

# PEAP in UWN con ACS 5.1 e Windows 2003 Server

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Installazione di Windows Enterprise 2003 con IIS, Certification Authority, DNS, DHCP \(CA\)](#)

[CA \(democa\)](#)

[Cisco 1121 Secure ACS 5.1](#)

[Installazione con l'accessorio serie CSACS-1121](#)

[Installare il server ACS](#)

[Configurazione controller Cisco WLC5508](#)

[Creare la configurazione necessaria per WPAv2/WPA](#)

[Autenticazione PEAP](#)

[Installare lo snap-in Modelli di certificato](#)

[Creare il modello di certificato per il server Web ACS](#)

[Abilita il nuovo modello di certificato server Web ACS](#)

[Configurazione certificato ACS 5.1](#)

[Configura certificato esportabile per ACS](#)

[Installare il certificato nel software ACS 5.1](#)

[Configura archivio identità ACS per Active Directory](#)

[Aggiunta di un controller ad ACS come client AAA](#)

[Configurazione dei criteri di accesso ACS per reti wireless](#)

[Crea regola di servizio e criterio di accesso ACS](#)

[Configurazione CLIENT per PEAP con Windows Zero Touch](#)

[Eseguire un'installazione e una configurazione di base](#)

[Installare la scheda di rete wireless](#)

[Configurazione della connessione di rete wireless](#)

[Risoluzione dei problemi di autenticazione wireless con ACS](#)

[Autenticazione PEAP non riuscita con server ACS](#)

[Informazioni correlate](#)

## [Introduzione](#)

In questo documento viene descritto come configurare l'accesso wireless sicuro utilizzando i

controller LAN wireless, il software Microsoft Windows 2003 e Cisco Secure Access Control Server (ACS) 5.1 tramite il protocollo PEAP (Protected Extensible Authentication Protocol) con Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) versione 2.

**Nota:** per informazioni sulla distribuzione di connessioni wireless sicure, fare riferimento al [sito Web Microsoft Wi-Fi](#) e al [Cisco SAFE Wireless Blueprint](#).

## Prerequisiti

### Requisiti

Si presume che il programma di installazione abbia una conoscenza sufficiente dell'installazione di base di Windows 2003 e del controller LAN wireless Cisco, in quanto nel presente documento vengono illustrate solo le configurazioni specifiche per semplificare i test.

Per informazioni sull'installazione iniziale e sulla configurazione dei Cisco serie 5508 Controller, fare riferimento alla [Guida all'installazione dei Cisco Wireless Controller serie 5500](#). Per informazioni sull'installazione iniziale e sulla configurazione dei Cisco serie 2100 Controller, fare riferimento alla [Guida introduttiva: Cisco serie 2100 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.

Windows Server 2003 con SP1, Enterprise Edition viene utilizzato per consentire la configurazione della registrazione automatica dei certificati utente e workstation per l'autenticazione PEAP. 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 2106 o 5508 con 7.0.98.0
- Cisco 1142 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise con Internet Information Server (IIS), CA (Certification Authority), DHCP e DNS (Domain Name System) installati
- Cisco 1121 Secure Access Control System Appliance (ACS) 5.1
- 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 3750 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.

## Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

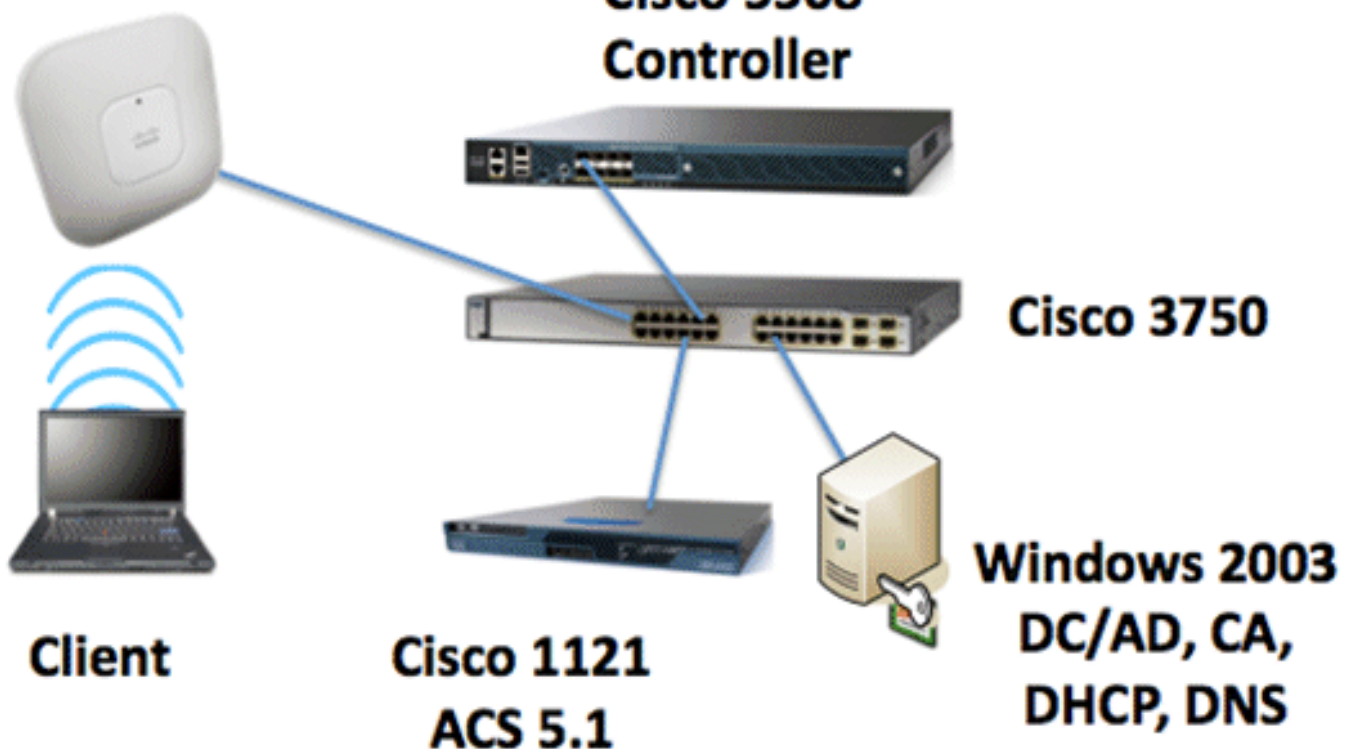
**Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

## Esempio di rete

Nel documento viene usata questa impostazione di rete:

Topologia Cisco Secure Wireless Lab

### **Access Point**



Lo scopo principale di questo documento è quello di fornire la procedura dettagliata per implementare PEAP in Unified Wireless Networks con ACS 5.1 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 Service Pack 2](#) .

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

## CA (democa)

CA è un computer che esegue Windows Server 2003 con SP2, Enterprise Edition ed esegue i seguenti ruoli:

- Un controller di dominio per il dominio **demo.local** che esegue IIS
- Un server DNS per il dominio DNS **demo.local**
- Un server DHCP
- CA radice dell'organizzazione per il dominio **demo.local**

Per configurare la CA per questi servizi, eseguire la procedura seguente:

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 i 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 di utenti wireless.](#)
13. [Aggiungere computer client al gruppo wirelessusers.](#)

## Eseguire l'installazione e la configurazione di base

Attenersi alla procedura seguente:

1. Installare Windows Server 2003 con SP2, Enterprise Edition come server autonomo.
2. Configurare il protocollo TCP/IP con l'indirizzo IP *10.0.10.10* e la subnet mask *255.255.255.0*.

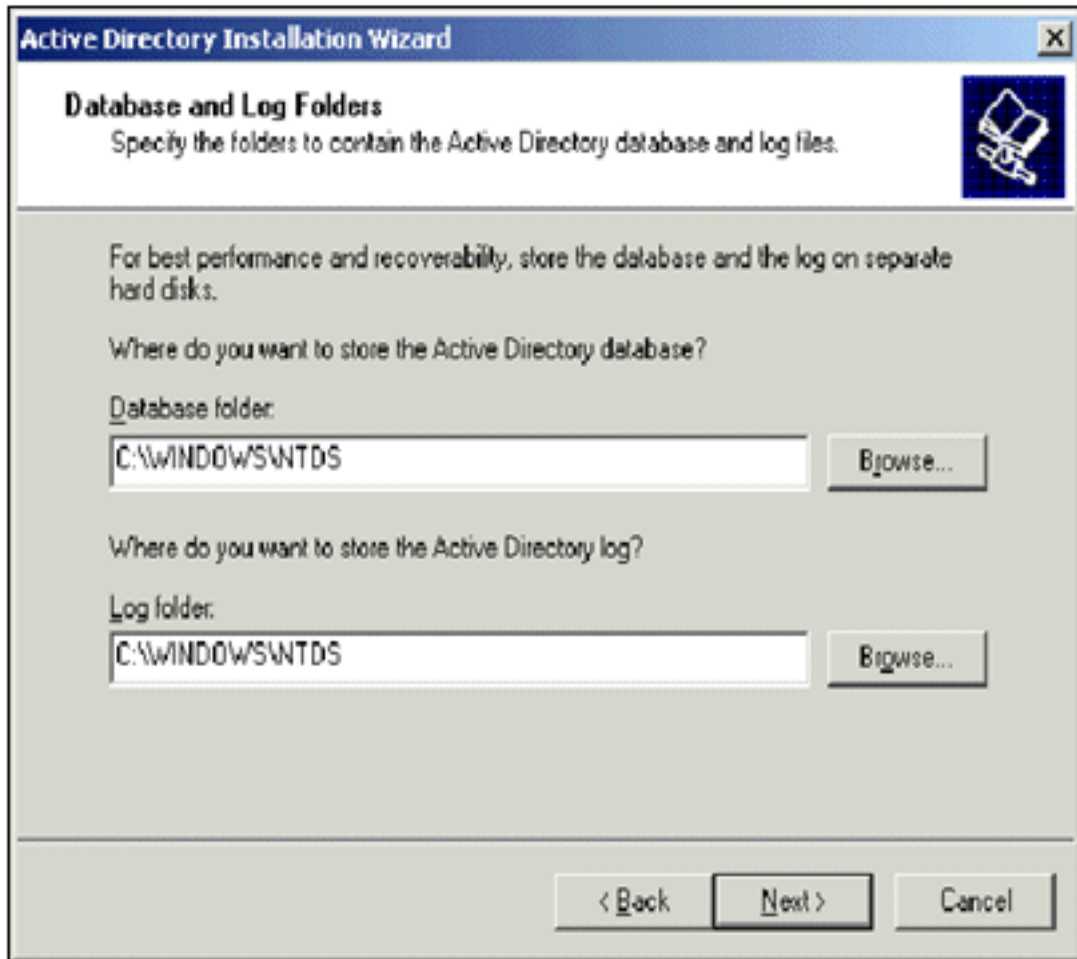
## Configurare il computer come controller di dominio

Attenersi alla procedura seguente:

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

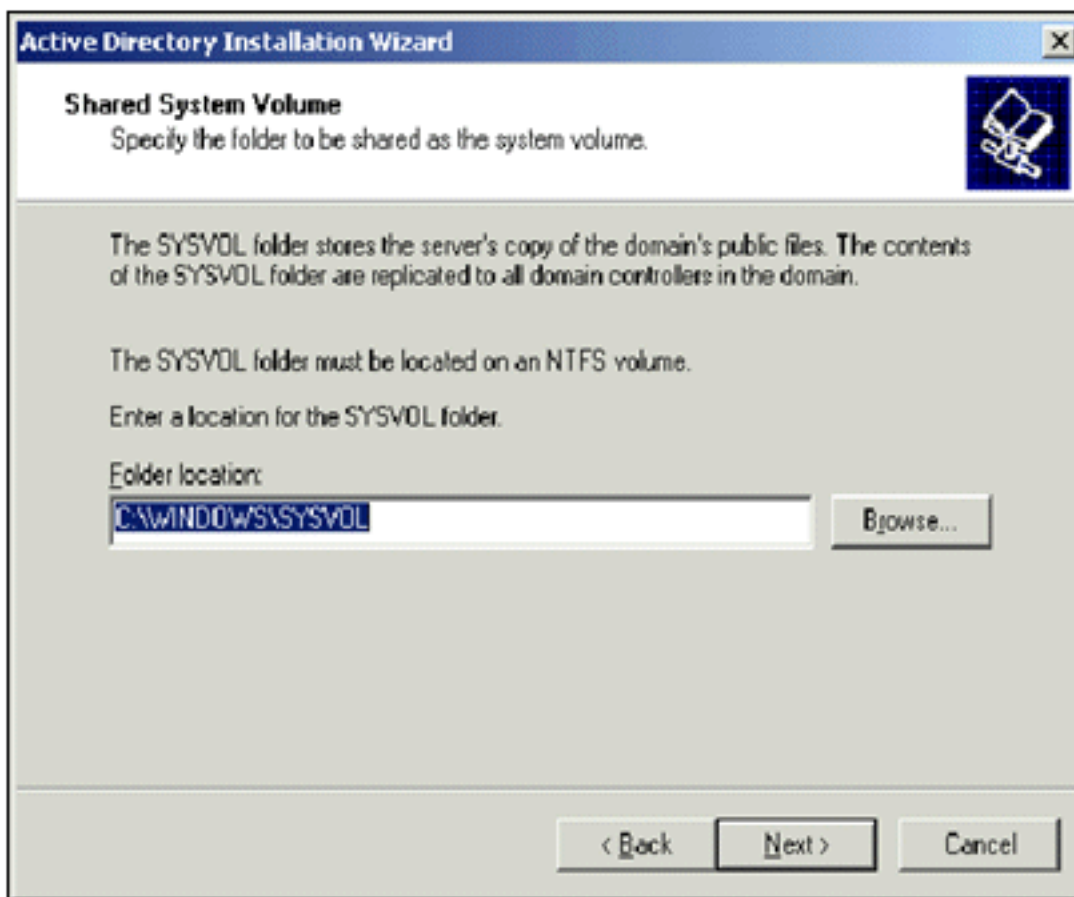
**Avanti.**

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 **demo.local** e fare clic su **Avanti**.
8. Nella pagina Nome di dominio NetBIOS, immettere il nome di dominio NetBIOS come **demo** e fare clic su **Avanti**.
9. Nella pagina Percorsi del database e delle cartelle di log accettare le directory predefinite del database e delle cartelle di log e fare clic su



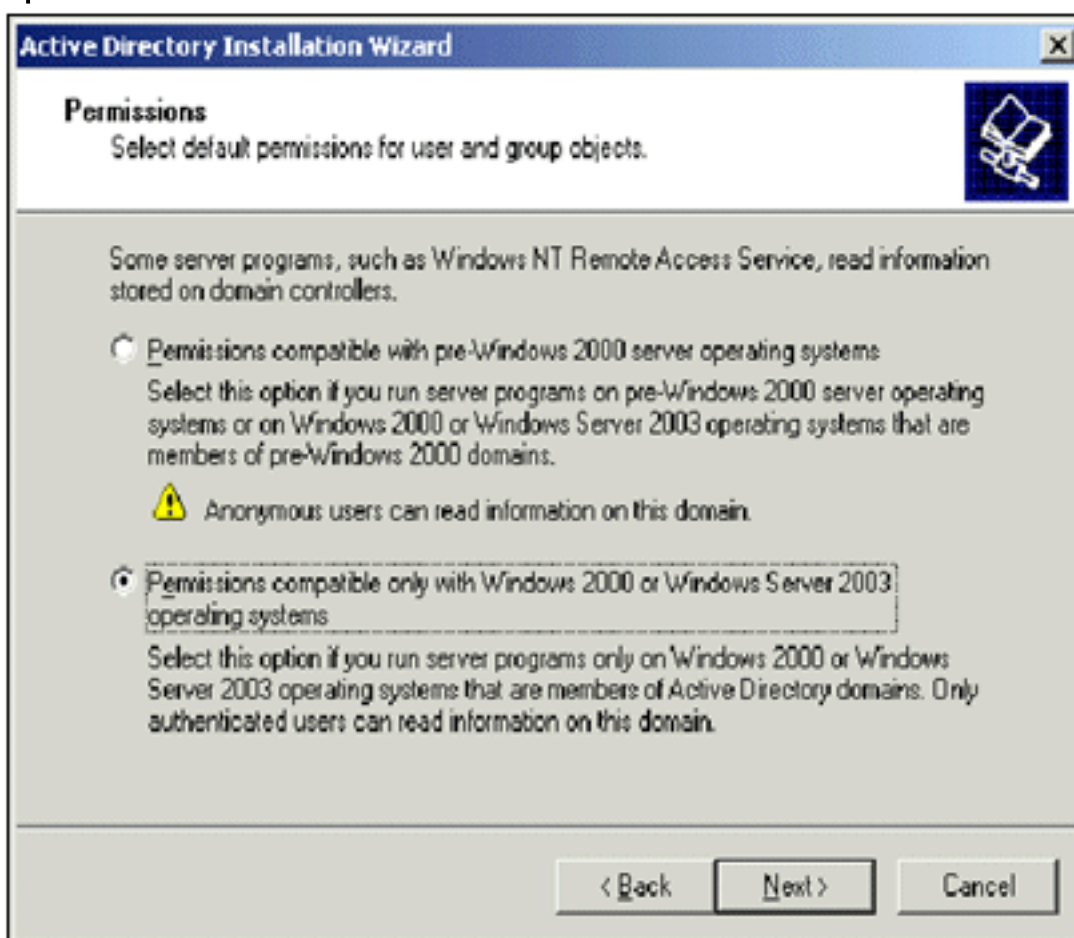
**Avanti.**

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



Avanti.

