使用Microsoft NPS的5760/3850系列WLC PEAP身份驗證配置示例

目錄

簡介

本檔案介紹如何在以Microsoft網路原則伺服器(NPS)作為RADIUS伺服器的思科融合存取無線LAN(WLAN)部署上，使用Microsoft詢問握手驗證通訊協定版本2(MS-CHAP v2)驗證設定受保護的可擴充驗證通訊協定(PEAP)。

必要條件

需求

思科建議您在嘗試本檔案所述的設定之前，先瞭解以下主題：

- Microsoft Windows 2008版基本安裝
- Cisco融合接入WLAN控制器安裝

嘗試此組態之前，請確保符合以下要求：

- 在測試實驗室中的每台伺服器上安裝Microsoft Windows Server 2008版作業系統(OS)。
- 更新所有Service Pack。
- 安裝控制器和輕量型存取點(LAP)。
- 配置最新的軟體更新。

> **附註**：有關Cisco融合接入WLAN控制器的初始安裝和配置資訊，請參閱[CT5760控制器和Catalyst 3850交換機配置示例]Cisco文章。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5760系列WLAN控制器版本3.3.2(下一代配線間(NGWC))
- Cisco 3602系列LAP
- Microsoft Windows XP與英特爾PROset請求方
- 運行具有域控制器角色的NPS的Microsoft Windows版本2008伺服器
- Cisco Catalyst 3560系列交換器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

PEAP使用傳輸級安全(TLS)在身份驗證PEAP客戶端（例如無線筆記型電腦）和PEAP身份驗證器（例如Microsoft NPS或任何RADIUS伺服器）之間建立加密通道。PEAP不指定身份驗證方法，但為其他可擴展身份驗證協定(EAP)提供額外的安全性，例如EAP-MS-CHAP v2，這些協定可以通過PEAP提供的TLS加密通道運行。PEAP身份驗證過程包括兩個主要階段。

PEAP第一階段：TLS加密通道

無線客戶端與接入點(AP)關聯。 基於IEEE 802.11的關聯在客戶端和AP之間建立安全關聯之前提供開放系統或共用金鑰身份驗證。在客戶端和AP之間成功建立基於IEEE 802.11的關聯後，與AP協商TLS會話。

在無線客戶端和NPS之間的身份驗證成功完成後，客戶端和NPS之間會協商TLS會話。在此交涉中匯出的金鑰用於加密所有後續通訊。

PEAP第二階段：EAP驗證通訊

EAP通訊（包括EAP協商）在PEAP身份驗證過程的第一階段內由PEAP建立的TLS通道內發生。NPS使用EAP-MS-CHAP v2對無線客戶端進行身份驗證。LAP和控制器僅在無線客戶端和RADIUS伺服器之間轉發消息。WLAN控制器(WLC)和LAP無法解密消息，因為WLC不是TLS端點。

以下是成功驗證嘗試的RADIUS訊息序列，其中使用者提供具有PEAP-MS-CHAP v2的有效密碼型憑證：

1. NPS向客戶端傳送身份請求消息：

   ```
   EAP-Request/Identity
   ```
2. 客戶端以身份響應消息進行響應：

   ```
   EAP-Response/Identity
   ```
3. NPS傳送MS-CHAP v2質詢消息：

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

4. 客戶端使用MS-CHAP v2質詢和響應進行響應：

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

5. 當伺服器成功驗證客戶端時，NPS將使用MS-CHAP v2成功資料包進行響應：

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

6. 當客戶端成功驗證伺服器時，客戶端會使用MS-CHAP v2成功資料包進行響應：

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

7. NPS傳送一個EAP型別長度值(TLV)，表示身份驗證成功。

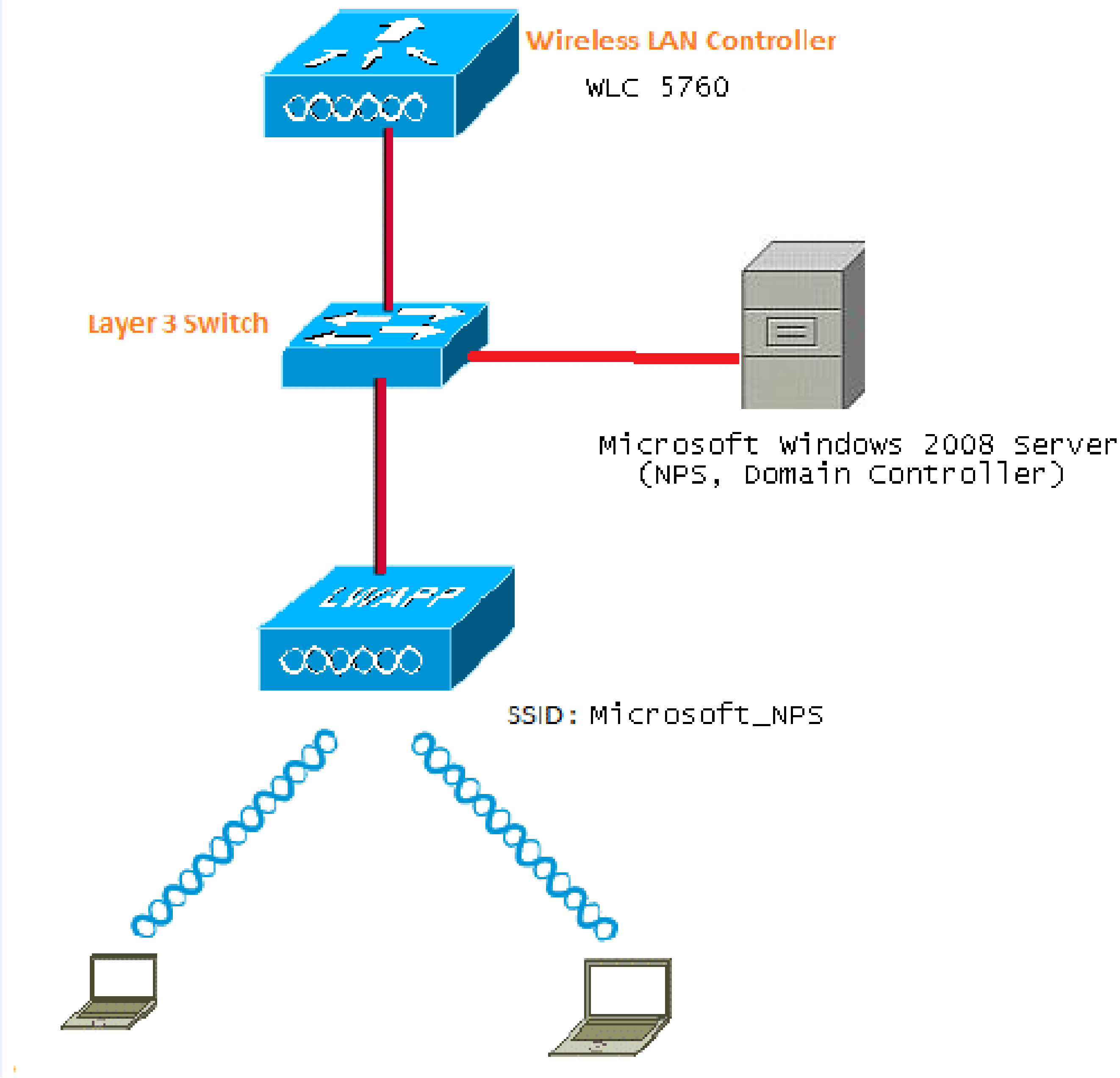
8. 客戶端以EAP-TLV狀態成功消息進行響應。

9. 伺服器完成身份驗證並以純文字檔案形式傳送EAP-Success消息。如果為客戶端隔離部署了VLAN，則此消息中會包含VLAN屬性。

設定

使用本節內容，可以在以Microsoft NPS作為RADIUS伺服器的思科融合接入WLC部署上使用MS-CHAP v2身份驗證配置PEAP。

網路圖表



在本示例中，Microsoft Windows Version 2008伺服器執行以下角色：

- **wireless**.com域**的域控制**器
- 網域名稱系統(DNS)伺服器
- 證書頒發機構(CA)伺服器
- NPS，用於對無線使用者進行身份驗證
- Active Directory(AD)以維護使用者資料庫

伺服器透過第2層(L2)交換器連線到有線網路，如圖所示。WLC和註冊的LAP也透過L2交換器連線到網路。

無線客戶端使用Wi-Fi保護訪問2(WPA2)- PEAP-MS-CHAP v2身份驗證連線到無線網路。

組態

本節所述的設定可通過兩個步驟完成：

1. 使用CLI或GUI設定5760/3850系列WLC。

2. 為AD上的NPS、域控制器和使用者帳戶配置Microsoft Windows Version 2008伺服器。

使用CLI配置融合接入WLC

完成以下步驟，為所需的使用者端VLAN設定WLAN，並使用CLI將其對應到驗證方法清單：

> **附註**：確保WLC上啟用了**dot1x system auth control**，否則dot1X無法正常工作。

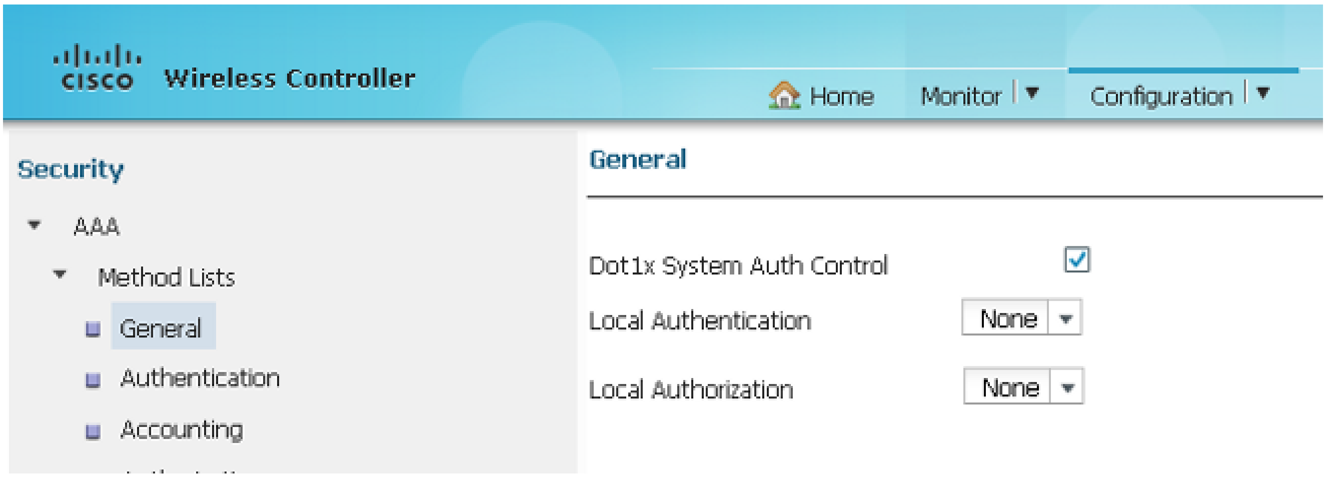
1. 啟用AAA**新模型功**能。
2. 設定RADIUS伺服器。
3. 將伺服器新增到伺服器組。
4. 將伺服器組對映到方法清單。
5. 將方法清單對映到WLAN。

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

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

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

使用GUI配置融合接入WLC

完成以下步驟，以便使用GUI設定融合存取WLC:

1. 啟用**dot1x system-auth-control**:



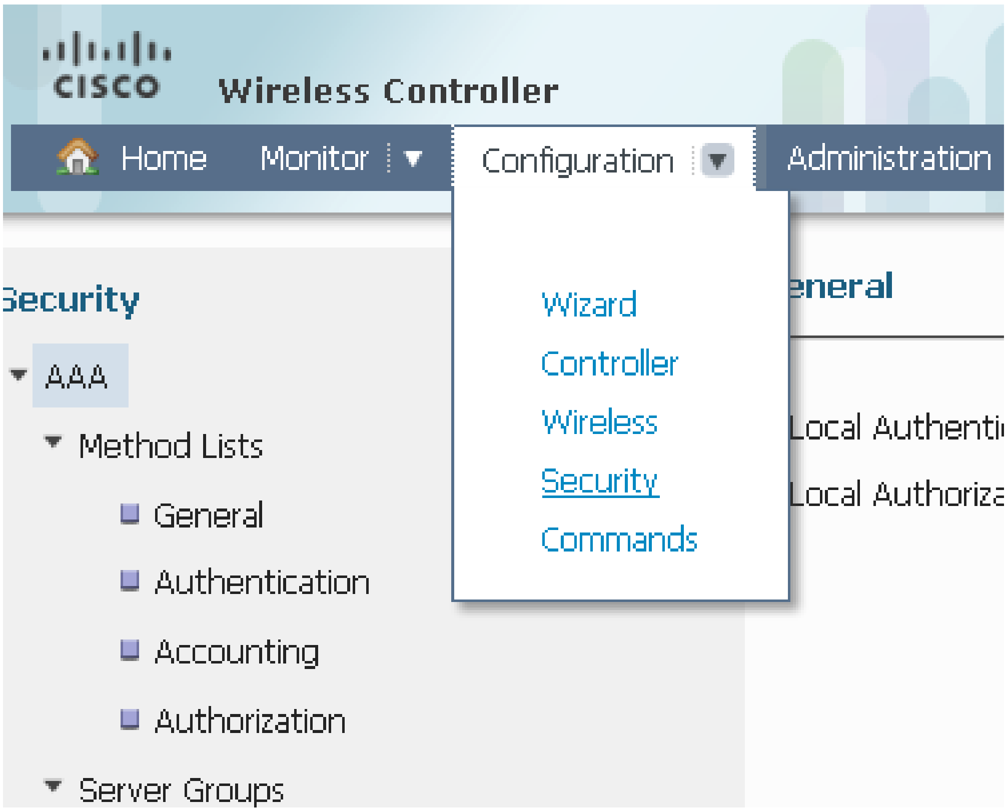
General

Dot1x System Auth Control ☑

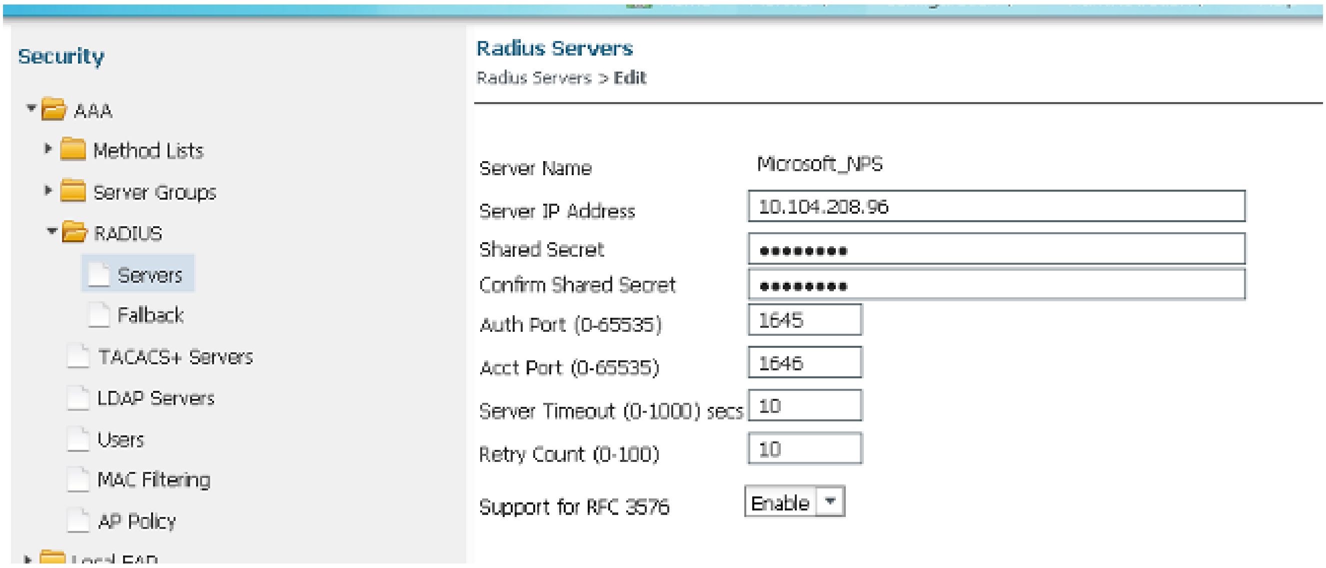
Local Authentication None

Local Authorization None

2. 導覽至**Configuration** > **Security** > **AAA**以新增RADIUS伺服器：



3. 導覽至**RADIUS > Servers**，按一下**NEW**，然後更新RADIUS伺服器的IP位址以及共用密碼。共用金鑰應該與RADIUS伺服器上設定的共用金鑰相符。

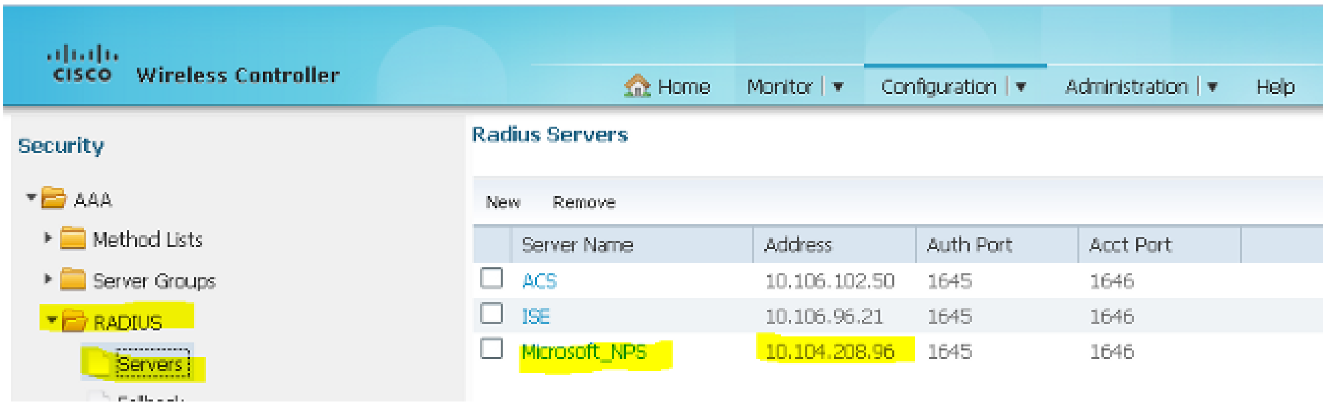


Radius Servers

Radius Servers > Edit

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

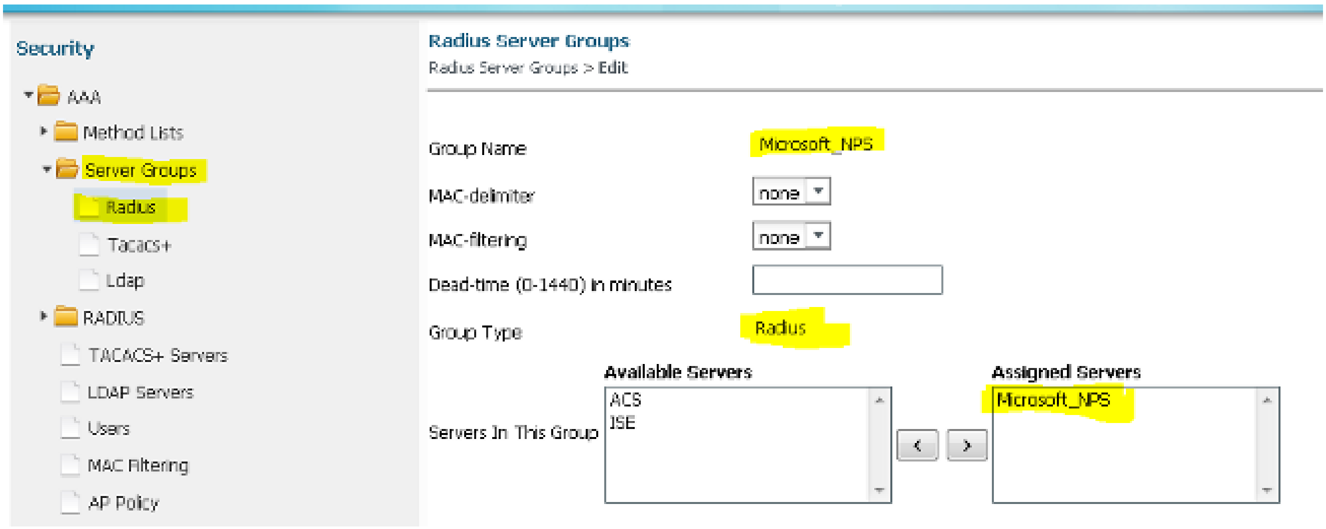
設定RADIUS伺服器後，「伺服器」索引標籤應顯示類似以下內容：



Radius Servers

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

4. 配置伺服器組，並為組型別選擇**Radius**。然後，新增在上一步中建立的RADIUS伺服器：



Radius Server Groups

Radius Server Groups > Edit

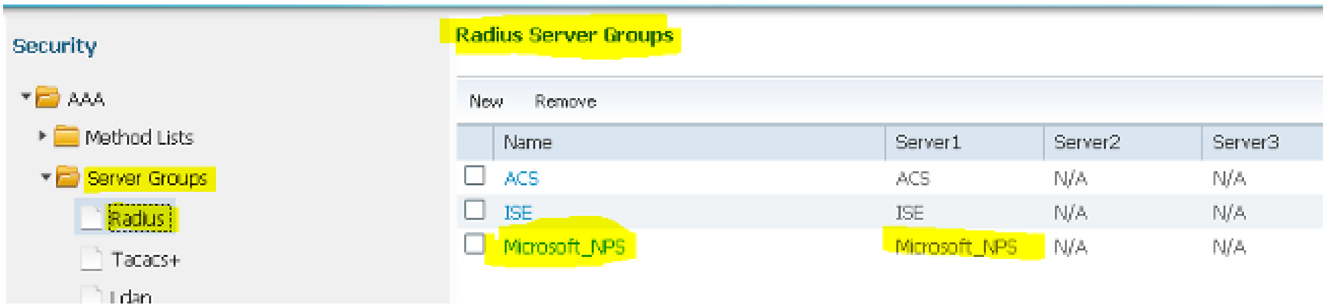
Group Name	Microsoft_NPS
MAC-delimiter	none
MAC-filtering	none
Dead-time (0-1440) in minutes	
Group Type	Radius

Servers In This Group

Available Servers: ACS, ISE

Assigned Servers: Microsoft_NPS

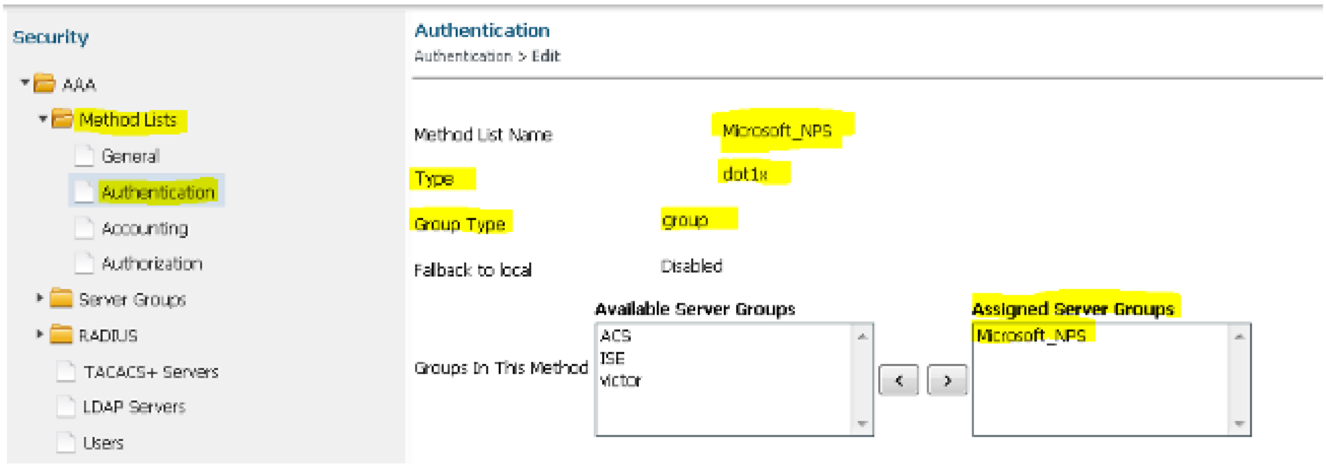
配置後，伺服器組應顯示類似以下內容：



Radius Server Groups

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

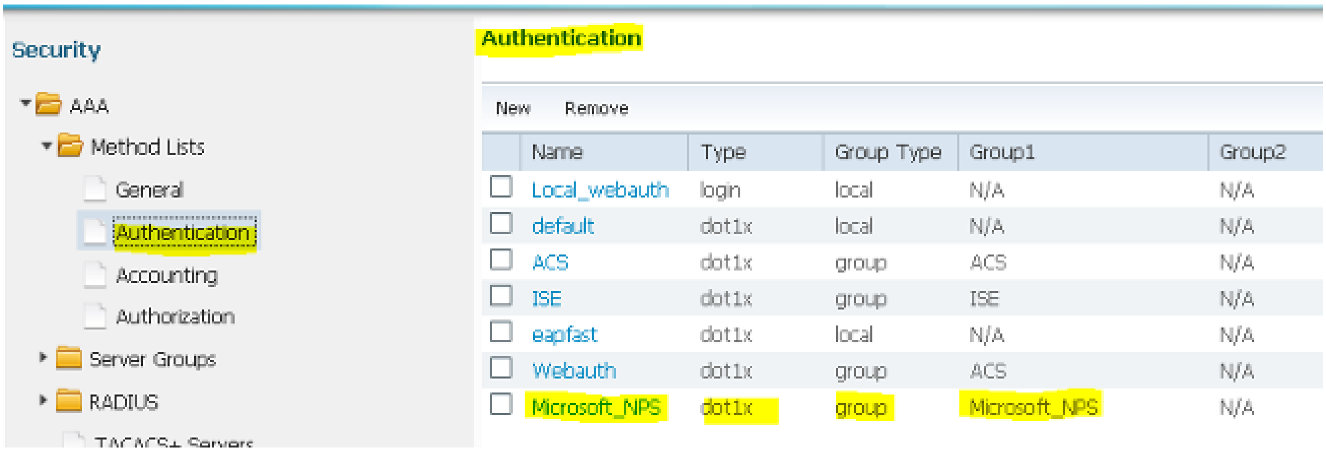
5. 選擇**dot1x**作為Authentication Method List Type和**Group**作為Group Type。然後，對映在上一步中配置的伺服器組：



Authentication
Authentication > Edit

Method List Name: Microsoft_NPS
Type: dot1x
Group Type: group
Fallback to local: Disabled
Groups In This Method:
Available Server Groups: ACS, ISE, Victor
Assigned Server Groups: Microsoft_NPS

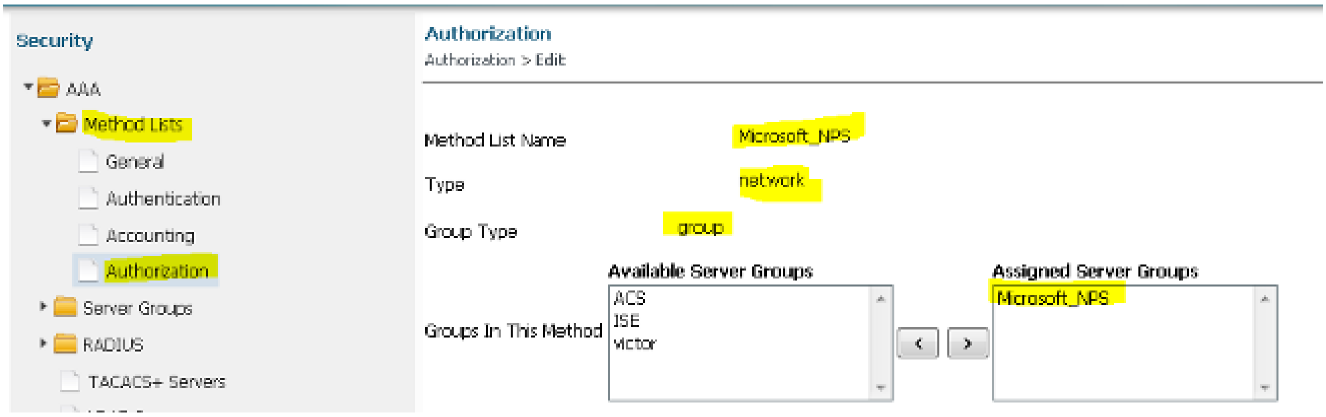
配置後，身份驗證方法清單應顯示類似以下內容：



Authentication

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

6. 選擇**Network**作為Authorization Method List Type和**Group**作為Group Type。然後，對映在上一步中配置的伺服器組：



Authorization
Authorization > Edit

Method List Name: Microsoft_NPS

Type: network

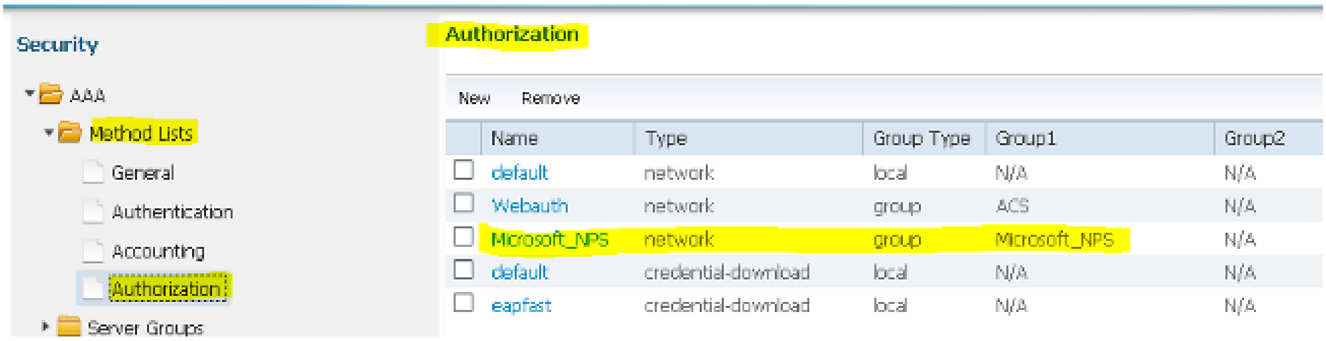
Group Type: group

Groups In This Method

Available Server Groups: ACS, ISE, Victor

Assigned Server Groups: Microsoft_NPS

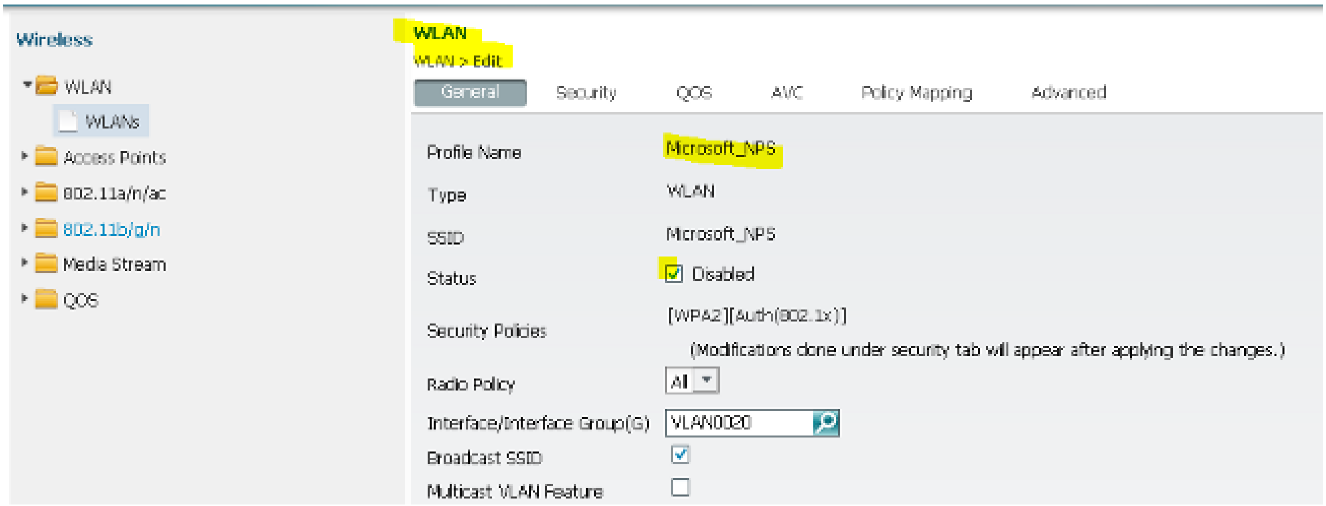
配置後，授權方法清單應顯示類似以下內容：



Authorization

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

7. 導覽至**Configure > Wireless**，然後按一下**WLAN**索引標籤。配置一個新的WLAN，使用者可以連線到該WLAN並通過採用EAP身份驗證的Microsoft NPS伺服器進行身份驗證：



WLAN
WLAN > Edit

Profile Name: Microsoft_NPS

Type: WLAN

SSID: Microsoft_NPS

Status: ☑ Disabled

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

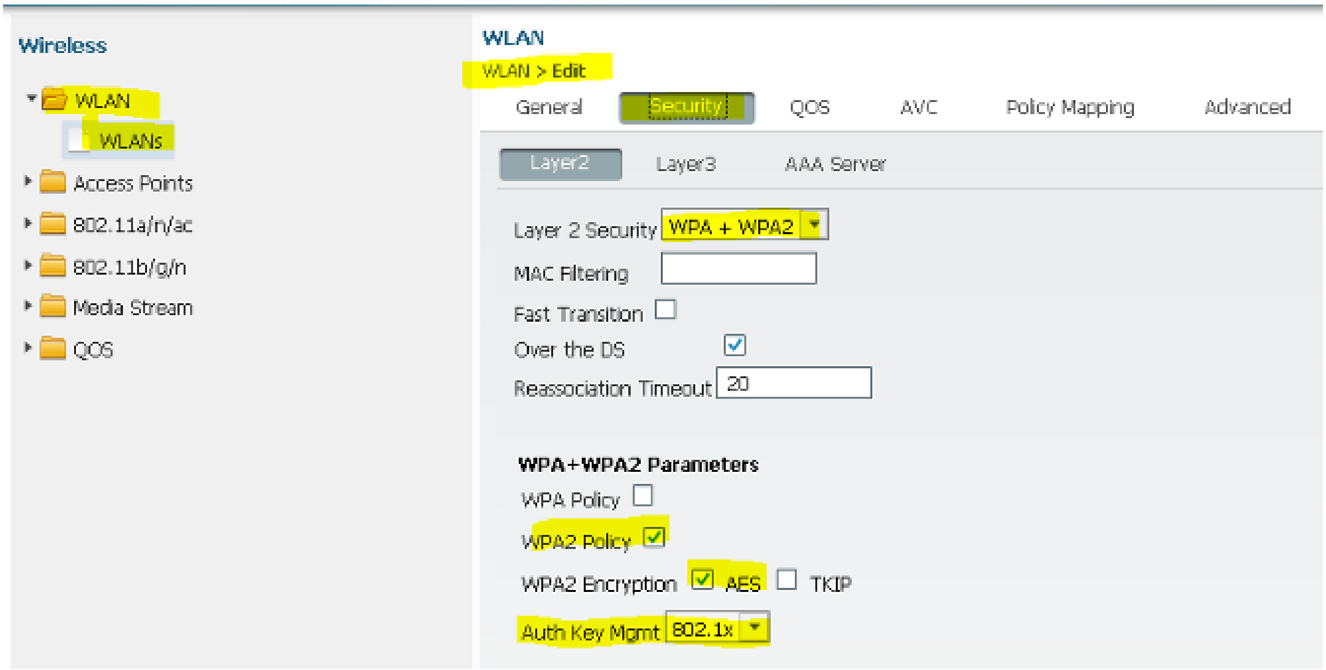
Radio Policy: All

Interface/Interface Group(G): VLAN0020

Broadcast SSID: ☑

Multicast VLAN Feature: □

配置後，安全L2頁籤應顯示類似以下內容：

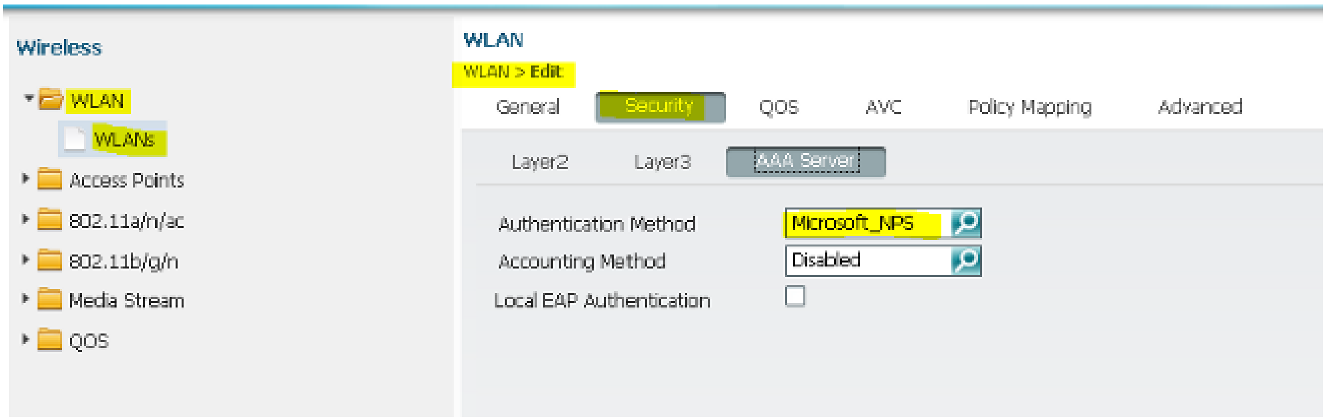


Layer 2 Security: WPA + WPA2
MAC Filtering: □
Fast Transition □
Over the DS ☑
Reassociation Timeout: 20

WPA+WPA2 Parameters

WPA Policy □
WPA2 Policy ☑
WPA2 Encryption ☑ AES □ TKIP
Auth Key Mgmt: 802.1x

8. 對映您在以上步驟中配置的方法清單。這有助於向正確的伺服器驗證客戶端。



Authentication Method: Microsoft_NPS
Accounting Method: Disabled
Local EAP Authentication □

