配置NPS、無線LAN控制器和無線網路

目錄

簡介

本文檔介紹如何使用Microsoft NPS作為RADIUS伺服器配置PEAP的MS-CHAP身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- Windows 2008基本安裝知識

- 思科控制器安裝知識

嘗試此組態之前，請確保已符合以下要求：

- 在測試實驗室中的每台伺服器上安裝Microsoft Windows Server 2008。
- 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。

有關Cisco 5508系列無線控制器的初始安裝和配置資訊，請參閱Cisco 5500系列無線控制器安裝指南。

附註：本文檔旨在為讀者提供一個Microsoft伺服器上進行PEAP-MS-CHAP身份驗證所需的配置示例。本文檔中介紹的Microsoft Windows伺服器配置已在實驗室中經過測試，並且發現可以按預期工作。如果配置有問題，請與Microsoft聯絡以獲得幫助。思科技術支援中心(TAC)不支援Microsoft Windows伺服器配置。

Microsoft Windows 2008安裝及設定指南可在Microsoft Tech Net上找到。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行韌體版本7.4的思科5508無線控制器
- 採用輕量型存取點通訊協定(LWAPP)的Cisco Aironet 3602存取點(AP)
- 安裝了NPS、證書頒發機構(CA)、動態主機控制協定(DHCP)和域名系統(DNS)服務的Windows 2008企業伺服器
- Microsoft Windows 7客戶端PC
- 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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

本文提供使用Microsoft Network Policy Server(NPS)作為RADIUS伺服器的思科統一無線網路中受保護的可擴展身份驗證協定(PEAP)和Microsoft Challenge Handshake身份驗證協定(MS-CHAP)版本2身份驗證的示例配置。

PEAP概述

PEAP使用傳輸級安全(TLS)在經過身份驗證的PEAP客戶端（如無線筆記型電腦）和PEAP身份驗證器（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，可以通過PEAP提供的TLS加密通道進行操作。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AP關聯。基於IEEE 802.11的關聯在客戶端和接入點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。在客戶端和接入點之間成功建立基於IEEE 802.11的關聯之後，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。在此協商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。無線LAN控制器(WLC)和LAP無法解密這些消息，因為它不是TLS端點。

成功進行身份驗證嘗試的RADIUS消息序列（其中使用者已提供具有PEAP-MS-CHAP v2的有效基於密碼的憑據）為：

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 — 響應/身份。
3. NPS傳送MS-CHAP v2質詢消息：EAP-Request/EAP-Type=EAP MS-CHAP-V2（質詢）。
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（響應）。
5. 當伺服器成功對客戶端進行身份驗證後，NPS將傳回MS-CHAP v2成功資料包：EAP-Request/EAP-Type=EAP-MS-CHAP-V2（成功）。
6. 當客戶端成功對伺服器進行身份驗證時，客戶端將使用MS-CHAP v2成功資料包進行響應：EAP-Response/EAP-Type=EAP-MS-CHAP-V2（成功）。
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。

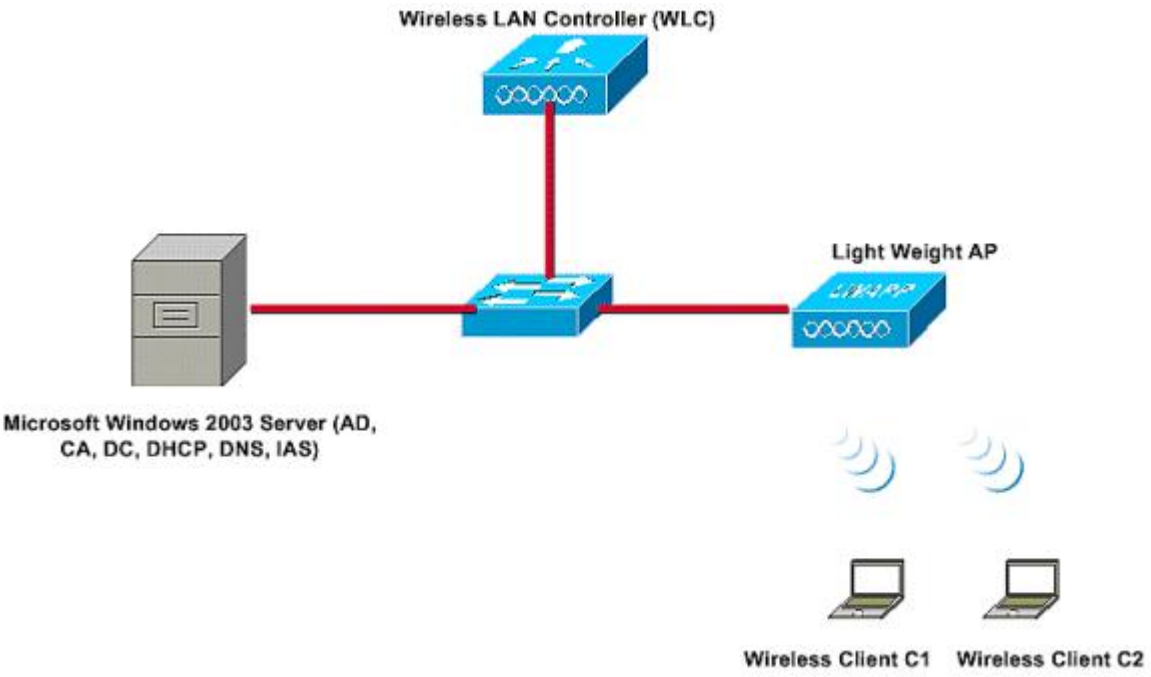
設定

本節提供配置PEAP-MS-CHAP v2的資訊。

附註：使用命令查詢工具可獲取本節所用命令的詳細資訊。只有註冊的思科使用者才能訪問內部思科工具和資訊。

網路圖表

此配置使用以下網路設定：



網路圖表

在此設定中，Microsoft Windows 2008伺服器執行以下角色：

- 域的域控制器
- DHCP/DNS伺服器
- CA伺服器
- NPS — 對無線使用者進行身份驗證
- Active Directory — 維護使用者資料庫

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

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

本示例的目的是配置Microsoft 2008伺服器、無線LAN控制器和輕量AP，以使用PEAP-MS-CHAP v2身份驗證對無線客戶端進行身份驗證。此過程有三個主要步驟：

1. 配置Microsoft Windows 2008 Server。
2. 配置WLC和輕量AP。
3. 配置無線客戶端。

配置Microsoft Windows 2008 Server

在本示例中，Microsoft Windows 2008伺服器的完整配置包括以下步驟：

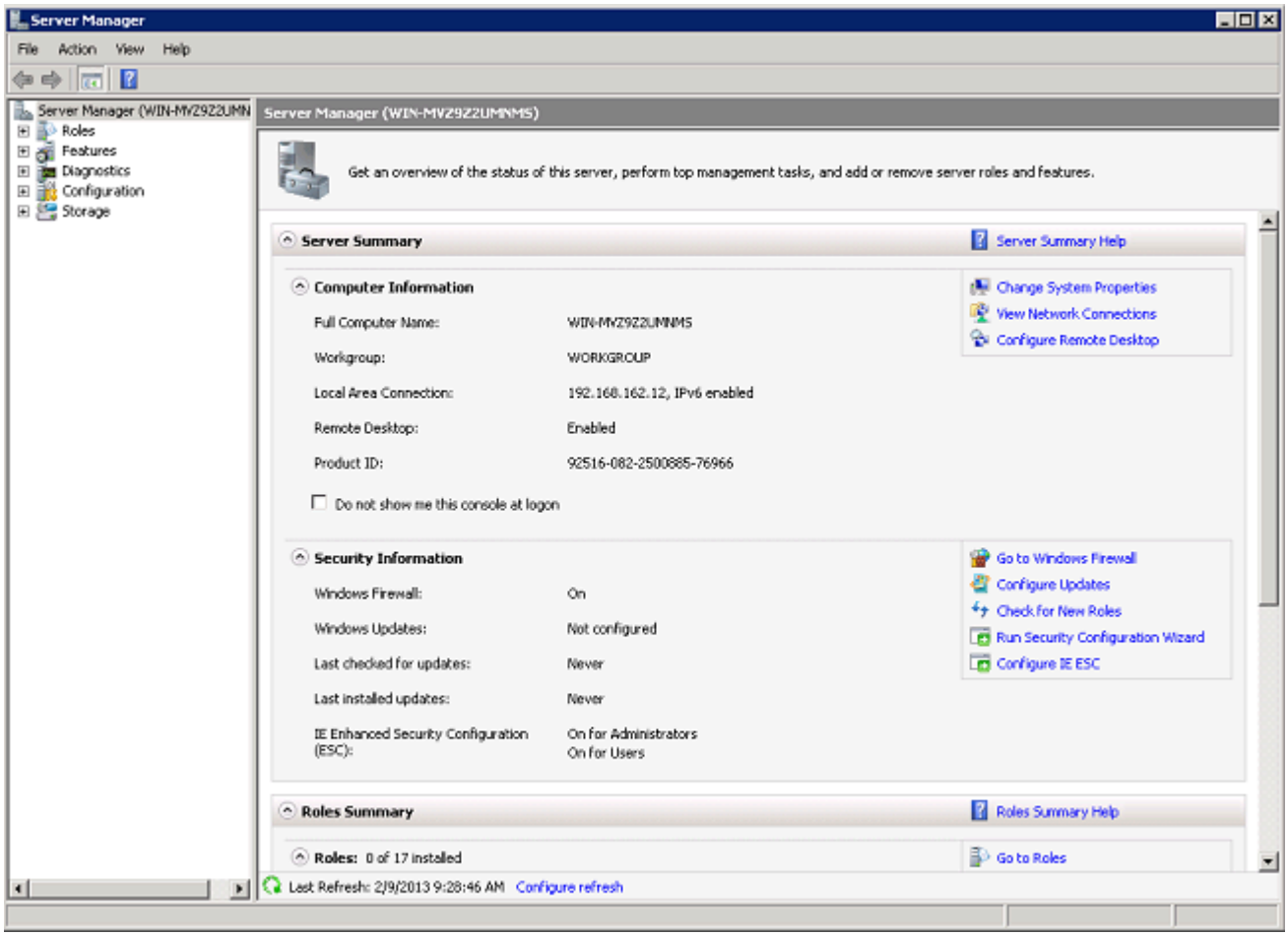
1. 將伺服器配置為域控制器。

2. 安裝和配置DHCP服務。
3. 將伺服器安裝並配置為CA伺服器。
4. 將客戶端連線到域。
5. 安裝NPS。
6. 安裝證書。
7. 配置NPS以進行PEAP身份驗證。
8. 將使用者新增到Active Directory。

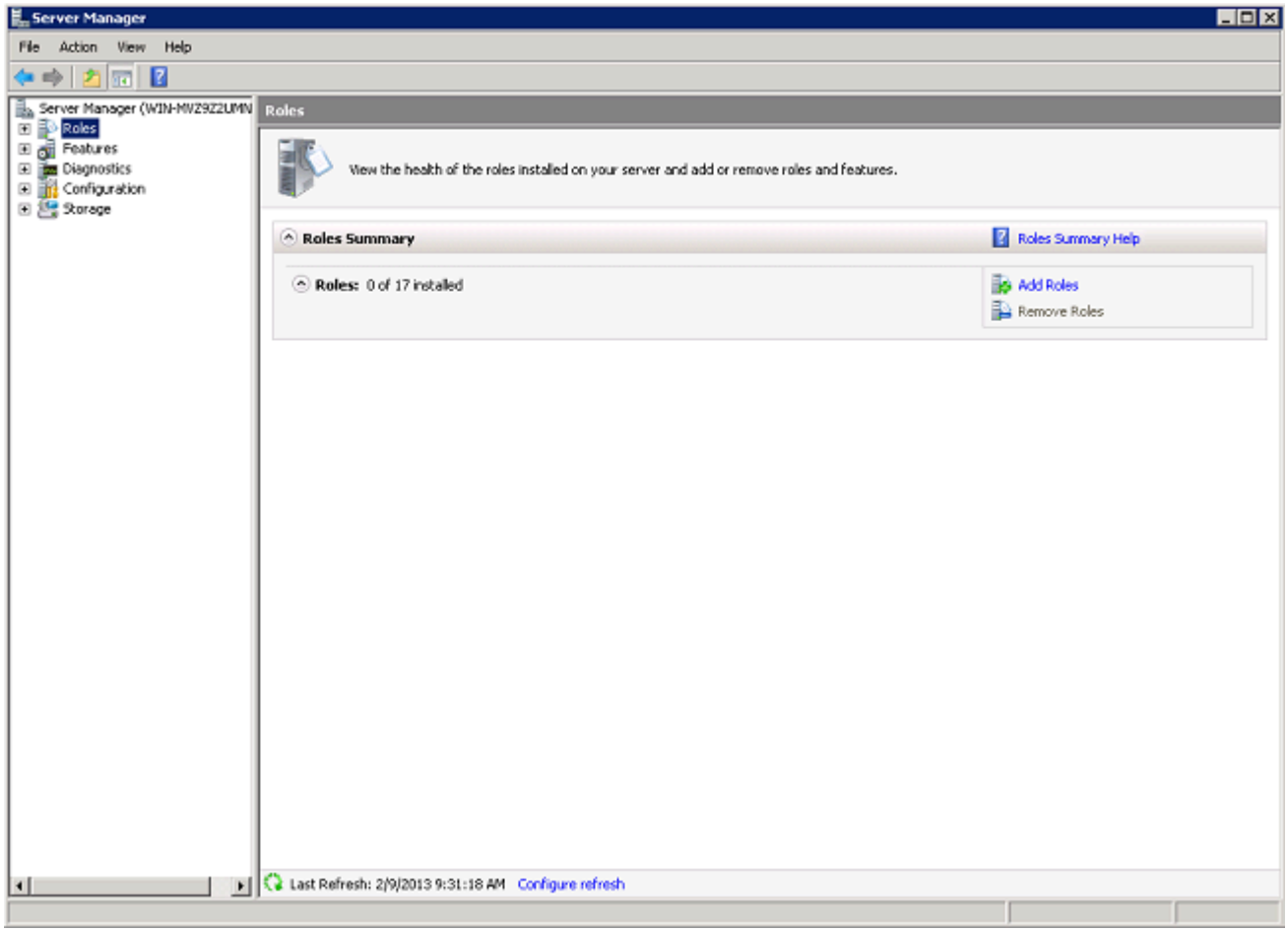
將Microsoft Windows 2008 Server配置為域控制器

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

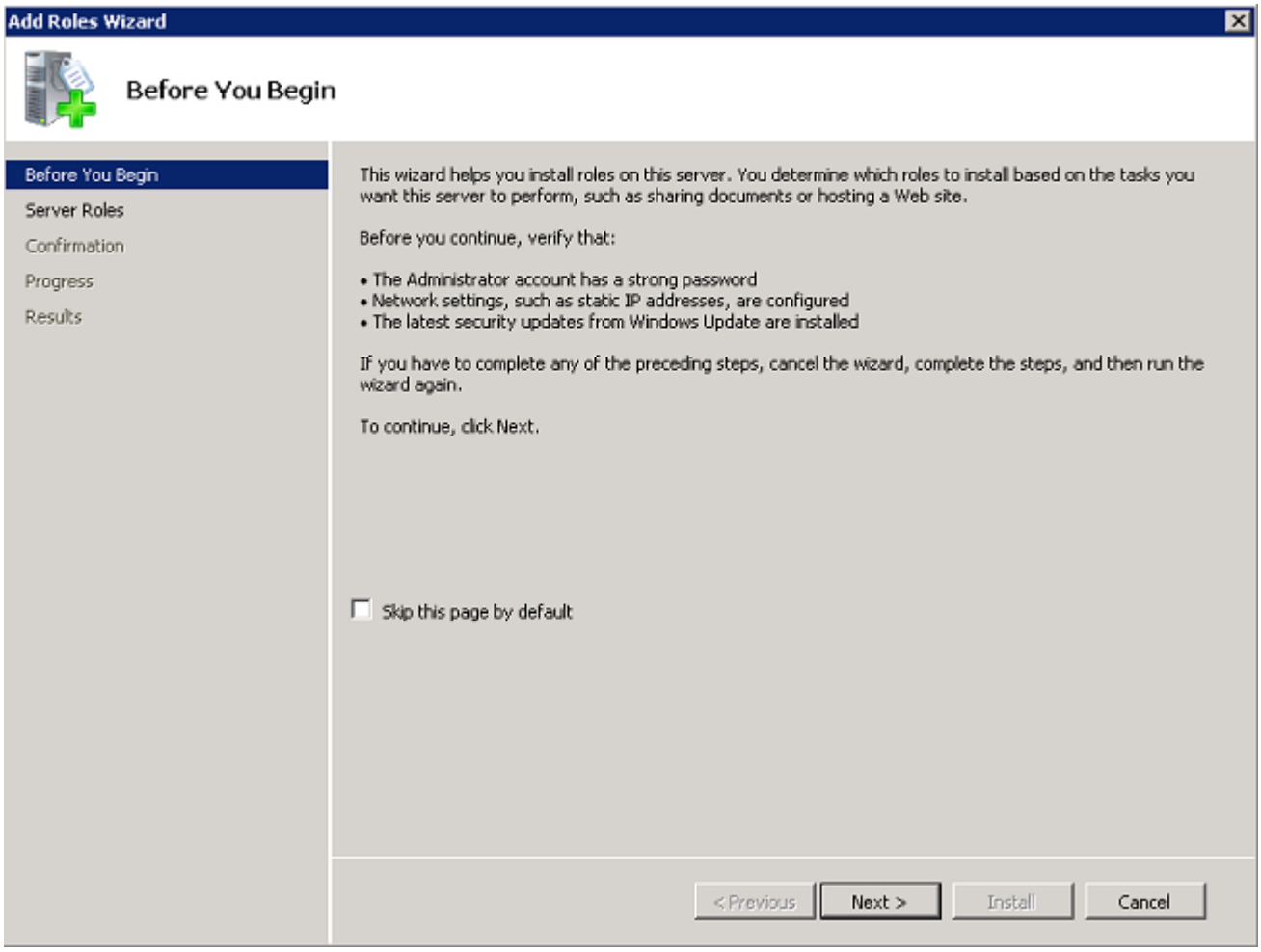
1. 按一下Start> Server Manager。



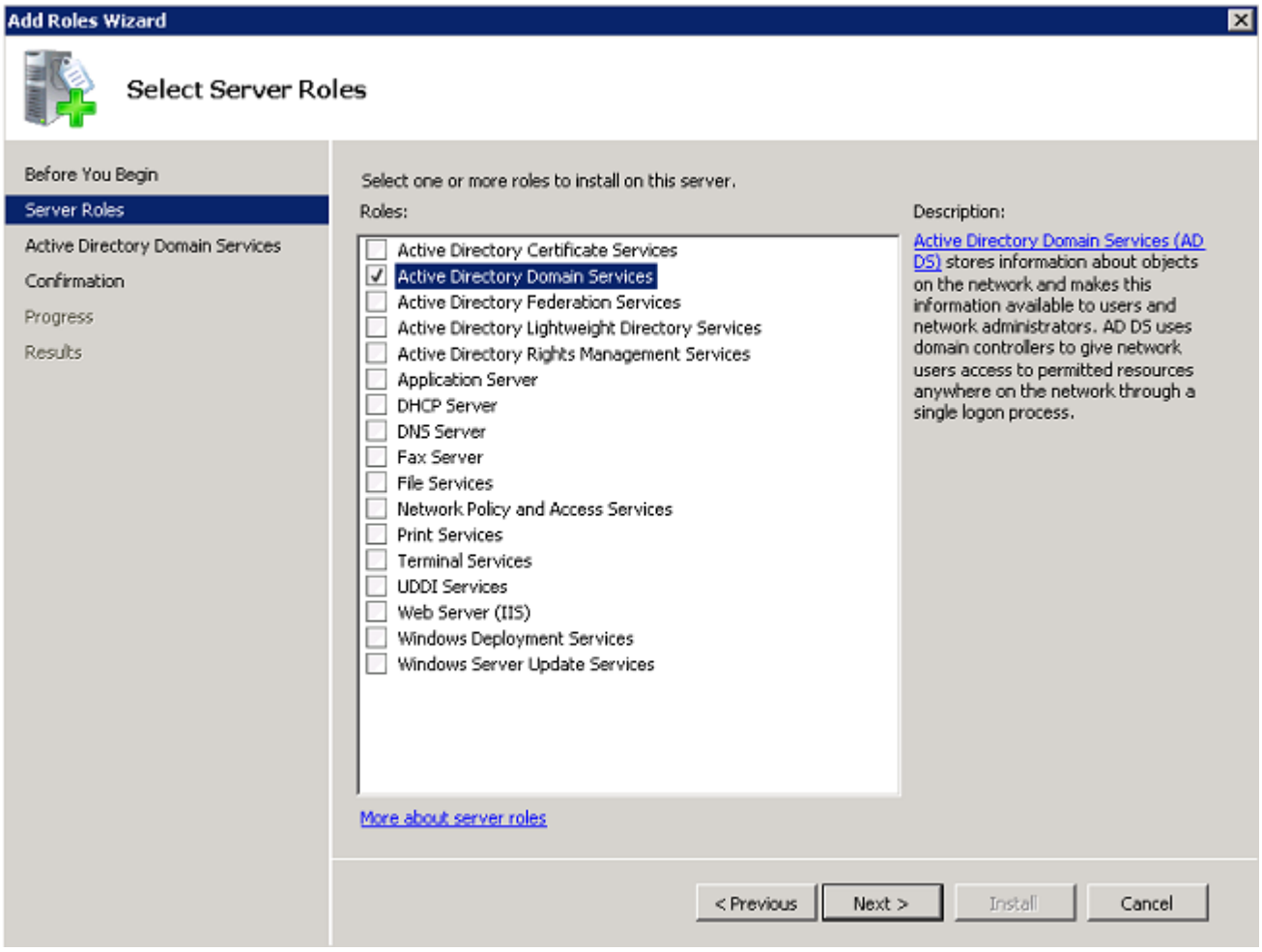
2. 按一下Roles> Add Roles。


Server Manager
File Action View Help
Server Manager (WIN-MVZ9ZZUMN
Roles
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 0 of 17 installed
Add Roles
Remove Roles
Last Refresh: 2/9/2013 9:31:18 AM Configure refresh

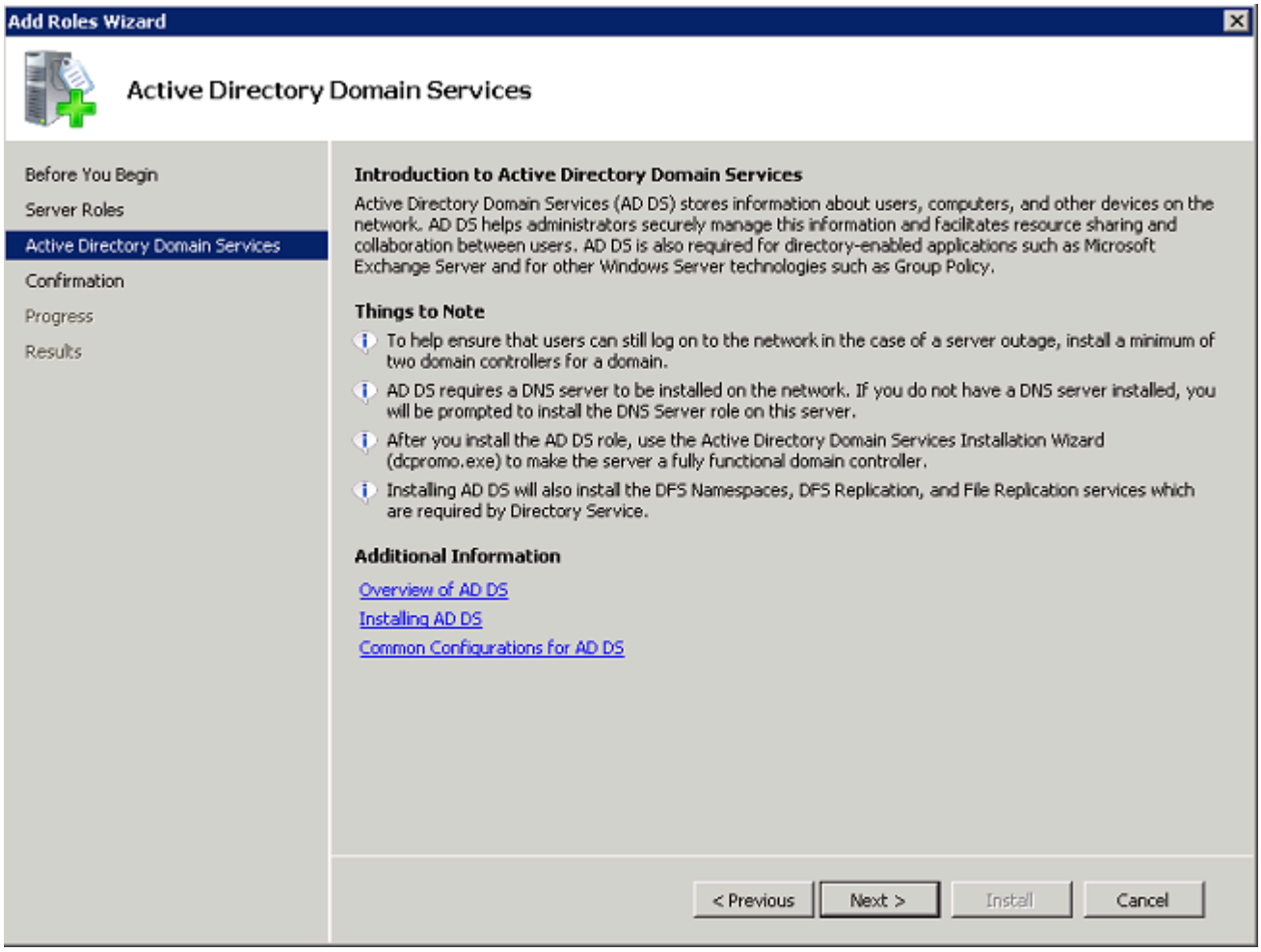
3. 按「Next」（下一步）。



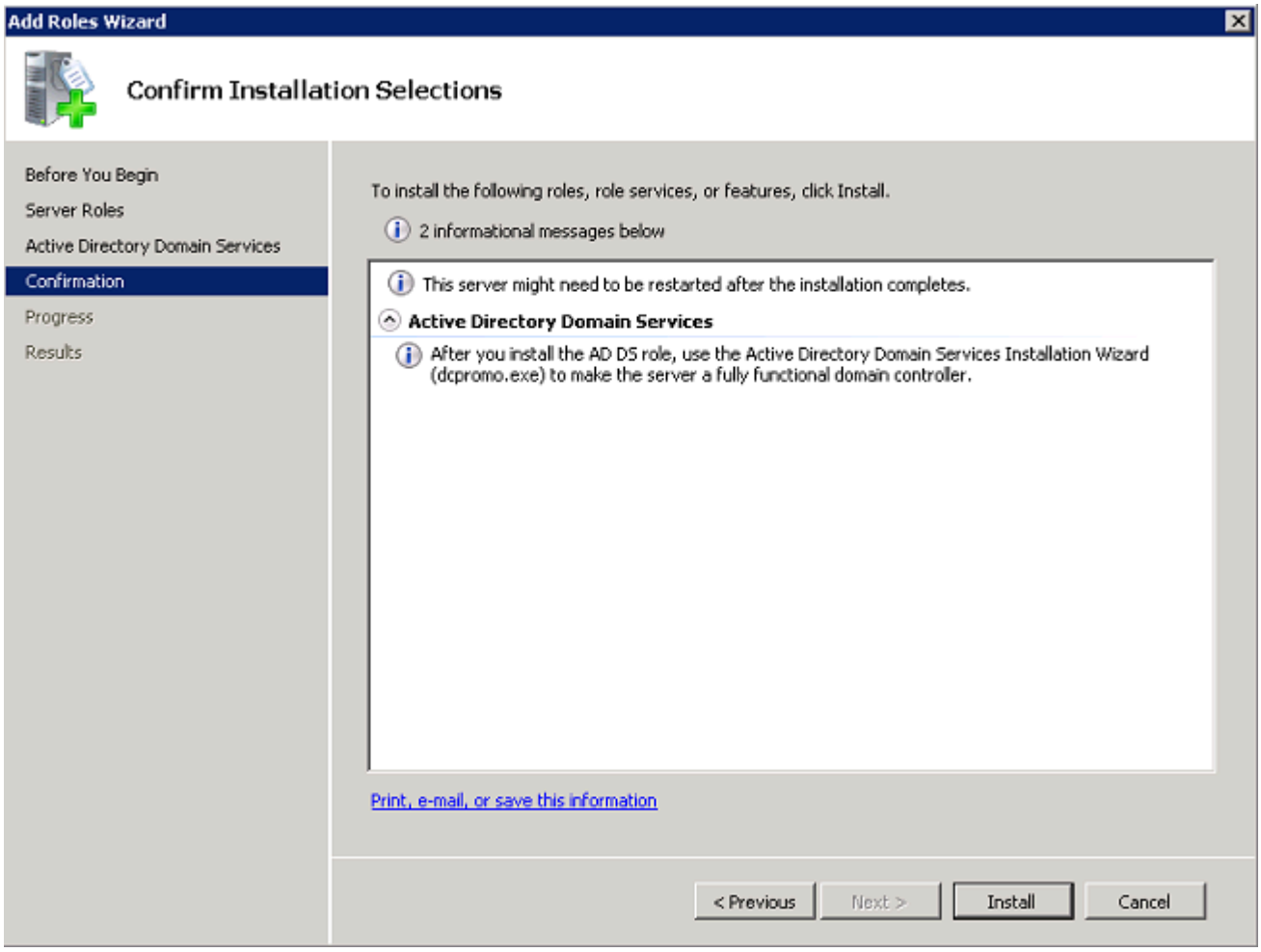
4. 選擇服務Active Directory域服務，然後按一下下一步。



5. 檢視Active Directory域服務簡介，然後按一下下一步。

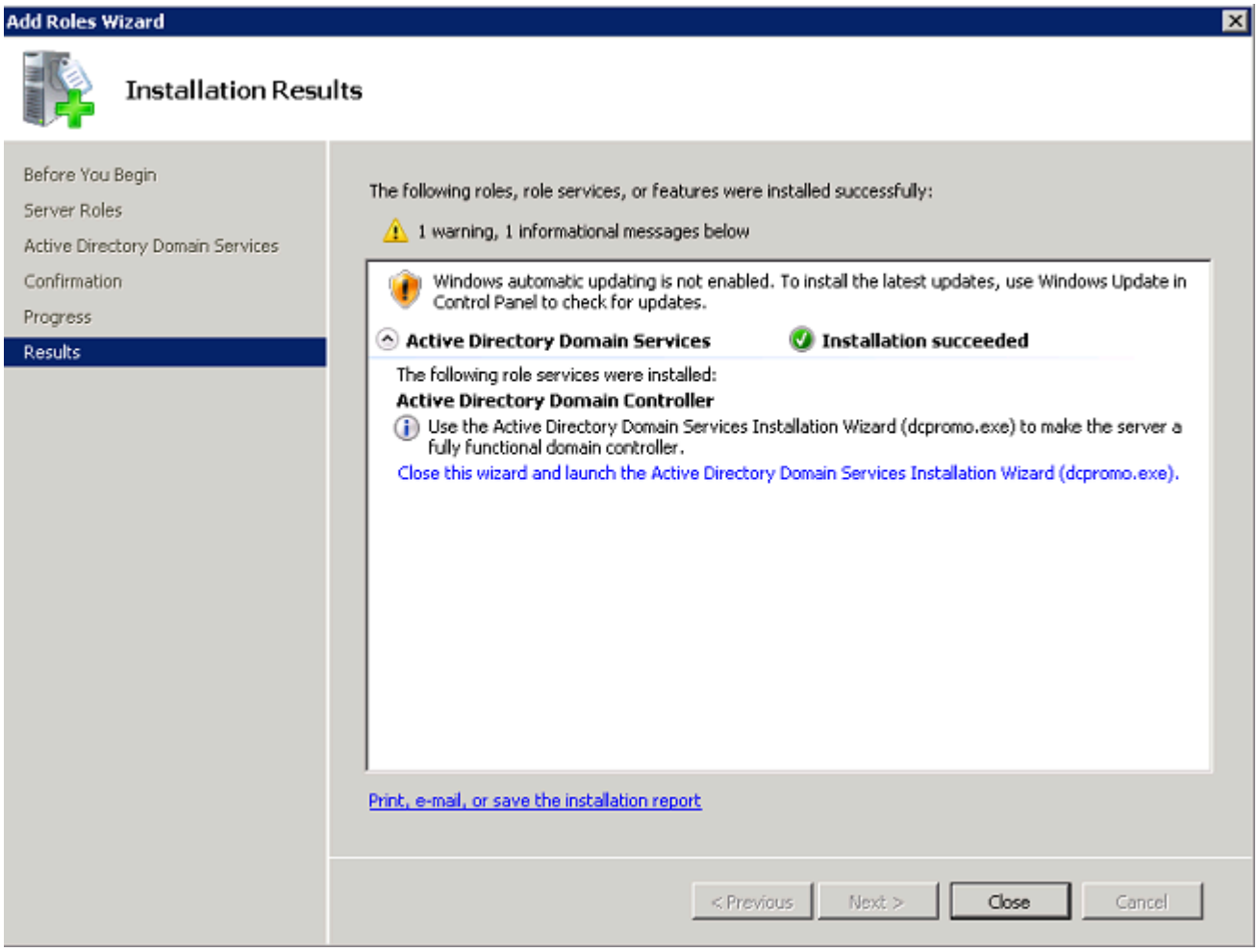


6. 按一下「Install」開始安裝過程。

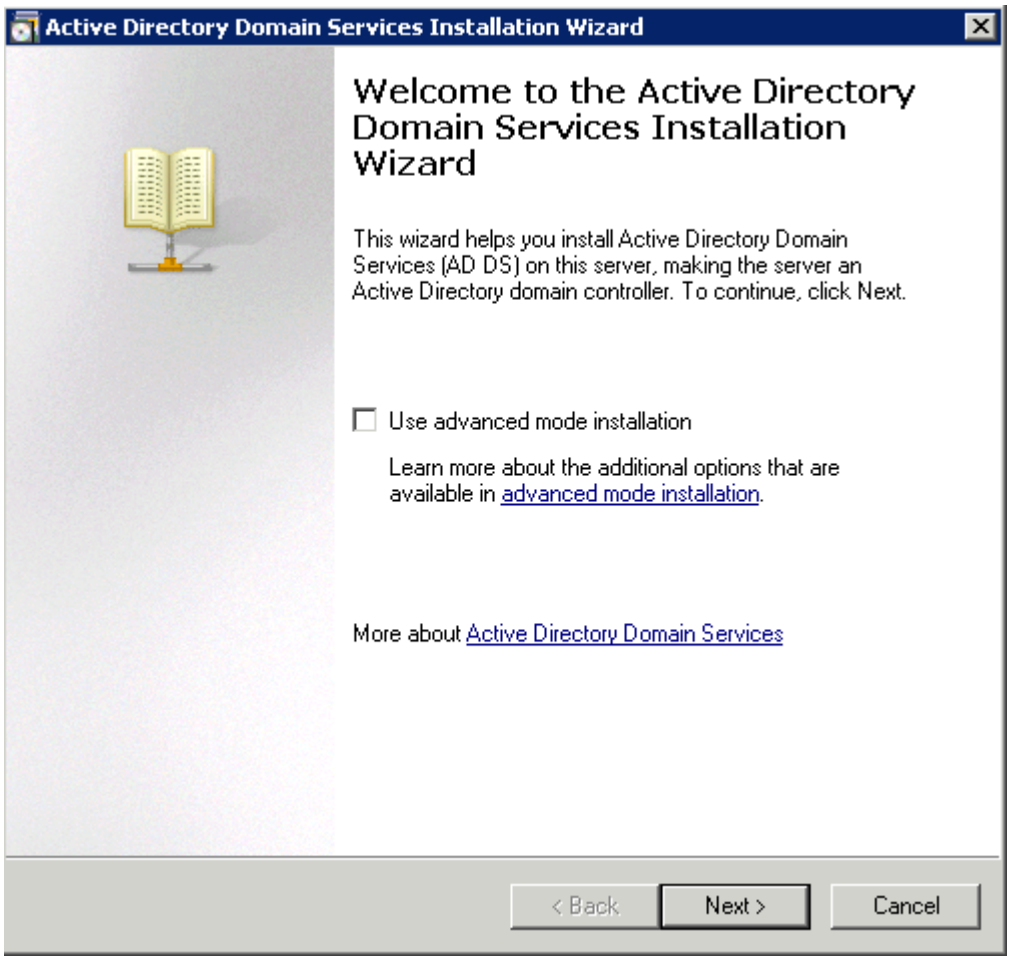


安裝繼續並完成。

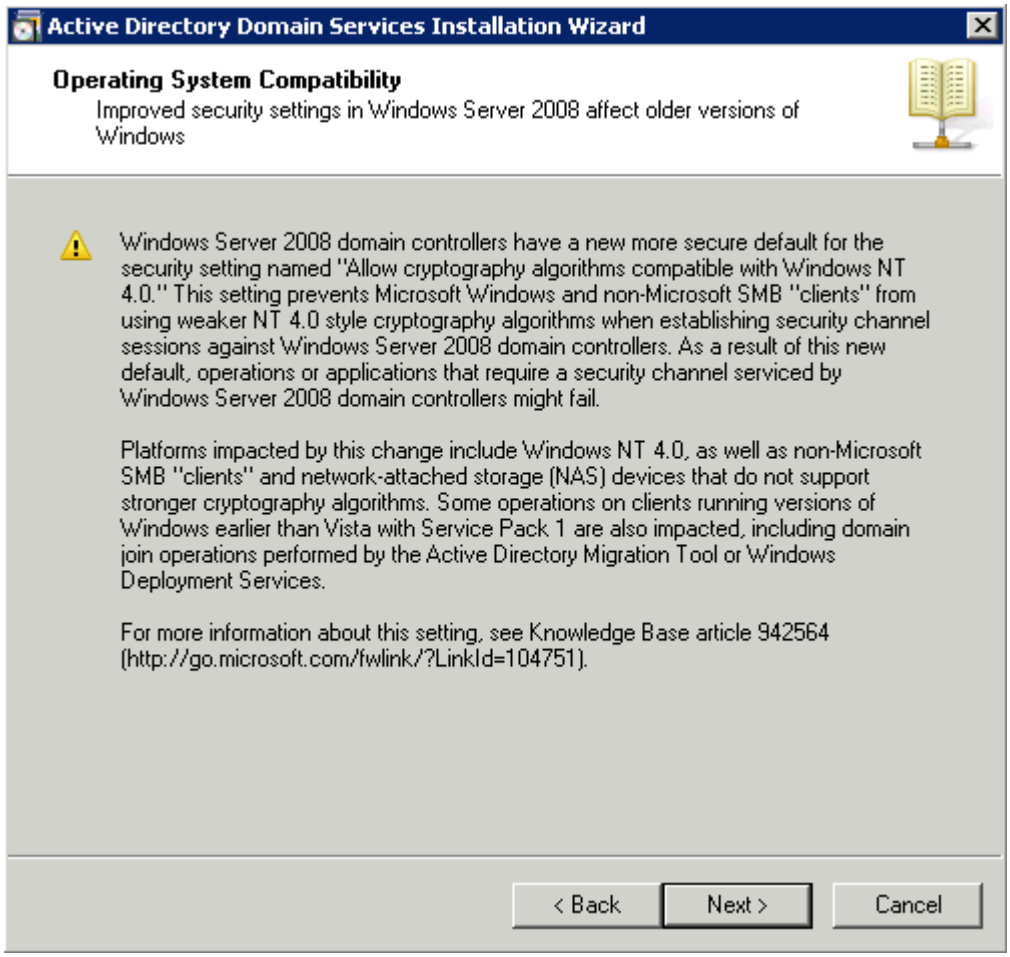
7. 按一下關閉此嚮導並啟動Active Directory域服務安裝嚮導(dcpromo.exe)，以繼續安裝和配置Active Directory。



