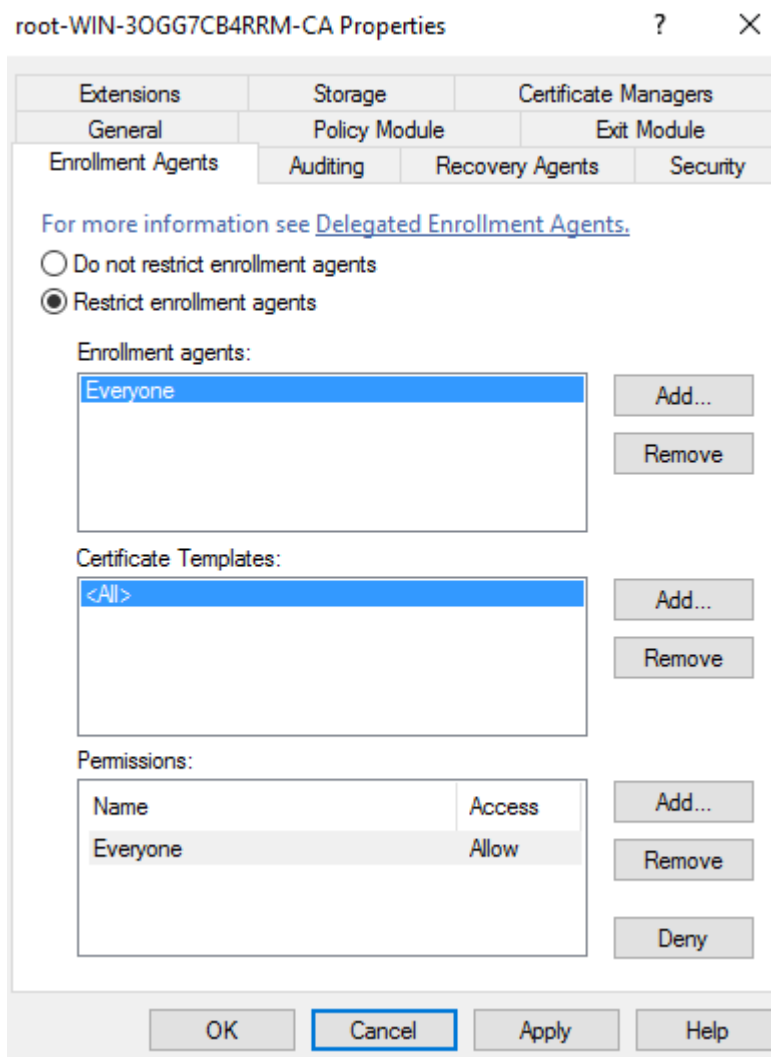
Same criteria as for enrollment

Valid existing certificate

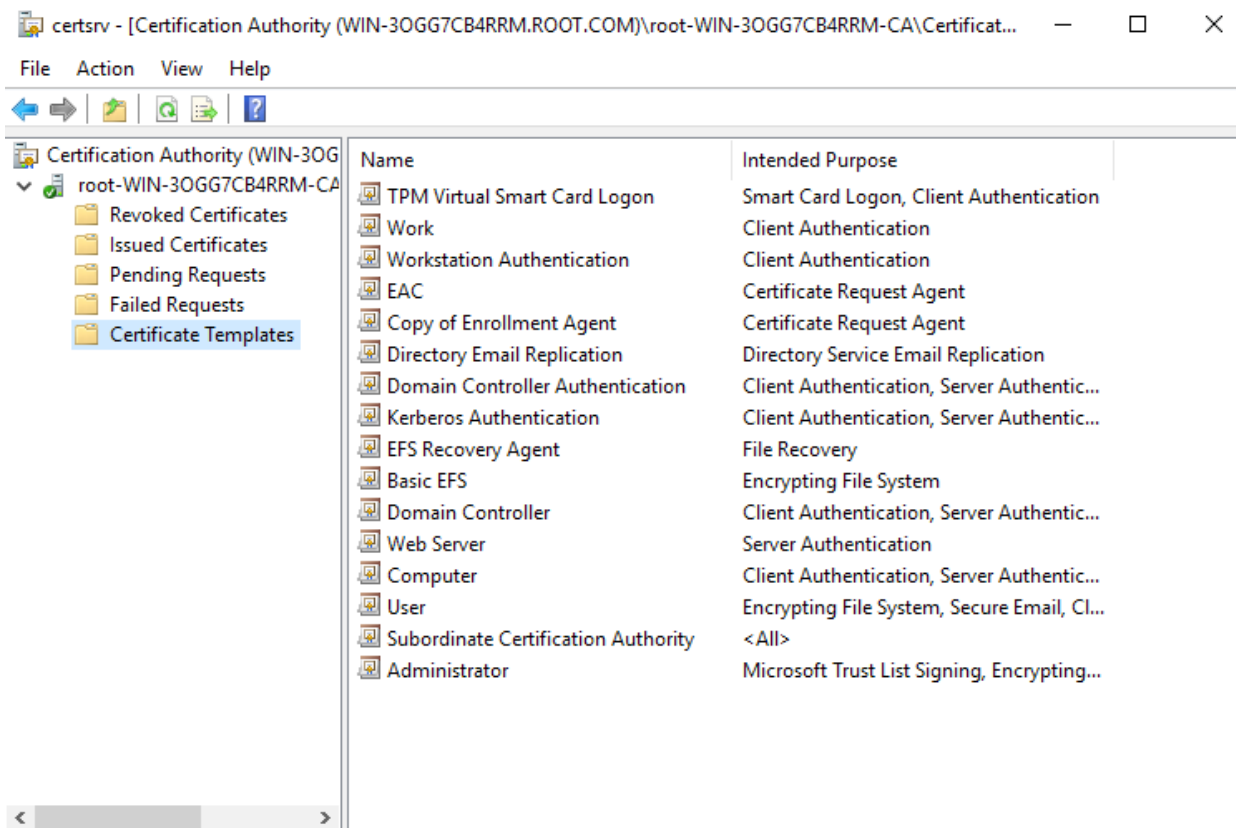
Allow key based renewal

