5760/3850 Series WLC PEAP Authentication with Microsoft NPS Configuration Example

Contents

Introduction

This document describes how to configure Protected Extensible Authentication Protocol (PEAP) with Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAP v2) authentication on a Cisco Converged Access Wireless LAN (WLAN) deployment with the Microsoft Network Policy Server (NPS) as the RADIUS server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics before you attempt the configuration described in this document:

- Basic Microsoft Windows Version 2008 installation
- Cisco Converged Access WLAN controller installation

Ensure that these requirements are met before you attempt this configuration:

- Install the Microsoft Windows Server Version 2008 Operating System (OS) on each of the servers in the test lab.
- Update all of the service packs.
- Install the controllers and Lightweight Access Points (LAPs).
- Configure the latest software updates.

> **Note**: For initial installation and configuration information for the Cisco Converged Access WLAN controllers, refer to the CT5760 Controller and Catalyst 3850 Switch Configuration Example Cisco article.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5760 Series WLAN Controller Version 3.3.2 (Next Generation Wiring Closet (NGWC))
- Cisco 3602 Series LAP
- Microsoft Windows XP with Intel PROset Supplicant
- Microsoft Windows Version 2008 Server that runs NPS with Domain Controller Roles
- Cisco Catalyst 3560 Series Switch

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

PEAP uses Transport Level Security (TLS) in order to create an encrypted channel between an authenticating PEAP client, such as a wireless laptop, and a PEAP authenticator, such as the Microsoft NPS or any RADIUS server. PEAP does not specify an authentication method but provides additional security for other Extensible Authentication Protocols (EAPs), such as EAP-MS-CHAP v2, that can operate through the TLS-encrypted channel that is provided by PEAP. The PEAP authentication process consists of two main phases.

PEAP Phase One: TLS-Encrypted Channel

The wireless client associates with the Access Point (AP). An IEEE 802.11-based association provides an open system or shared key authentication before a secure association is created between the client and the AP. After the IEEE 802.11-based association is successfully established between the client and the AP, the TLS session is negotiated with the AP.

After authentication is successfully completed between the wireless client and the NPS, the TLS session is negotiated between the client and the NPS. The key that is derived within this negotiation is used in order to encrypt all subsequent communication.

PEAP Phase Two: EAP-Authenticated Communication

EAP communication, which includes EAP negotiation, occurs inside of the TLS channel that is created by PEAP within the first stage of the PEAP authentication process. The NPS authenticates the wireless client with EAP-MS-CHAP v2. The LAP and the controller only forward messages between the wireless client and the RADIUS server. The WLAN Controller (WLC) and the LAP cannot decrypt the messages because the WLC is not the TLS endpoint.

Here is the RADIUS message sequence for a successful authentication attempt, where the user supplies valid password-based credentials with PEAP-MS-CHAP v2:

1. The NPS sends an identity request message to the client:

```
EAP-Request/Identity
```

2. The client responds with an identity response message:

   ```
   EAP-Response/Identity
   ```

3. The NPS sends an MS-CHAP v2 challenge message:

   ```
   EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge)
   ```

4. The client responds with an MS-CHAP v2 challenge and response:

   ```
   EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response)
   ```

5. The NPS responds with an MS-CHAP v2 success packet when the server successfully authenticates the client:

   ```
   EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success)
   ```

6. The client responds with an MS-CHAP v2 success packet when the client successfully authenticates the server:

   ```
   EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success)
   ```

7. The NPS sends an EAP-type-length-value (TLV) that indicates successful authentication.

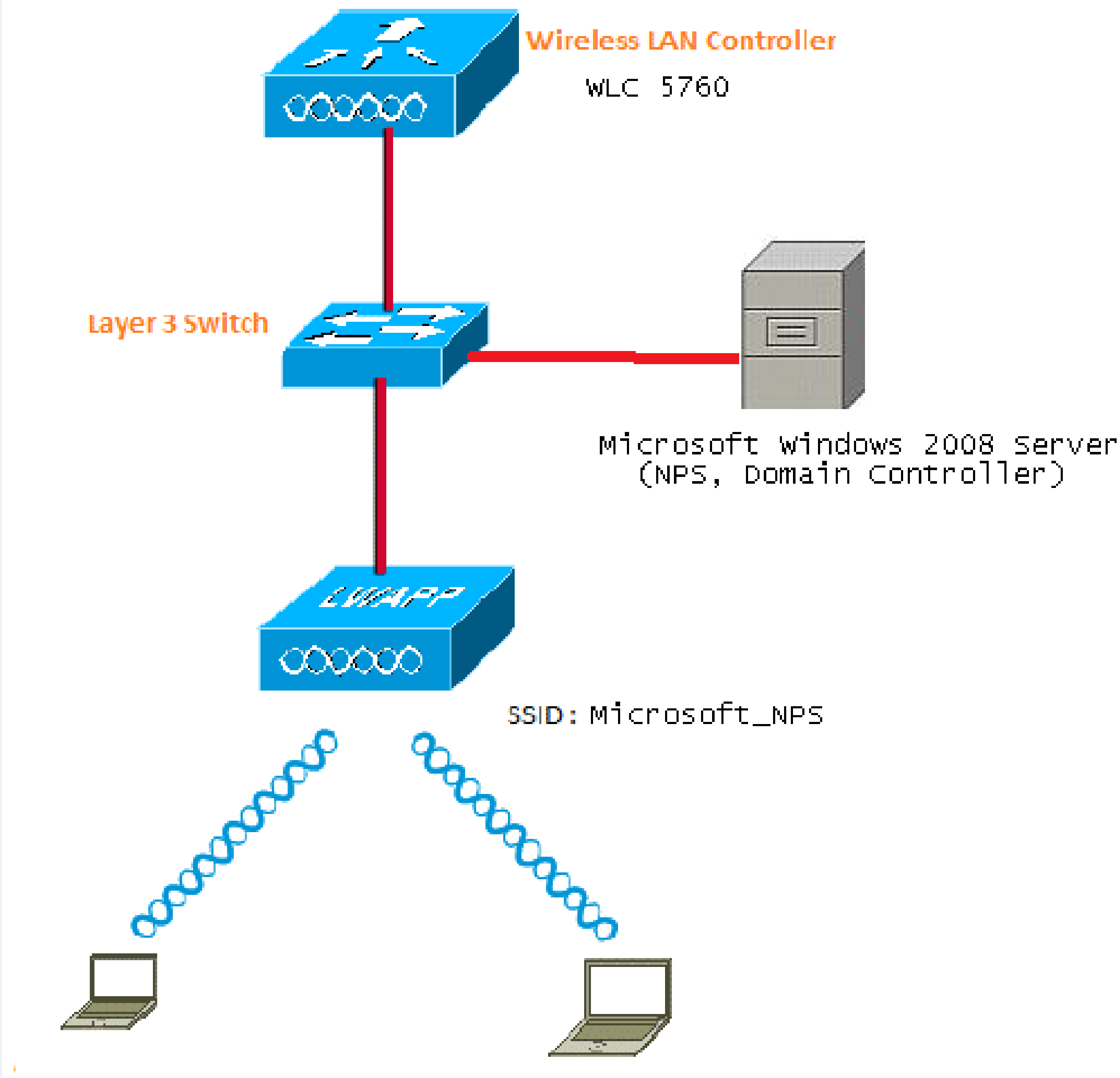
8. The client responds with an EAP-TLV status success message.

9. The server completes authentication and sends an EAP-Success message in plain text. If VLANs are deployed for client isolation, the VLAN attributes are included in this message.

Configure

Use this section in order to configure PEAP with MS-CHAP v2 authentication on a Cisco Converged Access WLC deployment with the Microsoft NPS as the RADIUS server.

Network Diagram



In this example, the Microsoft Windows Version 2008 server performs these roles:

- Domain controller for the **wireless.com** domain
- Domain Name System (DNS) server
- Certificate Authority (CA) server
- NPS in order to authenticate the wireless users
- Active Directory (AD) in order to maintain the user database

The server connects to the wired network through a Layer 2 (L2) switch, as shown. The WLC and the registered LAP also connect to the network through the L2 switch.

The wireless clients use Wi-Fi Protected Access 2 (WPA2) - PEAP-MS-CHAP v2 authentication in order to connect to the wireless network.

Configurations

The configuration that is described in this section is completed in two steps:

1. Configure the 5760/3850 Series WLC with the CLI or GUI.

2. Configure the Microsoft Windows Version 2008 server for NPS, Domain Controller, and User Accounts on the AD.

Configure Converged Access WLCs with the CLI

Complete these steps in order to configure the WLAN for the required client VLAN and map it to the Authentication Method List with the CLI:

> **Note**: Ensure that **dot1x system auth control** is enabled on the WLC, or the dot1X does not work.

1. Enable the **AAA new model** feature.

2. Configure the RADIUS server.

3. Add the server into the Server Group.

4. Map the Server Group to the Method List.

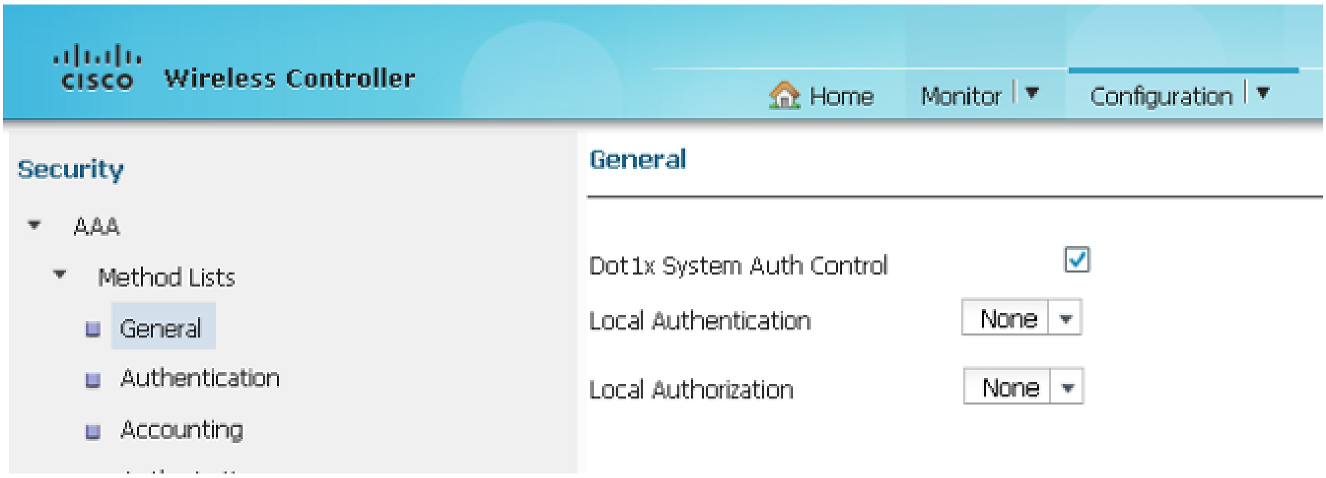
5. Map the Method List to the WLAN.

```
aaa new-model
!
!
aaa group server radius Microsoft_NPS
 server name Microsoft_NPS
!
aaa authentication dot1x Microsoft_NPS group Microsoft_NPS

aaa authorization network Microsoft_NPS group Microsoft_NPS
radius server Microsoft_NPS
 address ipv4 10.104.208.96 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 10
 key Cisco123

wlan Microsoft_NPS 8 Microsoft_NPS
 client vlan VLAN0020
 no exclusionlist
 security dot1x authentication-list Microsoft_NPS
 session-timeout 1800
 no shutdown
```

Configure Converged Access WLCs with the GUI

Complete these steps in order to configure the Converged Access WLCs with the GUI:

1. Enable the **dot1x system-auth-control**:



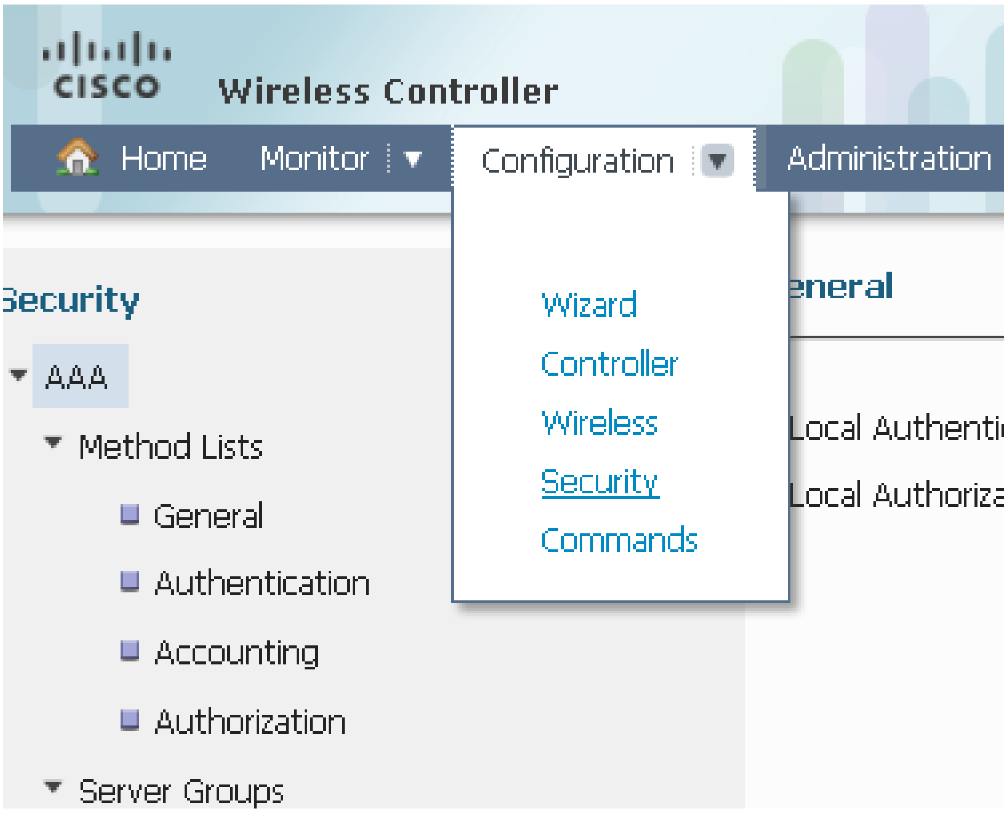
General

Dot1x System Auth Control ☑

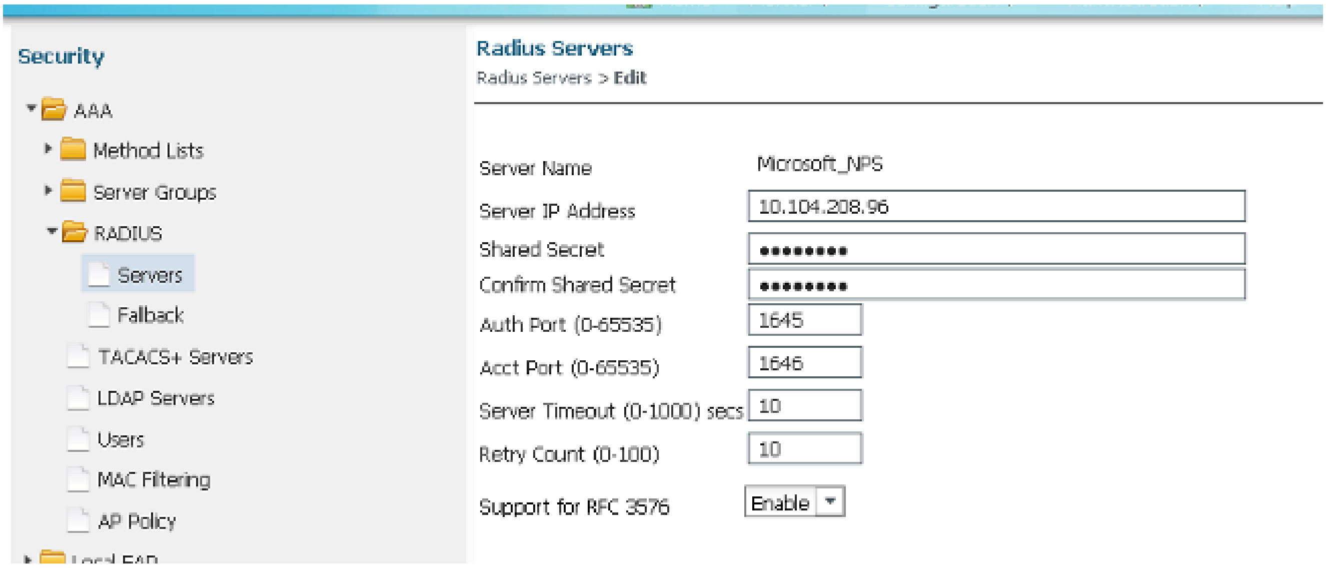
Local Authentication None

Local Authorization None

2. Navigate to **Configuration** > **Security** > **AAA** in order to add the RADIUS server:



3. Navigate to **RADIUS > Servers**, click **NEW**, and update the IP address of the RADIUS server along with the shared secret. The shared secret should match the shared secret that is configured on the RADIUS server as well.

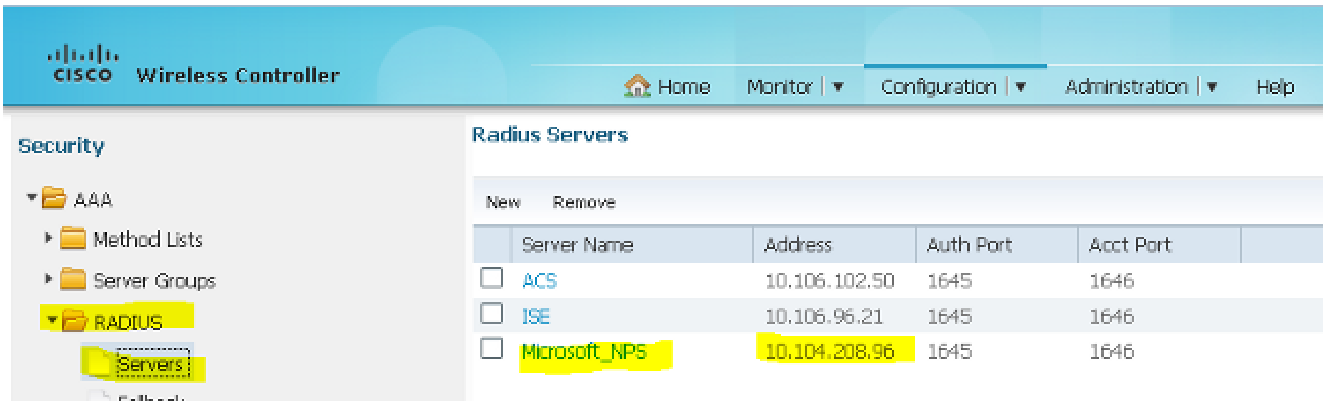


Radius Servers

Radius Servers > Edit

Server Name	Microsoft_NPS
Server IP Address	10.104.208.96
Shared Secret	••••••••
Confirm Shared Secret	••••••••
Auth Port (0-65535)	1645
Acct Port (0-65535)	1646
Server Timeout (0-1000) secs	10
Retry Count (0-100)	10
Support for RFC 3576	Enable

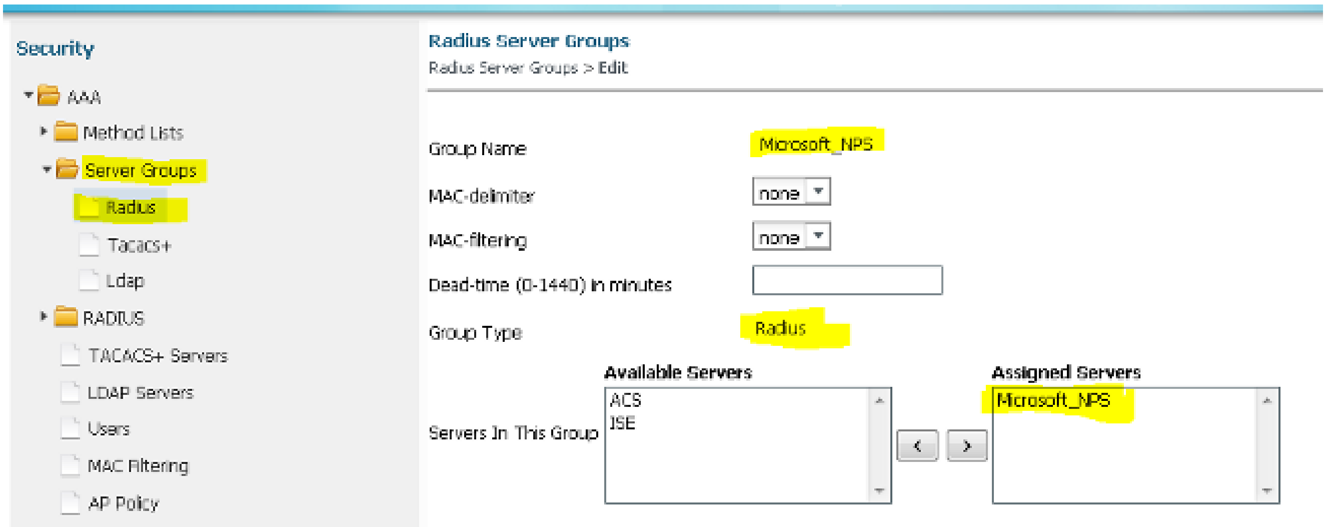
After you configure the RADIUS server, the Server tab should appear similar to this:



Radius Servers

	Server Name	Address	Auth Port	Acct Port
□	ACS	10.106.102.50	1645	1646
□	ISE	10.106.96.21	1645	1646
□	Microsoft_NPS	10.104.208.96	1645	1646

4. Configure a Server Group and select **Radius** for the Group Type. Then, add the RADIUS server that you created in the previous step:



Radius Server Groups

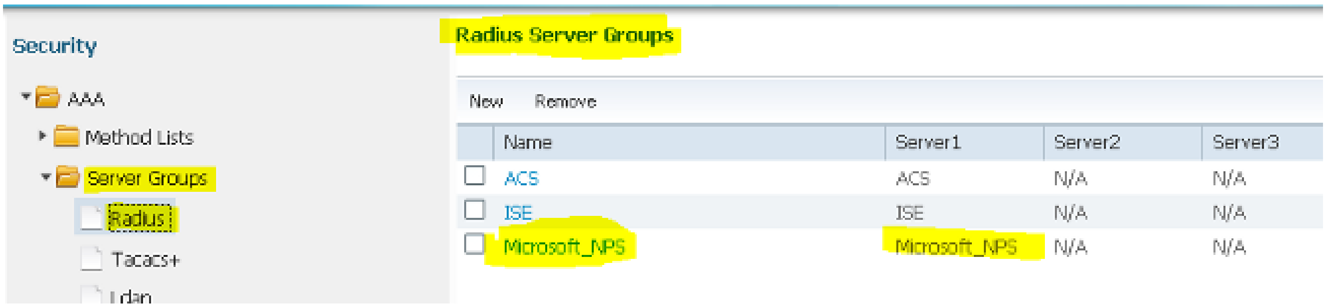
Radius Server Groups > Edit

Group Name	Microsoft_NPS
MAC-delimiter	none
MAC-filtering	none
Dead-time (0-1440) in minutes	
Group Type	Radius

Servers In This Group

Available Servers	Assigned Servers
ACS ISE	Microsoft_NPS

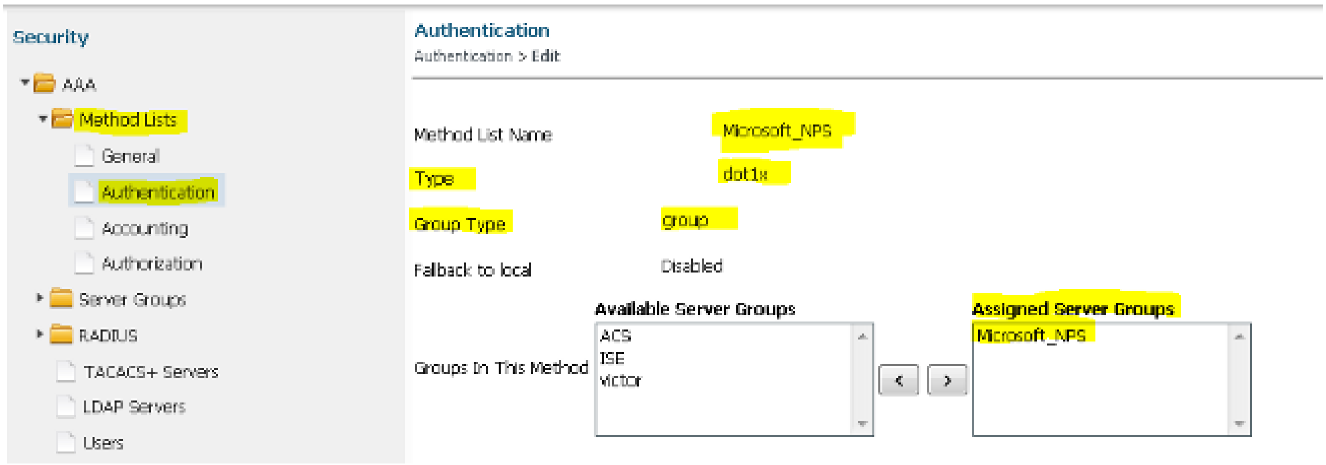
The Server Group should appear similar to this after the configuration:



Radius Server Groups

	Name	Server1	Server2	Server3
□	ACS	ACS	N/A	N/A
□	ISE	ISE	N/A	N/A
□	Microsoft_NPS	Microsoft_NPS	N/A	N/A

5. Select **dot1x** for the Authentication Method List Type and **Group** for the Group Type. Then, map the Server Group that you configured in the previous step:



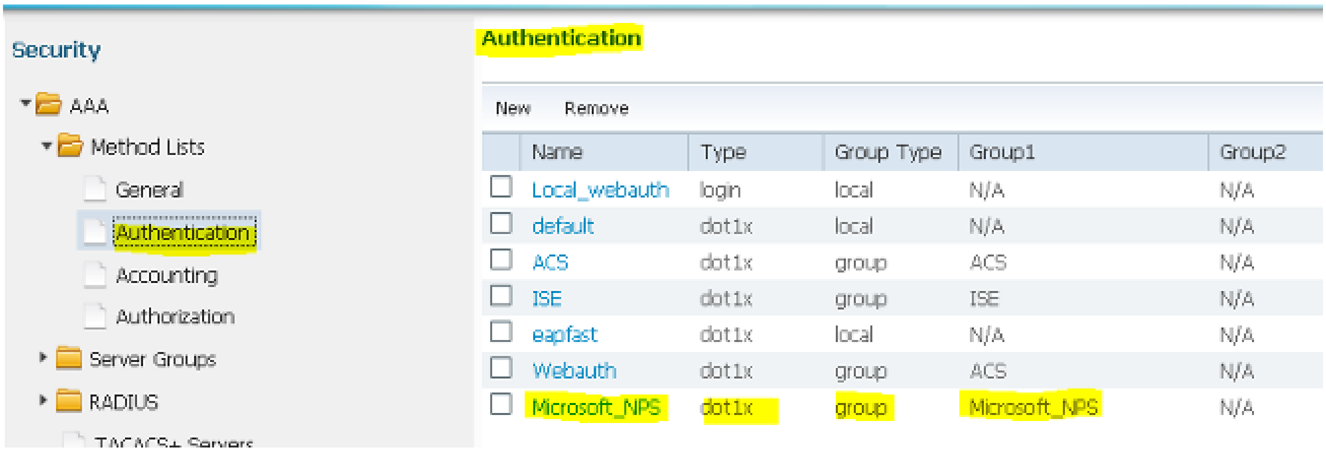
Authentication
Authentication > Edit

Method List Name	Microsoft_NPS
Type	dot1x
Group Type	group
Fallback to local	Disabled

Groups In This Method

Available Server Groups	Assigned Server Groups
ACS ISE victor	Microsoft_NPS

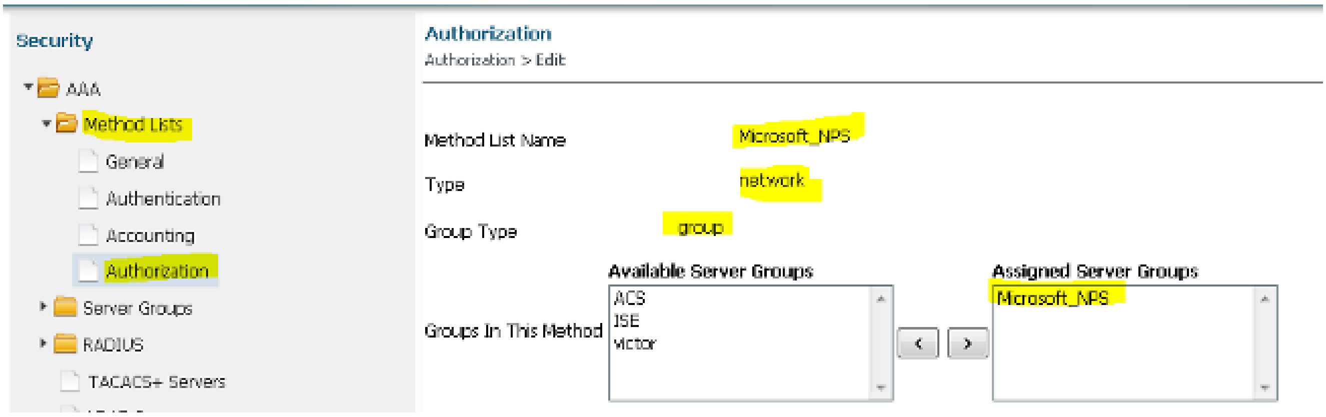
The Authentication Method List should appear similar to this after the configuration:



Authentication

	Name	Type	Group Type	Group1	Group2
□	Local_webauth	login	local	N/A	N/A
□	default	dot1x	local	N/A	N/A
□	ACS	dot1x	group	ACS	N/A
□	ISE	dot1x	group	ISE	N/A
□	eapfast	dot1x	local	N/A	N/A
□	Webauth	dot1x	group	ACS	N/A
□	Microsoft_NPS	dot1x	group	Microsoft_NPS	N/A

6. Select **Network** for the Authorization Method List Type and **Group** for the Group Type. Then, map the Server Group that you configured in the previous step:



Authorization

Authorization > Edit

Method List Name: Microsoft_NPS

Type: network

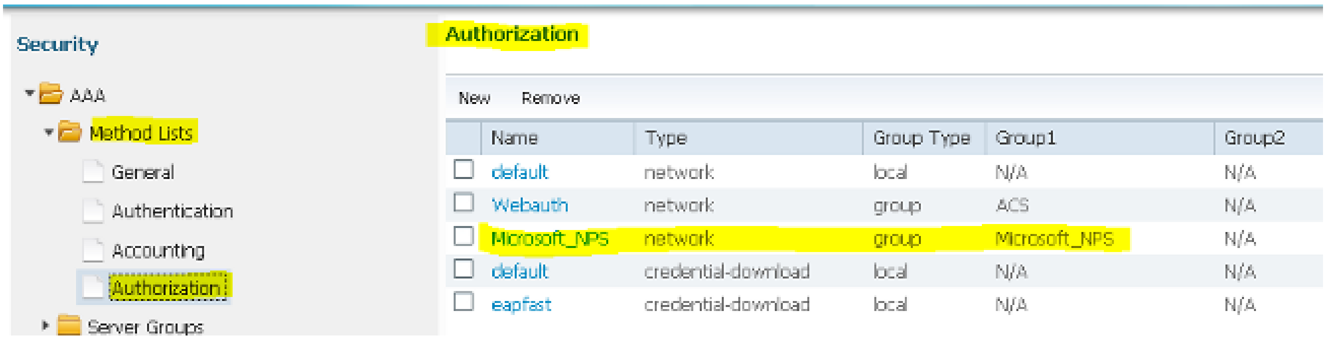
Group Type: group

Groups In This Method

Available Server Groups: ACS, ISE, Victor

Assigned Server Groups: Microsoft_NPS

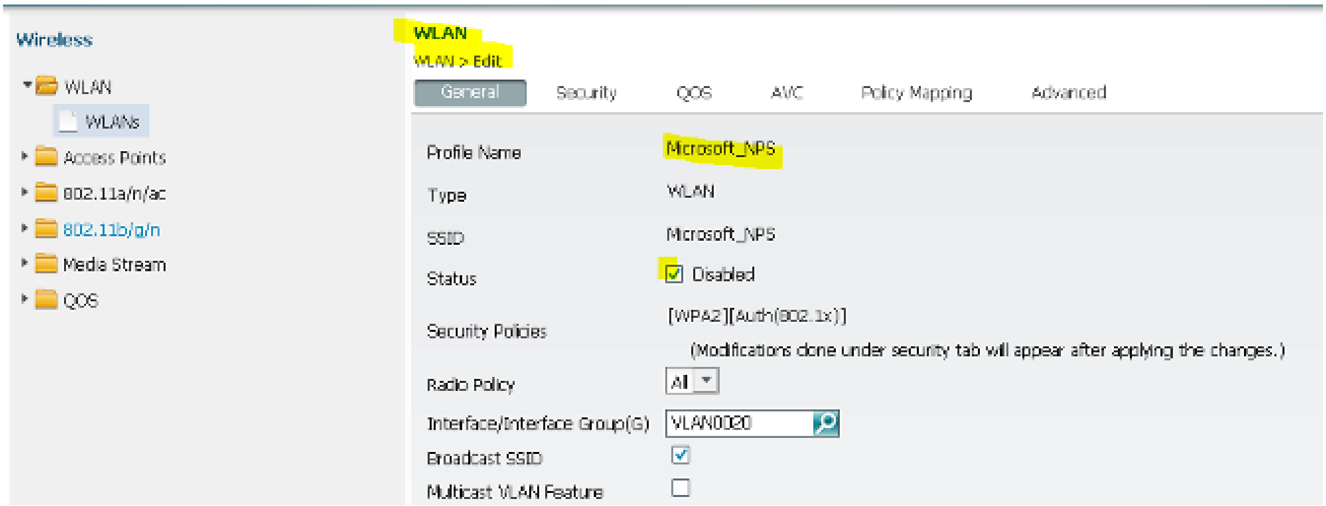
The Authorization Method List should appear similar to this after the configuration:



Authorization

	Name	Type	Group Type	Group1	Group2
□	default	network	local	N/A	N/A
□	Webauth	network	group	ACS	N/A
□	Microsoft_NPS	network	group	Microsoft_NPS	N/A
□	default	credential-download	local	N/A	N/A
□	eapfast	credential-download	local	N/A	N/A

7. Navigate to **Configure > Wireless** and click the **WLAN** tab. Configure a new WLAN to which users can connect and become authenticated through the Microsoft NPS server with EAP authentication:



WLAN

WLAN > Edit

Profile Name: Microsoft_NPS

Type: WLAN

SSID: Microsoft_NPS

Status: ☑ Disabled

Security Policies: [WPA2][Auth(802.1x)]

(Modifications done under security tab will appear after applying the changes.)

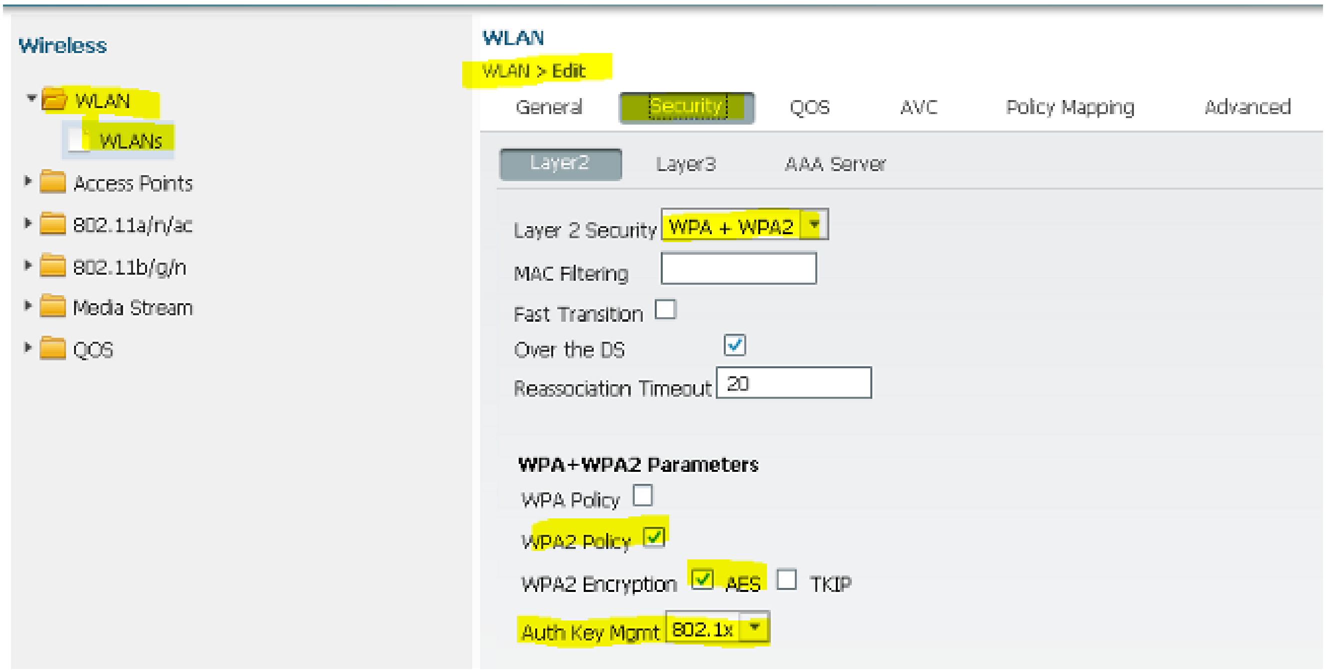
Radio Policy: All

Interface/Interface Group(G): VLAN0020

Broadcast SSID: ☑

Multicast VLAN Feature: □

The Security L2 tab should appear similar to this after the configuration:



Layer 2 Security WPA + WPA2

MAC Filtering

Fast Transition □

Over the DS ☑

Reassociation Timeout 20

WPA+WPA2 Parameters

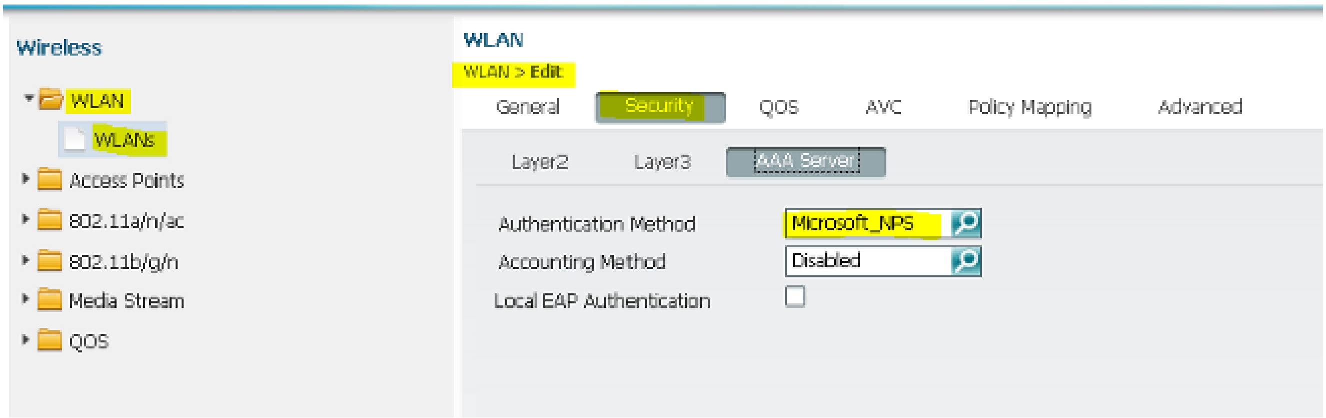
WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

Auth Key Mgmt 802.1x

8. Map the Method List that you configured in the previous steps. This helps authenticate the client to the correct server.



Authentication Method Microsoft_NPS

Accounting Method Disabled

Local EAP Authentication □

Configuration on the Microsoft Windows Version 2008 Server

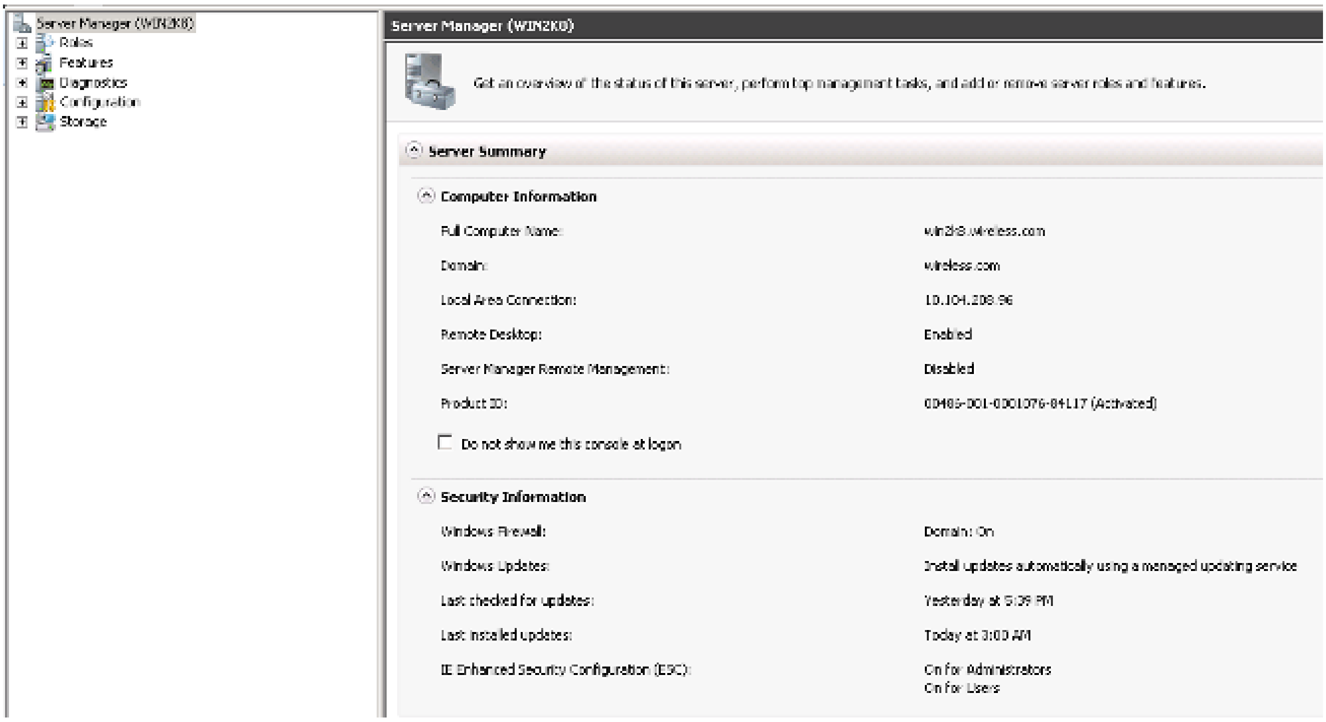
This section describes a complete configuration of the Microsoft Windows Version 2008 server. The configuration is completed in six steps:

1. Configure the server as a domain controller.
2. Install and configure the server as a CA server.
3. Install the NPS.
4. Install a certificate.
5. Configure the NPS for PEAP authentication.
6. Add users to the AD.