Microsoft Windows Version 2008 Server上的配置

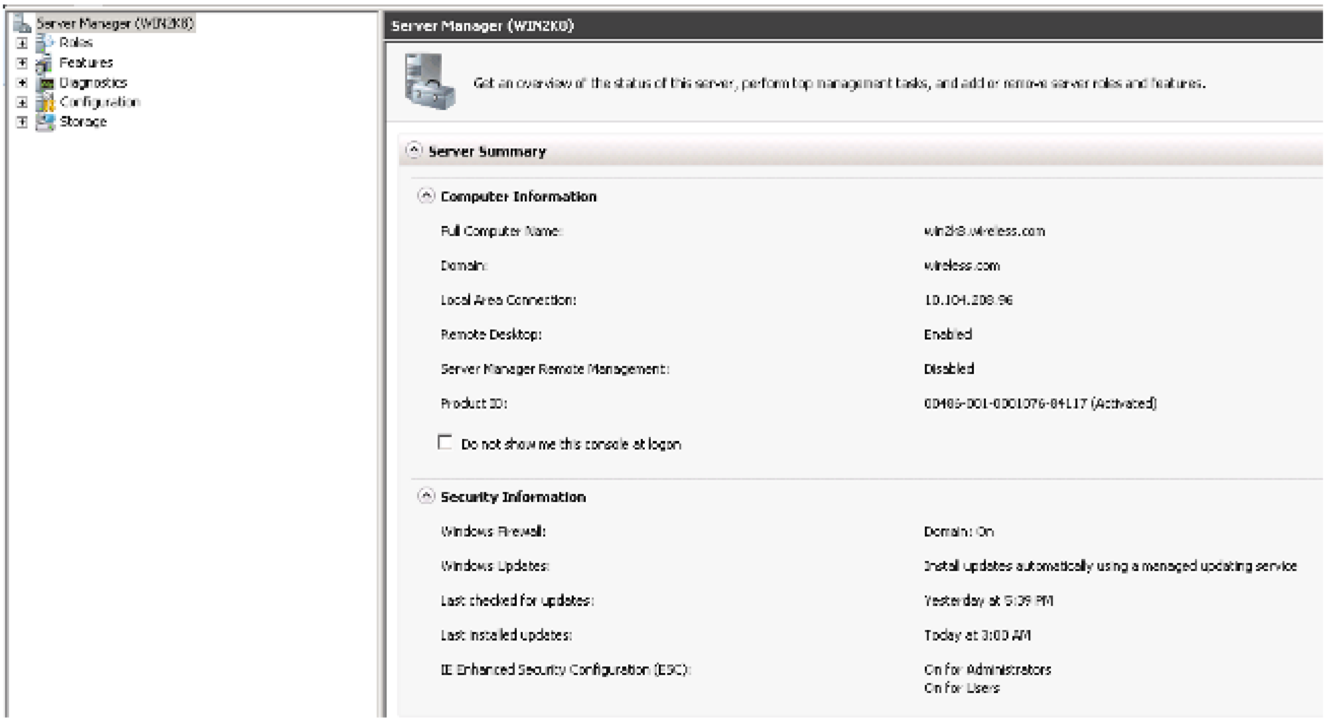
本節介紹Microsoft Windows Version 2008伺服器的完整配置。此配置分六個步驟完成：

1. 將伺服器配置為域控制器。
2. 安裝伺服器並將其配置為CA伺服器。
3. 安裝NPS。
4. 安裝證書。
5. 配置NPS進行PEAP身份驗證。
6. 將使用者新增到AD。

將Microsoft Windows 2008 Server配置為域控制器

完成以下步驟，將Microsoft Windows Version 2008伺服器配置為域控制器：

1. 導航到**開始** > **Server Manager** > Roles > **Add Roles**。



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

Server Summary

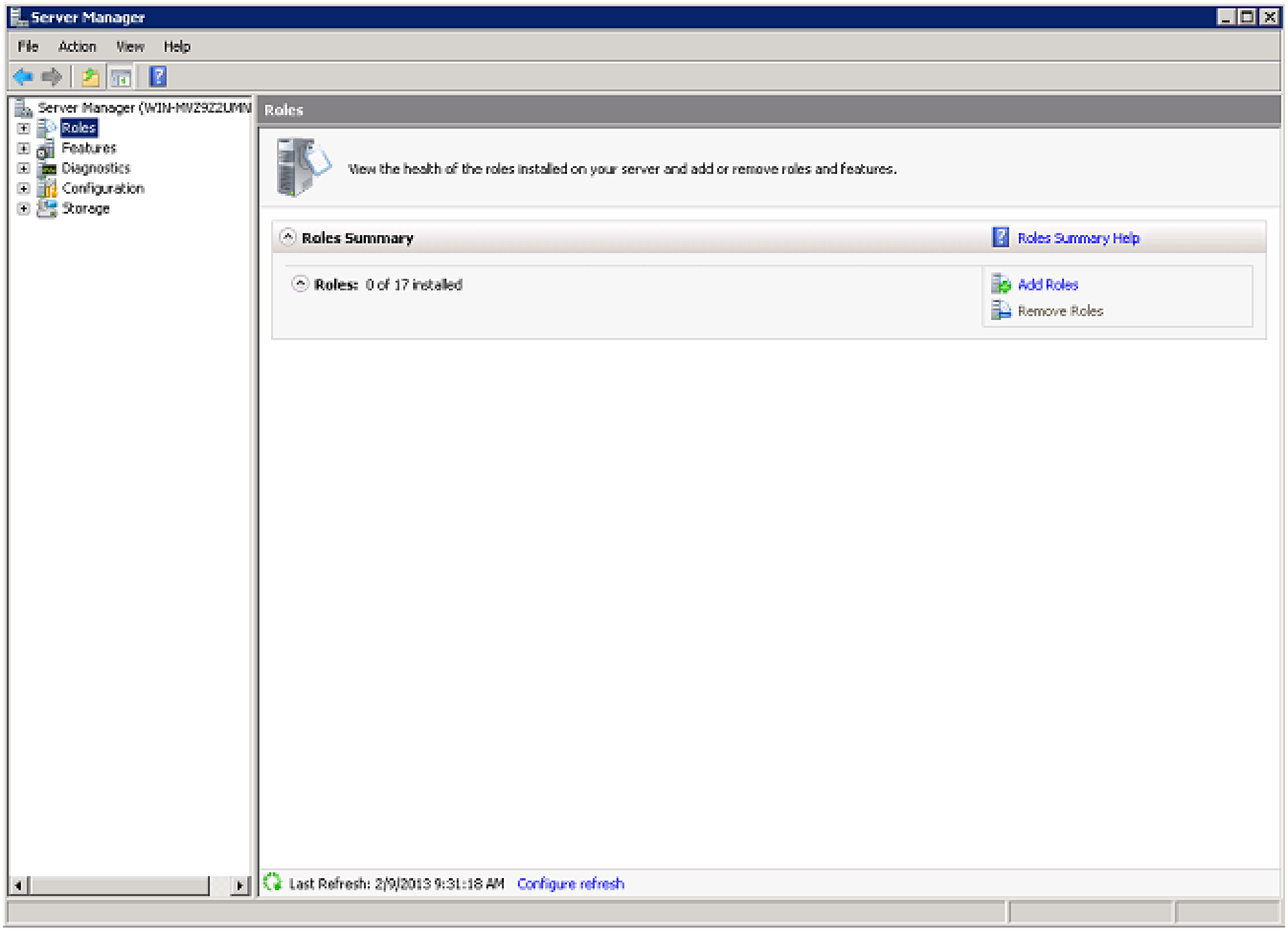
Computer Information

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

□ Do not show me this console at logon

Security Information

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



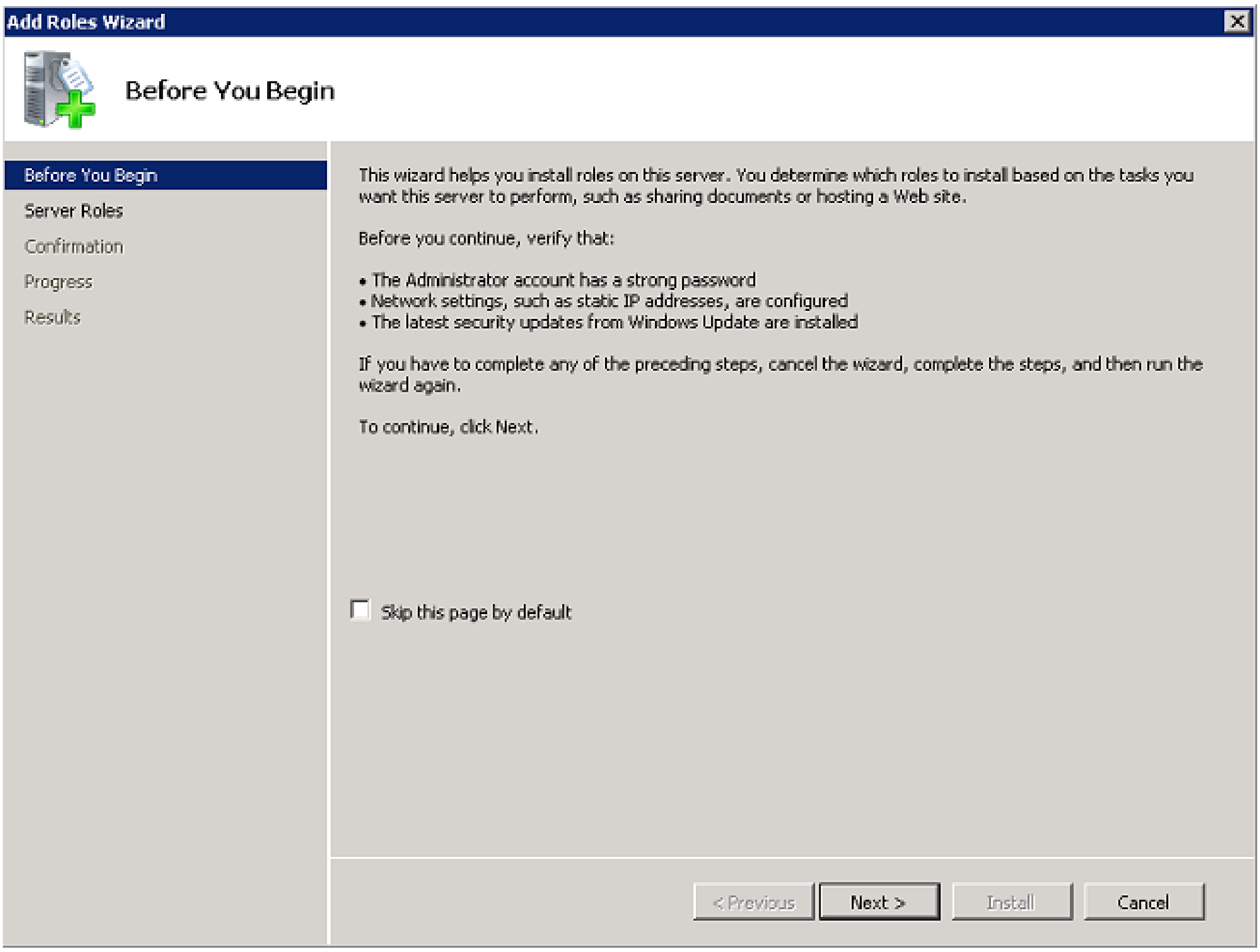
View the health of the roles installed on your server and add or remove roles and features.

Roles Summary

Roles: 0 of 17 installed

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

2. 按「**Next**」（下一步）。



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

Before you continue, verify that:

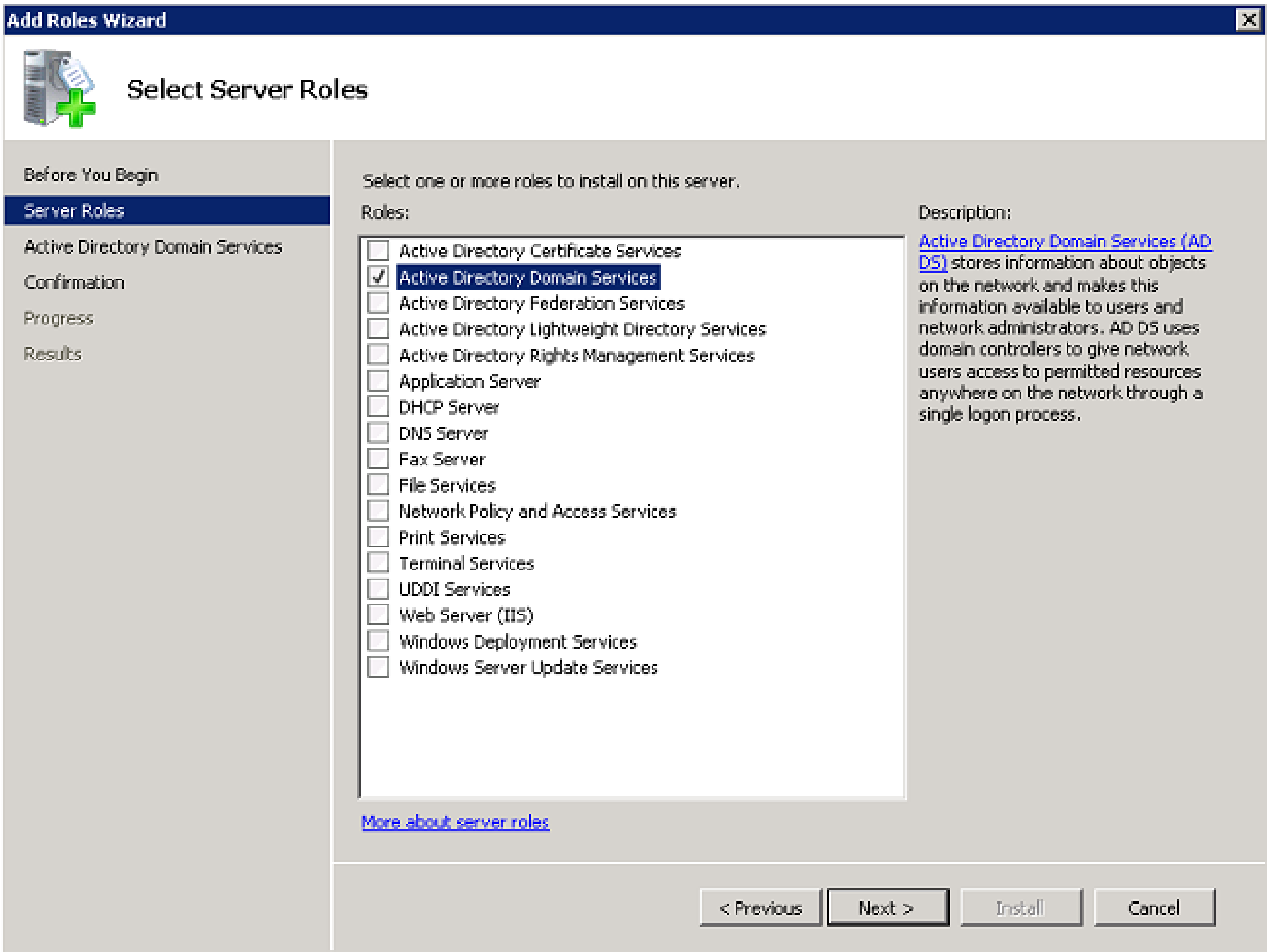
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

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

To continue, click Next.

□ Skip this page by default

3. 選中**Active Directory域服務**覈取方塊，然後按一下**下一步**。



Select one or more roles to install on this server.

Roles:

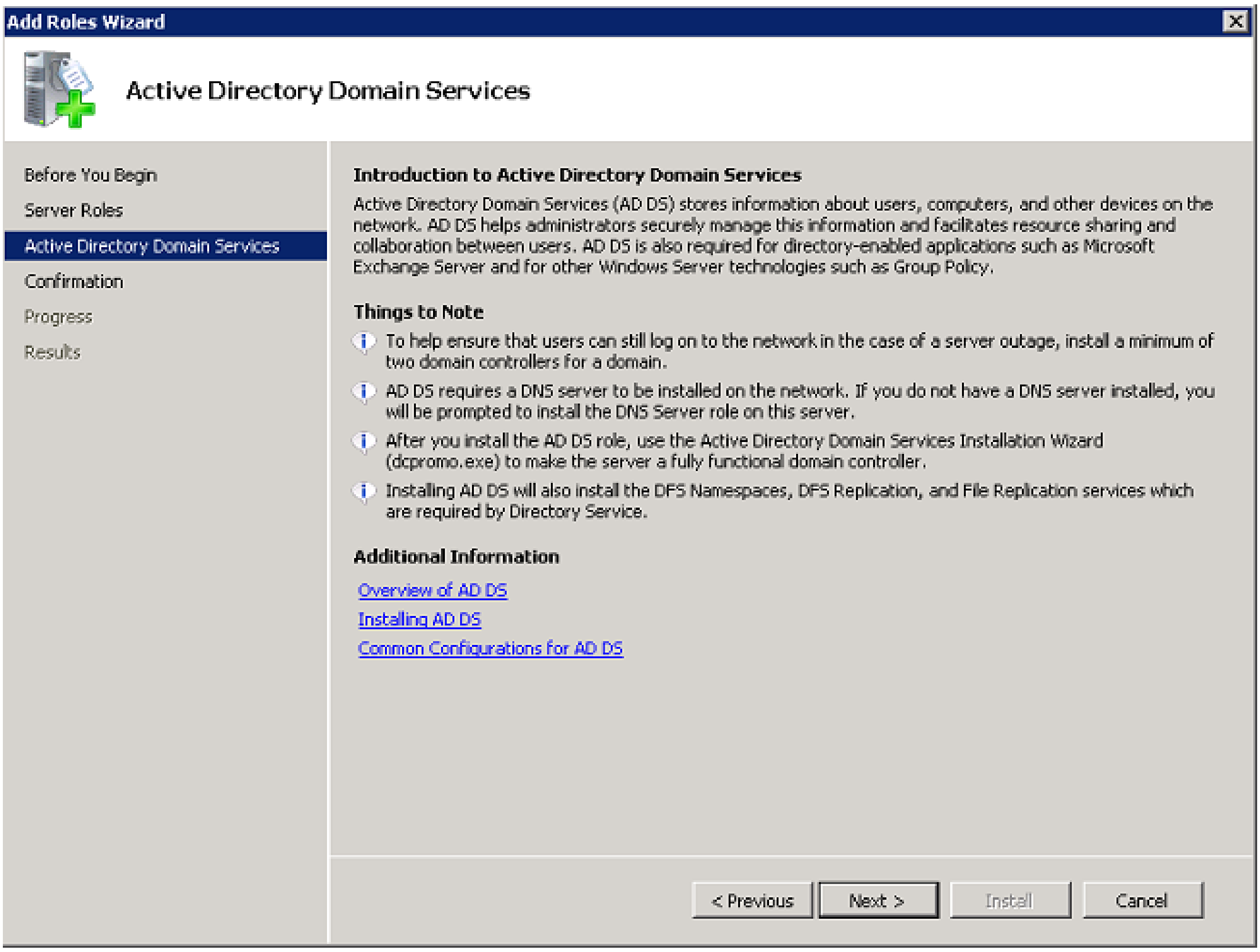
- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☐ File Services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

Description:

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

More about server roles

4. 檢視**Active Directory域服務簡介**，然後按一下**下一步**。



Introduction to Active Directory Domain Services

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

Things to Note

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

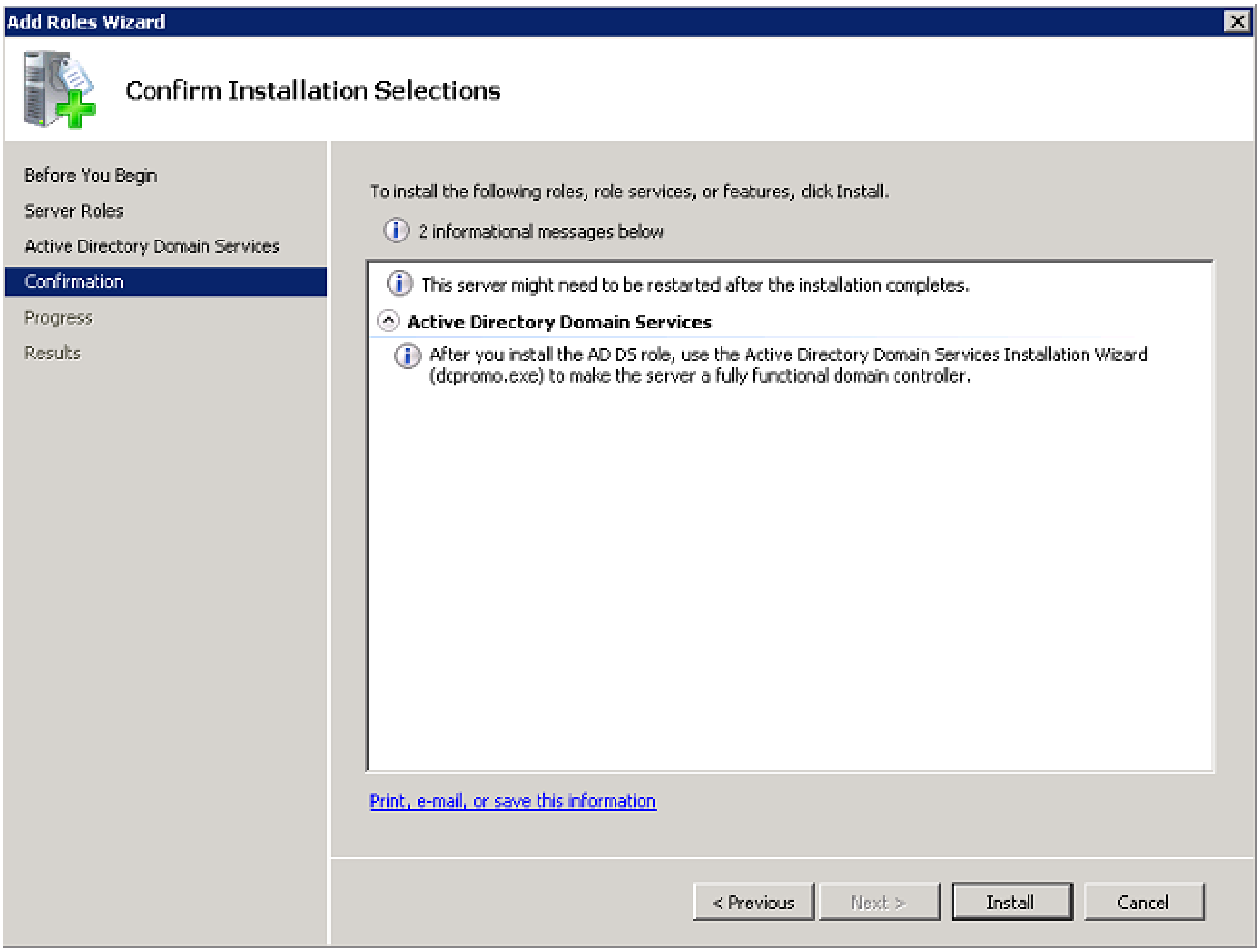
Additional Information

Overview of AD DS

Installing AD DS

Common Configurations for AD DS

5. 按一下「**Install**」以開始安裝過程。



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.

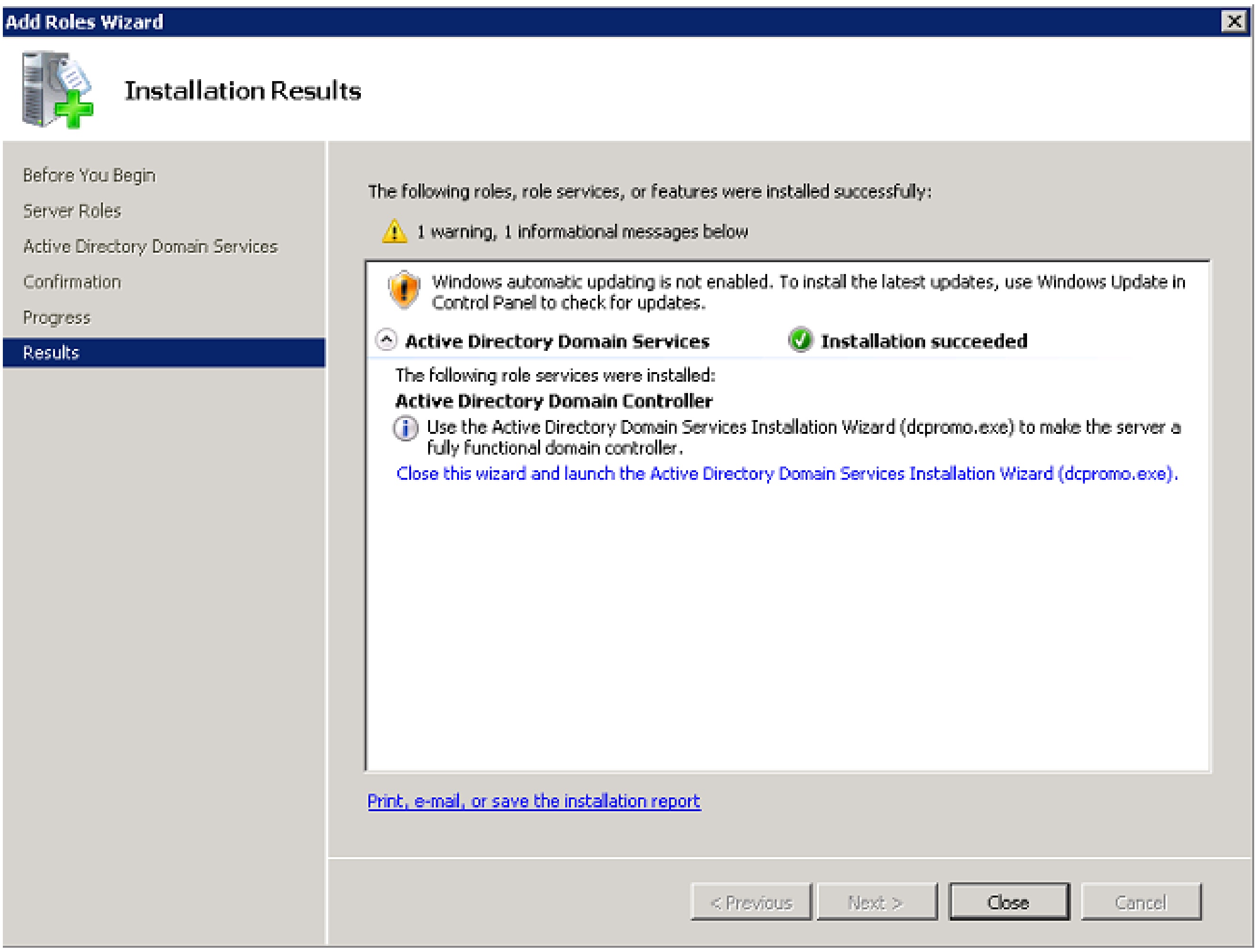
Active Directory Domain Services

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.

Print, e-mail, or save this information

安裝繼續並完成。

6. 按一下**關閉此嚮導並啟動Active Directory域服務安裝嚮導(dcpromo.exe)**，以繼續安裝和配置AD。



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

1 warning, 1 informational messages below

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

Active Directory Domain Services — Installation succeeded

The following role services were installed:

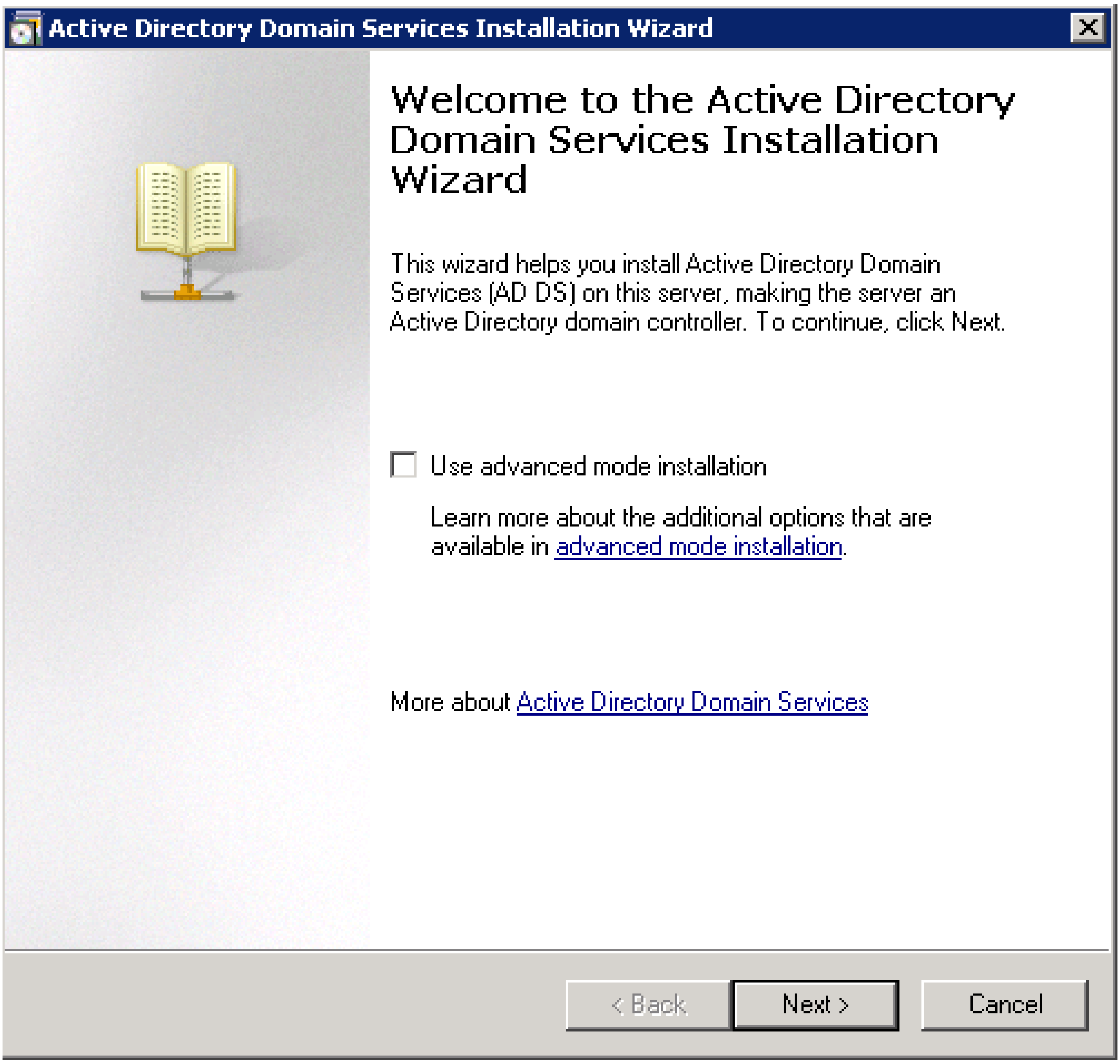
Active Directory Domain Controller

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

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

Print, e-mail, or save the installation report

7. 按一下**下一步**以運行**Active Directory域服務安裝嚮導**。



Active Directory Domain Services Installation Wizard

Welcome to the Active Directory Domain Services Installation Wizard

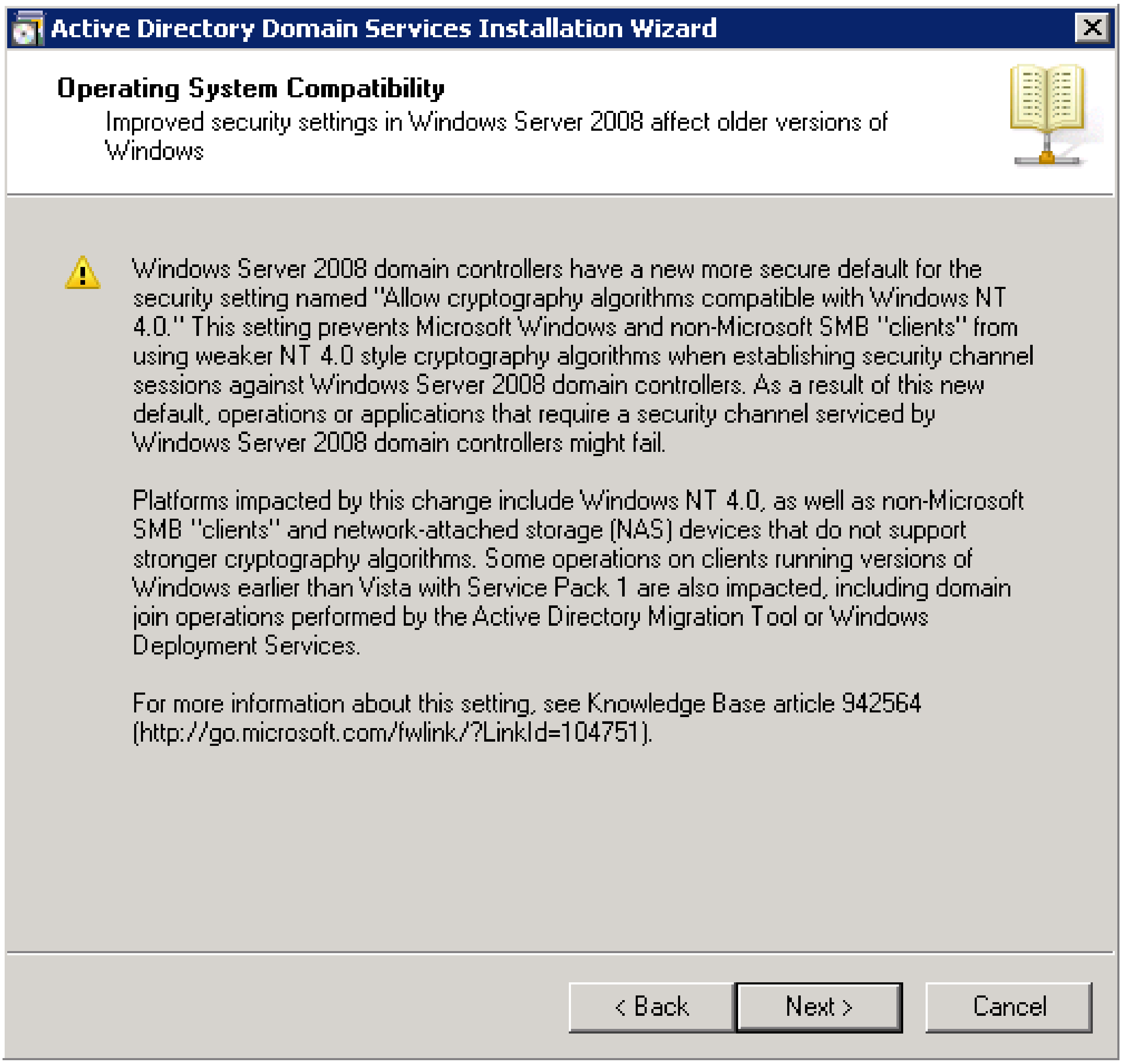
This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next.

☐ Use advanced mode installation

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

More about Active Directory Domain Services

8. 檢視有關**作業系統相容性**的資訊，然後按一下**下一步**。



Operating System Compatibility

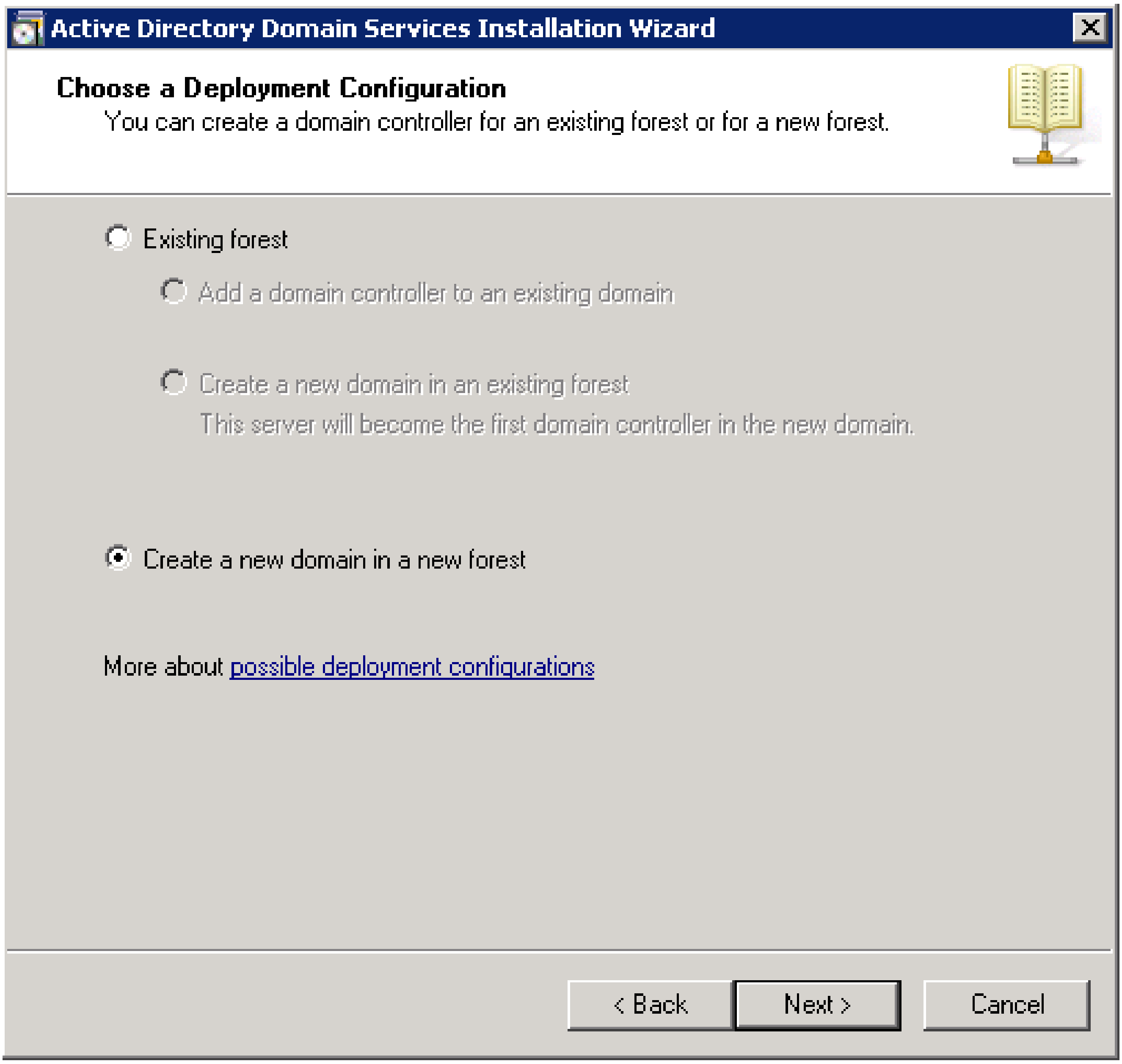
Improved security settings in Windows Server 2008 affect older versions of Windows

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

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

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

9. 按一下**在新林中建立新域**單選按鈕，然後按一下**下一步**以建立新域。



Active Directory Domain Services Installation Wizard

Choose a Deployment Configuration

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

○ Existing forest

○ Add a domain controller to an existing domain

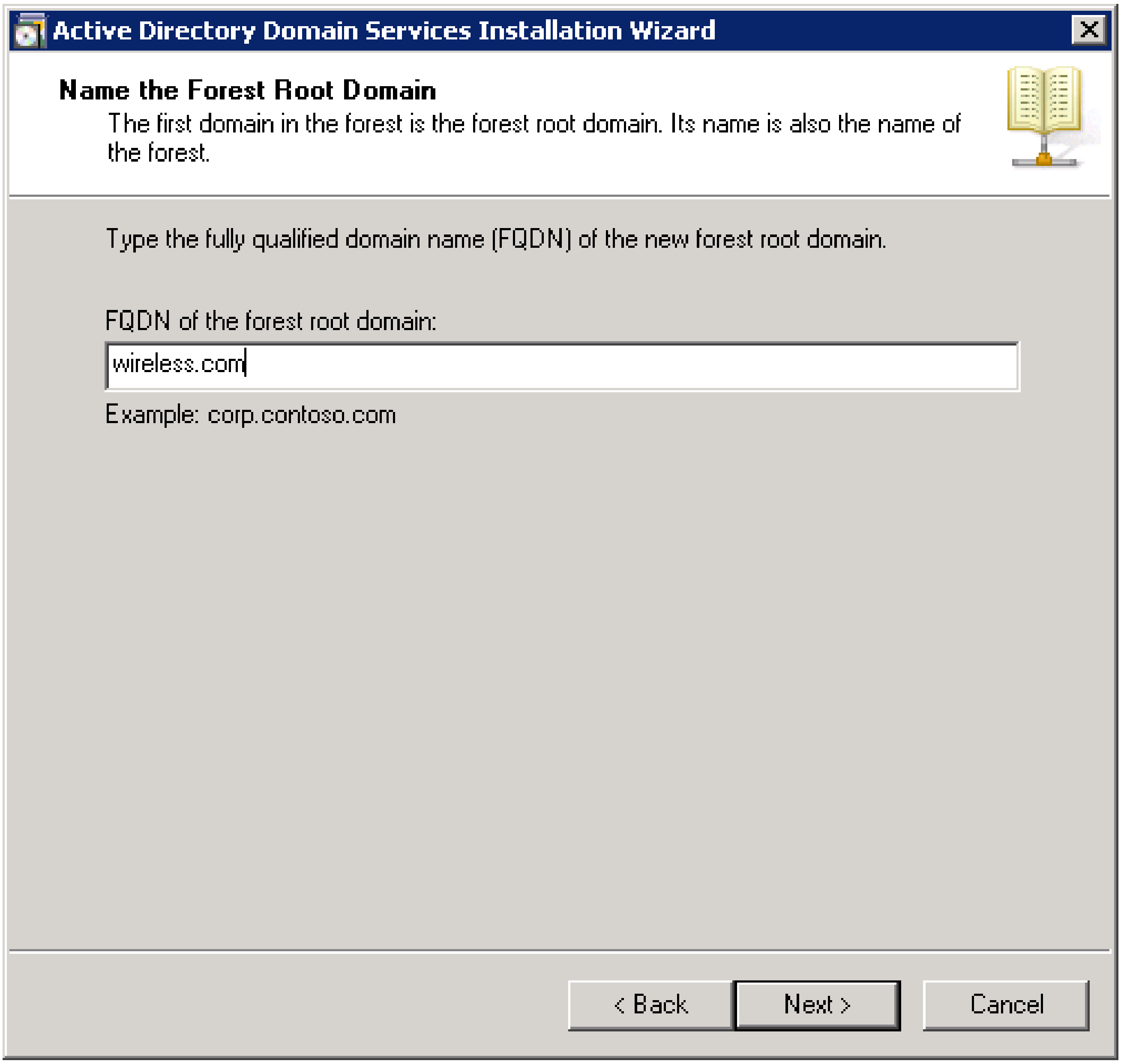
○ Create a new domain in an existing forest

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

● Create a new domain in a new forest

More about possible deployment configurations

10. 輸入新域的完整DNS名稱(在本例中為**wireless.com**)，然後按一下**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.

