Configurazione di NPS, dispositivi Wireless LAN Controller e reti wireless

Sommario

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.

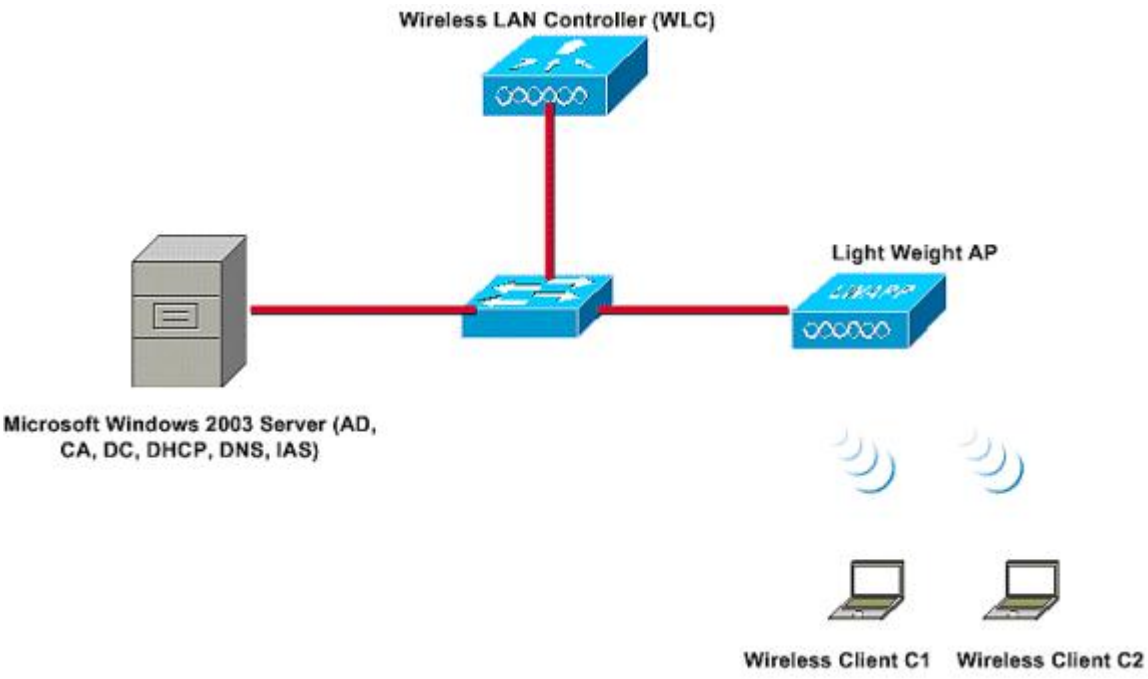
Configurazione

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:



Esempio 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

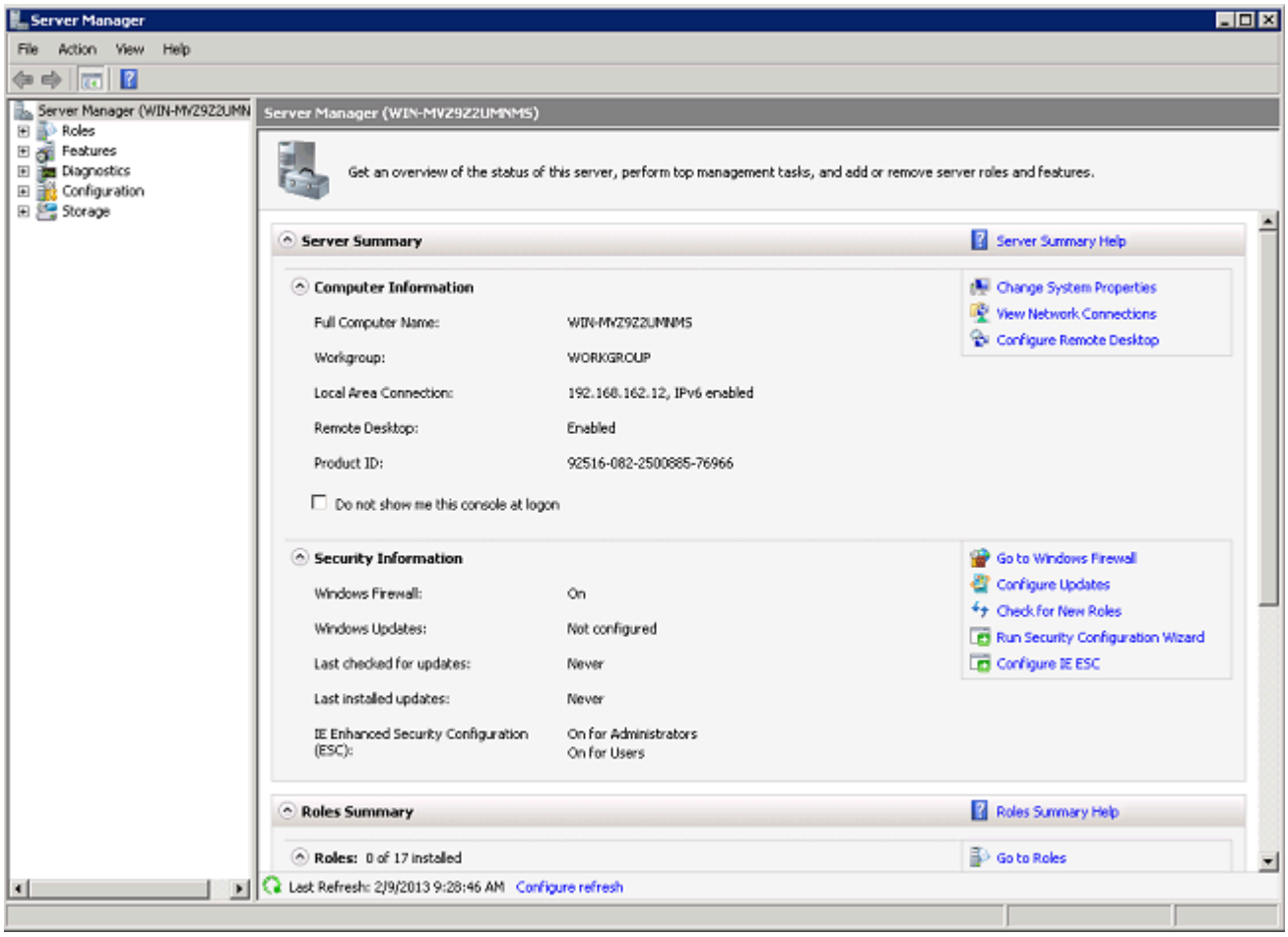
In questo esempio, una configurazione completa del server Microsoft Windows 2008 include i seguenti passaggi:

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.

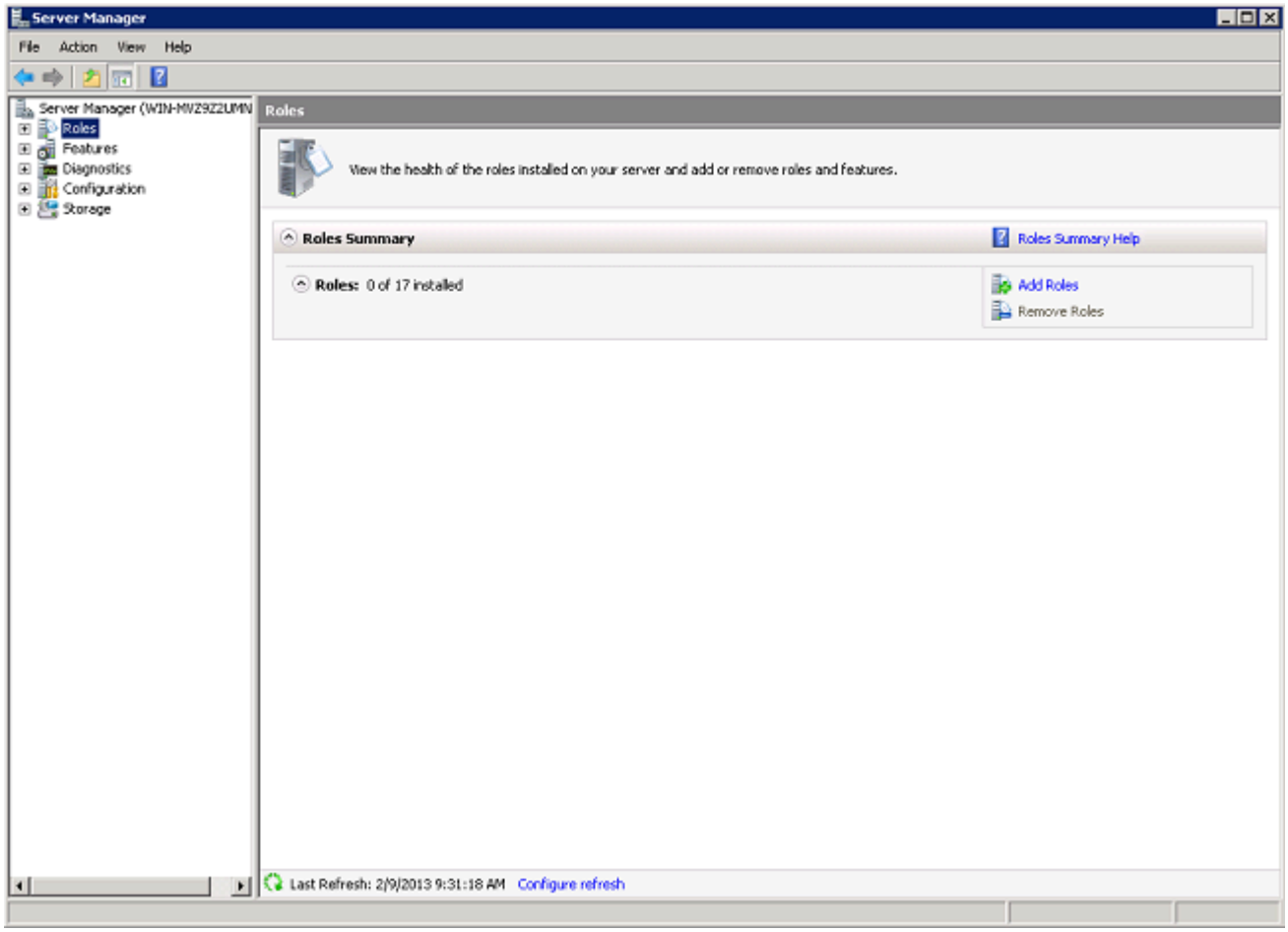
Configurare il server Microsoft Windows 2008 come controller di dominio

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

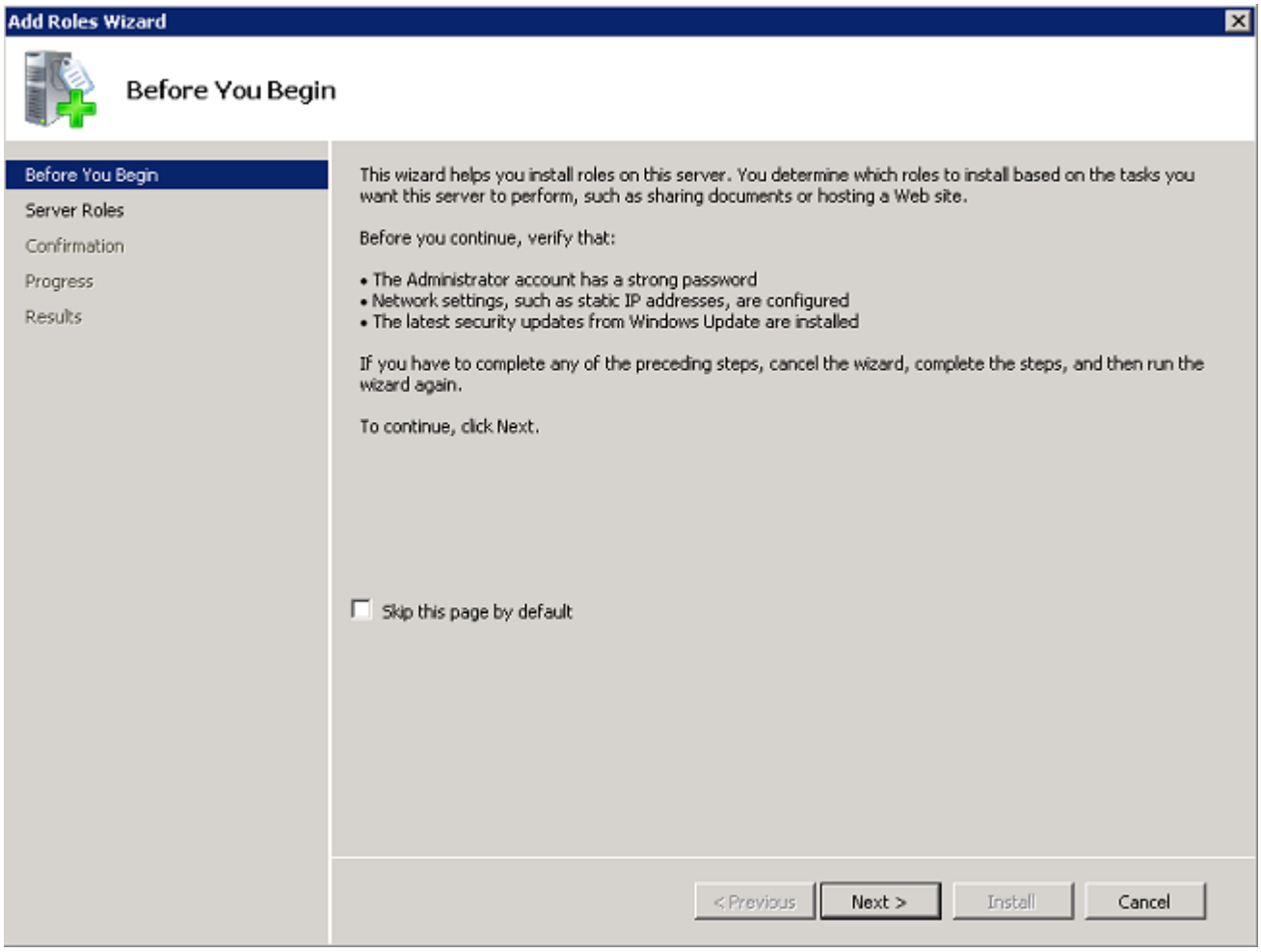
1. Fare clic su Start> Server Manager.



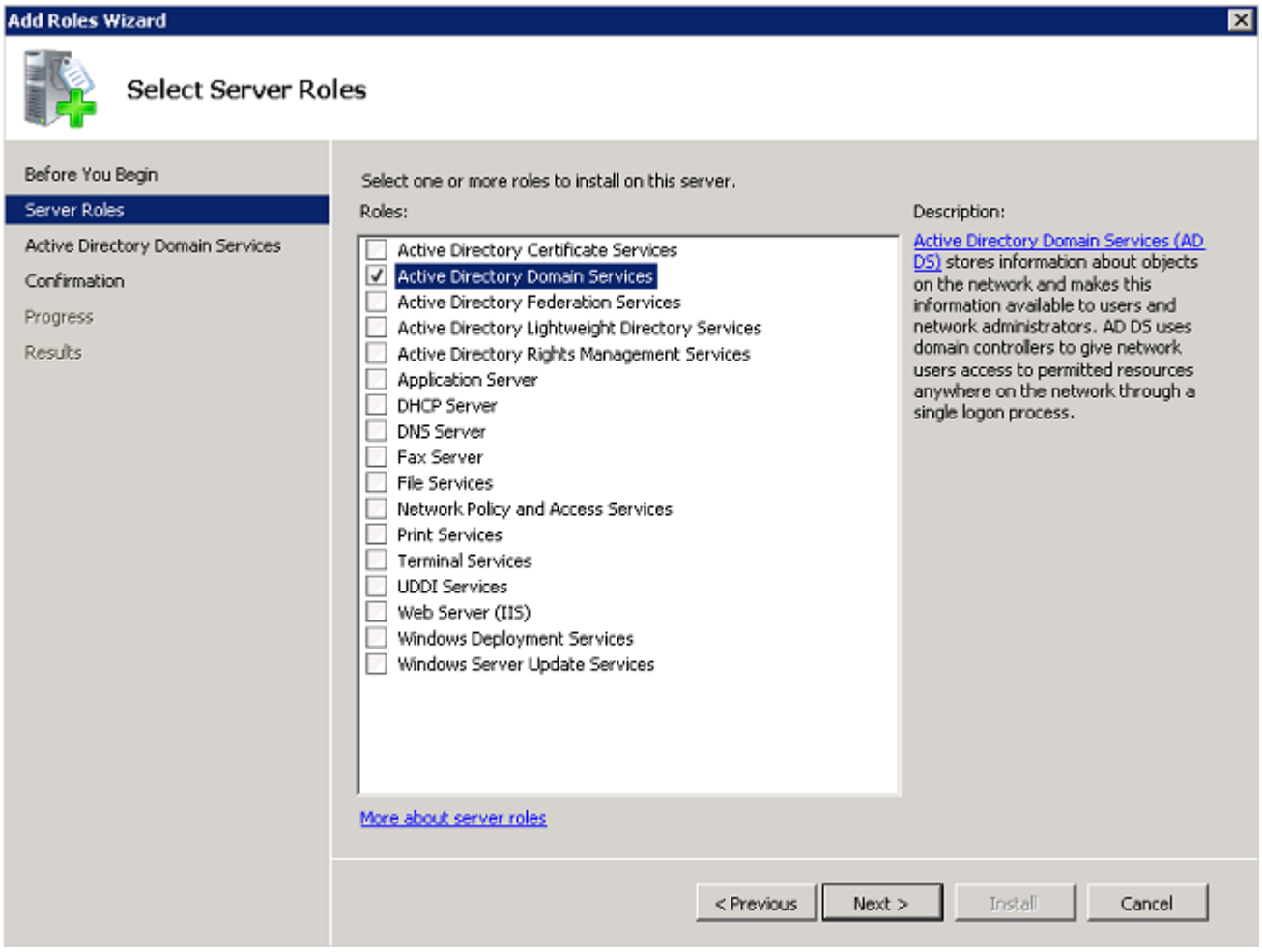
2. Fare clic su Ruoli> Aggiungi ruoli.



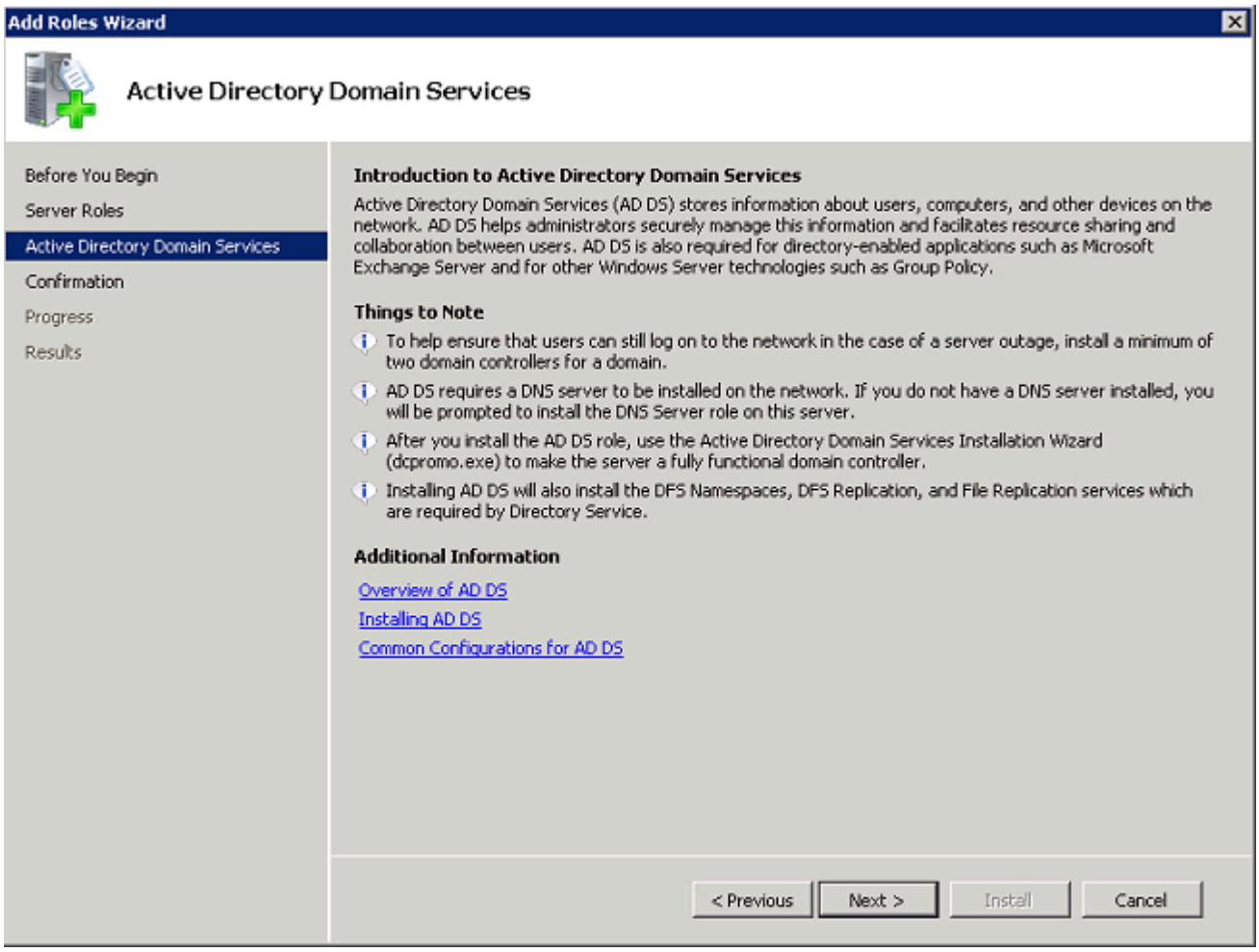
3. Fare clic su Next (Avanti).



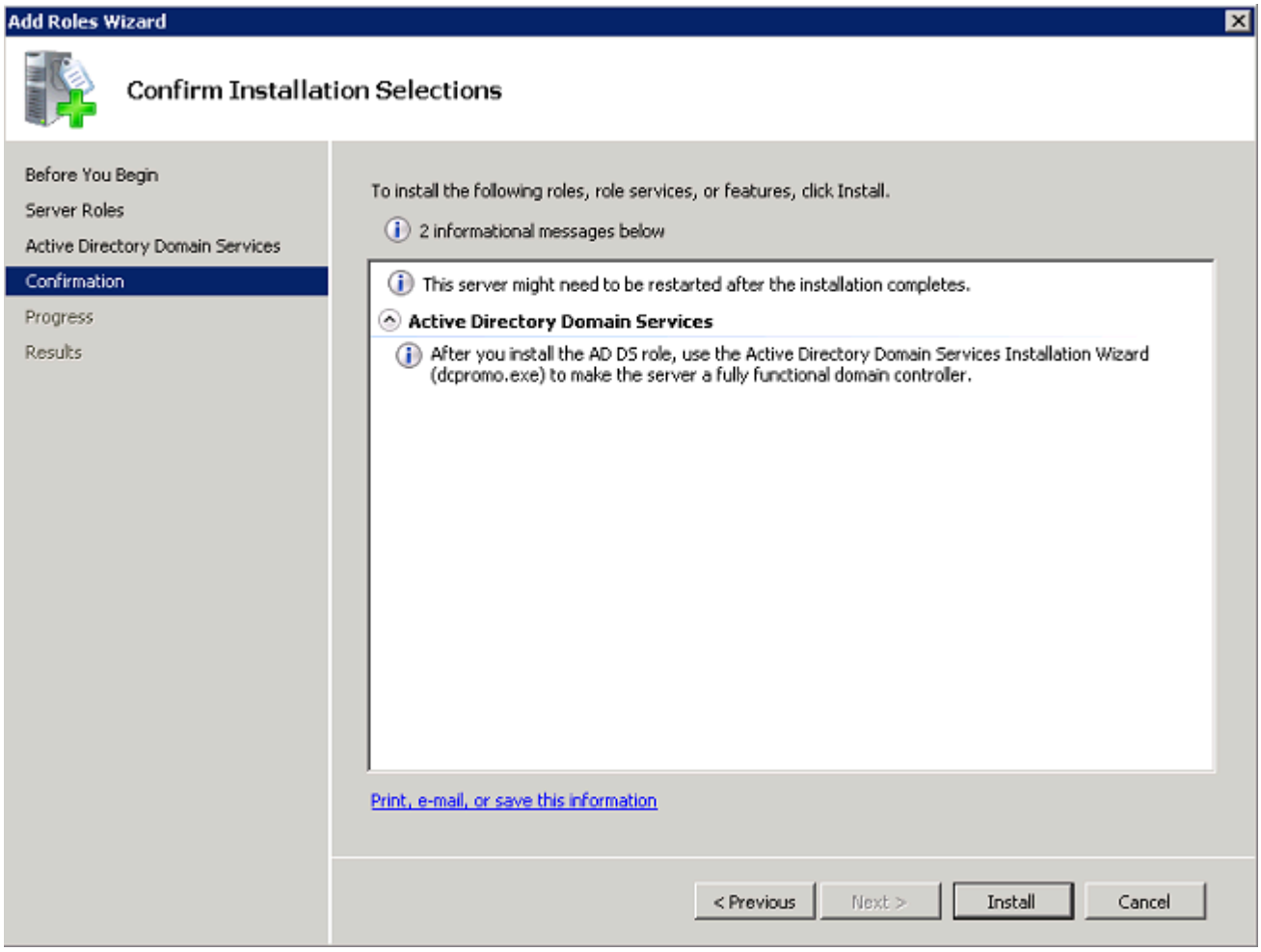
4. Selezionare il servizio Servizi di dominio Active Directory e fare clic su Avanti.



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

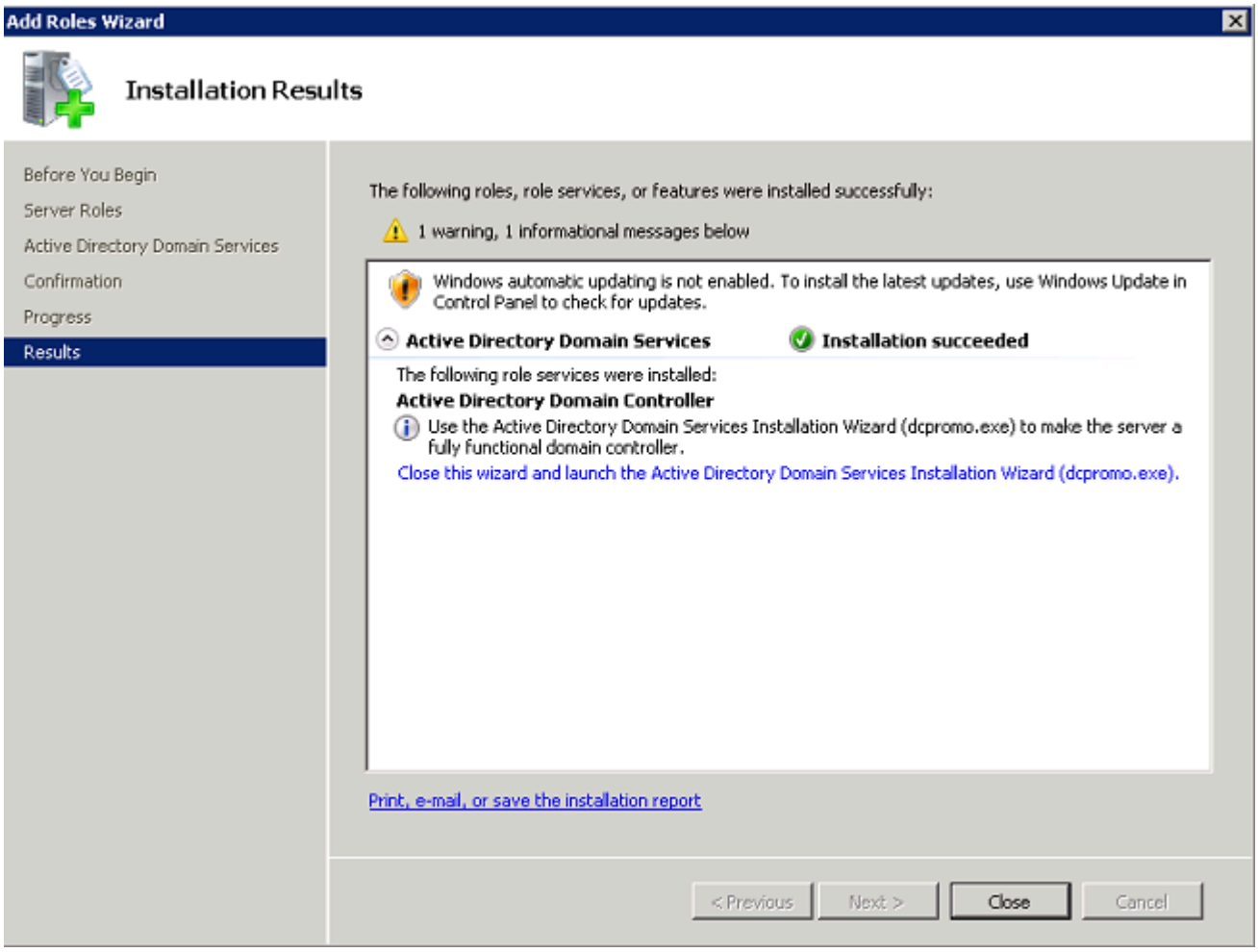


6. Fare clic su Installa per avviare il processo di installazione.

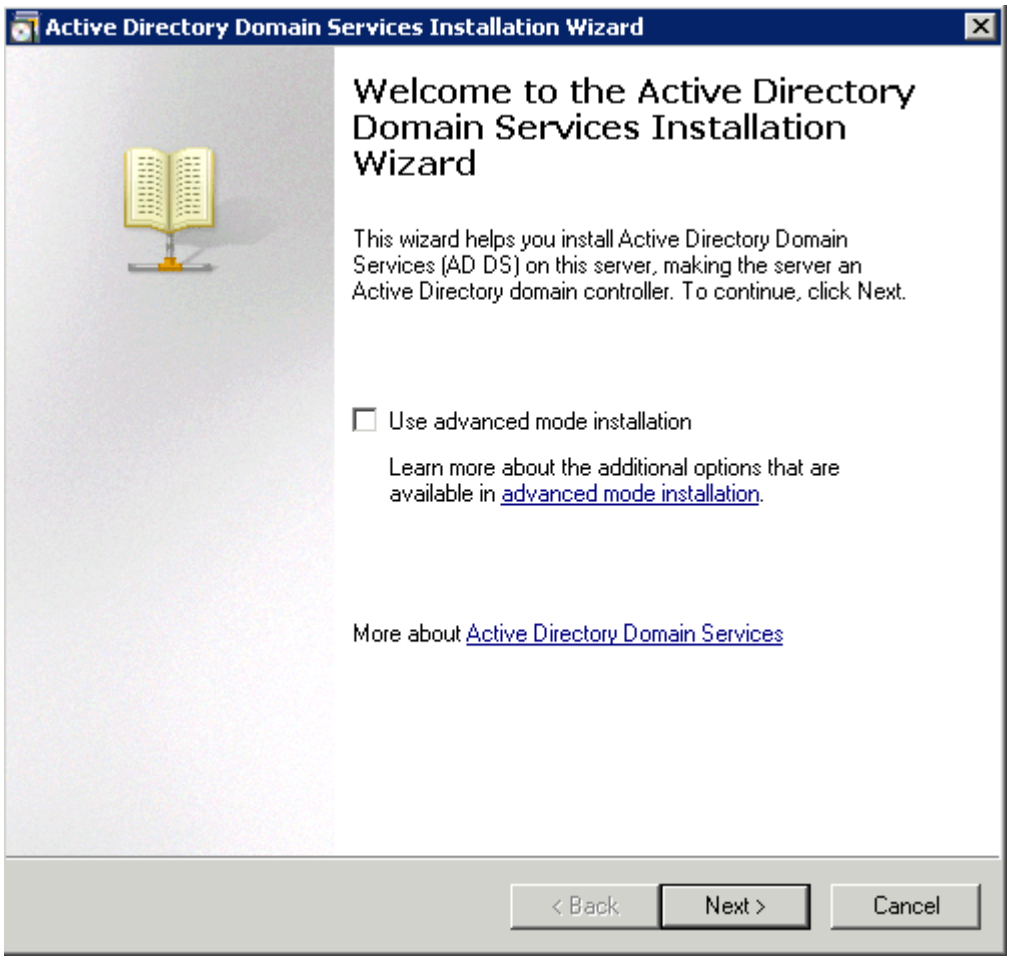


L'installazione procede e viene completata.

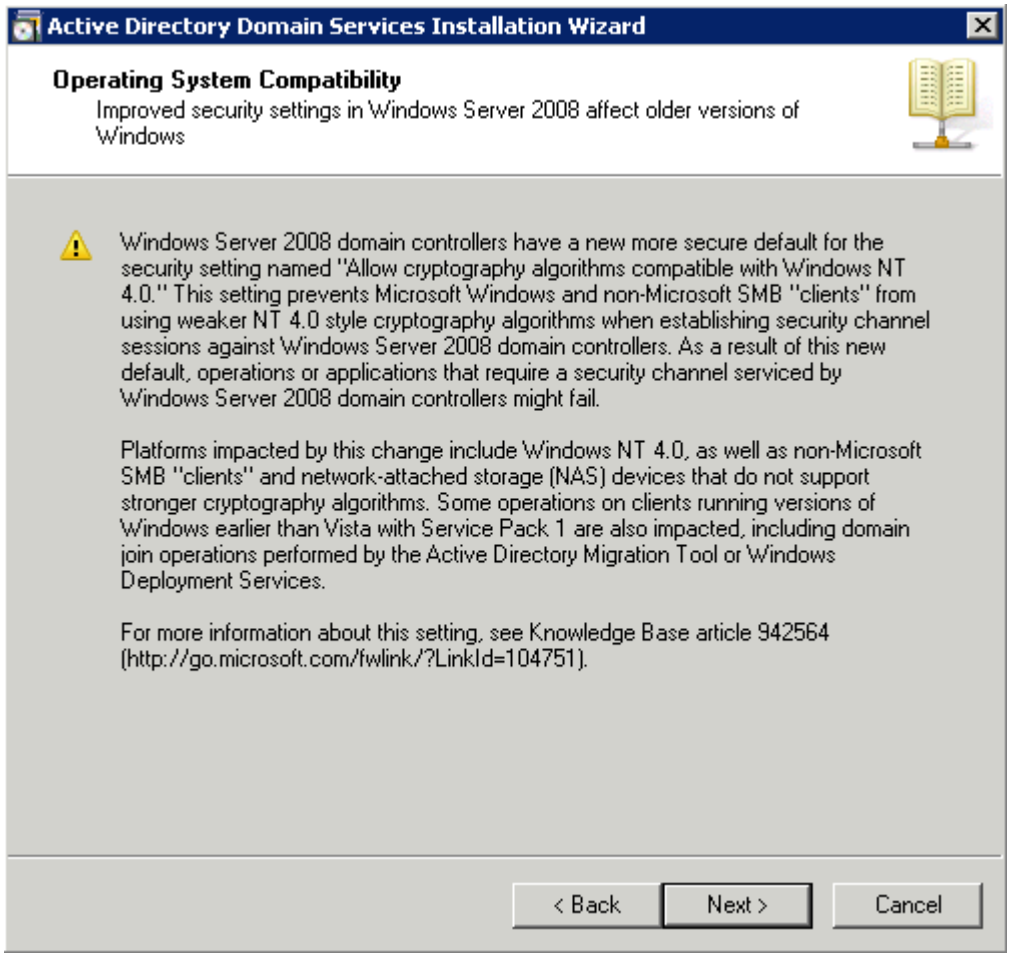
7. Fare clic su Chiudi la procedura guidata e avviare l'Installazione guidata Servizi di dominio Active Directory (dcpromo.exe) per continuare l'installazione e la configurazione di Active Directory.



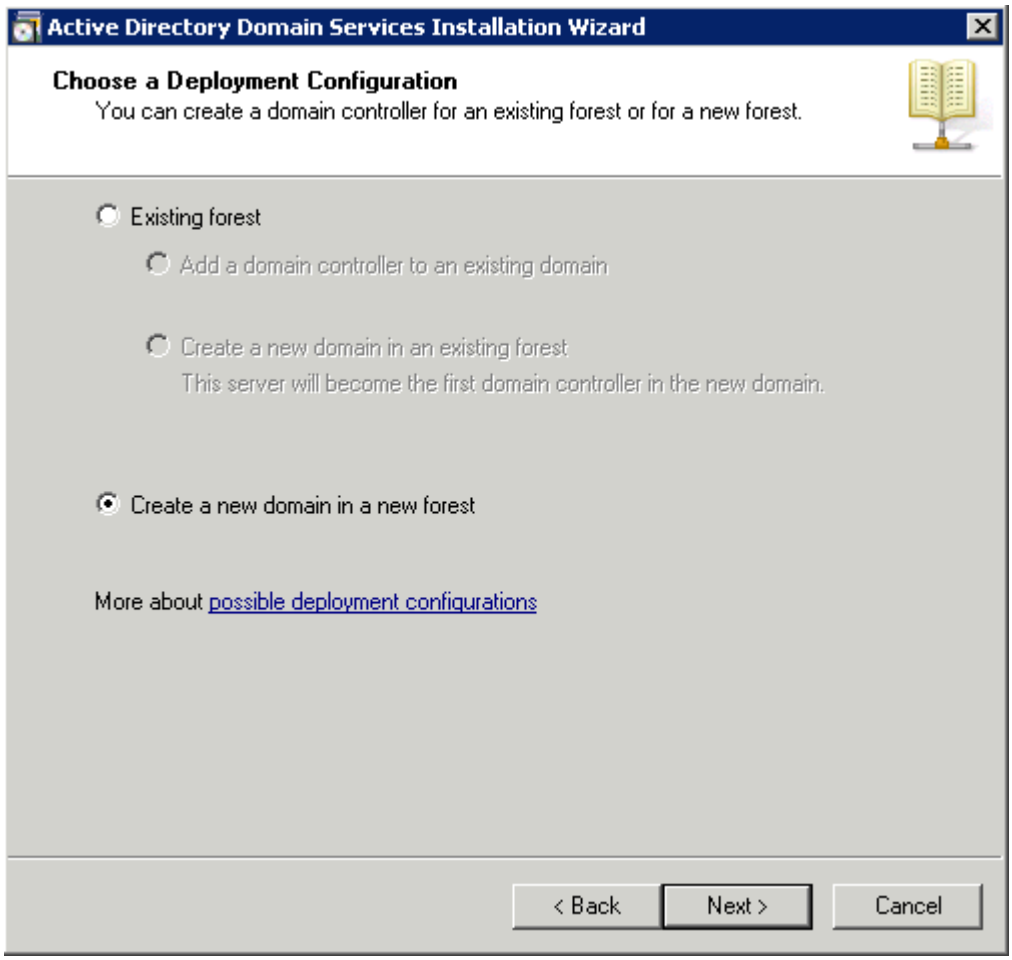
8. Fare clic su Avanti per eseguire l'Installazione guidata Servizi di dominio Active Directory.



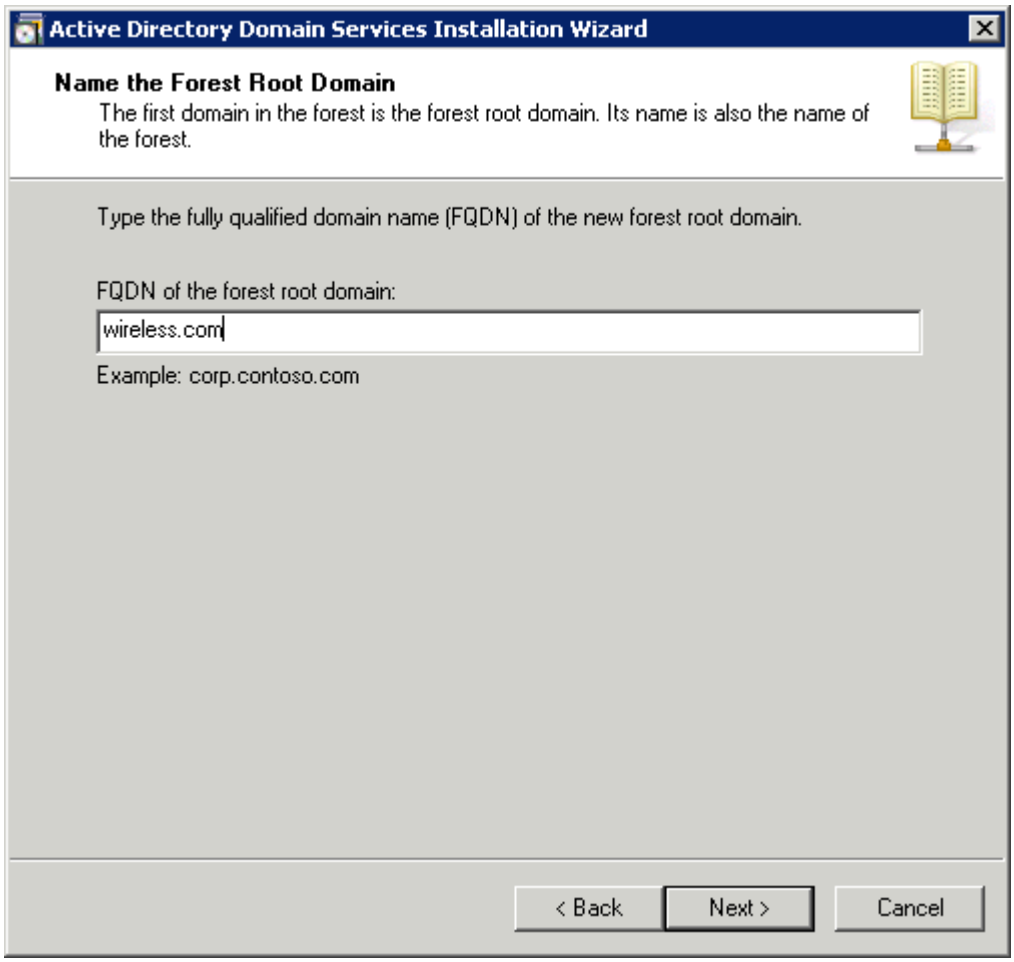
9. Esaminare le informazioni relative alla compatibilità del sistema operativo e fare clic su Avanti.



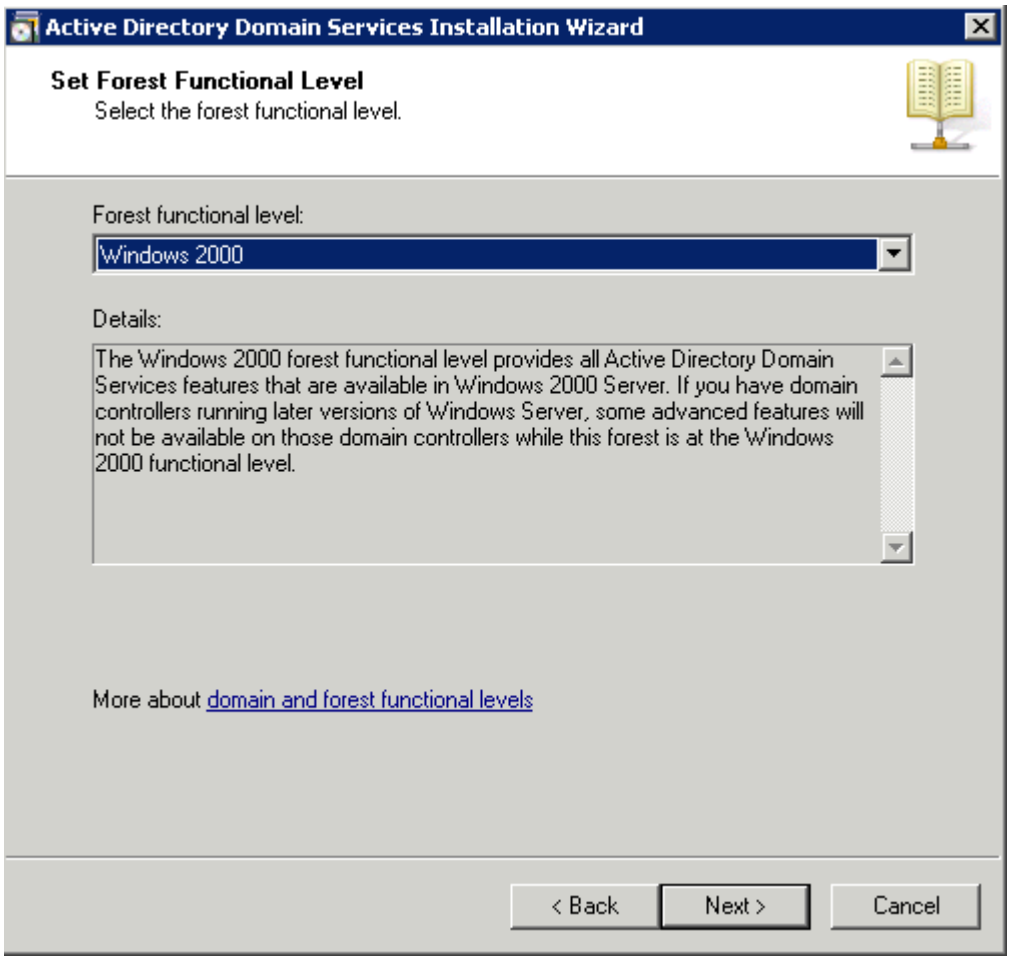
10. Per creare un nuovo dominio, fare clic su Crea un nuovo dominio in una nuova foresta >Avanti.



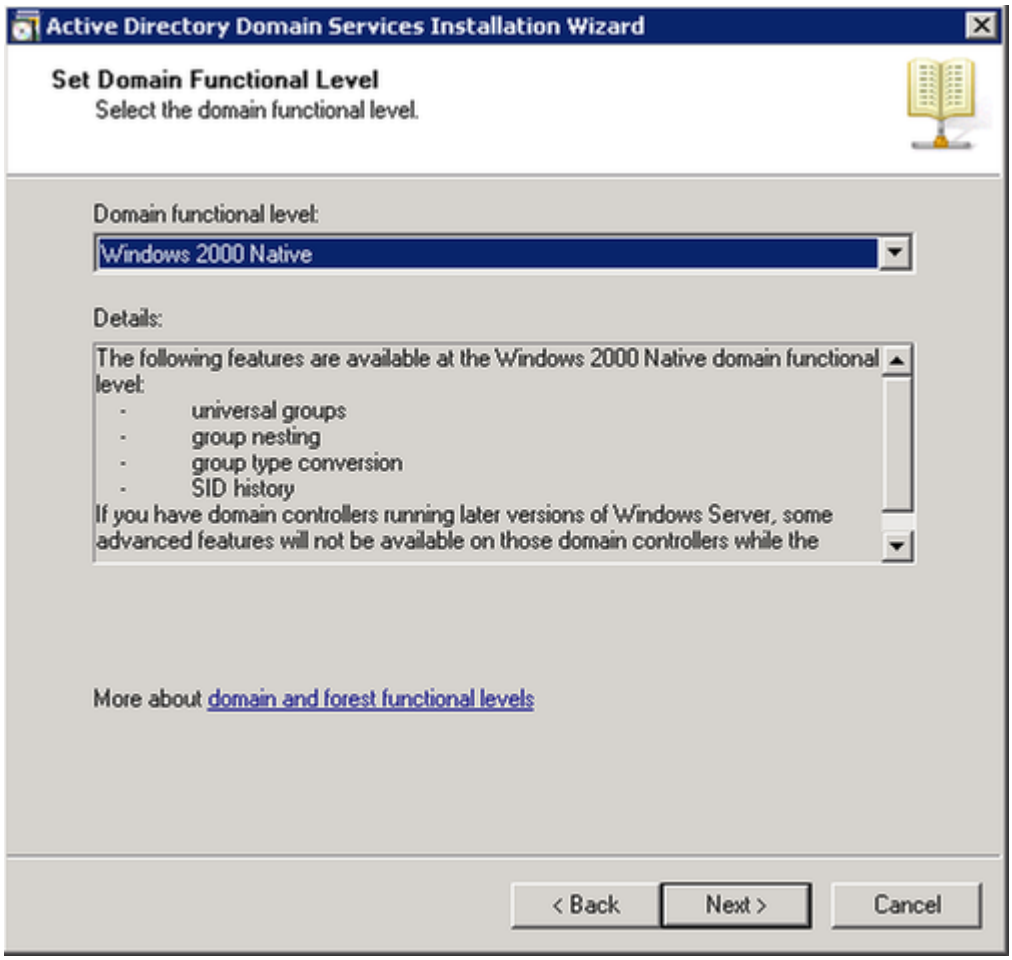
11. Immettere il nome DNS completo per il nuovo dominio e fare clic su Avanti.