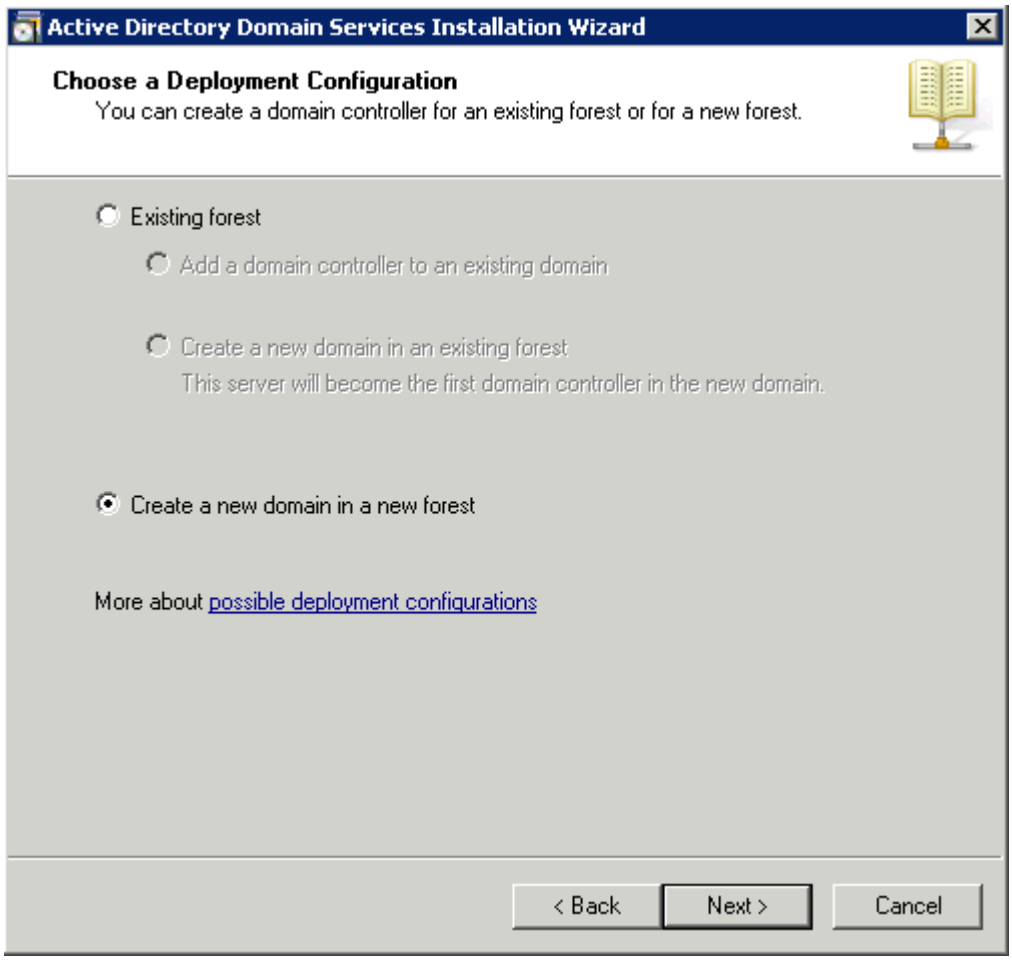
8. 按一下下一步以運行Active Directory域服務安裝嚮導。



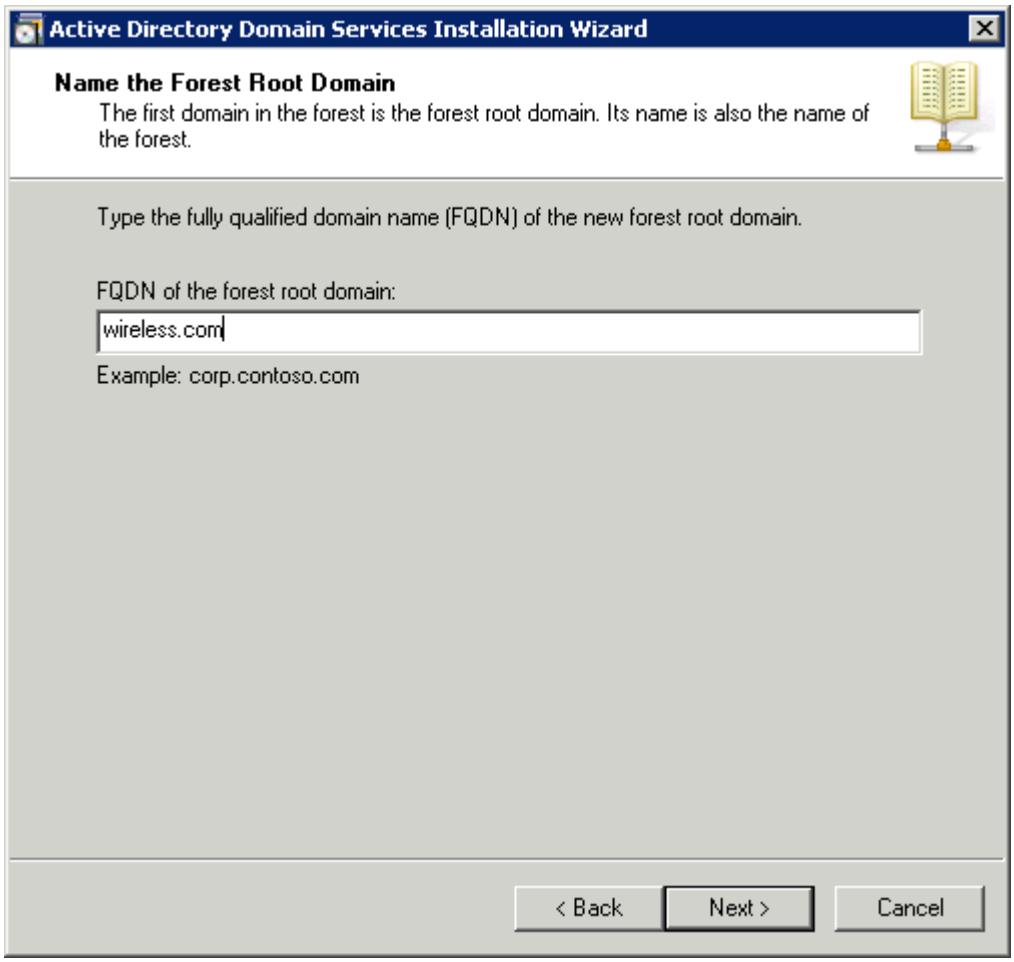
9. 檢視有關作業系統相容性的資訊，然後按一下下一步。



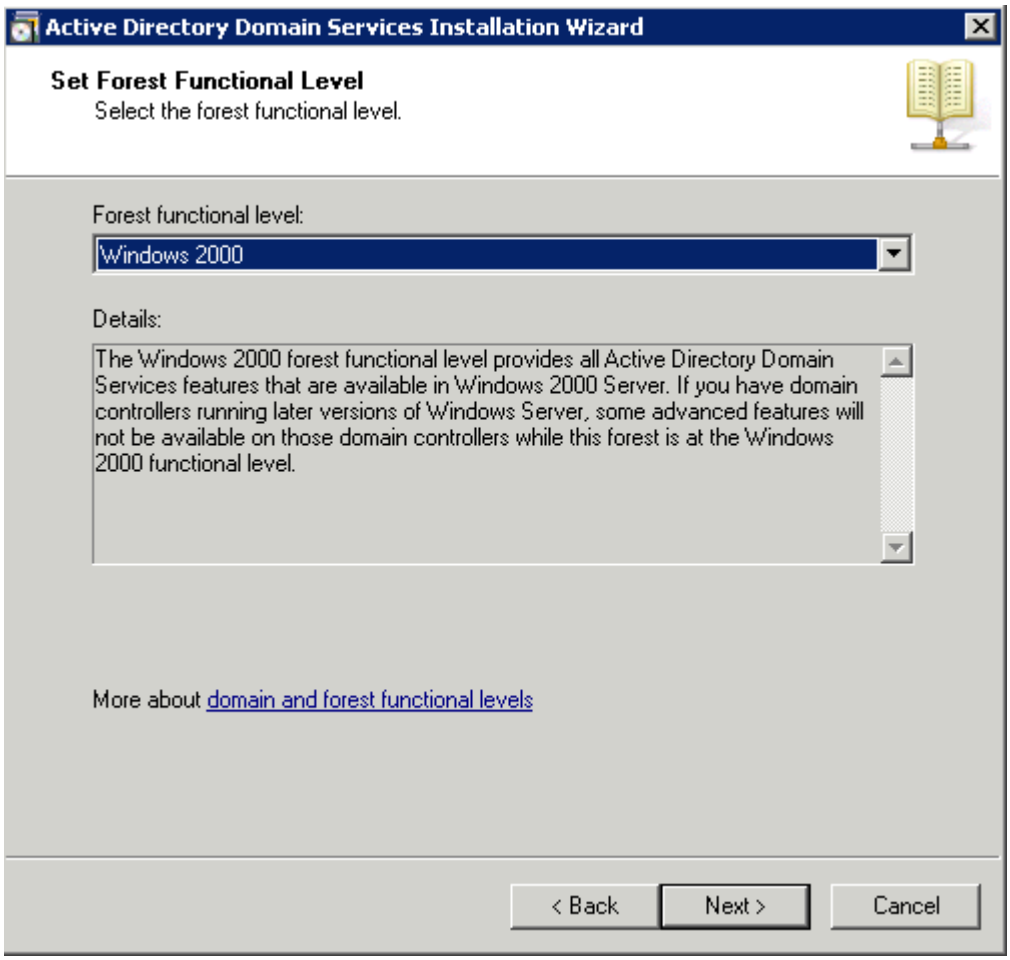
10. 按一下在新林中建立新域>下一步以建立新域。



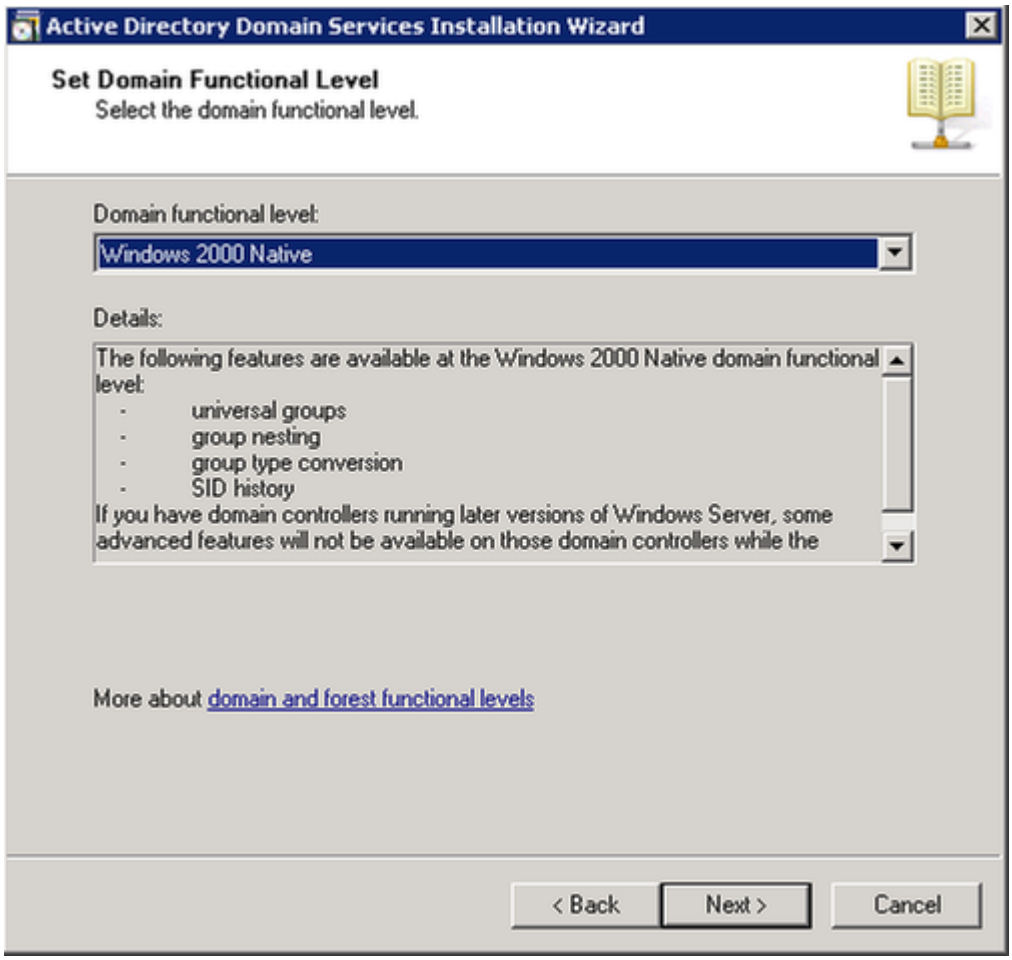
11. 輸入新域的完整DNS名稱，然後按一下Next。



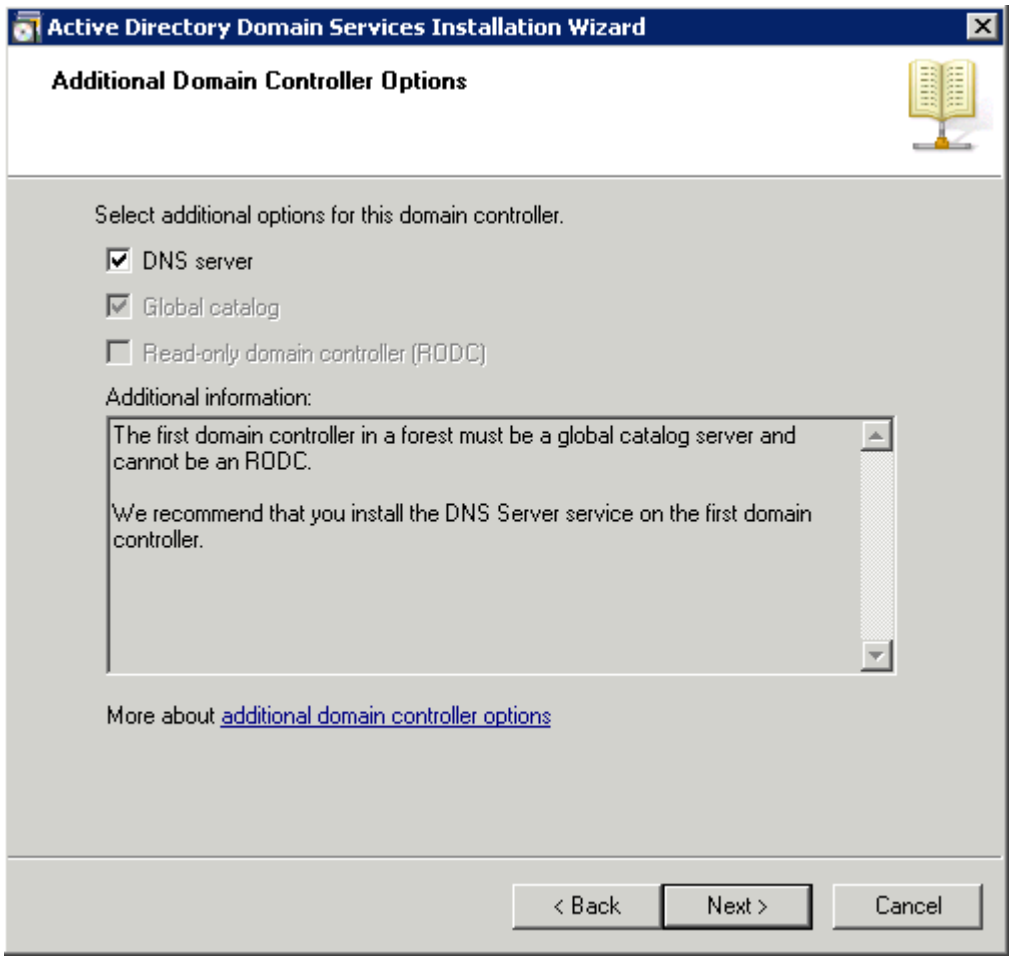
12. 選擇域的林功能級別，然後按一下下一步。



13. 選擇域的域功能級別，然後按一下下一步。

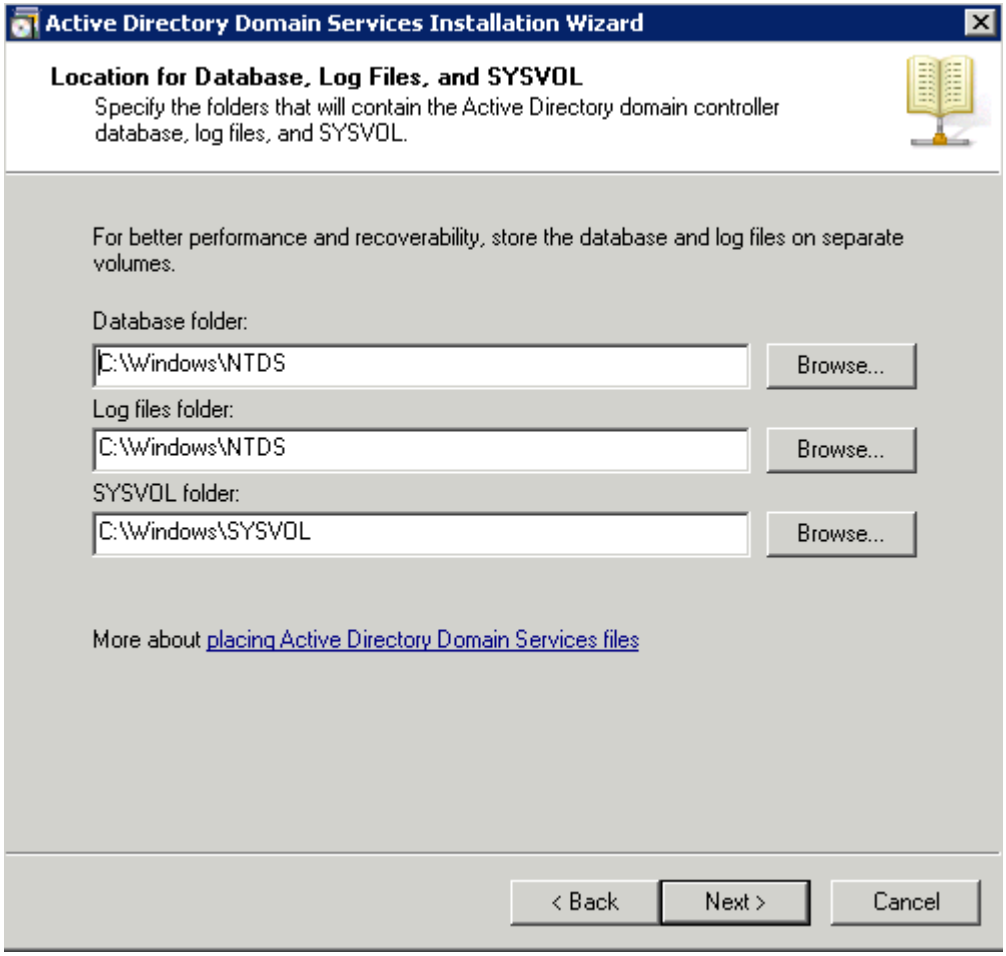


14. 確保已選擇DNS伺服器，然後按一下下一步。

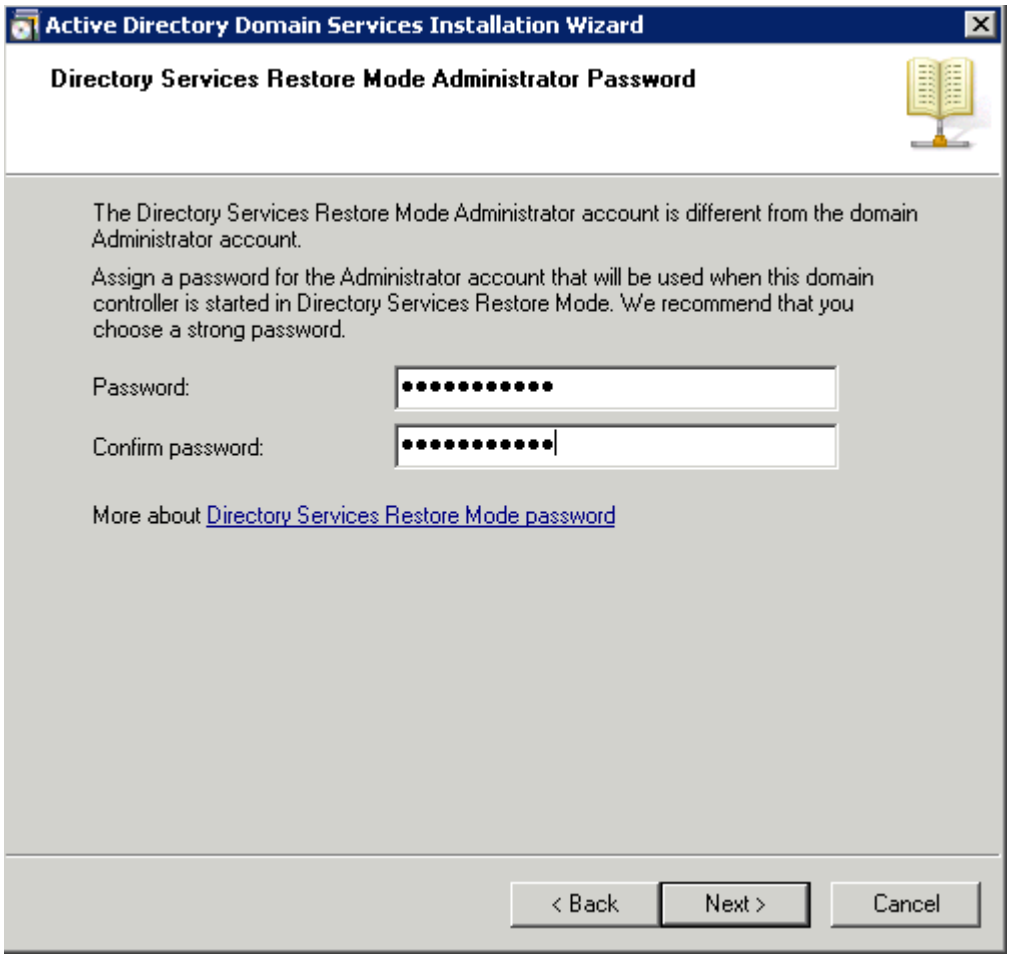


15. 按一下Yes安裝嚮導在DNS中為域建立一個新區域。

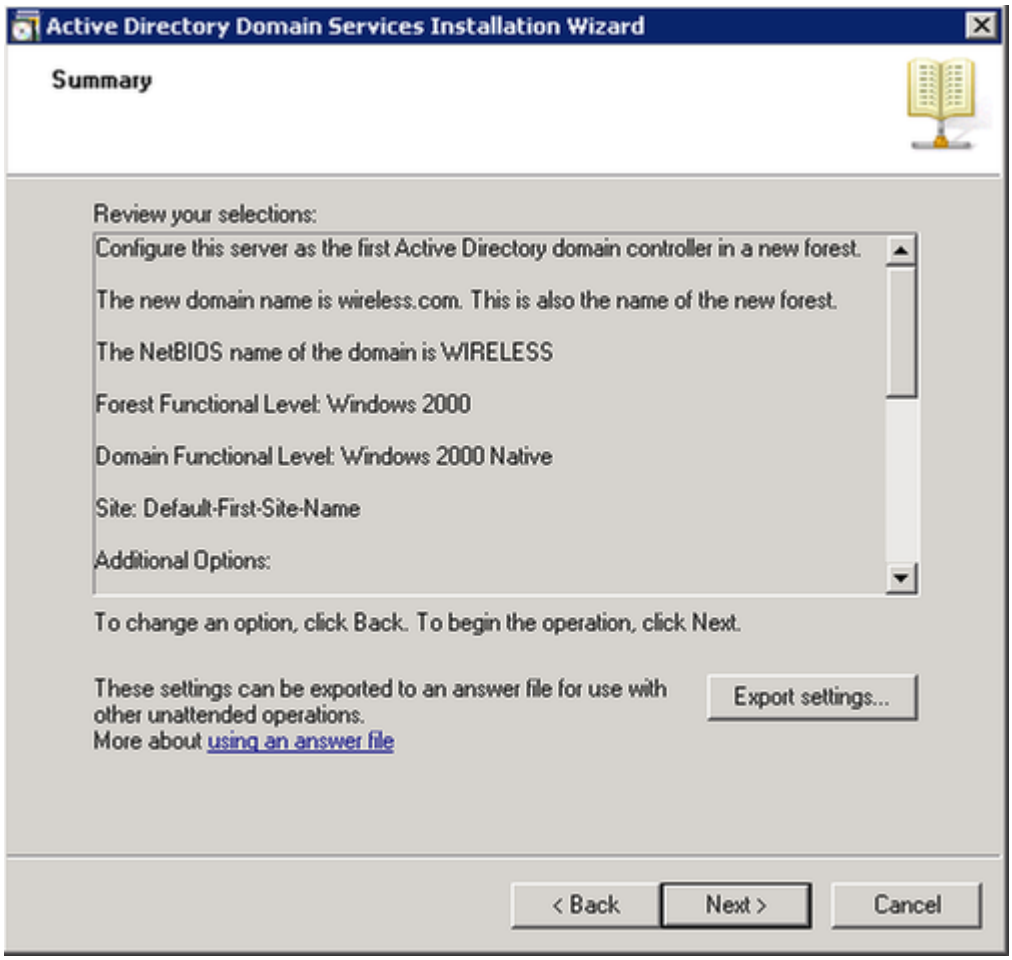
16. 選擇Active Directory必須用於其檔案的資料夾，然後按一下下一步。



17. 輸入管理員密碼，然後按一下下一步。

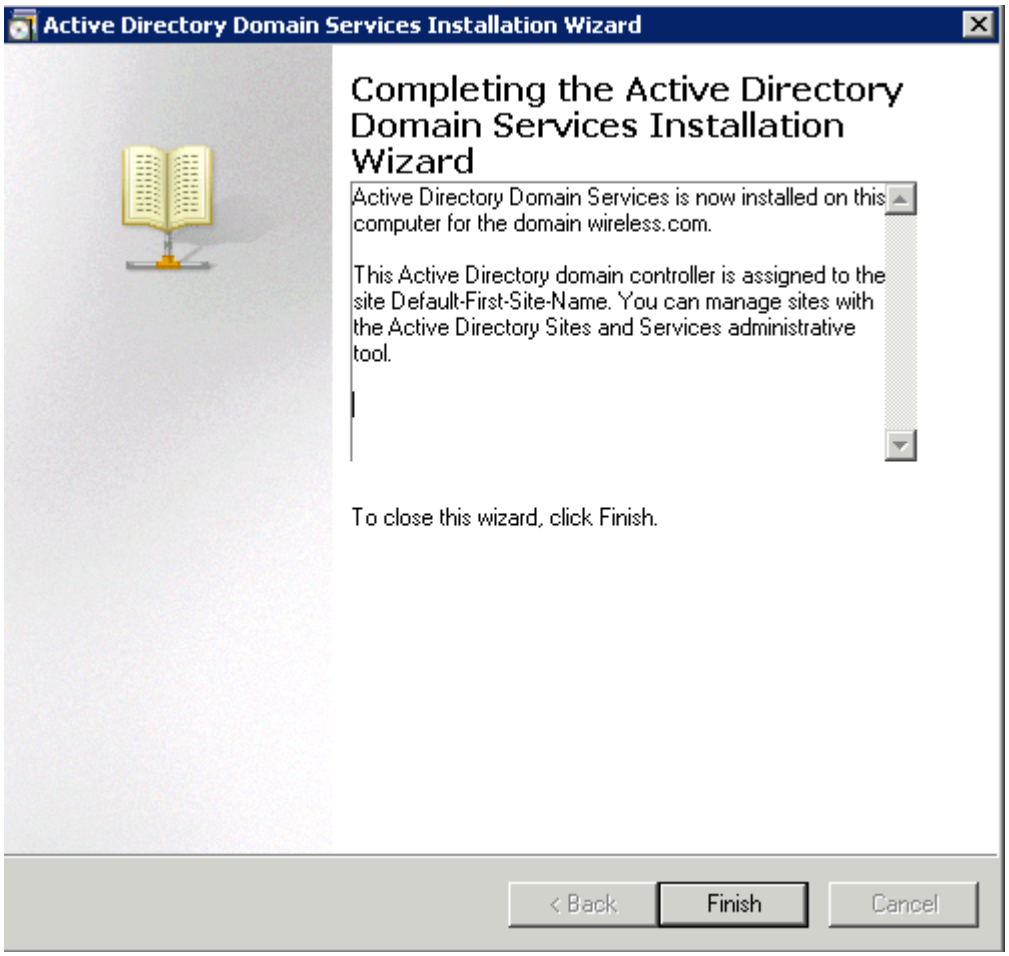


18. 檢查您的選擇，然後按一下下一步。

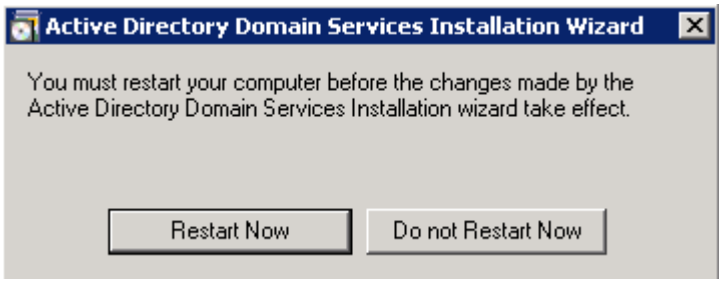


安裝繼續進行。

19. 按一下完成關閉嚮導。



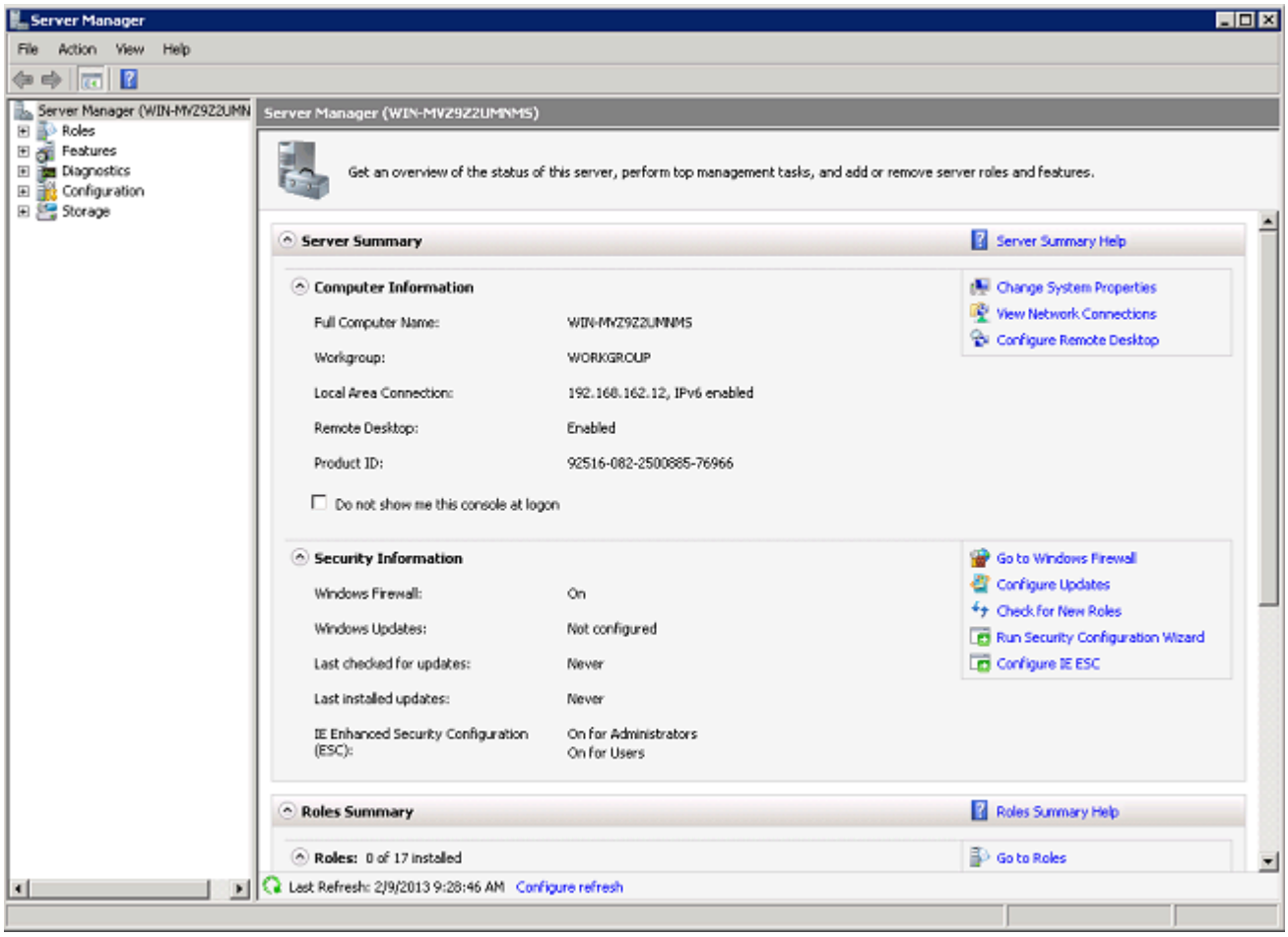
20. 重新啟動伺服器以使更改生效。



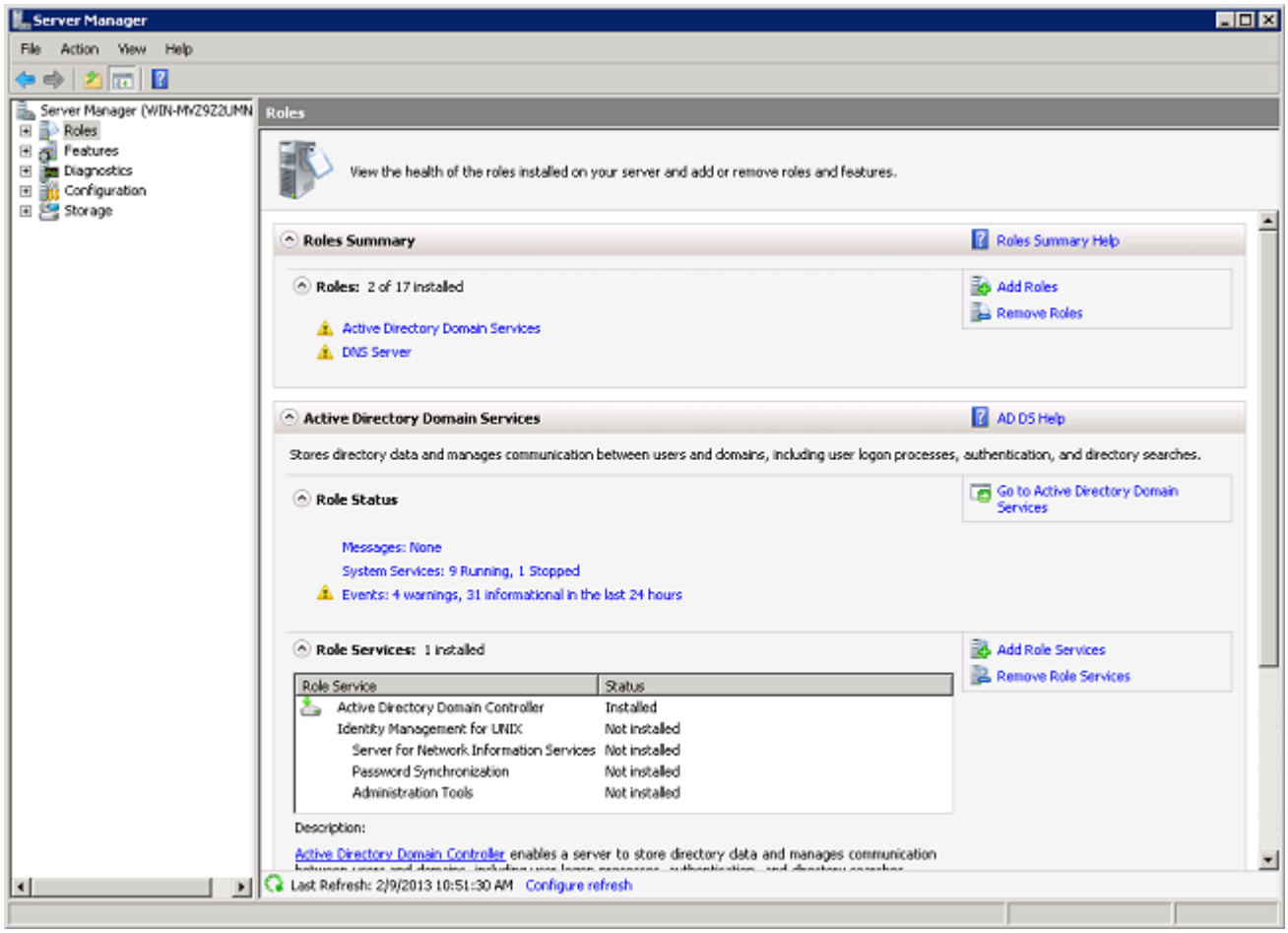
在Microsoft Windows 2008 Server上安裝並配置DHCP服務

Microsoft 2008伺服器上的DHCP服務用於向無線客戶端提供IP地址。完成以下步驟即可安裝和配置DHCP服務：

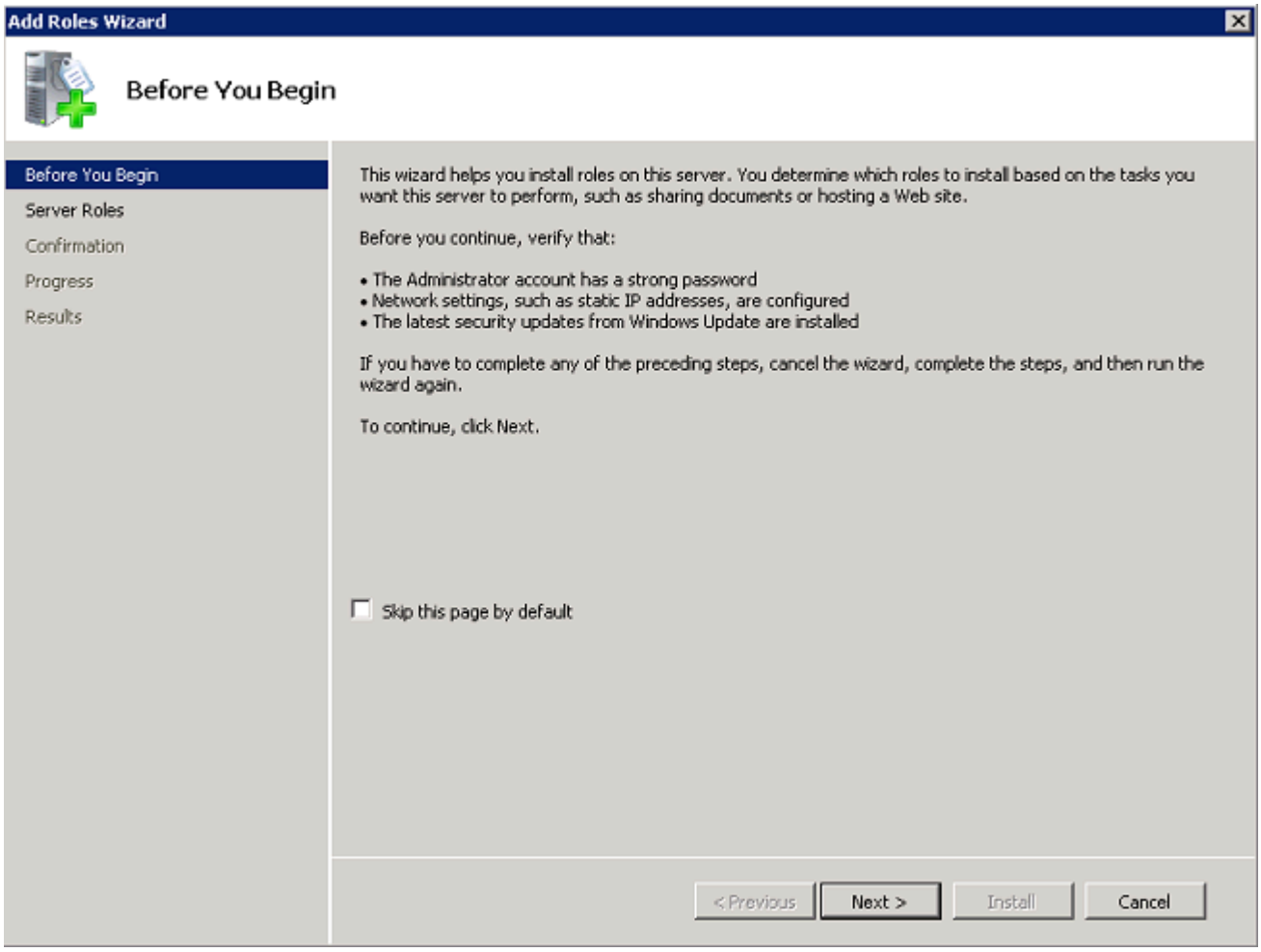
1. 按一下Start>Server Manager。



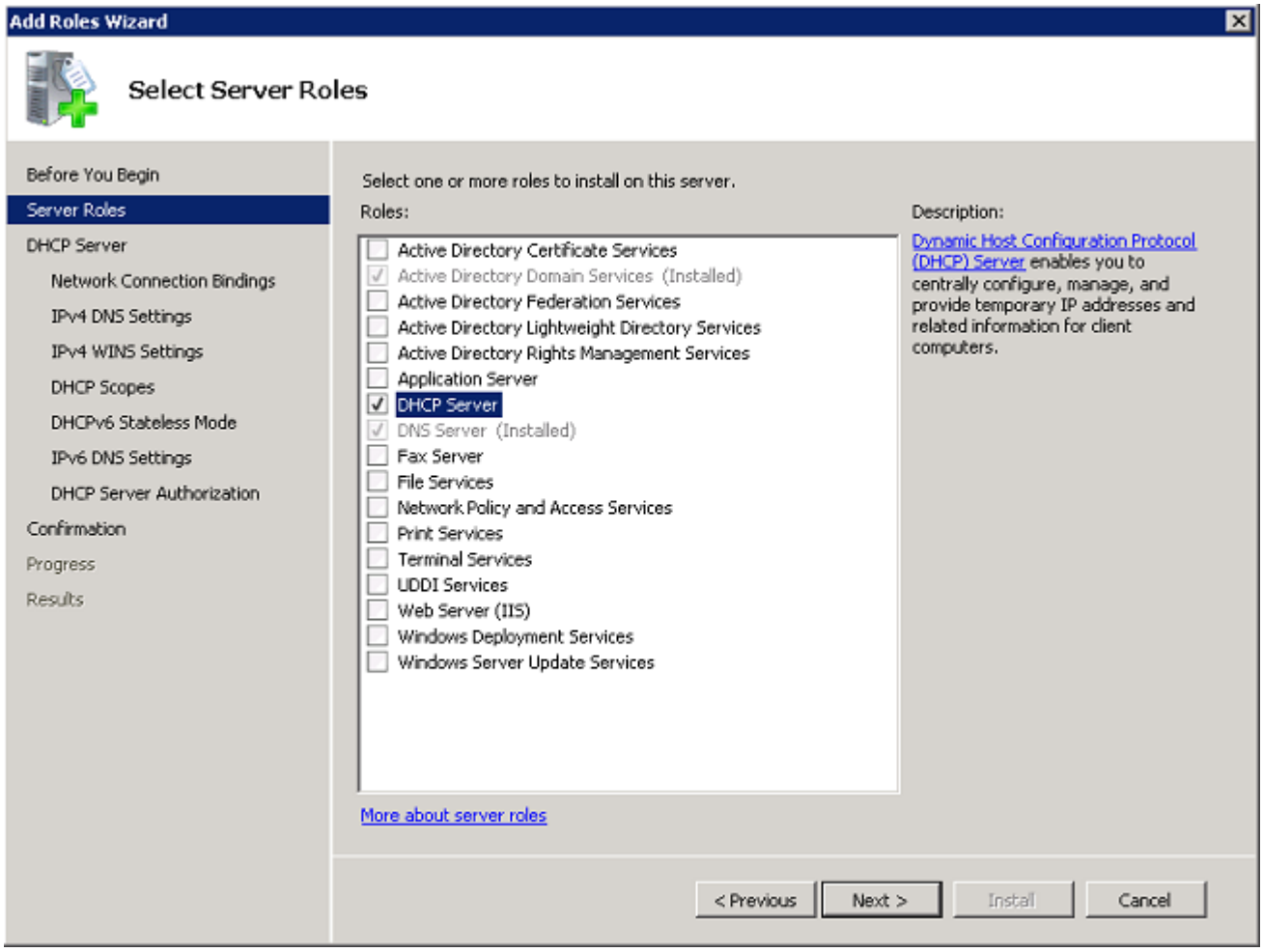
2. 按一下Roles> Add Roles。


Server Manager
File Action View Help
Server Manager (WIN-MV29Z2UMN
Roles
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 2 of 17 installed
Add Roles
Remove Roles
Active Directory Domain Services
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:
Active Directory Domain Controller enables a server to store directory data and manages communication
Last Refresh: 2/9/2013 10:51:30 AM
Configure refresh