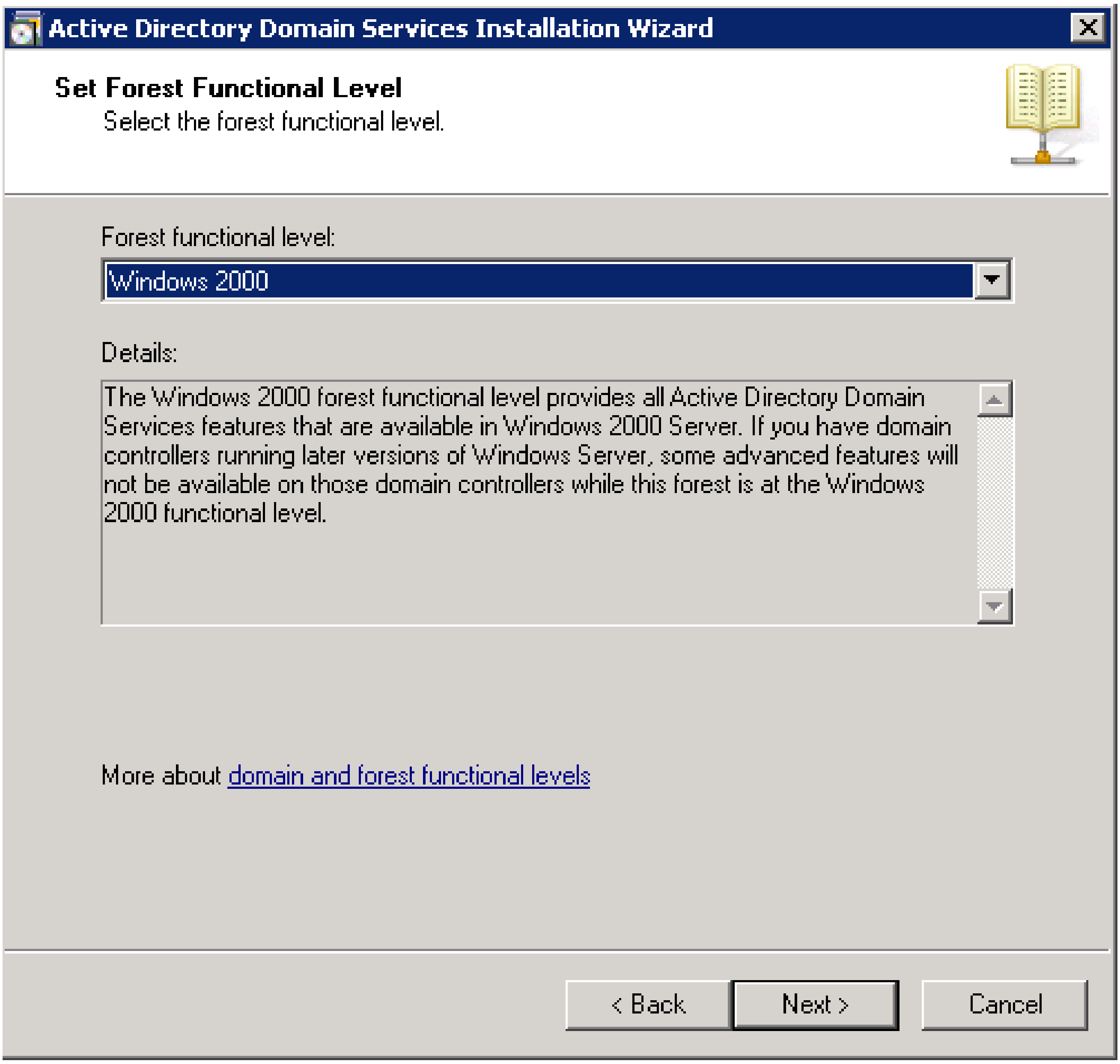
Type the fully qualified domain name (FQDN) of the new forest root domain.

FQDN of the forest root domain:

wireless.com

Example: corp.contoso.com

11. 選擇域的**林功能級別**，然後按一下**下一步**。



Active Directory Domain Services Installation Wizard

Set Forest Functional Level

Select the forest functional level.

Forest functional level:

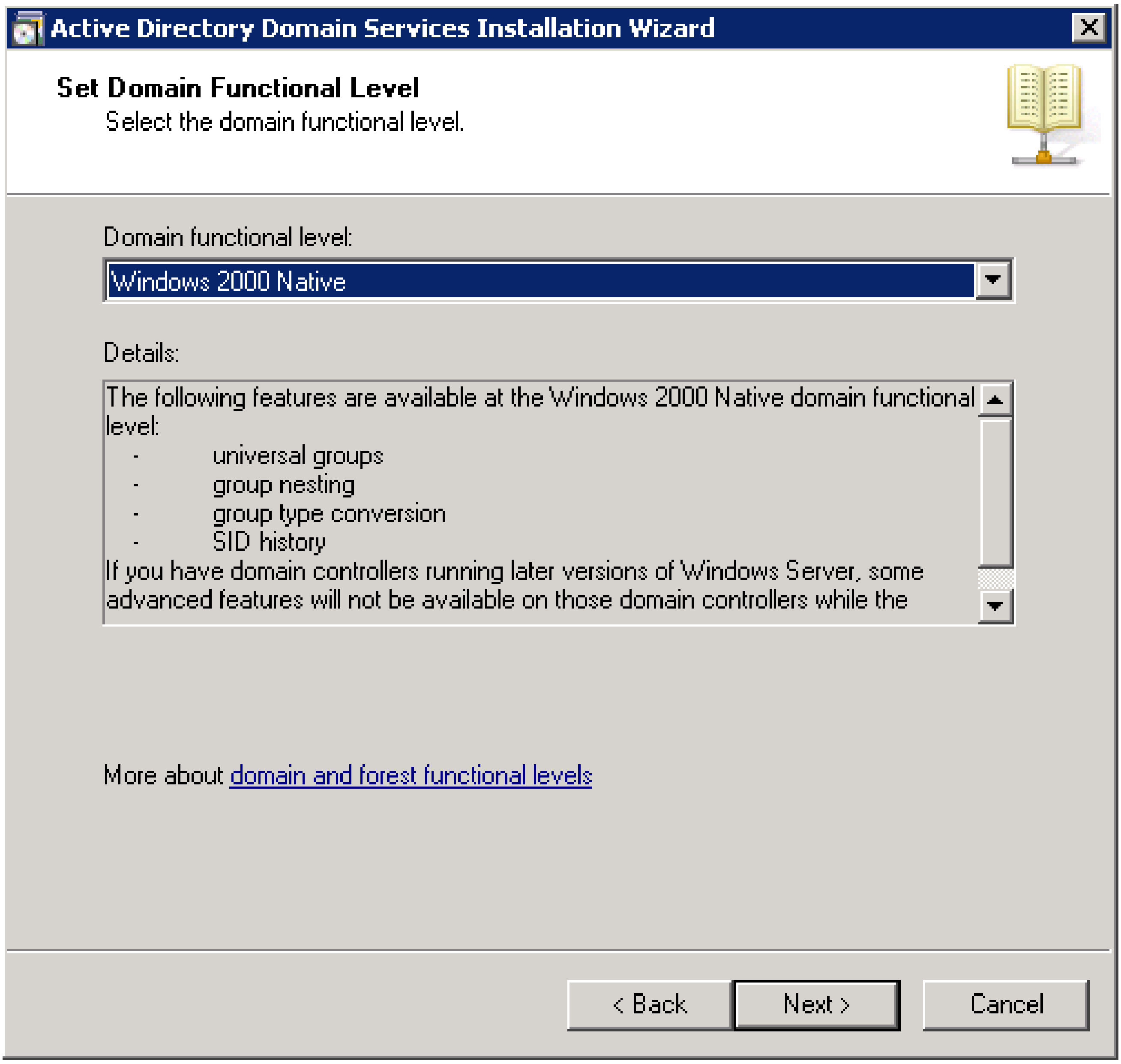
Windows 2000

Details:

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

More about domain and forest functional levels

12. 選擇域的**域功能級別**，然後按一下**下一步**。



Set Domain Functional Level

Select the domain functional level.

Domain functional level:

Windows 2000 Native

Details:

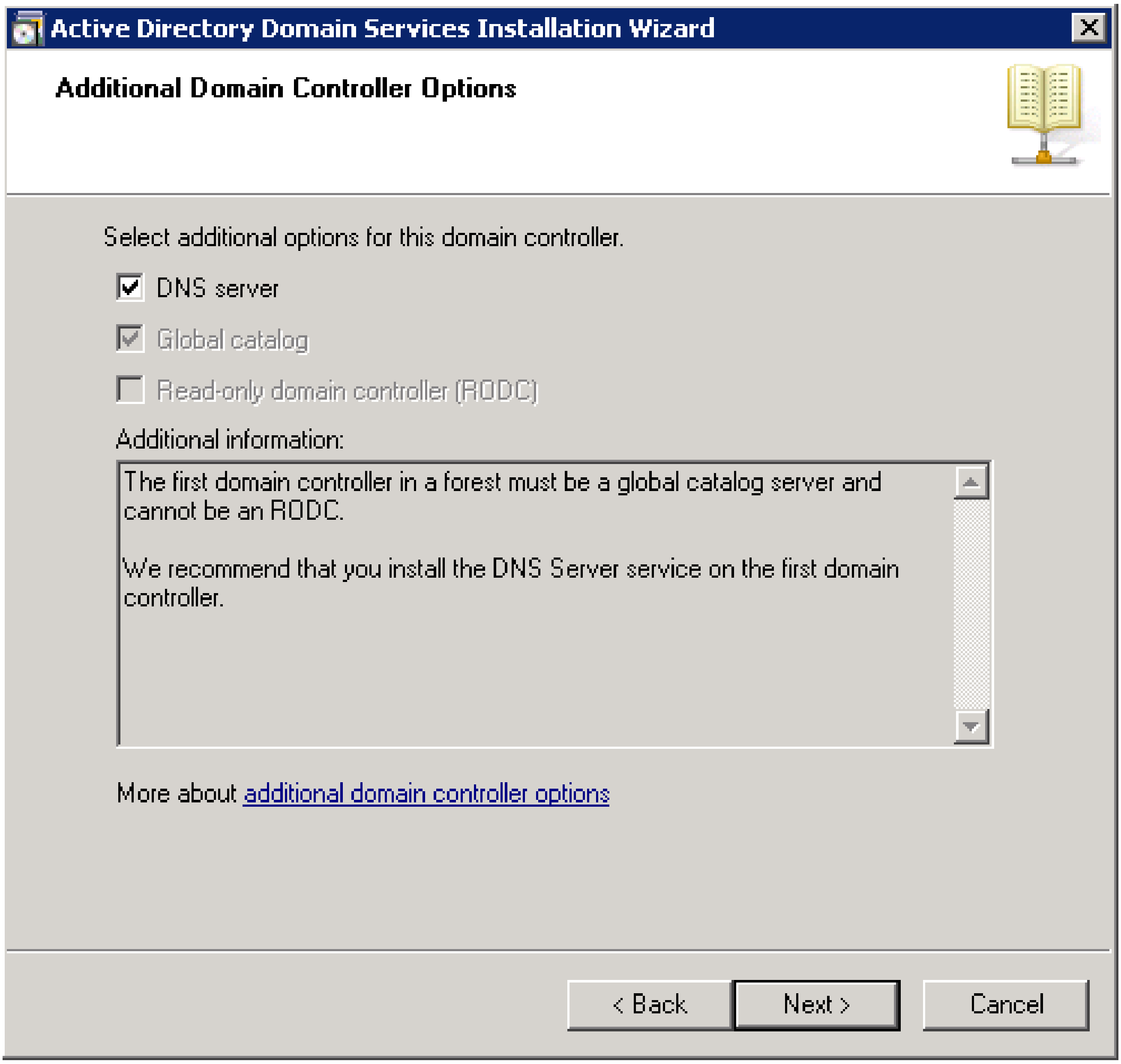
The following features are available at the Windows 2000 Native domain functional level:

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

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

More about domain and forest functional levels

13. 選中**DNS server**覈取方塊，然後按一下**Next**。



Additional Domain Controller Options

Select additional options for this domain controller.

☑ DNS server

☑ Global catalog

□ Read-only domain controller (RODC)

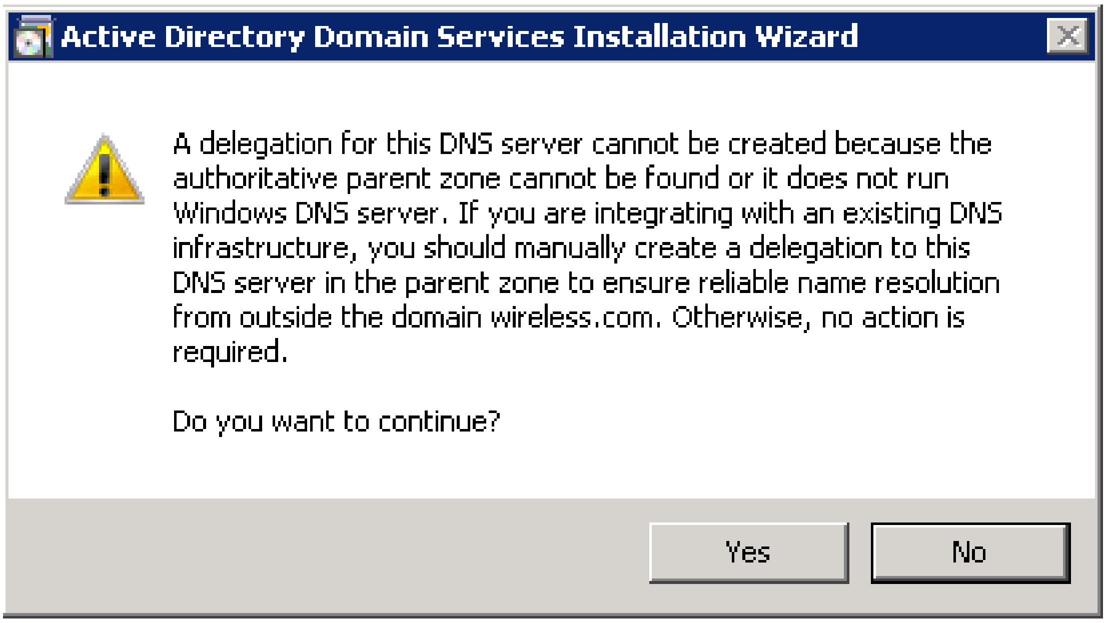
Additional information:

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

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

More about additional domain controller options

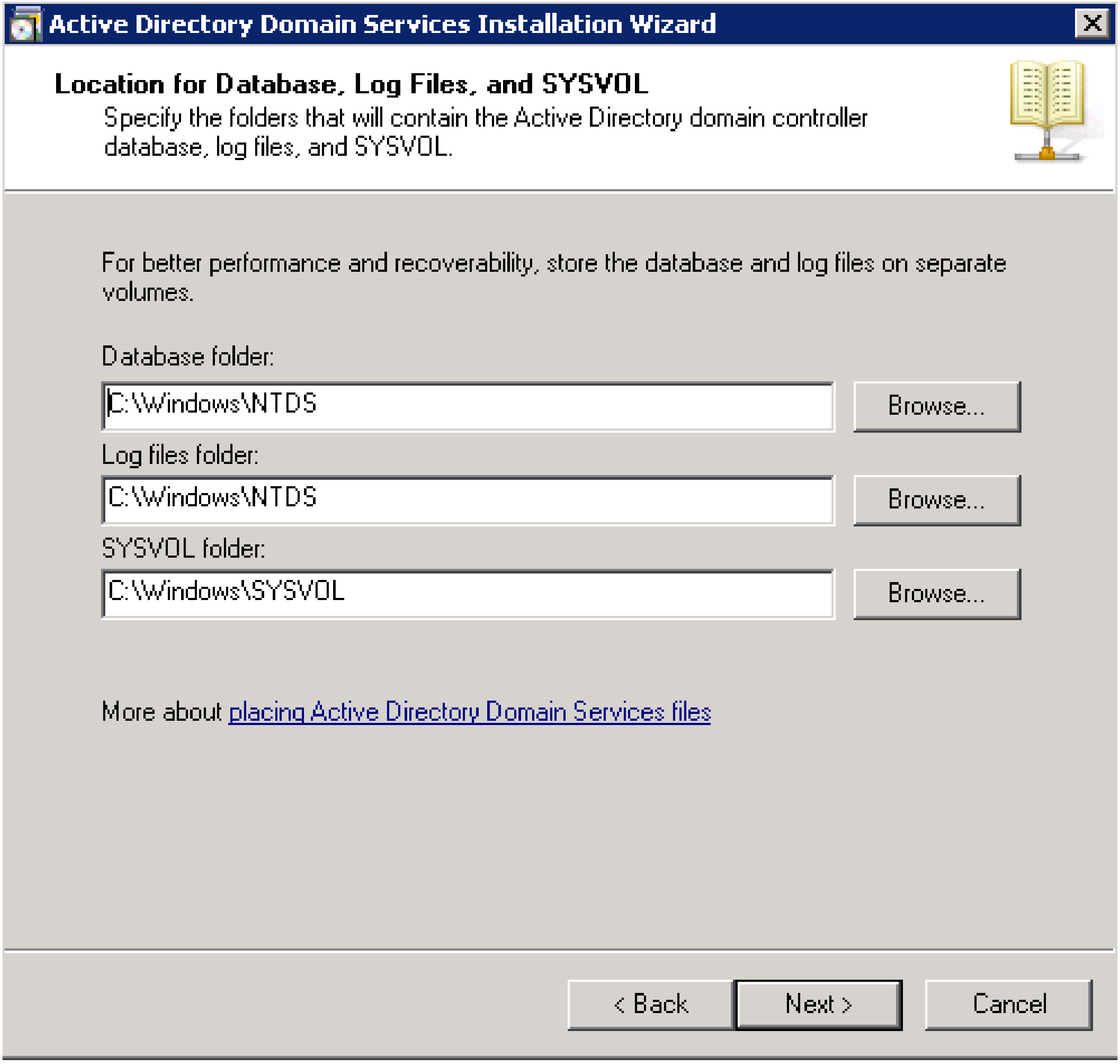
14. 出現「**Active Directory Domain Services Installation Wizard**」彈出視窗時，按一下**Yes**，以便在DNS中為域建立新區域。



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

Do you want to continue?

15. 選擇希望AD用於檔案的資料夾，然後按一下**下一步**。



Active Directory Domain Services Installation Wizard

Location for Database, Log Files, and SYSVOL

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

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

Database folder:

C:\Windows\NTDS

Log files folder:

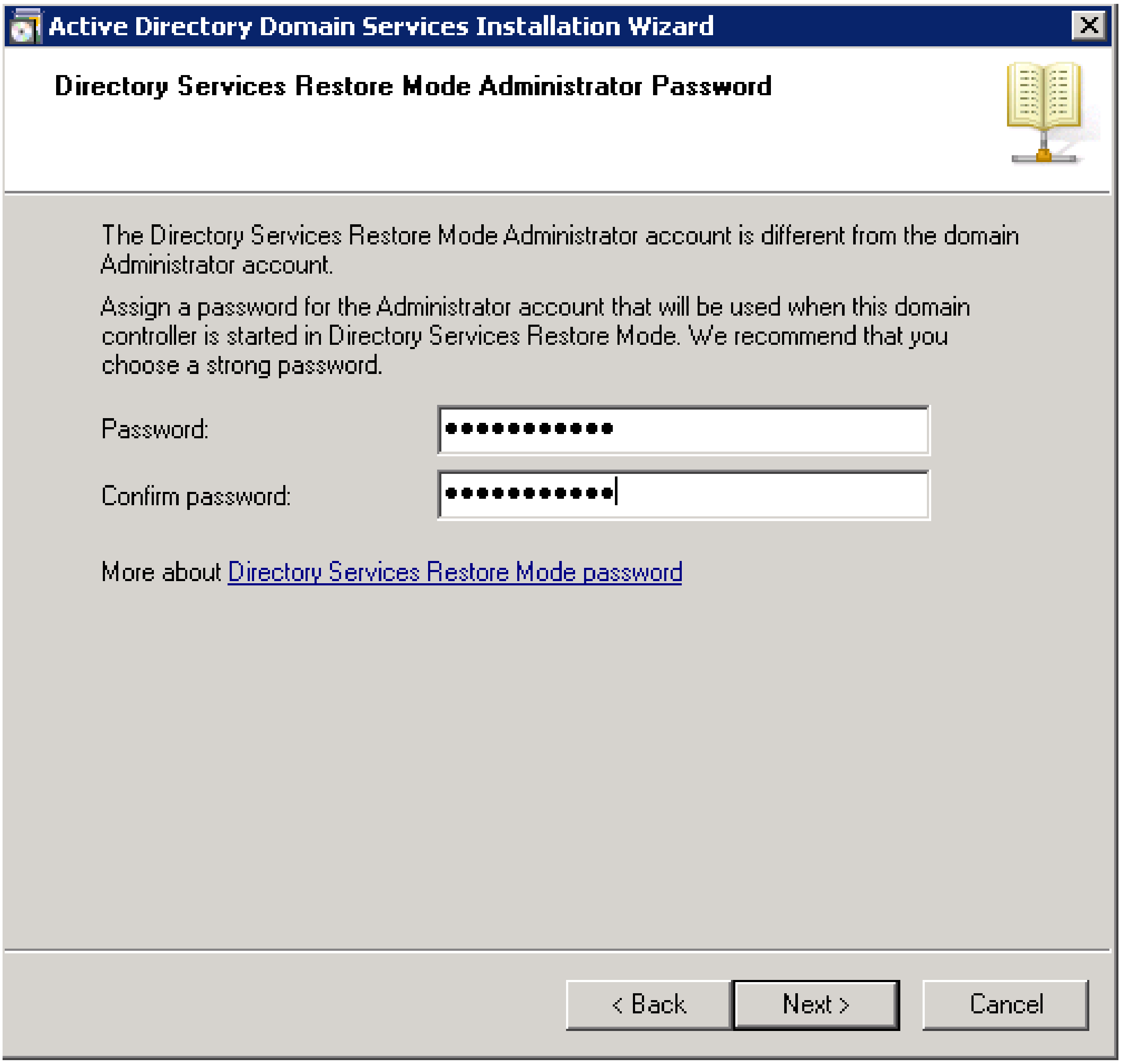
C:\Windows\NTDS

SYSVOL folder:

C:\Windows\SYSVOL

More about placing Active Directory Domain Services files

16. 輸入管理員密碼，然後按一下**下一步**。



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.

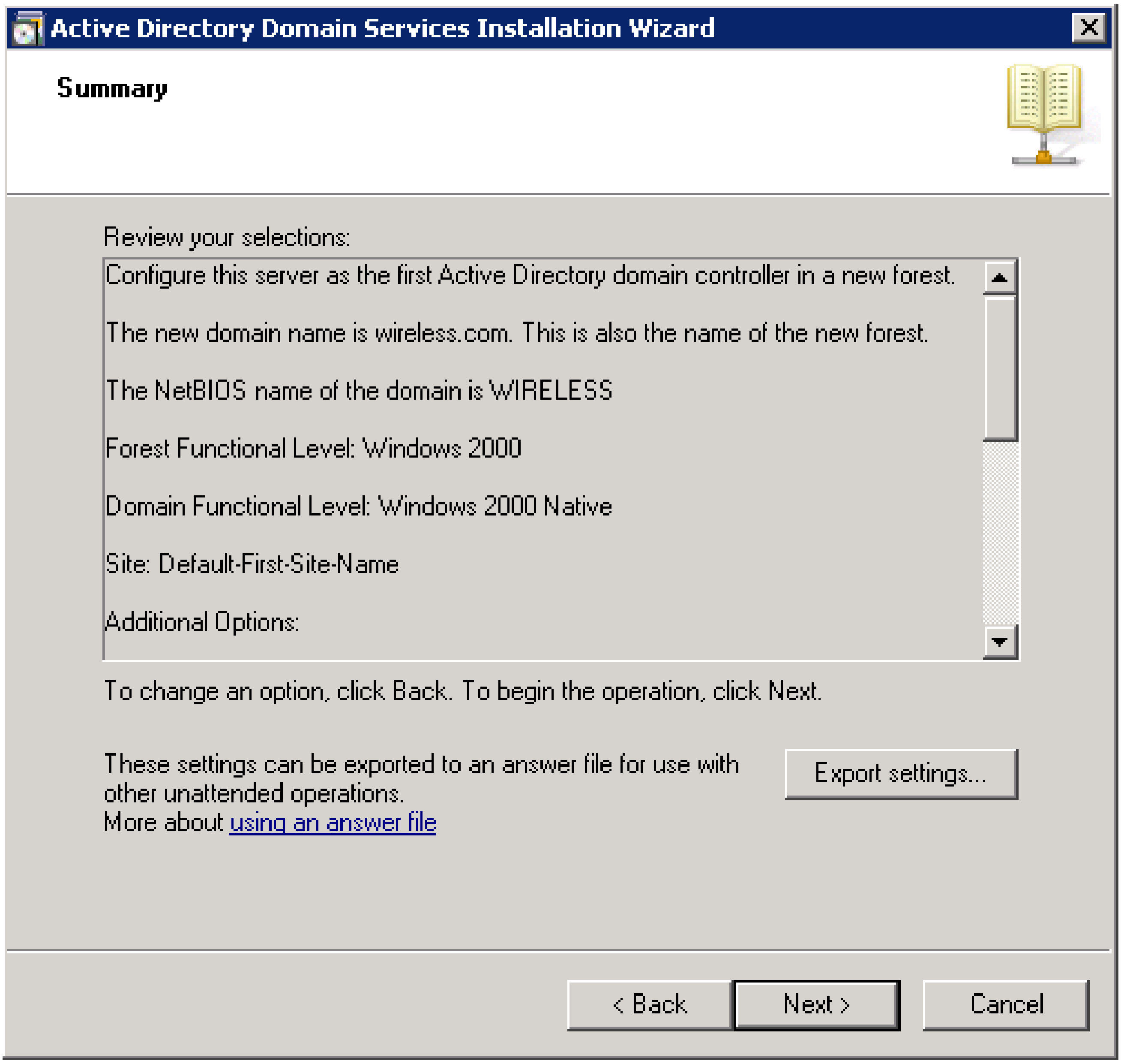
Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password: ●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●

More about Directory Services Restore Mode password

17. 檢視您的選擇，然後按一下**下一步**。



Active Directory Domain Services Installation Wizard

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

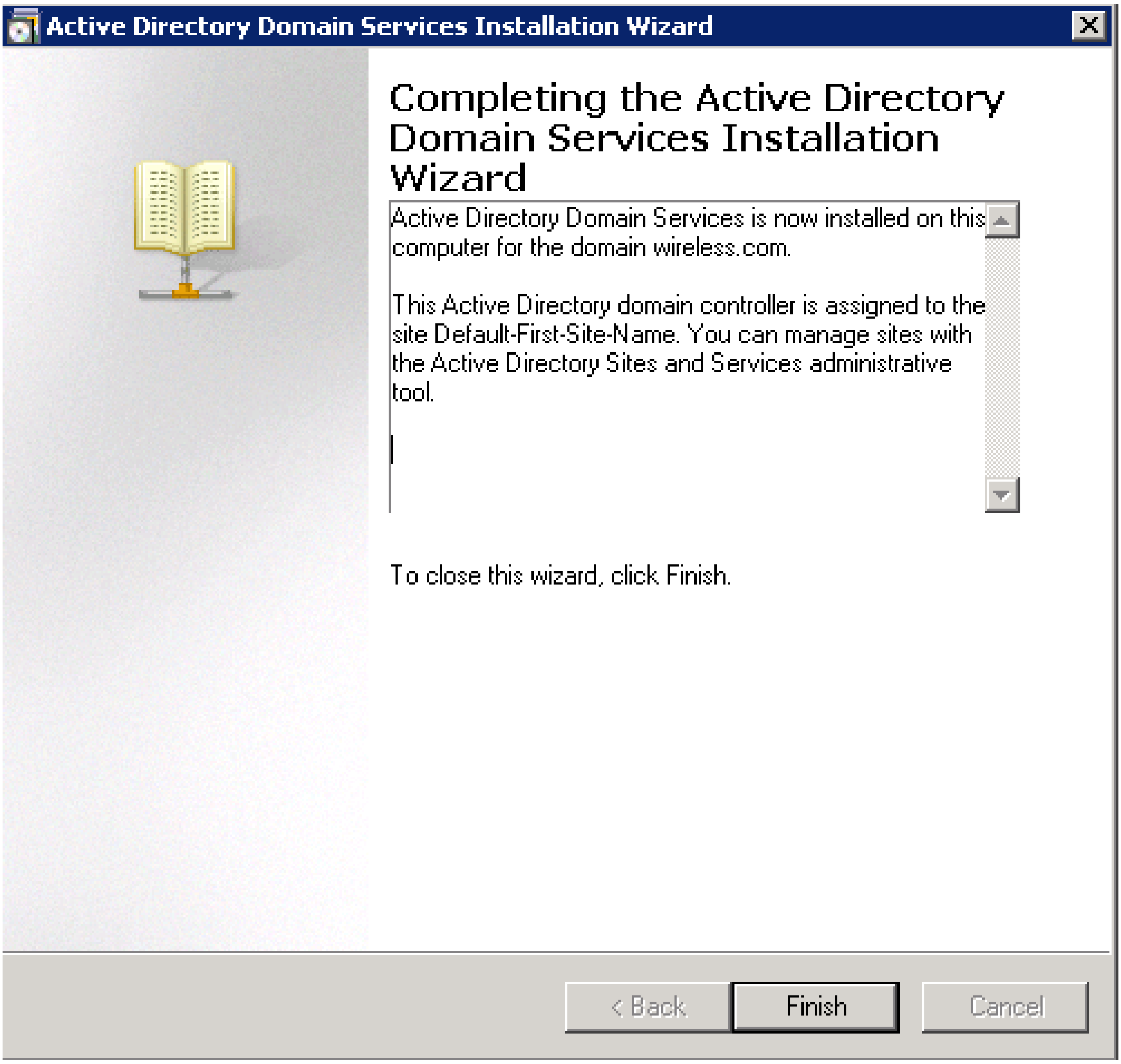
Additional Options:

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

安裝繼續進行。

18. 按一下**完成**關閉嚮導。



Active Directory Domain Services Installation Wizard

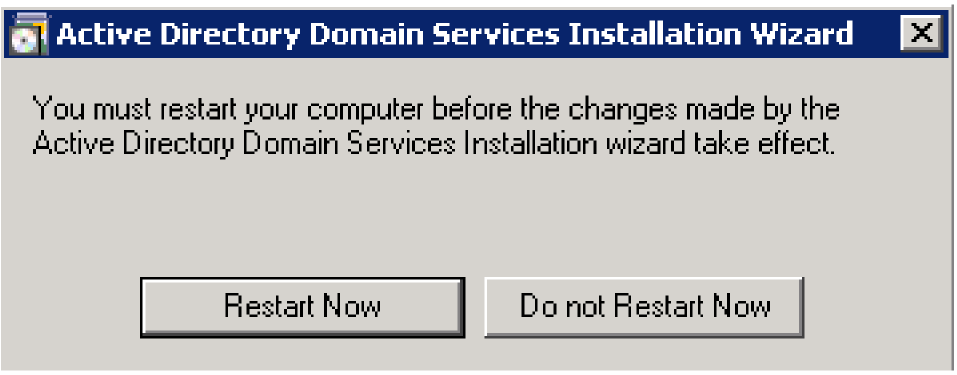
Completing the Active Directory Domain Services Installation Wizard

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.

19. 重新啟動伺服器以使更改生效。



Active Directory Domain Services Installation Wizard

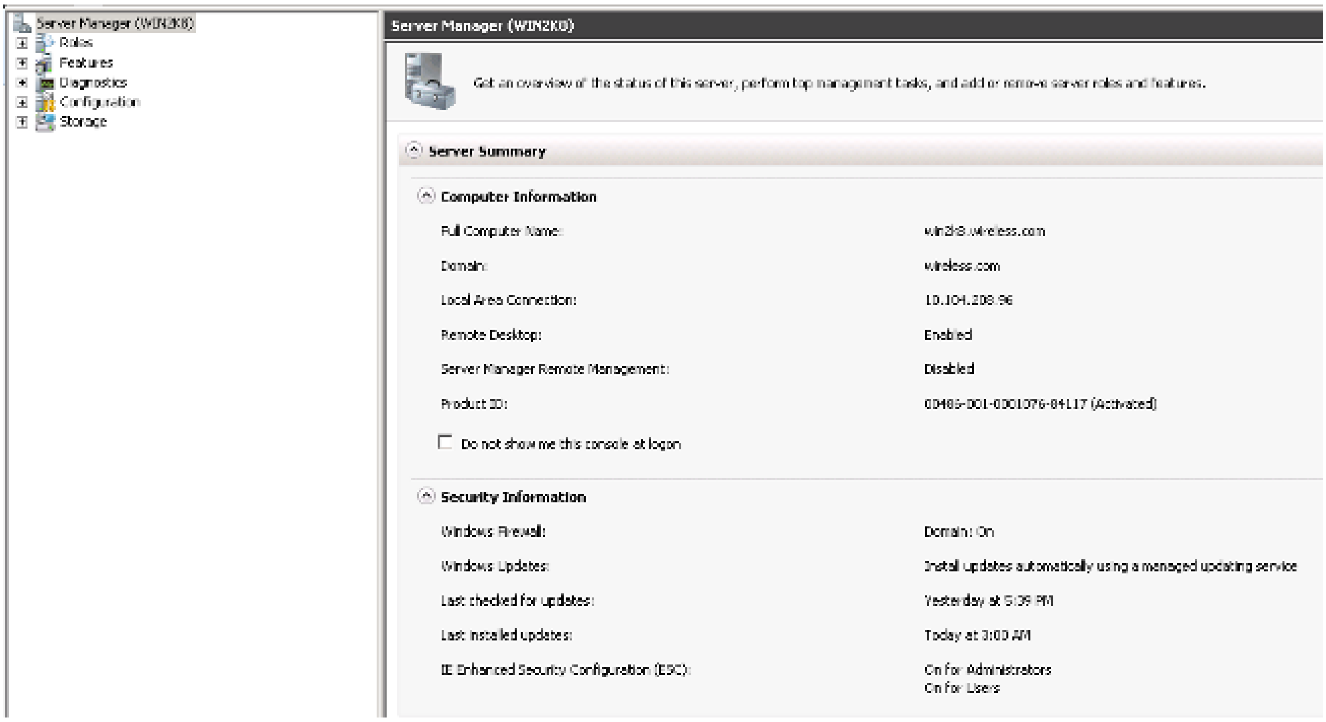
You must restart your computer before the changes made by the Active Directory Domain Services Installation wizard take effect.

