



Application Note: EAP-TLS with 9600 Phones

**Issue 2.0
January 2014**

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products.

Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <http://www.avaya.com/support>

Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, <http://support.avaya.com/Licenseinfo> ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING

THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo/> under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: <http://support.avaya.com/ThirdPartyLicense/>. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://www.avaya.com/support>.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading documents

For the most current versions of documentation, see the Avaya Support website:

<http://www.avaya.com/support>

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.

Table of Contents

1.	Introduction	7
2.	Authentication Workflow	8
3.	Certificate Authority Server	10
1)	Installation Pre-Requisite:	10
2)	Install Active Directory Certification Service	10
3)	Export the Root Certificate from the AD CS	31
4)	Verify Details of the Root Certificate	32
4.	RADIUS Server	33
1)	Installation Pre-Requisite:	33
2)	NPS Installation:	33
3)	Configure Template and Autoenrollment	37
4)	Register the NPS in Active Directory Domain Services	38
5)	Create a New Certificate Template	39
6)	Enable The Certificate Template	46
7)	Modify Registry	49
8)	NPS Configuration:	51
5.	Phone User Definition	74
6.	File Server	79
7.	LAN Switch Configuration	80
8.	Phone's Configuration and Settings	81
9.	Troubleshooting	87

1. Introduction

The IEEE 802.1X is a standard for a port based network access control, providing authentication mechanism to devices connected to a wired or wireless network. It defines the encapsulation of EAPOL (Extensive Authentication Protocol Over LAN) as the authentication protocol.

The EAPOL defines an interaction among three entities:

- Supplicant – End user device (i.e. the phone)
- Authenticator (i.e. network switch)
- Authentication server

It begins with the supplicant trying to access a certain restricted network resource, and upon successful authentication by the authentication server, the supplicant is granted access.

The process of authentication is aided by the authenticator. It communicates with the supplicant via L2 packets, since the supplicant might not even have an IP address. To forward the requests to the authentication server, the authenticator repackages the information in a different format, usually by RADIUS protocol, and forwards it to the authentication server.

In case of EAP-TLS, authentication is done through certificates. Both supplicant and authentication server authenticate each other. So the phone and the authentication server should trust a common certificate authority (CA) for this purpose.

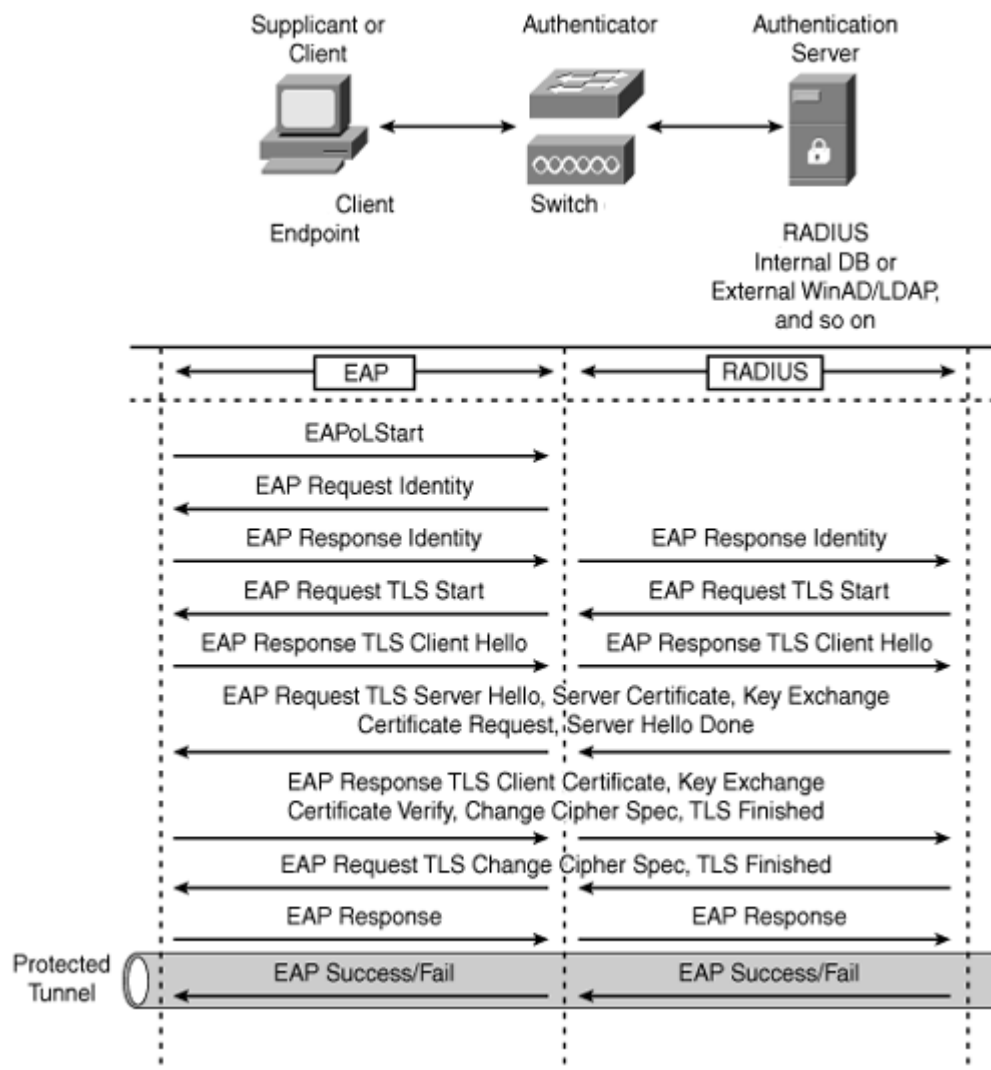
This document is a step-by-step guide of how to configure the various network components in order to obtain a successful 802.1X EAP-TLS authentication of a 9600 phone (H.323 or SIP) to the network.

This document is focused on the Microsoft Active Directory environment based on Windows Server 2008 R2 Enterprise. The configuration shown here is a simple example aimed to show the scope of work that needs to be done in order to implement EAP-TLS authentication with Avaya 9600 series phones. In our example the same Windows server has the Active Directory Server, Certificate Authority Server and RADIUS Server (NPS) roles. In real world implementations these servers may be installed on different machines, so the actual configuration might be different than shown.

Avaya 9600 series phones are environment independent and can support other environments than described here, as long as standard protocols are being used (802.1X, EAP, RADIUS, HTTP, SCEP).

2. Authentication Workflow

In a production network, when connecting a supplicant (could be an IP phone, a PC or any other end user device) to the network, the authentication is done according to the following workflow:



1. An IEEE 802.1X supplicant client initiates a connection request to the network by sending an EAPoL Start message to the authenticator (LAN switch).
2. The authenticator sends an EAP Identity Request message to the supplicant.
3. The supplicant replies with an EAP Identity Response to the authenticator.

4. The authenticator forwards the EAP Identity Response message to the authentication server encapsulated in RADIUS protocol.
5. The authentication server sends an EAP-TLS Start message to the authenticator, while the authenticator forwards it to the supplicant in Layer 2.
6. The supplicant replies with an EAP-TLS Client Hello message to the authenticator, which forwards it to authentication server over TCP protocol.
7. The authentication server replies with an EAP-TLS Server Hello message and includes its own server certificate and requests for the supplicant's certificate.
8. The supplicant verifies the server certificate using the server public key, sends the client certificate to the server, and sends the cipher trust protocol set.
9. The server verifies the client certificate, confirms the cipher trust protocol set, and validates the client credentials.
10. TLS tunnel is established and sends an EAP Success or Fail message to the supplicant via the protected tunnel.

Based on the authentication server reply (Pass or Fail), the authenticator (LAN switch) enables the port connected to the supplicant.

This workflow is achieved by properly configuring the following entities:

- Certificate Authority (CA) Server – A trusted service signing the certificates
- A RADIUS based authentication server
- File server – Providing the phone its settings file
- LAN switch – The authenticator
- Phone - Supplicant

3. Certificate Authority Server

This document relates to Certificate Authority Server running on **Windows Server 2008 R2 Enterprise**, named AD CS – Active Directory Certification Services.

Notes:

- This section doesn't relate to Certificate Authority server on Windows Server 2003 or any other Microsoft Windows Server version than the one stated above.
- This section doesn't relate to Certificate Authority server on Linux.

1) Installation Pre-Requisite:

Windows Server 2008 R2 Enterprise must be installed, with the following roles:

- Active Directory Domain Services
- Web Server (IIS)

Note:

The person performing the activities described in this section must login to the server with administrator privileges.

2) Install Active Directory Certification Service

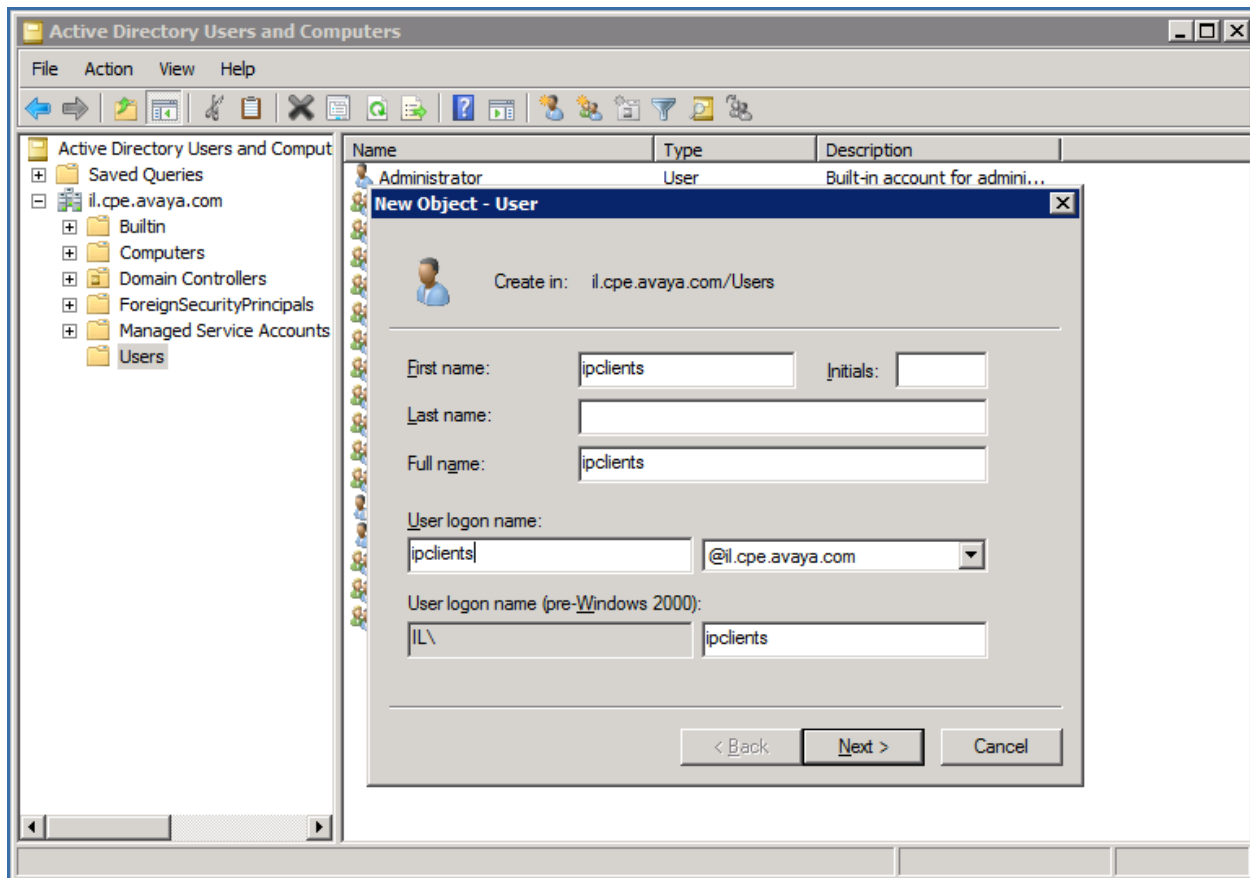
Step 1: Add a user into IIS_IUSRS group

This will be the user name under which the IP clients that access the Web Server for Network Device Enrollment. In our example the username will be "ipclients". To add the ipclients user, follow these steps:

Start Menu->Administrative Tools->Active Directory Users and Computers

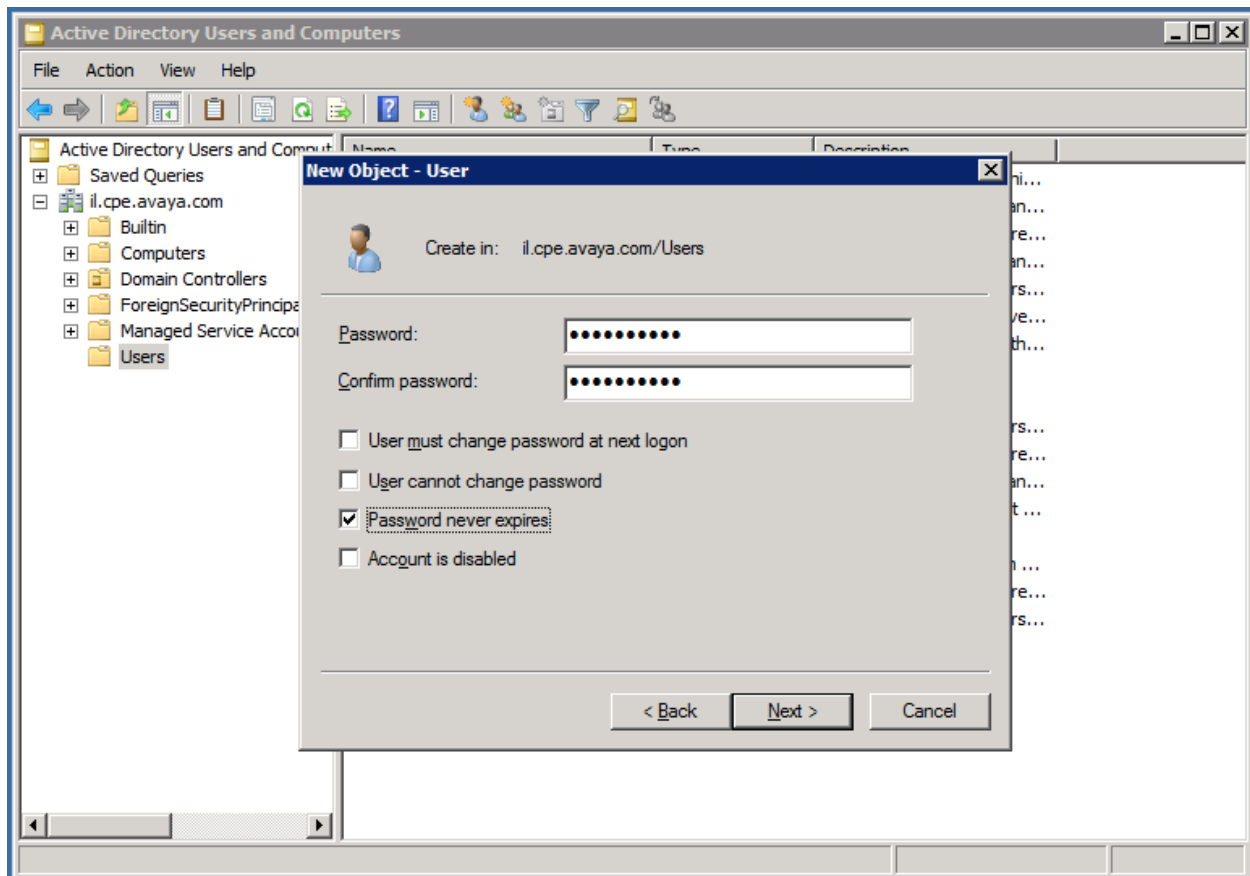
Right-click Users->New->User

User logon name: ipclients



Click **Next**.

The next screen is a password definition of the user. Give the user a password, and **uncheck User must change password at next logon** and check **Password never expires**.



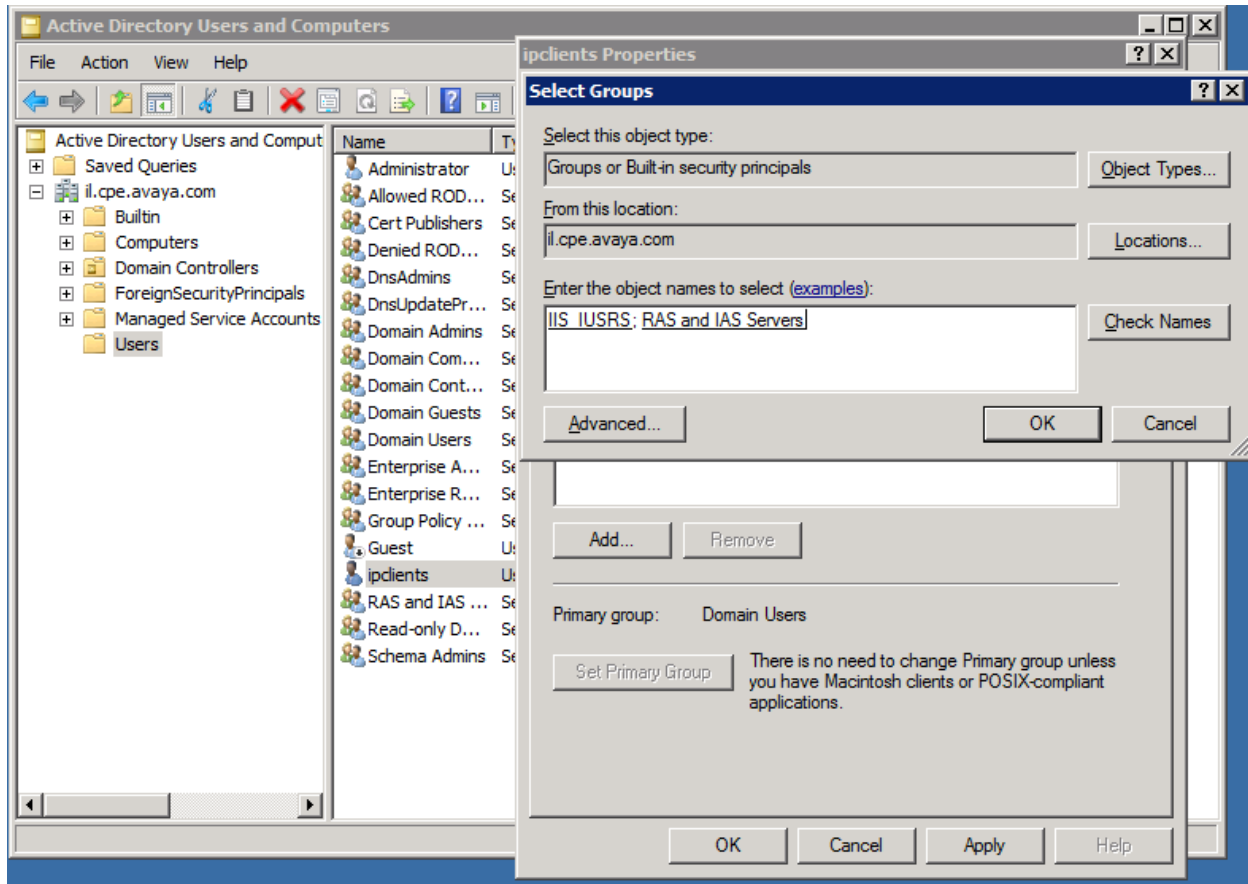
Click **Next**.

Click **Finish**.

Now assign the new added user to the IIS_IUSRS group:

Right-click user ipclients->Properties.
Click the **Member Of** tab, and then click **Add**.

In the appearing text box type:
IIS_IUSRS;RAS and IAS Servers



Click **OK**.

Click **OK**.

Now you can close the Active Directory Users and Computers window.

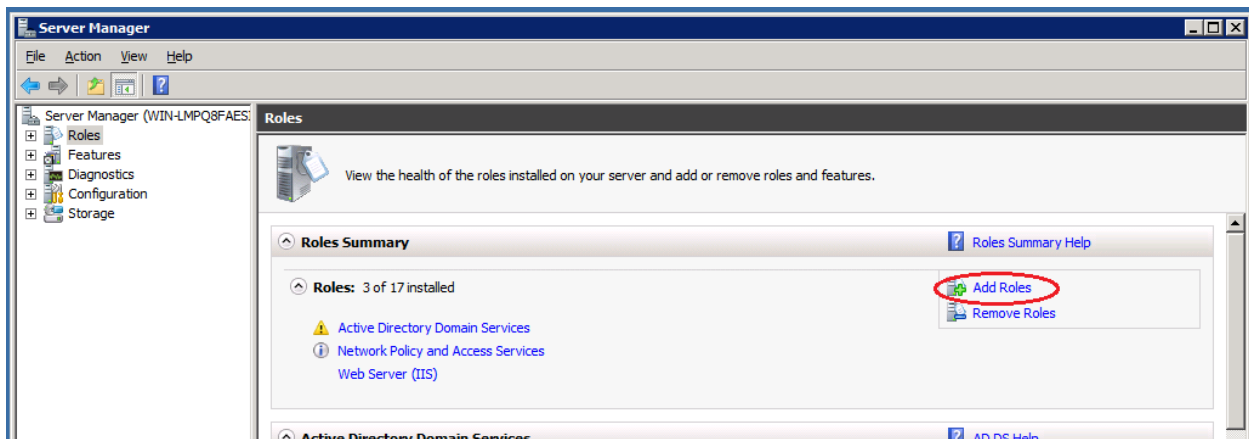
Step 2: Add Active Directory Certificate Services (AD CS)

Launch the **Server Manager** application by clicking its icon on the task bar:



(Or via the start menu: Start Menu->Administrative Tools->Server Manager)

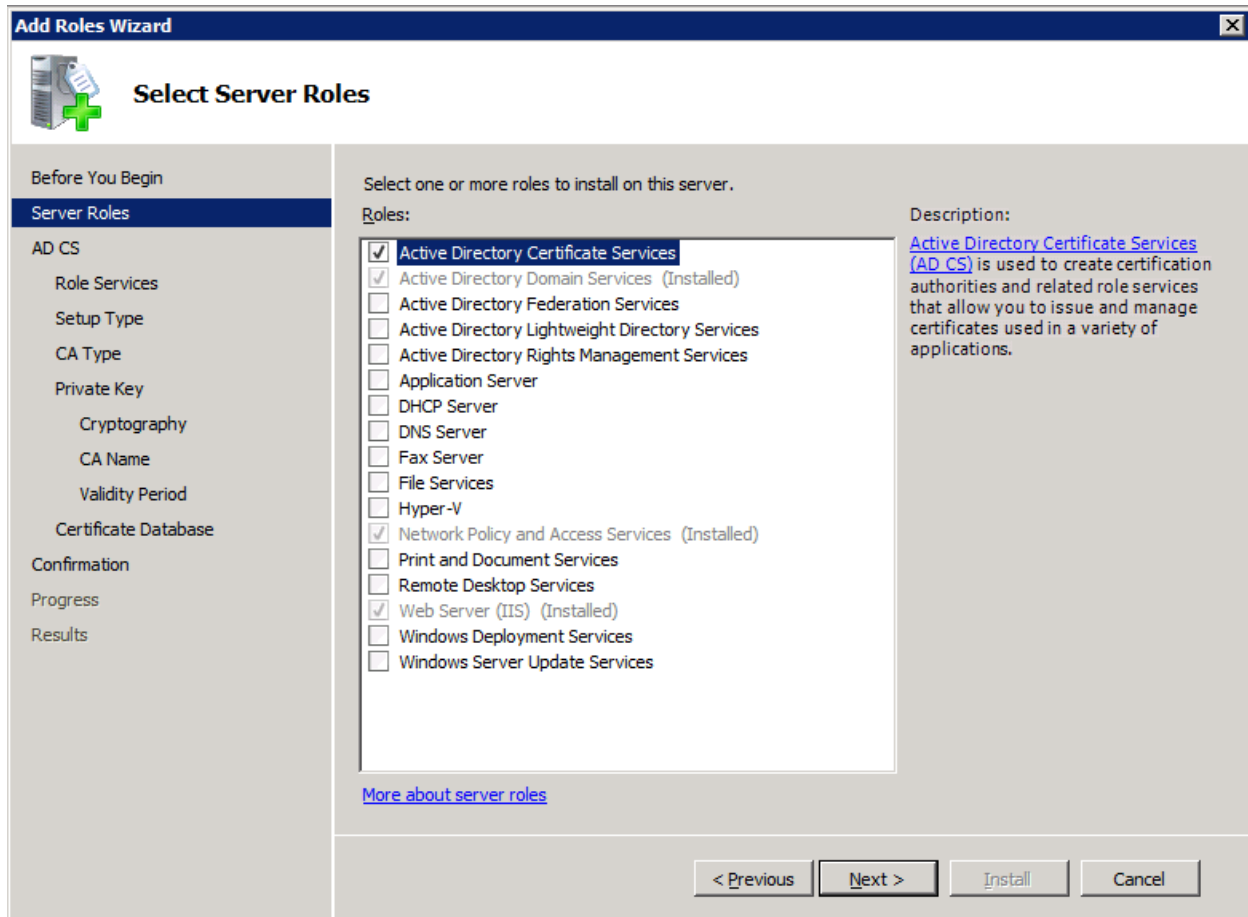
Navigate to the Server Roles and click **Add Roles**.



The Add Roles Wizard opens.

In the **Before You Begin** window, click **Next**.