Configure the Microsoft Windows 2008 Server as a Domain Controller

Complete these steps in order to configure the Microsoft Windows Version 2008 server as a domain controller:

1. Navigate to **Start** > **Server Manager > Roles** > **Add Roles**.



Server Manager (WIN2K8)

Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Server Summary

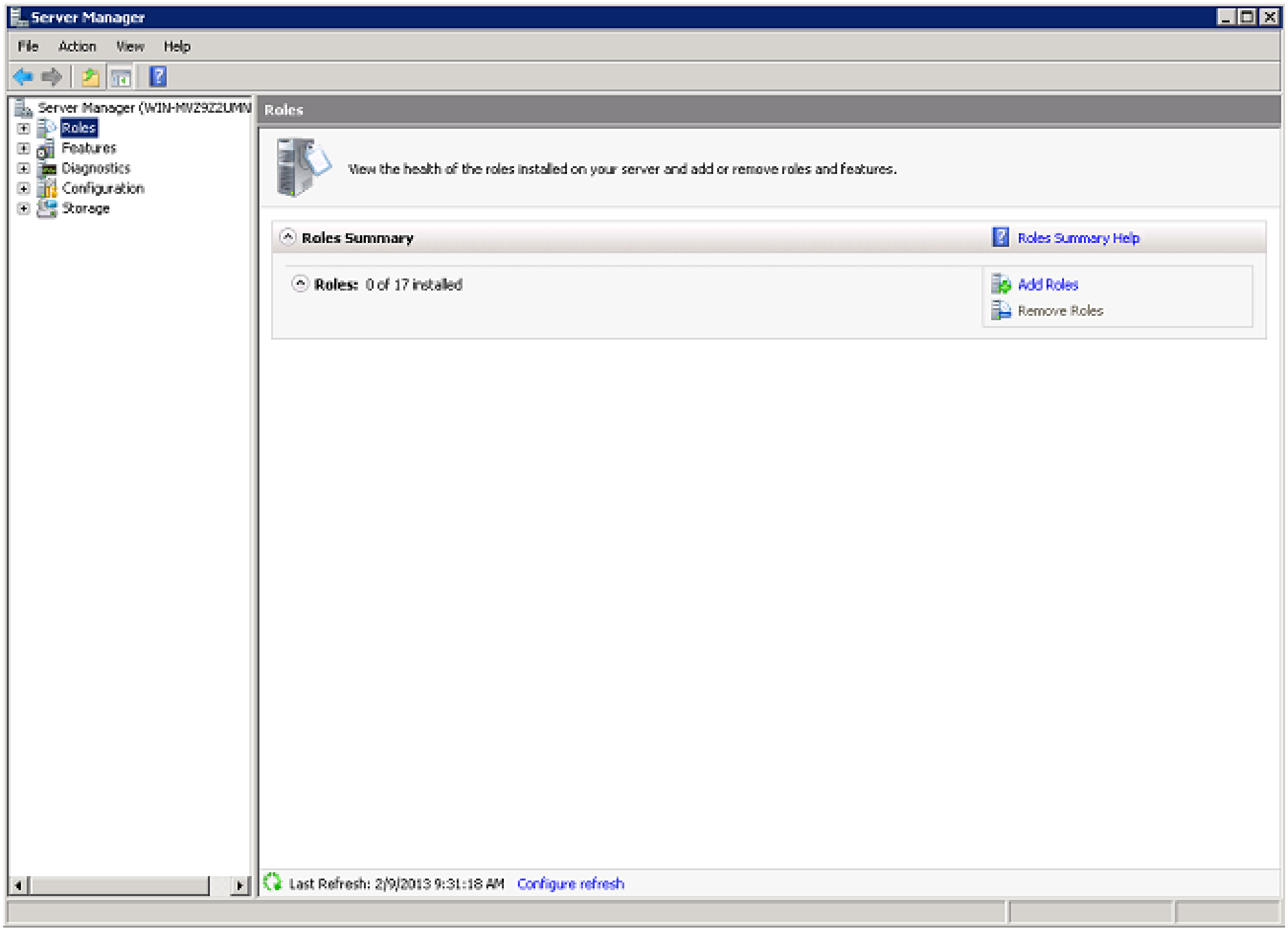
Computer Information

Full Computer Name:	win2k8.wireless.com
Domain:	wireless.com
Local Area Connection:	10.104.208.96
Remote Desktop:	Enabled
Server Manager Remote Management:	Disabled
Product ID:	00486-001-0001076-84117 (Activated)

□ Do not show me this console at logon

Security Information

Windows Firewall:	Domain: On
Windows Updates:	Install updates automatically using a managed updating service
Last checked for updates:	Yesterday at 5:39 PM
Last installed updates:	Today at 3:00 AM
IE Enhanced Security Configuration (ESC):	On for Administrators On for Users



Roles

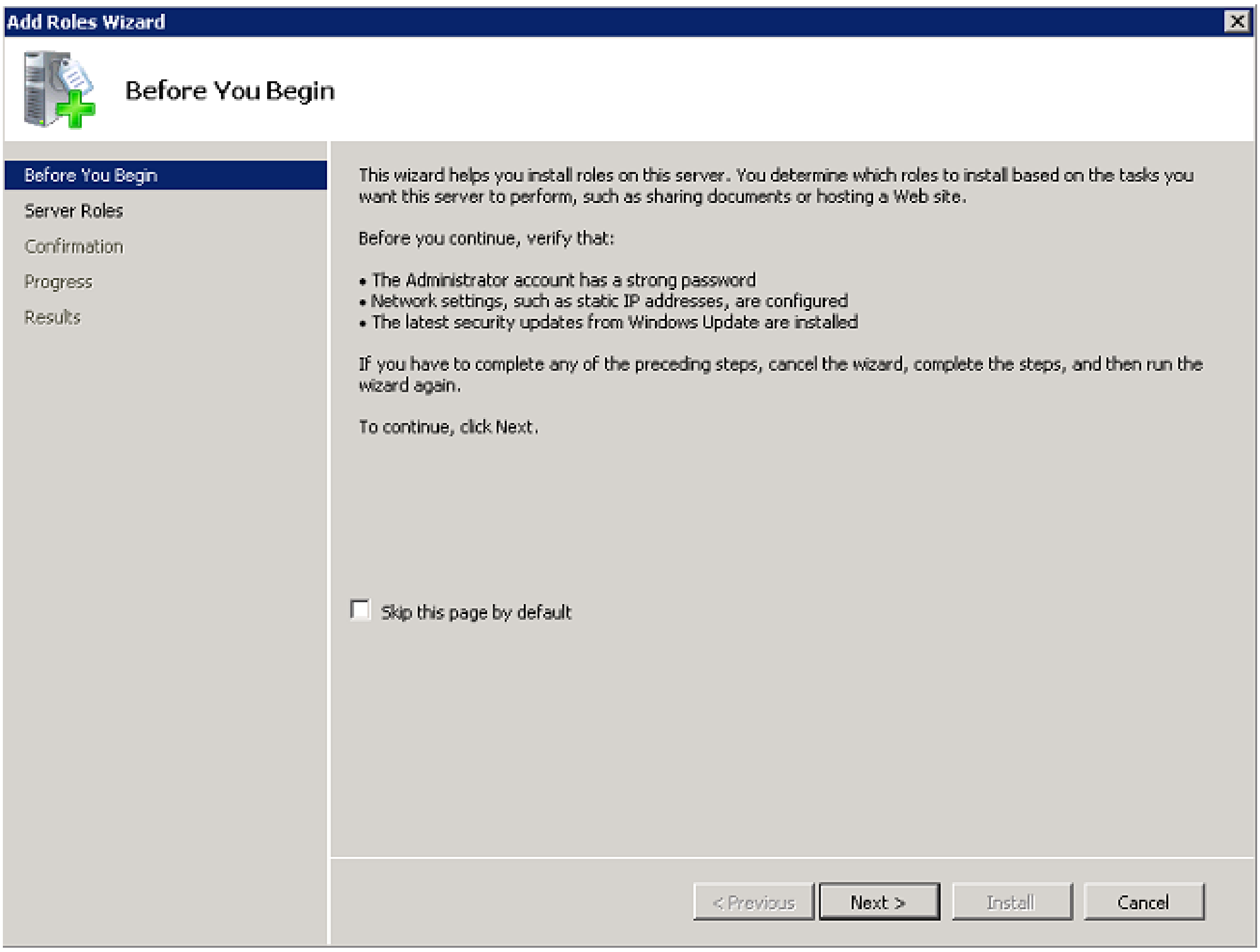
View the health of the roles installed on your server and add or remove roles and features.

Roles Summary

Roles: 0 of 17 installed

Last Refresh: 2/9/2013 9:31:18 AM

2. Click **Next**.



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

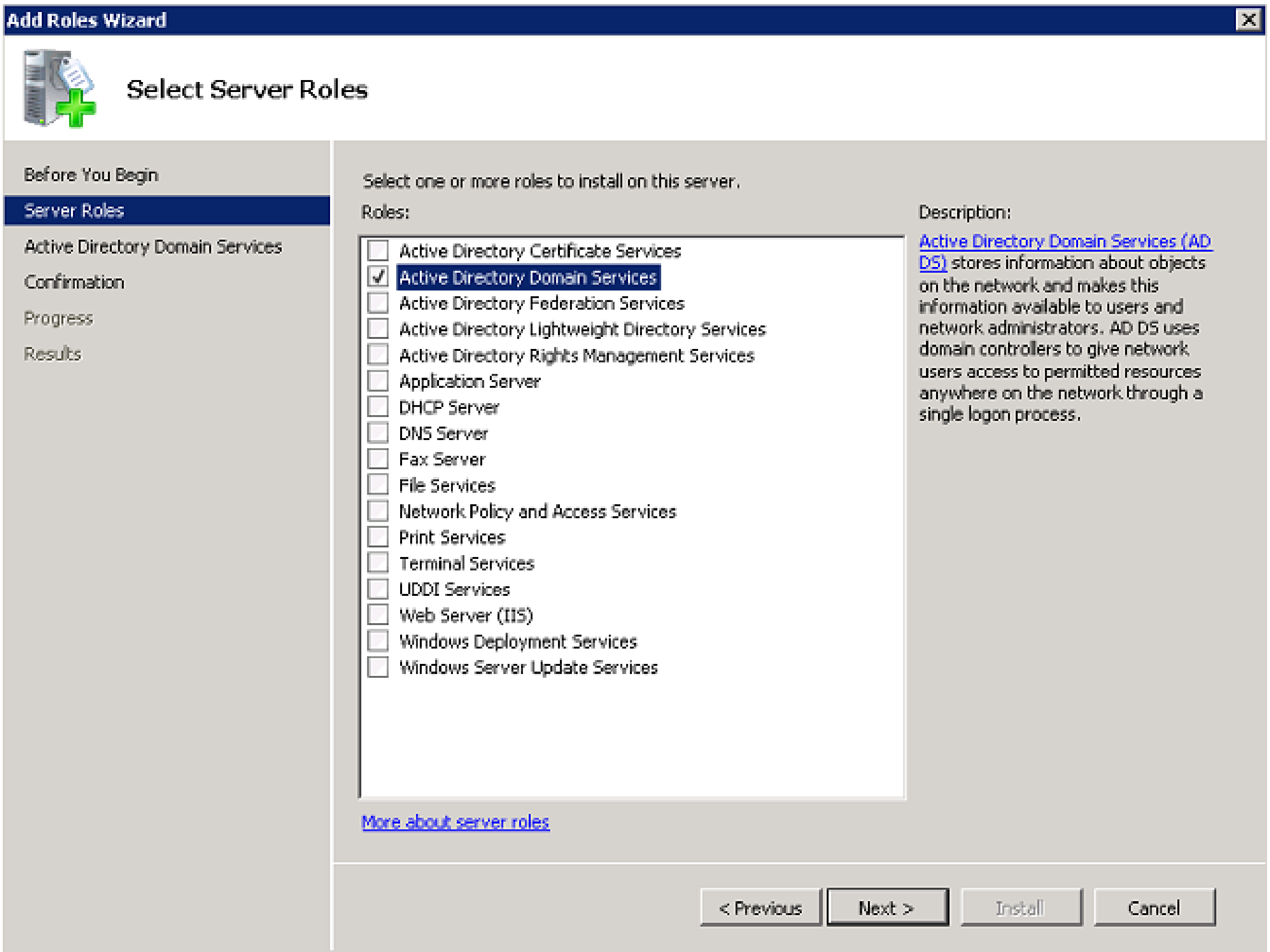
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

3. Check the **Active Directory Domain Services** check box and click **Next**.



Add Roles Wizard

Select Server Roles

- Before You Begin
- Server Roles
- Active Directory Domain Services
- Confirmation
- Progress
- Results

Select one or more roles to install on this server.

Roles:

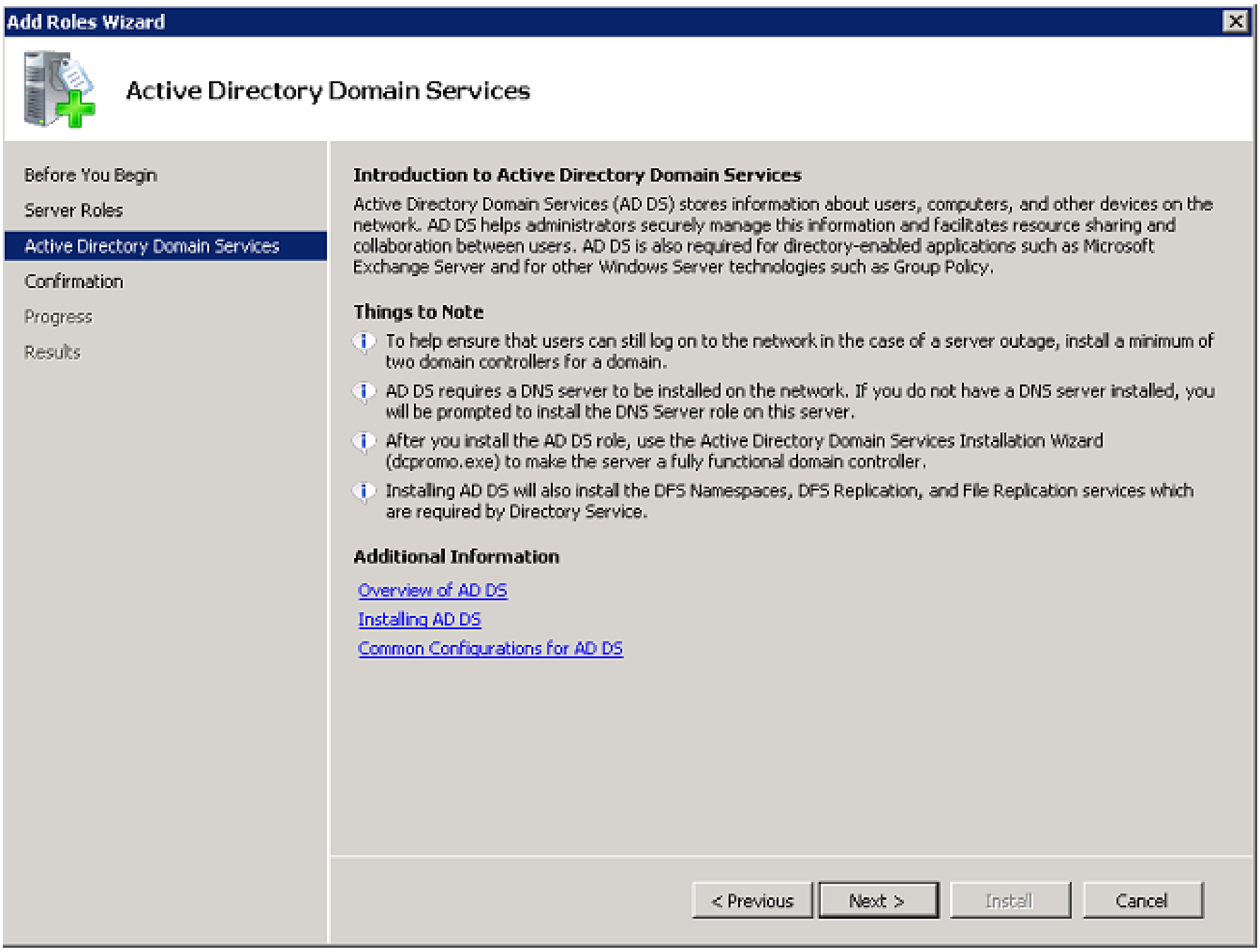
- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Network Policy and Access Services
- □ Print Services
- □ Terminal Services
- □ UDDI Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

More about server roles

4. Review the **Introduction to Active Directory Domain Services** and click **Next**.



Active Directory Domain Services

Introduction to Active Directory Domain Services

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.

Things to Note

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this server.
- After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.
- Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by Directory Service.

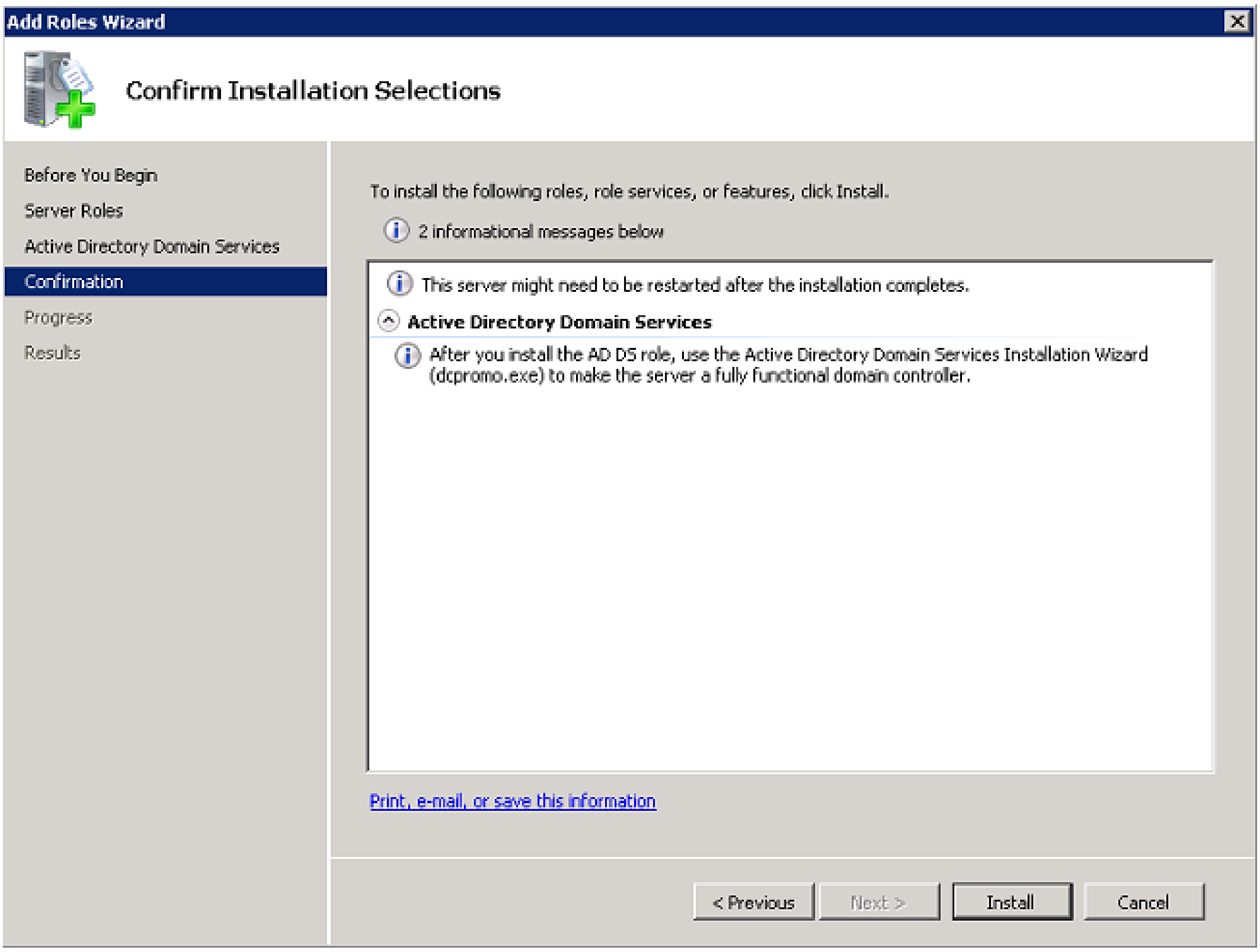
Additional Information

Overview of AD DS

Installing AD DS

Common Configurations for AD DS

5. Click **Install** in order to begin the installation process.



To install the following roles, role services, or features, click Install.

2 informational messages below

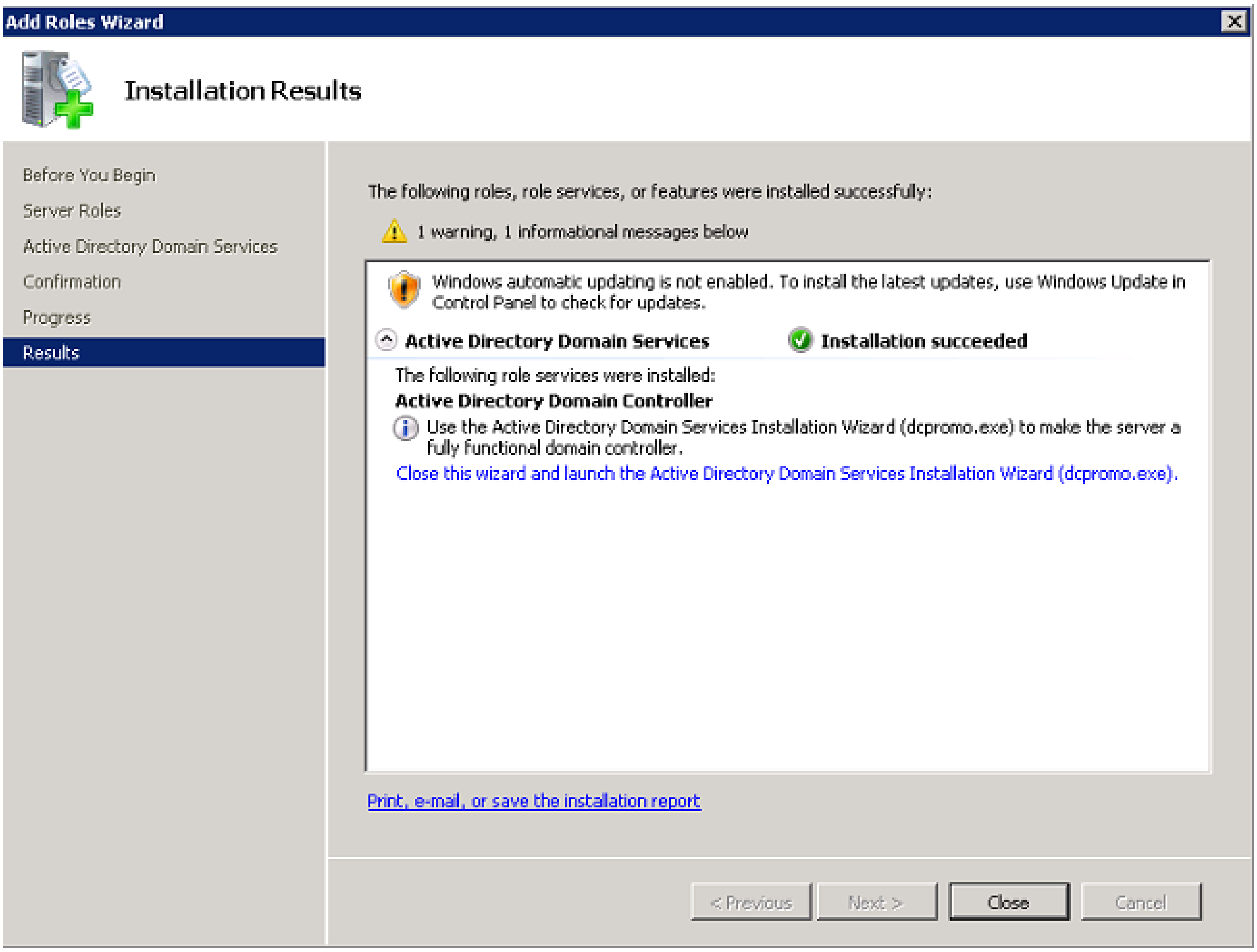
This server might need to be restarted after the installation completes.

Active Directory Domain Services

After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.

The installation proceeds and completes.

6. Click **Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe)** in order to continue the installation and configuration of the AD.



The following roles, role services, or features were installed successfully:

⚠ 1 warning, 1 informational messages below

Windows automatic updating is not enabled. To install the latest updates, use Windows Update in Control Panel to check for updates.

Active Directory Domain Services ✓ Installation succeeded

The following role services were installed:

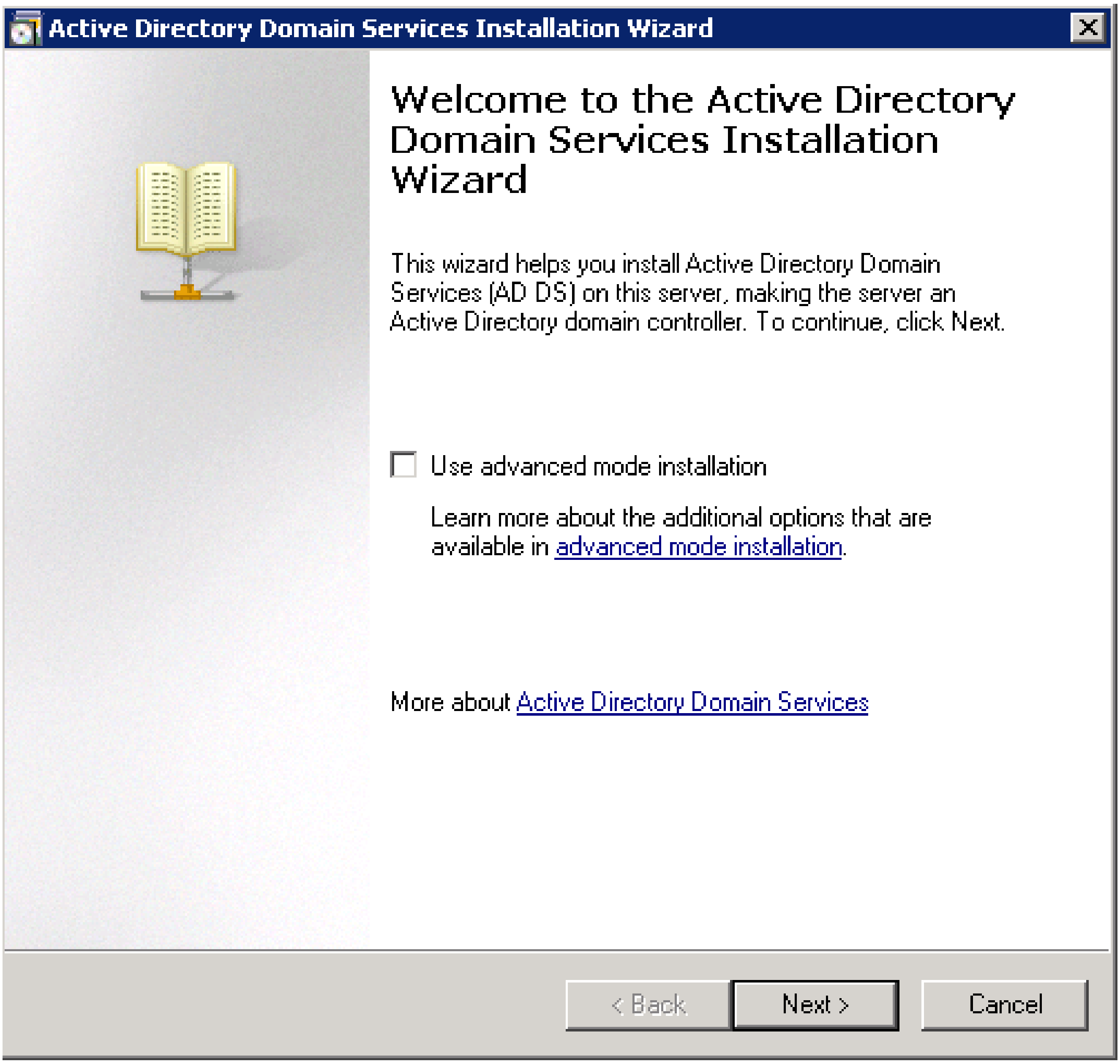
Active Directory Domain Controller

ⓘ Use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.

Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).

Print, e-mail, or save the installation report

7. Click **Next** in order to run the **Active Directory Domain Services Installation Wizard**.



Welcome to the Active Directory Domain Services Installation Wizard

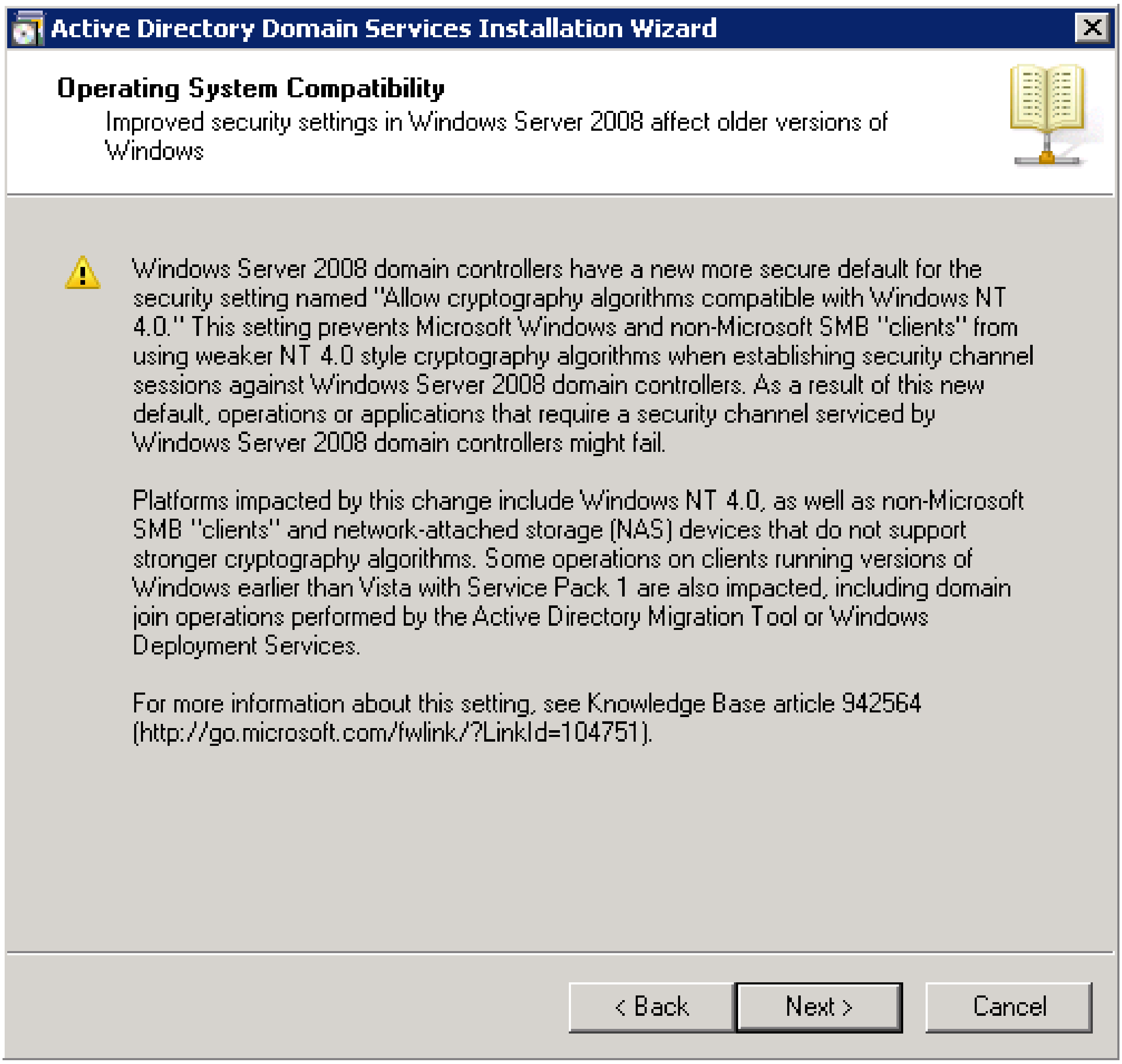
This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next.

☐ Use advanced mode installation

Learn more about the additional options that are available in advanced mode installation.

More about Active Directory Domain Services

8. Review the information about **Operating System Compatibility** and click **Next**.



Active Directory Domain Services Installation Wizard

Operating System Compatibility

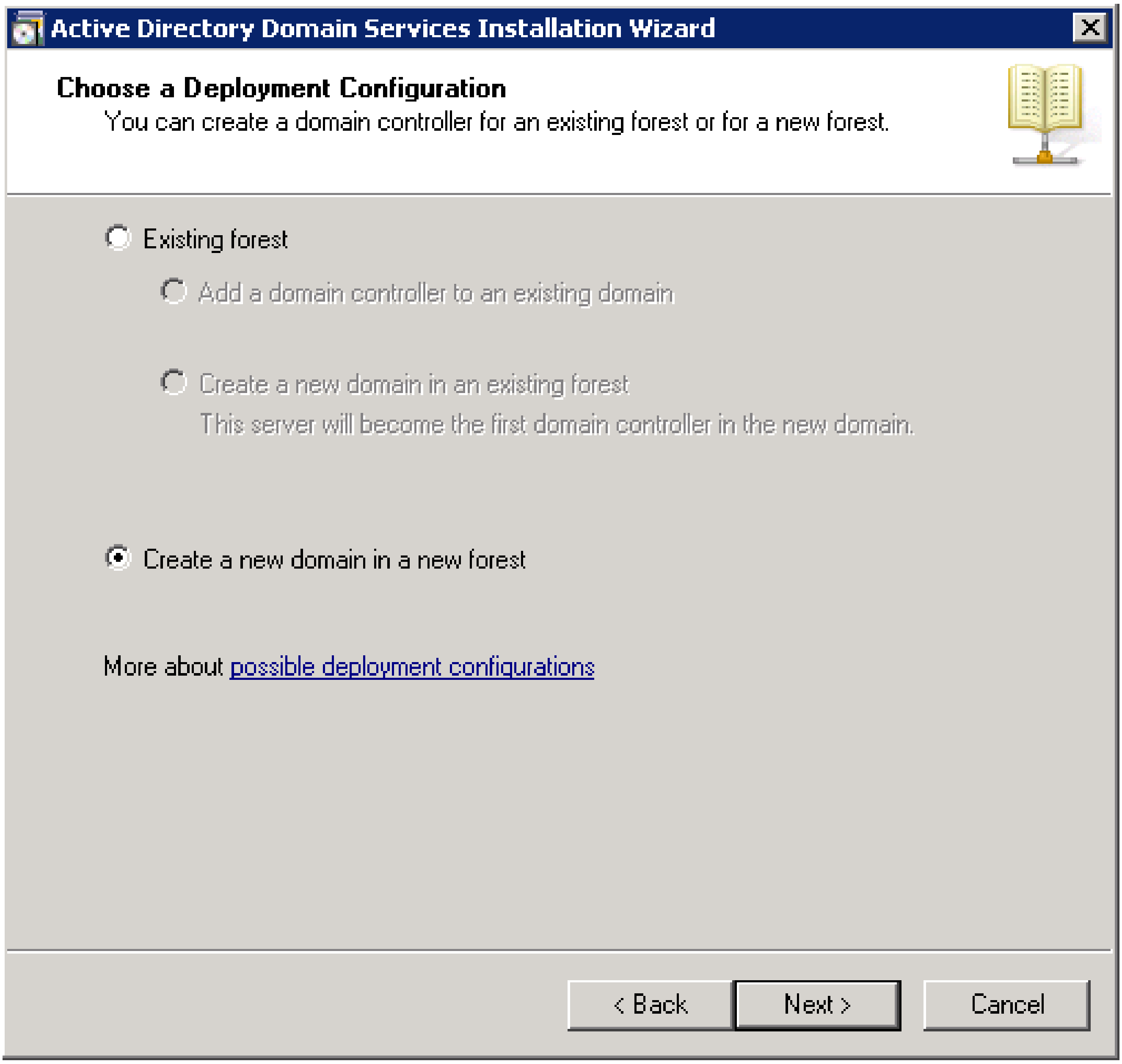
Improved security settings in Windows Server 2008 affect older versions of Windows

Windows Server 2008 domain controllers have a new more secure default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0." This setting prevents Microsoft Windows and non-Microsoft SMB "clients" from using weaker NT 4.0 style cryptography algorithms when establishing security channel sessions against Windows Server 2008 domain controllers. As a result of this new default, operations or applications that require a security channel serviced by Windows Server 2008 domain controllers might fail.

Platforms impacted by this change include Windows NT 4.0, as well as non-Microsoft SMB "clients" and network-attached storage (NAS) devices that do not support stronger cryptography algorithms. Some operations on clients running versions of Windows earlier than Vista with Service Pack 1 are also impacted, including domain join operations performed by the Active Directory Migration Tool or Windows Deployment Services.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

9. Click the **Create a new domain in a new forest** radio button and click **Next** in order to create a new domain.



Active Directory Domain Services Installation Wizard

Choose a Deployment Configuration

You can create a domain controller for an existing forest or for a new forest.

○ Existing forest

○ Add a domain controller to an existing domain

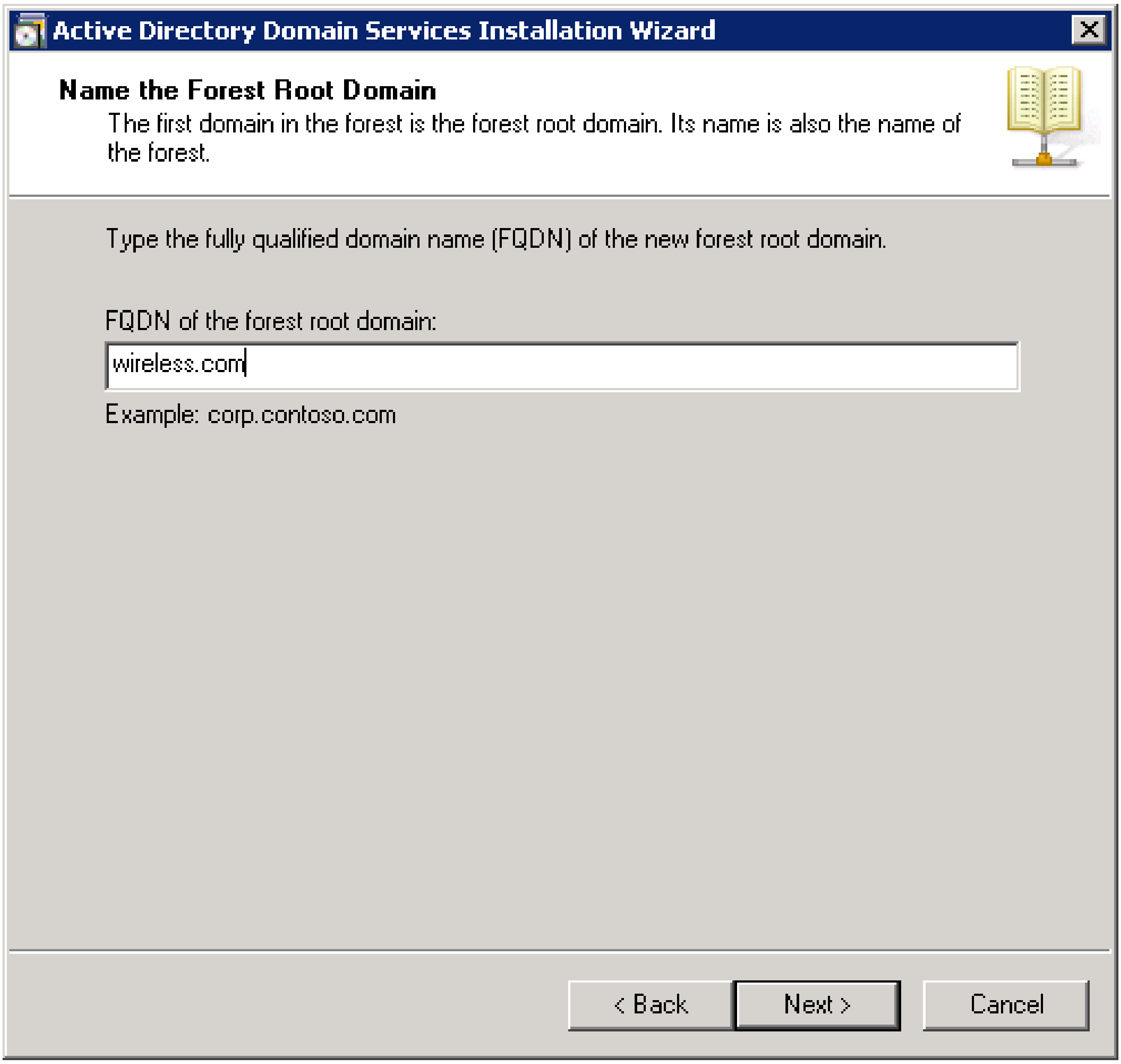
○ Create a new domain in an existing forest

This server will become the first domain controller in the new domain.