安裝並配置Microsoft Windows Version 2008 Server作為CA伺服器

使用EAP-MS-CHAP v2的PEAP根據伺服器上存在的證書驗證RADIUS伺服器。此外，伺服器證書必須由客戶端電腦信任的公共CA頒發。也就是說，公共CA證書已存在於客戶端電腦證書儲存上的受信任的根證書頒發機構資料夾中。

完成以下步驟，將Microsoft Windows Version 2008伺服器配置為向NPS頒發證書的CA伺服器：

1. 導航到**開始** > **Server Manager** > Roles > **Add Roles**。



Server Manager (WIN2K8)

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

Server Summary

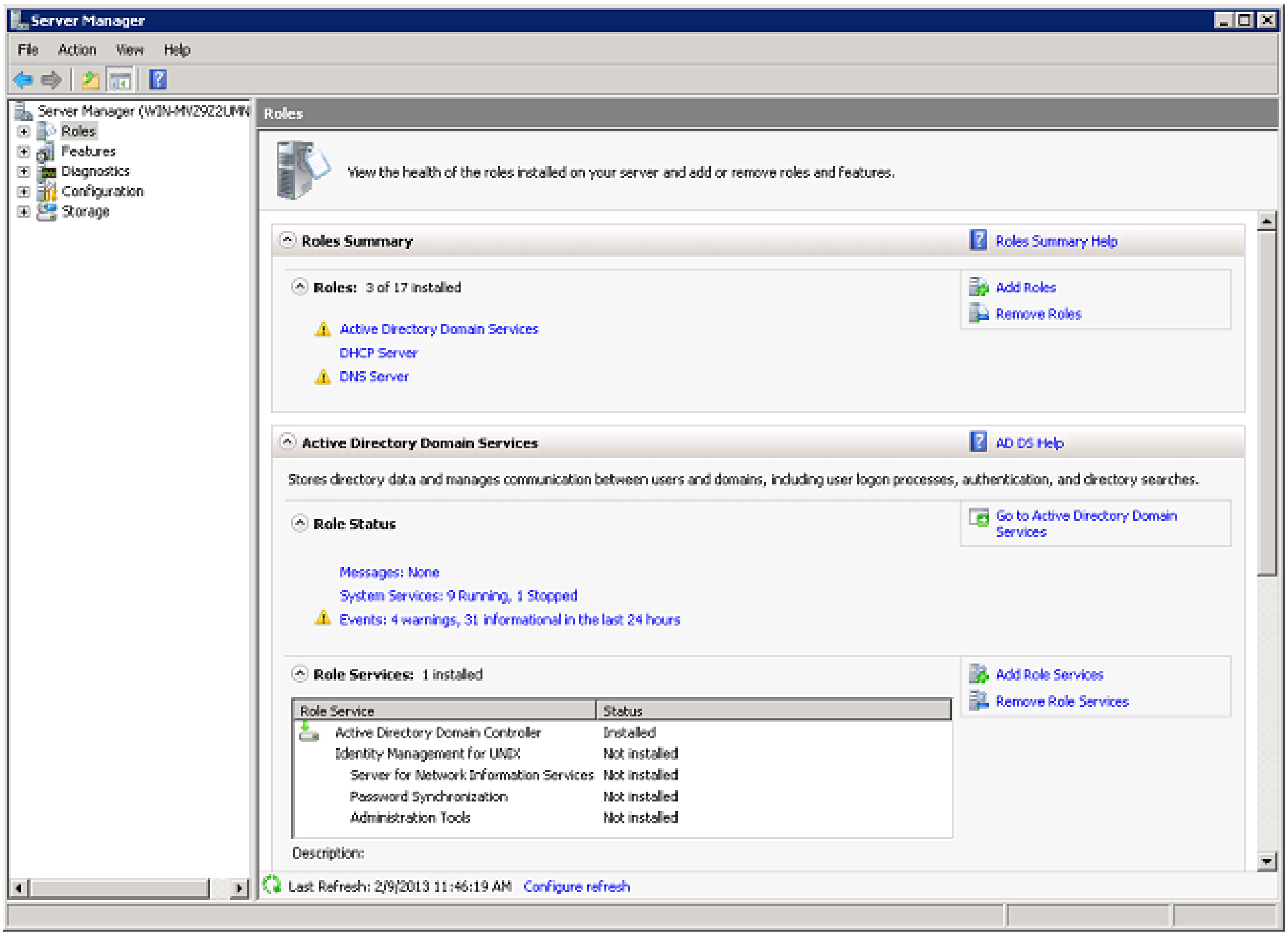
Computer Information

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

□ Do not show me this console at logon

Security Information

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



Roles

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

Roles Summary

Roles Summary Help

Roles: 3 of 17 installed

Add Roles

Remove Roles

⚠ Active Directory Domain Services

DHCP Server

⚠ DNS Server

Active Directory Domain Services

AD DS Help

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

Role Status

Go to Active Directory Domain Services

Messages: None

System Services: 9 Running, 1 Stopped

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

Role Services: 1 installed

Add Role Services

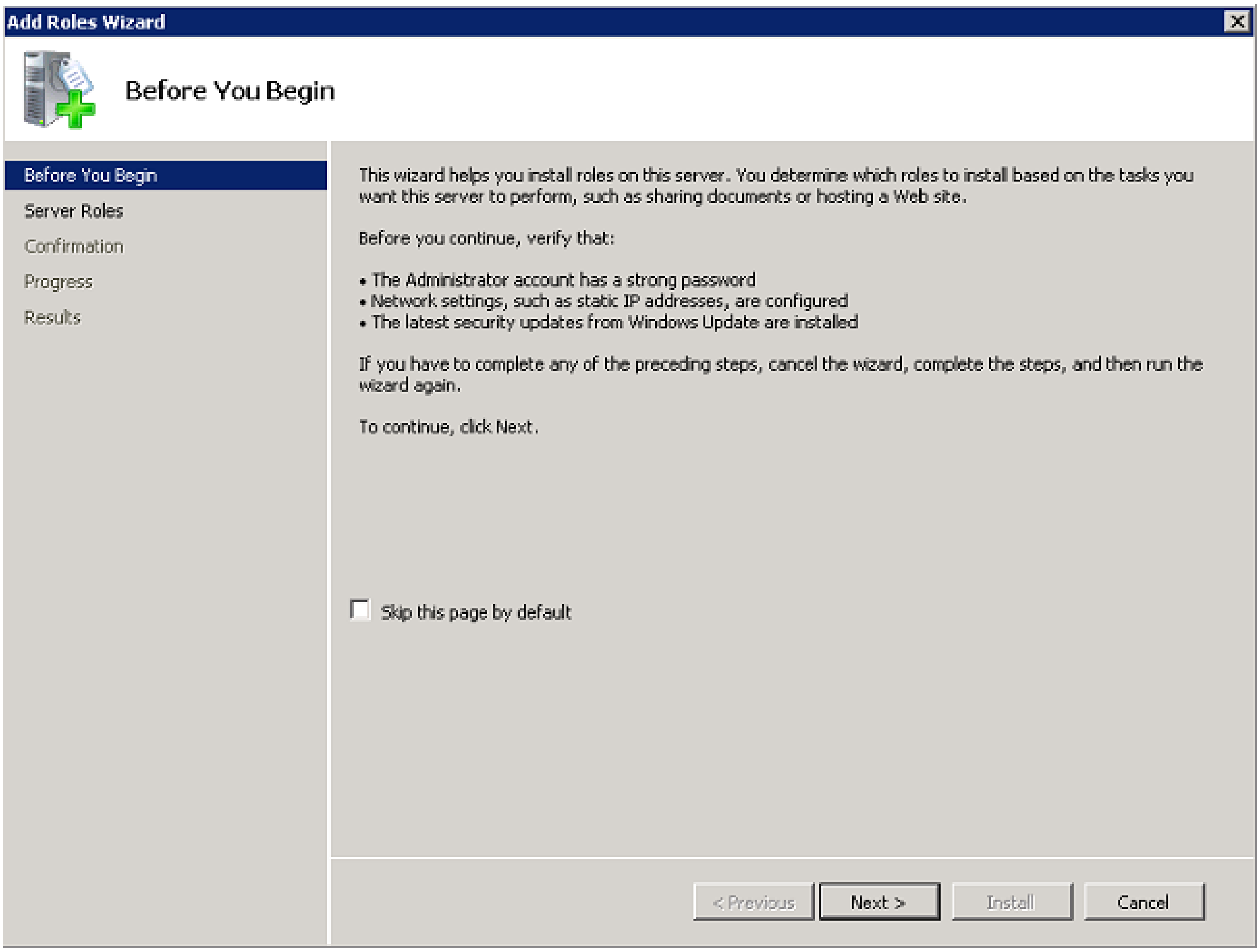
Remove Role Services

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 Configure refresh

2. 按「**Next**」（下一步）。



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

Before you continue, verify that:

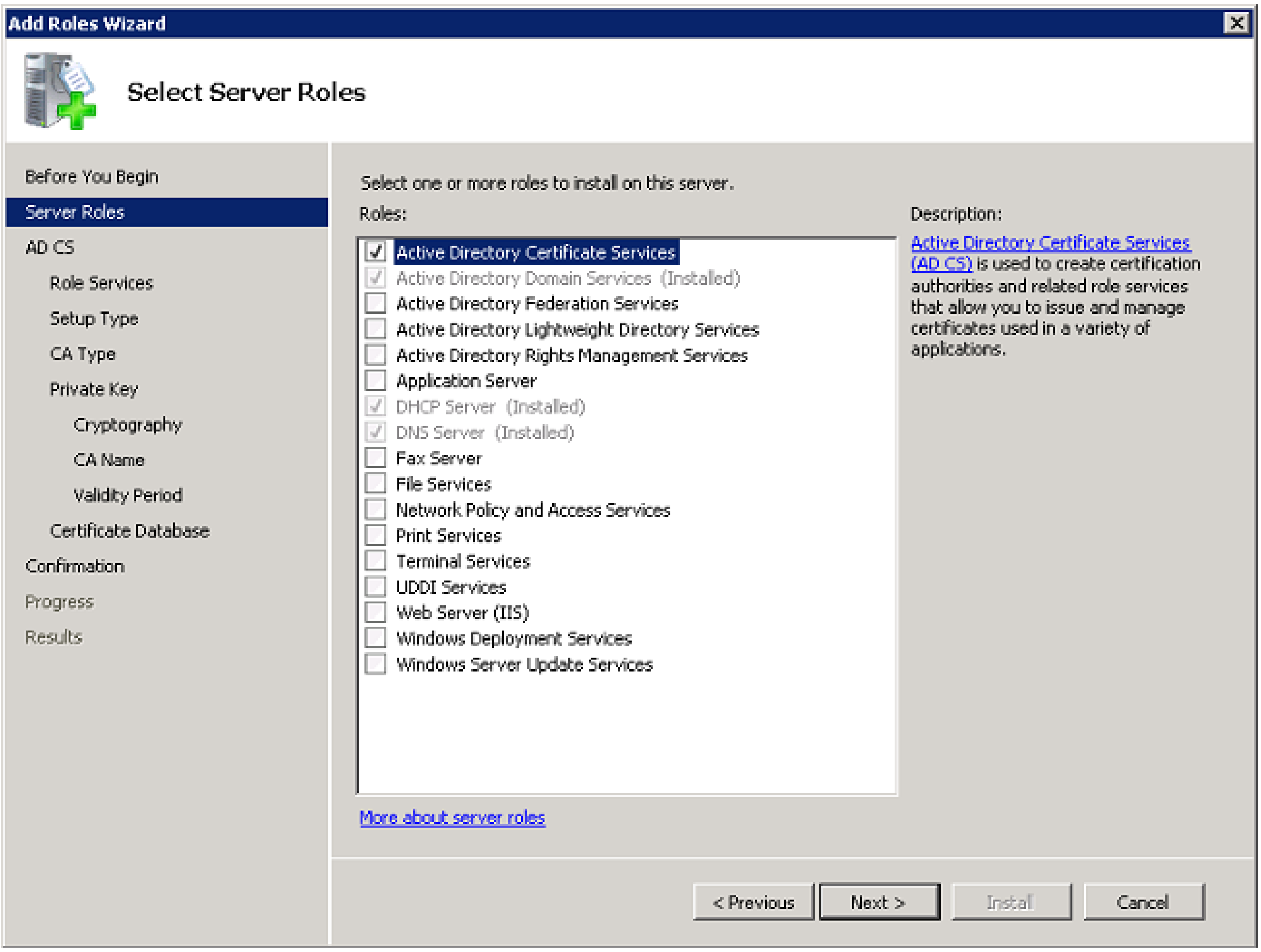
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

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

To continue, click Next.

□ Skip this page by default

3. 選中**Active Directory Certificate Services**覈取方塊，然後按一下**Next**。



Add Roles Wizard

Select Server Roles

Select one or more roles to install on this server.

Roles:

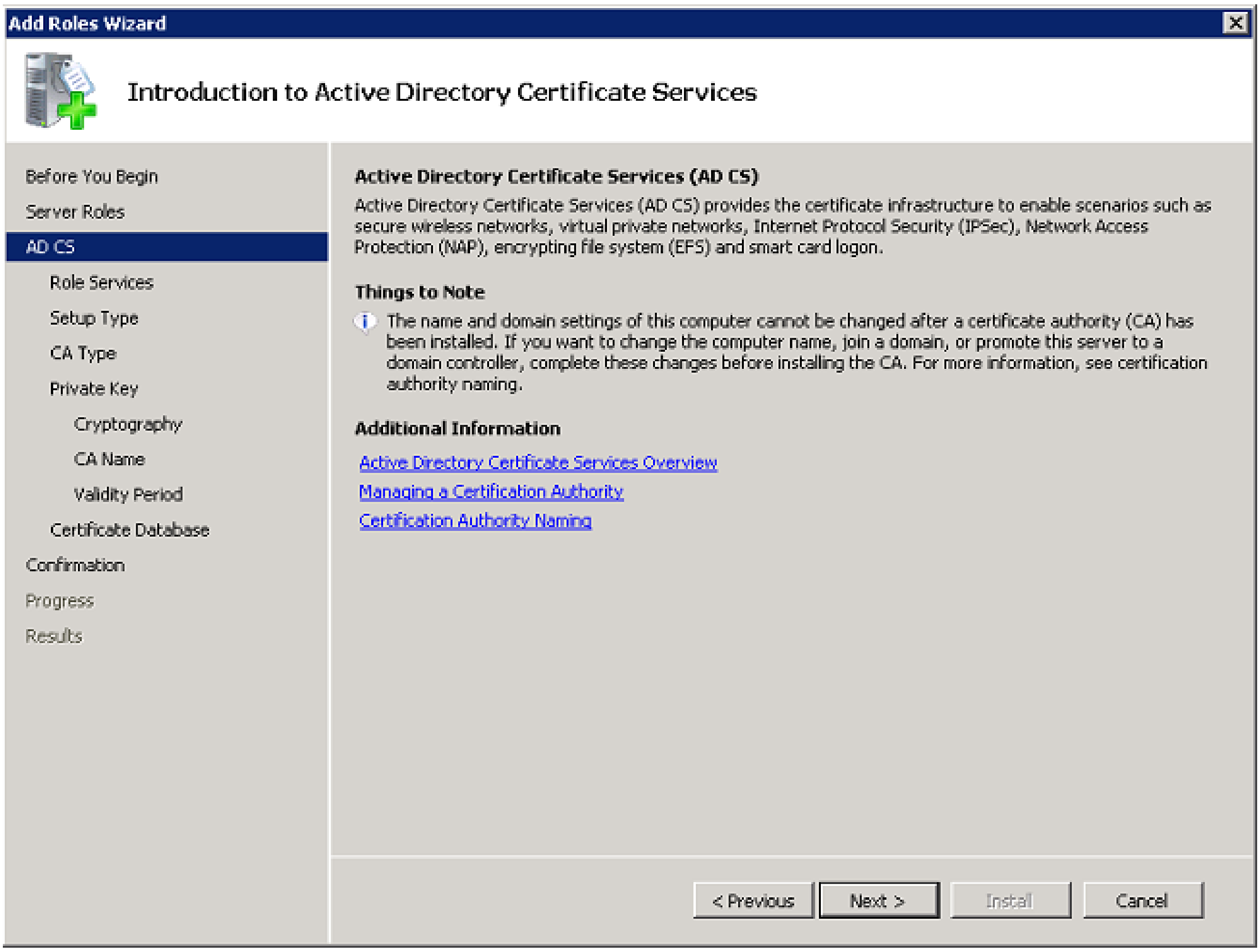
- ☑ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)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

4. 檢視**Active Directory證書服務簡介**，然後按一下**下一步**。



Active Directory Certificate Services (AD CS)

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

Things to Note

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

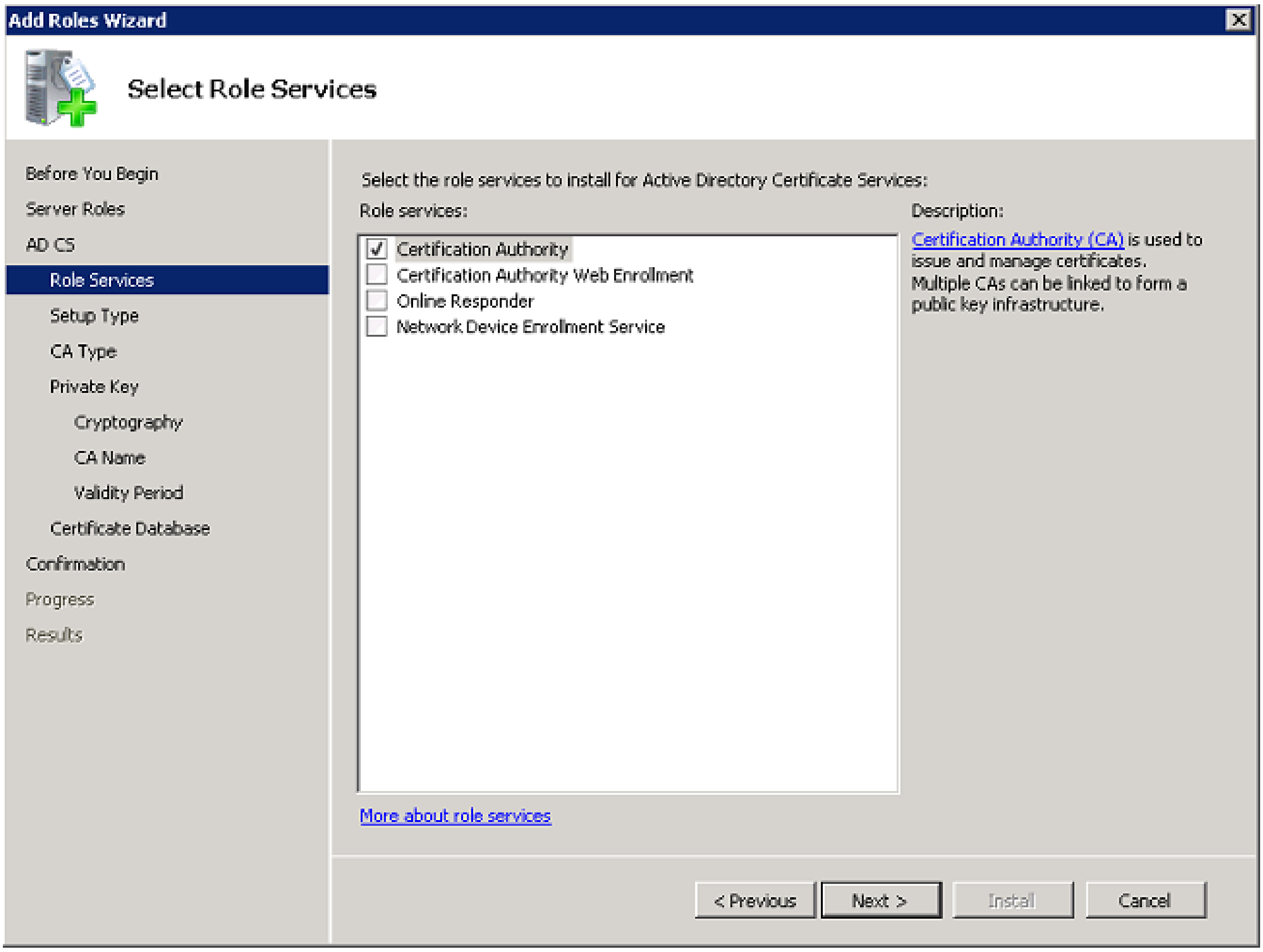
Additional Information

Active Directory Certificate Services Overview

Managing a Certification Authority

Certification Authority Naming

5. 選中**Certificate Authority**覈取方塊，然後按一下**Next**。



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

Role services:

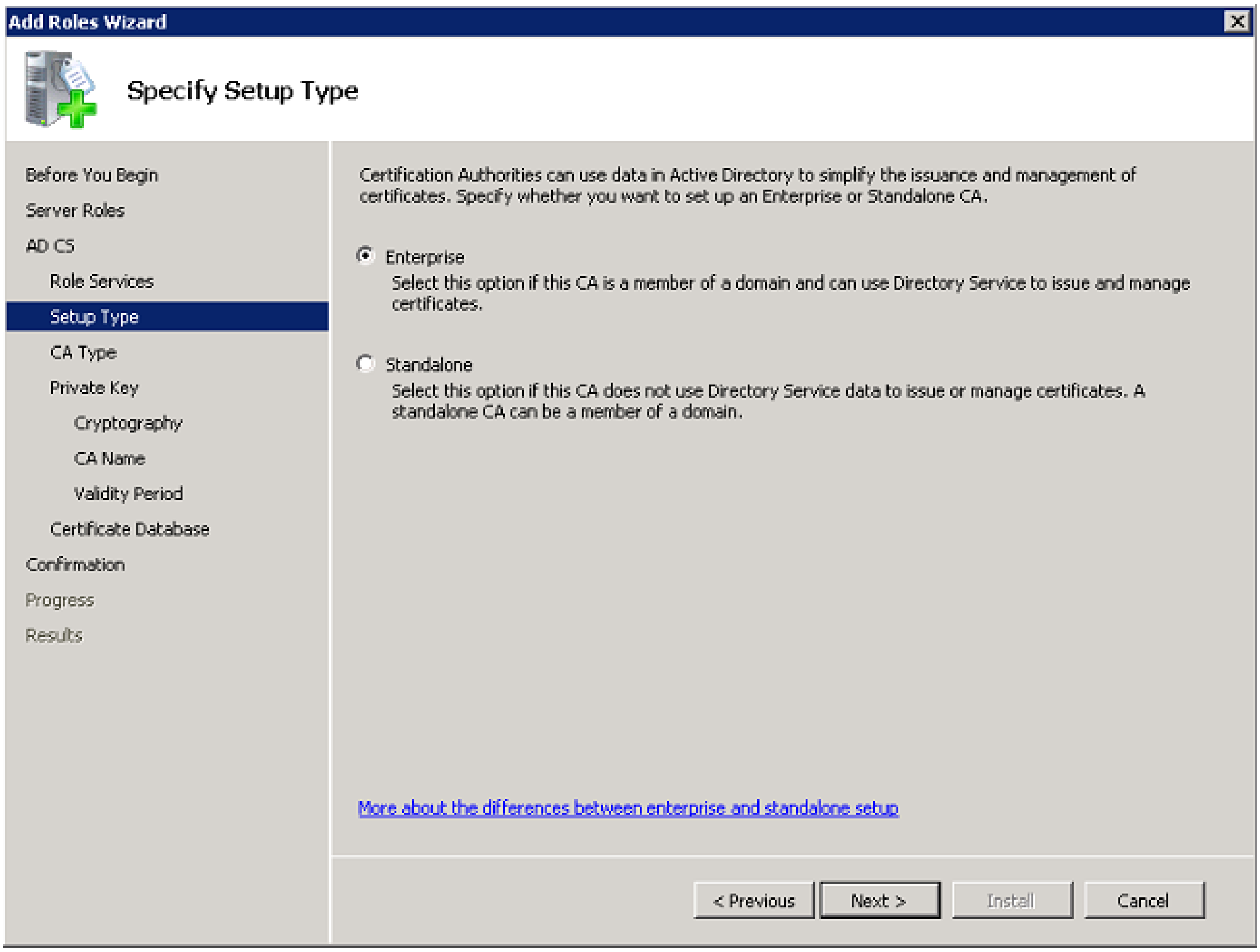
☑ Certification Authority
□ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service

Description:

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

More about role services

6. 按一下**Enterprise**單選按鈕，然後按一下**Next**。



Add Roles Wizard

Specify Setup Type

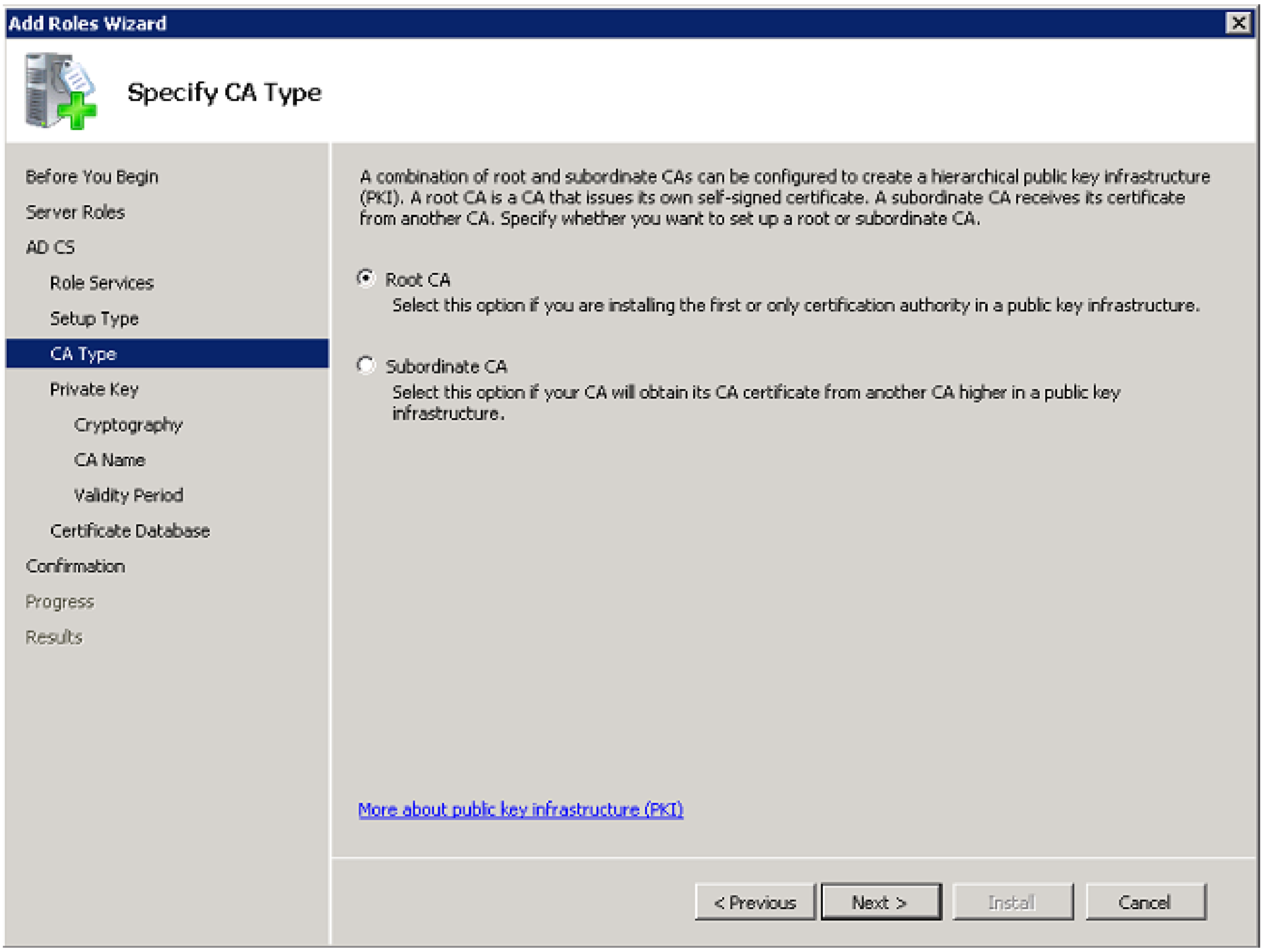
Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

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

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

More about the differences between enterprise and standalone setup

7. 按一下**根CA**單選按鈕，然後按一下**下一步**。

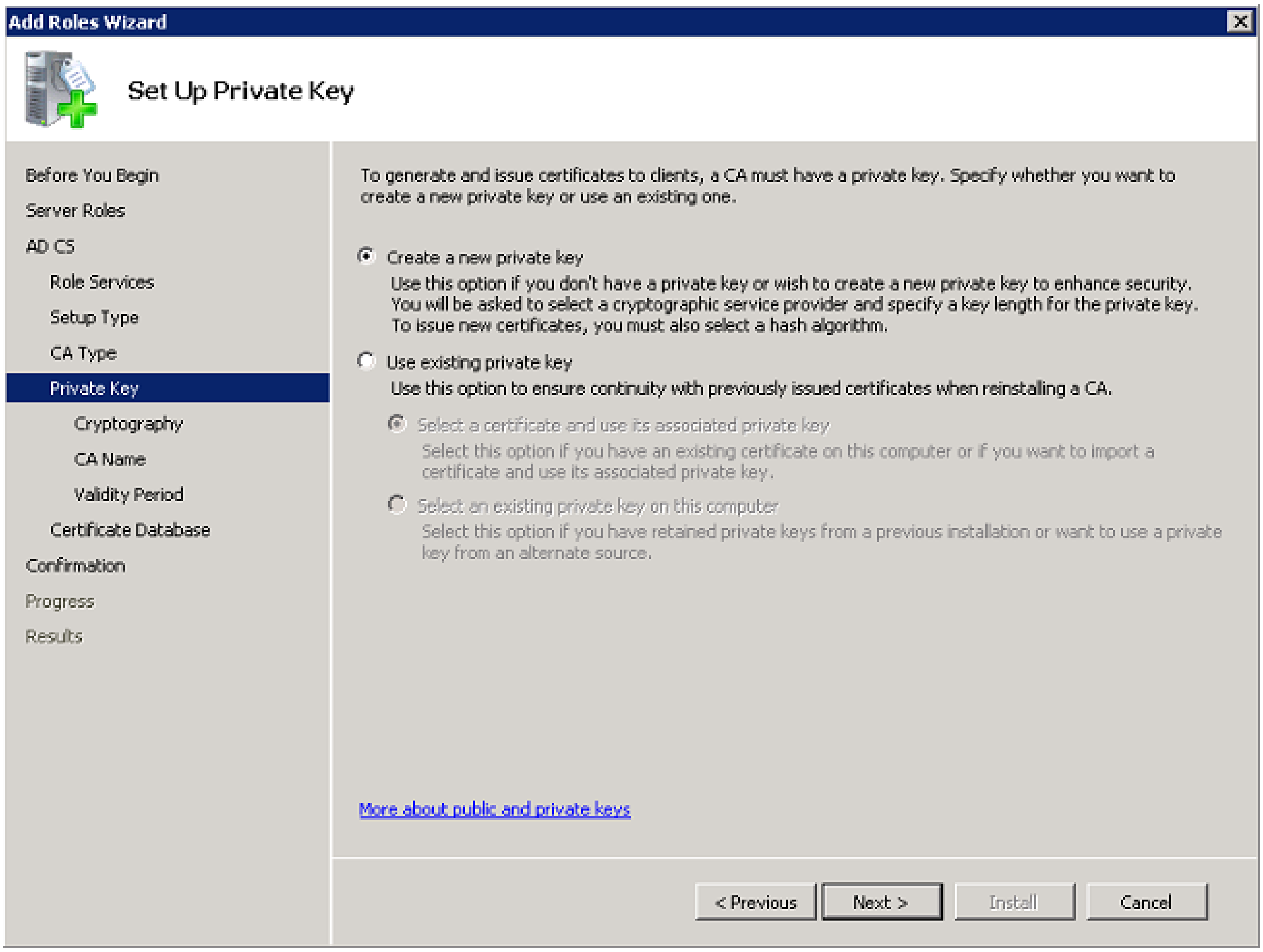


A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

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

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

8. 按一下**Create a new private key**單選按鈕，然後按一下**Next**。



Add Roles Wizard

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

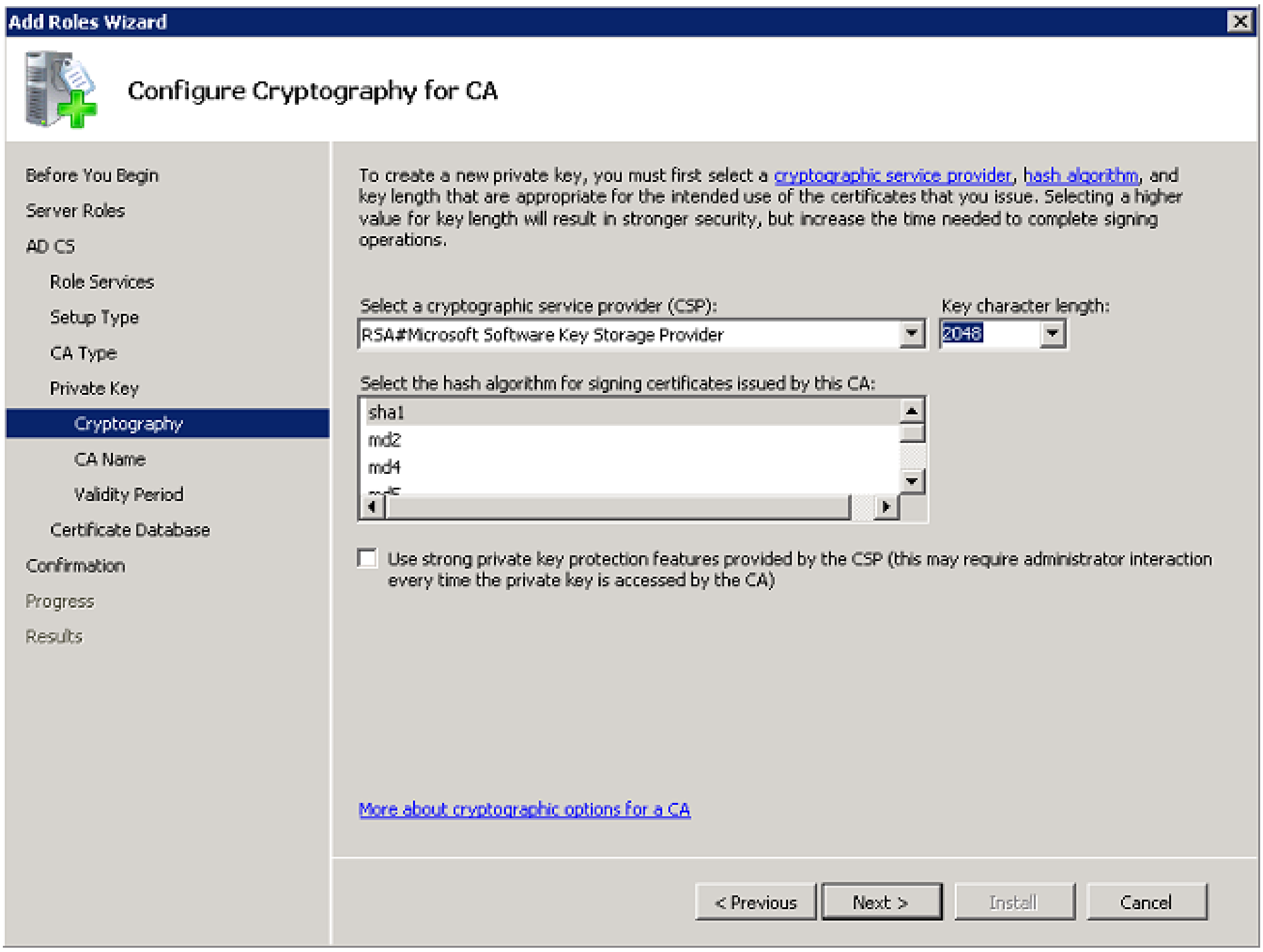
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ 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.

More about public and private keys

9. 在**Configuring Cryptography for CA**視窗中按一下**Next**。



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

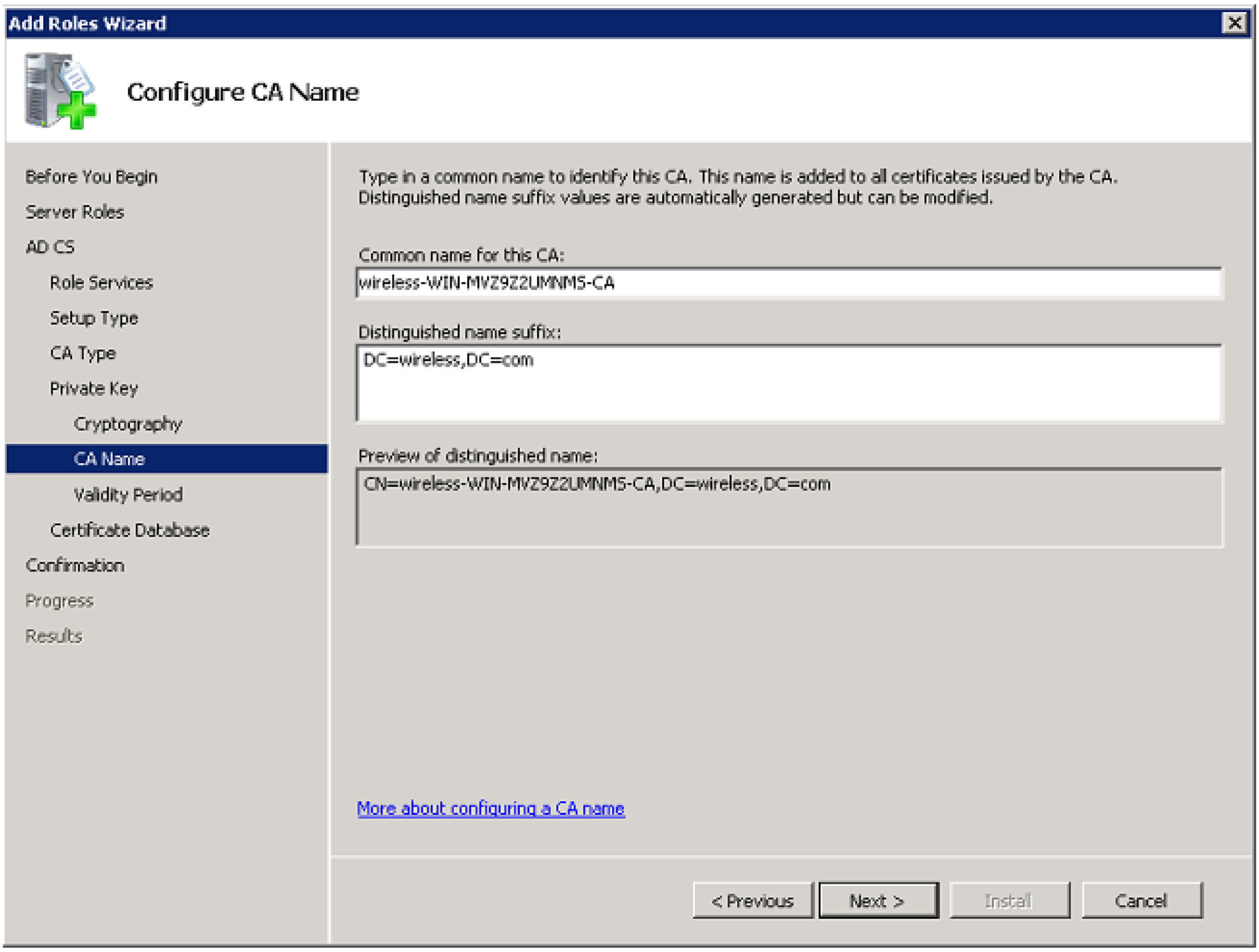
Select the hash algorithm for signing certificates issued by this CA:

sha1
md2
md4

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

More about cryptographic options for a CA

10. 按一下「**Next**」以接受此**CA預設名稱的公**用名稱。



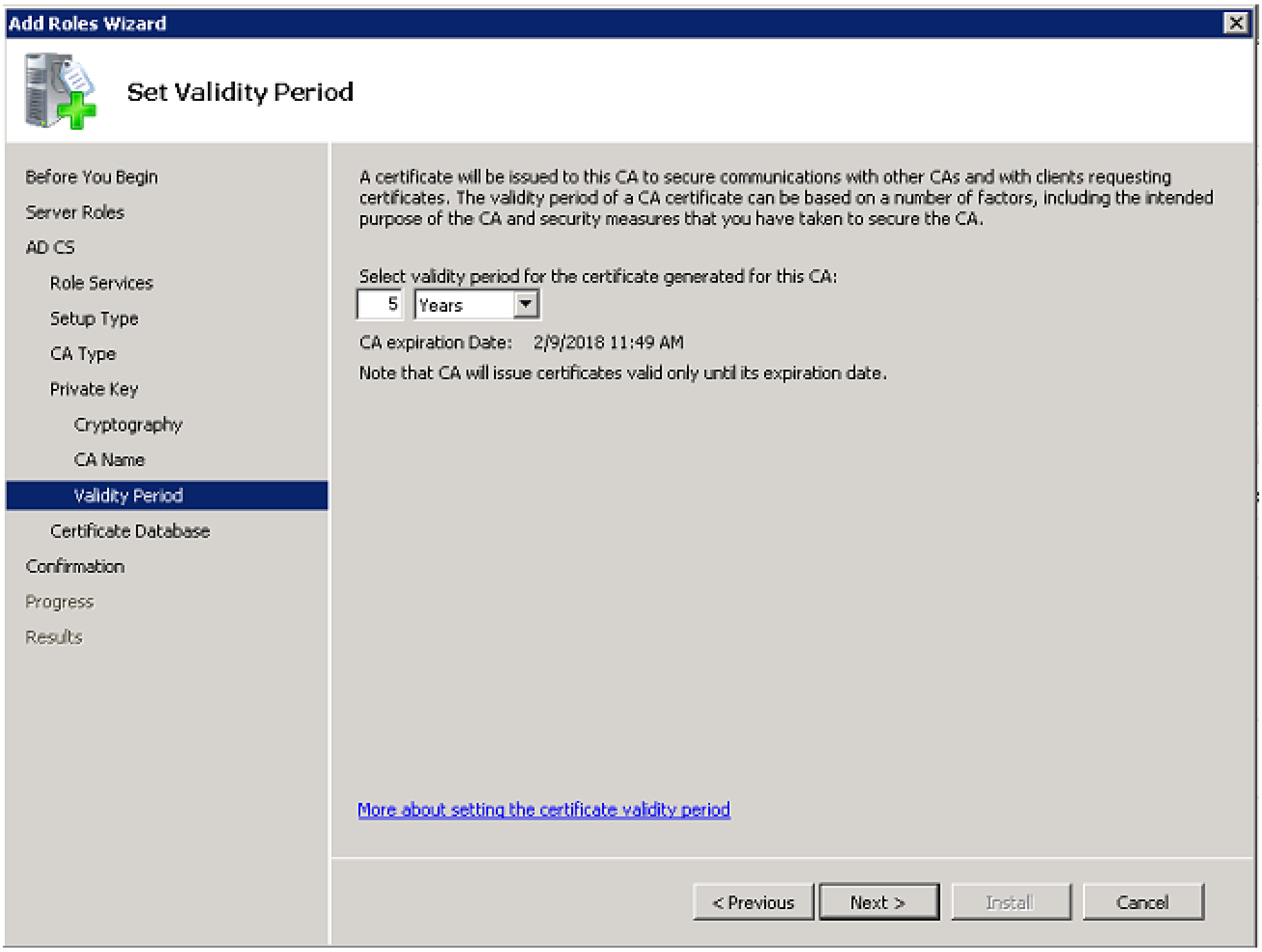
Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