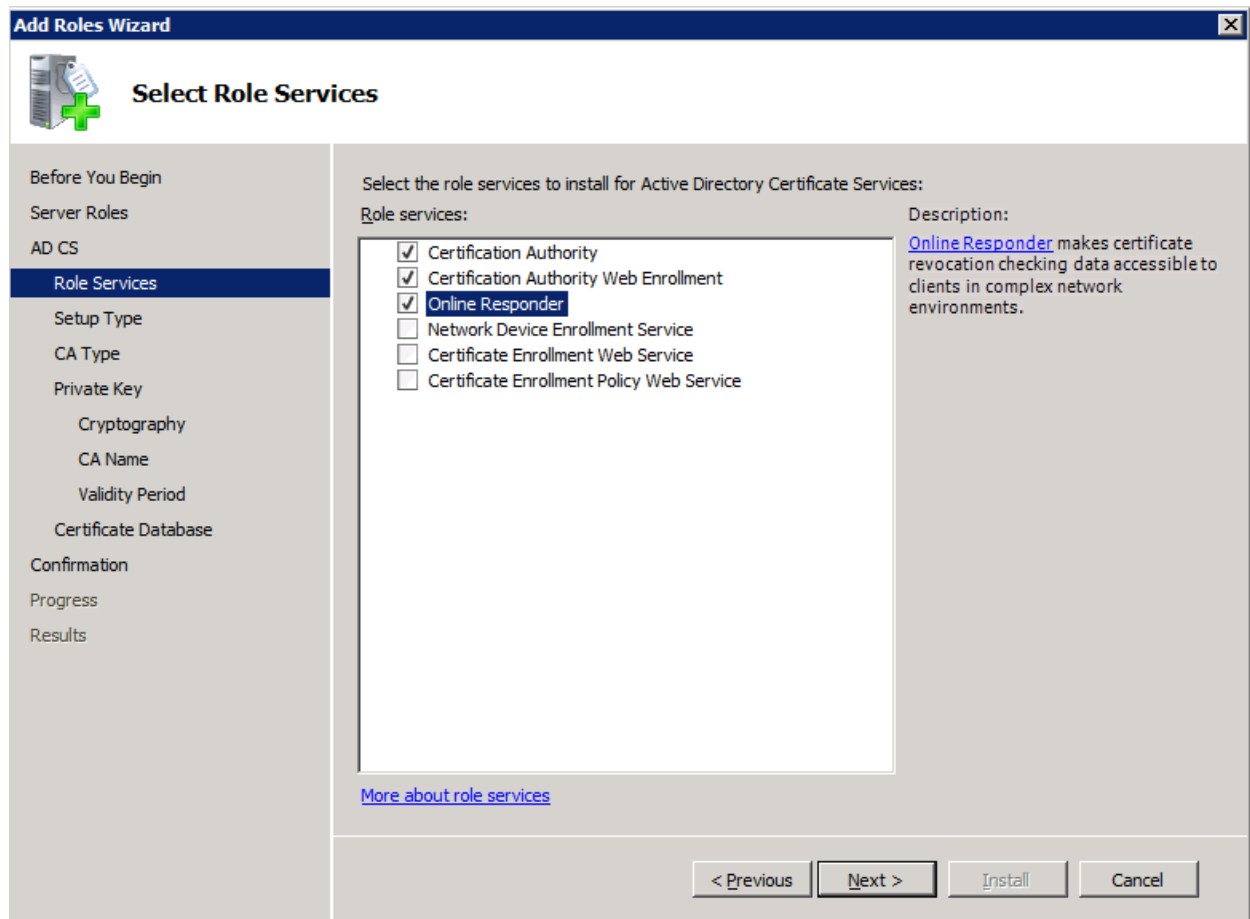
Select **Active Directory Certificate Services** in the Server Roles window, and then click **Next**.



The Add Roles Wizard is displayed. Click **Next** in the welcome window.

In the Select Roles Services window select the following roles:


- Certification Authority
- Certification Authority Web Enrollment
- Online Responder



Click **Next**.

In the Specify Setup Type window select **Enterprise** and click **Next**.

Add Roles Wizard

 **Specify Setup Type**

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

☒ **Enterprise**
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

☐ **Standalone**
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

[More about the differences between enterprise and standalone setup](#)

< Previous Next > Install Cancel

In the Specify CA Type window select **Root CA** and click **Next**.

The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard' and a close button. The window is divided into two main sections. On the left is a navigation pane with a tree view containing the following items: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type', 'CA Type' (which is highlighted with a blue background), 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. Above the 'Specify CA Type' title is an icon of a server with a green plus sign. The main content area on the right has a title 'Specify CA Type' and a paragraph explaining that a combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). It defines a root CA as one that issues its own self-signed certificate and a subordinate CA as one that receives its certificate from another CA. Below this text are two radio button options: 'Root CA' (which is selected) and 'Subordinate CA'. Each option has a descriptive sentence below it. At the bottom of the main content area is a blue hyperlink that reads 'More about public key infrastructure (PKI)'. At the very bottom of the window is a row of four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Add Roles Wizard

Specify CA Type

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

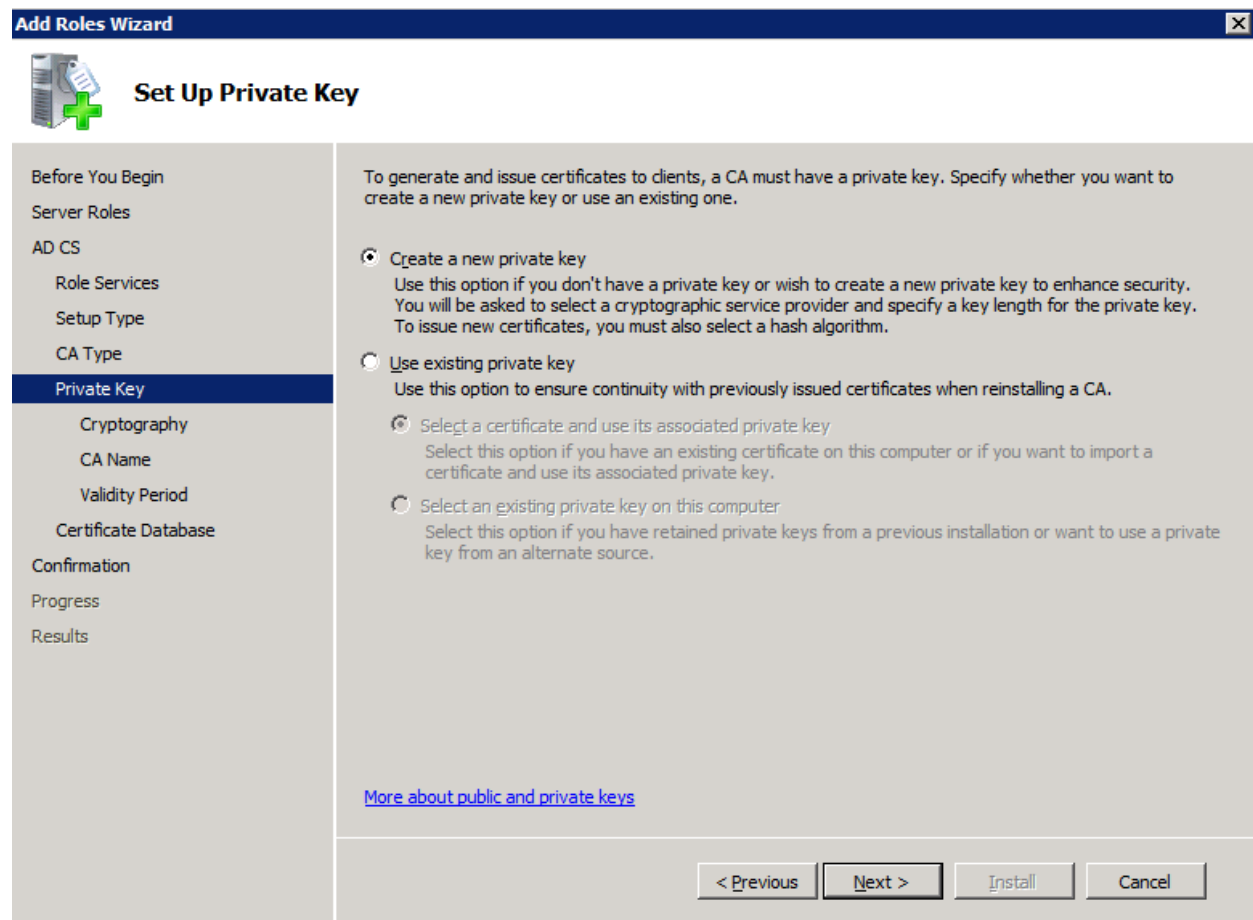
☒ Root CA
Select this option if you are installing the first or only certification authority in a public key infrastructure.

☐ Subordinate CA
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

[More about public key infrastructure \(PKI\)](#)

< Previous Next > Install Cancel

In the Set Up Private Key window select **Create a new private key** and click **Next**.



In the next screen you will have to configure the cryptography for the CA to meet your organization security standards and policy.

Select the appropriate cryptographic service provider (CSP), the key length and the desired hash algorithm.

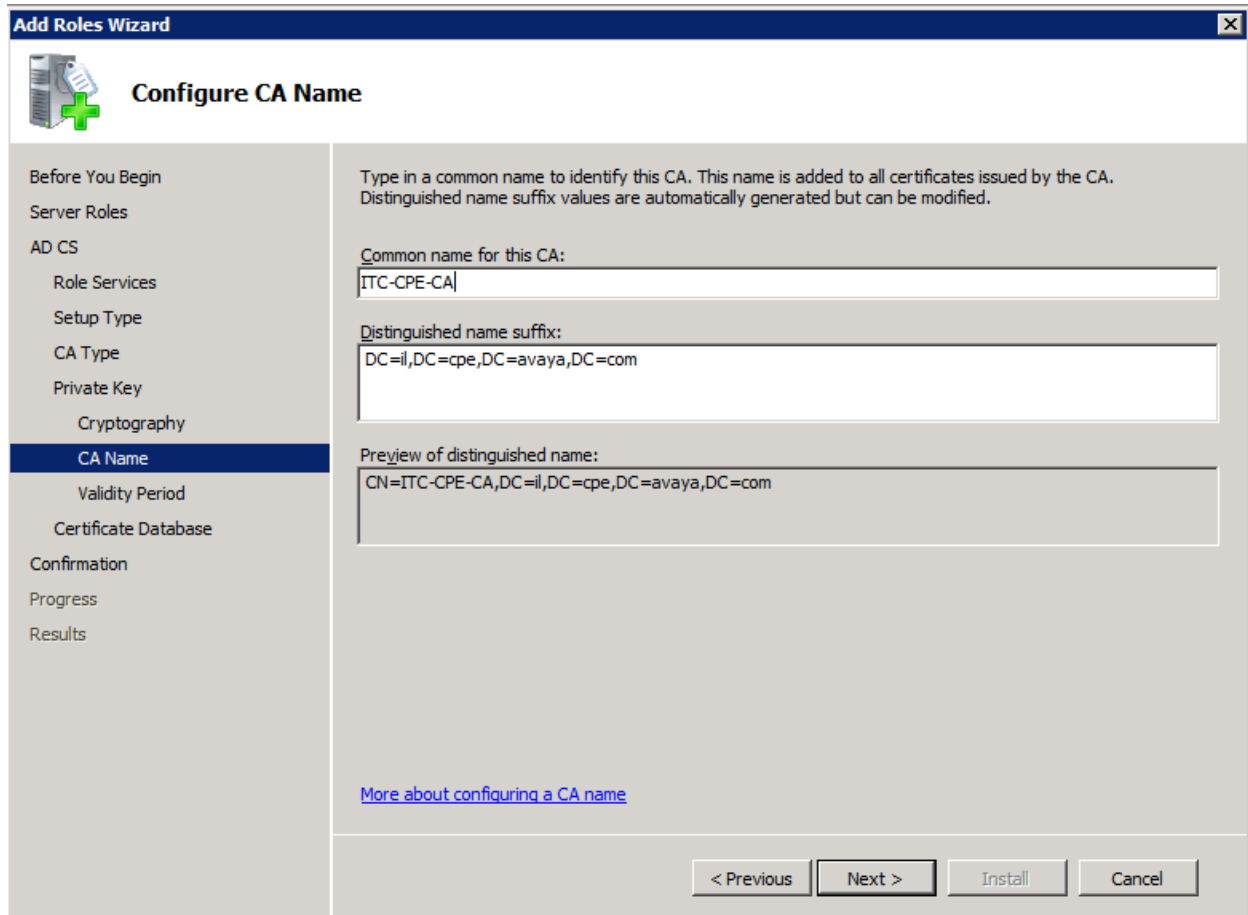
Selecting a higher value for key length will result in stronger security, but increases the time needed to complete signing operations.

When done, click **Next**.

Configure the CA Name.

This name is added to all certificates issued by the CA.

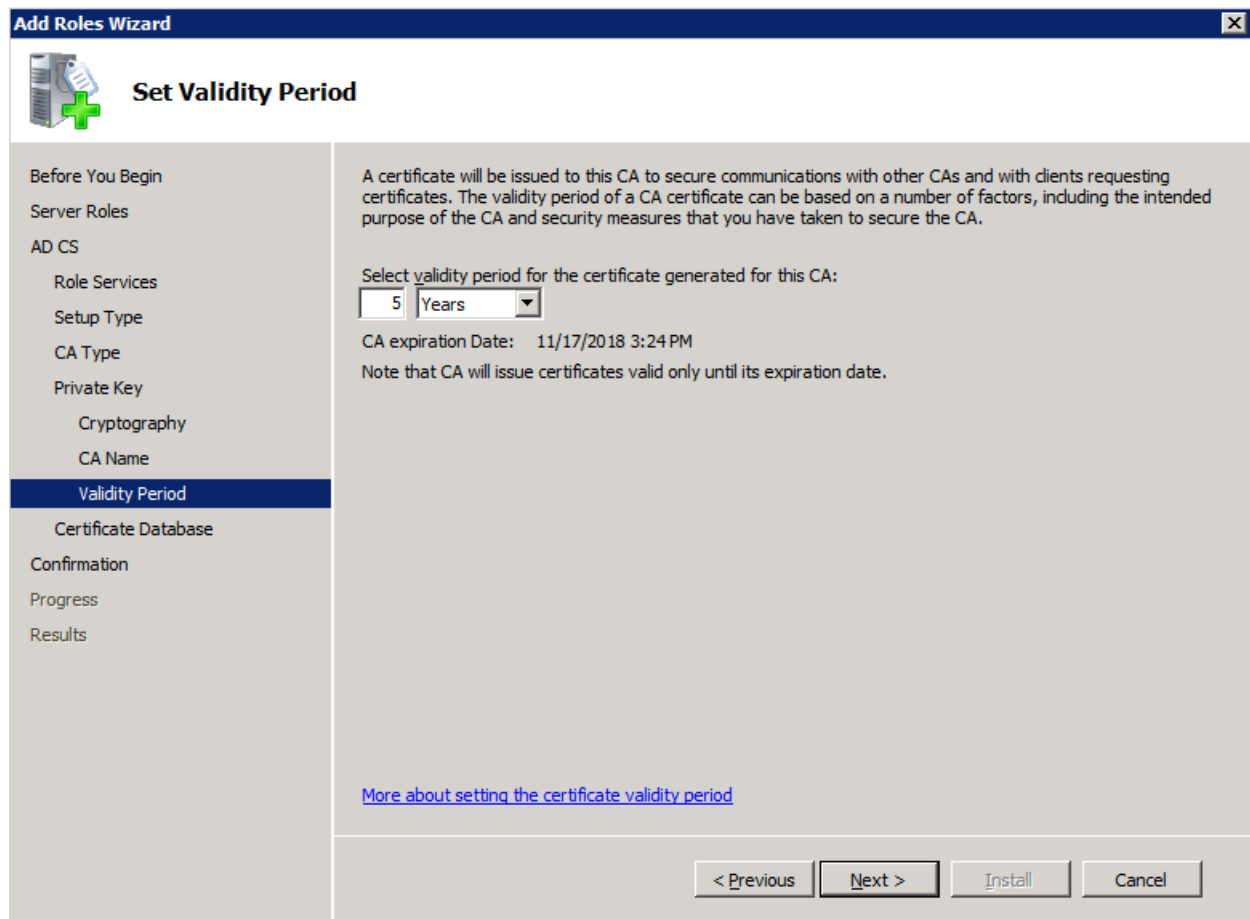
The screen below is just an example. Make sure you enter values according to your organization.



The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard' and a close button. The main window has a green plus icon and the title 'Configure CA Name'. On the left is a navigation pane with the following items: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name' (highlighted), 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main area contains the following text: 'Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.' Below this are three text boxes: 'Common name for this CA:' with the value 'ITC-CPE-CA', 'Distinguished name suffix:' with the value 'DC=il,DC=cpe,DC=avaya,DC=com', and 'Preview of distinguished name:' with the value 'CN=ITC-CPE-CA,DC=il,DC=cpe,DC=avaya,DC=com'. At the bottom right are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about configuring a CA name' is located above the 'Next >' button.

When done, click **Next**.

Set Validity Period for the certificate generated for this CA.



The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard' and a close button. The main window has a left-hand navigation pane and a right-hand content area. The navigation pane lists the following steps: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period' (which is highlighted with a blue background), 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The 'Set Validity Period' step is active in the content area. It contains the following text: 'A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.' Below this is a label 'Select validity period for the certificate generated for this CA:' followed by a text box containing the number '5' and a dropdown menu set to 'Years'. Further down, it shows 'CA expiration Date: 11/17/2018 3:24 PM' and a note: 'Note that CA will issue certificates valid only until its expiration date.' At the bottom of the content area is a blue hyperlink: 'More about setting the certificate validity period'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Add Roles Wizard

Set Validity Period

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.

Select validity period for the certificate generated for this CA:

5 Years

CA expiration Date: 11/17/2018 3:24 PM
Note that CA will issue certificates valid only until its expiration date.

[More about setting the certificate validity period](#)

< Previous Next > Install Cancel

Then click **Next**.

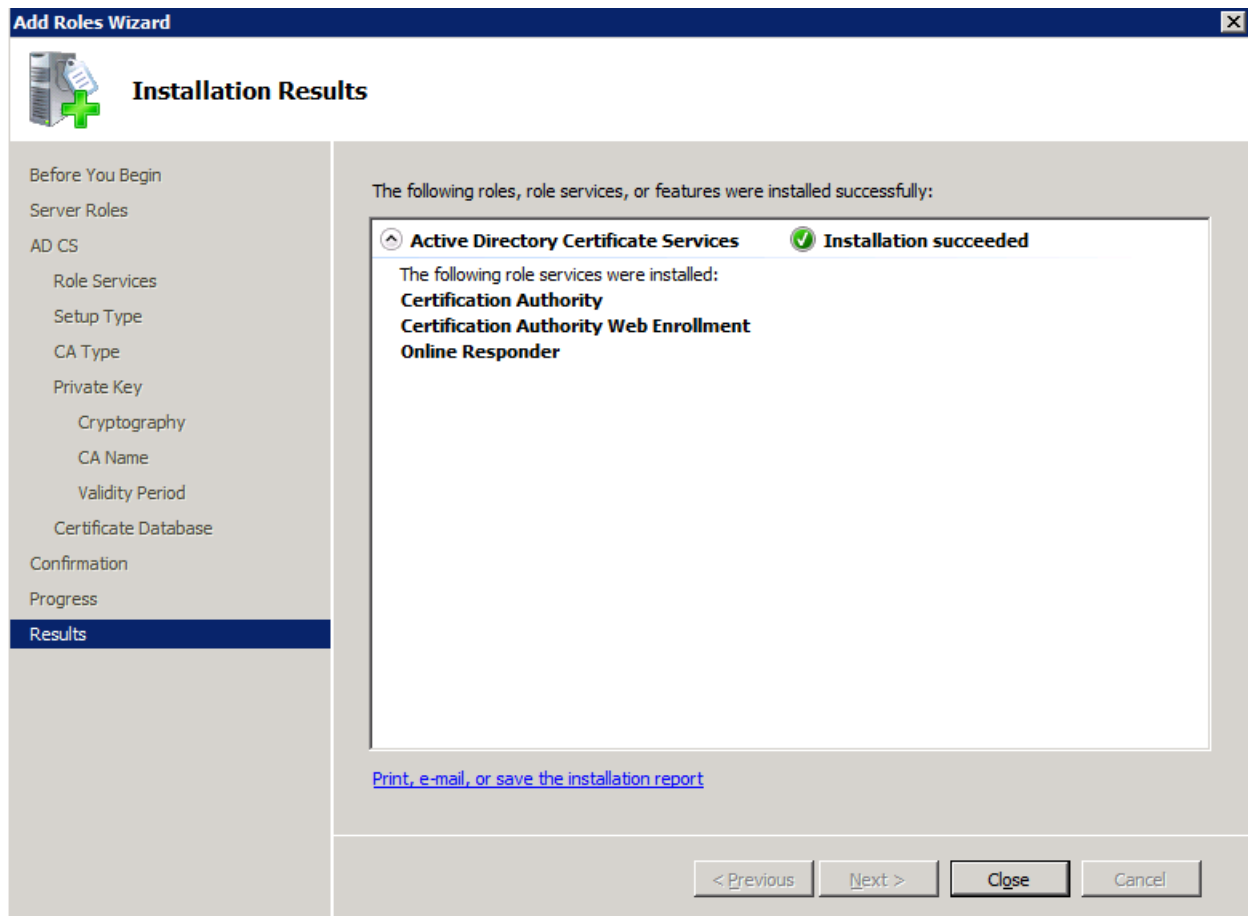
Configure Certificate Database location and database log location on the server.

The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard' and a close button. The main title is 'Configure Certificate Database' with a green plus icon. The left sidebar lists the wizard steps: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database' (highlighted), 'Confirmation', 'Progress', and 'Results'. The main area contains the following text: 'The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.' Below this, there are two text boxes. The first is labeled 'Certificate database location:' and contains 'C:\Windows\system32\CertLog', with a 'Browse...' button to its right. The second is labeled 'Certificate database log location:' and also contains 'C:\Windows\system32\CertLog', with a 'Browse...' button to its right. A checkbox labeled 'Use existing certificate database from previous installation at this location' is present between the two text boxes. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

When done, click **Next..**

After the confirmation screen appears, click **Install.**

When installation is done the Installation Results screen will appear with Installation Succeeded message.



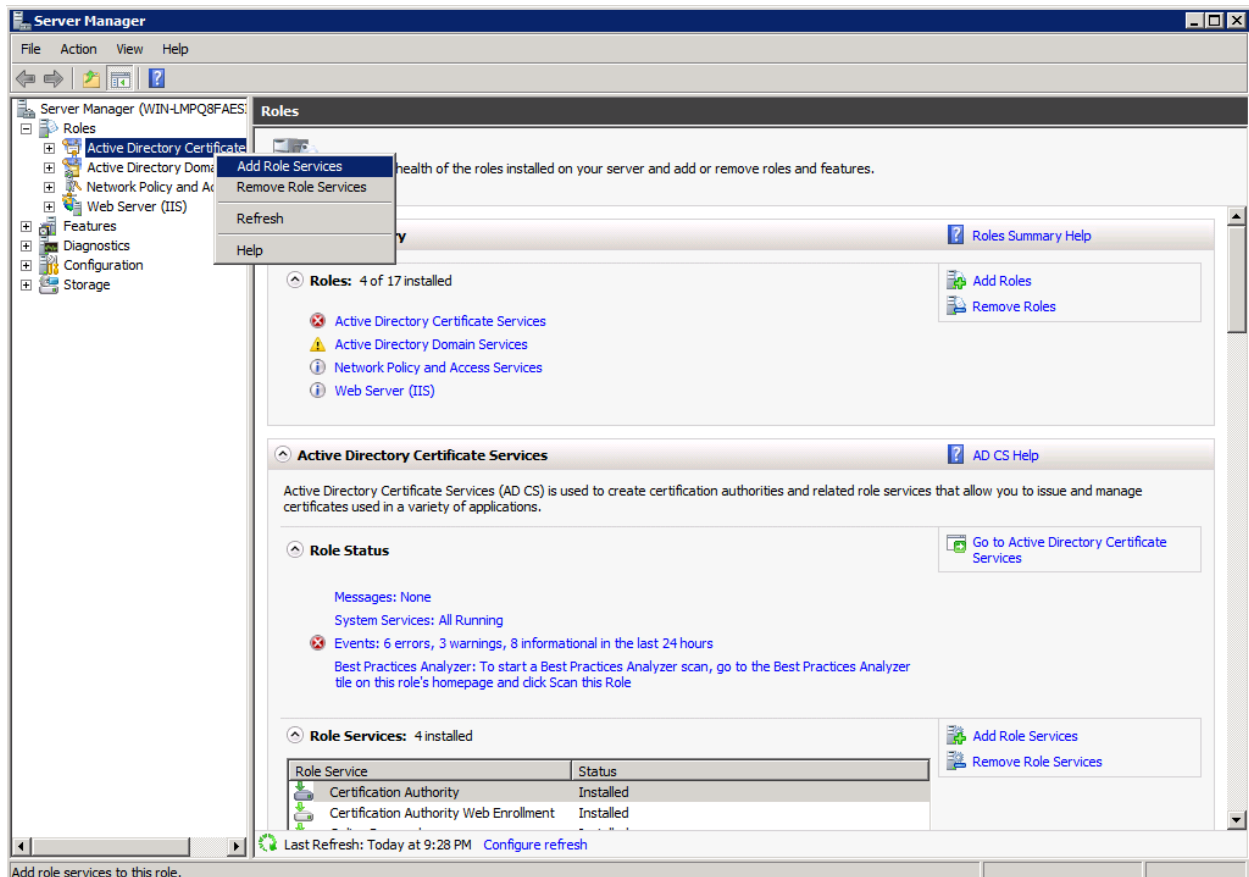
Click **Close**.