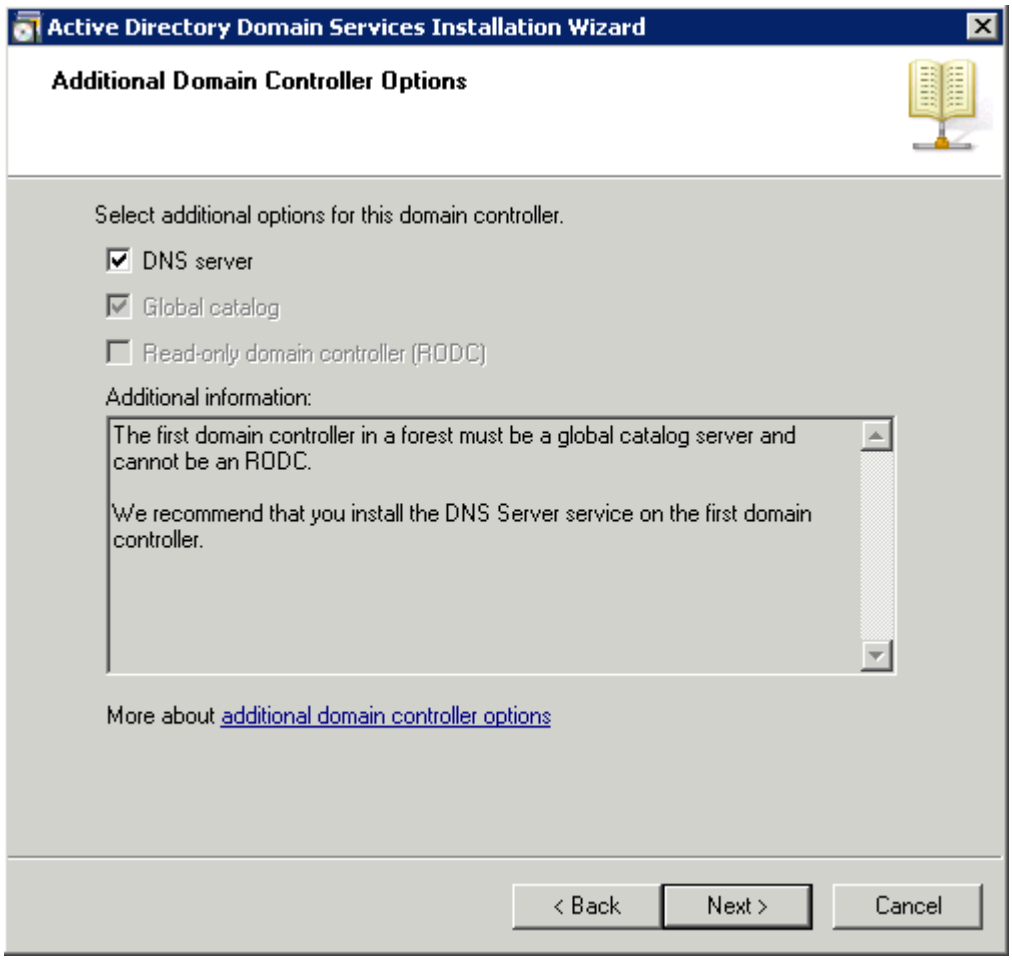
12. Selezionare il livello di funzionalità della foresta per il dominio e fare clic su Avanti.



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

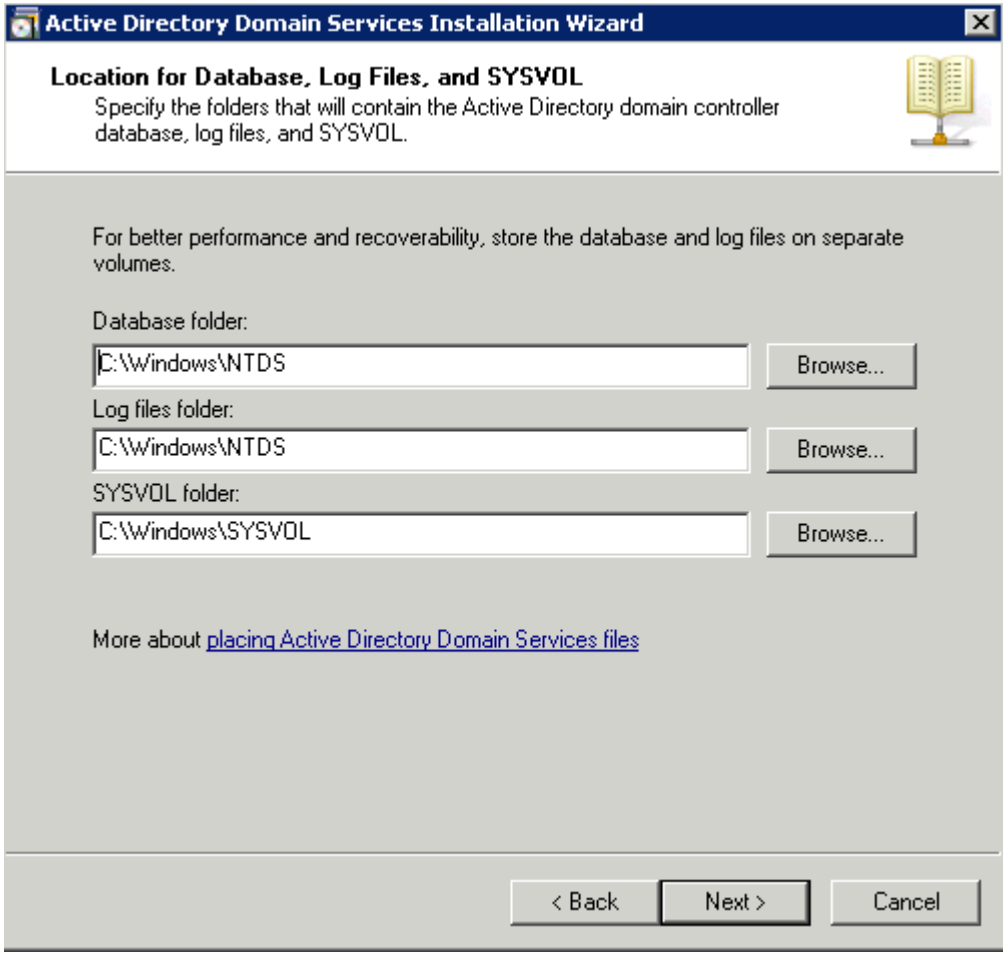


14. Verificare che il server DNS sia selezionato e fare clic su Avanti.

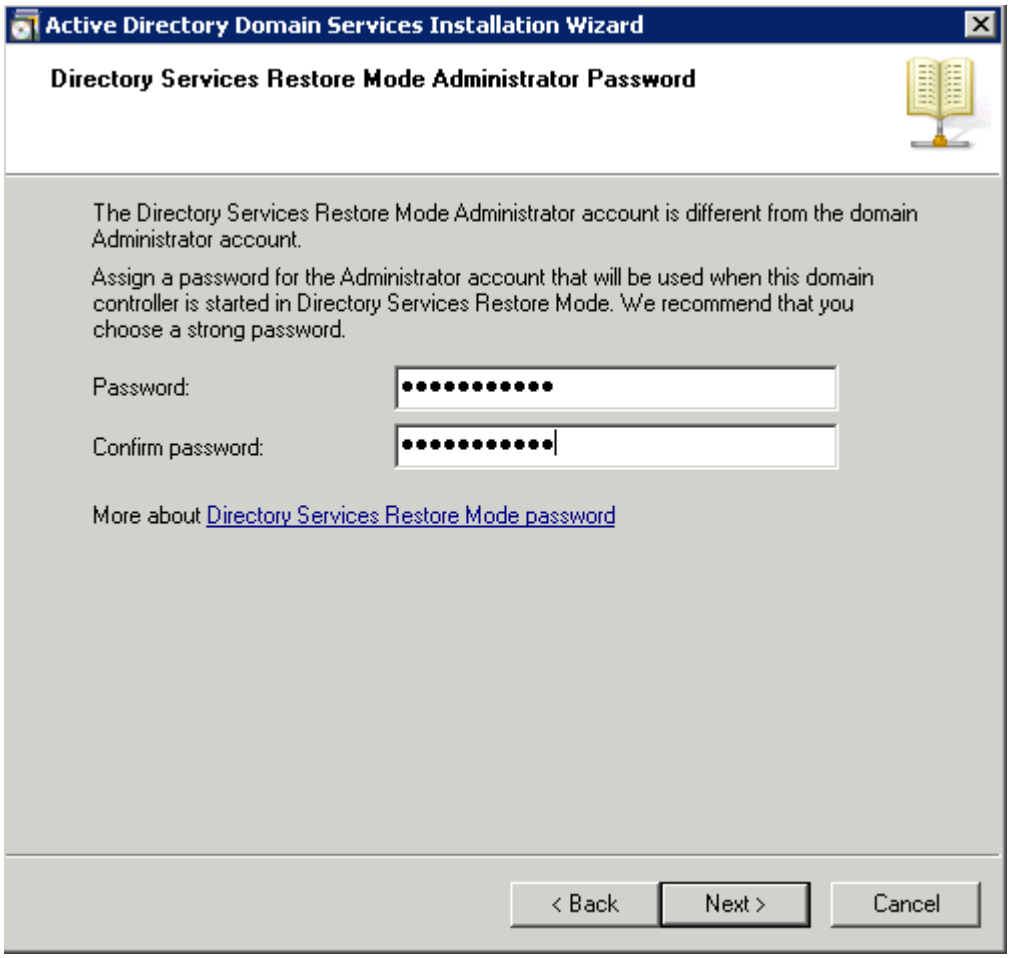


15. Fare clic su Sì per creare una nuova zona in DNS per il dominio durante l'installazione guidata.

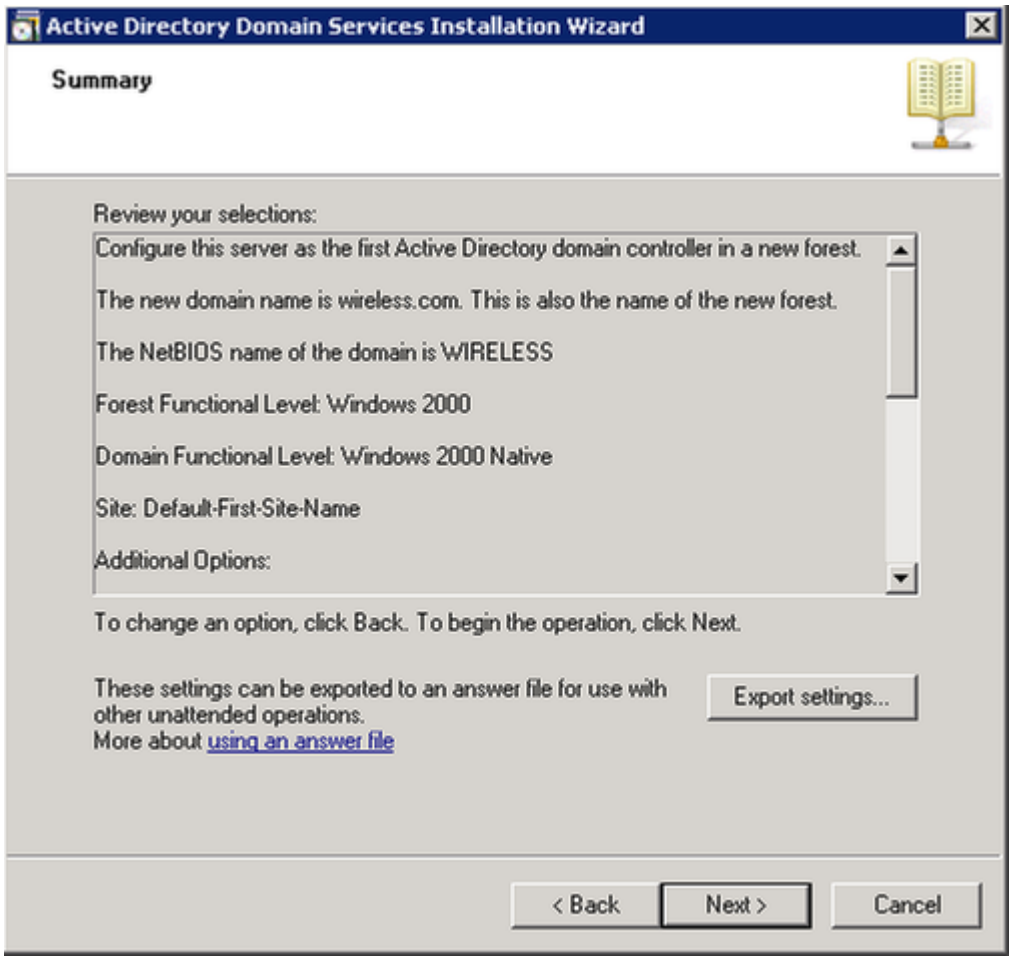
16. Selezionare le cartelle che devono essere utilizzate da Active Directory per i file e fare clic su Avanti.



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

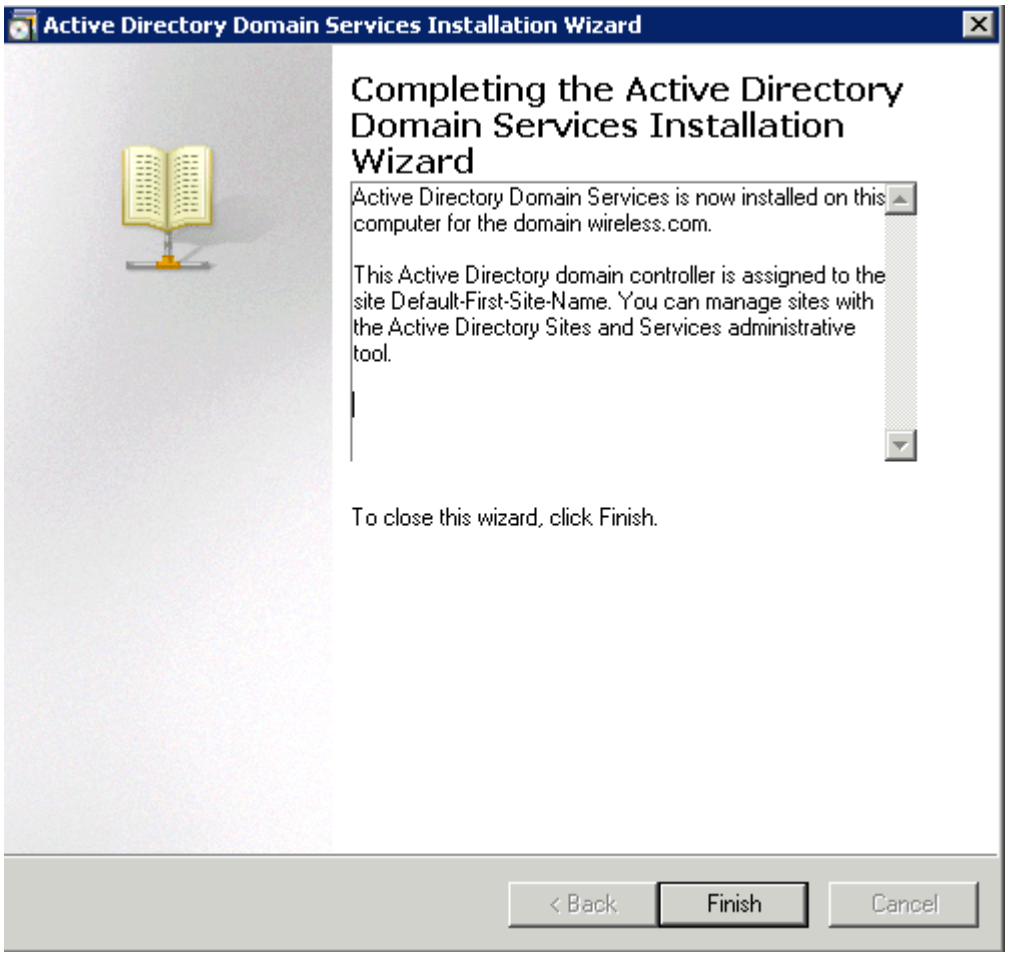


18. Verificare le selezioni e fare clic su Avanti.

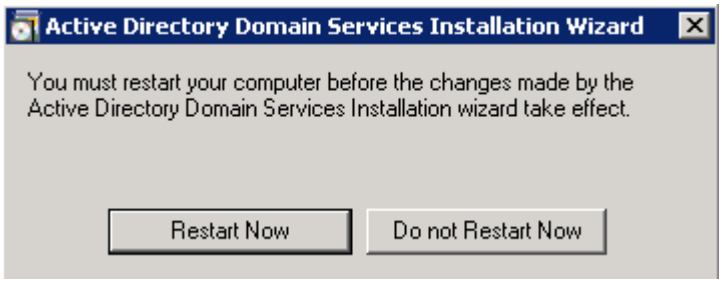


L'installazione procede.

19. Scegliere Fine per chiudere la procedura guidata.



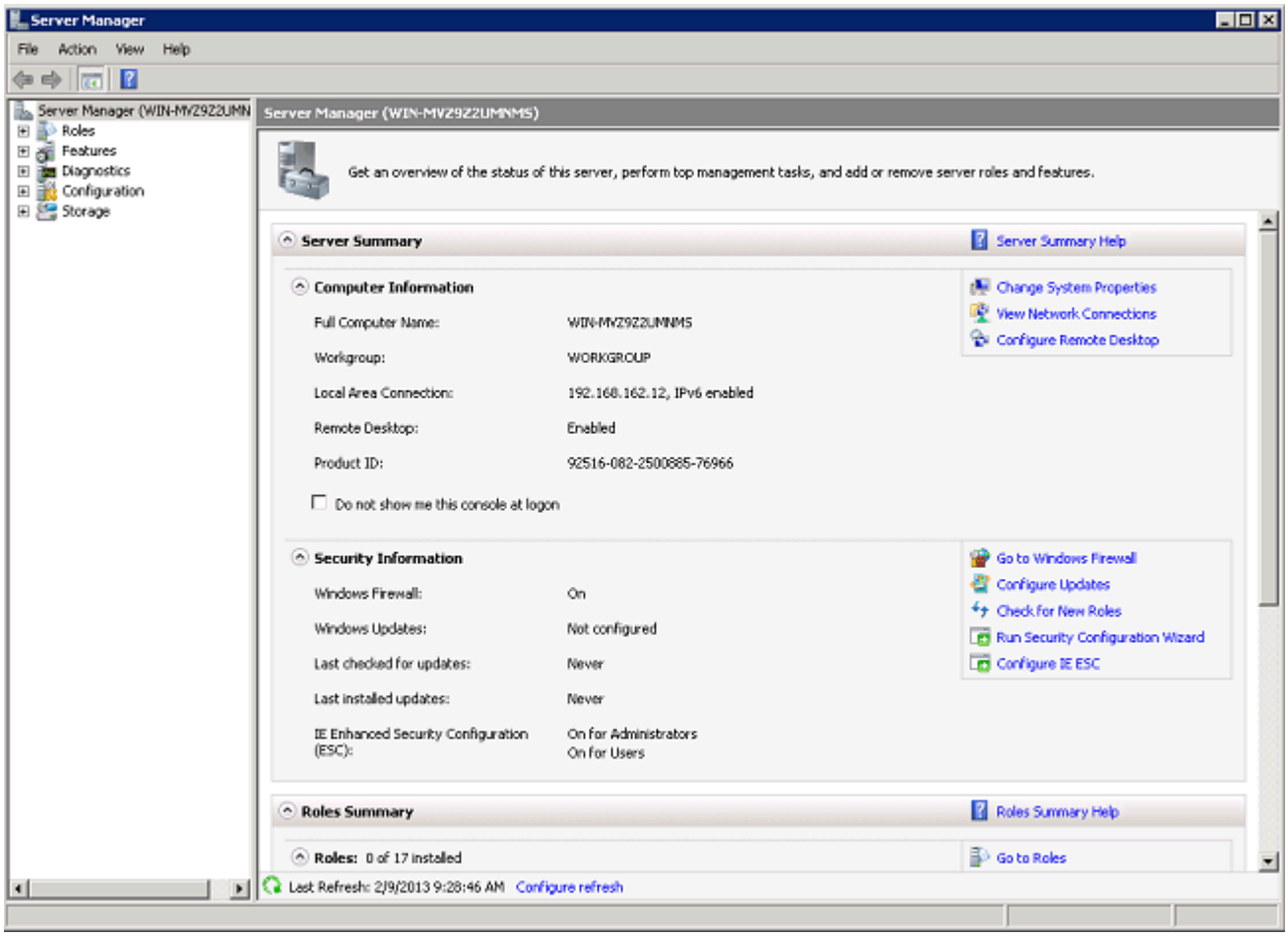
20. Riavviare il server per rendere effettive le modifiche.



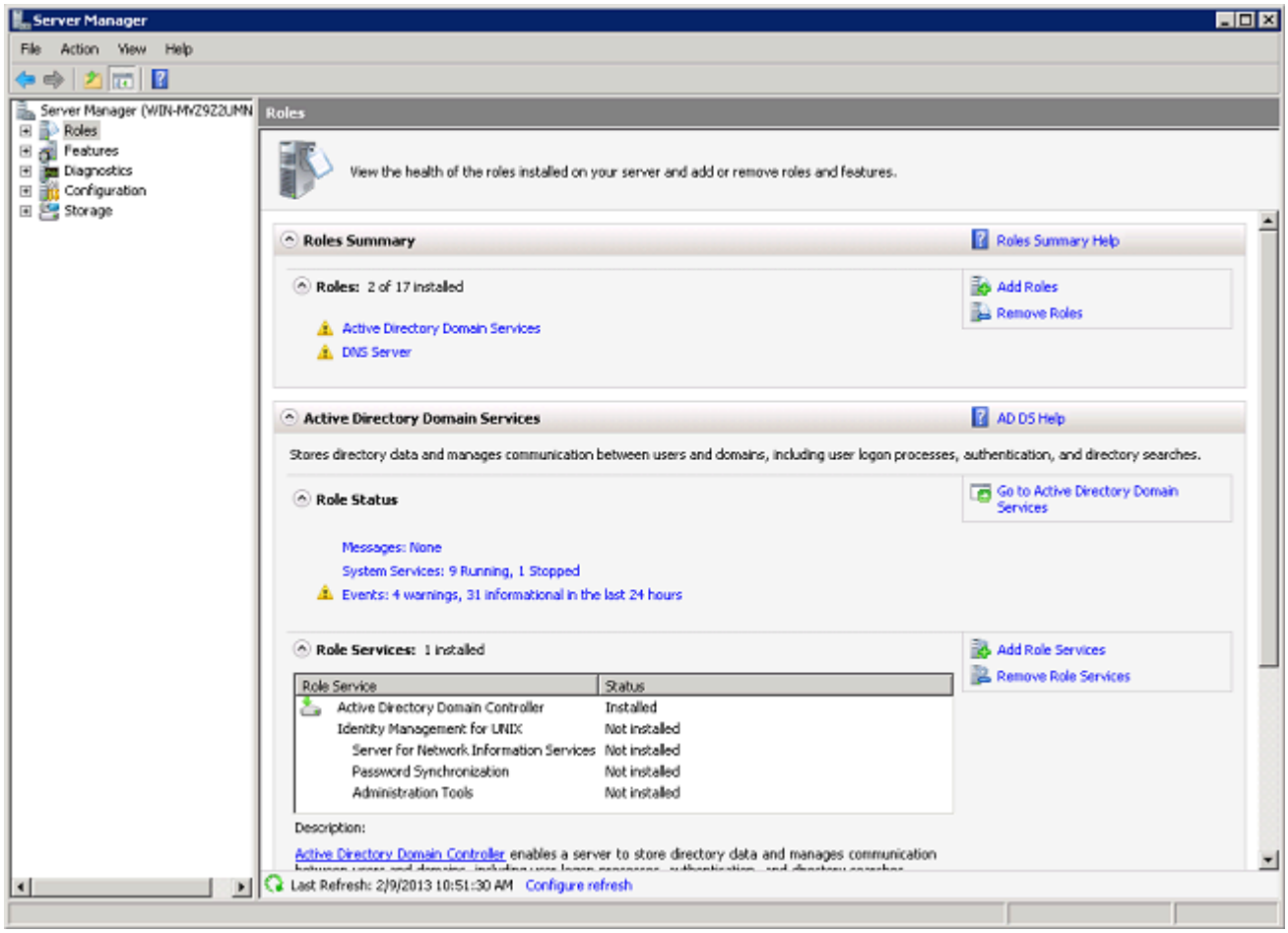
Installare e configurare i servizi DHCP in Microsoft Windows 2008 Server

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:

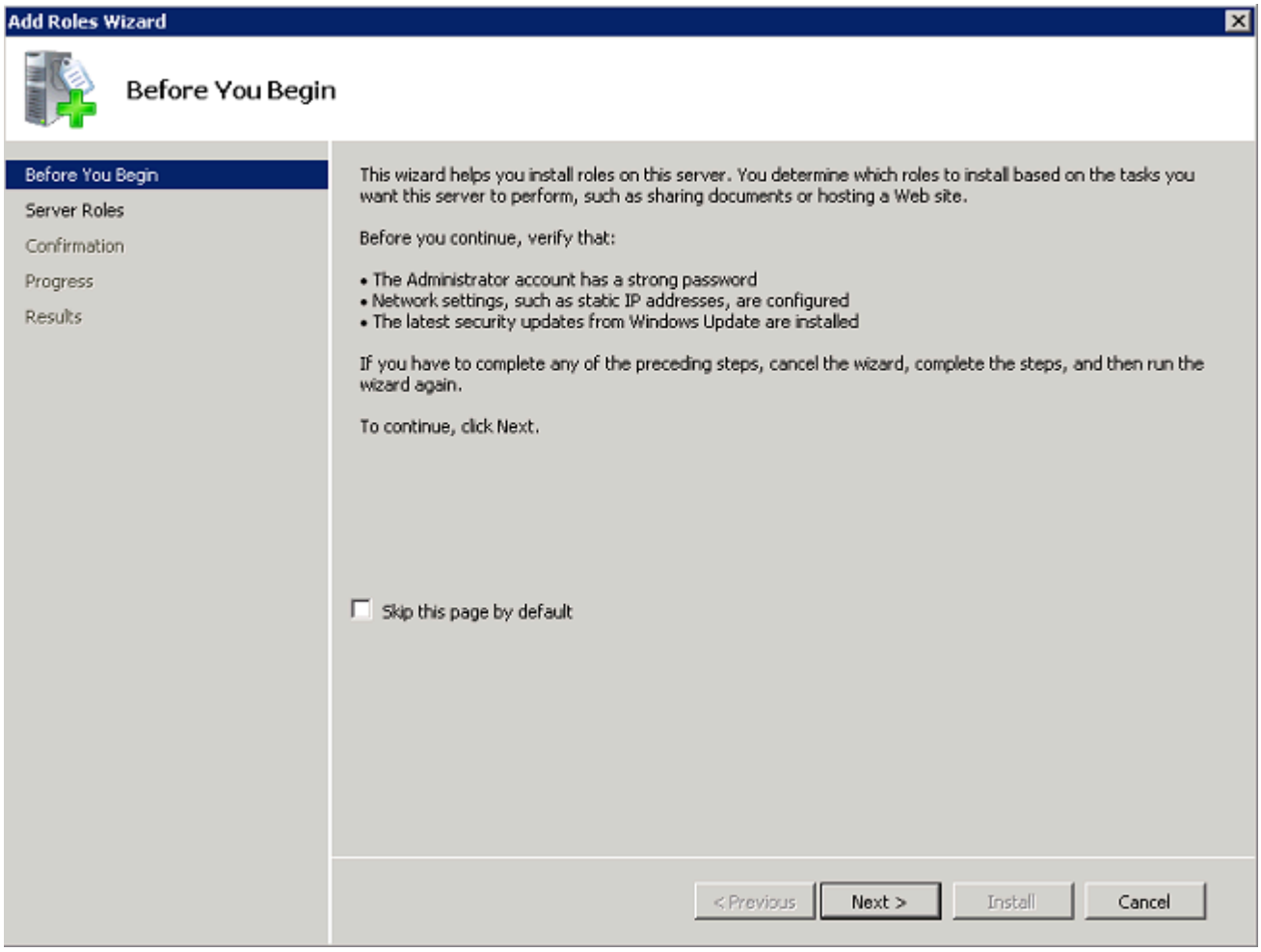
1. Fare clic su Start>Server Manager.



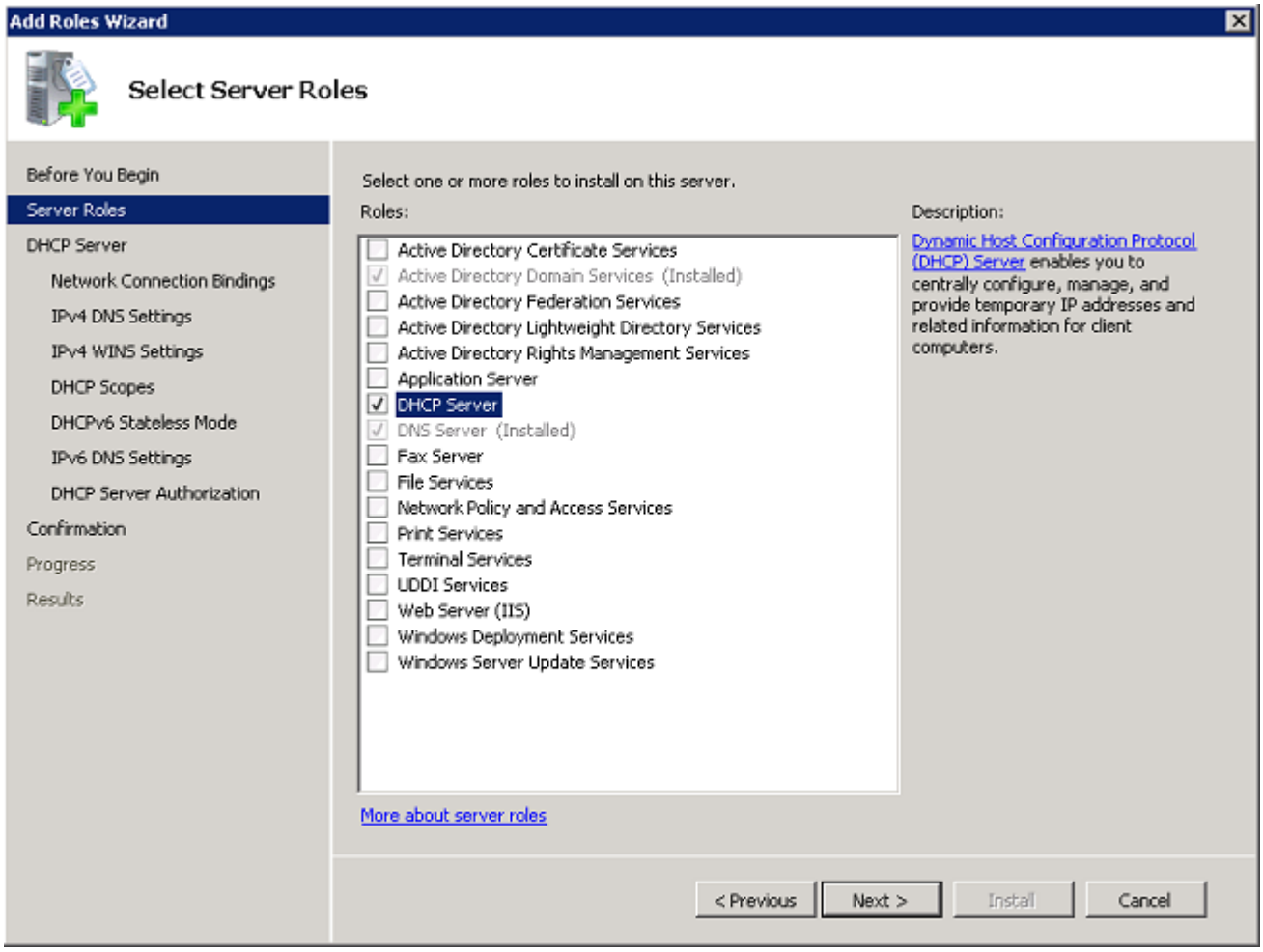
2. Fare clic su Ruoli> Aggiungi ruoli.



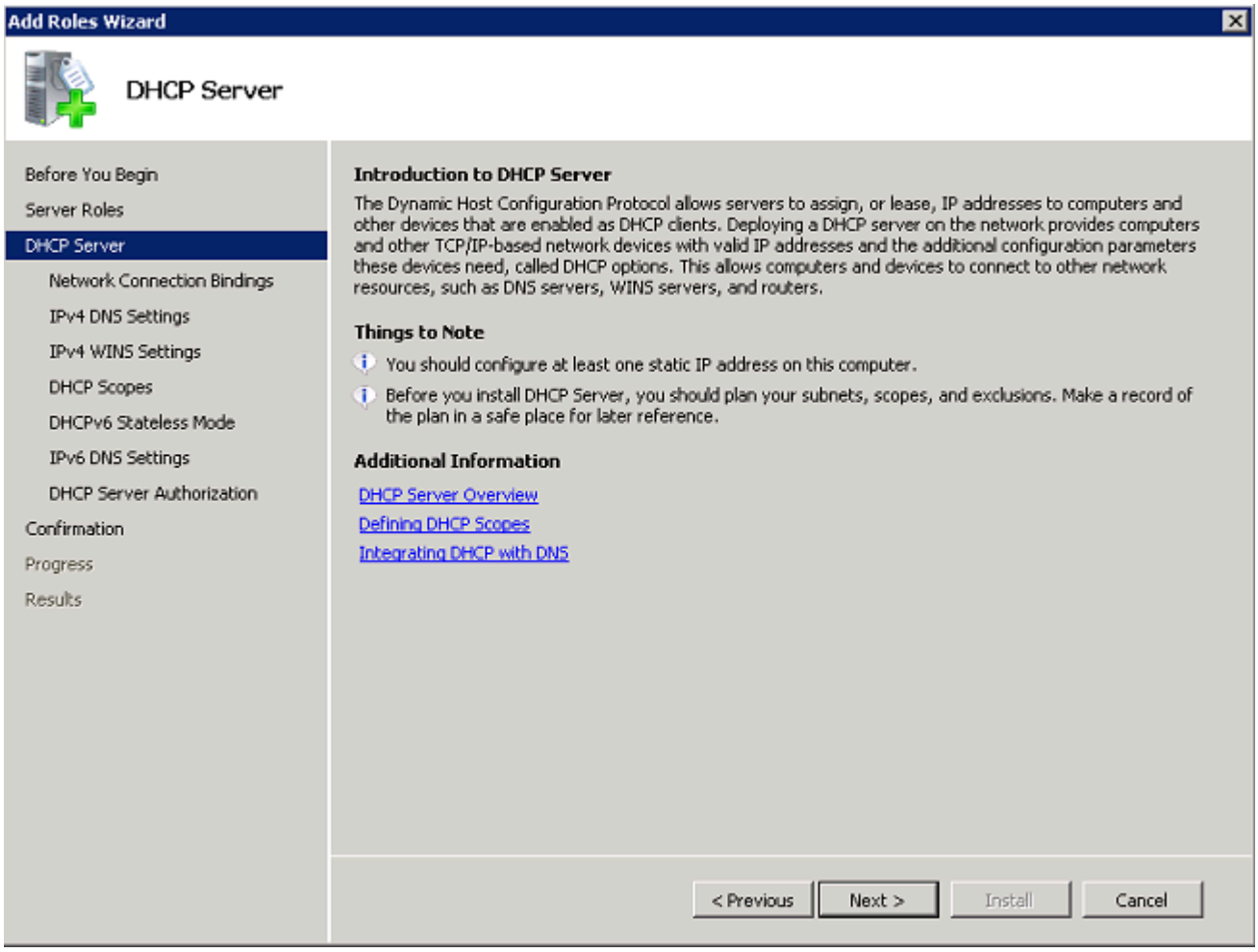
3. Fare clic su Next (Avanti).



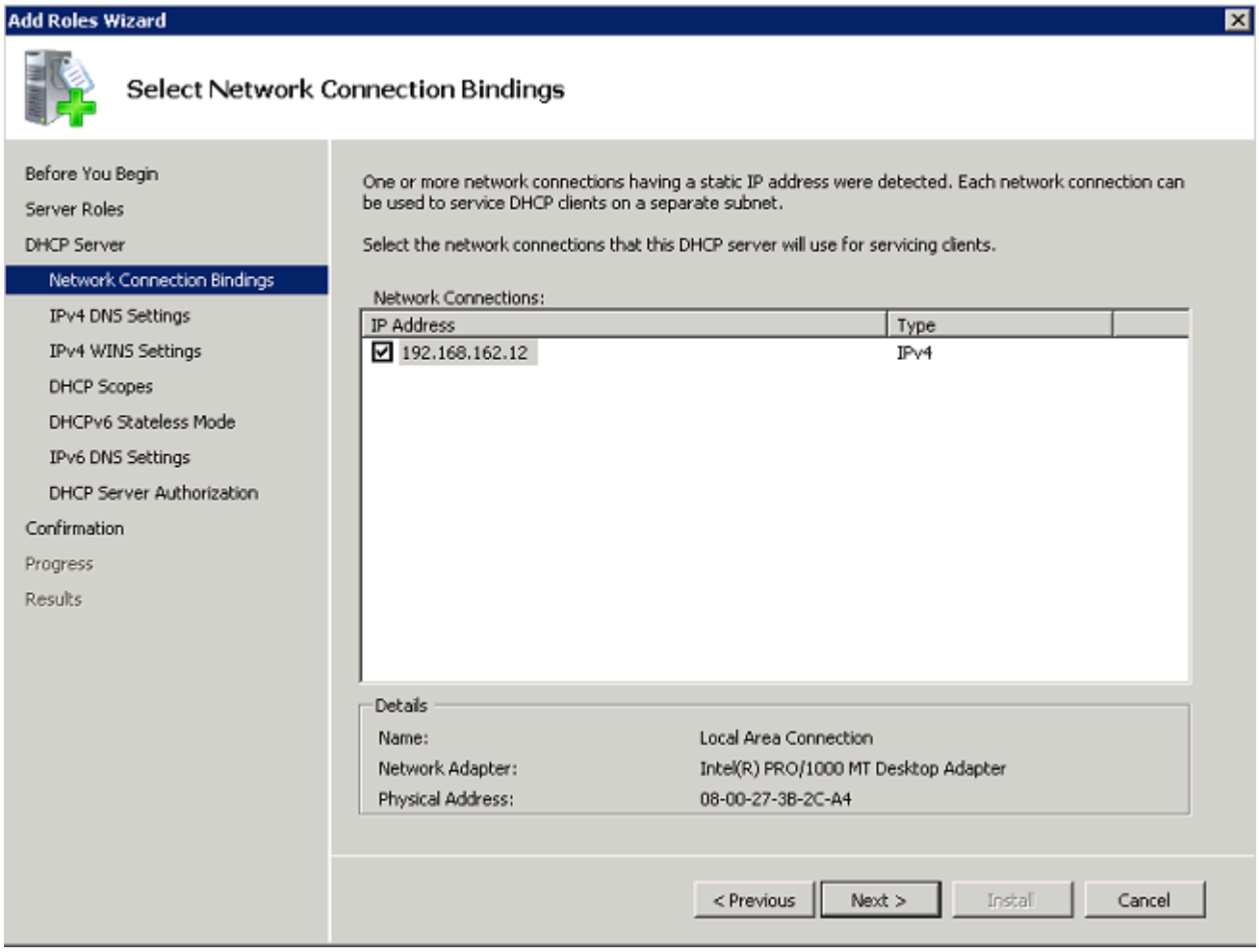
4. Selezionare il servizio DHCP Server, quindi fare clic su Avanti.



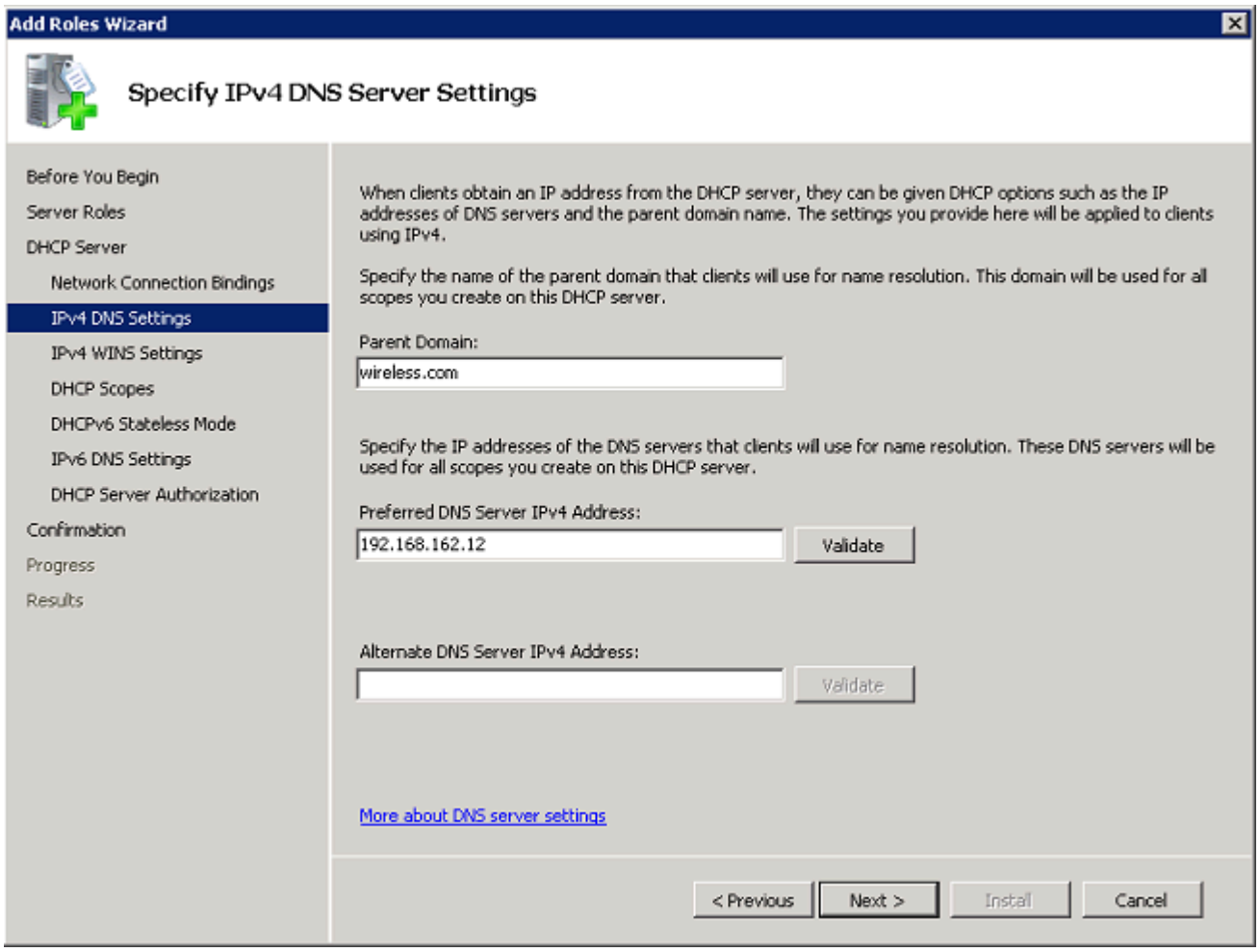
5. Rivedere l'Introduzione al server DHCP e fare clic su Avanti.



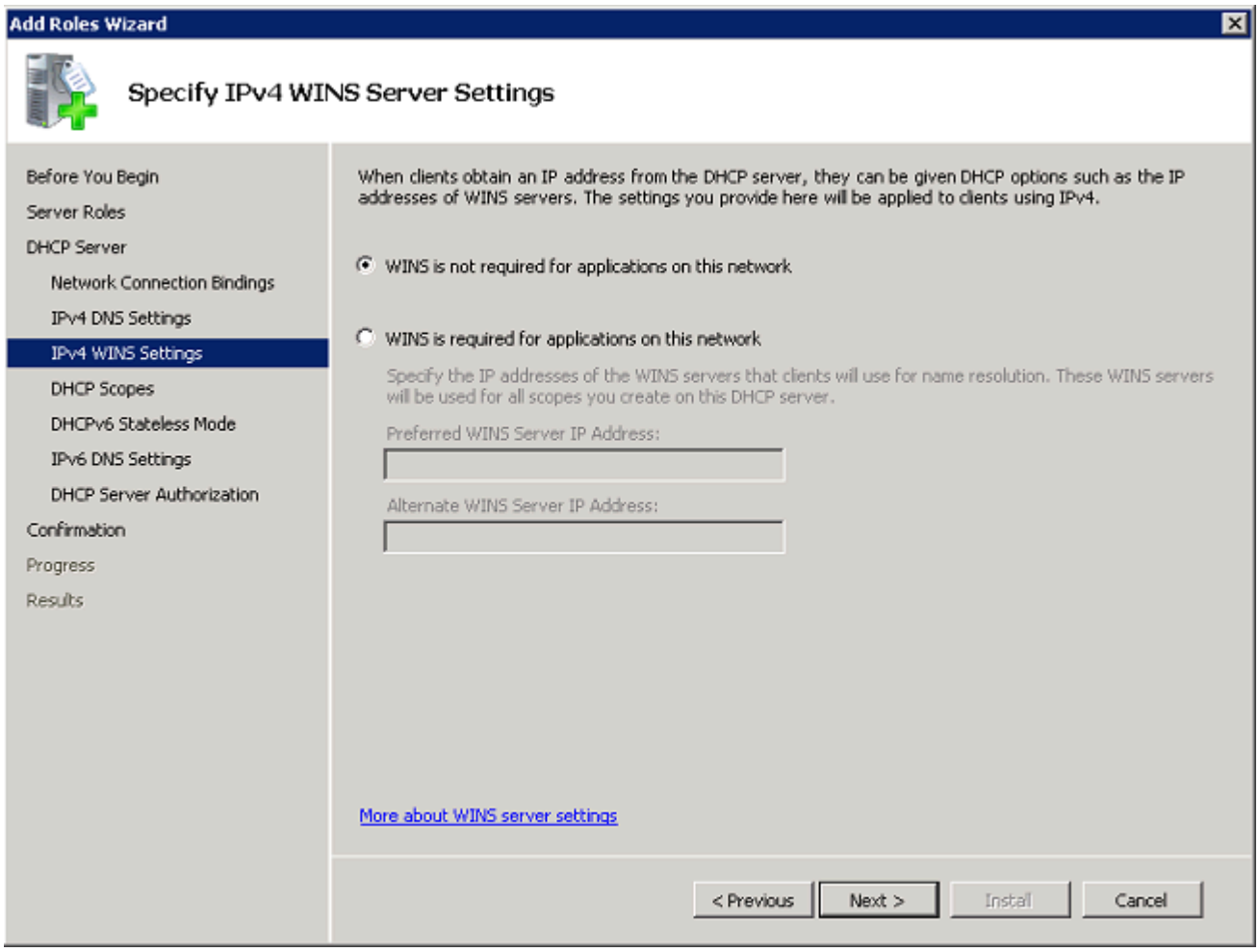
6. Selezionare l'interfaccia che il server DHCP deve monitorare per le richieste e fare clic su Avanti.



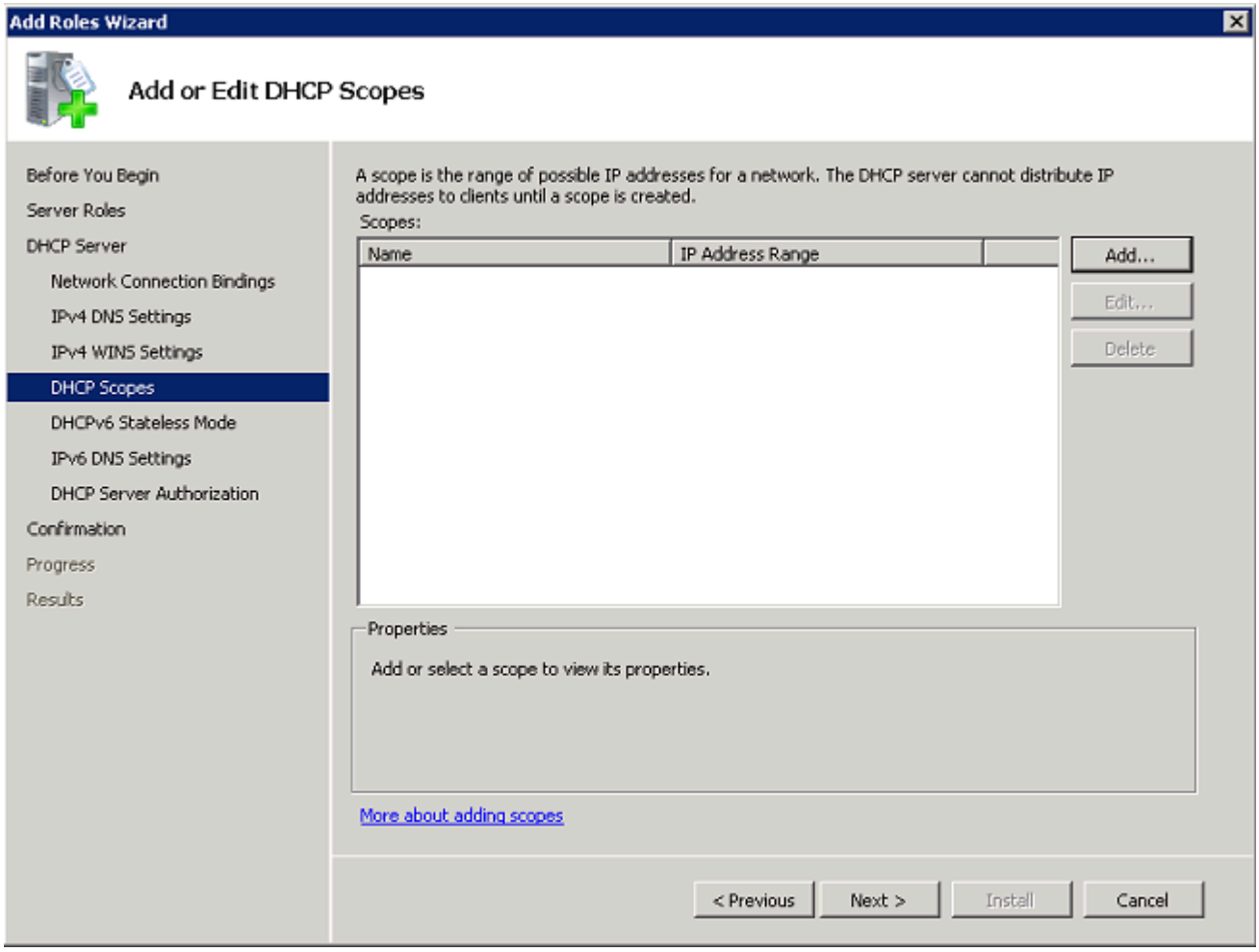
7. Configurare le impostazioni DNS predefinite che il server DHCP deve fornire ai client e fare clic su Avanti.