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

Distinguished name suffix:
DC=wireless,DC=com

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

11. 選擇CA證書有效的時間長度，然後按一下**下一步**。



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

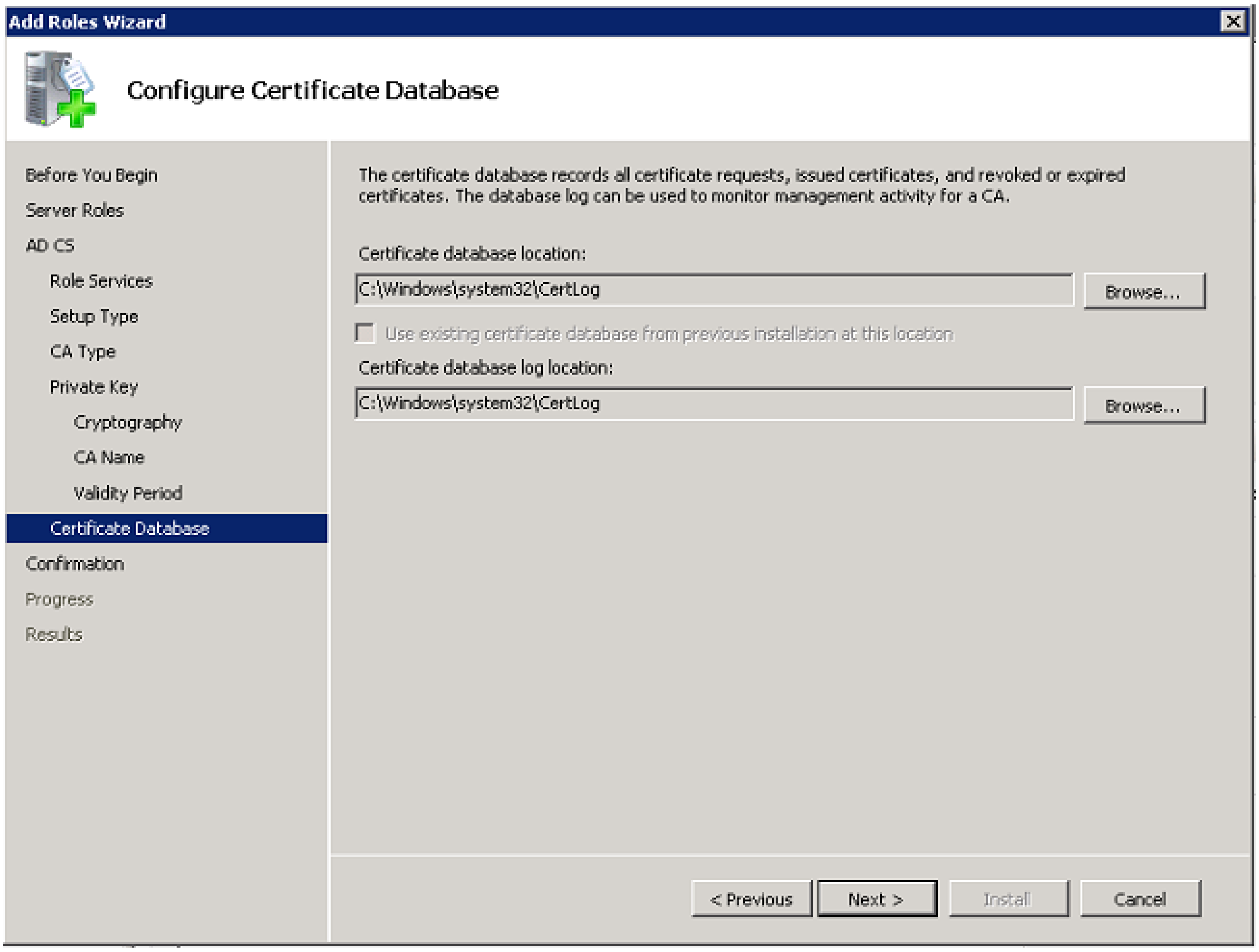
Select validity period for the certificate generated for this CA:

5 Years

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

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

12. 按一下**Next**以接受**Certificate database location**預設位置。



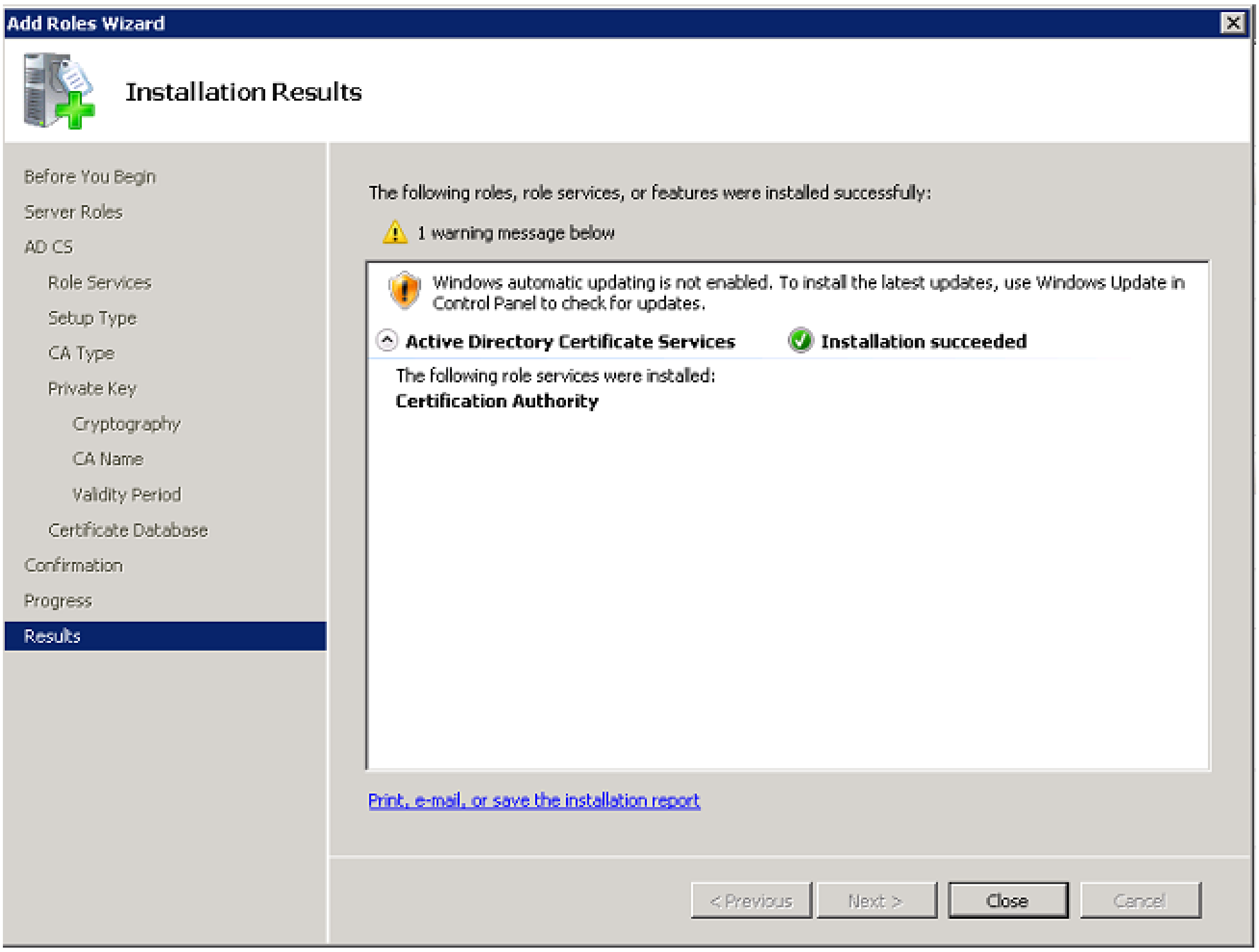
The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.

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

□ Use existing certificate database from previous installation at this location

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

13. 檢查配置並按一下**安裝**以開始**Active Directory證書服務**。



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

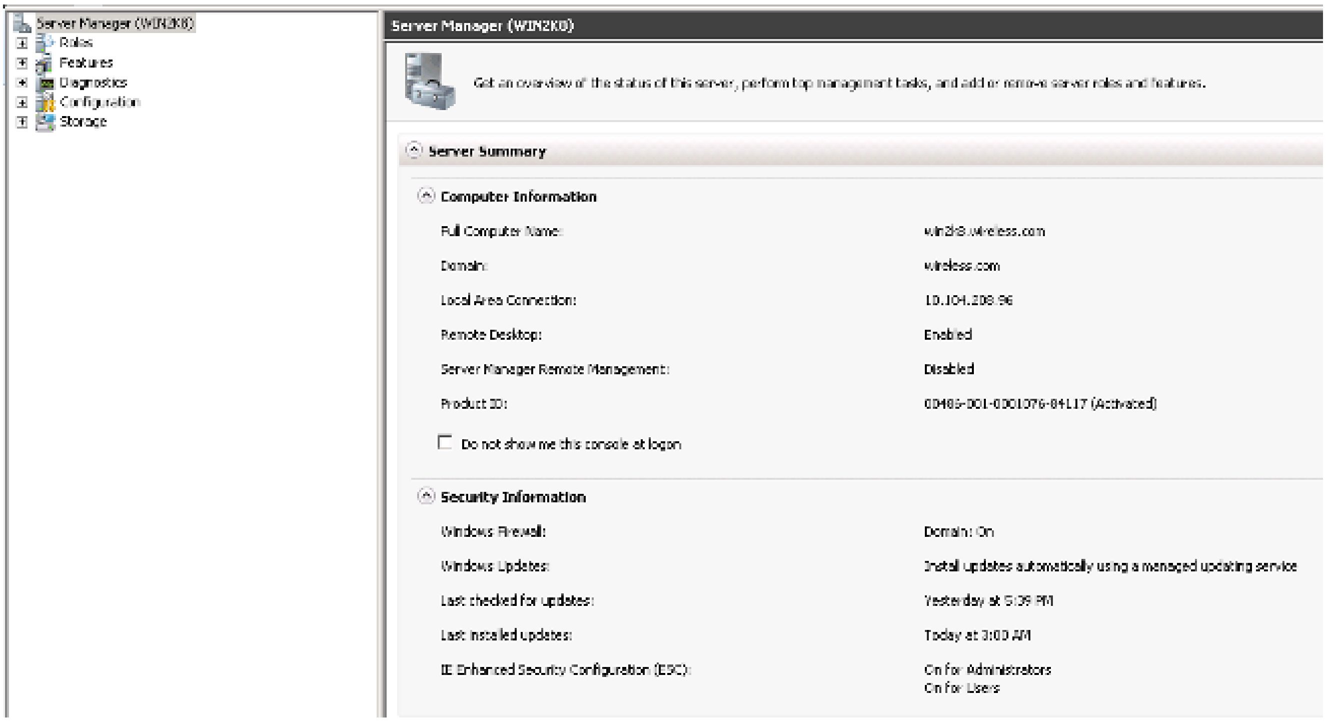
14. 安裝完成後，按一下「**Close**」。

在Microsoft Windows Version 2008 Server上安裝NPS

> **附註**：通過本節所述的設定，NPS用作RADIUS伺服器，以便使用PEAP身份驗證對無線客戶端進行身份驗證。

完成以下步驟，以便在Microsoft Windows Version 2008伺服器上安裝和配置NPS:

1. 導航到**開始** > **Server Manager** > Roles > **Add Roles**。



Server Manager (WIN2K8)

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

Server Summary

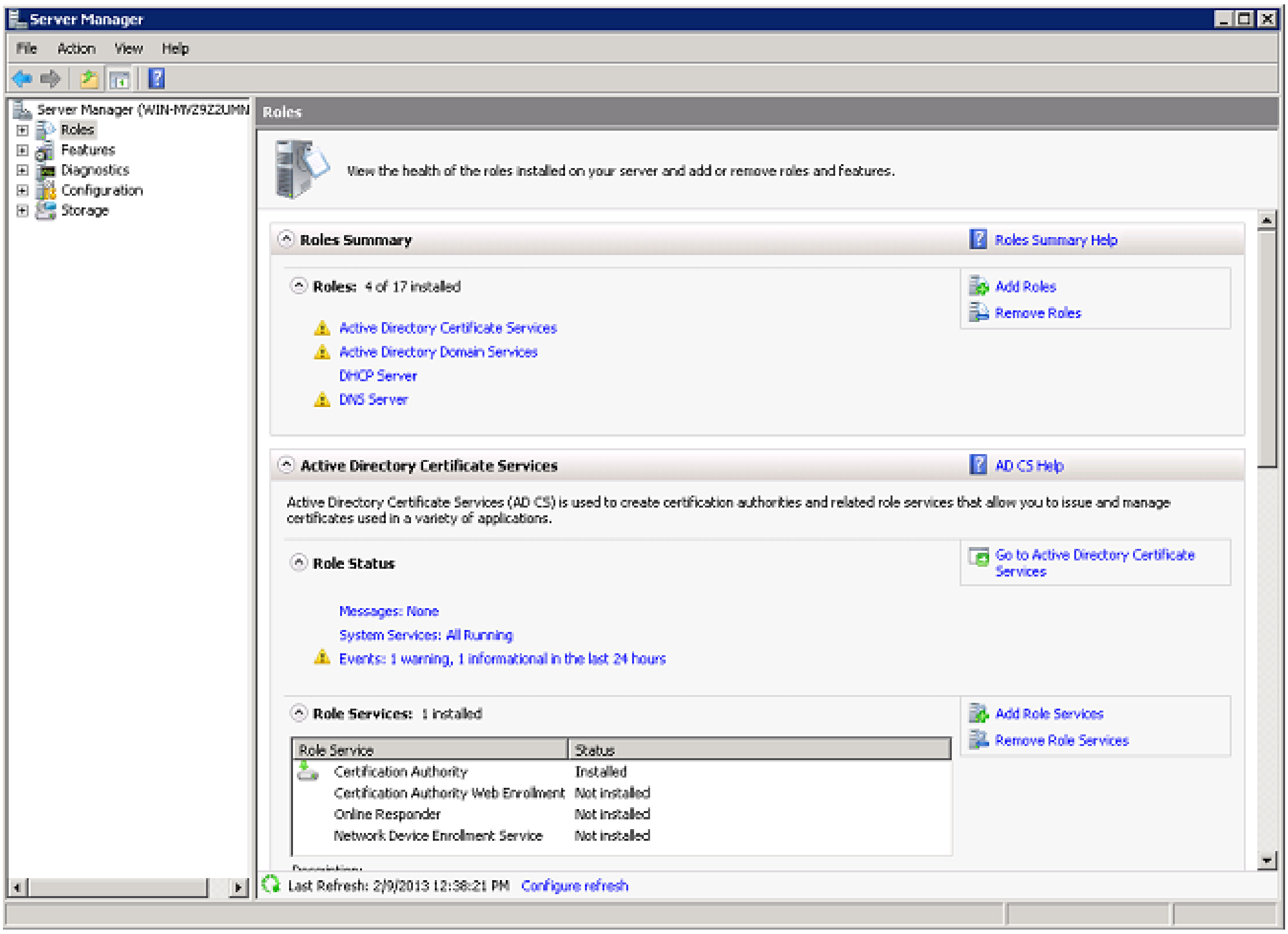
Computer Information

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

□ Do not show me this console at logon

Security Information

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



Roles

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

Roles Summary

Roles: 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

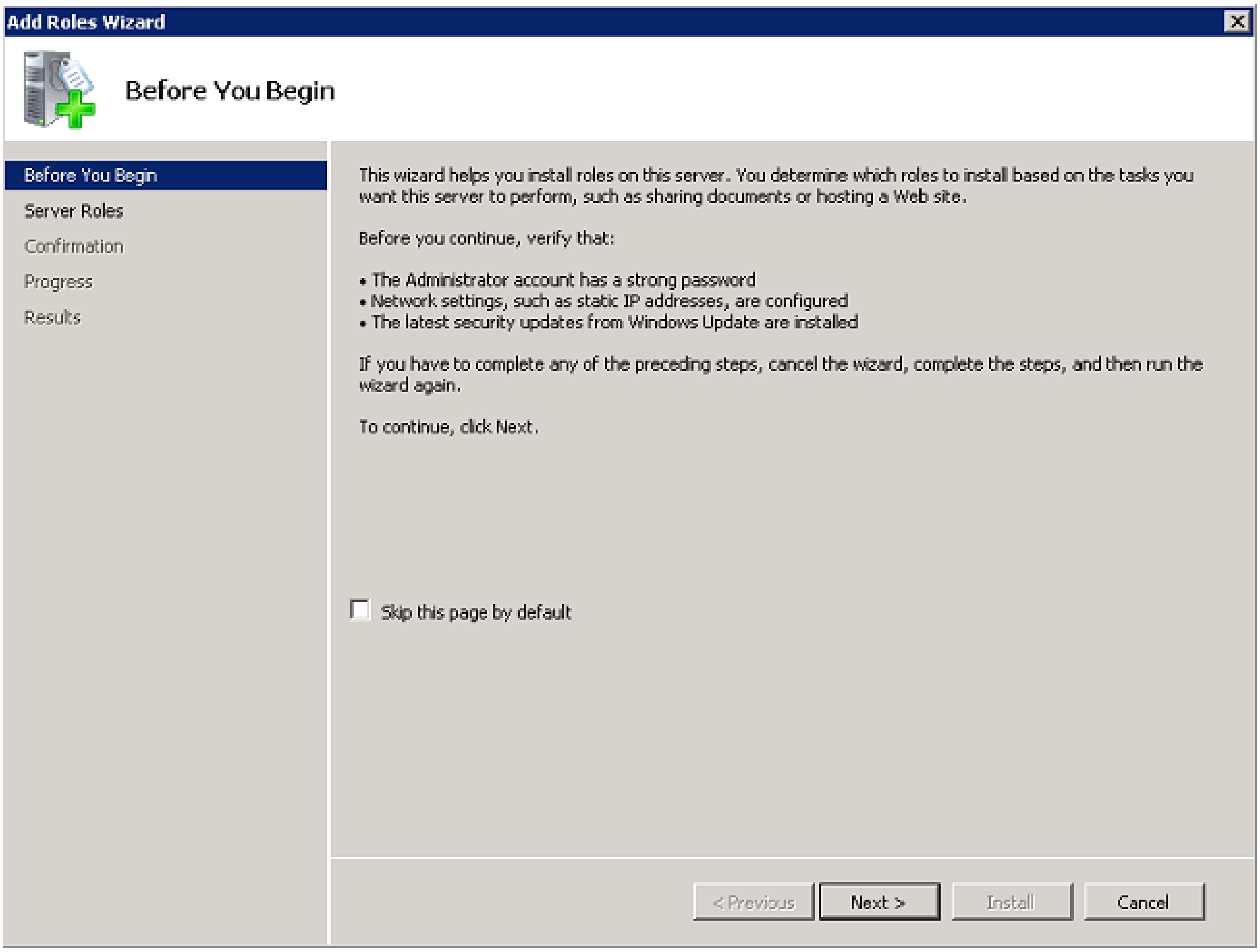
Events: 1 warning, 1 informational in the last 24 hours

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

2. 按「**Next**」（下一步）。



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

Before you continue, verify that:

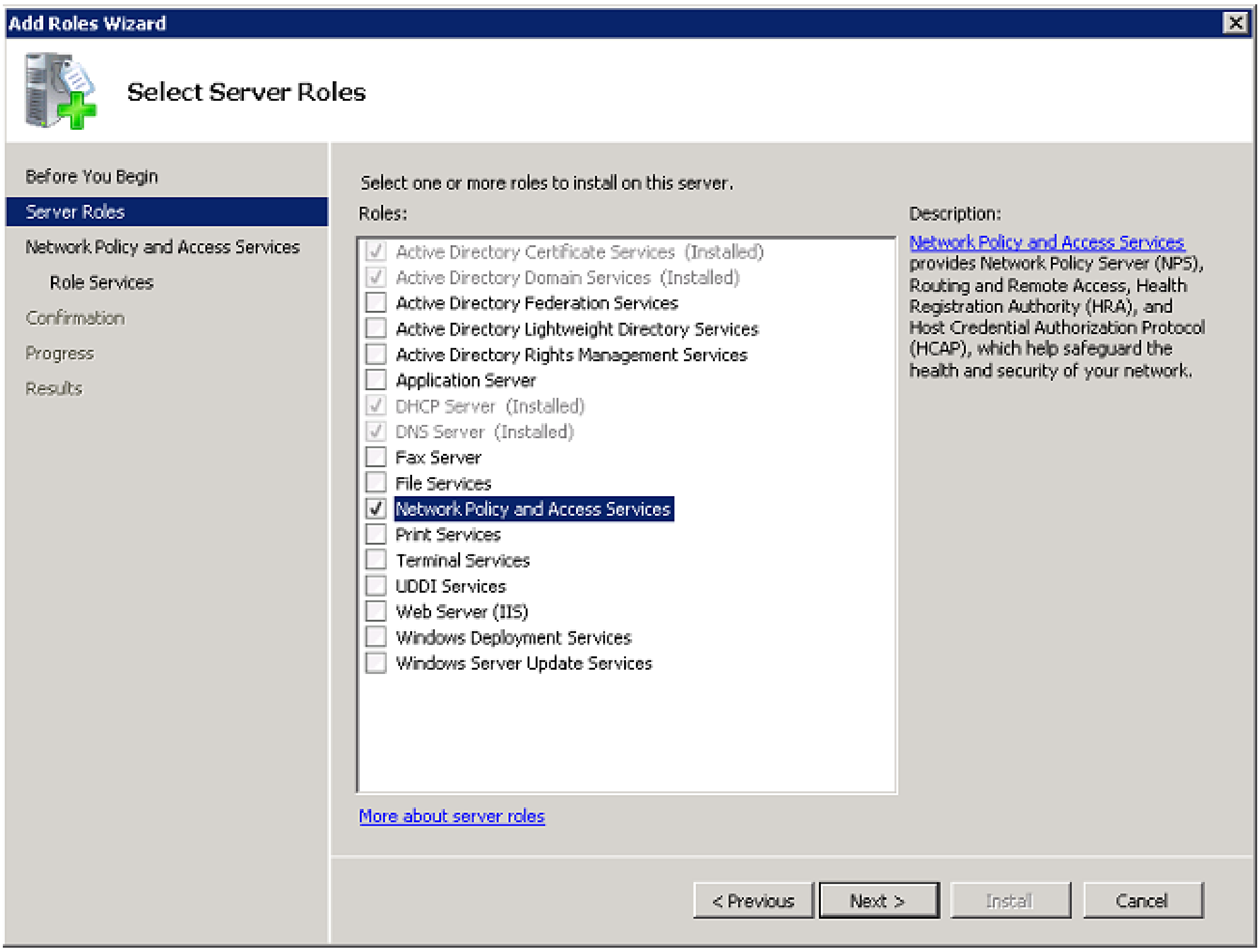
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

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

To continue, click Next.

□ Skip this page by default

3. 選中**Network Policy and Access Services**覈取方塊，然後按一下**Next**。



Add Roles Wizard

Select Server Roles

Select one or more roles to install on this server.

Roles:

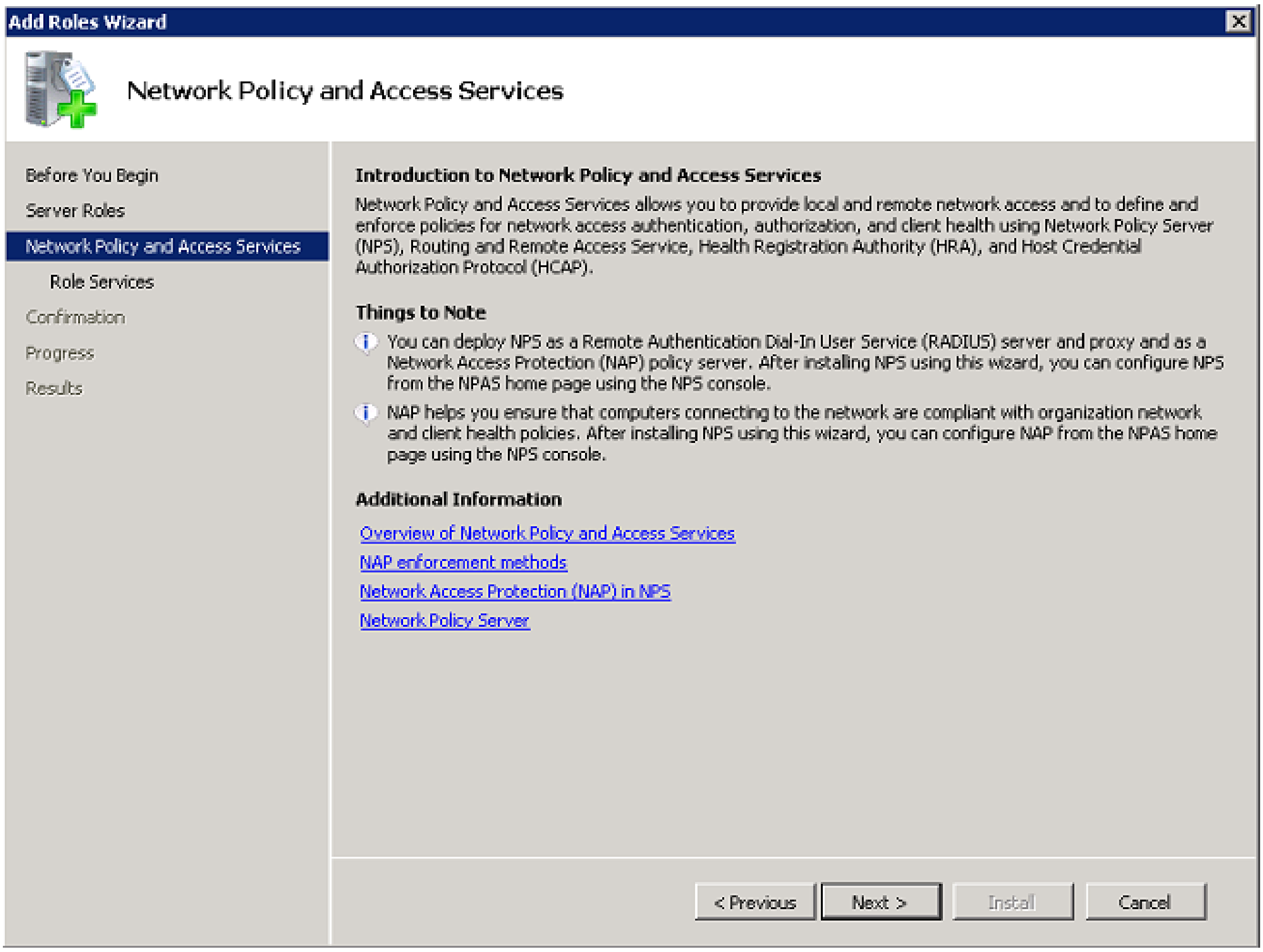
- ☑ Active Directory Certificate Services (Installed)
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS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

Description:

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

More about server roles

4. 檢視**Introduction to Network Policy and Access Services**，然後按一下**Next**。



Introduction to Network Policy and Access Services

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

Things to Note

You can deploy NPS as a Remote Authentication Dial-In User Service (RADIUS) server and proxy and as a Network Access Protection (NAP) policy server. After installing NPS using this wizard, you can configure NPS from the NPAS home page using the NPS console.

NAP helps you ensure that computers connecting to the network are compliant with organization network and client health policies. After installing NPS using this wizard, you can configure NAP from the NPAS home page using the NPS console.

Additional Information

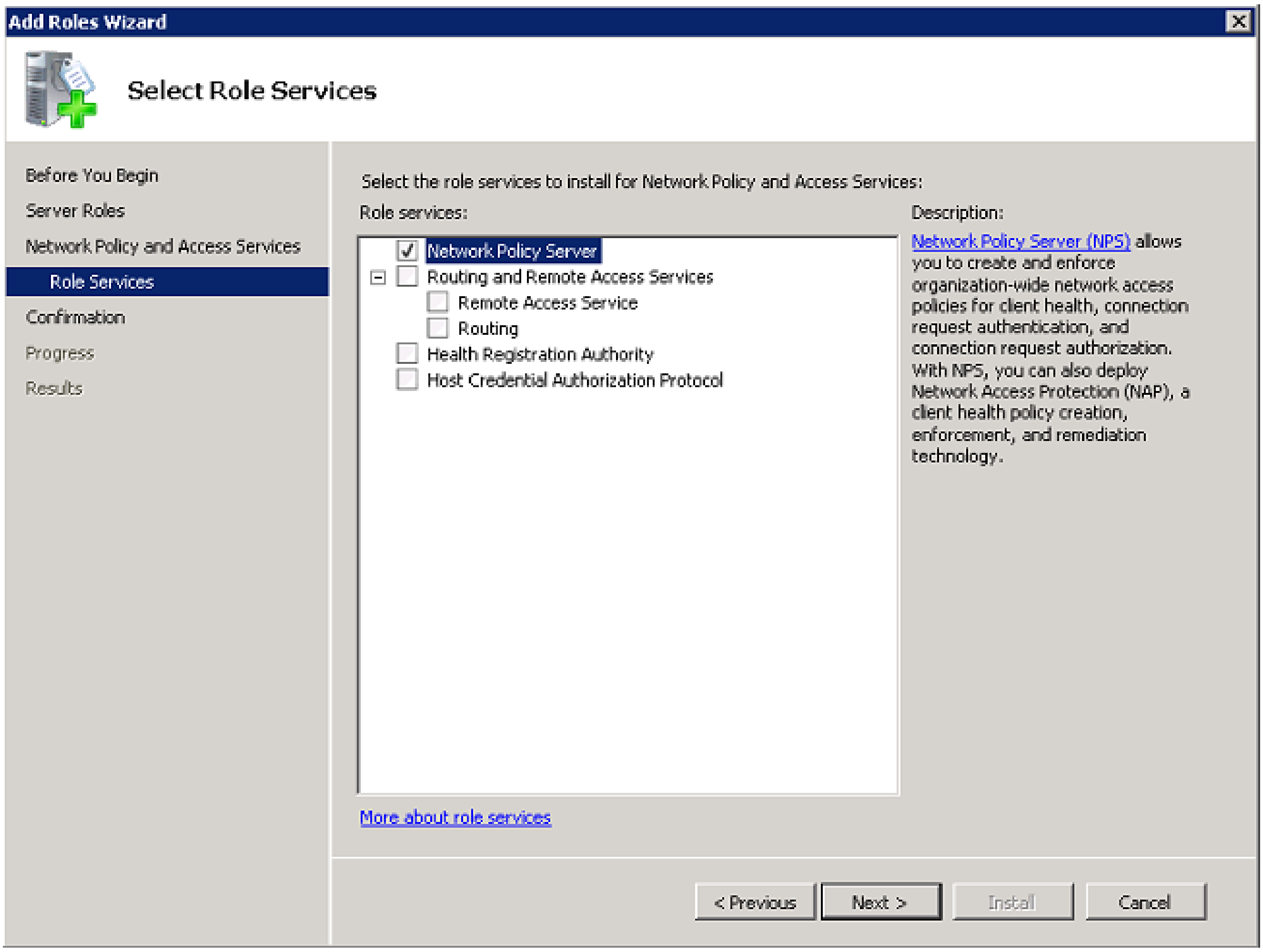
Overview of Network Policy and Access Services

NAP enforcement methods

Network Access Protection (NAP) in NPS

Network Policy Server

5. 選中**Network Policy Server**覈取方塊，然後按一下**Next**。



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

Role services:

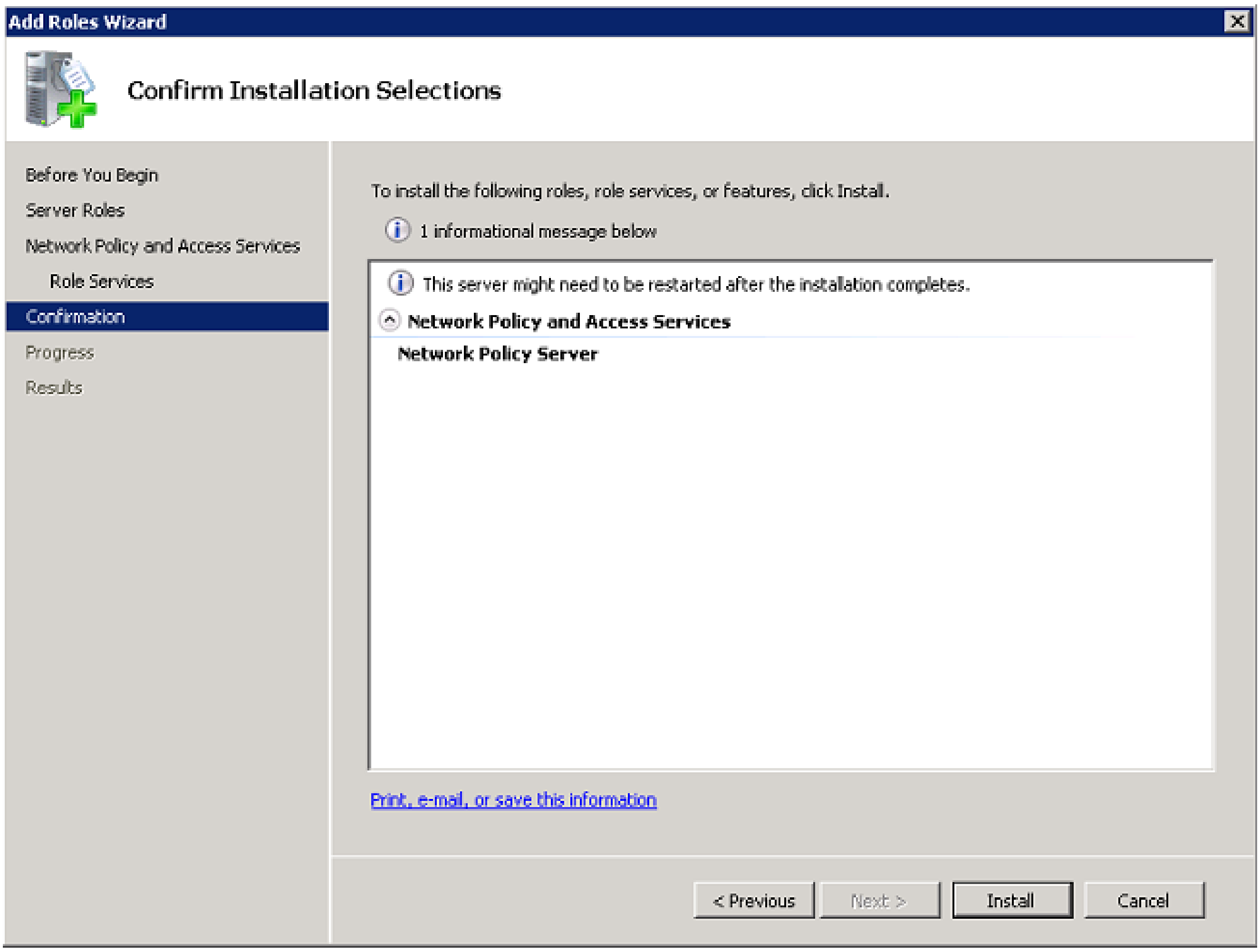
- ☑ Network Policy Server
- ☐ Routing and Remote Access Services
  - ☐ Remote Access Service
  - ☐ Routing
- ☐ Health Registration Authority
- ☐ Host Credential Authorization Protocol

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.

