EAP-TLS in Unified Wireless Network con ACS 4.0 e Windows 2003

Sommario

Introduzione

In questo documento viene descritto come configurare un accesso wireless sicuro utilizzando i Wireless LAN Controller (WLC), il software Microsoft Windows 2003 e Cisco Secure Access Control Server (ACS) 4.0 tramite il protocollo EAP-TLS (Extensible Authentication Protocol-Transport Layer Security).

Nota: per ulteriori informazioni sull'implementazione di connessioni wireless sicure, fare riferimento al sito Web Microsoft Wi-Fi e al Cisco SAFE Wireless Blueprint (Cisco SAFE Wireless Blueprint).

Prerequisiti

Requisiti

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

Per informazioni sull'installazione iniziale e sulla configurazione dei Cisco serie 4400 Controller, fare riferimento alla Guida introduttiva: Cisco serie 4400 Wireless LAN Controller. Per informazioni sull'installazione iniziale e sulla configurazione dei Cisco serie 2000 Controller, fare riferimento alla Guida introduttiva: Cisco serie 2000 Wireless LAN Controller.

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

Importante: Al momento della stesura di questo documento, SP1 è l'ultimo aggiornamento di Windows Server 2003 e SP2 con patch di aggiornamento è l'ultimo software per Windows XP Professional.

Windows Server 2003 con SP1, Enterprise Edition viene utilizzato per consentire la configurazione della registrazione automatica dei certificati utente e workstation per l'autenticazione EAP-TLS. Questa procedura è descritta nella sezione Autenticazione EAP-TLS di questo documento. La registrazione automatica e il rinnovo automatico dei certificati semplificano la distribuzione dei certificati e migliorano la protezione tramite la scadenza e il rinnovo automatici dei certificati.

Componenti usati

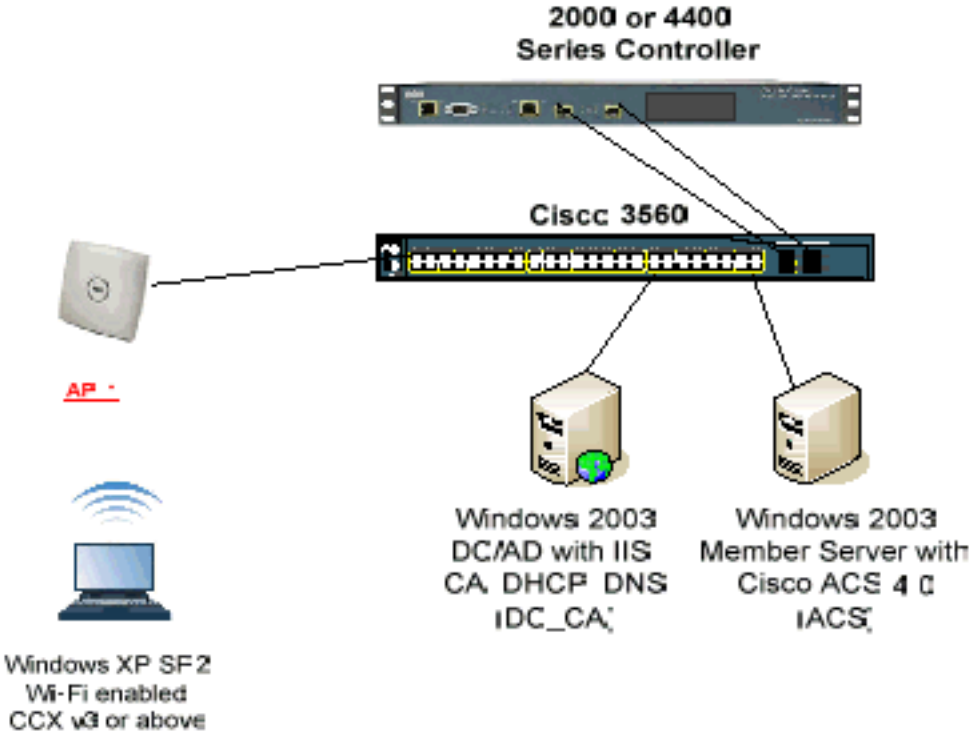
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Controller Cisco serie 2006 o 4400 con 3.2.16.21
- Cisco 1131 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise con Internet Information Server (IIS), CA (Certification Authority), DHCP e DNS (Domain Name System) installati
- Windows 2003 Standard con Access Control Server (ACS) 4.0
- Windows XP Professional con SP (e service pack aggiornati) e scheda di interfaccia di rete wireless (NIC) (con supporto CCX v3) o di terze parti.
- Cisco 3560 Switch

Esempio di rete

Nel documento viene usata questa impostazione di rete:

Topologia Cisco Secure Wireless Lab



Lo scopo principale di questo documento è quello di fornire la procedura dettagliata per implementare EAP-TLS in Unified Wireless Networks con ACS 4.0 e Windows 2003 Enterprise Server. L'enfasi principale è sulla registrazione automatica del client in modo che il client esegua la registrazione automatica e riceva il certificato dal server.

Nota: per aggiungere WPA (Wi-Fi Protected Access)/WPA2 con TKIP (Temporal Key Integrity Protocol)/AES (Advanced Encryption Standard) a Windows XP Professional con SP, consultare l'aggiornamento WPA2/Wireless Provisioning Services Information Element (WPS IE) per Windows XP con SP2 .

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.

Installazione di Windows Enterprise 2003 con IIS, Certification Authority, DNS, DHCP (DC_CA)

DC_CA (demo wireless)

DC_CA è un computer che esegue Windows Server 2003 con SP1, Enterprise Edition ed esegue i seguenti ruoli:

- Controller di dominio per il dominio wirelessdemo.local che esegue IIS
- Un server DNS per il dominio DNS wirelessdemo.local
- Un server DHCP
- CA radice dell'organizzazione per il dominio wirelessdemo.local

Completare questa procedura per configurare DC_CA per i seguenti servizi:

1. Eseguire un'installazione e una configurazione di base.
2. Configurare il computer come controller di dominio.
3. Aumentare il livello di funzionalità del dominio.
4. Installare e configurare DHCP.
5. Installare servizi certificati.
6. Verificare le autorizzazioni di amministratore per i certificati.
7. Aggiungere computer al dominio.
8. Consenti accesso wireless ai computer.
9. Aggiungere utenti al dominio.
10. Consenti accesso wireless agli utenti.
11. Aggiungere gruppi al dominio.
12. Aggiungere utenti al gruppo WirelessUsers.
13. Aggiungere computer client al gruppo WirelessUsers.

Passaggio 1: Eseguire l'installazione e la configurazione di base

Attenersi alla seguente procedura:

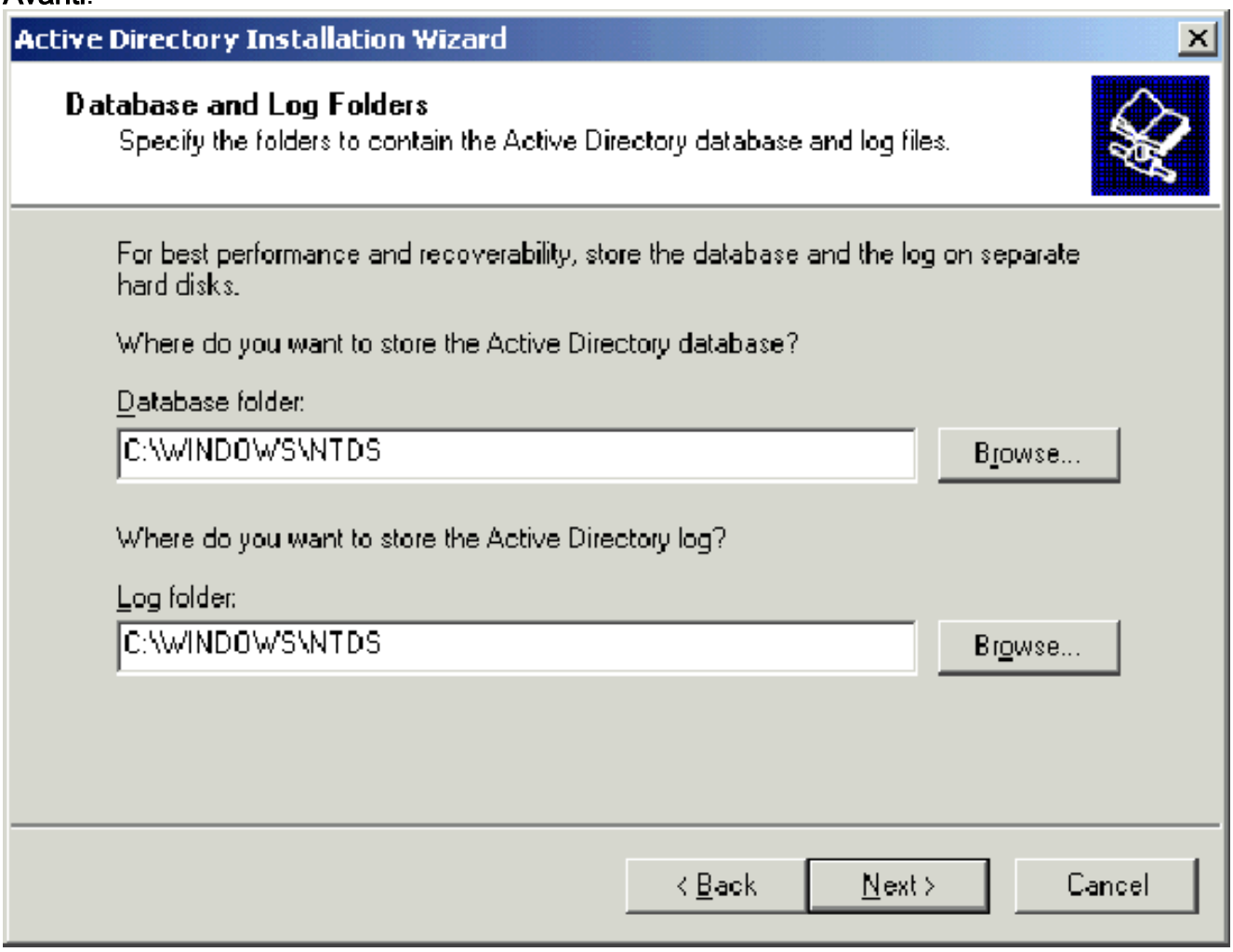
1. Installare Windows Server 2003 con SP1, Enterprise Edition come server autonomo.
2. Configurare il protocollo TCP/IP con l'indirizzo IP 172.16.100.26 e la subnet mask 255.255.255.0.

Passaggio 2: Configurare il computer come controller di dominio

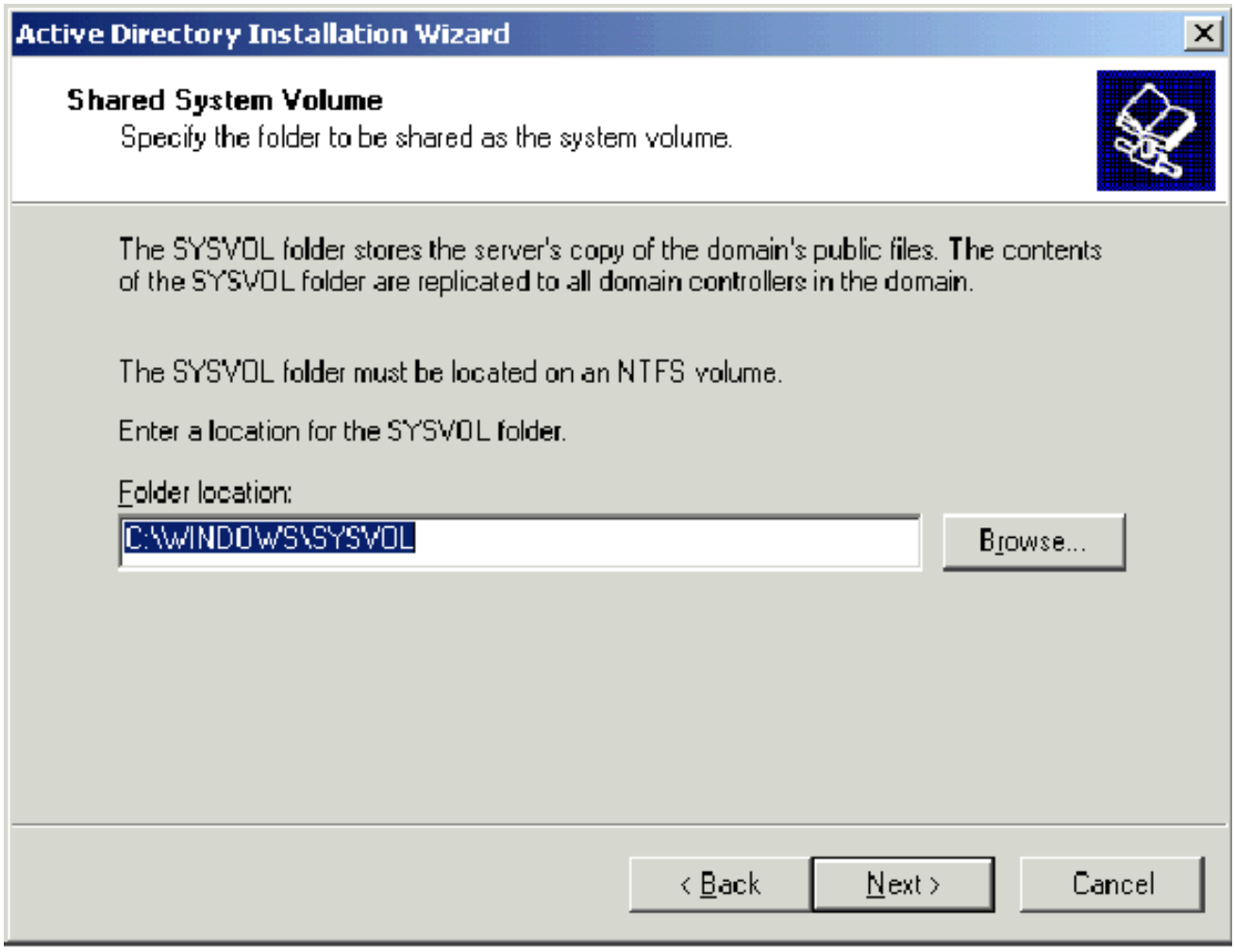
Attenersi alla seguente procedura:

1. Per avviare l'Installazione guidata di Active Directory, scegliere **Start > Esegui**, digitare **dcpromo.exe** e fare clic su **OK**.
2. Nella pagina Installazione guidata Active Directory fare clic su **Avanti**.
3. Nella pagina Compatibilità sistema operativo fare clic su **Avanti**.
4. Nella pagina Tipo di controller di dominio selezionare **Controller di dominio per un nuovo dominio** e fare clic su **Avanti**.
5. Nella pagina Crea nuovo dominio selezionare **Dominio in una nuova foresta** e fare clic su **Avanti**.
6. Nella pagina Installa o configura DNS selezionare **No, installa e configura DNS nel computer** e fare clic su **Avanti**.
7. Nella pagina Nuovo nome di dominio digitare **wirelessdemo.local** e fare clic su **Avanti**.
8. Nella pagina Nome di dominio NetBIOS, immettere il nome di dominio NetBIOS come **demo wireless** e fare clic su **Avanti**.

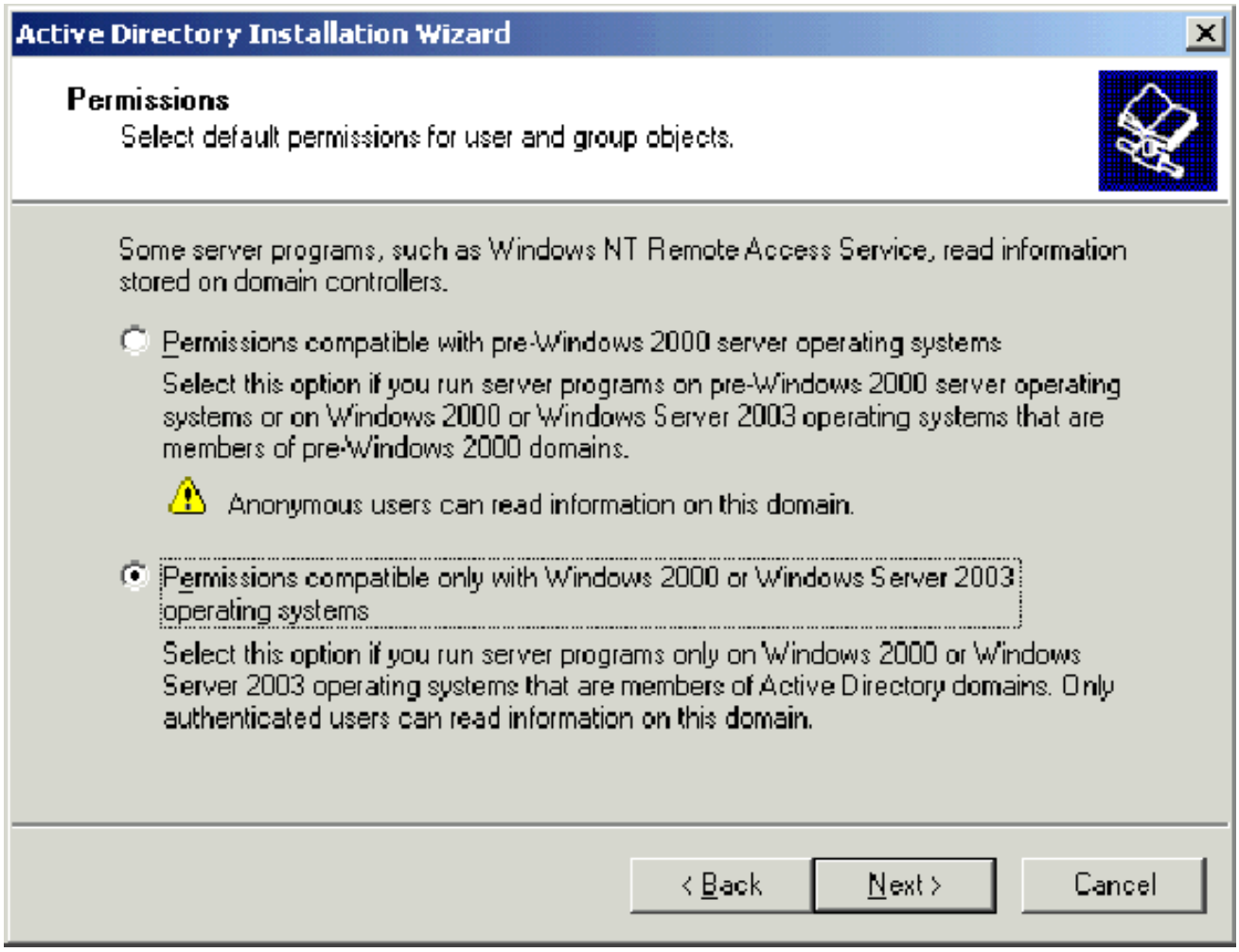
9. Nella pagina Percorso del database e delle cartelle di log accettare le directory predefinite del database e delle cartelle di log e fare clic su
   Avanti.



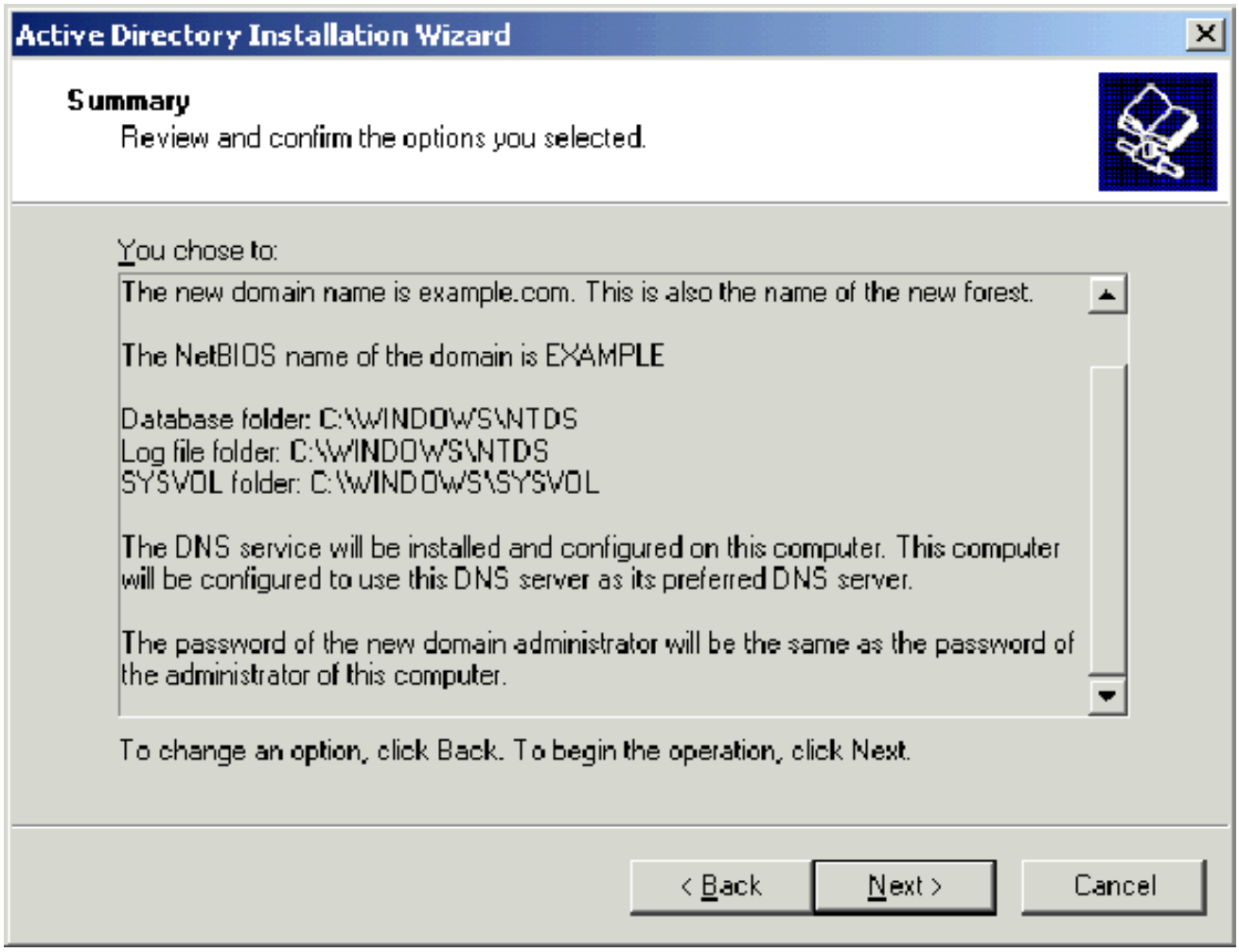
10. Nella finestra di dialogo Volume di sistema condiviso verificare che il percorso predefinito della cartella sia corretto e fare clic su
    Avanti.



11. Nella pagina Autorizzazioni verificare che **l'opzione Autorizzazioni compatibili solo con i sistemi operativi Windows 2000 o Windows Server 2003** sia selezionata e **fare clic su Avanti**.



12. Nella pagina Password di amministrazione modalità ripristino servizi directory lasciare vuote le caselle della password e fare clic su **Avanti**.
13. Rivedere le informazioni nella pagina Riepilogo e fare clic su **Avanti**.

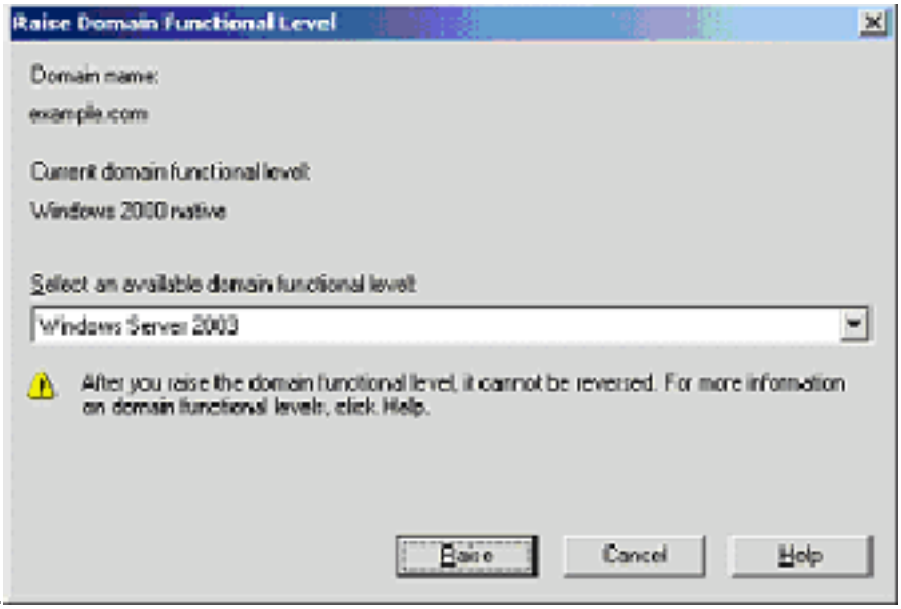


14. Nella pagina Completamento dell'Installazione guidata di Active Directory fare clic su **Fine**.
15. Quando viene richiesto di riavviare il computer, fare clic su **Riavvia ora**.

Passaggio 3: Aumentare il livello di funzionalità del dominio

Attenersi alla seguente procedura:

1. Aprire lo snap-in Domini e trust di Active Directory dalla cartella **Strumenti di amministrazione (Start > Strumenti di amministrazione > Domini e trust di Active Directory)**, quindi fare clic con il pulsante destro del mouse sul computer del dominio **DC_CA.wirelessdemo.local**.
2. Fare clic su **Aumenta livello funzionalità dominio** e quindi selezionare **Windows Server 2003** nella pagina Aumenta livello funzionalità

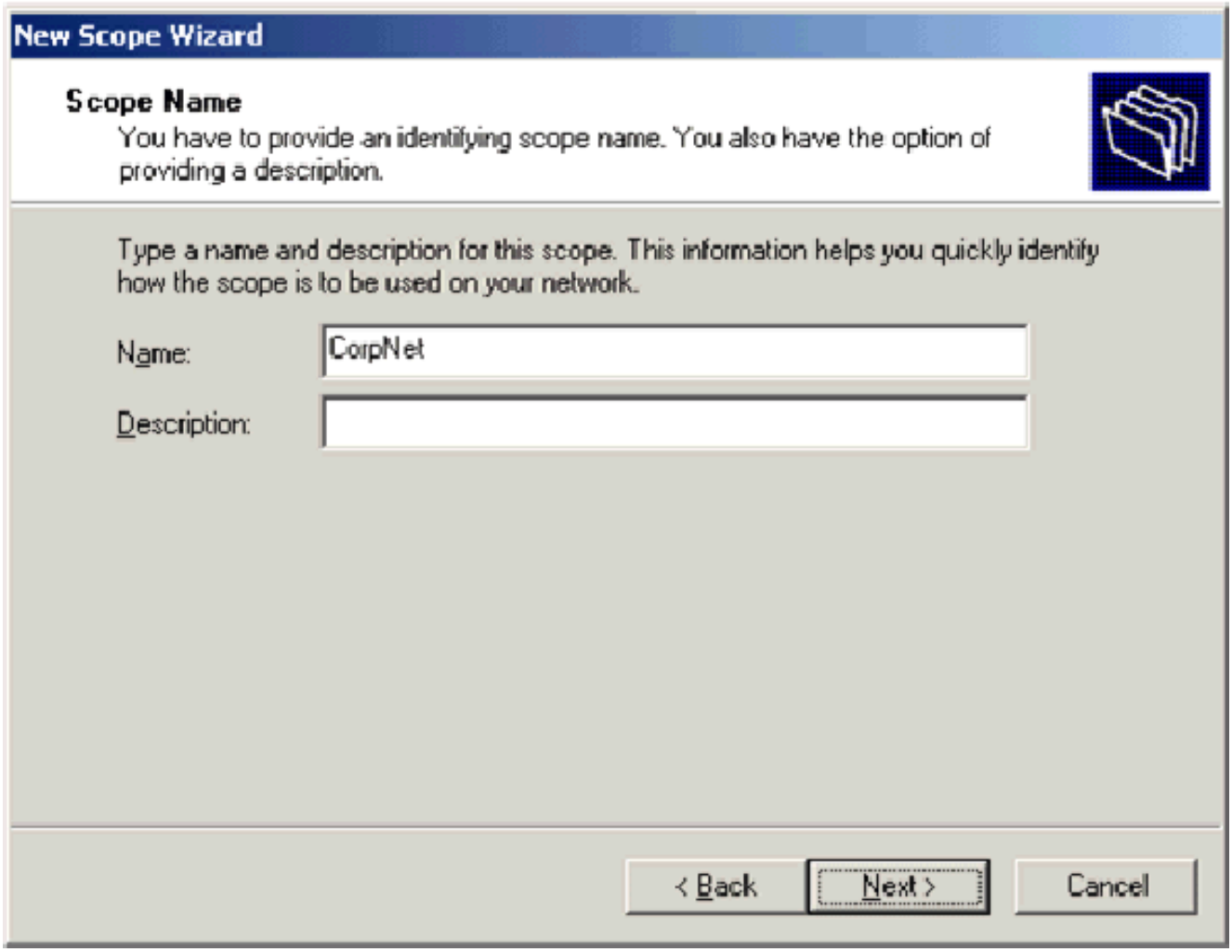
dominio. 

3. Fare clic su **Aumenta**, quindi su **OK** e infine di nuovo su **OK**.

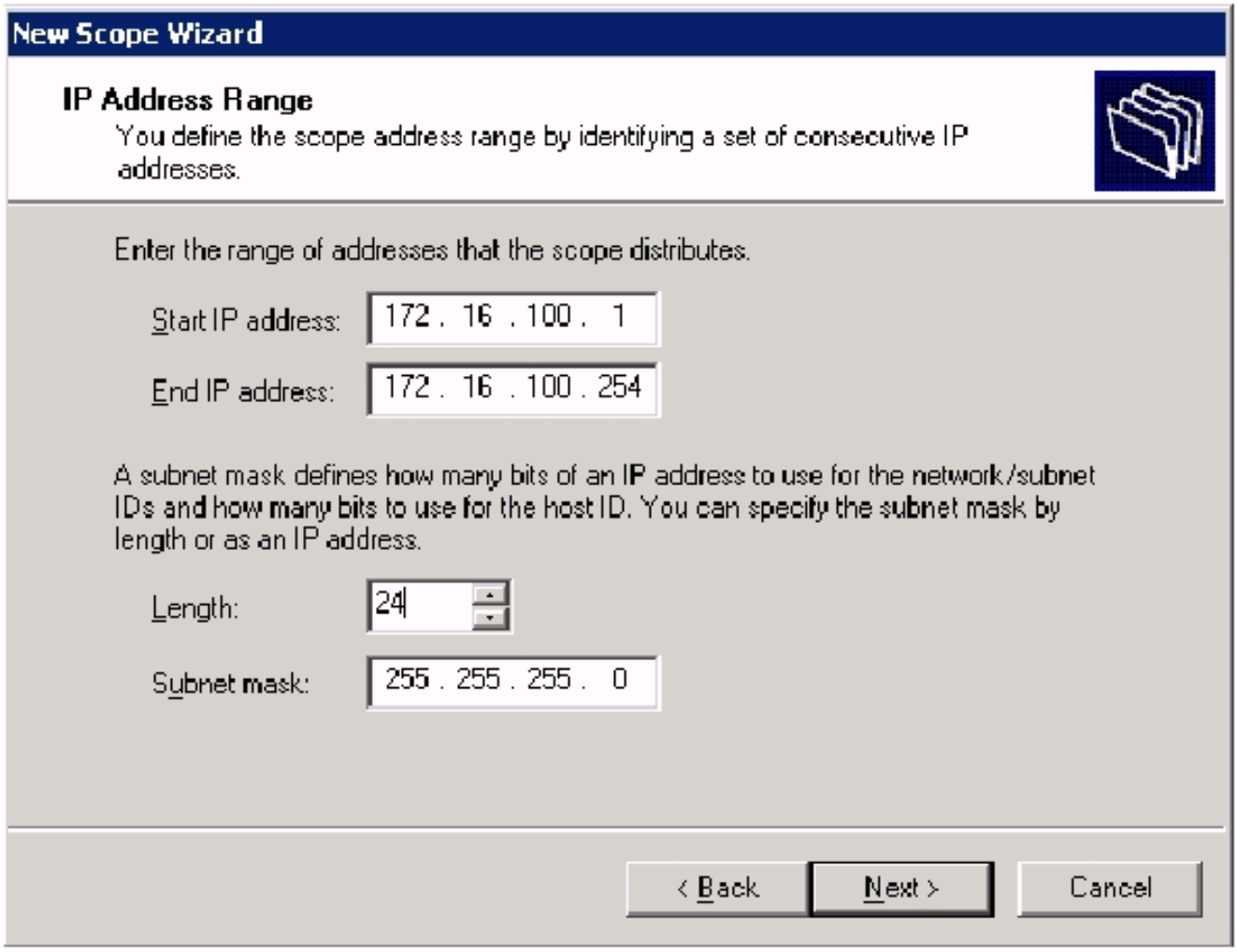
Passaggio 4: Installare e configurare DHCP

Attenersi alla seguente procedura:

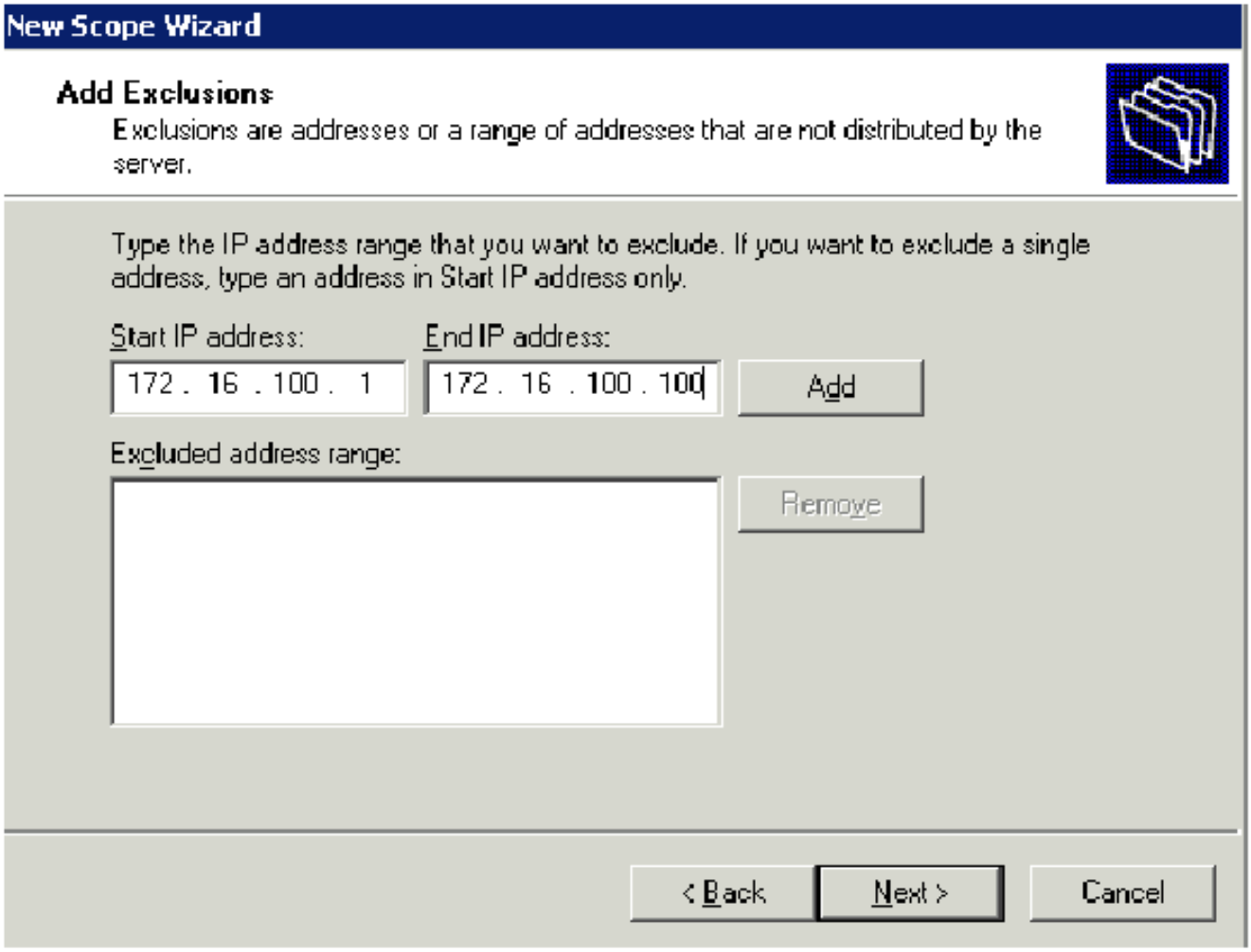
1. Installare il protocollo DHCP (Dynamic Host Configuration Protocol) come componente del servizio di rete utilizzando **Installazione applicazioni** nel Pannello di controllo.
2. Aprire lo snap-in DHCP dalla cartella Strumenti di amministrazione **(Start > Programmi > Strumenti di amministrazione > DHCP**, quindi evidenziare il server DHCP **DC_CA.wirelessdemo.local**.
3. Per autorizzare il servizio DHCP, fare clic su **Azione** e quindi su **Autorizza**.
4. Nell'albero della console fare clic con il pulsante destro del mouse su **DC_CA.wirelessdemo.local** e quindi scegliere **Nuovo ambito**.
5. Nella pagina iniziale della Creazione guidata ambito fare clic su **Avanti**.
6. Nella pagina Nome ambito digitare **CorpNet** nel campo Nome.