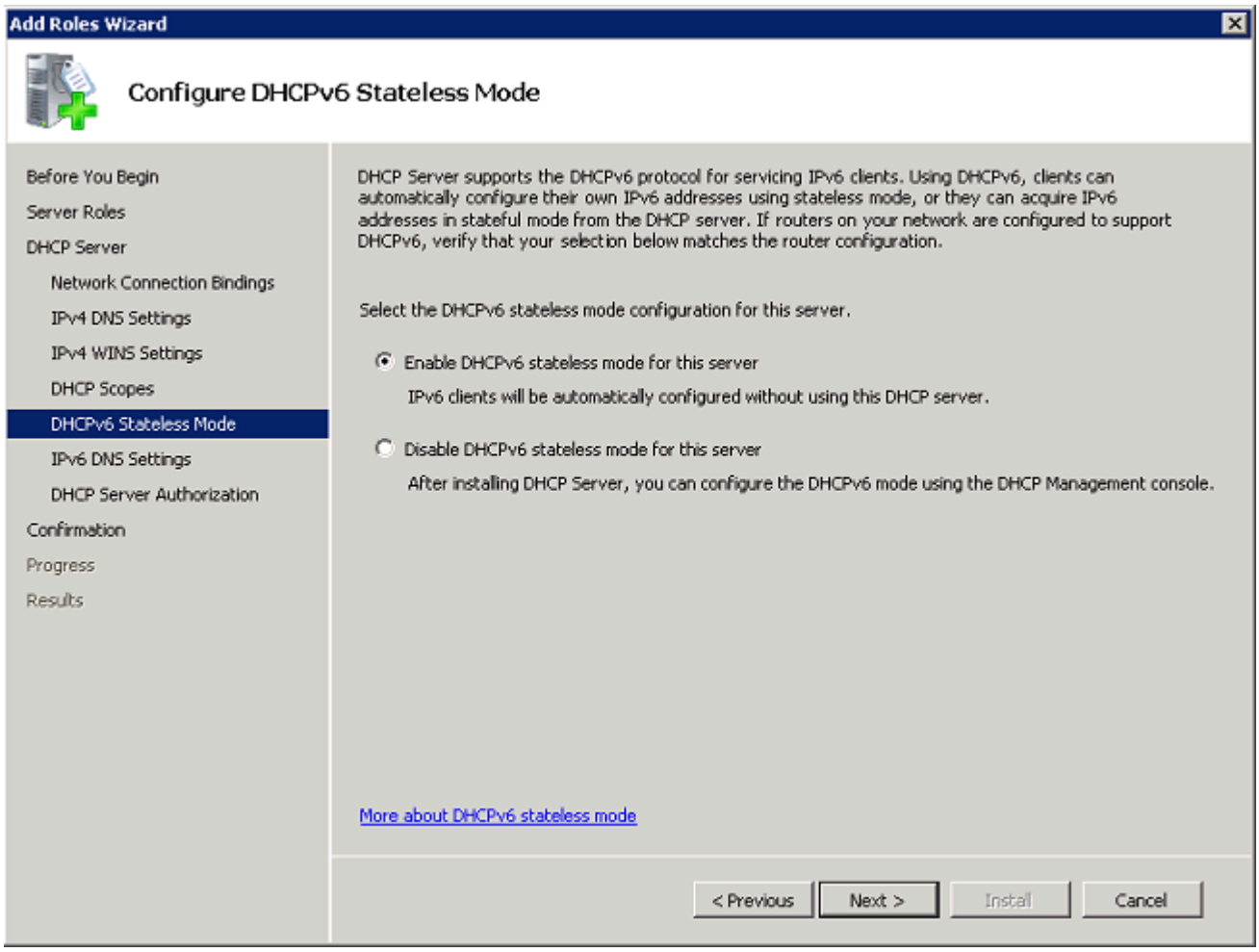
8. Configurare WINS se la rete supporta WINS.



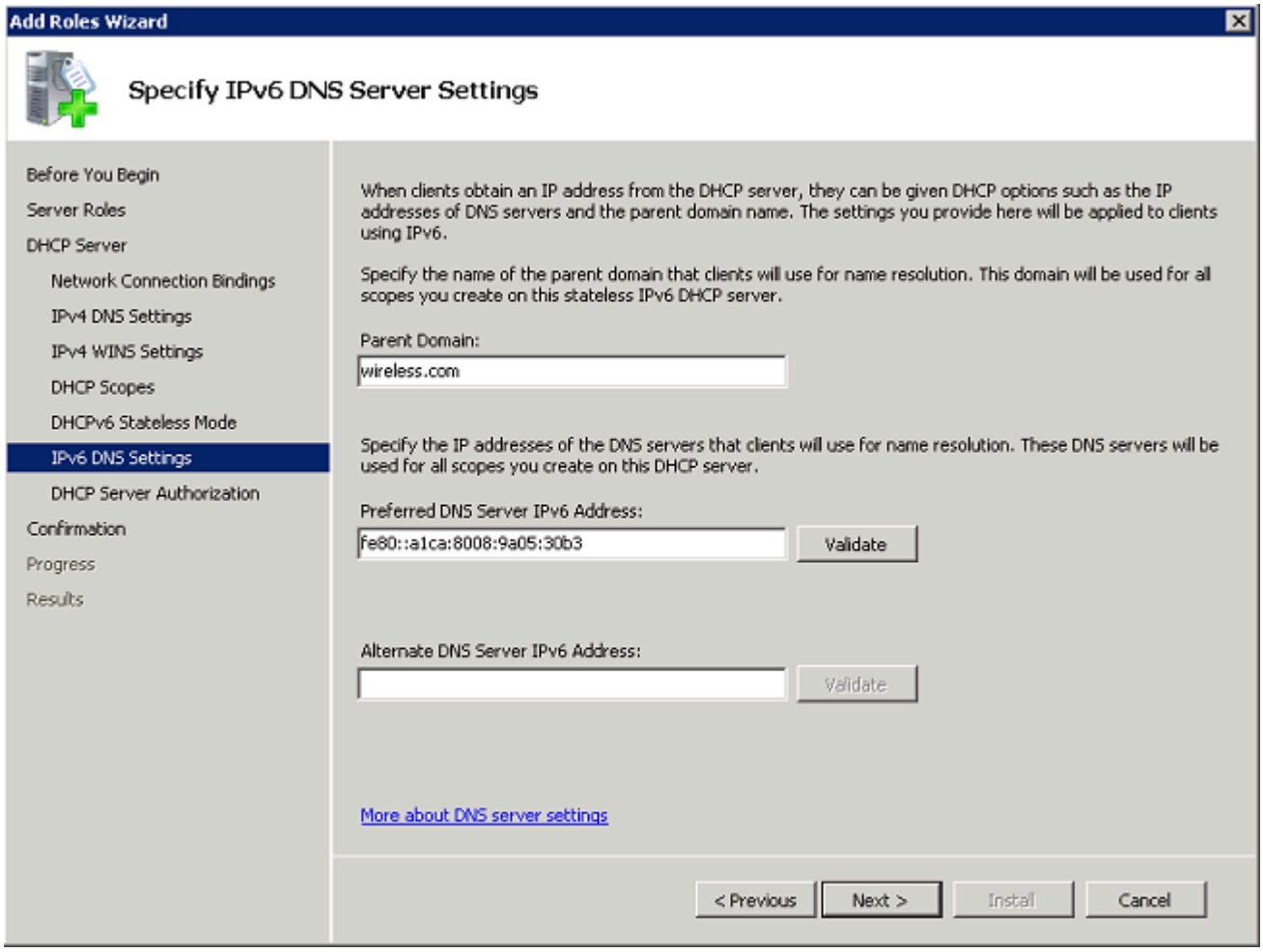
9. Fare clic su Add per utilizzare la procedura guidata e creare un ambito DHCP oppure fare clic su Next per creare un ambito DHCP in un secondo momento. Fare clic su Next (Avanti) per continuare.



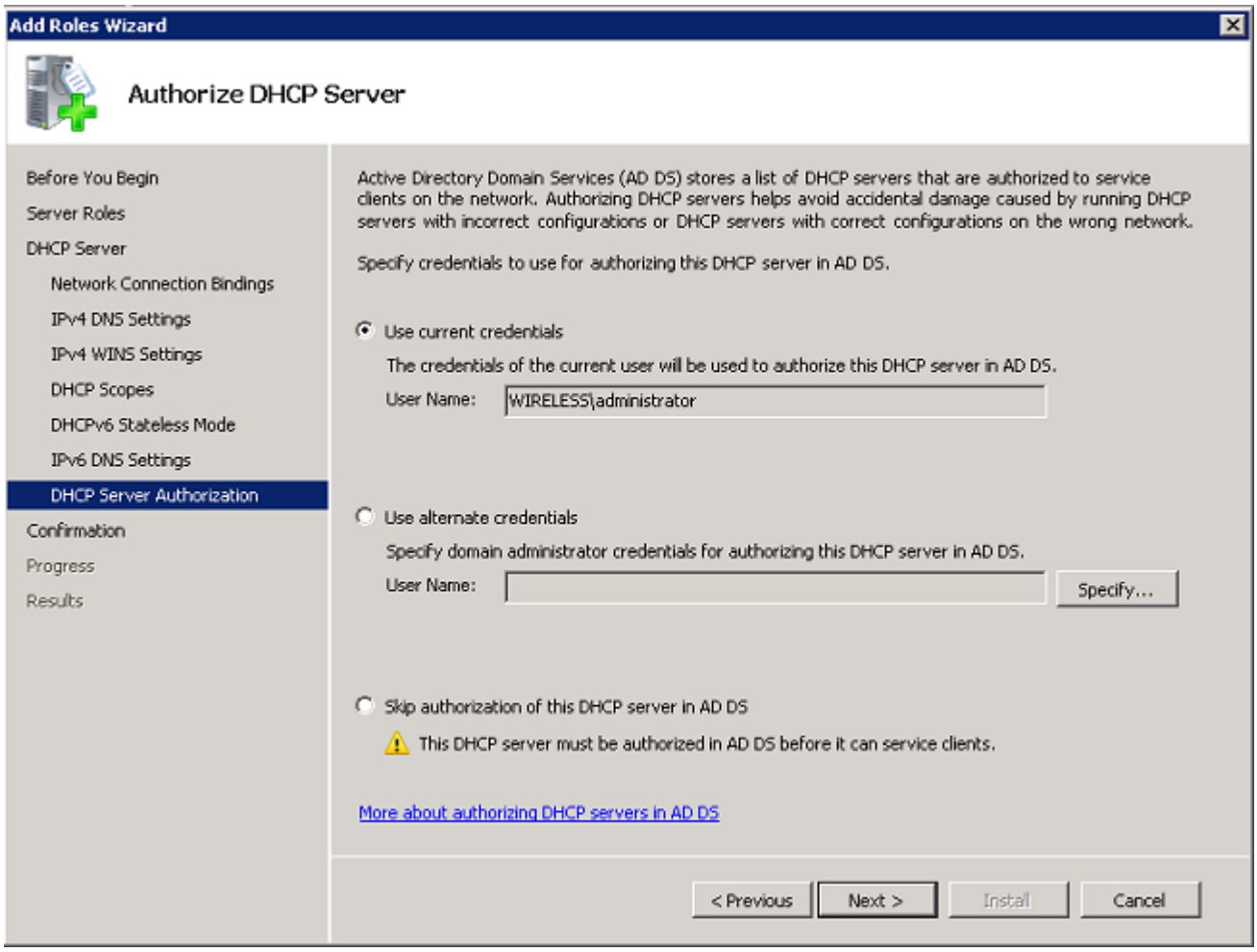
10. Attivare o disattivare il supporto per DHCPv6 nel server e fare clic su Avanti.



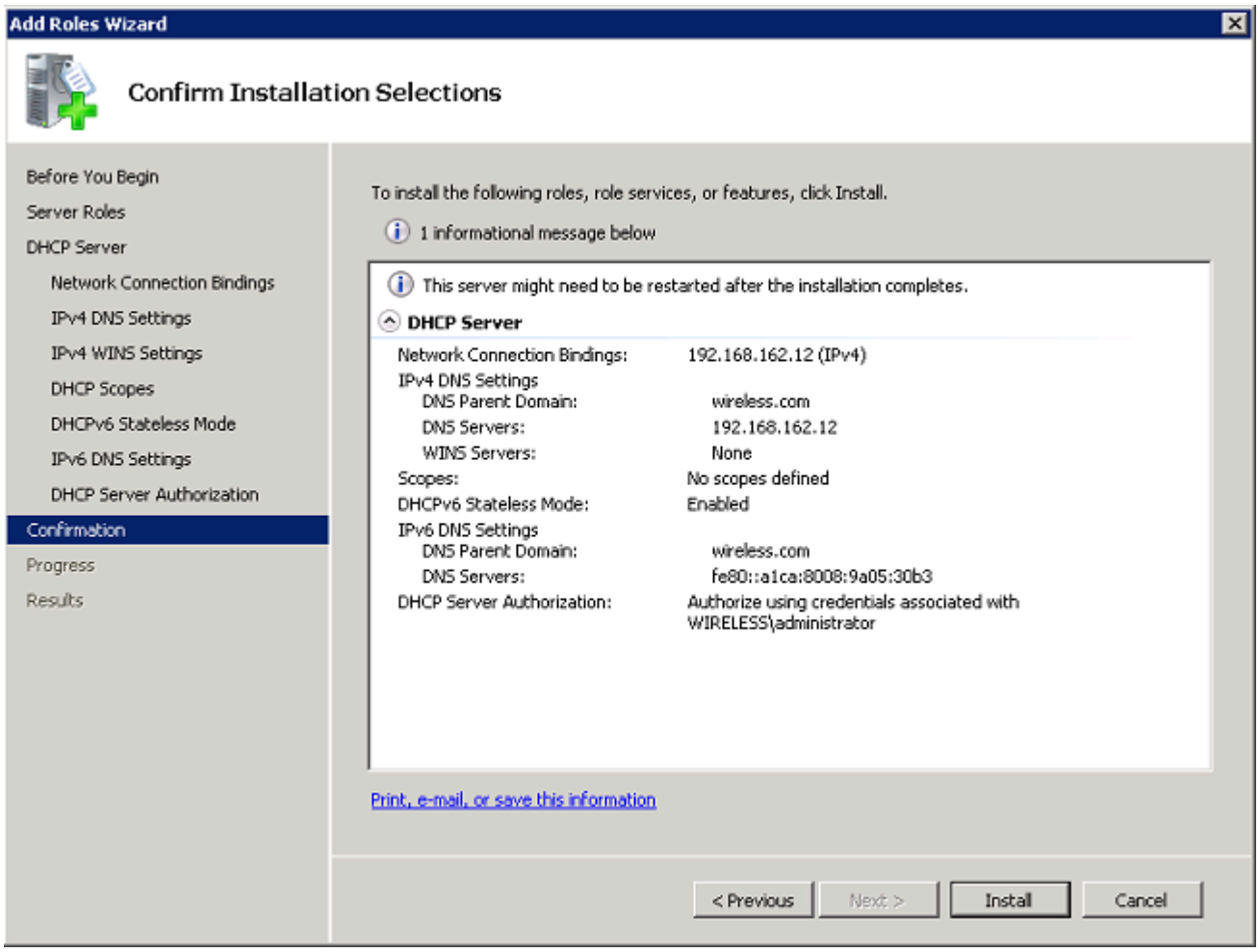
11. Configurare le impostazioni DNS IPv6 se DHCPv6 è stato abilitato nel passaggio precedente. Fare clic su Avanti per continuare.



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

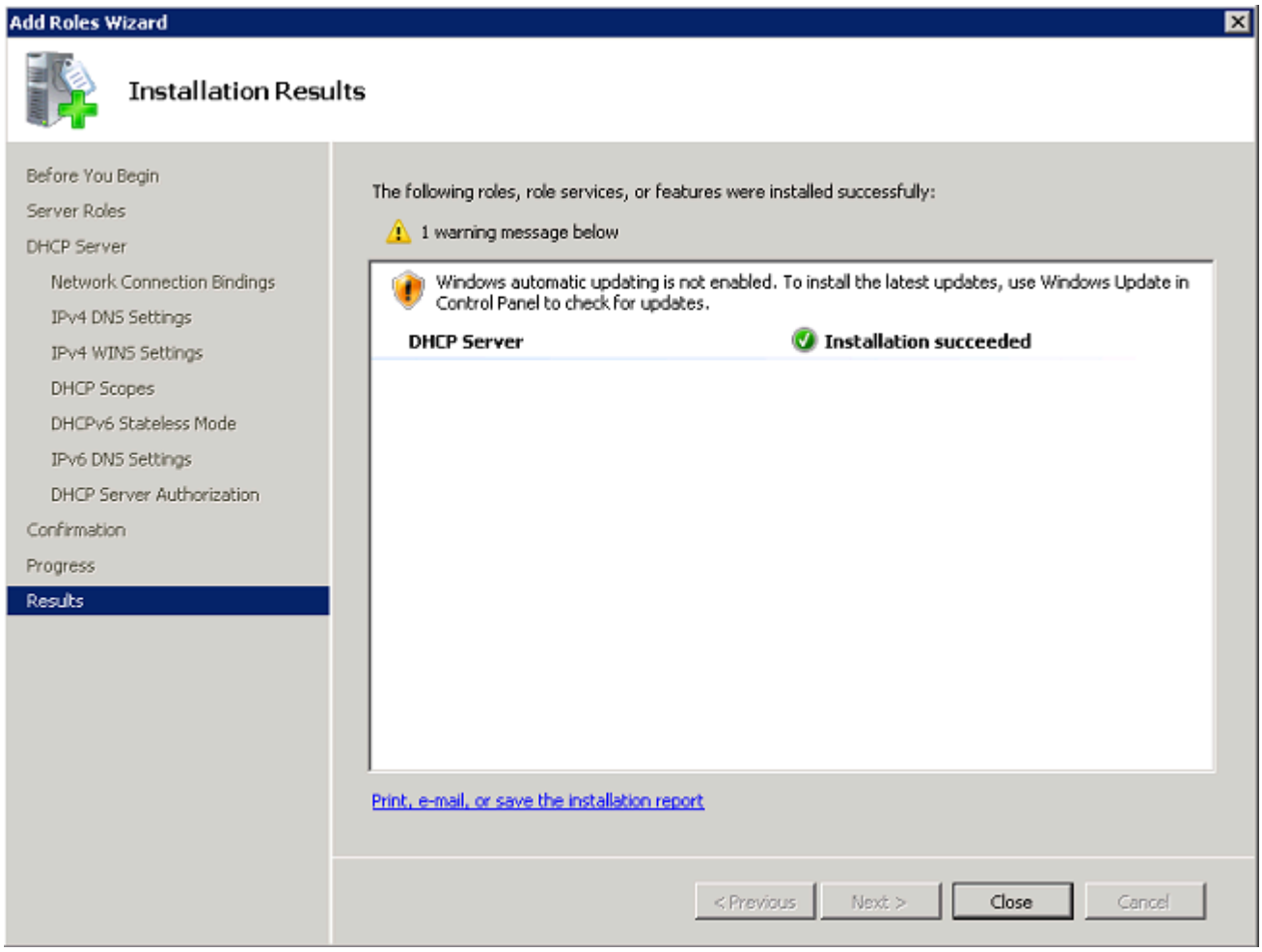


13. Esaminare la configurazione nella pagina di conferma e fare clic su Installa per completare l'installazione.



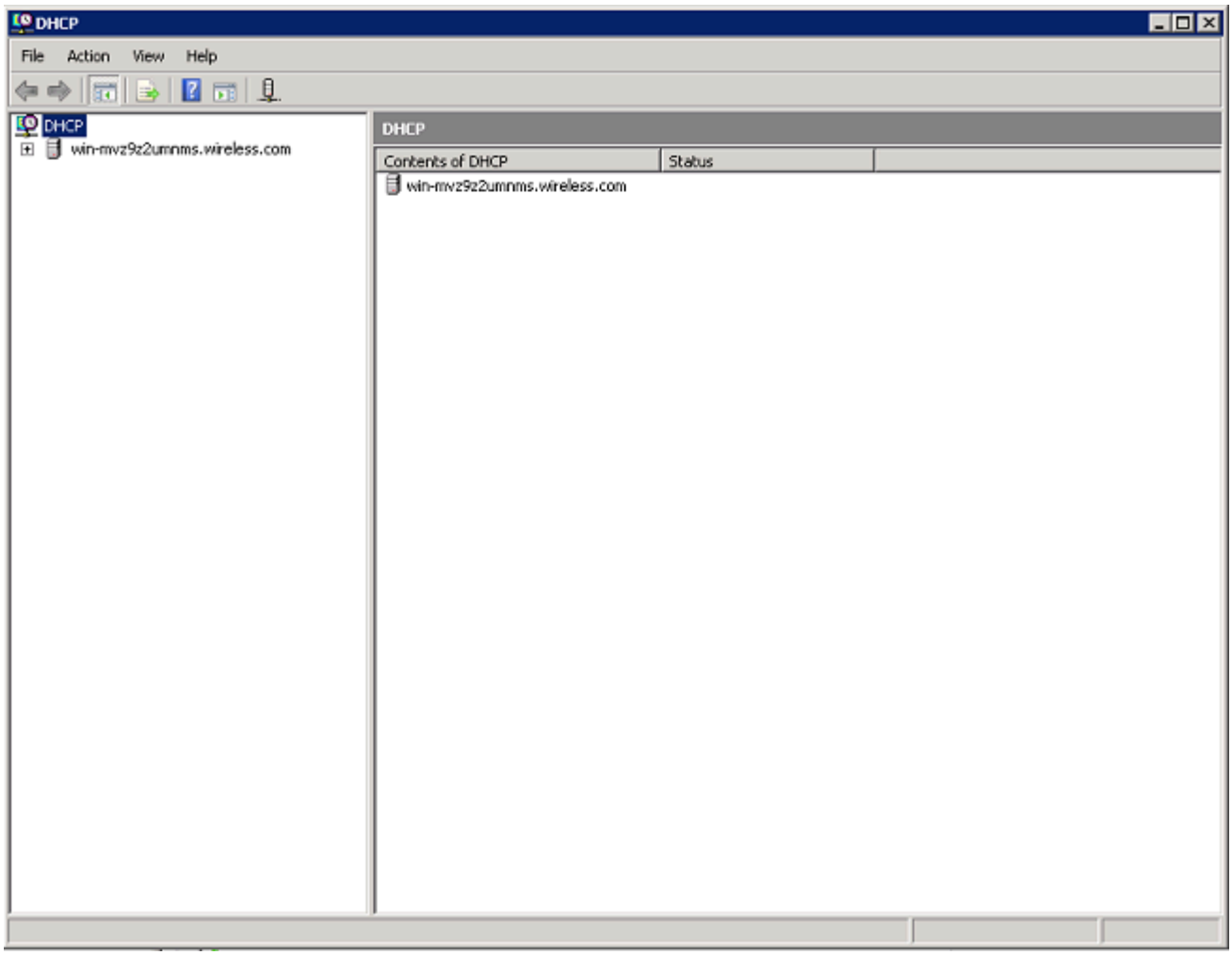
L'installazione procede.

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

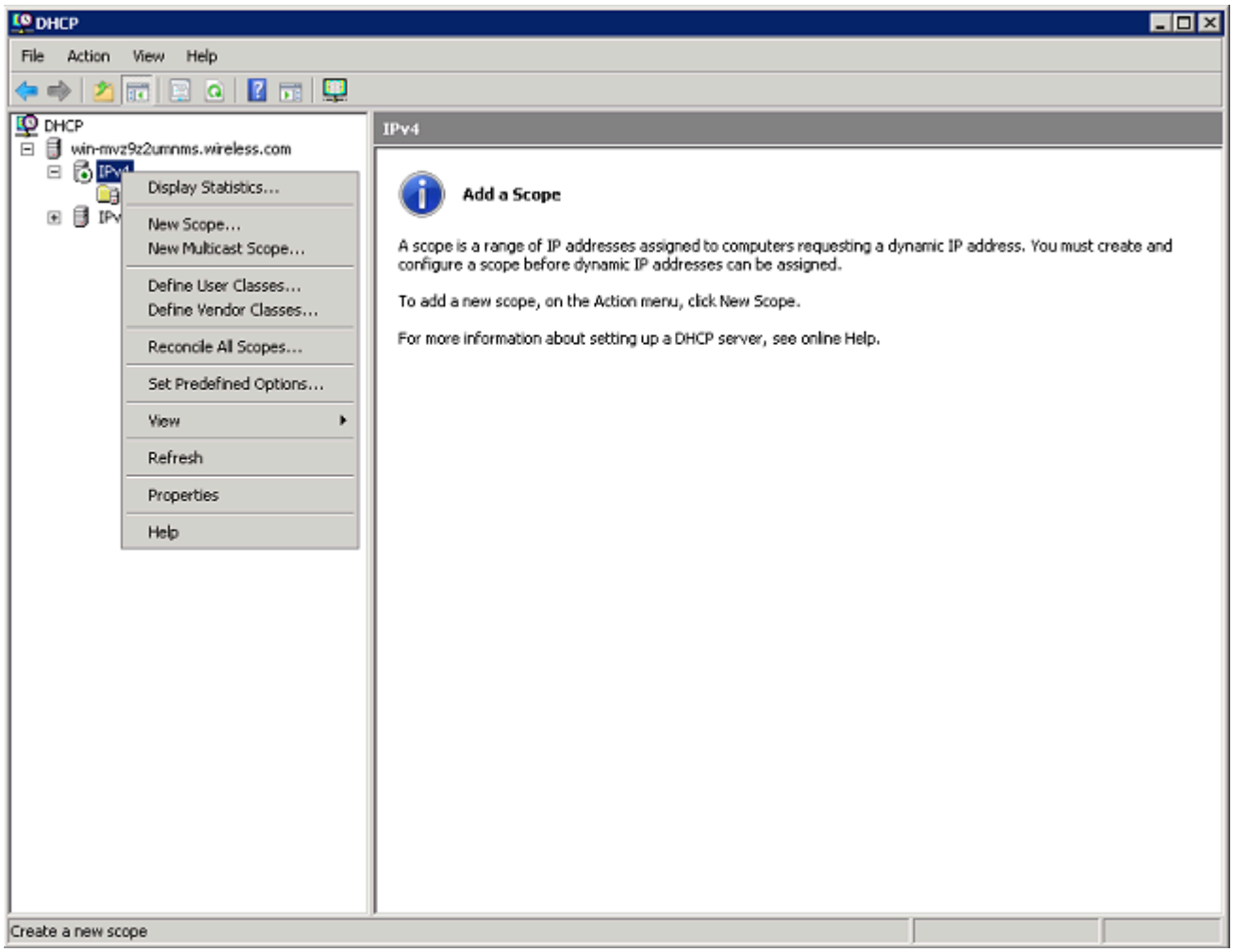


Il server DHCP è installato.

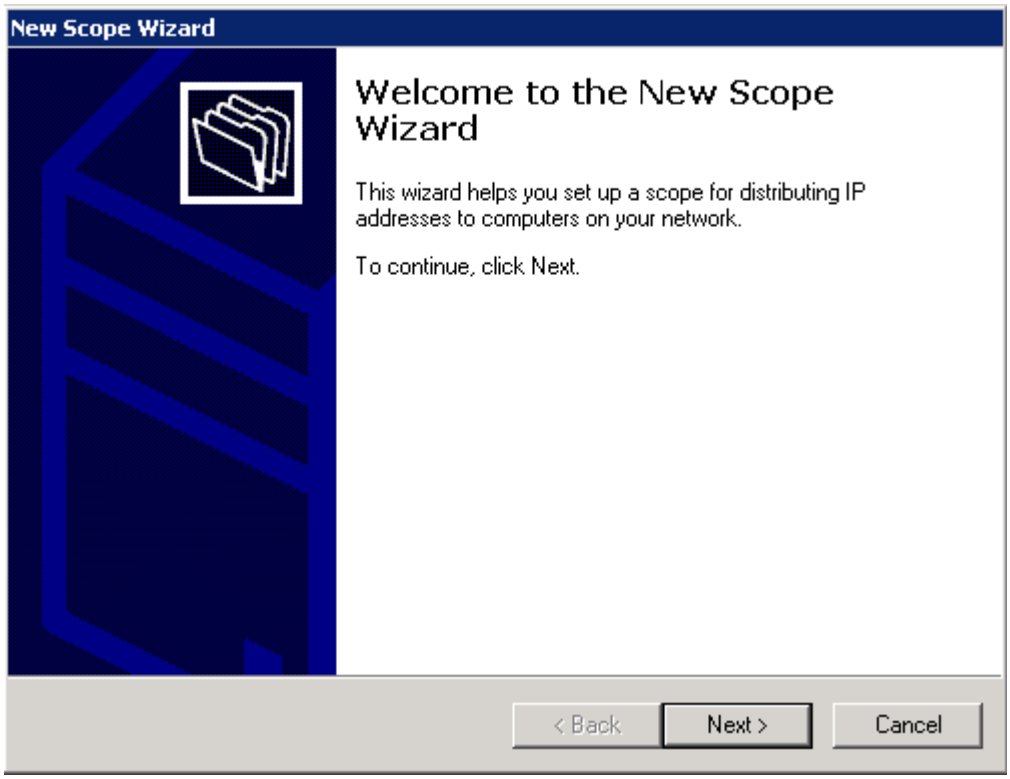
15. Fare clic su Start > Strumenti di amministrazione > DHCP per configurare il servizio DHCP.



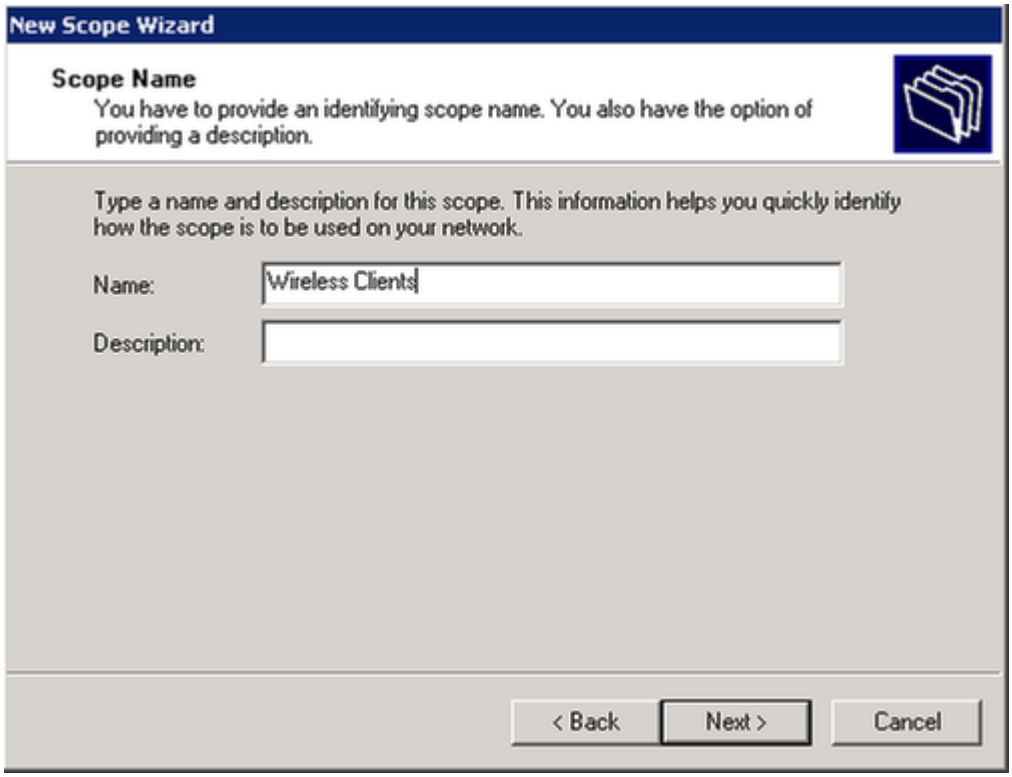
16. Espandere il server DHCP (come mostrato nell'immagine precedente dell'esempio), fare clic con il pulsante destro del mouse su IPv4, quindi selezionare New Scope (Nuovo ambito) per creare un ambito DHCP.



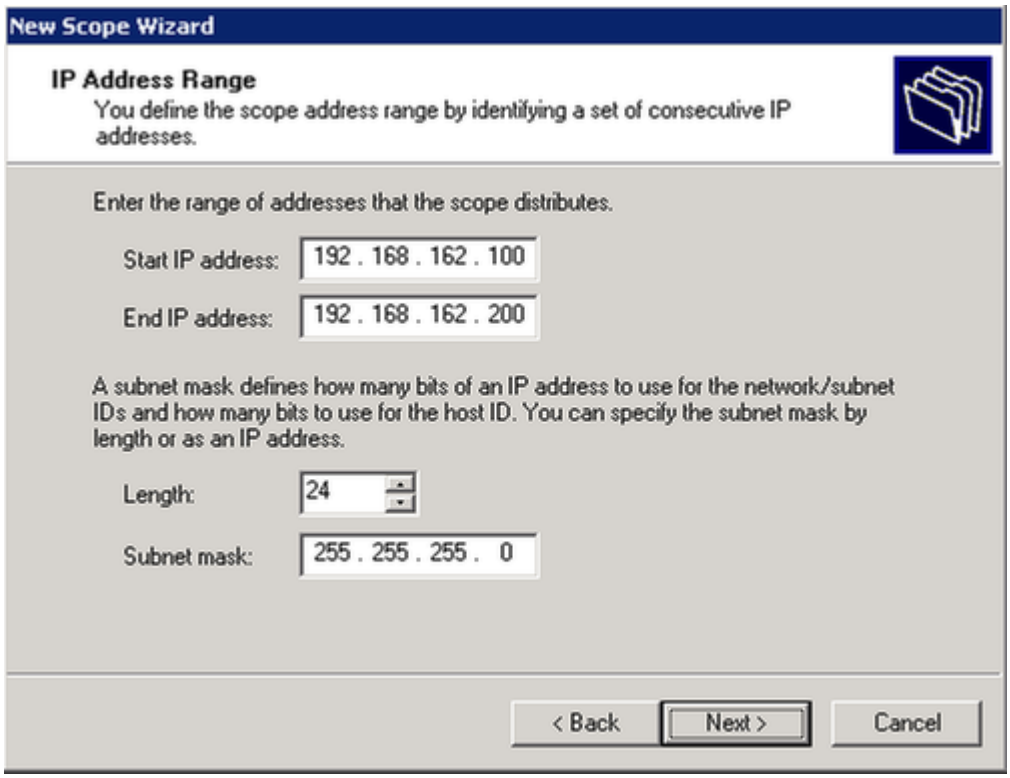
17. Fare clic su Avanti per configurare il nuovo ambito tramite la Creazione guidata ambito.



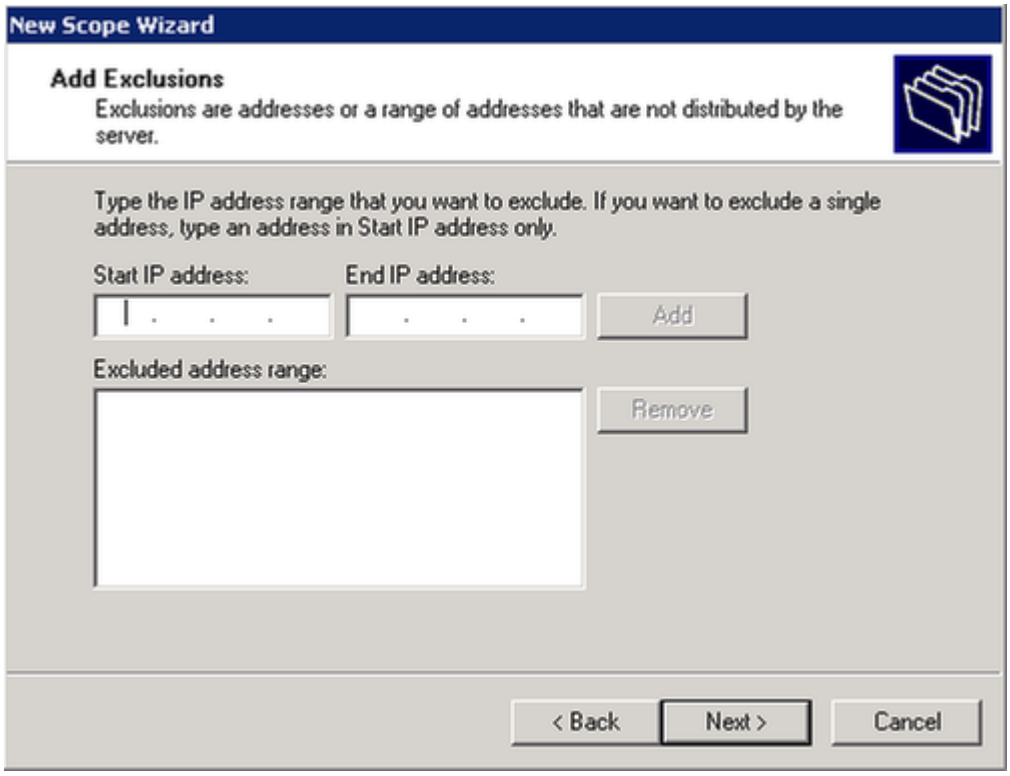
18. Specificare un nome per il nuovo ambito (in questo esempio Client wireless) e fare clic su Avanti.



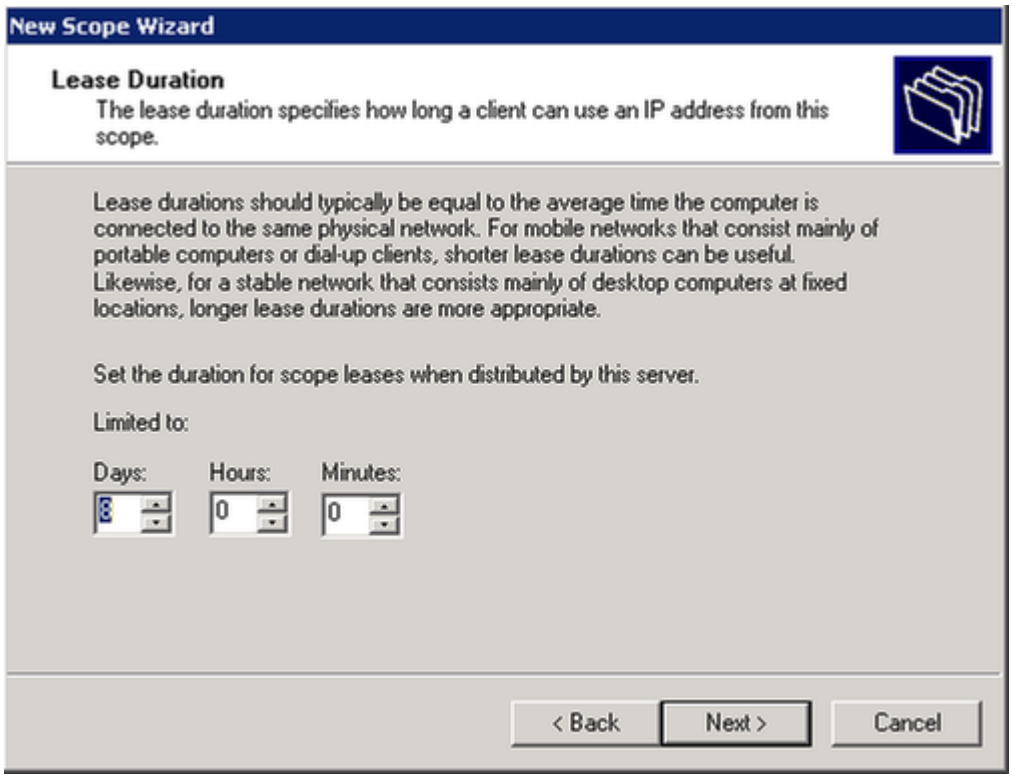
19. Immettere l'intervallo di indirizzi IP disponibili che possono essere utilizzati per i lease DHCP. Fare clic su Next (Avanti) per continuare.



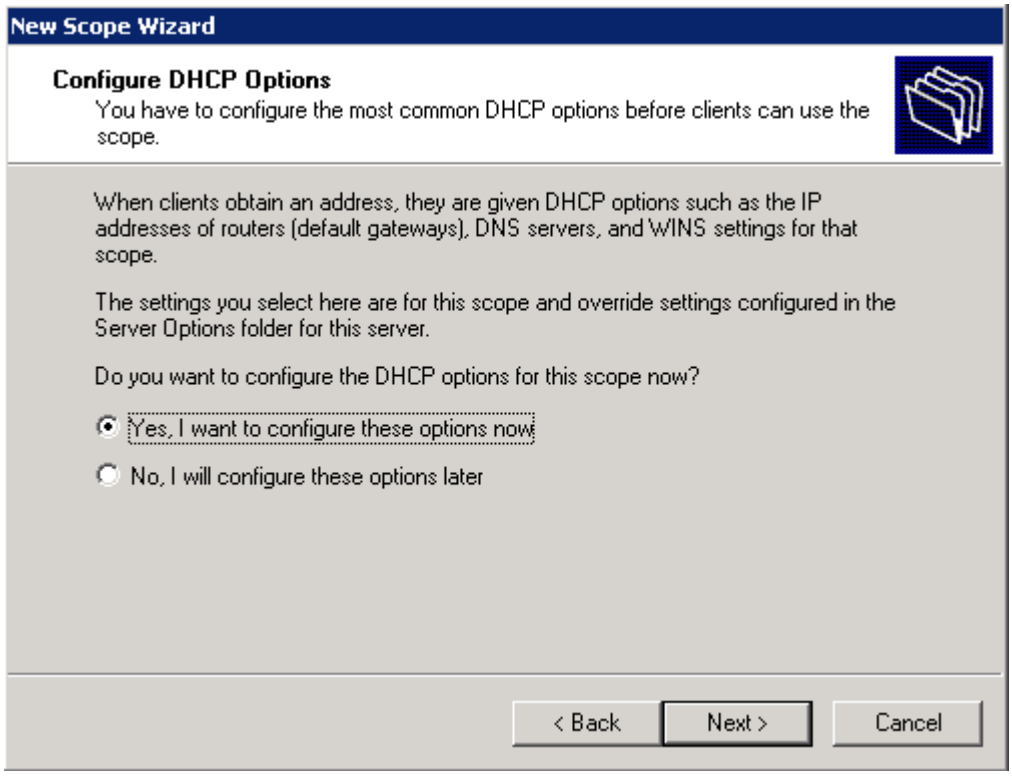
20. Creare un elenco facoltativo di indirizzi esclusi. Fare clic su Next (Avanti) per continuare.



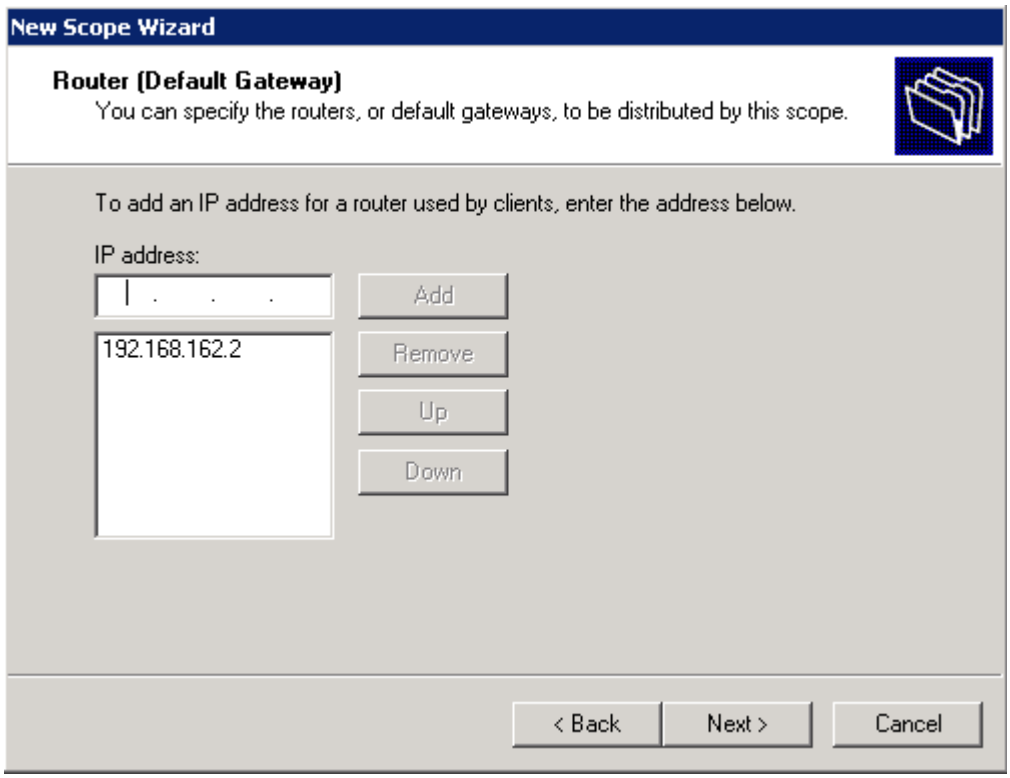
21. Configurare la durata del lease e fare clic su Avanti.



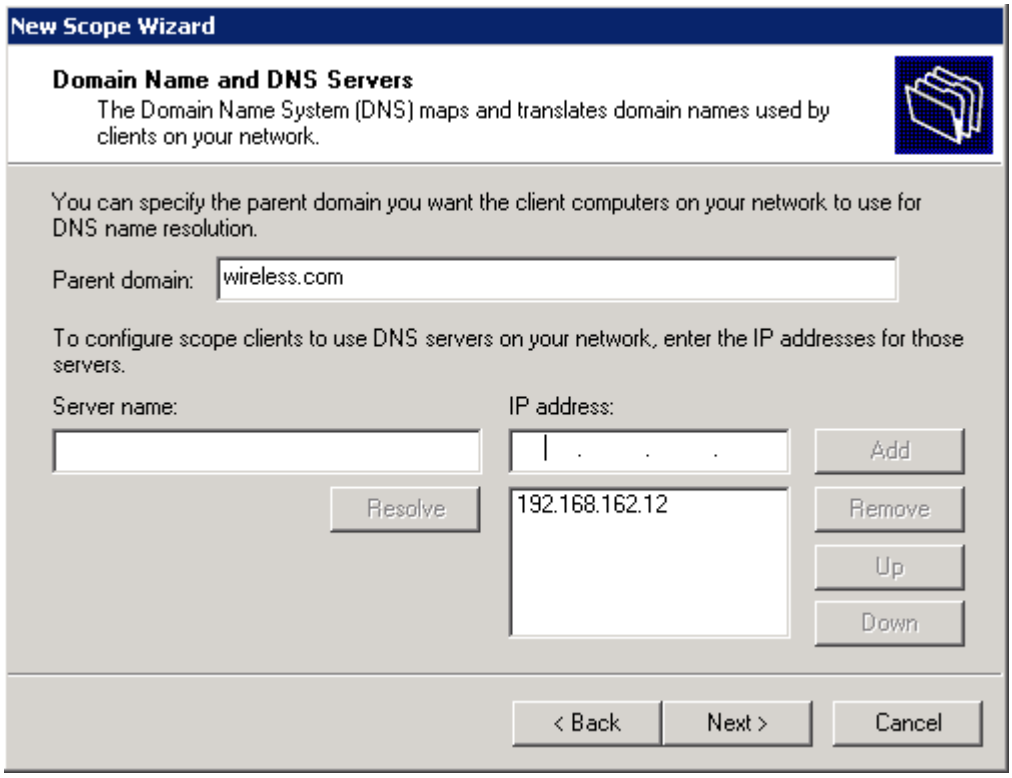
22. Fare clic su Sì, configurare le opzioni ora, quindi fare clic su Avanti.



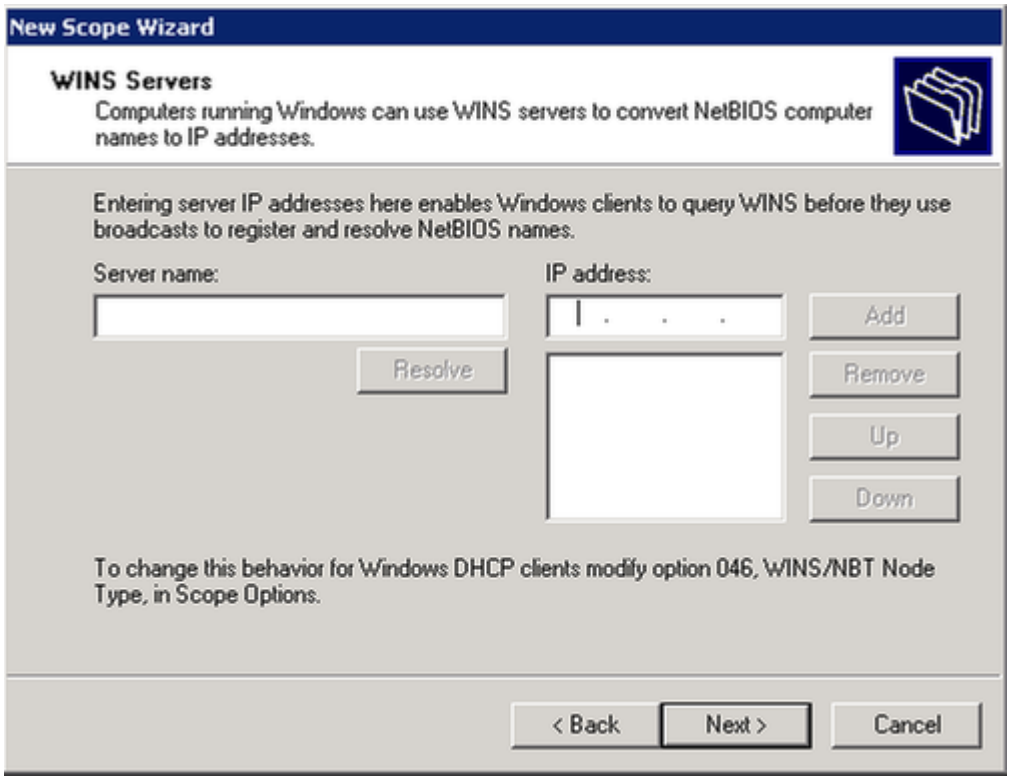
23. Immettere l'indirizzo IP del gateway predefinito per questo ambito, fare clic su Add > Next (Aggiungi > Avanti).



