Avaya Solution & Interoperability Test Lab

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

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.

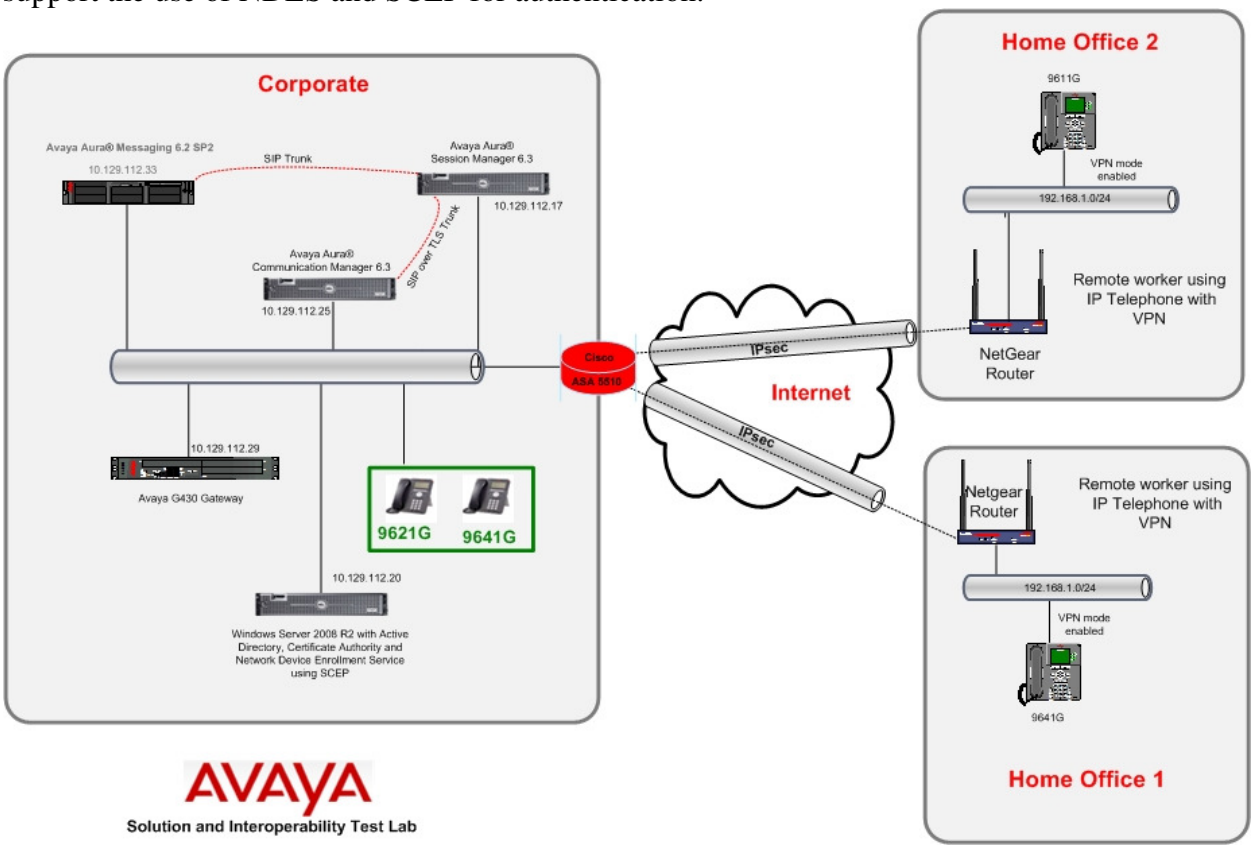


Figure 1: Windows Server 2008 R2 with Active Directory, Microsoft Certificate Authority and Network Device Enrollment Service using SCEP for 96x1 certificate authentication

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

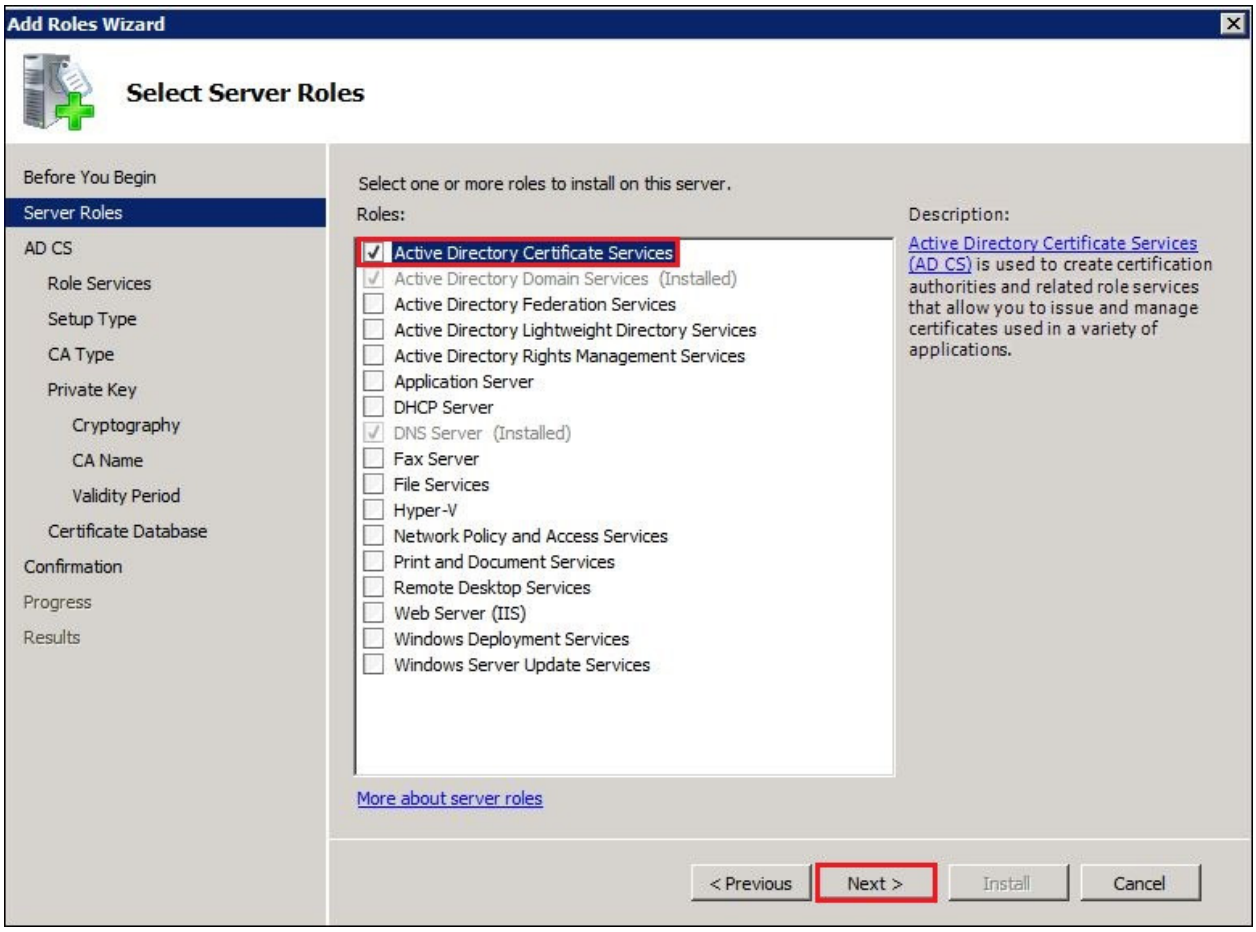
To access the Windows 2008 Server, open a remote desktop connection and input the IP Address of the Windows 2008 Server. This was **10.129.112.20**. Press **Connect** to access the Windows 2008 Server.

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

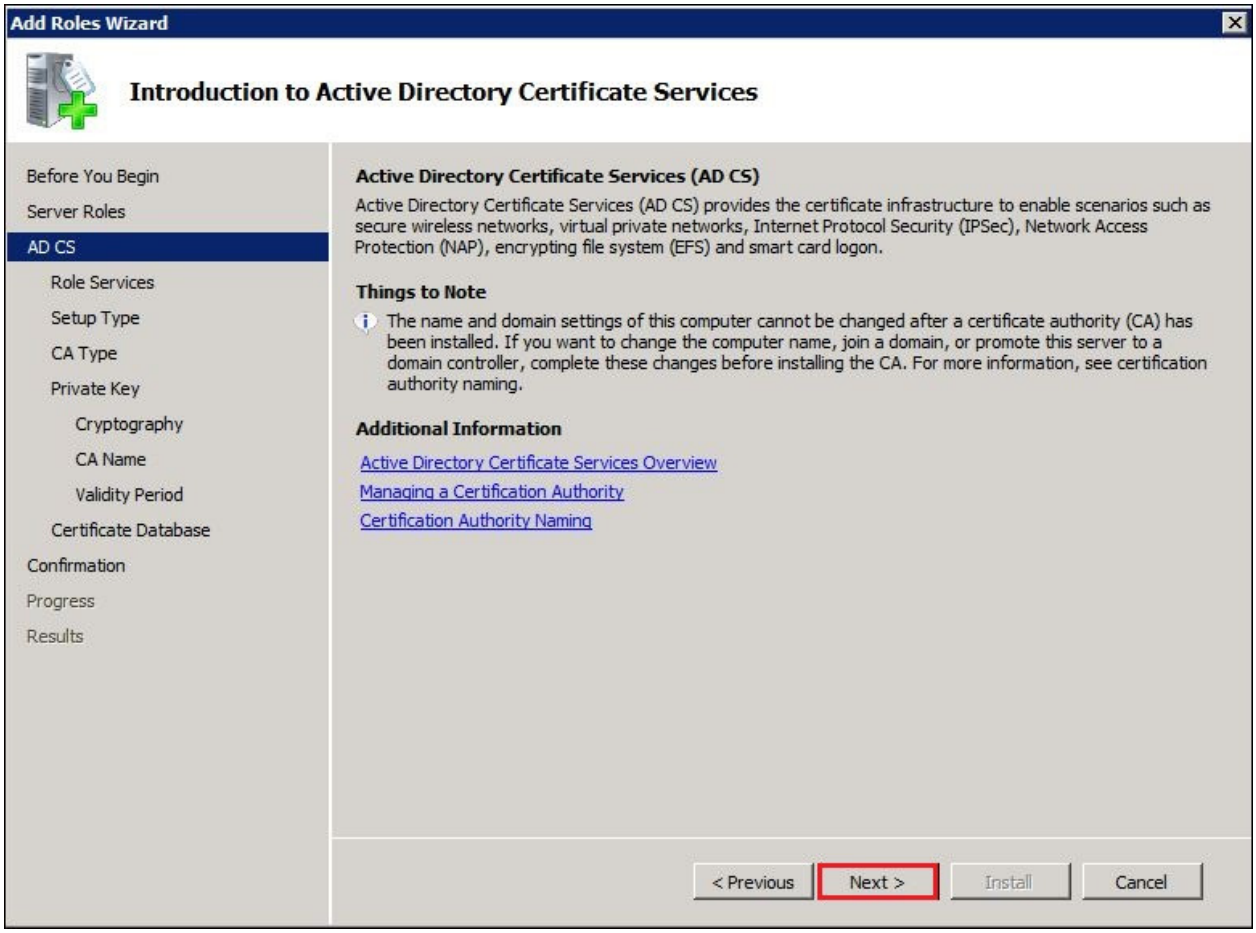
5.1. Install Microsoft Certificate Authority

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).

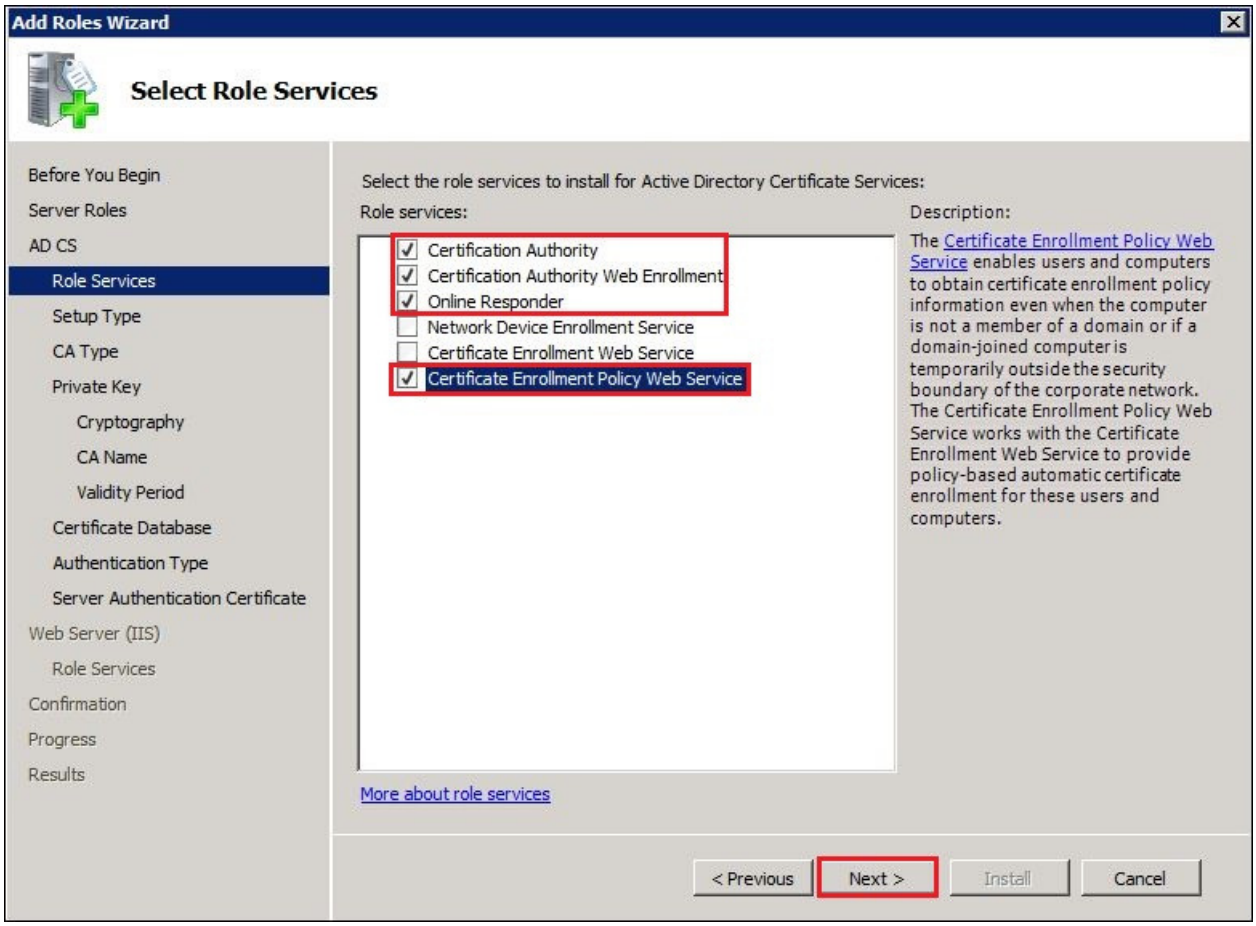
Place a check by **Active Directory Certificate Services.** Click **Next.** See below.



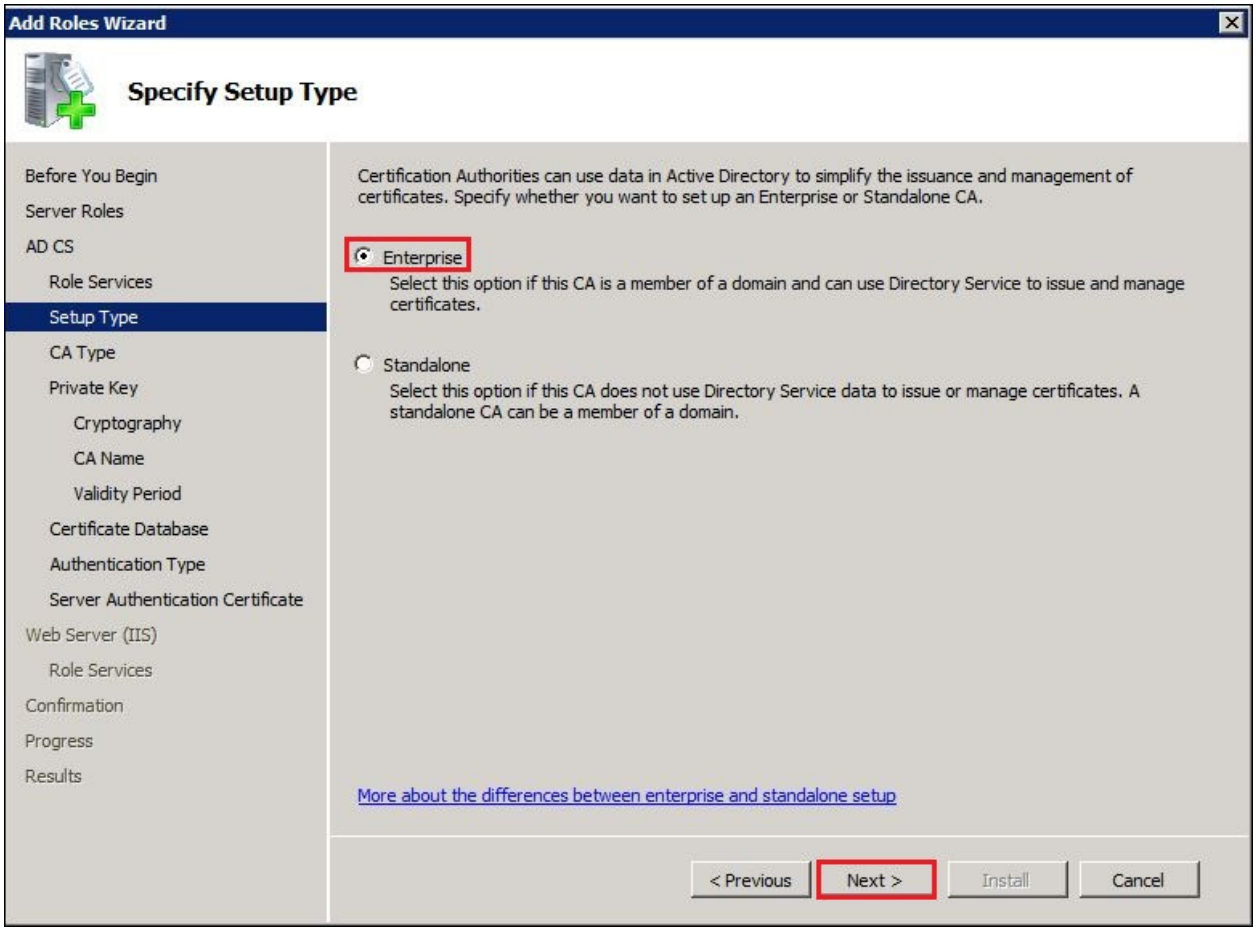
This is an informational screen. Click **Next**.



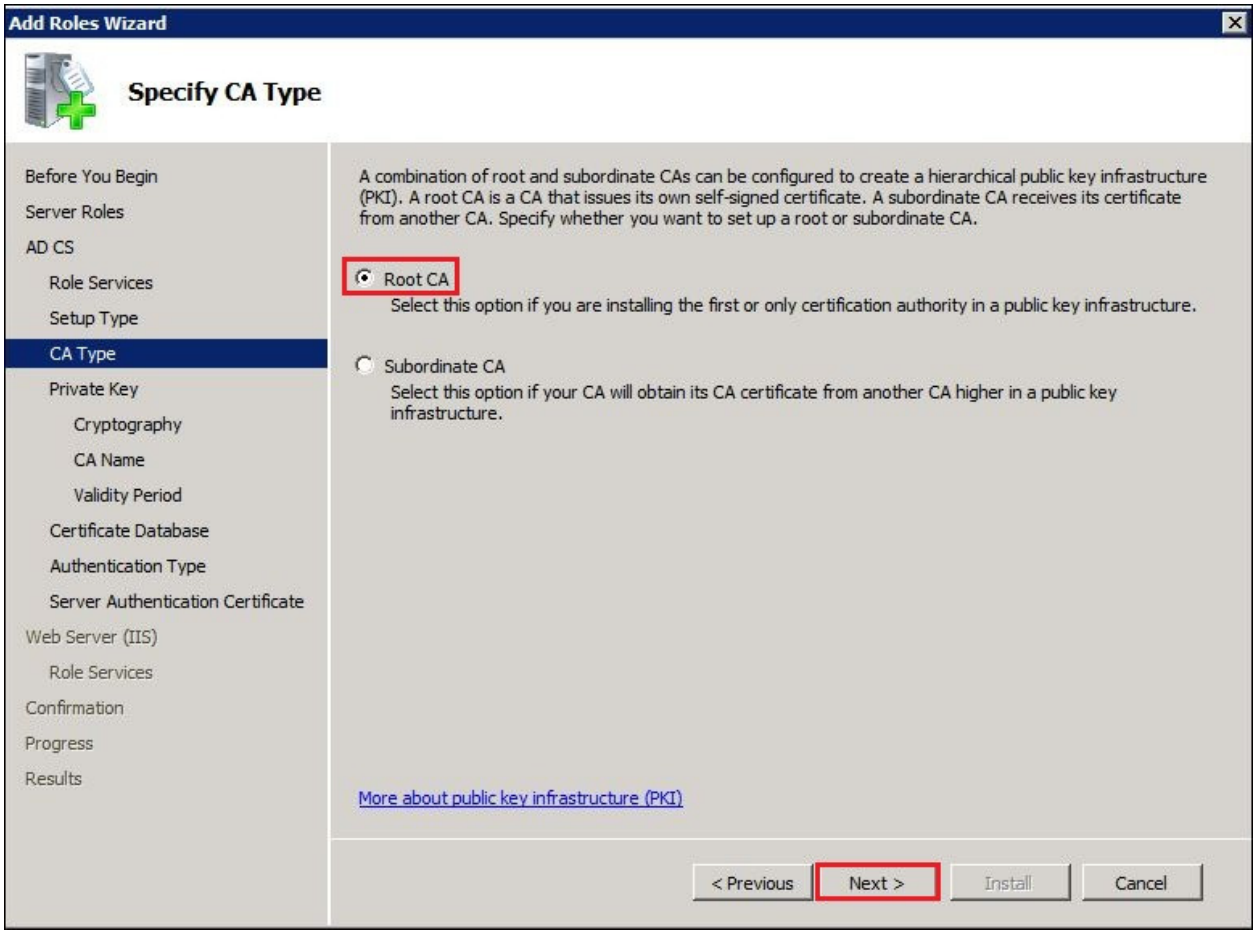
Check **Certification Authority**, **Certification Authority Web Enrollment**, **Online Responder** and **Certificate Enrollment Policy Web Service**. Network Device Enrollment Service and Certificate Enrollment Web Service cannot be installed at the same time as the Certificate Authority so will be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



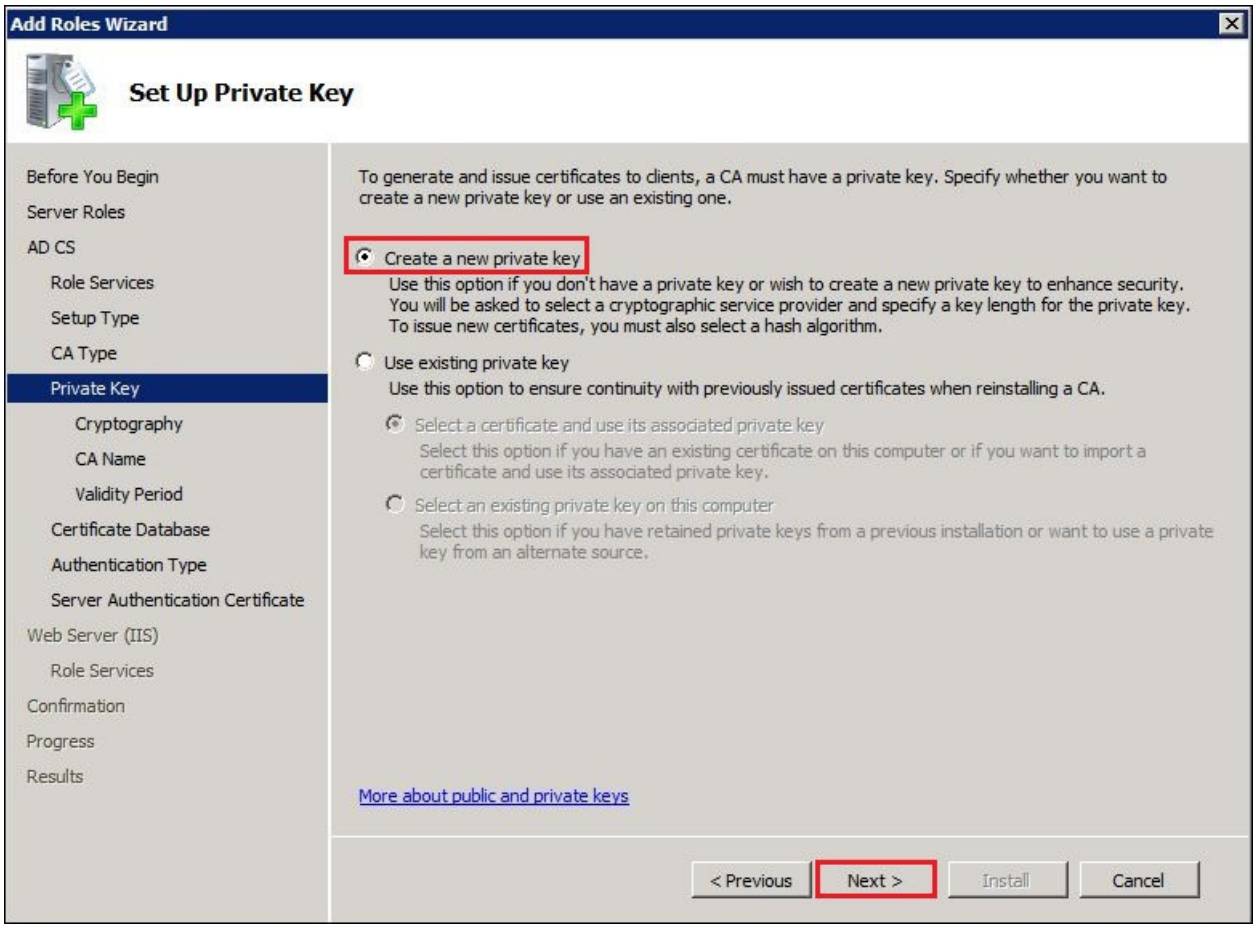
For the sample configuration **Enterprise** was selected. Click **Next**.



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



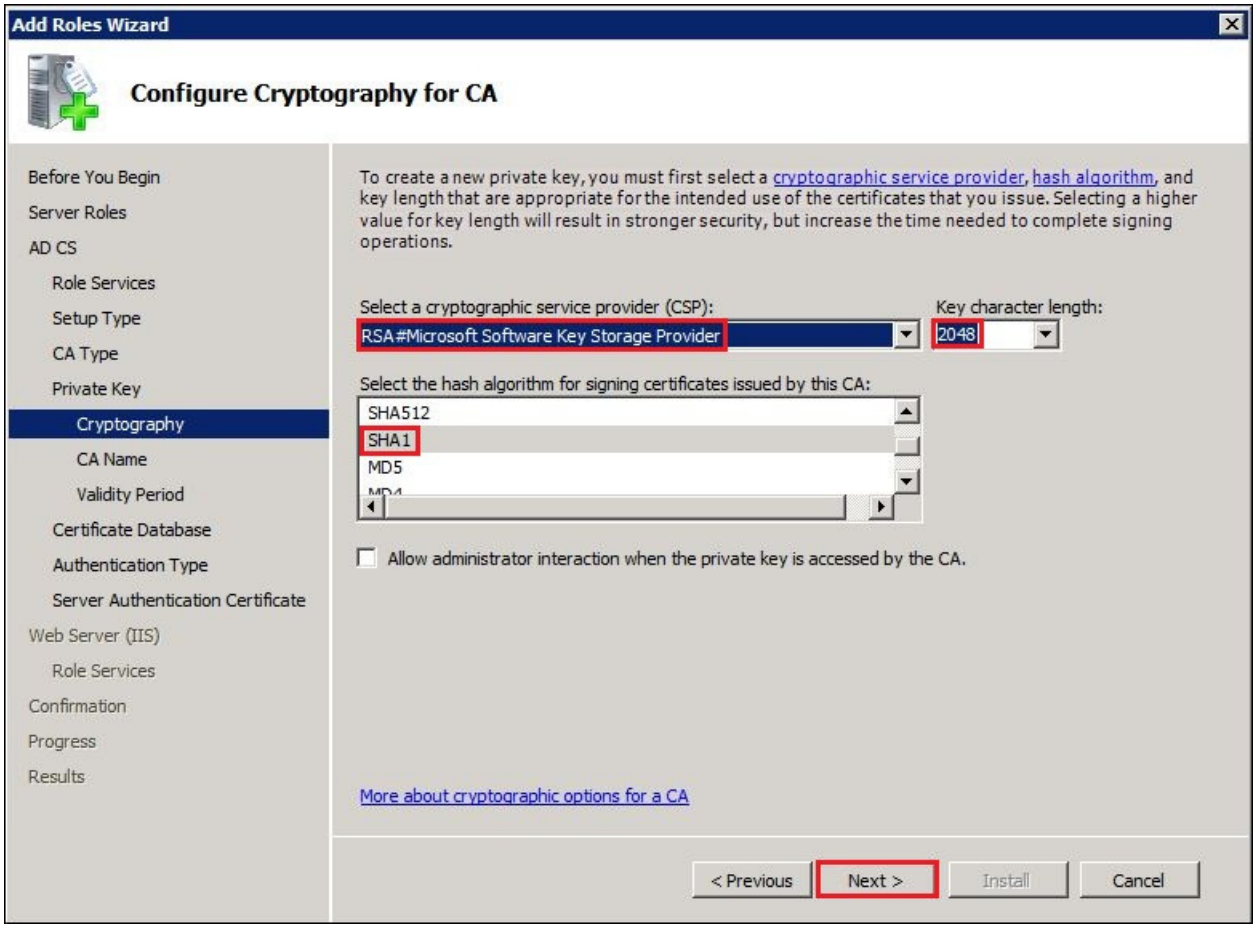
Create a Private Key for the new Certificate Authority. Select **Create a new private key**. Click on **Next**.