Requires subject information to be provided within the certificate request.

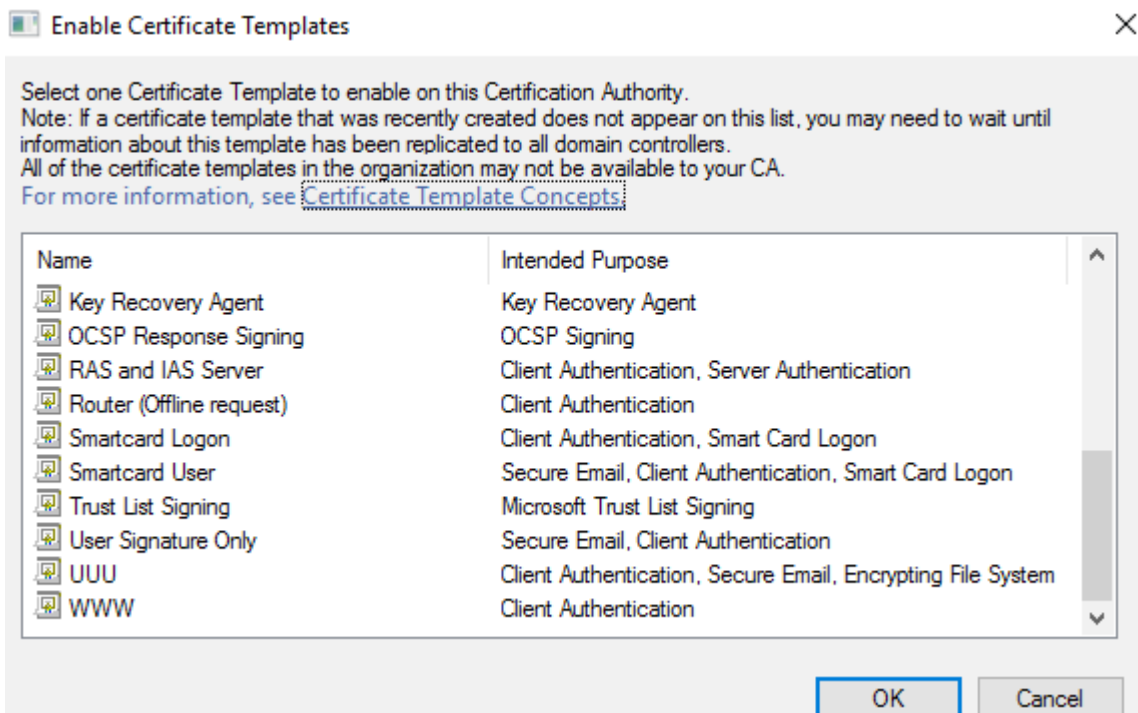
b) Double-click the CA name > Click 'Certificate Templates' :



