

PEAP in Unified Wireless Networks con Microsoft Internet Authentication Service (IAS)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Panoramica di PEAP](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione di Microsoft Windows 2003 Server](#)

[Configurazione di Microsoft Windows 2003 Server](#)

[Installare e configurare i servizi DHCP in Microsoft Windows 2003 Server](#)

[Installare e configurare il server Microsoft Windows 2003 come server CA \(Certification Authority\)](#)

[Connetti client al dominio](#)

[Installare il servizio di autenticazione Internet nel server Microsoft Windows 2003 e richiedere un certificato](#)

[Configurare il servizio di autenticazione Internet per l'autenticazione PEAP-MS-CHAP v2](#)

[Aggiungi utenti ad Active Directory](#)

[Consenti accesso wireless agli utenti](#)

[Configurazione del controller LAN wireless e dei Lightweight Access Point](#)

[Configurare il WLC per l'autenticazione RADIUS tramite il server MS IAS RADIUS](#)

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

[Configurazione dei client wireless](#)

[Configurazione dei client wireless per l'autenticazione PEAP-MS CHAPv2](#)

[Verifica e risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene fornito un esempio di configurazione per configurare l'autenticazione PEAP (Protected Extensible Authentication Protocol) con MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) versione 2 in una rete wireless unificata Cisco con Microsoft Internet Authentication Service (IAS) come server RADIUS.

[Prerequisiti](#)

Requisiti

Si presume che il lettore abbia una conoscenza dell'installazione di base di Windows 2003 e dell'installazione del controller Cisco, in quanto in questo documento vengono illustrate solo le configurazioni specifiche per facilitare i test.

Nota: questo documento ha lo scopo di fornire ai lettori un esempio della configurazione richiesta sul server MS per l'autenticazione PEAP - MS CHAP. La configurazione del server Microsoft illustrata in questa sezione è stata testata in laboratorio e ha rilevato che funziona come previsto. In caso di problemi durante la configurazione del server Microsoft, contattare Microsoft per assistenza. Cisco TAC non supporta la configurazione del server Microsoft Windows.

Per informazioni sull'installazione iniziale e sulla configurazione dei Cisco serie 4400 Controller, fare riferimento alla [Guida introduttiva: Cisco serie 4400 Wireless LAN Controller](#).

Le guide all'installazione e alla configurazione di Microsoft Windows 2003 sono disponibili all'indirizzo [Installazione di Windows Server 2003 R2](#).

Prima di iniziare, installare il sistema operativo Microsoft Windows Server 2003 con SP1 in ognuno dei server del laboratorio di prova e aggiornare tutti i Service Pack. Installare i controller e i Lightweight Access Point (LAP) e verificare che siano configurati gli ultimi aggiornamenti software.

Componenti usati

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

- Cisco serie 4400 Controller con firmware versione 4.0
- Cisco 1131 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise Server (SP1) con i servizi Internet Authentication Service (IAS), Certificate Authority (CA), DHCP e Domain Name System (DNS) installati
- Windows XP Professional con SP 2 (e Service Pack aggiornati) e Cisco Aironet 802.11a/b/g Wireless Network Interface Card (NIC)
- Aironet Desktop Utility versione 4.0
- Cisco 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](#).

Panoramica di PEAP

PEAP utilizza Transport Level Security (TLS) per creare un canale crittografato tra un client PEAP di autenticazione, ad esempio un laptop Wireless, e un autenticatore PEAP, ad esempio Microsoft

Internet Authentication Service (IAS) o qualsiasi server RADIUS. PEAP non specifica un metodo di autenticazione, ma fornisce una protezione aggiuntiva per altri protocolli di autenticazione EAP, ad esempio EAP-MSCHAPv2, che possono funzionare tramite il canale crittografato TLS fornito da PEAP. Il processo di autenticazione PEAP è costituito da due fasi principali:

PEAP fase uno: 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 (LAP). Una volta stabilita 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 il server IAS, la sessione TLS viene negoziata tra di essi. La chiave derivata in questa negoziazione viene utilizzata per crittografare tutte le comunicazioni successive.

PEAP fase due: comunicazione autenticata da 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 IAS 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 WLC e il LAP non possono decrittografare questi messaggi perché non è l'endpoint TLS.

Dopo che si è verificata la prima fase PEAP e il canale TLS è stato creato tra il server IAS e il client wireless 802.1X, per un tentativo di autenticazione riuscito in cui l'utente ha fornito credenziali basate su password valide con PEAP-MS-CHAP v2, la sequenza di messaggi RADIUS è la seguente:

1. Il server IAS invia un messaggio di richiesta di identità al client: EAP-Request/Identity.
2. Il client risponde con un messaggio di risposta di identità: Risposta EAP/Identità.
3. Il server IAS invia un messaggio di richiesta MS-CHAP v2: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (verifica).
4. Il client risponde con una richiesta MS-CHAP v2 e una risposta: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
5. Il server IAS restituisce un pacchetto MS-CHAP v2 con esito positivo quando il server ha autenticato correttamente il client: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (esito positivo).
6. Il client risponde con un pacchetto MS-CHAP v2 che ha avuto esito positivo quando ha autenticato correttamente il server: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (operazione riuscita).
7. Il server IAS invia un messaggio EAP-TLV che indica la riuscita dell'autenticazione.
8. Il client risponde con un messaggio di stato EAP-TLV riuscito.
9. Il server completa l'autenticazione e invia un messaggio di operazione riuscita EAP utilizzando testo normale. Se le VLAN vengono distribuite per l'isolamento del client, gli attributi VLAN sono inclusi in questo messaggio.

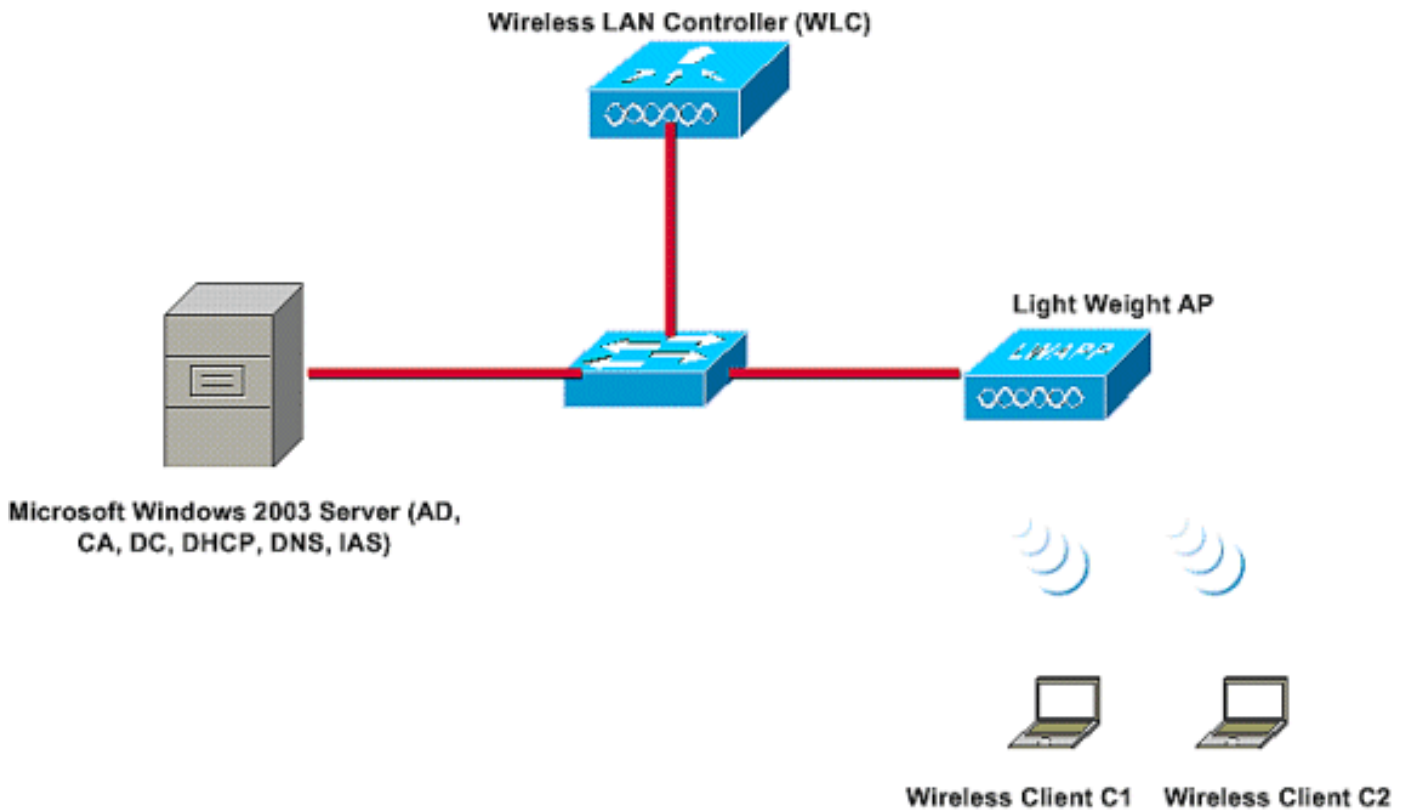
Configurazione

In questo documento viene illustrato un esempio di configurazione di PEAP MS-CHAP v2.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

[Esempio di rete](#)

Nel documento viene usata questa impostazione di rete:



In questa configurazione, un server Microsoft Windows 2003 svolge i seguenti ruoli:

- Controller di dominio per il dominio **Wireless.com**
- Server DHCP/DNS
- Server CA (Certification Authority)
- Active Directory - per gestire il database utenti
- Servizio di autenticazione Internet (IAS) - per autenticare gli utenti wireless

Il server si connette alla rete cablata tramite uno switch di layer 2, come mostrato.

Il controller WLC (Wireless LAN Controller) e il LAP registrato si connettono anche alla rete tramite lo switch di layer 2.

I client wireless C1 e C2 utilizzeranno l'autenticazione Wi-Fi Protected Access 2 (WPA2) - PEAP MSCHAP v2 per connettersi alla rete wireless.

L'obiettivo è configurare il server Microsoft 2003, il controller LAN wireless e il punto di accesso Light Weight per autenticare i client wireless con l'autenticazione PEAP MSCHAP v2.

La sezione successiva spiega come configurare i dispositivi per questa installazione.

[Configurazioni](#)

In questa sezione viene esaminata la configurazione necessaria per configurare l'autenticazione PEAP MS-CHAP v2 nella WLAN:

- Configurazione di Microsoft Windows 2003 Server
- Configurare il controller WLC (Wireless LAN Controller) e i punti di accesso Light Weight
- Configurazione dei client wireless

Iniziare con la configurazione del server Microsoft Windows 2003.

[Configurazione di Microsoft Windows 2003 Server](#)

[Configurazione di Microsoft Windows 2003 Server](#)

Come indicato nella sezione Installazione di rete, utilizzare il server Microsoft Windows 2003 nella rete per eseguire queste funzioni.

- **Controller di dominio** - per il dominio **Wireless**
- **Server DHCP/DNS**
- **Server CA (Certification Authority)**
- **Servizio di autenticazione Internet (IAS, Internet Authentication Service)** - per autenticare gli utenti wireless
- **Active Directory** - per gestire il database utenti

Configurare il server Microsoft Windows 2003 per questi servizi. Iniziare con la configurazione del server Microsoft Windows 2003 come controller di dominio.

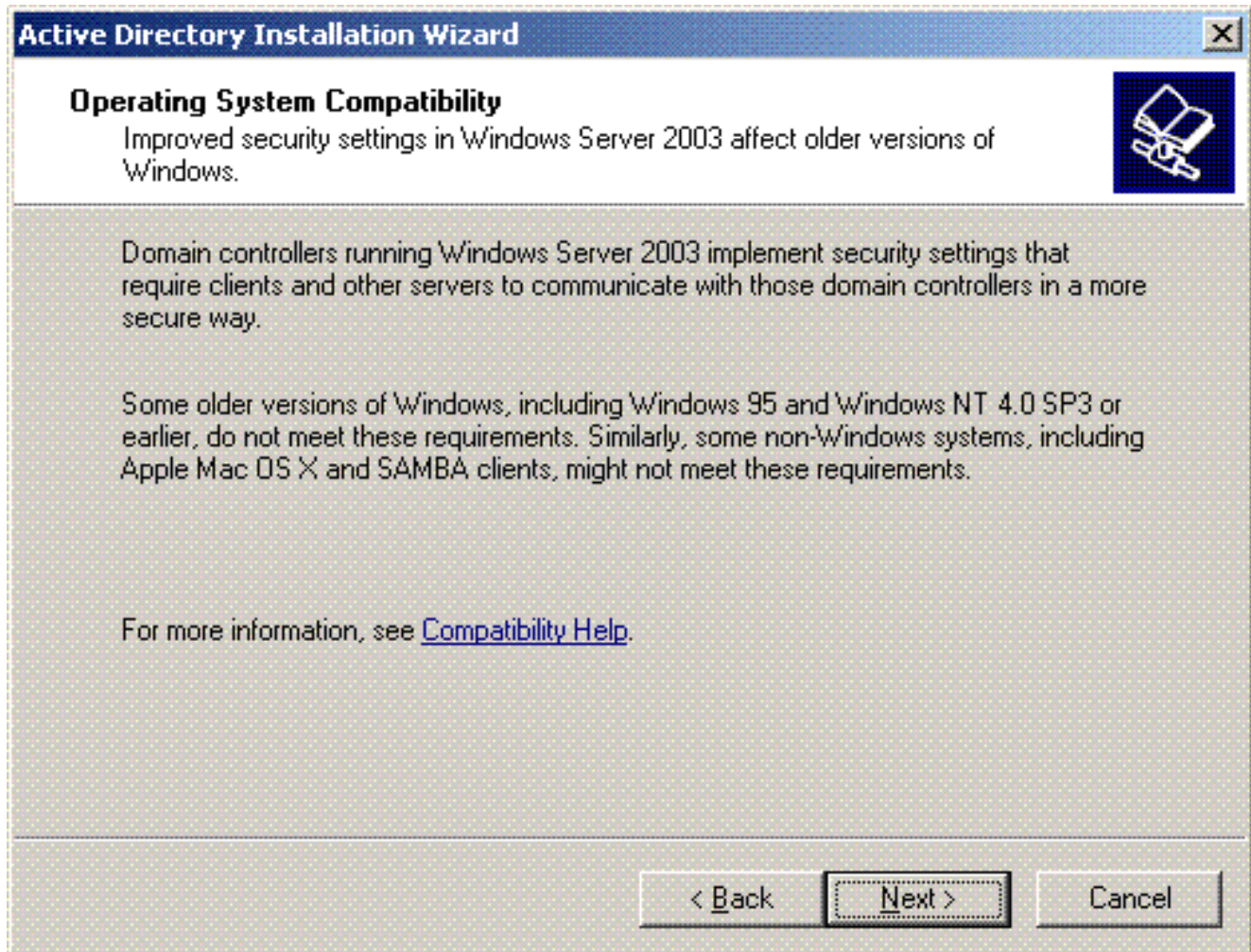
Configurare il server Microsoft Windows 2003 come controller di dominio

Per configurare il server Microsoft Windows 2003 come controller di dominio, attenersi alla seguente procedura:

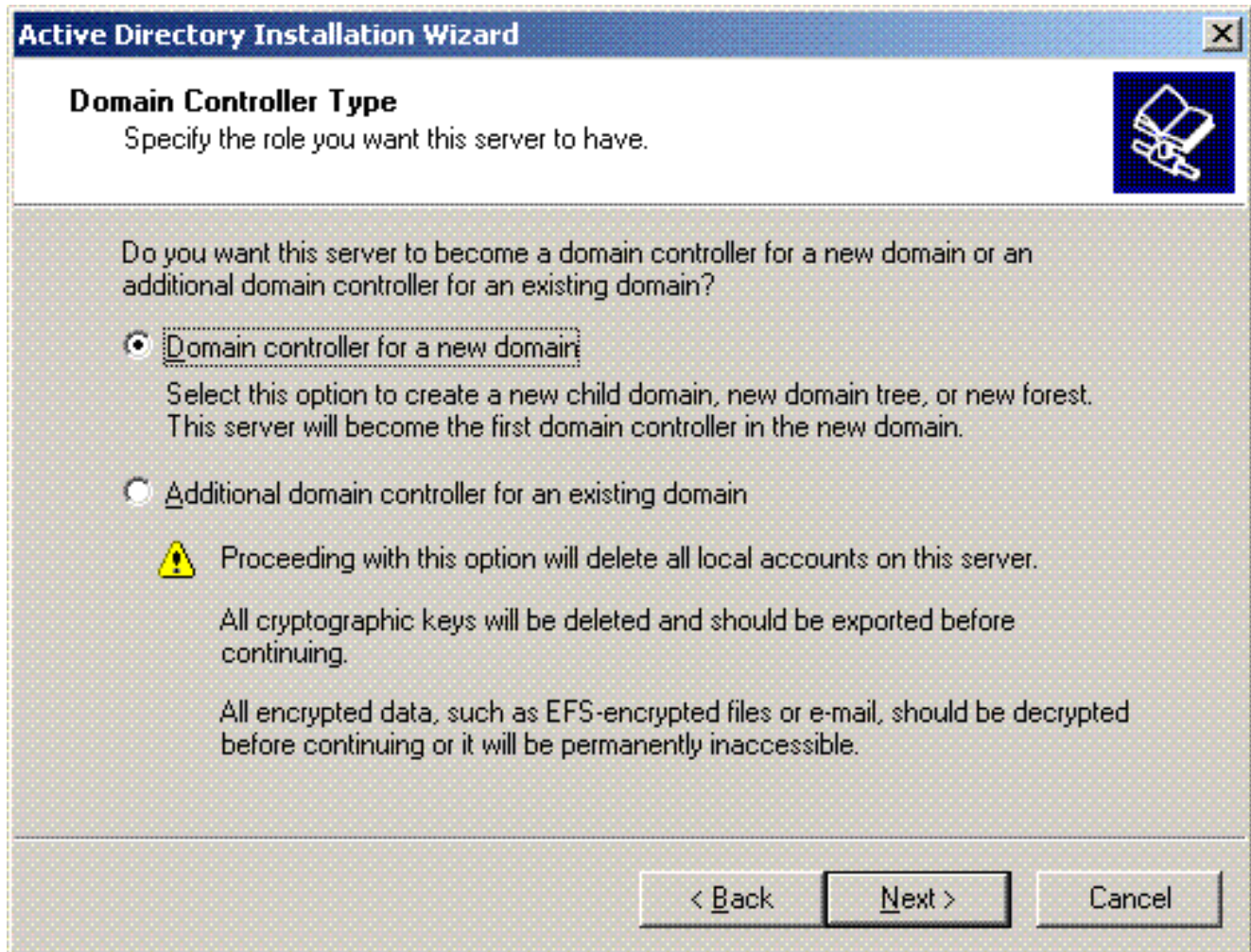
1. Fare clic sul pulsante **Start**, scegliere **Esegui**, digitare **dcpromo.exe** e quindi fare clic su **OK** per avviare l'Installazione guidata di Active Directory.



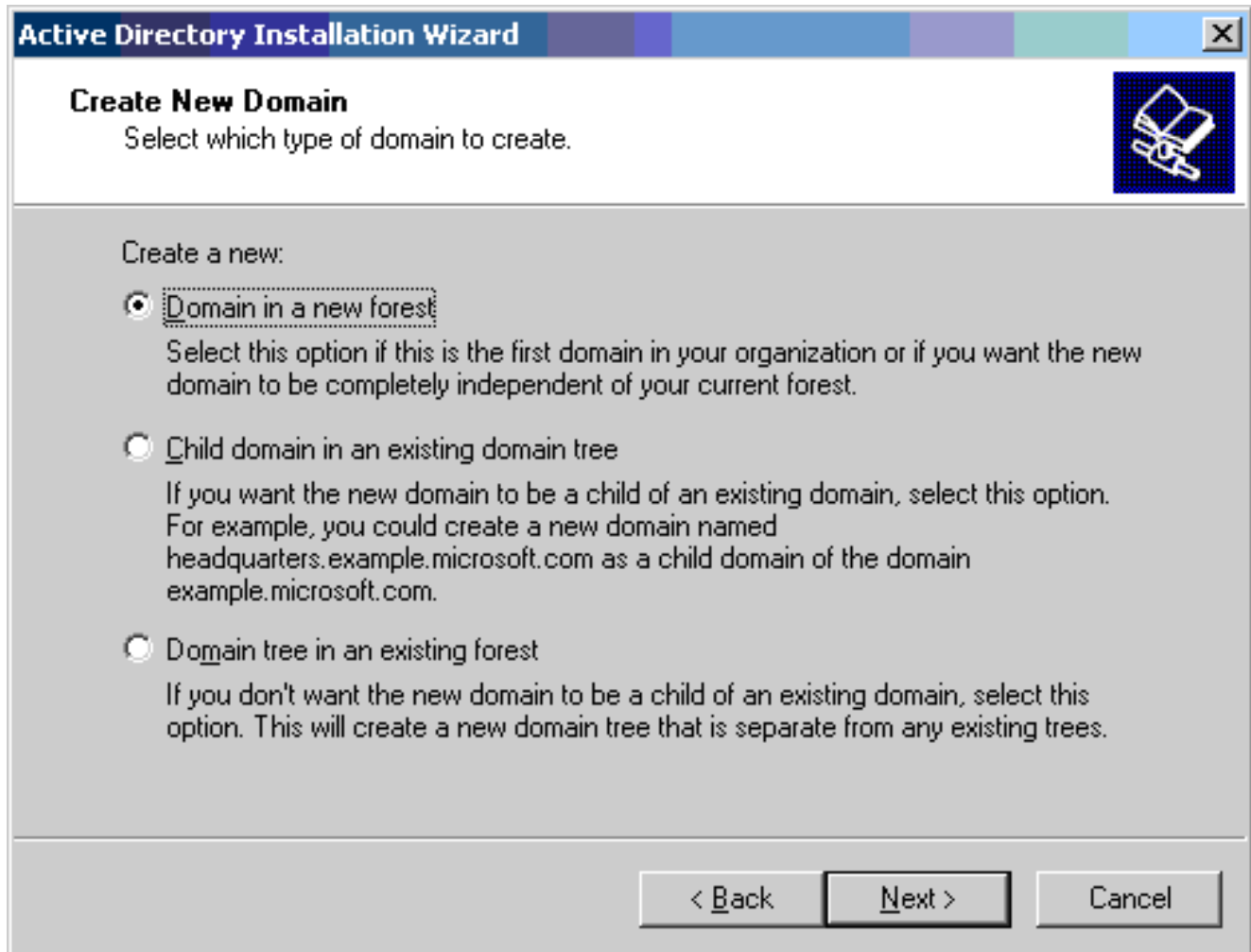
2. Fare clic su **Avanti** per eseguire l'installazione guidata Active Directory.



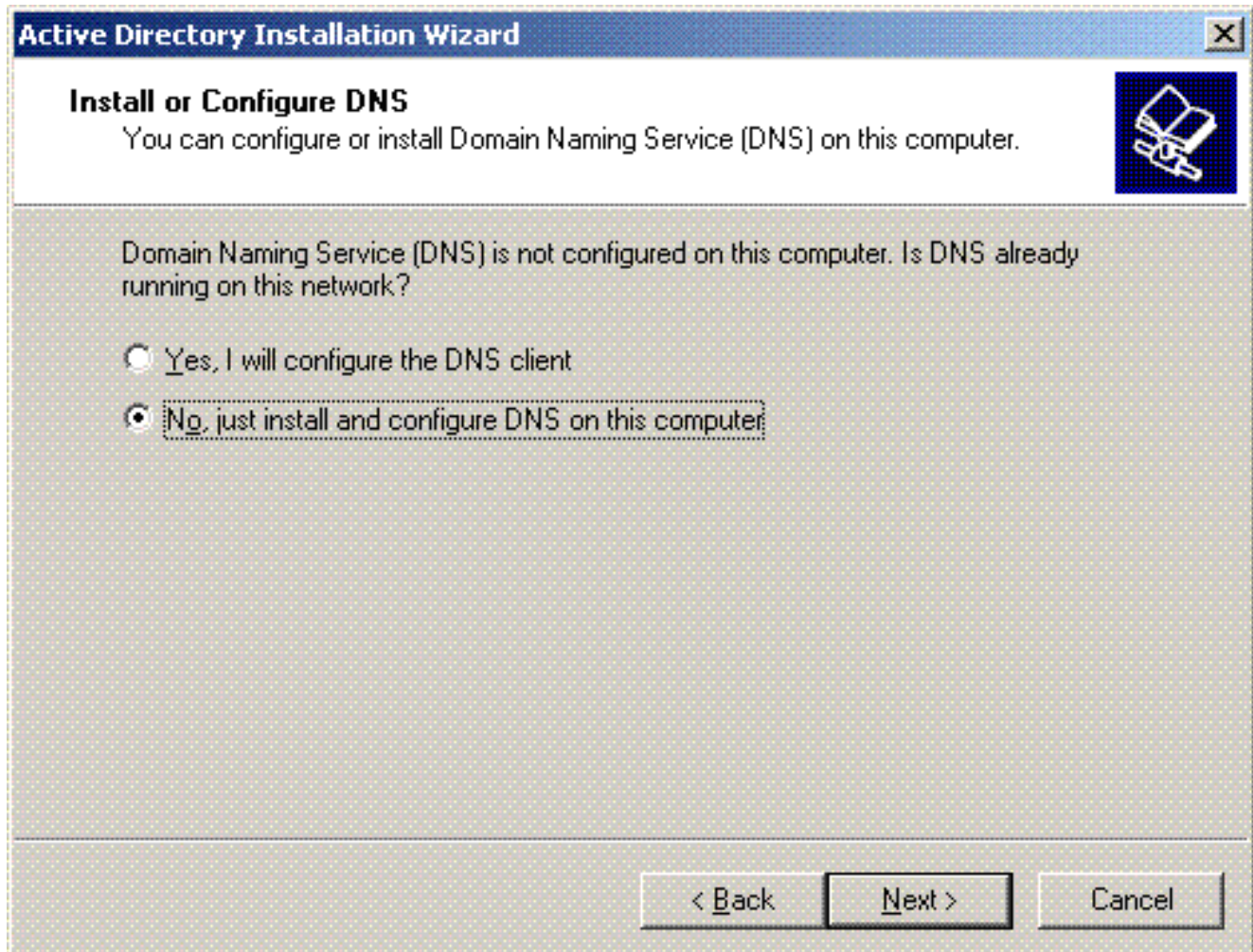
3. Per creare un nuovo dominio, scegliere l'opzione **Controller di dominio** per un nuovo dominio.



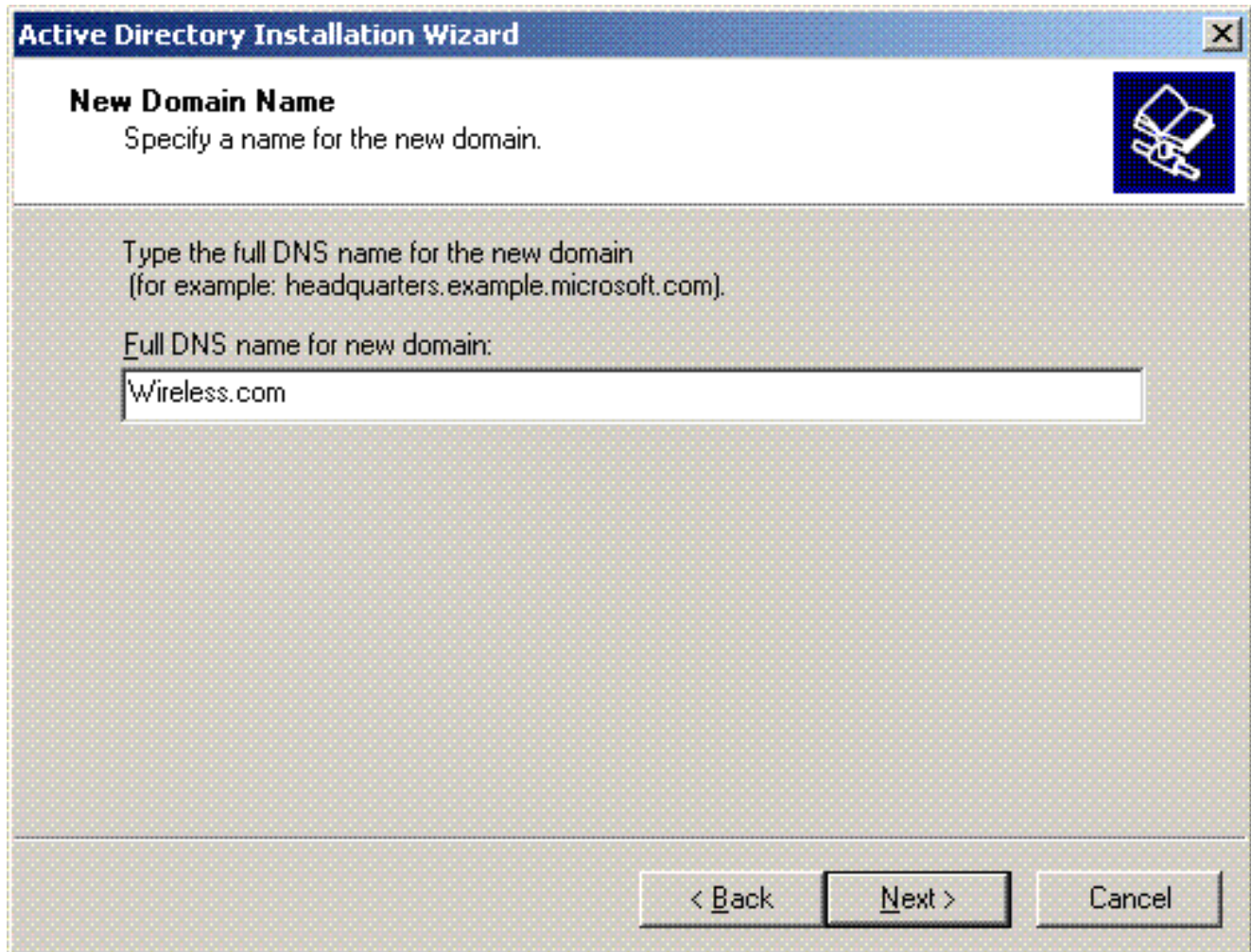
4. Fare clic su **Avanti** per creare una nuova foresta di alberi di dominio.