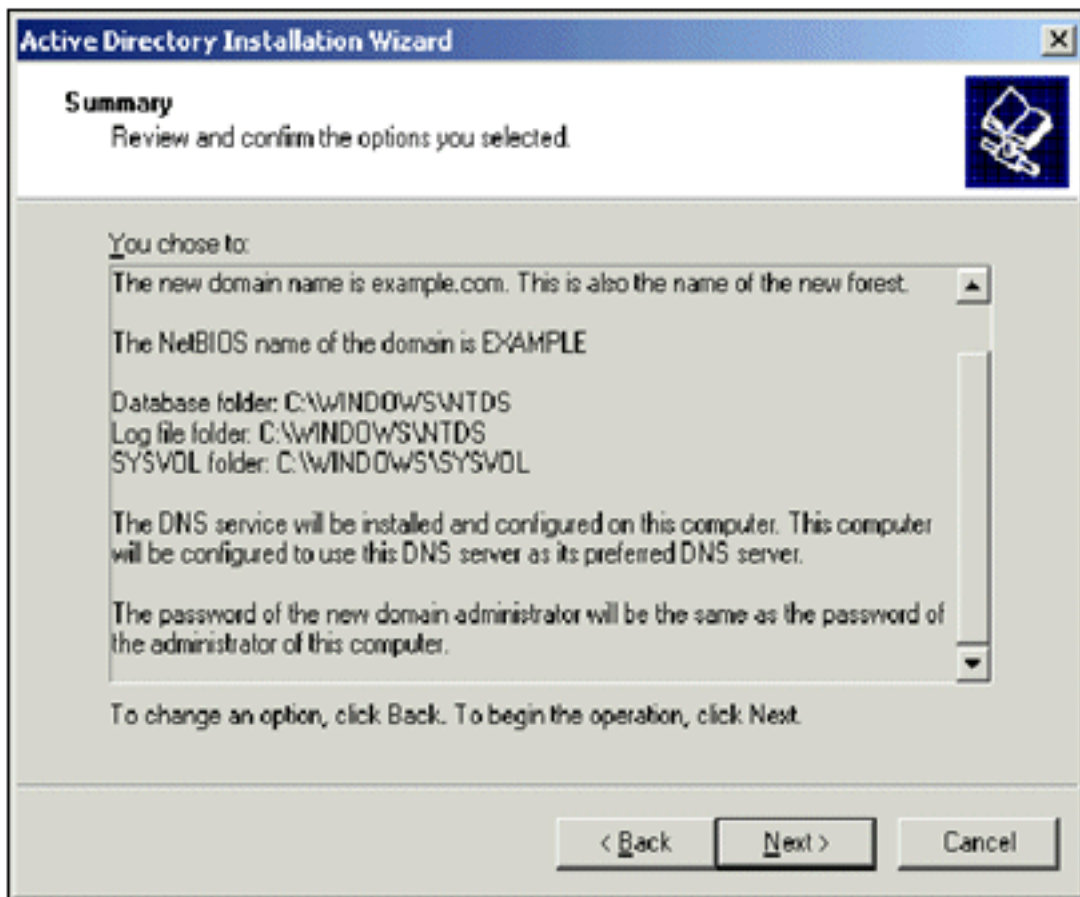
11. Nella pagina Autorizzazioni verificare che l'opzione **Autorizzazioni compatibili solo con i sistemi operativi Windows 2000 o Windows Server 2003** sia selezionata e fare clic su



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.

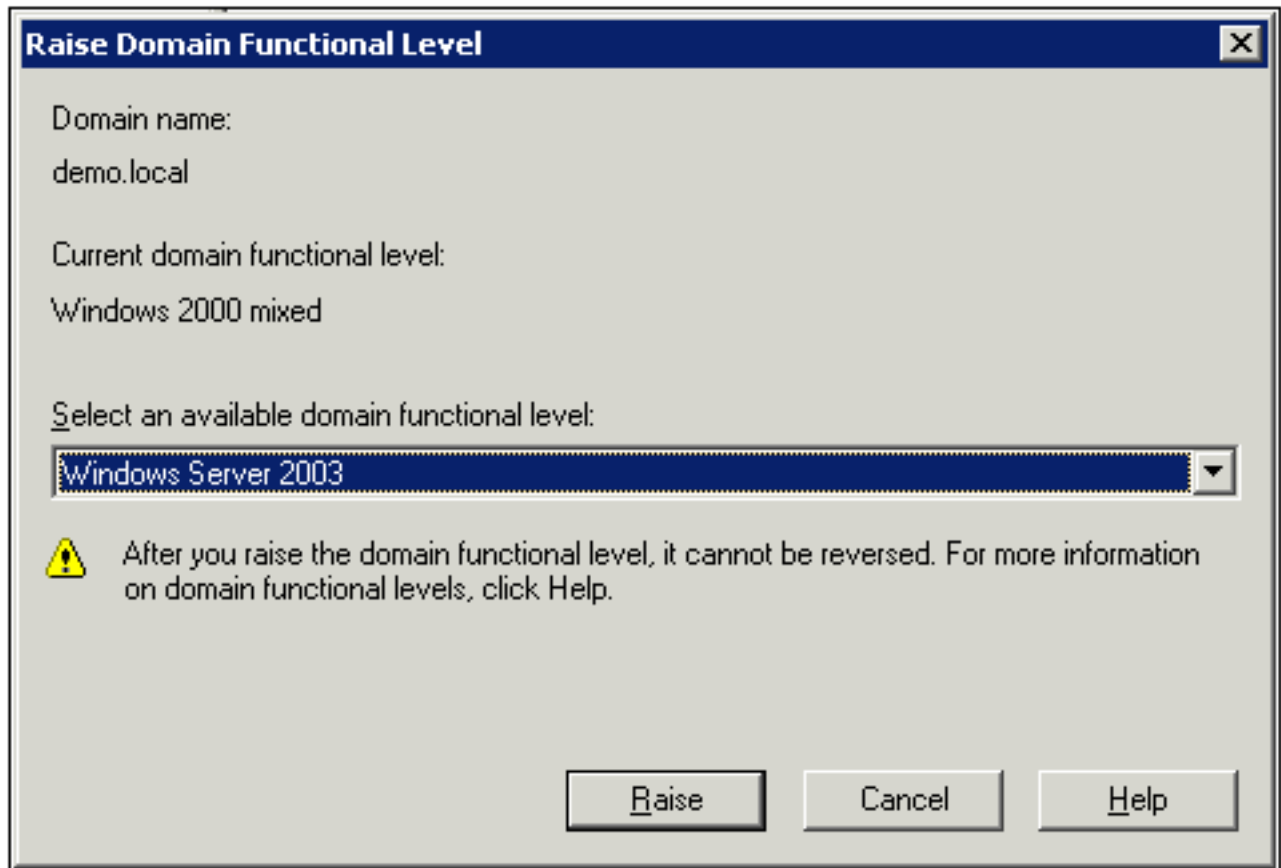
14. Al termine dell'installazione di Active Directory, fare clic su **Fine**.

15. Quando viene richiesto di riavviare il computer, fare clic su **Riavvia ora**.

### [Aumentare il livello di funzionalità del dominio](#)

Attenersi alla procedura seguente:

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



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

### [Installare e configurare DHCP](#)


Attenersi alla procedura seguente:

1. Installare **DHCP (Dynamic Host Configuration Protocol)** come componente **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, **CA.demo.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 **CA.demo.local**, 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.



**New Scope Wizard**

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



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

Name:

Description:

< Back   Next >   Cancel

7. Fare clic su **Avanti** e specificare i seguenti parametri: Indirizzo IP iniziale - **10.0.20.1** Indirizzo IP finale - **10.0.20.200** Lunghezza - **24** Subnet mask - **255.255.255.0**

**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:

End IP address:

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:

Subnet mask:

< Back    Next >    Cancel

8. Fare clic su **Next** (Avanti) e immettere *10.0.20.1* per l'indirizzo IP iniziale e *10.0.20.100* per l'indirizzo IP finale da escludere. Quindi fare clic su **Avanti**. Gli indirizzi IP compresi nell'intervallo da 10.0.20.1 a 10.0.20.100 vengono riservati. Questi indirizzi IP di riserva non sono assegnati dal server DHCP.

**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.

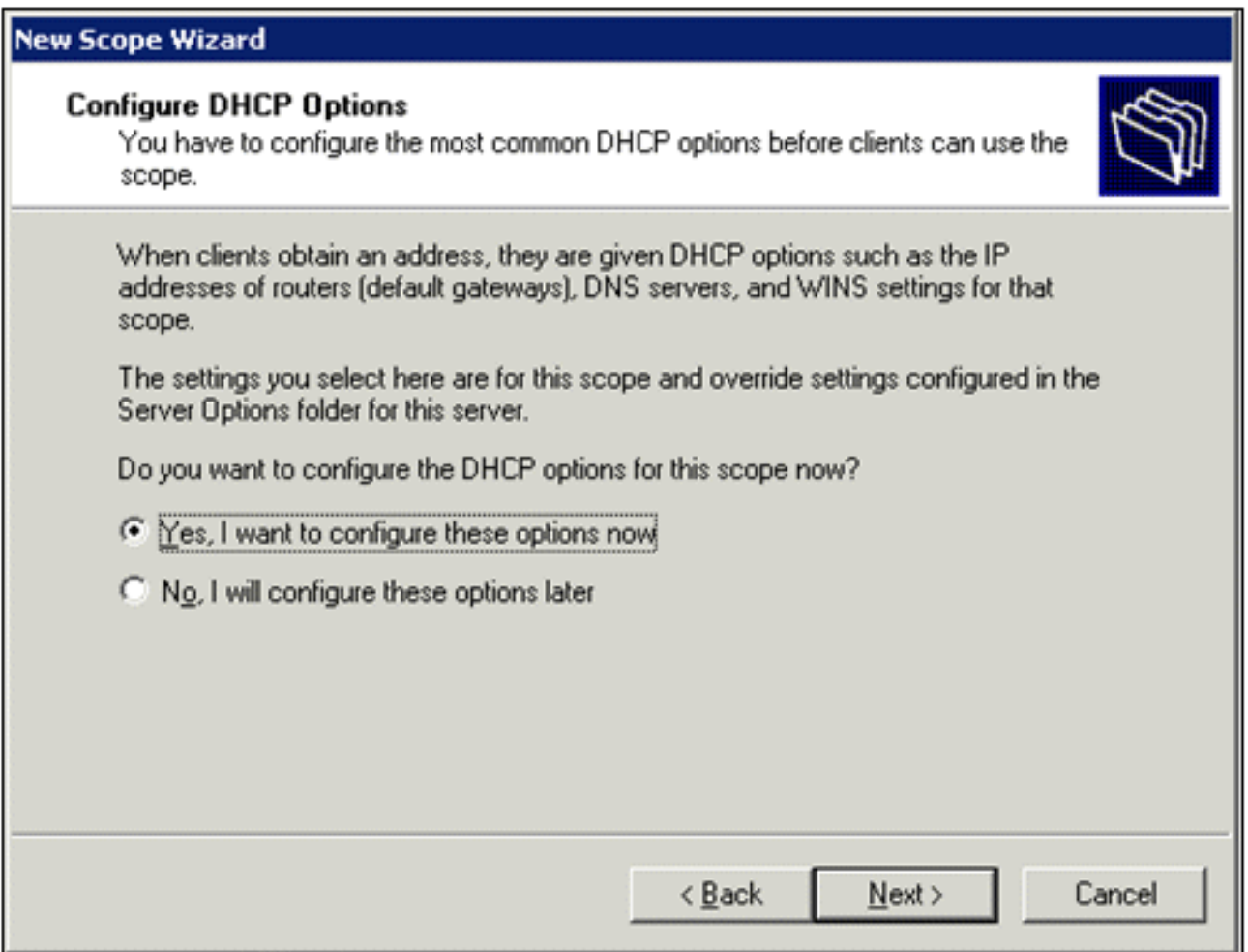
Start IP address:  End IP address:

Excluded address range:

< **Back**   **Next** >   Cancel

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 *10.0.20.1* 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:

10 . 0 . 20 . 1	Add
	Remove
	Up
	Down

< Back   Next >   Cancel

12. Nella pagina Nome dominio e server DNS digitare *demo.local* nel campo Dominio padre, digitare *10.0.10.10* nel campo Indirizzo IP e quindi fare clic su **Aggiungi** e fare clic su **Avanti**.

**New Scope Wizard**

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

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

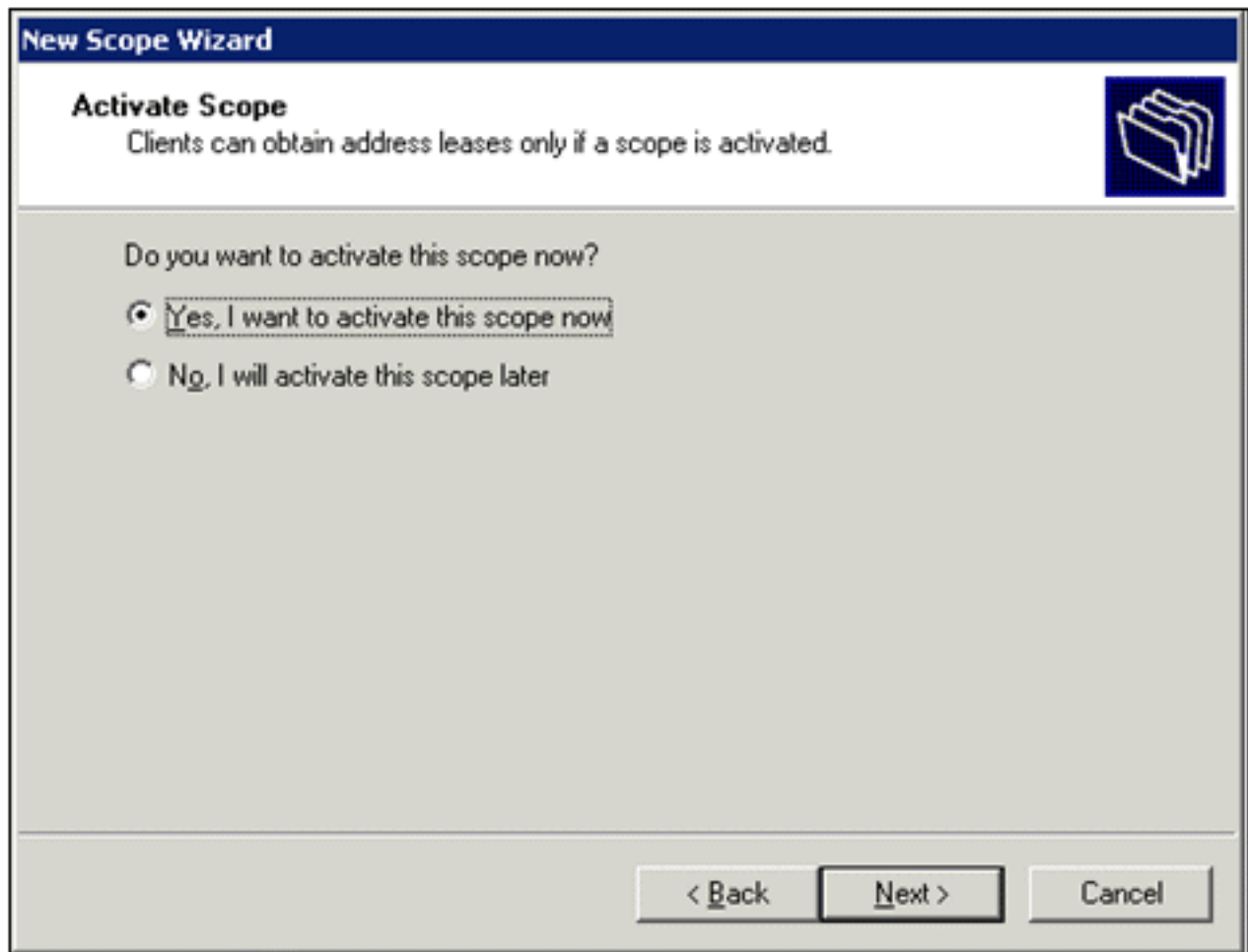
Parent domain:

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

Server name:	IP address:	
<input type="text"/>	<input type="text" value="  . . ."/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	<input type="text" value="10.0.10.10"/>	<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

13. Nella pagina Server WINS fare clic su **Avanti**.

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



15. Al termine, fare clic su **Fine**.

### [Installa Servizi certificati](#)

Attenersi alla procedura seguente:

