

# Configurazione di NPS, dispositivi Wireless LAN Controller e reti wireless

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Panoramica di PEAP](#)

[PEAP fase 1: Canale crittografato TLS](#)

[PEAP fase 2: Comunicazione autenticata EAP](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione di Microsoft Windows 2008 Server](#)

[Configurare il server Microsoft Windows 2008 come controller di dominio](#)

[Installare e configurare i servizi DHCP in Microsoft Windows 2008 Server](#)

[Installazione e configurazione di Microsoft Windows 2008 Server come server CA](#)

[Connetti client al dominio](#)

[Installare Server dei criteri di rete in Microsoft Windows 2008 Server](#)

[Installa un certificato](#)

[Configurare il servizio Server dei criteri di rete per l'autenticazione PEAP-MS-CHAP v2](#)

[Aggiungi utenti ad Active Directory](#)

[Configurazione del controller LAN wireless e dei LAP](#)

[Configurazione del WLC per l'autenticazione RADIUS](#)

[Configurazione di una WLAN per i client](#)

[Configurazione dei client wireless per l'autenticazione PEAP-MS-CHAP v2](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come configurare il protocollo PEAP con autenticazione MS-CHAP con Microsoft NPS come server RADIUS.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza dell'installazione di base di Windows 2008
- Conoscenza dell'installazione del controller Cisco

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti requisiti:

- Installare Microsoft Windows Server 2008 in ogni server del laboratorio di prova.
- Aggiorna tutti i Service Pack.
- Installare i controller e i Lightweight Access Point (LAP).
- Configurare gli aggiornamenti software più recenti.

Per informazioni sull'installazione iniziale e sulla configurazione dei Cisco Wireless Controller serie 5508, fare riferimento alla [Guida all'installazione di Cisco Wireless Controller serie 5500](#).



Nota: Questo documento ha lo scopo di fornire ai lettori un esempio della configurazione richiesta su un server Microsoft per l'autenticazione PEAP-MS-CHAP. La configurazione del server Microsoft Windows illustrata in questo documento è stata testata in laboratorio e ha funzionato come previsto. In caso di problemi con la configurazione, contattare Microsoft per assistenza. Il Cisco Technical Assistance Center (TAC) non supporta la configurazione del server Microsoft Windows.

Le guide all'installazione e alla configurazione di Microsoft Windows 2008 sono disponibili in Microsoft Tech Net.

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 5508 Wireless Controller con firmware versione 7.4
- Cisco Aironet 3602 Access Point (AP) con Lightweight Access Point Protocol (LWAPP)
- Windows 2008 Enterprise Server con Server dei criteri di rete, Autorità di certificazione (CA), DHCP (Dynamic Host Control Protocol) e DNS (Domain Name System) installati
- PC client Microsoft Windows 7
- Cisco Catalyst serie 3560 Switch

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

# Premesse

In questo documento viene fornita una configurazione di esempio per l'autenticazione PEAP (Protected Extensible Authentication Protocol) con MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) versione 2 in una rete wireless unificata Cisco con Server dei criteri di rete Microsoft come server RADIUS.

## Panoramica di PEAP

PEAP utilizza TLS (Transport Level Security) per creare un canale crittografato tra un client PEAP autenticato, ad esempio un laptop wireless, e un autenticatore PEAP, ad esempio Server dei criteri di rete Microsoft o qualsiasi server RADIUS. PEAP non specifica un metodo di autenticazione, ma fornisce una protezione aggiuntiva per altri protocolli di autenticazione estensibili (EAP), ad esempio EAP-MS-CHAP v2, che possono funzionare tramite il canale crittografato TLS fornito da PEAP. Il processo di autenticazione PEAP è costituito da due fasi principali.

### PEAP fase 1: Canale crittografato TLS

Il client wireless viene associato all'access point. Un'associazione basata su IEEE 802.11 fornisce un'autenticazione a sistema aperto o a chiave condivisa prima che venga creata un'associazione sicura tra il client e il punto di accesso. Dopo aver stabilito l'associazione basata su IEEE 802.11 tra il client e il punto di accesso, la sessione TLS viene negoziata con l'access point. Al termine dell'autenticazione tra il client wireless e Server dei criteri di rete, la sessione TLS viene negoziata tra il client e Server dei criteri di rete. La chiave derivata in questa negoziazione viene utilizzata per crittografare tutte le comunicazioni successive.

### PEAP fase 2: Comunicazione autenticata EAP

La comunicazione EAP, che include la negoziazione EAP, avviene all'interno del canale TLS creato da PEAP nella prima fase del processo di autenticazione PEAP. Il Server dei criteri di rete autentica il client wireless con EAP-MS-CHAP v2. Il LAP e il controller inoltrano messaggi solo tra il client wireless e il server RADIUS. Il controller WLC (Wireless LAN Controller) e il LAP non possono decrittografare questi messaggi perché non è l'endpoint TLS.

La sequenza di messaggi RADIUS per un tentativo di autenticazione riuscito (in cui l'utente ha fornito credenziali valide basate su password con PEAP-MS-CHAP v2) è:

1. Server dei criteri di rete invia un messaggio di richiesta di identità al client: EAP-Request/Identity.
2. Il client risponde con un messaggio di risposta di identità: EAP-Risposta/Identità.
3. Server dei criteri di rete invia un messaggio di verifica MS-CHAP v2: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (verifica).
4. Il client risponde con una richiesta di verifica e una risposta MS-CHAP v2: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Risposta).
5. Il Server dei criteri di rete restituisce un pacchetto MS-CHAP v2 che ha avuto esito positivo

quando il server ha autenticato correttamente il client: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (riuscito).

6. Il client risponde con un pacchetto MS-CHAP v2 che ha avuto esito positivo quando il client ha autenticato correttamente il server: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (riuscito).
7. Server dei criteri di rete invia un valore TLV (Type-Length-Value) di tipo EAP per indicare che l'autenticazione è stata eseguita correttamente.
8. Il client risponde con un messaggio di stato EAP-TLV riuscito.
9. Il server completa l'autenticazione e invia un messaggio di completamento EAP in testo normale. Se le VLAN vengono distribuite per l'isolamento del client, gli attributi VLAN sono inclusi in questo messaggio.

## Configurazione

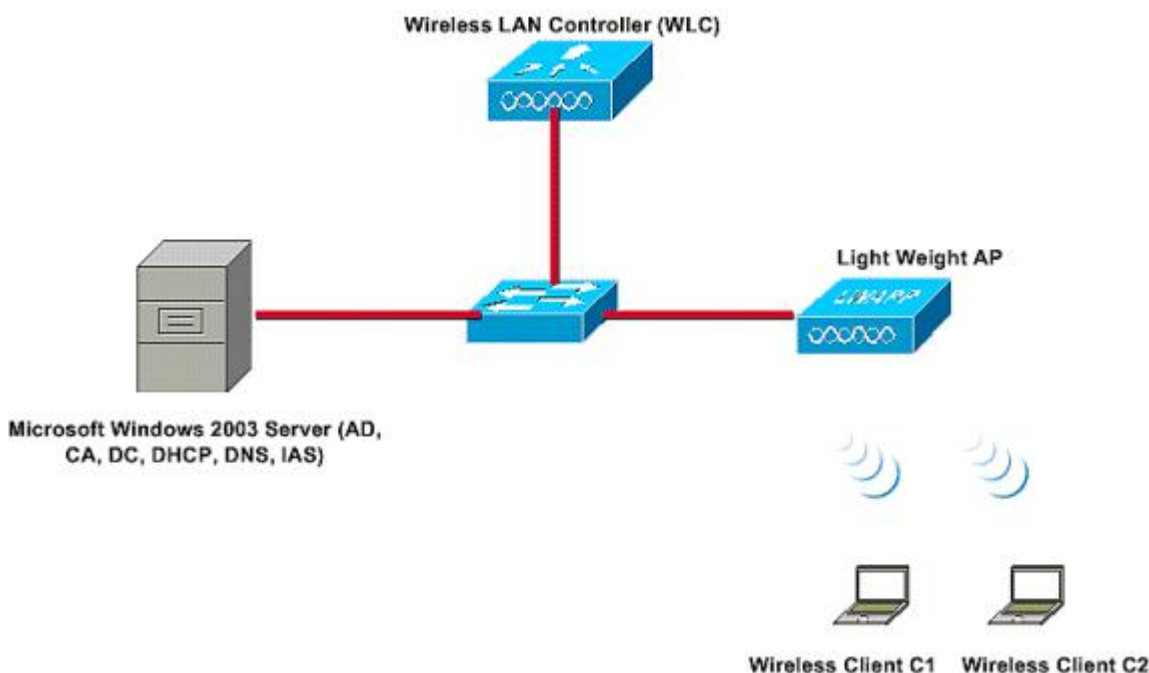
In questa sezione vengono presentate le informazioni necessarie per configurare PEAP-MS-CHAP v2.



Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi. Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interne di Cisco.

## Esempio di rete

Questa configurazione utilizza la seguente configurazione di rete:



In questa configurazione, un server Microsoft Windows 2008 svolge i seguenti ruoli:

- Controller di dominio del dominio
- Server DHCP/DNS
- server CA
- Server dei criteri di rete - per autenticare gli utenti wireless
- Active Directory - per gestire il database utenti

Il server si connette alla rete cablata tramite uno switch di layer 2, come mostrato. Il WLC e il LAP registrato si connettono alla rete anche tramite lo switch di layer 2.

I client wireless utilizzano l'autenticazione Wi-Fi Protected Access 2 (WPA2) - PEAP-MS-CHAP v2 per connettersi alla rete wireless.

## Configurazioni

L'obiettivo di questo esempio è configurare il server Microsoft 2008, il controller LAN wireless e il punto di accesso Light Weight per autenticare i client wireless con l'autenticazione PEAP-MS-CHAP v2. Questo processo prevede tre fasi principali:

1. Configurare il server Microsoft Windows 2008.
2. Configurare i WLC e i Lightweight Access Point.
3. Configurare i client wireless.

### Configurazione di Microsoft Windows 2008 Server

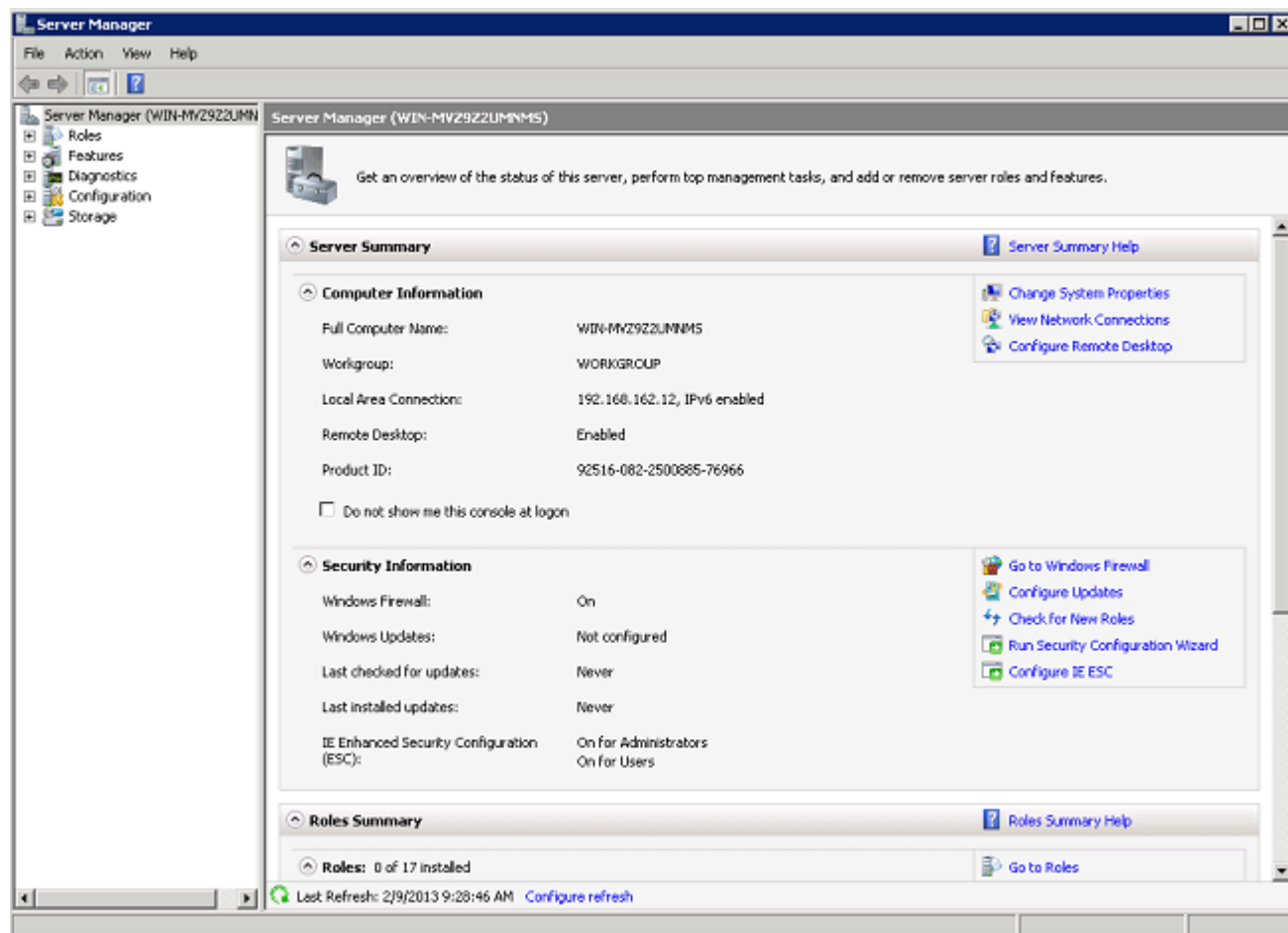
In questo esempio, una configurazione completa del server Microsoft Windows 2008 include i seguenti passaggi:

1. Configurare il server come controller di dominio.
2. Installare e configurare i servizi DHCP.
3. installare e configurare il server come server CA.
4. Connettere i client al dominio.
5. Installare Server dei criteri di rete.
6. Installare un certificato.
7. Configurare Server dei criteri di rete per l'autenticazione PEAP.
8. Aggiungere utenti ad Active Directory.

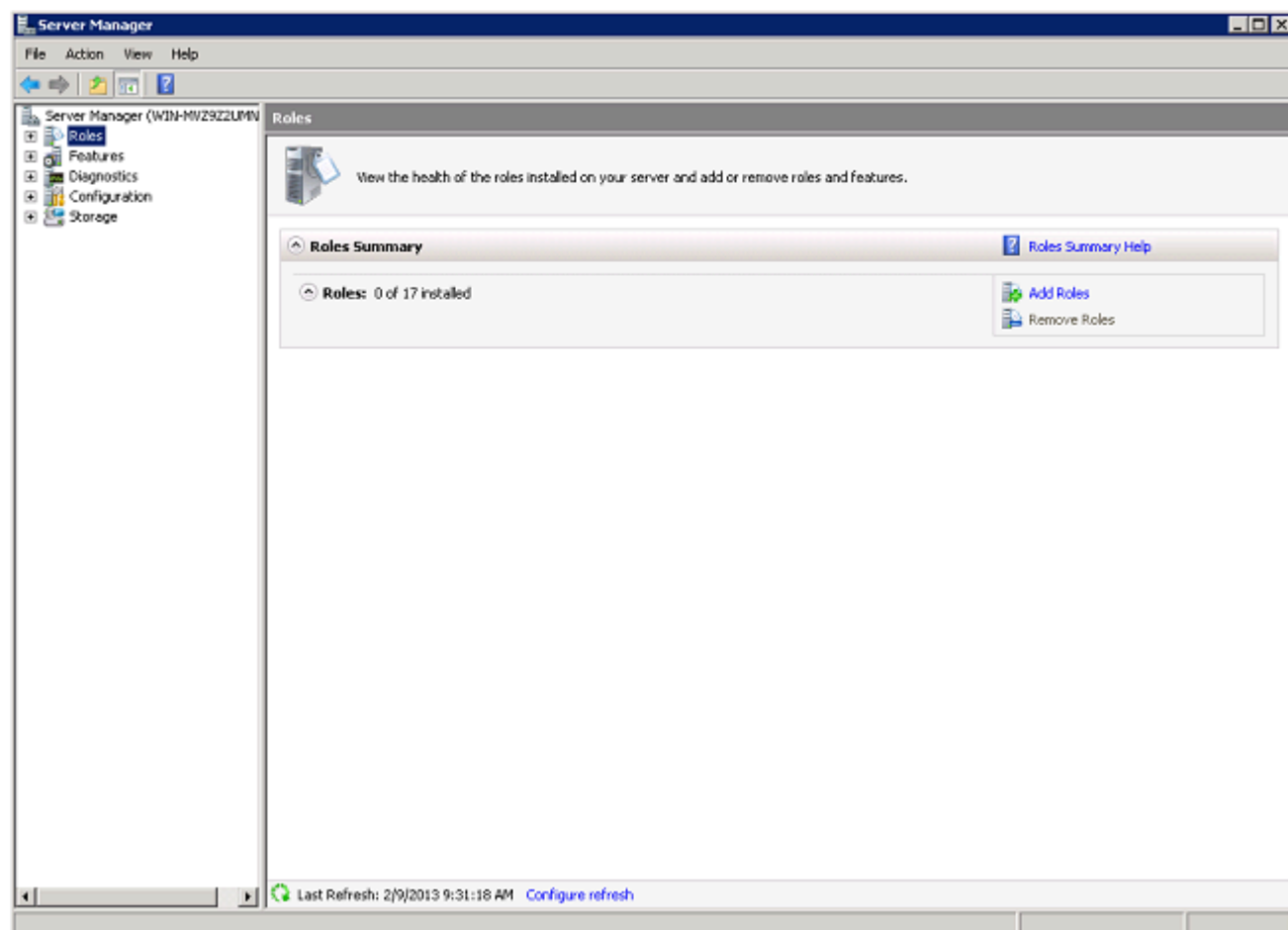
### Configurare il server Microsoft Windows 2008 come controller di dominio

Completare questa procedura per configurare il server Microsoft Windows 2008 come controller di dominio:

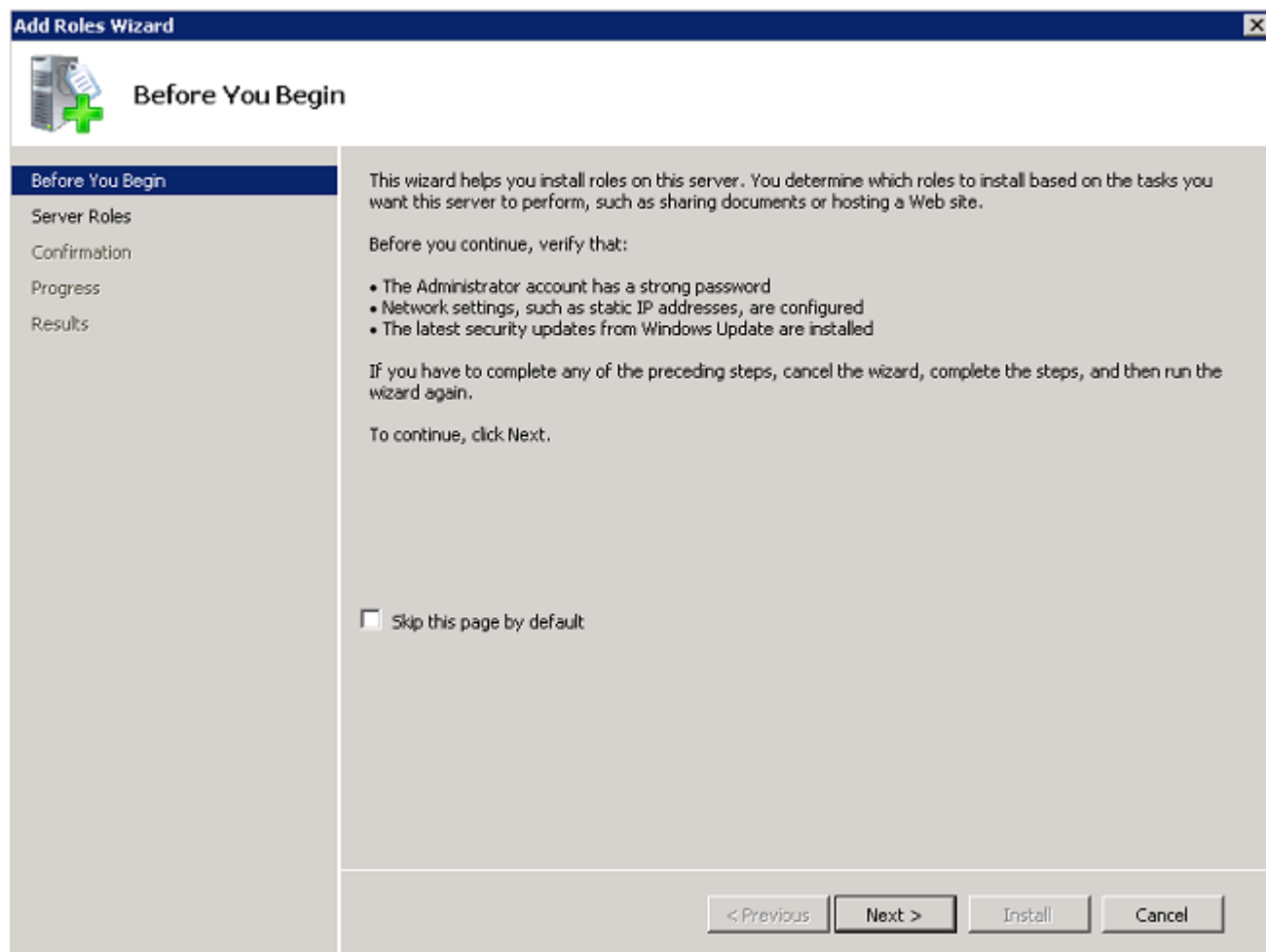
1. Fare clic su Start> Server Manager.



2. Fare clic su Ruoli> Aggiungi ruoli.

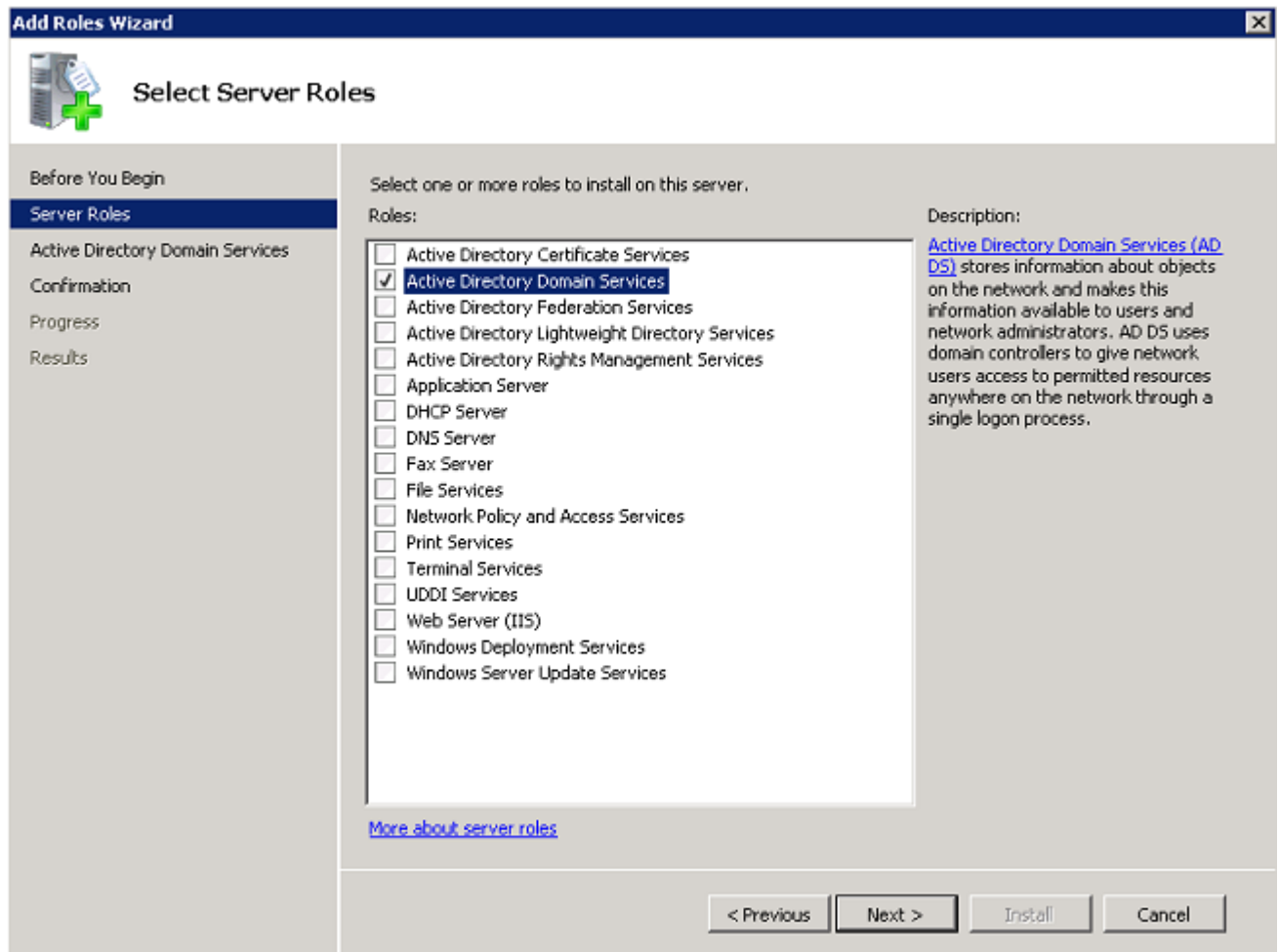


3. Fare clic su Next (Avanti).

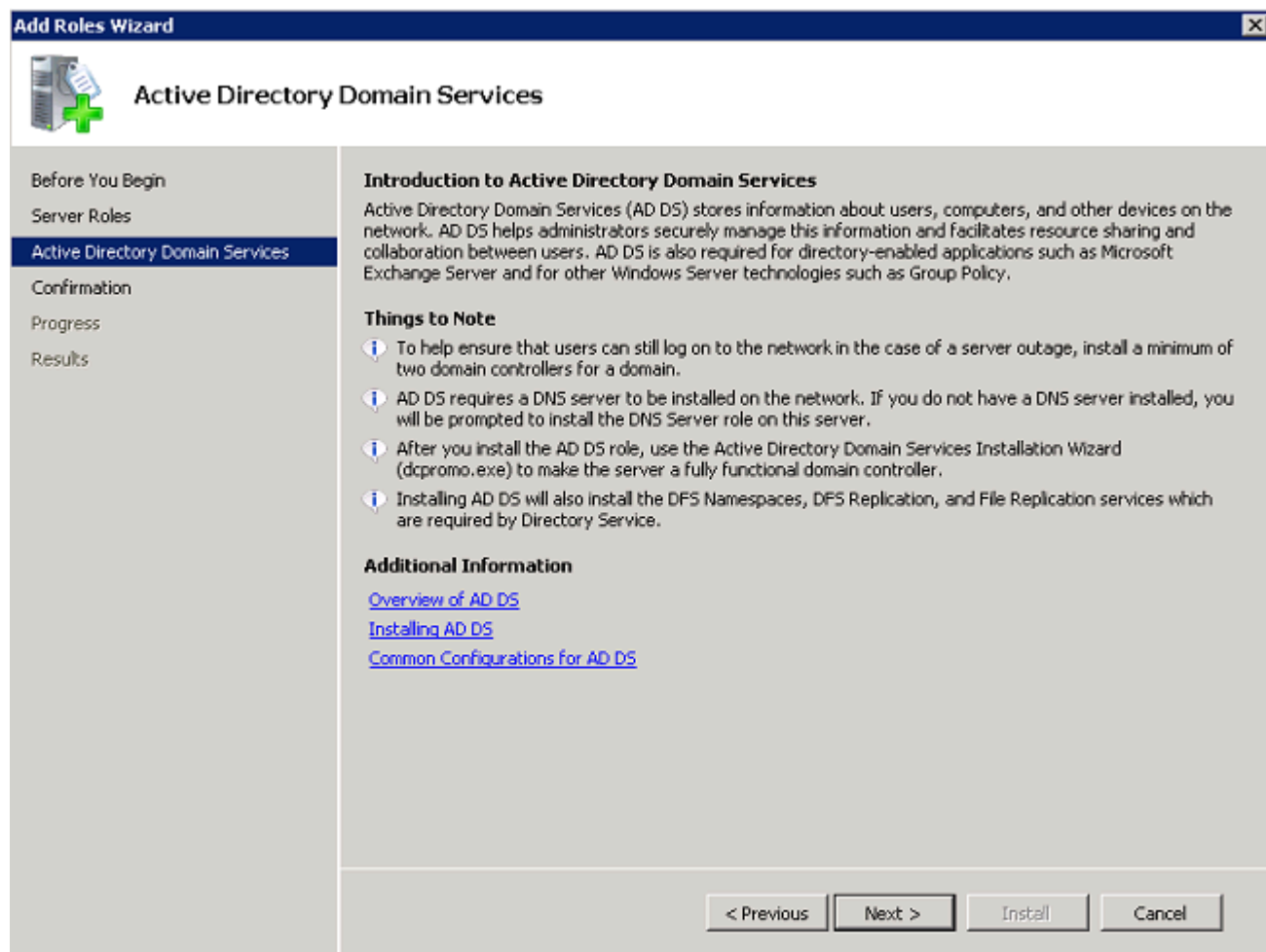


4. Selezionare il servizio Servizi di dominio Active Directory e fare clic su Avanti.

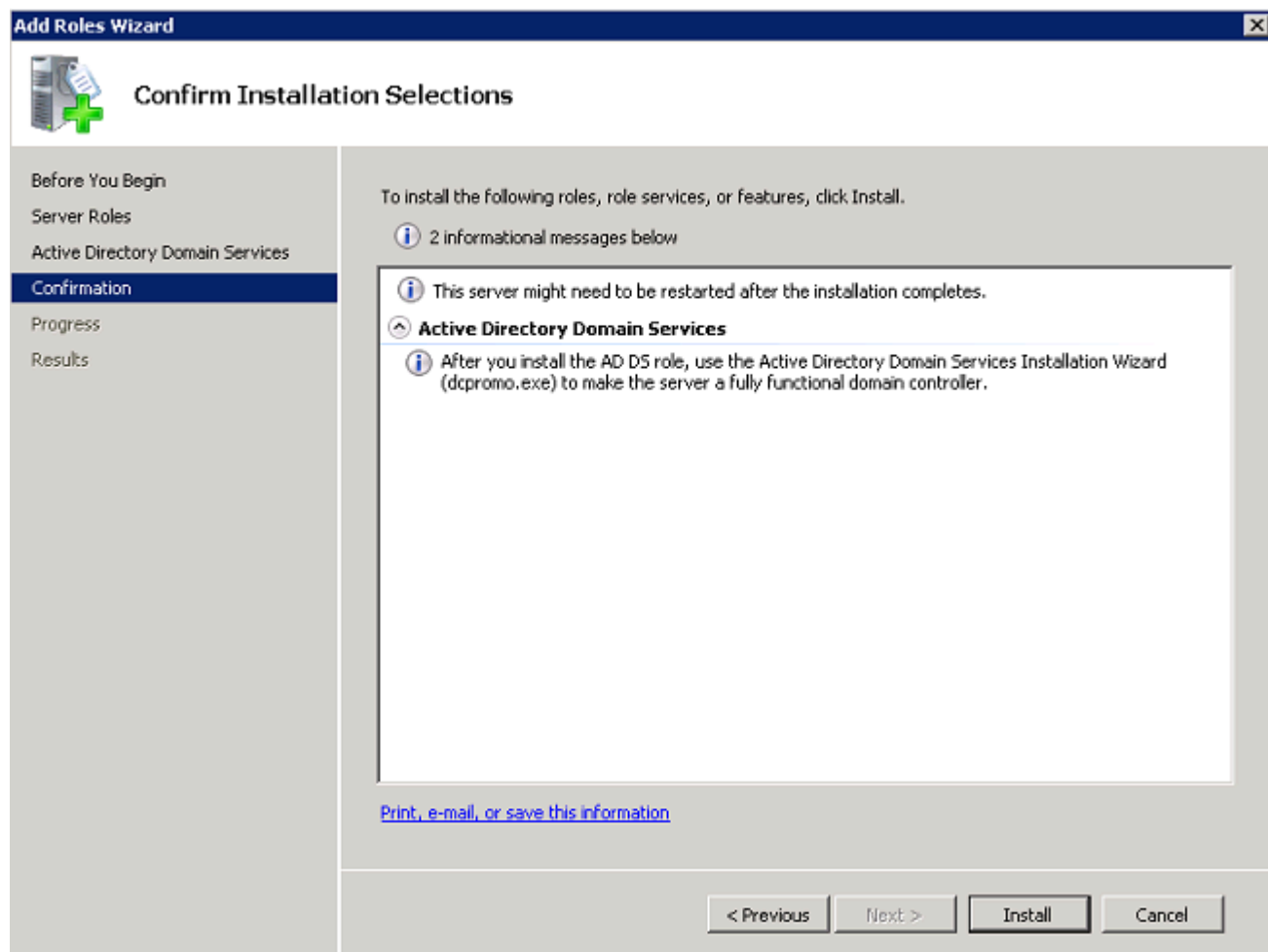




5. Rivedere l'Introduzione a Servizi di dominio Active Directory e fare clic su Avanti.

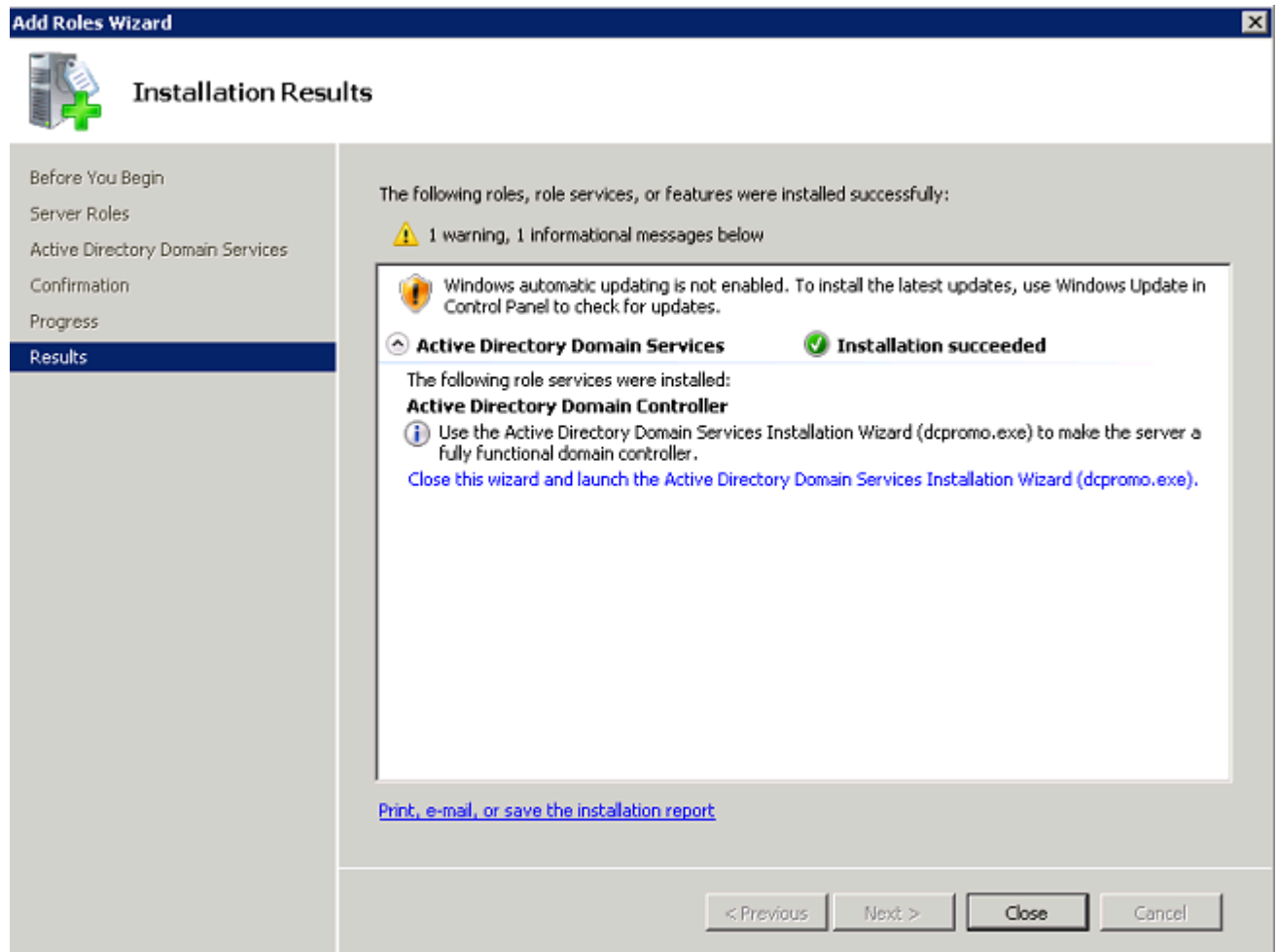


6. Fare clic su Installa per avviare il processo di installazione.



L'installazione procede e viene completata.

