NPS, Wireless LAN Controllers, and Wireless Networks Configuration Example

TAC **Document ID: 115988**

Contributed by Nick Tate, Cisco TAC Engineer.
Apr 02, 2013

Contents

Introduction

This document provides a sample configuration for the Protected Extensible Authentication Protocol (PEAP) with Microsoft Challenge Handshake Authentication Protocol (MS−CHAP) version 2 authentication in a Cisco Unified Wireless network with the Microsoft Network Policy Server (NPS) as the RADIUS server.

Prerequisites

Requirements

Ensure that you are familiar with these procedures before you attempt this configuration:

- Knowledge of basic Windows 2008 installation
- Knowledge of Cisco controller installation

Ensure that these requirements have been met before you attempt this configuration:

- Install the Microsoft Windows Server 2008 operating system on each of the servers in the test lab.
- Update all service packs.
- Install the controllers and lightweight access points (LAPs).
- Configure the latest software updates.

For initial installation and configuration information for the Cisco 5508 Series Wireless Controllers, refer to the Cisco 5500 Series Wireless Controller Installation Guide.

Note: This document is intended to give the readers an example on the configuration required on a Microsoft server for PEAP−MS−CHAP authentication. The Microsoft Windows server configuration presented in this document has been tested in the lab and found to work as expected. If you have trouble with the configuration, contact Microsoft for help. The Cisco Technical Assistance Center (TAC) does not support Microsoft Windows server configuration.

Microsoft Windows 2008 installation and configuration guides can be found on Microsoft Tech Net.

Components Used

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

- Cisco 5508 Wireless Controller that runs firmware Version 7.4
- Cisco Aironet 3602 Access Point (AP) with Lightweight Access Point Protocol (LWAPP)
- Windows 2008 Enterprise Server with NPS, Certificate Authority (CA), dynamic host control protocol (DHCP), and Domain Name System (DNS) services installed
- Microsoft Windows 7 client PC
- 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.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

PEAP Overview

PEAP uses Transport Level Security (TLS) to create an encrypted channel between an authenticating PEAP client, such as a wireless laptop, and a PEAP authenticator, such as 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 provided by PEAP. The PEAP authentication process consists of two main phases.

PEAP Phase One: TLS−Encrypted Channel

The wireless client associates with the 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 access point. After the IEEE 802.11−based association is successfully established between the client and the access point, the TLS session is negotiated with the AP. After authentication is successfully completed between the wireless client and NPS, the TLS session is negotiated between the client and NPS. The key that is derived within this negotiation is used to encrypt all subsequent communication.

PEAP Phase Two: EAP−Authenticated Communication

EAP communication, which includes EAP negotiation, occurs inside the TLS channel 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

RADIUS server. The Wireless LAN Controller (WLC) and the LAP cannot decrypt these messages because it is not the TLS end point.

The RADIUS message sequence for a successful authentication attempt (where the user has supplied valid password−based credentials with PEAP−MS−CHAP v2) is:

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 sends back an MS−CHAP v2 success packet when the server has successfully authenticated 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 has successfully authenticated 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.

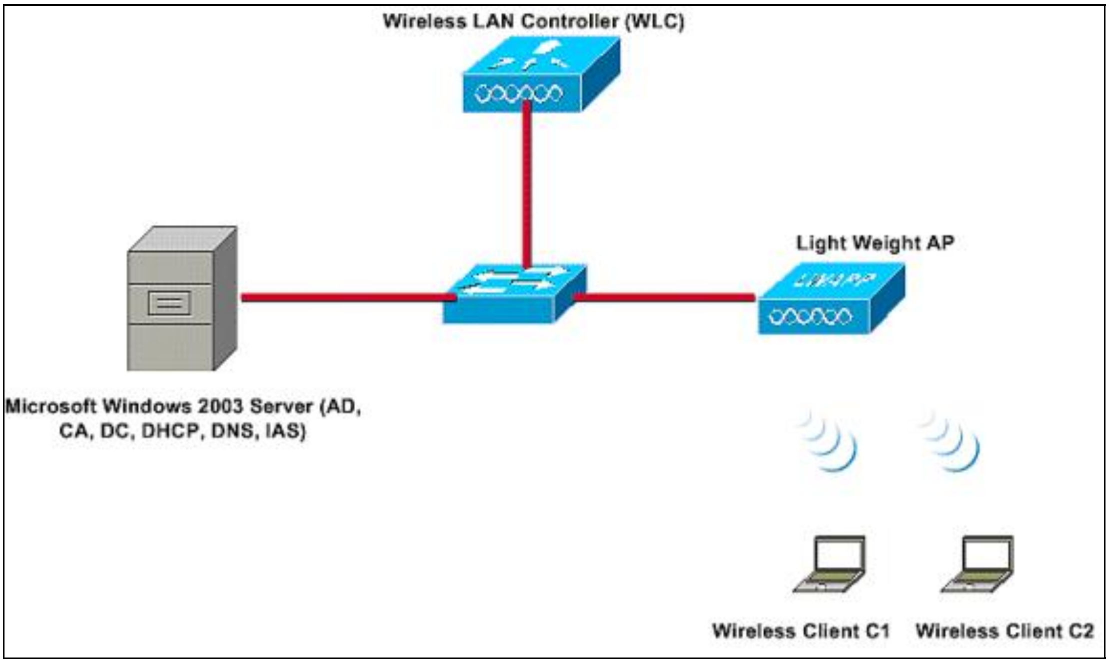
Configure

In this section, you are presented with the information to configure PEAP−MS−CHAP v2.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This configuration uses this network setup:


Wireless LAN Controller (WLC)
Light Weight AP
Microsoft Windows 2003 Server (AD, CA, DC, DHCP, DNS, IAS)
Wireless Client C1
Wireless Client C2

In this setup, a Microsoft Windows 2008 server performs these roles:

- Domain controller for the domain wireless.com
- DHCP/DNS server
- CA server
- NPS ? to authenticate the wireless users
- Active Directory ? to maintain the user database

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

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

Configurations

The objective of this example is to configure the Microsoft 2008 server, Wireless LAN Controller, and Light Weight AP to authenticate the wireless clients with PEAP−MS−CHAP v2 authentication. There are three major steps in this process:

1. Configure the Microsoft Windows 2008 Server.
2. Configure the WLC and the Light Weight APs.
3. Configure the wireless clients.

Configure the Microsoft Windows 2008 Server

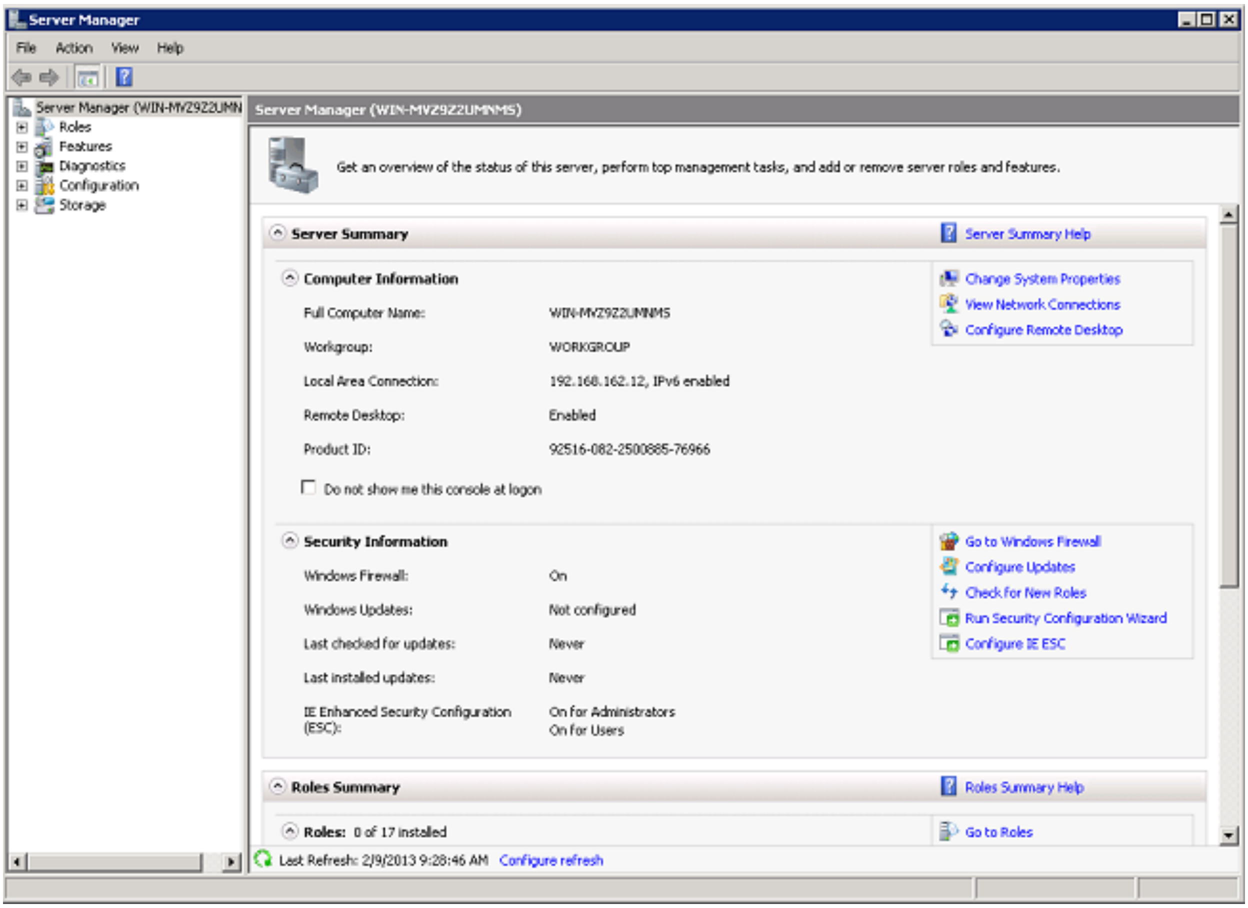
In this example, a complete configuration of the Microsoft Windows 2008 server includes these steps:

1. Configure the server as a domain controller.
2. Install and configure DHCP services.
3. install and configure the server as a CA server.
4. Connect clients to the domain.
5. Install the NPS.
6. Install a certificate.
7. Configure the NPS for PEAP authentication.
8. Add users to the Active Directory.

Configure the Microsoft Windows 2008 Server as a Domain Controller

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

1. Click ***Start*** > ***Server Manager***.



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

Computer Information

Full Computer Name: WIN-MVZ9Z2UMNMS

Workgroup: WORKGROUP

Local Area Connection: 192.168.162.12, IPv6 enabled

Remote Desktop: Enabled

Product ID: 92516-082-2500885-76966

□ Do not show me this console at logon

Security Information

Windows Firewall: On

Windows Updates: Not configured

Last checked for updates: Never

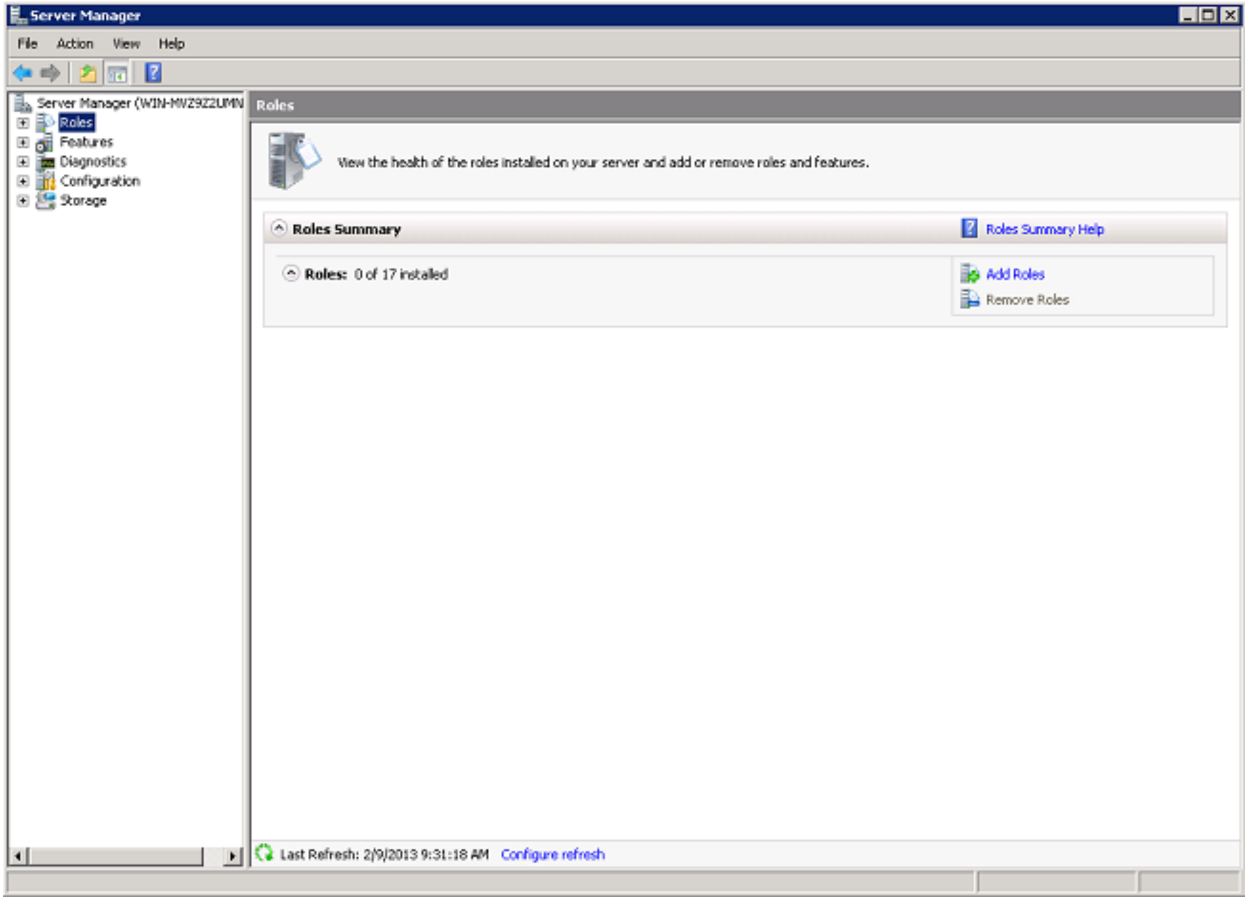
Last installed updates: Never

IE Enhanced Security Configuration (ESC): On for Administrators
On for Users

Roles: 0 of 17 installed

Last Refresh: 2/9/2013 9:28:46 AM

2. Click ***Roles*** > ***Add Roles***.

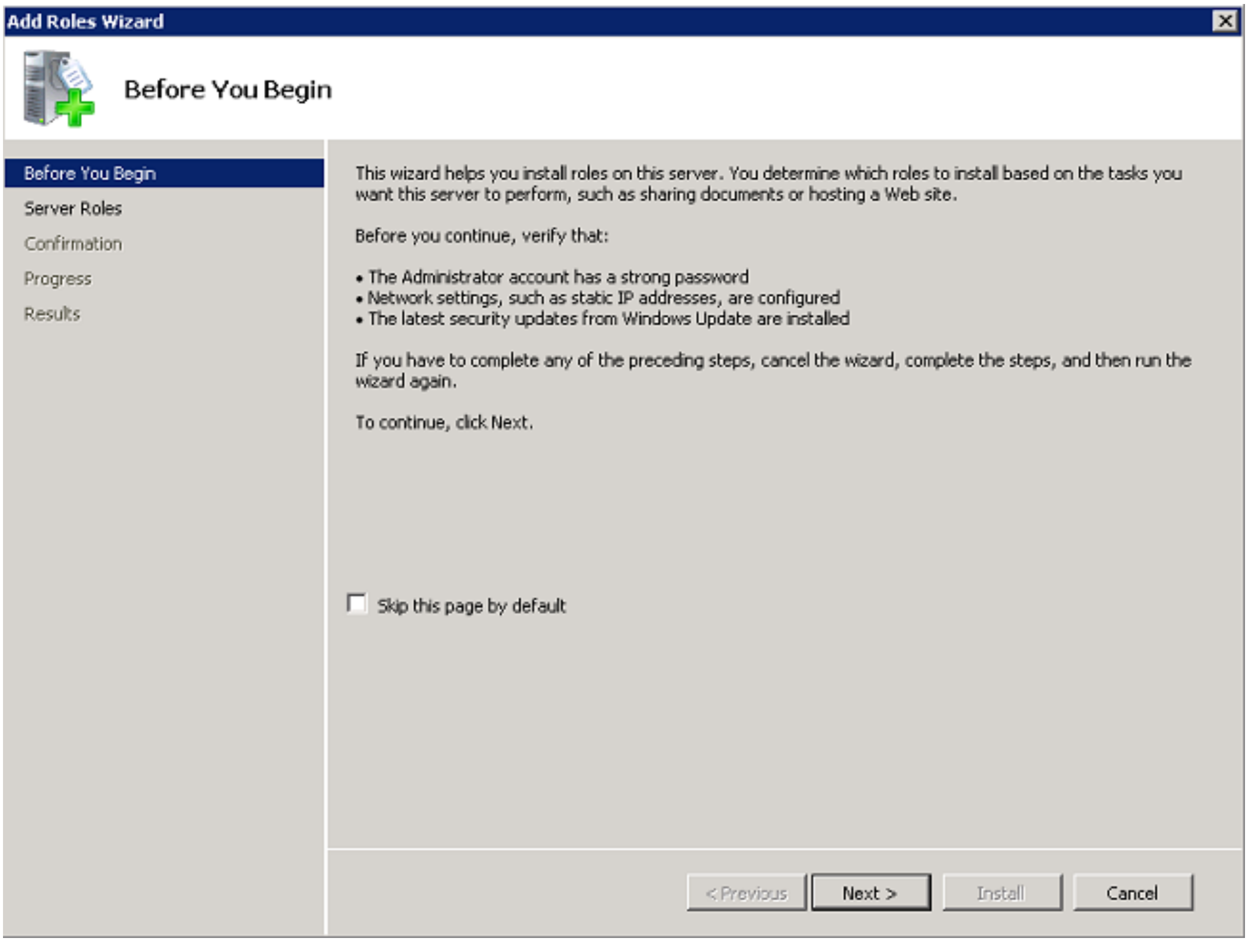


View the health of the roles installed on your server and add or remove roles and features.

Roles: 0 of 17 installed

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

3. Click ***Next***.



Add Roles Wizard

Before You Begin

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:

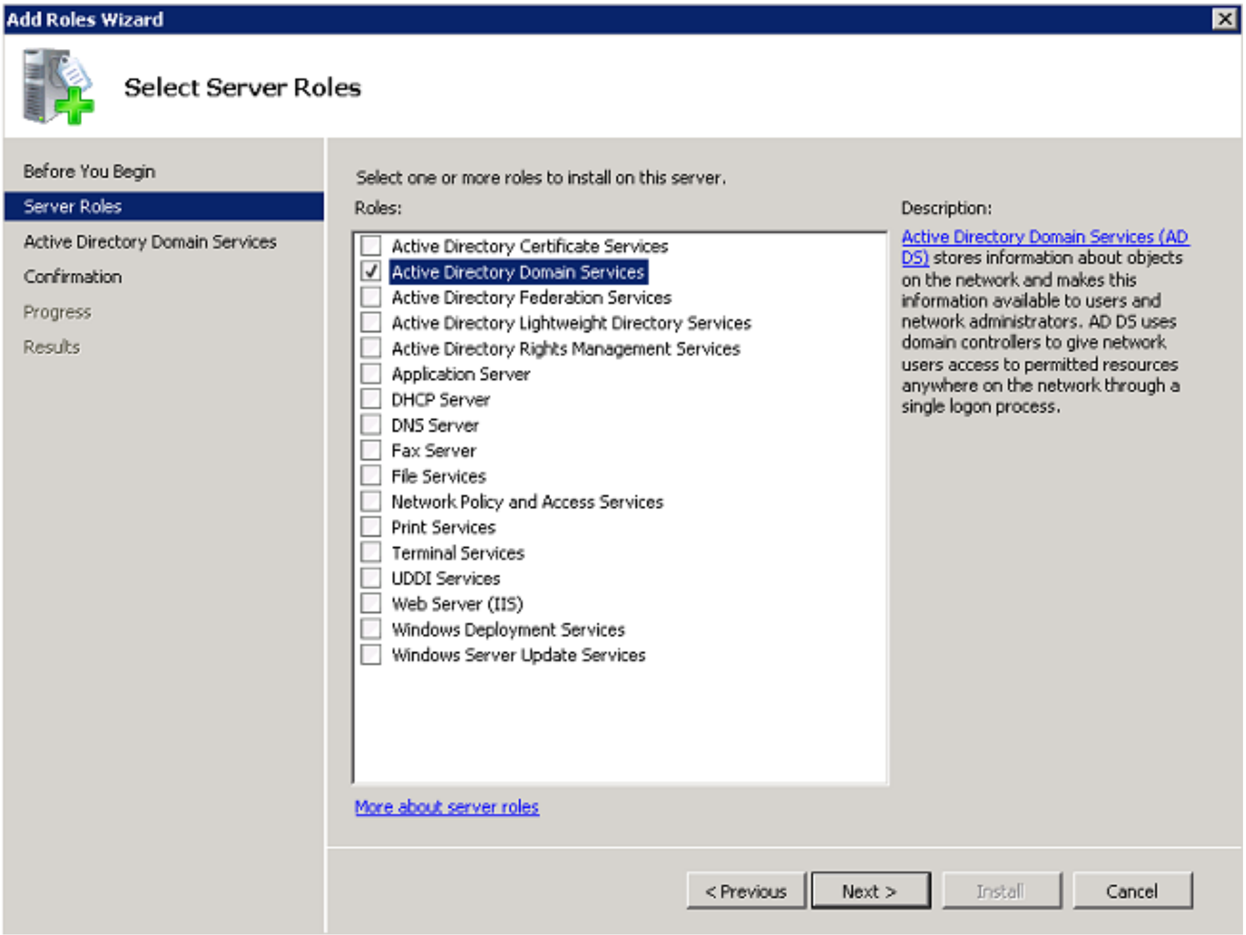
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

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

4. Select the service ***Active Directory Domain Services***, and click ***Next***.



Select Server Roles

Select one or more roles to install on this server.

Roles:

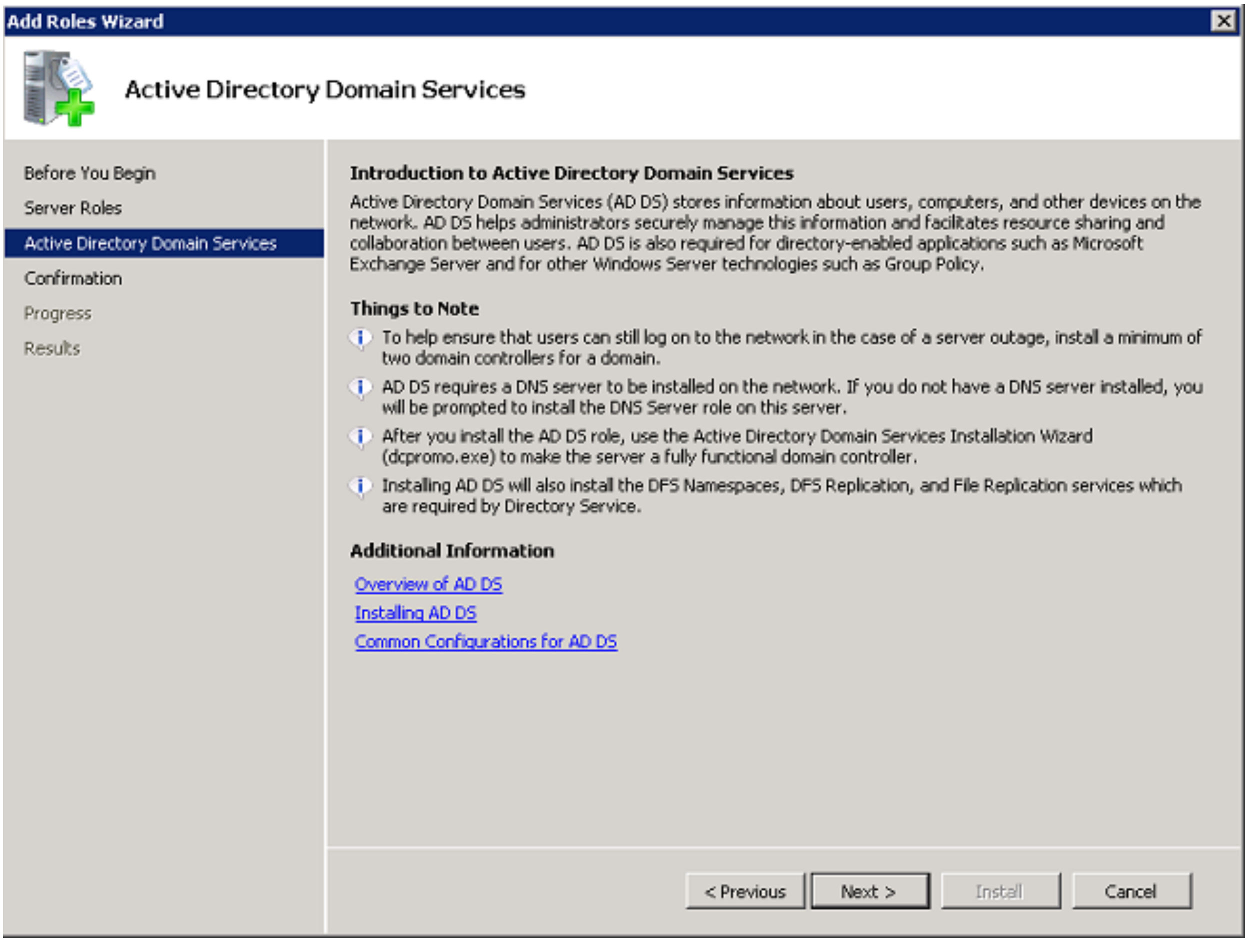
- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ 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

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



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.

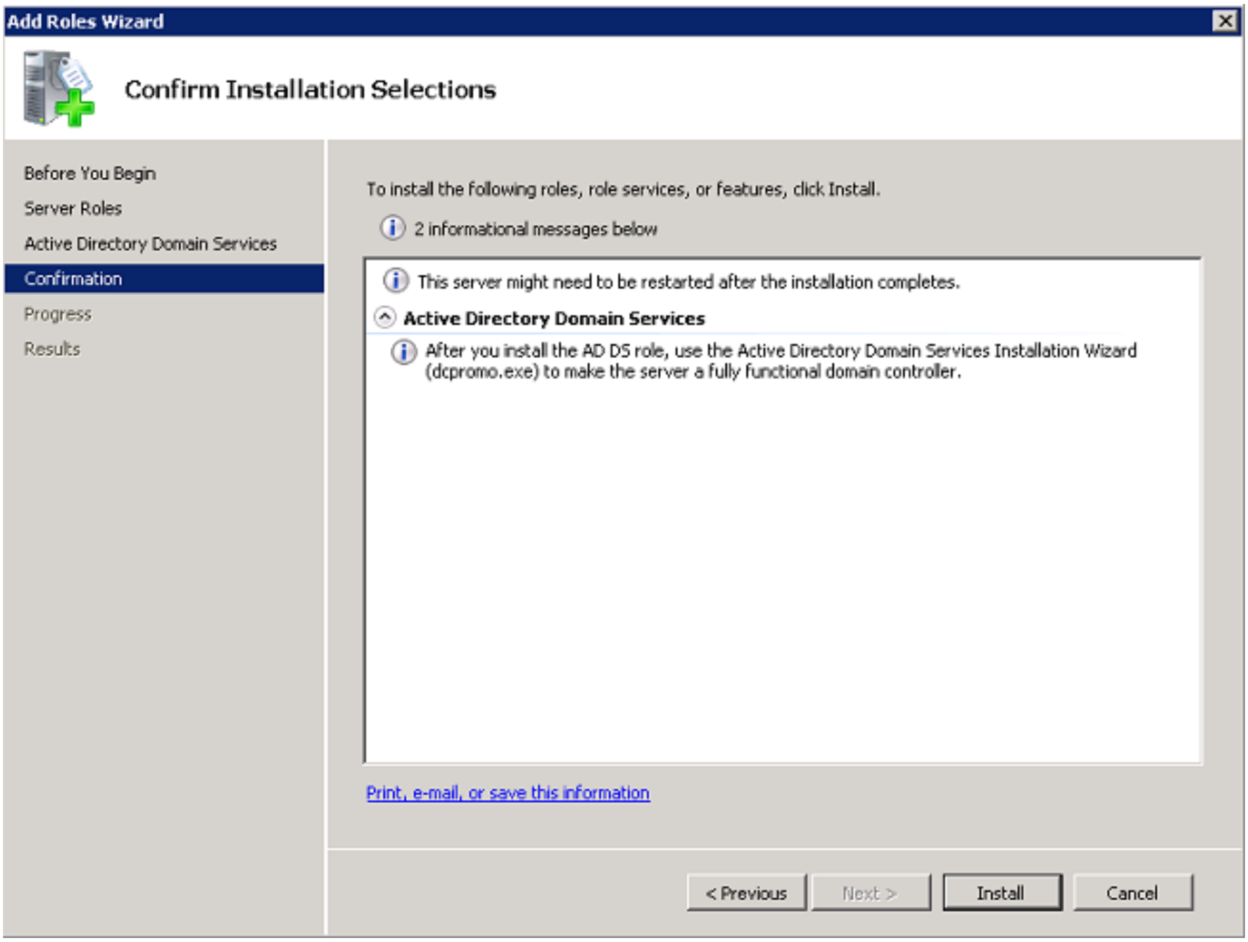
Additional Information

Overview of AD DS

Installing AD DS

Common Configurations for AD DS

6. Click ***Install*** to begin the installation process.


Add Roles Wizard
Confirm Installation Selections
Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results
Print, e-mail, or save this information
< Previous
Next >
Install
Cancel

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

2 informational messages below

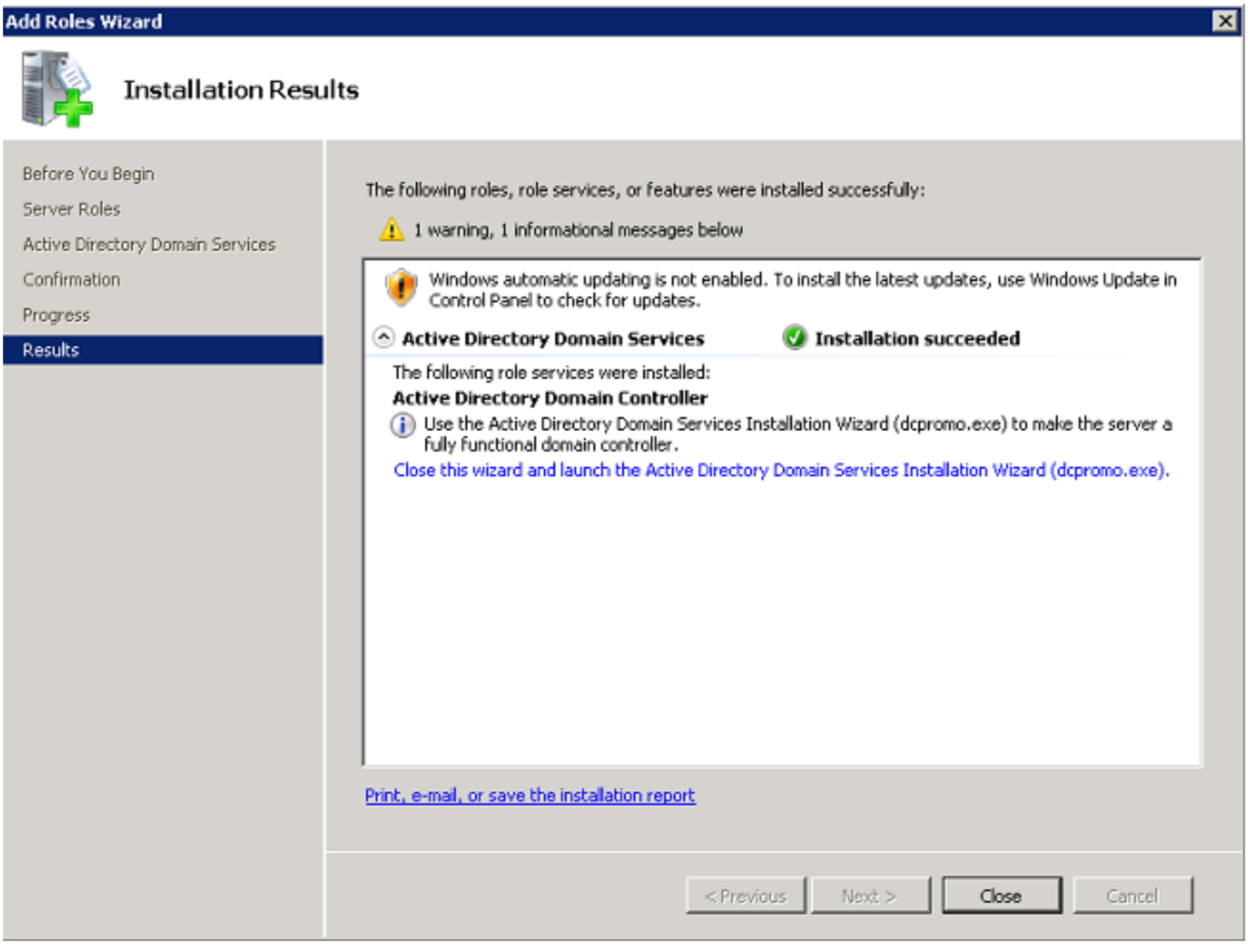
This server might need to be restarted after the installation completes.

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.

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



Add Roles Wizard

Installation Results

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:

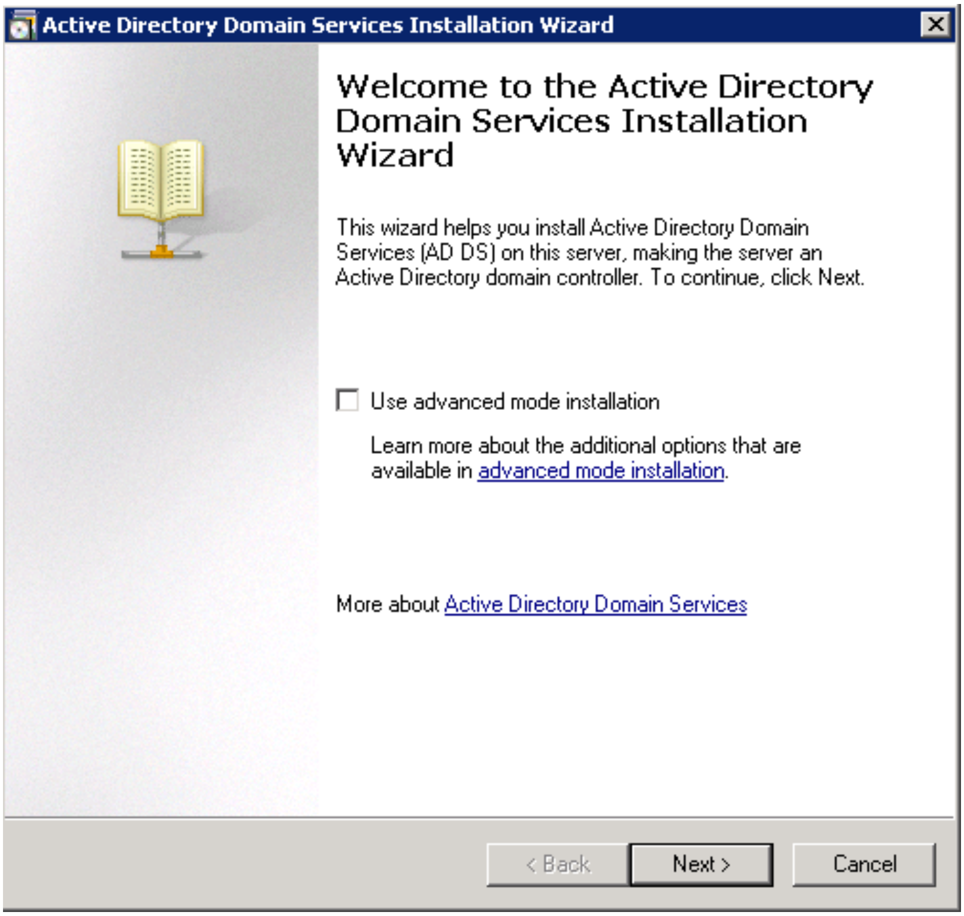
Active Directory Domain Controller

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

8. Click ***Next*** to run the Active Directory Domain Services Installation Wizard.



Welcome to the Active Directory Domain Services Installation Wizard

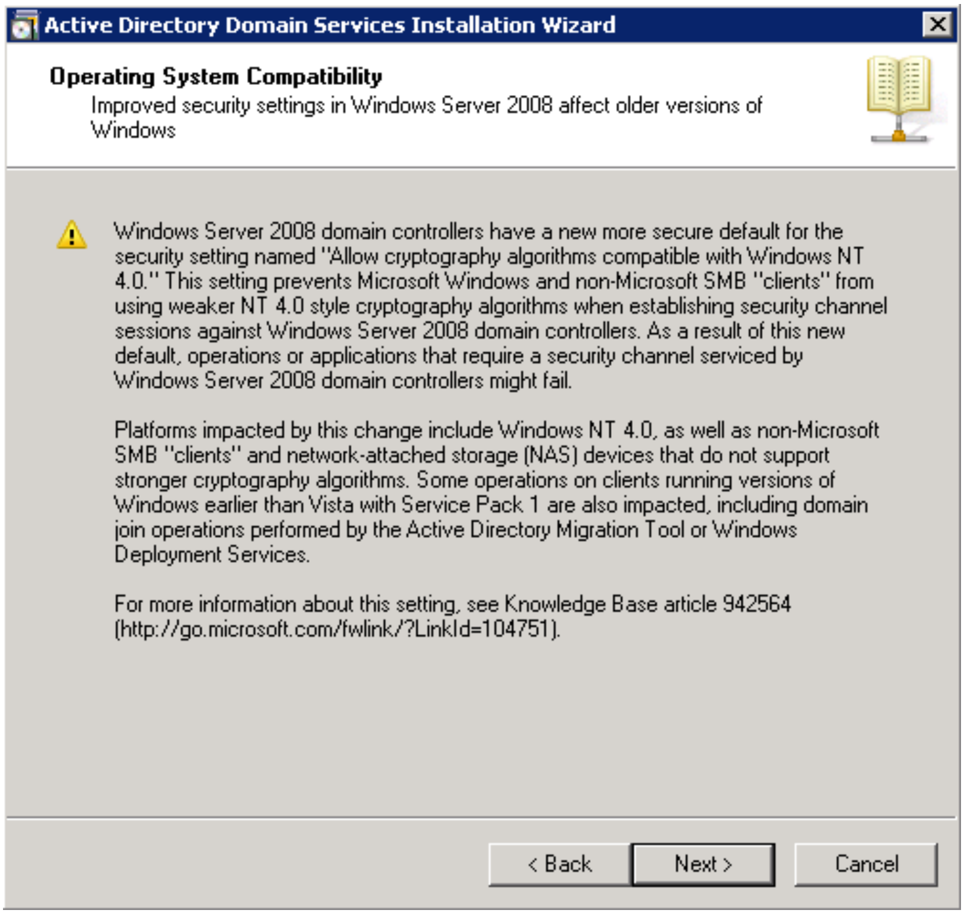
This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next.

□ Use advanced mode installation

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

More about Active Directory Domain Services

9. Review the information on Operating System Compatbilty, and click ***Next***.



Operating System Compatibility

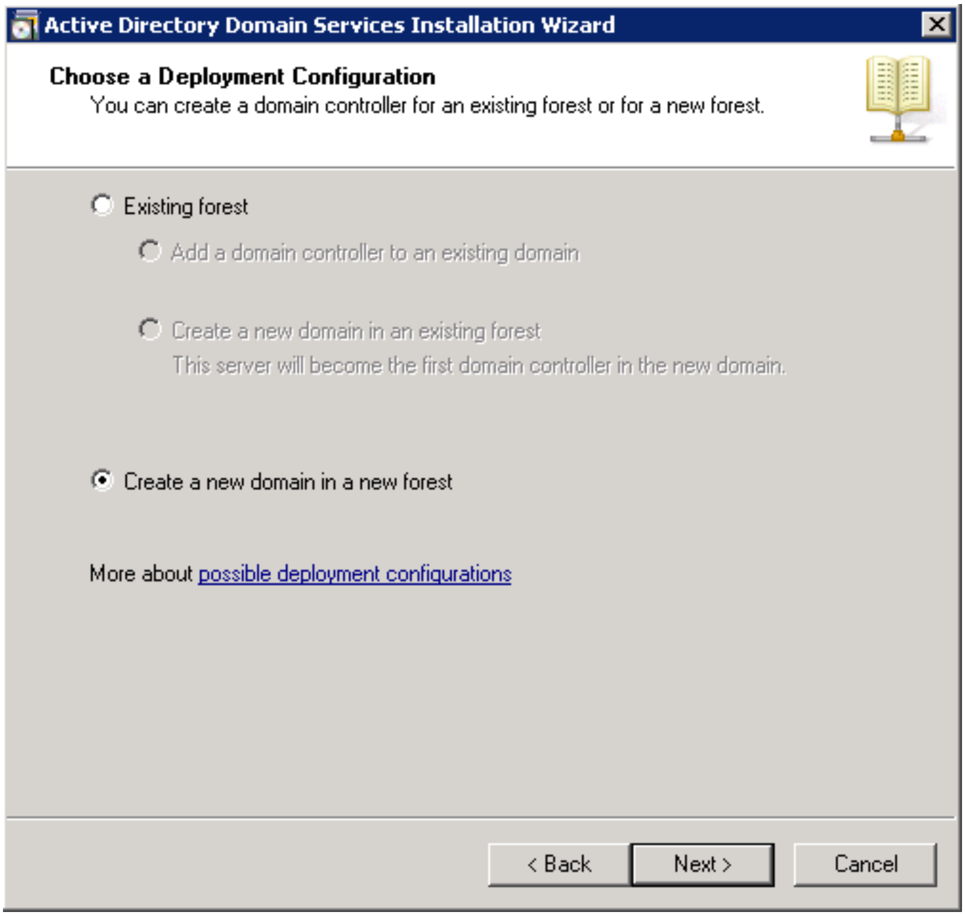
Improved security settings in Windows Server 2008 affect older versions of Windows

⚠ 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).

10. Click ***Create a new domain in a new forest*** > ***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

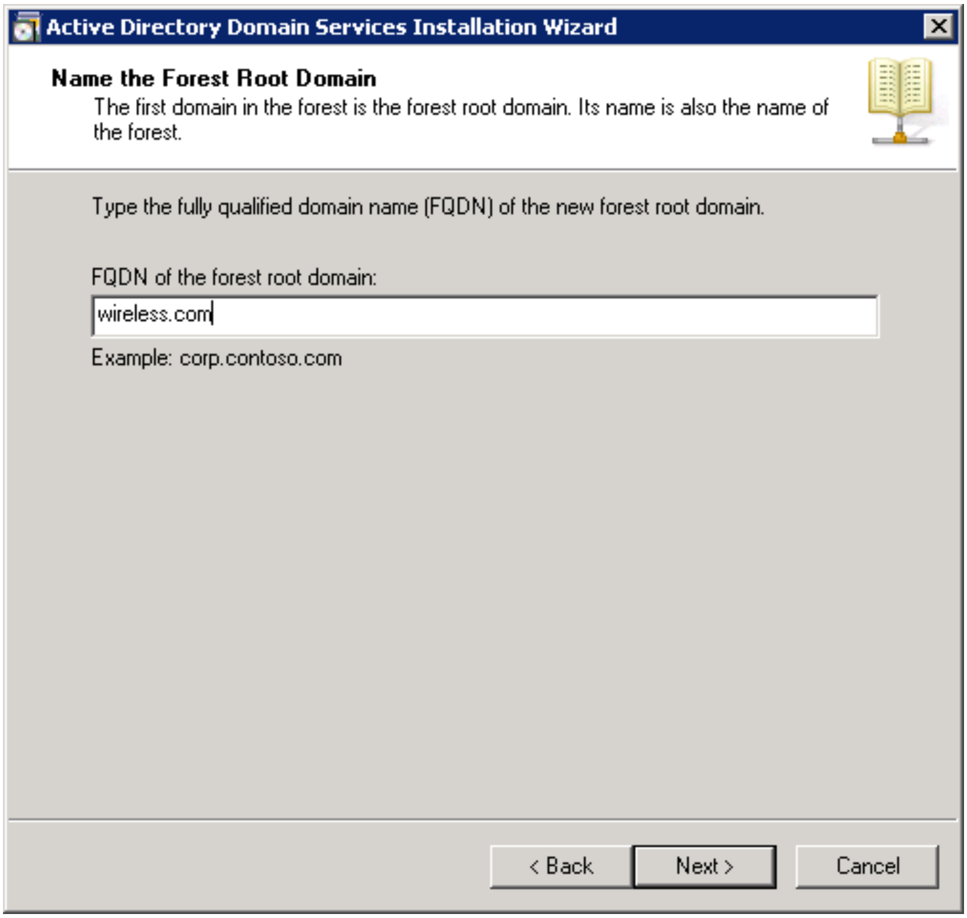
○ Add a domain controller to an existing domain

○ 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

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



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.

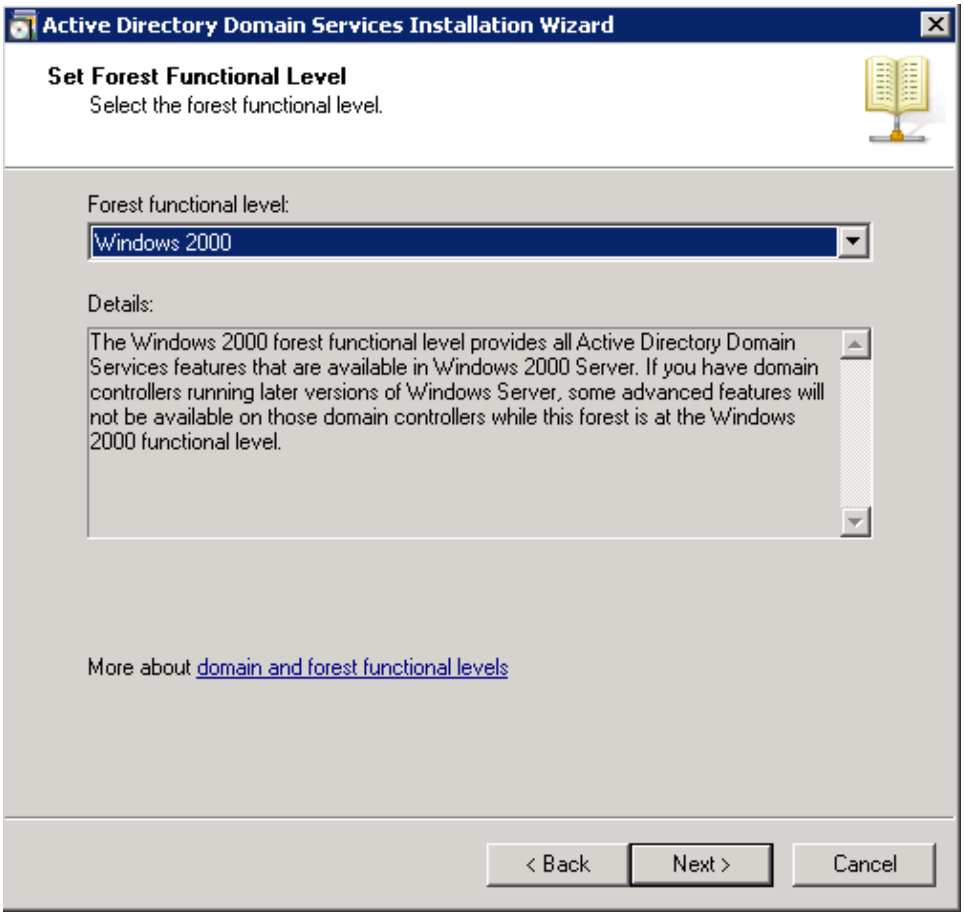
Type the fully qualified domain name (FQDN) of the new forest root domain.

FQDN of the forest root domain:

wireless.com

Example: corp.contoso.com

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



Set Forest Functional Level

Select the forest functional level.

Forest functional level:

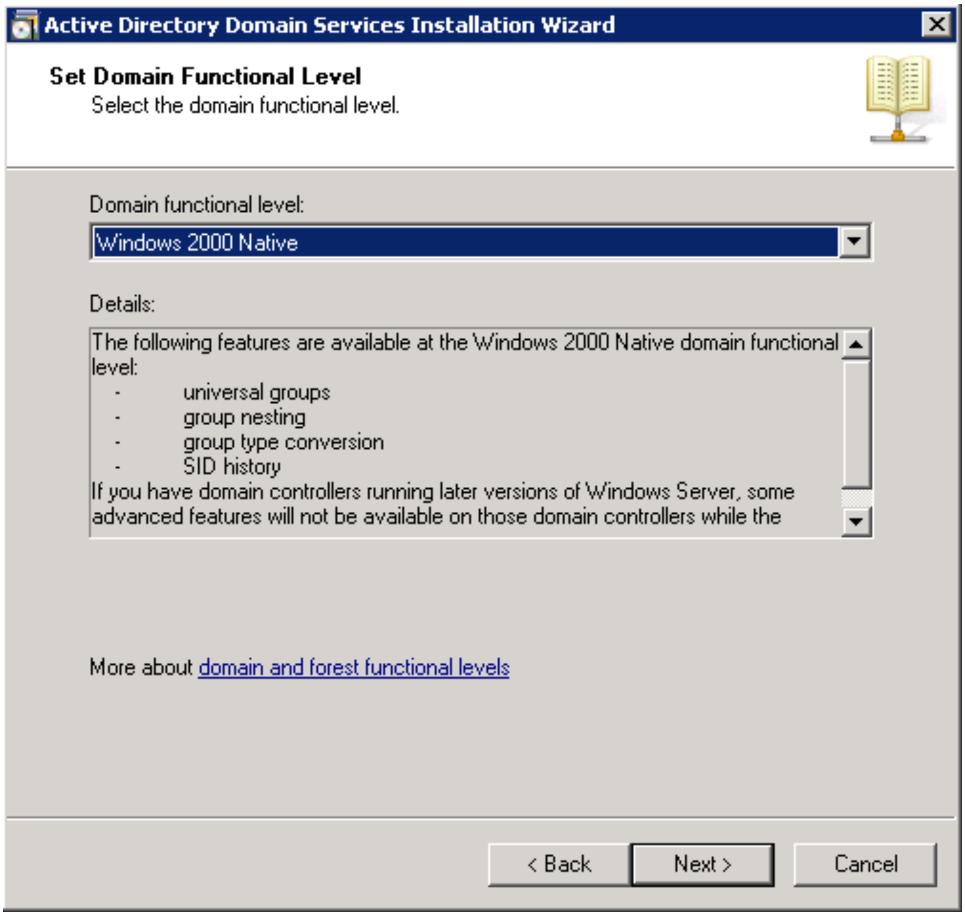
Windows 2000

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

13. 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:

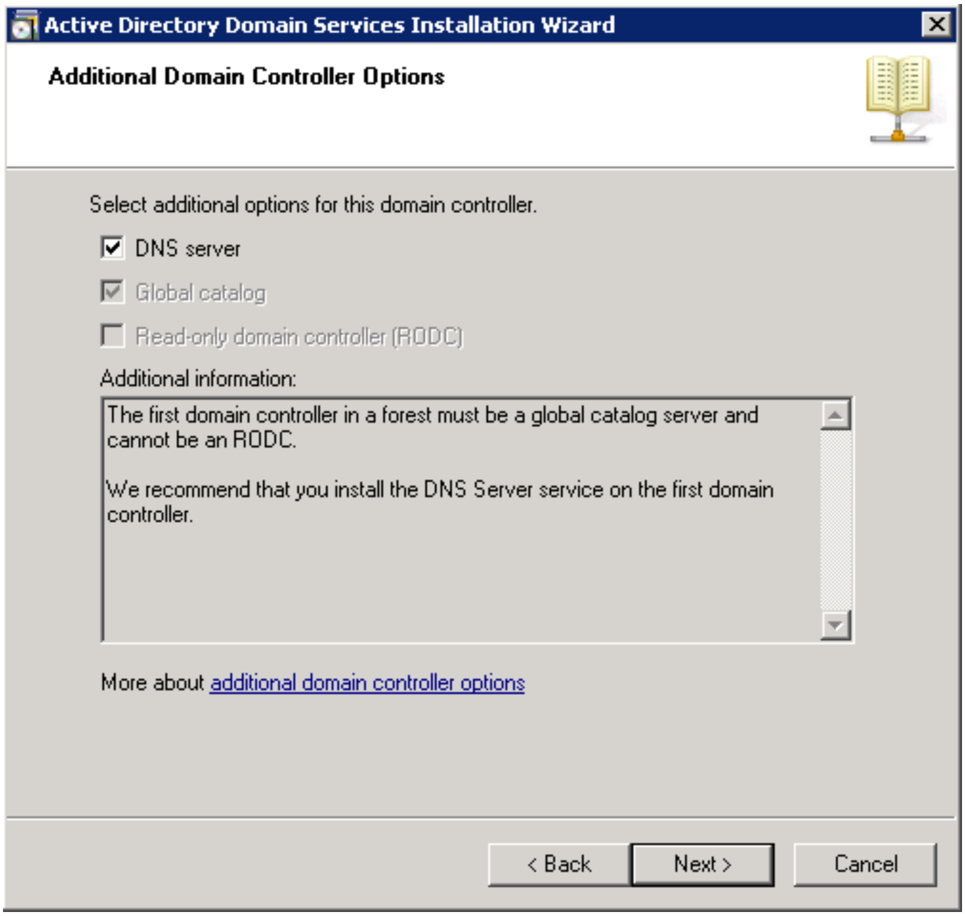
The following features are available at the Windows 2000 Native domain functional level:

- 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

14. Ensure DNS server is selected, and click ***Next***.



Active Directory Domain Services Installation Wizard

Additional Domain Controller Options

Select additional options for this domain controller.