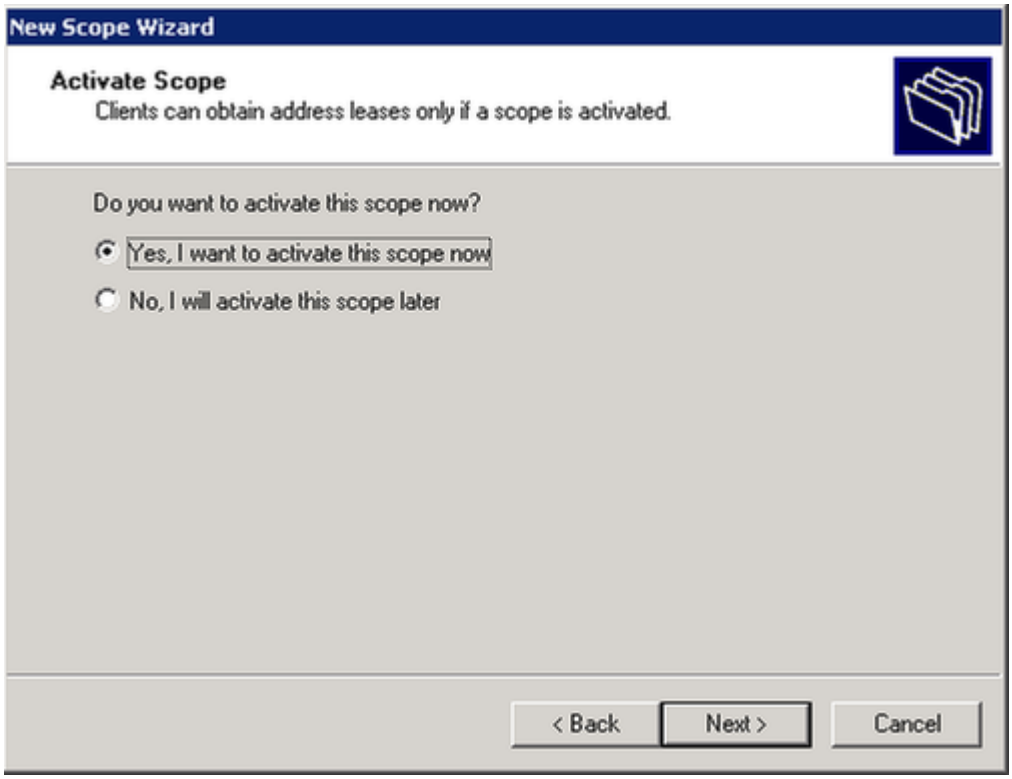
24. Configurare il nome di dominio DNS e il server DNS che verranno utilizzati dai client. Fare clic su Next (Avanti) per continuare.



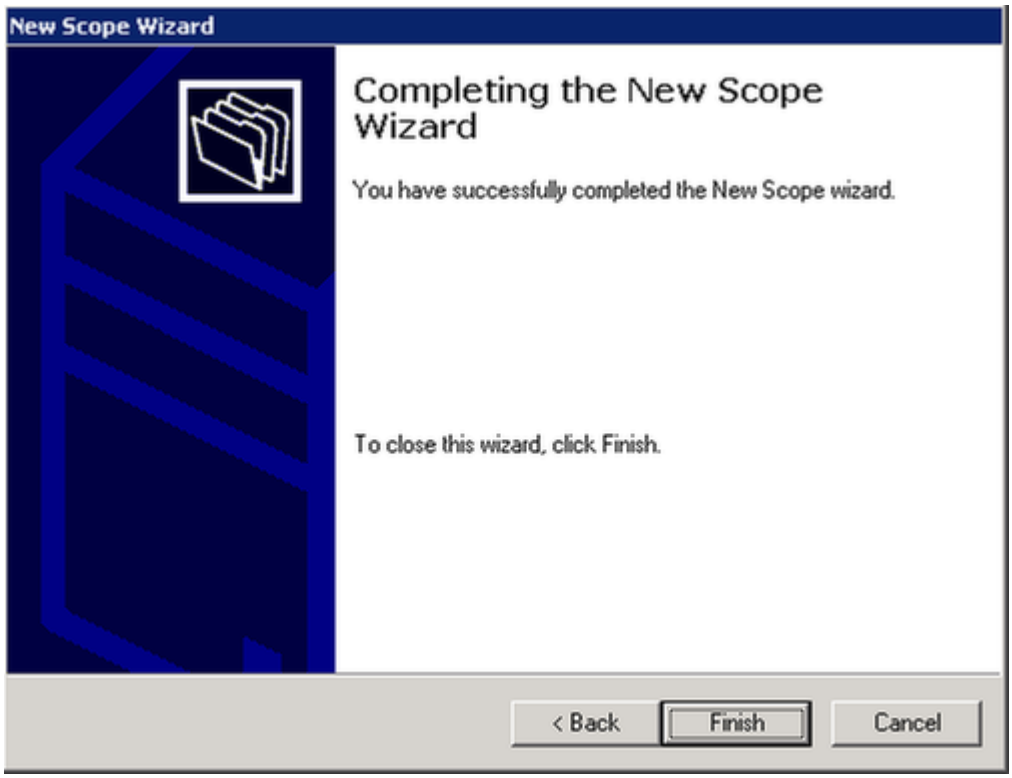
25. Immettere le informazioni WINS per questo ambito se la rete supporta WINS. Fare clic su Next (Avanti) per continuare.



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



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

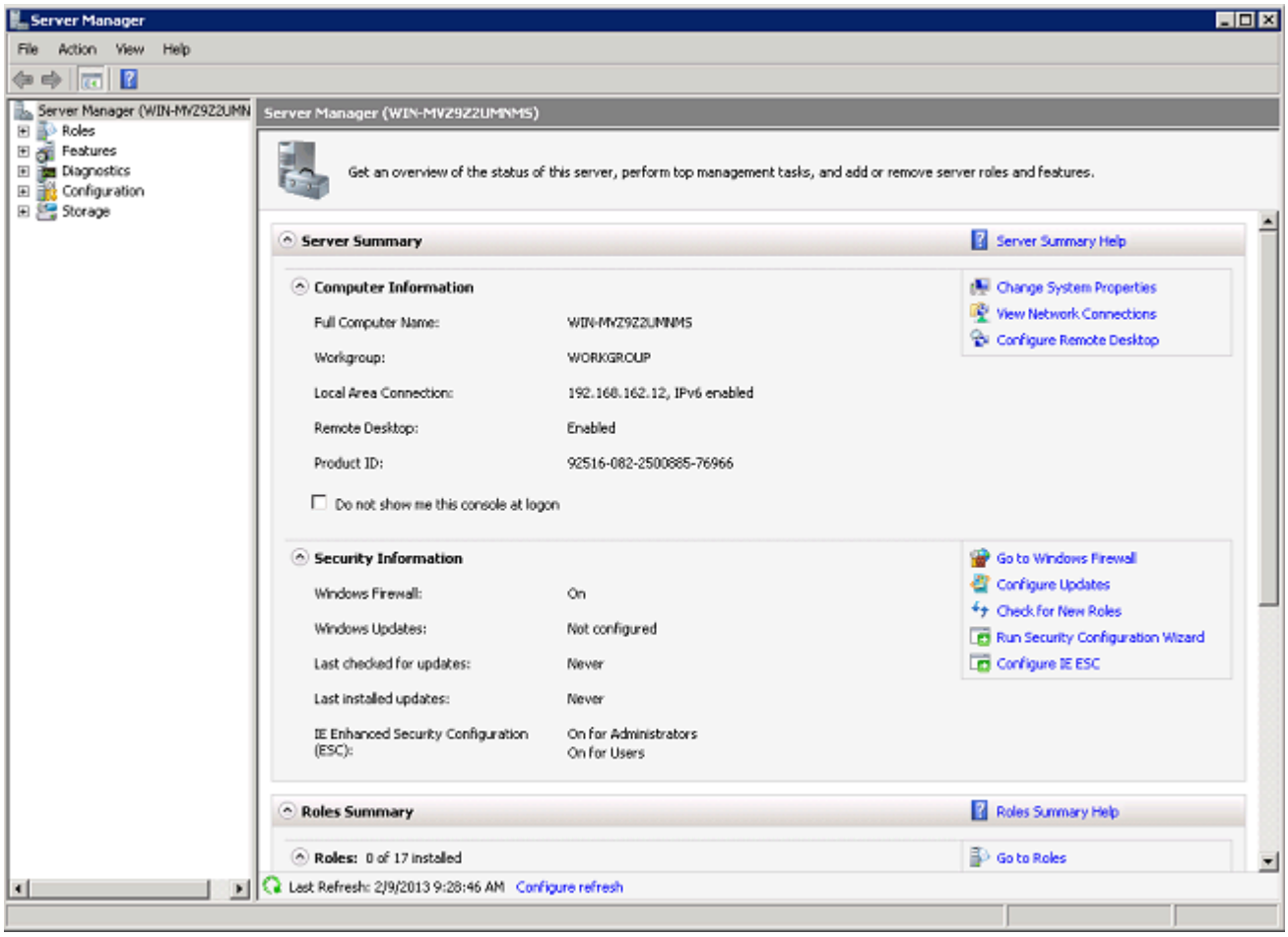


Installazione e configurazione di Microsoft Windows 2008 Server come server CA

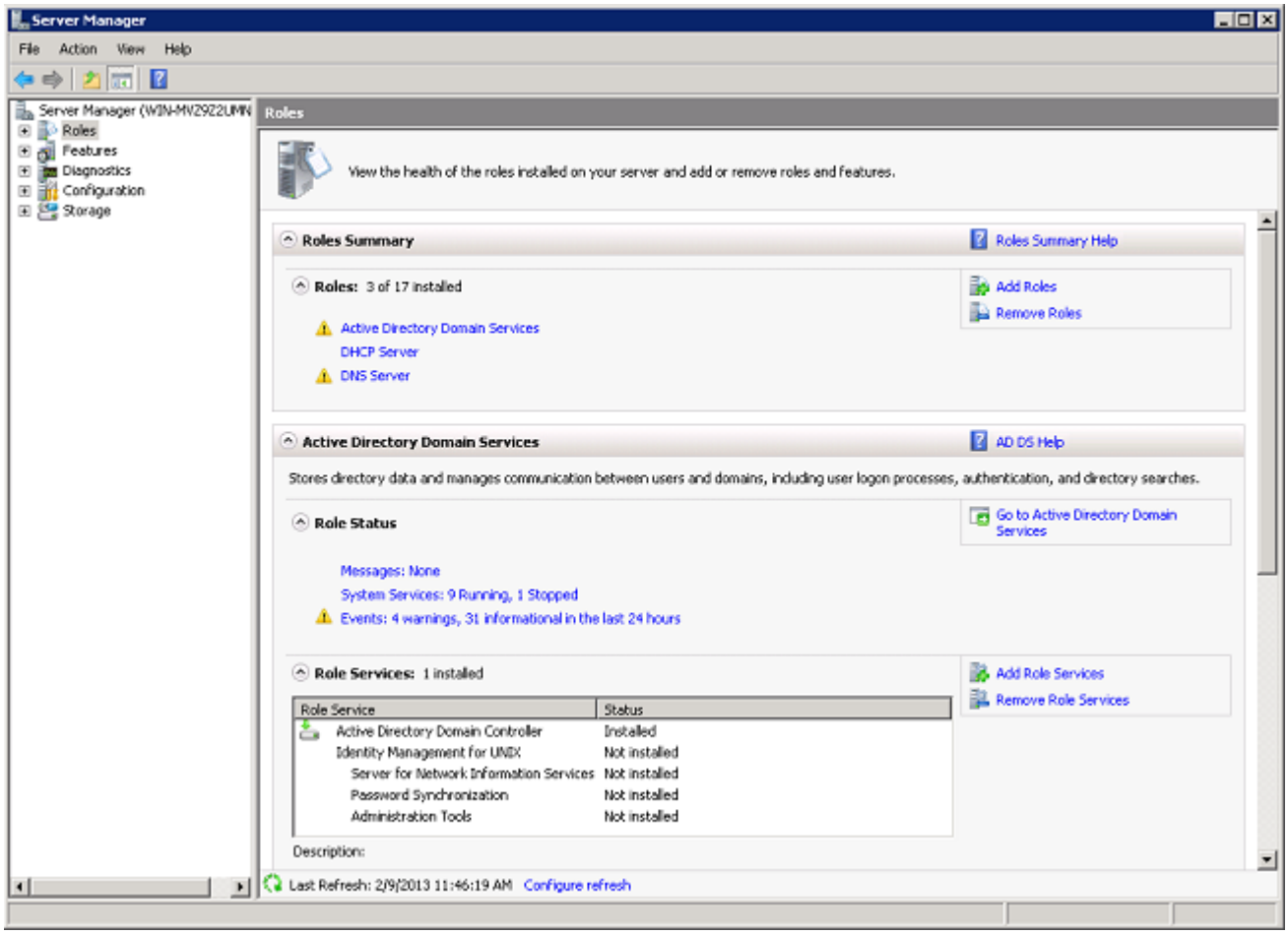
PEAP con EAP-MS-CHAP v2 convalida il server RADIUS in base al certificato presente sul server. Il certificato server deve inoltre essere rilasciato da una CA pubblica considerata attendibile dal computer client, ovvero il certificato CA pubblico esiste già nella cartella Autorità di certificazione radice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

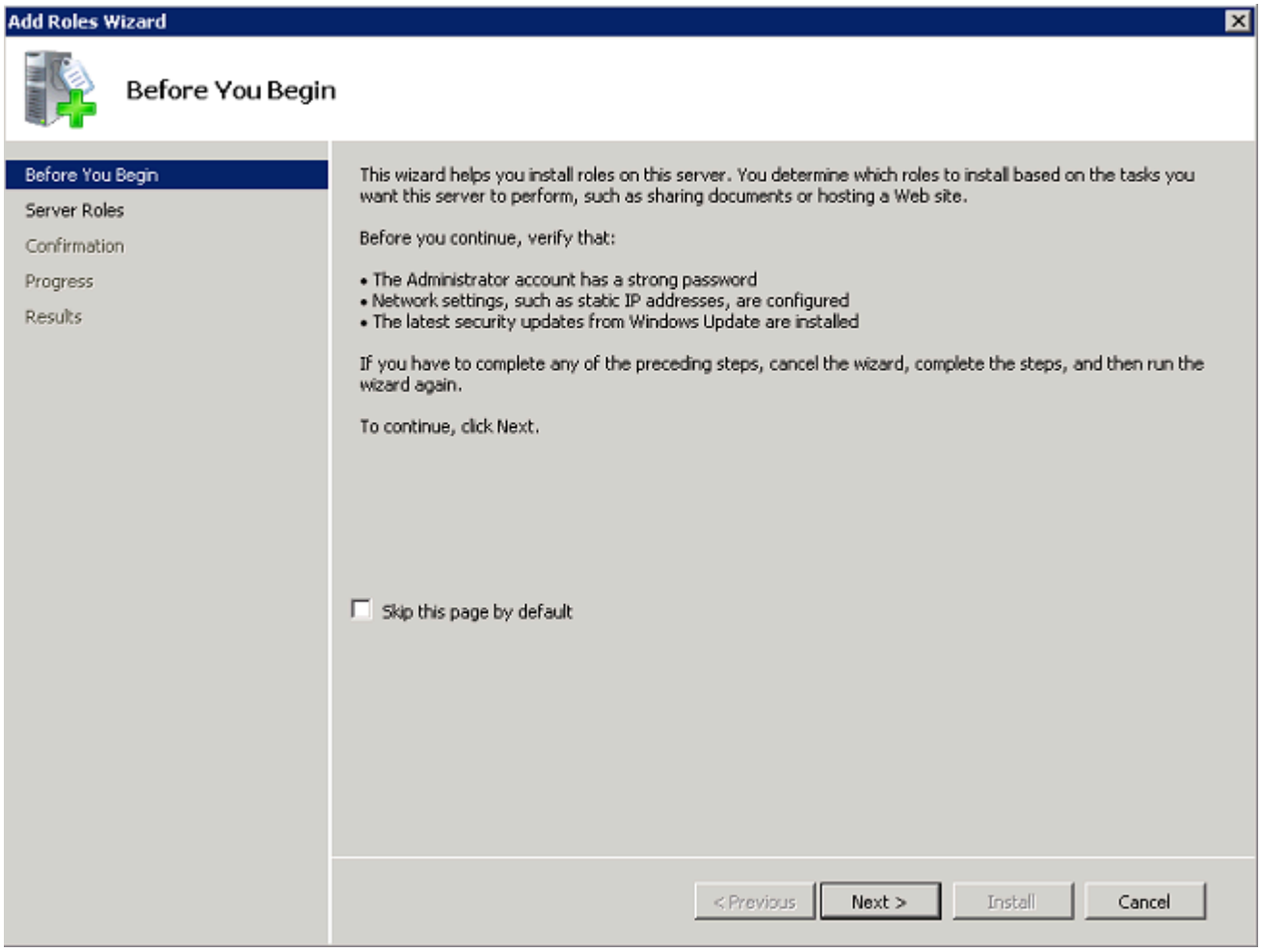
1. Fare clic su Start> Server Manager.



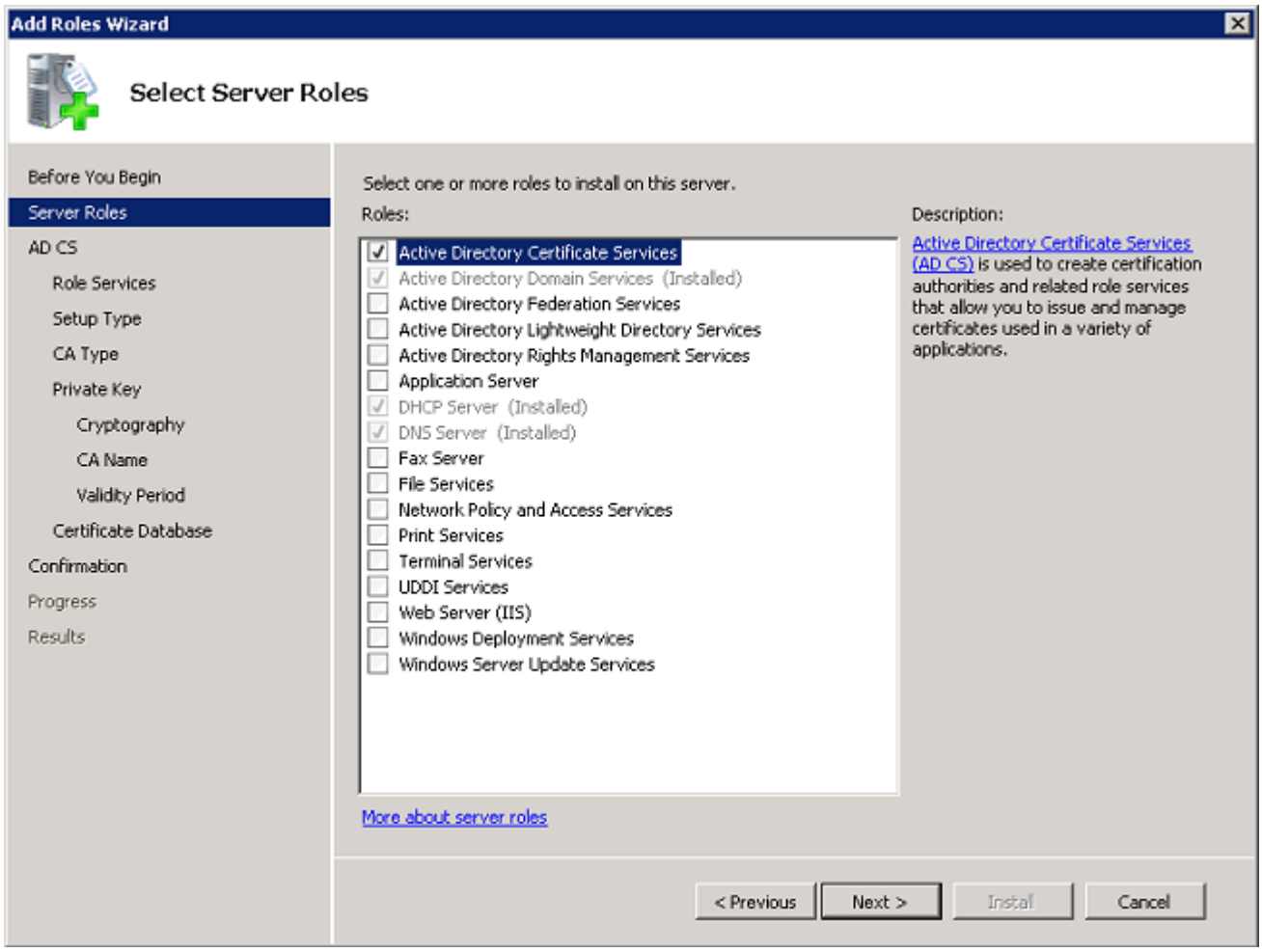
2. Fare clic su Ruoli> Aggiungi ruoli.



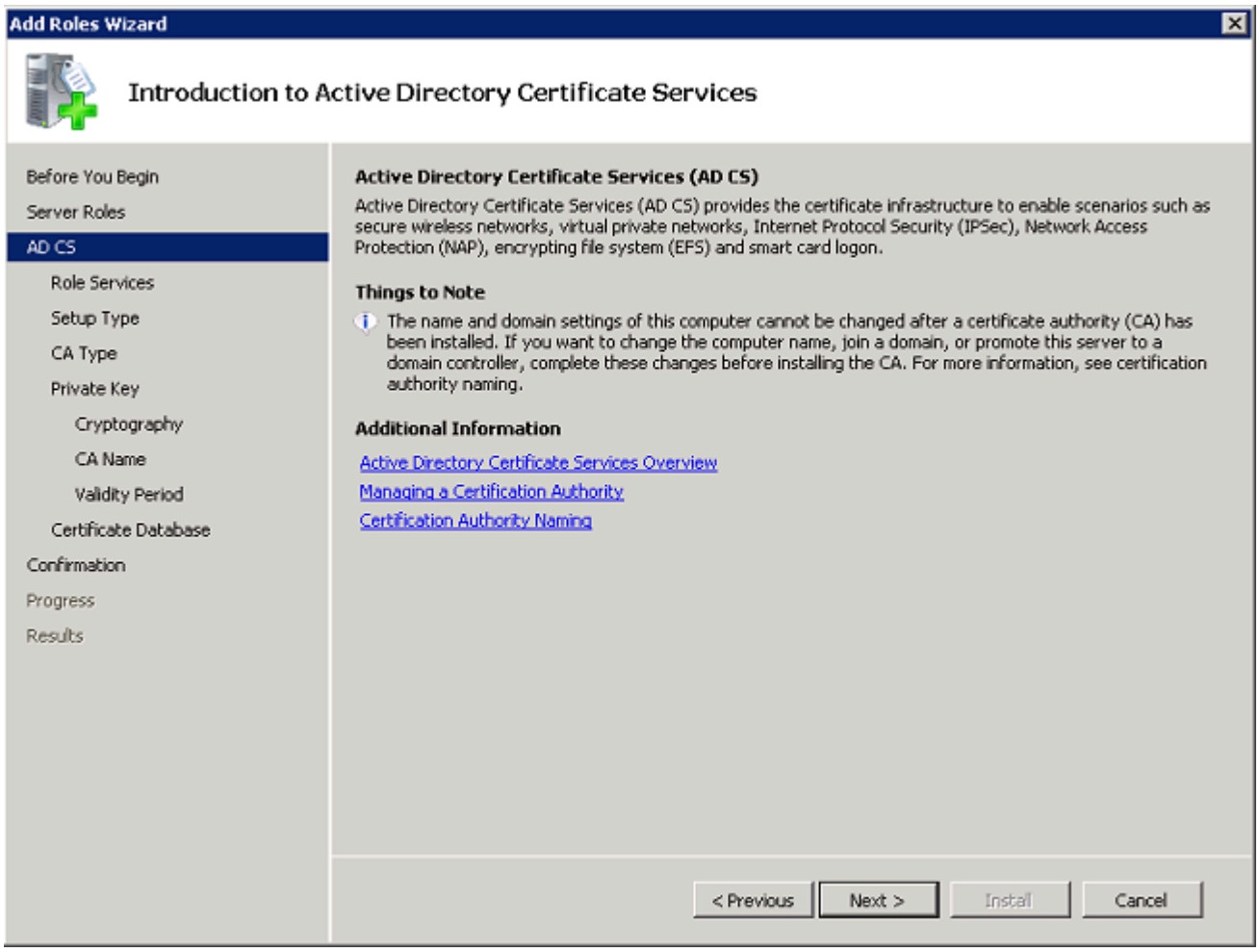
3. Fare clic su Next (Avanti).



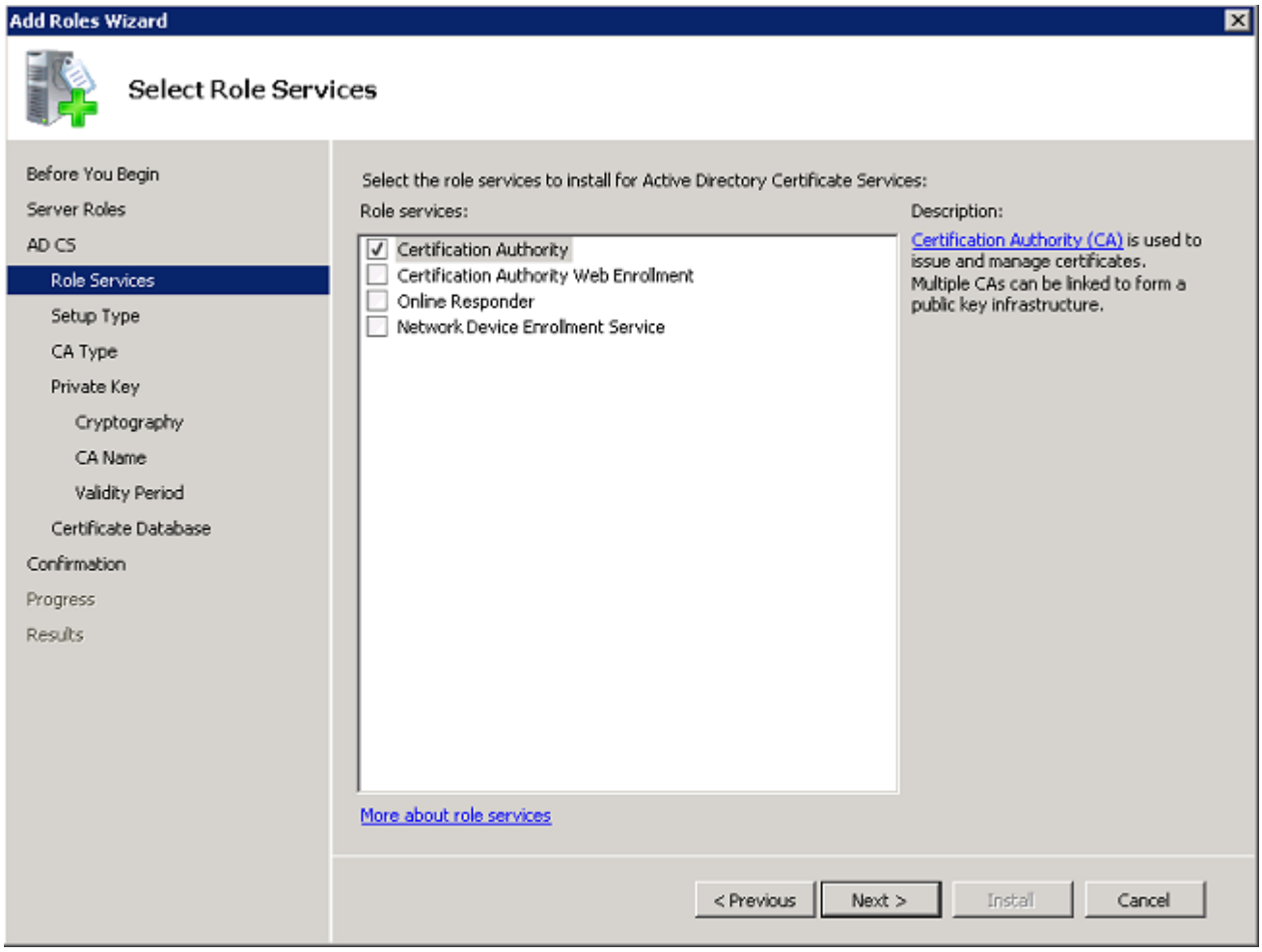
4. Selezionare il servizio Servizi certificati Active Directory e fare clic su Avanti.



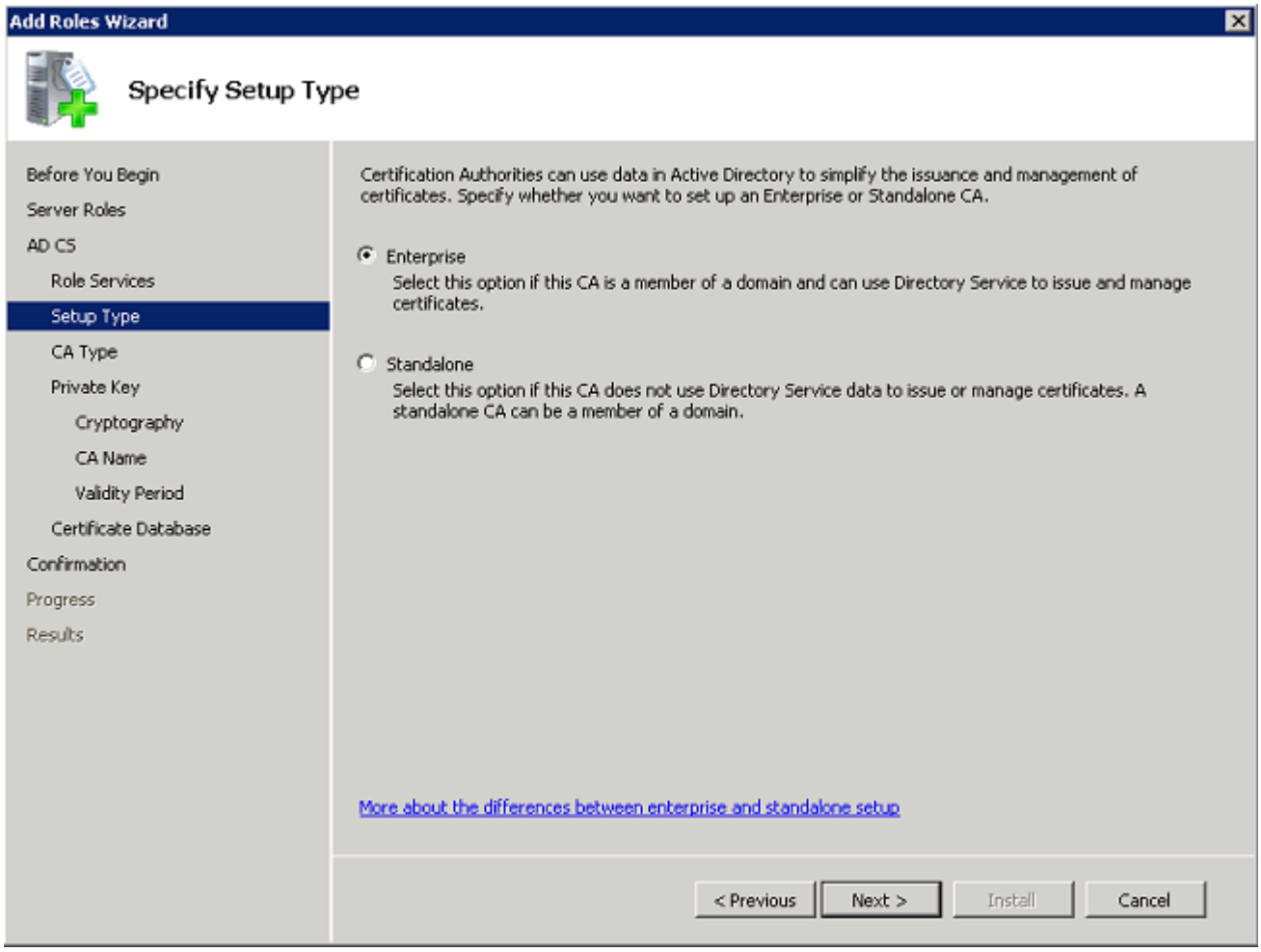
5. Rivedere l'Introduzione a Servizi certificati Active Directory e fare clic su Avanti.



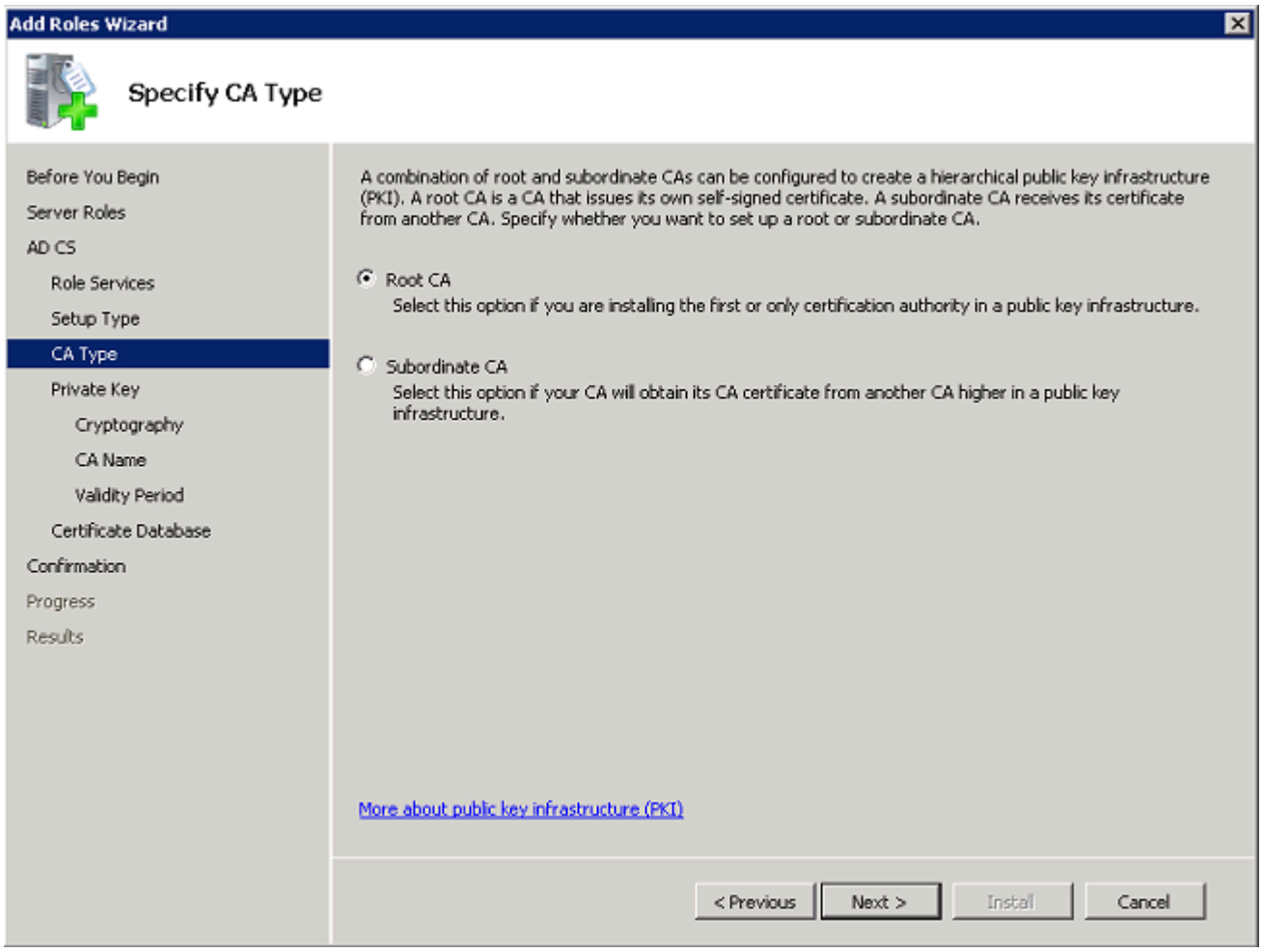
6. Selezionare l'Autorità di certificazione e fare clic su Avanti.



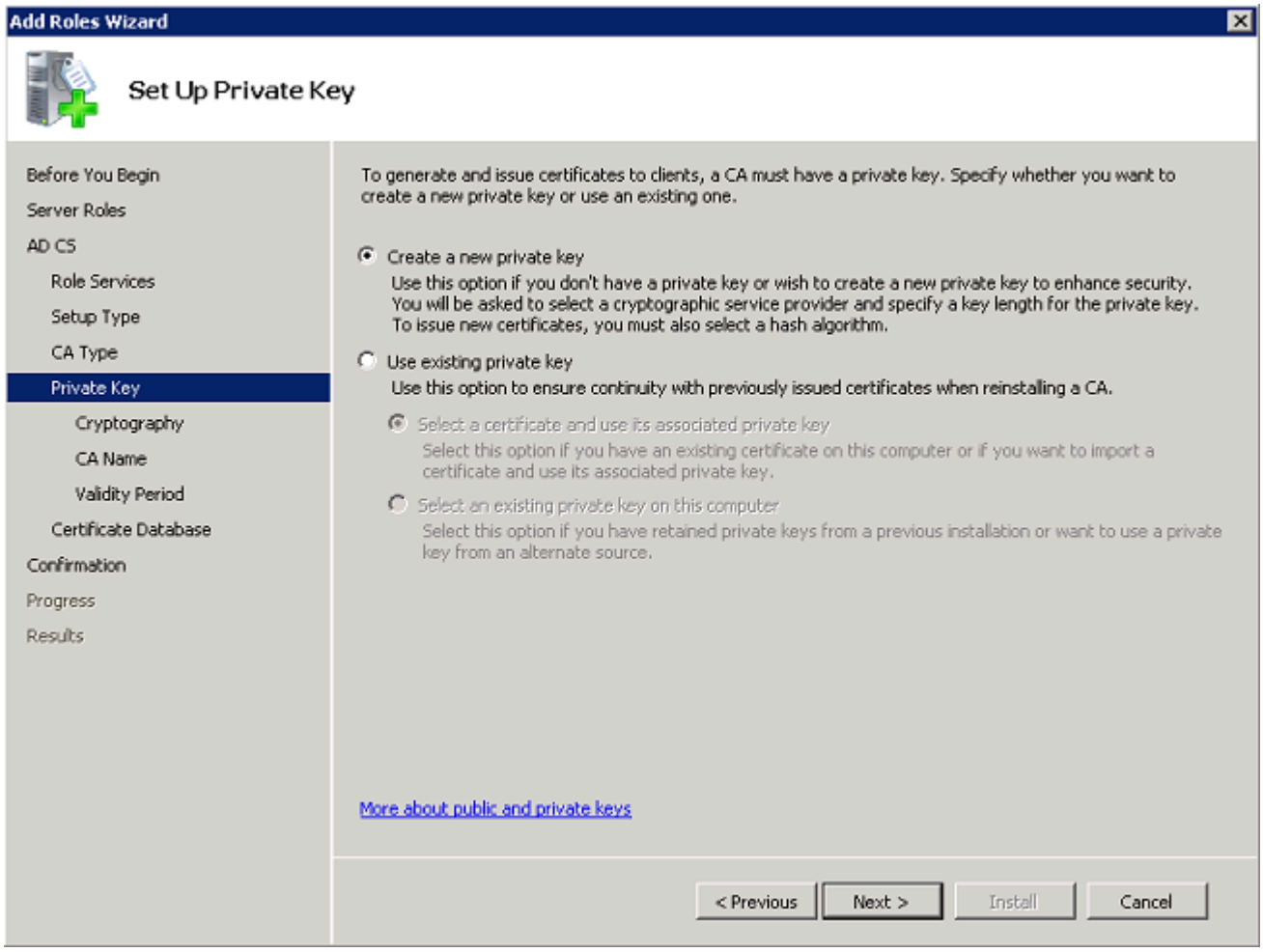
7. Selezionare Enterprise, quindi fare clic su Next (Avanti).



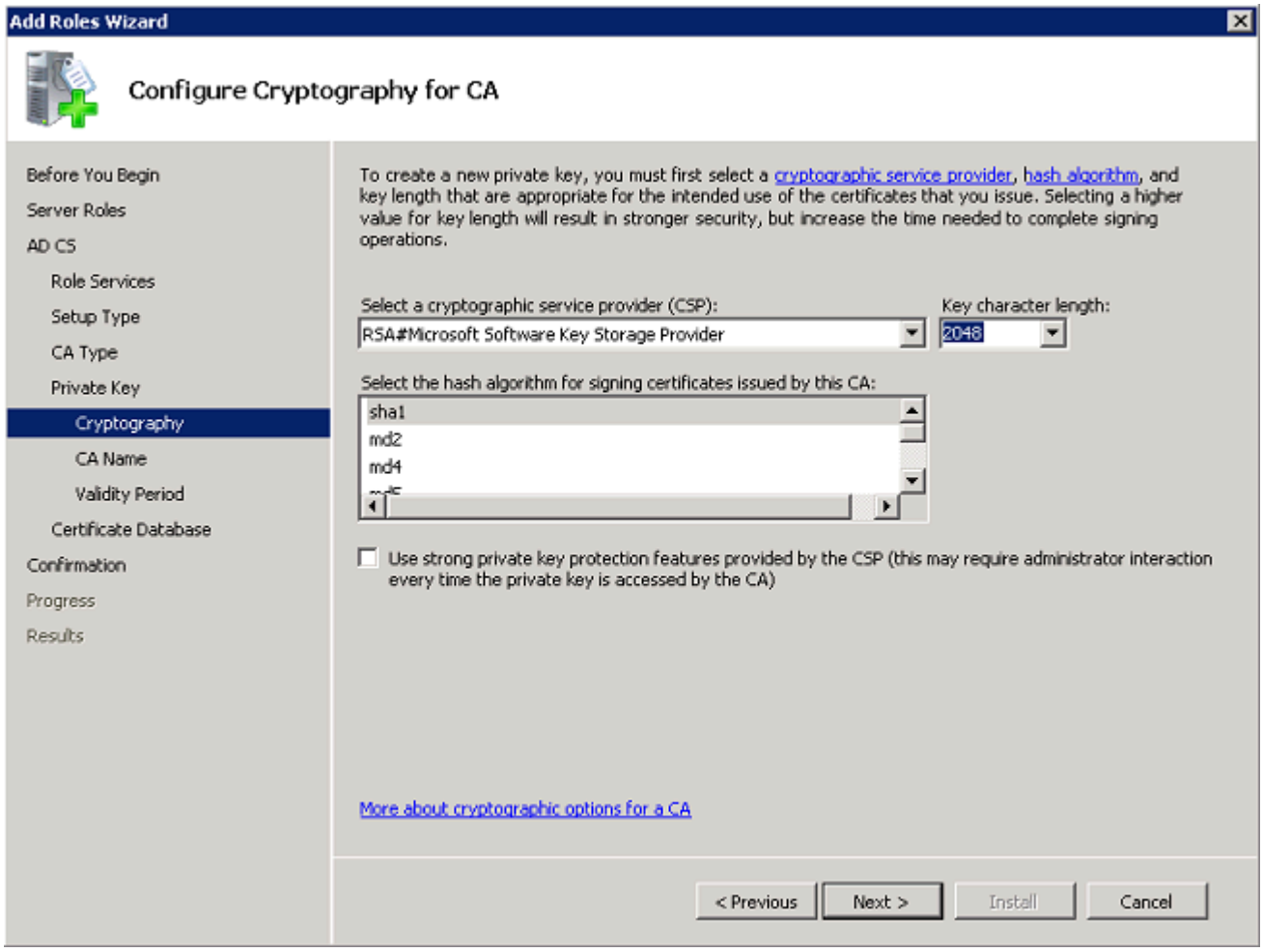
8. Selezionare CA radice, quindi fare clic su Avanti.



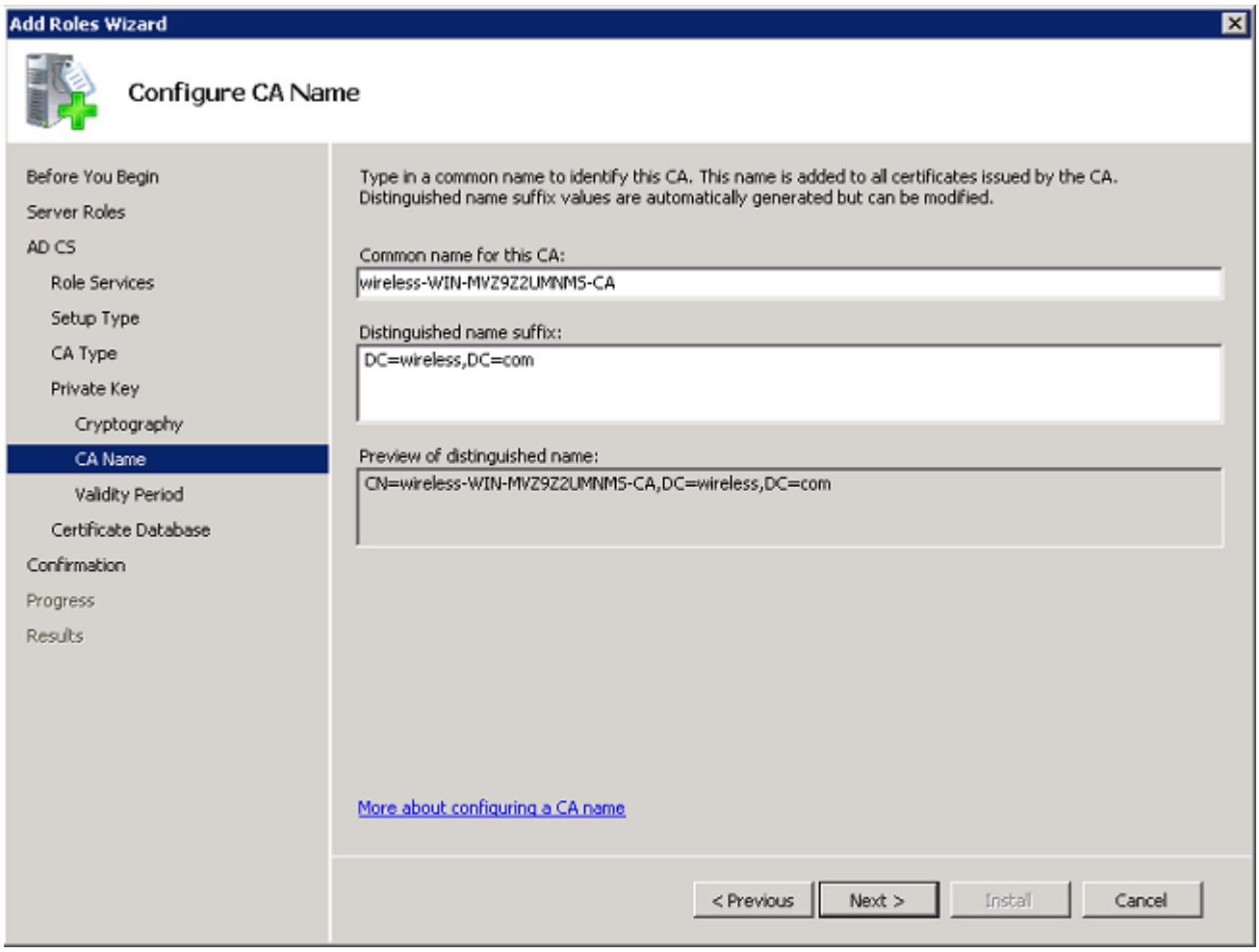
9. Selezionare Crea nuova chiave privata e fare clic su Avanti.