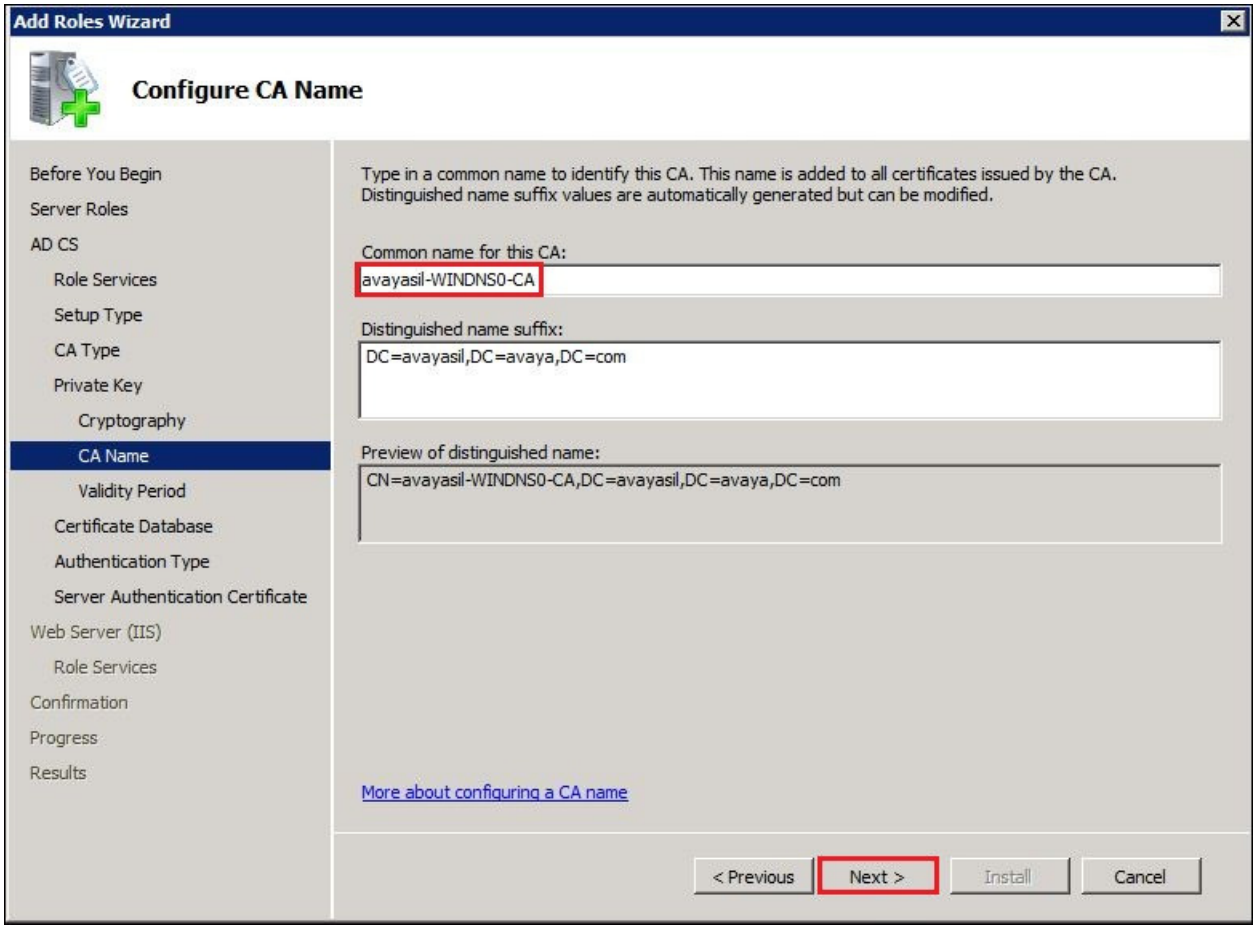
The Configure Cryptography for CA screen is displayed.

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

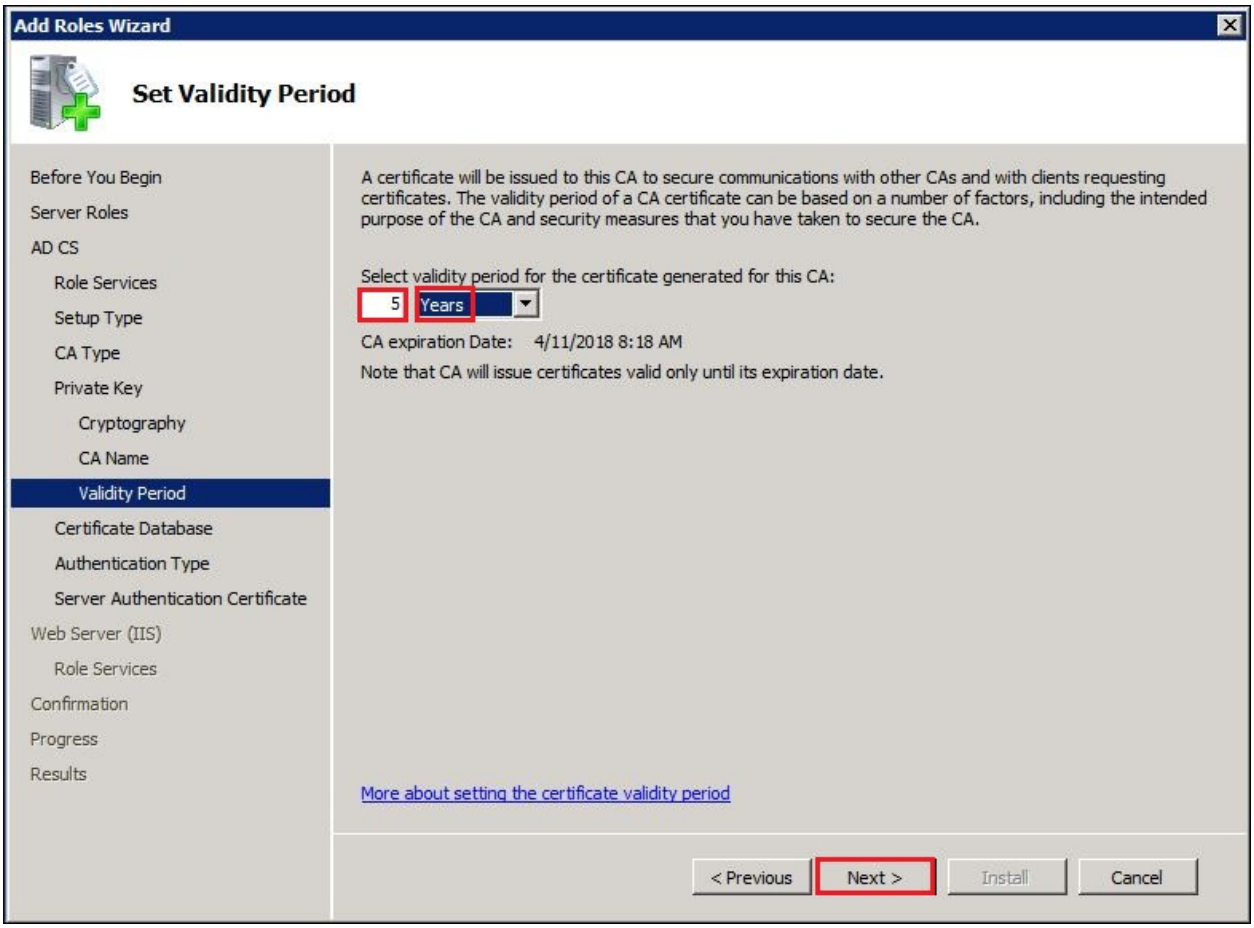
Click on **Next**.



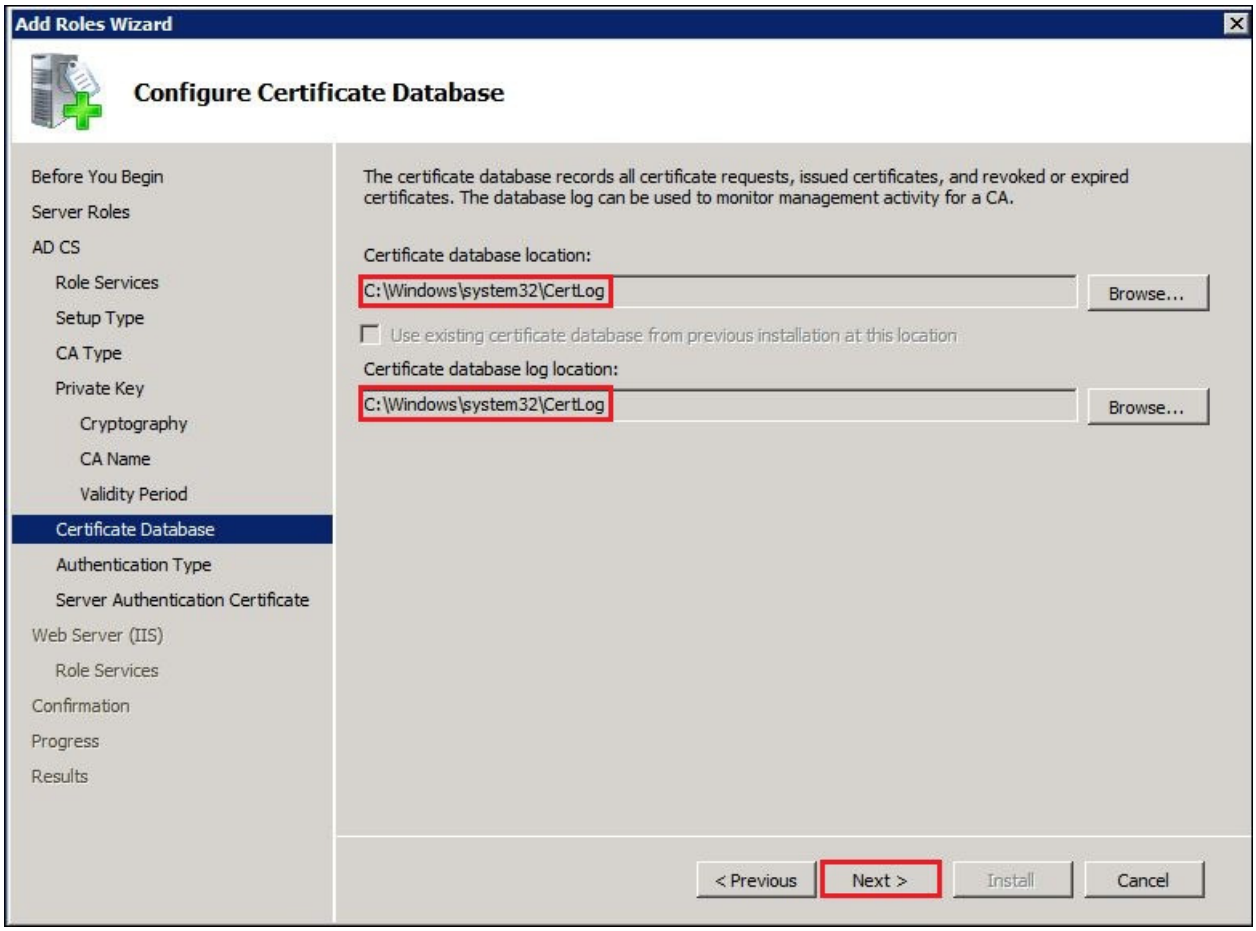
Accept the default **Common name for this CA** by Clicking on **Next**.



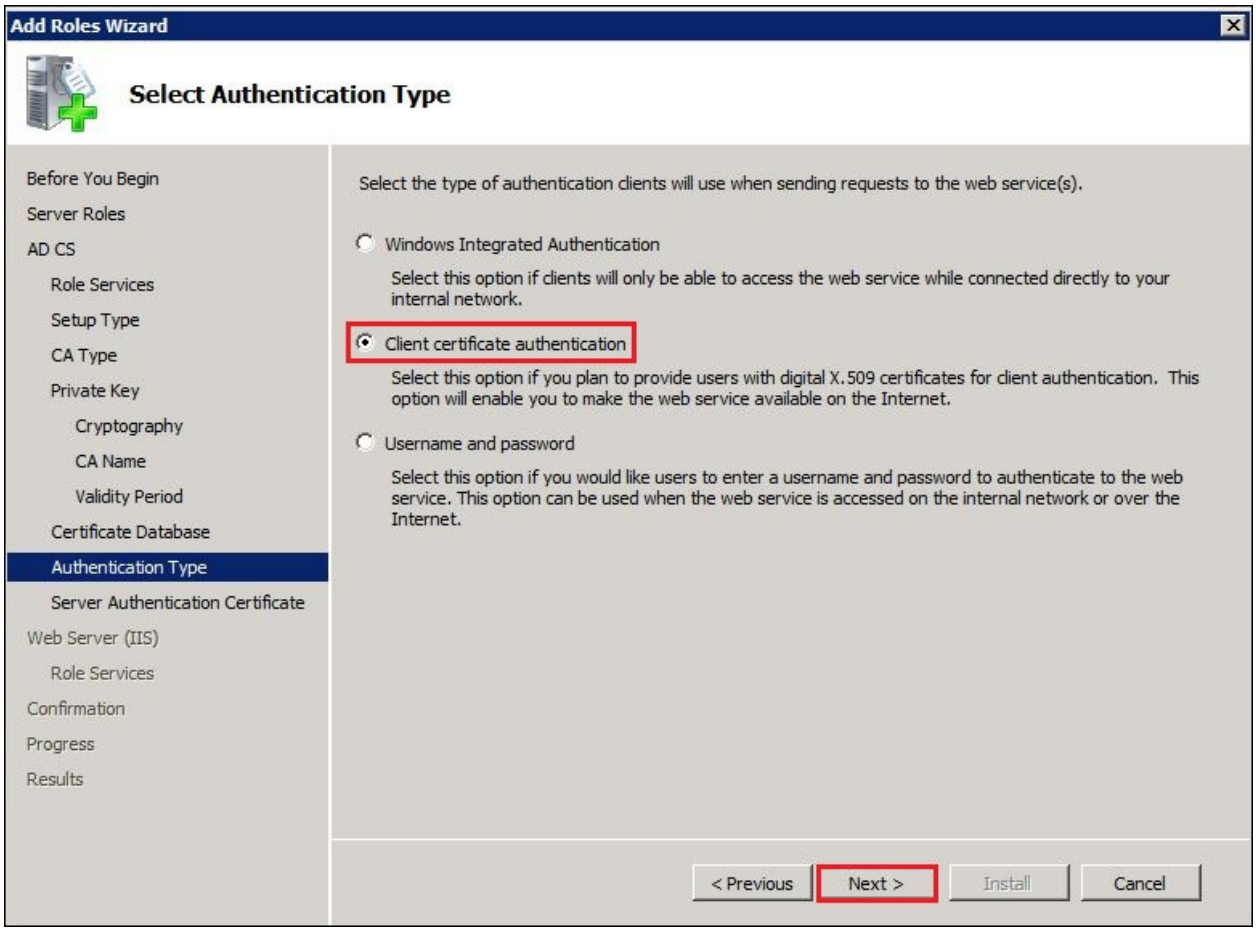
Determine the length of time that the certificates will be valid. 5 years is the default value. Click **Next**.



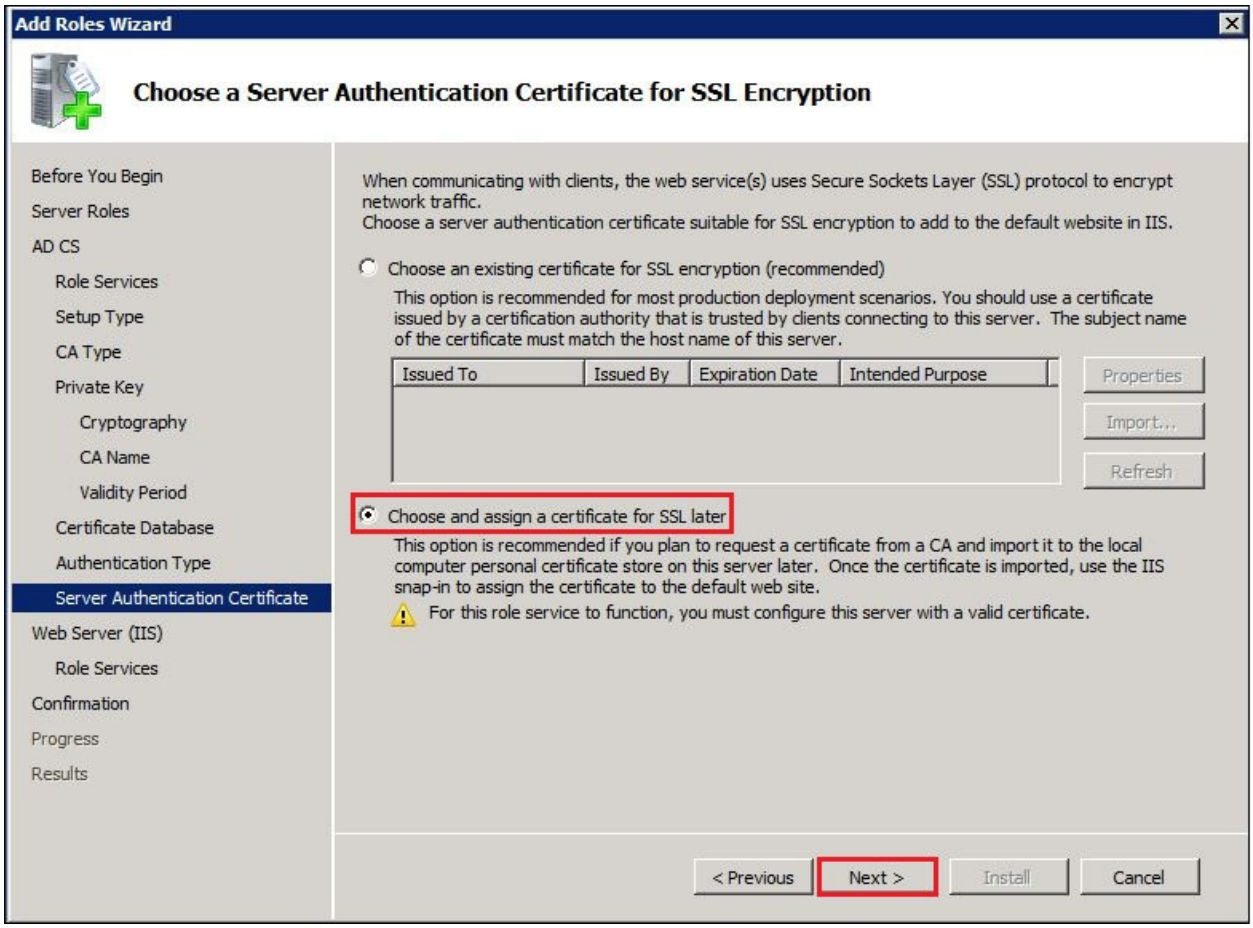
Accept the default location for the Certificate Database and Certificate Database Log by clicking **Next**.



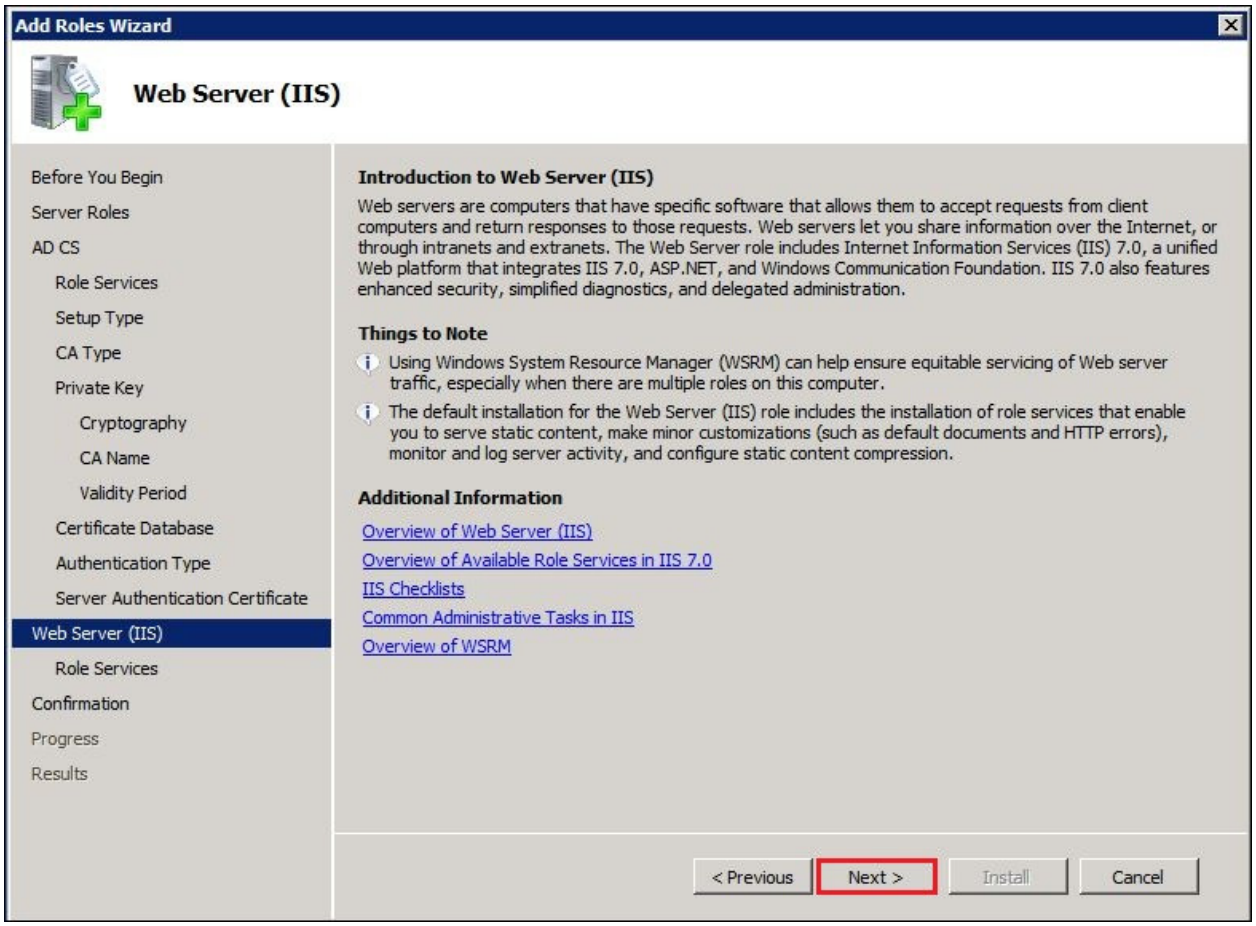
To use Avaya 96x1IP Telephones with certificates installed, Select **Client certificate authentication** and click on **Next**.



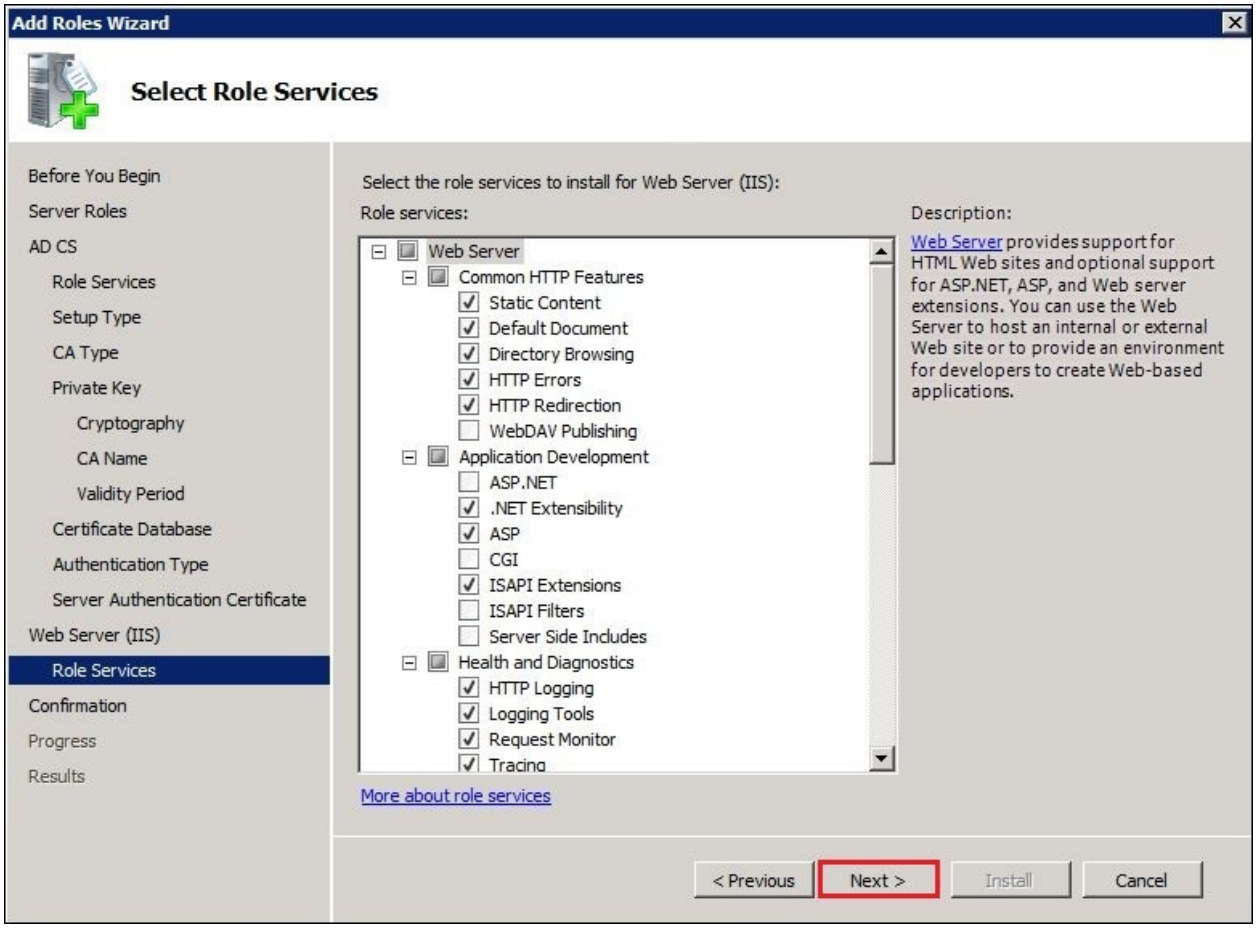
Since this is a standalone server, select **Choose and assign a certificate for SSL later** and Click on **Next**.