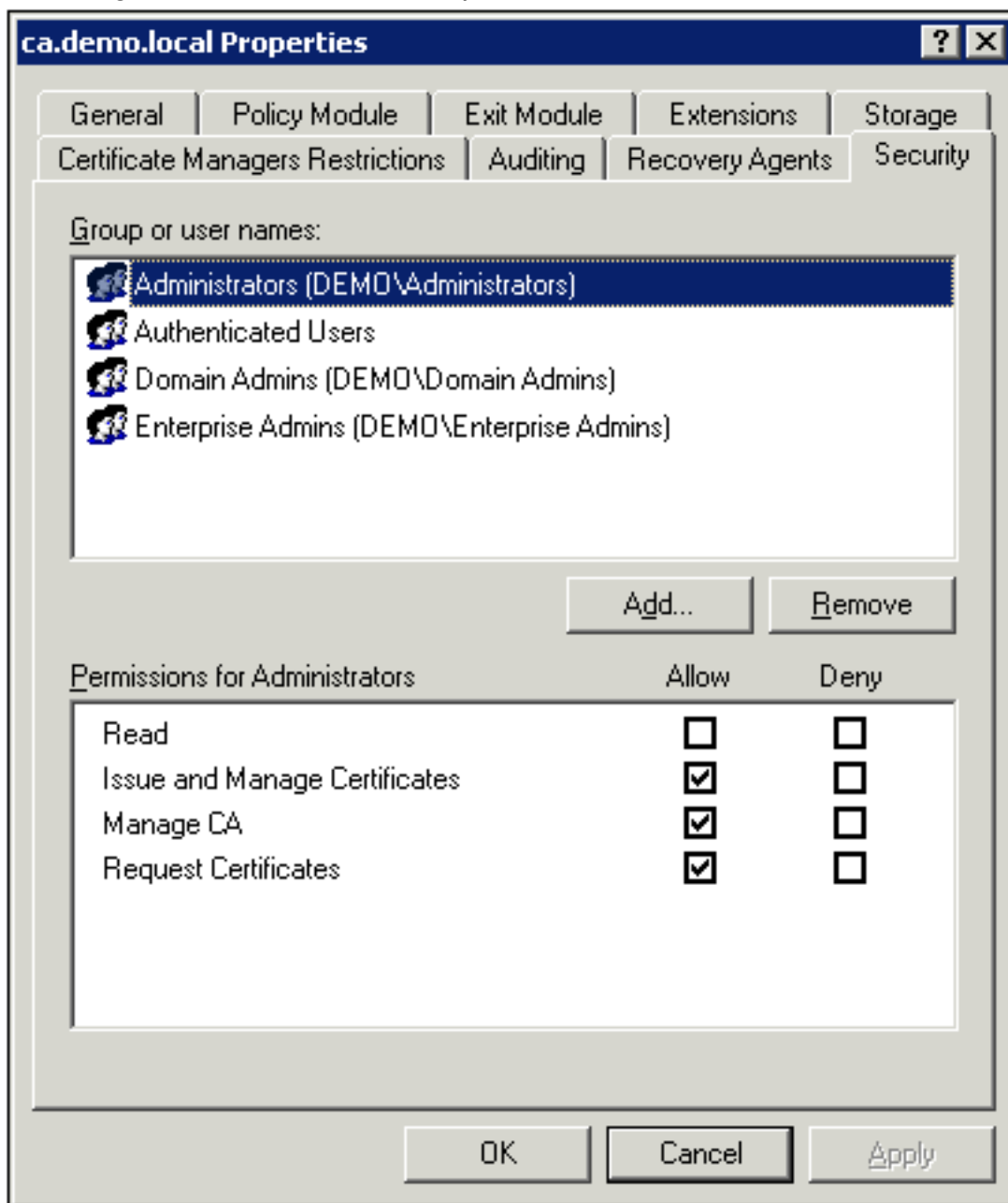
**Nota:** prima di installare Servizi certificati è necessario installare IIS e l'utente deve appartenere all'unità organizzativa Enterprise Admin.

1. Nel Pannello di controllo aprire **Installazione applicazioni** e quindi fare clic su **Installazione componenti di Windows**.
2. Nella pagina Aggiunta guidata componenti di Windows scegliere Servizi certificati e quindi fare clic su **Avanti**.
3. Nella pagina Tipo di CA scegliere CA radice dell'organizzazione (enterprise) e fare clic su **Avanti**.
4. Nella pagina Informazioni di identificazione della CA digitare *democa* nella casella Nome comune per la CA. È inoltre possibile immettere gli altri dettagli facoltativi. Fare quindi clic su **Avanti** e 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 il messaggio di avviso relativo all'installazione di IIS.

### [Verifica autorizzazioni amministratore per i certificati](#)

Attenersi alla procedura seguente:

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



**Consenti.**

5. Fare clic su **OK** per chiudere la finestra di dialogo Proprietà CA demo e quindi chiudere Autorità di certificazione.

### [Aggiungi computer al dominio](#)

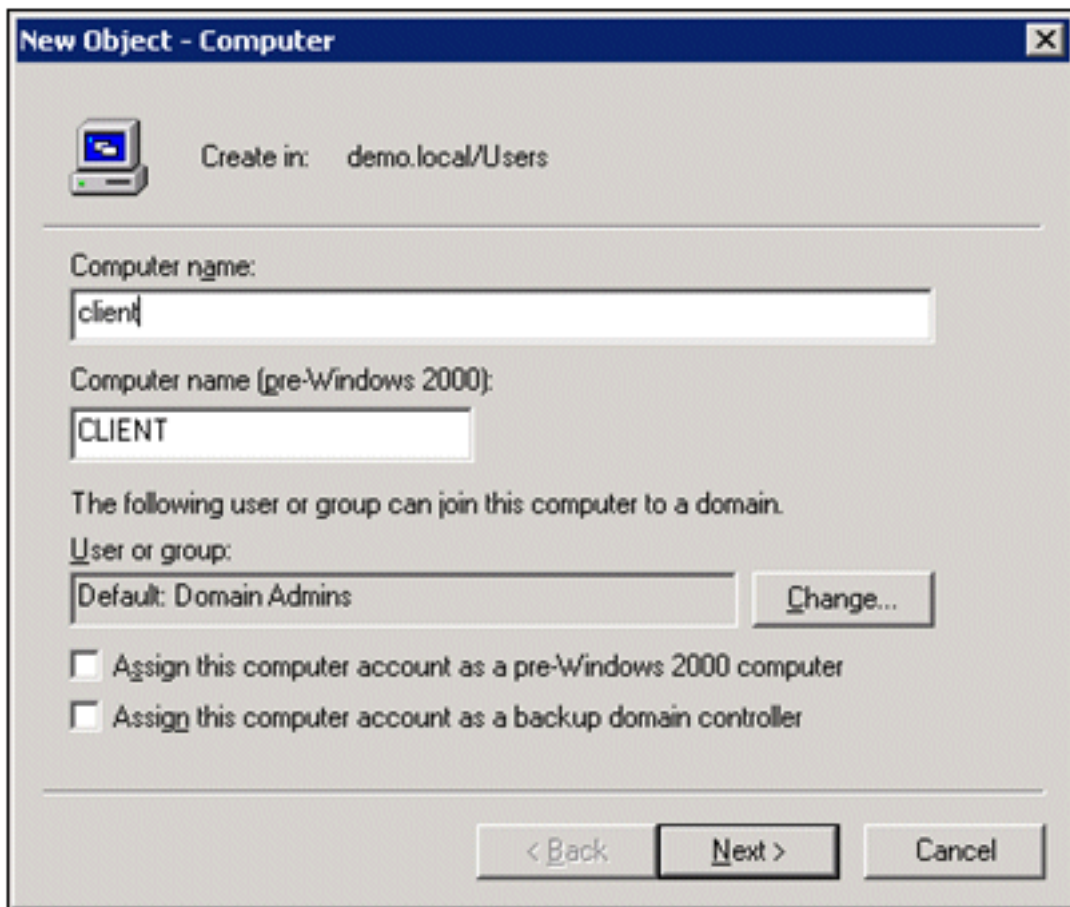
Attenersi alla procedura seguente:

**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 **demo.local**.



3. Fare clic con il pulsante destro del mouse su **Computer**, 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



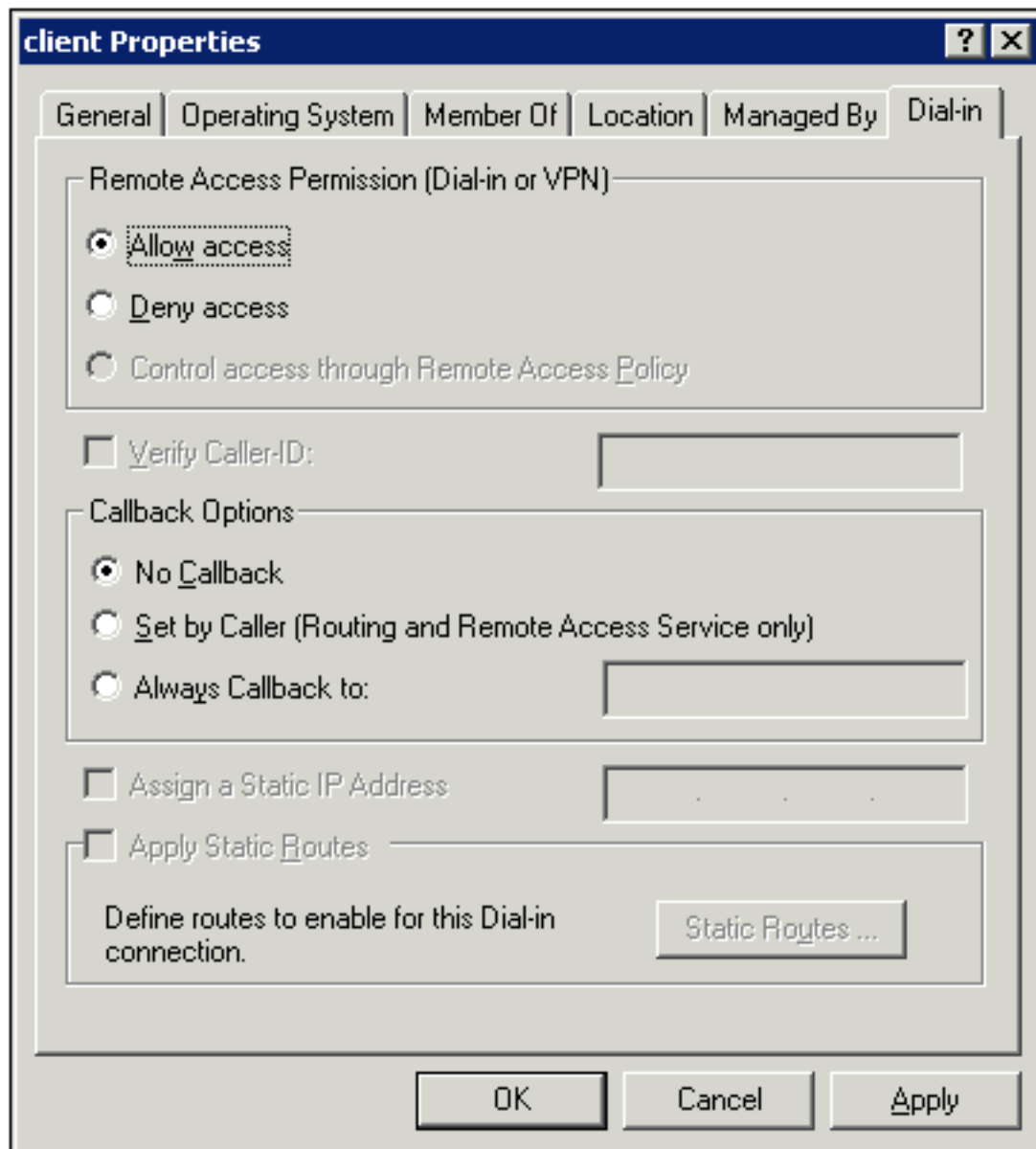
*Client.*

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

### [Consenti accesso wireless ai computer](#)

Attenersi alla procedura seguente:

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 computer **Client** aggiunta al passaggio 7. Fare clic su **Proprietà**, quindi selezionare la scheda **Connessione remota**.
2. In Autorizzazione di accesso remoto, scegliere **Consenti accesso**, quindi fare clic su




OK.

### [Aggiungi utenti al dominio](#)

Attenersi alla procedura seguente:

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**

**New Object - User** [X]

 Create in: demo.local/Users

---

First name:  Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

---

(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

Create in: demo.local/Users

Password: [masked]

Confirm password: [masked]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back    Next >    Cancel

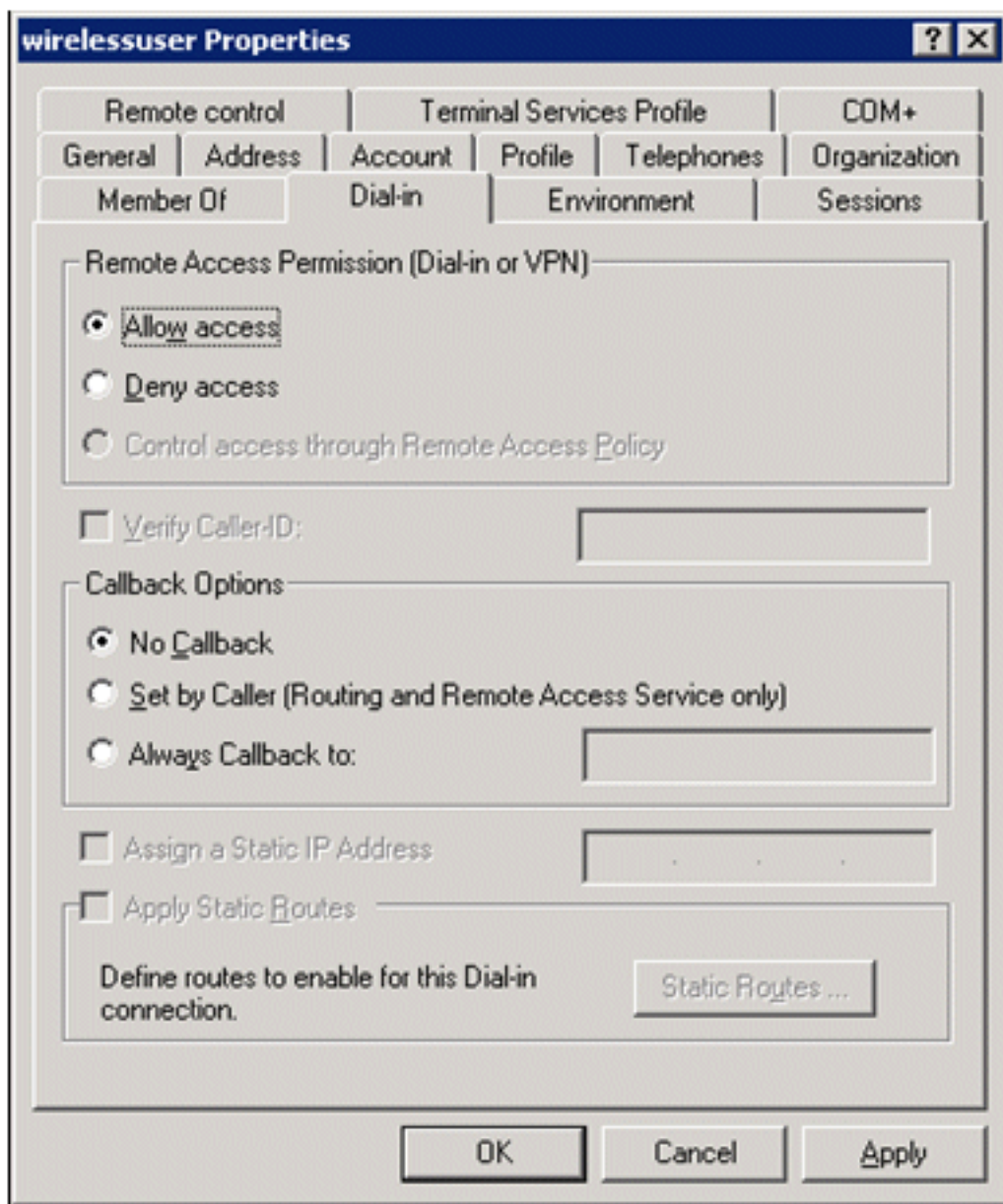
Avanti.

