



Configuring Microsoft Windows Server 2008 R2 Certificate Authority and Network Device Enrollment Service with Simple Certificate Enrollment Protocol for use with Avaya 96x1 IP Telephones in VPN Mode - Issue 1.0

Abstract

These Application Notes describes the configuration steps required to configure Microsoft Windows 2008 R2, Enterprise Edition, Certificate Authority and Network Device Enrollment Service certificate enrollment using Simple Certificate Enrollment Protocol for use with Avaya 96x1 IP Telephones in VPN Mode for remote, secure communications access.

Table of Contents

1.	Introduction	3
2.	Interoperability Testing	3
2.1.	Test Description and Coverage	3
2.2.	Test Results and Observations.....	3
3.	Test Configuration.....	4
4.	Equipment and Software Validated.....	5
5.	Install Microsoft Server 2008 Roles.....	6
5.1.	Install Microsoft Certificate Authority	7
5.2.	Install and Configure Network Device Enrollment Service.....	23
5.3.	Disable SCEP Password	45
5.4.	Create New Template for IPSec	47
5.5.	Issue Certificate Template.....	63
5.6.	Export Certificate to .CER file	66
5.7.	Execute setspn	73
6.	Configuration of Avaya 96x1 IP Telephones	74
6.1.	Configuration of 46xxsettings	74
6.2.	Upload Certificates to 96x1 IP Telephone	76
7.	Verification Steps	77
7.1.	Verify Staging	77
7.2.	Verify registration with Avaya Aura® Communication Server.....	77
7.3.	Verify IP Phone can Send and Receive Calls.....	77
8.	Conclusion.....	77
9.	Additional References	78

1. Introduction

These Application Notes document the configuration required for a Windows Server 2008 R2, Enterprise Edition, to become a Microsoft Certificate Authority and to authenticate devices using the Network Device Enrollment Service (NDES) with Simple Certificate Enrollment Protocol (SCEP). These Application Notes assume that Microsoft Server 2008 R2, Enterprise Edition is installed and configured with the Active Directory service.

The Microsoft Certificate Authority (CA) can issue multiple certificates in the form of a tree structure. A root certificate is the top most certificate of the tree, the private key of which is used to sign other certificates. All certificates immediately below the root certificate inherit the trustworthiness of the root certificate. A signature by a root certificate is somewhat analogous to notarizing an identity in the physical world. Certificates further down the tree also depend on the trustworthiness of the intermediates often known as subordinate certification authorities. Many software applications assume these root certificates are trustworthy on the user's behalf.

2. Interoperability Testing

This application note is a companion document to the application notes for **Configuring Avaya 96x1 Series IP Telephone VPN feature with Cisco 5510 Adaptive Security Appliance using Microsoft Windows Server 2008 Certificate Authority and SCEP**. It has been separated to its own application note due to its applicability to other instances where NDES and SCEP may be used.

2.1. Test Description and Coverage

For Interoperability testing IP phone registration was observed while other testing included making bi-directional calls between the staged and existing corporate phones.

2.2. Test Results and Observations

All tests passed. No unusual behavior was noted.

3. Test Configuration

The configuration shown in **Figure 1** is a sample that could be used with Windows Server 2008 R2 with Active Directory, Microsoft Certificate Authority and Network Device Enrollment Service using Simple Certificate Enrollment Protocol. Windows Server 2008 R2 with Microsoft CA and NDES can be used in other instances where SCEP is needed. Over a dozen vendors support the use of NDES and SCEP for authentication.

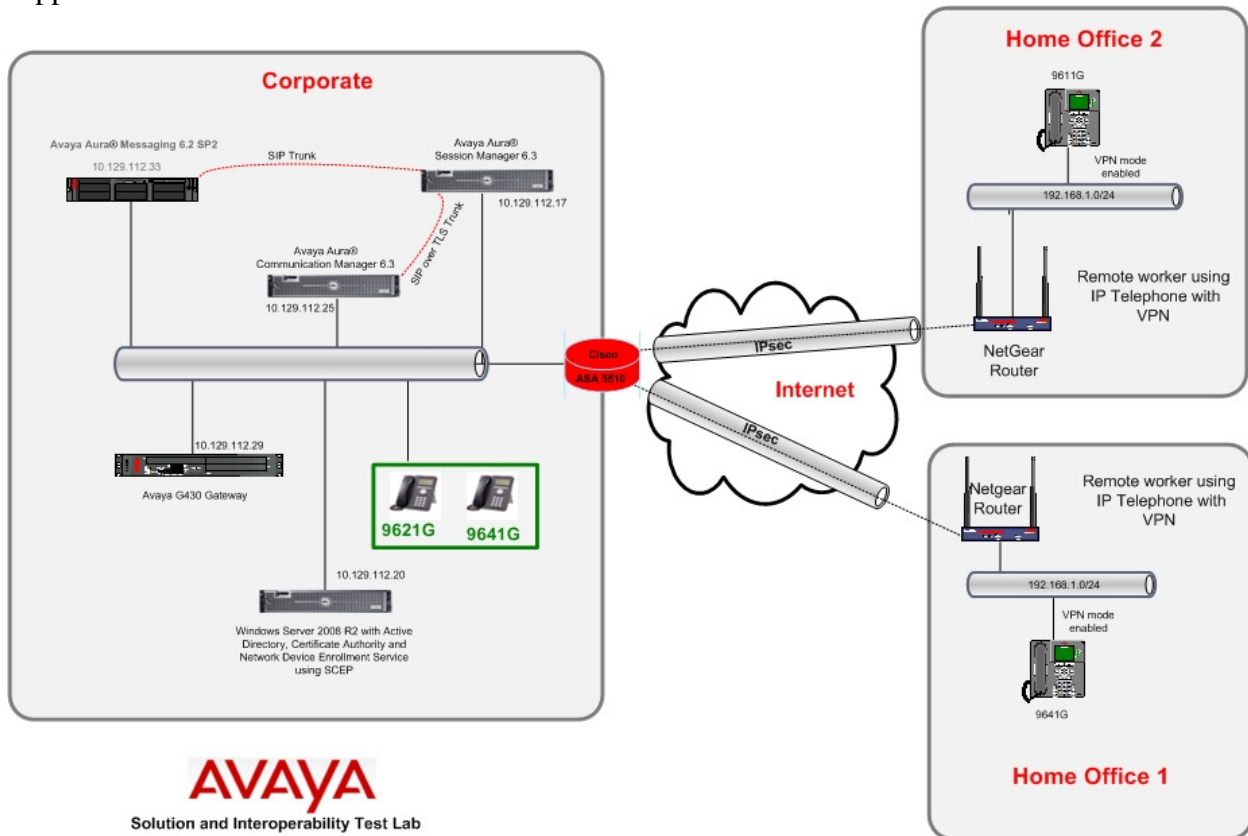


Figure 1: Windows Server 2008 R2 with Active Directory, Microsoft Certificate Authority and Network Device Enrollment Service using SCEP for 96x1 certificate authentication

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya Aura® System Manager on Avaya Server	6.3 (Build 6.3.2.4.1325)
Avaya Aura® Session Manager on Avaya Server	6.3 (Build 6.3.2.0.83005)
Avaya Aura® Communication Manager on Avaya Server	6.3 (Build 6.3.0.120.0)
Avaya Aura® Messaging on Avaya server	6.2 SP2 (Build 06.2-02.0.823.0-109)
Avaya G430 Media Gateway	Firmware 32.26.0
Avaya 9641G IP Telephone (H.323)	Release 6.2.3.13
Avaya 9611G IP Telephone (H.323)	Release 6.2.3.13
Dell PowerEdge R200 Server	Microsoft Windows Server 2008 R2, Enterprise Edition

5. Install Microsoft Server 2008 Roles

It is assumed that Microsoft Server 2008 R2, Enterprise Edition, with Active Directory and DNS is already installed. Post-installation of the Windows Server 2008 R2, Enterprise Edition, configuration steps may include the following:

- Change user password
- Set time zone
- Configure networking
- Provide Computer name and domain
- Enable automatic updates
- Download and install updates
- Enable remote desktop
- Configure windows firewall

Installation of the Active Directory services on the Windows Server 2008 R2 Enterprise Edition, include the following:

- Install **Active Directory services**
- Promote the server to a domain controller. (Go to **Server Manager** → **Active Directory Services** and scroll down to **Advanced Tools**. Select **Dcpromo.exe**.)

Additional tasks that must be performed are:

- Install Microsoft Certificate Authority
- Install Network Device Enrollment Service

To access the Windows 2008 Server, open a remote desktop connection and input the IP Address of the Windows 2008 Server. This was **10.129.112.20**. Press **Connect** to access the Windows 2008 Server.



Log in with the appropriate User name and password. The default administrative user is **Administrator**.

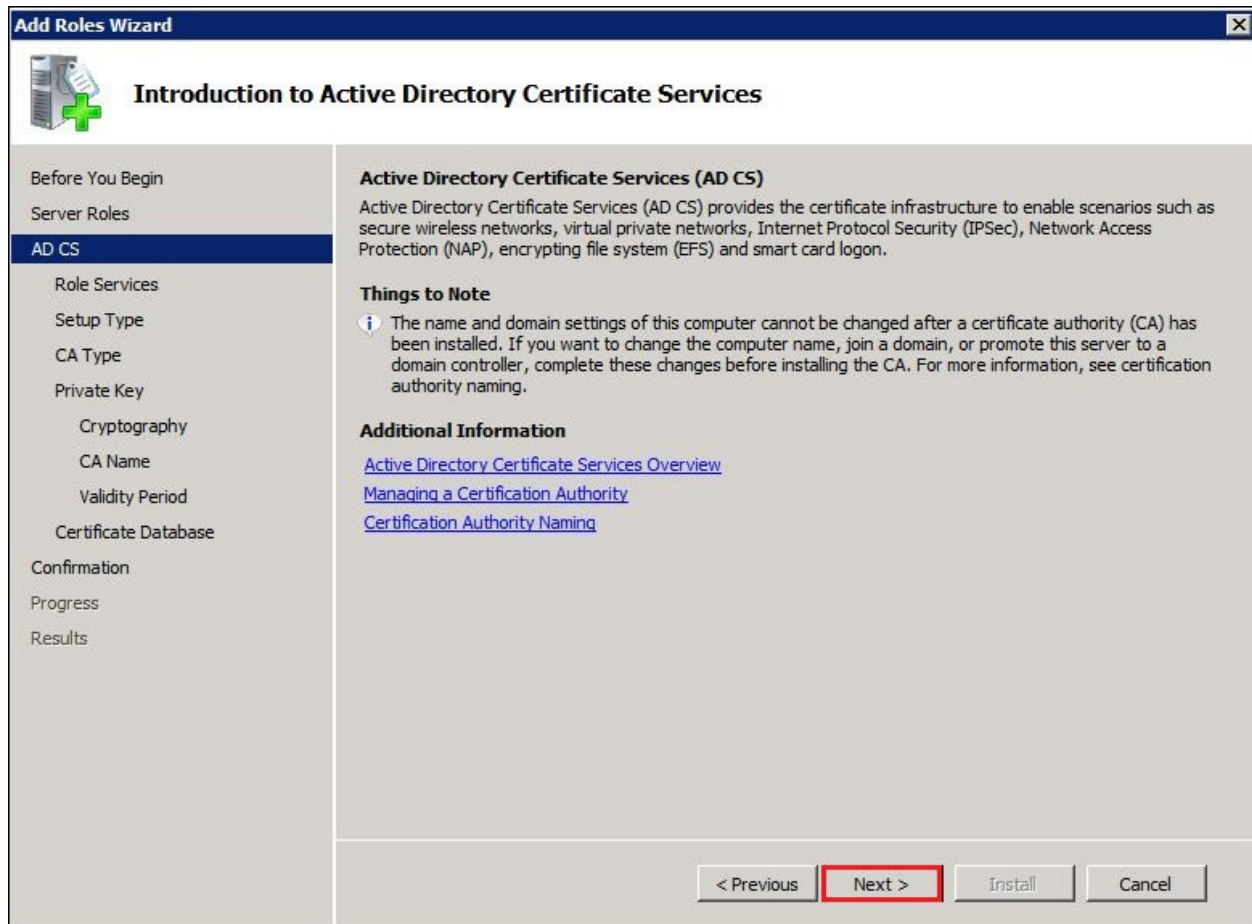
5.1. Install Microsoft Certificate Authority

Go to **Start** → **Administrative Tools** → **Server Manager**. Select **Server Manager**. Once the window for Server Manager opens, go to **Roles Summary**, and select **Add Roles**. A window will open for the Add Roles Wizard, Select **Next** (not shown).

Place a check by **Active Directory Certificate Services**. Click **Next**. See below.

The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard'. The main heading is 'Select Server Roles'. On the left, a navigation pane lists steps: 'Before You Begin', 'Server Roles' (selected), 'AD CS', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'Select one or more roles to install on this server.' and contains a list of roles. The 'Active Directory Certificate Services' role is checked and highlighted with a red box. Other roles include 'Active Directory Domain Services (Installed)', 'Active Directory Federation Services', 'Active Directory Lightweight Directory Services', 'Active Directory Rights Management Services', 'Application Server', 'DHCP Server', 'DNS Server (Installed)', 'Fax Server', 'File Services', 'Hyper-V', 'Network Policy and Access Services', 'Print and Document Services', 'Remote Desktop Services', 'Web Server (IIS)', 'Windows Deployment Services', and 'Windows Server Update Services'. To the right, a 'Description:' section explains that 'Active Directory Certificate Services (AD CS)' is used for creating certification authorities and related services. At the bottom, there are four buttons: '< Previous', 'Next >' (highlighted with a red box), 'Install', and 'Cancel'. A link 'More about server roles' is also present.

This is an informational screen. Click **Next**.



Check **Certification Authority**, **Certification Authority Web Enrollment**, **Online Responder** and **Certificate Enrollment Policy Web Service**. Network Device Enrollment Service and Certificate Enrollment Web Service cannot be installed at the same time as the Certificate Authority so will be installed later. Click **Next**.

Add Roles Wizard

Select Role Services

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

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

Role services:

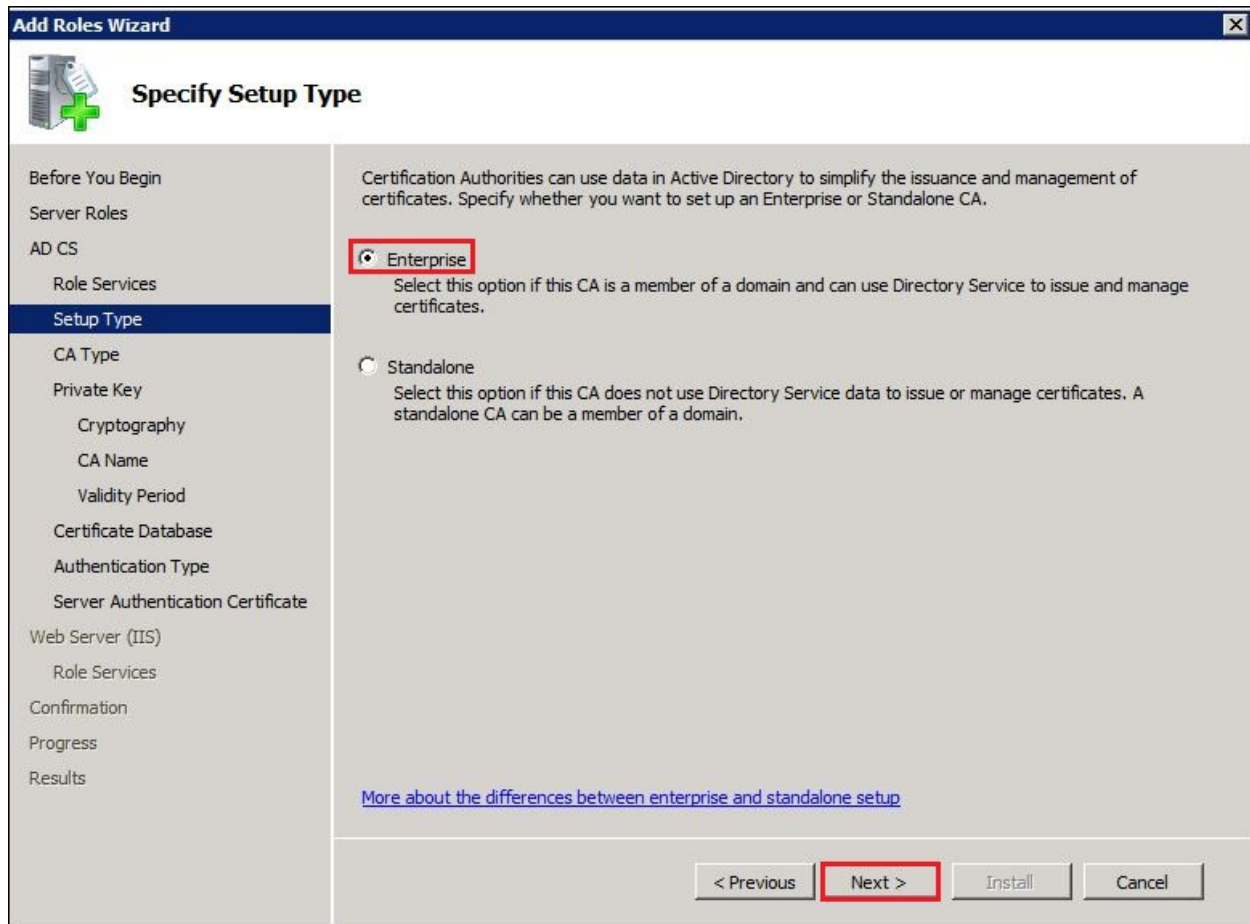
- ☒ Certification Authority
- ☒ Certification Authority Web Enrollment
- ☒ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☒ Certificate Enrollment Policy Web Service

Description:
The [Certificate Enrollment Policy Web Service](#) enables users and computers to obtain certificate enrollment policy information even when the computer is not a member of a domain or if a domain-joined computer is temporarily outside the security boundary of the corporate network. The Certificate Enrollment Policy Web Service works with the Certificate Enrollment Web Service to provide policy-based automatic certificate enrollment for these users and computers.

[More about role services](#)

< Previous **Next >** Install Cancel

For the sample configuration **Enterprise** was selected. 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
 Authentication Type
 Server Authentication Certificate
Web Server (IIS)
 Role Services
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

Install as a Root Certificate Authority. Select **Root CA** and click on **Next**.

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
 Authentication Type
 Server Authentication Certificate
Web Server (IIS)
 Role Services
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

Create a Private Key for the new Certificate Authority. Select **Create a new private key**. Click on **Next**.

Add Roles Wizard

Set Up Private Key

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

To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

☒ **Create a new private key**
Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

☐ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

☐ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about public and private keys](#)

< Previous **Next >** Install Cancel

The Configure Cryptography for CA screen is displayed.

- **Select a cryptographic service provider (CSP):** RSA#Microsoft Software key Storage Provider
- **Key character length:** 2048
- **Hash Algorithm for signing certificates:** SHA1

Click on **Next**.

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 Cryptography for CA'. 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' (highlighted with a blue bar), 'CA Name', 'Validity Period', 'Certificate Database', 'Authentication Type', 'Server Authentication Certificate', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main area contains the following text: 'To create a new private key, you must first select a [cryptographic service provider](#), [hash algorithm](#), and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.' Below this text are two dropdown menus: 'Select a cryptographic service provider (CSP):' with 'RSA#Microsoft Software Key Storage Provider' selected, and 'Key character length:' with '2048' selected. Below these is a list box for 'Select the hash algorithm for signing certificates issued by this CA:' with 'SHA1' selected. Below the list box is a checkbox labeled 'Allow administrator interaction when the private key is accessed by the CA.' which is unchecked. At the bottom of the main area is a link: '[More about cryptographic options for a CA](#)'. At the bottom of the window are four buttons: '< Previous', 'Next >' (highlighted with a red box), 'Install', and 'Cancel'.

Accept the default **Common name for this CA** by Clicking on **Next**.

Add Roles Wizard

Configure CA Name

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

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.

Common name for this CA:
avayasil-WINDNS0-CA

Distinguished name suffix:
DC=avayasil,DC=avaya,DC=com

Preview of distinguished name:
CN=avayasil-WINDNS0-CA,DC=avayasil,DC=avaya,DC=com

[More about configuring a CA name](#)

< Previous **Next >** Install Cancel

Determine the length of time that the certificates will be valid. 5 years is the default value. Click **Next**.

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' (expanded), 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period' (highlighted with a blue bar), 'Certificate Database', 'Authentication Type', 'Server Authentication Certificate', 'Web Server (IIS)', 'Role Services', '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 dropdown menu showing '5 Years'. The '5' and 'Years' are highlighted with red boxes. Below the dropdown, it says 'CA expiration Date: 4/11/2018 8:18 AM' and '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 >' (highlighted with a red box), '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
Authentication Type
Server Authentication Certificate
Web Server (IIS)
Role Services
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: 4/11/2018 8:18 AM
Note that CA will issue certificates valid only until its expiration date.

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

< Previous **Next >** Install Cancel

Accept the default location for the Certificate Database and Certificate Database Log by clicking **Next**.

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 main 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', 'Certificate Database' (highlighted with a blue bar), 'Authentication Type', 'Server Authentication Certificate', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main content area is titled 'Configure Certificate Database' and 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 text are two input fields. The first is labeled 'Certificate database location:' and contains the text 'C:\Windows\system32\CertLog', which is highlighted with a red box. To its right is a 'Browse...' button. Below this is a checkbox labeled 'Use existing certificate database from previous installation at this location', which is unchecked. The second input field is labeled 'Certificate database log location:' and also contains the text 'C:\Windows\system32\CertLog', which is highlighted with a red box. To its right is another 'Browse...' button. At the bottom of the window, there are four buttons: '< Previous', 'Next >' (highlighted with a red box), 'Install', and 'Cancel'.

Add Roles Wizard

Configure Certificate Database

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

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.

Certificate database location:
C:\Windows\system32\CertLog Browse...

☐ Use existing certificate database from previous installation at this location

Certificate database log location:
C:\Windows\system32\CertLog Browse...

< Previous **Next >** Install Cancel

To use Avaya 96x1IP Telephones with certificates installed, Select **Client certificate authentication** and click on **Next**.

Add Roles Wizard

Select Authentication Type

Before You Begin

Server Roles

AD CS

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Authentication Type

Server Authentication Certificate

Web Server (IIS)

Role Services

Confirmation

Progress

Results

Select the type of authentication clients will use when sending requests to the web service(s).

☐ Windows Integrated Authentication

Select this option if clients will only be able to access the web service while connected directly to your internal network.

☒ **Client certificate authentication**

Select this option if you plan to provide users with digital X.509 certificates for client authentication. This option will enable you to make the web service available on the Internet.

☐ Username and password

Select this option if you would like users to enter a username and password to authenticate to the web service. This option can be used when the web service is accessed on the internal network or over the Internet.

< Previous **Next >** Install Cancel

Since this is a standalone server, select **Choose and assign a certificate for SSL later** and Click on **Next**.