More about role services

6. 檢視確認資訊，然後按一下**安裝**。



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

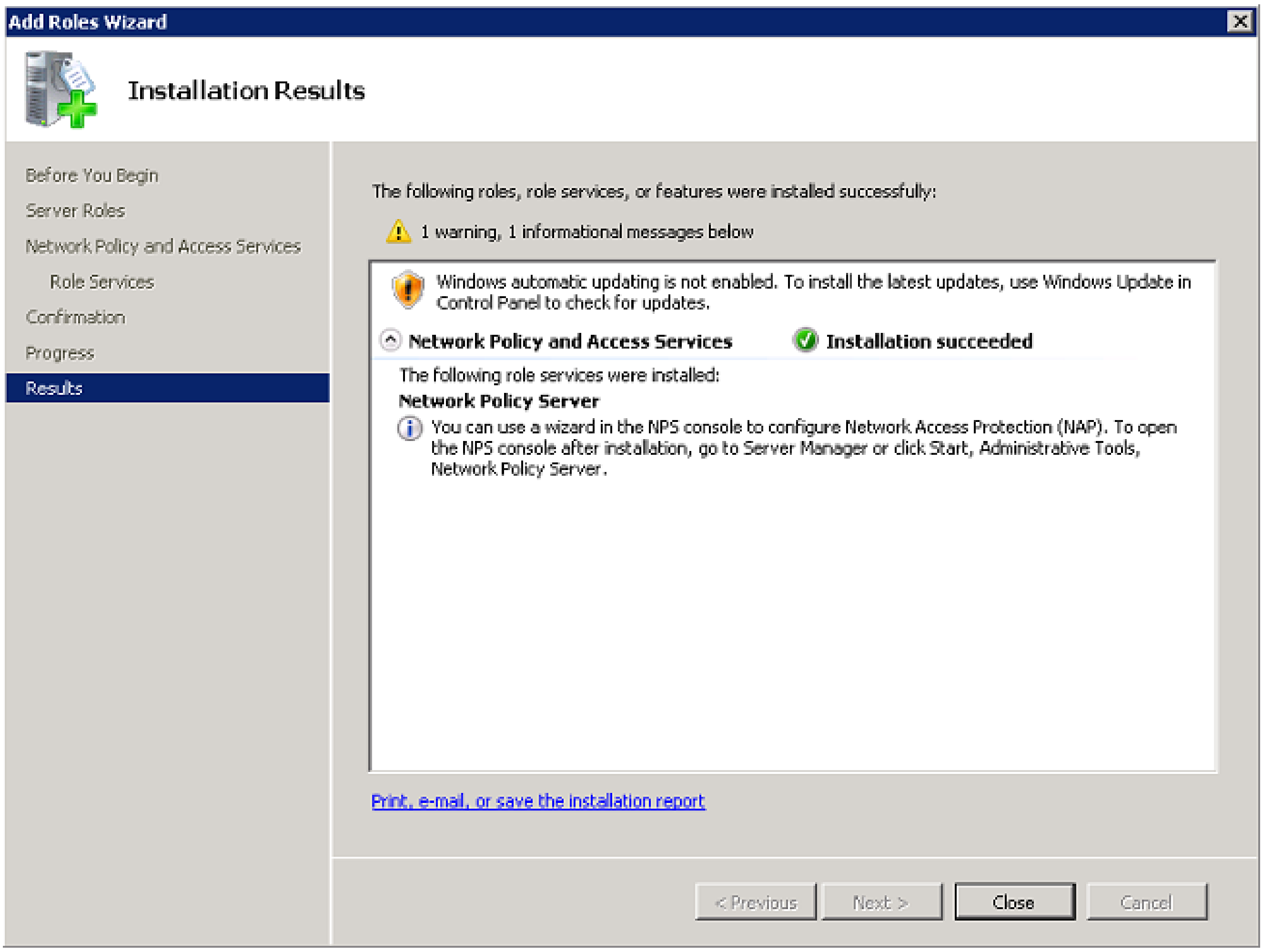
1 informational message below

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

Network Policy and Access Services

Network Policy Server

安裝完成後，將出現一個類似以下的螢幕：



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

7. 按一下「**Close**」。

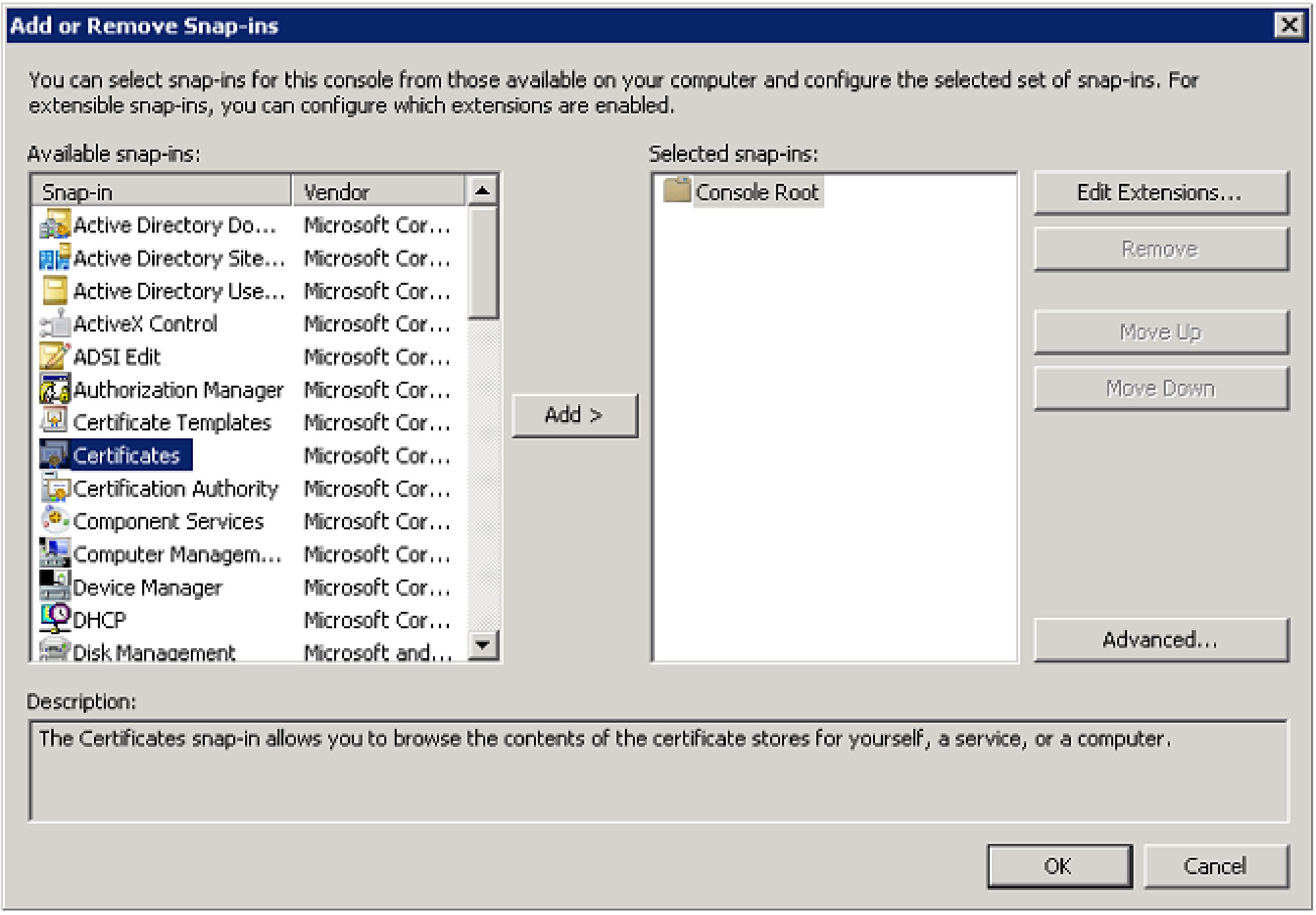
安裝證書

要安裝NPS的電腦證書，請完成以下步驟：

1. 按一下**Start**，輸入Microsoft Management Console(MMC)，然後按**Enter**。

2. 導航到**檔案**> **新增/刪除管理單元。**

3. 選擇「**Certificates**」，然後按一下「**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...

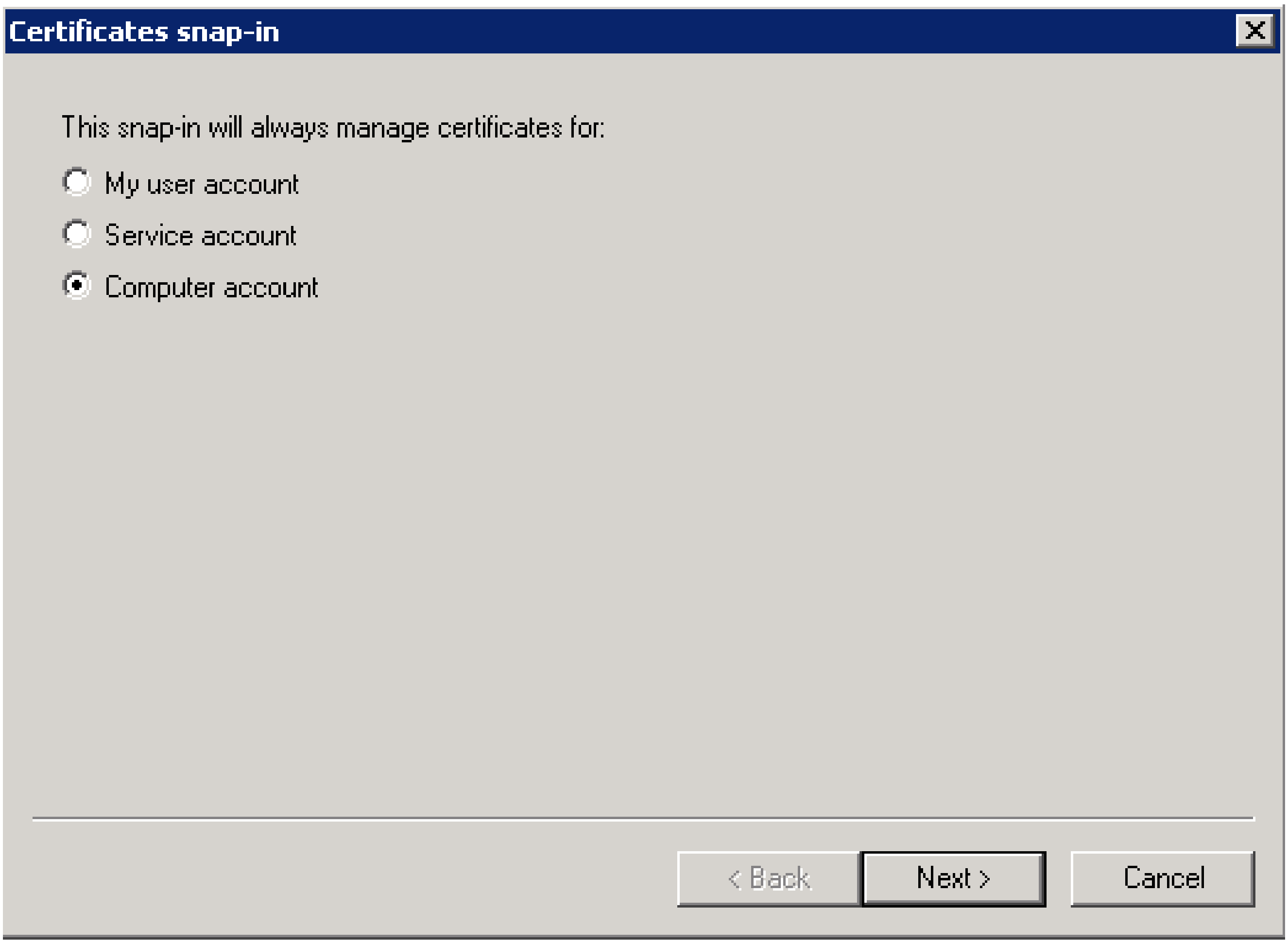
Selected snap-ins:

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. 按一下**Computer account**單選按鈕，然後按一下**Next**。



Certificates snap-in

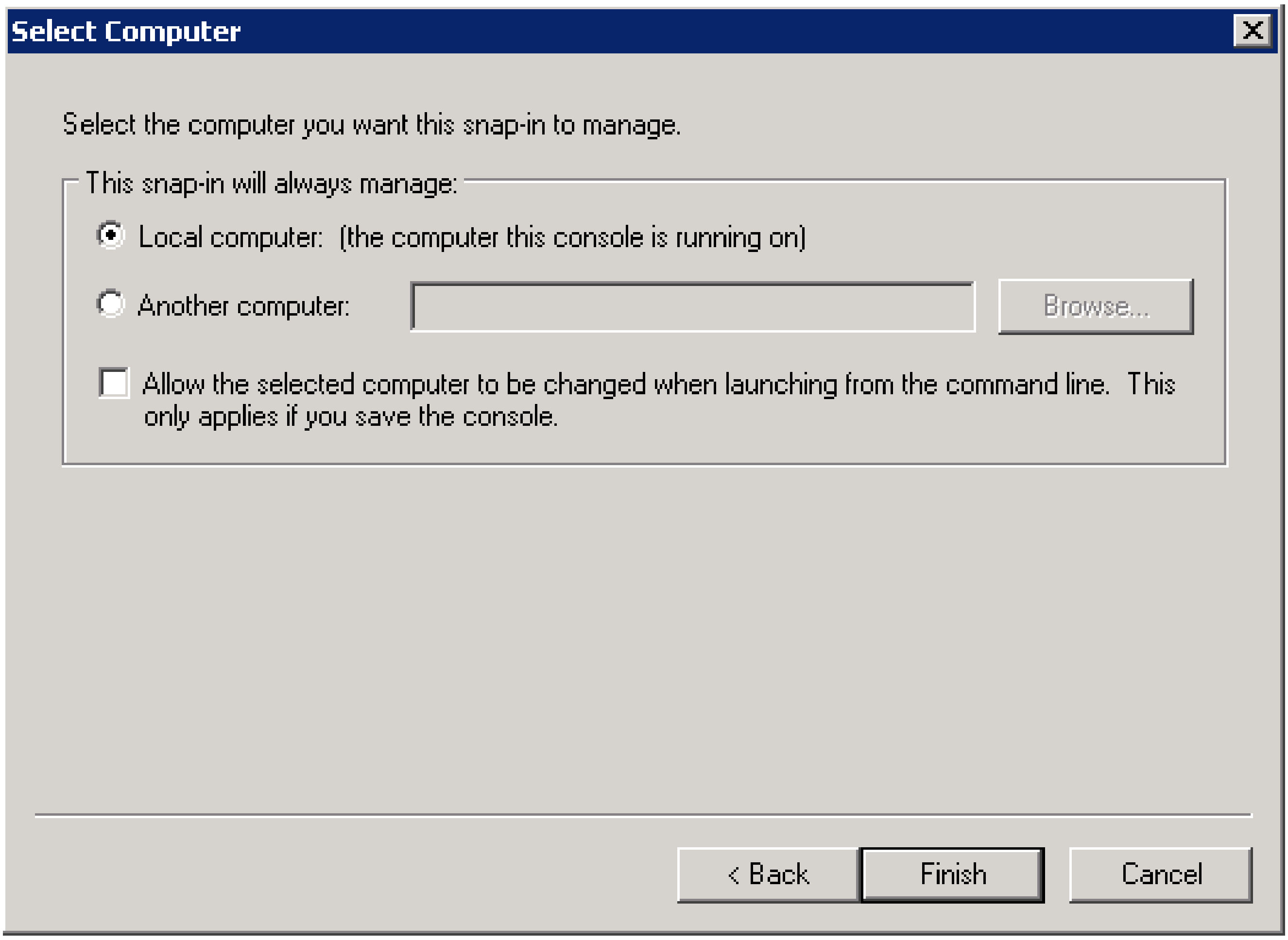
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

5. 按一下**Local Computer**單選按鈕，然後按一下**Finish**。



Select Computer

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

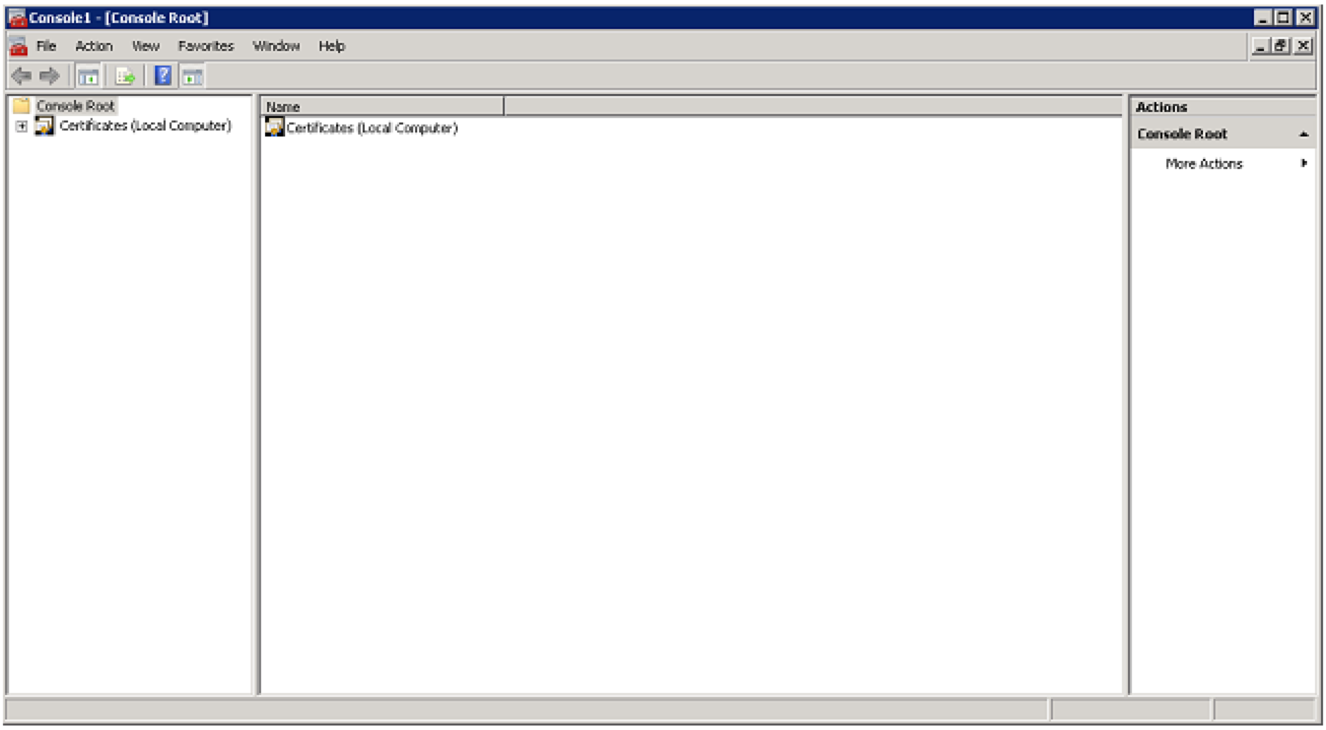
This snap-in will always manage:

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

○ Another computer:

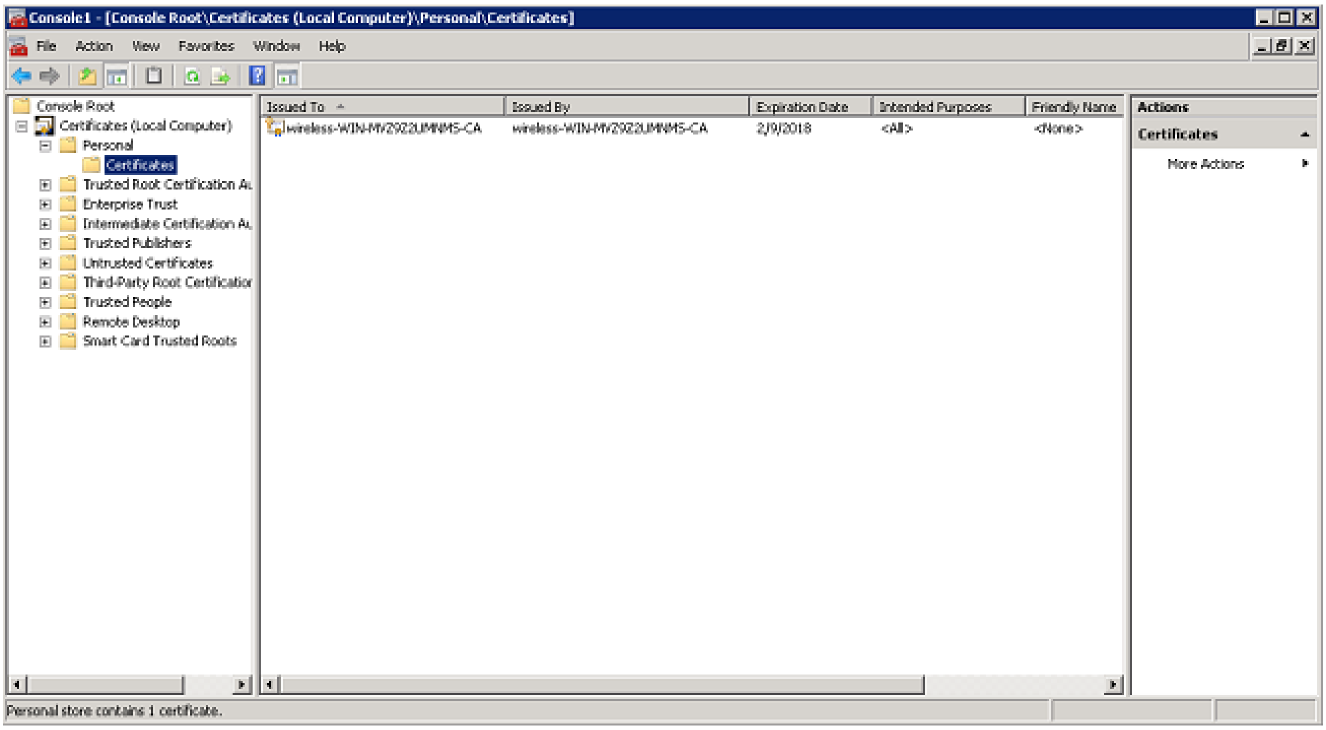
□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

6. 按一下**OK**以返回到MMC。



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

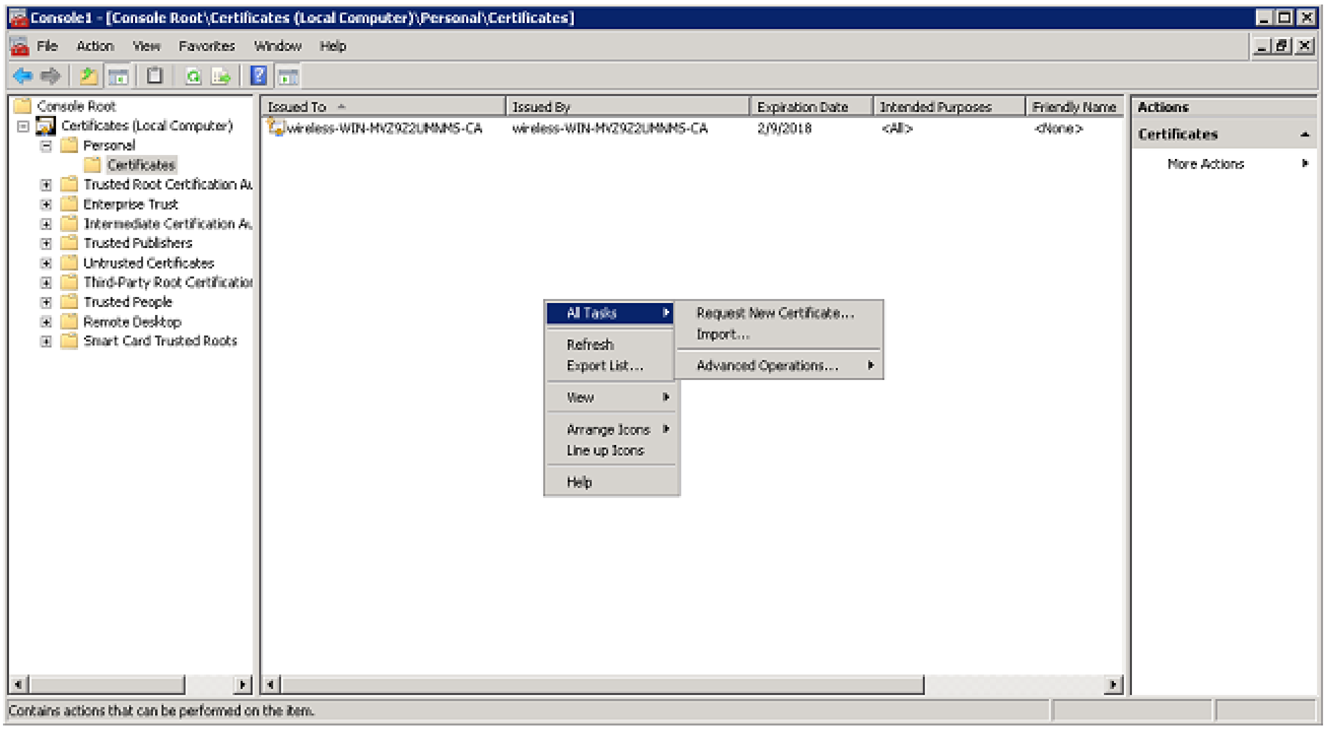
7. 展開**Certificates(Local Computer)**和**Personal**資料夾，然後按一下**Certificates**。



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

Personal store contains 1 certificate.

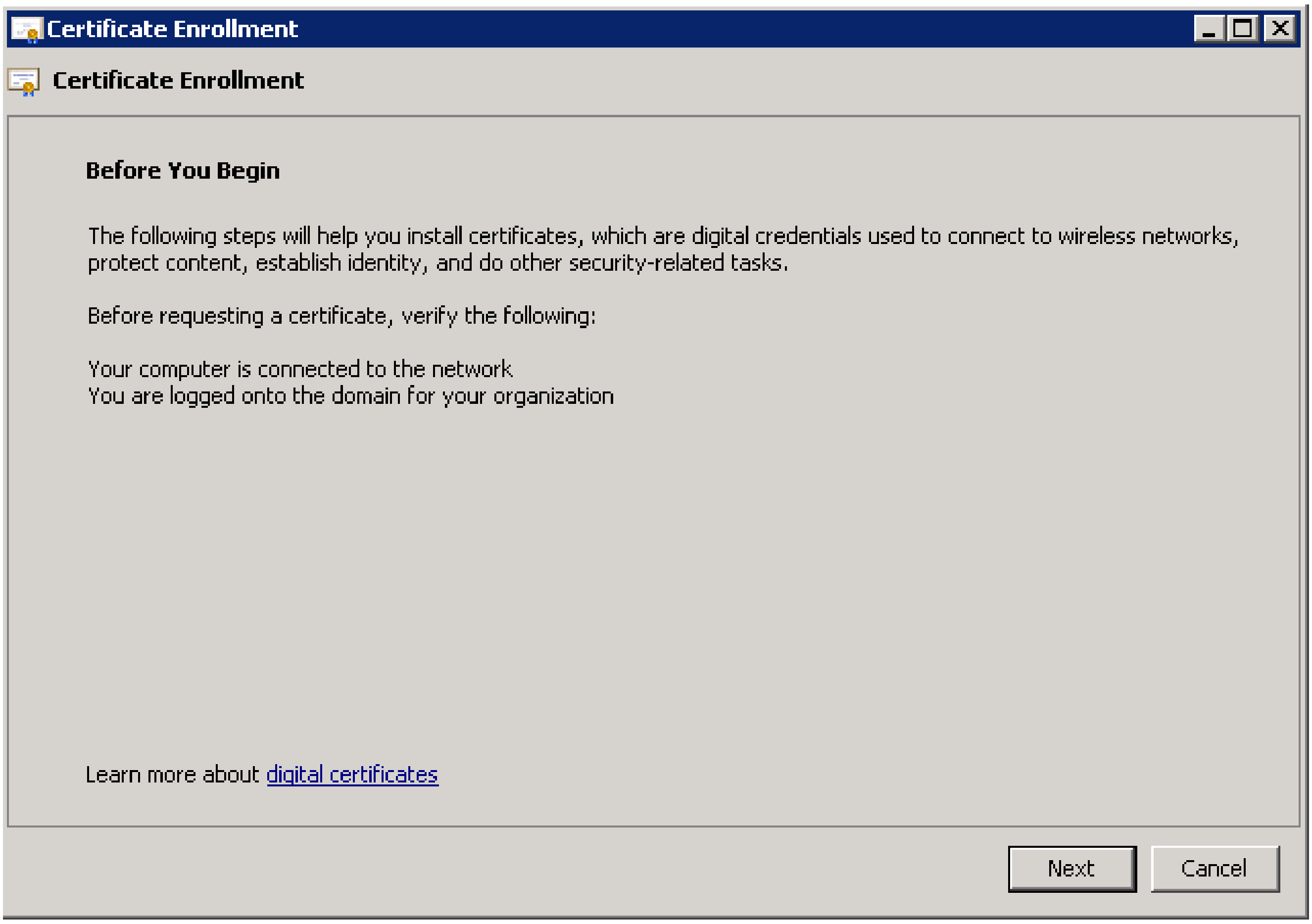
8. 按一下右鍵CA證書中的空白，然後選擇**所有任務** >**請求新證書**。



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

Contains actions that can be performed on the item.

9. 按「**Next**」（下一步）。



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.

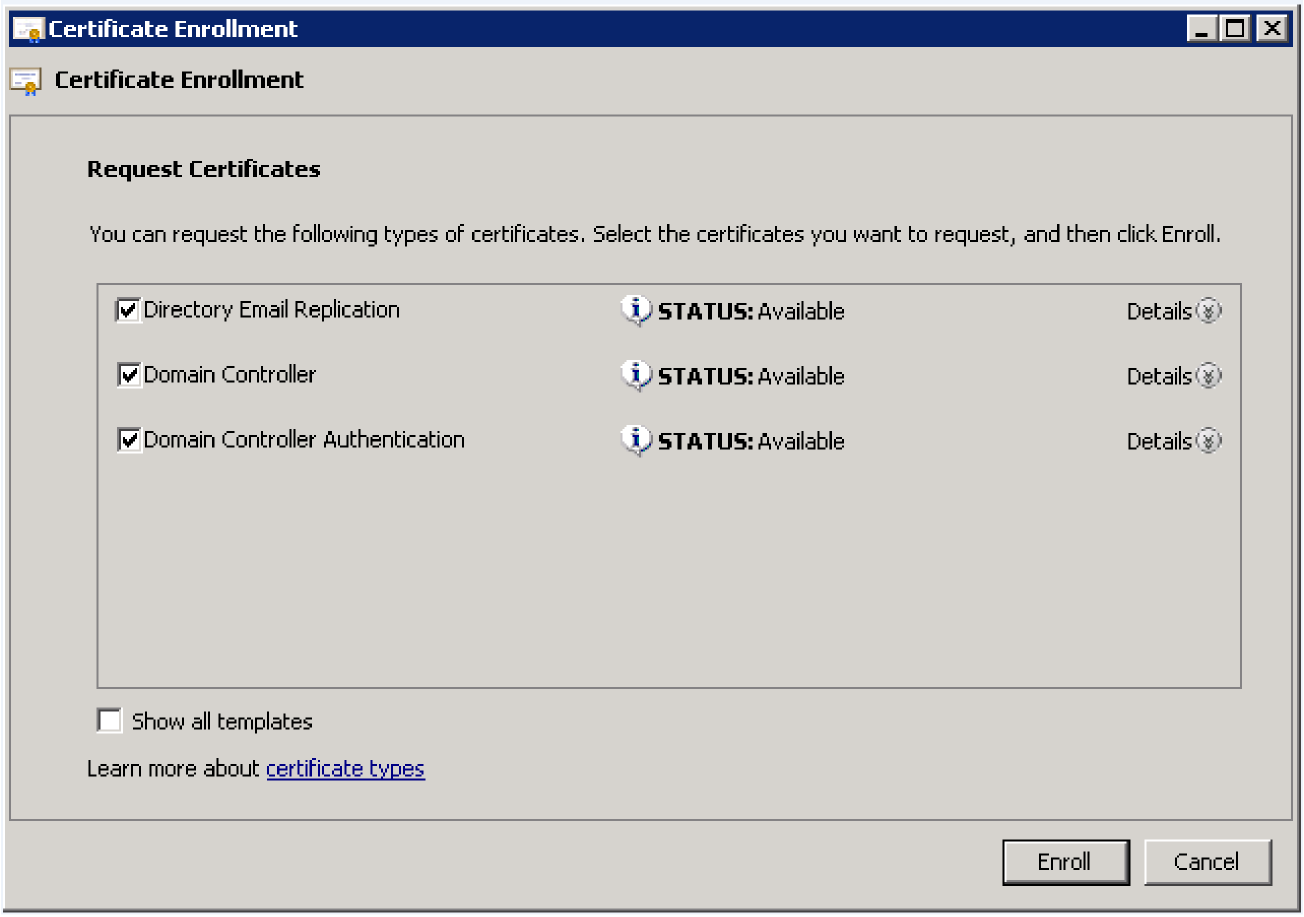
Before requesting a certificate, verify the following:

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

Learn more about digital certificates

10. 按一下**Domain Controller**覈取方塊，然後按一下**Enroll**。

    附註：如果客戶端身份驗證由於EAP證書錯誤而失敗，則在按一下**Enroll**之前，請確保此**Certificate Enrollment**頁面上選中了所有覈取方塊。這會產生大約三個憑證。



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

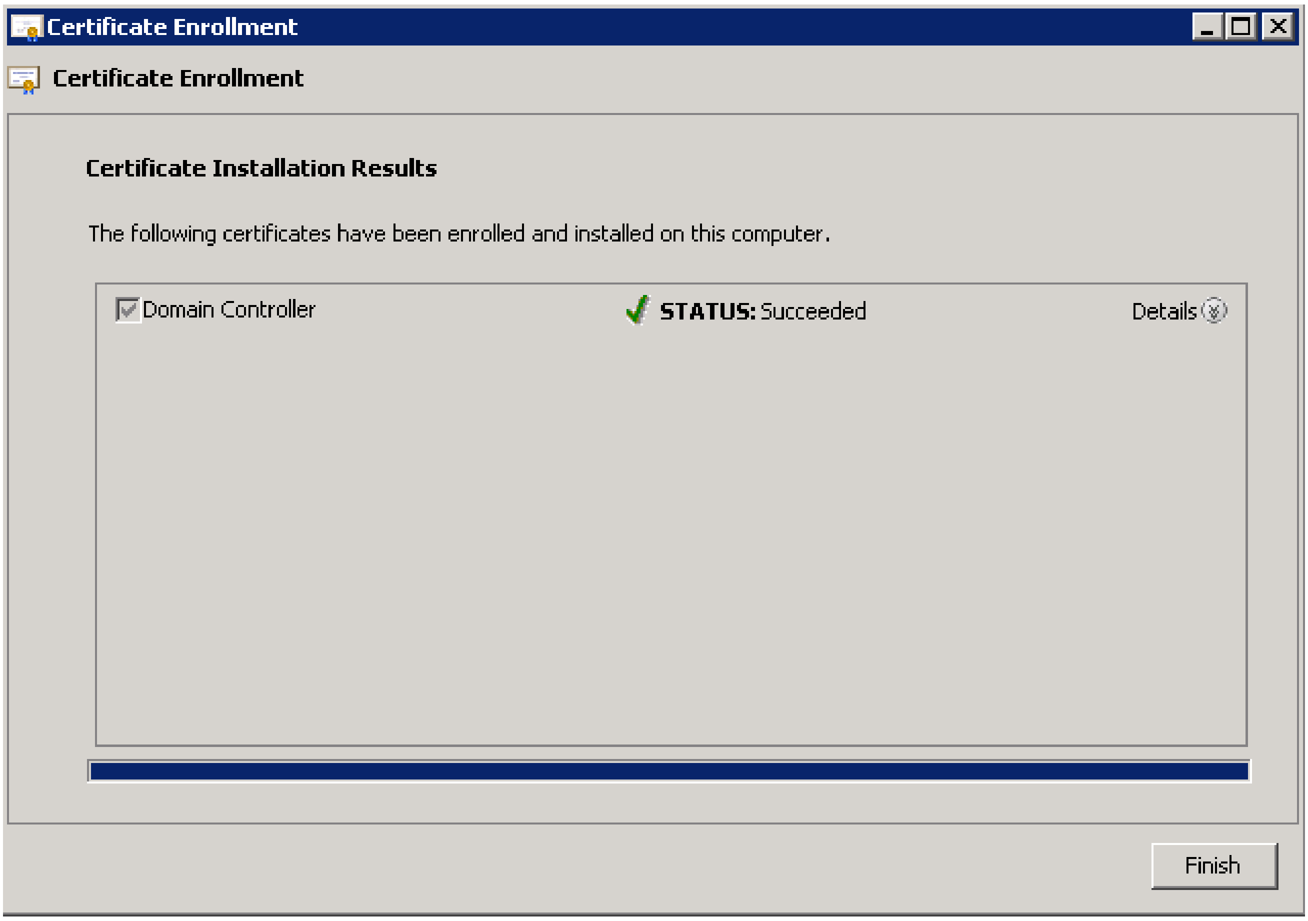
☑ Domain Controller — STATUS: Available — Details

☑ Domain Controller Authentication — STATUS: Available — Details

□ Show all templates

Learn more about certificate types

11. 安裝憑證後，按一下**Finish**。



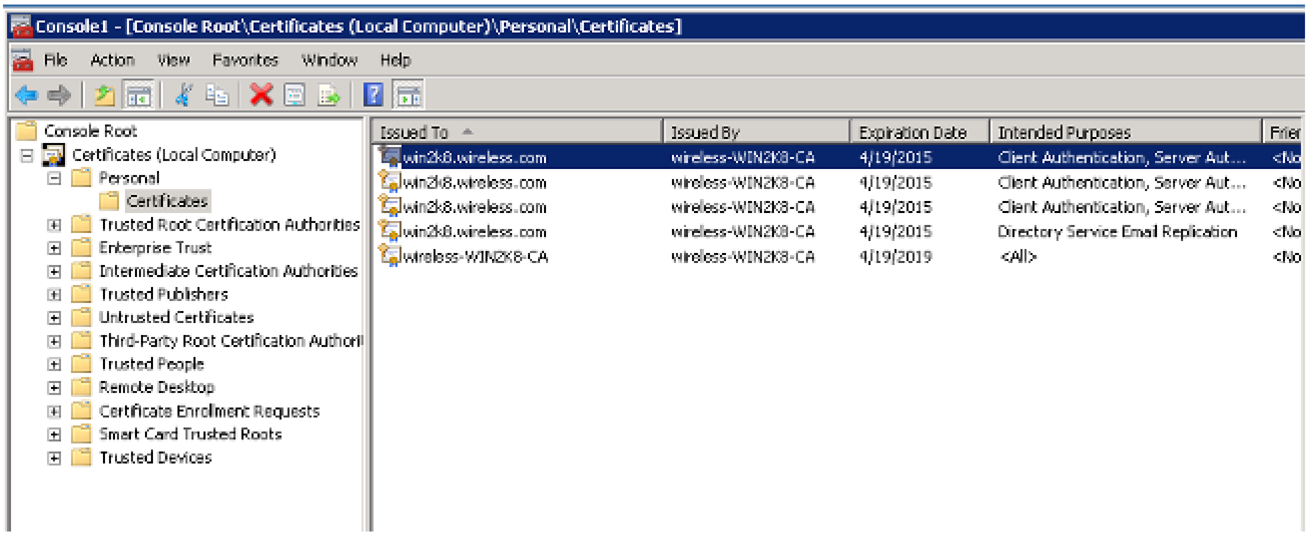
Certificate Installation Results

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

☑ Domain Controller — ✓ STATUS: Succeeded — Details

NPS證書現在已安裝。

12. 確保**Client Authentication**，**Server Authentication**出現在證書的「目標用途」列中。


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

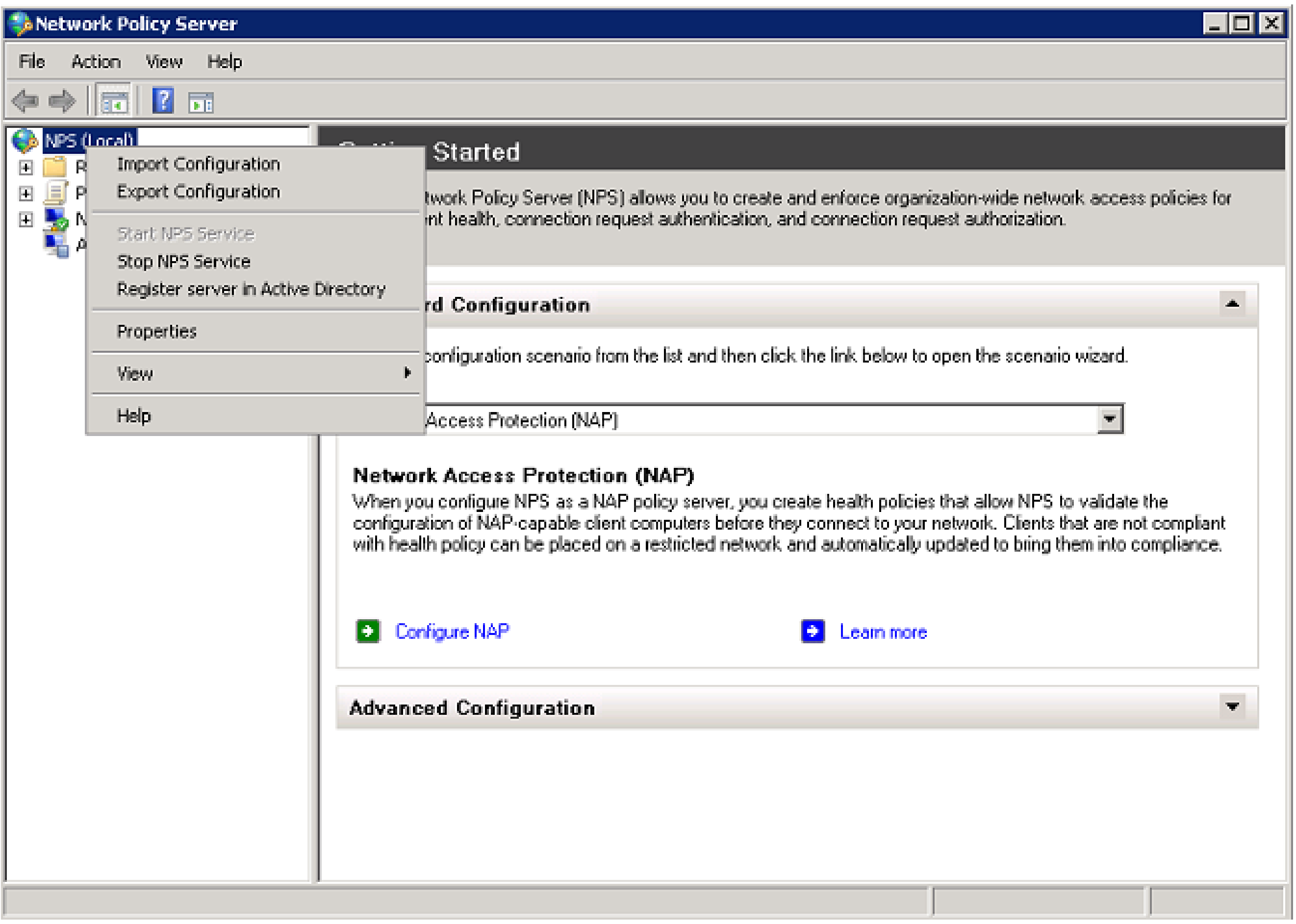
Issued To	Issued By	Expiration Date	Intended Purposes	Frie
win2k8.wireless.com	wireless-WIN2K8-CA	4/19/2015	Client Authentication, Server Aut...	<No
win2k8.wireless.com	wireless-WIN2K8-CA	4/19/2015	Client Authentication, Server Aut...	<No
win2k8.wireless.com	wireless-WIN2K8-CA	4/19/2015	Client Authentication,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

為PEAP-MS-CHAP v2身份驗證配置網路策略伺服器服務

完成以下步驟，配置NPS進行身份驗證：

1. 導覽至**Start**> Administrative Tools > **Network Policy Server**。

2. 按一下右鍵**NPS（本地）**，然後選擇**Register server in Active Directory**。



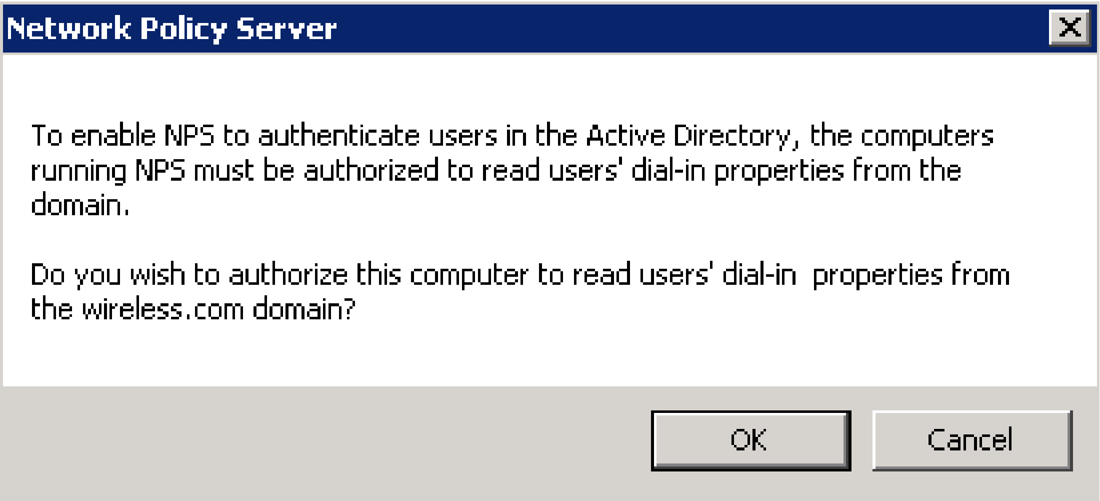
twork Policy Server (NPS) allows you to create and enforce organization-wide network access policies for nt health, connection request authentication, and connection request authorization.