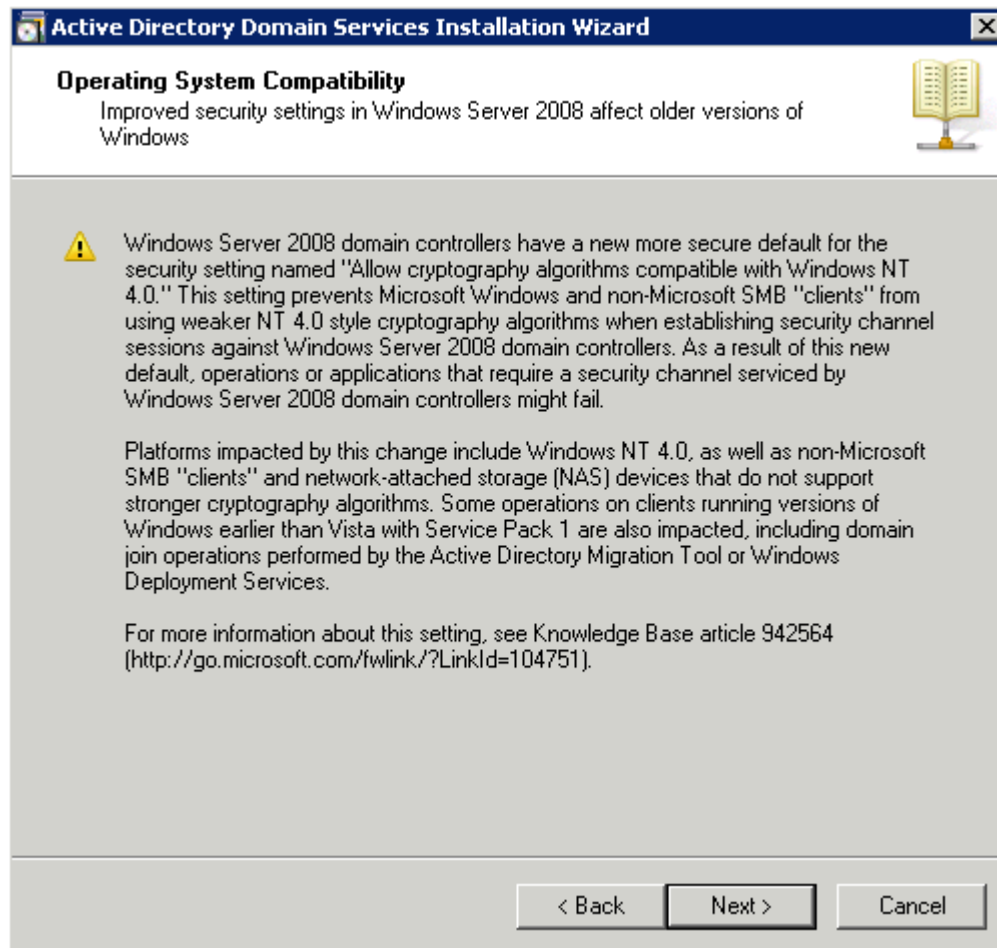
7. Fare clic su Chiudi la procedura guidata e avviare l'installazione guidata Servizi di dominio Active Directory (dcpromo.exe) per continuare l'installazione e la configurazione di Active Directory.



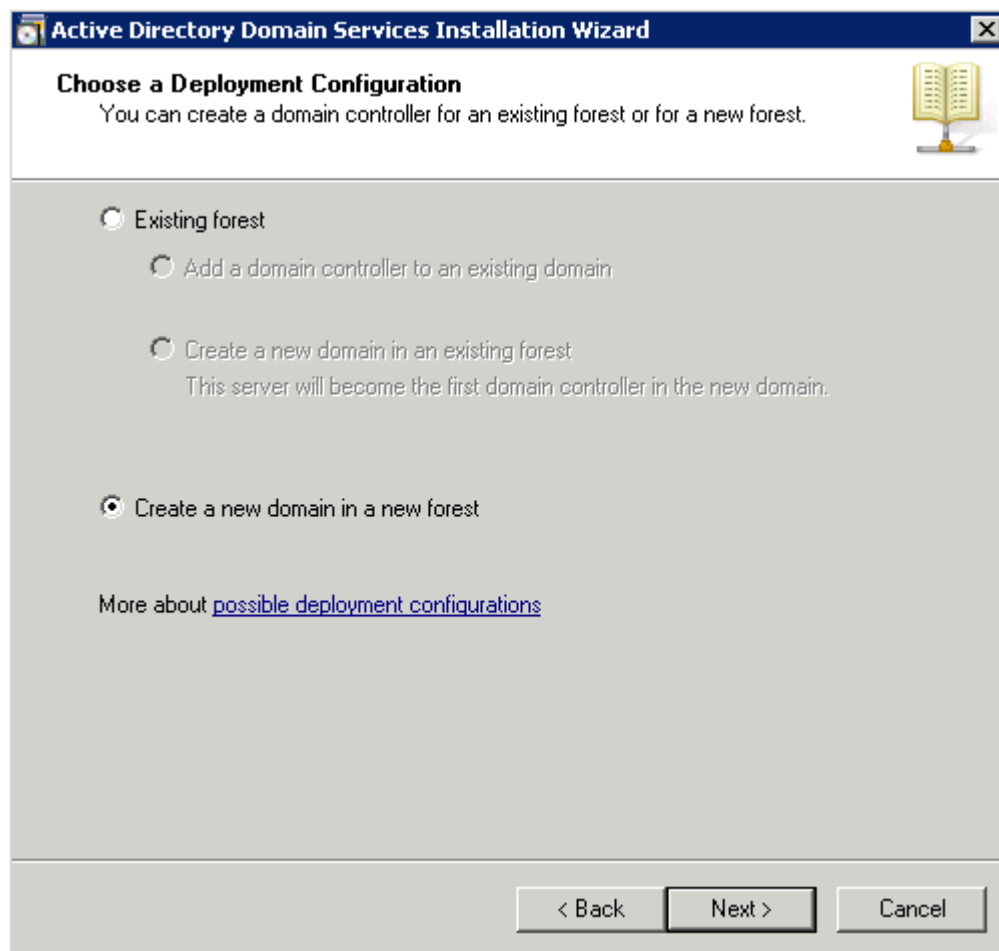
8. Fare clic su Avanti per eseguire l'installazione guidata Servizi di dominio Active Directory.



9. Esaminare le informazioni relative alla compatibilità del sistema operativo e fare clic su Avanti.



10. Per creare un nuovo dominio, fare clic su Crea un nuovo dominio in una nuova foresta >Avanti.



11. Immettere il nome DNS completo per il nuovo dominio e fare clic su Avanti.

**Active Directory Domain Services Installation Wizard**

**Name the Forest Root Domain**

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

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

FQDN of the forest root domain:

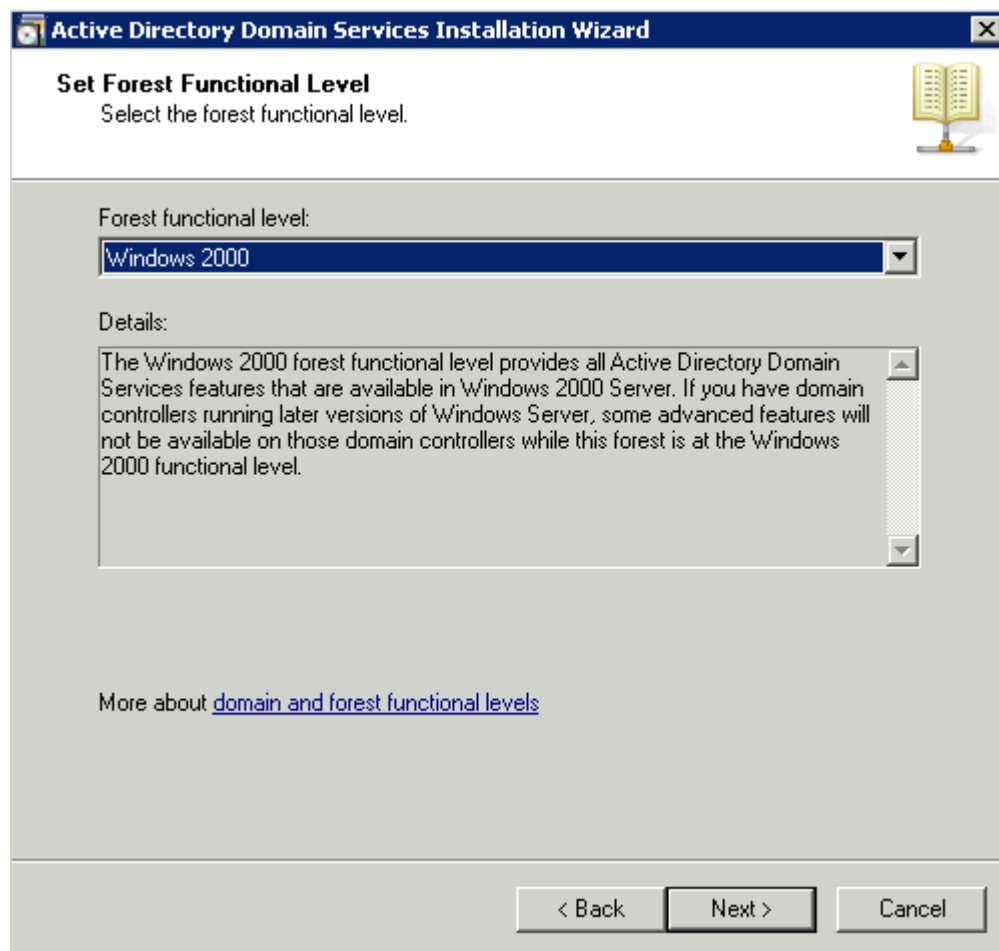
wireless.com

Example: corp.contoso.com

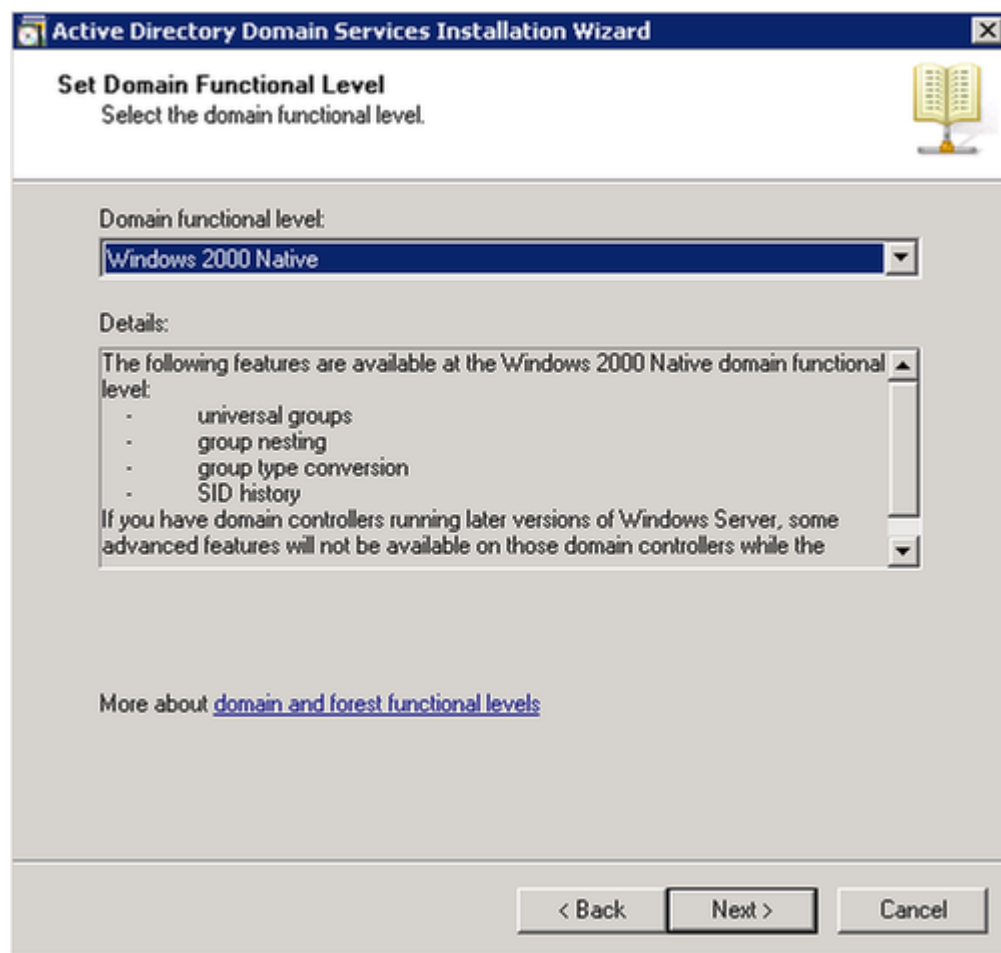
< Back   Next >   Cancel

12. Selezionare il livello di funzionalità della foresta per il dominio e fare clic su Avanti.

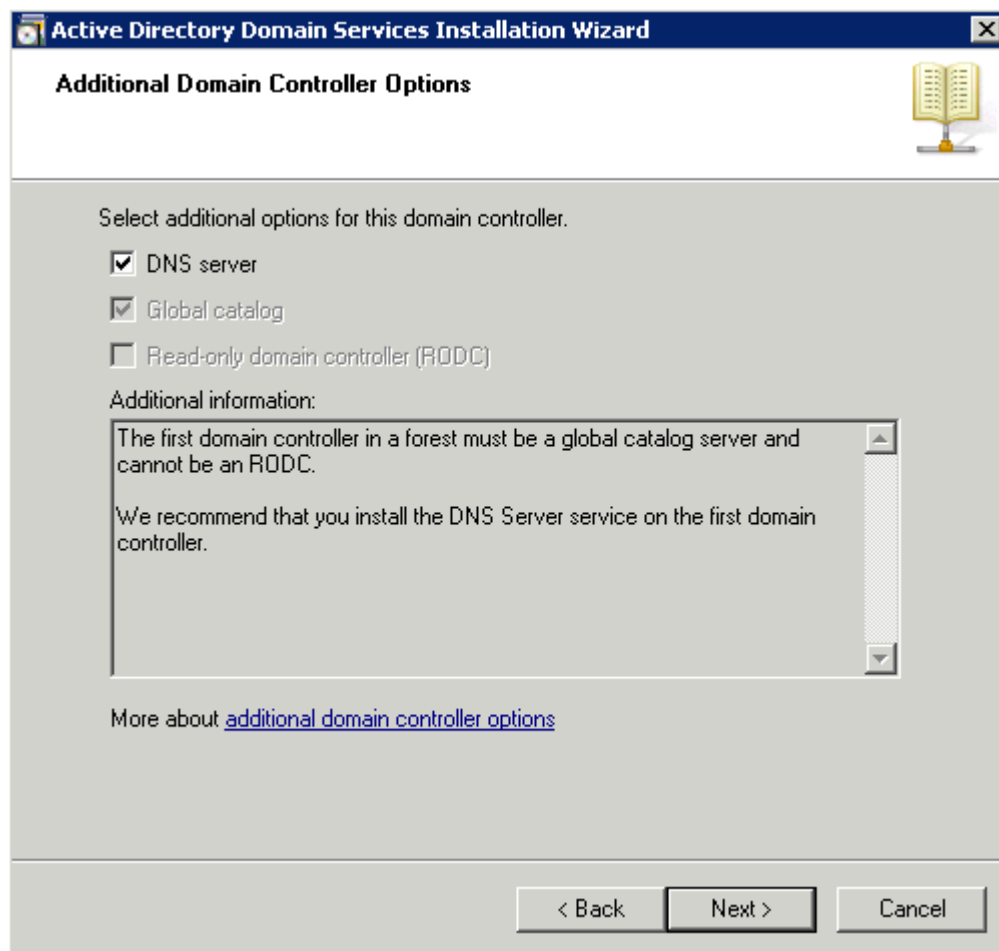




13. Selezionare il livello di funzionalità del dominio e fare clic su Avanti.



14. Verificare che il server DNS sia selezionato e fare clic su Avanti.



15. Fare clic su Sì per creare una nuova zona in DNS per il dominio durante l'installazione guidata.



16. Selezionare le cartelle che devono essere utilizzate da Active Directory per i file e fare clic su Avanti.

**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:

Log files folder:

SYSVOL folder:

More about [placing Active Directory Domain Services files](#)

17. Immettere la password dell'amministratore e fare clic su Avanti.

**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.

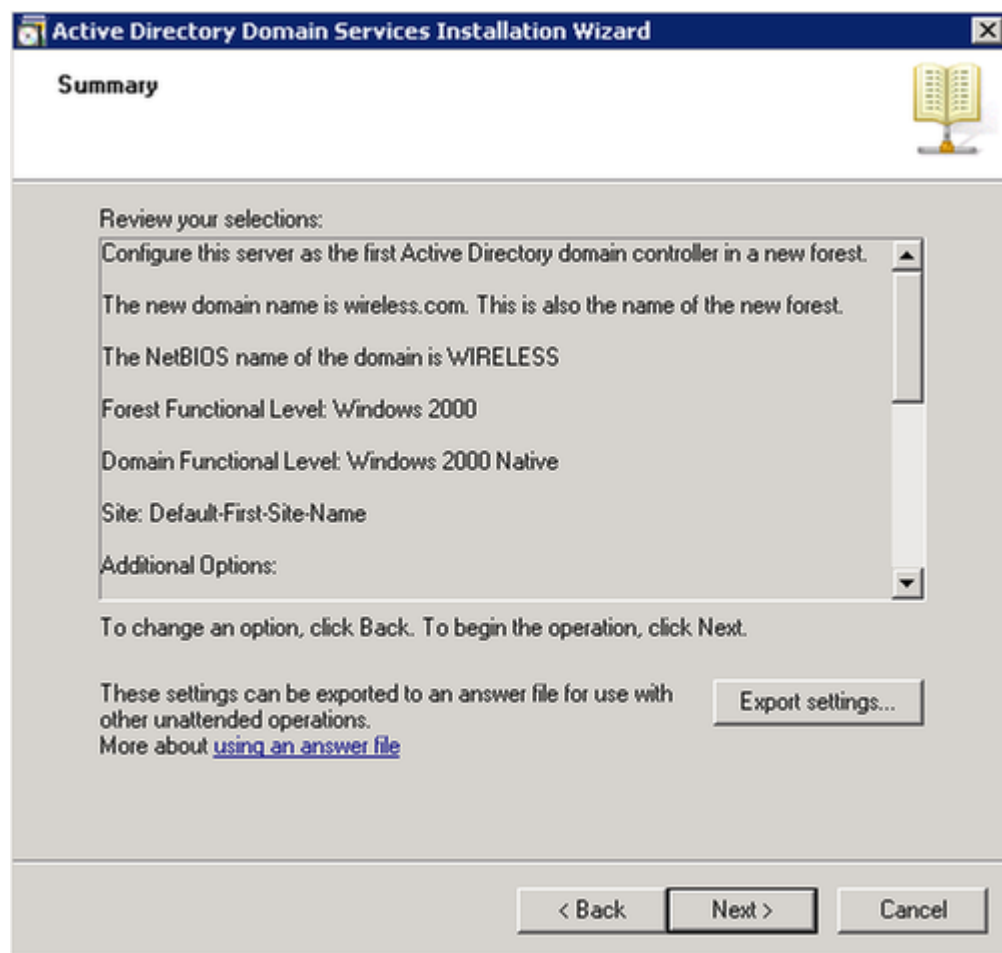
Password:

Confirm password:

More about [Directory Services Restore Mode password](#)

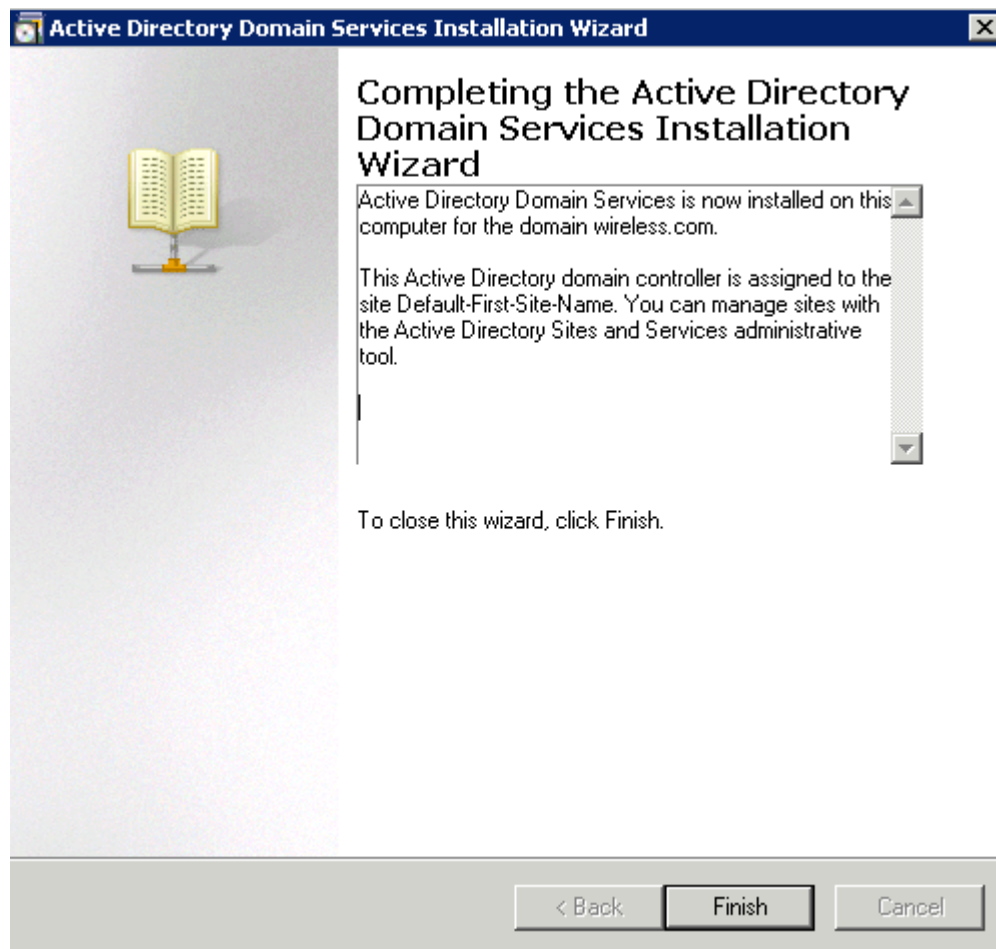
< Back   Next >   Cancel

18. Verificare le selezioni e fare clic su Avanti.

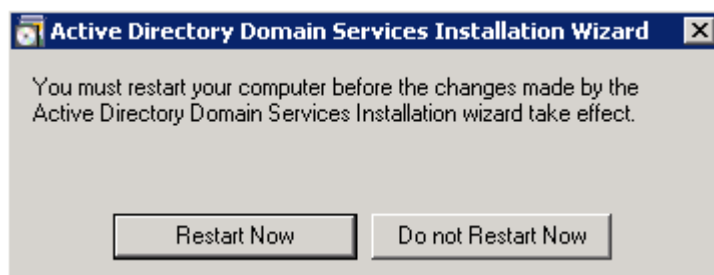


L'installazione procede.

19. Scegliere Fine per chiudere la procedura guidata.



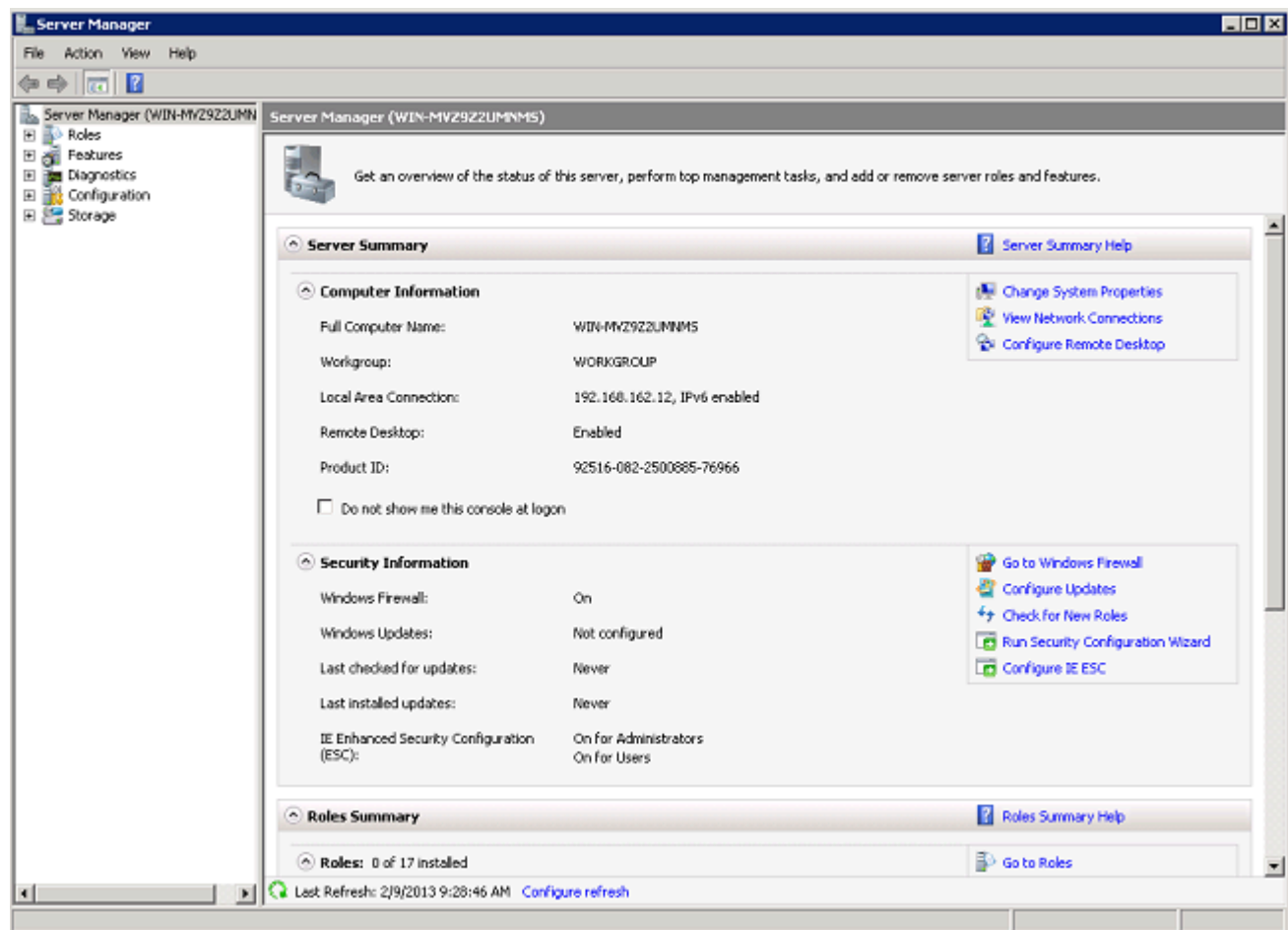
20. Riavviare il server per rendere effettive le modifiche.