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

### [Consenti accesso wireless agli utenti](#)

Attenersi alla procedura seguente:

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 **utente wireless**, scegliere **Proprietà** e quindi selezionare la scheda **Connessione remota**.
2. In Autorizzazione di accesso remoto, scegliere **Consenti accesso**, quindi fare clic su

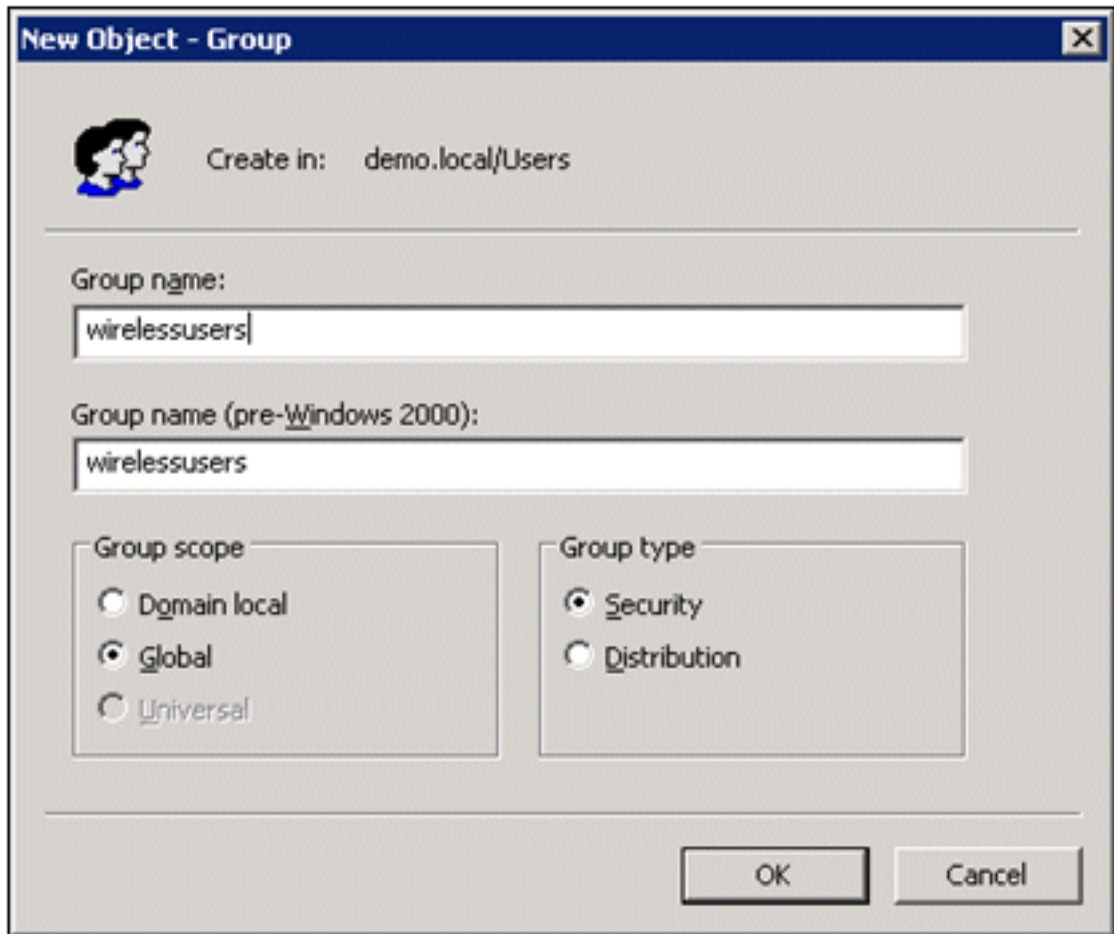


OK.

### [Aggiungi gruppi al dominio](#)

Attenersi alla procedura seguente:

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 **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 del gruppo *wireless*

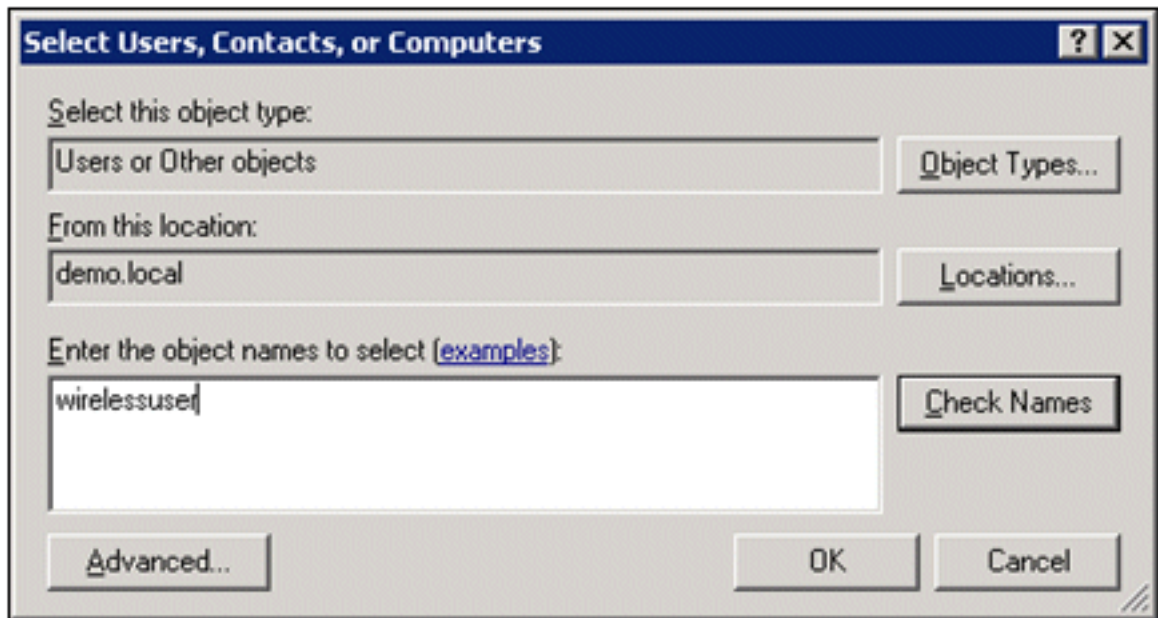


users.

### [Aggiungi utenti al gruppo di utenti wireless](#)

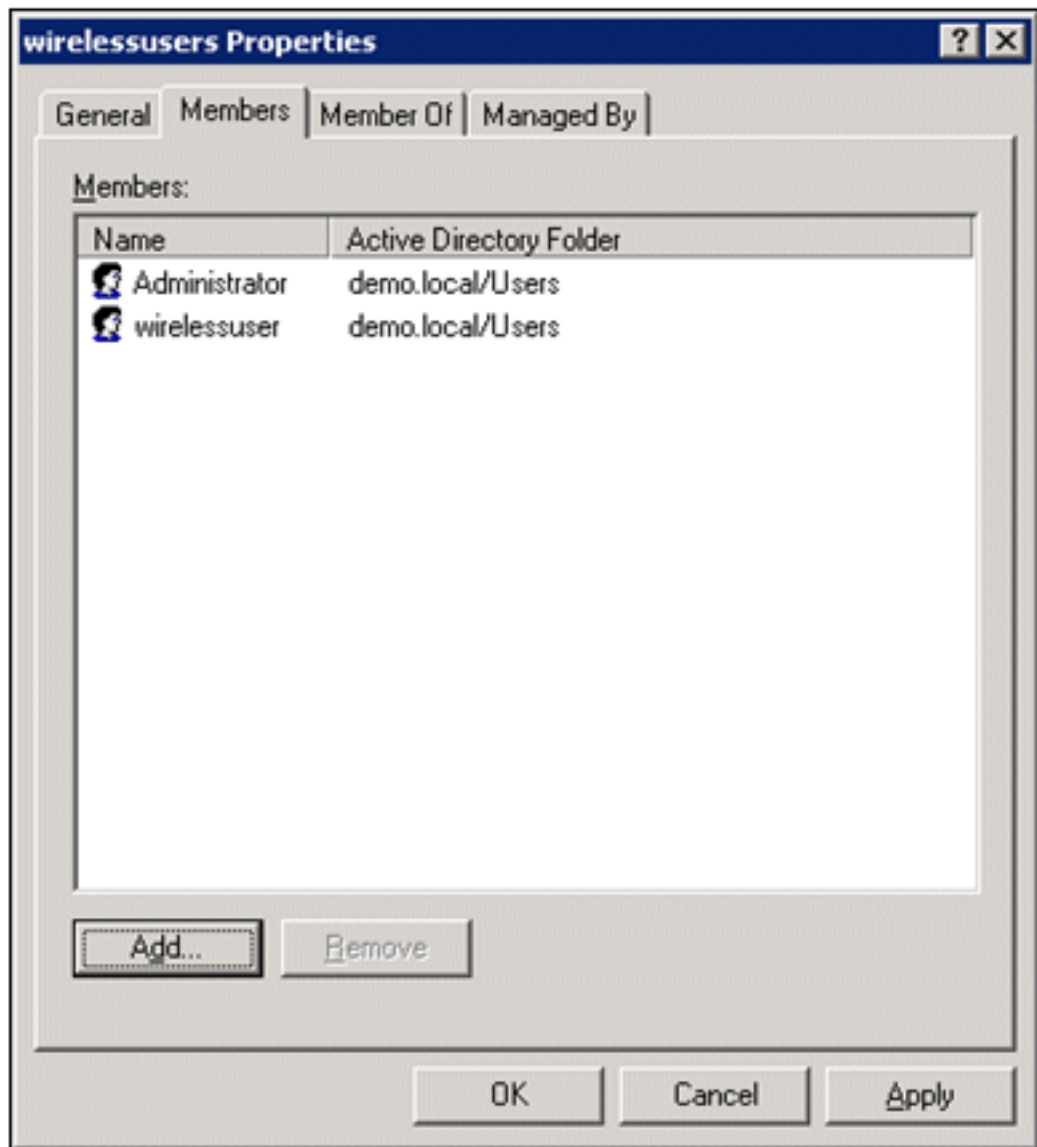
Attenersi alla procedura seguente:

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 wireless viene aggiunto al gruppo



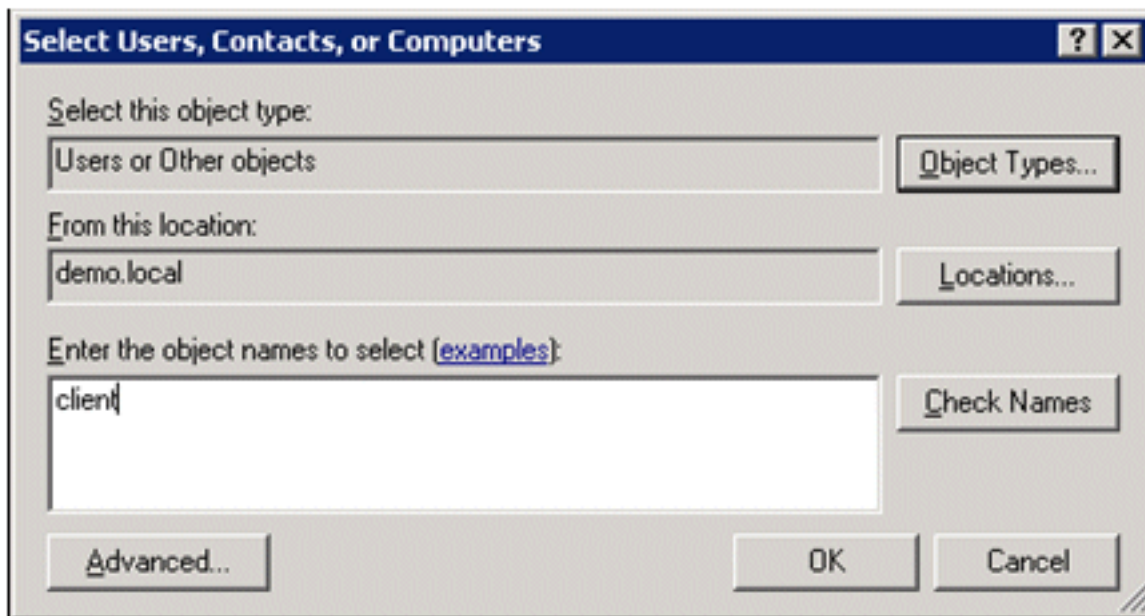
wirelessusers.

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

## [Aggiungi computer client al gruppo wireless Users](#)

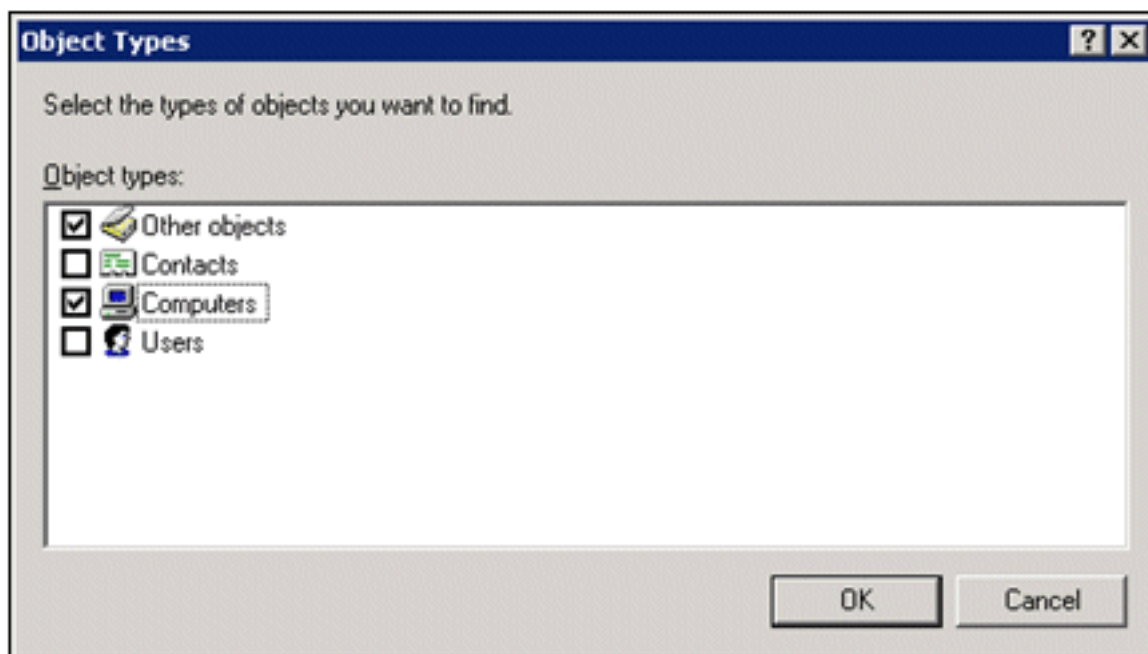
Attenersi alla procedura seguente:

1. Ripetere i passaggi 1 e 2 nella sezione [Aggiunta di utenti al gruppo di utenti wireless](#) 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



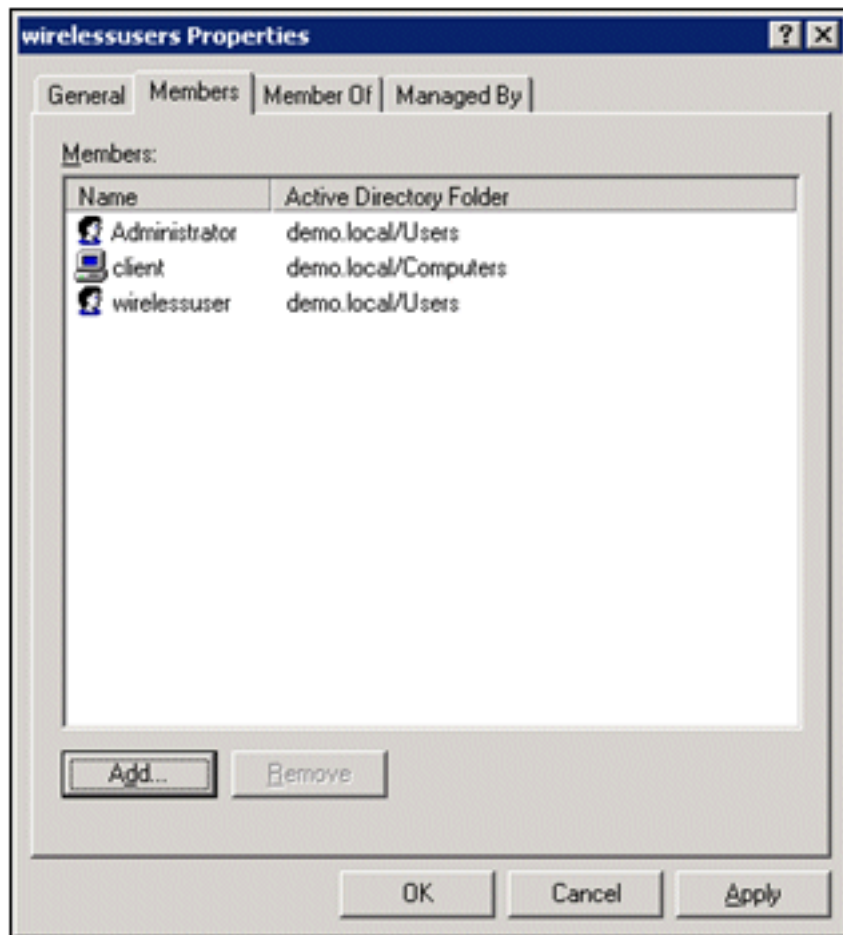
gruppo.

3. Fare clic su **Tipi di oggetto**, deselegionare 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.

## Cisco 1121 Secure ACS 5.1

### Installazione con l'accessorio serie CSACS-1121

L'accessorio CSACS-1121 è dotato del software ACS 5.1. In questa sezione viene fornita una panoramica del processo di installazione e delle attività da eseguire prima di installare ACS.

1. Collegare il CSACS-1121 alla rete e alla console dell'accessorio. Vedere [il Capitolo 4, "Collegamento dei cavi"](#).
2. Accendere il CSACS-1121. Vedere [il Capitolo 4, "Accensione dell'accessorio della serie CSACS-1121"](#).
3. Eseguire il comando **setup** al prompt della CLI per configurare le impostazioni iniziali per il server ACS. Vedere Esecuzione del programma di installazione.

### Installare il server ACS

In questa sezione viene descritto il processo di installazione del server ACS sugli accessori della serie CSACS-1121.