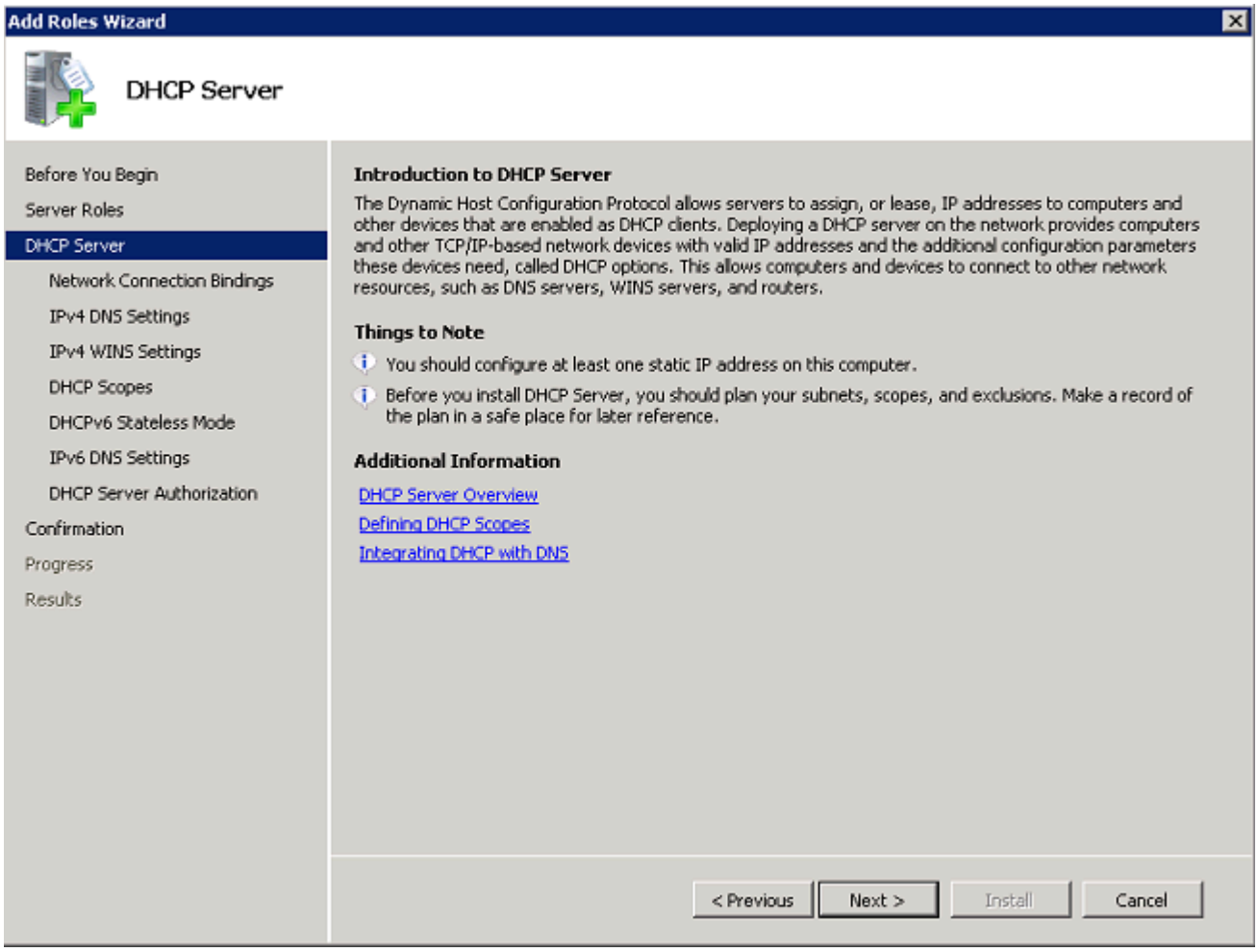
3. 按「Next」（下一步）。



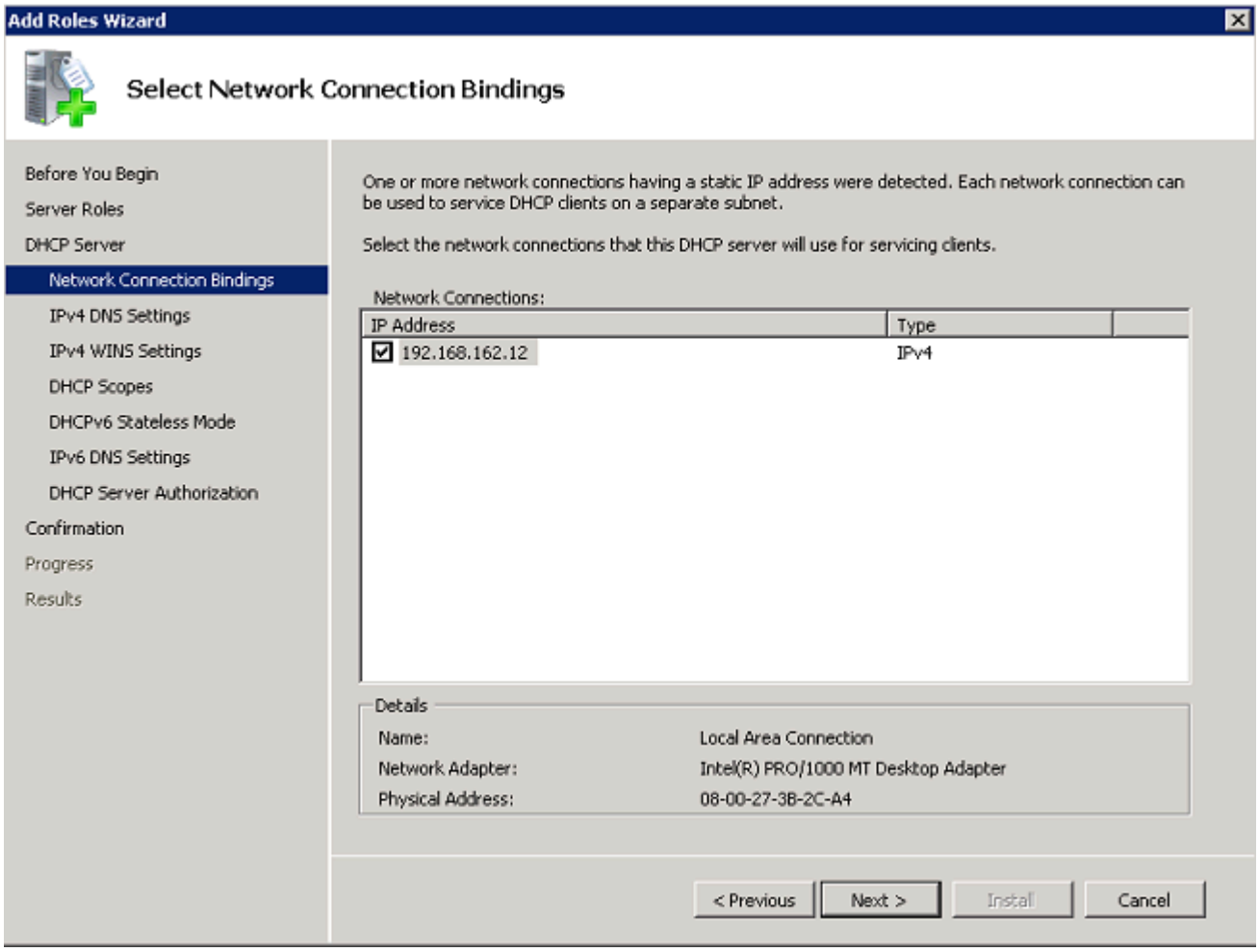
4. 選擇服務DHCP Server，然後按一下Next。



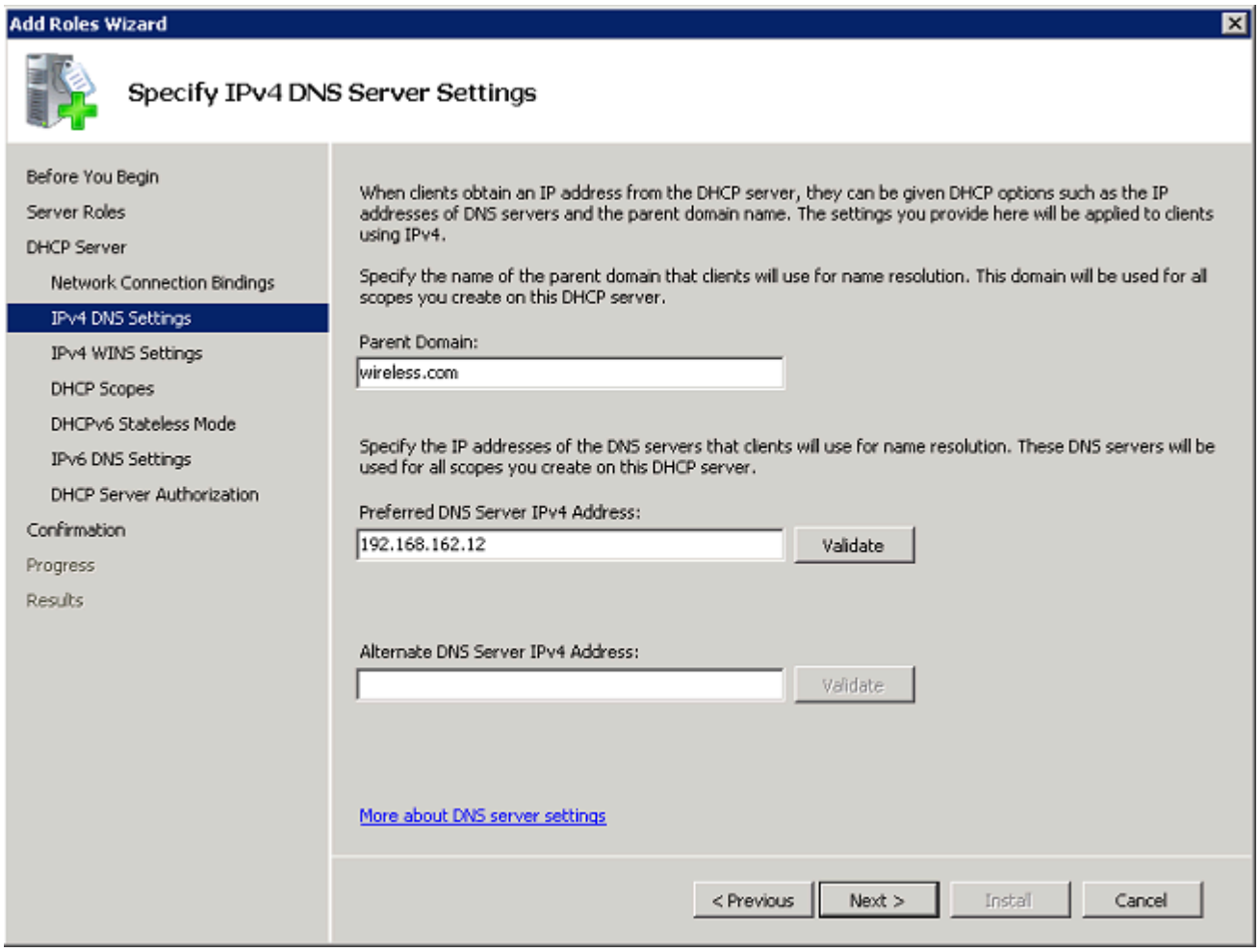
5. 檢視DHCP伺服器簡介，然後按一下下一步。



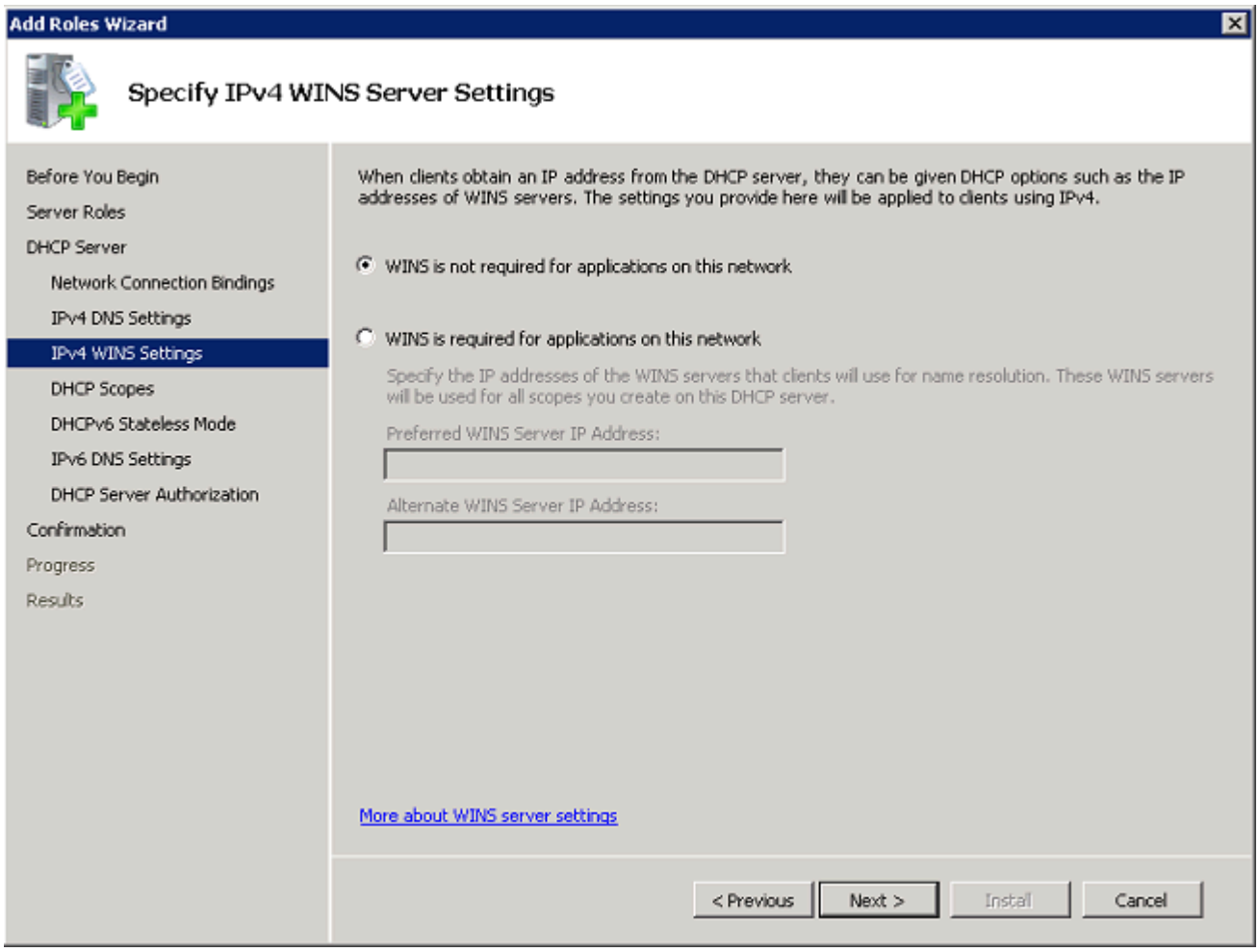
6. 選擇DHCP伺服器必須為請求監控的介面，然後按一下下一步。



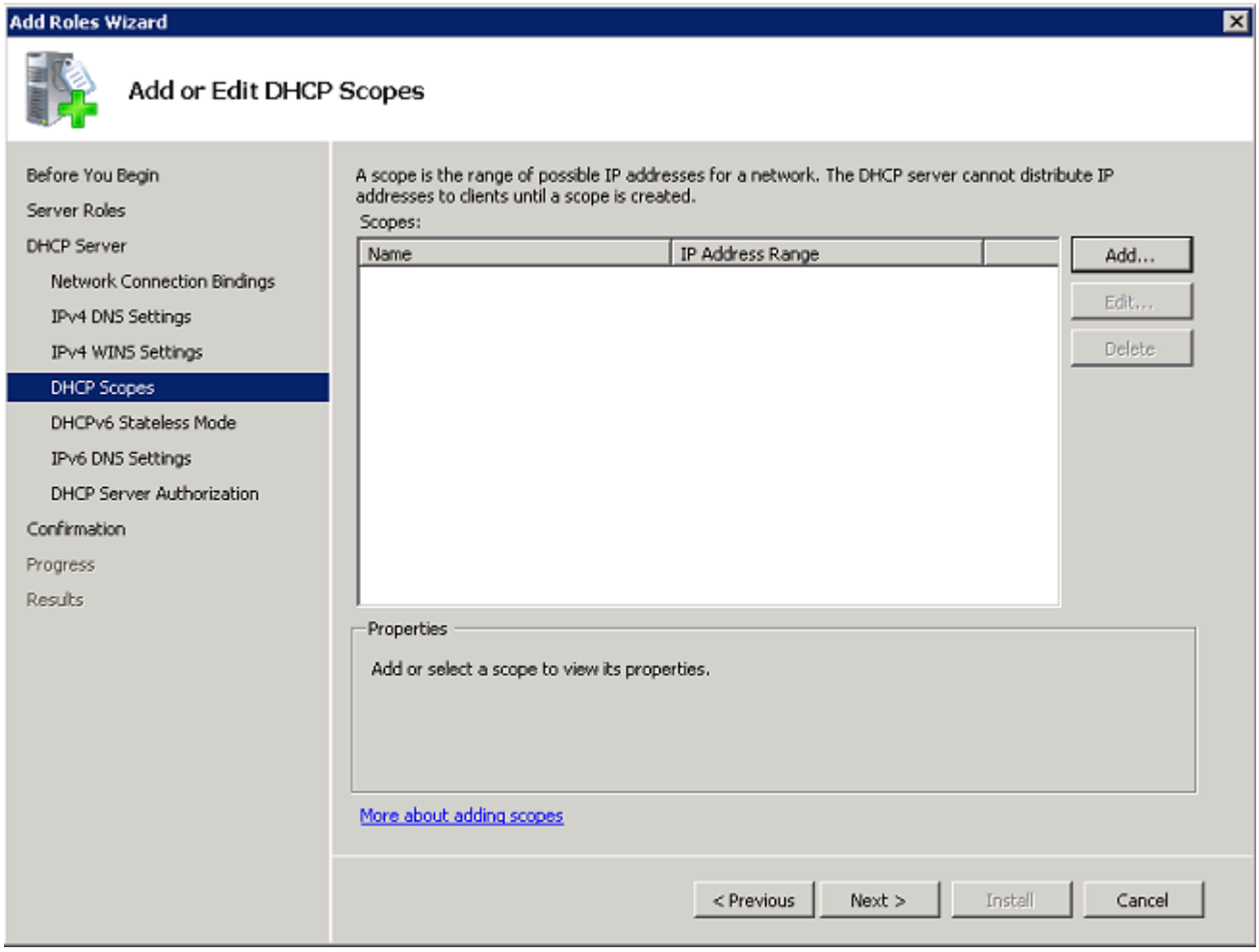
7. 配置DHCP伺服器必須提供給客戶端的預設DNS設定，然後按一下下一步。



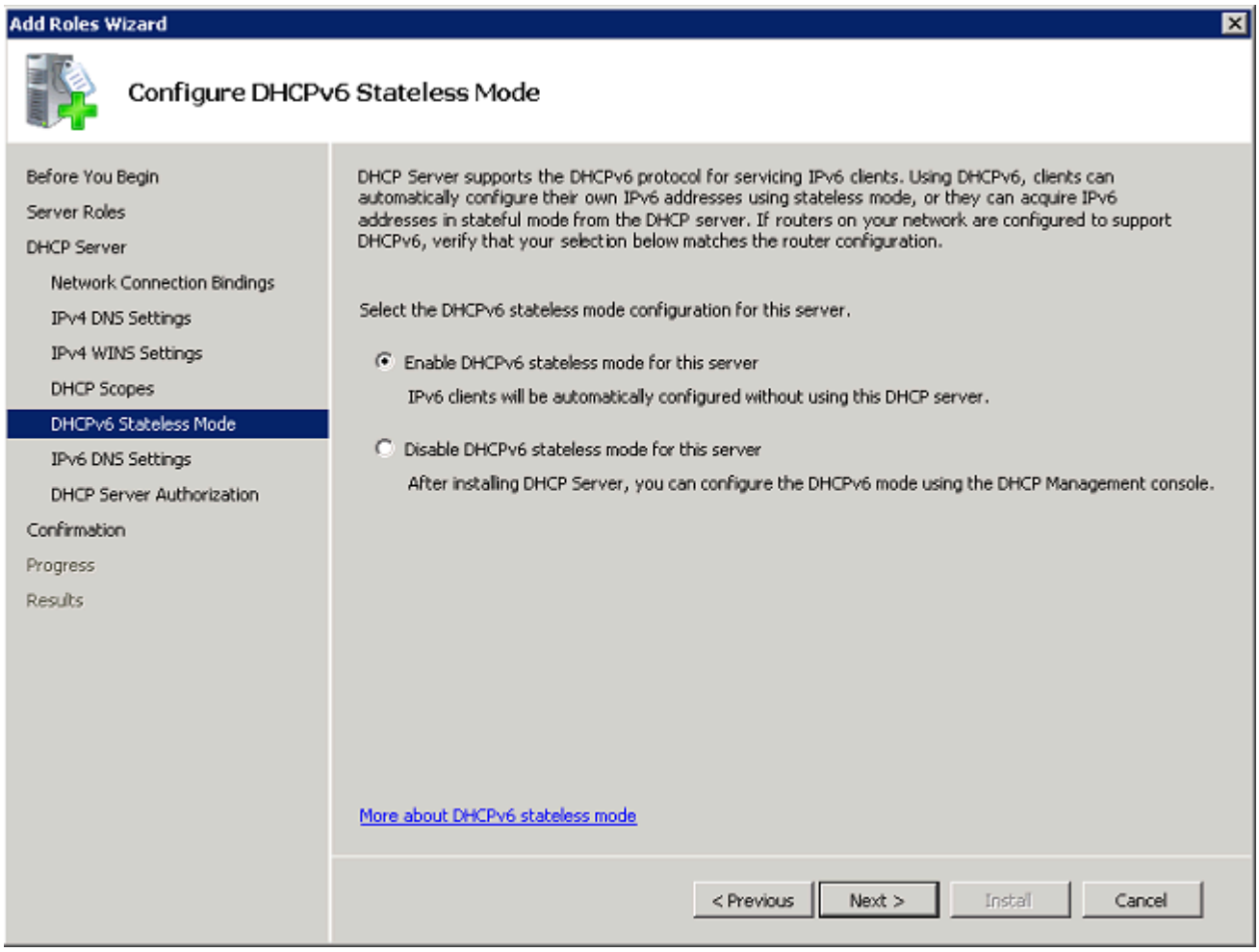
8. 如果網路支援WINS，則配置WINS。



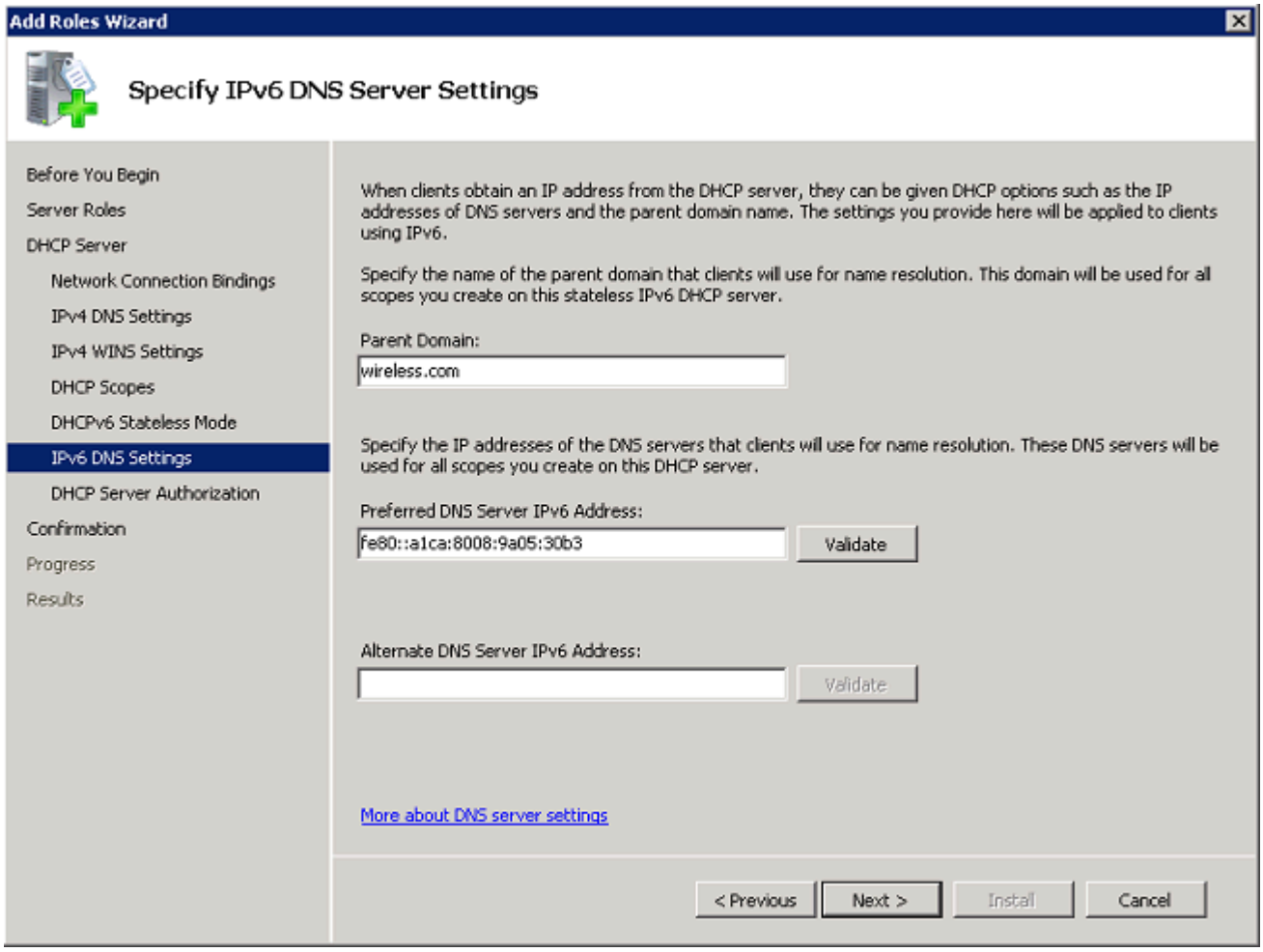
9. 按一下Add以使用嚮導建立DHCP作用域，或按一下Next稍後建立DHCP作用域。按一下下一步繼續。



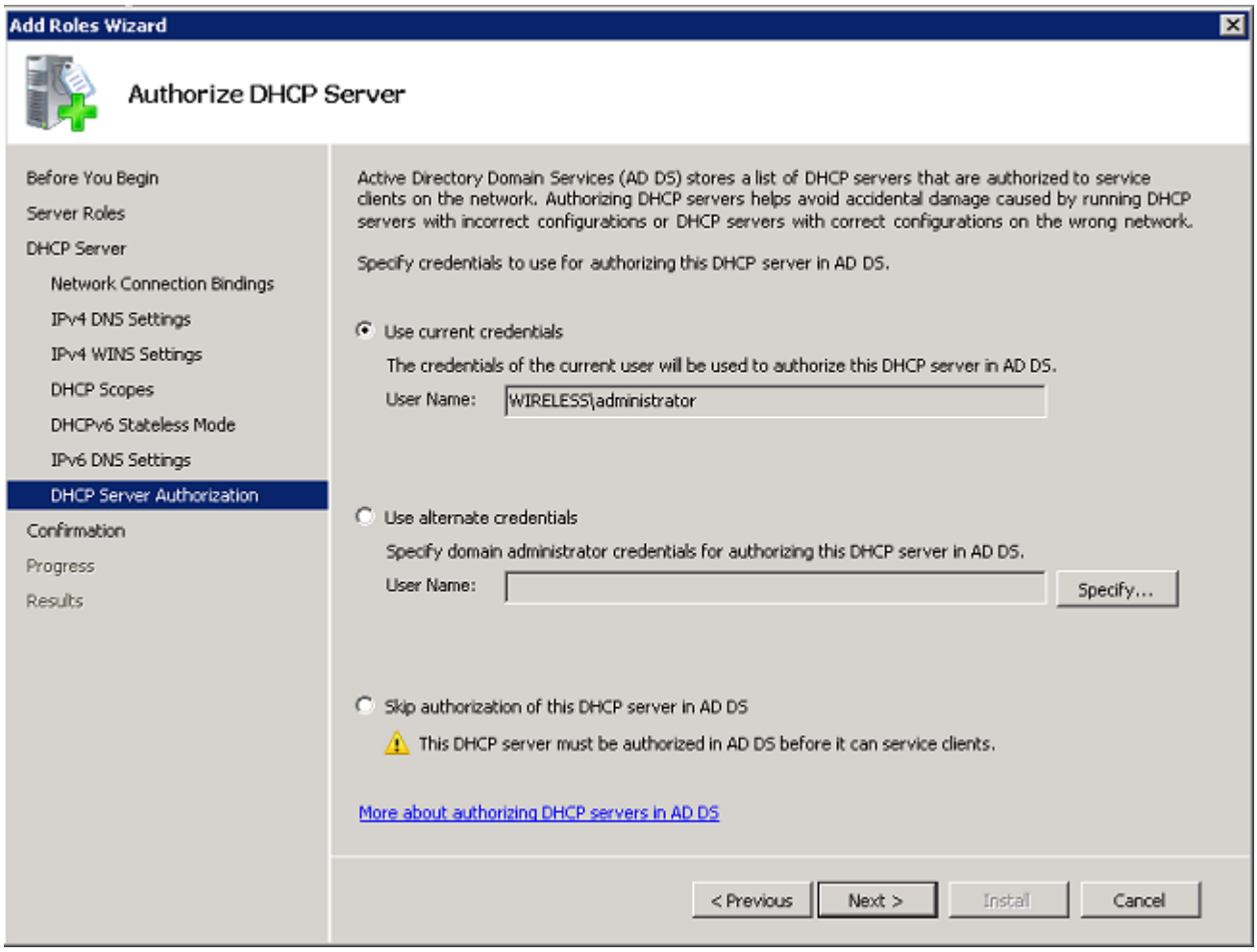
10. 在伺服器上啟用或禁用DHCPv6支援，然後按一下下一步。



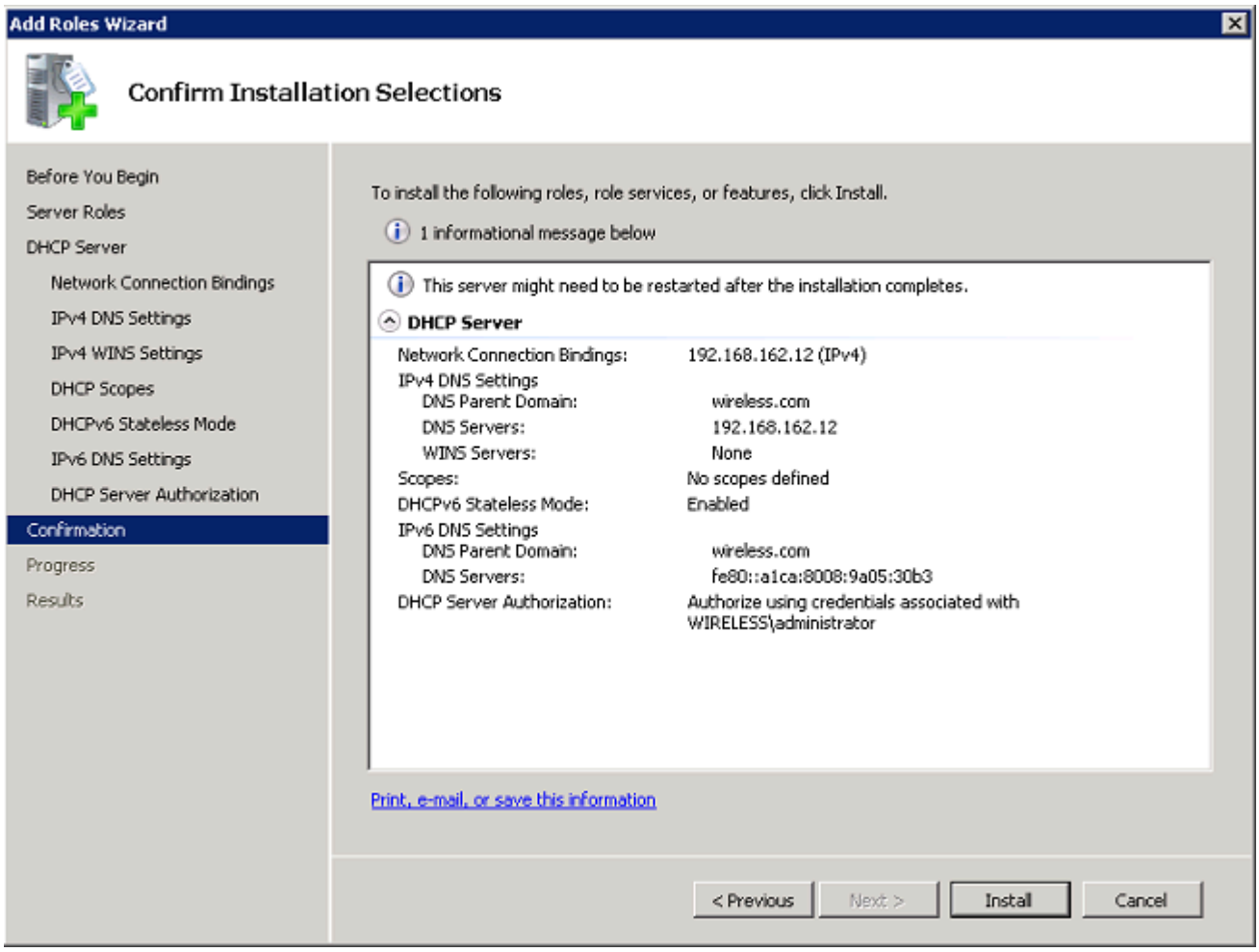
11. 如果上一步啟用了DHCPv6，則配置IPv6 DNS設定。按一下下一步繼續。



12. 提供域管理員憑據以授權Active Directory中的DHCP伺服器，然後按一下下一步。

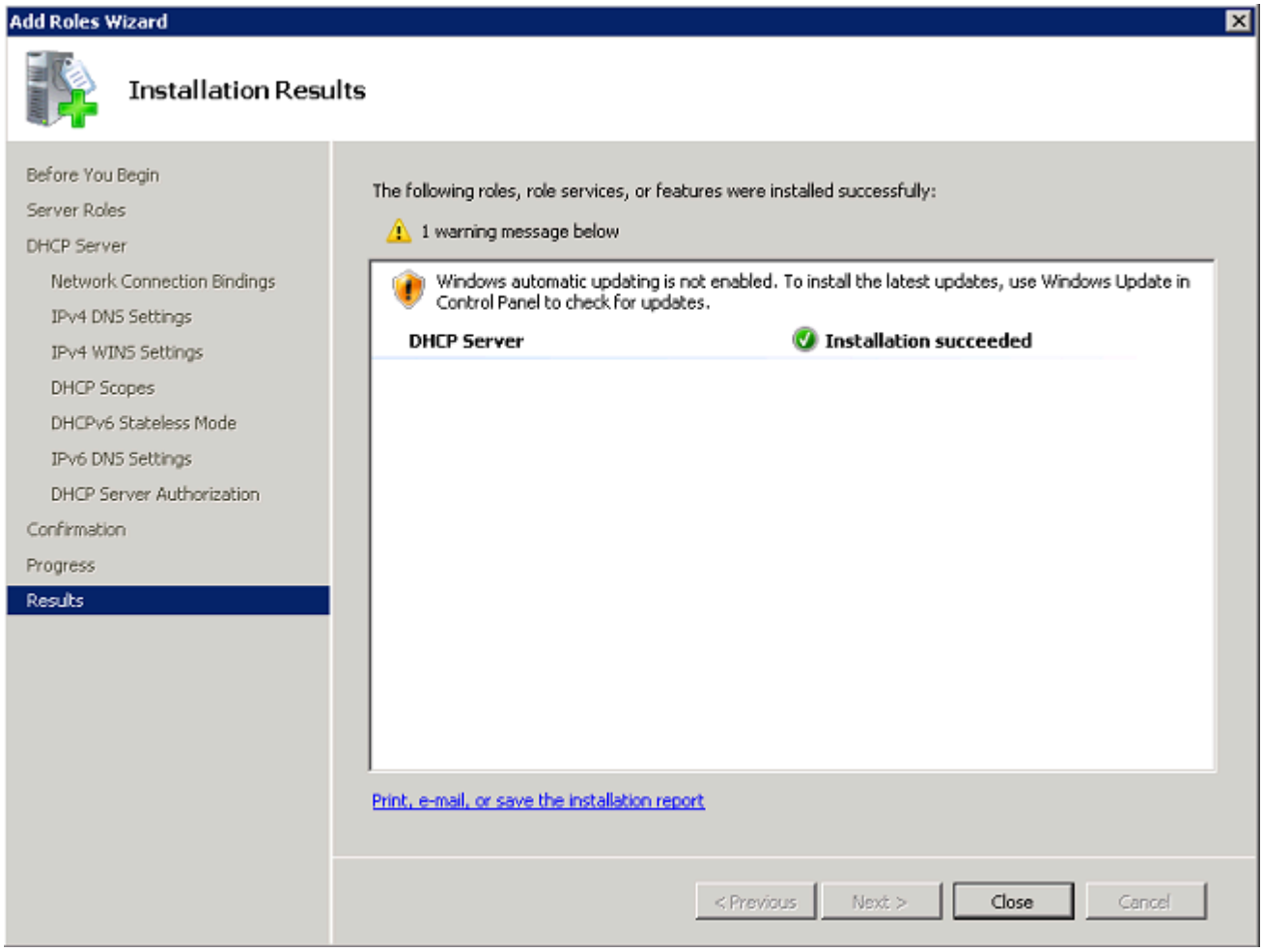


13. 檢視確認頁上的配置，然後按一下安裝以完成安裝。



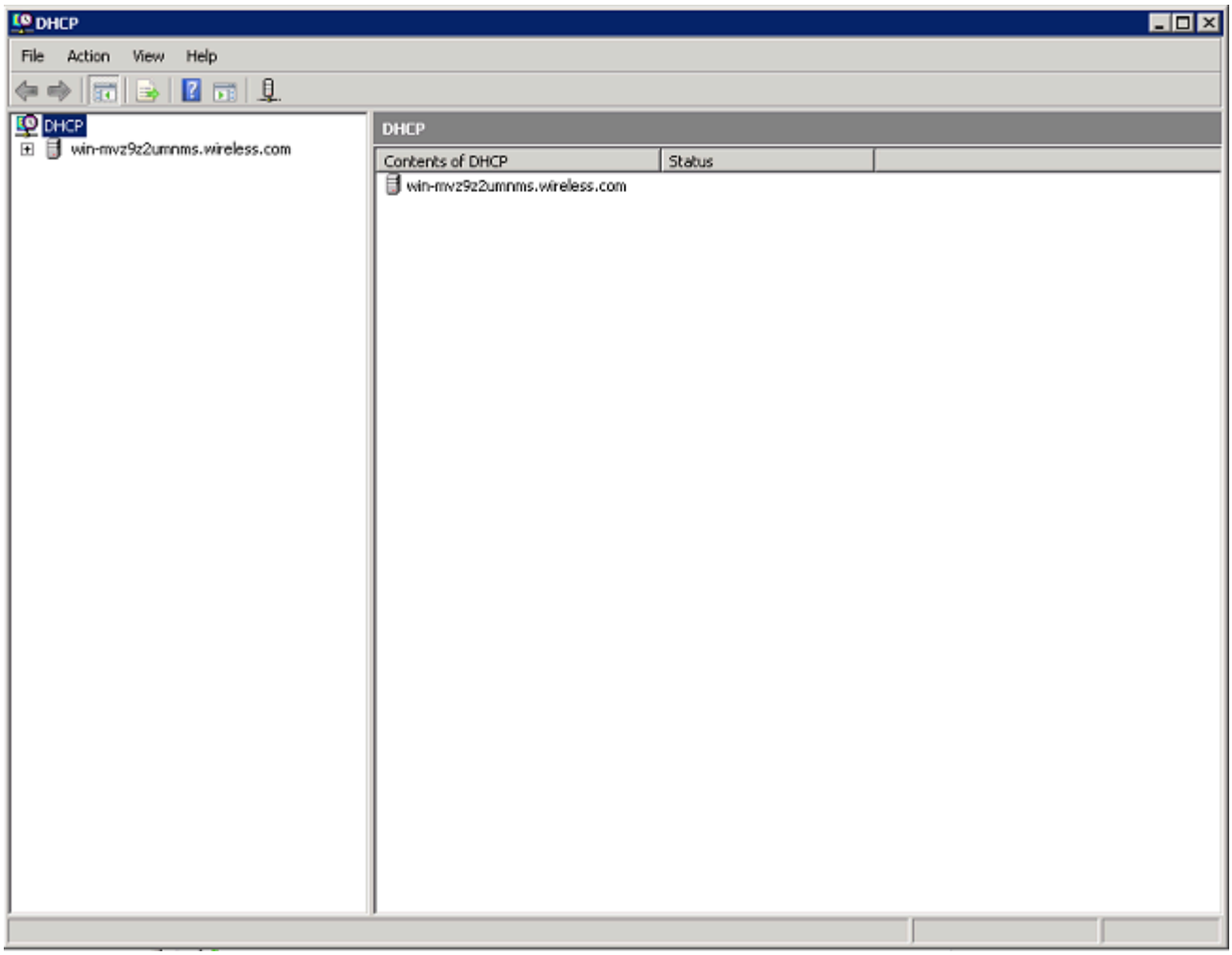
安裝繼續進行。

14. 按一下Close關閉嚮導。

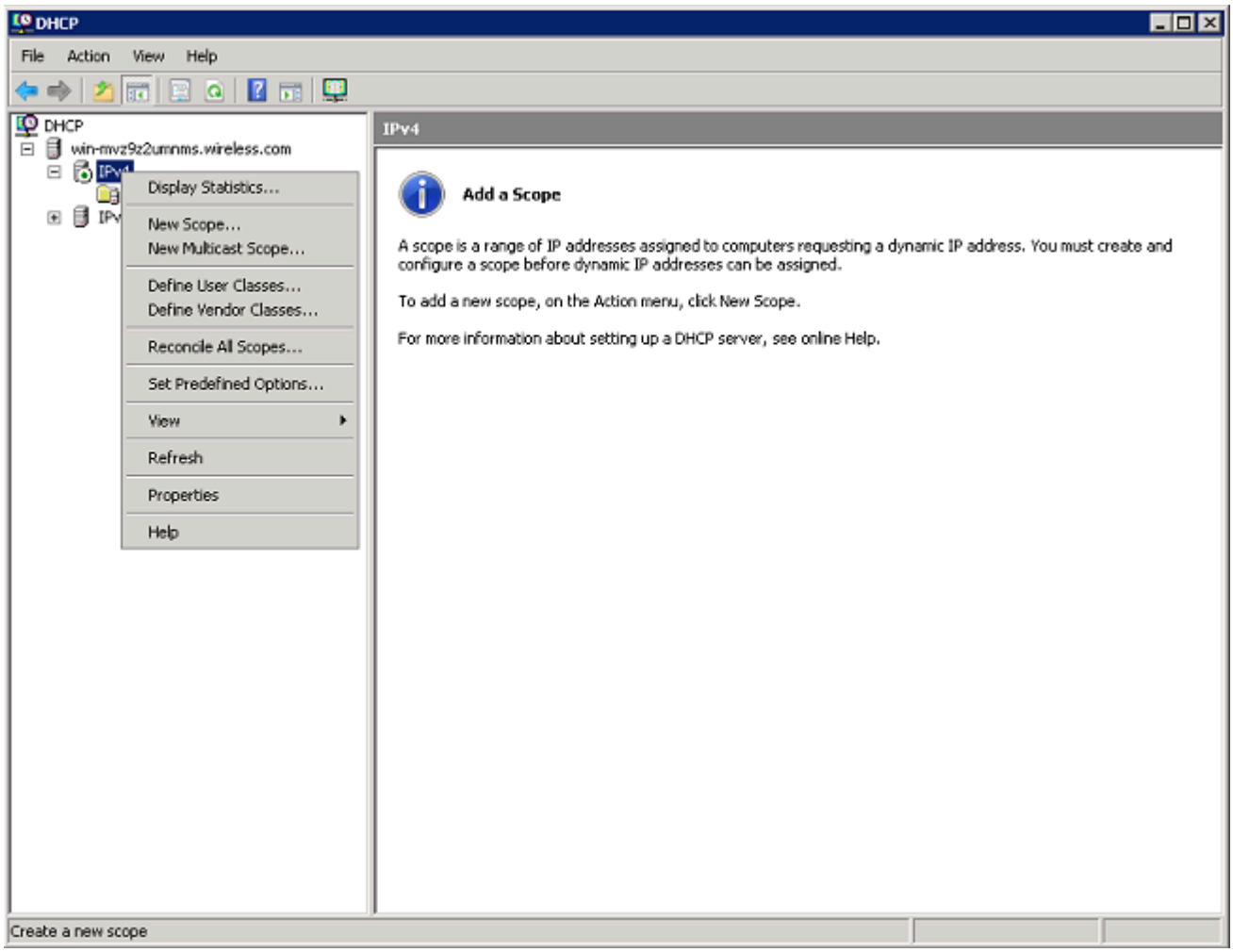


現在已安裝DHCP伺服器。

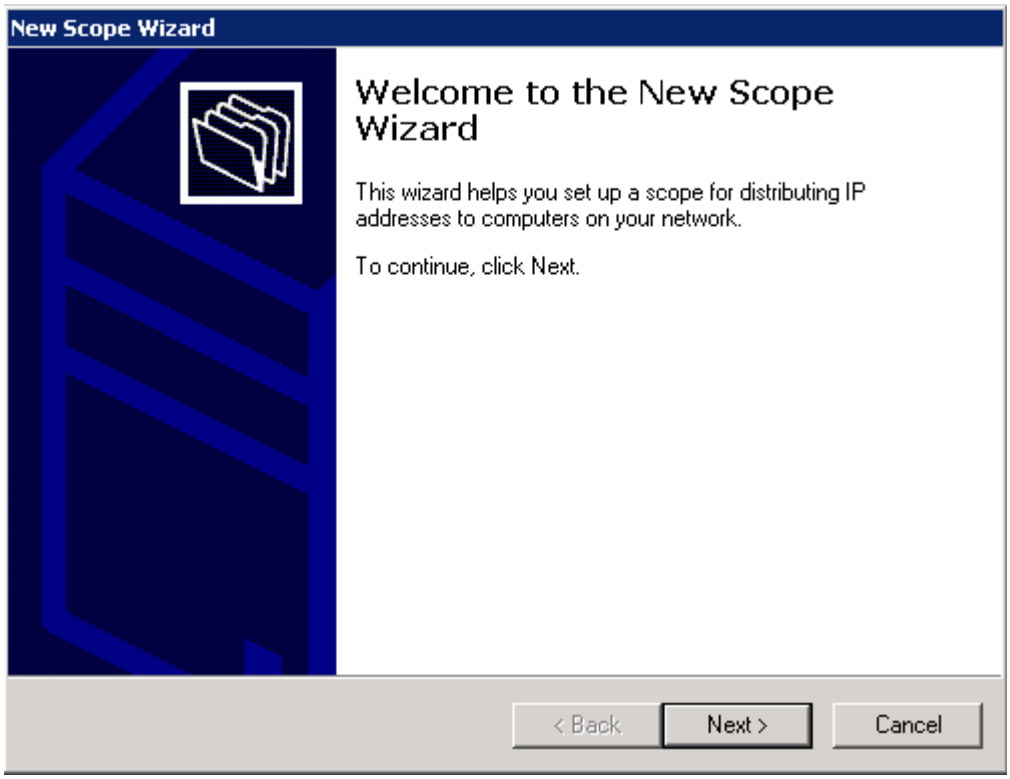
15. 按一下開始>管理工具 >DHCP以配置DHCP服務。



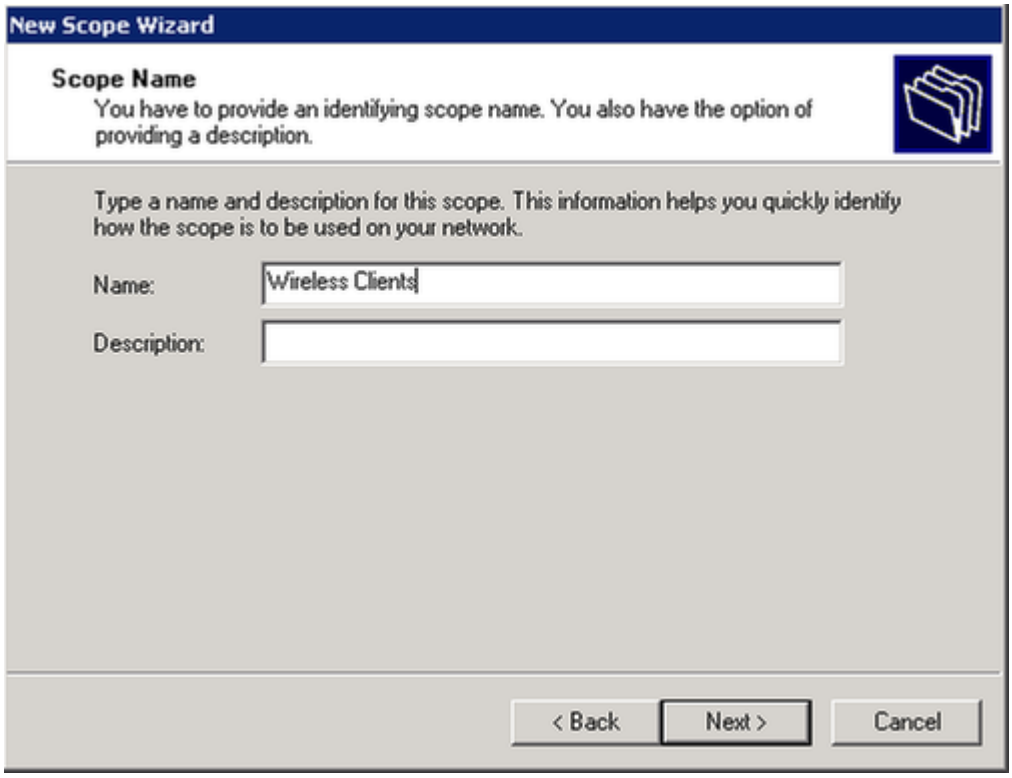
16. 展開DHCP伺服器（如本示例的上一映像所示），按一下右鍵IPv4，然後選擇New Scope以建立DHCP範圍。



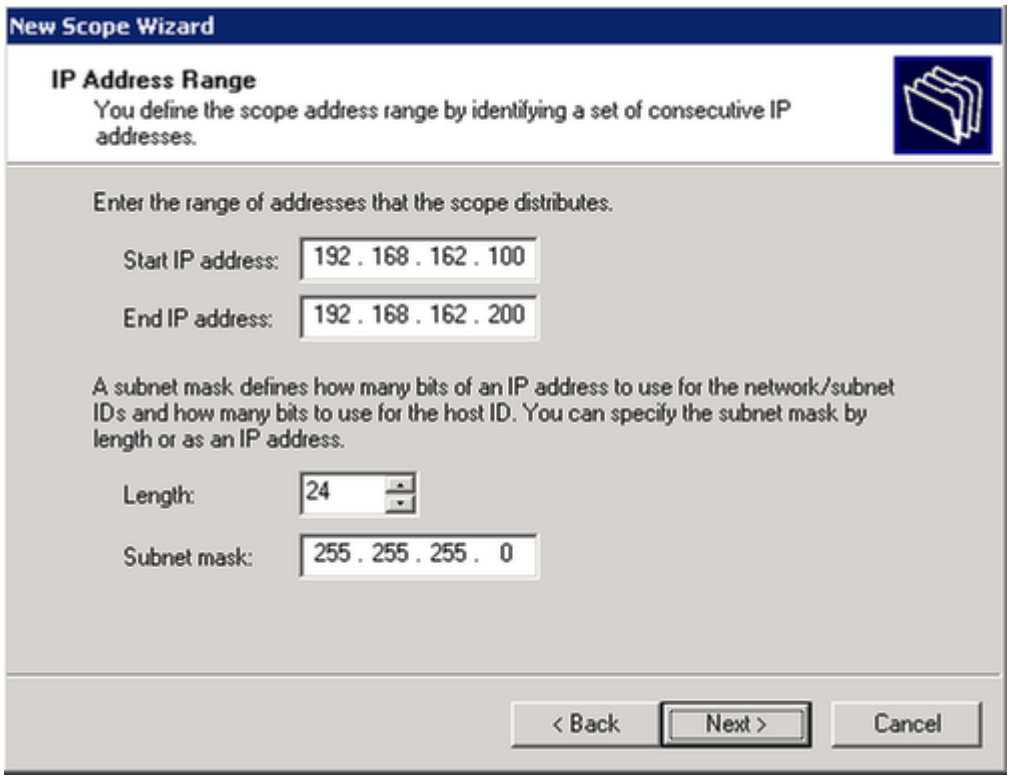
17. 按一下下一步，通過「新建範圍嚮導」配置新範圍。



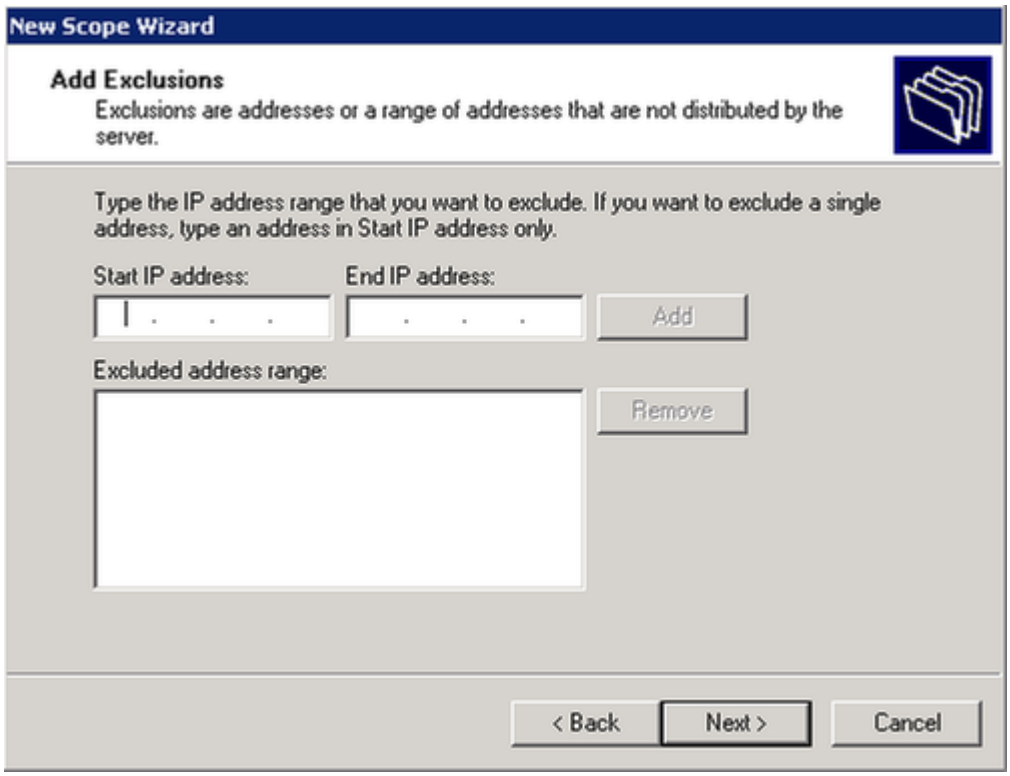
18. 為新作用域提供名稱（在本示例中為Wireless Clients），然後按一下Next。



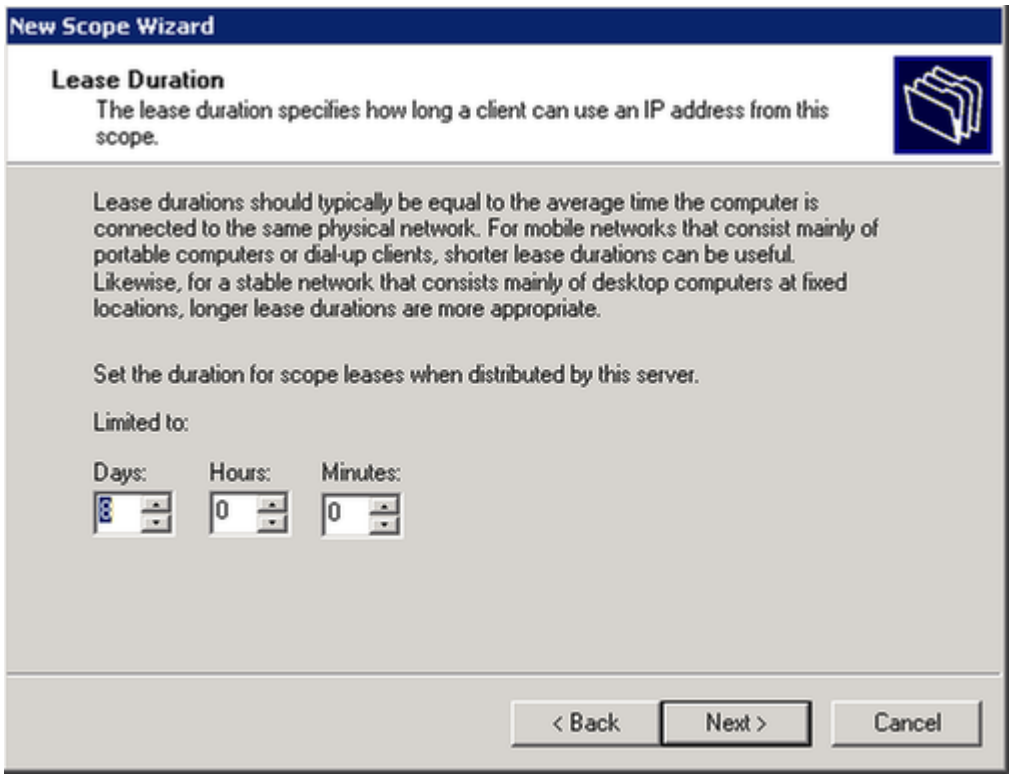
19. 輸入可用於DHCP租用的IP地址範圍。按一下下一步繼續。



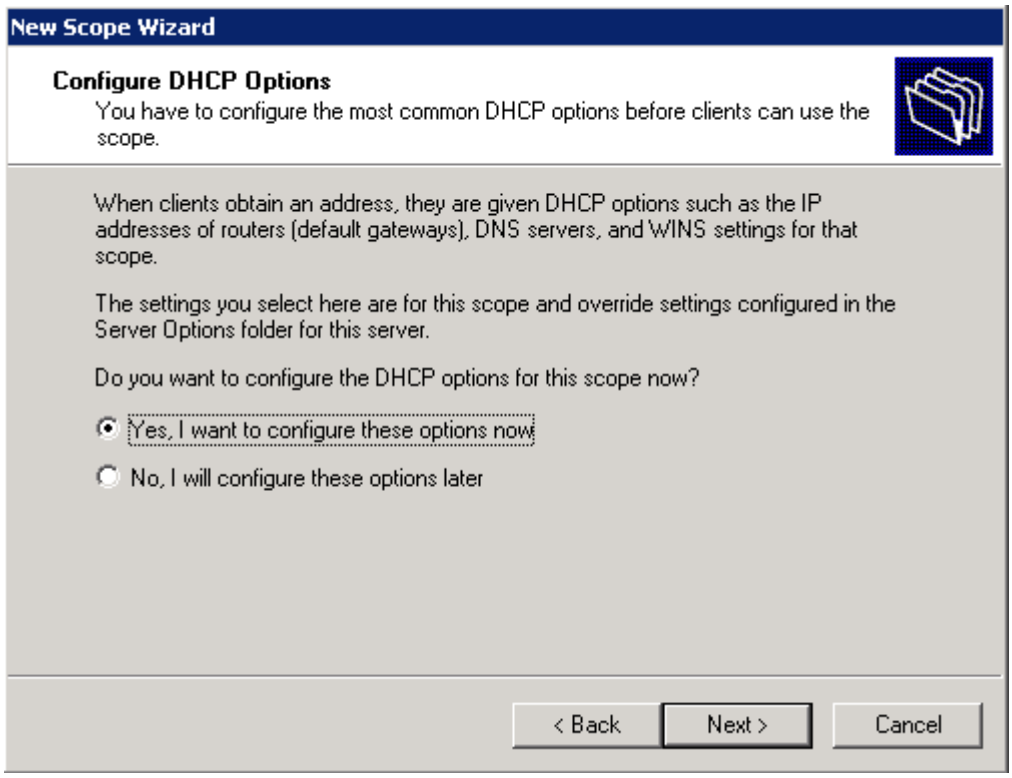
20. 建立排除地址的可選清單。按一下下一步繼續。



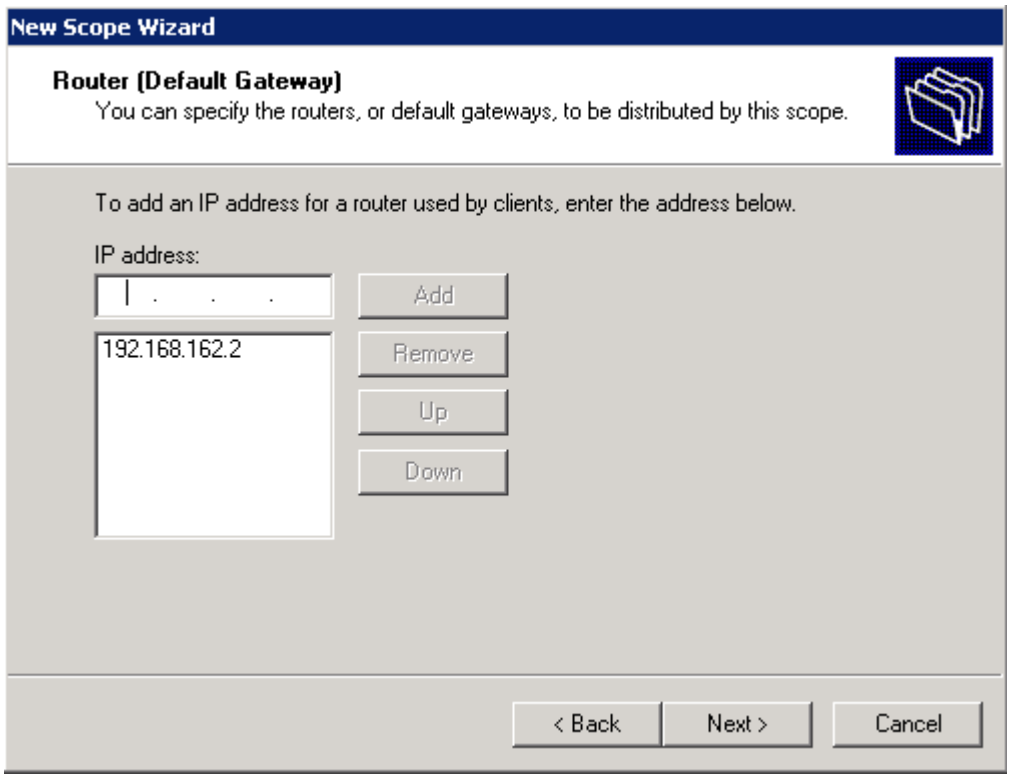
21. 配置租用時間，然後按一下下一步。



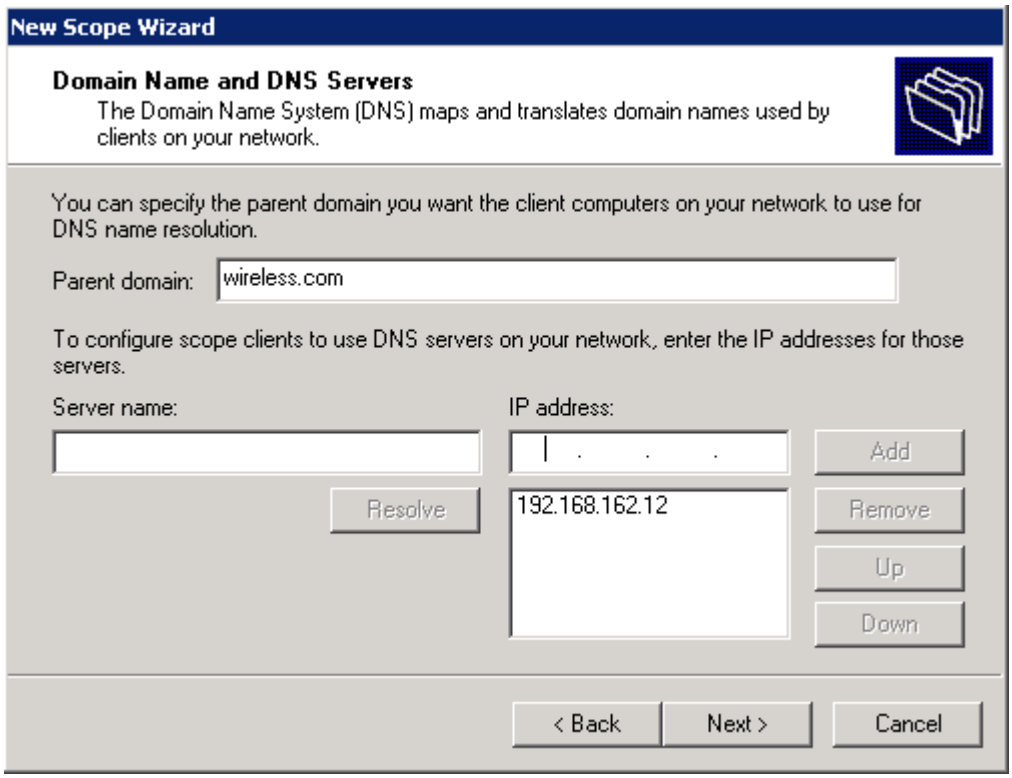
22. 按一下Yes， I want to configure these options now，然後按一下Next。