1. Right-click within this file list area > 'New' > 'Certificate Template to Issue'



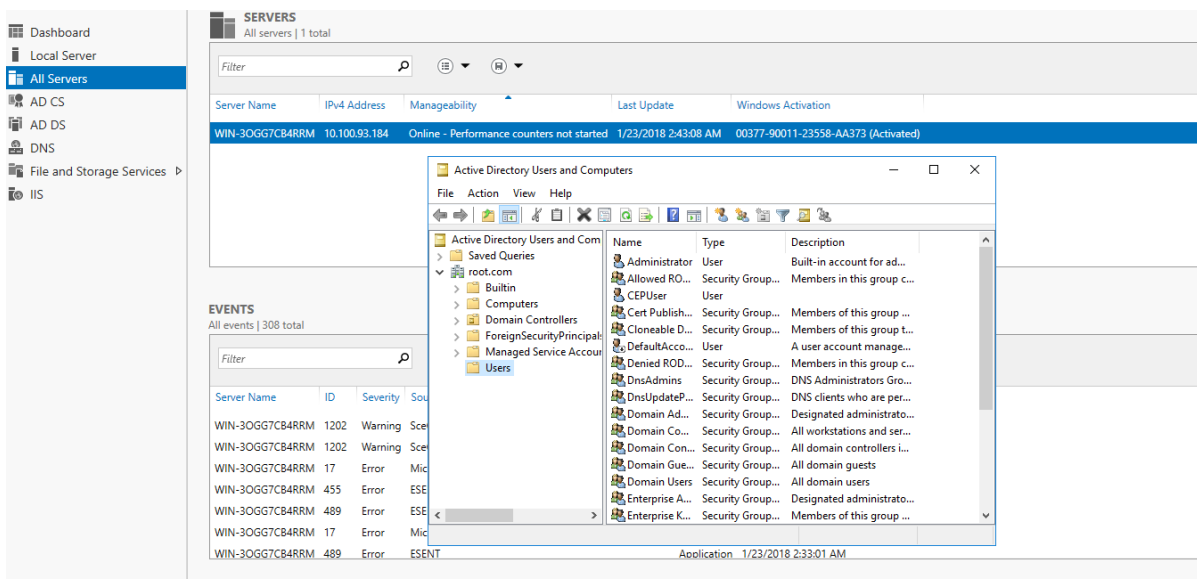
- Add the template that you modified earlier to the CA. In the example below, 'WWW' is the new template:



- Restart the CA server

Setting the 'Requester properties' for the 'Enroll-on-behalf' feature:

- (a) Open the Server Manager
- (b) Choose 'All Servers' in the left panel
- (c) Right-click any CA server name and choose 'Active Directory Users and Computers'
- (d) Change the domain, if necessary to get the one, that matches the user which was specified as Domain Administrator during MS-Agent installation, displayed
- (e) Choose 'Users' sub-menu (or the relevant organization unit) for this domain (that matches the user which was specified as Domain Administrator during MS-Agent installation):