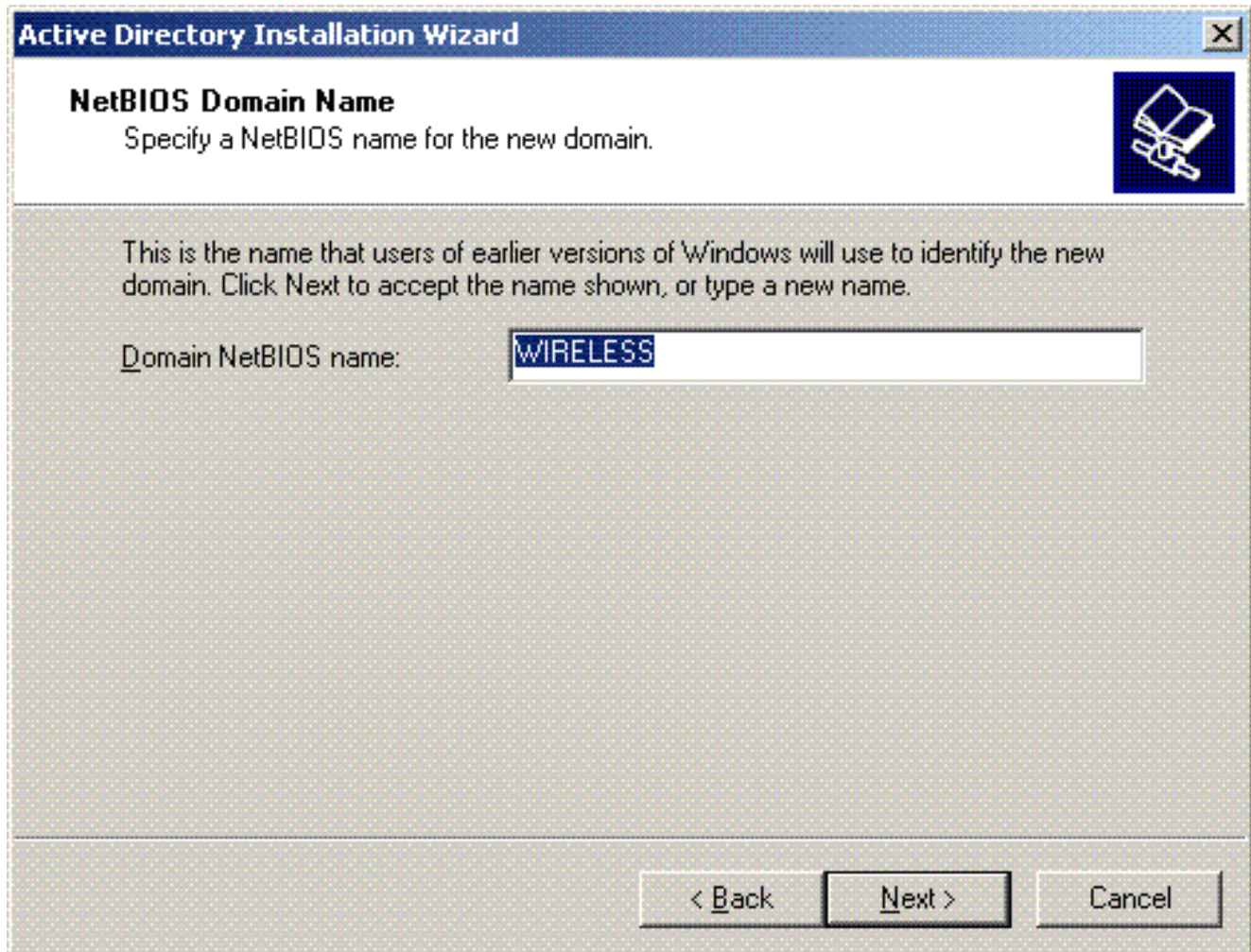
5. Se DNS non è installato nel sistema, la procedura guidata fornisce le opzioni per configurare DNS. Scegliere **No, Installa e configura DNS** nel computer. Fare clic su **Next** (Avanti).



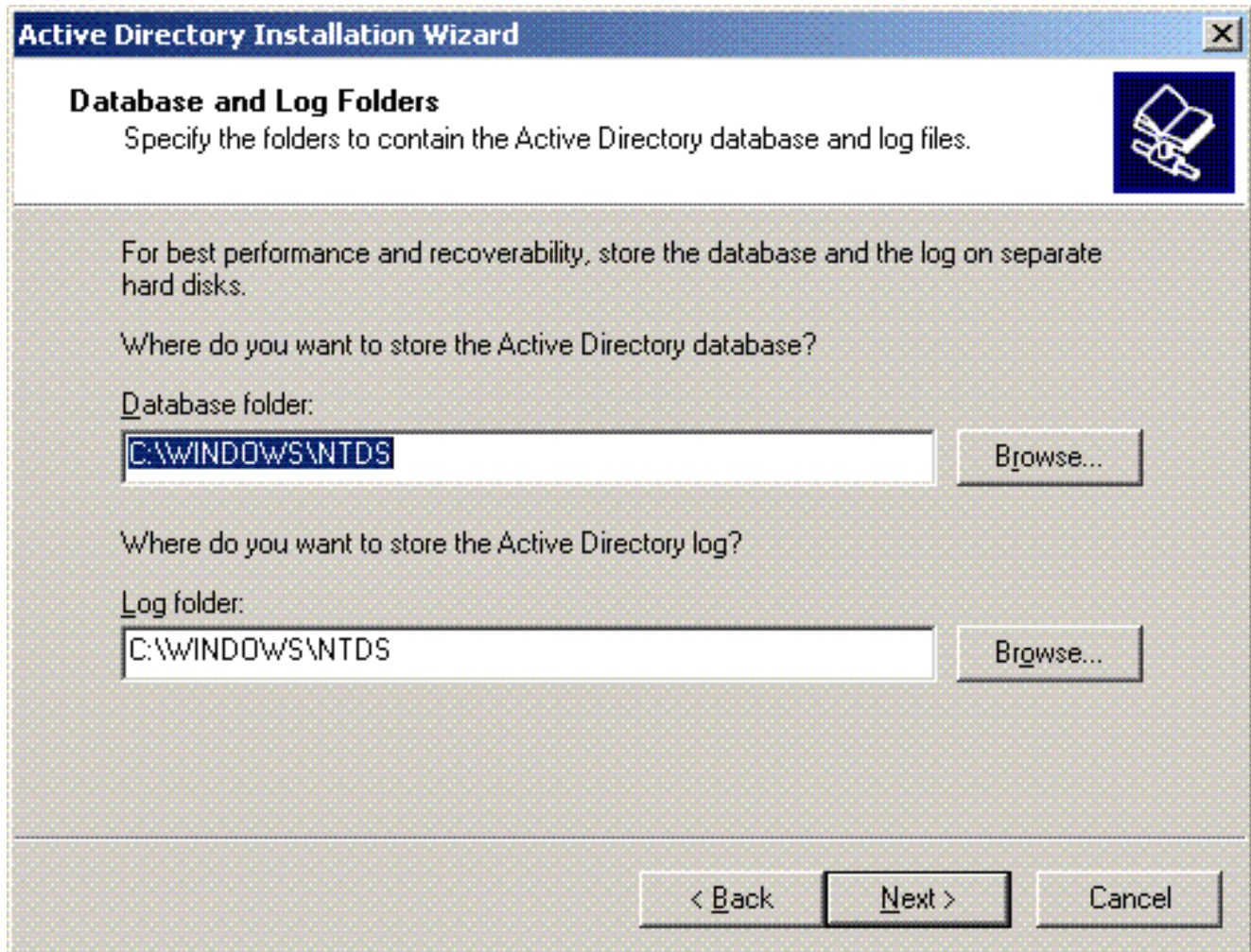
6. Digitare il nome DNS completo per il nuovo dominio. In questo esempio viene utilizzato **Wireless.com** e fare clic su **Avanti**.



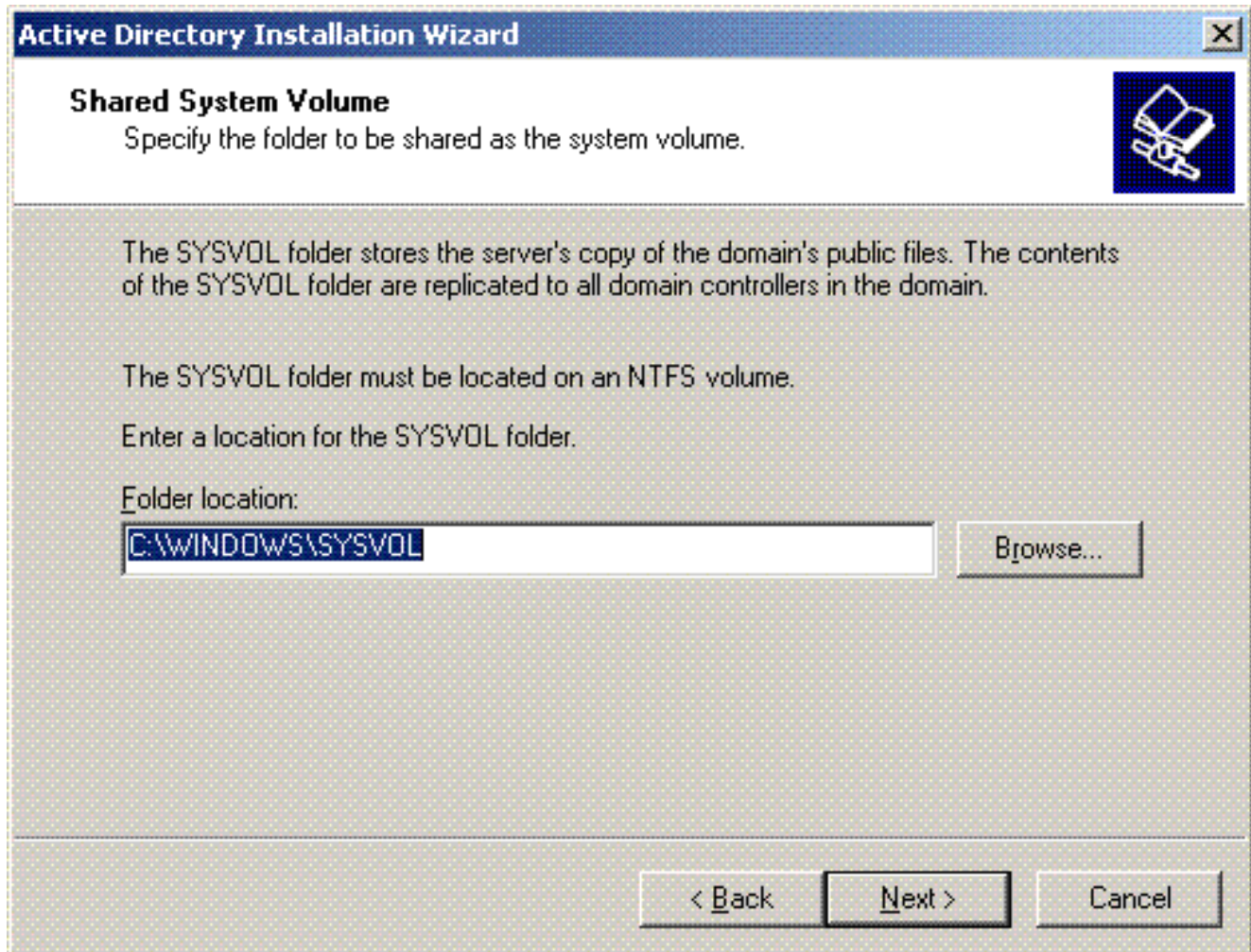
7. Immettere il nome NETBIOS del dominio e fare clic su **Avanti**. In questo esempio viene utilizzato **WIRELESS**.



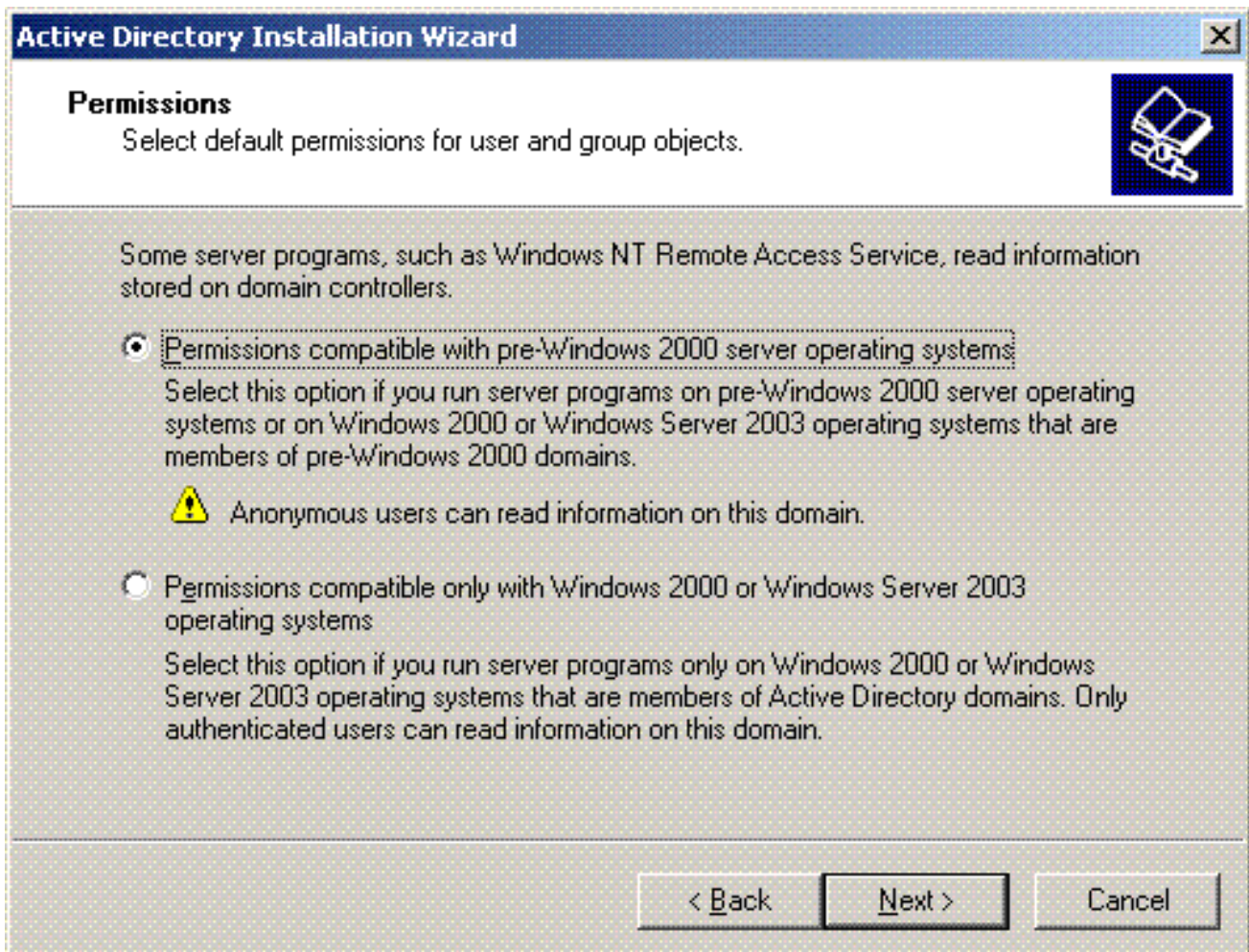
8. Scegliere i percorsi del database e del registro per il dominio. Fare clic su **Next** (Avanti).



9. Scegliere un percorso per la cartella Sysvol. Fare clic su **Next** (Avanti).



10. Scegliere le autorizzazioni predefinite per gli utenti e i gruppi. Fare clic su **Next** (Avanti).



11. Impostare la password dell'amministratore e fare clic su **Avanti**.

Active Directory Installation Wizard

Directory Services Restore Mode Administrator Password

This password is used when you start the computer in Directory Services Restore Mode.

Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.

The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.

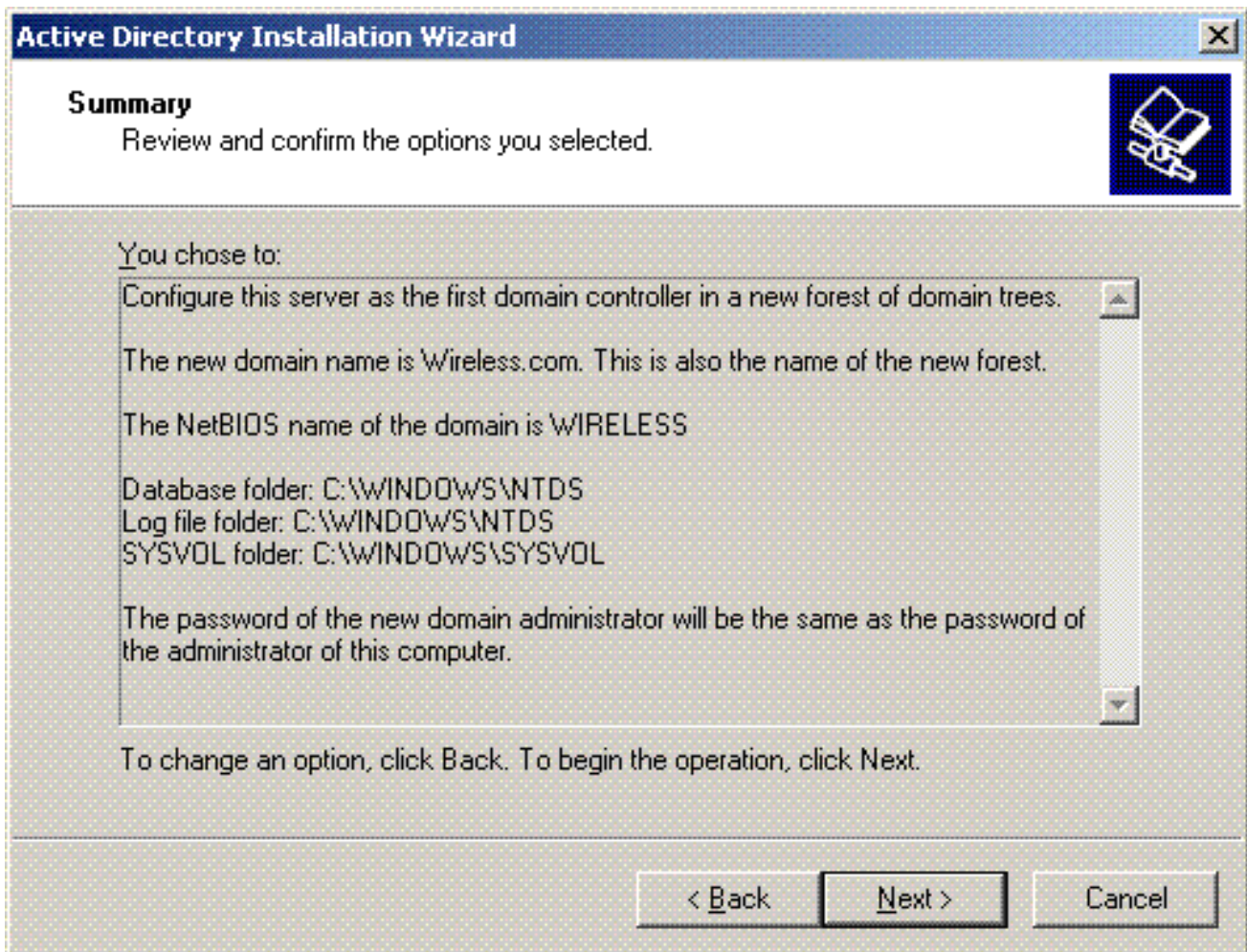
Restore Mode Password:

Confirm password:

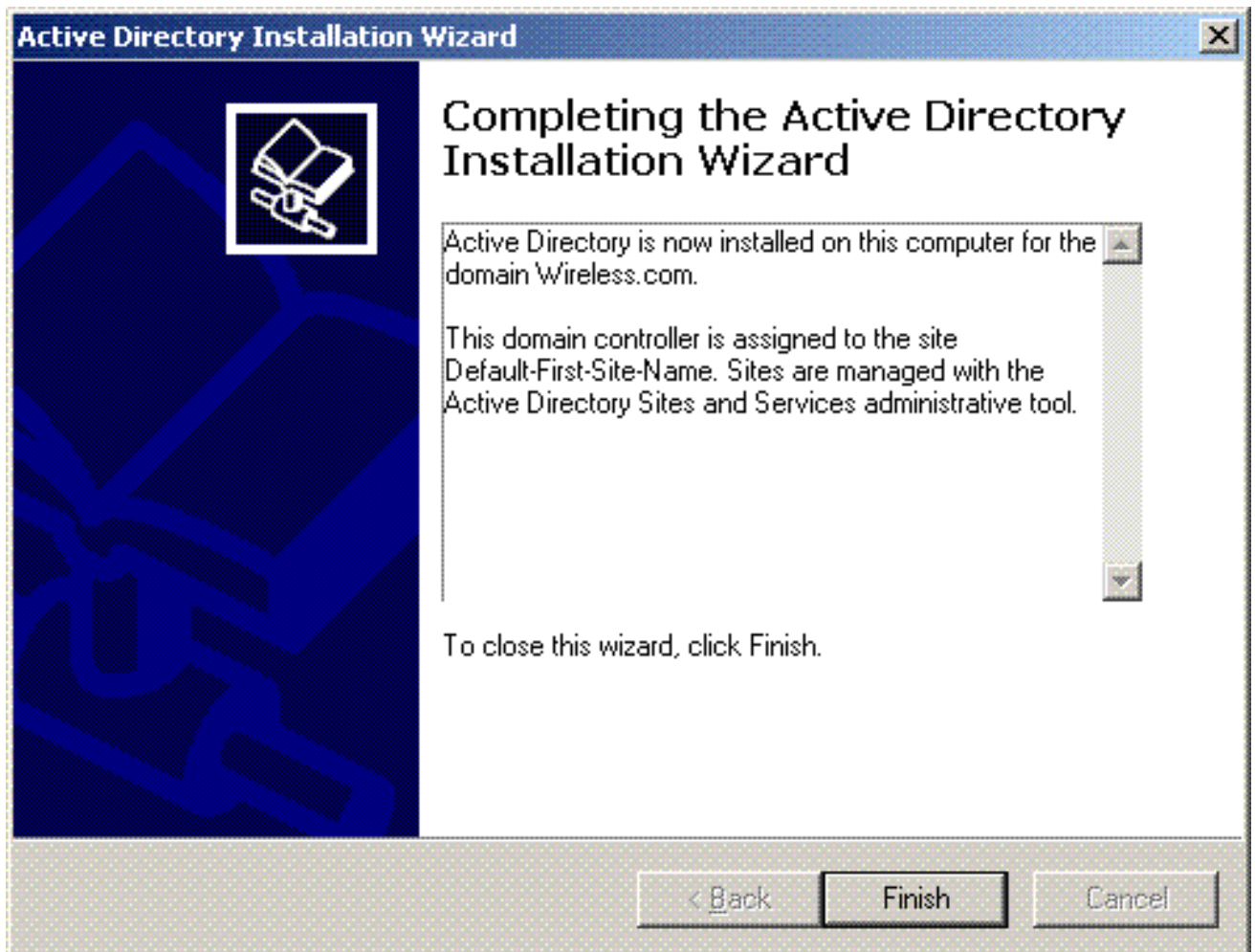
For more information about Directory Services Restore Mode, see [Active Directory Help](#).

< Back Next > Cancel

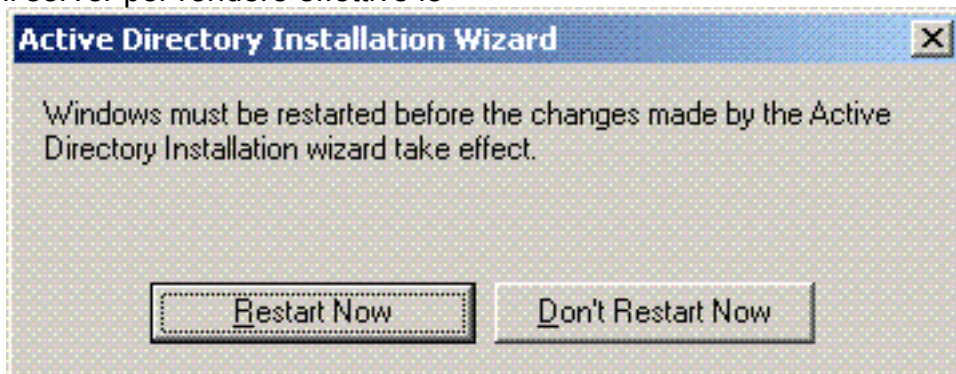
12. Fare clic su **Avanti** per accettare le opzioni di dominio impostate in precedenza.



13. Fare clic su **Fine** per chiudere l'Installazione guidata Active Directory.



14. Riavviare il server per rendere effettive le



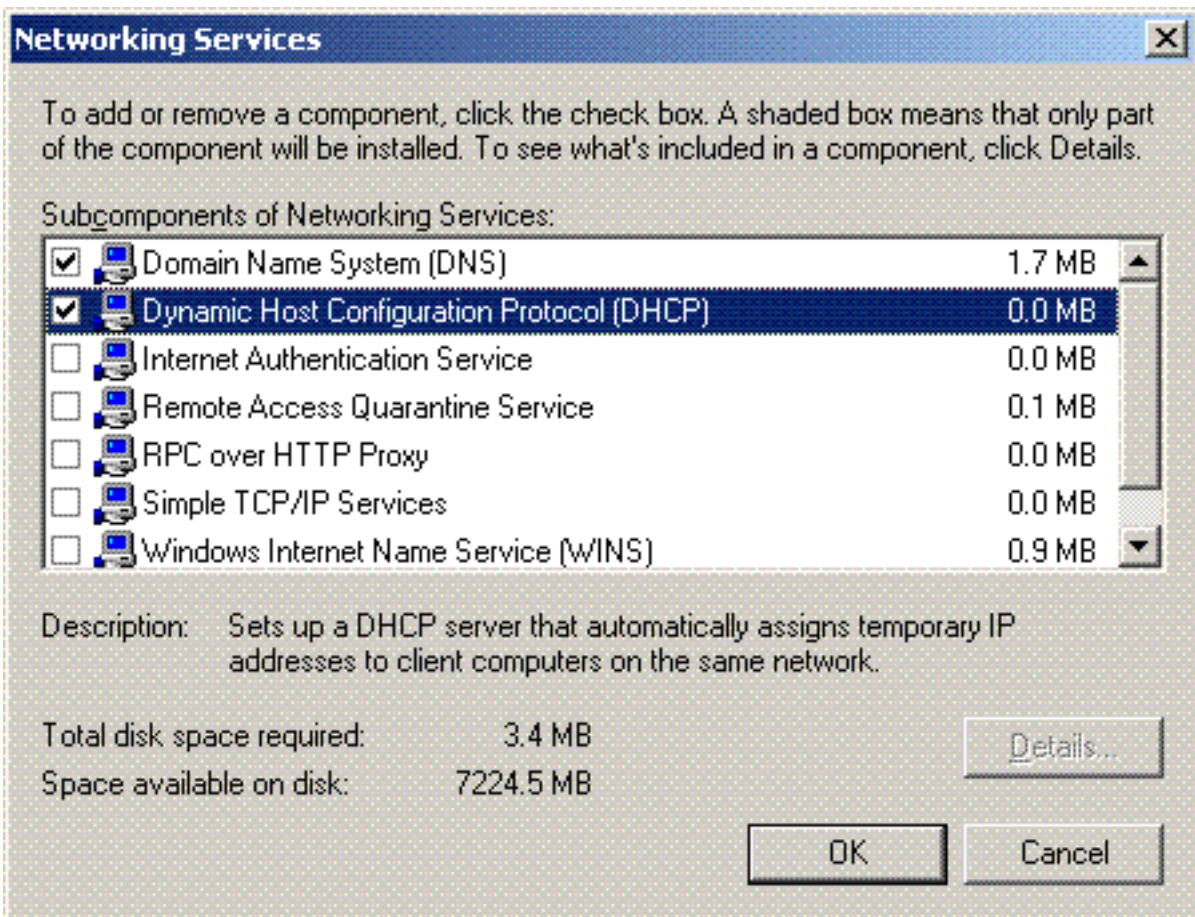
modifiche.

In questo passaggio è stato configurato il server Microsoft Windows 2003 come controller di dominio e creato un nuovo dominio **Wireless.com**. Configurare quindi i servizi DHCP nel server.

[Installare e configurare i servizi DHCP in Microsoft Windows 2003 Server](#)

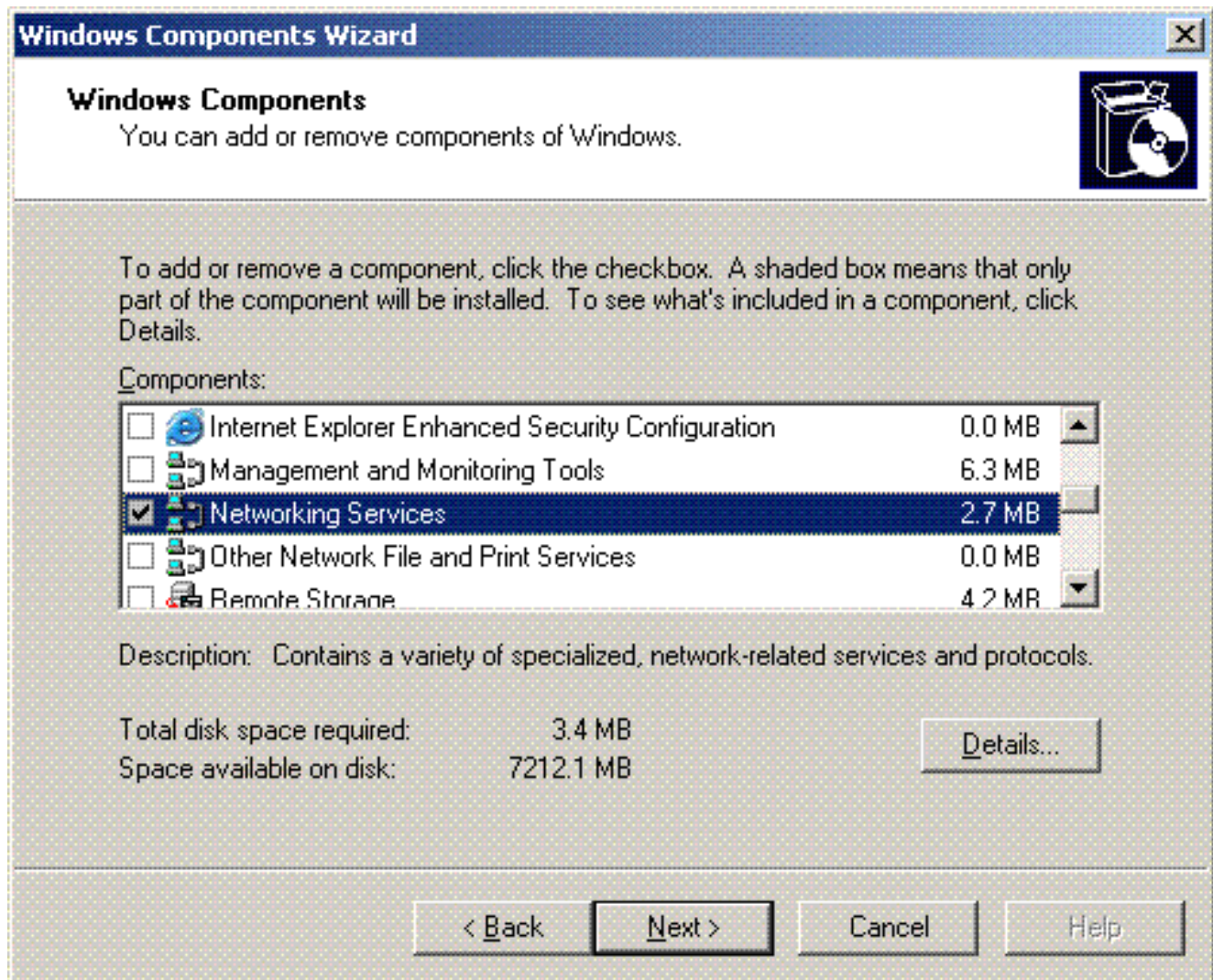
Il servizio DHCP sul server Microsoft 2003 viene utilizzato per fornire indirizzi IP ai client wireless. Per installare e configurare i servizi DHCP in questo server, attenersi alla seguente procedura:

1. Scegliere **Installazione applicazioni** nel Pannello di controllo.
2. Fare clic su **Aggiungi/Rimuovi componenti di Windows**.
3. Scegliere **Servizi di rete** e fare clic su **Dettagli**.
4. Selezionare **DHCP (Dynamic Host Configuration Protocol)** e fare clic su



OK.