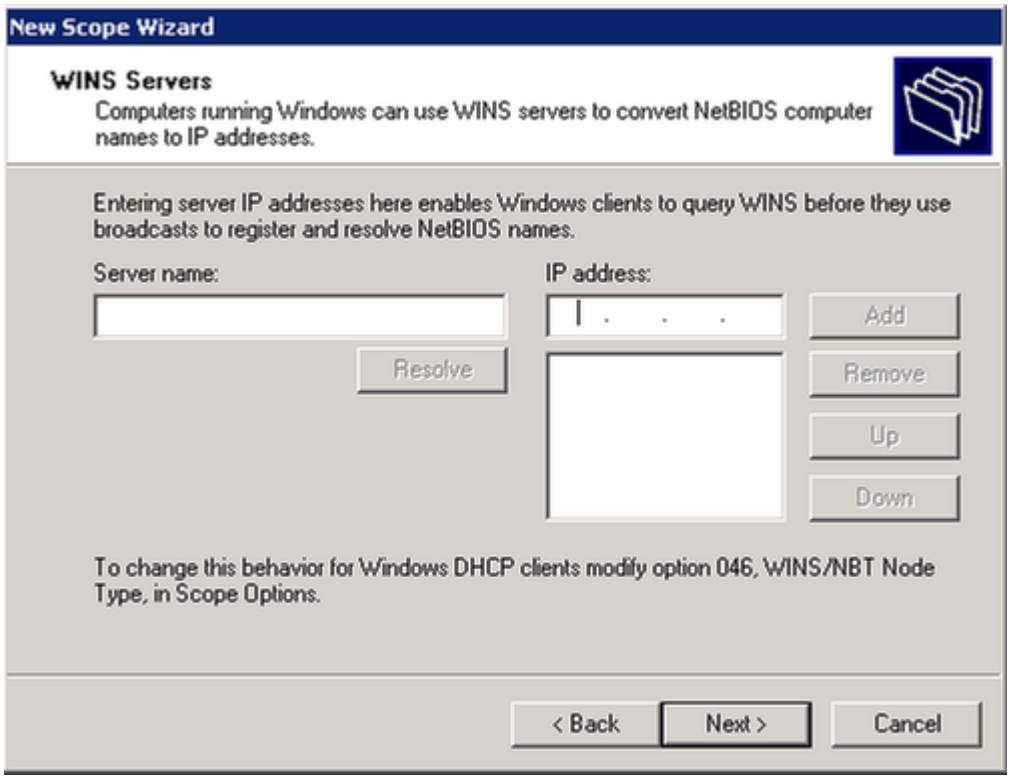
23. 輸入此作用域的預設網關的IP地址，按一下Add > Next。



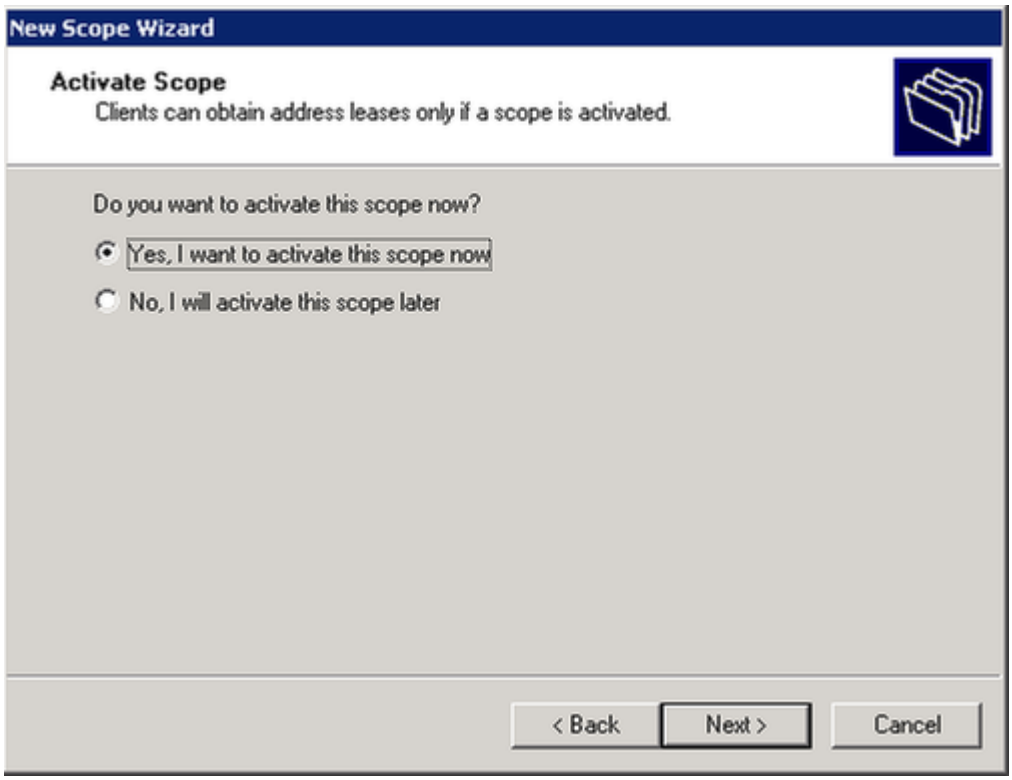
24. 配置客戶端要使用的DNS域名和DNS伺服器。按一下下一步繼續。



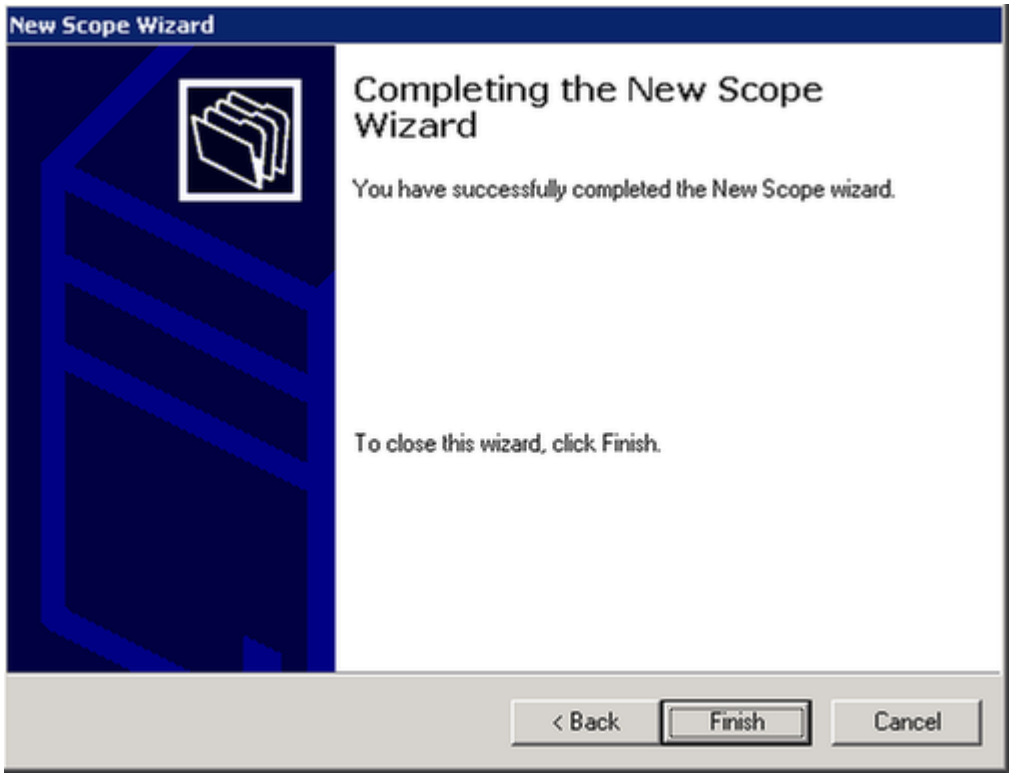
25. 如果網路支援WINS，請輸入此作用域的WINS資訊。按一下下一步繼續。



26. 要啟用此作用域，請單擊Yes， I want to activate this scope now> Next。



27. 按一下完成完成並關閉嚮導。



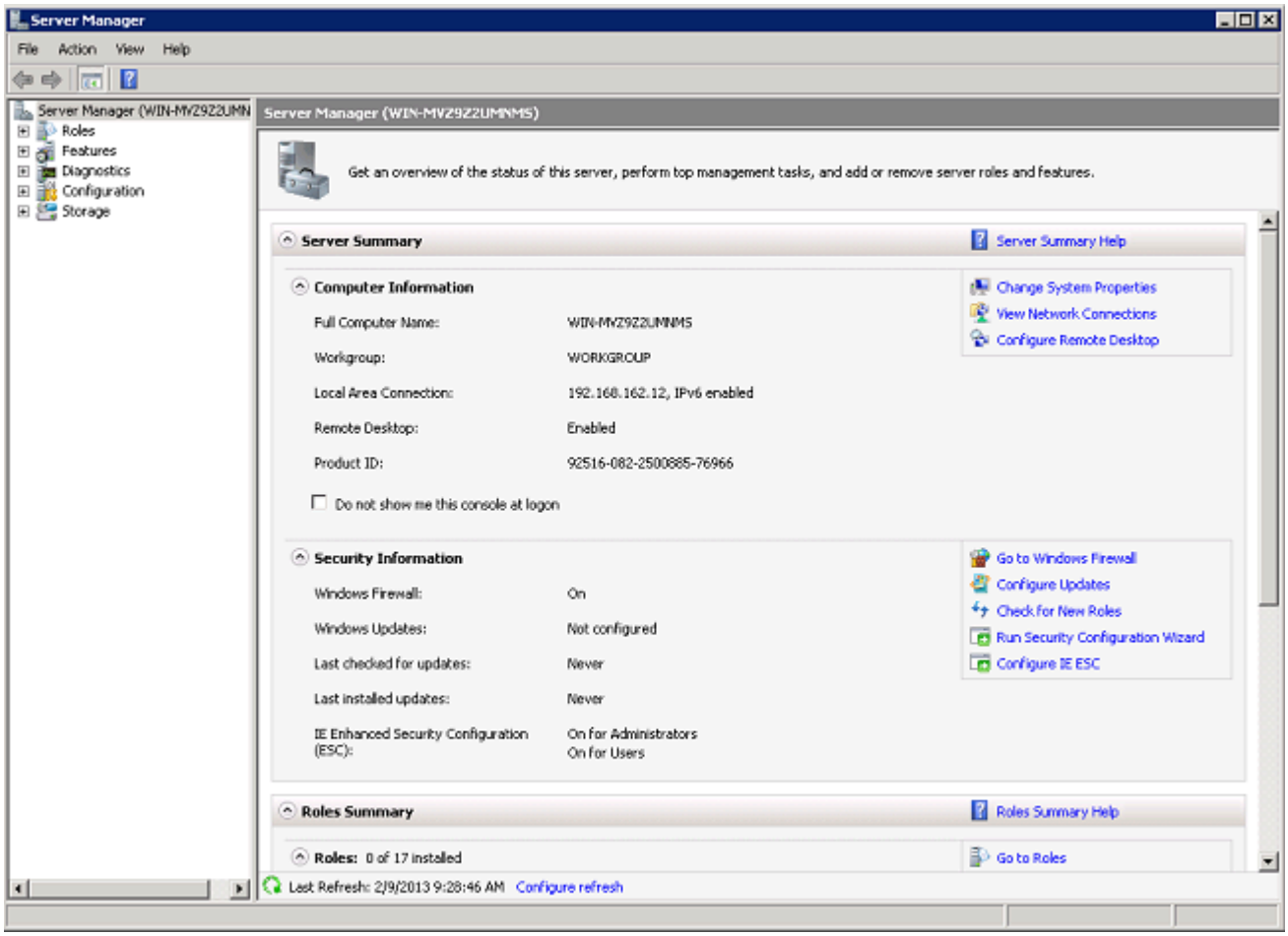
安裝Microsoft Windows 2008 Server並將其配置為CA伺服器

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，伺服器證書必須由受客戶端電腦信任的公共CA頒發（即，公共CA證書已存在於客戶端電腦證書儲存上的受信

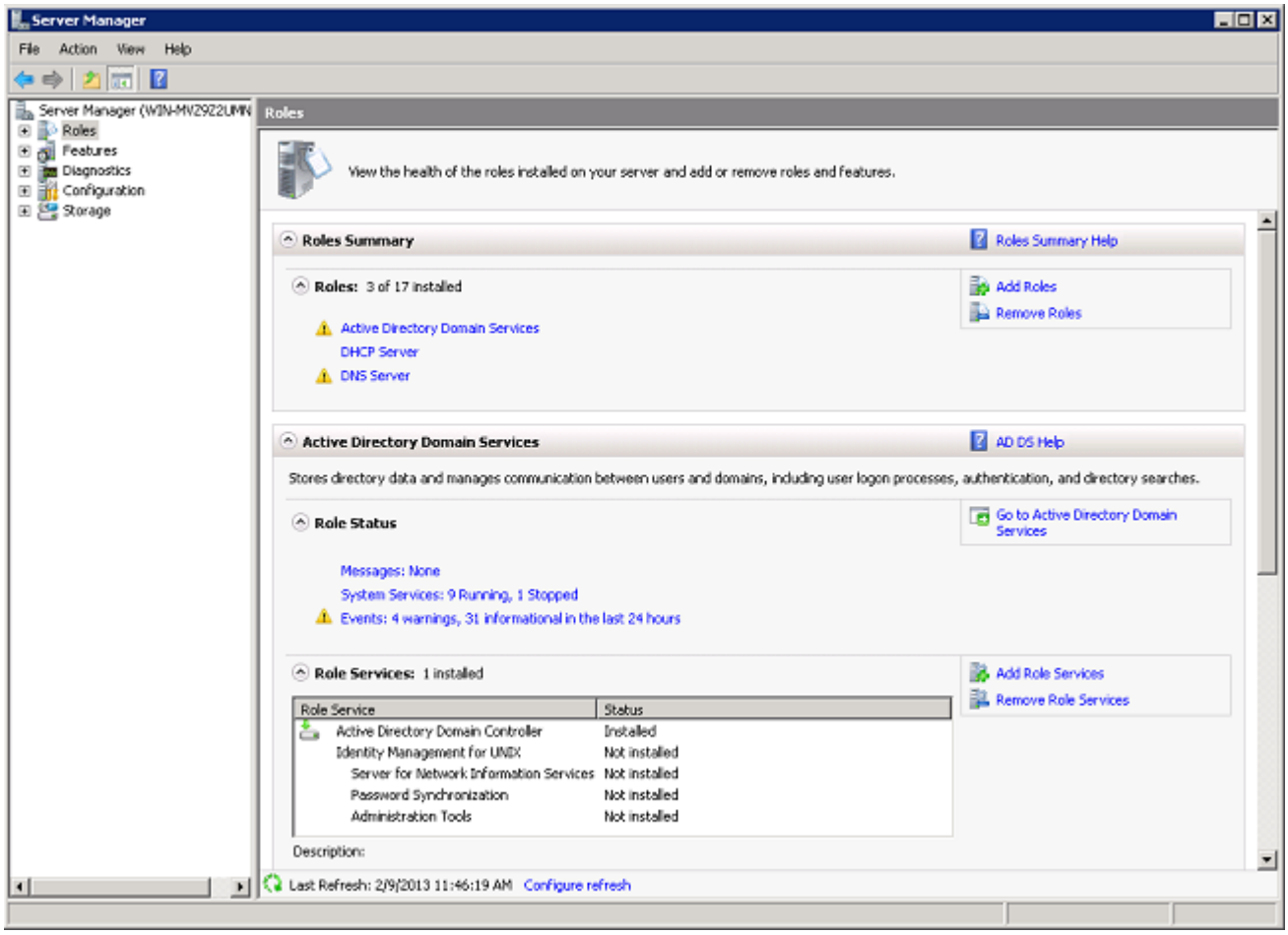
任的根證書頒發機構資料夾中）。

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

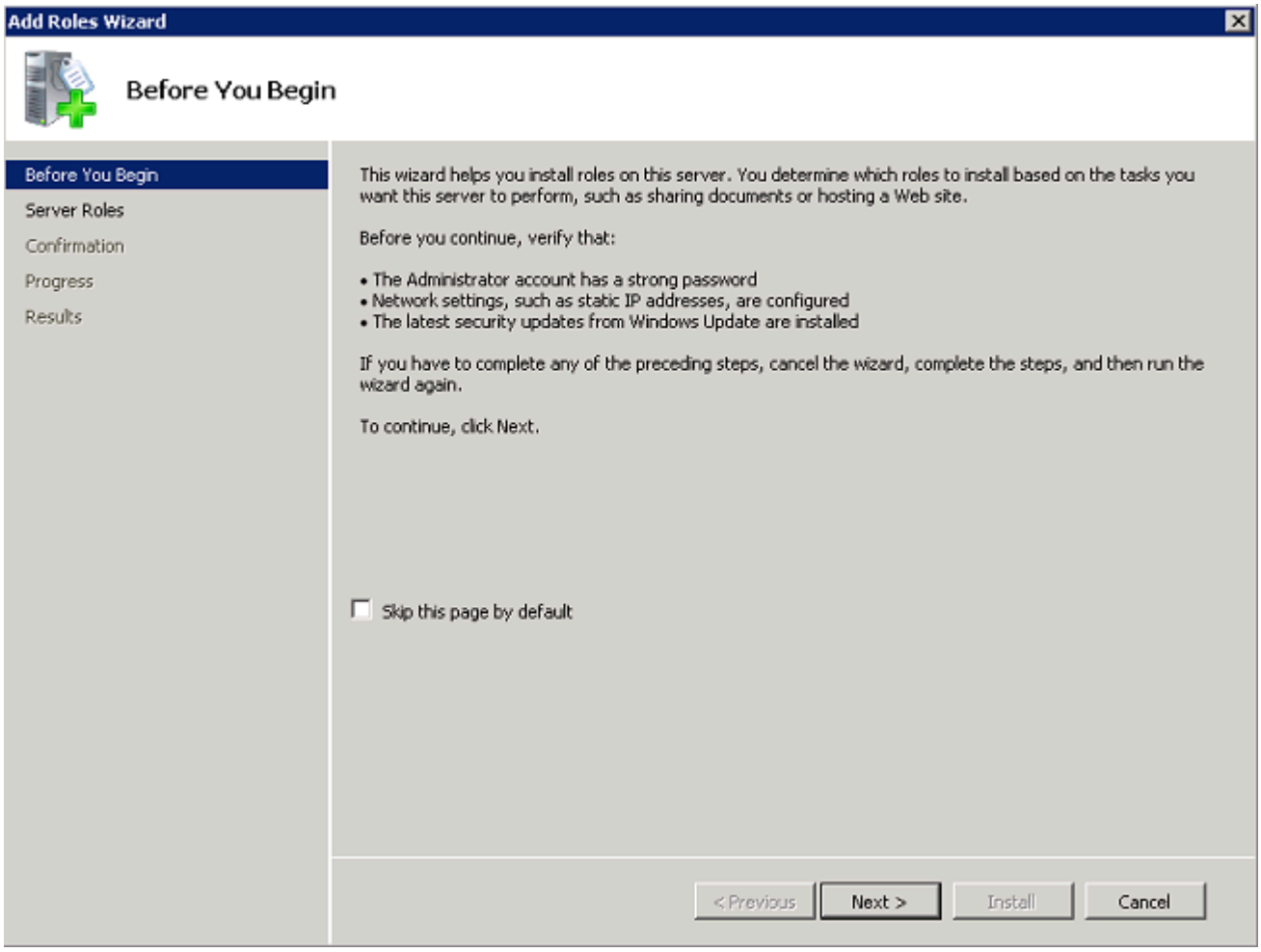
1. 按一下Start> Server Manager。



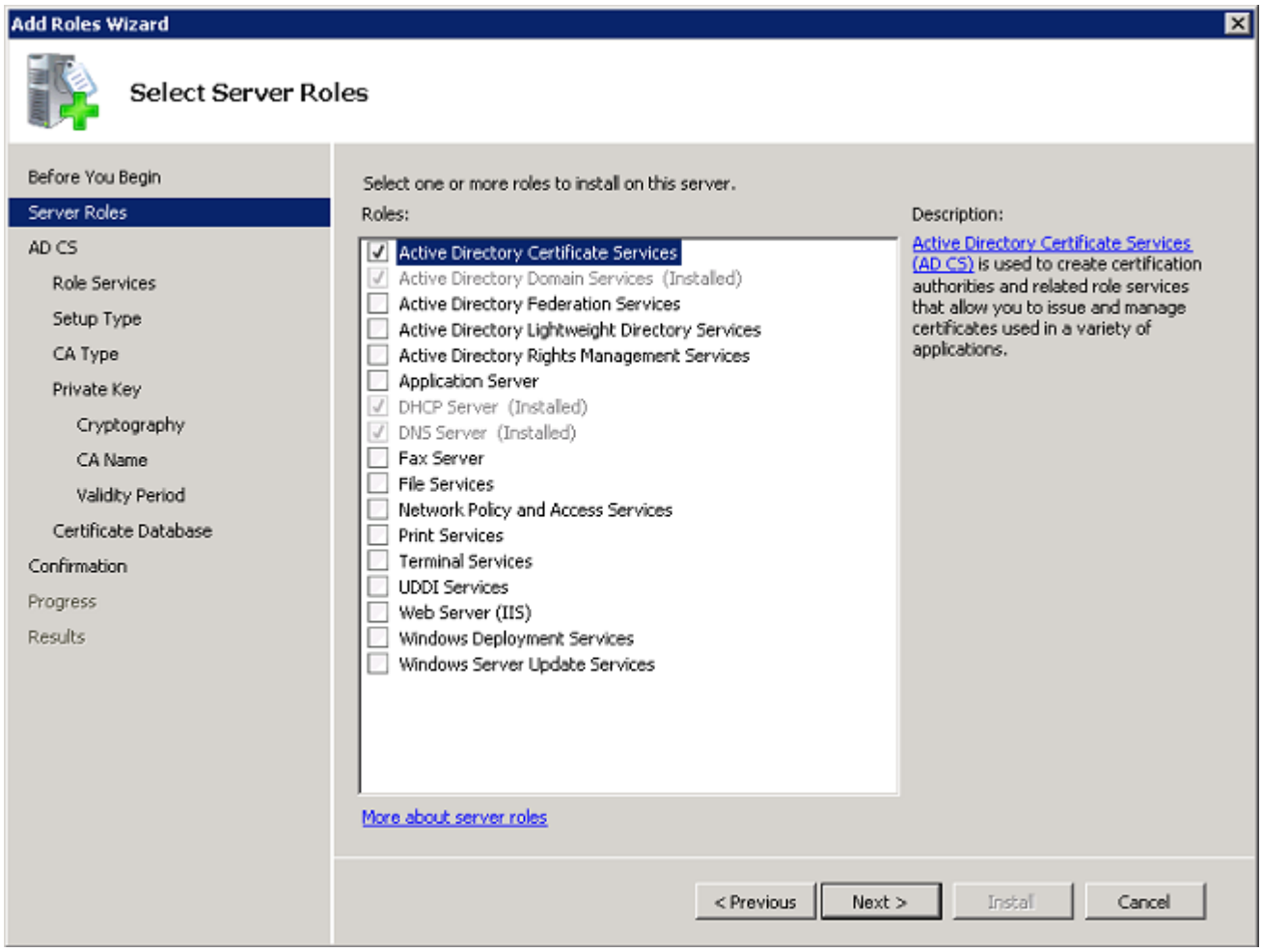
2. 按一下Roles> Add Roles。


Server Manager
File Action View Help
Server Manager (WIN-MV292...
Roles
Features
Diagnostics
Configuration
Storage
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

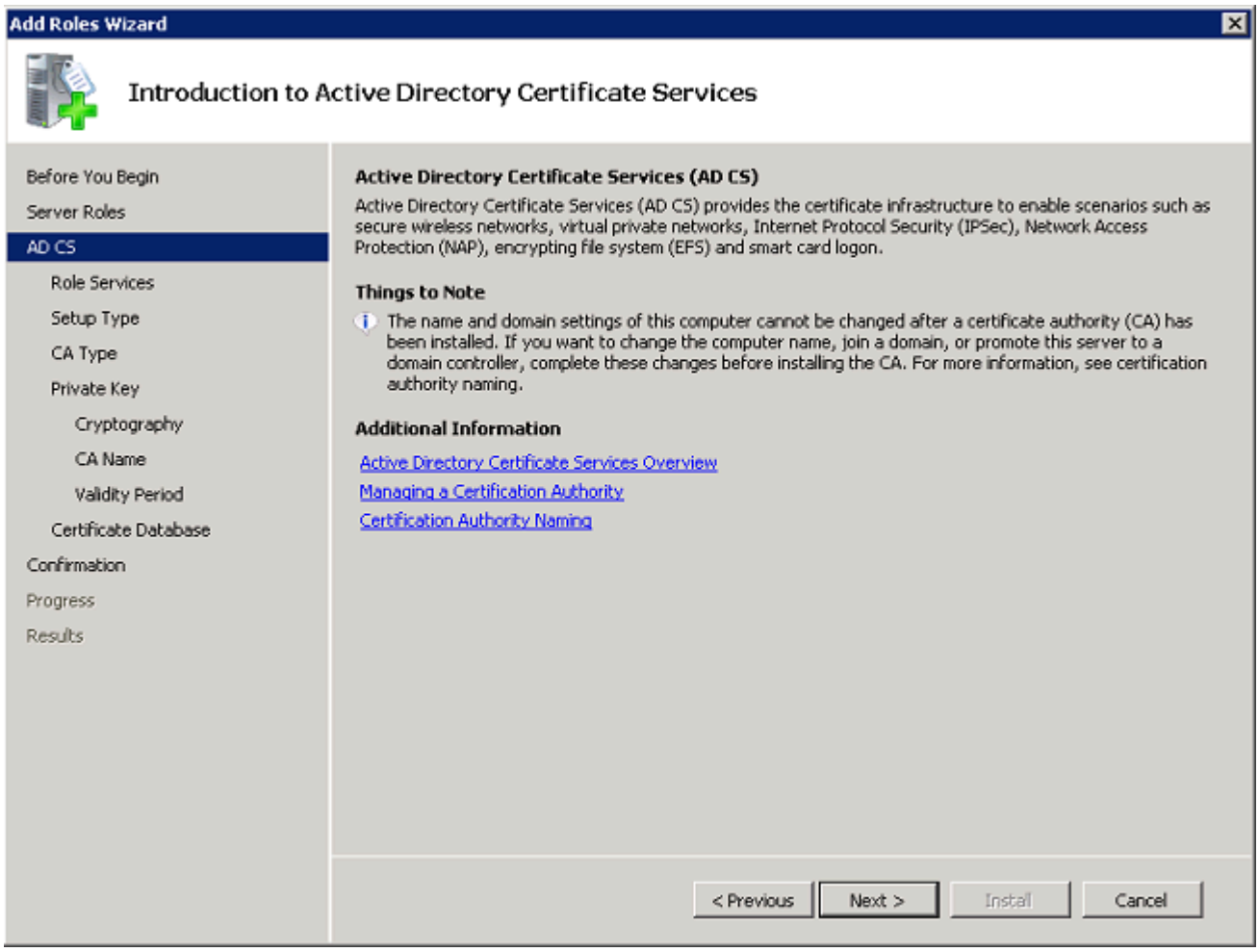
3. 按「Next」（下一步）。



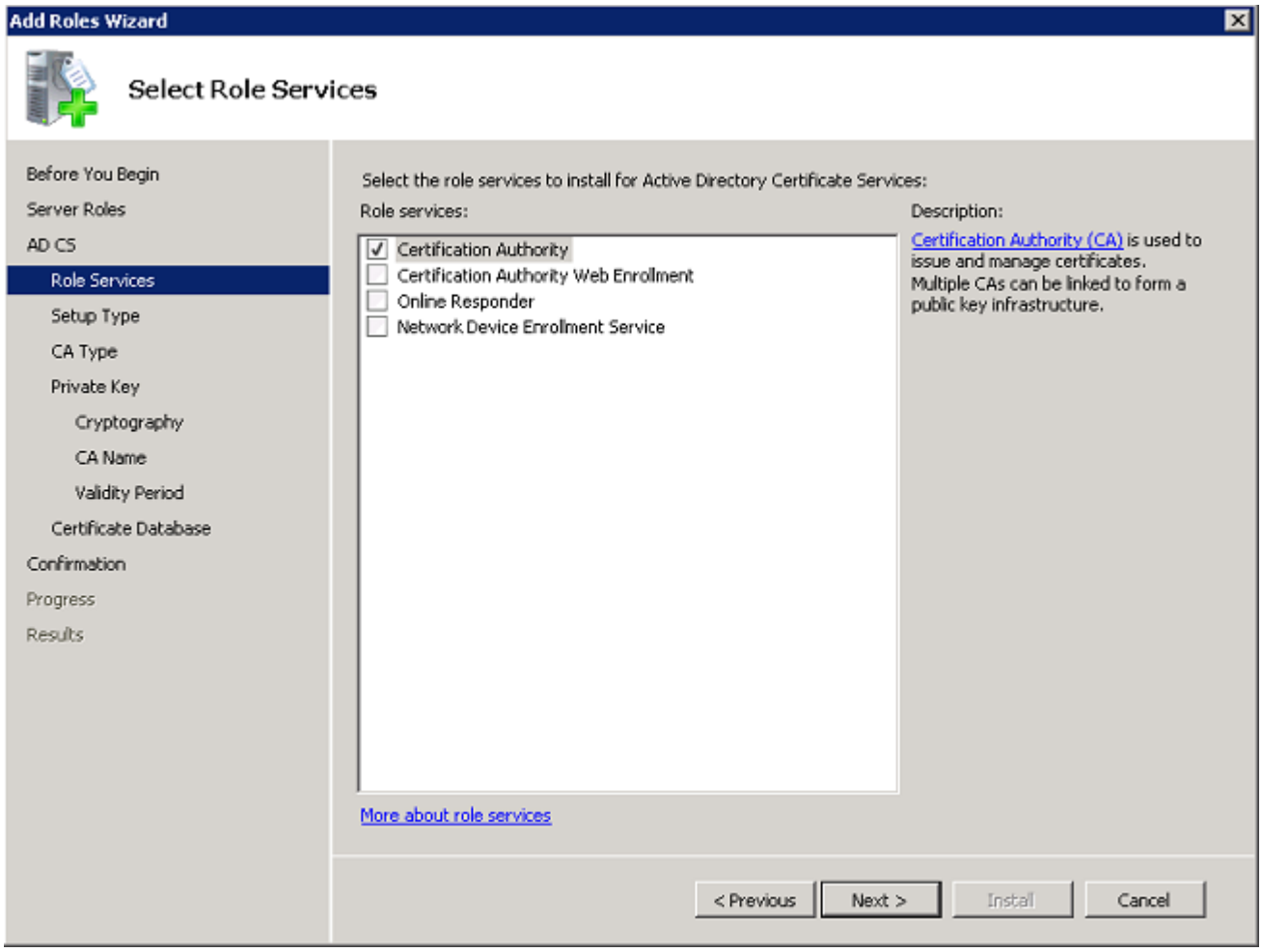
4. 選擇服務Active Directory證書服務，然後按一下下一步。



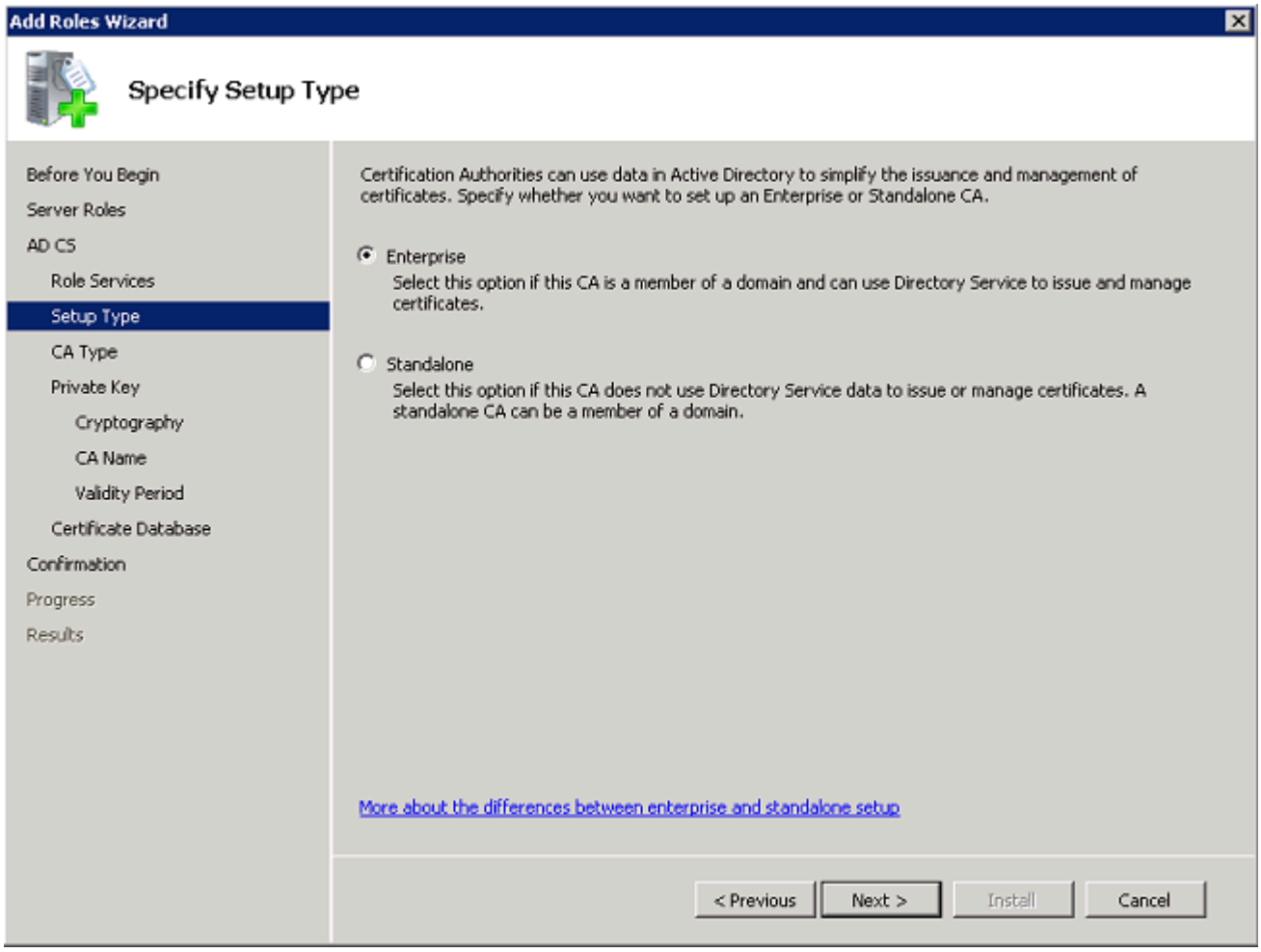
5. 檢視Active Directory證書服務簡介，然後按一下下一步。



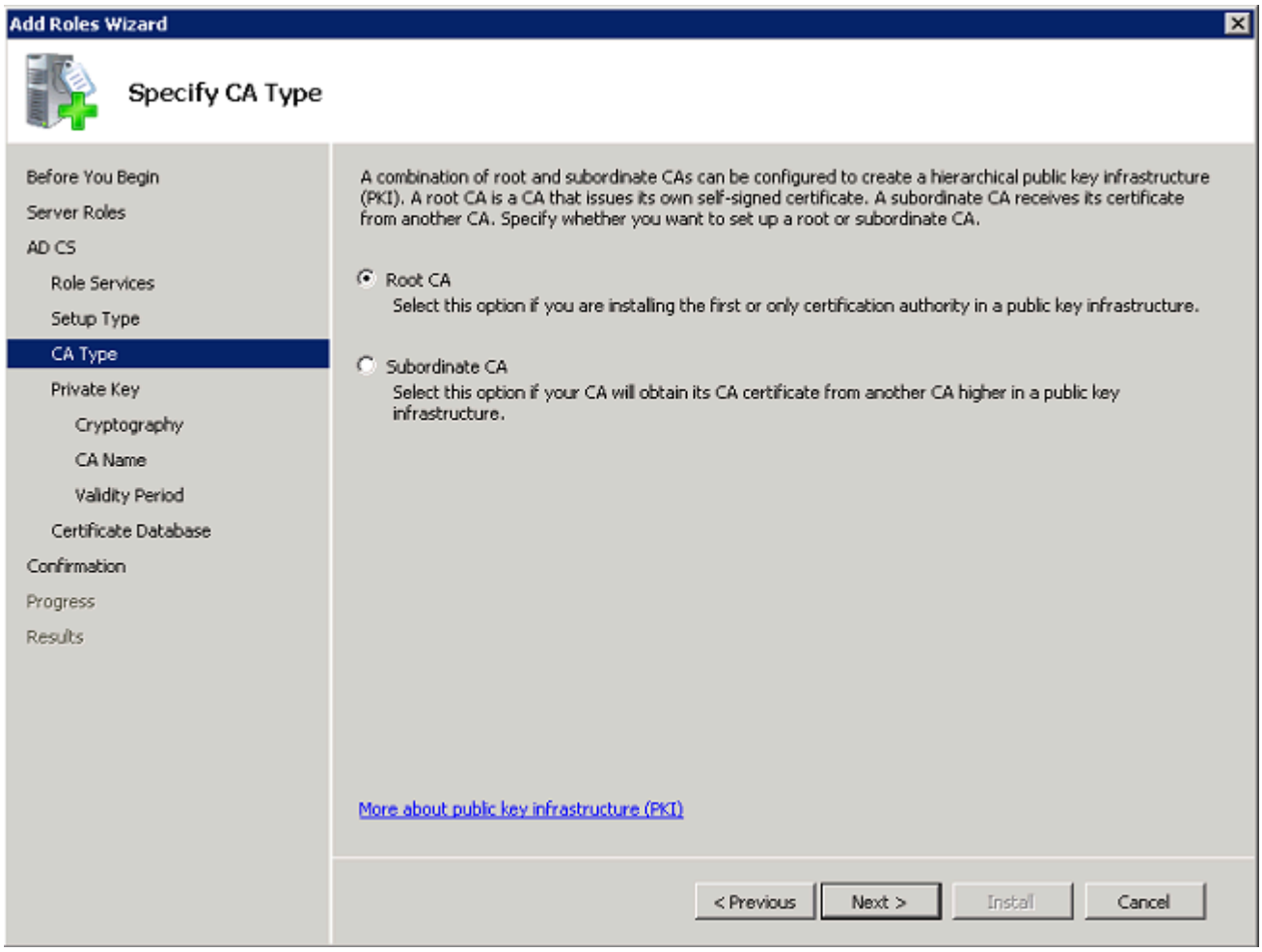
6. 選擇Certificate Authority，然後按一下Next。



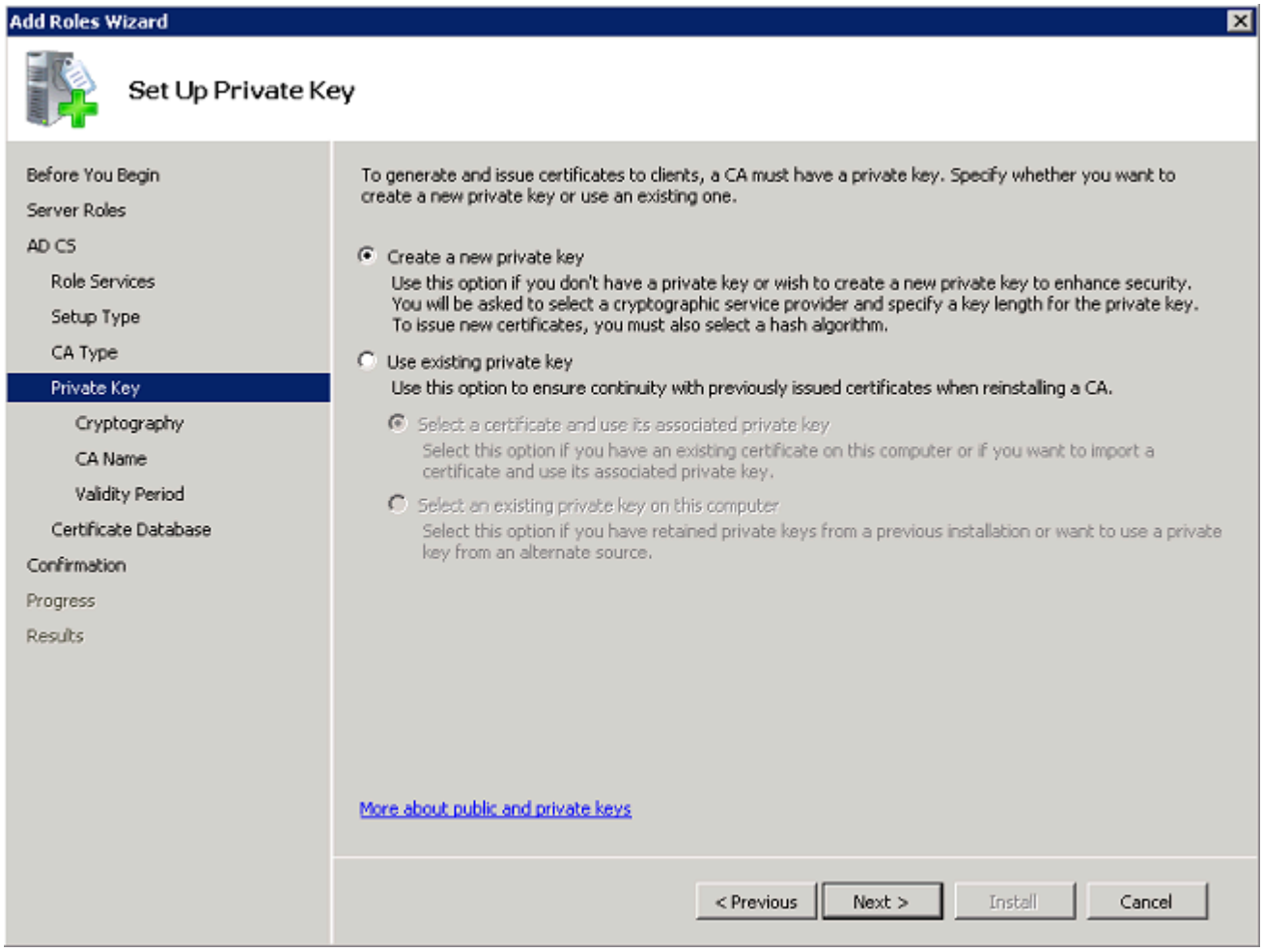
7. 選擇Enterprise，然後按一下Next。



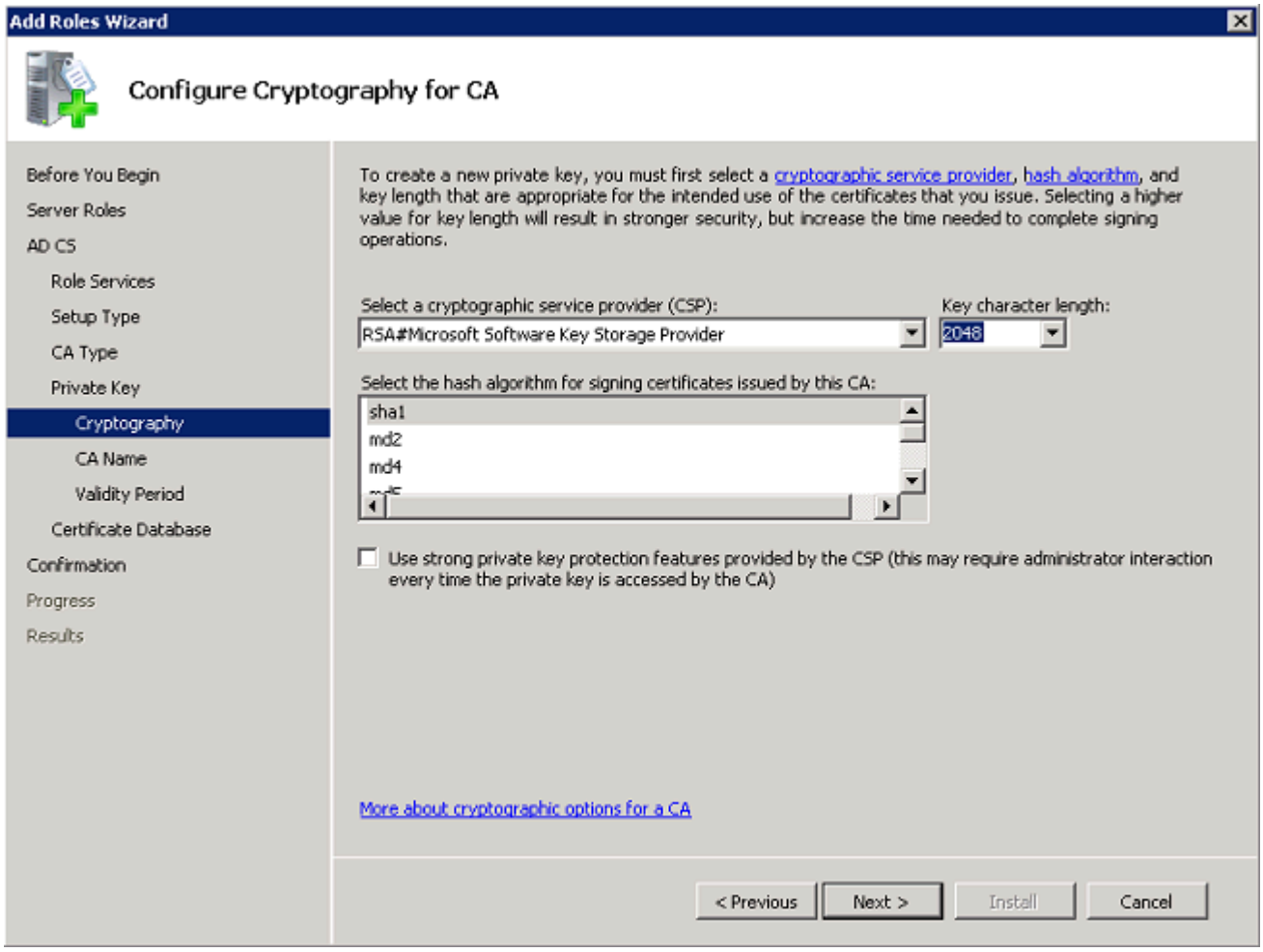
8. 選擇根CA，然後按一下下一步。



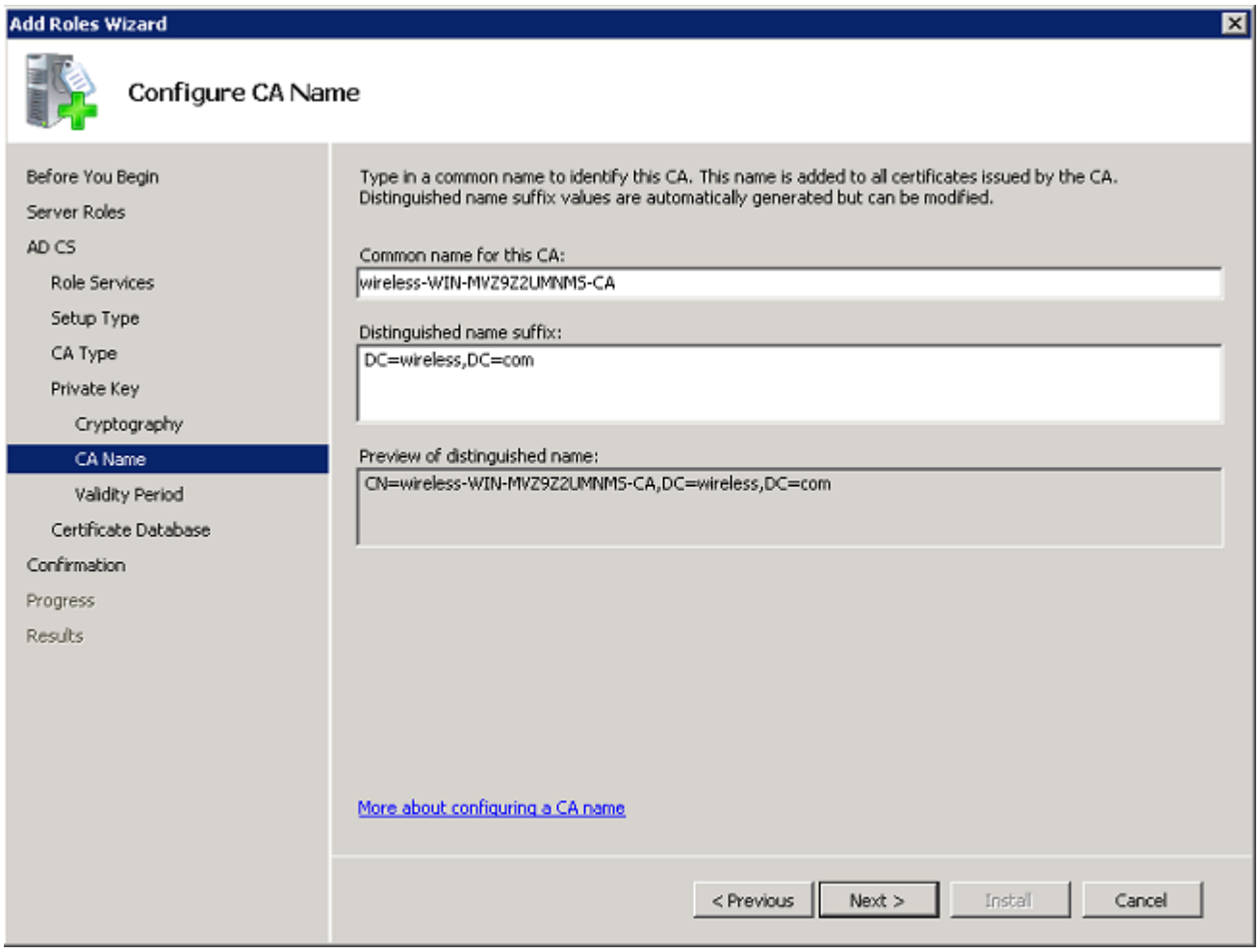
9. 選擇Create a new private key，然後按一下Next。



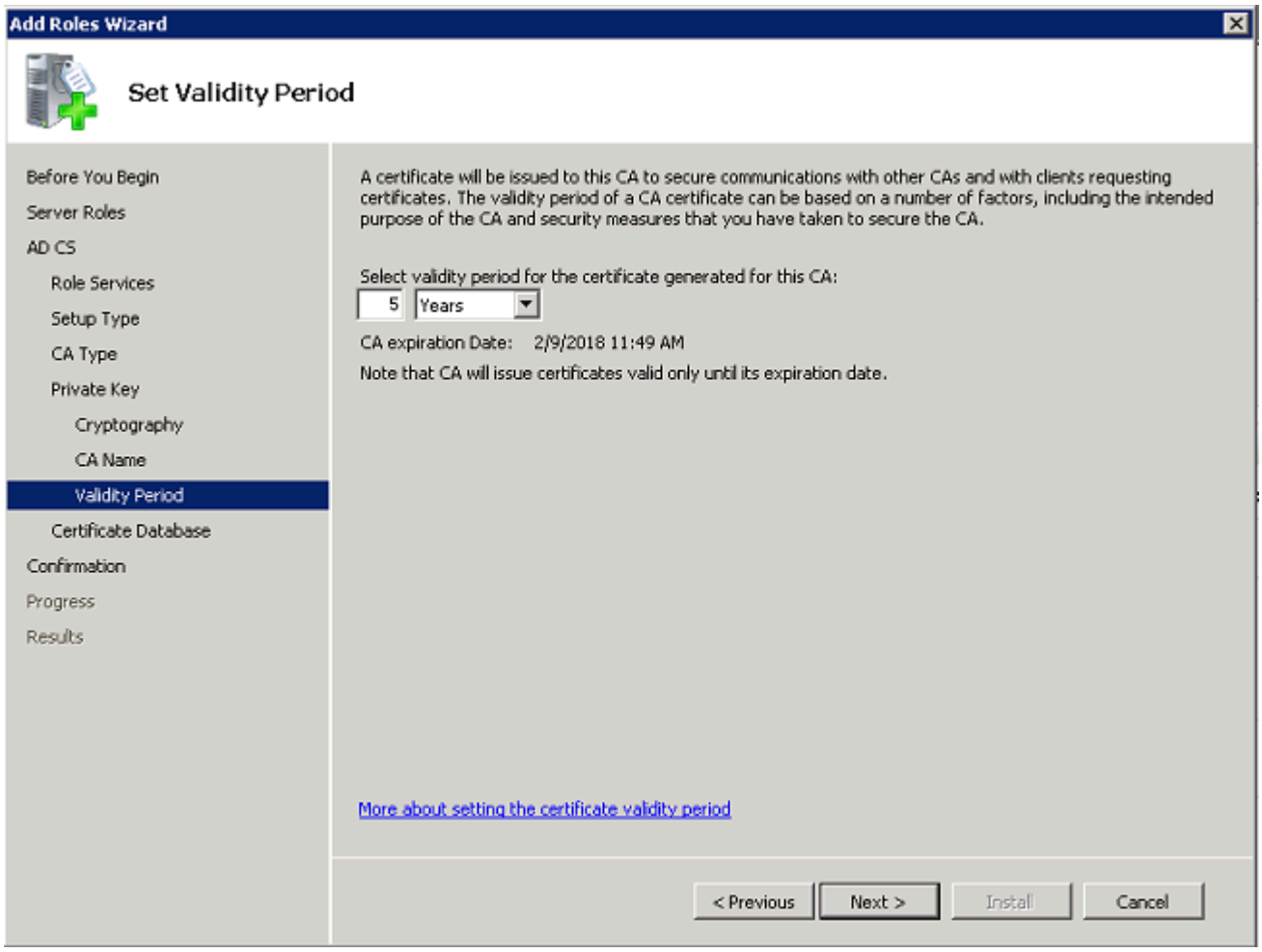
10. 在Configure Cryptography for CA上按一下Next。