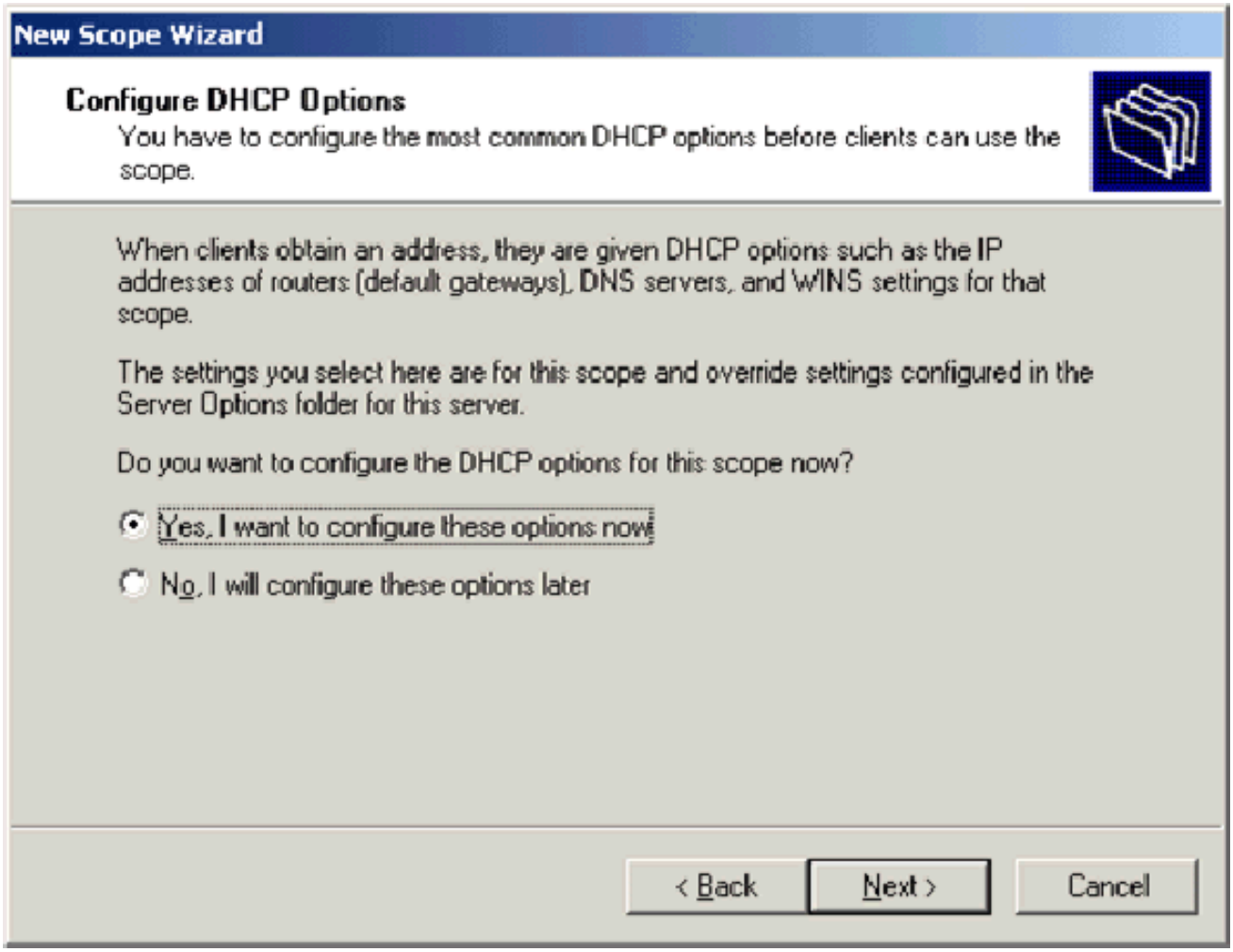
7. Fare clic su **Avanti** e specificare i seguenti parametri:Indirizzo IP iniziale—**172.16.100.1**Indirizzo IP finale—**172.16.100.254**Lunghezza—**24**Subnet mask—**255.255.255.0**



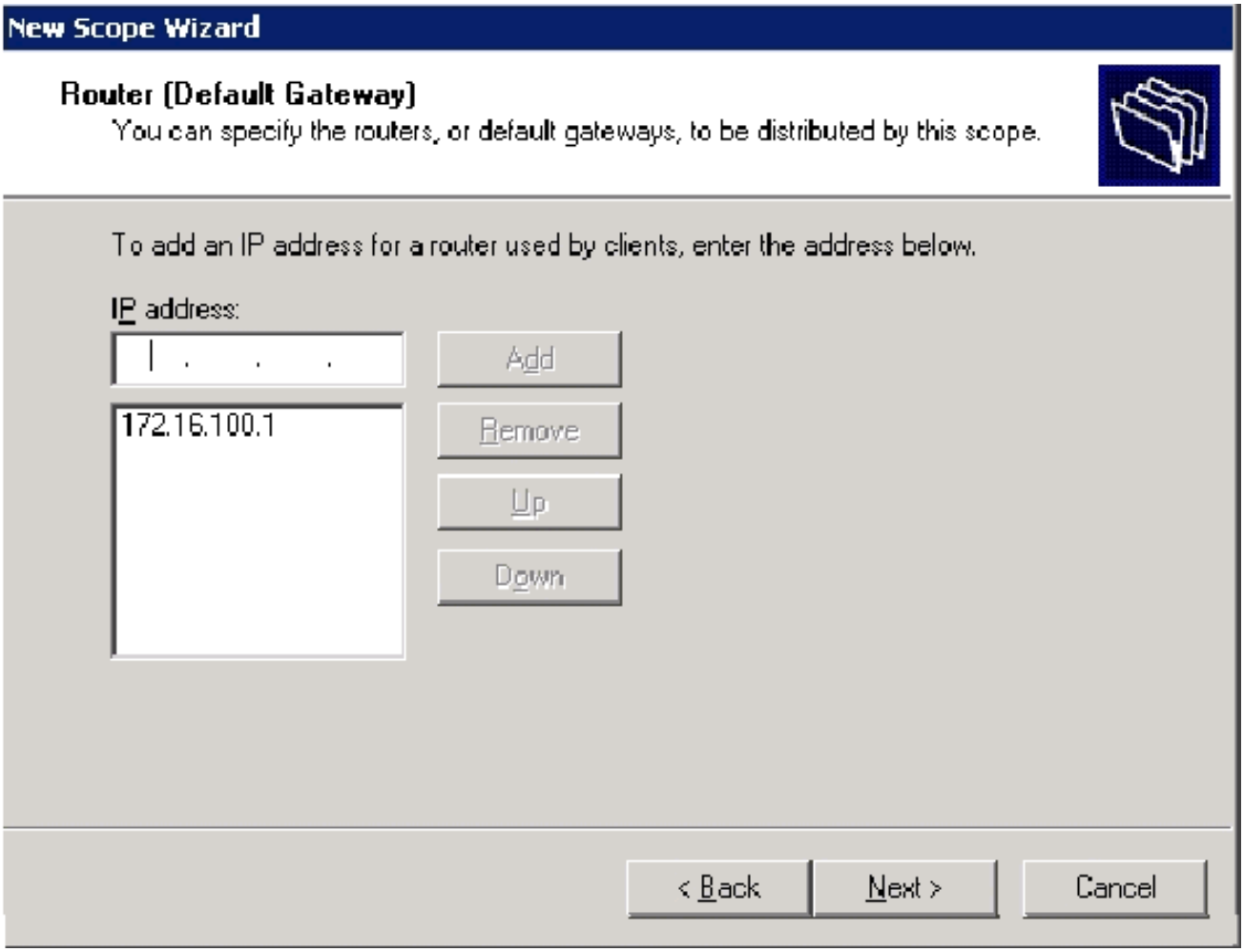
8. Fare clic su **Next** (Avanti) e immettere **172.16.100.1** per l'indirizzo IP iniziale e **172.16.100.100** per l'indirizzo IP finale da escludere. Quindi fare clic su **Avanti**. In questo modo gli indirizzi IP compresi nell'intervallo da 172.16.100.1 a 172.16.100.100 vengono riservati. Questi indirizzi IP riservati non vengono assegnati dal server DHCP.



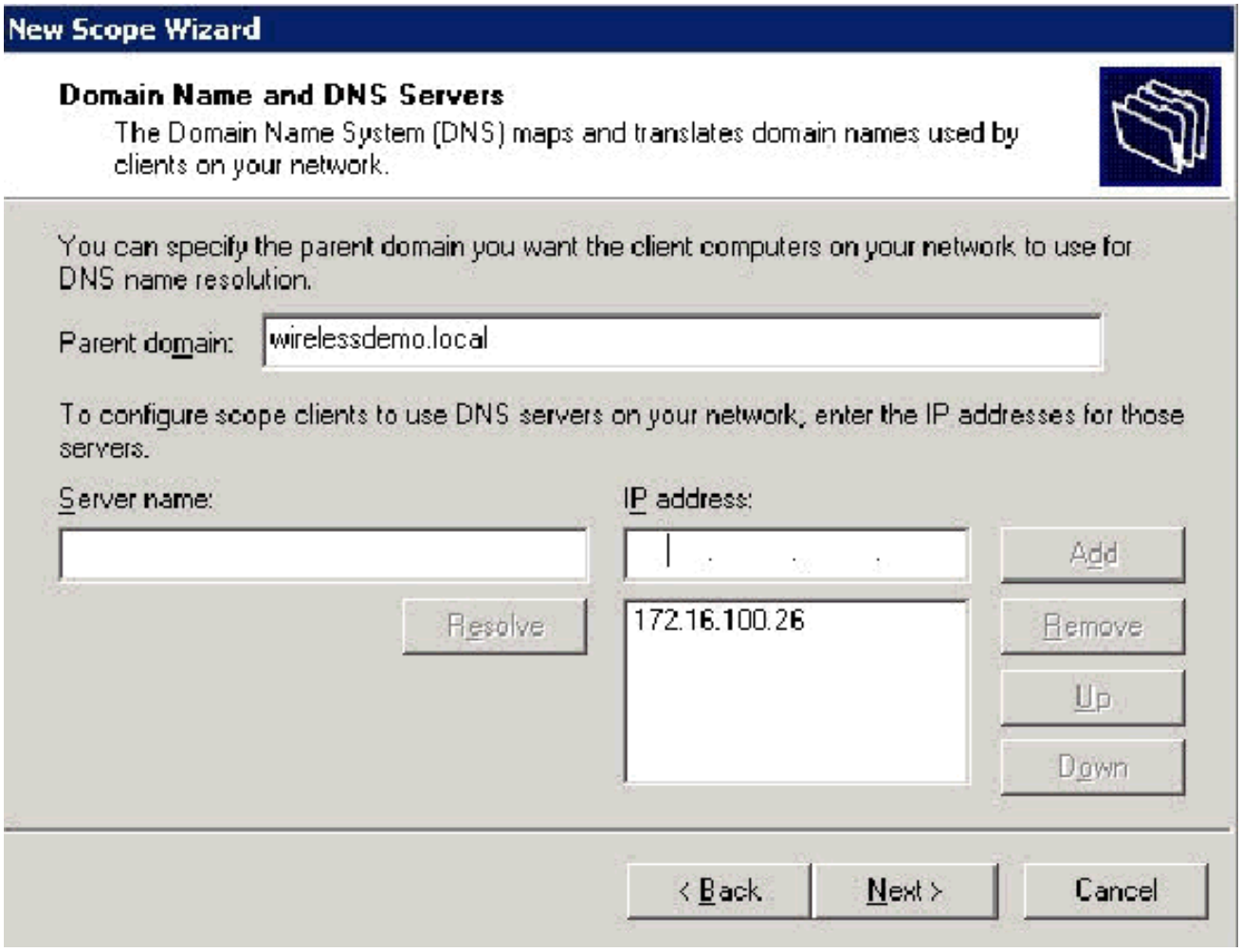
9. Nella pagina Durata lease fare clic su **Avanti**.
10. Nella pagina Configura opzioni DHCP, selezionare **Sì, configurare le opzioni** e fare clic su **Avanti**.



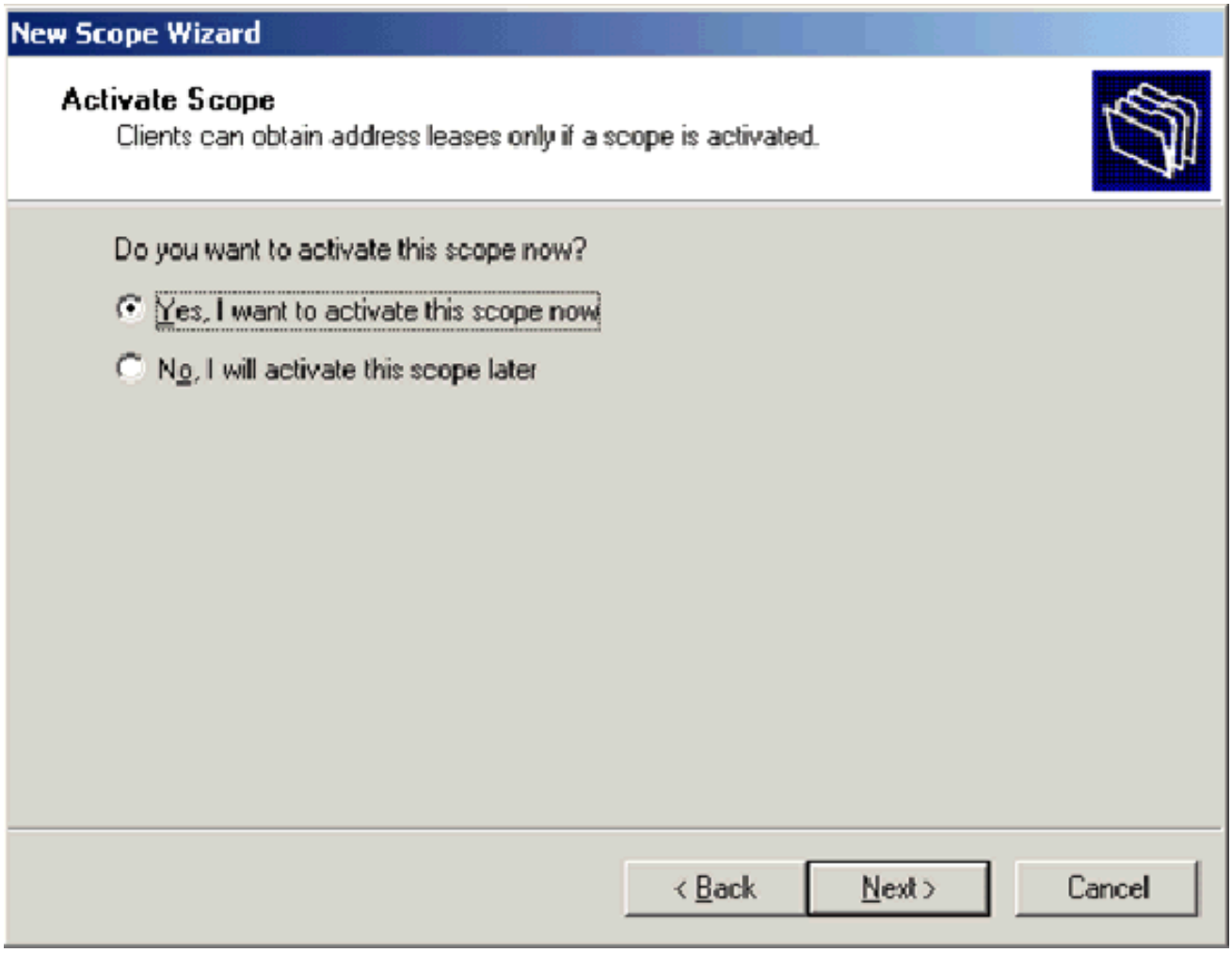
11. Nella pagina Router (gateway predefinito) aggiungere l'indirizzo del router predefinito **172.16.100.1** e fare clic su **Avanti**.



12. Nella pagina Nome dominio e server DNS digitare **wirelessdemo.local** nel campo Dominio padre, digitare **172.16.100.26** nel campo Indirizzo IP e quindi fare clic su **Aggiungi** e su **Avanti**.



13. Nella pagina Server WINS fare clic su **Avanti**.
14. Nella pagina Attiva ambito scegliere **Sì, attiva l'ambito** e fare clic su **Avanti**.



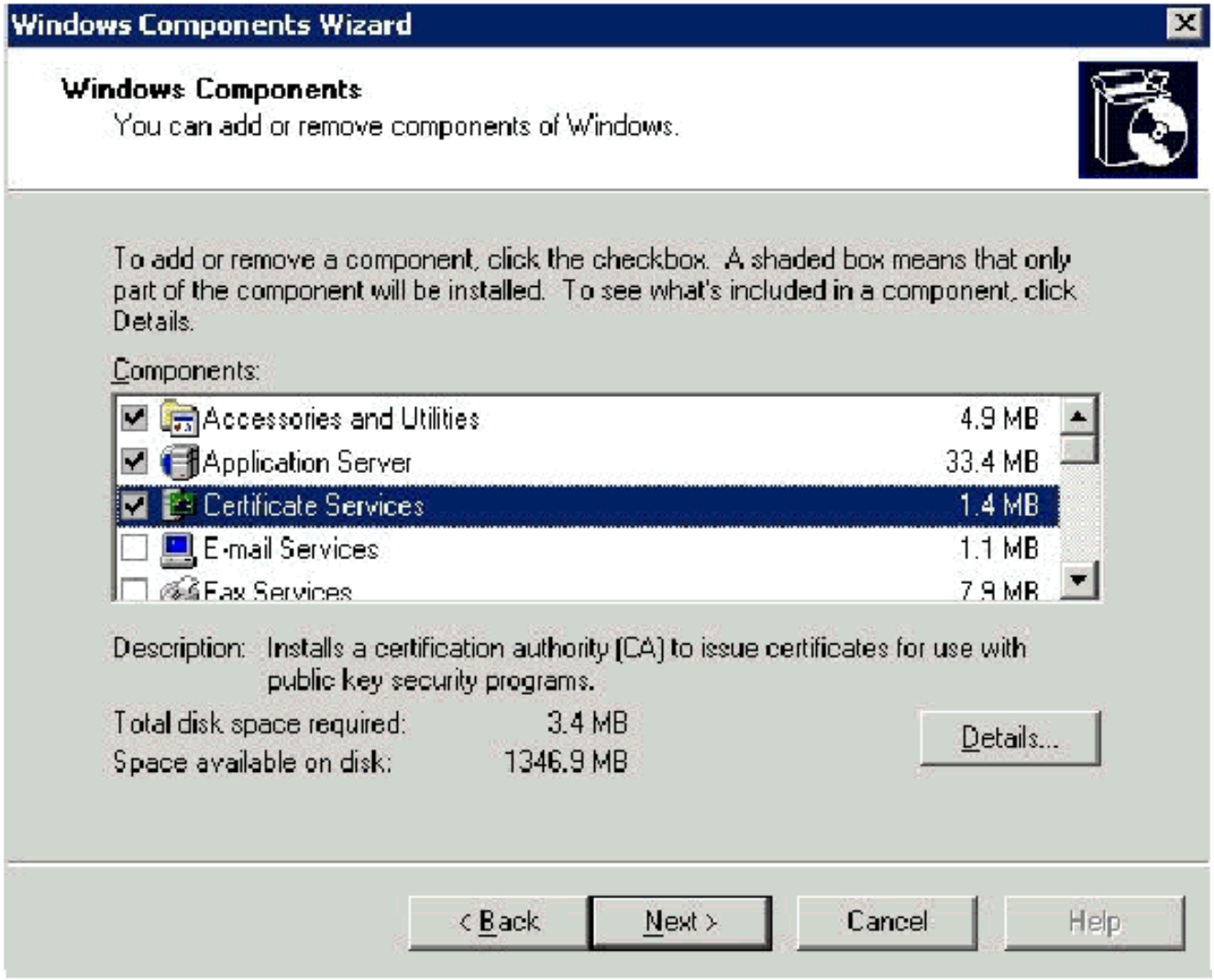
15. Nella pagina Completamento della Creazione guidata ambito fare clic su **Fine**.

Passaggio 5: Installa Servizi certificati

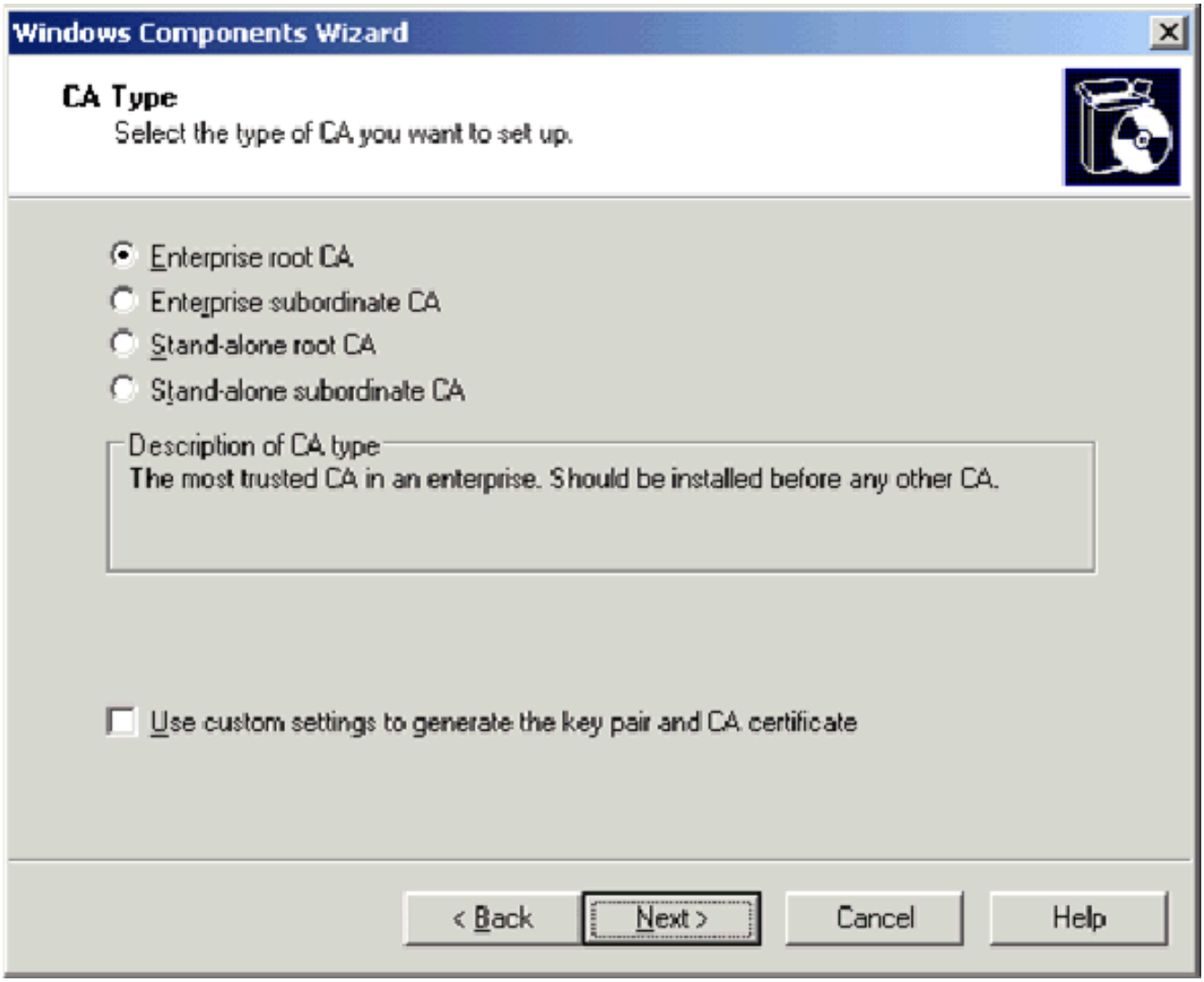
Attenersi alla seguente procedura:

Nota: prima di installare Servizi certificati è necessario installare IIS e l'utente deve appartenere all'unità organizzativa Enterprise Admin.

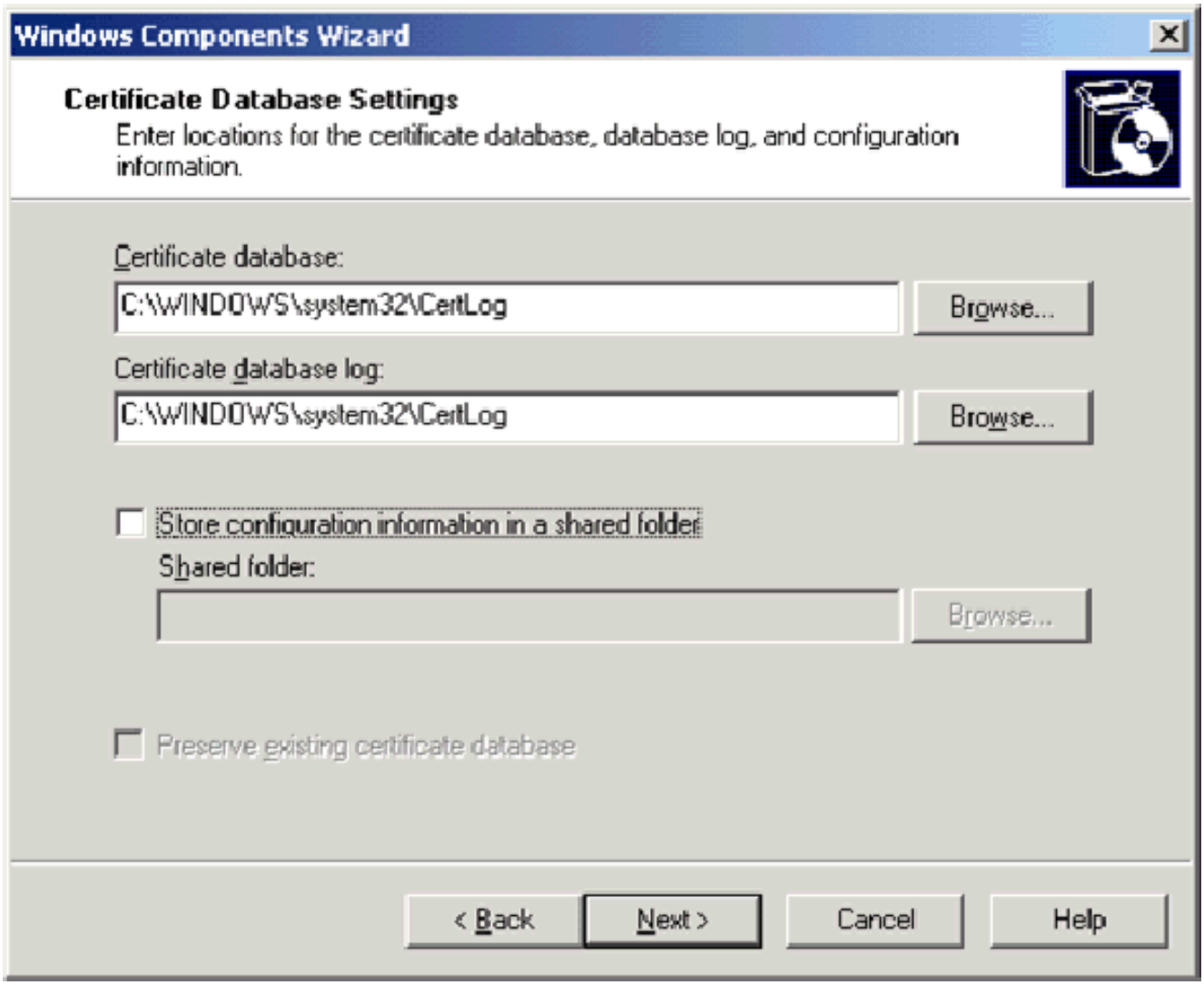
1. Nel Pannello di controllo aprire **Installazione applicazioni** e quindi fare clic su **Installazione componenti di Windows**.
2. Nella pagina Componenti guidati di Windows scegliere **Servizi certificati** e quindi fare clic su **Avanti**.



3. Nella pagina Tipo di CA scegliere **CA radice dell'organizzazione** e fare clic su **Avanti**.



4. Nella pagina Informazioni di identificazione della CA digitare **wirelessdemoca** nella casella Nome comune per la CA. È possibile immettere gli altri dettagli facoltativi e quindi fare clic su **Avanti**. Accettare le impostazioni predefinite nella pagina Impostazioni database certificati.

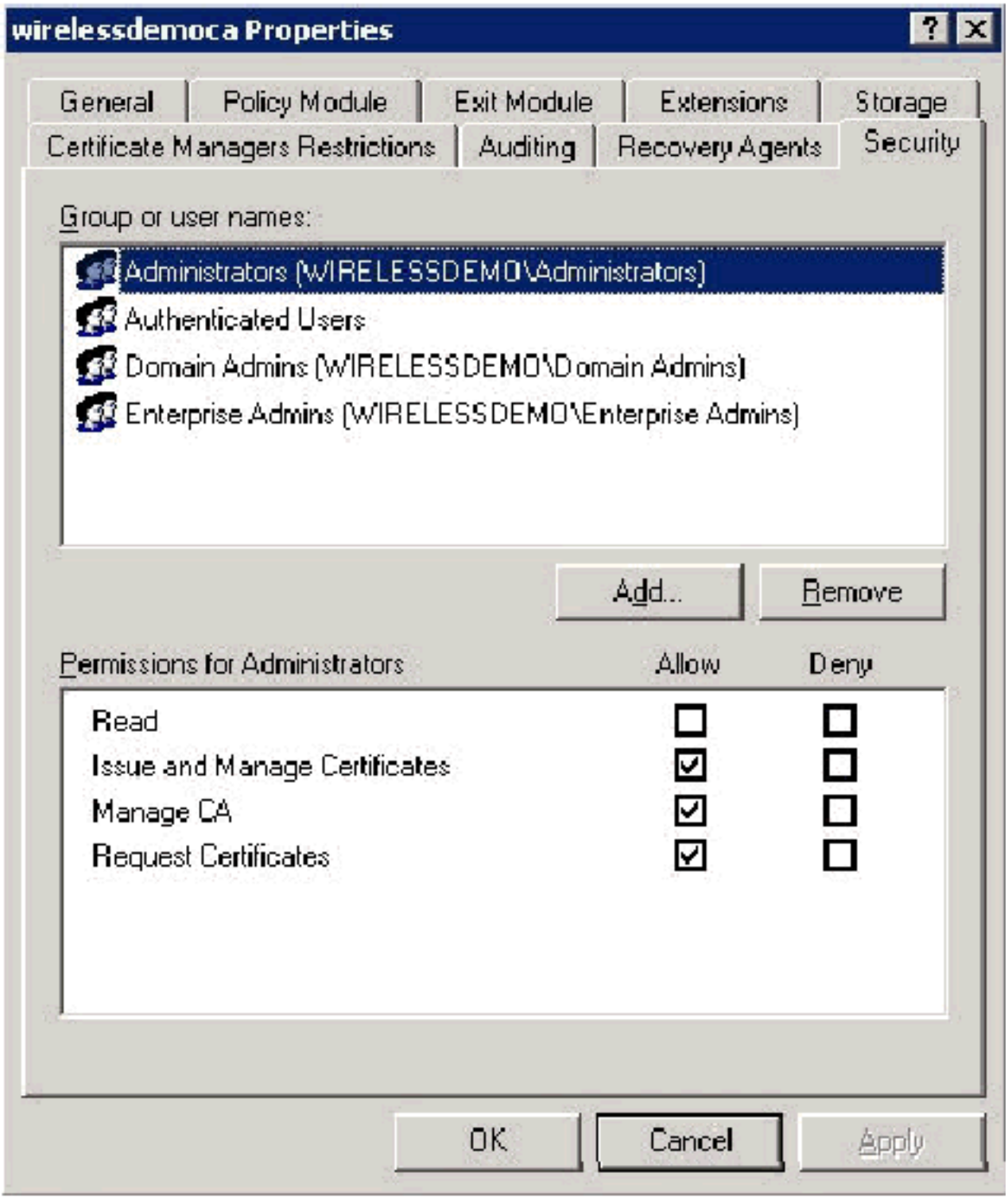


5. Fare clic su **Next** (Avanti). Al termine dell'installazione, fare clic su **Fine**.
6. Fare clic su **OK** dopo aver letto l'avviso relativo all'installazione di IIS.

Passaggio 6: Verifica autorizzazioni amministratore per certificati

Attenersi alla seguente procedura:

1. Scegliere **Start > Strumenti di amministrazione > Autorità di certificazione**.
2. Fare clic con il pulsante destro del mouse su **wirelessdemoca CA** e quindi scegliere **Proprietà**.
3. Nella scheda Protezione fare clic su **Amministratori** nell'elenco Utenti e gruppi.
4. Nell'elenco Autorizzazioni o Amministratori verificare che queste opzioni siano impostate su **Consenti**:Rilasciare e gestire certificatiGestisci CARichiedi certificatiSe una di queste opzioni è impostata su Nega o non è selezionata, impostare l'autorizzazione su **Consenti**.



5. Fare clic su **OK** per chiudere la finestra di dialogo Proprietà Autorità di certificazione Wireless e quindi chiudere l'Autorità di certificazione.

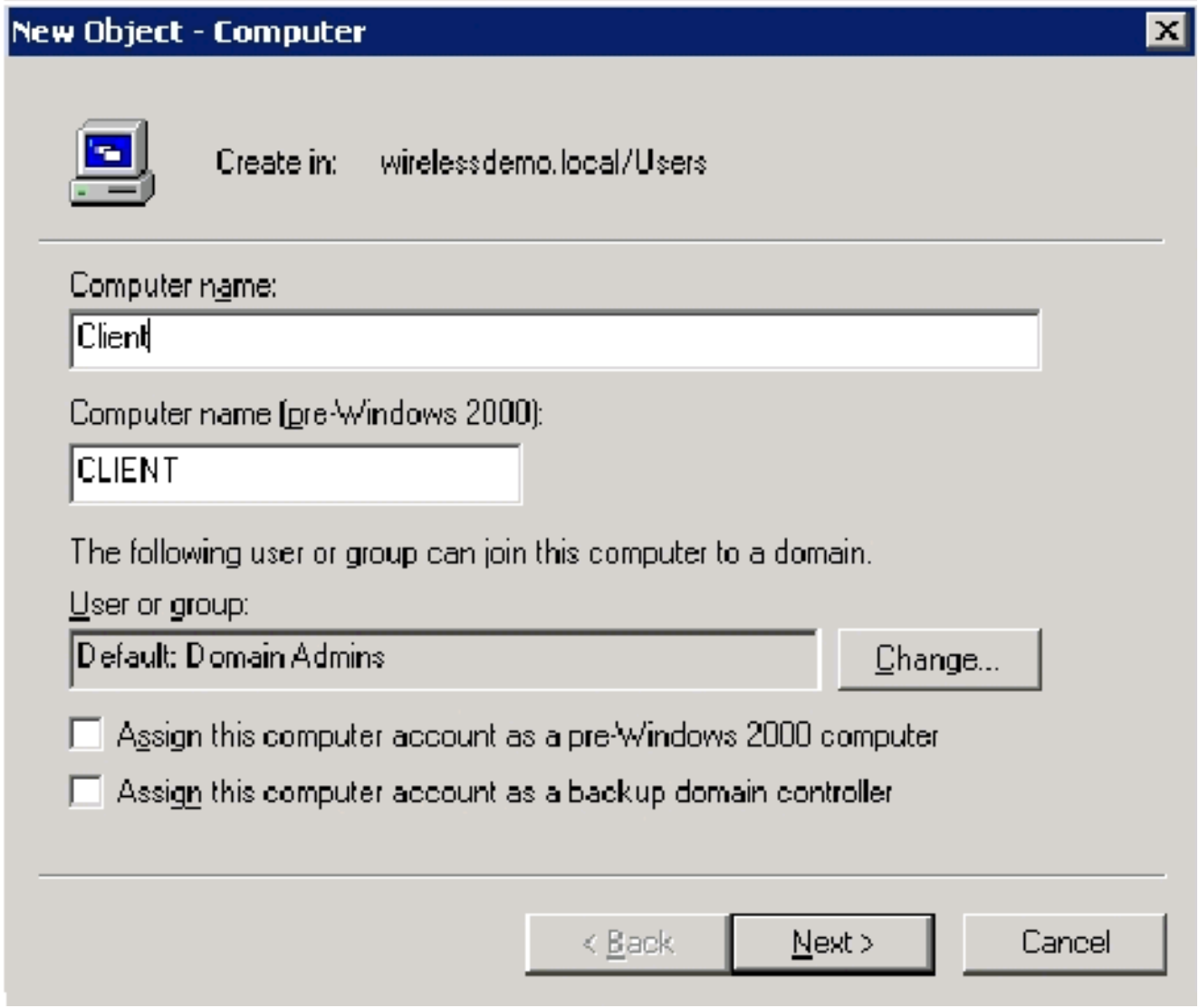
Passaggio 7: Aggiungi computer al dominio

Attenersi alla seguente procedura:

Nota: se il computer è già stato aggiunto al dominio, passare a Aggiungi utenti al dominio.

1. Aprire lo snap-in Utenti e computer di Active Directory.
2. Nell'albero della console espandere **wirelessdemo.local**.
3. Fare clic con il pulsante destro del mouse su **Utenti**, scegliere **Nuovo** e quindi **Computer**.
4. Nella finestra di dialogo Nuovo oggetto - Computer digitare il nome del computer nel campo

Nome computer e fare clic su **Avanti**. In questo esempio viene utilizzato il nome del computer **Client**.