Installare e configurare i servizi DHCP in Microsoft Windows 2008 Server

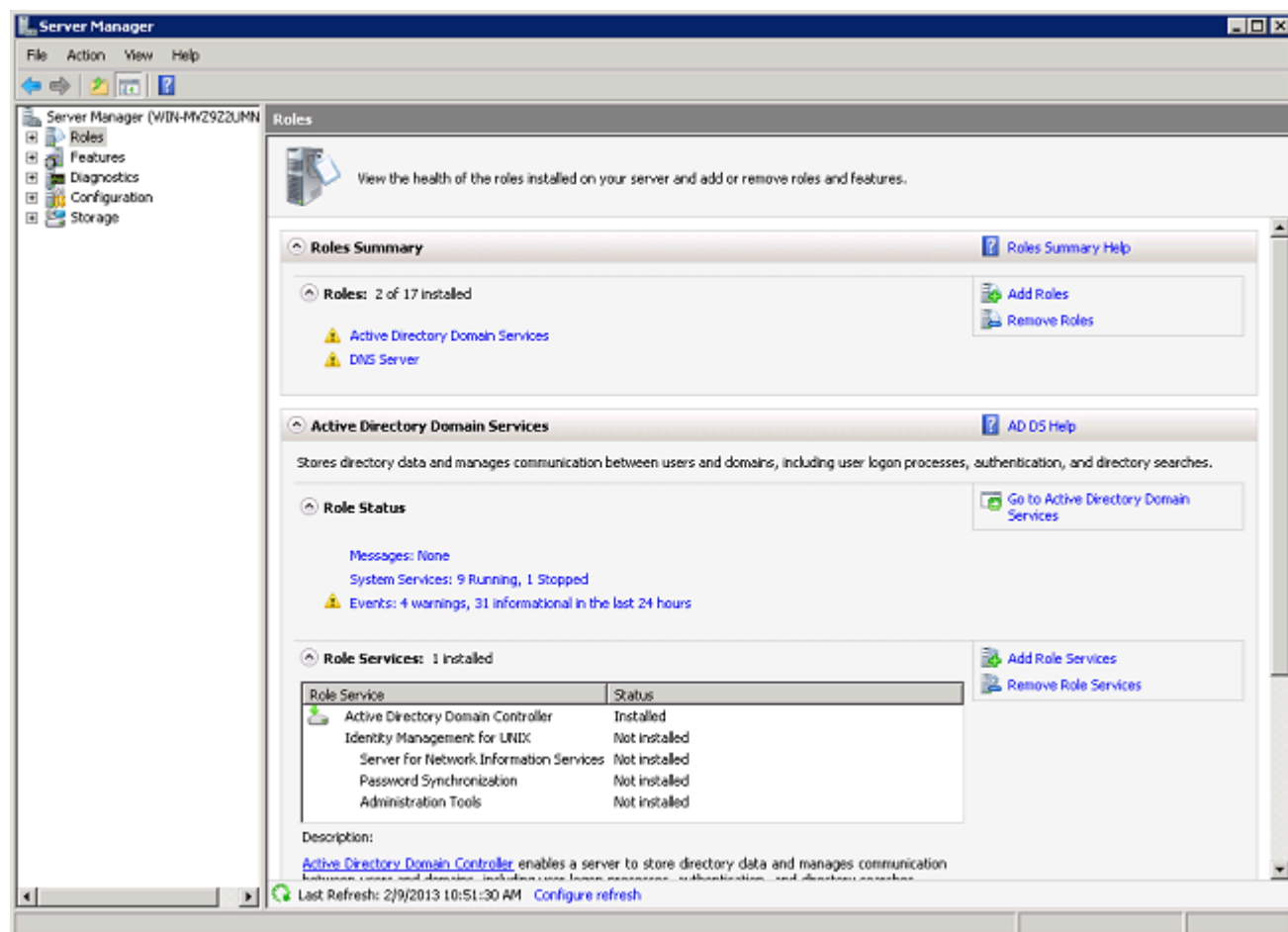
Il servizio DHCP nel server Microsoft 2008 viene utilizzato per fornire indirizzi IP ai client wireless. Completare questa procedura per installare e configurare i servizi DHCP:

1. Fare clic su Start>Server Manager.




2. Fare clic su Ruoli> Aggiungi ruoli.





3. Fare clic su Next (Avanti).

**Add Roles Wizard**

 **Before You Begin**

**Before You Begin**

Server Roles

Confirmation

Progress

Results

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

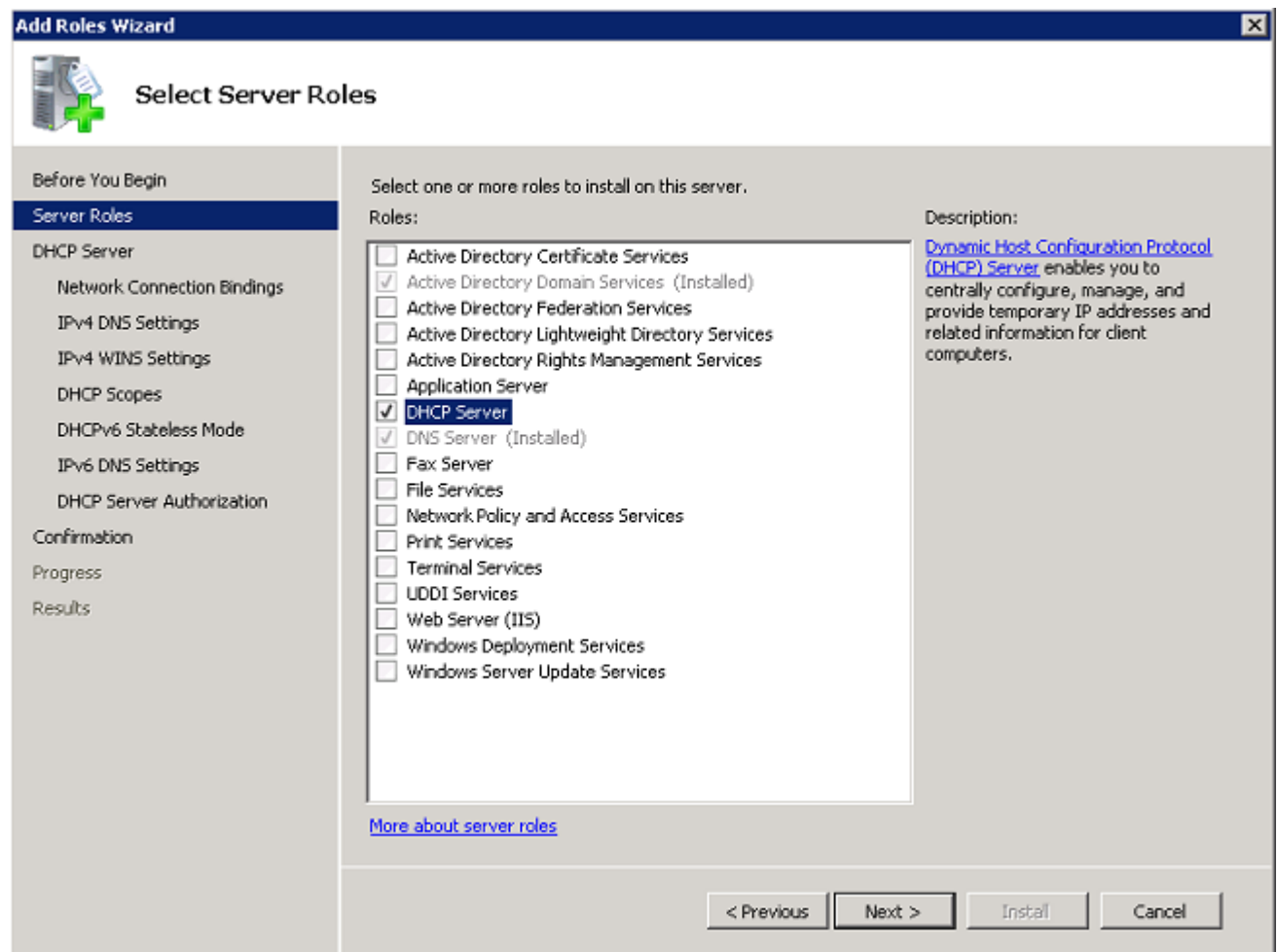
If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

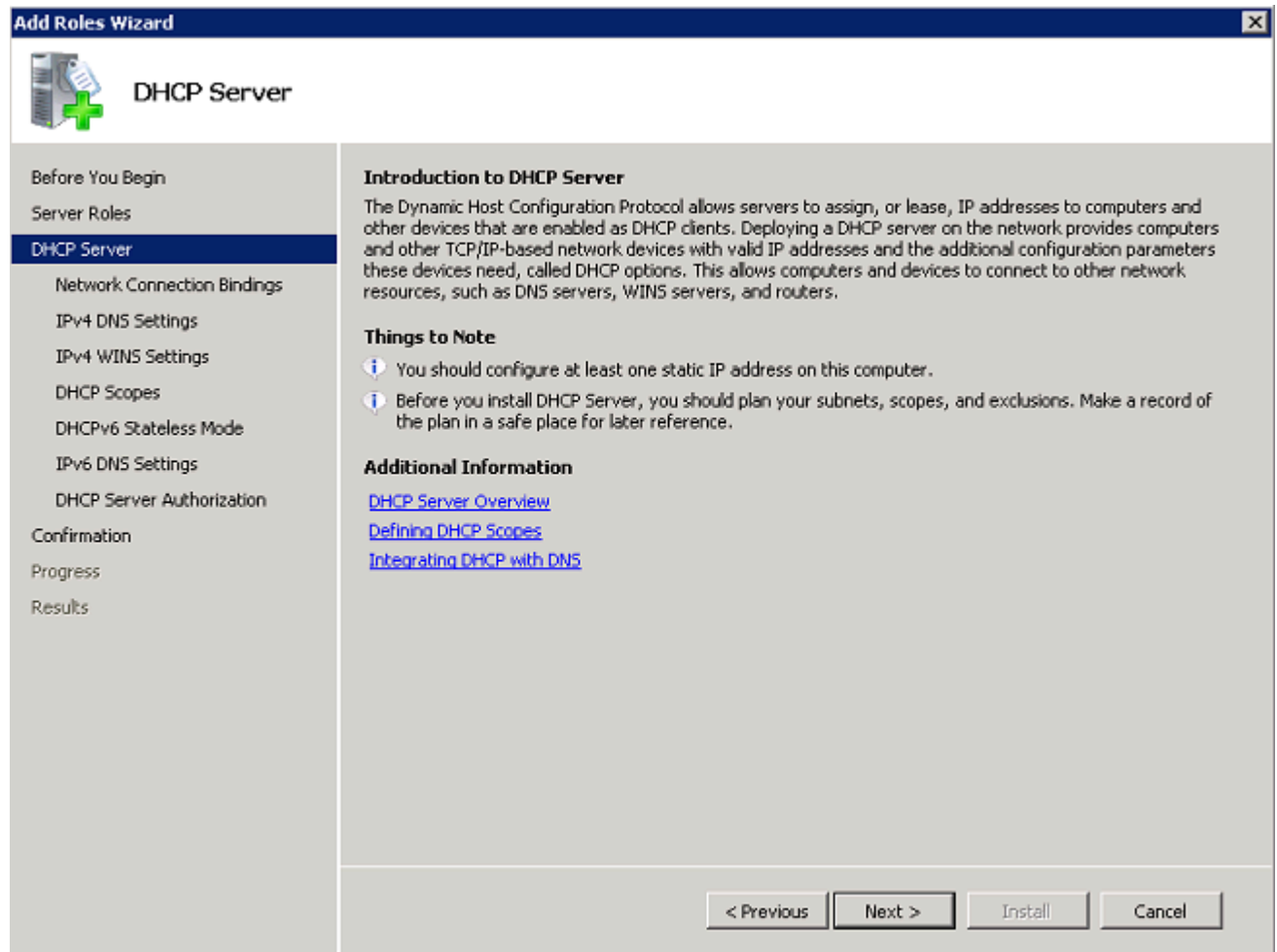
☐ Skip this page by default

< Previous   **Next >**   Install   Cancel

4. Selezionare il servizio DHCP Server, quindi fare clic su Avanti.




5. Rivedere l'Introduzione al server DHCP e fare clic su Avanti.



6. Selezionare l'interfaccia che il server DHCP deve monitorare per le richieste e fare clic su Avanti.

**Add Roles Wizard**

 **Select Network Connection Bindings**

Before You Begin  
Server Roles  
DHCP Server  
**Network Connection Bindings**  
IPv4 DNS Settings  
IPv4 WINS Settings  
DHCP Scopes  
DHCPv6 Stateless Mode  
IPv6 DNS Settings  
DHCP Server Authorization  
Confirmation  
Progress  
Results

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

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

Network Connections:

IP Address	Type
<input checked="" type="checkbox"/> 192.168.162.12	IPv4


Details

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

< Previous   Next >   Install   Cancel

7. Configurare le impostazioni DNS predefinite che il server DHCP deve fornire ai client e fare clic su Avanti.

**Add Roles Wizard**

 **Specify IPv4 DNS Server Settings**

**Before You Begin**

Server Roles

DHCP Server

Network Connection Bindings

**IPv4 DNS Settings**

IPv4 WINS Settings

DHCP Scopes

DHCPv6 Stateless Mode

IPv6 DNS Settings

DHCP Server Authorization

Confirmation

Progress

Results

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

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

Parent Domain:

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


Preferred DNS Server IPv4 Address:

Alternate DNS Server IPv4 Address:

[More about DNS server settings](#)

8. Configurare WINS se la rete supporta WINS.

**Add Roles Wizard**

 **Specify IPv4 WINS Server Settings**

**Before You Begin**

**Server Roles**

**DHCP Server**

Network Connection Bindings

IPv4 DNS Settings

**IPv4 WINS Settings**

DHCP Scopes

DHCPv6 Stateless Mode

IPv6 DNS Settings

DHCP Server Authorization

**Confirmation**

Progress

Results

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

☒ WINS is not required for applications on this network

☐ WINS is required for applications on this network

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

Preferred WINS Server IP Address:


Alternate WINS Server IP Address:

[More about WINS server settings](#)

< Previous   Next >   Install   Cancel

9. Fare clic su Add per utilizzare la procedura guidata e creare un ambito DHCP oppure fare clic su Next per creare un ambito DHCP in un secondo momento. Fare clic su Next (Avanti) per continuare.

**Add Roles Wizard**

 **Add or Edit DHCP Scopes**

Before You Begin  
Server Roles  
DHCP Server  
  Network Connection Bindings  
  IPv4 DNS Settings  
  IPv4 WINS Settings  
**DHCP Scopes**  
  DHCPv6 Stateless Mode  
  IPv6 DNS Settings  
  DHCP Server Authorization  
Confirmation  
Progress  
Results

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

Scopes:

Name	IP Address Range
------	------------------

**Add...**  
**Edit...**  
**Delete**

Properties  
Add or select a scope to view its properties.


[More about adding scopes](#)

< Previous    Next >    Install    Cancel

10. Attivare o disattivare il supporto per DHCPv6 nel server e fare clic su Avanti.



**Add Roles Wizard**

 **Configure DHCPv6 Stateless Mode**

**Before You Begin**

Server Roles

DHCP Server

Network Connection Bindings

IPv4 DNS Settings

IPv4 WINS Settings

DHCP Scopes

**DHCPv6 Stateless Mode**

IPv6 DNS Settings

DHCP Server Authorization

Confirmation

Progress

Results

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

Select the DHCPv6 stateless mode configuration for this server.

☒ Enable DHCPv6 stateless mode for this server  
IPv6 clients will be automatically configured without using this DHCP server.


☐ Disable DHCPv6 stateless mode for this server  
After installing DHCP Server, you can configure the DHCPv6 mode using the DHCP Management console.

[More about DHCPv6 stateless mode](#)

< Previous   Next >   Install   Cancel

11. Configurare le impostazioni DNS IPv6 se DHCPv6 è stato abilitato nel passaggio precedente. Fare clic su Avanti per continuare.

**Add Roles Wizard**

 **Specify IPv6 DNS Server Settings**

**Before You Begin**

Server Roles

DHCP Server

- Network Connection Bindings
- IPv4 DNS Settings
- IPv4 WINS Settings
- DHCP Scopes
- DHCPv6 Stateless Mode
- IPv6 DNS Settings**
- DHCP Server Authorization

Confirmation

Progress

Results

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

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

Parent Domain:

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

Preferred DNS Server IPv6 Address:

Alternate DNS Server IPv6 Address:


[More about DNS server settings](#)

< Previous   Next >   Install   Cancel

12. Specificare le credenziali dell'amministratore di dominio per autorizzare il server DHCP in Active Directory e fare clic su Avanti.

**Add Roles Wizard**

### Authorize DHCP Server



Before You Begin

Server Roles

DHCP Server

- Network Connection Bindings
- IPv4 DNS Settings
- IPv4 WINS Settings
- DHCP Scopes
- DHCPv6 Stateless Mode
- IPv6 DNS Settings
- DHCP Server Authorization**

Confirmation

Progress

Results

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

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

☒ Use current credentials

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


User Name:

☐ Use alternate credentials

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

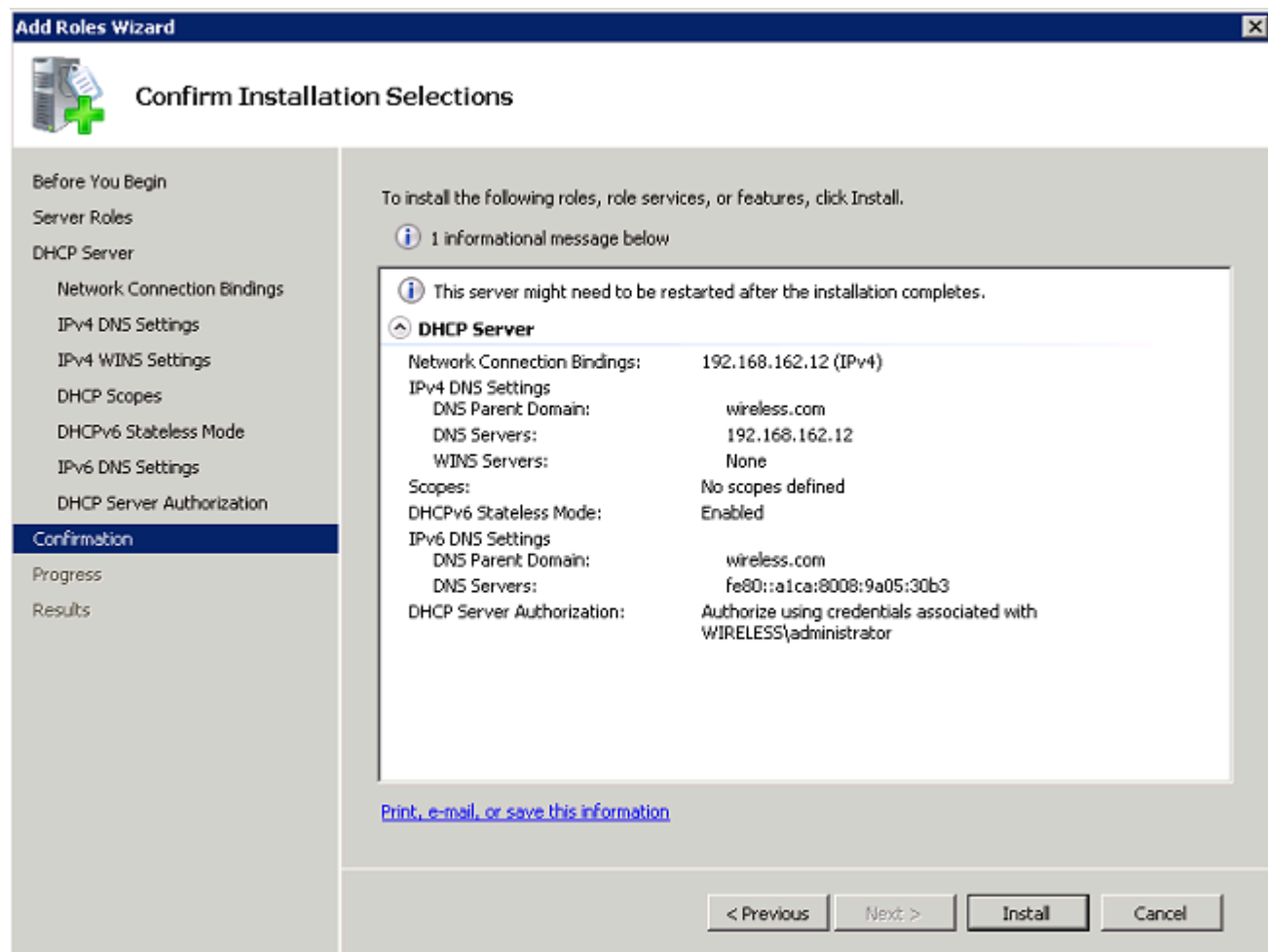
User Name:

☐ Skip authorization of this DHCP server in AD DS

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

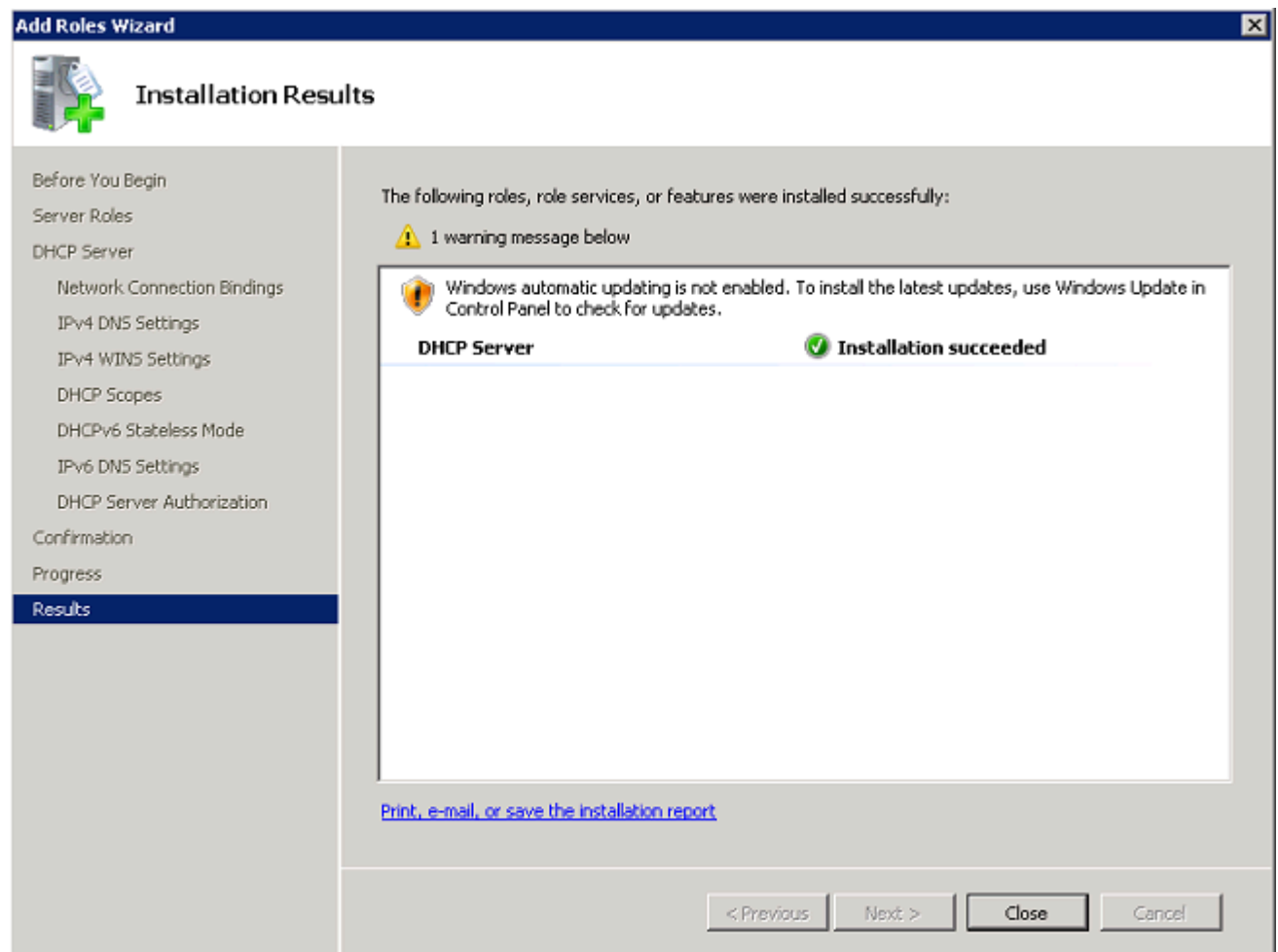
[More about authorizing DHCP servers in AD DS](#)

13. Esaminare la configurazione nella pagina di conferma e fare clic su Installa per completare l'installazione.



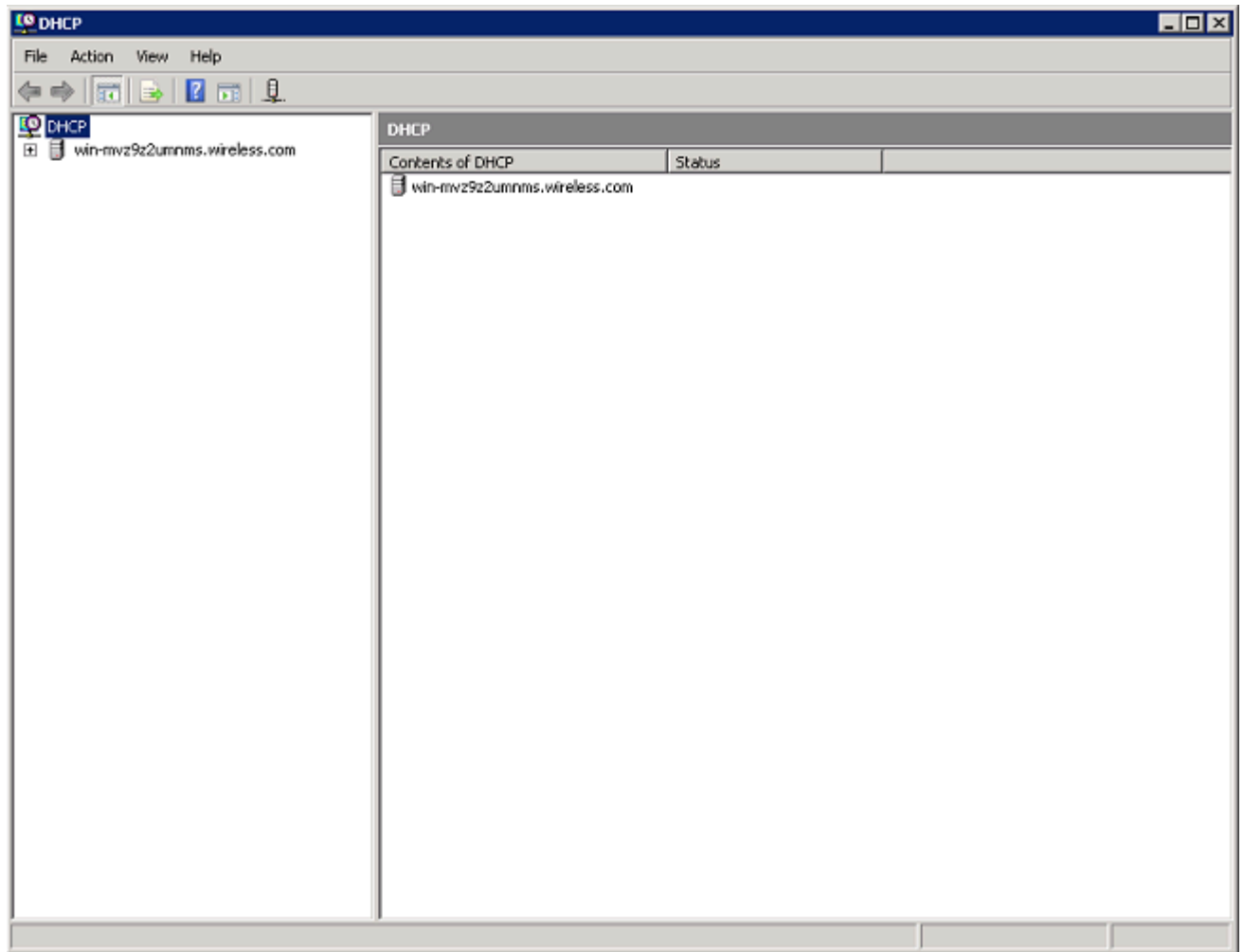
L'installazione procede.

14. Fare clic su Chiudi per chiudere la procedura guidata.

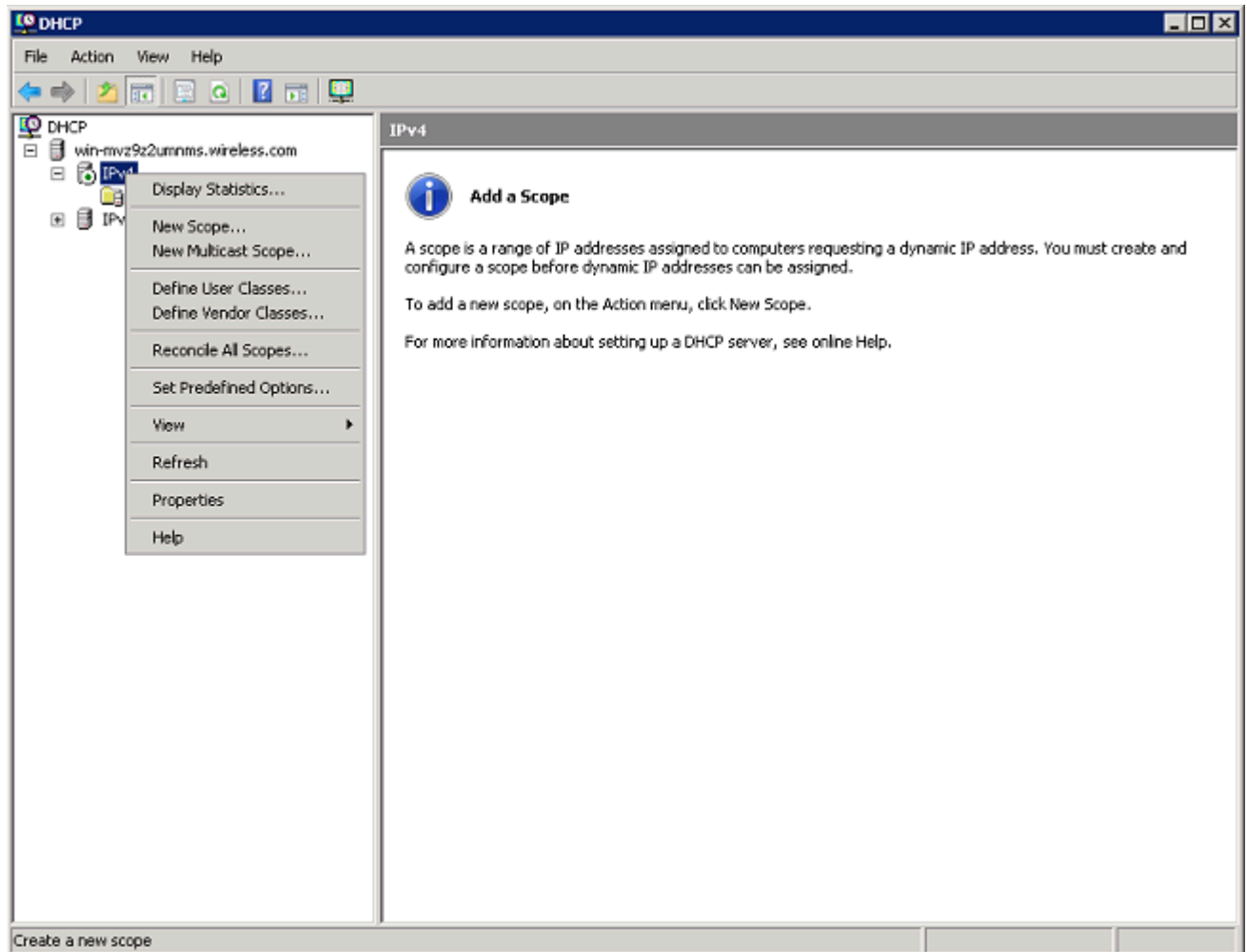


Il server DHCP è installato.

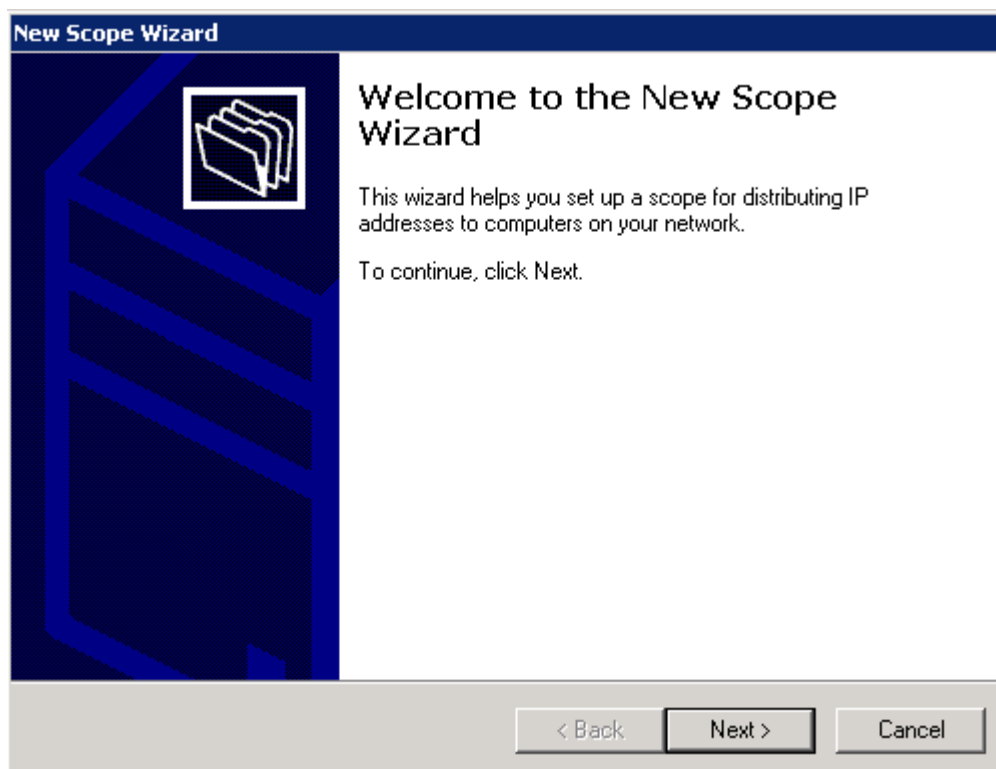
15. Fare clic su Start > Strumenti di amministrazione > DHCP per configurare il servizio DHCP.



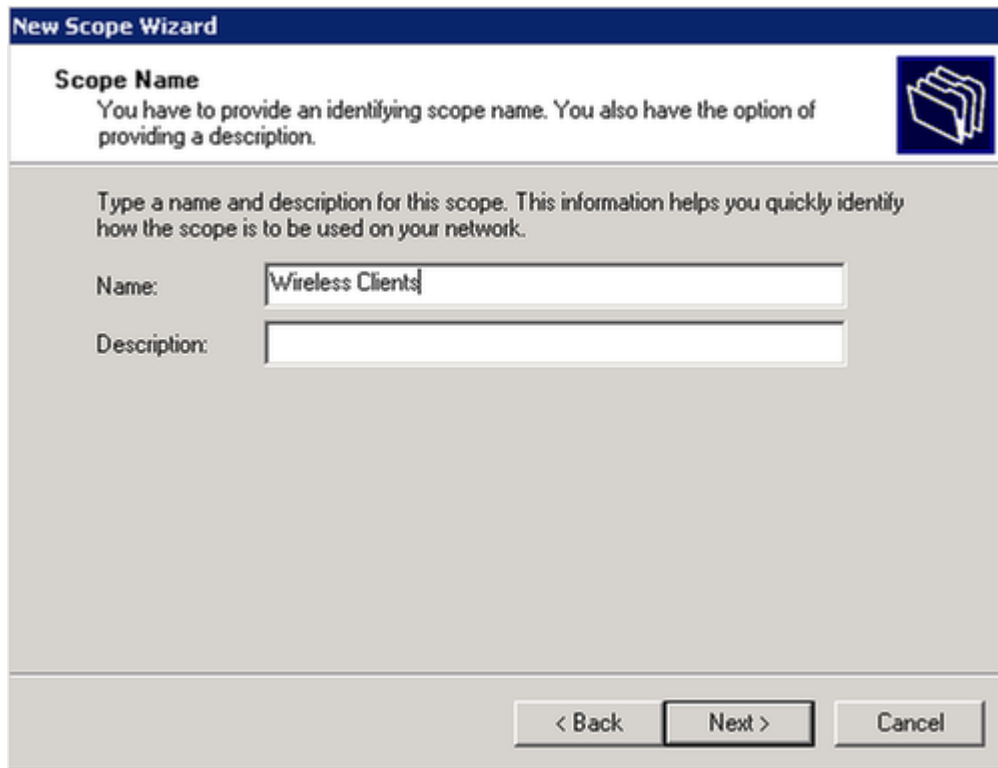
16. Espandere il server DHCP (come mostrato nell'immagine precedente dell'esempio), fare clic con il pulsante destro del mouse su IPv4, quindi selezionare New Scope (Nuovo ambito) per creare un ambito DHCP.



17. Fare clic su Avanti per configurare il nuovo ambito tramite la Creazione guidata ambito.



18. Specificare un nome per il nuovo ambito (in questo esempio Client wireless) e fare clic su Avanti.



The image shows a 'New Scope Wizard' dialog box. The title bar is dark blue with the text 'New Scope Wizard' in white. The main area has a light gray background. At the top, there is a section titled 'Scope Name' in bold, followed by the text 'You have to provide an identifying scope name. You also have the option of providing a description.' To the right of this text is a small icon of a folder with a document. Below this, there is a paragraph of text: 'Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.' Underneath, there are two input fields. The first is labeled 'Name:' and contains the text 'Wireless Clients'. The second is labeled 'Description:' and is empty. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**New Scope Wizard**

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

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

Name:

Description:

< Back   Next >   Cancel

19. Immettere l'intervallo di indirizzi IP disponibili che possono essere utilizzati per i lease DHCP. Fare clic su Next (Avanti) per continuare.



**New Scope Wizard**

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

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 162 . 100

End IP address: 192 . 168 . 162 . 200

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

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

20. Creare un elenco facoltativo di indirizzi esclusi. Fare clic su Next (Avanti) per continuare.

**New Scope Wizard**

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

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

Start IP address: . . . End IP address: . . . Add

Excluded address range:

Remove

< Back Next > Cancel

21. Configurare la durata del lease e fare clic su Avanti.

**New Scope Wizard**

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

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

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

Limited to:

Days:  Hours:  Minutes:

< Back   Next >   Cancel

22. Fare clic su Sì, configurare le opzioni ora, quindi fare clic su Avanti.

**New Scope Wizard**

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

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

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

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

☒ Yes, I want to configure these options now

☐ No, I will configure these options later

< Back   Next >   Cancel

23. Immettere l'indirizzo IP del gateway predefinito per questo ambito, fare clic su Add > Next (Aggiungi > Avanti).

**New Scope Wizard**

**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

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

IP address:

. . .	Add
192.168.162.2	Remove
	Up
	Down

< Back   Next >   Cancel

24. Configurare il nome di dominio DNS e il server DNS che verranno utilizzati dai client. Fare clic su Next (Avanti) per continuare.