Add Roles Wizard

Choose a Server Authentication Certificate for SSL Encryption

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

When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) protocol to encrypt network traffic.
Choose a server authentication certificate suitable for SSL encryption to add to the default website in IIS.

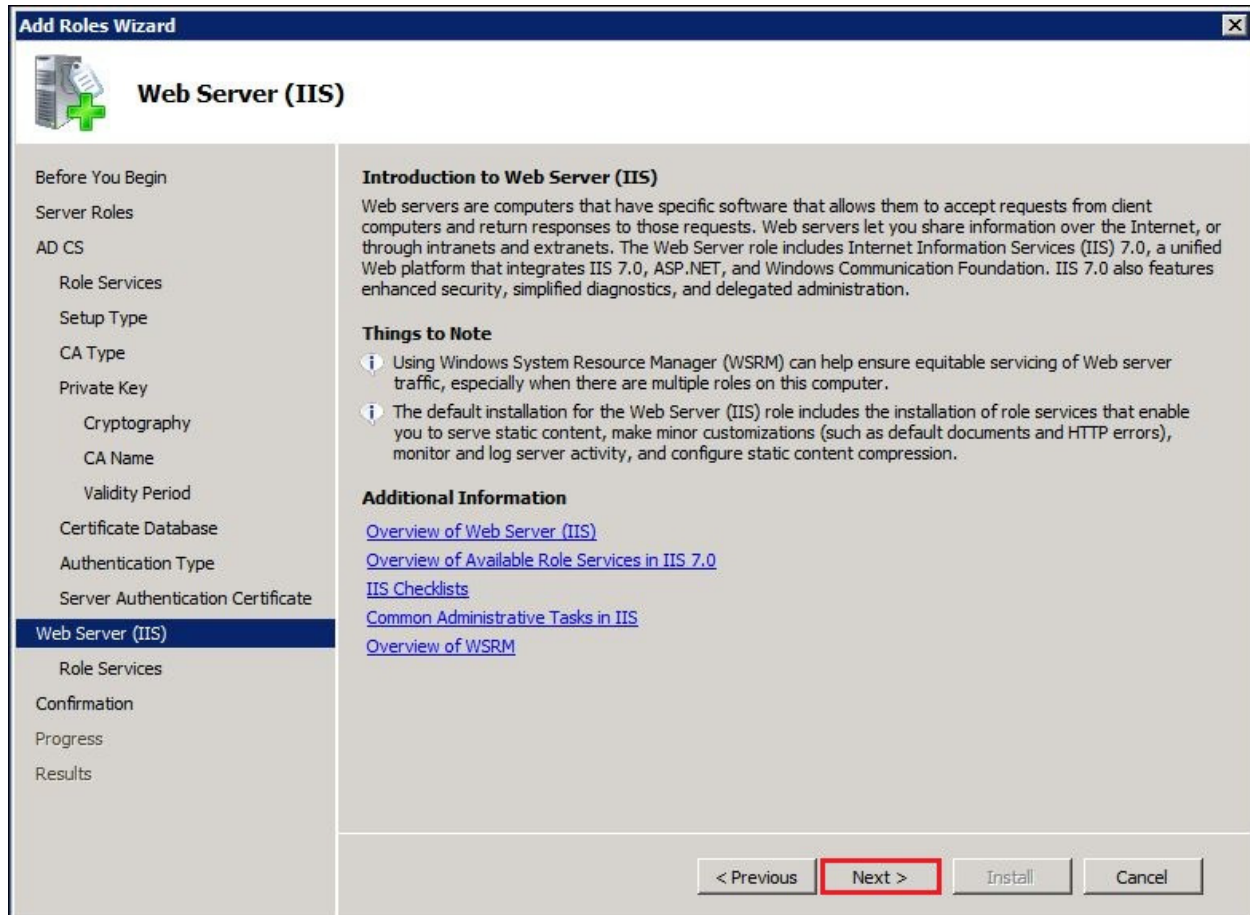
☐ Choose an existing certificate for SSL encryption (recommended)
This option is recommended for most production deployment scenarios. You should use a certificate issued by a certification authority that is trusted by clients connecting to this server. The subject name of the certificate must match the host name of this server.

Issued To	Issued By	Expiration Date	Intended Purpose
-----------	-----------	-----------------	------------------

☒ **Choose and assign a certificate for SSL later**
This option is recommended if you plan to request a certificate from a CA and import it to the local computer personal certificate store on this server later. Once the certificate is imported, use the IIS snap-in to assign the certificate to the default web site.
 For this role service to function, you must configure this server with a valid certificate.

Next >

This screen is informational. Installation of Microsoft's web server, Internet Information Services or IIS, is required for the Microsoft Certificate Authority. Click on **Next**.



To accept the defaults, click on **Next**.

Add Roles Wizard

Select Role Services

Before You Begin

Server Roles

AD CS

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Authentication Type

Server Authentication Certificate

Web Server (IIS)

Role Services

Confirmation

Progress

Results

Select the role services to install for Web Server (IIS):

Role services:

- ☒ Web Server
 - ☒ Common HTTP Features
 - ☒ Static Content
 - ☒ Default Document
 - ☒ Directory Browsing
 - ☒ HTTP Errors
 - ☒ HTTP Redirection
 - ☐ WebDAV Publishing
 - ☒ Application Development
 - ☐ ASP.NET
 - ☒ .NET Extensibility
 - ☒ ASP
 - ☐ CGI
 - ☒ ISAPI Extensions
 - ☐ ISAPI Filters
 - ☐ Server Side Includes
 - ☒ Health and Diagnostics
 - ☒ HTTP Logging
 - ☒ Logging Tools
 - ☒ Request Monitor
 - ☒ Tracing

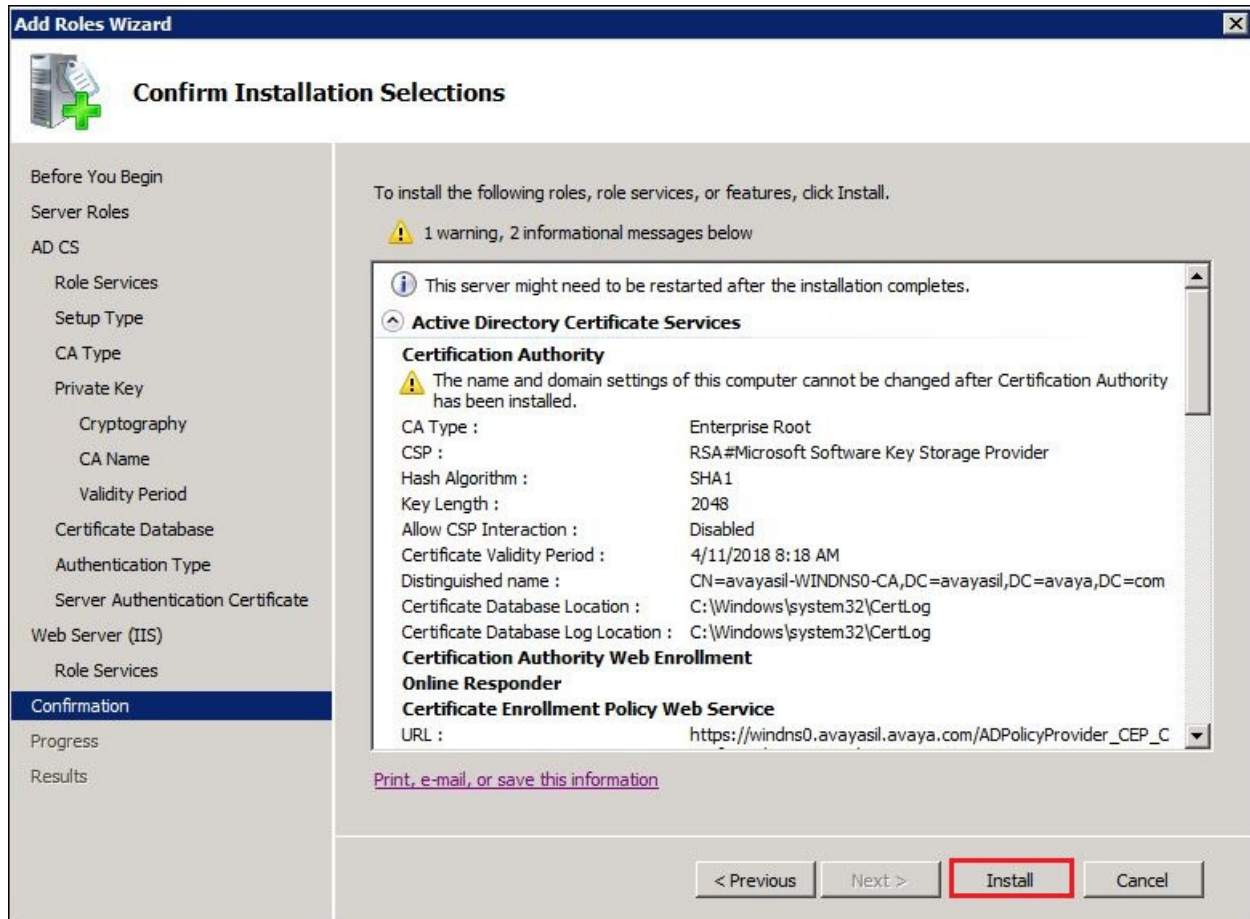
Description:

[Web Server](#) provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

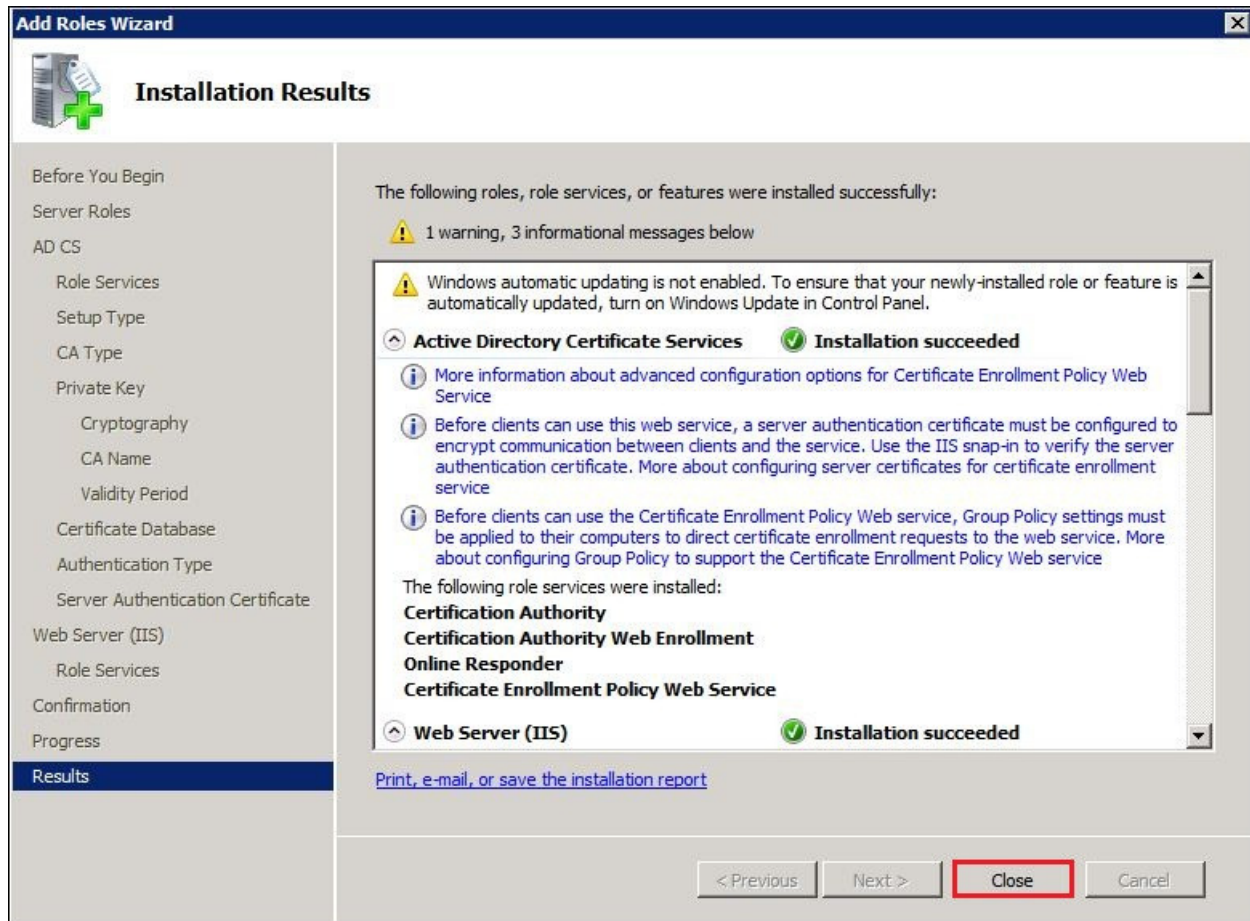
[More about role services](#)

< Previous **Next >** Install Cancel

To **Confirm Installation Selections** and start the installation of Microsoft Certificate Authority and IIS, click on **Install**.



After Installation is completed the following screen is displayed. Click on **Close**.



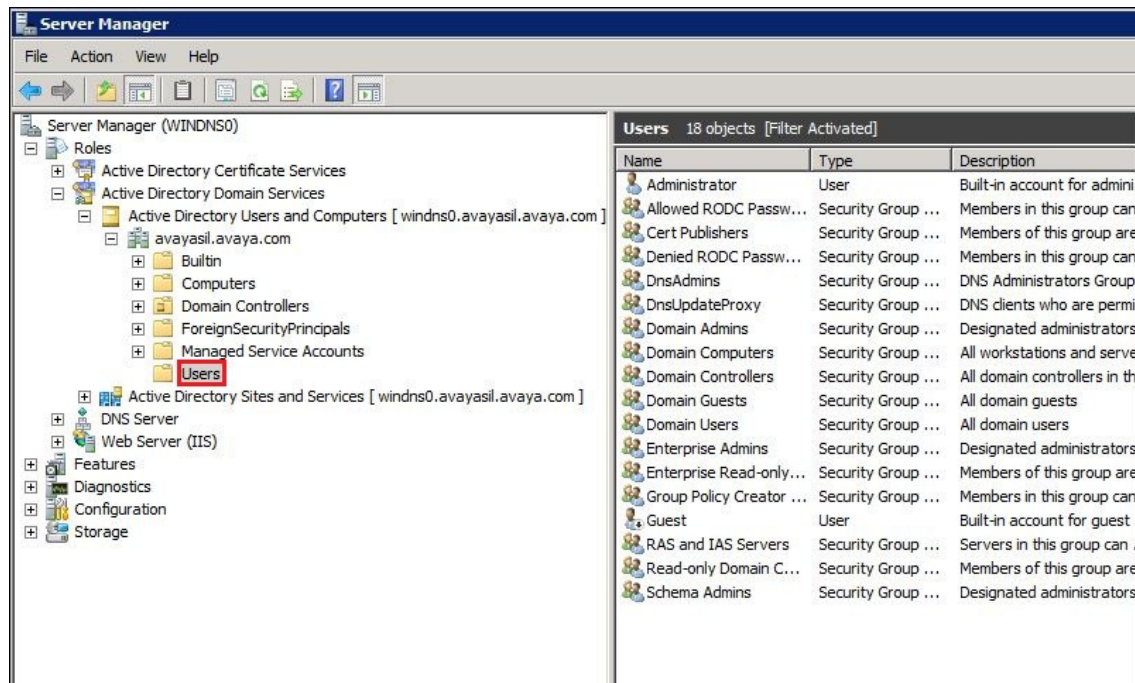
5.2. Install and Configure Network Device Enrollment Service

This section describes how to install the Network Device Enrollment Service on an existing Microsoft Windows Server 2008 R2, Enterprise Edition. It assumes the Windows Server 2008 R2, Enterprise Edition, with Active Directory and Microsoft Certificate Authority is already installed.

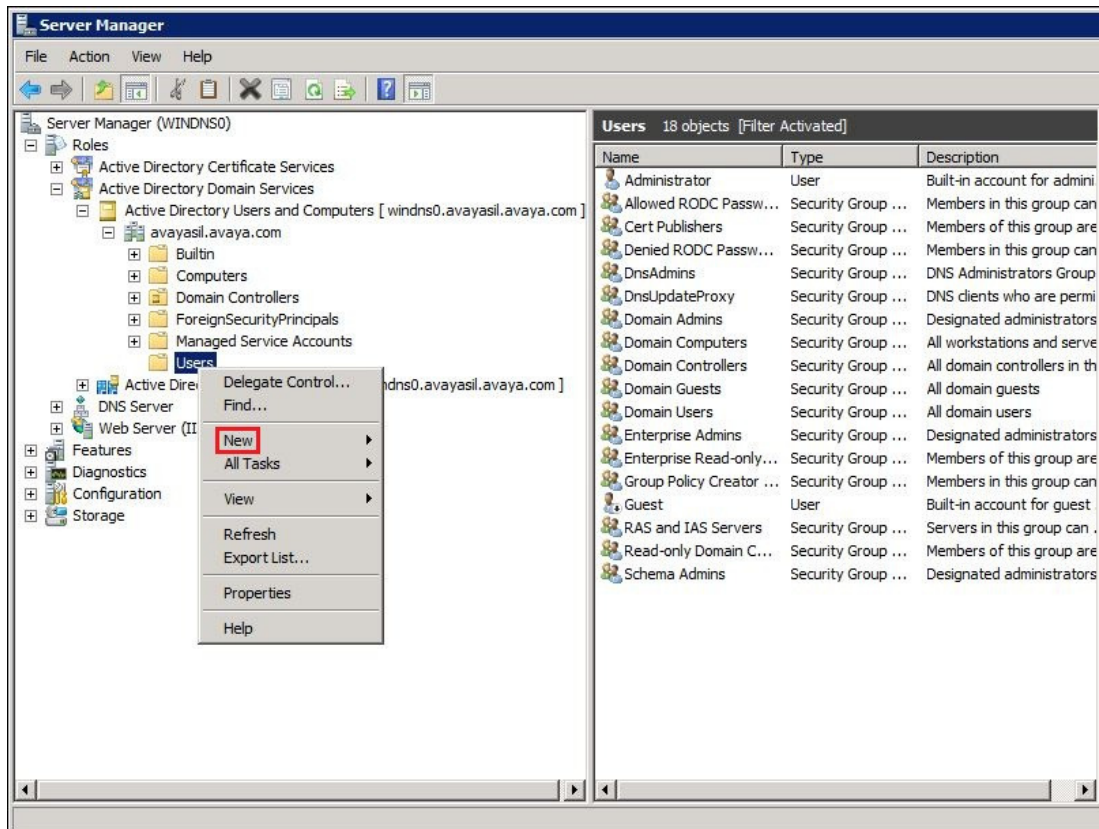
Step 1. Create Service Account User

Three users are required for the Network Device Enrollment Service. In Microsoft's NDES installation documentation these roles are referred to as Service Administrator, Service Account and Device Administrator. For this sample configuration, Administrator was used for Service Administrator and Device Administrator. For the Service Account the user **silcert** was created.

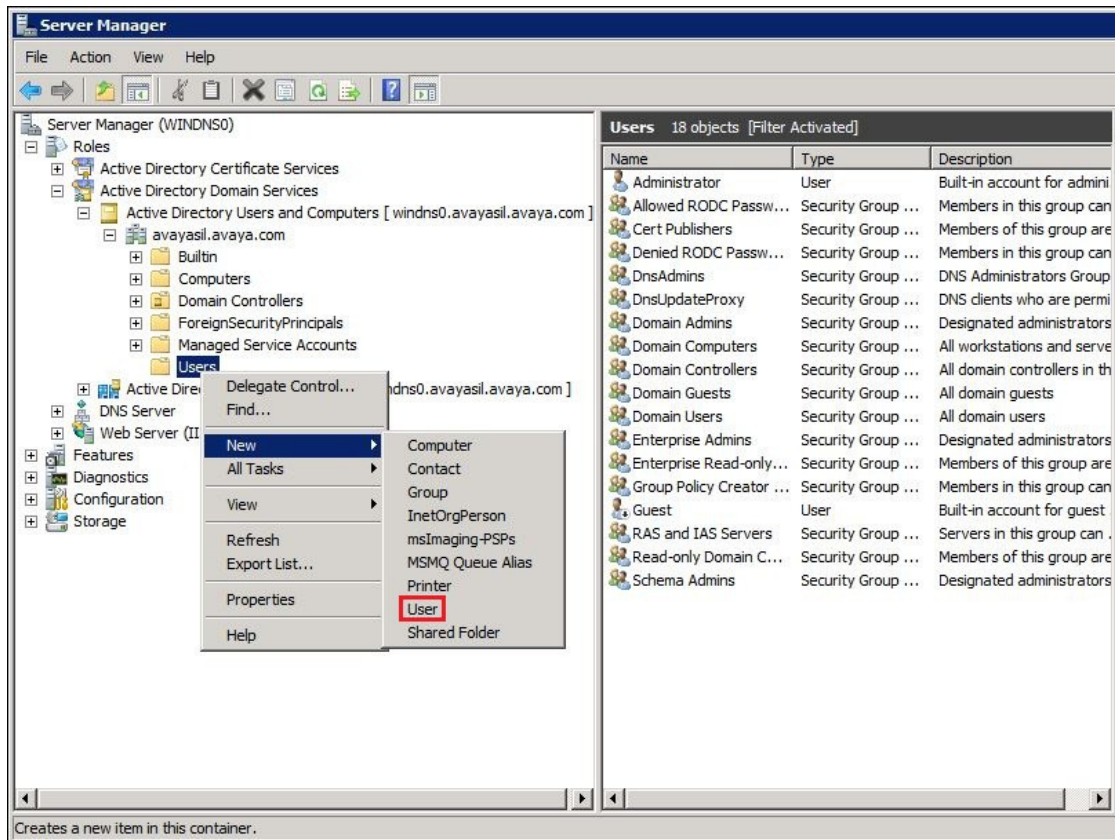
Go to **Server Manager** → **Roles** → **Active Directory Domain Services** → **Active Directory Users and Computers** → **avayasil.avaya.com (the domain)** → **Users**.



To create the user right click on **Users** and select **New**. See below.



Select **User**. See below.