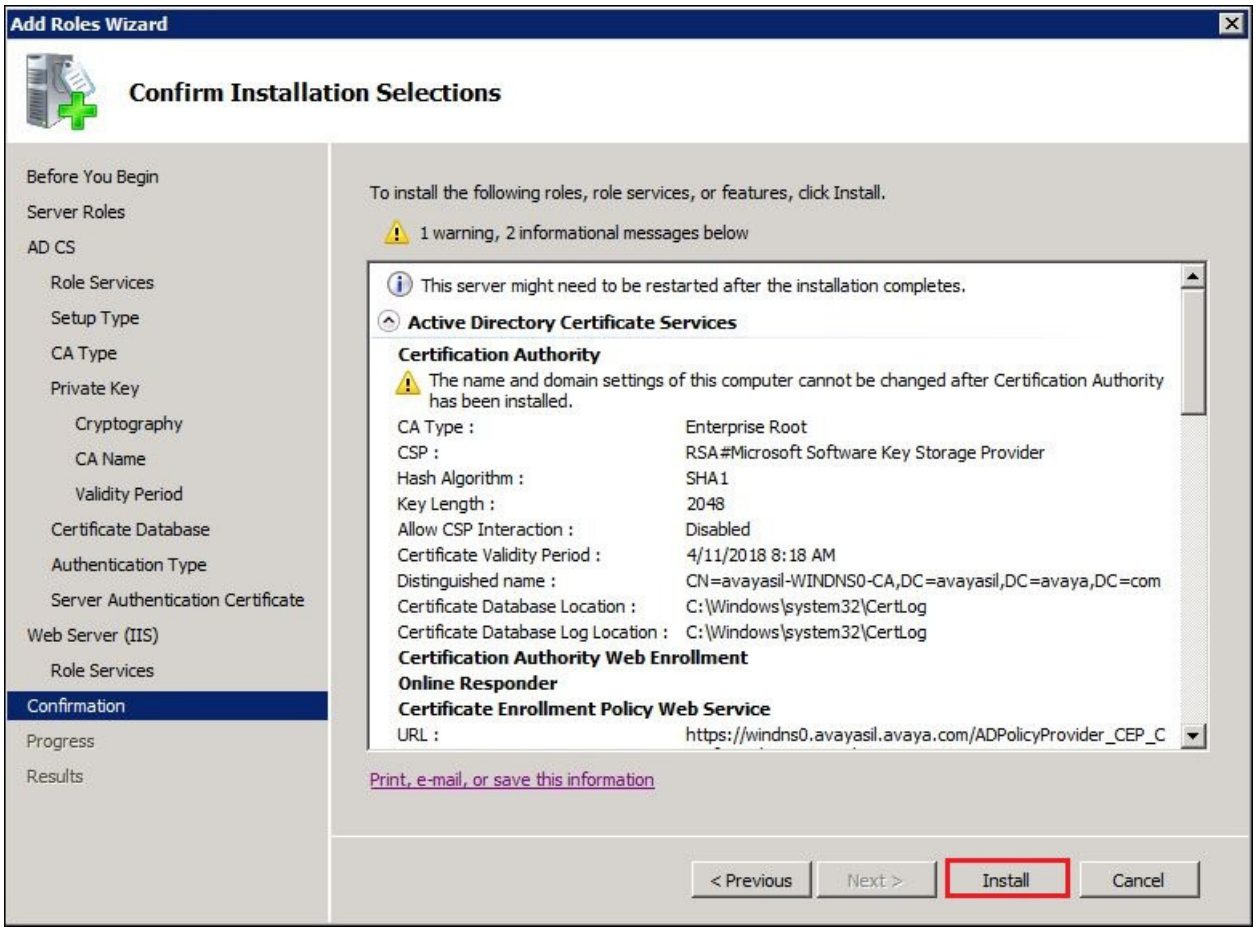
This screen is informational. Installation of Microsoft's web server, Internet Information Services or IIS, is required for the Microsoft Certificate Authority. Click on **Next**.



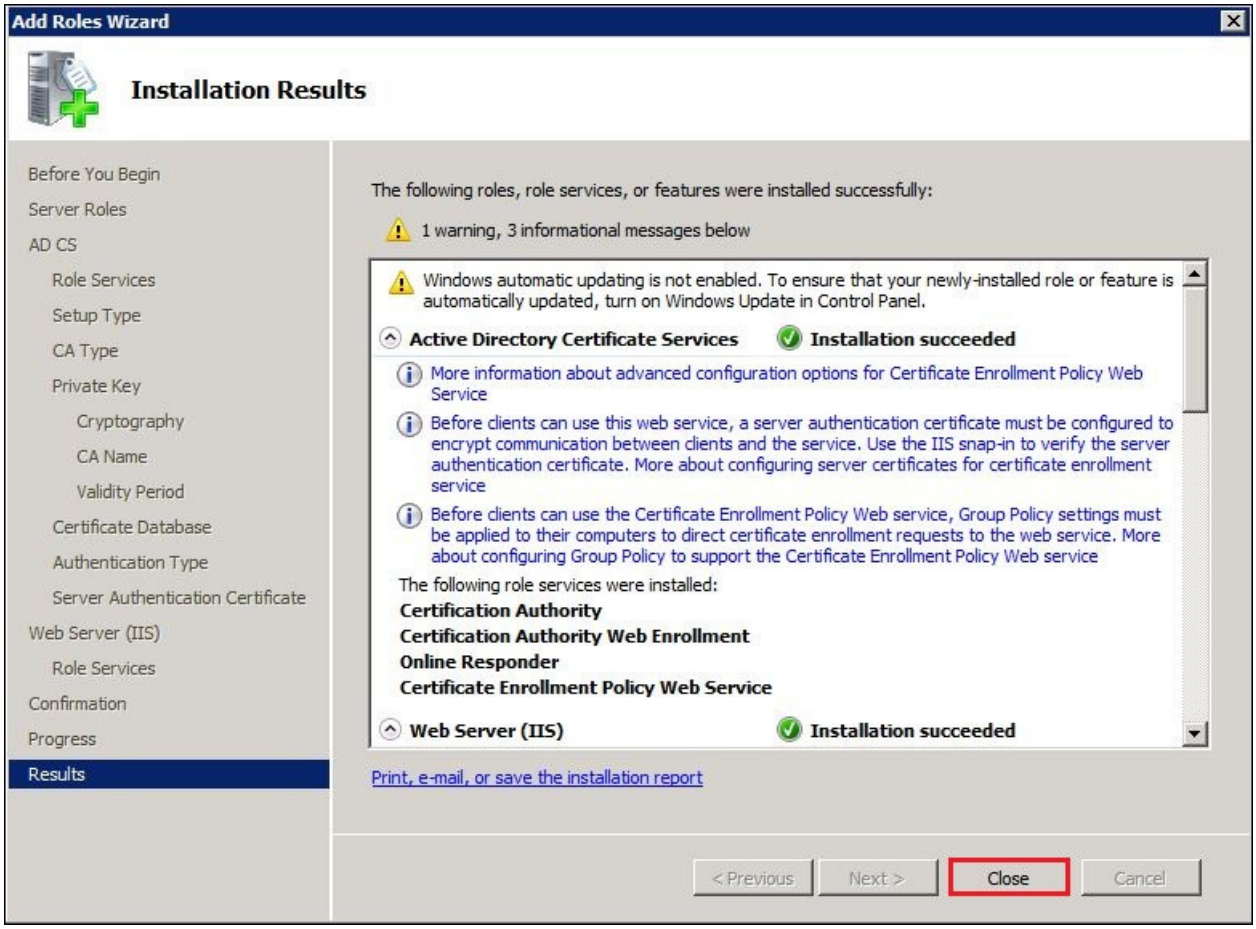
To accept the defaults, click on **Next**.



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**.



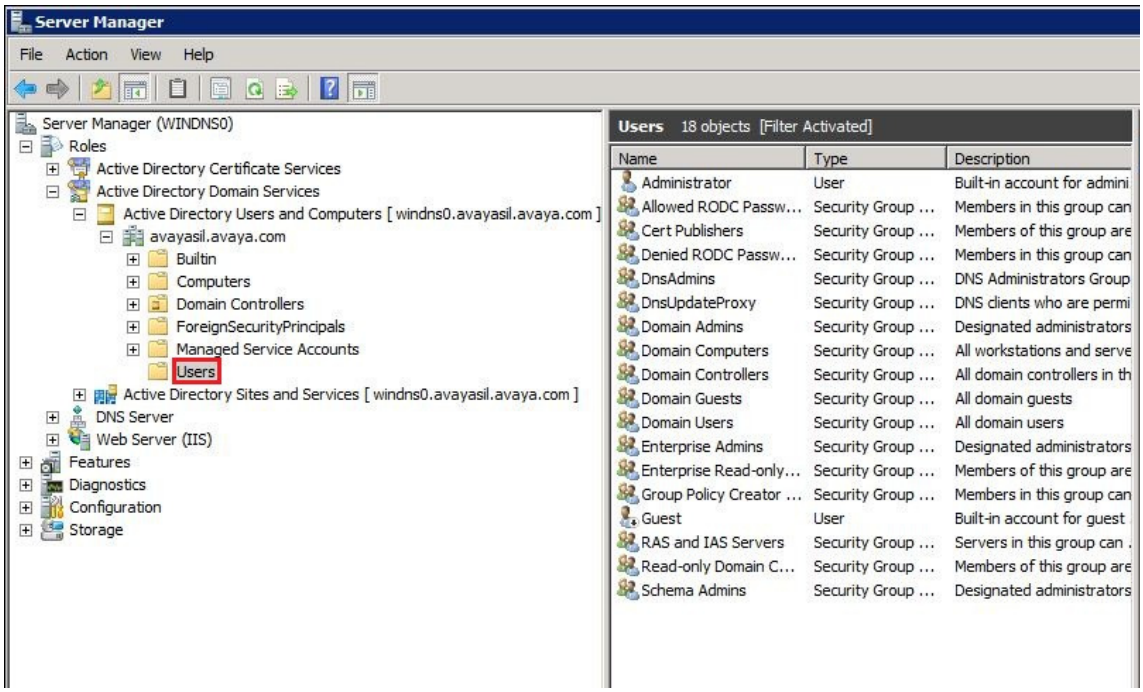
5.2. Install and Configure Network Device Enrollment Service

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.

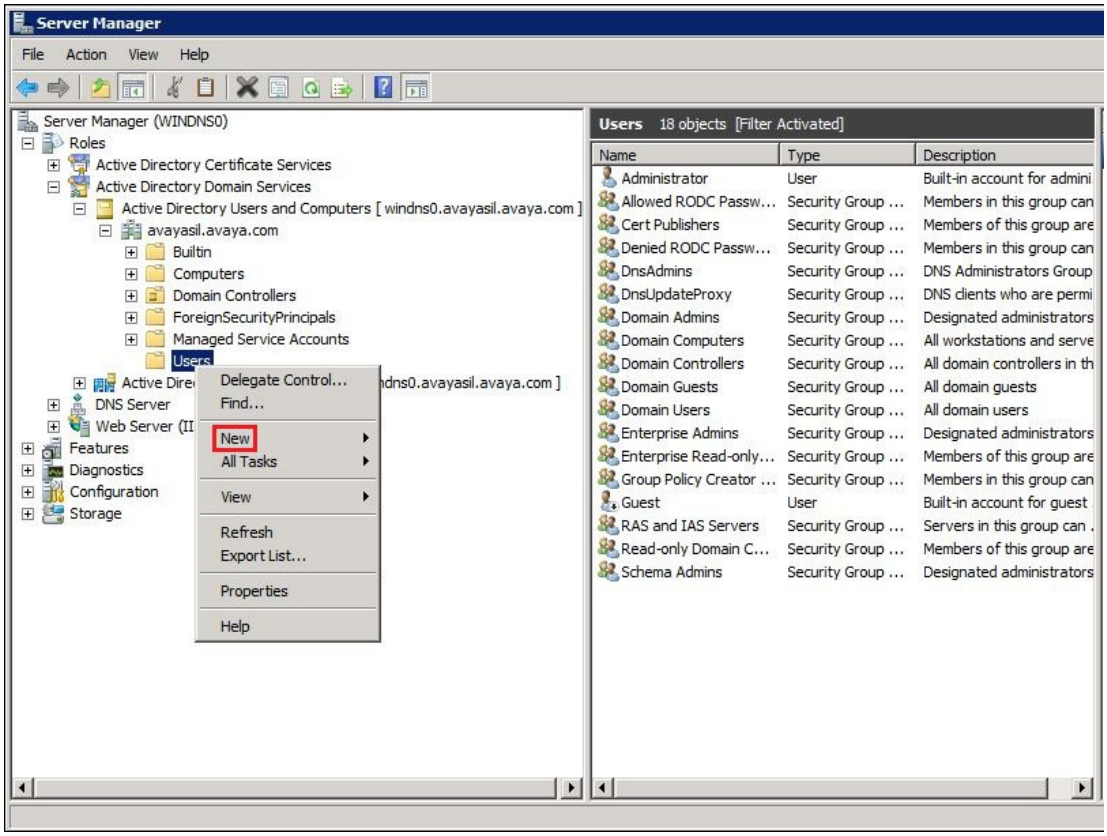
Step 1. Create Service Account User

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.

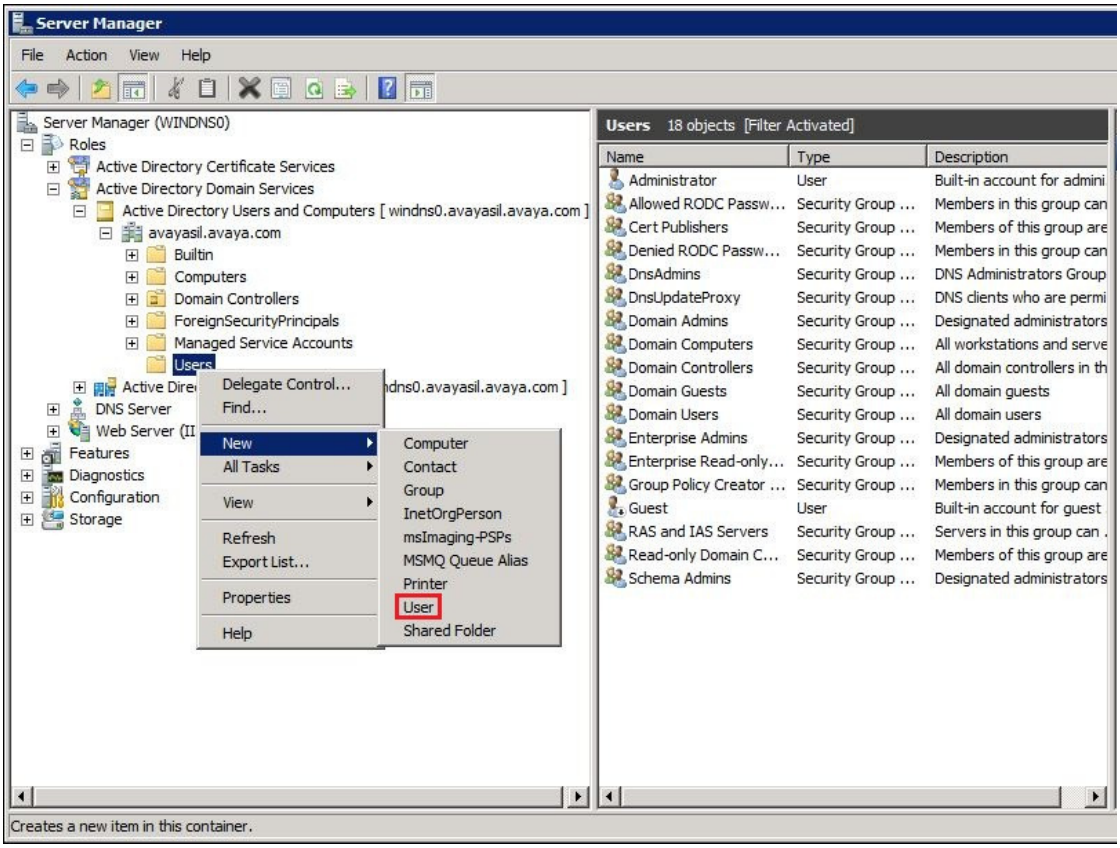
Go to **Server Manager → Roles → Active Directory Domain Services → Active Directory Users and Computers → avayasil.avaya.com (the domain) → Users**.



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



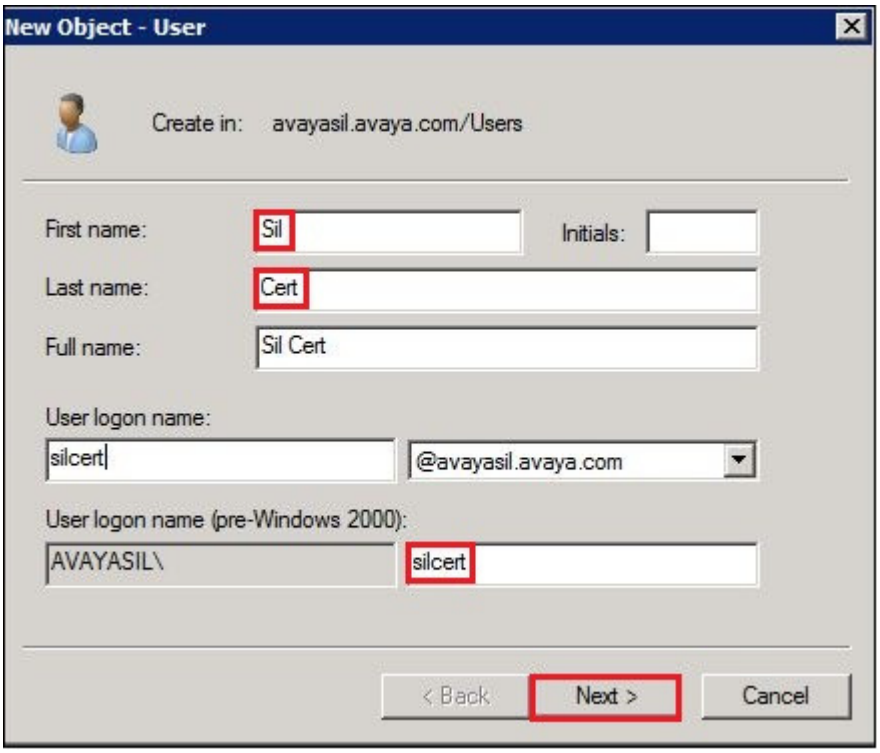
Select **User**. See below.



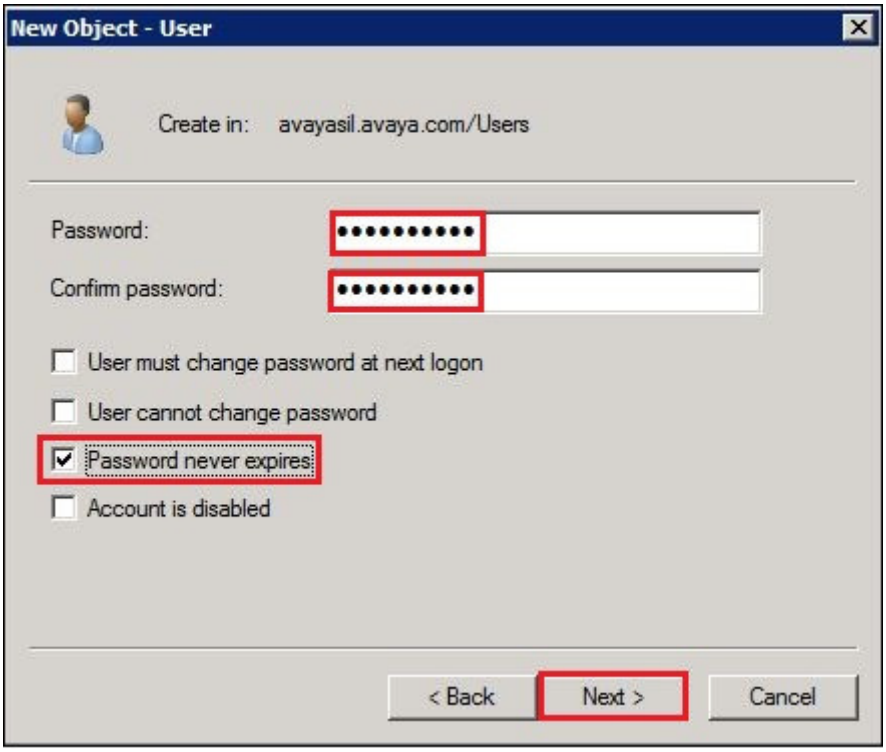
To create the new user:

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

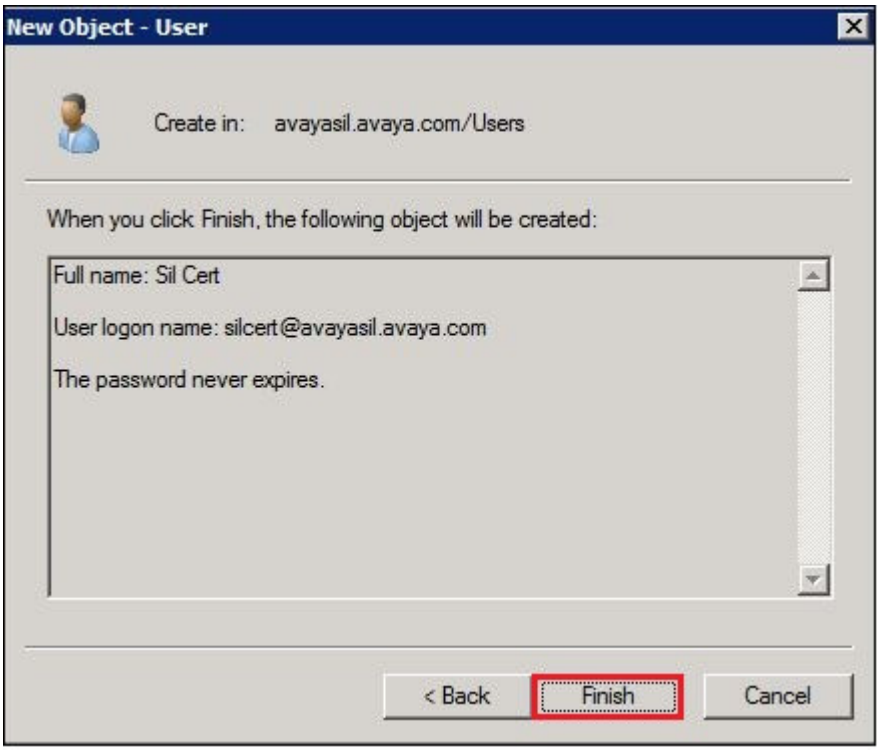
Click on **Next**.



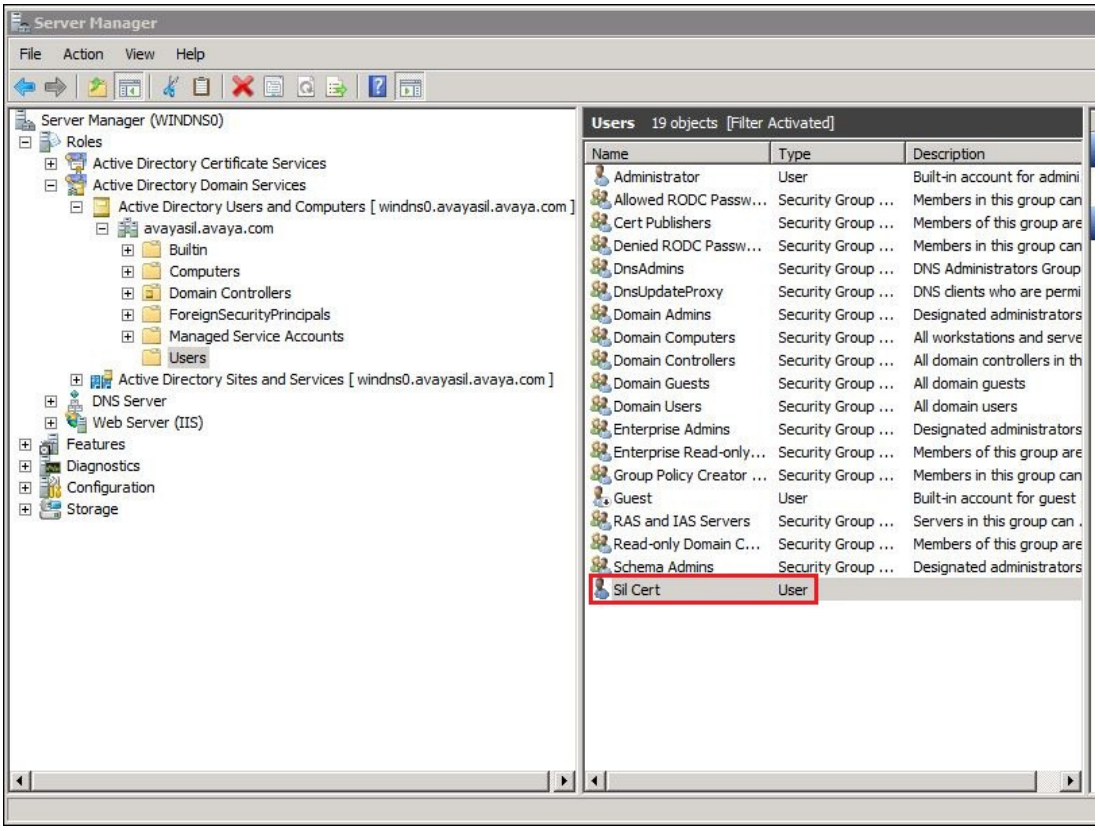
Input a suitable password and check **Password never expires**. Click on **Next**.



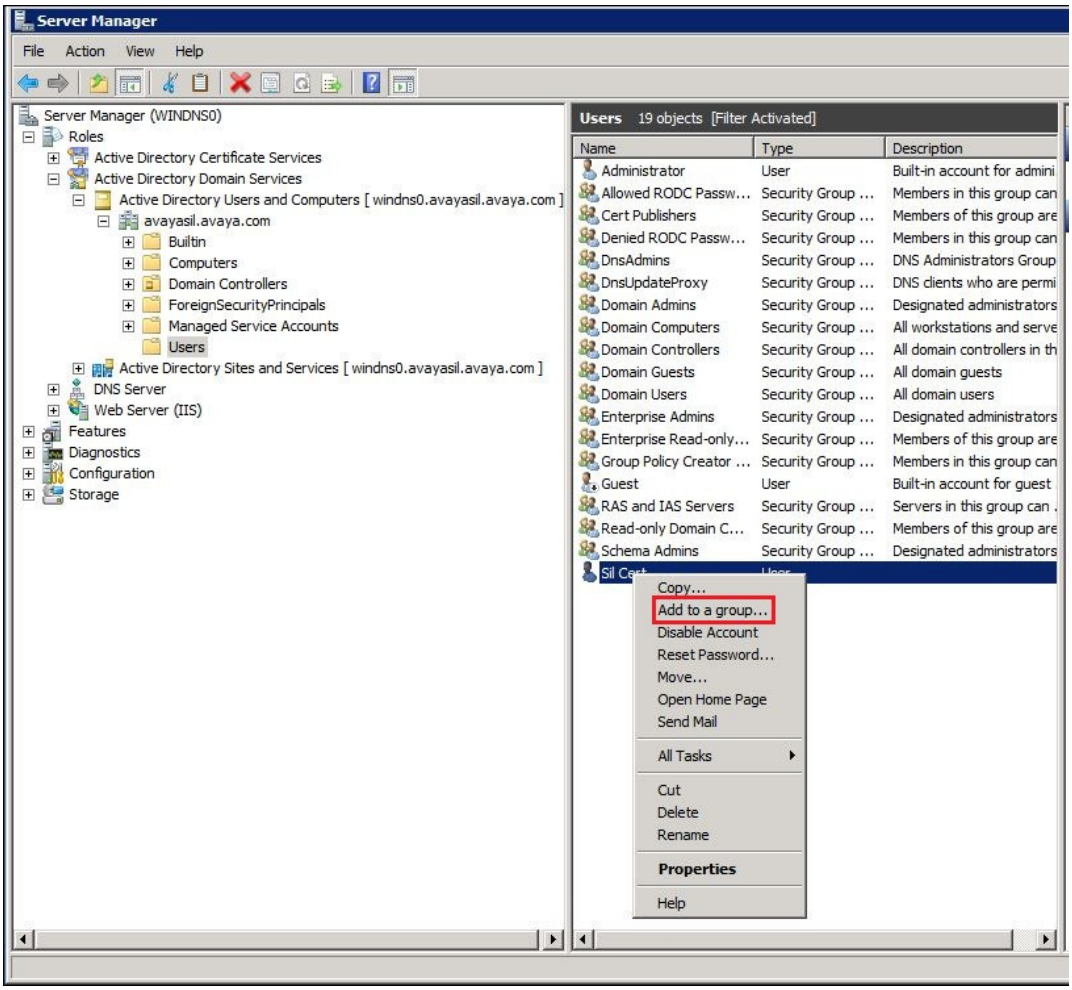
Verify user information and click on **Finish** to create the user.



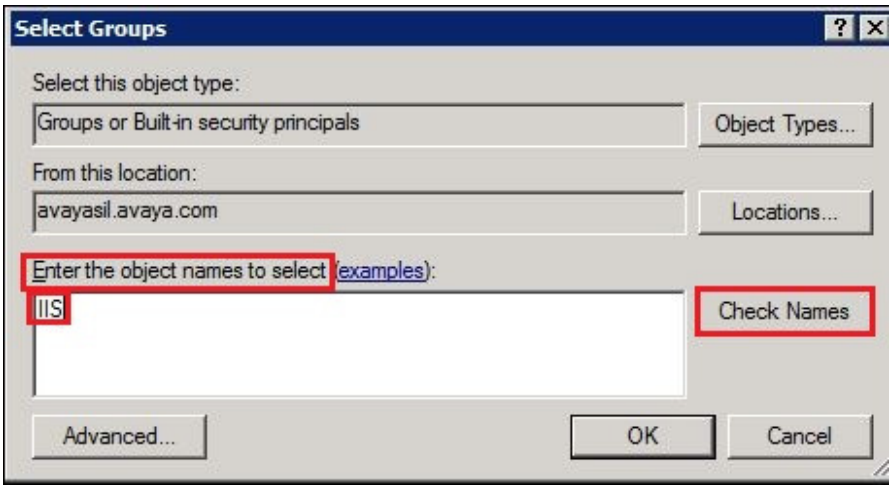
The new user that was created is displayed in the Users window. See below.