☑ DNS server

☑ Global catalog

□ Read-only domain controller (RODC)

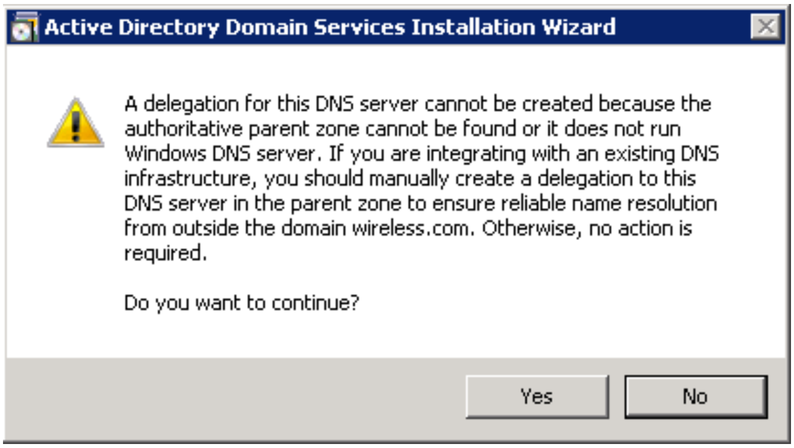
Additional information:

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

15. Click ***Yes*** for the installation wizard to create a new zone in DNS for the domain.

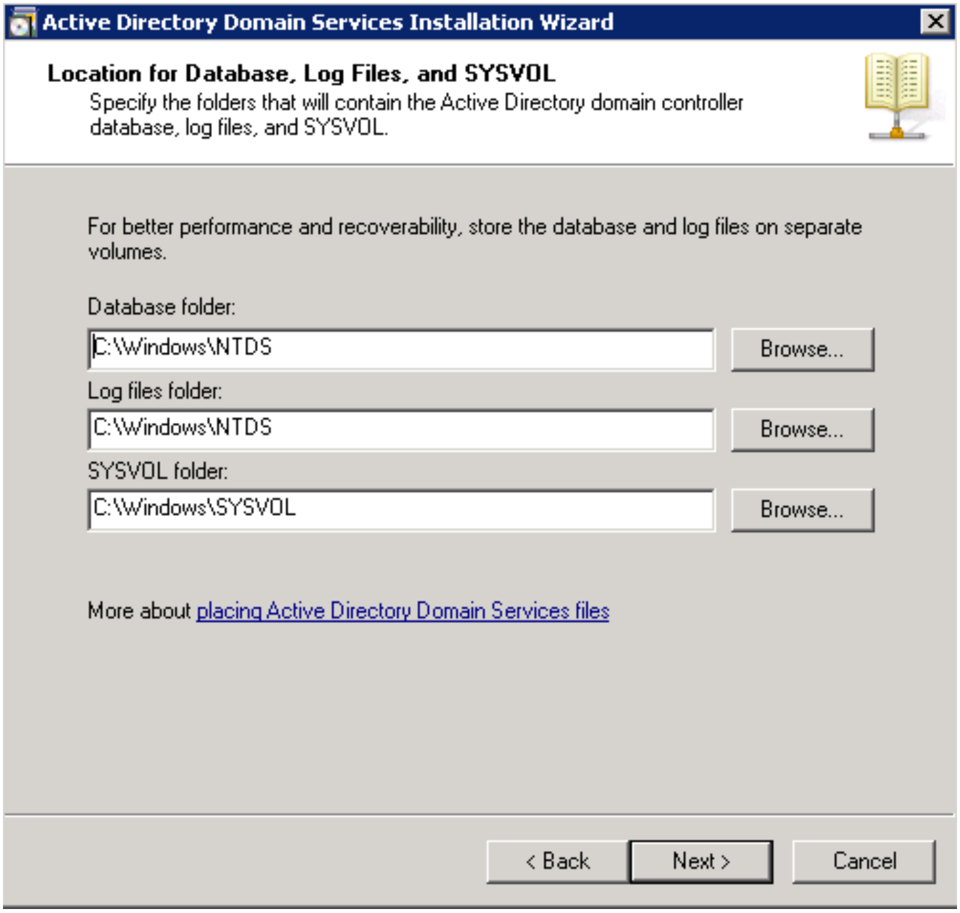


Active Directory Domain Services Installation Wizard

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?

16. Select the folders Active Directory should use for its 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.

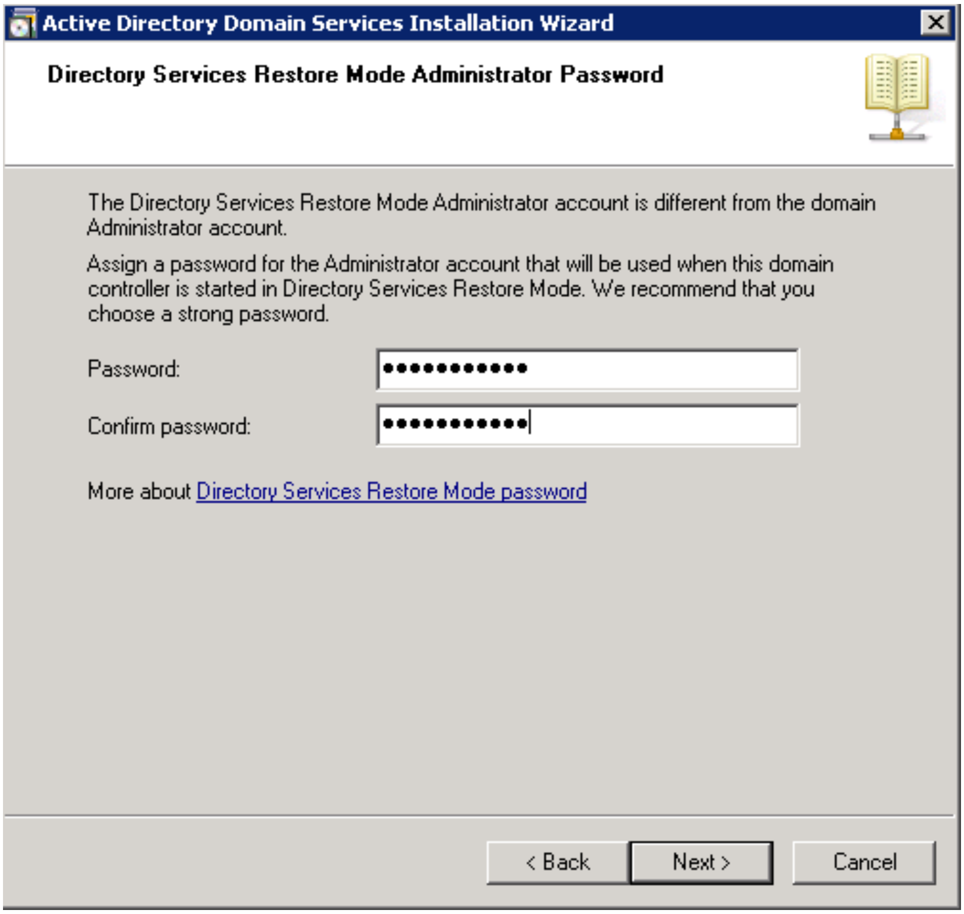
Database folder: C:\Windows\NTDS

Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

More about placing Active Directory Domain Services files

17. Enter the Administrator Password, and click ***Next***.



Active Directory Domain Services Installation Wizard

Directory Services Restore Mode Administrator Password

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

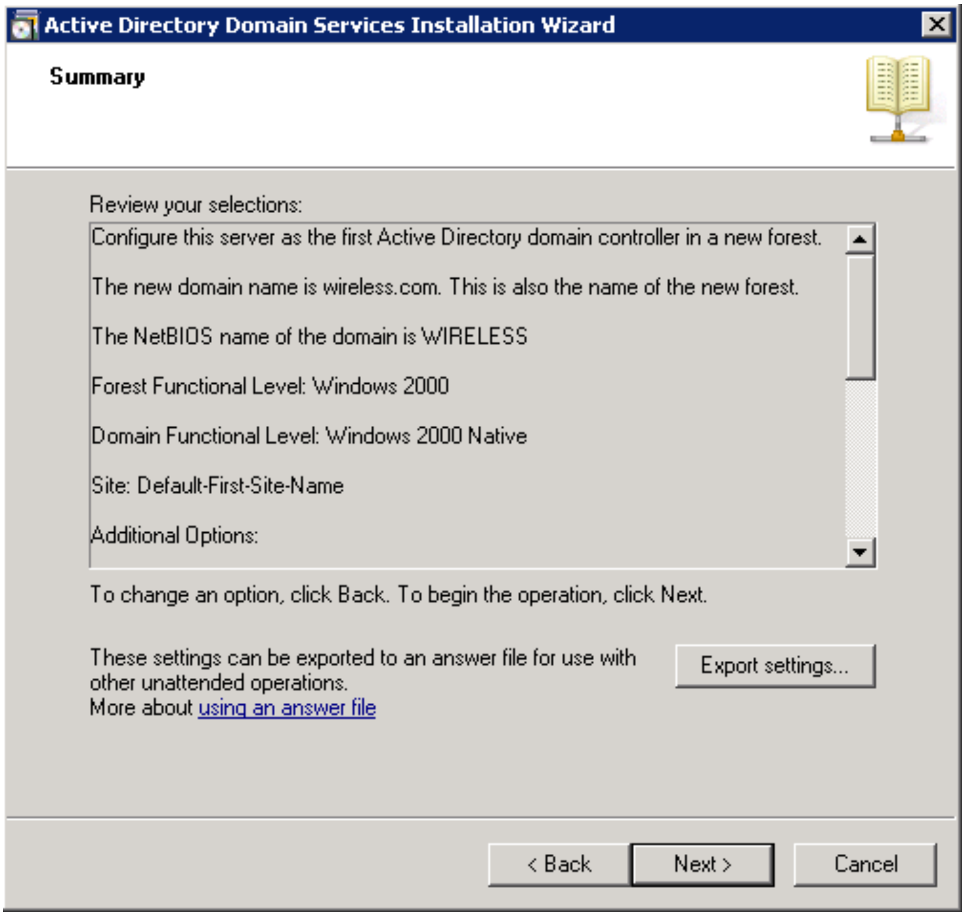
Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password: ●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●

More about Directory Services Restore Mode password

18. Review your selections, and click ***Next***.



Summary

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

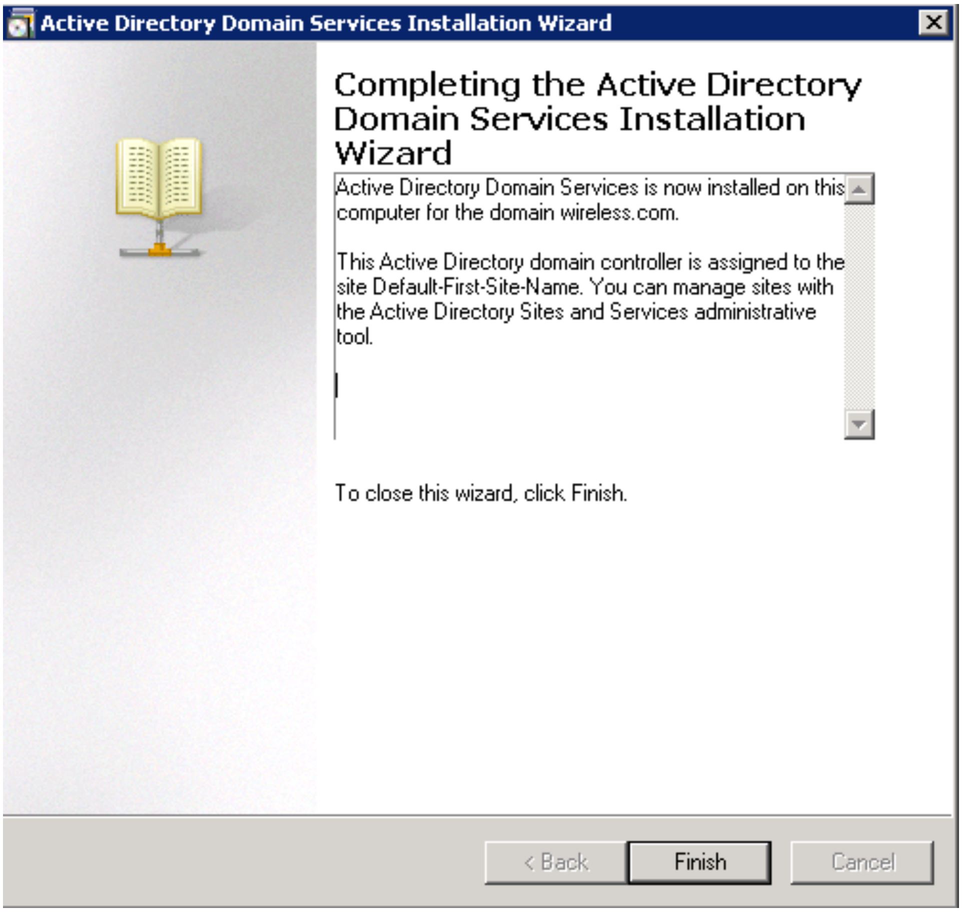
Additional Options:

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.

19. Click ***Finish*** to close the wizard.



Active Directory Domain Services Installation Wizard

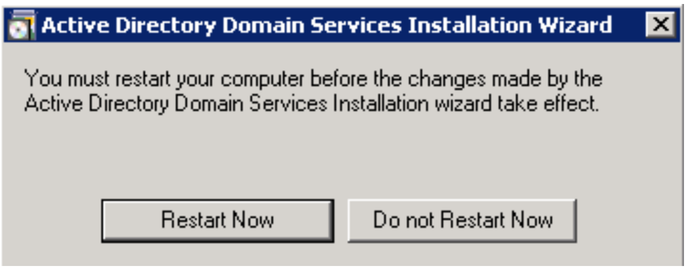
Completing the Active Directory Domain Services Installation Wizard

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.

20. Restart the server for the changes to take effect.



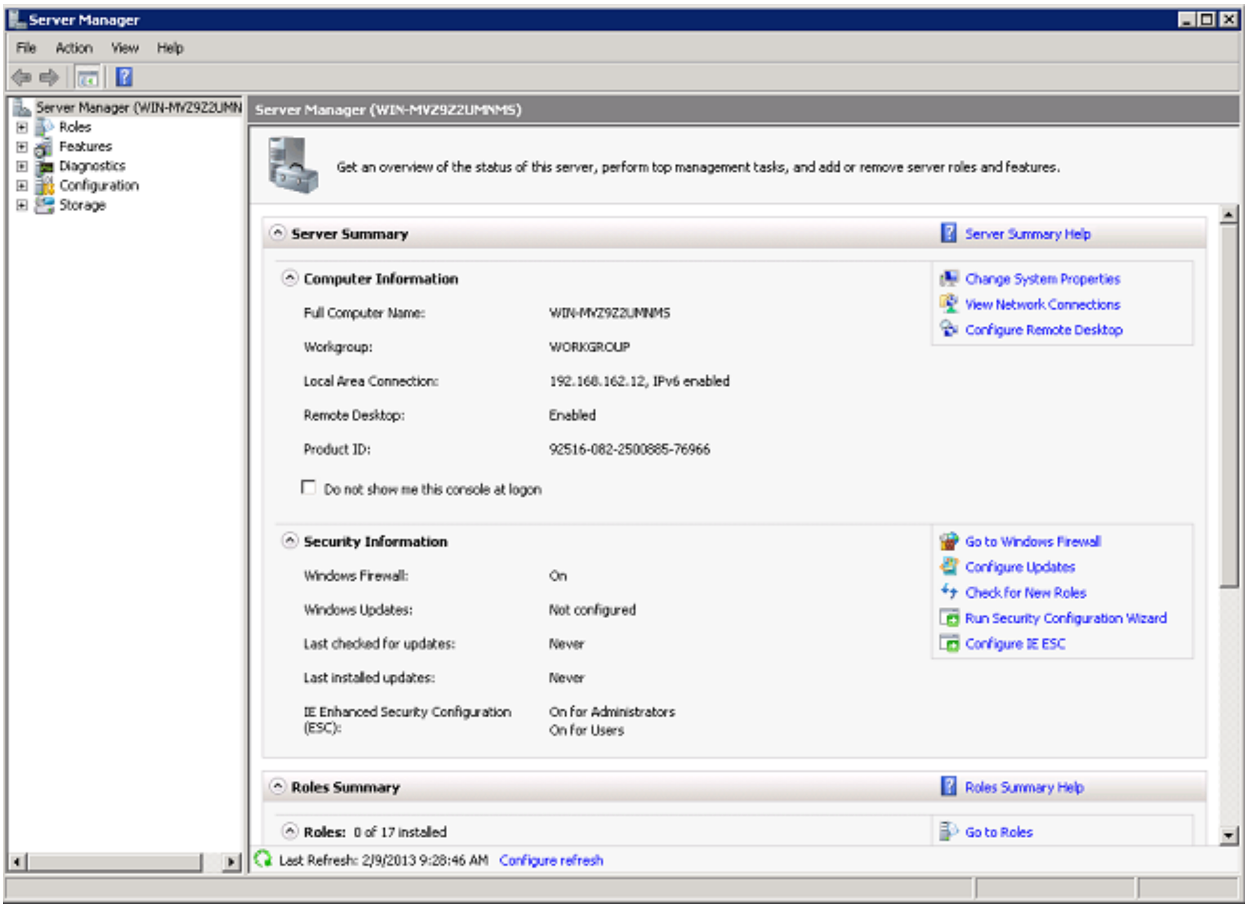
Active Directory Domain Services Installation Wizard

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

Install and Configure DHCP Services on the Microsoft Windows 2008 Server

The DHCP service on the Microsoft 2008 server is used to provide IP addresses to the wireless clients. Complete these steps in order to install and configure DHCP services:

1. Click ***Start*** > ***Server Manager***.



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:	WIN-MVZ9Z2UMNMS
Workgroup:	WORKGROUP
Local Area Connection:	192.168.162.12, IPv6 enabled
Remote Desktop:	Enabled
Product ID:	92516-082-2500885-76966

□ Do not show me this console at logon

Security Information

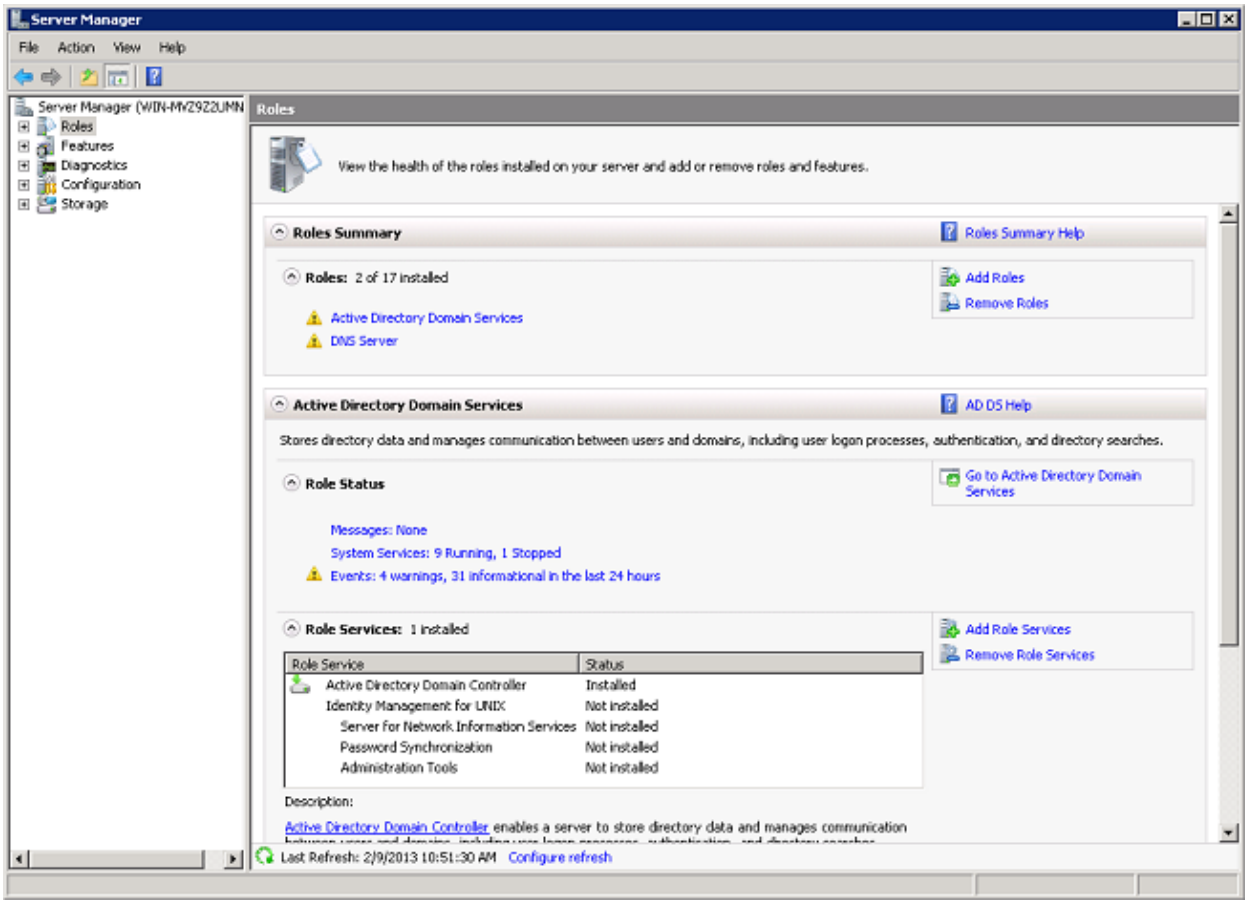
Windows Firewall:	On
Windows Updates:	Not configured
Last checked for updates:	Never
Last installed updates:	Never
IE Enhanced Security Configuration (ESC):	On for Administrators On for Users

Roles Summary

Roles: 0 of 17 installed

Last Refresh: 2/9/2013 9:28:46 AM

2. Click ***Roles*** > ***Add Roles***.



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

Roles Summary

Roles: 2 of 17 installed

Active Directory Domain Services

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

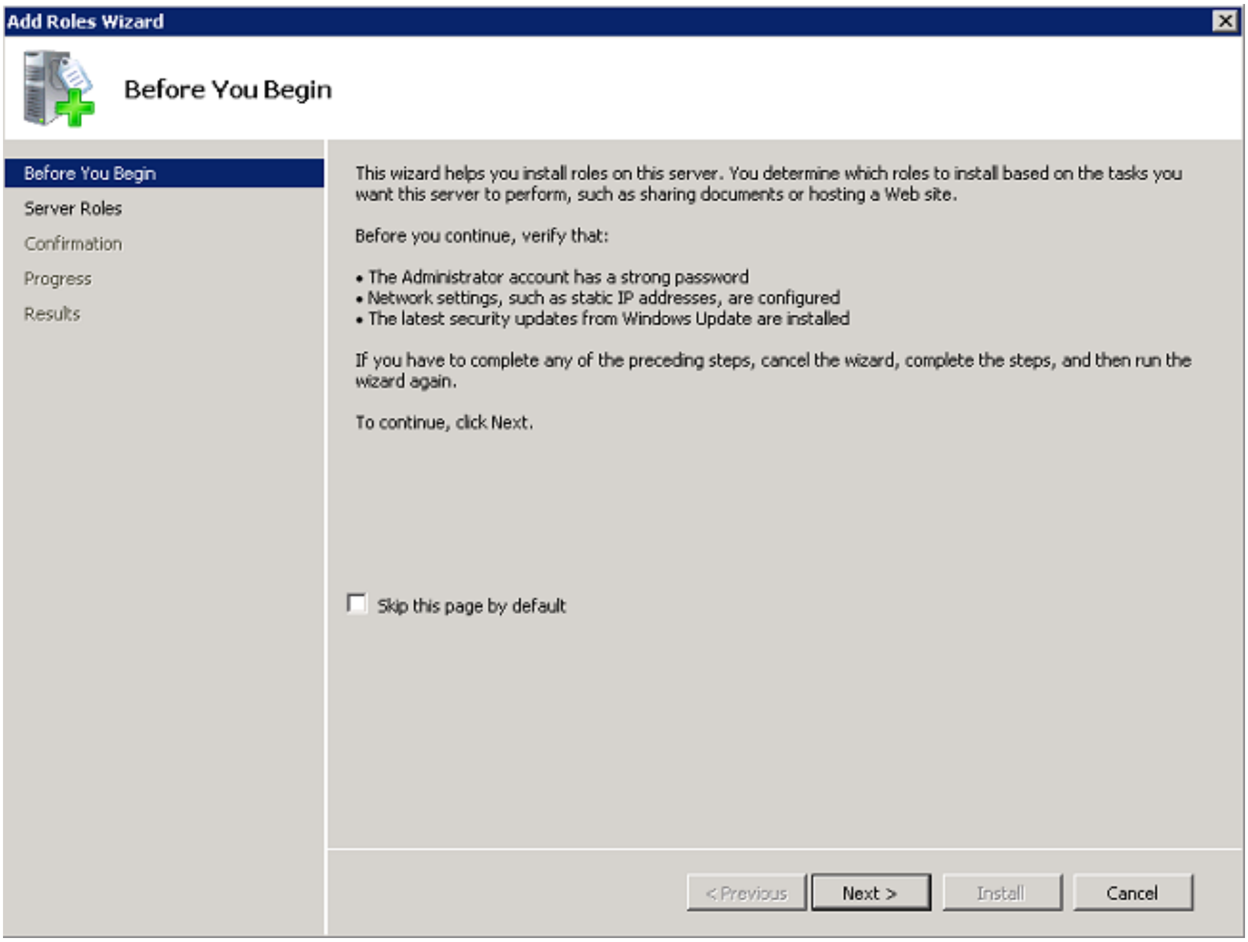
Role Service	Status
Active Directory Domain Controller	Installed
Identity Management for UNIX	Not installed
Server for Network Information Services	Not installed
Password Synchronization	Not installed
Administration Tools	Not installed

Description:

Active Directory Domain Controller enables a server to store directory data and manages communication

Last Refresh: 2/9/2013 10:51:30 AM

3. Click ***Next***.



Add Roles Wizard

Before You Begin

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:

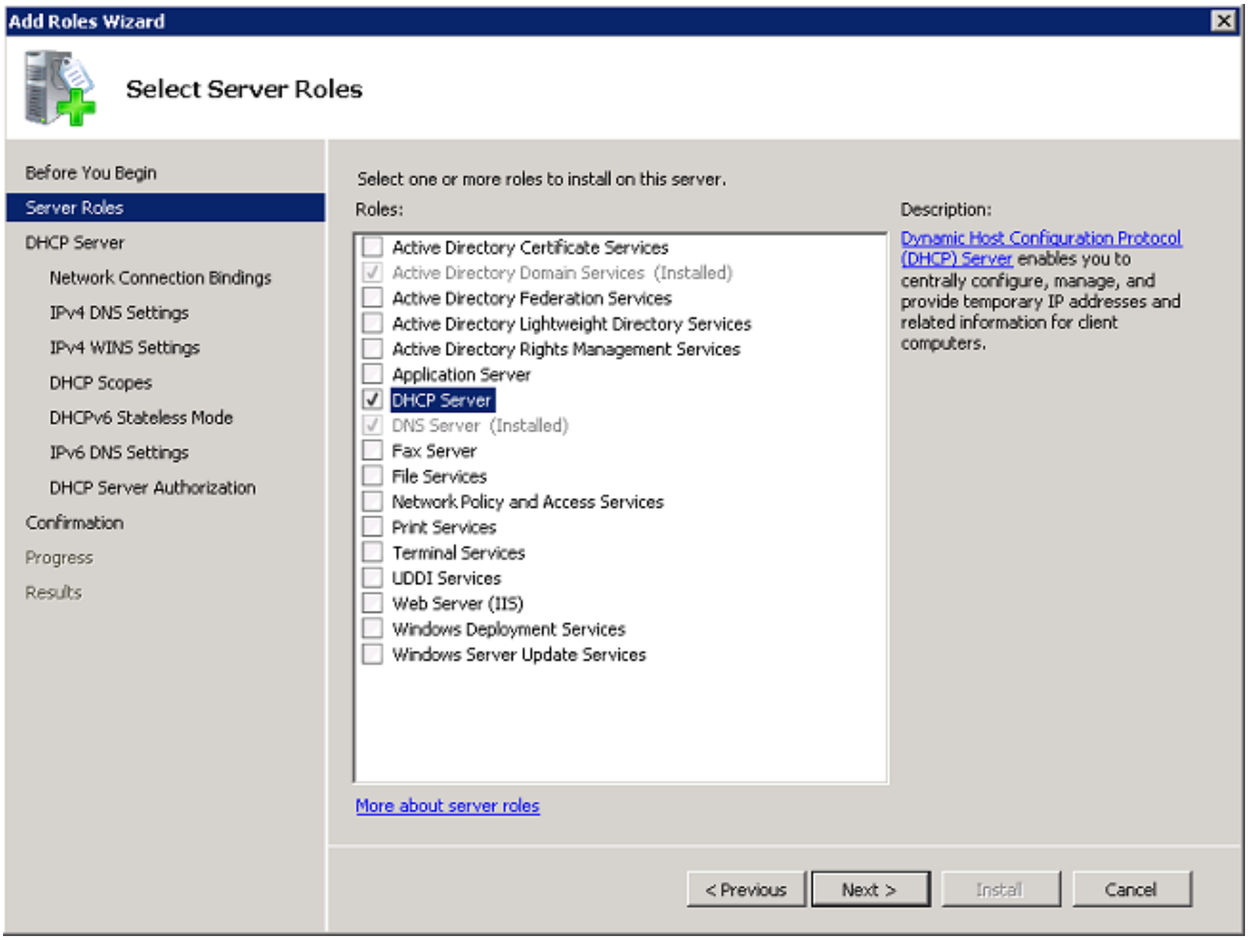
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

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

4. Select the service ***DHCP Server***, and click ***Next***.



Select one or more roles to install on this server.

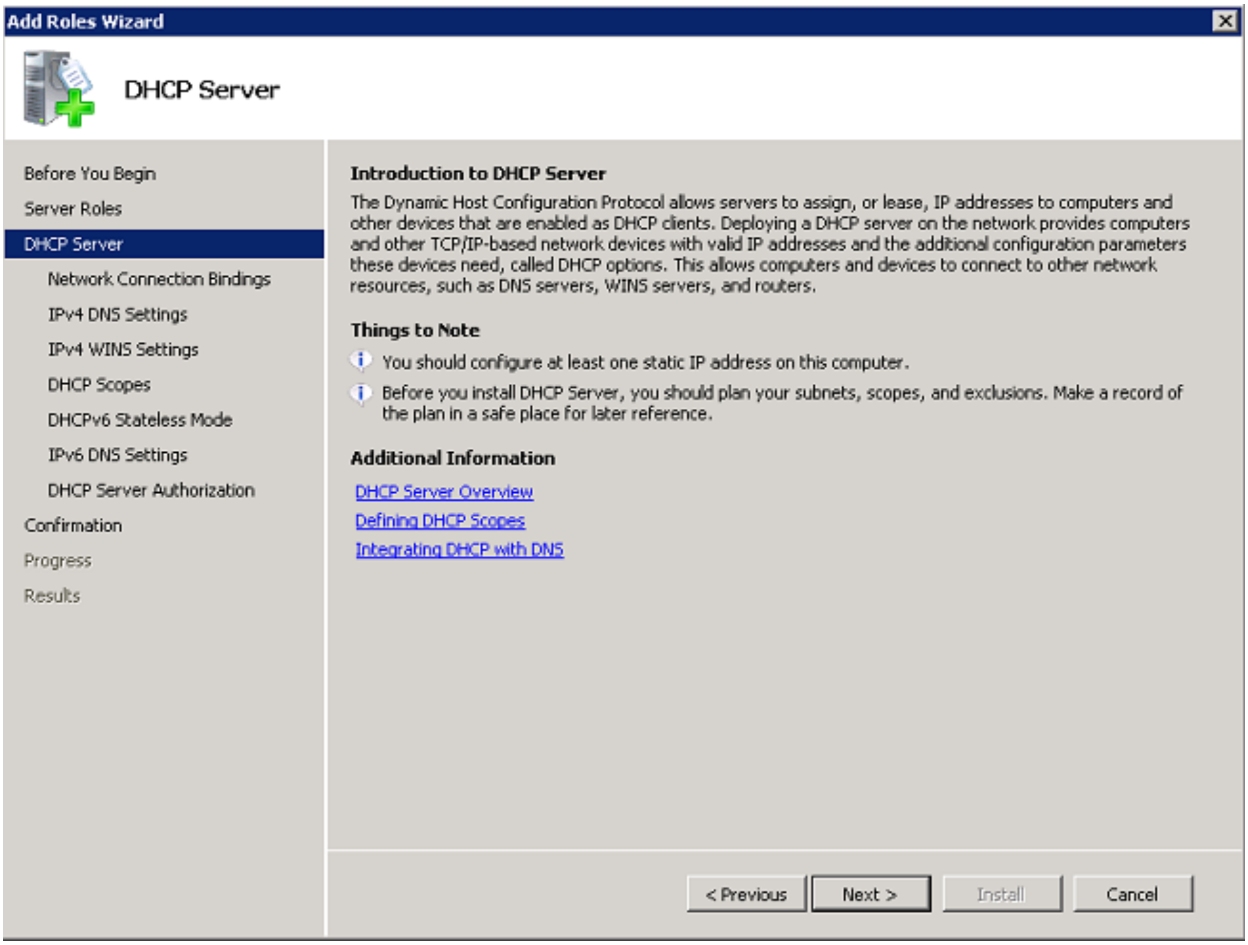
Roles:

□ 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
☑ 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:

Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.

5. Review the Introduction to DHCP Server, and click ***Next***.



Introduction to DHCP Server

The Dynamic Host Configuration Protocol allows servers to assign, or lease, IP addresses to computers and other devices that are enabled as DHCP clients. Deploying a DHCP server on the network provides computers and other TCP/IP-based network devices with valid IP addresses and the additional configuration parameters these devices need, called DHCP options. This allows computers and devices to connect to other network resources, such as DNS servers, WINS servers, and routers.

Things to Note

ⓘ You should configure at least one static IP address on this computer.

ⓘ Before you install DHCP Server, you should plan your subnets, scopes, and exclusions. Make a record of the plan in a safe place for later reference.

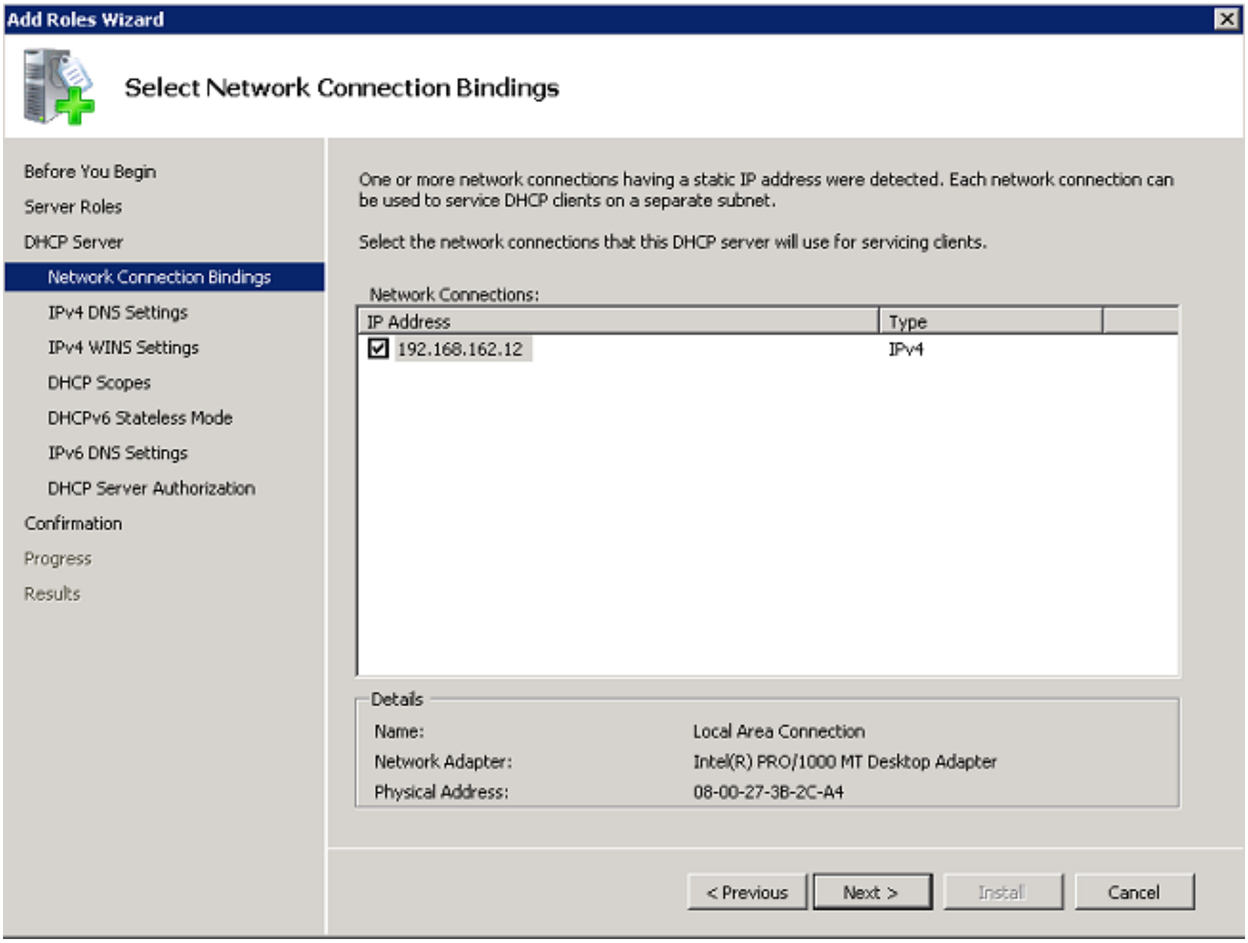
Additional Information

DHCP Server Overview

Defining DHCP Scopes

Integrating DHCP with DNS

6. Select the interface that the DHCP server should monitor for requests, and click ***Next***.



Select Network Connection Bindings

One or more network connections having a static IP address were detected. Each network connection can be used to service DHCP clients on a separate subnet.

Select the network connections that this DHCP server will use for servicing clients.

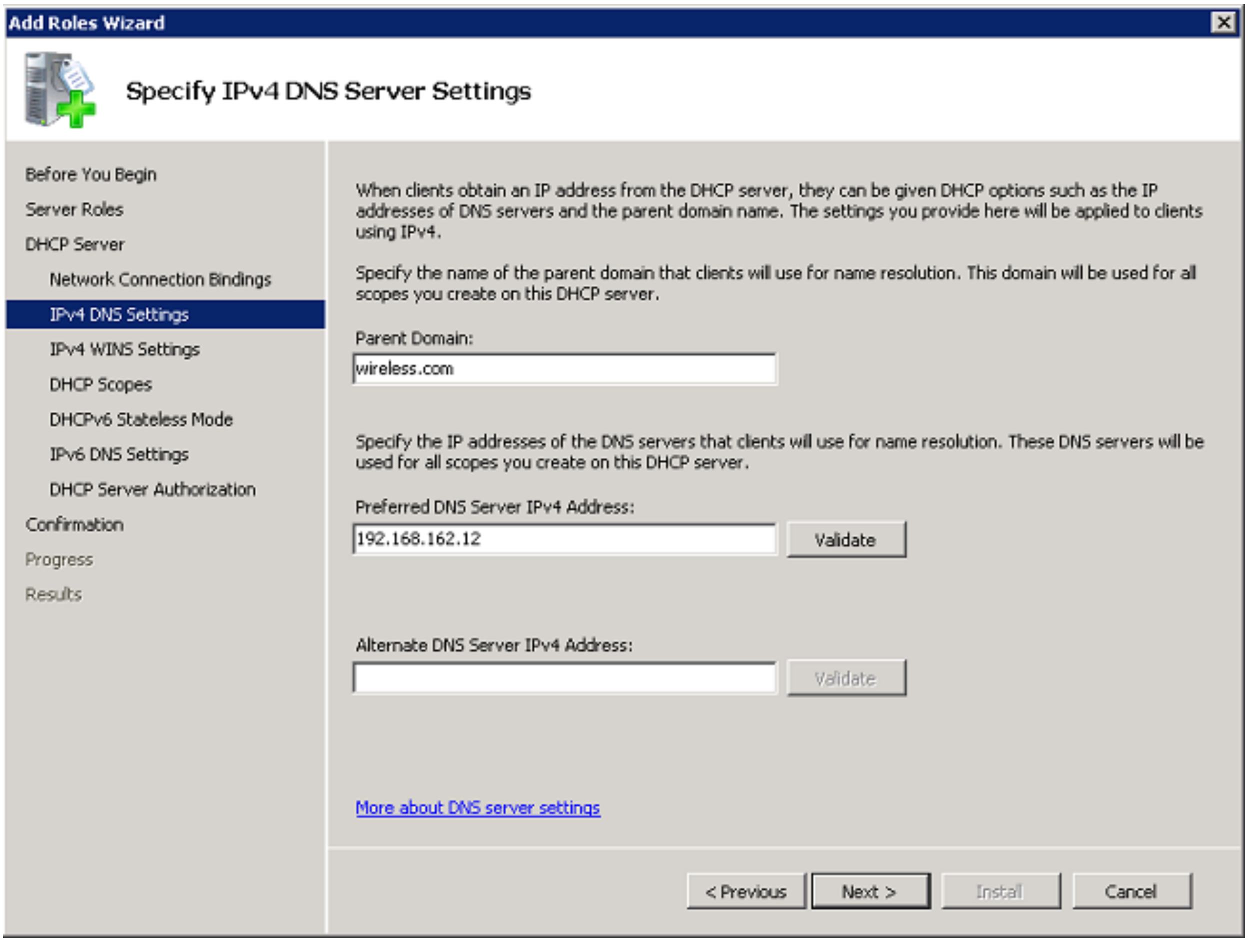
Network Connections:

IP Address	Type
☑ 192.168.162.12	IPv4

Details

Name:	Local Area Connection
Network Adapter:	Intel(R) PRO/1000 MT Desktop Adapter
Physical Address:	08-00-27-3B-2C-A4

7. Configure the default DNS settings the DHCP server should provide to clients, and click ***Next***.



When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of DNS servers and the parent domain name. The settings you provide here will be applied to clients using IPv4.

Specify the name of the parent domain that clients will use for name resolution. This domain will be used for all scopes you create on this DHCP server.

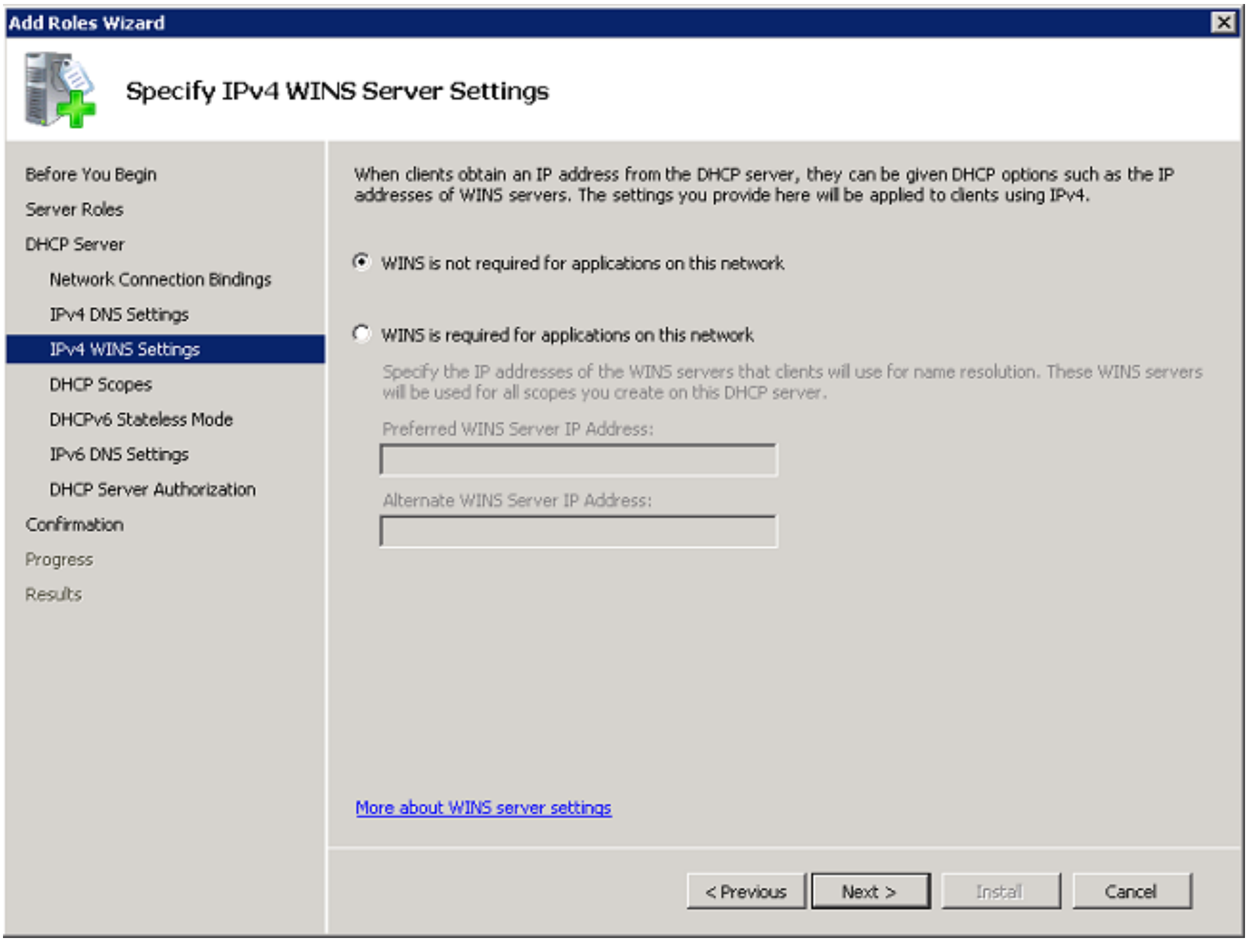
Parent Domain: wireless.com

Specify the IP addresses of the DNS servers that clients will use for name resolution. These DNS servers will be used for all scopes you create on this DHCP server.

Preferred DNS Server IPv4 Address: 192.168.162.12

Alternate DNS Server IPv4 Address:

8. Configure WINS if the network supports WINS.



Add Roles Wizard

Specify IPv4 WINS Server Settings

When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of WINS servers. The settings you provide here will be applied to clients using IPv4.

● WINS is not required for applications on this network

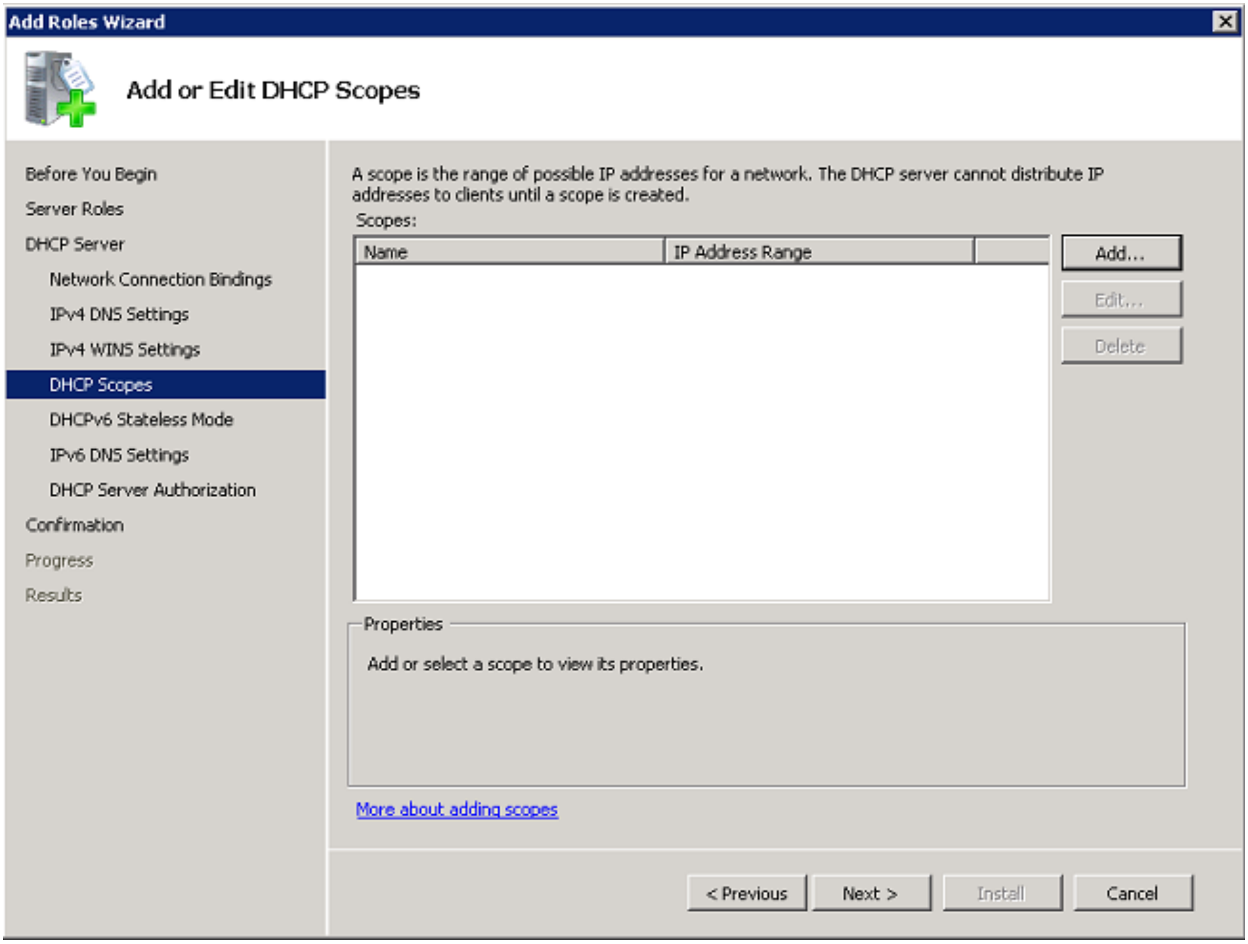
○ WINS is required for applications on this network

Specify the IP addresses of the WINS servers that clients will use for name resolution. These WINS servers will be used for all scopes you create on this DHCP server.