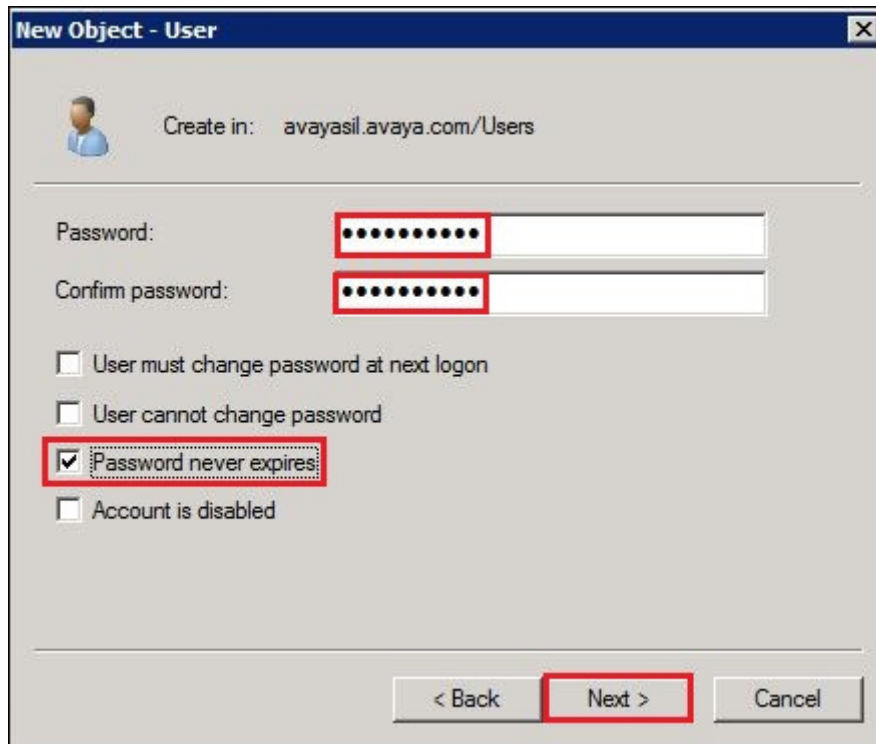
To create the new user:

- **First Name:** Sil
- **Last Name:** Cert
- **User Logon name:** silcert

Click on **Next**.

The screenshot shows a 'New Object - User' dialog box. At the top, it says 'Create in: avayasil.avaya.com/Users'. Below this, there are several input fields: 'First name:' with 'Sil' entered, 'Last name:' with 'Cert' entered, and 'Full name:' with 'Sil Cert' entered. There is also an 'Initials:' field which is empty. Below these, there is a 'User logon name:' section with a text box containing 'silcert' and a dropdown menu showing '@avayasil.avaya.com'. Below that, there is a 'User logon name (pre-Windows 2000):' section with a text box containing 'AVAYASIL\' and another text box containing 'silcert'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

Input a suitable password and check **Password never expires**. Click on **Next**.



The 'New Object - User' dialog box shows the 'Create in' field set to 'avayasil.avaya.com/Users'. The 'Password' and 'Confirm password' fields are filled with dots and are highlighted with red boxes. Below these fields, the 'Password never expires' checkbox is checked and highlighted with a red box. At the bottom, the 'Next >' button is highlighted with a red box.

Create in: avayasil.avaya.com/Users

Password: [dots]

Confirm password: [dots]

☐ User must change password at next logon

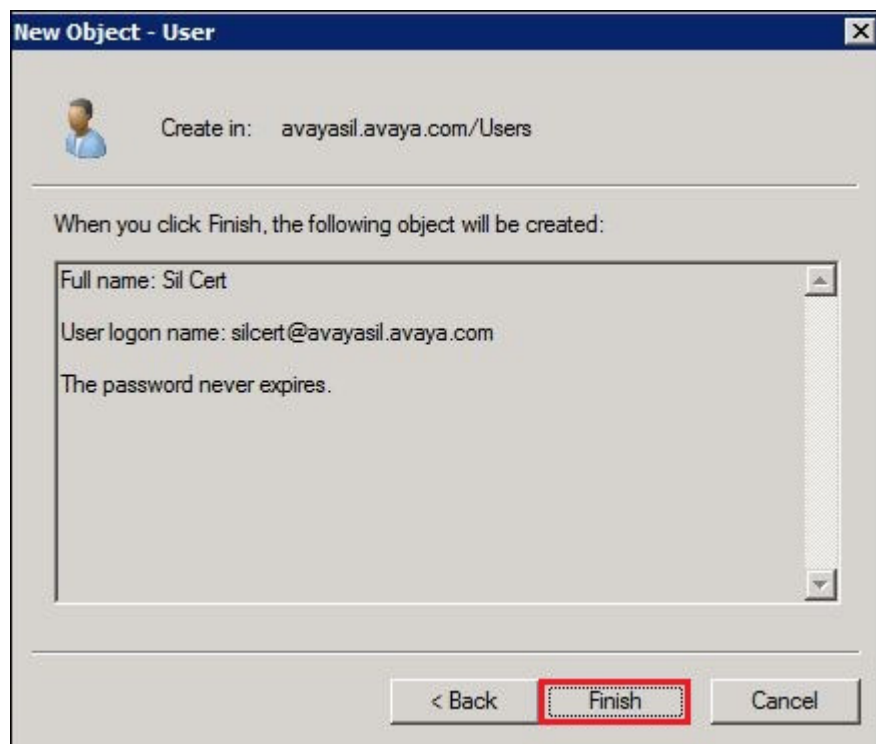
☐ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

Verify user information and click on **Finish** to create the user.



The 'New Object - User' dialog box shows the 'Create in' field set to 'avayasil.avaya.com/Users'. Below the 'Create in' field, the text 'When you click Finish, the following object will be created:' is displayed. A scrollable text area contains the following information: 'Full name: Sil Cert', 'User logon name: silcert@avayasil.avaya.com', and 'The password never expires.' At the bottom, the 'Finish' button is highlighted with a red box.

Create in: avayasil.avaya.com/Users

When you click Finish, the following object will be created:

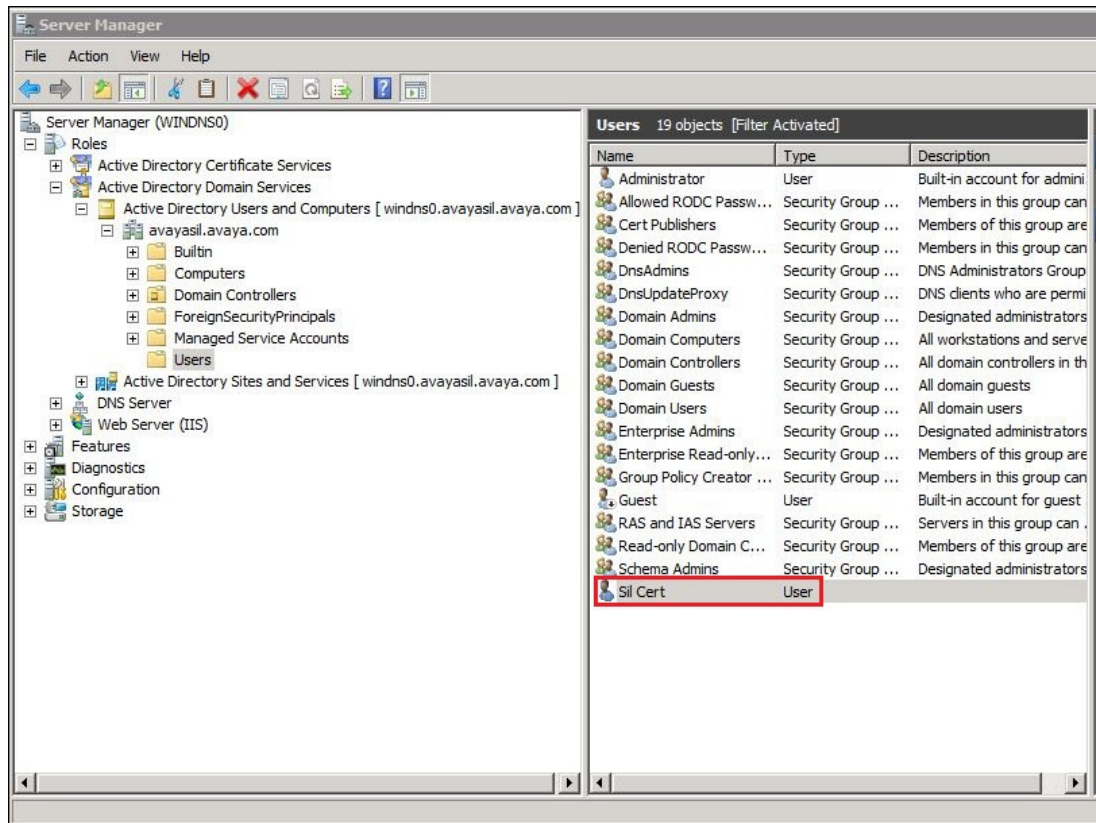
Full name: Sil Cert

User logon name: silcert@avayasil.avaya.com

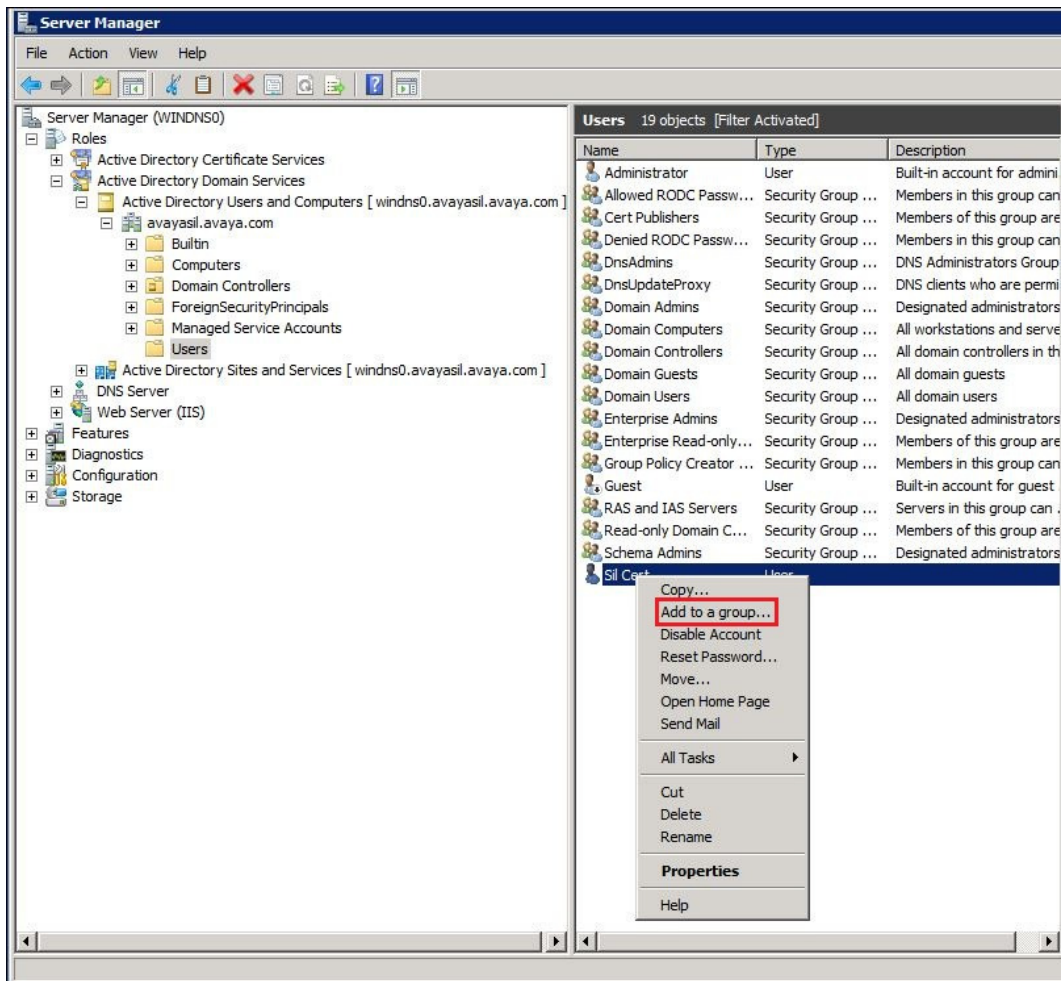
The password never expires.

< Back Finish Cancel

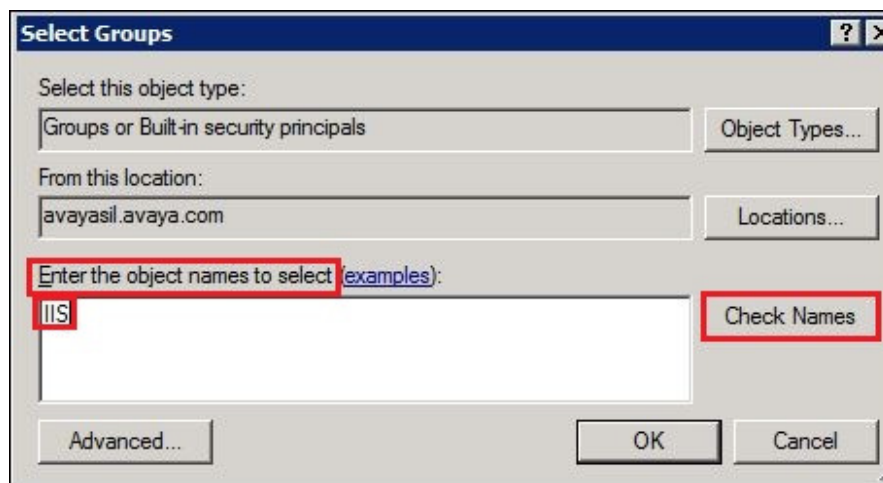
The new user that was created is displayed in the Users window. See below.



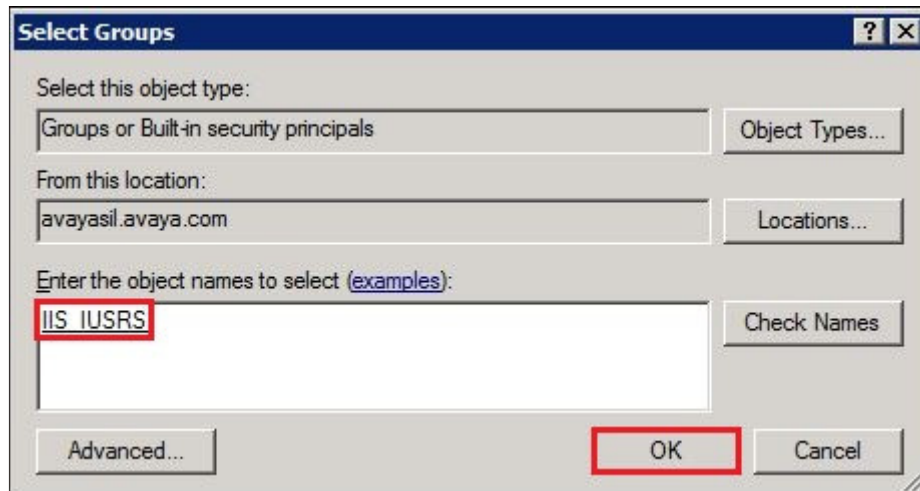
The user that was just created must be a member of the IIS group. To add this user to the IIS group, right click on the user and select **Add to a group**.



In the window **Enter the object names to select**, input **IIS** and click on **Check Names**.



The group **IIS_IUSRS** will be displayed. Click on **OK**.

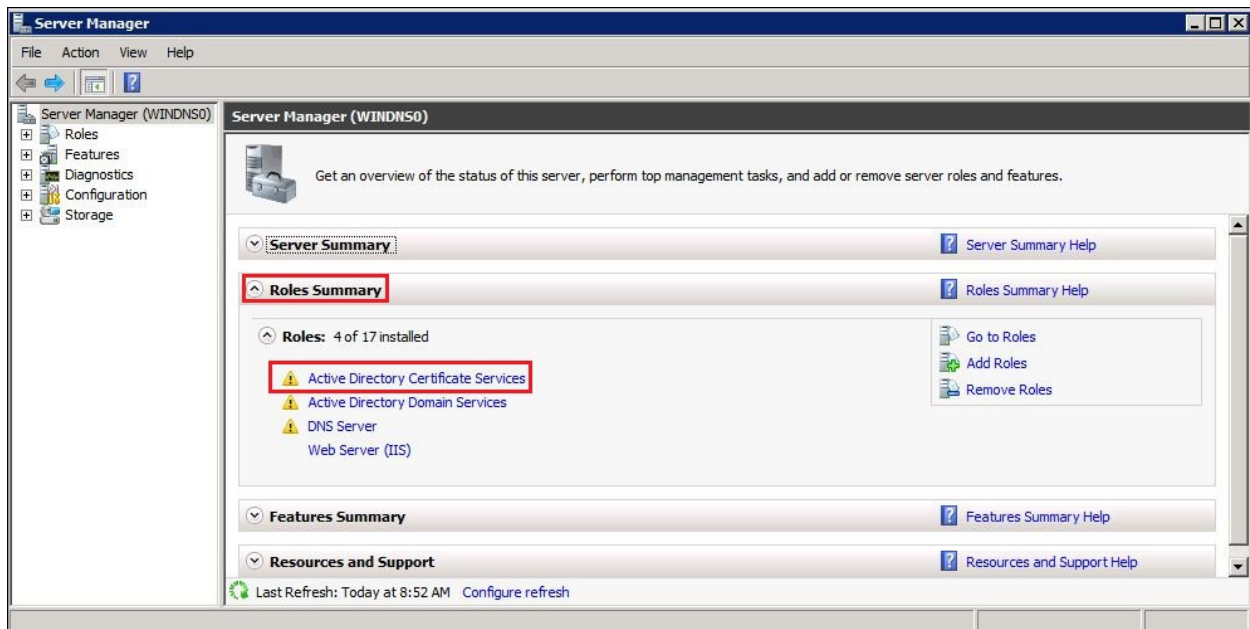


The user has been added to the IIS group. Click on **OK** to exit.

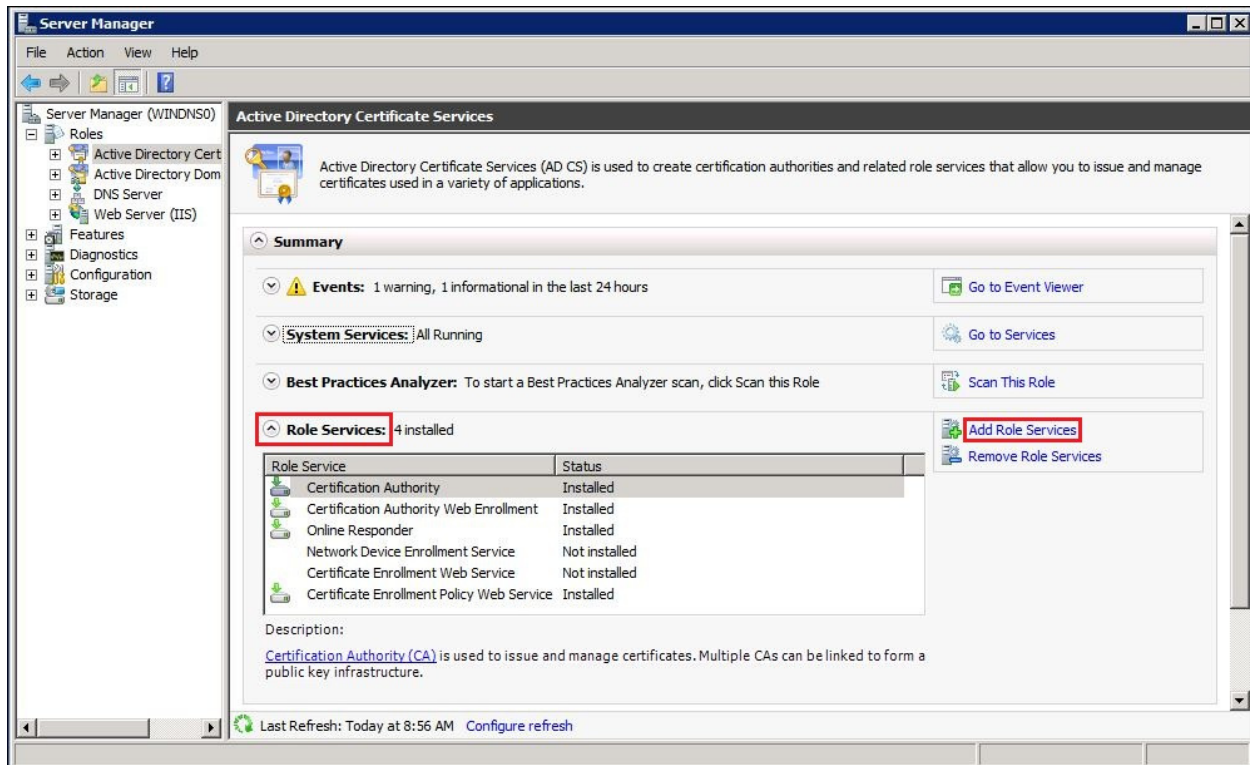


Step 2. Install Network Device Enrollment Service

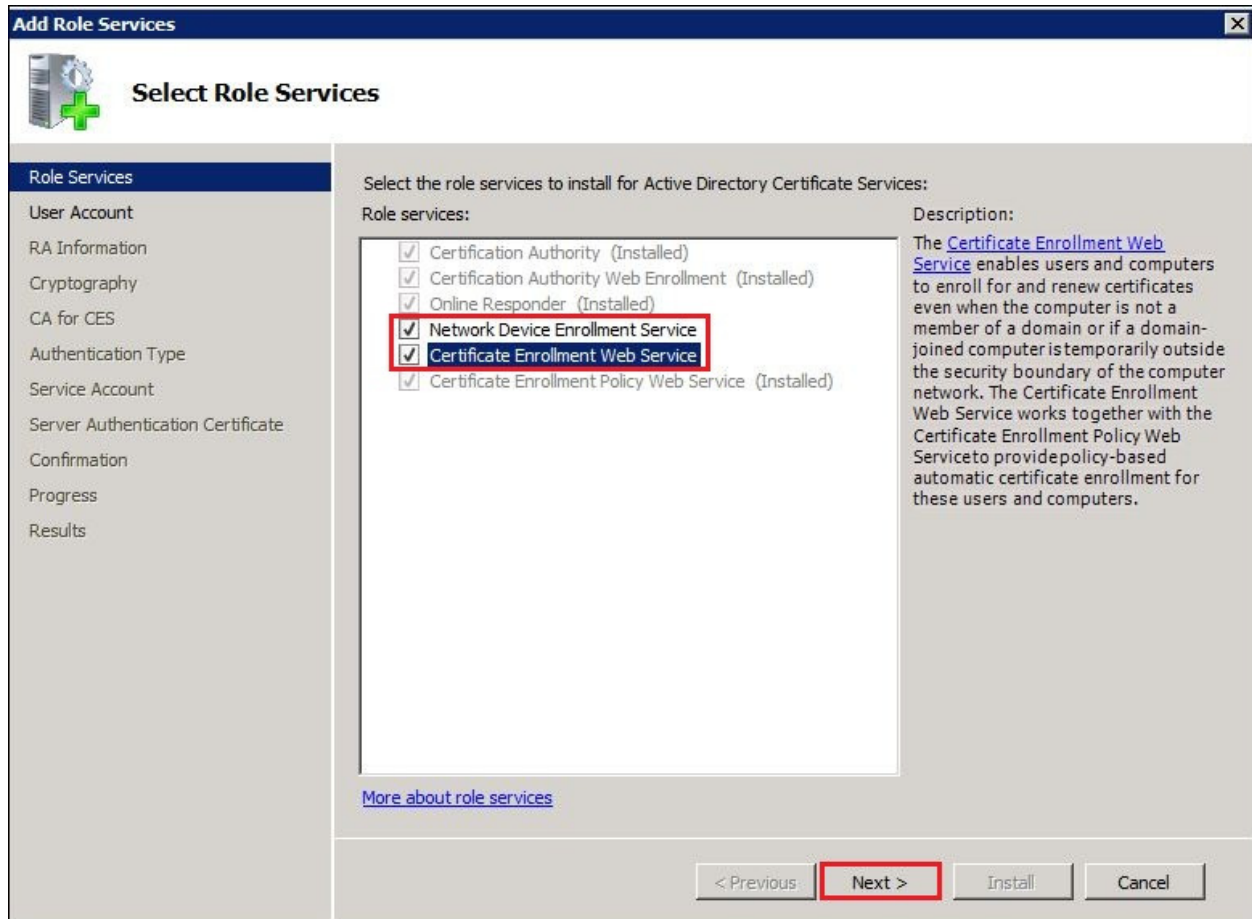
To install the Network Device Enrollment Service scroll down to **Roles Summary** and Select **Active Directory Certificate Services**.