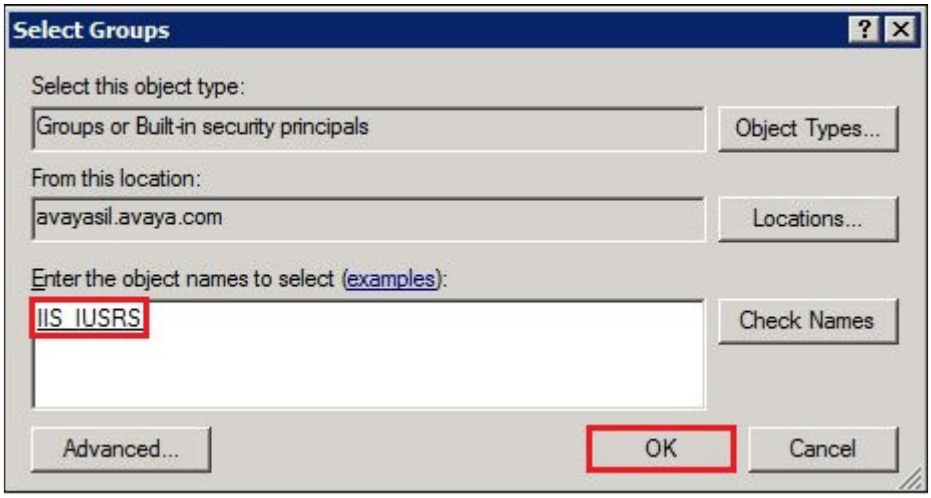
The user that was just created must be a member of the IIS group. To add this user to the IIS group, right click on the user and select **Add to a group**.



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



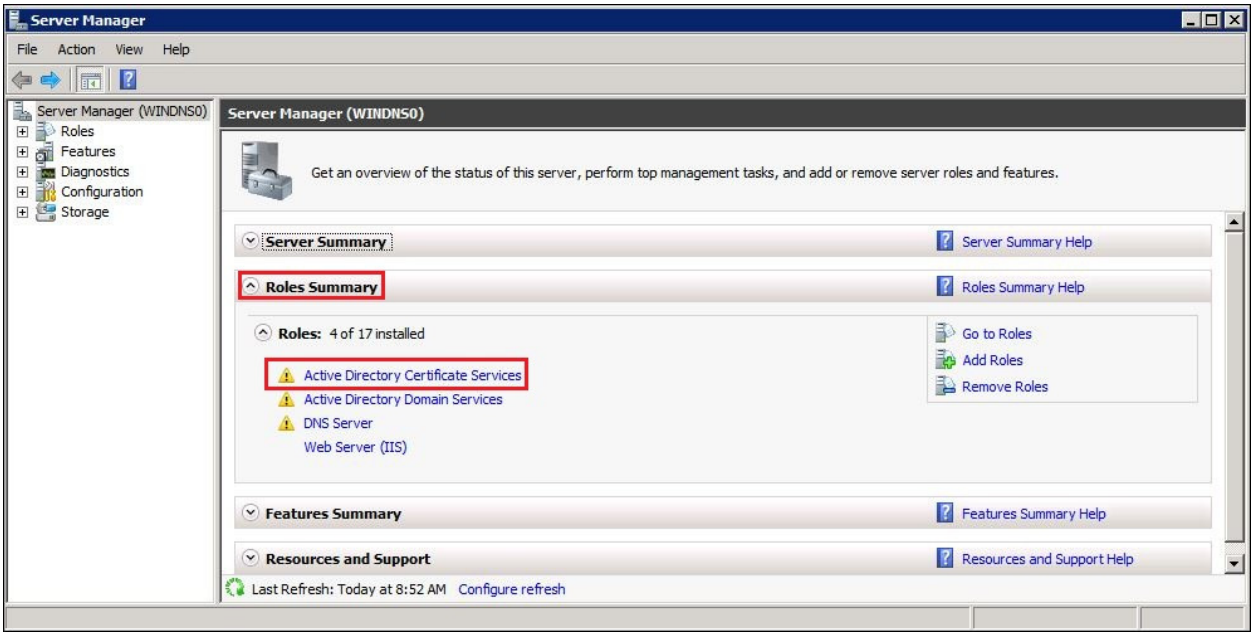
The group **IIS_IUSRS** will be displayed. Click on **OK**.



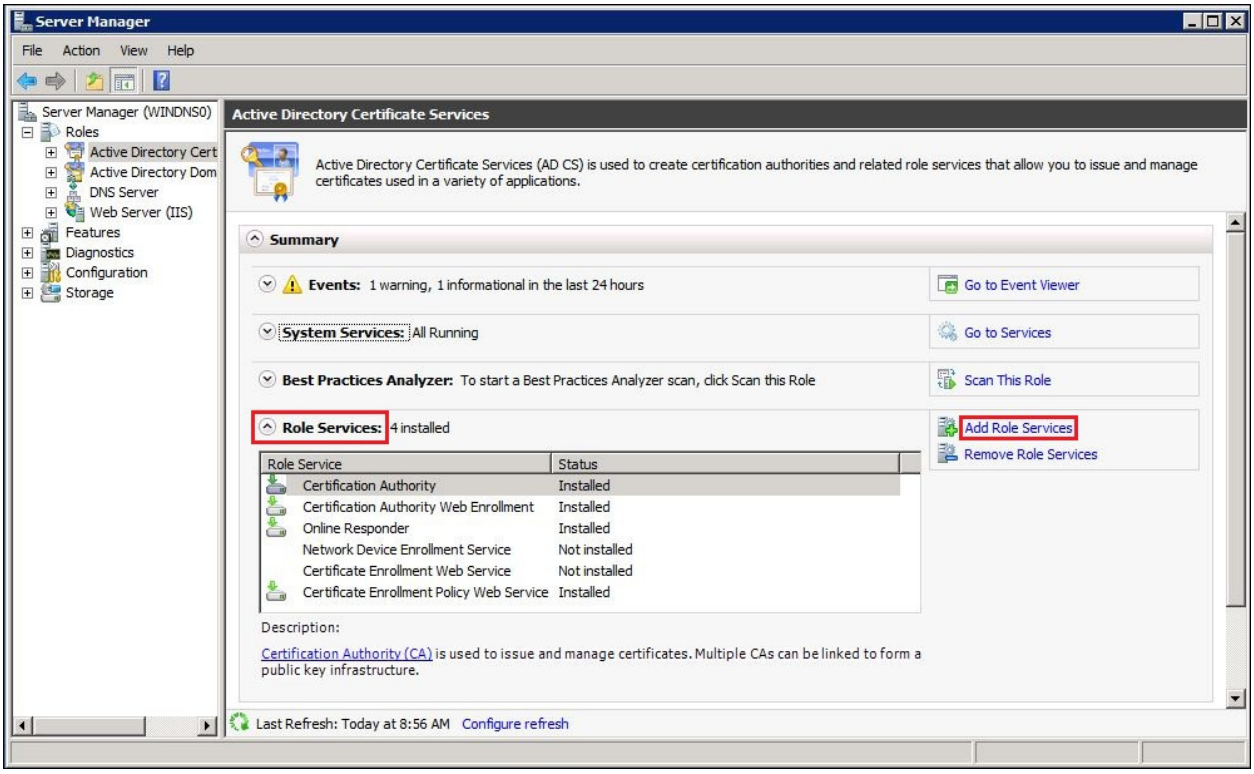
The user has been added to the IIS group. Click on **OK** to exit.

Step 2. Install Network Device Enrollment Service

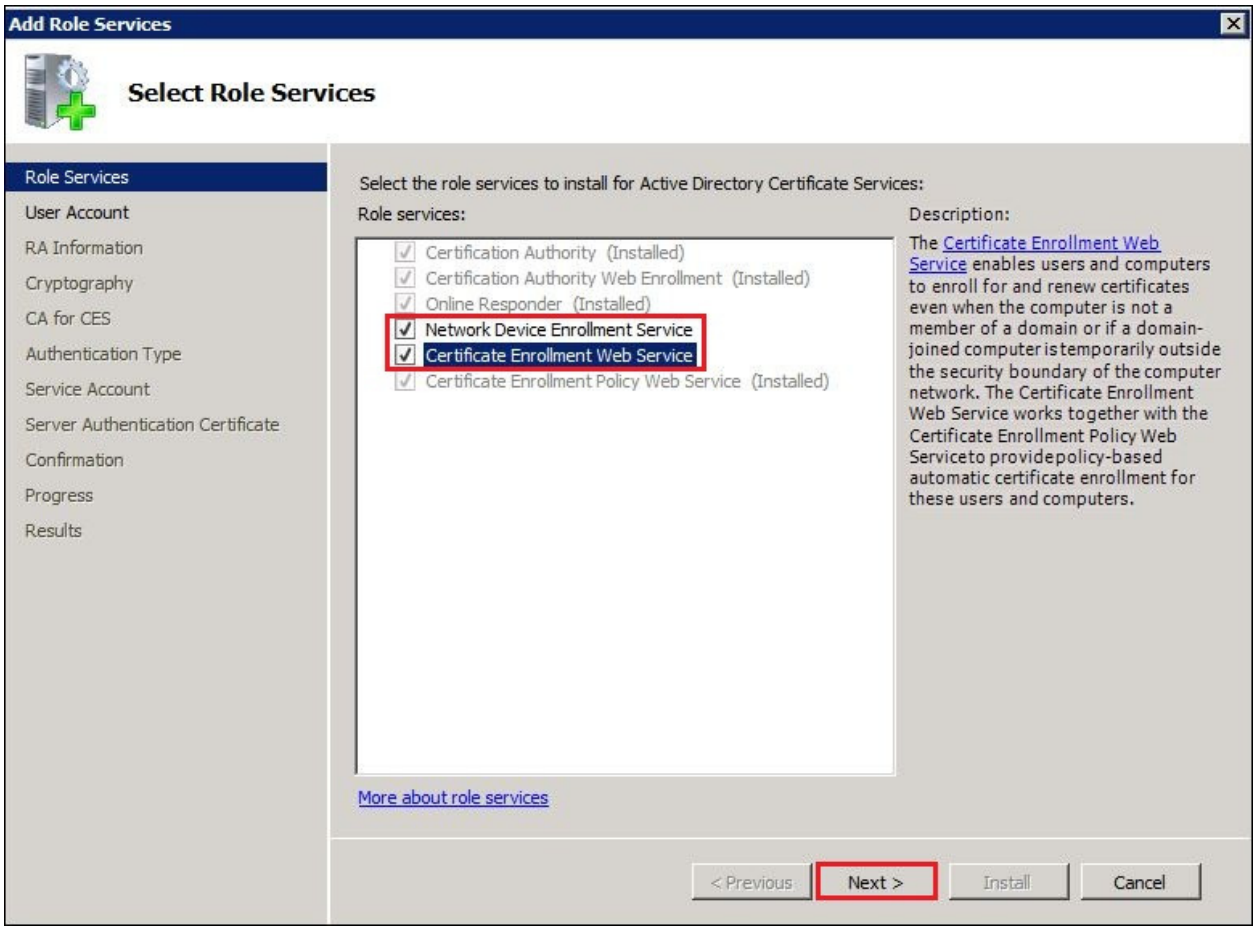
To install the Network Device Enrollment Service scroll down to **Roles Summary** and Select **Active Directory Certificate Services.**



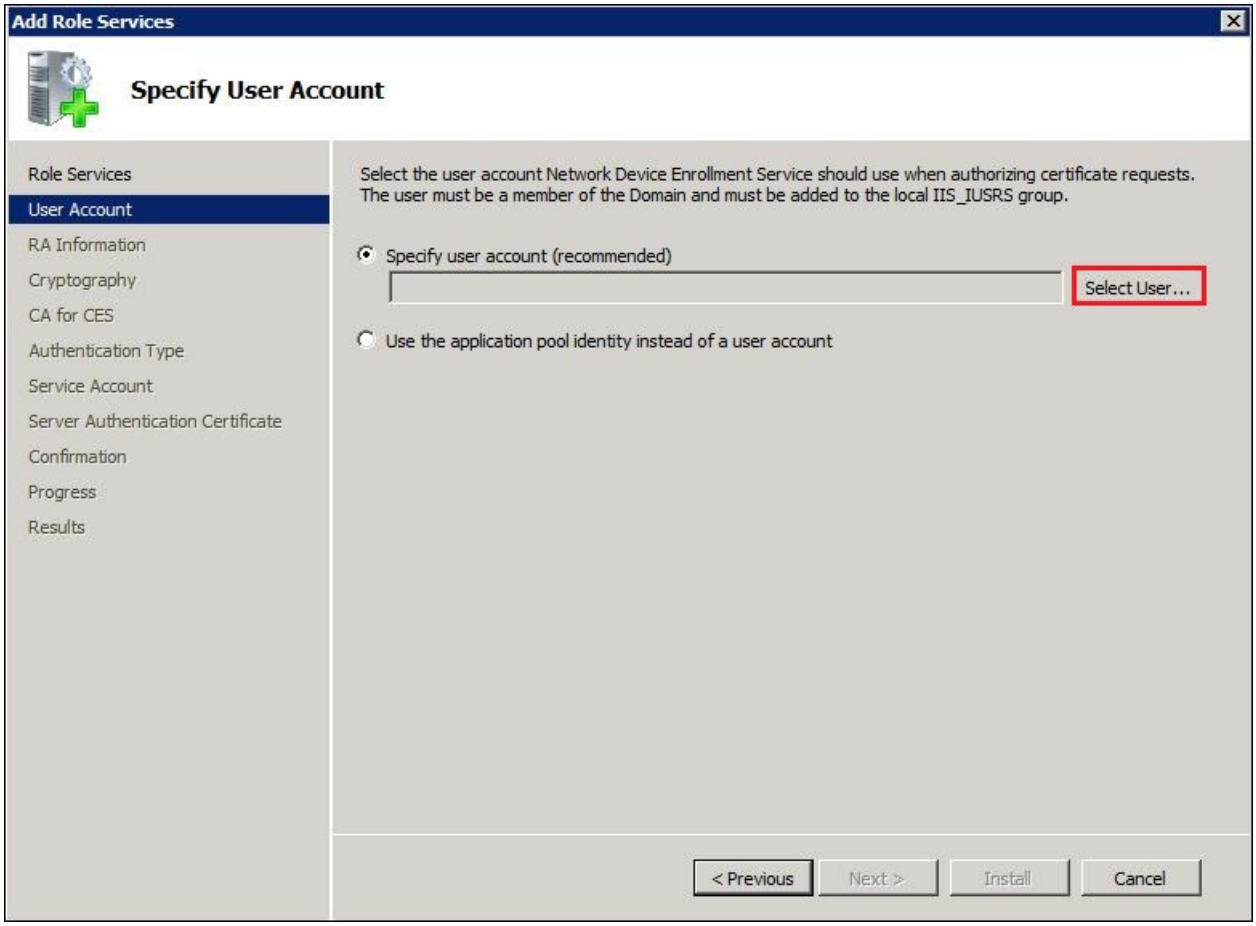
Scroll down to the **Role Services** heading and Select **Add Role Services**.



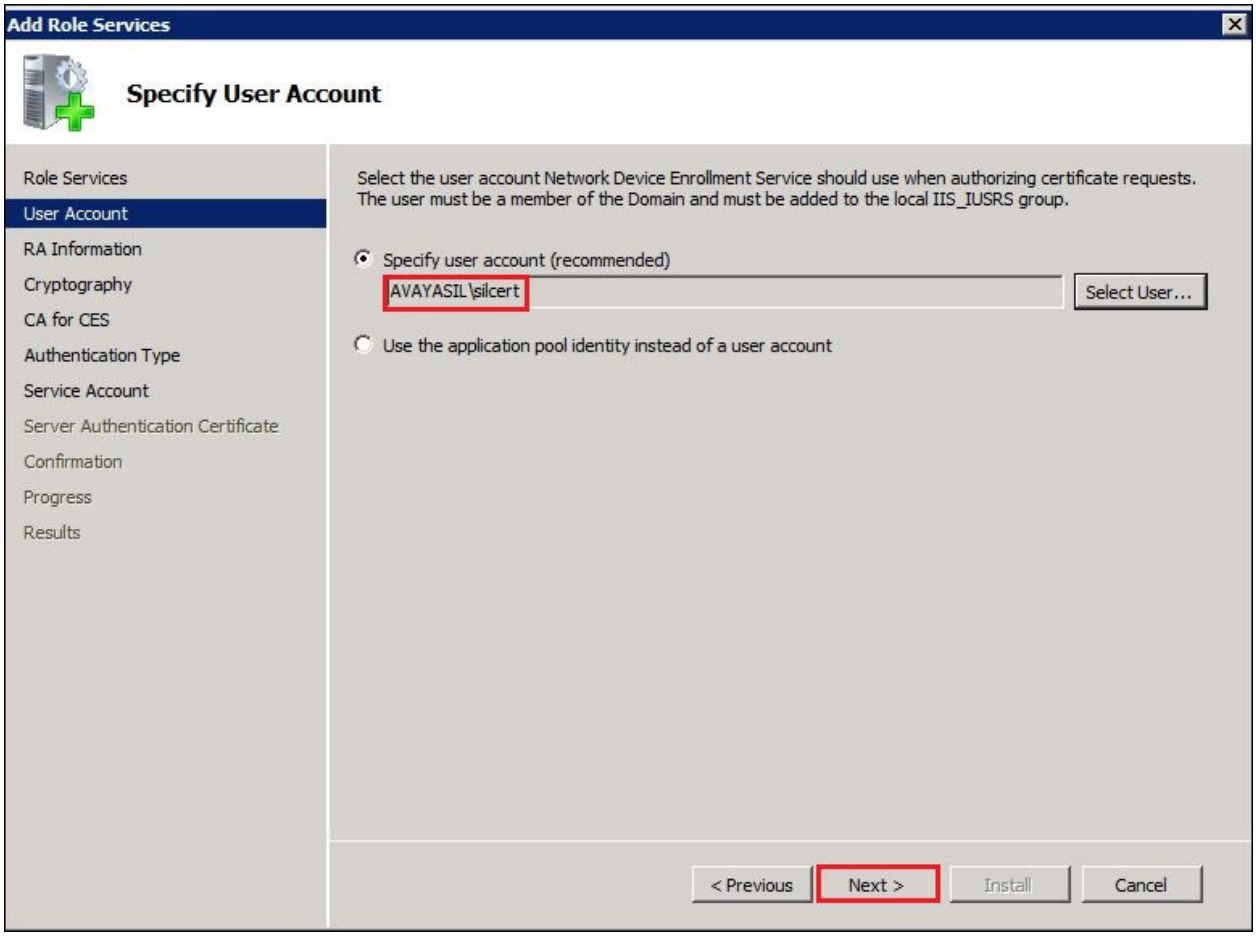
Check **Network Device Enrollment Service** and **Certificate Enrollment Web Service** and click on **Next.**



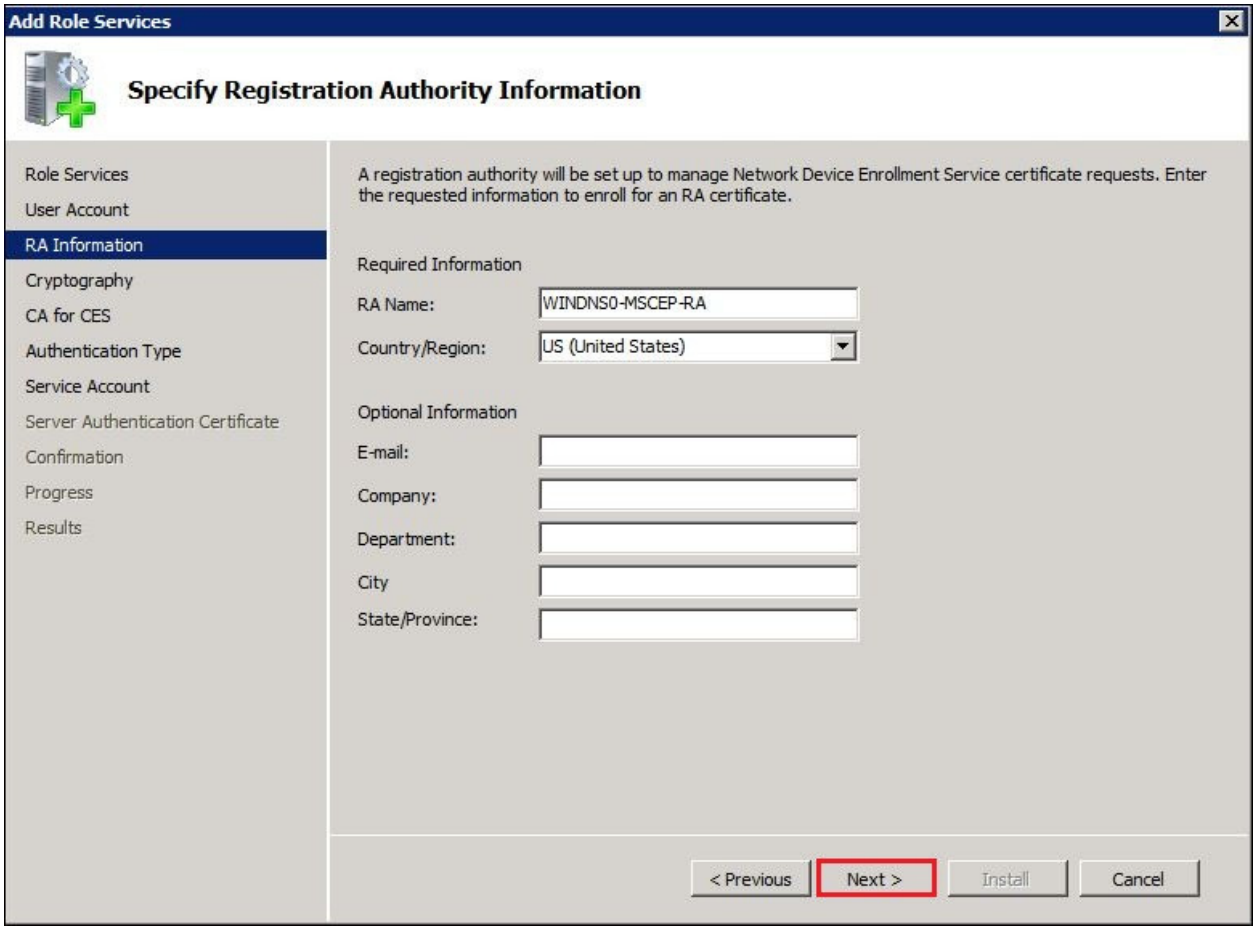
Click on **Select User**.



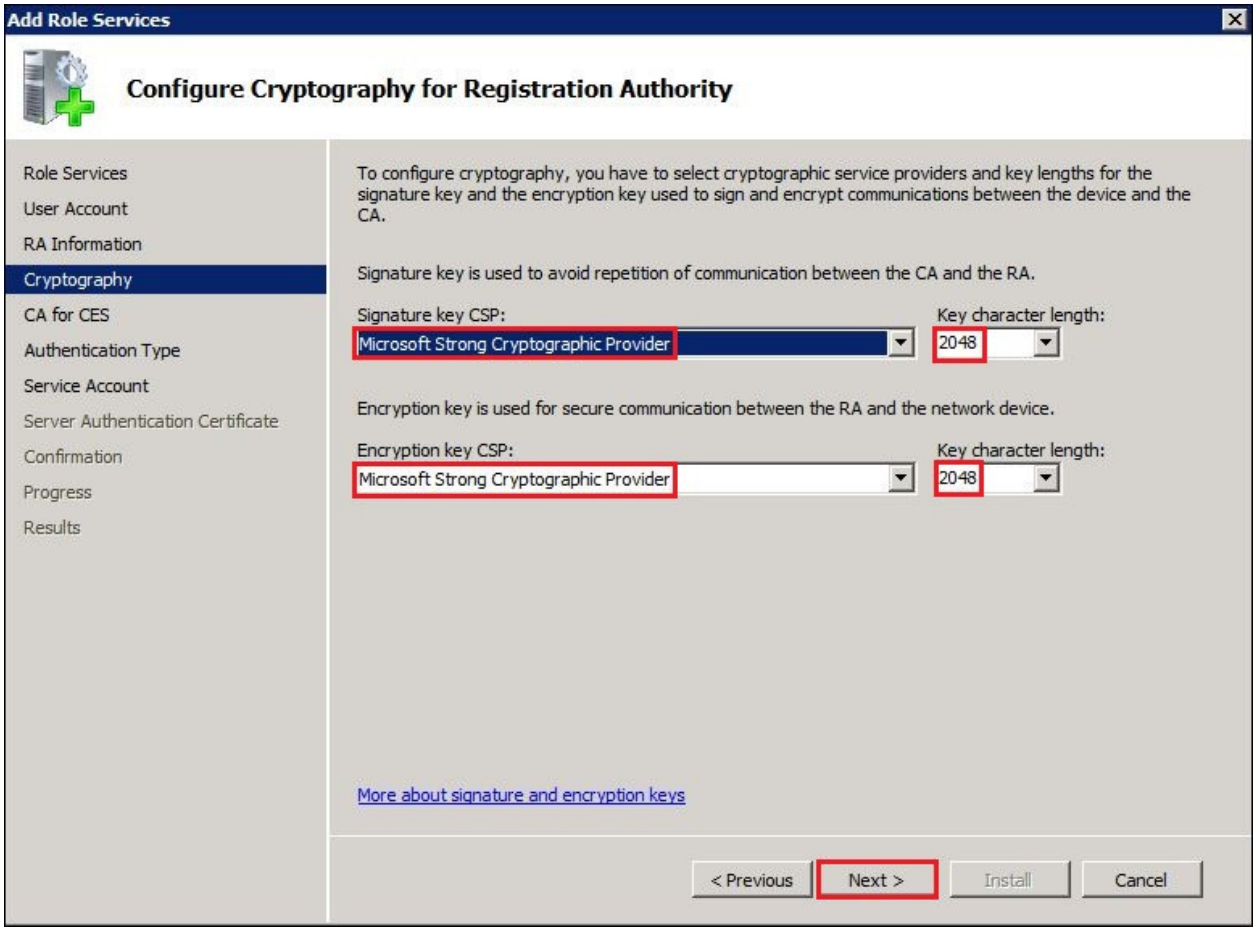
Select the user created in **Section 5.2 Step 1**. Click **Next**.



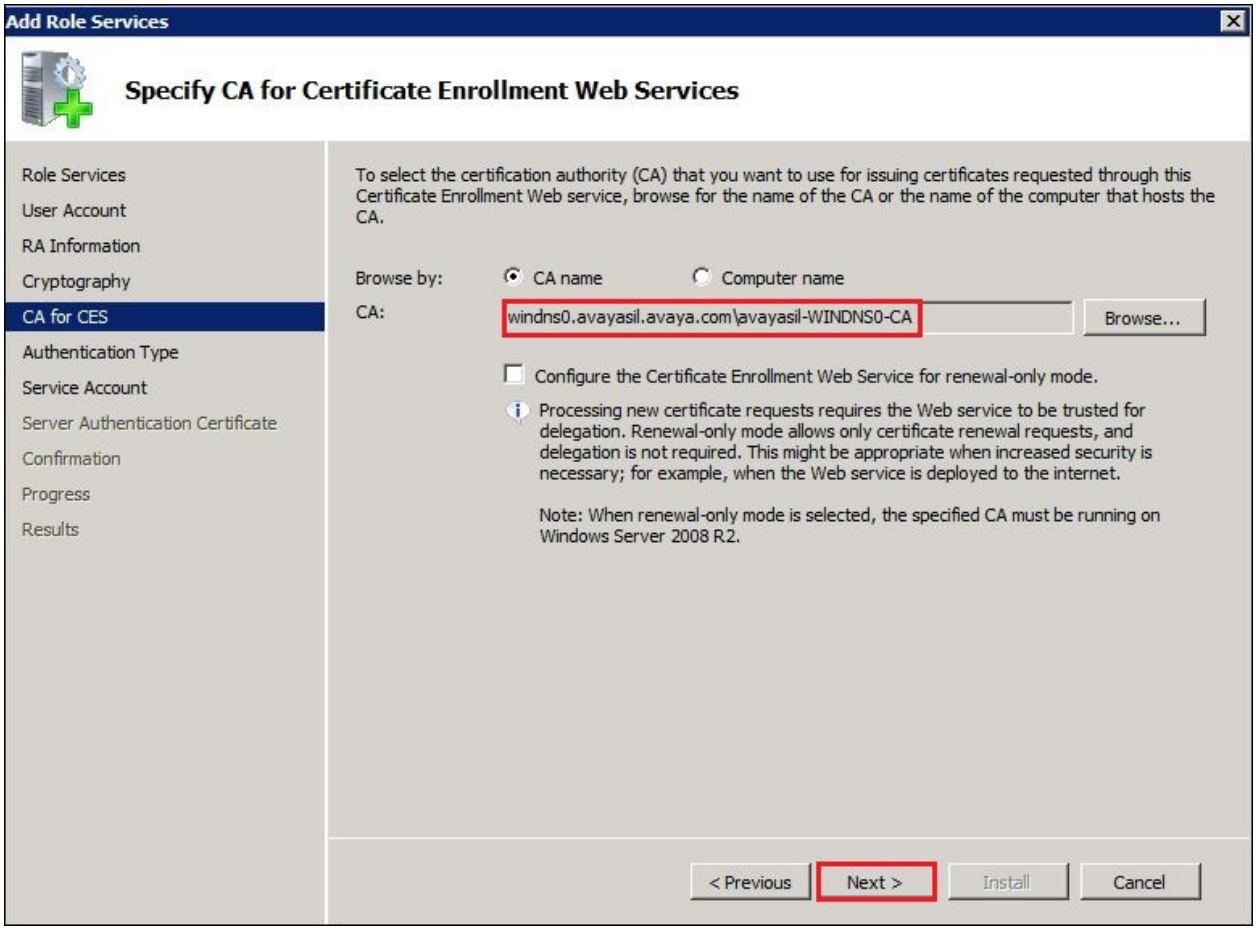
For **Specify Registration Authority Information**, accept the defaults by Clicking on **Next**.