5. Nella finestra di dialogo Gestito fare clic su **Avanti**.
6. Nella finestra di dialogo Nuovo computer-oggetto fare clic su **Fine**.
7. Ripetere i passaggi da 3 a 6 per creare altri account computer.

Passaggio 8: Consenti accesso wireless ai computer

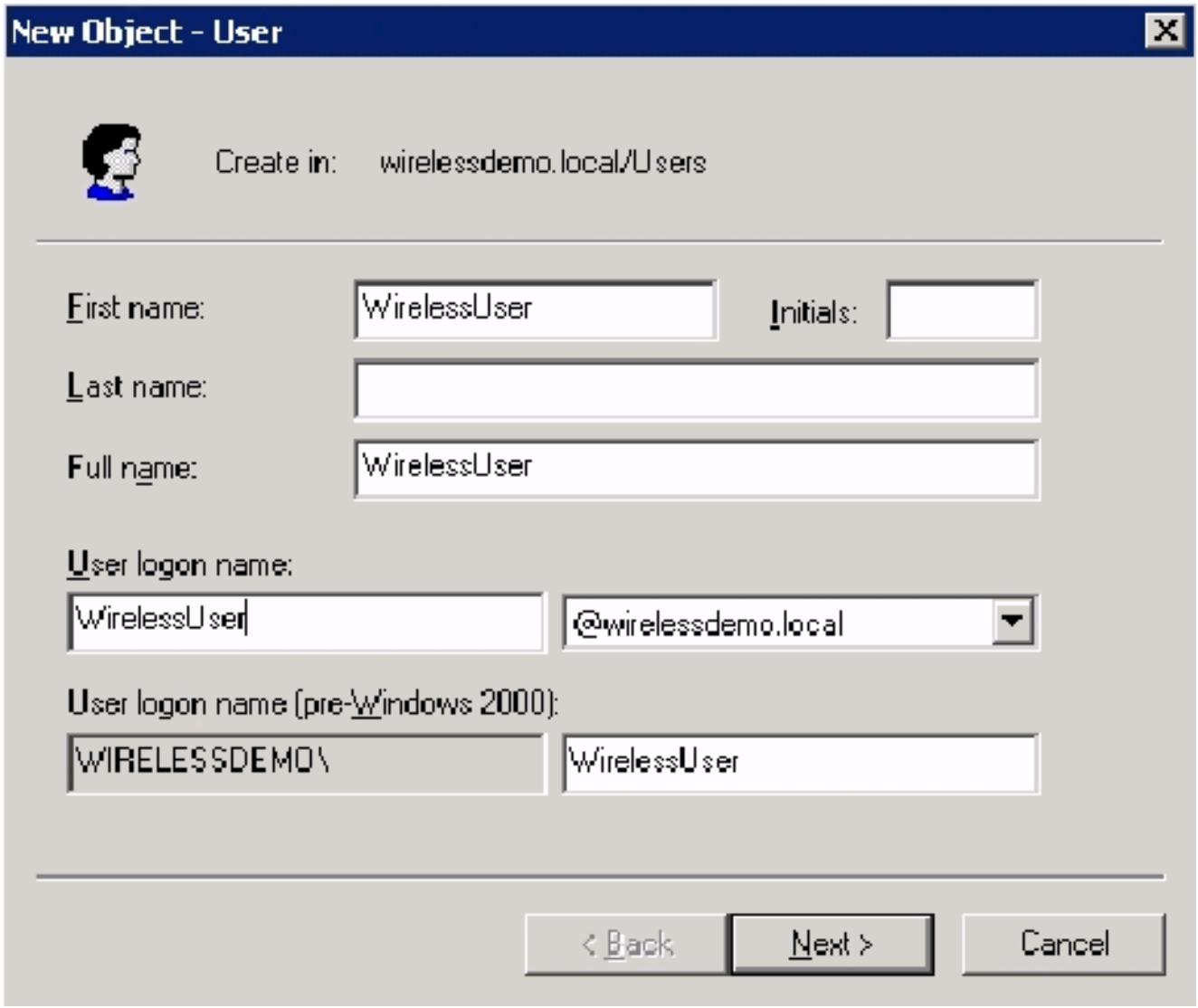
Attenersi alla seguente procedura:

1. Nell'albero della console Utenti e computer di Active Directory fare clic sulla cartella **Computer** e fare clic con il pulsante destro del mouse sul computer per cui si desidera assegnare l'accesso wireless. In questo esempio viene illustrata la procedura con il computer **CLIENT** aggiunta al passaggio 7.
2. Fare clic su **Proprietà** e quindi sulla scheda Connessione remota.
3. Scegliere **Consenti accesso** e fare clic su **OK**.

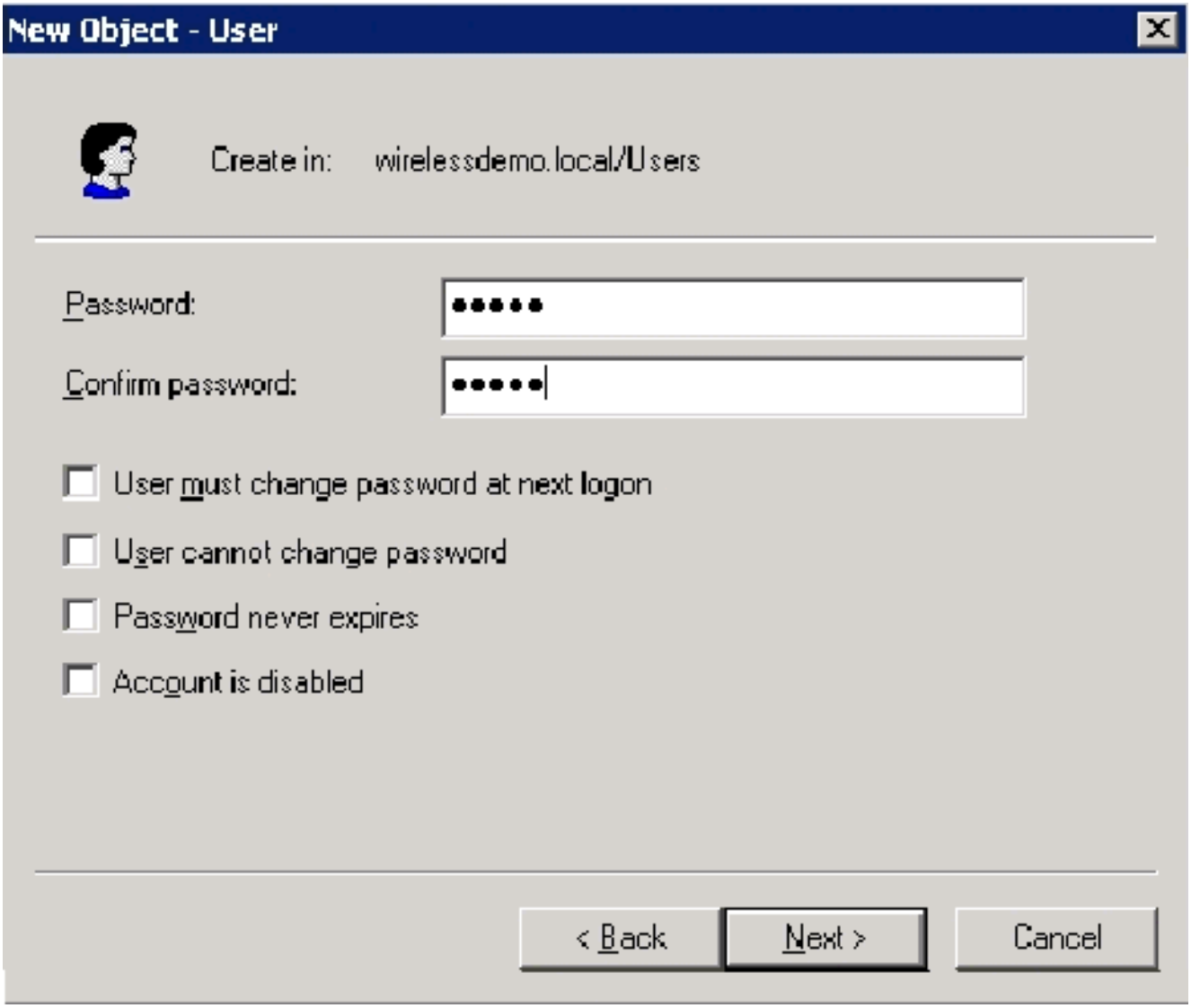
Passaggio 9: Aggiungi utenti al dominio

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 **Utente**.
2. Nella finestra di dialogo Nuovo oggetto - Utente digitare **WirelessUser** nel campo Nome, quindi digitare **WirelessUser** nel campo Nome di accesso utente e fare clic su **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 **Avanti**.



4. Nella finestra di dialogo Nuovo oggetto - Utente fare clic su **Fine**.
5. Ripetere i passaggi da 2 a 4 per creare altri account utente.

Passaggio 10: Consenti accesso wireless agli utenti

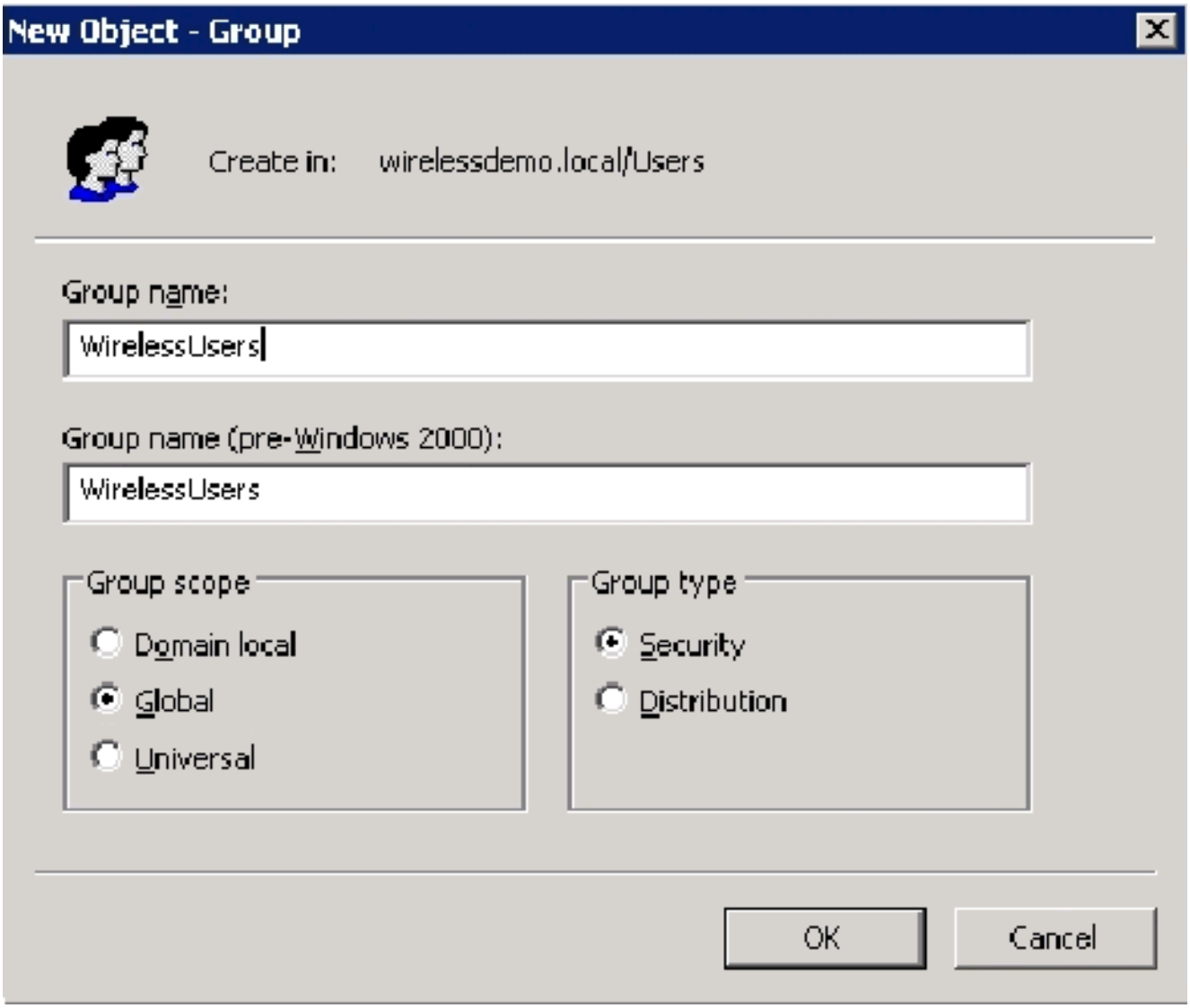
Attenersi alla seguente procedura:

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** e fare clic su **OK**.

Passaggio 11: Aggiungi gruppi al dominio

Attenersi alla seguente procedura:

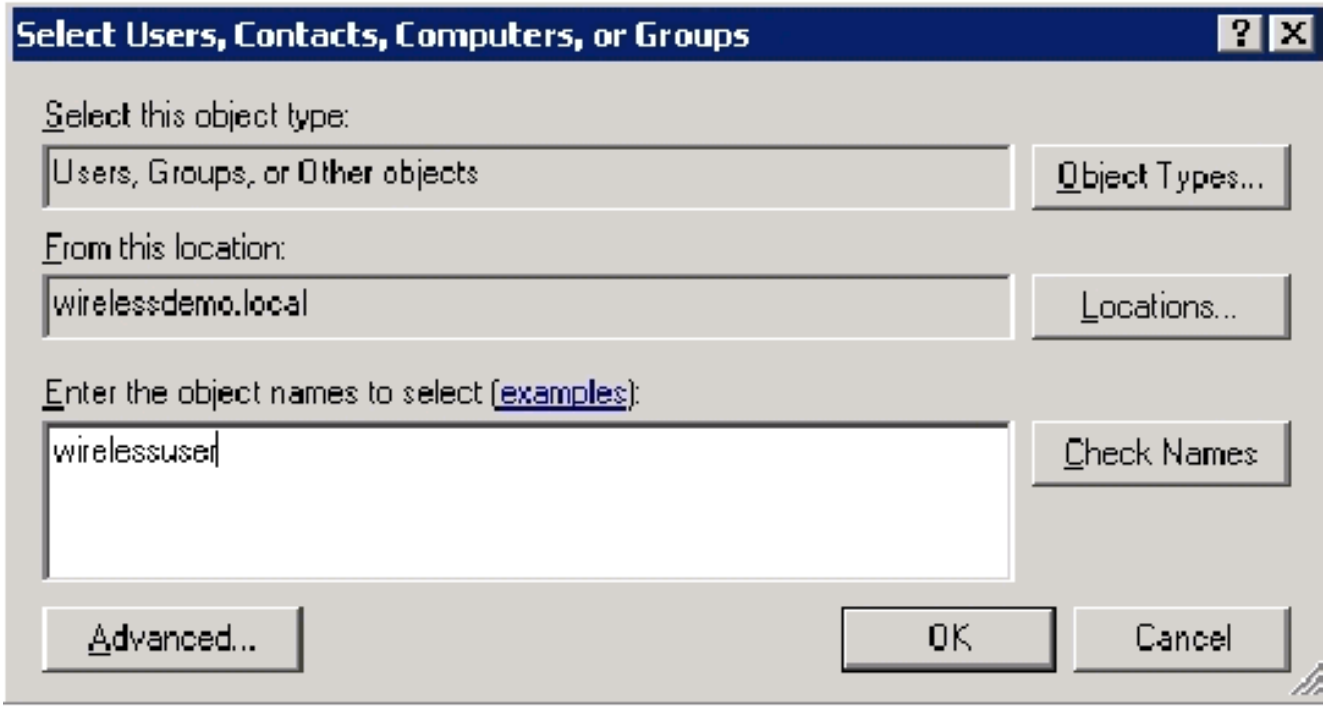
1. Nell'albero della console Utenti e computer di Active Directory fare clic con il pulsante destro del mouse su **Utenti**, scegliere **Nuovo** e quindi **Raggruppa**.
2. Nella finestra di dialogo Nuovo oggetto - Gruppo digitare il nome del gruppo nel campo Nome gruppo e fare clic su **OK**. Nel documento viene utilizzato il nome di gruppo **WirelessUsers**.



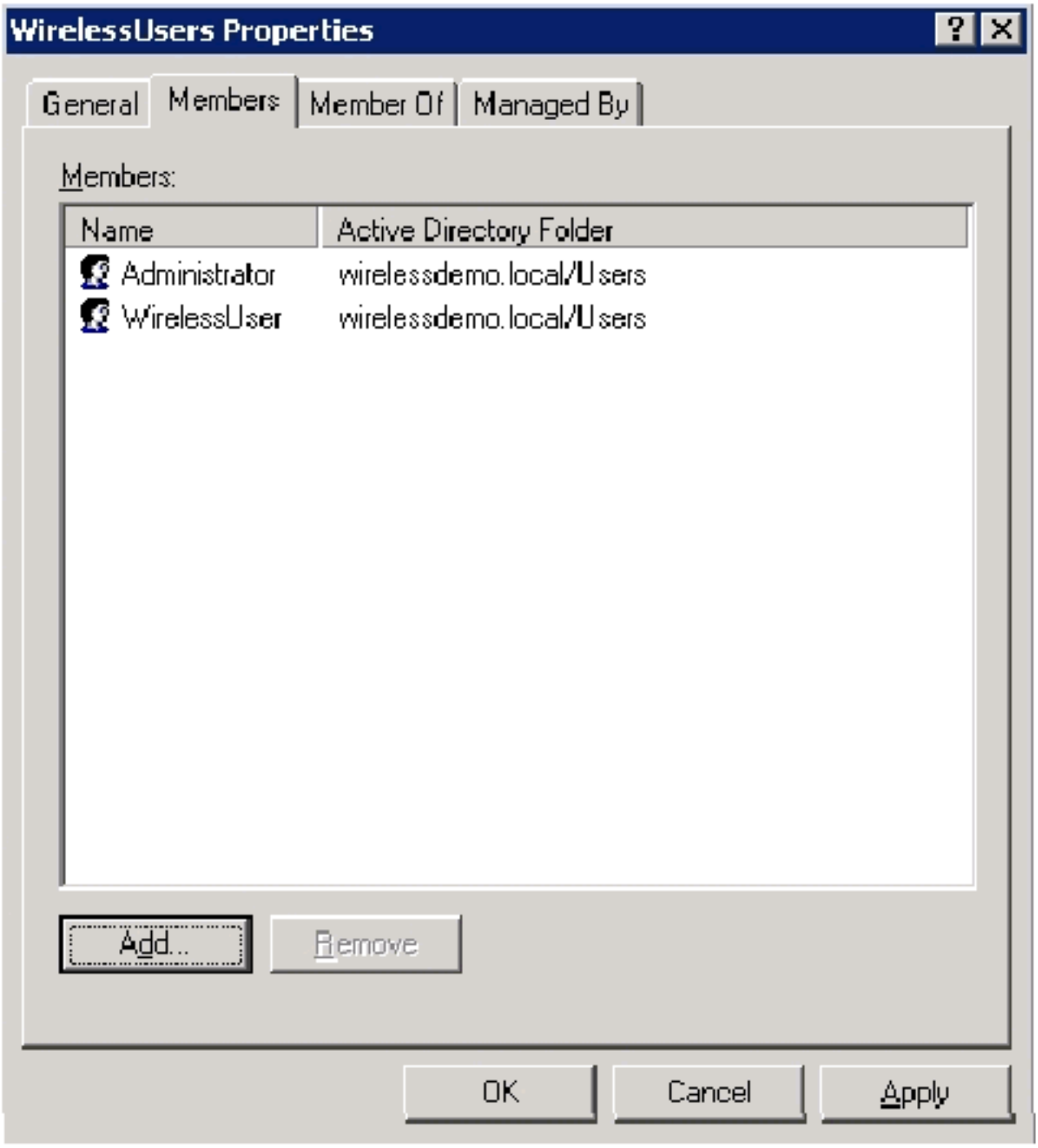
Passaggio 12: Aggiungi utenti al gruppo WirelessUsers

Attenersi alla seguente procedura:

1. Nel riquadro dei dettagli di Utenti e computer di Active Directory fare doppio clic sul gruppo **WirelessUsers**.
2. Passare alla scheda Membri e fare clic su **Aggiungi**.
3. Nella finestra di dialogo Seleziona utenti, contatti, computer o gruppi digitare il nome degli utenti che si desidera aggiungere al gruppo. In questo esempio viene illustrato come aggiungere l'utente **wireless** al gruppo. Fare clic su **OK**.



4. Nella finestra di dialogo Trovati più nomi fare clic su **OK**. L'account utente WirelessUser viene aggiunto al gruppo WirelessUsers.

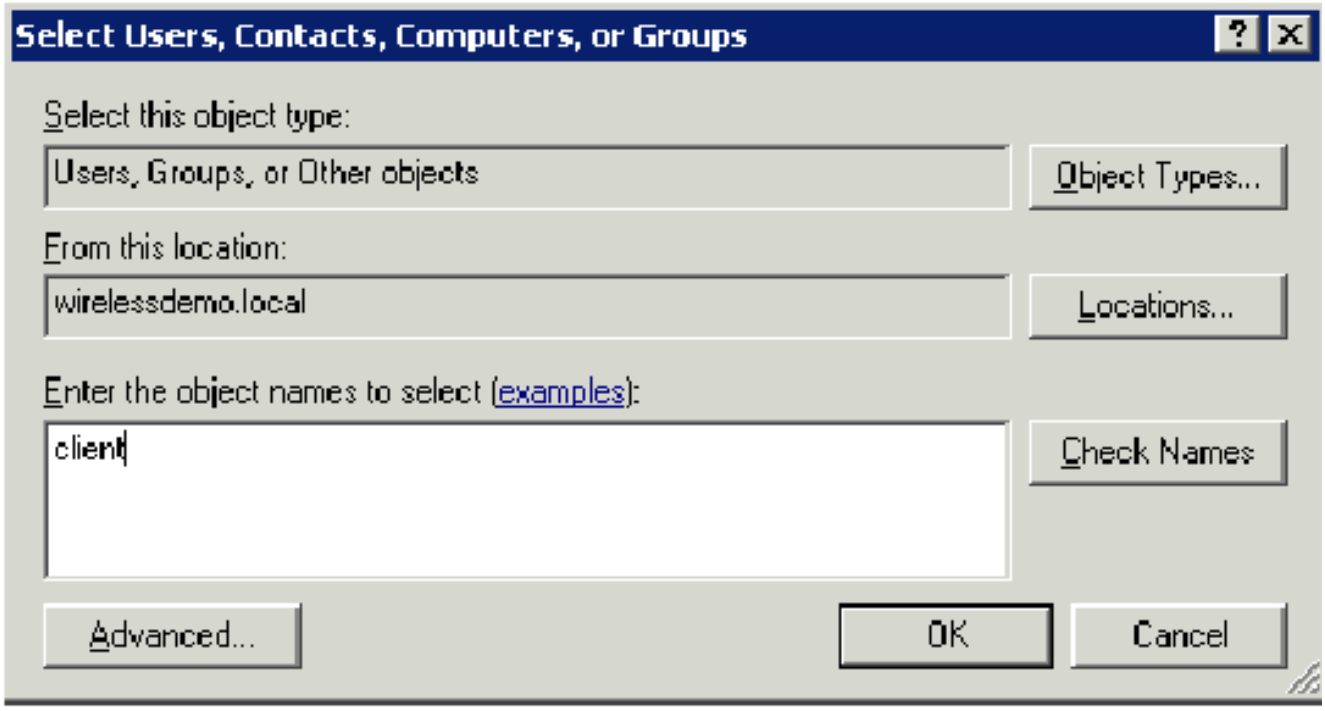


5. Per salvare le modifiche apportate al gruppo WirelessUsers, fare clic su **OK**.
6. Ripetere questa procedura per aggiungere altri utenti al gruppo.

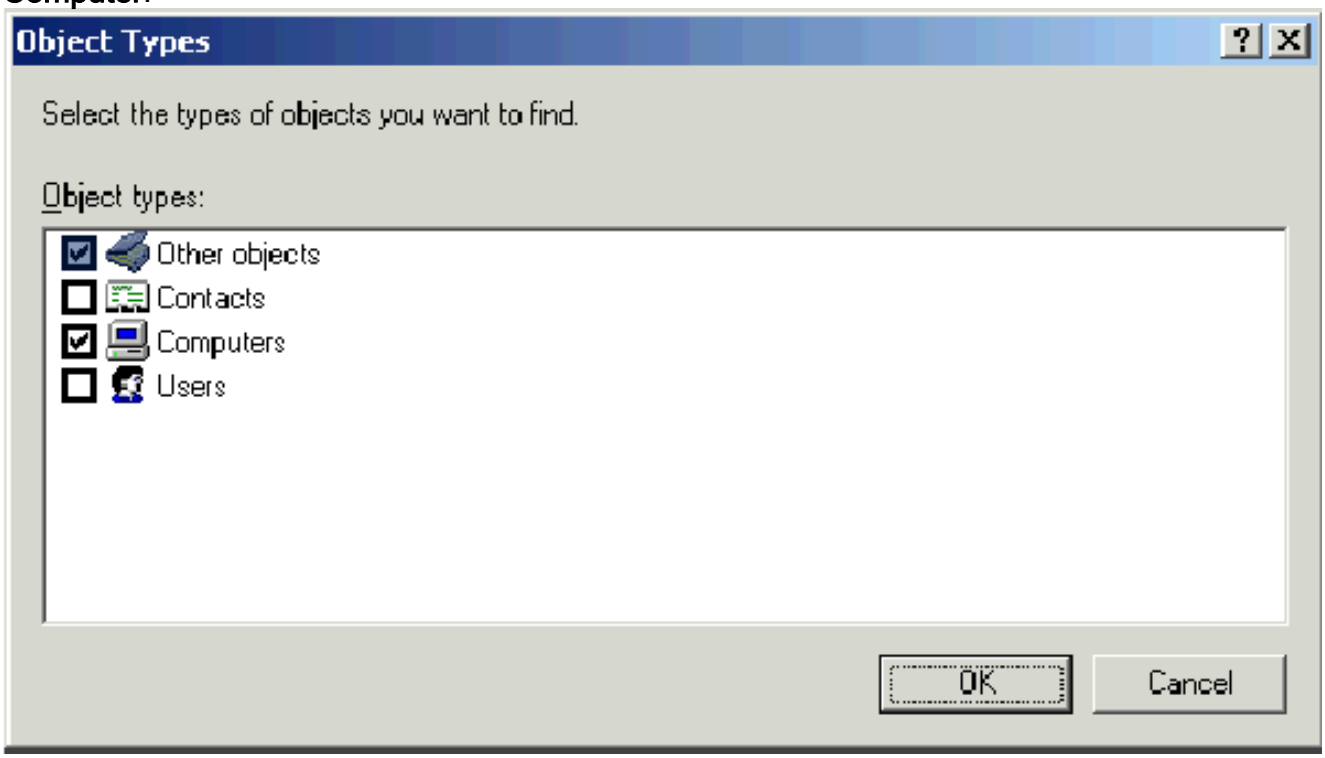
Passaggio 13: Aggiungi computer client al gruppo WirelessUsers

Attenersi alla seguente procedura:

1. Ripetere i passaggi 1 e 2 nella sezione Aggiunta di utenti al gruppo WirelessUsers di questo documento
2. Nella finestra di dialogo Seleziona utenti, contatti o computer digitare il nome del computer che si desidera aggiungere al gruppo. In questo esempio viene illustrato come aggiungere il computer denominato **client** al
gruppo.



3. Fare clic su **Tipi di oggetto**, deselezionare la casella di controllo **Utenti** e quindi selezionare **Computer**.



4. Fare clic su **OK** due volte. L'account del computer CLIENT viene aggiunto al gruppo WirelessUsers.
5. Ripetere la procedura per aggiungere altri computer al gruppo.

Installazione di Windows Standard 2003 con Cisco Secure ACS 4.0

Cisco Secure ACS è un computer che esegue Windows Server 2003 con SP1, Standard Edition, che fornisce l'autenticazione e l'autorizzazione RADIUS per il controller. Completare le procedure descritte in questa sezione per configurare ACS come server RADIUS:

Installazione e configurazione di base

Attenersi alla seguente procedura:

1. Installare Windows Server 2003 con SP1, Standard Edition come **server membro** denominato **ACS** nel dominio **wirelessdemo.local**.**Nota:** nelle altre configurazioni, il nome del server ACS viene visualizzato come cisco_w2003. Sostituire ACS o cisco_w2003 sull'installazione lab rimanente.
2. Per la connessione alla rete locale, configurare il protocollo TCP/IP con l'indirizzo IP **172.16.100.26**, la subnet mask **255.255.255.0** e l'indirizzo IP del server DNS **127.0.0.1**.

Installazione di Cisco Secure ACS 4.0

Nota: per ulteriori informazioni su come configurare Cisco Secure ACS 4.0 per Windows, consultare la Guida all'installazione di Cisco Secure ACS 4.0 per Windows.

Attenersi alla seguente procedura:

1. Utilizzando un account di amministratore di dominio, accedere al computer denominato ACS con Cisco Secure ACS.**Nota:** sono supportate solo le installazioni eseguite nel computer in cui si installa Cisco Secure ACS. Le installazioni remote eseguite utilizzando Servizi terminal Windows o prodotti quali VNC (Virtual Network Computing) non vengono testate e non sono supportate.
2. Inserire il CD Cisco Secure ACS nell'apposita unità del computer.
3. Se l'unità CD-ROM supporta la funzione di esecuzione automatica di Windows, viene visualizzata la finestra di dialogo Cisco Secure ACS for Windows Server.**Nota:** se nel computer non è installato un Service Pack necessario, viene visualizzata una finestra di dialogo. I service pack di Windows possono essere applicati prima o dopo l'installazione di Cisco Secure ACS. È possibile continuare l'installazione, ma il Service Pack richiesto deve essere applicato al termine dell'installazione. In caso contrario, Cisco Secure ACS potrebbe non funzionare in modo affidabile.
4. Eseguire una delle seguenti attività:Se viene visualizzata la finestra di dialogo Cisco Secure ACS for Windows Server, fare clic su **Installa**.Se la finestra di dialogo Cisco Secure ACS for Windows Server non viene visualizzata, eseguire **setup.exe**, che si trova nella directory principale del CD di Cisco Secure ACS.
5. Nella finestra di dialogo Cisco Secure ACS Setup viene visualizzato il contratto di licenza software.
6. Leggere il contratto di licenza del software. Se si accetta il contratto di licenza, fare clic su **Accetto**.Nella finestra di dialogo Benvenuti vengono visualizzate informazioni di base sul programma di installazione.
7. Dopo aver letto le informazioni nella finestra di dialogo iniziale, fare clic su **Avanti**.
8. Nella finestra di dialogo Prima di iniziare sono elencati gli elementi da completare prima di continuare con l'installazione. Se sono stati completati tutti gli elementi elencati nella finestra di dialogo Prima di iniziare, selezionare la casella corrispondente per ogni elemento e fare clic su **Avanti**.**Nota:** se non sono stati completati tutti gli elementi elencati nella casella Prima di iniziare, fare clic su **Annulla** e quindi su **Esci dall'installazione**. Dopo aver completato tutti gli elementi elencati nella finestra di dialogo Prima di iniziare, riavviare l'installazione.
9. Viene visualizzata la finestra di dialogo Scegli percorso di destinazione. In Cartella di

destinazione viene visualizzato il percorso di installazione. L'unità e il percorso in cui il programma di installazione installa Cisco Secure ACS.

10. Se si desidera modificare il percorso di installazione, attenersi alla seguente procedura:Fare clic su **Sfoglia**. Viene visualizzata la finestra di dialogo Scegli cartella. La casella Percorso contiene il percorso di installazione.Modificare il percorso di installazione. È possibile digitare il nuovo percorso nella casella Percorso oppure utilizzare gli elenchi Unità e directory per selezionare una nuova unità e directory. Il percorso di installazione deve trovarsi in un'unità locale del computer.**Nota:** non specificare un percorso contenente un carattere percentuale, "%". In questo caso, l'installazione potrebbe continuare correttamente ma non riuscire prima del completamento.Fare clic su **OK**.**Nota:** se è stata specificata una cartella che non esiste, il programma di installazione visualizza una finestra di dialogo per confermare la creazione della cartella. Per continuare, fare clic su **Sì**.
11. Nella finestra di dialogo Scegli percorso di destinazione, il nuovo percorso di installazione viene visualizzato in Cartella di destinazione.
12. Fare clic su **Next** (Avanti).
13. Nella finestra di dialogo Configurazione database di autenticazione sono elencate le opzioni per l'autenticazione degli utenti. È possibile eseguire l'autenticazione solo con il database utenti Cisco Secure o anche con un database utenti di Windows.**Nota:** dopo aver installato Cisco Secure ACS, è possibile configurare il supporto dell'autenticazione per tutti i tipi di database utenti esterni oltre ai database utenti di Windows.
14. Per autenticare gli utenti solo con il database Cisco Secure User, selezionare l'opzione **Check the Cisco Secure ACS database only**.
15. Se si desidera autenticare gli utenti tramite un database utenti di Windows Security Access Manager (SAM) o un database utenti di Active Directory oltre al database utenti di Cisco Secure, attenersi alla seguente procedura:Scegliere l'opzione **Controlla anche il database utenti di Windows**.La casella di controllo **Sì, fare riferimento a Concedi l'autorizzazione di accesso all'utente** diventa disponibile.**Nota:** la casella di controllo **Sì, fare riferimento all'**impostazione **"Concedi l'autorizzazione di chiamata all'utente"** si applica a tutte le forme di accesso controllate da Cisco Secure ACS, non solo all'accesso dial-in. Ad esempio, un utente che accede alla rete tramite un tunnel VPN non accede a un server di accesso alla rete. Tuttavia, se è selezionata la casella di impostazione **Sì, fare riferimento a Concedi autorizzazione di accesso remoto all'utente**, Cisco Secure ACS applica le autorizzazioni di accesso remoto dell'utente di Windows per determinare se concedere o meno all'utente l'accesso alla rete.Se si desidera consentire l'accesso agli utenti autenticati da un database utenti di dominio di Windows solo se dispongono dell'autorizzazione per la connessione remota nel proprio account di Windows, selezionare la casella di **impostazione Sì, fare riferimento a Concedi autorizzazione per la connessione remota all'utente**.
16. Fare clic su **Next** (Avanti).
17. Il programma di installazione installa Cisco Secure ACS e aggiorna il Registro di sistema di Windows.
18. Nella finestra di dialogo Opzioni avanzate sono elencate diverse funzionalità di Cisco Secure ACS non abilitate per impostazione predefinita. Per ulteriori informazioni su queste funzionalità, consultare la Guida per l'utente di Cisco Secure ACS per Windows Server, versione 4.0.**Nota:** le funzionalità elencate vengono visualizzate nell'interfaccia HTML di Cisco Secure ACS solo se vengono abilitate. Dopo l'installazione, è possibile attivarle o disattivarle nella pagina Opzioni avanzate della sezione Configurazione interfaccia.
19. Selezionare la casella corrispondente per ogni funzionalità che si desidera attivare.
20. Fare clic su **Next** (Avanti).

21. Verrà visualizzata la finestra di dialogo Monitoraggio servizio attivo.**Nota:** dopo l'installazione, è possibile configurare le funzionalità di controllo del servizio attivo nella pagina Gestione servizio attivo della sezione Configurazione di sistema.
22. Se si desidera che Cisco Secure ACS controlli i servizi di autenticazione degli utenti, selezionare la casella di controllo **Abilita monitoraggio accesso**. Dalla lista Script da eseguire scegliere l'opzione da applicare in caso di errore di un servizio di autenticazione:**Nessuna azione correttiva**: Cisco Secure ACS non esegue uno script.**Nota:** questa opzione è utile se si abilitano le notifiche tramite posta elettronica.**Riavvio**: Cisco Secure ACS esegue uno script che riavvia il computer su cui è in esecuzione Cisco Secure ACS.**Restart All**: Cisco Secure ACS riavvia tutti i servizi Cisco Secure ACS.**Restart RADIUS/TACACS+**—Cisco Secure ACS riavvia solo i servizi RADIUS e TACACS+.
23. Se si desidera che Cisco Secure ACS invii un messaggio di posta elettronica quando il monitoraggio del servizio rileva un evento, selezionare la casella **Notifica tramite posta**.
24. Fare clic su **Next** (Avanti).
25. Verrà visualizzata la finestra di dialogo Password crittografia database.**Nota:** la password di crittografia del database viene crittografata e archiviata nel Registro di sistema di ACS. Potrebbe essere necessario riutilizzare la password in caso di problemi critici e accedere al database manualmente. Tenere a portata di mano questa password per consentire al supporto tecnico di accedere al database. La password può essere modificata ad ogni scadenza.
26. Immettere una password per la crittografia del database. La password deve contenere almeno otto caratteri e contenere sia caratteri che cifre. Nessun carattere non valido. Fare clic su **Next** (Avanti).
27. Il programma di installazione termina e viene visualizzata la finestra di dialogo Cisco Secure ACS Service Initiation.
28. Selezionare la casella corrispondente per ciascuna opzione Cisco Secure ACS Services Initiation desiderata. Le azioni associate alle opzioni vengono eseguite al termine del programma di installazione.**Sì, avviare il servizio Cisco Secure ACS ora**—Avvia i servizi Windows che compongono Cisco Secure ACS. Se non si seleziona questa opzione, l'interfaccia HTML di Cisco Secure ACS non è disponibile a meno che non si riavvia il computer o il servizio CSAdmin.**Sì, avvia Cisco Secure ACS Administrator dal browser dopo l'installazione.** Apre l'interfaccia HTML Cisco Secure ACS nel browser Web predefinito per l'account utente di Windows corrente.**Sì, visualizza il file Leggimi**: apre il file README.TXT nel Blocco note di Windows.
29. Fare clic su **Next** (Avanti).
30. Se è stata selezionata un'opzione, vengono avviati i servizi Cisco Secure ACS. Nella finestra di dialogo Installazione completata vengono visualizzate informazioni sull'interfaccia HTML Cisco Secure ACS.
31. Fare clic su **Finish** (Fine).**Nota:** il resto della configurazione è documentato nella sezione relativa al tipo EAP configurato.