● Create a new domain in a new forest

More about possible deployment configurations

10. Enter the full DNS name for the new domain (**wireless.com** in this example) and click **Next**.



Active Directory Domain Services Installation Wizard

Name the Forest Root Domain

The first domain in the forest is the forest root domain. Its name is also the name of the forest.

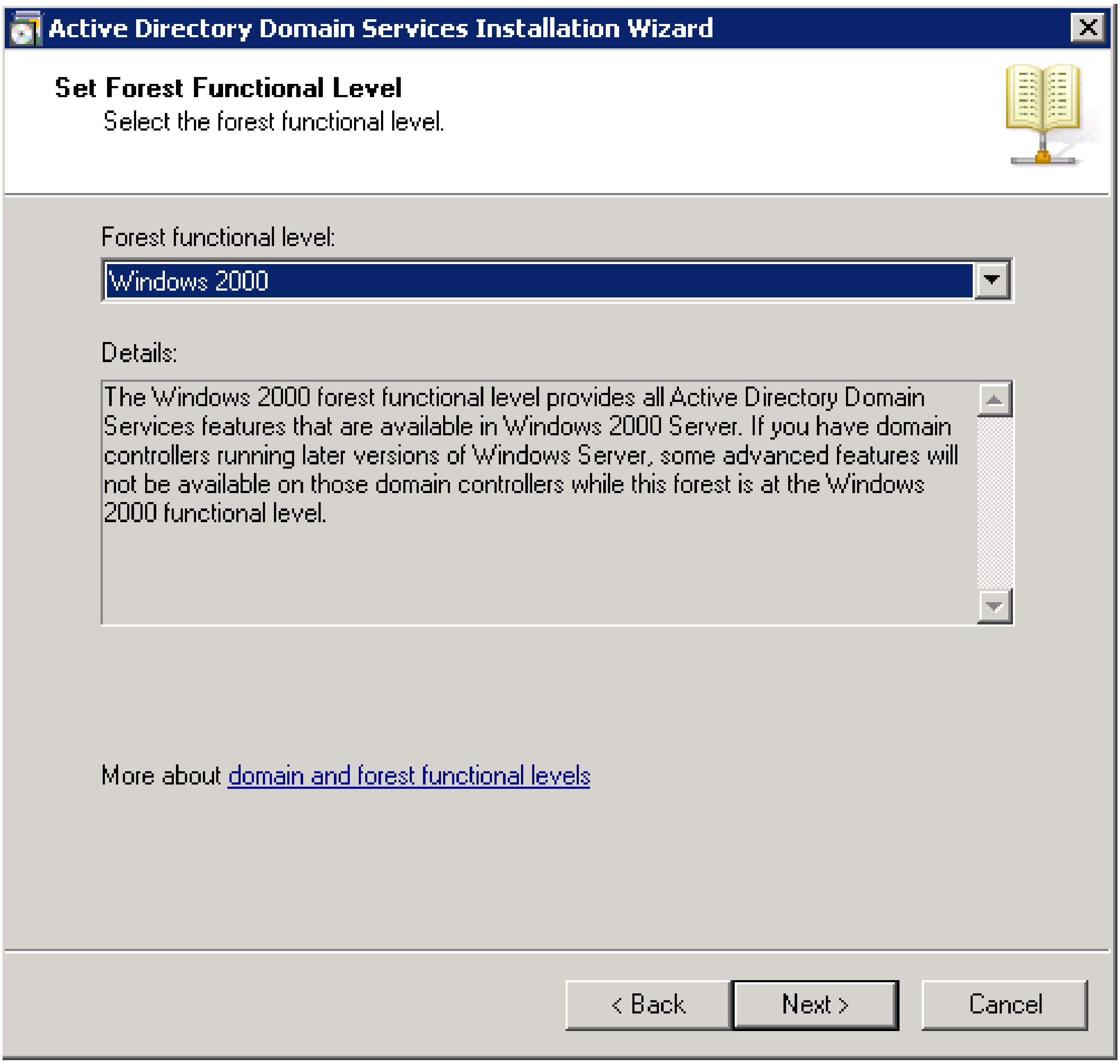
Type the fully qualified domain name (FQDN) of the new forest root domain.

FQDN of the forest root domain:

wireless.com

Example: corp.contoso.com

11. Select the **Forest functional level** for your domain and click **Next**.



Set Forest Functional Level

Select the forest functional level.

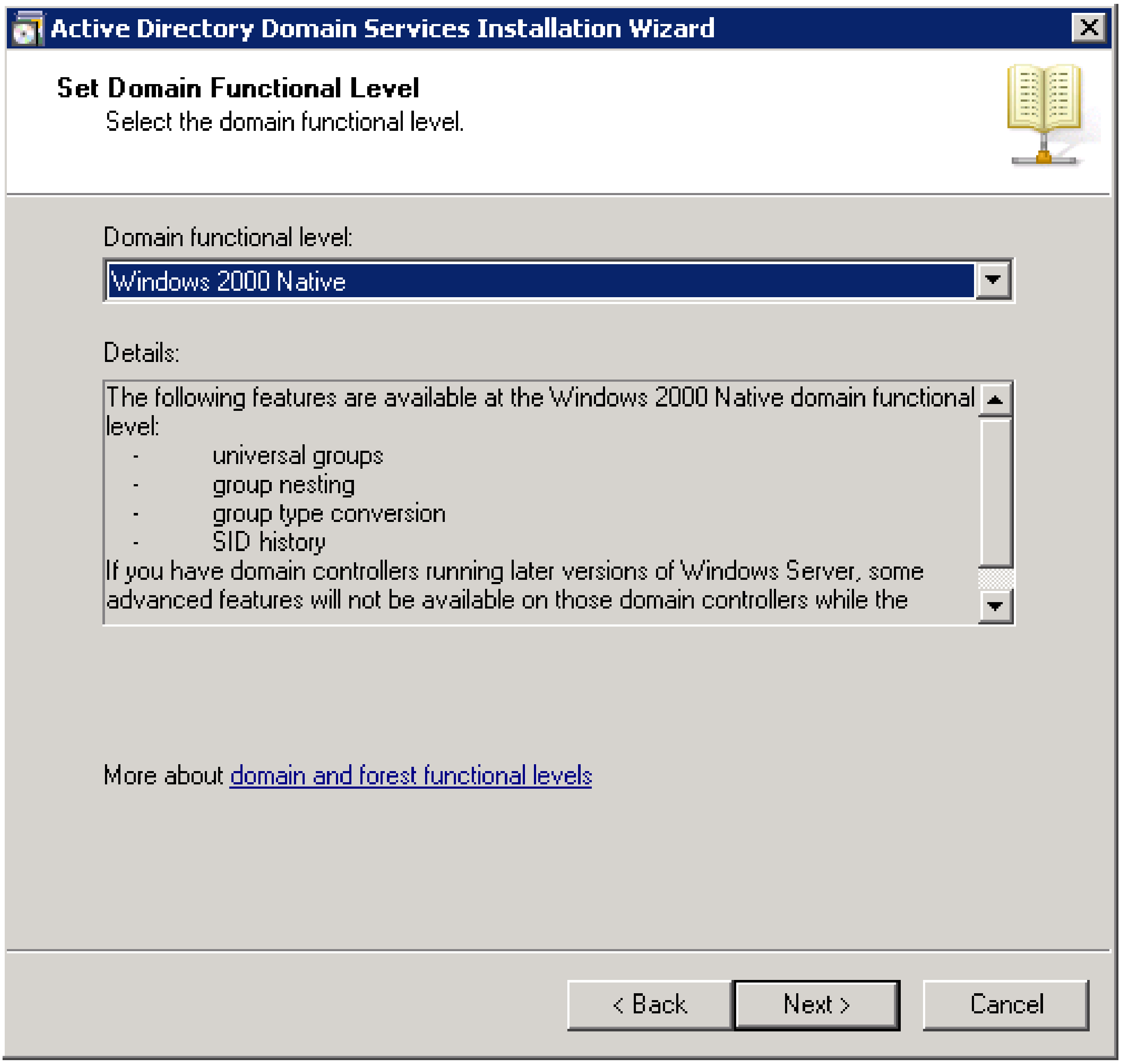
Forest functional level: Windows 2000

Details:

The Windows 2000 forest functional level provides all Active Directory Domain Services features that are available in Windows 2000 Server. If you have domain controllers running later versions of Windows Server, some advanced features will not be available on those domain controllers while this forest is at the Windows 2000 functional level.

More about domain and forest functional levels

12. Select the **Domain functional level** for your domain and click **Next**.



Set Domain Functional Level

Select the domain functional level.

Domain functional level:

Windows 2000 Native

Details:

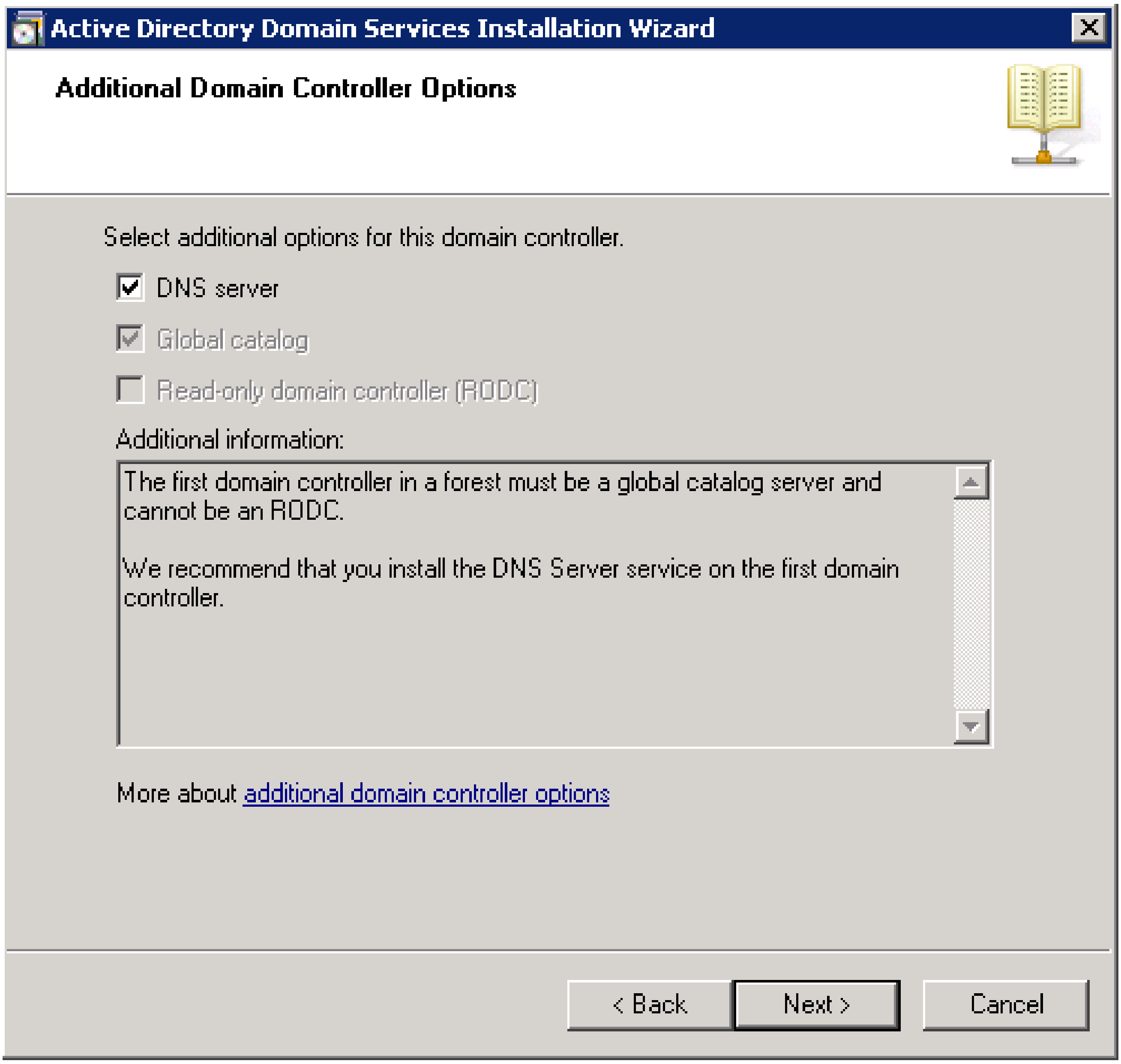
The following features are available at the Windows 2000 Native domain functional level:

- universal groups
- group nesting
- group type conversion
- SID history

If you have domain controllers running later versions of Windows Server, some advanced features will not be available on those domain controllers while the

More about domain and forest functional levels

13. Check the **DNS server** check box and click **Next**.



Additional Domain Controller Options

Select additional options for this domain controller.

☑ DNS server

☑ Global catalog

□ Read-only domain controller (RODC)

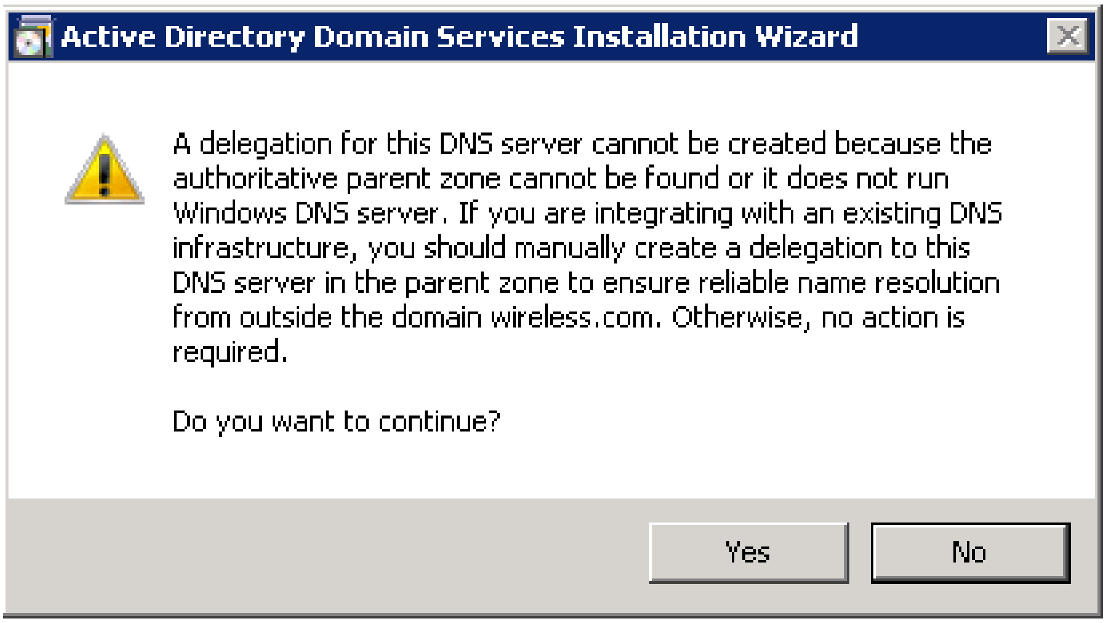
Additional information:

The first domain controller in a forest must be a global catalog server and cannot be an RODC.

We recommend that you install the DNS Server service on the first domain controller.

More about additional domain controller options

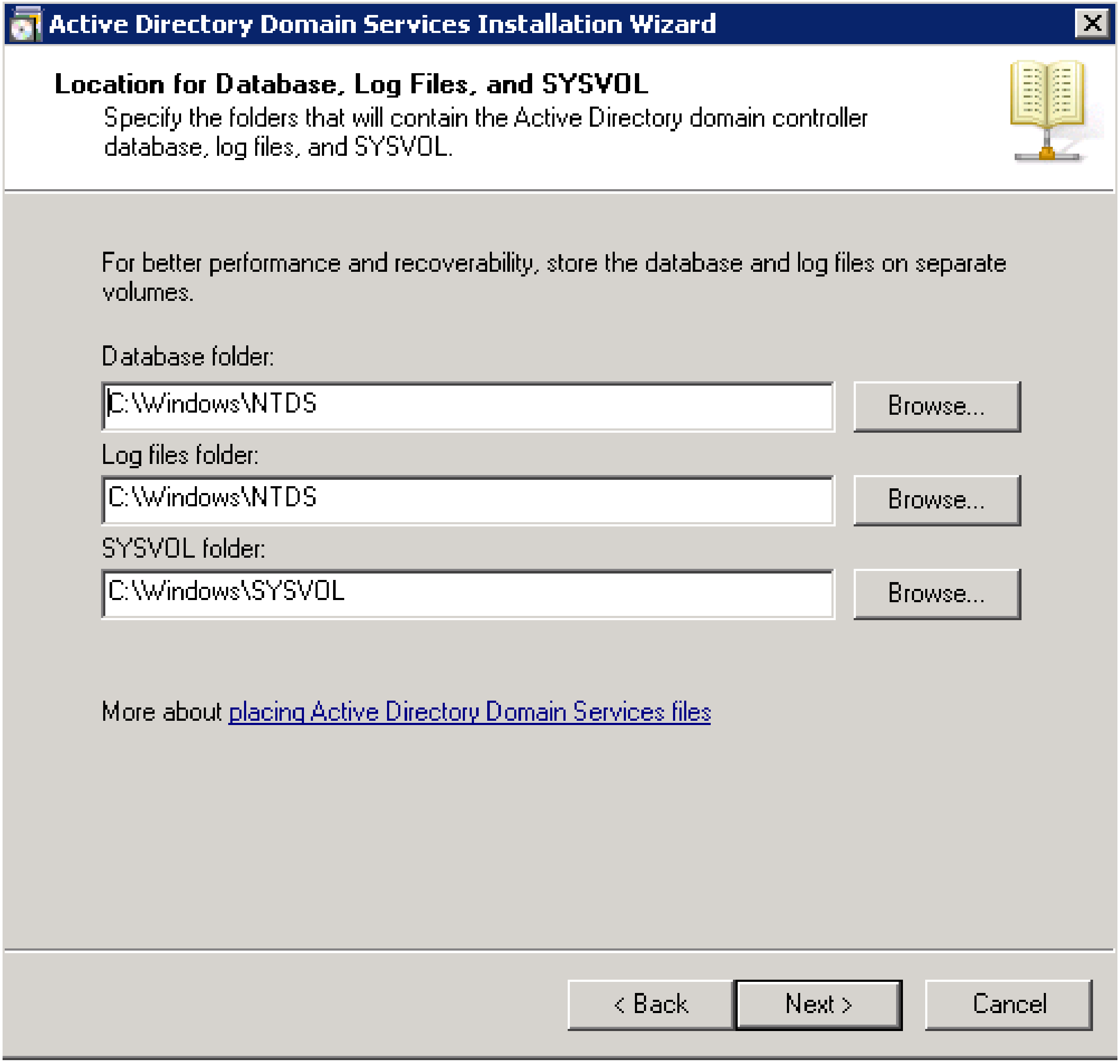
14. Click **Yes** when the **Active Directory Domain Services Installation Wizard** pop-up window appears in order to create a new zone in the DNS for the domain.



A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain wireless.com. Otherwise, no action is required.

Do you want to continue?

15. Select the folders that you want the AD to use for files and click **Next**.



Active Directory Domain Services Installation Wizard

Location for Database, Log Files, and SYSVOL

Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.

For better performance and recoverability, store the database and log files on separate volumes.

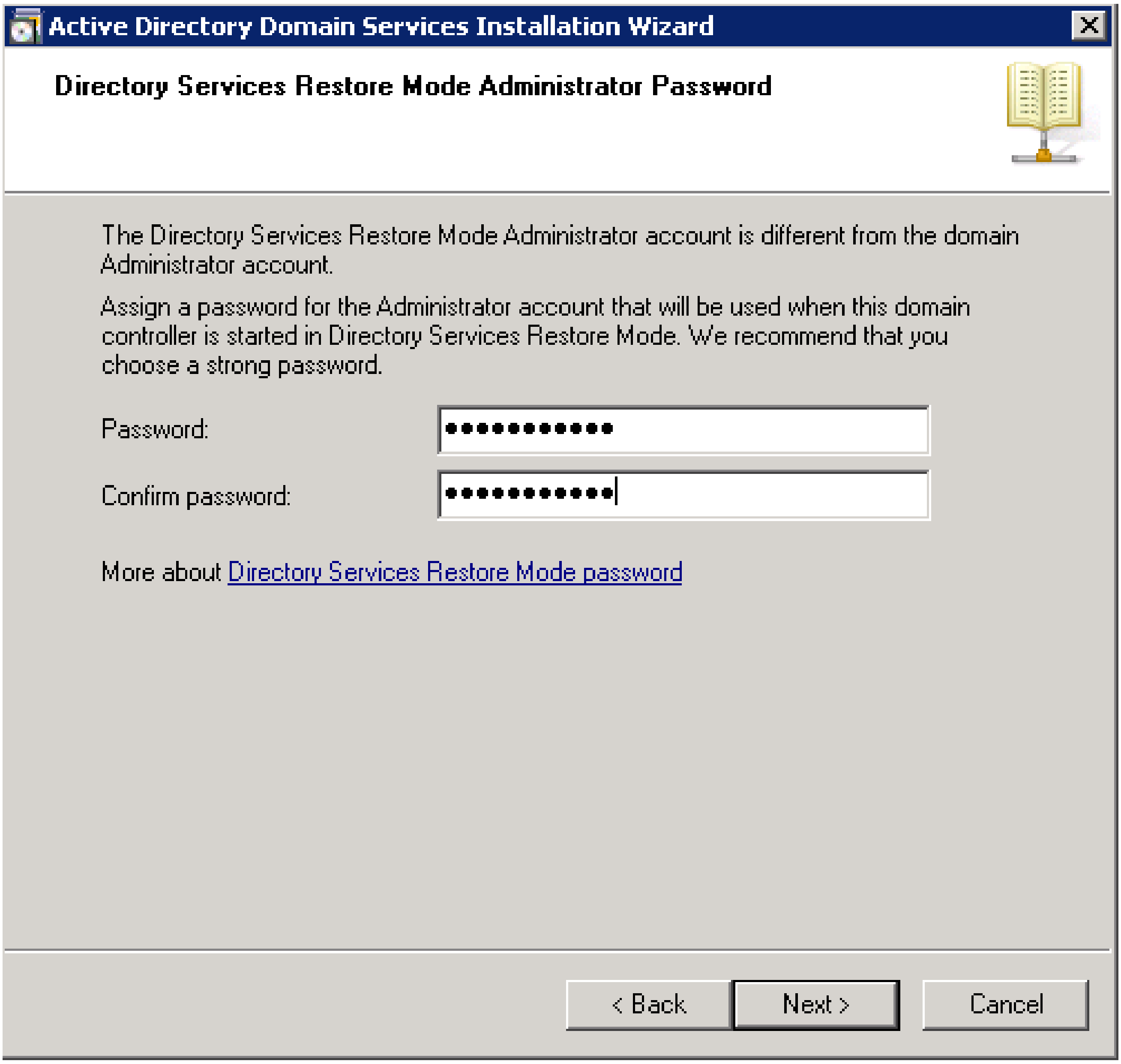
Database folder: C:\Windows\NTDS

Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

More about placing Active Directory Domain Services files

16. Enter the Administrator Password and click **Next**.



Directory Services Restore Mode Administrator Password

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

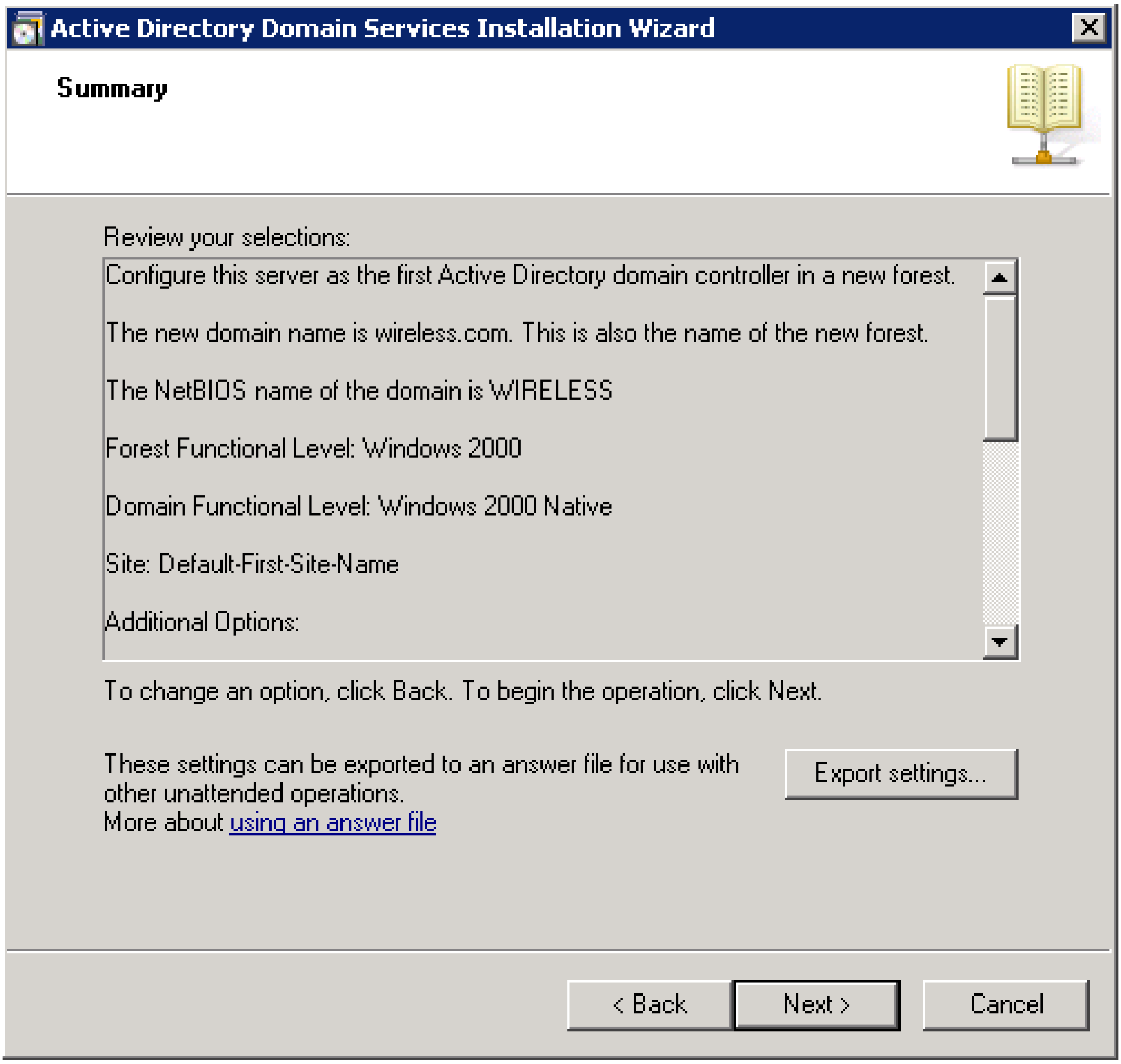
Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password: ●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●

More about Directory Services Restore Mode password

17. Review your selections and click **Next**.



Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is wireless.com. This is also the name of the new forest.

The NetBIOS name of the domain is WIRELESS

Forest Functional Level: Windows 2000

Domain Functional Level: Windows 2000 Native

Site: Default-First-Site-Name

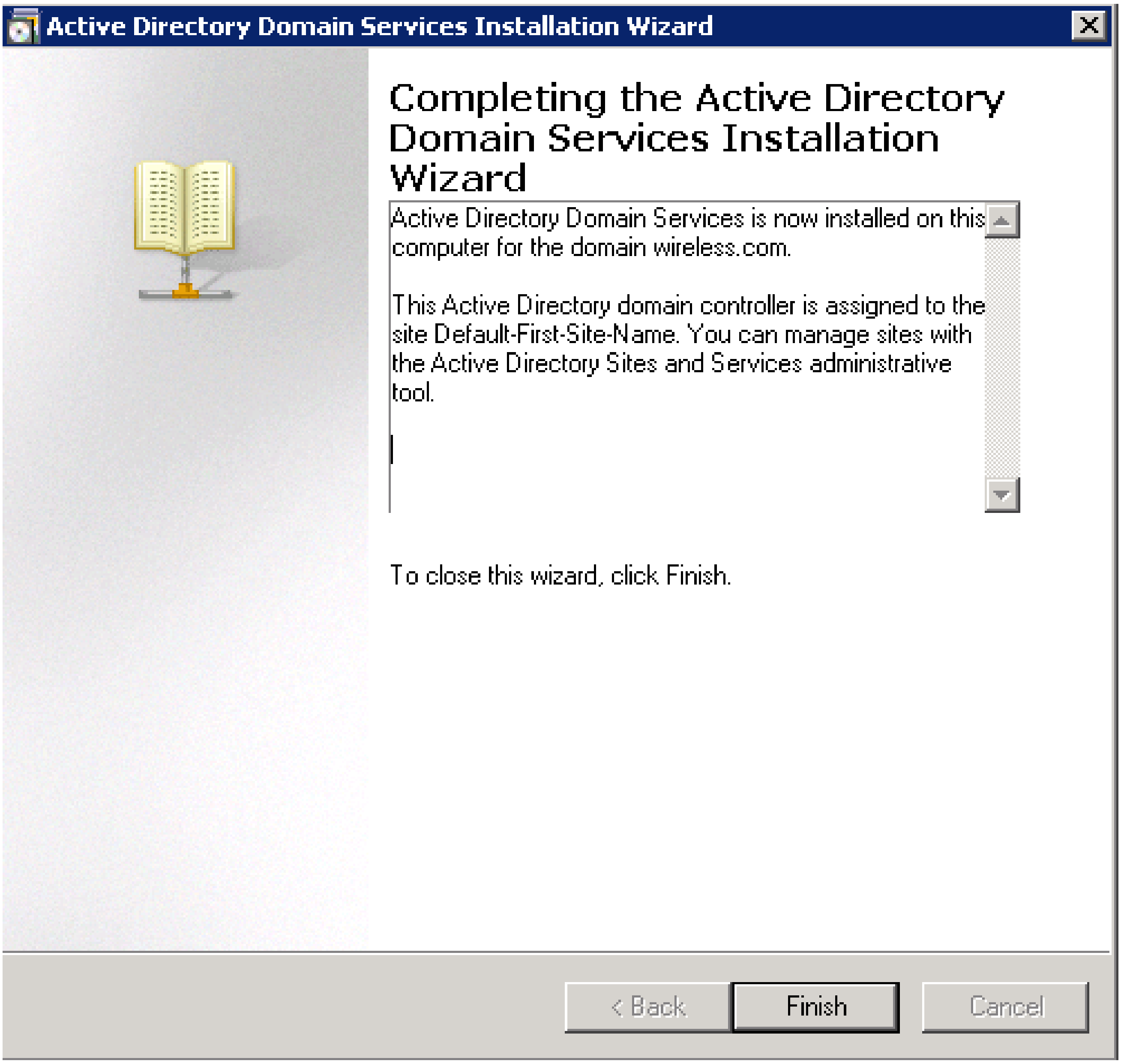
Additional Options:

To change an option, click Back. To begin the operation, click Next.

These settings can be exported to an answer file for use with other unattended operations.
More about using an answer file

The installation proceeds.

18. Click **Finish** in order to close the wizard.



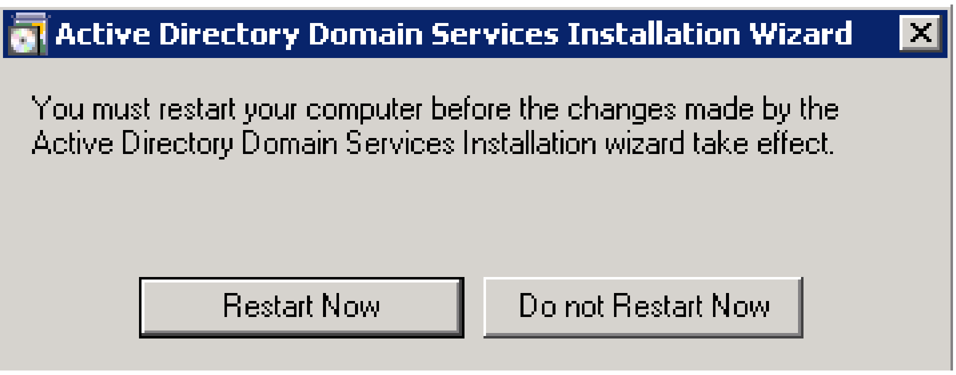
Completing the Active Directory Domain Services Installation Wizard

Active Directory Domain Services is now installed on this computer for the domain wireless.com.

This Active Directory domain controller is assigned to the site Default-First-Site-Name. You can manage sites with the Active Directory Sites and Services administrative tool.

To close this wizard, click Finish.

19. Restart the server in order for the changes to take effect.



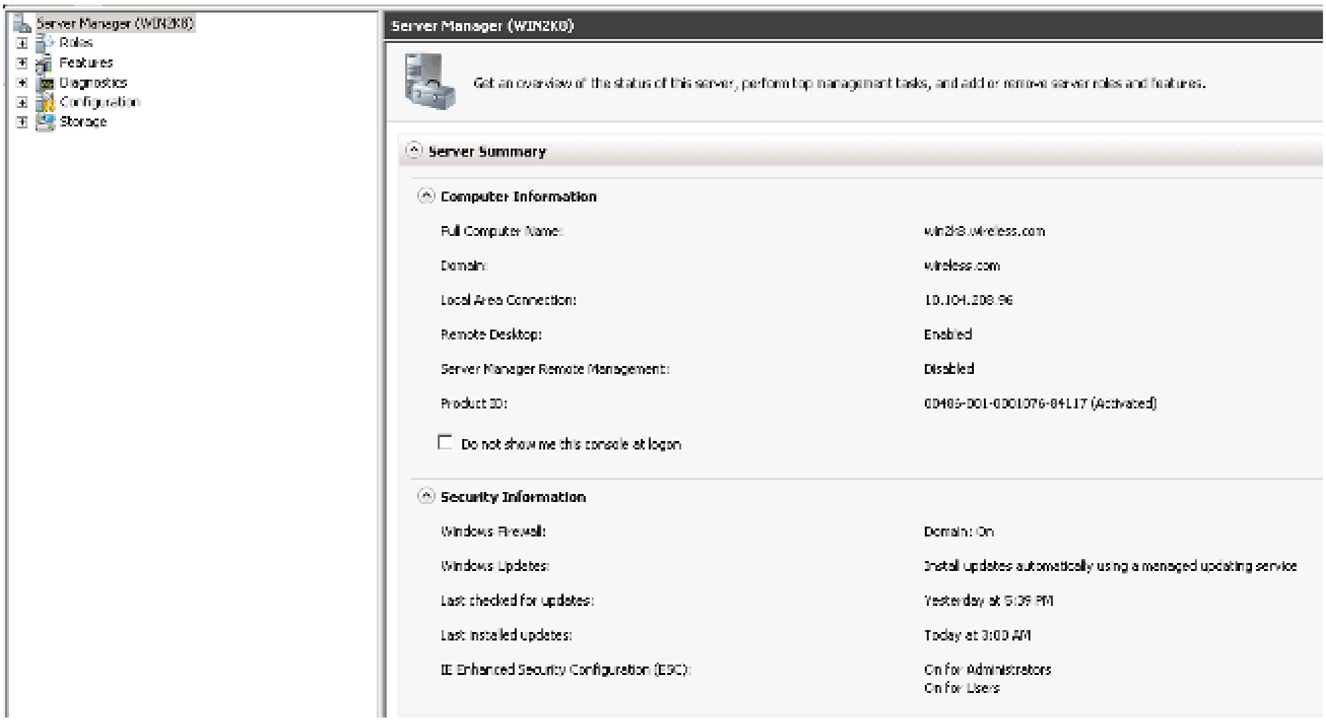
You must restart your computer before the changes made by the Active Directory Domain Services Installation wizard take effect.

Install and Configure the Microsoft Windows Version 2008 Server as a CA Server

PEAP with EAP-MS-CHAP v2 validates the RADIUS server based upon the certificate that is present on the server. Additionally, the server certificate must be issued by a public CA that is trusted by the client computer. That is, the public CA certificate already exists in the Trusted Root Certification Authority folder on the client computer certificate store.

Complete these steps in order to configure the Microsoft Windows Version 2008 server as a CA server that issues the certificate to the NPS:

1. Navigate to **Start** > **Server Manager > Roles** > **Add Roles**.



Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Server Summary

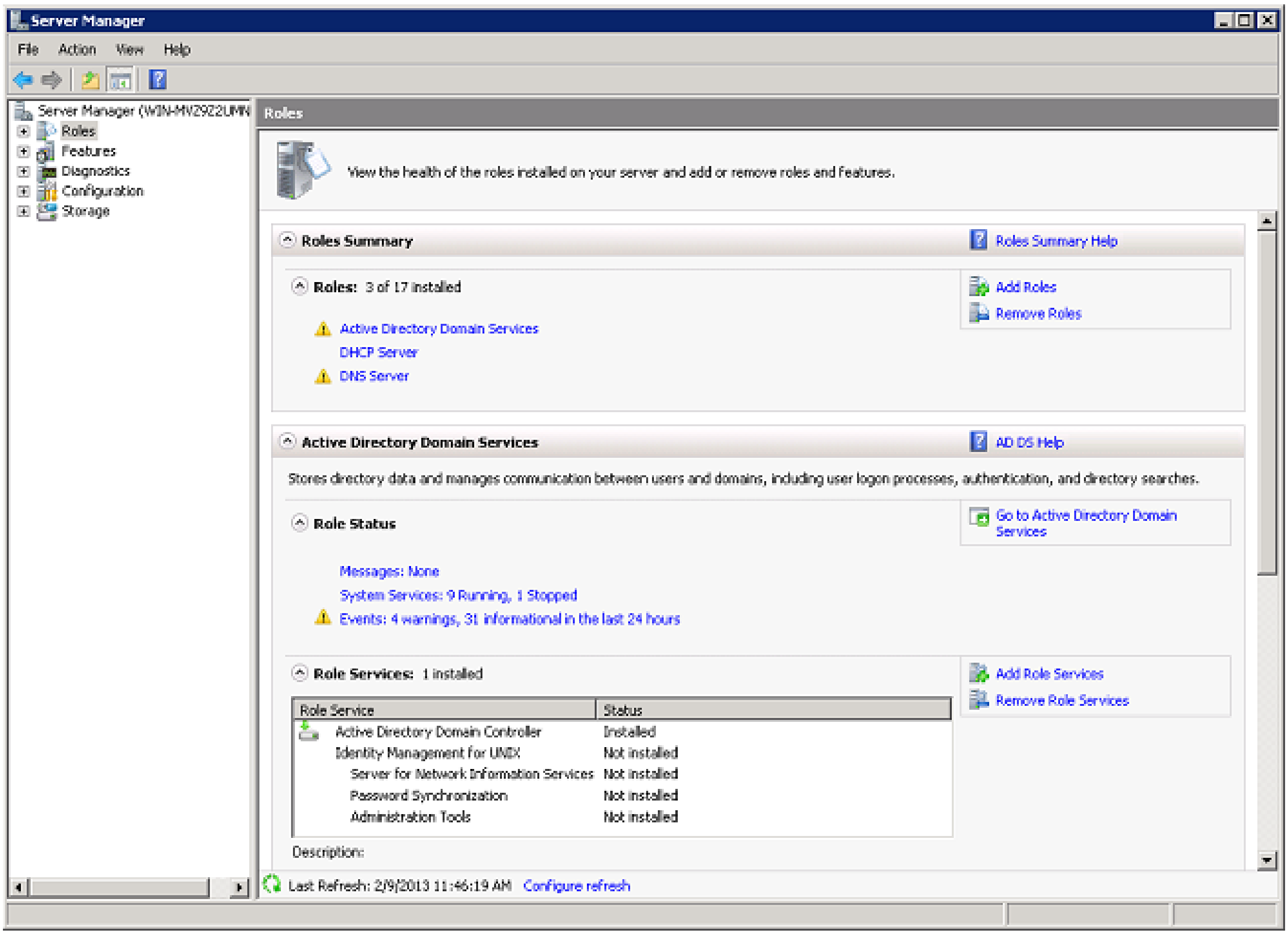
Computer Information

Full Computer Name:	win2k8.wireless.com
Domain:	wireless.com
Local Area Connection:	10.104.208.96
Remote Desktop:	Enabled
Server Manager Remote Management:	Disabled
Product ID:	00486-001-0001076-84117 (Activated)

□ Do not show me this console at logon

Security Information

Windows Firewall:	Domain: On
Windows Updates:	Install updates automatically using a managed updating service
Last checked for updates:	Yesterday at 5:39 PM
Last installed updates:	Today at 3:00 AM
IE Enhanced Security Configuration (ESC):	On for Administrators On for Users



View the health of the roles installed on your server and add or remove roles and features.