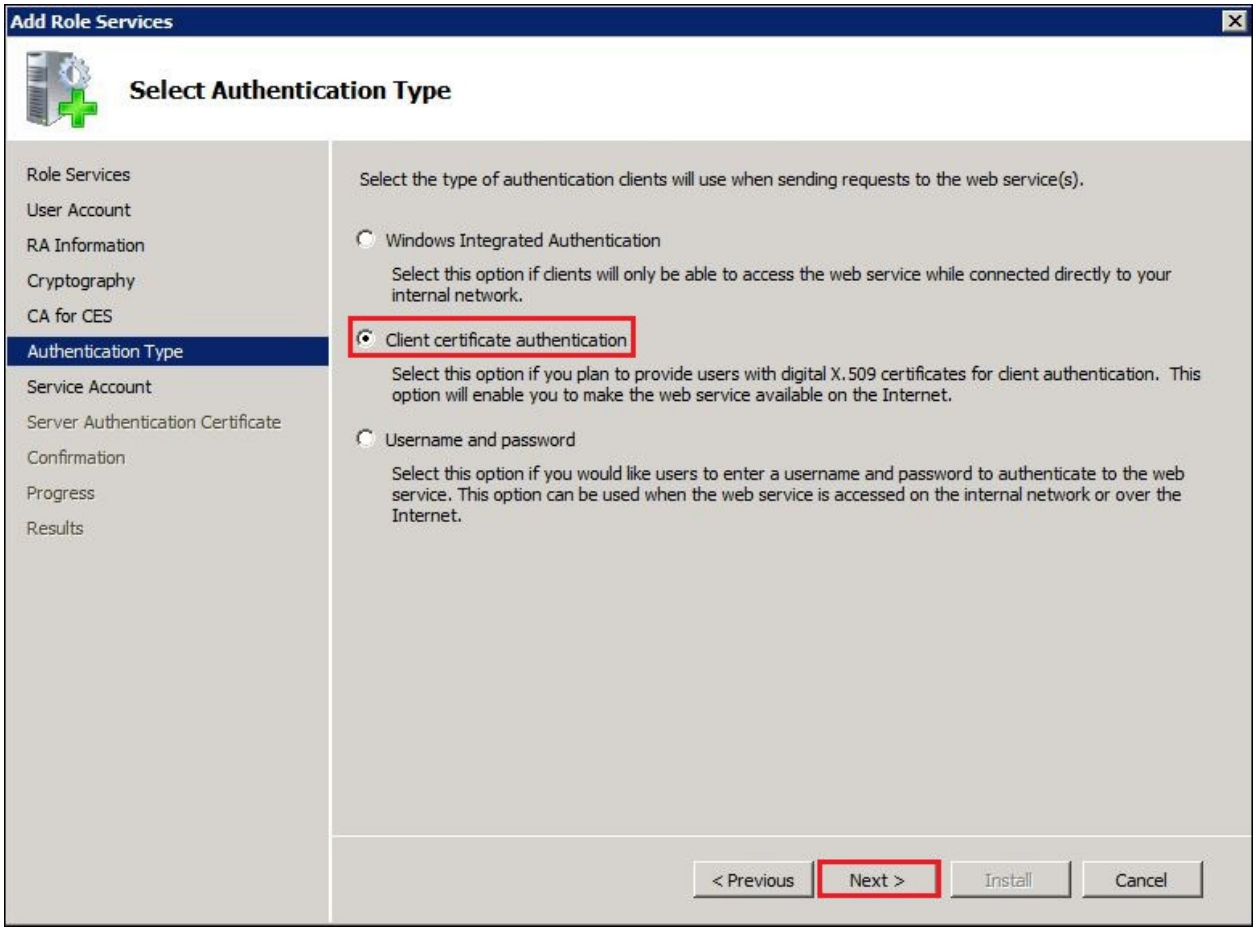
For **Signature key CSP** and **Encryption key CSP**, Verify **Microsoft Strong Cryptographic Provider** is selected and **Key character length:** is set to **2048**. These are the defaults. Click on **Next**.



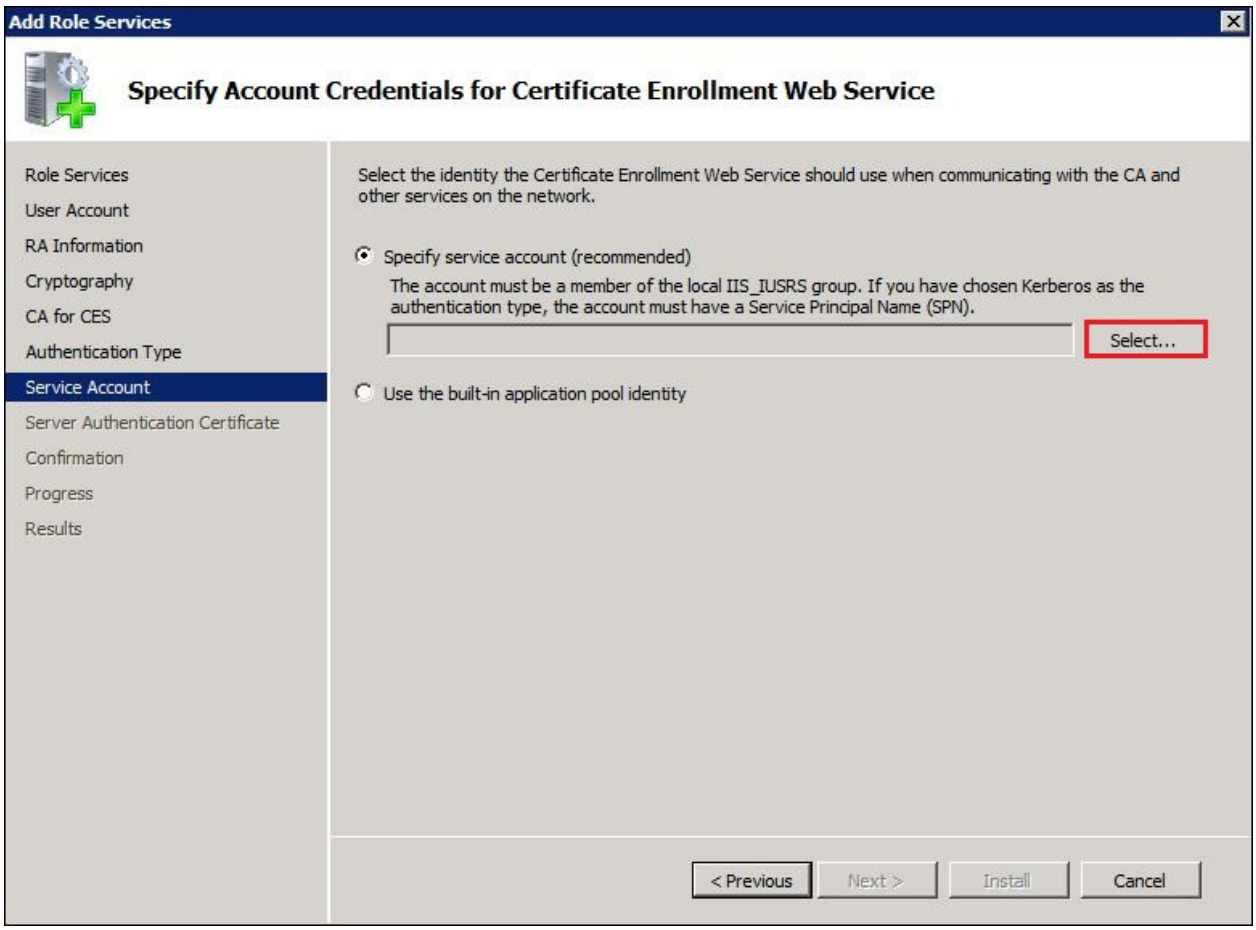
Select the CA created in **Section 5.1**. Click on **Next**.



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

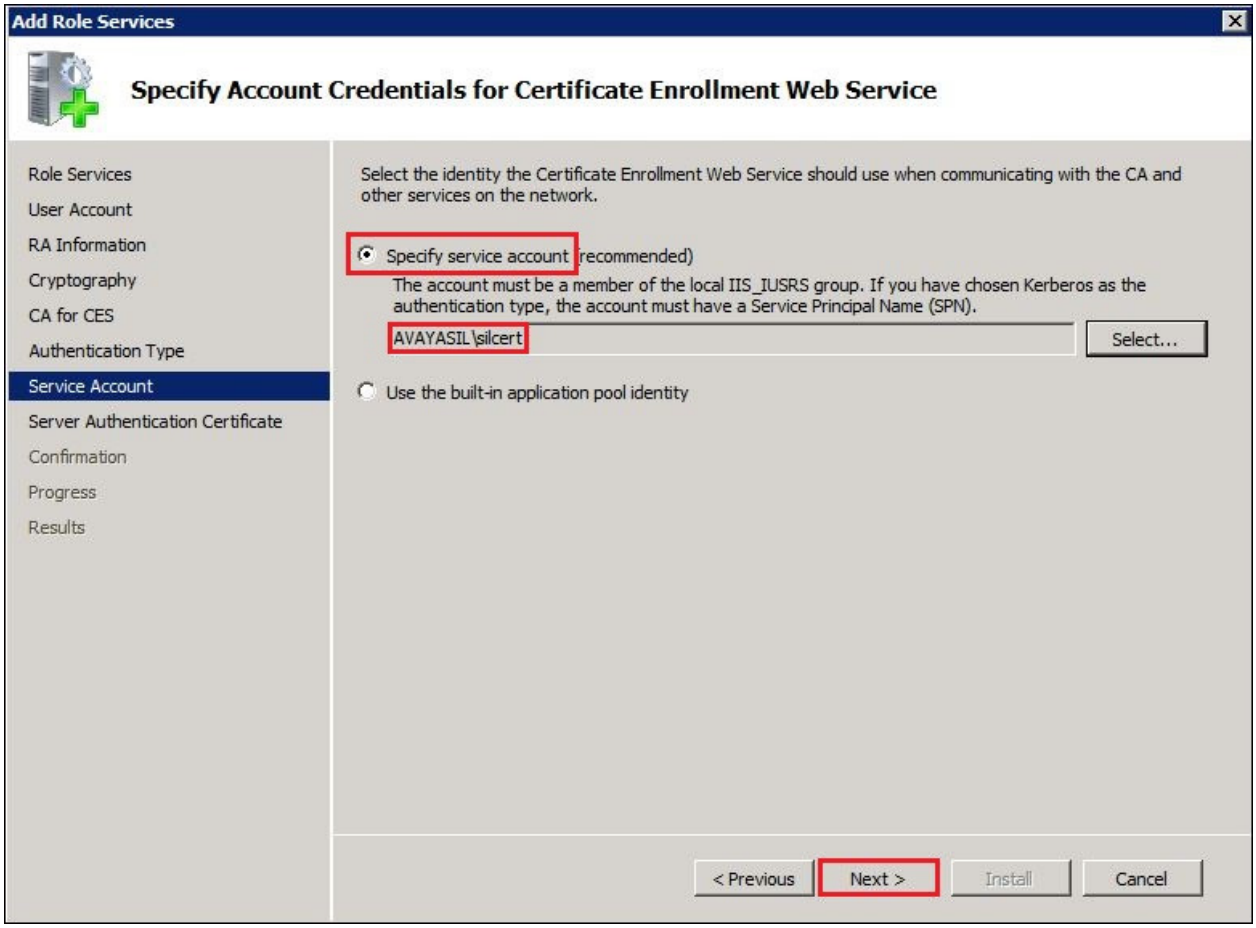


Select the user created in **Section 5.2 Step 1**. Click on **Next**.

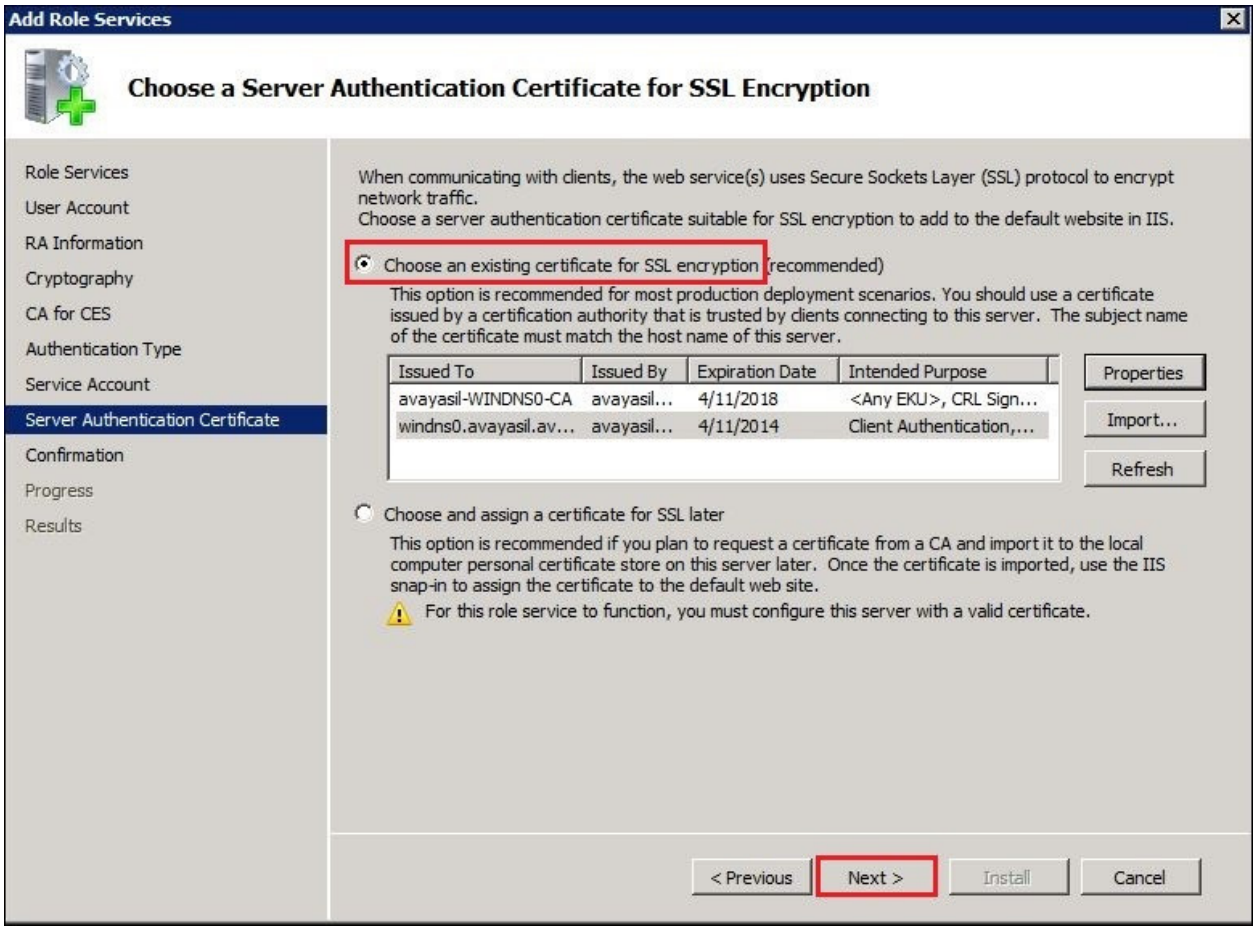


To select the account displayed, click on **OK**.

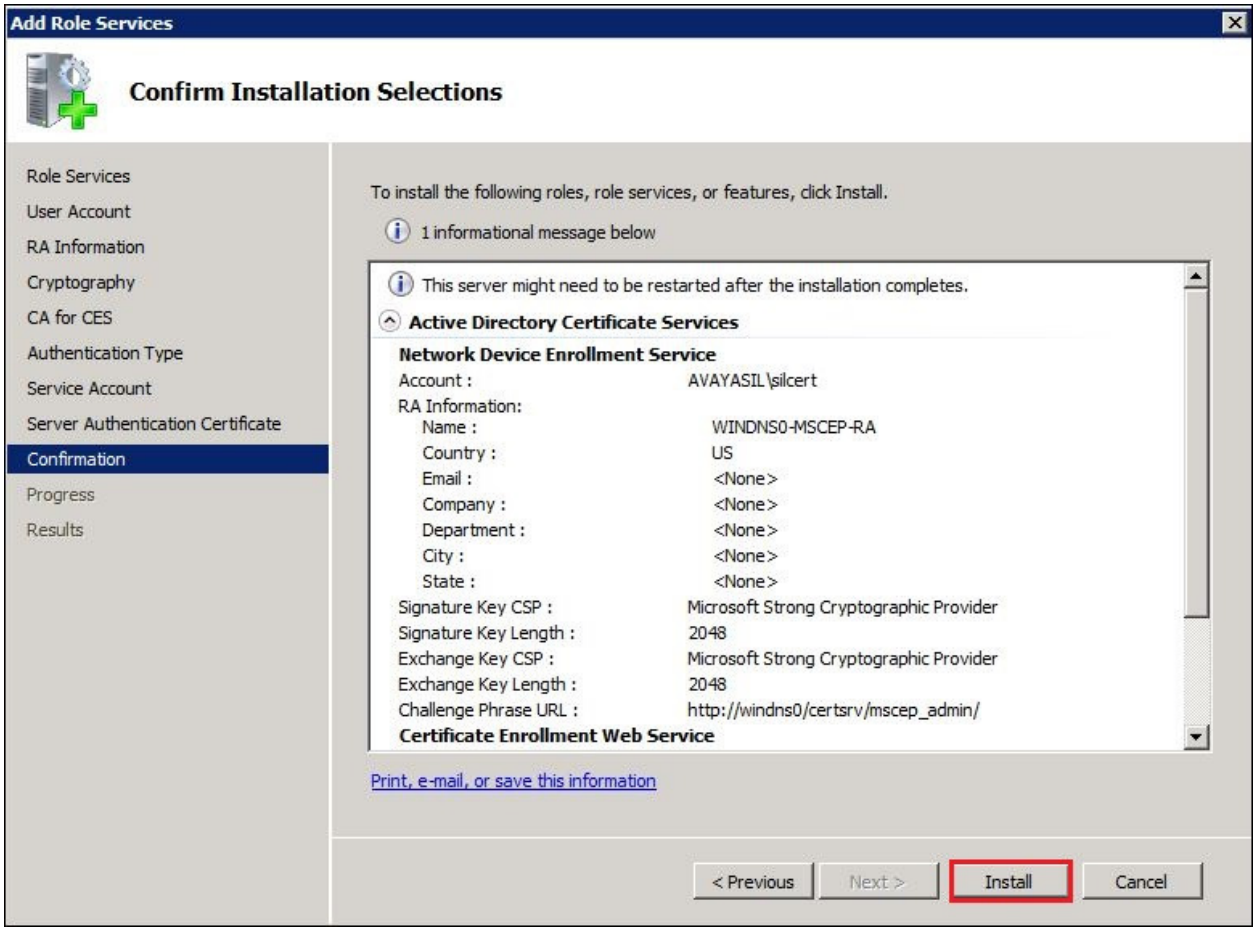
The service account that was just selected will be displayed. Click on **Next**.



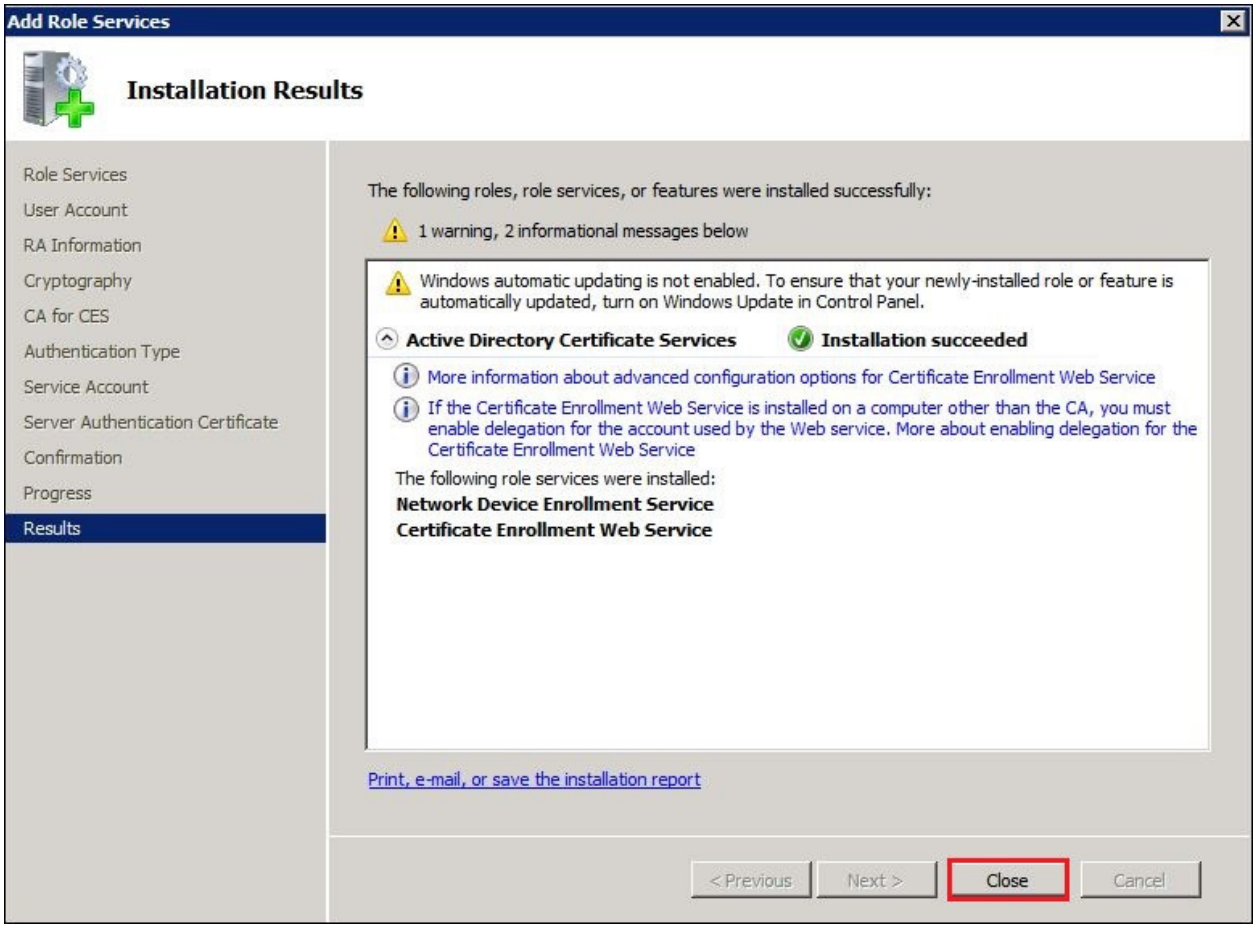
The Microsoft Certificate Authority is already installed so select **Choose an existing certificate for SSL encryption**. Click on **Next**.



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



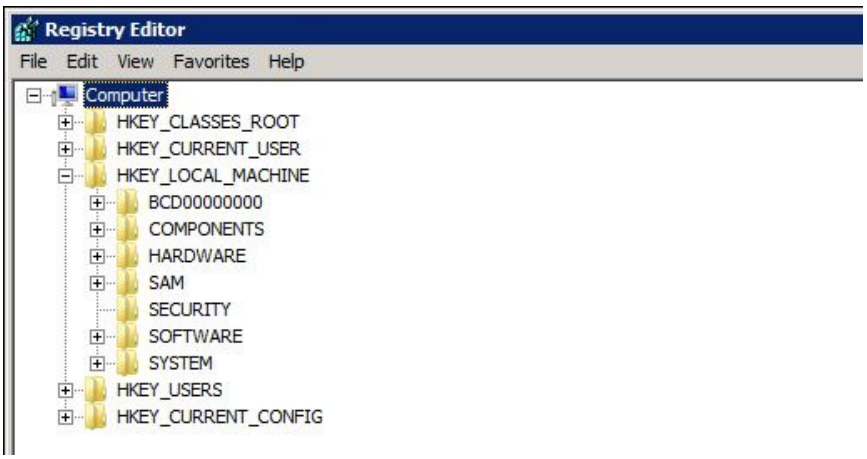
After installation completes, the Installation Results screen will be displayed. Click on **Close**.



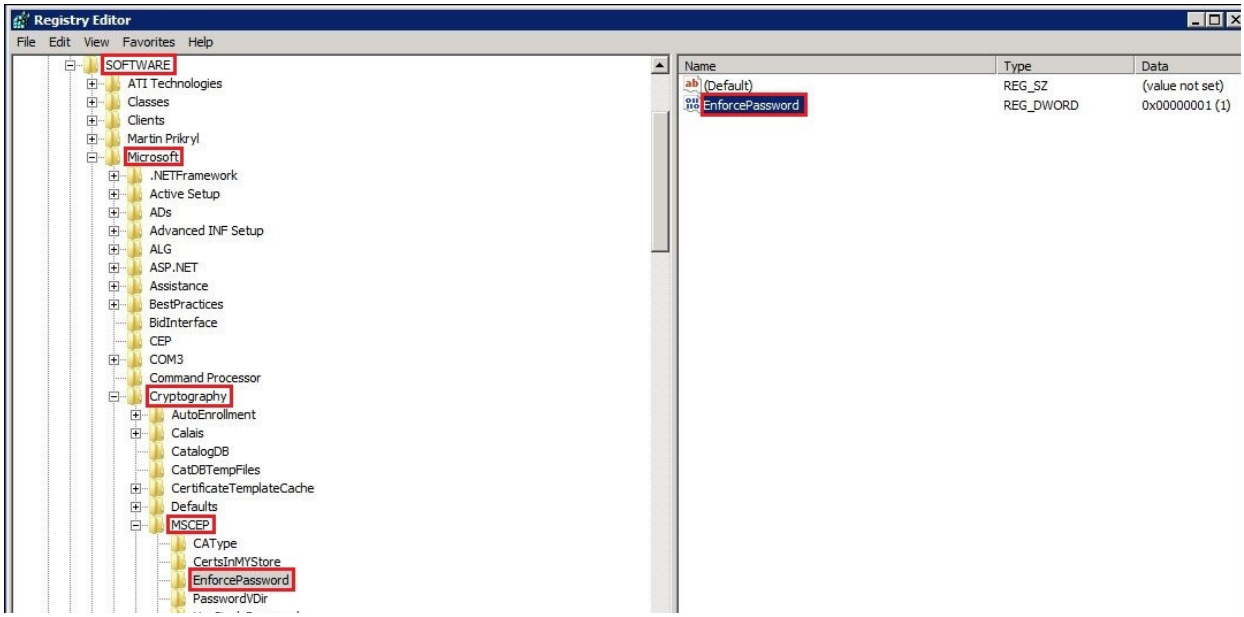
5.3. Disable SCEP Password

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

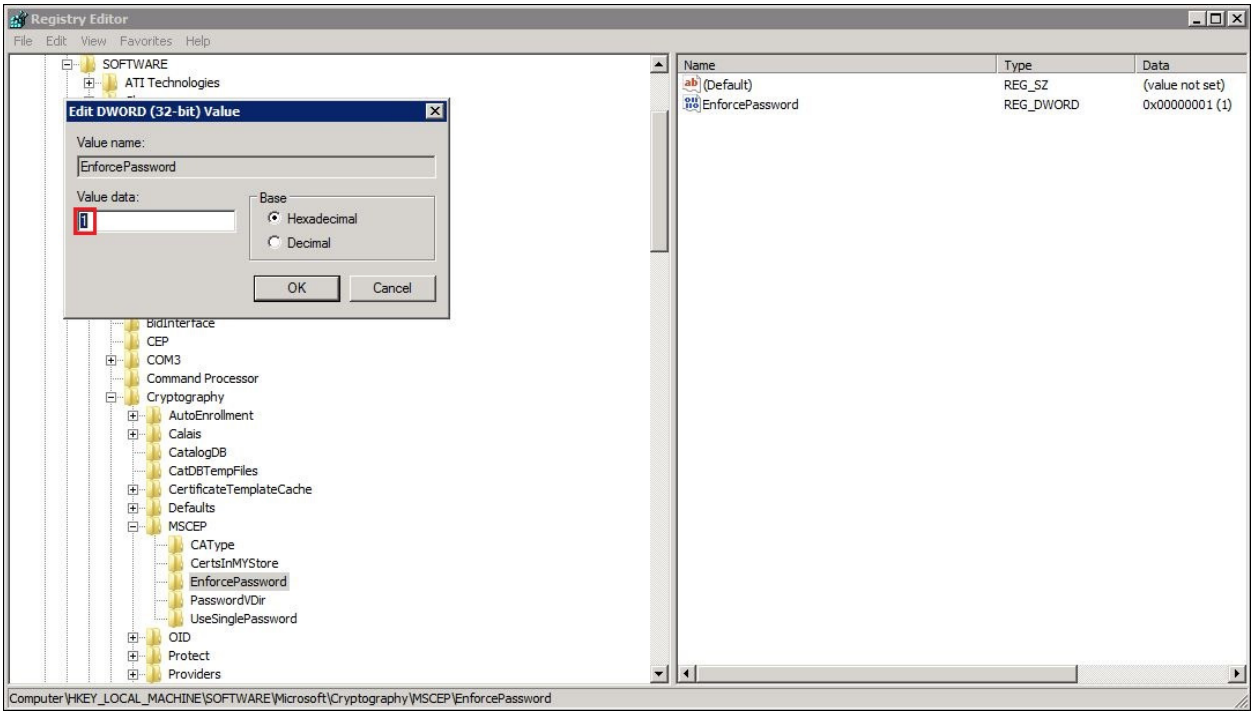
Login remotely to the Windows Server 2008. Go to **Start** (not shown). In the Search programs and files line**,** type in **regedit** and press **Enter** (not shown). The regedit program will execute and display the following screen.