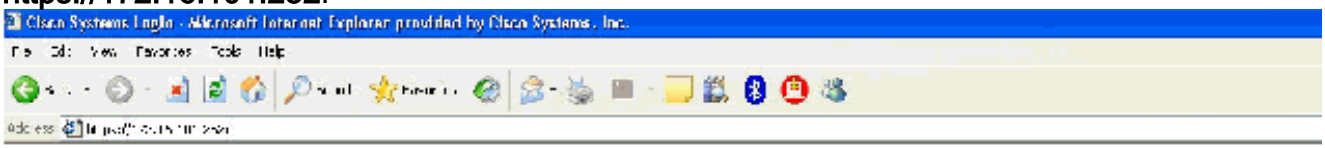
Configurazione controller Cisco LWAPP

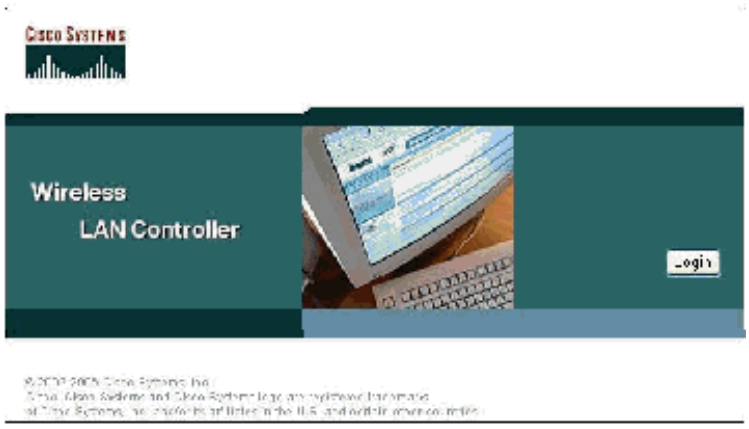
Creare la configurazione necessaria per WPA2/WPA

Attenersi alla seguente procedura:

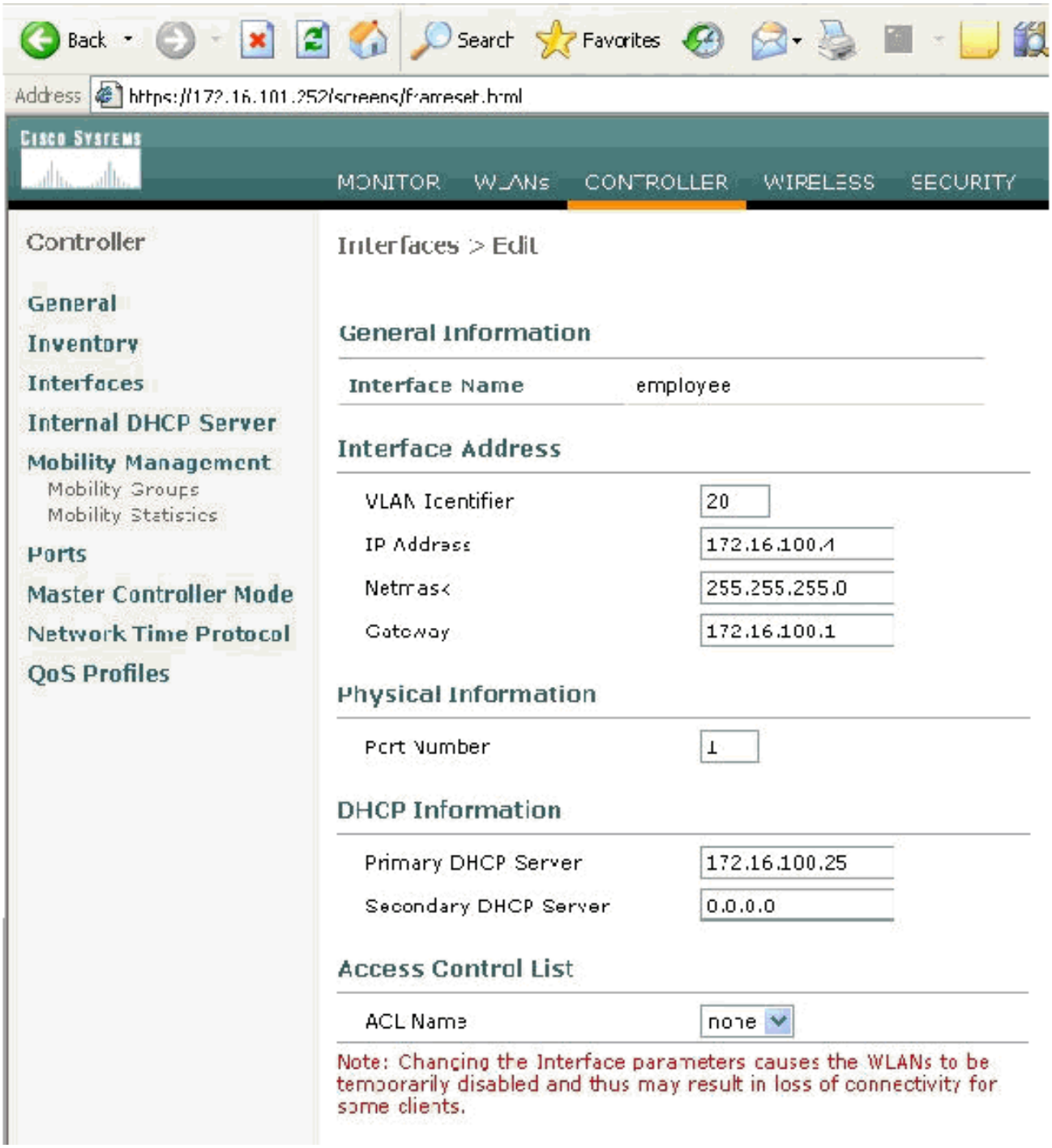
Nota: si presume che il controller disponga della connettività di base alla rete e che la raggiungibilità IP dell'interfaccia di gestione abbia esito positivo.

1. Accedere al controller selezionando **https://172.16.101.252**.

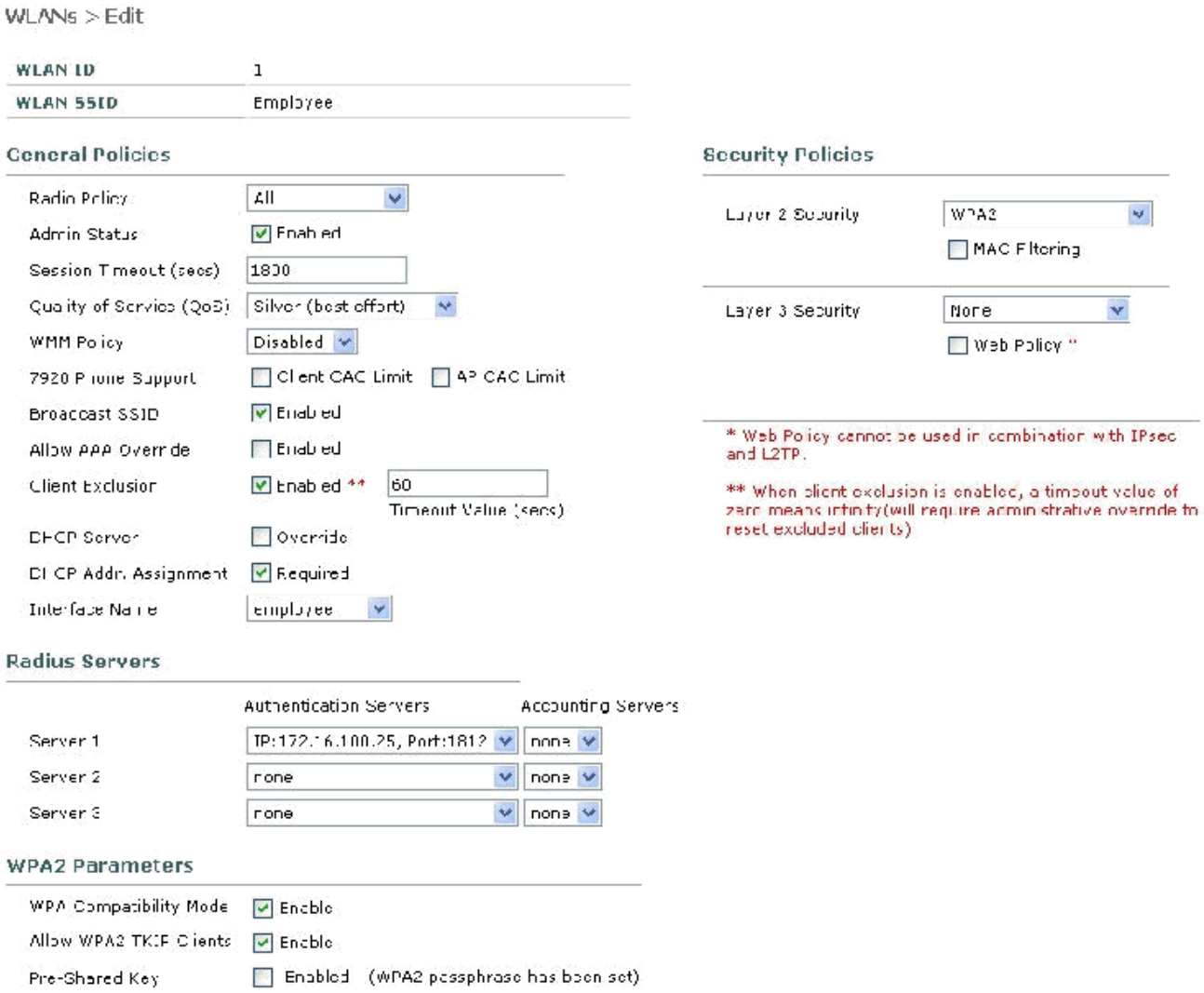




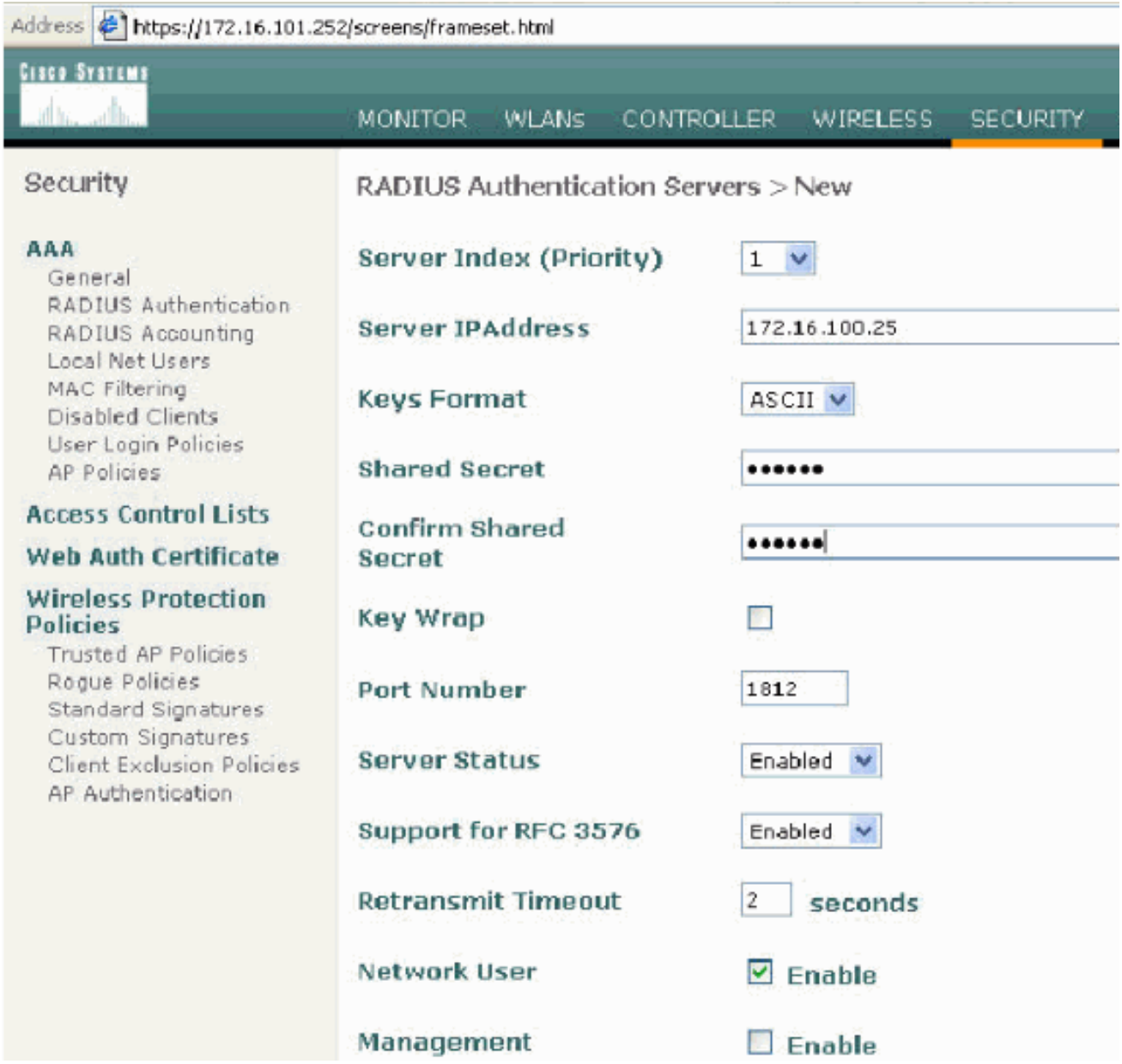
2. Fare clic su **Login**.
3. Accedere con l'utente **admin** predefinito e la password **admin** predefinita.
4. Creare il mapping dell'interfaccia VLAN nel menu Controller.
5. Fare clic su **Interfacce**.
6. Fare clic su **New**.
7. Nel campo Nome interfaccia digitare **Dipendente**. Questo campo può contenere qualsiasi valore.
8. Nel campo ID VLAN, digitare **20**. (Questo campo può essere qualsiasi VLAN trasportata nella rete.)
9. Fare clic su **Apply** (Applica).
10. Configurare le informazioni come mostrato nella finestra Interfacce > Modifica.

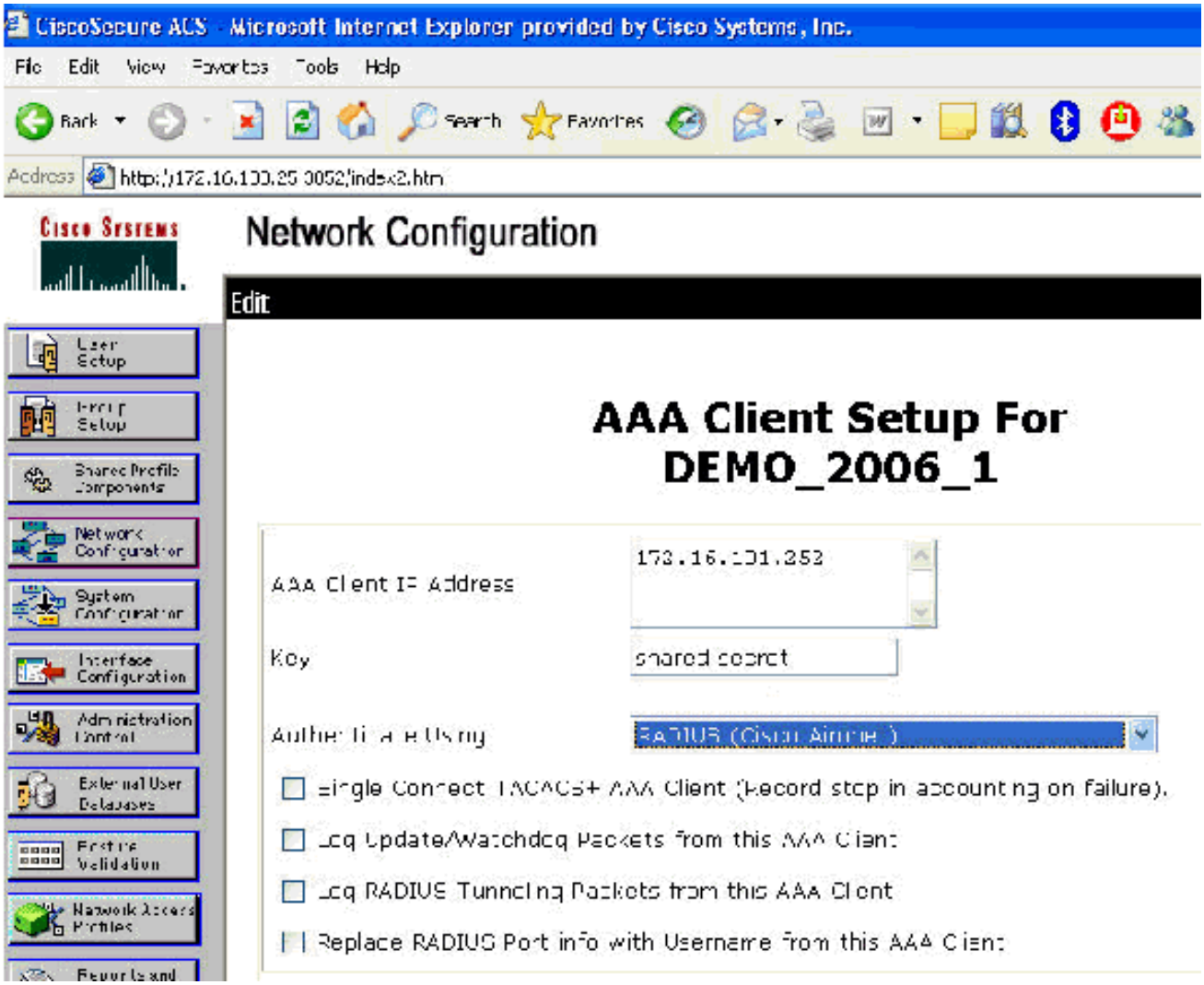


11. Fare clic su **Apply** (Applica).
12. Fare clic su **WLAN**.
13. Fare clic su **New**.
14. Nel campo SSID WLAN digitare **Dipendente**.
15. Fare clic su **Apply** (Applica).
16. Configurare le informazioni come mostrato in questa finestra WLAN > Modifica.**Nota:** WPA2 è il metodo di crittografia di livello 2 scelto per questa esercitazione. Per consentire l'associazione di WPA con i client TKIP-MIC a questo SSID, è inoltre possibile selezionare le caselle **Modalità compatibilità WPA** e **Consenti client TKIP WPA2** o i client che non supportano il metodo di crittografia 802.11i
AES.



17. Fare clic su **Apply** (Applica).
18. Fare clic sul menu **Protezione** e aggiungere il server RADIUS.
19. Fare clic su **New**.
20. Aggiungere l'indirizzo IP del server RADIUS (172.16.100.25) che è il server ACS configurato in precedenza.
21. Verificare che la chiave condivisa corrisponda al client AAA configurato nel server ACS.
22. Fare clic su **Apply** (Applica).


Address
https://172.16.101.252/screens/frameset.html
Cisco Systems
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
Security
AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Web Auth Certificate
Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Client Exclusion Policies
AP Authentication
RADIUS Authentication Servers > New
Server Index (Priority)
1
Server IPAddress
172.16.100.25
Keys Format
ASCII
Shared Secret
Confirm Shared Secret
Key Wrap
Port Number
1812
Server Status
Enabled
Support for RFC 3576
Enabled
Retransmit Timeout
2
seconds
Network User
Enable
Management
Enable



23. La configurazione di base è stata completata ed è possibile iniziare a eseguire il test di EAP-TLS.

Autenticazione EAP-TLS

L'autenticazione EAP-TLS richiede certificati computer e utente sul client wireless, l'aggiunta di EAP-TLS come tipo EAP al criterio di accesso remoto per l'accesso wireless e una riconfigurazione della connessione di rete wireless.

Per configurare DC_CA in modo che fornisca la registrazione automatica per i certificati del computer e degli utenti, completare le procedure descritte in questa sezione.

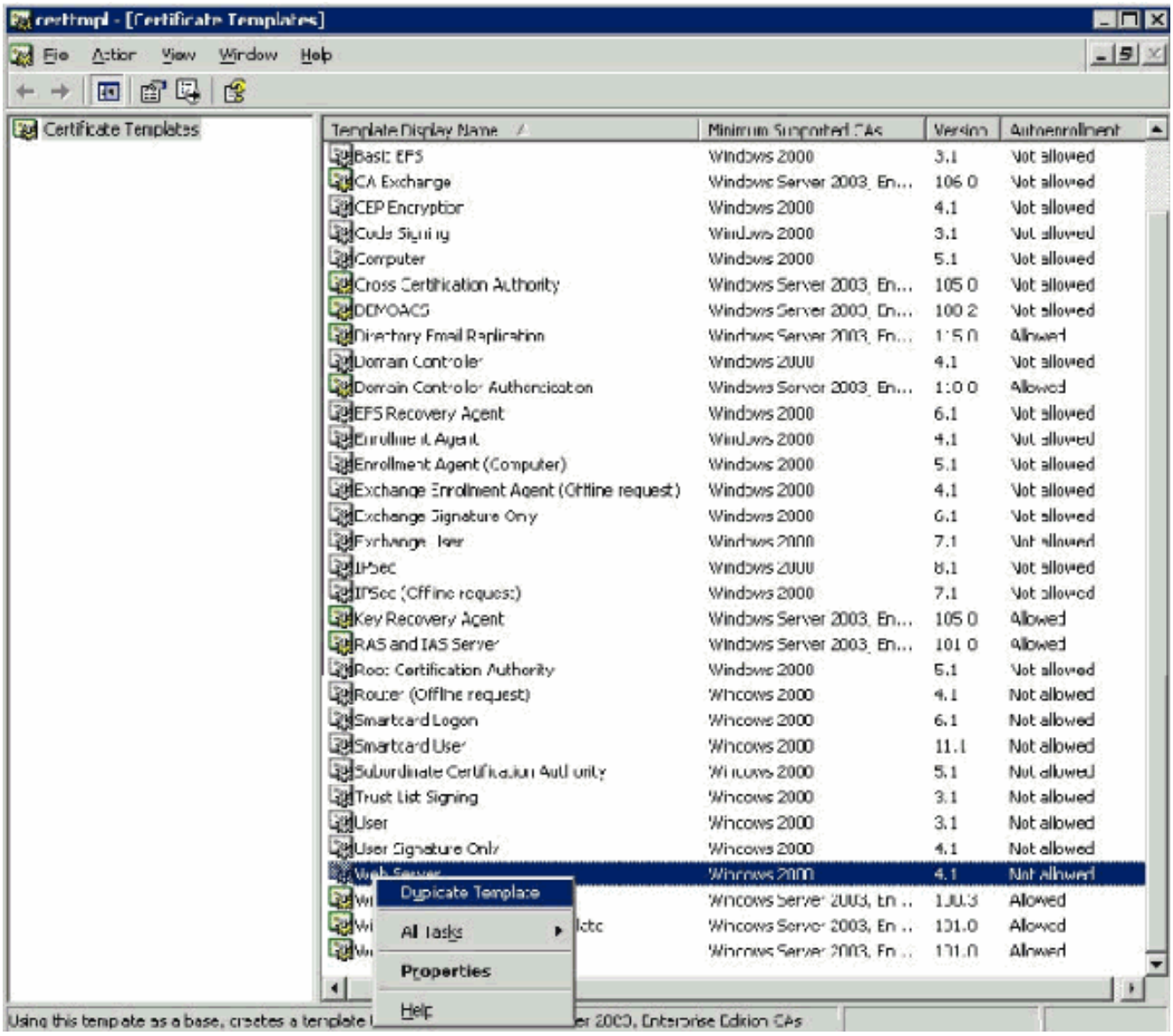
Nota: Microsoft ha modificato il modello Server Web con la release di Windows 2003 Enterprise CA in modo che le chiavi non siano più esportabili e l'opzione non sia disponibile. Non sono disponibili altri modelli di certificato forniti con i servizi certificati per l'autenticazione server e consentono di contrassegnare le chiavi come esportabili disponibili nell'elenco a discesa, pertanto è necessario creare un nuovo modello per tale operazione.

Nota: Windows 2000 consente l'esportazione di chiavi e queste procedure non devono essere seguite se si utilizza Windows 2000.

Installare lo snap-in Modelli di certificato

Attenersi alla seguente procedura:

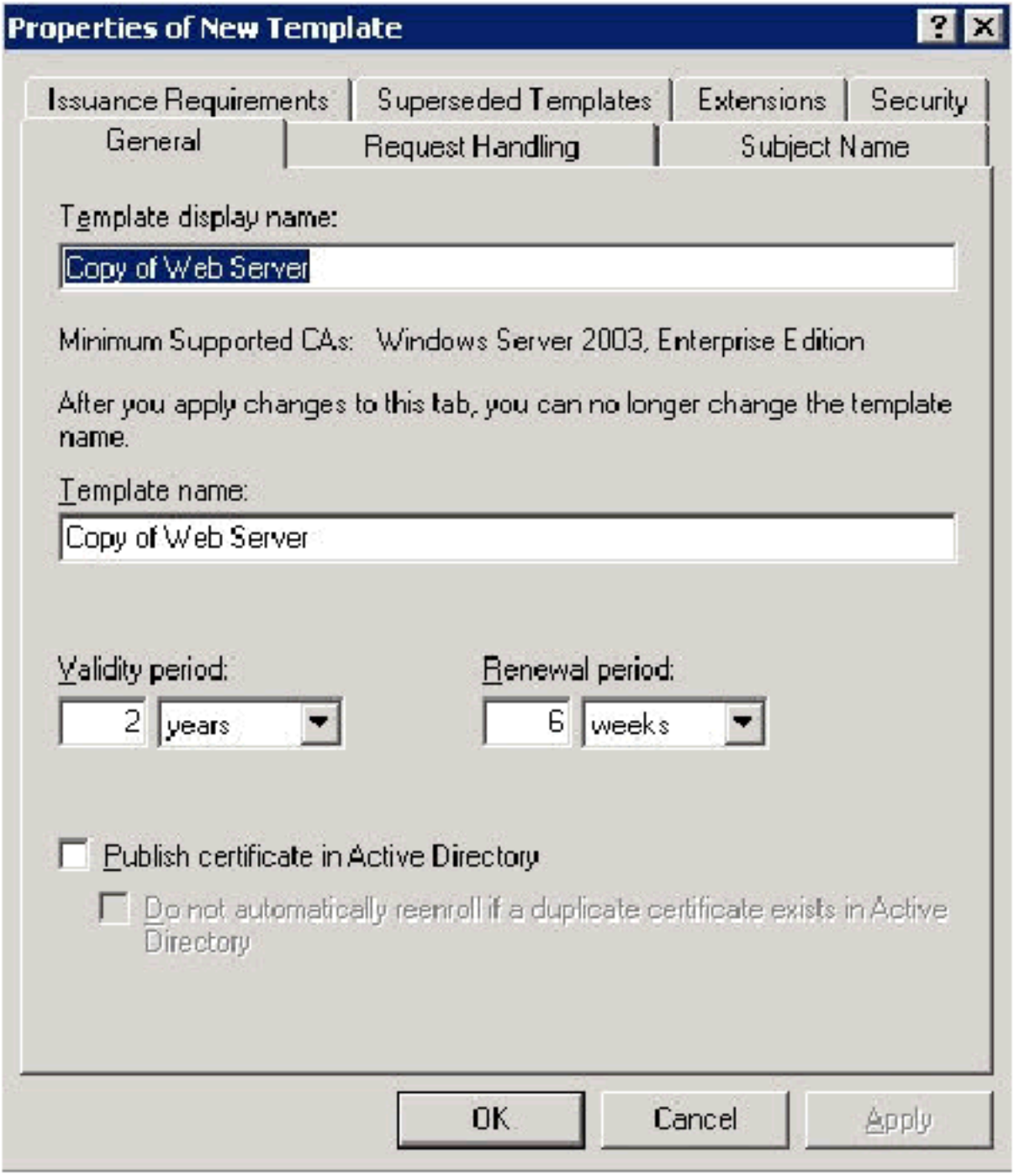
1. Scegliere **Start > Esegui**, digitare **mmc**, quindi fare clic su **OK**.
2. Scegliere **Aggiungi/Rimuovi snap-in** dal menu File e quindi fare clic su **Aggiungi**.
3. In Snap-in fare doppio clic su **Modelli di certificato**, fare clic su **Chiudi** e quindi su **OK**.
4. Nell'albero della console fare clic su **Modelli di certificato**. Tutti i modelli di certificato vengono visualizzati nel riquadro dei dettagli.
5. Per ignorare i passaggi da 2 a 4, digitare **certtmpl.msc** per aprire lo snap-in Modelli di certificato.



Creare il modello di certificato per il server Web ACS

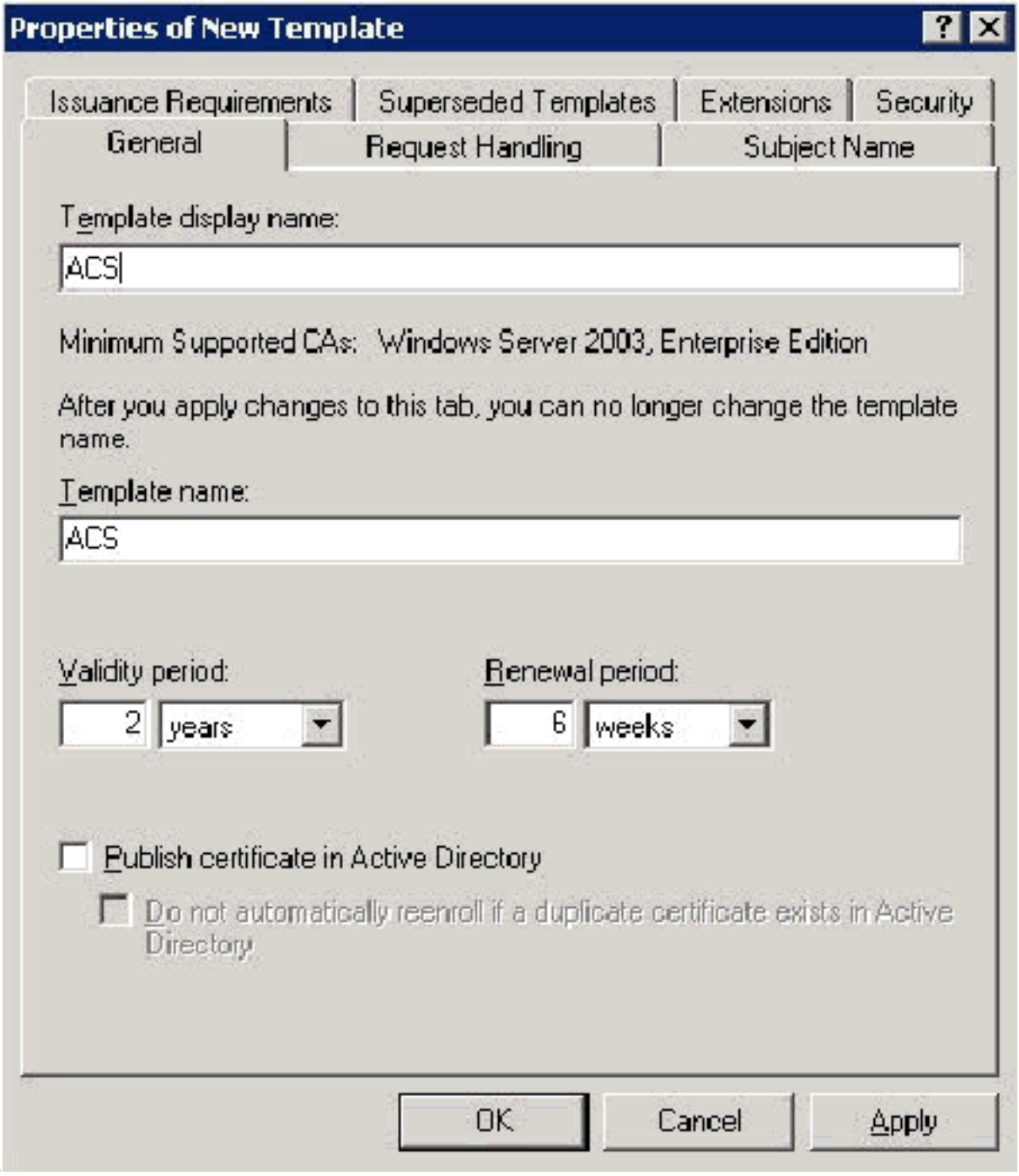
Attenersi alla seguente procedura:

1. Nel riquadro dei dettagli dello snap-in Modelli di certificato fare clic sul modello **Server Web**.
2. Scegliere **Duplica modello** dal menu



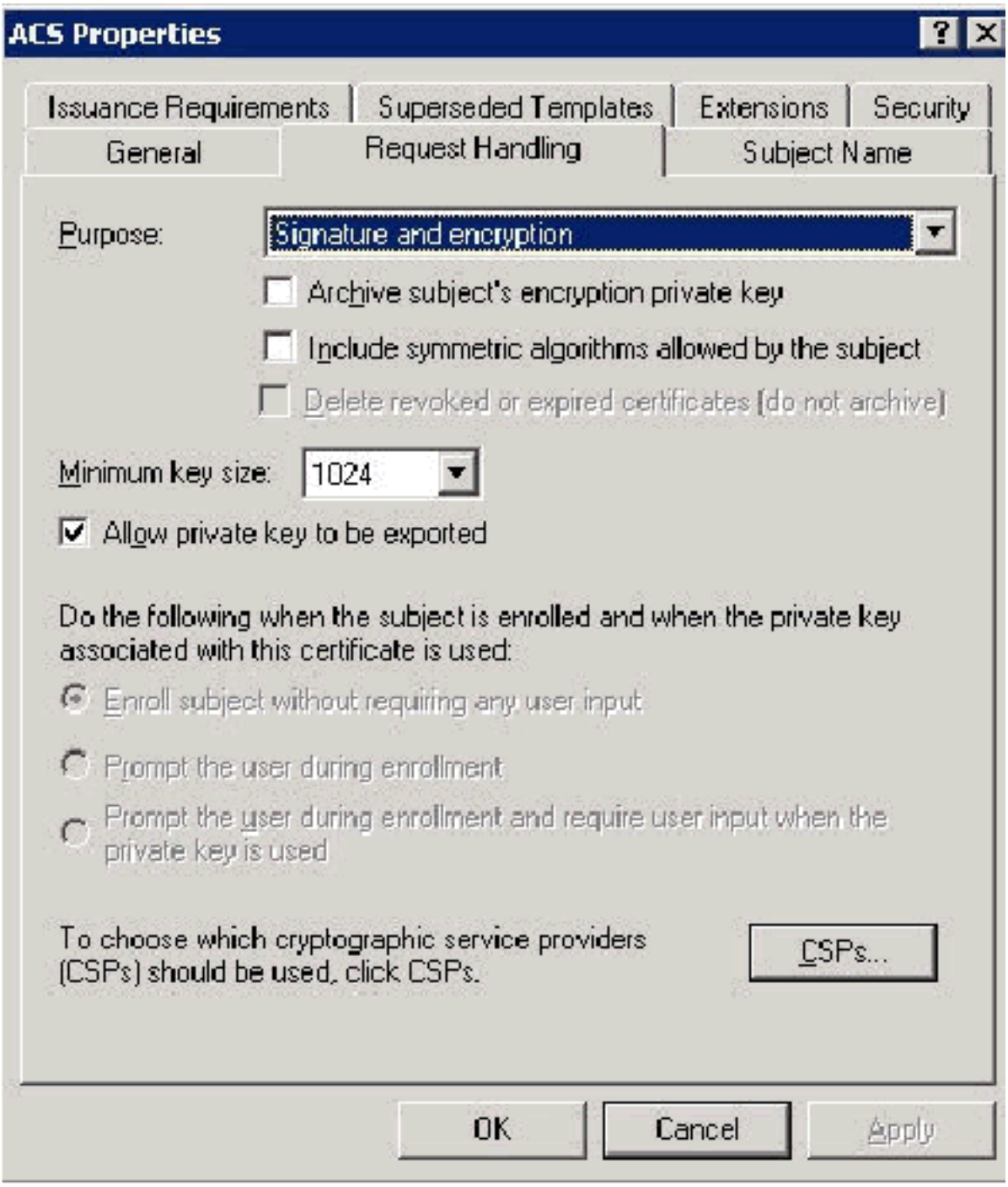
Azione.