**New Scope Wizard**

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

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

Parent domain: wireless.com

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

Server name:	IP address:	Add
	. . .	
Resolve	192.168.162.12	Remove
		Up
		Down

< Back   Next >   Cancel

25. Immettere le informazioni WINS per questo ambito se la rete supporta WINS. Fare clic su Next (Avanti) per continuare.

**New Scope Wizard**

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

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

Server name:  IP address:

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

26. Per attivare l'ambito, fare clic su Sì, attiva l'ambito adesso> Avanti.

**New Scope Wizard**

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

Do you want to activate this scope now?

☒ Yes, I want to activate this scope now

☐ No, I will activate this scope later

27. Scegliere Fine per completare e chiudere la procedura guidata.

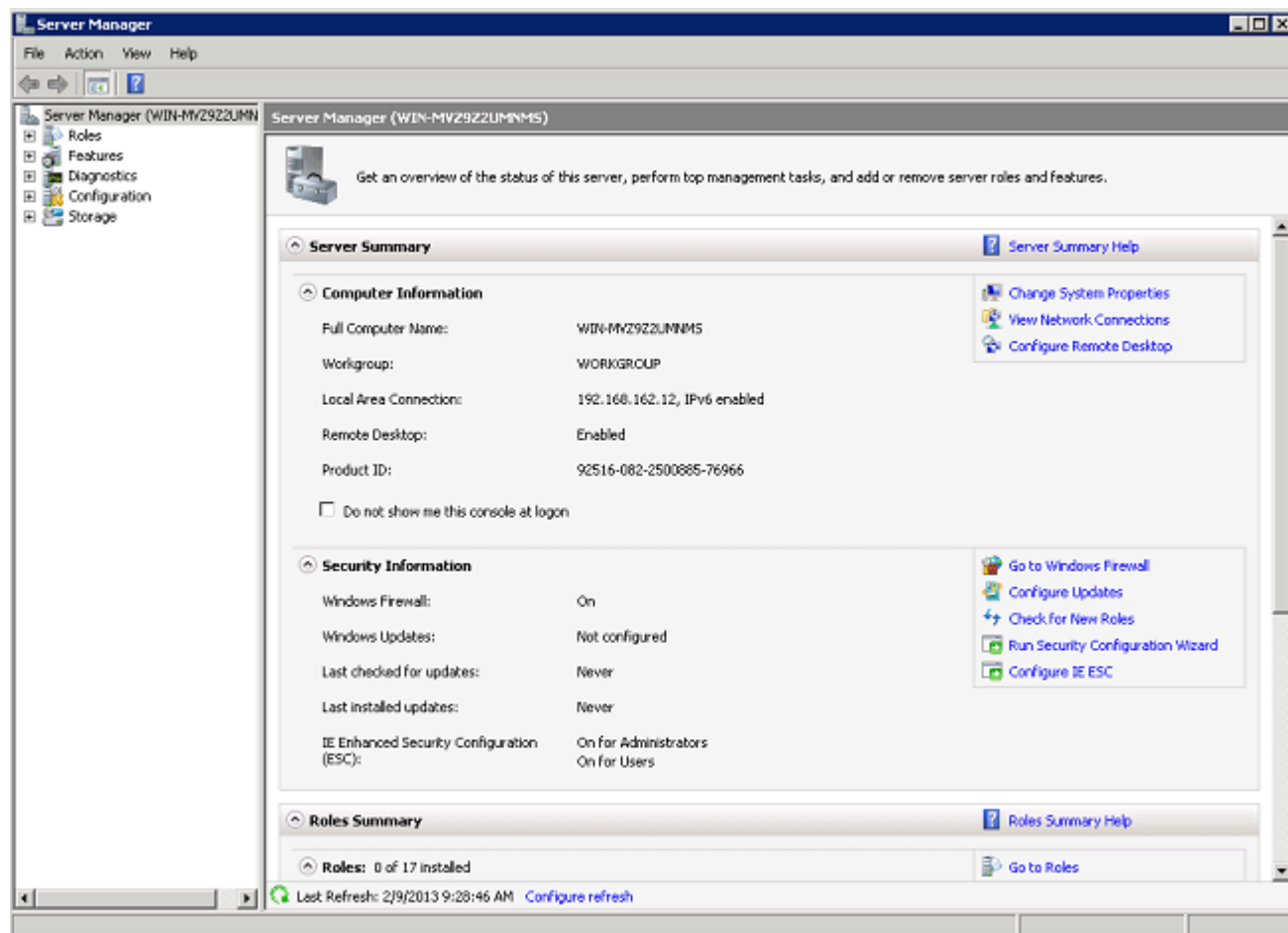


Installazione e configurazione di Microsoft Windows 2008 Server come server CA

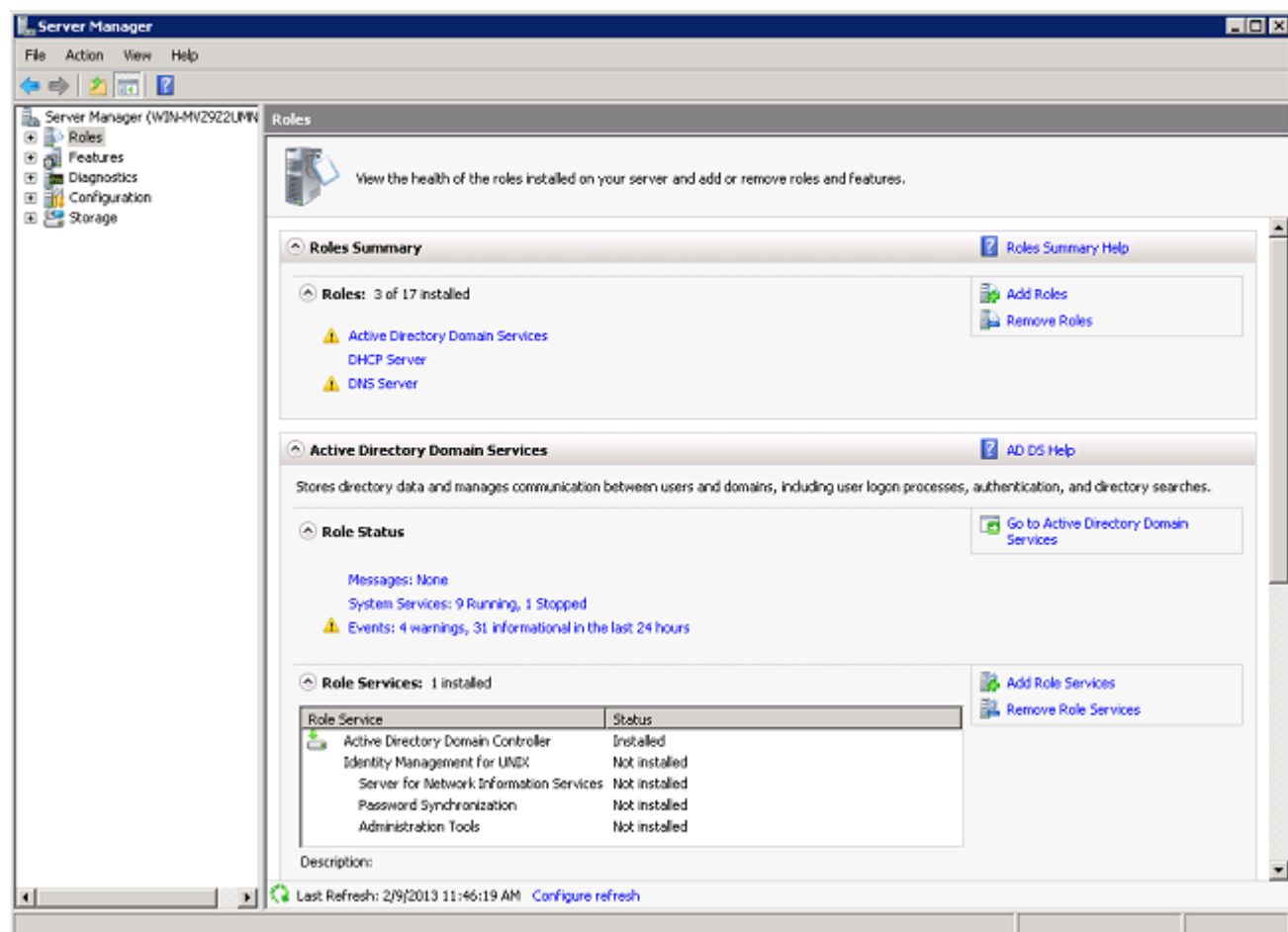
PEAP con EAP-MS-CHAP v2 convalida il server RADIUS in base al certificato presente sul server. Il certificato server deve inoltre essere rilasciato da una CA pubblica considerata attendibile dal computer client, ovvero il certificato CA pubblico esiste già nella cartella Autorità di certificazione radice attendibile nell'archivio certificati del computer client.

Completare la procedura seguente per configurare il server Microsoft Windows 2008 come server CA che rilascia il certificato al Server dei criteri di rete:

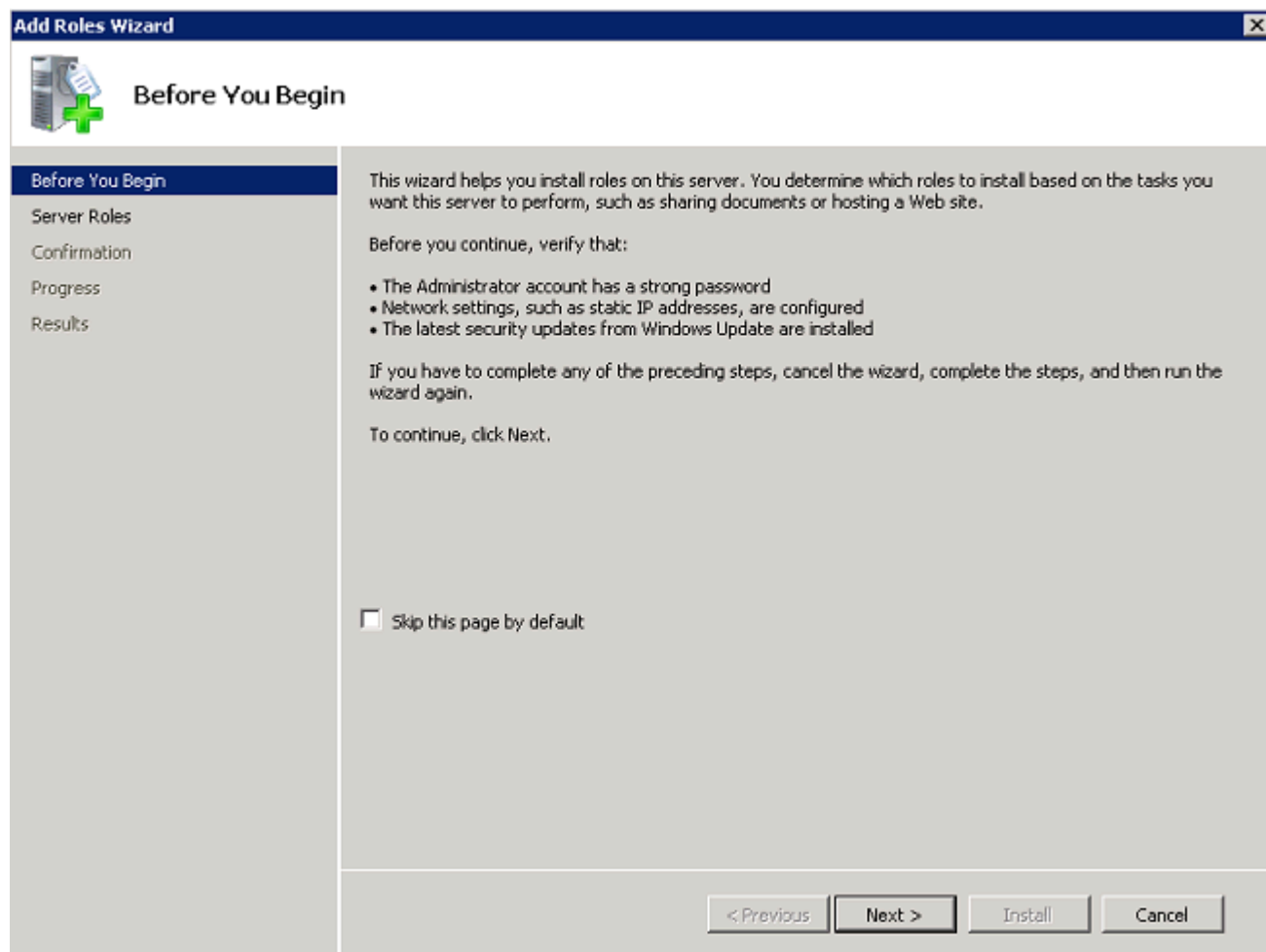
1. Fare clic su Start> Server Manager.



2. Fare clic su Ruoli> Aggiungi ruoli.

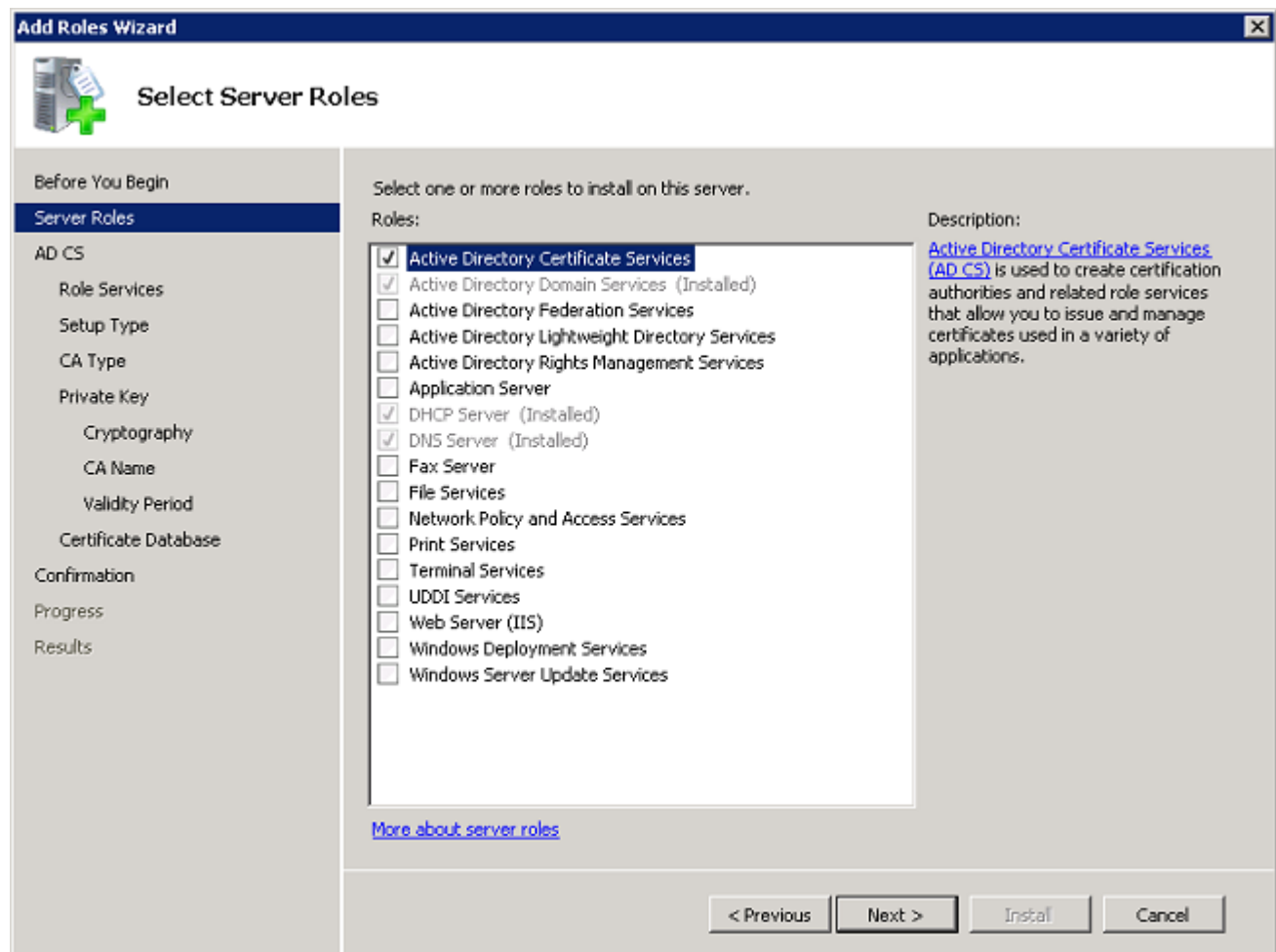


3. Fare clic su Next (Avanti).

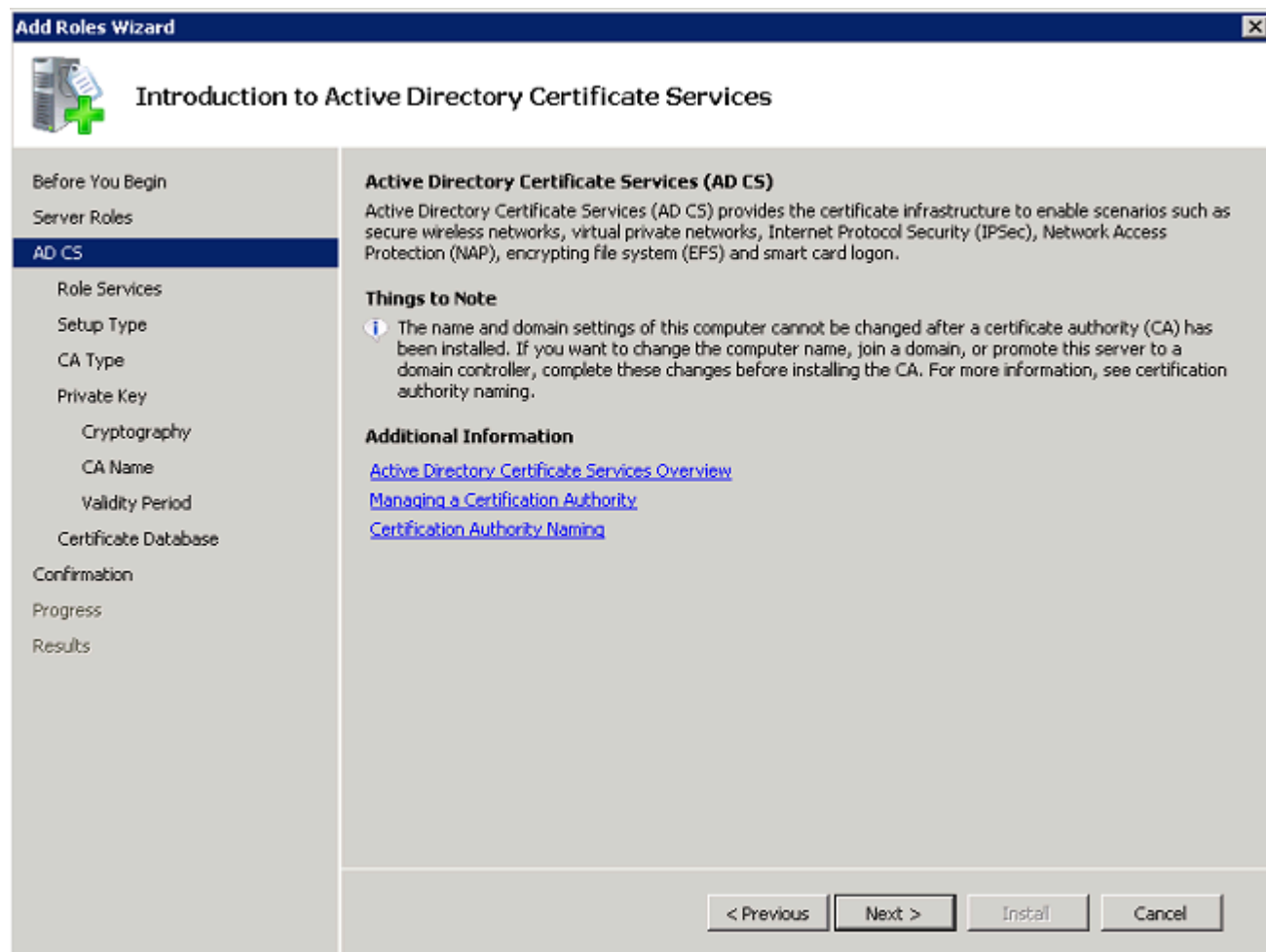


4. Selezionare il servizio Servizi certificati Active Directory e fare clic su Avanti.

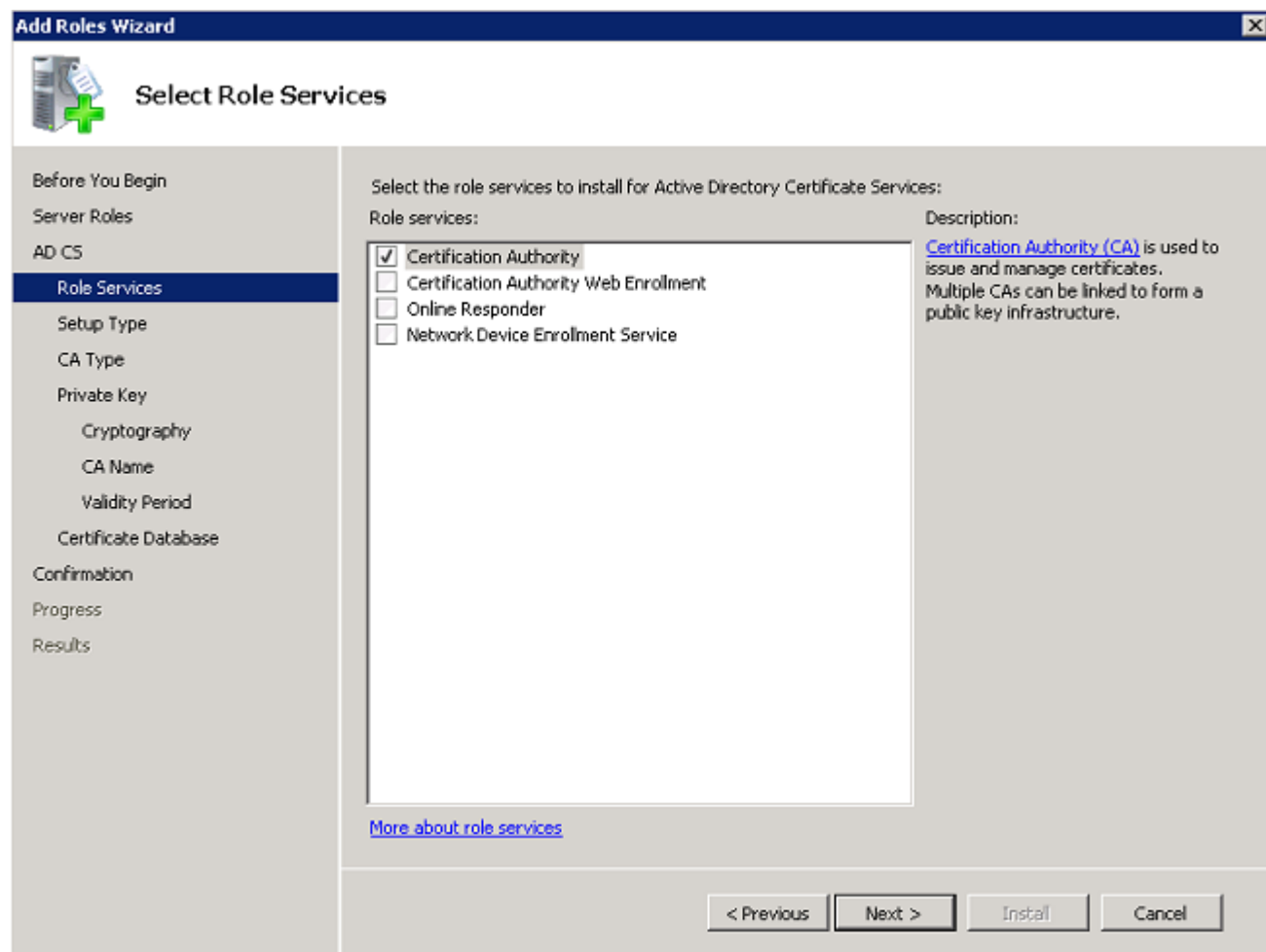




5. Rivedere l'Introduzione a Servizi certificati Active Directory e fare clic su Avanti.




6. Selezionare l'Autorità di certificazione e fare clic su Avanti.



7. Selezionare Enterprise, quindi fare clic su Next (Avanti).

**Add Roles Wizard**

 **Specify Setup Type**

Before You Begin  
Server Roles  
AD CS  
Role Services  
**Setup Type**  
CA Type  
Private Key  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

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](#)

< Previous   Next >   Install   Cancel

8. Selezionare CA radice, quindi fare clic su Avanti.

**Add Roles Wizard**

 **Specify CA Type**

**Before You Begin**

**Server Roles**

**AD CS**

Role Services

Setup Type

**CA Type**

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

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.

[More about public key infrastructure \(PKI\)](#)

< Previous   Next >   Install   Cancel

9. Selezionare Crea nuova chiave privata e fare clic su Avanti.

**Add Roles Wizard**

 **Set Up Private Key**

**Before You Begin**

**Server Roles**

**AD CS**

Role Services

Setup Type

CA Type

**Private Key**

Cryptography

CA Name

Validity Period

Certificate Database

**Confirmation**

Progress

Results

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](#)

< Previous   Next >   Install   Cancel

10. Fare clic su Next (Avanti) in Configure Cryptography for CA.

**Add Roles Wizard**

 **Configure Cryptography for CA**

Before You Begin  
Server Roles  
AD CS  
  Role Services  
  Setup Type  
  CA Type  
  Private Key  
**Cryptography**  
  CA Name  
  Validity Period  
  Certificate Database  
Confirmation  
Progress  
Results

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  
sha256


☐ 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](#)

< Previous    Next >    Install    Cancel

11. Fare clic su Avanti per accettare il nome comune predefinito per questa CA.

**Add Roles Wizard**

 **Configure CA Name**

Before You Begin  
Server Roles  
AD CS  
  Role Services  
  Setup Type  
  CA Type  
  Private Key  
  Cryptography  
**CA Name**  
  Validity Period  
  Certificate Database  
Confirmation  
Progress  
Results

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

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

Distinguished name suffix:  
DC=wireless,DC=com

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


[More about configuring a CA name](#)

< Previous    Next >    Install    Cancel

12. Selezionare la durata di validità del certificato CA e fare clic su Avanti.



**Add Roles Wizard**

 **Set Validity Period**

**Before You Begin**

**Server Roles**

**AD CS**

- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
- Validity Period**
- Certificate Database
- Confirmation
- Progress
- Results

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:

**Years**

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


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

[More about setting the certificate validity period](#)

< Previous   Next >   Install   Cancel

13. Fare clic su Avanti per accettare il percorso predefinito del database certificati.

**Add Roles Wizard**

 **Configure Certificate Database**

**Before You Begin**

**Server Roles**

**AD CS**

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

**Certificate Database**

Confirmation

Progress

Results

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 Browse...

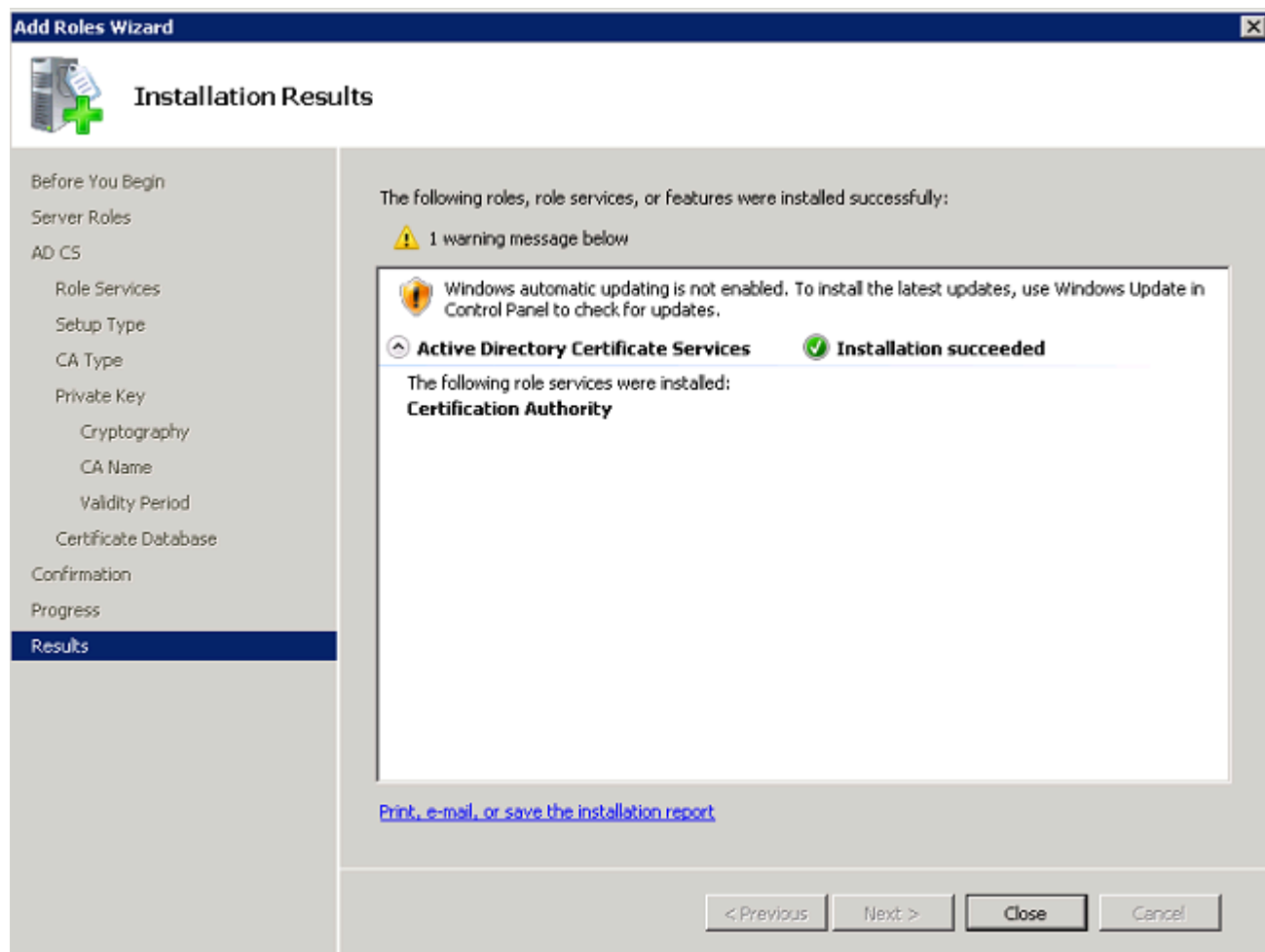
☐ Use existing certificate database from previous installation at this location

Certificate database log location:

C:\Windows\system32\CertLog Browse...

< Previous Next > Install Cancel

14. Verificare la configurazione e fare clic su Installa per avviare Servizi certificati Active Directory.

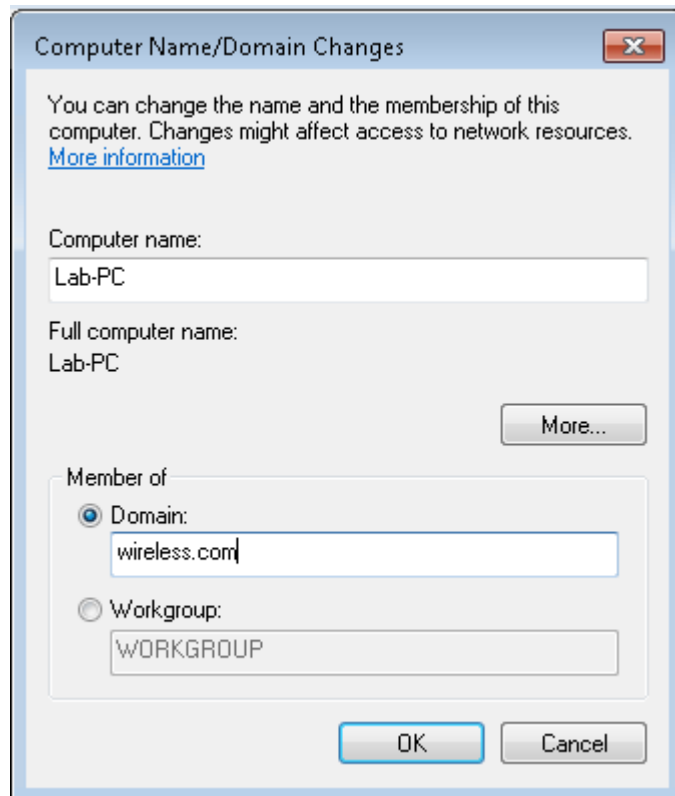


15. Al termine dell'installazione, fare clic su Chiudi.

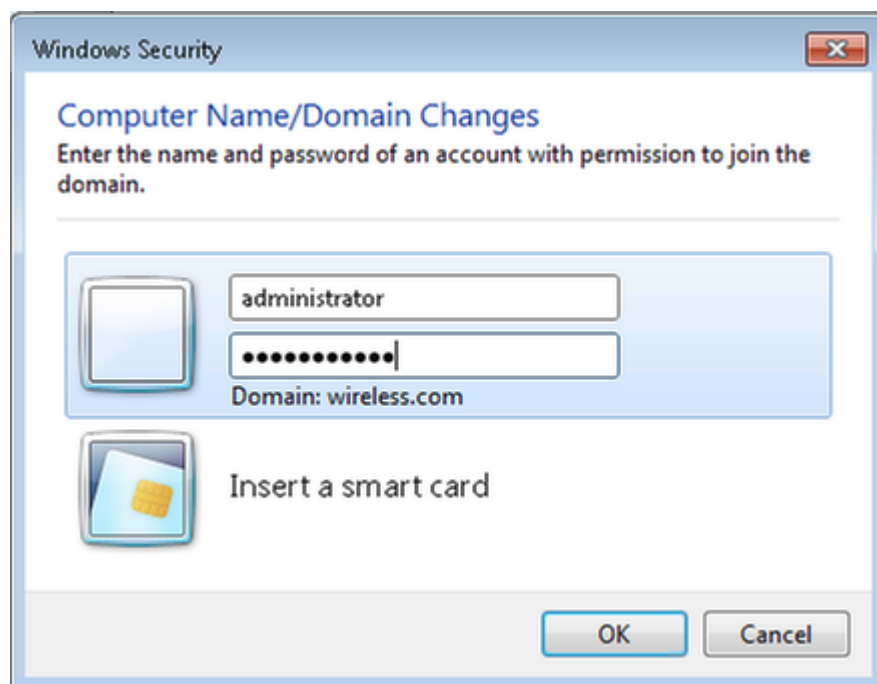
#### Connetti client al dominio

Completare questa procedura per connettere i client alla rete cablata e scaricare le informazioni specifiche del dominio dal nuovo dominio:

1. Collegare i client alla rete cablata con un cavo Ethernet straight-through.
2. Avviare il client e accedere con il nome utente e la password del client.
3. Fare clic su Start>Esegui, immettere cmd e fare clic su OK.
4. Al prompt dei comandi, immettere ipconfig e fare clic su Enter per verificare che DHCP funzioni correttamente e che il client abbia ricevuto un indirizzo IP dal server DHCP.
5. Per aggiungere il client al dominio, fare clic su Start, fare clic con il pulsante destro del mouse su Computer, scegliere Proprietà e scegliere Modifica impostazioni in basso a destra.
6. Fare clic su Cambia.
7. Fare clic su Dominio, immettere il nome di dominio, wireless, per questo esempio, e fare clic su OK.