- [Eseguire il programma di installazione](#)
- [Verifica del processo di installazione](#)
- [Operazioni successive all'installazione](#)

Per informazioni dettagliate sull'installazione di Cisco Secure ACS Server, consultare la [guida](#)

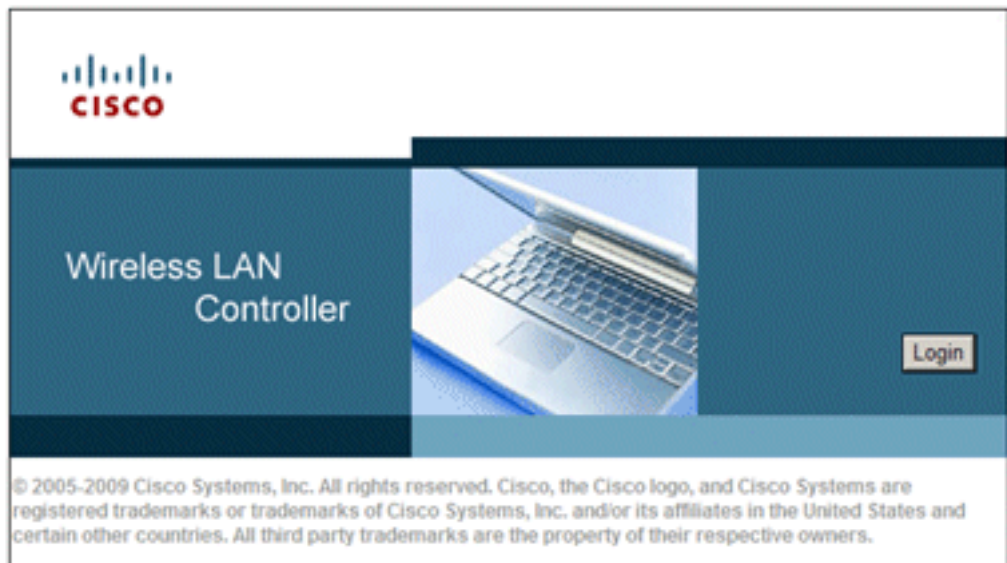
## Configurazione controller Cisco WLC5508

### Creare la configurazione necessaria per WPAv2/WPA

Attenersi alla procedura seguente:

**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. Per accedere al controller, selezionare



<https://10.0.1.10>.

2. Fare clic su **Login**.
3. Accedere con l'utente *admin* predefinito e la password *admin* predefinita.
4. Creare una nuova interfaccia per il mapping della VLAN nel menu **Controller**.
5. Fare clic su **Interfacce**.
6. Fare clic su **New**.
7. Nel campo Nome interfaccia immettere *Dipendente*. Questo campo può contenere qualsiasi valore.
8. Nel campo VLAN ID, immettere *20*. (Questo campo può essere qualsiasi VLAN trasportata nella rete).
9. Fare clic su **Apply** (Applica).
10. Configurare le informazioni come mostrato in questa finestra Interfacce > Modifica:Indirizzo IP interfaccia - **10.0.20.2**Maschera di rete - **255.255.255.0**Gateway - **10.0.10.1**DHCP primario - **10.0.10.10**

Save Configuration | Ping | Logout | Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Controller

Interfaces > Edit < Back Apply

General  
Inventory  
Interfaces  
Multicast  
Network Routes  
Internal DHCP Server  
Mobility Management  
Ports  
NTP  
CDP  
Advanced

**General Information**

Interface Name employee  
MAC Address 00:24:97:69:4d:e0

**Configuration**

Guest Lan   
Quarantine   
Quarantine Vlan Id

**Physical Information**

Port Number   
Backup Port   
Active Port 0  
Enable Dynamic AP Management

**Interface Address**

VLAN Identifier   
IP Address   
Netmask   
Gateway

**DHCP Information**

Primary DHCP Server   
Secondary DHCP Server

**Access Control List**

ACL Name

*Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.*

11. Fare clic su **Apply** (Applica).
12. Fare clic sulla scheda **WLAN**.
13. Scegliere **Crea nuovo**, quindi fare clic su **Vai**.
14. Immettere il nome di un profilo e nel campo SSID WLAN immettere *Employee*.

Save Configuration | Ping | Logout | Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs

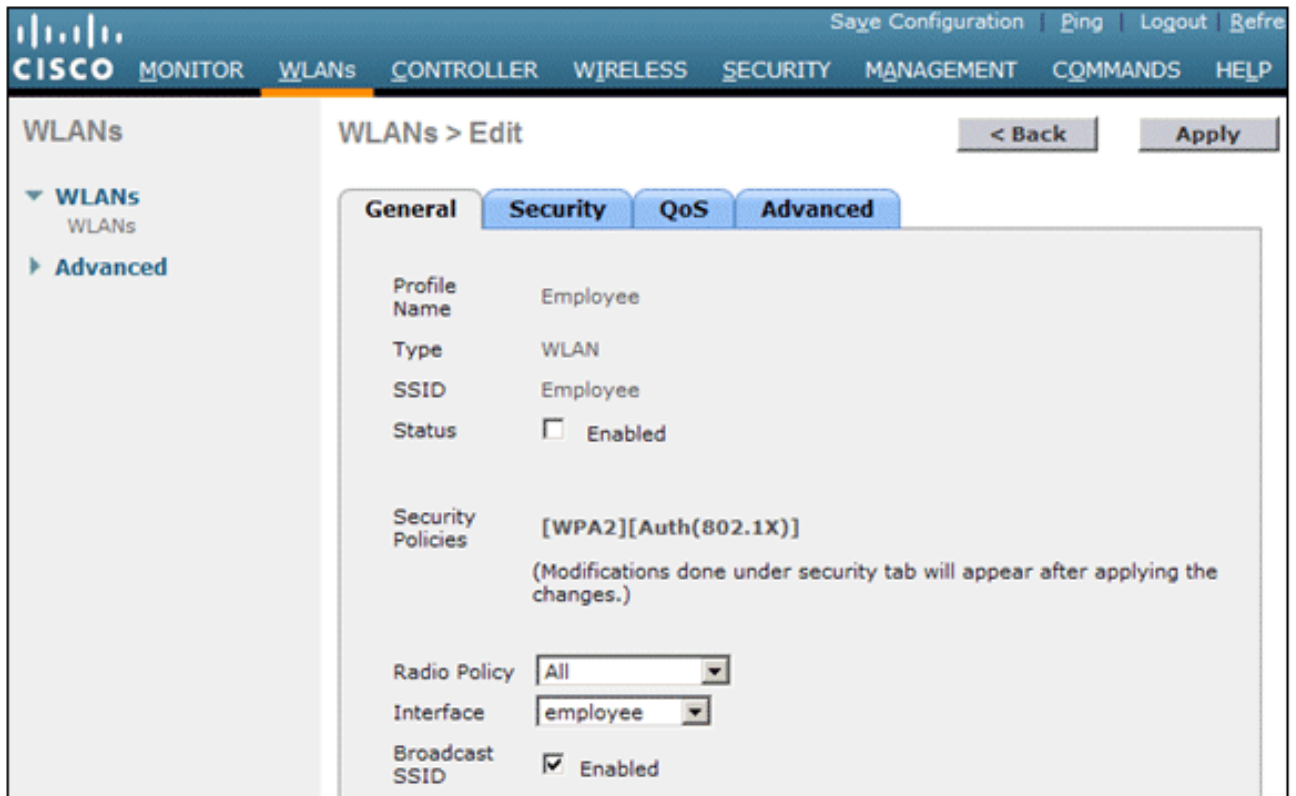
WLANs > New < Back Apply

WLANs  
Advanced

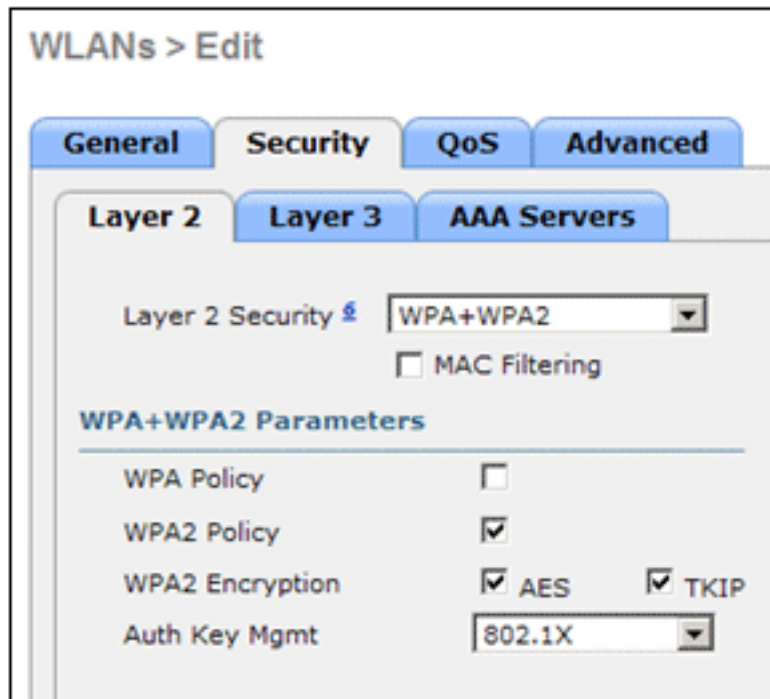
Type   
Profile Name   
SSID   
ID

15. Selezionare l'ID della WLAN e fare clic su **Apply** (Applica).

16. Configurare le informazioni per questa WLAN quando viene visualizzata la finestra WLAN > Modifica. **Nota:** WPAv2 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. Nella schermata WLAN > Modifica, fare clic sulla scheda **Generale**.
18. Verificare che la casella Stato sia selezionata per **Abilitato** e che sia selezionata l'**interfaccia** appropriata (dipendente). Verificare inoltre che la casella di controllo **Abilitato** per Broadcast SSID sia selezionata.



19. Fare clic sulla scheda **Protezione**.
20. Nel sottomenu di layer 2, selezionare **WPA + WPA2** per Sicurezza di layer 2. Per la crittografia WPA2, selezionare **AES + TKIP** per consentire i client TKIP.
21. Scegliere **802.1x** come metodo di



autenticazione.

22. Ignorare il sottomenu di layer 3 poiché non è necessario. Una volta configurato il server RADIUS, è possibile scegliere il server appropriato dal menu Autenticazione.
23. Le schede **QoS** e **Advanced** possono essere lasciate in posizione predefinita, a meno che non siano richieste configurazioni speciali.
24. Fare clic sul menu **Security** per aggiungere il server RADIUS.
25. Nel sottomenu RADIUS fare clic su **Autenticazione**. Fare quindi clic su **Nuovo**.
26. Aggiungere l'indirizzo IP del server RADIUS (10.0.10.20), che è il server ACS configurato in precedenza.
27. Verificare che la chiave condivisa corrisponda al client AAA configurato nel server ACS. Verificare che la casella **Utente di rete** sia selezionata e fare clic su **Applica**.

28. La configurazione di base è stata completata ed è possibile iniziare a eseguire il test di PEAP.

## Autenticazione PEAP

PEAP con MS-CHAP versione 2 richiede certificati sui server ACS ma non sui client wireless. La registrazione automatica dei certificati dei computer per i server ACS può essere utilizzata per semplificare una distribuzione.

Per configurare il server CA in modo che fornisca la registrazione automatica per i certificati del computer e dell'utente, 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 che consenta di eseguire questa operazione.

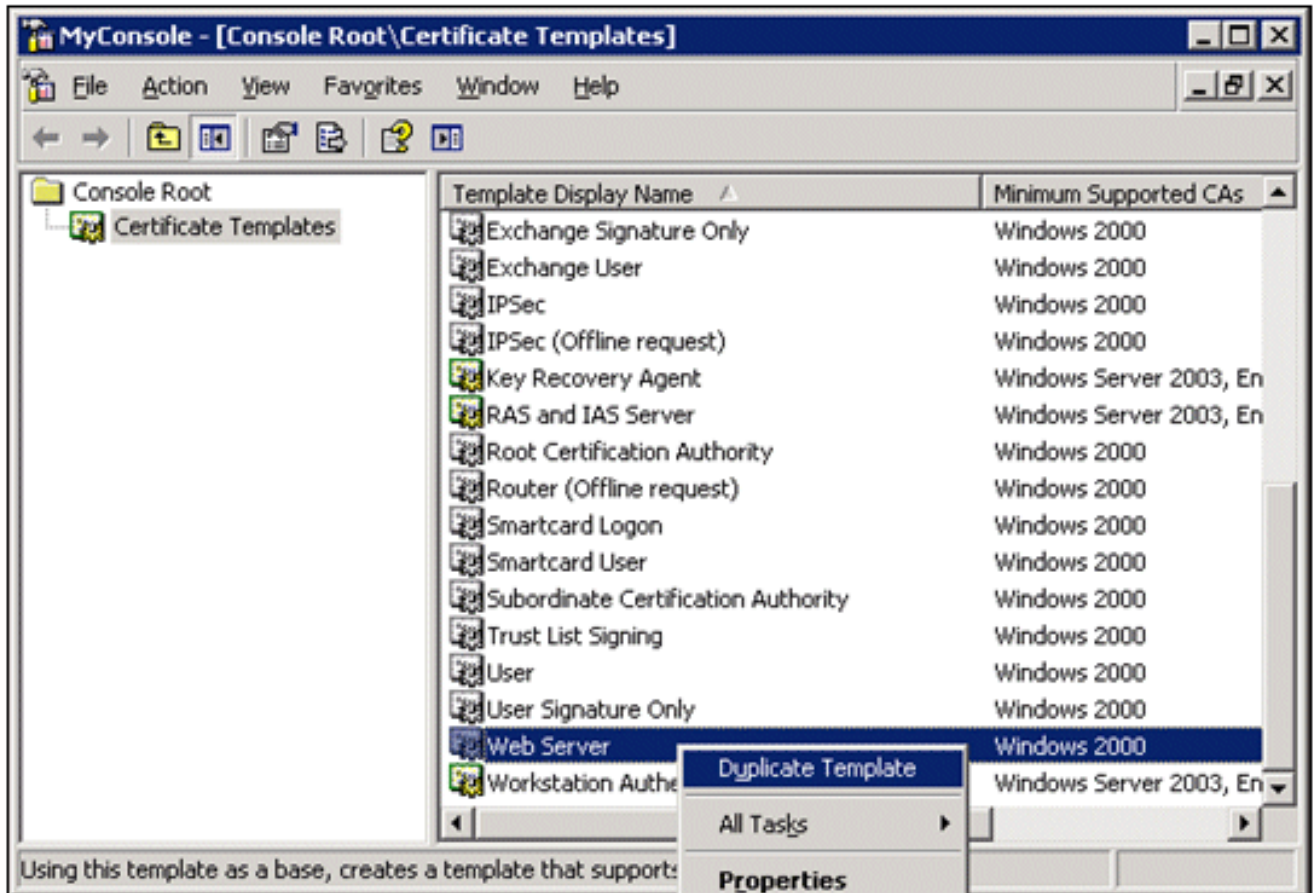
**Nota:** Windows 2000 consente l'esportazione di chiavi e queste procedure non devono essere seguite se si utilizza Windows 2000.

## Installare lo snap-in Modelli di certificato

Attenersi alla procedura seguente:

1. Scegliere **Start > Esegui**, immettere *mmc* e 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, immettere *certtmpl.msc* per aprire lo snap-in Modelli di certificato.



## [Creare il modello di certificato per il server Web ACS](#)

Attenersi alla procedura seguente:

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

**Properties of New Template** [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:  
Copy of Web Server

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:  
Copy of Web Server

Validity period: 2 years | Renewal period: 6 weeks

Publish certificate in Active Directory  
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

Azione.