3. Nel campo Nome visualizzato modello, digitare



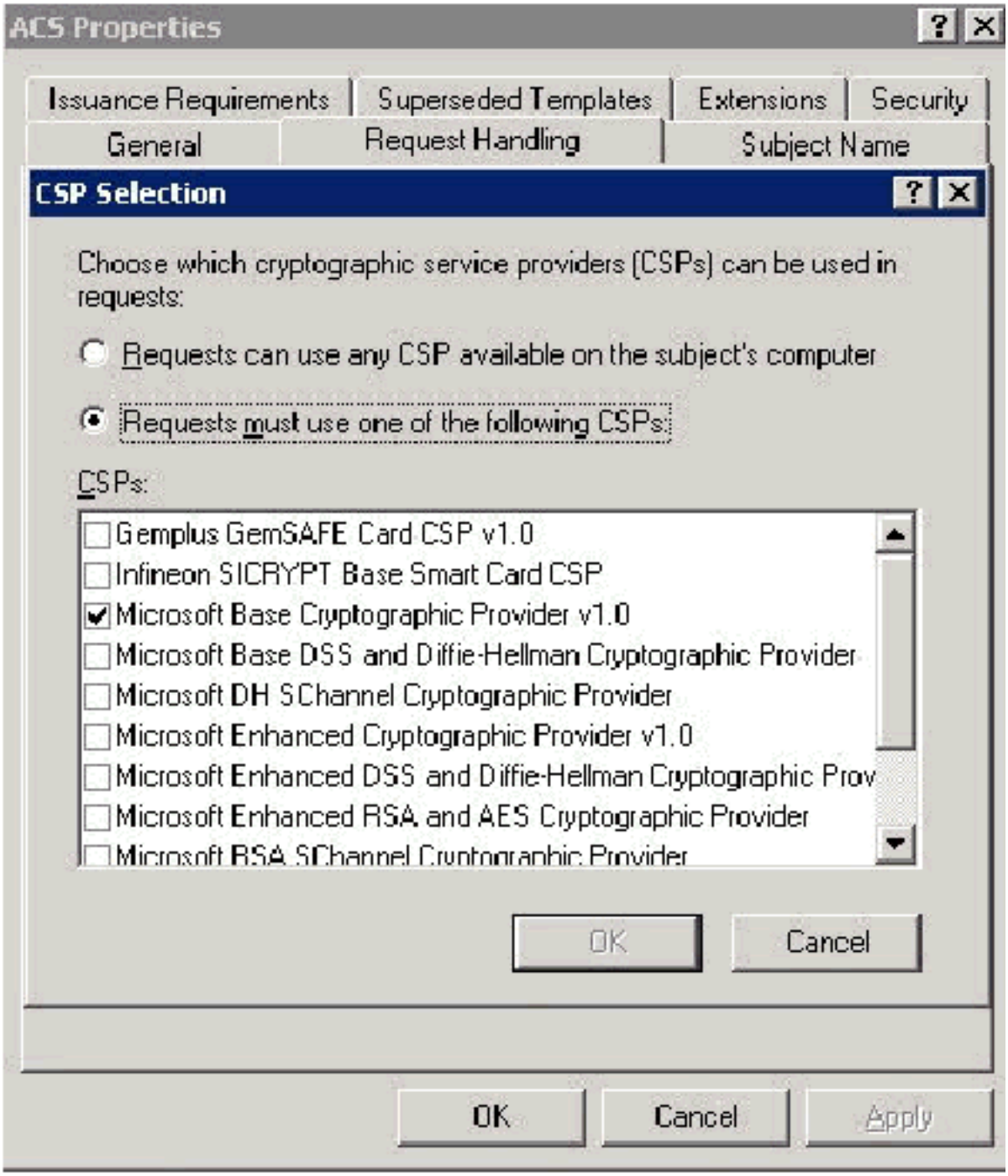
ACS.

4. Andare alla scheda Gestione richieste e selezionare **Consenti esportazione della chiave**



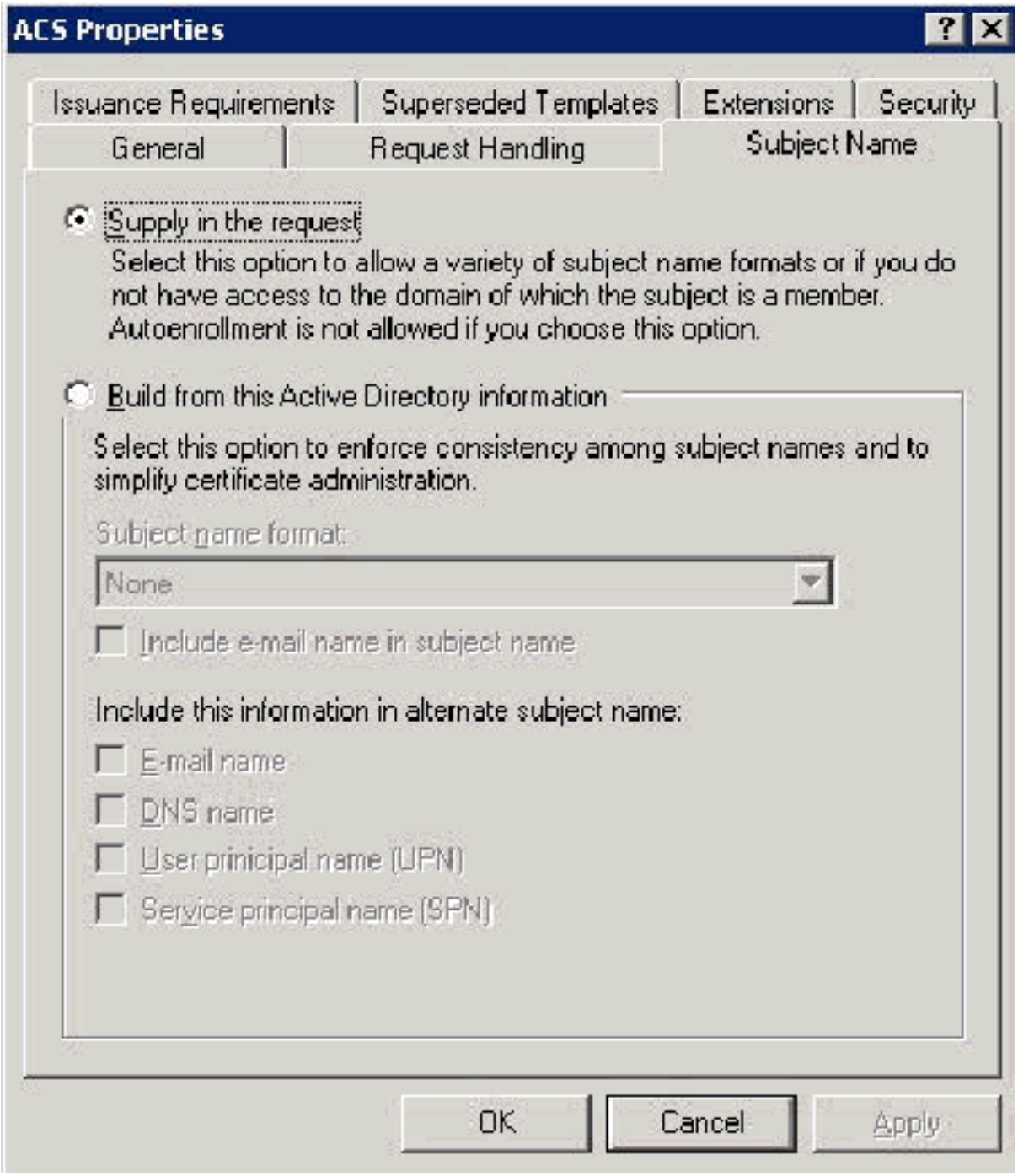
privata.

5. Scegliere **Le richieste devono utilizzare uno dei seguenti CSP** e selezionare **Microsoft Base Cryptographic Provider v1.0**. Deselezionare tutti gli altri CSP selezionati e fare clic su



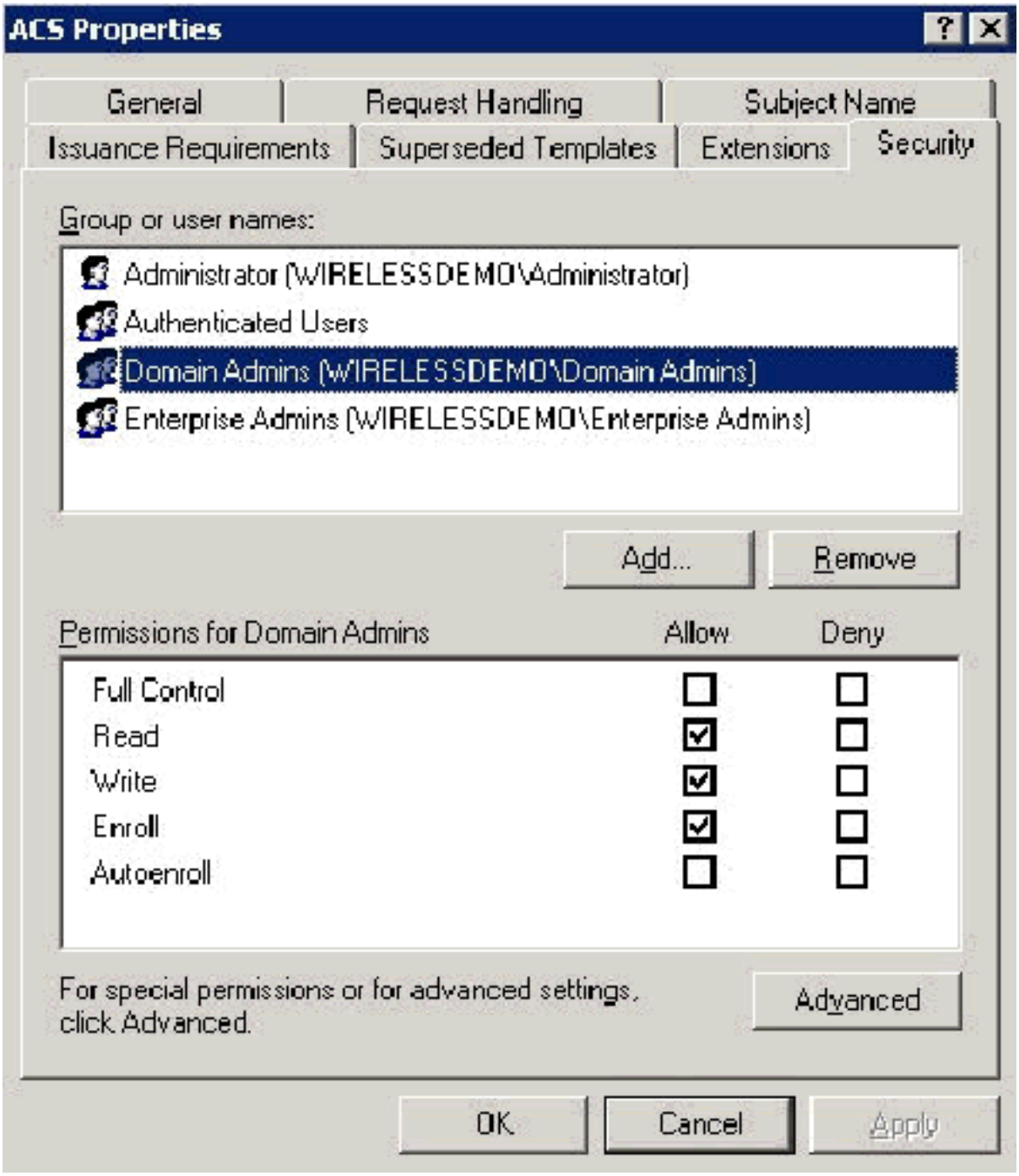
OK.

6. Andare alla scheda Nome soggetto, scegliere **Fornitura nella richiesta** e fare clic su

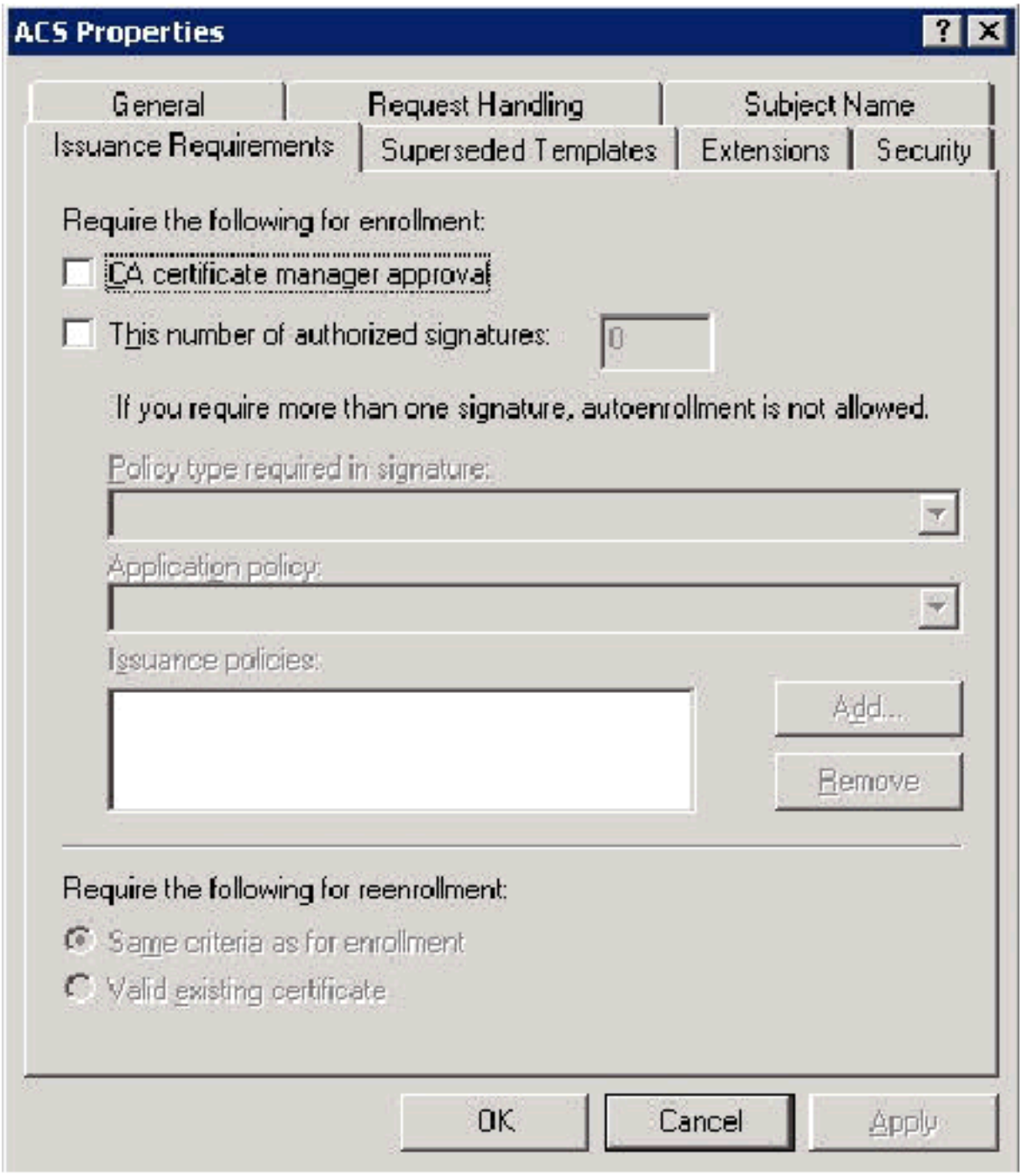


OK.

7. Selezionare la scheda Protezione, evidenziare il **gruppo Domain Admins** e verificare che l'opzione **Enroll** sia selezionata in Allowed.**Importante:** Se si sceglie di compilare solo da queste informazioni di Active Directory, selezionare **Nome dell'entità utente (UPN)** e deselezionare **Includi nome di posta elettronica** in Nome oggetto e Nome di posta elettronica perché non è stato immesso un nome di posta elettronica per l'account WirelessUser nello snap-in Utenti e computer di Active Directory. Se queste due opzioni non vengono disattivate, la registrazione automatica tenterà di utilizzare la posta elettronica, generando un errore di registrazione
automatica.



8. Se necessario, sono disponibili misure di protezione aggiuntive per impedire che i certificati vengano automaticamente estratti. Tali informazioni sono disponibili nella scheda Requisiti di rilascio. Ciò non viene ulteriormente discusso nel presente documento.

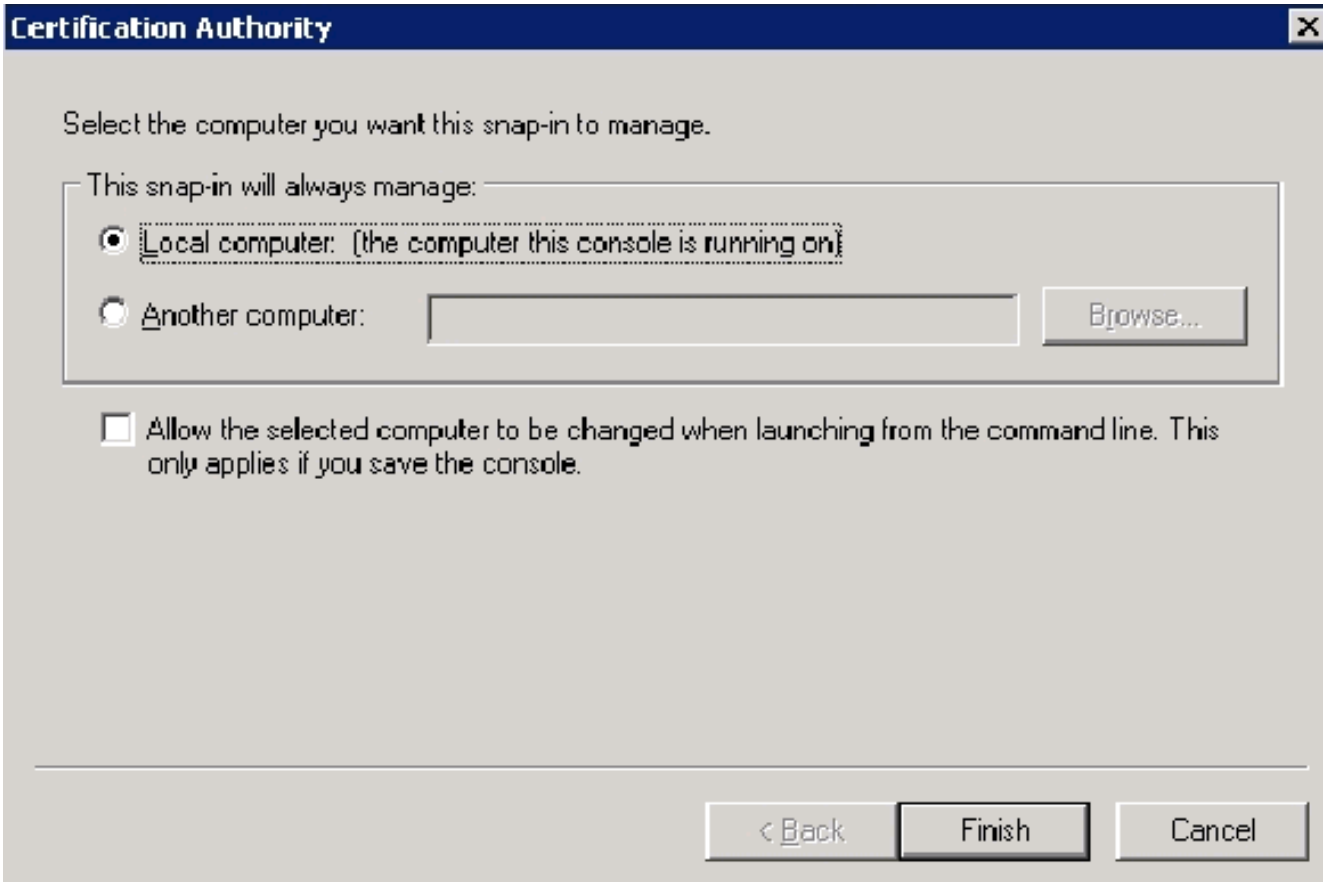


9. Fare clic su **OK** per salvare il modello e passare alla generazione del modello dallo snap-in Autorità di certificazione.

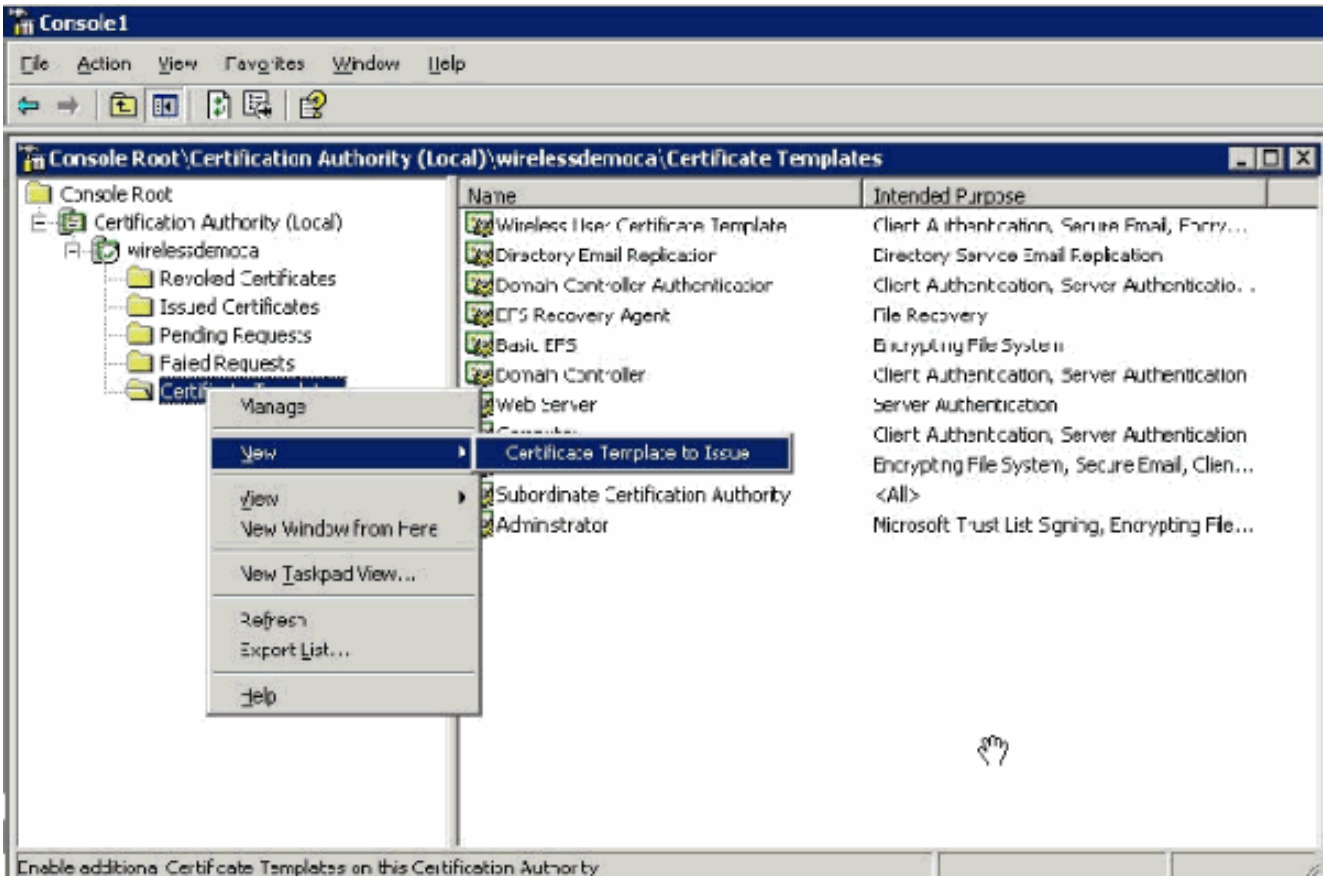
Abilita il nuovo modello di certificato server Web ACS

Attenersi alla seguente procedura:

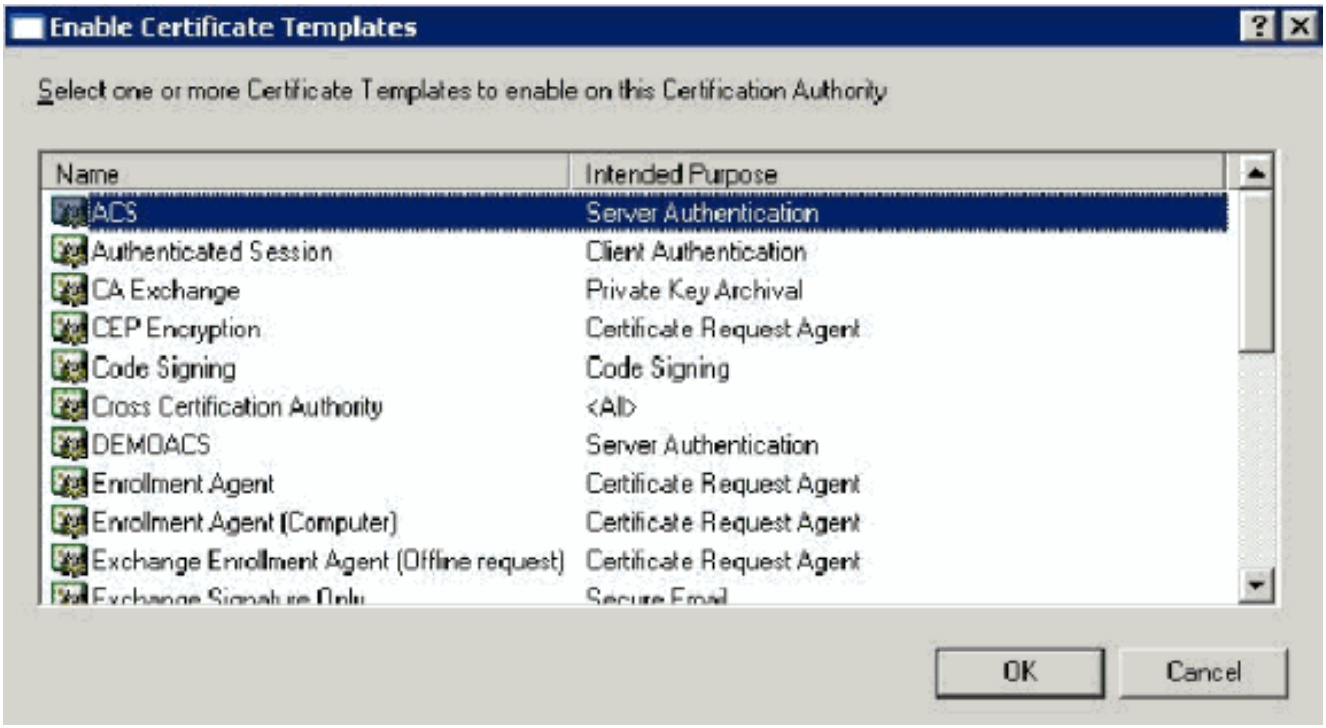
1. Aprire lo snap-in **Autorità di certificazione**. Seguire i passaggi da 1 a 3 nella sezione Creazione del modello di certificato per il server Web ACS, scegliere l'opzione **Autorità di certificazione**, scegliere **Computer locale** e fare clic su **Fine**.



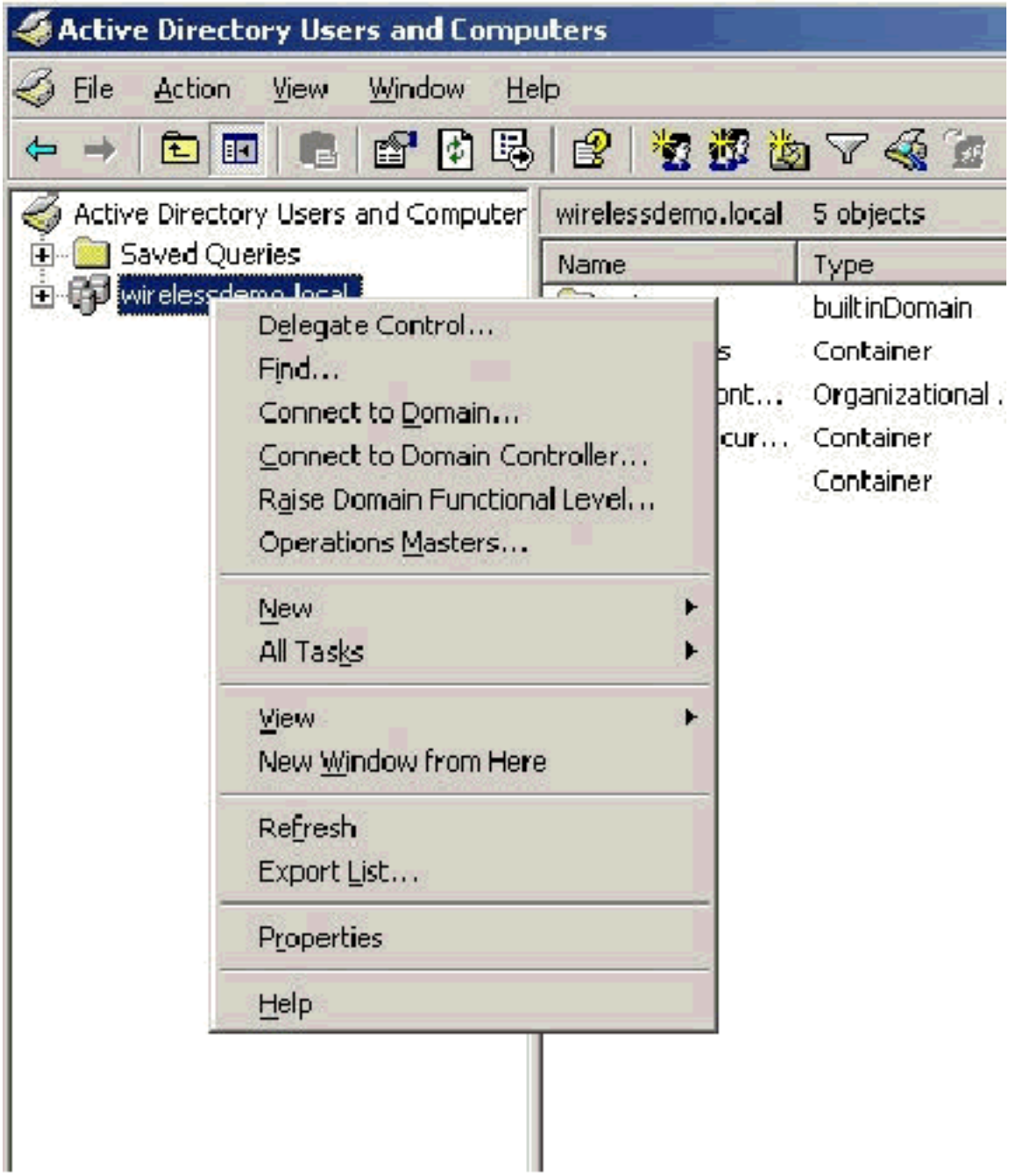
2. Nell'albero della console espandere **demo wireless** e quindi fare clic con il pulsante destro del mouse su **Modelli di certificato**.



3. Scegliere **Nuovo > Modello di certificato da rilasciare**.
4. Fare clic sul modello di certificato **ACS**.

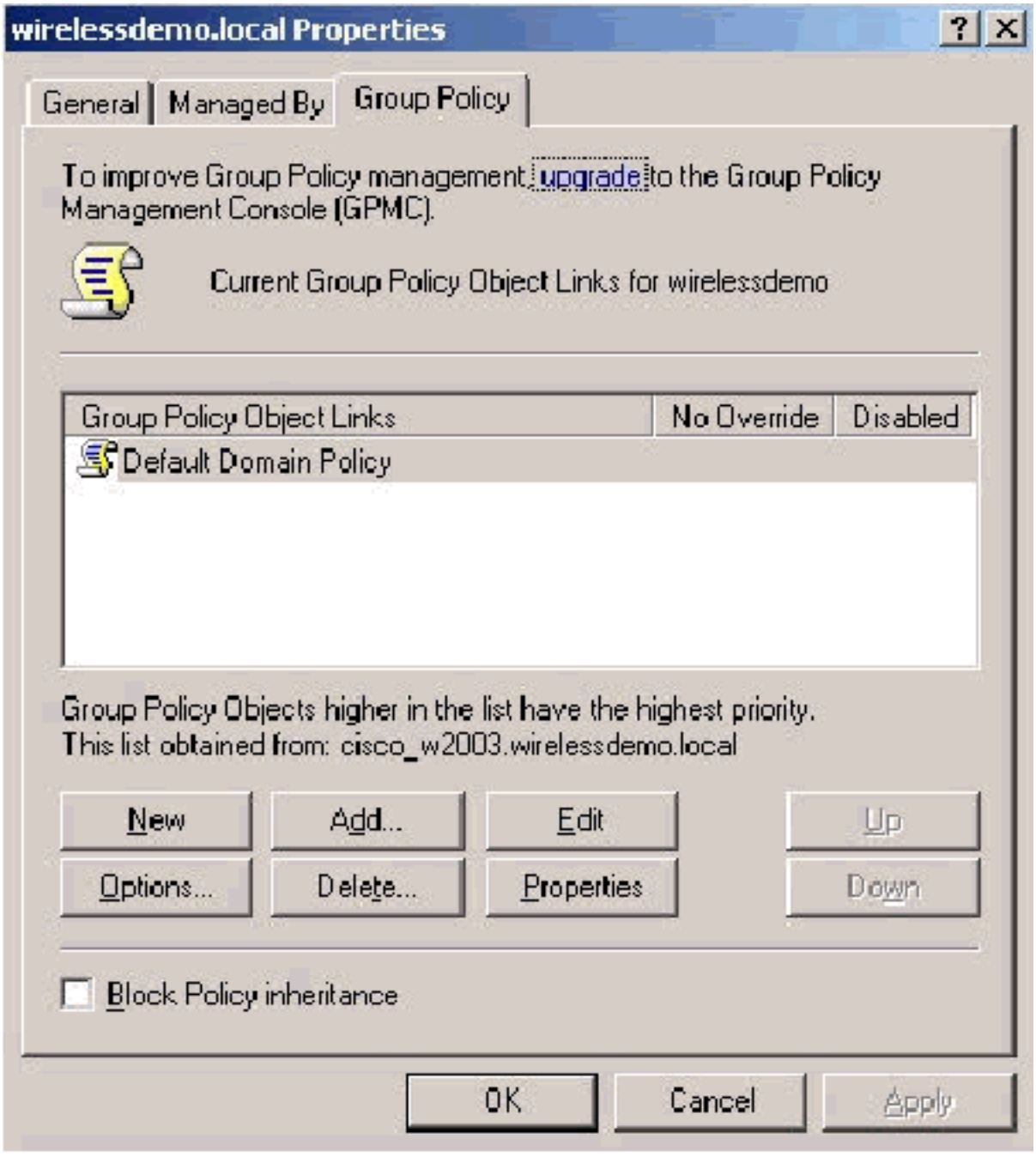


5. Fare clic su **OK** e aprire **lo snap-in Utenti e computer di Active Directory**.
6. Nell'albero della console fare doppio clic su **Utenti e computer di Active Directory**, fare clic con il pulsante destro del mouse sul **dominio wirelessdemo.local** e quindi scegliere



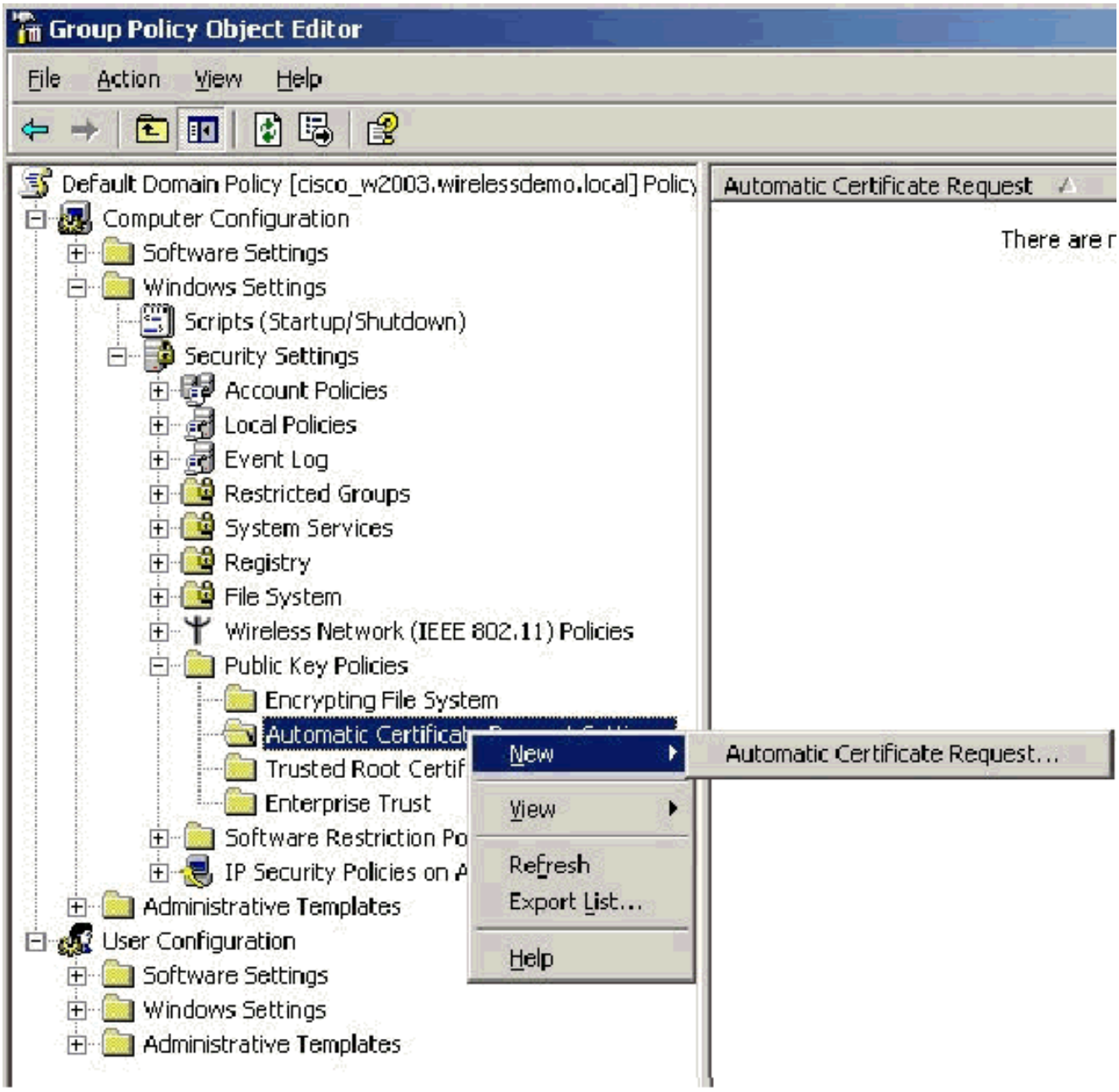
Proprietà.