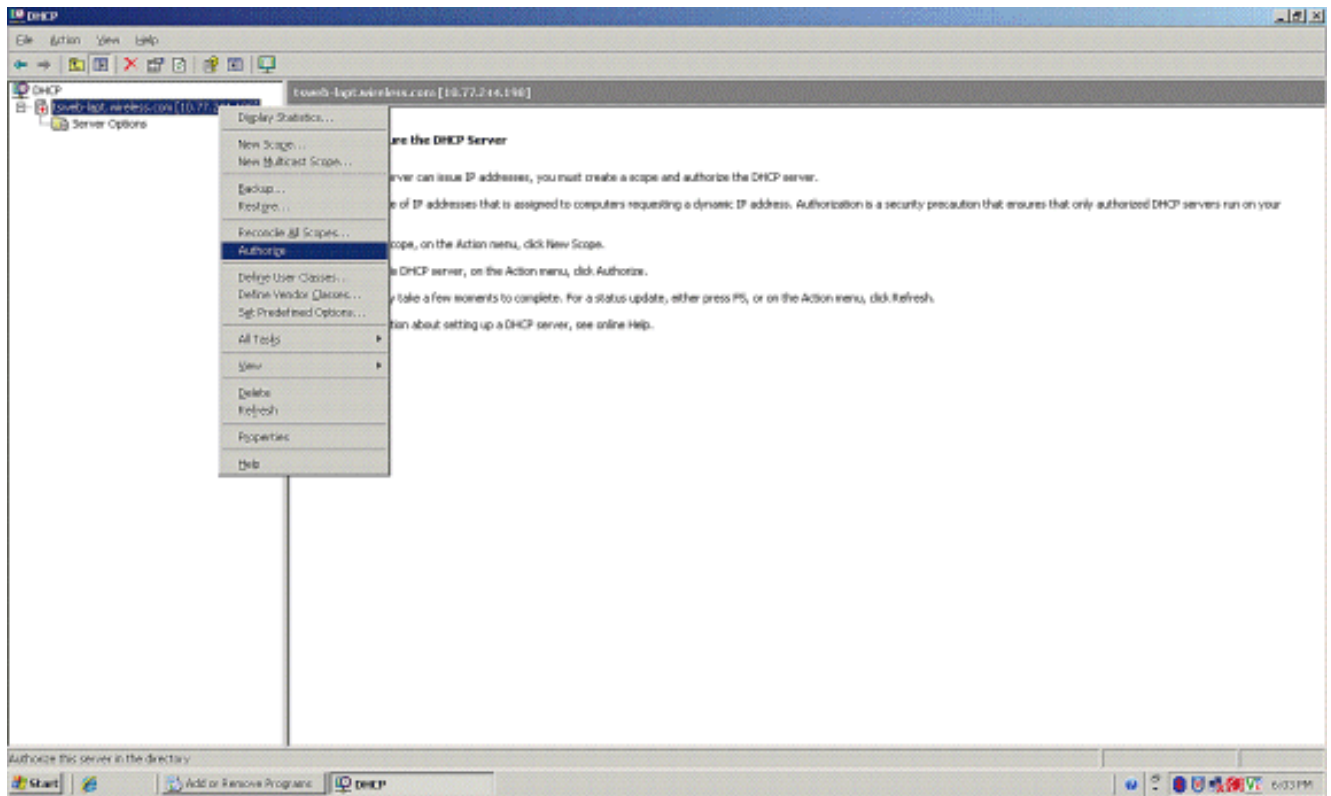
5. Fare clic su **Avanti** per installare il servizio DHCP.



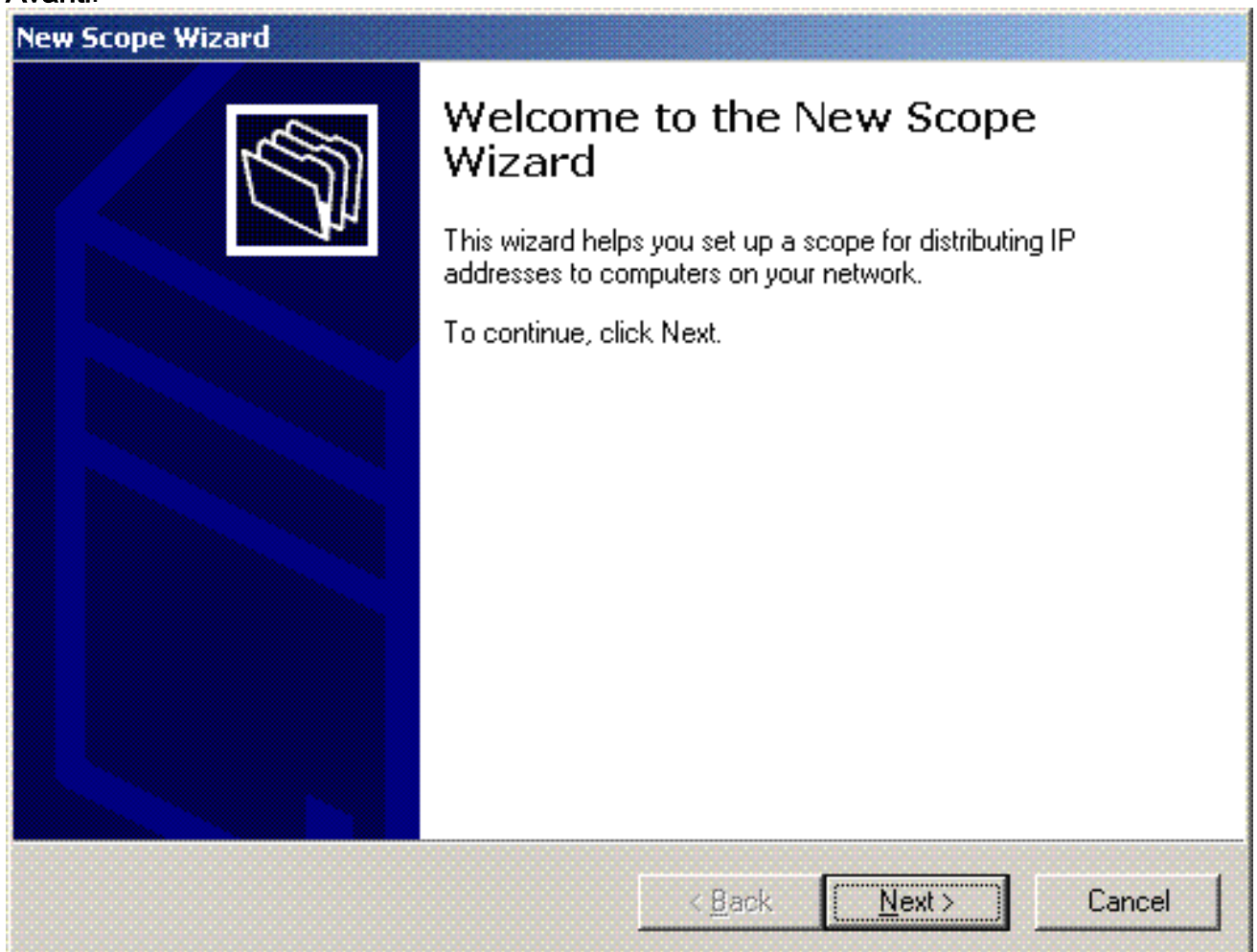
6. Fare clic su **Fine** per completare l'installazione.



7. Per configurare i servizi DHCP, fare clic su **Start > Programmi > Strumenti di amministrazione** e fare clic sullo snap-in **DHCP**.
8. Selezionare il server DHCP - **tsweb-lapt.wireless.com** (nell'esempio).
9. Fare clic su **Azione**, quindi su **Autorizza** per autorizzare il servizio DHCP.



10. Nell'albero della console fare clic con il pulsante destro del mouse su **tsweb-lapt.wireless.com**, quindi scegliere **Nuovo ambito** per definire un intervallo di indirizzi IP per i client wireless.
11. Nella pagina Creazione guidata ambito della Creazione guidata ambito fare clic su **Avanti**.



12. Nella pagina Nome ambito digitare il nome dell'ambito DHCP. In questo esempio, utilizzare

DHCP-Clients come nome dell'ambito. Fare clic su **Next** (Avanti).

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: DHCP-Clients

Description: DHCP Server for Wireless Clients

< Back Next > Cancel

13. Nella pagina Intervallo di indirizzi IP immettere gli indirizzi IP iniziale e finale dell'ambito e fare clic su **Avanti**.

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: 10 . 77 . 244 . 218

End IP address: 10 . 77 . 244 . 219

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: 8

Subnet mask: 255 . 0 . 0 . 0

< Back

Next >

Cancel

14. Nella pagina Aggiungi esclusioni specificare l'indirizzo IP che si desidera riservare/escludere dall'ambito DHCP. Fare clic su **Next** (Avanti).

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

15. Indicare la durata del lease nella pagina Durata 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:
<input type="text" value="8"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

< Back

Next >

Cancel

16. Nella pagina Configura opzioni DHCP, scegliere **Sì, configura ora l'opzione DHCP**, 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

17. Se è presente un router gateway predefinito, indicare l'indirizzo IP del router gateway nella pagina Router (gateway predefinito) e fare clic su **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

Remove

Up

Down

< Back

Next >

Cancel

18. Nella pagina Nome dominio e server DNS digitare il nome del dominio configurato in precedenza. Nell'esempio, utilizzare **Wireless.com**. Immettere l'indirizzo IP del server. Fare clic su **Add**.

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

< Back

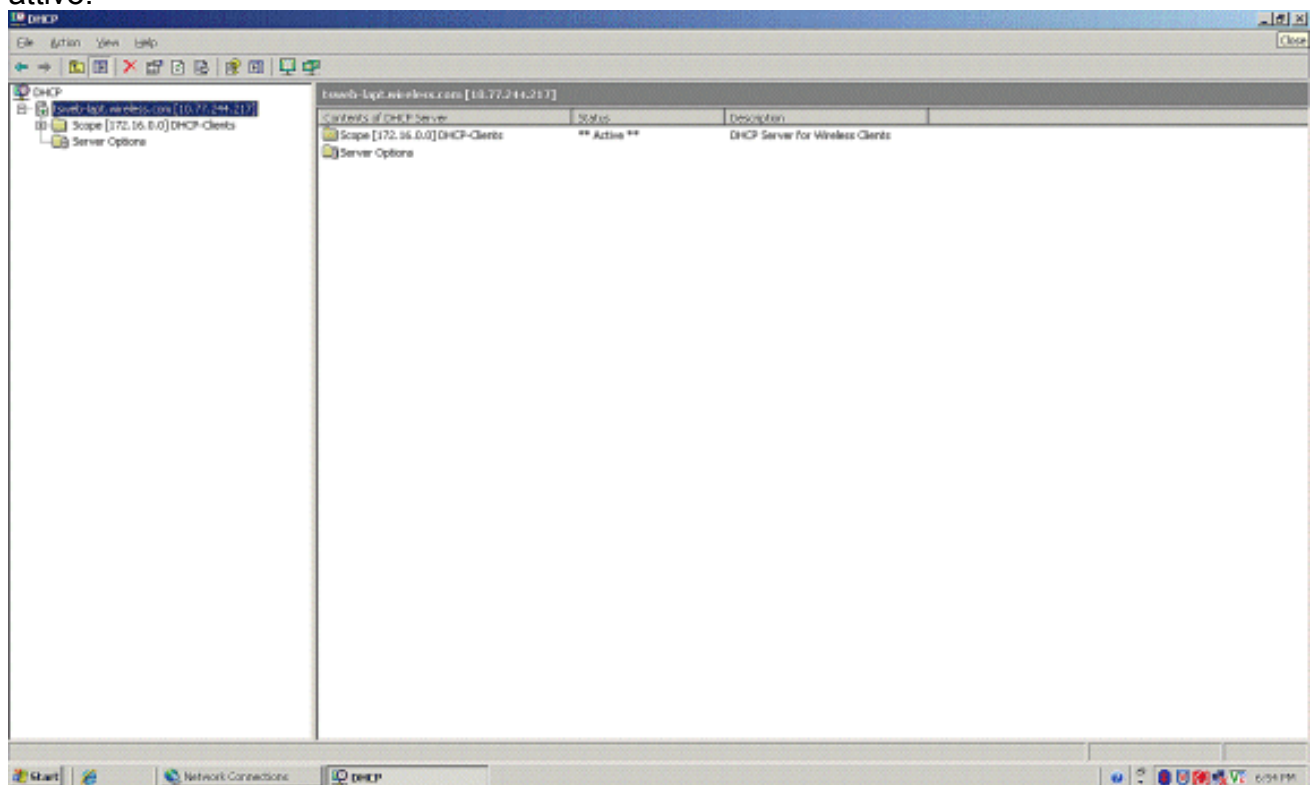
Next >

Cancel

22. Al termine della Creazione guidata ambito, fare clic su **Fine**.



23. Nella finestra Snap-in DHCP verificare che l'ambito DHCP creato sia attivo.



Ora che il server DHCP/DNS è abilitato sul server, configurarlo come server Enterprise Certificate Authority (CA).

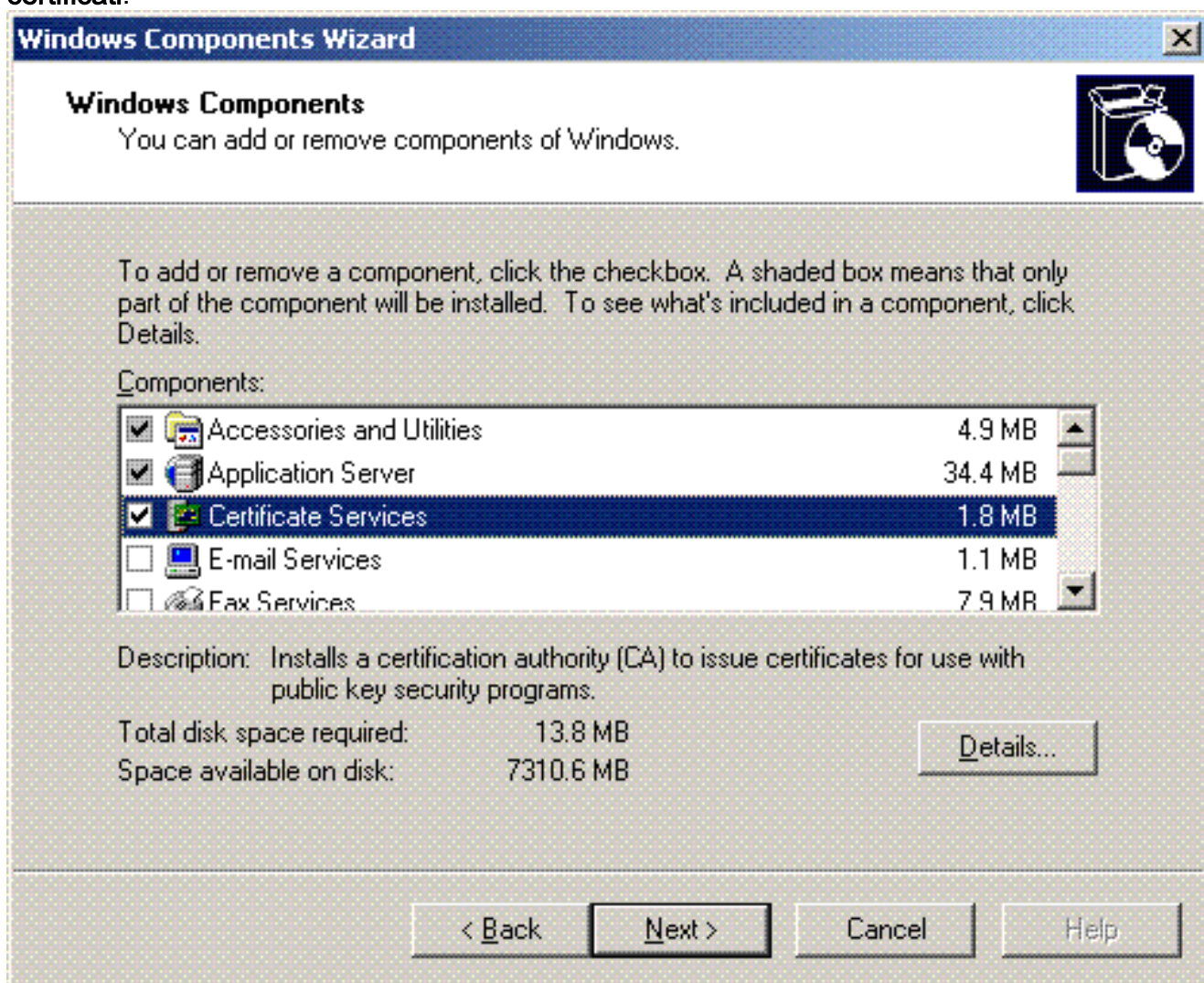
[Installare e configurare il server Microsoft Windows 2003 come server CA](#)

(Certification Authority)

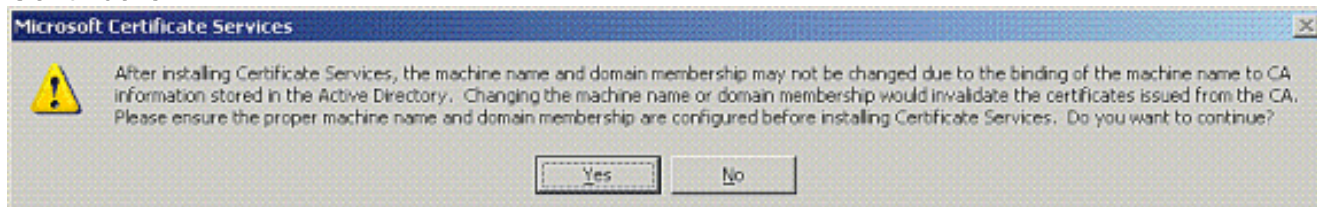
PEAP con EAP-MS-CHAPv2 convalida il server RADIUS in base al certificato presente sul server. Il certificato server deve inoltre essere rilasciato da un'Autorità di certificazione (CA) pubblica considerata attendibile dal computer client, ovvero il certificato CA pubblico esiste già nella cartella Autorità di certificazione radice attendibile nell'archivio certificati del computer client. In questo esempio, configurare il server Microsoft Windows 2003 come autorità di certificazione (CA) che rilascia il certificato al servizio di autenticazione Internet (IAS).

Per installare e configurare i servizi certificati nel server, eseguire la procedura seguente:

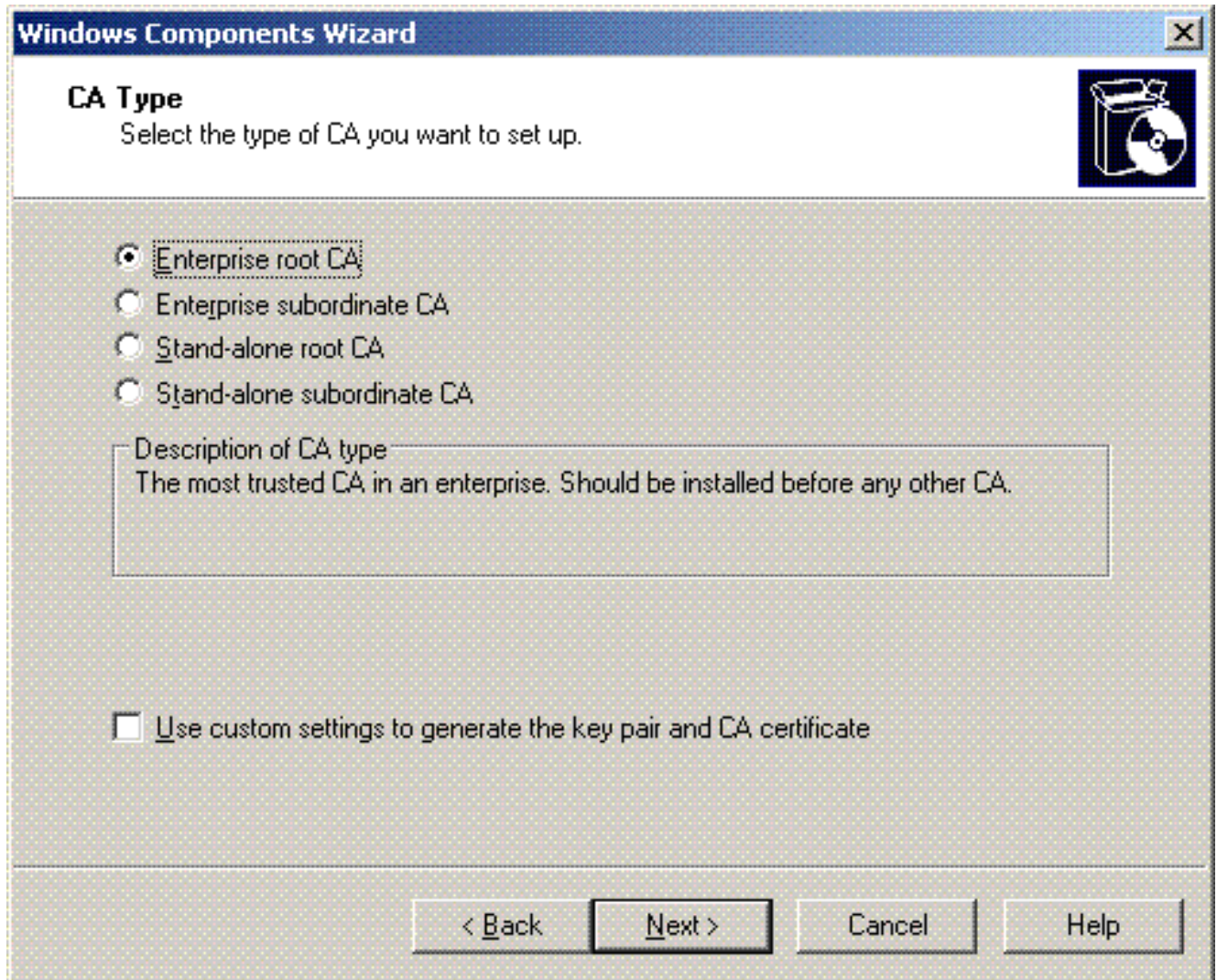
1. Fare clic su **Installazione applicazioni nel Pannello di controllo**.
2. Fare clic su **Aggiungi/Rimuovi componenti di Windows**.
3. Fare clic su **Servizi certificati**.



4. Fare clic su **Sì** per visualizzare il messaggio di avviso **Dopo l'installazione di Servizi certificati, non è possibile rinominare il computer né aggiungerlo o rimuoverlo da un dominio. Continuare?**



5. In Tipo Autorità di certificazione scegliere **CA radice dell'organizzazione** e fare clic su **Avanti**.



6. Immettere un nome per identificare la CA. In questo esempio viene utilizzato **Wireless-CA**. Fare clic su **Next** (Avanti).

Windows Components Wizard

CA Identifying Information
Enter information to identify this CA.

Common name for this CA:
Wireless-CA

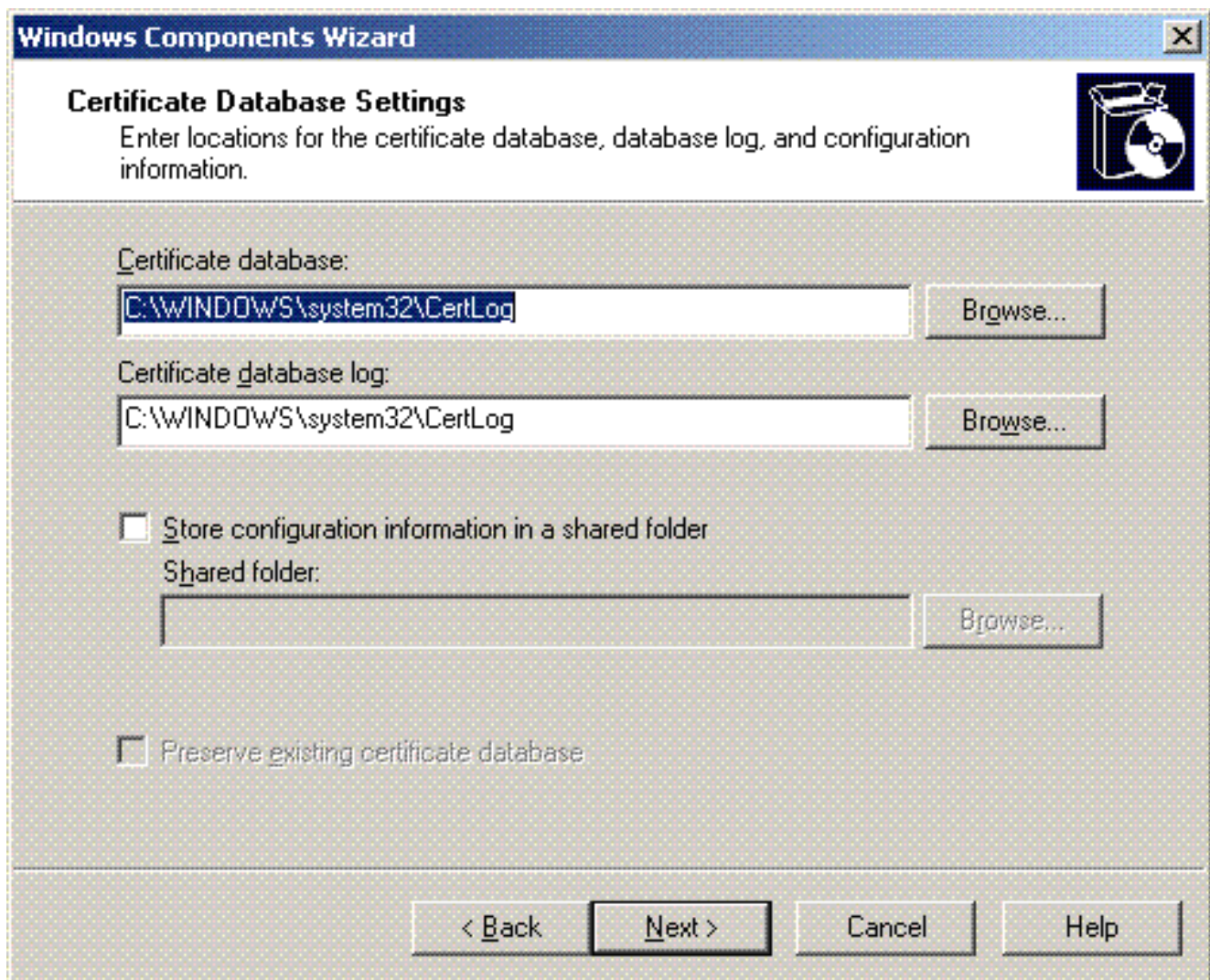
Distinguished name suffix:
DC=Wireless,DC=com

Preview of distinguished name:
CN=Wireless-CA,DC=Wireless,DC=com

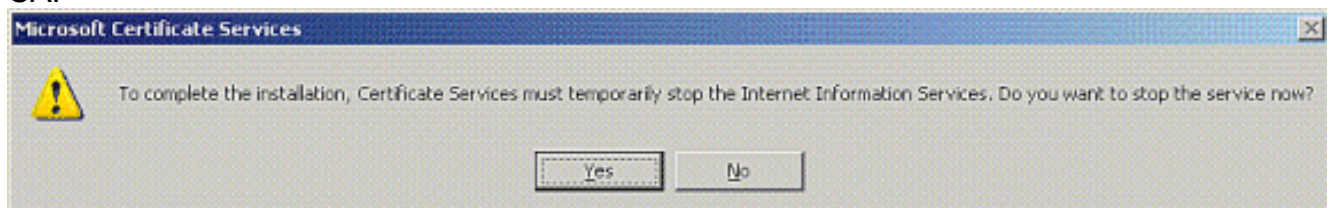
Validity period: 5 Years Expiration date: 12/12/2012 7:01 PM

< Back Next > Cancel Help

7. Viene creata una directory "Registro certificati" per l'archiviazione del database dei certificati. Fare clic su **Next** (Avanti).



8. Se IIS è attivato, è necessario arrestarlo prima di procedere. Fare clic su **OK** per visualizzare il messaggio di avviso che indica che IIS deve essere arrestato. Si riavvia automaticamente dopo l'installazione di CA.



9. Fare clic su **Fine** per completare l'installazione dei servizi CA.

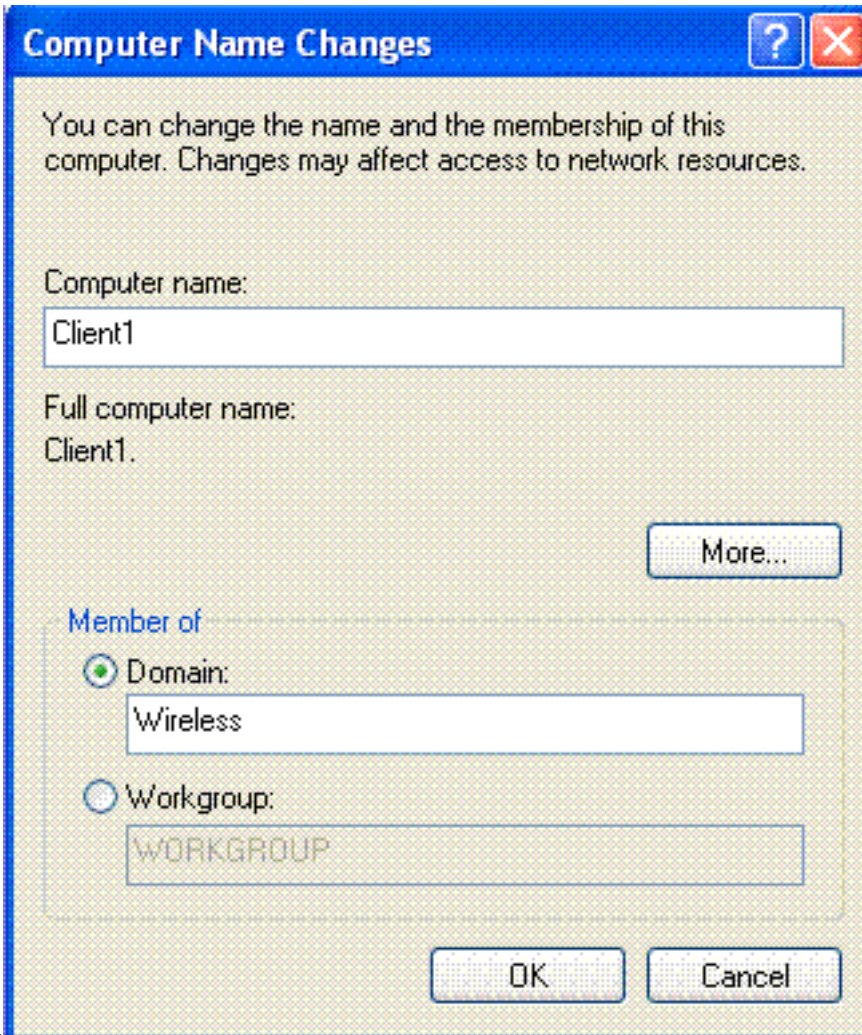


Il passaggio successivo consiste nell'installare e configurare il servizio di autenticazione Internet nel server Microsoft Windows 2003.