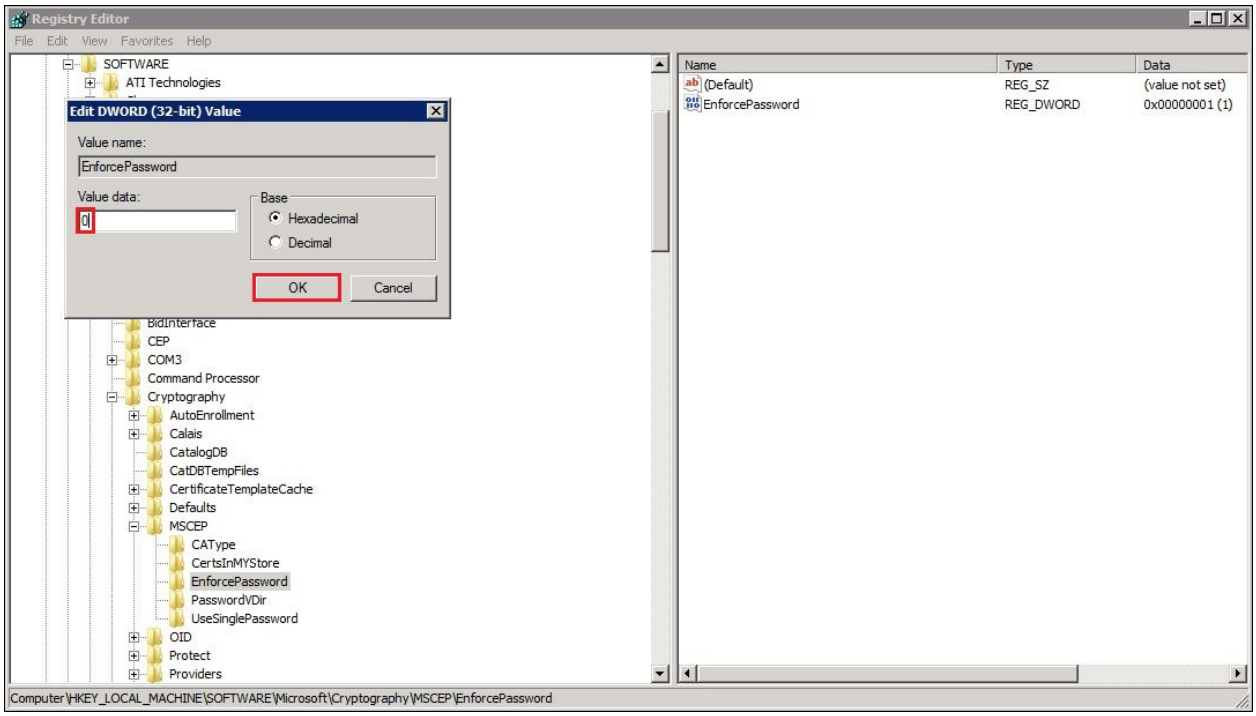
Go to **Computer → HKEY_LOCAL_MACHINE → SOFTWARE → Microsoft → Cryptography → MSCEP** and select **EnforcePassword**. See below.



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



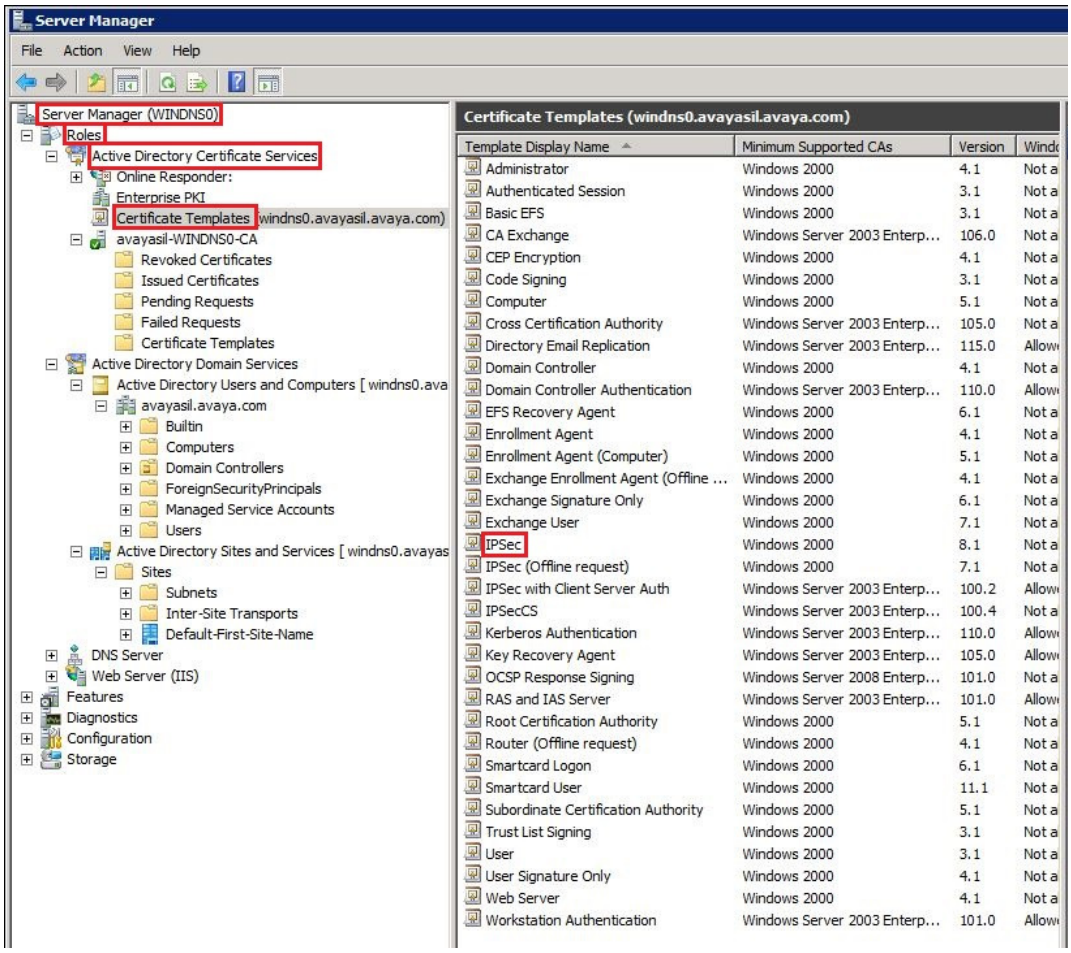
Update **Value data:** to **0** to disable password enforcement and select **OK**. See below.



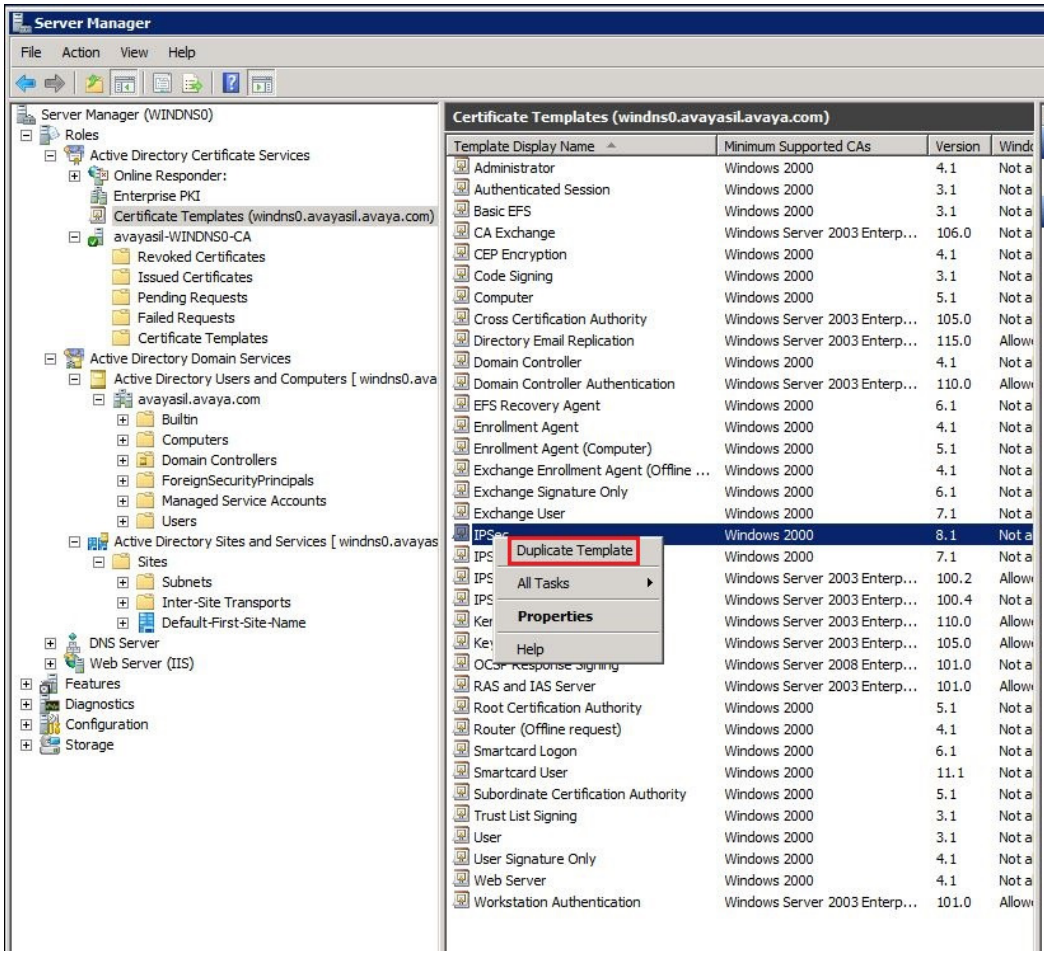
Important Note: For the changes to take effect, **Restart IIS**.

5.4. Create New Template for IPSec

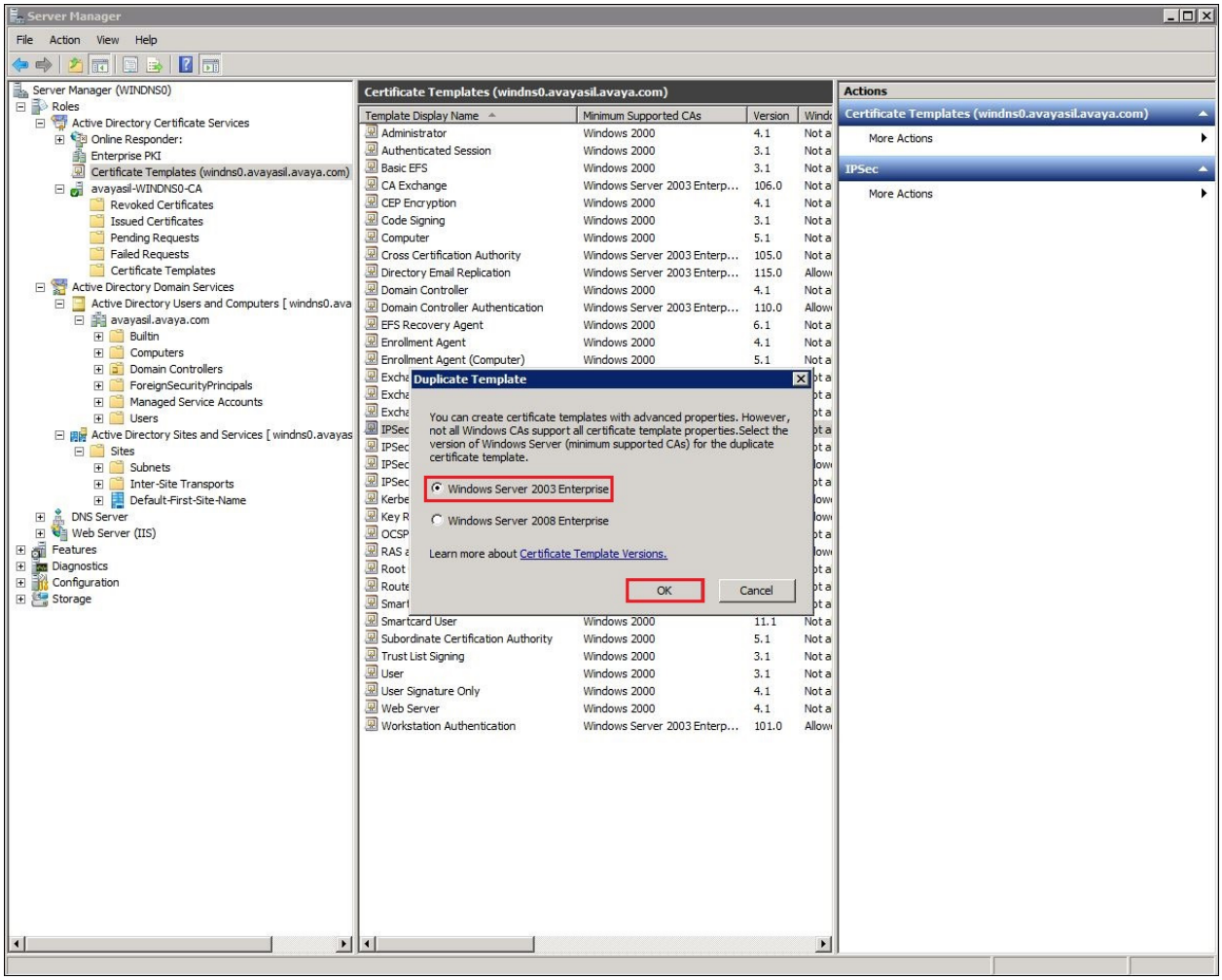
Make a duplicate template from IPSec. Go to **Server Manager → Roles → Active Directory Certificate Services →Certificate Templates** and find **IPSec**.



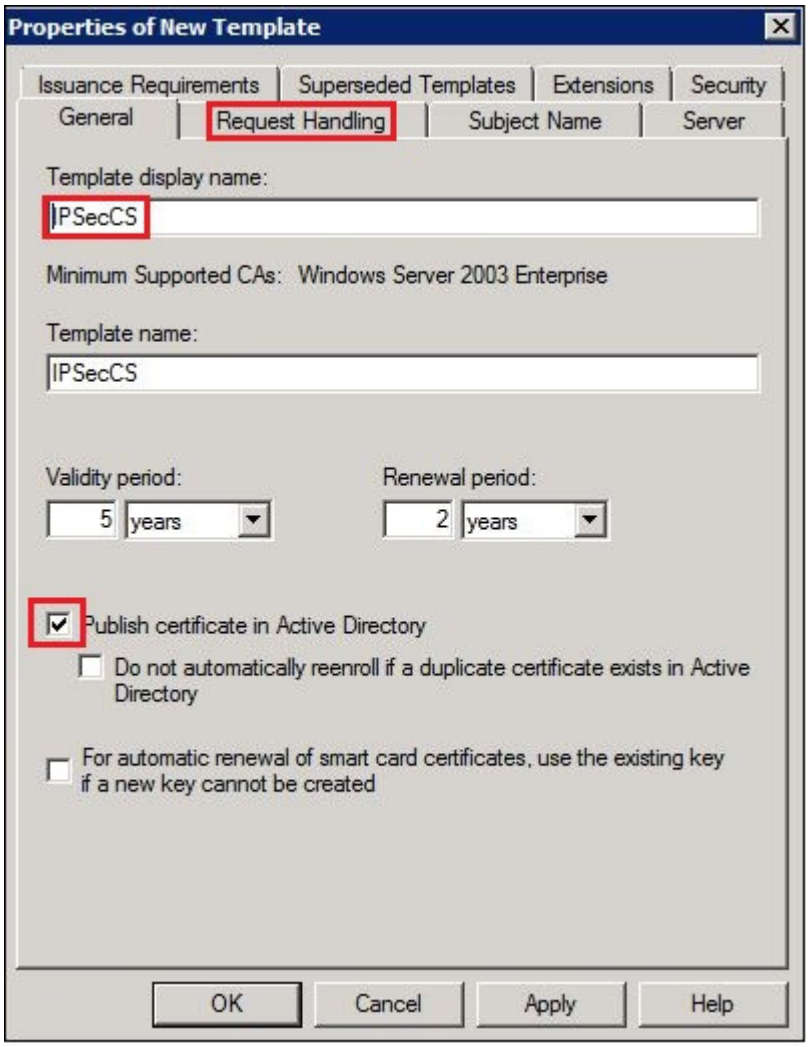
Right click on **IPSec.** Select **Duplicate Template.**



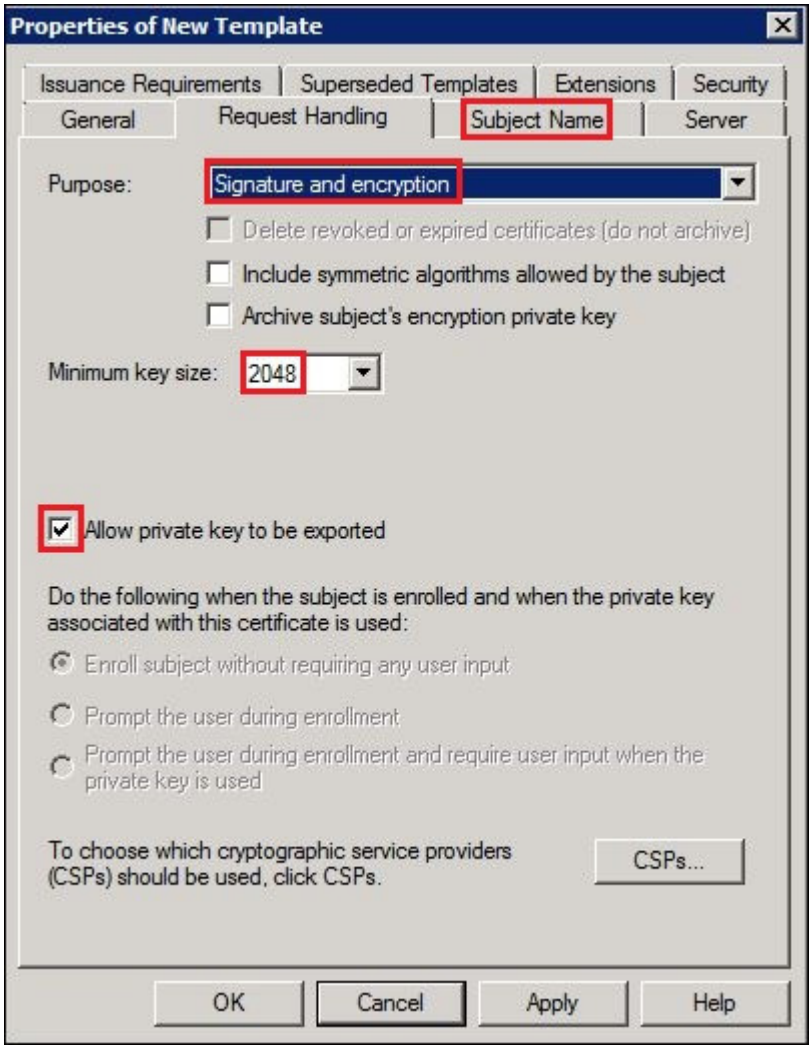
For this template select **Windows Server 2003 Enterprise** and click on **OK**.



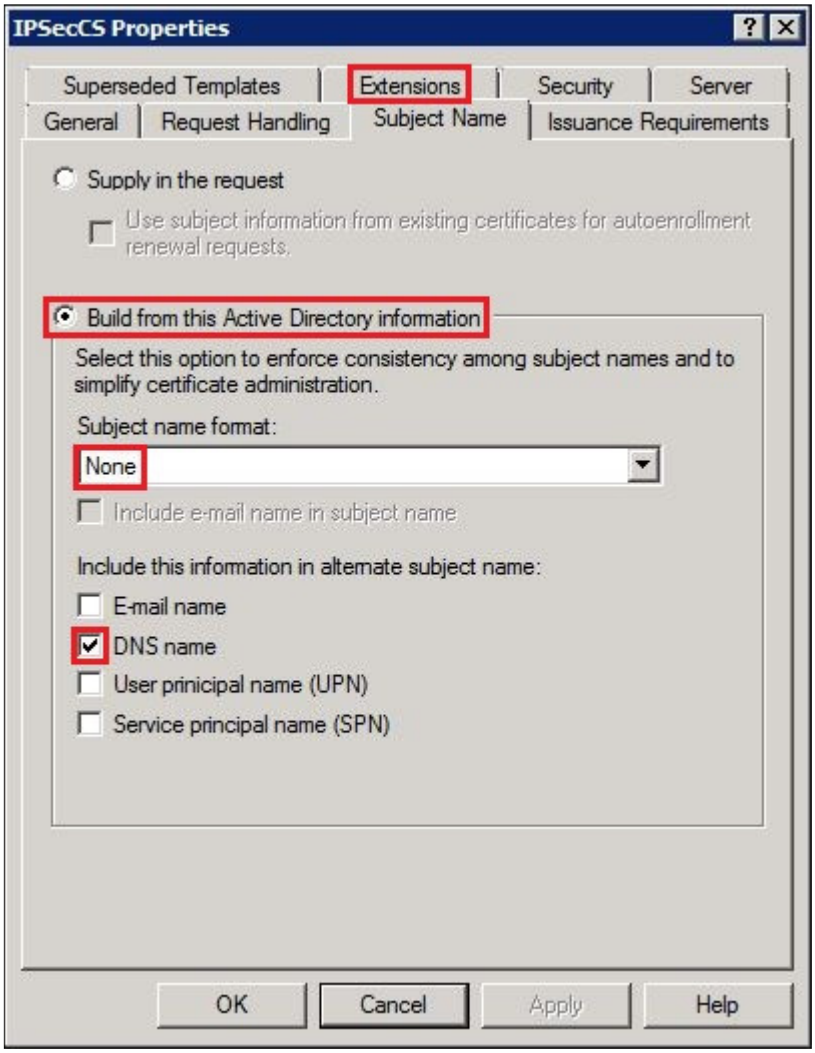
Input a suitable name for the new template under **Template display name**. Place a check beside **Publish certificate in Active Directory**. Select the **Request Handling** tab. See below.



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.

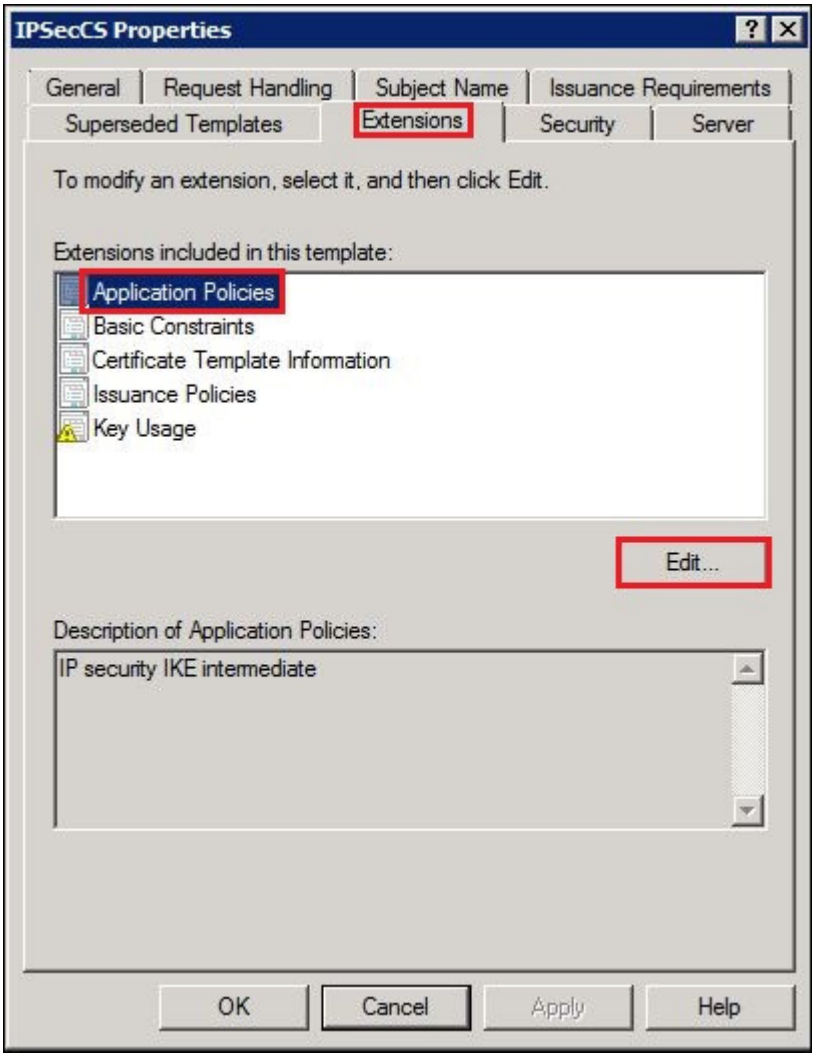


Under **Subject Name**, verify **Build from this Active Directory information** is selected. For this sample configuration **Subject name format** was set to **None**. Under **Include this information in alternate subject name**, verify there is a check beside **DNS name**. Select the **Extensions**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

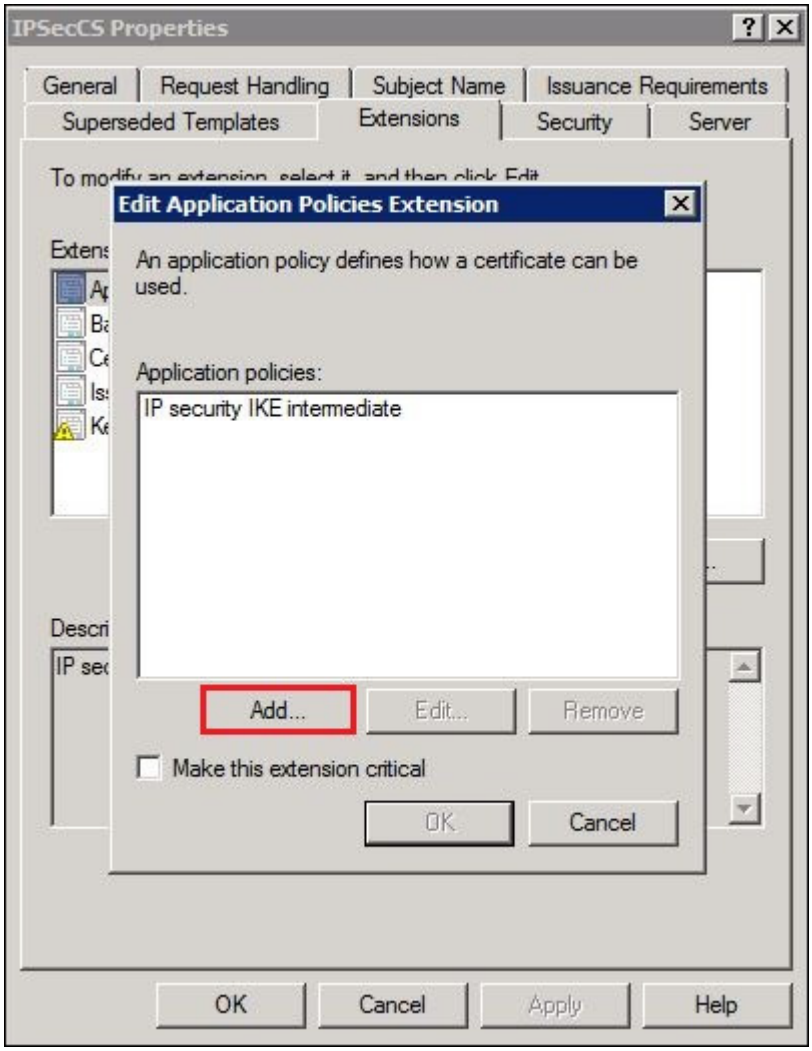


Note: For increased security select **Supply in the request**.