7. Nella scheda Criteri di gruppo fare clic su **Criterio dominio predefinito** e quindi su **Modifica**. Verrà aperto lo snap-in Editor oggetti Criteri di

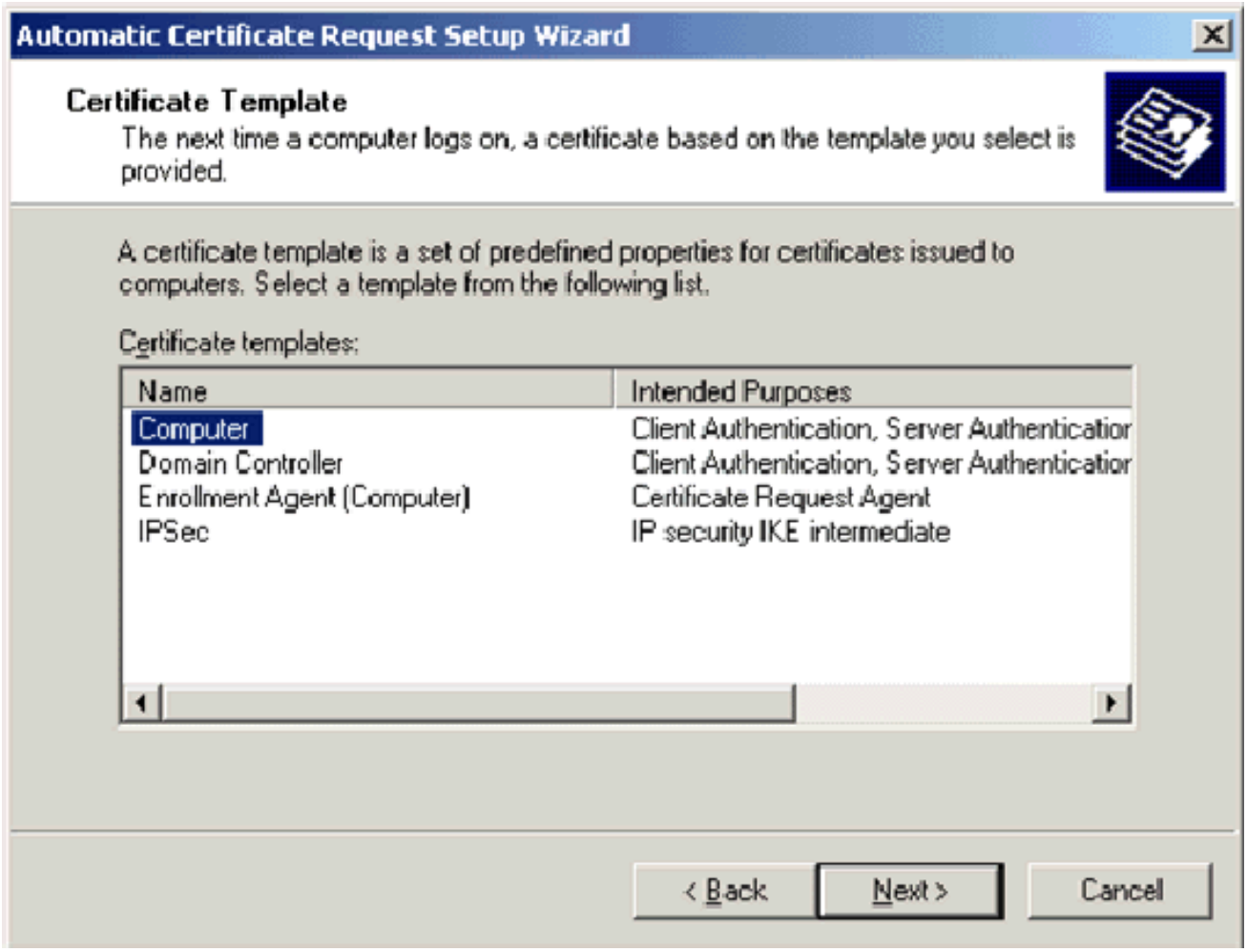


gruppo.

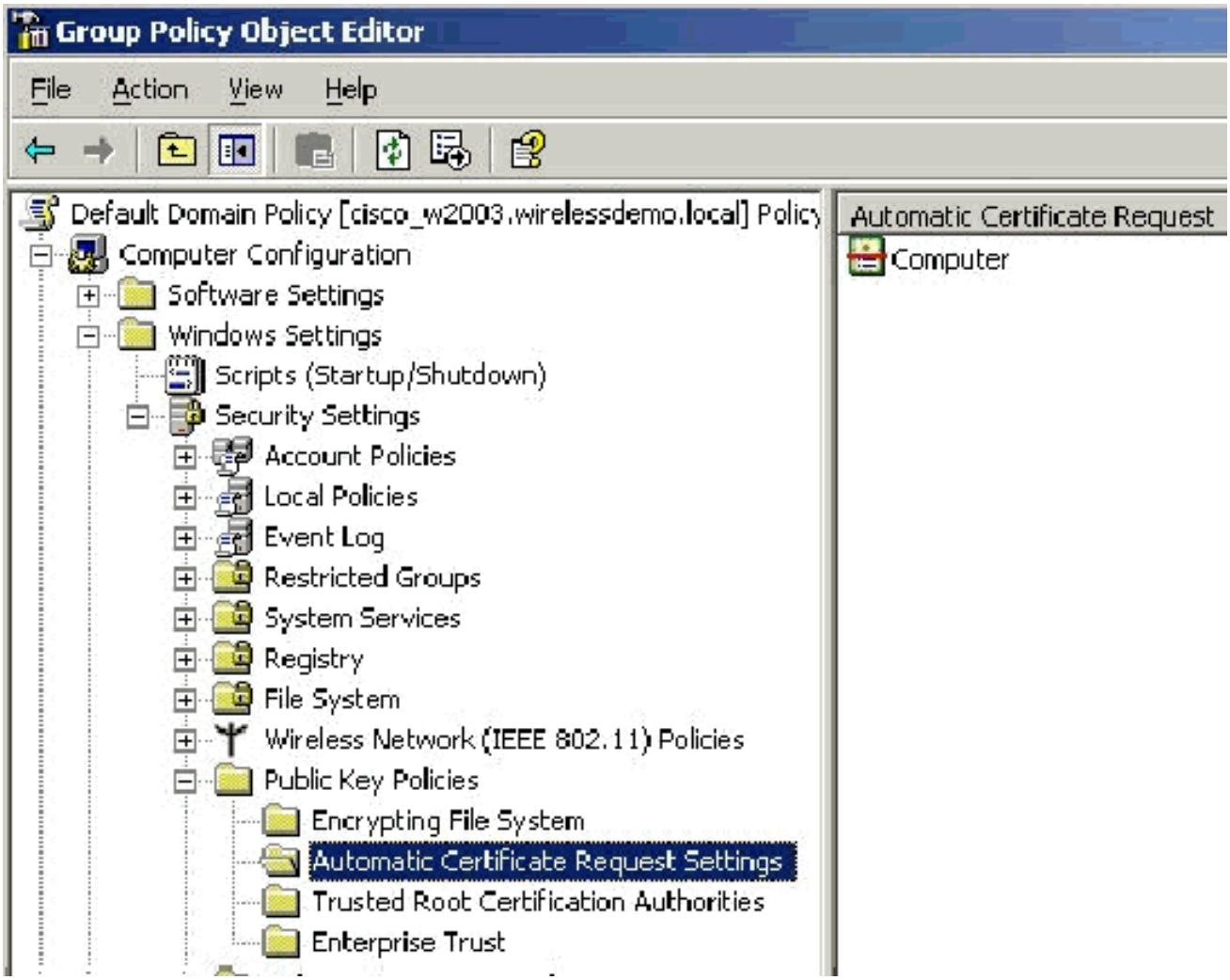
8. Nell'albero della console espandere **Configurazione computer > Impostazioni di Windows > Impostazioni protezione > Criteri chiave pubblica**, quindi selezionare **Impostazioni richiesta automatica certificati**.



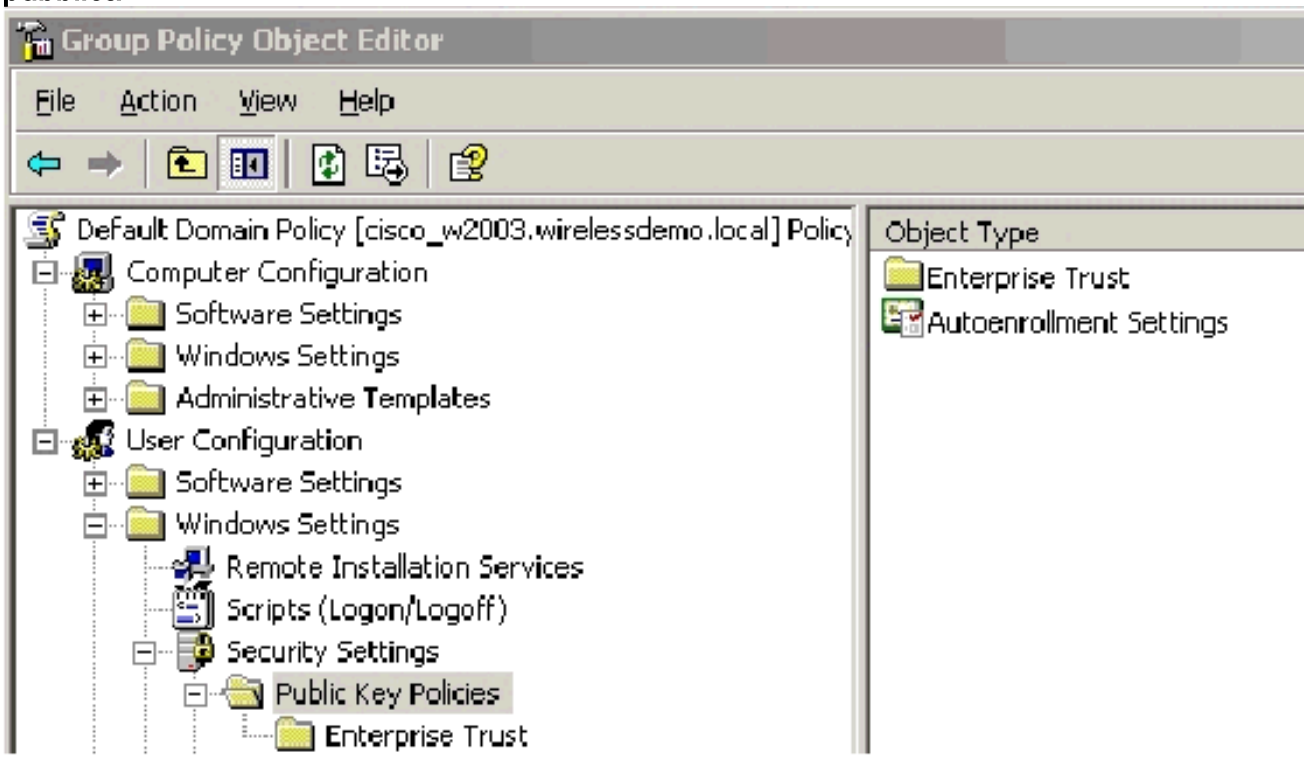
9. Fare clic con il pulsante destro del mouse su **Impostazioni richiesta automatica certificati** e scegliere **Nuovo > Richiesta automatica certificati**.
10. Nella pagina Installazione guidata richiesta automatica certificati fare clic su **Avanti**.
11. Nella pagina Modello di certificato fare clic su **Computer**, quindi su **Avanti**.



12. Nella pagina Completamento dell'Installazione guidata richiesta automatica certificati fare clic su **Fine**.Il tipo di certificato Computer verrà visualizzato nel riquadro dei dettagli dello snap-in Editor oggetti Criteri di
gruppo.

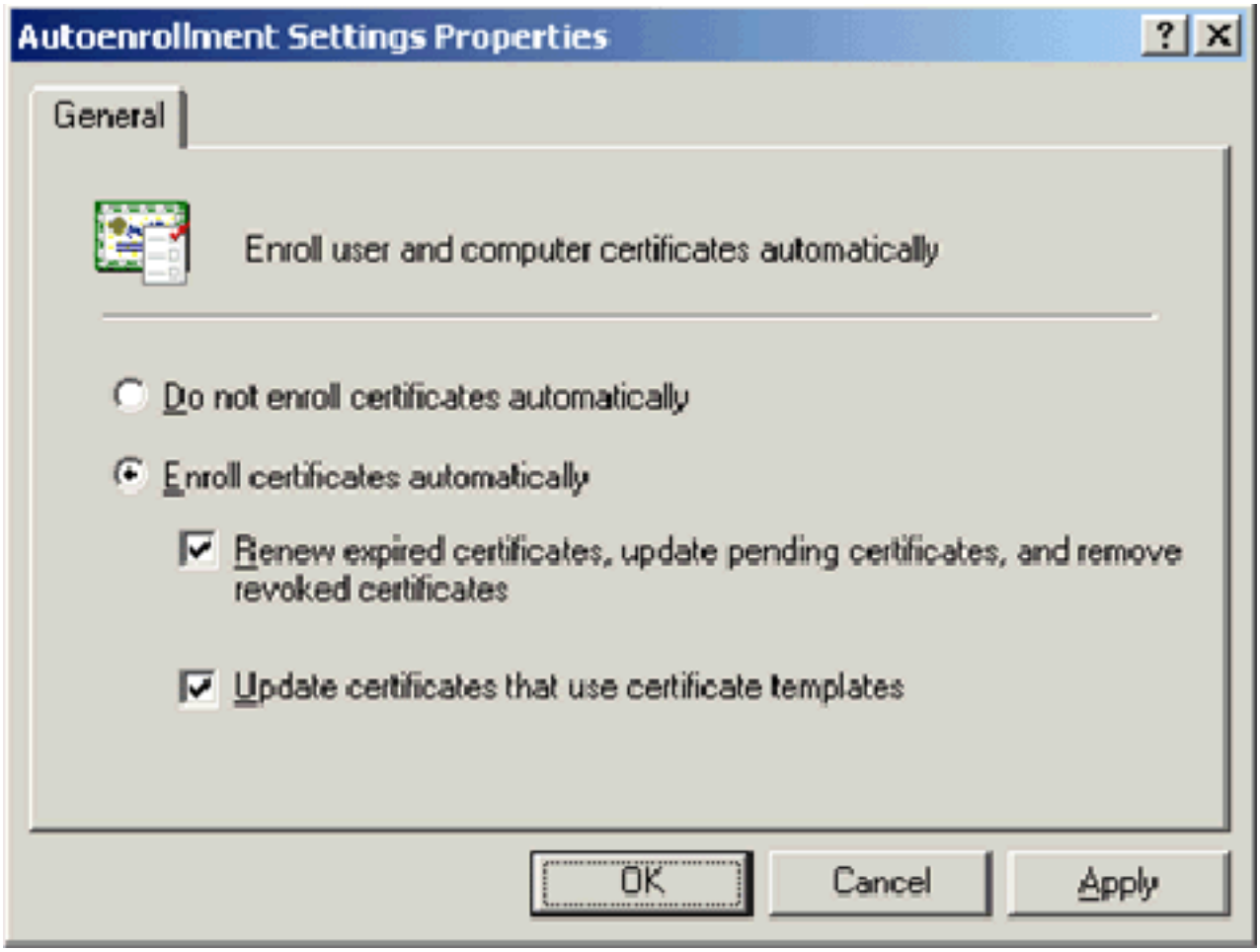


13. Nell'albero della console espandere **Configurazione utente > Impostazioni di Windows > Impostazioni protezione > Criteri chiave pubblica**.



14. Nel riquadro dei dettagli fare doppio clic su **Impostazioni registrazione automatica**.
15. Scegliere **Registra automaticamente i certificati** e selezionare **Rinnova i certificati scaduti,**

aggiorna i certificati in sospeso e rimuovi i certificati revocati e Aggiorna i certificati che utilizzano modelli di
certificato.



16. Fare clic su **OK**.

Installazione certificato ACS 4.0

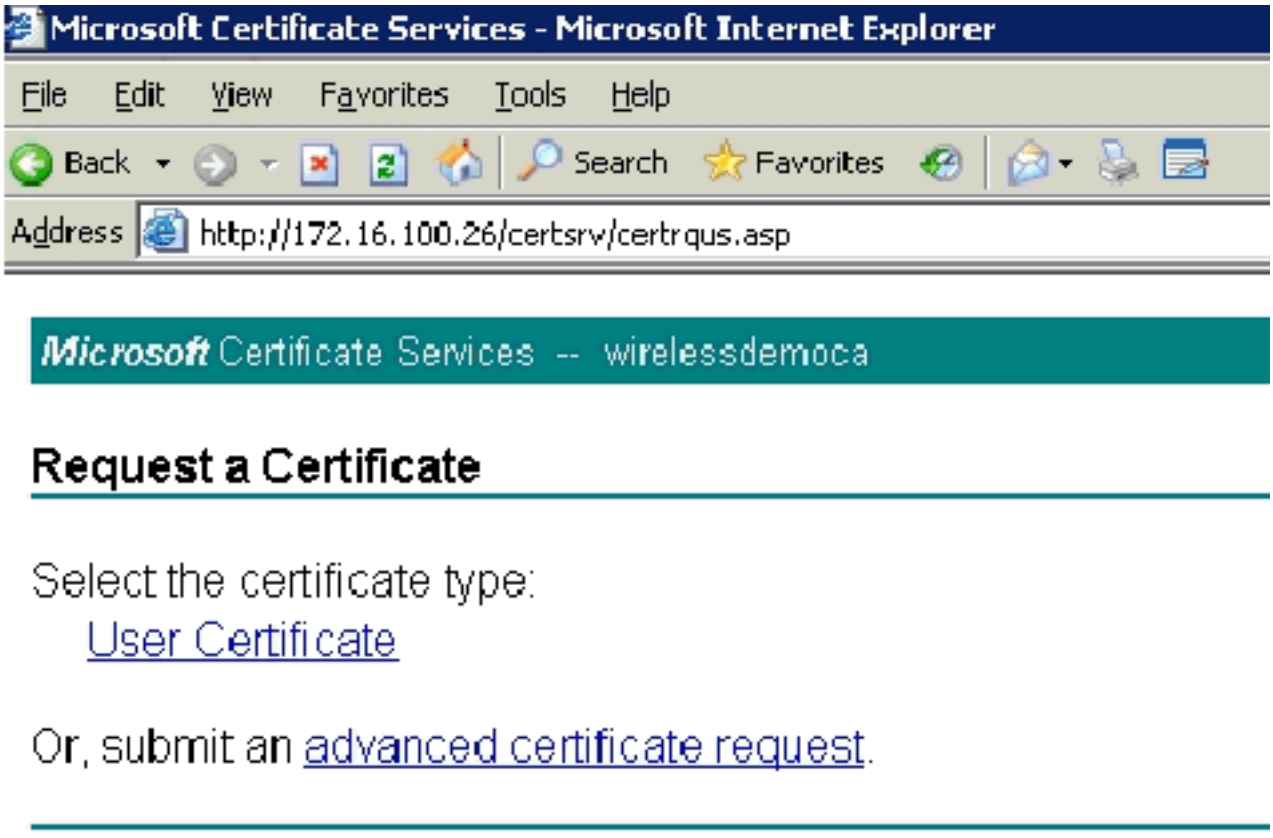
Configura certificato esportabile per ACS

Importante: Per autenticare un client WLAN EAP-TLS, il server ACS deve ottenere un certificato server dal server CA radice dell'organizzazione (enterprise).

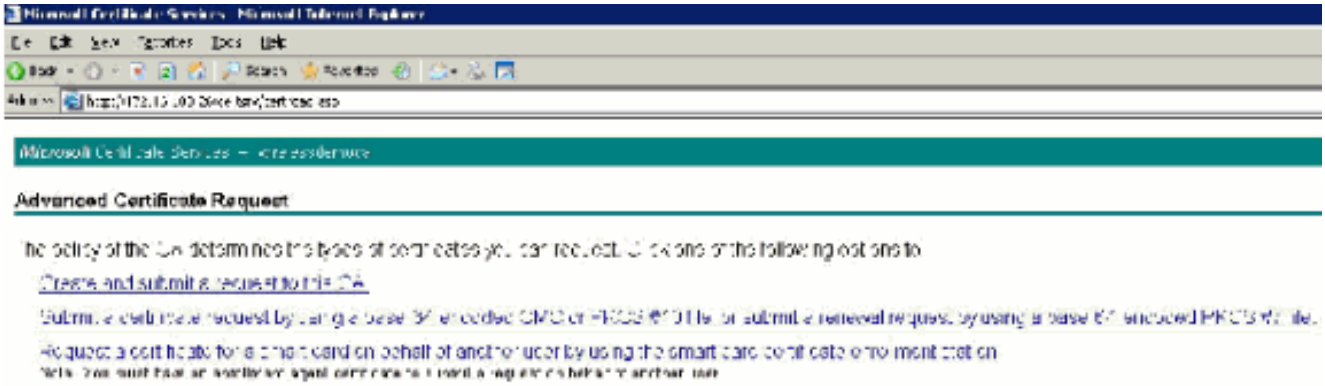
Importante: Verificare che Gestione IIS non sia aperto durante il processo di installazione del certificato poiché causa problemi con le informazioni memorizzate nella cache.

1. Accedere al server ACS con un account con diritti di amministratore dell'organizzazione.
2. Sul computer ACS locale, puntare il browser sul server dell'Autorità di certificazione Microsoft all'indirizzo **http://IP-address-of-Root-CA/certsrv**. In questo caso, l'indirizzo IP è **172.16.100.26**.
3. Accedere come
amministratore.

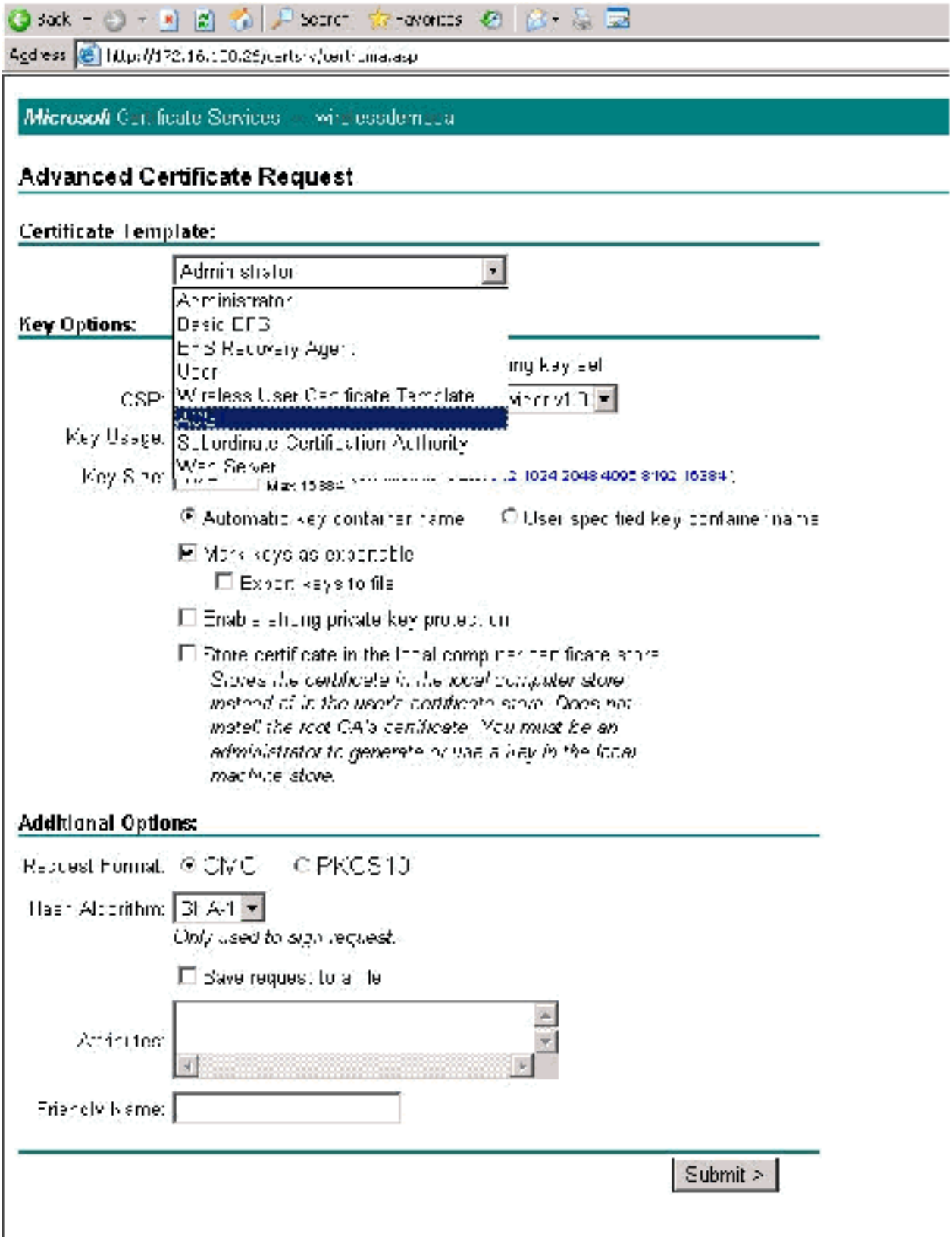
4. Scegliere **Richiedi certificato** e fare clic su **Avanti**.



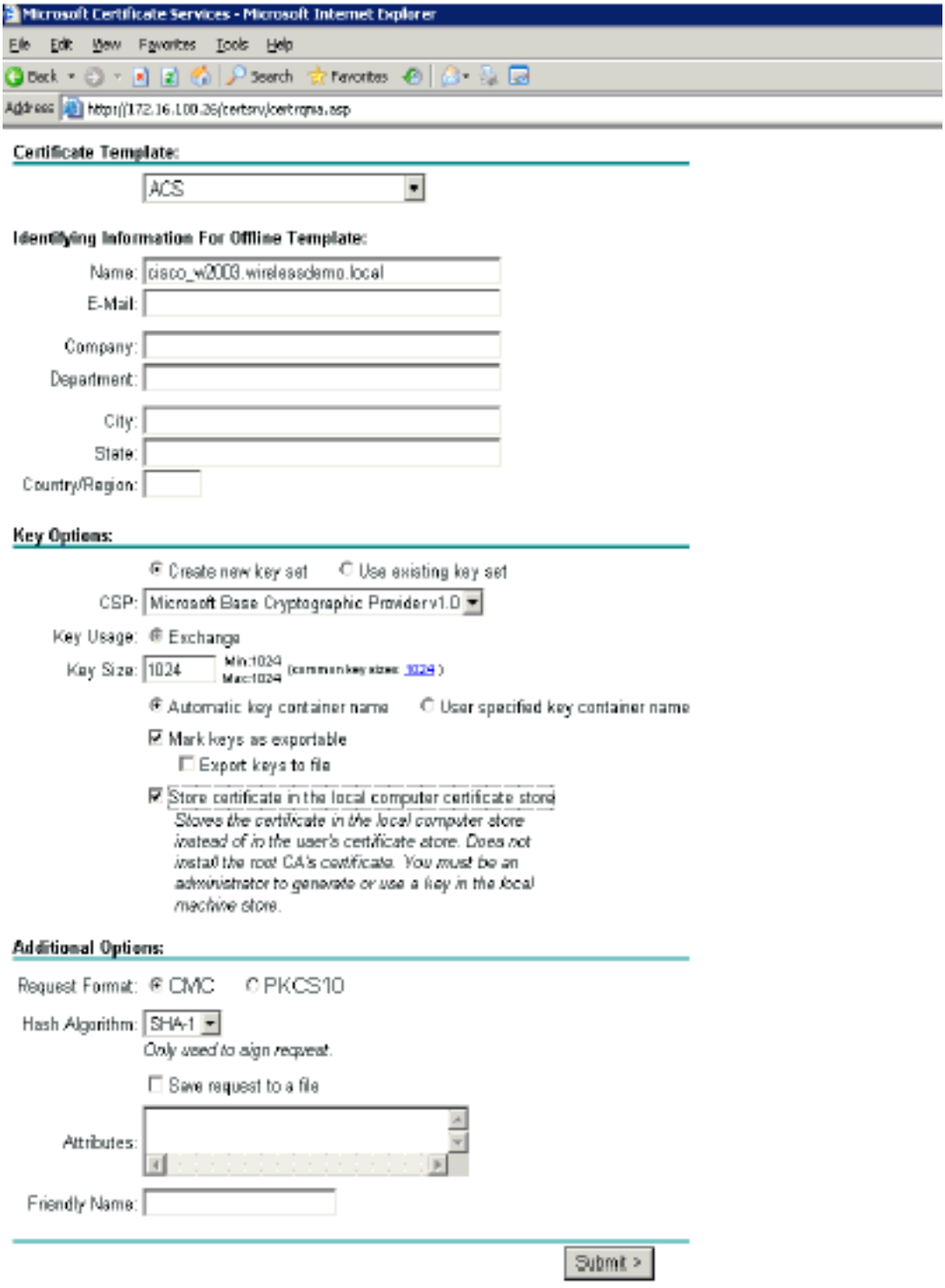
5. Scegliere **Richiesta avanzata** e fare clic su **Avanti**.



6. Scegliere **Crea e invia una richiesta a questa CA** e fare clic su **Avanti**.**Importante:** Questo passaggio è dovuto al fatto che Windows 2003 non consente l'esportazione di chiavi ed è necessario generare una richiesta di certificato basata sul certificato ACS creato in precedenza.

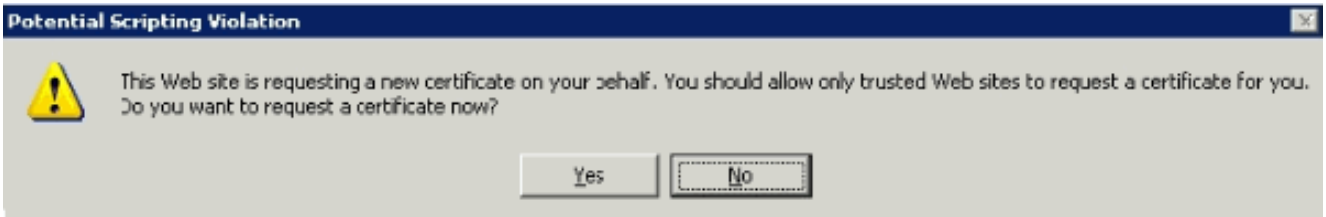


7. In Modelli di certificato selezionare il modello di certificato creato in precedenza e denominato **ACS**. Le opzioni cambiano dopo la selezione del modello.
8. Configurare il nome in modo che sia il nome di dominio completo del server ACS. In questo caso, il nome del server ACS è cisco_w2003.wirelessdemo.local. Verificare che l'opzione **Archivia certificato nell'archivio certificati del computer locale** sia selezionata e fare clic su

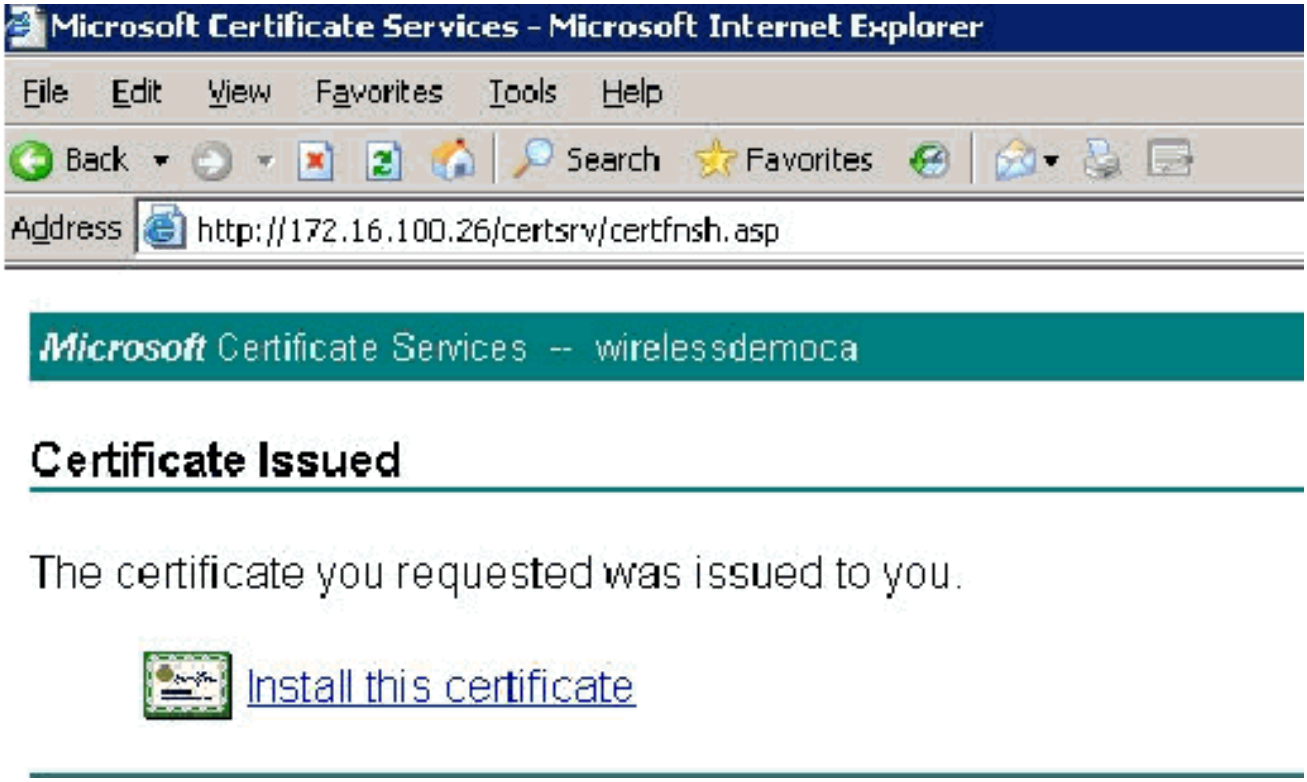


Invia.

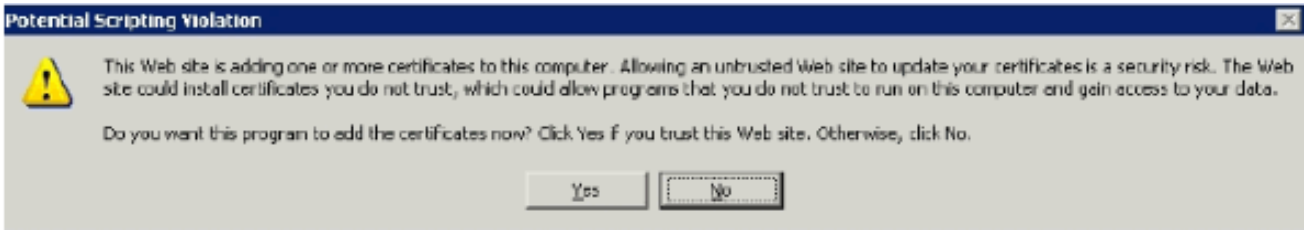
9. Viene visualizzata una finestra popup che avverte di una potenziale violazione di script. Fare clic su **Sì**.



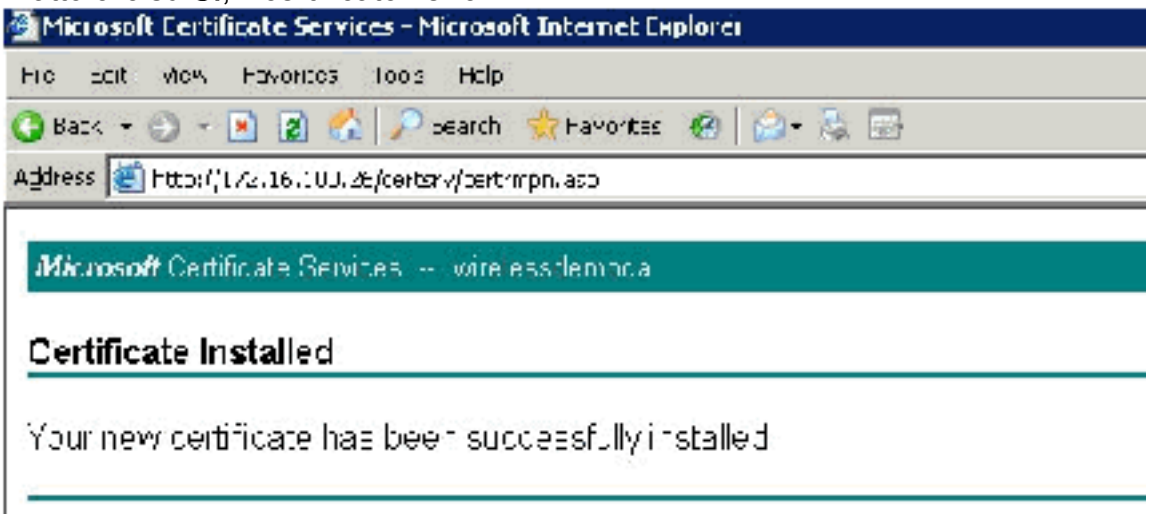
10. Fare clic su **Installa il certificato**.