Scroll down to the **Role Services** heading and Select **Add Role Services**.



Check **Network Device Enrollment Service** and **Certificate Enrollment Web Service** and click on **Next**.



Click on **Select User**.

The screenshot shows the 'Add Role Services' wizard window. The title bar reads 'Add Role Services'. The main heading is 'Specify User Account'. On the left is a navigation pane with the following items: 'Role Services', 'User Account' (highlighted), 'RA Information', 'Cryptography', 'CA for CES', 'Authentication Type', 'Service Account', 'Server Authentication Certificate', 'Confirmation', 'Progress', and 'Results'. The main area contains the instruction: '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 and a 'Select User...' button, which is highlighted with a red rectangle. At the bottom right are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Add Role Services

Specify User Account

Role Services

User Account

RA Information

Cryptography

CA for CES

Authentication Type

Service Account

Server Authentication Certificate

Confirmation

Progress

Results

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.

☒ Specify user account (recommended)

☐ Use the application pool identity instead of a user account

Select User...

< Previous Next > Install Cancel

Select the user created in **Section 5.2 Step 1**. Click **Next**.

The screenshot shows the 'Add Role Services' wizard window. The title bar reads 'Add Role Services'. The left sidebar contains a list of steps: 'Role Services', 'User Account' (highlighted), 'RA Information', 'Cryptography', 'CA for CES', 'Authentication Type', 'Service Account', 'Server Authentication Certificate', '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)' (selected) and 'Use the application pool identity instead of a user account'. Below the first option is a text box containing 'AVAYASIL\silcert', which is highlighted with a red rectangle. To the right of the text box is a 'Select User...' button. At the bottom of the window, there are four buttons: '< Previous', 'Next >' (highlighted with a red rectangle), 'Install', and 'Cancel'.

For **Specify Registration Authority Information**, accept the defaults by Clicking on **Next**.

The screenshot shows the 'Add Role Services' wizard window. The title bar reads 'Add Role Services'. The main heading is 'Specify Registration Authority Information'. On the left is a navigation pane with the following items: 'Role Services', 'User Account', 'RA Information' (highlighted), 'Cryptography', 'CA for CES', 'Authentication Type', 'Service Account', 'Server Authentication Certificate', 'Confirmation', 'Progress', and 'Results'. The main area contains the following text: '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'. Under 'Required Information', there is a text box for 'RA Name' containing 'WINDNS0-MSCEP-RA' and a dropdown for 'Country/Region' set to 'US (United States)'. Under 'Optional Information', there are five empty text boxes for 'E-mail:', 'Company:', 'Department:', 'City', and 'State/Province:'. At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a red border), 'Install', and 'Cancel'.

Add Role Services

Specify Registration Authority Information

Role Services
User Account
RA Information
Cryptography
CA for CES
Authentication Type
Service Account
Server Authentication Certificate
Confirmation
Progress
Results

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: WINDNS0-MSCEP-RA

Country/Region: US (United States)

Optional Information

E-mail:

Company:

Department:

City:

State/Province:

< Previous **Next >** Install Cancel

For **Signature key CSP** and **Encryption key CSP**, Verify **Microsoft Strong Cryptographic Provider** is selected and **Key character length**: is set to **2048**. These are the defaults. Click on **Next**.

The screenshot shows the 'Add Role Services' wizard window. The title bar says 'Add Role Services'. The main title is 'Configure Cryptography for Registration Authority'. On the left is a navigation pane with the following items: Role Services, User Account, RA Information, Cryptography (selected), CA for CES, Authentication Type, Service Account, Server Authentication Certificate, Confirmation, Progress, and Results. The main content area has a paragraph: '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, there are two sections. The first section is for the 'Signature key' and includes the text 'Signature key is used to avoid repetition of communication between the CA and the RA.' It has a 'Signature key CSP:' dropdown menu set to 'Microsoft Strong Cryptographic Provider' and a 'Key character length:' dropdown menu set to '2048'. The second section is for the 'Encryption key' and includes the text 'Encryption key is used for secure communication between the RA and the network device.' It has an 'Encryption key CSP:' dropdown menu set to 'Microsoft Strong Cryptographic Provider' and a 'Key character length:' dropdown menu set to '2048'. At the bottom of the main content area is a link: 'More about signature and encryption keys'. At the bottom of the window are four buttons: '< Previous', 'Next >' (highlighted with a red box), 'Install', and 'Cancel'.

Add Role Services

Configure Cryptography for Registration Authority

Role Services
User Account
RA Information
Cryptography
CA for CES
Authentication Type
Service Account
Server Authentication Certificate
Confirmation
Progress
Results

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.

Signature key is used to avoid repetition of communication between the CA and the RA.

Signature key CSP: **Microsoft Strong Cryptographic Provider** Key character length: **2048**

Encryption key is used for secure communication between the RA and the network device.

Encryption key CSP: **Microsoft Strong Cryptographic Provider** Key character length: **2048**

[More about signature and encryption keys](#)

< Previous **Next >** Install Cancel

Select the CA created in **Section 5.1**. Click on **Next**.

The screenshot shows the 'Add Role Services' wizard window. The title bar reads 'Add Role Services'. The main title is 'Specify CA for Certificate Enrollment Web Services'. On the left is a navigation pane with the following items: Role Services, User Account, RA Information, Cryptography, CA for CES (highlighted), Authentication Type, Service Account, Server Authentication Certificate, Confirmation, Progress, and Results. The main area contains the following text: 'To select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web service, browse for the name of the CA or the name of the computer that hosts the CA.' Below this, there are two radio buttons: 'CA name' (selected) and 'Computer name'. A text box labeled 'CA:' contains the text 'windns0.avayasil.avaya.com\avayasil-WINDNS0-CA', which is highlighted with a red rectangle. To the right of the text box is a 'Browse...' button. Below the text box, there is a checkbox labeled 'Configure the Certificate Enrollment Web Service for renewal-only mode.' which is unchecked. Below the checkbox is an information icon followed by the text: 'Processing new certificate requests requires the Web service to be trusted for delegation. Renewal-only mode allows only certificate renewal requests, and delegation is not required. This might be appropriate when increased security is necessary; for example, when the Web service is deployed to the internet.' Below this is a note: 'Note: When renewal-only mode is selected, the specified CA must be running on Windows Server 2008 R2.' At the bottom right are four buttons: '< Previous', 'Next >' (highlighted with a red rectangle), 'Install', and 'Cancel'.

Add Role Services

Specify CA for Certificate Enrollment Web Services

Role Services
User Account
RA Information
Cryptography
CA for CES
Authentication Type
Service Account
Server Authentication Certificate
Confirmation
Progress
Results

To select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web service, browse for the name of the CA or the name of the computer that hosts the CA.

Browse by: ☒ CA name ☐ Computer name

CA: windns0.avayasil.avaya.com\avayasil-WINDNS0-CA Browse...

☐ Configure the Certificate Enrollment Web Service for renewal-only mode.

Processing new certificate requests requires the Web service to be trusted for delegation. Renewal-only mode allows only certificate renewal requests, and delegation is not required. This might be appropriate when increased security is necessary; for example, when the Web service is deployed to the internet.

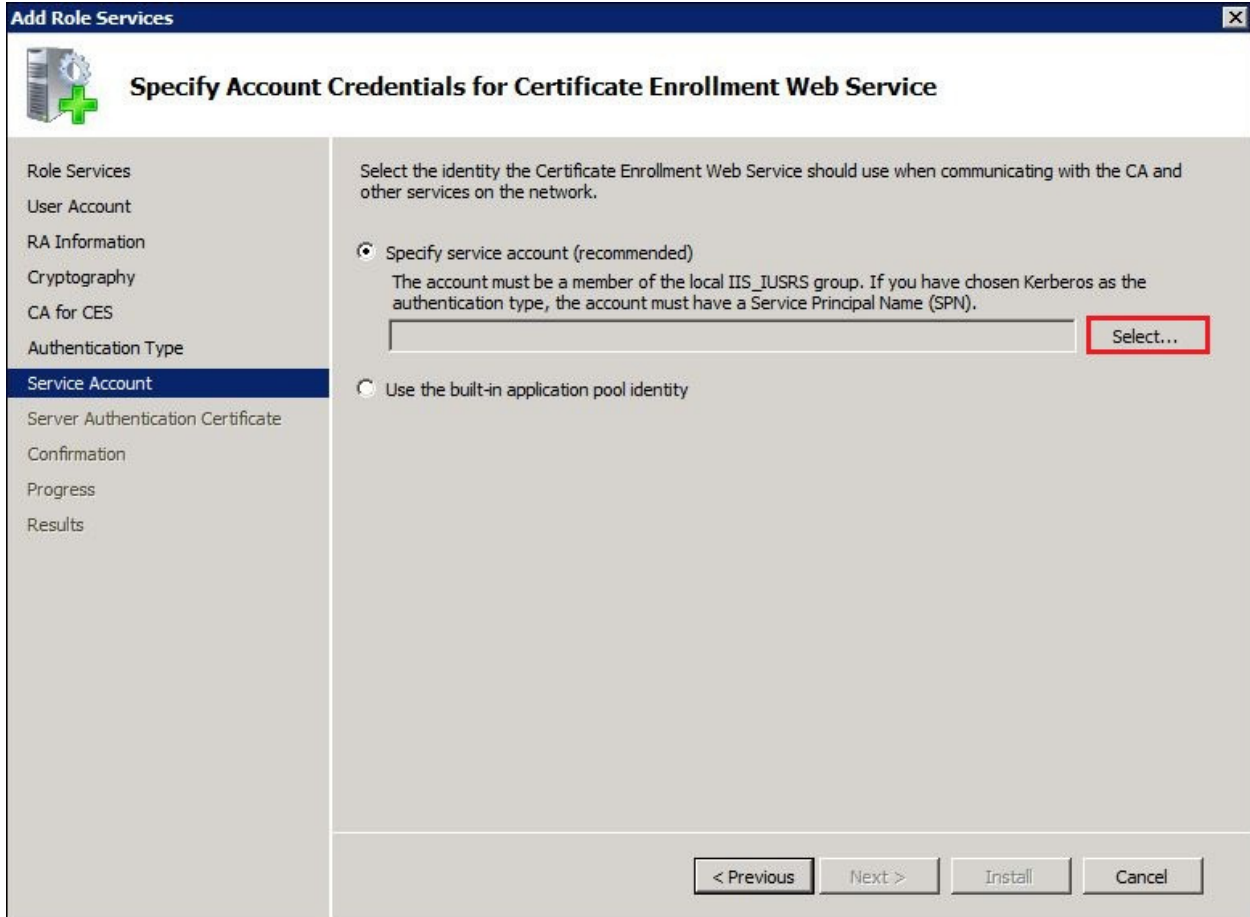
Note: When renewal-only mode is selected, the specified CA must be running on Windows Server 2008 R2.

< Previous **Next >** Install Cancel

Select **Client certificate authentication**. Click on **Next**.

The screenshot shows the 'Add Role Services' wizard window. The title bar reads 'Add Role Services'. The main window has a left-hand navigation pane with the following items: 'Role Services', 'User Account', 'RA Information', 'Cryptography', 'CA for CES', 'Authentication Type' (highlighted in blue), 'Service Account', 'Server Authentication Certificate', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'Select Authentication Type' and contains the instruction: 'Select the type of authentication clients will use when sending requests to the web service(s)'. There are three radio button options: 'Windows Integrated Authentication' (with a description: 'Select this option if clients will only be able to access the web service while connected directly to your internal network.'), 'Client certificate authentication' (which is selected and highlighted with a red rectangle, with a description: 'Select this option if you plan to provide users with digital X.509 certificates for client authentication. This option will enable you to make the web service available on the Internet.'), and 'Username and password' (with a description: 'Select this option if you would like users to enter a username and password to authenticate to the web service. This option can be used when the web service is accessed on the internal network or over the Internet.'). At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a red rectangle), 'Install', and 'Cancel'.

Select the user created in **Section 5.2 Step 1**. Click on **Next**.



The screenshot shows the 'Add Role Services' wizard window. The title bar is 'Add Role Services'. The main title is 'Specify Account Credentials for Certificate Enrollment Web Service'. On the left is a navigation pane with the following items: Role Services, User Account, RA Information, Cryptography, CA for CES, Authentication Type, **Service Account** (highlighted), Server Authentication Certificate, Confirmation, Progress, and Results. The main area contains the following text: 'Select the identity the Certificate Enrollment Web Service should use when communicating with the CA and other services on the network.' There are two radio button options: 'Specify service account (recommended)' (selected) and 'Use the built-in application pool identity'. Below the first option is a text box with the placeholder text: 'The account must be a member of the local IIS_IUSRS group. If you have chosen Kerberos as the authentication type, the account must have a Service Principal Name (SPN).' To the right of the text box is a 'Select...' button. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

To select the account displayed, click on **OK**.



The screenshot shows a 'Windows Security' dialog box titled 'Add Role Services'. The subtitle is 'Specify a name and password.' Below this is a text box containing 'silcert' and a password box with masked characters. Below the password box is the text 'Domain: AVAYASIL'. There is an icon of a smart card and the text 'Insert a smart card'. At the bottom are 'OK' and 'Cancel' buttons.

The service account that was just selected will be displayed. Click on **Next**.

The screenshot shows the 'Add Role Services' wizard window. The title bar reads 'Add Role Services'. The main title is 'Specify Account Credentials for Certificate Enrollment Web Service'. On the left is a navigation pane with the following items: Role Services, User Account, RA Information, Cryptography, CA for CES, Authentication Type, **Service Account** (highlighted), Server Authentication Certificate, Confirmation, Progress, and Results. The main area contains the following text: 'Select the identity the Certificate Enrollment Web Service should use when communicating with the CA and other services on the network.' There are two radio button options: 'Specify service account (recommended)' (which is selected and highlighted with a red box) and 'Use the built-in application pool identity'. Below the first option is a text box containing 'AVAYASIL\silcert' (highlighted with a red box) and a 'Select...' button. Below the second option is no text. At the bottom right are four buttons: '< Previous', 'Next >' (highlighted with a red box), 'Install', and 'Cancel'.

Add Role Services

Specify Account Credentials for Certificate Enrollment Web Service

Role Services
User Account
RA Information
Cryptography
CA for CES
Authentication Type
Service Account
Server Authentication Certificate
Confirmation
Progress
Results

Select the identity the Certificate Enrollment Web Service should use when communicating with the CA and other services on the network.

☒ **Specify service account** (recommended)
The account must be a member of the local IIS_IUSRS group. If you have chosen Kerberos as the authentication type, the account must have a Service Principal Name (SPN).
AVAYASIL\silcert Select...

☐ Use the built-in application pool identity

< Previous **Next >** Install Cancel

The Microsoft Certificate Authority is already installed so select **Choose an existing certificate for SSL encryption** for SSL encryption. Click on **Next**.

The screenshot shows the 'Add Role Services' wizard window. The title bar is 'Add Role Services'. The main heading is 'Choose a Server Authentication Certificate for SSL Encryption'. On the left is a navigation pane with the following items: Role Services, User Account, RA Information, Cryptography, CA for CES, Authentication Type, Service Account, **Server Authentication Certificate** (highlighted), Confirmation, Progress, and Results. The main content area has a sub-header 'Choose a Server Authentication Certificate for SSL Encryption' and a description: 'When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) protocol to encrypt network traffic. Choose a server authentication certificate suitable for SSL encryption to add to the default website in IIS.' There are two radio button options. The first option, 'Choose an existing certificate for SSL encryption (recommended)', is selected and highlighted with a red box. Below it is a table of certificates. The second option is 'Choose and assign a certificate for SSL later'. At the bottom right are buttons for '< Previous', 'Next >' (highlighted with a red box), 'Install', and 'Cancel'. A warning icon and text are also present.

Role Services
User Account
RA Information
Cryptography
CA for CES
Authentication Type
Service Account
Server Authentication Certificate
Confirmation
Progress
Results

Choose a Server Authentication Certificate for SSL Encryption

When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) protocol to encrypt network traffic.
Choose a server authentication certificate suitable for SSL encryption to add to the default website in IIS.

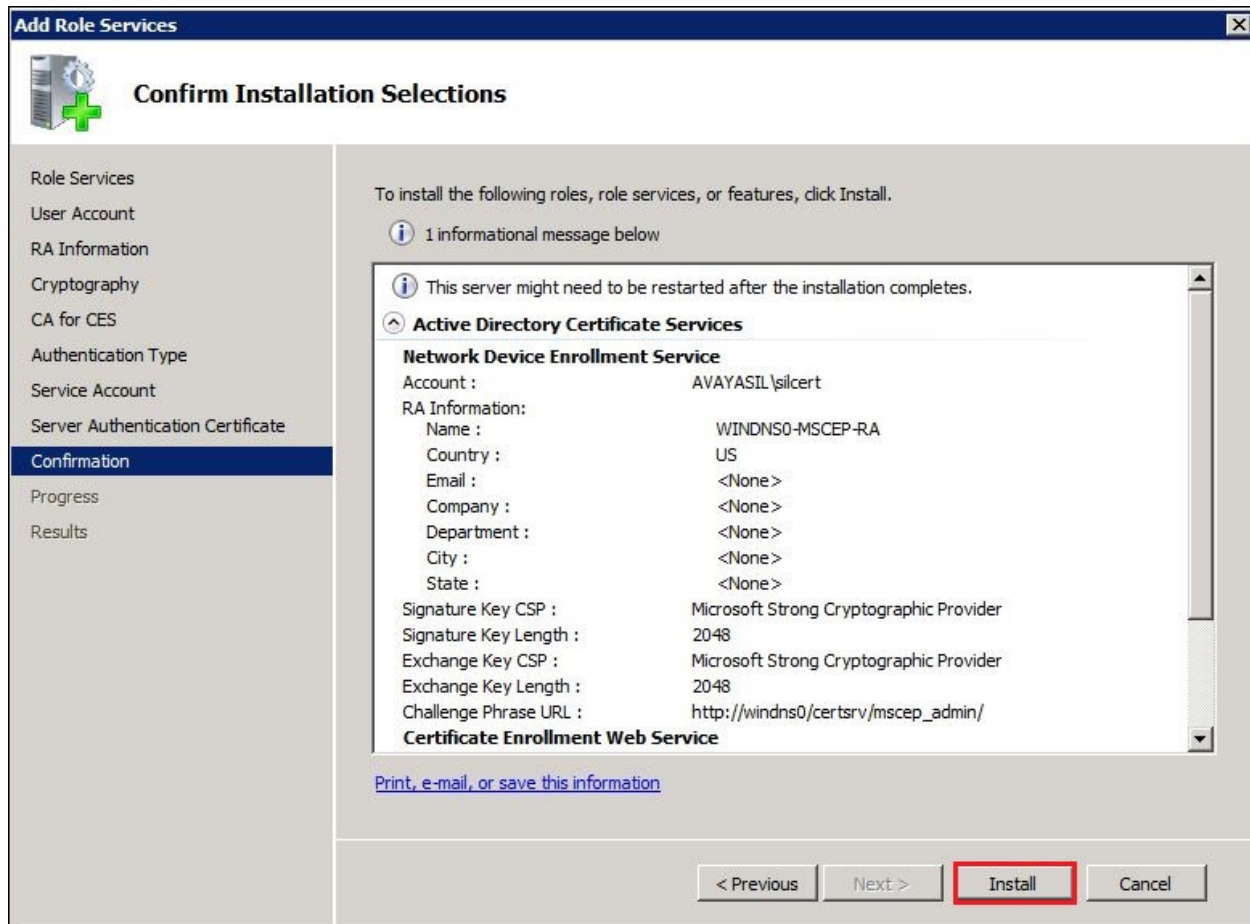
☒ Choose an existing certificate for SSL encryption (recommended)
This option is recommended for most production deployment scenarios. You should use a certificate issued by a certification authority that is trusted by clients connecting to this server. The subject name of the certificate must match the host name of this server.

Issued To	Issued By	Expiration Date	Intended Purpose
avayasil-WINDNS0-CA	avayasil...	4/11/2018	<Any EKU>, CRL Sign...
windns0.avayasil.av...	avayasil...	4/11/2014	Client Authentication,...

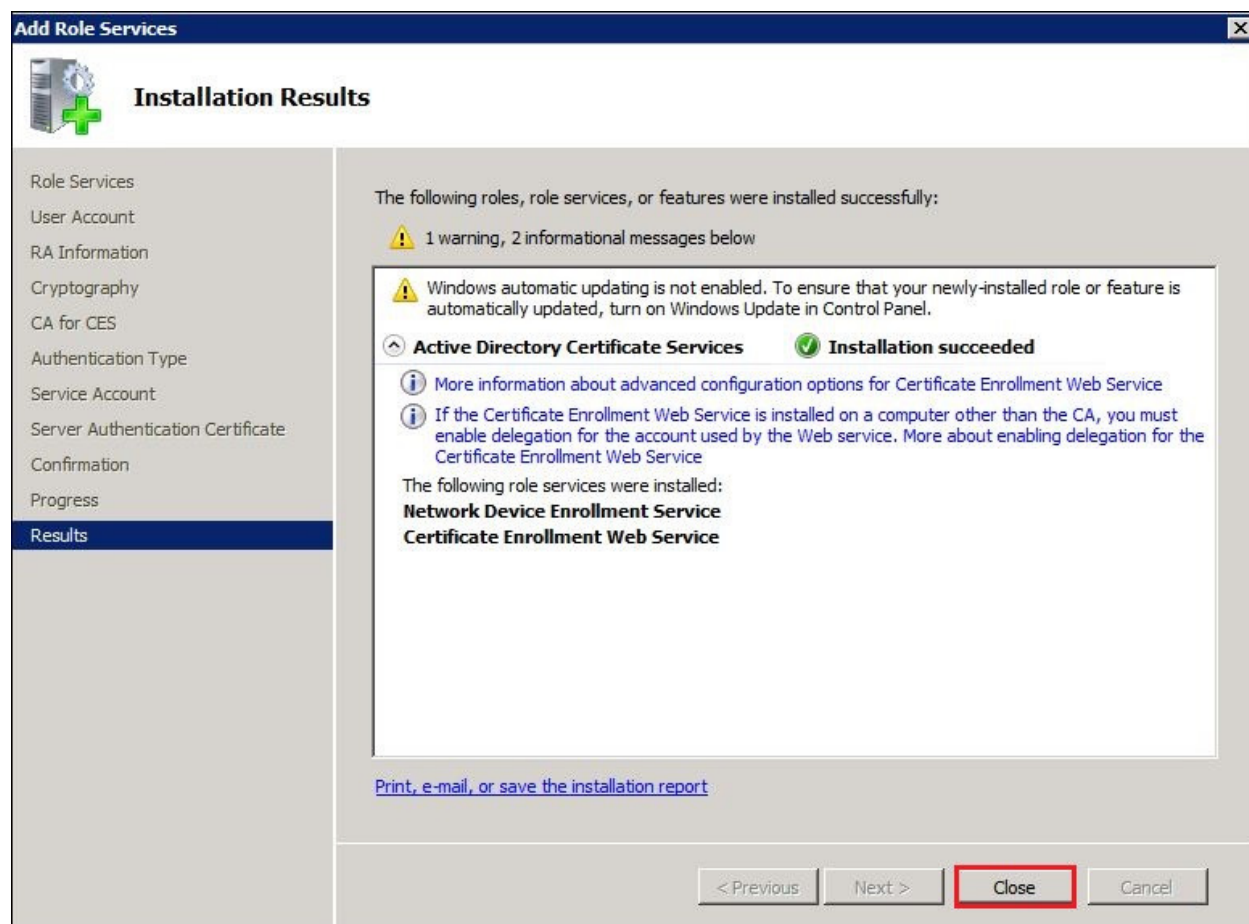
☐ Choose and assign a certificate for SSL later
This option is recommended if you plan to request a certificate from a CA and import it to the local computer personal certificate store on this server later. Once the certificate is imported, use the IIS snap-in to assign the certificate to the default web site.
 For this role service to function, you must configure this server with a valid certificate.