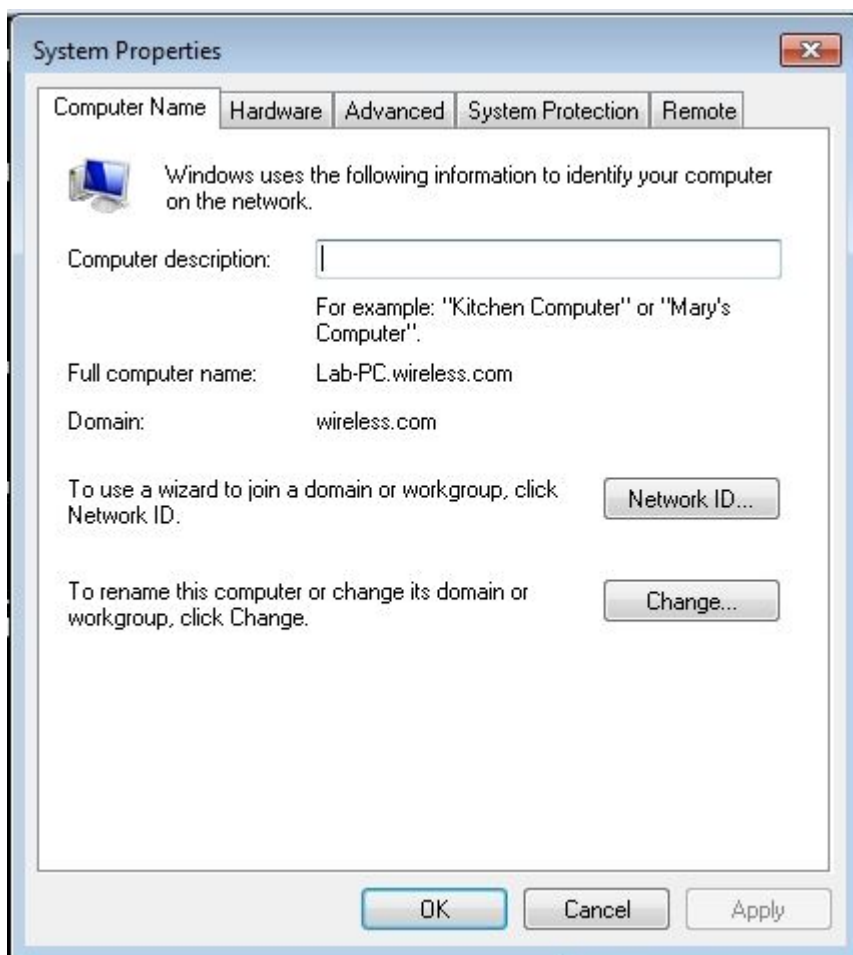
8. Immettere il nome utente administrator e la password specifica del dominio a cui il client viene aggiunto. Si tratta dell'account amministratore in Active Directory sul server.



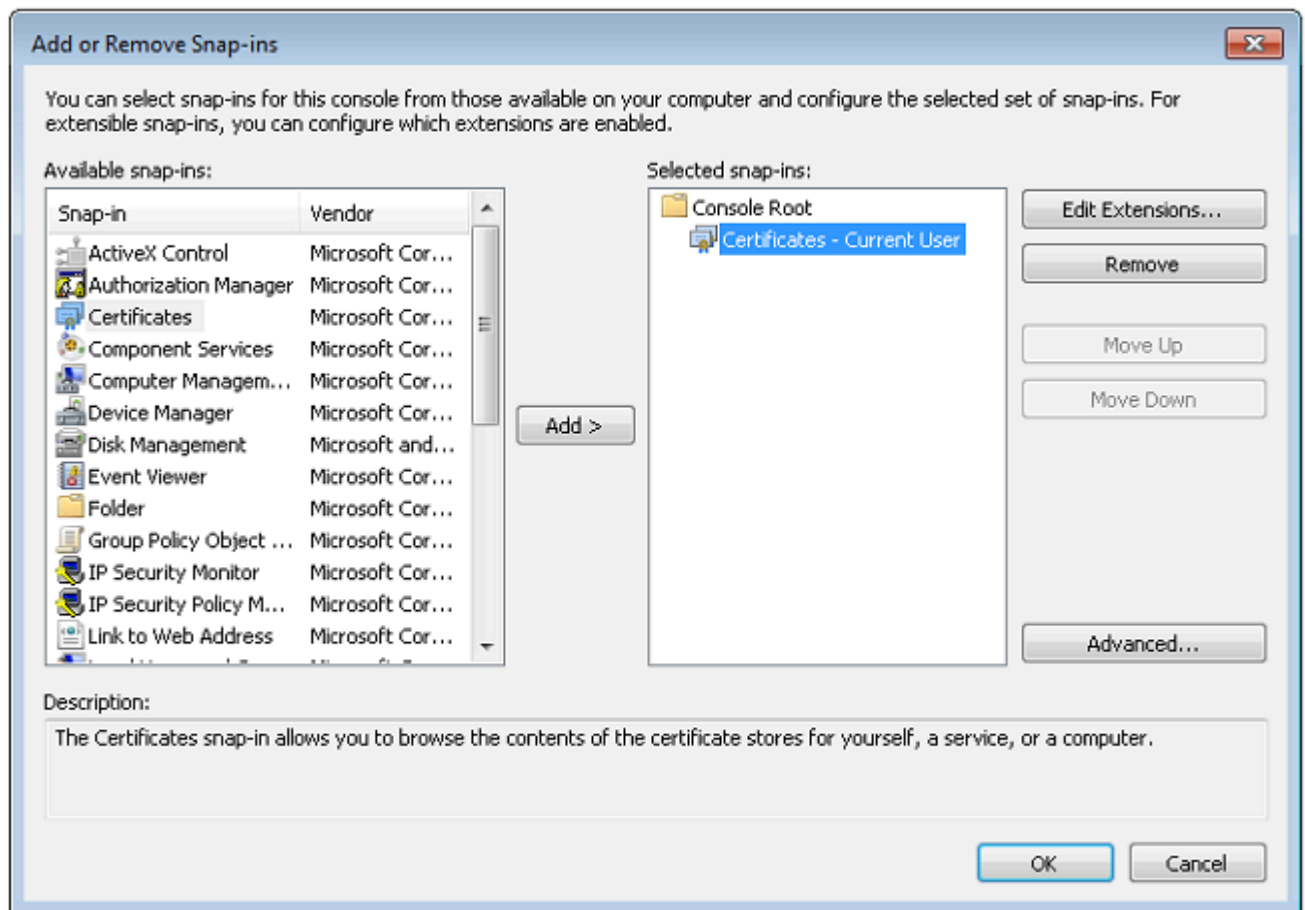
9. Fare clic su OK, quindi fare di nuovo clic su OK.



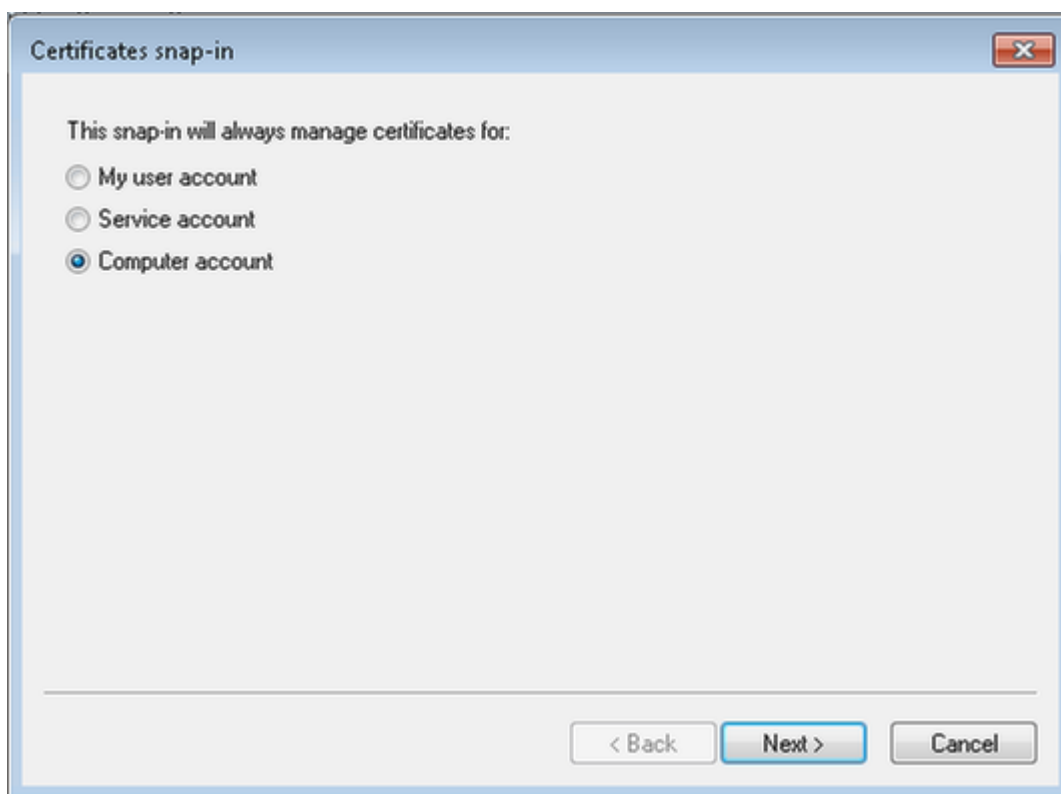
10. Fare clic su Close>Restart Now (Chiudi>Riavvia ora) per riavviare il computer.
11. Una volta riavviato il computer, accedere con: Username = Amministratore; Password = <password dominio>; Domain = wireless.
12. Fare clic su Start, fare clic con il pulsante destro del mouse su Computer, scegliere Proprietà, quindi selezionare Modifica impostazioni in basso a destra per verificare di appartenere al dominio wireless.
13. Il passaggio successivo consiste nel verificare che il client abbia ricevuto il certificato CA (trust) dal server.



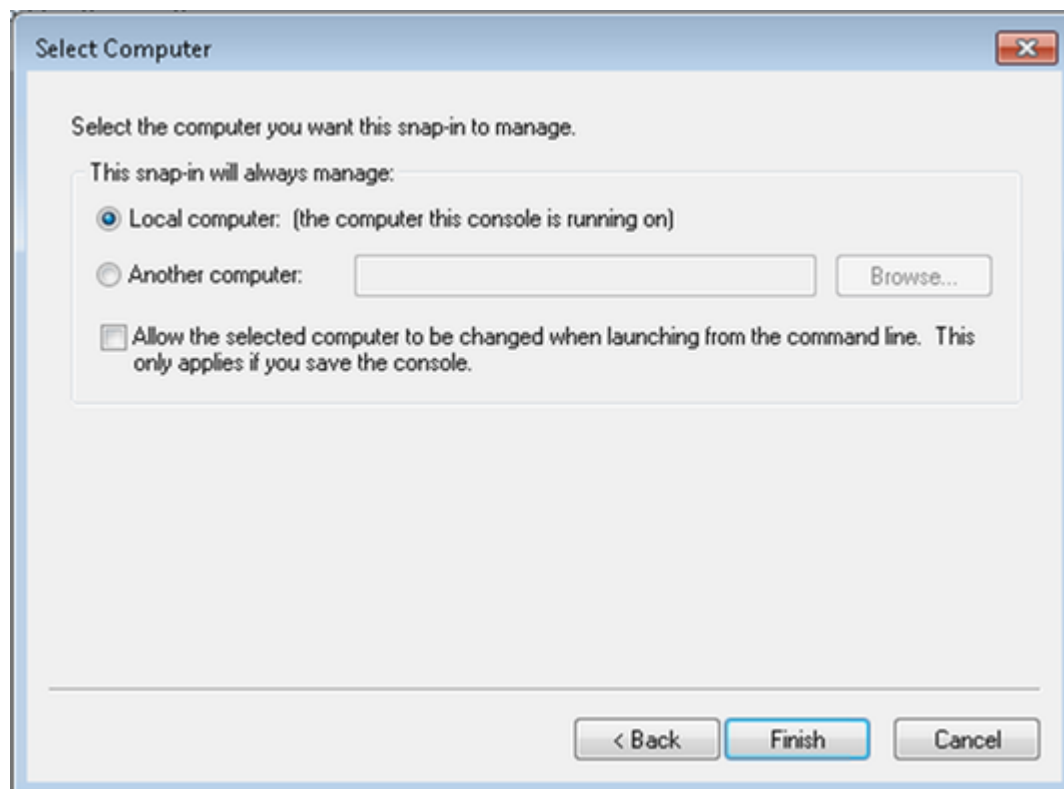
14. Fare clic su Start, immettere mmc e premere Invio.
15. Fare clic su File, quindi su Aggiungi/Rimuovi snap-in.
16. Scegliere Certificati, quindi fare clic su Aggiungi.



17. Fare clic su Account computer e quindi su Avanti.

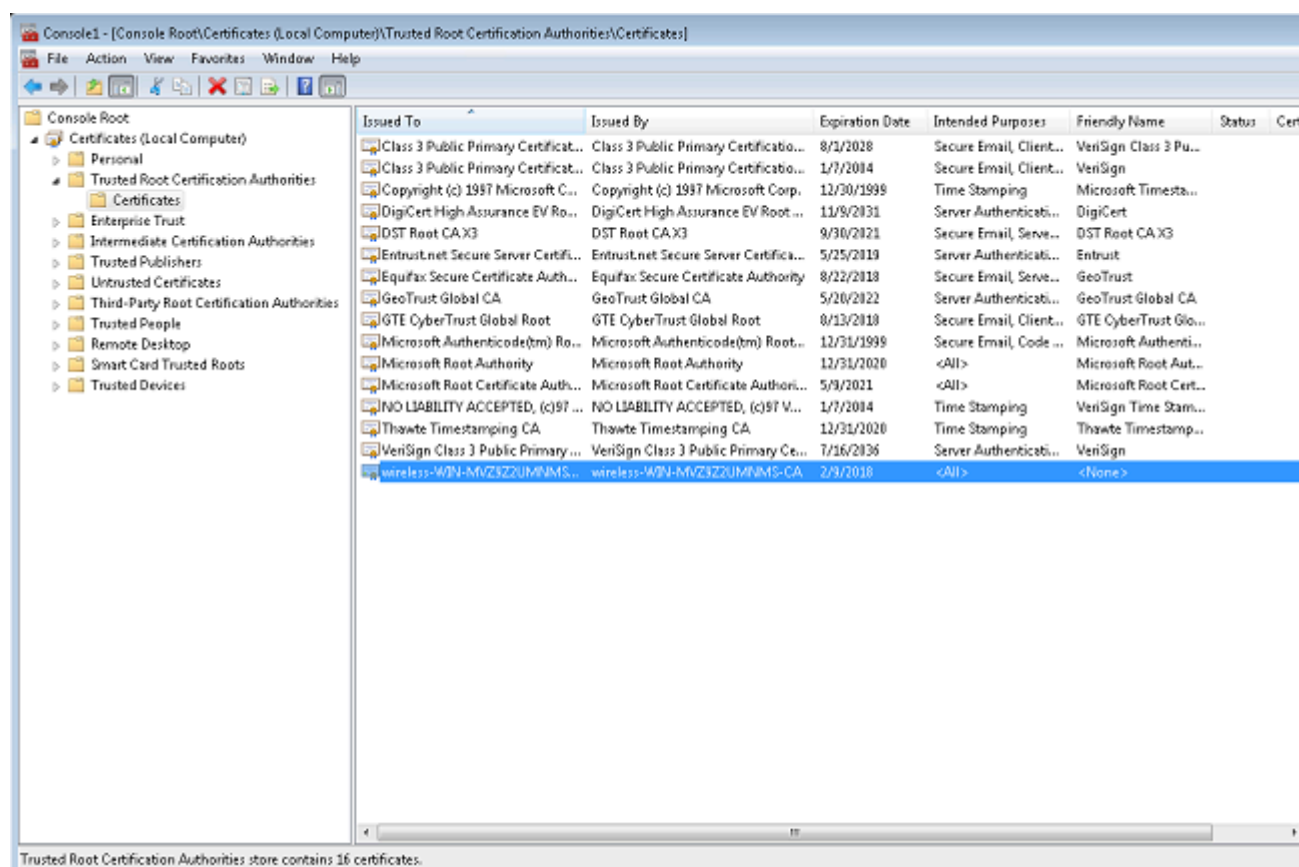


18. Fare clic su Computer locale e quindi su Avanti.



19. Fare clic su OK.

20. Espandere le cartelle Certificati (computer locale) e Autorità di certificazione radice attendibili e fare clic su Certificati. Trovare il certificato CA del dominio wireless nell'elenco. In questo esempio, il certificato CA è denominato wireless-WIN-MVZ9Z2UMNMS-CA.

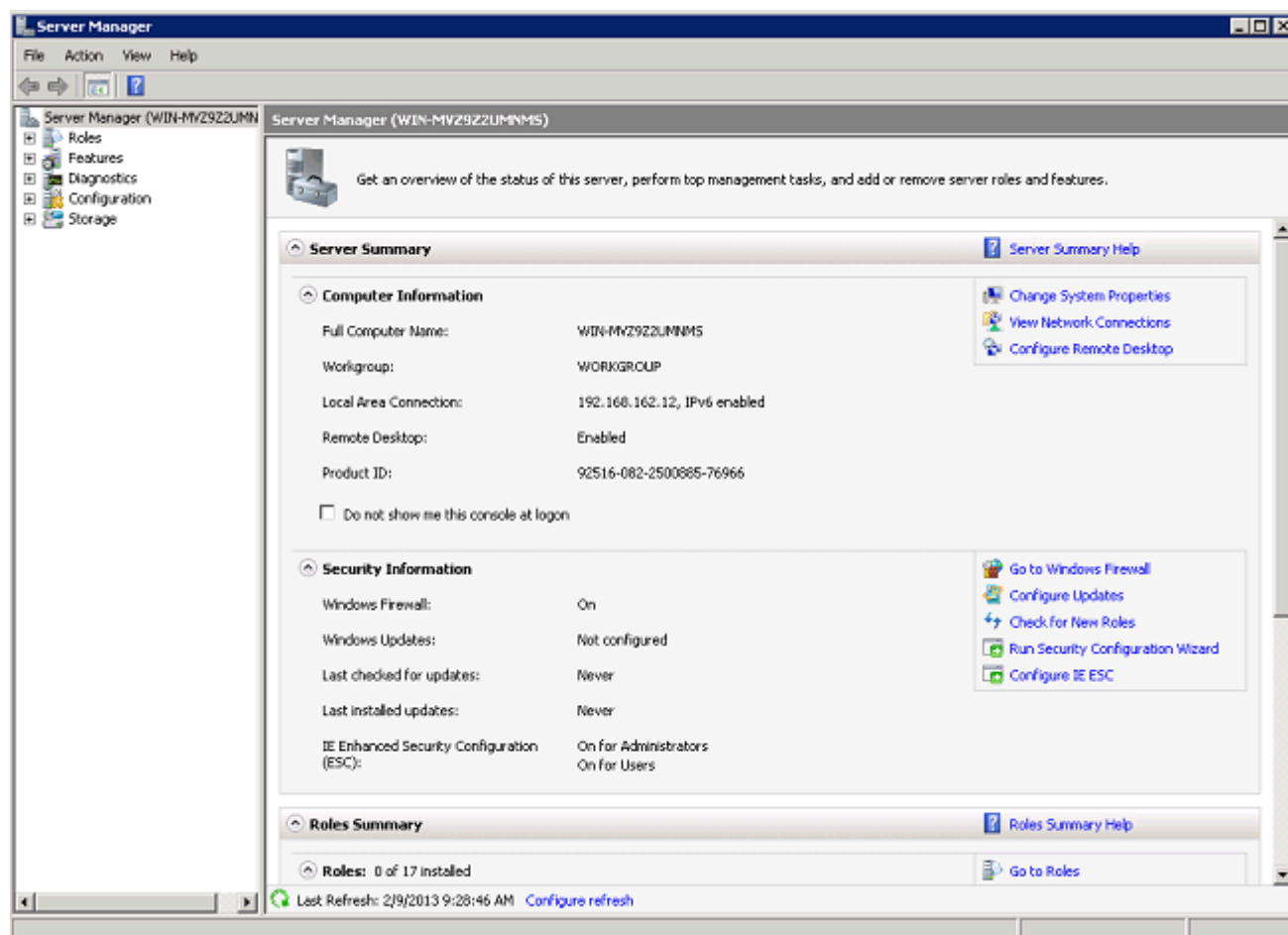


21. Ripetere questa procedura per aggiungere altri client al dominio.

Installare Server dei criteri di rete in Microsoft Windows 2008 Server

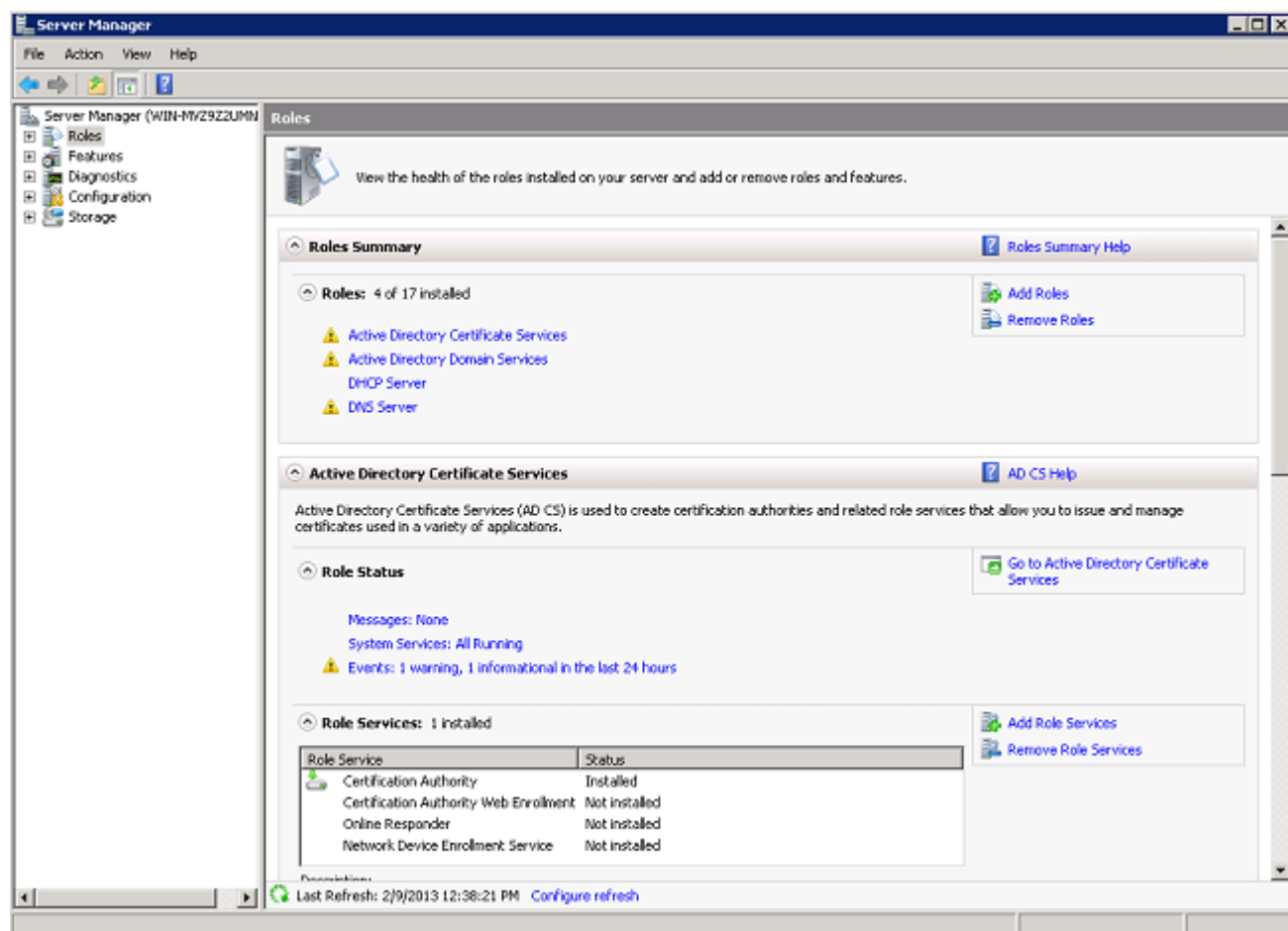
In questa installazione Server dei criteri di rete viene utilizzato come server RADIUS per autenticare i client wireless con l'autenticazione PEAP. Per installare e configurare Server dei criteri di rete nel server Microsoft Windows 2008, completare la procedura seguente:

1. Fare clic su Start> Server Manager.

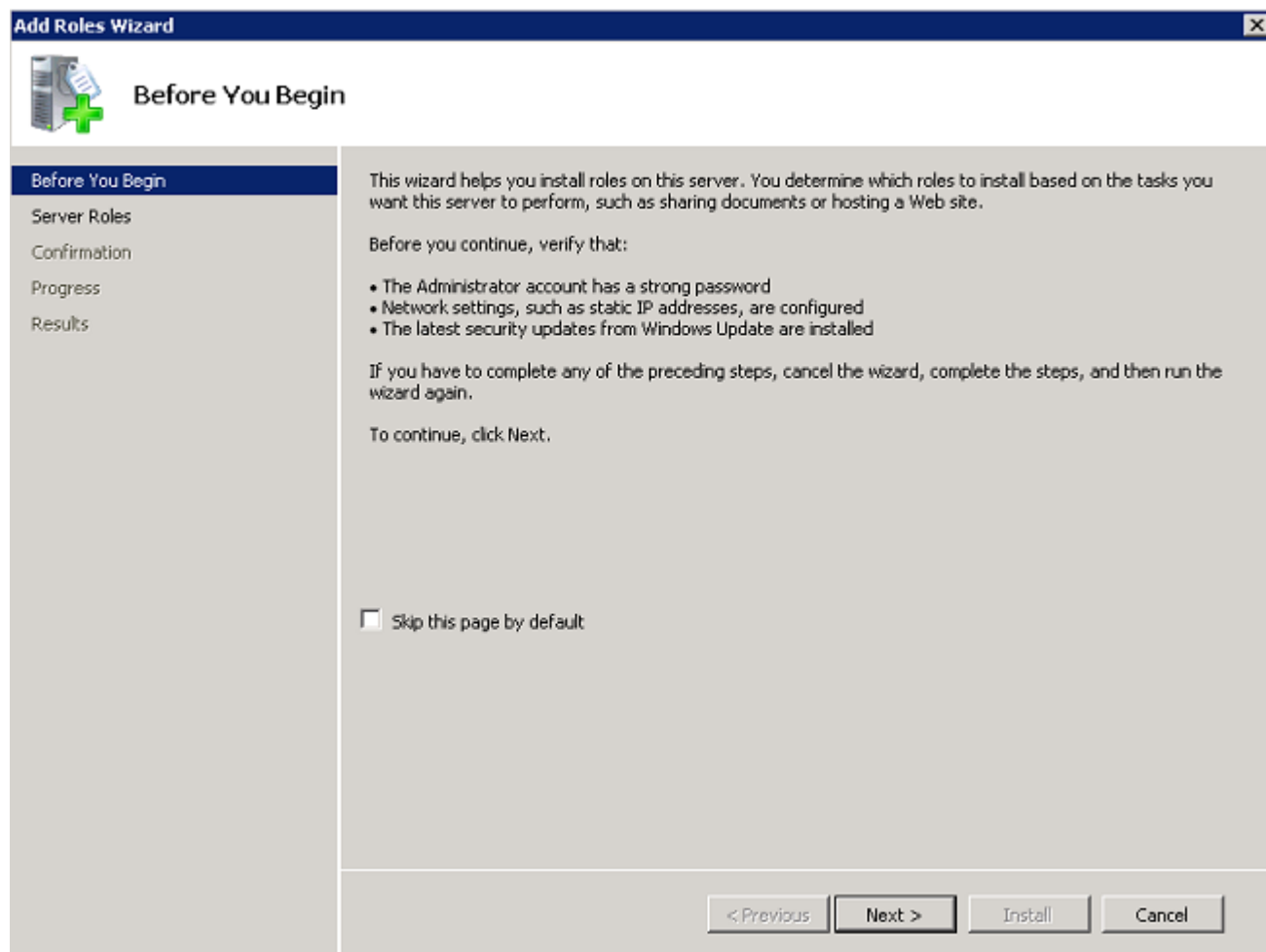


2. Fare clic su Ruoli> Aggiungi ruoli.

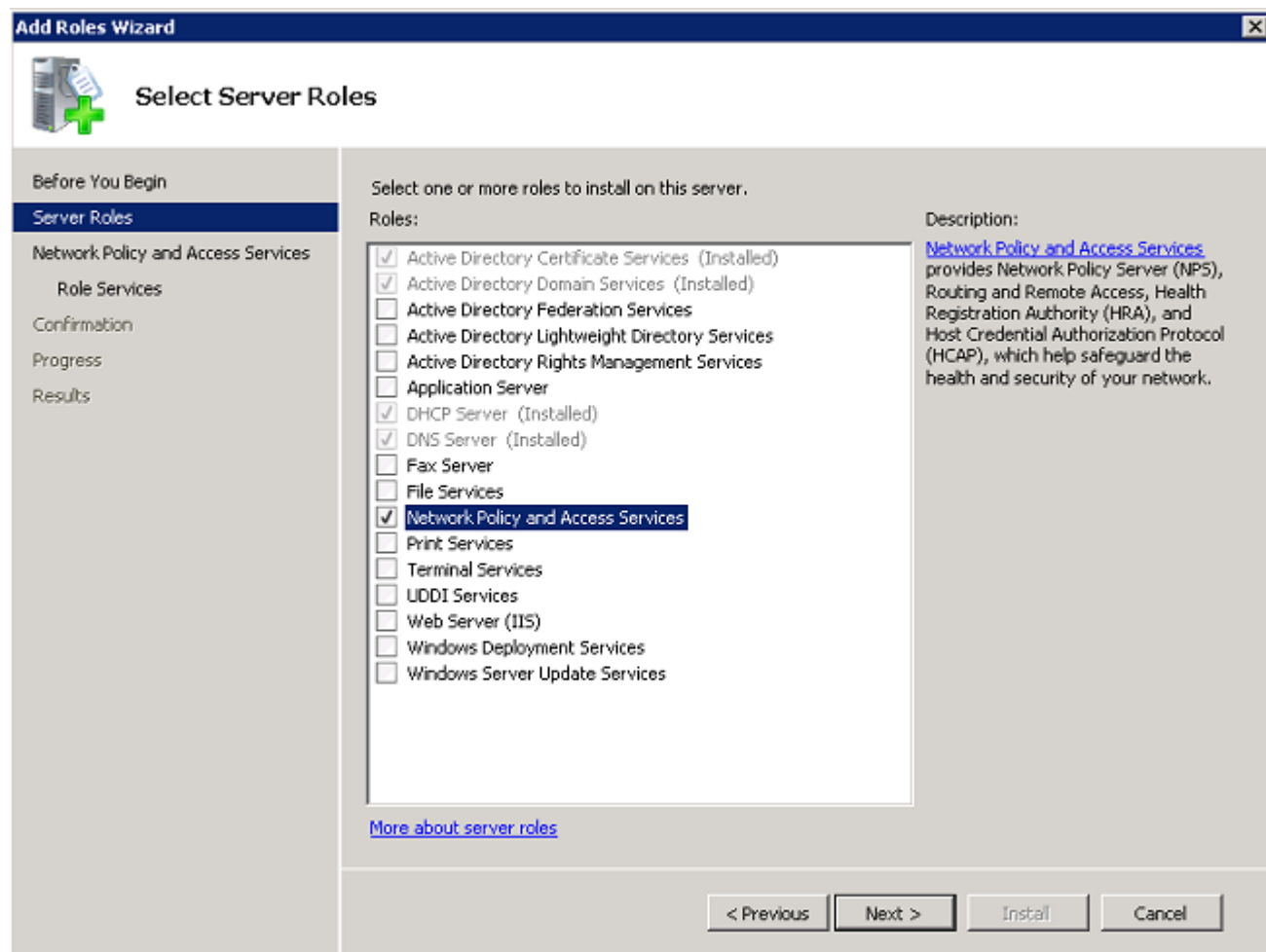




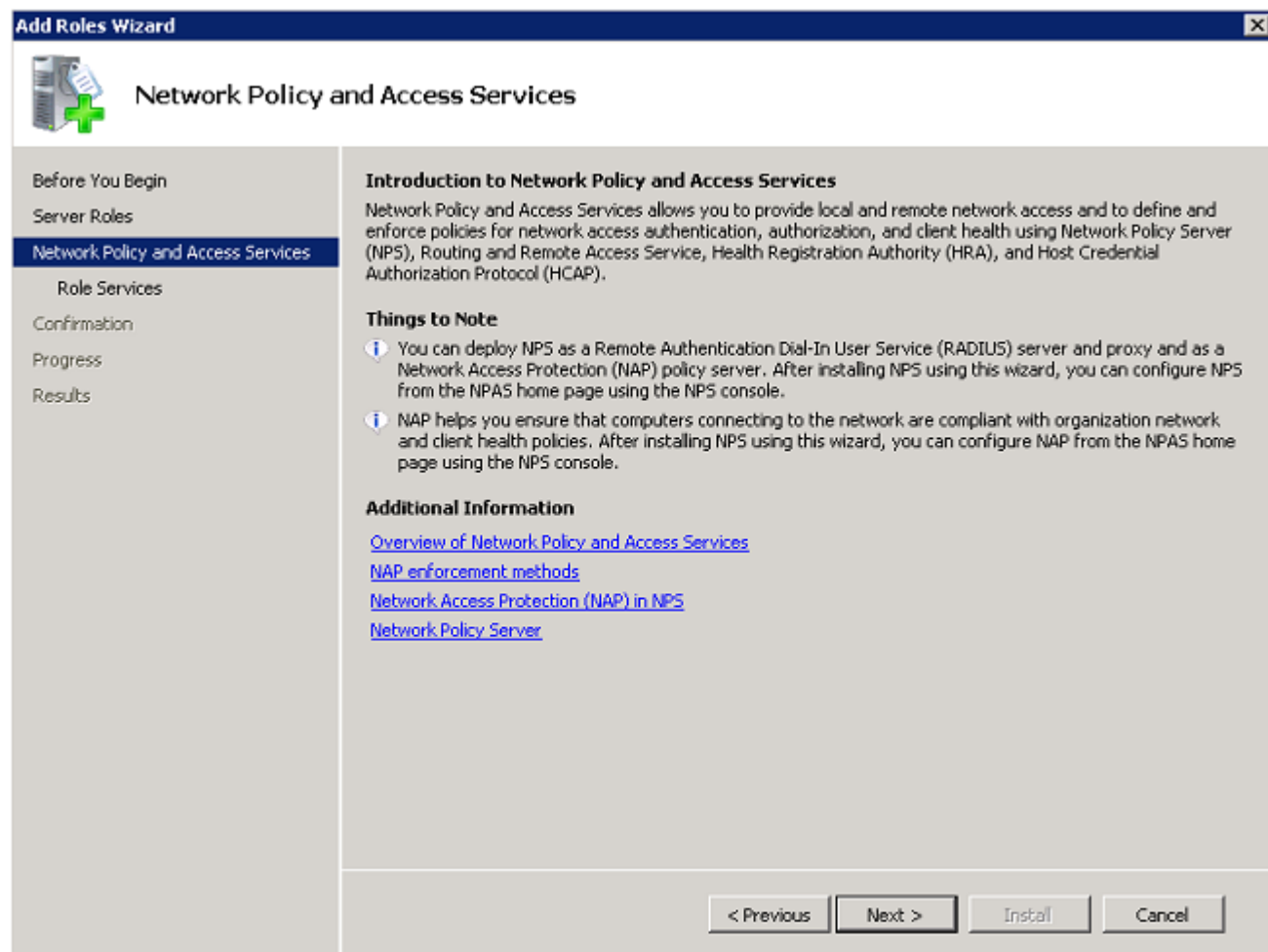
3. Fare clic su Next (Avanti).