Step 3: Add Network Device Enrollment Service to the AD CS

Launch the **Server Manager** and navigate to the Server Roles.

Right-click **Active Directory Certificate Services**.

Select **Add Role Services**.



The Select Role Services window will appear.

Check **Network Device Enrollment Service**.

Add Role Services

Select Role Services

Role Services

- User Account
- RA Information
- Cryptography
- Confirmation
- Progress
- Results

Select the role services to install for Active Directory Certificate Services:

Role services:

- ☒ Certification Authority (Installed)
- ☒ Certification Authority Web Enrollment (Installed)
- ☒ Online Responder (Installed)
- ☒ **Network Device Enrollment Service**
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

Description:

[Network Device Enrollment Service](#) makes it possible to issue and manage certificates for routers and other network devices that do not have network accounts.

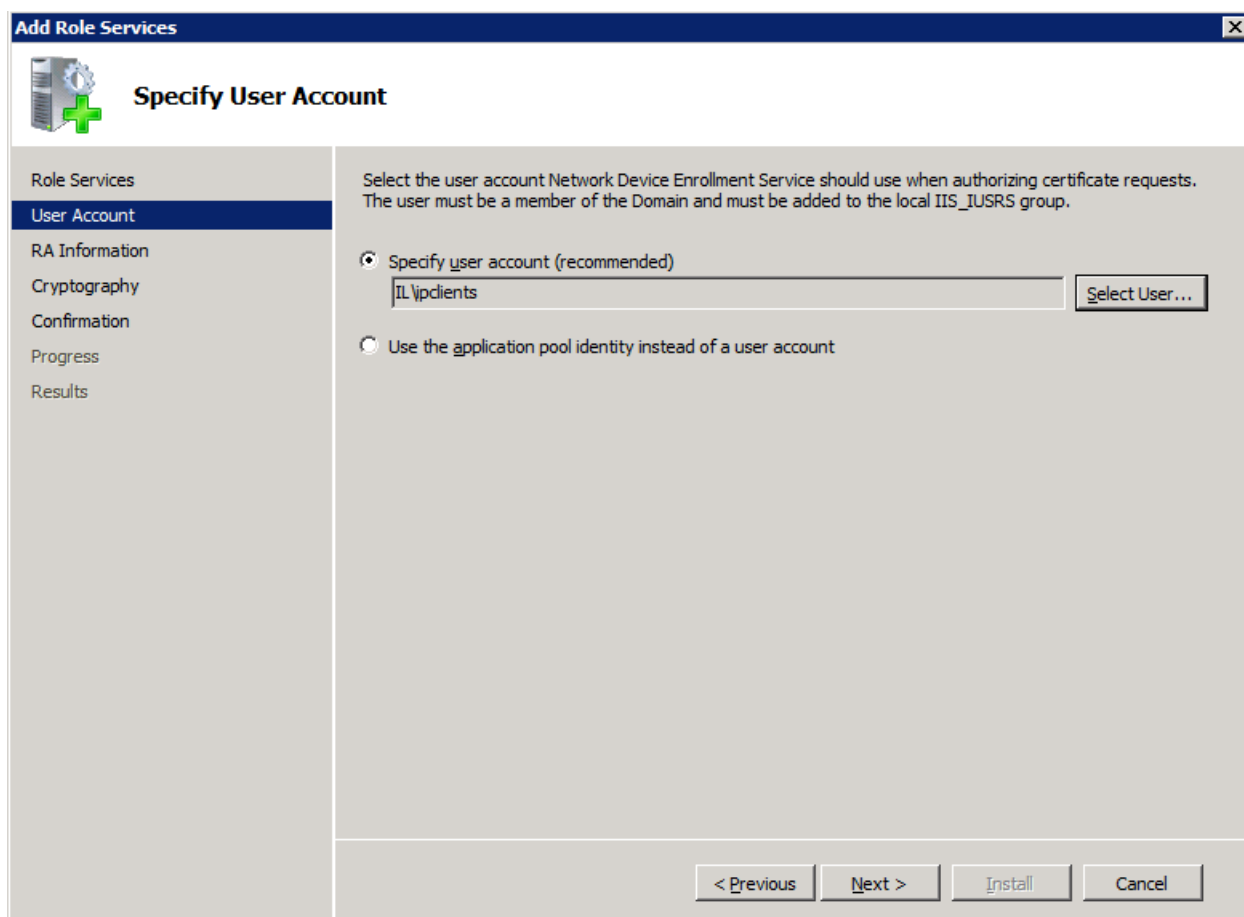
[More about role services](#)

< Previous **Next >** Install Cancel

Click **Next**.

Specify User Account for Network Device Enrollment. This is the account which was defined in step 1 above. Click **Select User** and enter the user name and the password as assigned in step 1.

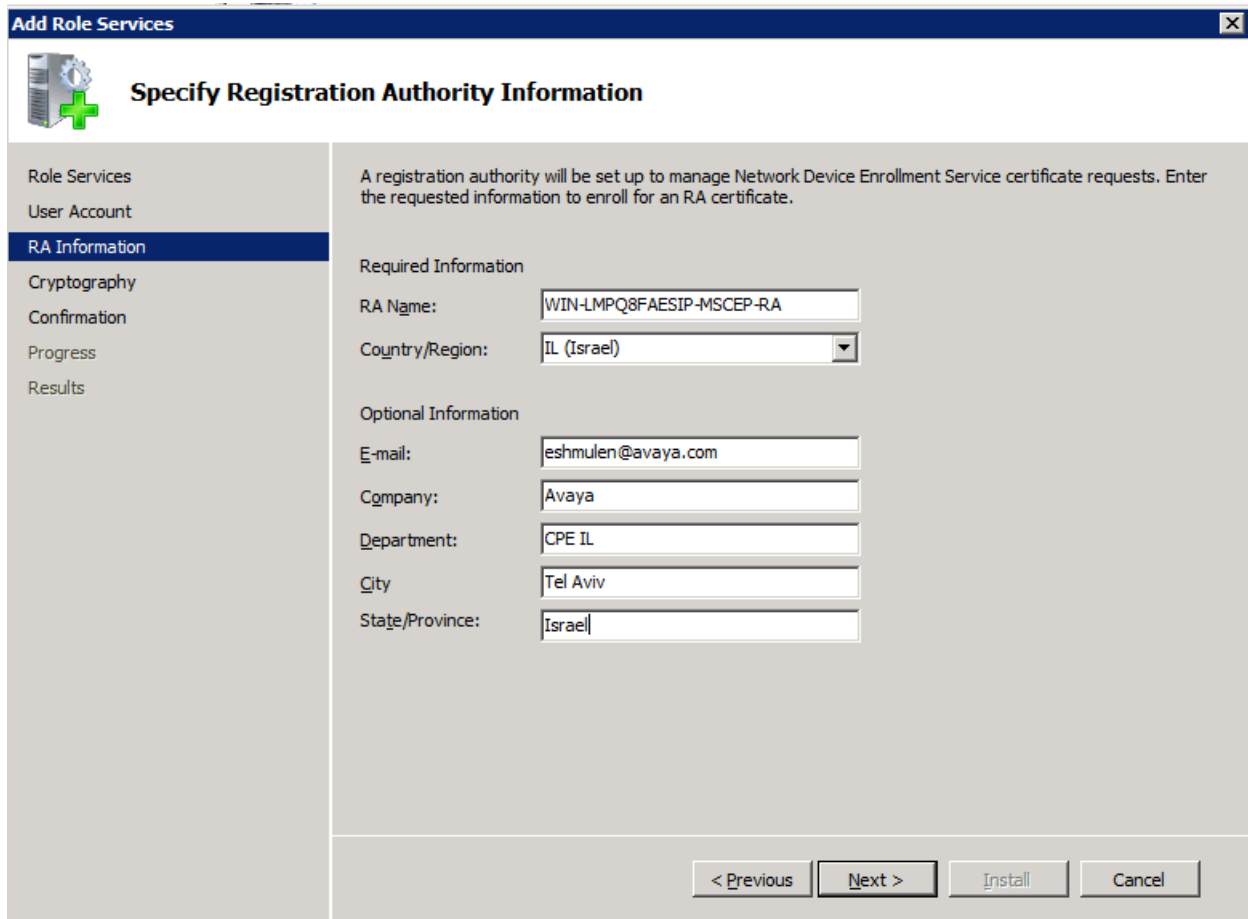
In our example the user is ipclients.



The screenshot shows the 'Add Role Services' wizard window. The title bar reads 'Add Role Services'. The left sidebar contains a tree view with the following items: 'Role Services', 'User Account' (highlighted), 'RA Information', 'Cryptography', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'Specify User Account' and contains the following text: 'Select the user account Network Device Enrollment Service should use when authorizing certificate requests. The user must be a member of the Domain and must be added to the local IIS_IUSRS group.' There are two radio button options: 'Specify user account (recommended)' (which is selected) and 'Use the application pool identity instead of a user account'. Below the first option is a text box containing 'IL\ipclients' and a 'Select User...' button. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Click **Next**.

Specify Registration Authority Information which will be setup to manage Network Device Enrollment Service certificate requests.



The screenshot shows a Windows-style dialog box titled "Add Role Services" with a close button in the top right corner. On the left is a vertical navigation pane with icons and labels: "Role Services" (gear icon), "User Account" (person icon), "RA Information" (highlighted with a blue bar and a plus icon), "Cryptography" (key icon), "Confirmation" (checkmark icon), "Progress" (progress bar icon), and "Results" (document icon). The main area is titled "Specify Registration Authority Information" and contains a descriptive paragraph: "A registration authority will be set up to manage Network Device Enrollment Service certificate requests. Enter the requested information to enroll for an RA certificate." Below this, there are two sections: "Required Information" and "Optional Information". The "Required Information" section has two fields: "RA Name:" with the text "WIN-LMPQ8FAESIP-MSCEP-RA" and "Country/Region:" with a dropdown menu showing "IL (Israel)". The "Optional Information" section has five fields: "E-mail:" with "eshmullen@avaya.com", "Company:" with "Avaya", "Department:" with "CPE IL", "City:" with "Tel Aviv", and "State/Province:" with "Israel". At the bottom right of the main area are four buttons: "< Previous", "Next >", "Install", and "Cancel".

Add Role Services

Specify Registration Authority Information

A registration authority will be set up to manage Network Device Enrollment Service certificate requests. Enter the requested information to enroll for an RA certificate.

Required Information

RA Name: WIN-LMPQ8FAESIP-MSCEP-RA

Country/Region: IL (Israel)

Optional Information

E-mail: eshmullen@avaya.com

Company: Avaya

Department: CPE IL

City: Tel Aviv

State/Province: Israel

< Previous Next > Install Cancel

Click **Next**.

Configure Cryptography for Registration Authority, which will be used for the signature key and the encryption key to sign and encrypt communication between the device and the CA.

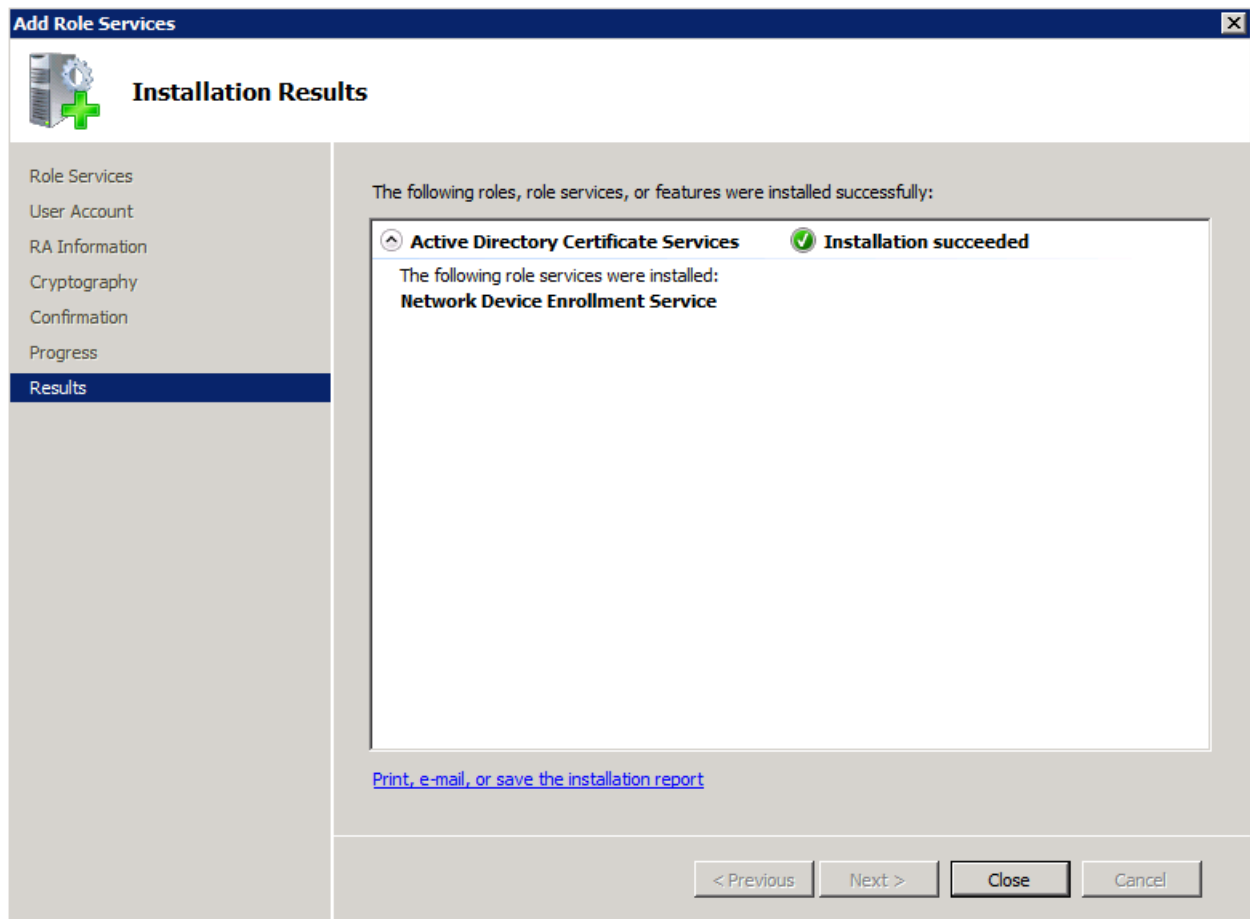
Select the parameters that fit your organization policy.

The screenshot shows the 'Add Role Services' wizard window. The title bar says 'Add Role Services'. The main heading is 'Configure Cryptography for Registration Authority'. On the left is a navigation pane with the following items: 'Role Services', 'User Account', 'RA Information', 'Cryptography' (which is selected and highlighted in blue), 'Confirmation', 'Progress', and 'Results'. The main content area has the following text: 'To configure cryptography, you have to select cryptographic service providers and key lengths for the signature key and the encryption key used to sign and encrypt communications between the device and the CA.' Below this, it says 'Signature key is used to avoid repetition of communication between the CA and the RA.' Then there are two dropdown menus: 'Signature key CSP:' with 'Microsoft Strong Cryptographic Provider' selected, and 'Key character length:' with '2048' selected. Below that, it says 'Encryption key is used for secure communication between the RA and the network device.' Then there are two more dropdown menus: 'Encryption key CSP:' with 'Microsoft Strong Cryptographic Provider' selected, and 'Key character length:' with '2048' selected. At the bottom left of the main content area is a blue hyperlink: 'More about signature and encryption keys'. At the bottom right are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

When done, click **Next**.

Confirm installation selections and click **Install**.

After installation is complete, make sure Installation succeeded message displayed.



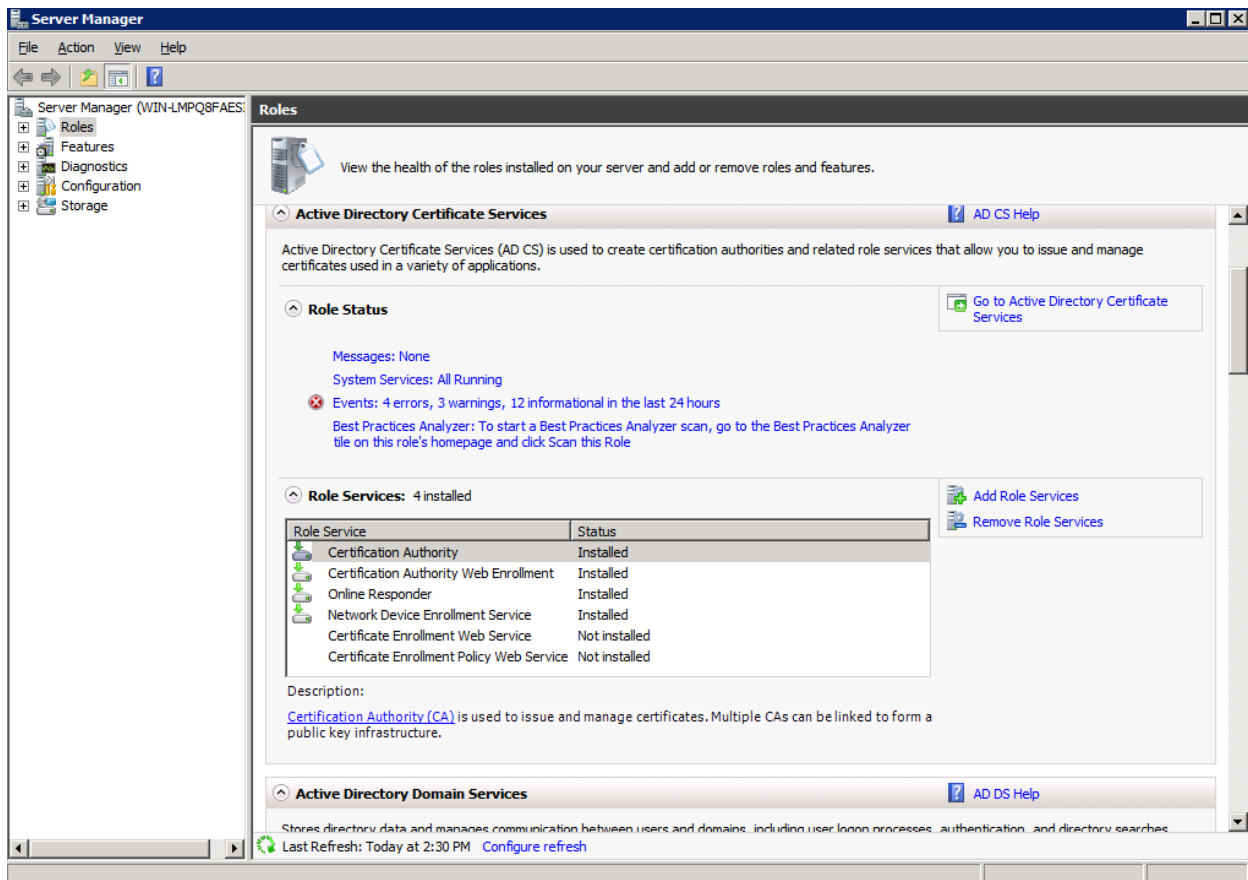
Click **Close**.

Step 4: Verify Four Role Services Have Been Installed in AD CS Role

By now the following four roles should have been installed in the AD CS role:

- Certificate Authority
- Certificate Authority Web Enrollment
- Online Responder
- Network Device Enrollment Service

For verification, launch the Server Manager and click Roles. Then scroll down to the Active Directory Certificate Service section. You should see the four above services as Installed.



If one of these services doesn't appear to be installed then make sure to complete previous steps 2-3.

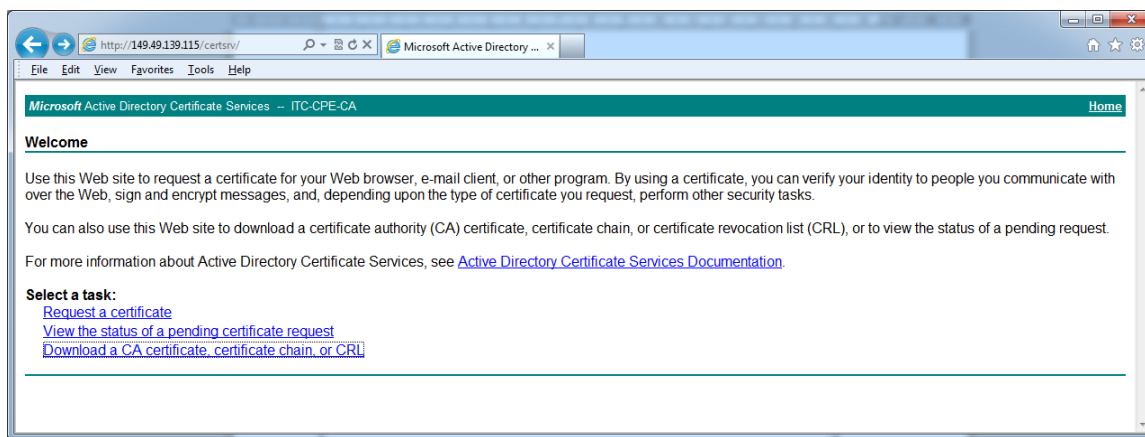
3) Export the Root Certificate from the AD CS

Open a Web Browser and go to the following URL:

http://<server_ip_address>/certsrv

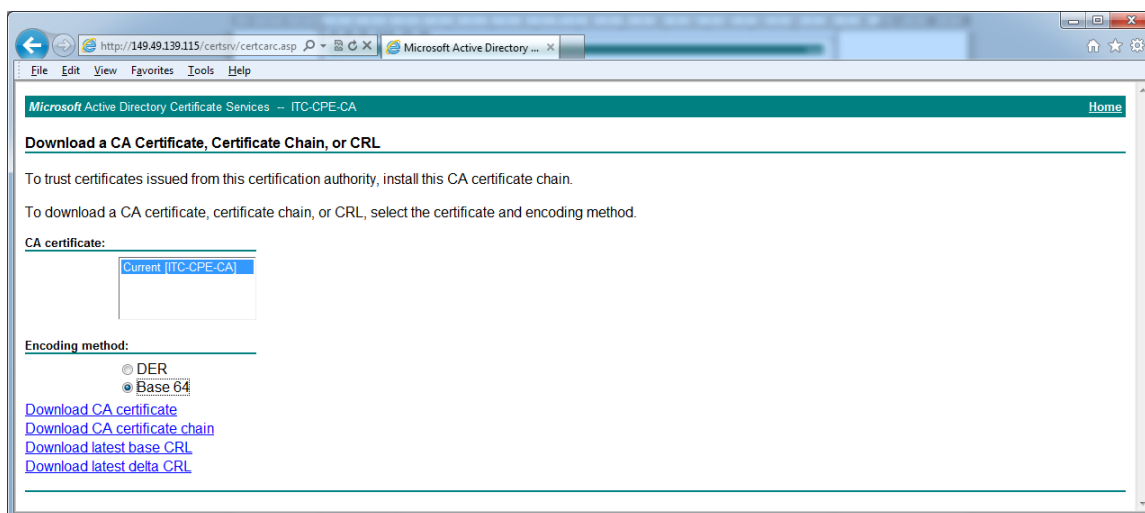
When prompted for user/password, enter the ipclients user credentials.

Click **Download a CA certificate, certificate chain, or CRL**.



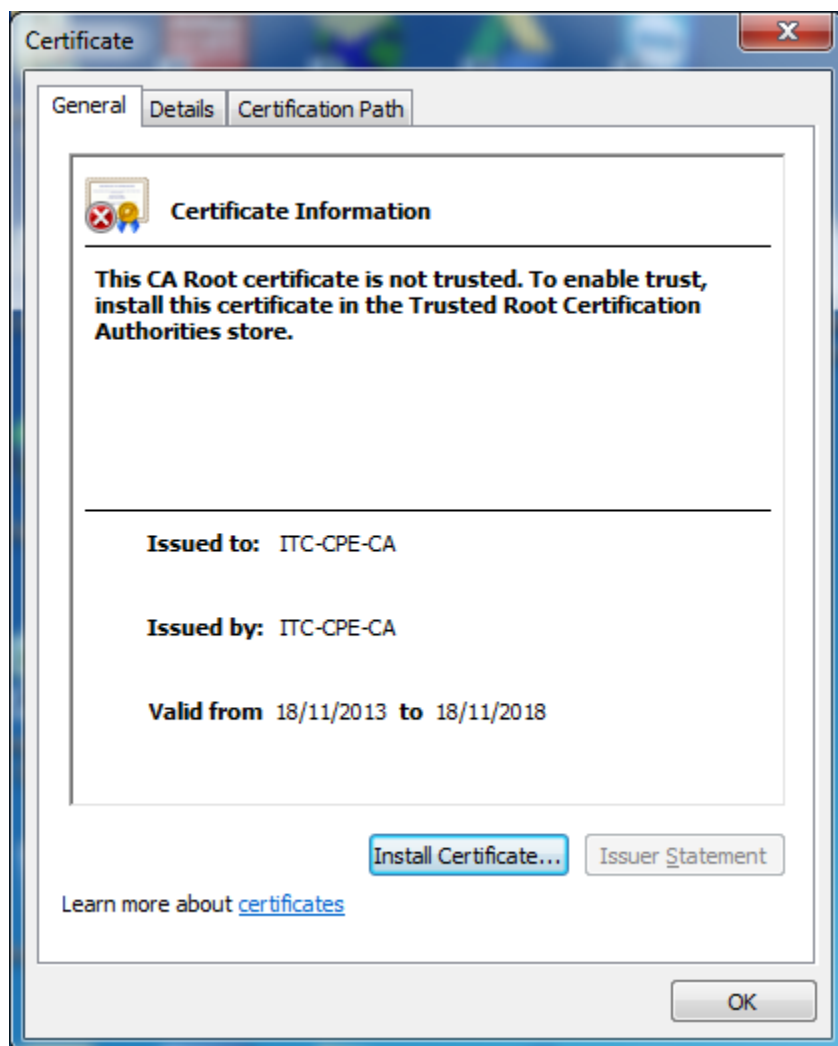
Select **Base 64** as the Encoding Method.