< Previous **Next >** Install Cancel

Verify the settings. To start the installation, click on **Install**.



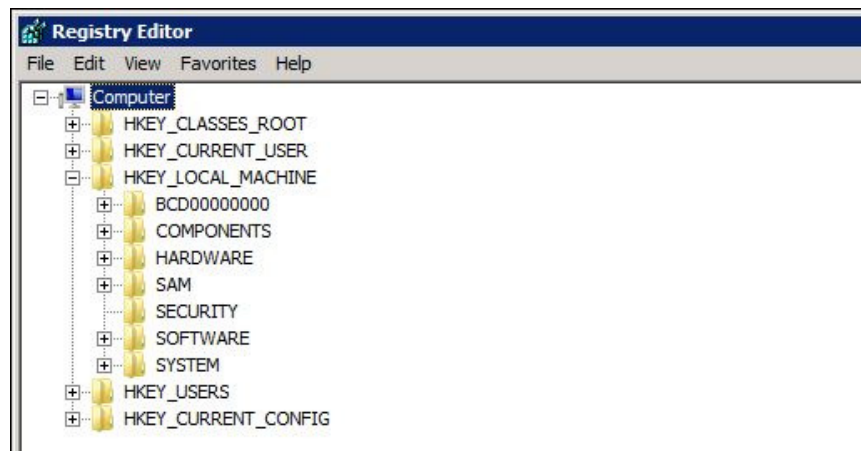
After installation completes, the Installation Results screen will be displayed. Click on **Close**.



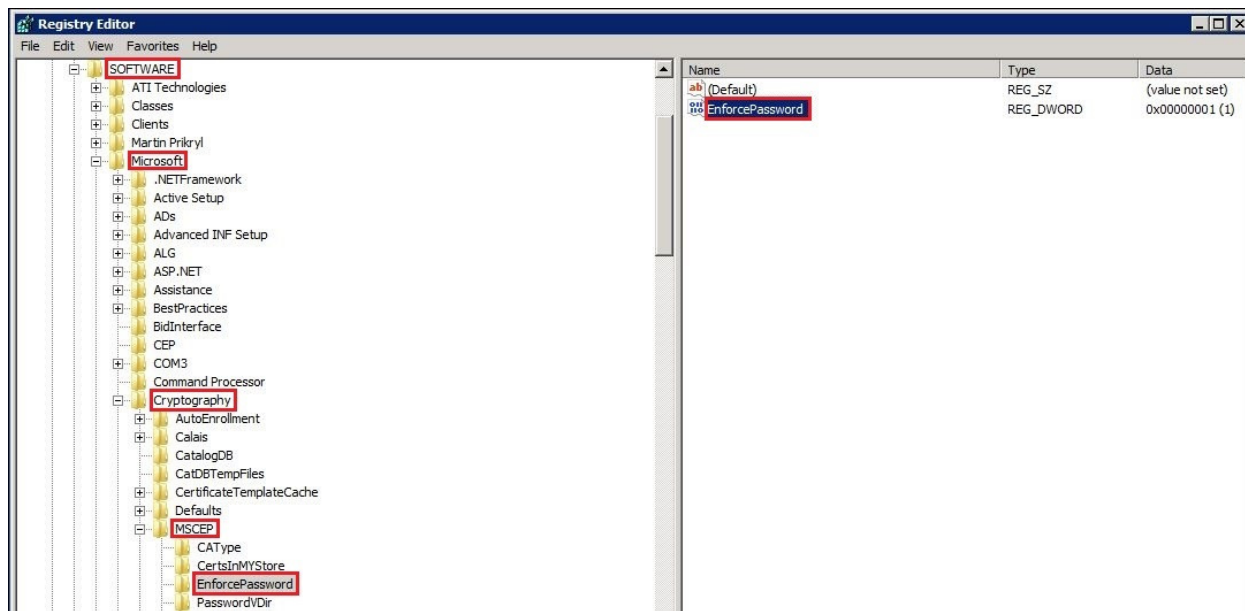
5.3. Disable SCEP Password

This sample configuration did not use Enrollment Passwords so **EnforcePassword** was disabled.

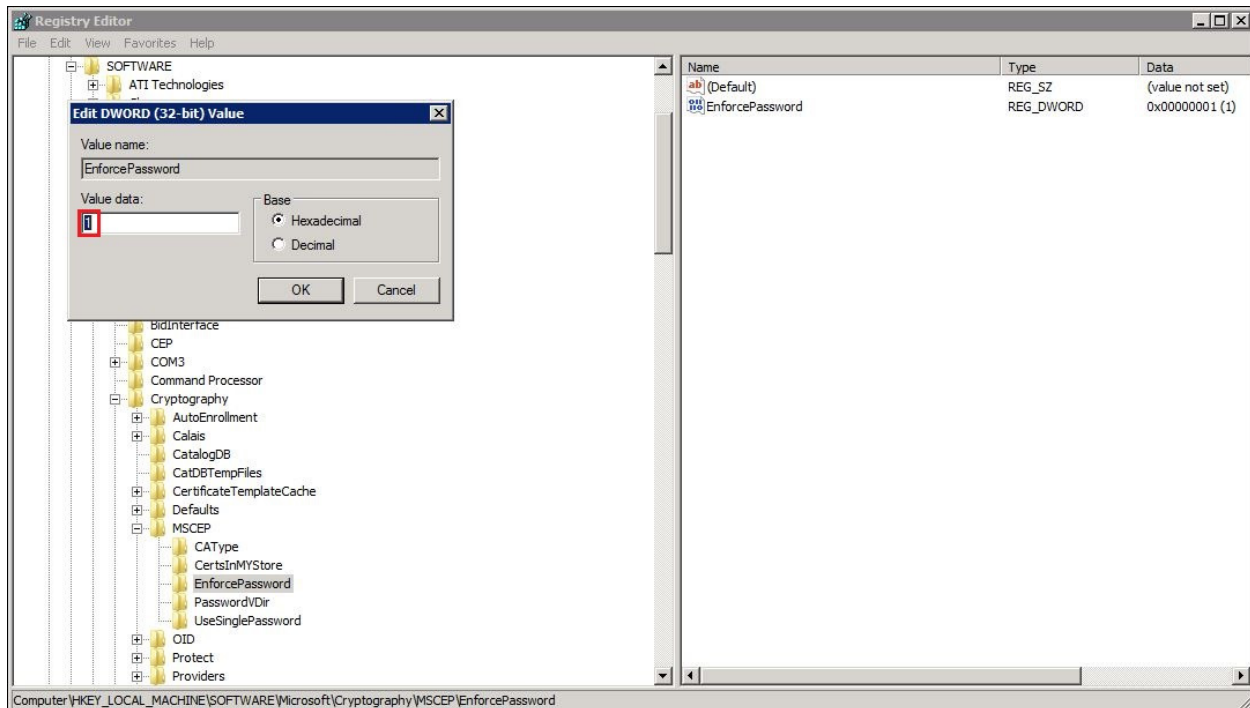
Login remotely to the Windows Server 2008. Go to **Start** (not shown). In the Search programs and files line, type in **regedit** and press **Enter** (not shown). The regedit program will execute and display the following screen.



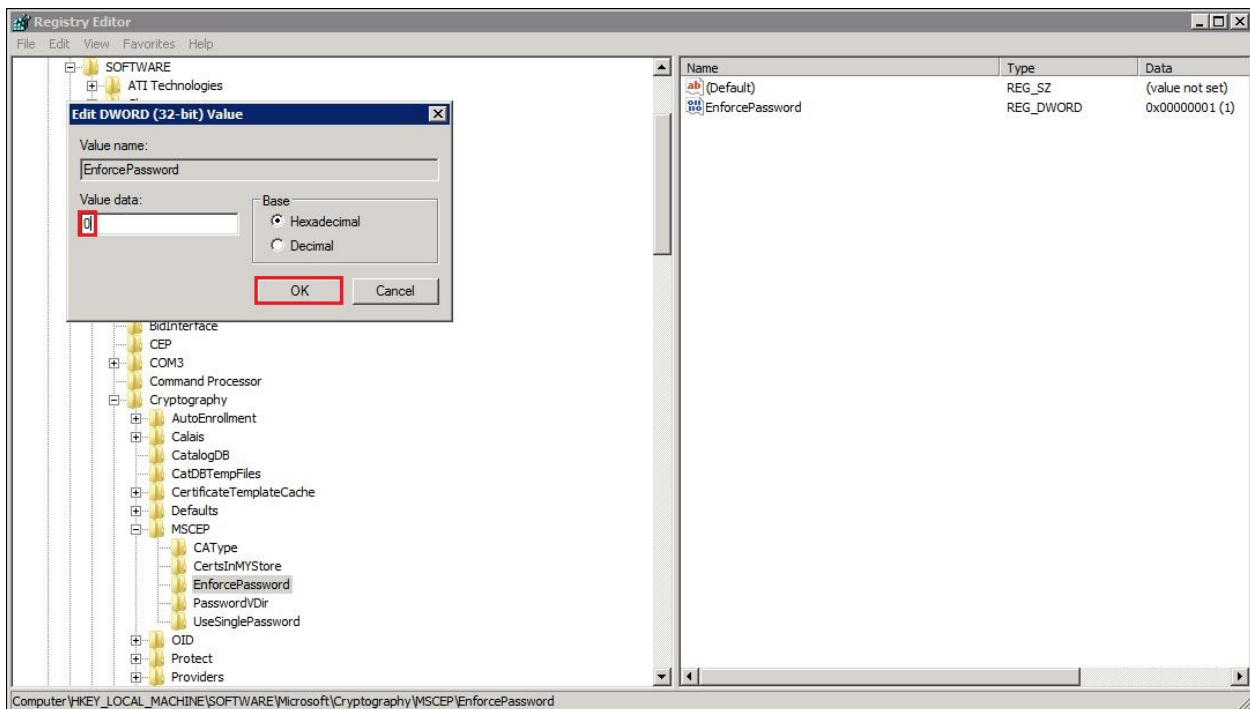
Go to **Computer** → **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Microsoft** → **Cryptography** → **MSCEP** and select **EnforcePassword**. See below.



Right click on **EnforcePassword** to edit the value. See below.



Update **Value data:** to **0** to disable password enforcement and select **OK**. See below.



Important Note: For the changes to take effect, **Restart IIS**.

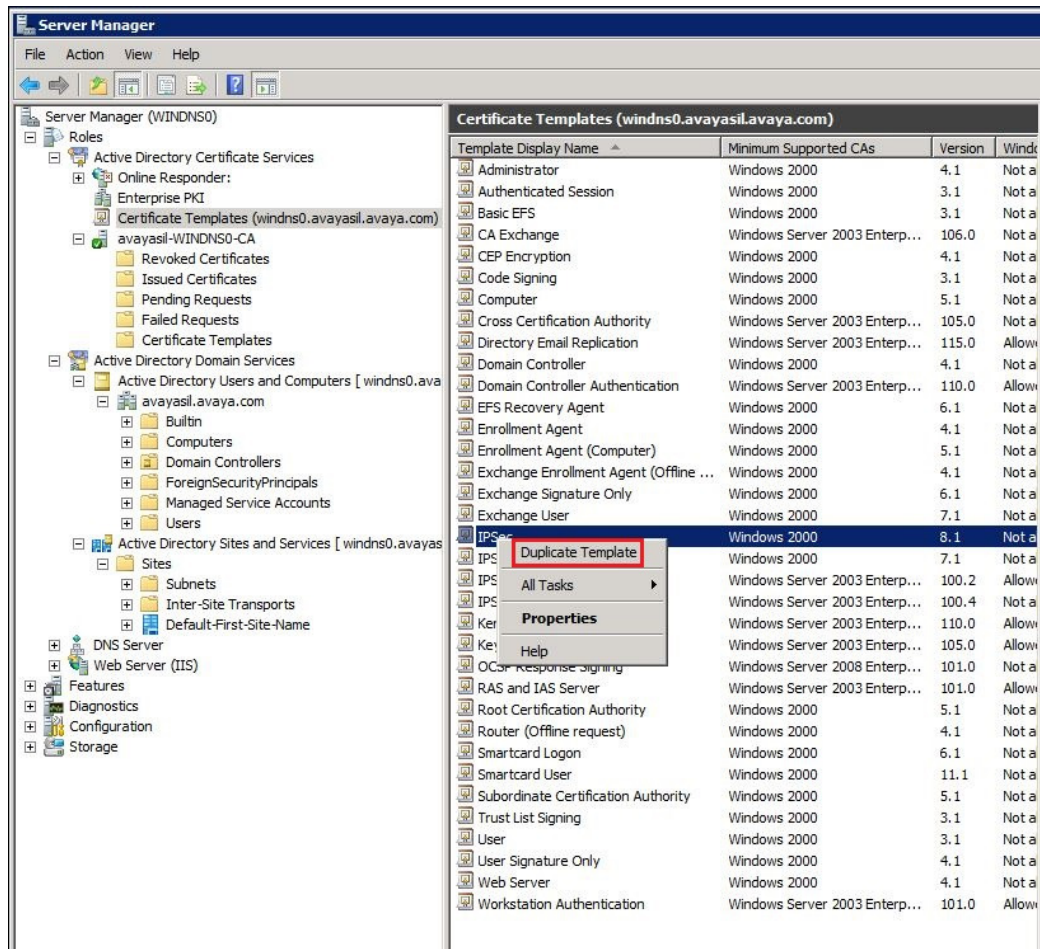
5.4. Create New Template for IPSec

Make a duplicate template from IPSec. Go to **Server Manager** → **Roles** → **Active Directory Certificate Services** → **Certificate Templates** and find **IPSec**.

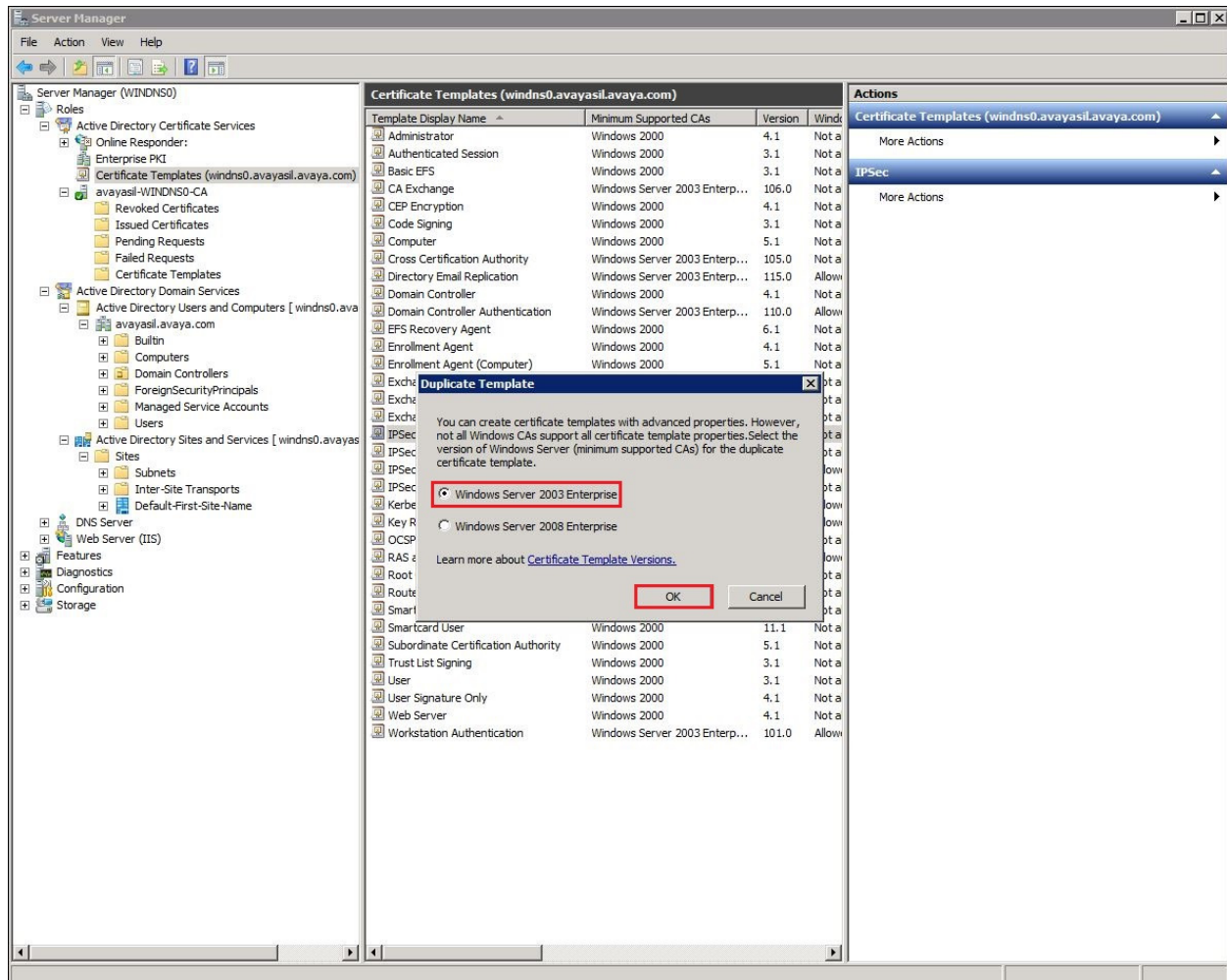
The screenshot shows the Windows Server Manager console. In the left-hand tree view, the following path is highlighted with red boxes: **Server Manager (WINDNS0)** > **Roles** > **Active Directory Certificate Services** > **Certificate Templates (windns0.avayasil.avaya.com)**. The right-hand pane displays a table of available certificate templates.

Template Display Name	Minimum Supported CAs	Version	Windk
Administrator	Windows 2000	4.1	Not a
Authenticated Session	Windows 2000	3.1	Not a
Basic EFS	Windows 2000	3.1	Not a
CA Exchange	Windows Server 2003 Enterp...	106.0	Not a
CEP Encryption	Windows 2000	4.1	Not a
Code Signing	Windows 2000	3.1	Not a
Computer	Windows 2000	5.1	Not a
Cross Certification Authority	Windows Server 2003 Enterp...	105.0	Not a
Directory Email Replication	Windows Server 2003 Enterp...	115.0	Allowi
Domain Controller	Windows 2000	4.1	Not a
Domain Controller Authentication	Windows Server 2003 Enterp...	110.0	Allowi
EFS Recovery Agent	Windows 2000	6.1	Not a
Enrollment Agent	Windows 2000	4.1	Not a
Enrollment Agent (Computer)	Windows 2000	5.1	Not a
Exchange Enrollment Agent (Offline ...	Windows 2000	4.1	Not a
Exchange Signature Only	Windows 2000	6.1	Not a
Exchange User	Windows 2000	7.1	Not a
IPSec	Windows 2000	8.1	Not a
IPSec (Offline request)	Windows 2000	7.1	Not a
IPSec with Client Server Auth	Windows Server 2003 Enterp...	100.2	Allowi
IPSecCS	Windows Server 2003 Enterp...	100.4	Not a
Kerberos Authentication	Windows Server 2003 Enterp...	110.0	Allowi
Key Recovery Agent	Windows Server 2003 Enterp...	105.0	Allowi
OCSP Response Signing	Windows Server 2008 Enterp...	101.0	Not a
RAS and IAS Server	Windows Server 2003 Enterp...	101.0	Allowi
Root Certification Authority	Windows 2000	5.1	Not a
Router (Offline request)	Windows 2000	4.1	Not a
Smartcard Logon	Windows 2000	6.1	Not a
Smartcard User	Windows 2000	11.1	Not a
Subordinate Certification Authority	Windows 2000	5.1	Not a
Trust List Signing	Windows 2000	3.1	Not a
User	Windows 2000	3.1	Not a
User Signature Only	Windows 2000	4.1	Not a
Web Server	Windows 2000	4.1	Not a
Workstation Authentication	Windows Server 2003 Enterp...	101.0	Allowi

Right click on **IPSec**. Select **Duplicate Template**.



For this template select **Windows Server 2003 Enterprise** and click on **OK**.



Input a suitable name for the new template under **Template display name**. Place a check beside **Publish certificate in Active Directory**. Select the **Request Handling** tab. See below.

The screenshot shows the 'Properties of New Template' dialog box with the 'Request Handling' tab selected. The 'Template display name' field contains 'IPSecCS'. The 'Template name' field also contains 'IPSecCS'. The 'Validity period' is set to 5 years and the 'Renewal period' is set to 2 years. The checkbox 'Publish certificate in Active Directory' is checked. Below it, the checkbox 'Do not automatically reenroll if a duplicate certificate exists in Active Directory' is unchecked. At the bottom, the checkbox 'For automatic renewal of smart card certificates, use the existing key if a new key cannot be created' is also unchecked. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom right.

Properties of New Template

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

Template display name:
IPSecCS

Minimum Supported CAs: Windows Server 2003 Enterprise

Template name:
IPSecCS

Validity period: 5 years Renewal period: 2 years

☒ 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 **Request Handling** tab, verify purpose is set to **Signature and encryption** and **Minimum key size** is set to **2048**. Place a check beside **Allow private key to be exported**. Select the **Subject Name** tab. See below.