[Connetti client al dominio](#)

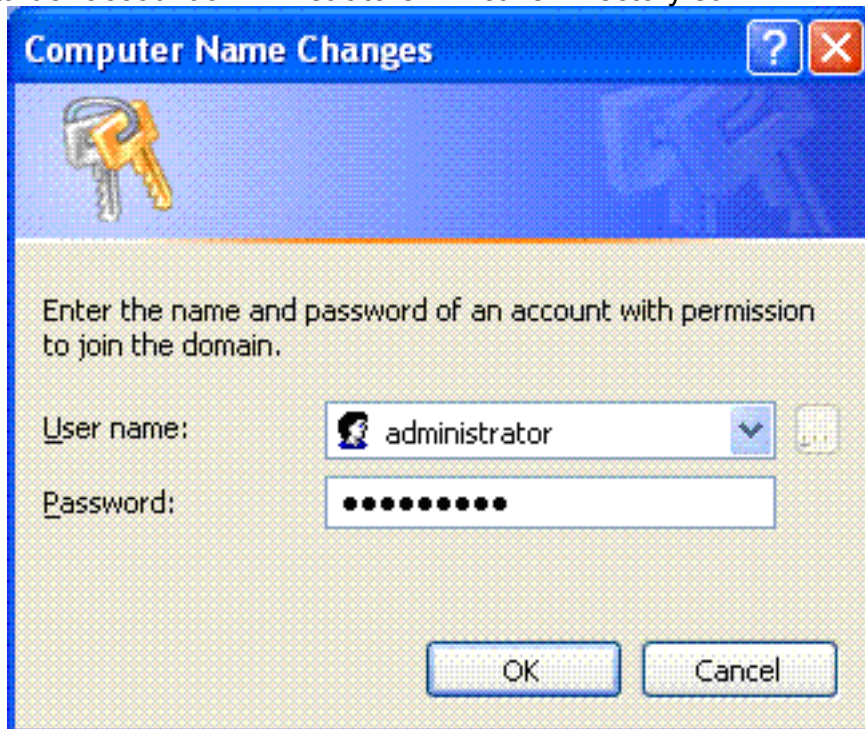
Il passaggio successivo consiste nel connettere i client alla rete cablata e scaricare le informazioni specifiche del dominio dal nuovo dominio. In altre parole, connettere i client al dominio. A tale scopo, effettuare le seguenti operazioni:

1. Collegare i client alla rete cablata con un cavo Ethernet straight-through.
2. Avviare il client ed eseguire il login con il nome utente e la password del client.
3. Fare clic su **Start**; fare clic su **Esegui**; digitare **cmd**; e fare clic su **OK**.
4. Al prompt dei comandi, digitare **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 con il pulsante destro del mouse su **Risorse del computer**, quindi selezionare **Proprietà**.
6. Fare clic sulla scheda **Nome computer**.
7. Fare clic su **Cambia**.
8. Fare clic su **Dominio**; digitare **wireless.com**; e fare clic su



OK.

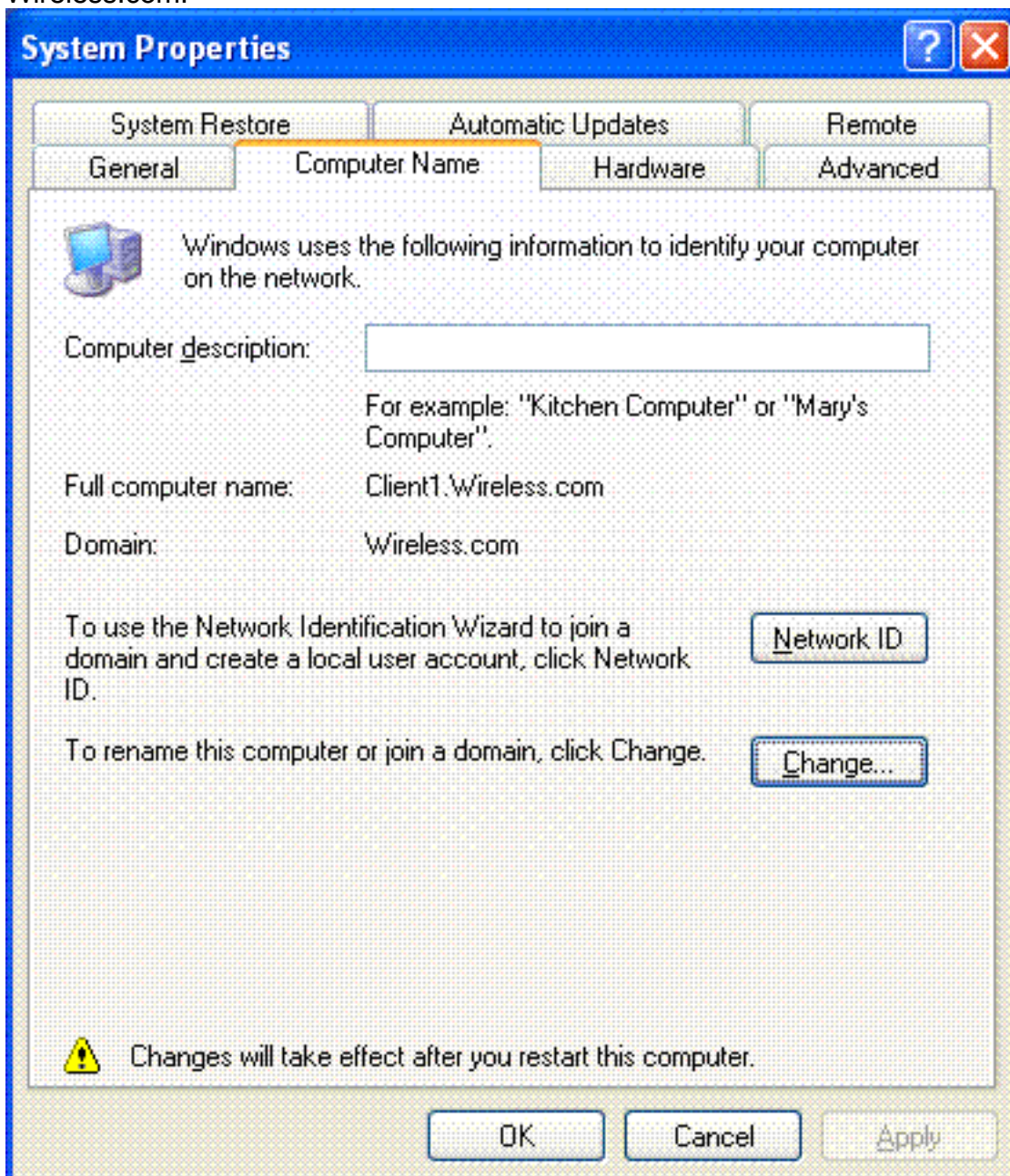
9. Digitare **Username Administrator** e la password specifica del dominio a cui il client si unisce. Si tratta dell'account amministratore in Active Directory sul



server.



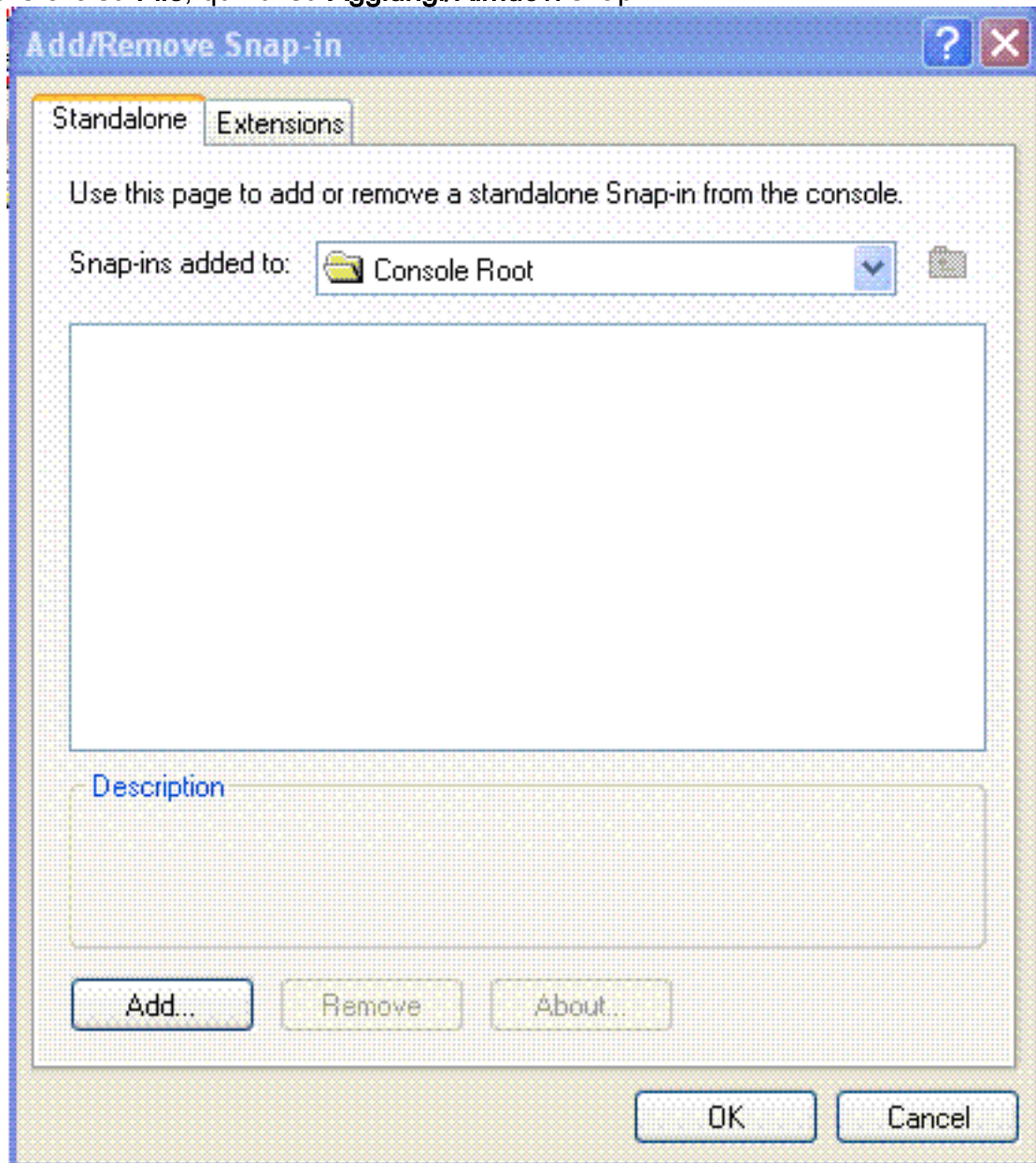
10. Fare clic su **OK**.
11. Fare clic su **Sì** per riavviare il computer.
12. Una volta riavviato il computer, effettuare l'accesso con queste informazioni: Username = **Administrator**; Password = <domain password>; Domain = **Wireless**.
13. Fare clic con il pulsante destro del mouse su **Risorse del computer**, quindi scegliere **Proprietà**.
14. Fare clic sulla scheda **Nome computer** per verificare che ci si trovi nel dominio Wireless.com.



15. Il passaggio successivo consiste nel verificare che il client abbia ricevuto il certificato CA (trust) dal server.

16. Fare clic su **Start**; fare clic su **Esegui**; digitare **mmc** e fare clic su **OK**.

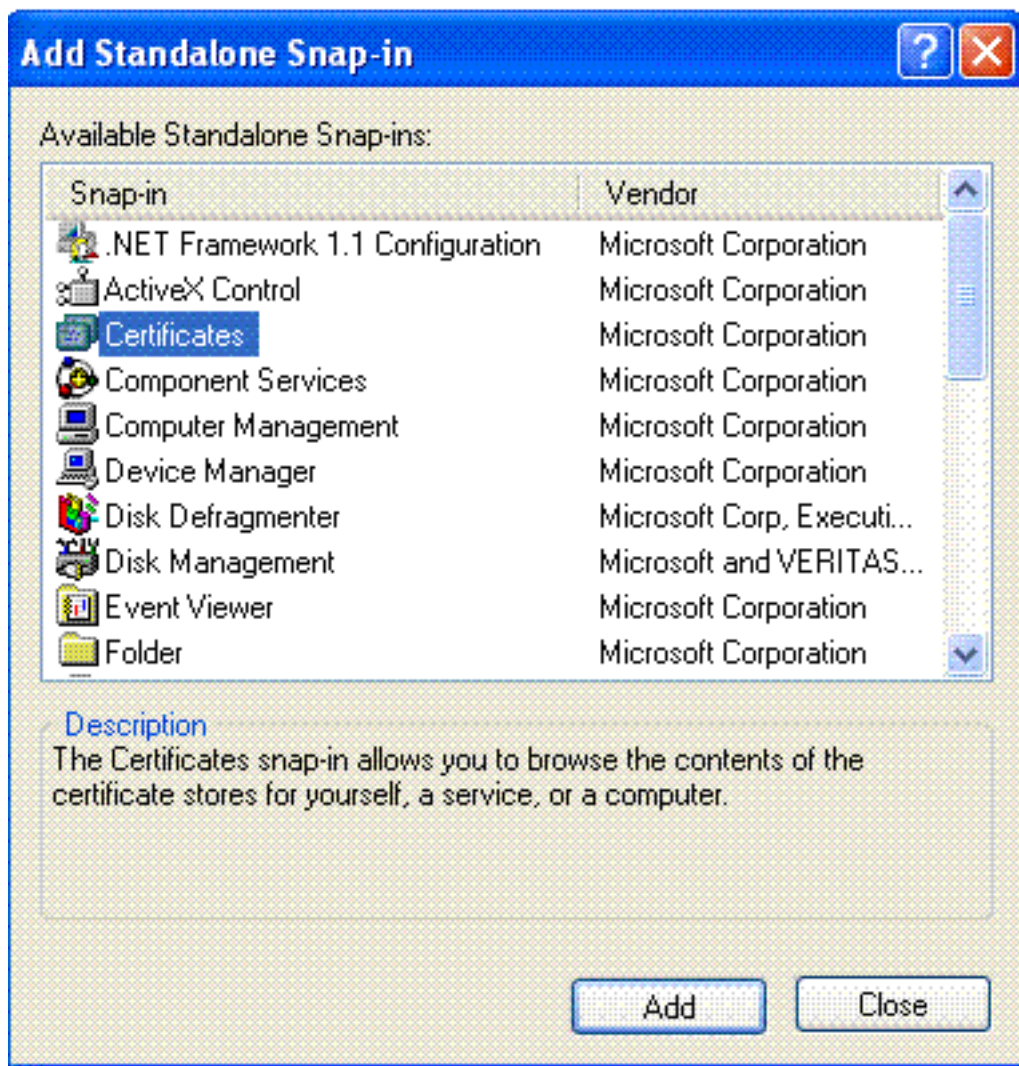
17. Fare clic su **File**, quindi su **Aggiungi/Rimuovi snap-**



in.

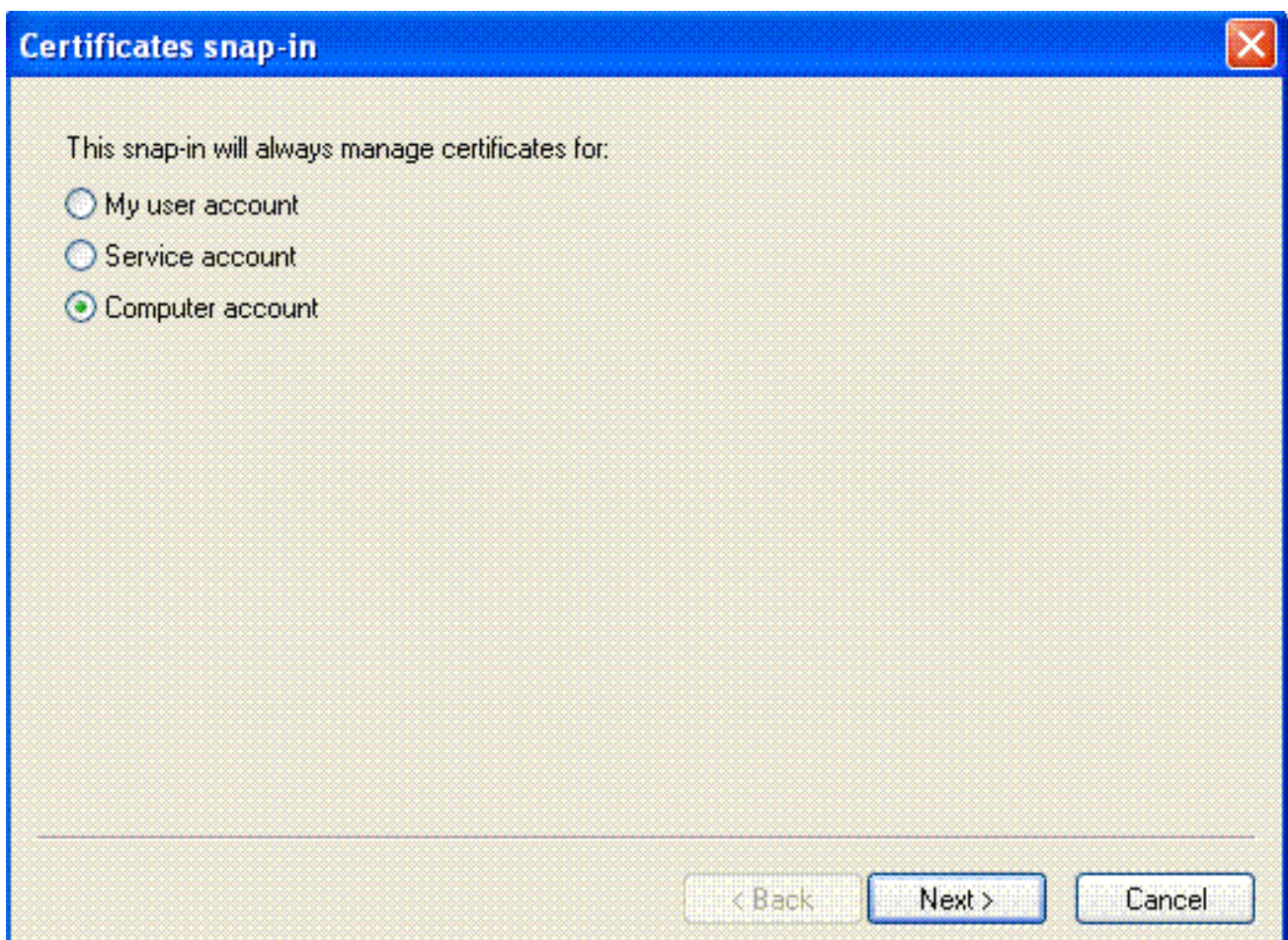
18. Fare clic su **Add**.

19. Scegliere **Certificato**, quindi fare clic su

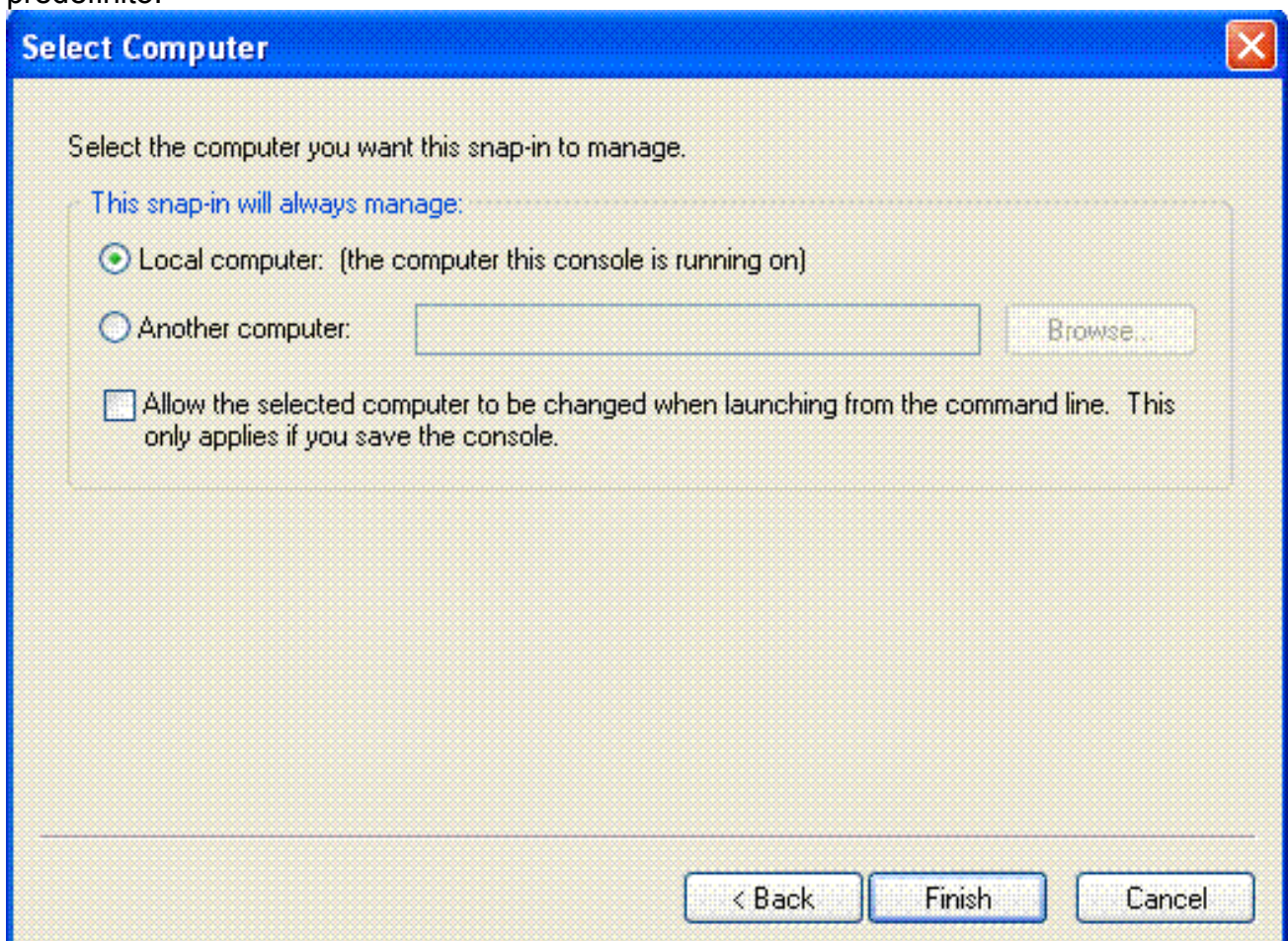


Aggiungi.

20. Scegliere **Account computer**, quindi fare clic su **Avanti**.

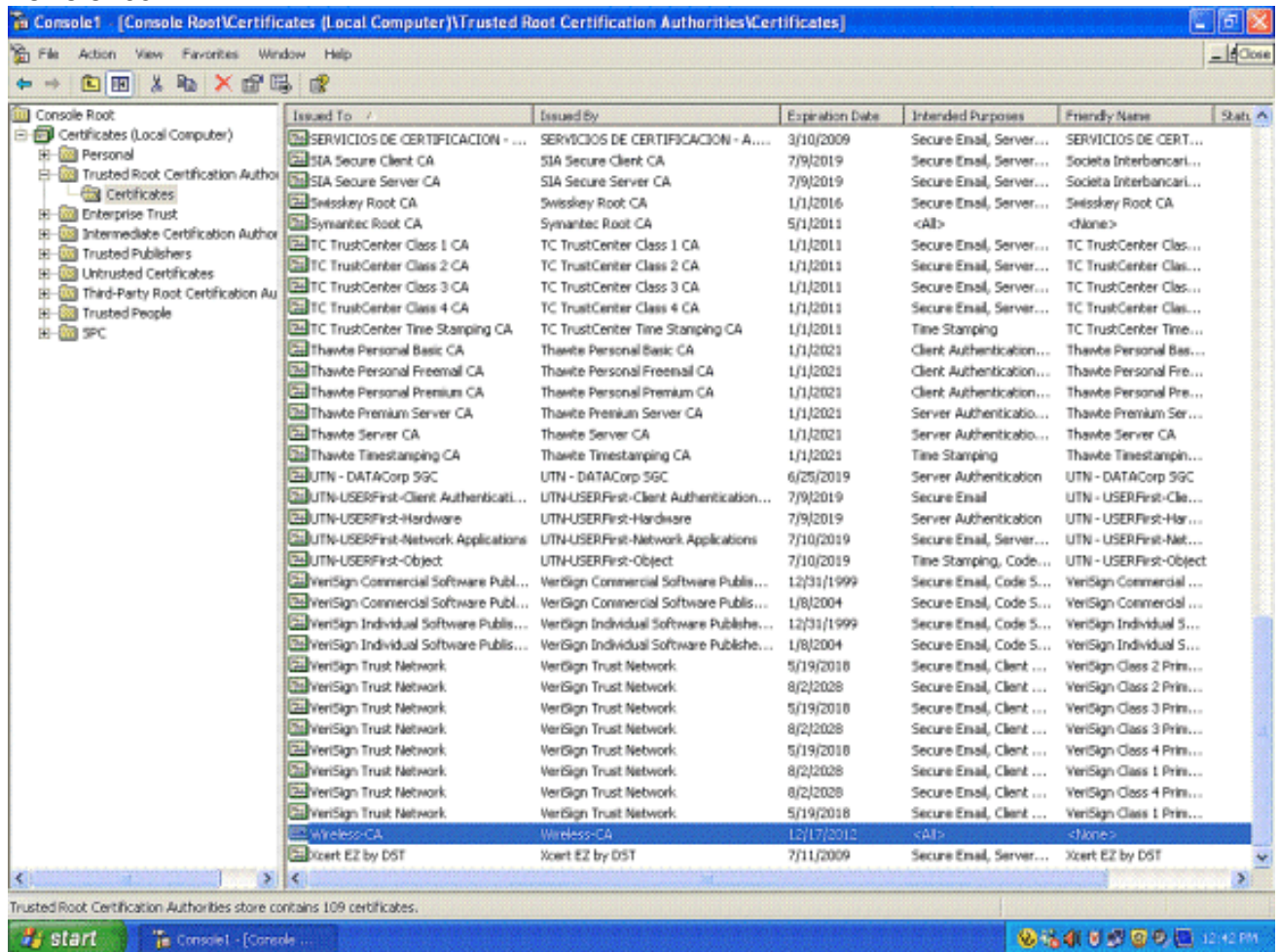


21. Fare clic su **Fine** per accettare il computer locale predefinito.



22. Fare clic su **Close** (Chiudi), quindi su **OK**.

23. Espandere **Certificati (computer locale)**, **Autorità di certificazione radice attendibili** e fare clic su **Certificati**. Trovare **Wireless** nell'elenco.



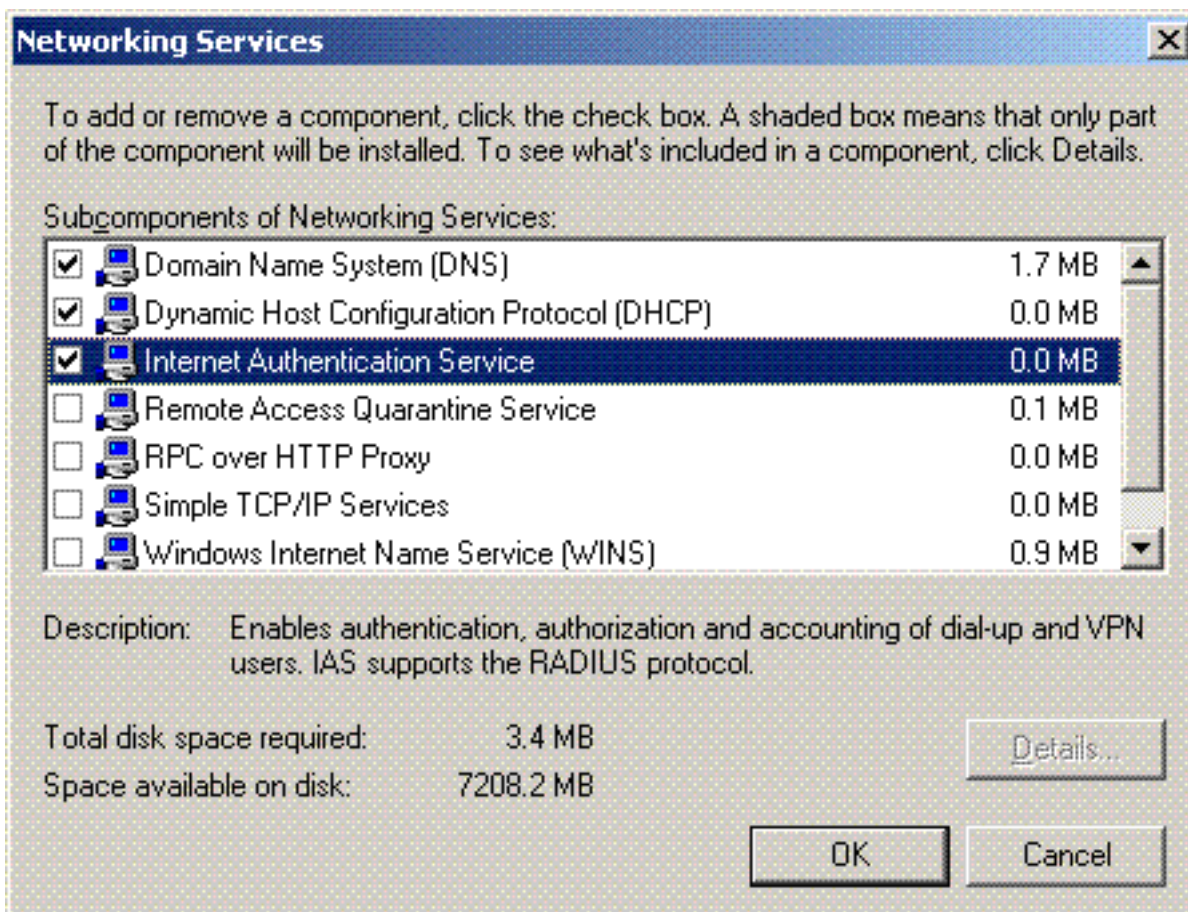
24. Ripetere questa procedura per aggiungere altri client al dominio.

[Installare il servizio di autenticazione Internet nel server Microsoft Windows 2003 e richiedere un certificato](#)

In questa configurazione, il servizio di autenticazione Internet (IAS, Internet Authentication Service) viene utilizzato come server RADIUS per autenticare i client wireless con l'autenticazione PEAP.

Completare la procedura seguente per installare e configurare IAS sul server.