Roles Summary

Roles: 3 of 17 installed

Active Directory Domain Services
DHCP Server
DNS Server

Active Directory Domain Services

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Role Status

Messages: None
System Services: 9 Running, 1 Stopped
Events: 4 warnings, 31 informational in the last 24 hours

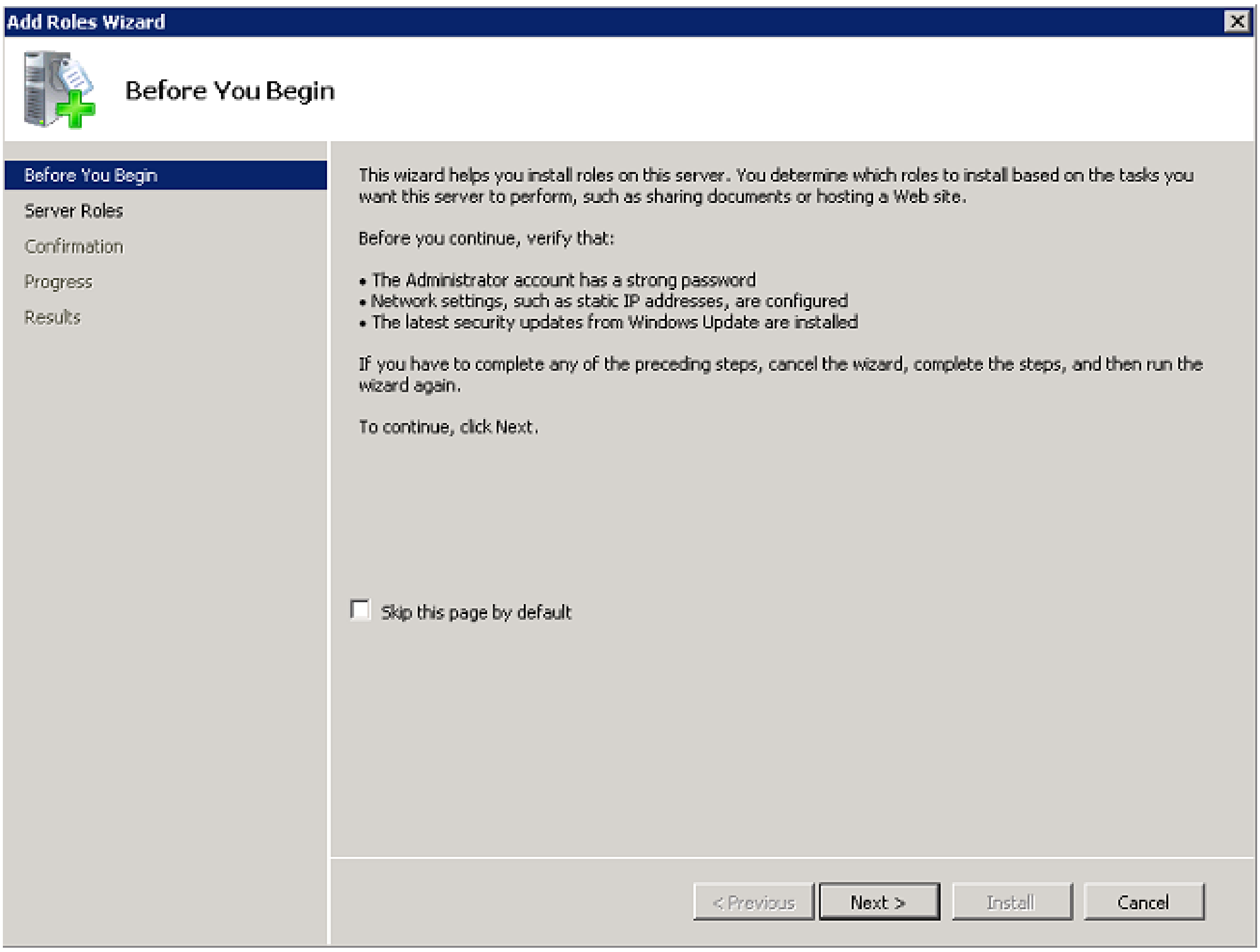
Role Services: 1 installed

Role Service	Status
Active Directory Domain Controller	Installed
Identity Management for UNIX	Not installed
Server for Network Information Services	Not installed
Password Synchronization	Not installed
Administration Tools	Not installed

Description:

Last Refresh: 2/9/2013 11:46:19 AM

2. Click **Next**.



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

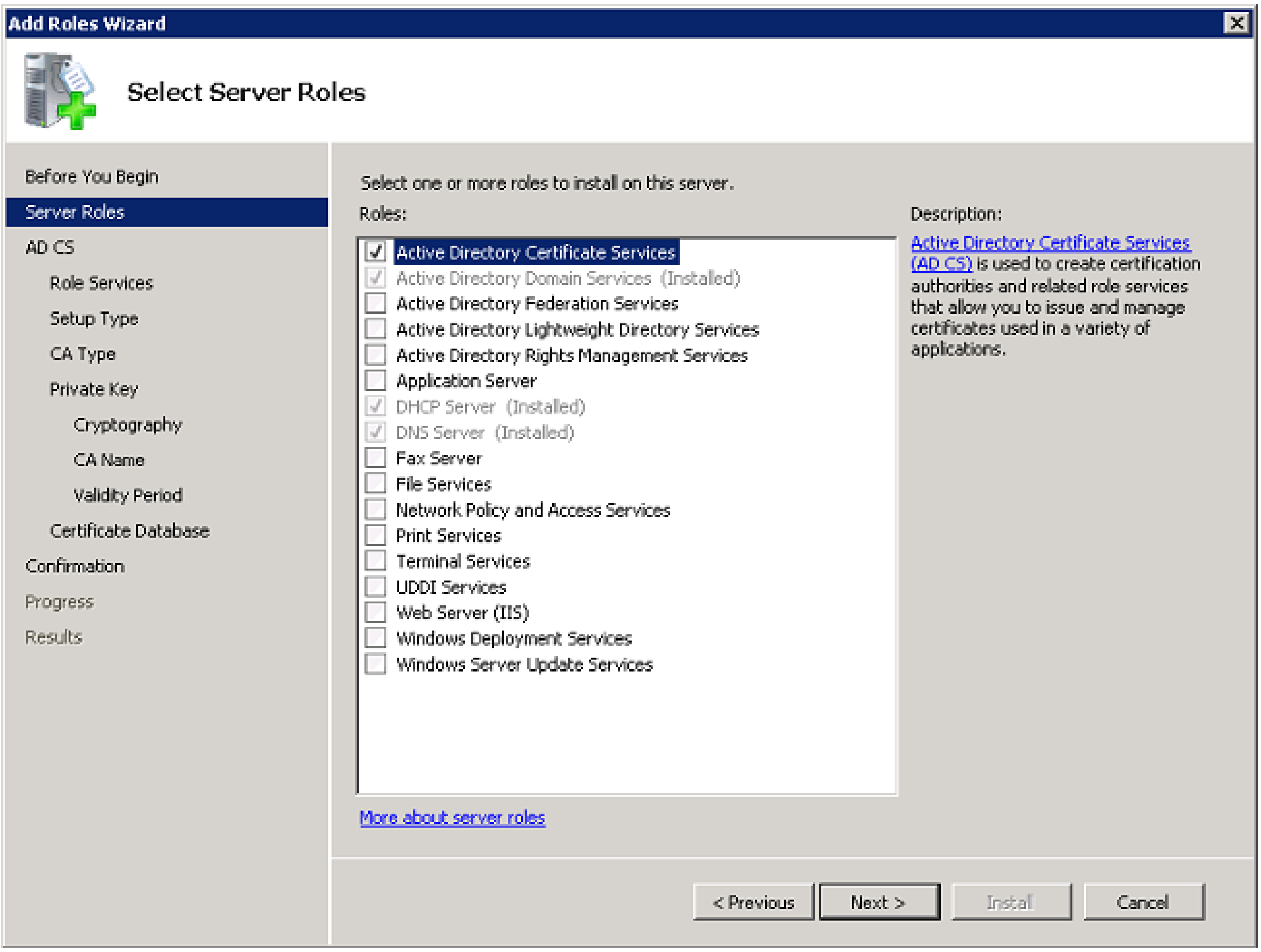
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

3. Check the **Active Directory Certificate Services** check box and click **Next**.



Select Server Roles

Select one or more roles to install on this server.

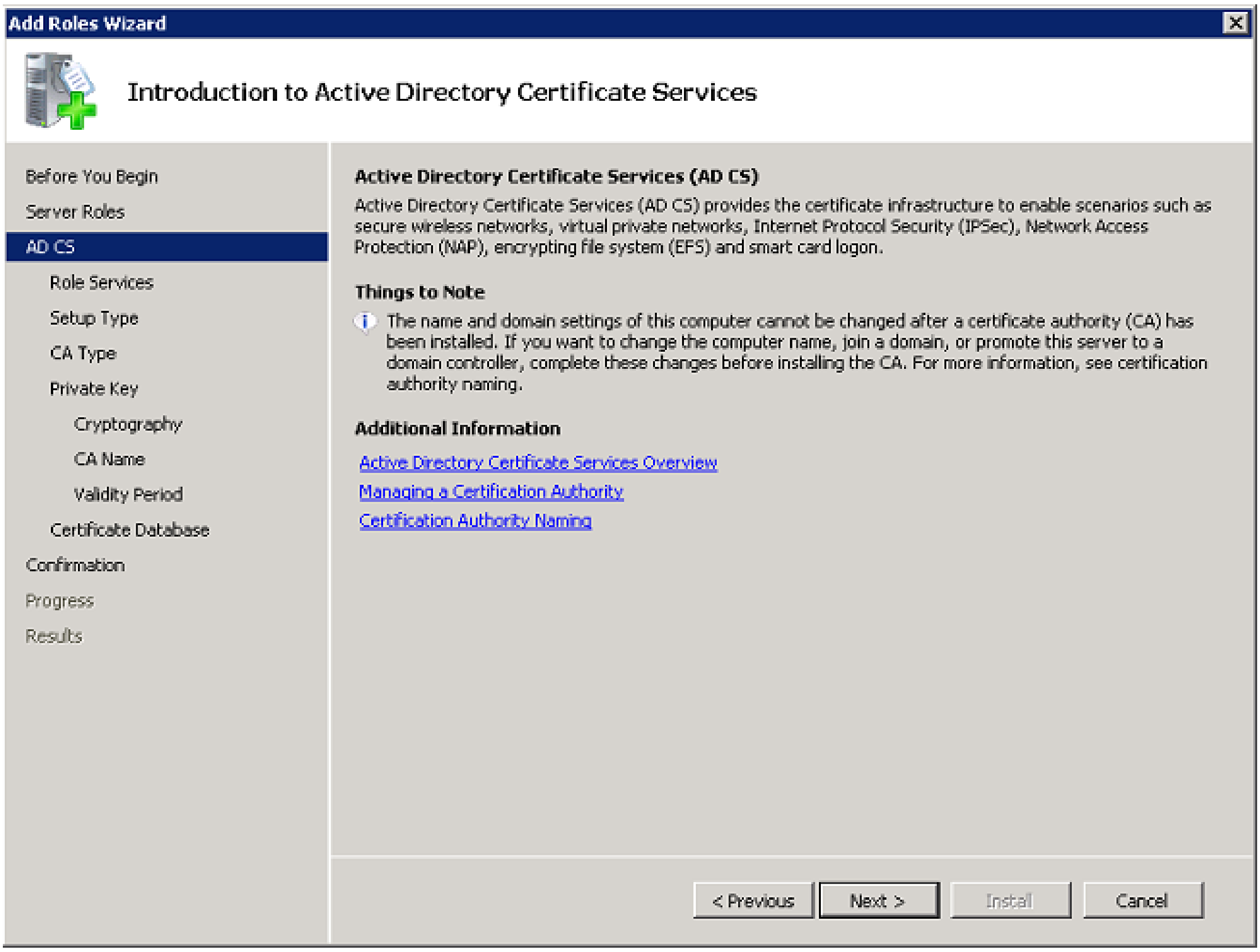
Roles:

- ☑ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- □ Fax Server
- □ File Services
- □ Network Policy and Access Services
- □ Print Services
- □ Terminal Services
- □ UDDI Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

4. Review the **Introduction to Active Directory Certificate Services** and click **Next**.



Introduction to Active Directory Certificate Services

Active Directory Certificate Services (AD CS)

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card logon.

Things to Note

The name and domain settings of this computer cannot be changed after a certificate authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

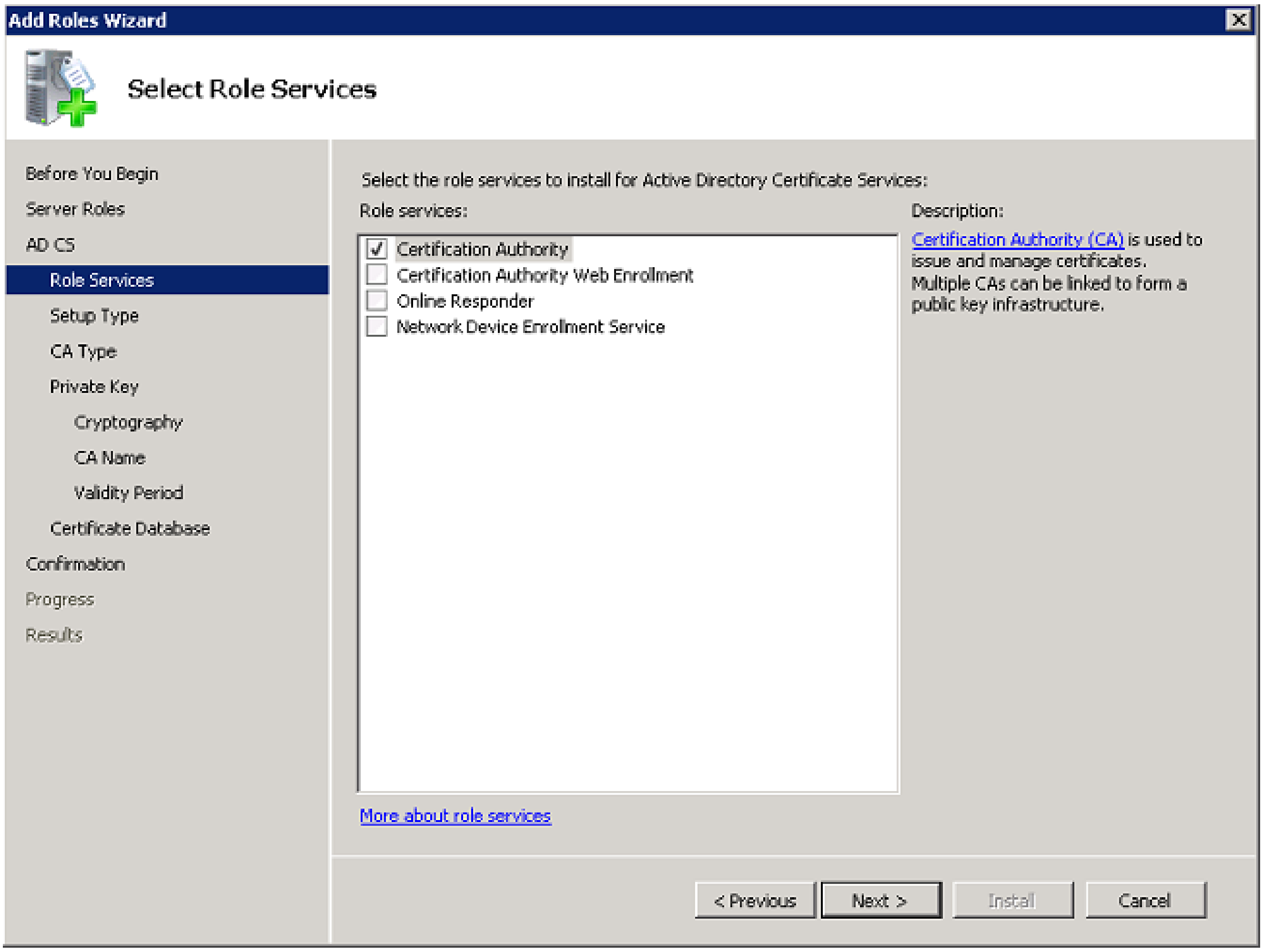
Additional Information

Active Directory Certificate Services Overview

Managing a Certification Authority

Certification Authority Naming

5. Check the **Certificate Authority** check box and click **Next**.



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

Role services:

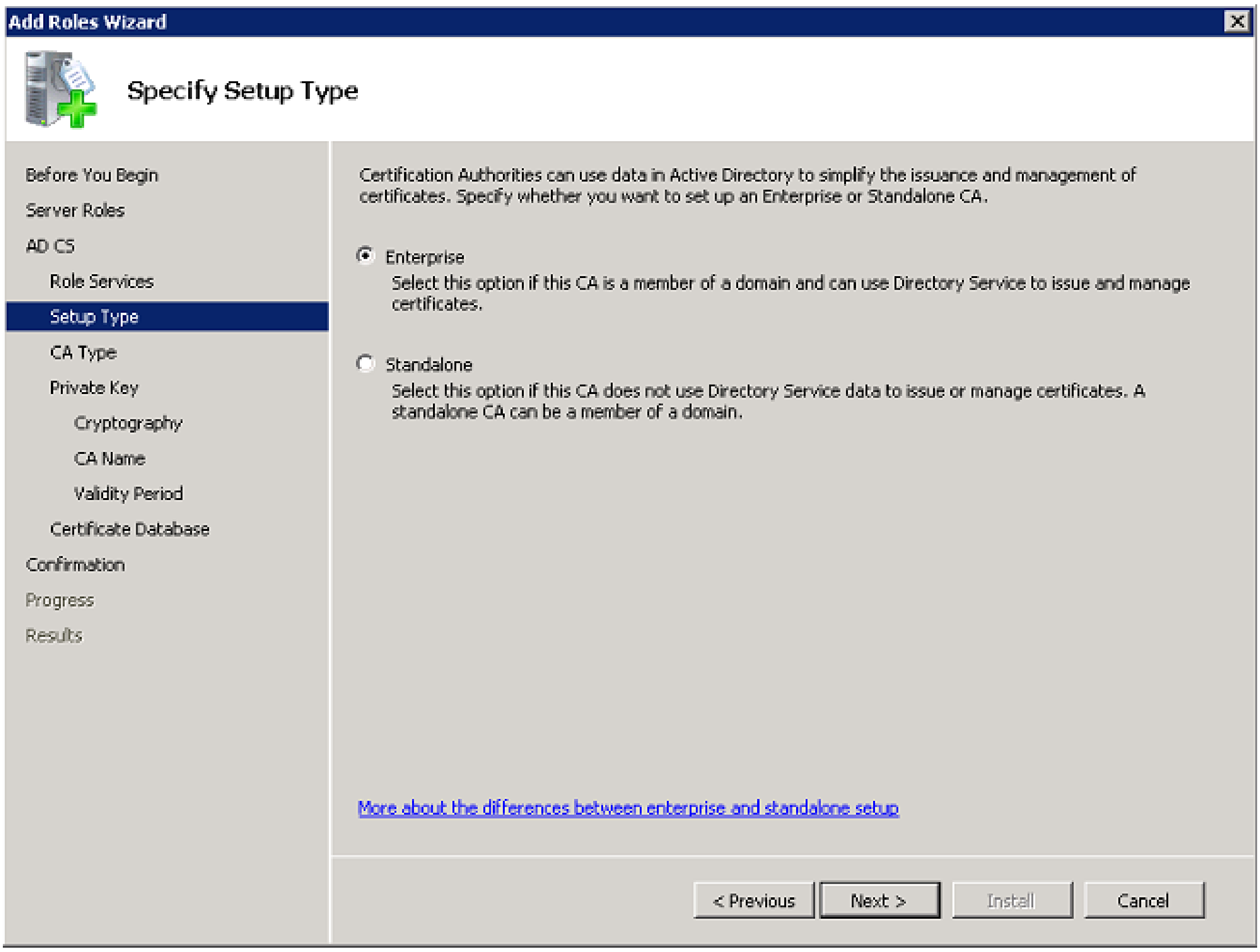
☑ Certification Authority
□ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service

Description:

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

More about role services

6. Click the **Enterprise** radio button and click **Next**.



Add Roles Wizard

Specify Setup Type

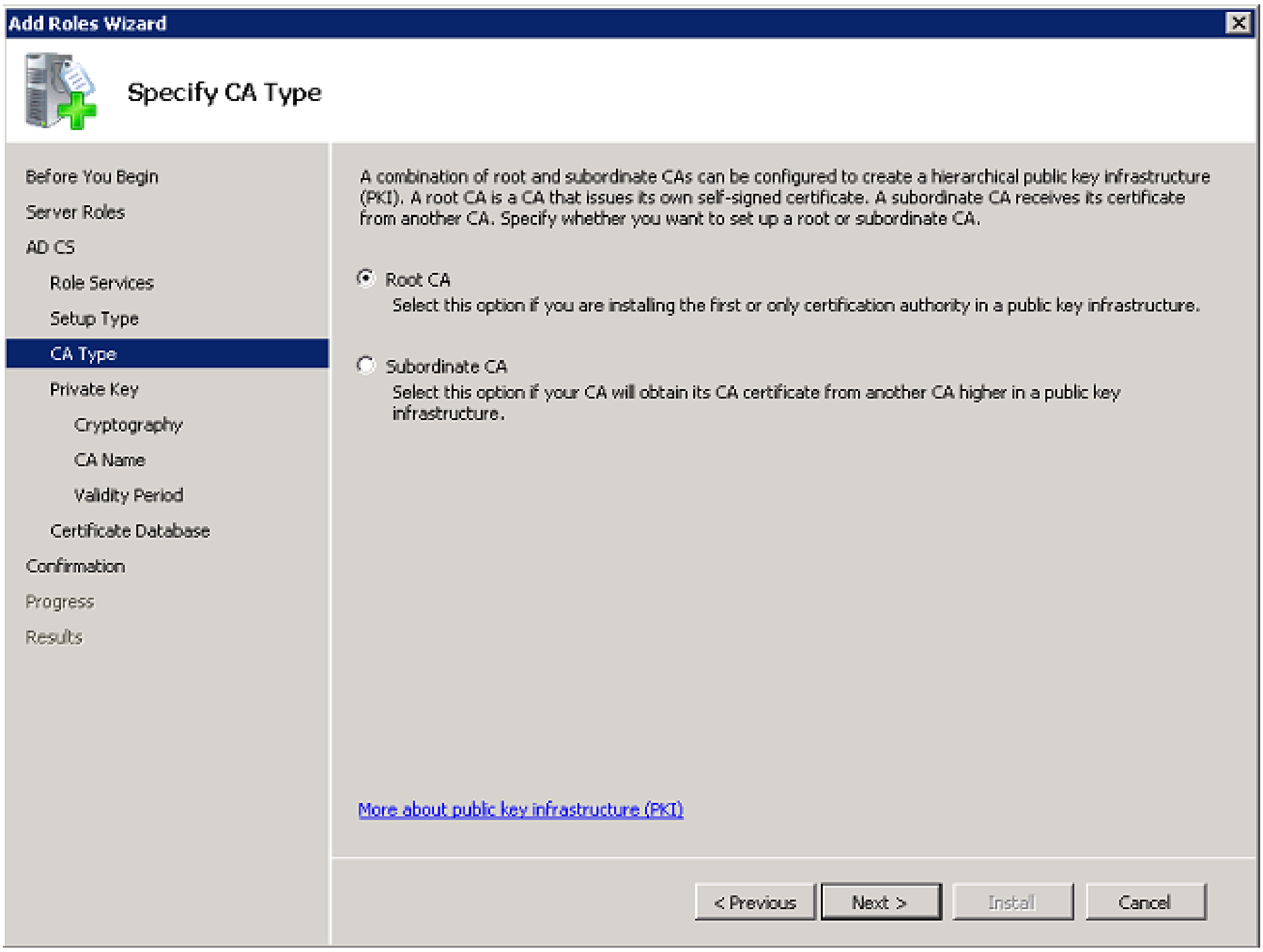
Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

● 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

7. Click the **Root CA** radio button and click **Next**.

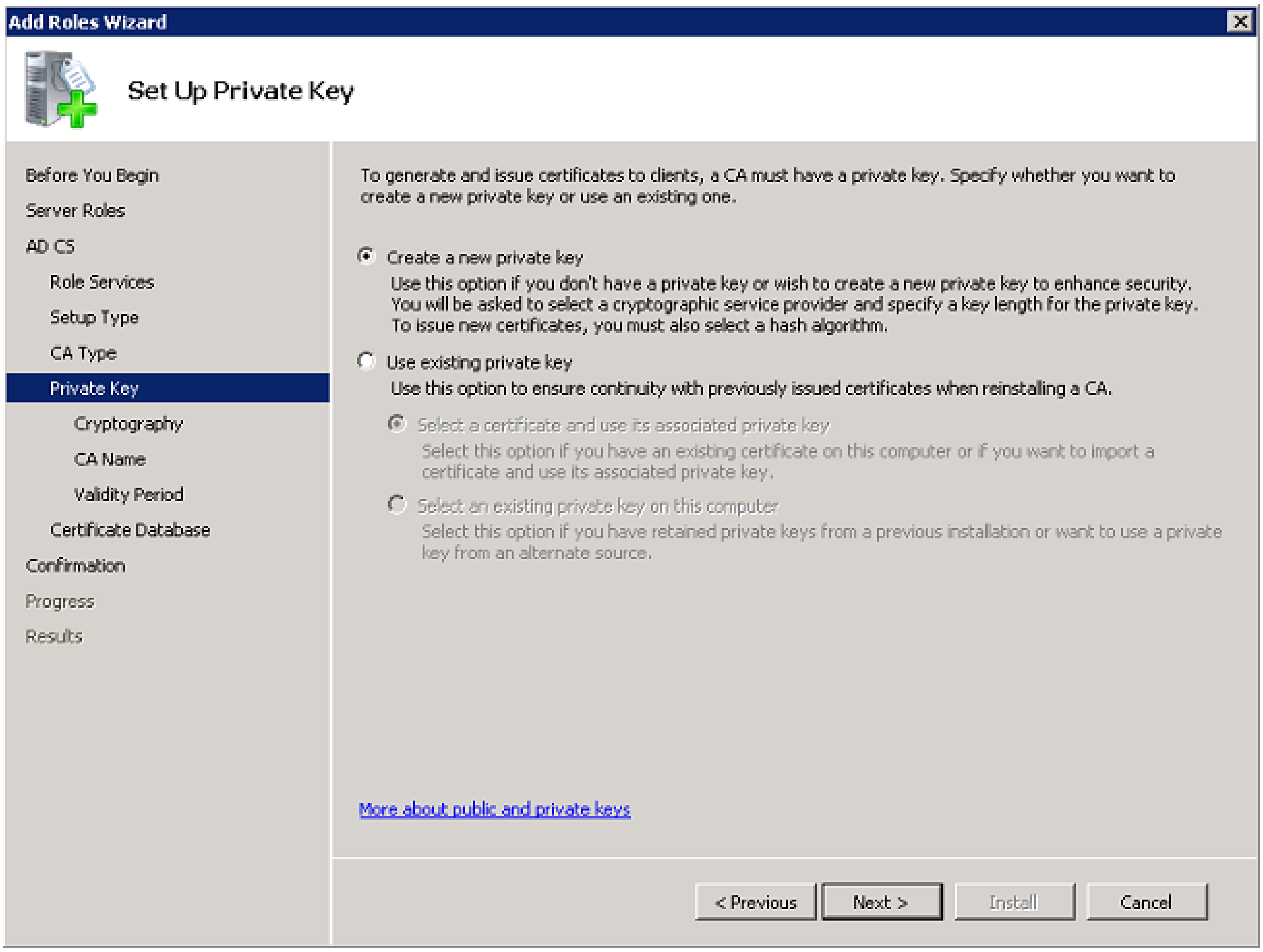


A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

● 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.

8. Click the **Create a new private key** radio buttonand click **Next**.



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.

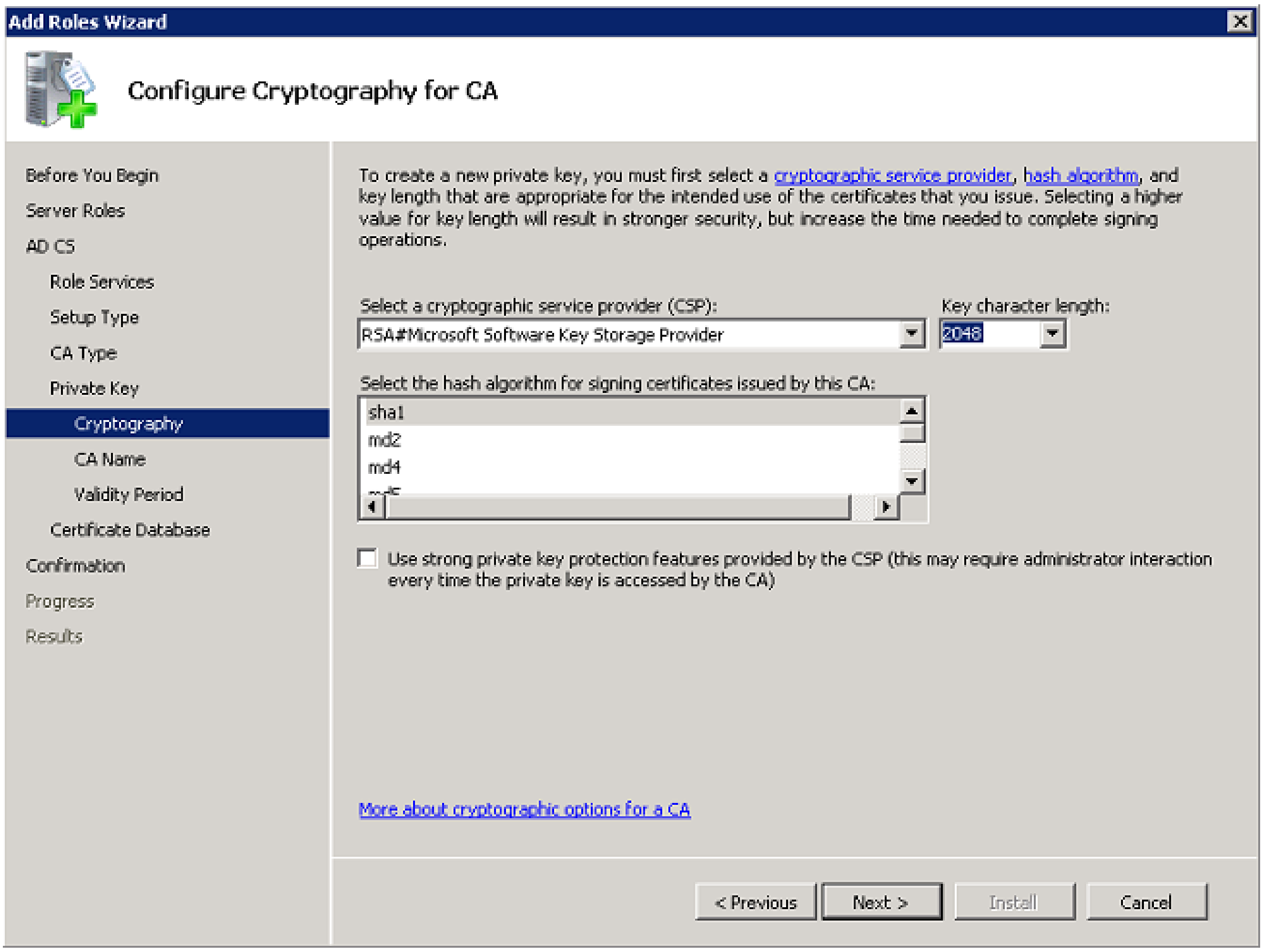
● Select a certificate and use its associated private key

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.

9. Click **Next** in the **Configuring Cryptography for CA** window.



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.

Select a cryptographic service provider (CSP): RSA#Microsoft Software Key Storage Provider

Key character length: 2048

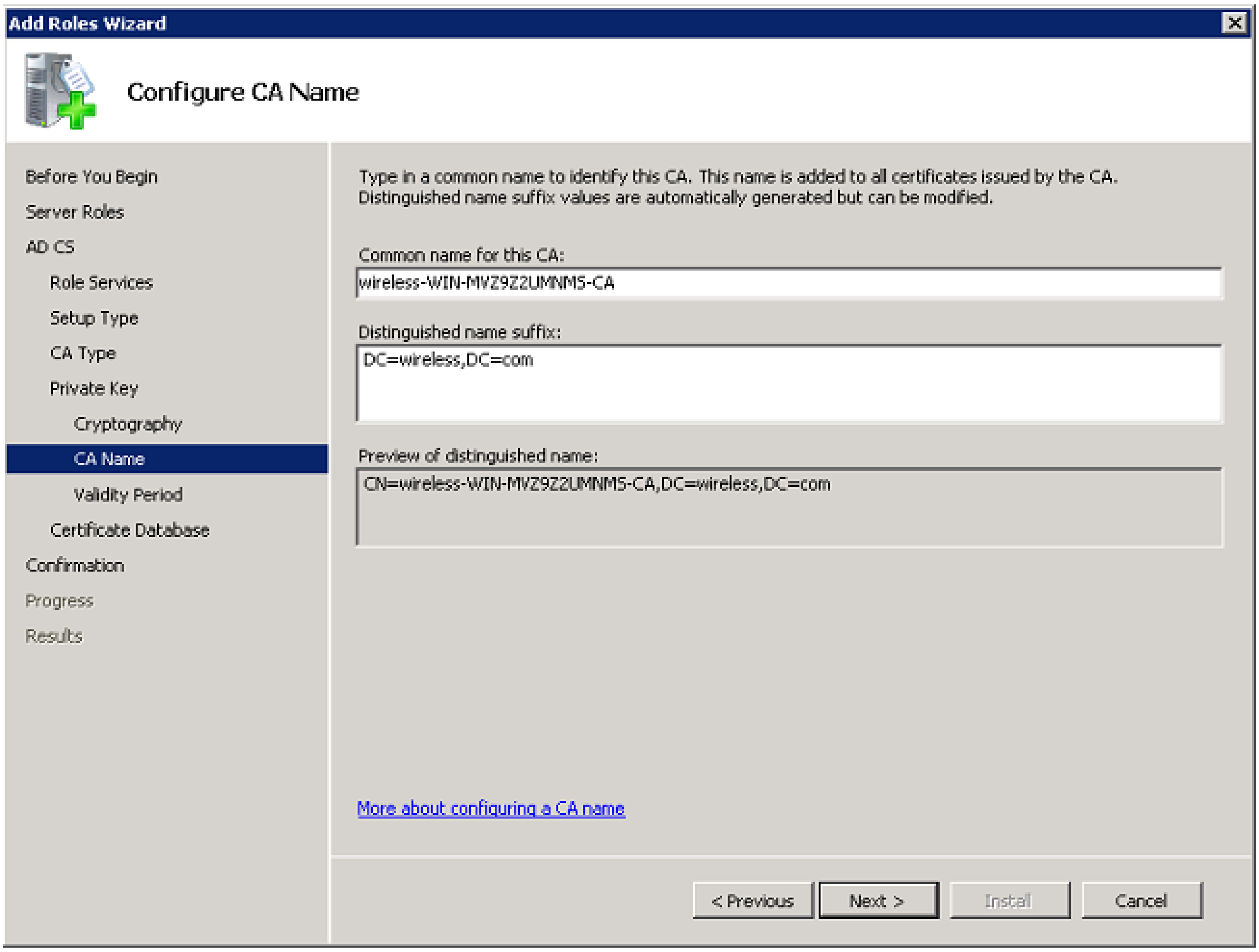
Select the hash algorithm for signing certificates issued by this CA:

sha1
md2
md4
md5

□ Use strong private key protection features provided by the CSP (this may require administrator interaction every time the private key is accessed by the CA)

More about cryptographic options for a CA

10. Click **Next** in order to accept the **Common name for this CA** default name.



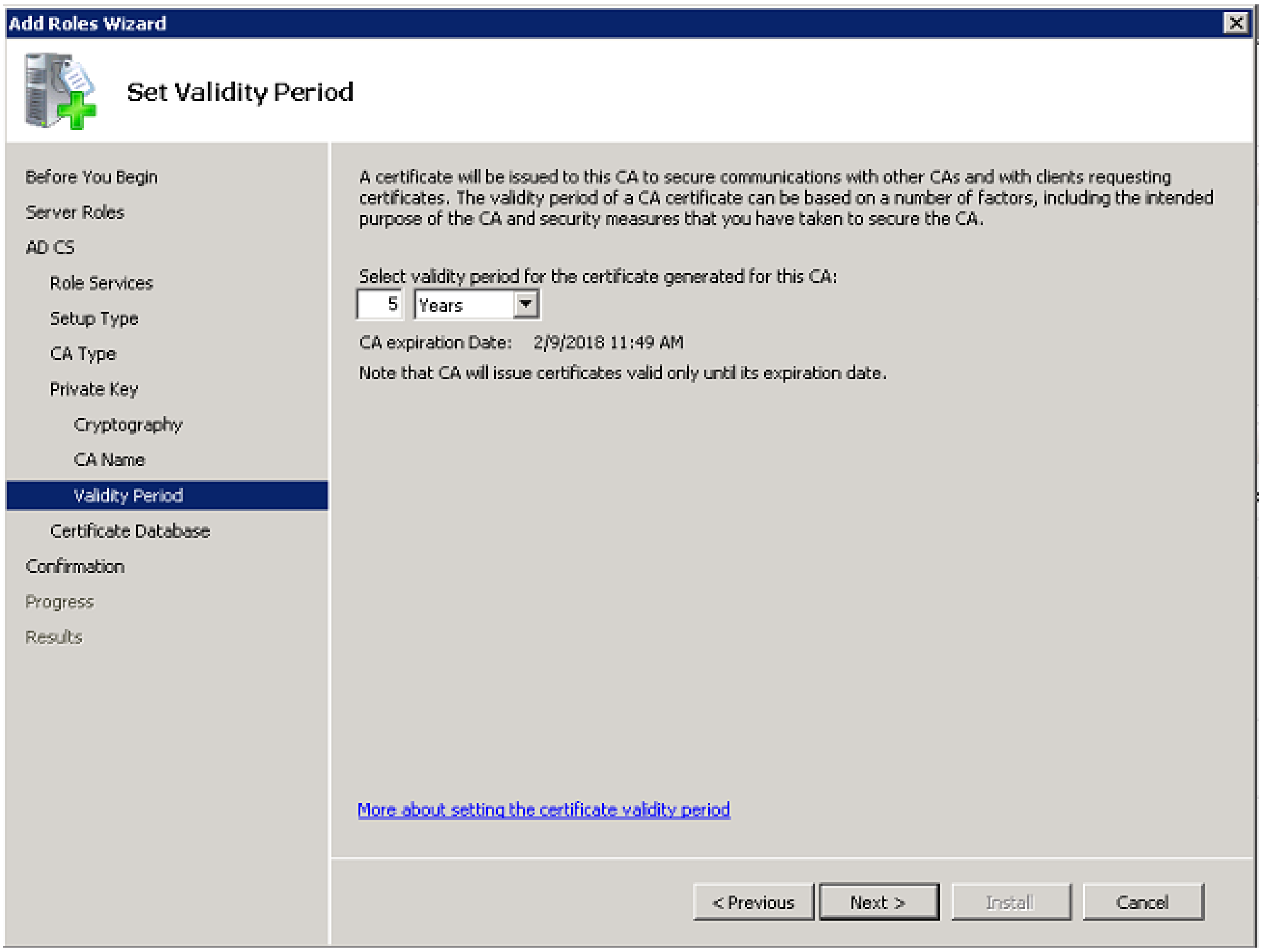
Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: wireless-WIN-MVZ9Z2UMNM5-CA

Distinguished name suffix: DC=wireless,DC=com

Preview of distinguished name: CN=wireless-WIN-MVZ9Z2UMNM5-CA,DC=wireless,DC=com

11. Select the length of time for which the CA certificate is valid and click **Next**.



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.

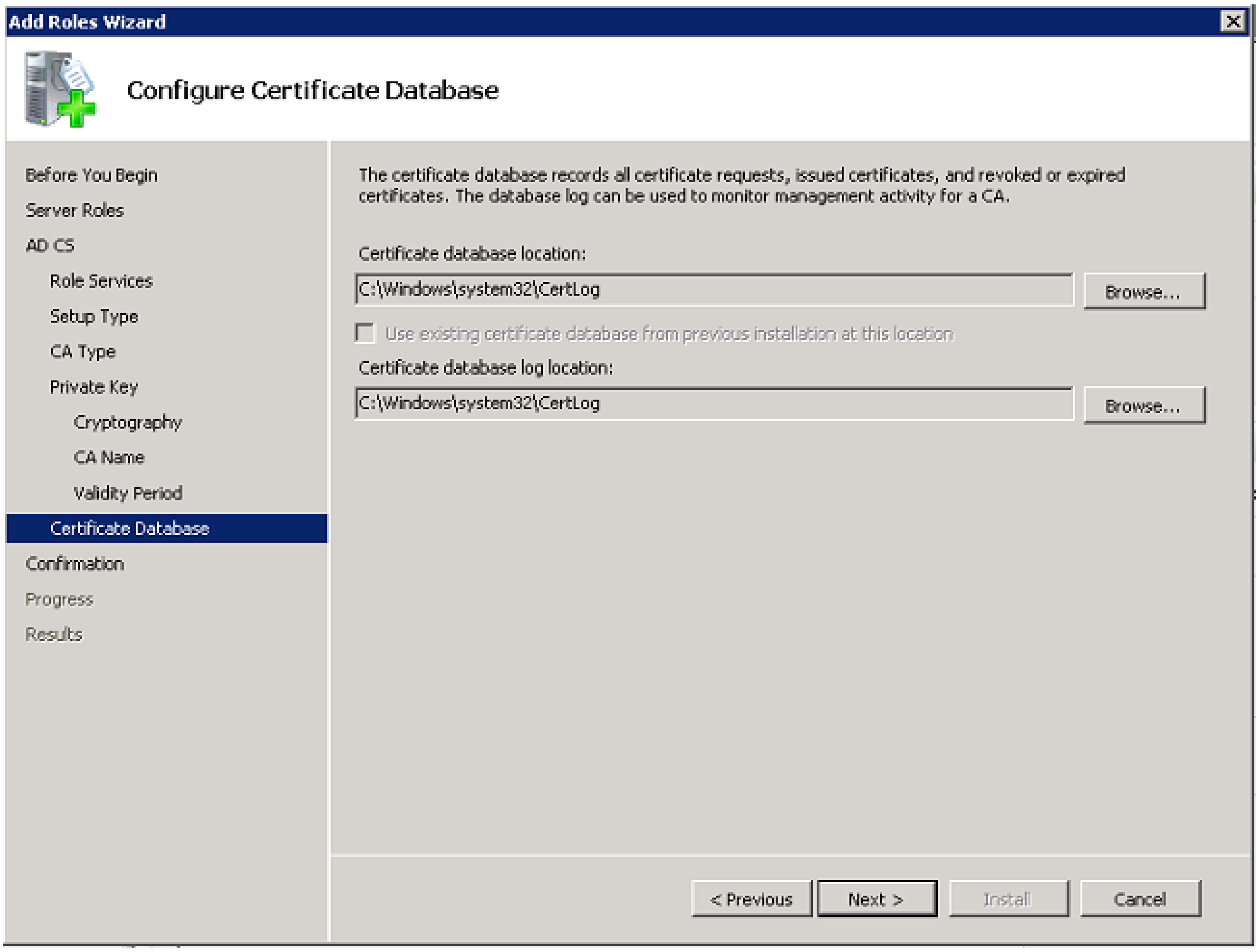
Select validity period for the certificate generated for this CA:

5 Years

CA expiration Date: 2/9/2018 11:49 AM

Note that CA will issue certificates valid only until its expiration date.