The screenshot shows the 'Properties of New Template' dialog box with the 'Subject Name' tab selected. The 'Purpose' dropdown is set to 'Signature and encryption'. The 'Minimum key size' is set to '2048'. The checkbox 'Allow private key to be exported' is checked. Below this, there are three radio button options for enrollment: 'Enroll subject without requiring any user input' (selected), 'Prompt the user during enrollment', and 'Prompt the user during enrollment and require user input when the private key is used'. At the bottom, there is a button labeled 'CSPs...' and a note: 'To choose which cryptographic service providers (CSPs) should be used, click CSPs.' The dialog box has standard 'OK', 'Cancel', 'Apply', and 'Help' buttons at the bottom.

Properties of New Template

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | **Subject Name** | Server

Purpose: **Signature and encryption**

☐ Delete revoked or expired certificates (do not archive)

☐ Include symmetric algorithms allowed by the subject

☐ Archive subject's encryption private key

Minimum key size: **2048**

☒ Allow private key to be exported

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

☒ Enroll subject without requiring any user input

☐ Prompt the user during enrollment

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

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

CSPs...

OK Cancel Apply Help

Under **Subject Name**, verify **Build from this Active Directory information** is selected. For this sample configuration **Subject name format** was set to **None**. Under **Include this information in alternate subject name**, verify there is a check beside **DNS name**. Select the **Extensions** tab.

The screenshot shows the 'IPSecCS Properties' dialog box with the 'Extensions' tab selected. The 'Subject Name' sub-tab is also active. Under 'Supply in the request', the 'Build from this Active Directory information' radio button is selected. The 'Subject name format' dropdown is set to 'None'. Under 'Include this information in alternate subject name', the 'DNS name' checkbox is checked, while 'E-mail name', 'User principal name (UPN)', and 'Service principal name (SPN)' are unchecked. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

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

☐ Supply in the request

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

☒ Build 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

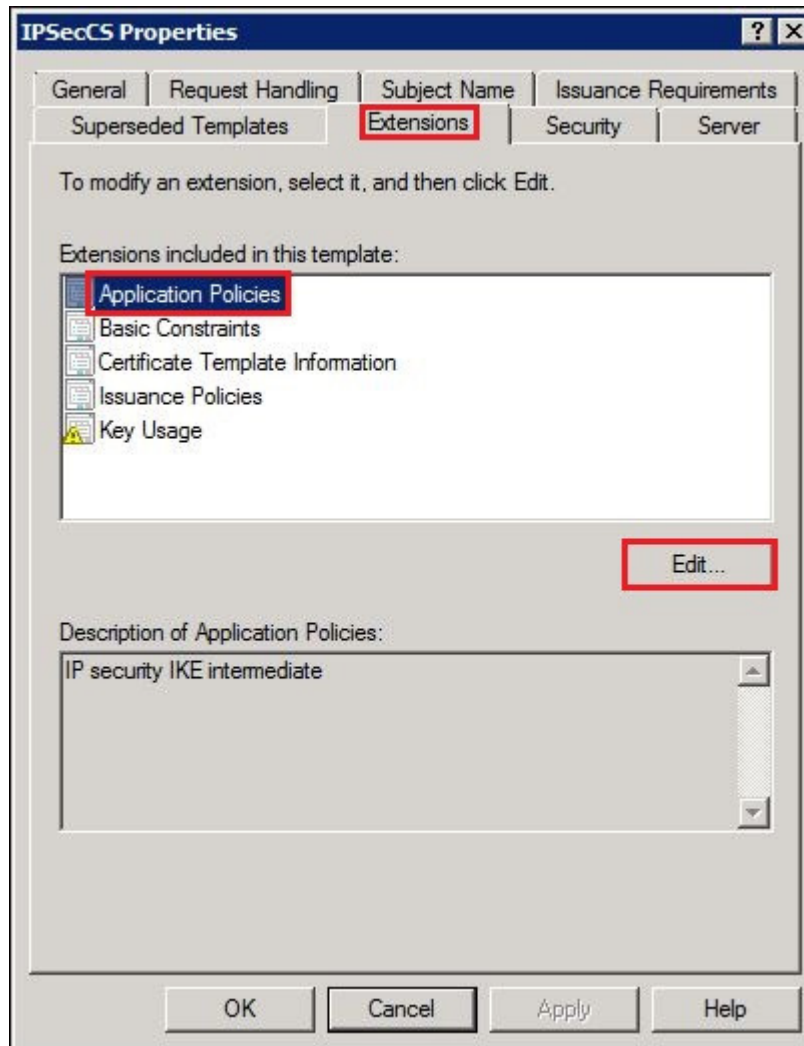
☐ User principal name (UPN)

☐ Service principal name (SPN)

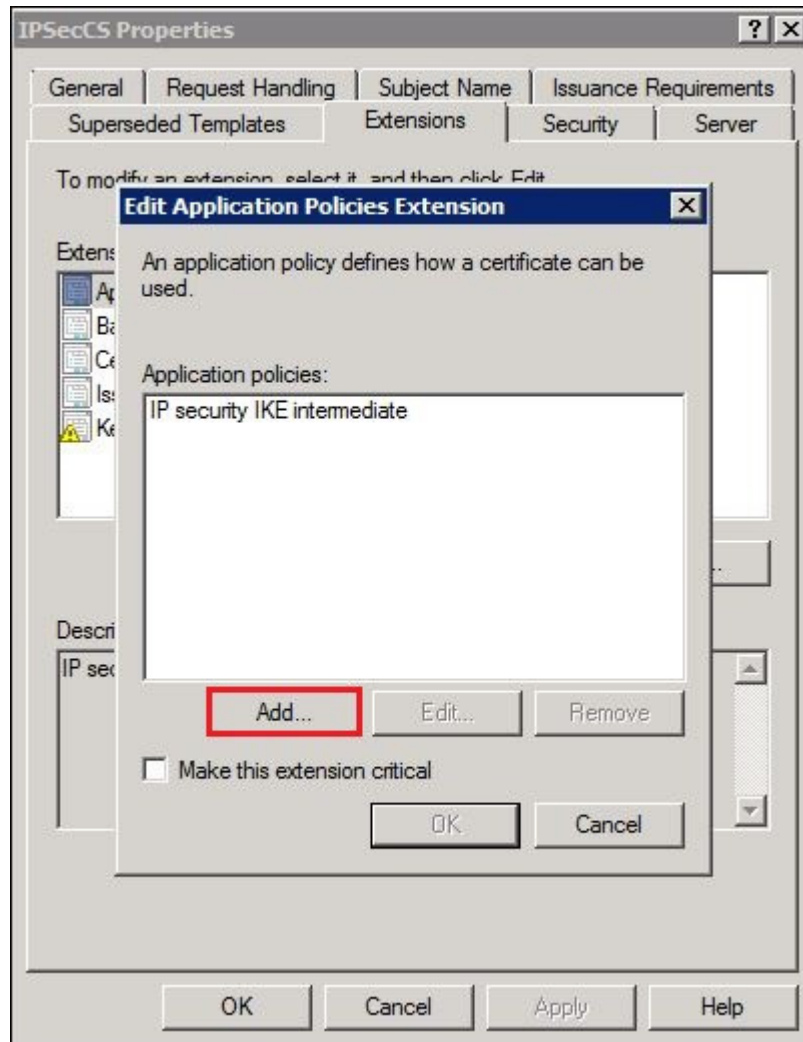
OK Cancel Apply Help

Note: For increased security select **Supply in the request**.

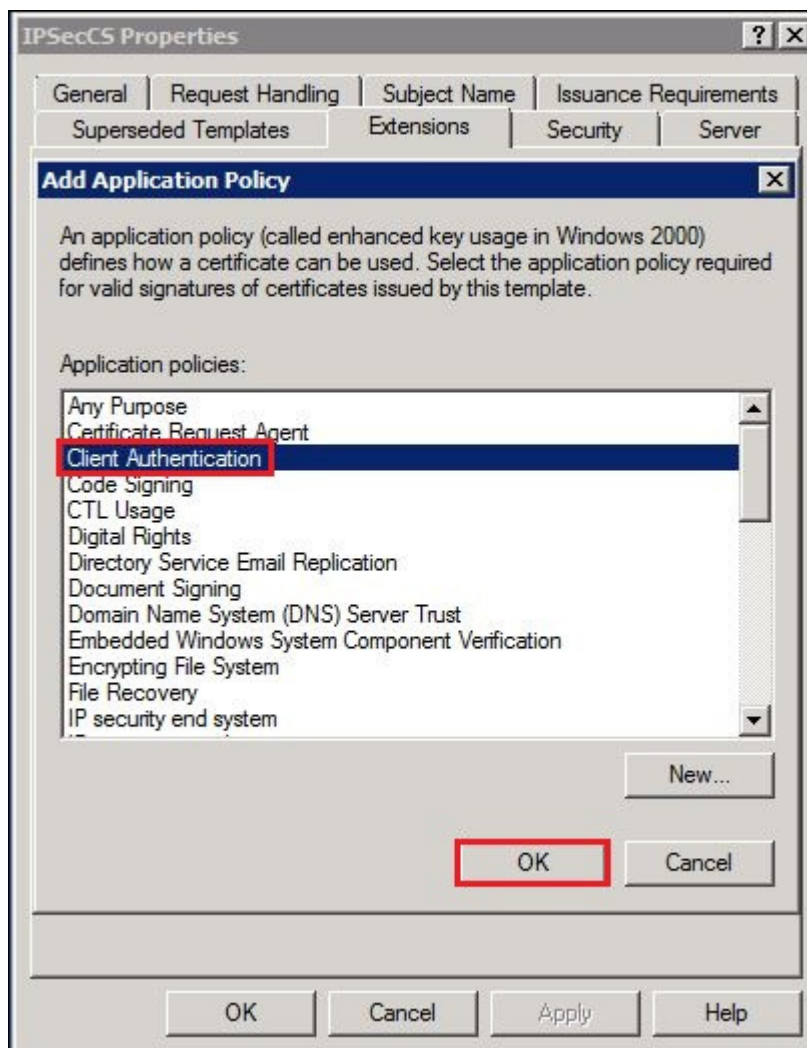
Under **Extensions**, select **Application Policies** and **Edit**.



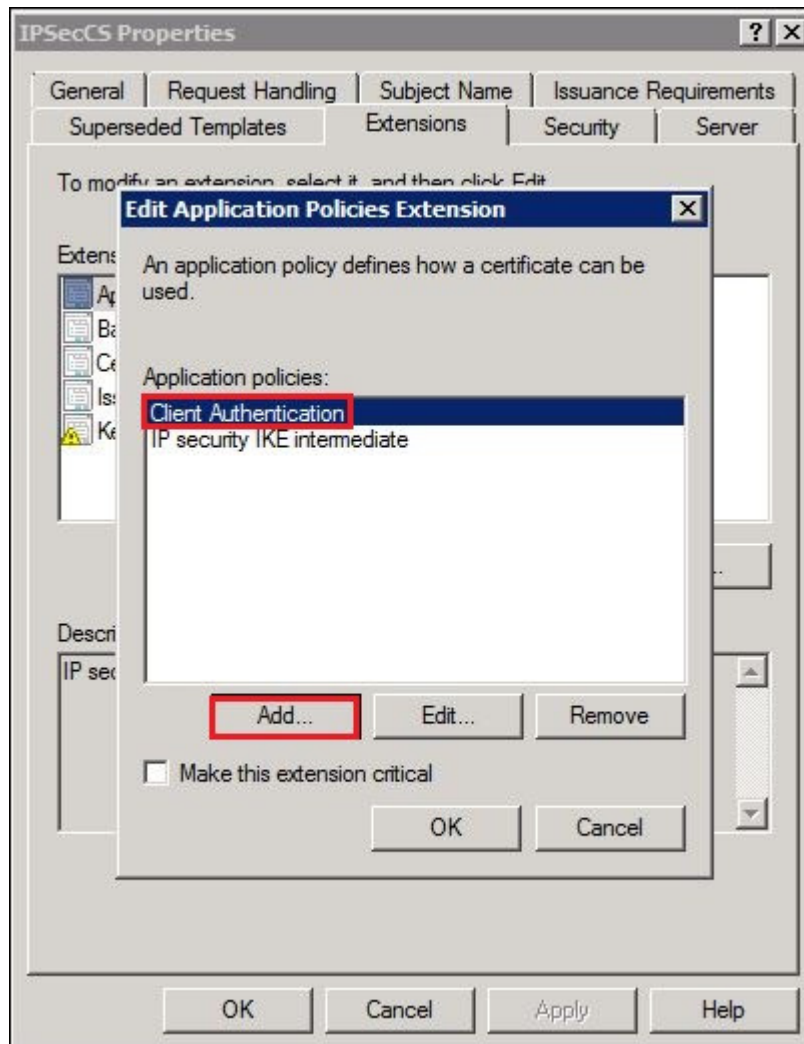
The **Edit Applications Policies Extension** window will open. Select **Add**.



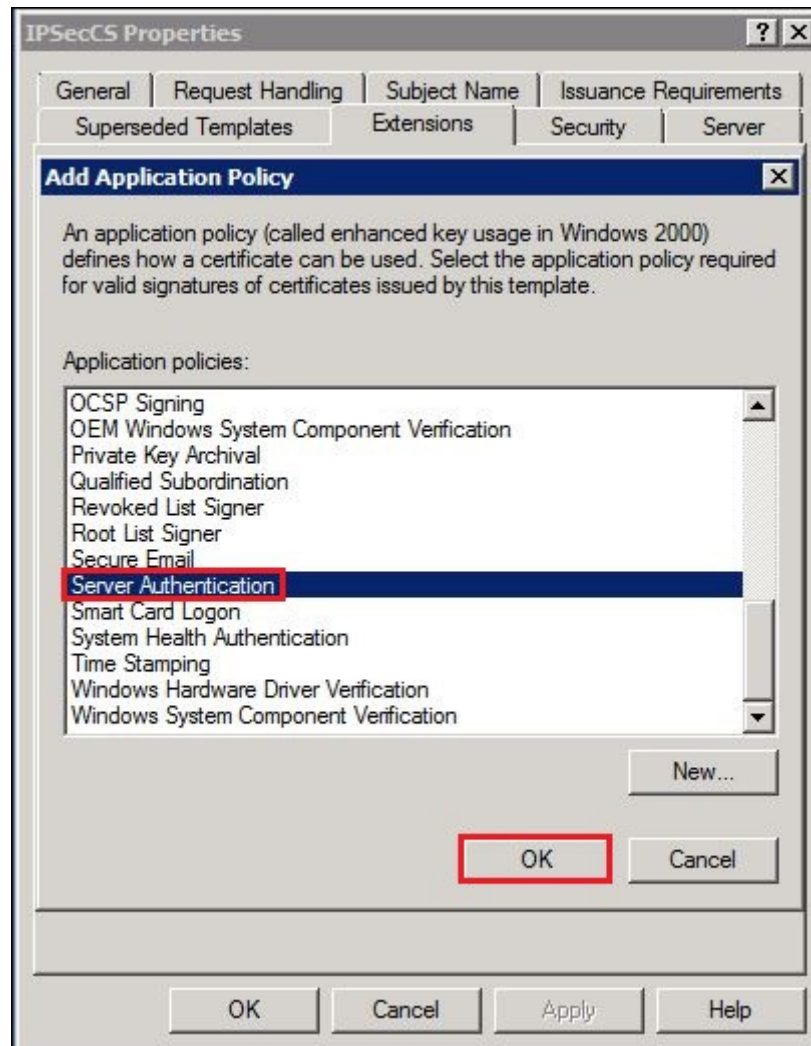
The **Add Application Policy** window will open. Select **Client Authentication** and click on **OK**.



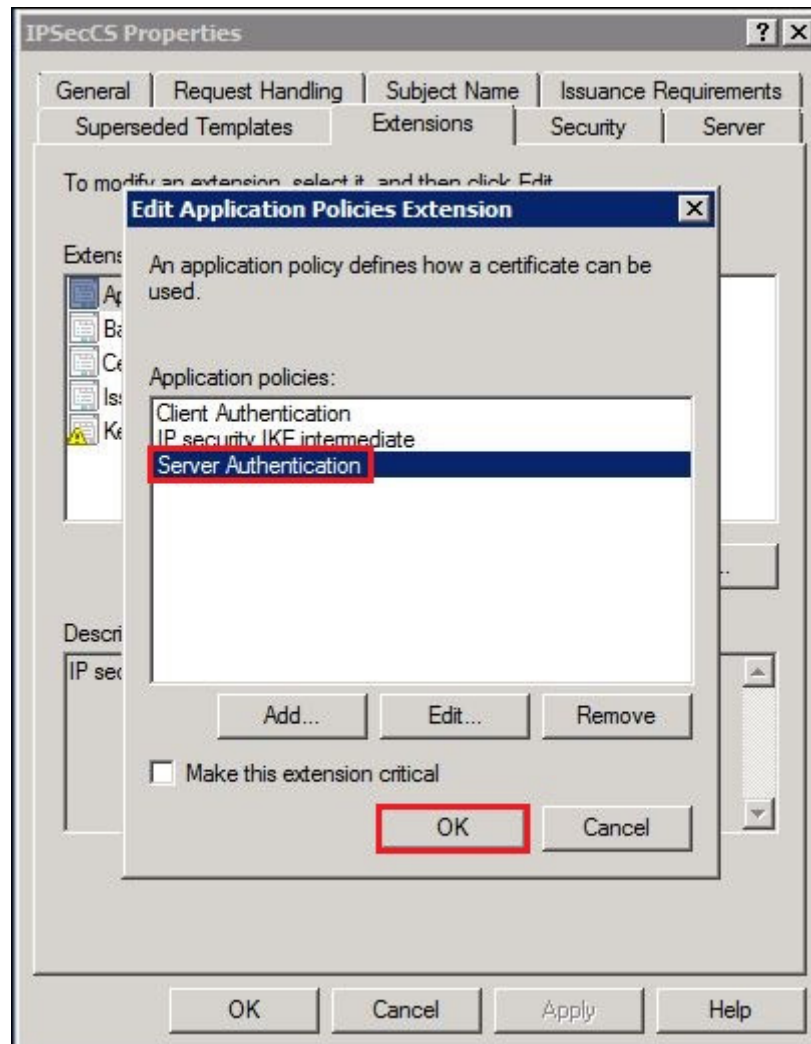
The **Edit Application Policies Extension** window will be displayed and show that **Client Authentication** has been added. Again, click on **Add**.



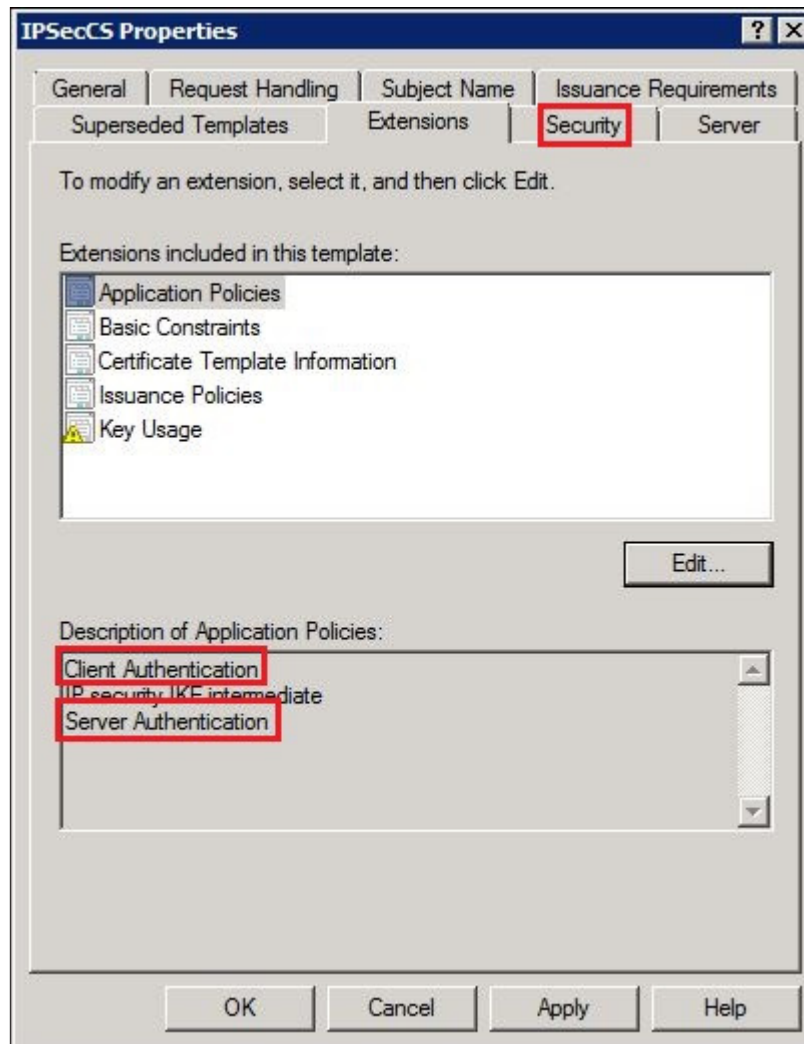
Again, the **Add Application Policy** window will open. Scroll down and select **Server Authentication**. Click on **OK**.



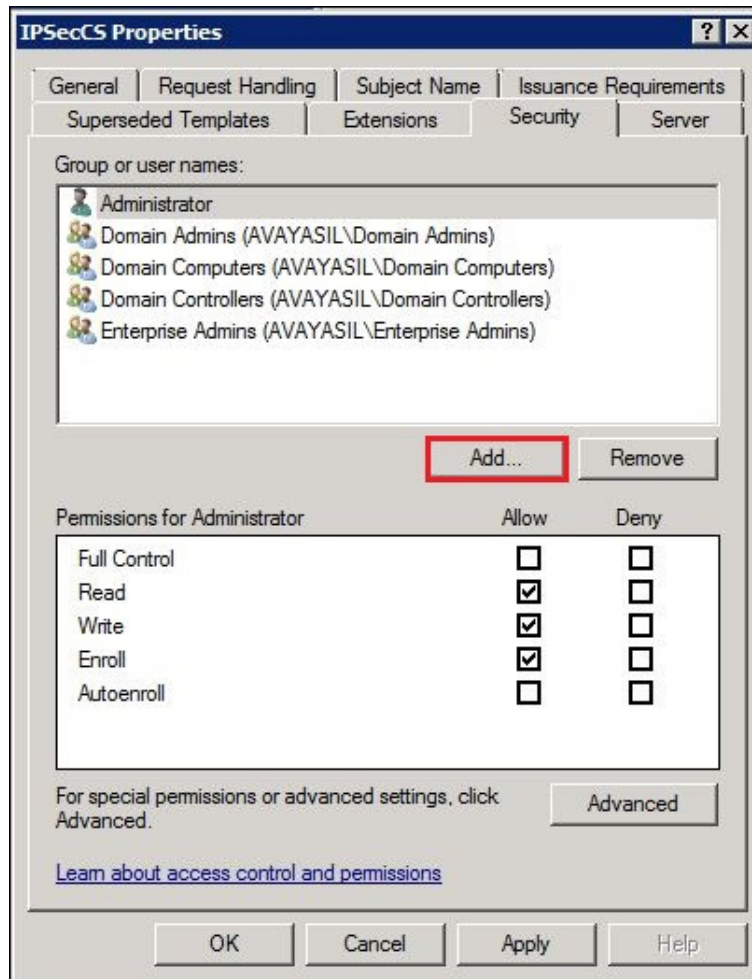
The **Edit Application Policies Extension** window will be displayed and show that **Server Authentication** has been added. Click on **OK**.