3. Nel campo Nome visualizzato modello, immettere

**Properties of New Template** [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:  
ACS

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:  
ACS

Validity period: 2 years | Renewal period: 6 weeks

Publish certificate in Active Directory  
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

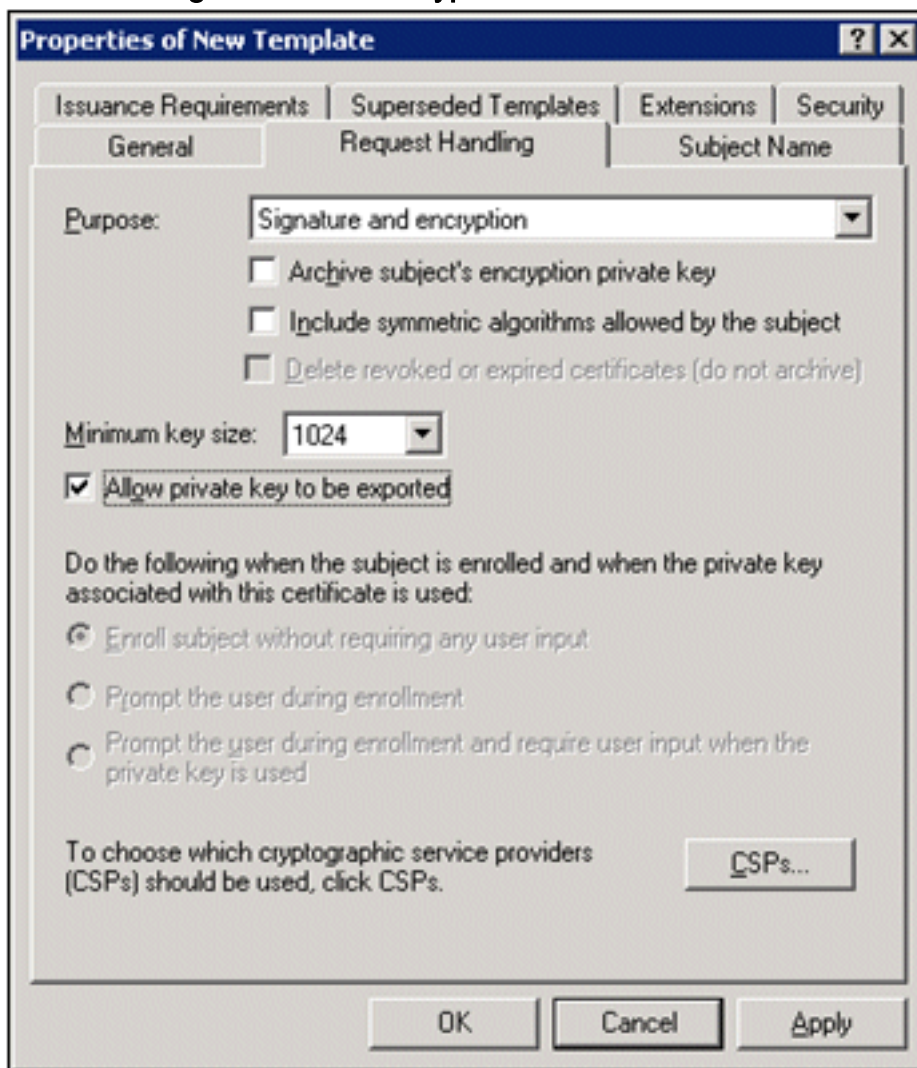
OK Cancel Apply

ACS.

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

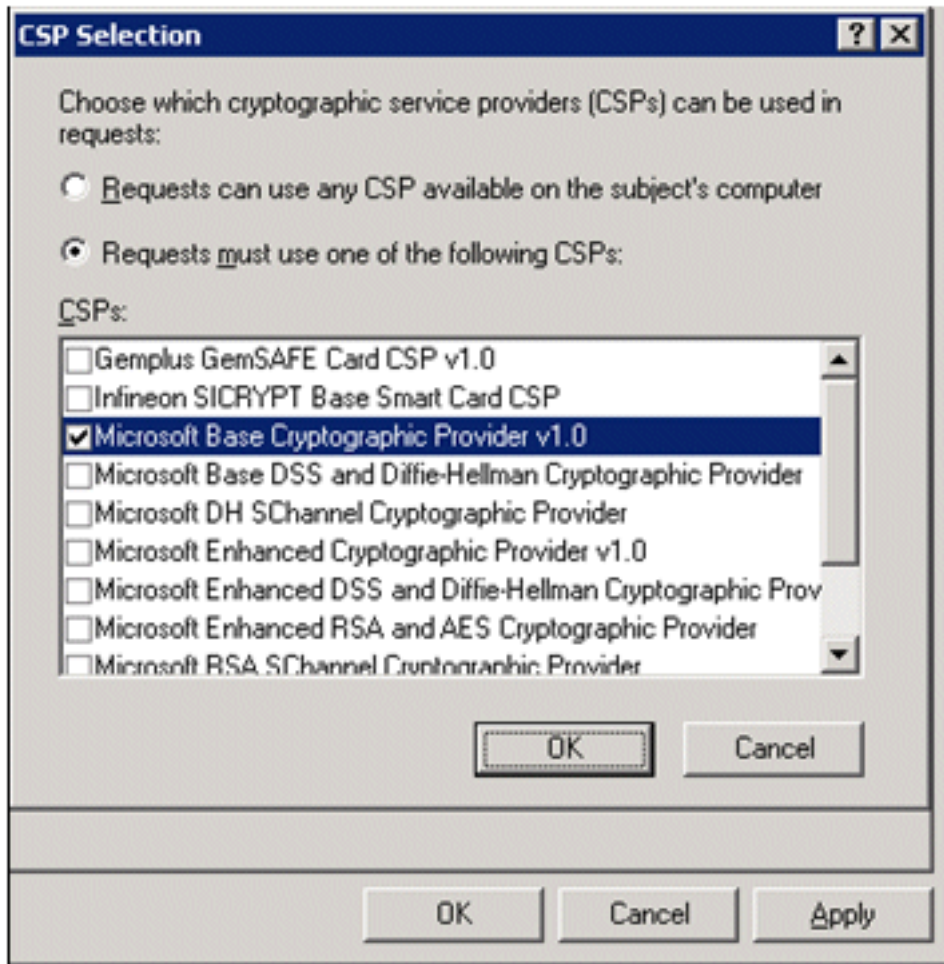


privata. Verificare inoltre che **Signature and Encryption** sia selezionato dal menu a discesa



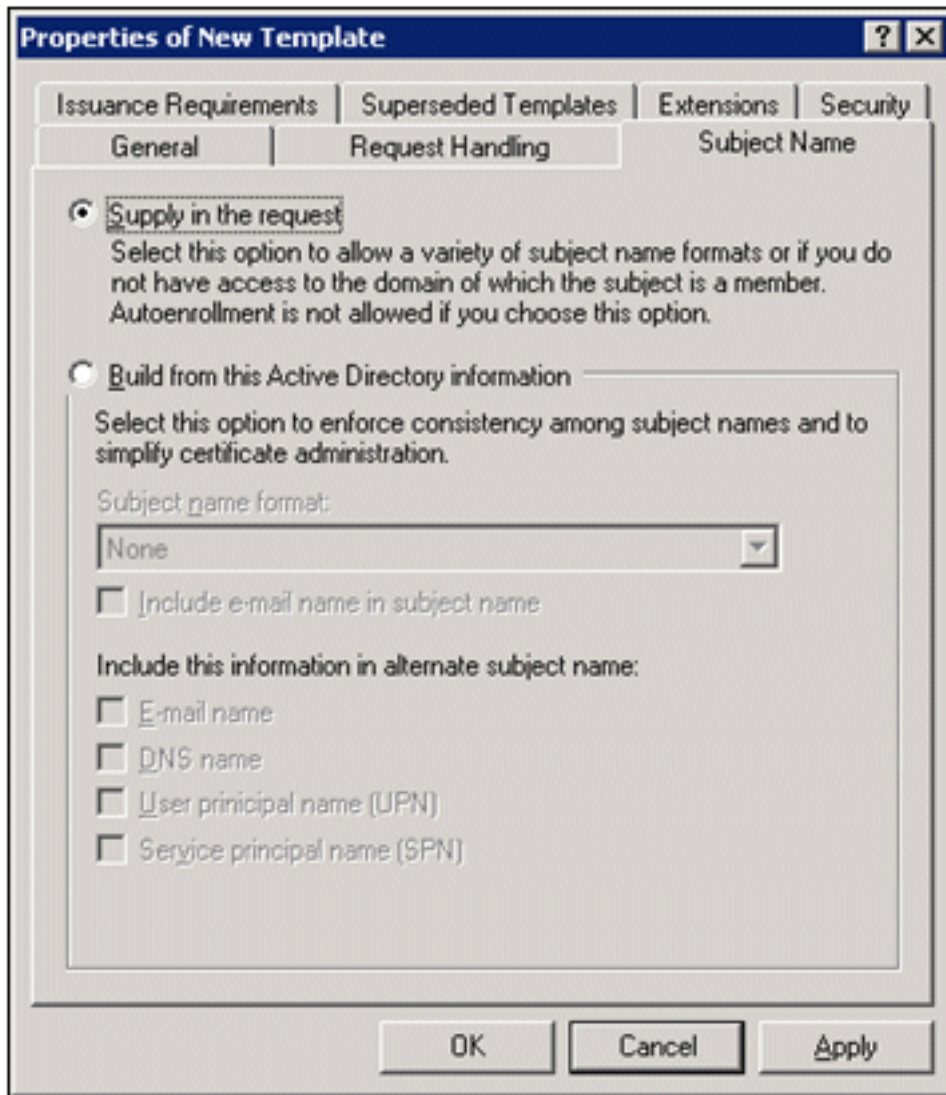
Purpose (Scopo).

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



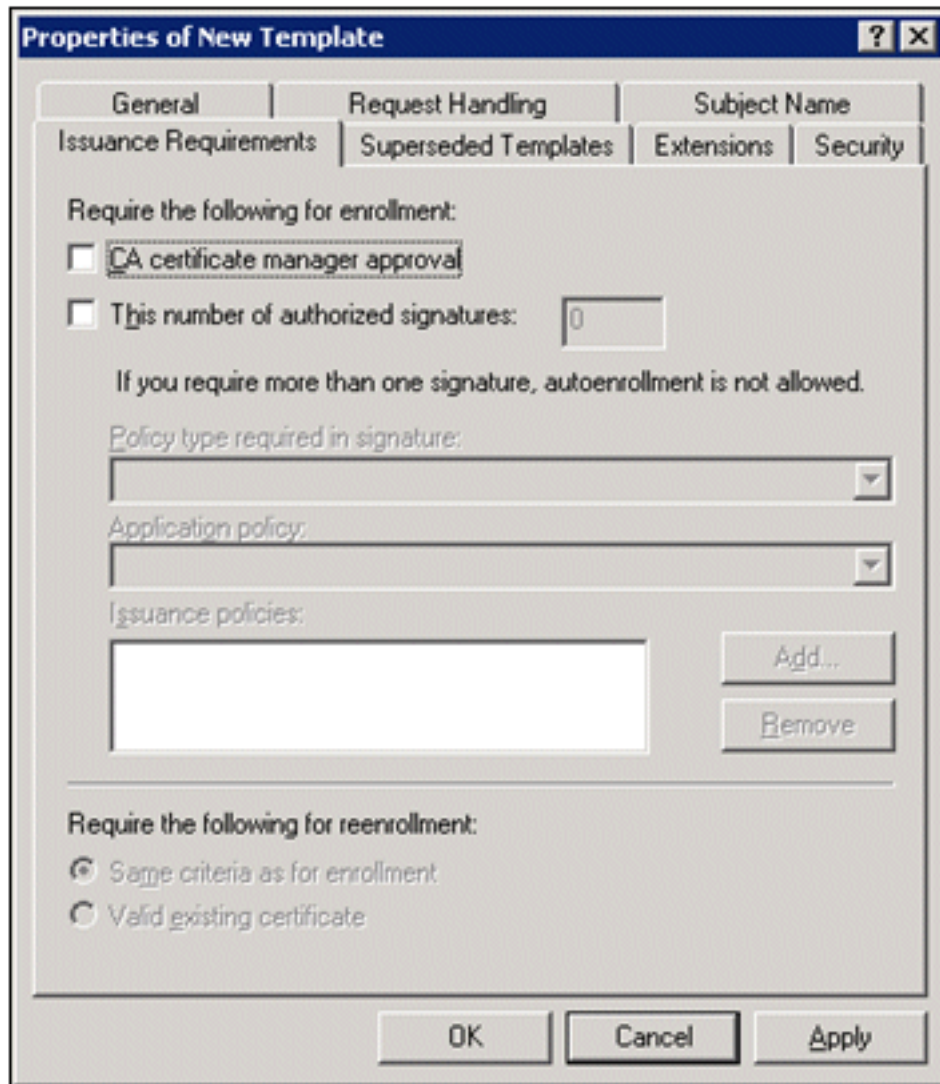
OK.

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



OK.

7. Andare alla scheda **Protezione**, evidenziare il **gruppo Domain Admins** e assicurarsi che l'opzione **Enroll** sia selezionata in Allowed. **Nota:** se si sceglie di compilare da queste informazioni di Active Directory, controllare solo il **nome dell'entità utente (UPN)** e deselezionare l'opzione **Includi nome di posta elettronica** nel nome dell'oggetto e nel nome di posta elettronica. Non è stato immesso un nome di posta elettronica per l'account utente wireless 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 relativo.
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. Questo punto non viene ulteriormente discusso nel presente



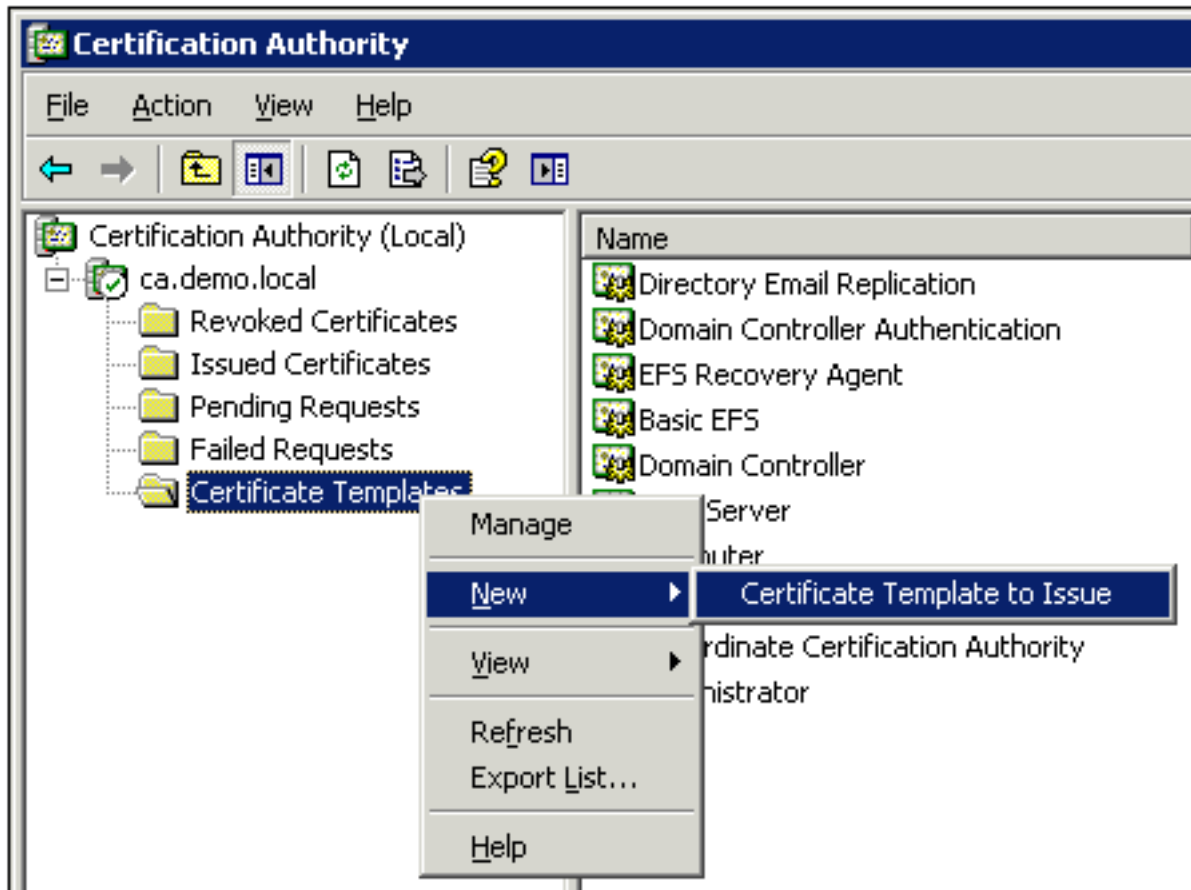
documento.