Click **Download CA certificate** and save it as a file on your local machine. Make sure you save it with .cer extension.



4) Verify Details of the Root Certificate

You can view the details of the downloaded certificate on any Windows PC by double-clicking on the previously downloaded .cer certificate file.



Click the Details tab to see the full certificate details.

By viewing the certificate details you can assure the certificate is valid and built with the desired characteristics.

4. RADIUS Server

The authentication function is performed by the RADIUS server - the authentication server. Its purpose is to authenticate the supplicants and grant or deny their access to the network resources. It has to hold the proper certificate so that the supplicant will be able to validate that it is being authenticated by a trusted authenticator.

There are many authentication servers that support RADIUS protocol out there. In this document we will describe how to use **Microsoft Network Policy Server (NPS)**.

1) Installation Pre-Requisite:

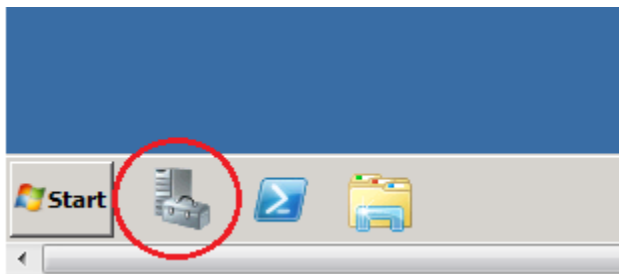
Windows Server 2008 R2 Enterprise must be installed.

Note:

The person performing the activities described in this section must login to the server with administrator privileges.

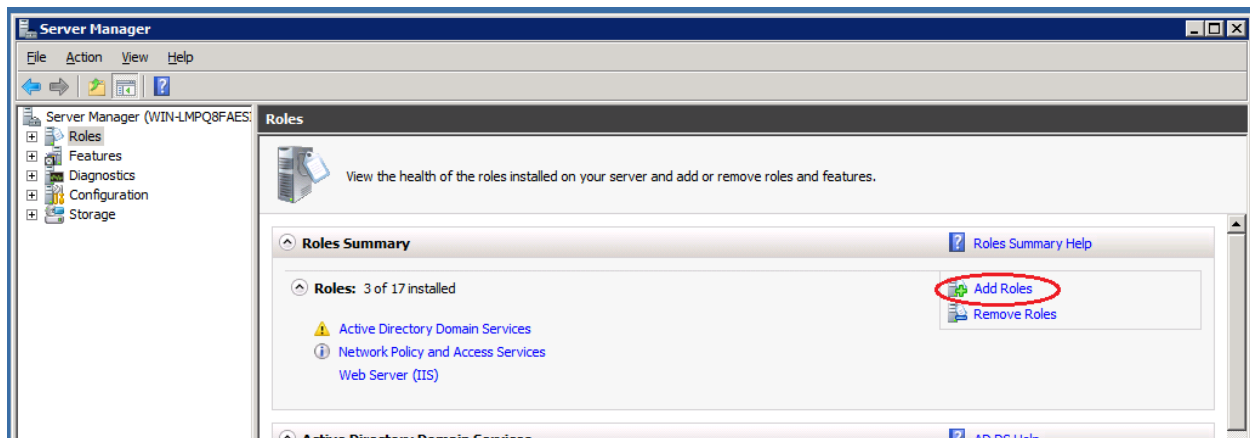
2) NPS Installation:

Launch the Server Manager application by clicking its icon on the task bar:



(Or via the start menu: Start Menu->Administrative Tools->Server Manager)

Navigate to the Server Roles and click Add Roles.

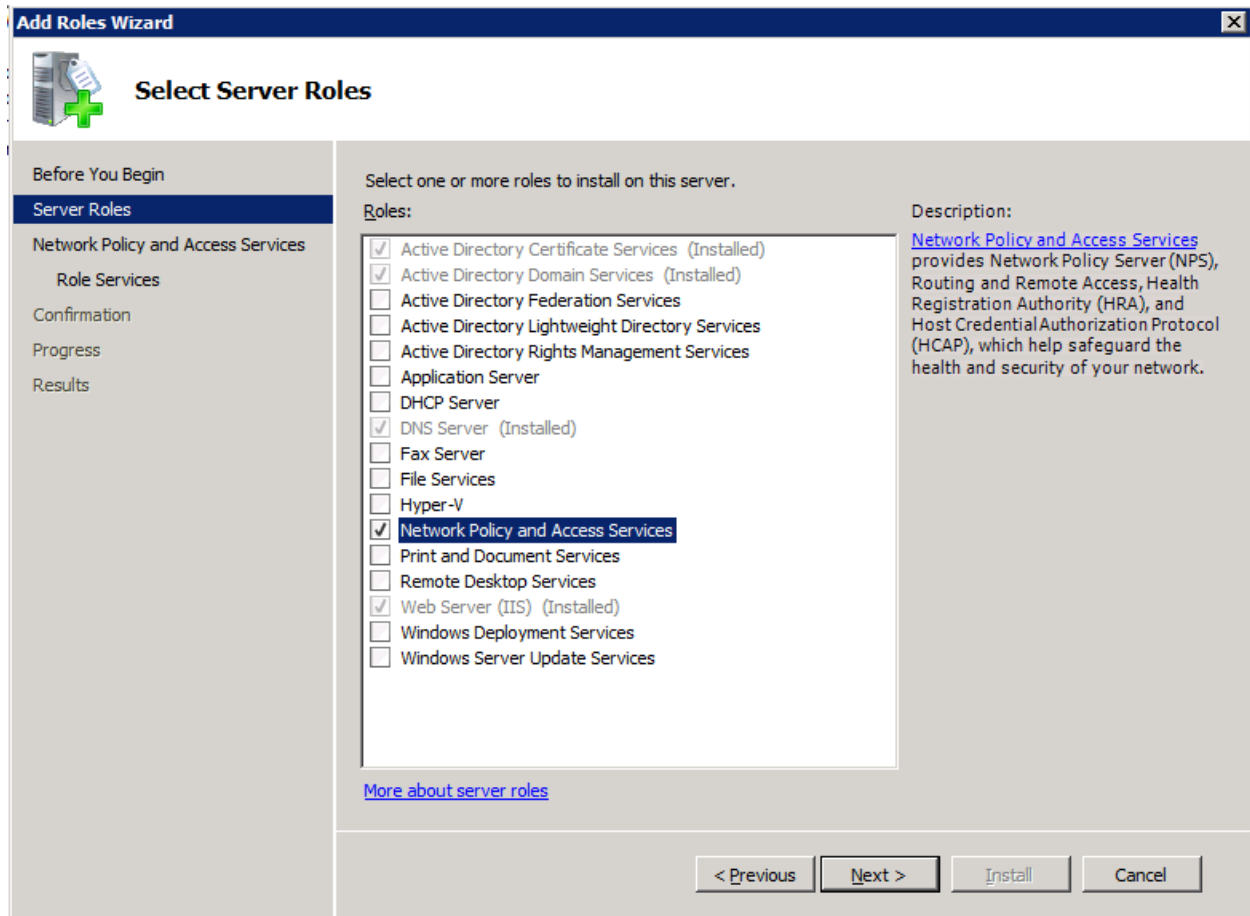


The **Add Roles Wizard** opens.

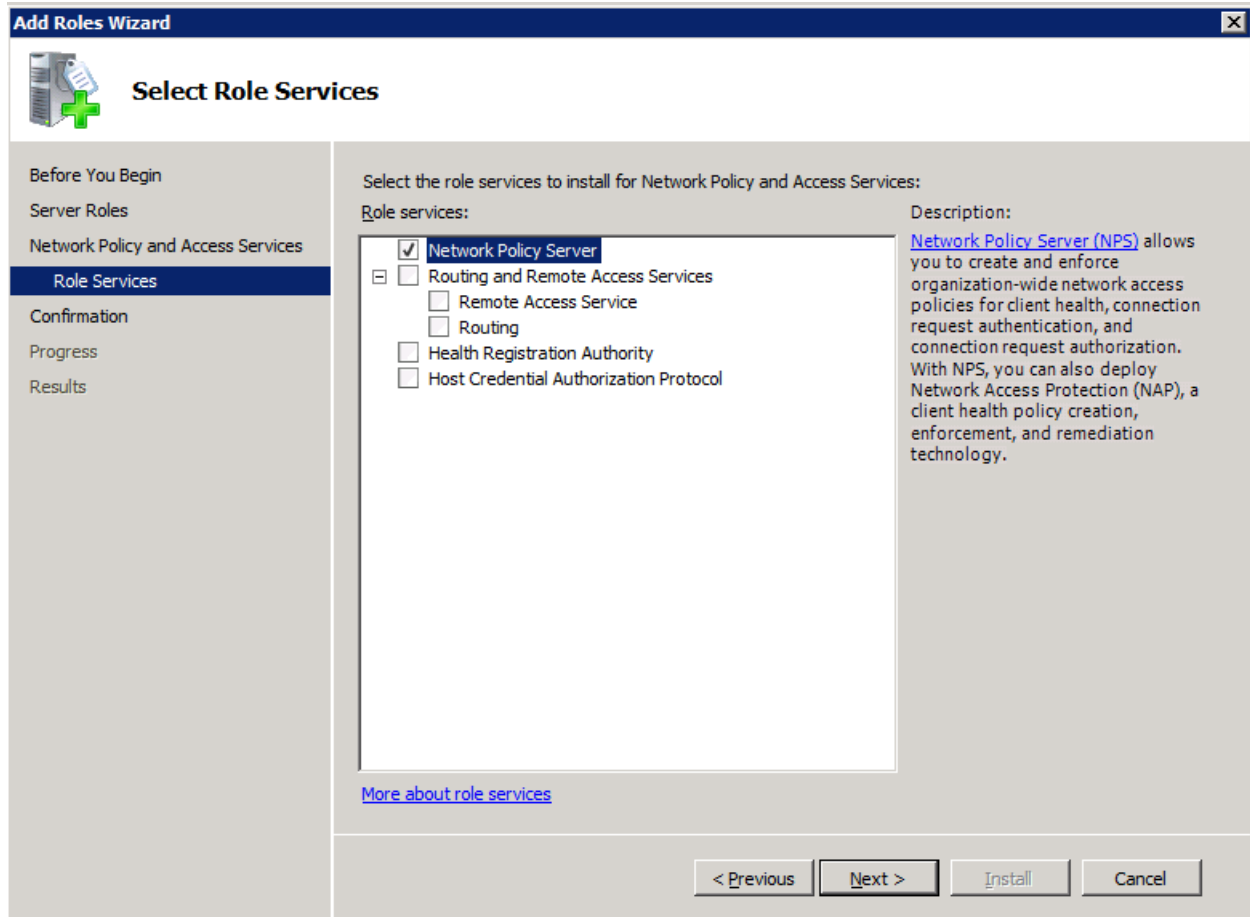
In **Before You Begin**, click **Next**.

In **Select Server Roles**, in **Roles**, select **Network Policy and Access Services**, and then click **Next**.

In **Network Policy and Access Services**, click **Next**.



In **Select Role Services**, in **Role Services**, select **Network Policy Server**, and then click **Next**.



In **Confirm Installation Selections**, click **Install**.

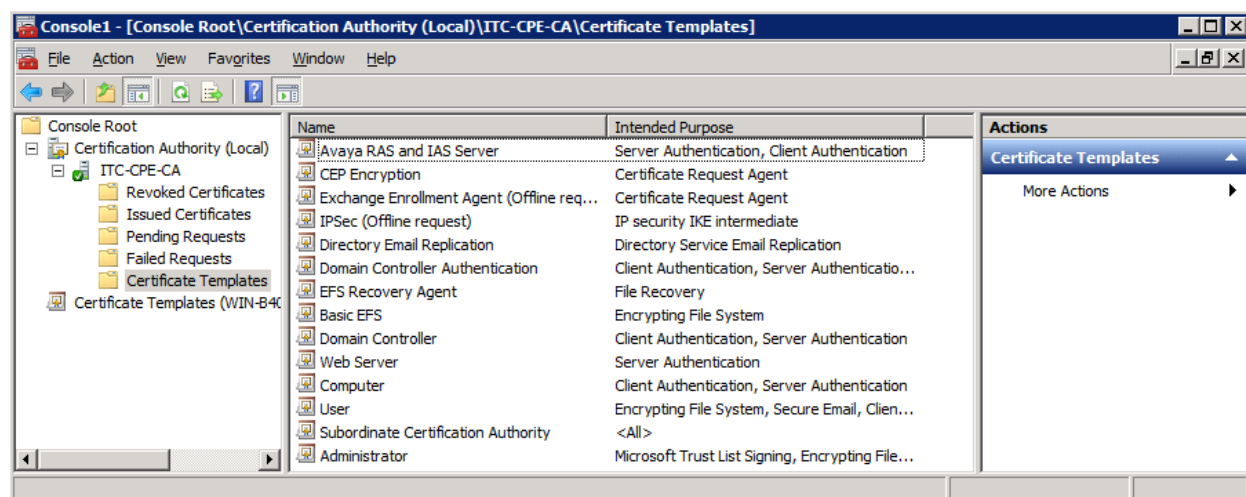
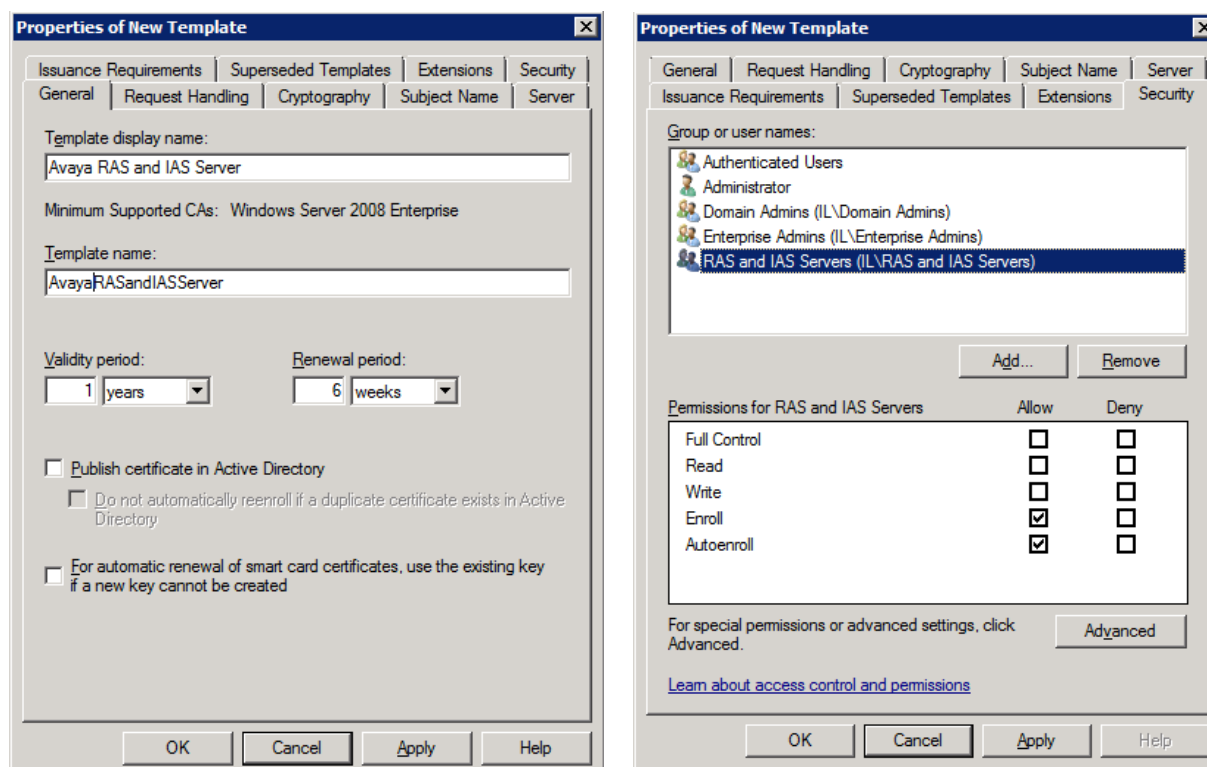
When done, in **Installation Results**, review your installation results, and then click **Close**.

3) Configure Template and Auto-enrollment

Follow the steps described by Microsoft in:

<http://technet.microsoft.com/en-us/library/cc754198.aspx>

Some related example screen shots are presented here:



4) Register the NPS in Active Directory Domain Services

When Network Policy Server (NPS) is a member of an Active Directory Domain Services (AD DS) domain, NPS performs authentication by comparing user credentials that it receives from network access servers with the credentials that are stored for the user account in AD DS. In addition, NPS authorizes connection requests by using network policy and by checking user account dial-in properties in AD DS.

For NPS to have permission to access user account credentials and dial-in properties in AD DS, the server running NPS must be registered in AD DS:

Click Start Menu->Administrative Tools->Network Policy Server.

Right-click **NPS (Local)**, and then click **Register server in Active Directory**. When the **Register Network Policy Server in Active Directory** dialog box appears, click **OK**.

Note:

Alternative register options are described by Microsoft in the following URL:

<http://technet.microsoft.com/en-us/library/cc754878.aspx>

5) Create a New Certificate Template

The new certificate template is based on the existing Workstation Authentication template.

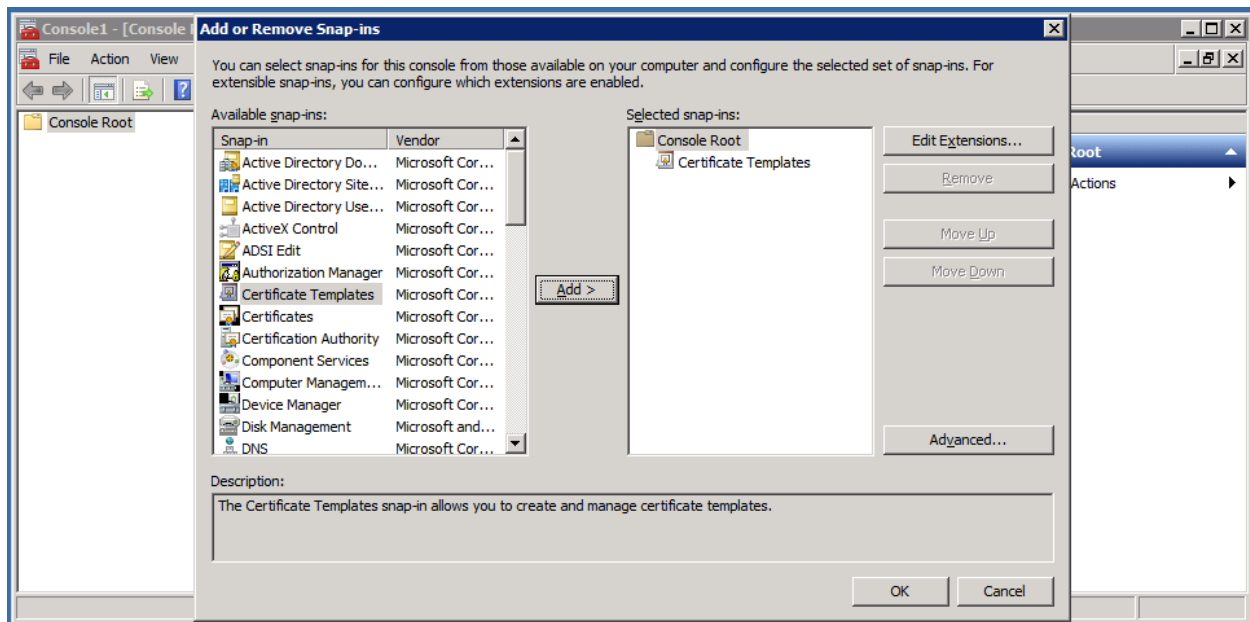
Start Menu->Run

Type: mmc

Click **OK**.

Click File->Add/Remove Snap in...

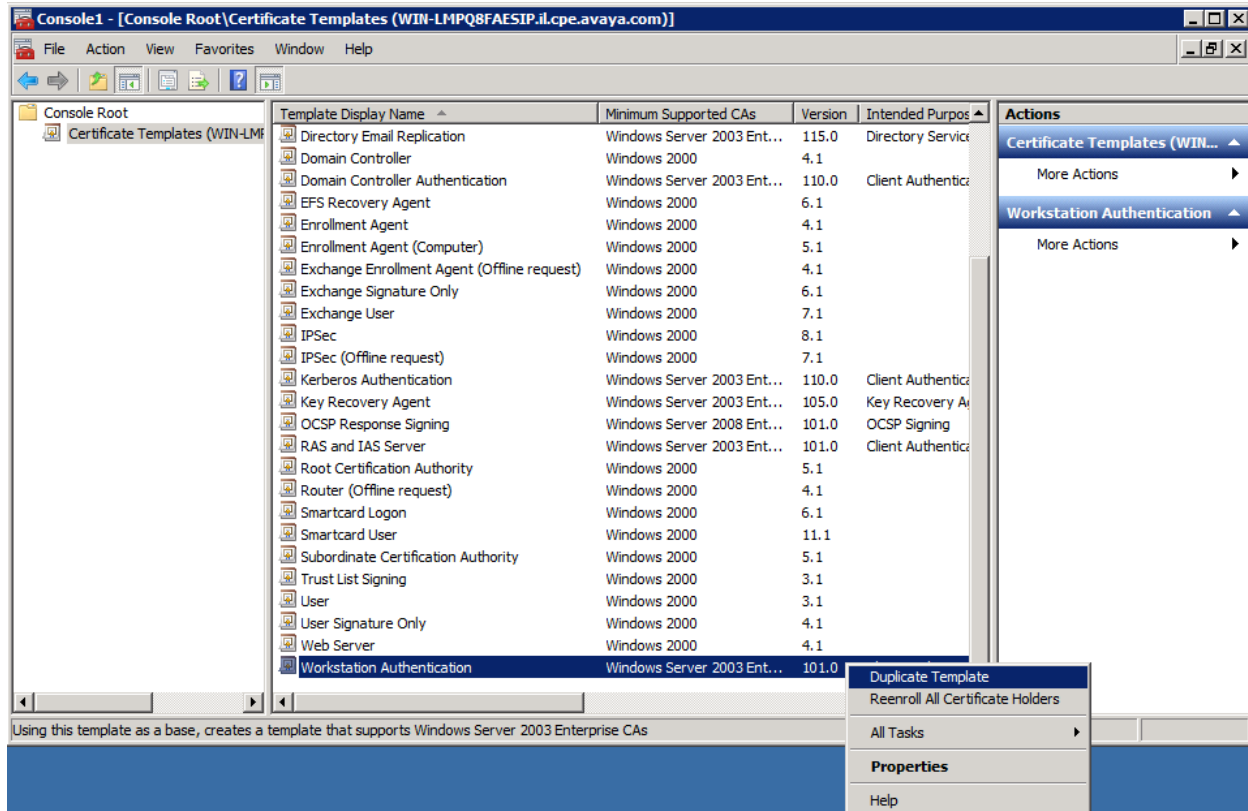
Select **Certificate Templates** and click **Add>**.



Click **OK**.

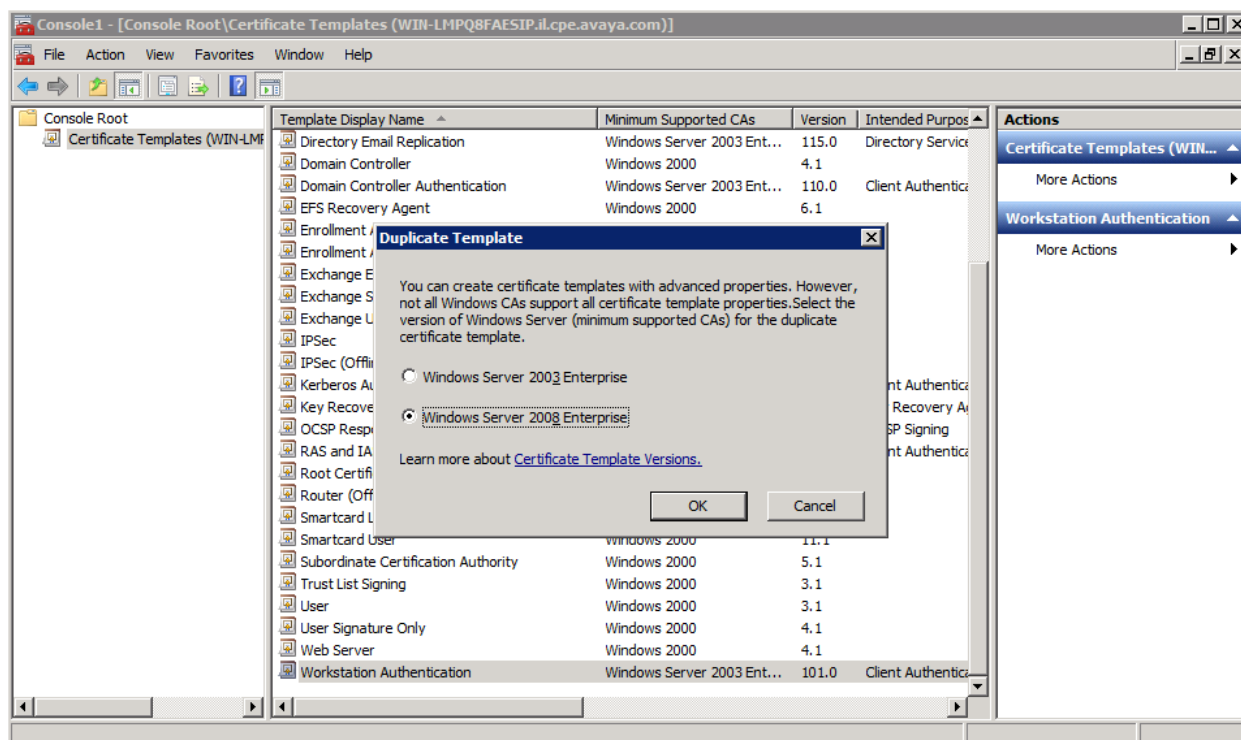
Click **Certificate Templates**.