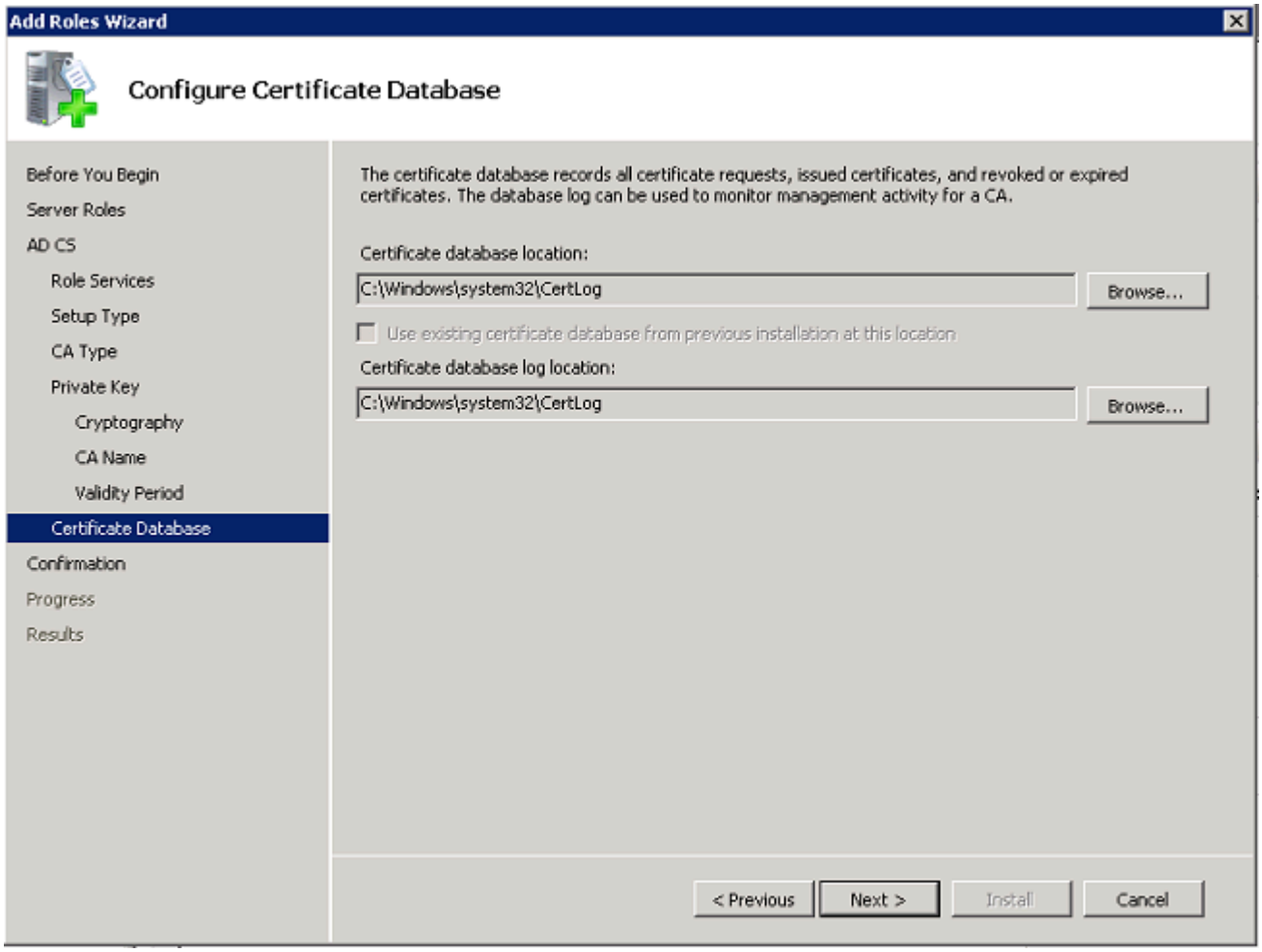
11. 按一下下一步接受此CA的預設公用名。



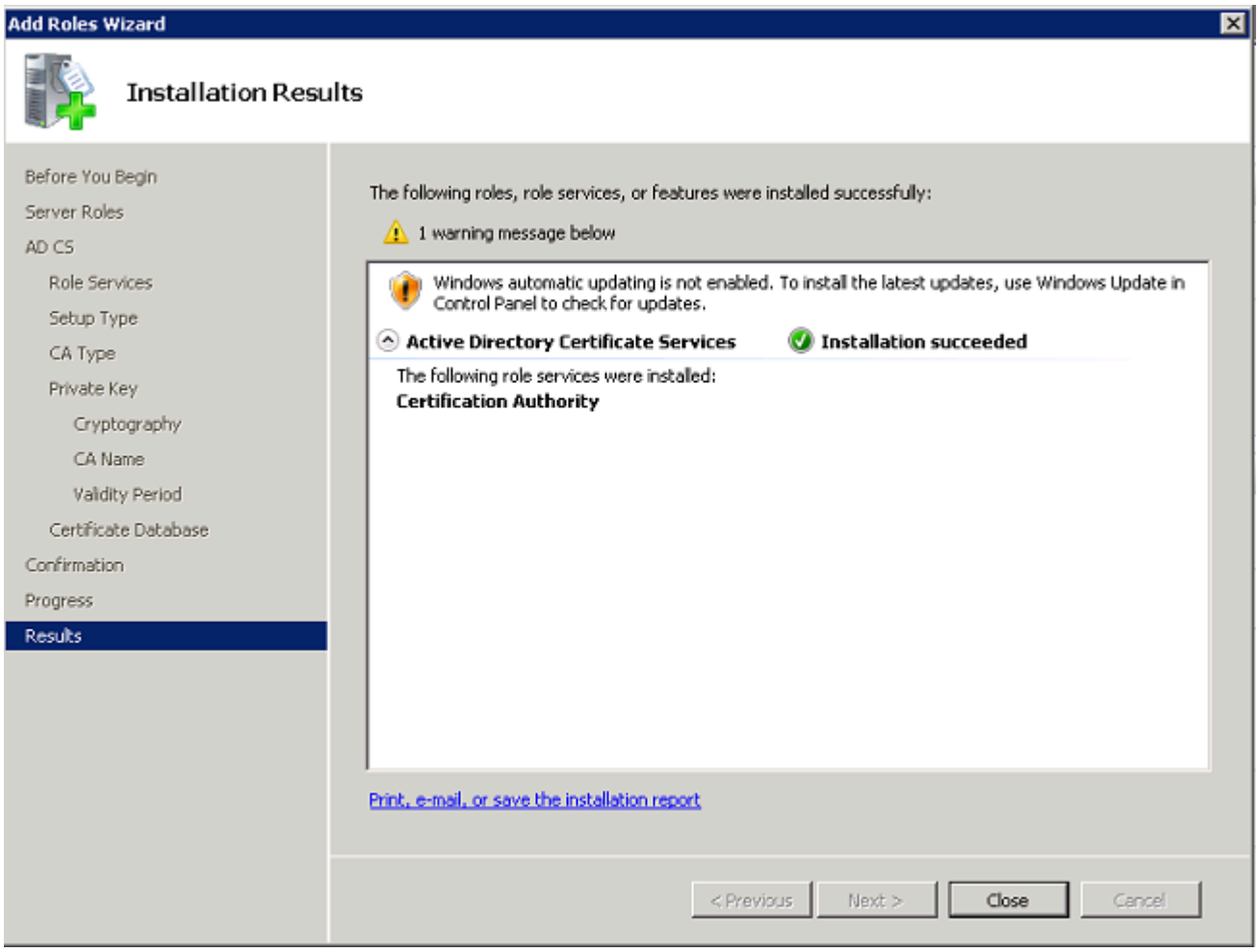
12. 選擇此CA證書的有效時間長度，然後按一下下一步。



13. 按一下下一步接受預設證書資料庫位置。



14. 檢查配置，然後按一下安裝以啟動Active Directory證書服務。

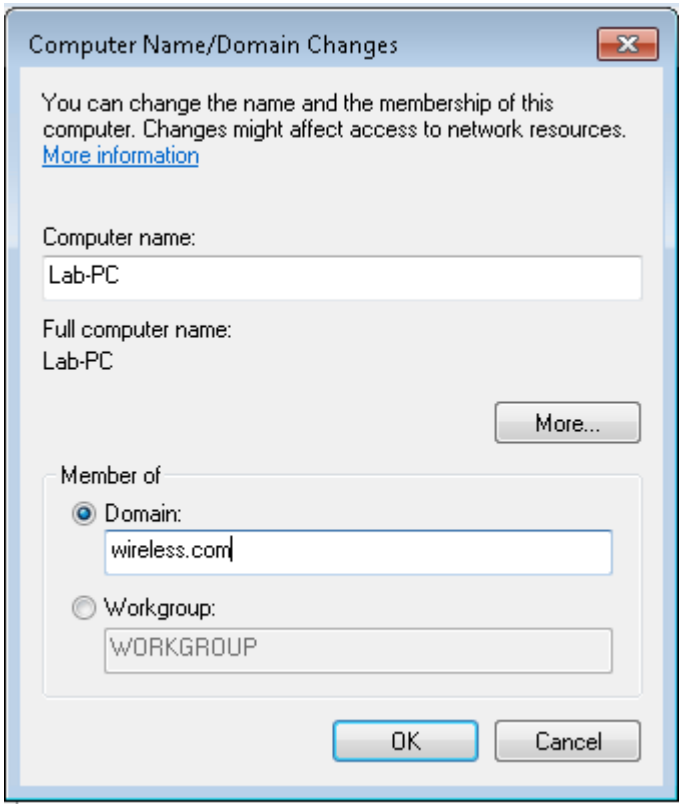


15. 安裝完成後，按一下「Close」。

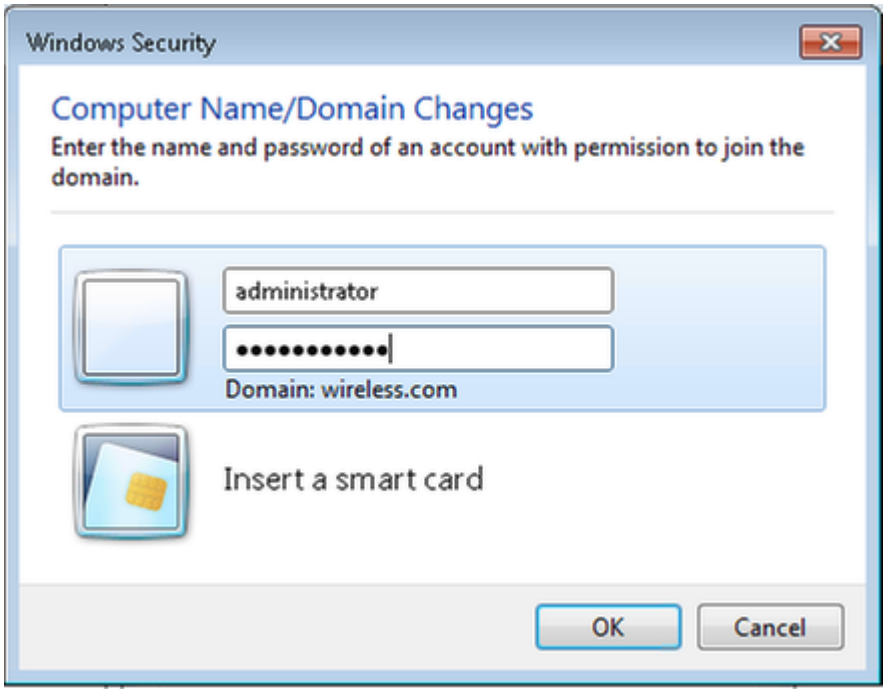
將客戶端連線到域

完成以下步驟，將使用者端連線到有線網路，並從新網域下載網域特定資訊：

1. 使用直通乙太網電纜將客戶端連線到有線網路。
2. 啟動客戶端，並使用客戶端使用者名稱和密碼登入。
3. 按一下「Start」>「Run」，輸入「cmd」，然後按一下「OK」。
4. 在命令提示符下，輸入ipconfig，然後按一下Enter以驗證DHCP是否正常工作，以及客戶端是否從DHCP伺服器收到IP地址。
5. 若要將客戶端加入域，請按一下開始，按一下右鍵電腦，選擇屬性，然後選擇右下角的更改設定。
6. 按一下「Change」。
7. 按一下Domain，輸入domain name（域名），wireless（例如，wireless），然後按一下OK。

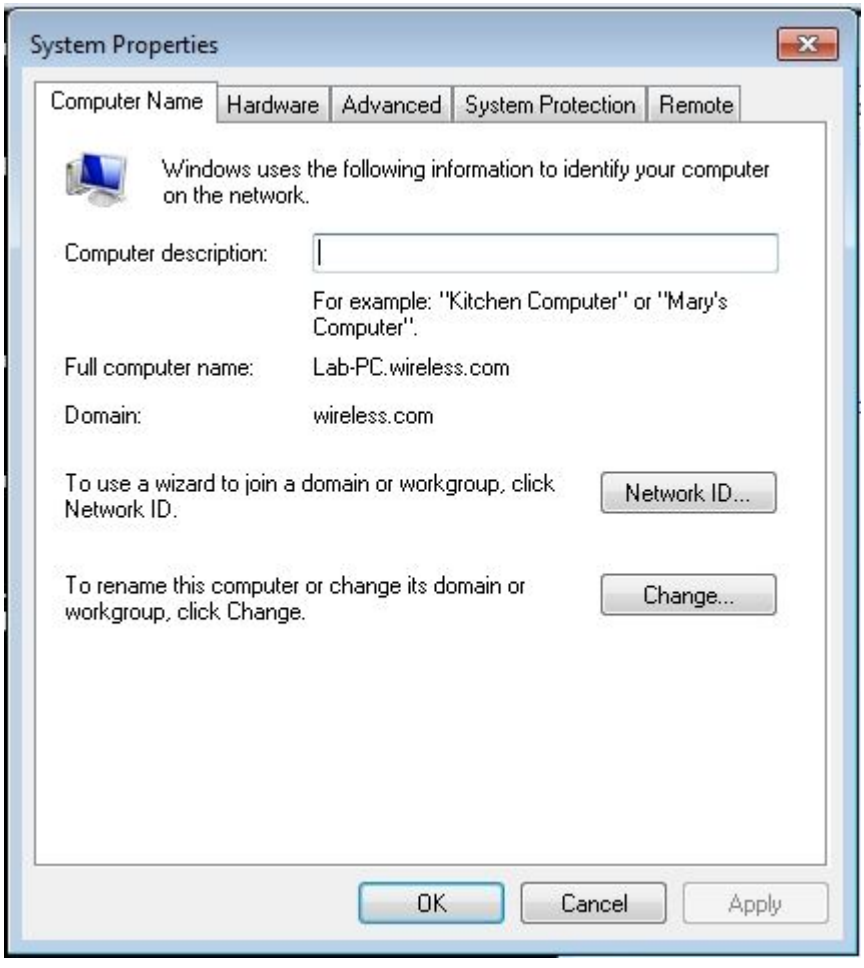


8. 輸入用戶名administrator以及客戶機加入的域特定的密碼。這是伺服器上Active Directory中的管理員帳戶。

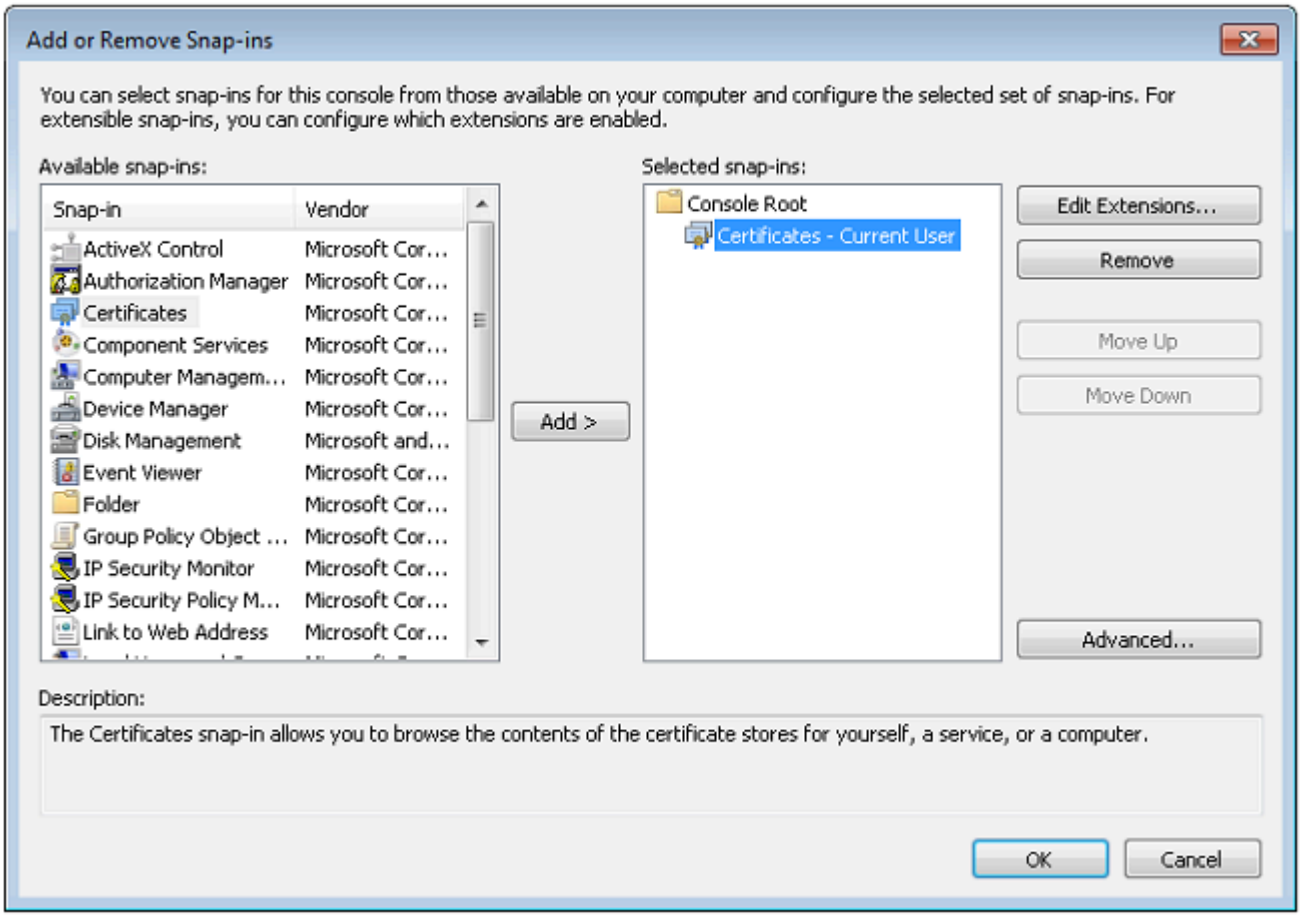


9. 按一下「OK」，然後再次按一下「OK」。

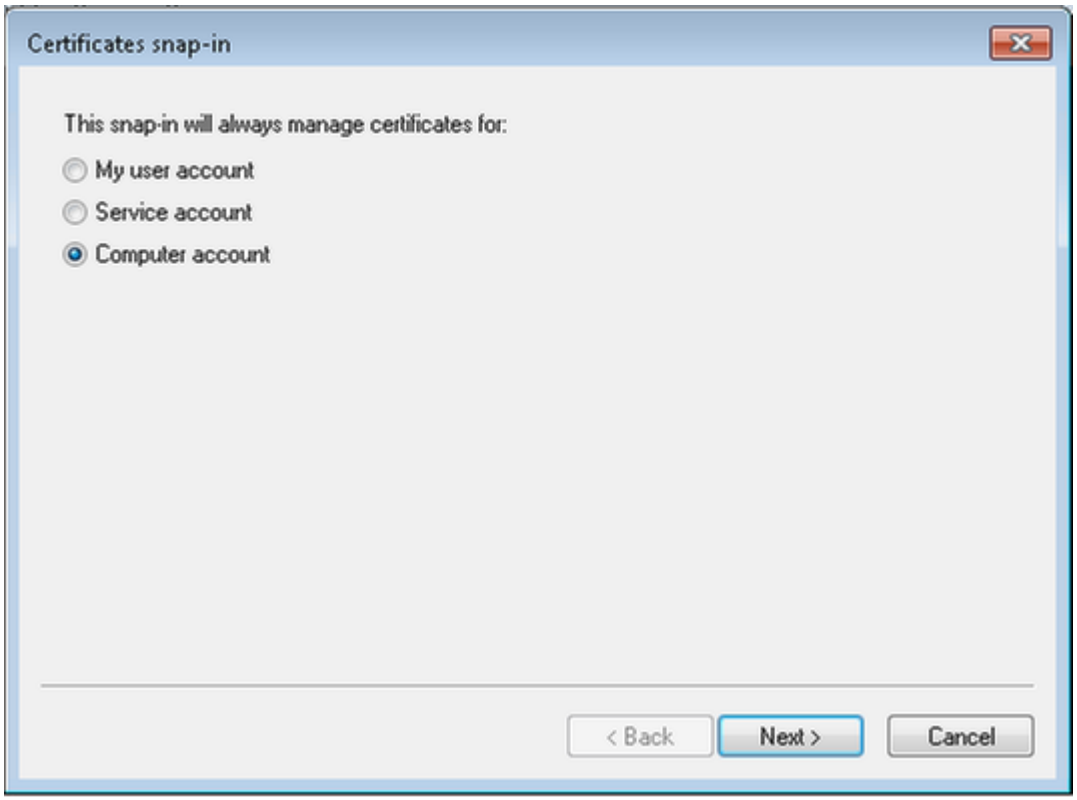
10. 按一下Close>Restart Now重新啟動電腦。
11. 電腦重新啟動後，使用以下命令登入：使用者名稱=管理員；密碼= <域密碼>;域=無線。
12. 按一下Start，按一下右鍵Computer，選擇Properties，然後選擇右下角的Change Settings以驗證您是否位於無線域中。
13. 下一步是驗證使用者端是否從伺服器收到CA憑證（信任）。



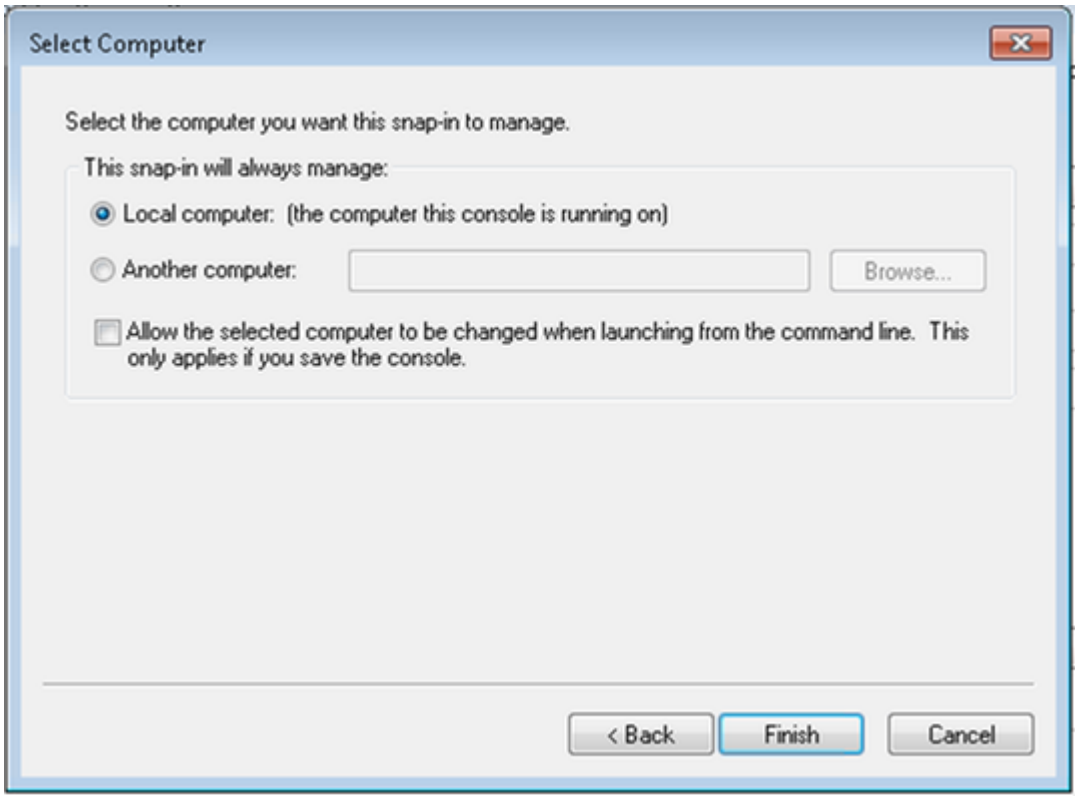
14. 按一下Start，輸入mmc，然後按Enter。
15. 按一下檔案，然後按一下新增/刪除管理單元。
16. 選擇「Certificates」，然後按一下「Add」。



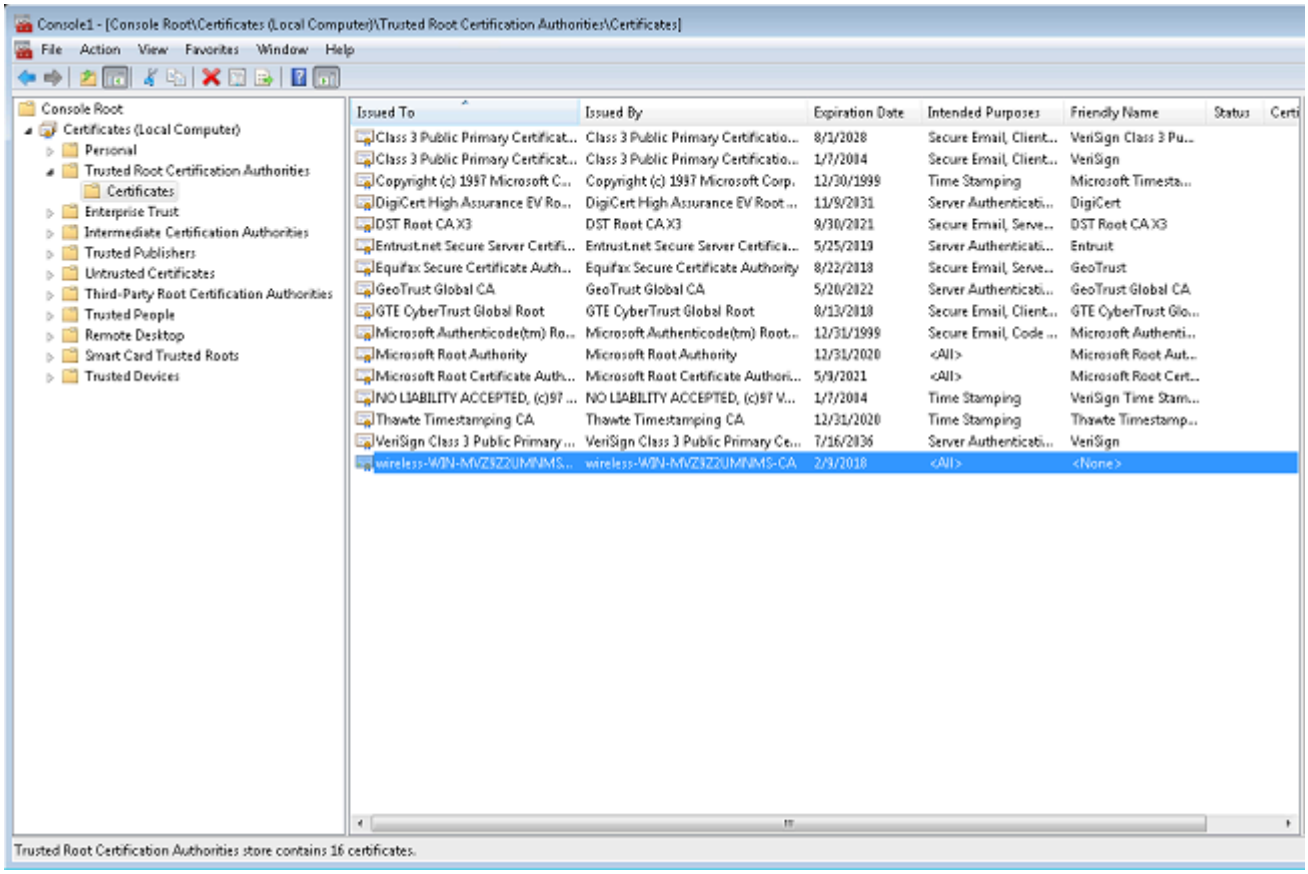
17. 按一下Computer account，然後按一下Next。



18. 按一下Local computer，然後按一下Next。



19. 按一下「OK」（確定）。
20. 展開Certificates(Local Computer)和Trusted Root Certification Authorities資料夾，然後按一下Certificates。在清單中查詢無線域CA證書。在本例中，CA證書稱為wireless-WIN-MVZ9Z2UMNMS-CA。

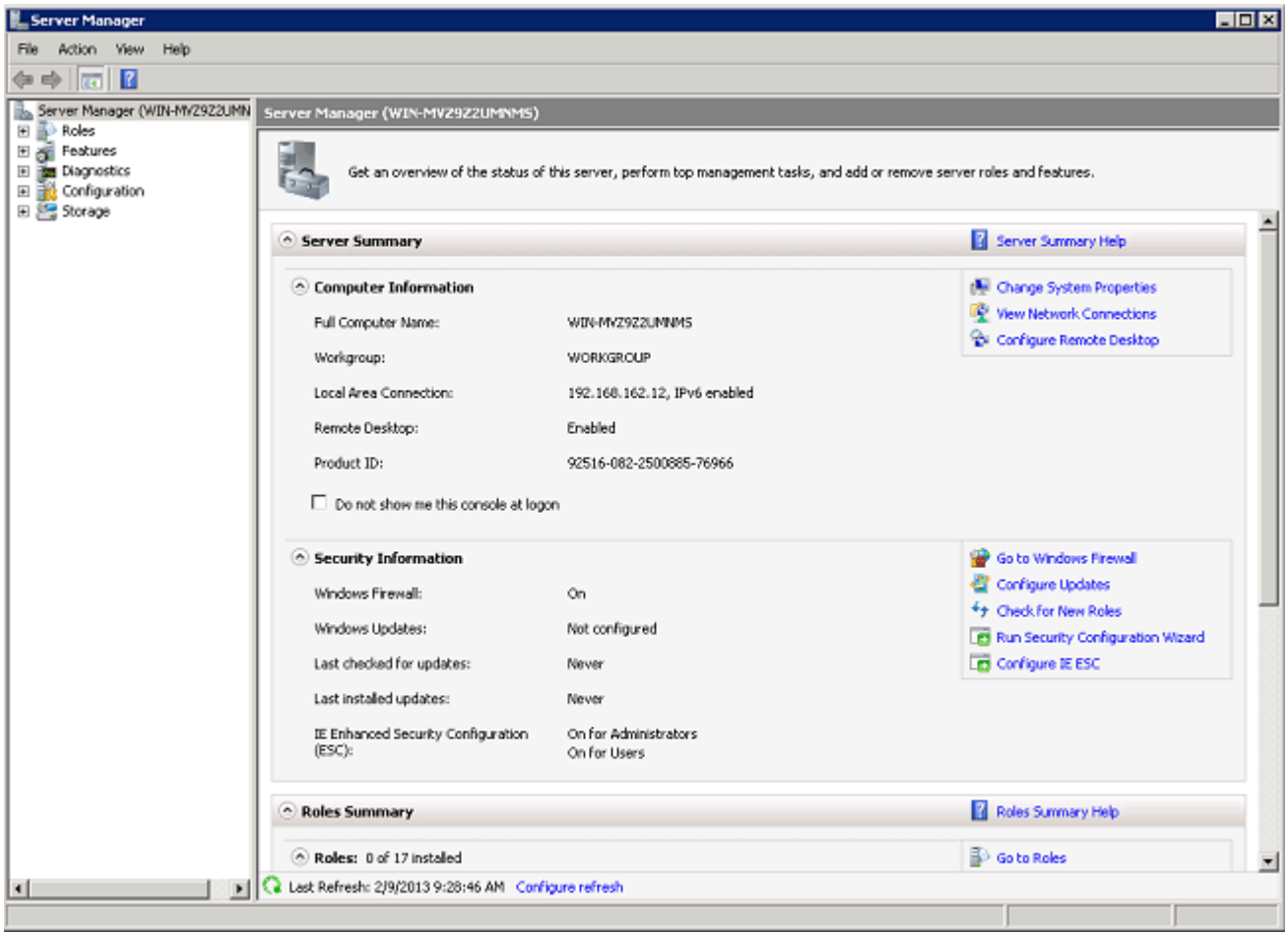


21. 重複此過程，向域中新增更多客戶端。

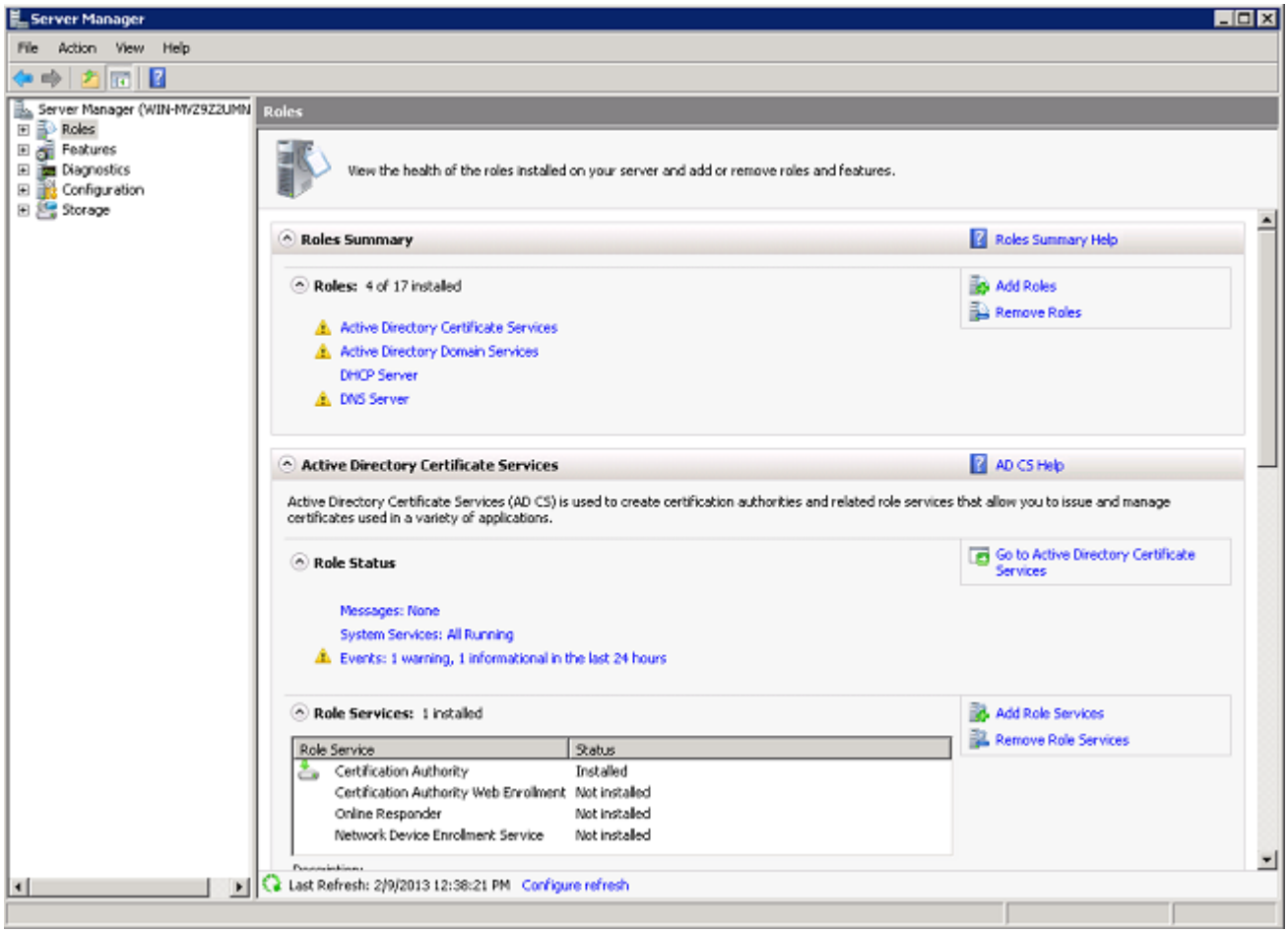
在Microsoft Windows 2008 Server上安裝網路策略伺服器

在此安裝程式中，NPS用作RADIUS伺服器，通過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 2008伺服器上安裝和配置NPS:

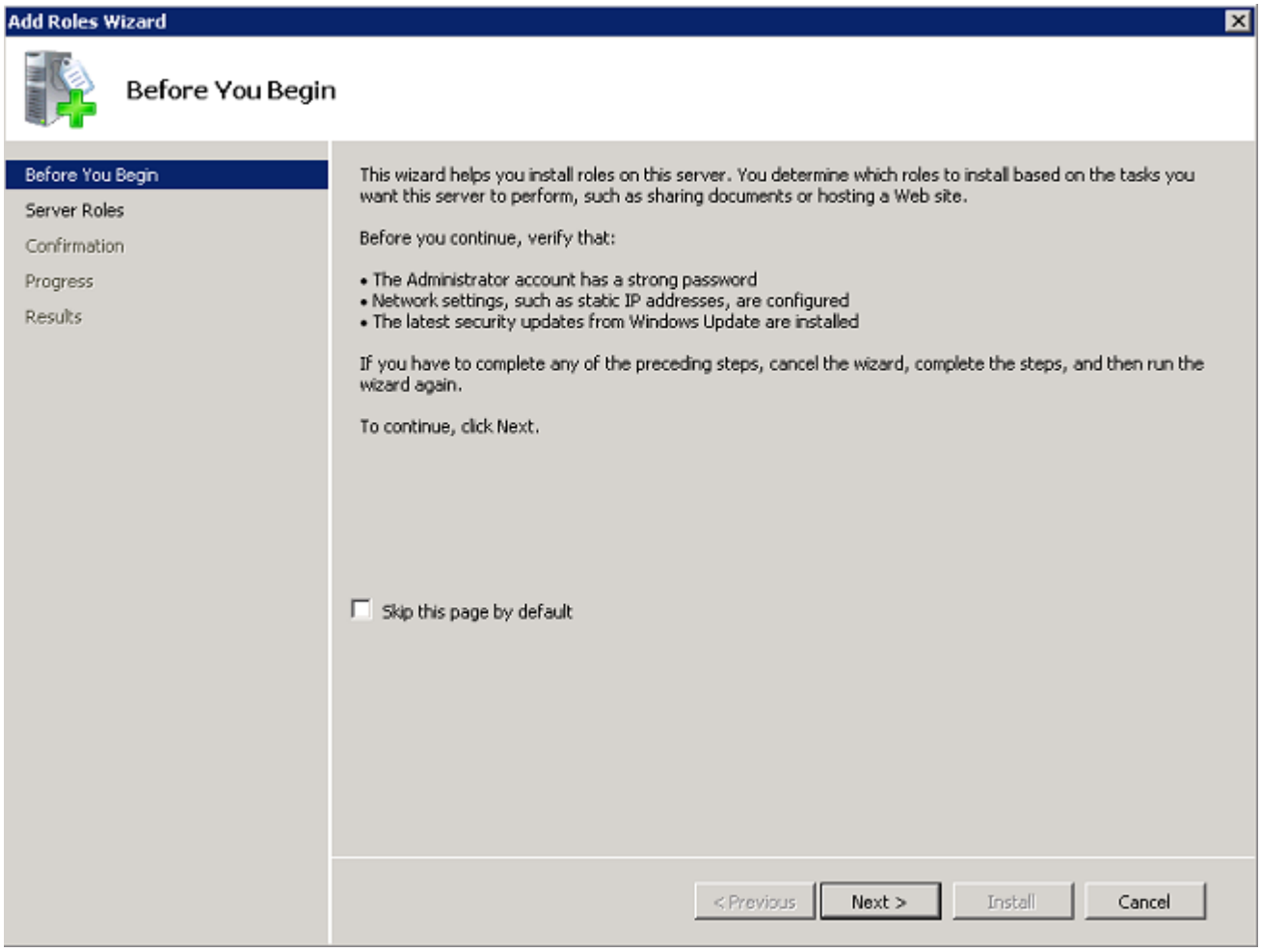
1. 按一下Start> Server Manager。



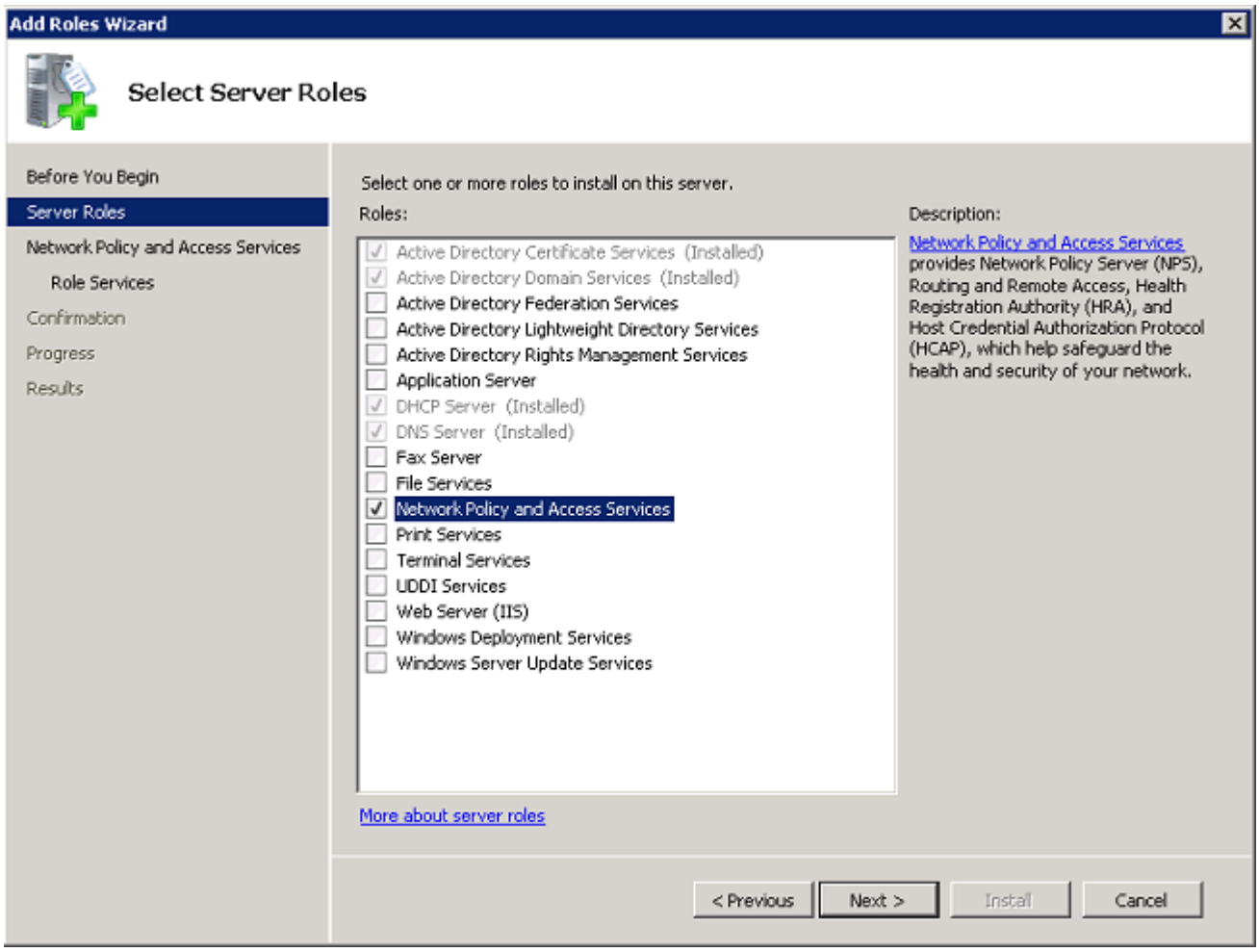
2. 按一下Roles> Add Roles。


Server Manager
File Action View Help
Server Manager (WIN-NVZ9ZZUMN
Roles
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 4 of 17 installed
Add Roles
Remove Roles
Active Directory Certificate Services
Active Directory Domain Services
DHCP Server
DNS Server
Active Directory Certificate Services
AD CS Help
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
Role Status
Go to Active Directory Certificate Services
Messages: None
System Services: All Running
Events: 1 warning, 1 informational in the last 24 hours
Role Services: 1 installed
Add Role Services
Remove Role Services
Role Service
Status
Certification Authority
Installed
Certification Authority Web Enrollment
Not installed
Online Responder
Not installed
Network Device Enrollment Service
Not installed
Last Refresh: 2/9/2013 12:38:21 PM
Configure refresh

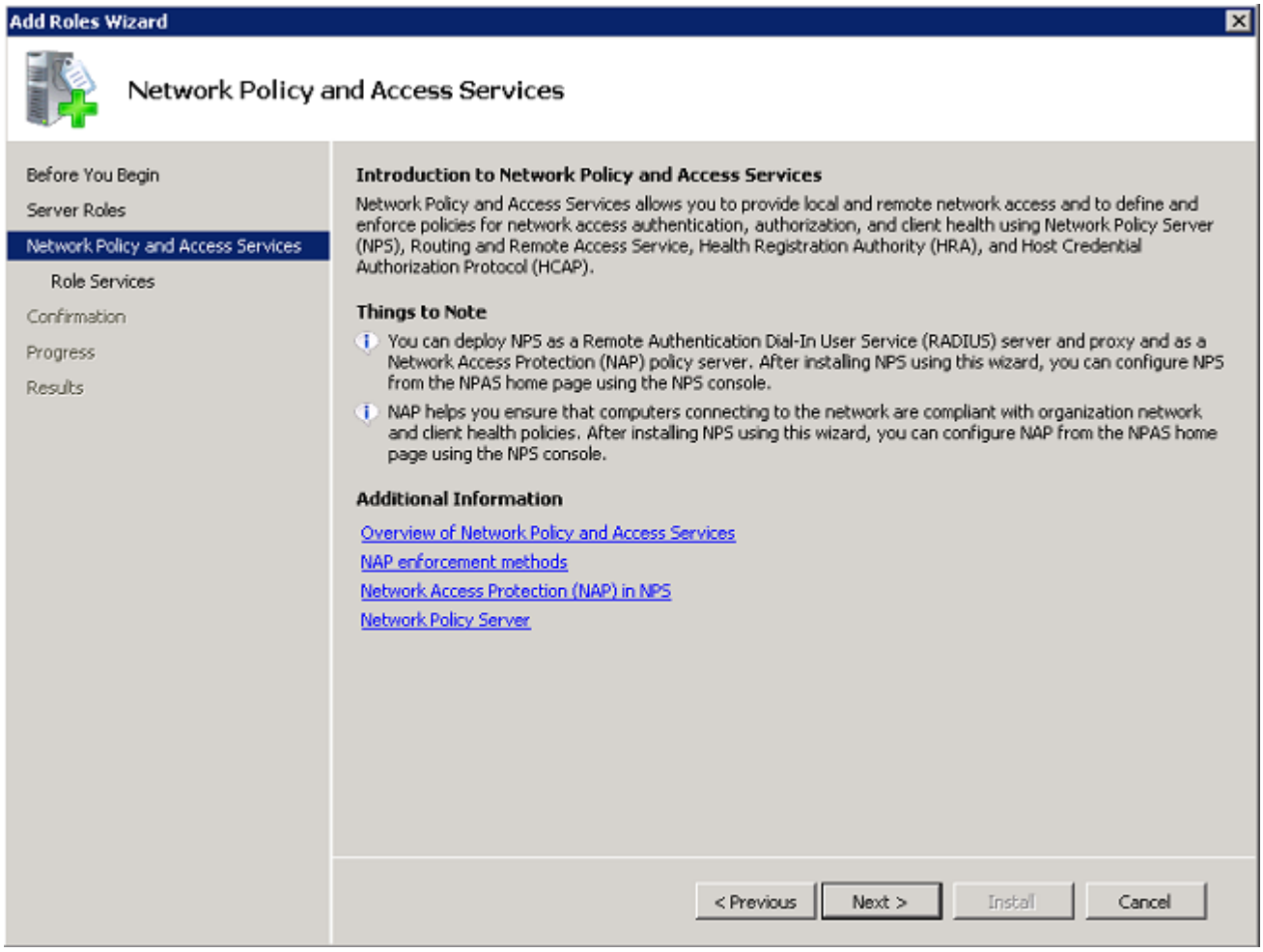
3. 按「Next」（下一步）。



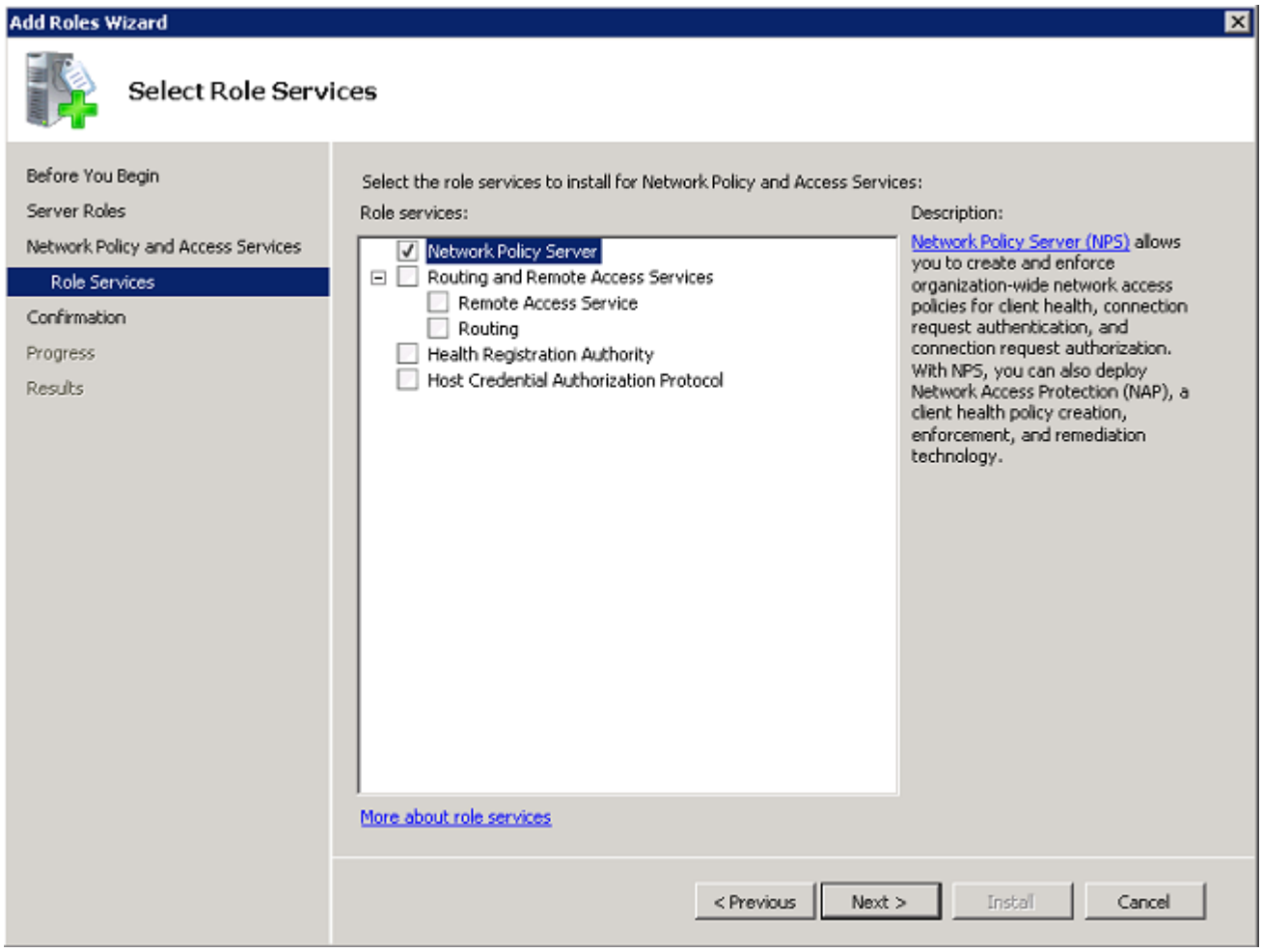
4. 選擇服務Network Policy and Access Services，然後按一下Next。