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

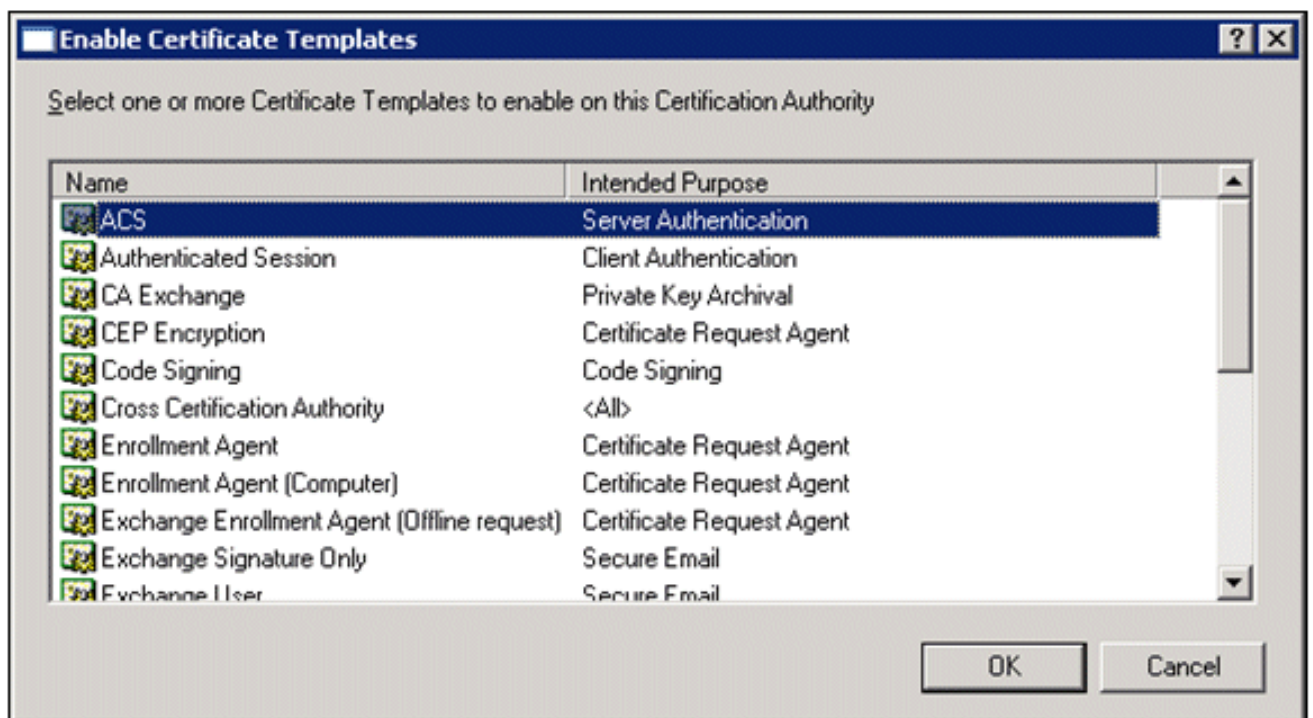
## [Abilita il nuovo modello di certificato server Web ACS](#)

Attenersi alla procedura seguente:

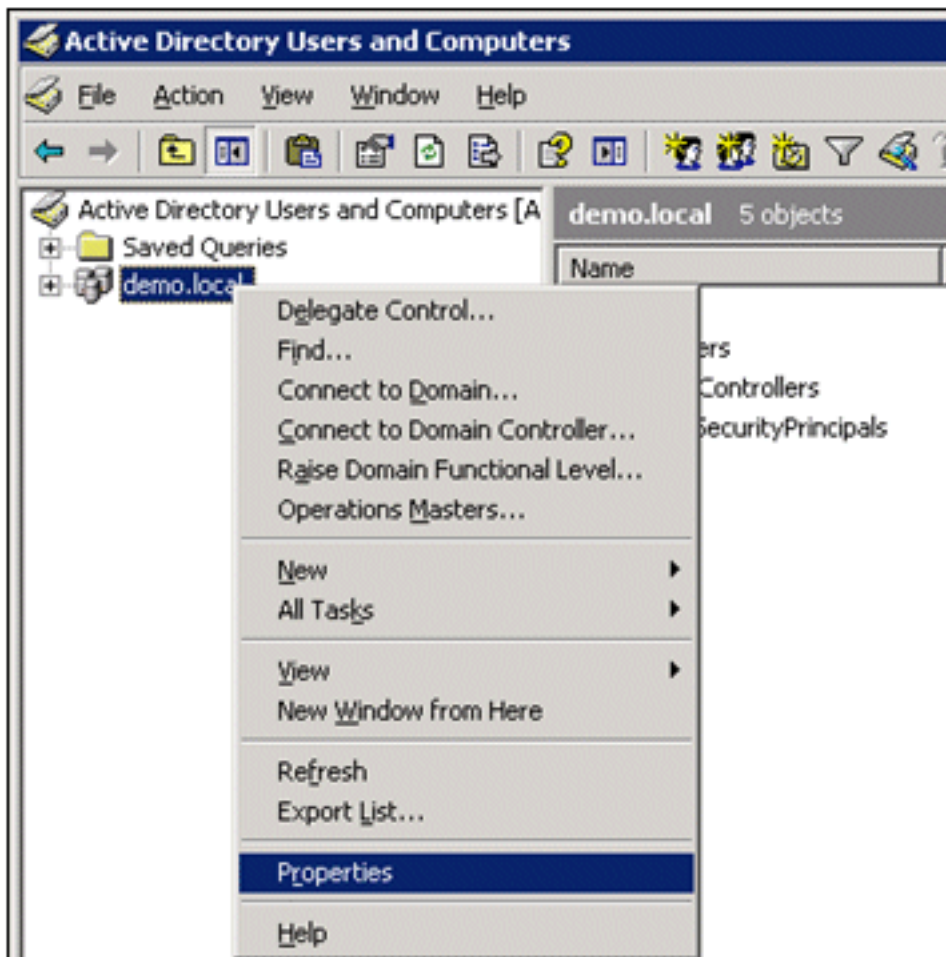
1. Aprire lo snap-in Autorità di certificazione. Eseguire i passaggi da 1 a 3 della sezione [Creazione del modello di certificato per il server Web ACS](#), scegliere l'opzione **Autorità di certificazione**, scegliere **Computer locale** e fare clic su **Fine**.
2. Nell'albero della console Autorità di certificazione espandere **ca.demo.local**, quindi fare clic con il pulsante destro del mouse su **Modelli di certificato**.
3. Andare a **Nuovo > Modello di certificato da emettere**.



4. Fare clic sul **modello di certificato ACS**.

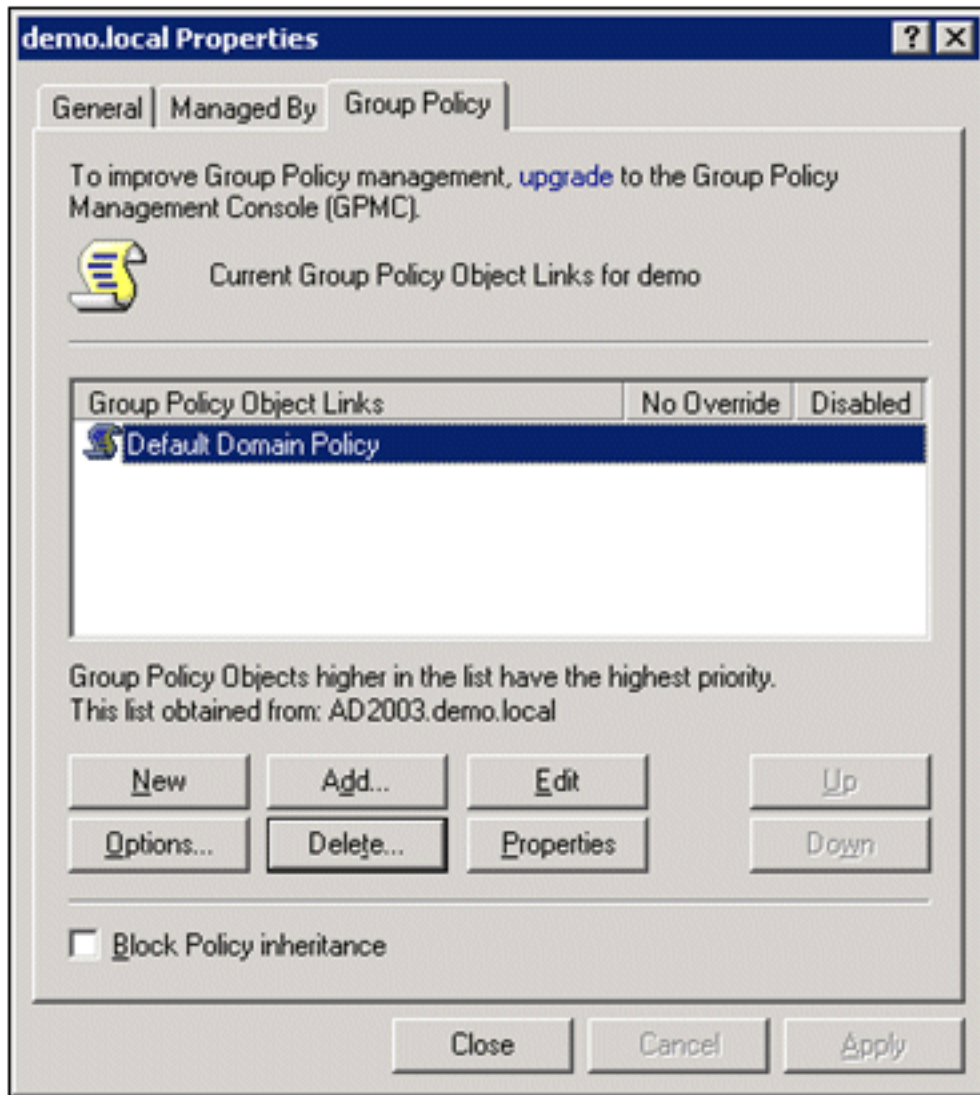


5. Fare clic su **OK** e aprire lo **snap-in Utenti e computer di Active Directory**.
6. Nell'albero della console fare doppio clic su **Utenti e computer di Active Directory**, fare clic con il pulsante destro del mouse su **demo.local** e quindi scegliere



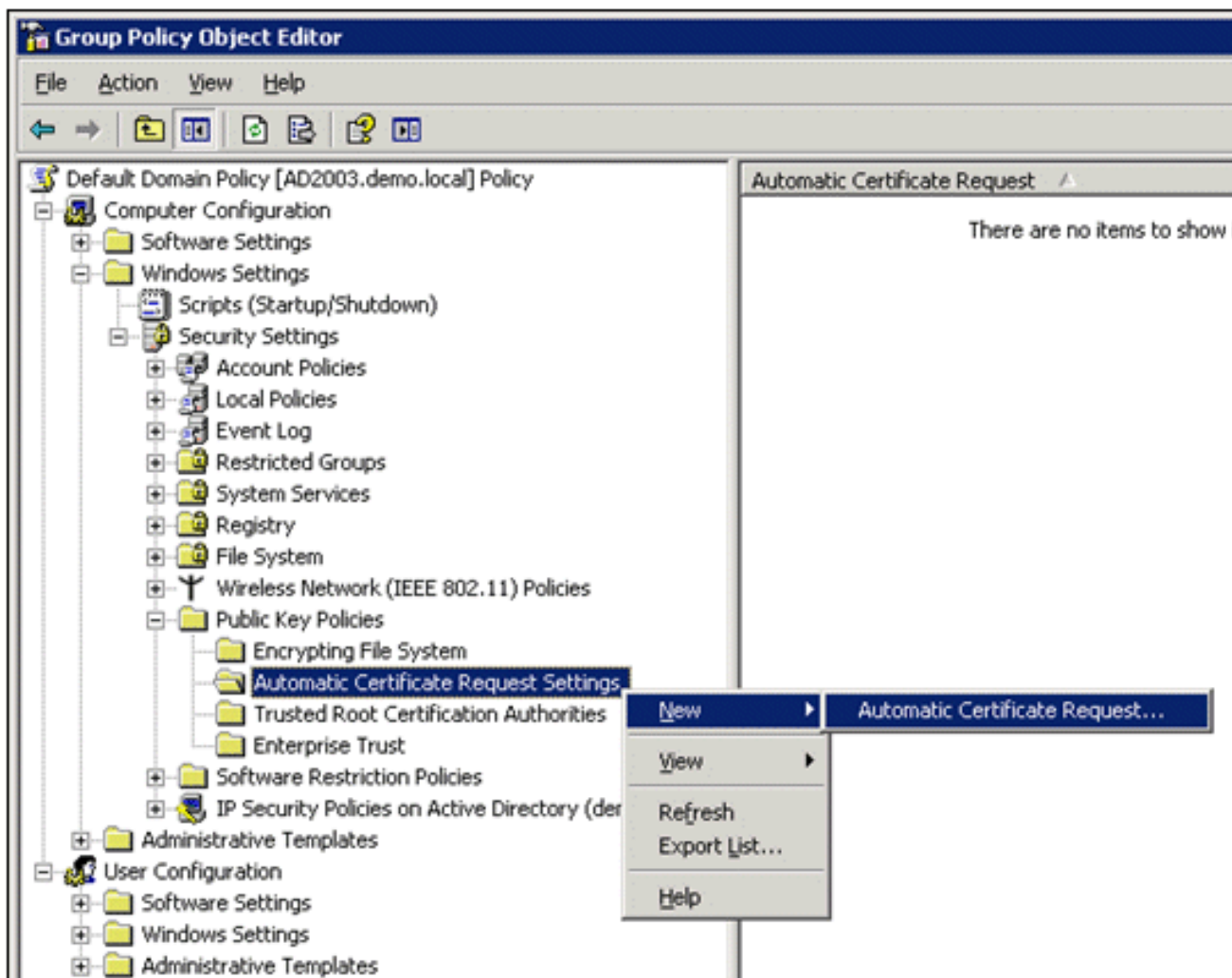
Proprietà.

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



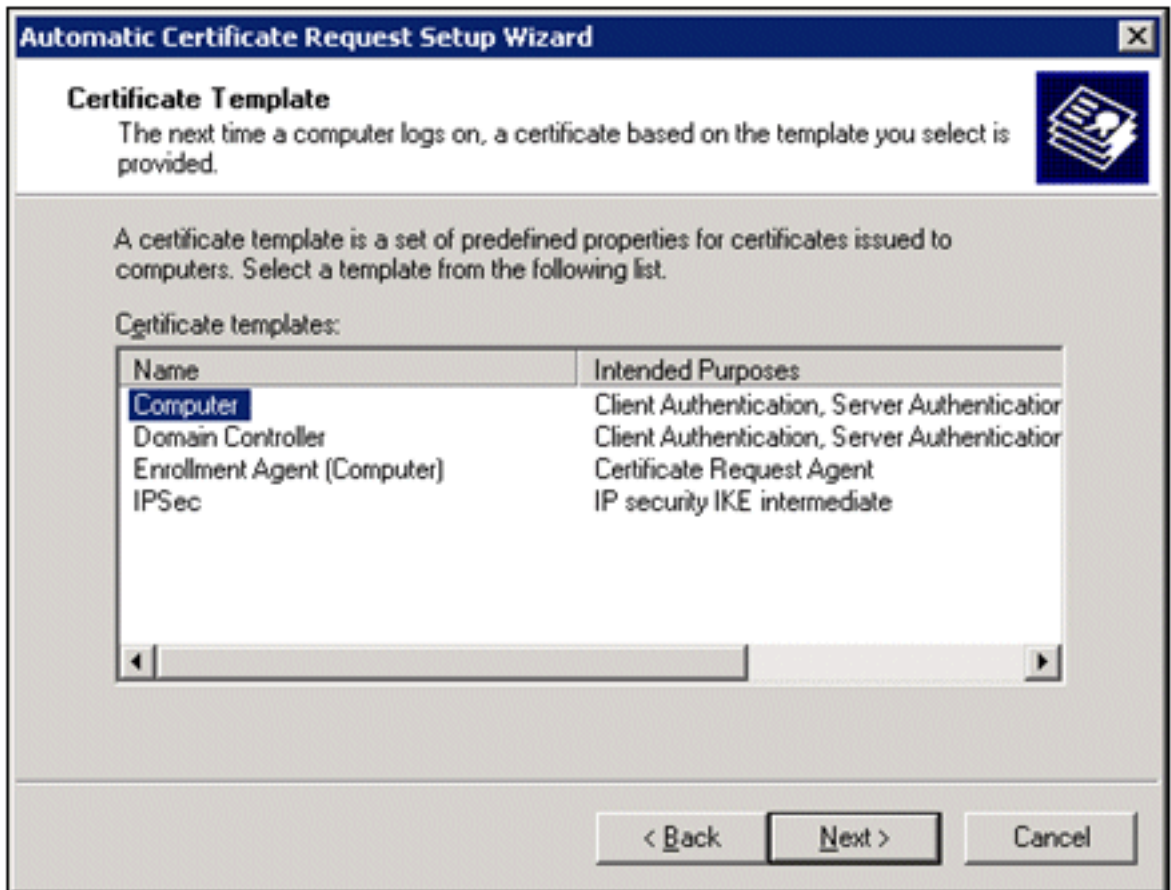
gruppo.