Right-click **Workstation Authentication** and select **Duplicate Template**.



Select **Windows Server 2008 Enterprise** for minimum supported CA for the duplicate certificate template.

Click **OK**.



A **Properties of New Template** window will be displayed.

Under the General tab, assign a template name. In this example we'll give the name **"mycert"**.

Properties of New Template

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Cryptography | Subject Name | Server

Template display name:
mycert

Minimum Supported CAs: Windows Server 2008 Enterprise

Template name:
mycert

Validity period: 1 years
Renewal period: 6 weeks

☐ Publish certificate in Active Directory

☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

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

OK Cancel Apply Help

Under the Cryptography tab, change the Minimum key size to the desired value. We'll use 2048 in our example.

Select the desired request hash. We will use SHA256 in our example.

The screenshot shows the 'Properties of New Template' dialog box with the 'Cryptography' tab selected. The 'Algorithm name' is set to 'RSA' and the 'Minimum key size' is set to '2048'. Under 'Choose which cryptographic providers can be used for requests', the option 'Requests can use any provider available on the subject's computer' is selected. The 'Providers' list is empty. The 'Request hash' is set to 'SHA256'. The 'Use alternate signature format' checkbox is unchecked. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Properties of New Template	
Issuance Requirements	Superseded Templates
General	Request Handling
Cryptography	Subject Name
Security	Server

Algorithm name: RSA

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

☒ Requests can use any provider available on the subject's computer

☐ Requests must use one of the following providers:

Providers:

- ☐ Microsoft Smart Card Key Storage Provider
- ☐ Microsoft Software Key Storage Provider

Request hash: SHA256

☐ Use alternate signature format.

For more information about restrictions and compatibility click [here](#).

OK Cancel Apply Help

Under the Subject Name tab, select **Supply in the request**.

The screenshot shows the 'Properties of New Template' dialog box with the 'Subject Name' tab selected. The 'Supply in the request' radio button is selected. Below it is an unchecked checkbox for 'Use subject information from existing certificates for autoenrollment renewal requests.' The 'Build from this Active Directory information' radio button is also selected. Below it is a text box for 'Subject name format' with 'None' selected in the dropdown. There is an unchecked checkbox for 'Include e-mail name in subject name'. Below that is a section titled 'Include this information in alternate subject name:' with four unchecked checkboxes: 'E-mail name', 'DNS name', 'User principal name (UPN)', and 'Service principal name (SPN)'. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Properties of New Template

Issuance Requirements | Superseded Templates | Extensions | Security |
General | Request Handling | Cryptography | **Subject Name** | Server

☒ **S**upply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests.

☒ **B**uild from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

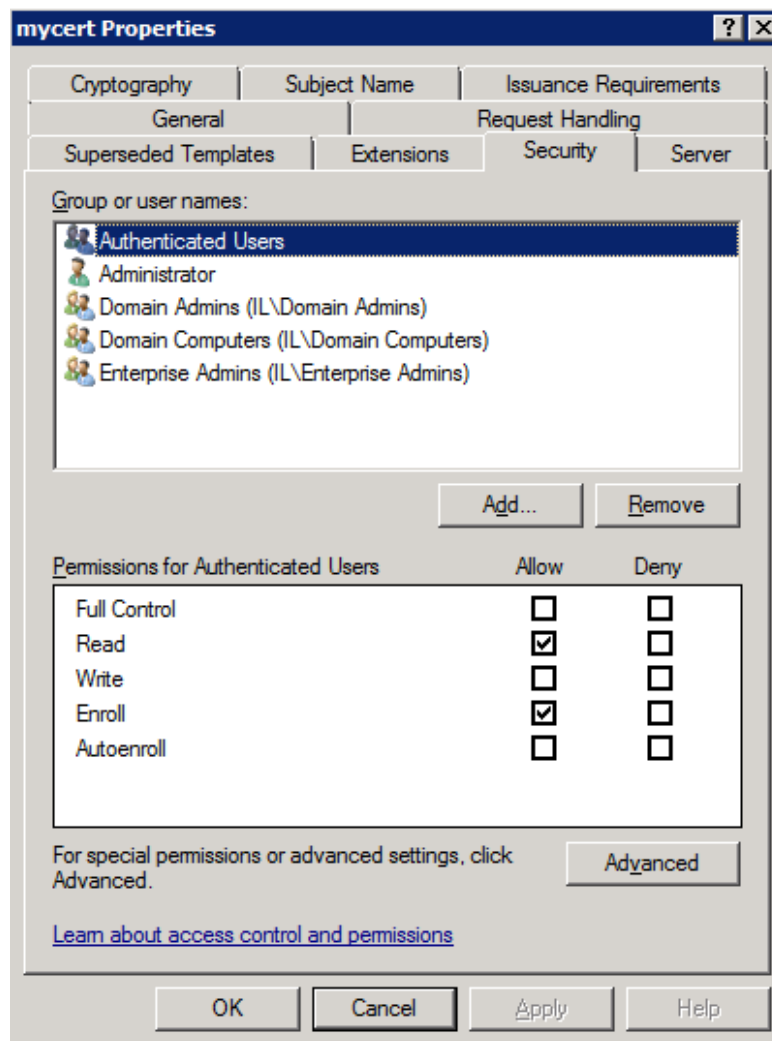
☐ DNS name

☐ User principal name (UPN)

☐ Service principal name (SPN)

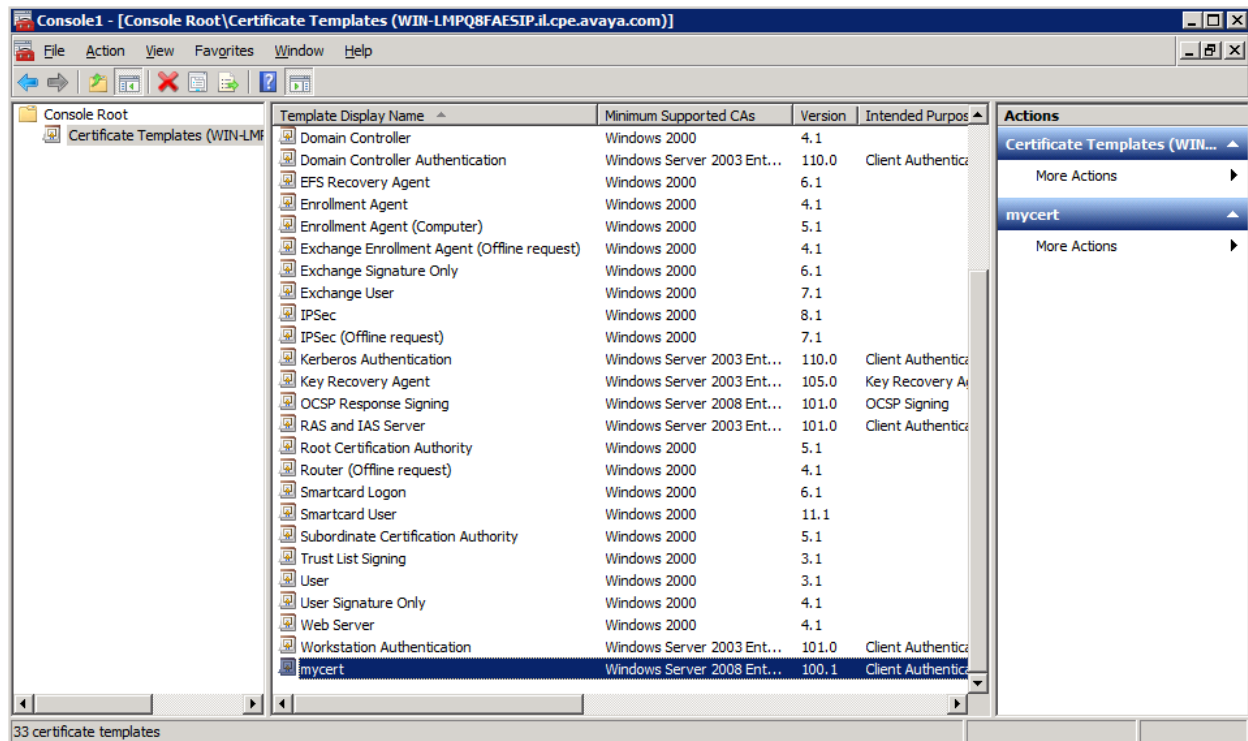
OK Cancel Apply Help

Under the Security tab, in the Group or user name list select **Authenticated Users**. In the Permission for Authenticated Users list select **Allow** for Enroll and Read.



Click **OK**.

Now you should see the newly added template in the template list.



6) Enable The Certificate Template

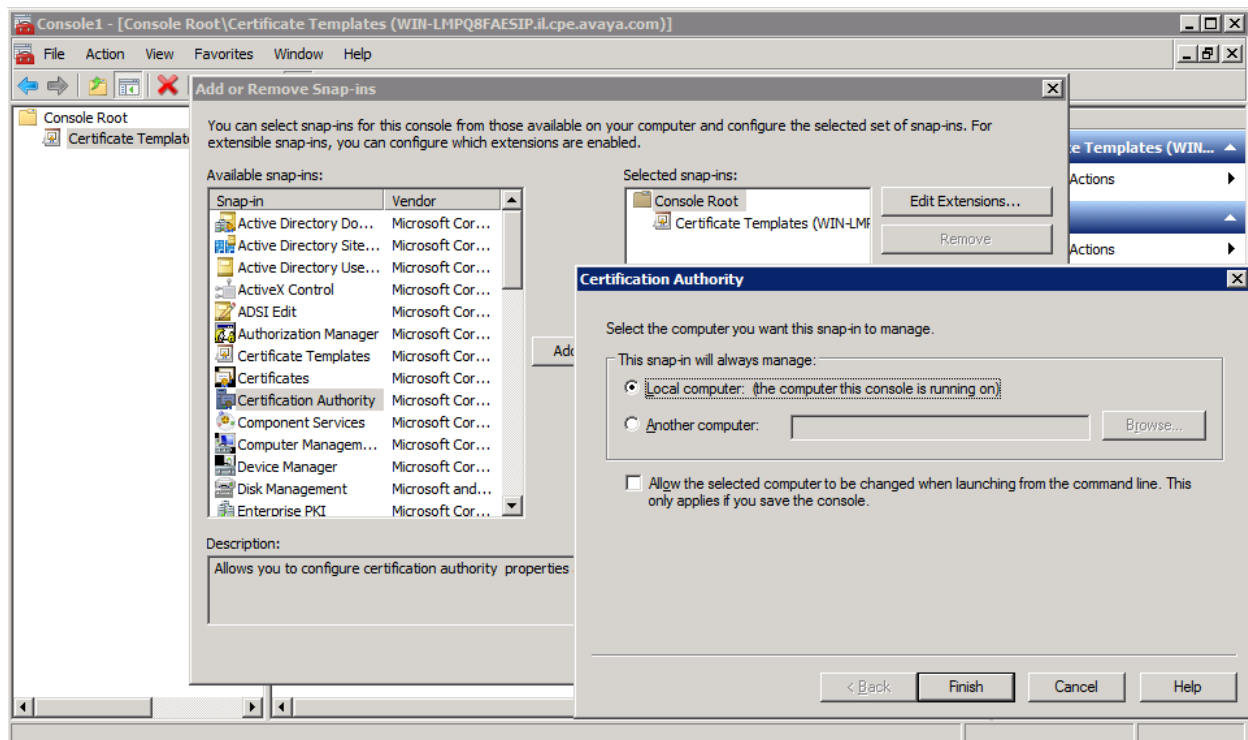
From the Management Console, add the Certification Authority by:

File->Add/Remove Snap-in...

Select **Certificate Authority** and Click **Add>**

Select **Local Computer**.

Click **Finish**.

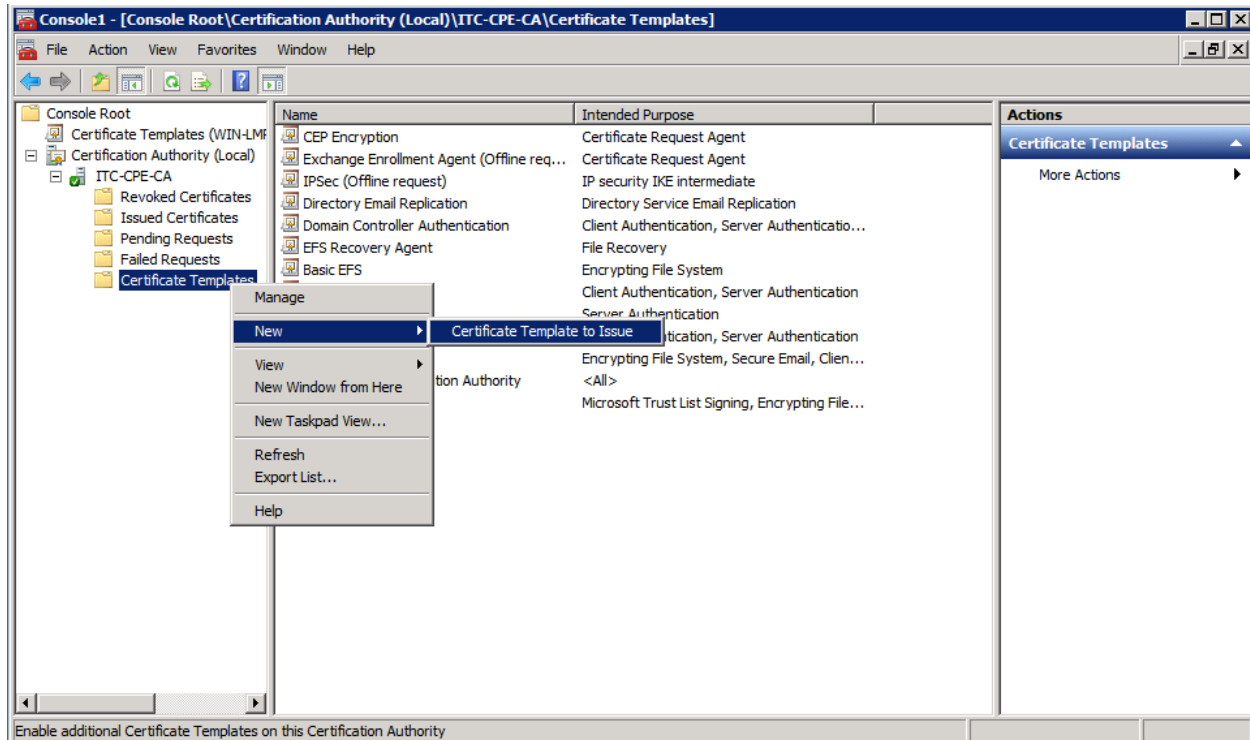


Click **OK**.

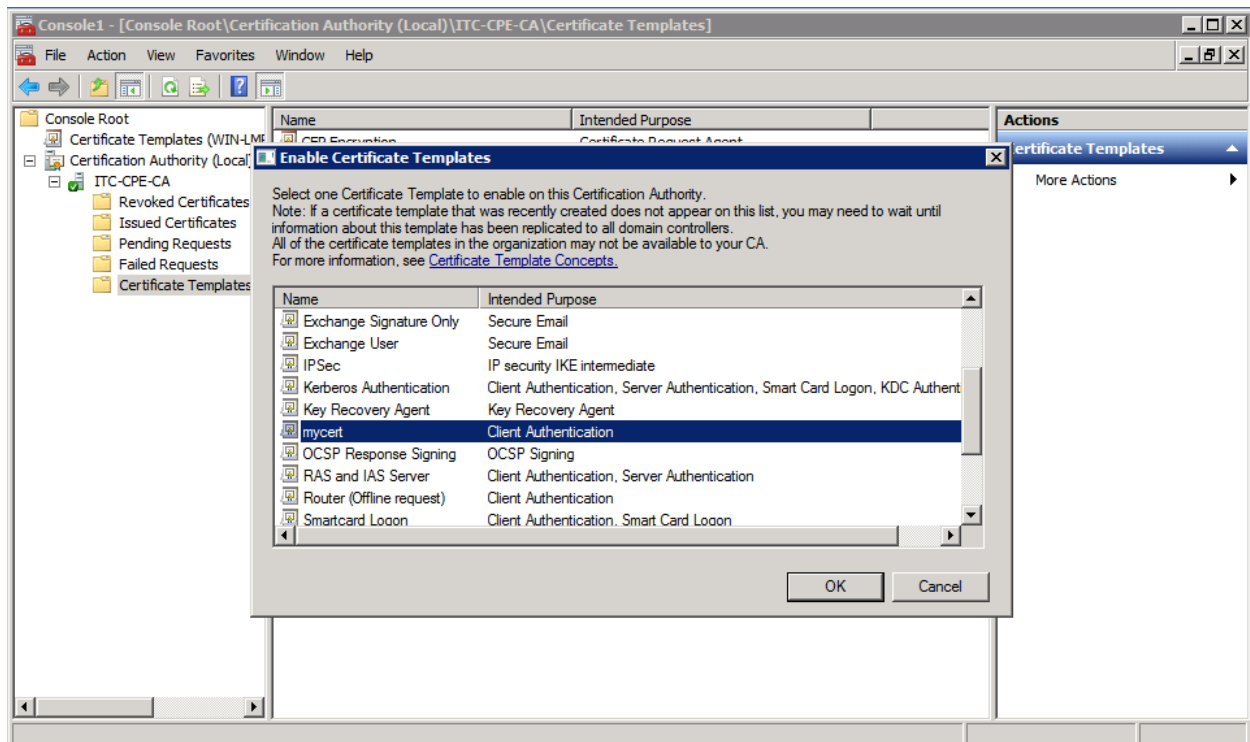
Browse to **Console Root->Certificate Authority->SEVER_NAME->Certificate Templates**

Right-click **Certificate Templates**.

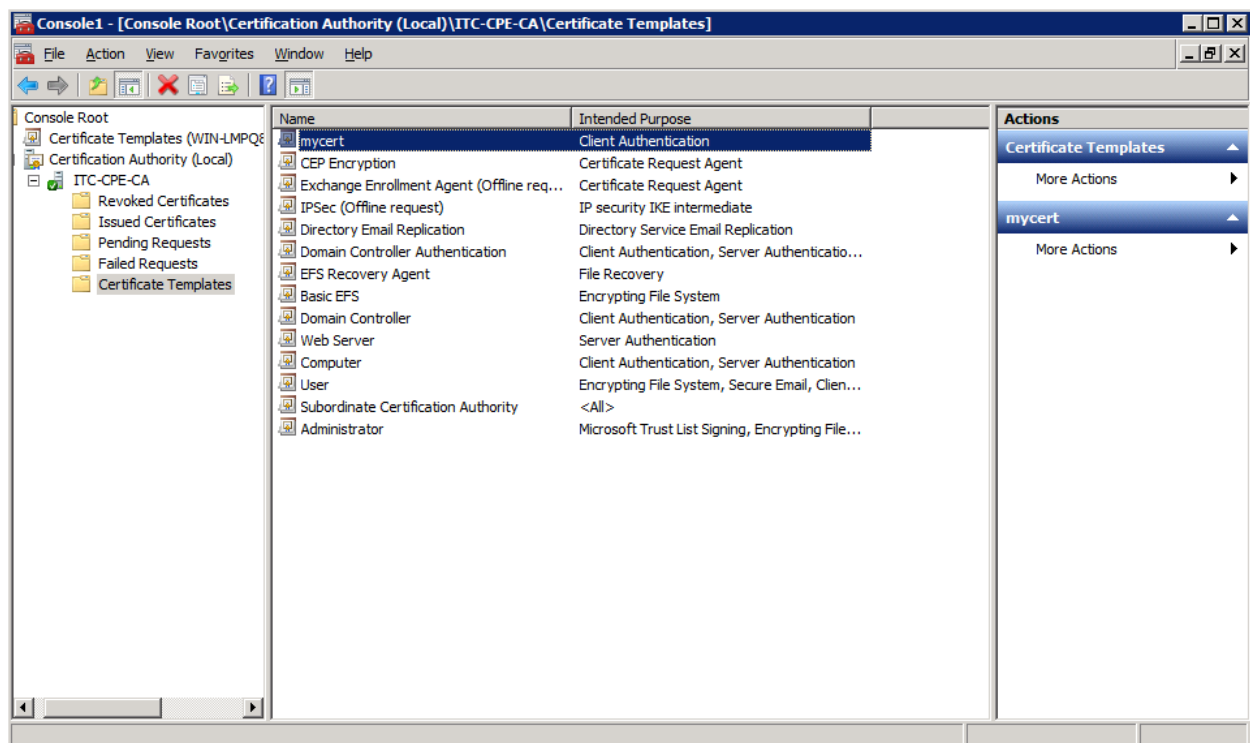
Select **New->Certificate Template to Issue**



In the **Enable Certificate Templates** window select the template created in previous step. In our example it is **mycert**.



Click **OK**.