Preferred WINS Server IP Address:

Alternate WINS Server IP Address:

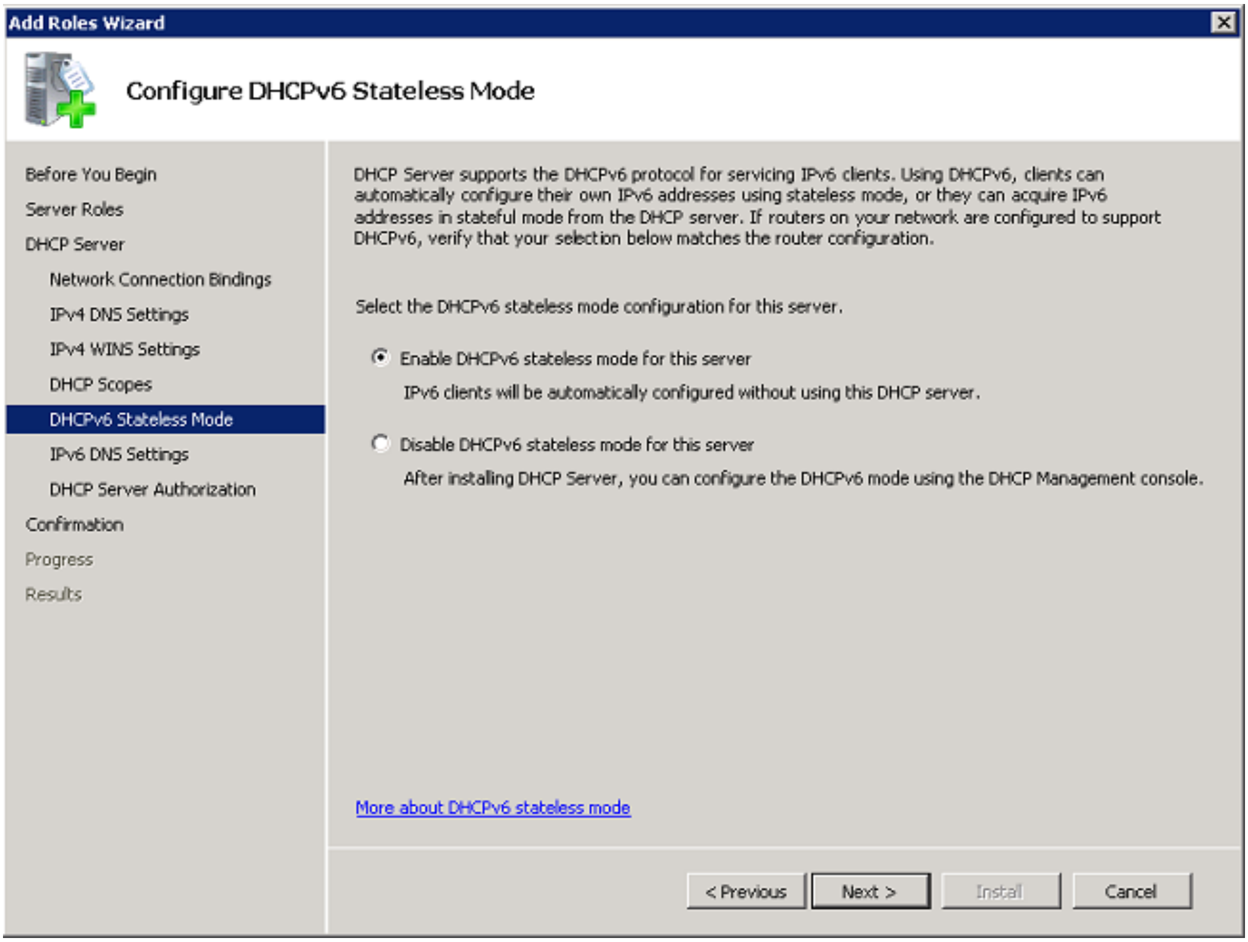
9. Click ***Add*** to use the wizard to create a DHCP Scope or click ***Next*** to create a DHCP scope later. Click ***Next*** to continue.



A scope is the range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.

Add or select a scope to view its properties.

10. Enable or disable DHCPv6 support on the server, and click ***Next***.



Configure DHCPv6 Stateless Mode

DHCP Server supports the DHCPv6 protocol for servicing IPv6 clients. Using DHCPv6, clients can automatically configure their own IPv6 addresses using stateless mode, or they can acquire IPv6 addresses in stateful mode from the DHCP server. If routers on your network are configured to support DHCPv6, verify that your selection below matches the router configuration.

Select the DHCPv6 stateless mode configuration for this server.

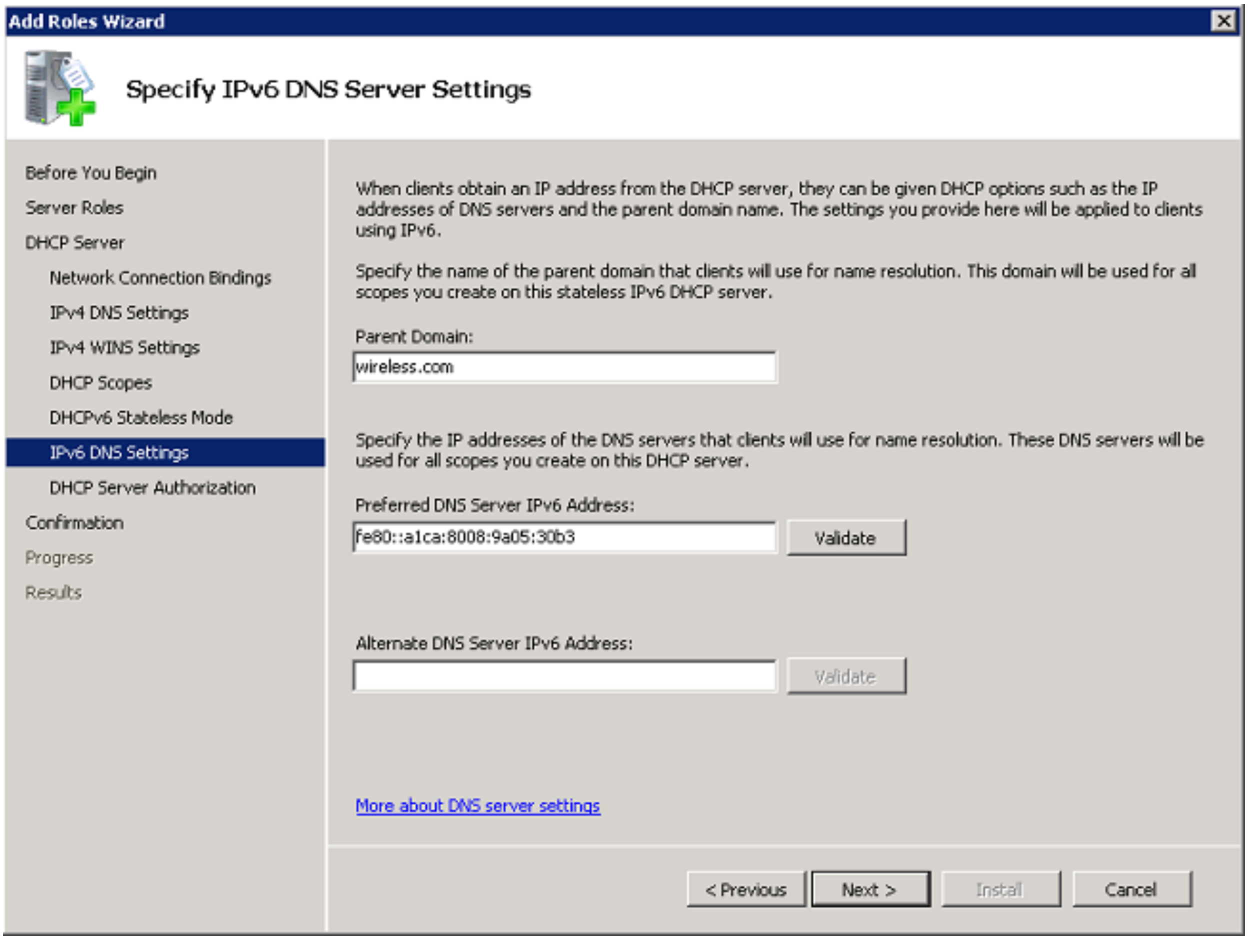
● Enable DHCPv6 stateless mode for this server

IPv6 clients will be automatically configured without using this DHCP server.

○ Disable DHCPv6 stateless mode for this server

After installing DHCP Server, you can configure the DHCPv6 mode using the DHCP Management console.

11. Configure IPv6 DNS settings if DHCPv6 was enabled in the preceding step. Click ***Next*** to continue.



When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of DNS servers and the parent domain name. The settings you provide here will be applied to clients using IPv6.

Specify the name of the parent domain that clients will use for name resolution. This domain will be used for all scopes you create on this stateless IPv6 DHCP server.

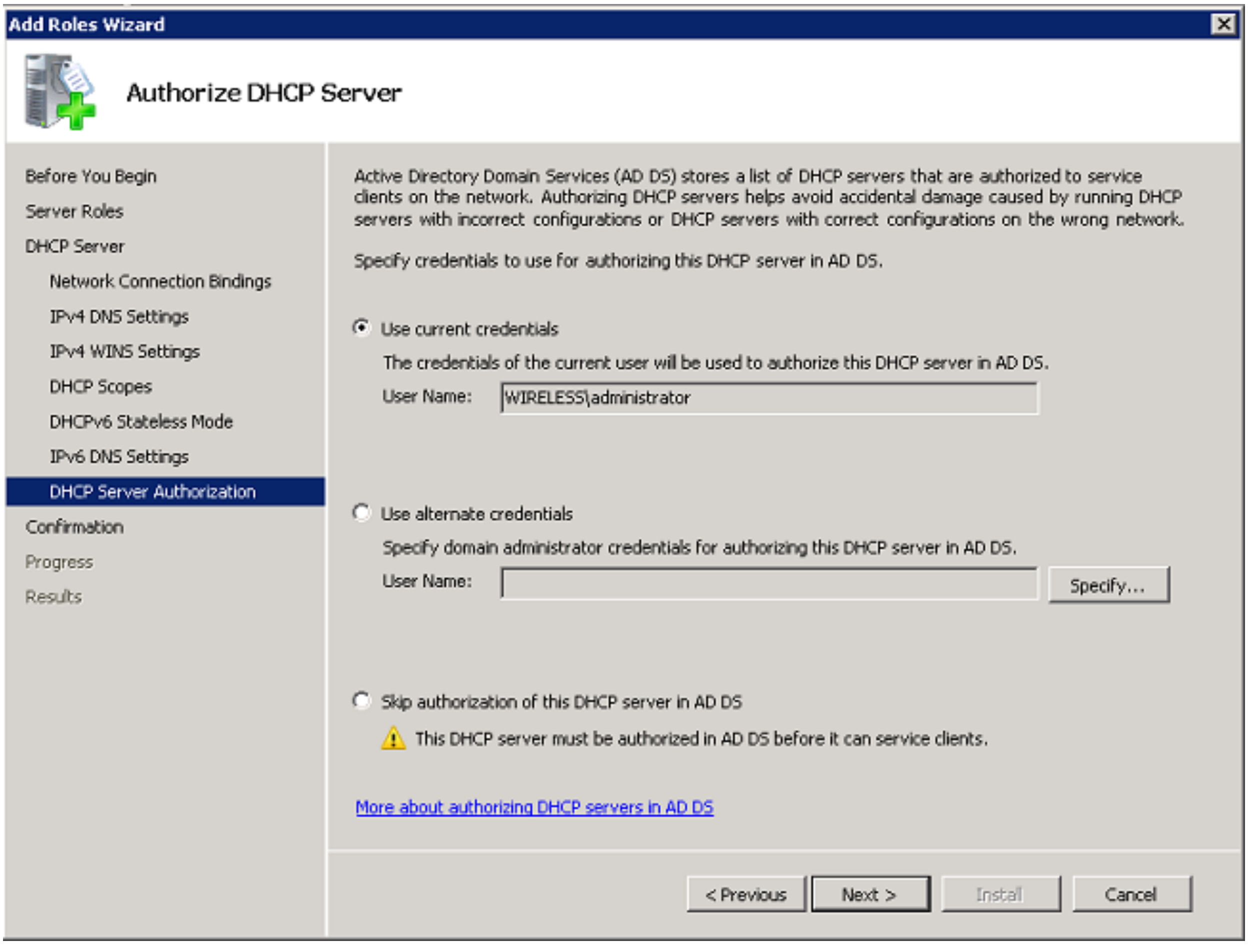
Parent Domain: wireless.com

Specify the IP addresses of the DNS servers that clients will use for name resolution. These DNS servers will be used for all scopes you create on this DHCP server.

Preferred DNS Server IPv6 Address: fe80::a1ca:8008:9a05:30b3

Alternate DNS Server IPv6 Address:

12. Provide domain administrator credentials to authorize the DHCP server in Active Directory, and click ***Next***.



Active Directory Domain Services (AD DS) stores a list of DHCP servers that are authorized to service clients on the network. Authorizing DHCP servers helps avoid accidental damage caused by running DHCP servers with incorrect configurations or DHCP servers with correct configurations on the wrong network.

Specify credentials to use for authorizing this DHCP server in AD DS.

● Use current credentials

The credentials of the current user will be used to authorize this DHCP server in AD DS.

User Name: WIRELESS\administrator

○ Use alternate credentials

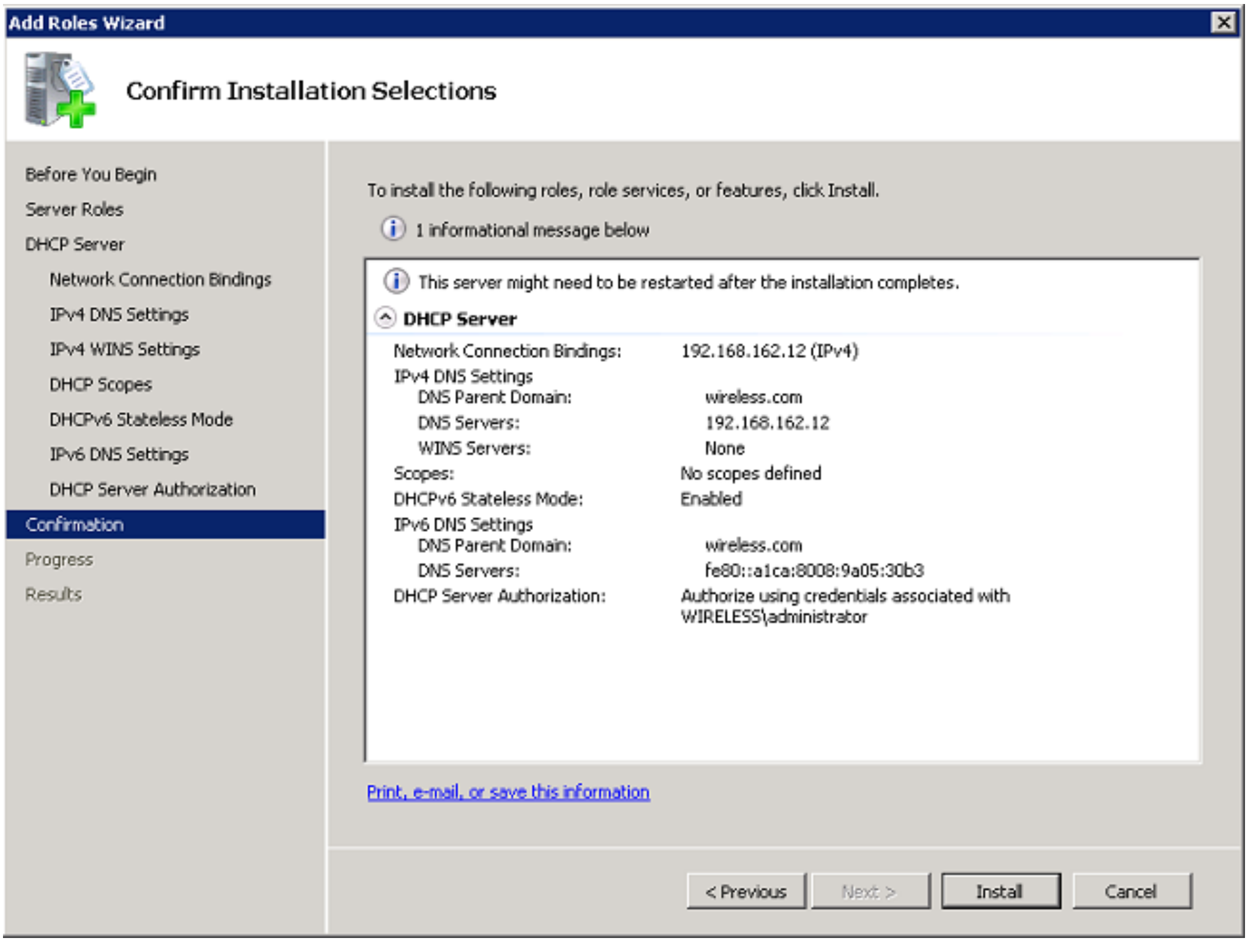
Specify domain administrator credentials for authorizing this DHCP server in AD DS.

User Name:

○ Skip authorization of this DHCP server in AD DS

⚠ This DHCP server must be authorized in AD DS before it can service clients.

13. Review the configuration on the confirmation page, and click ***Install*** to complete the install.



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

1 informational message below

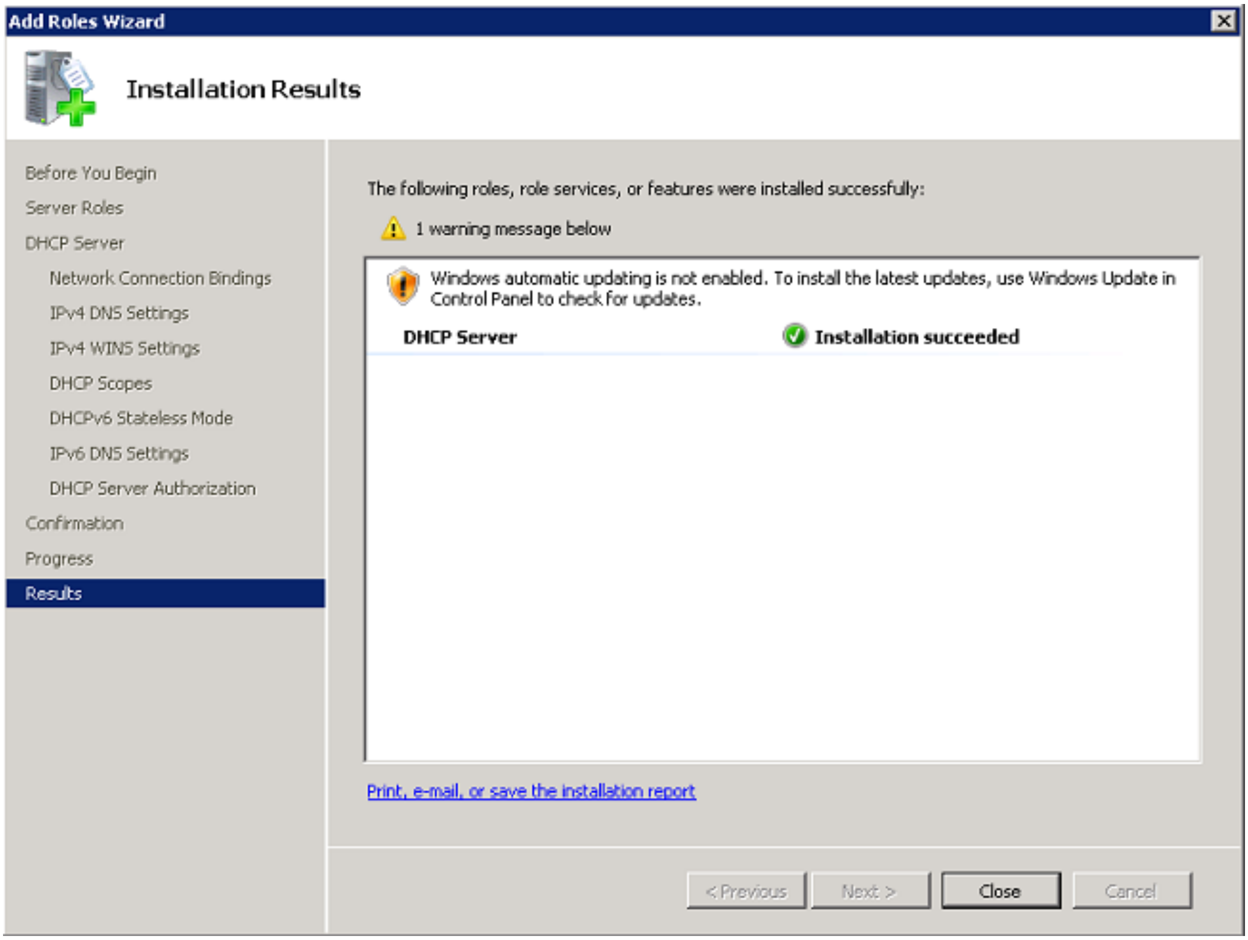
This server might need to be restarted after the installation completes.

DHCP Server

Network Connection Bindings:	192.168.162.12 (IPv4)
IPv4 DNS Settings	
DNS Parent Domain:	wireless.com
DNS Servers:	192.168.162.12
WINS Servers:	None
Scopes:	No scopes defined
DHCPv6 Stateless Mode:	Enabled
IPv6 DNS Settings	
DNS Parent Domain:	wireless.com
DNS Servers:	fe80::a1ca:8008:9a05:30b3
DHCP Server Authorization:	Authorize using credentials associated with WIRELESS\administrator

The installation proceeds.

14. Click ***Close*** to close the wizard.



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

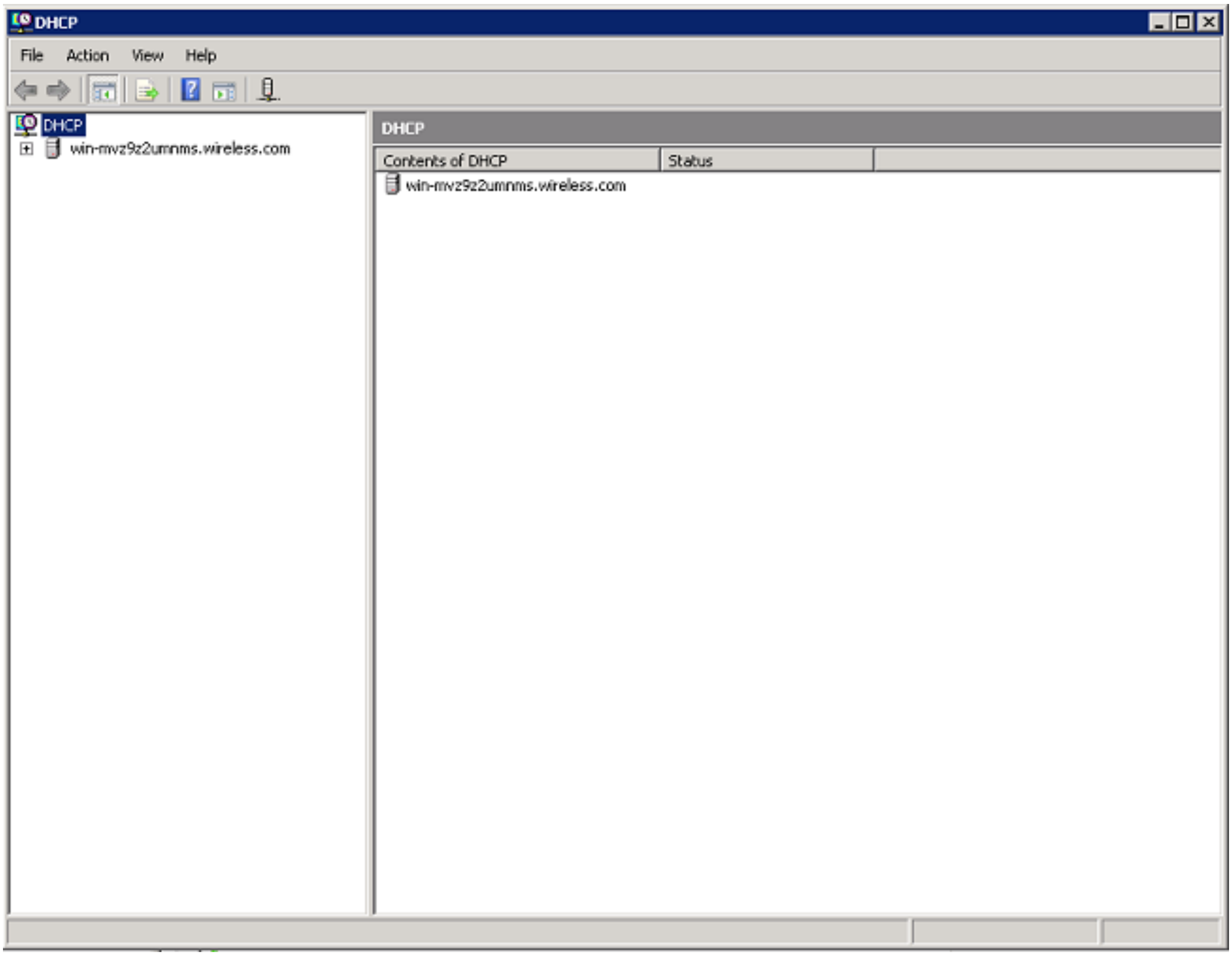
⚠ 1 warning message below

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

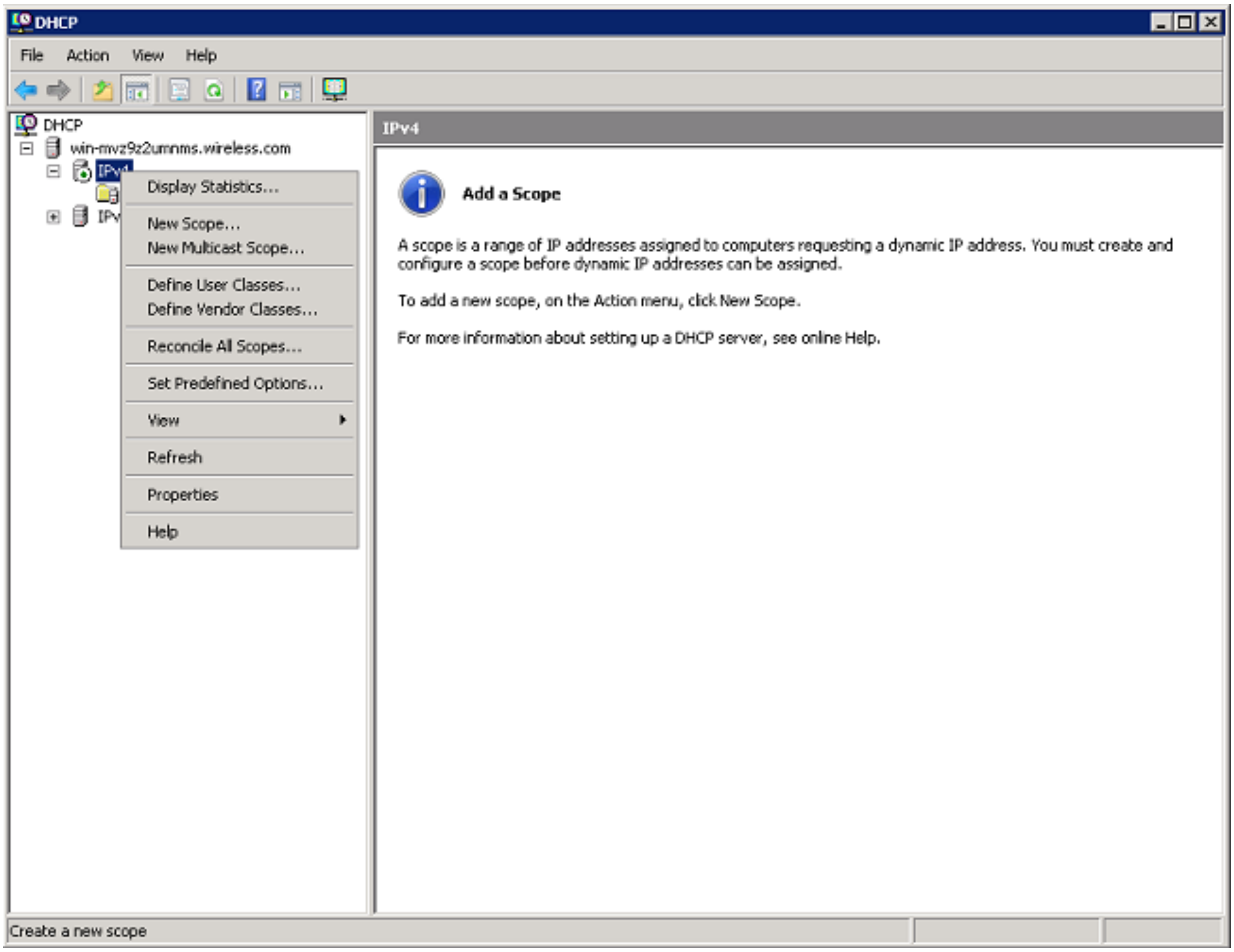
DHCP Server	✓ **Installation succeeded**

The DHCP Server is now installed.

15. Click ***Start*** > ***Administrative Tools*** > ***DHCP*** to configure DHCP service.



16. Expand the DHCP server (win−mvz9z2umms.wireless.com in this example), right−click IPv4, and choose ***New Scope***. to create a DHCP Scope.



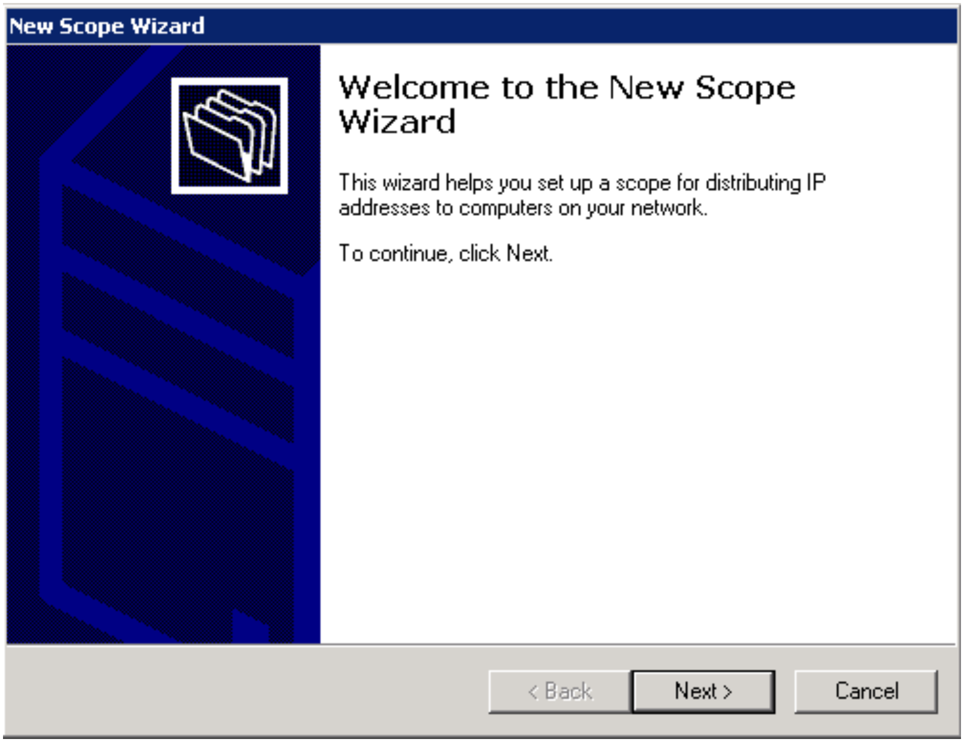
Add a Scope

A scope is a range of IP addresses assigned to computers requesting a dynamic IP address. You must create and configure a scope before dynamic IP addresses can be assigned.

To add a new scope, on the Action menu, click New Scope.

For more information about setting up a DHCP server, see online Help.

17. Click ***Next*** to configure the new scope via the New Scope Wizard.

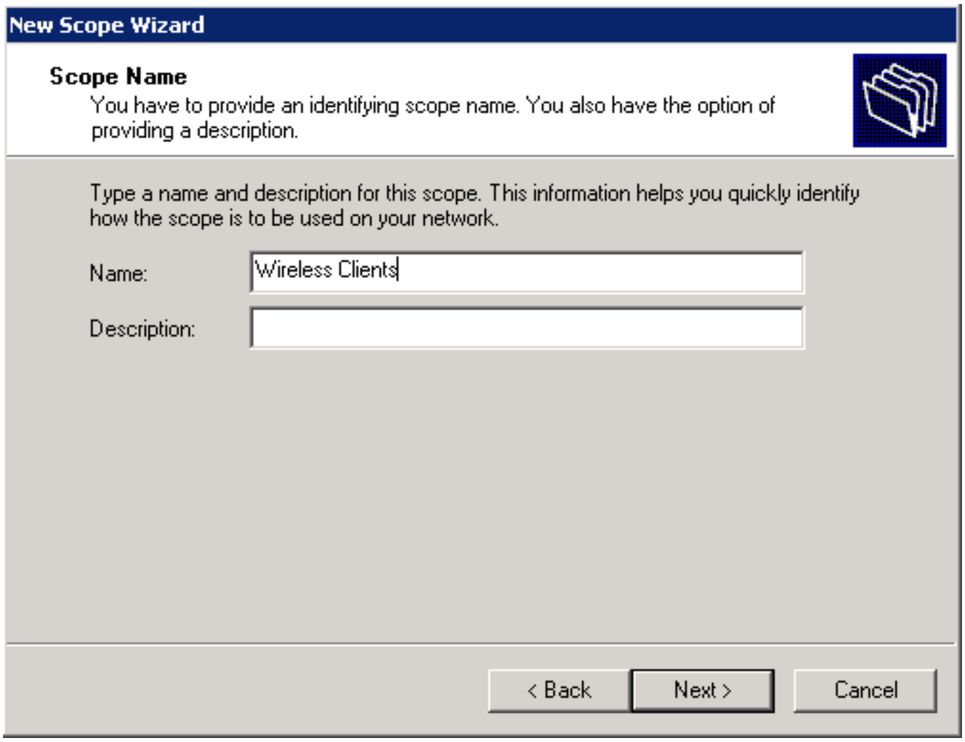


Welcome to the New Scope Wizard

This wizard helps you set up a scope for distributing IP addresses to computers on your network.

To continue, click Next.

18. Provide a name for the new scope (Wireless Clients in this example), and click ***Next***.



New Scope Wizard

Scope Name

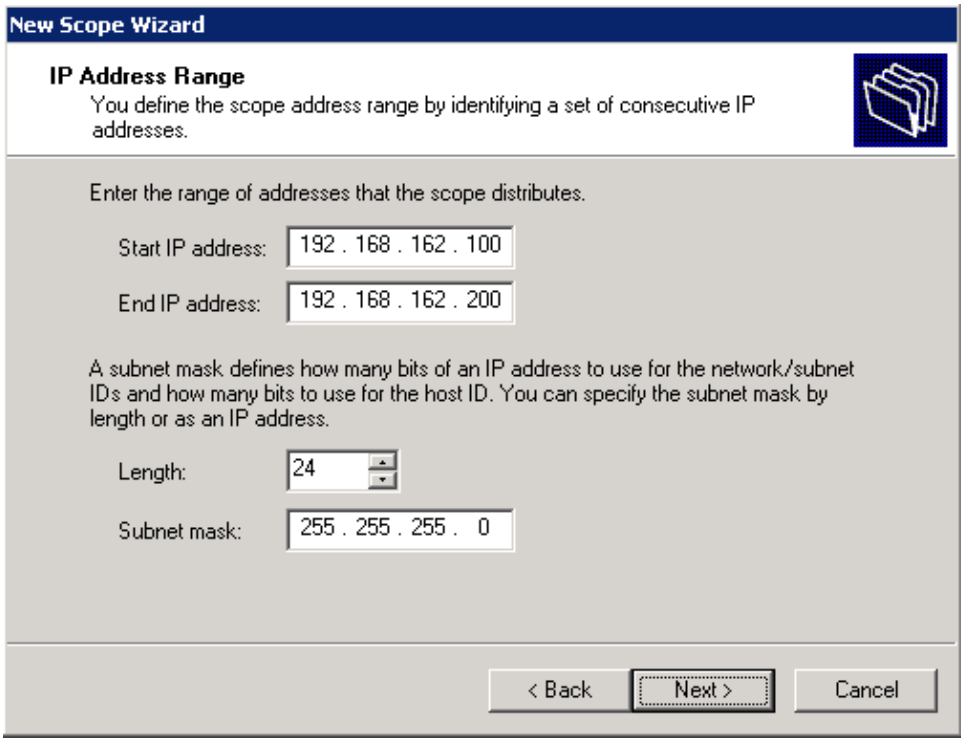
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: Wireless Clients

Description:

19. Enter the range of available IP addresses that can be used for DHCP leases. Click ***Next*** to continue.



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 162 . 100

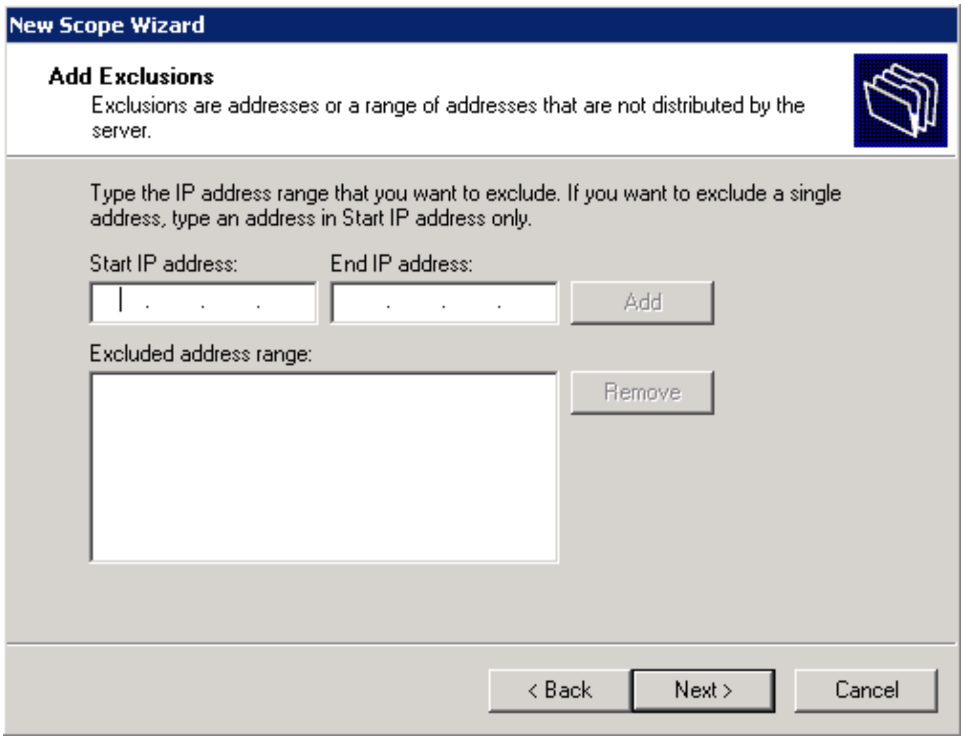
End IP address: 192 . 168 . 162 . 200

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

20. Create an optional list of excluded addresses. Click ***Next*** to continue.



New Scope Wizard

Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.

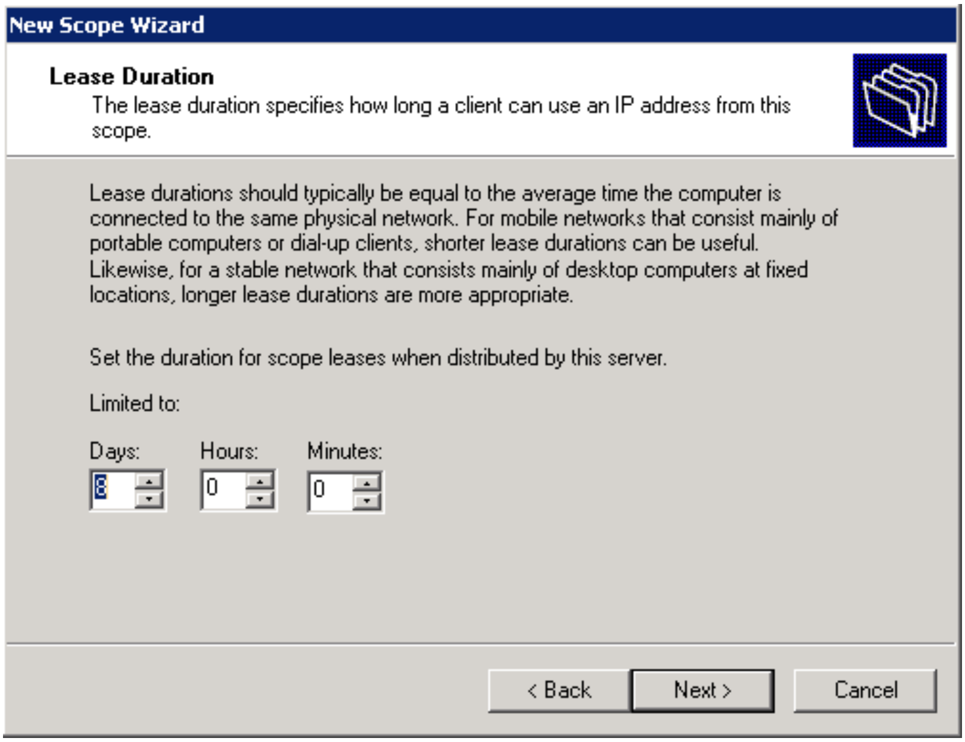
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Excluded address range:

21. Configure the lease time, and click ***Next***.



New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

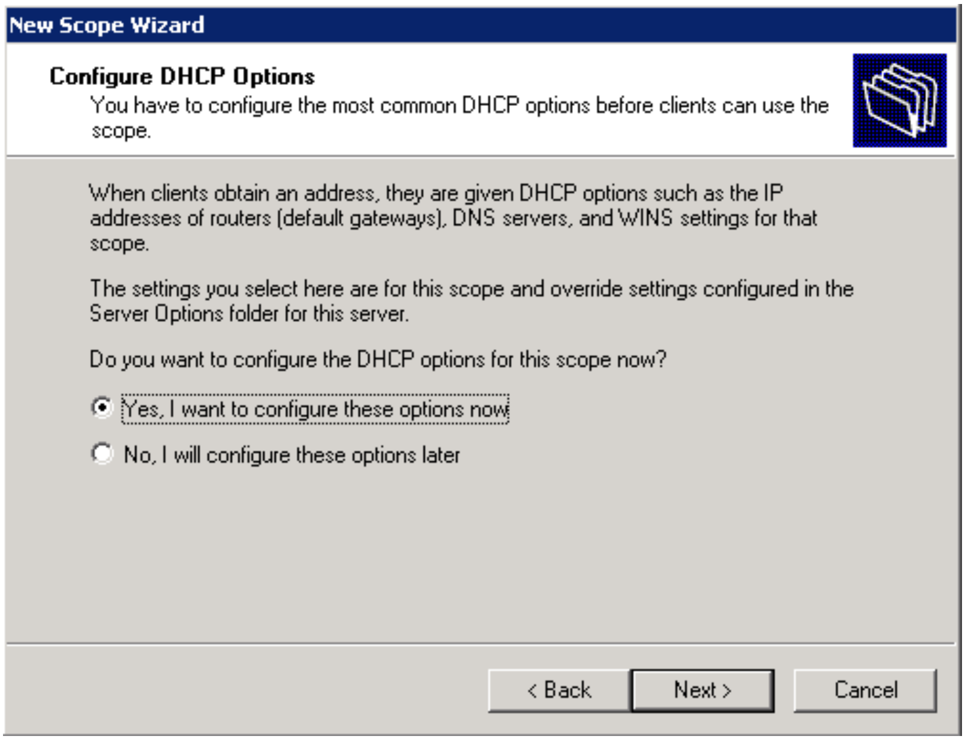
Limited to:

Days: 8

Hours: 0

Minutes: 0

22. Click ***Yes, I want to configure these options now***, and click ***Next***.


New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

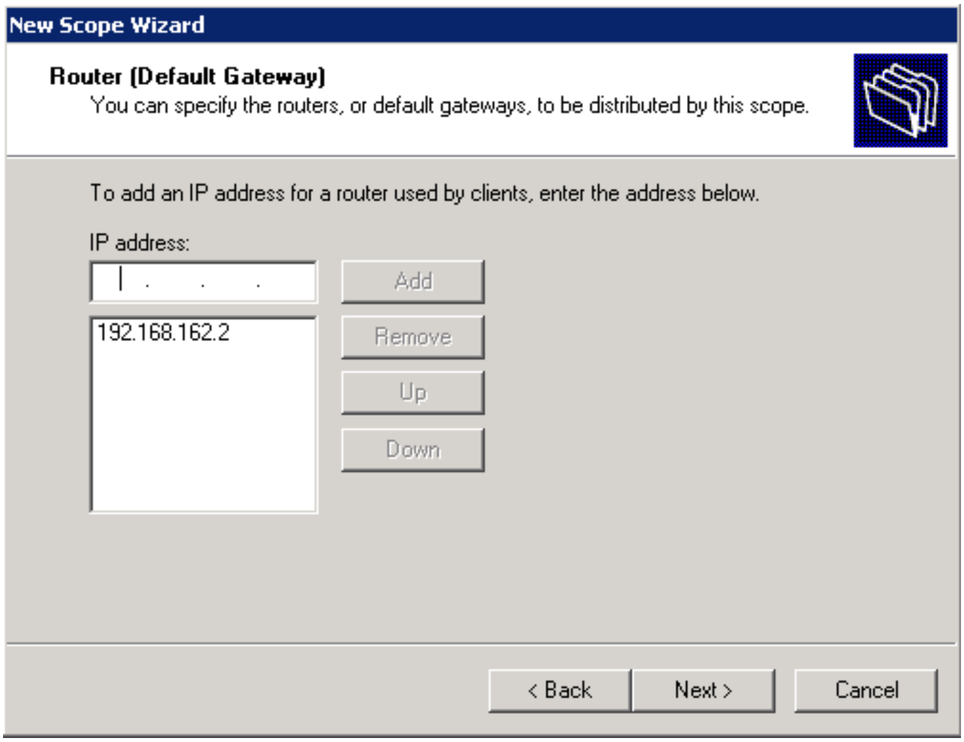
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

● Yes, I want to configure these options now

○ No, I will configure these options later

23. Enter the IP address of the default gateway for this scope, click ***Add*** > ***Next***.


New Scope Wizard

Router (Default Gateway)

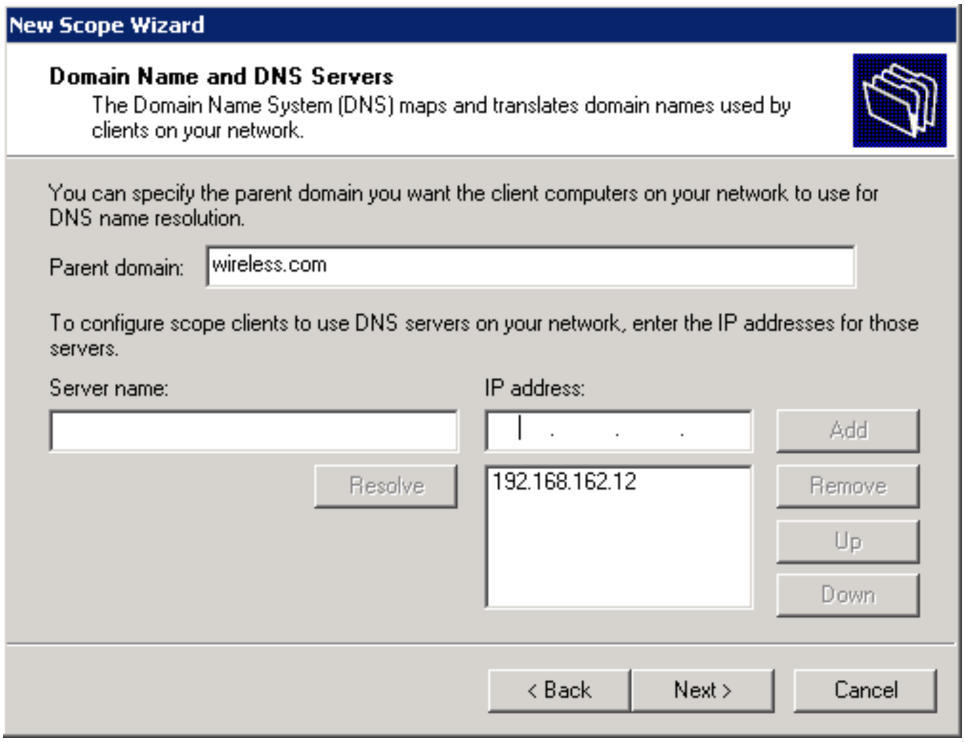
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

192.168.162.2

24. Configure the DNS domain name and DNS server to be used by the clients. Click ***Next*** to continue.



New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain: wireless.com

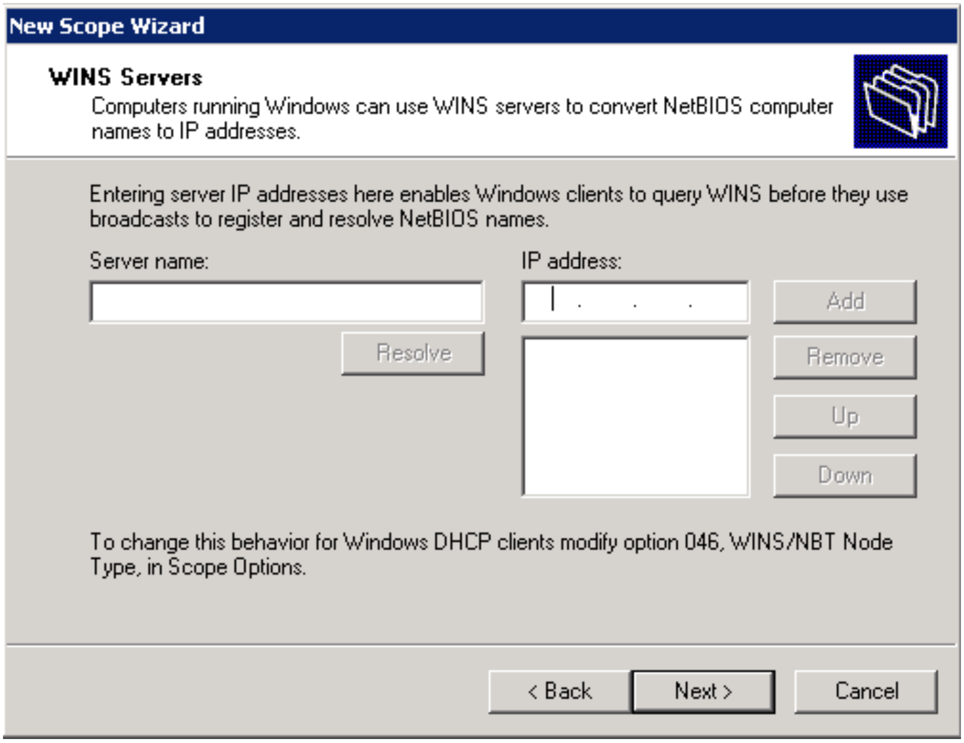
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

192.168.162.12

25. Enter WINS information for this scope if the network supports WINS. Click ***Next*** to continue.



New Scope Wizard

WINS Servers

Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

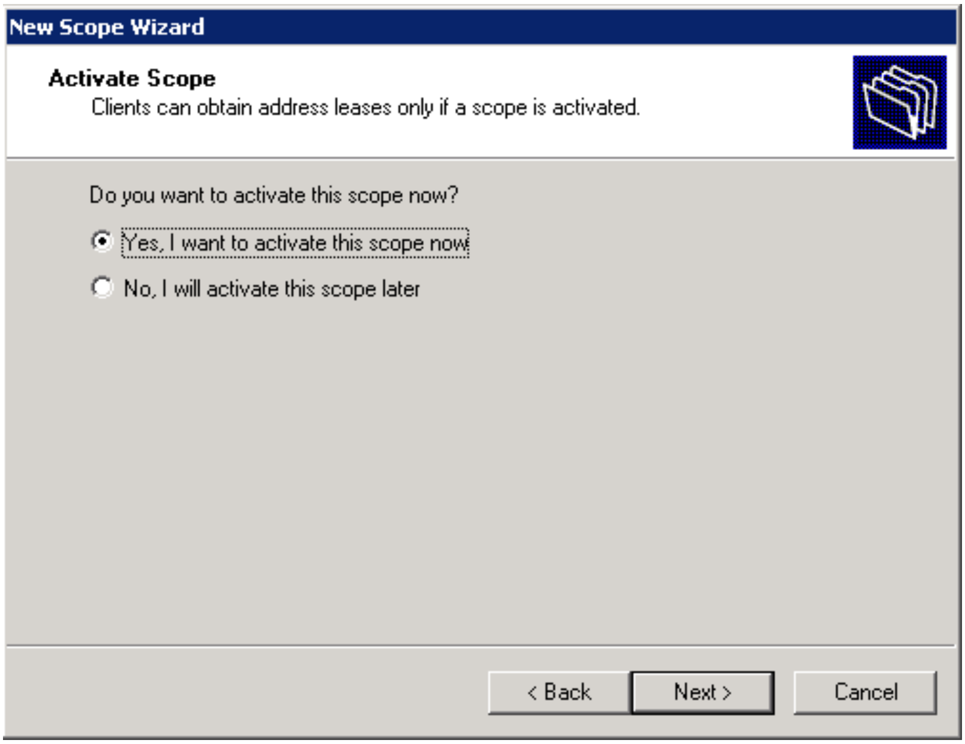
Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name:

IP address:

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

26. To activate this scope, click ***Yes, I want to activate this scope now*** > ***Next***.


New Scope Wizard

Activate Scope

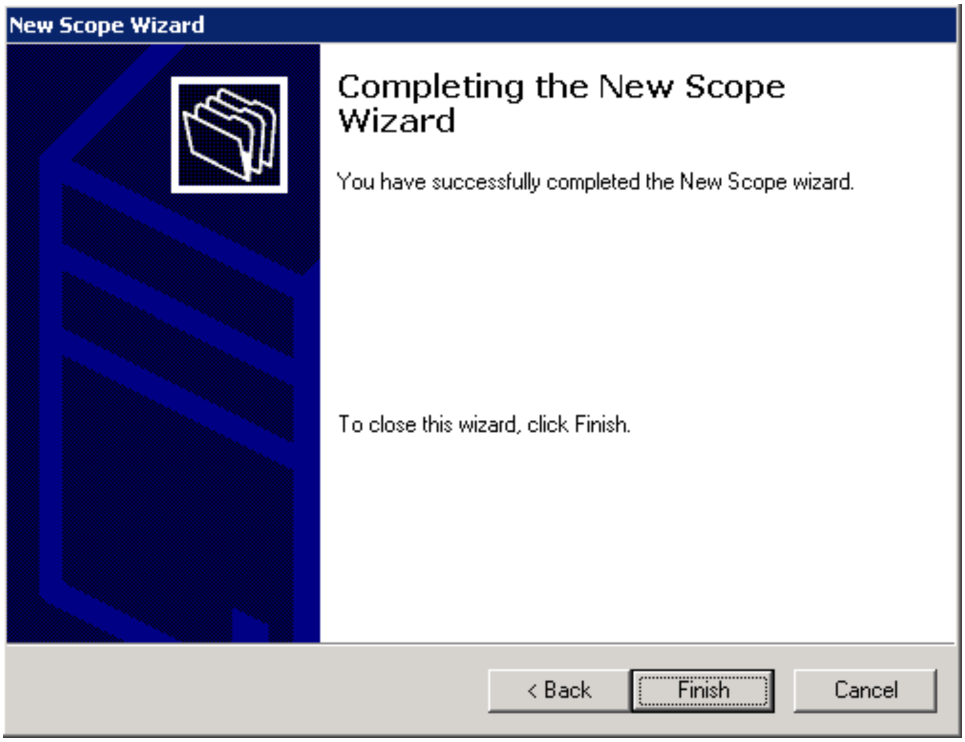
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

● Yes, I want to activate this scope now

○ No, I will activate this scope later

27. Click ***Finish*** to complete and close the wizard.


New Scope Wizard

Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

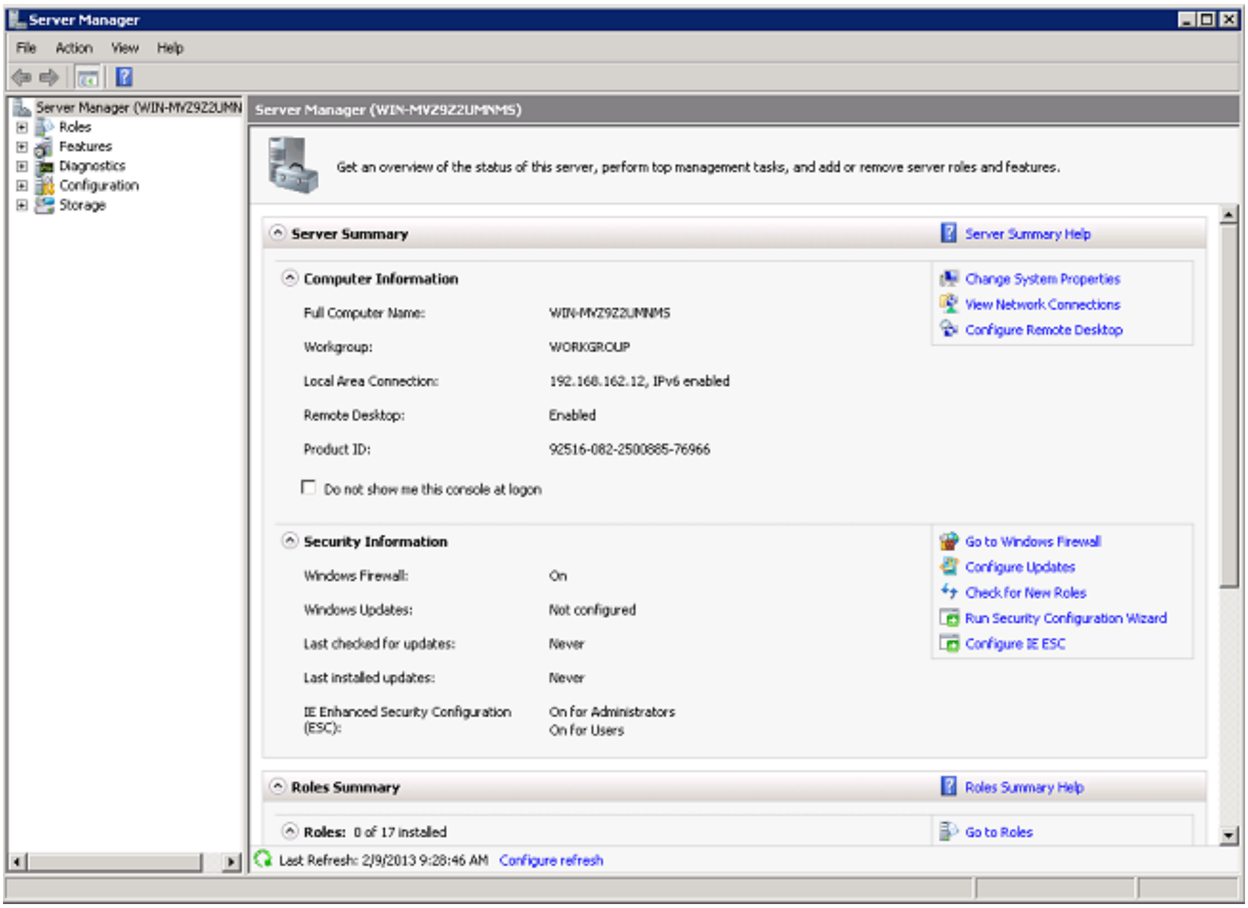
To close this wizard, click Finish.