Under **Description of Application Policies**, verify **Client Authentication** and **Server Authentication** have been added. Click on the **Security** tab.



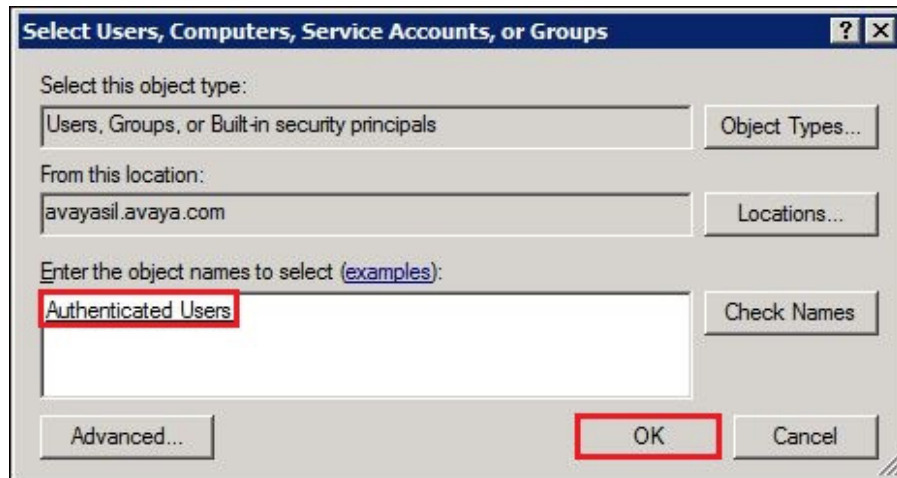
Under the **Security** tab, select **Add**. See below.



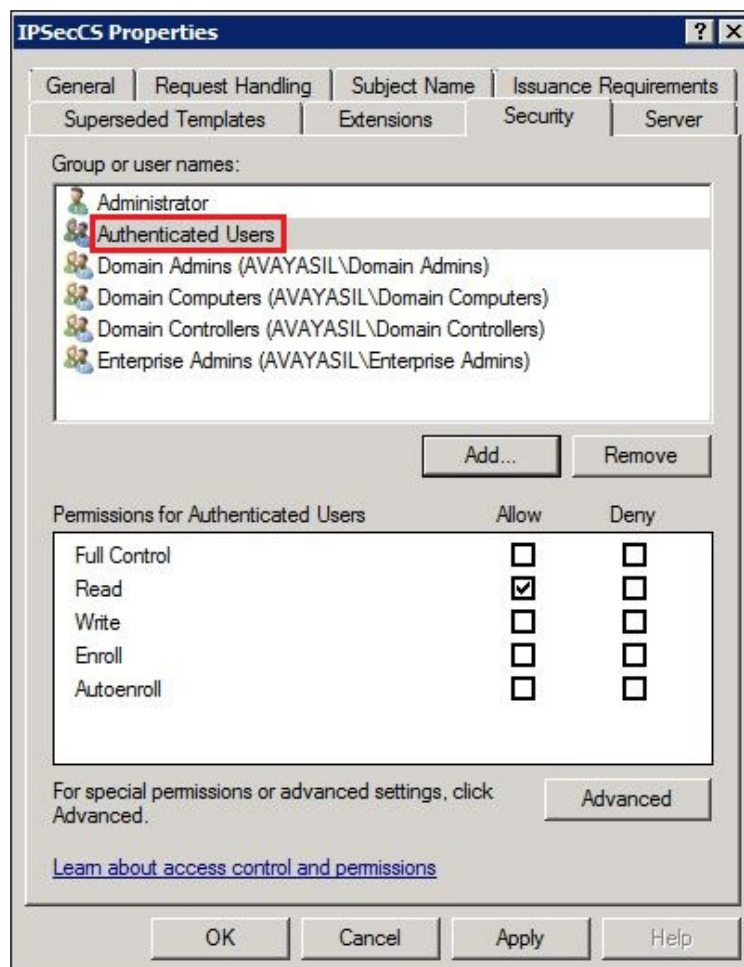
Input **authenticated** and click on **Check Names**.



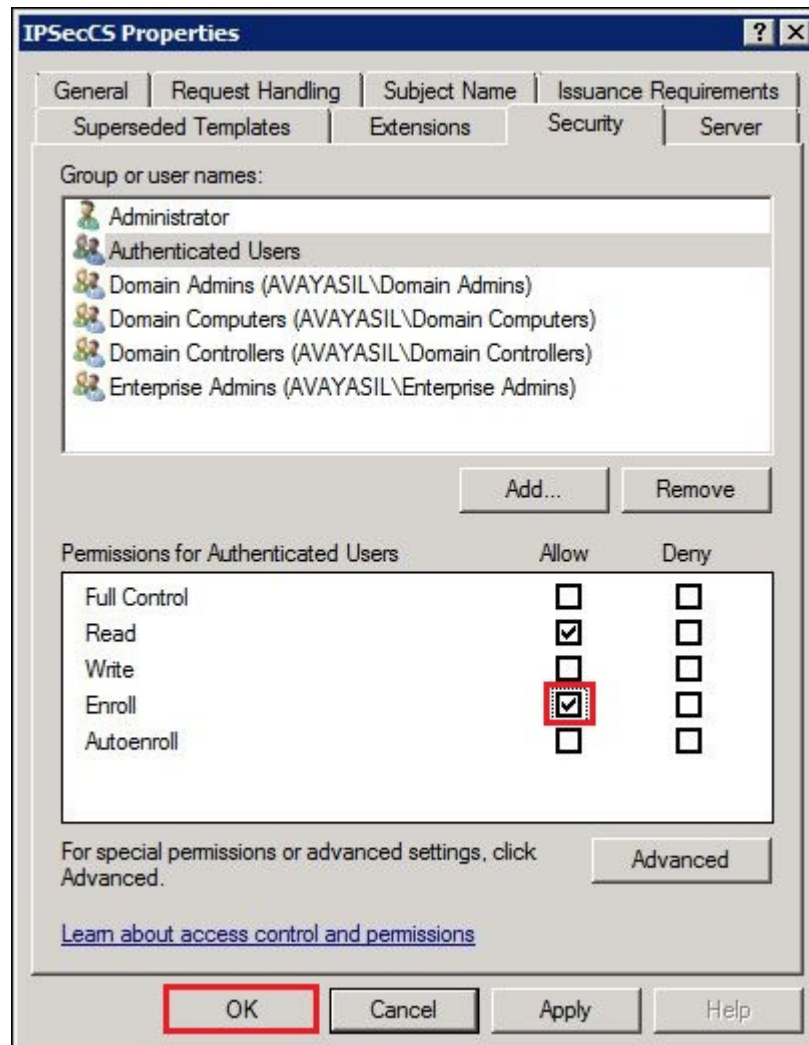
Verify the correct user group was found, **Authenticated Users**. Click on **OK**.



Verify the group is added to the list of **Group or user names**:

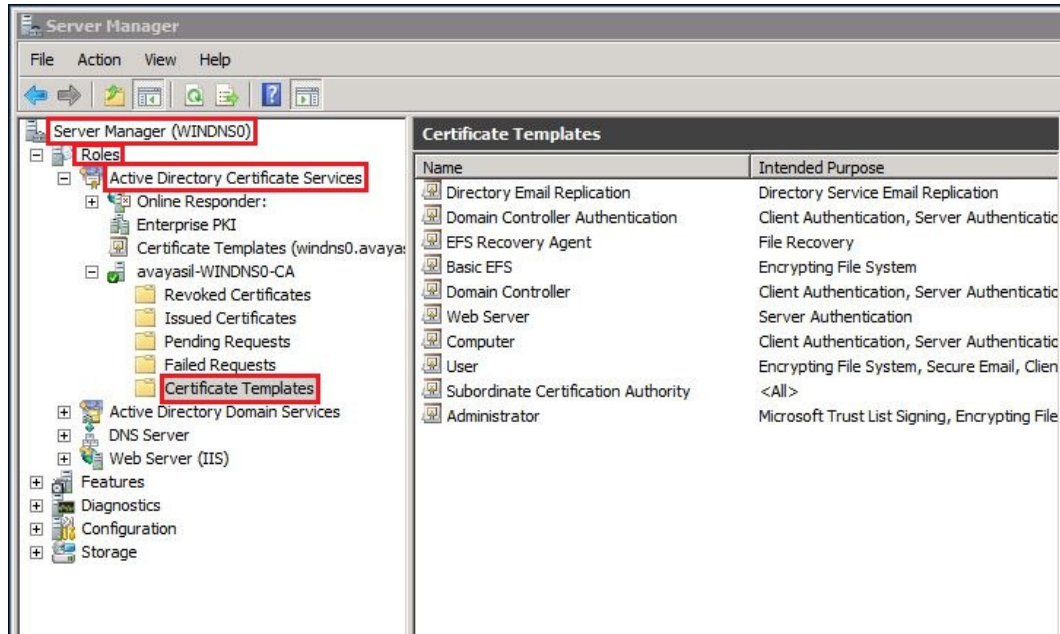


Under **Permissions for Authenticated Users**, check **Enroll** and select **OK** to create the new template.

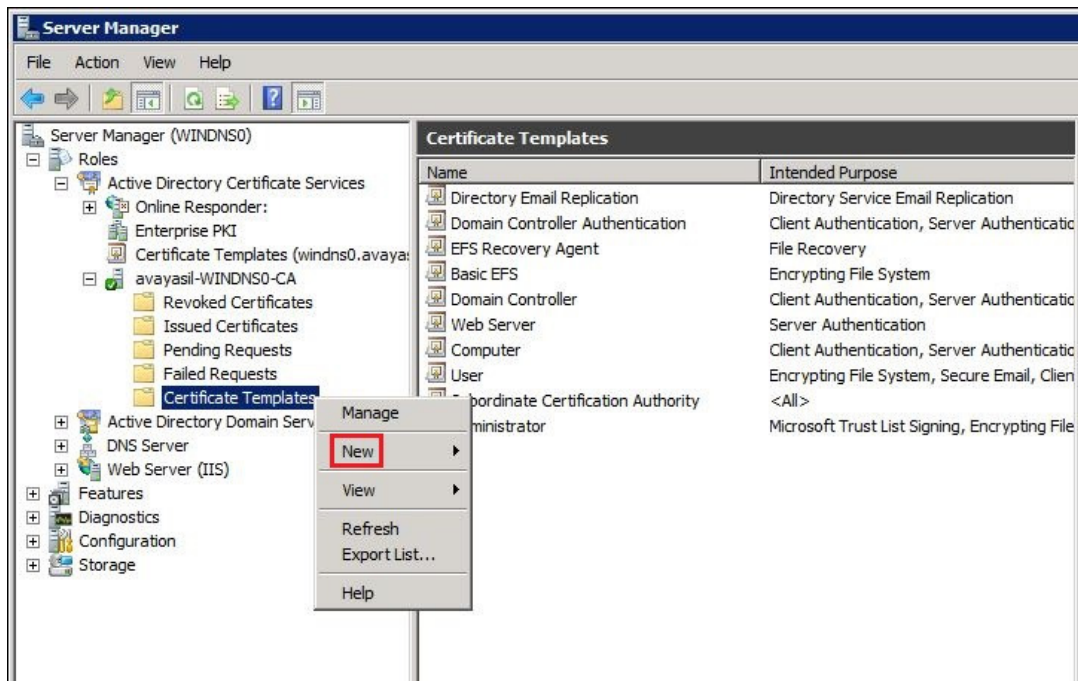


5.5. Issue Certificate Template.

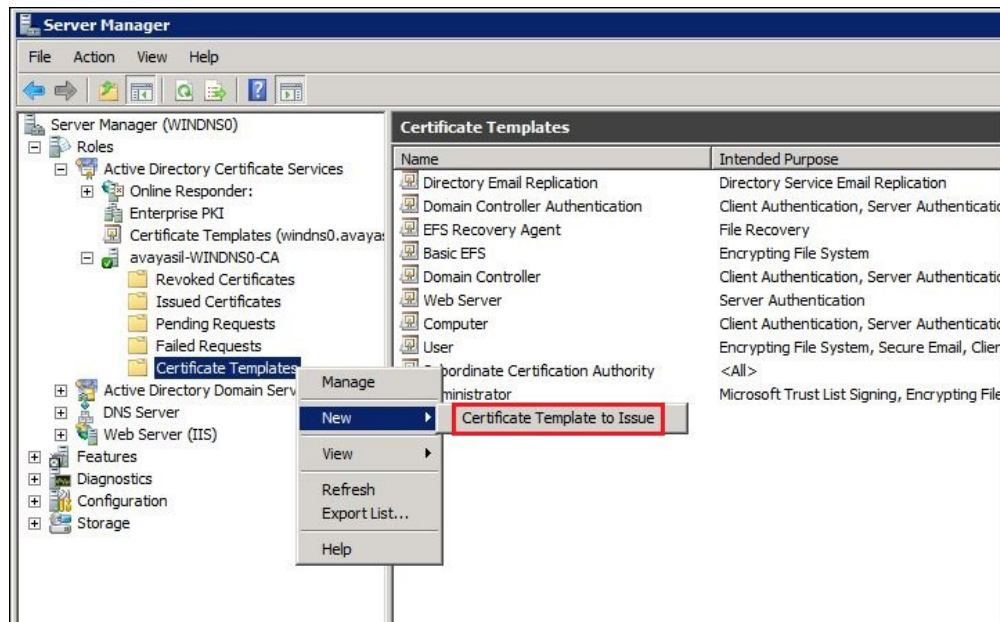
Go to **Server Manager** → **Roles** → **Active Directory Certificate Services** → **Certificate Templates**. See below.



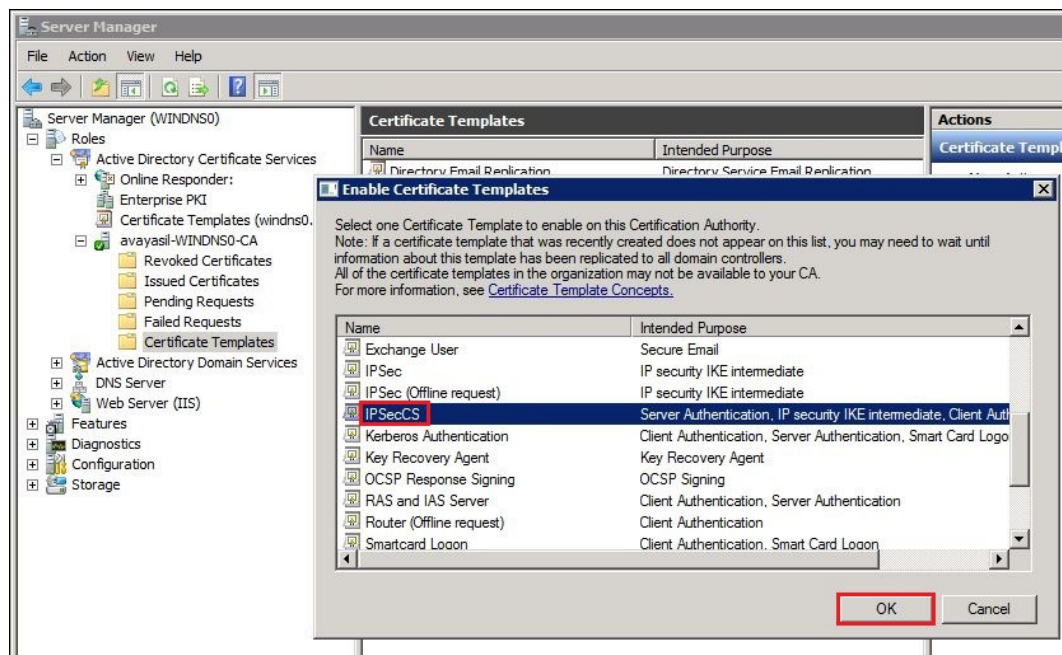
Right click on **Certificate Templates**. Select **New**.



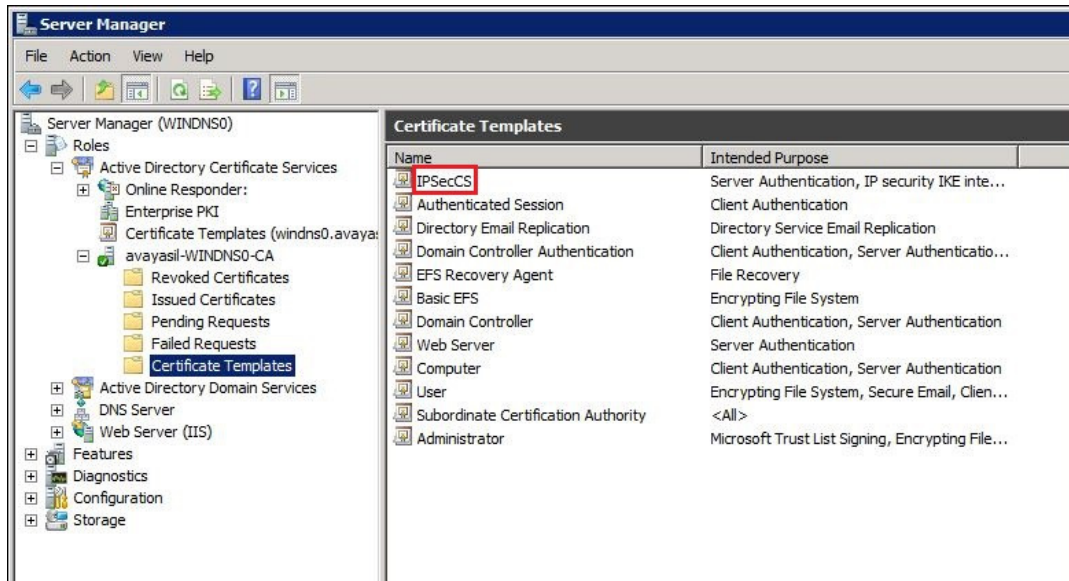
Select **Certificate Template to Issue**.



Scroll down to the template that was created in **Section 5.4**. Select the template and click **OK**.



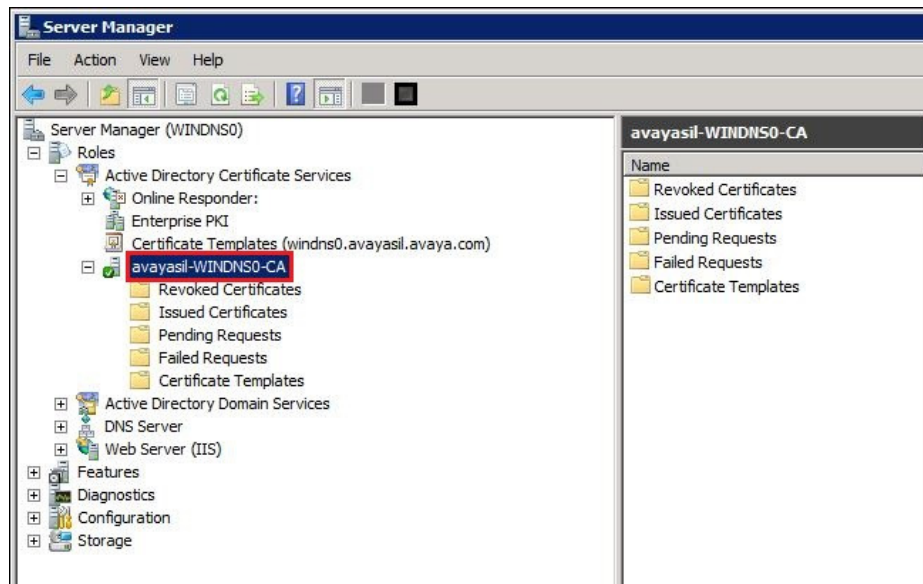
The certificate template has been issued and will be listed under **Certificate Templates**. See below.



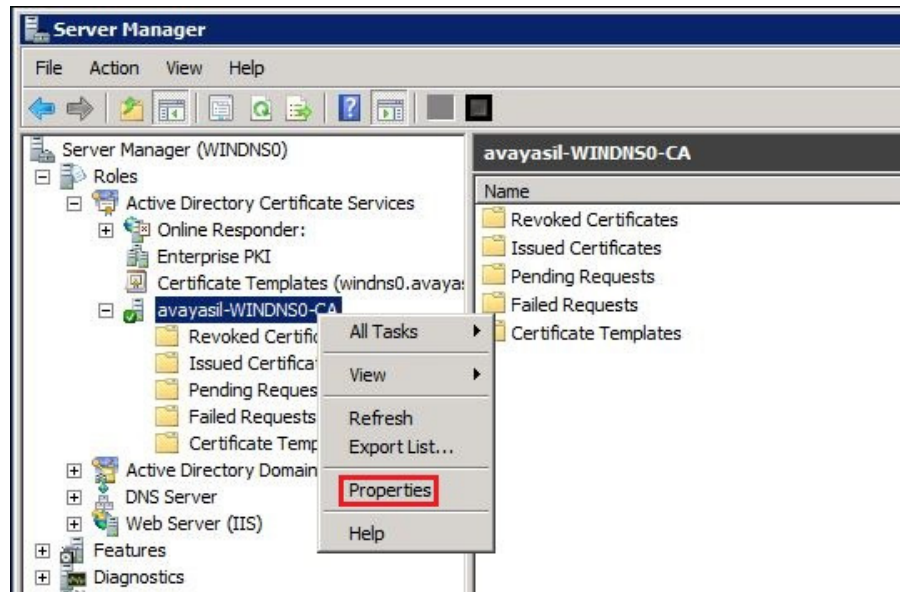
5.6. Export Certificate to .CER file

For the Avaya 96x1 IP telephone to download the digital certificate, the certificate must first be exported from the Microsoft CA to a file with a .cer extension. Microsoft Windows associates files containing a .cer extension with a file type of Security Certificate. The .cer file is then copied to the upload directory of the HTTP server.