7) Modify Registry

First, we have to check which template is currently active on the server. This is done by looking into the server's registry. Make sure you are logged into the server with administrator privileges and run the Registry Editor (regedit) to access the registry:

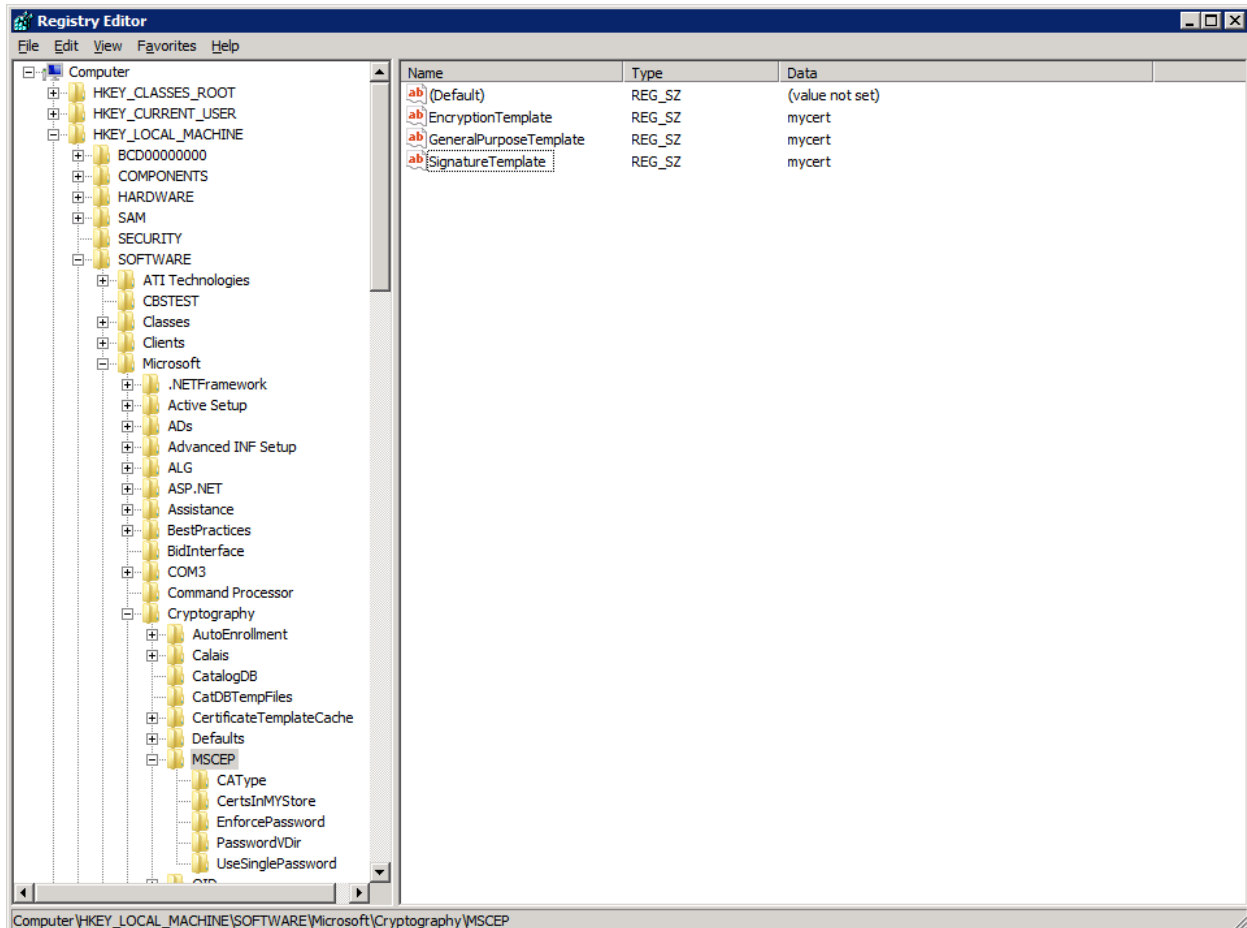
Start menu->Run

Type: regedit

Click **OK**. Browse to:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP

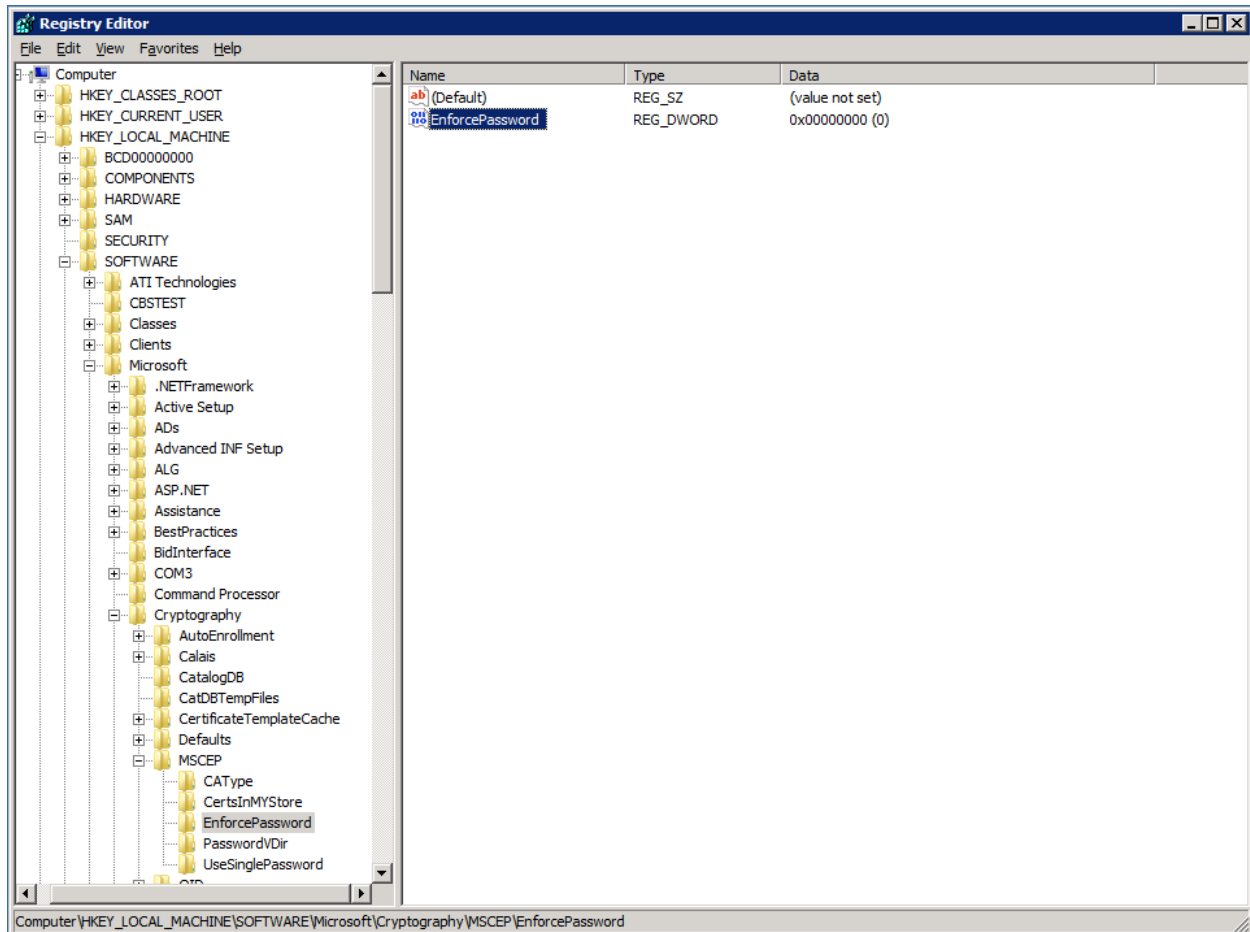
Modify the parameters **EncryptionTemplate**, **GeneralPurposeTemplate** and **SignatureTemplate** to the newly created template (in our example: **mycert**).



Browse to:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

Modify the parameter **EnforcePassword** from 1 to 0. This will prevent the server from requesting a password during certificate enrollment.



After making the changes, exit from regedit application and **restart** the server.

8) NPS Configuration:

Step 1: Configure RADIUS clients

The RADIUS clients are the authenticators – The 802.1X enabled switched that request for authentication in order to grant users (supplicants) access to network resources.

Launch the Network Policy Server application:

Start Menu->Administrative Tools->Network Policy Server

Browse to RADIUS Clients and Servers->RADIUS Clients

Right-click **RADIUS Clients**

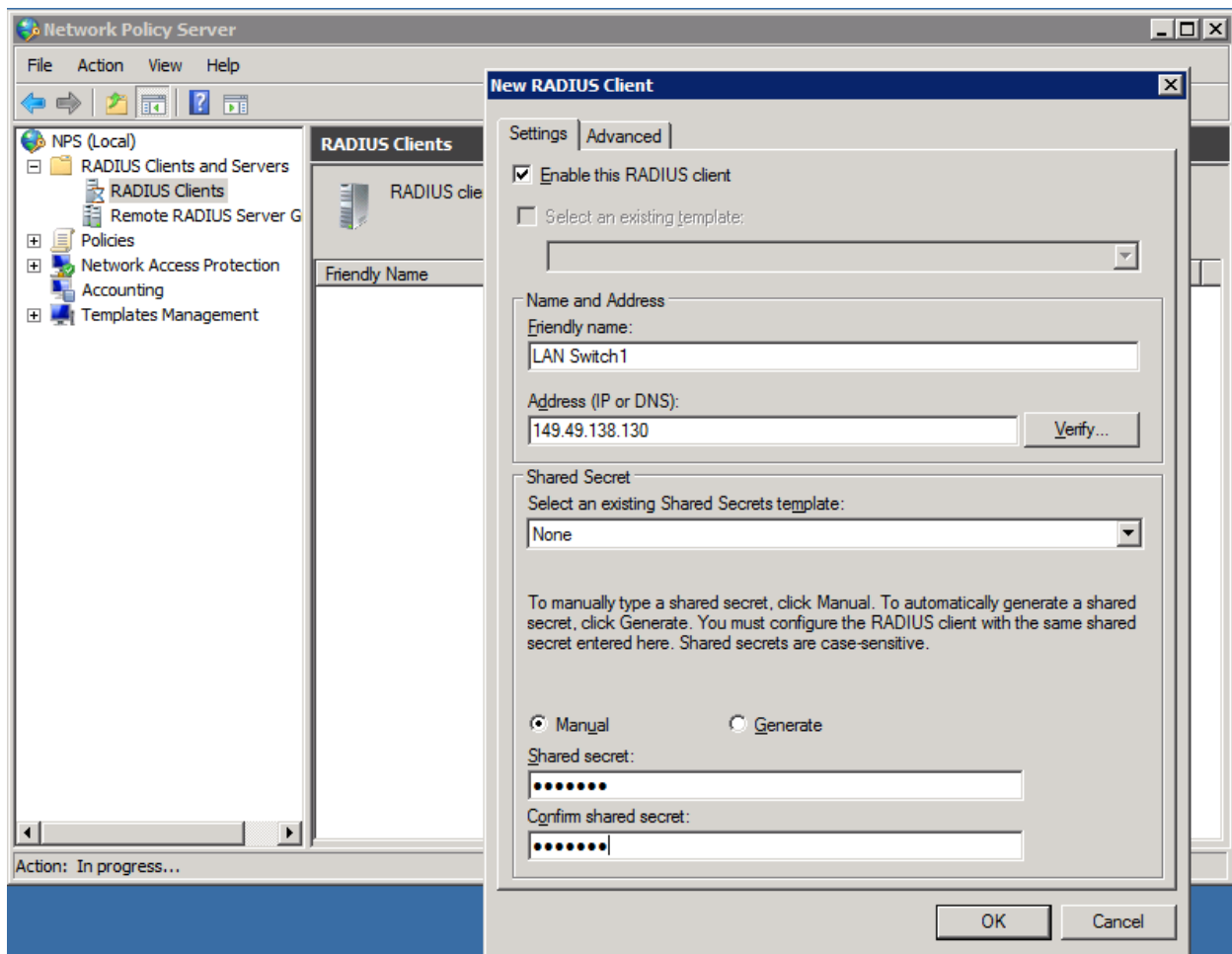
Select **New**

In the New RADIUS Client window:

Check **Enable the RADIUS client** checkbox

Give a friendly name and provide the IP address or the DNS name of the RADIUS client you want to add.

Define a shared secret manually.



Click **OK** when done.

Repeat the above step for each RADIUS client on the network.

You have to define all your 802.1X access control network devices (network switches, access points, etc.) as clients.

Eventually all defined RADIUS clients should be listed under RADIUS Clients.

Step 2: Define Connection Request Policies

Connection request policies tell the server how to treat connection requests.

From the Network Policy Server application browse to Policies

Right-click **Connection Request Policies**.

Select **New**.

In the New Connection Request Policy window give a policy name.

In Type of network access server, select **Unspecified**.

The screenshot shows the 'Secure Wired (Ethernet) Connections Properties' dialog box with the 'Conditions' tab selected. The 'Policy name' field contains 'Secure Wired (Ethernet) Connections'. The 'Policy State' section has 'Policy enabled' checked. The 'Network connection method' section has 'Type of network access server' selected, and the dropdown menu shows 'Unspecified'. The 'Vendor specific' section is not selected. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Secure Wired (Ethernet) Connections Properties

Overview | Conditions | Settings

Policy name: Secure Wired (Ethernet) Connections

Policy State
If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evaluate this policy.

☒ Policy enabled

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server:
Unspecified

☐ Vendor specific:
10

OK Cancel Apply

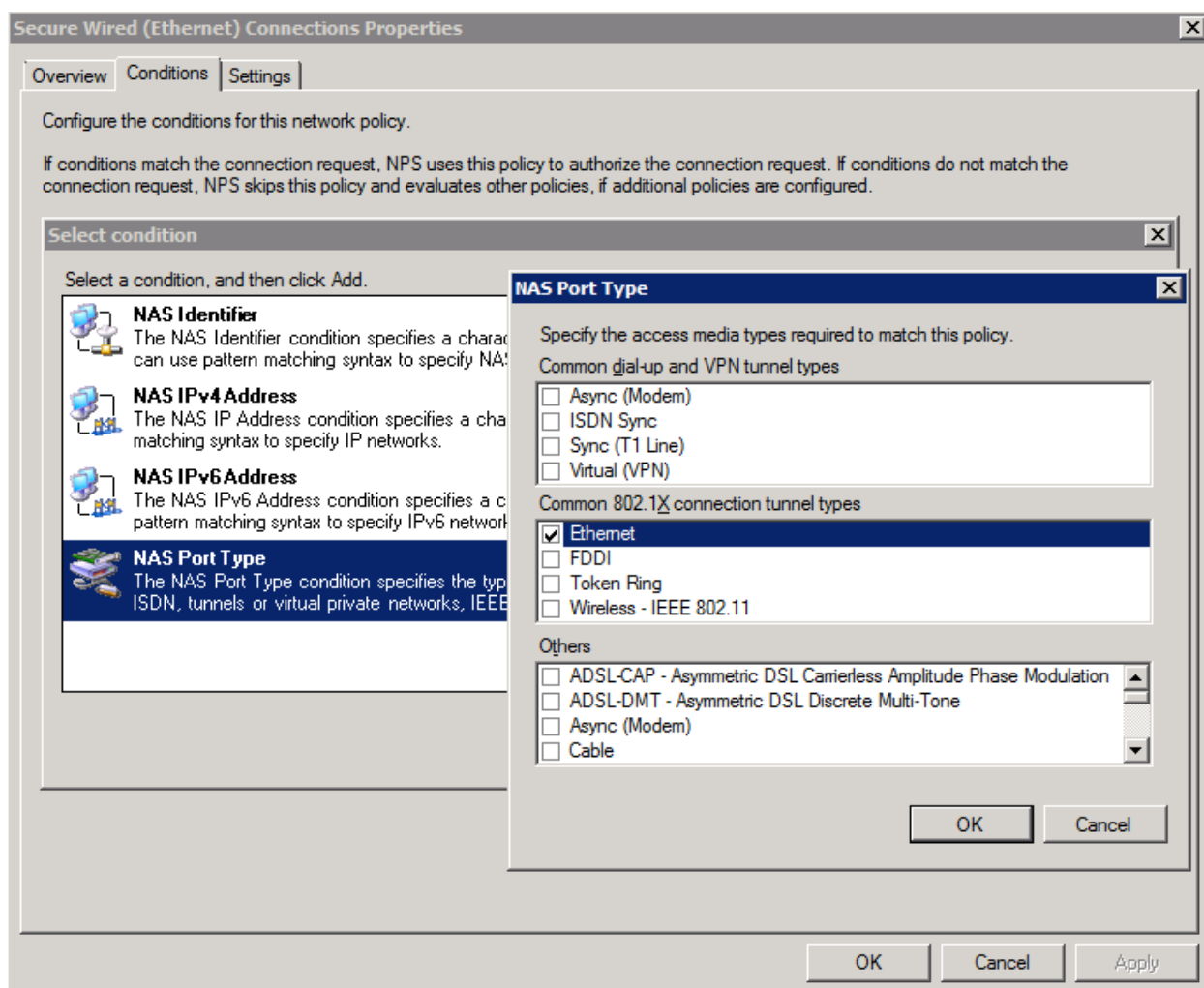
Click **Next**.

In the following screen you need to specify the conditions that determine this connection request.

Click **Add...**

From the presented conditions list, select **NAS Port Type** and click **Add...**

Select the **Ethernet** checkbox under Common 802.1X connection tunnel types.



Click **OK**.

There are additional conditions you can add, based on your organization security policy.

When done click **Next**.

In case no connection request forwarding is required, in the following screen select **Authenticate requests on this server** and click **Next**.



Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

Forwarding Connection Request

→ Authentication

Accounting

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

- ☒ Authenticate requests on this server
- ☐ Forward requests to the following remote RADIUS server group for authentication:

<not configured>

New...

- ☐ Accept users without validating credentials

Previous

Next

Finish

Cancel

In the Authentication Methods window, check **Override network authentication settings**.

Click **Add...**

Select **Microsoft: Smart Card or other certificate**, and click **OK**.

The screenshot shows the 'New Connection Request Policy' dialog box with the 'Specify Authentication Methods' tab selected. The dialog has a title bar with a close button. Below the title bar is a section with a computer icon and the title 'Specify Authentication Methods'. The text below the icon reads: 'Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP.'

Below this is a checkbox labeled 'Override network policy authentication settings' which is checked. Below the checkbox is a paragraph: 'These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.'

Below the paragraph is another paragraph: 'EAP types are negotiated between NPS and the client in the order in which they are listed.'

Below this is a section titled 'EAP Types:'. It contains a list box with one item: 'Microsoft: Smart Card or other certificate'. To the right of the list box are two buttons: 'Move Up' and 'Move Down'. Below the list box are three buttons: 'Add...', 'Edit...', and 'Remove'.

Below the 'EAP Types' section is a section titled 'Less secure authentication methods:'. It contains a list of checkboxes with their corresponding labels: 'Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)', 'Microsoft Encrypted Authentication (MS-CHAP)', 'Encrypted authentication (CHAP)', 'Unencrypted authentication (PAP, SPAP)', and 'Allow clients to connect without negotiating an authentication method.'.

At the bottom of the dialog are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

Click **Next**.

The following screen requests for attributes definition. In our application there is no need for attributes so just click **Next**.

New Connection Request Policy

Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

Configure the settings for this network policy.
If conditions match the connection request and the policy grants access, settings are applied.

Settings:

Specify a Realm Name

- Attribute

RADIUS Attributes

- ☐ Standard
- ☒ Vendor Specific

Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list.


Attribute:

Rules:

Find	Replace With
------	--------------

Click **Finish** in the policy completion screen.

New Connection Request Policy [X]

 **Completing Connection Request Policy Wizard**

You have successfully created the following connection request policy:

Secure Wired (Ethernet) Connection

Policy conditions:

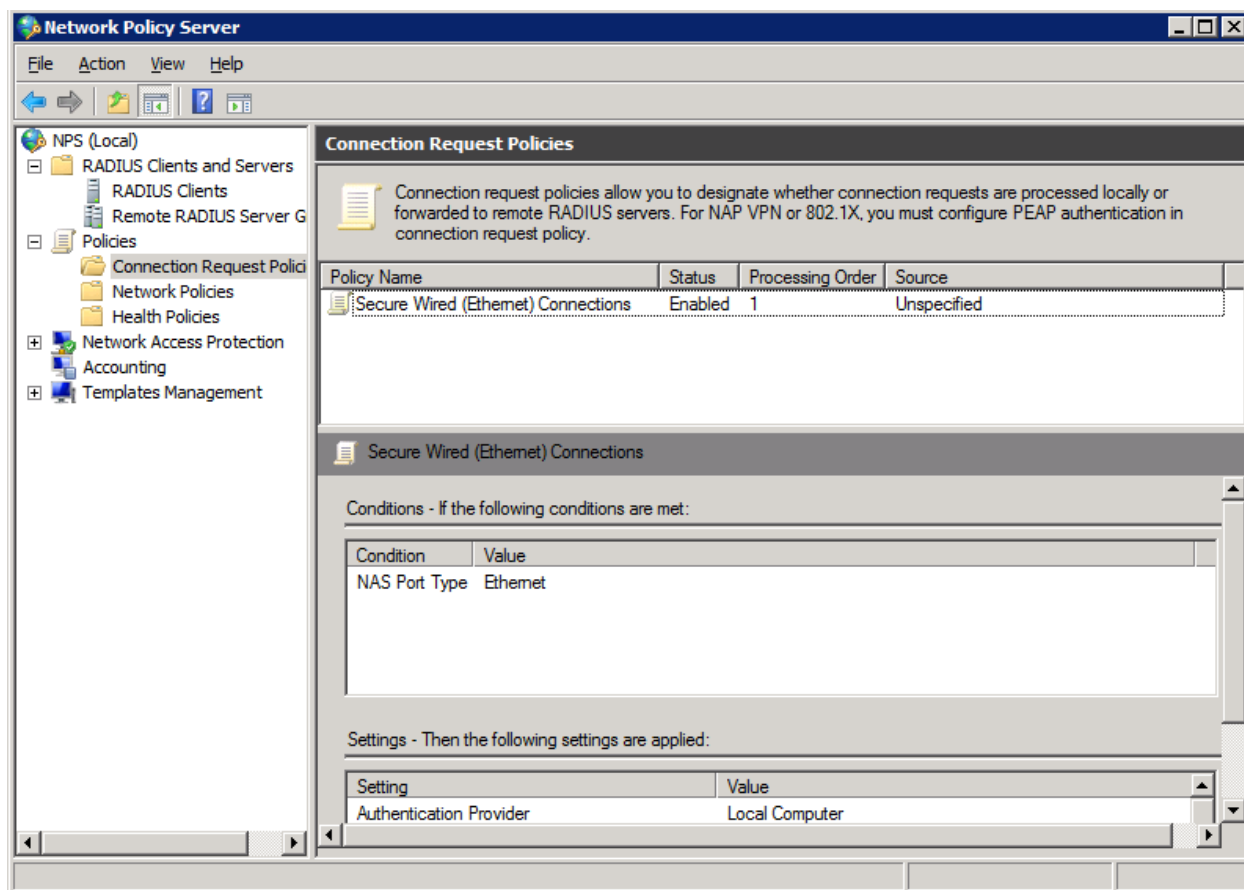
Condition	Value
NAS Port Type	Ethernet

Policy settings:

Condition	Value
Authentication Provider	Local Computer
Override Authentication	Enabled
Authentication Method	EAP
Extensible Authentication Protocol Method	Microsoft: Smart Card or other certificate

To close this wizard, click Finish.

Now you should see your newly defined policy in the **Connection Request Policies** section.



Step 3: Associate TLS Network Policy with Windows Groups

Launch the Network Policy Server application:

Start Menu->Administrative Tools->Network Policy Server

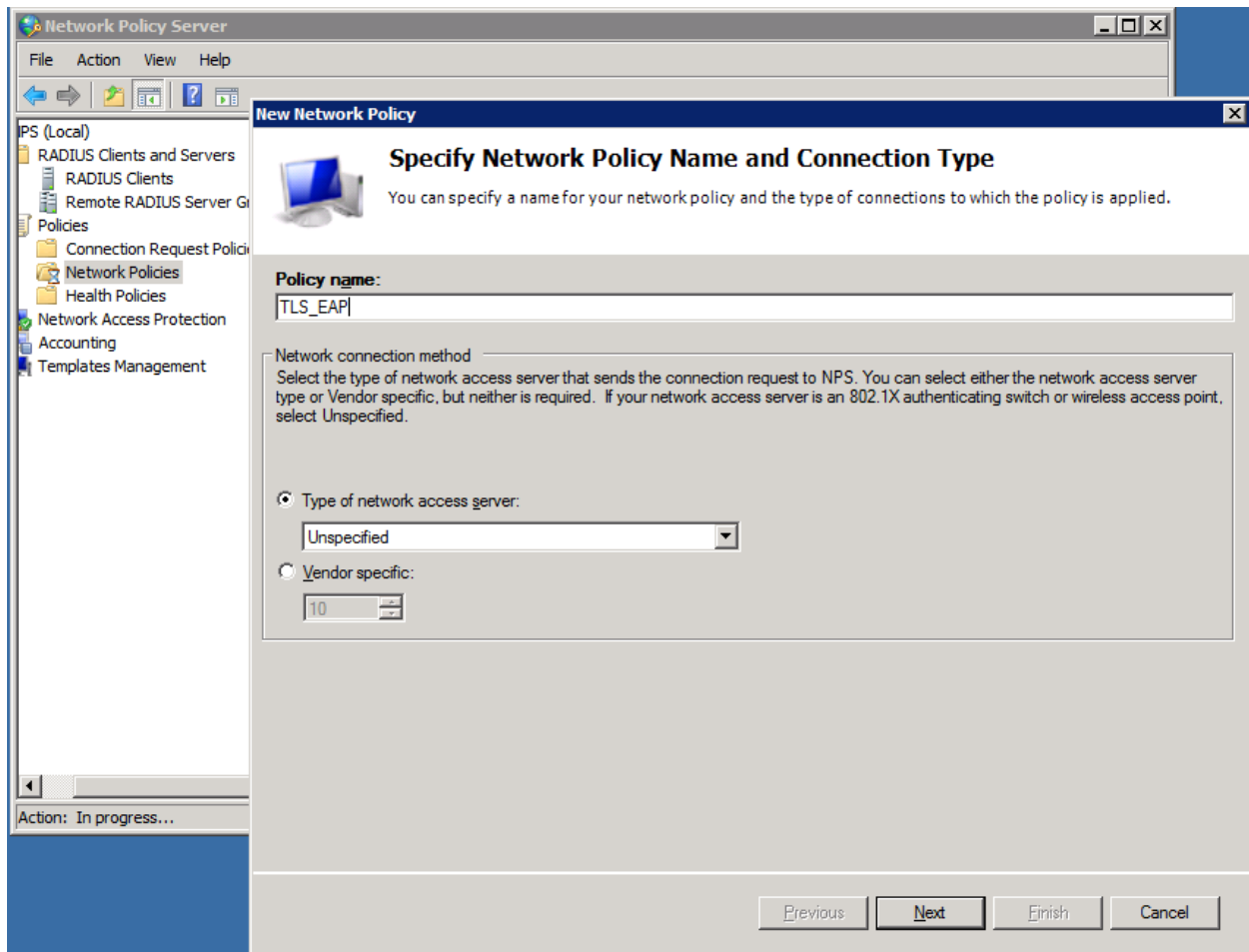
Browse to Policies

Right-click **Network Policies**

Select **New**

Type in your preferred policy name.

Click **Next**.