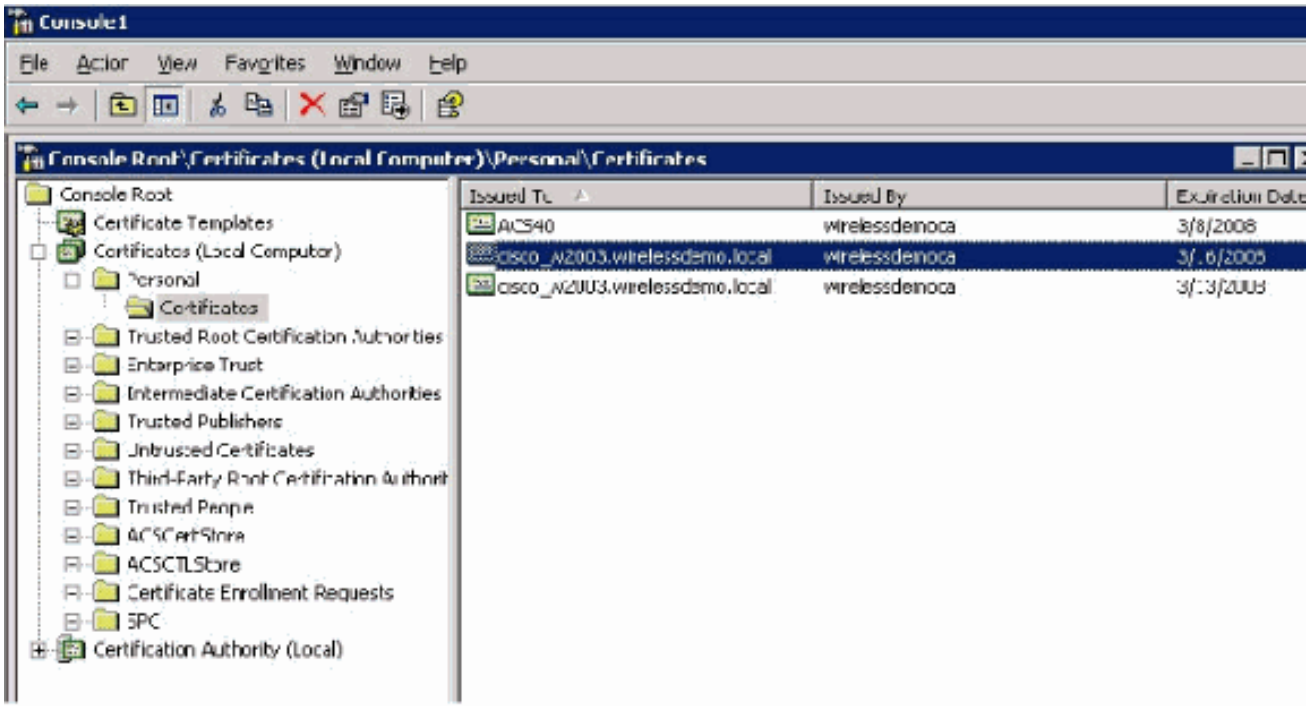
11. Viene nuovamente visualizzata una finestra popup che avverte di una potenziale violazione di script. Fare clic su **Sì**.



12. Dopo aver fatto clic su **Sì**, il certificato verrà installato.



13. A questo punto, il certificato viene installato nella cartella Certificati. Per accedere a questa cartella, scegliere **Start > Esegui**, digitare **mmc**, premere **Invio** e scegliere **Personale > Certificati**.

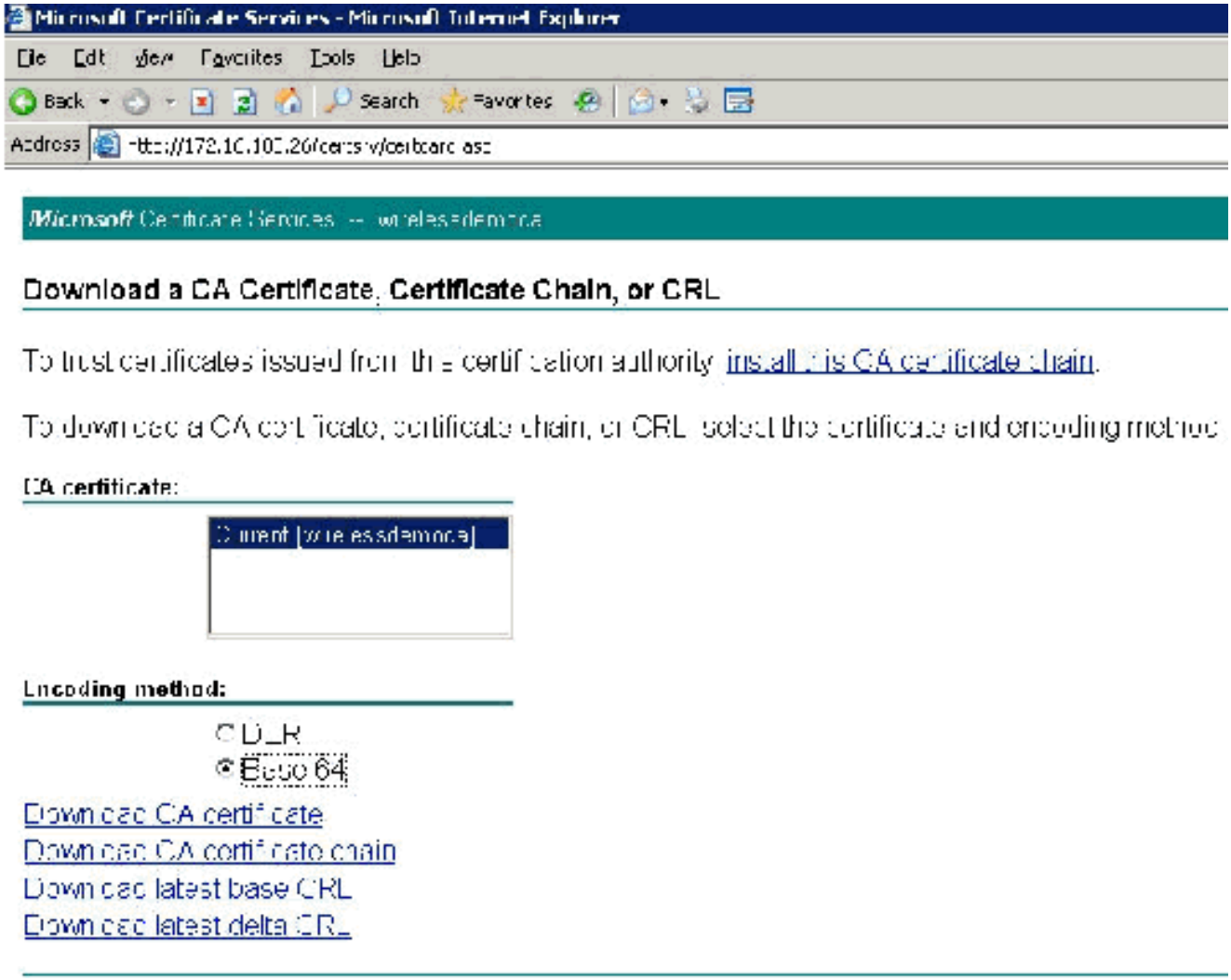


14. Ora che il certificato è installato nel computer locale (ACS o cisco_w2003 in questo esempio), è necessario generare un file di certificato (.cer) per la configurazione del file di certificato ACS 4.0.
15. Sul server ACS (cisco_w2003 nell'esempio), puntare il browser sul server Microsoft Certification Authority a **http://172.16.100.26 /certsrv**.

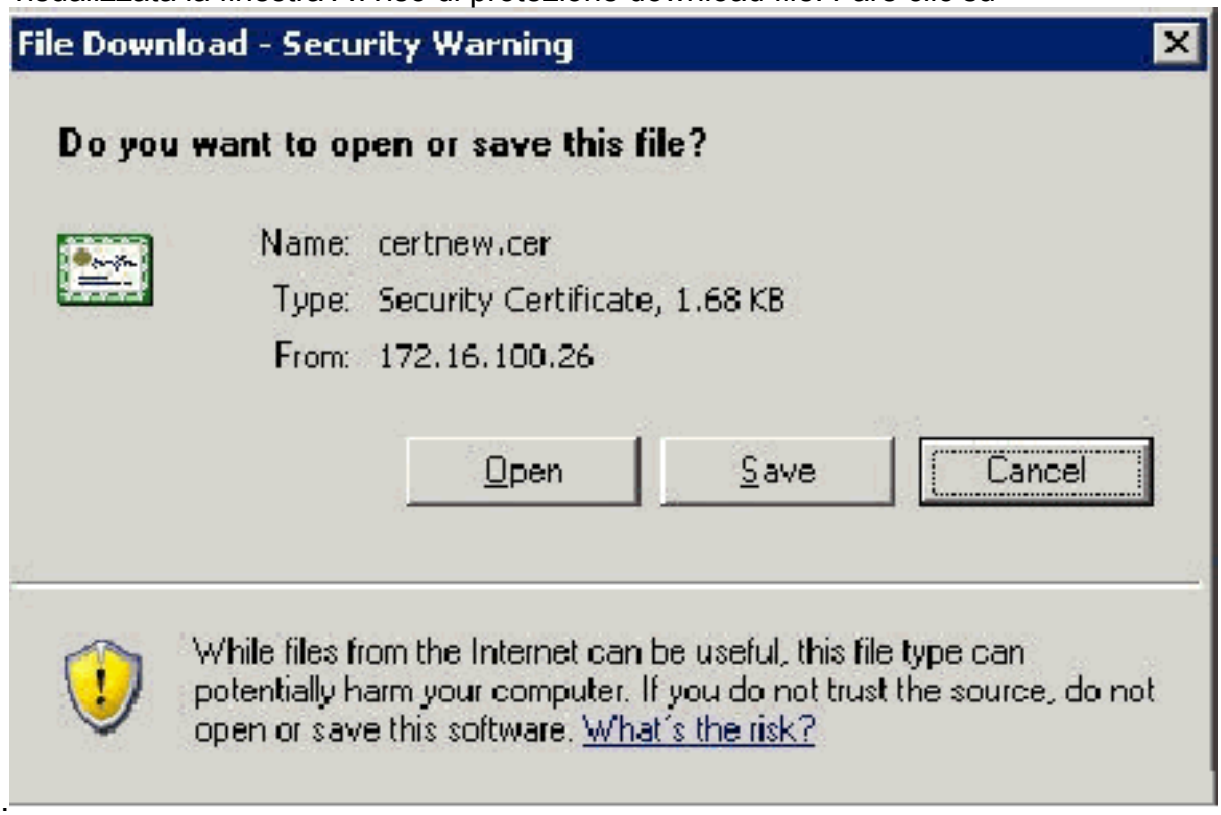
Installare il certificato nel software ACS 4.0

Attenersi alla seguente procedura:

1. Sul server ACS (cisco_w2003 in questo esempio), puntare il browser sul server CA Microsoft a **http://172.16.100.26 /certsrv**.
2. Dall'opzione Seleziona attività scegliere **Scarica un certificato CA, una catena di certificati o un CRL**.
3. Scegliere il metodo di codifica radio **Base 64** e fare clic su **Scarica certificato CA**.

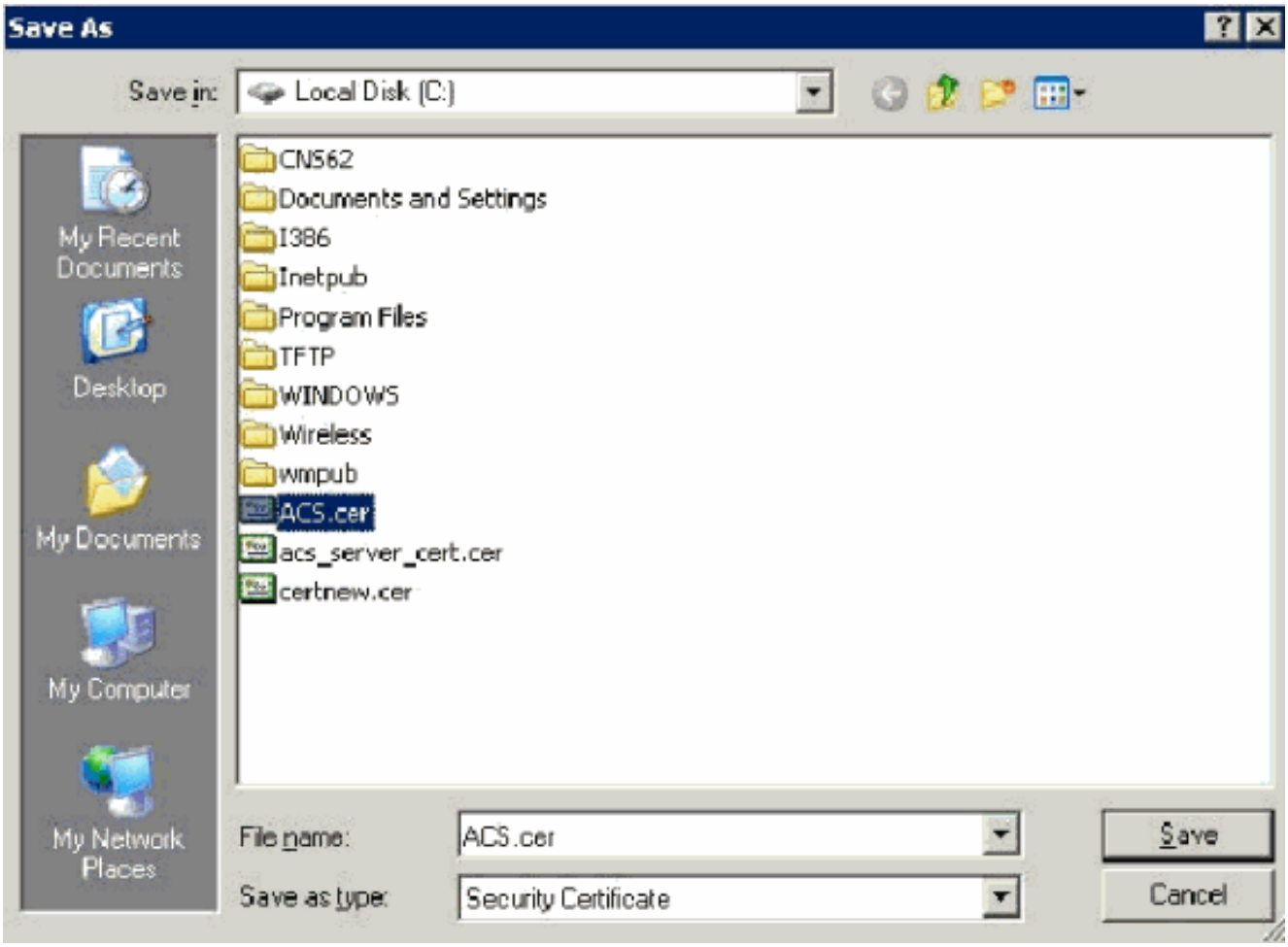


4. Viene visualizzata la finestra Avviso di protezione download file. Fare clic su **Salva**.

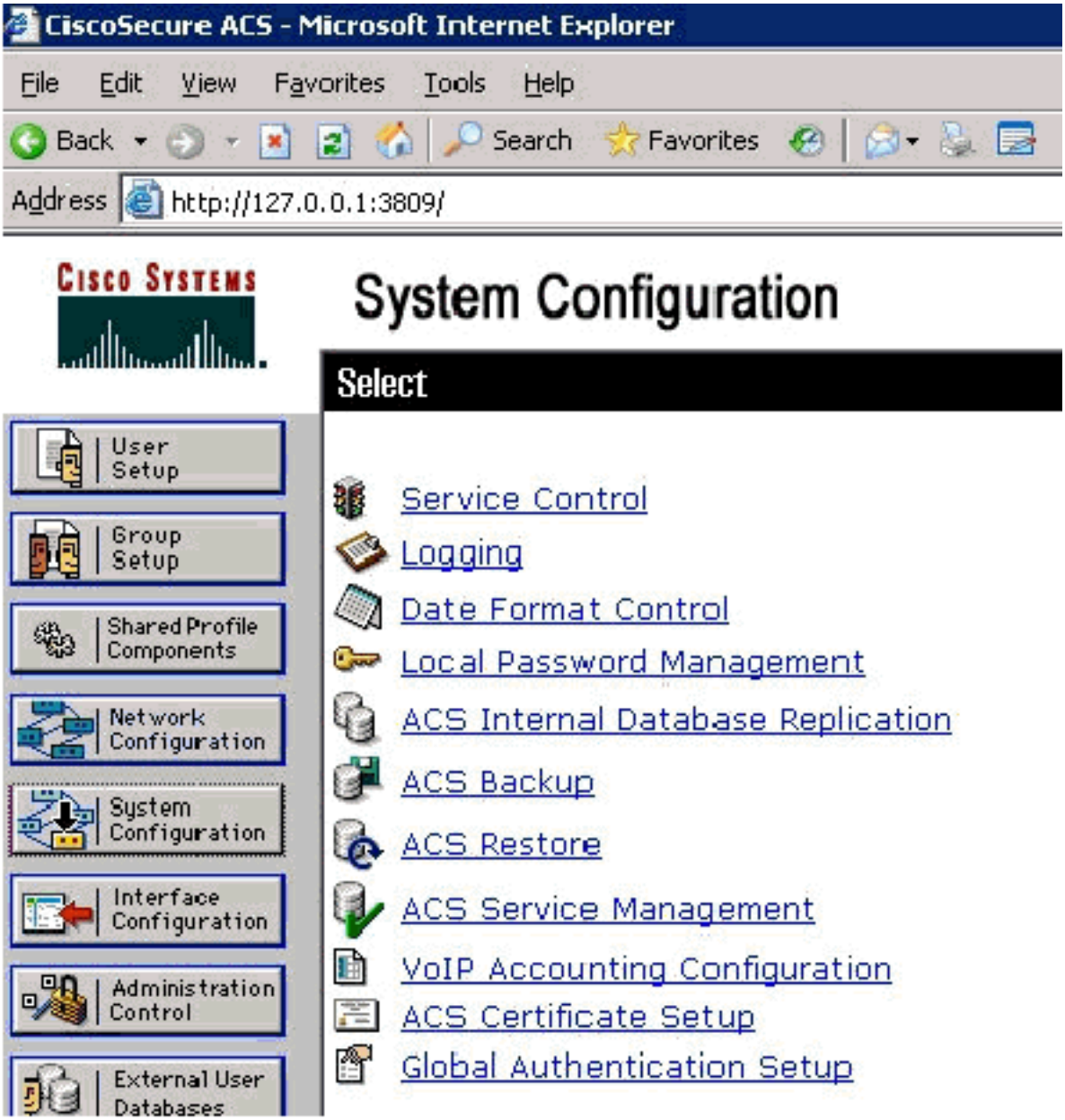


5. Salvare il file con un nome quale ACS.cer o con qualsiasi altro nome desiderato. Tenere presente questo nome poiché viene utilizzato durante l'installazione di ACS Certificate Authority in ACS

4.0.



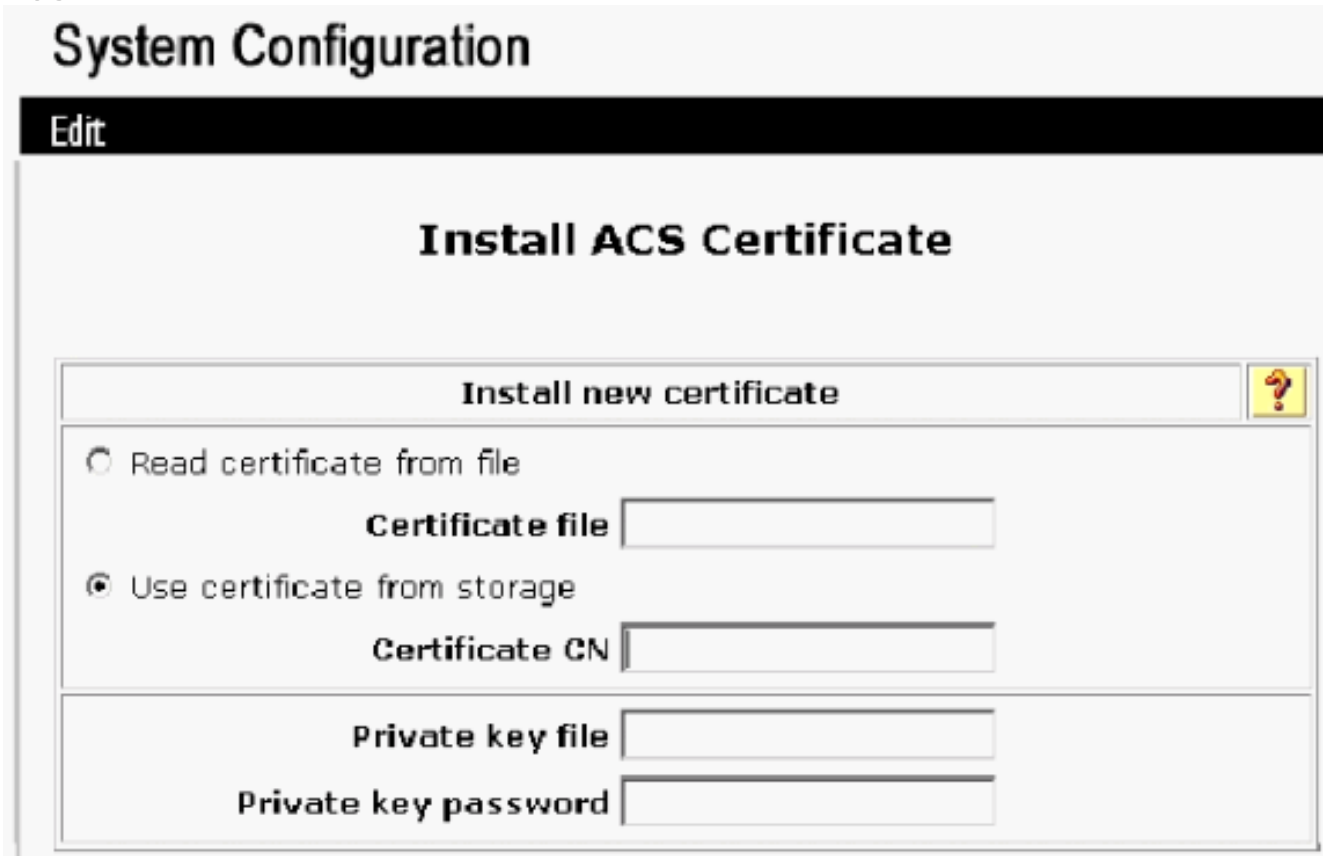
6. Aprire **ACS Admin** dal collegamento sul desktop creato durante l'installazione.
7. Fare clic su **Configurazione di**



sistema.

8. Fare clic su **Configurazione certificato ACS**.

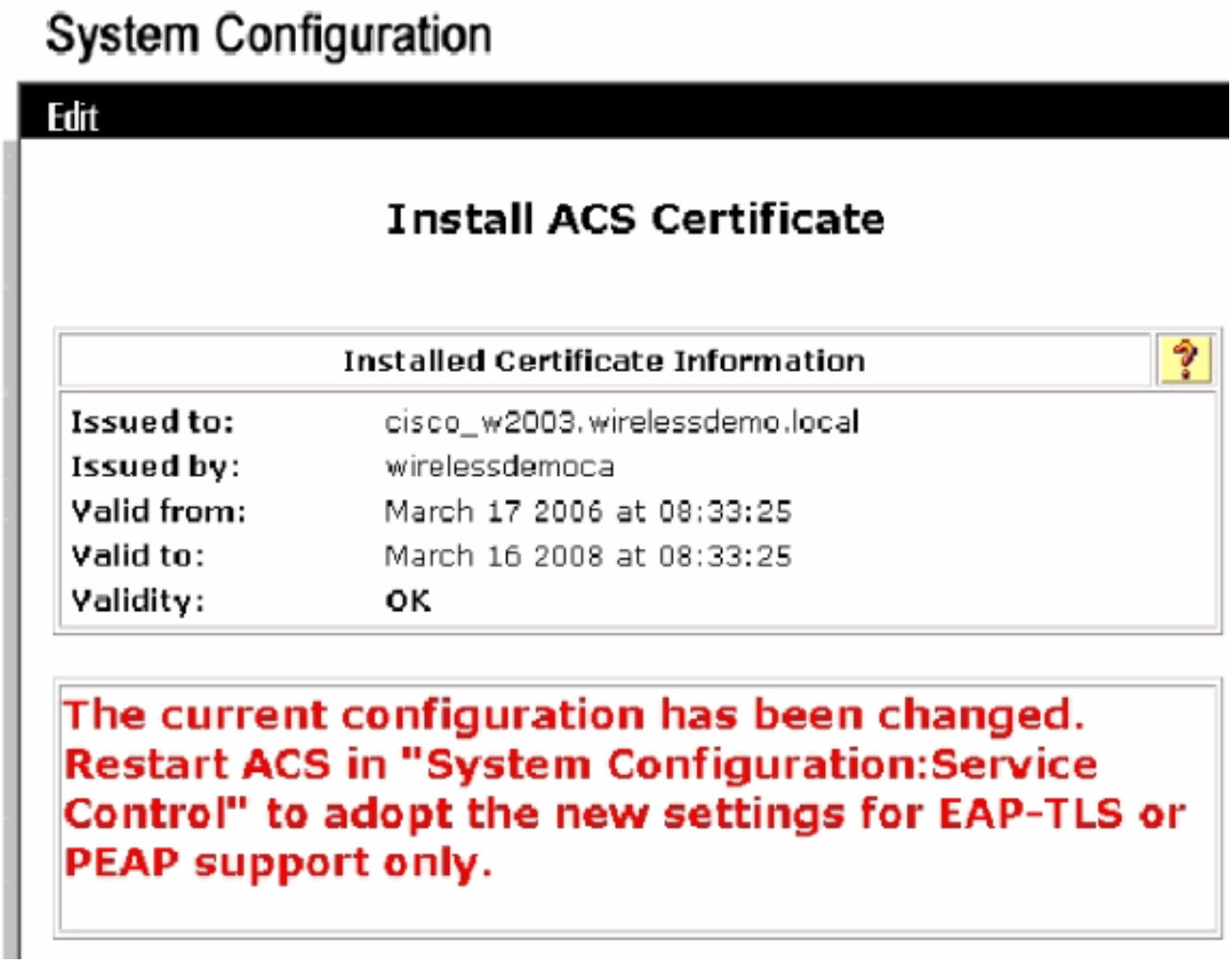
9. Fare clic su **Installa certificato ACS**.



10. Selezionare **Use certificate from storage** (Usa certificato da archiviazione) e immettere il nome di dominio completo **cisco_w2003.wirelessdemo.local** (o **ACS.wirelessdemo.local** se è stato utilizzato ACS come

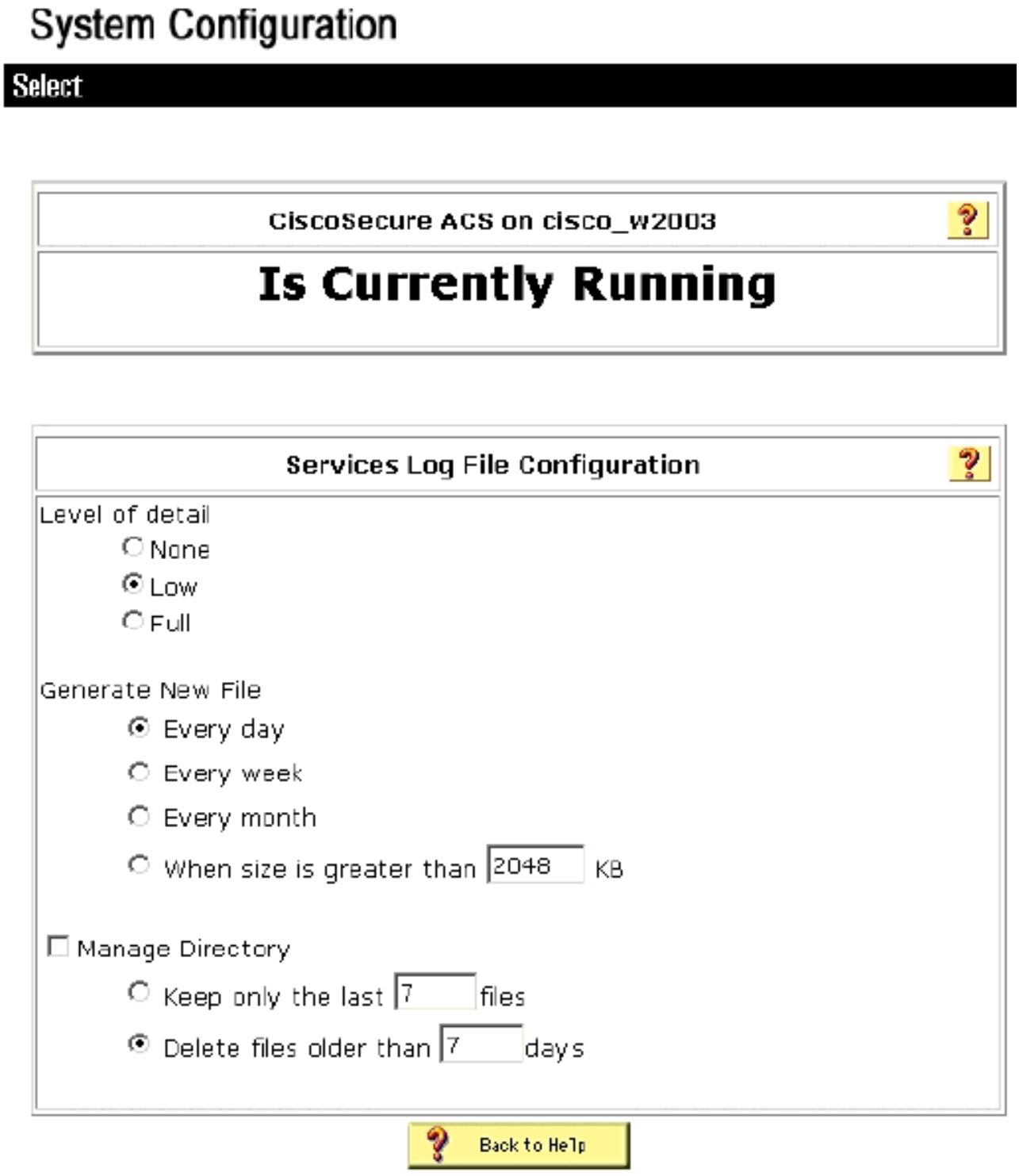
nome).

11. Fare clic su **Invia**.

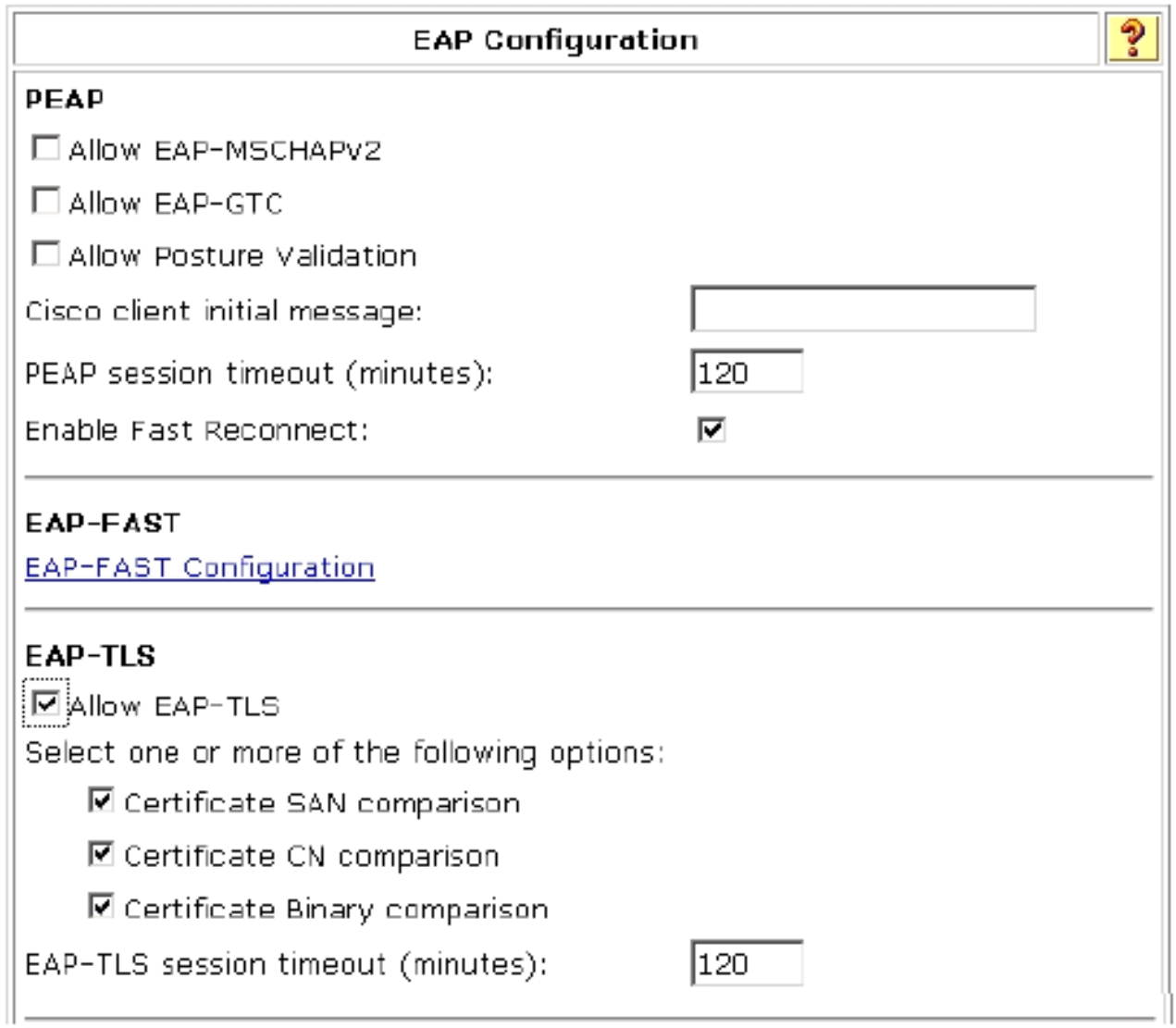


12. Fare clic su **Configurazione di sistema**.

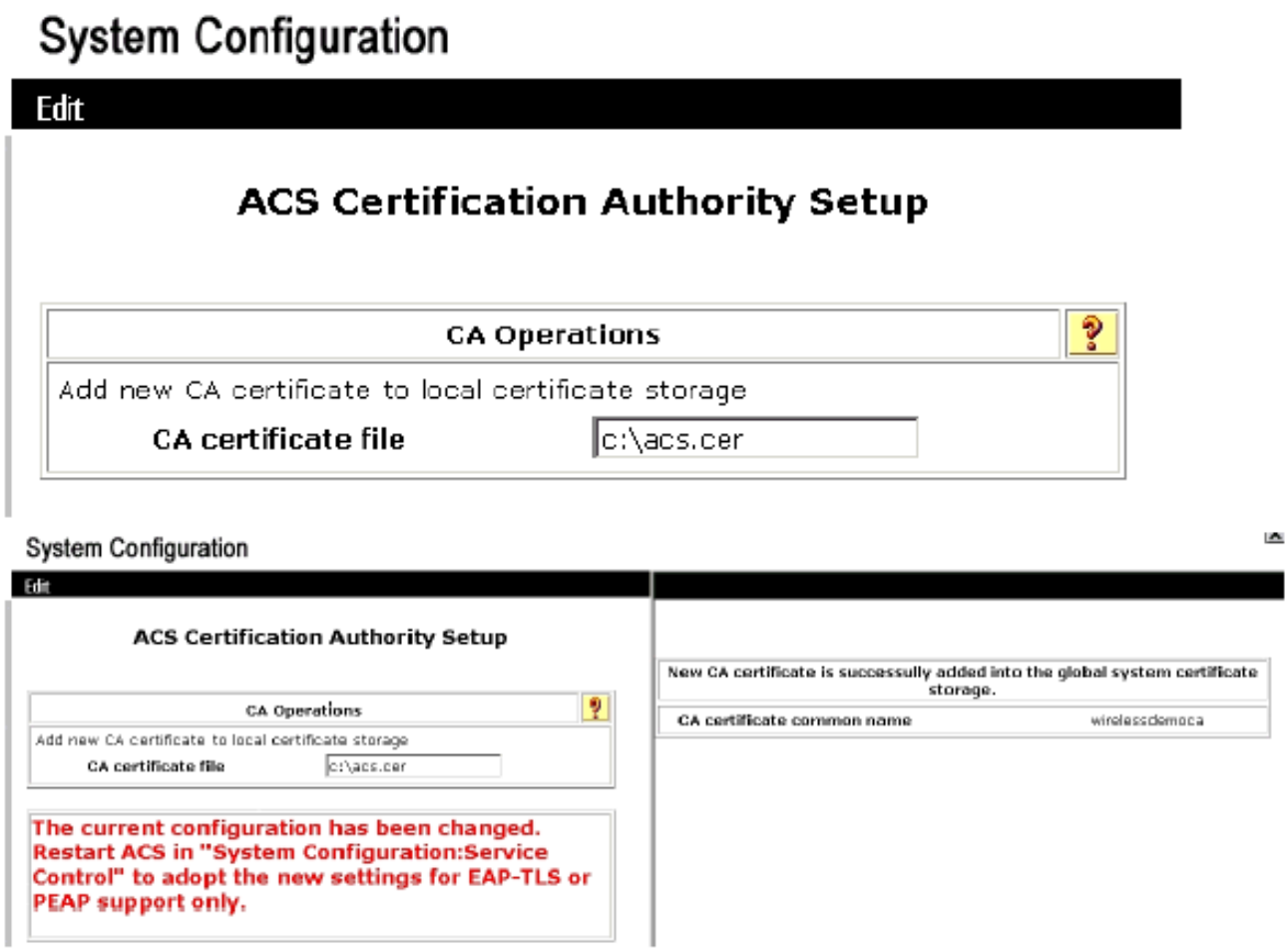
13. Fare clic su **Controllo servizio** e quindi su **Riavvia**.