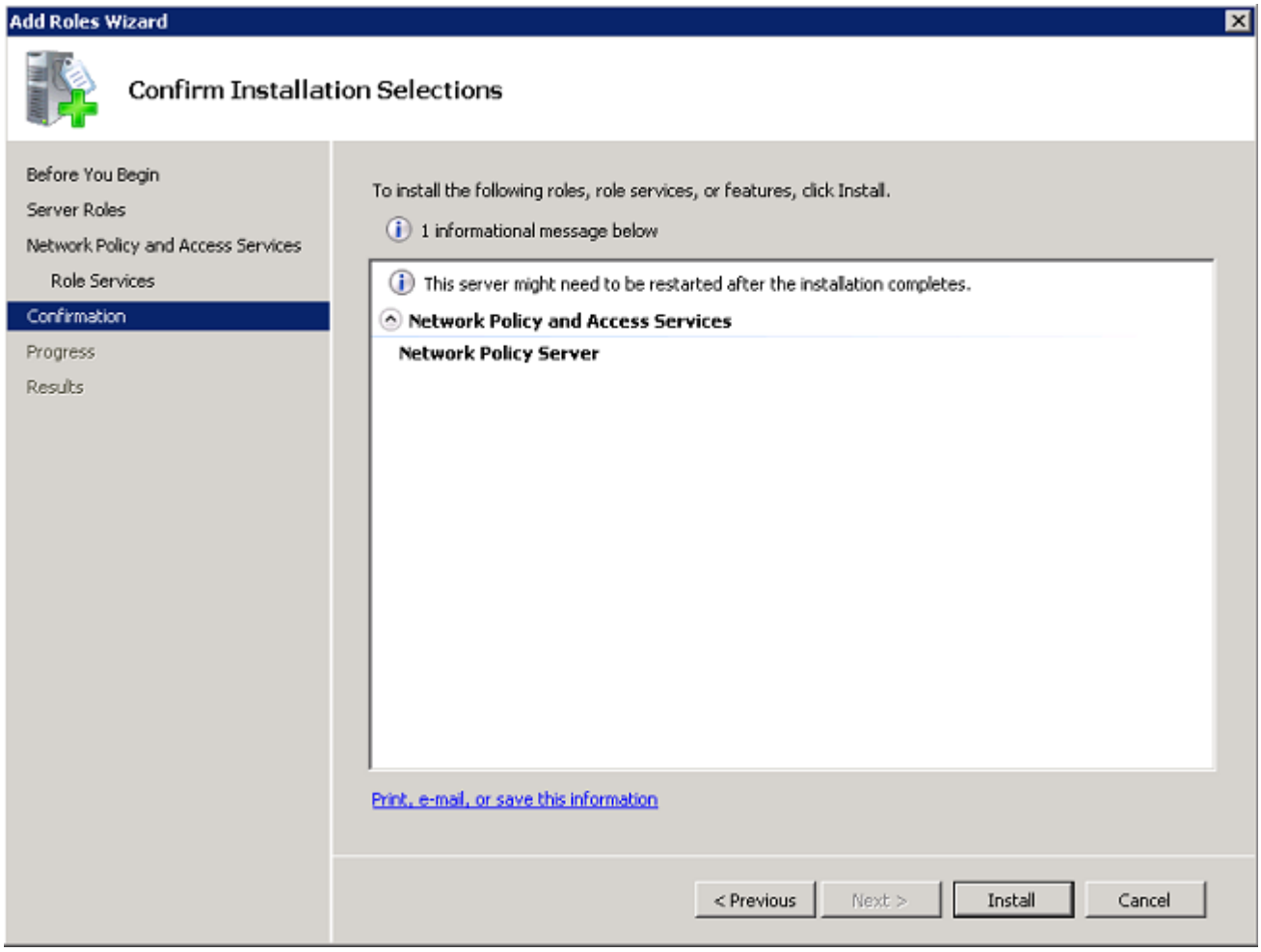
5. 檢視Introduction to Network Policy and Access Services，然後按一下Next。



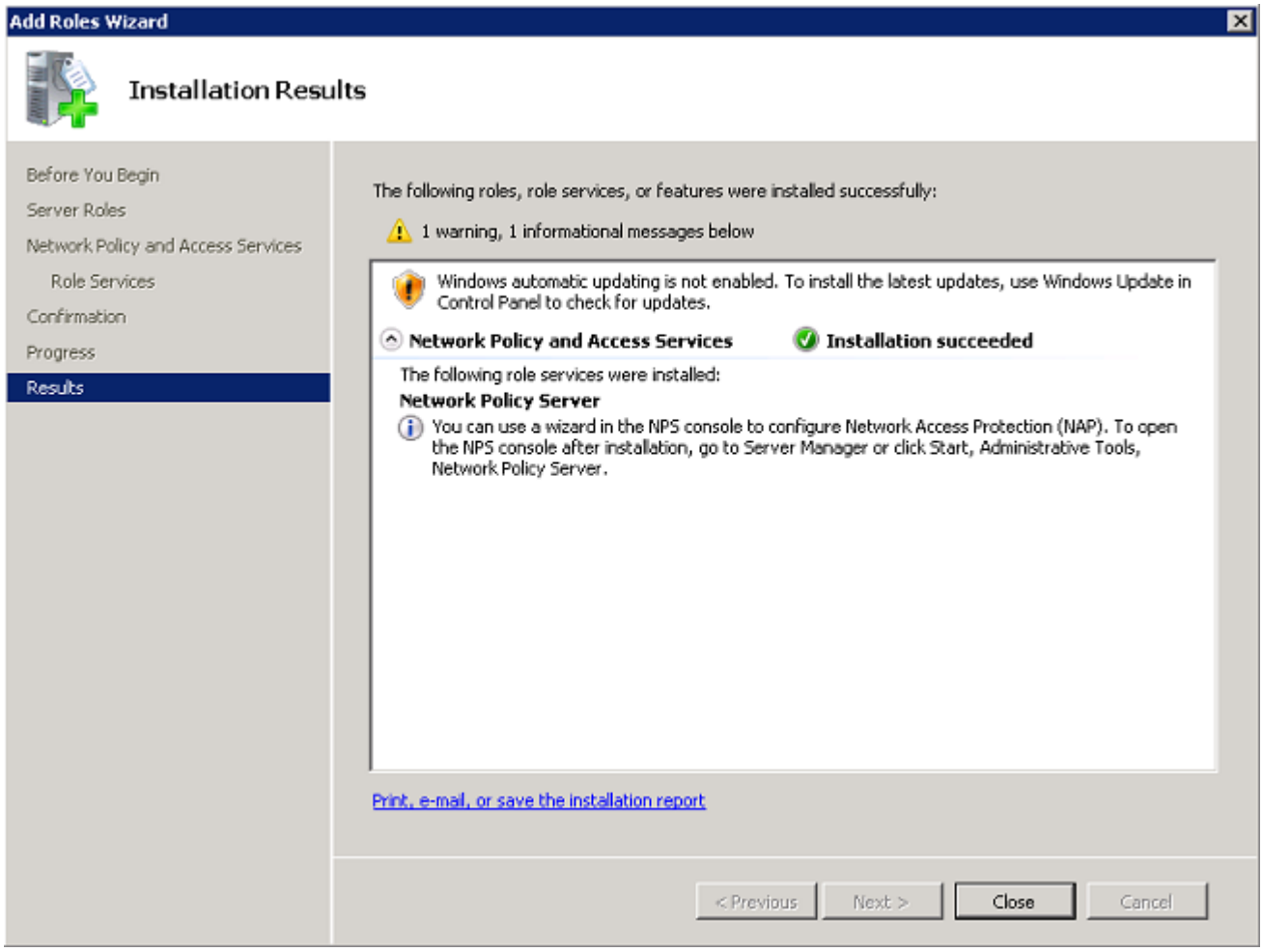
6. 選擇Network Policy Server，然後按一下Next。



7. 檢視確認，然後點選安裝。



安裝完成後，將顯示一個與此類似的螢幕。

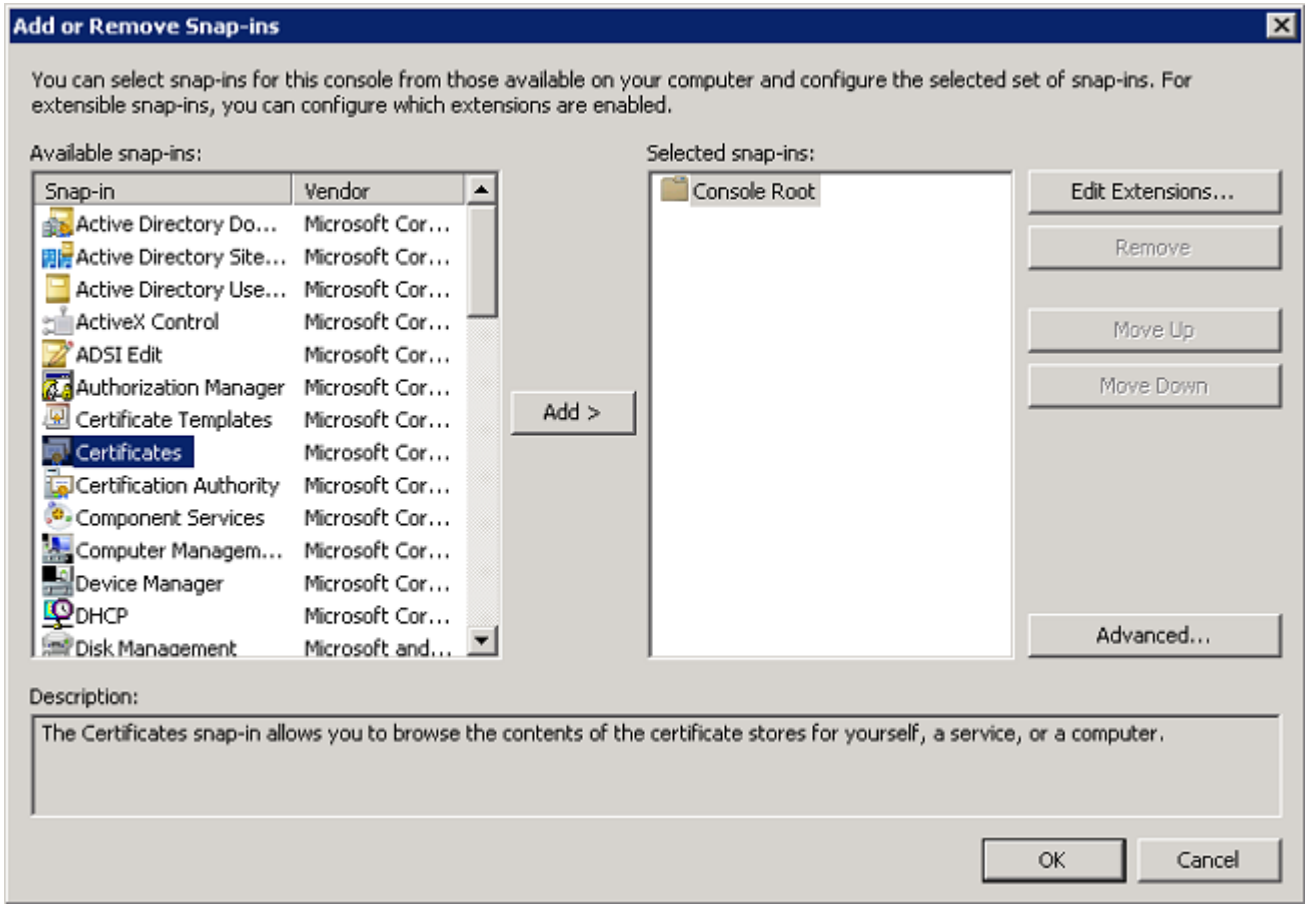


8. 按一下「Close」。

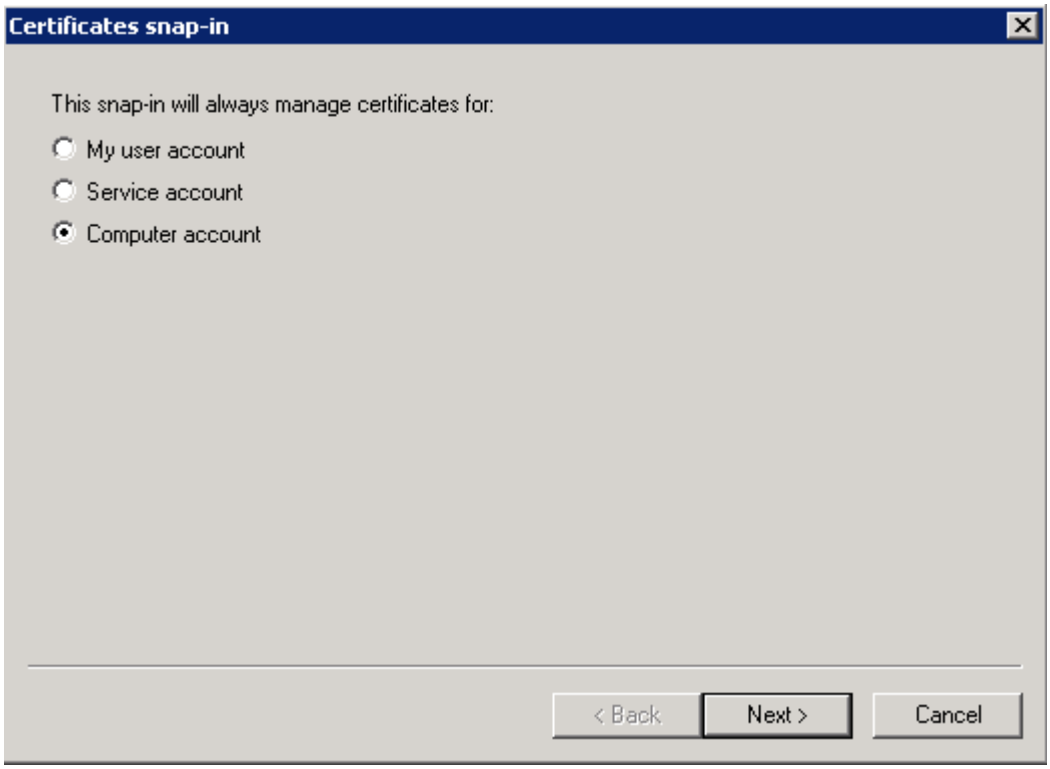
安裝證書

要安裝NPS的電腦證書，請完成以下步驟：

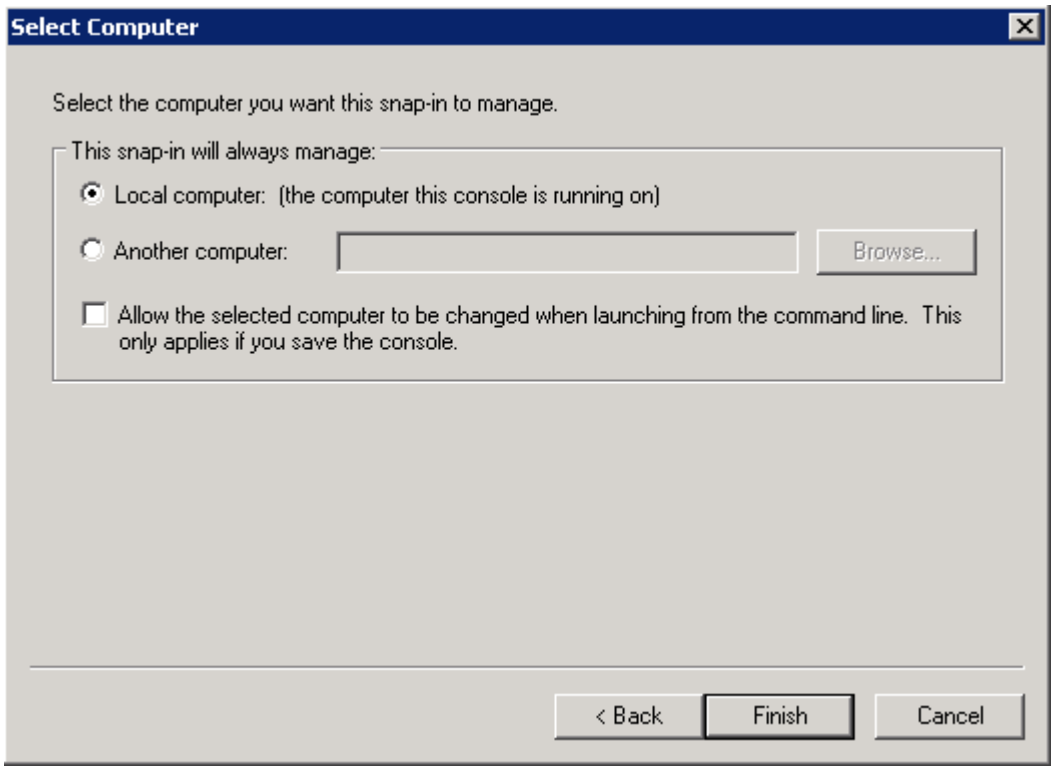
1. 按一下Start，輸入mmc，然後按Enter。
2. 按一下File > Add/Remove Snap-in。
3. 選擇「Certificates」，然後按一下「Add」。



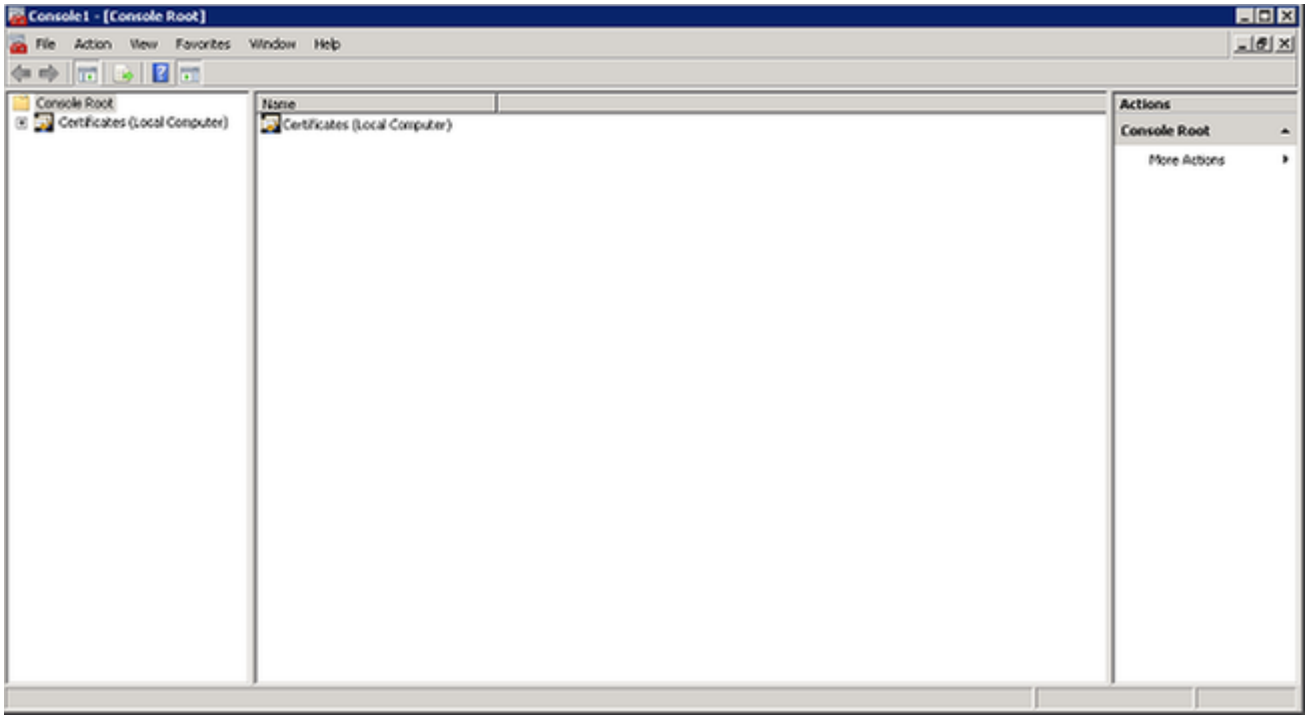
4. 選擇「Computer account」，然後按一下「Next」。



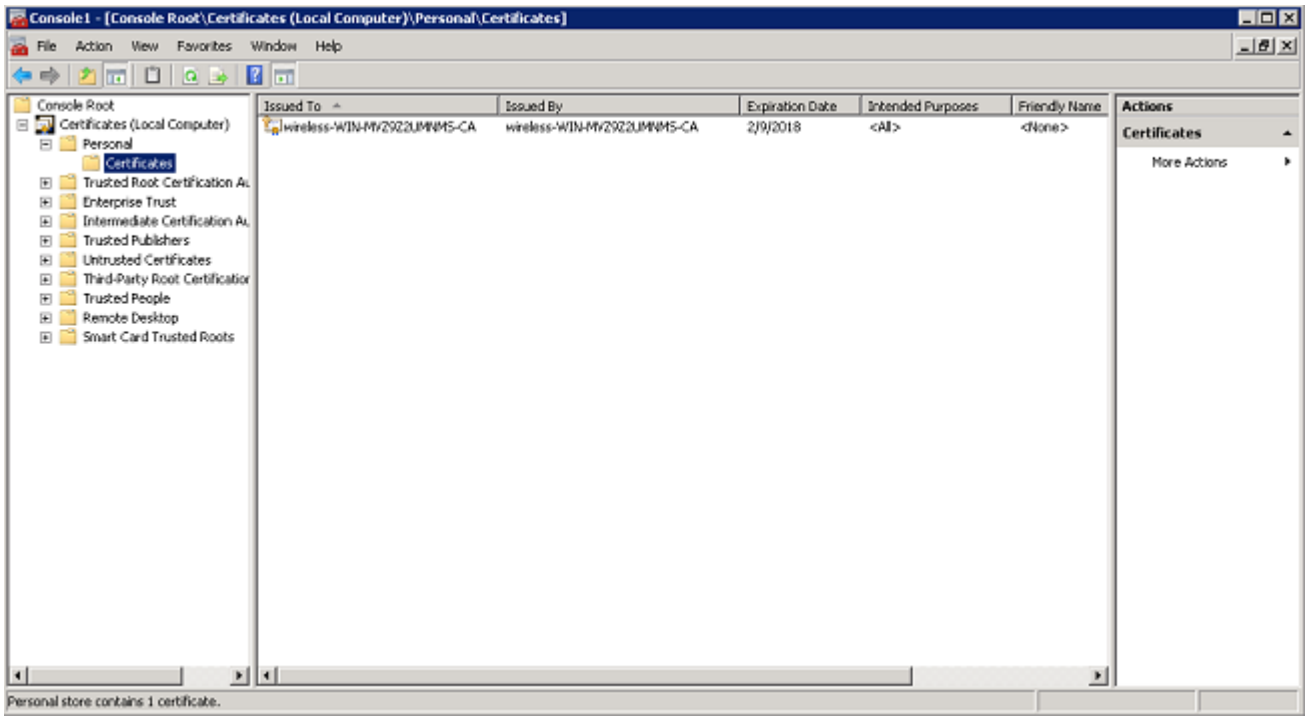
5. 選擇Local Computer，然後按一下Finish。



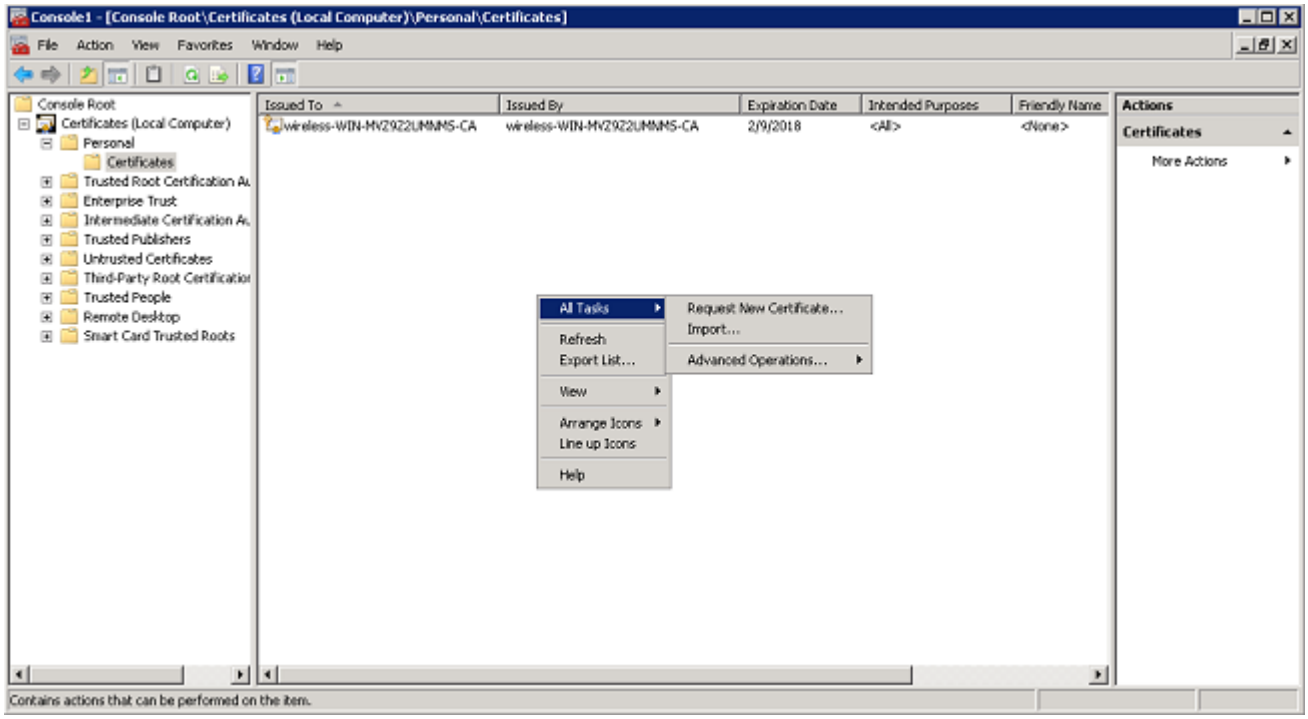
6. 按一下OK以返回Microsoft管理控制檯(MMC)。



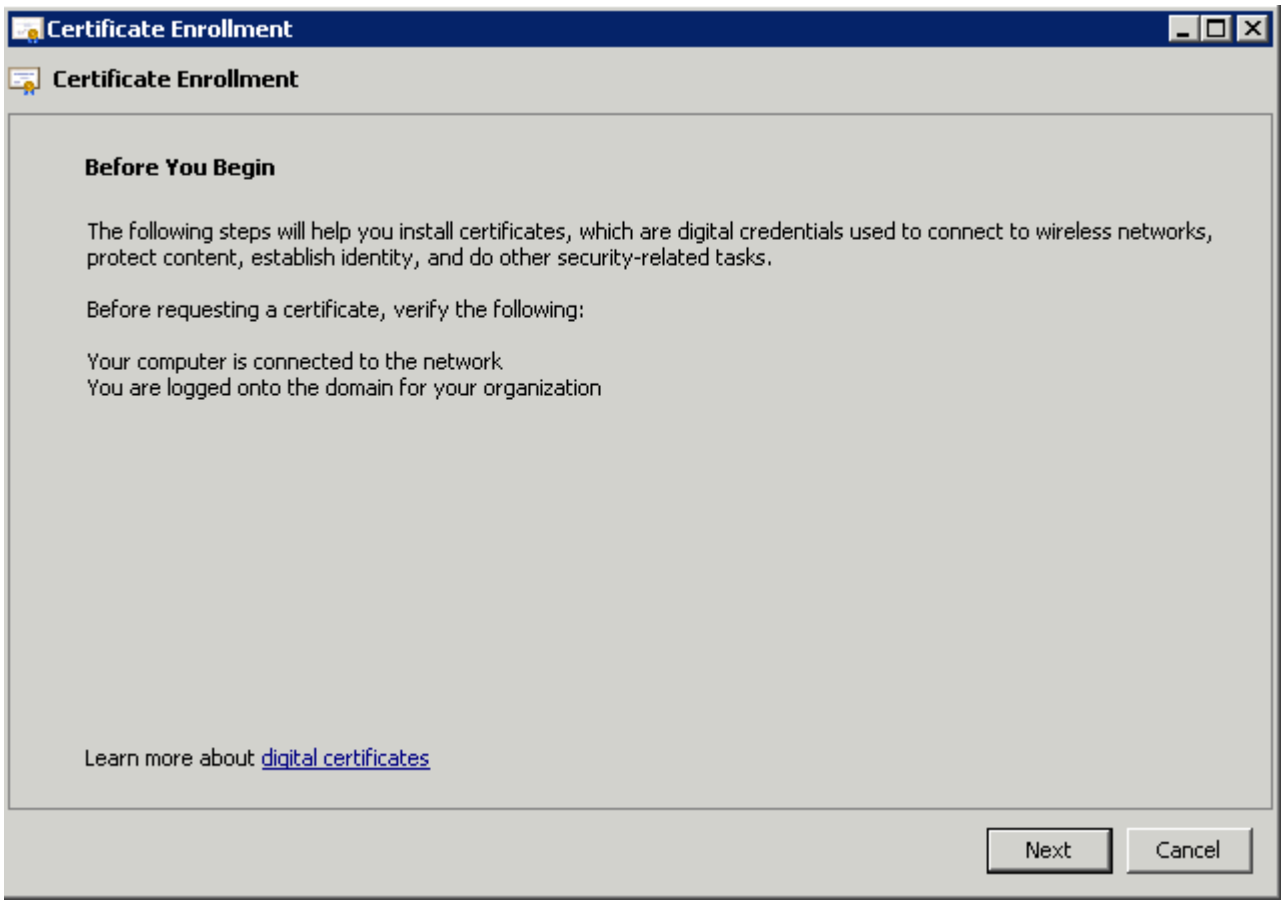
7. 展開Certificates(Local Computer)和Personal資料夾，然後按一下Certificates。



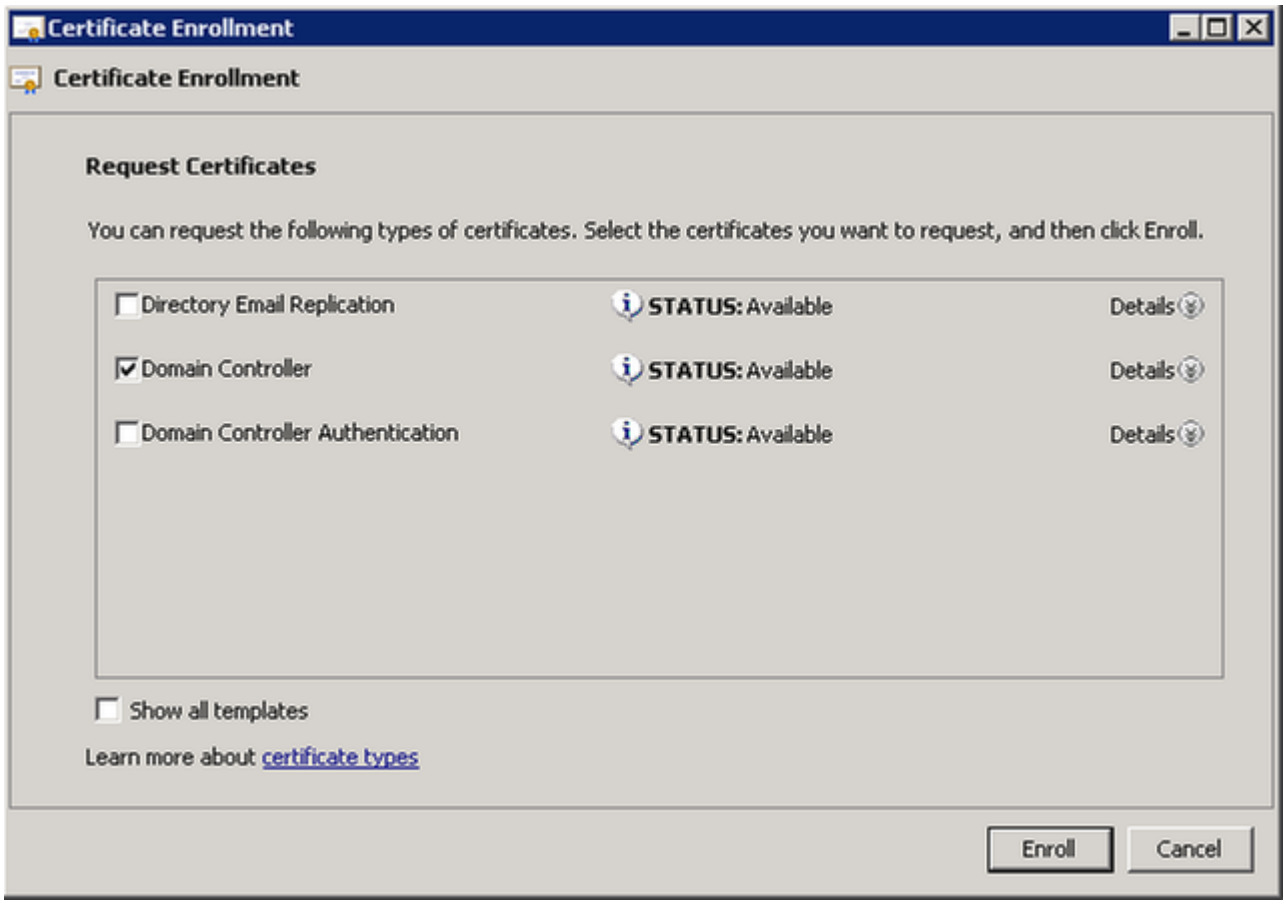
8. 在CA證書下的空白處按一下右鍵，然後選擇All Tasks > Request New Certificate。



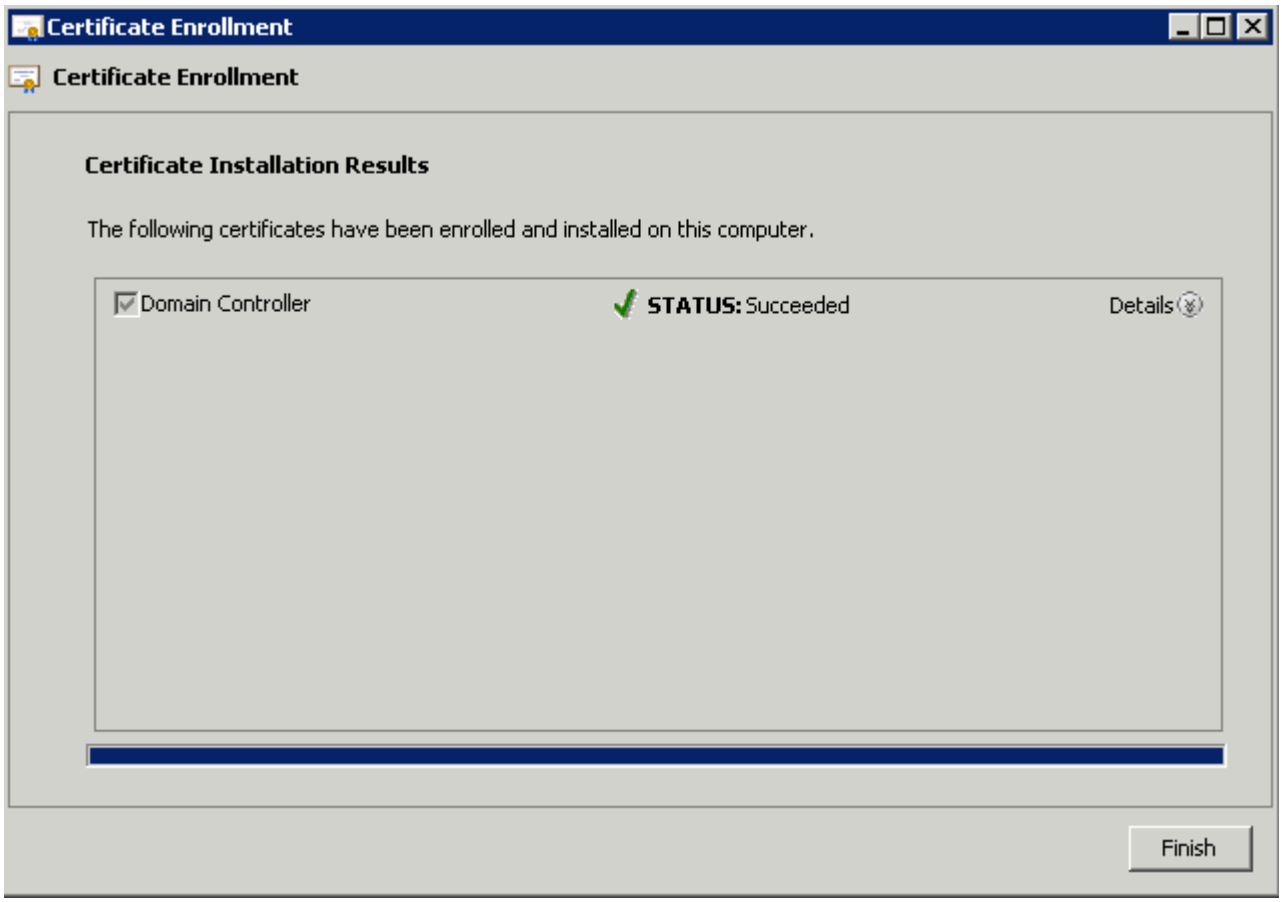
9. 按「Next」（下一步）。



10. 選擇Domain Controller，然後按一下Enroll。

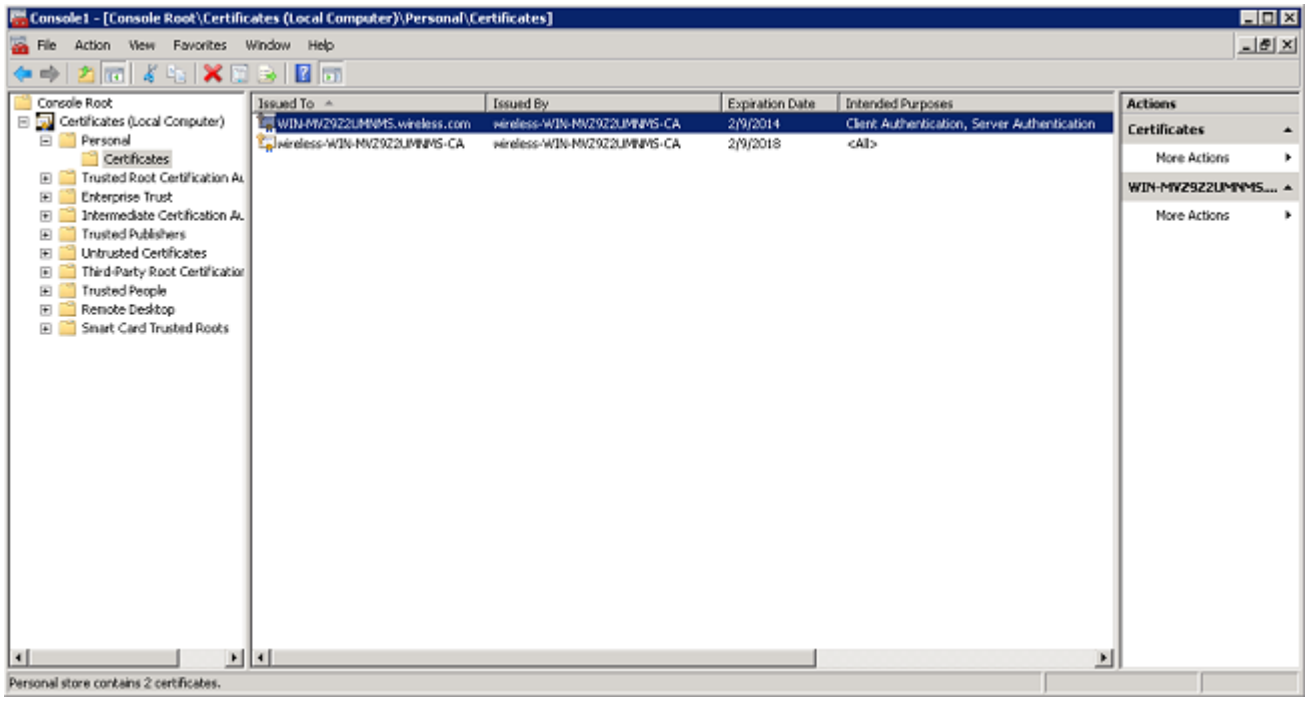


11. 安裝憑證後，按一下Finish。



NPS證書現在已安裝。

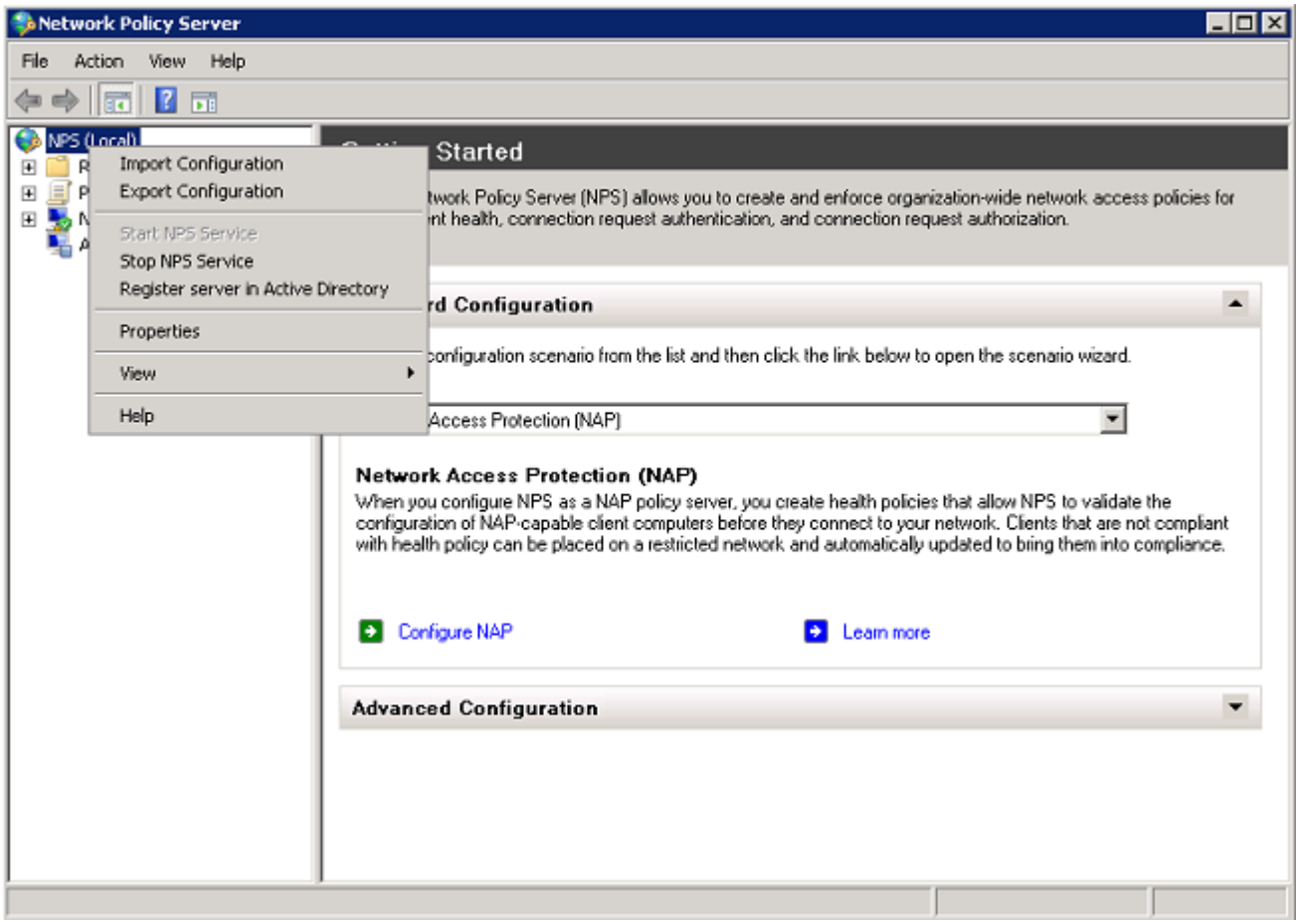
12. 確保證書的預期用途為「Client Authentication， Server Authentication」。



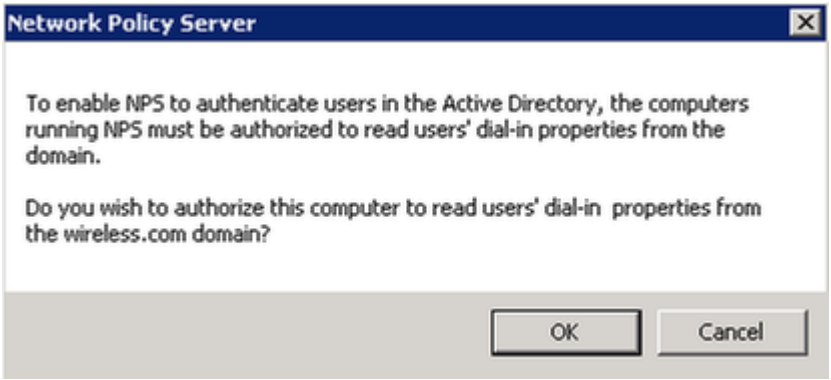
為PEAP-MS-CHAP v2身份驗證配置網路策略伺服器服務

完成以下步驟，配置NPS進行身份驗證：

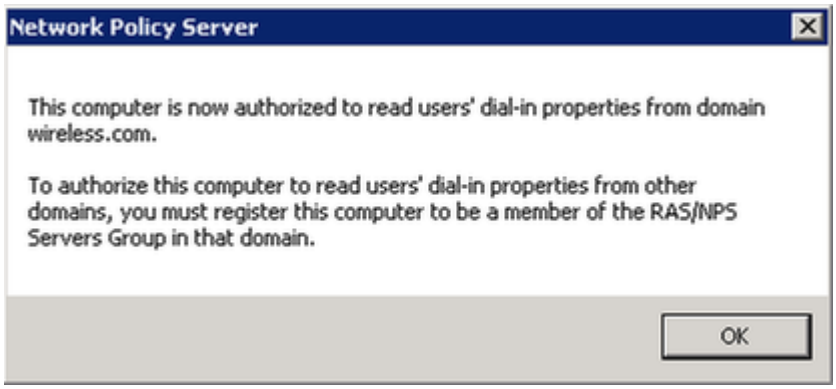
1. 按一下Start> Administrative Tools> Network Policy Server。
2. 按一下右鍵NPS（本地），然後選擇Register server in Active Directory。



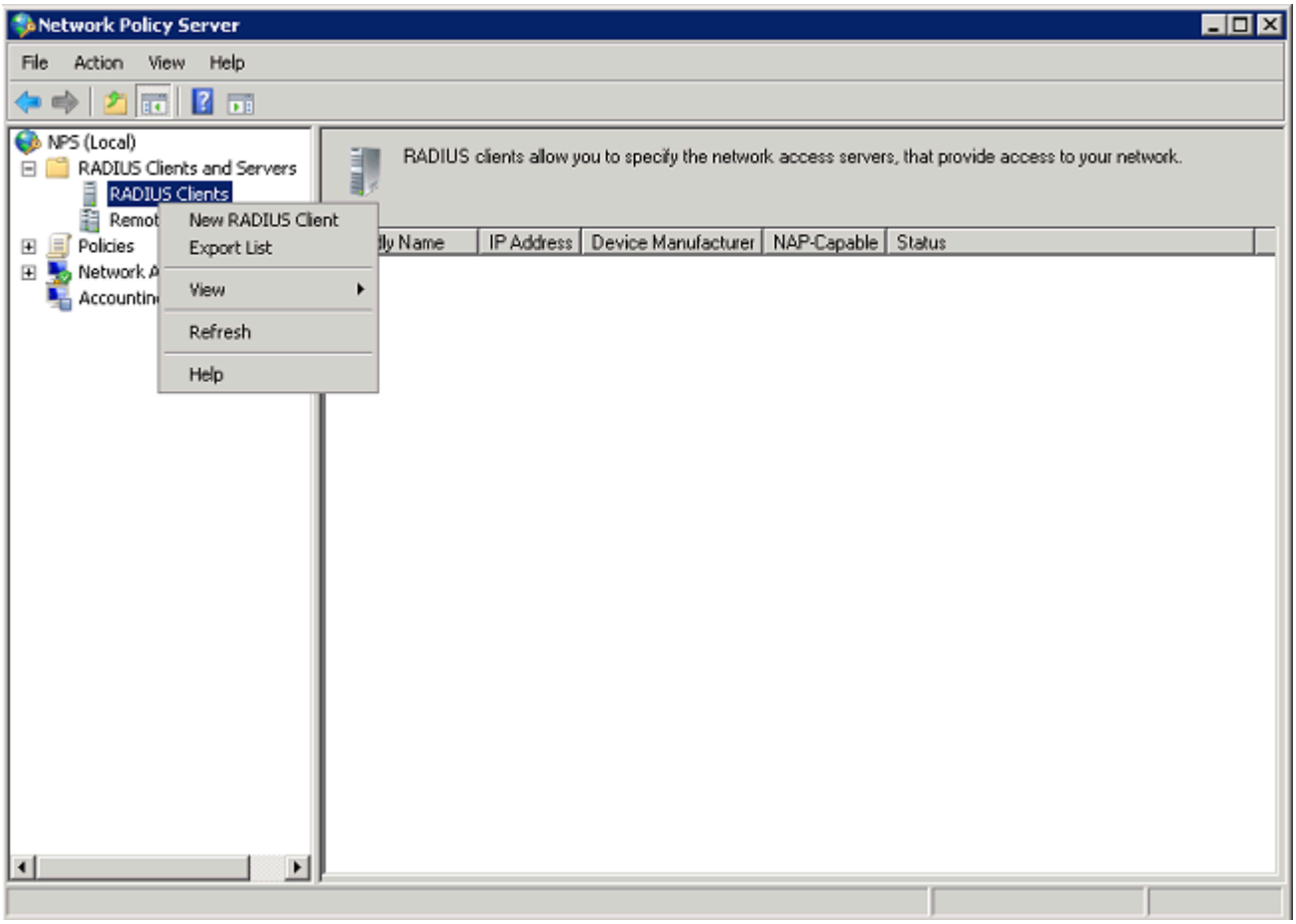
3. 按一下「OK」（確定）。



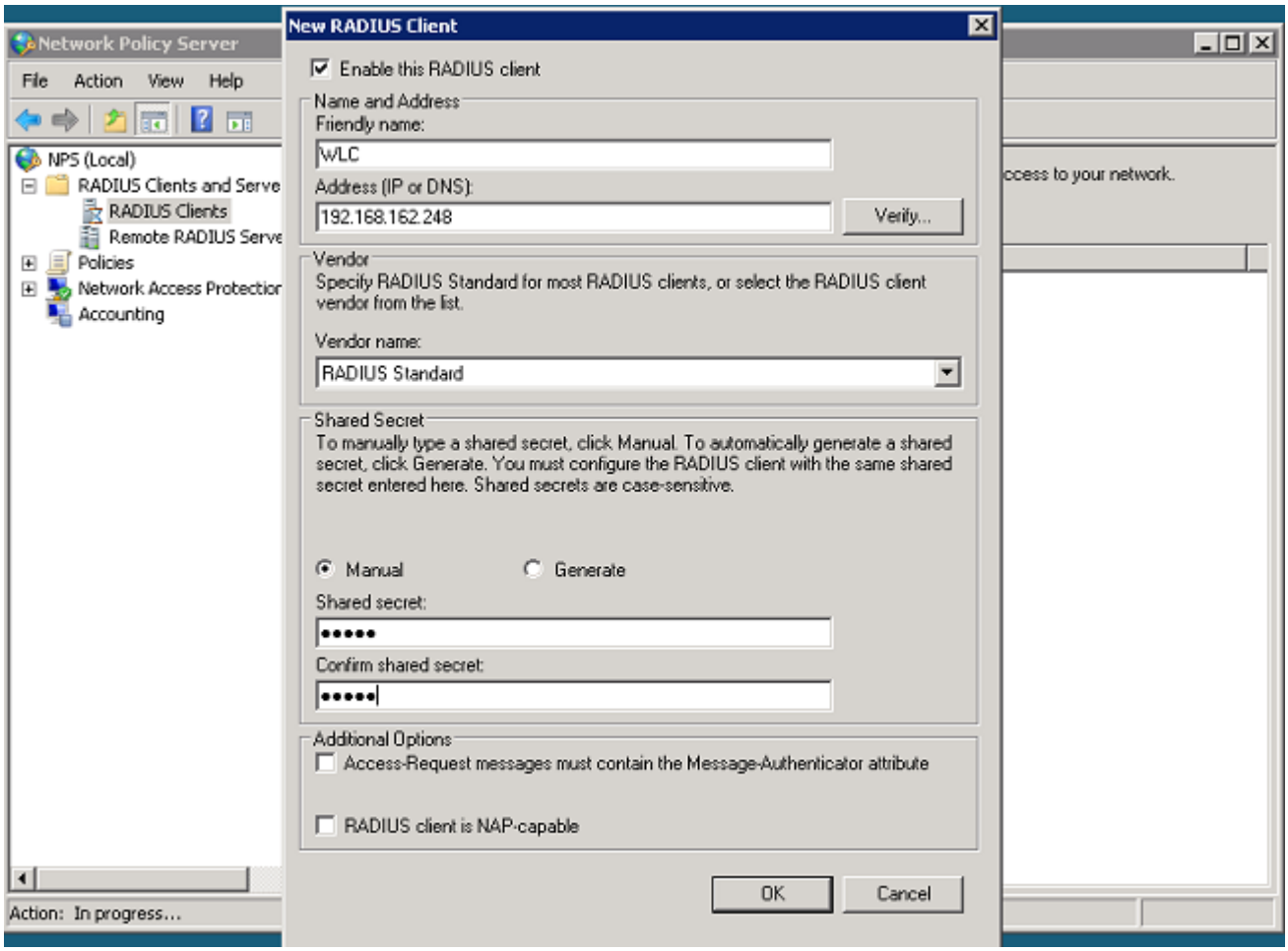
4. 按一下「OK」（確定）。



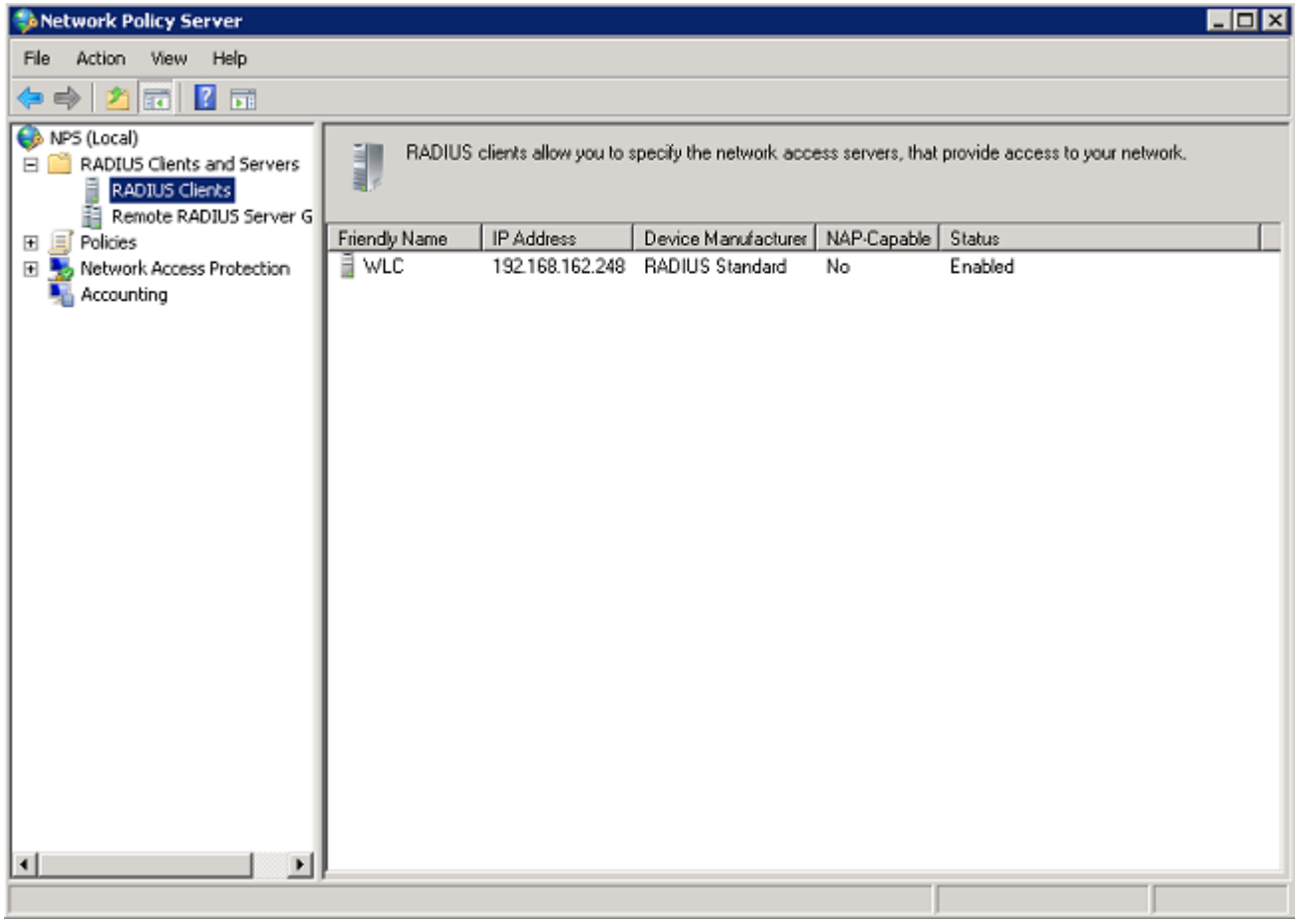
5. 將無線LAN控制器新增為NPS上的身份驗證、授權和記帳(AAA)客戶端。
6. 展開RADIUS客戶端和伺服器。按一下右鍵RADIUS Clients，然後選擇New RADIUS Client。