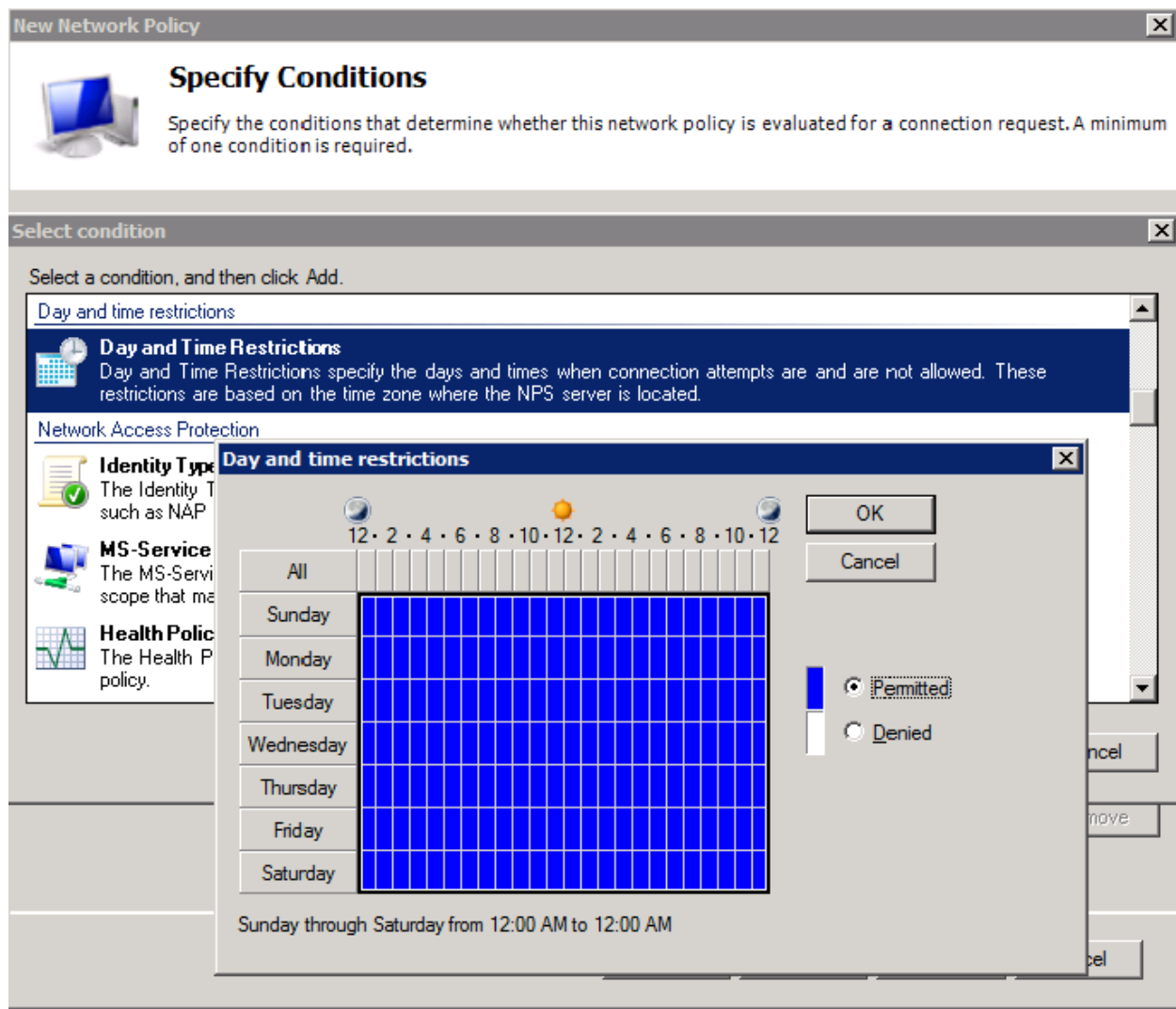


In the following window you have to specify conditions that determine whether this network policy is evaluated for a connection request.

Click **Add...**

Select **Day and Time Restrictions** and click **Add...**

Select the days and time to the system to permit or deny access. In our example we will permit access all days at all times.



Click **OK**.

Click **Add...**

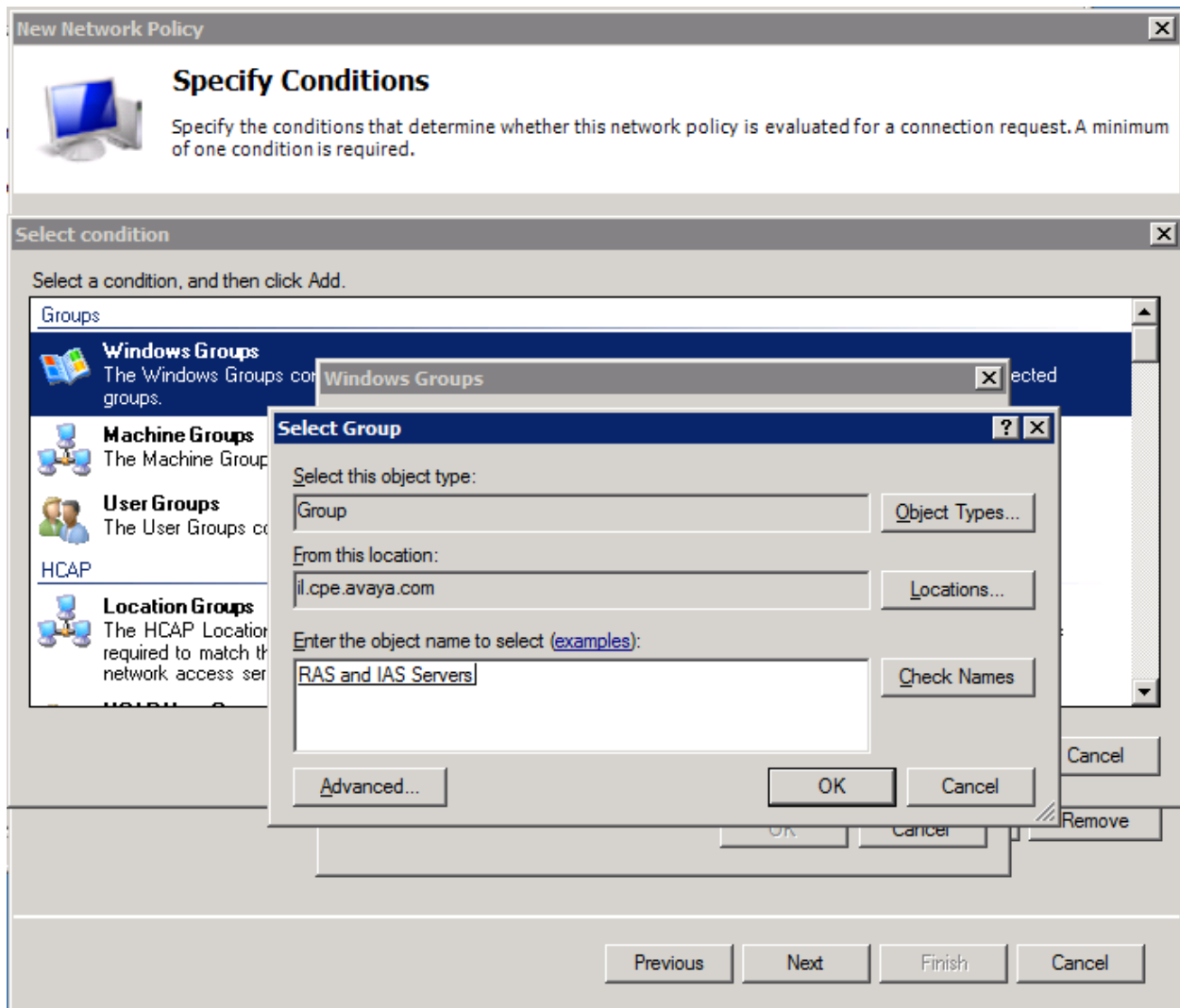
Select **Windows Groups** and click **Add...**

Click **Add Groups...**

Enter the following group: RAS and IAS Servers

Click **Check Names** to make sure this group exists.

Click **OK**.




Click **OK**.

Click **Next**.

Select **Access granted** radio button in the Access Permission screen.

New Network Policy [X]

 **Specify Access Permission**

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

☒ **Access granted**
Grant access if client connection attempts match the conditions of this policy.

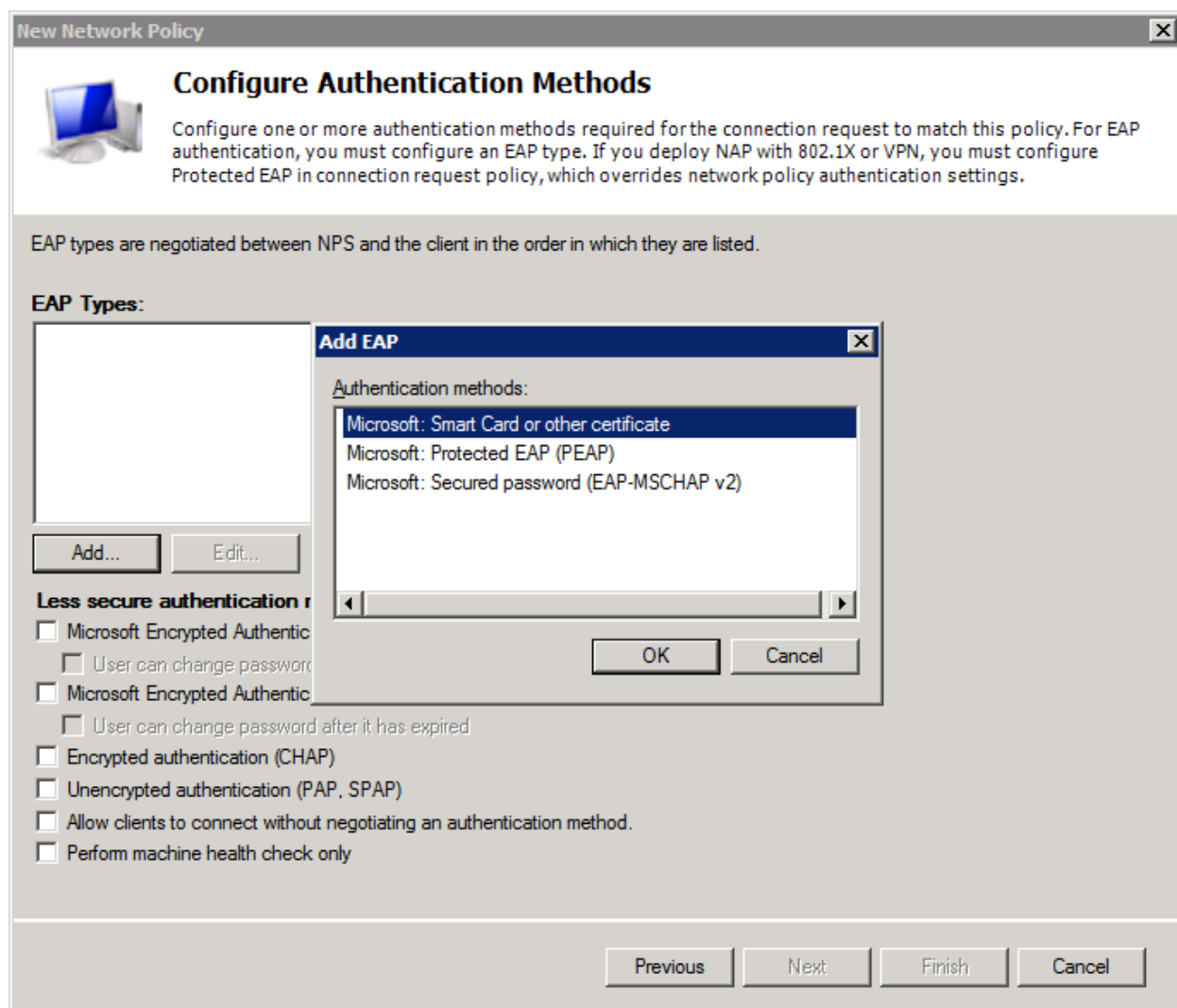
☐ **Access denied**
Deny access if client connection attempts match the conditions of this policy.

☐ **Access is determined by User Dial-in properties (which override NPS policy)**
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Click **Next**.

In the Authentication Methods window, click **Add...**

Select **Microsoft: Smart Card or other certificate**, and click **OK**.



Uncheck all other Less secure authentication methods.

Click **Next**.

The following screen allows you to configure constraints, which are additional parameters of the network policy that required to match the connection requests.

If none are required then just click **Next**.

New Network Policy [X]






Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints

-  Idle Timeout
-  Session Timeout
-  Called Station ID
-  Day and time restrictions
-  NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

[Previous](#) [Next](#) [Finish](#) [Cancel](#)

Click **Next**.

Select **NAS Port Type** and select **Ethernet** checkbox under Common 802.1X connection tunnel types.

The screenshot shows the 'New Network Policy' dialog box with the 'Configure Constraints' tab selected. On the left, a list of constraints includes 'Idle Timeout', 'Session Timeout', 'Called Station ID', 'Day and time restrictions', and 'NAS Port Type', which is highlighted. The main area is titled 'Specify the access media types required to match this policy'. It contains three sections: 'Common dial-up and VPN tunnel types' with checkboxes for 'Async (Modem)', 'ISDN Sync', 'Sync (T1 Line)', and 'Virtual (VPN)'; 'Common 802.1X connection tunnel types' with checkboxes for 'Ethernet' (checked), 'FDDI', 'Token Ring', and 'Wireless - IEEE 802.11'; and 'Others' with checkboxes for 'ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation', 'ADSL-DMT - Asymmetric DSL Discrete Multi-Tone', 'Async (Modem)', and 'Cable'. At the bottom are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'.

New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type**

Specify the access media types required to match this policy

Common dial-up and VPN tunnel types

- ☐ Async (Modem)
- ☐ ISDN Sync
- ☐ Sync (T1 Line)
- ☐ Virtual (VPN)

Common 802.1X connection tunnel types

- ☒ Ethernet
- ☐ FDDI
- ☐ Token Ring
- ☐ Wireless - IEEE 802.11

Others

- ☐ ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation
- ☐ ADSL-DMT - Asymmetric DSL Discrete Multi-Tone
- ☐ Async (Modem)
- ☐ Cable

Previous **Next** **Finish** **Cancel**

Click **Next**.



Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.

If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

Standard

☒ Vendor Specific

Network Access Protection

NAP Enforcement

Extended State

Routing and Remote Access

Multilink and Bandwidth Allocation Protocol (BAP)

IP Filters

Encryption

☒ IP Settings

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add...

Edit...

Remove

Previous

Next

Finish

Cancel

Click **NAP Enforcement** setting on the left.

Select the **Allow full network access** radio button.

Check the **Enable auto-remediation of client computers** checkbox.

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes**
 - Standard
 - ☒ Vendor Specific
- Network Access Protection**
 - NAP Enforcement**
 - Extended State
- Routing and Remote Access**
 - Multilink and Bandwidth Allocation Protocol (BAP)
 - IP Filters
 - Encryption
 - ☒ IP Settings

☐ **Allow full network access for a limited time**
Allows unrestricted network access until the specified date and time. After the specified date and time, health policy is enforced and non-compliant computers can access only the restricted network.

Date: Time:

☐ **Allow limited access**
Non-compliant clients are allowed access only to a restricted network for updates.

Remediation Server Group and Troubleshooting URL
To configure a Remediation Server Group, a Troubleshooting URL, or both, click **Configure...**

Auto remediation
☒ **Enable auto-remediation of client computers**
Automatically remediate computers that do not meet health requirements defined in this policy.

Previous **Next** **Finish** **Cancel**

Click **Multiple Bandwidth Allocation Protocol (BAP)** setting on the left.

Select **Server settings determine Multilink usage**.

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes**
 - Standard
 - Vendor Specific
- Network Access Protection**
 - NAP Enforcement
 - Extended State
- Routing and Remote Access**
 - Multilink and Bandwidth Allocation Protocol (BAP)**
 - IP Filters
 - Encryption
 - IP Settings

Multilink
Specify how you would like to handle multiple connections to the network.

☒ **Server settings determine Multilink usage**

☐ Do not allow Multilink connections

☐ Specify Multilink settings
Maximum number of ports allowed:

Bandwidth Allocation Protocol
If the lines of a Multilink connection fall below the following percentage of capacity for the specified period of time, reduce the connection by one line.

Percentage of capacity:

Period of time: min

☐ Require BAP for dynamic Multilink requests

Navigation: Previous Next Finish Cancel

Click **IP Filters** setting on the left.

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes**
 - Standard
 - ☒ Vendor Specific
- Network Access Protection**
 - NAP Enforcement
 - ☒ Extended State
- Routing and Remote Access**
 - Multilink and Bandwidth Allocation Protocol (BAP)
 - IP Filters**
 - Encryption
 - ☒ IP Settings

Select an existing IP Filter template:
None

IPv4

To control the IPv4 packets this interface sends, click Input Filters. **Input Filters...**

To control the IPv4 packets this interface receives, click Output Filters. **Output Filters...**

IPv6

To control the IPv6 packets this interface sends, click Input Filters. **Input Filters...**

To control the IPv6 packets this interface receives, click Output Filters. **Output Filters...**

Previous **Next** **Finish** **Cancel**

Click **Encryption** setting on the left.

Check the following checkboxes:

- Basic encryption (MPPE 40-bit)
- Strong encryption (MPPE 56-bit)
- Strongest encryption (MPPE 128-bit)
- No encryption

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes**
 - Standard
 - ☒ Vendor Specific
- Network Access Protection**
 - NAP Enforcement
 - Extended State
- Routing and Remote Access**
 - Multilink and Bandwidth Allocation Protocol (BAP)
 - IP Filters
 - Encryption**
 - ☒ IP Settings

The encryption settings are supported by computers running Microsoft Routing and Remote Access Service.

If you use different network access servers for dial-up or VPN connections, ensure that the encryption settings you select are supported by your servers.

If No encryption is the only option selected, traffic from access clients to the network access server is not secured by encryption. This configuration is not recommended.

☒ Basic encryption (MPPE 40-bit)
☒ Strong encryption (MPPE 56-bit)
☒ Strongest encryption (MPPE 128-bit)
☒ No encryption

[Previous](#) [Next](#) [Finish](#) [Cancel](#)

Click **IP Settings** setting on the left.

Select the **Server settings determine IP address assignment** radio button.

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes**
 - Standard
 - Vendor Specific
- Network Access Protection**
 - NAP Enforcement
 - Extended State
- Routing and Remote Access**
 - Multilink and Bandwidth Allocation Protocol (BAP)
 - IP Filters
 - Encryption
 - IP Settings**

Specify the client IP address assignment rules for this policy.

☐ Server must supply an IP address

☐ Client may request an IP address

☒ **Server settings determine IP address assignment**

☐ Assign a static IPv4 address


To configure IPv6 settings, go to the Standard page of RADIUS Attributes.

Previous **Next** **Finish** **Cancel**

Click **Next**.

New Network Policy

Completing New Network Policy



You have successfully created the following network policy:

TLS_EAP

Policy conditions:

Condition	Value
Windows Groups	IL\RAS and IAS Servers
Day and time restrictions	Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00 Thursday 00:...

Policy settings:

Condition	Value
Authentication Method	EAP
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

[Previous](#) [Next](#) [Finish](#) [Cancel](#)

Click **Finish** in the completion screen.

5. Phone User Definition

All phones (suplicants) that are required to be authenticated with 802.1X network access should be defined as users in the Active Directory server.

The Avaya 9600 series phones can be distinguished by their MAC address or serial number. So the user names for the phones should be based on one of those, hence must be unique.

Note:

- All user names should be based either on phone's MAC address or serial number.
- For EAP-TLS authentication, phone passwords can be alphanumeric. For MD5 authentication the phone's passwords must be numeric only (MD5 is out of scope of this document).
- Make sure your phone's password aligns with the domain password policy.

Step 1: Create a New Phone User

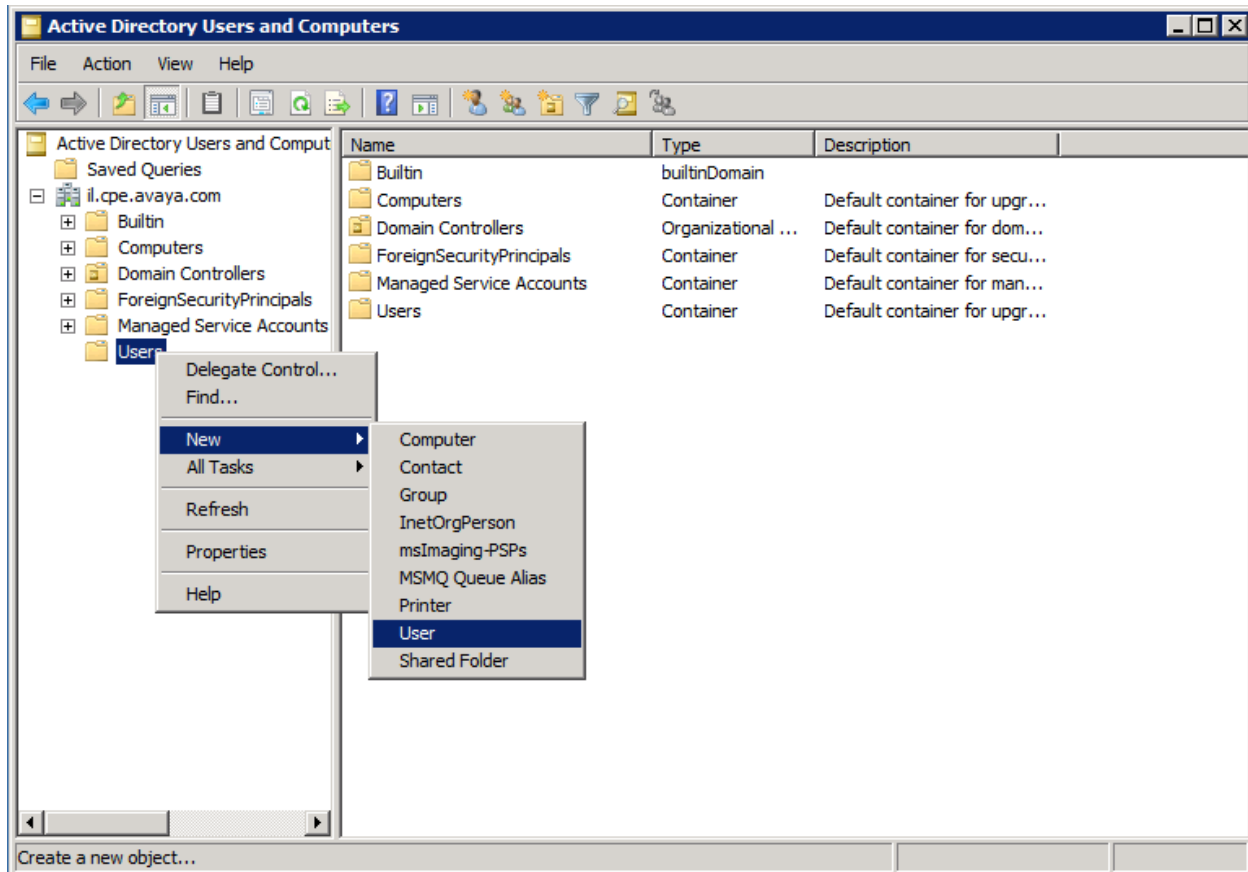
Here is an example how to define a phone in the Active Directory based on its MAC address:

Launch the **Active Directory Users and Computers** application on the Windows 2008 Server:

Start Menu->Administrative Tools->Active Directory Users and Computers

Right-click **Users** section on the right.

On the drop down menu, select **New->User**.



In the New Object-User screen enter the following:

First name: Enter a name

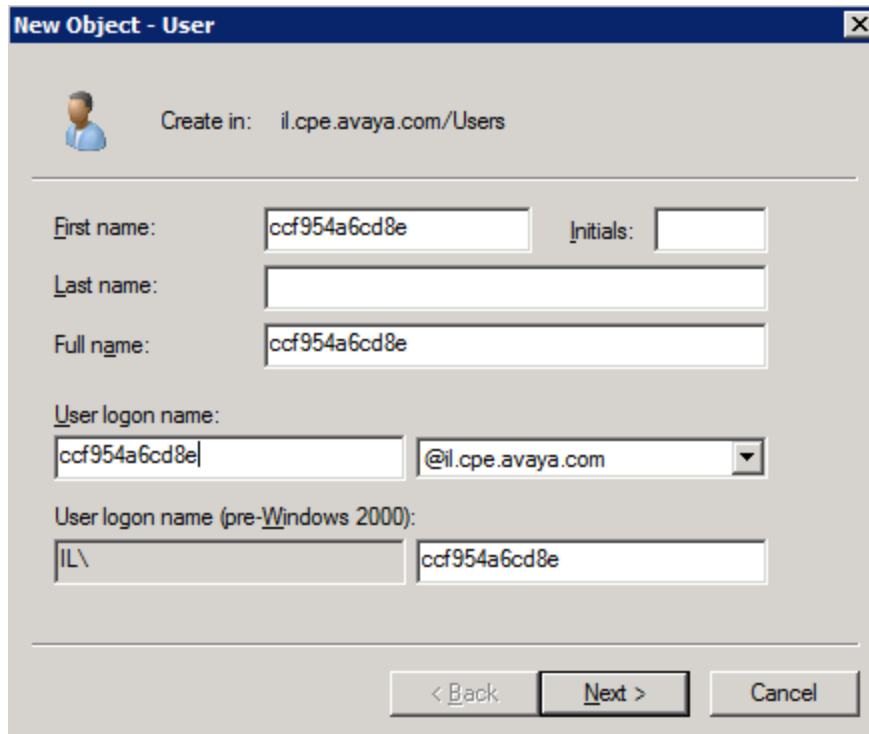
Last name: You can leave it empty

Full name: It will copy the entered first name by default.

User logon name: Should be phone's MAC address or the phone's serial number. In our example we will use the MAC address CC:F9:54:A6:CD:8E to authenticate a phone.

Notes:

- Phone's MAC address and serial number are labeled on the back of the phone. They also can be viewed on the phone's user interface:
 - o On Non-touch phones: Menu/Home button->Network Information. Then browse left to see the Miscellaneous screen.
 - o On Touch phones: Home button->Settings->Network Information. Then browse left to see the Miscellaneous screen.
- The user name must not include spaces, colons or dashes.