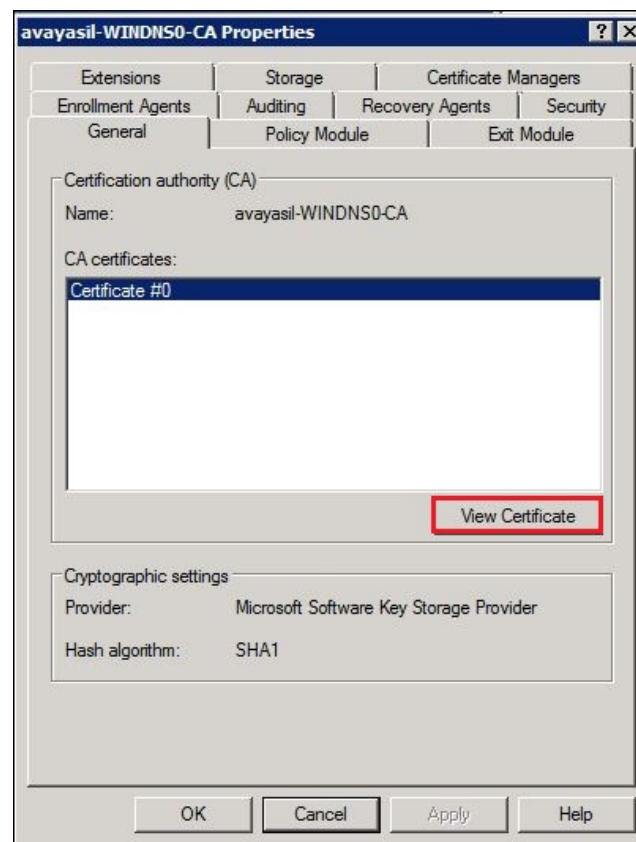
Go to **Start → Administrative Tools → Server Manager**. Select **Server Manager** (not shown). After the window for Server Manager opens, go to **Active Directory Certificate Services** and select the Certificate Authority created in **Section 5.1**. See below.



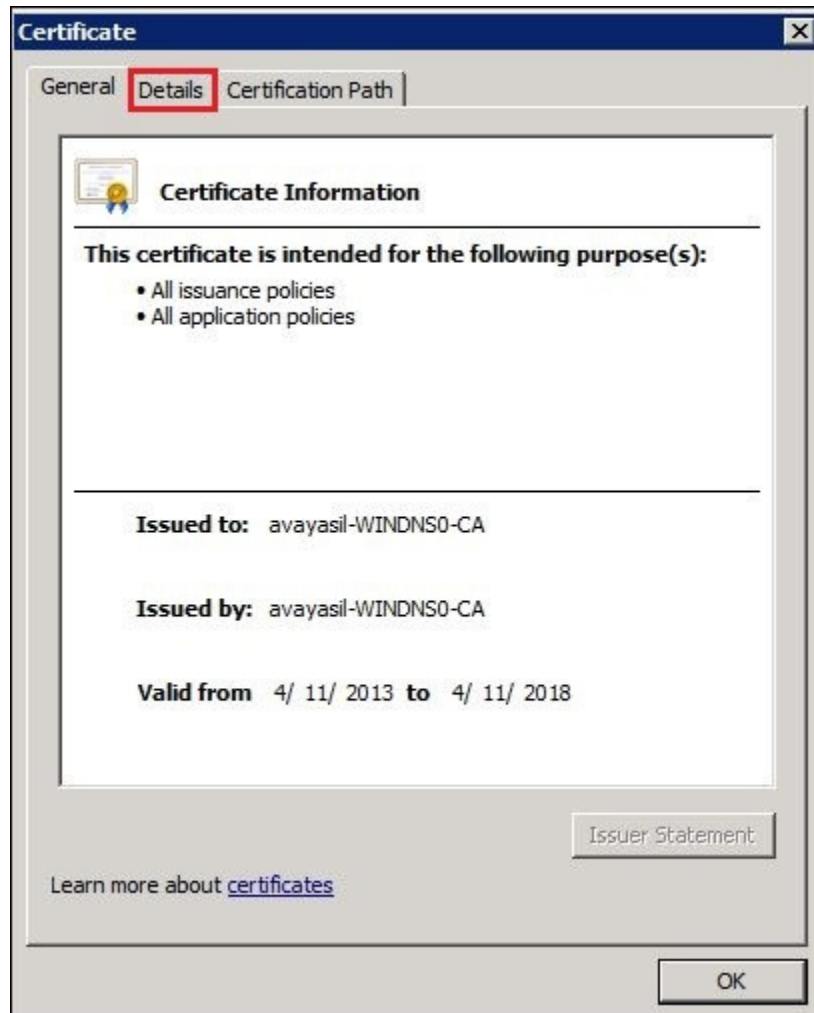
Right click on the Certificate Authority and select **Properties**.



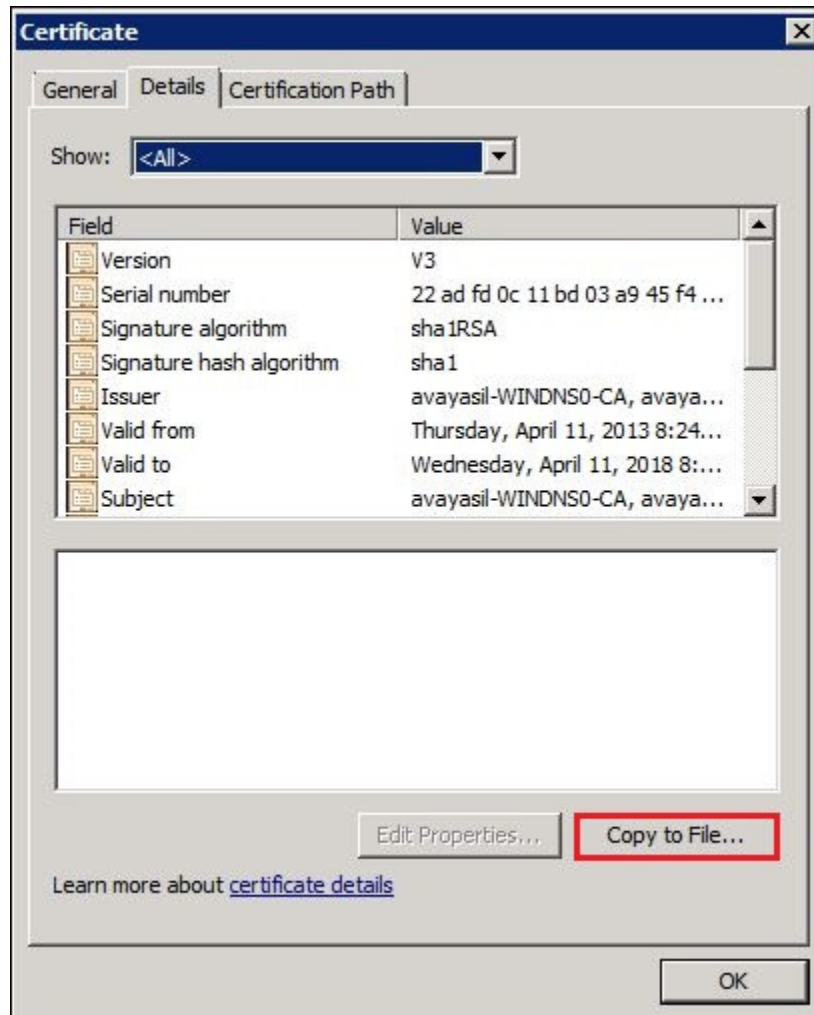
Click on **View Certificate**.



Click on the **Detail** tab of the **Certificate** window.



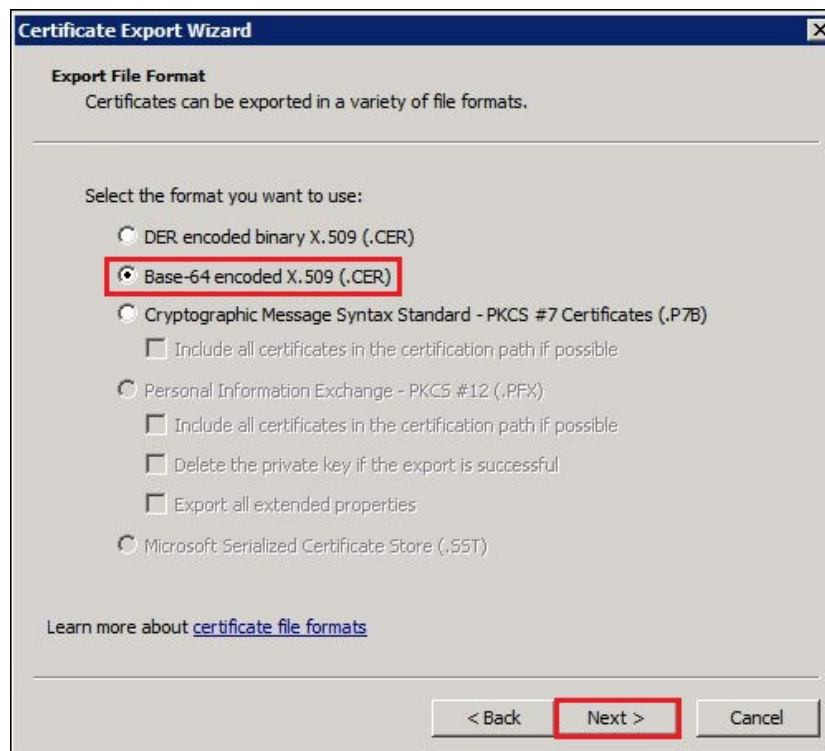
Select **Copy to File**.



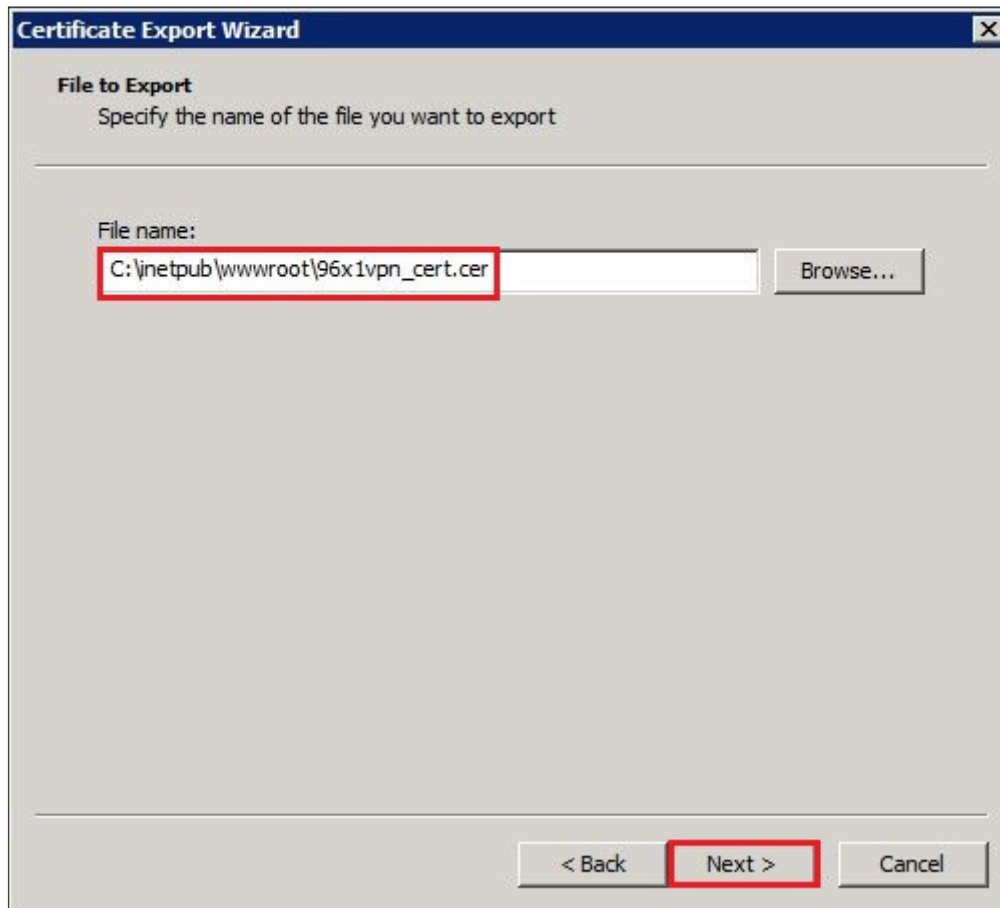
The **Welcome to the Certificate Export Wizard** page is displayed. Click on the **Next** button.



Select the **Base-64 encoded X.509 (.CER)** option. Select **Next**.



Specify a location to store the certificate file. The file was stored in the root directory for Microsoft IIS, **C:\inetpub\wwwroot**. Select the **Next** button.



The image shows a 'Certificate Export Wizard' dialog box. The title bar is blue with the text 'Certificate Export Wizard' and a close button. The main area is light gray. At the top, it says 'File to Export' and 'Specify the name of the file you want to export'. Below this is a 'File name:' label and a text input field containing 'C:\inetpub\wwwroot\96x1vpn_cert.cer'. A 'Browse...' button is to the right of the input field. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red border.

Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name:
C:\inetpub\wwwroot\96x1vpn_cert.cer

Browse...

< Back **Next >** Cancel

The **Completing the Certificate Export Wizard** screen is shown. Select the **Finish** button.



The **export was successful** dialog box is shown to confirm the successful export of the certificates. Click OK.



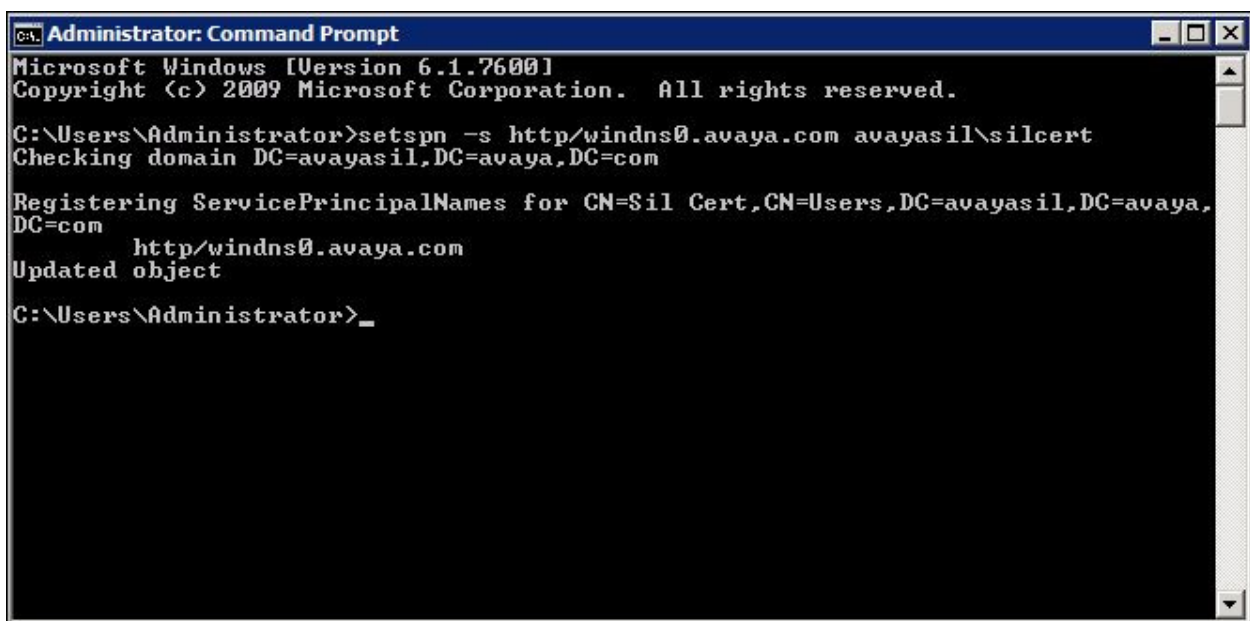
5.7. Execute setspn

The **setspn** command reads, modifies and deletes the Service Principal Names (SPN) directory property for an Active Directory Account. SPNs are used to locate a target principal name for running a service. In this case, the service is NDES. It is a command-line tool built into Windows Server 2008.

As administrator, open a Command Prompt. Input the following command:

```
setspn -s http/windows0.avaya.com avayasil\silcert
```

See the screen below.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -s http/windows0.avaya.com avayasil\silcert
Checking domain DC=avayasil,DC=avaya,DC=com

Registering ServicePrincipalNames for CN=Sil Cert,CN=Users,DC=avayasil,DC=avaya,
DC=com
    http/windows0.avaya.com
Updated object

C:\Users\Administrator>
```

6. Configuration of Avaya 96x1 IP Telephones

The Avaya IP Telephones must undergo staging before being deployed to a remote location. Staging consists of accessing an HTTP server and downloading new firmware, 46xxsettings.txt file, 96Hupgrade.txt file and the certificate to each Avaya IP Telephone. The HTTP server can be Microsoft IIS on the Windows Server 2008 R2. Files needed are the current firmware file, unzipped, the 46xxsettings.file and the certificate file.

6.1. Configuration of 46xxsettings

The 46xxsettings file controls the behavior of the 96x1 IP telephone. For a detailed description of these settings see **Reference 1** in **Section 9**.

SET NVVPNMODE 1

This variable dictates when the VPN Client is started. If its value is 1, VPN Client is started immediately after TCP/IP stack is initialized, If its value is 0, VPN Client is disabled.

SET NVVPNCFGPROF 8

For Cisco authentication with certificates choose option number 8.

The following variables are set to specified value when **NVVPNCFGPROF** is set to **8**:

NVIKECONFIGMODE 1

NVIKEIDTYPE 11

NVIKEXCHGMODE 1

SET NVSGIP 192.145.131.1

Specifies a list of IP addresses for VPN security gateways. Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters; the default value is null ("").

SET NVVPNPSWDTYPE 1

This variable determines how password should be treated. By default, password type is set to 1. You must set this variable to 3 or 4 if using One Time Password such as SecureID from RSA.

SET NVVPNCOPYTOS 1

The value of this variable decides whether TOS bits should be copied from inner header to outer header or not. If its value is 1, TOS bits are copied otherwise not. By default TOS bits are not copied from inner header to outer header. Some Internet Service Providers don't route the IP packets properly if TOS bits are set to anything other than 0.

SET NVVPNENCAPS 0

Specifies type of UDP encapsulation method to use if there is a NAT device between phone and the security gateway. By default UDP Encapsulation 4500-4500 is used.

0 4500-4500

1 Disable

2 2070-500

4 RFC (As per RFC 3947 and 3948)

SET NVIKEID VPNPHONE

The phones use this string as IKE Identifier during phase 1 negotiation. Some XAuth documentation refer to this variable as group name because same IKE Id is shared among a group of user and individual user authentication is done using XAuth after establishing IKE phase 1 security association. The default value is "VPNPHONE".

SET NVIKEXCHGMODE 2

Specifies the exchange method to be used for IKE Phase 1.

- 1 Aggressive Mode (default)
- 2 Main Mode

SET NVIKEDHGRP 2

This variable contains the value of the DH group to use during phase 1 negotiation. By default phones use Group 2.

SET NVPFSDHGRP 2

This variable contains the value of DH group to use during phase 2 negotiation for establishing IPsec security associations also known as perfect forward secrecy (PFS). By default PFS is disabled.

SET NVIKEP1ENCALG 1

Security Gateway picks the algorithm mandated by administrator.

- 0 ANY
- 1 AES-128**
- 2 3DES
- 3 DES
- 4 AES-192
- 5 AES-256

SET NVIKEP2ENCALG 1

Security Gateway picks the algorithm mandated by administrator.

- 0 ANY
- 1 AES-128**
- 2 3DES
- 3 DES
- 4 AES-192
- 5 AES-256

SET NVIKEP1AUTHALG 2

- 0 ANY
- 1 MD5
- 2 SHA1**

SET NVIKEP2AUTHALG 2

0 ANY
1 MD5
2 SHA1

SET TRUSTCERTS 96x1vpn_cert.cer

List of trusted certificates to download to phone. This parameter may contain one or more certificate filenames, separated by commas without any intervening spaces. Files may contain only PEM-formatted certificates.

SET MYCERTKEYLEN 2048

Specifies the bit length of the public and private keys generated for the SCEP certificate request. 4 ASCII numeric digits, "1024" through "2048"; the default value is "1024".

SET MYCERTWAIT 0

Specifies whether the telephone will wait until a pending certificate request is complete, or whether it will periodically check in the background.

SET MYCERTURL <http://10.129.112.20/certsrv/mscep/mscep.dll>

URI used to access SCEP server.

6.2. Upload Certificates to 96x1 IP Telephone

To upload the exported certificates to the 96x1 IP telephone the 46xxsettings file is used. A number of settings need to be adjusted within the settings file to accomplish this. The SET TRUSTCERTS is set to the file name **96x1vpn_cert.cer**, the file name of the exported certificates in **Section 5.6**. With these settings in the 46xxsettings file, the 96x1 IP telephone is rebooted to upload the new 46xxsettings file to the 96x1 IP telephone. When the 96x1 IP telephone receives the 46xxsettings file, the IP telephone will enroll with the Microsoft CA. The 96x1 IP telephone begins the uploading of the certificates to the IP telephone. The SCEP timeout is displayed on the 96x1 IP telephone as the certificates are uploaded.

SCEP 10 secs

The 96x1 IP telephone has begun requesting the certificates from the Microsoft CA and will continue requesting the certificate for 60 minutes until the certificate is issued.

The following screen is displayed on the 96x1 IP telephone.

SCEP Successful

7. Verification Steps

The following verification steps were tested using the sample configuration.

7.1. Verify Staging

Using HTTP, the Avaya IP Phone must download the following files:

- 96x1Hupgrade.txt
- 46xxsettings.txt
- 96x1vpn_cert.cer

Once the certificate is installed, SCEP displays **Successful**. (See **Section 6.2**).

7.2. Verify registration with Avaya Aura® Communication Server.

The Avaya 96x1 IP Telephone will prompt for extension and password then locate the call server.

7.3. Verify IP Phone can Send and Receive Calls

Place a call from the staged IP Telephone to a corporate phone. Insure bi-directional audio.
Place a call from a corporate IP Telephone to a staged phone. Insure bi-directional audio.

8. Conclusion

These Application Notes describe the steps required to install Windows Server 2008 R2, Enterprise Edition, with Microsoft Certificate Authority and Network Device Enrollment Service using Simple Certificate Enrollment Protocol for certificate authentication with Avaya 96x1 IP Telephones in VPN mode.

9. Additional References

This section references the documentation relevant to these Application Notes.

For Avaya, additional product documentation is available at <http://support.avaya.com>.

1. VPN Setup Guide for 9600 Series IP Telephones Release 3.1 and 6.2, January 2013, Doc ID 16-602968
2. Administering Avaya Aura® Communication Manager, Release 6.2, Doc ID 03-300509, Issue 7.0, February 2012
3. Administering Avaya Aura® Messaging, Release 6.2, Issue 2.1, February 2013

Avaya Application Notes

4. Configuring an IPSec Tunnel between Avaya 96xx Series IP Phones and the Cisco Adaptive Security Appliance 5510
5. Configuring Avaya 9600 Series IP Telephone VPN feature for Certificate Authentication using Cisco 5510 Adaptive Security Appliance and Microsoft Certificate Authority with Avaya Aura™ Communication Manager
6. Configuring Avaya 96x1 Series IP Telephone VPN feature with Cisco 5510 Adaptive Security Appliance using Microsoft Windows Server 2008 Certificate Authority and Network Device Enrollment Service with Simple Certificate Enrollment Protocol

Product documentation for Microsoft products may be found at <http://www.microsoft.com>

7. Introducing Windows Server 2008 R2, by Charlie Russell and Craig Zacker with the Windows Server Team at Microsoft, e-book published by Microsoft, 2010.
8. Windows Server 2008 and Windows Server 2008 R2, [http://technet.microsoft.com/en-us/library/dd349801\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd349801(v=ws.10).aspx)

©2013 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com