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. 按一下「**OK**」（確定）。

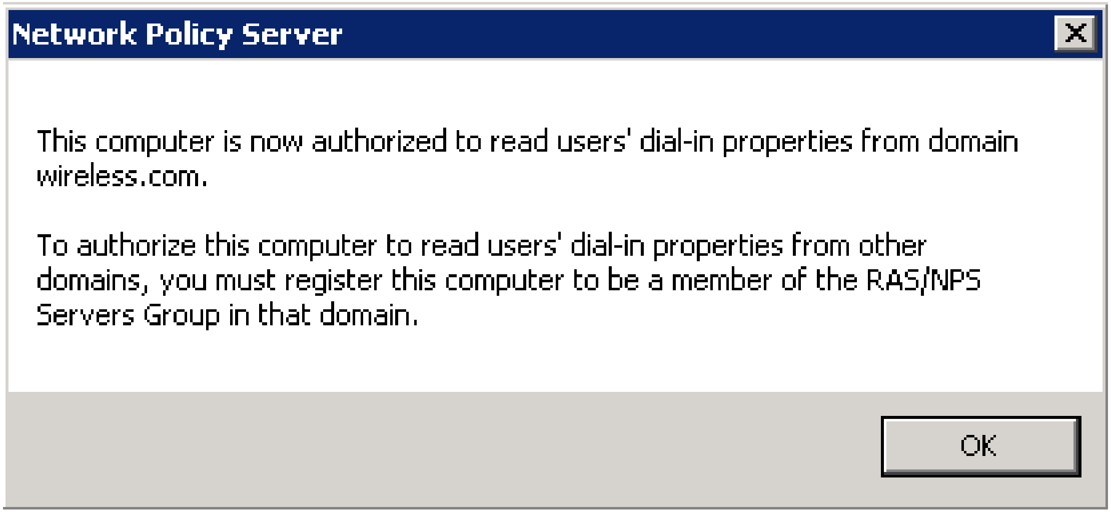


Network Policy Server

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

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

4. 按一下「**OK**」（確定）。



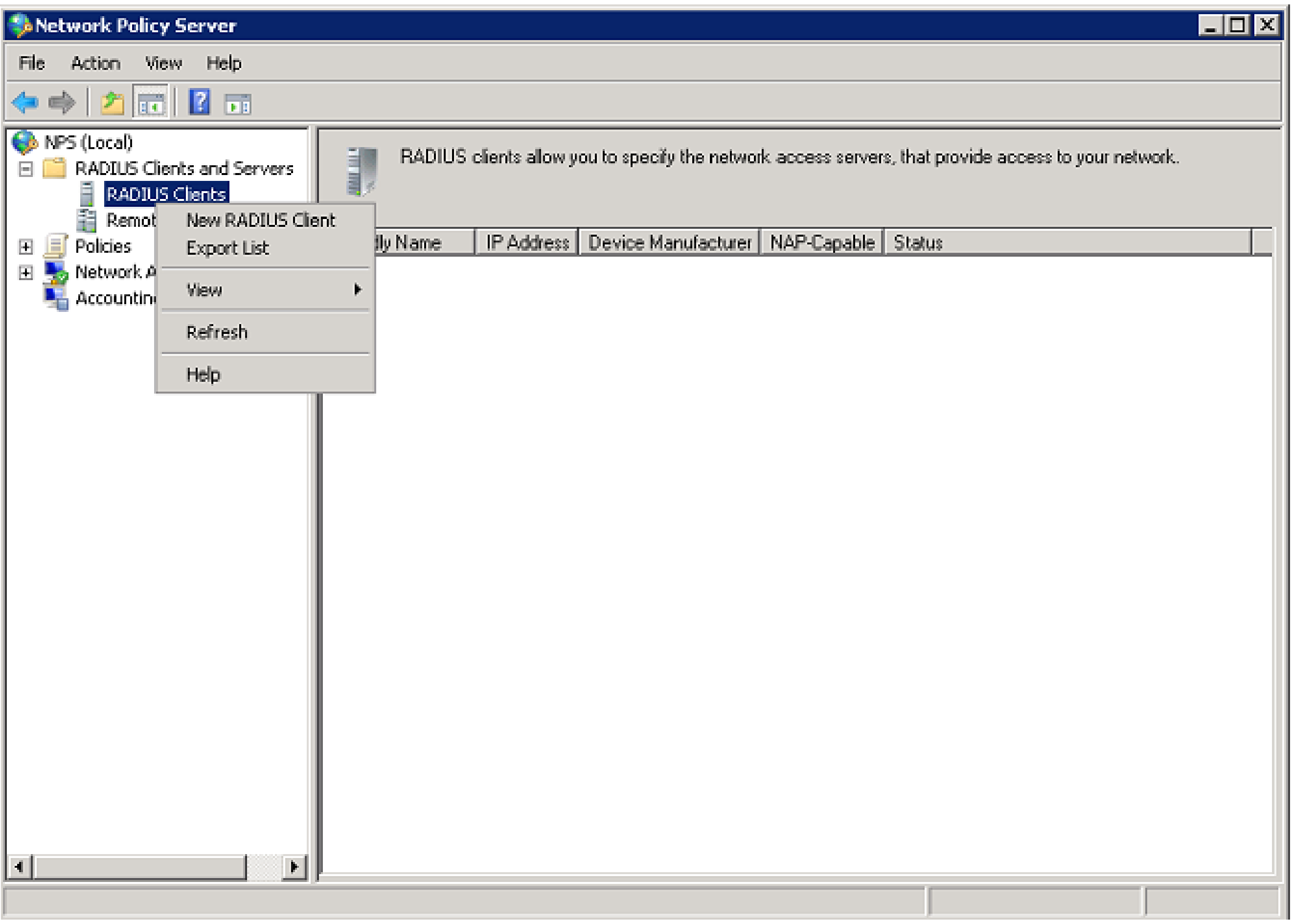
Network Policy Server

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

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

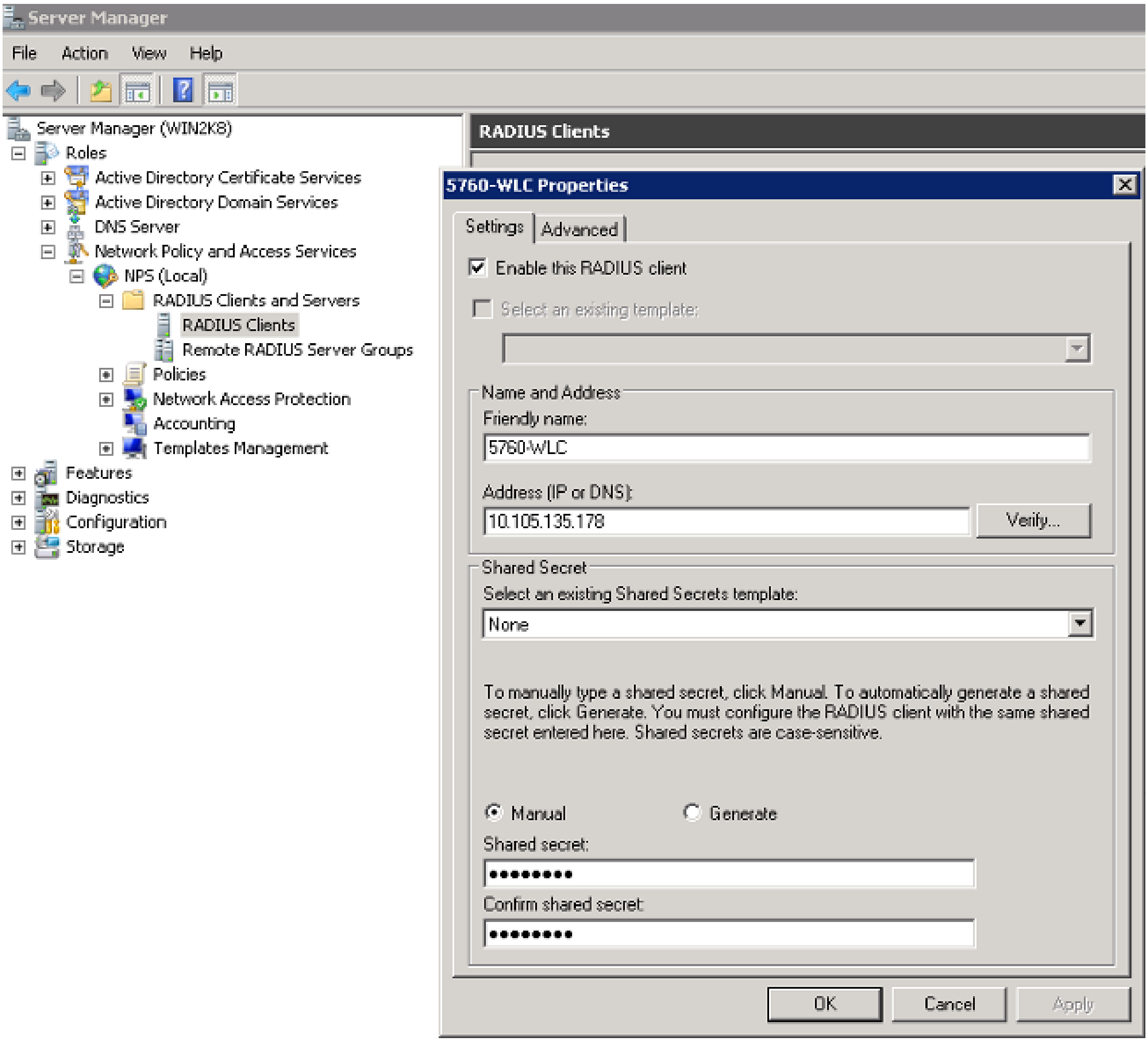
5. 將WLC新增為NPS上的驗證、授權和記帳(AAA)使用者端。

6. 展開**RADIUS客戶端和伺服器**。按一下右鍵**RADIUS Clients**，然後選擇**New RADIUS Client**:



7. 輸入名稱(此範例中為**WLC**)、WLC的管理IP位址(此範例中為**10.105.135.178**)和共用密碼。

附註：使用相同的共用金鑰設定WLC。



☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: 5760-WLC

Address (IP or DNS): 10.105.135.178

Shared Secret

Select an existing Shared Secrets template: None

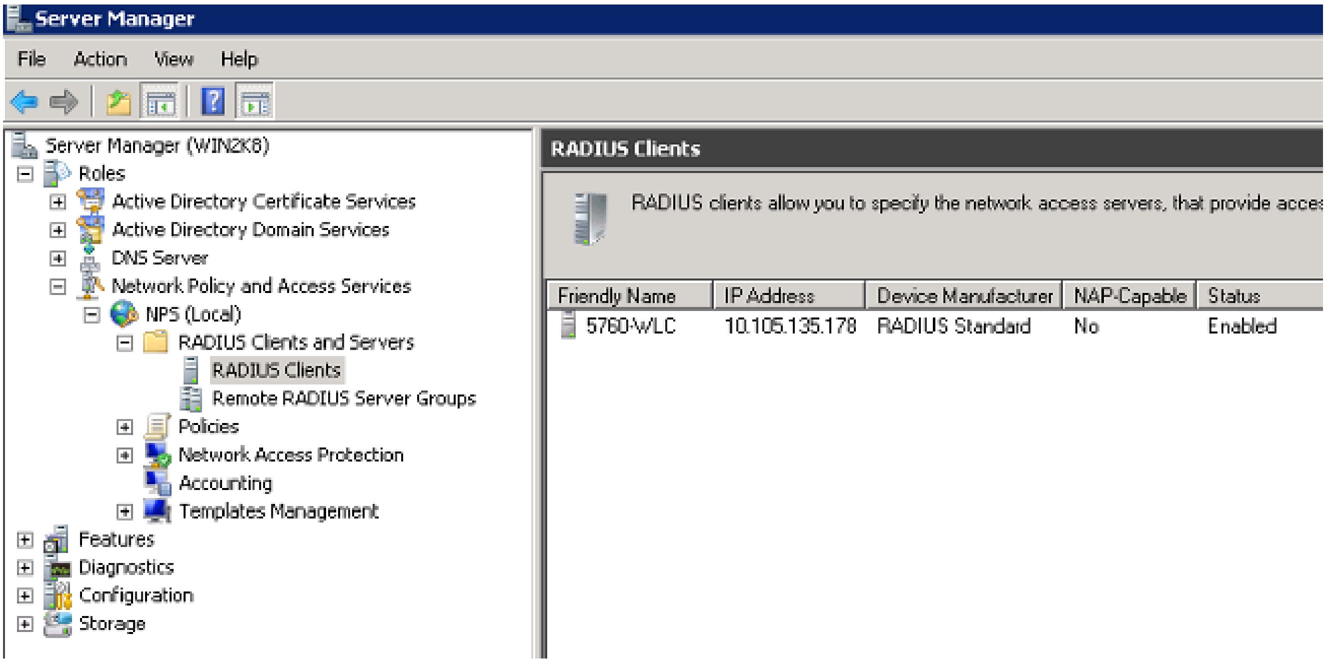
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ●●●●●●●●●

Confirm shared secret: ●●●●●●●●●

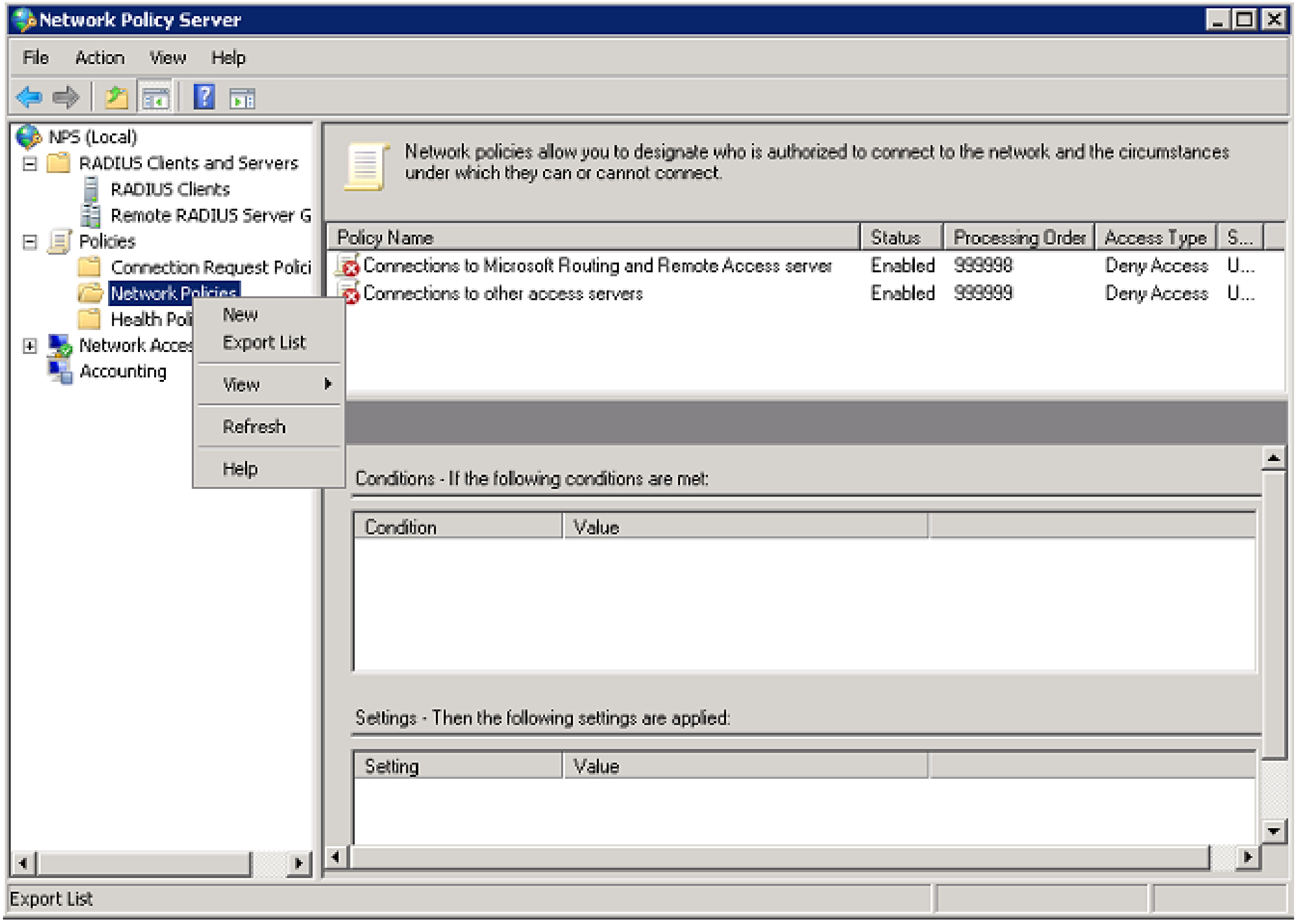
8. 按一下「OK」以返回上一個畫面。



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

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

9. 為無線使用者建立新的網路策略。展開**Policies**，按一下右鍵**Network Policies**，然後選擇**New**:



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

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

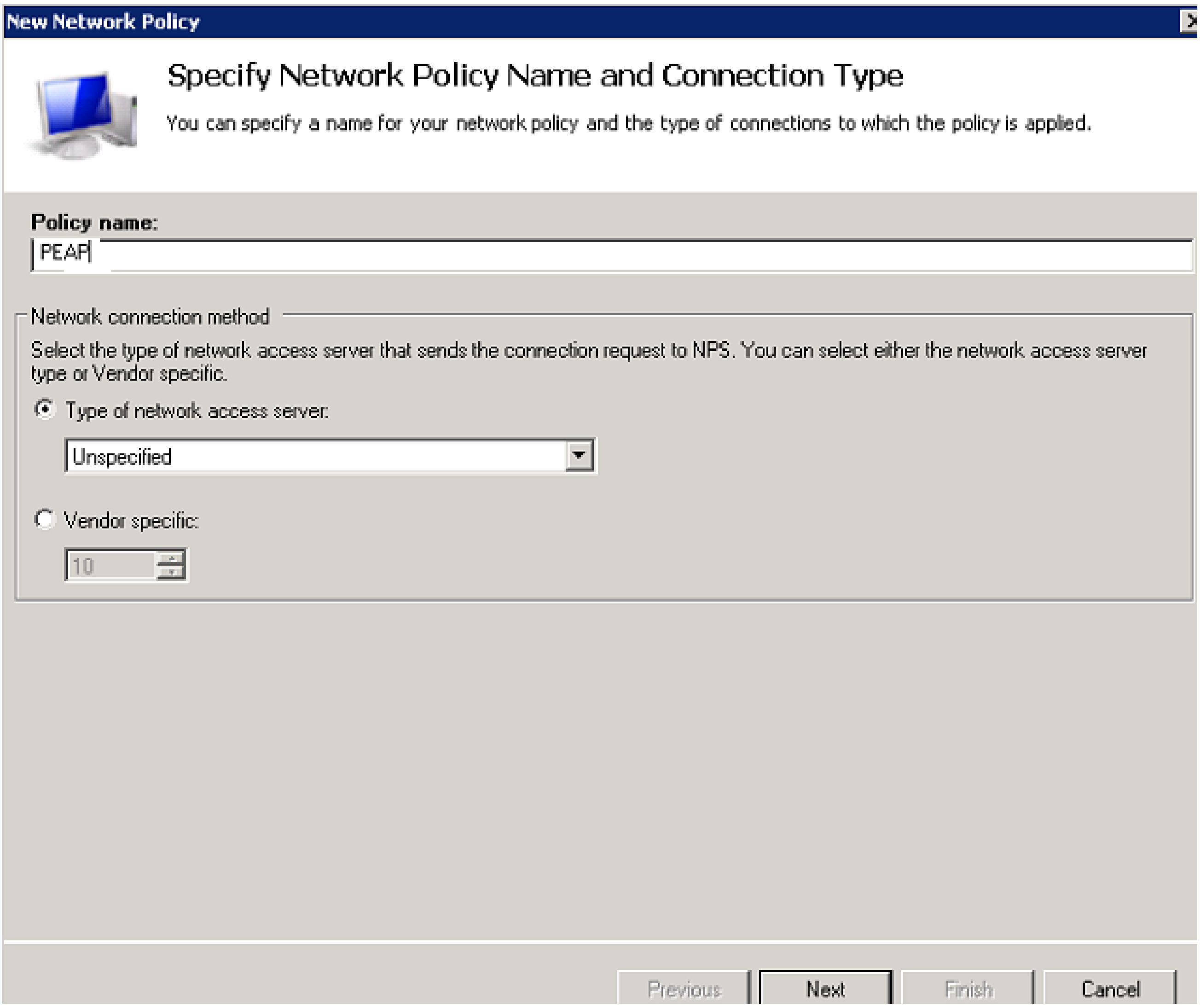
Conditions - If the following conditions are met:

Condition	Value

Settings - Then the following settings are applied:

Setting	Value

10. 輸入此規則的策略名稱(**本示例**中的PEAP)，然後按一下**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:

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.

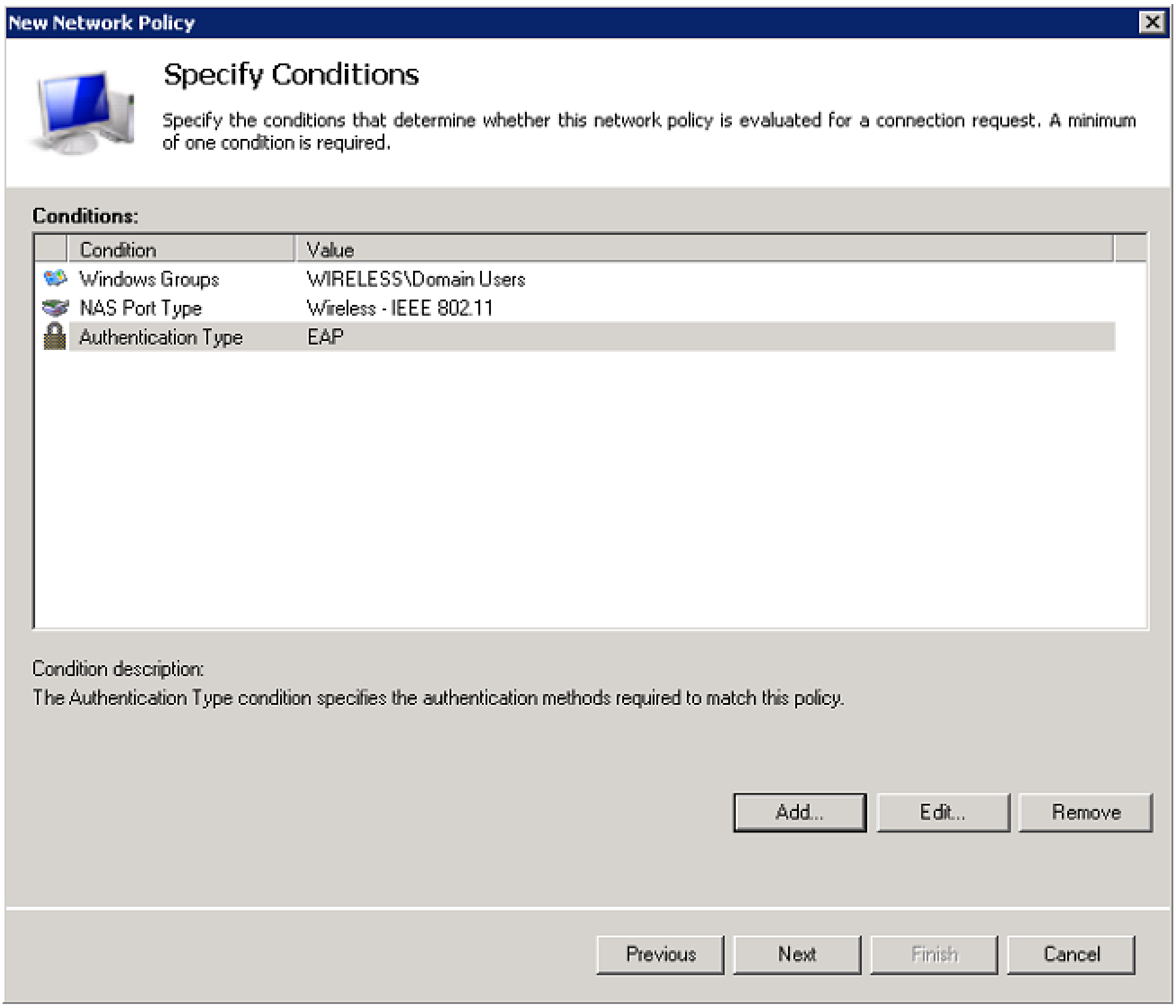
● Type of network access server:

Unspecified

○ Vendor specific:

10

11. 若要將此策略配置為僅允許無線域使用者，請新增以下三個條件，然後按一下**下一步**:



New Network Policy

Specify Conditions

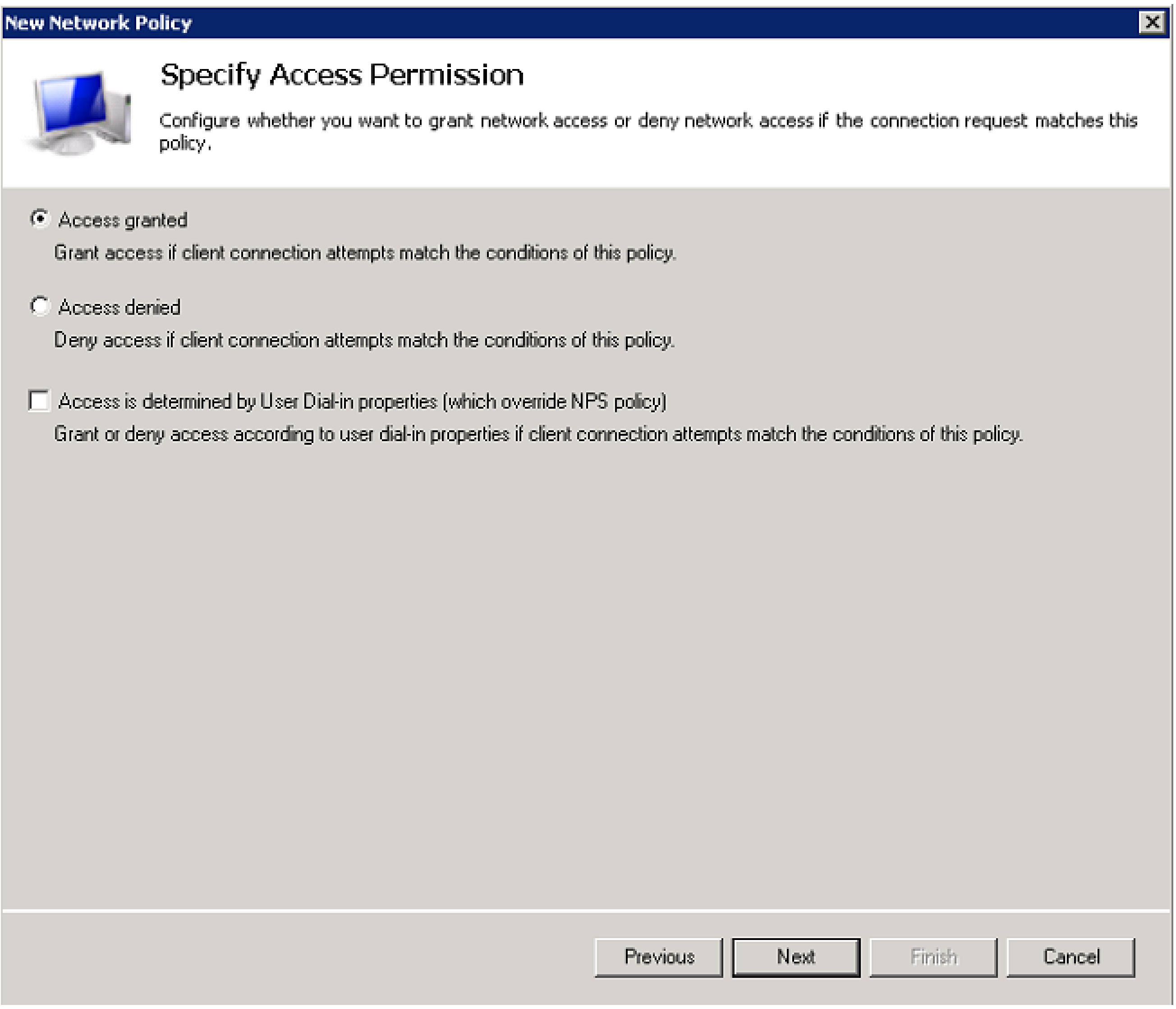
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

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. 按一下**Access granted**單選按鈕以授予與此策略匹配的連線嘗試，然後按一下**Next**。



Specify Access Permission

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

● Access granted

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

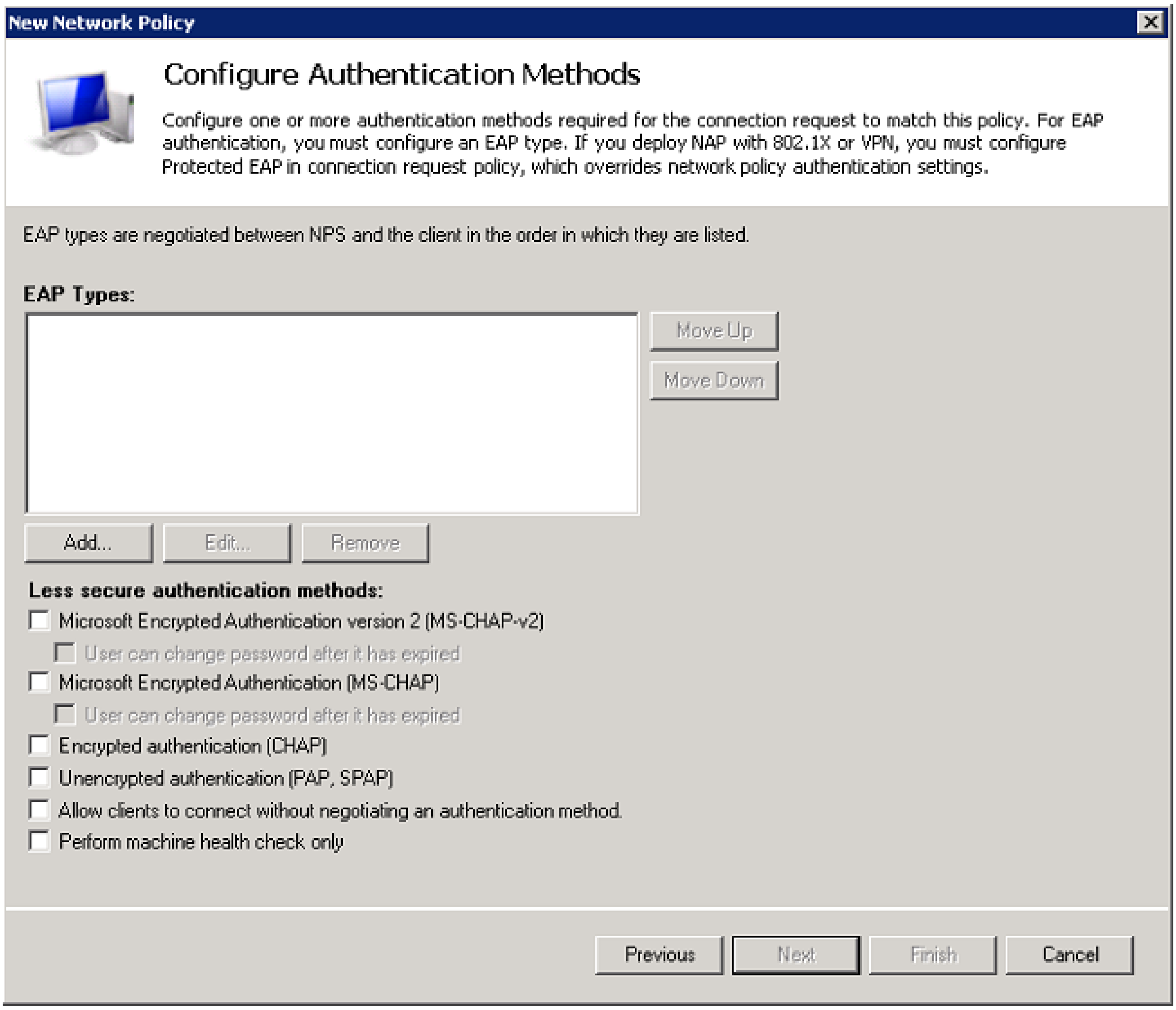
○ Access denied

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

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

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

13. 禁用所有不安全**的身份驗證方法**:



New Network Policy

Configure Authentication Methods

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

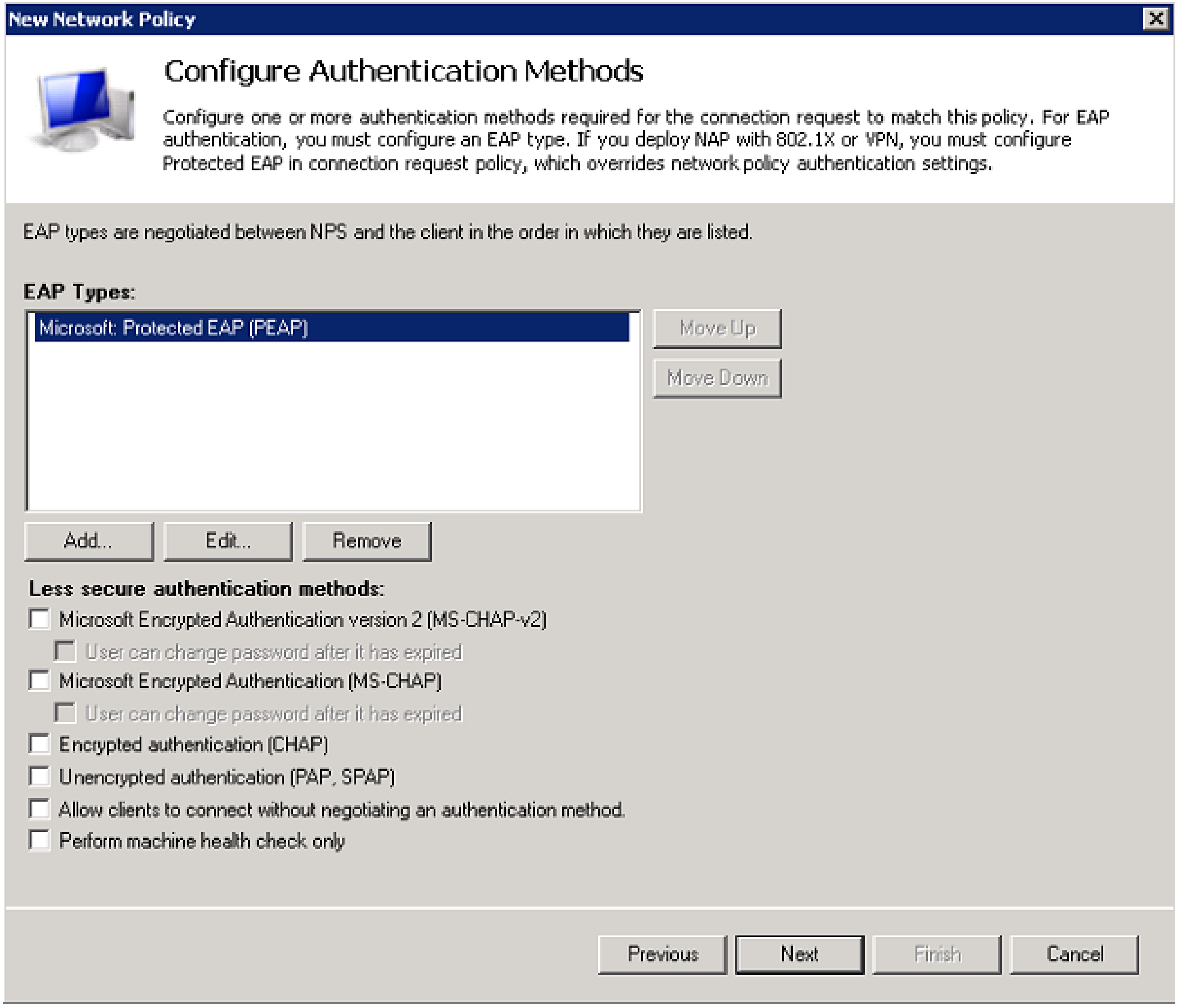
EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