The image shows a 'New Object - User' dialog box. At the top, it says 'Create in: il.cpe.avaya.com/Users'. Below this, there are several input fields: 'First name:' with the value 'ccf954a6cd8e', 'Initials:' (empty), 'Last name:' (empty), 'Full name:' with the value 'ccf954a6cd8e', 'User logon name:' with the value 'ccf954a6cd8e' and a dropdown menu showing '@il.cpe.avaya.com', and 'User logon name (pre-Windows 2000):' with the value 'IL\' and another field with the value 'ccf954a6cd8e'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

New Object - User

Create in: il.cpe.avaya.com/Users

First name: ccf954a6cd8e Initials:

Last name:

Full name: ccf954a6cd8e

User logon name: ccf954a6cd8e @il.cpe.avaya.com

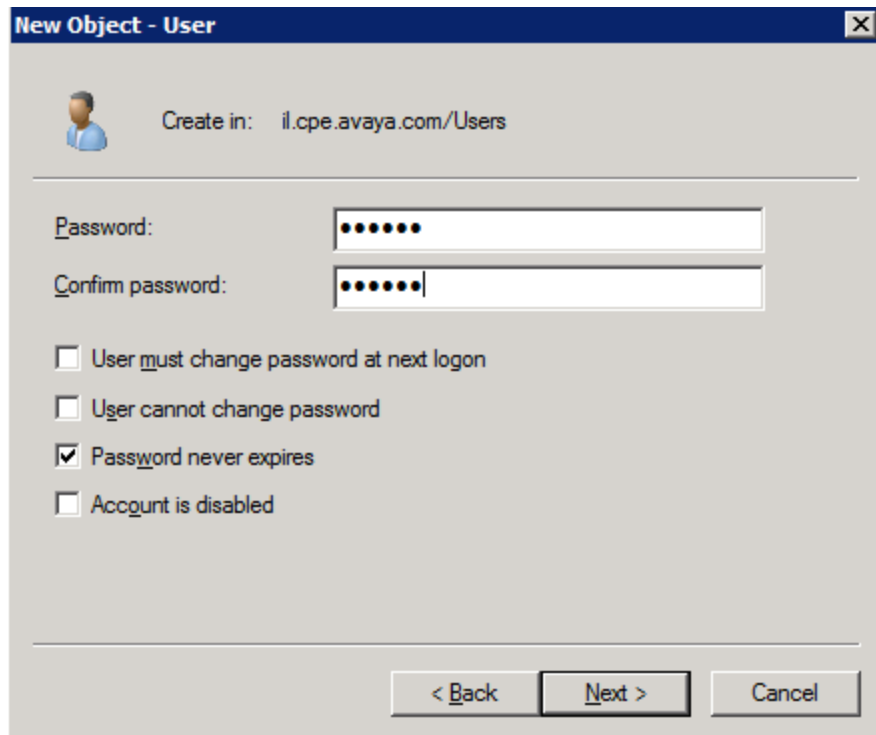
User logon name (pre-Windows 2000): IL\ ccf954a6cd8e

< Back Next > Cancel

Click **Next**.

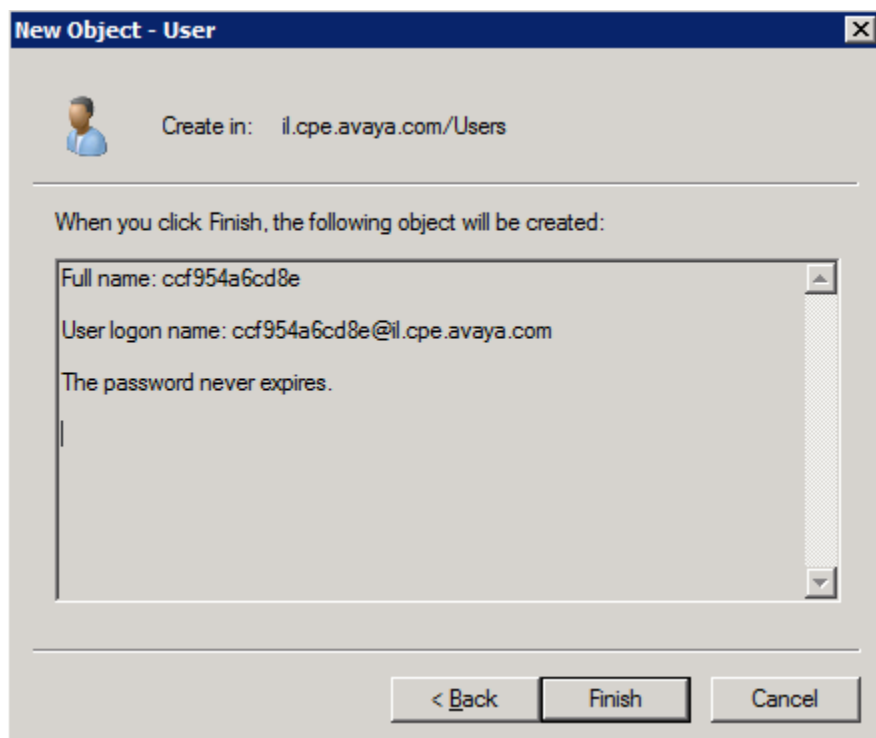
Enter password and confirm it in the following field.

Check only the **Password never expires** checkbox.



The dialog box is titled "New Object - User" with a close button (X) in the top right corner. Below the title bar, there is a user icon and the text "Create in: il.cpe.avaya.com/Users". The main area contains two password input fields: "Password:" and "Confirm password:", both filled with dots. Below these are four checkboxes: "User must change password at next logon" (unchecked), "User cannot change password" (unchecked), "Password never expires" (checked), and "Account is disabled" (unchecked). At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Click **Next**.



The dialog box is titled "New Object - User" with a close button (X) in the top right corner. Below the title bar, there is a user icon and the text "Create in: il.cpe.avaya.com/Users". The main area contains a text box with the following content: "When you click Finish, the following object will be created:", "Full name: ccf954a6cd8e", "User logon name: ccf954a6cd8e@il.cpe.avaya.com", and "The password never expires." Below the text box are three buttons: "< Back", "Finish", and "Cancel".

Click **Finish**.

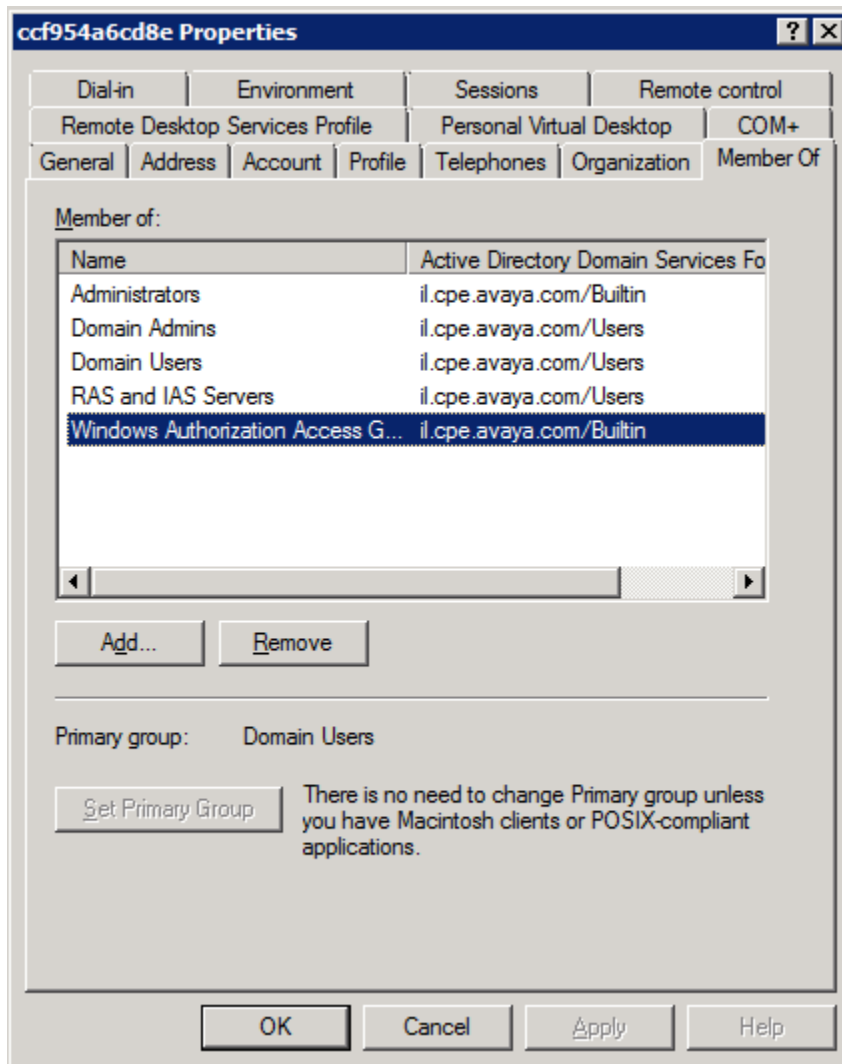
Step 2: Assign the Phone User to Windows Groups

On the **Active Directory Users and Computers** application window double click the phone's user as created in the previous step.

Go to the **Member Of** tab and click **Add...**

Type in the following groups:

RAS and IAS Servers ; Windows Authorization Access Group



Click **OK**.

Click **OK**.

Repeat the above steps for each phone that needs to be authenticated.

6. File Server

The file server is used to hold the phone's firmware, settings and certificate files which the phone will read during its initiation. The phone uses HTTP or HTTPS to access the file server and read these files.

Notes:

- Firmware files are read via HTTP only (default port is 80).
- Settings and certificate files can be read via HTTP or HTTPS (default port 411).
- File server IP address can be manually configured on the phone's CRAFT menu or via DHCP option 242 (HTTPSRVR or TLSSRV parameters). See 96XX Administrator Guide for details.

The file server could be any preferable web server application.

Make sure to place the following files in the web server's document (home) directory:

- Current firmware files (.bin)
- Preferred language files (mlf) - optional
- signatures directory
- Avaya default certificate files (_pem_)
- 96xxupgrade.txt or 96x1Hupgrade.txt scripts
- 46xxsettings.txt file
- Root certificate (.cer) file, as exported from the CA server in section 1 of this document.

The firmware files, language files, signature directory, Avaya certificates and upgrade scripts should be extracted from the firmware packaged zip or tar.gz file (can be obtained from <http://support.avaya.com> website).

Note:

The file server configuration is out of scope of this document.

The description and the content of the 46xxsettings.txt file is explained in the section 8.

7. LAN Switch Configuration

The LAN switch is the device responsible, among its other duties, to provide access control to the network. It acts as RADIUS client by asking the phone for credentials and requesting the access permission from the RADIUS server on behalf of the phone.

Below is a configuration example for Avaya Ethernet Routing Switch 4000 series (only 802.1X relevant configuration is shown here):

```
! Embedded ASCII Configuration Generator Script

! Model = Ethernet Routing Switch 4850GTS-PWR+

! Software version = v5.6.0.008

! Configure the RADIUS server IP address:

radius server host 149.49.139.115

! Configure the RADIUS server shared key:

radius server host key "123456789"

!

eapol enable
interface FastEthernet ALL

! The uplink port with forced authentication:

eapol port 25 re-authentication enable re-authentication-period 60

! The supplicant port with EAP-TLS 802.1X authentication, the phone will be
connected to:

eapol port 1 status auto re-authentication enable re-authentication-period 60
quiet-interval 10
```

Notes:

- Make sure that only client attached ports are enabled with 802.1X authentication. Defining uplink ports with 802.1X authentication may cause network outage.
- Avaya 9600 series phones support other vendor 802.1X standard compliant LAN switches, not just Avaya branded LAN switches.

8. Phone's Configuration and Settings

The relevant phone's configuration parameters are defined in the phone's setting file – 46xxsettings.txt. As stated in the previous section, this file has to be placed on the file server and be available for the phone to download it when it initiates.

This section describes how to set up the Avaya 9600 phone to work with EAP-TLS authentication for 802.1X.

The phone configuration will be performed in two phases: **Staging** and **Production**.

During the staging phase we will configure the phone to load the required settings from the file server, obtain the required certificates and store them in the NVRAM, ready for use from now on. This stage is required in most cases, as usually production networks with access control (i.e. 802.1X) will not allow access to network resources without successful authentication. But since in order to authenticate the phone needs to have the certificates first, it will obtain them through the staged network. When all certificates and the configurations are in place we will be ready to connect the phone to the production network.

This document will guide you through both phases.

Step 1: Configure the Settings File for Staging

This step describes the parameters that are required to be included in the 46xxsettings.txt file:

Note:

There are many other related parameters that are optional. They are not described in this section. For a description of all available configuration parameters please refer to the 96XX Administrators Guide.

- Configure 802.1X to EAP-TLS authentication:

```
SET DOT1XEAPS TLS
```

- Configure the identification method.

The following example is identification based on phone's MAC address in the domain

il.cpe.avaya.com:

```
SET MYCERTCN $MACADDR@il.cpe.avaya.com
```

The following example is identification based on phone's Serial Number in the domain

il.cpe.avaya.com:

```
SET MYCERTCN $SERIALNO@il.cpe.avaya.com
```

Note:

Only one identification method is supported at a time (MAC based or serial number based).

- Configure the phone to download its own certificate using SCEP from the CA server and store it in its NVRAM. The following example relates to Microsoft AD CS which uses 149.49.139.115 IP address:

```
SET MYCERTURL http://149.49.139.115/certsrv/mscep/mscep.dll
```

- Provide the phone the CA root certificate, as was downloaded from the CA server in previous section. This certificate file must be available for the phone on the file server. In the following example the certificate file name is **certnew.cer**:

```
SET TRUSTCERTS certnew.cer
```

- Configure the key length, which is 2048 bits in our example (default is 1024 bits):

```
SET MYCERTKEYLEN 2048
```

- Enable 802.1X:

```
SET DOT1XSTAT 2
```

Note:

- The valid values for DOT1XSTAT paramter are:
 - 0 - Supplicant disabled (default, unless indicated otherwise below)
 - 1 - Supplicant enabled, but responds only to received unicast EAPOL messages
 - 2 - Supplicant enabled; responds to received unicast and multicast EAPOL messages
- Another option is to enable 802.1X through the phone's CRAFT menu. This setting will be stored in the phone's NVRAM. But that has to be done after passing through the staging phase in step 2 below.

Step 2: Connect the Phone to a Staged Network

Connect a new phone (or a phone with **cleared** values , by selecting CLEAR in the CRAFT menu) to a staged network. The staged network should have no 802.1X authentication and it should allow the phone with HTTP/HTTPS access to the file server and the CA server. Make sure phone's IP settings are configured properly.

Note:

You can configure the phone's IP parameters manually (as well as the file server address) from the phone's CRAFT menu or setup DHCP for automatic IP allocation. In that case the file server should be configured via DHCP option 242 by using the HTTPSRRV or TLSSRRV parameter (see 96XX Administrator Guide for details).

When the phone initiates on the staged network it will download the 46xxsettings.txt file and the root certificate from the file server and obtain its own certificate from the CA server using SCEP protocol.

During the phone's initiation process, it will display the files it tries to download and the download result. A "HTTP: 1 200" result means a successful download. You should track the phone's display and make sure you see "HTTP: 1 200" response after each download attempt of the following files:

- 96xxupgrade.txt or 96x1Hupgrade.txt file
- 46xxsettings.txt file
- Root certificate (certnew.cer file in our example)

If one of the above failed to download successfully, check your file server configuration and repeat this step until successful completion.

Note:

Any other response code than "HTTP:1 200" means unsuccessful file download. You will not be able to proceed until all the above files are downloaded successfully.

After the phone has successfully completed downloading the root certificate it will proceed to the certificate enrollment.

Upon successful enrollment the phone will display the following message:

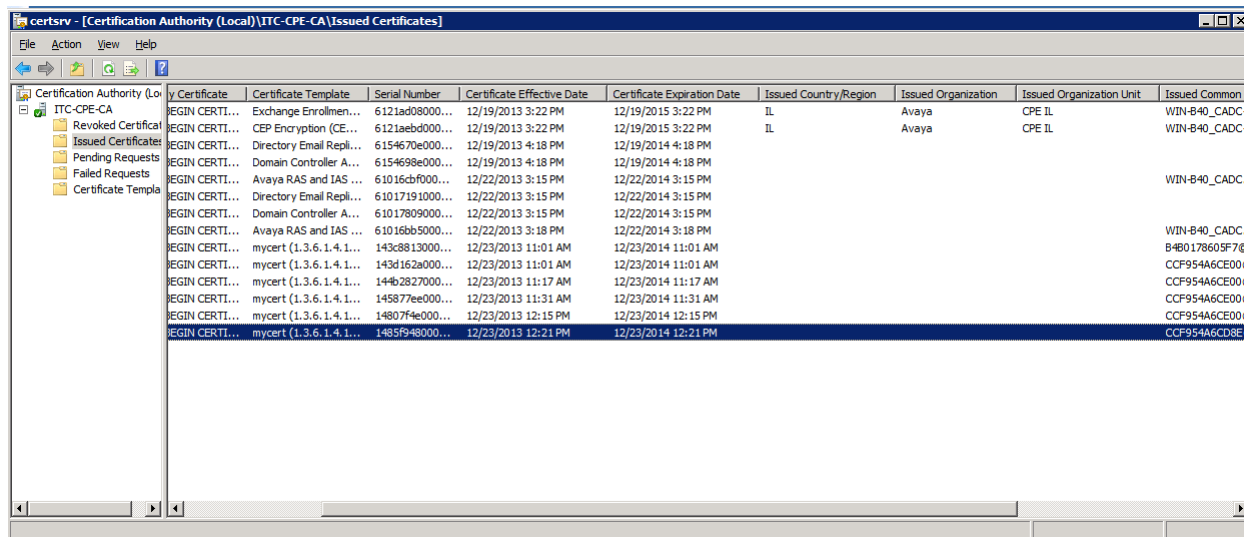
SCEP: Successful

You can also see the certificate allocation on the AD CS server:

Launch the Certification Authority application by clicking on Start Menu->Administrative Tools->Certification Authority

Click **Issued Certificates**.

All issued certificates are listed, as well as the phone's based on its MAC address (or serial number).



The screenshot shows the 'certsrv - [Certification Authority (Local)]\ITC-CPE-CA\Issued Certificates' window. The left pane shows the tree structure with 'Issued Certificates' selected. The main pane displays a table of issued certificates.

Issued Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration Date	Issued Country/Region	Issued Organization	Issued Organization Unit	Issued Common Name
EGIN CERTI...	Exchange Enrollmen...	6121ad08000...	12/19/2013 3:22 PM	12/19/2015 3:22 PM	IL	Avaya	CPE IL	WIN-B40_CADC...
EGIN CERTI...	CEP Encryption (CE...	6121aebd000...	12/19/2013 3:22 PM	12/19/2015 3:22 PM	IL	Avaya	CPE IL	WIN-B40_CADC...
EGIN CERTI...	Directory Email Repl...	6154670e000...	12/19/2013 4:18 PM	12/19/2014 4:18 PM				
EGIN CERTI...	Domain Controller A...	6154698e000...	12/19/2013 4:18 PM	12/19/2014 4:18 PM				
EGIN CERTI...	Avaya RAS and IAS ...	61016cbf000...	12/22/2013 3:15 PM	12/22/2014 3:15 PM				WIN-B40_CADC...
EGIN CERTI...	Directory Email Repl...	61017191000...	12/22/2013 3:15 PM	12/22/2014 3:15 PM				
EGIN CERTI...	Domain Controller A...	61017809000...	12/22/2013 3:15 PM	12/22/2014 3:15 PM				
EGIN CERTI...	Avaya RAS and IAS ...	61016bb5000...	12/22/2013 3:18 PM	12/22/2014 3:18 PM				WIN-B40_CADC...
EGIN CERTI...	mycert (1.3.6.1.4.1...	143c8813000...	12/23/2013 11:01 AM	12/23/2014 11:01 AM				B4B0178605F70...
EGIN CERTI...	mycert (1.3.6.1.4.1...	143d162a000...	12/23/2013 11:01 AM	12/23/2014 11:01 AM				CCF954A6CE000...
EGIN CERTI...	mycert (1.3.6.1.4.1...	14462827000...	12/23/2013 11:17 AM	12/23/2014 11:17 AM				CCF954A6CE000...
EGIN CERTI...	mycert (1.3.6.1.4.1...	145877ee000...	12/23/2013 11:31 AM	12/23/2014 11:31 AM				CCF954A6CE000...
EGIN CERTI...	mycert (1.3.6.1.4.1...	148077fe000...	12/23/2013 12:15 PM	12/23/2014 12:15 PM				CCF954A6CE000...
EGIN CERTI...	mycert (1.3.6.1.4.1...	1485f948000...	12/23/2013 12:21 PM	12/23/2014 12:21 PM				CCF954A6CD8E0...

The phone will store the root certificate and its issued certificate in its non-volatile memory (NVRAM) and use them until these files are overwritten, the phone is cleared to factory defaults or certificate renewal is required.

Note:

In case of certificate issuing failure the phone will display "SCEP: Failed" message. This will be logged in **Certification Authority** application under **Failed Requests** screen. Use the **Event Viewer** application, under **Windows Logs\Application**, for more detailed logs.

Step 3: Place the Phone on the Production Network

Take out the phone from the staged network and place it on the production network. Make sure phone's IP settings are configured properly.

Note:

You can configure the phone's IP parameters manually (as well as the file server address) from the phone's CRAFT menu or setup DHCP for automatic IP allocation. In that case the file server should be configured via DHCP option 242 by using the HTTPSRVR or TLSSVR parameter (see 96XX Administrator Guide for details).

In the production network your LAN switch the phone is attached to, should support 802.1X authentication and should be properly configured as a RADIUS client on the RADIUS server (see section 7 for LAN switch configuration example).

In EAP-TLS authentication method, the phone is authenticated with its obtained certificate based on its serial number or MAC address. So the user will not be prompted for 802.1X user/password (as in MD5).

Upon successful authentication the phone will communicate with the file server, check for the latest available firmware, download the 46xxsettings.txt file and register to Communication Manager.

9. Troubleshooting

If things don't work as expected, there are few procedures you can do in order to troubleshoot the problem, or at least to obtain information that will assist in the troubleshooting process.

Problem	Action
The phone is displaying "HTTP: 1-1" message during start up	<p>The phone has failed to reach the file server.</p> <ul style="list-style-type: none"> - Check for HTTP or HTTPS server configuration in the phone's IP settings (manual setting or DHCP option 242). - Check the file server reachability. - Make sure the HTTP service is up and running and with the correct TCP port (default port for HTTP is 80 and for HTTPS is 411).
The phone is displaying "HTTP: 1 404" message during start up	<p>The phone has failed to download a file from the file server.</p> <ul style="list-style-type: none"> - Before it displayed this message the phone displayed a message indicating which file it tried to download. Reboot the phone and track which file it tried to download before displaying this message. - Make sure the requested file exists on the file server's home directory.
The phone is displaying "SCEP: Failed" message	<p>The phone has failed to obtain the valid certificate from the CA server (AD CS).</p> <ul style="list-style-type: none"> - Open a web browser on your PC, and go to the following URL: http://CA-SERVER-IP/certsrv/mscep/mscep.dll. Enter ipclients user credentials. If you are not getting "Network Device Enrollment Service" page then your CA server is not working properly. Go back to section 3 and make sure you have completed all the steps. - Make sure to connect the phone to an open switch port (where 802.1X authentication is disabled) and that the phone can reach the CA server, as required in the staging state (see section 7). Ping the phone from the CA server to make sure the network connection is good. If ping fails check the network connectivity. - On the AD CS server, go to Start Menu->Administrative Tools->Certification Authority. Click CA name and browse to Failed Requests. Look at the Request Common Name column and find the phone's MAC address or serial number to locate the relevant entry. The Request Status Code column should state the reason for the certificate allocation failure. - Review the 46xxsettings.txt file. - Upon successful certificate allocation, the phone's details will be recorded in the Issued Certificates section.
The phone is displaying "802.1x Failure" message	<p>Phone fails to successfully perform 802.1X authentication.</p> <ul style="list-style-type: none"> - Open the Active Directory Users and Computers application and

	<p>make sure you have the correct phone user definition, as described in section 5.</p> <ul style="list-style-type: none"> - Make sure the phone has successfully loaded the valid root certificate file from the CA server during the staging phase in section 7. - All successful and failed access attempts are logged on the server and can be reviewed by the Event Viewer application, under Custom Views\Server Roles\Network Policy and Access Services section.
The phone is displaying "Waiting for 802.1x authentication..." message	<p>The phone is expecting the LAN switch to send EAPOL to initiate the 802.1X authentication process.</p> <ul style="list-style-type: none"> - Check the LAN switch 802.1X (EAPOL) configuration on the physical port the phone is attached to. - Check the LAN switch RADIUS server configuration and its reachability. - Go back to staging state (section 7) and make sure your 46xxsettings.txt file includes SET DOT1XWAIT 0. It will make the phone to continue its normal initiation process without waiting for 802.1X authentication to complete. It should resume to normal operation after approximately one minute.
The phone is displaying "Discovering" message	<p>The phone can't register to Communication Manager as it is unable to reach it.</p> <ul style="list-style-type: none"> - Check phone's network connectivity and the validity of its IP parameters as were obtained from DHCP server or as were manually configured. - Make sure the switch LAN port to which the phone is attached is properly configured. - Reboot the phone and follow its initiation. See if the 802.1X authentication was successfully completed. If there were no related 802.1X messages displayed then go back to the staging phase (section 7) and make sure the phone has loaded the required configuration.

Additional resources you can use:

- Avaya one-X Deskphone H.323 96x1 Administrator Guide, 13-300698
- Avaya one-X Deskphone SIP 96x1 Administrator Guide, 13-601944
- Avaya one-X Deskphone 9600 Series Administrator Guide, 16-300698
- Microsoft Windows Server 2008 R2 help:

<http://technet.microsoft.com/en-us/library/dd851728.aspx>