12. Click **Next** in order to accept the **Certificate database location** default location.



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:

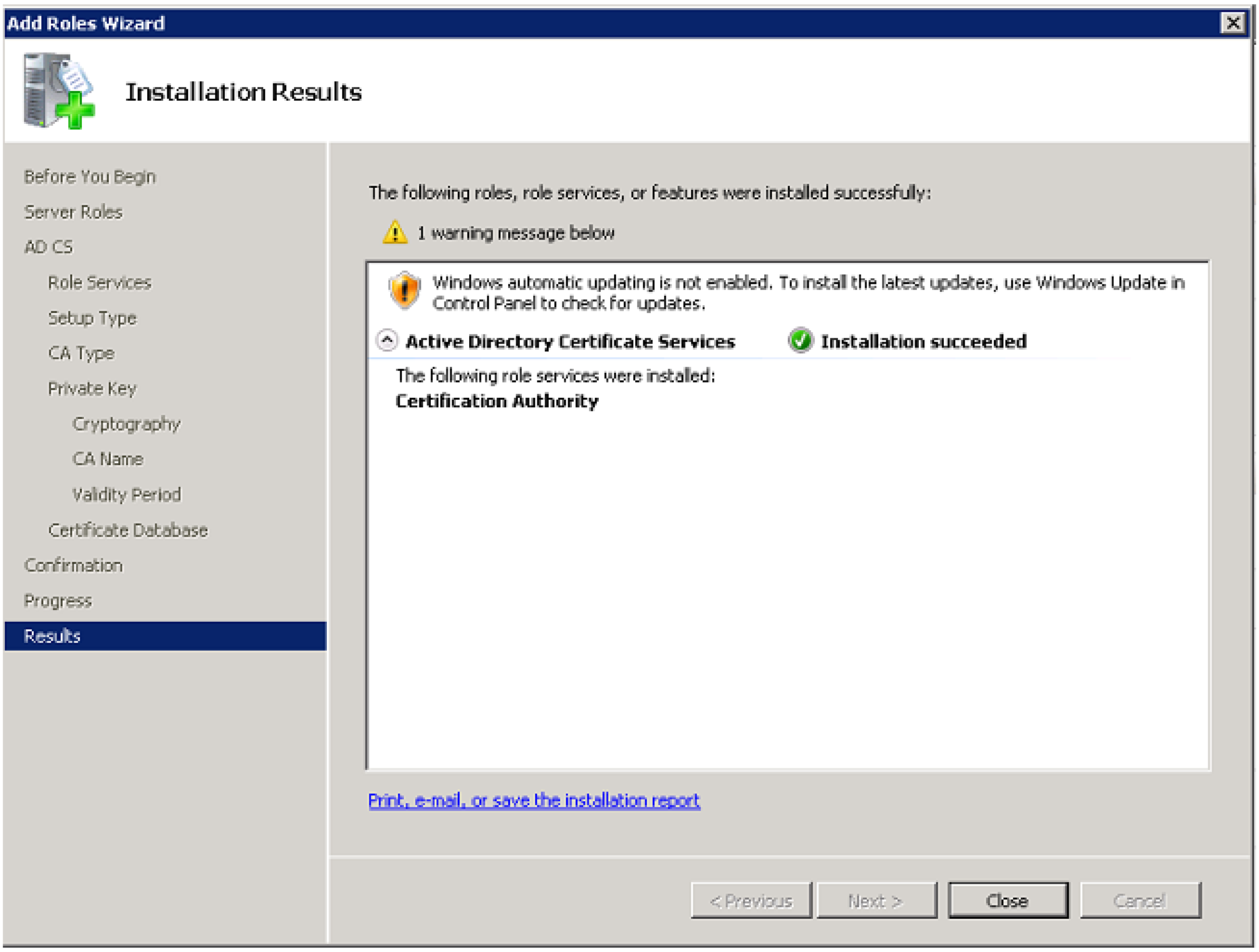
C:\Windows\system32\CertLog

□ Use existing certificate database from previous installation at this location

Certificate database log location:

C:\Windows\system32\CertLog

13. Review the configuration and click **Install** in order to begin the **Active Directory Certificate Services**.



Add Roles Wizard

Installation Results

The following roles, role services, or features were installed successfully:

⚠ 1 warning message below

Windows automatic updating is not enabled. To install the latest updates, use Windows Update in Control Panel to check for updates.

Active Directory Certificate Services ✓ Installation succeeded

The following role services were installed:
Certification Authority

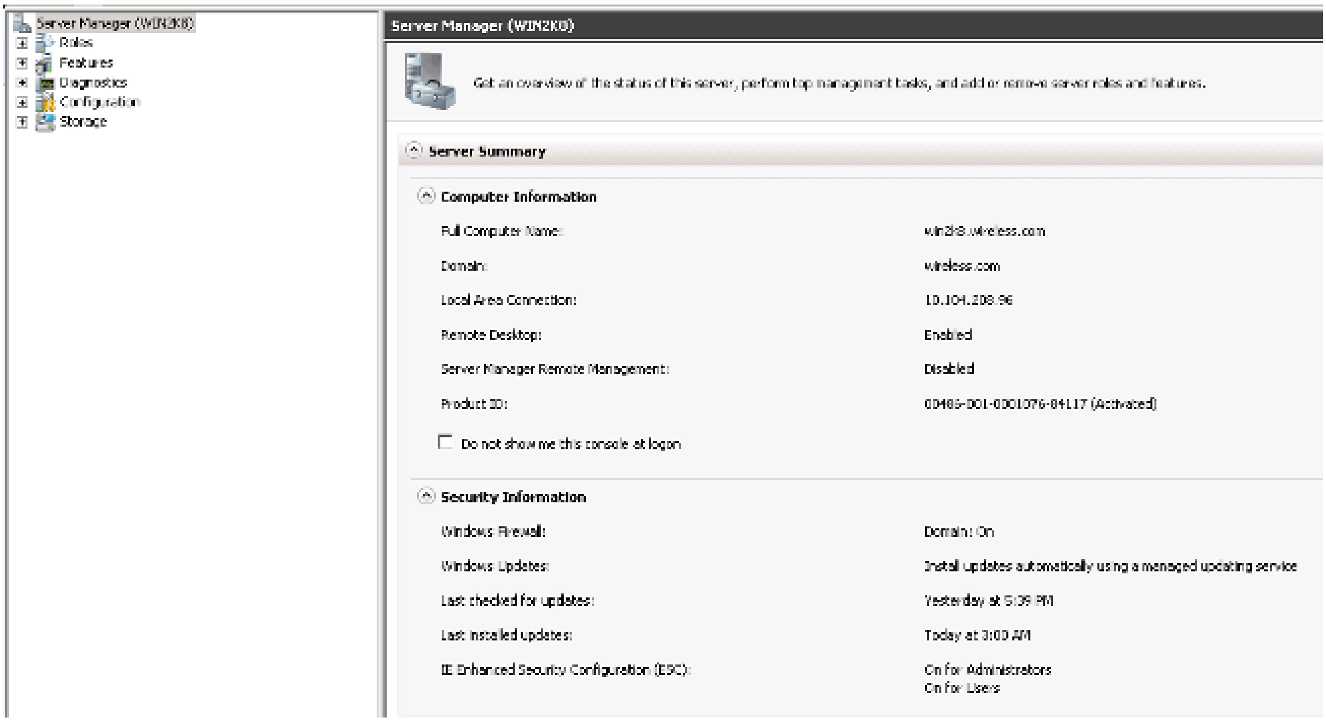
14. After the installation is completed, click **Close**.

Install the NPS on the Microsoft Windows Version 2008 Server

> **Note**: With the setup that is described in this section, the NPS is used as a RADIUS server in order to authenticate the wireless clients with PEAP authentication.

Complete these steps in order to install and configure the NPS on the Microsoft Windows Version 2008 server:

1. Navigate to **Start** > **Server Manager > Roles** > **Add Roles**.



Server Manager (WIN2K8)

Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Server Summary

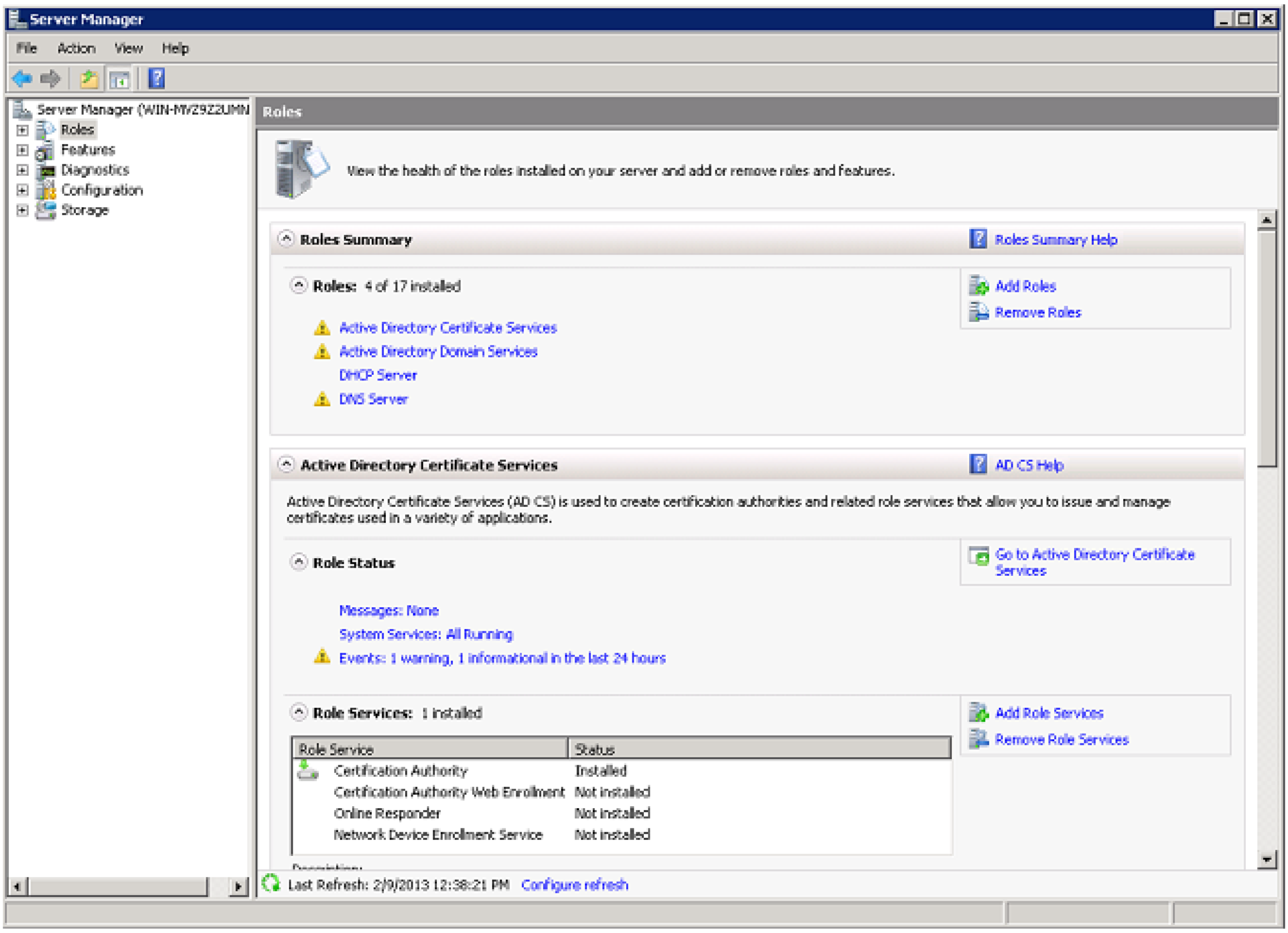
Computer Information

Full Computer Name:	win2k8.wireless.com
Domain:	wireless.com
Local Area Connection:	10.104.208.96
Remote Desktop:	Enabled
Server Manager Remote Management:	Disabled
Product ID:	00486-001-0001076-84117 (Activated)

□ Do not show me this console at logon

Security Information

Windows Firewall:	Domain: On
Windows Updates:	Install updates automatically using a managed updating service
Last checked for updates:	Yesterday at 5:39 PM
Last installed updates:	Today at 3:00 AM
IE Enhanced Security Configuration (ESC):	On for Administrators On for Users



Roles

View the health of the roles installed on your server and add or remove roles and features.

Roles Summary

Roles Summary Help

Roles: 4 of 17 installed

Add Roles

Remove Roles

- Active Directory Certificate Services
- Active Directory Domain Services
- DHCP Server
- DNS Server

Active Directory Certificate Services

AD CS Help

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Role Status

Go to Active Directory Certificate Services

Messages: None

System Services: All Running

Events: 1 warning, 1 informational in the last 24 hours

Role Services: 1 installed

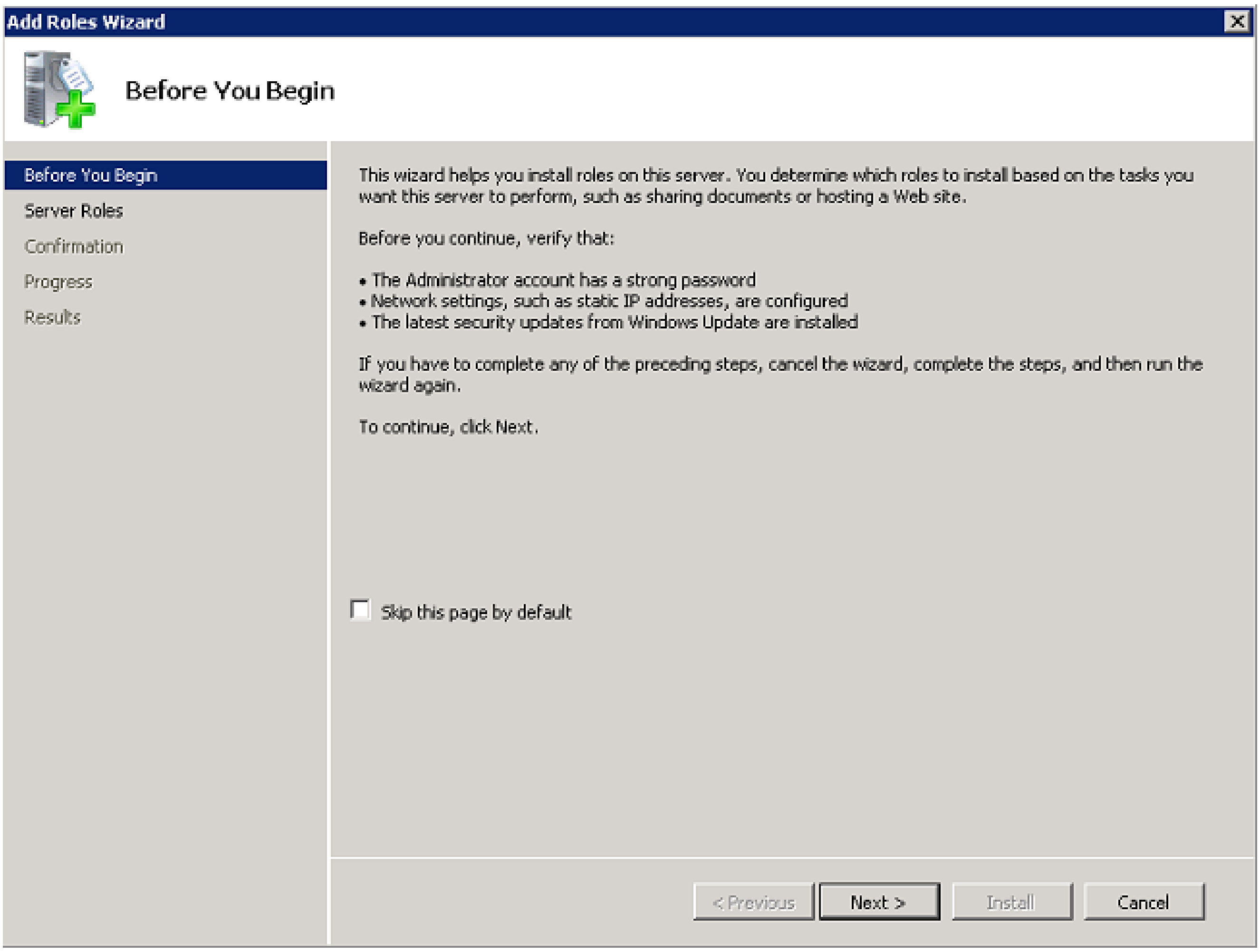
Add Role Services

Remove Role Services

Role Service	Status
Certification Authority	Installed
Certification Authority Web Enrollment	Not installed
Online Responder	Not installed
Network Device Enrollment Service	Not installed

Last Refresh: 2/9/2013 12:38:21 PM Configure refresh

2. Click **Next**.



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

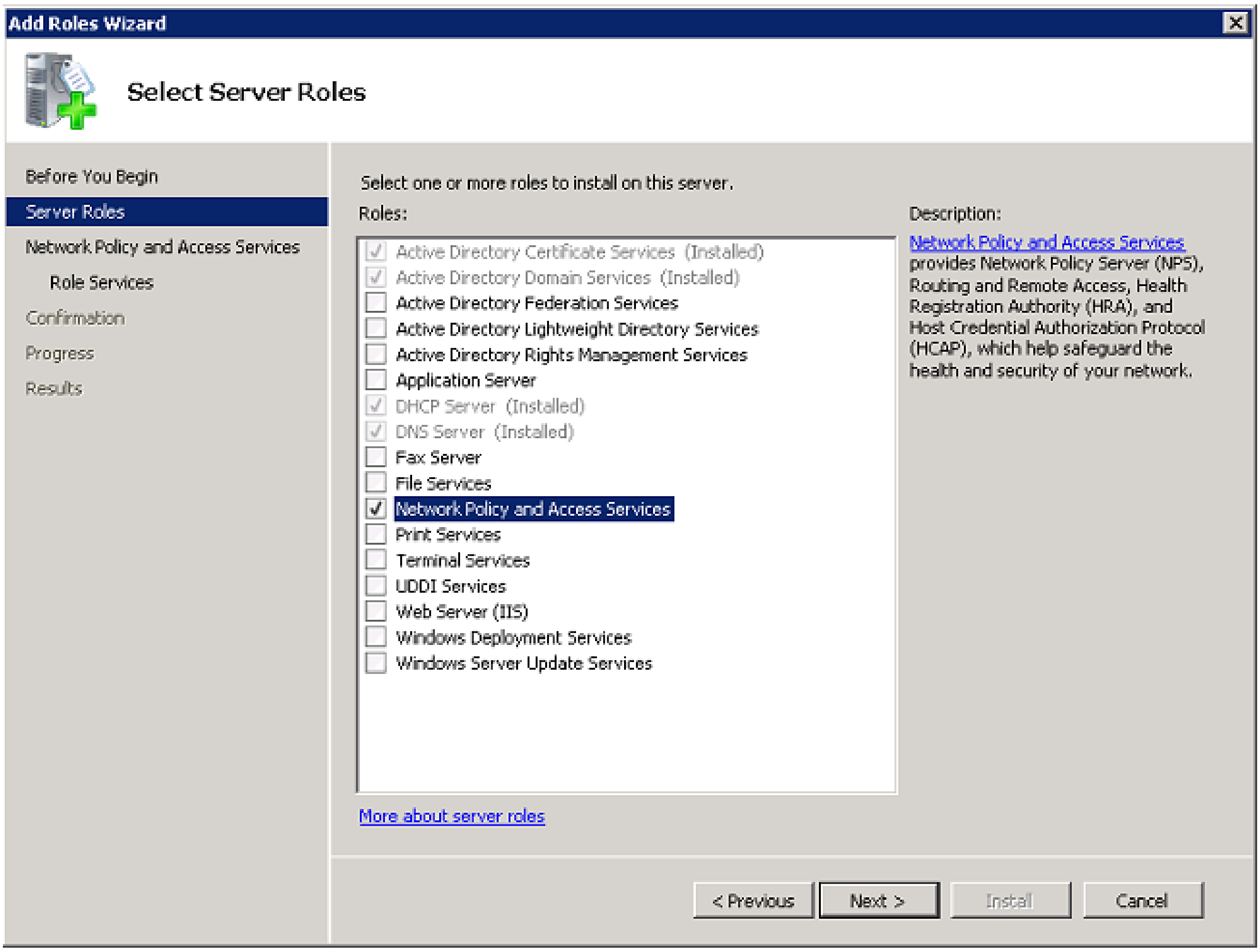
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

3. Check the **Network Policy and Access Services** check box and click **Next**.



Select Server Roles

Select one or more roles to install on this server.

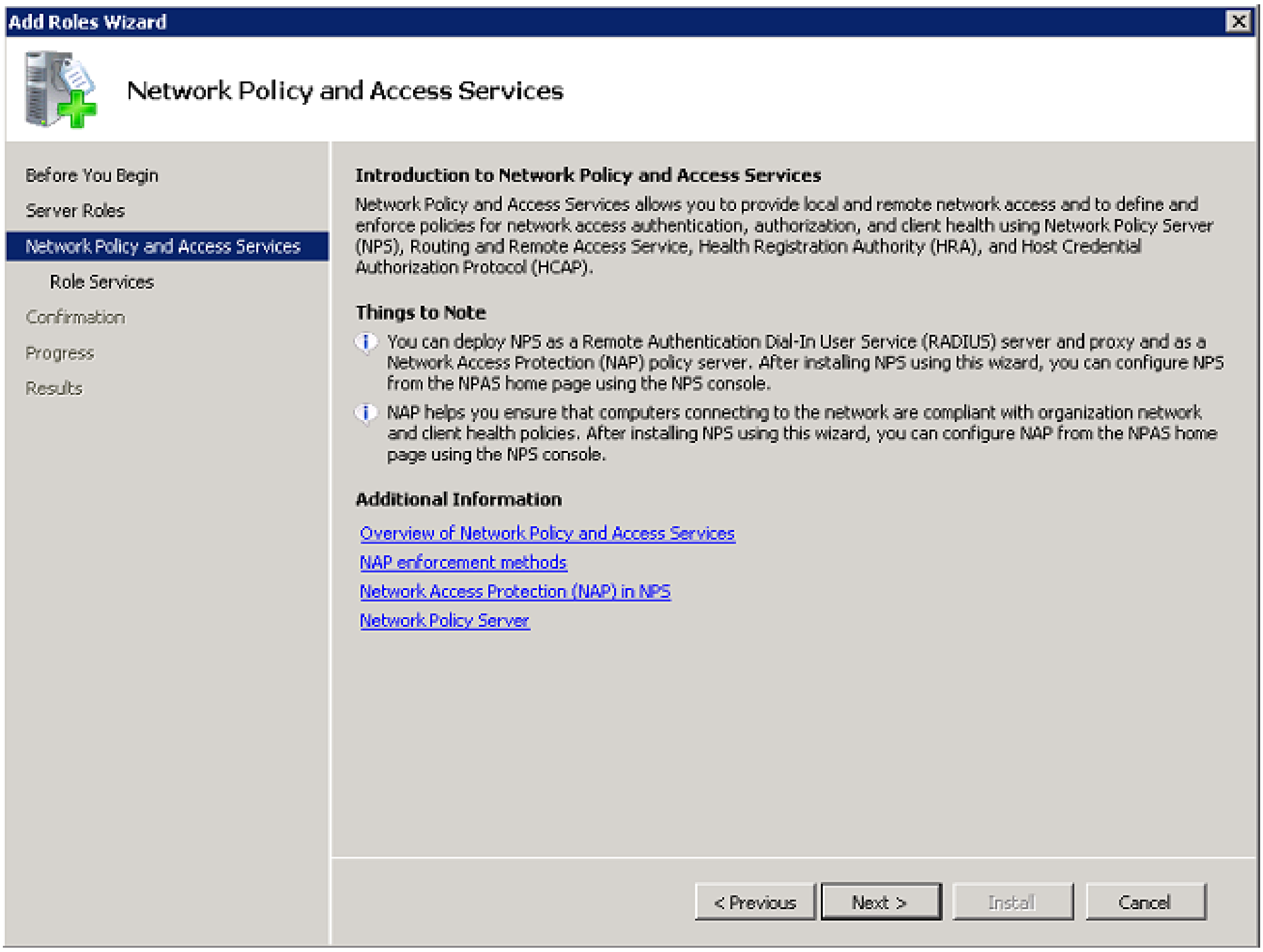
Roles:

☑ Active Directory Certificate Services (Installed)
☑ Active Directory Domain Services (Installed)
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Application Server
☑ DHCP Server (Installed)
☑ DNS Server (Installed)
□ Fax Server
□ File Services
☑ Network Policy and Access Services
□ Print Services
□ Terminal Services
□ UDDI Services
□ Web Server (IIS)
□ Windows Deployment Services
□ Windows Server Update Services

Description:

Network Policy and Access Services provides Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.

4. Review the **Introduction to Network Policy and Access Services** and click **Next**.



Introduction to Network Policy and Access Services

Network Policy and Access Services allows you to provide local and remote network access and to define and enforce policies for network access authentication, authorization, and client health using Network Policy Server (NPS), Routing and Remote Access Service, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP).

Things to Note

- You can deploy NPS as a Remote Authentication Dial-In User Service (RADIUS) server and proxy and as a Network Access Protection (NAP) policy server. After installing NPS using this wizard, you can configure NPS from the NPAS home page using the NPS console.
- NAP helps you ensure that computers connecting to the network are compliant with organization network and client health policies. After installing NPS using this wizard, you can configure NAP from the NPAS home page using the NPS console.

Additional Information

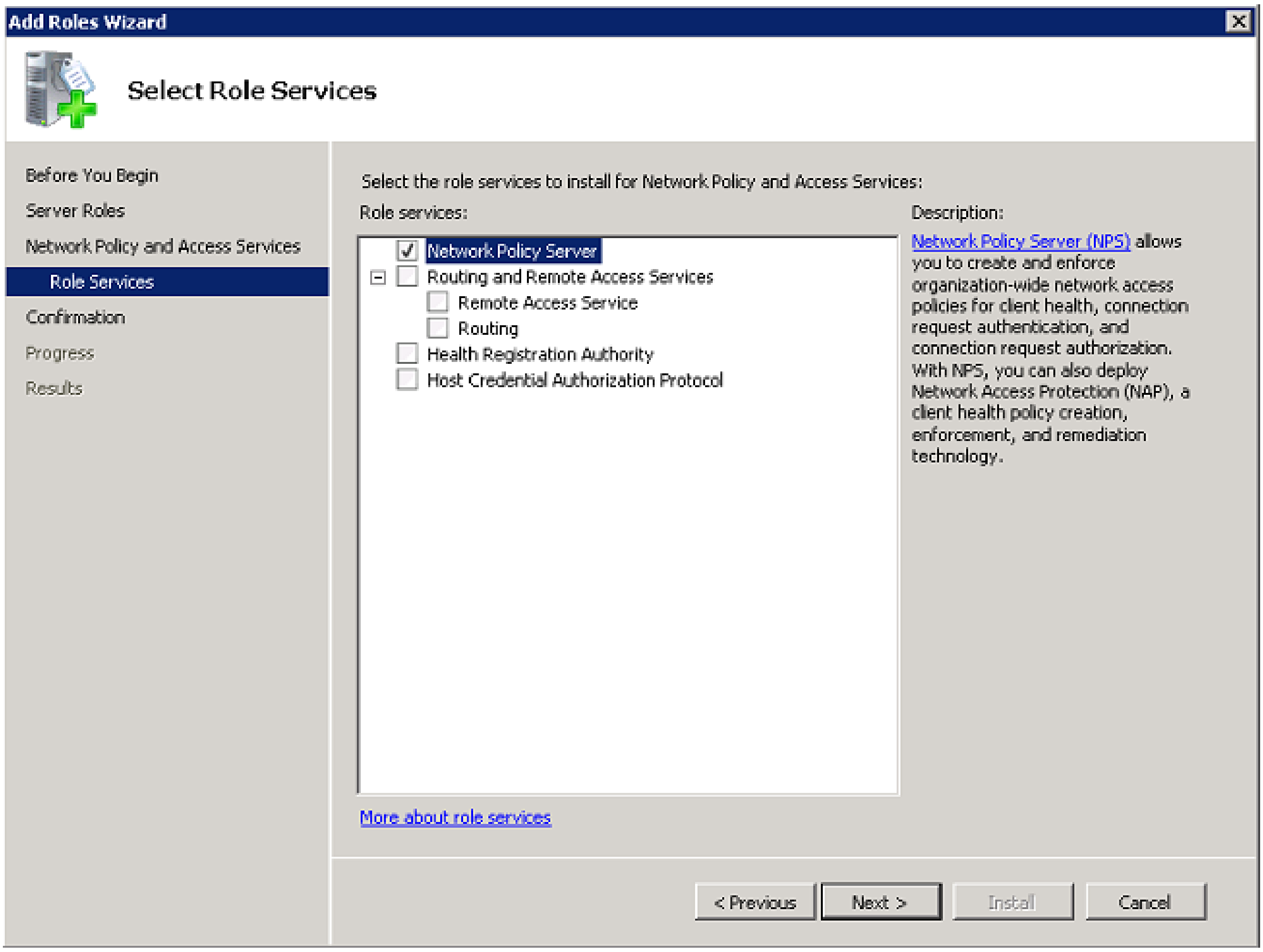
Overview of Network Policy and Access Services

NAP enforcement methods

Network Access Protection (NAP) in NPS

Network Policy Server

5. Check the **Network Policy Server** check boxand click **Next**.



Select Role Services

Select the role services to install for Network Policy and Access Services:

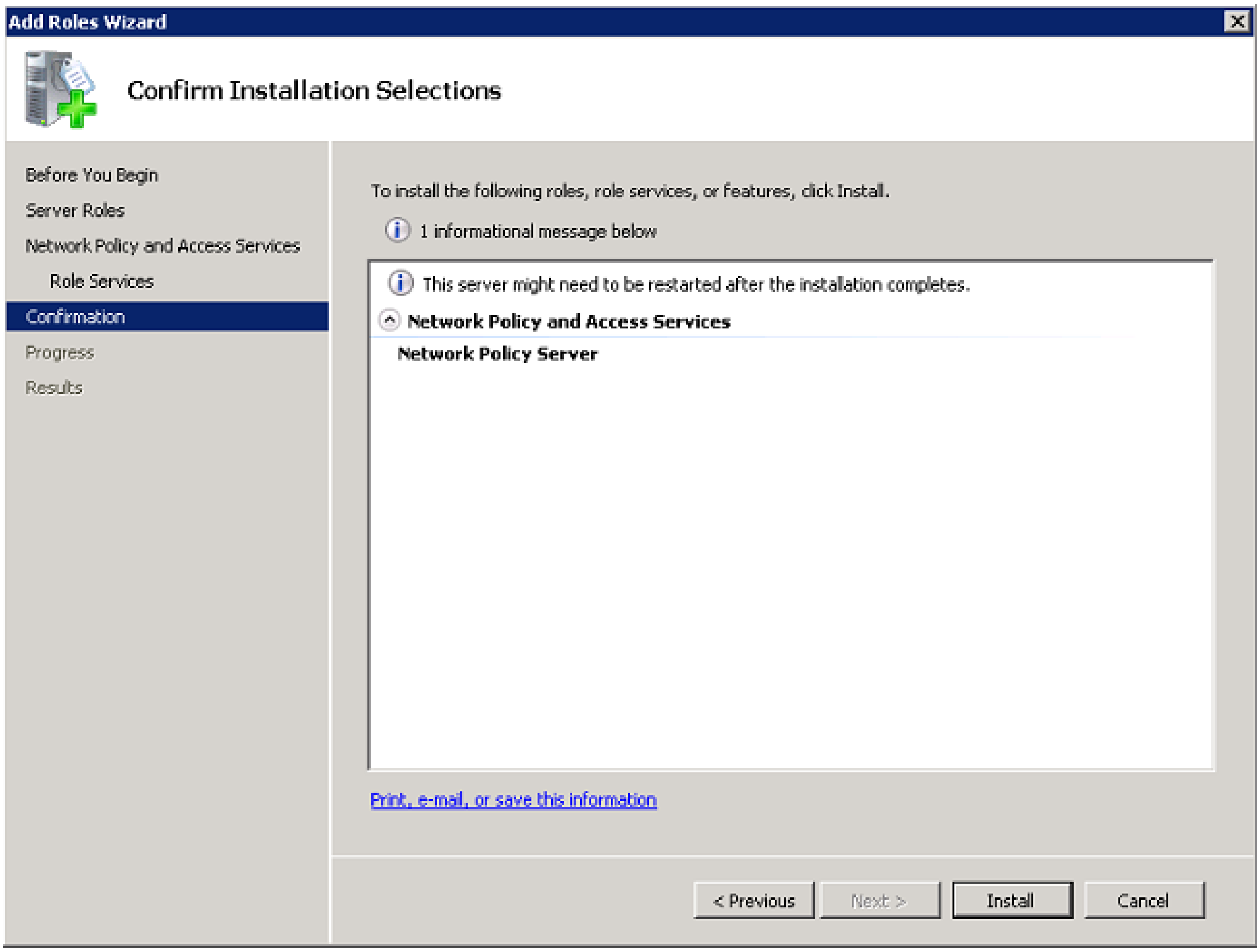
Role services:

- ☑ Network Policy Server
- ☐ Routing and Remote Access Services
  - ☐ Remote Access Service
  - ☐ Routing
- ☐ Health Registration Authority
- ☐ Host Credential Authorization Protocol

Description:

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.

6. Review the confirmation and click **Install**.



Confirm Installation Selections

To install the following roles, role services, or features, click Install.

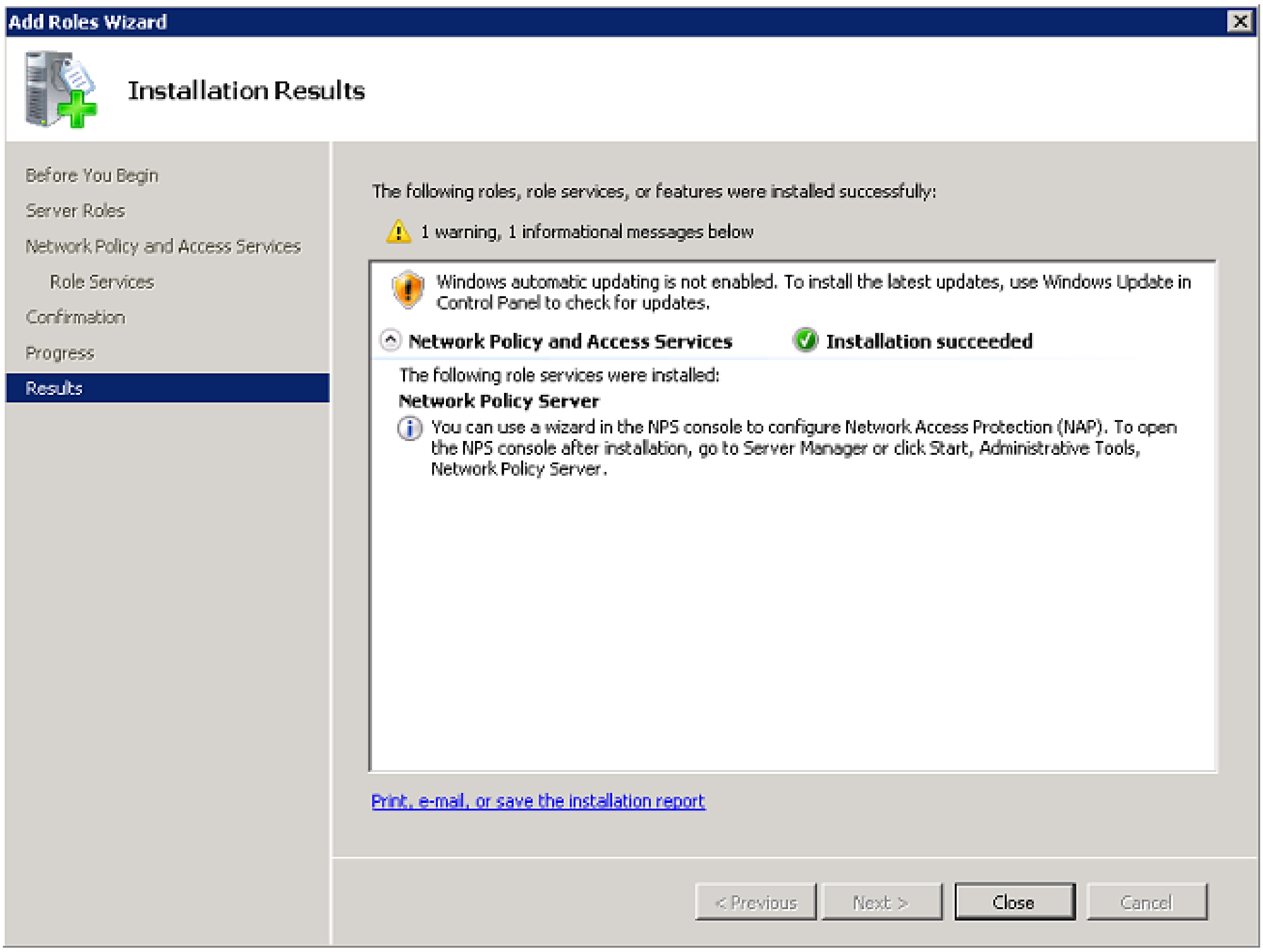
1 informational message below

This server might need to be restarted after the installation completes.

Network Policy and Access Services

Network Policy Server

After the installation is complete, a screen similar to this should appear:



The following roles, role services, or features were installed successfully:

⚠ 1 warning, 1 informational messages below

Windows automatic updating is not enabled. To install the latest updates, use Windows Update in Control Panel to check for updates.

Network Policy and Access Services ✓ Installation succeeded

The following role services were installed:

Network Policy Server

ⓘ You can use a wizard in the NPS console to configure Network Access Protection (NAP). To open the NPS console after installation, go to Server Manager or click Start, Administrative Tools, Network Policy Server.

7. Click **Close**.

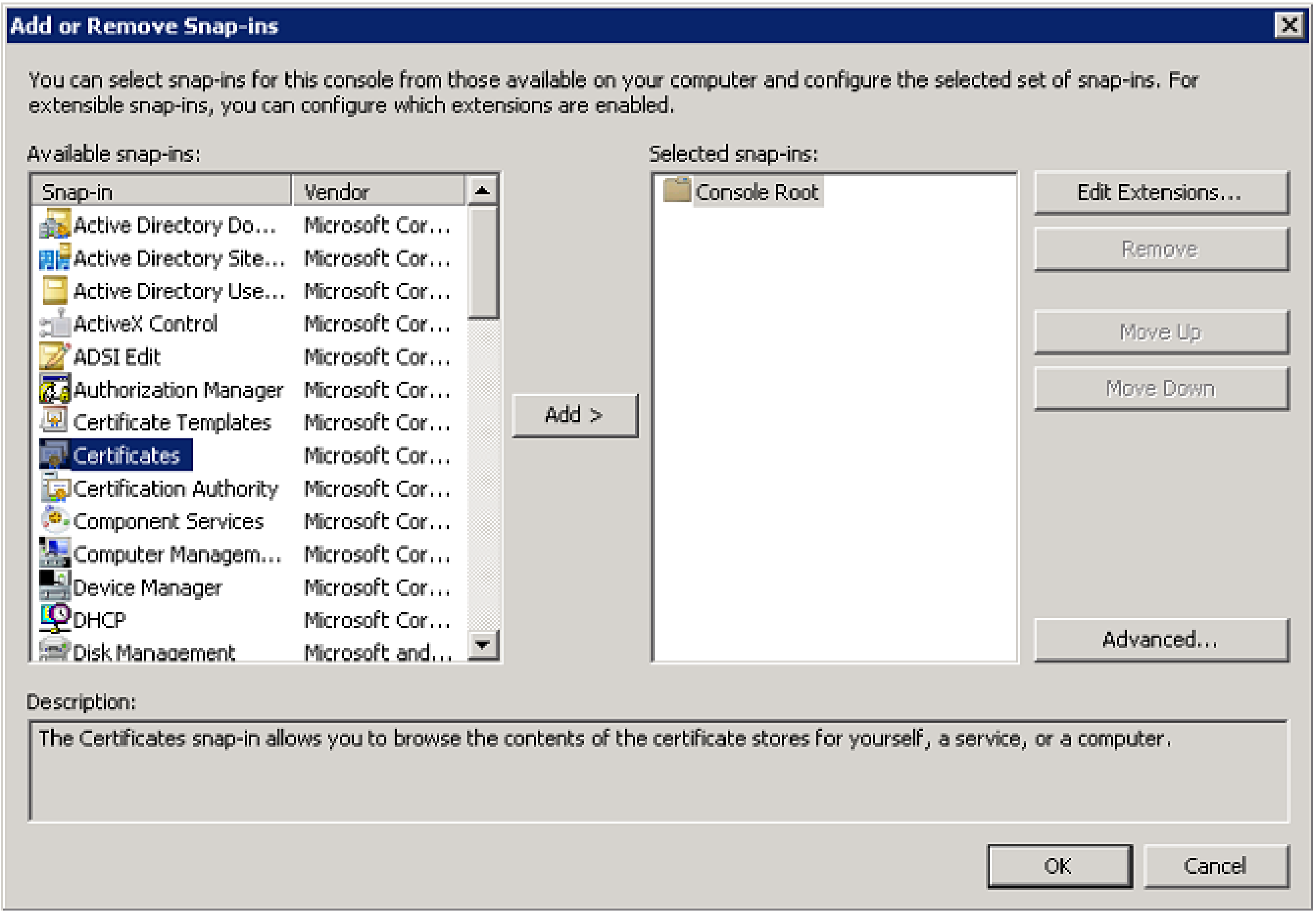
Install a Certificate

Complete these steps in order to install the computer certificate for the NPS:

1. Click **Start**, enter the Microsoft Management Console (MMC), and press **Enter**.

2. Navigate to **File** > **Add/Remove Snap-in**.

3. Choose **Certificates** and click **Add**.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
DHCP	Microsoft Cor...
Disk Management	Microsoft and...