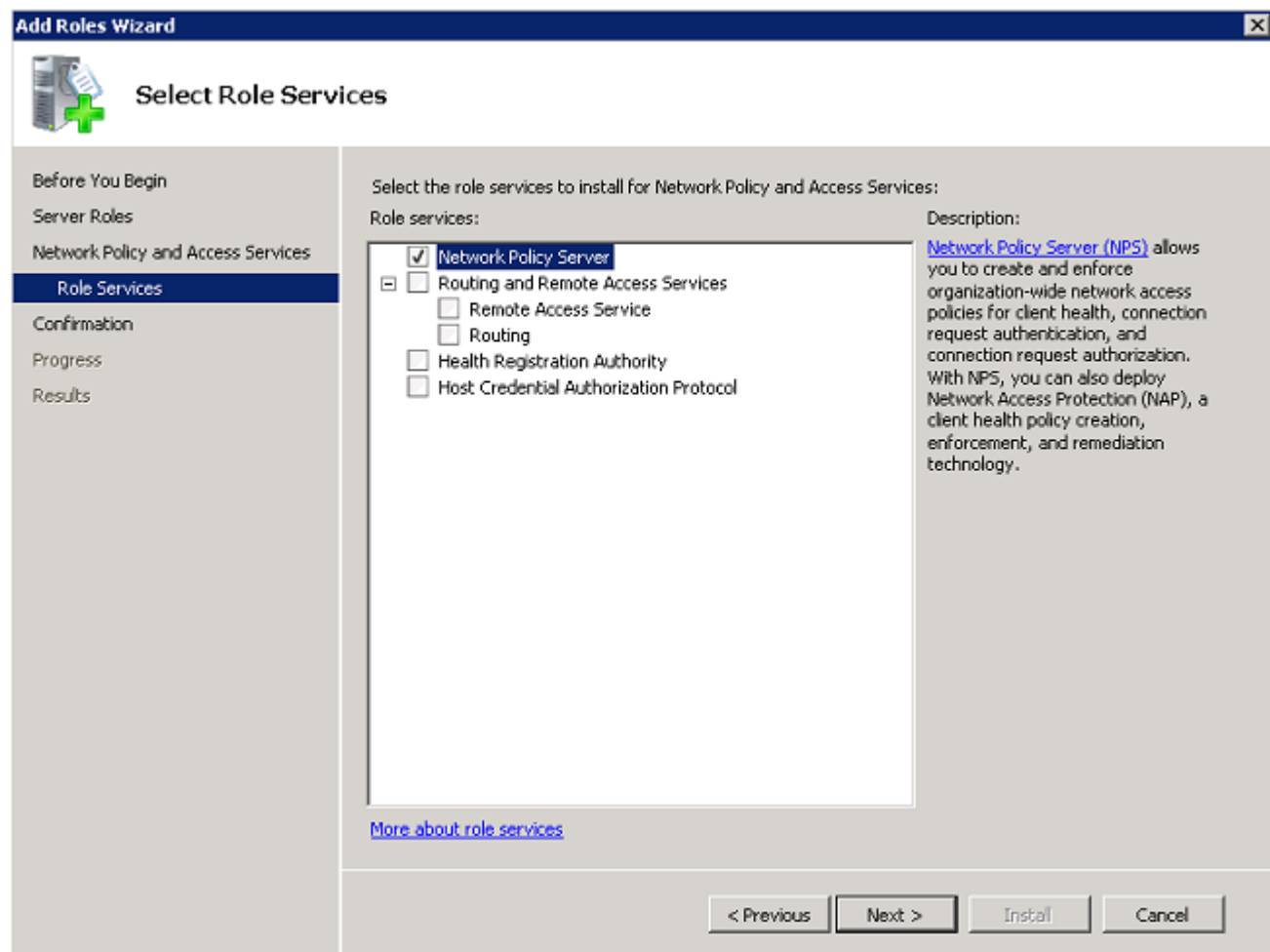
4. Selezionare il servizio Servizi di accesso e criteri di rete e fare clic su Avanti.



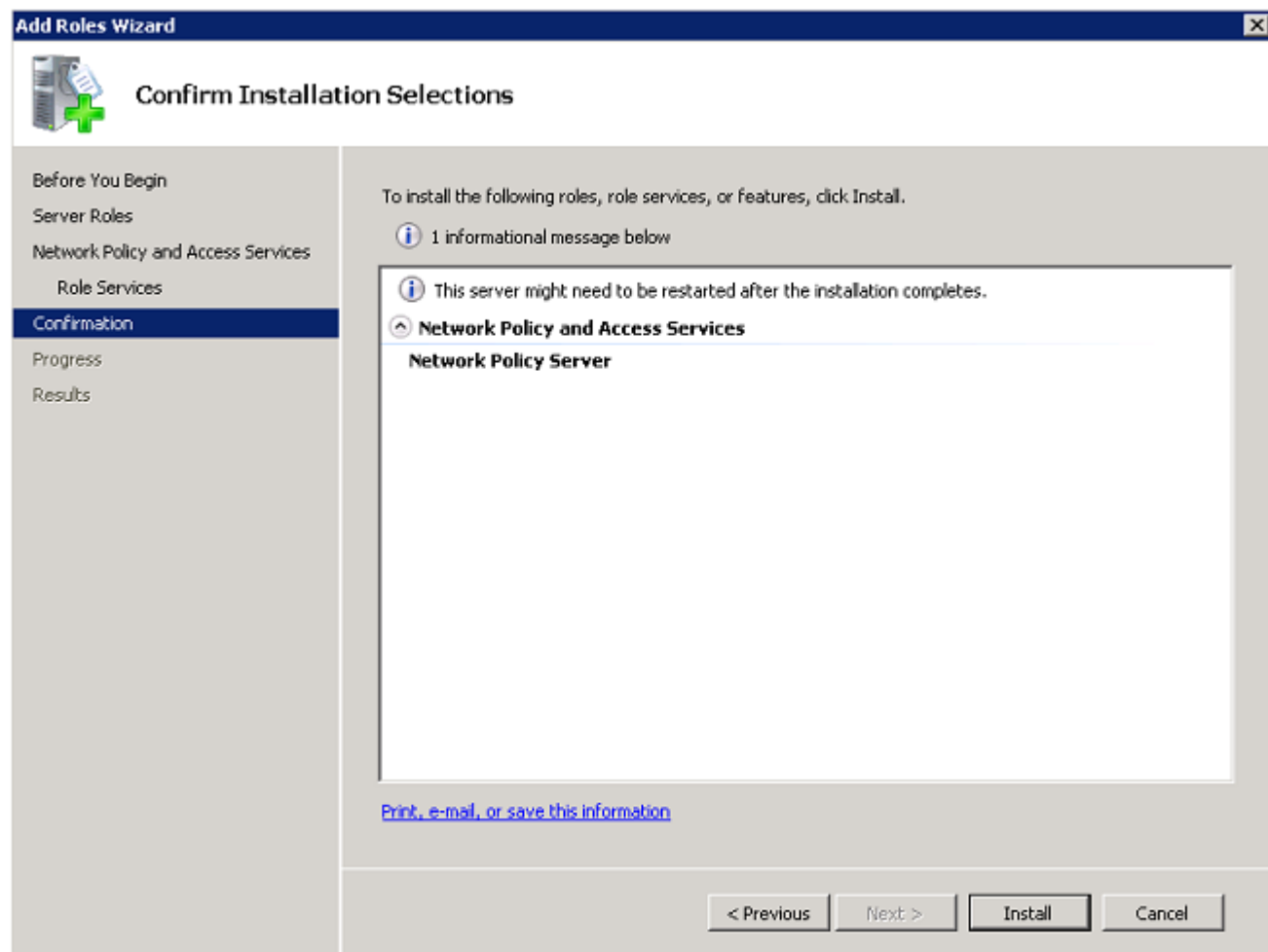
5. Rivedere l'Introduzione a Servizi di accesso e criteri di rete e fare clic su Avanti.



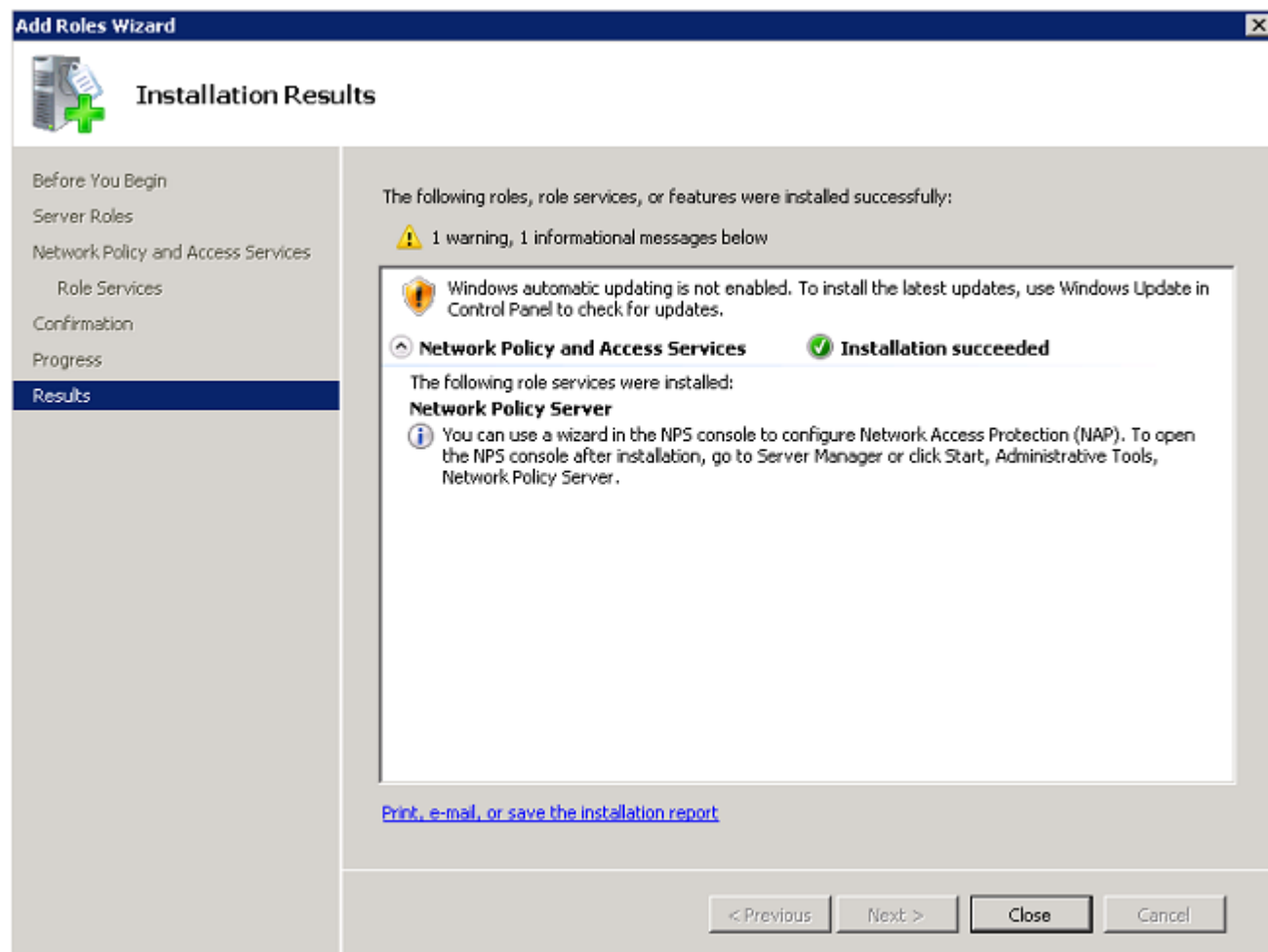
6. Selezionare Server dei criteri di rete, quindi fare clic su Avanti.



7. Verificare la conferma e fare clic su Installa.



Al termine dell'installazione, viene visualizzata una schermata simile a questa.

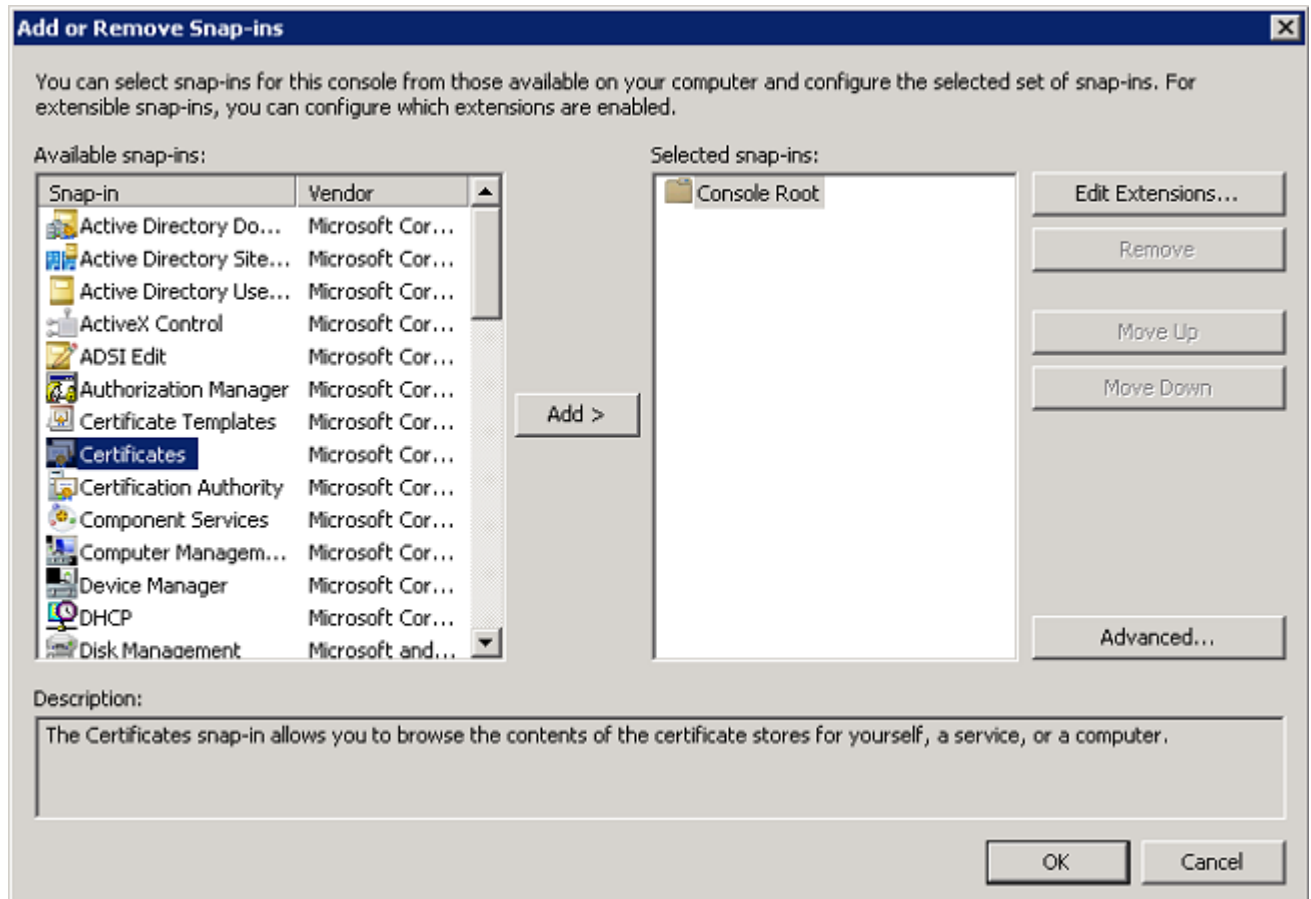


8. Fare clic su Close (Chiudi).

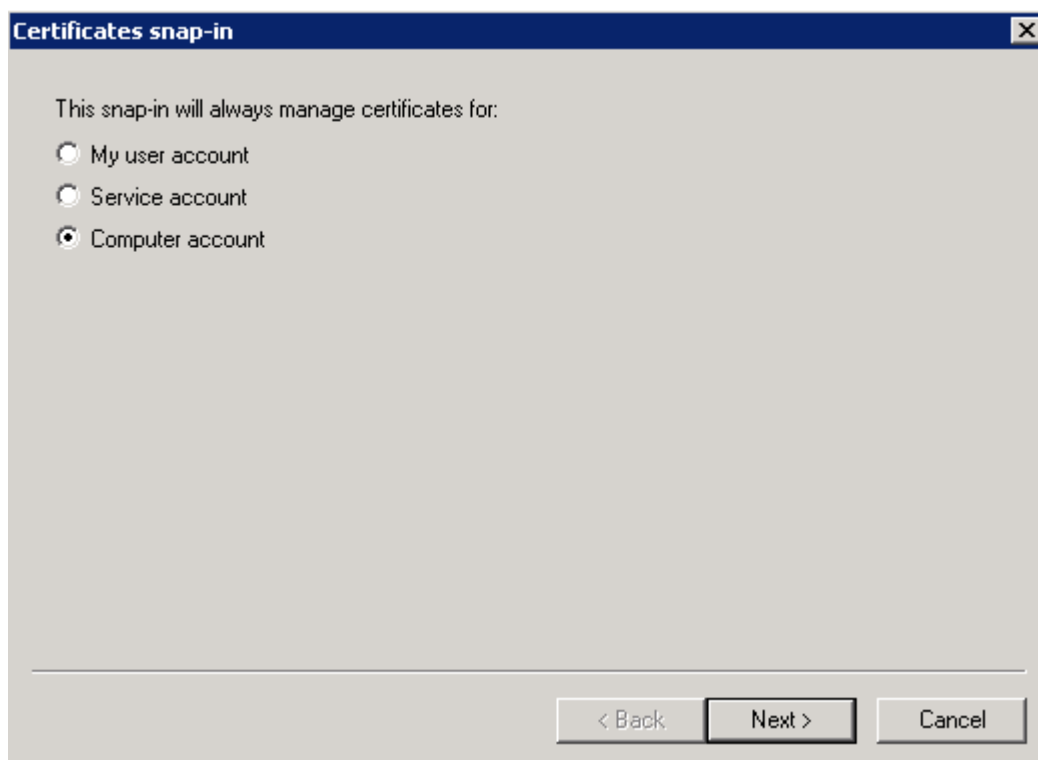
## Installa un certificato

Per installare il certificato del computer per Server dei criteri di rete, completare la procedura seguente:

1. Fare clic su Start, immettere mmc e premere Invio.
2. Fare clic su File > Aggiungi/Rimuovi snap-in.
3. Scegliere Certificati, quindi fare clic su Aggiungi.

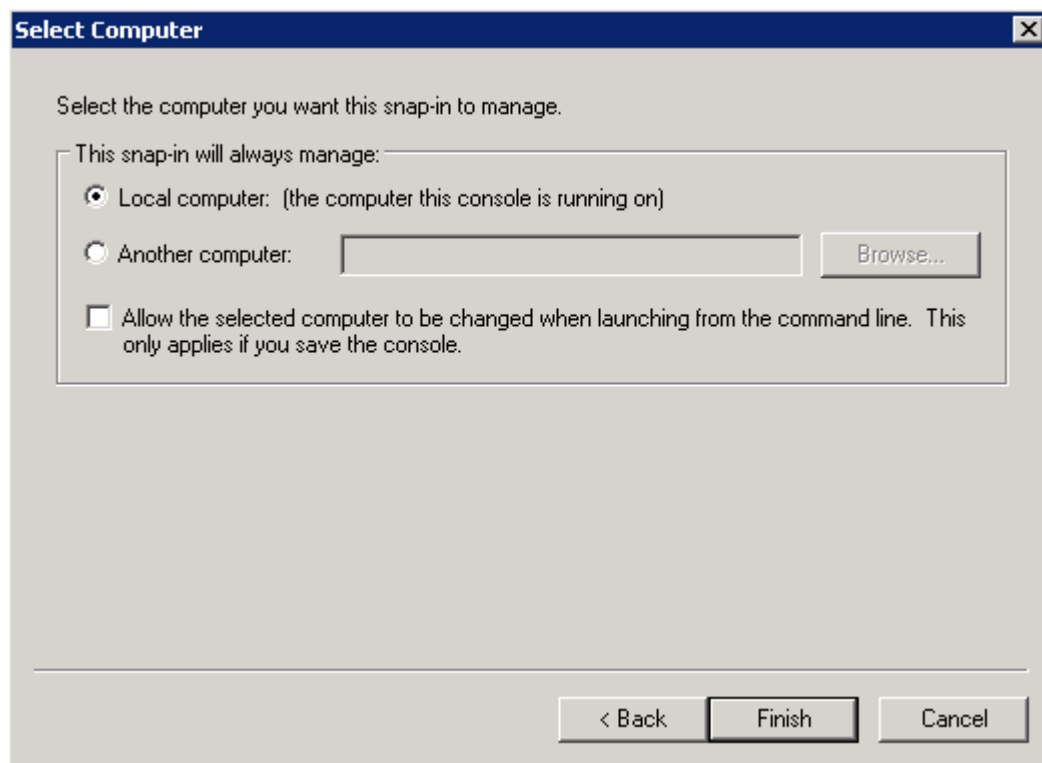


4. Scegliere Account computer e fare clic su Avanti.

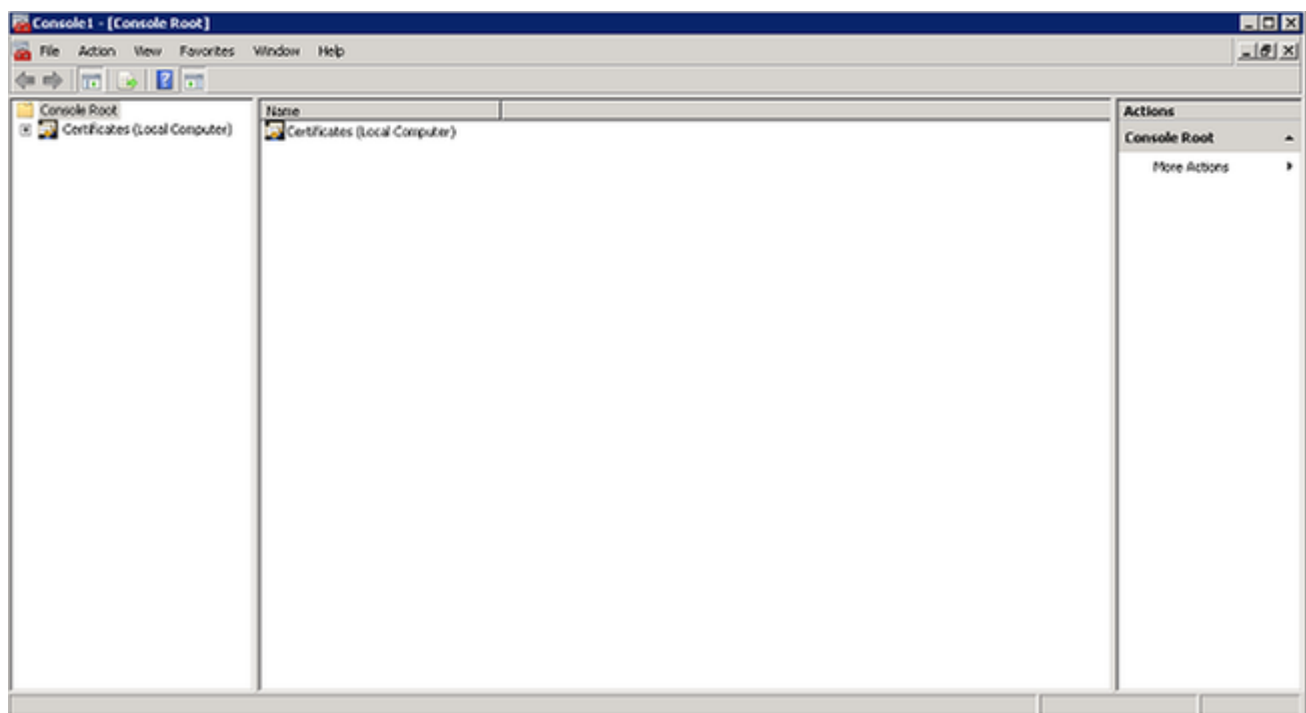


5. Selezionare Computer locale e fare clic su Fine.

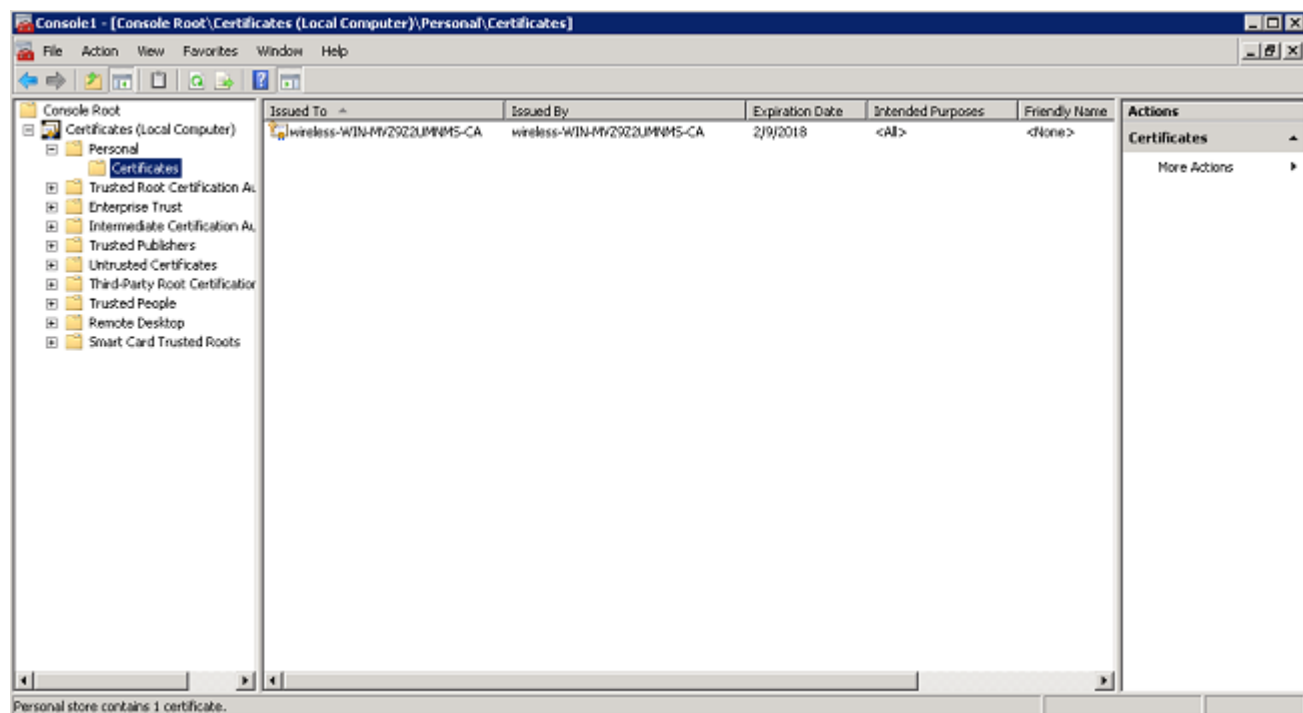




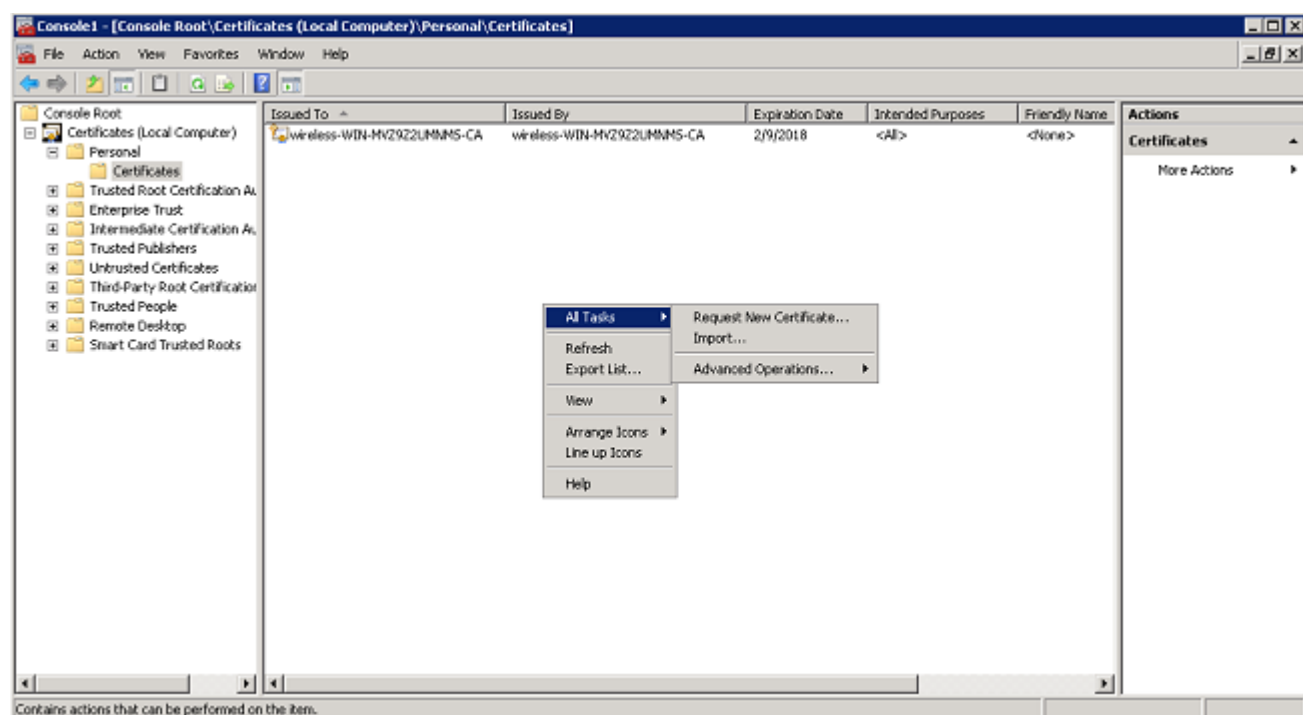
6. Fare clic su OK per tornare a Microsoft Management Console (MMC).