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

PEAP with EAP−MS−CHAP v2 validates the RADIUS server based on the certificate 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 2008 server as a CA server that issues the certificate to the NPS:

1. Click ***Start*** > ***Server Manager***.



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: WIN-MVZ9Z2UMNMS

Workgroup: WORKGROUP

Local Area Connection: 192.168.162.12, IPv6 enabled

Remote Desktop: Enabled

Product ID: 92516-082-2500885-76966

□ Do not show me this console at logon

Security Information

Windows Firewall: On

Windows Updates: Not configured

Last checked for updates: Never

Last installed updates: Never

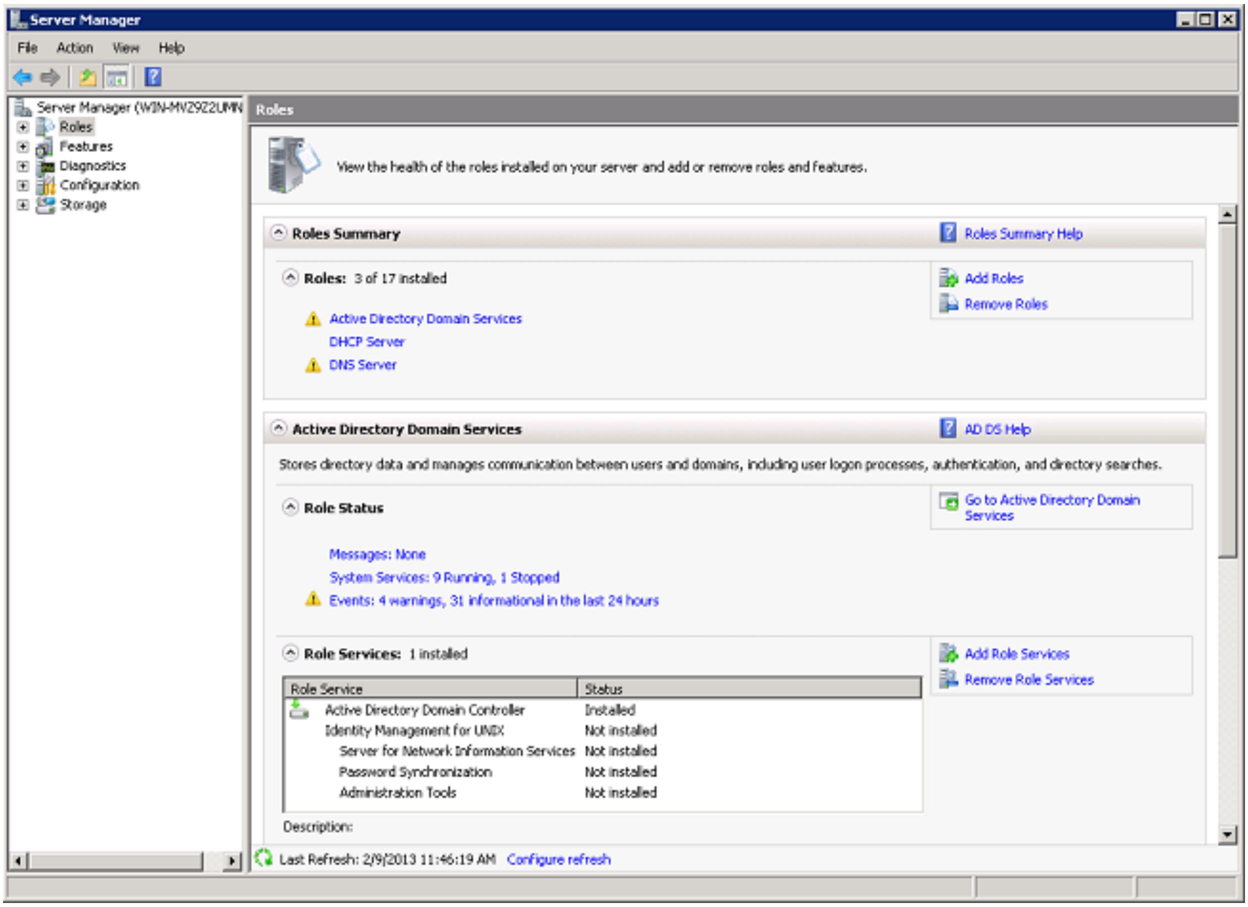
IE Enhanced Security Configuration (ESC): On for Administrators
On for Users

Roles Summary

Roles: 0 of 17 installed

Last Refresh: 2/9/2013 9:28:46 AM

2. Click ***Roles*** > ***Add Roles***.



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

Roles: 3 of 17 installed

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

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

Messages: None

System Services: 9 Running, 1 Stopped

⚠ Events: 4 warnings, 31 informational in the last 24 hours

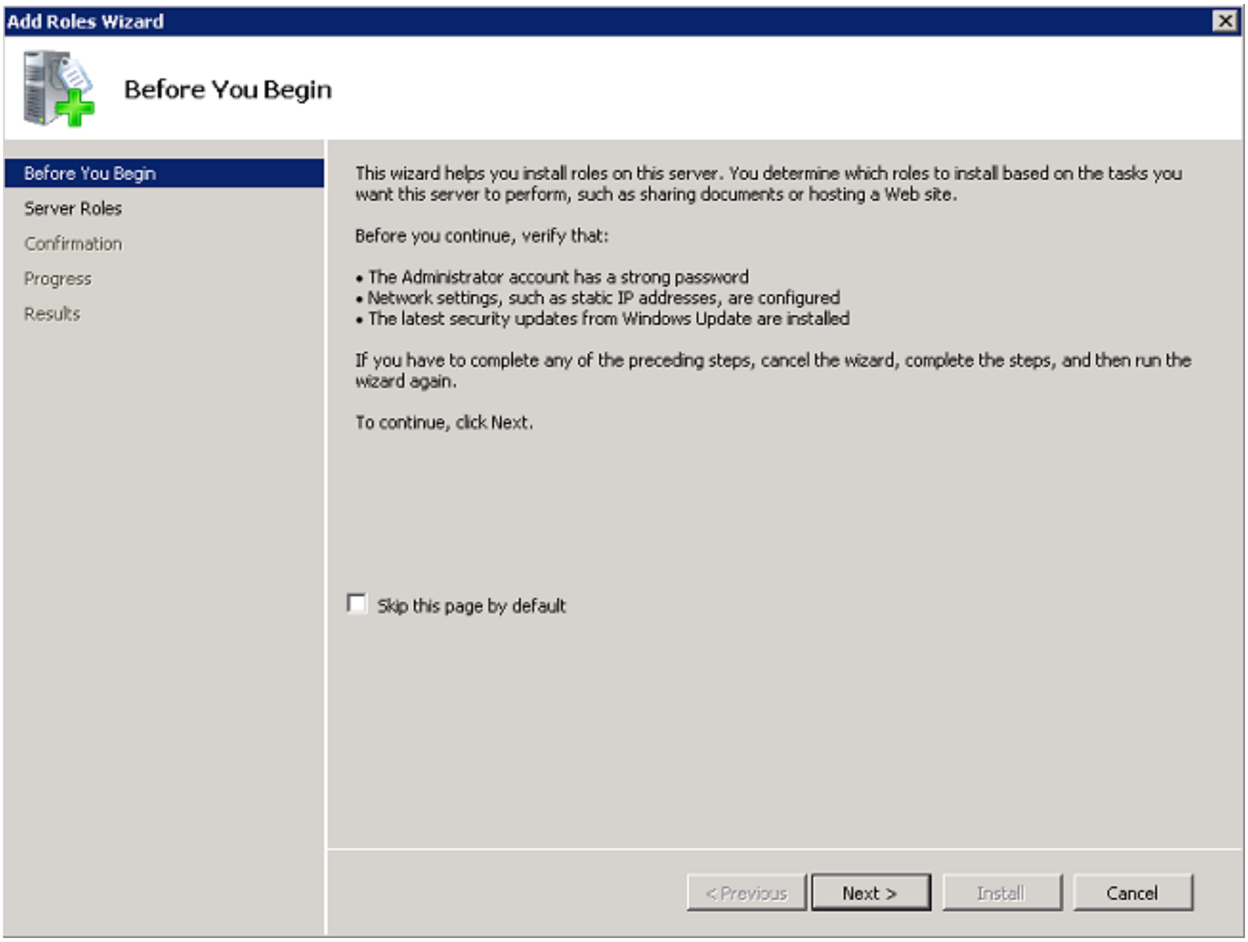
Role Services: 1 installed

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

3. 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:

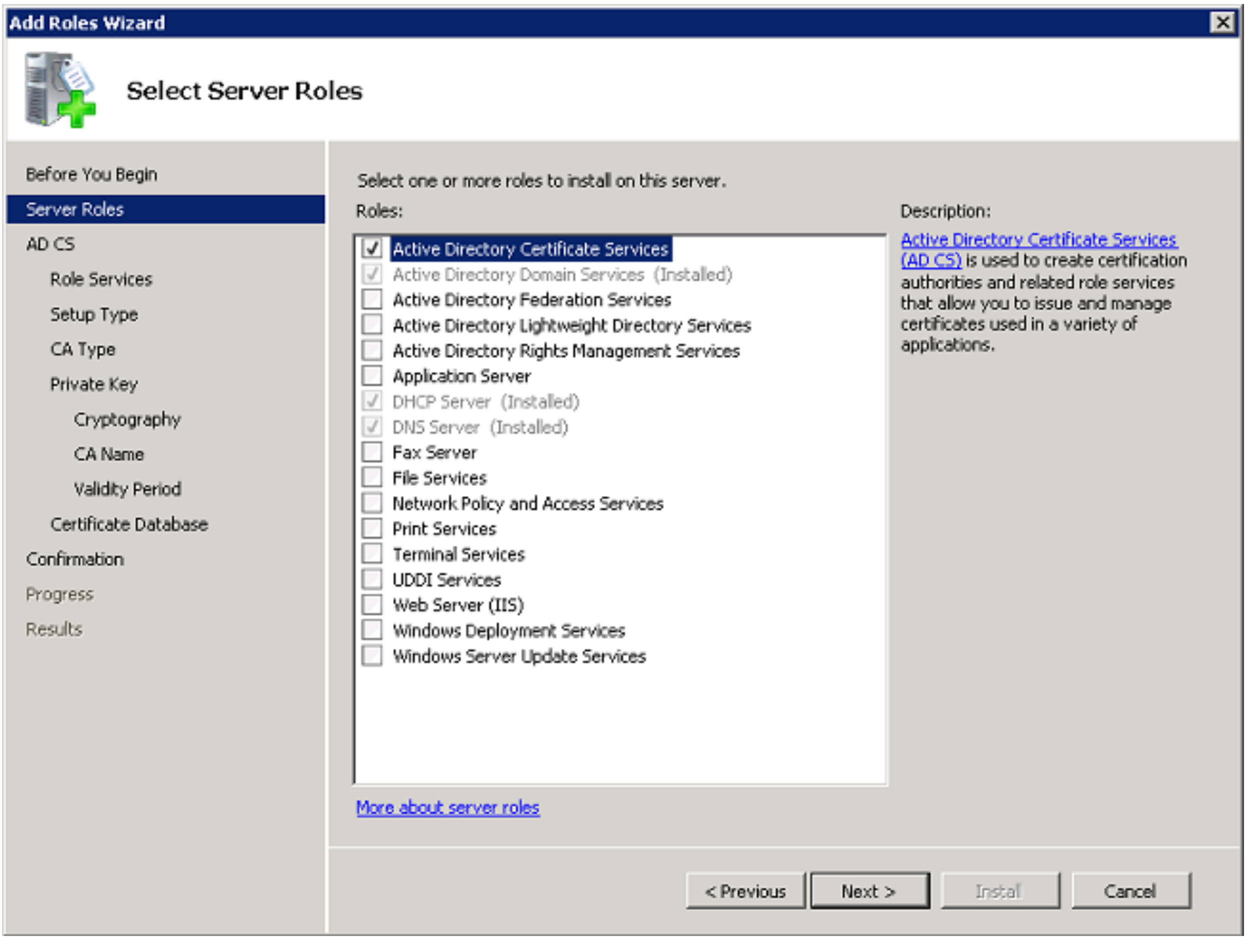
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

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

4. Select the service ***Active Directory Certificate Services***, and click ***Next***.



Select Server Roles

Select one or more roles to install on this server.

Roles:

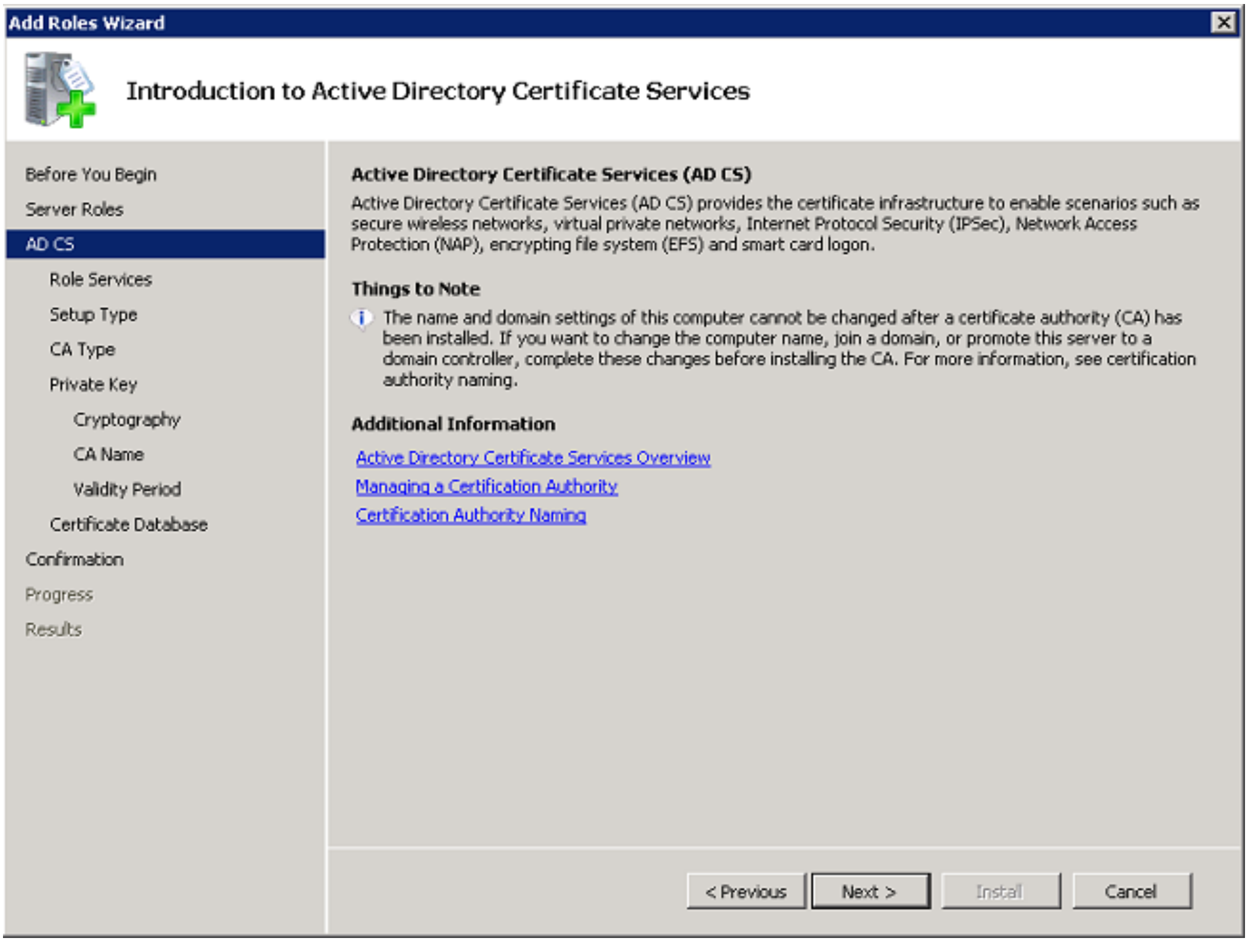
☑ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Application Server
☑ DHCP Server (Installed)
☑ DNS Server (Installed)
□ Fax Server
□ 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.

More about server roles

5. 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.

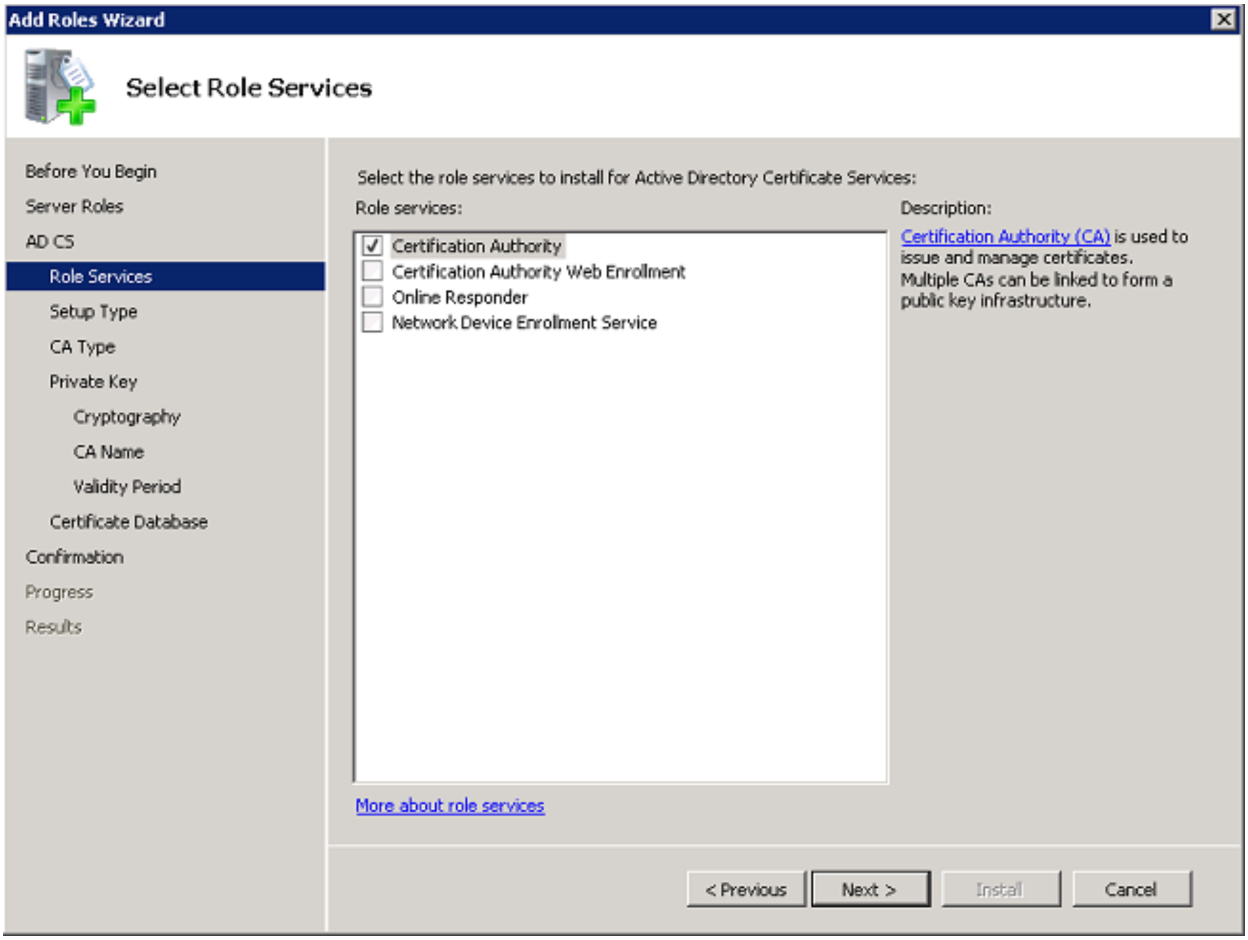
Additional Information

Active Directory Certificate Services Overview

Managing a Certification Authority

Certification Authority Naming

6. Select the ***Certificate Authority***, and click ***Next***.



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

Role services:

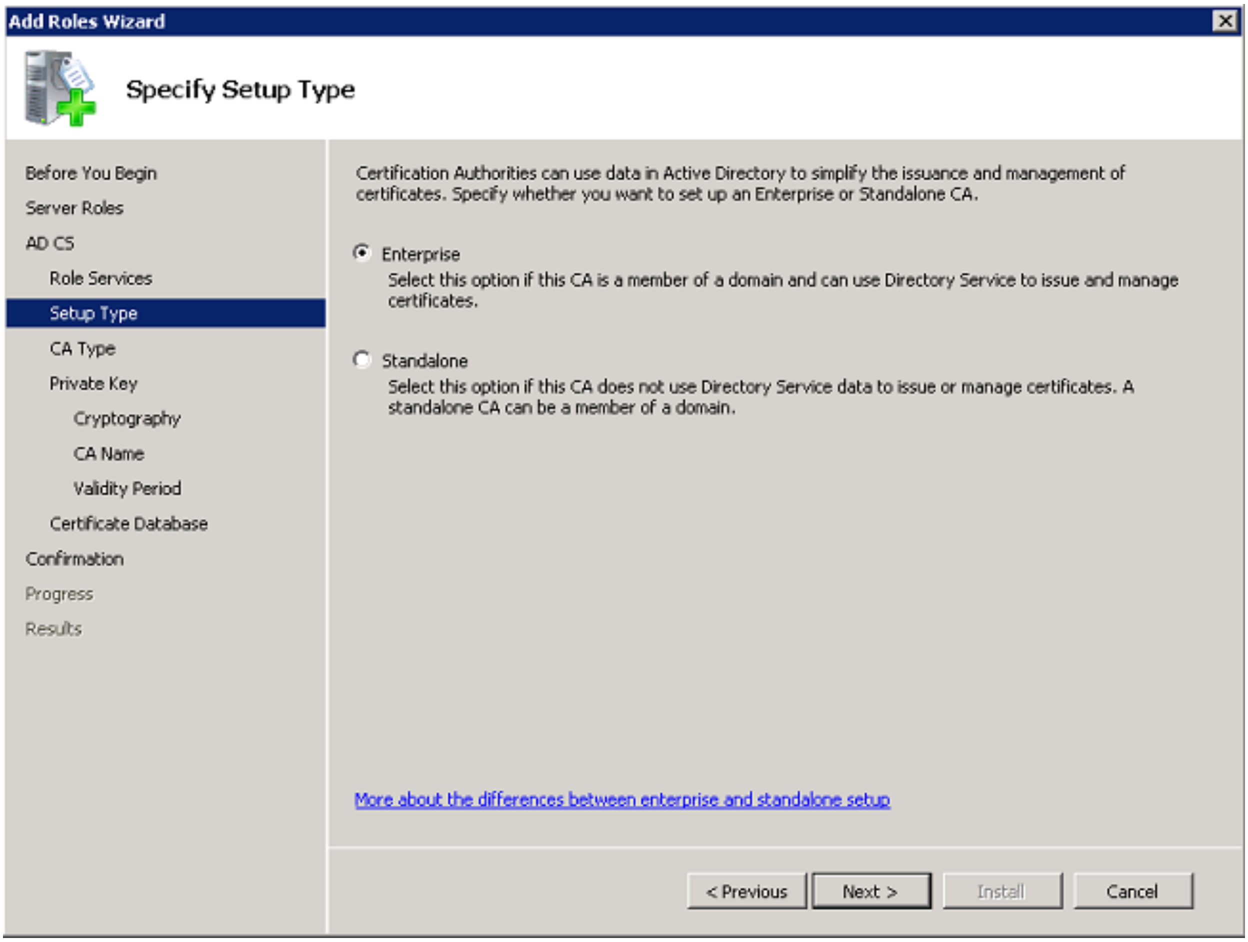
☑ Certification Authority
□ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service

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

7. Select ***Enterprise***, and click ***Next***.

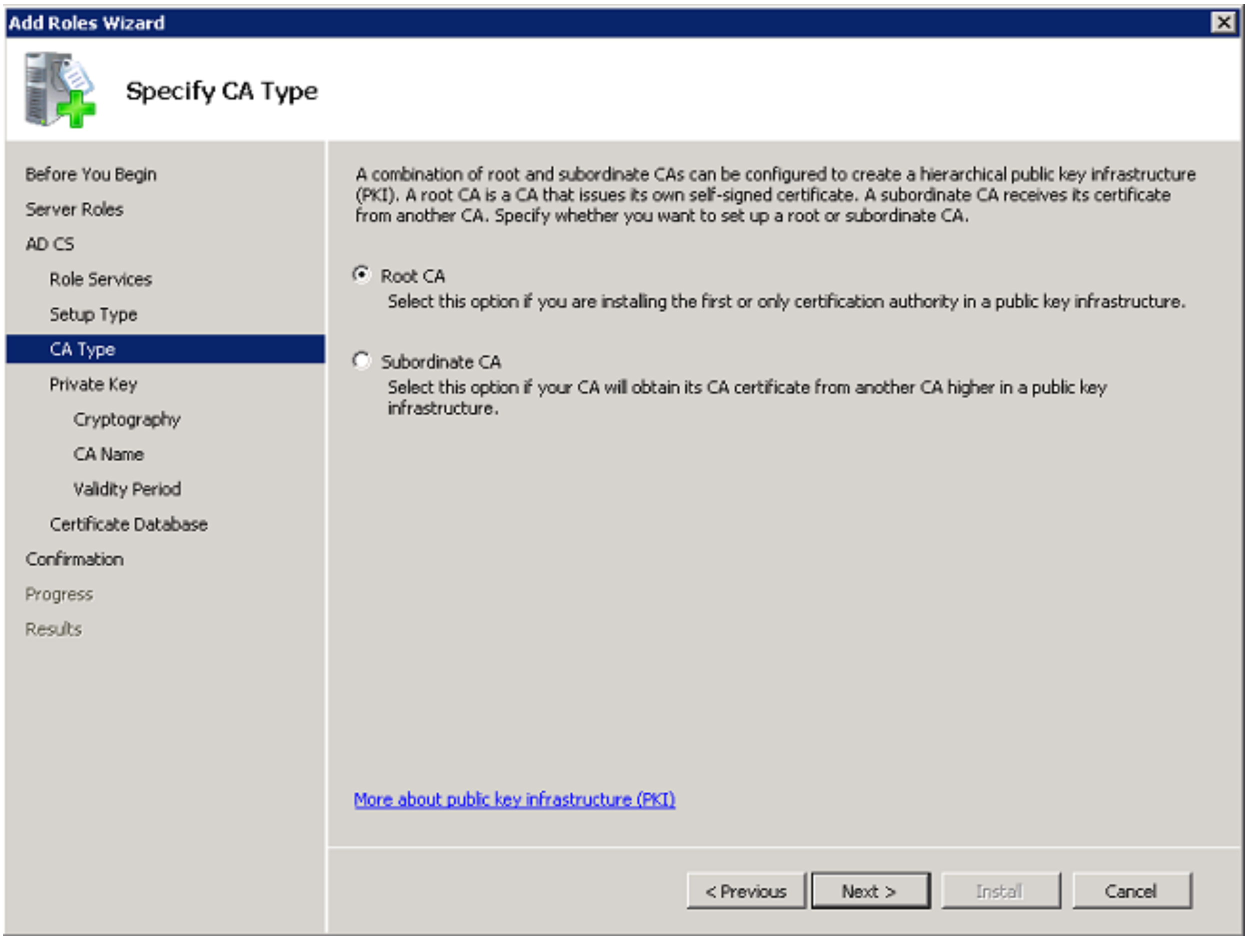


Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

● 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.

8. Select ***Root CA***, and click ***Next***.

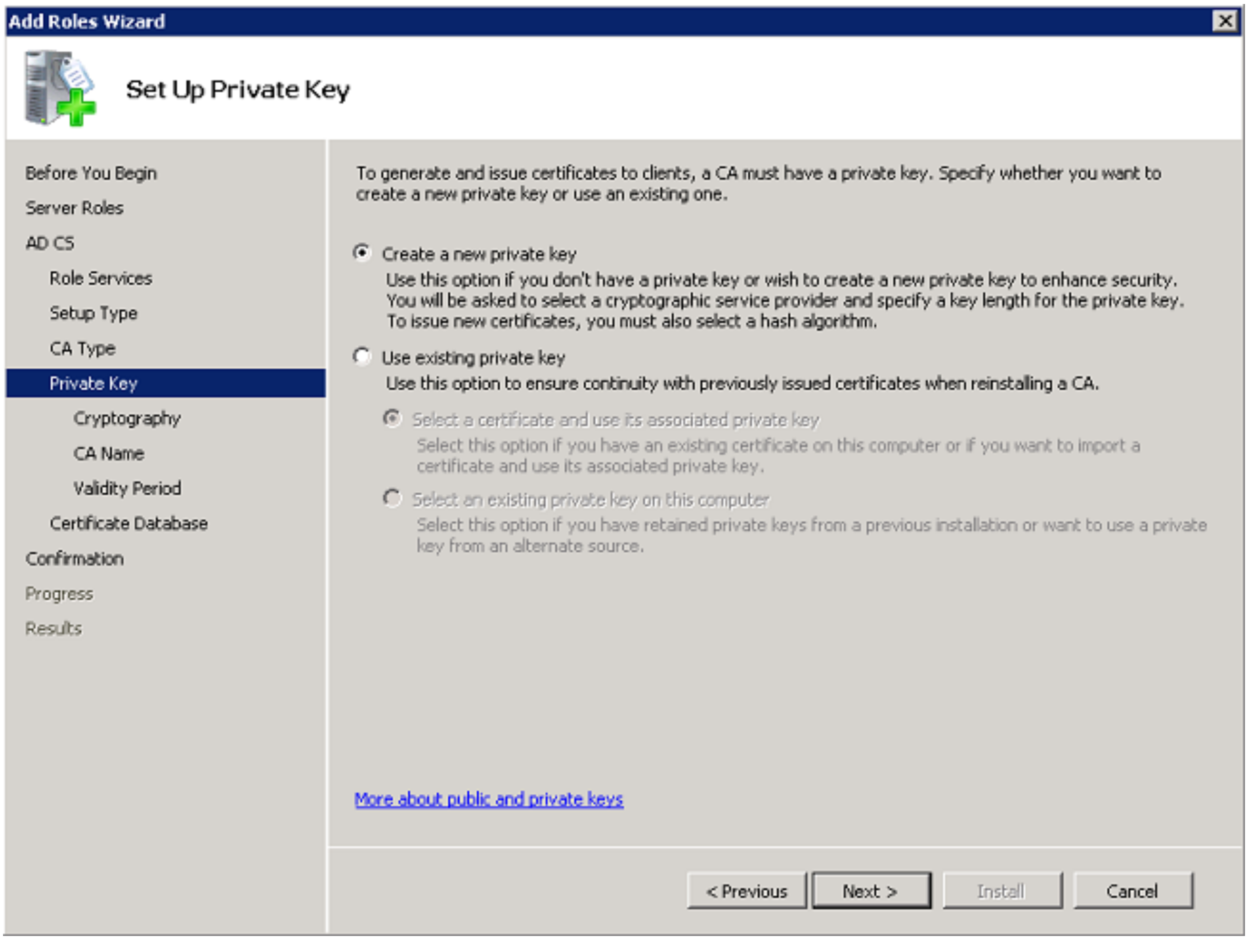


A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

● 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.

9. Select ***Create a new private key***, and click ***Next***.



Set Up Private Key

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.

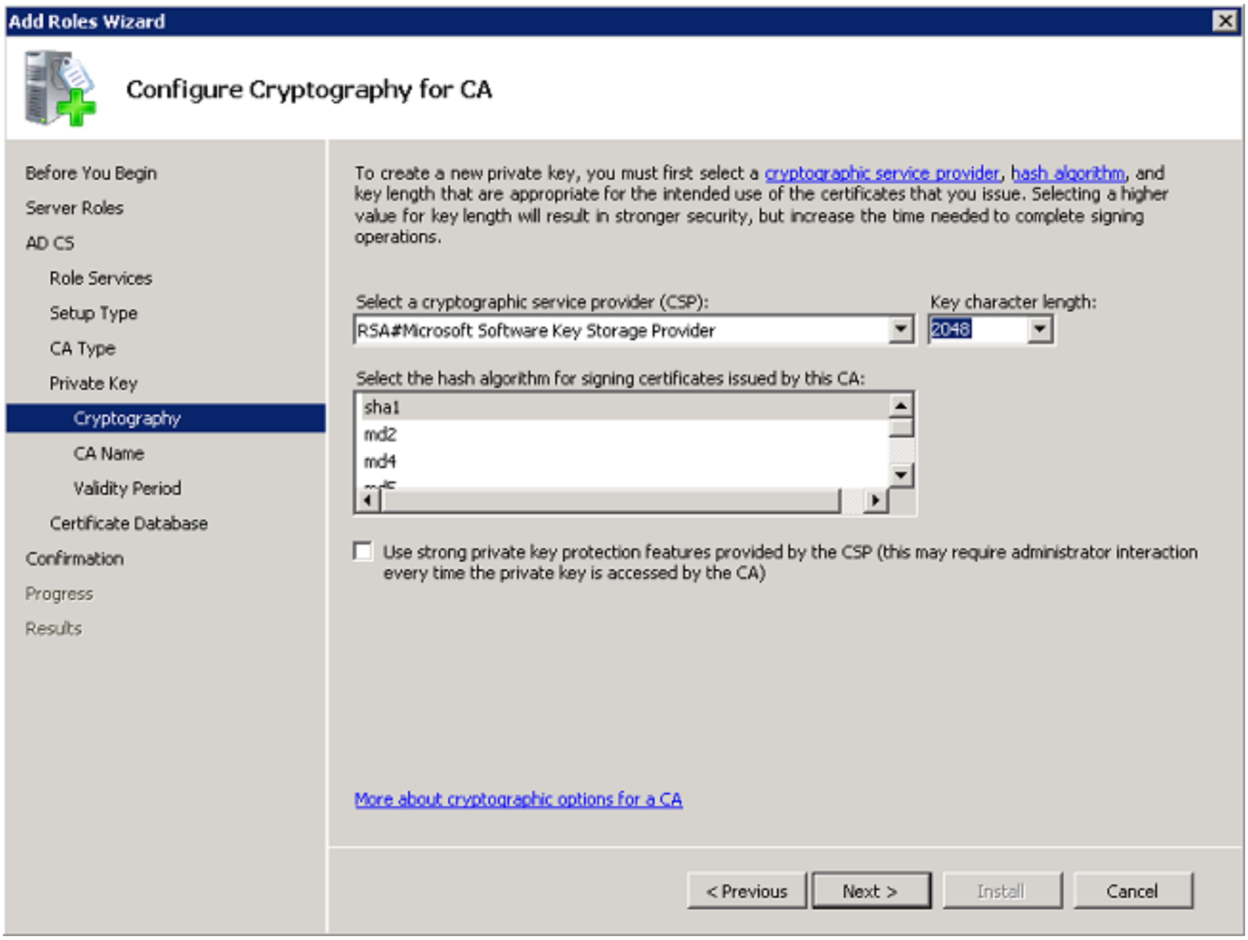
● Select a certificate and use its associated private key

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.

10. Click ***Next*** on Configuring Cryptography for CA.



Add Roles Wizard

Configure Cryptography for CA

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

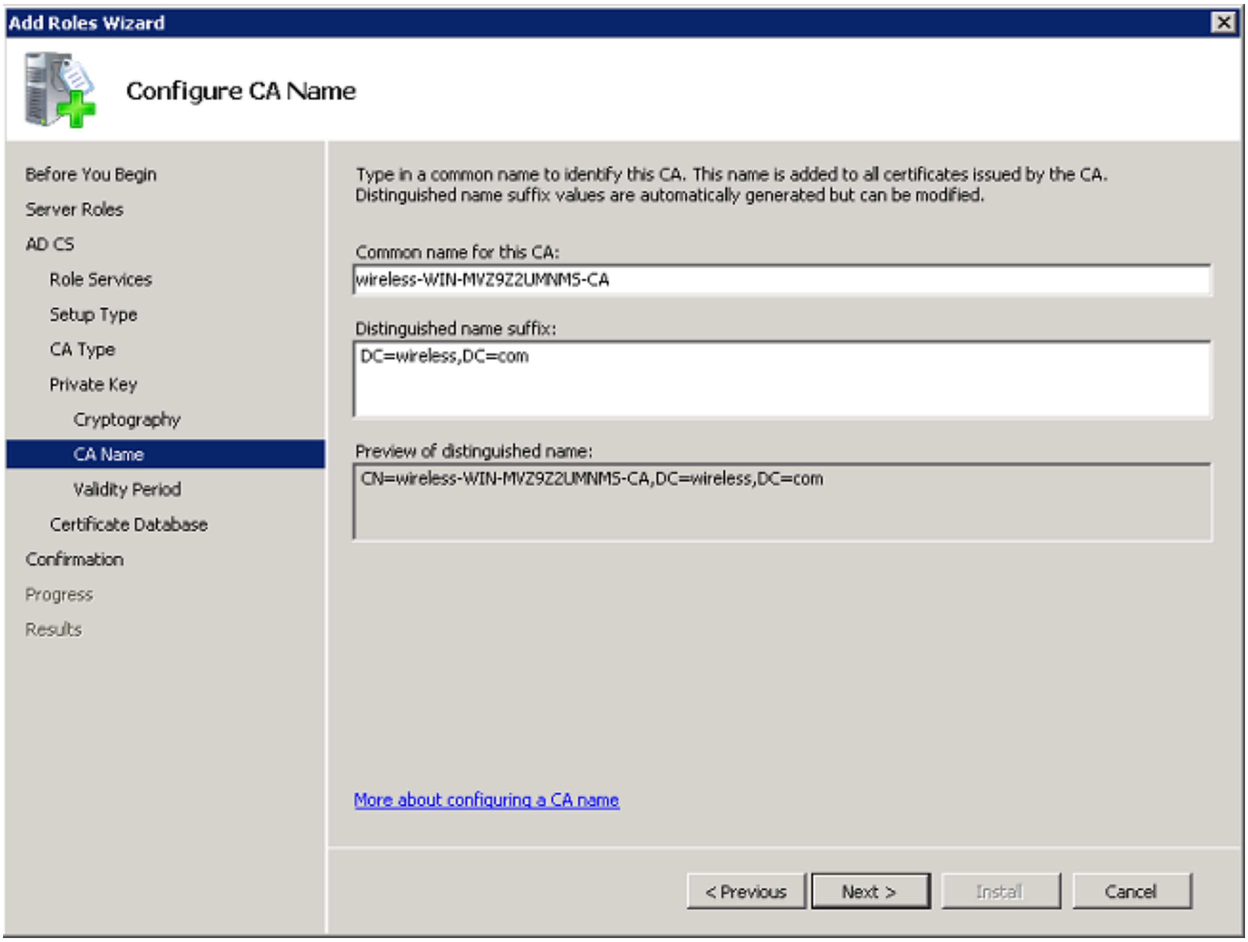
Select the hash algorithm for signing certificates issued by this CA:

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

11. Click ***Next*** to accept the default Common name for this CA.



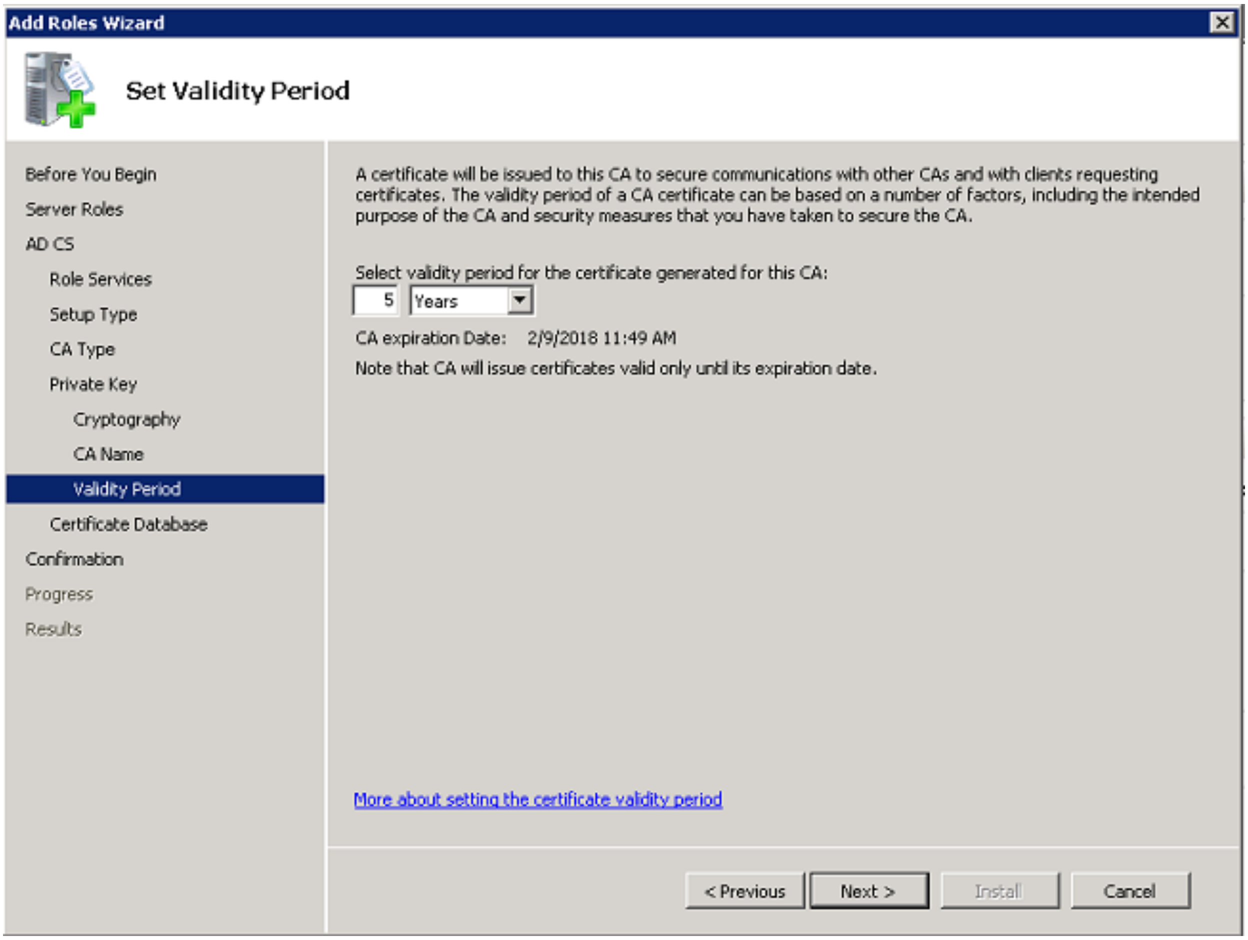
Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: wireless-WIN-MVZ9Z2UMNMS-CA

Distinguished name suffix: DC=wireless,DC=com

Preview of distinguished name: CN=wireless-WIN-MVZ9Z2UMNMS-CA,DC=wireless,DC=com

12. Select the length of time this 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.

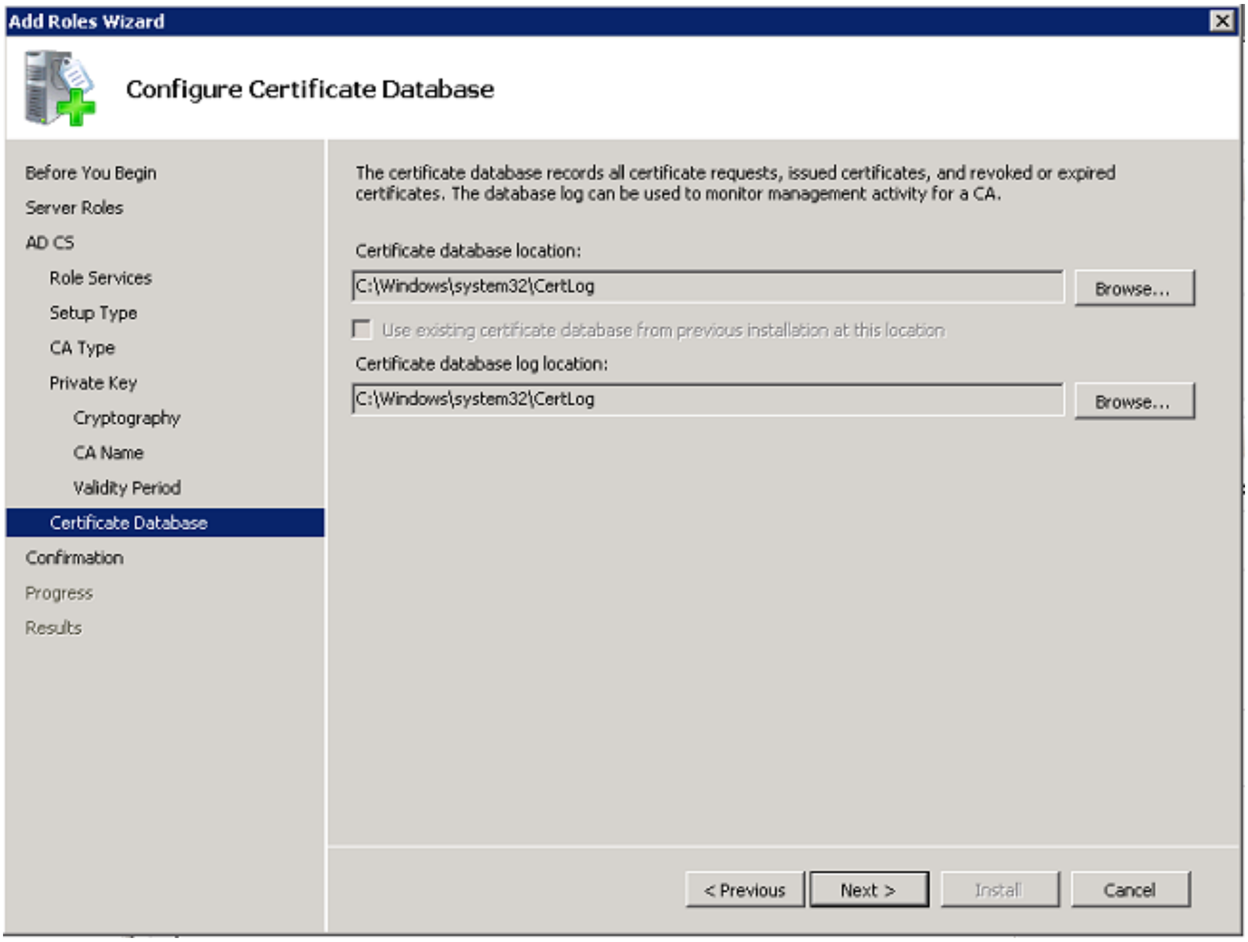
Select validity period for the certificate generated for this CA:

5 Years

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

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

13. Click ***Next*** to accept the default Certificate database location.



Configure Certificate Database

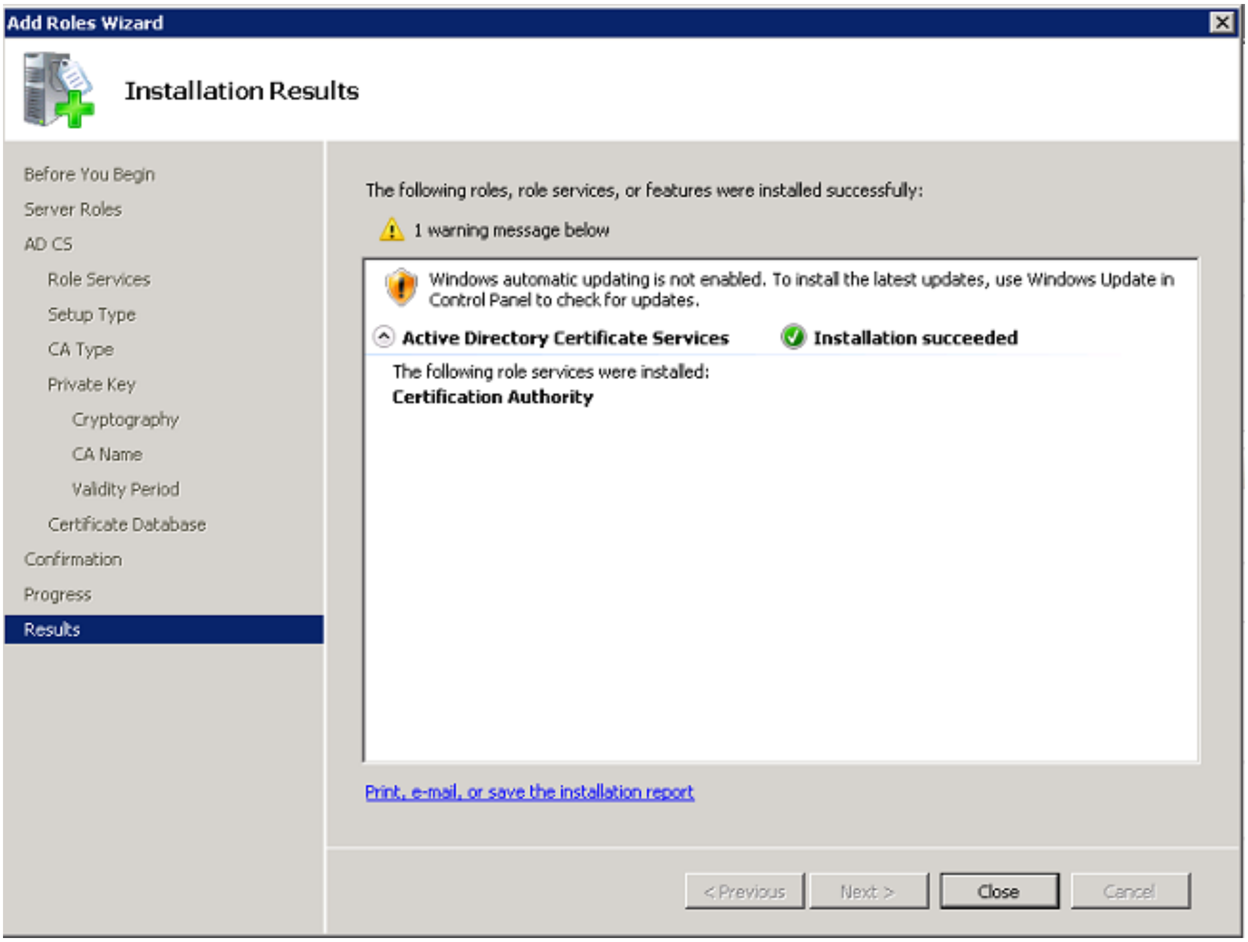
The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.