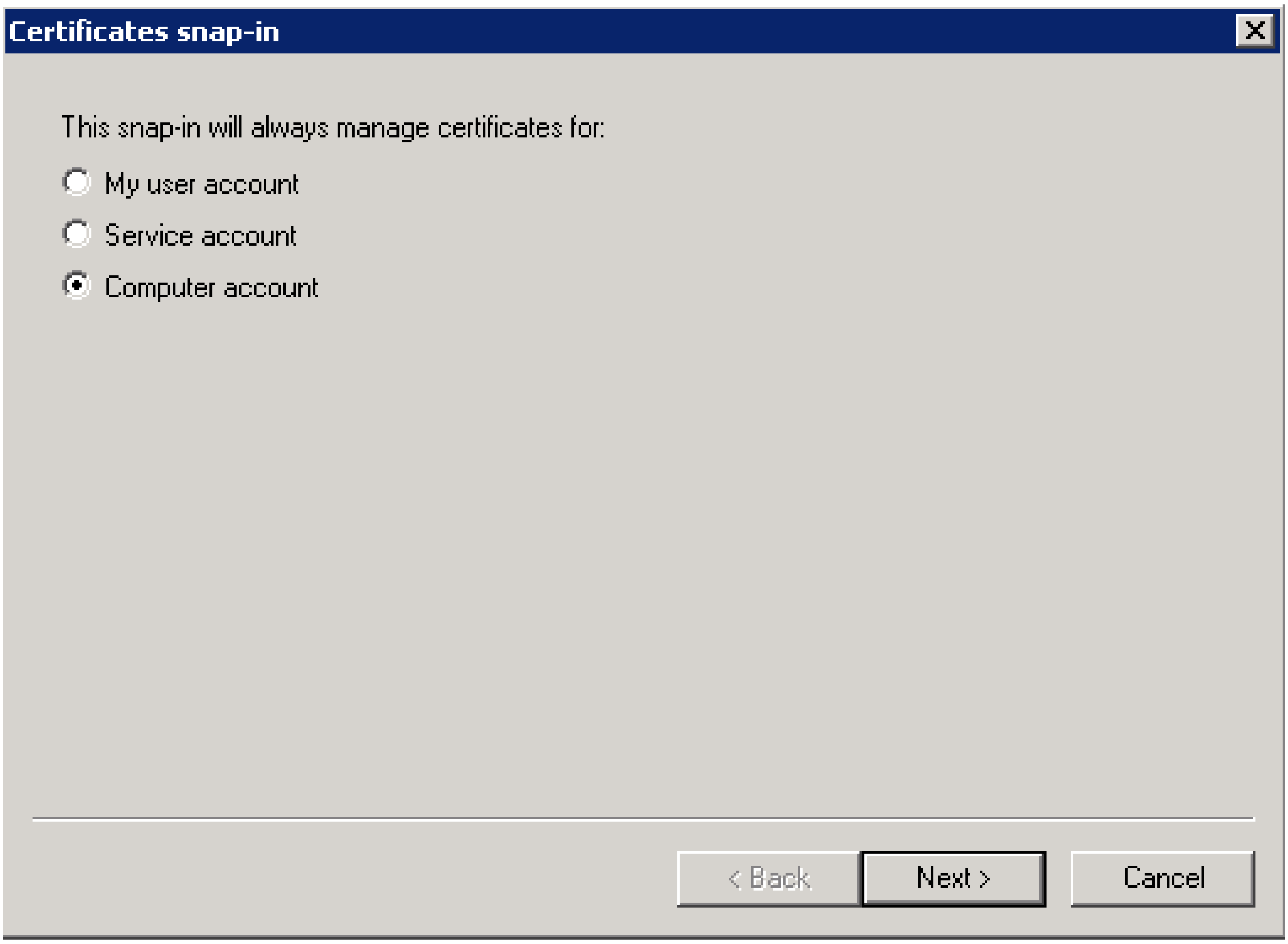
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

4. Click the **Computer account** radio button and click **Next**.



Certificates snap-in

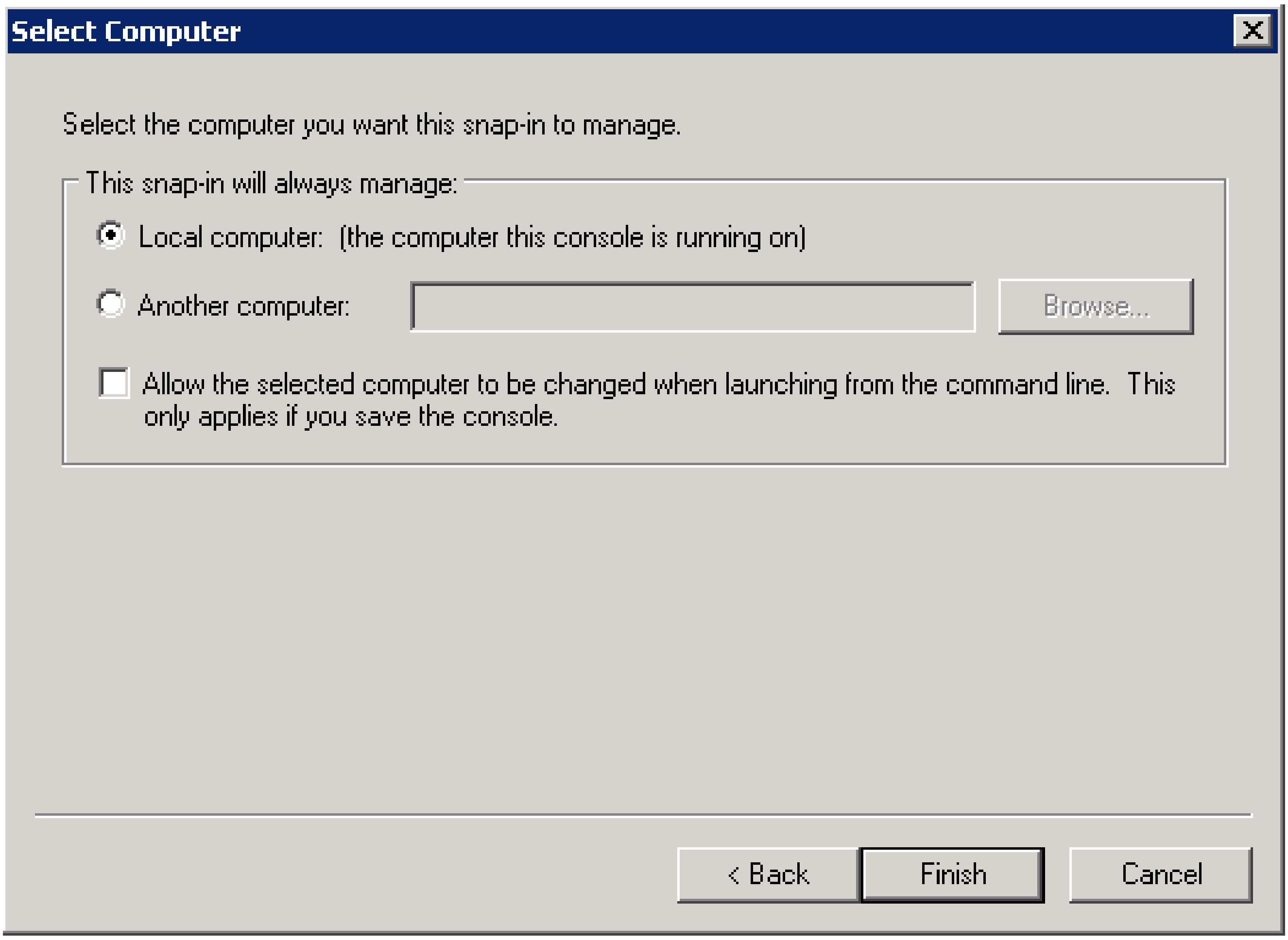
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

5. Click the **Local Computer** radio buttonand click **Finish**.



Select Computer

Select the computer you want this snap-in to manage.

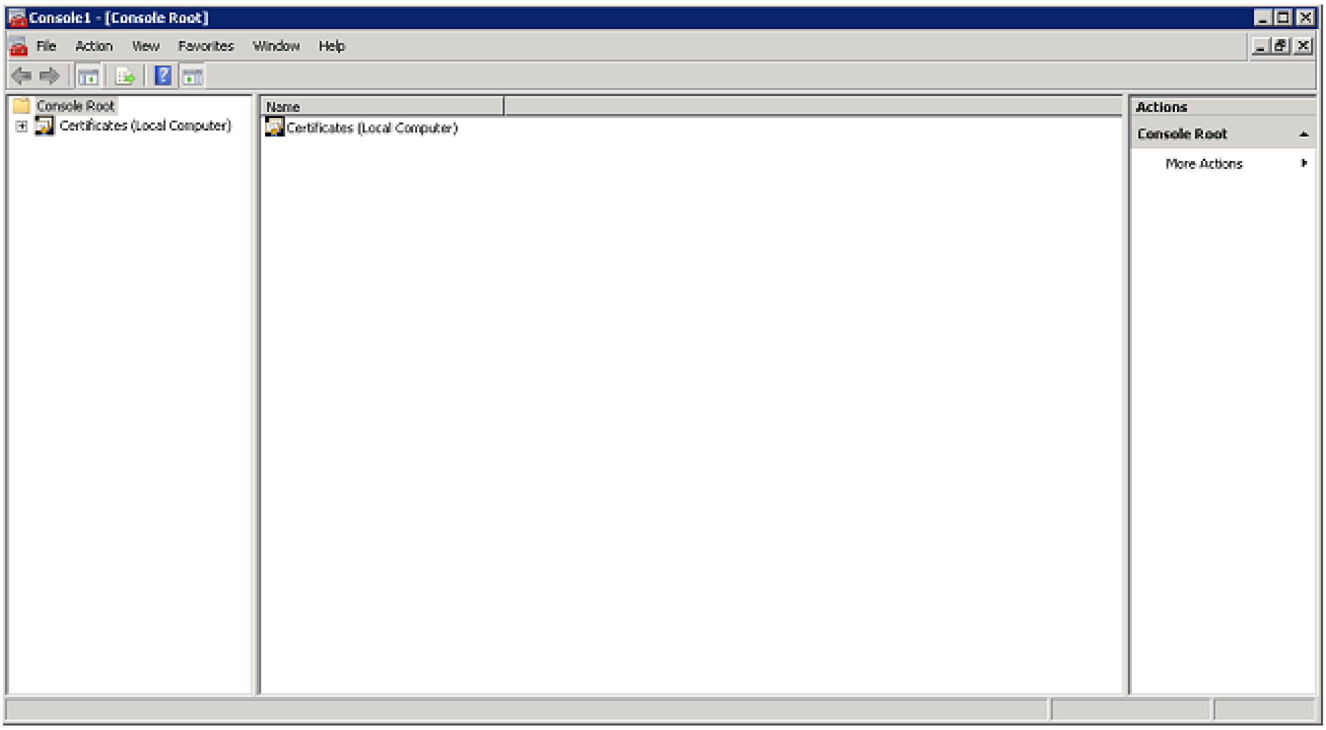
This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

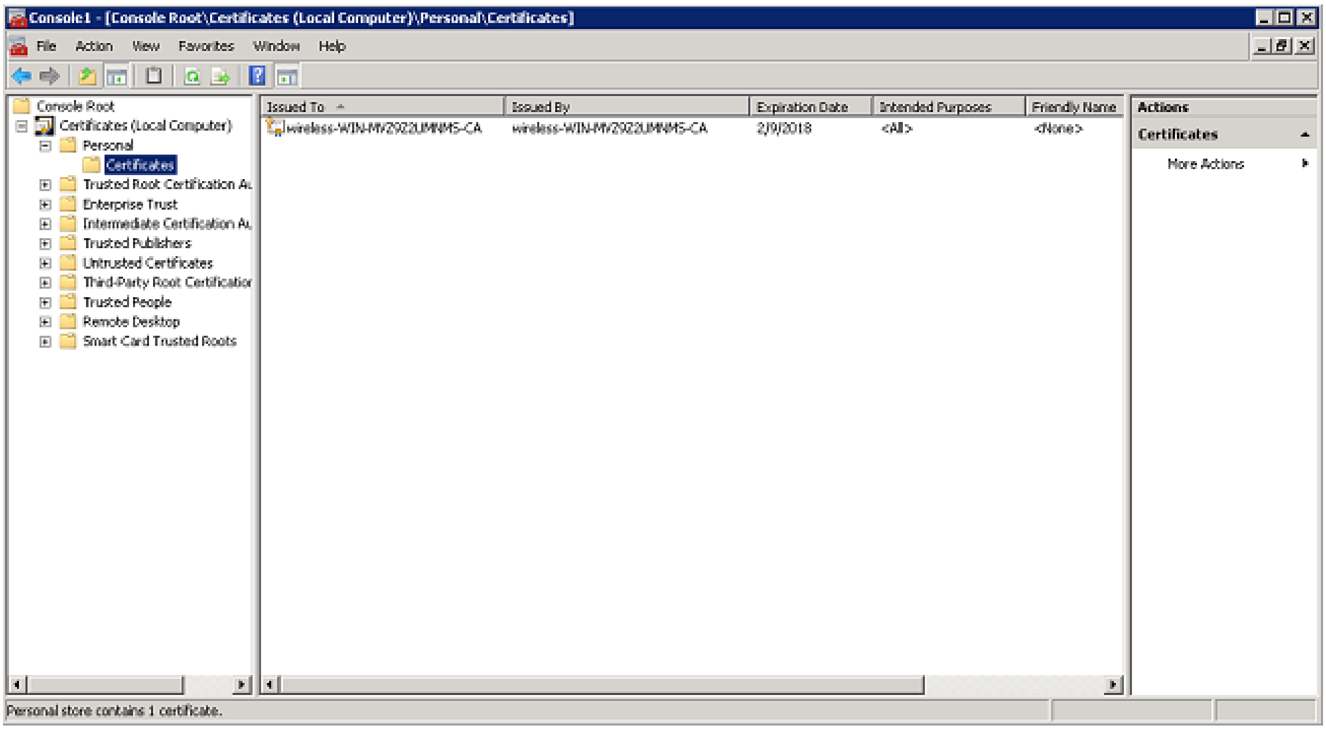
□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

6. Click **OK** in order to return to the MMC.



Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Name
Certificates (Local Computer)
Actions
Console Root
More Actions

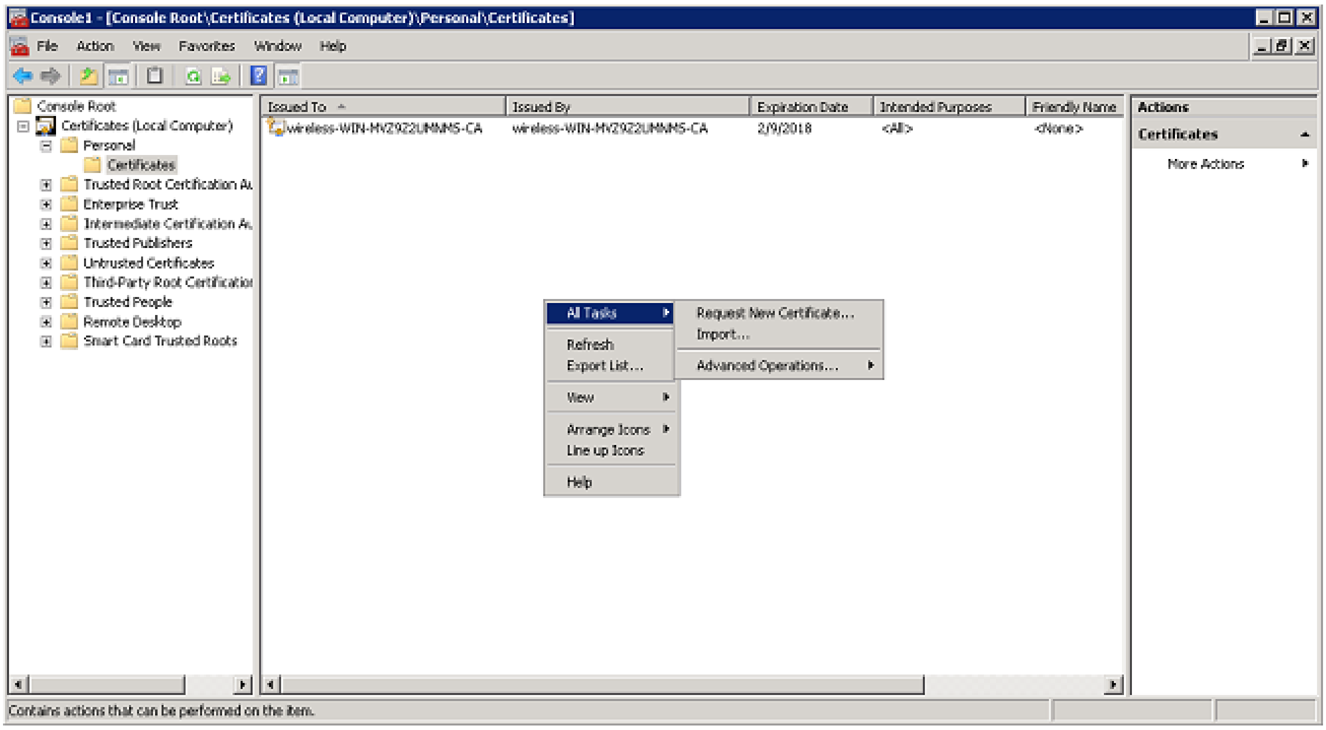
7. Expand the **Certificates (Local Computer)** and **Personal** folders, and click **Certificates**.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
wireless-WIN-MVZ9Z2UMNMS-CA	wireless-WIN-MVZ9Z2UMNMS-CA	2/9/2018	<All>	<None>

Personal store contains 1 certificate.

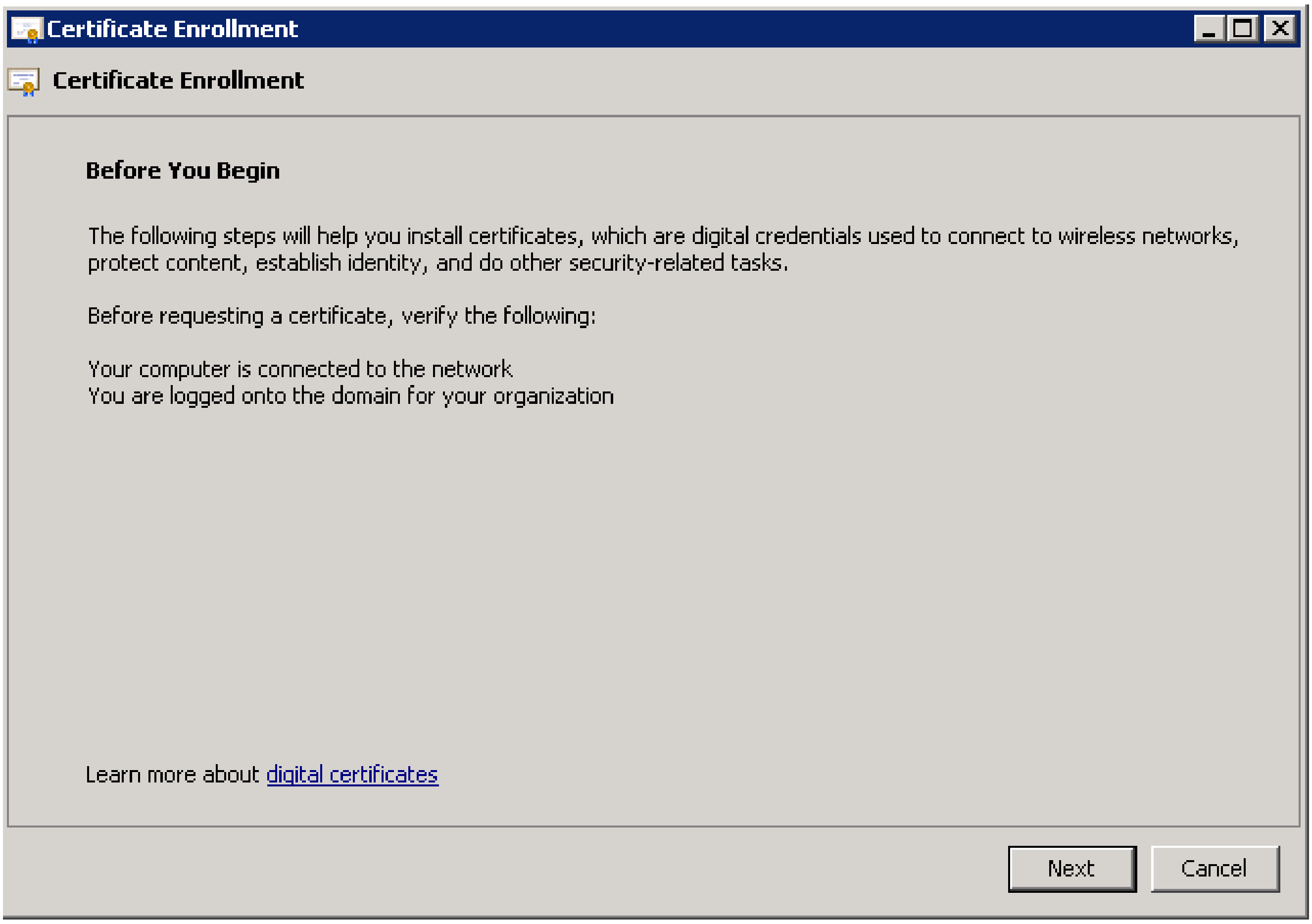
8. Right-click the white space in the CA certificate, and choose **All Tasks** > **Request New Certificate**.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
wireless-WIN-MVZ9Z2UMNMS-CA	wireless-WIN-MVZ9Z2UMNMS-CA	2/9/2018	<All>	<None>

Contains actions that can be performed on the item.

9. Click **Next**.



Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

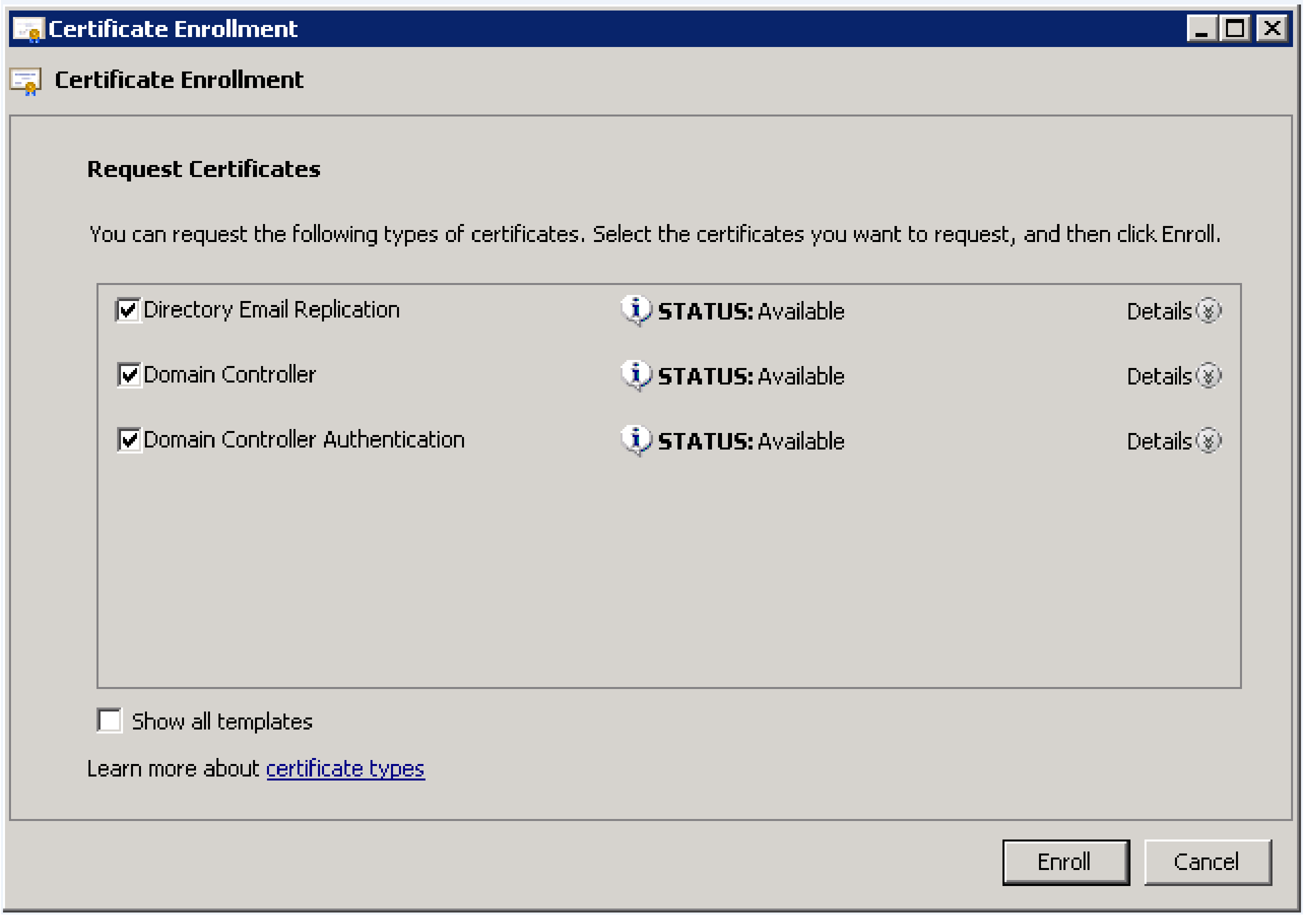
Before requesting a certificate, verify the following:

Your computer is connected to the network
You are logged onto the domain for your organization

Learn more about digital certificates

10. Click the **Domain Controller** check box, and click **Enroll**.

    Note: If the client authentication fails due to an EAP certificate error, then ensure that all of the check boxes are checked on this **Certificate Enrollment** page before you click **Enroll**. This creates approximately three certificates.



Certificate Enrollment

Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

☑ Directory Email Replication — STATUS: Available — Details

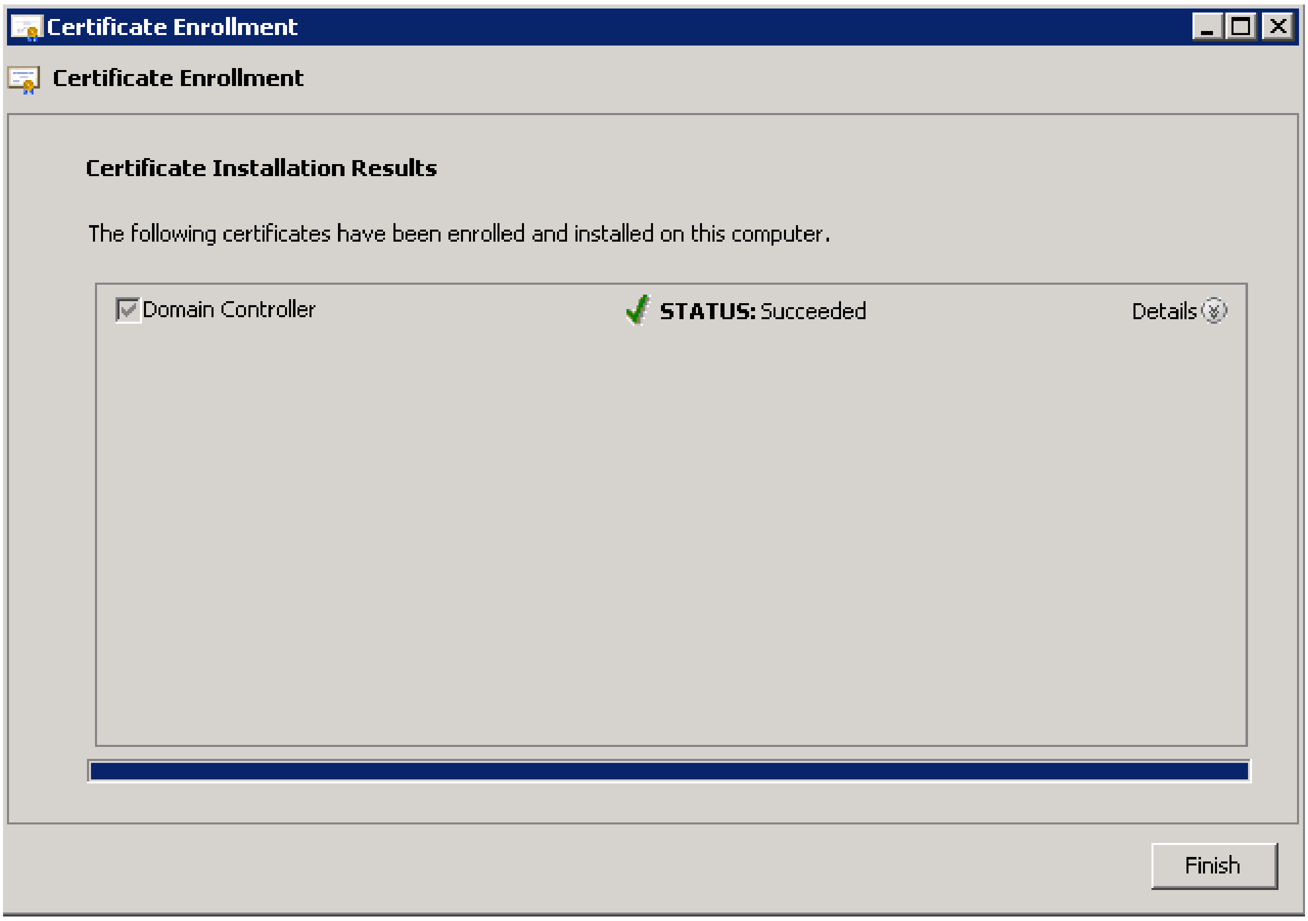
☑ Domain Controller — STATUS: Available — Details

☑ Domain Controller Authentication — STATUS: Available — Details

□ Show all templates

Learn more about certificate types

11. Click **Finish** once the certificate is installed.



Certificate Enrollment

Certificate Enrollment

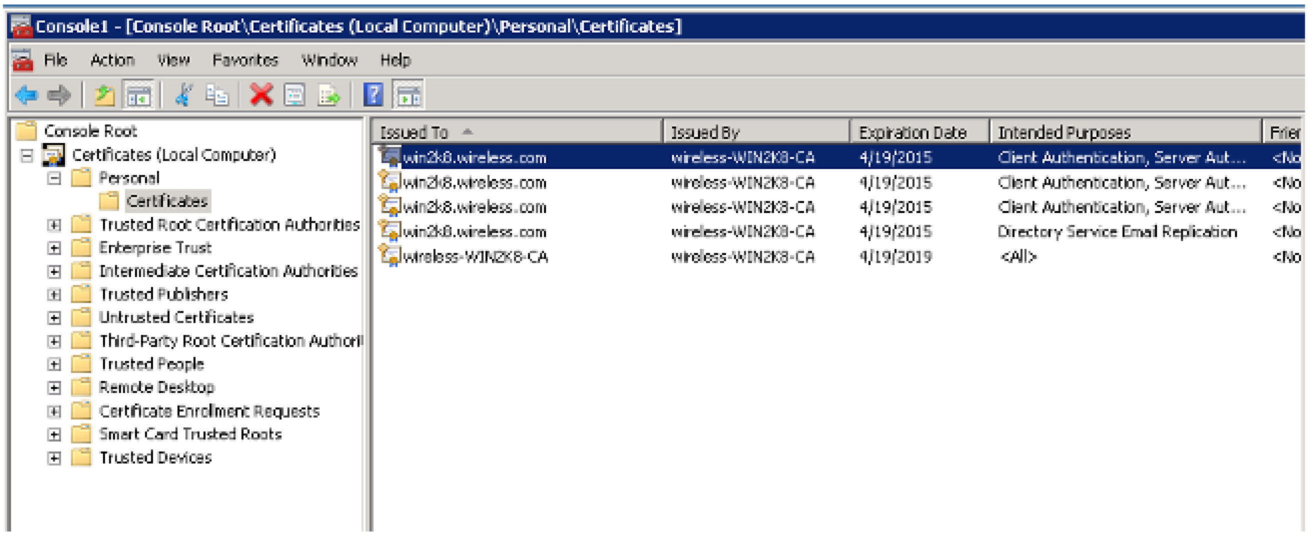
Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

☑ Domain Controller — ✓ STATUS: Succeeded — Details

The NPS certificate is now installed.

12. Ensure that **Client Authentication, Server Authentication** appears in the Intended Purposes column for the certificate.



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authori
Trusted People
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices

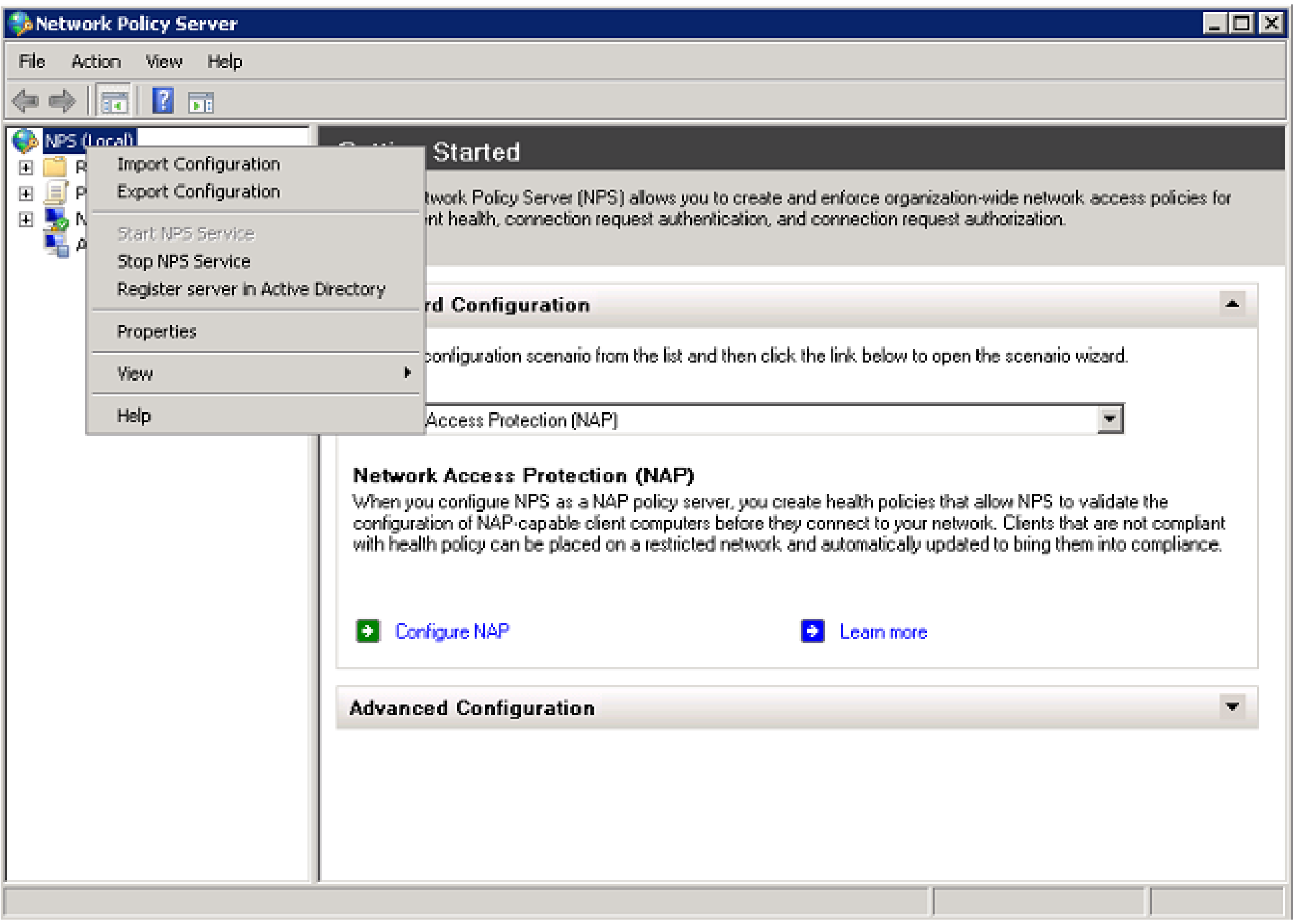
Issued To	Issued By	Expiration Date	Intended Purposes	Frier
win2k8.wireless.com	wireless-WIN2K8-CA	4/19/2015	Client Authentication, Server Aut...	<No
win2k8.wireless.com	wireless-WIN2K8-CA	4/19/2015	Client Authentication, Server Aut...	<No
win2k8.wireless.com	wireless-WIN2K8-CA	4/19/2015	Client Authentication, Server Aut...	<No
win2k8.wireless.com	wireless-WIN2K8-CA	4/19/2015	Directory Service Email Replication	<No
wireless-WIN2K8-CA	wireless-WIN2K8-CA	4/19/2019	<All>	<No

Configure the Network Policy Server Service for PEAP-MS-CHAP v2 Authentication

Complete these steps in order to configure the NPS for authentication:

1. Navigate to **Start > Administrative Tools** > **Network Policy Server**.

2. Right-click **NPS (Local)**and choose **Register server in Active Directory**.



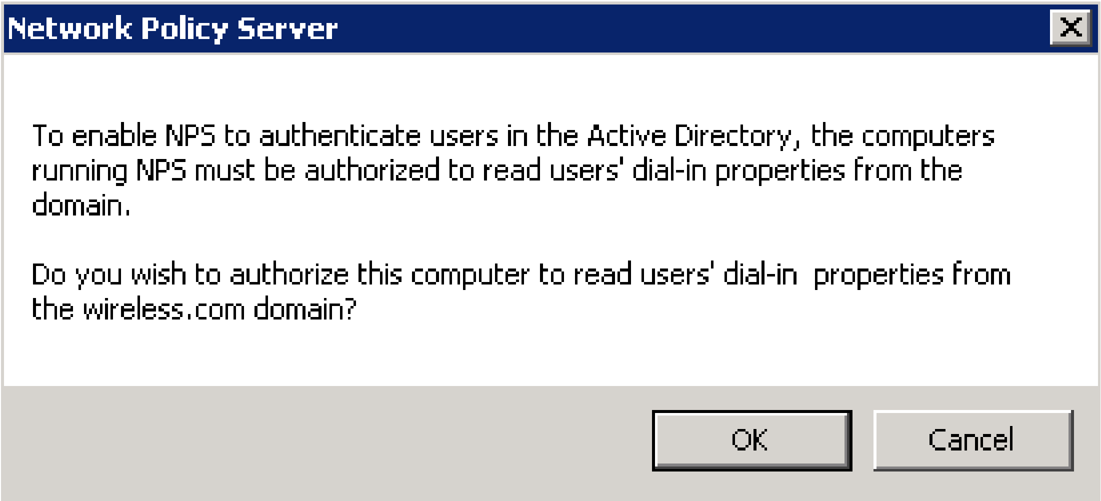
twork Policy Server (NPS) allows you to create and enforce organization-wide network access policies for nt health, connection request authentication, and connection request authorization.

configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP)

When you configure NPS as a NAP policy server, you create health policies that allow NPS to validate the configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.

3. Click **OK**.

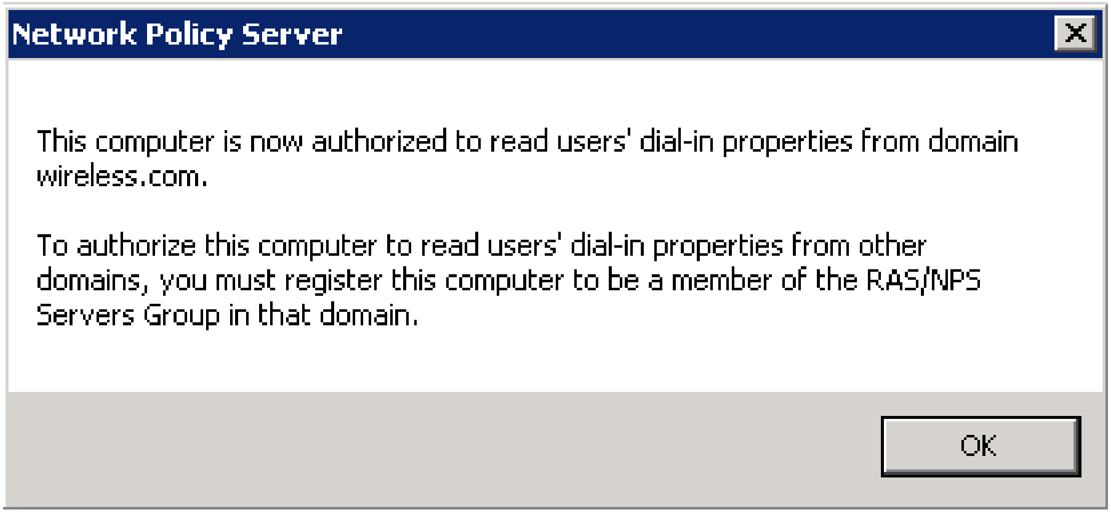


Network Policy Server

To enable NPS to authenticate users in the Active Directory, the computers running NPS must be authorized to read users' dial-in properties from the domain.