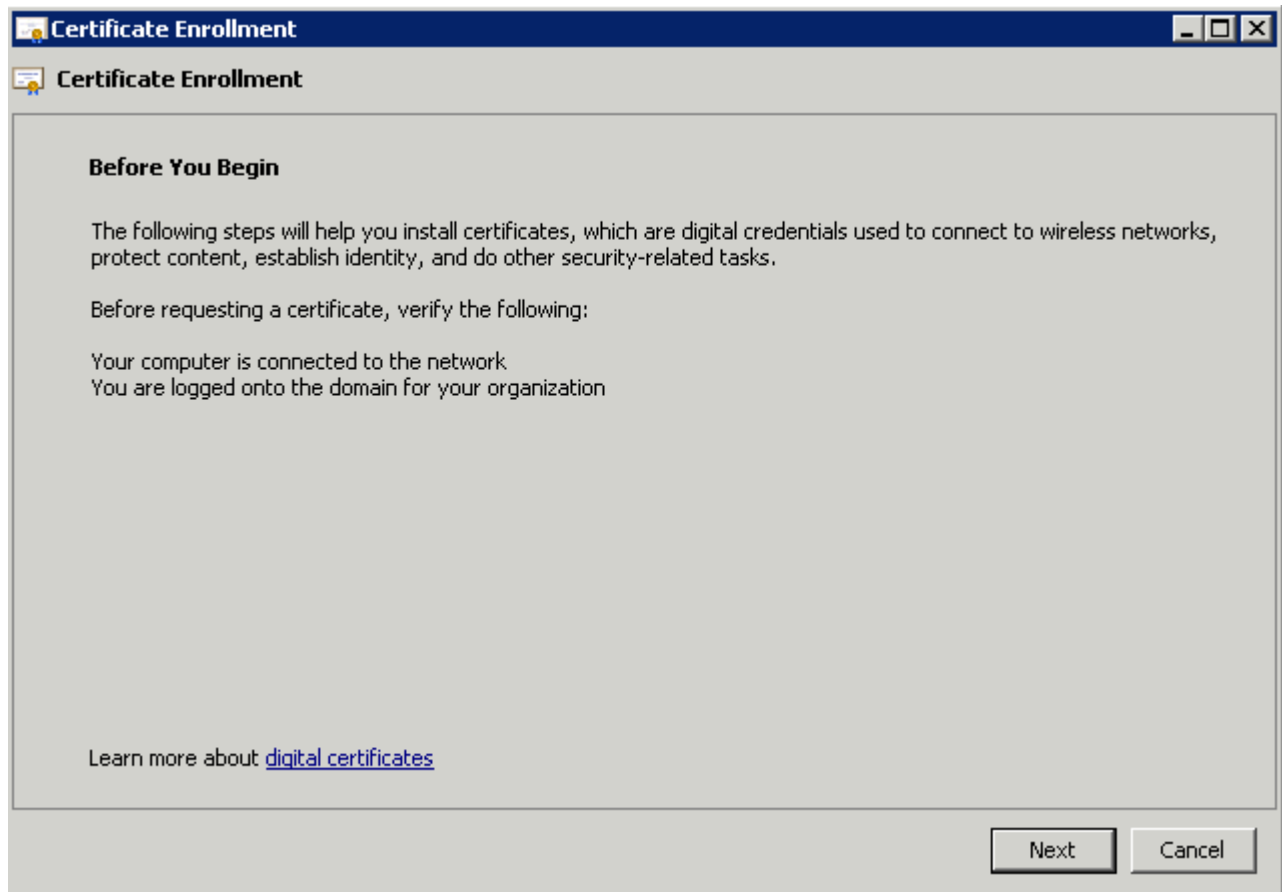
7. Espandere le cartelle Certificati (computer locale) e Personale e fare clic su Certificati.



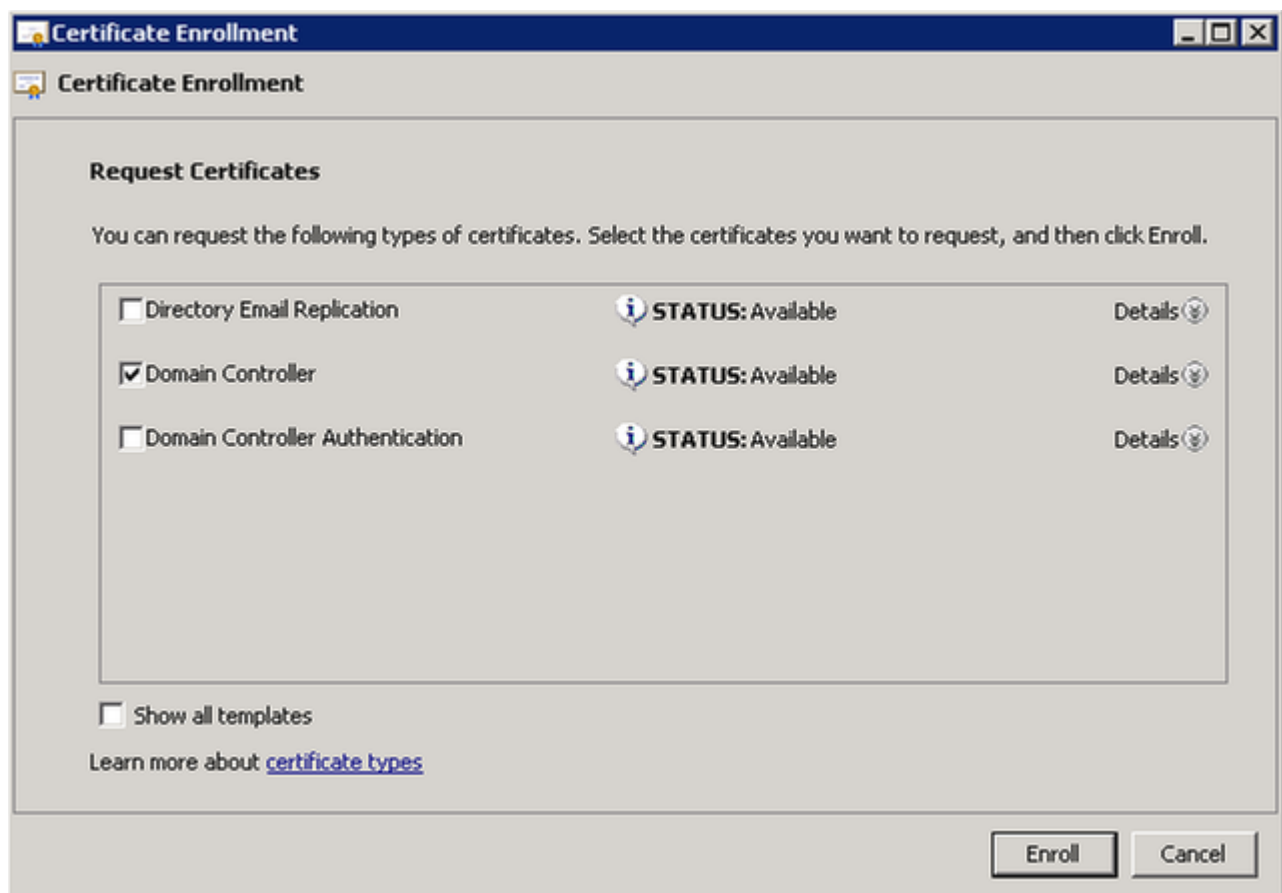
8. Fare clic con il pulsante destro del mouse nello spazio sotto il certificato CA e scegliere Tutte le attività > Richiedi nuovo certificato.



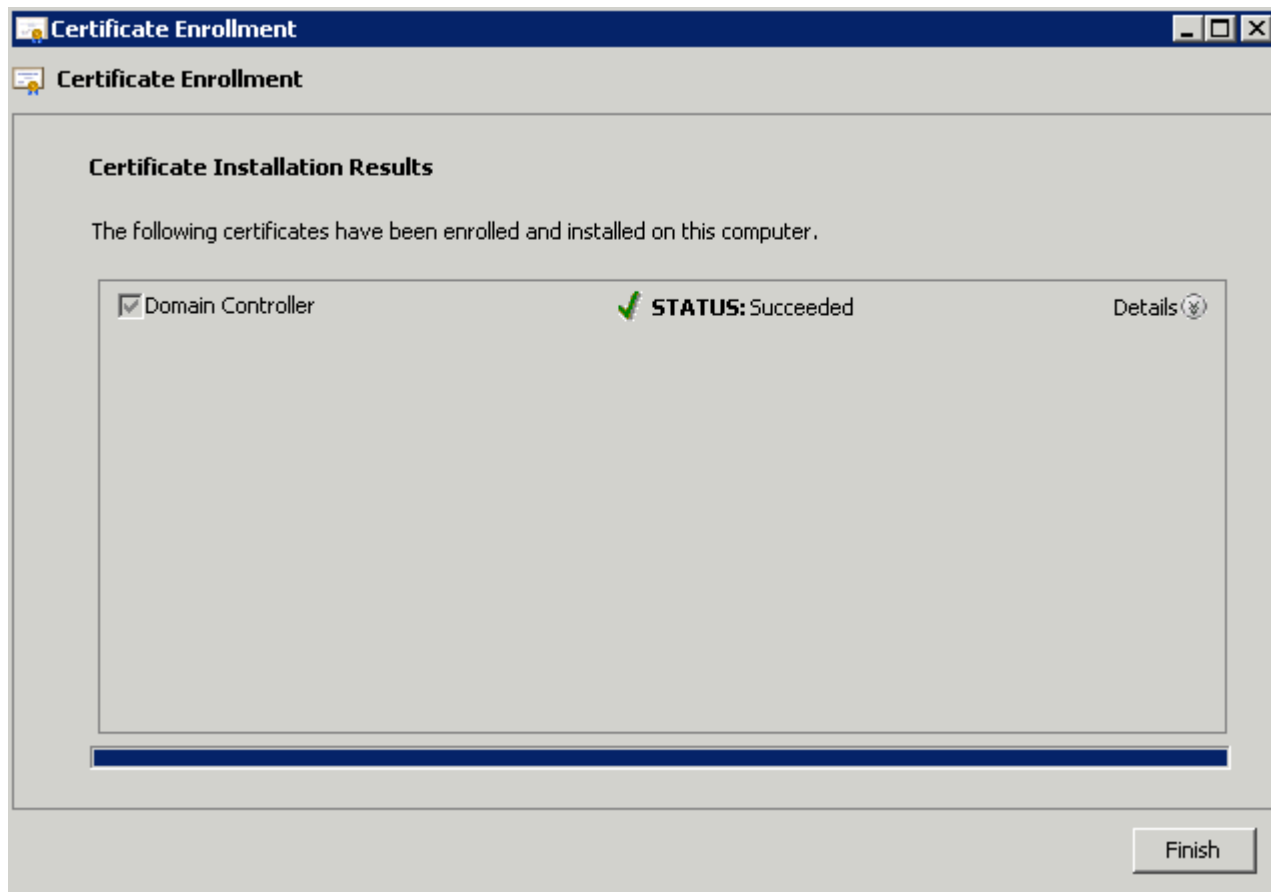
9. Fare clic su Next (Avanti).



10. Selezionare Controller di dominio, quindi fare clic su Registra.

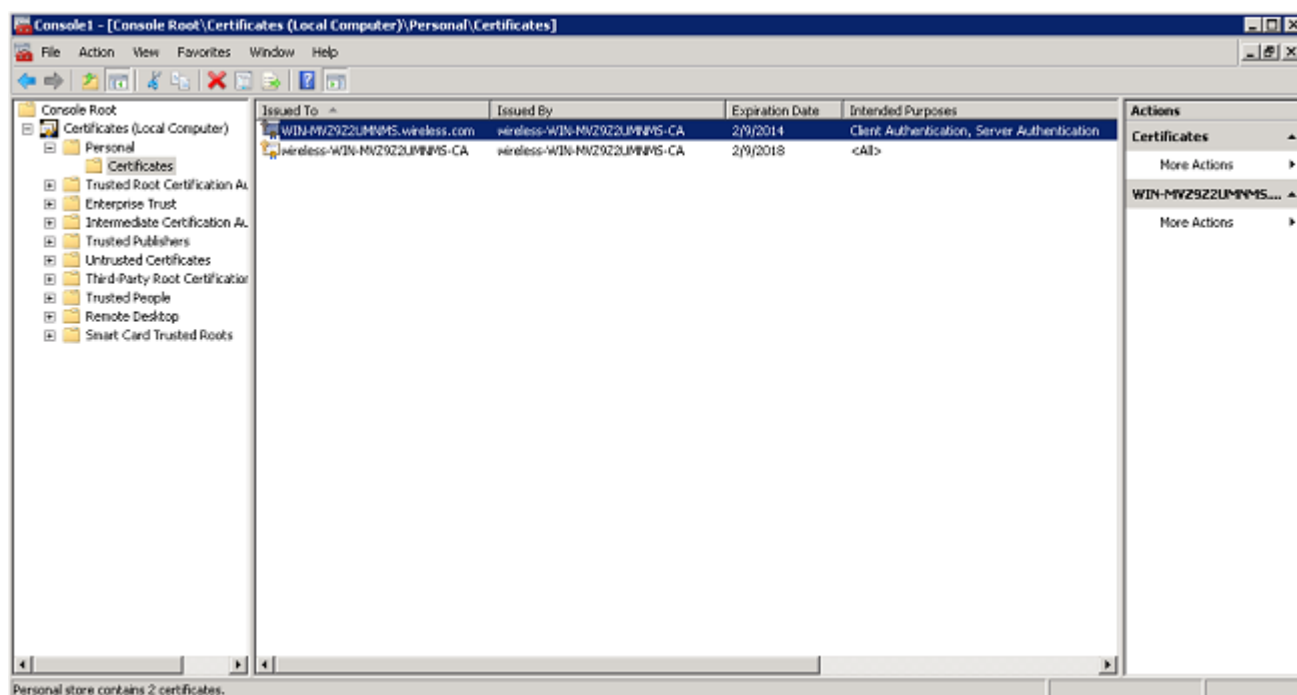


11. Una volta installato il certificato, fare clic su Fine.



Il certificato del Server dei criteri di rete è installato.

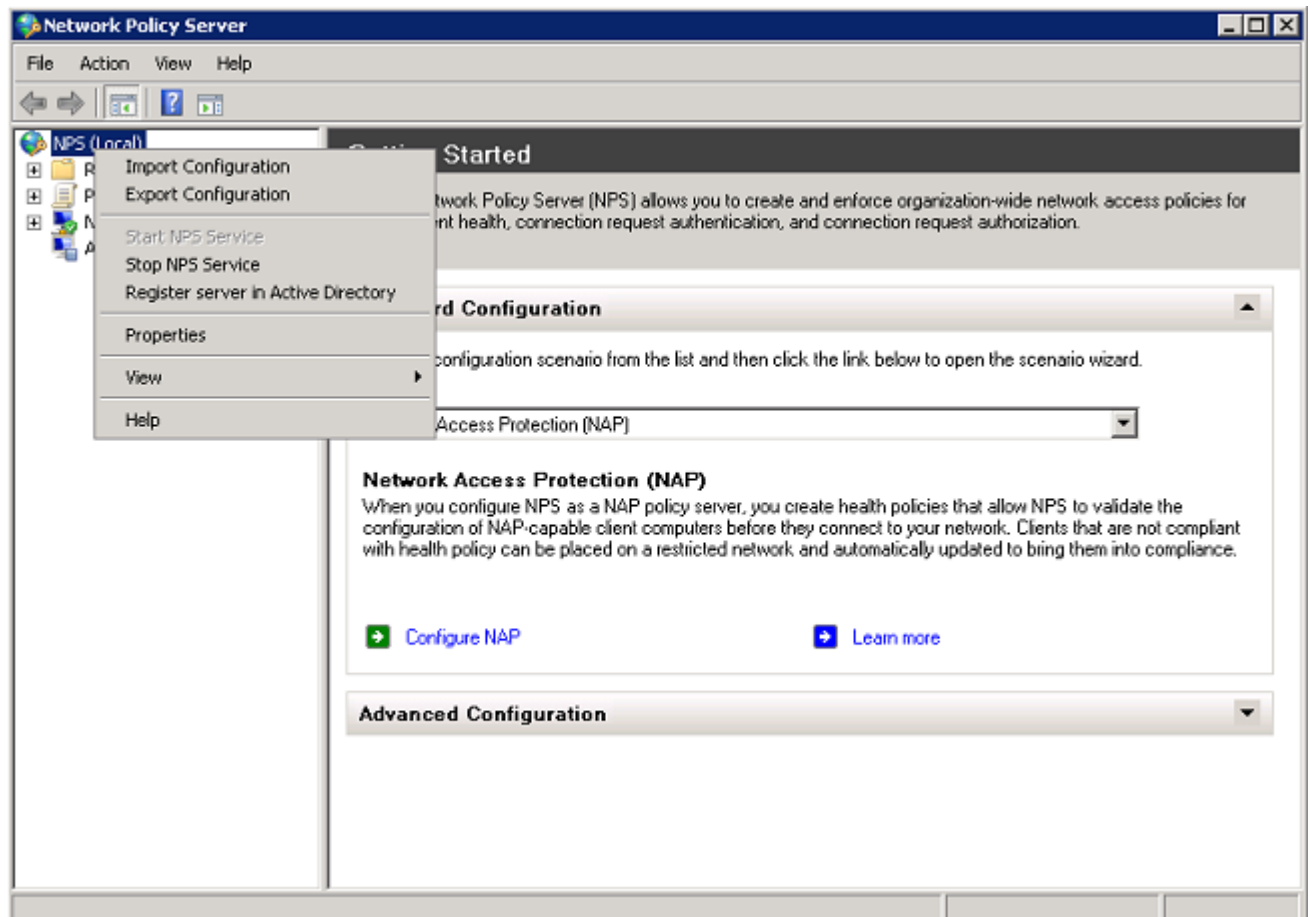
12. Verificare che lo scopo previsto del certificato sia Autenticazione client, Autenticazione server.



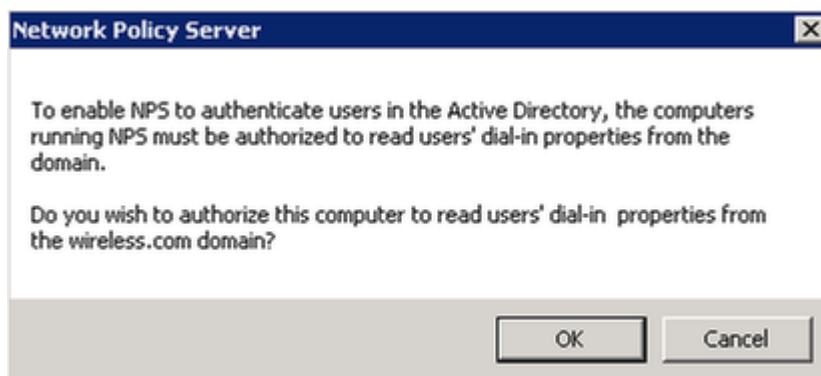
Configurare il servizio Server dei criteri di rete per l'autenticazione PEAP-MS-CHAP v2

Completare la procedura seguente per configurare Server dei criteri di rete per l'autenticazione:

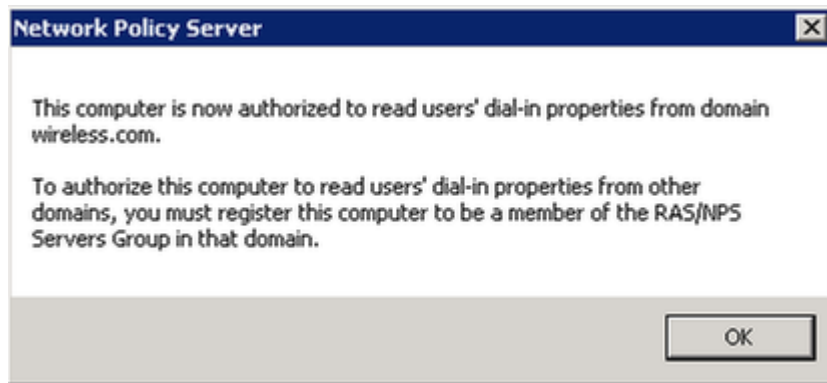
1. Fare clic su Start > Strumenti di amministrazione> Server dei criteri di rete.
2. Fare clic con il pulsante destro del mouse su Server dei criteri di rete (locale) e scegliere Registra server in Active Directory.



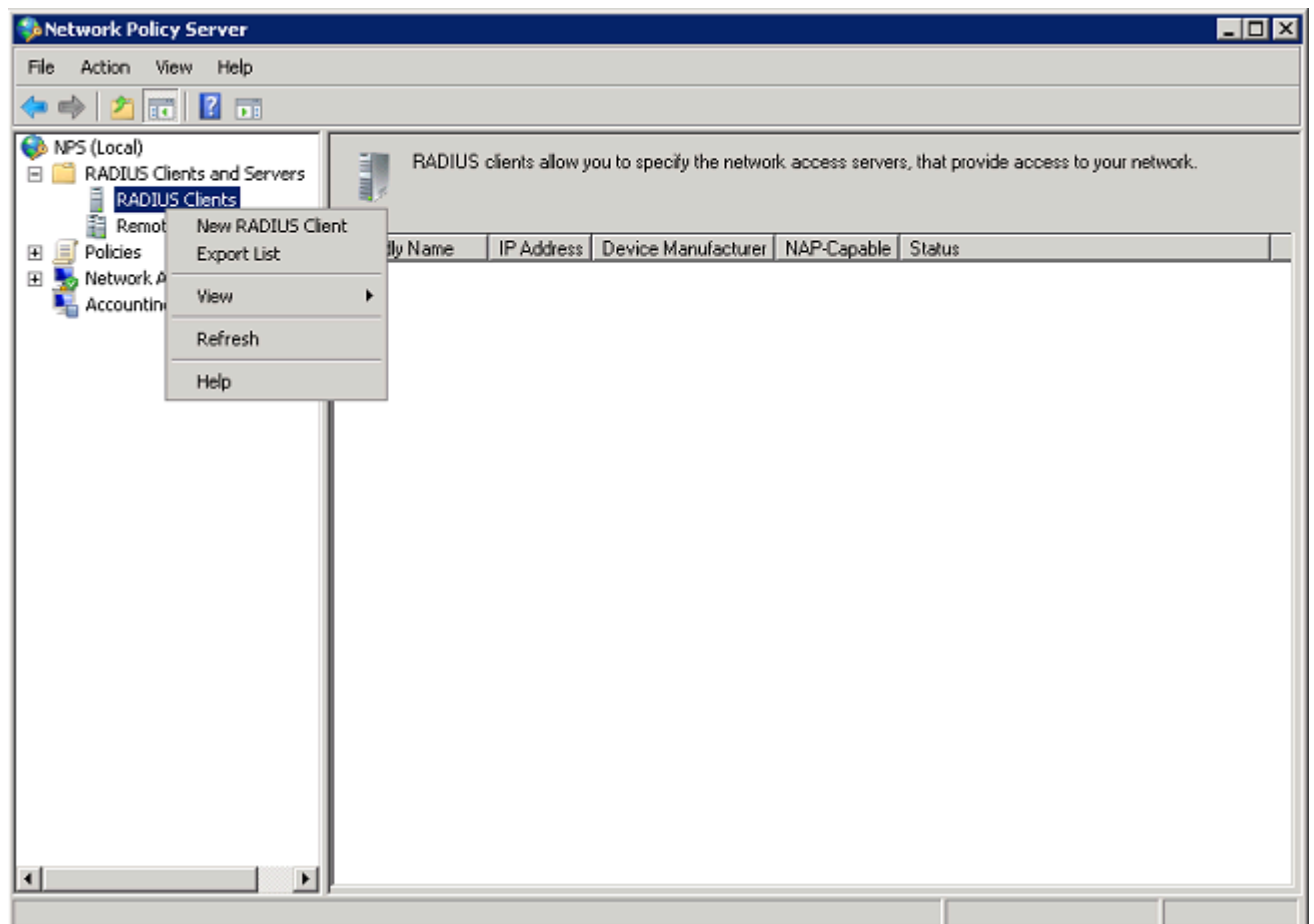
3. Fare clic su OK.



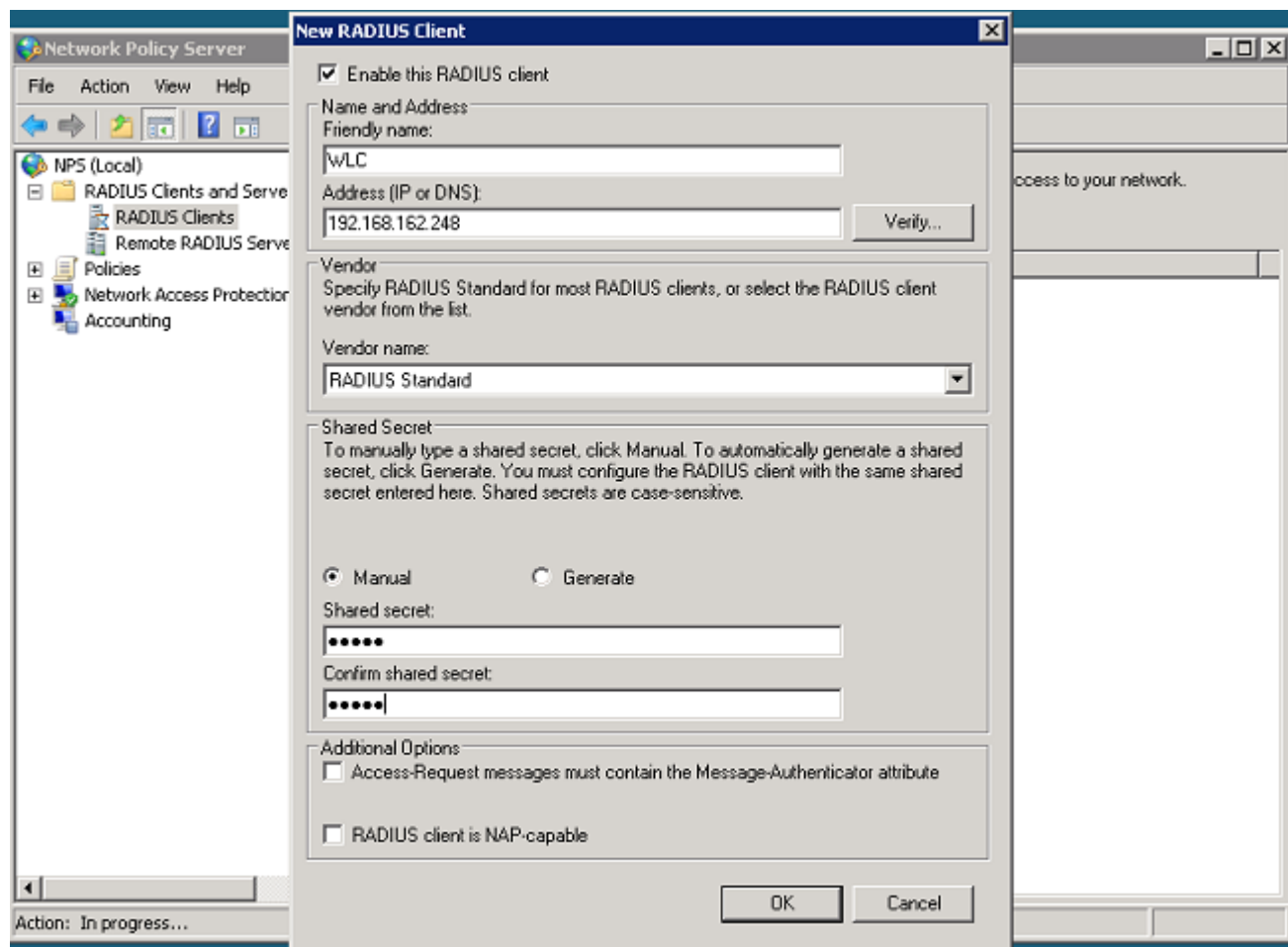
4. Fare clic su OK.



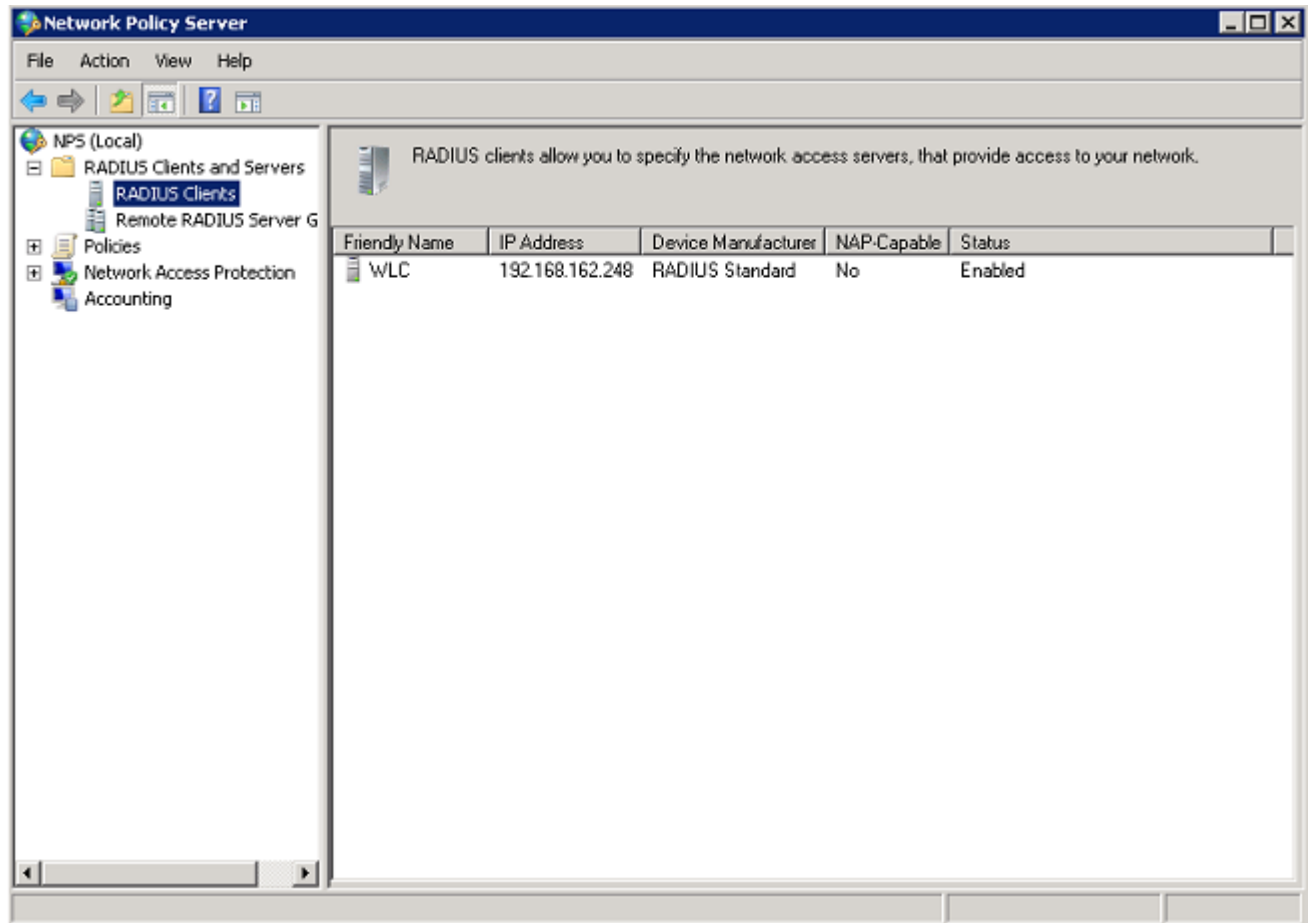
5. Aggiungere il controller LAN wireless come client di autenticazione, autorizzazione e accounting (AAA) nel Server dei criteri di rete.
6. Espandere Client e server RADIUS. Fare clic con il pulsante destro del mouse su Client RADIUS, quindi scegliere Nuovo client RADIUS.



7. Immettere un nome descrittivo (WLC in questo esempio), l'indirizzo IP di gestione del WLC (192.168.162.248 in questo esempio) e un segreto condiviso. Lo stesso segreto condiviso viene utilizzato per configurare il WLC.

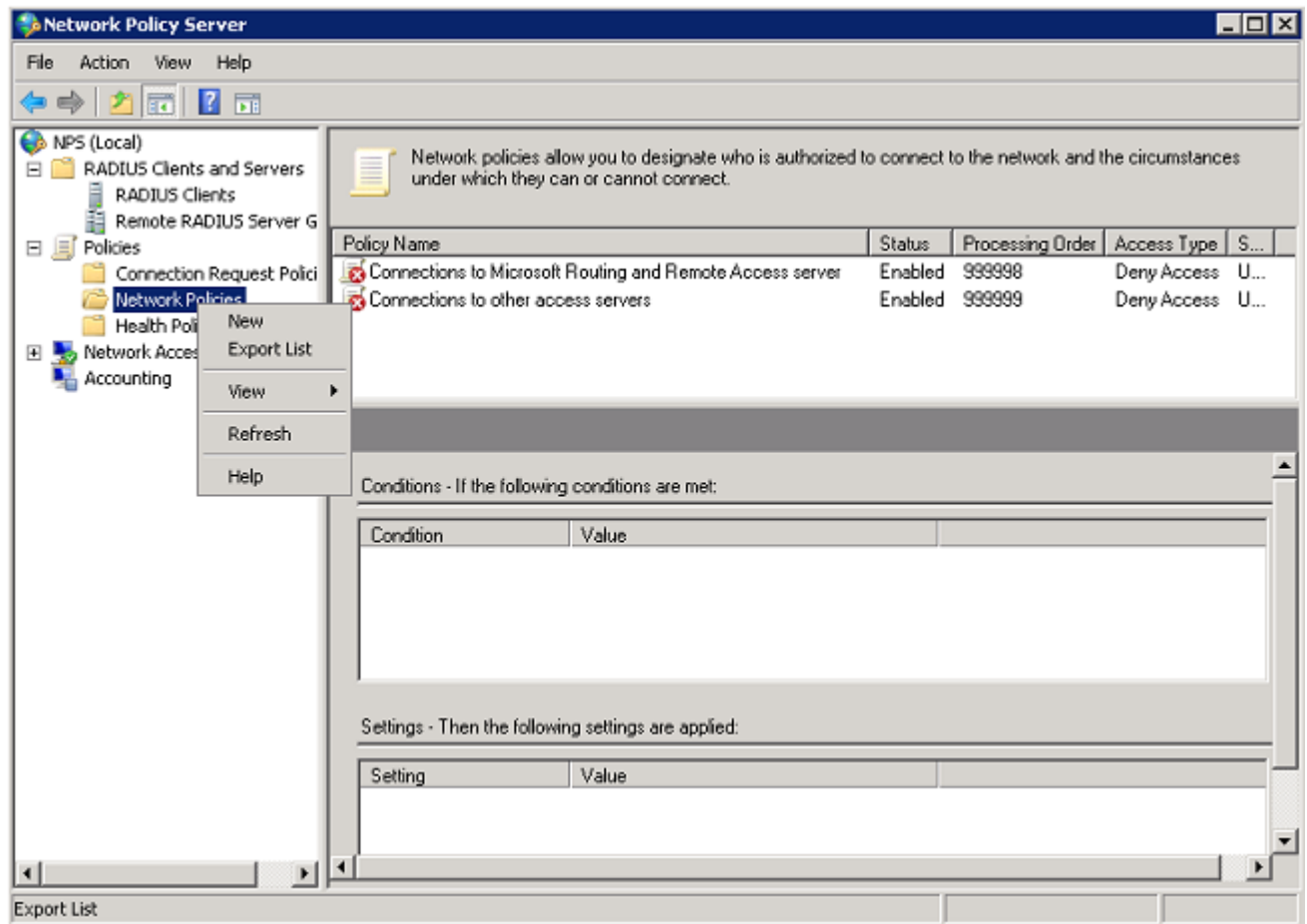


8. Fare clic su OK per tornare alla schermata precedente.



9. Creare un nuovo criterio di rete per gli utenti wireless. Espandere Criteri, fare clic con il pulsante destro del mouse su Criteri di rete e scegliere Nuovo.