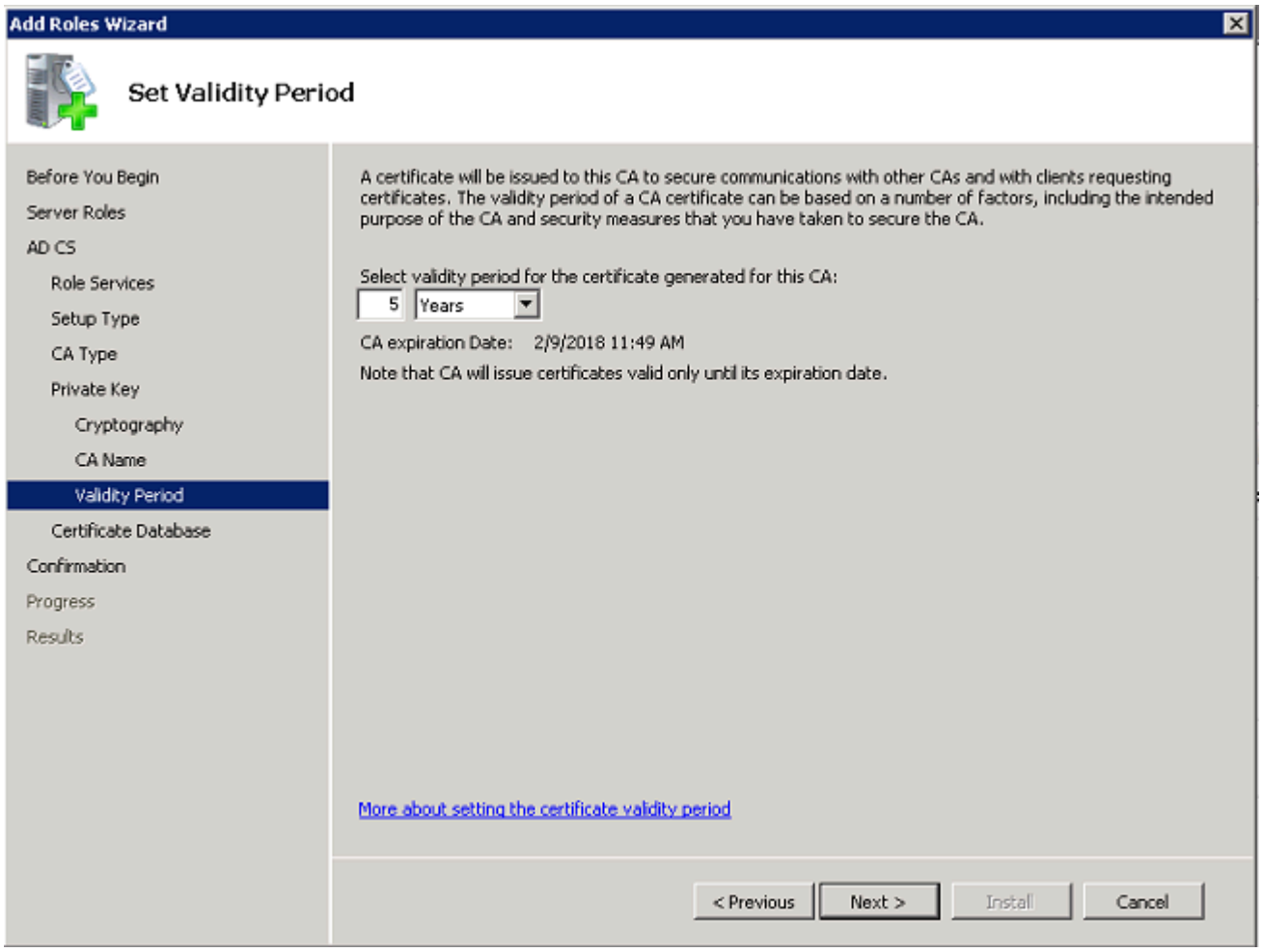
10. Fare clic su Next (Avanti) in Configure Cryptography for CA.



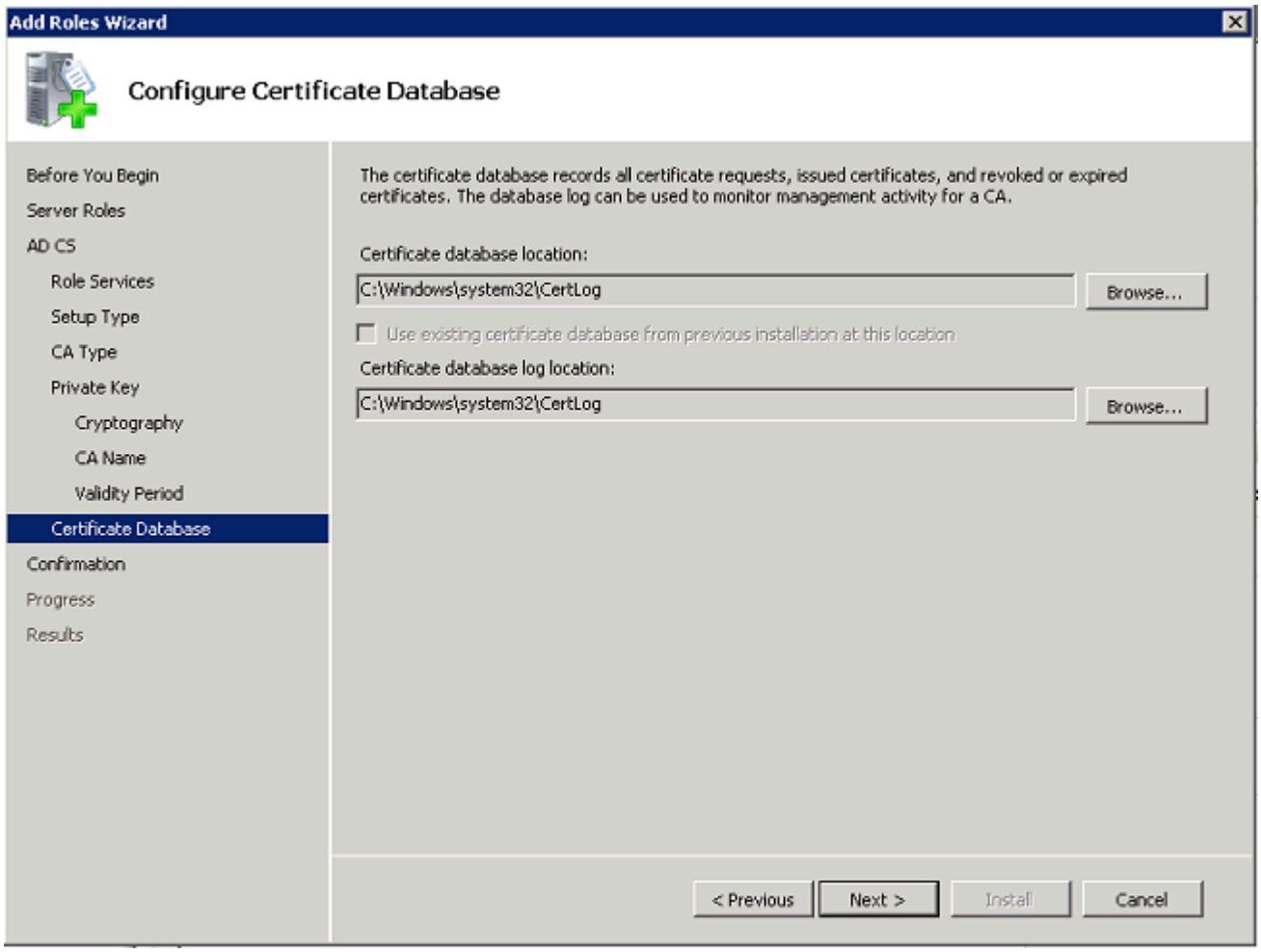
11. Fare clic su Avanti per accettare il nome comune predefinito per questa CA.



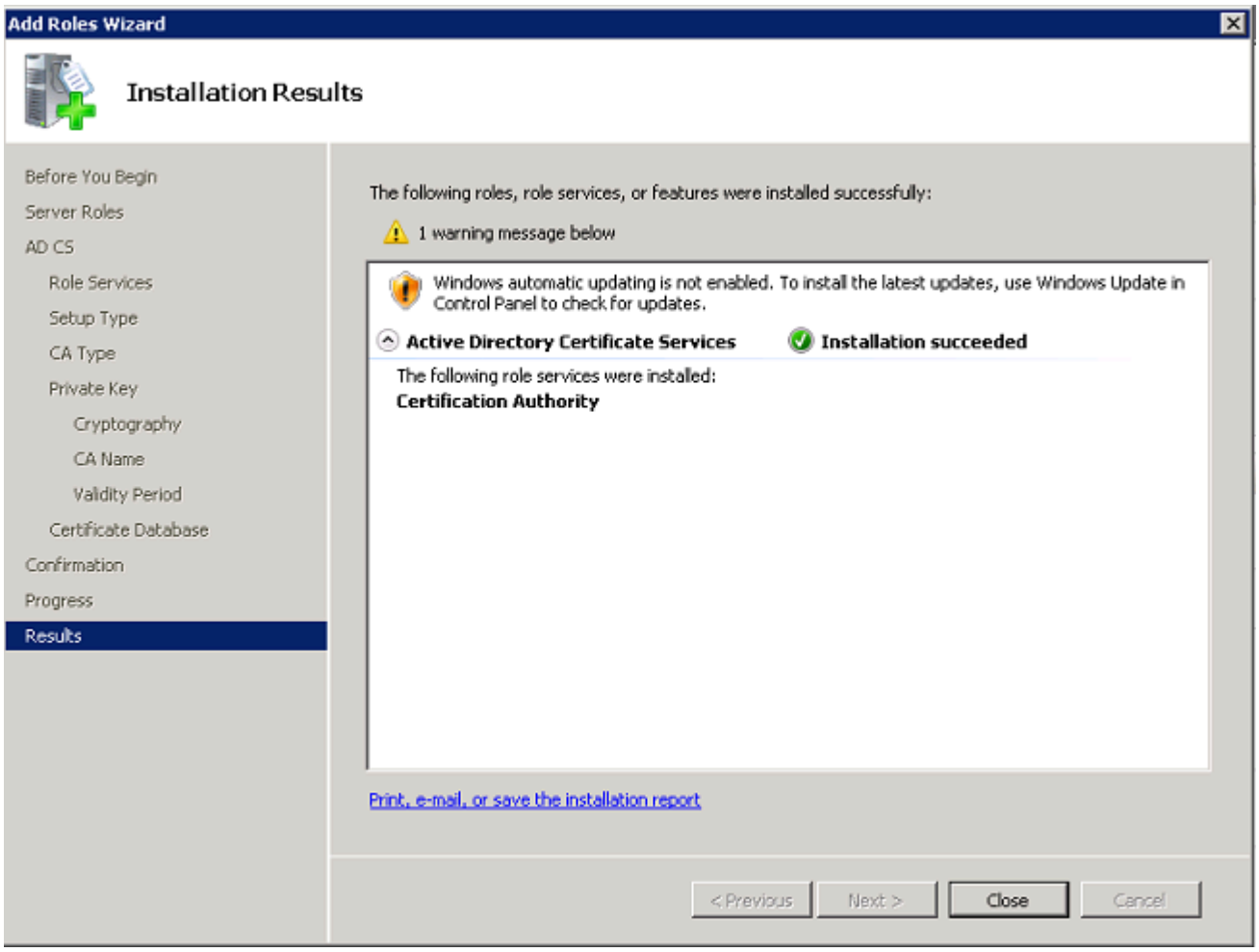
12. Selezionare la durata di validità del certificato CA e fare clic su Avanti.



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



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

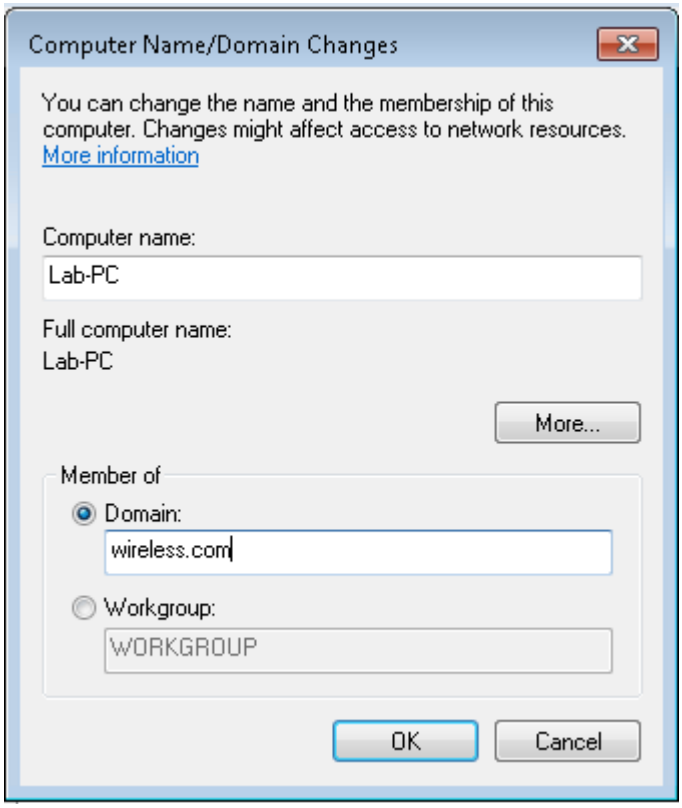


15. Al termine dell'installazione, fare clic su Chiudi.

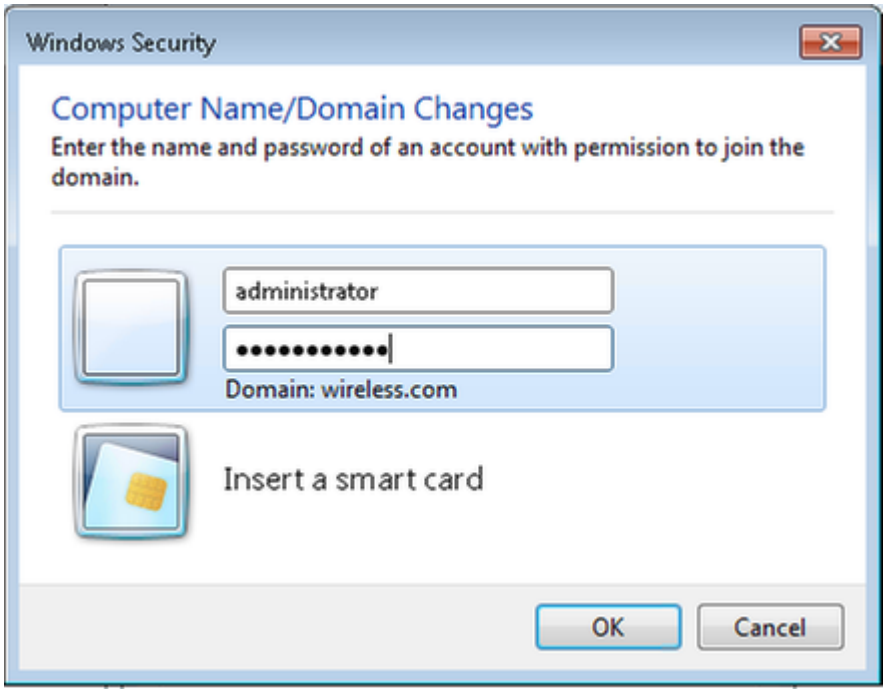
Connetti client al dominio

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.

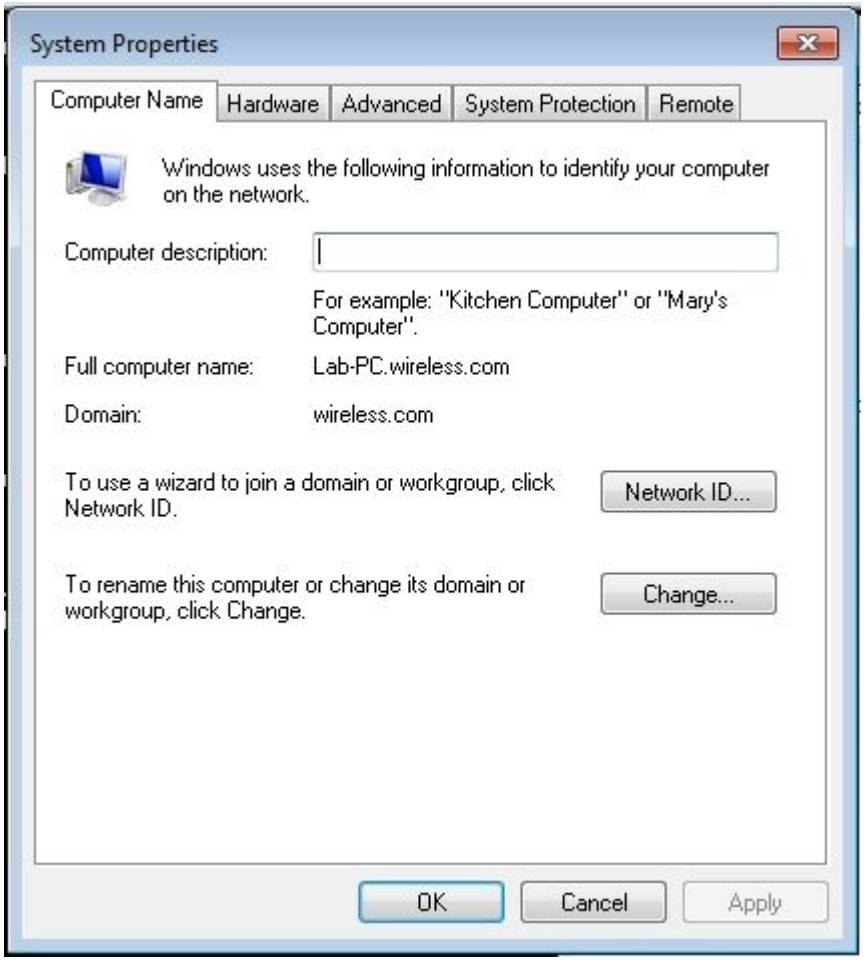


8. Immettere il nome utente administrator e la password specifica del dominio a cui il client viene aggiunto. Si tratta dell'account amministratore in Active Directory sul server.

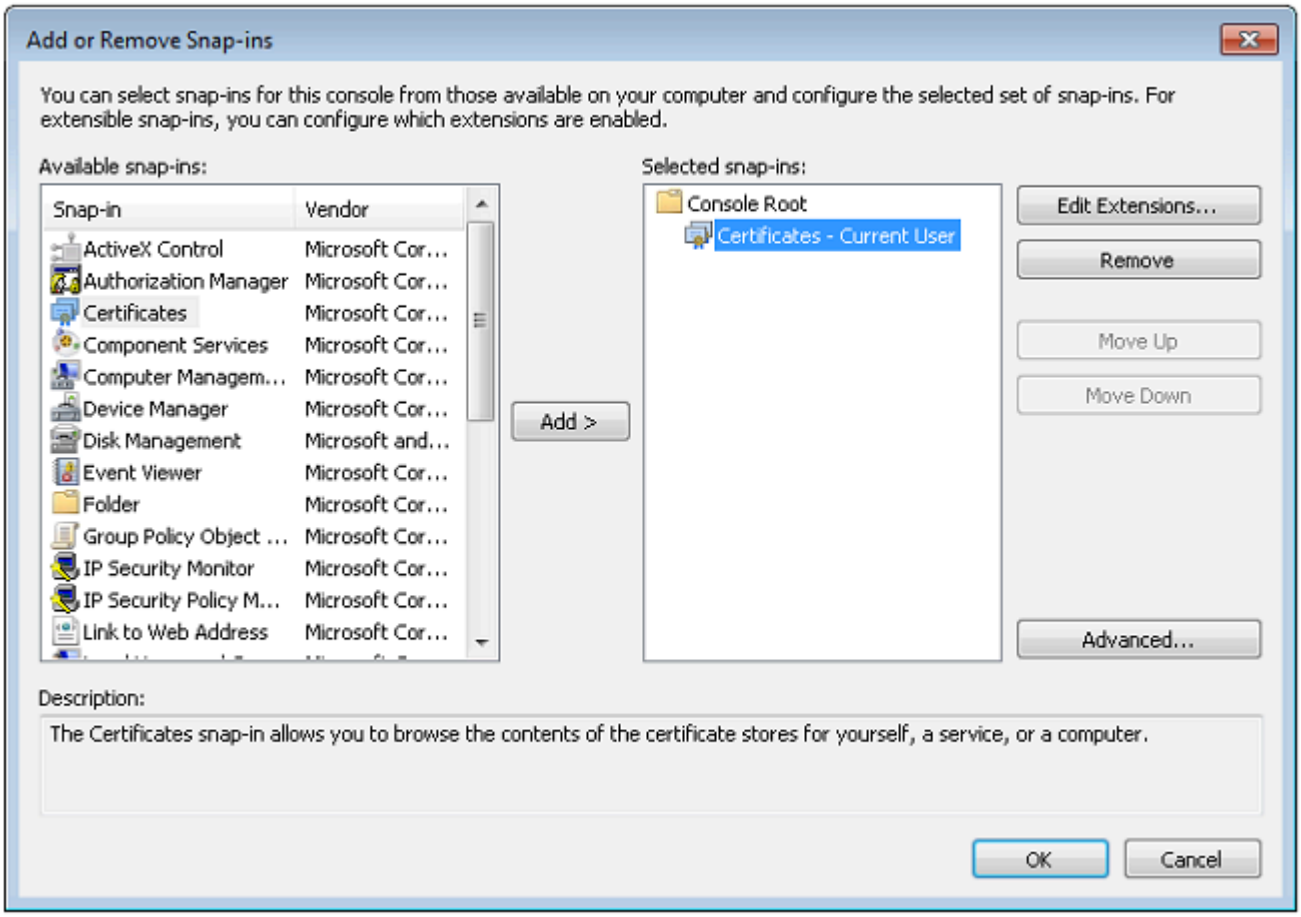


9. Fare clic su OK, quindi fare di nuovo clic su OK.

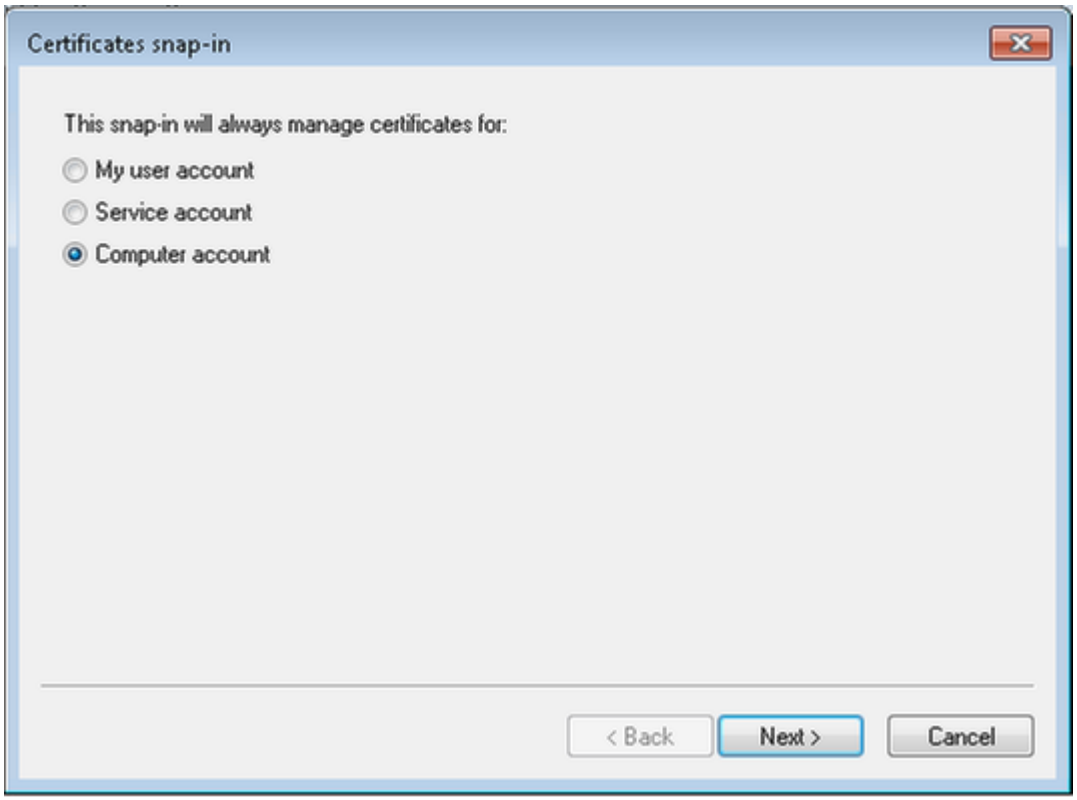
10. Fare clic su Close>Restart Now (Chiudi>Riavvia ora) per riavviare il computer.
11. Una volta riavviato il computer, accedere con: Username = Amministratore; Password = <password dominio>; Domain = wireless.
12. Fare clic su Start, fare clic con il pulsante destro del mouse su Computer, scegliere 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.



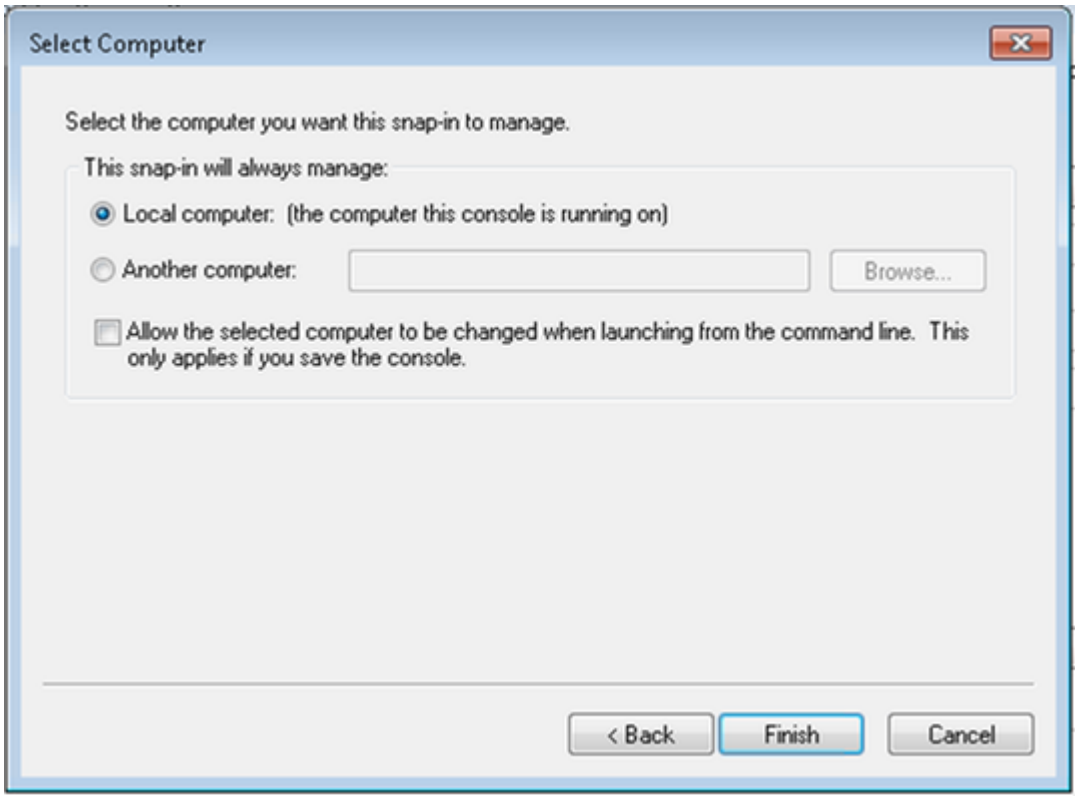
14. Fare clic su Start, immettere mmc e premere Invio.
15. Fare clic su File, quindi su Aggiungi/Rimuovi snap-in.
16. Scegliere Certificati, quindi fare clic su Aggiungi.



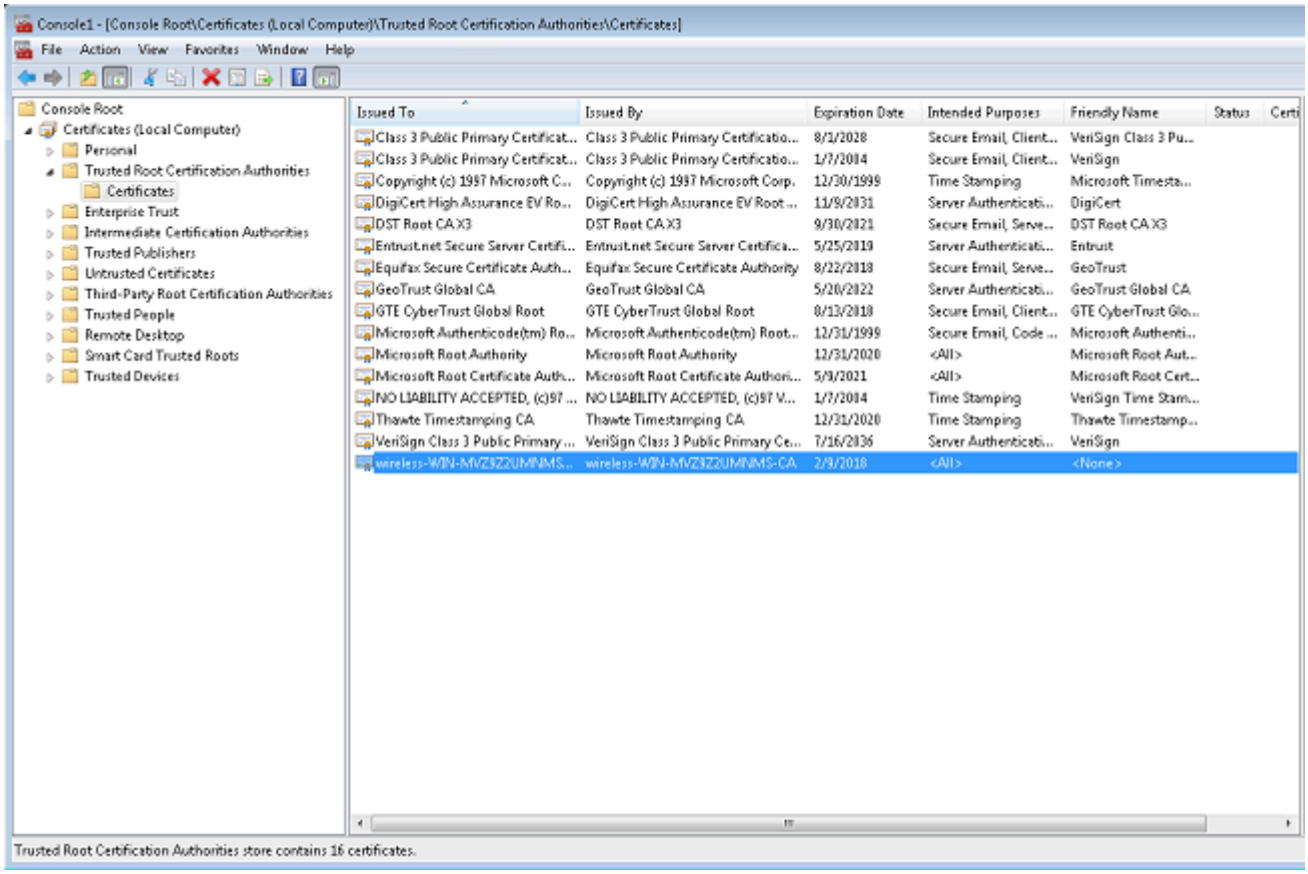
17. Fare clic su Account computer e quindi su Avanti.



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.

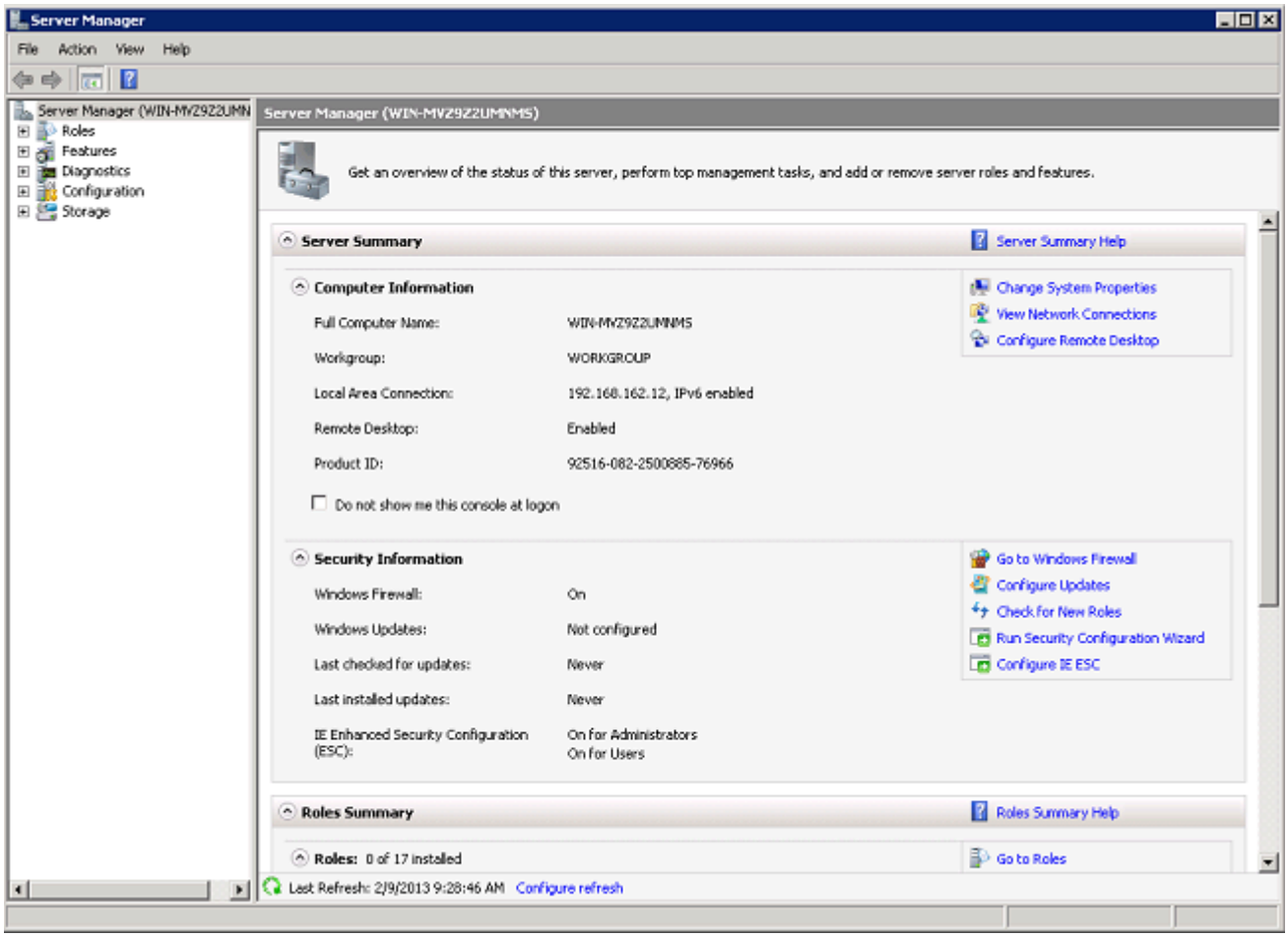


21. Ripetere questa procedura per aggiungere altri client al dominio.

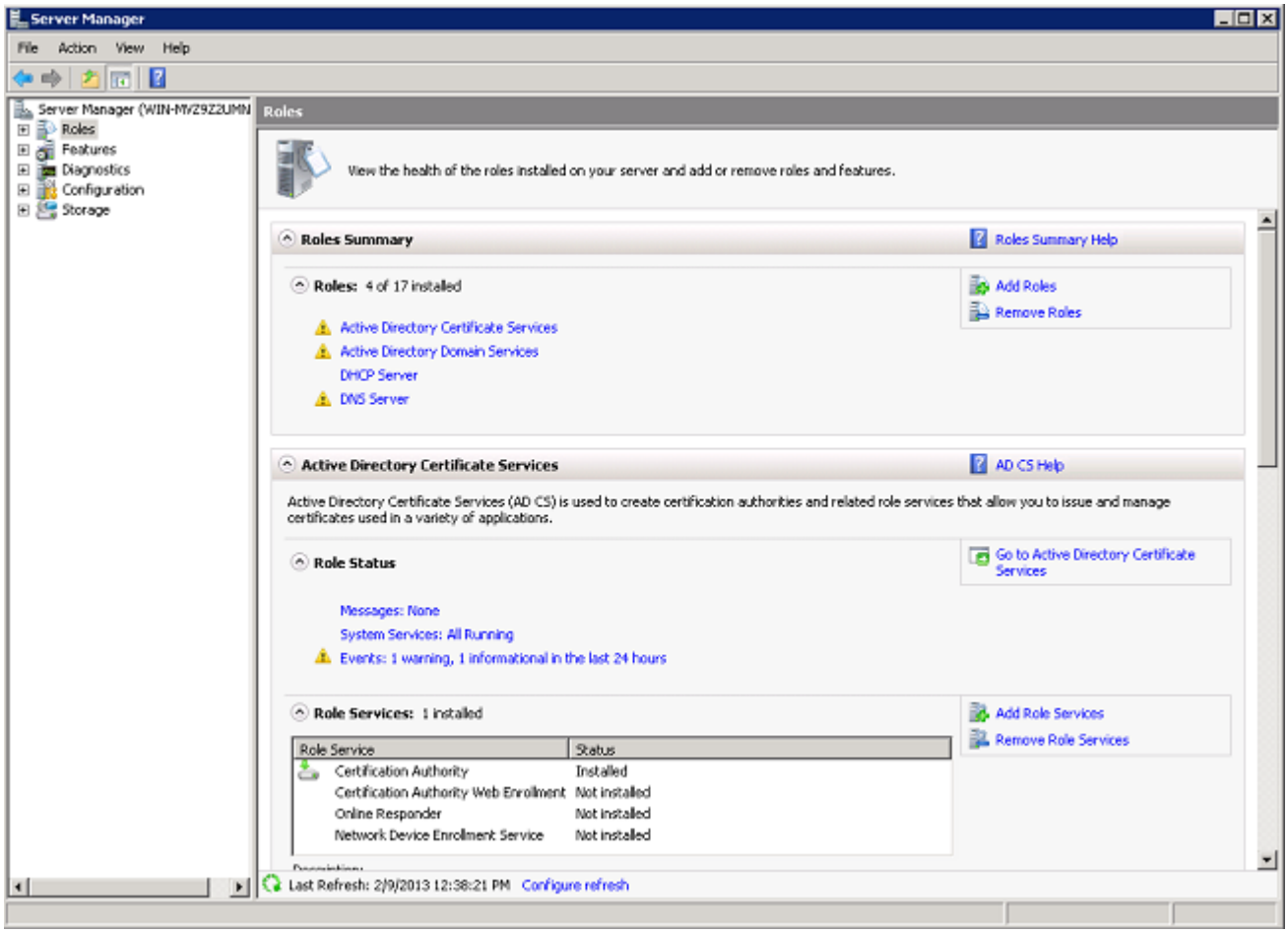
Installare Server dei criteri di rete in Microsoft Windows 2008 Server

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:

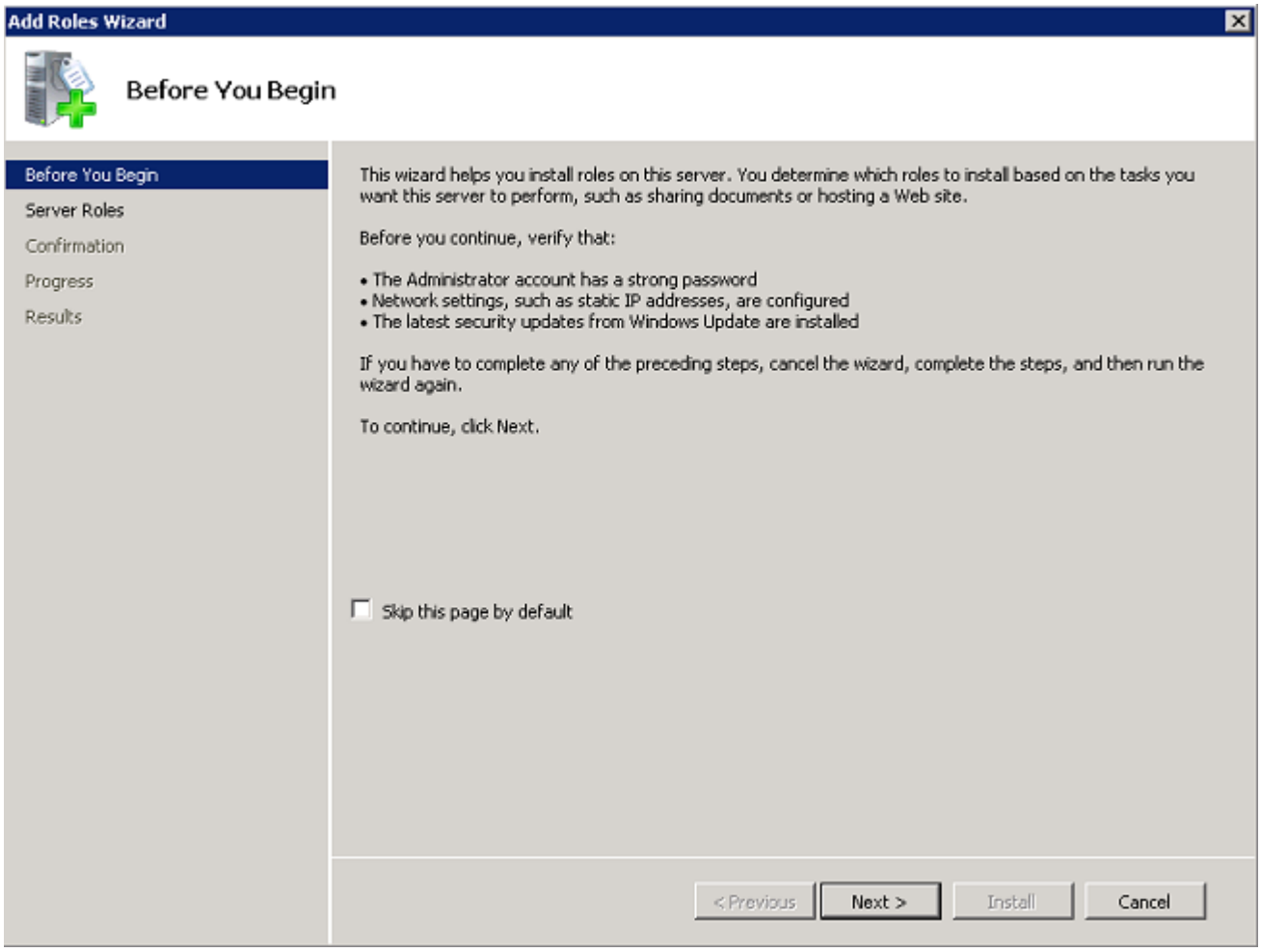
1. Fare clic su Start> Server Manager.



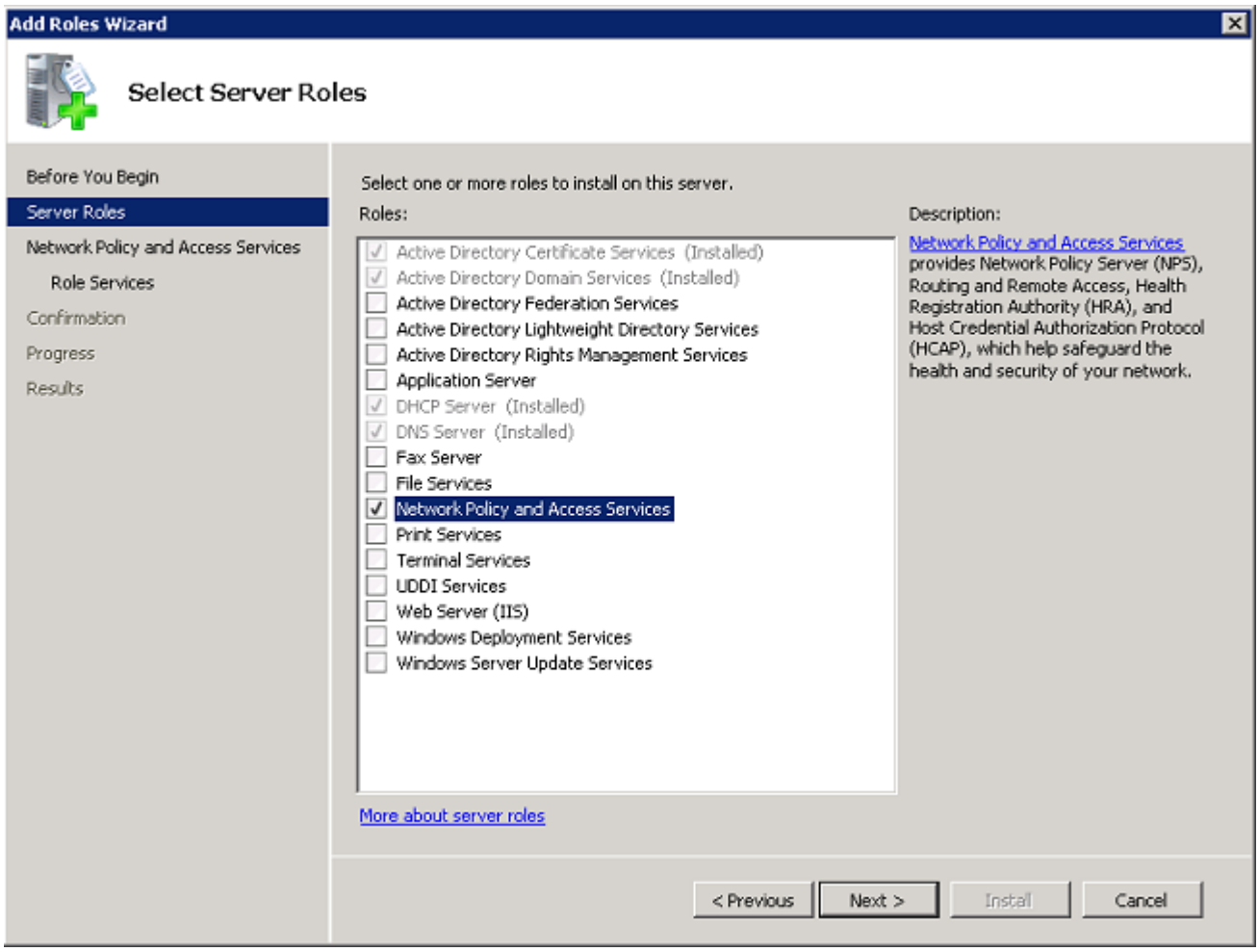
2. Fare clic su Ruoli> Aggiungi ruoli.



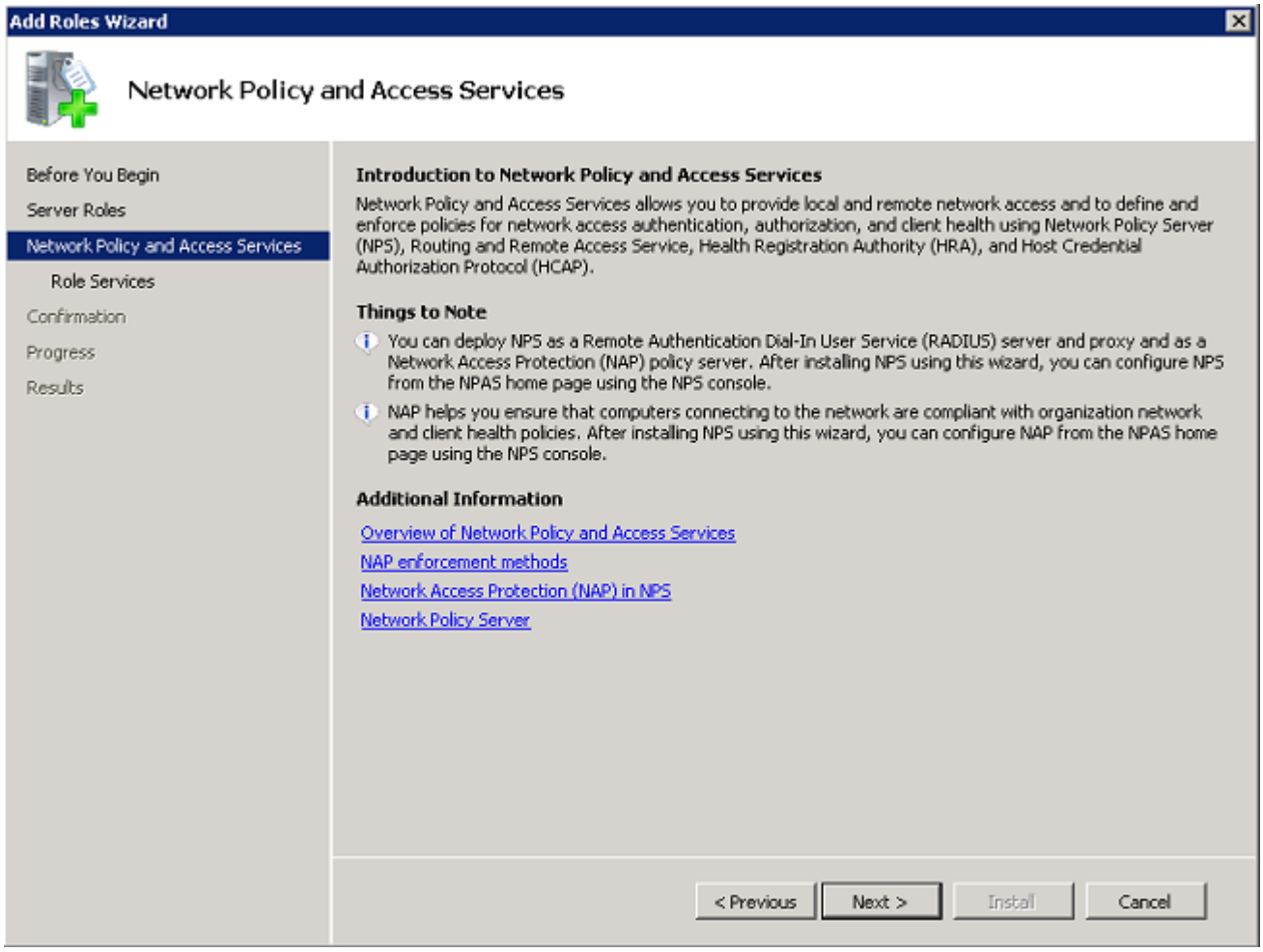
3. Fare clic su Next (Avanti).