Do you wish to authorize this computer to read users' dial-in properties from the wireless.com domain?

4. Click **OK**.



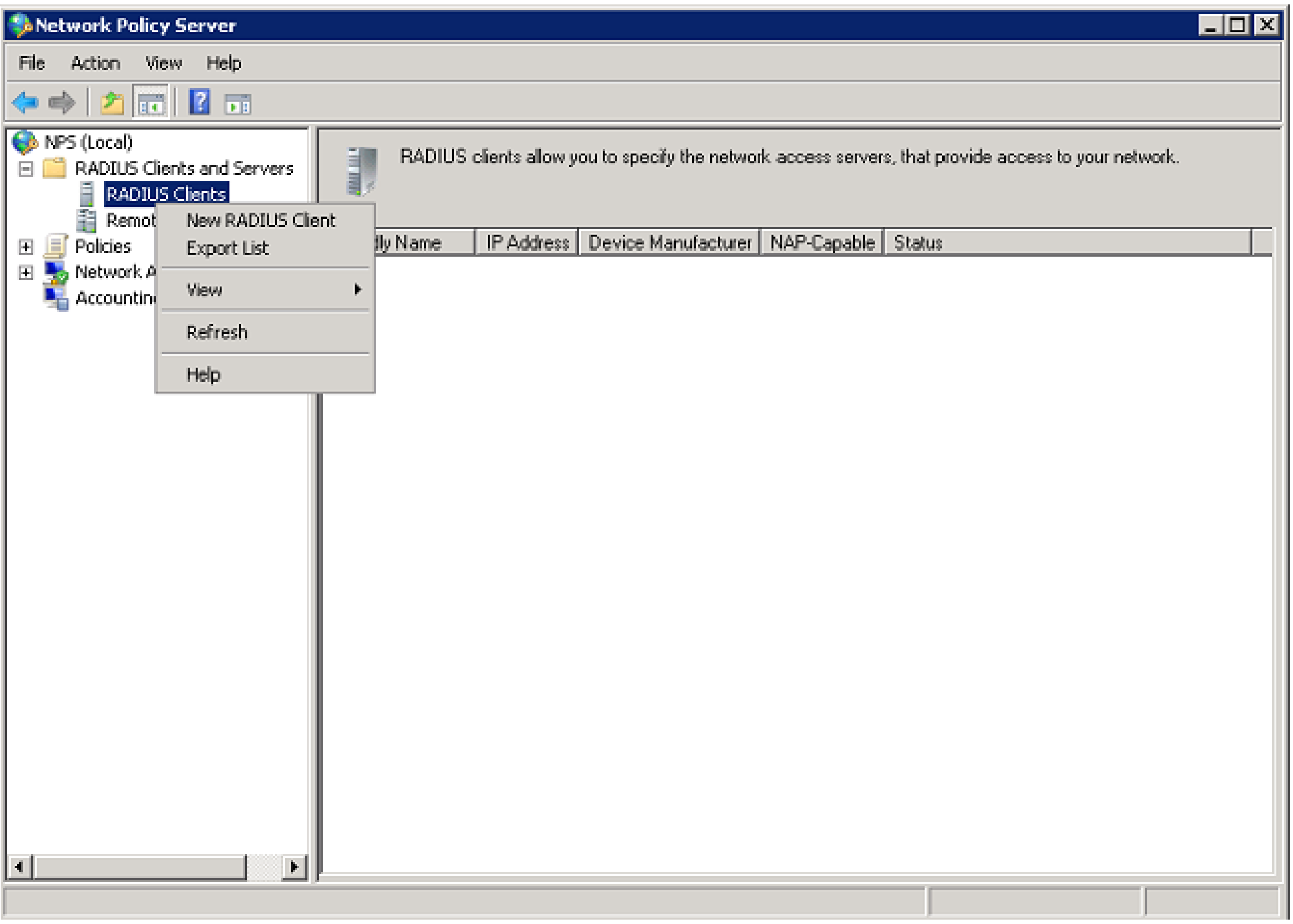
Network Policy Server

This computer is now authorized to read users' dial-in properties from domain wireless.com.

To authorize this computer to read users' dial-in properties from other domains, you must register this computer to be a member of the RAS/NPS Servers Group in that domain.

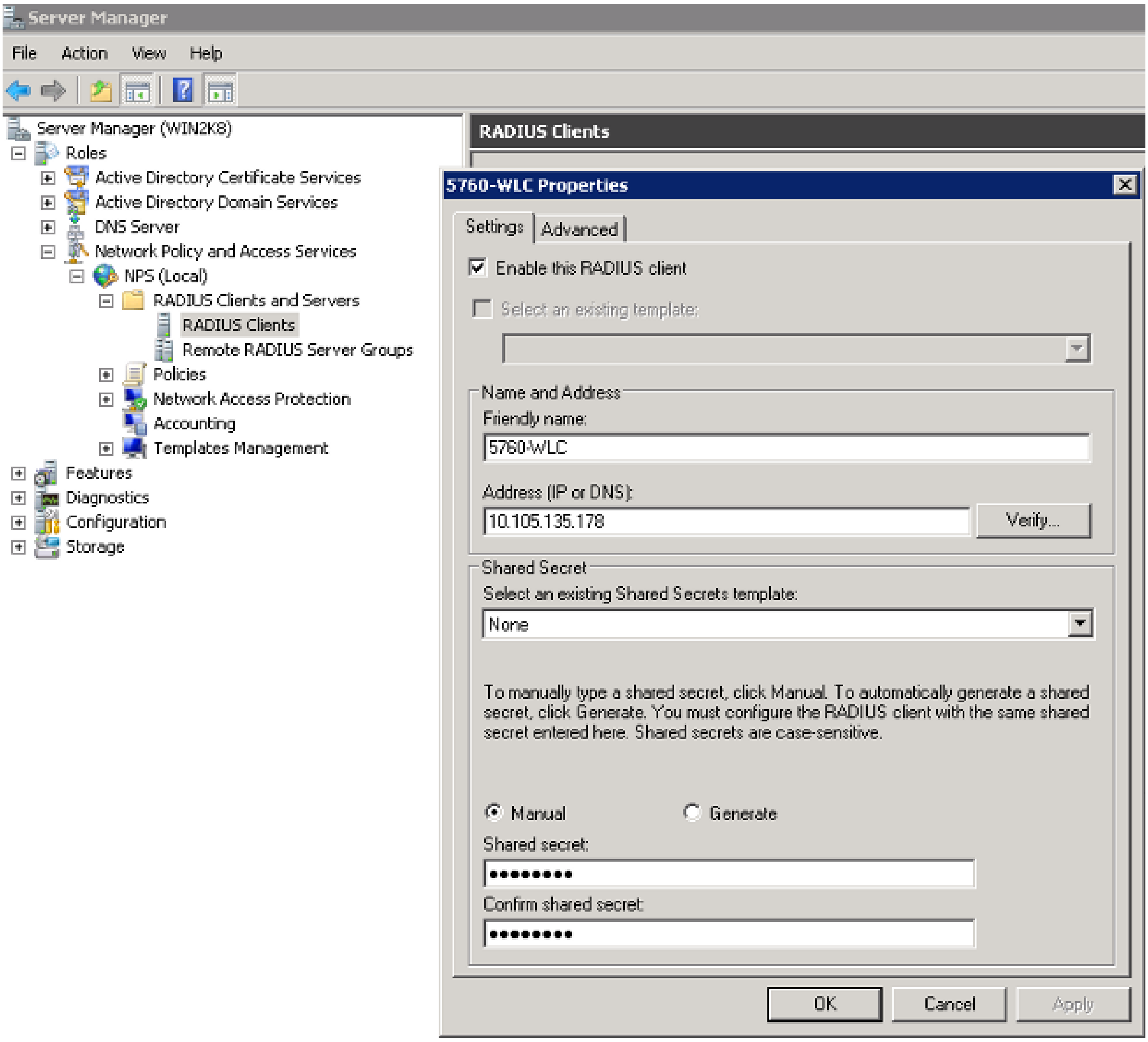
5. Add the WLC as an Authentication, Authorization, and Accounting (AAA) client on the NPS.

6. Expand **RADIUS Clients and Servers**. Right-click **RADIUS Clients** and choose **New RADIUS Client**:



7. Enter a name (**WLC** in this example), the management IP address of the WLC (**10.105.135.178** in this example), and a shared secret.

   Note: The same shared secret is used in order to configure the WLC.



☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: 5760-WLC

Address (IP or DNS): 10.105.135.178

Shared Secret

Select an existing Shared Secrets template: None

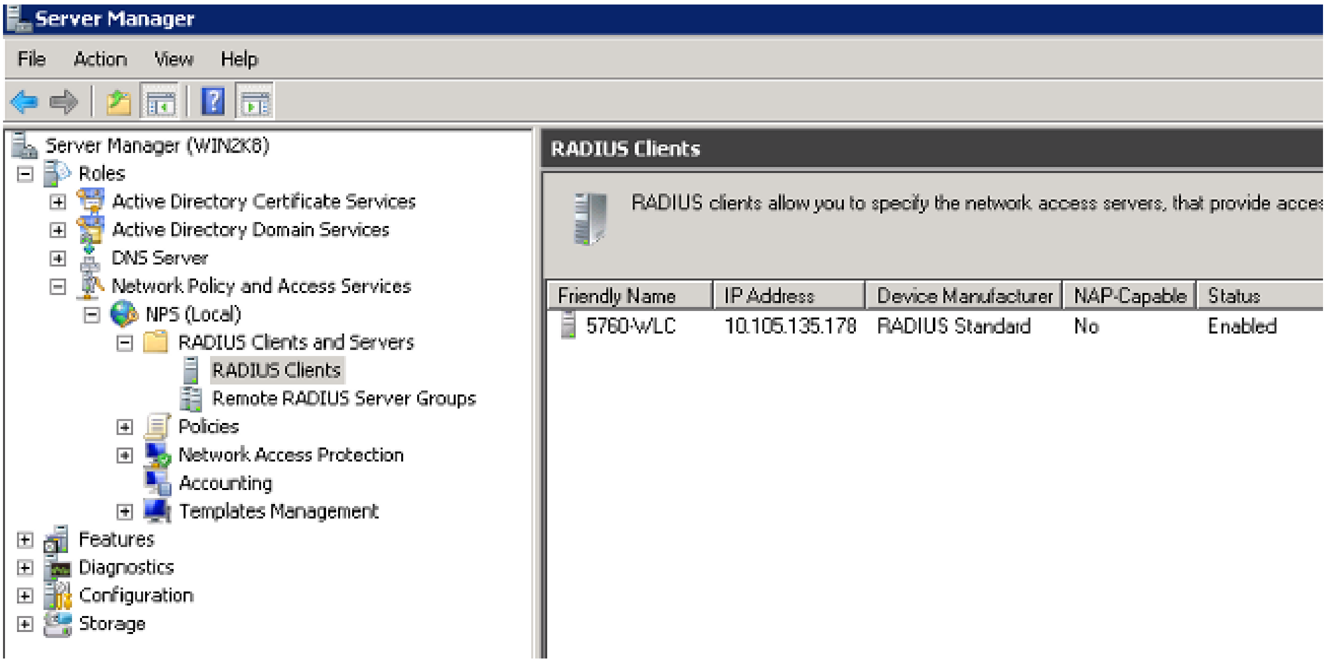
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: •••••••••

Confirm shared secret: •••••••••

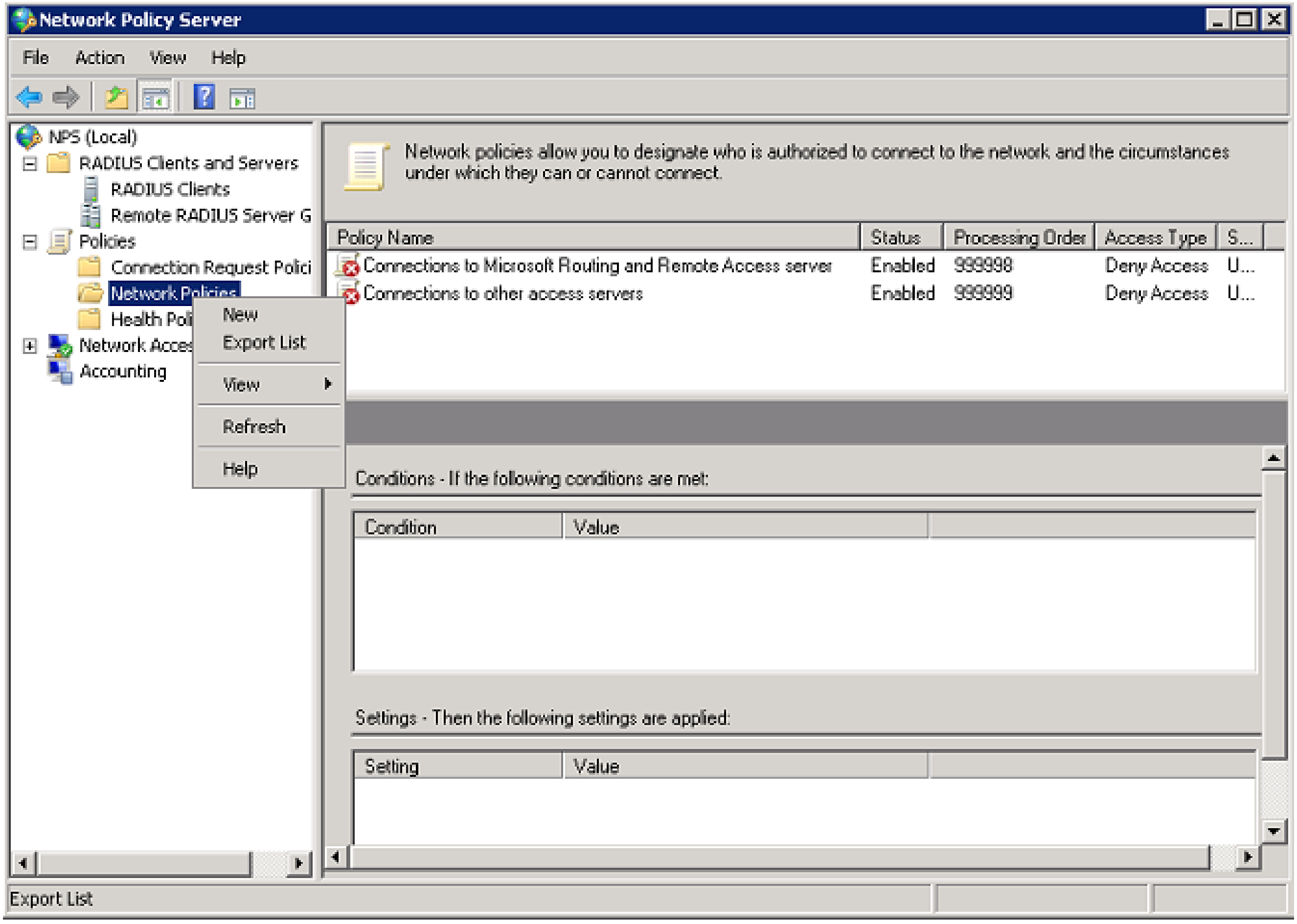
8. Click **OK** in order to return to the previous screen.



RADIUS clients allow you to specify the network access servers, that provide acces

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
5760-WLC	10.105.135.178	RADIUS Standard	No	Enabled

9. Create a new Network Policy for the wireless users. Expand **Policies**, right-click **Network Policies**,and choose **New**:



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	S...
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	U...
Connections to other access servers	Enabled	999999	Deny Access	U...

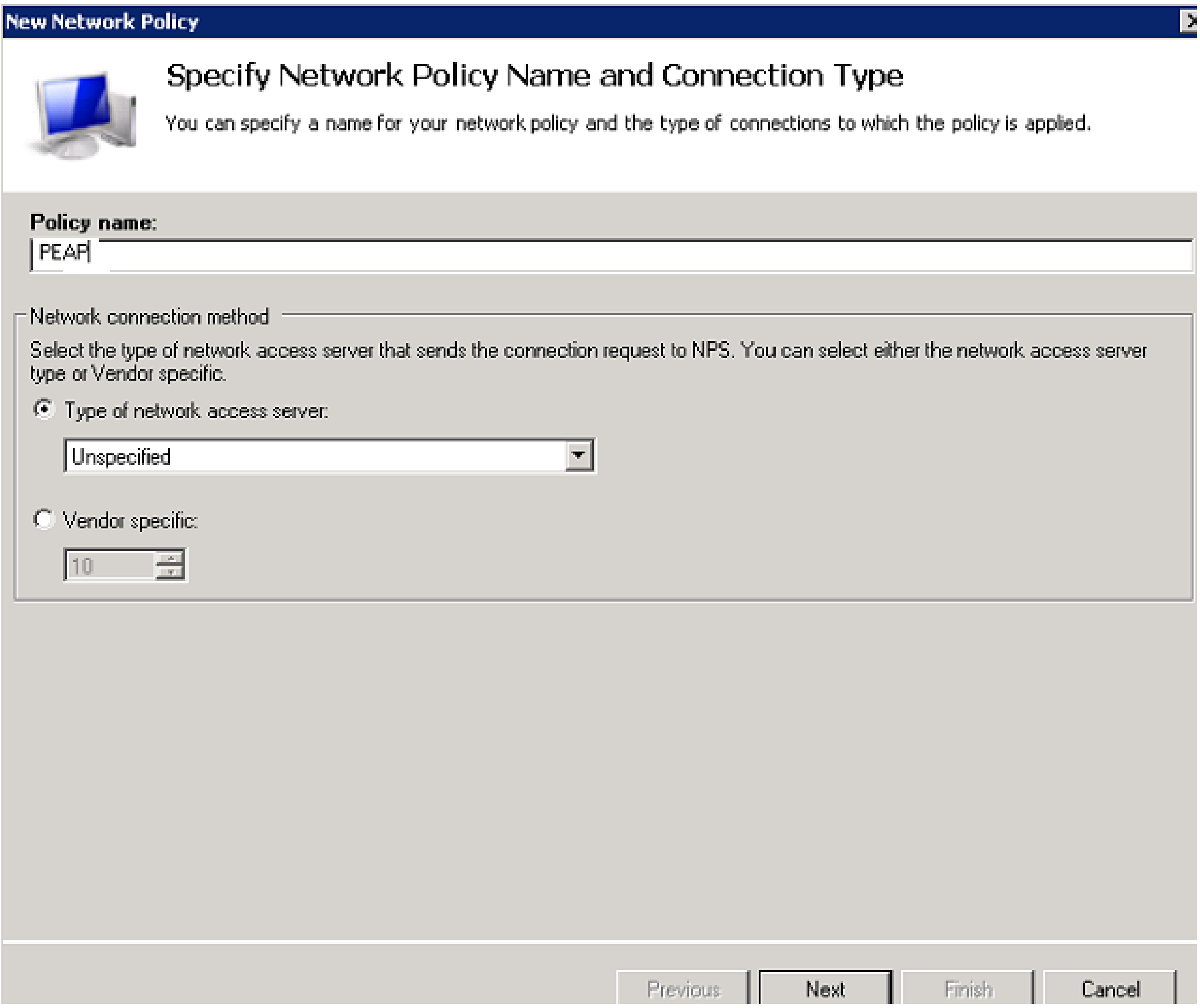
Conditions - If the following conditions are met:

Condition	Value

Settings - Then the following settings are applied:

Setting	Value

10. Enter a policy name for this rule (**PEAP** in this example) and click **Next.**



Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name: PEAP

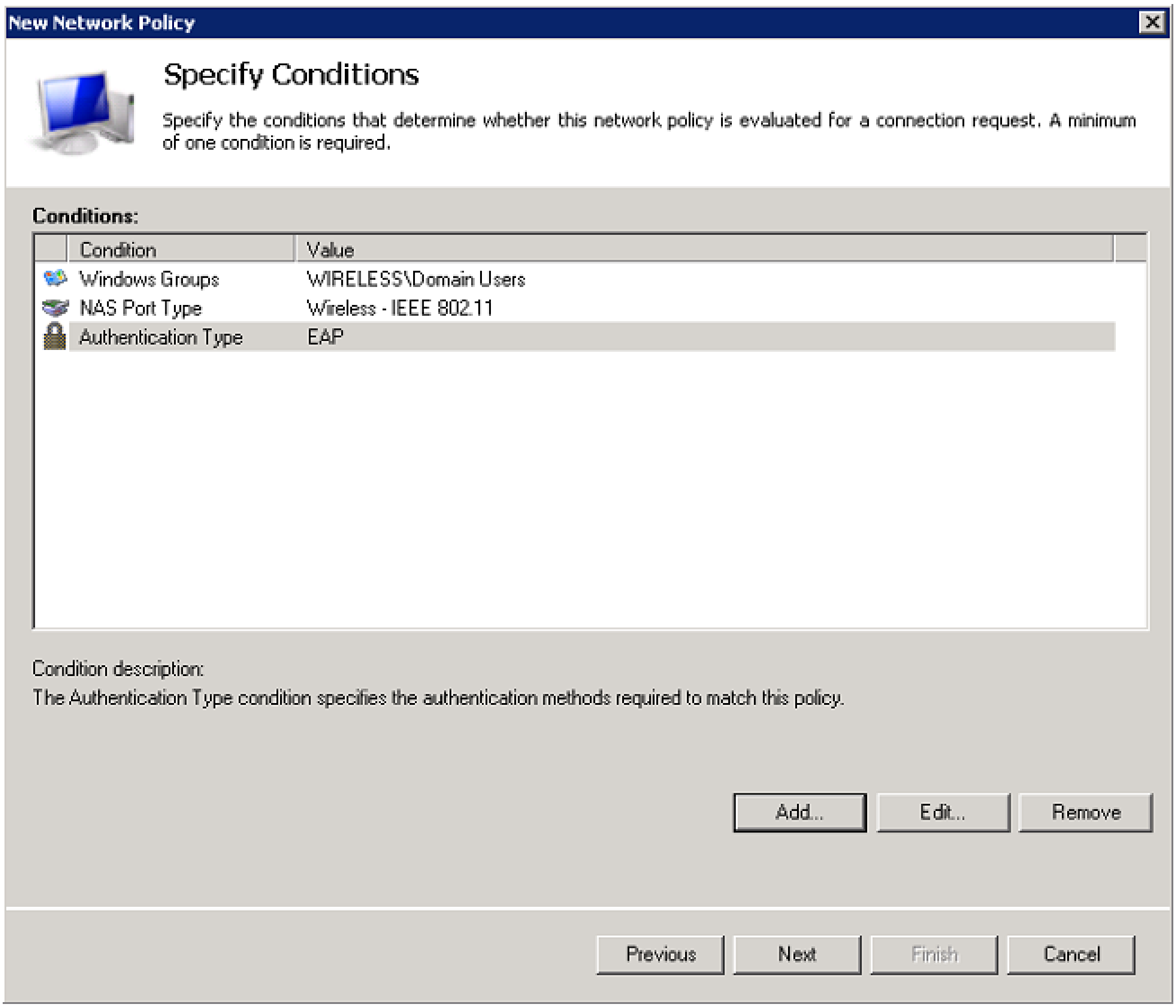
Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

● Type of network access server: Unspecified

○ Vendor specific: 10

11. In order to configure this policy to allow only wireless domain users, add these three conditions and click **Next**:



Specify Conditions

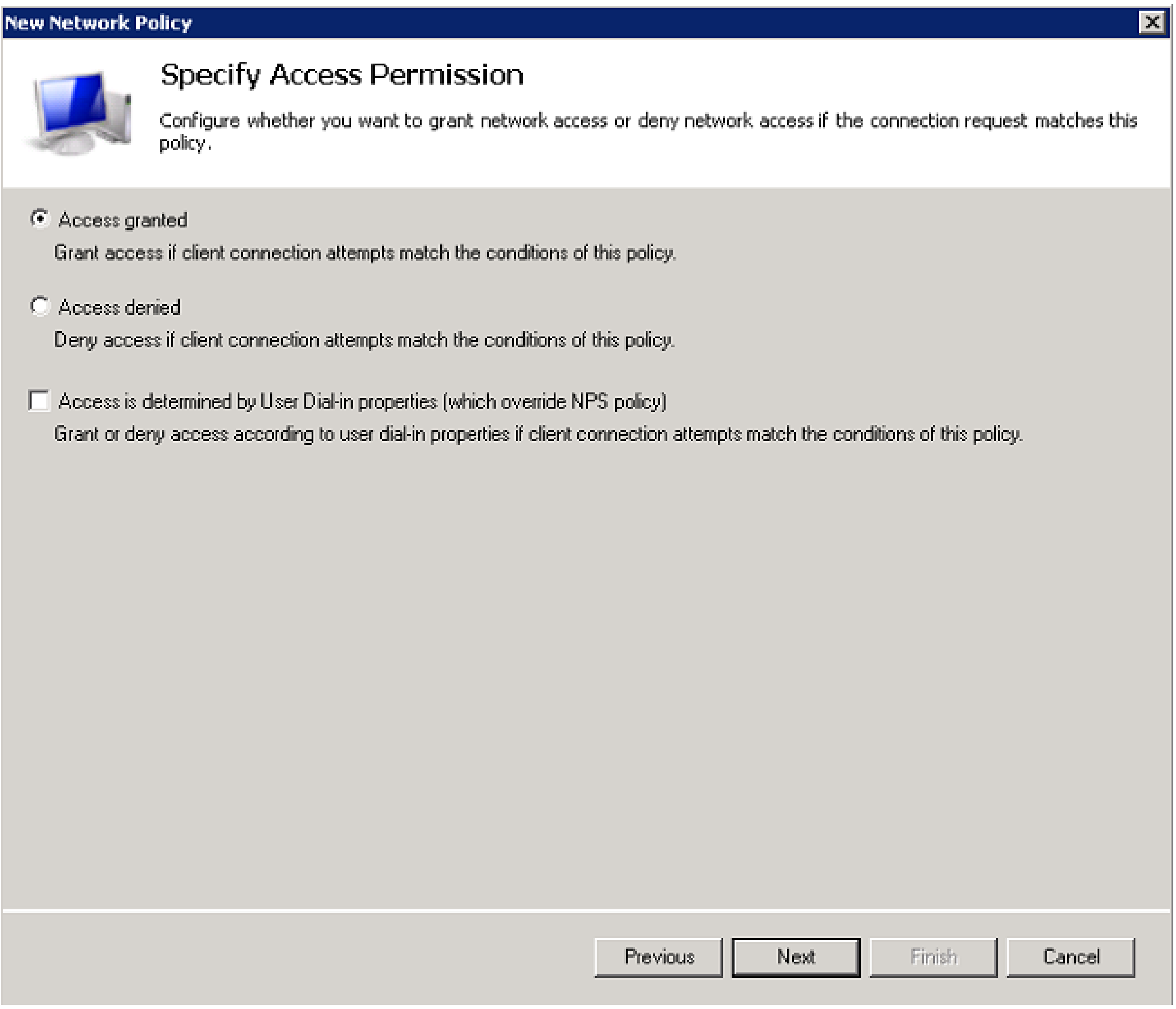
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
Windows Groups	WIRELESS\Domain Users
NAS Port Type	Wireless - IEEE 802.11
Authentication Type	EAP

Condition description:
The Authentication Type condition specifies the authentication methods required to match this policy.

12. Click the **Access granted** radio button in order to grant connection attempts that match this policy and click **Next**.



Specify Access Permission

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

● Access granted

Grant access if client connection attempts match the conditions of this policy.

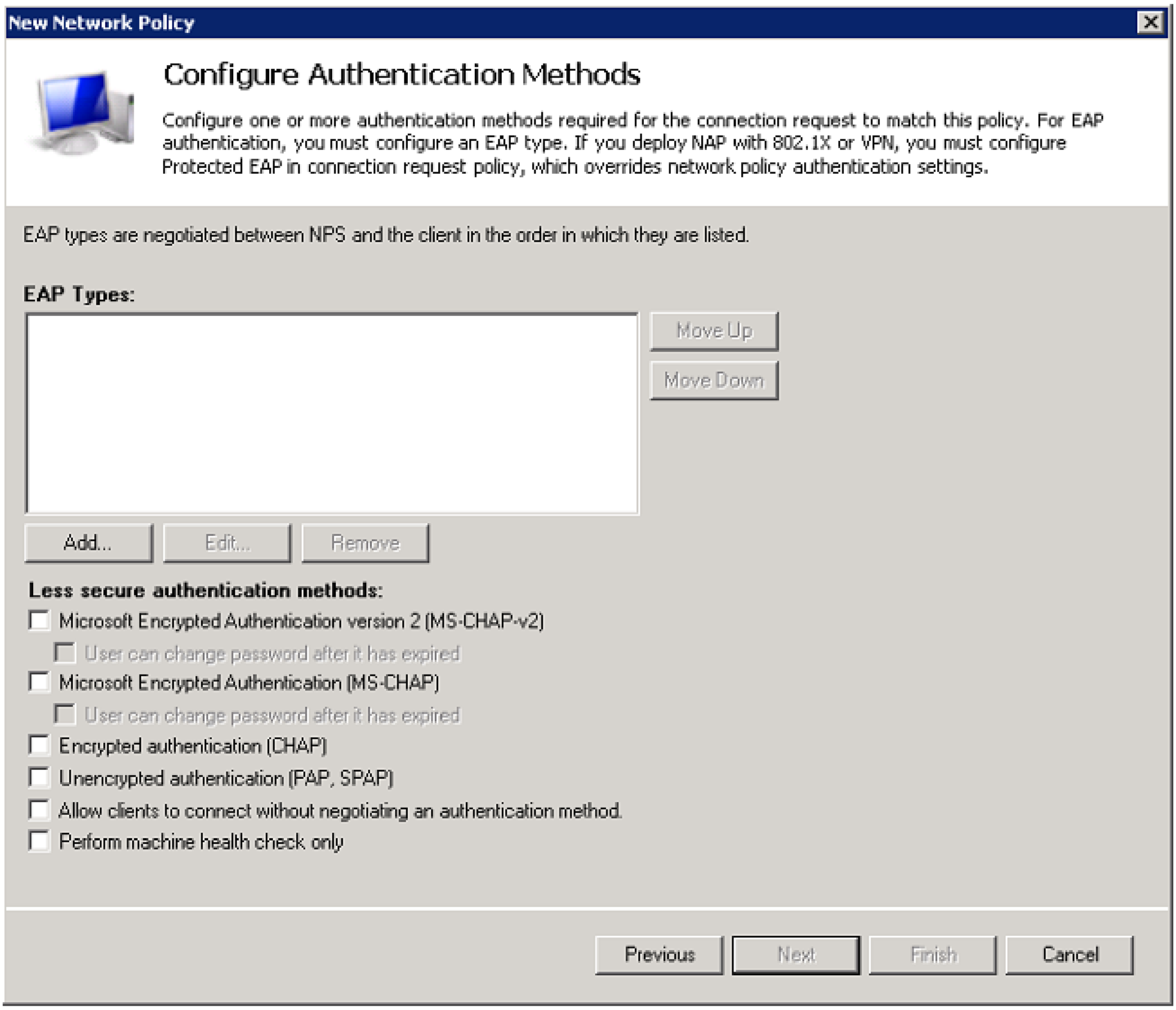
○ Access denied

Deny access if client connection attempts match the conditions of this policy.

□ Access is determined by User Dial-in properties (which override NPS policy)

Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

13. Disable all of the **Less secure authentication methods**:



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

☐ User can change password after it has expired

☐ Microsoft Encrypted Authentication (MS-CHAP)

☐ User can change password after it has expired

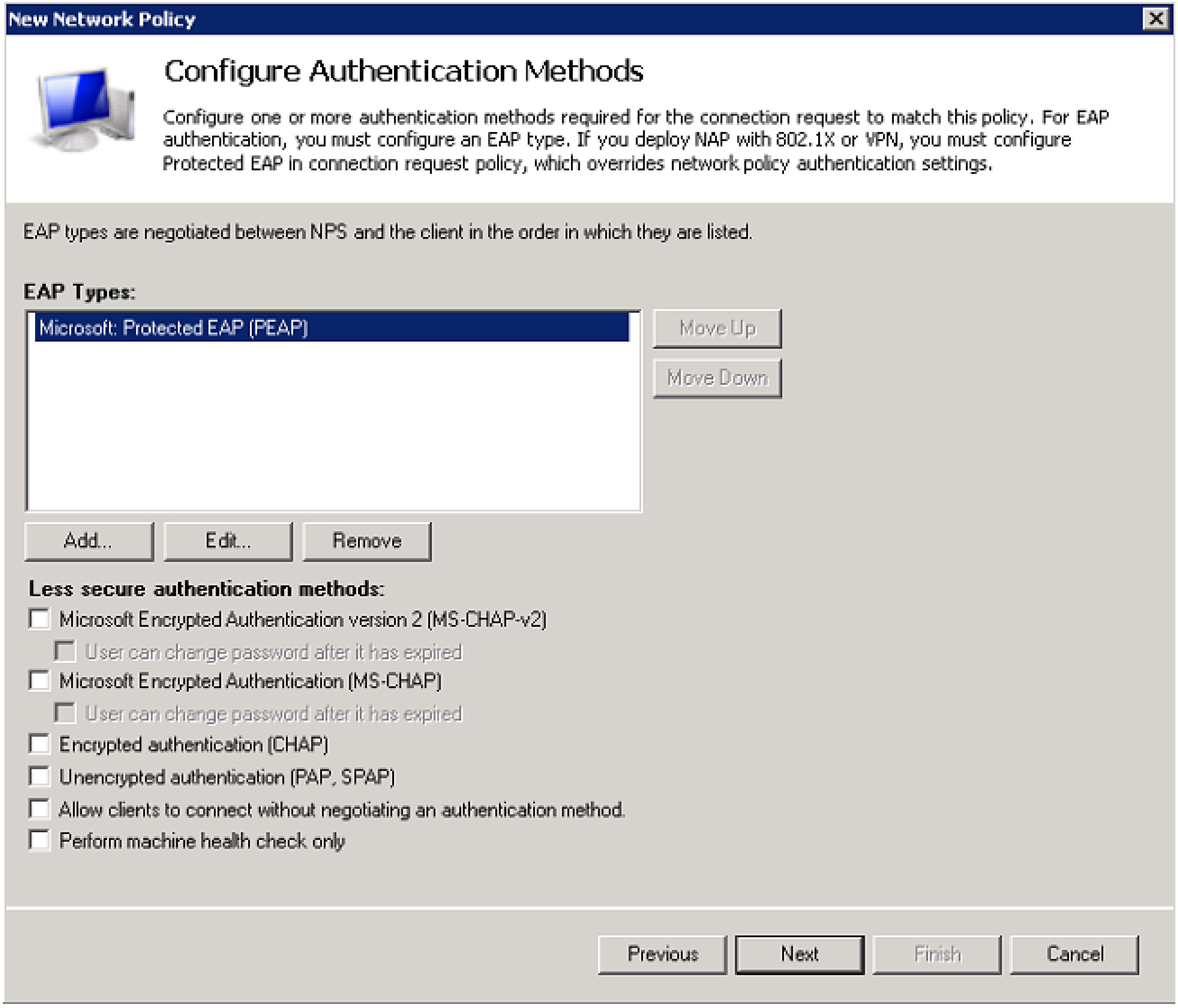
☐ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method.

☐ Perform machine health check only

14. Click **Add**, select the **Microsoft: Protected EAP (PEAP)**EAP Type, and click **OK** in order to enable PEAP.



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Microsoft: Protected EAP (PEAP)

Less secure authentication methods:

□ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

□ User can change password after it has expired

□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

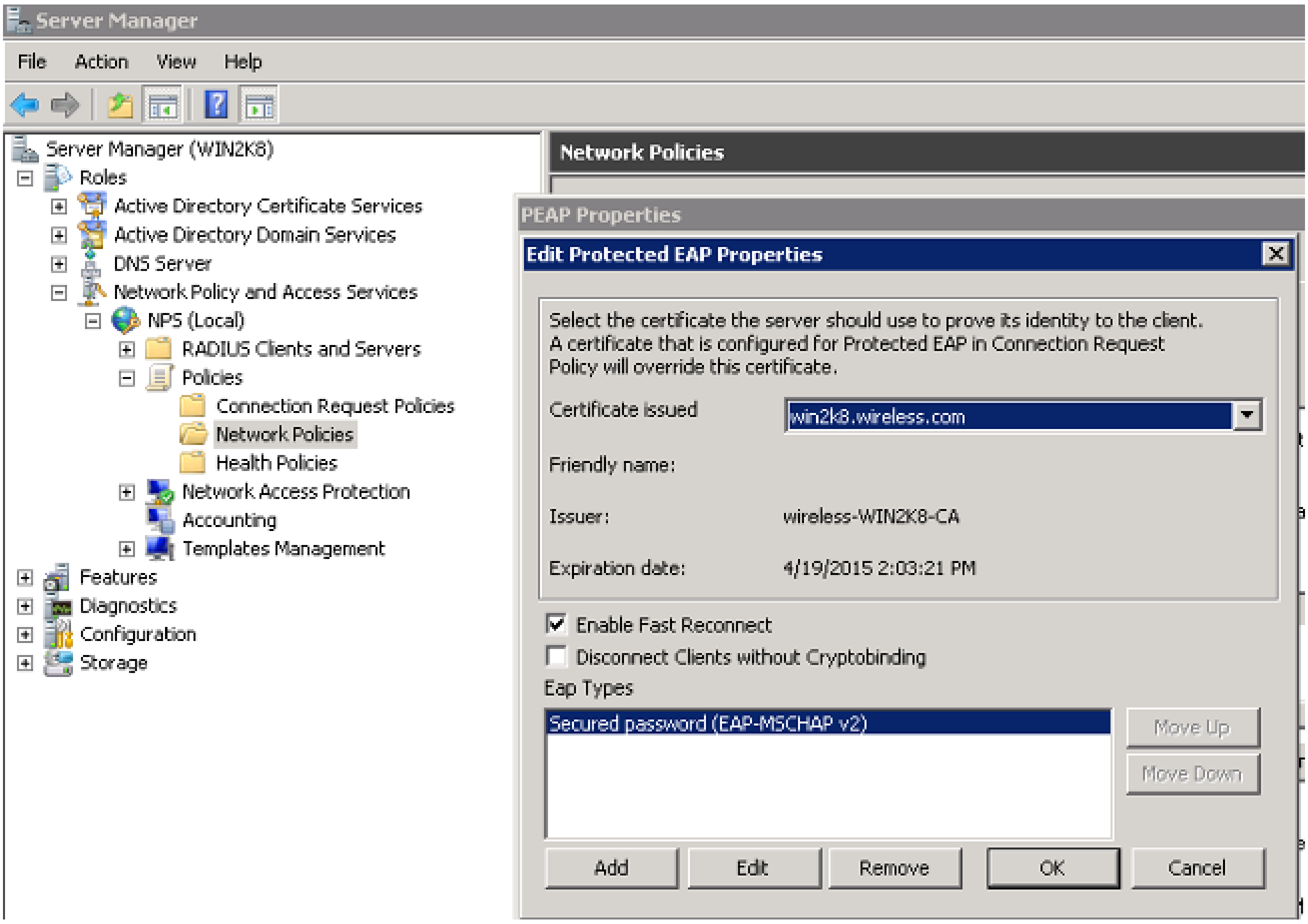
□ Encrypted authentication (CHAP)

□ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method.

□ Perform machine health check only

15. Select **Microsoft: Protected EAP (PEAP)** and click **Edit**. Ensure that the previously-created domain controller certificate is selected in the Certificate issued drop-down list and click **Ok**.



Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.