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

14. Review the configuration, and click ***Install*** to start the Active Directory Certificate Services.



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

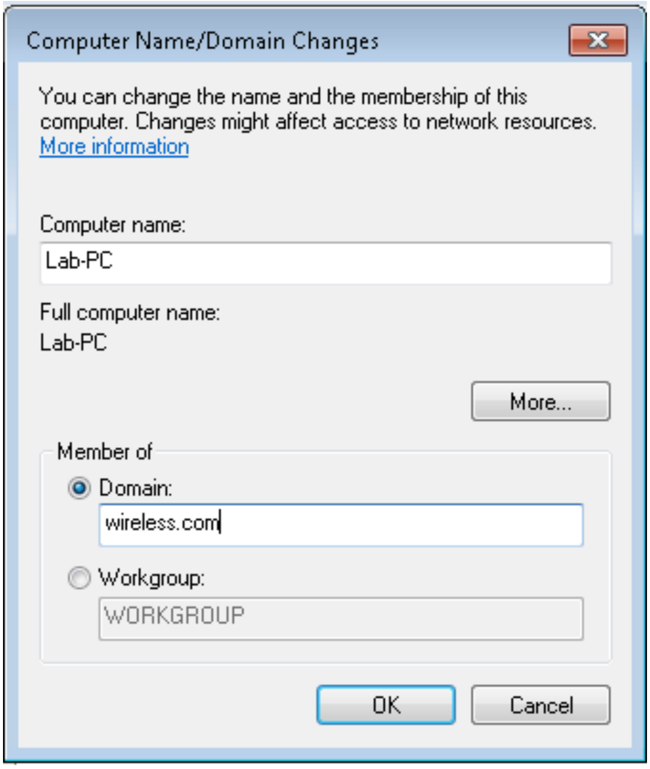
Print, e-mail, or save the installation report

15. After the install is completed, click ***Close***.

Connect Clients to the Domain

Complete these steps in order to connect the clients to the wired network and to download the domain specific information from the new domain:

1. Connect the clients to the wired network with a straight through Ethernet cable.
2. Boot up the client, and log in with the client username and password.
3. Click ***Start*** > ***Run***, enter ***cmd***, and click ***OK***.
4. At the command prompt, enter ***ipconfig***, and click ***Enter*** to verify that DHCP works correctly and that the client received an IP address from the DHCP server.
5. In order to join the client to the domain, click ***Start***, right−click ***Computer***, choose ***Properties***, and choose ***Change Settings*** at the bottom right.
6. Click ***Change***.
7. Click ***Domain***, enter ***wireless.com***, and click ***OK***.


Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources. More information

Computer name: Lab-PC

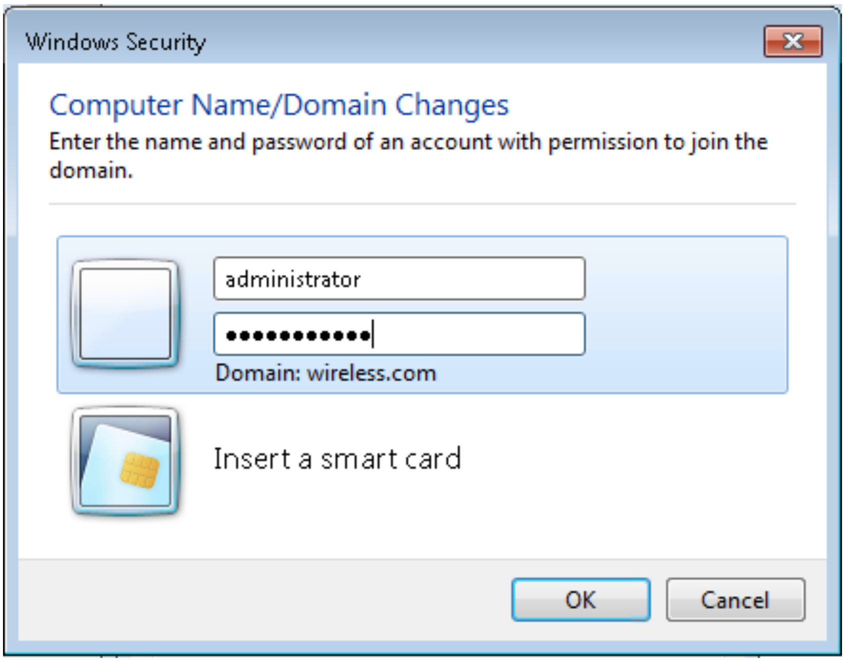
Full computer name: Lab-PC

Member of

● Domain: wireless.com

○ Workgroup: WORKGROUP

8. Enter username ***administrator*** and the password specific to the domain to which the client joins. This is the administrator account in the Active Directory on the server.


Windows Security

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

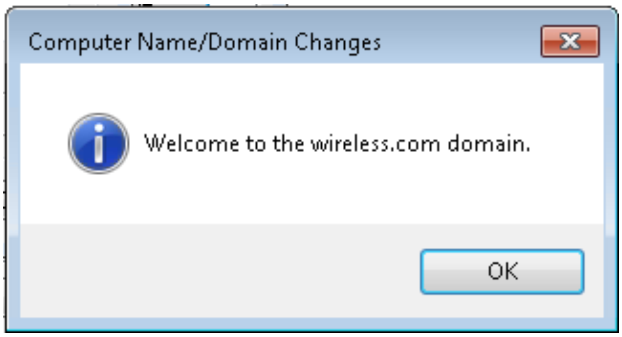
administrator

●●●●●●●●●●●

Domain: wireless.com

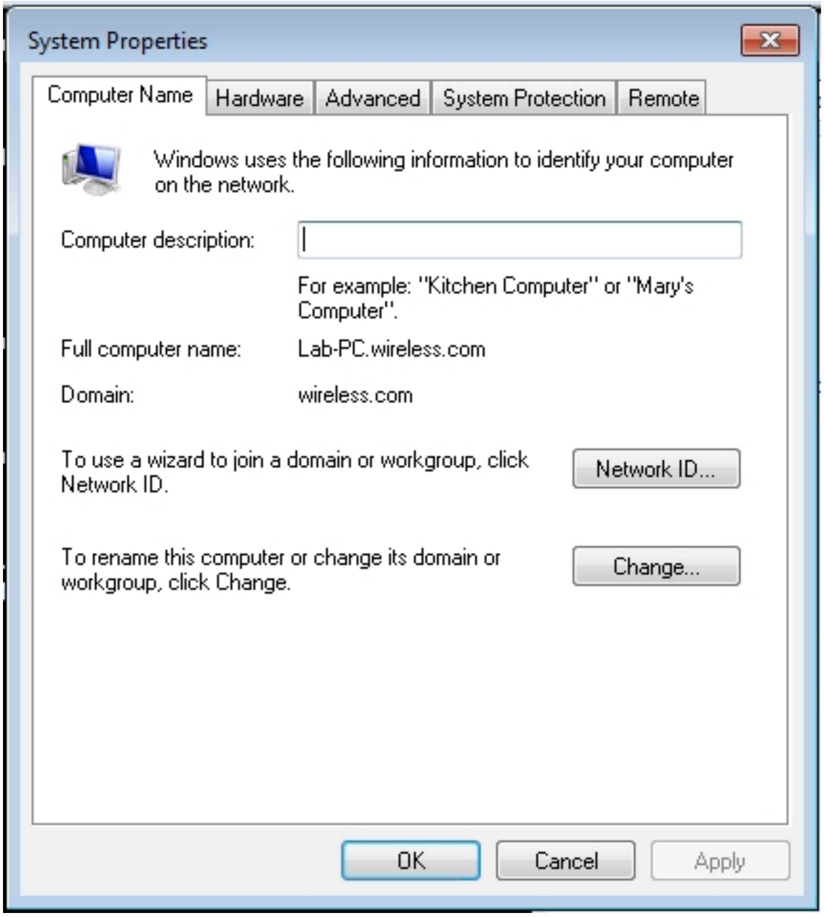
Insert a smart card

9. Click ***OK***, and click ***OK*** again.


Computer Name/Domain Changes

Welcome to the wireless.com domain.

10. Click ***Close*** > ***Restart Now*** to restart the computer.
11. Once the computer restarts, log in with this information: Username = Administrator; Password = <domain password>; Domain = wireless.
12. Click ***Start***, right−click ***Computer***, choose ***Properties***, and choose ***Change Settings*** at the bottom right to verify that you are on the wireless.com domain.
13. The next step is to verify that the client received the CA certificate (trust) from the server.


System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

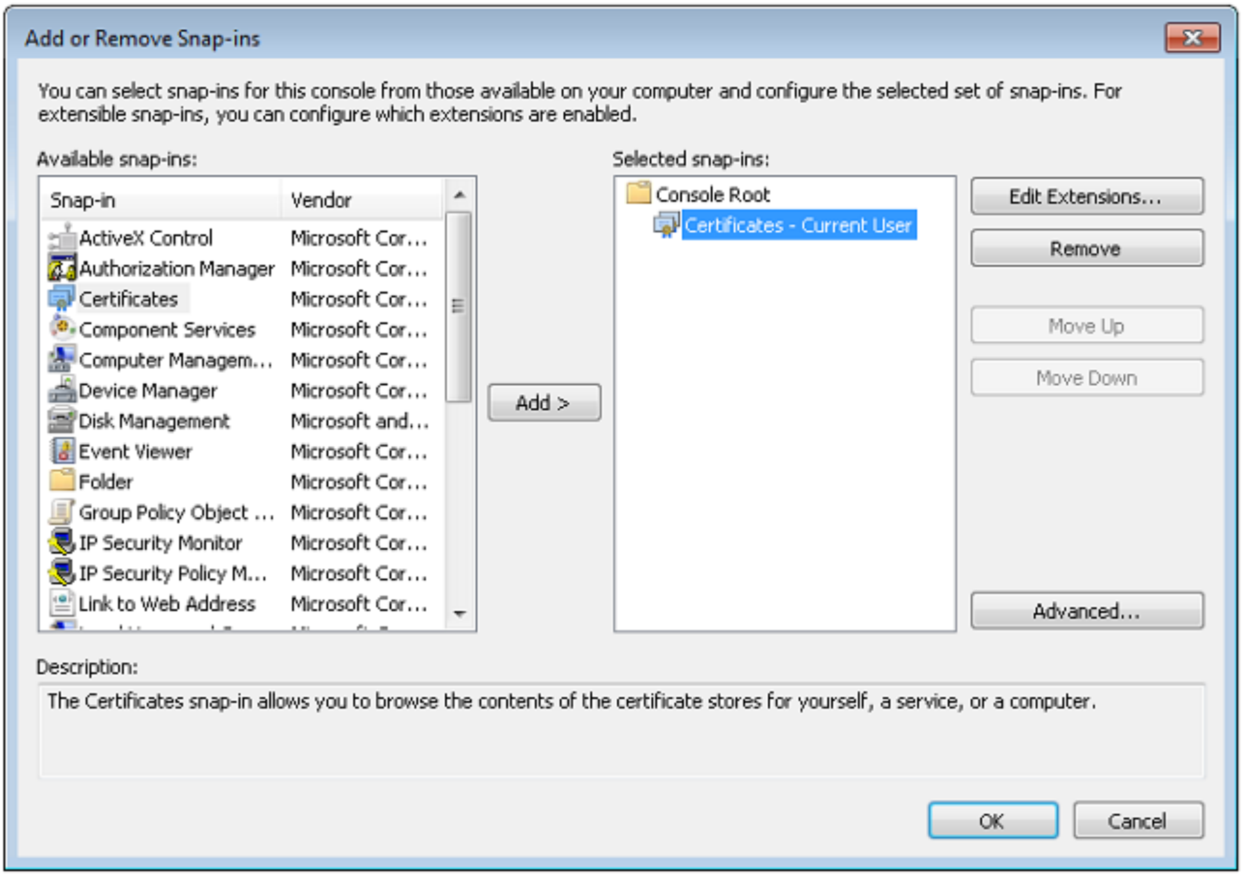
Full computer name: Lab-PC.wireless.com

Domain: wireless.com

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

14. Click ***Start***, enter ***mmc***, and press ***Enter***.
15. Click ***File***, and click ***Add/Remove*** snap−in.
16. Choose ***Certificates***, and click ***Add***.



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
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

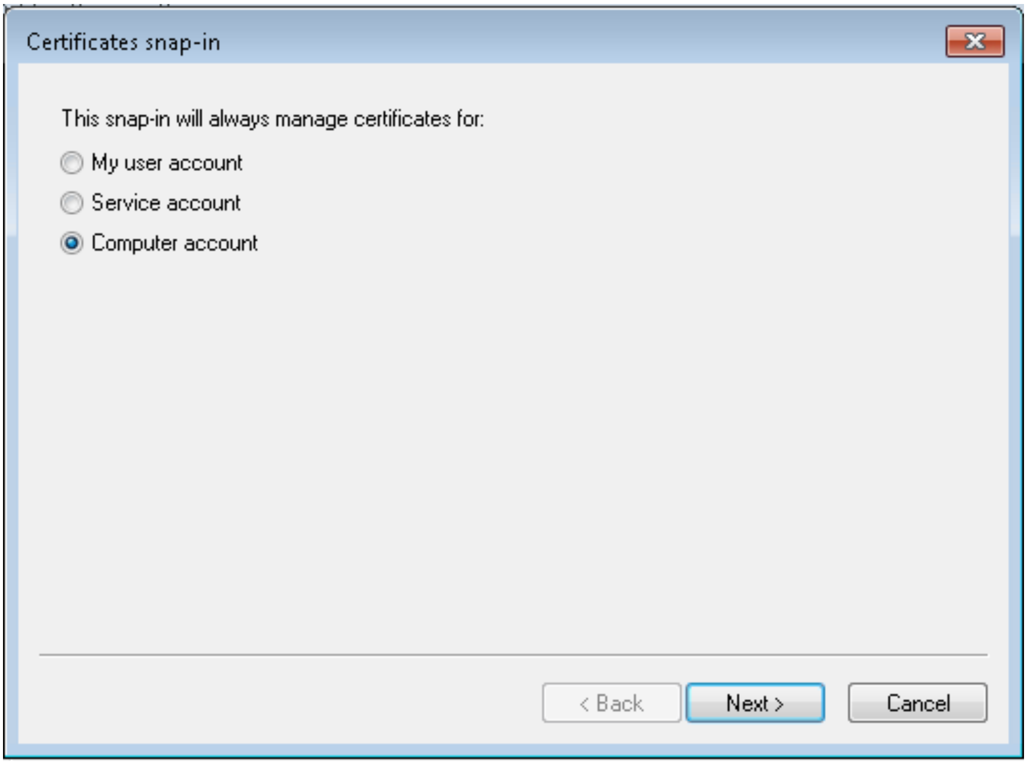
Selected snap-ins:

- Console Root
  - Certificates - Current User

Description:

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

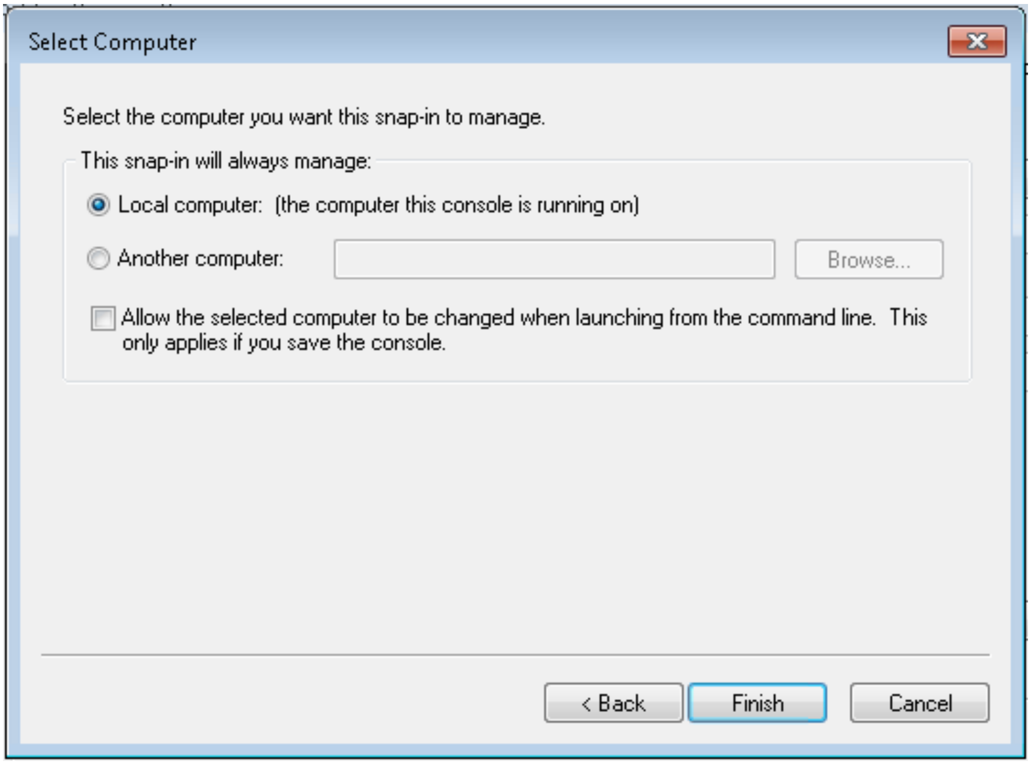
17. Click ***Computer account***, and click ***Next***.



This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

18. Click ***Local computer***, and click ***Next***.



Select Computer

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

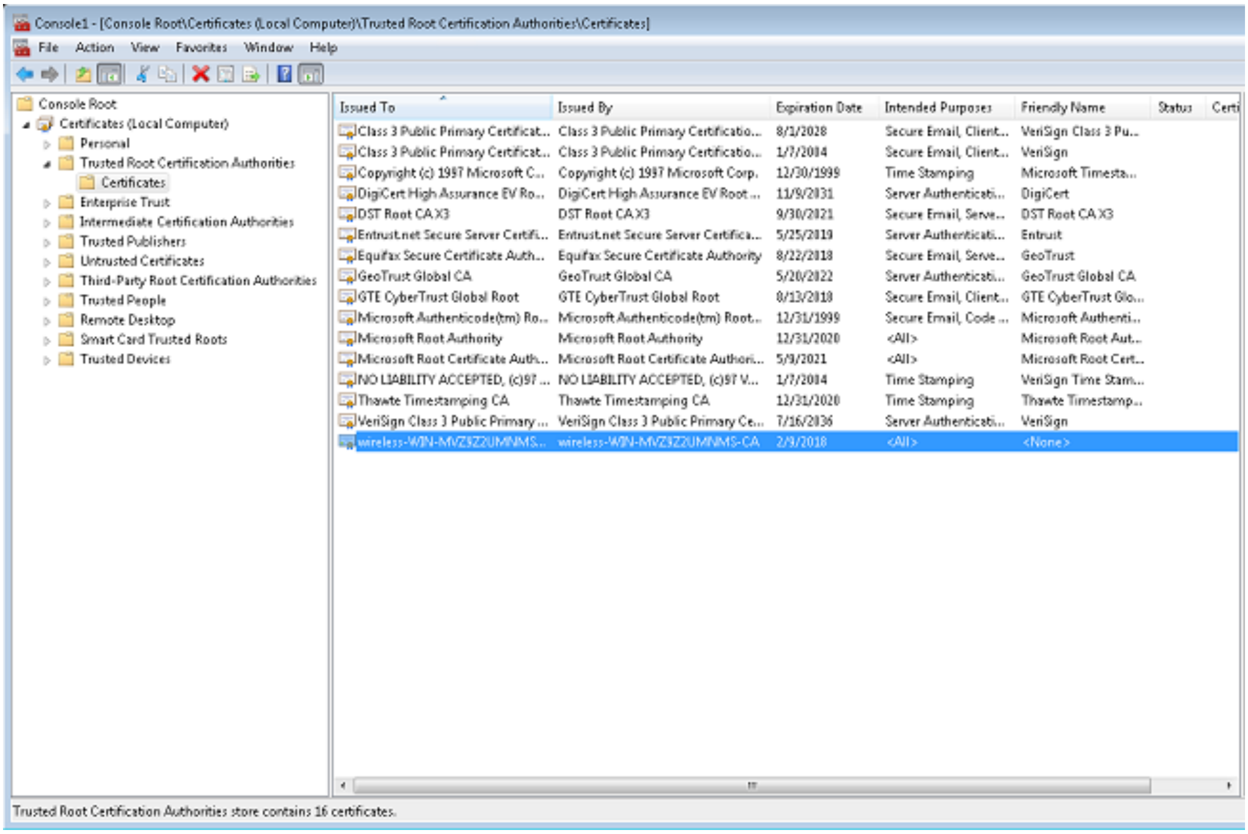
This snap-in will always manage:

● 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.

19. Click ***OK***.
20. Expand the ***Certificates (Local Computer)*** and ***Trusted Root Certification Authorities*** folders, and click ***Certificates***. Find ***wireless domain CA cert*** in the list. In this example, the CA cert is called wireless−WIN−MVZ9Z2UMNMS−CA.



Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...	VeriSign		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert		
DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, Serve...	DST Root CA X3		
Entrust.net Secure Server Certifi...	Entrust.net Secure Server Certifica...	5/25/2019	Server Authenticati...	Entrust		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
GeoTrust Global CA	GeoTrust Global CA	5/20/2022	Server Authenticati...	GeoTrust Global CA		
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...	GTE CyberTrust Glo...		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping	VeriSign Time Stam...		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp...		
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Server Authenticati...	VeriSign		
wireless-WIN-MVZ9Z2UMNMS...	wireless-WIN-MVZ9Z2UMNMS-CA	2/9/2018	<All>	<None>		

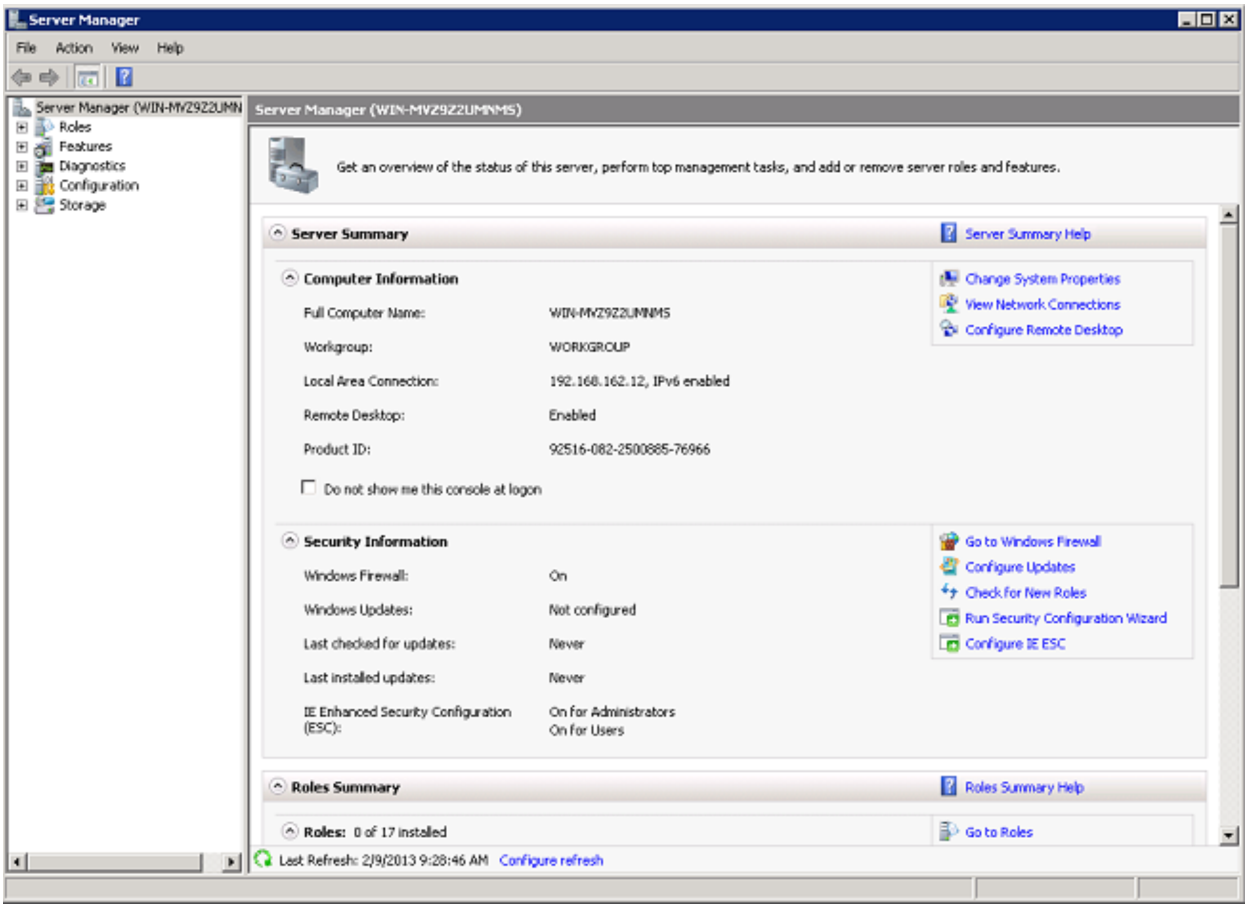
Trusted Root Certification Authorities store contains 16 certificates.

21. Repeat this procedure to add more clients to the domain.

Install the Network Policy Server on the Microsoft Windows 2008 Server

In this setup, the NPS is used as a RADIUS server to authenticate wireless clients with PEAP authentication. Complete these steps in order to install and configure NPS on the Microsoft WIndows 2008 server:

1. Click ***Start*** > ***Server Manager***.



Server Manager (WIN-MVZ9Z2UMNMS)

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: WIN-MVZ9Z2UMNMS

Workgroup: WORKGROUP

Local Area Connection: 192.168.162.12, IPv6 enabled

Remote Desktop: Enabled

Product ID: 92516-082-2500885-76966

□ Do not show me this console at logon

Security Information

Windows Firewall: On

Windows Updates: Not configured

Last checked for updates: Never

Last installed updates: Never

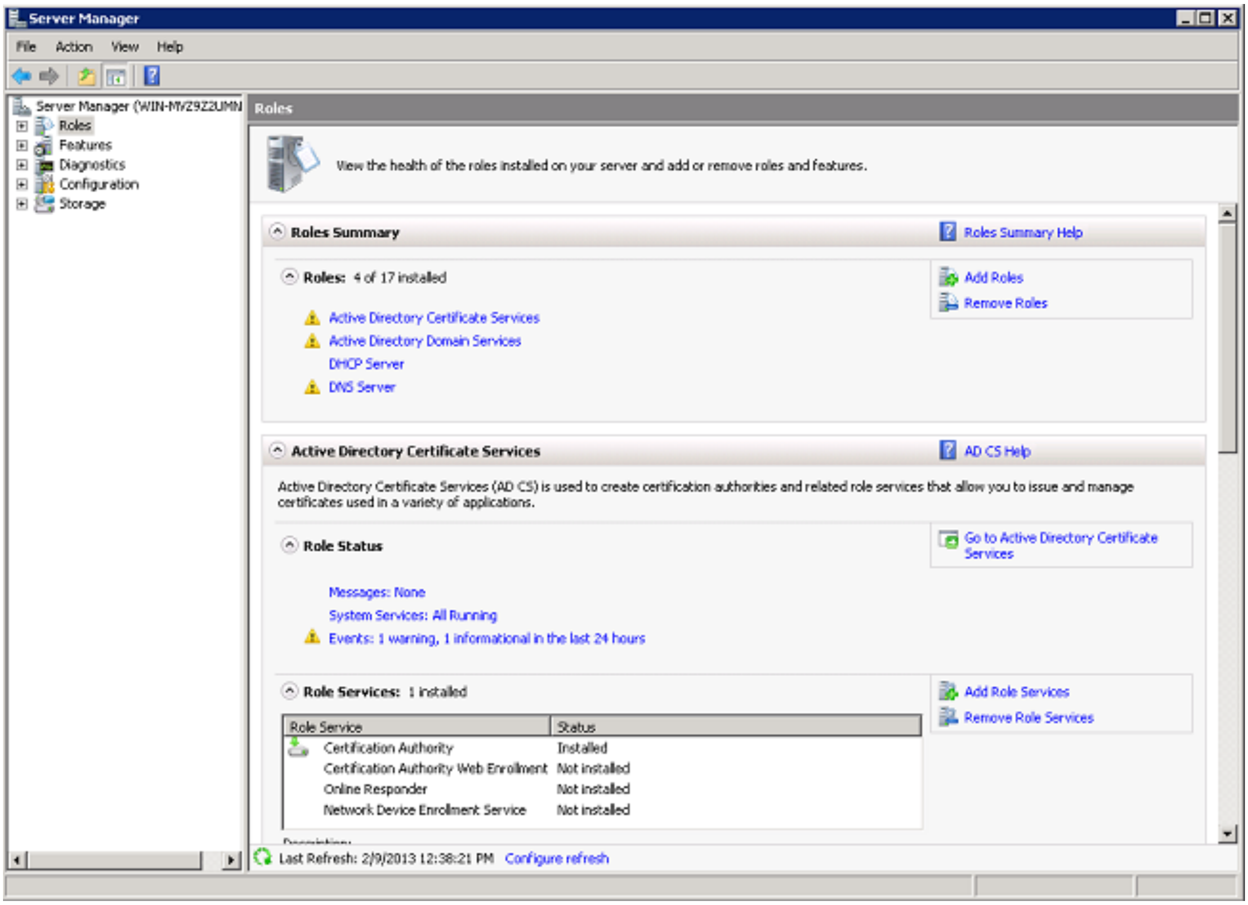
IE Enhanced Security Configuration (ESC): On for Administrators
On for Users

Roles Summary

Roles: 0 of 17 installed

Last Refresh: 2/9/2013 9:28:46 AM

2. Click ***Roles*** > ***Add Roles***.



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

Roles Summary

Roles: 4 of 17 installed

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

Active Directory Certificate Services

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

Messages: None

System Services: All Running

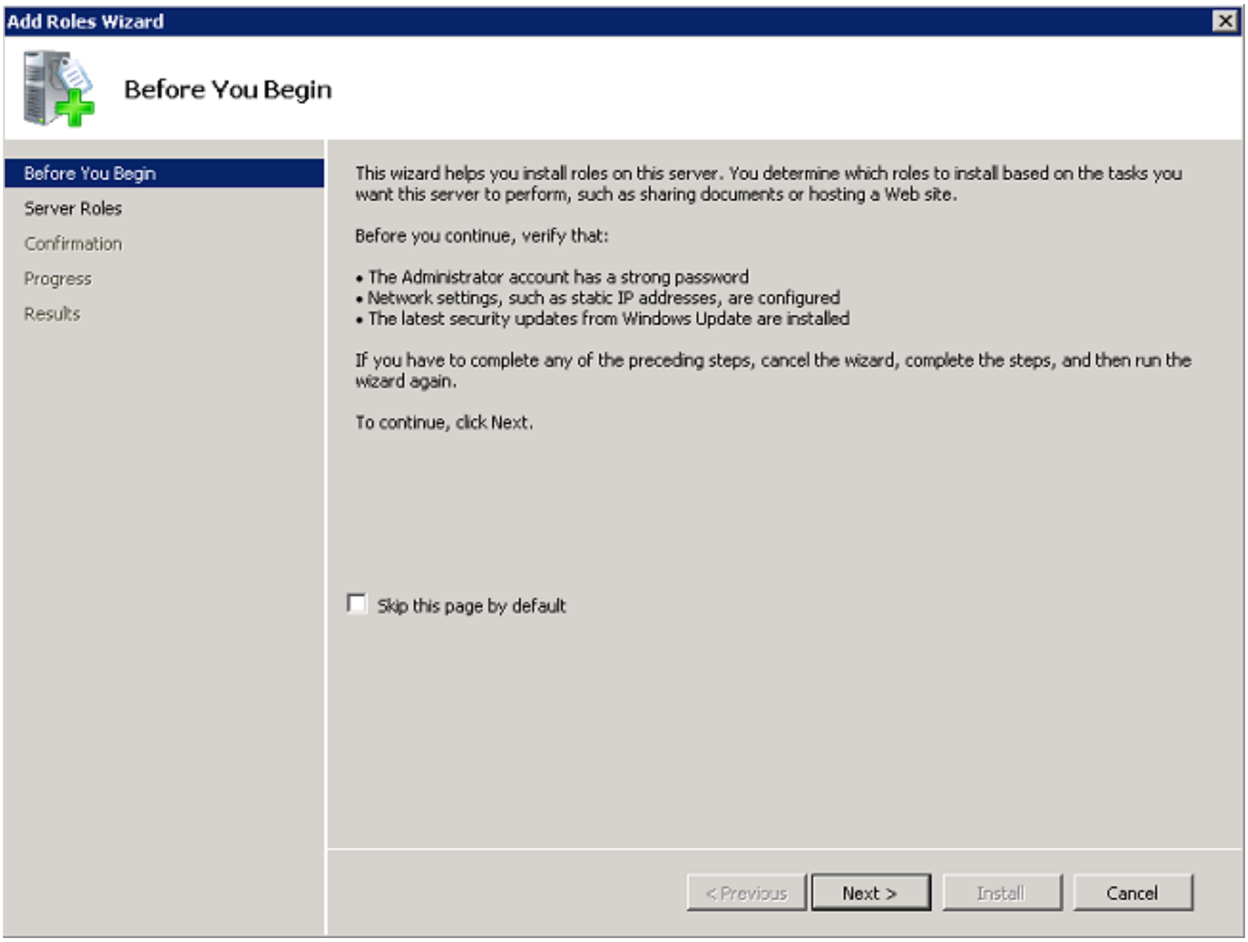
⚠ Events: 1 warning, 1 informational in the last 24 hours

Role Services: 1 installed

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

3. 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:

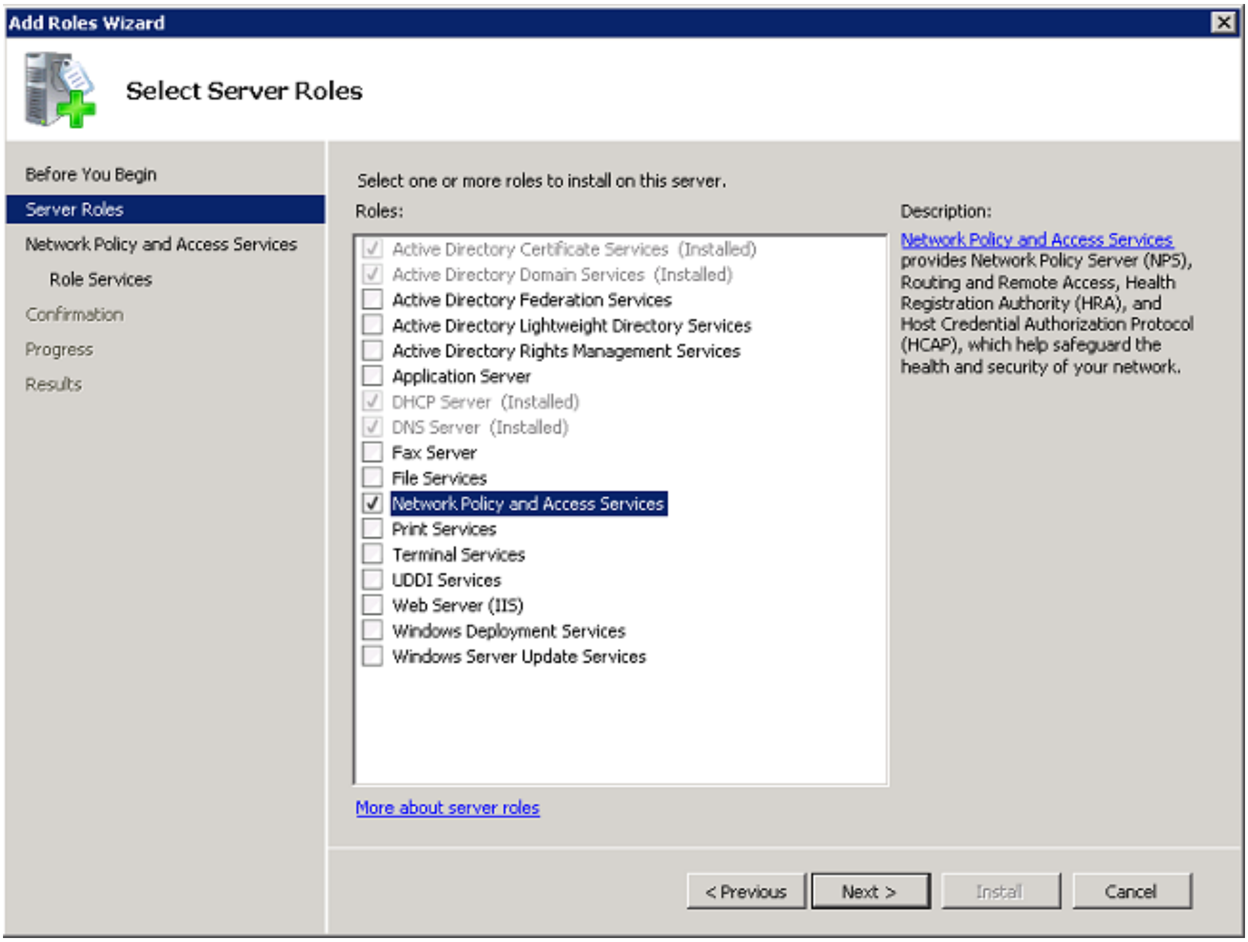
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

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

4. Select the service ***Network Policy and Access Services***, and click ***Next***.



Select one or more roles to install on this server.

Roles:

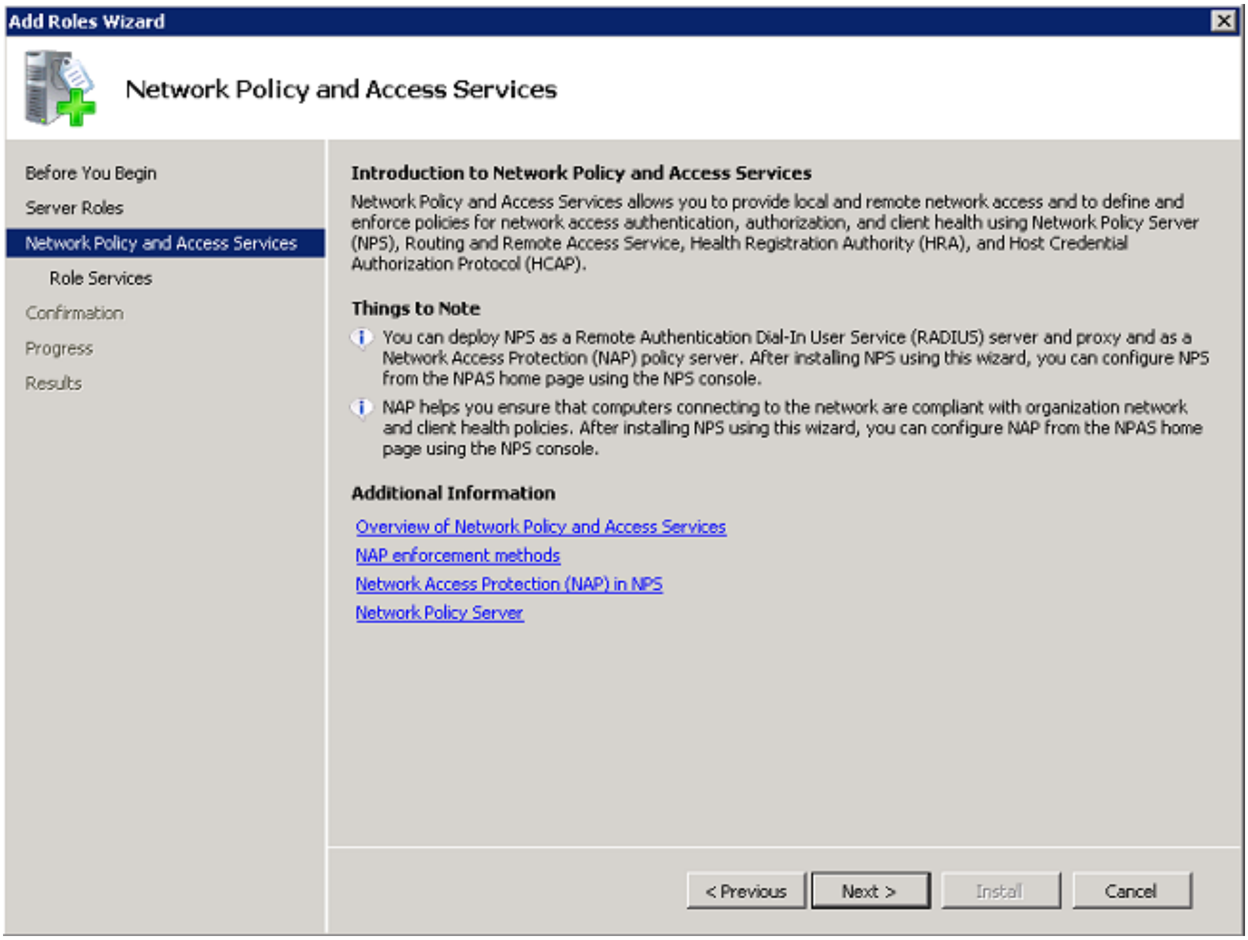
- ☑ Active Directory Certificate Services (Installed)
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS 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.

More about server roles

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



Network Policy and Access Services

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

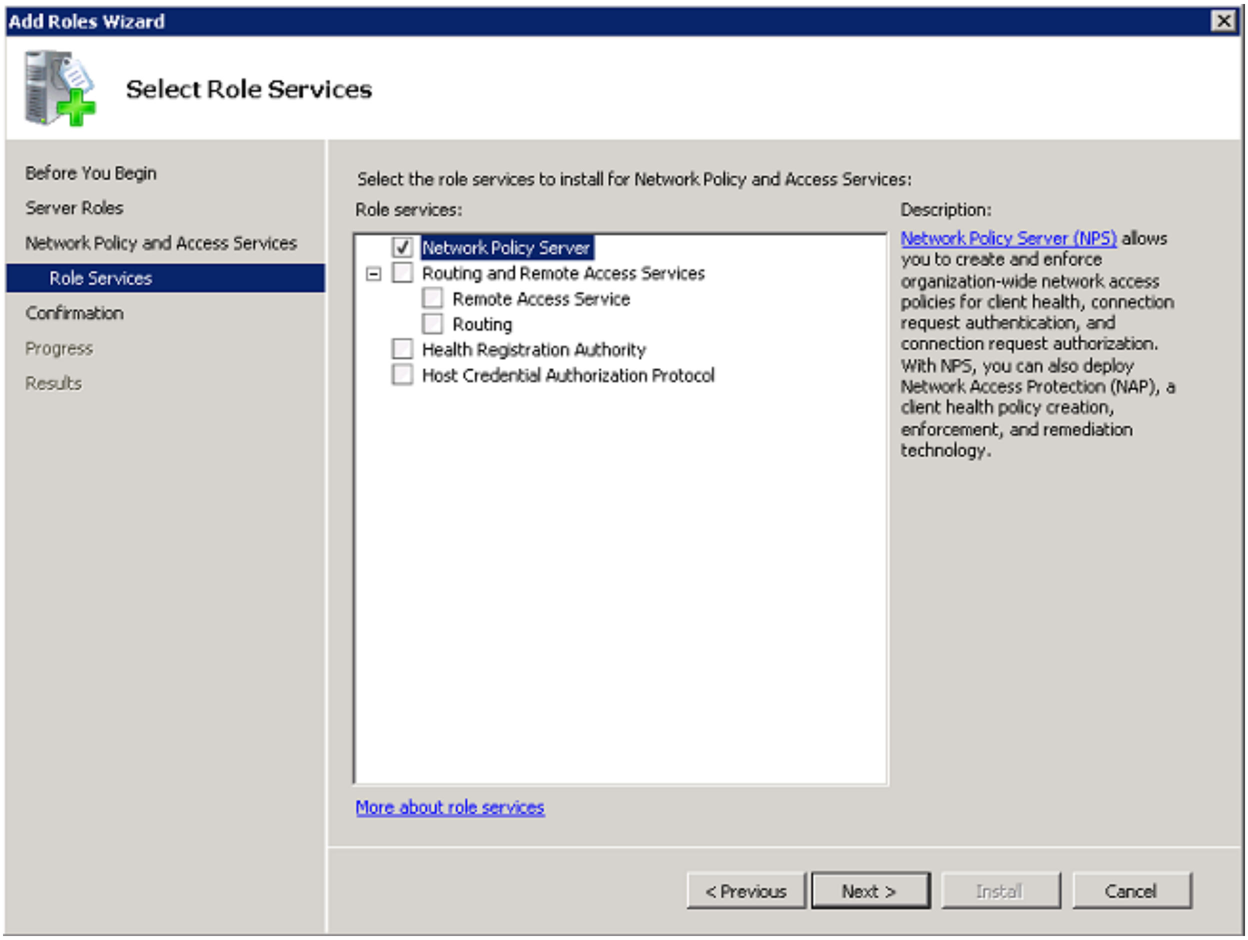
Overview of Network Policy and Access Services

NAP enforcement methods

Network Access Protection (NAP) in NPS

Network Policy Server

6. Select ***Network Policy Server***, and click ***Next***.



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

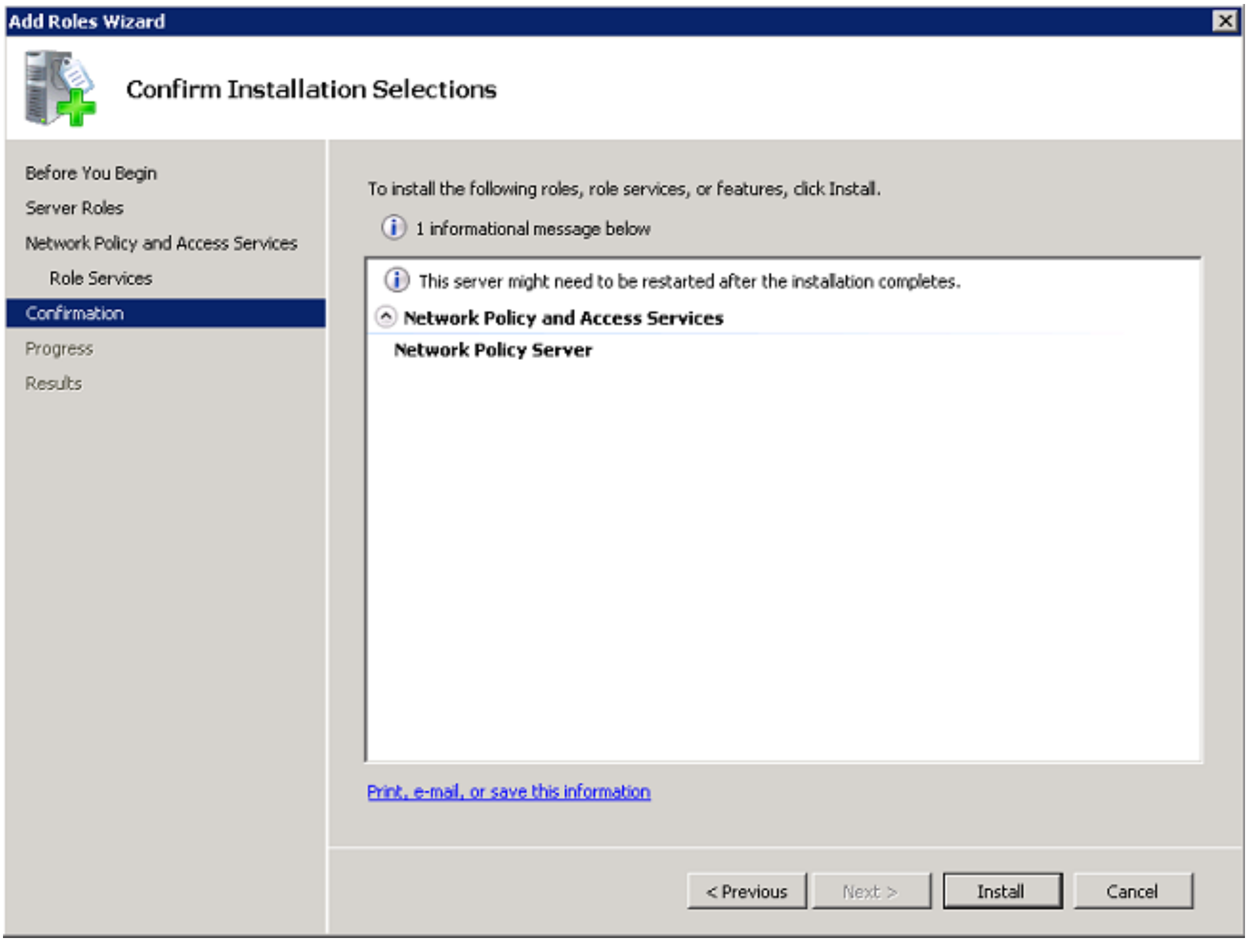
Role services:

- ☑ 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.