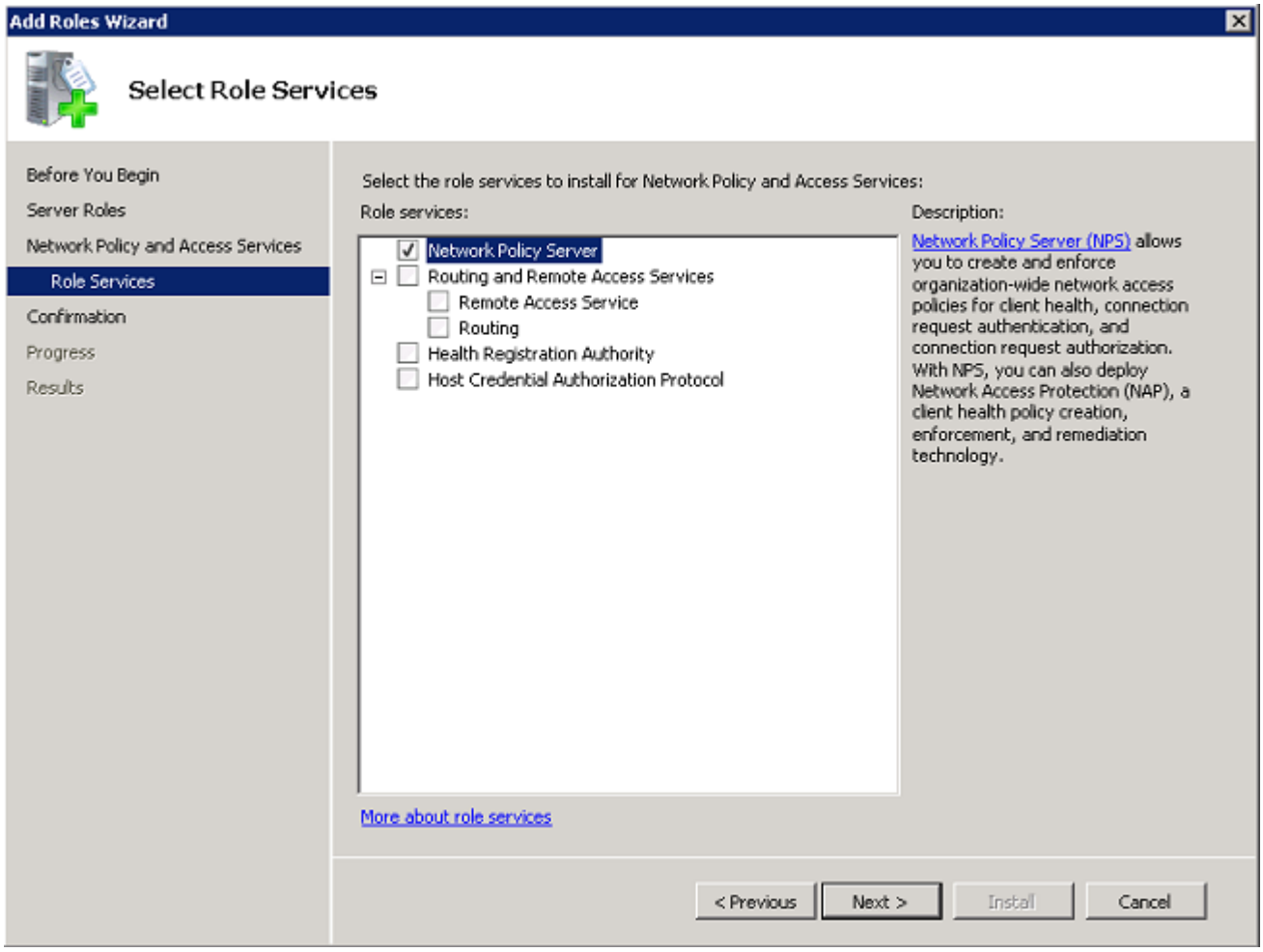
4. Selezionare il servizio Servizi di accesso e criteri di rete e fare clic su Avanti.



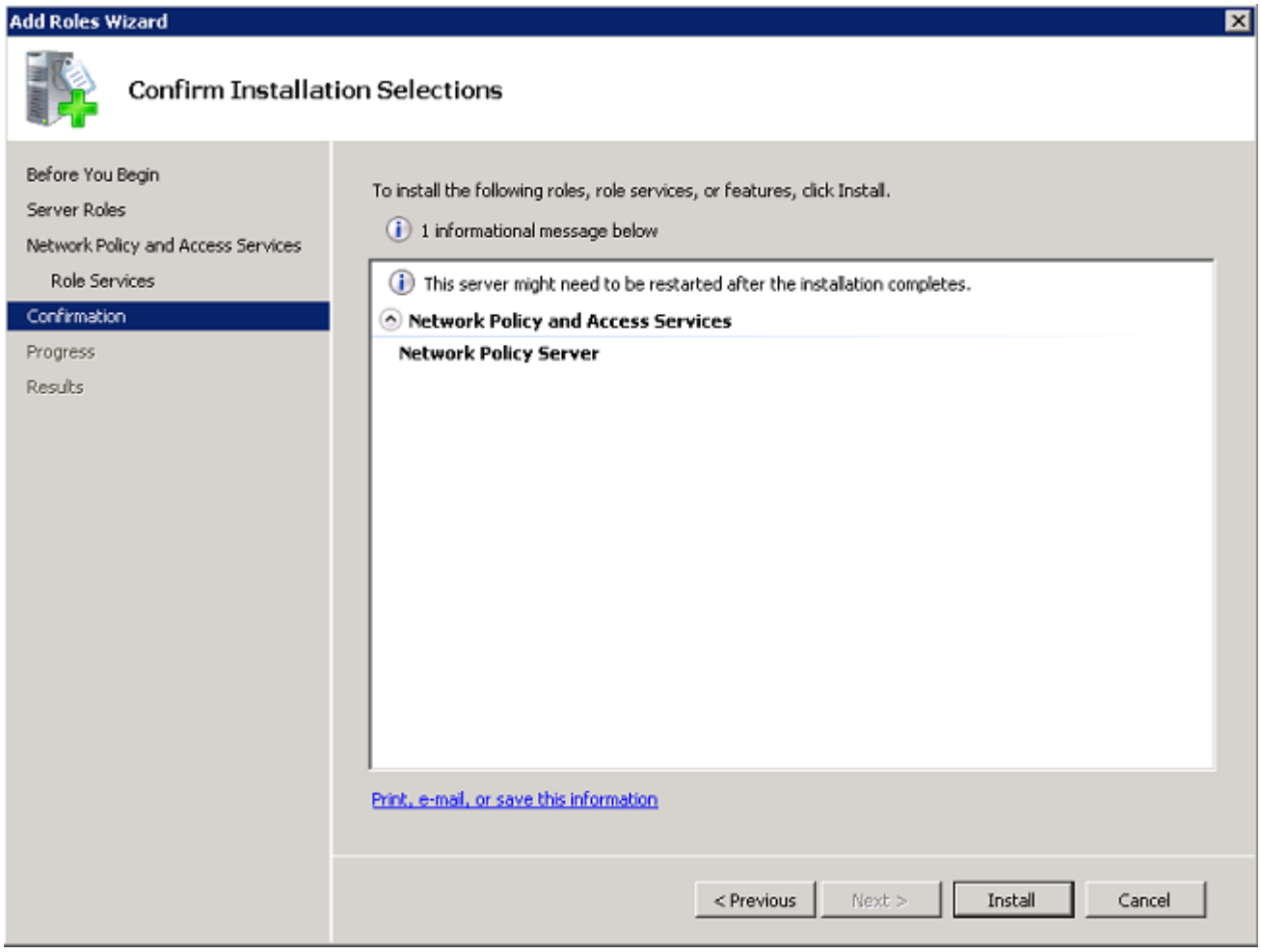
5. Rivedere l'Introduzione a Servizi di accesso e criteri di rete e fare clic su Avanti.



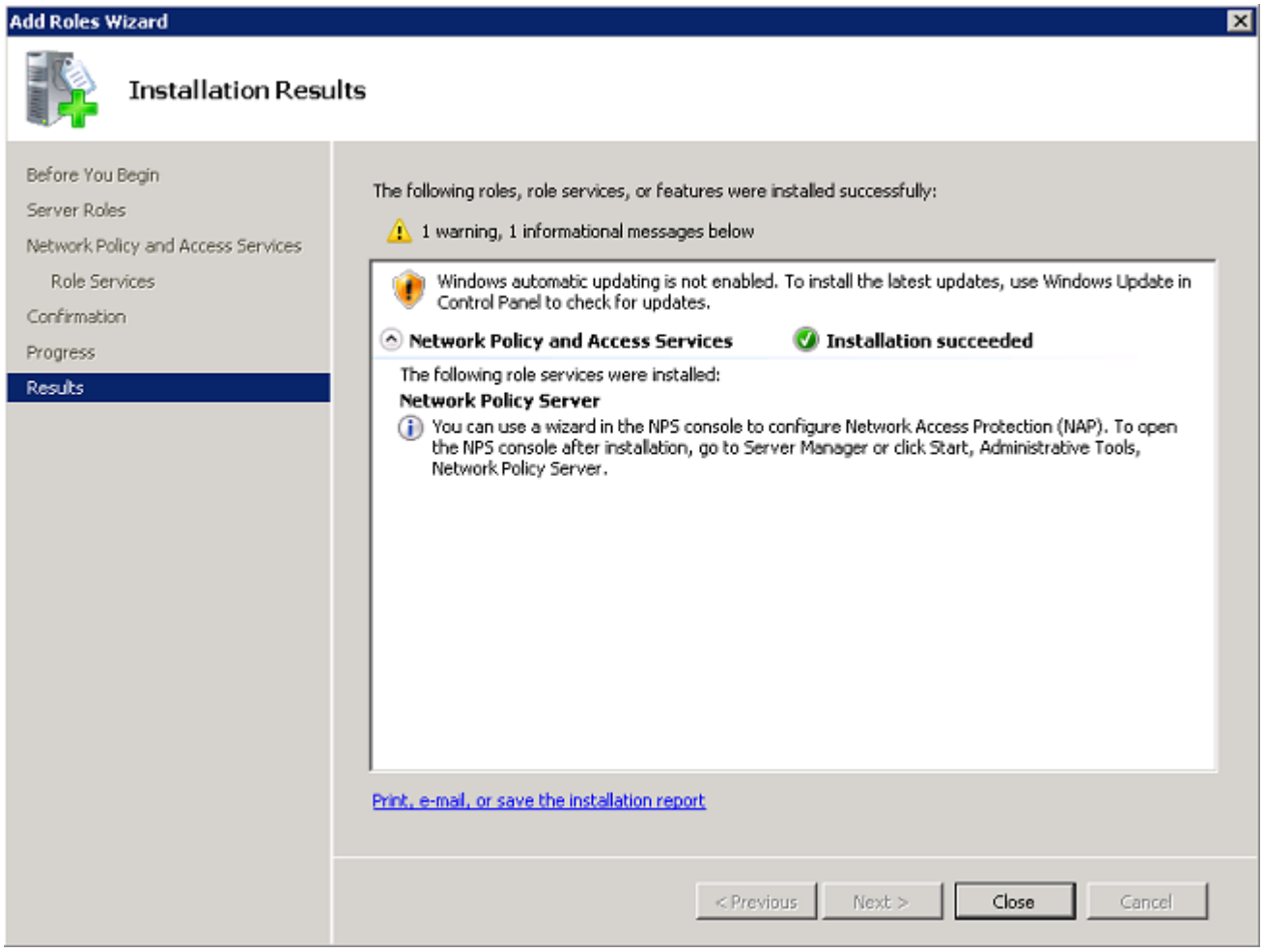
6. Selezionare Server dei criteri di rete, quindi fare clic su Avanti.



7. Verificare la conferma e fare clic su Installa.



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

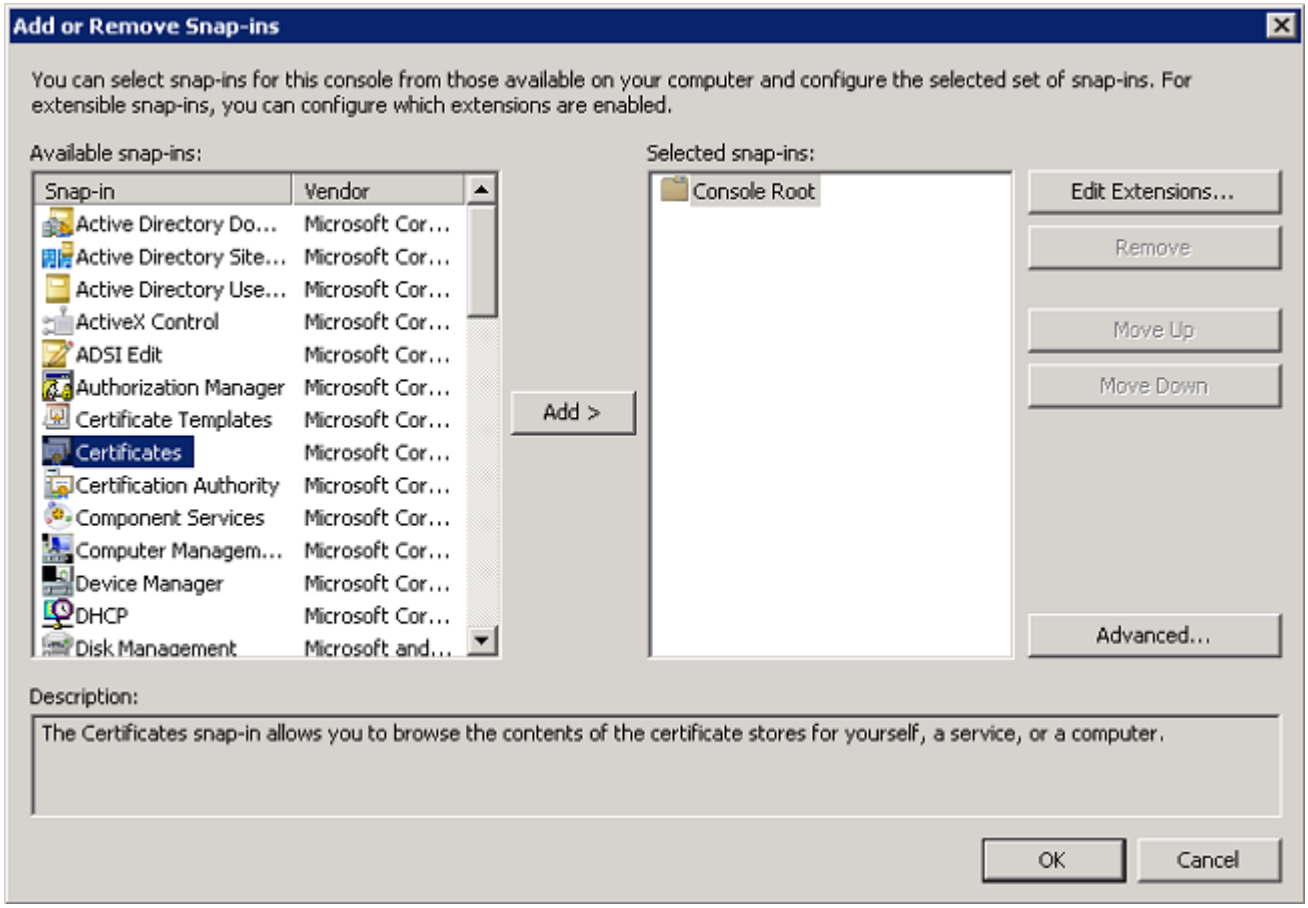


8. Fare clic su Close (Chiudi).

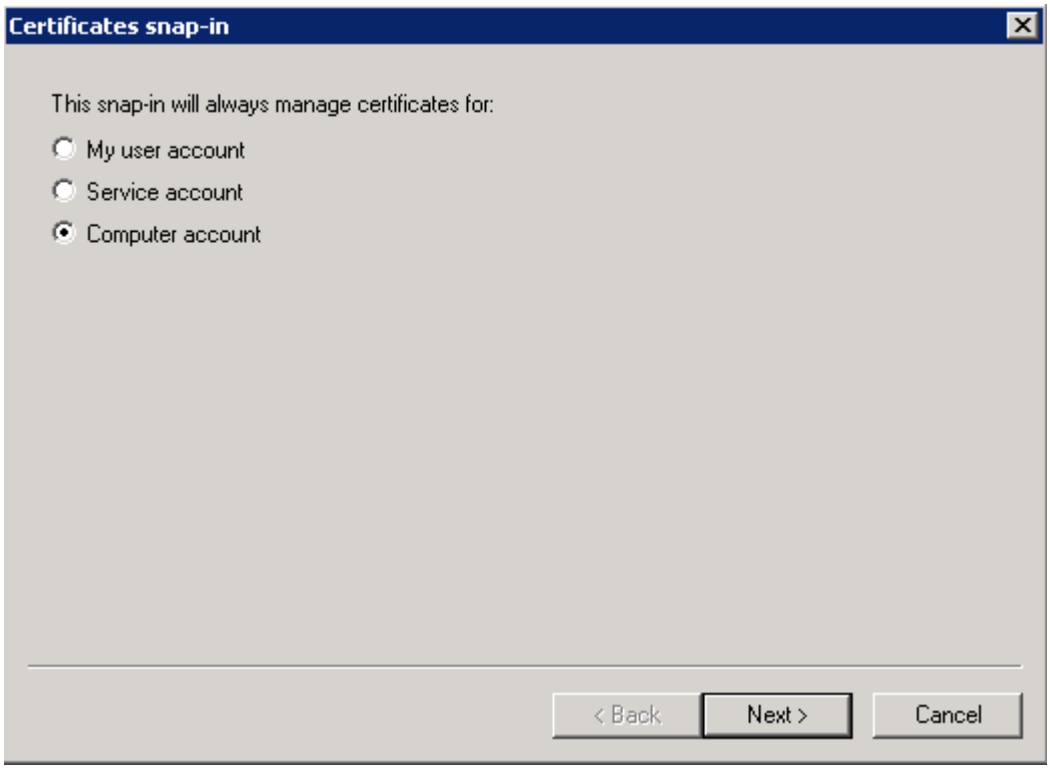
Installa un certificato

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

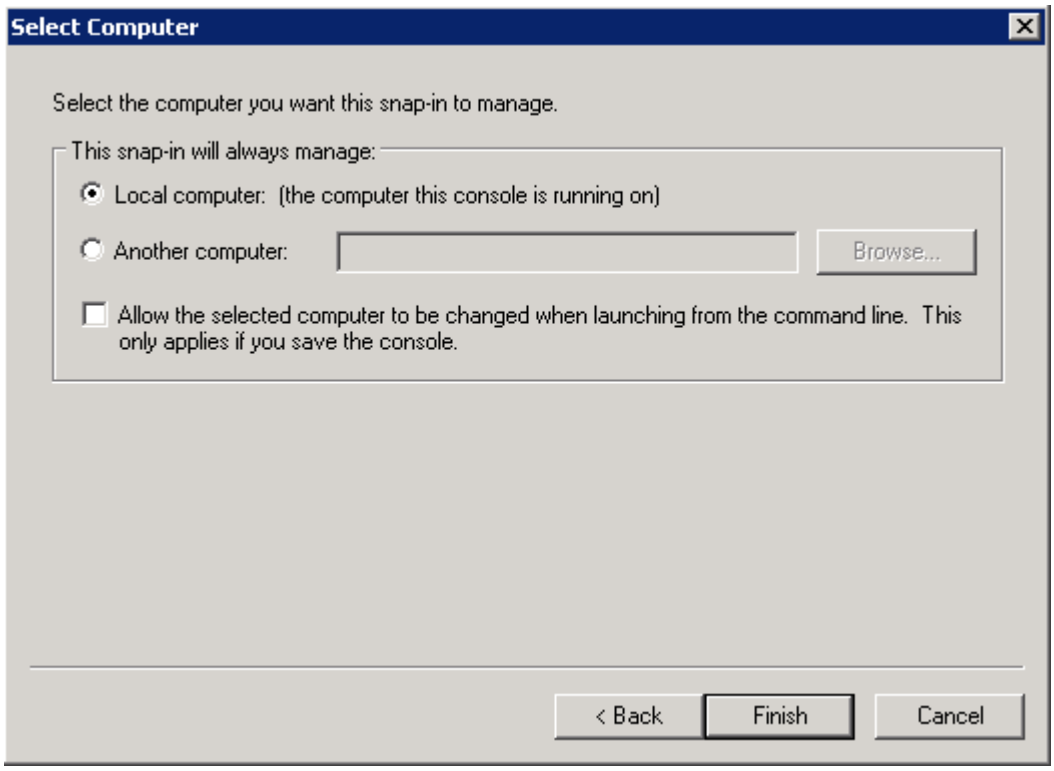
1. Fare clic su Start, immettere mmc e premere Invio.
2. Fare clic su File > Aggiungi/Rimuovi snap-in.
3. Scegliere Certificati, quindi fare clic su Aggiungi.



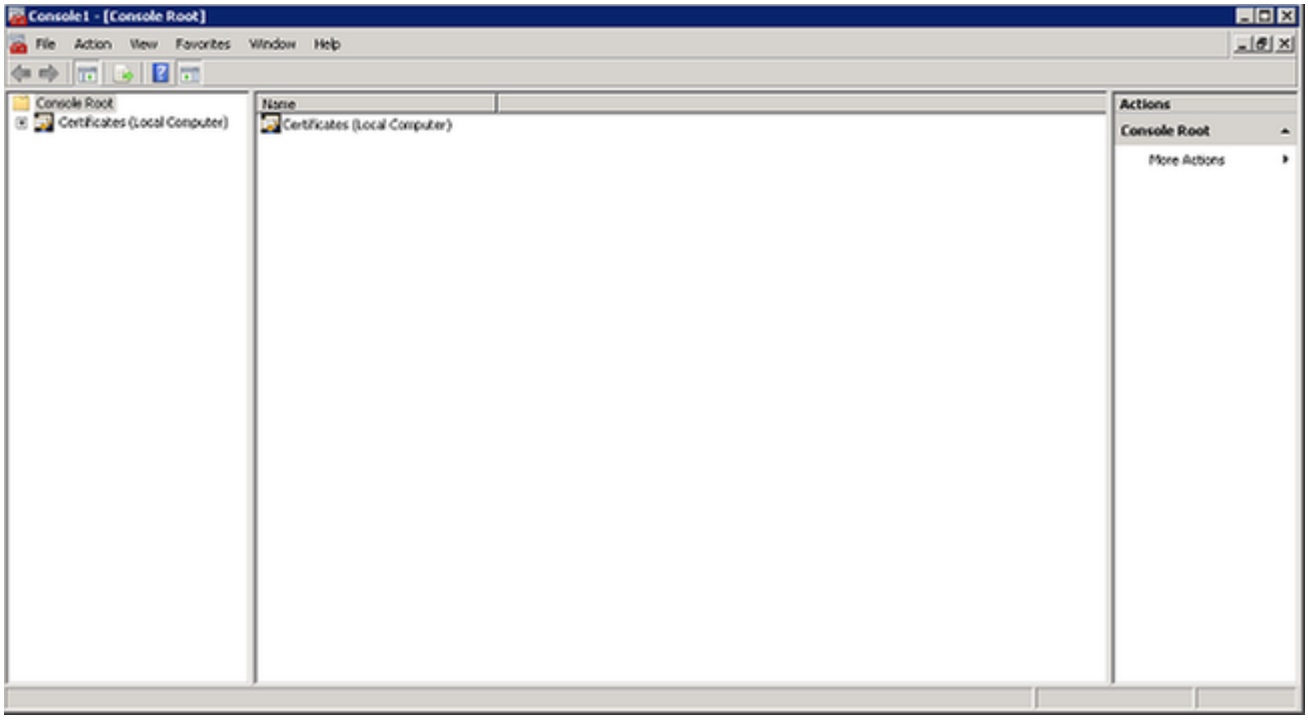
4. Scegliere Account computer e fare clic su Avanti.



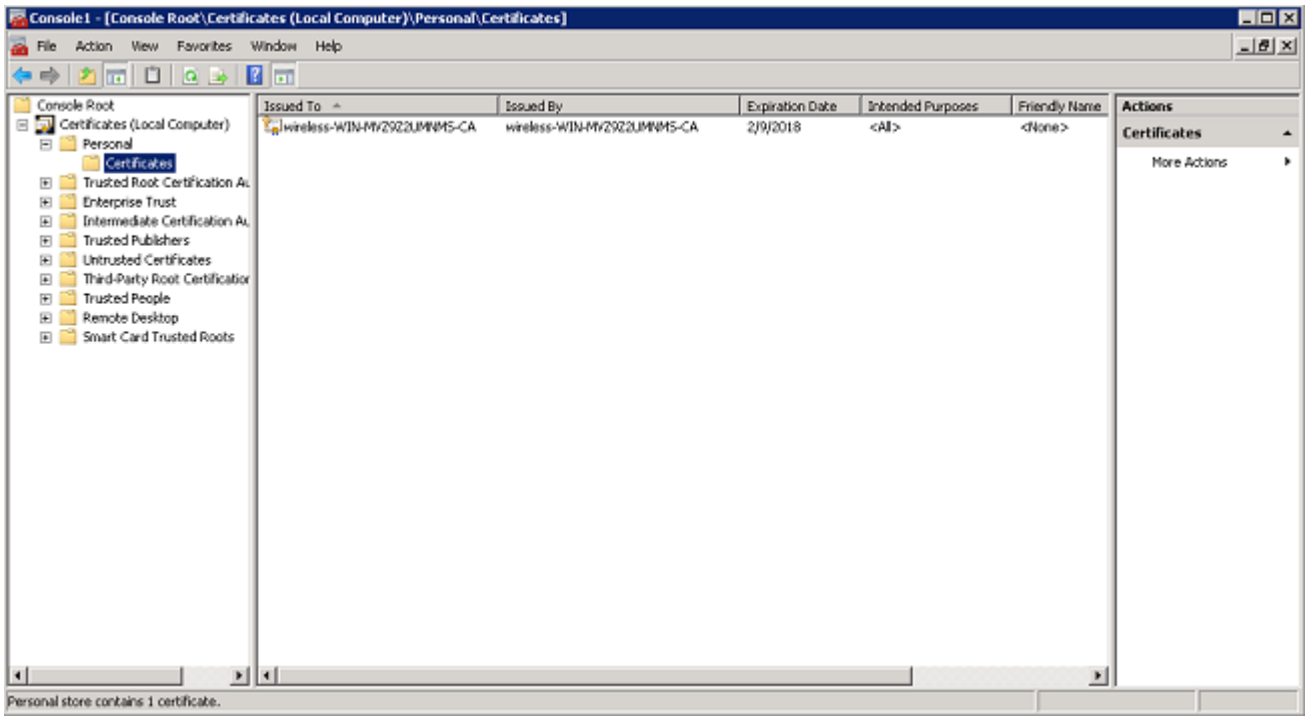
5. Selezionare Computer locale e fare clic su Fine.



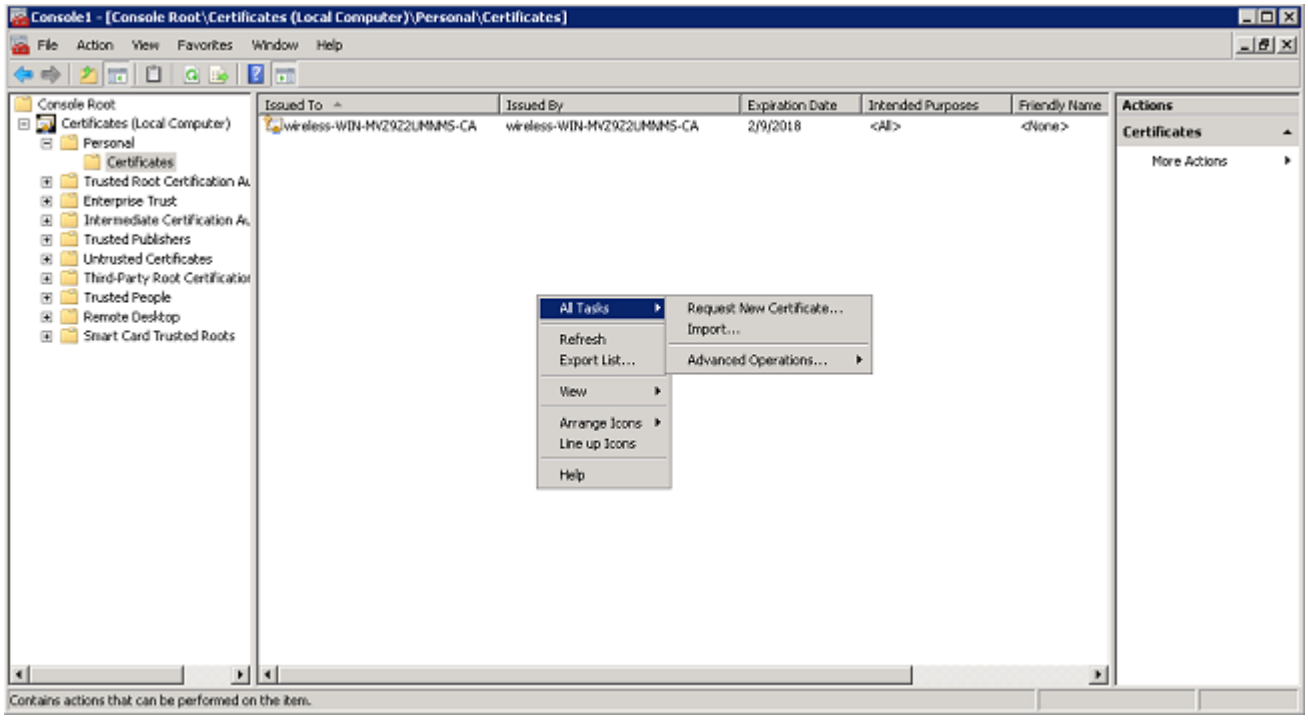
6. Fare clic su OK per tornare a Microsoft Management Console (MMC).



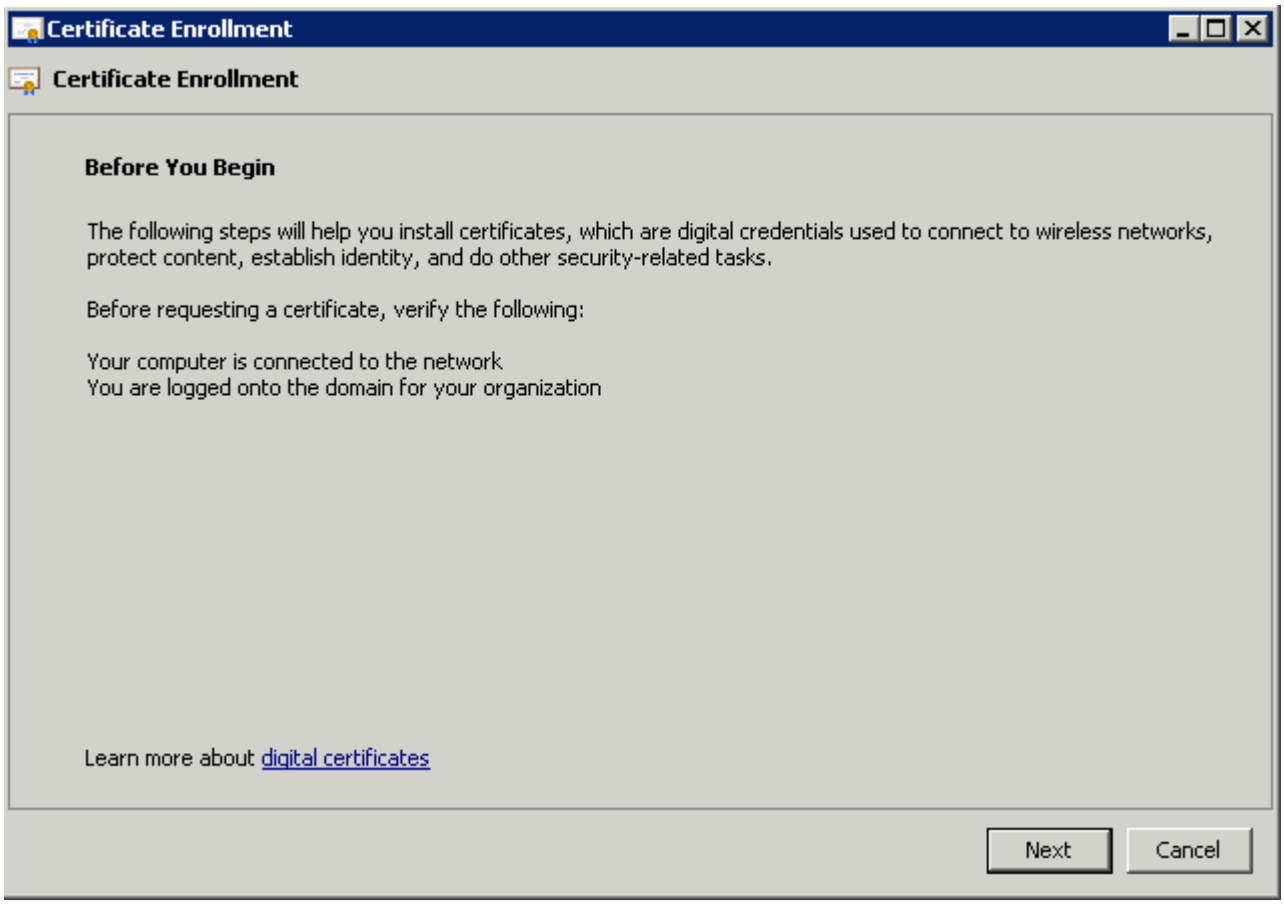
7. Espandere le cartelle Certificati (computer locale) e Personale e fare clic su Certificati.



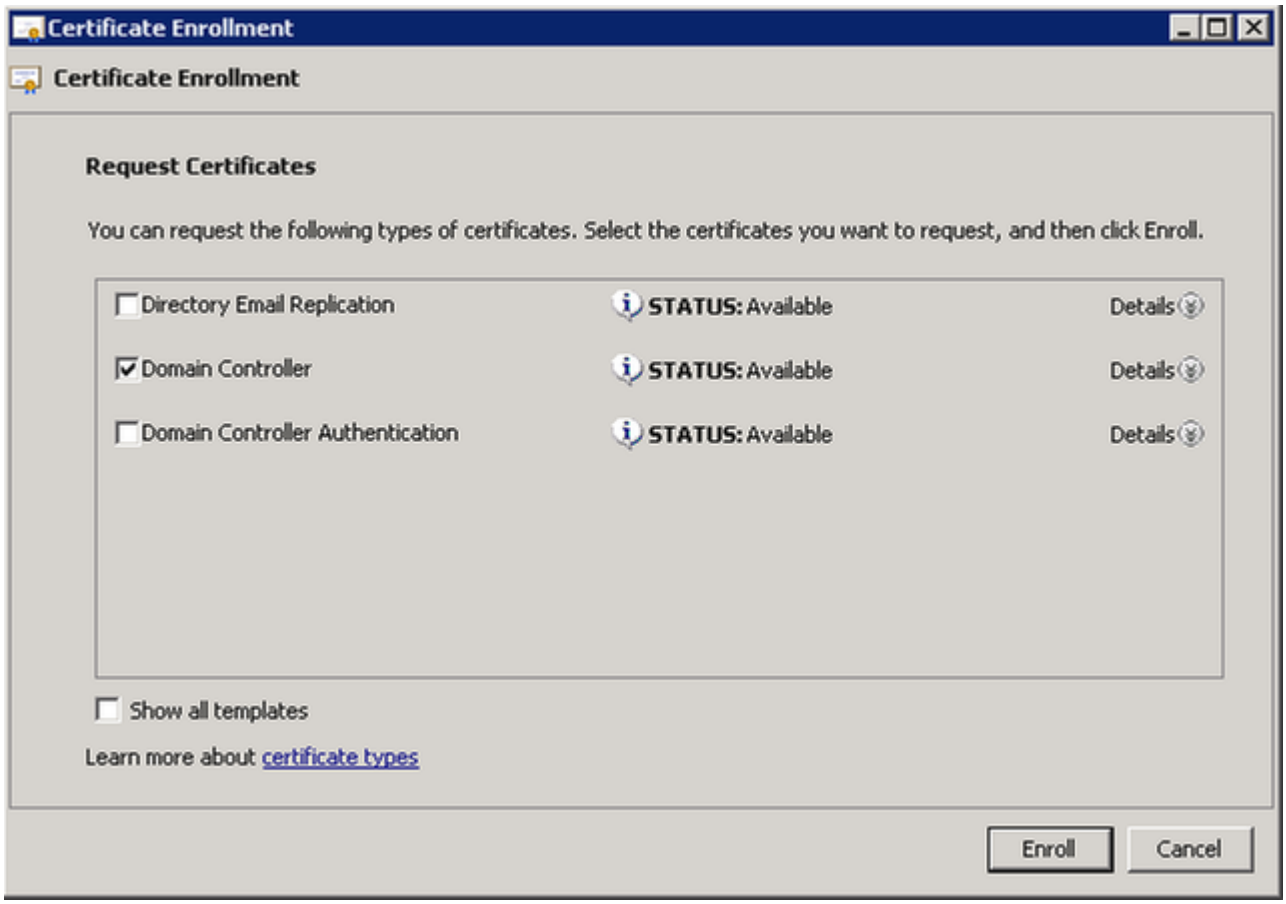
8. Fare clic con il pulsante destro del mouse nello spazio sotto il certificato CA e scegliere Tutte le attività > Richiedi nuovo certificato.



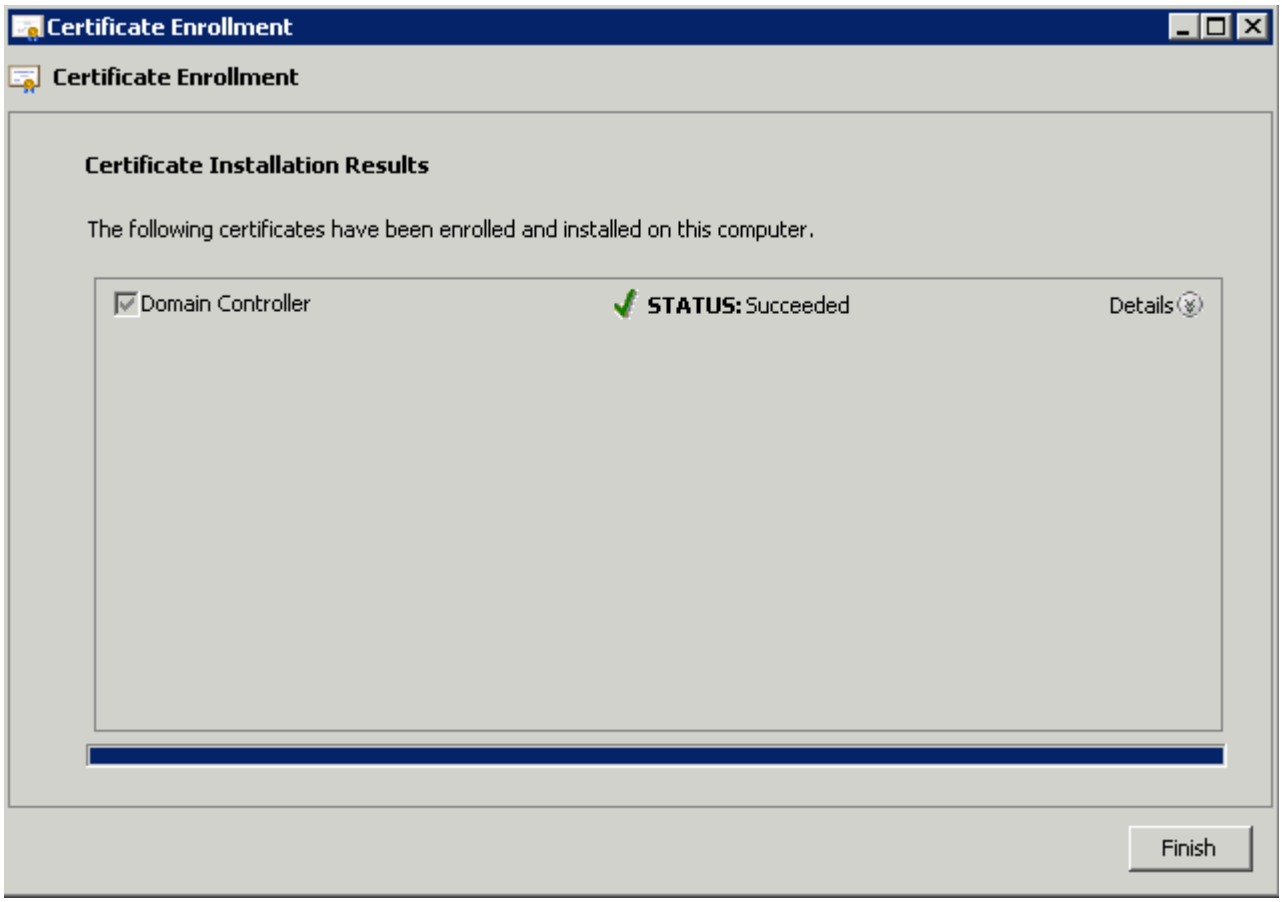
9. Fare clic su Next (Avanti).



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

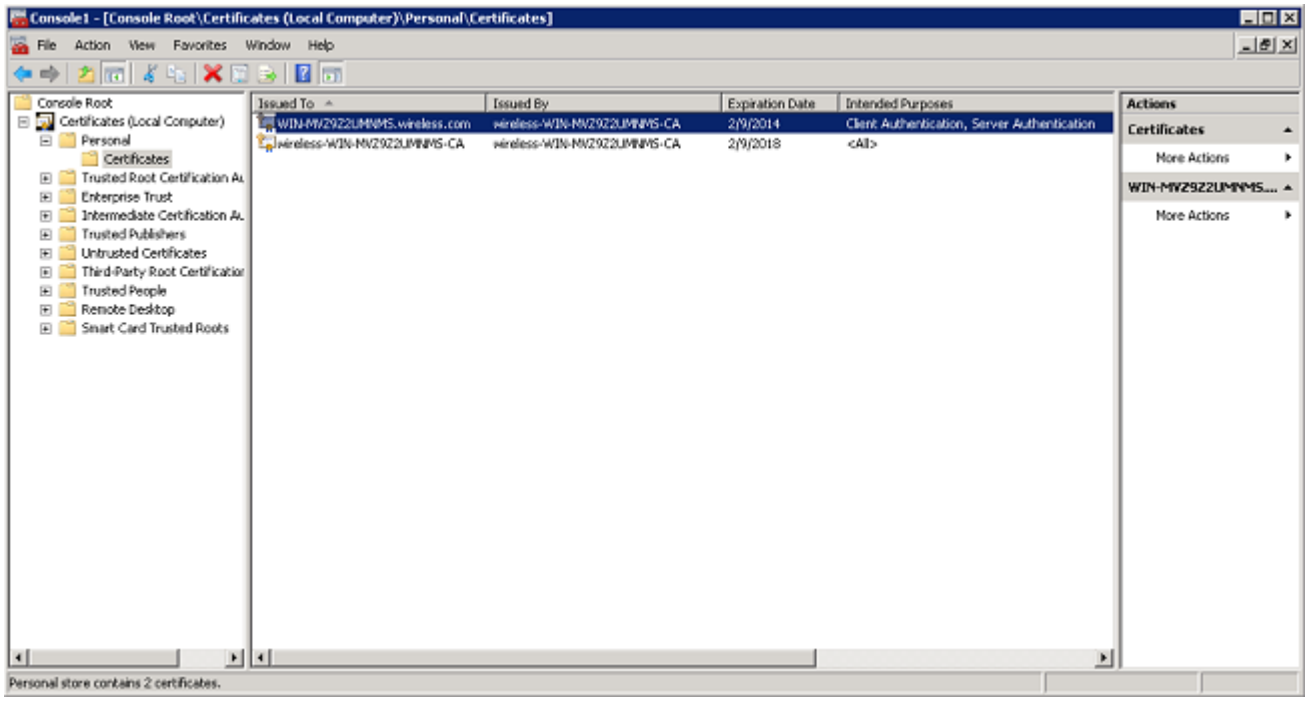


11. Una volta installato il certificato, fare clic su Fine.



Il certificato del Server dei criteri di rete è installato.

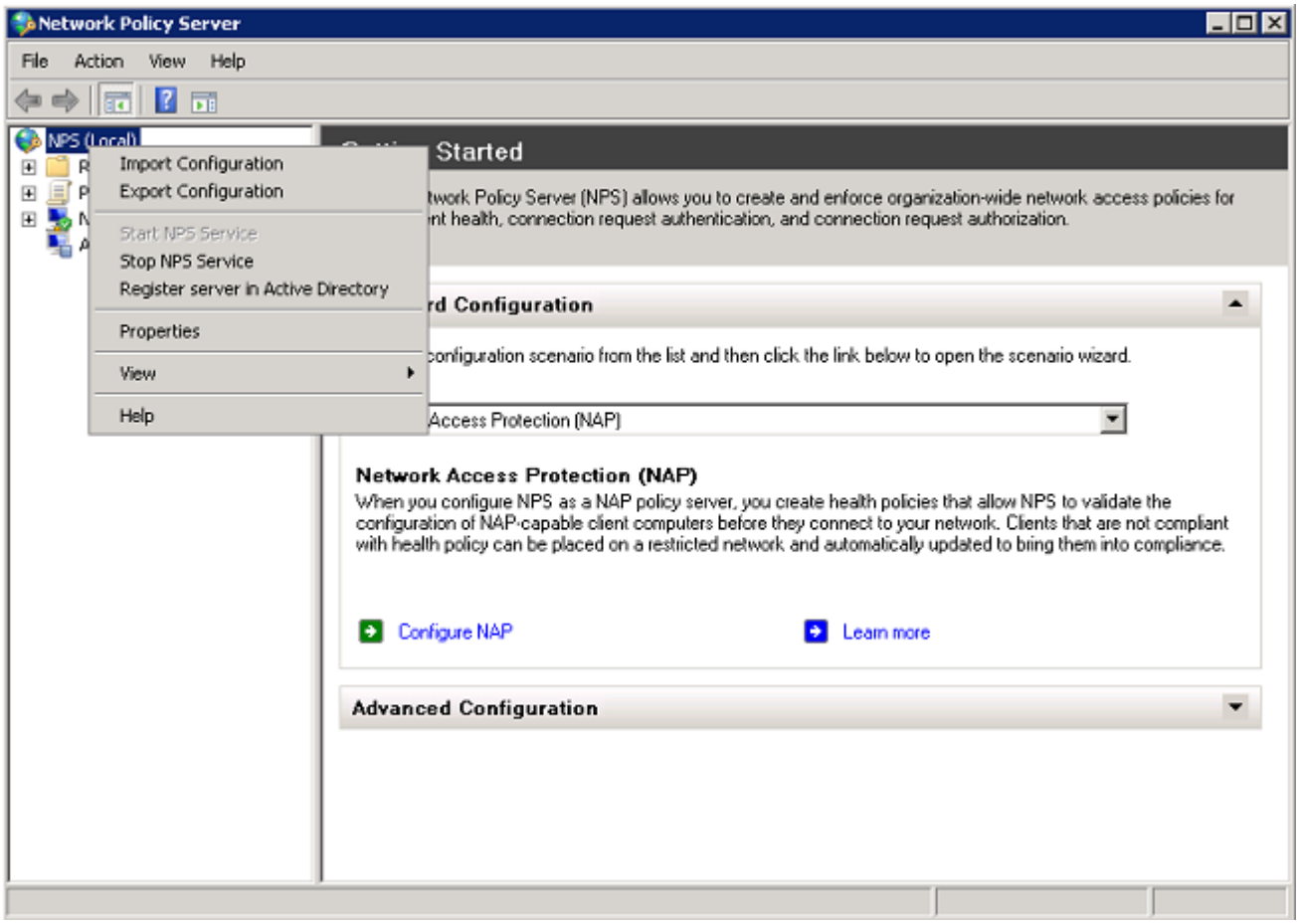
12. Verificare che lo scopo previsto del certificato sia Autenticazione client, Autenticazione server.



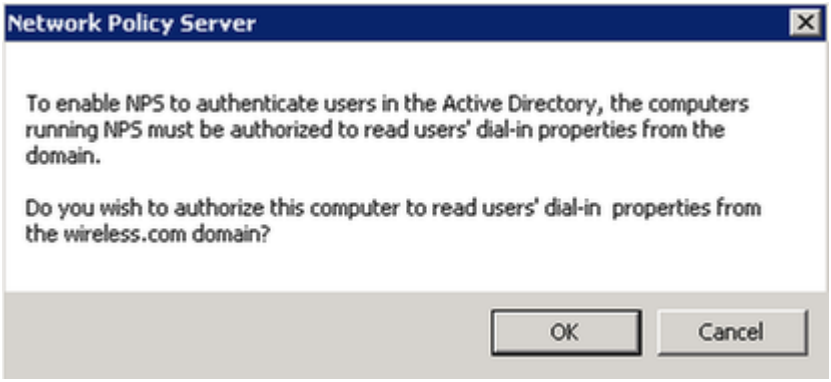
Configurare il servizio Server dei criteri di rete per l'autenticazione PEAP-MS-CHAP v2

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

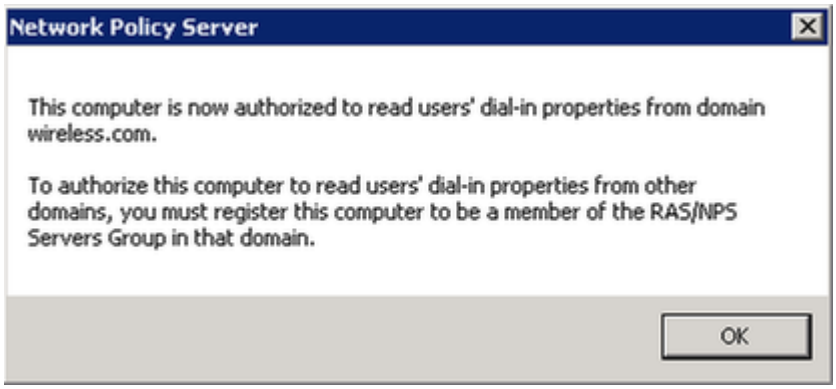
1. Fare clic su Start > Strumenti di amministrazione> Server dei criteri di rete.
2. Fare clic con il pulsante destro del mouse su Server dei criteri di rete (locale) e scegliere Registra server in Active Directory.