1. Scegliere **Installazione applicazioni** nel Pannello di controllo.
2. Fare clic su **Aggiungi/Rimuovi componenti di Windows**.
3. Scegliere **Servizi di rete**, quindi fare clic su **Dettagli**.
4. Scegliere **Servizio di autenticazione Internet**; fare clic su **OK**; e fare clic su

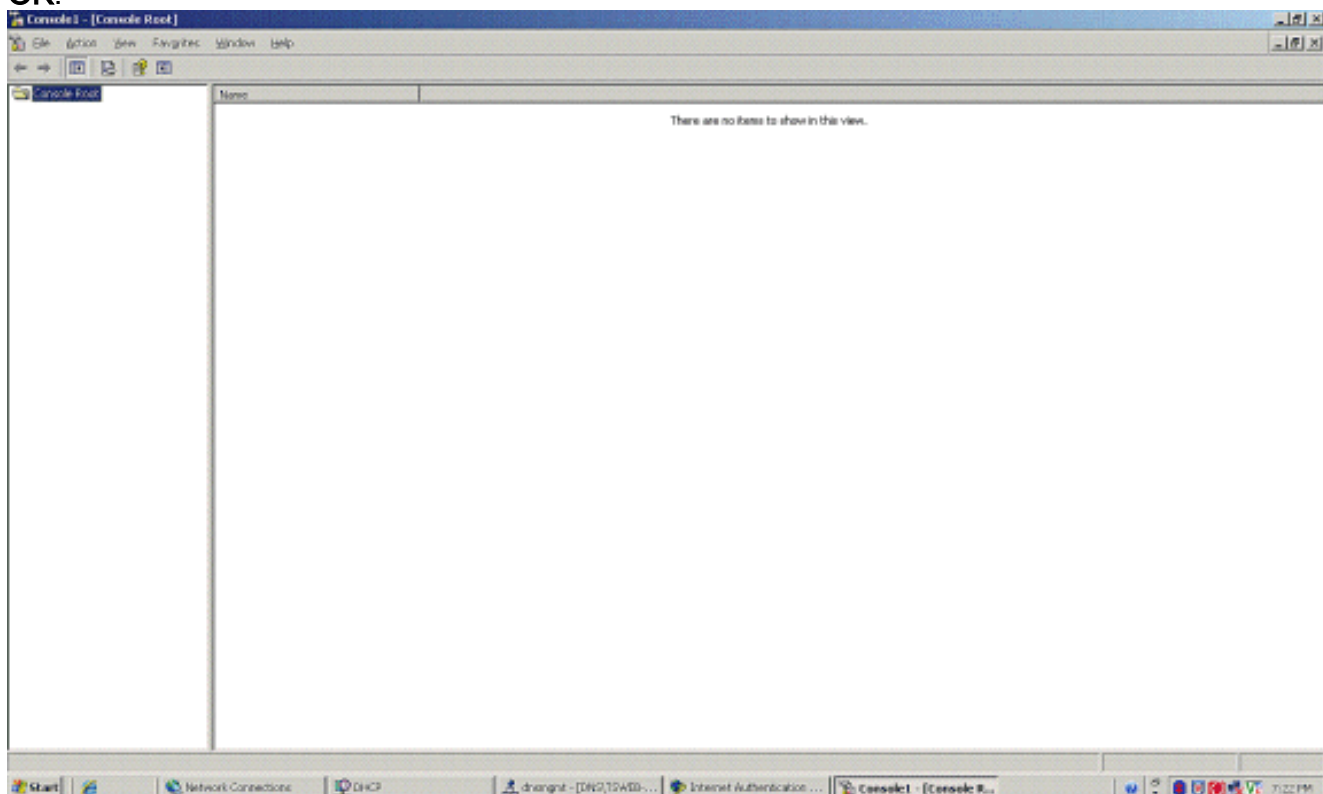


Avanti.

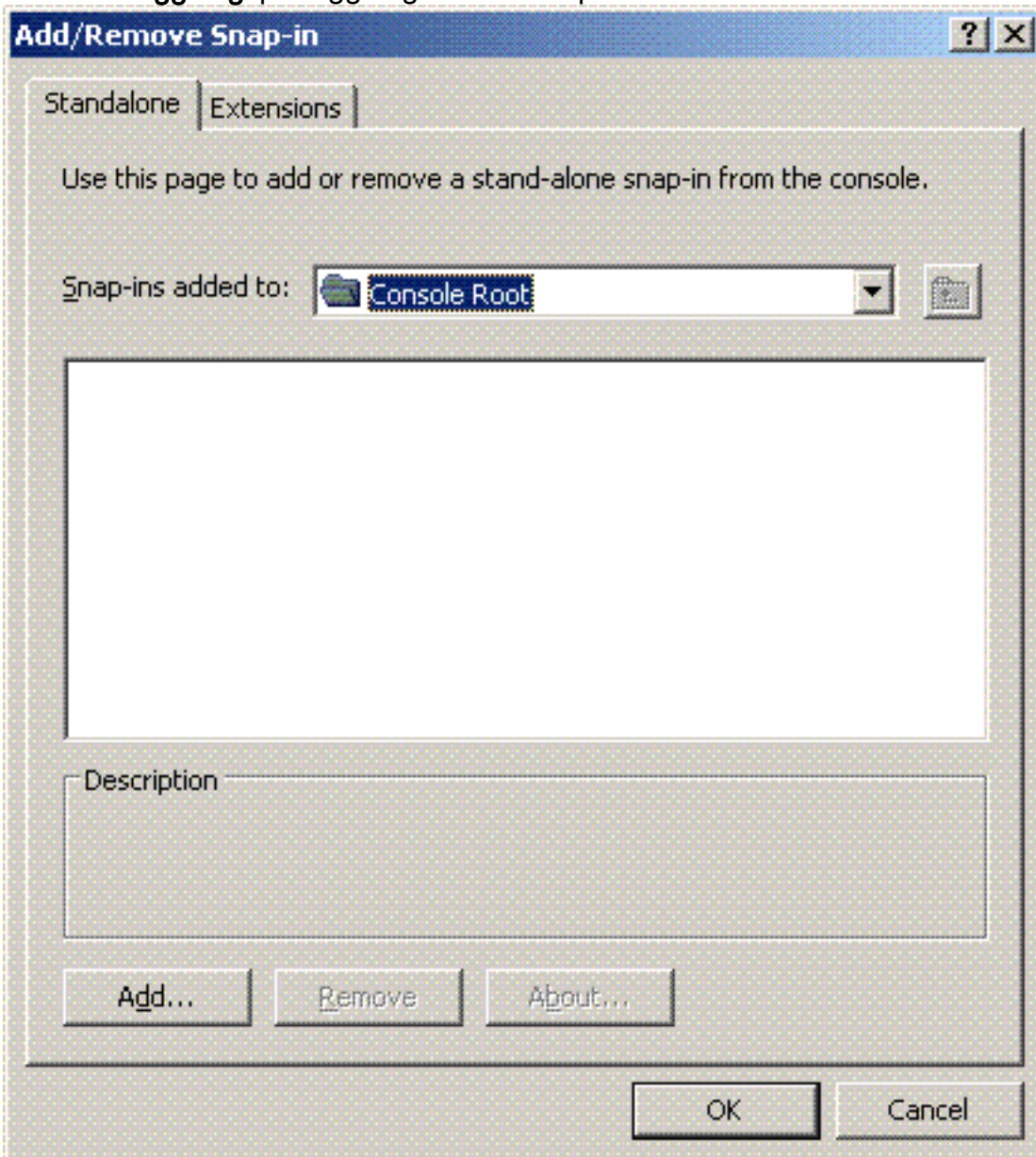
5. Fare clic su **Fine** per completare l'installazione di IAS.



6. Il passaggio successivo consiste nell'installare il certificato del computer per il servizio di autenticazione Internet (IAS).
7. Fare clic su **Start**; fare clic su **Esegui**; digitare **mmc**; e fare clic su **OK**.

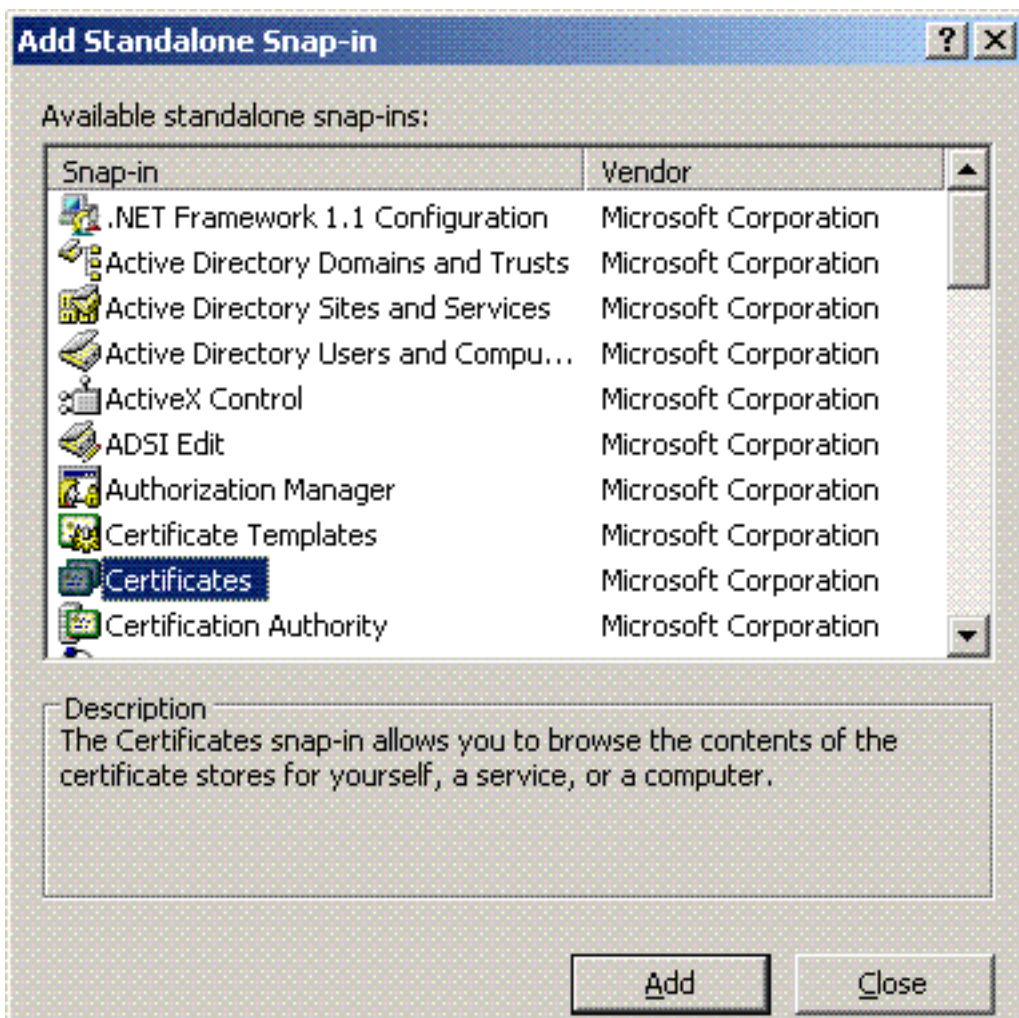


8. Scegliere **Console** dal menu file, quindi **Aggiungi/Rimuovi** snap-in.
9. Fare clic su **Aggiungi** per aggiungere uno snap-



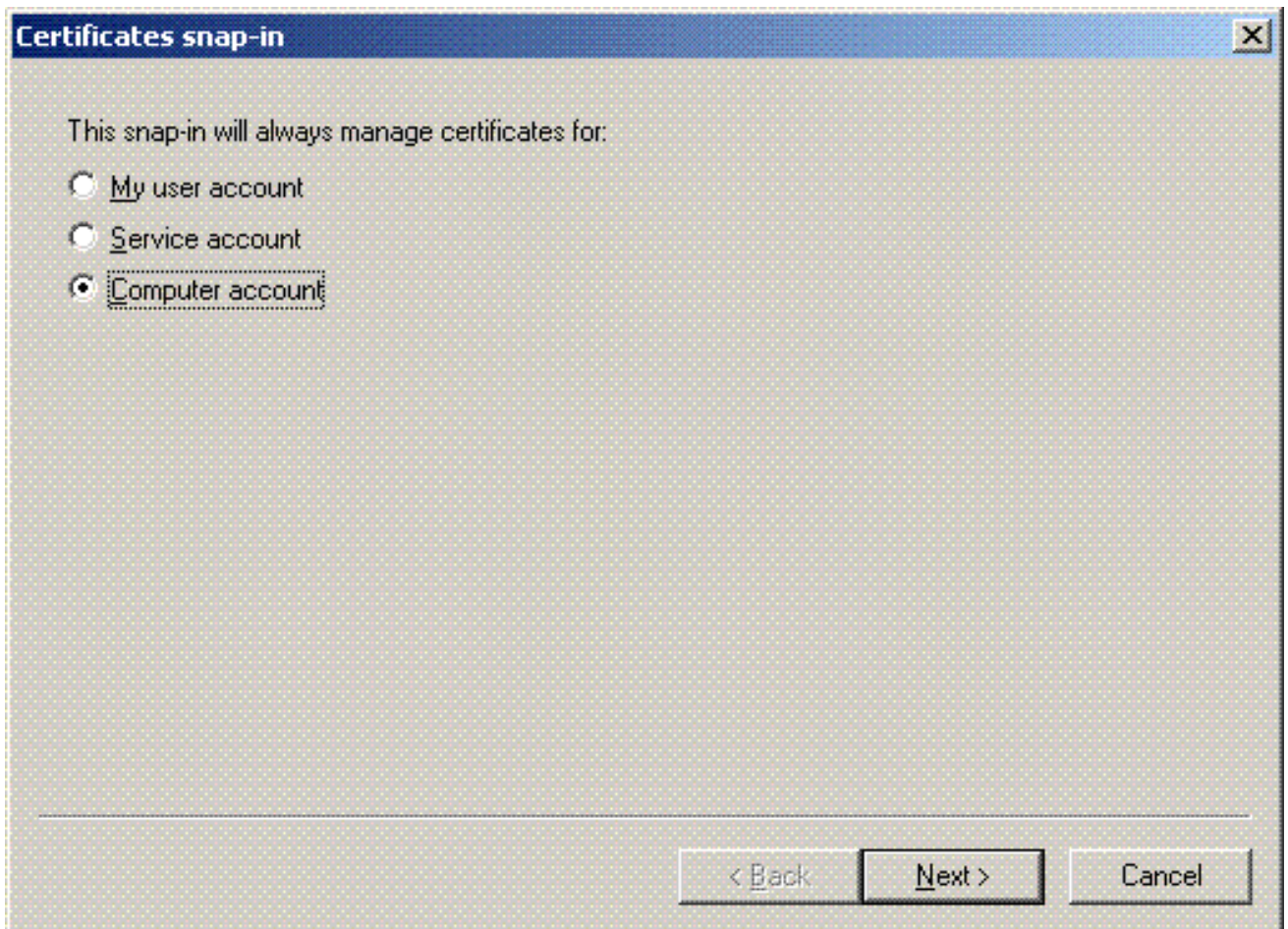
in.

10. Scegliere **Certificati** dall'elenco degli snap-in e fare clic su

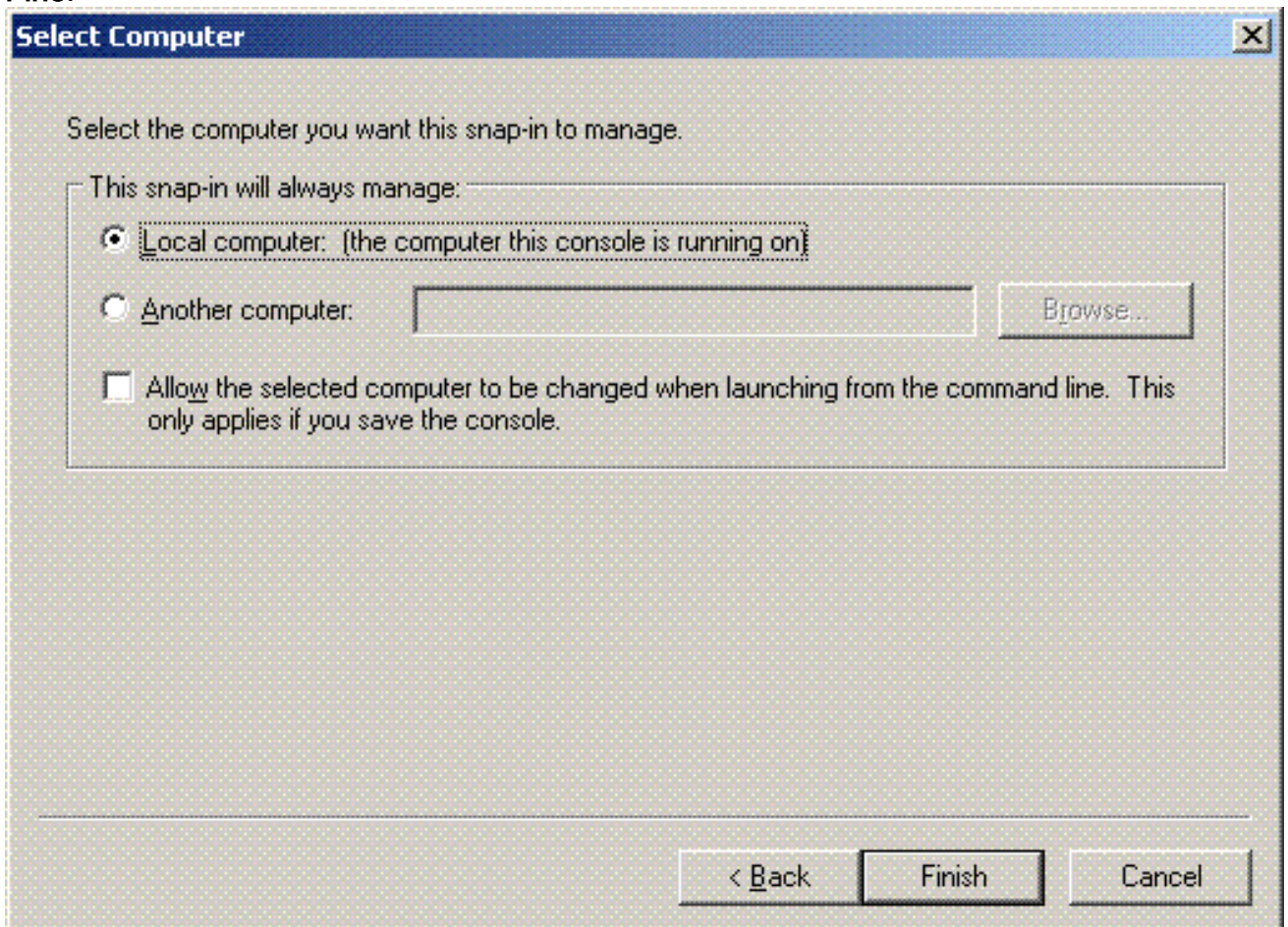


Aggiungi.

11. Scegliere **Account computer** e fare clic su **Avanti**.

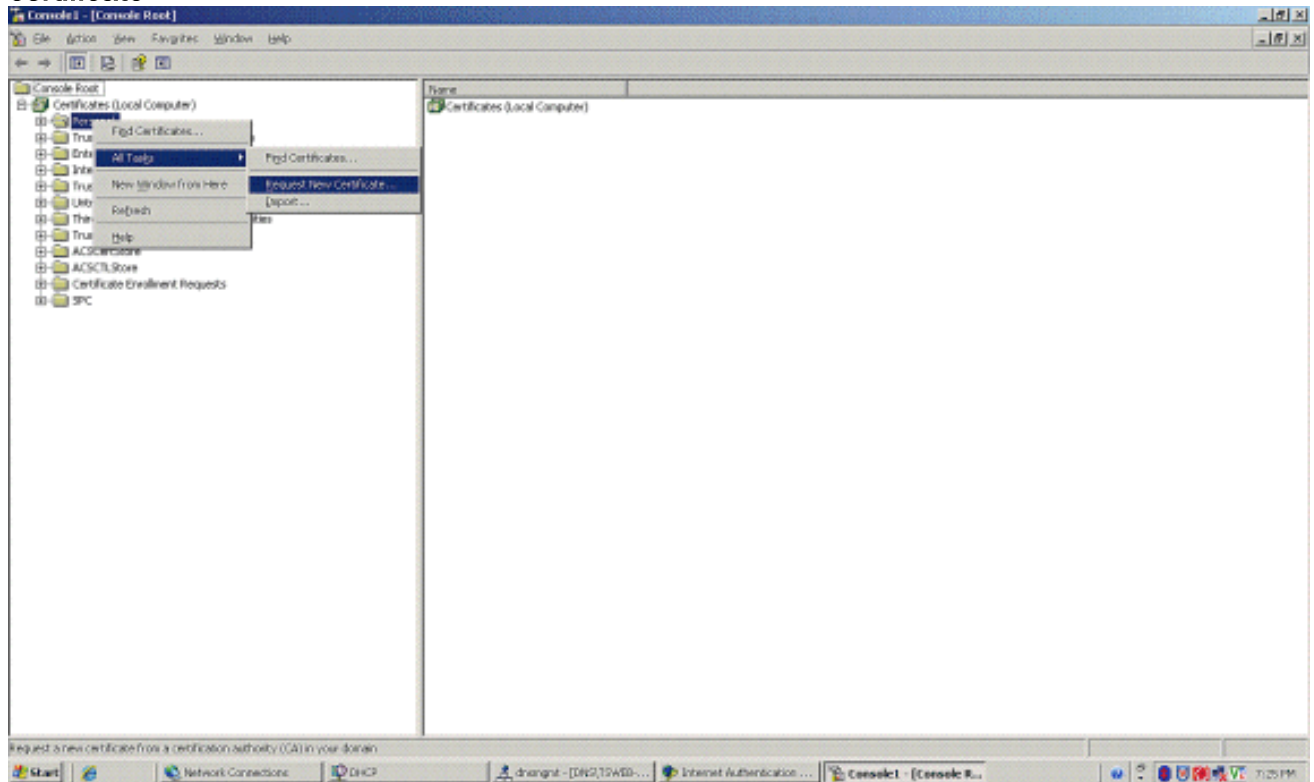


12. Scegliere **Computer locale**, quindi fare clic su **Fine**.



13. Fare clic su **Close** (Chiudi), quindi su **OK**.

14. Espandere **Certificati (computer locale)**; fare clic con il pulsante destro del mouse su **Cartella personale**; scegliere **Tutte le attività** e quindi **Richiedi nuovo certificato**.



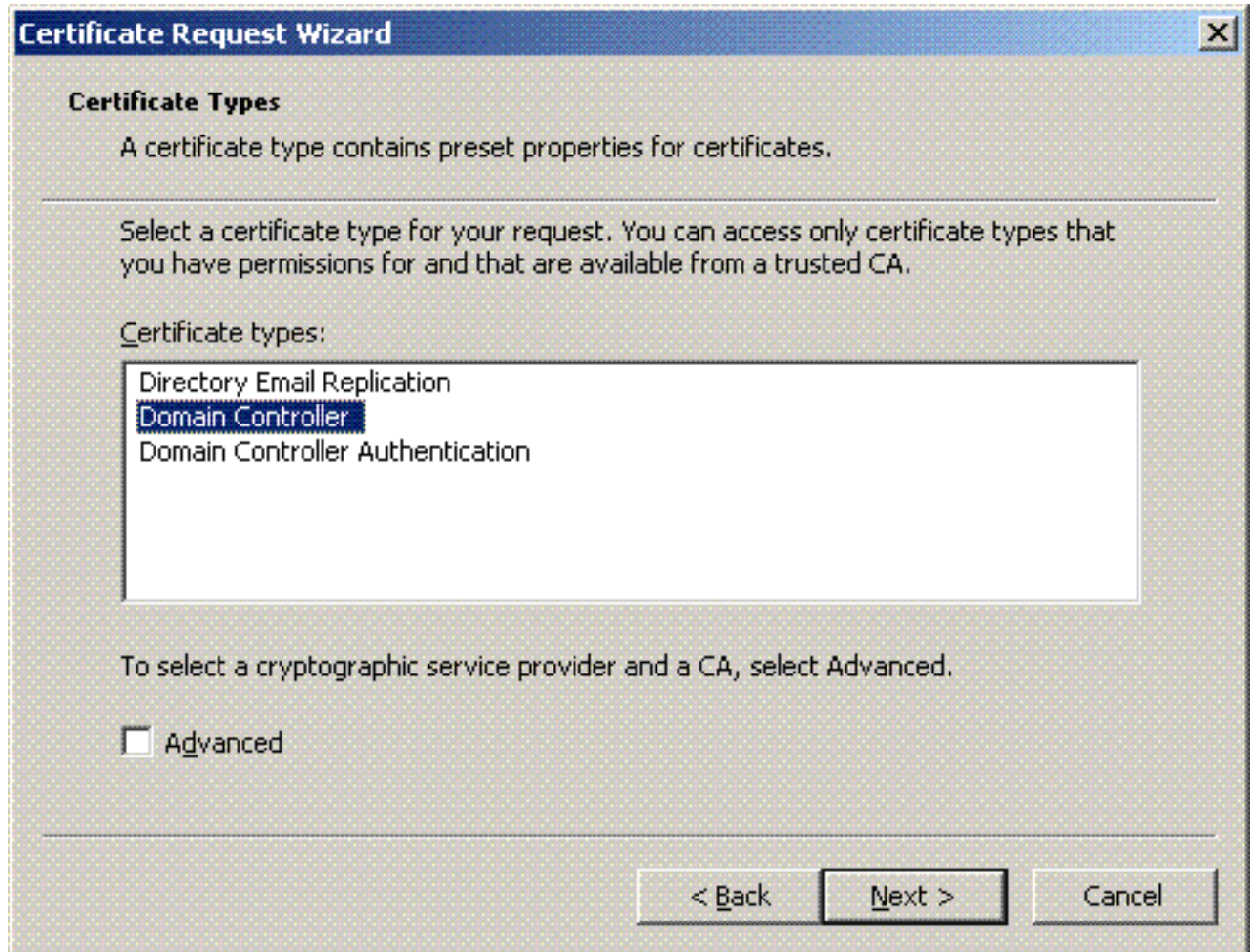
15. Fare clic su **Avanti** nella **Richiesta guidata certificato**



16. Scegliere il modello di certificato **Controller di dominio** (se si richiede un certificato computer

in un server diverso dal controller di dominio, scegliere un modello di certificato **computer**) e fare clic su

Avanti.



17. Digitare un nome e una descrizione per il certificato.

Certificate Request Wizard [X]

Certificate Friendly Name and Description

You can provide a name and description that help you quickly identify a specific certificate.

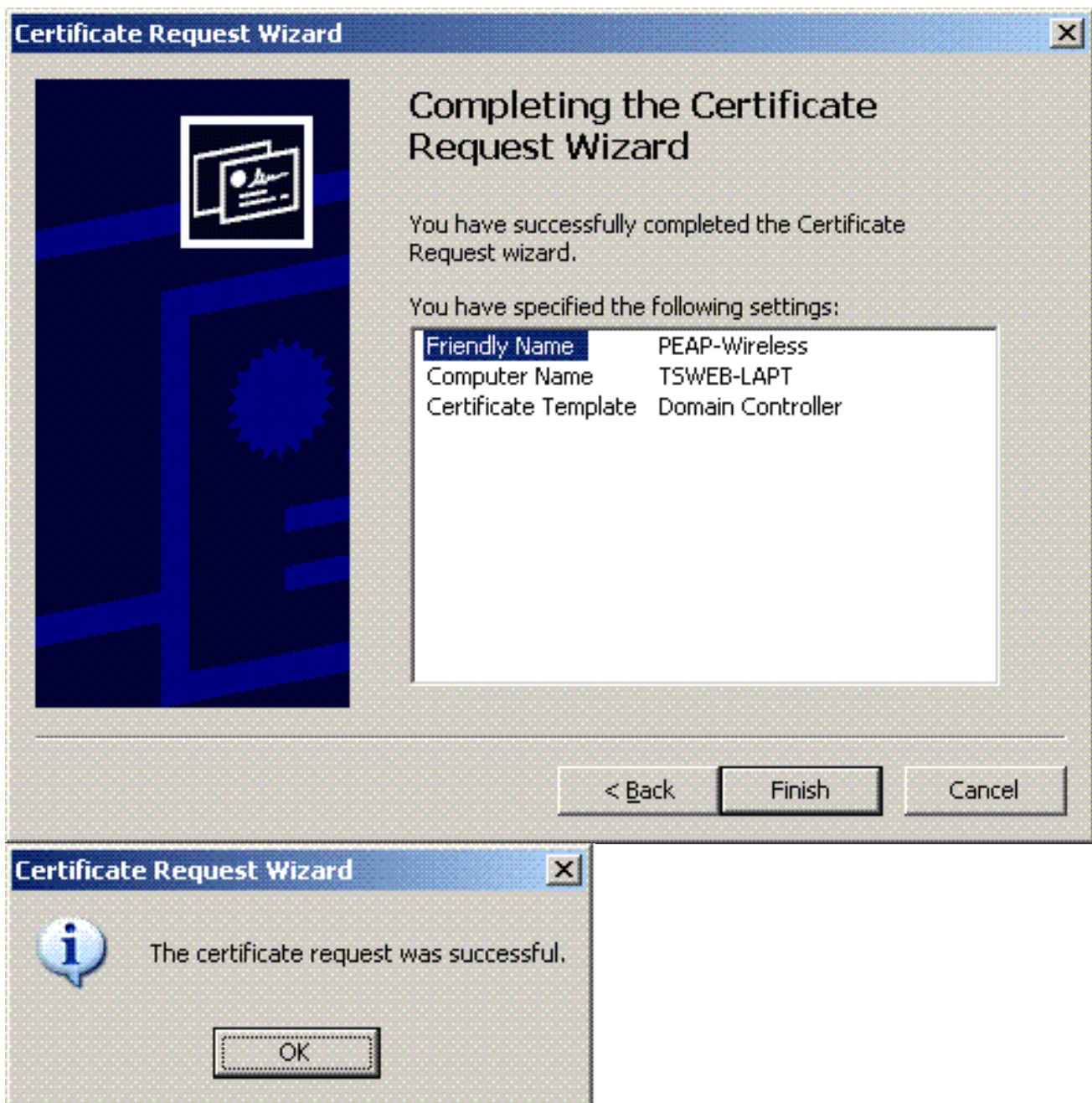
Type a friendly name and description for the new certificate.

Friendly name:

Description:

< Back Next > Cancel

18. Fare clic su **Fine** per completare la procedura guidata per la richiesta di certificazione.

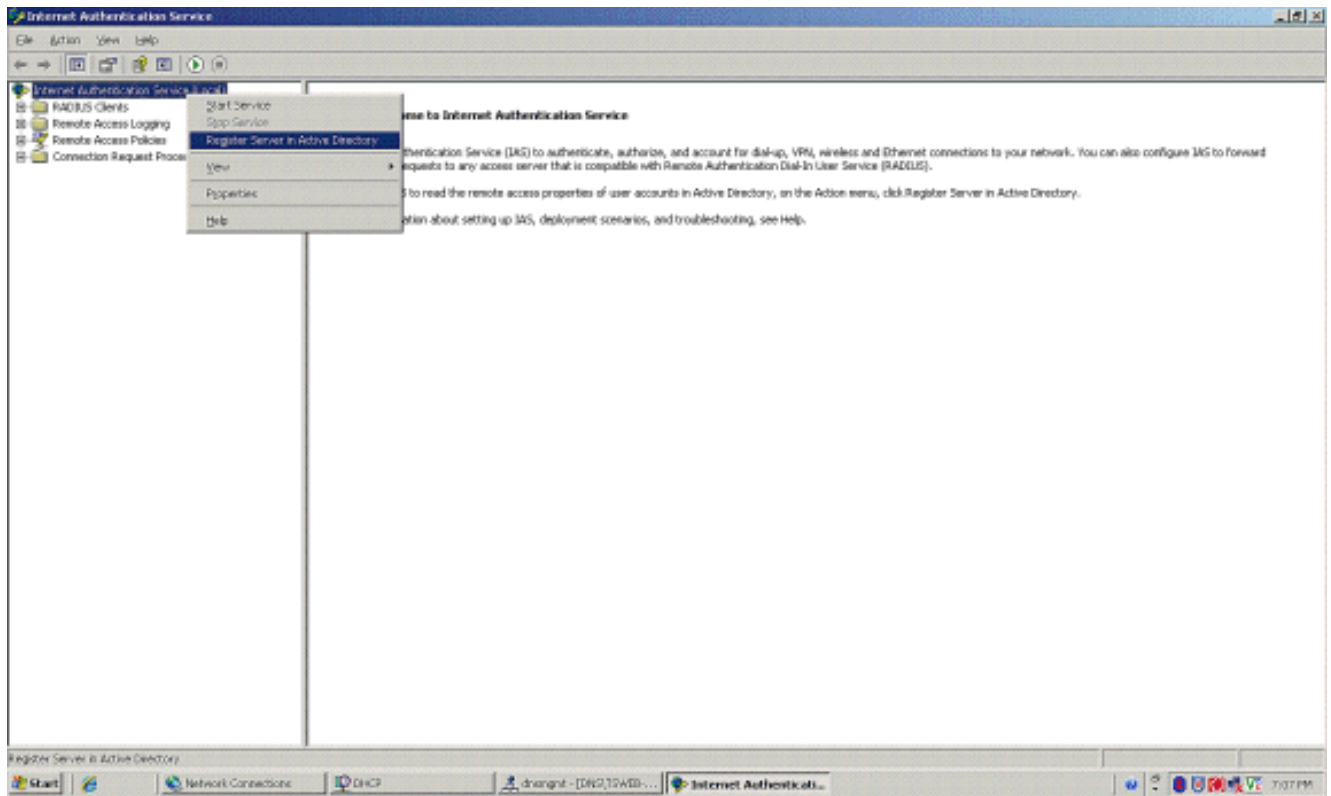


[Configurare il servizio di autenticazione Internet per l'autenticazione PEAP-MS-CHAP v2](#)

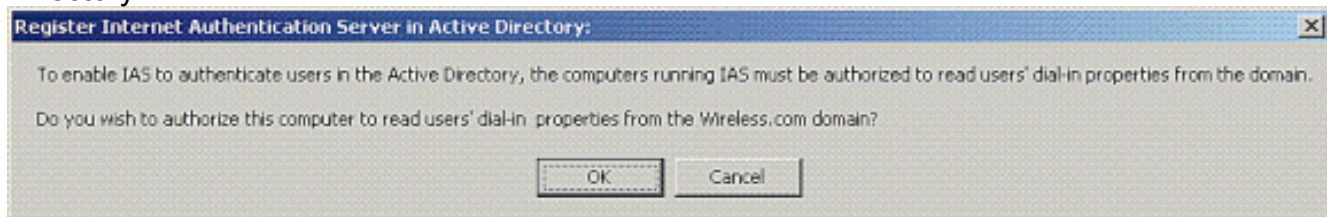
Dopo aver installato e richiesto un certificato per IAS, configurare IAS per l'autenticazione.