Certificate issued: win2k8.wireless.com

Friendly name:

Issuer: wireless-WIN2K8-CA

Expiration date: 4/19/2015 2:03:21 PM

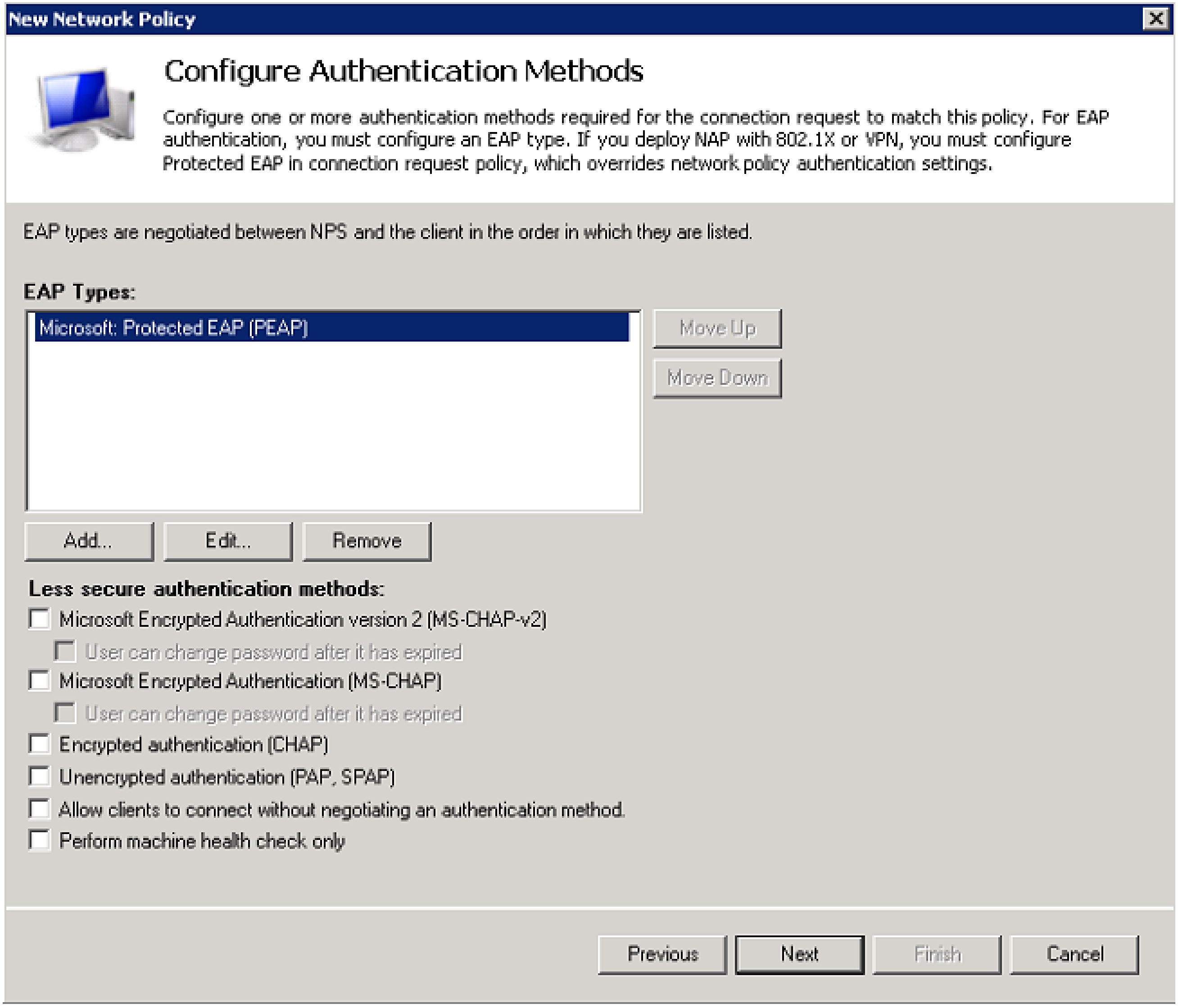
☑ Enable Fast Reconnect

□ Disconnect Clients without Cryptobinding

Eap Types

Secured password (EAP-MSCHAP v2)

16. Click **Next**.



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Microsoft: Protected EAP (PEAP)

Less secure authentication methods:

□ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

□ User can change password after it has expired

□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

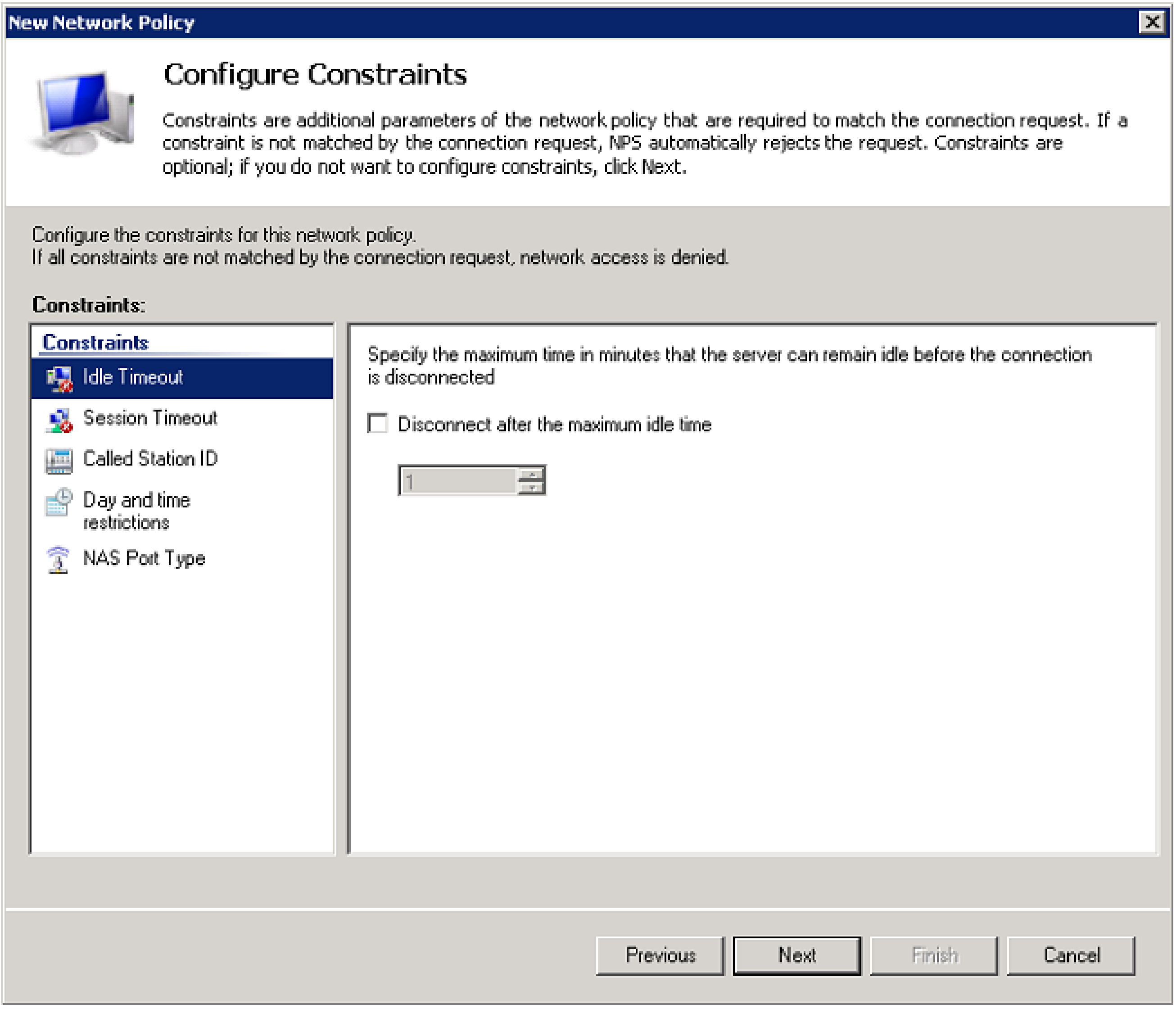
□ Encrypted authentication (CHAP)

□ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method.

□ Perform machine health check only

17. Click **Next**.



New Network Policy

Configure Constraints

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

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

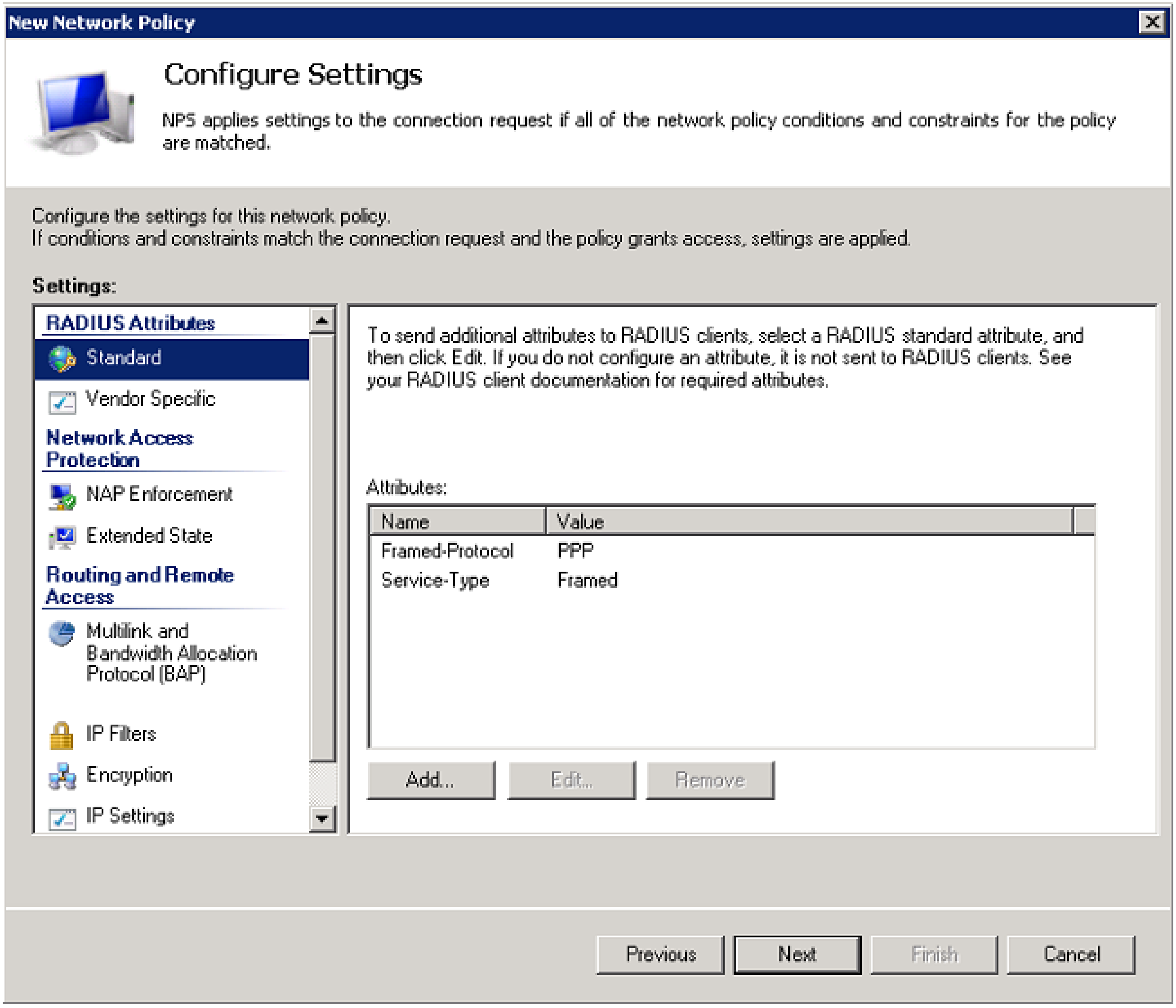
Constraints:

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

□ Disconnect after the maximum idle time

1

18. Click **Next**.



Configure Settings

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

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

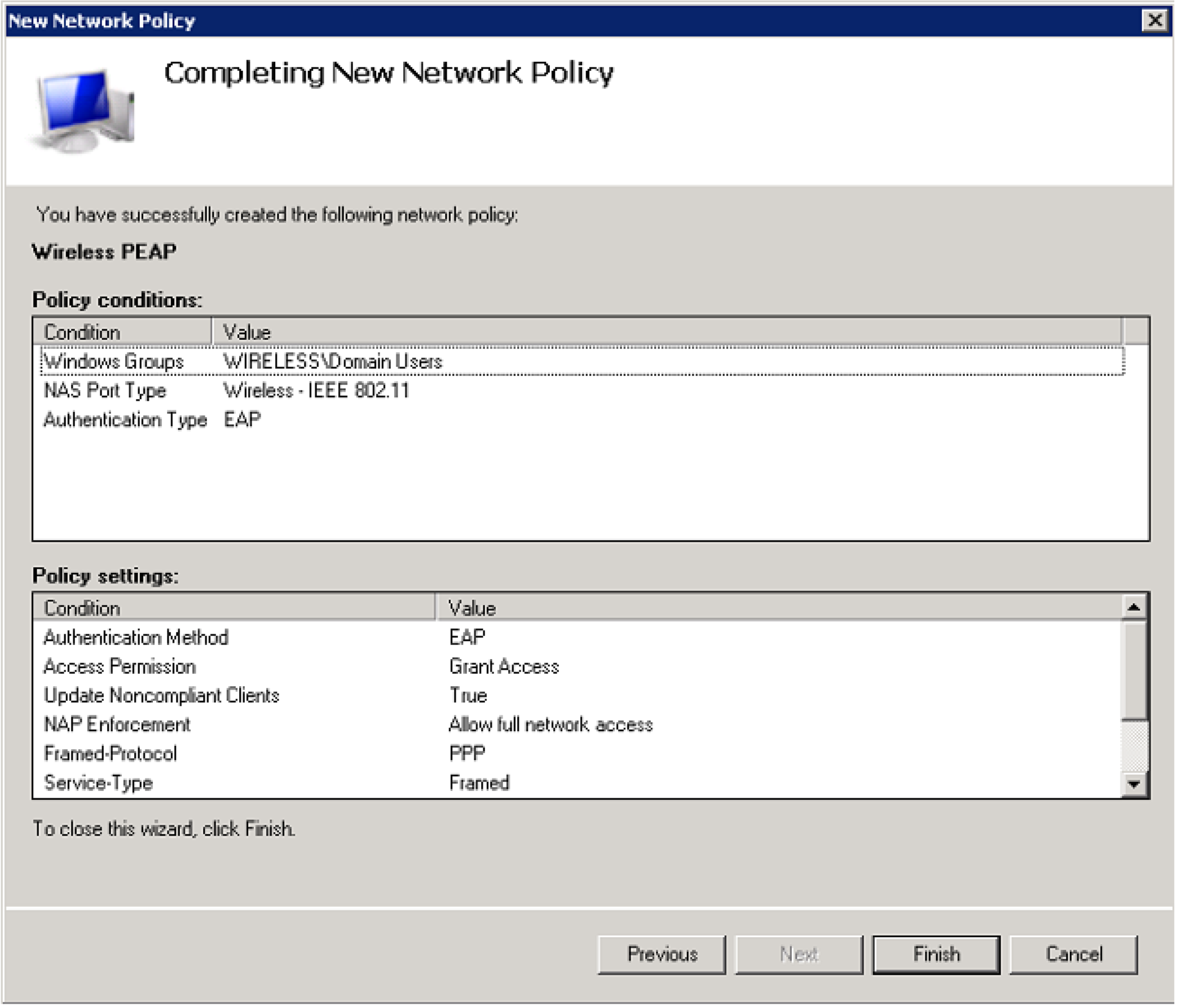
Settings:

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

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

19. Click **Finish**.



Completing New Network Policy

You have successfully created the following network policy:

Wireless PEAP

Policy conditions:

Condition	Value
Windows Groups	WIRELESS\Domain Users
NAS Port Type	Wireless - IEEE 802.11
Authentication Type	EAP

Policy settings:

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

To close this wizard, click Finish.

Note: Dependent upon your needs, you might need to configure **Connection Request Policies** on the NPS in order to allow the PEAP profile or the policy.

Add Users to the Active Directory

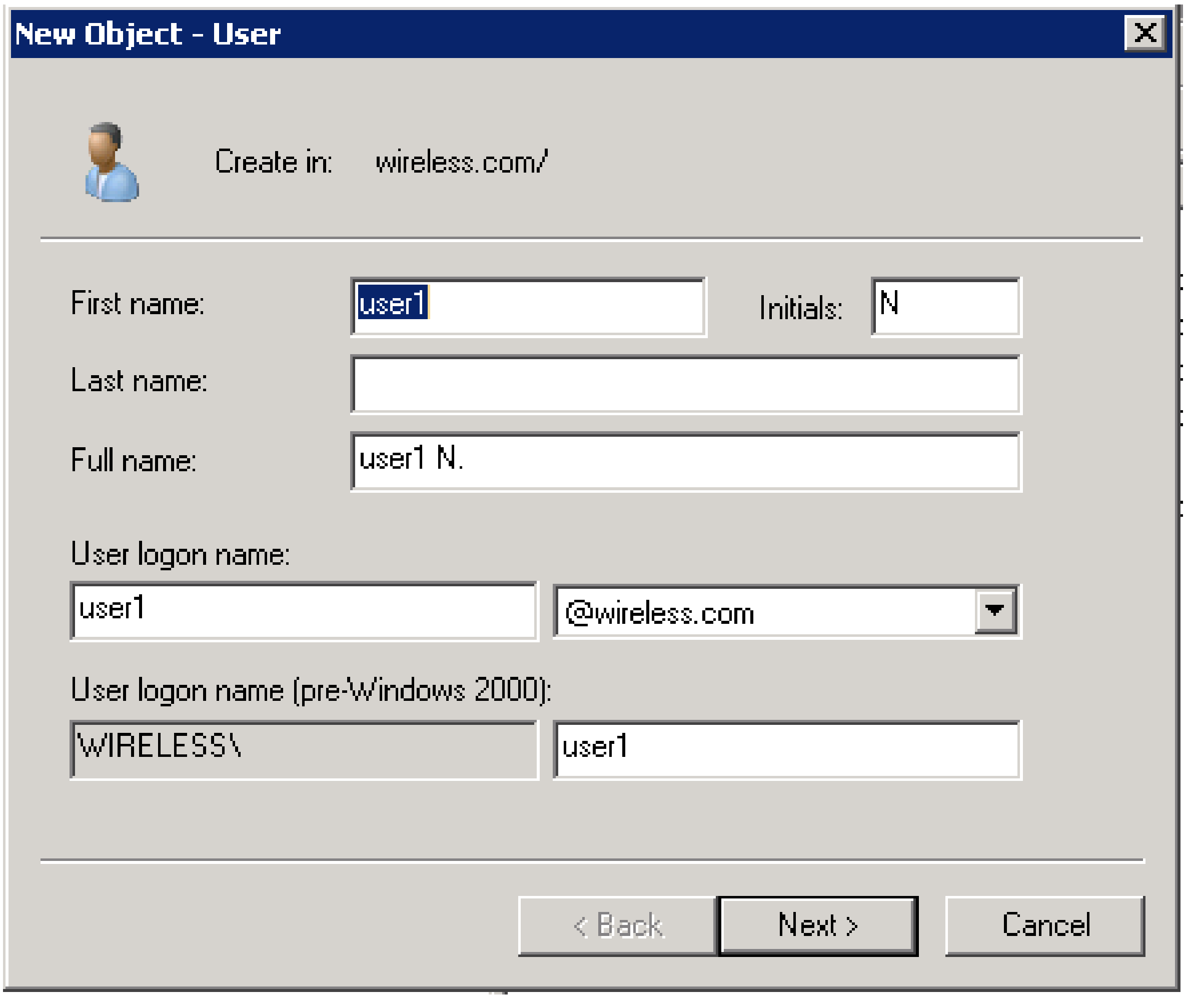
Note: In this example, the user database is maintained on the AD.

Complete these steps in order to add users to the AD database:

1. Navigate to **Start** > **Administrative Tools** > **Active Directory Users and Computers**.

2. In the Active Directory Users and Computers console tree, expand the domain, right-click **Users** and **New**, and choose **User**.

3. In the New Object - User dialog box, enter the name of the wireless user. This example uses **Client1** in the First Name field and **Client1** in the User logon name field. Click **Next**.



New Object - User

Create in: wireless.com/

First name: user1

Initials: N

Last name:

Full name: user1 N.

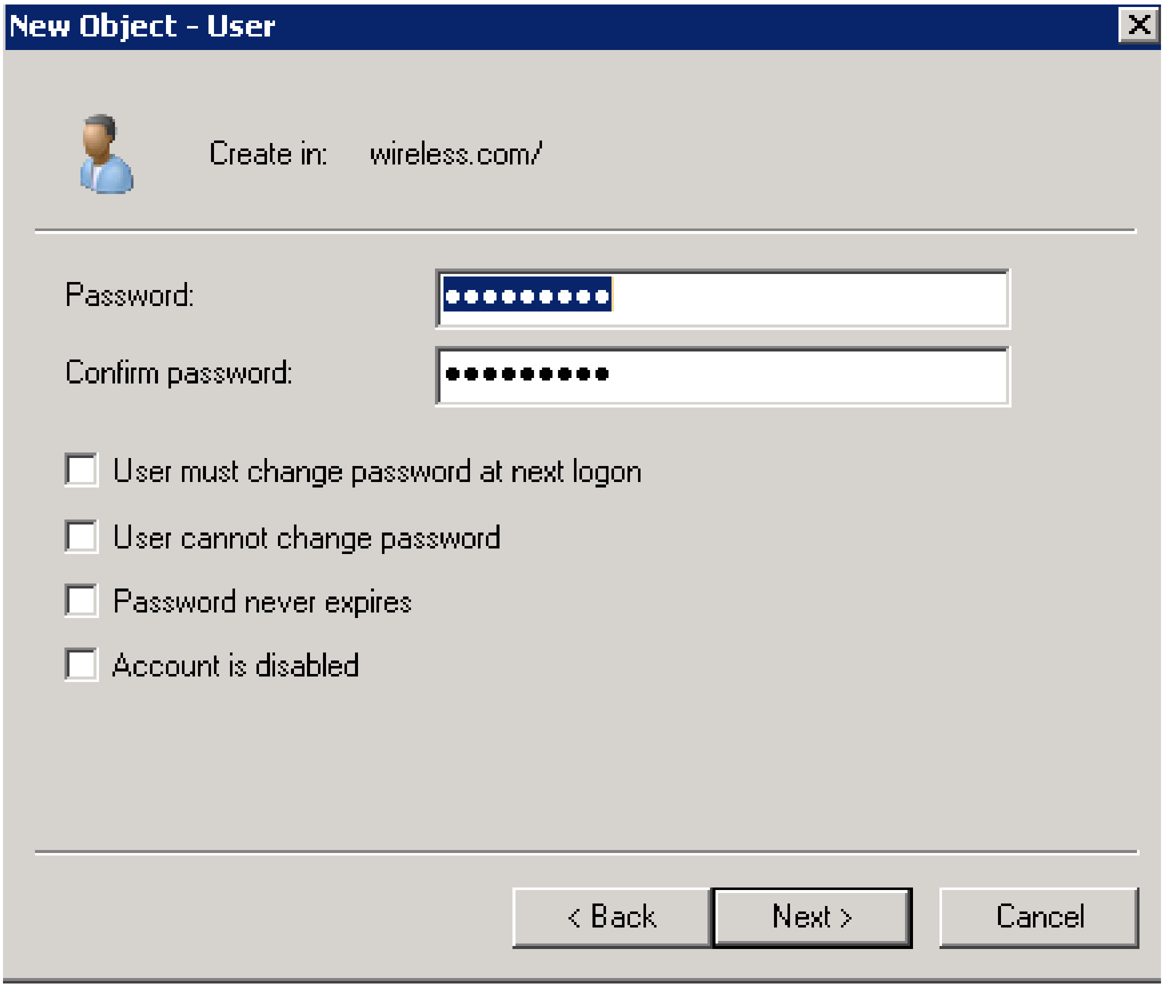
User logon name:

user1 @wireless.com

User logon name (pre-Windows 2000):

WIRELESS\ user1

4. In the New Object - User dialog box, enter a password of your choice in the Password and Confirm password fields. Uncheck the **User must change password at next logon** check box and click **Next**.



Create in: wireless.com/

Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●●

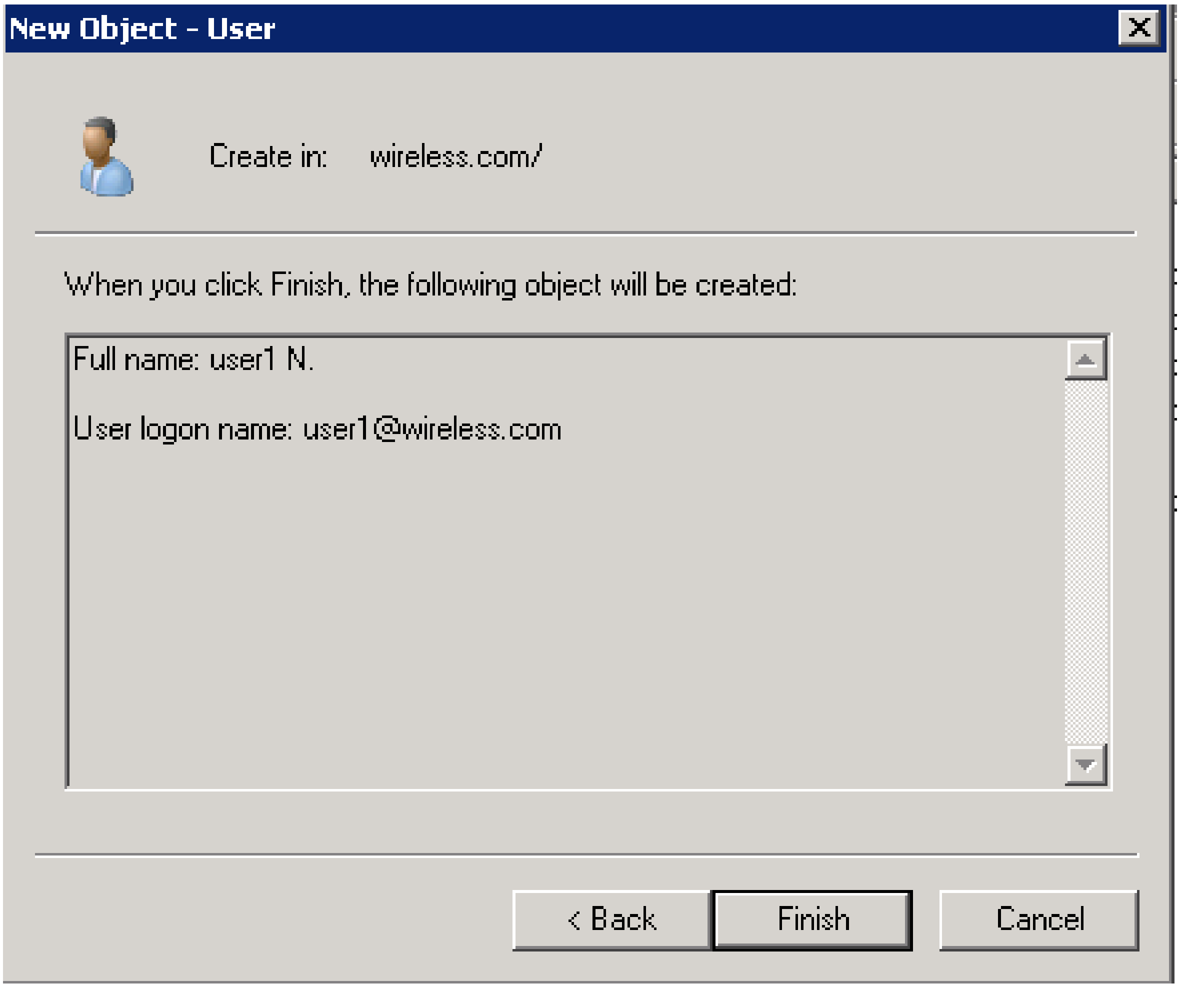
□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

5. In the New Object - User dialog box, click **Finish**.



Create in: wireless.com/

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

Full name: user1 N.

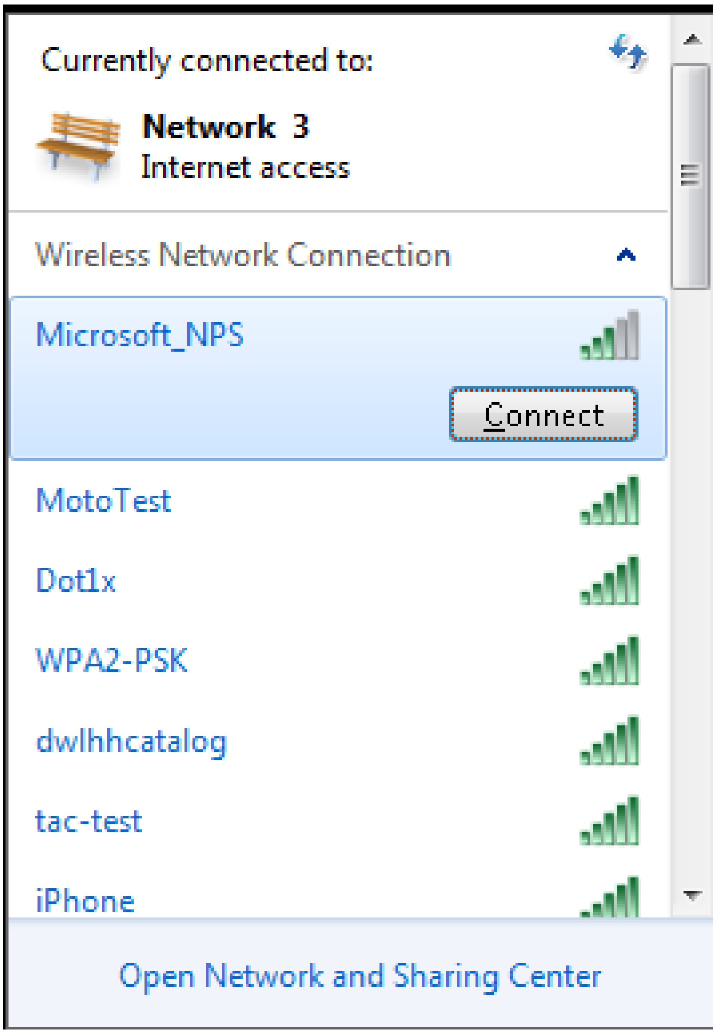
User logon name: user1@wireless.com

6. Repeat Steps 2 through 4 in order to create additional user accounts.

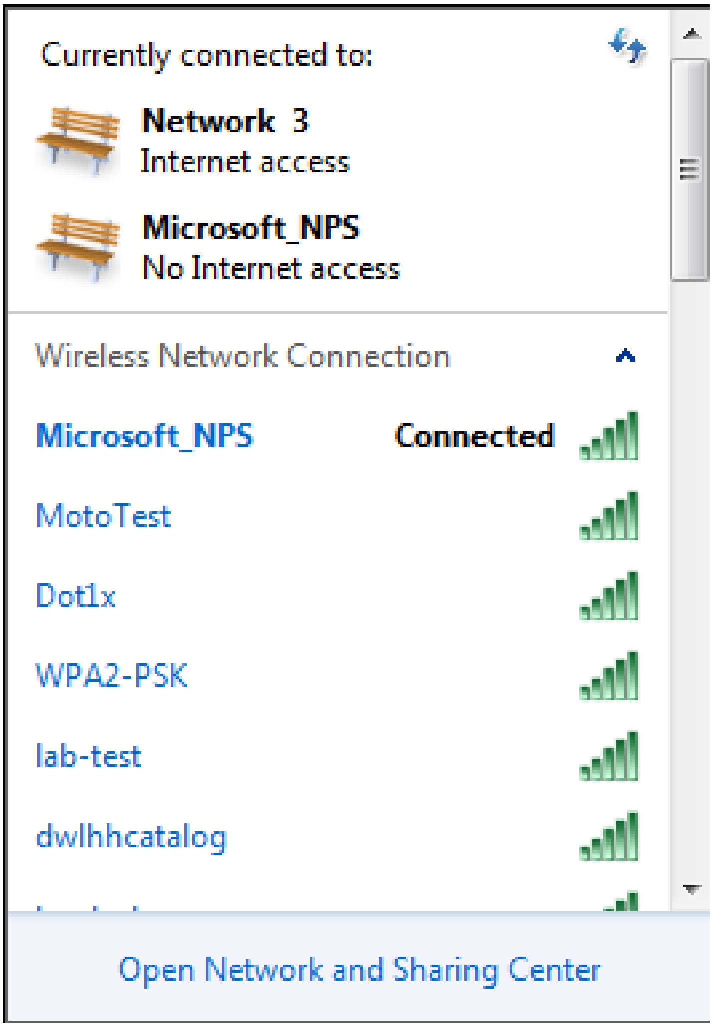
Verify

Complete these steps in order to verify your configuration:

1. Search for the Service Set Identification (SSID) on the client machine.



2. Ensure that the client is connected successfully:



Currently connected to:

Network 3
Internet access

Microsoft_NPS
No Internet access

Wireless Network Connection

Microsoft_NPS Connected

MotoTest

Dot1x

WPA2-PSK

lab-test

dwlhhcatalog

Open Network and Sharing Center

Troubleshoot

> **Note**: Cisco recommends that you use traces in order to troubleshoot wireless issues. Traces are saved in the circular buffer and are not processor intensive.

Enable these traces in order to obtain the **L2 auth logs**:

- **set trace group-wireless-secure level debug**
- **set trace group-wireless-secure filter mac 0017.7C2F.B69A**

Enable these traces in order to obtain the **dot1X AAA events**:

- **set trace wcm-dot1x aaa level debug**
- **set trace wcm-dot1x aaa filter mac 0017.7C2F.B69A**

Enable these traces in order to receive the **DHCP events**:

- **set trace dhcp events level debug**
- **set trace dhcp events filter mac 0017.7C2F.B69A**

Enable these traces in order to disable the traces and clear the buffer:

- **set trace control sys-filtered-traces clear**
- **set trace wcm-dot1x aaa level default**
- **set trace wcm-dot1x aaa filter none**

- **set trace group-wireless-secure level default**
- **set trace group-wireless-secure filter none**

Enter the **show trace sys-filtered-traces** command in order to view the traces:

```
[04/23/14 21:27:51.963 IST 1 8151] 0017.7c2f.b69a Adding mobile on LWAPP AP
 1caa.076f.9e10 (0)
[04/23/14 21:27:51.963 IST 2 8151] 0017.7c2f.b69a Local Policy:  Created MSCB
 Just AccessVLAN = 0 and SessionTimeout  is 0 and apfMsTimeout is 0

[04/23/14 21:27:51.963 IST 8 8151] 0017.7c2f.b69a Local Policy:Setting local
 bridging VLAN  name VLAN0020 and VLAN ID  20

[04/23/14 21:27:51.963 IST 9 8151] 0017.7c2f.b69a Applying WLAN ACL policies
 to client
[04/23/14 21:27:51.963 IST a 8151] 0017.7c2f.b69a No Interface ACL used for
 Wireless client in WCM(NGWC)
[04/23/14 21:27:51.963 IST b 8151] 0017.7c2f.b69a Applying site-specific IPv6
 override for station  0017.7c2f.b69a  - vapId 8, site 'test',
 interface 'VLAN0020'
[04/23/14 21:27:51.963 IST c 8151] 0017.7c2f.b69a Applying local bridging
 Interface Policy for station  0017.7c2f.b69a  - vlan 20,
 interface 'VLAN0020'
[04/23/14 21:27:51.963 IST d 8151] 0017.7c2f.b69a
 **** Inside applyLocalProfilingPolicyAction ****

04/23/14 21:27:51.963 IST f 8151] 0017.7c2f.b69a     Local Profiling Values :
 isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
 sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,
 applyPolicyAtRun= 0
[04/23/14 21:27:51.963 IST 10 8151] 0017.7c2f.b69a          ipv4ACL = [],
 ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[04/23/14 21:27:51.963 IST 11 8151] 0017.7c2f.b69a STA - rates (4):
 130 132 139 150 0 0 0 0 0 0 0 0 0 0 0 0
[04/23/14 21:27:51.963 IST 12 8151] 0017.7c2f.b69a STA - rates (12):
 130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
[04/23/14 21:27:51.963 IST 13 8151] 0017.7c2f.b69a Processing RSN IE type 48,
 length 20 for mobile  0017.7c2f.b69a
[04/23/14 21:27:51.963 IST 14 8151] 0017.7c2f.b69a Received RSN IE with 0
 PMKIDsfrom mobile  0017.7c2f.b69a


[04/23/14 21:27:51.964 IST 1b 8151] 0017.7c2f.b69a Change state to AUTHCHECK
 (2) last state START (0)

[04/23/14 21:27:51.964 IST 1c 8151] 0017.7c2f.b69a Change state to 8021X_REQD
 (3) last state AUTHCHECK (2)


[04/23/14 21:27:51.964 IST 25 8151] 0017.7c2f.b69a apfProcessAssocReq
 (apf_80211.c:6272) Changing state for mobile  0017.7c2f.b69a  on AP
 1caa.076f.9e10  from Associated to Associated

[04/23/14 21:27:51.971 IST 26 8151] 0017.7c2f.b69a 1XA: Initiating
 authentication
[04/23/14 21:27:51.971 IST 27 8151] 0017.7c2f.b69a 1XA: Setting reauth
 timeout to 1800 seconds
[04/23/14 21:27:51.971 IST 28 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 0

[04/23/14 21:27:51.971 IST 29 8151] 0017.7c2f.b69a 1XA: Allocated uid 40
[04/23/14 21:27:51.971 IST 2a 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr
 to authenticate client 4975000000003e uid 40
```

```
[04/23/14 21:27:51.971 IST 2b 8151] 0017.7c2f.b69a 1XA: Session Start from
 wireless client

[04/23/14 21:27:51.971 IST 2c 8151] 0017.7c2f.b69a Session Manager Call Client
 4975000000003e, uid 40, capwap id 7ae8c000000013,Flag 0, Audit-Session ID
 0a6987b25357e2ff00000028, method list Microsoft_NPS, policy name (null)

[04/23/14 21:27:51.971 IST 2d 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0017.7c2f.b69a, Ca3] Session start request from Client[1] for 0017.7c2f.b69a
 (method: Dot1X, method list: Microsoft_NPS, aaa id: 0x00000028),  policy
[04/23/14 21:27:51.971 IST 2e 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0017.7c2f.b69a, Ca3]  - client iif_id: 4975000000003E, session ID:
 0a6987b25357e2ff00000028 for 0017.7c2f.b69a


[04/23/14 21:27:51.972 IST 43 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting !EAP_RESTART on Client 0x22000025
[04/23/14 21:27:51.972 IST 44 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:enter connecting state
[04/23/14 21:27:51.972 IST 45 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025: restart connecting
[04/23/14 21:27:51.972 IST 46 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting RX_REQ on Client 0x22000025
[04/23/14 21:27:51.972 IST 47 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025: authenticating state entered
[04/23/14 21:27:51.972 IST 48 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:connecting authenticating action
[04/23/14 21:27:51.972 IST 49 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting AUTH_START for 0x22000025
[04/23/14 21:27:51.972 IST 4a 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:entering request state
[04/23/14 21:27:51.972 IST 4b 291] ACCESS-METHOD-DOT1X-NOTF:
 [0017.7c2f.b69a, Ca3] Sending EAPOL packet
[04/23/14 21:27:51.972 IST 4c 291] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Platform changed src mac  of EAPOL packet
[04/23/14 21:27:51.972 IST 4d 291] ACCESS-METHOD-DOT1X-NOTF:
 [0017.7c2f.b69a, Ca3] Sending out EAPOL packet
[04/23/14 21:27:51.972 IST 4e 291] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] EAPOL packet sent to client 0x22000025


[04/23/14 21:27:52.112 IST 7d 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[04/23/14 21:27:52.112 IST 7e 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:52.112 IST 7f 211] AAA SRV(00000000): Authen method=SERVER_GROUP
 Microsoft_NPS
[04/23/14 21:27:52.112 IST 80 211] AAA SRV(00000000): Selecting SG = DIAMETER
[04/23/14 21:27:52.113 IST 81 186] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Queuing an EAPOL pkt on Authenticator Q
[04/23/14 21:27:52.113 IST 82 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting EAPOL_EAP for 0x22000025
[04/23/14 21:27:52.278 IST 83 220] AAA SRV(00000000): protocol reply
 GET_CHALLENGE_RESPONSE for Authentication
[04/23/14 21:27:52.278 IST 84 220] AAA SRV(00000000): Return Authentication
 status=GET_CHALLENGE_RESPONSE
[04/23/14 21:27:52.278 IST 85 291] ACCESS-METHOD-DOT1X-DEB:[0017.7c2f.b69a,Ca3]
 Posting EAP_REQ for 0x22000025
```

Here is the rest of the EAP output:

```
[04/23/14 21:27:54.690 IST 12b 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:54.690 IST 12c 211] AAA SRV(00000000): Authen
 method=SERVER_GROUP Microsoft_NPS
[04/23/14 21:27:54.690 IST 12d 211] AAA SRV(00000000): Selecting SG =
 DIAMETER
[04/23/14 21:27:54.694 IST 12e 220] AAA SRV(00000000): protocol reply PASS
 for Authentication
[04/23/14 21:27:54.694 IST 12f 220] AAA SRV(00000000): Return Authentication
 status=PASS
[04/23/14 21:27:54.694 IST 130 189] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Received an EAP Success


[04/23/14 21:27:54.695 IST 186 8151] 0017.7c2f.b69a Starting key exchange with
 mobile - data forwarding is disabled
[04/23/14 21:27:54.695 IST 187 8151] 0017.7c2f.b69a 1XA: Sending EAPOL message
 to mobile, WLAN=8 AP WLAN=8
[04/23/14 21:27:54.706 IST 188 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL
 message (len 121) from mobile
[04/23/14 21:27:54.706 IST 189 8151] 0017.7c2f.b69a 1XA: Received EAPOL-Key
 from mobile
[04/23/14 21:27:54.706 IST 18a 8151] 0017.7c2f.b69a 1XK: Received EAPOL-key in
 PTK_START state (msg 2) from mobile
[04/23/14 21:27:54.706 IST 18b 8151] 0017.7c2f.b69a 1XK: Stopping retransmission
 timer
[04/23/14 21:27:54.706 IST 18c 8151] 0017.7c2f.b69a 1XA: Sending EAPOL message
 to mobile, WLAN=8 AP WLAN=8
[04/23/14 21:27:54.717 IST 18d 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL
 message (len 99) from mobile
[04/23/14 21:27:54.717 IST 18e 8151] 0017.7c2f.b69a 1XA: Received EAPOL-Key
 from mobile
[04/23/14 21:27:54.717 IST 18f 8151] 0017.7c2f.b69a 1XK: Received EAPOL-key in
 PTKINITNEGOTIATING state (msg 4) from mobile
[04/23/14 21:27:54.717 IST 190 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 1

[04/23/14 21:27:54.717 IST 191 8151] 0017.7c2f.b69a 1XK: Key exchange complete
 - updating PEM
[04/23/14 21:27:54.717 IST 192 8151] 0017.7c2f.b69a apfMs1xStateInc
[04/23/14 21:27:54.717 IST 193 8151] 0017.7c2f.b69a Change state to
 L2AUTHCOMPLETE (4) last state 8021X_REQD (3)


[04/23/14 21:27:58.277 IST 1df 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:27:58.277 IST 1e0 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:28:05.279 IST 1e1 269] DHCPD: Adding binding to hash tree
[04/23/14 21:28:05.279 IST 1e2 269] DHCPD: DHCPOFFER notify setup address
20.20.20.5 mask 255.255.255.0


[04/23/14 21:28:05.306 IST 1f4 8151] 0017.7c2f.b69a Change state to RUN (20)
 last state DHCP_REQD (7)
```