10. Immettere un nome di criterio per la regola (in questo esempio, Wireless PEAP) e fare clic su Avanti.

**New Network Policy**

**Specify Network Policy Name and Connection Type**

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

**Policy name:**

Wireless PEAP

**Network connection method**

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

☒ Type of network access server:

Unspecified

☐ Vendor specific:

10

Previous Next Finish Cancel

11. Per fare in modo che questo criterio consenta solo gli utenti del dominio wireless, aggiungere le tre condizioni seguenti e fare clic su Avanti:

- Gruppi di Windows - Utenti del dominio
- Tipo porta NAS - Wireless - IEEE 802.11
- Tipo di autenticazione - EAP

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.

Add... Edit... Remove

Previous Next Finish Cancel

12. Fare clic su Accesso concesso per concedere i tentativi di connessione corrispondenti al criterio e quindi su Avanti.

New Network Policy ✕



## Specify Access Permission

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

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

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

☐ Access is determined by User Dial-in properties (which override NPS policy)  
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

13. Disabilitare tutti i metodi di autenticazione in Metodi di autenticazione meno sicuri.

**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:**

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

14. Fare clic su Add, selezionare PEAP e fare clic su OK per abilitare 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)

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

15. Selezionare Microsoft: PEAP (Protected EAP), quindi fare clic su Modifica. Verificare che il certificato del controller di dominio creato in precedenza sia selezionato nell'elenco a discesa Certificato emesso e fare clic su 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

Previous Next Finish Cancel

16. Fare clic su Next (Avanti).

**New Network Policy** [X]

## 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. Fare clic su Next (Avanti).



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. Fare clic su Next (Avanti).

New Network Policy




## Configure Settings

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

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


**Settings:**

**RADIUS Attributes**


Standard


☒
Vendor Specific


**Network Access Protection**



NAP Enforcement

☒
Extended State

**Routing and Remote Access**


Multilink and Bandwidth Allocation Protocol (BAP)


IP Filters


Encryption

☒
IP 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

Add...
Edit...
Remove

Previous
Next
Finish
Cancel

19. Fare clic su Finish (Fine).

**New Network Policy**

## 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.

Previous Next Finish Cancel

### Aggiungi utenti ad Active Directory

In questo esempio il database utenti viene gestito in Active Directory. Per aggiungere utenti al database di Active Directory, effettuare le operazioni riportate di seguito.

1. Aprire Utenti e computer di Active Directory. Fare clic su Start> Strumenti di amministrazione> Utenti e computer di Active Directory.
2. Nell'albero della console Utenti e computer di Active Directory espandere il dominio, fare clic con il pulsante destro del mouse su Utenti> Nuovo e scegliere Utente.
3. Nella finestra di dialogo Nuovo oggetto - Utente, immettere il nome dell'utente wireless. In questo esempio viene utilizzato il nome Client1 nel campo Nome e Client1 nel campo Nome di accesso utente. Fare clic su Next (Avanti).

New Object - User

Create in: wireless.com/Users

First name: Client1 Initials:

Last name:

Full name: Client1

User logon name: Client1 @wireless.com

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

< Back Next > Cancel

4. Nella finestra di dialogo Nuovo oggetto - Utente, immettere una password a scelta nei campi Password e Conferma password. Verificare che la casella di controllo Cambiamento obbligatorio password all'accesso successivo non sia selezionata e fare clic su Avanti.

New Object - User

Create in: wireless.com/Users

Password: .....

Confirm password: .....

☐ User must change password at next logon

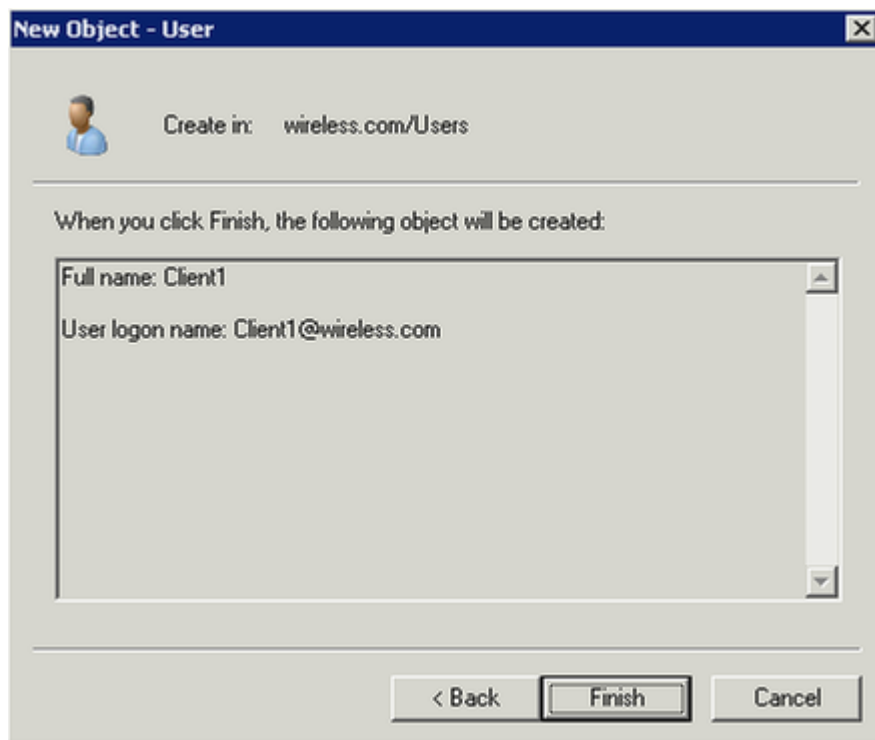
☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back Next > Cancel

5. Nella finestra di dialogo Nuovo oggetto - Utente fare clic su Fine.



6. Ripetere i passaggi da 2 a 4 per creare altri account utente.

#### Configurazione del controller LAN wireless e dei LAP

Configurare le periferiche wireless (i Wireless LAN Controller e LAP) per questa installazione.

#### Configurazione del WLC per l'autenticazione RADIUS

Configurare il WLC in modo che utilizzi Server dei criteri di rete come server di autenticazione. Per inoltrare le credenziali dell'utente a un server RADIUS esterno, è necessario configurare il WLC. Il server RADIUS esterno convalida quindi le credenziali dell'utente e fornisce l'accesso ai client wireless.

Completare questa procedura per aggiungere Server dei criteri di rete come server RADIUS nella pagina Sicurezza > Autenticazione RADIUS:

1. Scegliere Sicurezza> RADIUS > Autenticazione dall'interfaccia del controller per visualizzare la pagina Server di autenticazione RADIUS. Per definire un server RADIUS, fare clic su New (Nuovo).

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

### Security

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
  - TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- TrustSec SXP
- Advanced

### RADIUS Authentication Servers

Apply New...

Call Station ID Type [i](#) IP Address

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

MAC Delimiter Hyphen

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
1. Call Station ID Type will be applicable only for non 802.1x authentication only.						

2. Definire i parametri del server RADIUS. Questi parametri includono l'indirizzo IP, il segreto condiviso, il numero di porta e lo stato del server RADIUS. Le caselle di controllo Utente di rete e Gestione di rete determinano se l'autenticazione basata su RADIUS viene applicata agli utenti di rete e di gestione (wireless). In questo esempio viene utilizzato Server dei criteri di rete come server RADIUS con indirizzo IP 192.168.162.12. Fare clic su Applica.

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

### Security

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
  - TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- TrustSec SXP
- Advanced

### RADIUS Authentication Servers > New

< Back Apply

Server Index (Priority) 1

Server IP Address 192.168.162.12

Shared Secret Format ASCII

Shared Secret .....

Confirm Shared Secret .....

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

Port Number 1812

Server Status Enabled

Support for RFC 3576 Enabled

Server Timeout 2 seconds

Network User ☒ Enable

Management ☒ Enable

IPSec ☐ Enable

## Configurazione di una WLAN per i client

Configurare l'identificatore del set di servizi (SSID) (WLAN) a cui si connettono i client wireless. In questo esempio, creare il SSID e denominarlo PEAP.

Definire l'autenticazione di layer 2 come WPA2 in modo che i client eseguano l'autenticazione basata su EAP (PEAP-MS-CHAP v2 in questo esempio) e utilizzino lo standard AES (Advanced Encryption Standard) come meccanismo di crittografia. Mantenere tutti gli altri valori ai valori predefiniti.



Nota: In questo documento la WLAN è associata alle interfacce di gestione. Se la rete contiene più VLAN, è possibile creare una VLAN separata e associarla all'SSID. Per informazioni su come configurare le VLAN sui WLC, fare riferimento all'esempio di configurazione delle VLAN sui controller LAN wireless.

Per configurare una WLAN sul WLC, completare i seguenti passaggi:

1. Per visualizzare la pagina WLAN, fare clic su WLAN dall'interfaccia del controller. In questa pagina vengono elencate le WLAN esistenti sul controller.
2. Per creare una nuova WLAN, selezionare New (Nuovo). Immettere l'ID WLAN e l'SSID WLAN per la WLAN, quindi fare clic su Applica.

The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The top navigation bar includes links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'. The main menu has tabs for 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' tab is selected, and the 'WLANs > New' page is displayed. On the left, there is a sidebar with 'WLANs' and 'Advanced' options. The main form area contains the following fields:

Type	WLAN
Profile Name	PEAP
SSID	PEAP
ID	1

At the bottom right of the form, there are two buttons: '< Back' and 'Apply'.

3. Per configurare l'SSID per 802.1x, attenersi alla seguente procedura:
  1. Fare clic sulla scheda General (Generale) e abilitare la WLAN.

WLANs > Edit 'PEAP' < Back Apply

**General** **Security** **QoS** **Advanced**

Profile Name: PEAP  
 Type: WLAN  
 SSID: PEAP  
 Status: ☒ Enabled

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

Radio Policy: All  
 Interface/Interface Group(G): management  
 Multicast Vlan Feature: ☐ Enabled  
 Broadcast SSID: ☒ Enabled  
 NAS-ID: 2504

- Fare clic sulle schede Protezione > Livello 2, impostare Protezione di Livello 2 su WPA + WPA2, selezionare le caselle di controllo Parametri WPA+WPA2 (ad esempio, WPA2 AES) in base alle esigenze e fare clic su 802.1x come Gestione chiavi di autenticazione.

WLANs > Edit 'PEAP' < Back Apply

**General** **Security** **QoS** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Layer 2 Security: WPA+WPA2  
 MAC Filtering: ☐

**Fast Transition**  
 Fast Transition: ☐

**Protected Management Frame**  
 PMF: Disabled

**WPA+WPA2 Parameters**  
 WPA Policy: ☐  
 WPA2 Policy: ☒  
 WPA2 Encryption: ☒ AES ☐ TKIP

**Authentication Key Management**  
 802.1X: ☒ Enable  
 CCKM: ☐ Enable  
 PSK: ☐ Enable  
 FT 802.1X: ☐ Enable

- Fare clic sulla scheda Sicurezza > Server AAA, scegliere l'indirizzo IP del Server dei criteri di rete dall'elenco a discesa Server 1 e fare clic su Applica.



WLANs > Edit 'PEAP'

General
Security
QoS
Advanced

Layer 2
Layer 3
AAA Servers

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

**Radius Servers**

Radius Server Overwrite interface ☐ Enabled

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
	<input type="text" value="IP:192.168.162.12, Port:1812"/>	<input type="text" value="None"/>
Server 2	<input type="text" value="None"/>	<input type="text" value="None"/>
Server 3	<input type="text" value="None"/>	<input type="text" value="None"/>
Server 4	<input type="text" value="None"/>	<input type="text" value="None"/>
Server 5	<input type="text" value="None"/>	<input type="text" value="None"/>
Server 6	<input type="text" value="None"/>	<input type="text" value="None"/>

**Radius Server Accounting**

Interim Update ☐

**Local EAP Authentication**

Local EAP Authentication ☐ Enabled

**LDAP Servers**

Server 1

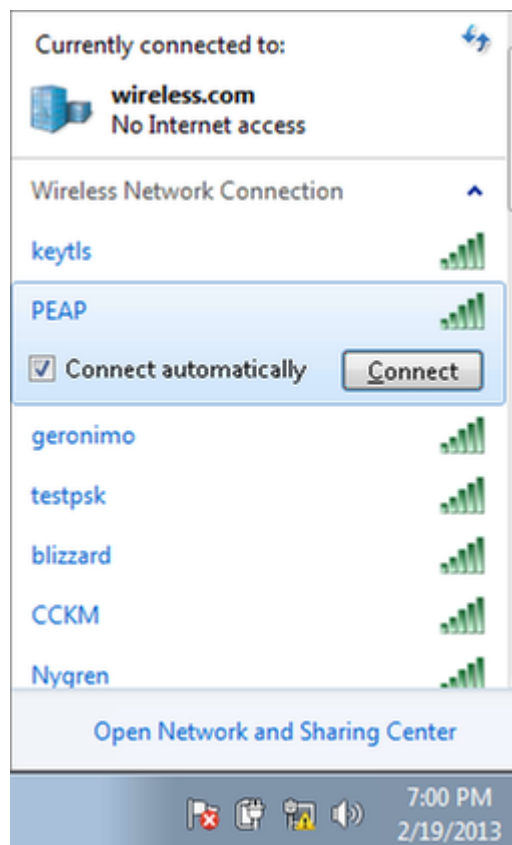
Server 2

Server 3

Configurazione dei client wireless per l'autenticazione PEAP-MS-CHAP v2

Completare la procedura descritta di seguito per configurare il client wireless con lo strumento Zero Config di Windows per la connessione alla WLAN PEAP.

1. Fare clic sull'icona Rete nella barra delle applicazioni. Fare clic su PEAP SSID, quindi su Connetti.



2. Il client deve essere connesso alla rete.



3. Se la connessione non riesce, provare a riconnettersi alla WLAN. Se il problema persiste, consultare la sezione Risoluzione dei problemi.

# Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

Se il client non si è connesso alla WLAN, in questa sezione vengono fornite informazioni che è possibile utilizzare per risolvere i problemi relativi alla configurazione.

Per diagnosticare gli errori di autenticazione 802.1x è possibile utilizzare due strumenti: utilizzare il comando debug client e il Visualizzatore eventi di Windows.

Se si esegue il debug di un client dal WLC, non si tratta di un'operazione che richiede molte risorse e non influisce sul servizio. Per avviare una sessione di debug, aprire l'interfaccia della riga di comando (CLI) del WLC e immettere debug client mac address, dove mac address è l'indirizzo mac wireless del client wireless che non è in grado di connettersi. Durante l'esecuzione del debug, provare a connettere il client; sulla CLI del WLC, deve essere presente un output simile a quello dell'esempio seguente:

```
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db 192.168.142.136 WNM (20) Changing IP=4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2018)
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db 192.168.142.136 WNM (20) Changing IP=4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2246)
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db In processAddIE:4205 setting Central switched to TRUE
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db In processAddIE:4205 apVapId = 1 and Split Acl Id = 65535
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db Applying site-specific Local Bridging override for station 78:e4:00:b2:ef:db - vapId 1, site 'default-group', interface 'management'
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db Applying Local Bridging Interface Policy for station 78:e4:00:b2:ef:db - vlan 243, interface id 0, interface 'management'
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db processAddIEf statusCode is 0 and status is 0
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db processAddIEf saidDone flag is 0 finishFlag is 0
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db STA - rates (8): 130 132 139 155 36 48 72 108 12 18 24 96 0 0 0 0
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db suppRates statusCode is 0 and getSuppRatesElement is 1
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db STA - rates (12): 130 132 139 150 36 48 72 108 12 18 24 96 0 0 0 0
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db csiSuppRates statusCode is 0 and getcsiSuppRatesElement is 1
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Processing RSN IE type 48, length 40 for mobile 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Received RSN IE with 0 PMKIDs from mobile 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Found an cache entry for RSNID c8:f9:f9:1a:20:40 in PMKID cache at index 0 of station 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Removing RSNID c8:f9:f9:1a:20:40 from PMKID cache of station 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Resetting NUCB PMK Cache Entry 0 for station 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Setting active key cache index 0 ----> 0
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db unsetting PendingValidatedKey
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db apMgmtDataDec
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db apMgmtDataDec
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.142.136 WNM (20) Change state to START (0) last state WNM (20)
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db genApfAddMobileStation2: APF_MH_PEM_WAIT_13_AUTH_COMPLETE = 0.
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.142.136 START (0) Initializing policy
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.142.136 START (0) Change state to AUTHCHECK (2) last state START (0)
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.142.136 AUTHCHECK (2) Change state to 0021X_REQD (3) last state AUTHCHECK (2)
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db N66 Using WNM Compliance mode qosCap 00
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.142.136 0021X_REQD (3) Plumbed mobile LWAPP rule on AP c8:f9:f9:1a:20:40 vapId 1 apVapId 1 file-acl-name:
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db apfVpnAddUser2 (apf_policy.c:276) Changing state for mobile 78:e4:00:b2:ef:db on AP c8:f9:f9:1a:20:40 from Associated to Associated
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db apfVpnAddUser2:session timeout forestation 78:e4:00:b2:ef:db - Session Your 0, apMgmtTimeOut "0" and sessionTimeRunning flag is 0
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Stopping deletion of Mobile Station: (callerId: 48)
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Func: apfVpnAddUser2, Ms Timeout = 0, Session Timeout = 0
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Sending Assoc Response to station on RSNID c8:f9:f9:1a:20:40 (statusCode 0) ApVapId 1 Slot 0
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db apfProcessAssocReq (apf_00211.c:7191) Changing state for mobile 78:e4:00:b2:ef:db on AP c8:f9:f9:1a:20:40 from Associated to Associated
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.142.136 WNM (20) Removed RPT entry.
*dot11MgtTask: Feb 19 20:57:07.620: 78:e4:00:b2:ef:db Disable re-auth, use PMK lifetime.
*dot11MgtTask: Feb 19 20:57:07.620: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Connecting state
*dot11MgtTask: Feb 19 20:57:07.620: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 1)
*dot11_MN_MgtTask_2: Feb 19 20:57:07.636: 78:e4:00:b2:ef:db Received EAPOL START from mobile 78:e4:00:b2:ef:db
*dot11_MN_MgtTask_3: Feb 19 20:57:07.636: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Connecting state
*dot11_MN_MgtTask_3: Feb 19 20:57:07.639: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 2)
*dot11_MN_MgtTask_3: Feb 19 20:57:07.651: 78:e4:00:b2:ef:db Received EAPOL EAPREQ from mobile 78:e4:00:b2:ef:db
*dot11_MN_MgtTask_3: Feb 19 20:57:07.655: 78:e4:00:b2:ef:db Received EAP Response packet with mismatching id (currentid=2, eapId=1) from mobile 78:e4:00:b2:ef:db
*dot11_MN_MgtTask_3: Feb 19 20:57:07.656: 78:e4:00:b2:ef:db Received EAPOL EAPREQ from mobile 78:e4:00:b2:ef:db
*dot11_MN_MgtTask_3: Feb 19 20:57:07.656: 78:e4:00:b2:ef:db Received Identity Response (current=2) from mobile 78:e4:00:b2:ef:db
*dot11_MN_MgtTask_3: Feb 19 20:57:07.656: 78:e4:00:b2:ef:db RSP State update from Connecting to Authenticating for mobile 78:e4:00:b2:ef:db
*dot11_MN_MgtTask_3: Feb 19 20:57:07.656: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Authenticating state
```

Questo è un esempio di un problema che potrebbe verificarsi con una configurazione errata. In questo caso, il debug WLC mostra che il WLC è passato allo stato di autenticazione, ossia è in attesa di una risposta dal Server dei criteri di rete. Ciò è in genere dovuto a un segreto condiviso non corretto sul WLC o sul Server dei criteri di rete. È possibile verificare questa condizione tramite il Visualizzatore eventi di Windows Server. Se non si trova un registro, la richiesta non è mai stata inviata al Server dei criteri di rete.

Un altro esempio restituito dal debug WLC è access-reject. Un messaggio di rifiuto di accesso

indica che il Server dei criteri di rete ha ricevuto e rifiutato le credenziali del client. Questo è un esempio di client che riceve un messaggio di rifiuto di accesso:

```
*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 EAPFRT 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)
```

Quando viene visualizzato un messaggio di rifiuto di accesso, controllare i registri nei registri eventi di Windows Server per determinare il motivo per cui il Server dei criteri di rete ha risposto al client con un messaggio di rifiuto di accesso.

Se l'autenticazione ha esito positivo, nel debug del client è presente access-accept, come mostrato nell'esempio seguente:

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

Per risolvere i problemi di rifiuto di accesso e di timeout di risposta, è necessario accedere al server RADIUS. Il WLC funge da autenticatore per il passaggio dei messaggi EAP tra il client e il server RADIUS. Il produttore del servizio RADIUS deve esaminare e diagnosticare un server RADIUS che risponde con un timeout di accesso, rifiuto o risposta.



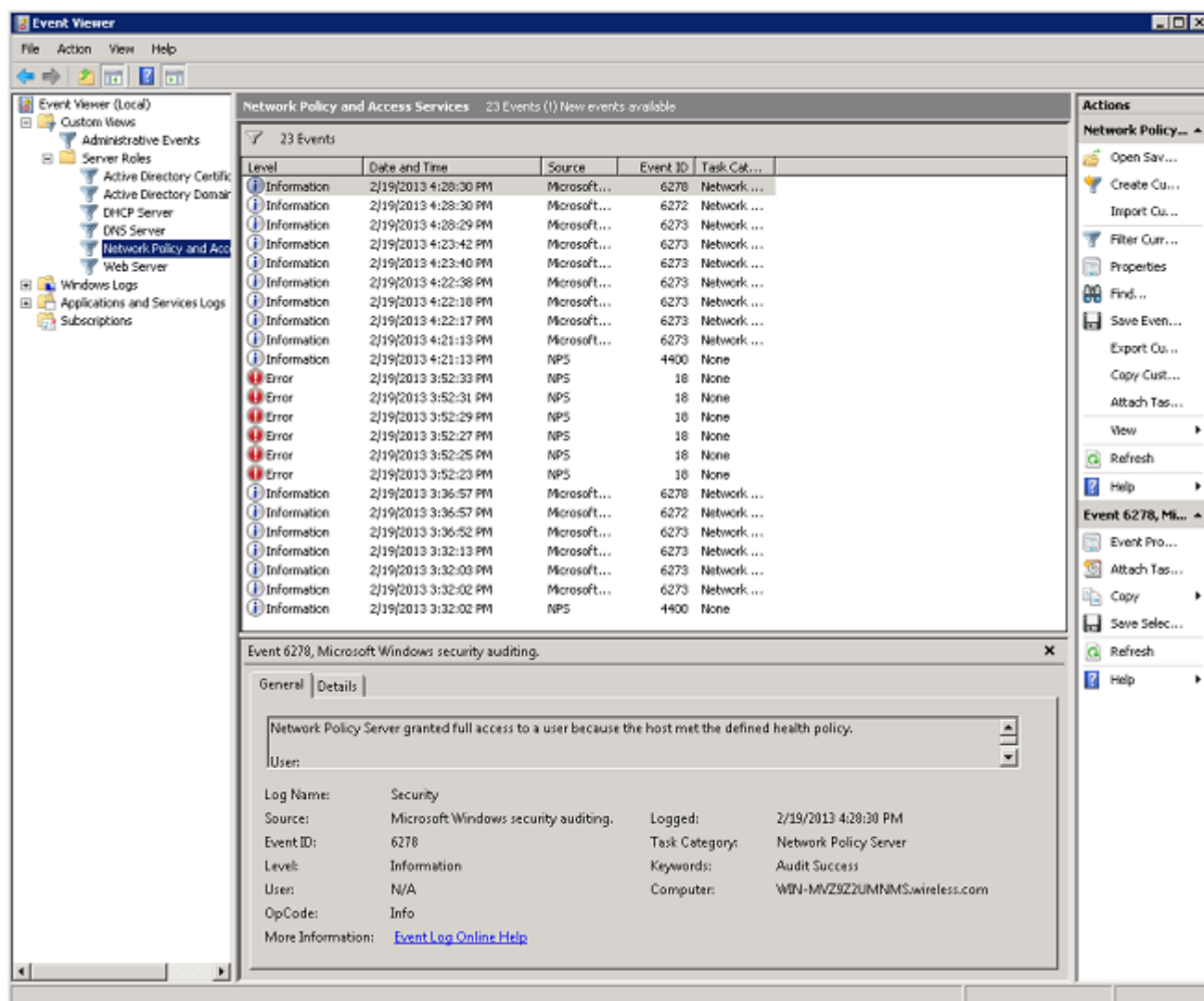
Nota: TAC non fornisce supporto tecnico per server RADIUS di terze parti; tuttavia, i registri sul server RADIUS spiegano in genere il motivo per cui una richiesta client è stata



rifiutata o ignorata.

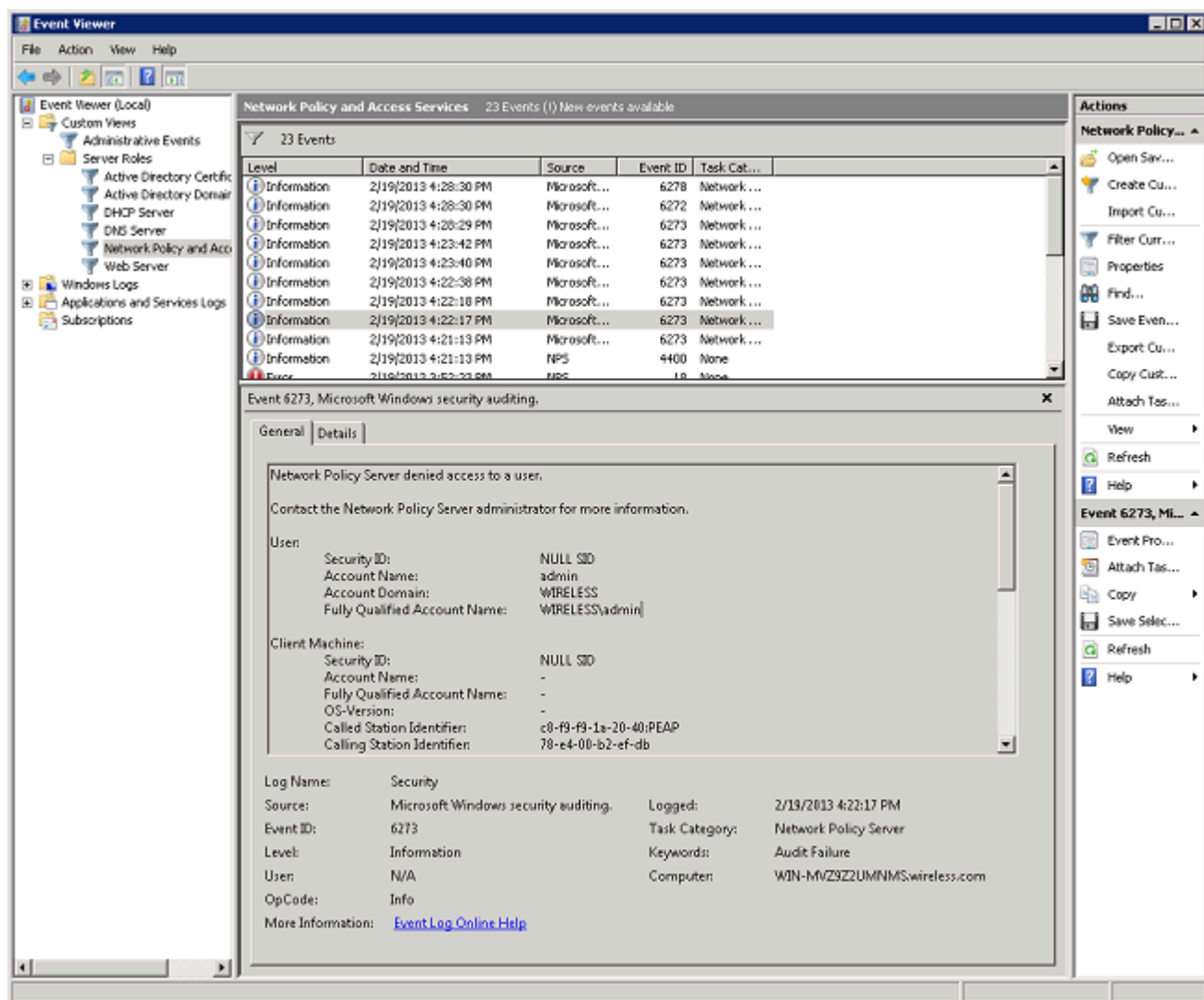
Per risolvere i problemi relativi ai rifiuti di accesso e ai timeout di risposta da Server dei criteri di rete, esaminare i registri di Server dei criteri di rete nel Visualizzatore eventi di Windows sul server.

1. Fare clic su Start > Strumenti di amministrazione > Visualizzatore eventi per avviare il Visualizzatore eventi ed esaminare i registri di Server dei criteri di rete.
2. Espandere Visualizzazioni personalizzate > Ruoli del server > Criteri di rete e accesso.



In questa sezione della Visualizzazione eventi sono presenti registri di autenticazioni passate e non riuscite. Esaminare questi registri per risolvere i problemi relativi al mancato passaggio dell'autenticazione da parte di un client. Sia le autenticazioni passate che quelle non riuscite vengono visualizzate come informazioni. Scorrere i log per trovare il nome utente che non è stato autenticato e che ha ricevuto un rifiuto di accesso basato sui debug WLC.

Questo è un esempio di Server dei criteri di rete in cui viene negato l'accesso a un utente:



Quando si esamina un'istruzione di rifiuto nel Visualizzatore eventi, esaminare la sezione Dettagli autenticazione. In questo esempio è possibile notare che il Server dei criteri di rete ha negato l'accesso all'utente a causa di un nome utente non corretto:

Authentication Details:

Proxy Policy Name: Use Windows authentication for all users

Network Policy Name: -

Authentication Provider: Windows

Authentication Server: WIN-MVZ9Z2UMNMS.wireless.com

Authentication Type: EAP

EAP Type: -

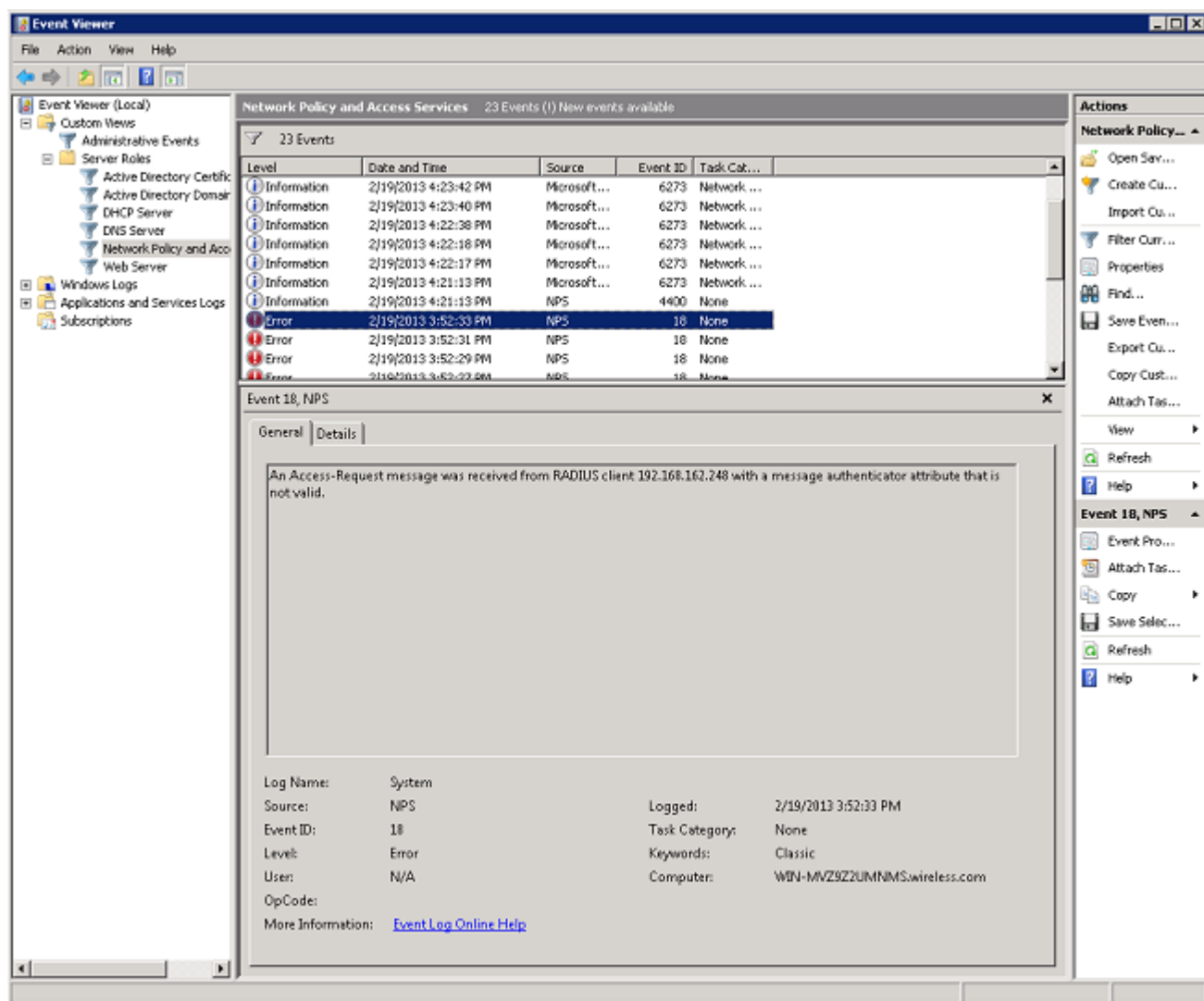
Account Session Identifier: -

Reason Code: 8

Reason: The specified user account does not exist.

La Visualizzazione eventi nel Server dei criteri di rete consente inoltre di risolvere i problemi se il WLC non riceve una risposta dal Server dei criteri di rete. Ciò è in genere causato da un segreto condiviso non corretto tra il Server dei criteri di rete e il WLC.

In questo esempio, il Server dei criteri di rete ignora la richiesta del WLC a causa di un segreto condiviso non corretto:



## Informazioni correlate

- [Supporto tecnico Cisco e download](#)

### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).