7. Review the confirmation, and click ***Install***.



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

1 informational message below

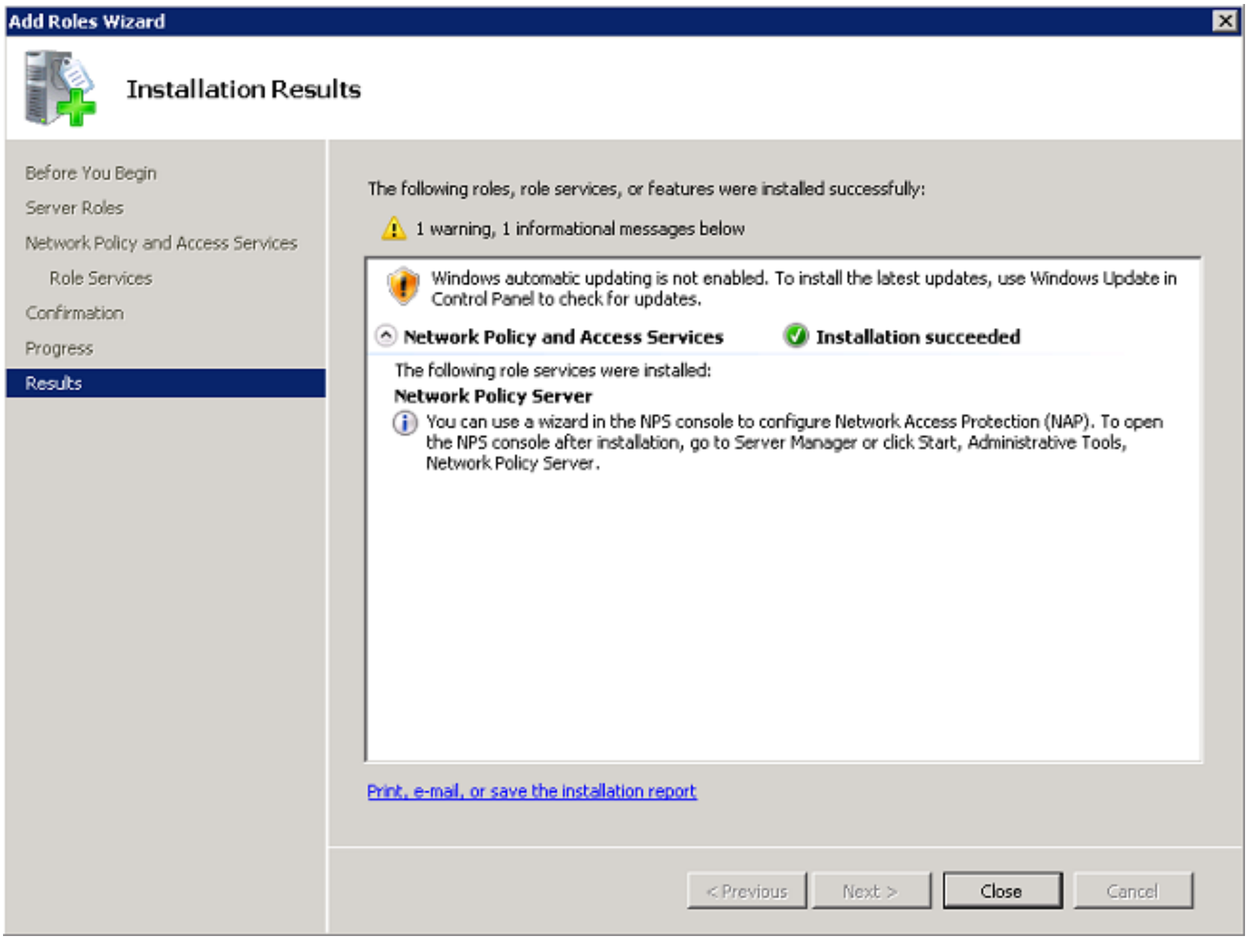
This server might need to be restarted after the installation completes.

Network Policy and Access Services

Network Policy Server

Print, e-mail, or save this information

After the install is completed, a screen similar to this one is displayed.



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.

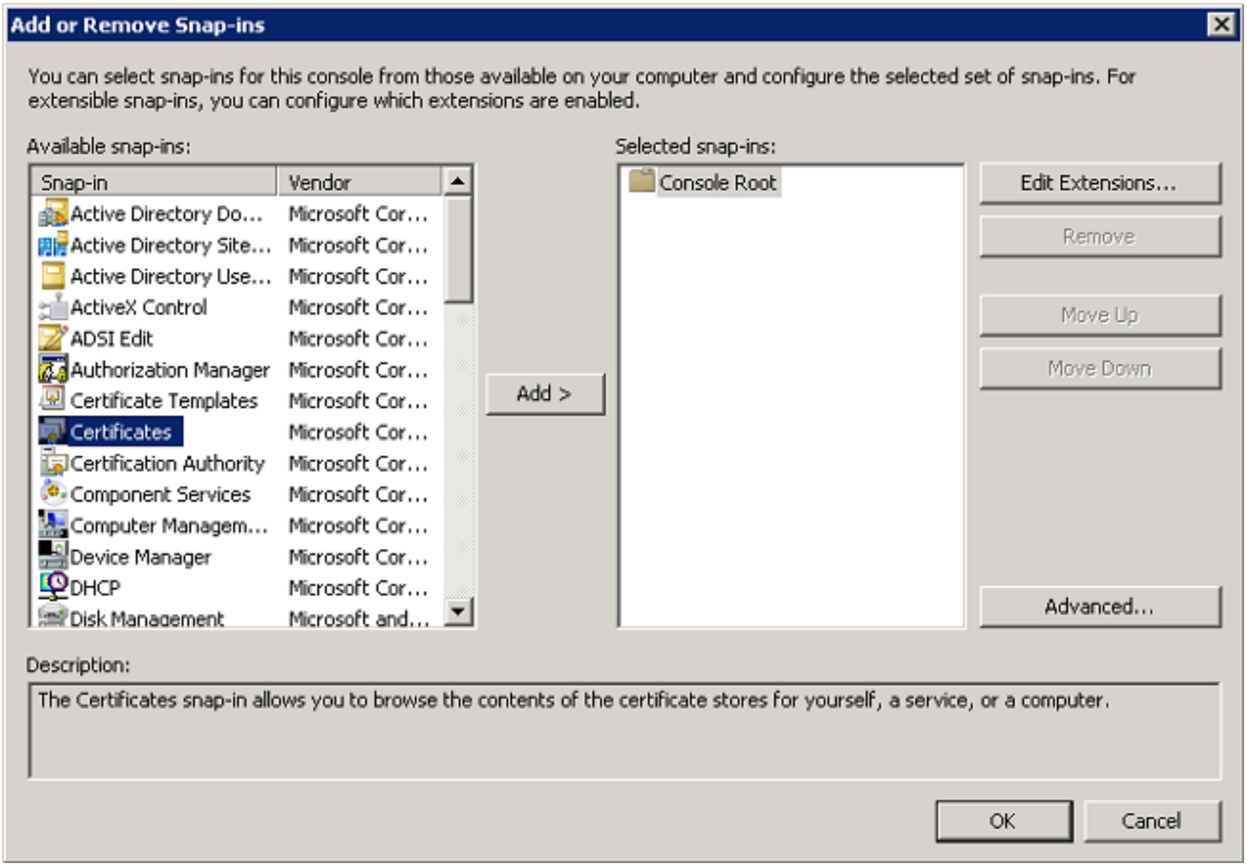
Print, e-mail, or save the installation report

8. Click ***Close***.

Install a Certificate

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

1. Click ***Start***, enter ***mmc***, and press ***Enter***.
2. Click ***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...

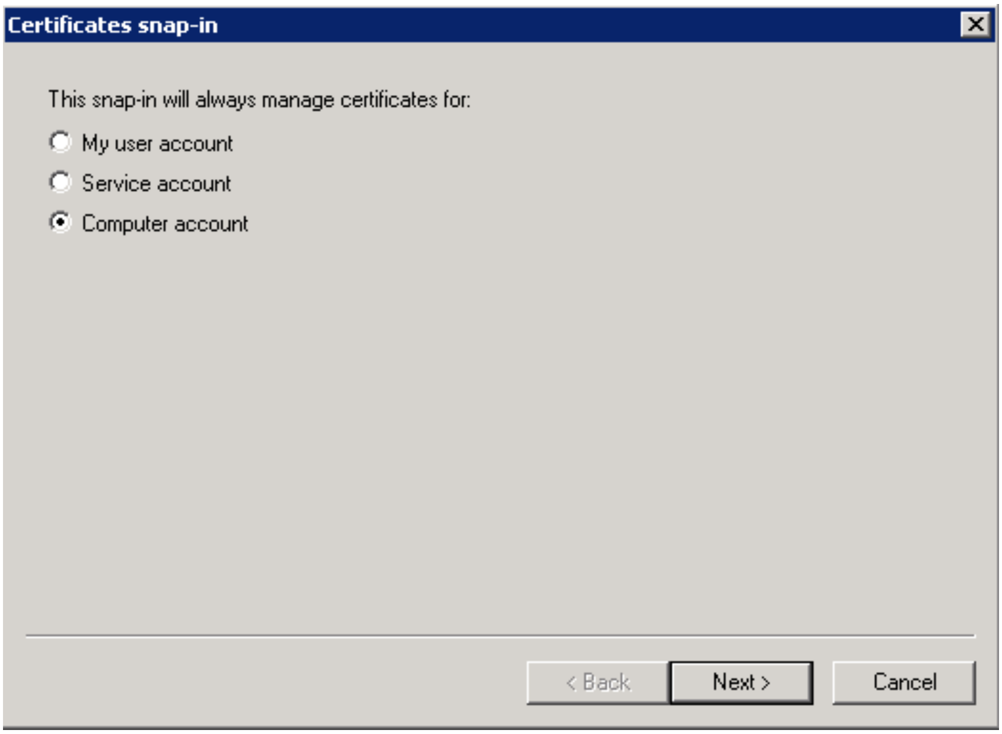
Selected snap-ins:

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. Choose ***Computer account***, and click ***Next***.



Certificates snap-in

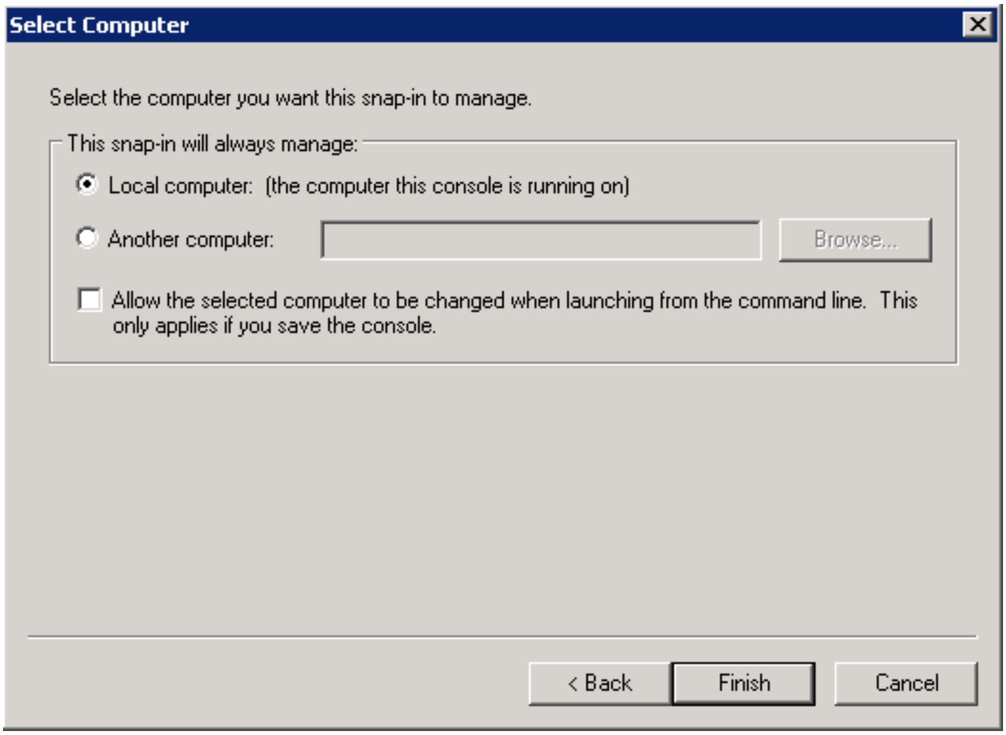
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

5. Select ***Local Computer***, and click ***Finish***.



Select Computer

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

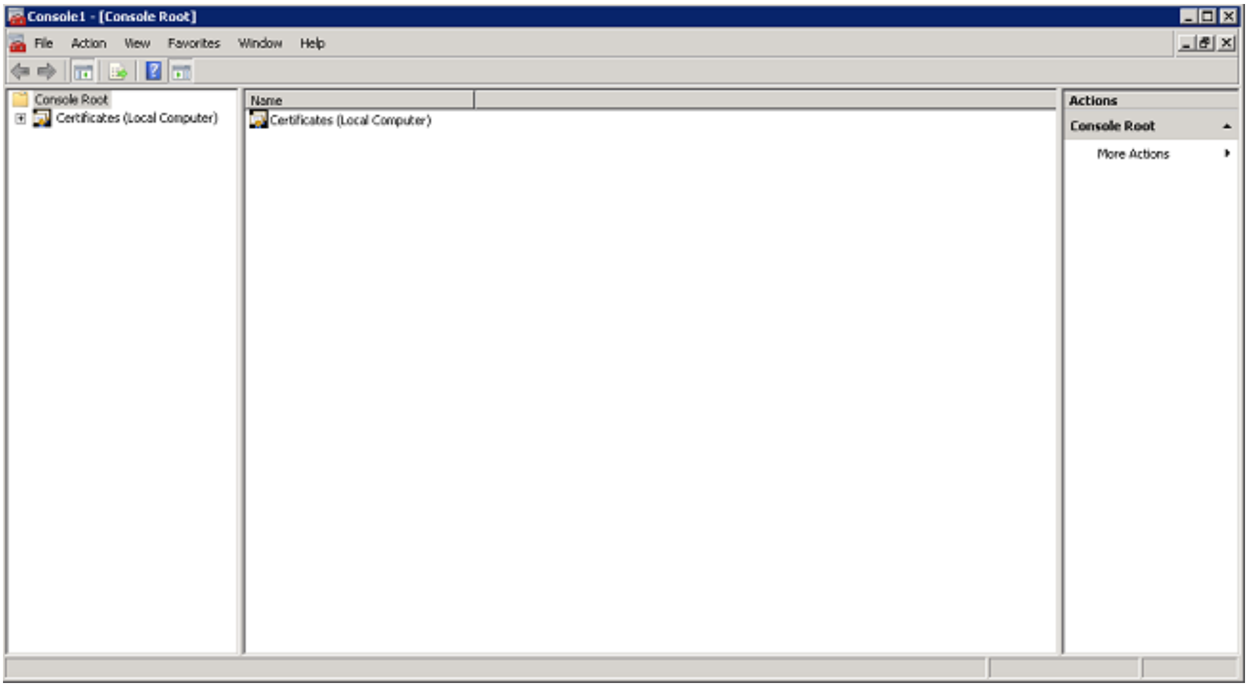
This snap-in will always manage:

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

○ Another computer:

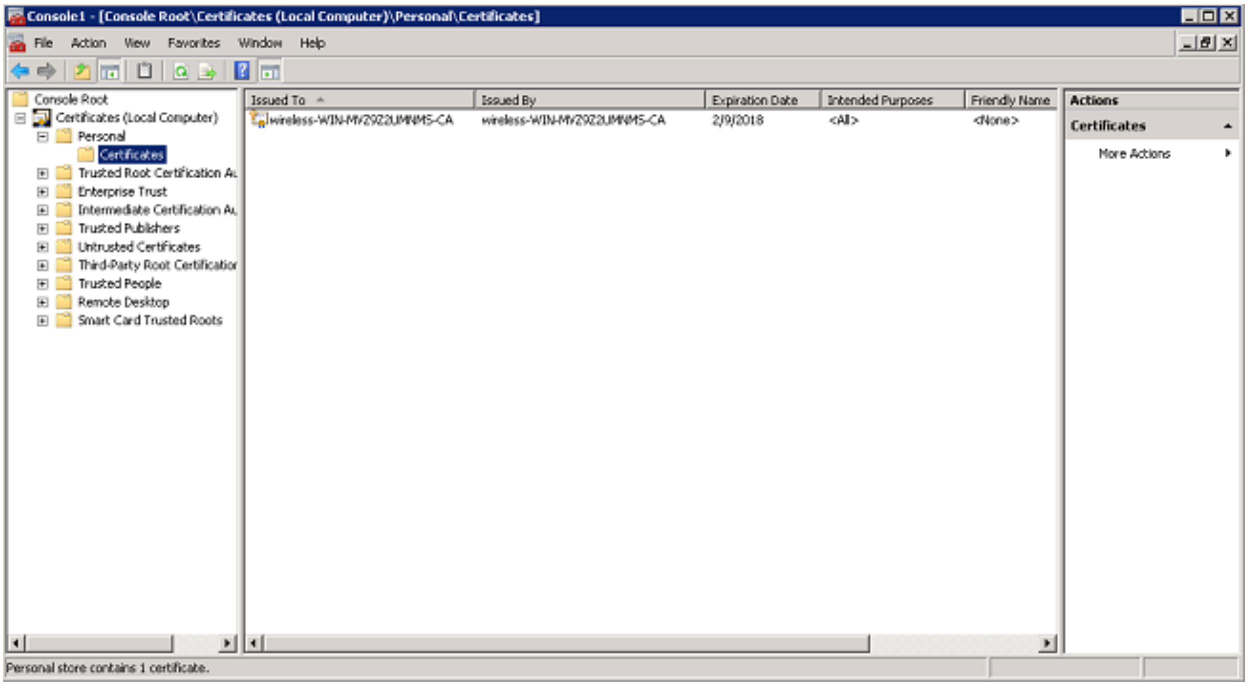
□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

6. Click ***OK*** to return to the Microsoft Management Console (MMC).



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

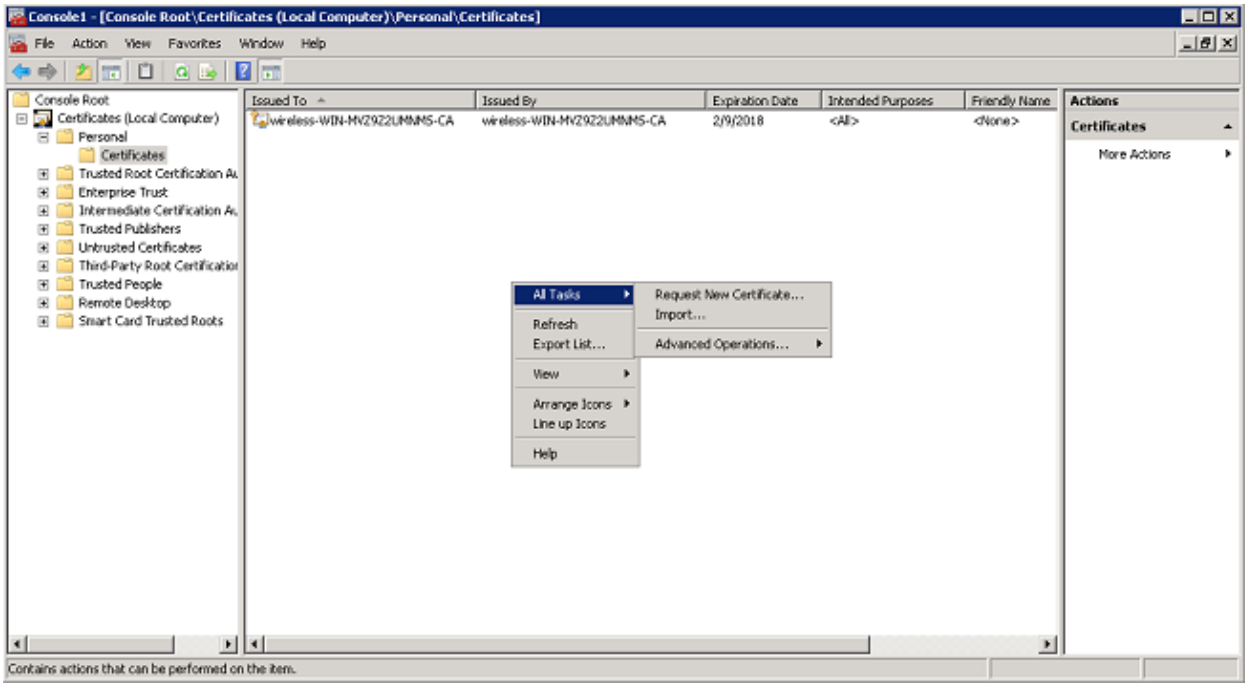
7. Expand the ***Certificates (Local Computer)*** and ***Personal*** folders, and click ***Certificates***.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
wireless-WIN-MV2922UMNMS-CA	wireless-WIN-MV2922UMNMS-CA	2/9/2018	<All>	<None>

Personal store contains 1 certificate.

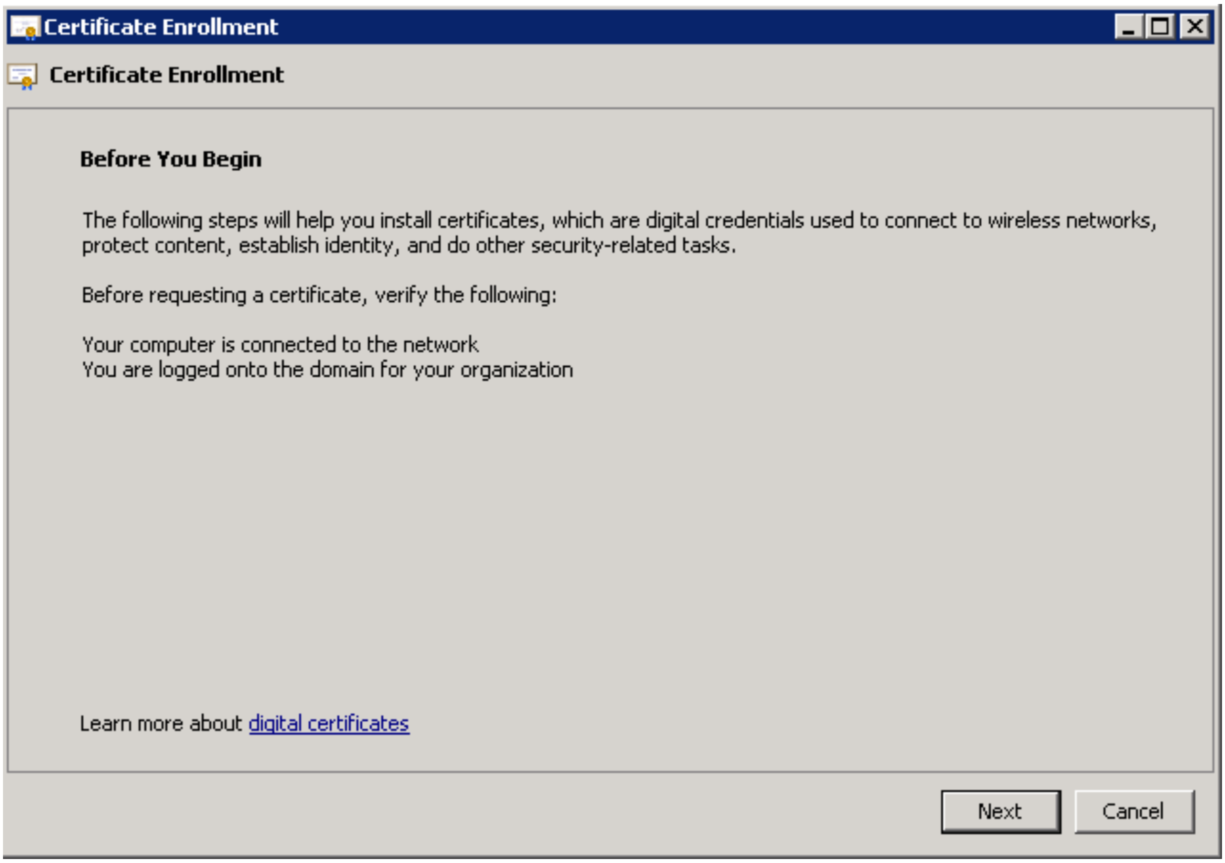
8. Right−click in the whitespace beneath the CA certificate, and choose ***All Tasks*** > ***Request New Certificate***.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
wireless-WIN-MV2922UMNMS-CA	wireless-WIN-MV2922UMNMS-CA	2/9/2018	<All>	<None>

Contains actions that can be performed on the item.

9. Click ***Next***.



Certificate Enrollment

Certificate Enrollment

Before You Begin

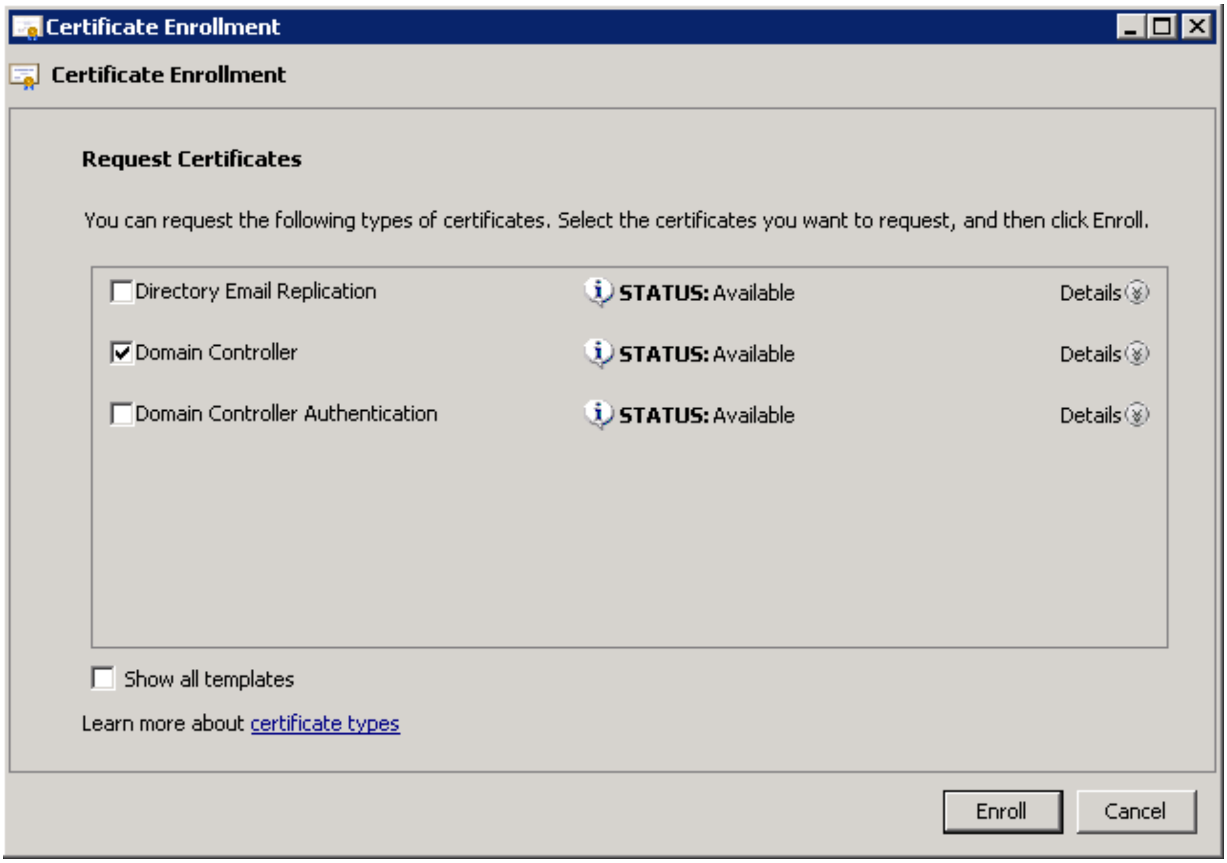
The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

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. Select ***Domain Controller***, and click ***Enroll***.



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

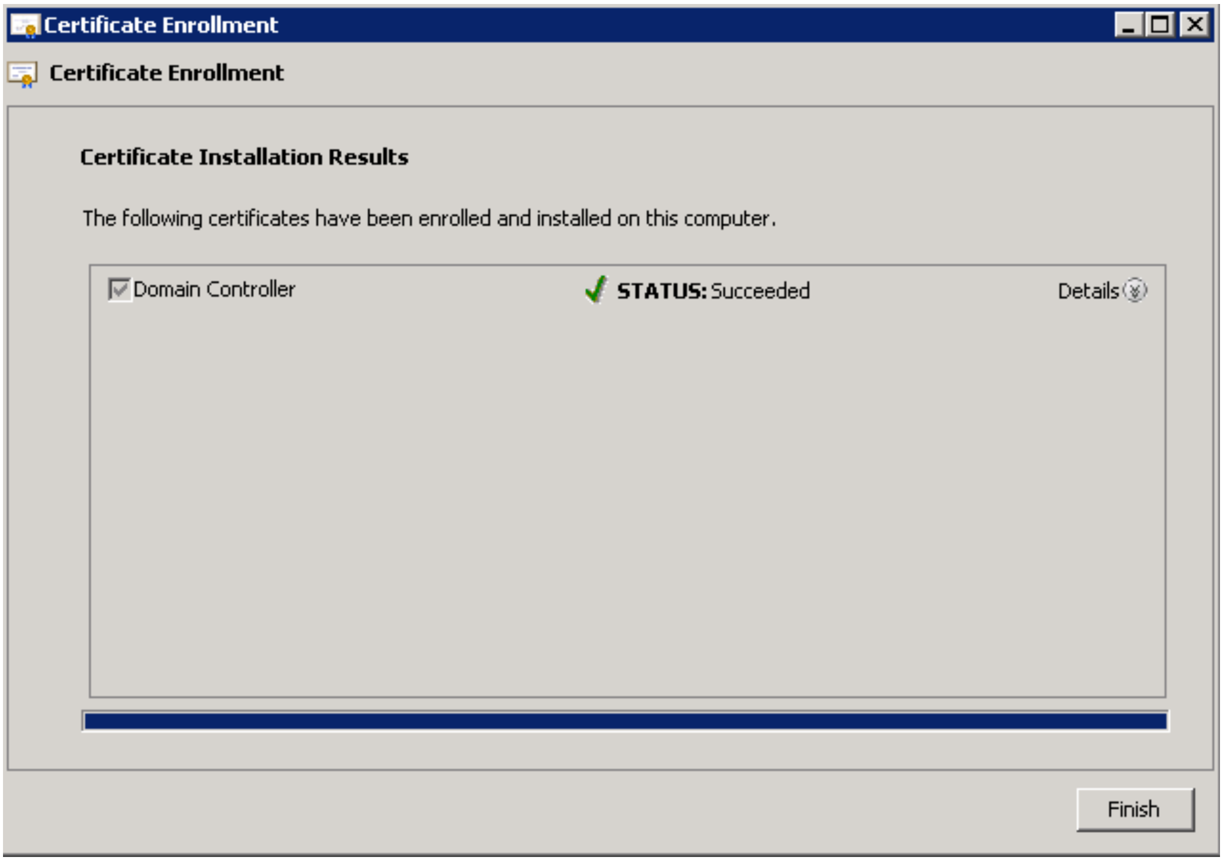
☑ Domain Controller — **STATUS:** Available — Details

☐ Domain Controller Authentication — **STATUS:** Available — Details

☐ Show all templates

Learn more about certificate types

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



Certificate Enrollment

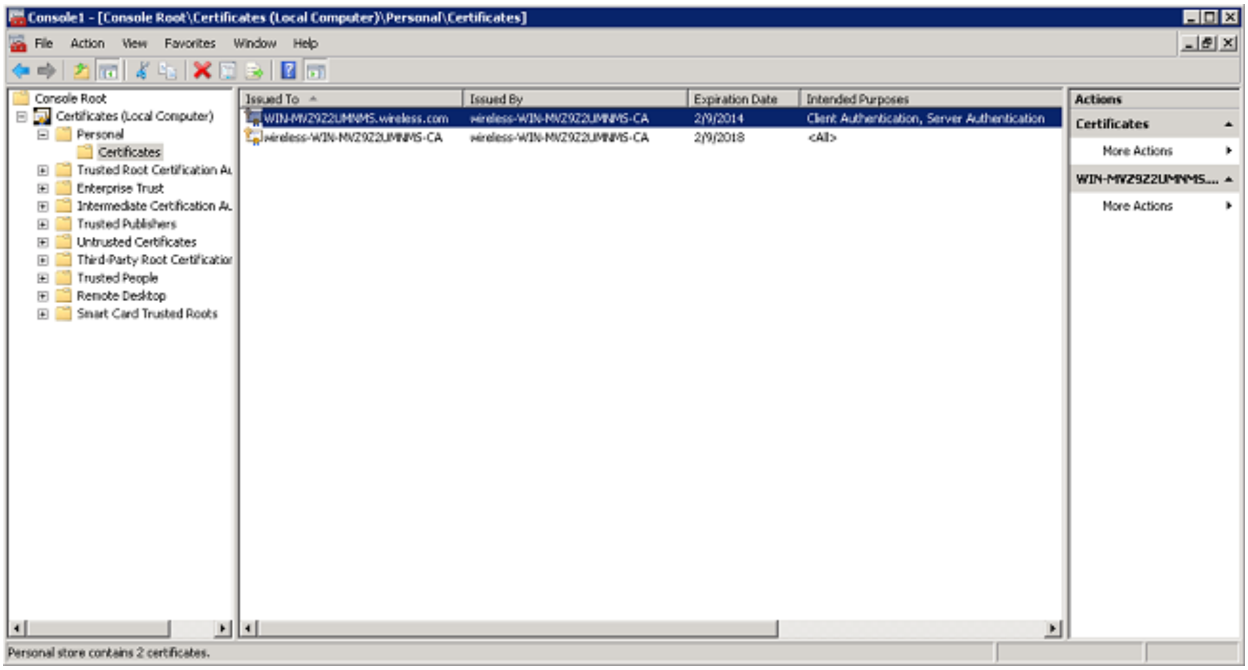
Certificate Installation Results

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 the Intended Purpose of the certificate reads ***Client Authentication, Server Authentication***.



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

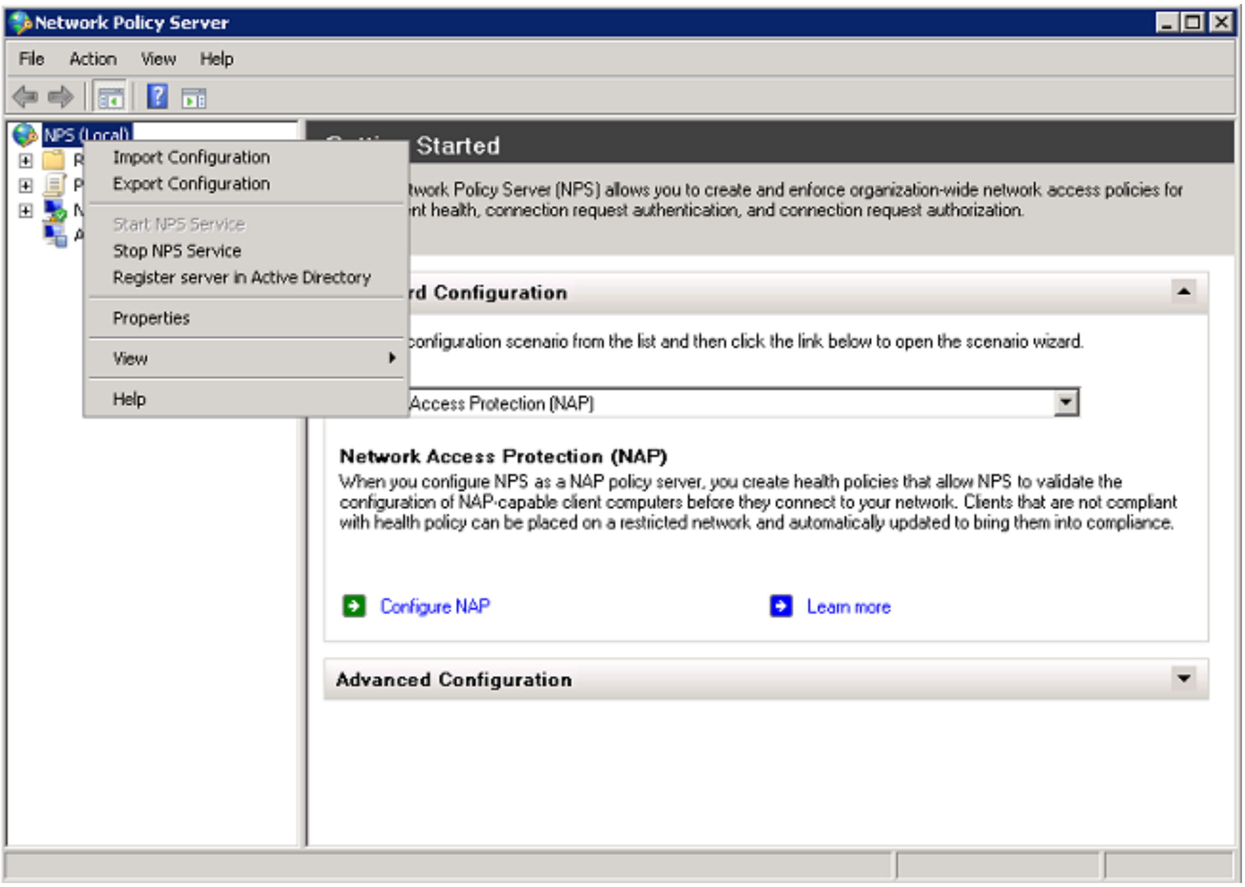
Issued To	Issued By	Expiration Date	Intended Purposes
WIN-MVZ9Z2UMNMS.wireless.com	wireless-WIN-MVZ9Z2UMNMS-CA	2/9/2014	Client Authentication, Server Authentication
wireless-WIN-MVZ9Z2UMNMS-CA	wireless-WIN-MVZ9Z2UMNMS-CA	2/9/2018	<All>

Personal store contains 2 certificates.

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

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

1. Click ***Start*** > ***Administrative Tools*** > ***Network Policy Server***.
2. Right−click ***NPS (Local)***, and choose ***Register server in Active Directory***.



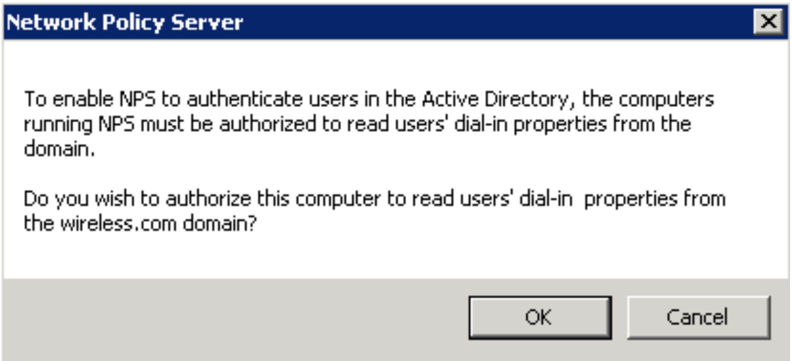
twork Policy Server (NPS) allows you to create and enforce organization-wide network access policies for nt health, connection request authentication, and connection request authorization.

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.

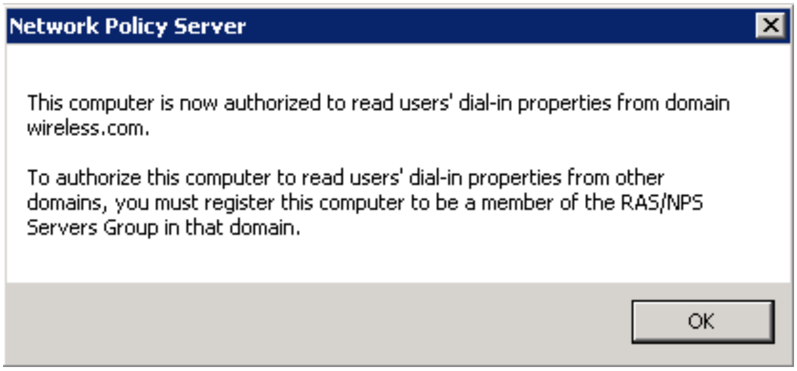
3. Click ***OK***.



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?

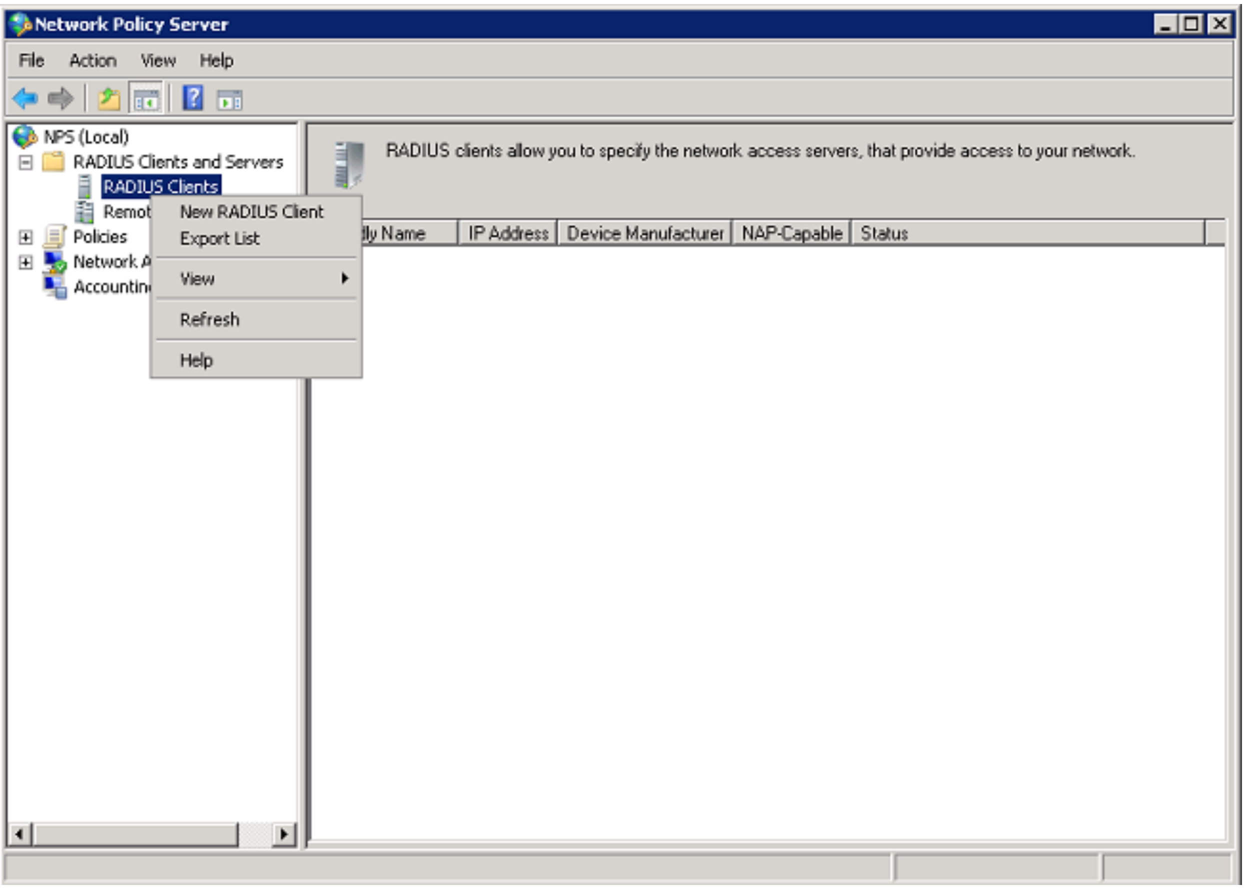
4. Click ***OK***.



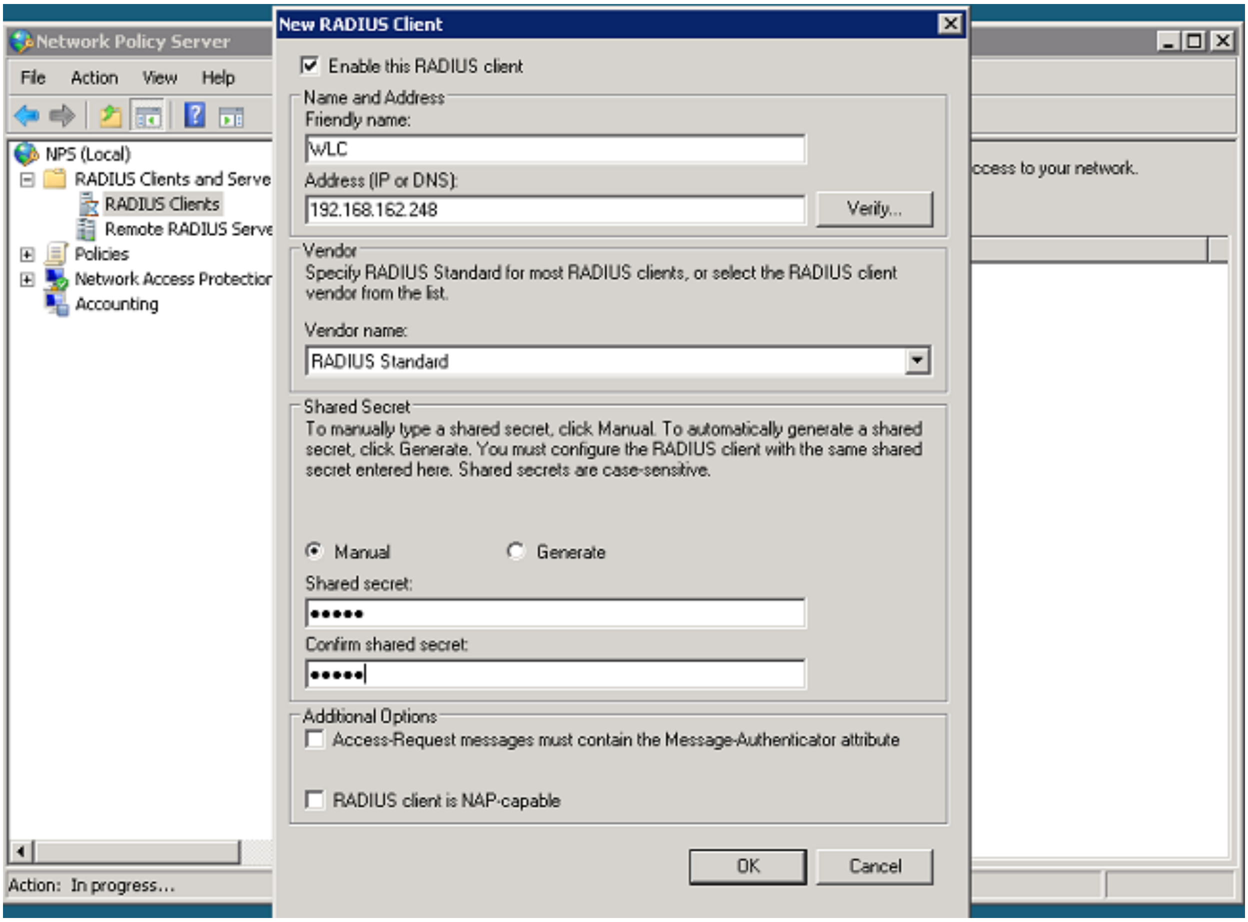
This computer is now authorized to read users' dial-in properties from domain wireless.com.

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 Wireless LAN Controller 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 Friendly name (WLC in this example), the management IP address of the WLC (192.168.162.248 in this example) and a shared secret. The same shared secret is used to configure the WLC.



New RADIUS Client

☑ Enable this RADIUS client

Name and Address

Friendly name: WLC

Address (IP or DNS): 192.168.162.248

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

Shared Secret

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: ●●●●●

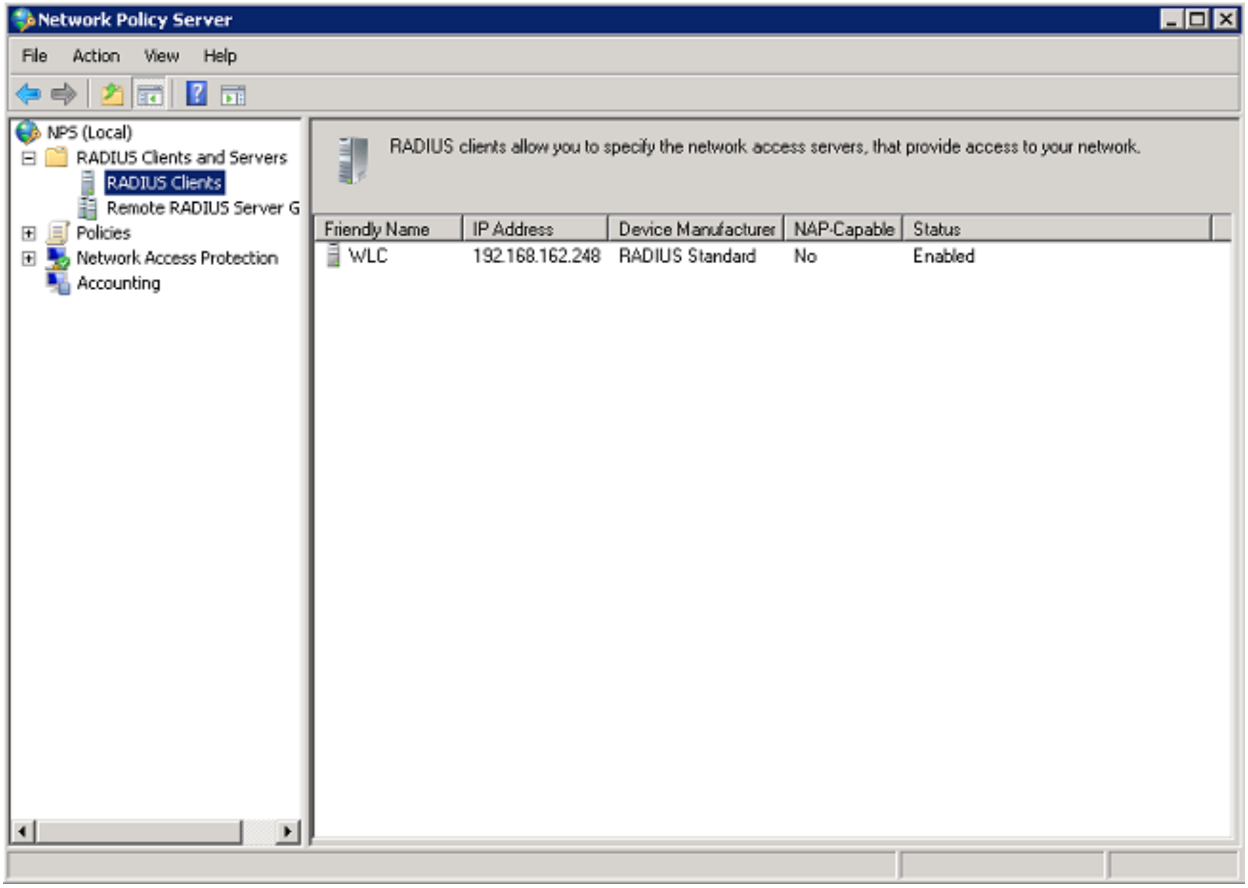
Additional Options

□ Access-Request messages must contain the Message-Authenticator attribute

□ RADIUS client is NAP-capable

Action: In progress...