(f) Right-click Admin name, who was specified as Domain Administrator during MS-Agent installation, and who will provision the certificate requests against this certificate template > 'Properties' > Set the detailed properties as shown below :

- Mandatorily add the e-mail of this Administrator:

Administrator Properties [?] [X]

Published Certificates	Member Of	Password Replication	Dial-in	Object	
Security	Environment	Sessions	Remote control		
Remote Desktop Services Profile	COM+	Attribute Editor			
General	Address	Account	Profile	Telephones	Organization

 Administrator

First name: Initials:

Last name:

Display name:

Description:

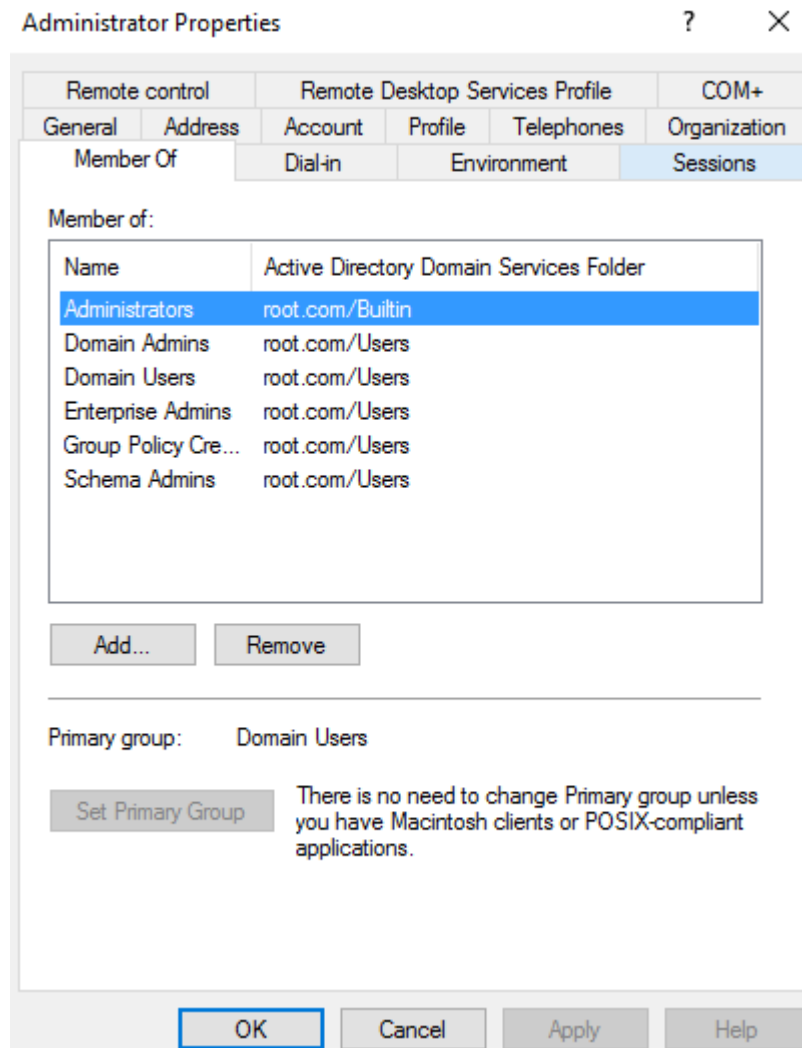
Office:

Telephone number:

E-mail:

Web page:

- Check the administrator's properties and ensure that this Admin is included in 'Domain Admins' group :



(g) Right-click Admin name who will need to request certificate against this template > 'Properties' > Mandatorily add the e-mail of this Administrator in order to populate Subject and SAN of the certificate this Admin will be enrolling for.

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, Greater Manchester M5 3EQ,
United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767