14. Fare clic su **Configurazione di sistema**.
15. Fare clic su **Global Authentication Setup**.
16. Selezionare **Allow EAP-TLS** e tutte le caselle sottostanti.



17. Fare clic su **Invia + Riavvia**.
18. Fare clic su **Configurazione di sistema**.
19. Fare clic su **Configurazione Autorità di certificazione ACS**.
20. Nella finestra Impostazione Autorità di certificazione ACS digitare il nome e la posizione del file *.cer creato in precedenza. In questo esempio, il file *.cer creato è **ACS.cer** nella directory principale c:\.
21. Digitare **c:\acs.cer** nel campo File del certificato CA e fare clic su **Invia**.



22. Riavviare il servizio ACS.

Configurazione CLIENT per EAP-TLS con Windows Zero Touch

CLIENT è un computer che esegue Windows XP Professional con SP2 e che funge da client wireless e ottiene l'accesso alle risorse Intranet tramite il punto di accesso wireless. Completare le procedure descritte in questa sezione per configurare il client come client wireless.

Eseguire un'installazione e una configurazione di base

Attenersi alla seguente procedura:

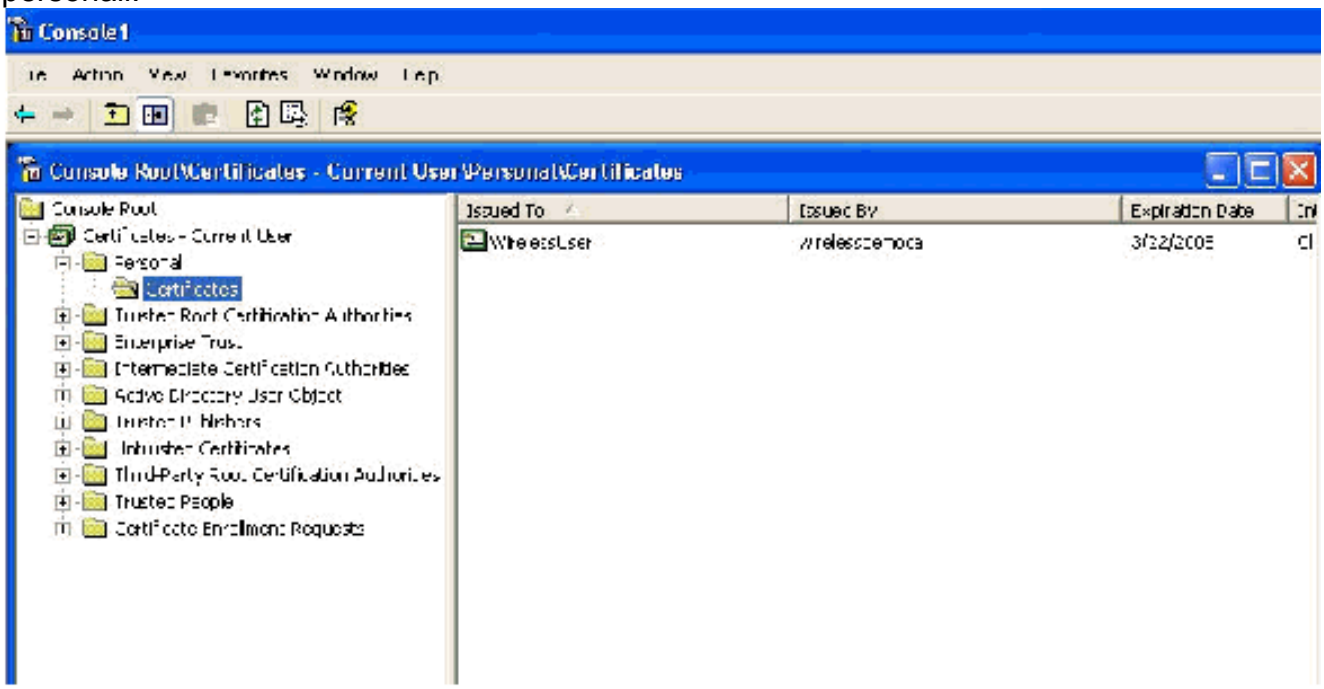
1. Collegare il CLIENT al segmento della rete Intranet utilizzando un cavo Ethernet collegato allo switch.
2. Sul CLIENT, installare Windows XP Professional con SP2 come computer membro denominato **CLIENT** nel dominio wirelessdemo.local.
3. Installare Windows XP Professional con SP2. È necessario installare questo programma per poter disporre del supporto per EAP-TLS e PEAP.**Nota:** Windows Firewall viene attivato automaticamente in Windows XP Professional con SP2. Non disattivare il firewall.

Configurazione della connessione di rete wireless

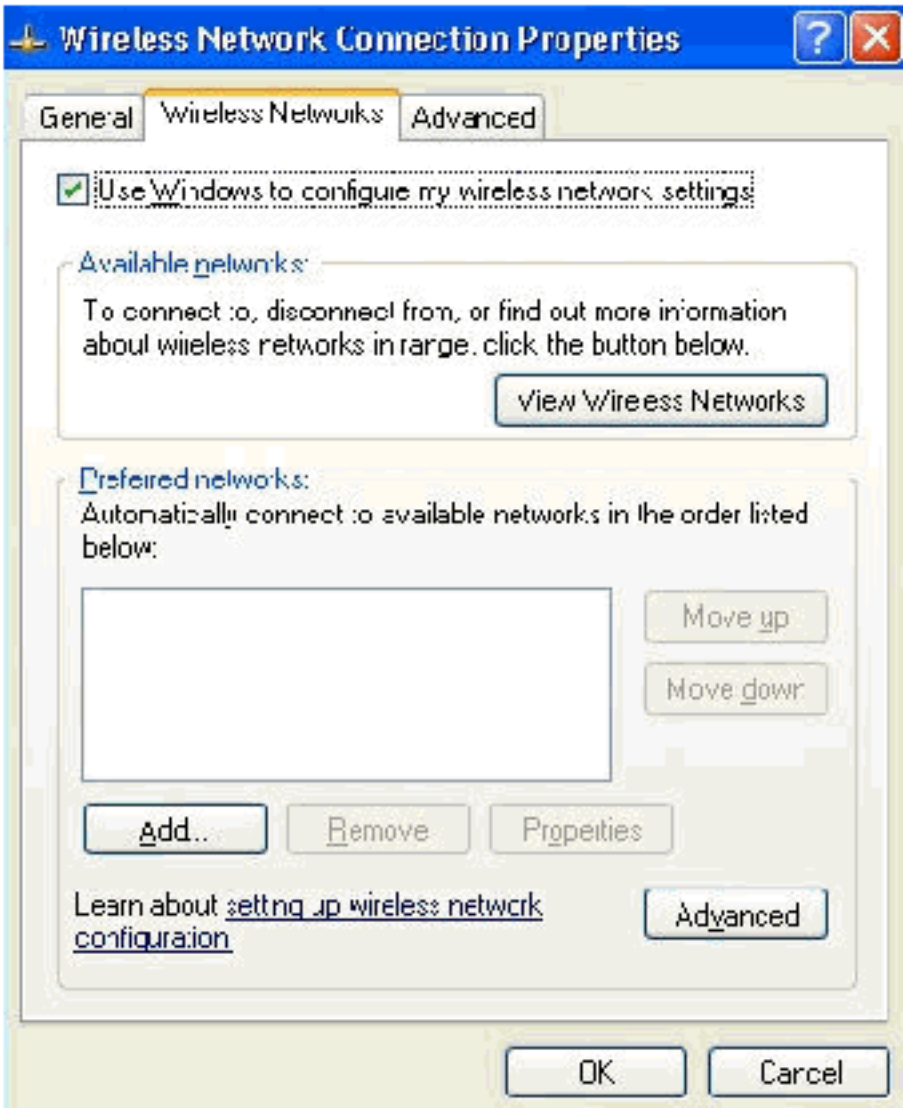
Attenersi alla seguente procedura:

1. Disconnettersi e quindi accedere utilizzando l'account WirelessUser nel dominio

wirelessdemo.local.**Nota:** aggiornare le impostazioni dei Criteri di gruppo di configurazione computer e utente e ottenere immediatamente un certificato computer e utente per il computer client wireless digitando **gpupdate** al prompt dei comandi. In caso contrario, alla disconnessione e all'accesso verrà eseguita la stessa funzione di **gpupdate**. È necessario essere connessi al dominio tramite connessione.**Nota:** per verificare che il certificato sia installato automaticamente sul client, aprire MMC certificato e verificare che il certificato WirelessUser sia disponibile nella cartella Certificati personali.

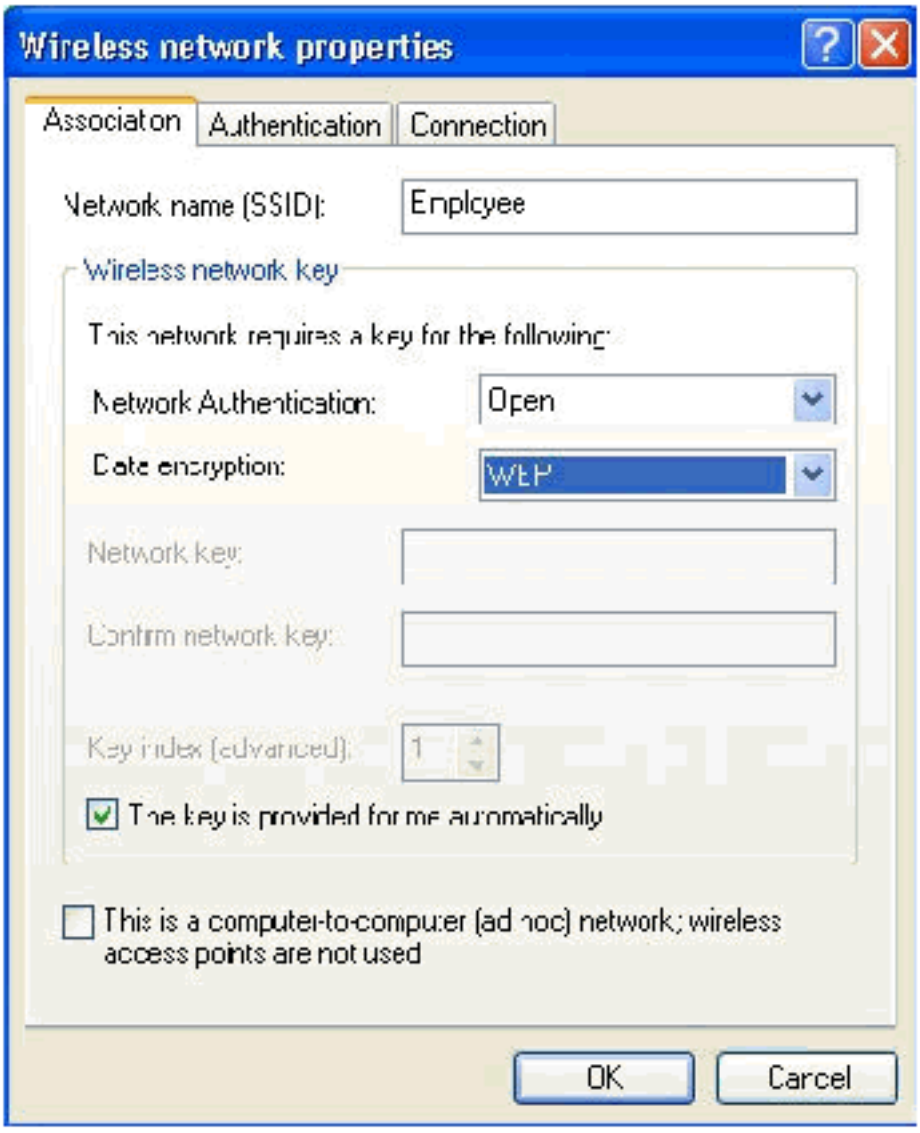


2. Scegliere **Start > Pannello di controllo**, fare doppio clic su **Connessioni di rete** e quindi fare clic con il pulsante destro del mouse su **Connessione rete wireless**.
3. Fare clic su **Proprietà**, andare alla scheda Reti wireless e verificare che **le finestre utente per la configurazione delle impostazioni di rete wireless** siano



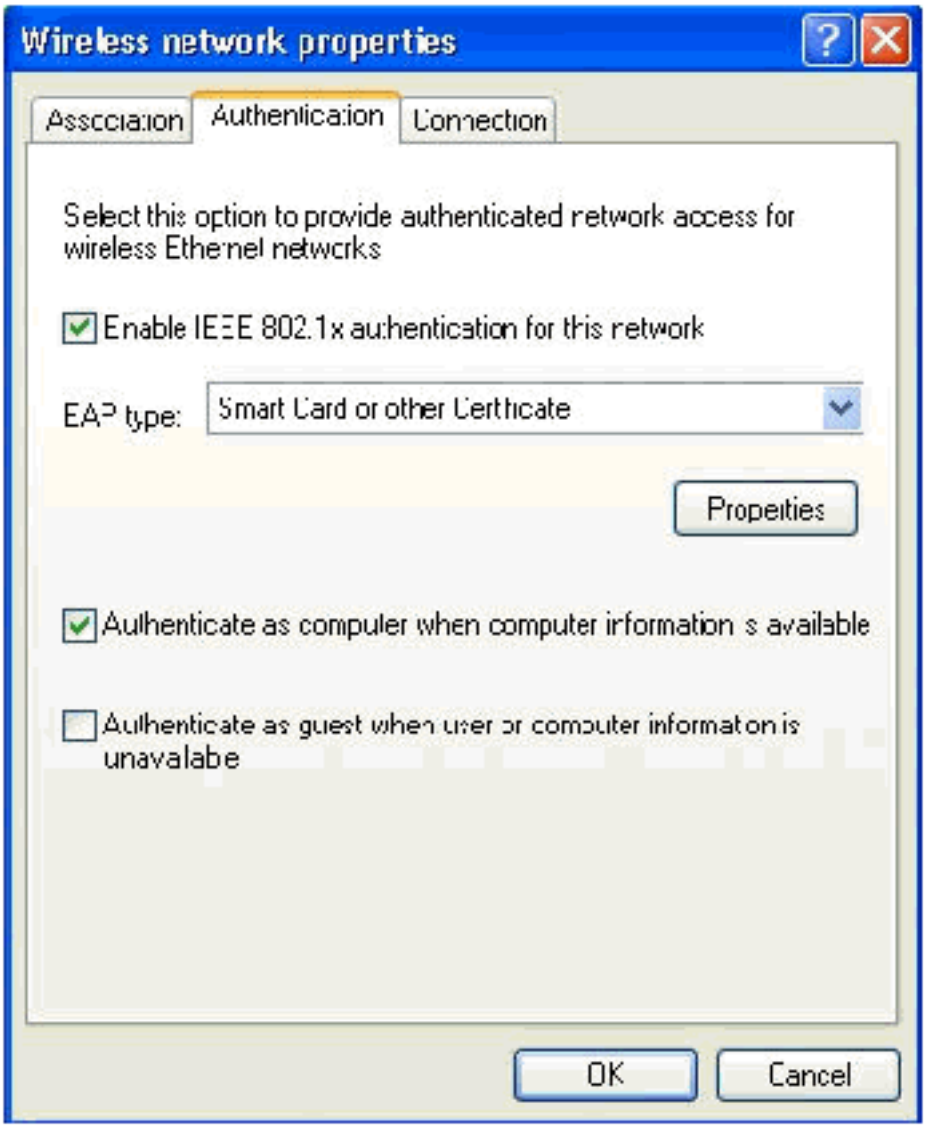
selezionate.

4. Fare clic su **Add**.
5. Andare alla scheda Associazione e digitare **Dipendente** nel campo Nome rete (SSID).
6. Verificare che Data Encryption (Crittografia dati) sia impostato su **WEP** e che **la chiave fornita automaticamente** sia



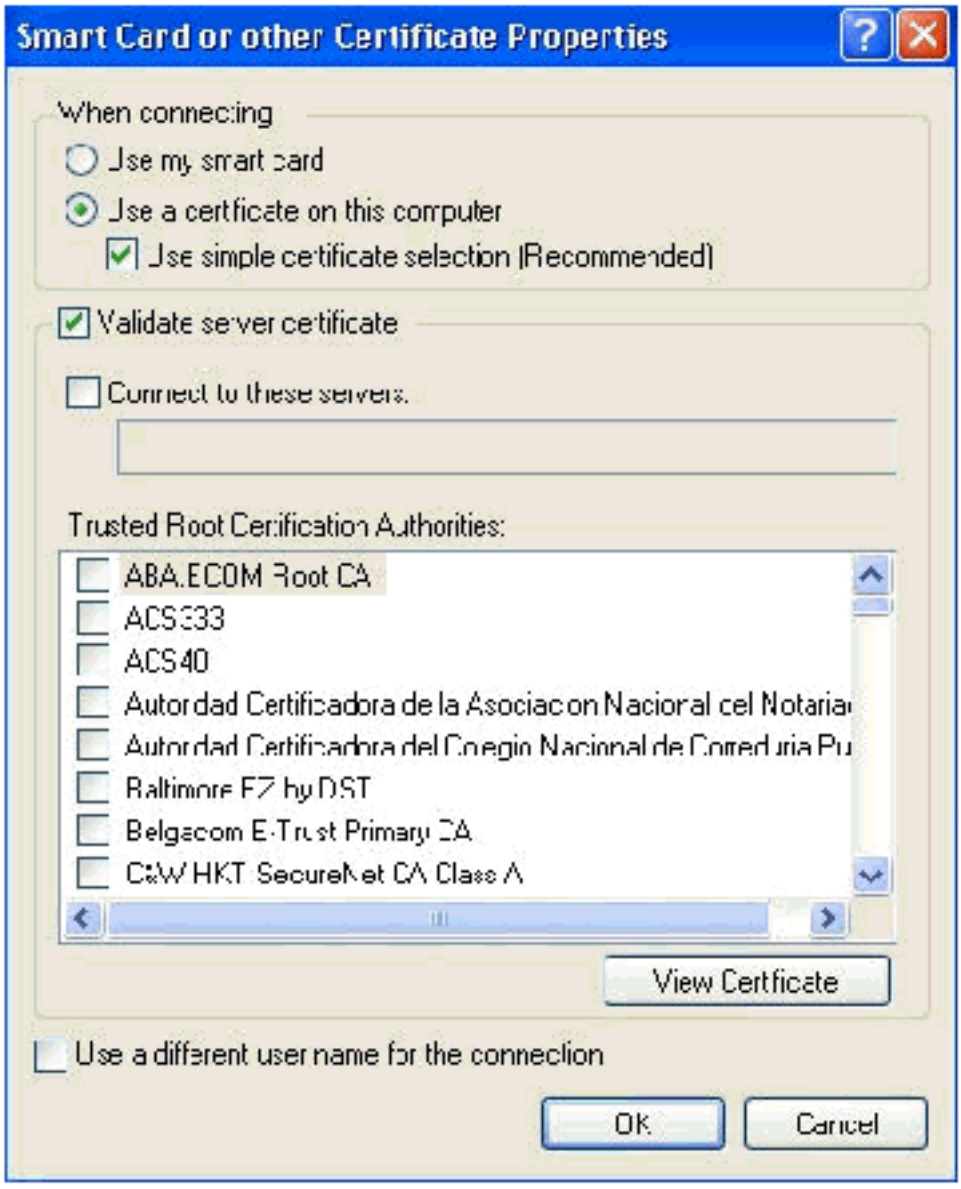
selezionata.

7. Andare alla scheda Autenticazione.
8. Verificare che il tipo EAP sia configurato per l'utilizzo di **smart card o altri certificati**. In caso contrario, selezionarlo dal menu a discesa.
9. Se si desidera che il computer venga autenticato prima dell'accesso (che consente l'applicazione di script di accesso o push di Criteri di gruppo), selezionare l'opzione **Autentica come computer quando sono disponibili informazioni sul**



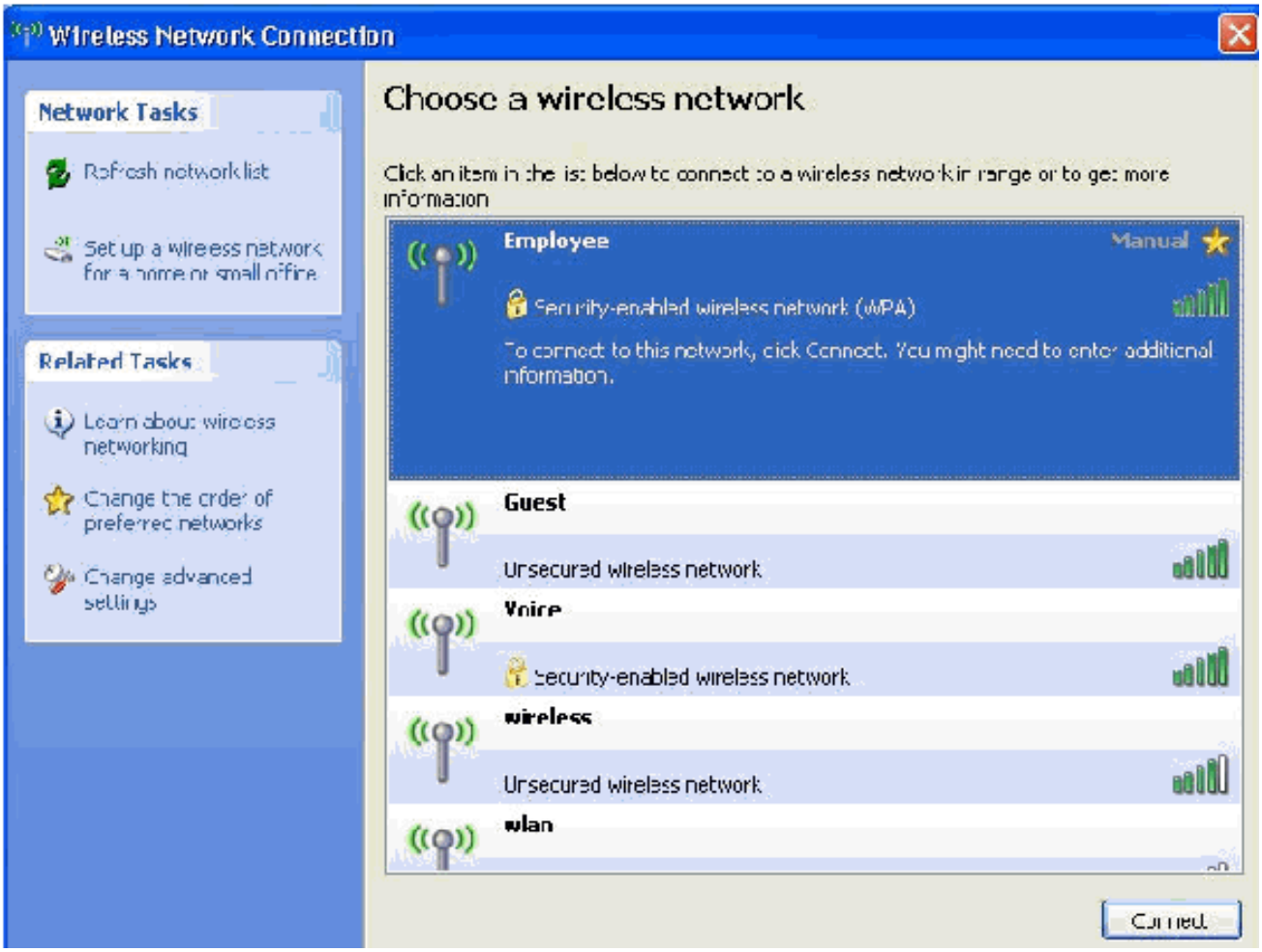
computer.

10. Fare clic su **Proprietà**.
11. Assicurarsi che le caselle in questa finestra siano

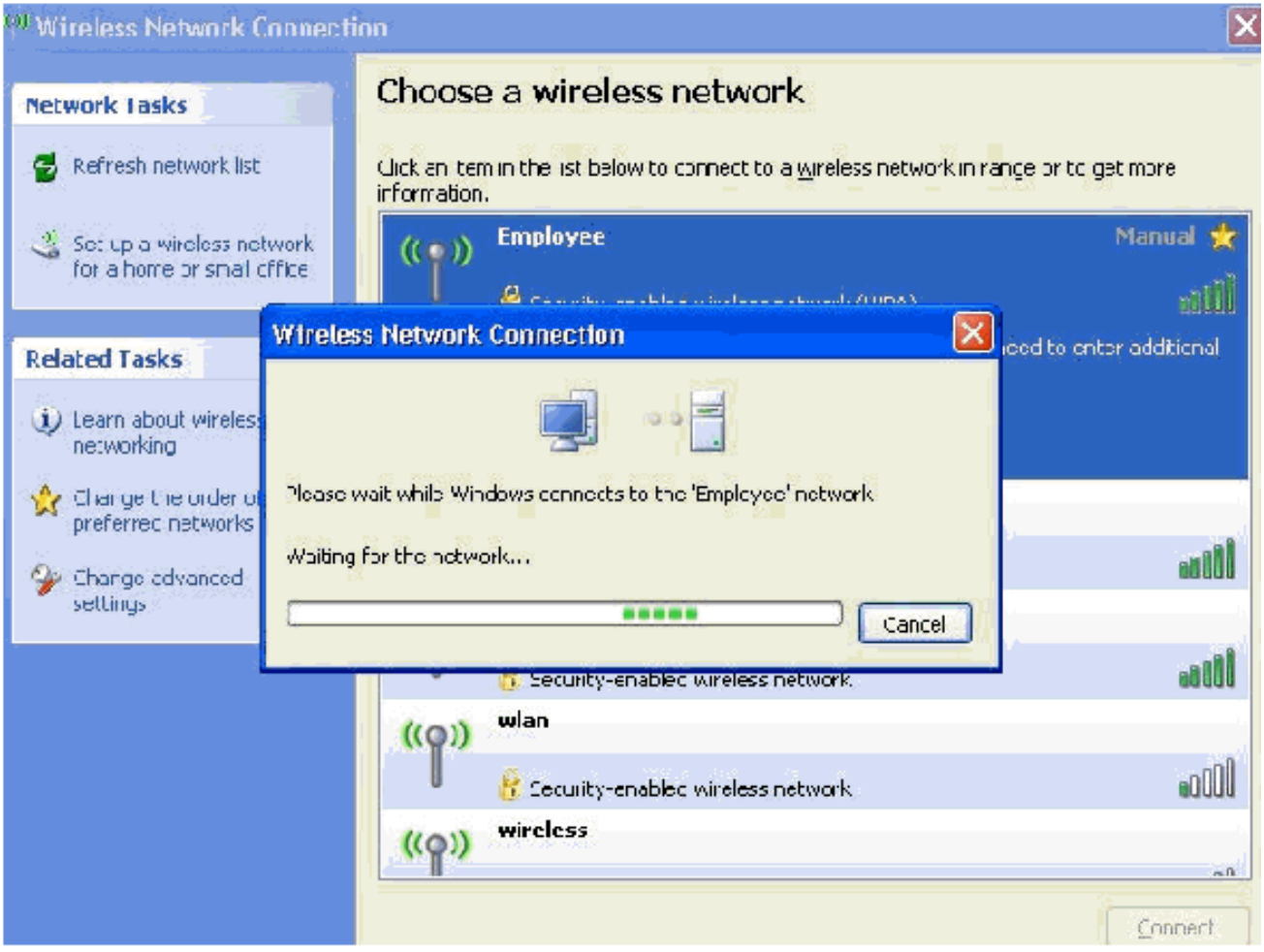


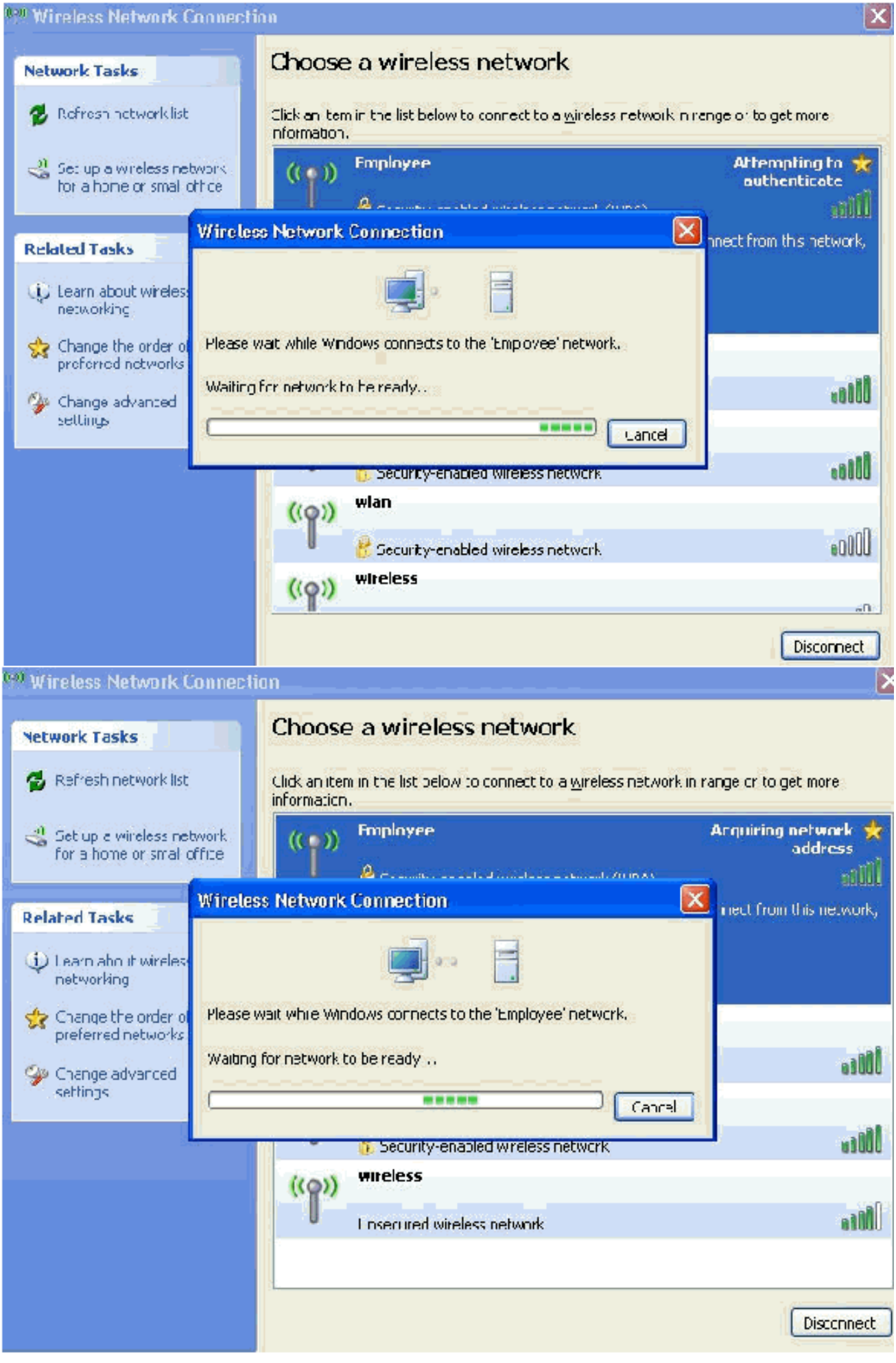
selezionate.

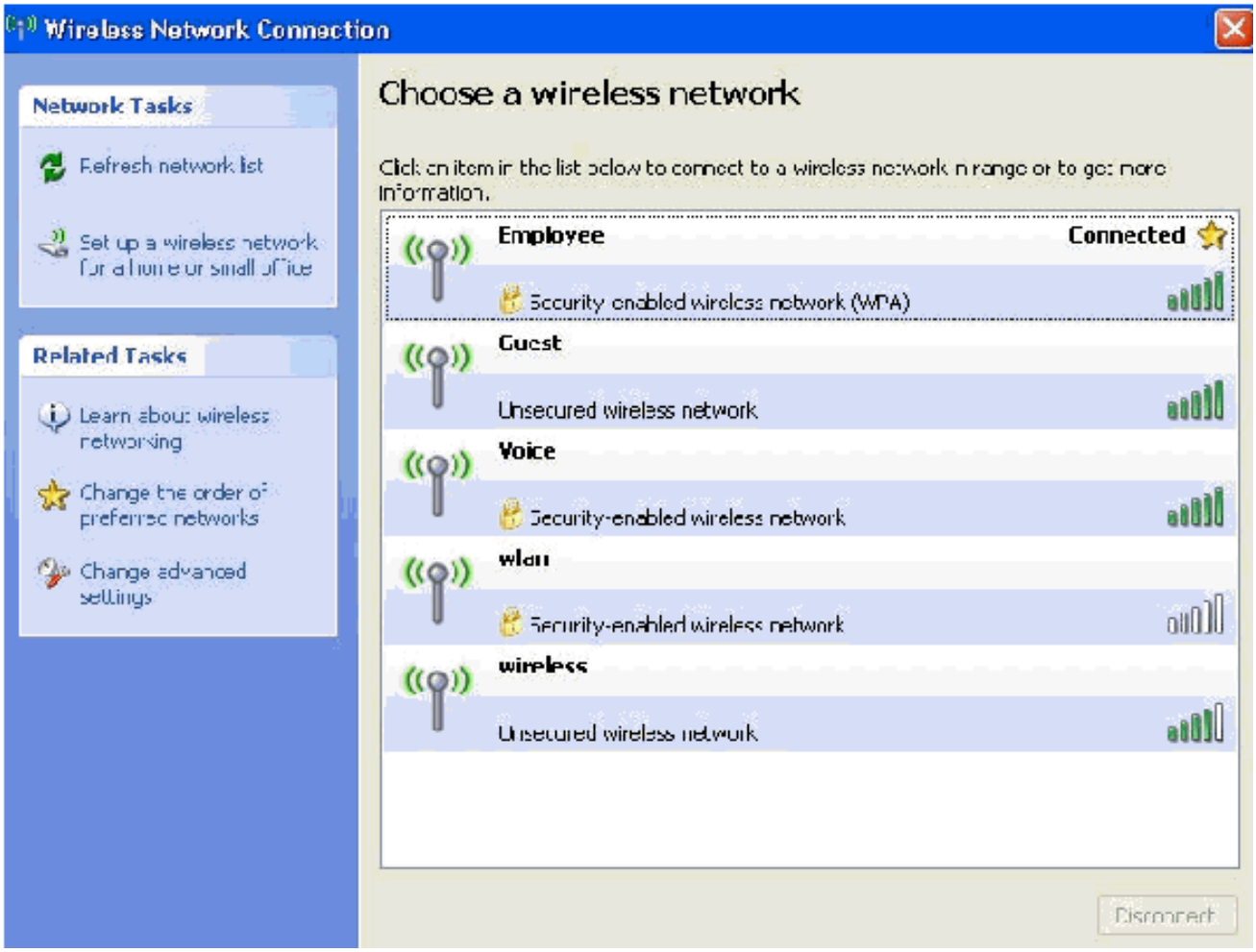
12. Fare clic su **OK** tre volte.
13. Fare clic con il pulsante destro del mouse sull'icona della connessione di rete wireless in systray e quindi scegliere **Visualizza reti wireless disponibili**.
14. Fare clic sulla rete wireless **Employee** e quindi su **Connetti**.



Queste schermate indicano se la connessione è stata completata correttamente.




Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Employee
Attempting to authenticate
Wireless Network Connection
Please wait while Windows connects to the 'Employee' network.
Waiting for network to be ready...
Cancel
Security-enabled wireless network
wlan
Security-enabled wireless network
wireless
Disconnect
Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Employee
Acquiring network address
Wireless Network Connection
Please wait while Windows connects to the 'Employee' network.
Waiting for network to be ready...
Cancel
Security-enabled wireless network
wireless
Unsecured wireless network
Disconnect



15. Al termine dell'autenticazione, controllare la configurazione TCP/IP per la scheda di rete wireless utilizzando Connessioni di rete. Deve avere un intervallo di indirizzi compreso tra 172.16.100.100-172.16.100.254 dall'ambito DHCP o dall'ambito creato per i client wireless.
16. Per verificare la funzionalità, aprire un browser e selezionare **http://wirelessdemoca** (o l'indirizzo IP del server CA Enterprise).

Informazioni correlate

- Esempio di configurazione dell'autenticazione EAP con i controller WLAN (WLC)
- Guida alla configurazione di Wireless LAN Controller
- Esempio di configurazione base di Wireless LAN Controller e Lightweight Access Point
- Esempio di configurazione delle VLAN nei Wireless LAN Controller
- Esempio di configurazione di VLAN di gruppo AP con controller LAN wireless
- Documentazione e supporto tecnico – Cisco Systems