Attenersi alla seguente procedura:

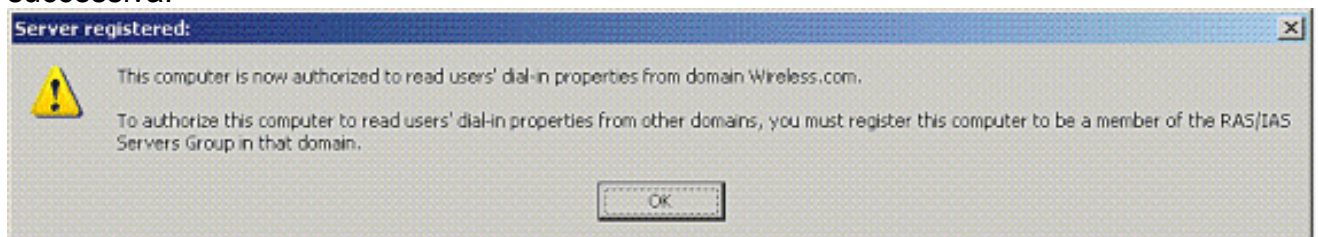
1. Fare clic su **Start > Programmi > Strumenti di amministrazione**, quindi fare clic su Snap-in **Servizio di autenticazione Internet**.
2. Fare clic con il pulsante destro del mouse su **Servizio di autenticazione Internet (IAS)** e quindi scegliere **Registra servizio in Active Directory**.



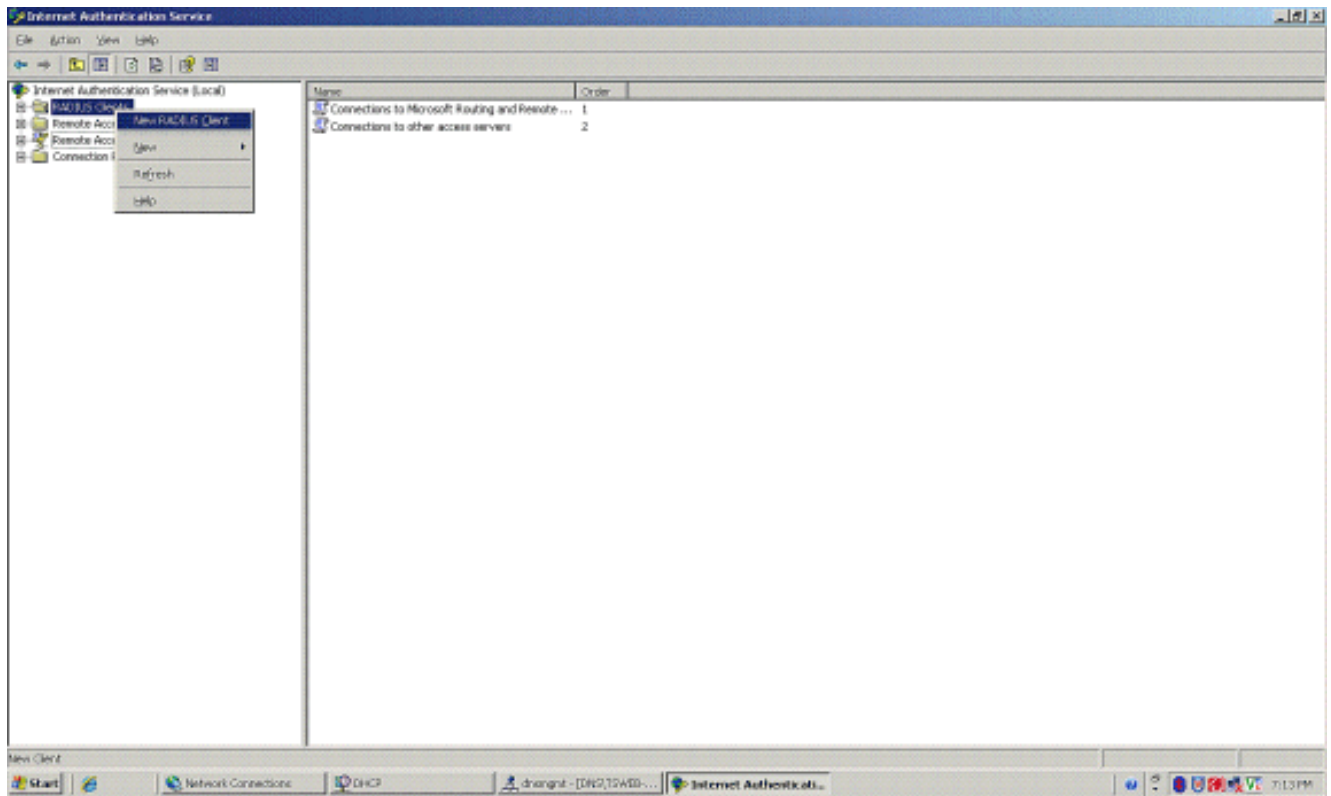
3. Verrà visualizzata la finestra di dialogo **Registra servizio di autenticazione Internet in Active Directory**. Fare clic su **OK**. In questo modo IAS è in grado di autenticare gli utenti in Active Directory.



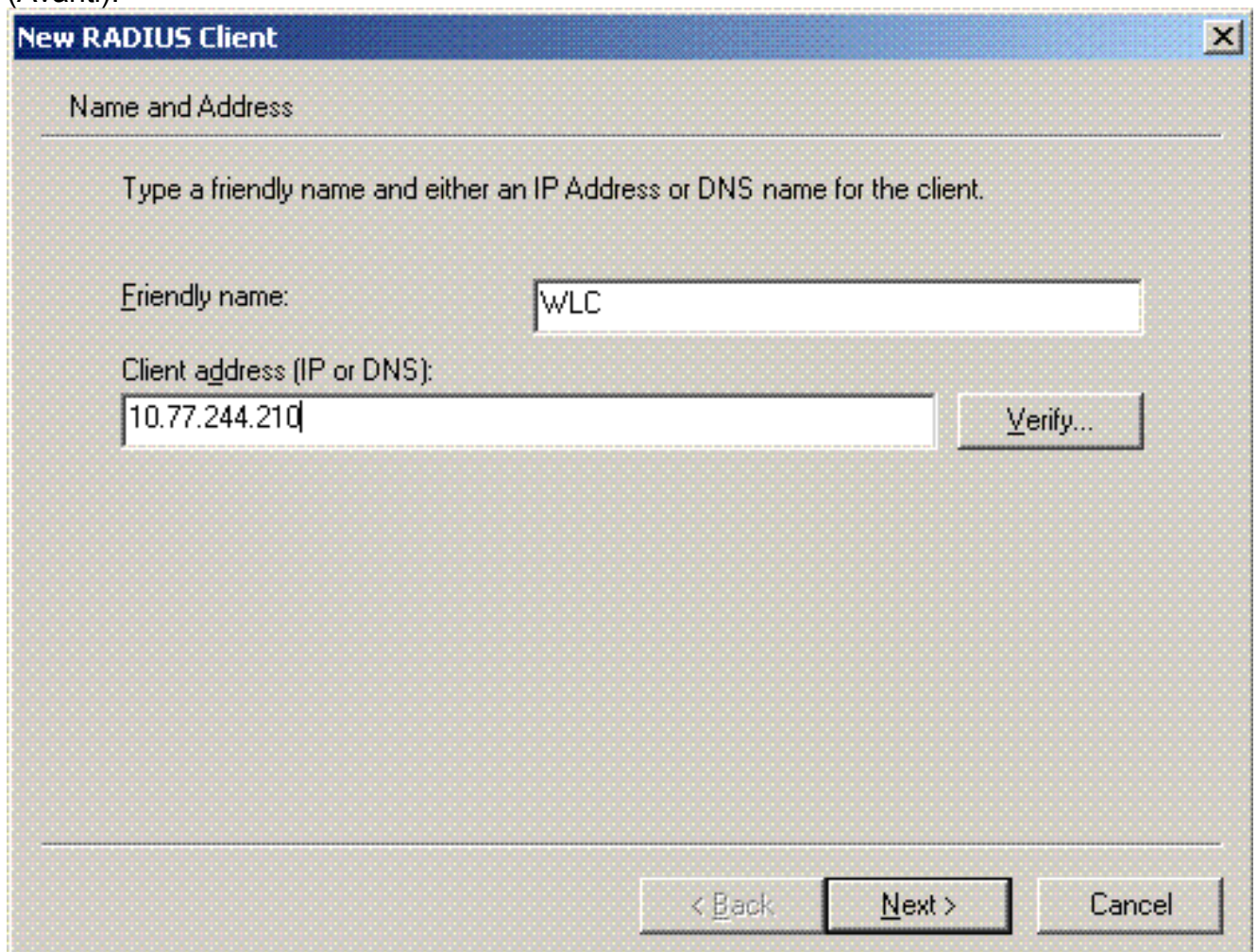
4. Fate clic su **OK** nella finestra di dialogo successiva.



5. Aggiungere il controller LAN wireless come client AAA sul server MS IAS.
6. Fare clic con il pulsante destro del mouse su **Client RADIUS**, quindi scegliere **Nuovo client RADIUS**.

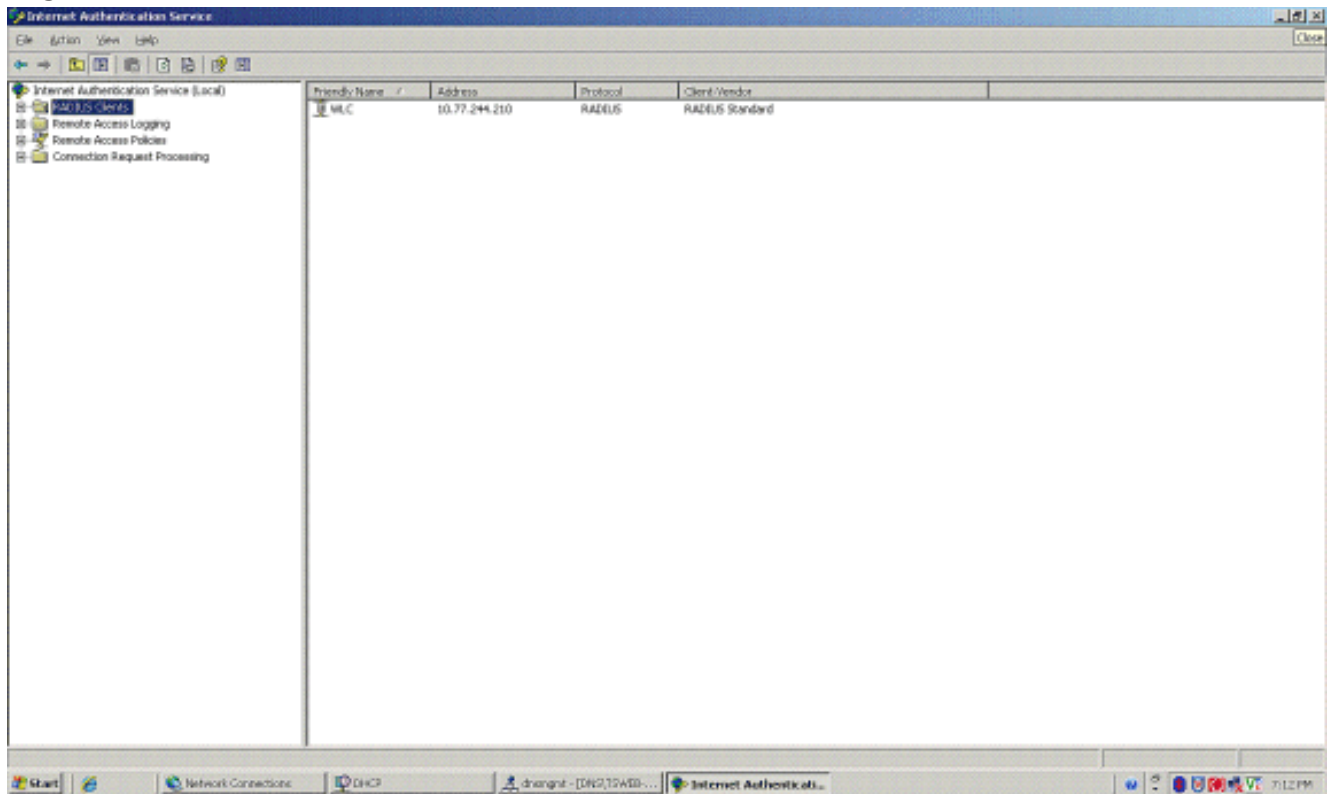


7. Digitare il nome del client (in questo caso WLC) e immettere l'indirizzo IP del WLC. Fare clic su **Next** (Avanti).



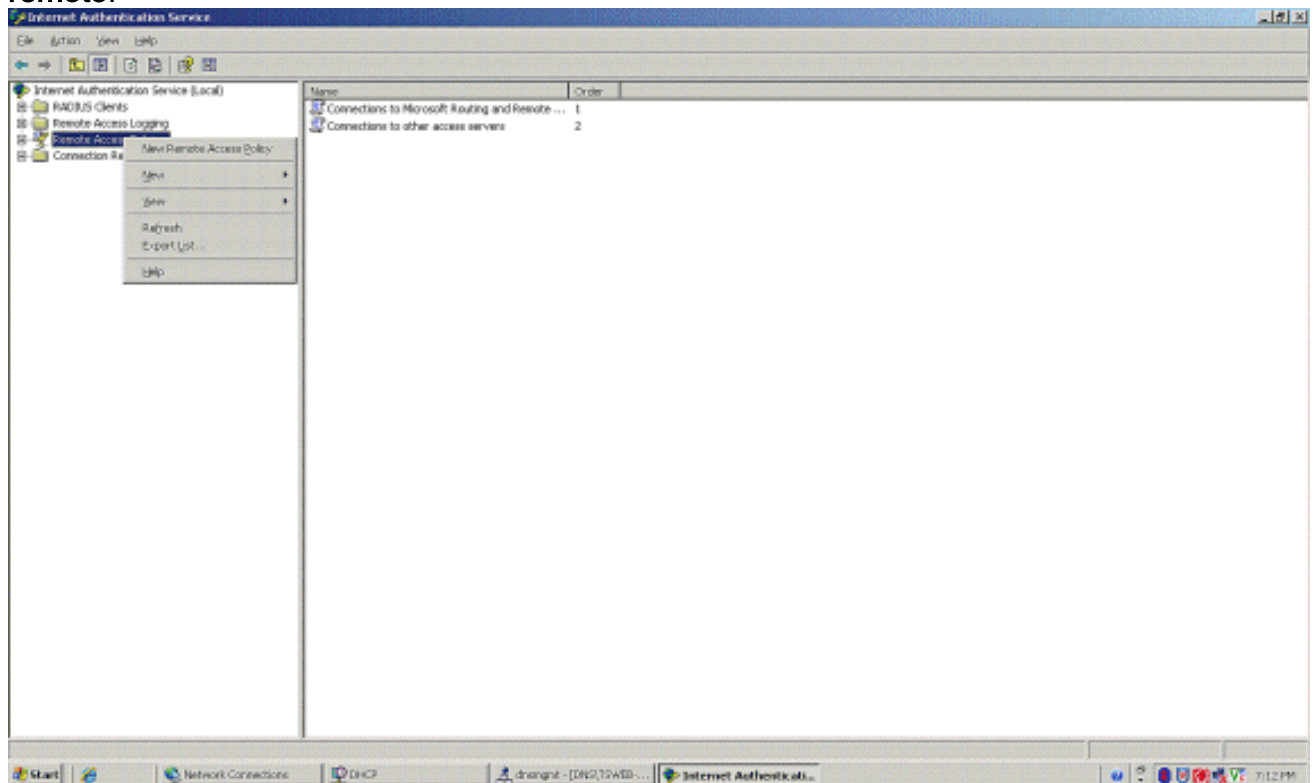
8. Nella pagina successiva, in Client-Vendor, scegliere **RADIUS Standard**, immettere il segreto condiviso e fare clic su **Fine**.

9. Notare che il WLC viene aggiunto come client AAA sullo IAS.



10. Creare un criterio di accesso remoto per i client.

11. A tale scopo, fare clic con il pulsante destro del mouse su **Criteri di accesso remoto** e scegliere **Nuovi criteri di accesso remoto**.




12. Digitare un nome per il criterio di accesso remoto. Nell'esempio, utilizzare il nome **PEAP**. Quindi fare clic su **Avanti**.

New Remote Access Policy Wizard [X]

Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.



How do you want to set up this policy?

Use the wizard to set up a typical policy for a common scenario

Set up a custom policy

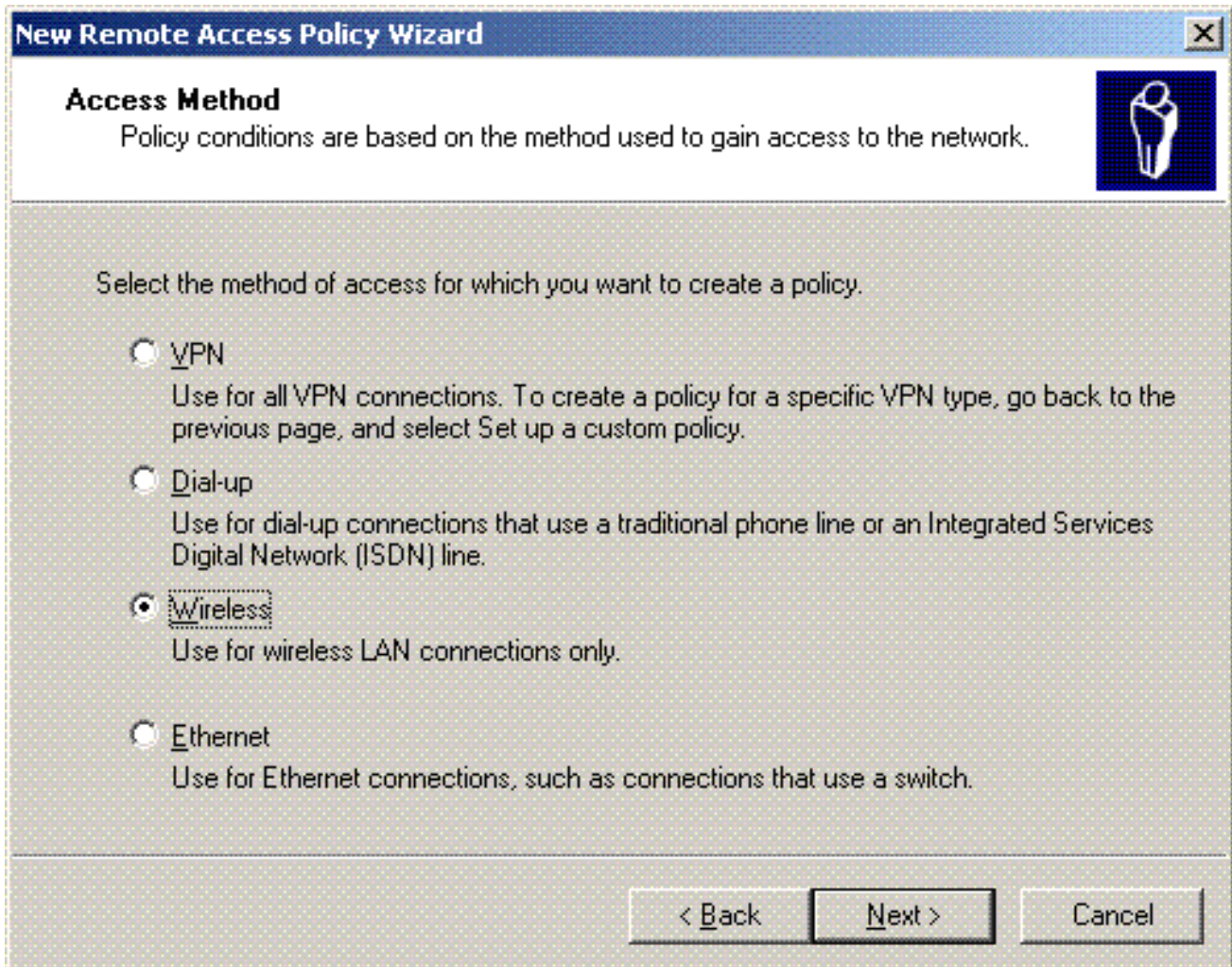
Type a name that describes this policy.

Policy name:

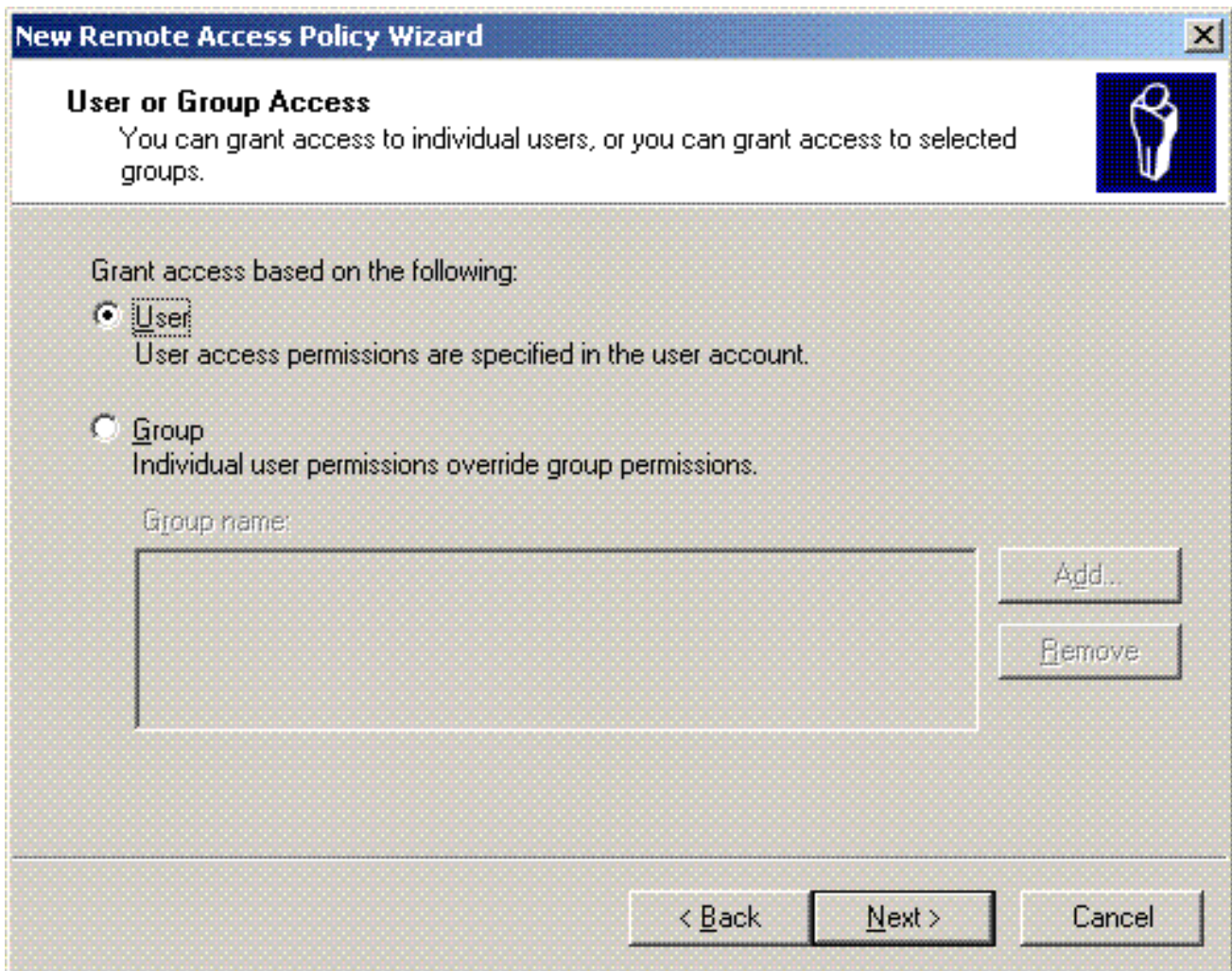
Example: Authenticate all VPN connections.

< Back Next > Cancel

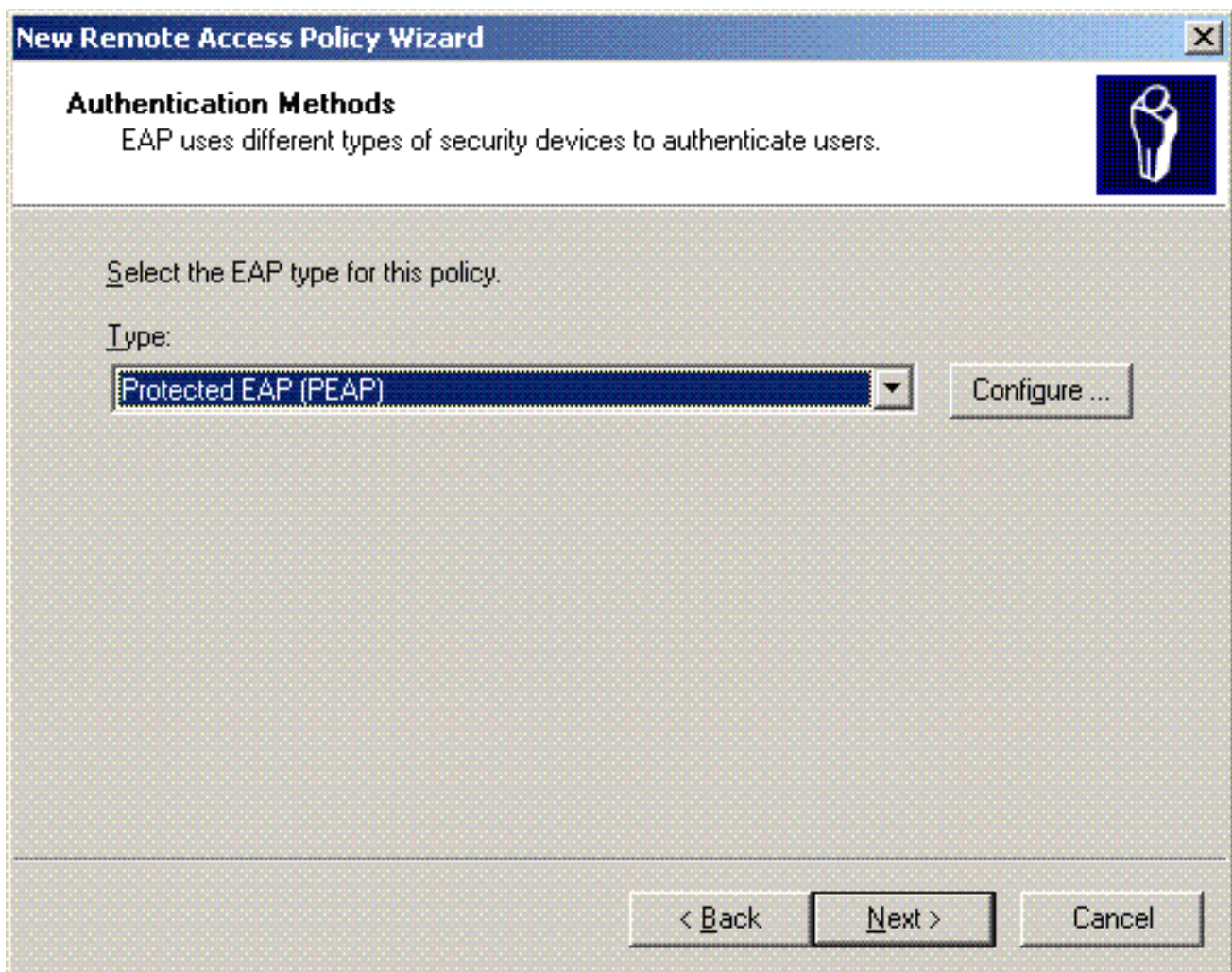
13. Scegliere gli attributi dei criteri in base alle proprie esigenze. In questo esempio, scegliere **Wireless**.



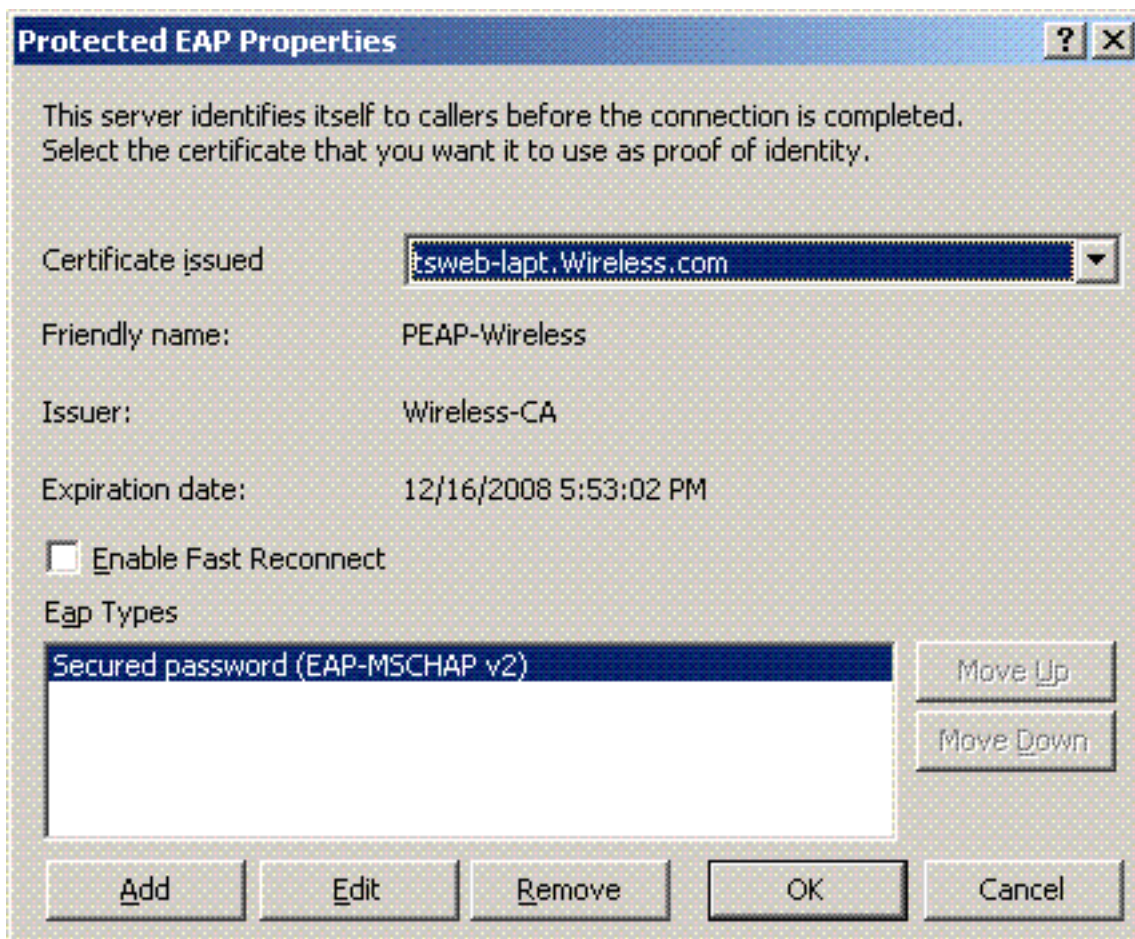
14. Nella pagina successiva scegliere **Utente** per applicare il criterio di accesso remoto all'elenco di utenti.