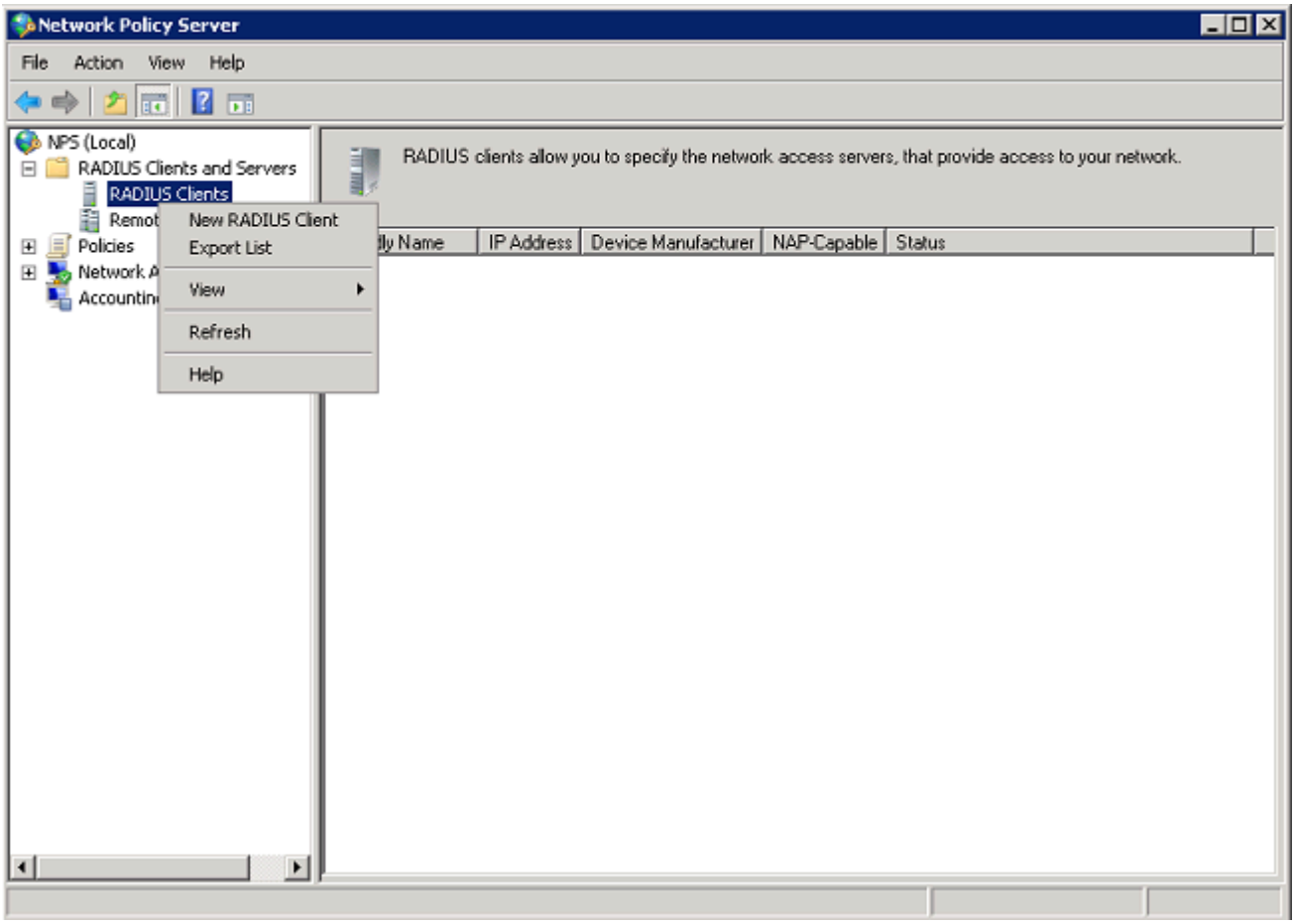
3. Fare clic su OK.



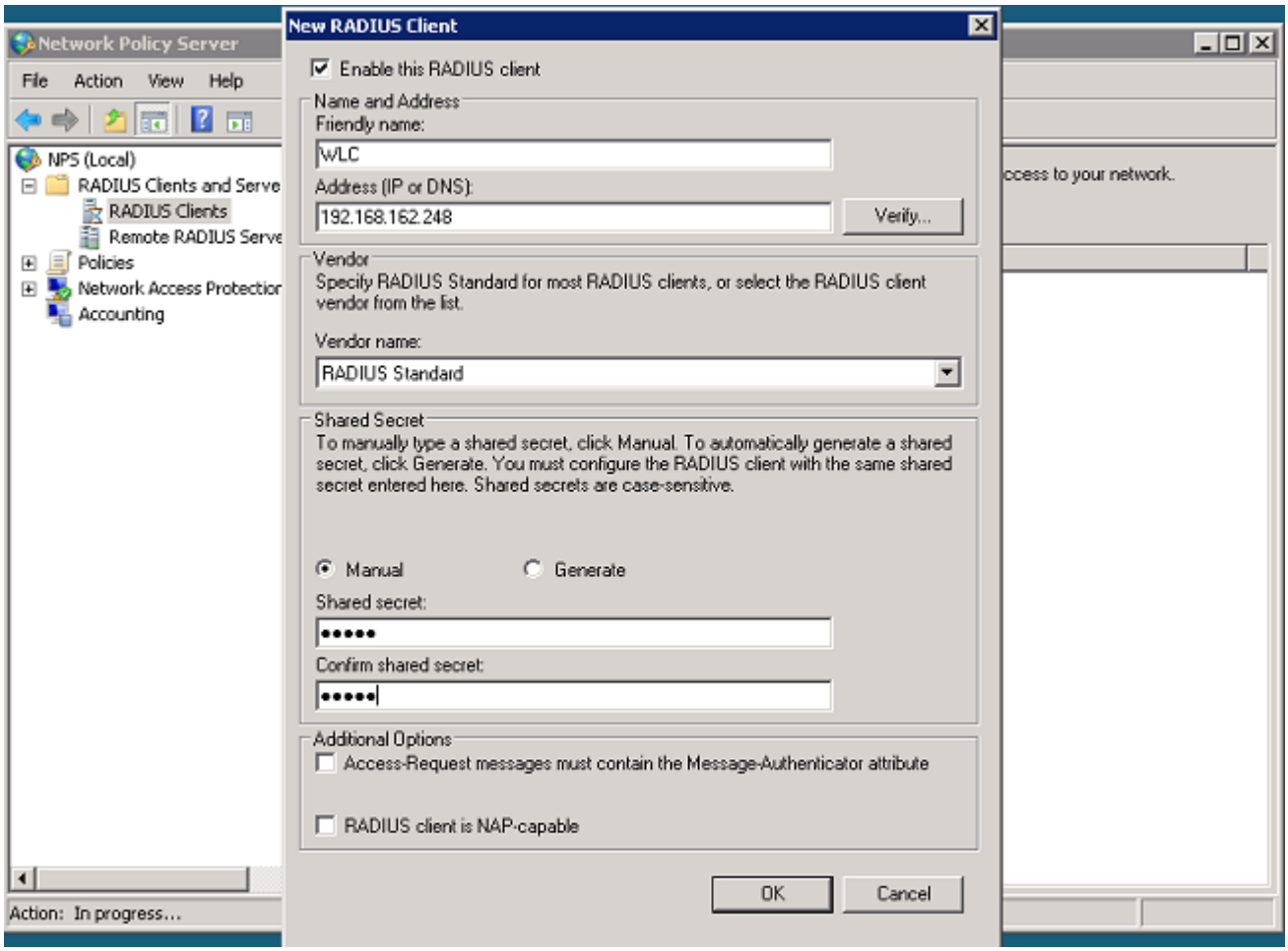
4. Fare clic su OK.



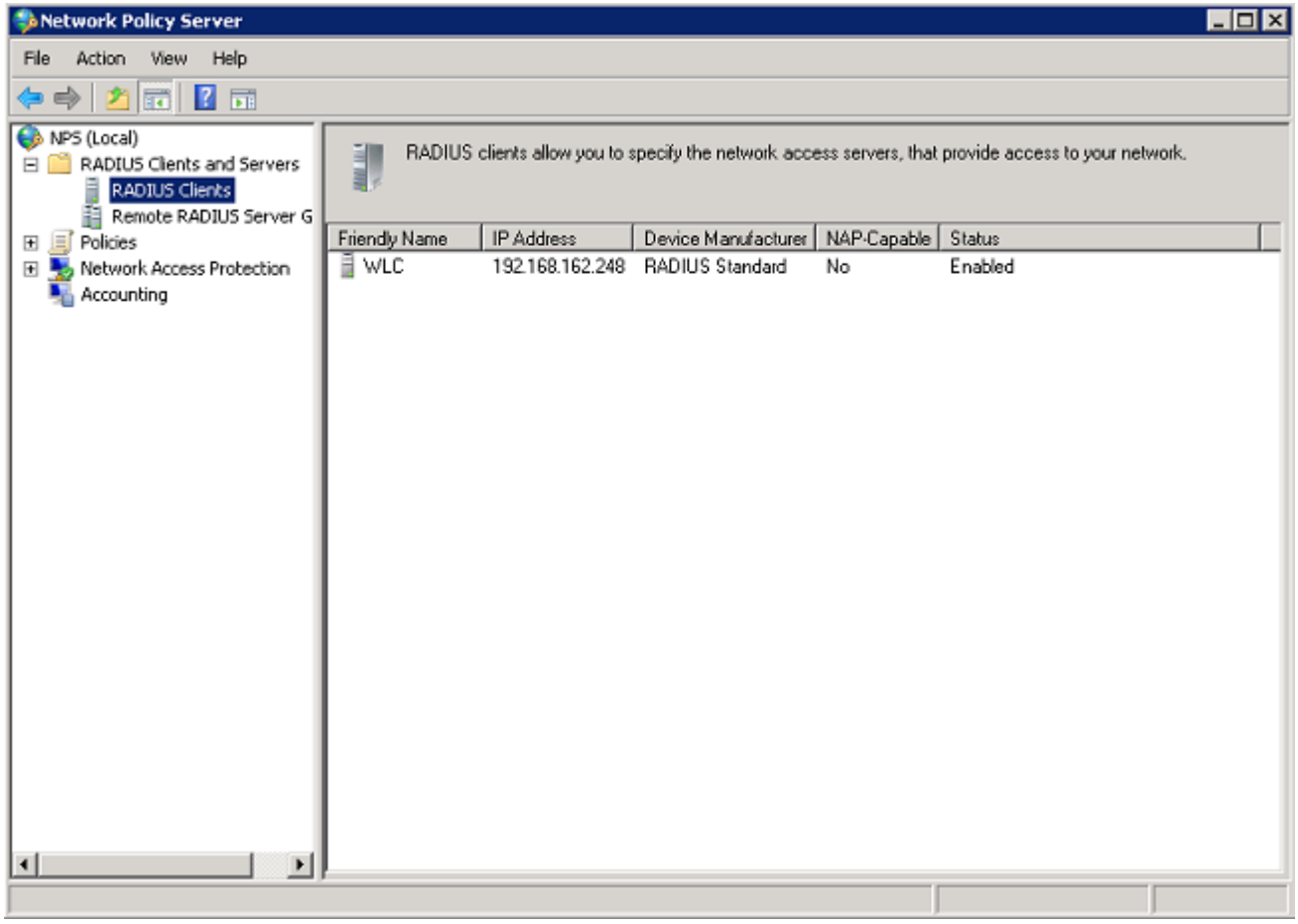
5. Aggiungere il controller LAN wireless come client di autenticazione, autorizzazione e accounting (AAA) nel Server dei criteri di rete.
6. Espandere Client e server RADIUS. Fare clic con il pulsante destro del mouse su Client RADIUS, quindi scegliere Nuovo client RADIUS.



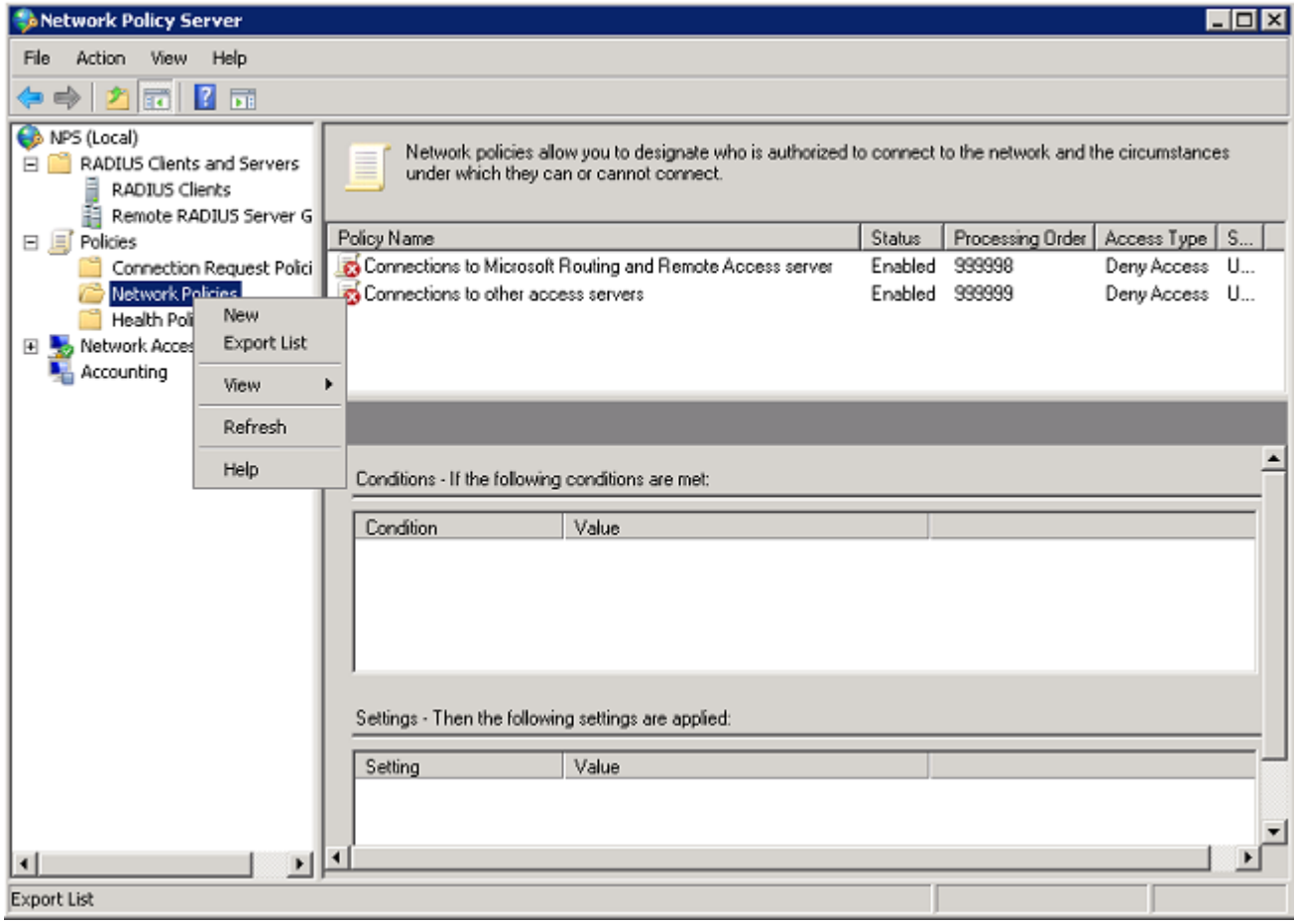
7. Immettere un nome descrittivo (WLC in questo esempio), l'indirizzo IP di gestione del WLC (192.168.162.248 in questo esempio) e un segreto condiviso. Lo stesso segreto condiviso viene utilizzato per configurare il WLC.



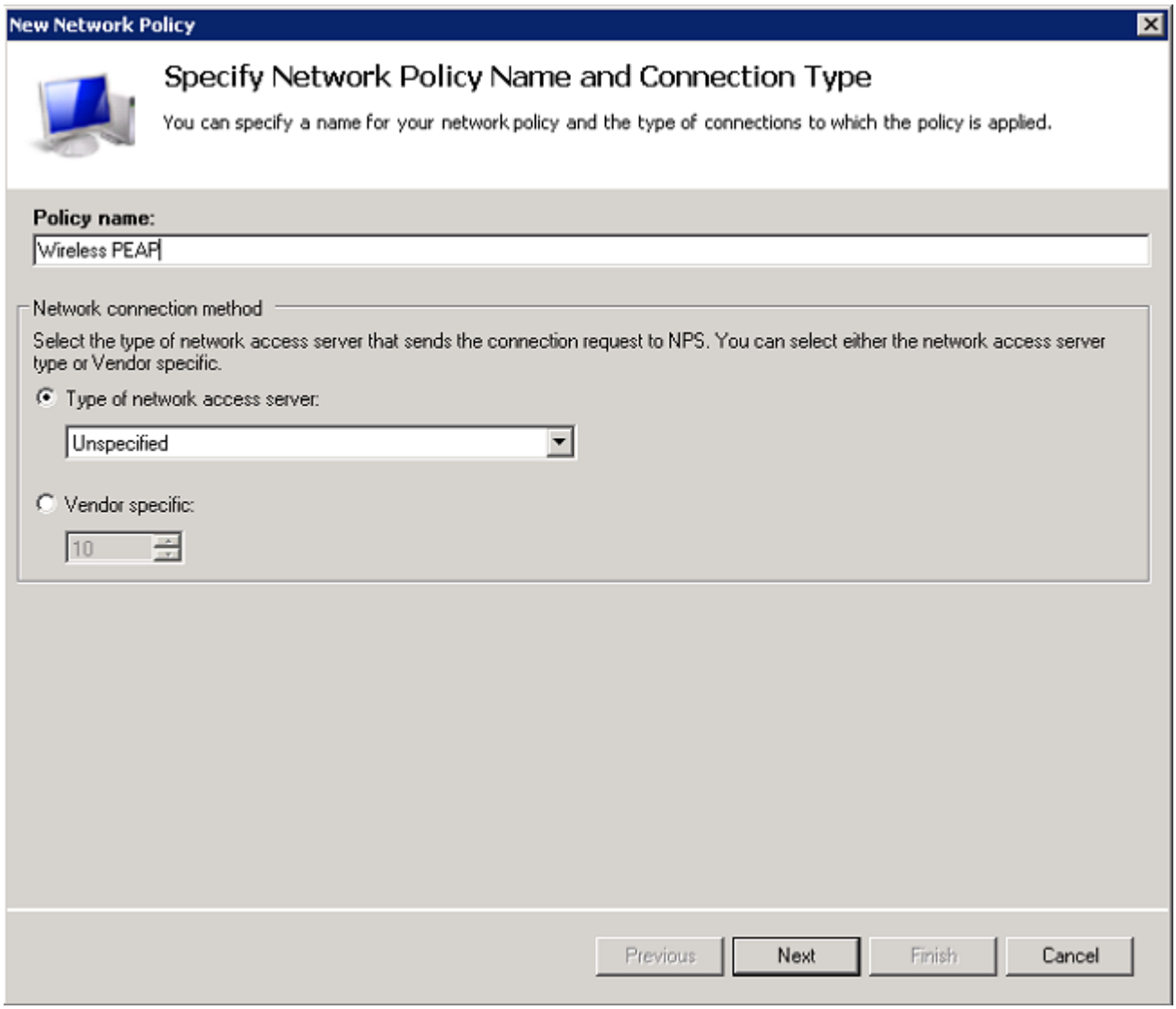
8. Fare clic su OK per tornare alla schermata precedente.



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.

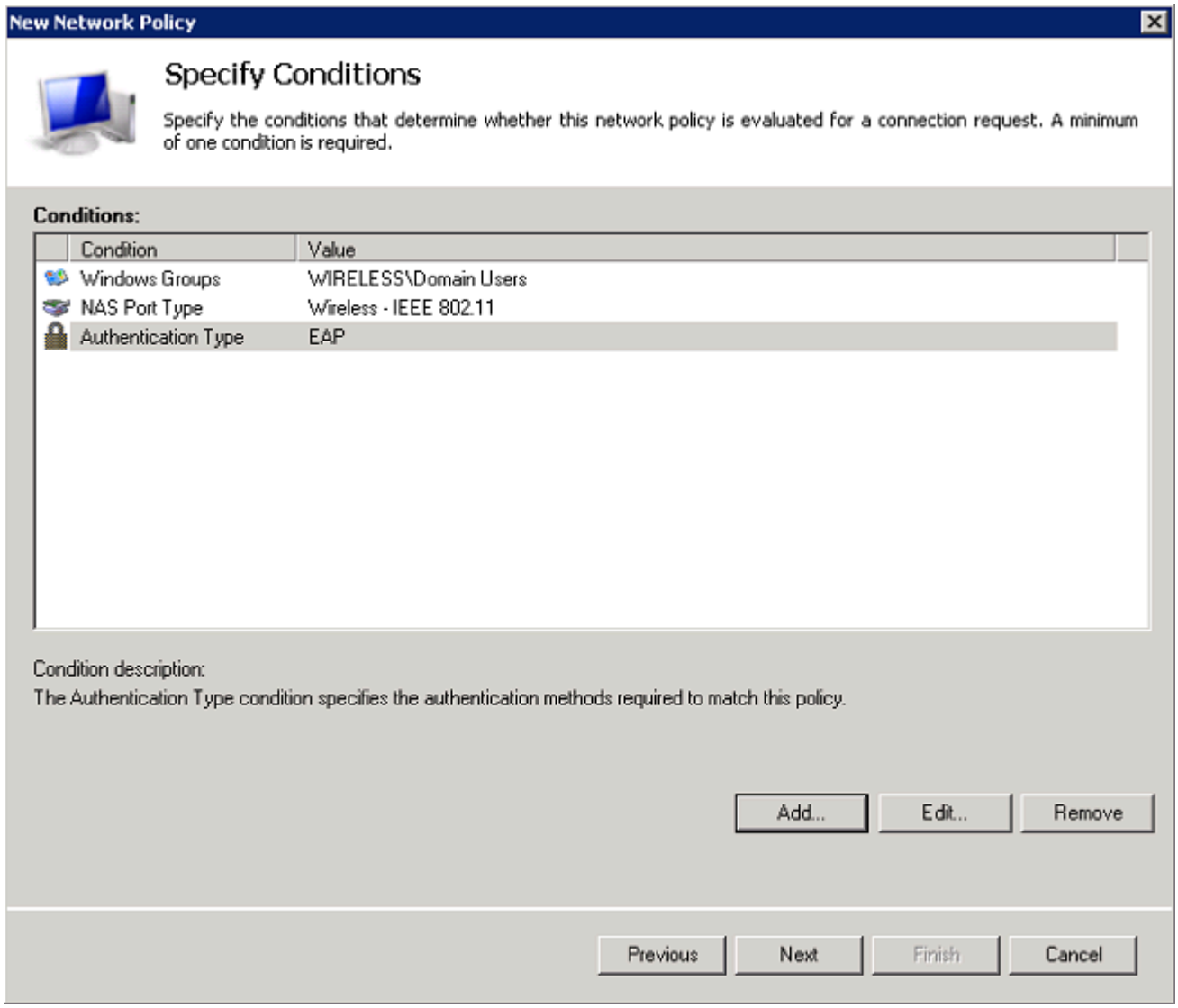


10. Immettere un nome di criterio per la regola (in questo esempio, Wireless PEAP) e fare clic su Avanti.

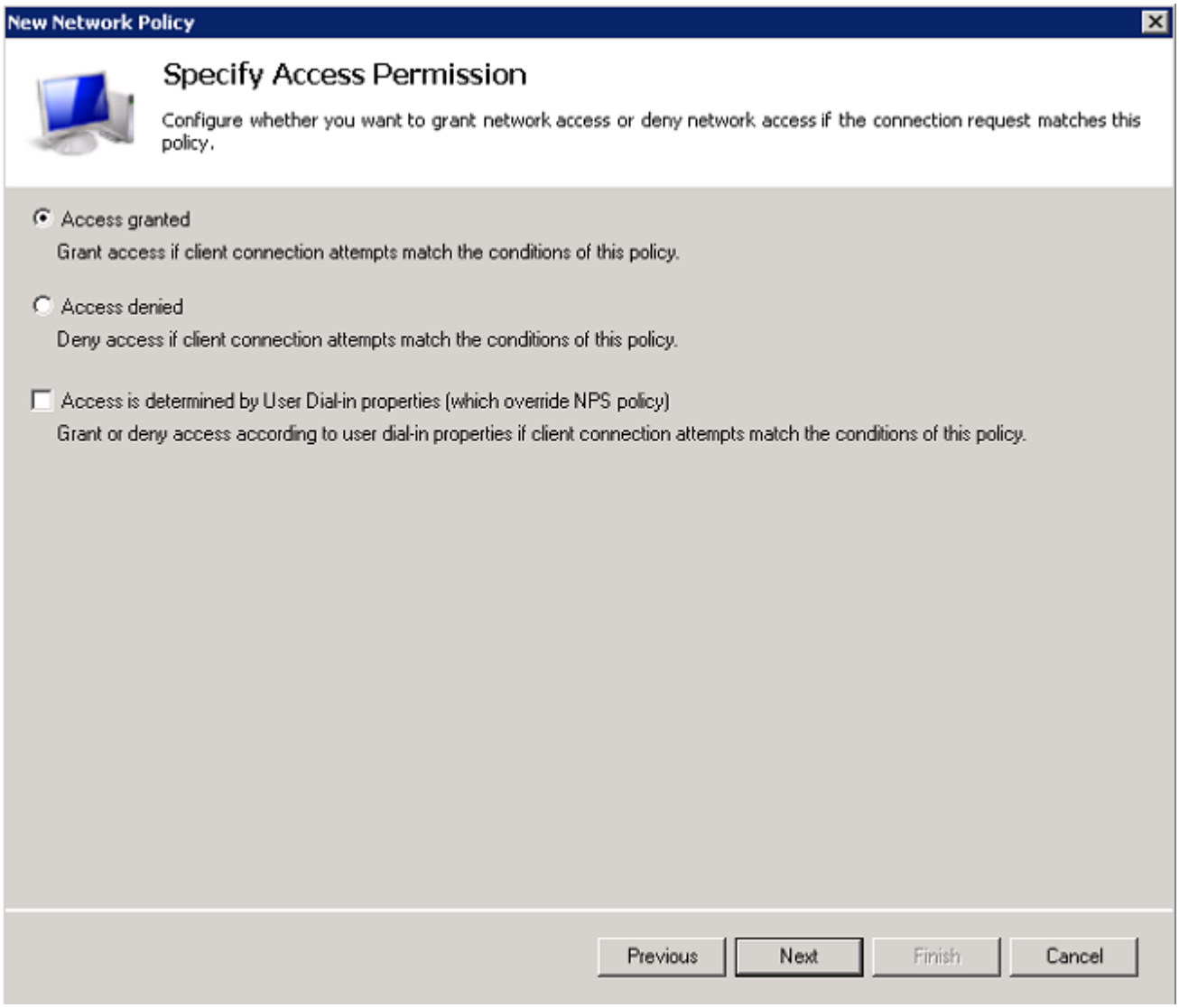


11. Per fare in modo che questo criterio consenta solo gli utenti del dominio wireless, aggiungere le tre condizioni seguenti e fare clic su Avanti:

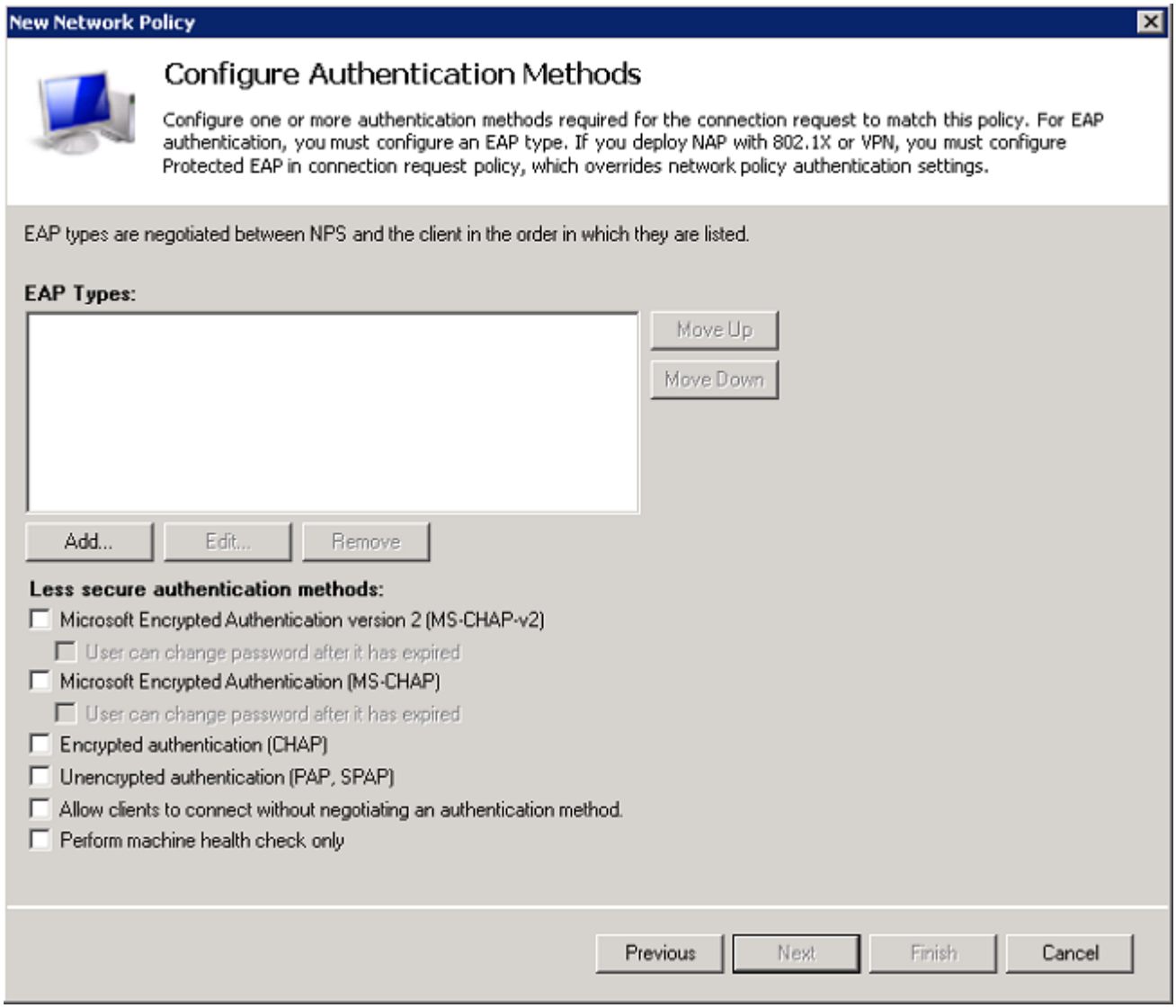
    - Gruppi di Windows - Utenti del dominio
    - Tipo porta NAS - Wireless - IEEE 802.11
    - Tipo di autenticazione - EAP



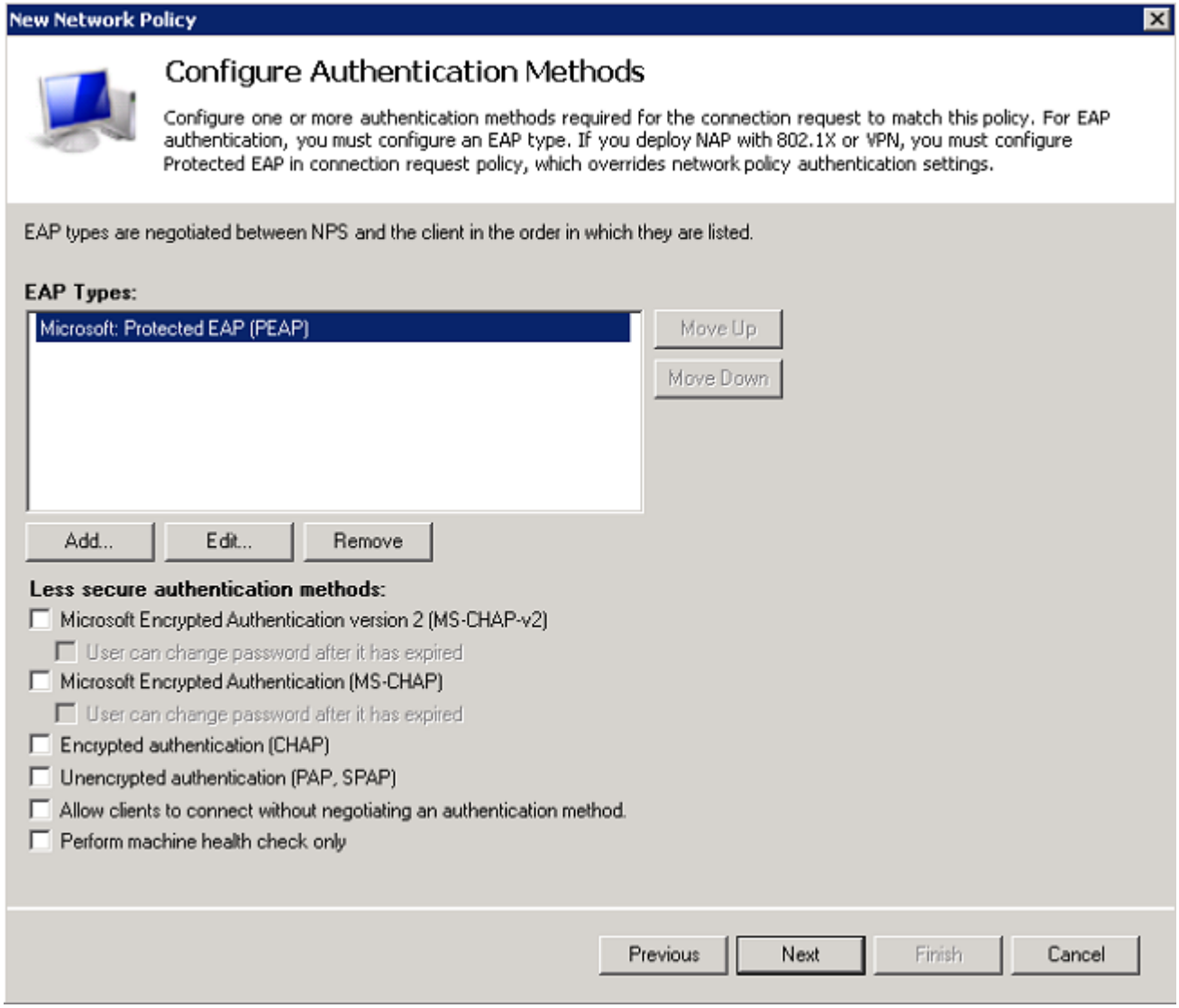
12. Fare clic su Accesso concesso per concedere i tentativi di connessione corrispondenti al criterio e quindi su Avanti.



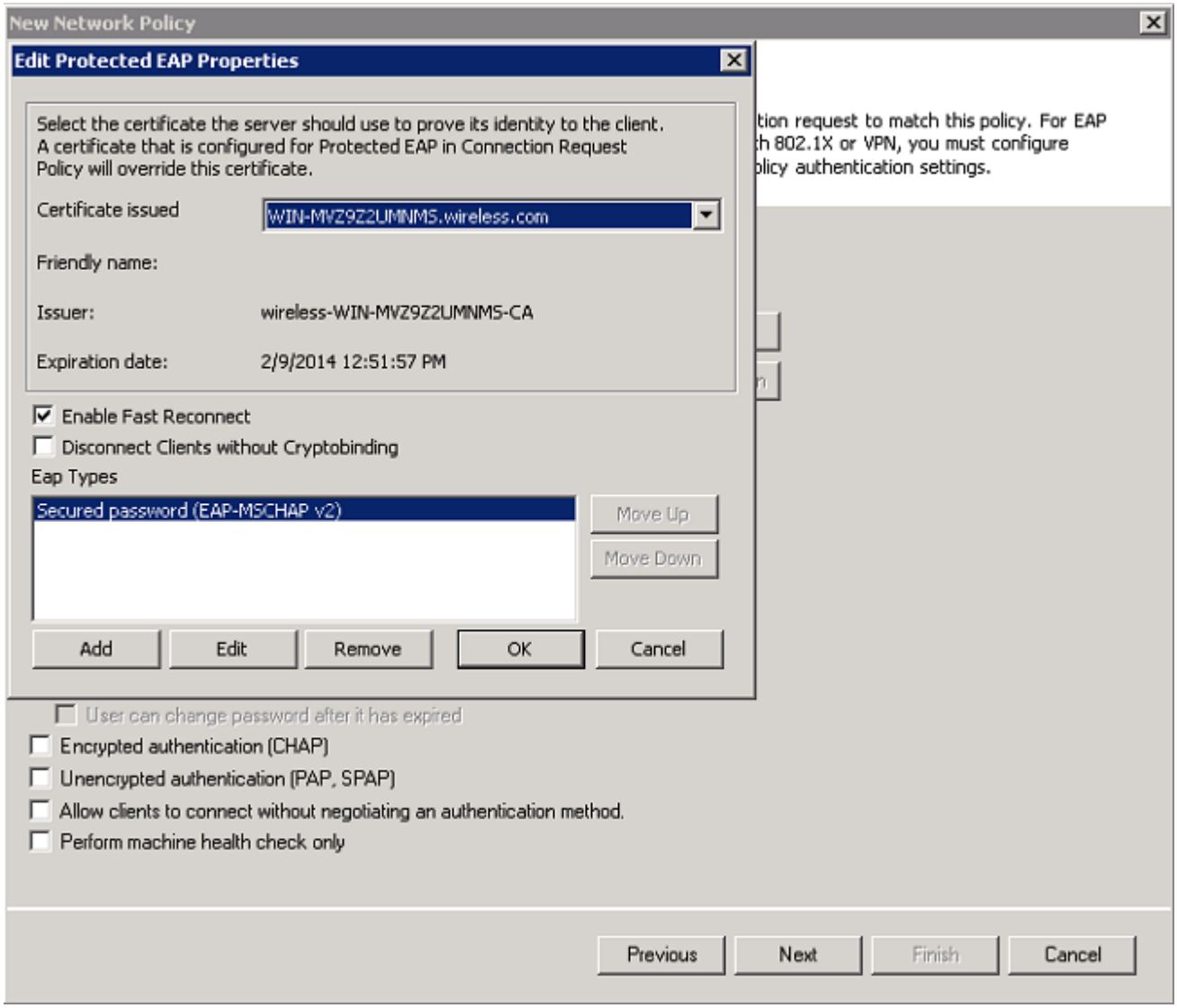
13. Disabilitare tutti i metodi di autenticazione in Metodi di autenticazione meno sicuri.



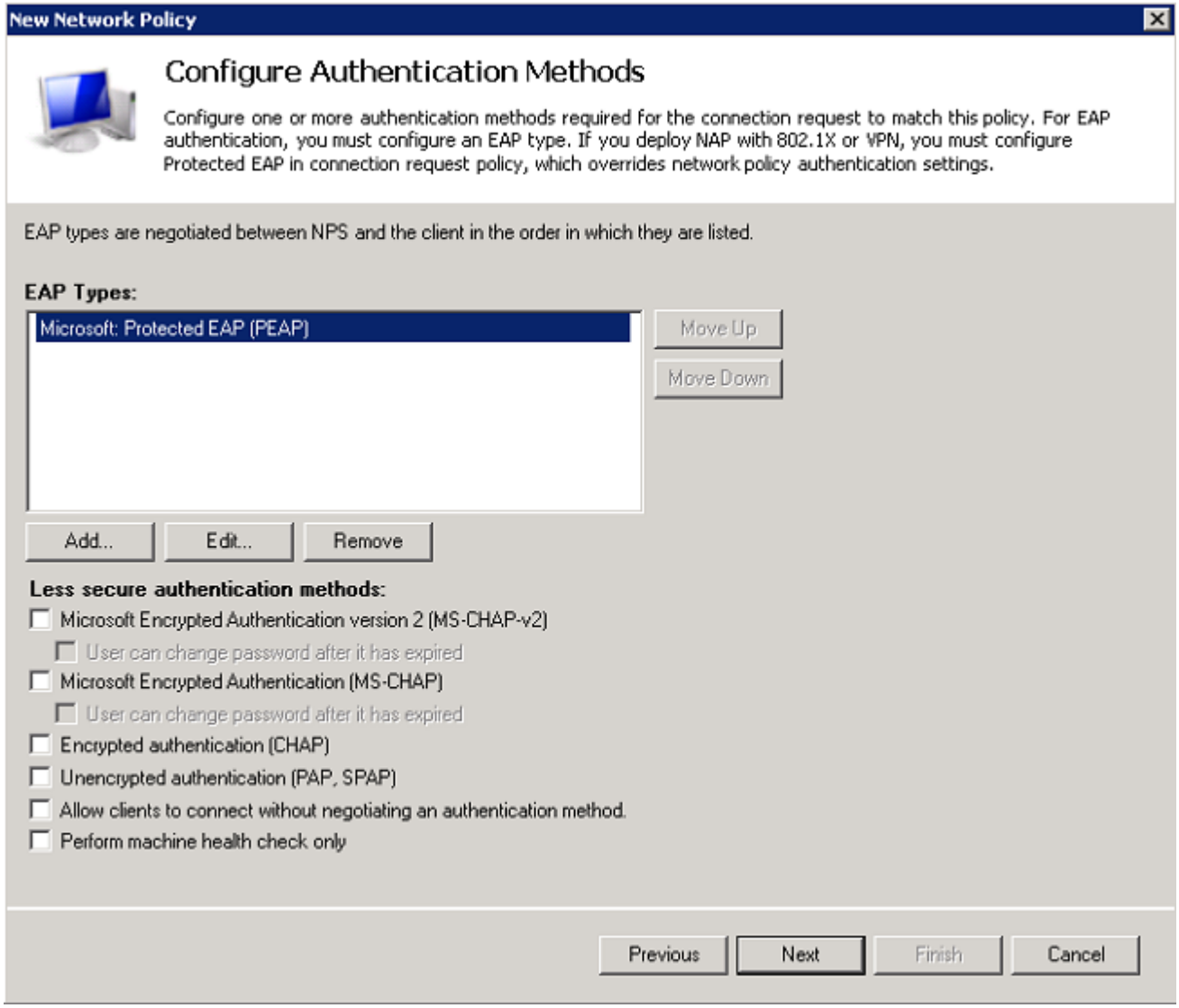
14. Fare clic su Add, selezionare PEAP e fare clic su OK per abilitare PEAP.



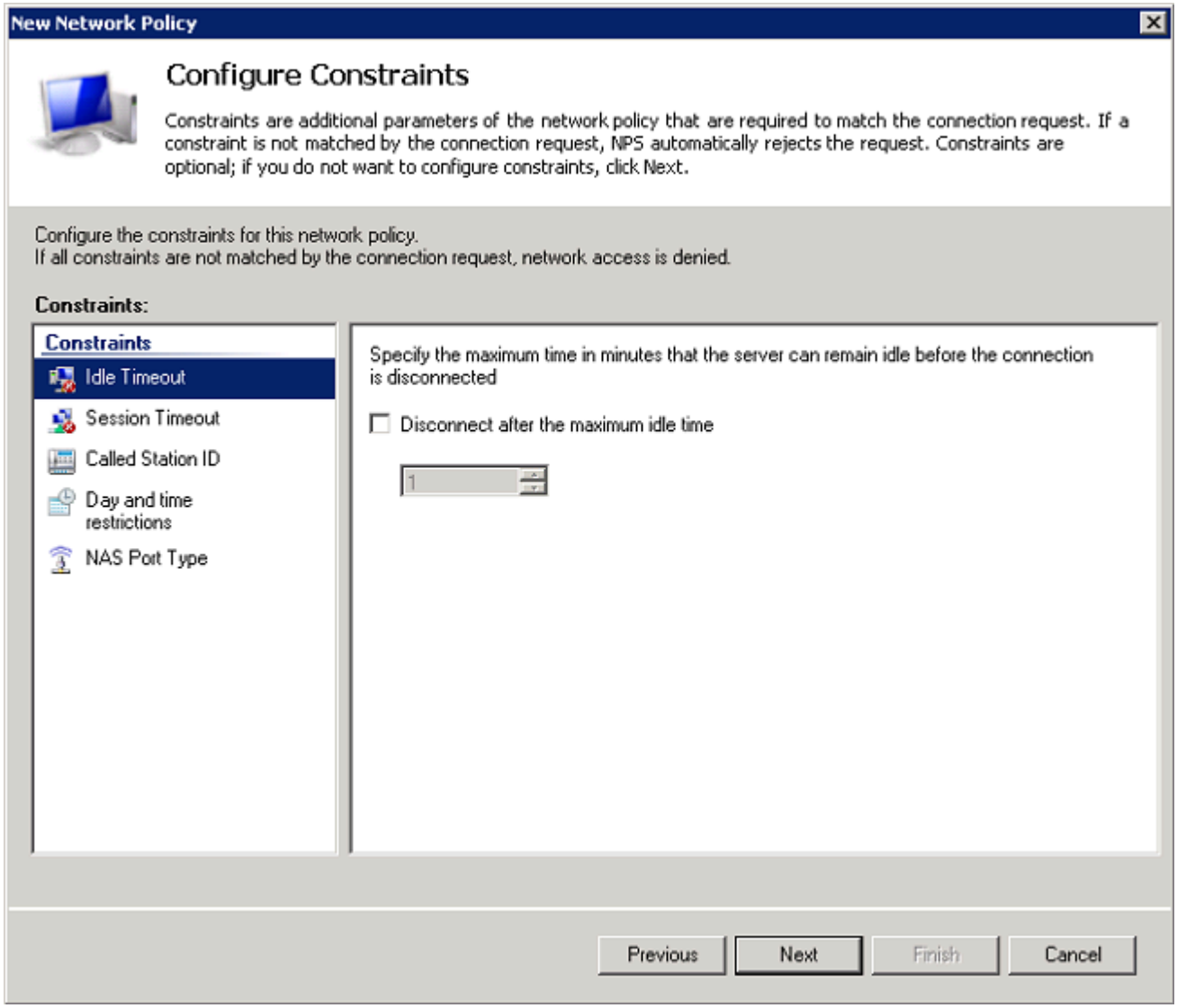
15. Selezionare Microsoft: PEAP (Protected EAP), quindi fare clic su Modifica. Verificare che il certificato del controller di dominio creato in precedenza sia selezionato nell'elenco a discesa Certificato emesso e fare clic su OK.



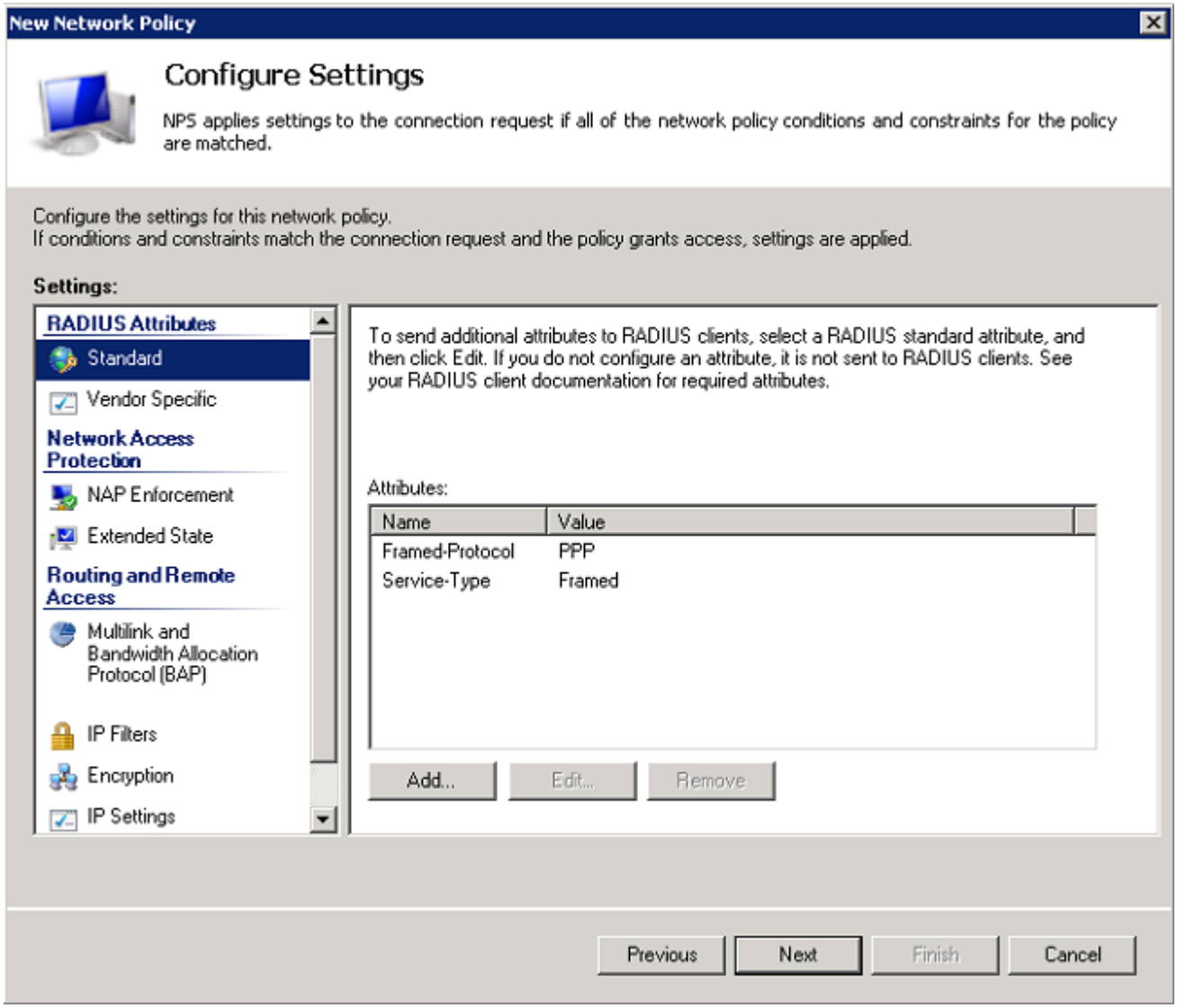
16. Fare clic su Next (Avanti).