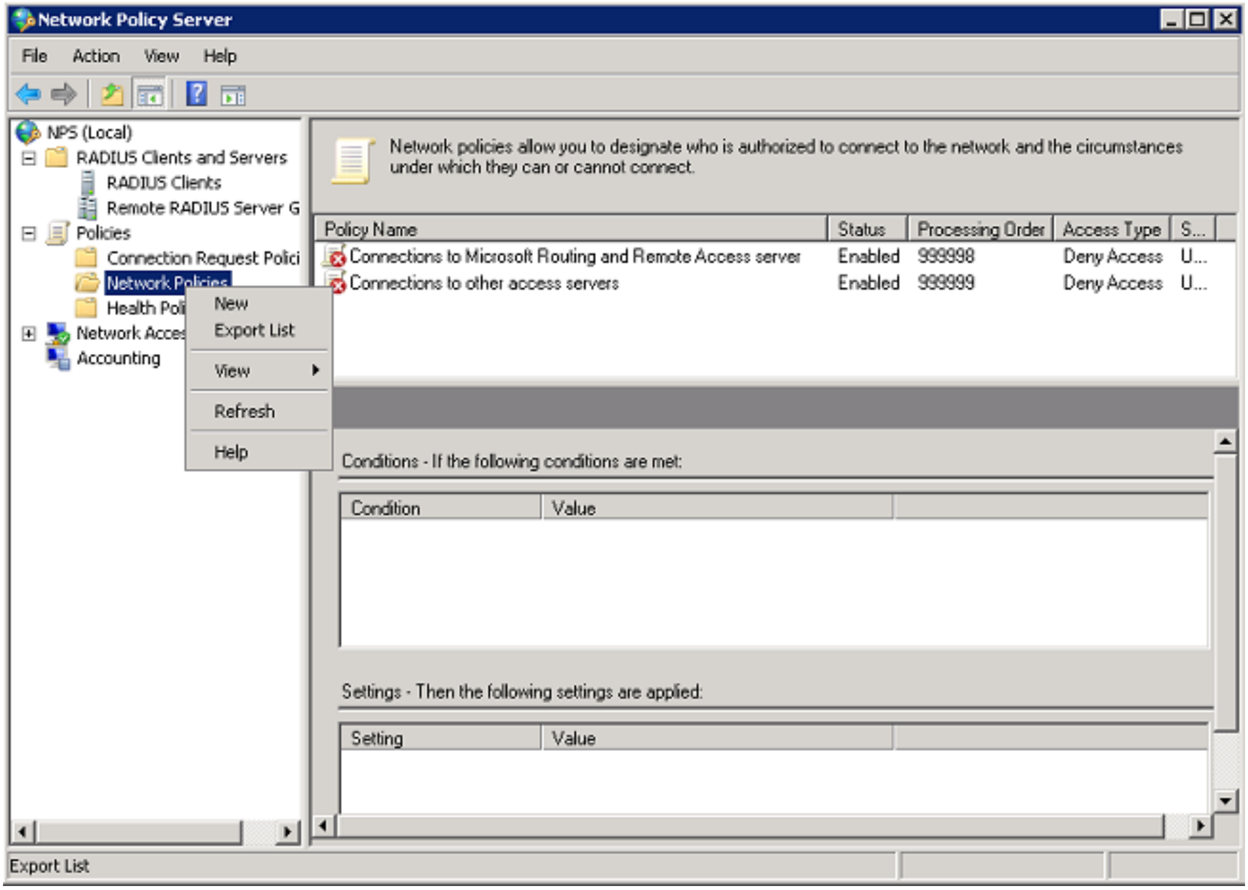
8. Click ***OK*** to return to the previous screen.



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

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
WLC	192.168.162.248	RADIUS Standard	No	Enabled

9. Create a new Network Policy for 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:

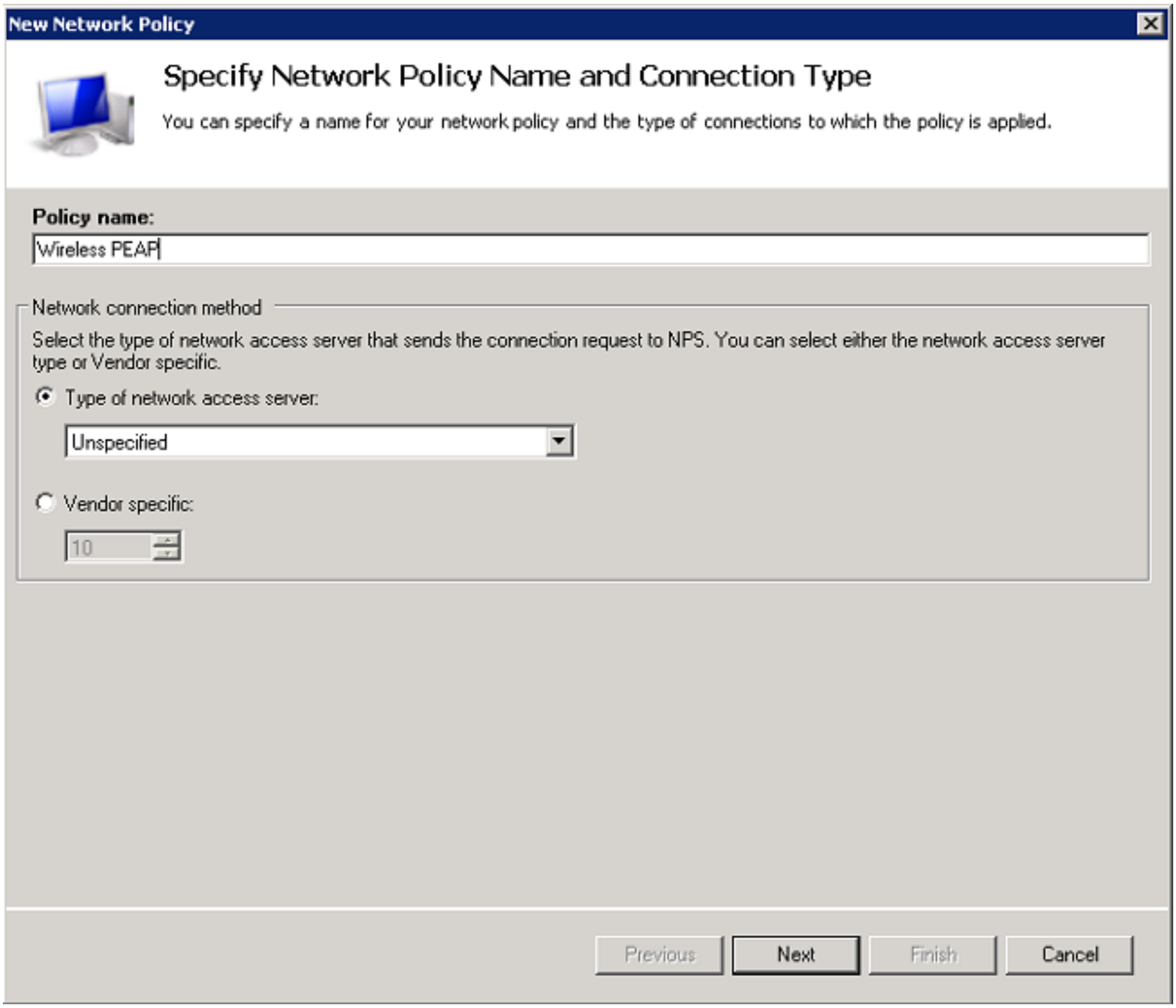
Condition	Value

Settings - Then the following settings are applied:

Setting	Value

Export List

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



New Network Policy

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:
Wireless PEAP

Network connection method

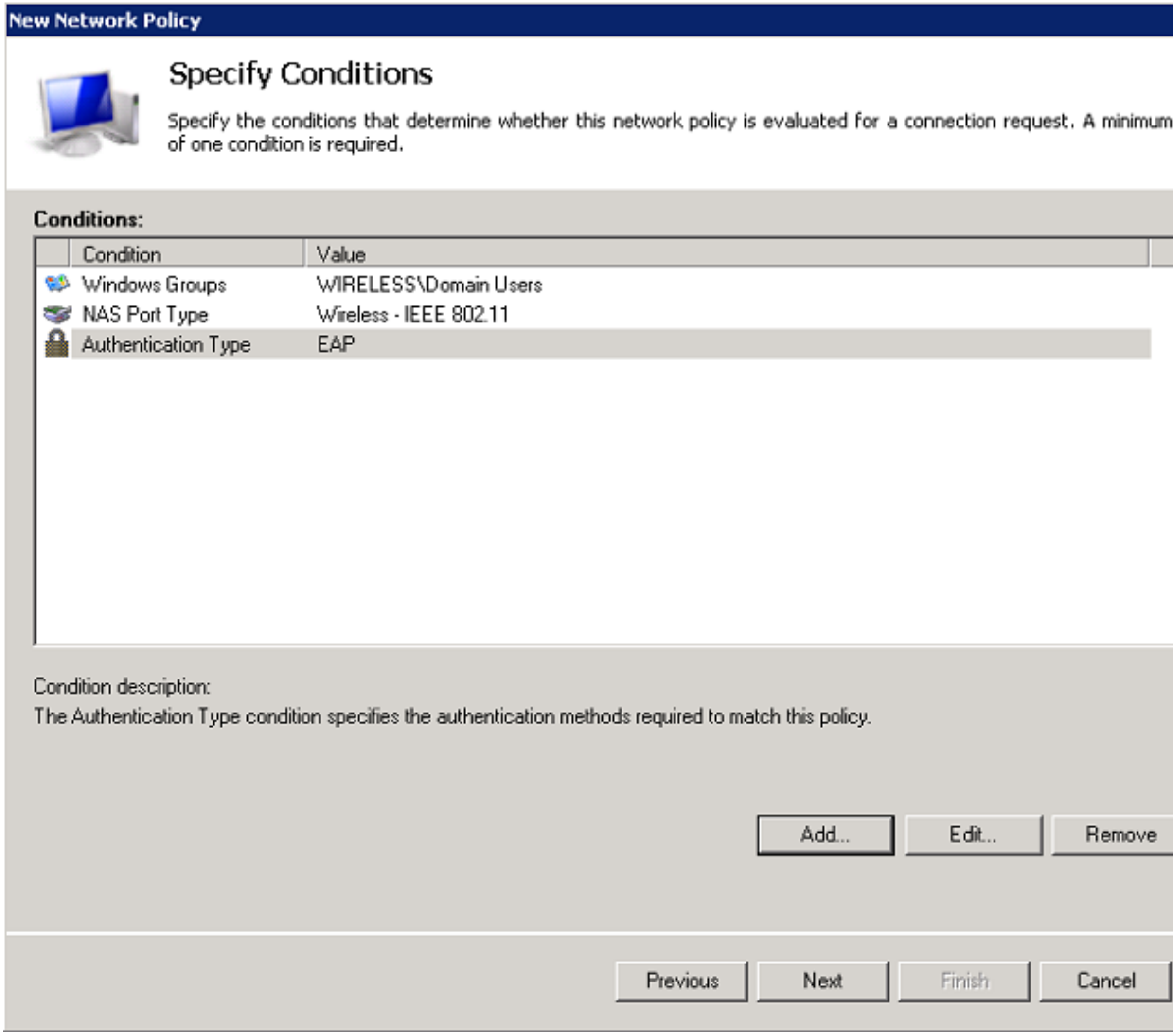
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

● Type of network access server:
Unspecified

○ Vendor specific:
10

11. To have this policy allow only wireless domain users, add these three conditions, and click ***Next***:

   - Windows Groups − Domain Users
   - NAS Port Type − Wireless − IEEE 802.11
   - Authentication Type − EAP



Specify Conditions

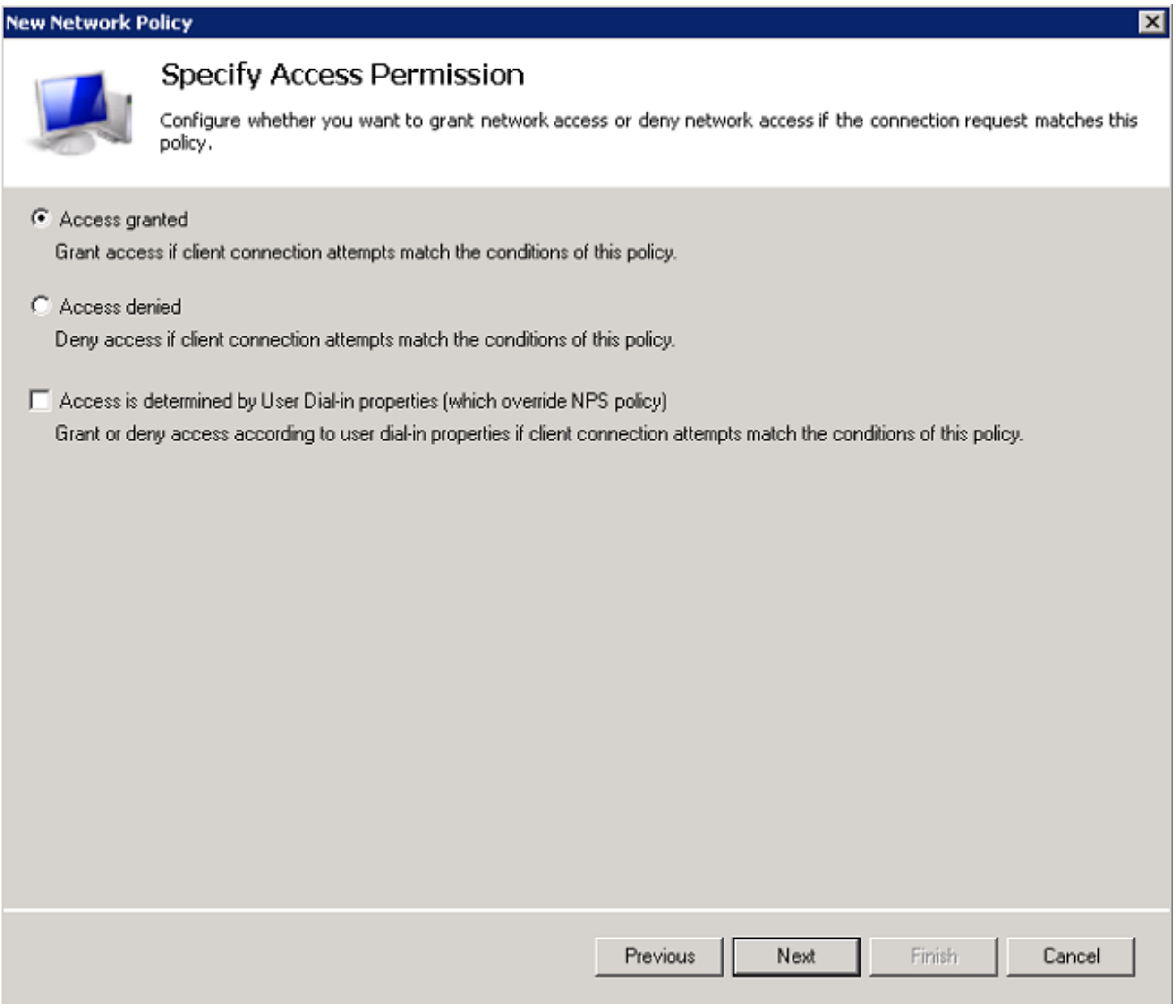
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

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 ***Access granted*** to grant connection attempts that match this policy, and click ***Next***.



New Network Policy

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.

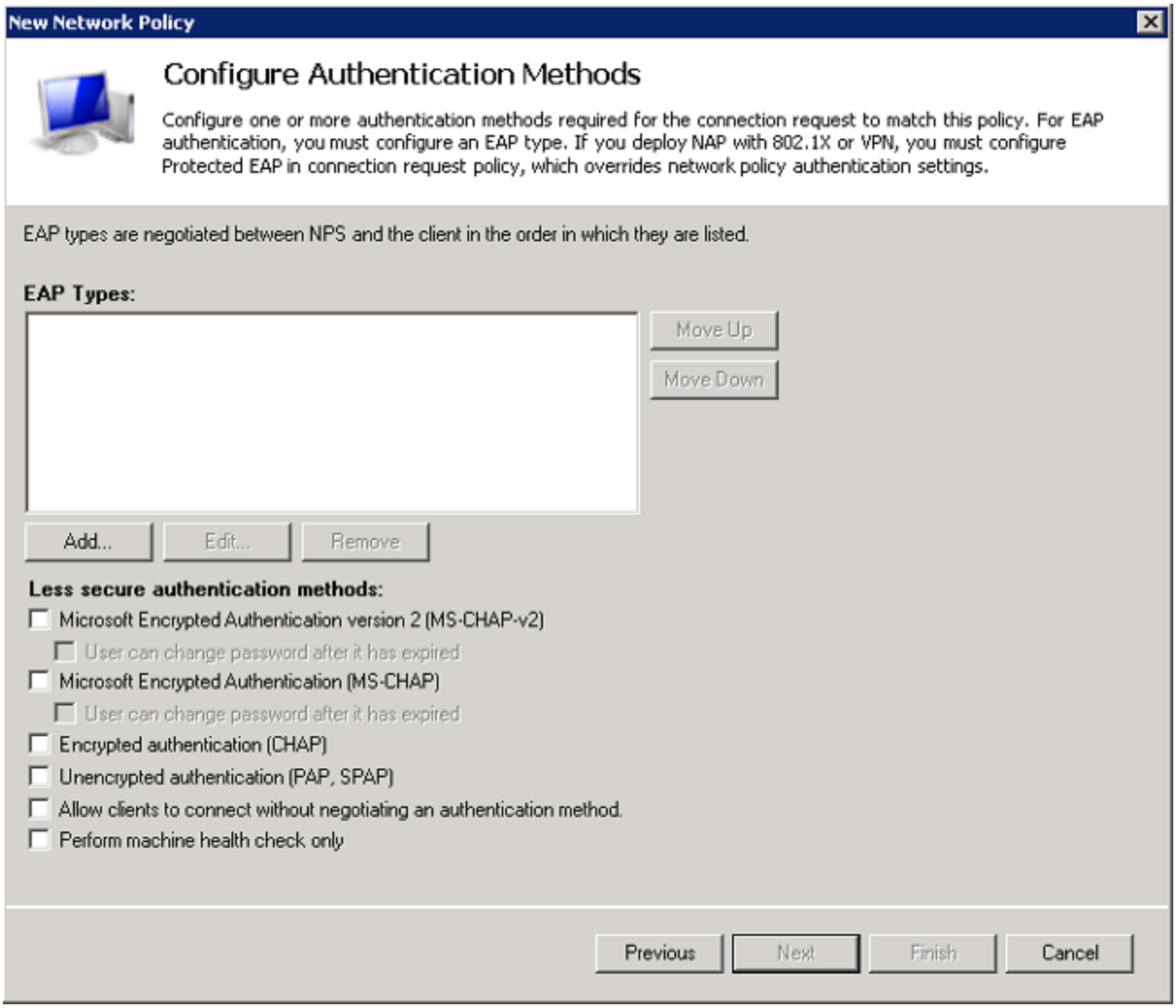
○ Access denied

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 the authentication methods under Less secure authentication methods.



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

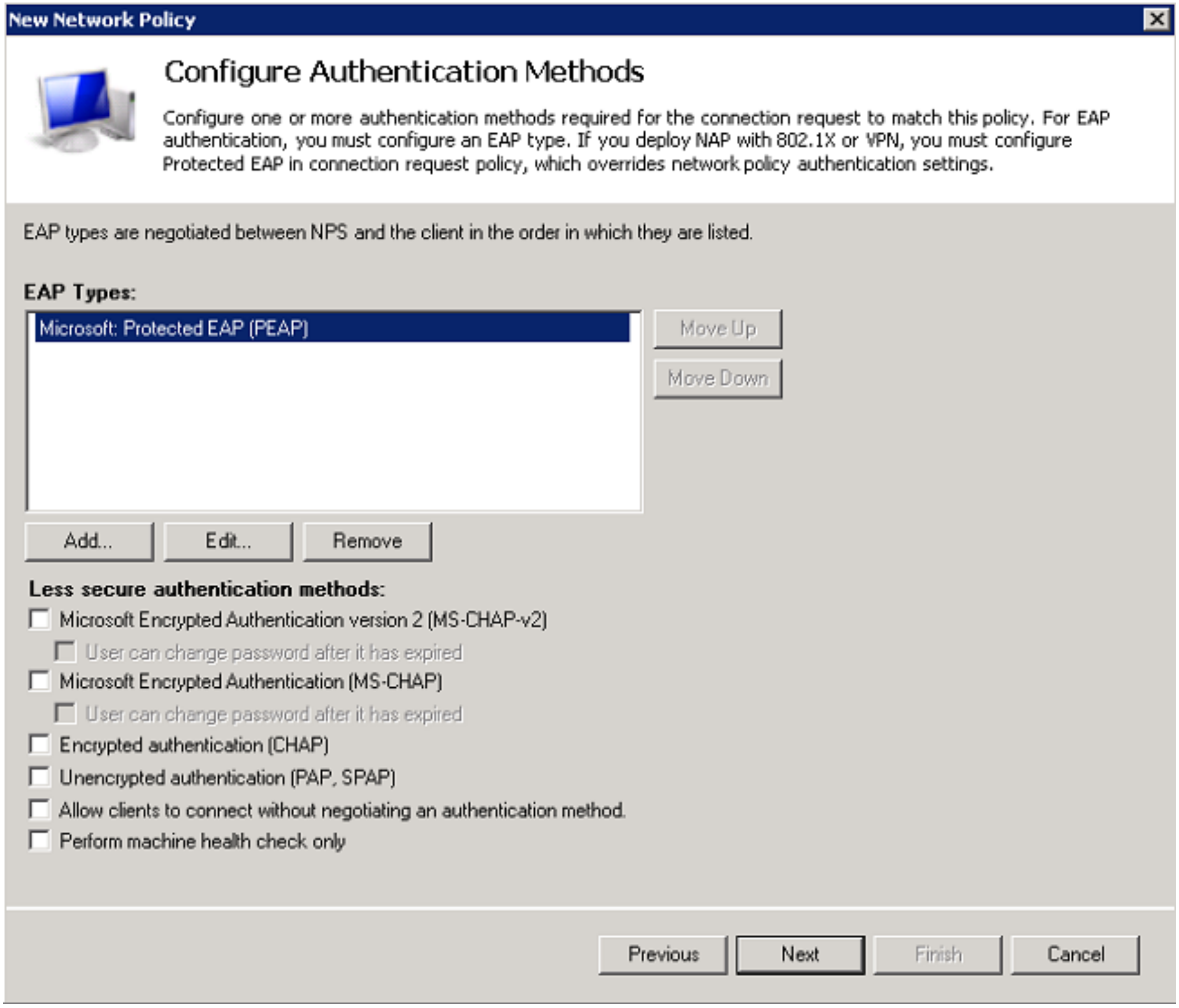
☐ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method.

☐ Perform machine health check only

14. Click ***Add***, select PEAP, and click ***OK*** to enable PEAP.



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

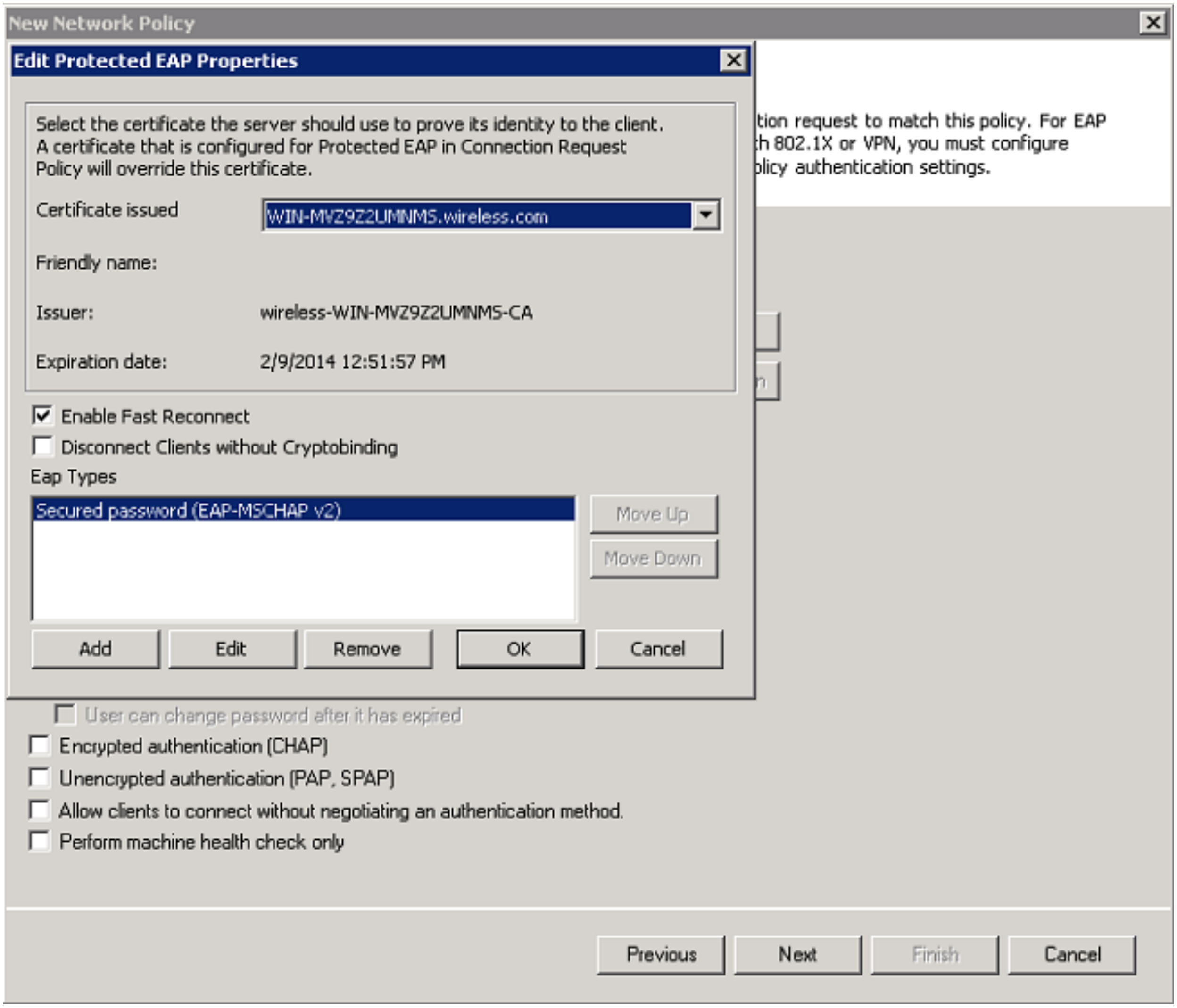
□ Encrypted authentication (CHAP)

□ 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 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: WIN-MVZ9Z2UMNMS.wireless.com

Friendly name:

Issuer: wireless-WIN-MVZ9Z2UMNMS-CA

Expiration date: 2/9/2014 12:51:57 PM

☑ Enable Fast Reconnect

☐ Disconnect Clients without Cryptobinding

Eap Types

Secured password (EAP-MSCHAP v2)

tion request to match this policy. For EAP
h 802.1X or VPN, you must configure
licy authentication settings.

☐ User can change password after it has expired

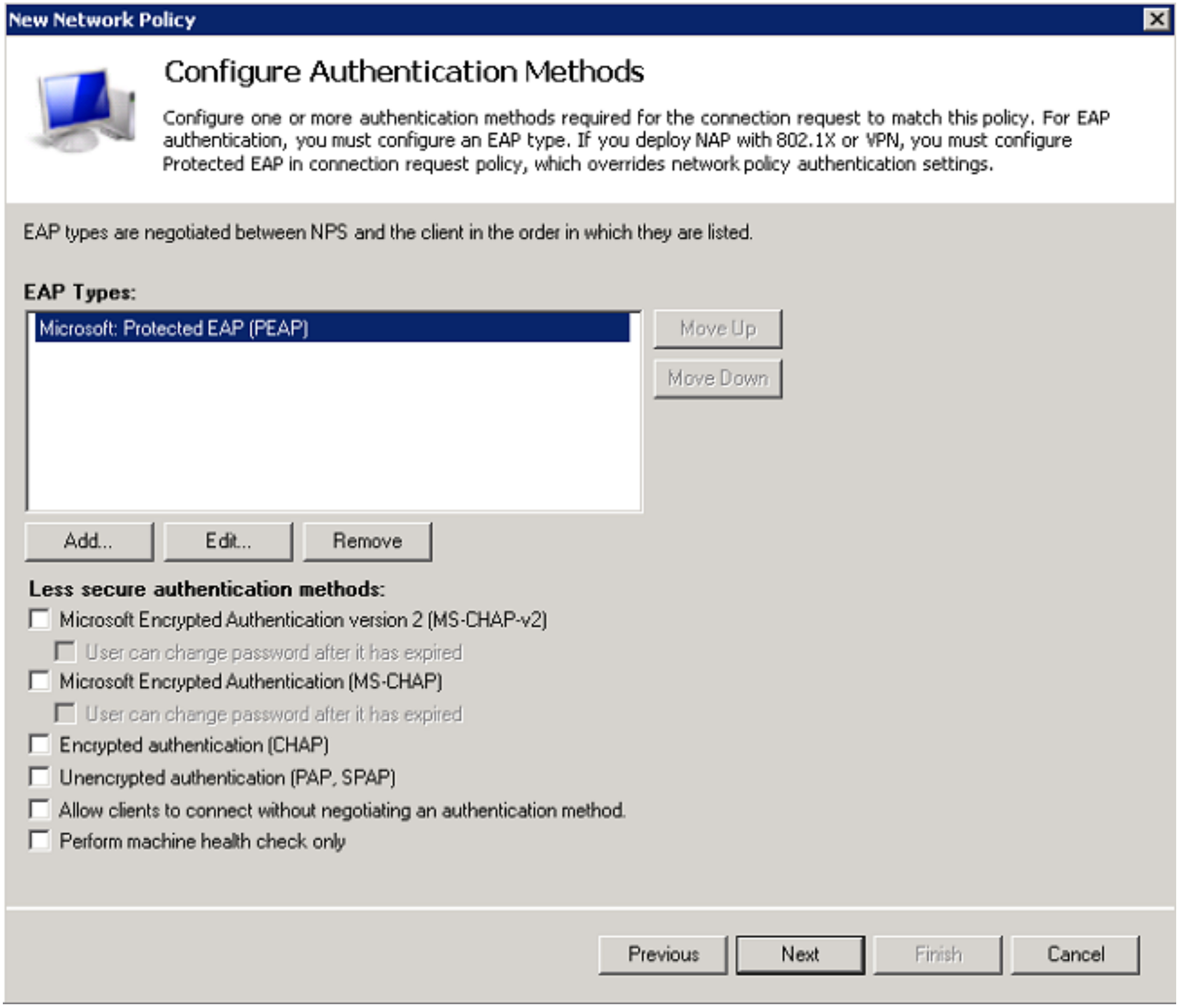
☐ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method.

☐ Perform machine health check only

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.

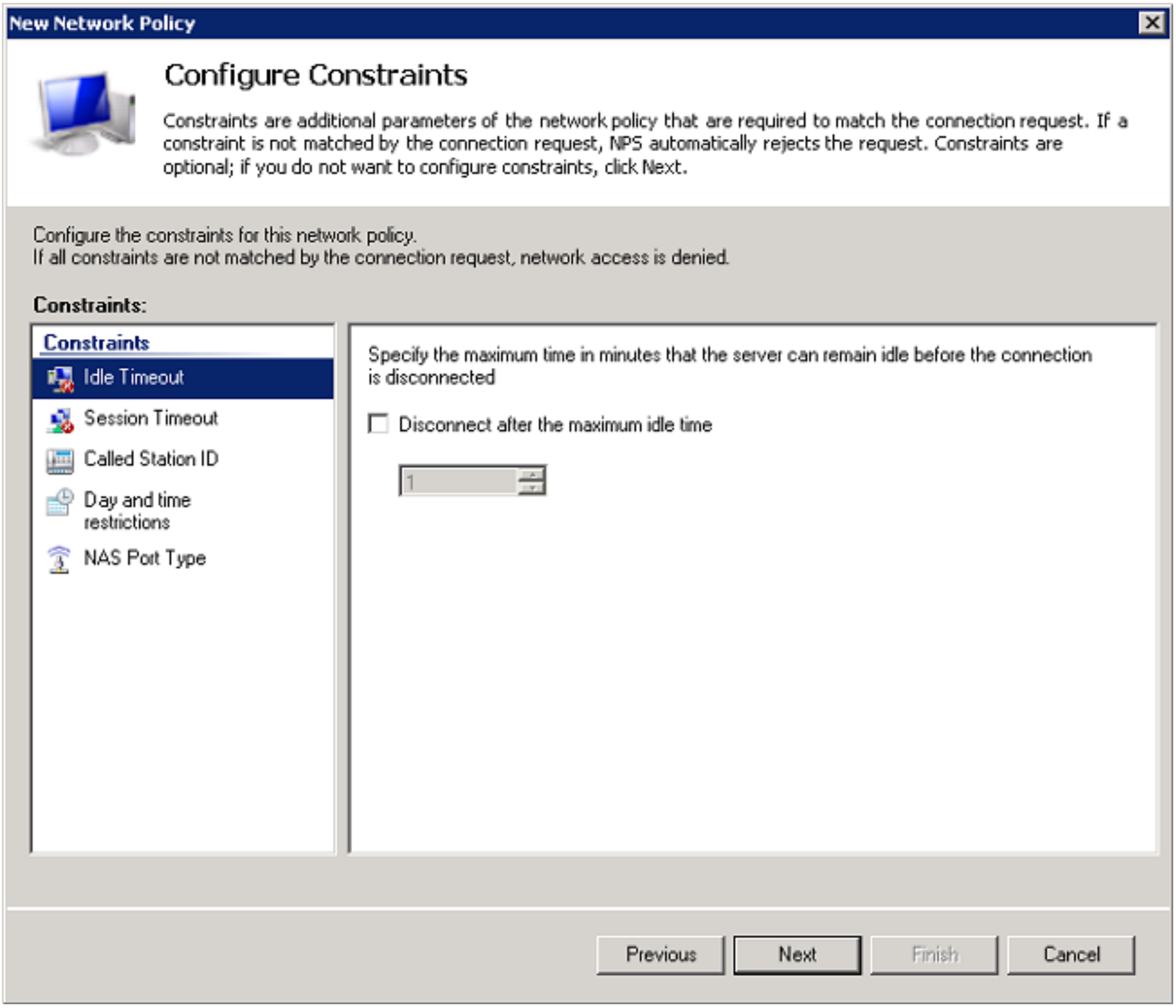
EAP Types:

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.

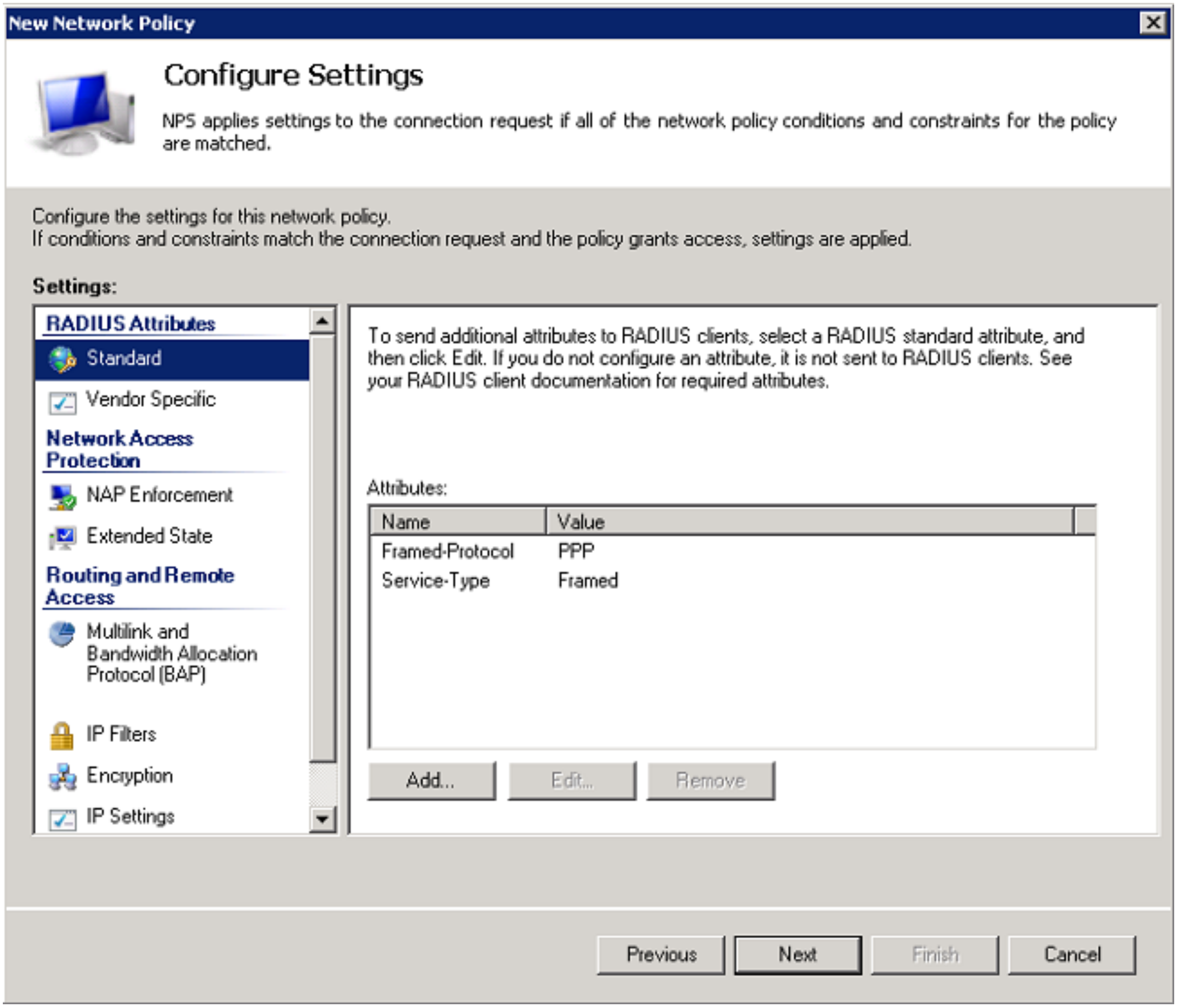
Constraints:

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***.



New Network Policy

Configure Settings

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

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

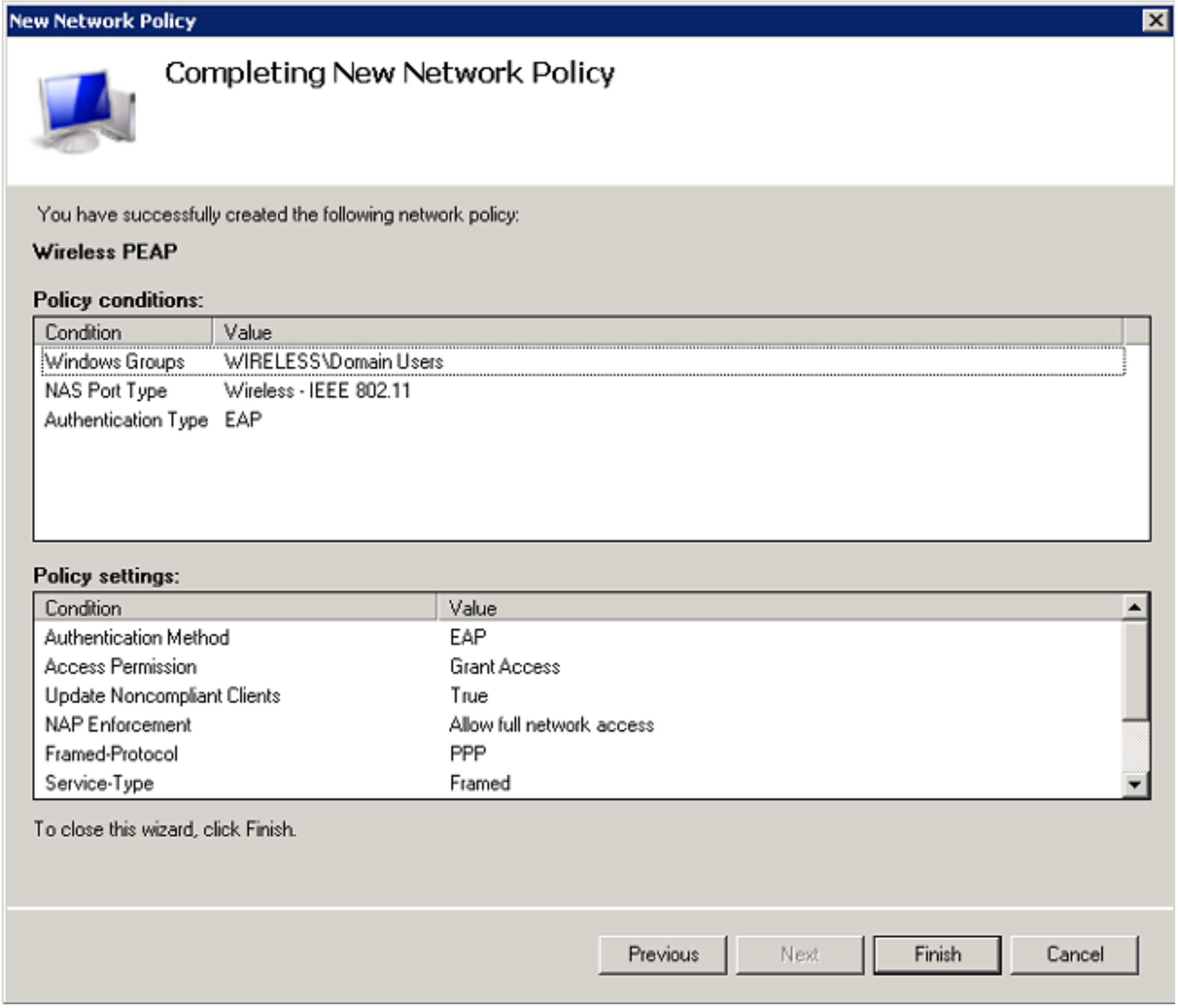
Settings:

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***.



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:

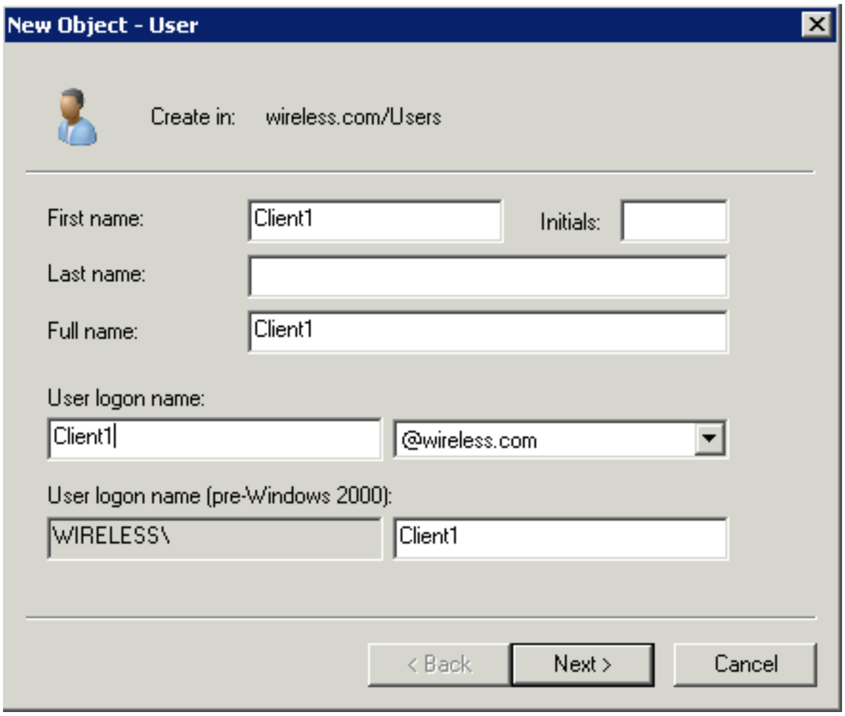
Condition	Value
Authentication Method	EAP
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Add Users to the Active Directory

In this example, the user database is maintained on the Active Directory. Complete these steps in order to add users to the Active Directory database:

1. Open Active Directory Users and Computers. Click ***Start*** > ***Administrative Tools*** > ***Active Directory Users and Computers***.
2. In the Active Directory Users and Computers console tree, expand the domain, right−click ***Users*** > ***New***, and choose ***User***.
3. In the New Object ? User dialog box, enter the name of the wireless user. This example uses the name Client1 in the First name field and Client1 in the User logon name field. Click ***Next***.



Create in: wireless.com/Users

First name: Client1

Initials:

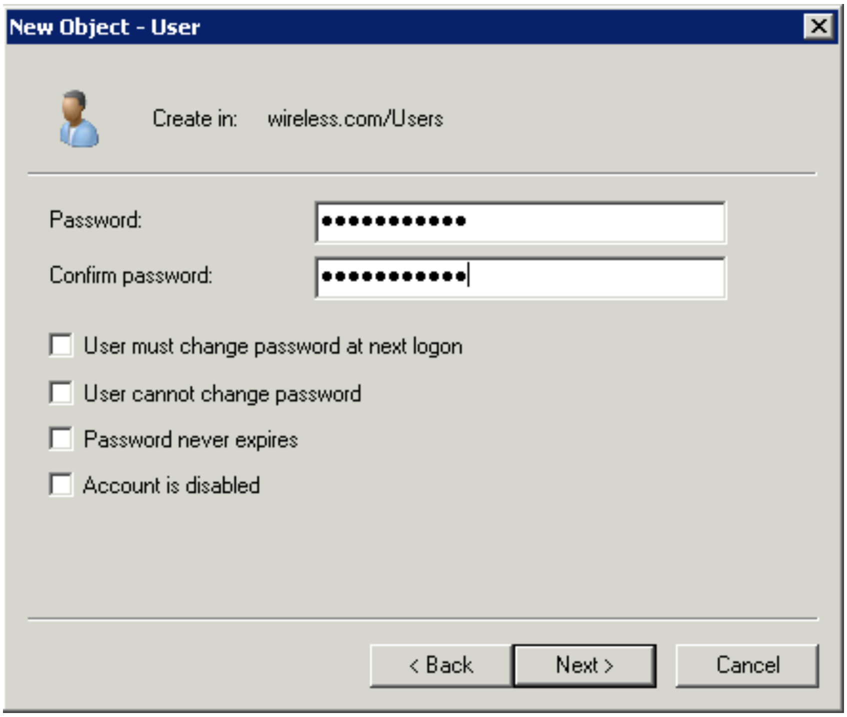
Last name:

Full name: Client1

User logon name: Client1 @wireless.com

User logon name (pre-Windows 2000): WIRELESS\ Client1

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/Users

Password: ●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●

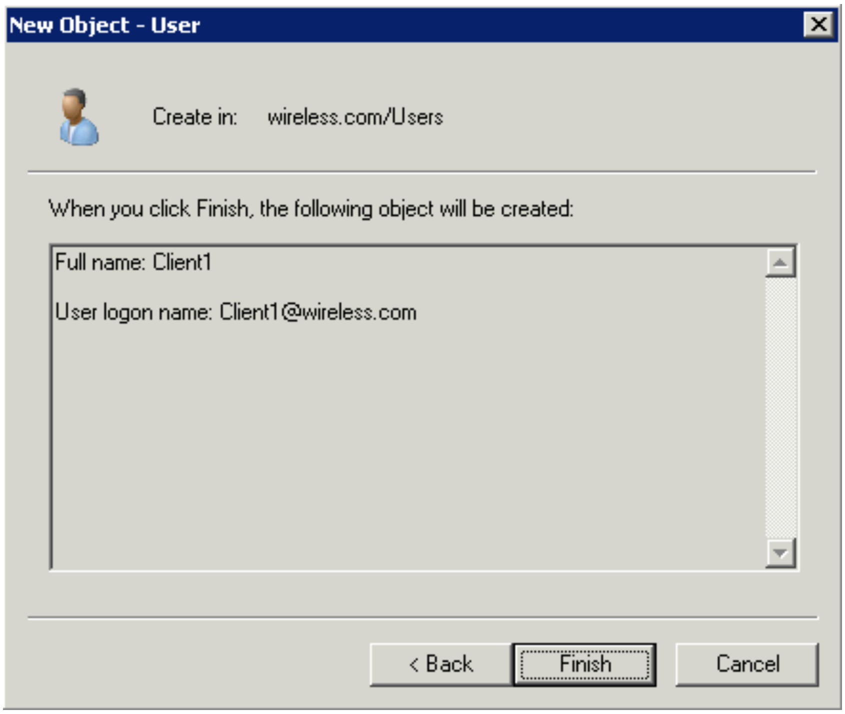
□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

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



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

Full name: Client1

User logon name: Client1@wireless.com

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

Configure the Wireless LAN Controller and LAPs

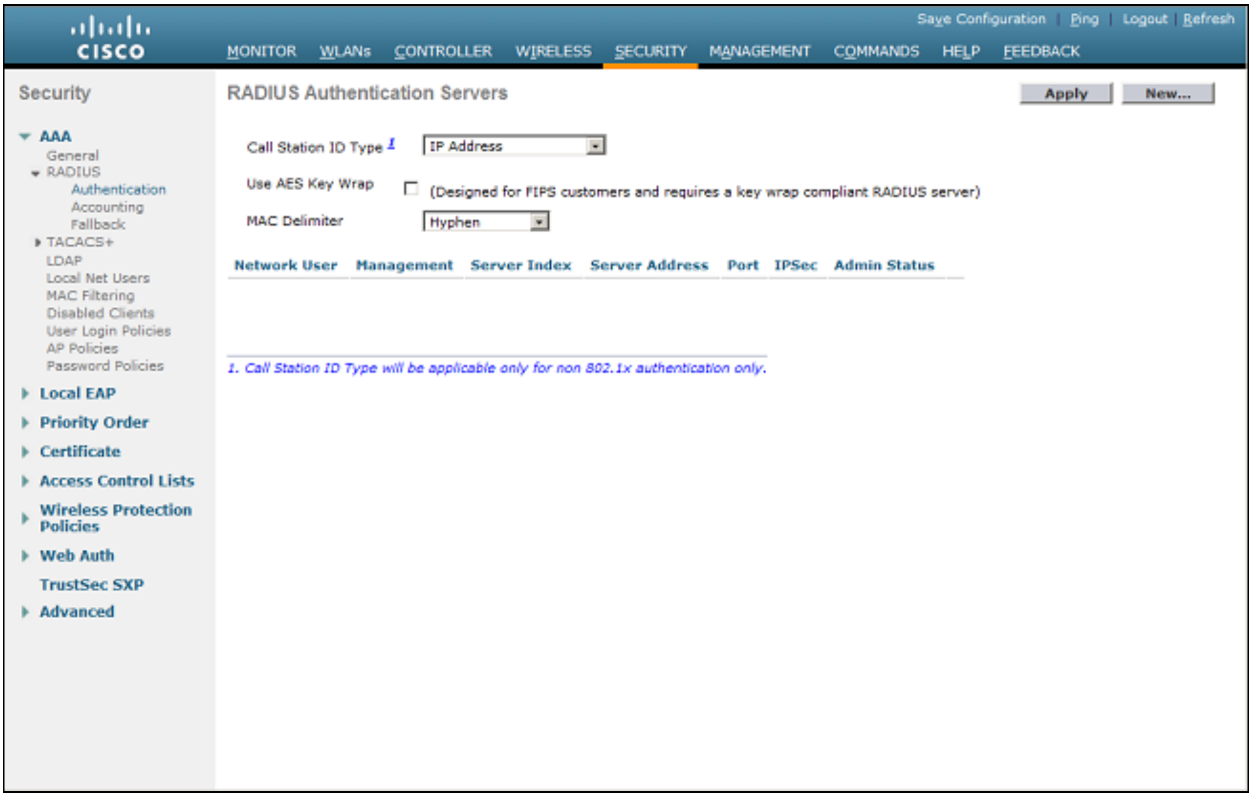
Configure the wireless devices (the Wireless LAN Controllers and LAPs) for this setup.

Configure the WLC for RADIUS Authentication

Configure the WLC to use the NPS as the authentication server. The WLC must be configured in order to forward the user credentials to an external RADIUS server. The external RADIUS server then validates the user credentials and provides access to the wireless clients.

Complete these steps in order to add the NPS as a RADIUS server in the ***Security*** > ***RADIUS Authentication*** page:

1. Choose ***Security*** > ***RADIUS*** > ***Authentication*** from the controller interface to display the RADIUS Authentication Servers page. Click ***New*** in order to define a RADIUS server.