15. In Metodi di autenticazione scegliere **PEAP (Protected EAP)**, quindi fare clic su **Configura**.

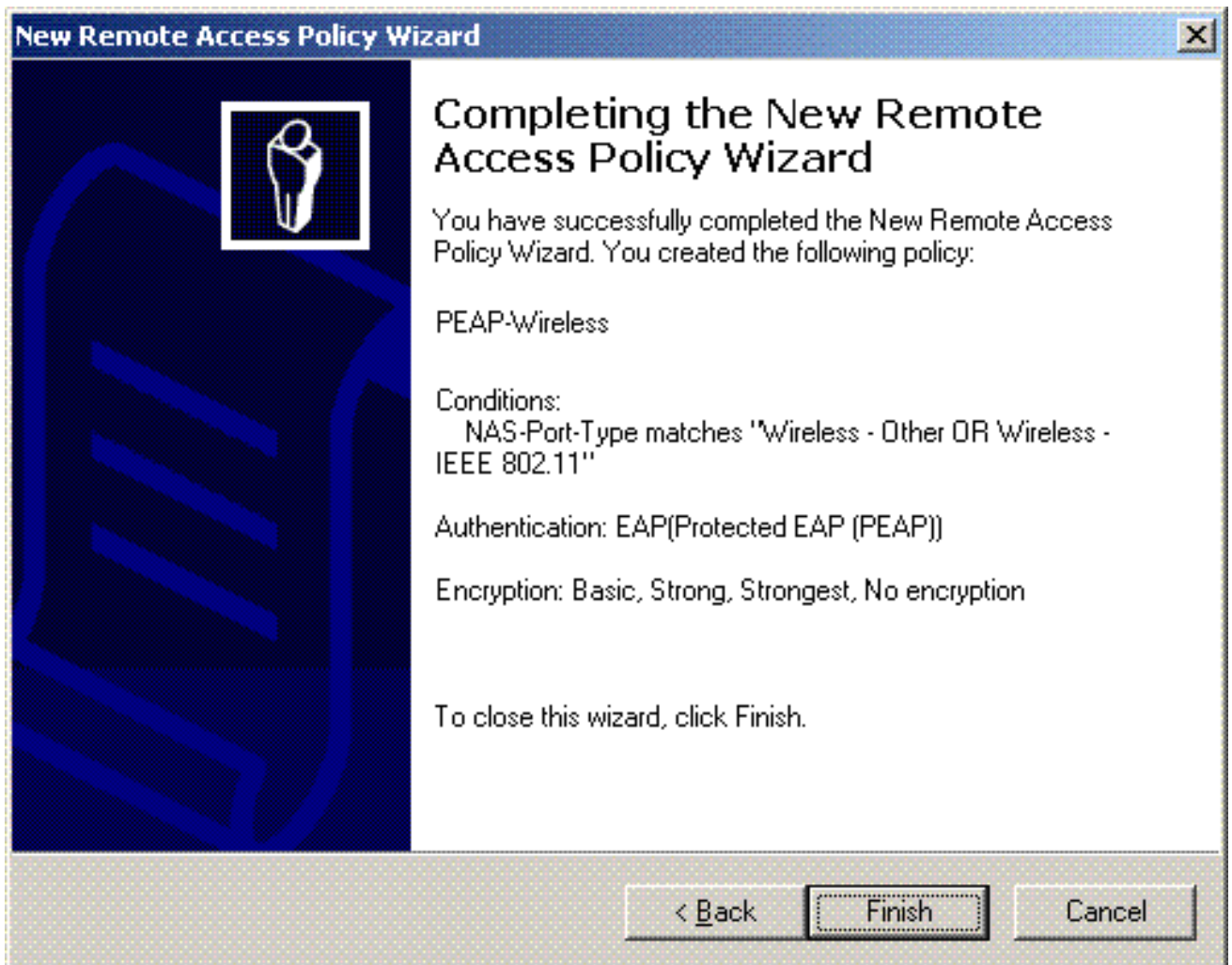


16. Nella pagina **Proprietà PEAP**, scegliere il certificato appropriato dal menu a discesa
Certificato emesso e fare clic su

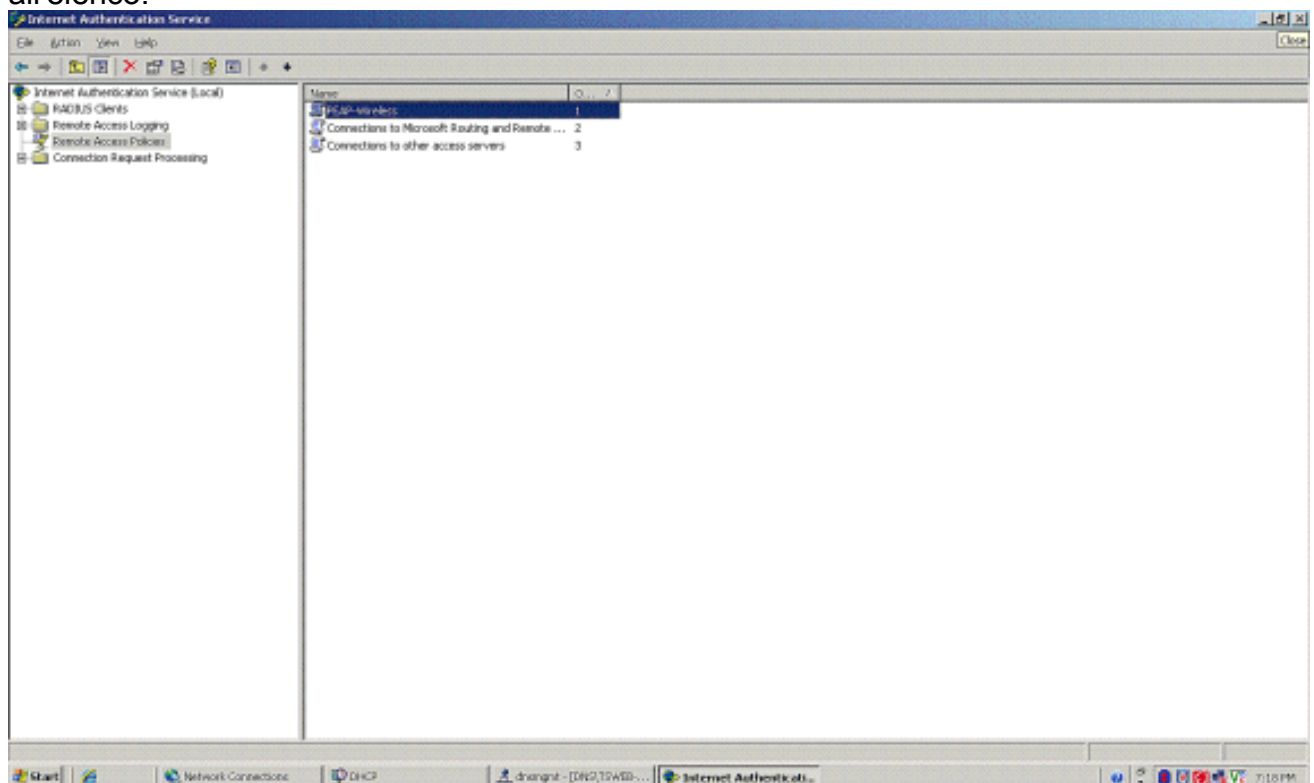


OK.

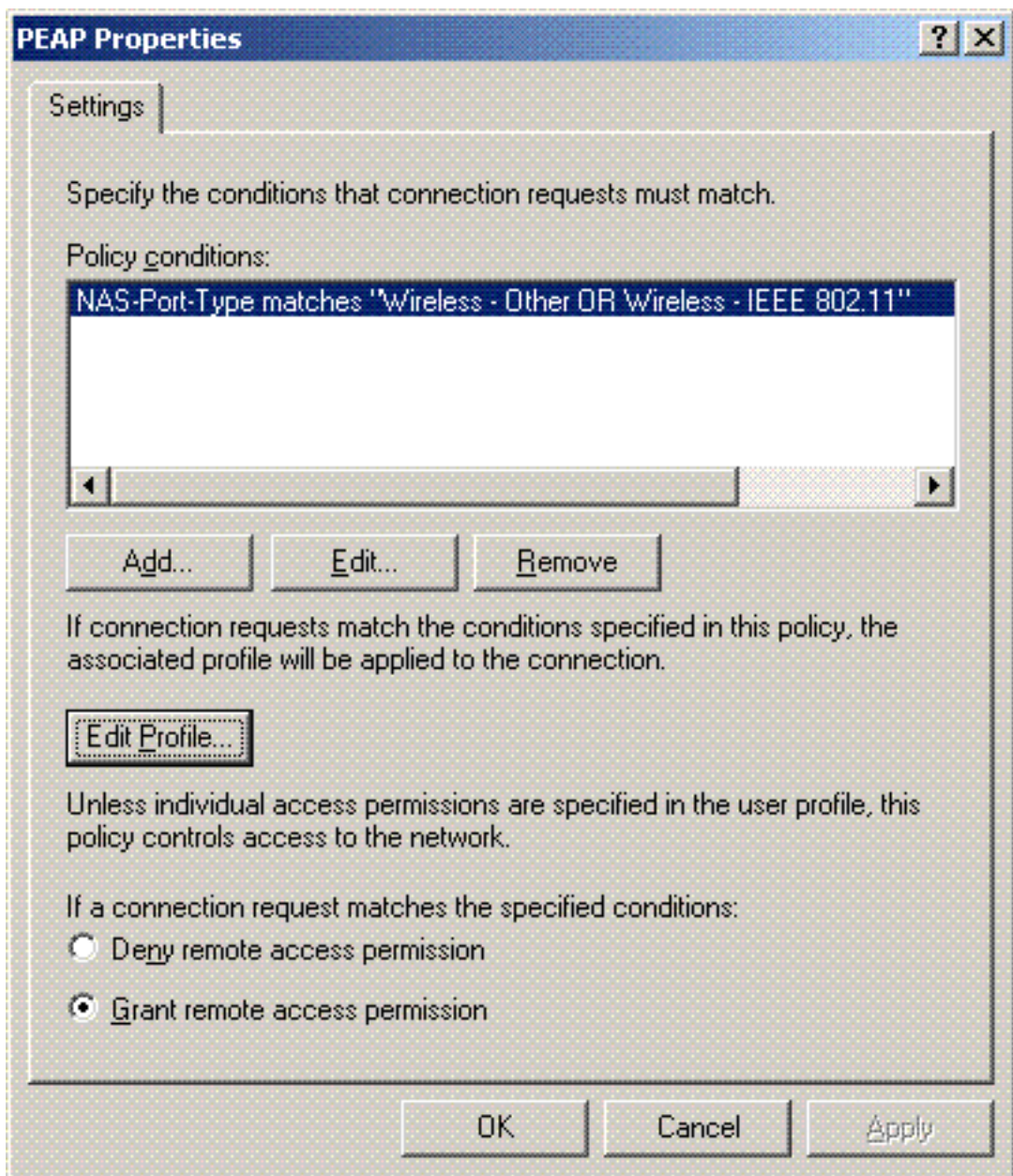
17. Verificare i dettagli dei criteri di accesso remoto e fare clic su **Fine**.



18. I criteri di accesso remoto sono stati aggiunti all'elenco.



19. Fare clic con il pulsante destro del mouse sul criterio e quindi scegliere **Proprietà**. Scegliere "Concedi autorizzazione di accesso remoto" in "Se una richiesta di connessione soddisfa le condizioni"



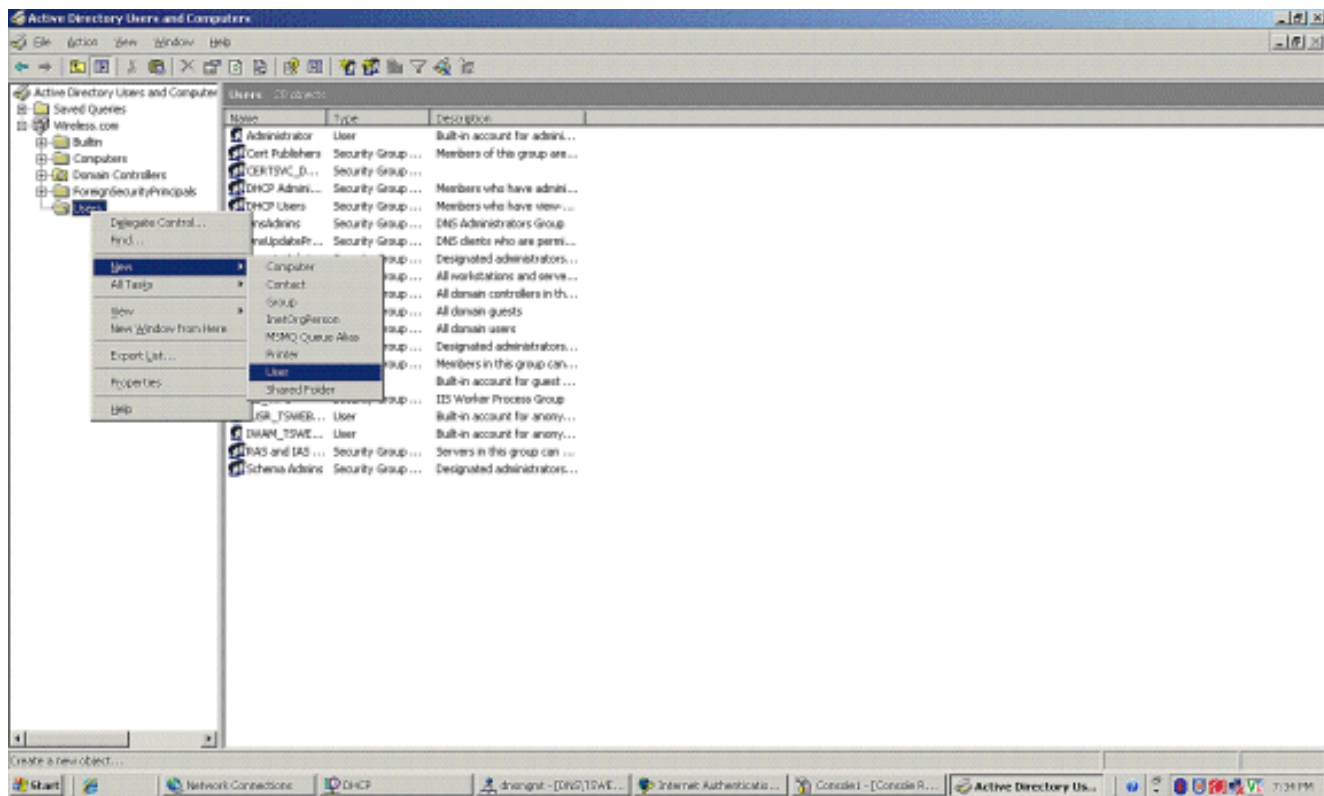
specificate".

[Aggiungi utenti ad Active Directory](#)

In questa configurazione, il database degli utenti viene gestito in Active Directory.

Per aggiungere utenti al database di Active Directory, attenersi alla seguente procedura:

1. Nell'albero della console Utenti e computer di Active Directory fare clic con il pulsante destro del mouse su **Utenti**, scegliere **Nuovo** e quindi fare clic su **Utente**.




2. Nella finestra di dialogo Nuovo oggetto - Utente digitare il nome dell'utente wireless. In questo esempio viene utilizzato il nome **WirelessUser** nel campo Nome e **WirelessUser** nel campo Nome di accesso utente. Fare clic su **Next**

(Avanti).

3. Nella finestra di dialogo Nuovo oggetto - Utente digitare una password a scelta nei campi Password e Conferma password. Deselezionare la casella di controllo **Cambiamento obbligatorio password all'accesso successivo** e fare clic su

New Object - User [X]

 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

Avanti.

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

New Object - User [X]

 Create in: Wireless.com/Users

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

Full name: Client 1

User logon name: Client1@Wireless.com

< Back Finish Cancel

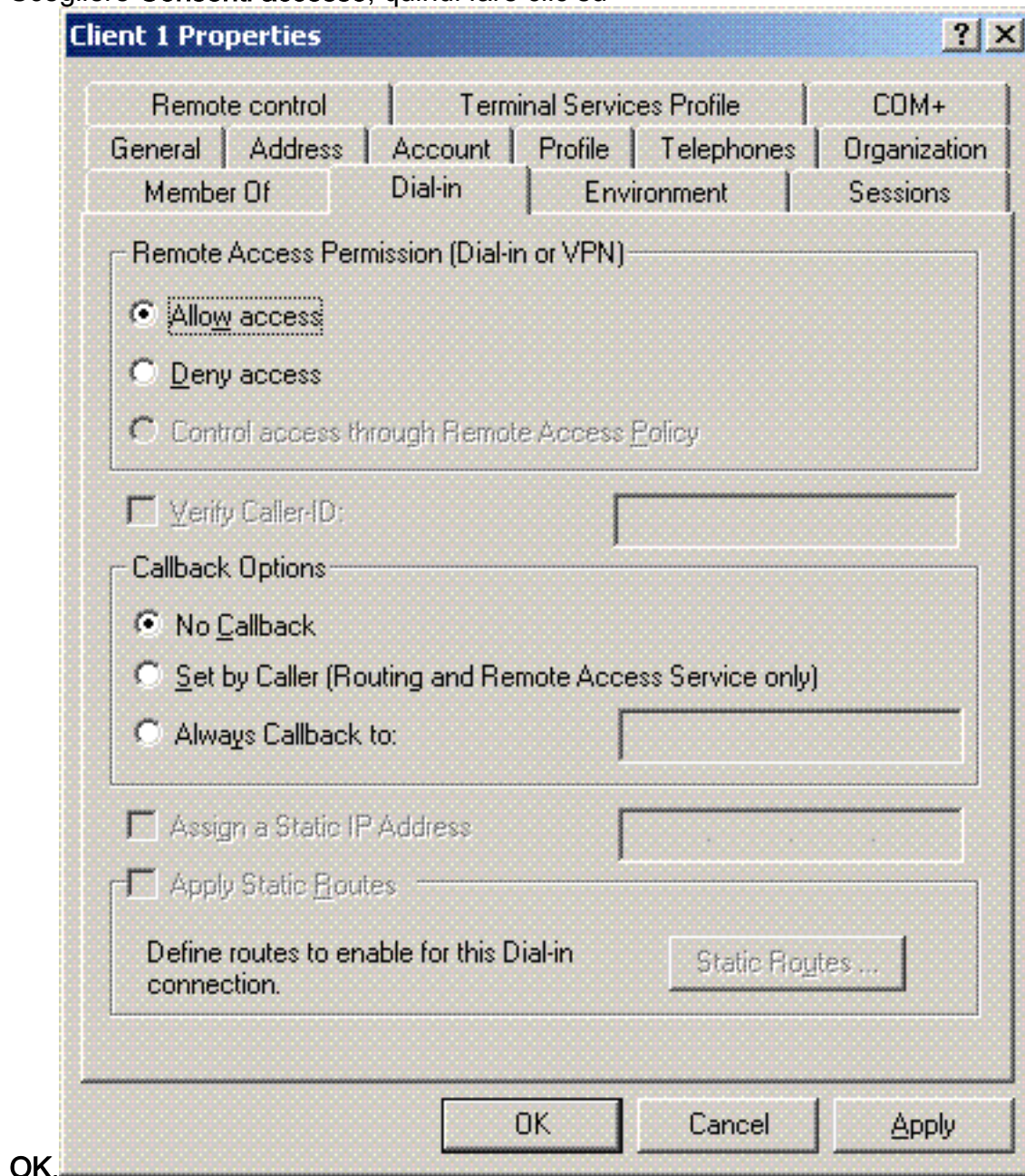
Fine.

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

Consenti accesso wireless agli utenti

Attenersi alla seguente procedura:

1. Nell'albero della console Utenti e computer di Active Directory fare clic sulla cartella **Utenti**, fare clic con il pulsante destro del mouse su **WirelessUser**, scegliere **Proprietà** e quindi passare alla **scheda Connessione remota**.
2. Scegliere **Consenti accesso**, quindi fare clic su



OK.

Configurazione del controller LAN wireless e dei Lightweight Access Point

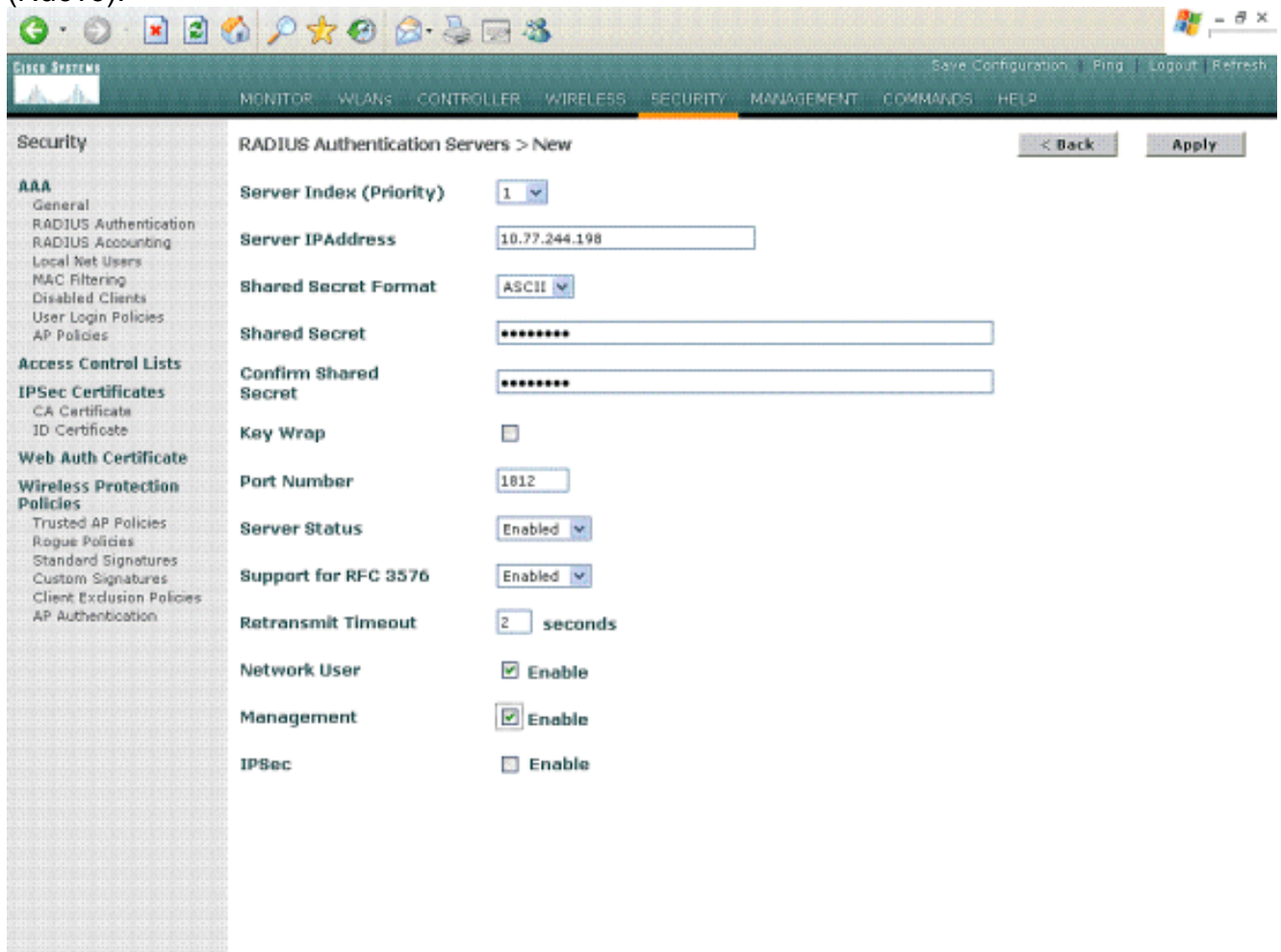
Configurare ora le periferiche wireless per questa installazione. tra cui la configurazione dei Wireless LAN Controller, dei Lightweight Access Point e dei client wireless.

[Configurare il WLC per l'autenticazione RADIUS tramite il server MS IAS RADIUS](#)

Configurare innanzitutto il WLC in modo che utilizzi MS IAS 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. A tale scopo, aggiungere il server MS IAS come server RADIUS nella pagina **Sicurezza > Autenticazione RADIUS**.

Attenersi alla seguente procedura:

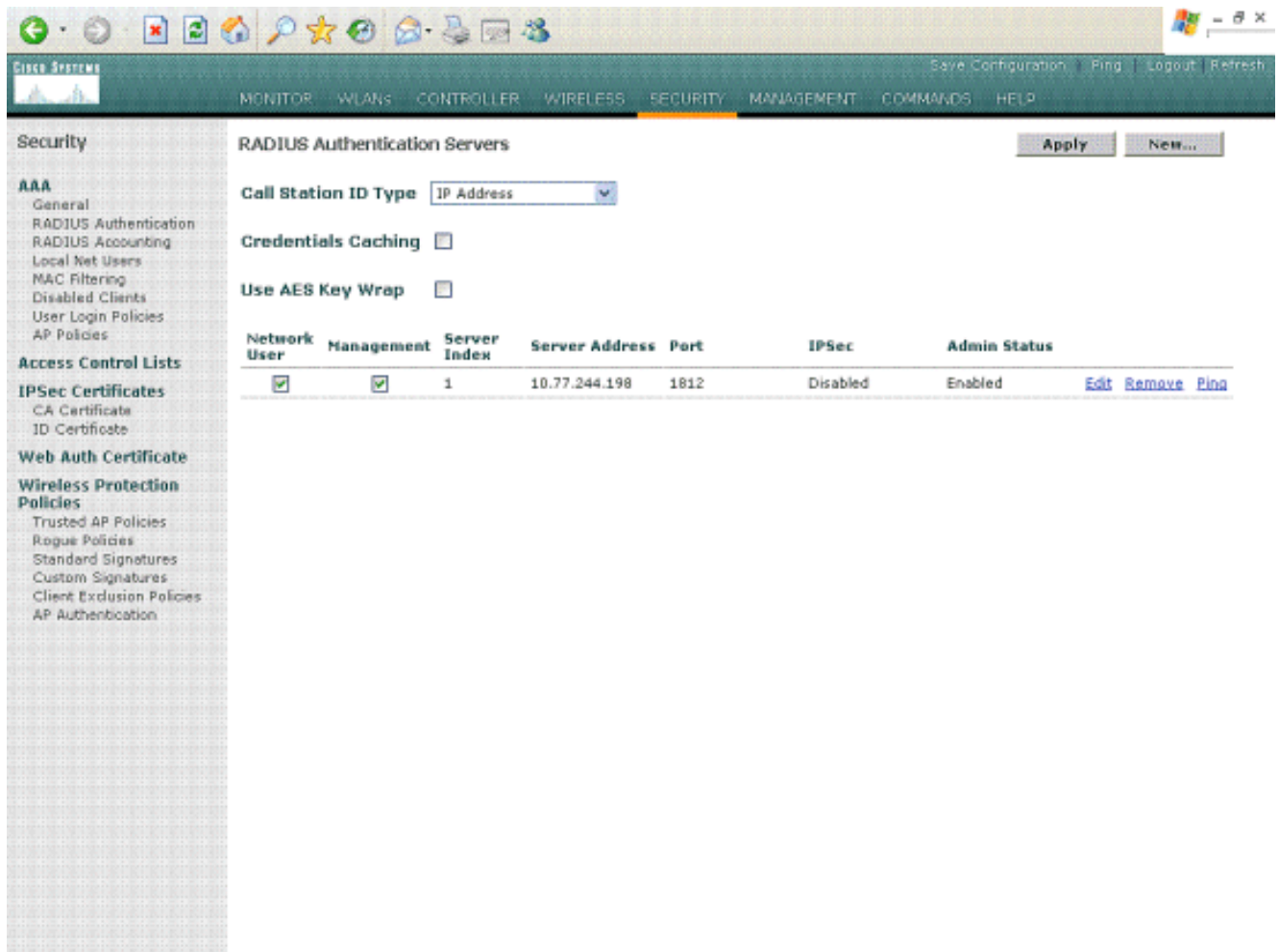
1. Scegliere **Sicurezza e Autenticazione RADIUS** dall'interfaccia utente del controller per visualizzare la pagina Server di autenticazione RADIUS. Per definire un server RADIUS, fare clic su **New** (Nuovo).



The screenshot shows the Cisco Systems configuration interface for RADIUS Authentication Servers. The page title is "RADIUS Authentication Servers > New". The interface includes a navigation menu on the left with categories like AAA, Access Control Lists, IPsec Certificates, Web Auth Certificate, Wireless Protection Policies, and IPsec. The main configuration area contains the following fields:

Field	Value
Server Index (Priority)	1
Server IP Address	10.77.244.198
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/>
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Retransmit Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPsec	<input type="checkbox"/> Enable

2. Definire i parametri del server RADIUS nella pagina **Server di autenticazione RADIUS > Nuovo**. 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 consentono di determinare se l'autenticazione basata su RADIUS è valida per gli utenti di rete e di gestione. In questo esempio viene utilizzato MS IAS come server RADIUS con indirizzo IP 10.77.244.198.



3. Fare clic su **Apply** (Applica).
4. Il server MS IAS è stato aggiunto al WLC come server Radius e può essere utilizzato per autenticare i client wireless.