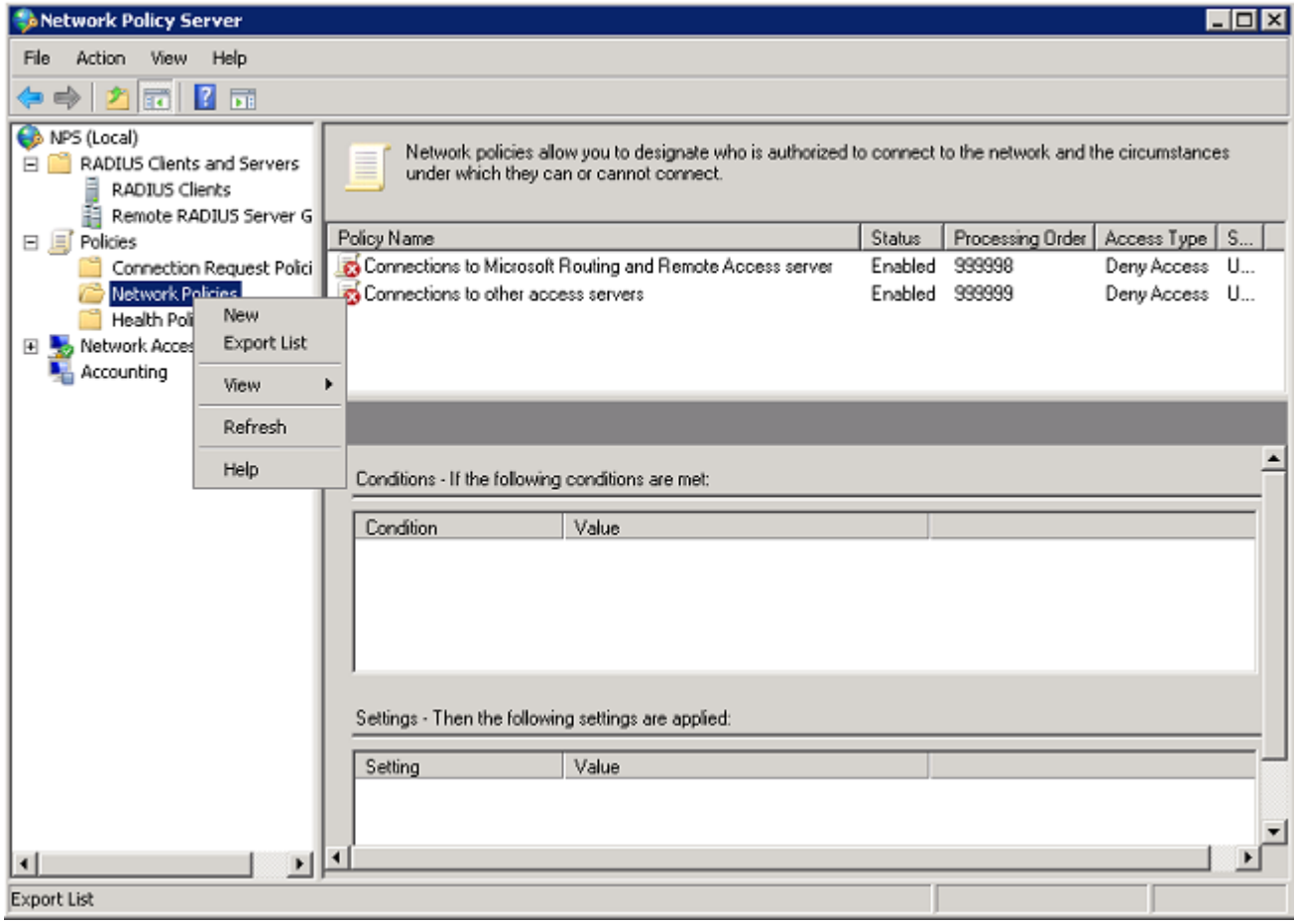
7. 輸入友好名稱（在本範例中為WLC）、WLC的管理IP位址（在本範例中為192.168.162.248）和共用密碼。使用相同的共用金鑰設定WLC。



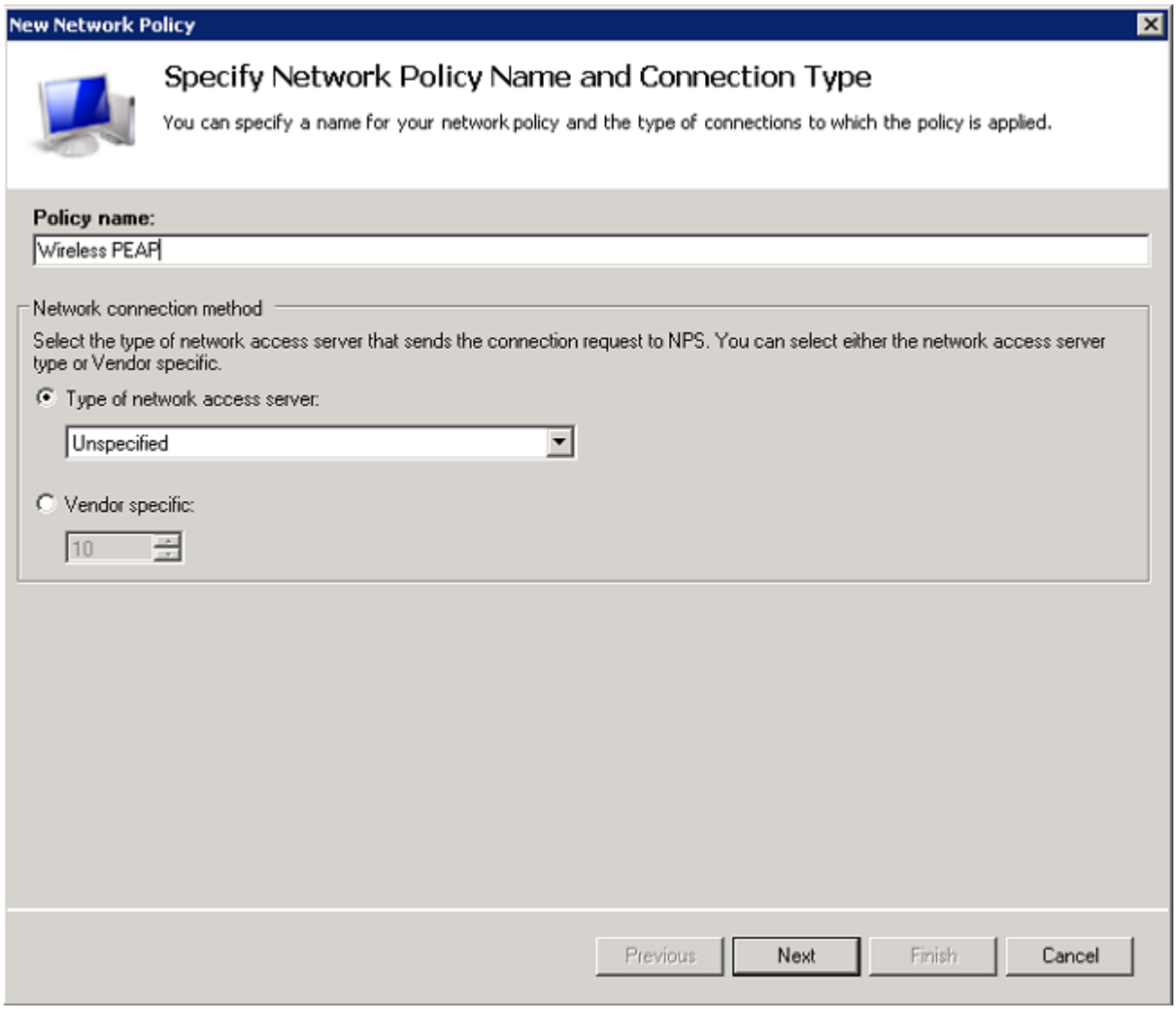
8. 按一下OK返回上一個螢幕。



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。

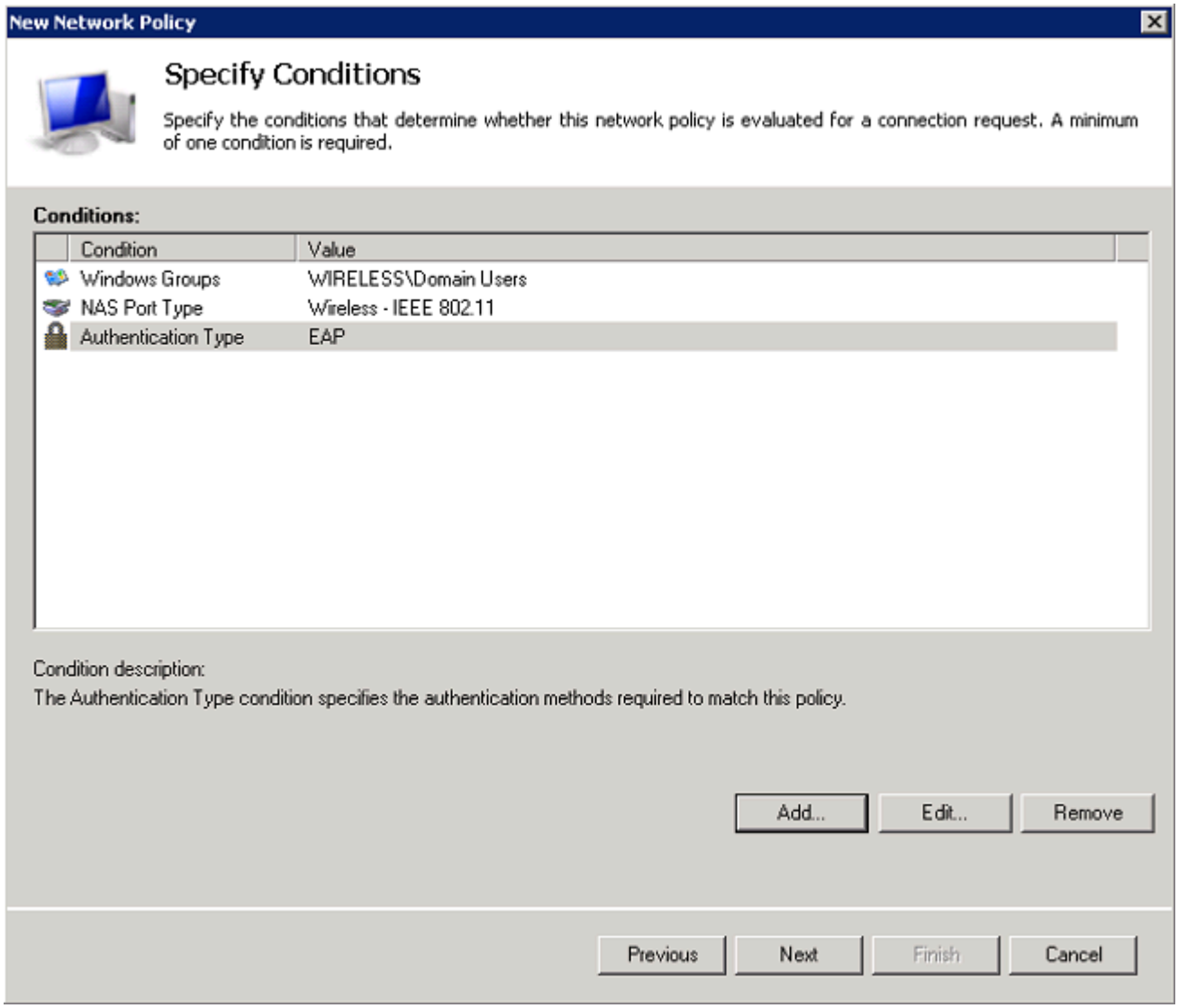


10. 輸入此規則的策略名稱（在本例中為Wireless PEAP），然後按一下Next。

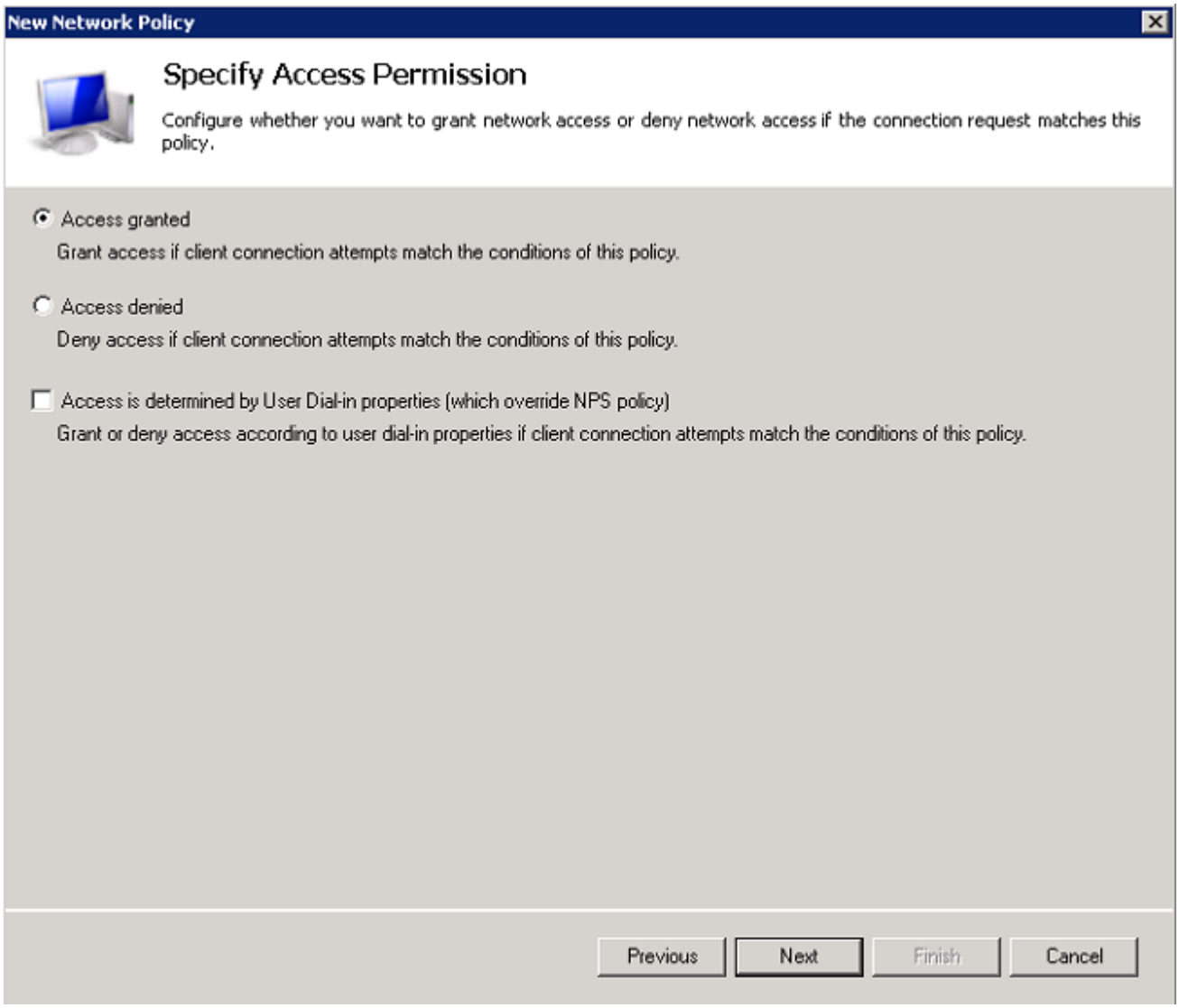


11. 要使此策略僅允許無線域使用者，請新增以下三個條件，然後按一下下一步:

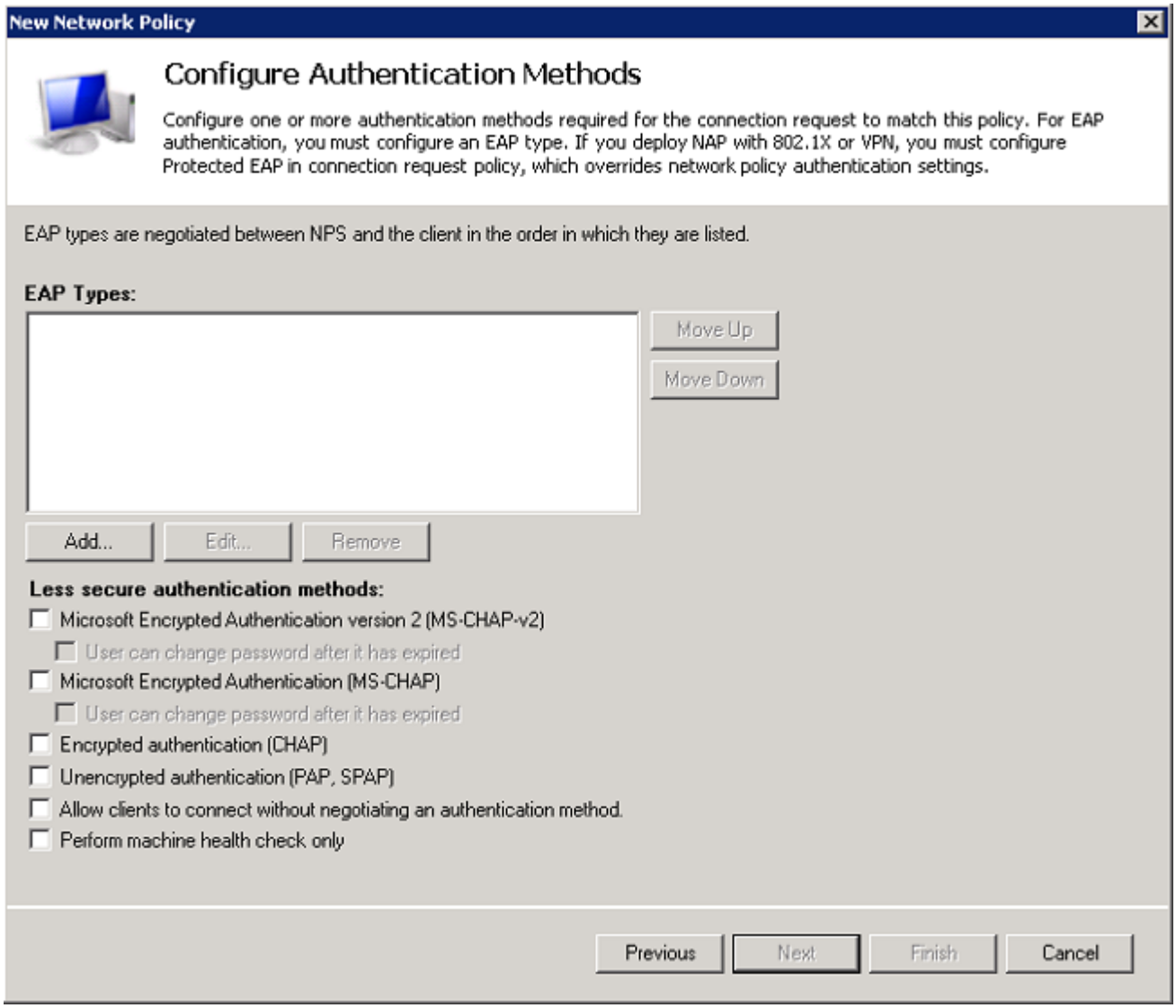
- Windows組 — 域使用者
- NAS埠型別 — 無線 — IEEE 802.11
- 身份驗證型別 — EAP



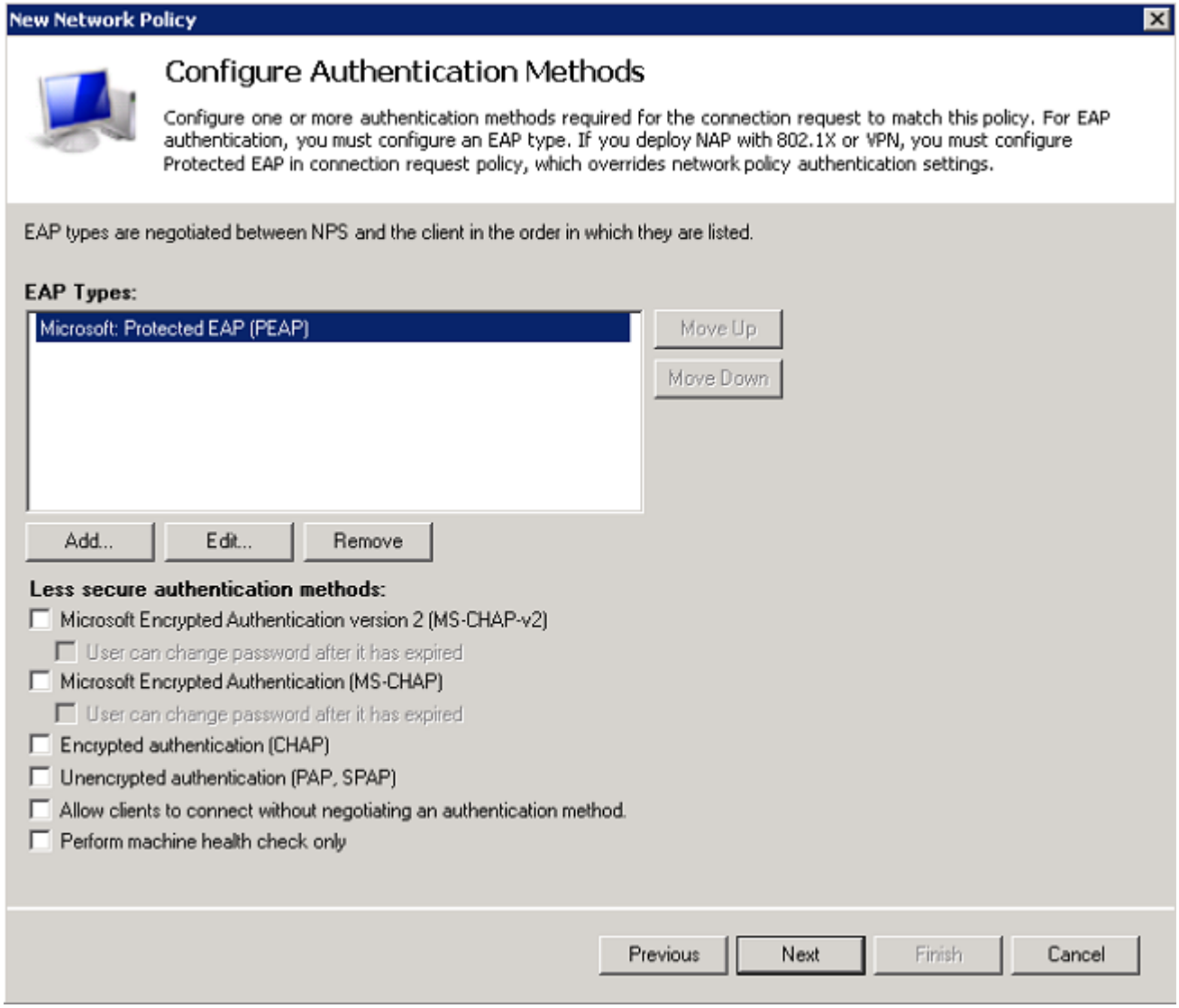
12. 按一下Access granted以授予與此策略匹配的連線嘗試，然後按一下Next。



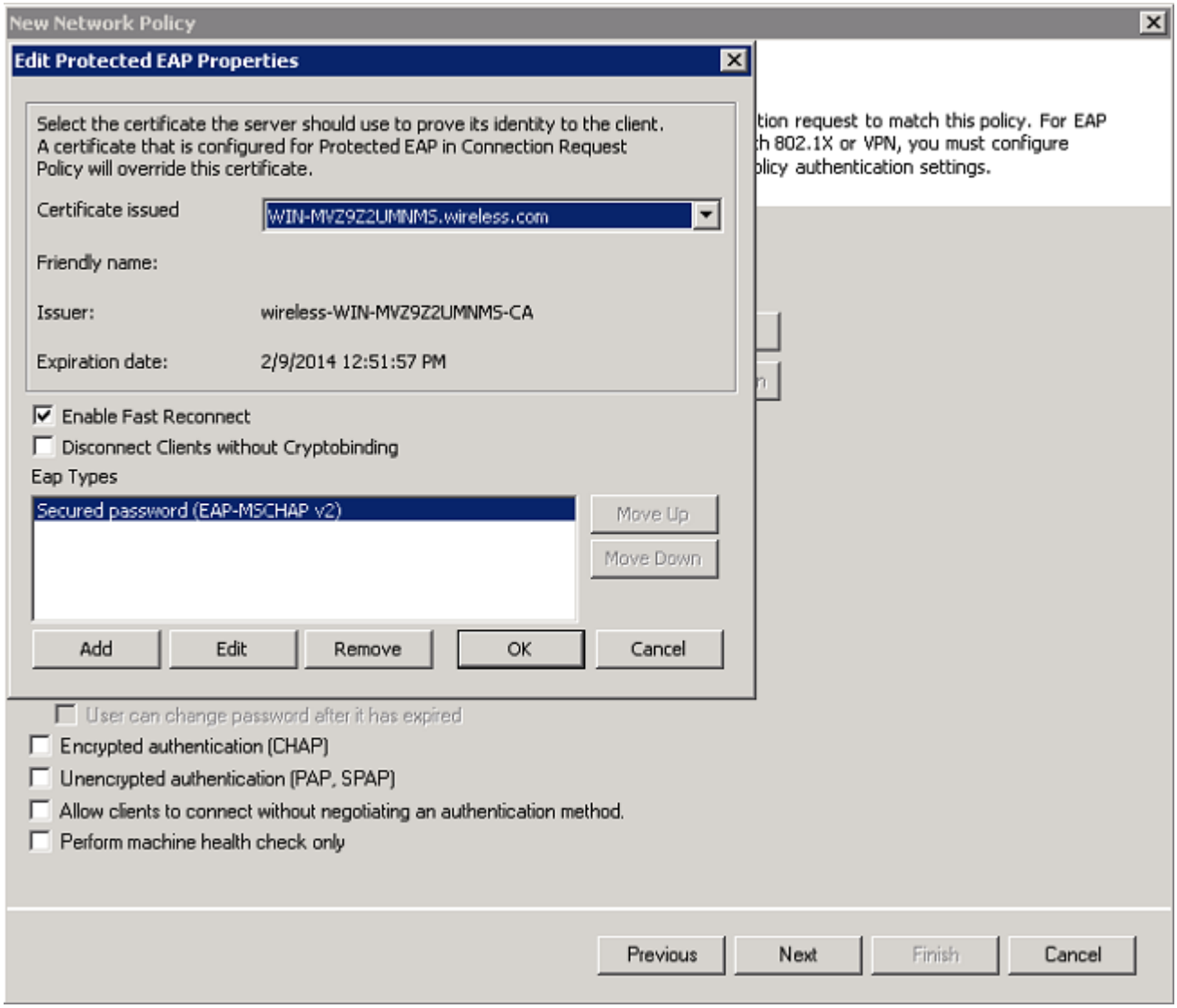
13. 在Less secure authentication methods下禁用所有身份驗證方法。



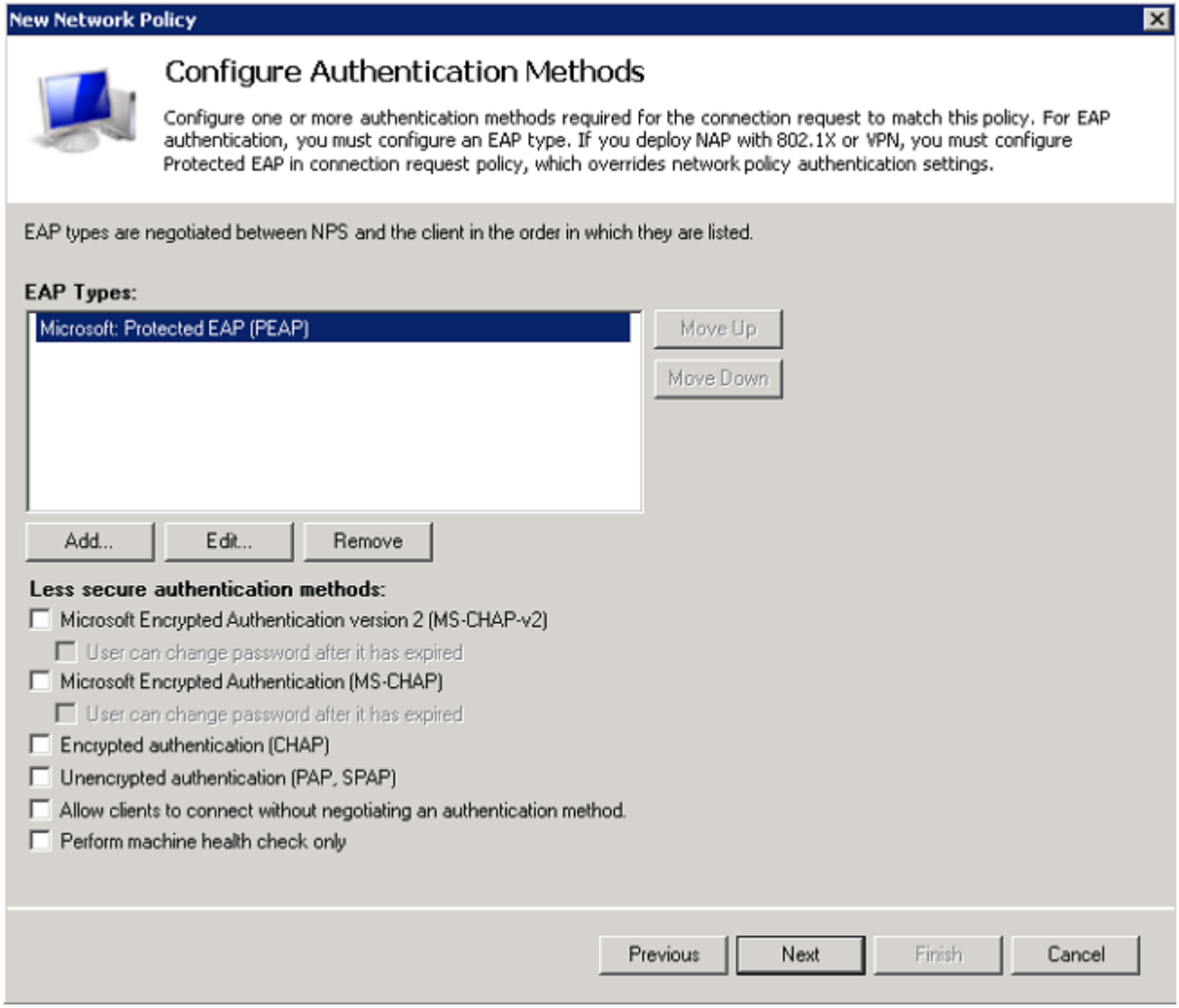
14. 按一下Add，選擇PEAP，然後按一下OK以啟用PEAP。



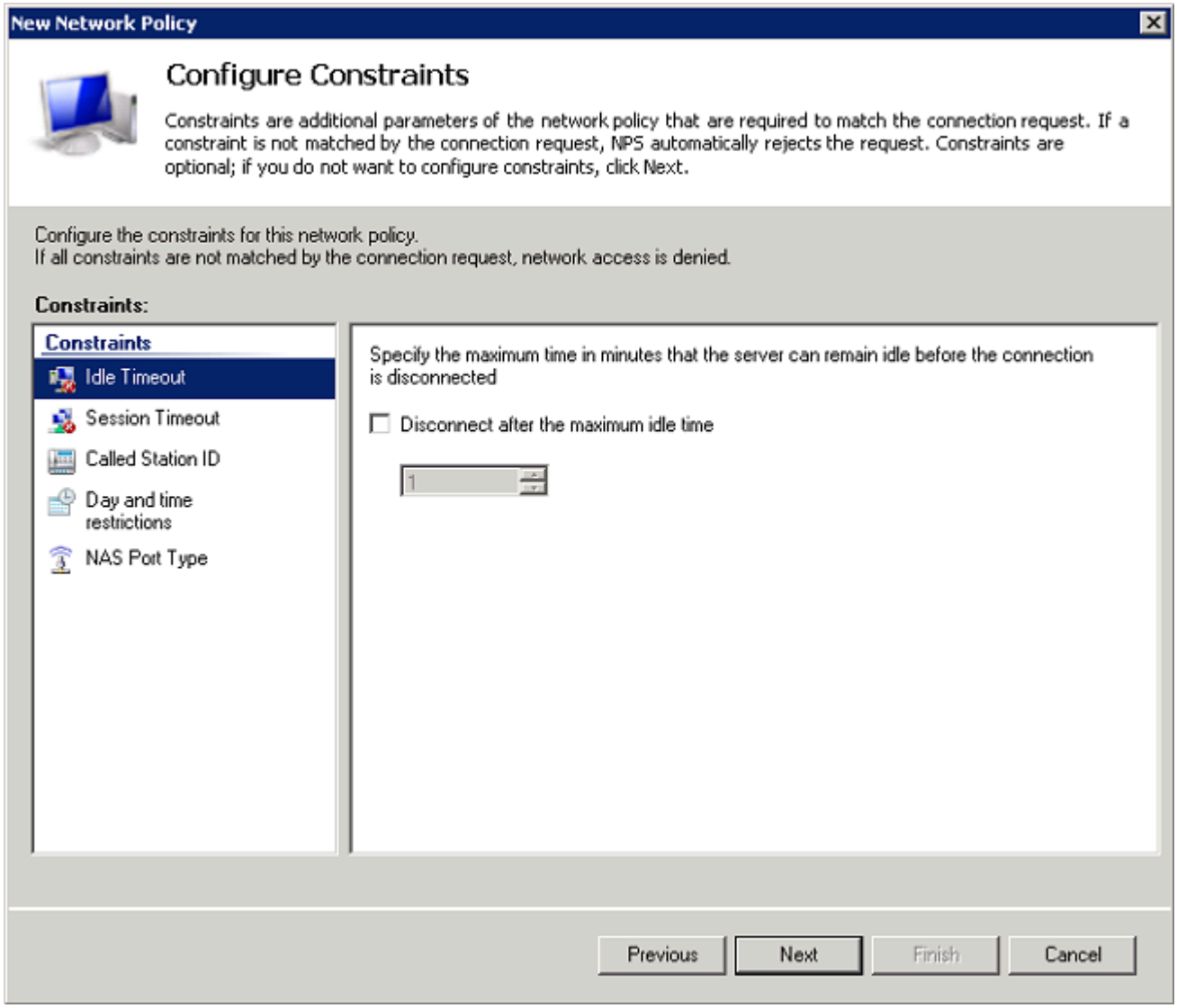
15. 選擇Microsoft:受保護的EAP(PEAP)，然後點選編輯。確保在Certificate issued下拉選單中選擇先前建立的域控制器證書，然後按一下OK。


New Network Policy
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
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)
Move Up
Move Down
Add
Edit
Remove
OK
Cancel
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
tion request to match this policy. For EAP
h 802.1X or VPN, you must configure
olicy authentication settings.
Previous
Next
Finish
Cancel

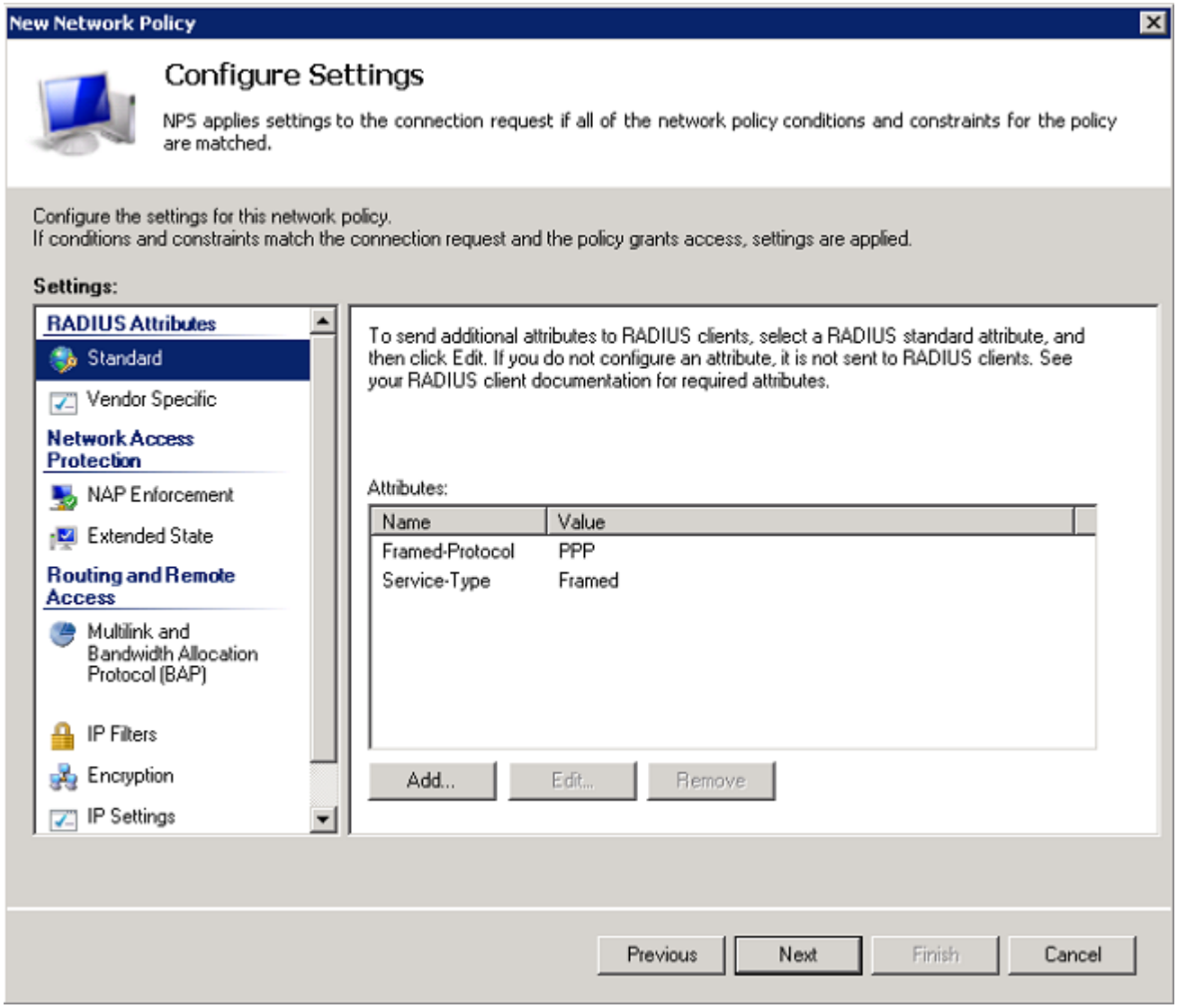
16. 按「Next」（下一步）。


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)
Move Up
Move Down
Add...
Edit...
Remove
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
Previous
Next
Finish
Cancel

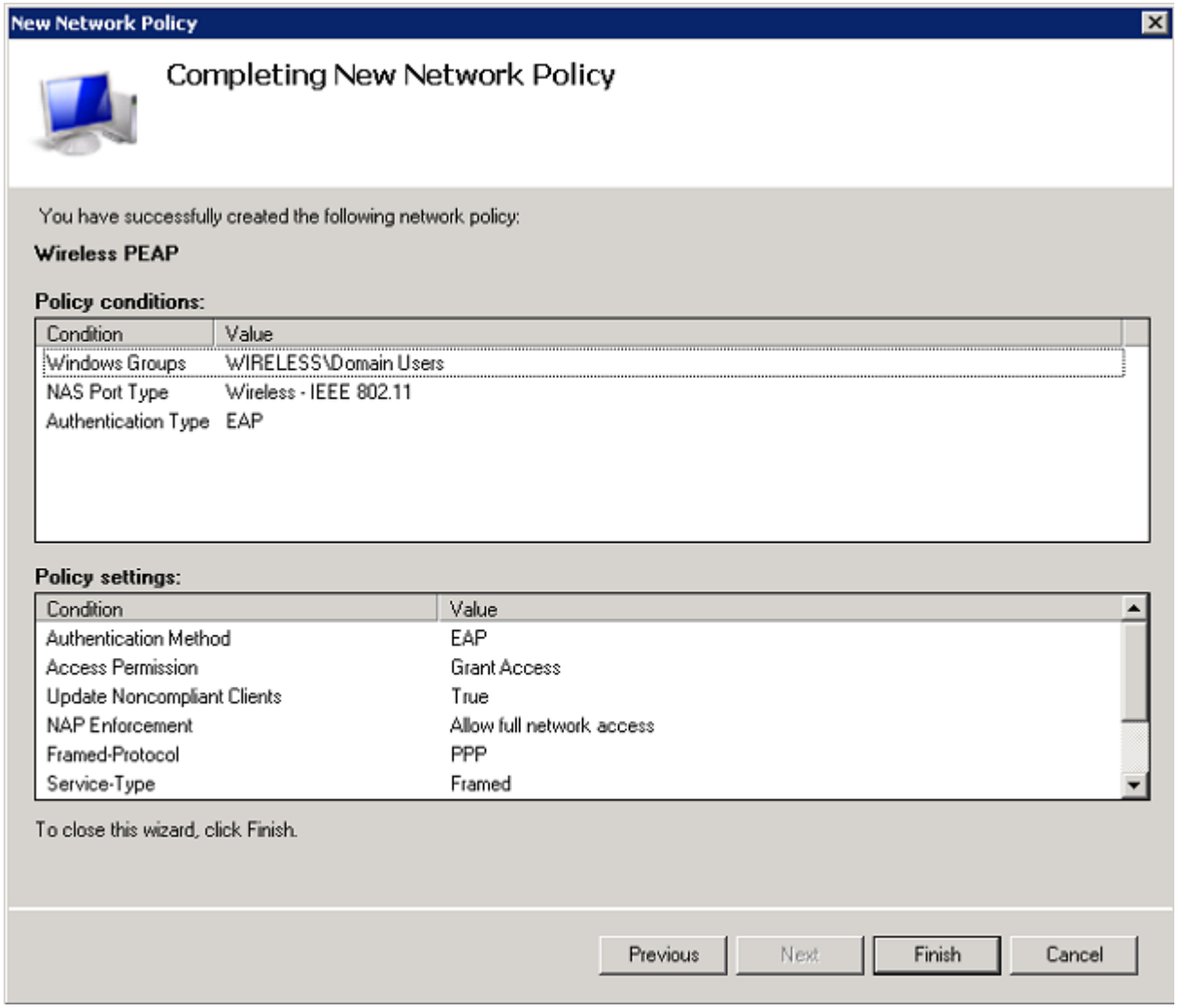
17. 按「Next」（下一步）。


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:
Constraints
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Specify the maximum time in minutes that the server can remain idle before the connection is disconnected
Disconnect after the maximum idle time
1
Previous
Next
Finish
Cancel

18. 按「Next」（下一步）。



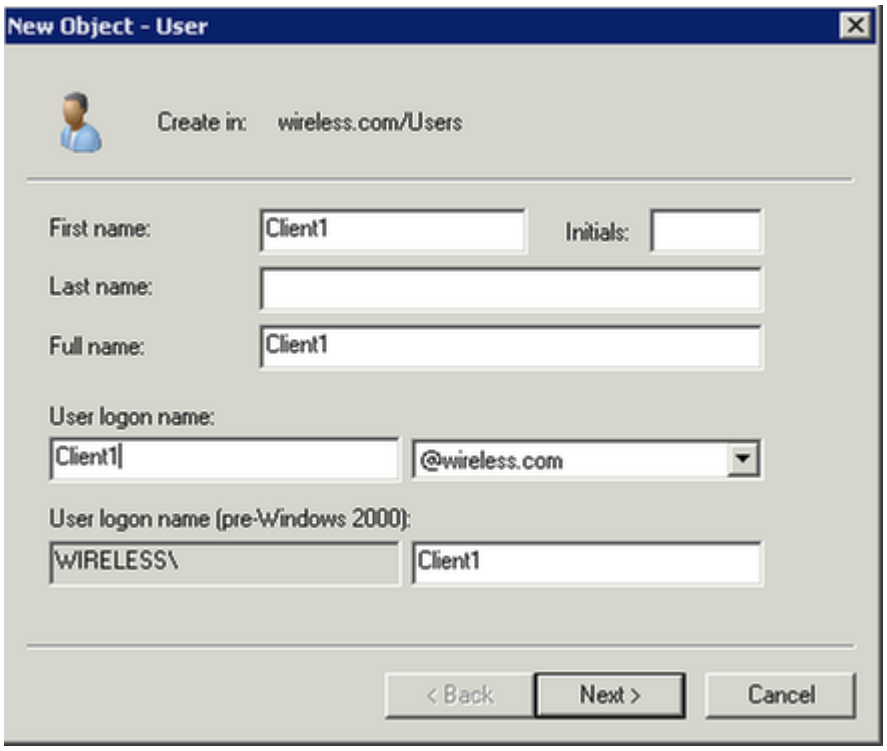
19. 按一下「Finish」（結束）。



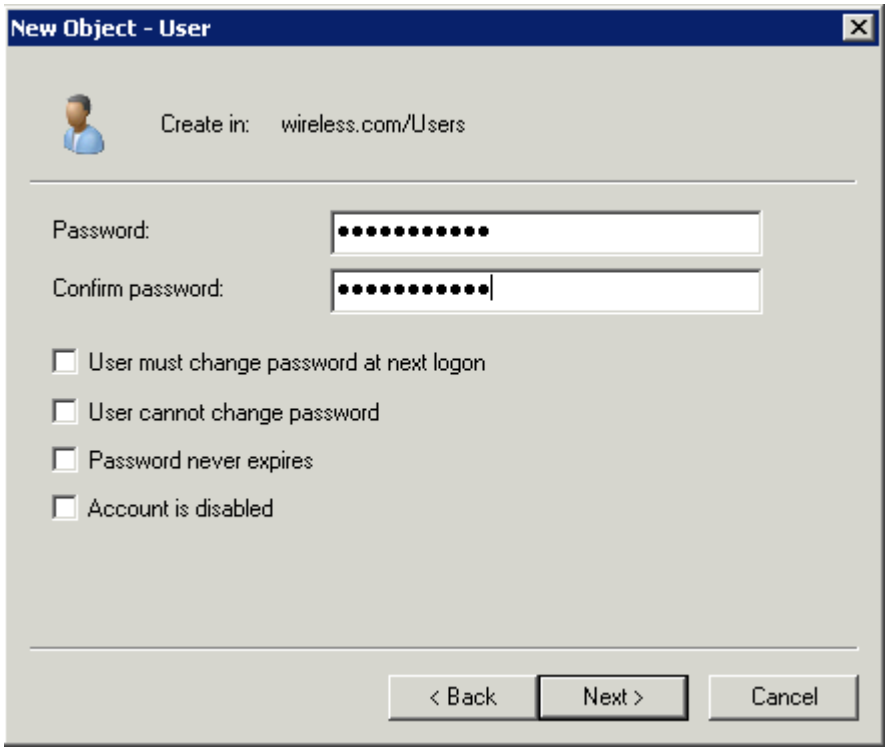
將使用者新增到Active Directory

在此示例中，使用者資料庫在Active Directory上維護。完成以下步驟以將使用者新增到Active Directory資料庫：

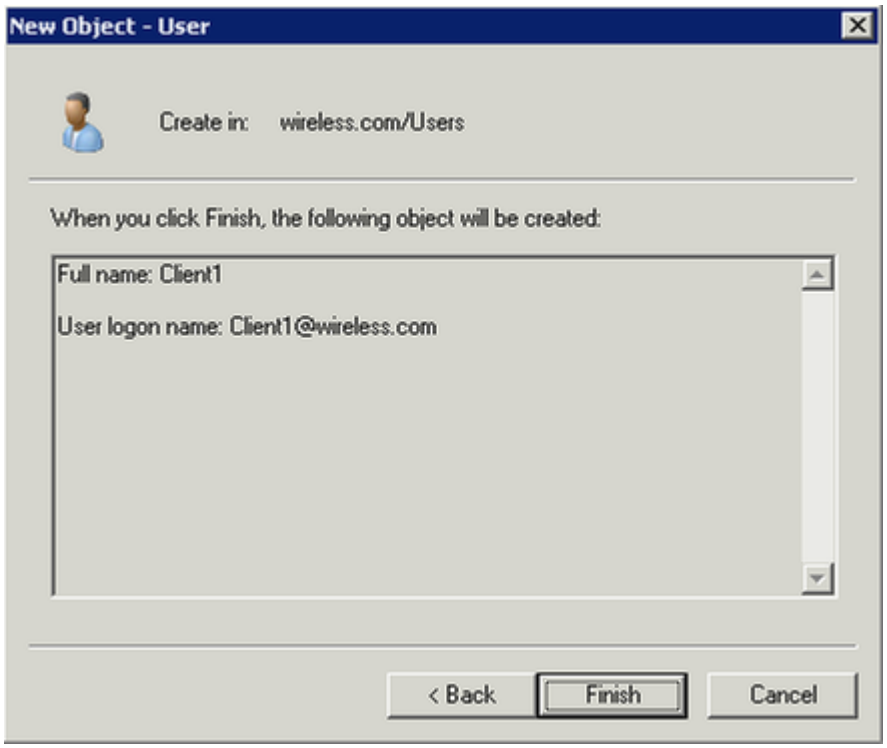
1. 開啟Active Directory使用者和電腦。按一下Start> Administrative Tools> Active Directory Users and Computers。
2. 在「Active Directory使用者和電腦」控制檯樹中，展開域，按一下右鍵Users> New，然後選擇User。
3. 在「新建對象 — 使用者」對話方塊中，輸入無線使用者的名稱。此示例在First name欄位中使用名稱Client1，在User logon name欄位中使用名稱Client1。按「Next」（下一步）。