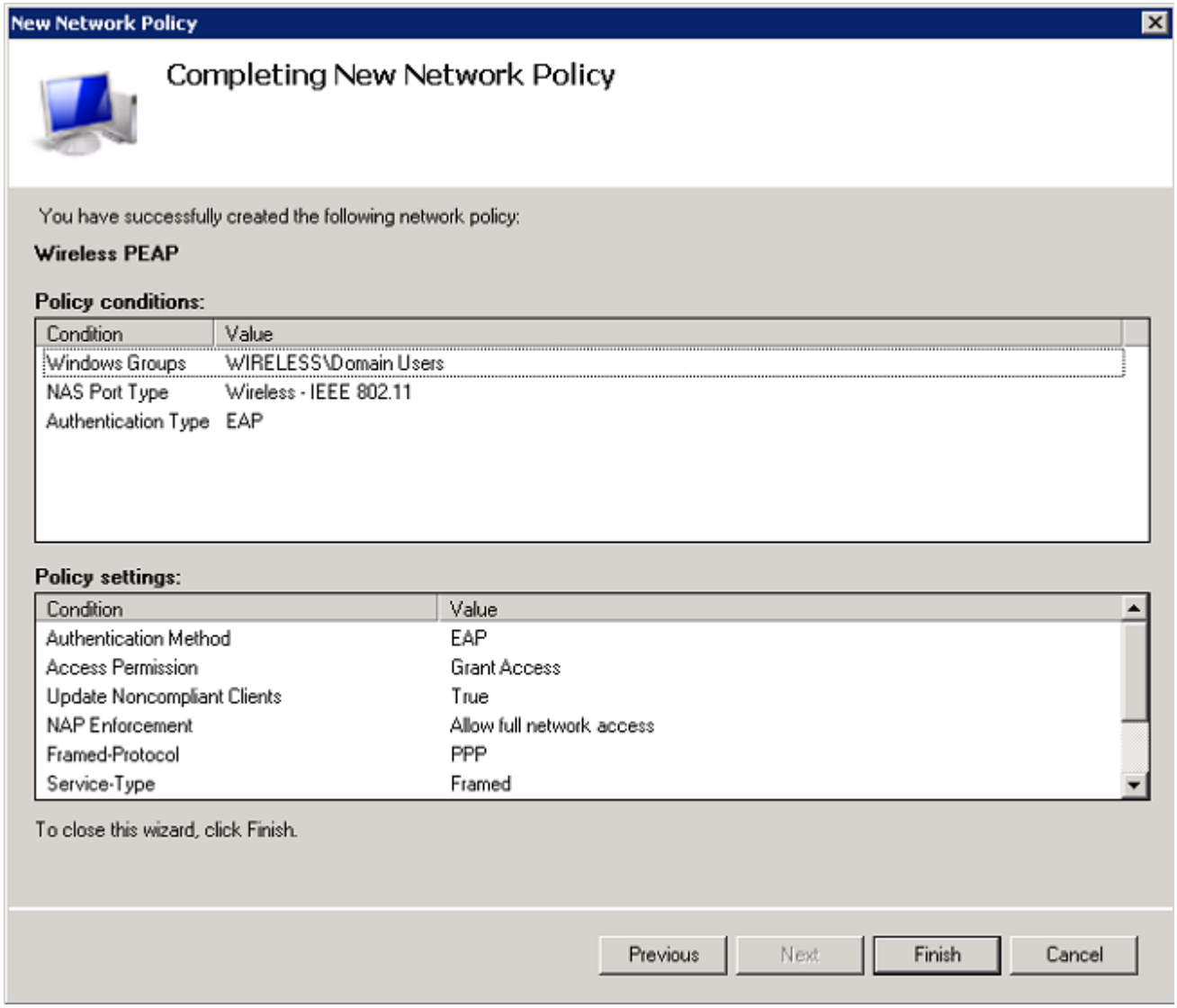
17. Fare clic su Next (Avanti).



18. Fare clic su Next (Avanti).



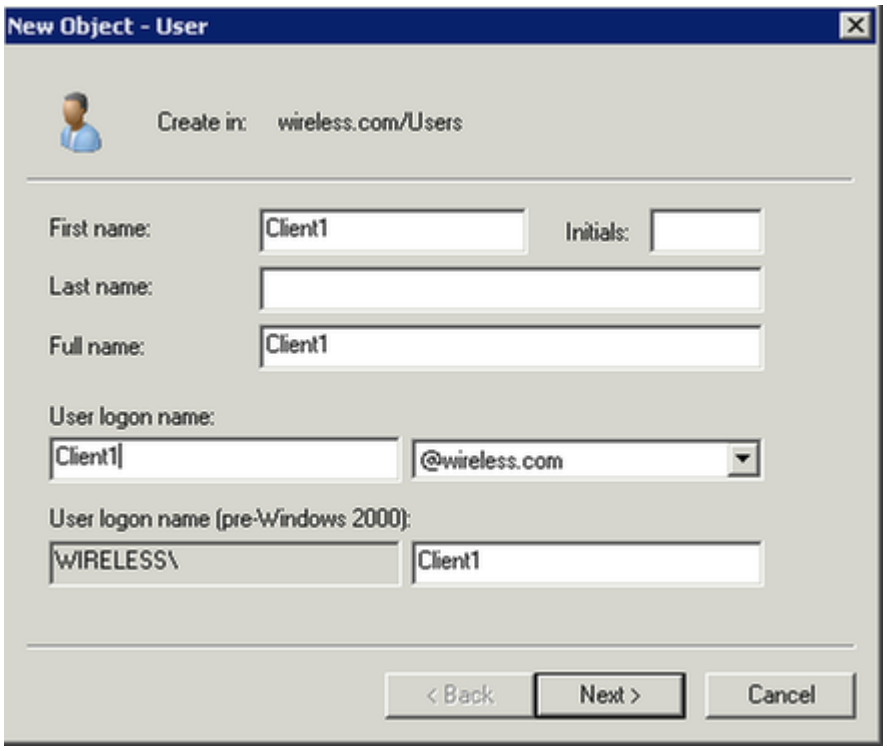
19. Fare clic su Finish (Fine).



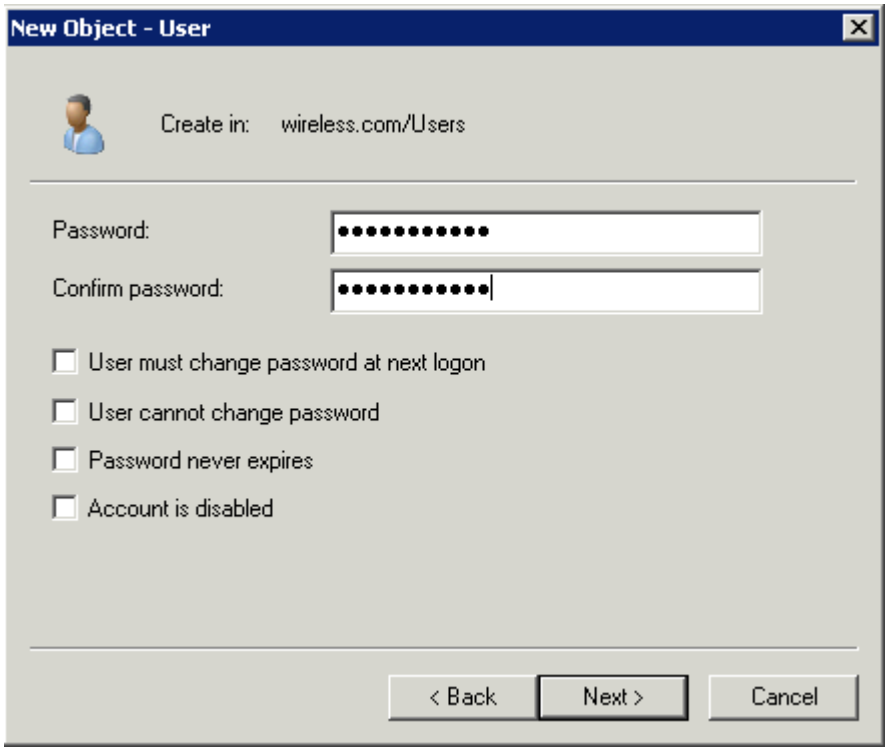
Aggiungi utenti ad Active Directory

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.

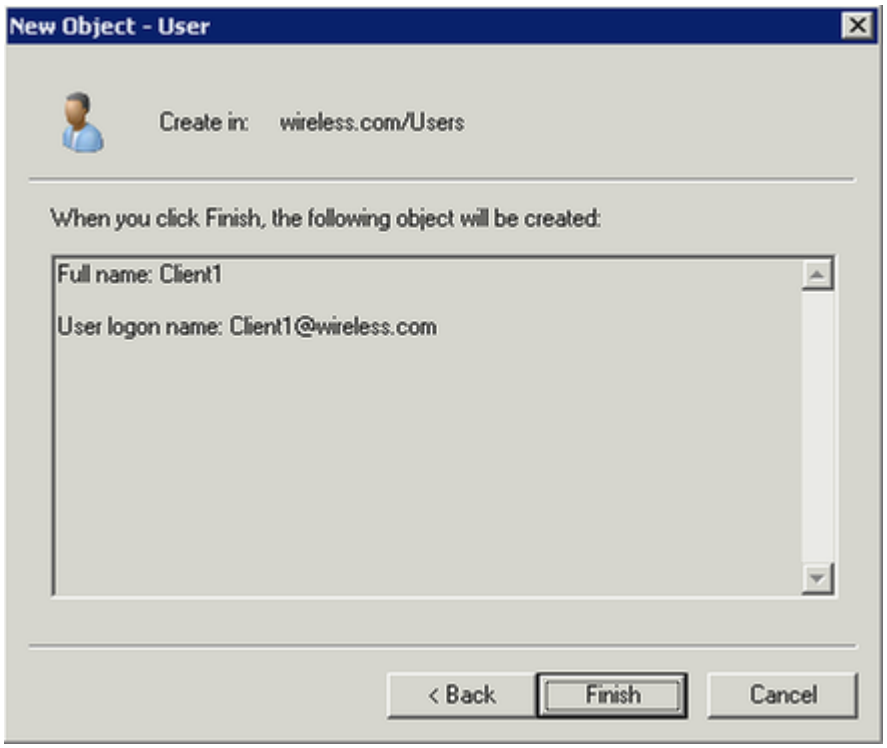
1. Aprire Utenti e computer di Active Directory. Fare clic su Start> Strumenti di amministrazione> Utenti e computer di Active Directory.
2. Nell'albero della console Utenti e computer di Active Directory espandere il dominio, fare clic con il pulsante destro del mouse su Utenti> Nuovo e scegliere Utente.
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).



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.



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

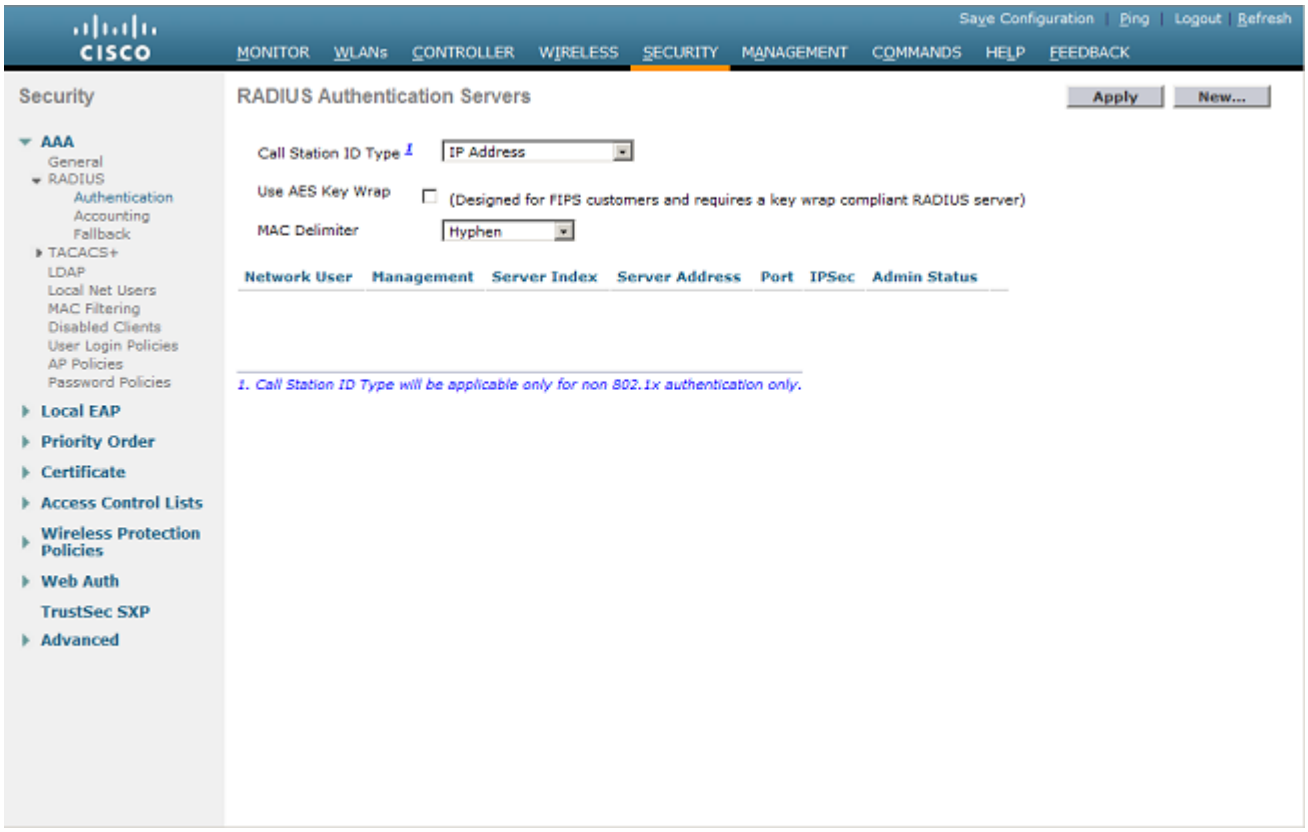
Configurare le periferiche wireless (i Wireless LAN Controller e LAP) per questa installazione.

Configurazione del WLC per l'autenticazione RADIUS

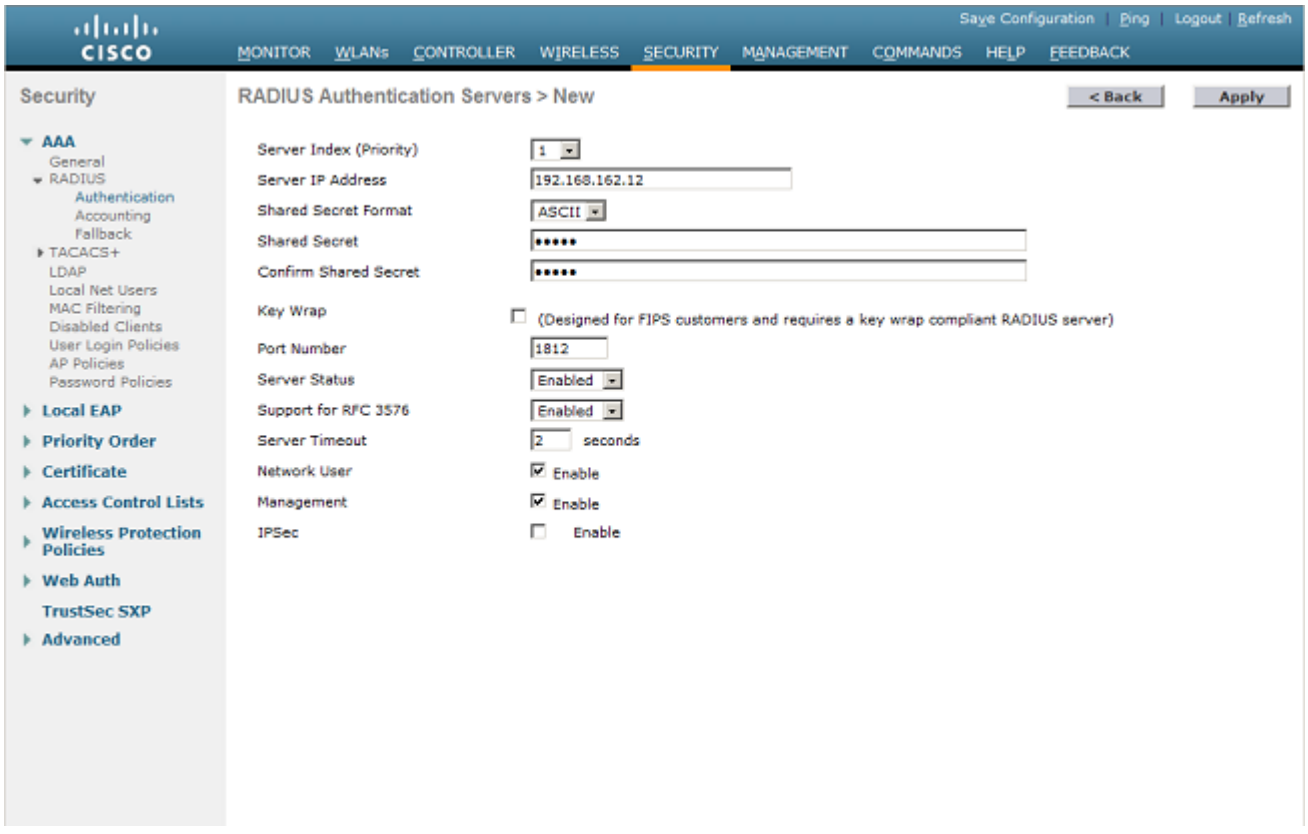
Configurare il WLC in modo che utilizzi Server dei criteri di rete come server di autenticazione. Per inoltrare le credenziali dell'utente a un server RADIUS esterno, è necessario configurare il WLC. Il server RADIUS esterno convalida quindi le credenziali dell'utente e fornisce l'accesso ai client wireless.

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).



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.



Configurazione di una WLAN per i client

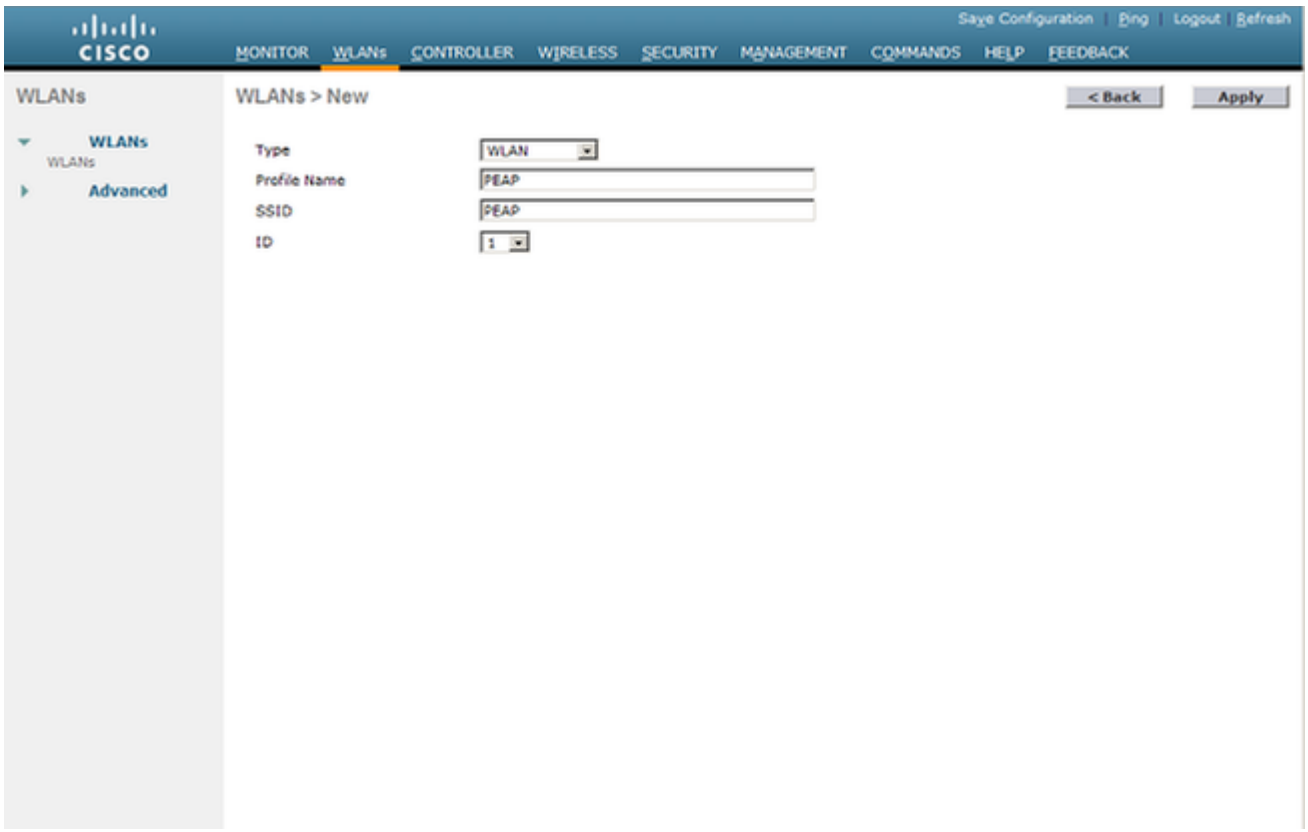
Configurare l'identificatore del set di servizi (SSID) (WLAN) a cui si connettono i client wireless. In questo esempio, creare il SSID e denominarlo PEAP.

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.

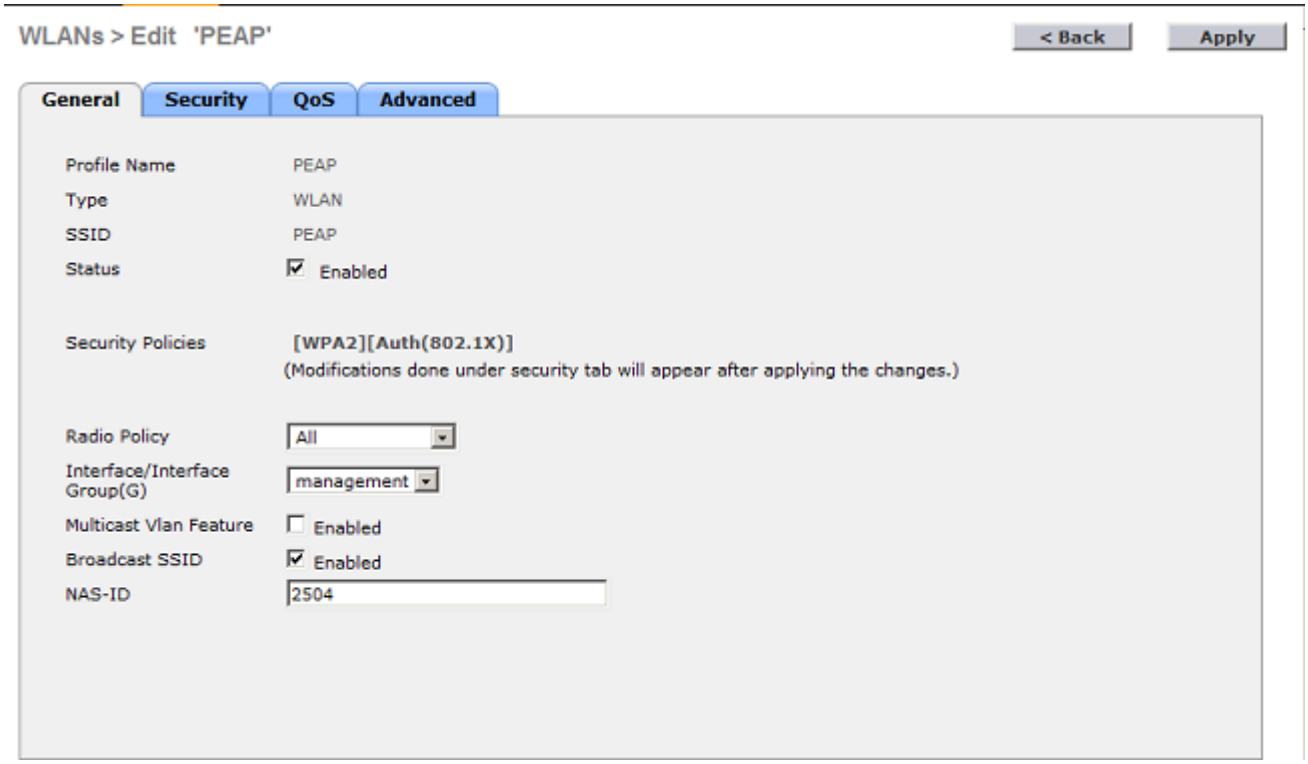
Nota: In questo documento la WLAN è associata alle interfacce di gestione. Se la rete contiene più VLAN, è possibile creare una VLAN separata e associarla all'SSID. Per informazioni su come configurare le VLAN sui WLC, fare riferimento all'esempio di configurazione delle VLAN sui controller LAN wireless.

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

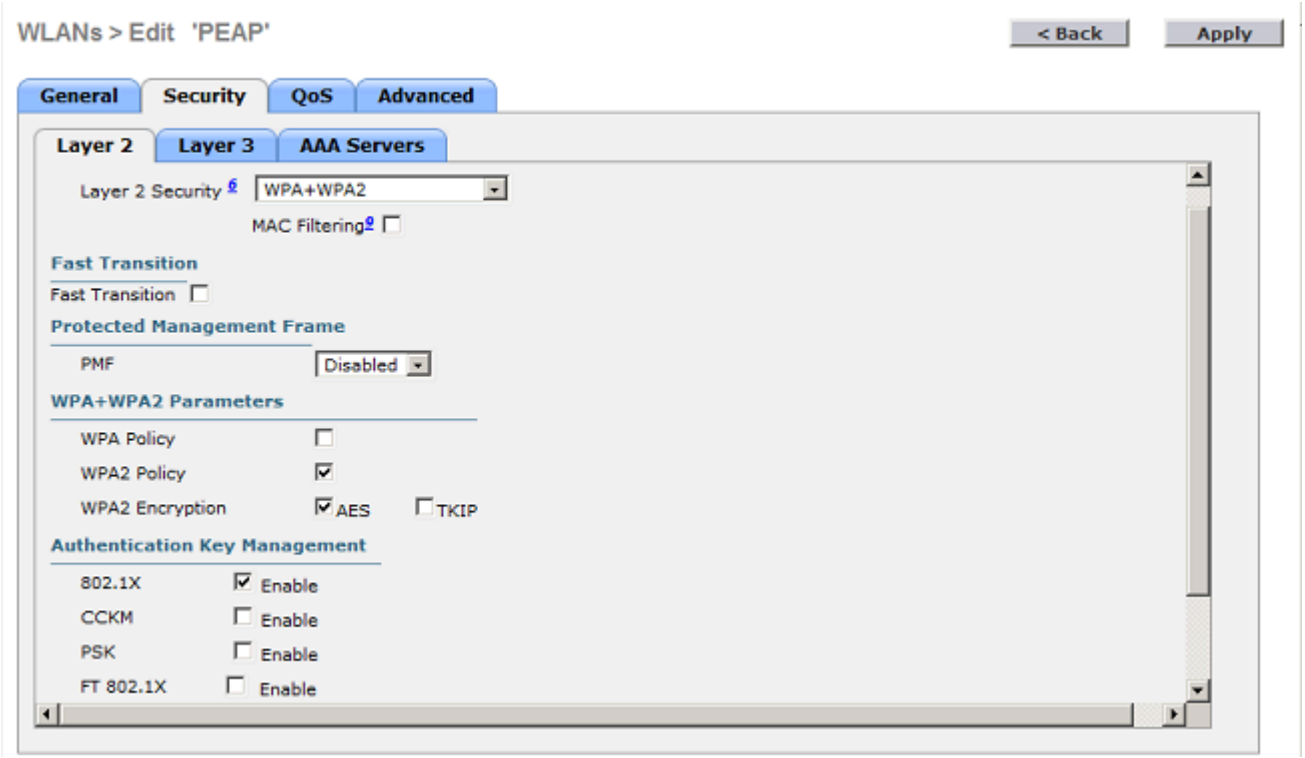
1. Per visualizzare la pagina WLAN, fare clic su WLAN dall'interfaccia del controller. In questa pagina vengono elencate le WLAN esistenti sul controller.
2. Per creare una nuova WLAN, selezionare New (Nuovo). Immettere l'ID WLAN e l'SSID WLAN per la WLAN, quindi fare clic su Applica.



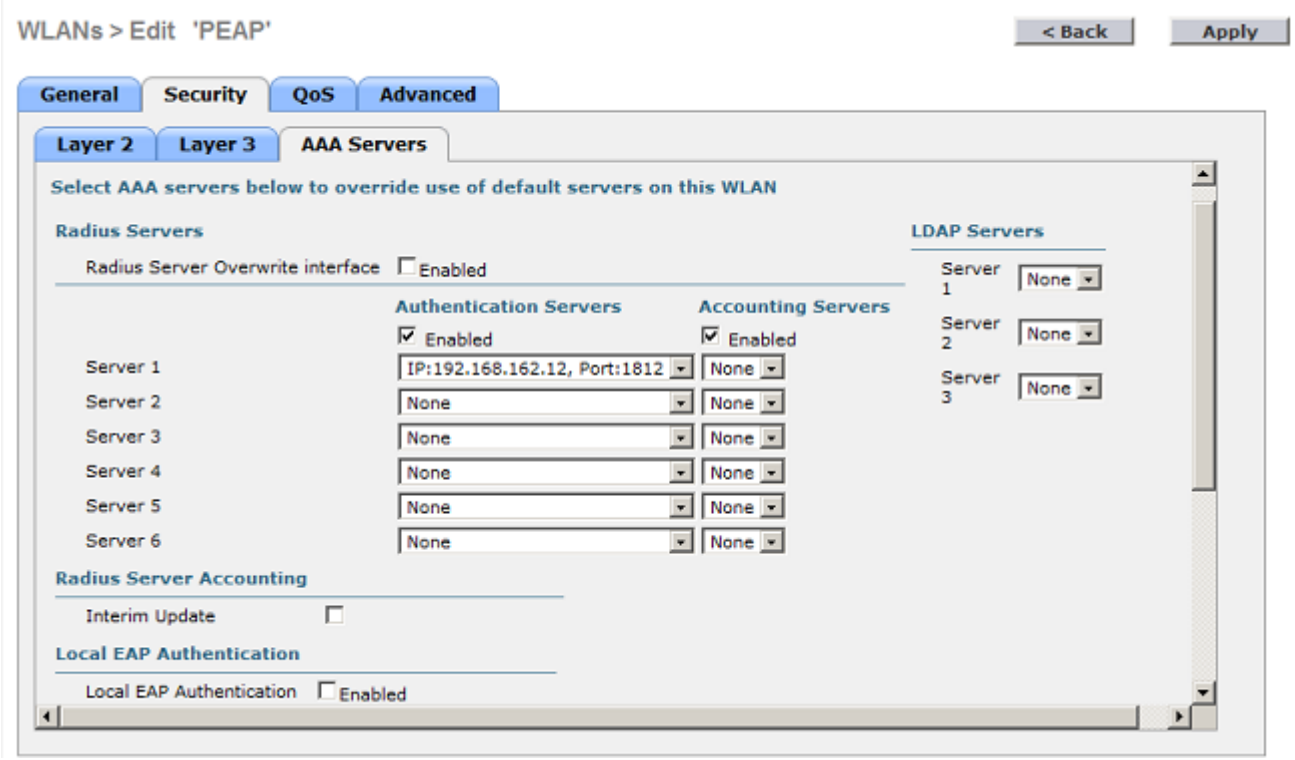
3. Per configurare l'SSID per 802.1x, attenersi alla seguente procedura:
    1. Fare clic sulla scheda General (Generale) e abilitare la WLAN.



2. 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.



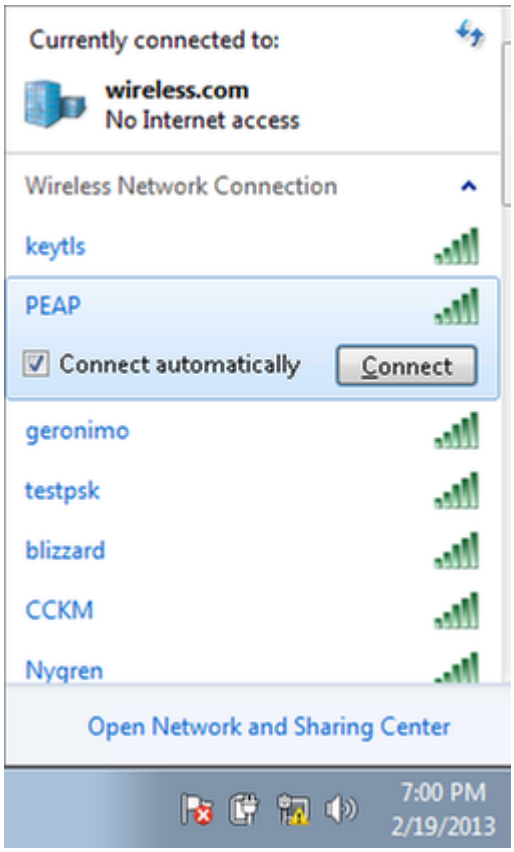
3. Fare clic sulla scheda Sicurezza > Server AAA, scegliere l'indirizzo IP del Server dei criteri di rete dall'elenco a discesa Server 1 e fare clic su Applica.



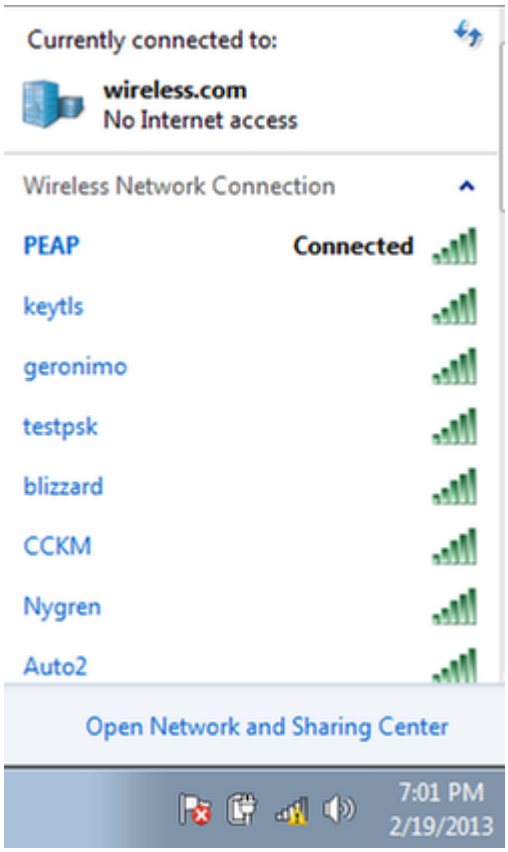
Configurazione dei client wireless per l'autenticazione PEAP-MS-CHAP v2

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

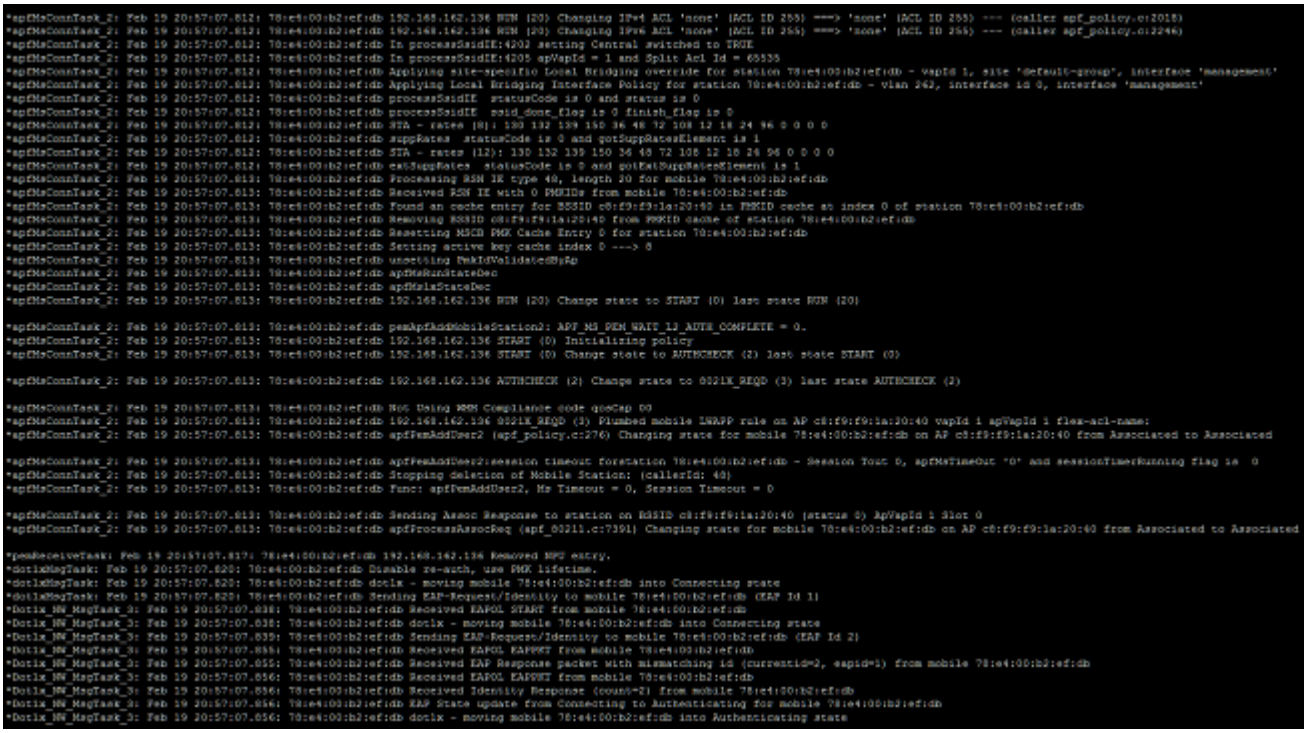
Attualmente non è disponibile una procedura di verifica per questa configurazione.

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:



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 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)
```

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

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.

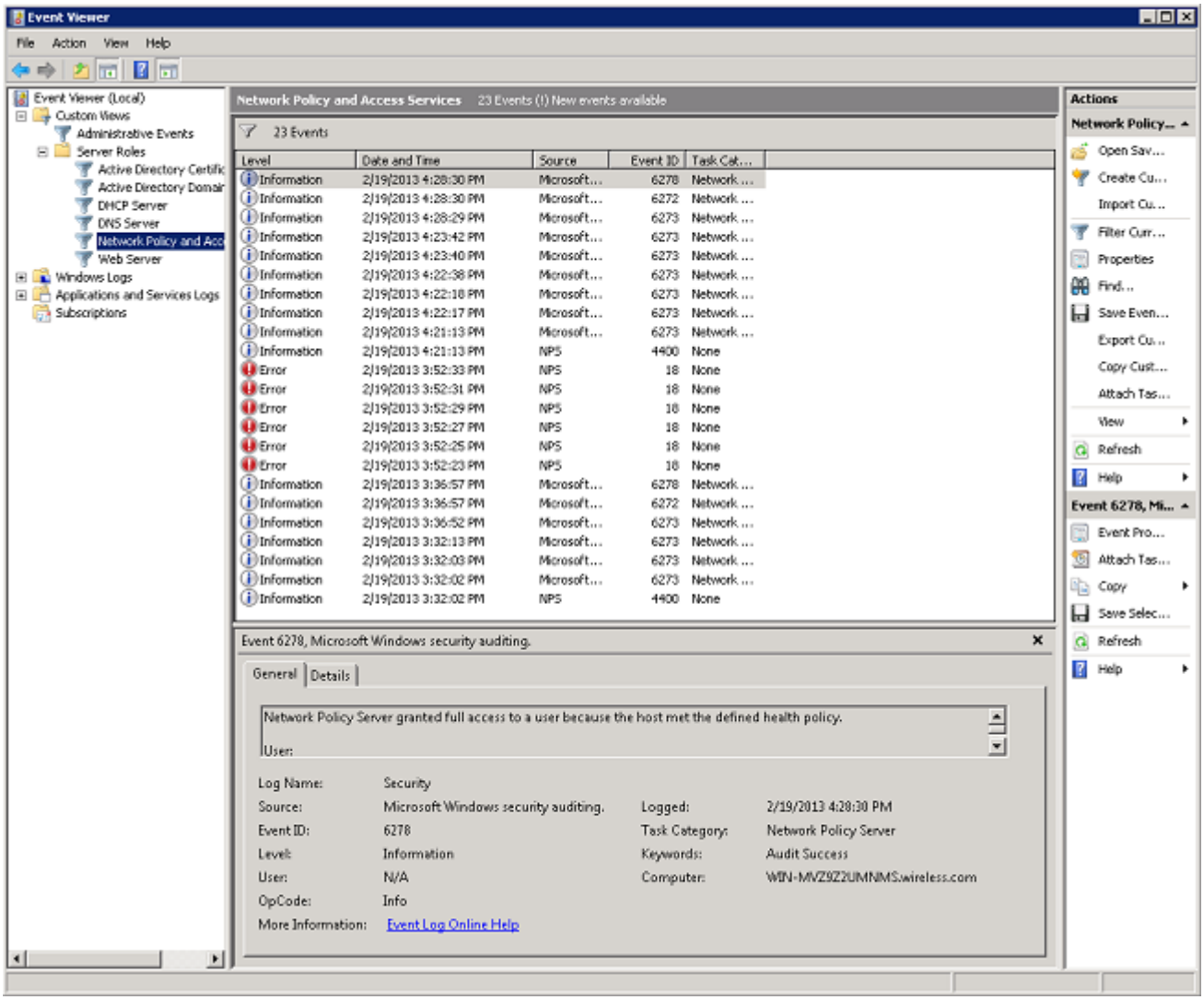
Nota: TAC non fornisce supporto tecnico per server RADIUS di terze parti; tuttavia, i registri sul server RADIUS spiegano in genere il motivo per cui una richiesta client è stata

---

rifiutata o ignorata.

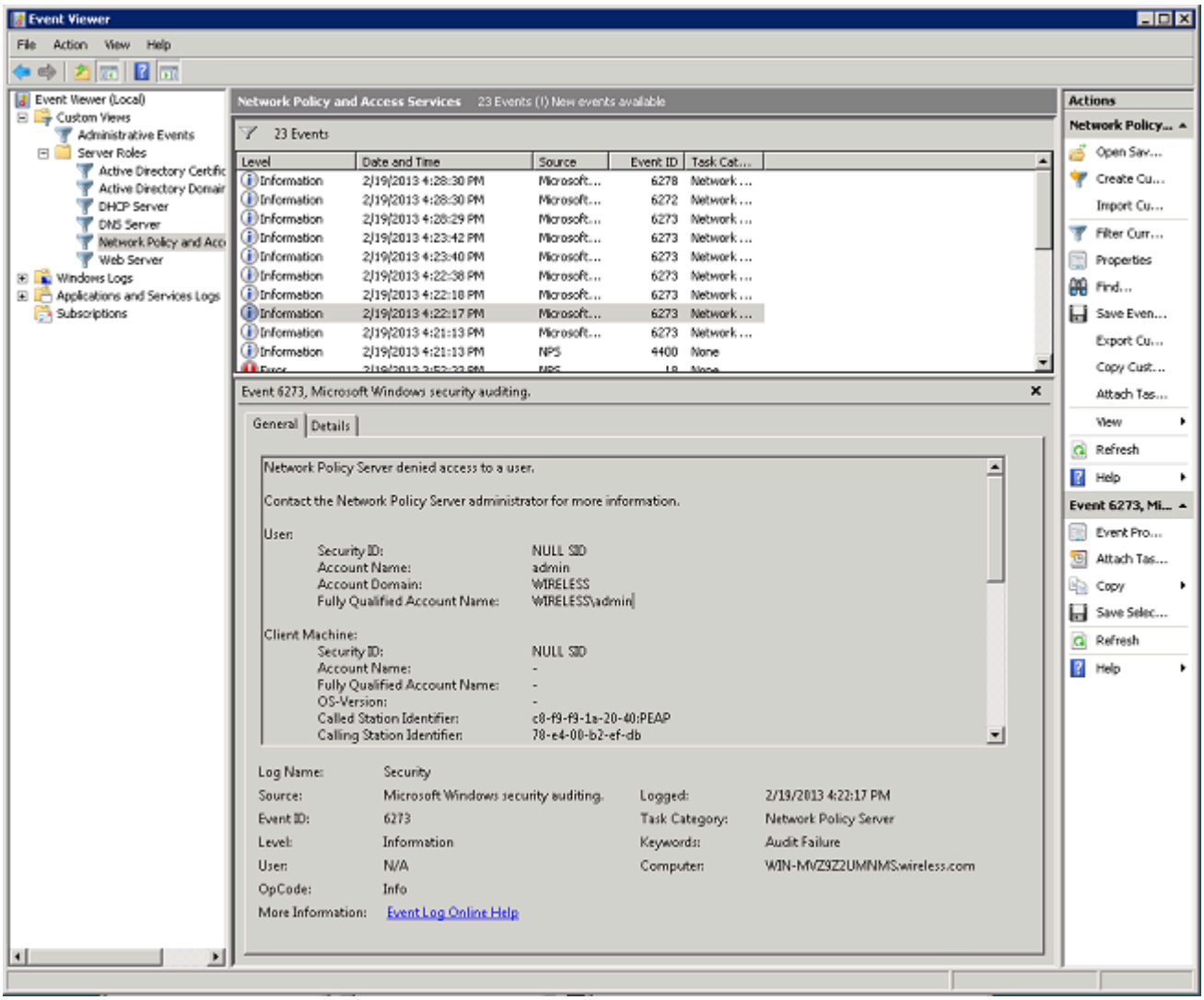
Per risolvere i problemi relativi ai rifiuti di accesso e ai timeout di risposta da Server dei criteri di rete, esaminare i registri di Server dei criteri di rete nel Visualizzatore eventi di Windows sul server.

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:

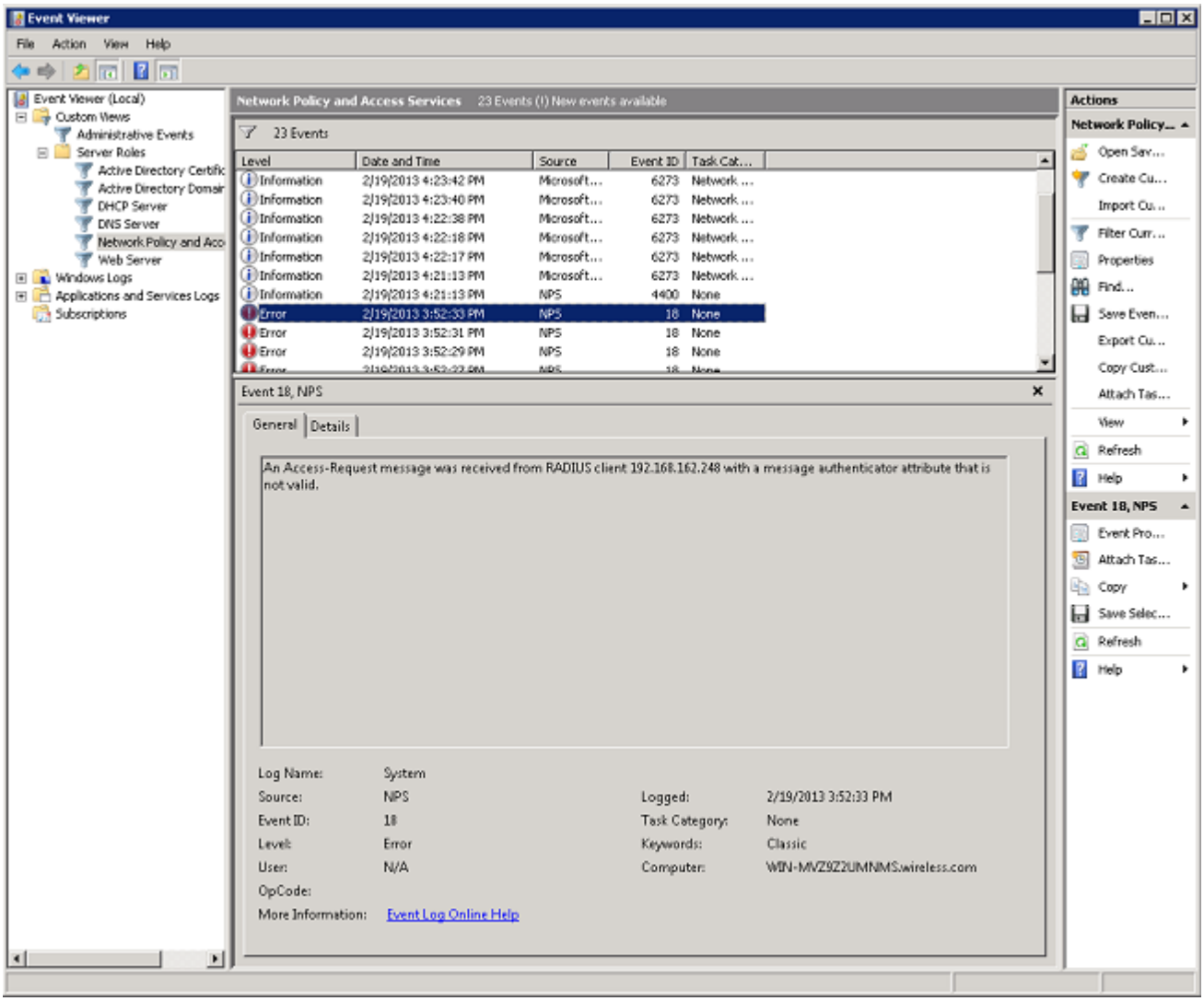


Quando si esamina un'istruzione di rifiuto nel Visualizzatore eventi, esaminare la sezione Dettagli autenticazione. In questo esempio è possibile notare che il Server dei criteri di rete ha negato l'accesso all'utente a causa di un nome utente non corretto:

```
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).