Configurazione di una WLAN per i client

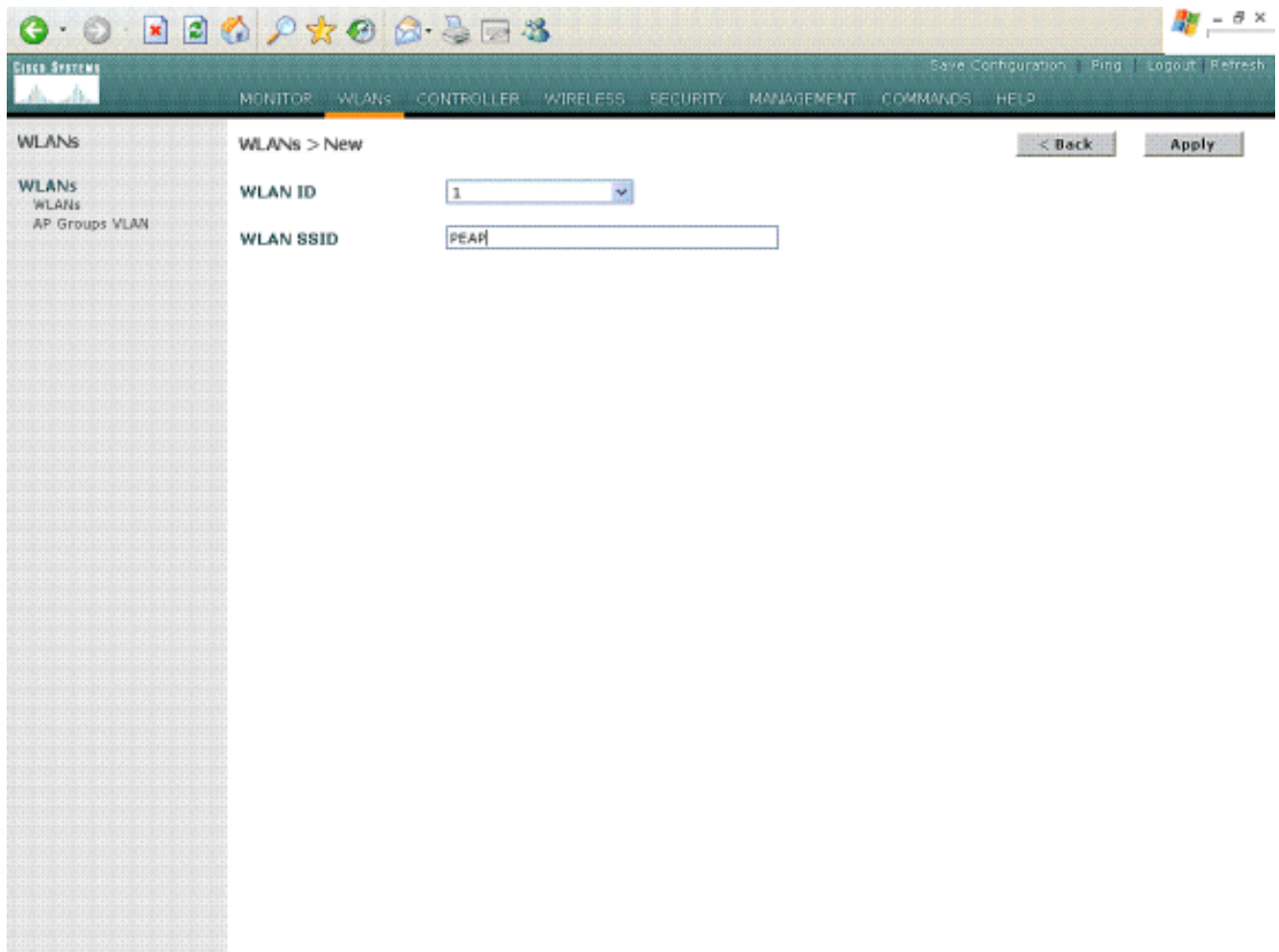
Configurare il SSID (WLAN) a cui si connettono i client wireless. In questo esempio, creare il SSID e denominarlo **PEAP**.

Definire l'autenticazione di layer 2 come WPA2 in modo che i client eseguano l'autenticazione basata su EAP (PEAP-MSCHAPv2 in questo caso) e utilizzino AES come meccanismo di crittografia. Mantenere tutti gli altri valori ai valori predefiniti.

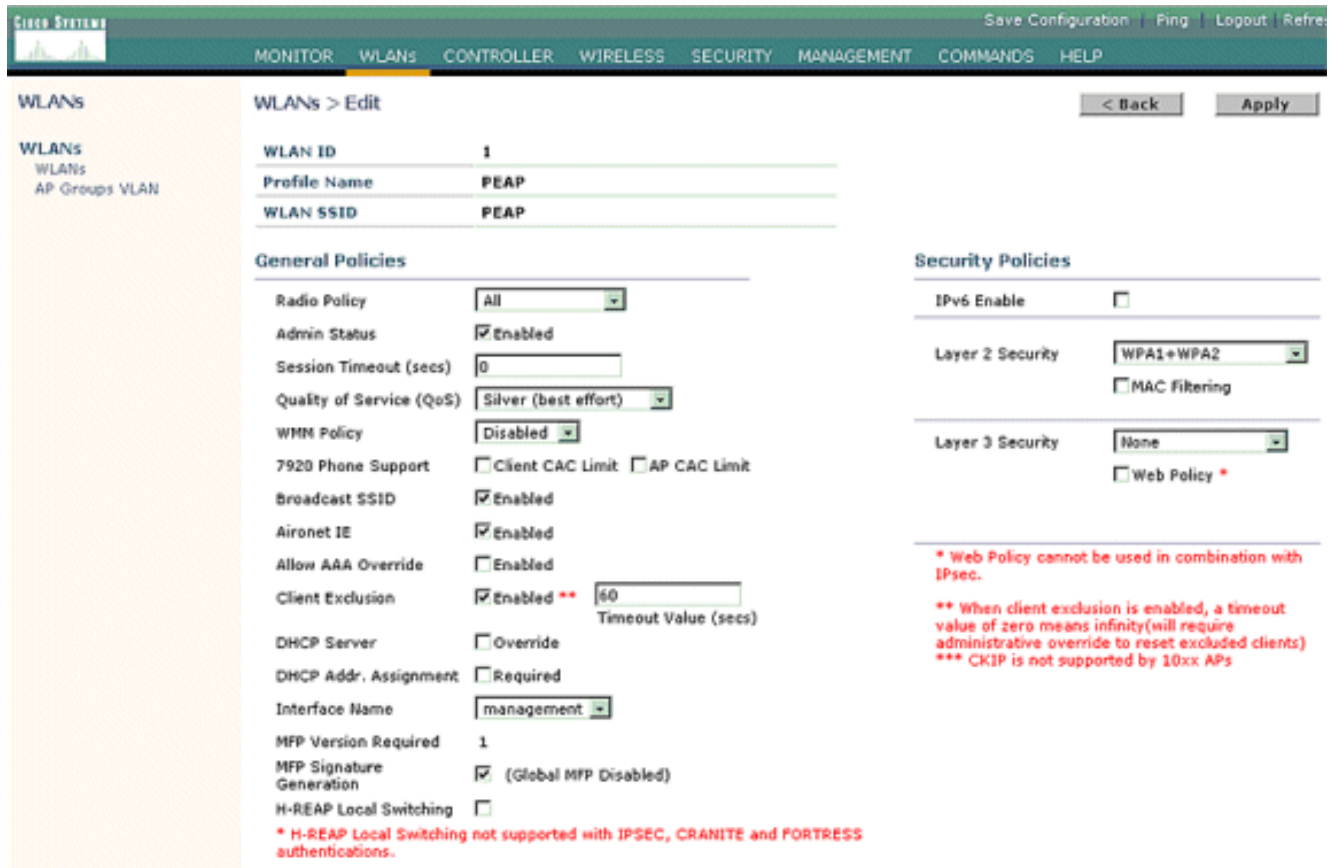
Nota: questo documento associa la WLAN alle interfacce di gestione. Se la rete contiene più VLAN, è possibile creare una VLAN separata e associarla all'SSID. Per informazioni su come configurare le VLAN sui WLC, fare riferimento all'[esempio di configurazione delle VLAN sui controller LAN wireless](#).

Per configurare una WLAN sul WLC, attenersi alla seguente procedura:

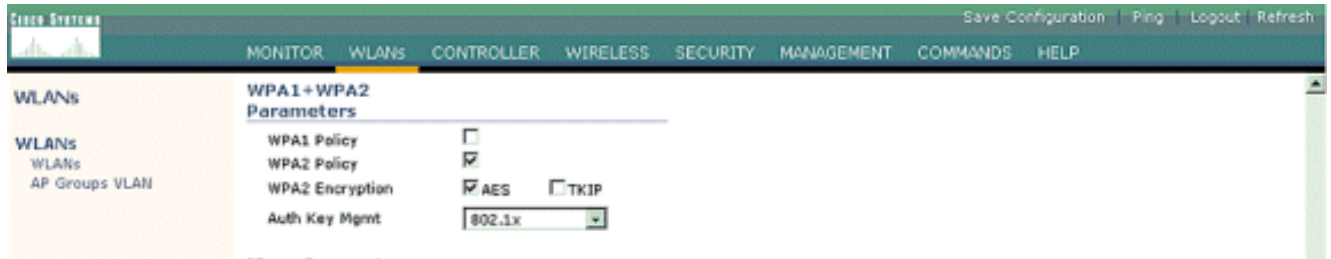
1. Fare clic su **WLAN** dall'interfaccia utente del controller per visualizzare la pagina WLAN. In questa pagina vengono elencate le WLAN esistenti sul controller.
2. Per creare una nuova WLAN, selezionare **New** (Nuovo). Immettere l'ID WLAN e l'SSID WLAN per la WLAN, quindi fare clic su **Applica**.



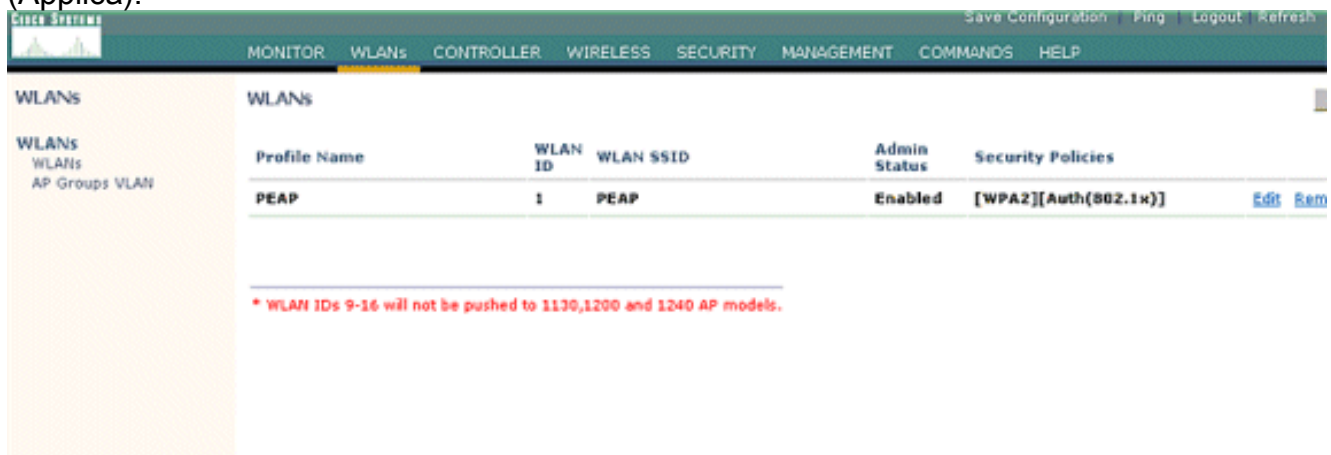
3. Dopo aver creato una nuova WLAN, viene visualizzata la pagina **WLAN > Modifica** per la nuova WLAN. In questa pagina è possibile definire vari parametri specifici per la WLAN, tra cui Criteri generali, Server RADIUS, Criteri di sicurezza e Parametri 802.1x.



- Per abilitare la WLAN, controllare **lo stato dell'amministratore** in Criteri generali. Se si desidera che l'access point trasmetta l'SSID nei frame del beacon, selezionare **Broadcast SSID**.
- In Protezione di livello 2, scegliere **WPA1+WPA2**. Ciò abilita WPA sulla WLAN. Scorrere la pagina verso il basso e scegliere il criterio WPA. In questo esempio viene utilizzata la crittografia WPA2 e AES. Scegliere il server RADIUS appropriato dal menu a discesa in Server RADIUS. Nell'esempio, utilizzare **10.77.244.198** (indirizzo IP del server MS IAS). Gli altri parametri possono essere modificati in base ai requisiti della rete WLAN.



- Fare clic su **Apply** (Applica).



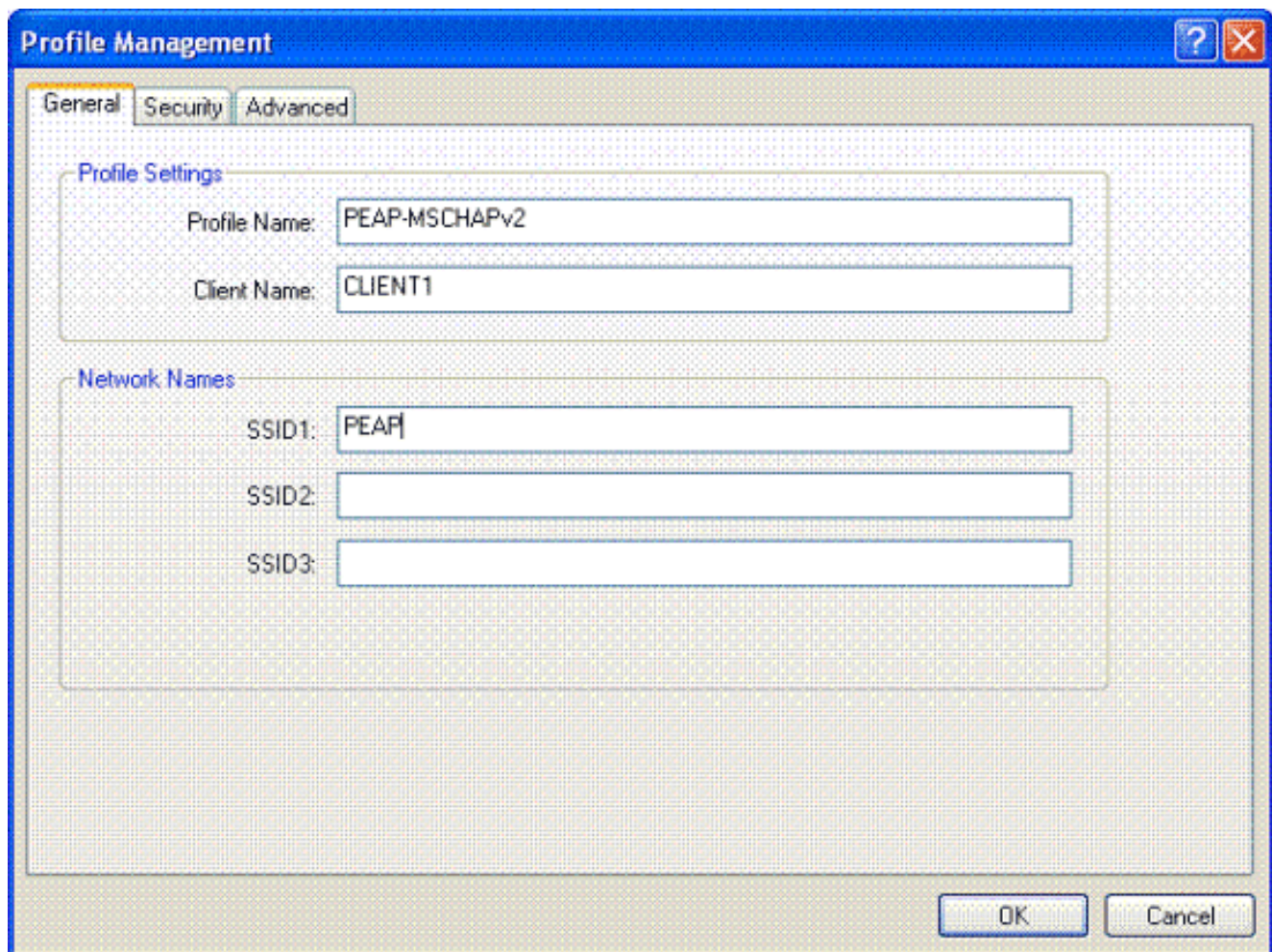
[Configurazione dei client wireless](#)

[Configurazione dei client wireless per l'autenticazione PEAP-MS CHAPv2](#)

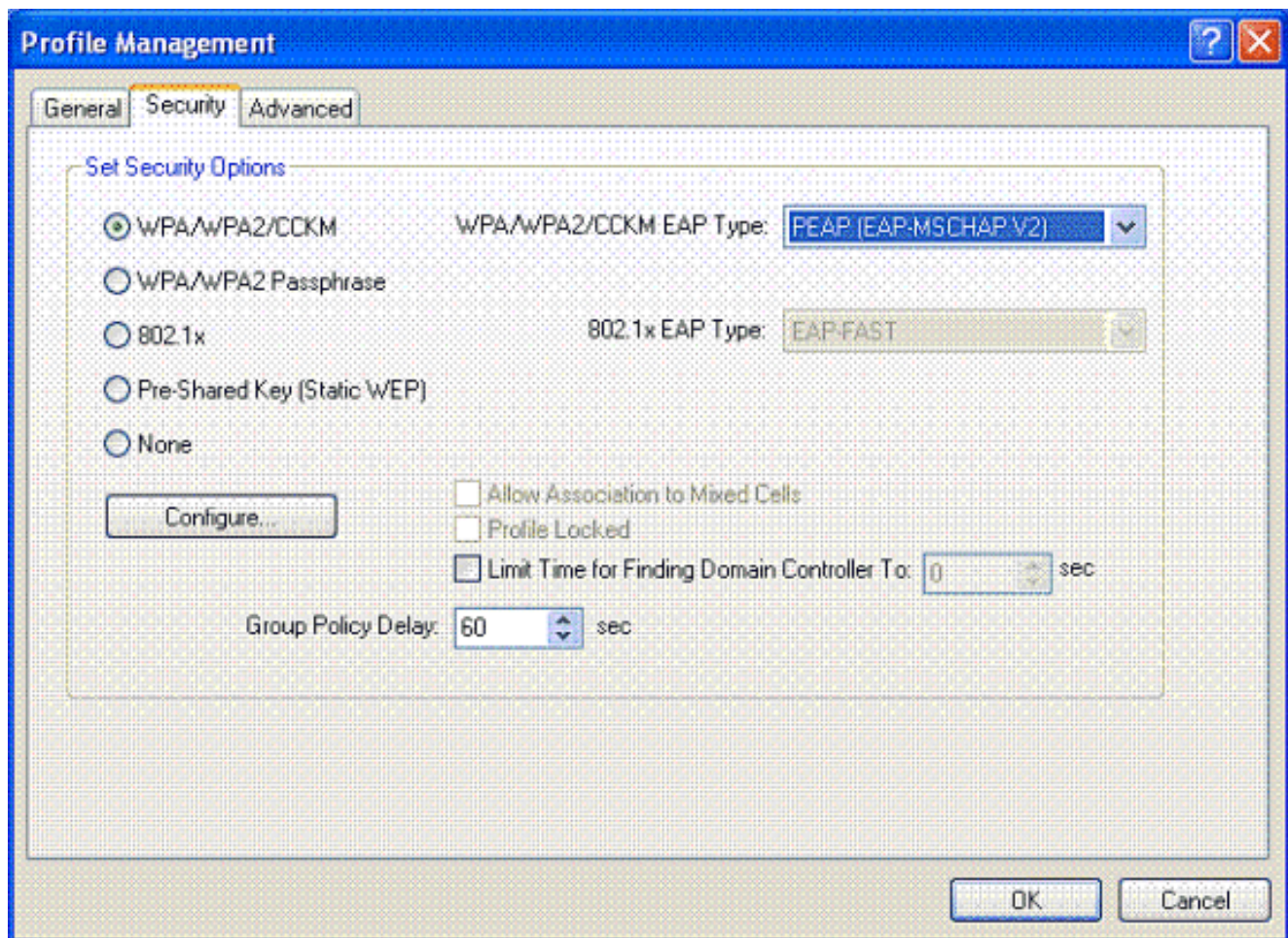
In questo esempio vengono fornite informazioni su come configurare il client wireless con Cisco Aironet Desktop Utility. Prima di configurare l'adattatore client, verificare che sia utilizzata la versione più recente del firmware e dell'utility. La versione più recente del firmware e delle utility è disponibile nella pagina dei download wireless all'indirizzo Cisco.com.

Per configurare la scheda client wireless Cisco Aironet 802.11 a/b/g con l'ADU, attenersi alla seguente procedura:

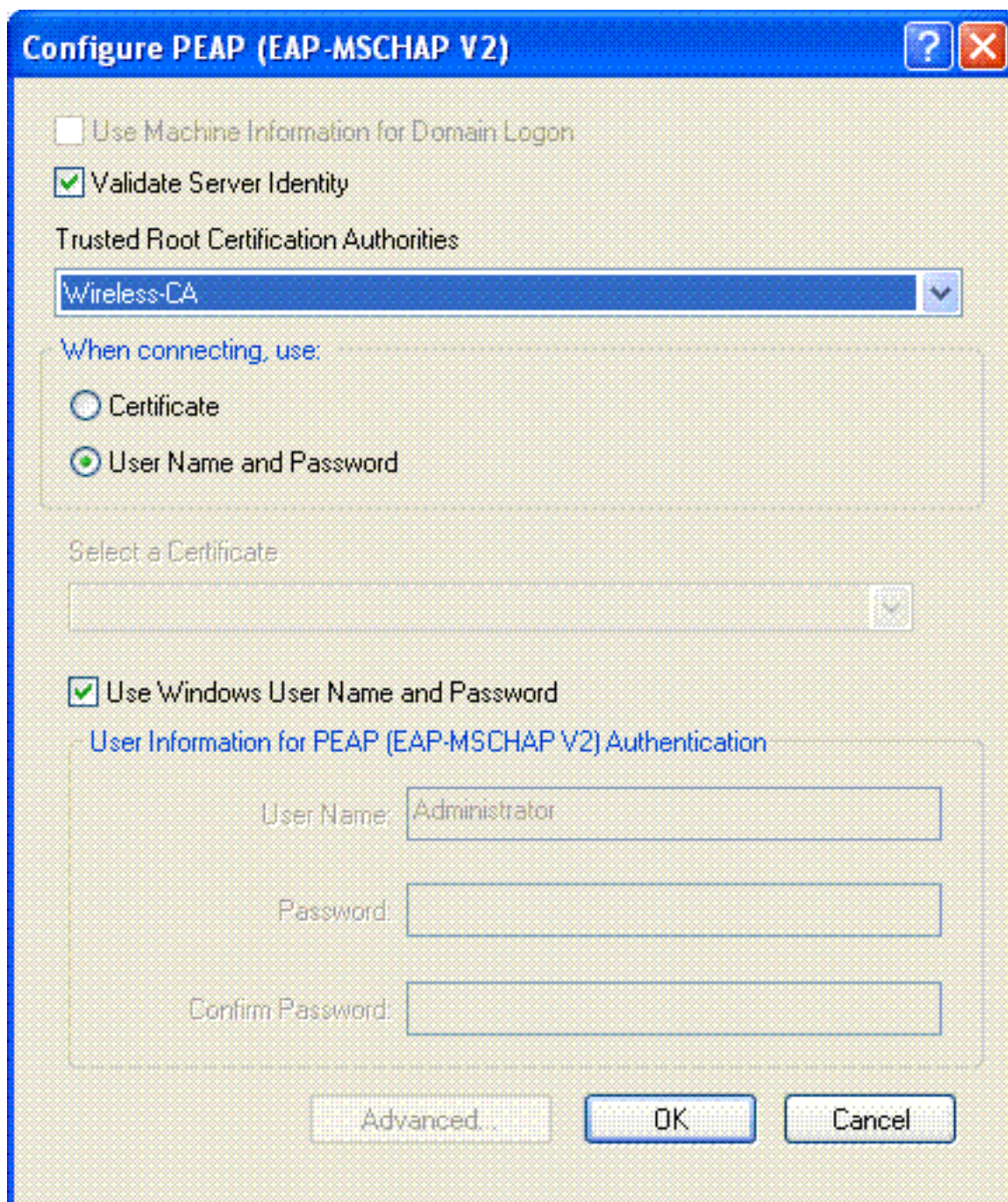
- Aprire Aironet Desktop Utility.
- Fare clic su **Gestione profili**, quindi su **Nuovo** per definire un profilo.
- Nella scheda Generale, immettere il nome del profilo e il SSID. Nell'esempio, utilizzare il SSID configurato sul WLC (PEAP).



4. Selezionare la scheda Protezione, scegliere **WPA/WPA2/CCKM**, in WPA/WPA2/CCKM EAP digitare choose **PEAP [EAP-MSCHAPv2]**, quindi fare clic su **Configura**.



5. Scegliere **Convalida certificato server**, quindi **Wireless-CA** dal menu a discesa Autorità di certificazione fonti

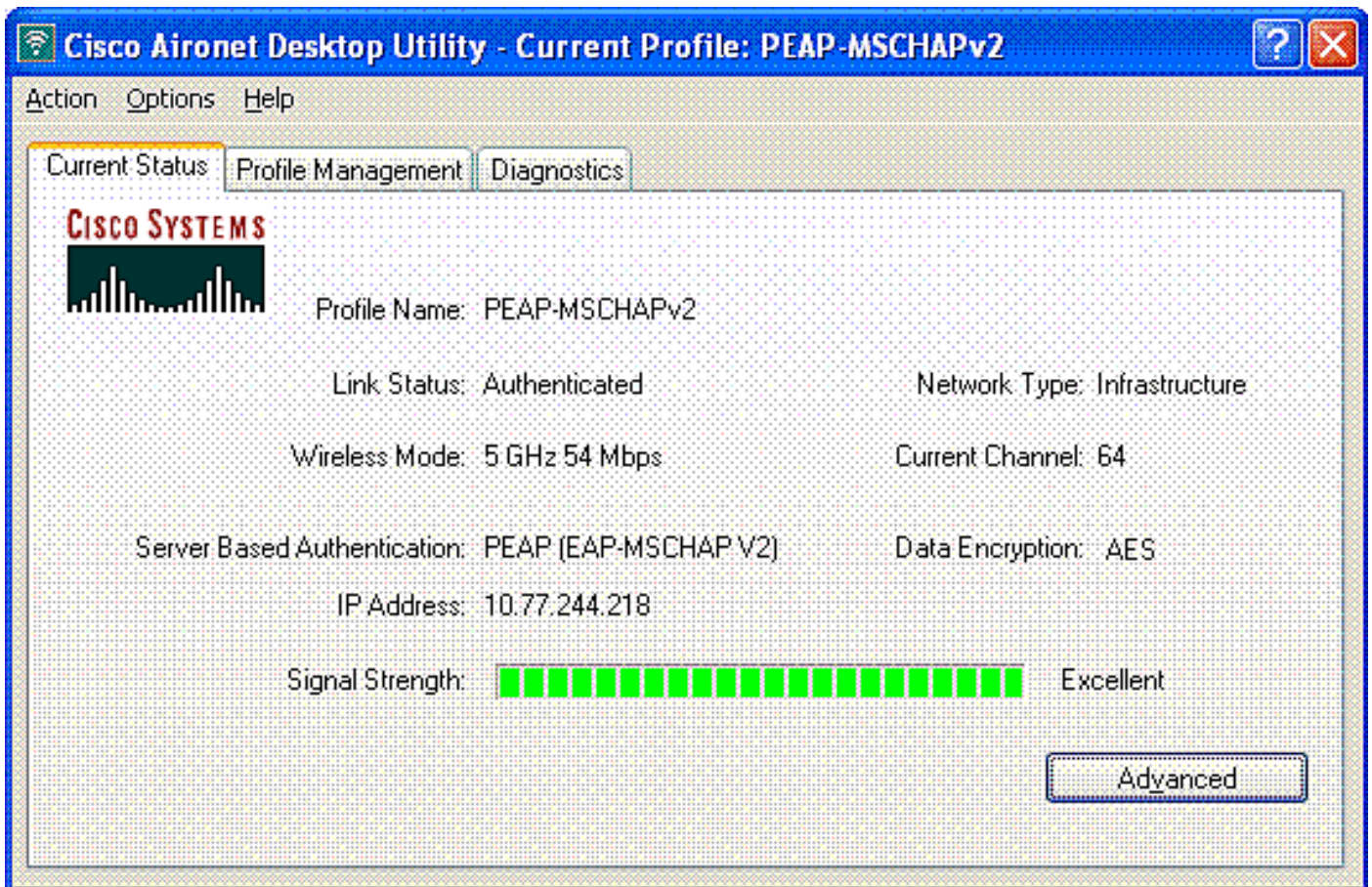


attendibili.

6. Fare clic su **OK** e attivare il profilo. **Nota:** quando si utilizza PEAP-MSCHAPv2 (Protected EAP-Microsoft Challenge Handshake Authentication Protocol versione 2) con Microsoft XP SP2 e la scheda wireless è gestita da Microsoft Wireless Zero Configuration (WZC), è necessario applicare l'hotfix KB885453 di Microsoft. In questo modo si evitano diversi problemi di autenticazione relativi alla funzionalità di ripristino rapido di PEAP.

Verifica e risoluzione dei problemi

Per verificare se la configurazione funziona come previsto, attivare il profilo PEAP-MSCHAPv2 sul client wireless Client1.



Una volta attivato il profilo PEAP-MSCHAPv2 sull'ADU, il client esegue l'autenticazione 802.11 open e quindi l'autenticazione PEAP-MSCHAPv2. Di seguito è riportato un esempio di autenticazione PEAP-MSCHAPv2 riuscita.

Utilizzare i comandi di debug per comprendere la sequenza di eventi che si verificano.

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Questi comandi di debug sul controller LAN wireless sono utili.

- **debug dot1x events enable**: per configurare il debug degli eventi 802.1x
- **debug aaa events enable**: per configurare il debug degli eventi AAA
- **debug mac addr <indirizzo mac>** - Per configurare il debug MAC, usare il comando **debug mac**
- **debug dhcp message enable**: per configurare il debug dei messaggi di errore DHCP

Di seguito vengono riportati gli output di esempio dei comandi **debug dot1x events enable** e **debug client <indirizzo mac>**.

debug dot1x events enable:

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
mobile 00:40:96:ac:e6:57 (EAP Id 2)
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
```


mobile 00:40:96:ac:e6:57 (EAP Id 13)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to**
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to**
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in**
Authenticating state for mobile 00:40:96:ac:e6:57

debug mac addr <Indirizzo MAC>:

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from**
mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 -
rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20)**
Change state to START (0)
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0)**
Initializing policy
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0)**
Change state to AUTHCHECK (2)
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2)**
Change state to 8021X_REQD (3)
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3)**
Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for**
mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of
Mobile Station: 00:40:96:ac:e6:57 (callerId: 48)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to
station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for
mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry.
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving
mobile 00:40:96:ac:e6:57 into Connecting state
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP-**
Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from**
mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from**
Connecting to Authenticating for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x -**
moving mobile 00:40:96:ac:e6:57 into Authenticating state
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57

Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Accept for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending default RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
8021X_REQD (3) **Change state to L2AUTHCOMPLETE (4)**
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
L2AUTHCOMPLETE (4) Change state to RUN (20)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached PLUMBFASPATH: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Replacing Fast Path rule
type = Airespace AP Client

```
on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
Card = 0 (slot 0), InHandle = 0x00000000,
OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

Nota: se si utilizza il supplicant Microsoft per autenticarsi con un Cisco Secure ACS per l'autenticazione PEAP, il client potrebbe non eseguire l'autenticazione correttamente. A volte la connessione iniziale può essere autenticata correttamente, ma i successivi tentativi di autenticazione con connessione rapida non riescono a connettersi. Si tratta di un problema noto. I dettagli di questo problema e la soluzione corrispondente sono disponibili [qui](#).

[Informazioni correlate](#)

- [PEAP in Unified Wireless Networks con ACS 4.0 e Windows 2003](#)
- [Esempio di configurazione dell'autenticazione EAP con i controller WLAN \(WLC\)](#)
- [Aggiornamento del software Wireless LAN Controller \(WLC\) alle versioni 3.2, 4.0 e 4.1](#)
- [Guide alla configurazione di Cisco Wireless LAN Controller serie 4400](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

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).