4. 在New Object - User對話方塊中，在Password和Confirm password欄位中輸入您選擇的密碼。確保未選中User must change password at next logon 覈取方塊，然後按一下Next。



5. 在「新建對象 — 使用者」對話框中，按一下「完成」。



6. 重複步驟2至4以建立其他使用者帳戶。

配置無線區域網控制器和LAP

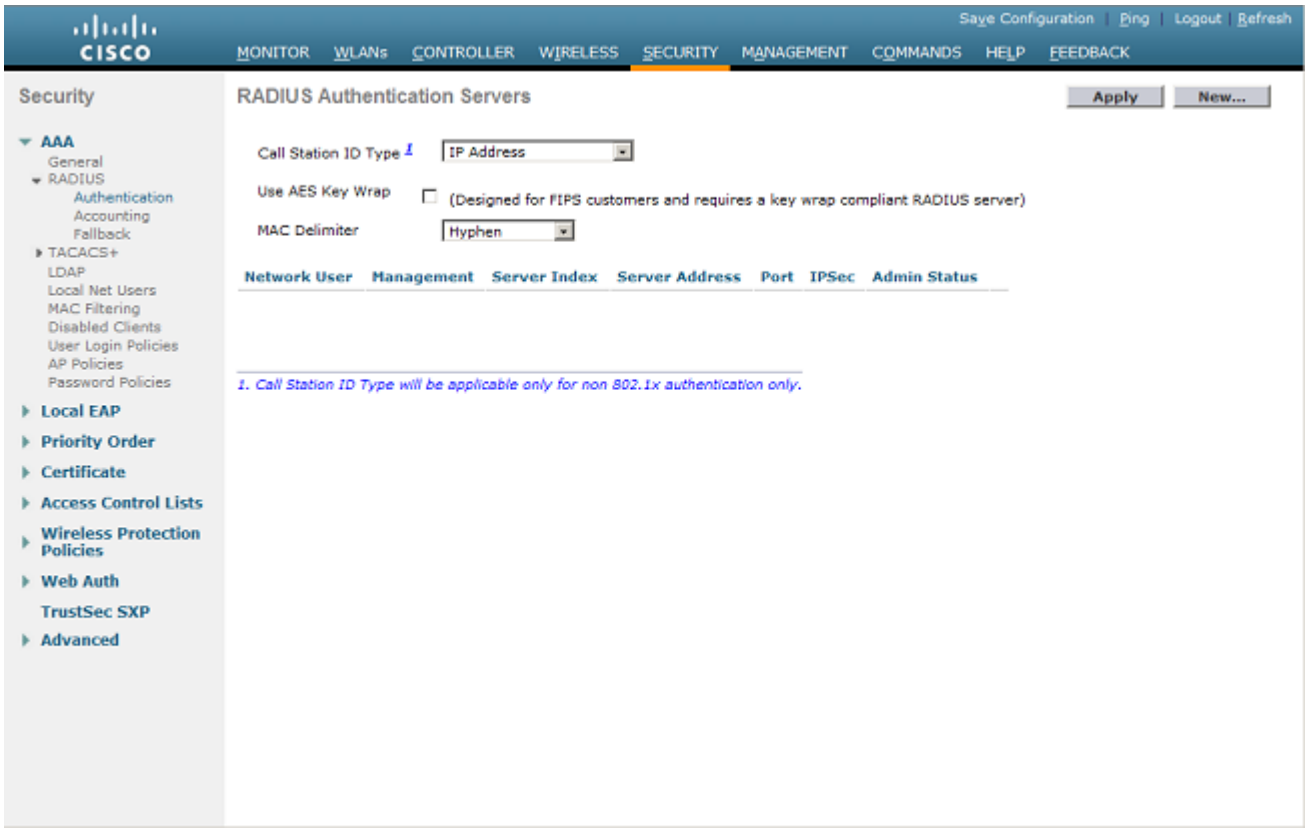
為此設定配置無線裝置（無線LAN控制器和LAP）。

設定WLC以進行RADIUS驗證

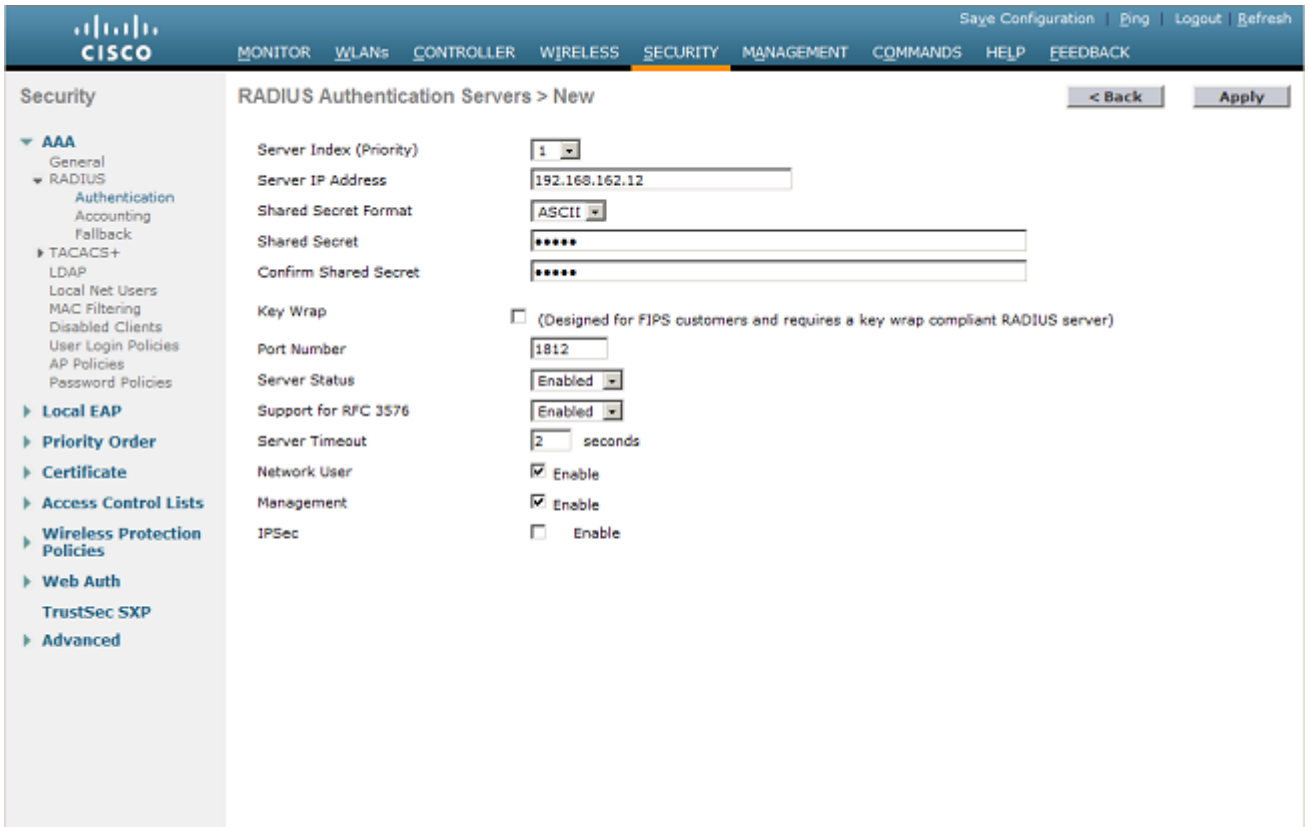
配置WLC以使用NPS作為身份驗證伺服器。必須配置WLC才能將使用者憑據轉發到外部RADIUS伺服器。外部RADIUS伺服器接著驗證使用者認證並提供對無線使用者端的存取許可權。

完成以下步驟，以便在Security > RADIUS Authentication頁面中將NPS新增為RADIUS伺服器：

1. 從控制器介面選擇「Security」>「RADIUS > Authentication」，以顯示「RADIUS Authentication Servers」頁面。按一下New以定義RADIUS伺服器。



2. 定義RADIUS伺服器引數。這些引數包括RADIUS伺服器IP地址、共用金鑰、埠號和伺服器狀態。Network User和Management覈取方塊確定基於RADIUS的身份驗證是否適用於管理和網路（無線）使用者。此示例使用NPS作為IP地址為192.168.162.12的RADIUS伺服器。按一下Apply。



為客戶端配置WLAN

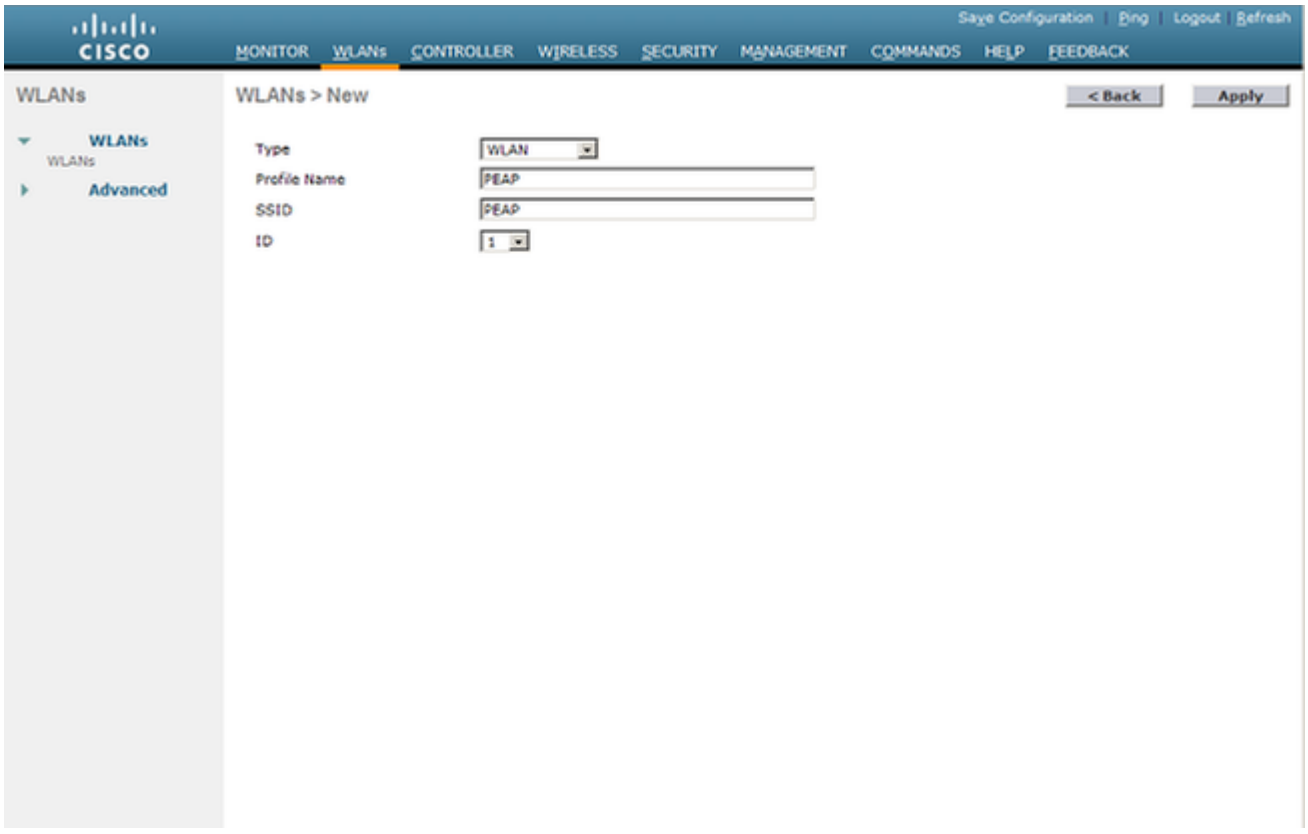
設定無線使用者端連線的服務組識別碼(SSID)(WLAN)。在本示例中，建立SSID並將其命名為PEAP。

將第2層身份驗證定義為WPA2，以便客戶端執行基於EAP的身份驗證（本示例中為PEAP-MS-CHAP v2），並使用高級加密標準(AES)作為加密機制。將所有其他值保留為預設值。

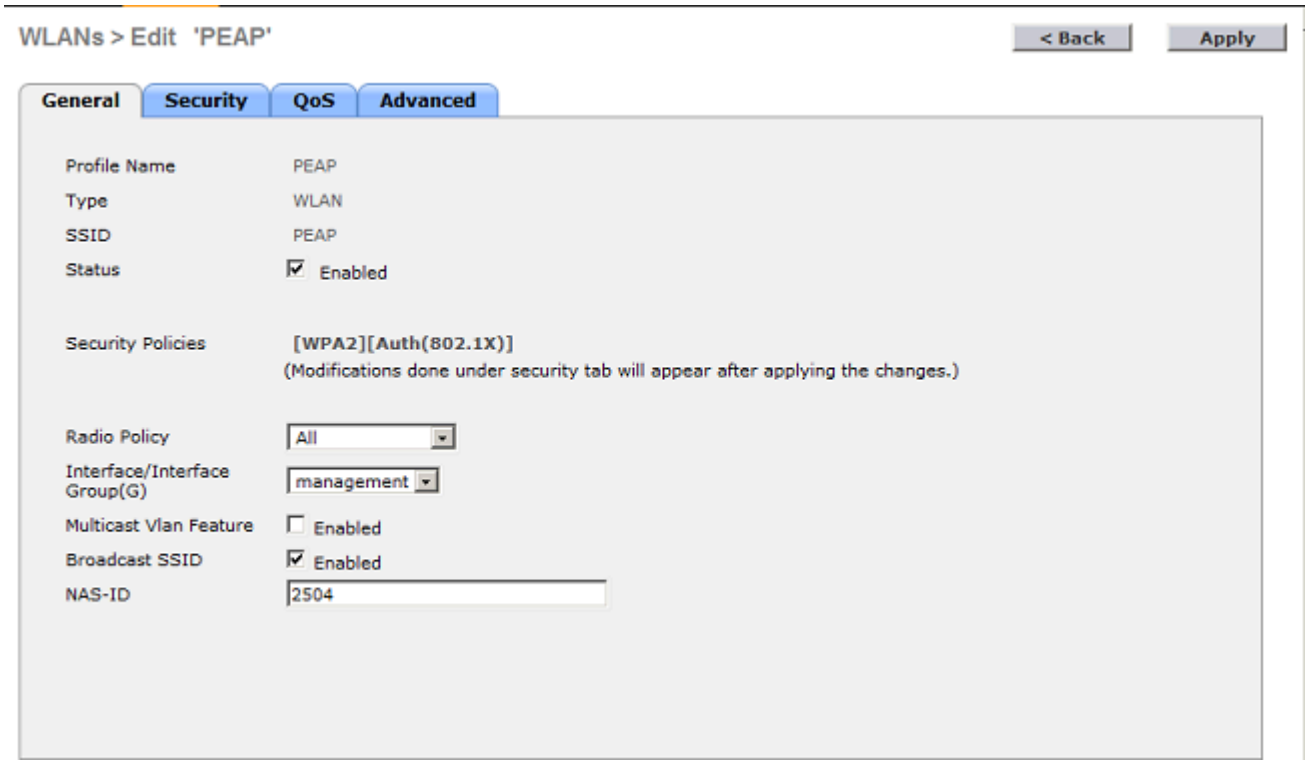
附註：本檔案會將WLAN與管理介面結合。當網路中有多個VLAN時，您可以建立一個單獨的VLAN並將其繫結到SSID。有關如何在WLC上設定VLAN的資訊，請參閱無線LAN控制器上的VLAN組態範例。

完成以下步驟，以便在WLC上設定WLAN:

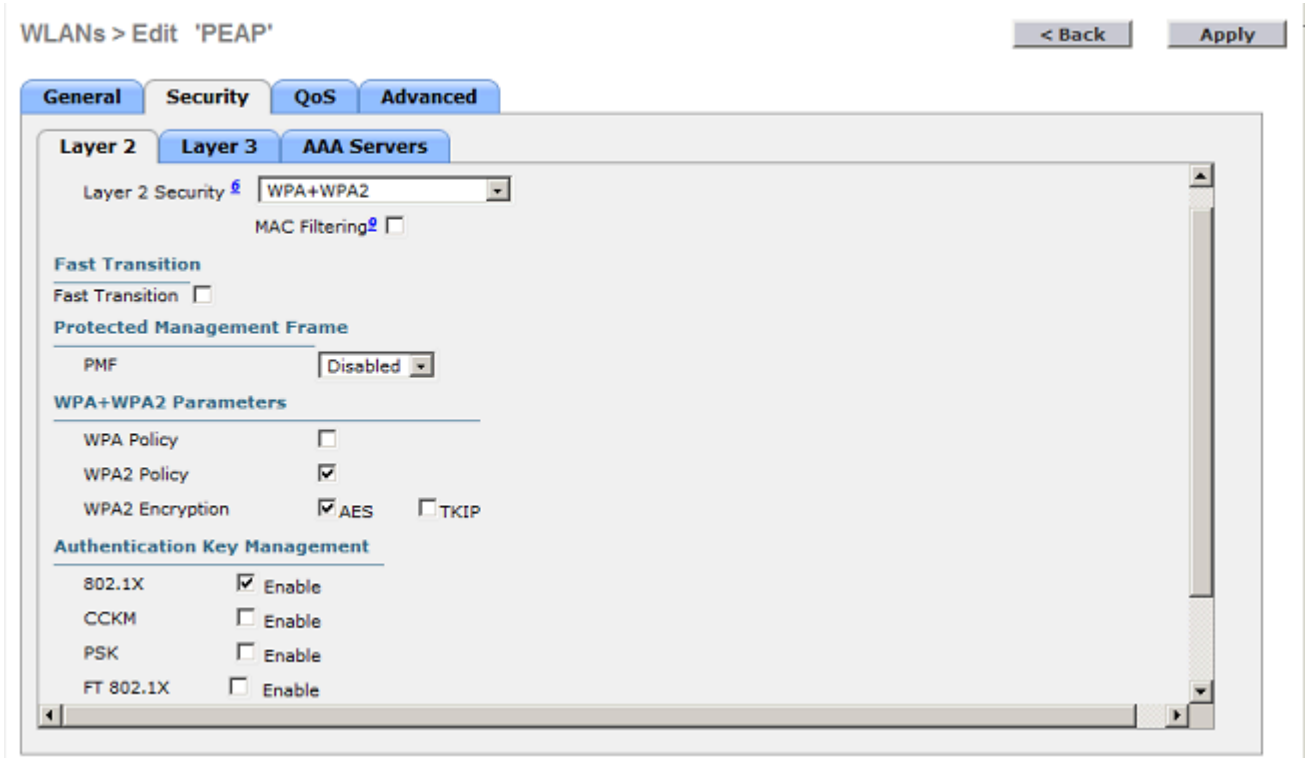
1. 從控制器介面按一下WLANs以顯示WLANs頁面。此頁面列出控制器上存在的WLAN。
2. 選擇New以建立一個新的WLAN。輸入WLAN的WLAN ID和WLAN SSID，然後按一下Apply。



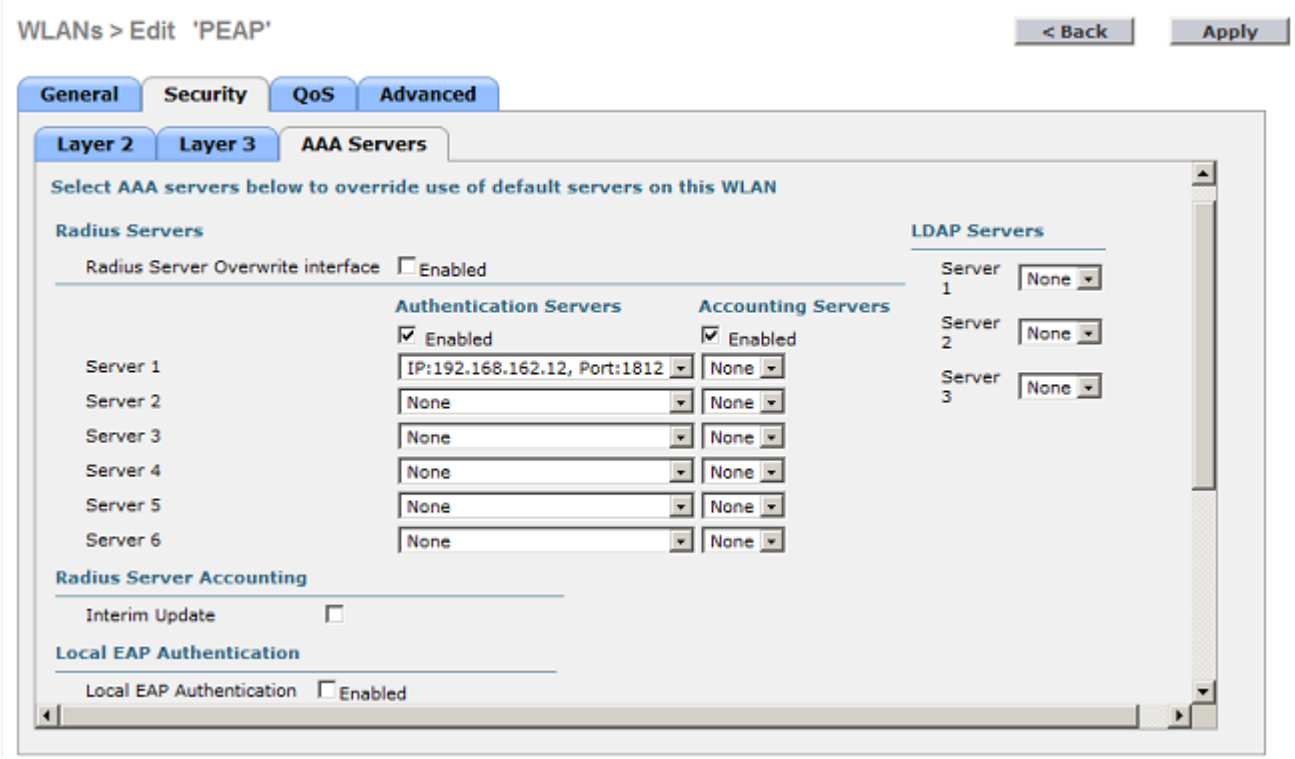
3. 要為802.1x配置SSID，請完成以下步驟：
    1. 按一下General頁籤並啟用WLAN。



2. 按一下Security > Layer 2頁籤，將Layer 2 security設定為WPA + WPA2，根據需要選中WPA+WPA2 Parameters（例如WPA2 AES）覈取方塊，然後按一下802.1x作為身份驗證金鑰管理。



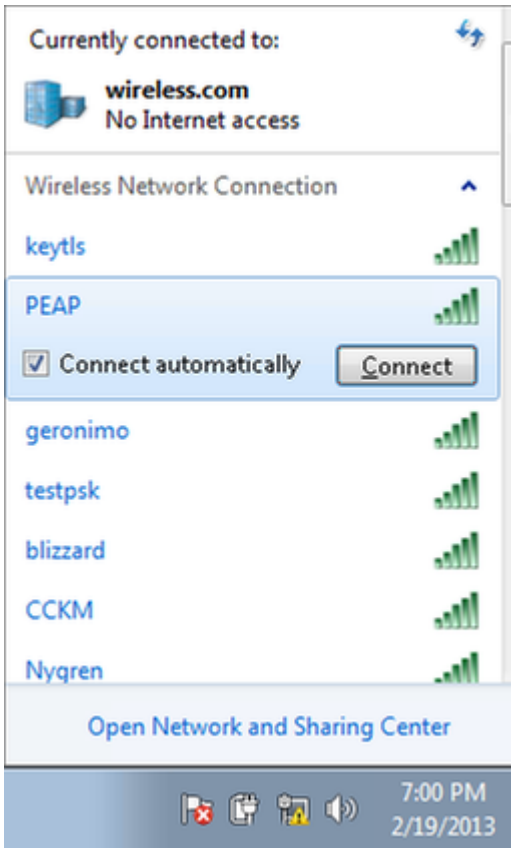
3. 按一下Security > AAA Servers頁籤，從Server 1下拉選單中選擇NPS的IP地址，然後按一下Apply。



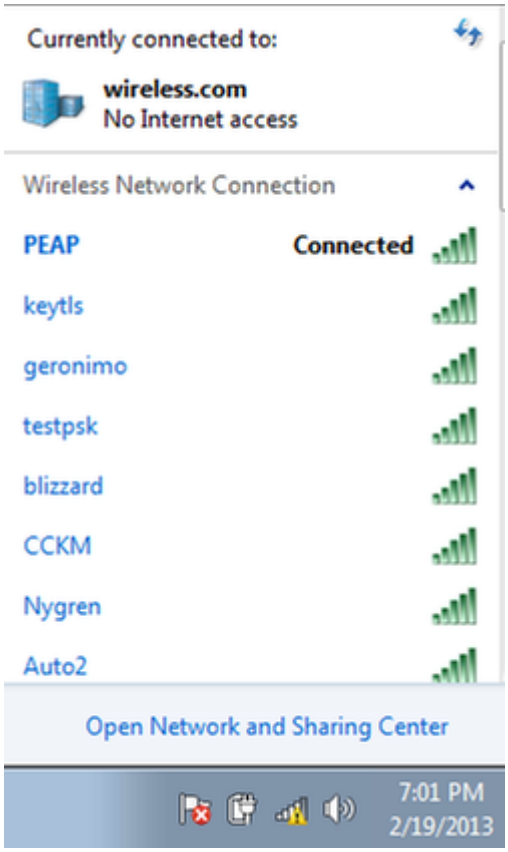
為PEAP-MS-CHAP v2身份驗證配置無線客戶端

完成以下步驟，使用Windows零配置工具配置無線客戶端以連線到PEAP WLAN。

1. 按一下工作列中的Network圖示。按一下PEAP SSID，然後按一下Connect。



2. 客戶端現在必須連線到網路。



3. 如果連線失敗，請嘗試重新連線到WLAN。如果問題仍然存在，請參閱故障排除部分。

驗證

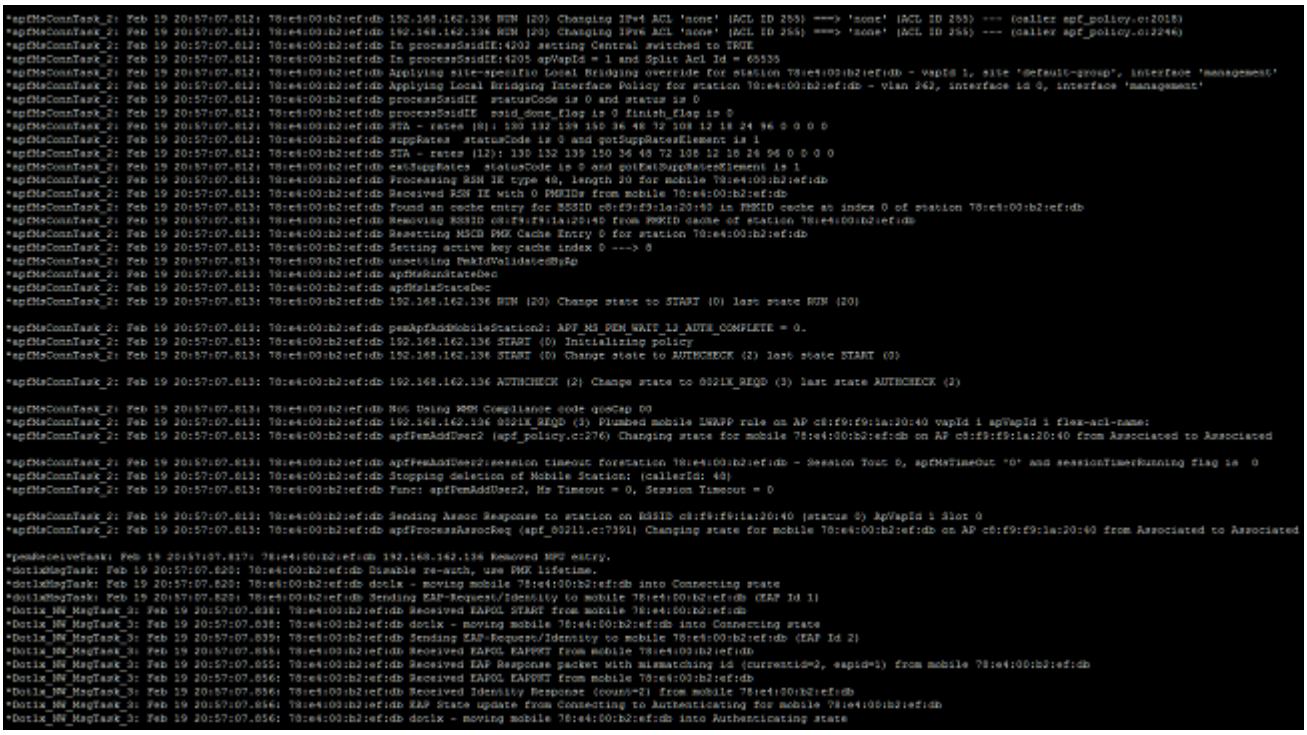
目前沒有適用於此組態的驗證程序。

疑難排解

如果您的使用者端沒有連線到WLAN，本節提供的資訊可用於對組態進行疑難排解。

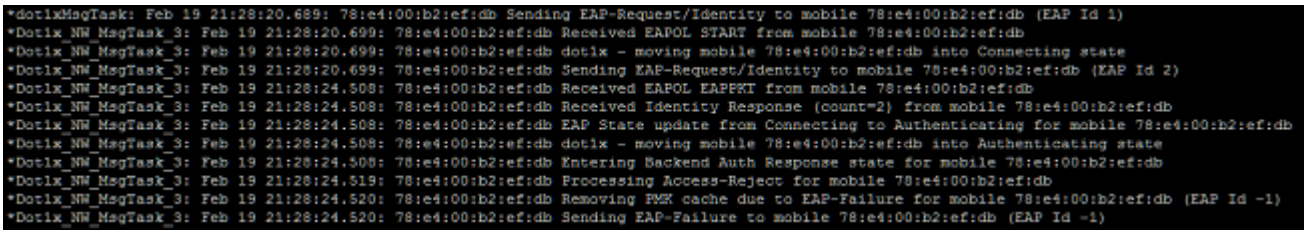
有兩個工具可用於診斷802.1x身份驗證故障：Windows中的debug client命令和Event Viewer。

如果從WLC執行使用者端偵錯，則會佔用大量資源，而且不會影響服務。若要啟動偵錯作業階段，請開啟WLC的指令行介面(CLI)，並輸入debug client mac address，其中mac位址是無法連線的無線使用者端的無線mac位址。運行此調試時，請嘗試連線客戶端；wlc的CLI上必須存在類似以下範例的輸出：



以下是組態錯誤時可能會發生的問題的範例。此處，WLC偵錯顯示WLC已進入驗證狀態，這表示WLC等待來自NPS的回應。這通常是由於WLC或NPS上的共用密碼不正確所致。您可通過Windows伺服器事件檢視器確認此操作。如果您找不到日誌，則請求從未傳送到NPS。

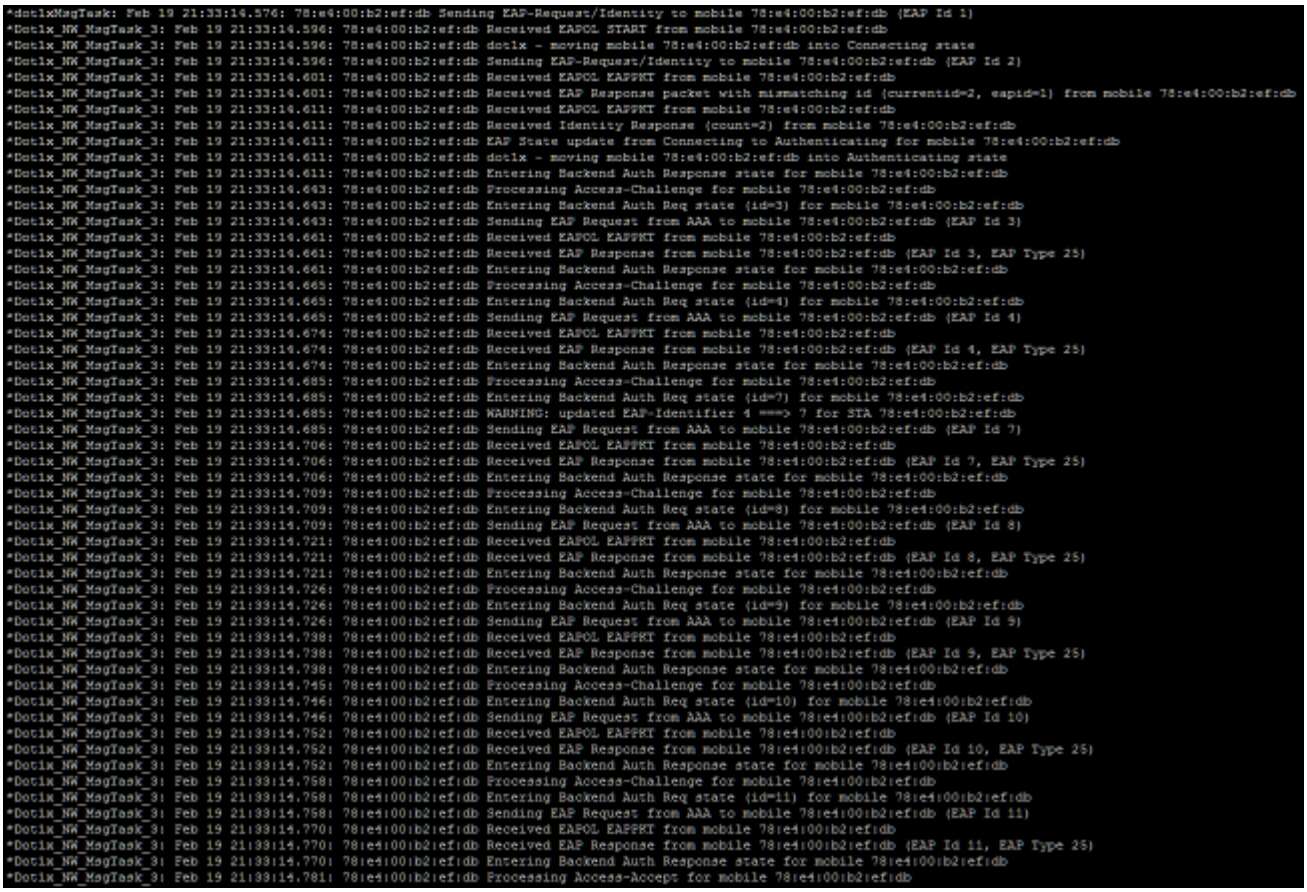
從WLC偵錯找到的另一個範例是access-reject。Access-reject顯示NPS接收並拒絕客戶端憑證。以下是接收存取拒絕的使用者端範例：



```
*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)
```

當您看到訪問拒絕時，請檢查Windows Server事件日誌中的日誌，以確定NPS使用訪問拒絕響應客戶端的原因。

成功的身份驗證在客戶端調試中具有access-accept，如以下示例所示：

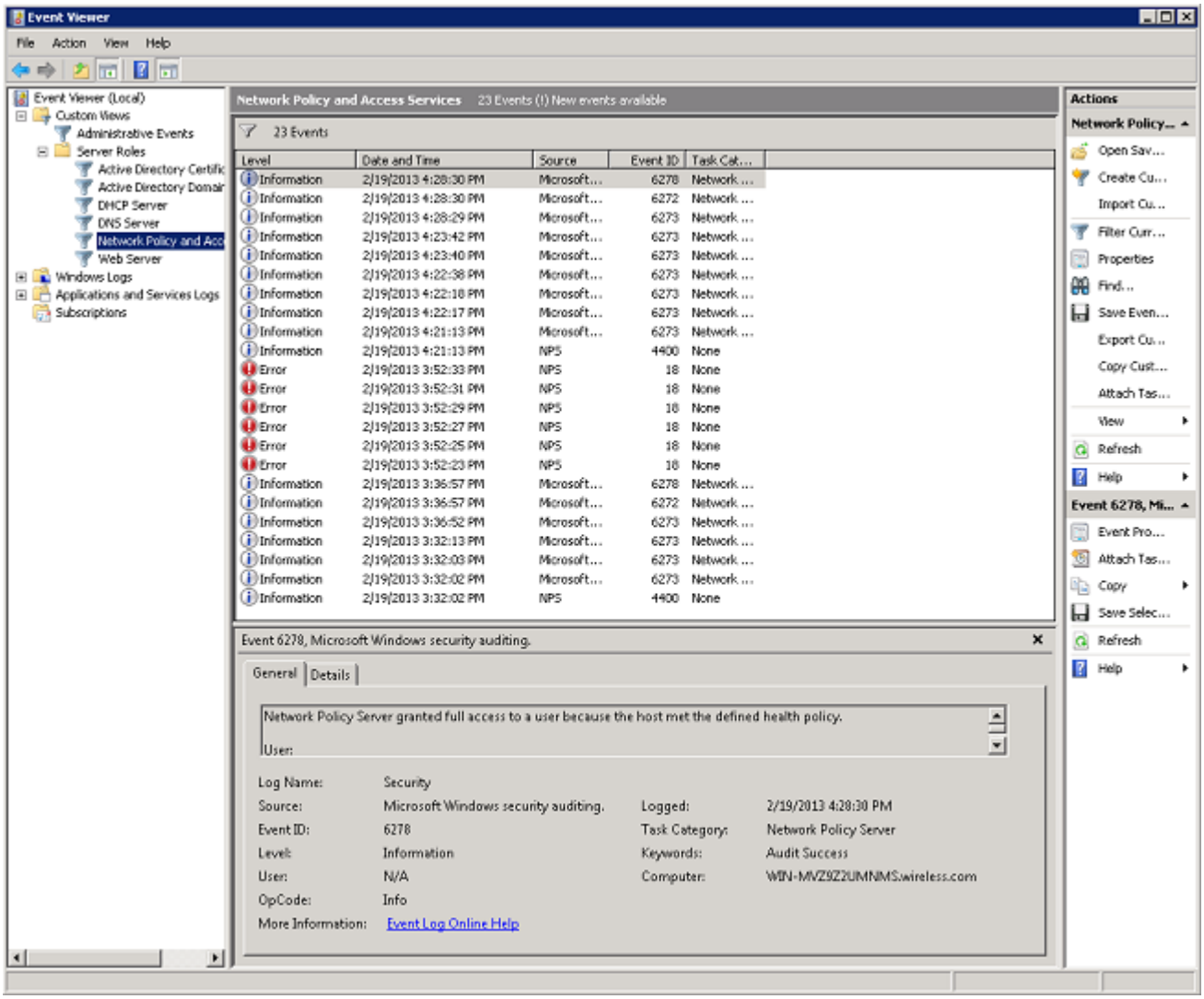


如果要排解存取拒絕和回應逾時的疑難問題，則需要存取RADIUS伺服器。WLC充當在客戶端和RADIUS伺服器之間傳遞EAP消息的驗證器。RADIUS服務的製造商必須檢查並診斷以訪問拒絕或響應超時響應的RADIUS伺服器。

附註：TAC不為第三方RADIUS伺服器提供技術支援；但是，RADIUS伺服器上的日誌通常解釋客戶端請求被拒絕或忽略的原因。

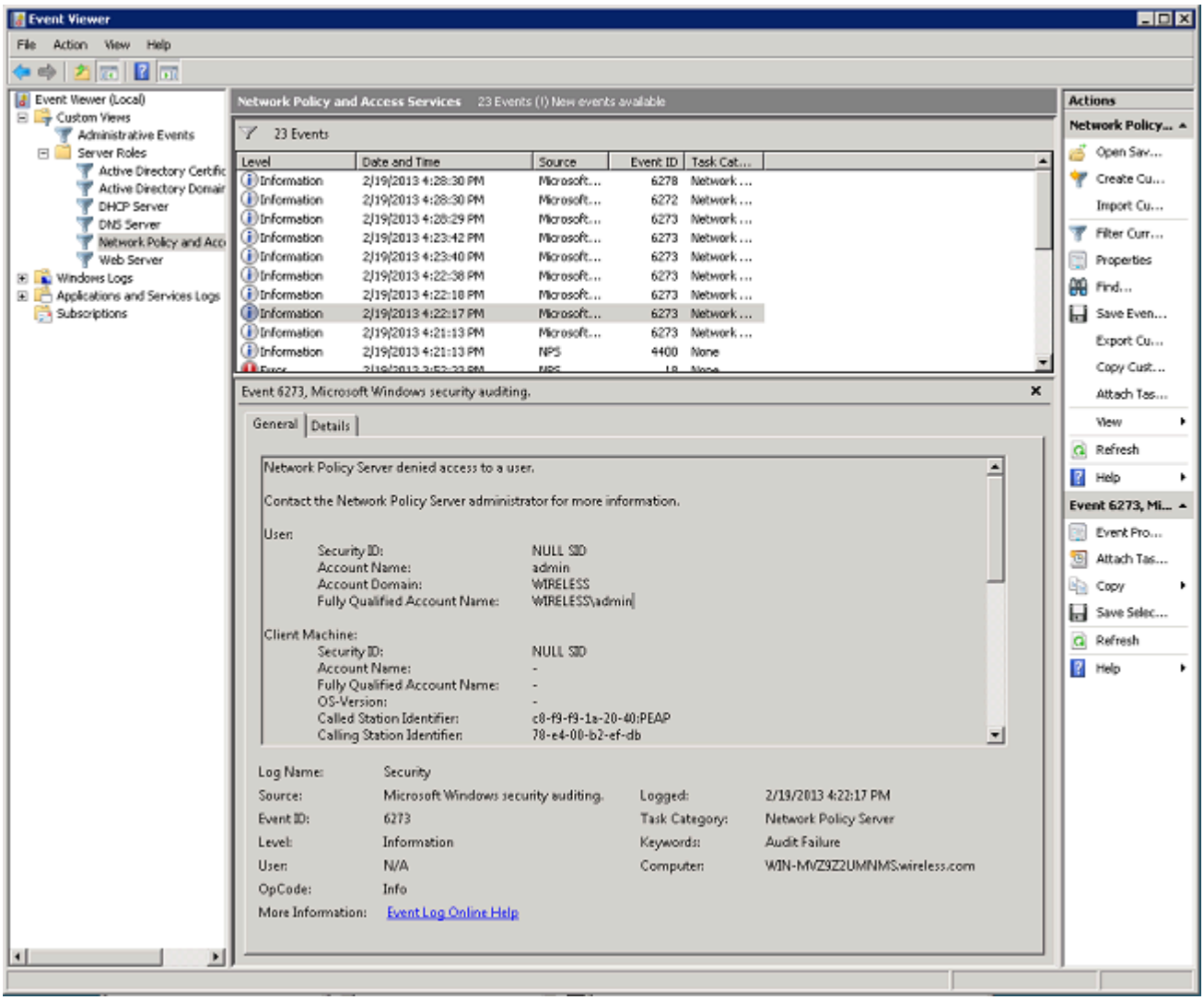
為了對來自NPS的訪問拒絕和響應超時進行故障排除，請檢查伺服器上的Windows事件檢視器中的NPS日誌。

1. 按一下開始>管理員工具>事件檢視器以啟動事件檢視器並檢視NPS日誌。
2. 展開Custom Views > Server Roles > Network Policy and Access。

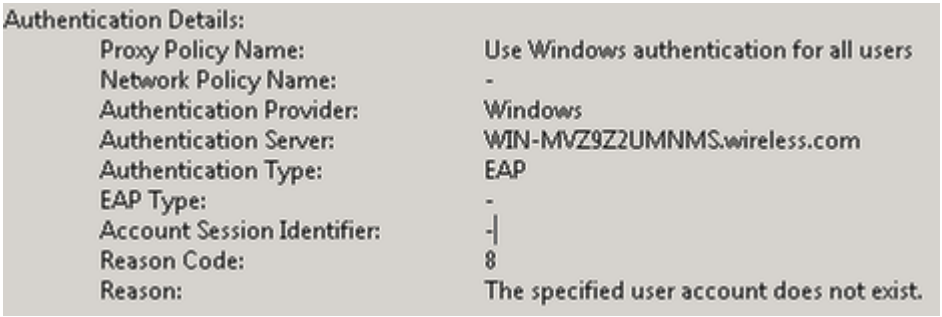


在「事件檢視」的此部分中，有已通過和失敗的身份驗證的日誌。檢查這些日誌，對客戶端未通過身份驗證的原因進行故障排除。傳遞的身份驗證和失敗的身份驗證均顯示為「資訊」。滾動瀏覽日誌，查詢身份驗證失敗且收到基於WLC調試的訪問拒絕的使用者名稱。

以下是NPS拒絕使用者訪問時的示例：

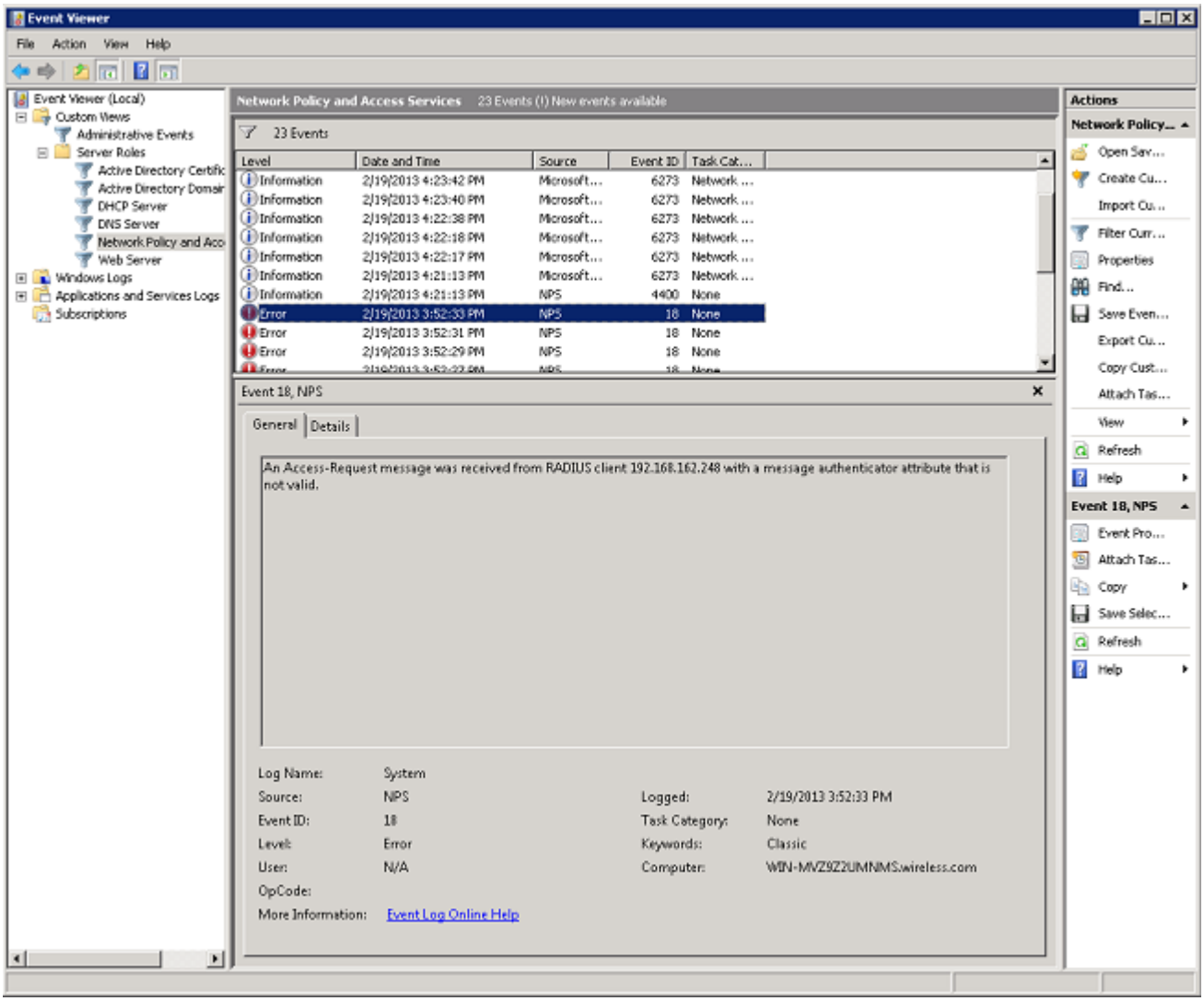


當您在事件檢視器中檢視deny語句時，請檢查Authentication Details部分。在此示例中，您可以看到NPS因為使用者名稱不正確而拒絕使用者訪問：



如果WLC沒有收到來自NPS的響應，則NPS上的事件檢視也有助於您進行故障排除。 這通常是由於NPS和WLC之間的共用金鑰不正確造成的。

在本例中，NPS由於共用金鑰不正確而丟棄來自WLC的請求：



相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。