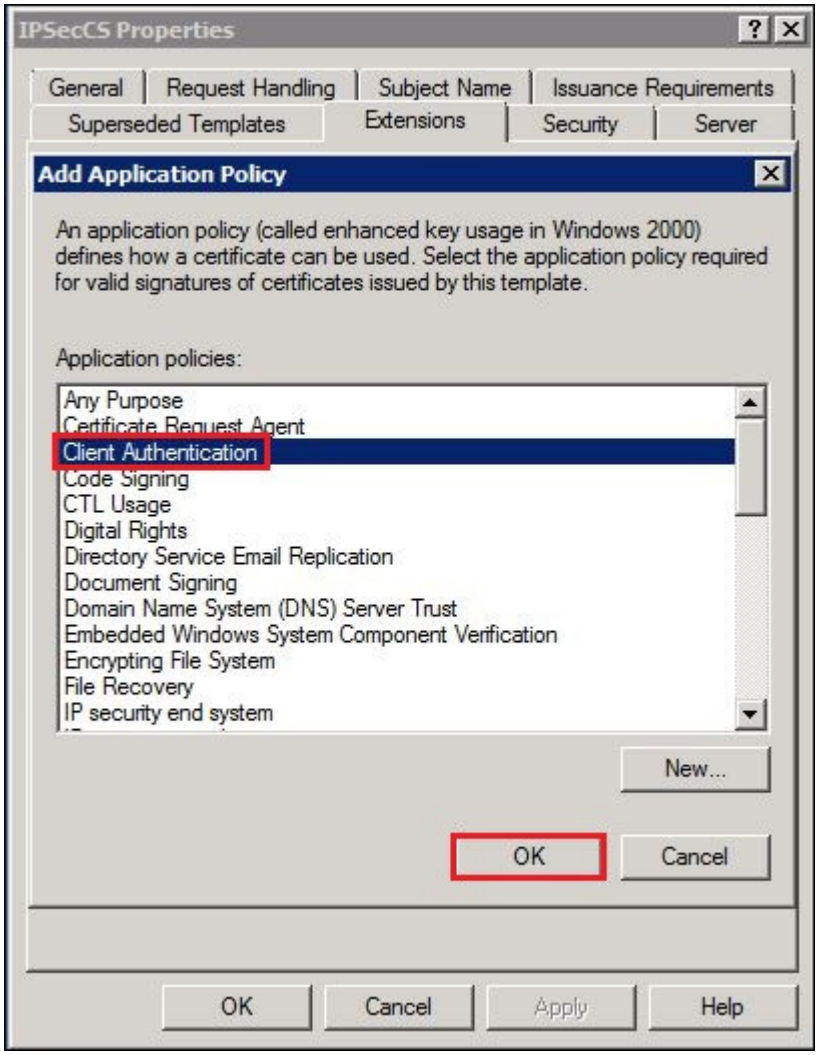
Under **Extensions**, select **Application Policies** and **Edit**.



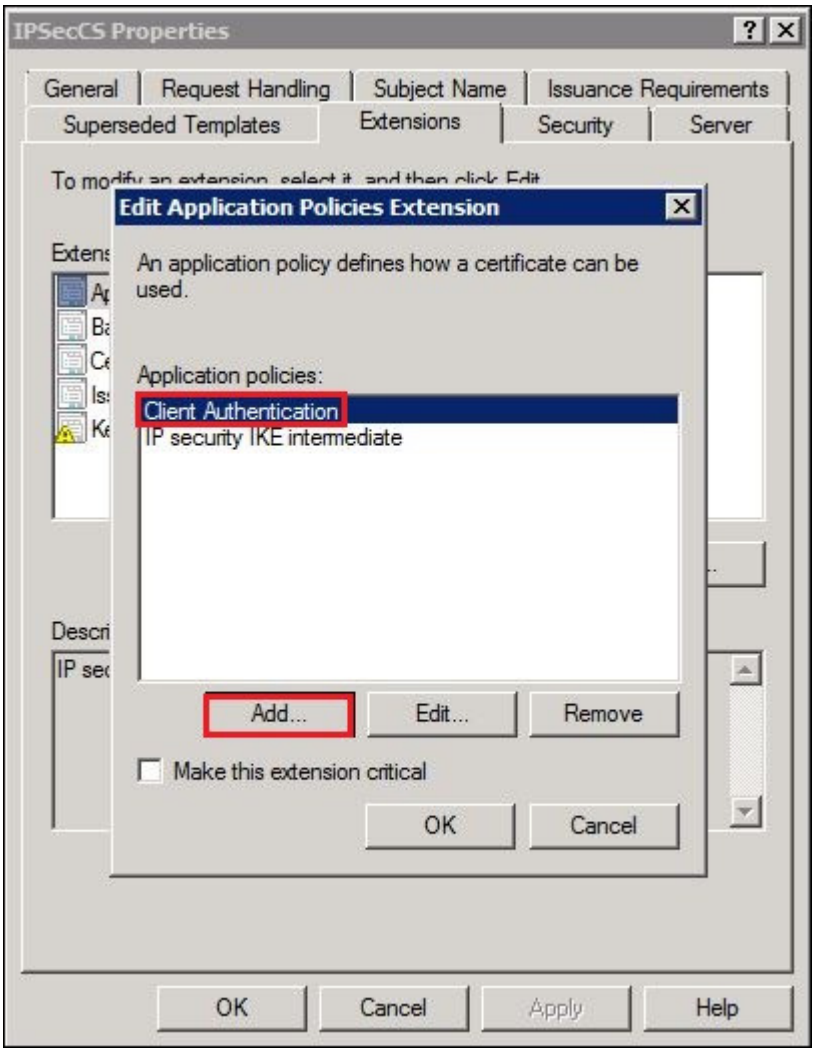
The **Edit Applications Policies Extension** window will open. Select **Add**.



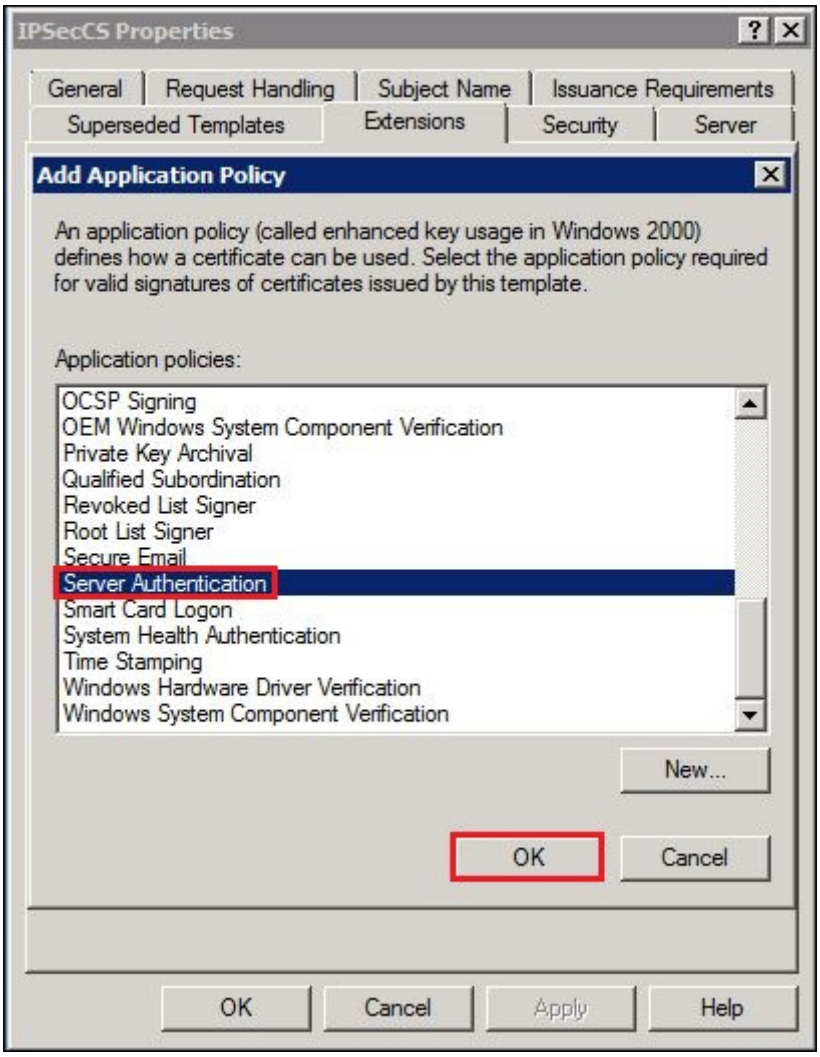
The **Add Application Policy** window will open. Select **Client Authentication** and click on **OK**.



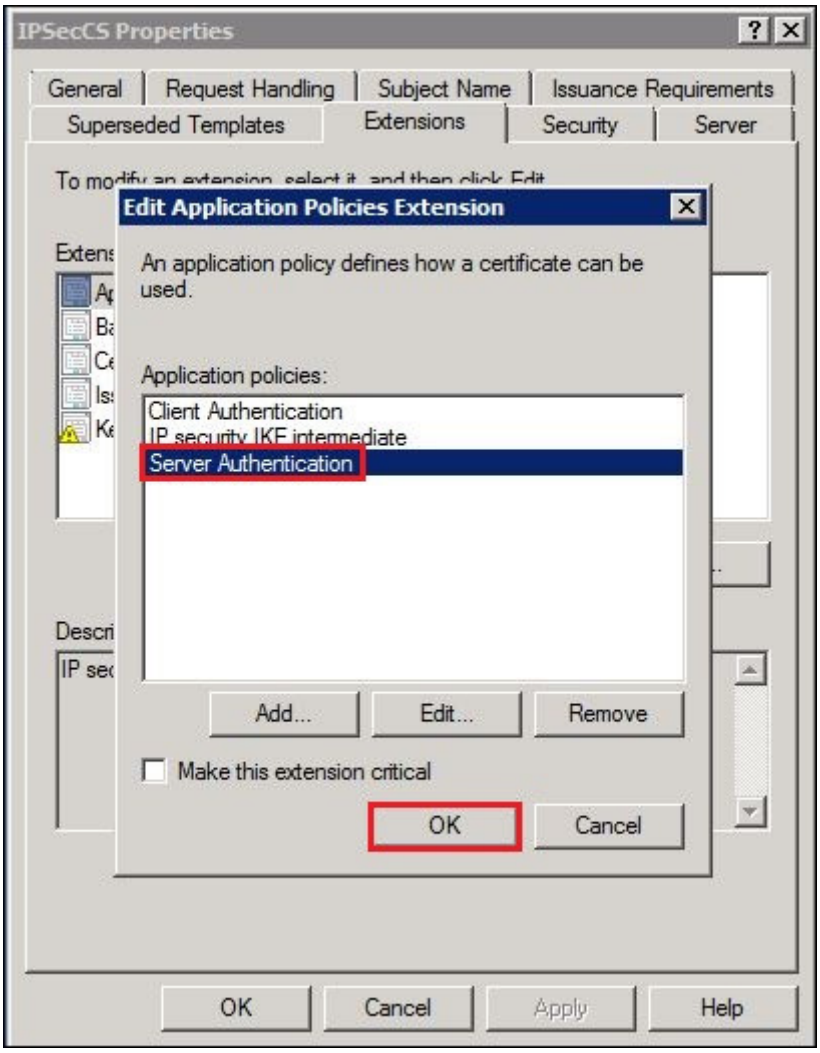
The **Edit Application Policies Extension** window will be displayed and show that **Client Authentication** has been added. Again, click on **Add**.



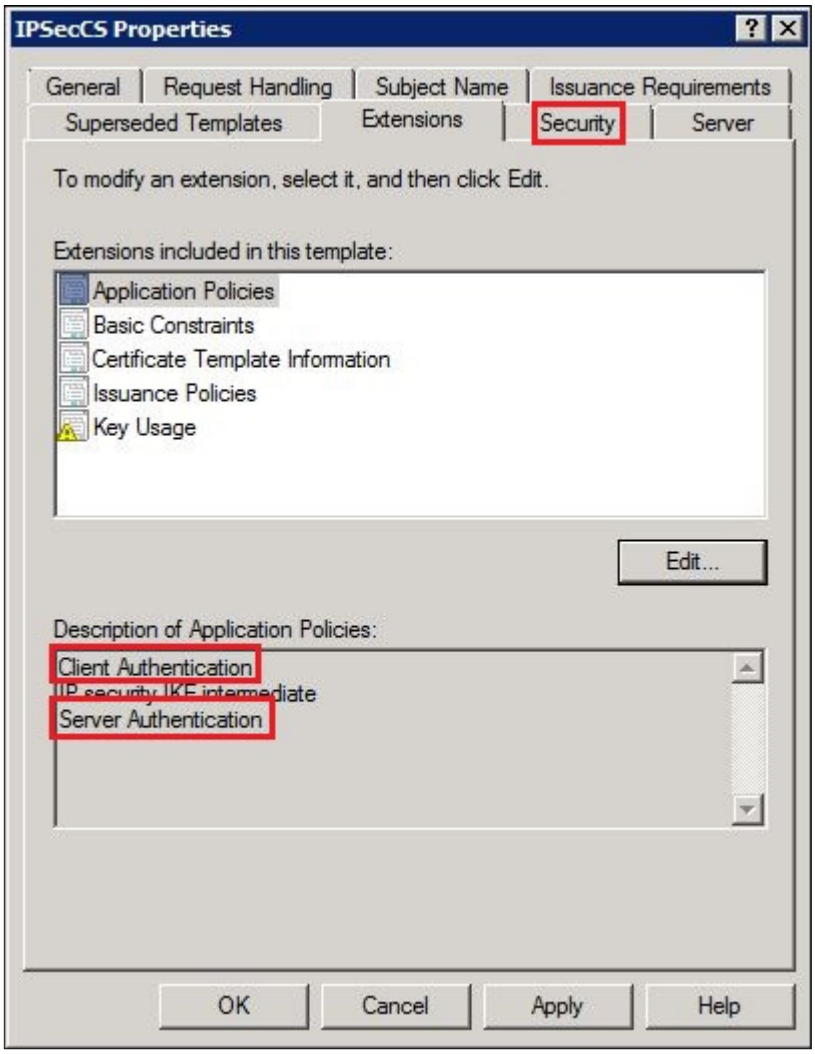
Again, the **Add Application Policy** window will open. Scroll down and select **Server Authentication.** Click on **OK**.



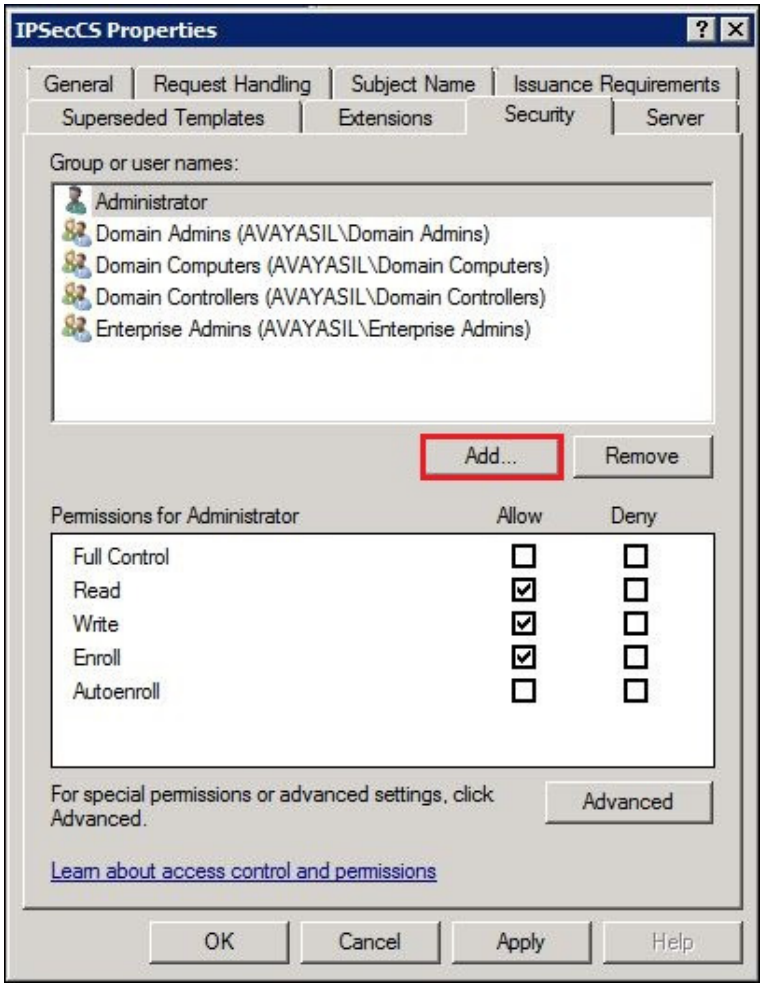
The **Edit Application Policies Extension** window will be displayed and show that **Server Authentication** has been added. Click on **OK**.



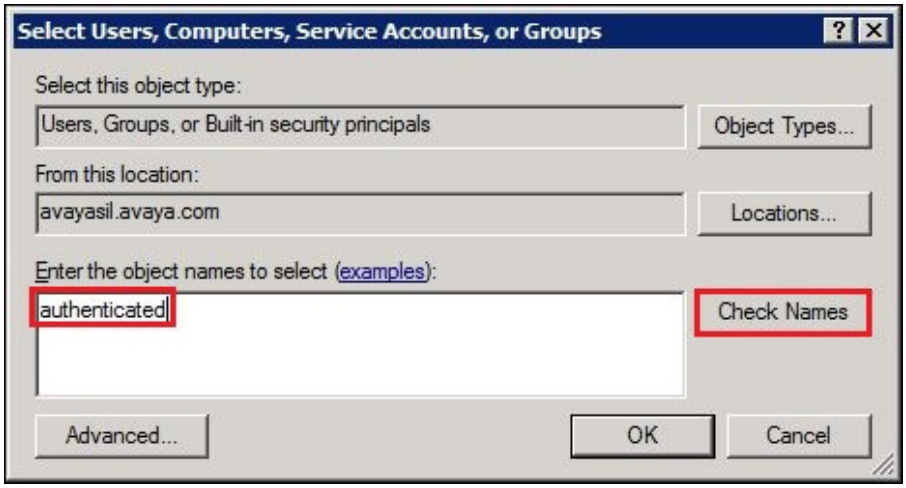
Under **Description of Application Policies**, verify **Client Authentication** and **Server Authentication** have been added. Click on the **Security** tab.



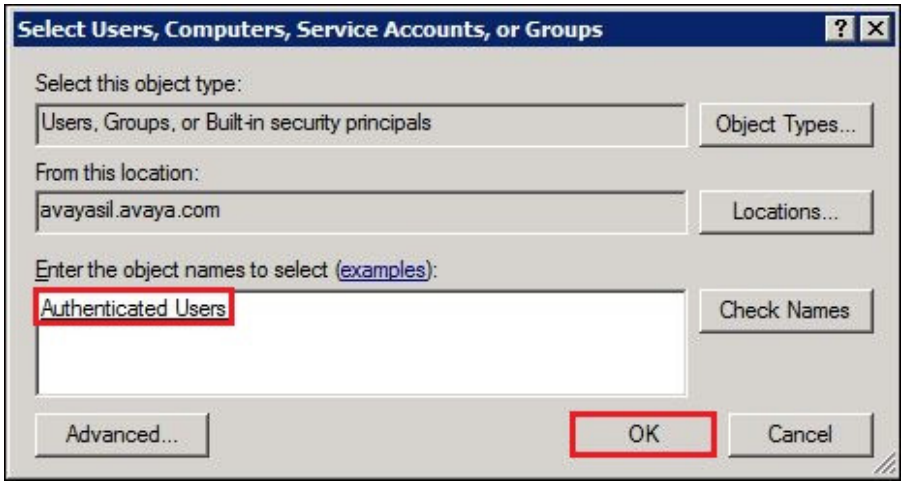
Under the **Security** tab, select **Add**. See below.



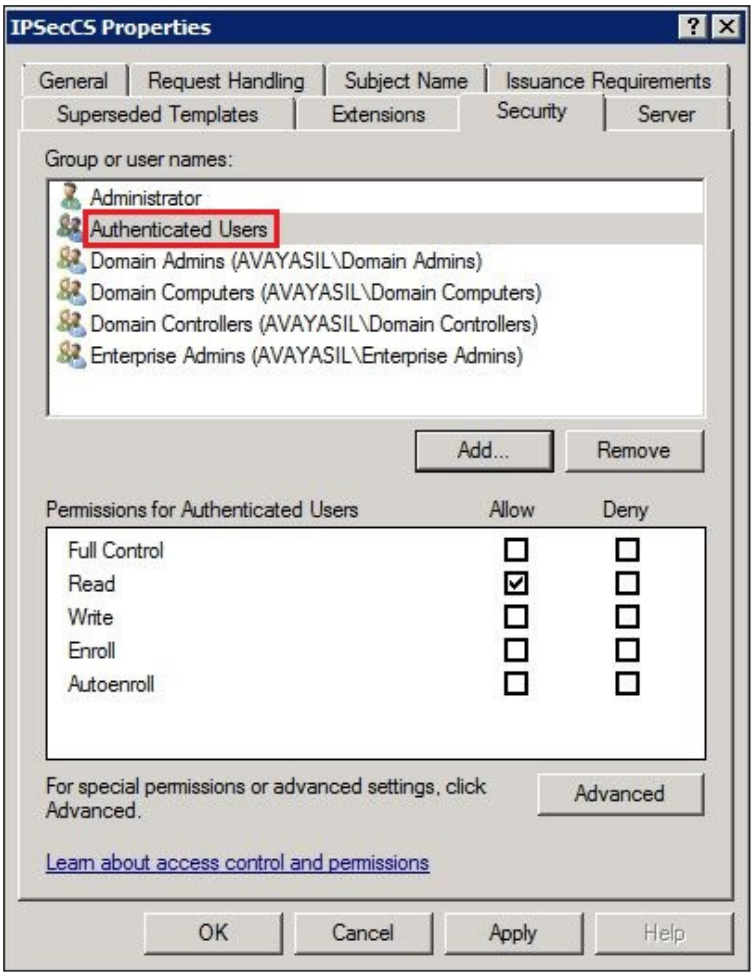
Input **authenticated** and click on **Check Names**.



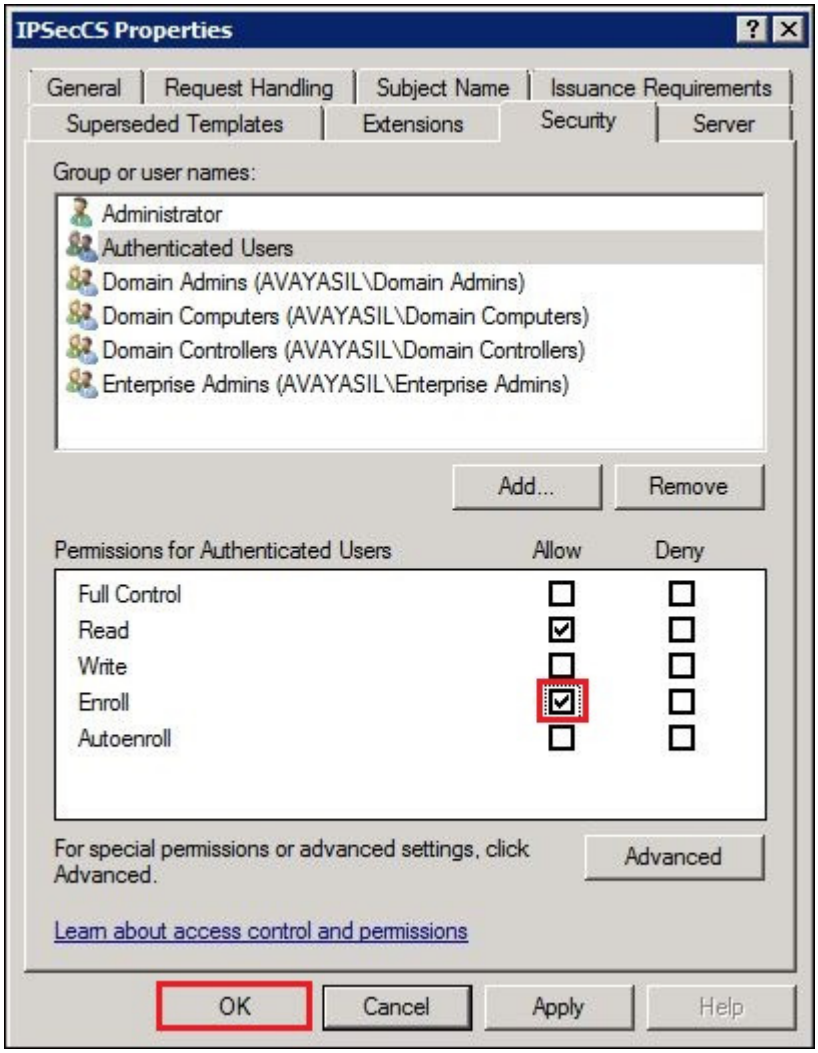
Verify the correct user group was found, **Authenticated Users**. Click on **OK**.



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

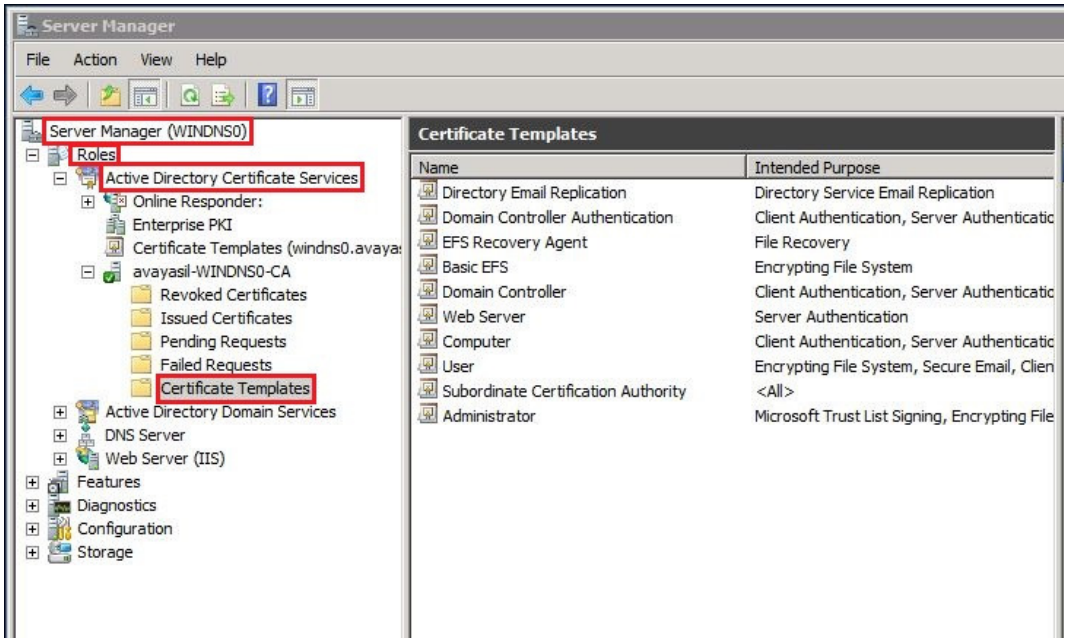


Under **Permissions for Authenticated Users**, check **Enroll** and select **OK** to create the new template.