RADIUS Authentication Servers

Call Station ID Type [1] IP Address

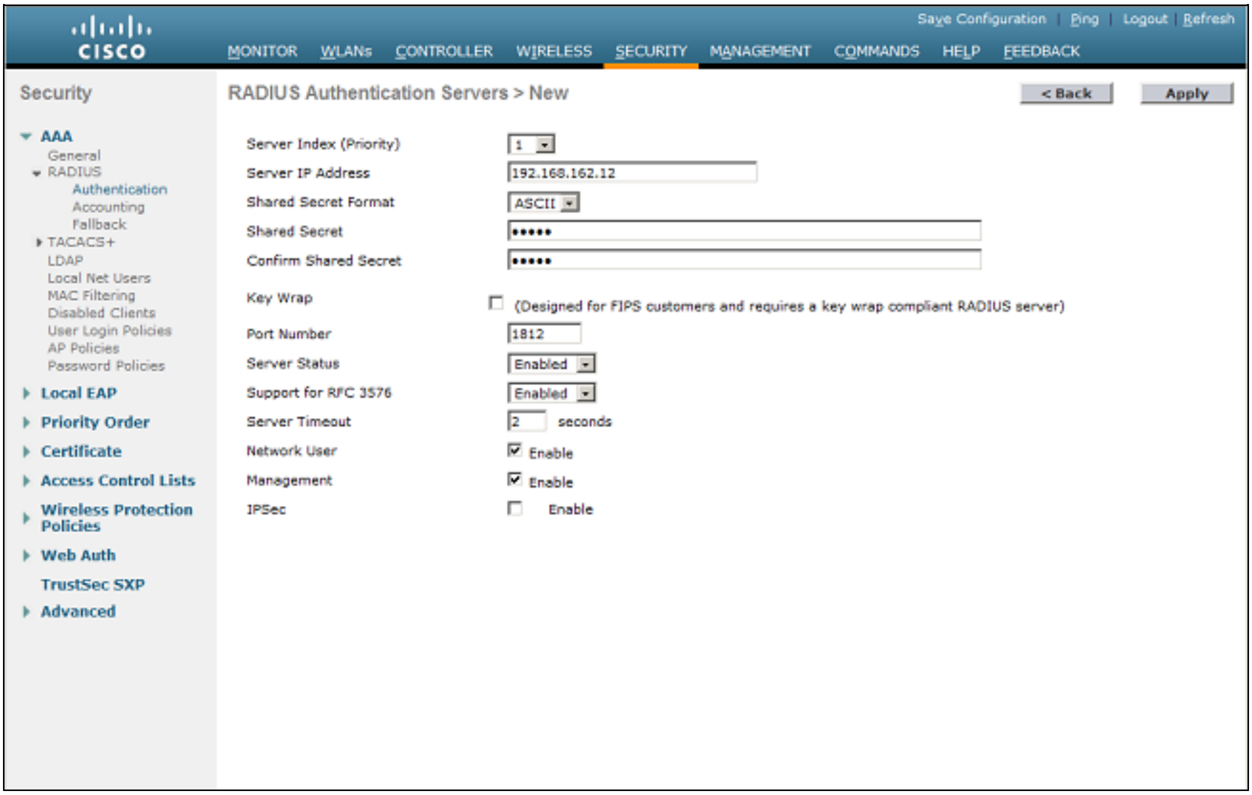
Use AES Key Wrap □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter Hyphen

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status

1. Call Station ID Type will be applicable only for non 802.1x authentication only.

2. Define the RADIUS server parameters. These parameters include the RADIUS Server IP Address, Shared Secret, Port Number, and Server Status. The Network User and Management check boxes determine if RADIUS−based authentication applies to management and network (wireless) users. This example uses the NPS as the RADIUS server with an IP address of 192.168.162.12. Click ***Apply***.



RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IP Address	192.168.162.12
Shared Secret Format	ASCII
Shared Secret	•••••
Confirm Shared Secret	•••••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
Management	☑ Enable
IPSec	□ Enable

Configure a WLAN for the Clients

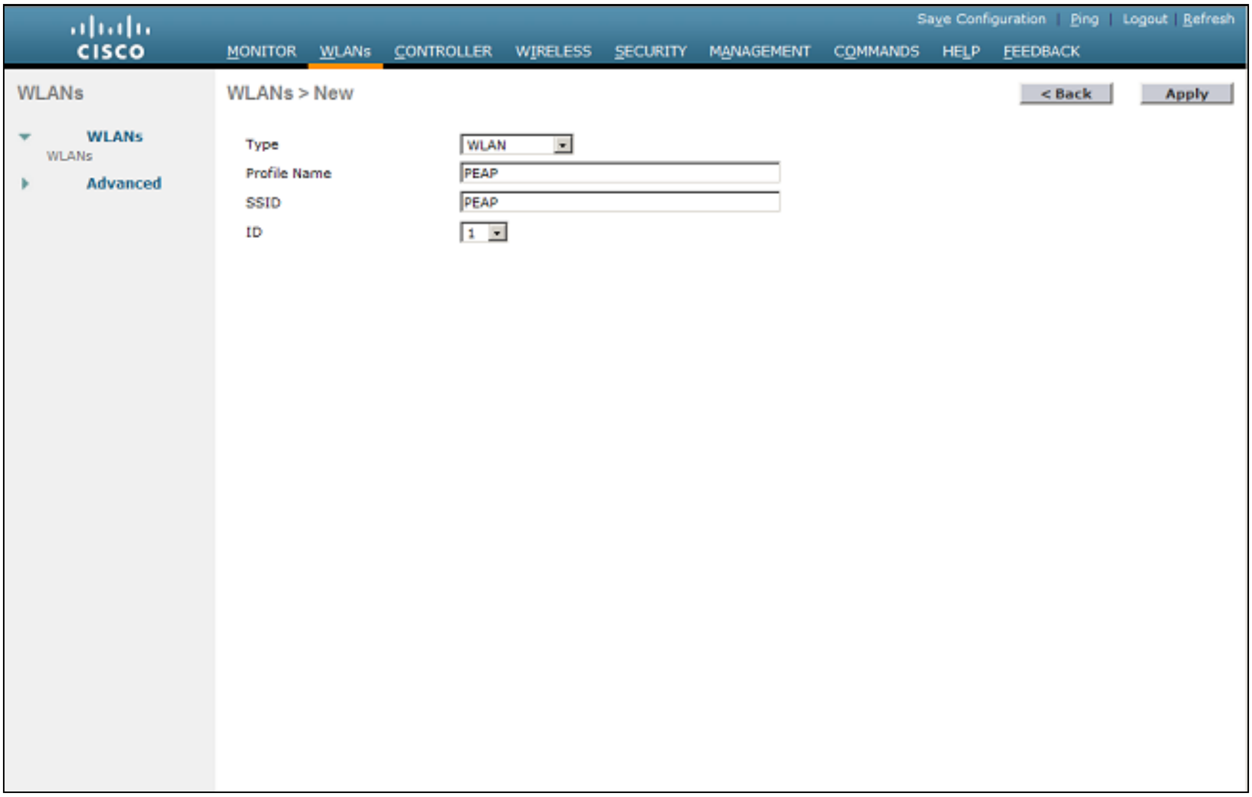
Configure the service set identfier (SSID) (WLAN) to which the wireless clients connects. In this example, create the SSID, and name it PEAP.

Define the Layer 2 Authentication as WPA2 so that the clients perform EAP−based authentication (PEAP−MS−CHAP v2 in this example) and use the advanced encryption standard (AES) as the encryption mechanism. Leave all other values at their defaults.

Note: This document binds the WLAN with the management interfaces. When you have multiple VLANs in your network, you can create a separate VLAN and bind it to the SSID. For information on how to configure VLANs on WLCs, refer to VLANs on Wireless LAN Controllers Configuration Example.

Complete these steps in order to configure a WLAN on the WLC:

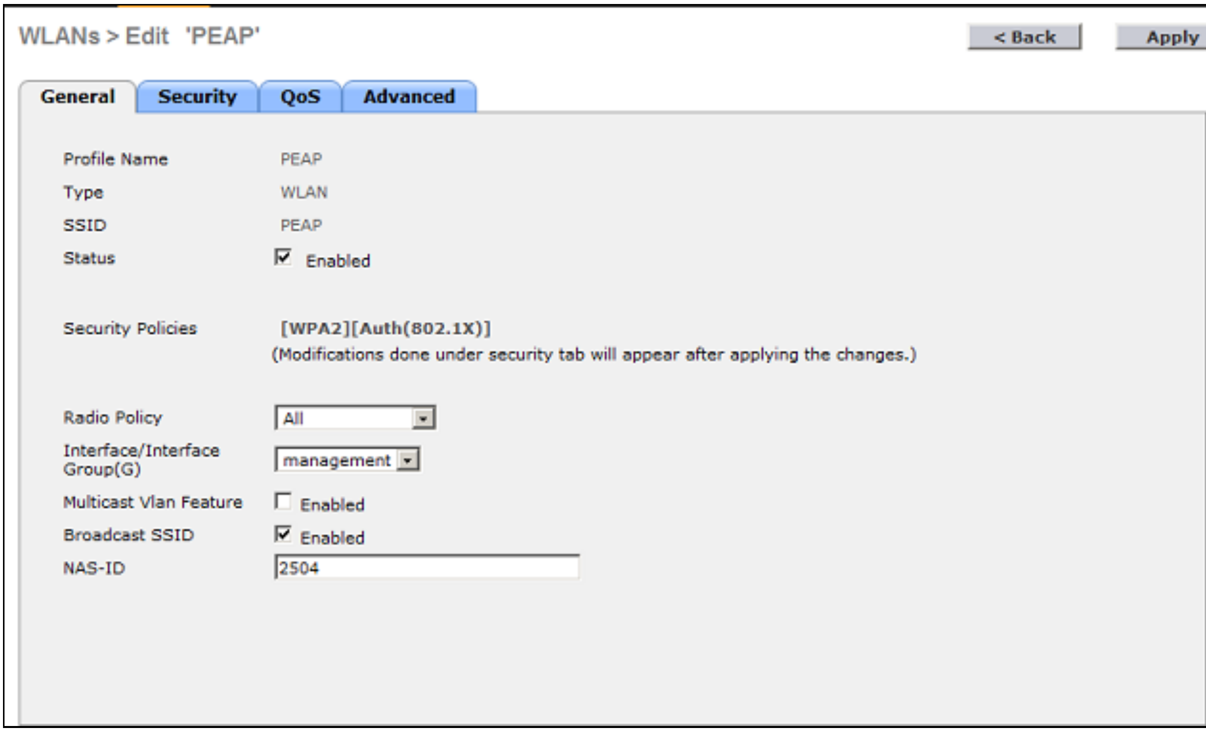
1. Click ***WLANs*** from the controller interface in order to display the WLANs page. This page lists the WLANs that exist on the controller.
2. Choose ***New*** in order to create a new WLAN. Enter the WLAN ID and the WLAN SSID for the WLAN, and click ***Apply***.


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply

WLANs > New

Type: WLAN
Profile Name: PEAP
SSID: PEAP
ID: 1

3. To configure the SSID for 802.1x, complete these steps:
    1. Click the ***General*** tab and enable the WLAN.



Profile Name PEAP

Type WLAN

SSID PEAP

Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

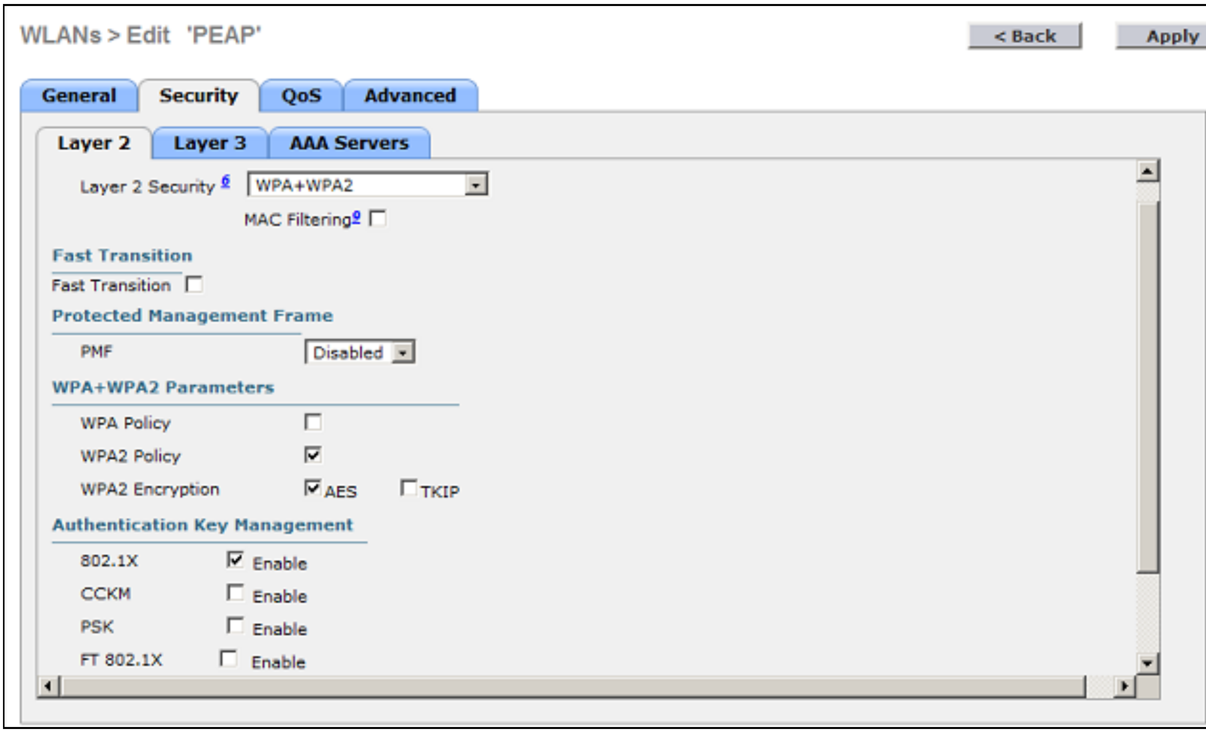
Interface/Interface Group(G) management

Multicast Vlan Feature ☐ Enabled

Broadcast SSID ☑ Enabled

NAS-ID 2504

2. Click the *Security* > *Layer 2* tabs, set Layer 2 security to ***WPA + WPA2***, check the WPA+WPA2 Parameters (for example, WPA2 AES) check boxesas needed, and click ***802.1x*** as the Authentication Key Management.



Layer 2 Security 6 WPA+WPA2

MAC Filtering9 ☐

Fast Transition

Fast Transition ☐

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☑

WPA2 Encryption ☑ AES ☐ TKIP

Authentication Key Management

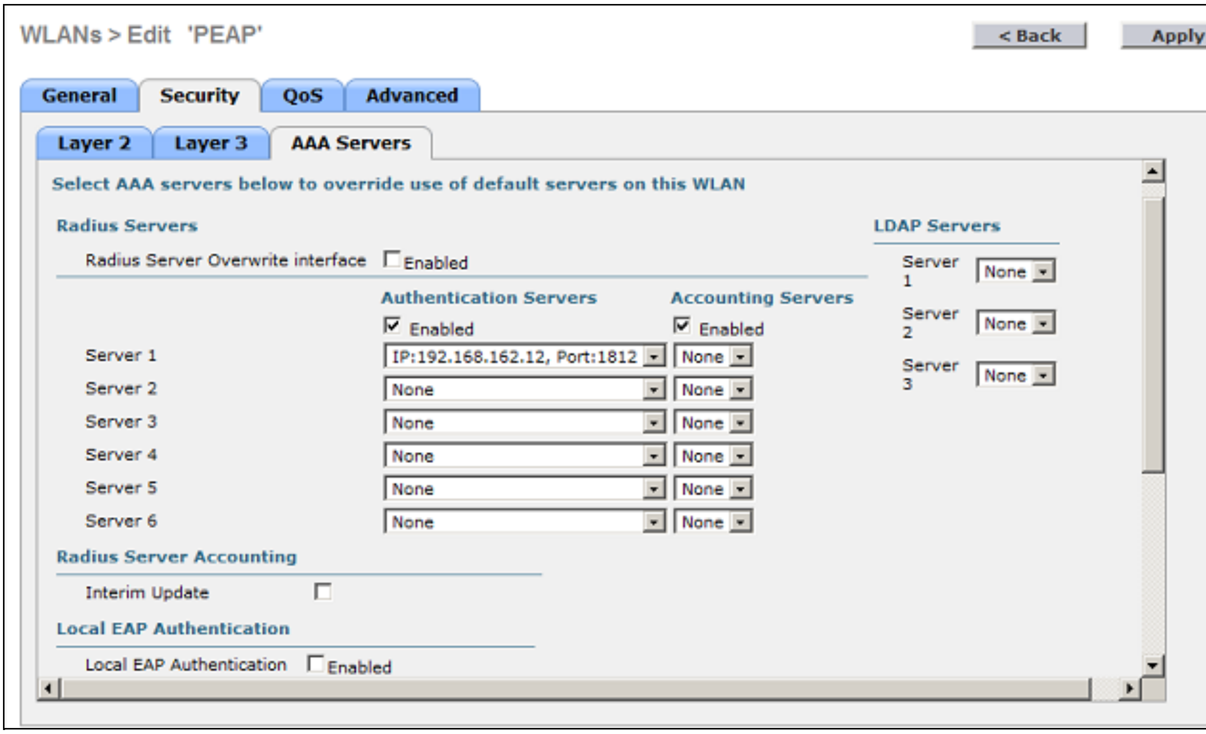
802.1X ☑ Enable

CCKM ☐ Enable

PSK ☐ Enable

FT 802.1X ☐ Enable

3. Click the ***Security*** > ***AAA Servers*** tabs, choose the IP address of the NPS from the ***Server 1*** drop−down list, and click ***Apply***.



WLANs > Edit 'PEAP'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:192.168.162.12, Port:1812	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

Radius Server Accounting

Interim Update □

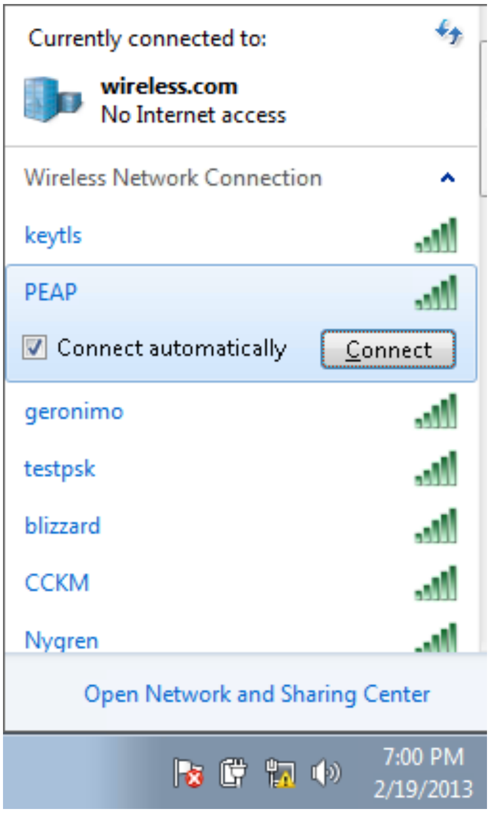
Local EAP Authentication

Local EAP Authentication □ Enabled

Configure the Wireless Clients for PEAP−MS−CHAP v2 Authentication

Complete these steps to configure the wireless client with the Windows Zero Config Tool to connect to the PEAP WLAN.

1. Click the ***Network*** icon in the task bar. Click the ***PEAP*** SSID, and click ***Connect***.



Currently connected to:

wireless.com
No Internet access

Wireless Network Connection

keytls

PEAP

☑ Connect automatically

geronimo

testpsk

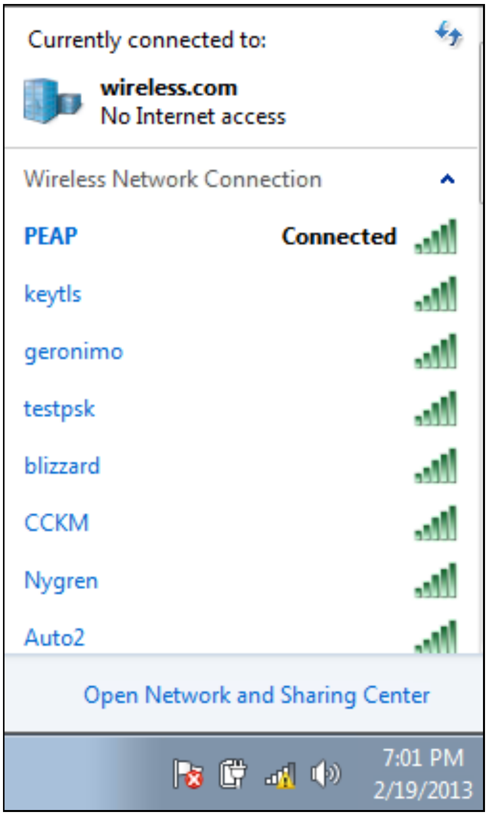
blizzard

CCKM

Nygren

7:00 PM
2/19/2013

2. The client should now be connected to the network.



Currently connected to:

wireless.com
No Internet access

Wireless Network Connection

PEAP **Connected**
keytls
geronimo
testpsk
blizzard
CCKM
Nygren
Auto2

Open Network and Sharing Center

7:01 PM
2/19/2013

3. If the connection fails, try to reconnect to the WLAN. If the issue persists, refer to the Troubleshoot section.

Verify

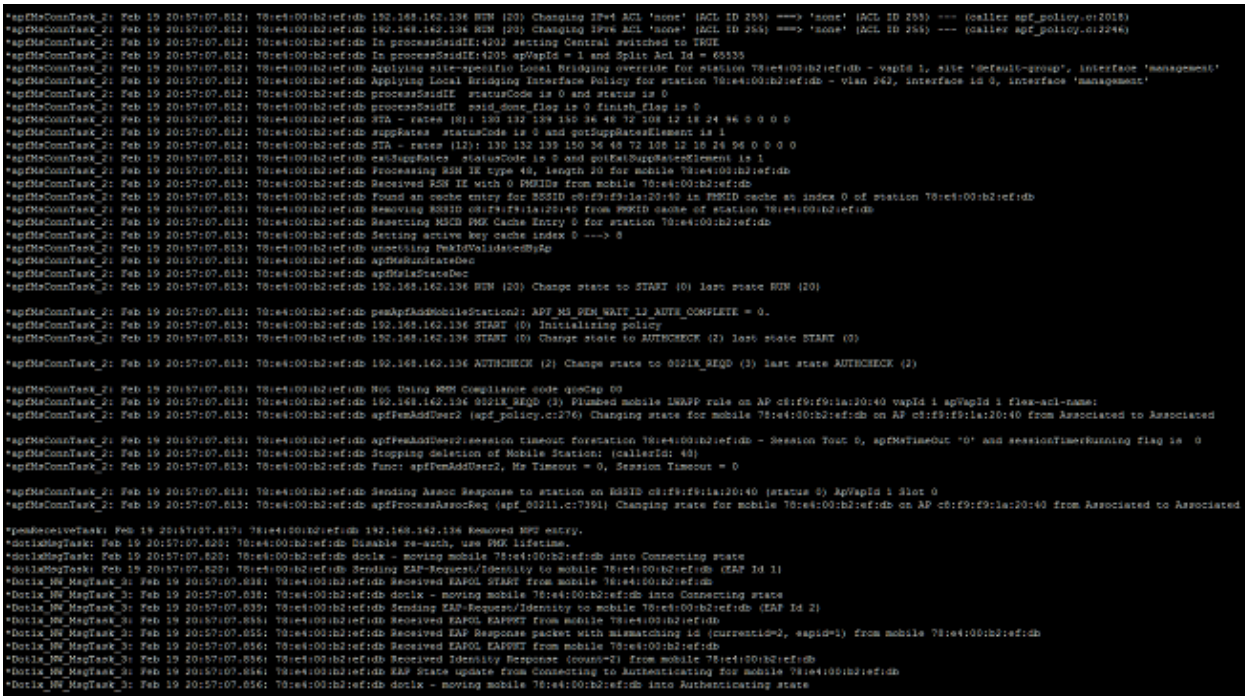
There is currently no verification procedure available for this configuration.

Troubleshoot

If your client did not connect to the WLAN, this section provides information you can use to troubleshoot the configuration.

There are two tools that can be used to diagnose 802.1x authentication failures: the ***debug client*** command and the ***Event Viewer*** in Windows.

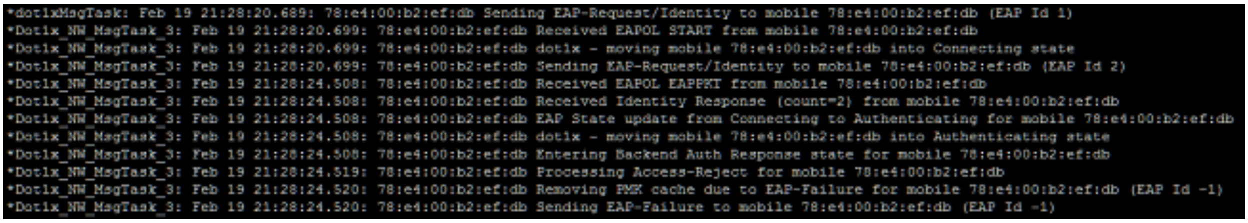
Performing a client debug from the WLC is not resource intensive and does not imnpact service. To start a debug session, open the command−line interface (CLI) of the WLC, and enter ***debug client*** *mac address*, where the mac address is the wireless mac address of the wireless client that is unable to connect. While this debug runs, try to connect the client; there should be output on the CLI of the WLC that looks similar to this example:



```
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db 192.168.162.136 RUN (20) Changing IPv4 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2018)
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db 192.168.162.136 RUN (20) Changing IPv6 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2246)
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db In processSsidIE:4202 setting Central switched to TRUE
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db In processSsidIE:4205 apVapId = 1 and Split Acl Id = 65535
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db Applying site-specific Local Bridging override for station 78:e4:00:b2:ef:db - vapId 1, site 'default-group', interface 'management'
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db Applying Local Bridging Interface Policy for station 78:e4:00:b2:ef:db - vlan 262, interface id 0, interface 'management'
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db processSsidIE  statusCode is 0 and status is 0
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db processSsidIE  ssid_done_flag is 0 finish_flag is 0
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db STA - rates (8): 130 132 139 150 36 48 72 108 12 18 24 96 0 0 0 0
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db suppRates  statusCode is 0 and gotSuppRatesElement is 1
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db STA - rates (12): 130 132 139 150 36 48 72 108 12 18 24 96 0 0 0 0
*apfMsConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db extSuppRates  statusCode is 0 and gotExtSuppRatesElement is 1
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Processing RSN IE type 48, length 20 for mobile 78:e4:00:b2:ef:db
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Received RSN IE with 0 PMKIDs from mobile 78:e4:00:b2:ef:db
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Found an cache entry for BSSID c8:f9:f9:1a:20:40 in PMKID cache at index 0 of station 78:e4:00:b2:ef:db
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Removing BSSID c8:f9:f9:1a:20:40 from PMKID cache of station 78:e4:00:b2:ef:db
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Resetting MSCB PMK Cache Entry 0 for station 78:e4:00:b2:ef:db
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Setting active key cache index 0 ---> 8
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db unsetting PmkIdValidatedByAp
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db apfMsRunStateDec
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db apfMs1xStateDec
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db 192.168.162.136 RUN (20) Change state to START (0) last state RUN (20)

*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db pemApfAddMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db 192.168.162.136 START (0) Initializing policy
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db 192.168.162.136 START (0) Change state to AUTHCHECK (2) last state START (0)

*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db 192.168.162.136 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db NoS Using WMM Compliance code qosCap 00
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db 192.168.162.136 8021X_REQD (3) Plumbed mobile LWAPP rule on AP c8:f9:f9:1a:20:40 vapId 1 apVapId 1 flex-acl-name:
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db apfPemAddUser2 (apf_policy.c:276) Changing state for mobile 78:e4:00:b2:ef:db on AP c8:f9:f9:1a:20:40 from Associated to Associated

*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db apfPemAddUser2:session timeout forstation 78:e4:00:b2:ef:db - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is  0
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Stopping deletion of Mobile Station: (callerId: 48)
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0

*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Sending Assoc Response to station on BSSID c8:f9:f9:1a:20:40 (status 0) ApVapId 1 Slot 0
*apfMsConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db apfProcessAssocReq (apf_80211.c:7391) Changing state for mobile 78:e4:00:b2:ef:db on AP c8:f9:f9:1a:20:40 from Associated to Associated

*pemReceiveTask: Feb 19 20:57:07.817: 78:e4:00:b2:ef:db 192.168.162.136 Removed NPU entry.
*dot1xMsgTask: Feb 19 20:57:07.820: 78:e4:00:b2:ef:db Disable re-auth, use PMK lifetime.
*dot1xMsgTask: Feb 19 20:57:07.820: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Connecting state
*dot1xMsgTask: Feb 19 20:57:07.820: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 1)
*Dot1x_NW_MsgTask_3: Feb 19 20:57:07.838: 78:e4:00:b2:ef:db Received EAPOL START from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 20:57:07.838: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Connecting state
*Dot1x_NW_MsgTask_3: Feb 19 20:57:07.839: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 2)
*Dot1x_NW_MsgTask_3: Feb 19 20:57:07.855: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 20:57:07.855: 78:e4:00:b2:ef:db Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 20:57:07.856: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 20:57:07.856: 78:e4:00:b2:ef:db Received Identity Response (count=2) from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 20:57:07.856: 78:e4:00:b2:ef:db EAP State update from Connecting to Authenticating for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 20:57:07.856: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Authenticating state
```

This is an example of an issue that could occur with a misconfiguration. Here, the WLC debug shows the WLC has moved into the authenticating state, which means the WLC is waiting for a response from the NPS. This is usually due to an incorrect shared secret on either the WLC or the NPS. You can confirm this via the Windows Server Event Viewer. If you do not find a log, the request never made it to the NPS.

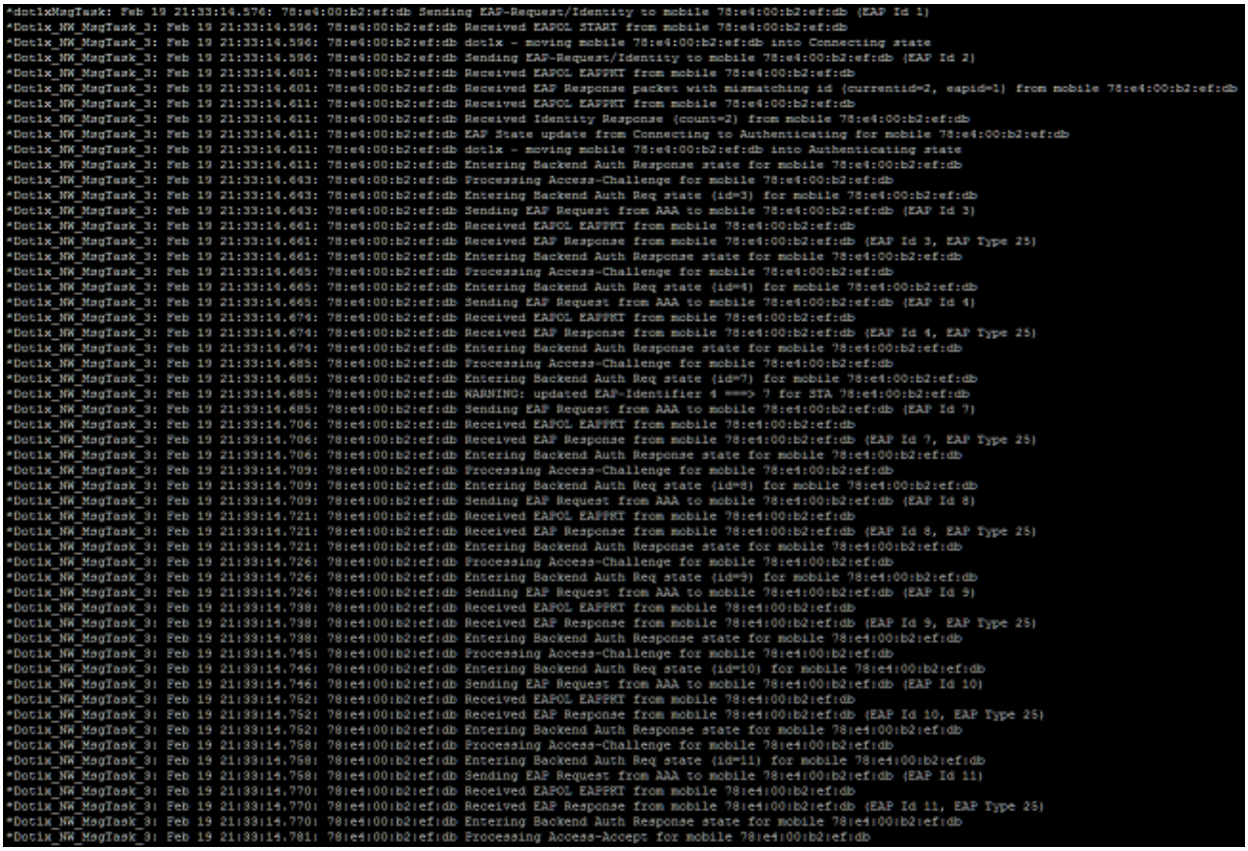
Another example that is found from the WLC debug is an access−reject. An access−reject shows that the NPS received and rejected the client credentials. This is an example of a client receiving an access−reject:



```
*dot1xMsgTask: Feb 19 21:28:20.689: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 1)
*Dot1x_NW_MsgTask_3: Feb 19 21:28:20.699: 78:e4:00:b2:ef:db Received EAPOL START from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:20.699: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Connecting state
*Dot1x_NW_MsgTask_3: Feb 19 21:28:20.699: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 2)
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.508: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.508: 78:e4:00:b2:ef:db Received Identity Response (count=2) from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.508: 78:e4:00:b2:ef:db EAP State update from Connecting to Authenticating for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.508: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Authenticating state
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.508: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.519: 78:e4:00:b2:ef:db Processing Access-Reject for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.520: 78:e4:00:b2:ef:db Removing PMK cache due to EAP-Failure for mobile 78:e4:00:b2:ef:db (EAP Id -1)
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.520: 78:e4:00:b2:ef:db Sending EAP-Failure to mobile 78:e4:00:b2:ef:db (EAP Id -1)
```

When you see an access−reject, check the logs on the Windows Server Event logs to determine why the NPS responded to the client with an access−reject.

A successful authentication has an access−accept in the client debug, as seen in this example:



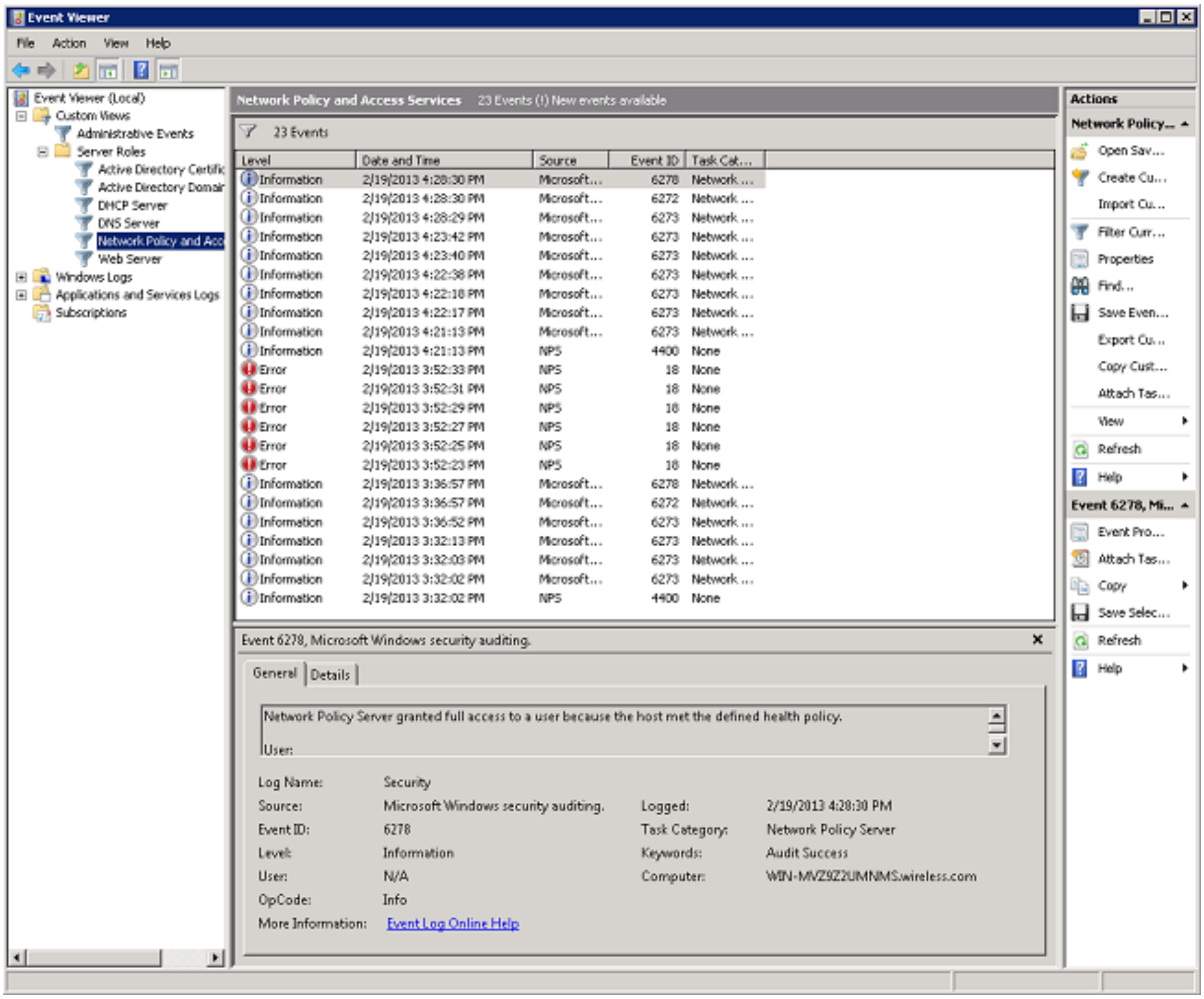
```
*dot1xMsgTask: Feb 19 21:33:14.576: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 1)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.596: 78:e4:00:b2:ef:db Received EAPOL START from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.596: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Connecting state
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.596: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 2)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.601: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.601: 78:e4:00:b2:ef:db Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Received Identity Response (count=2) from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db EAP State update from Connecting to Authenticating for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Authenticating state
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.643: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.643: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=3) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.643: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 3)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.661: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.661: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 3, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.661: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.665: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.665: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=4) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.665: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 4)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.674: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.674: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 4, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.674: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=7) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db WARNING: updated EAP-Identifier 4 ===> 7 for STA 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 7)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.706: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.706: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 7, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.706: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.709: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.709: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=8) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.709: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 8)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.721: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.721: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 8, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.721: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.726: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.726: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=9) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.726: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 9)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.738: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.738: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 9, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.738: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.745: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.746: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=10) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.746: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 10)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.752: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.752: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 10, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.752: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.758: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.758: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=11) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.758: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 11)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.770: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.770: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 11, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.770: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.781: 78:e4:00:b2:ef:db Processing Access-Accept for mobile 78:e4:00:b2:ef:db
```

Troubleshooting access−rejects and response timeouts requires access to the RADIUS server. The WLC acts as an authenticator that passes EAP messages between the client and the RADIUS server. A RADIUS server responding with an access−reject or response timeout should be examined and diagnosed by the manufacturer of the RADIUS service.

Note: TAC does not provide technical support for third−party RADIUS servers; however, the logs on the RADIUS server generally explain why a client request was rejected or ignored.

In order to troubleshoot access−rejects and response timeouts from the NPS, examine the NPS logs in the Windows Event Viewer on the server.

1. Click ***Start*** > ***Administrator Tools*** > ***Event Viewer*** to start the Event Viewer and review the NPS logs.
2. Expand ***Custom Views*** > ***Server Roles*** > ***Network Policy and Access***.



Network Policy and Access Services 23 Events (!) New events available

23 Events

Level	Date and Time	Source	Event ID	Task Cat...
Information	2/19/2013 4:28:30 PM	Microsoft...	6278	Network ...
Information	2/19/2013 4:28:30 PM	Microsoft...	6272	Network ...
Information	2/19/2013 4:28:29 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:23:42 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:23:40 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:38 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:18 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:17 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:21:13 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:21:13 PM	NPS	4400	None
Error	2/19/2013 3:52:33 PM	NPS	18	None
Error	2/19/2013 3:52:31 PM	NPS	18	None
Error	2/19/2013 3:52:29 PM	NPS	18	None
Error	2/19/2013 3:52:27 PM	NPS	18	None
Error	2/19/2013 3:52:25 PM	NPS	18	None
Error	2/19/2013 3:52:23 PM	NPS	18	None
Information	2/19/2013 3:36:57 PM	Microsoft...	6278	Network ...
Information	2/19/2013 3:36:57 PM	Microsoft...	6272	Network ...
Information	2/19/2013 3:36:52 PM	Microsoft...	6273	Network ...
Information	2/19/2013 3:32:13 PM	Microsoft...	6273	Network ...
Information	2/19/2013 3:32:03 PM	Microsoft...	6273	Network ...
Information	2/19/2013 3:32:02 PM	Microsoft...	6273	Network ...
Information	2/19/2013 3:32:02 PM	NPS	4400	None

Event 6278, Microsoft Windows security auditing.

General | Details

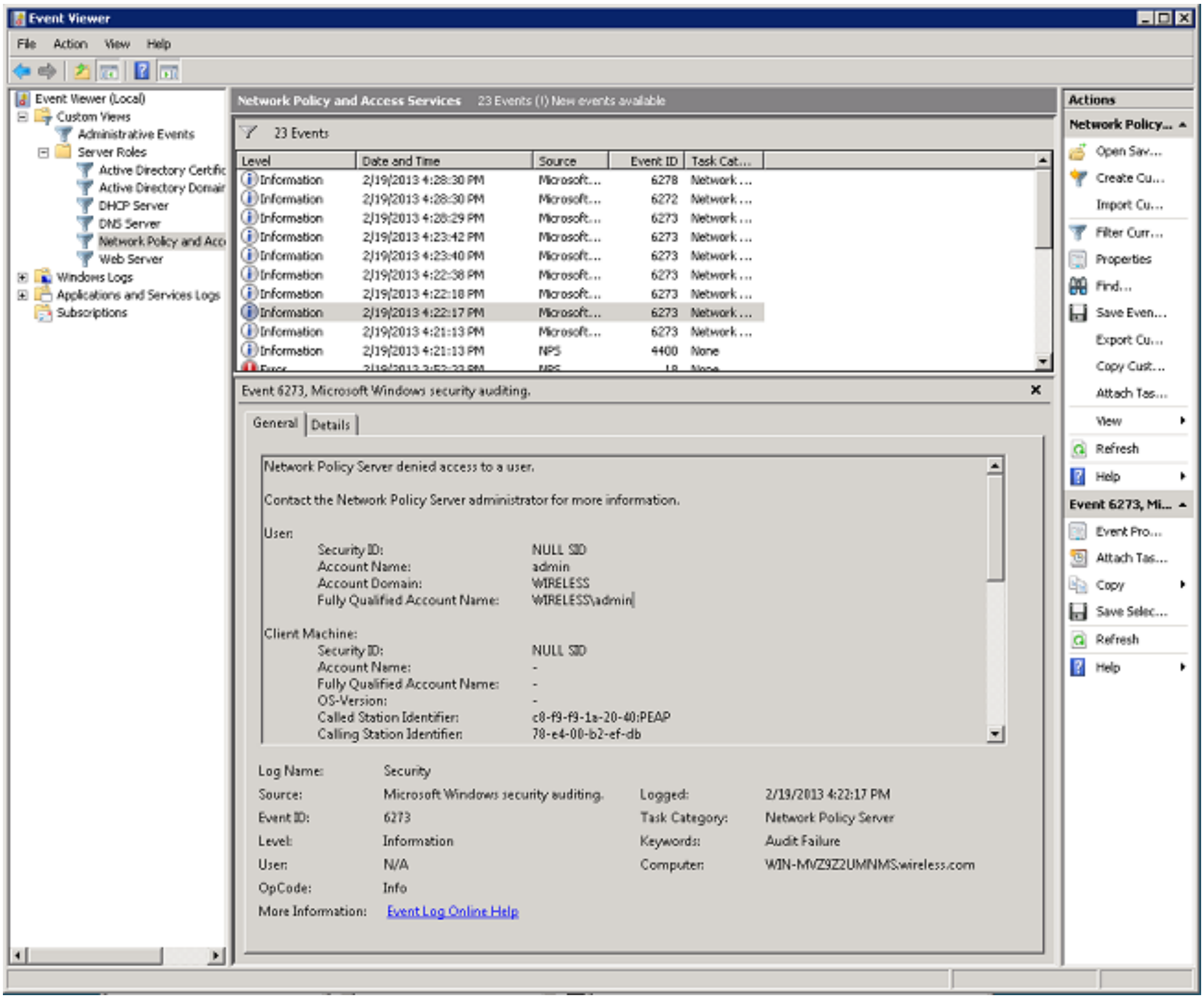
Network Policy Server granted full access to a user because the host met the defined health policy.

User:

Log Name:	Security		
Source:	Microsoft Windows security auditing.	Logged:	2/19/2013 4:28:30 PM
Event ID:	6278	Task Category:	Network Policy Server
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-MVZ9Z2UMNMS.wireless.com
OpCode:	Info		
More Information:	Event Log Online Help		

In this section of the Event View, there are logs of passed and failed authentications. Examine these logs to troubleshoot why a client is not passing authentication. Both passed and failed authentications show up as Informational. Scroll through the logs to find the username that has failed authentication and received an access−reject according to the WLC debugs.

This is an example of the NPS denying a user access:



Network Policy and Access Services 23 Events (!) New events available

23 Events

Level	Date and Time	Source	Event ID	Task Cat...
Information	2/19/2013 4:28:30 PM	Microsoft...	6278	Network ...
Information	2/19/2013 4:28:30 PM	Microsoft...	6272	Network ...
Information	2/19/2013 4:28:29 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:23:42 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:23:40 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:38 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:18 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:17 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:21:13 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:21:13 PM	NPS	4400	None
Error	2/19/2013 3:52:23 PM	NPS	18	None

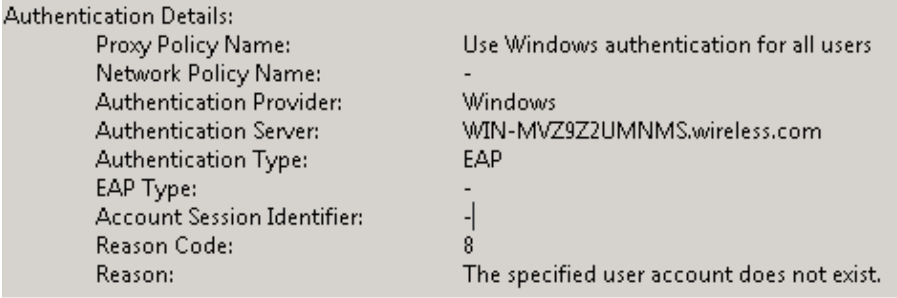
Event 6273, Microsoft Windows security auditing.

General | Details

```
Network Policy Server denied access to a user.

Contact the Network Policy Server administrator for more information.

User:
        Security ID:                    NULL SID
        Account Name:                   admin
        Account Domain:                 WIRELESS
        Fully Qualified Account Name:   WIRELESS\admin

Client Machine:
        Security ID:                    NULL SID
        Account Name:                   -
        Fully Qualified Account Name:   -
        OS-Version:                     -
        Called Station Identifier:      c8-f9-f9-1a-20-40:PEAP
        Calling Station Identifier:     78-e4-00-b2-ef-db
```

Log Name:	Security		
Source:	Microsoft Windows security auditing.	Logged:	2/19/2013 4:22:17 PM
Event ID:	6273	Task Category:	Network Policy Server
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	WIN-MVZ9Z2UMNMS.wireless.com
OpCode:	Info		
More Information:	Event Log Online Help		

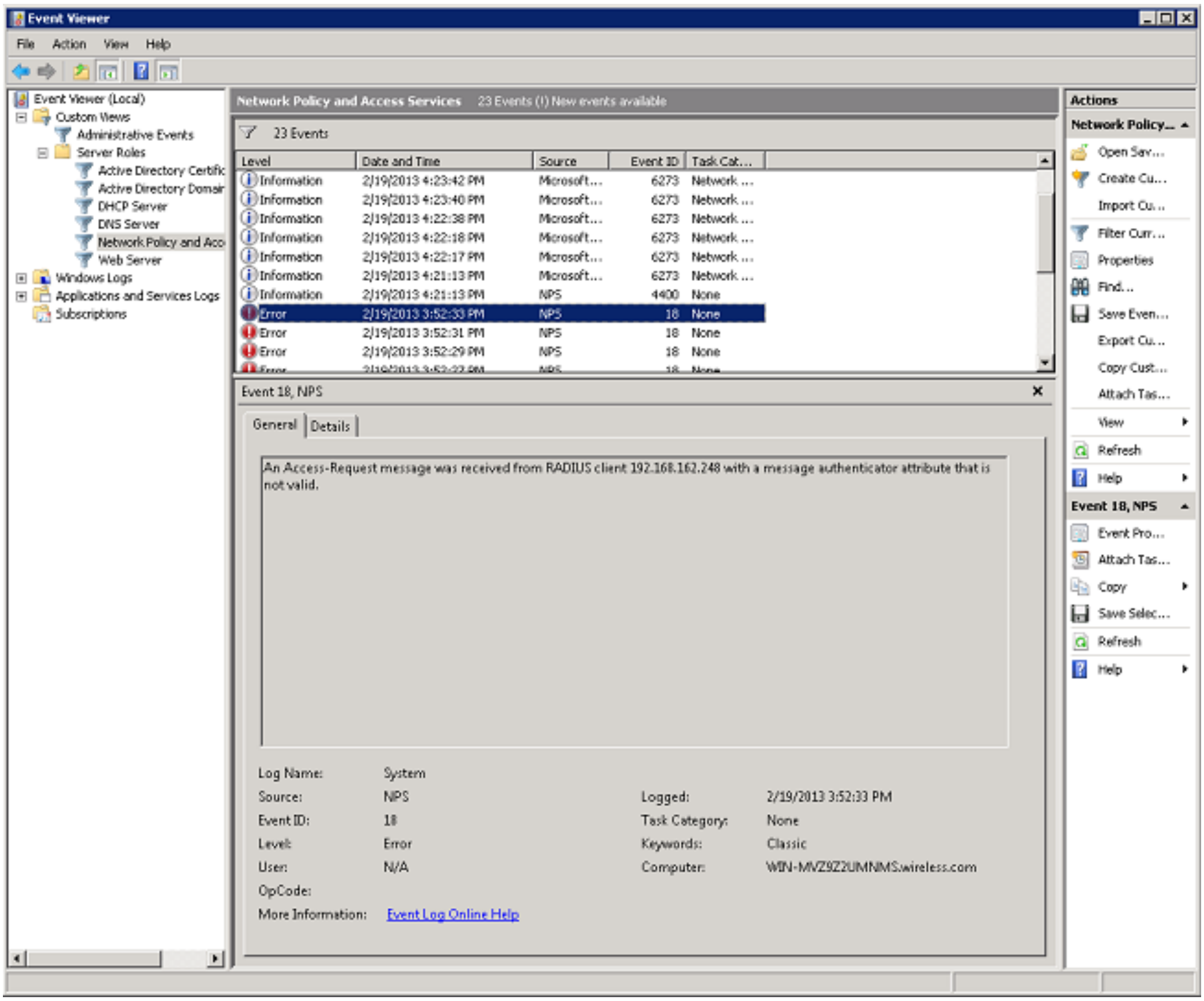
When reviewing a deny statement in the Event Viewer, examine the Authentication Details section. In this example, you can see that the NPS denied the user access due to an incorrect username:



```
Authentication Details:
        Proxy Policy Name:              Use Windows authentication for all users
        Network Policy Name:            -
        Authentication Provider:        Windows
        Authentication Server:          WIN-MVZ9Z2UMNMS.wireless.com
        Authentication Type:            EAP
        EAP Type:                       -
        Account Session Identifier:     -
        Reason Code:                    8
        Reason:                         The specified user account does not exist.
```

The Event View on the NPS also assists with troubleshooting if the WLC does not receive a response back from the NPS. This is usually caused by an incorrect shared secret between the NPS and the WLC.

In this example, the NPS discards the request from the WLC due to an incorrect shared secret:



Network Policy and Access Services 23 Events (!) New events available

23 Events

Level	Date and Time	Source	Event ID	Task Cat...
Information	2/19/2013 4:23:42 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:23:40 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:38 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:18 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:17 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:21:13 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:21:13 PM	NPS	4400	None
Error	2/19/2013 3:52:33 PM	NPS	18	None
Error	2/19/2013 3:52:31 PM	NPS	18	None
Error	2/19/2013 3:52:29 PM	NPS	18	None
Error	2/19/2013 3:52:27 PM	NPS	18	None

Event 18, NPS

An Access-Request message was received from RADIUS client 192.168.162.248 with a message authenticator attribute that is not valid.

Log Name: System
Source: NPS
Logged: 2/19/2013 3:52:33 PM
Event ID: 18
Task Category: None
Level: Error
Keywords: Classic
User: N/A
Computer: WIN-MVZ9Z2UMNMS.wireless.com
OpCode:
More Information: Event Log Online Help

Related Information

- ***Technical Support & Documentation − Cisco Systems***