- □ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - □ User can change password after it has expired
- □ Microsoft Encrypted Authentication (MS-CHAP)
  - □ User can change password after it has expired
- □ Encrypted authentication (CHAP)
- □ Unencrypted authentication (PAP, SPAP)
- □ Allow clients to connect without negotiating an authentication method.
- □ Perform machine health check only

14. 按一下**Add**，選擇**Microsoft:受保護的EAP(PEAP**)EAP型別，然後按一下**OK**以啟用PEAP。


New Network Policy

Configure Authentication Methods

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

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

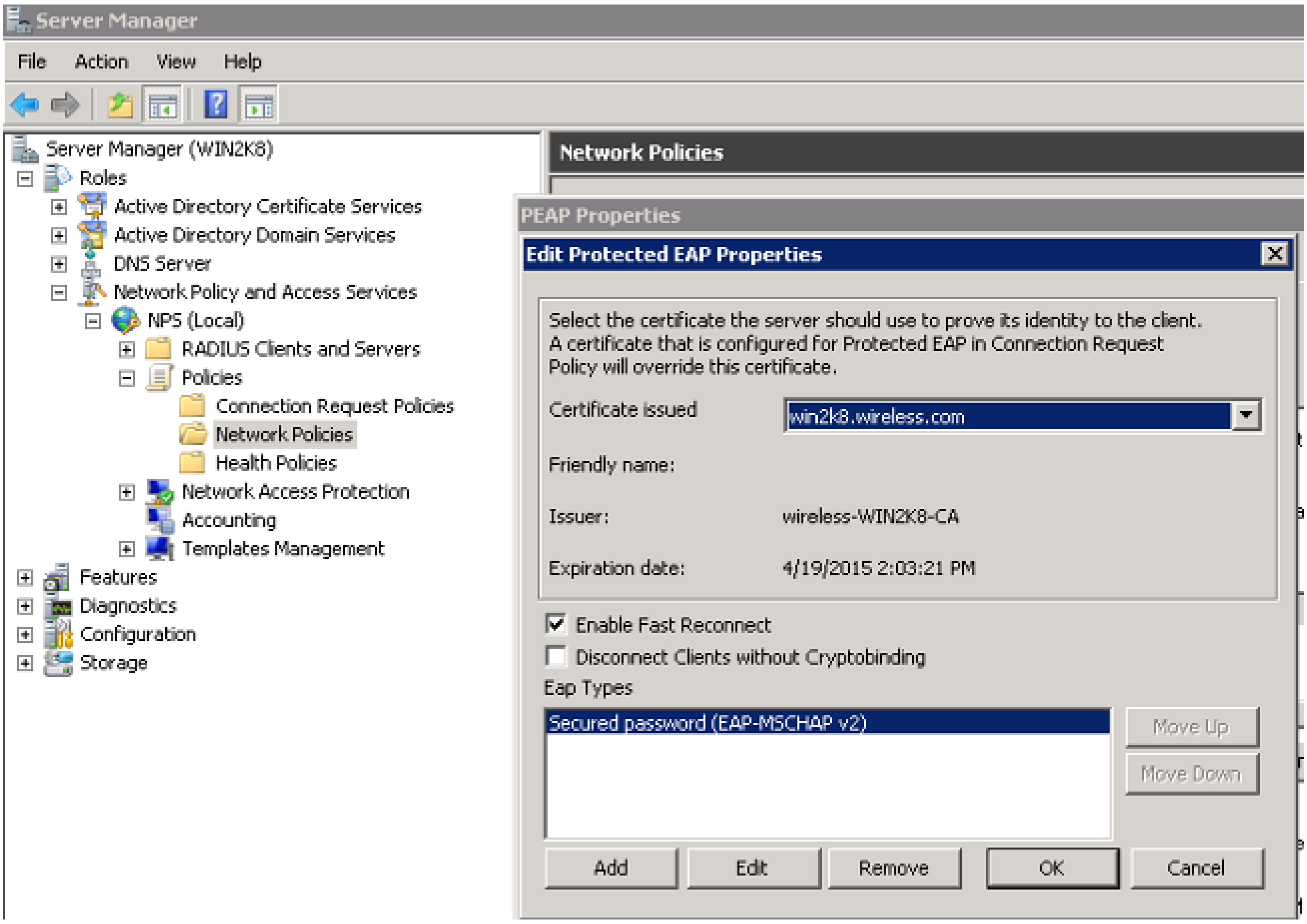
EAP Types:

Microsoft: Protected EAP (PEAP)

Less secure authentication methods:

- ☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - ☐ User can change password after it has expired
- ☐ Microsoft Encrypted Authentication (MS-CHAP)
  - ☐ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☐ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method.
- ☐ Perform machine health check only

15. 選擇**Microsoft:受保護的EAP(PEAP),**然後點選**編輯**。確保在Certificate issued下拉選單中選中先前建立的域控制器證書，然後按一下**Ok**。



Edit Protected EAP Properties

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

Certificate issued: win2k8.wireless.com

Friendly name:

Issuer: wireless-WIN2K8-CA

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

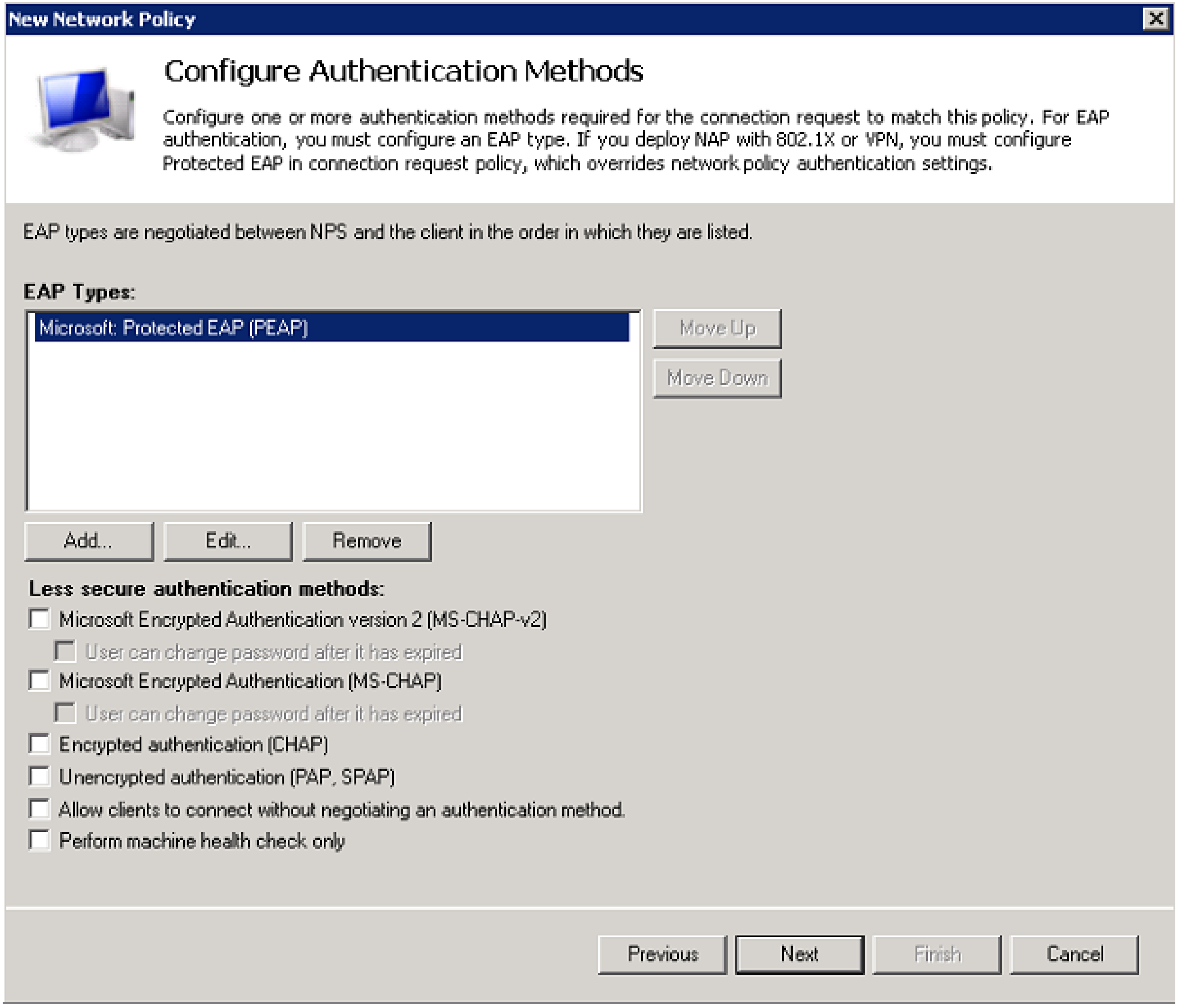
☑ Enable Fast Reconnect

☐ Disconnect Clients without Cryptobinding

Eap Types

Secured password (EAP-MSCHAP v2)

16. 按「**Next**」（下一步）。



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.

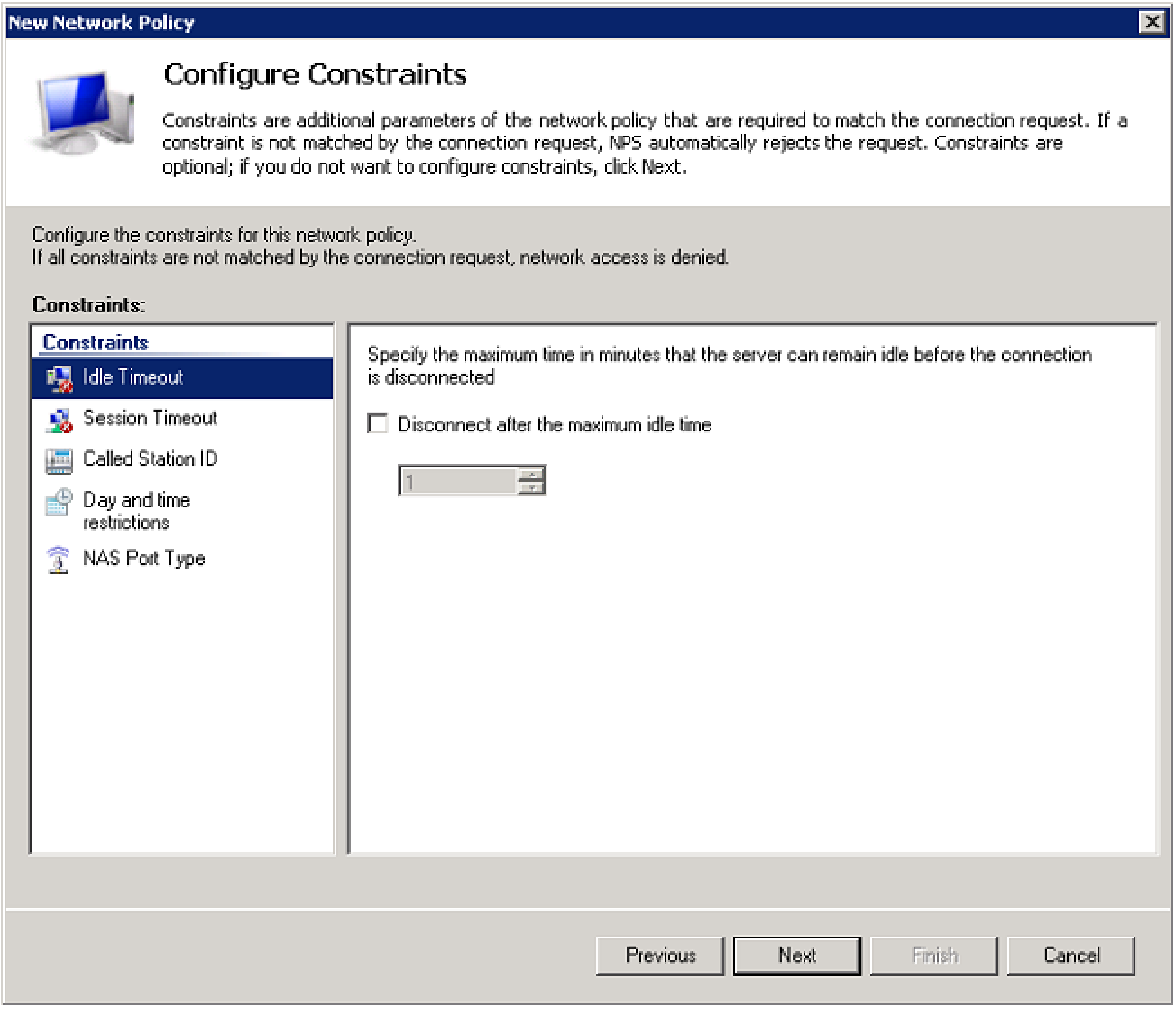
EAP Types:

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. 按「**Next**」（下一步）。



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.

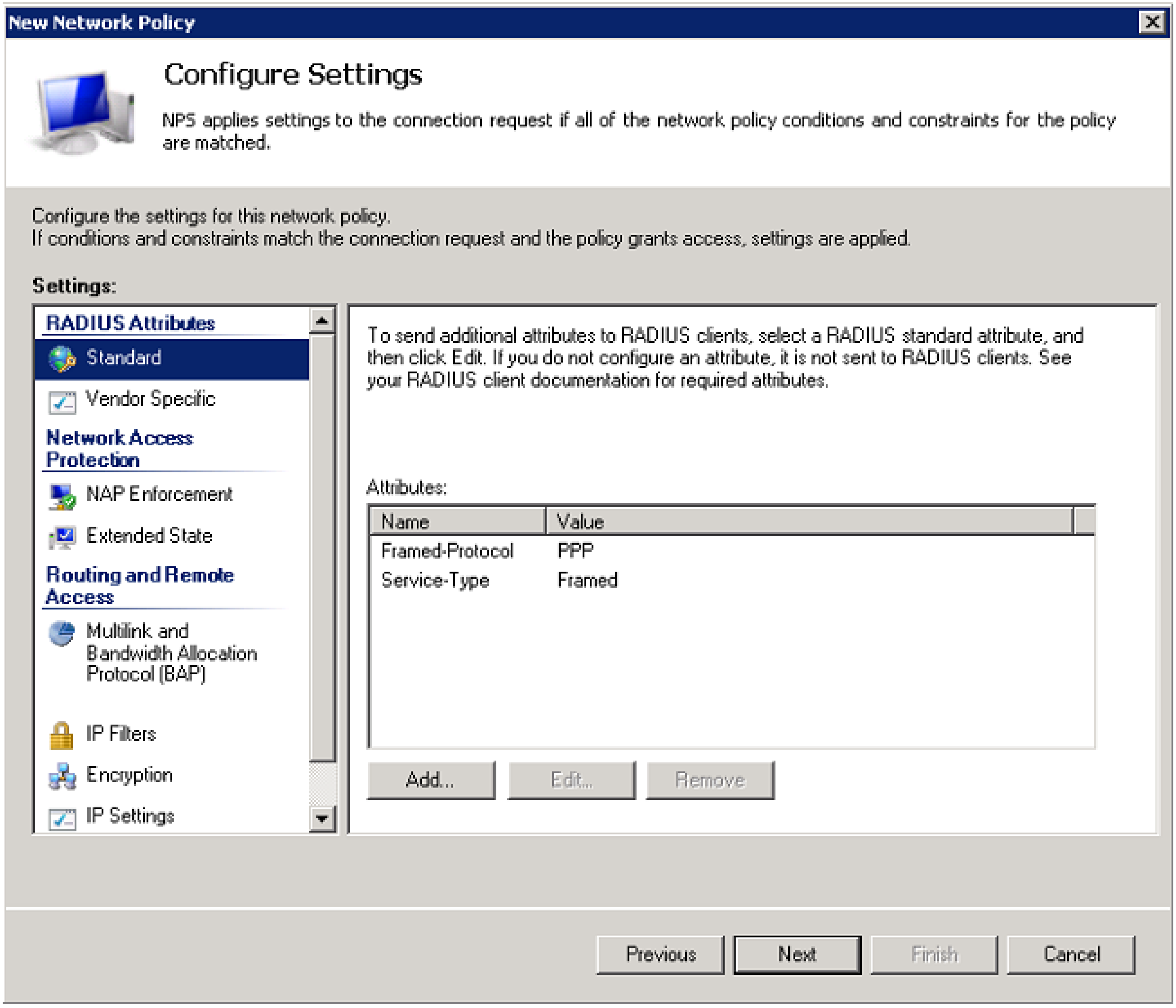
Constraints:

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. 按「**Next**」（下一步）。



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.

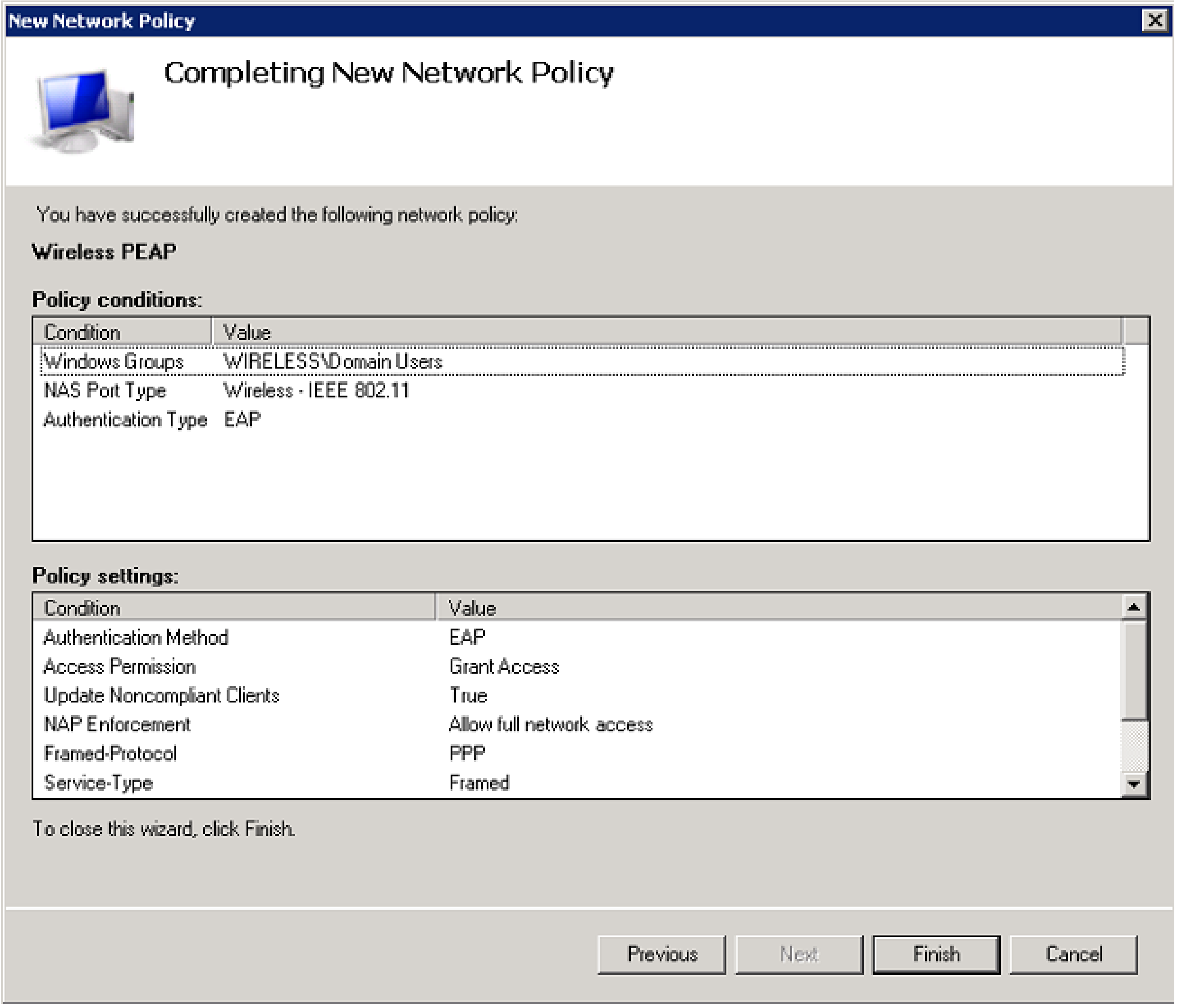
Settings:

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. 按一下「**Finish**」（結束）。



Completing New Network Policy

You have successfully created the following network policy:

Wireless PEAP

Policy conditions:

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

Policy settings:

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

To close this wizard, click Finish.

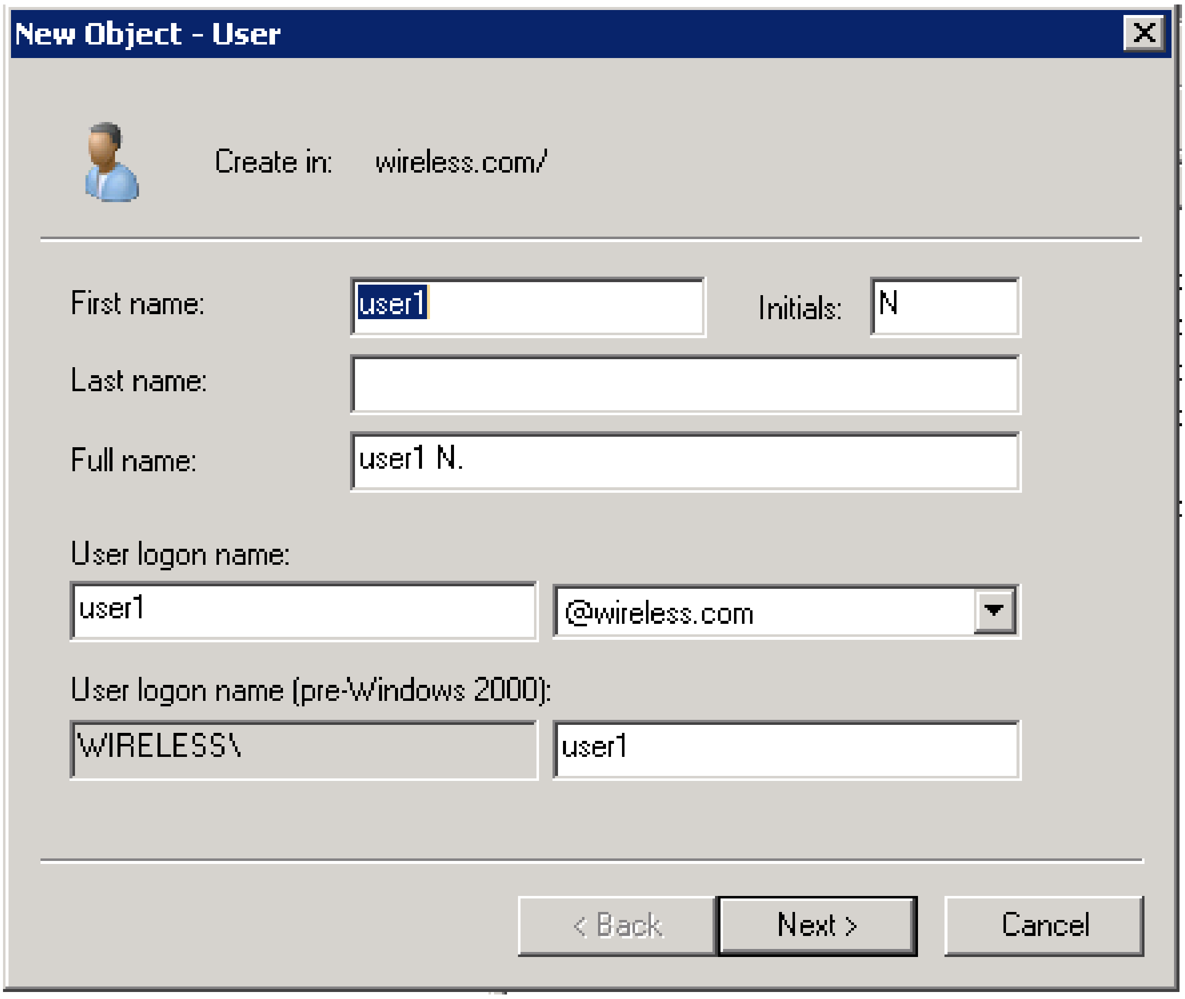
附註：根據需要，您可能需要在NPS上配置**連線請求策略**，以便允許PEAP配置檔案或策略。

將使用者新增到Active Directory

附註：在本示例中，使用者資料庫在AD上維護。

完成以下步驟，以便向AD資料庫新增使用者：

1. 導覽至**開始** > **管理**工具 > **Active Directory使用者和電腦**。
2. 在「Active Directory使用者和電腦」控制檯樹中，展開域，按一下右鍵**Users**和**New**，然後選擇**User**。
3. 在新對象 — 使用者對話方塊中，輸入無線使用者的名稱。此示例在First Name欄位中使用**Client1**，在**User logon name欄位中使用Client1**。按「**Next**」（下一步）。



New Object - User

Create in: wireless.com/

First name: user1

Initials: N

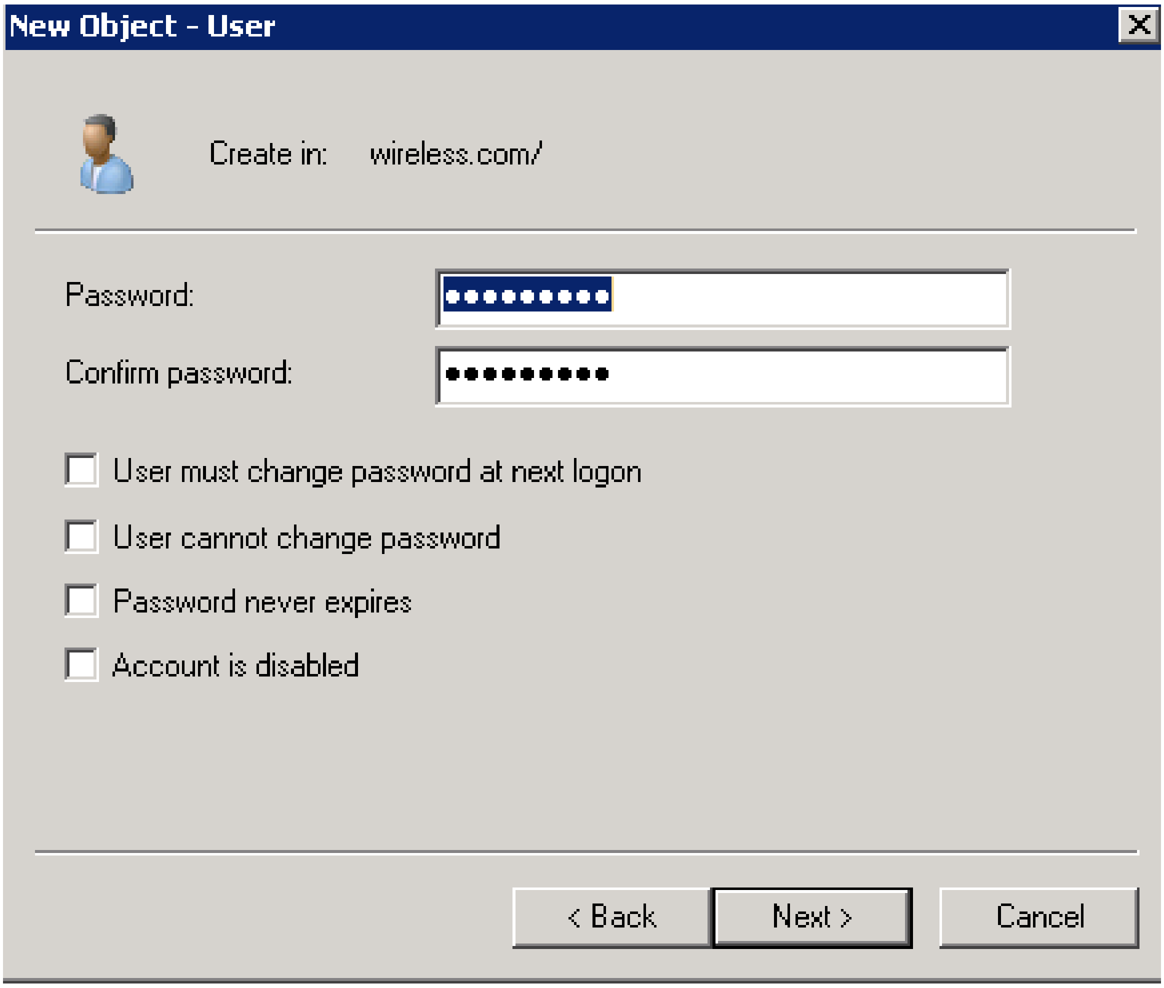
Last name:

Full name: user1 N.

User logon name: user1 @wireless.com

User logon name (pre-Windows 2000): WIRELESS\ user1

4. 在「新建對象 — 使用者」對話方塊中，在「密碼」和「確認密碼」欄位中輸入您選擇的密碼。取消選中**User must change password at next logon**覈取方塊，然後按一下**Next**。



New Object - User

Create in: wireless.com/

Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●●

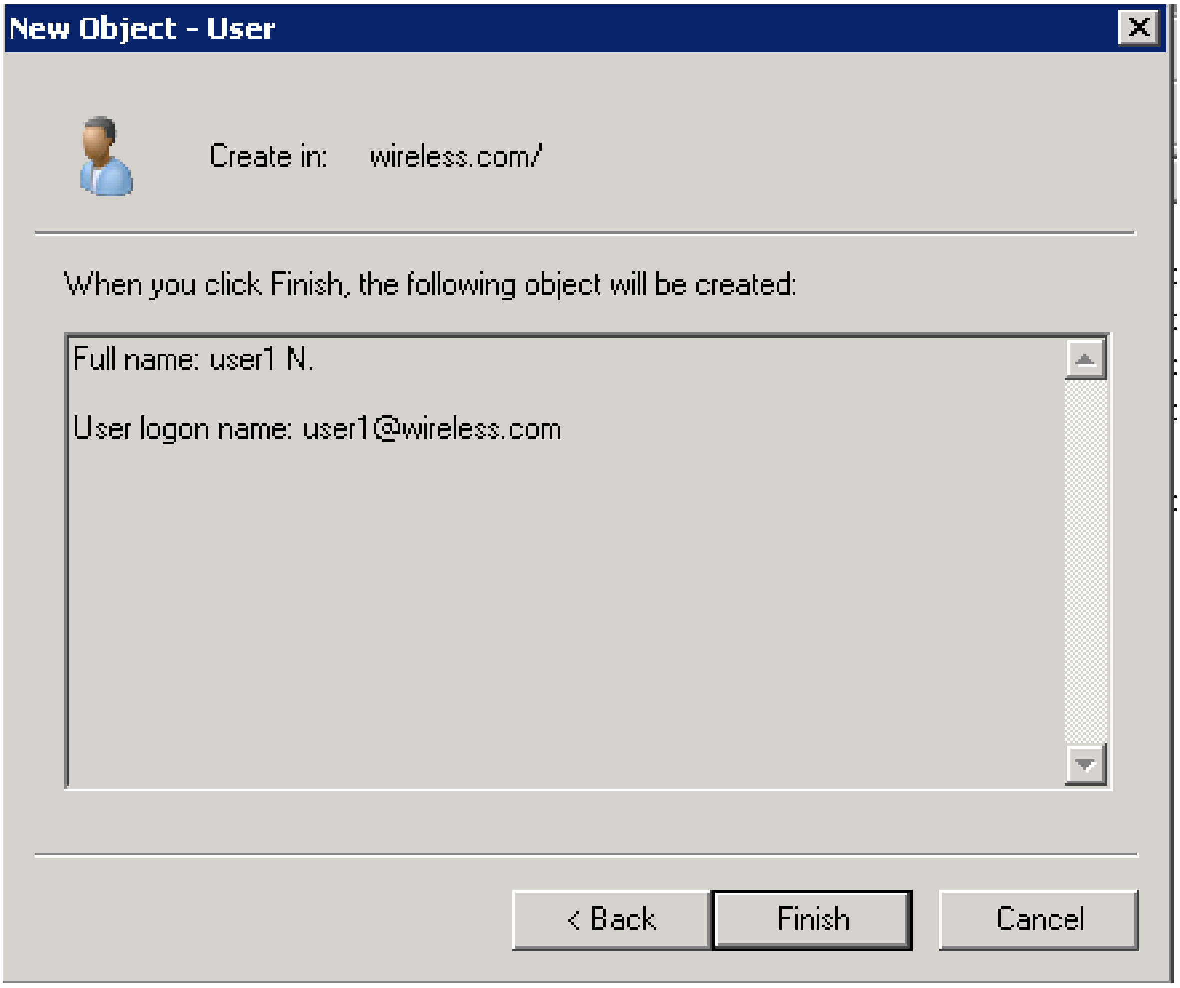
□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

5. 在「新建對象 — 使用者」對話方塊中，按一下**完成**。



Create in: wireless.com/

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

Full name: user1 N.

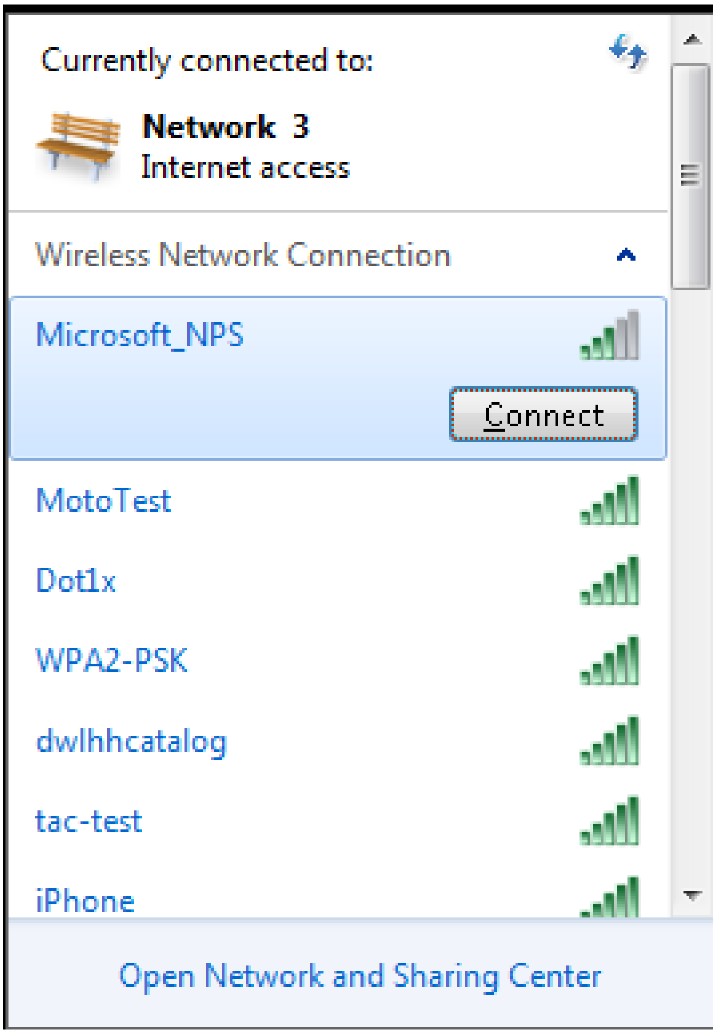
User logon name: user1@wireless.com

6. 重複步驟2至4以建立其他使用者帳戶。

驗證

完成以下步驟以驗證您的設定：

1. 在客戶端電腦上搜尋服務集標識(SSID)。



Currently connected to:

Network 3
Internet access

Wireless Network Connection

Microsoft_NPS

Connect

MotoTest

Dot1x

WPA2-PSK

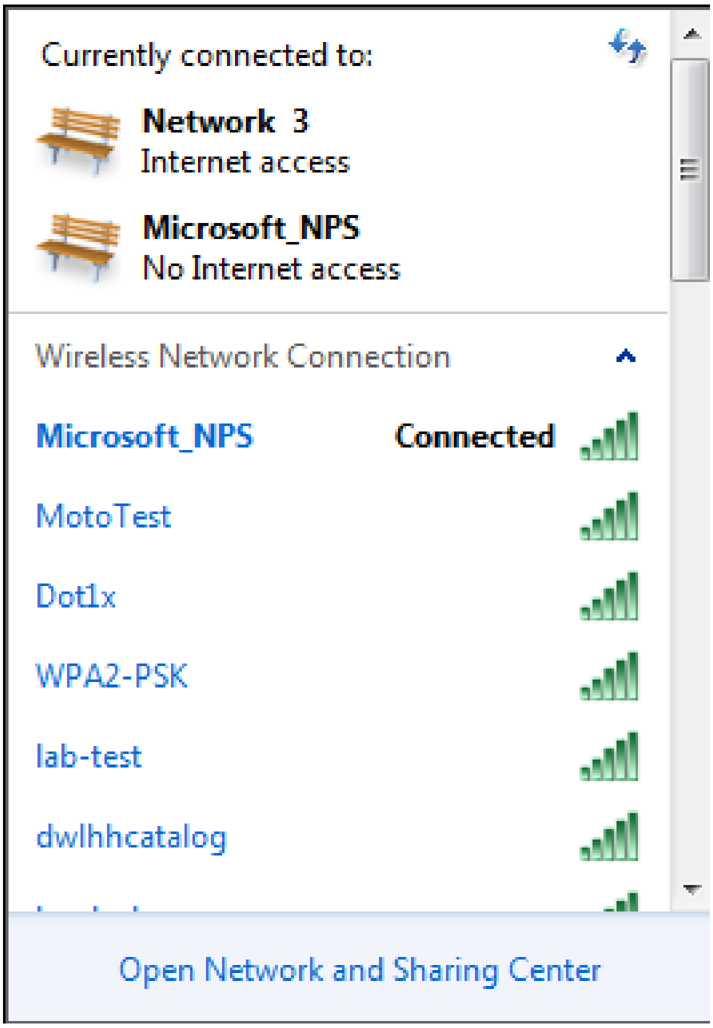
dwlhhcatalog

tac-test

iPhone

Open Network and Sharing Center

2. 確保客戶端成功連線：



疑難排解

附註：思科建議您使用追蹤來排解無線問題。跟蹤儲存在循環緩衝區中，不佔用大量處理器。

啟用這些追蹤以取得**L2驗證日誌**:

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

啟用這些跟蹤以獲取**dot1X AAA事件**:

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

啟用這些跟蹤以接收DHCP**事件**:

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

啟用這些追蹤以停用追蹤並清除緩衝區：

- set trace control sys-filtered-trace clear
- set trace wcm-dot1x aaa level default
- set trace wcm-dot1x aaa filter none
- set trace group-wireless-secure level default

- set trace group-wireless-secure filter none

輸入show trace sys-filtered-traces命令以檢視跟蹤：

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

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

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

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


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

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


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

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

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

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

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


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


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

以下是EAP輸出的其餘部分：

```
[04/23/14 21:27:54.690 IST 12b 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:54.690 IST 12c 211] AAA SRV(00000000): Authen
 method=SERVER_GROUP Microsoft_NPS
[04/23/14 21:27:54.690 IST 12d 211] AAA SRV(00000000): Selecting SG =
 DIAMETER
[04/23/14 21:27:54.694 IST 12e 220] AAA SRV(00000000): protocol reply PASS
```

```
 for Authentication
[04/23/14 21:27:54.694 IST 12f 220] AAA SRV(00000000): Return Authentication
 status=PASS
[04/23/14 21:27:54.694 IST 130 189] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Received an EAP Success


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

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


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


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