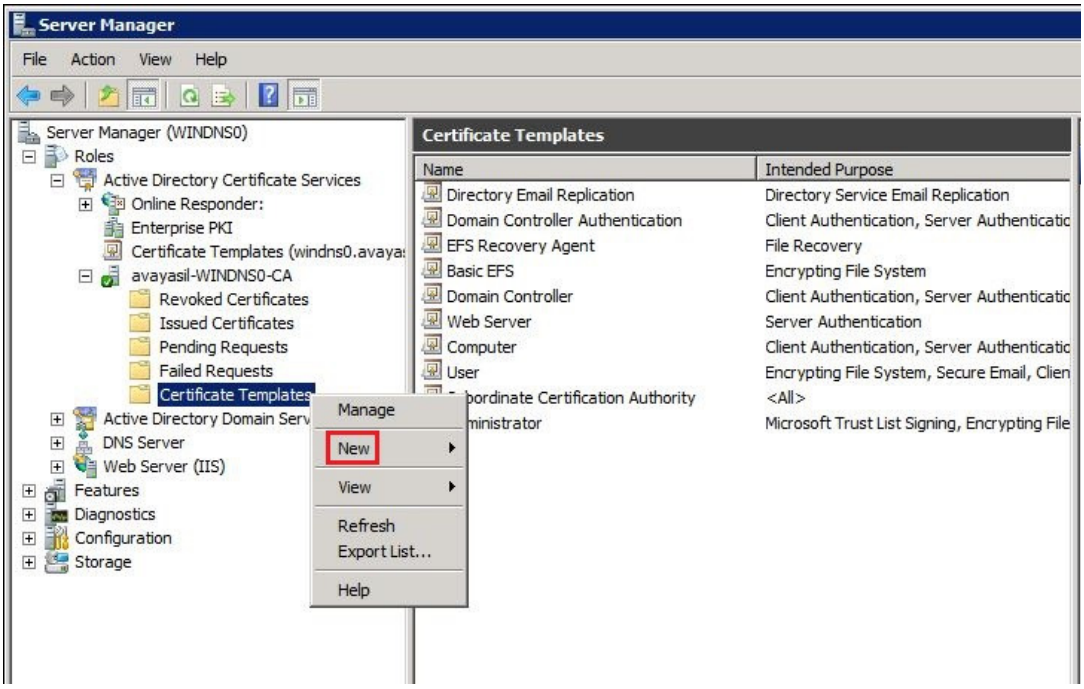


5.5. Issue Certificate Template.

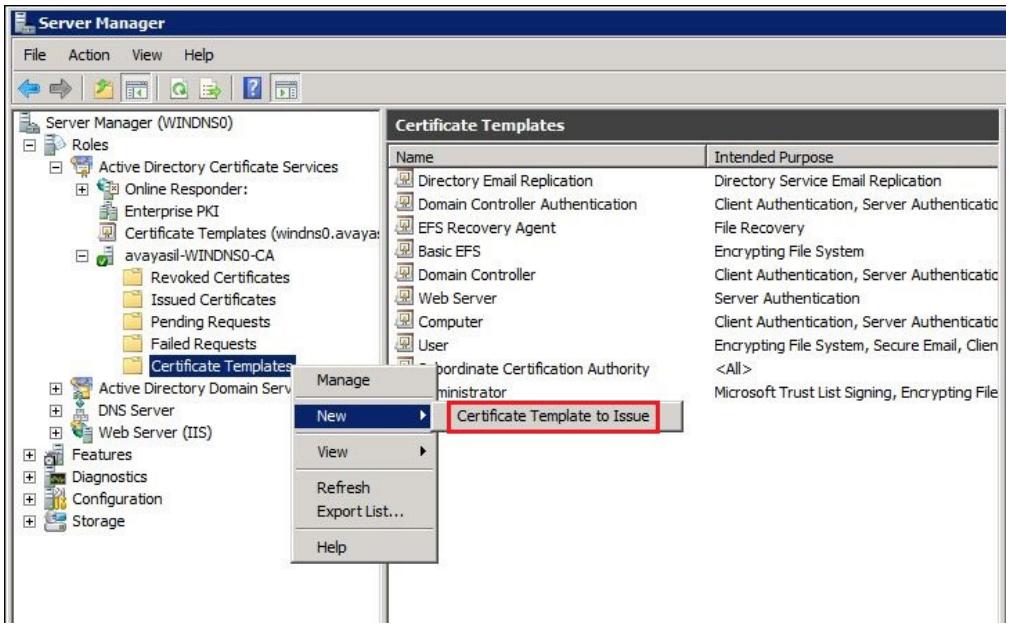
Go to **Server Manager → Roles → Active Directory Certificate Services →Certificate Templates.** See below.



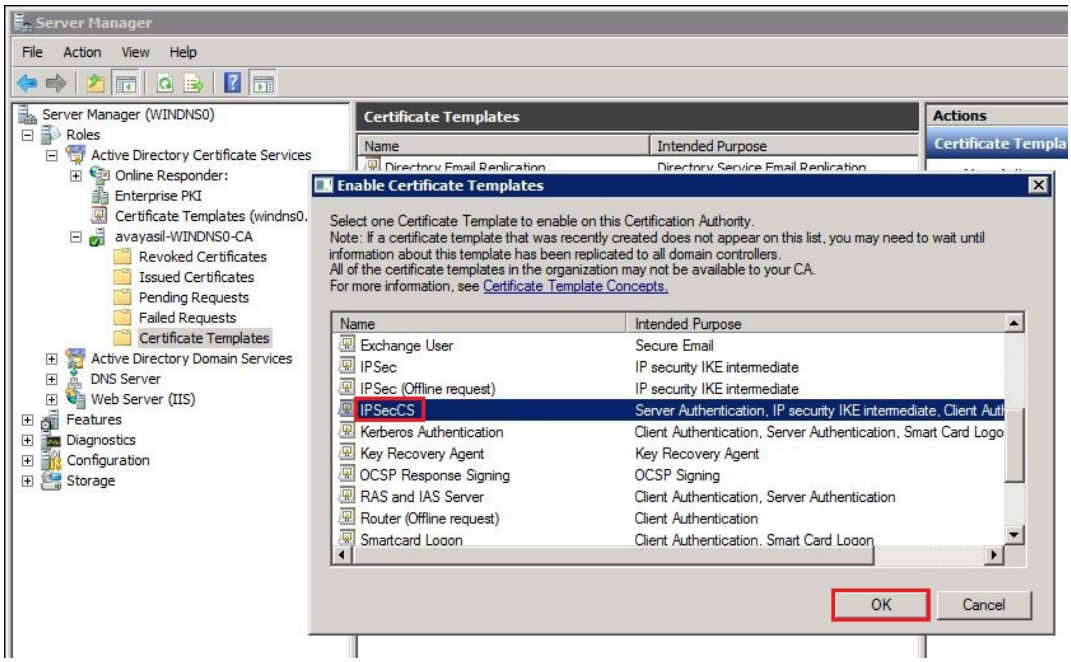
Right click on **Certificate Templates**. Select **New**.



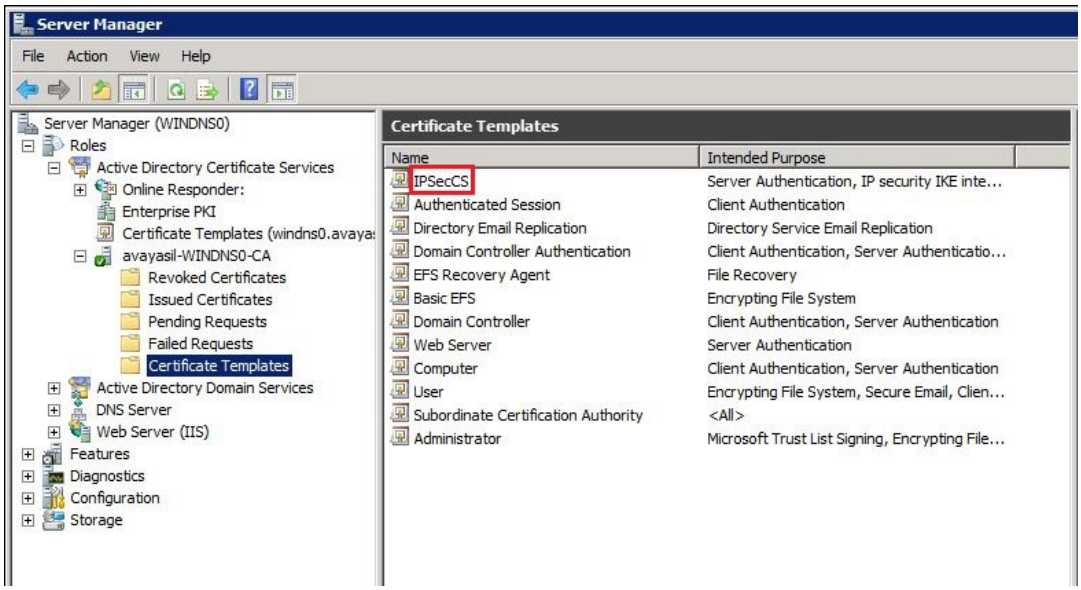
Select **Certificate Template to Issue**.



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



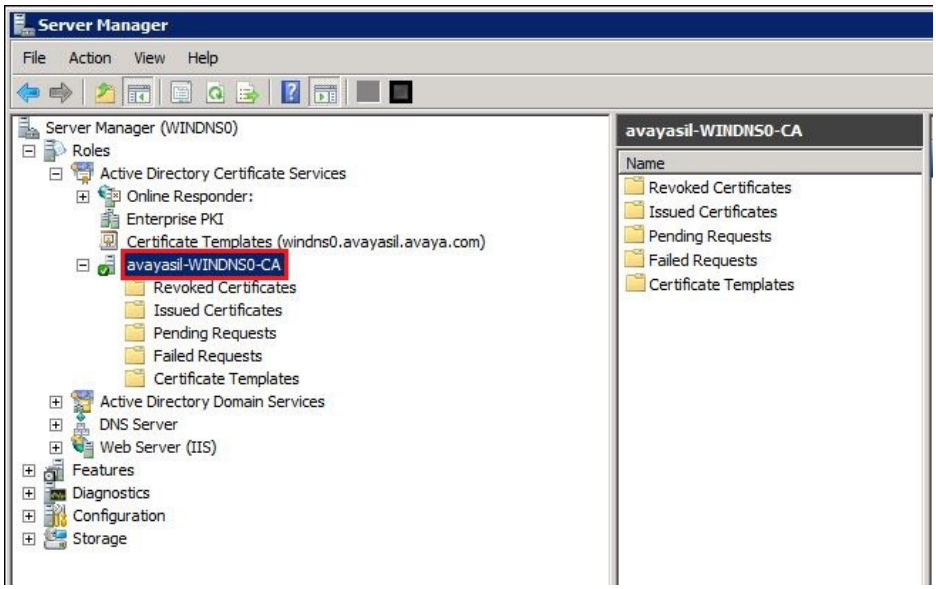
The certificate template has been issued and will be listed under **Certificate Templates**. See below.



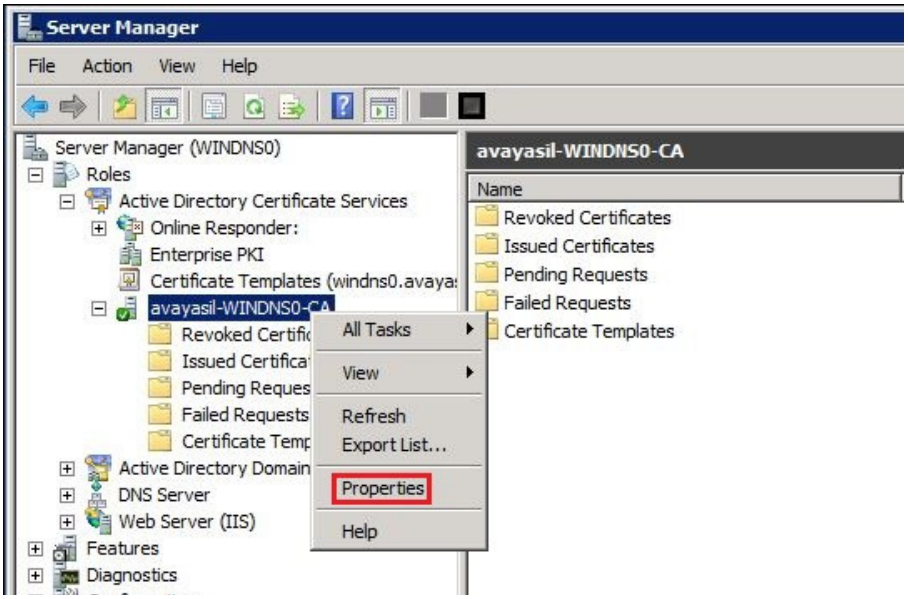
5.6. Export Certificate to .CER file

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.

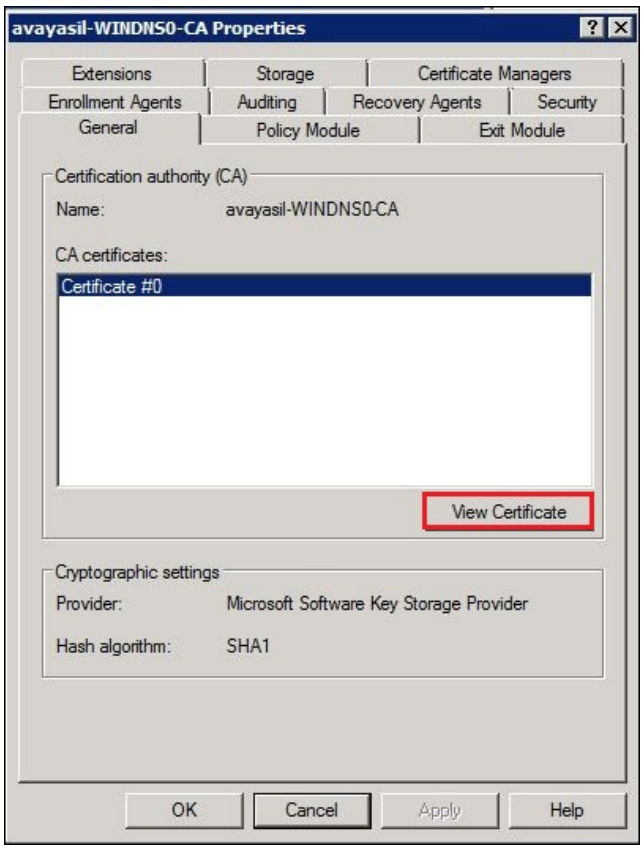
Go to **Start → Administrative Tools → Server Manager**. Select **Server Manager** (not shown). After the window for Server Manager opens, go to **Active Directory Certificate Services** and select the Certificate Authority created in **Section 5.1**. See below.



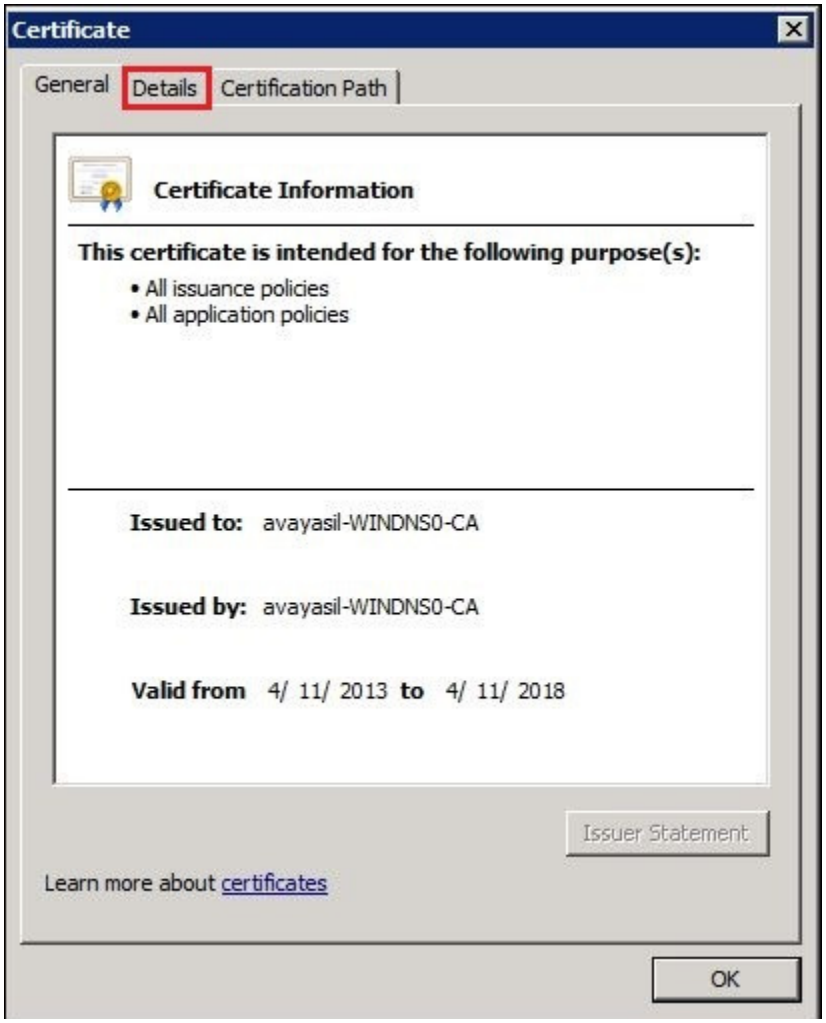
Right click on the Certificate Authority and select **Properties**.



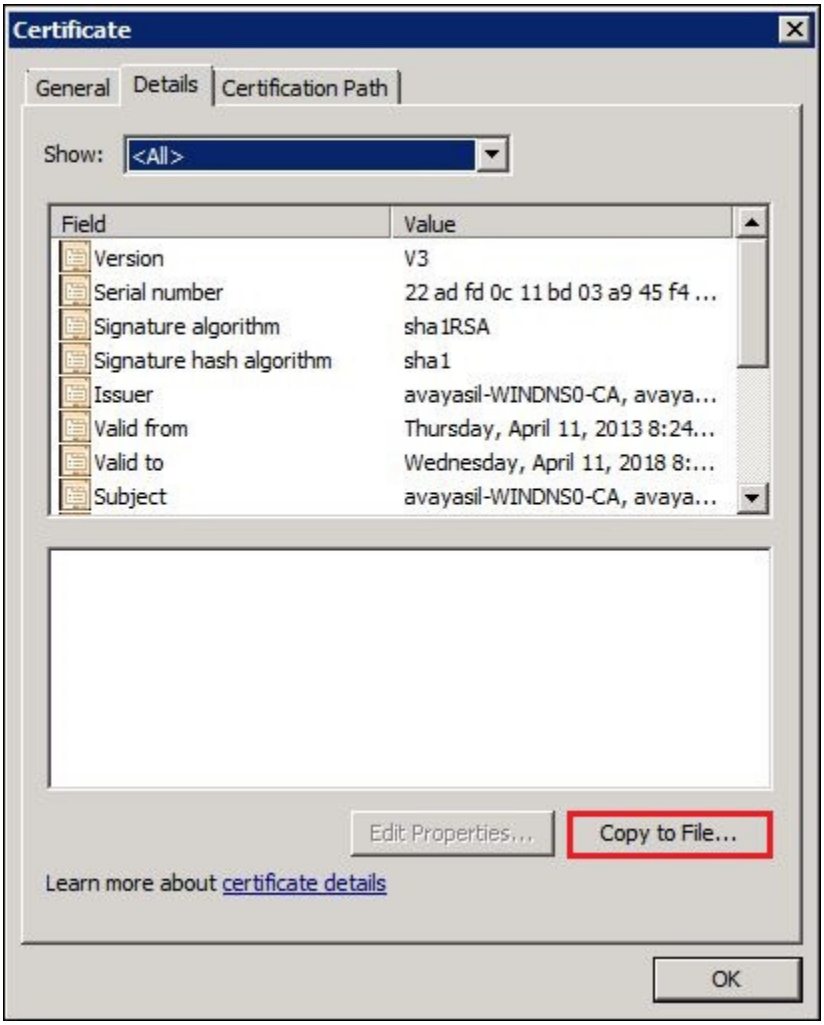
Click on **View Certificate.**



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

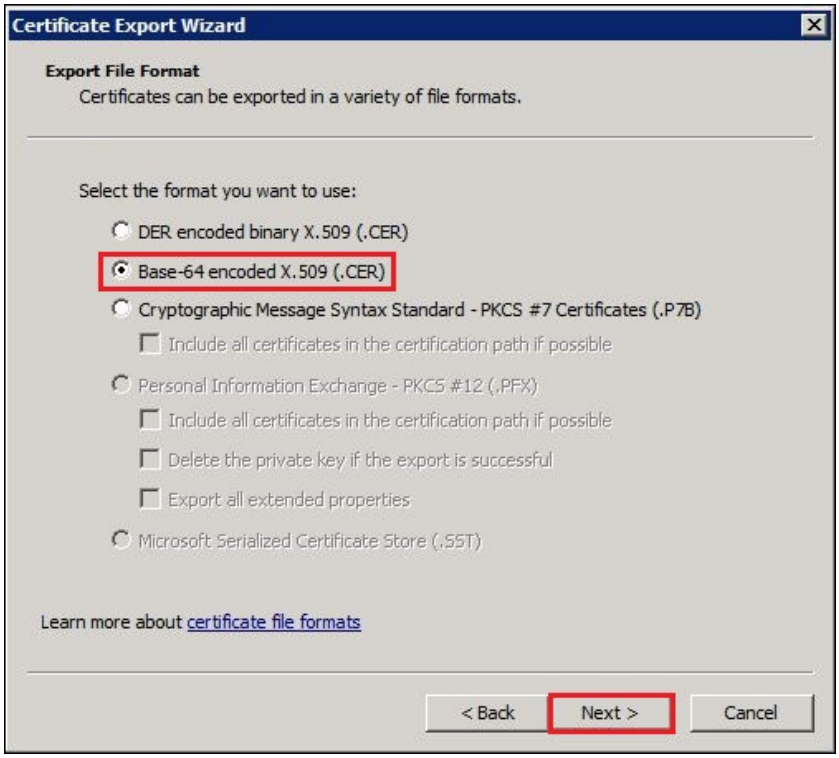


Select **Copy to File**.

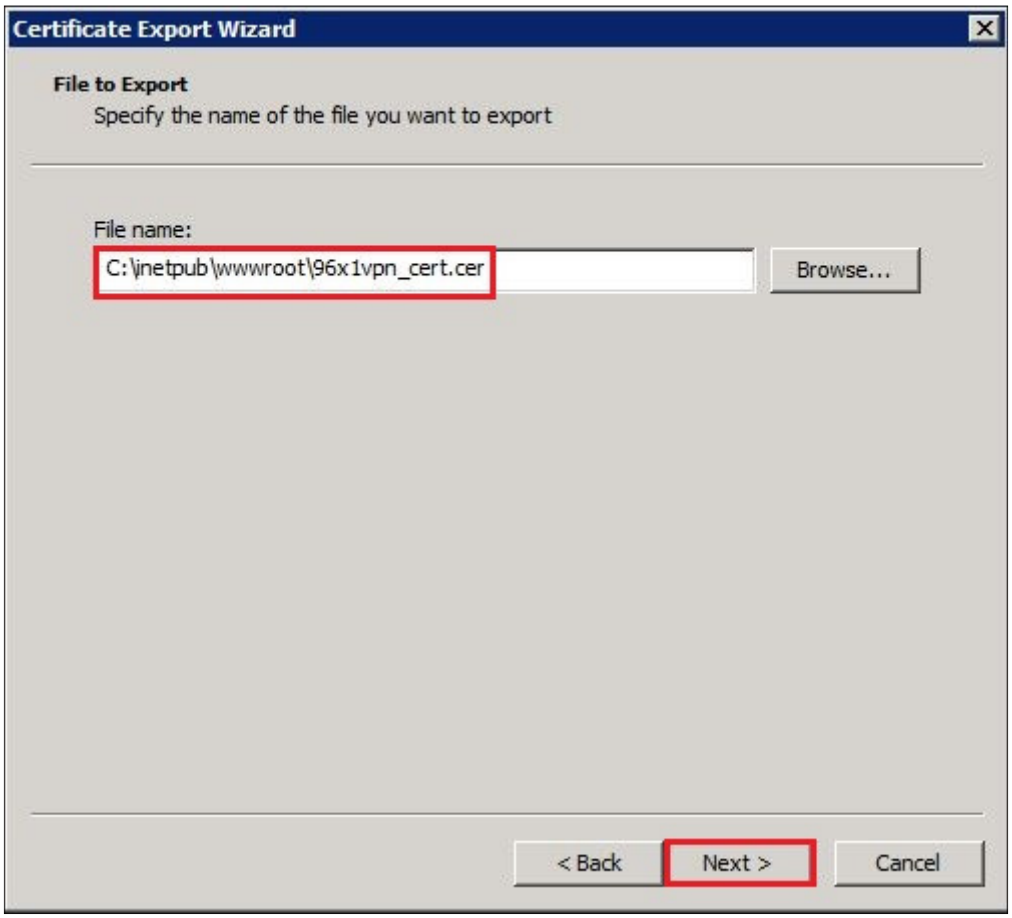


The **Welcome to the Certificate Export Wizard** page is displayed. Click on the **Next** button.

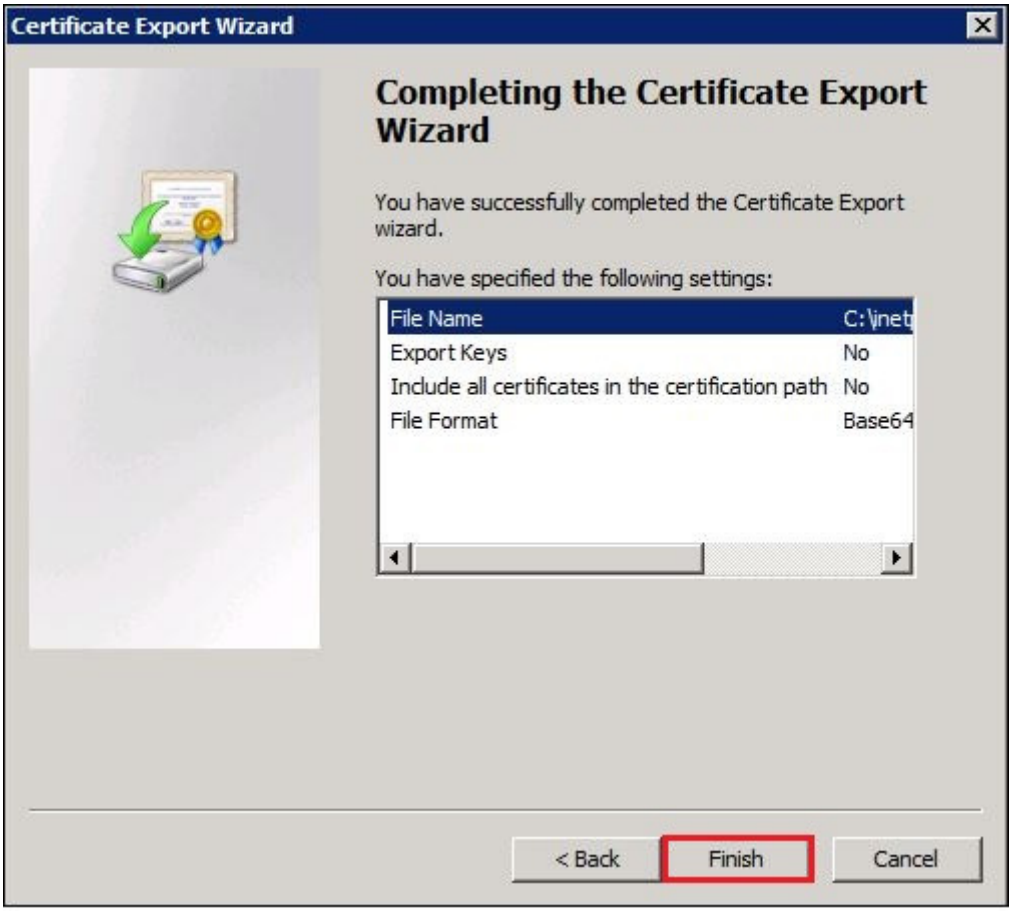
Select the **Base-64 encoded X.509 (.CER)** option. Select **Next**.



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 **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.

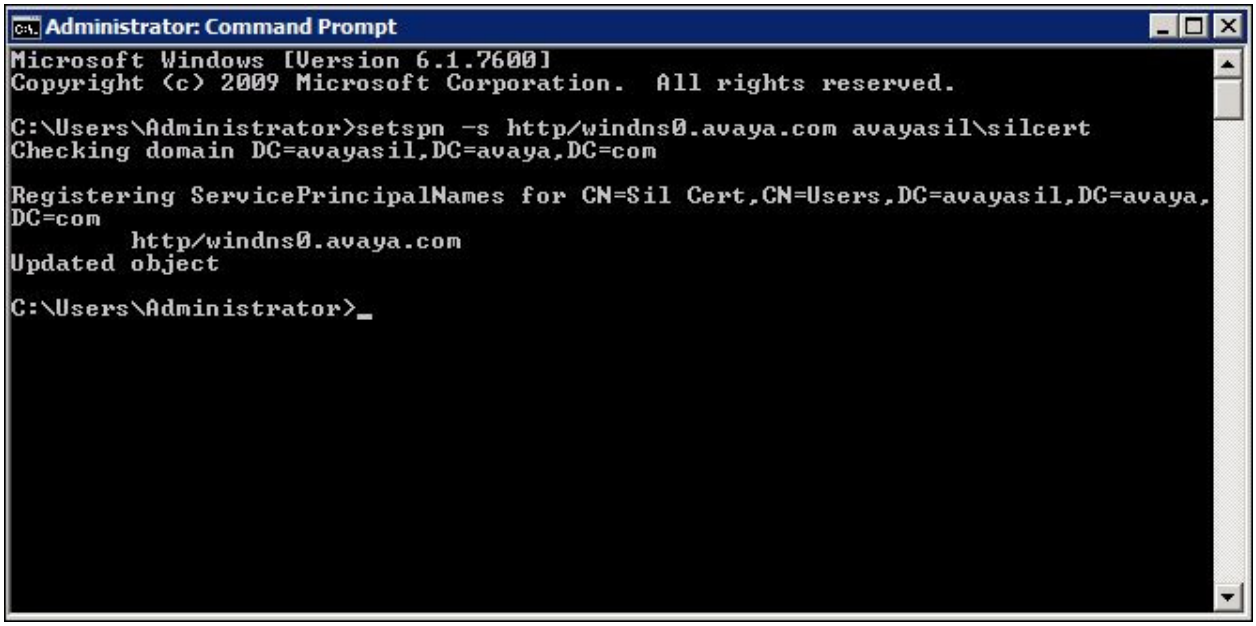
5.7. Execute setspn

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.



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

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