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



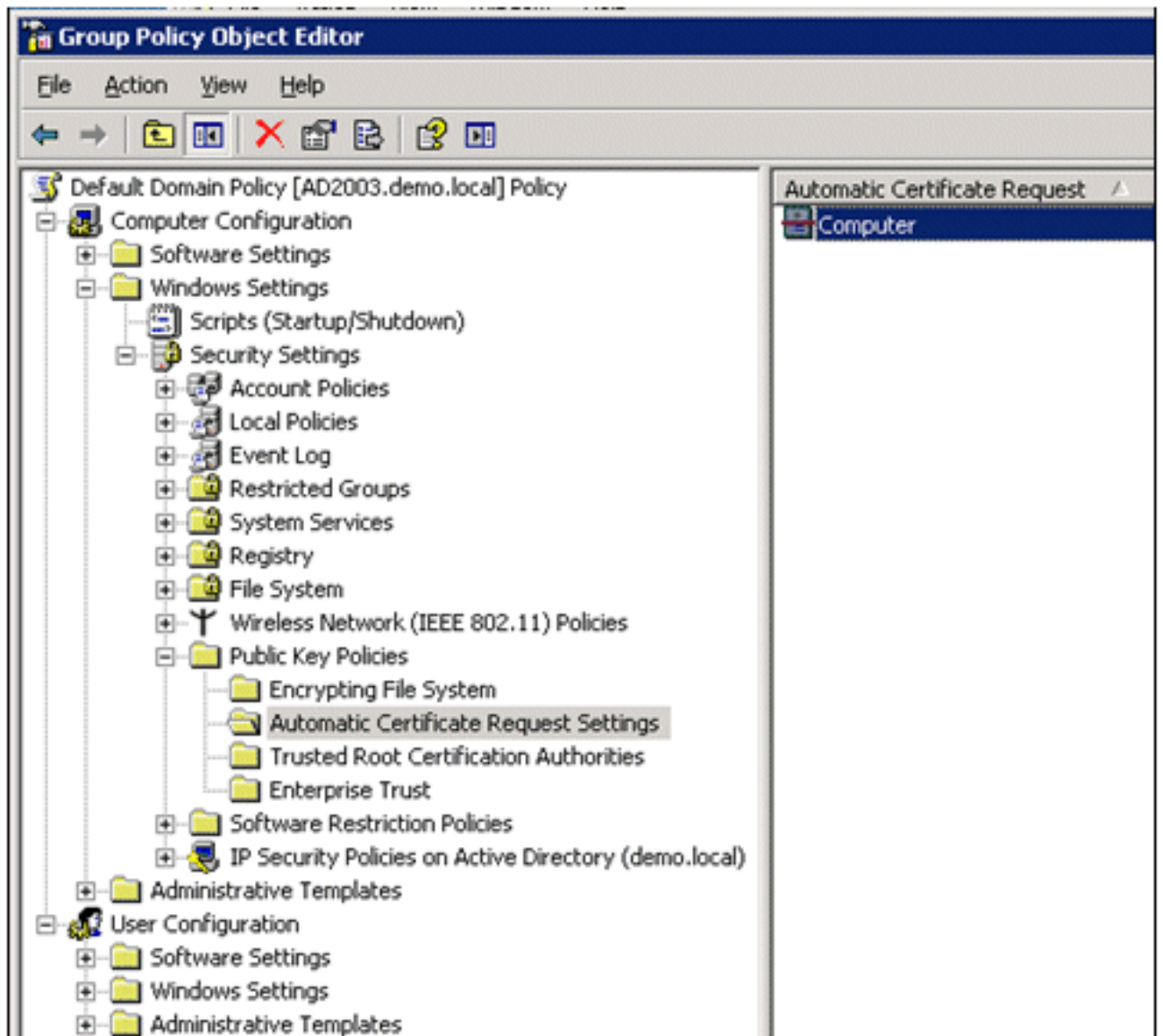
9. Fare clic con il pulsante destro del mouse su **Impostazioni richiesta automatica certificati**, quindi scegliere **Nuovo > Richiesta automatica certificati**.
10. Nella pagina Installazione guidata richiesta automatica certificati fare clic su **Avanti**.
11. Nella pagina Modello di certificato fare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



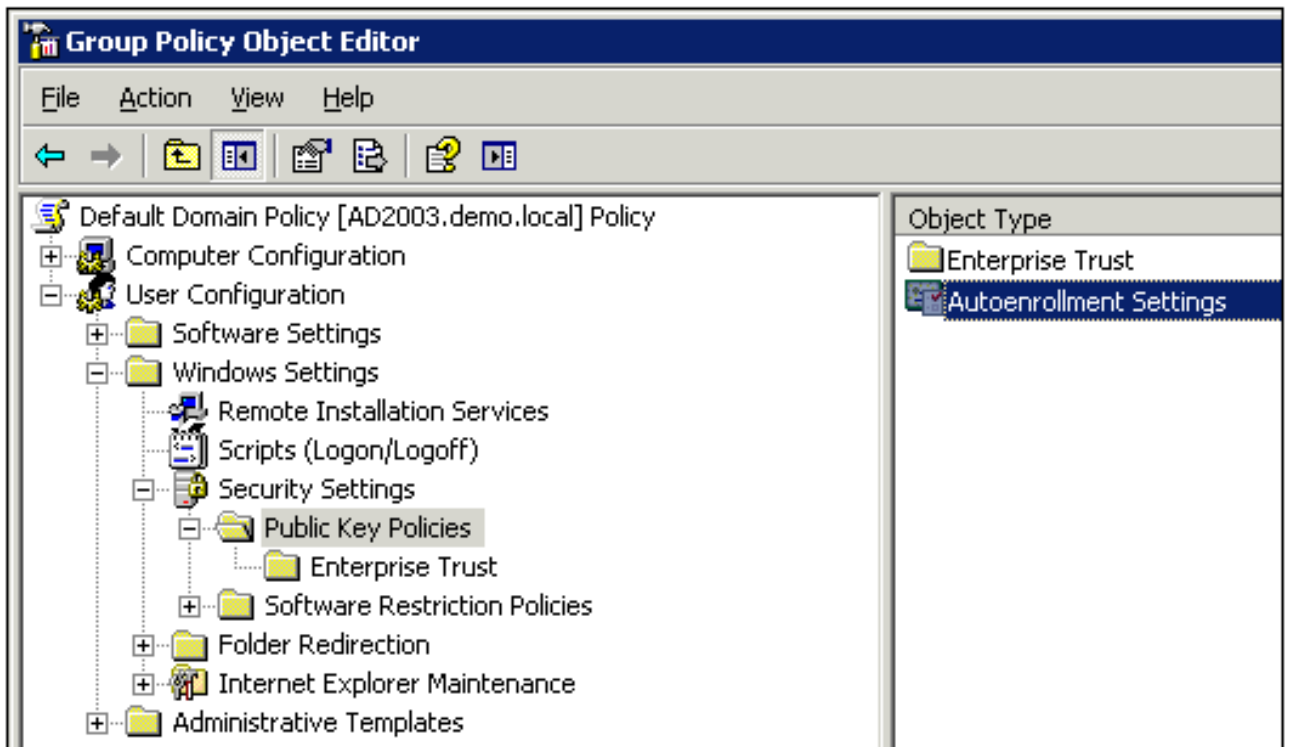


**Avanti.**

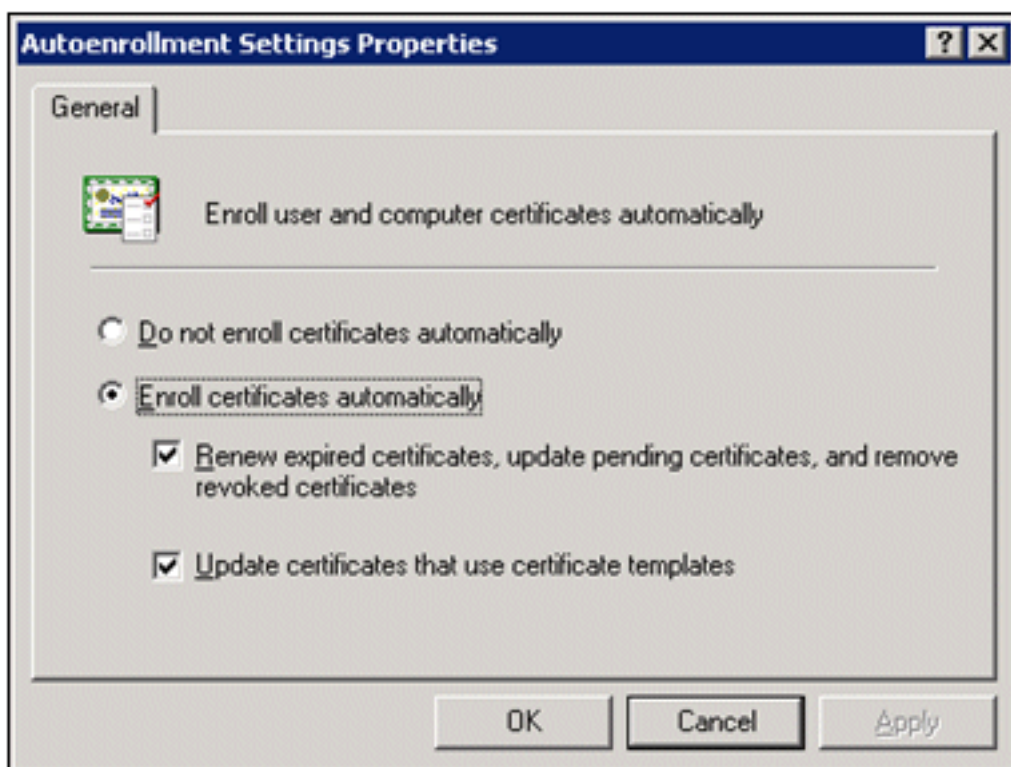
12. Al termine dell'installazione guidata richiesta automatica certificati, fare clic su **Fine**. Il tipo di certificato Computer verrà visualizzato nel riquadro dei dettagli dello snap-in Editor oggetti Criteri di gruppo.



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**.

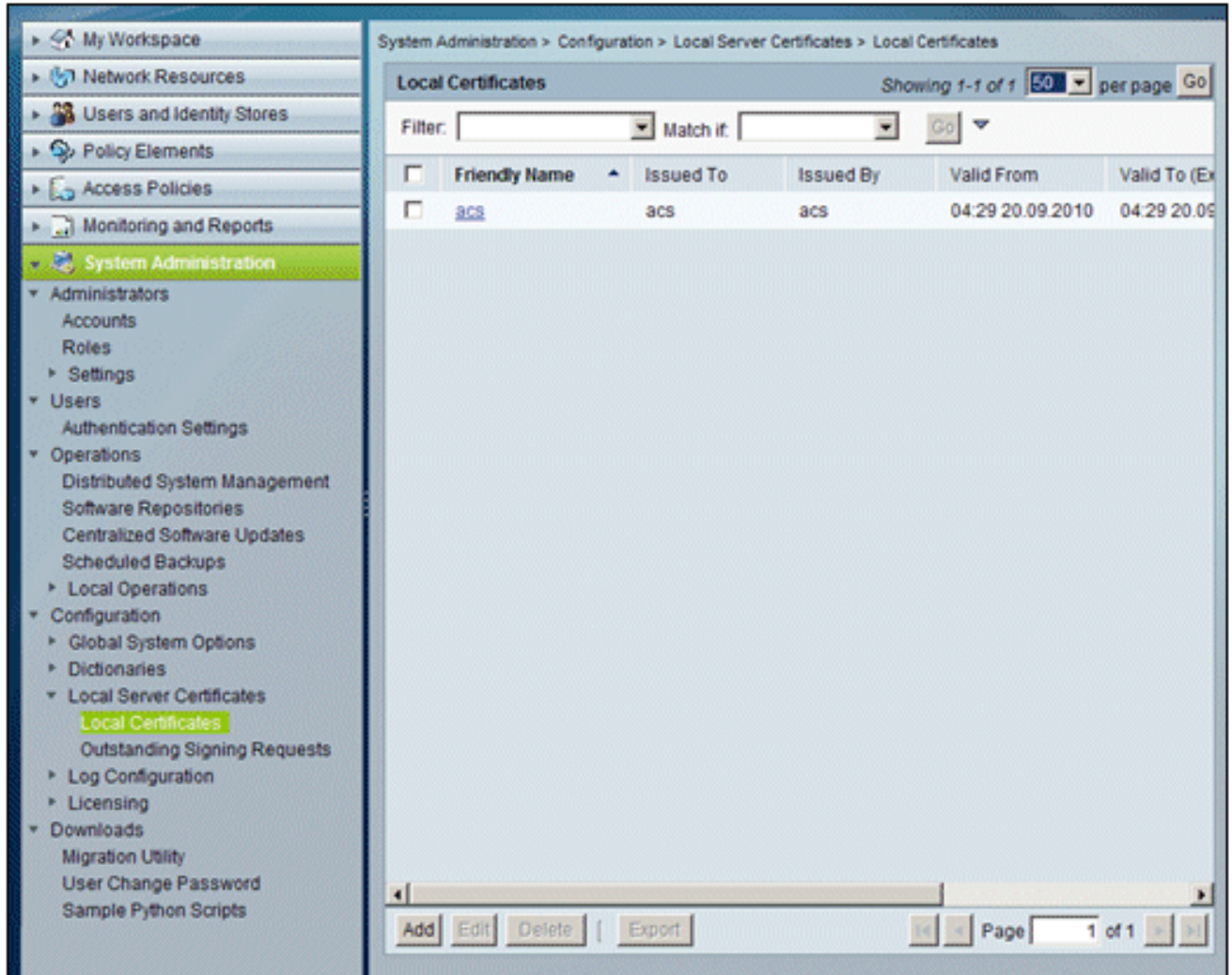
## [Configurazione certificato ACS 5.1](#)

### [Configura certificato esportabile per ACS](#)

**Nota:** per autenticare un client PEAP WLAN, il server ACS deve ottenere un certificato server dal server CA radice dell'organizzazione (enterprise).

**Nota:** verificare che Gestione IIS non sia aperto durante il processo di installazione del certificato perché causa problemi con le informazioni memorizzate nella cache.

1. Accedere al server ACS con diritti di amministratore di account.
2. Selezionare **Amministrazione sistema > Configurazione > Certificati server locale**. Fare clic su **Add**.



3. Quando si sceglie un metodo per la creazione di un certificato server, scegliere **Genera richiesta di firma del certificato**. Fare clic su **Next** (Avanti).

Cisco Secure ACS  
NFR(Days left: 296)

acsadmin acs (Primary) Log Out About Help

My Workspace  
Network Resources  
Users and Identity Stores  
Policy Elements  
Access Policies  
Monitoring and Reports  
System Administration  
Administrators  
Accounts  
Roles  
Settings  
Users  
Authentication Settings  
Operations  
Distributed System Management  
Software Repositories  
Centralized Software Updates  
Scheduled Backups  
Local Operations  
Configuration  
Global System Options  
Dictionaries  
Local Server Certificates  
Local Certificates  
Outstanding Signing Requests  
Log Configuration  
Licensing  
Downloads  
Migration Utility  
User Change Password  
Sample Python Scripts

System Administration > Configuration > Local Server Certificates > Local Certificates > Create

Select server certificate creation method

### Step 1 - Select server certificate creation method

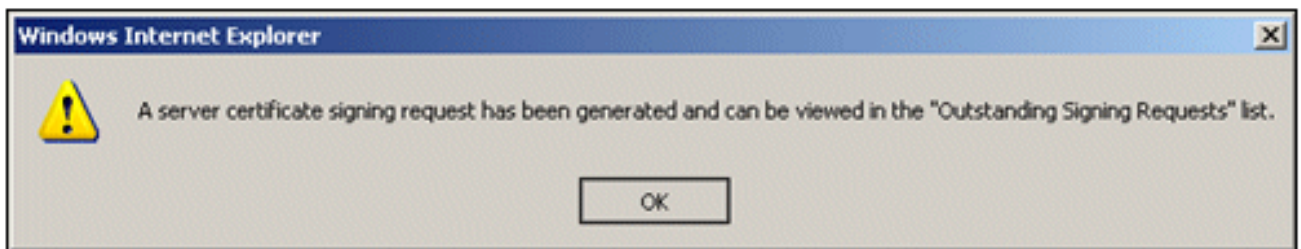
- Import Server Certificate  
Use this option if you have a Server Certificate file and corresponding private key file (and password, if the private key file is encrypted).
- Generate Self Signed Certificate  
Use this option to have the ACS server generate a Self-Signed Certificate.
- Generate Certificate Signing Request  
Use this option to have the ACS server generate a certificate signing request to present to your local Certificate Authority. Once you have generated the signing request, go to the "Outstanding Signing Requests" list, select the signing request, and export a copy of the signing request (save a copy on your client system). Once you receive a certificate from your CA, you will use the "Bind CA Signed Certificate" option below to install it.
- Bind CA Signed Certificate  
After using the previous option to generate a certificate signing request, this option is used to bind/install the certificate received from your CA. ACS will automatically match the certificate with the appropriate outstanding signing request.

Back Next Cancel

4. Immettere l'oggetto del certificato e la lunghezza della chiave, quindi fare clic su Fine: Oggetto certificato - CN=acs.demo.local Lunghezza chiave - 1024

The screenshot shows the Cisco Secure ACS web interface. The top navigation bar includes the Cisco logo, 'Cisco Secure ACS', 'NFR(Days left: 296)', and user information 'acsadmin', 'acs (Primary)', and 'Log Out'. The left sidebar contains a navigation menu with categories like 'My Workspace', 'Network Resources', 'Users and Identity Stores', 'Policy Elements', 'Access Policies', 'Monitoring and Reports', and 'System Administration'. The 'System Administration' menu is expanded, showing sub-items like 'Administrators', 'Users', 'Operations', 'Configuration', and 'Local Server Certificates'. The 'Local Certificates' sub-item is highlighted. The main content area shows the breadcrumb 'System Administration > Configuration > Local Server Certificates > Local Certificates > Create'. Below this, there is a radio button selection for 'Generate Certificate Signing Request'. The 'Step 2 -Generate Certificate Signing Request' section contains a 'Certificate Subject' field with the value 'CN=acs.demo.local', a 'Key Length' dropdown menu set to '1024', and a 'Digest to Sign with' field set to 'SHA1'. At the bottom right of the main content area, there are 'Back' and 'Finish' buttons.

5. ACS richiederà di generare una richiesta di firma del certificato. Fare clic su OK.



6. In Amministrazione sistema, passare a **Configurazione > Certificati server locale > Richieste di firma in attesa**. **Nota:** 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.

Cisco Secure ACS  
NFR(Days left: 296)

acsadmin acs (Primary) Log Out About Help

System Administration > Configuration > Local Server Certificates > Outstanding Signing Requests

Certificate Signing Request Showing 1-1 of 1 50 per page Go

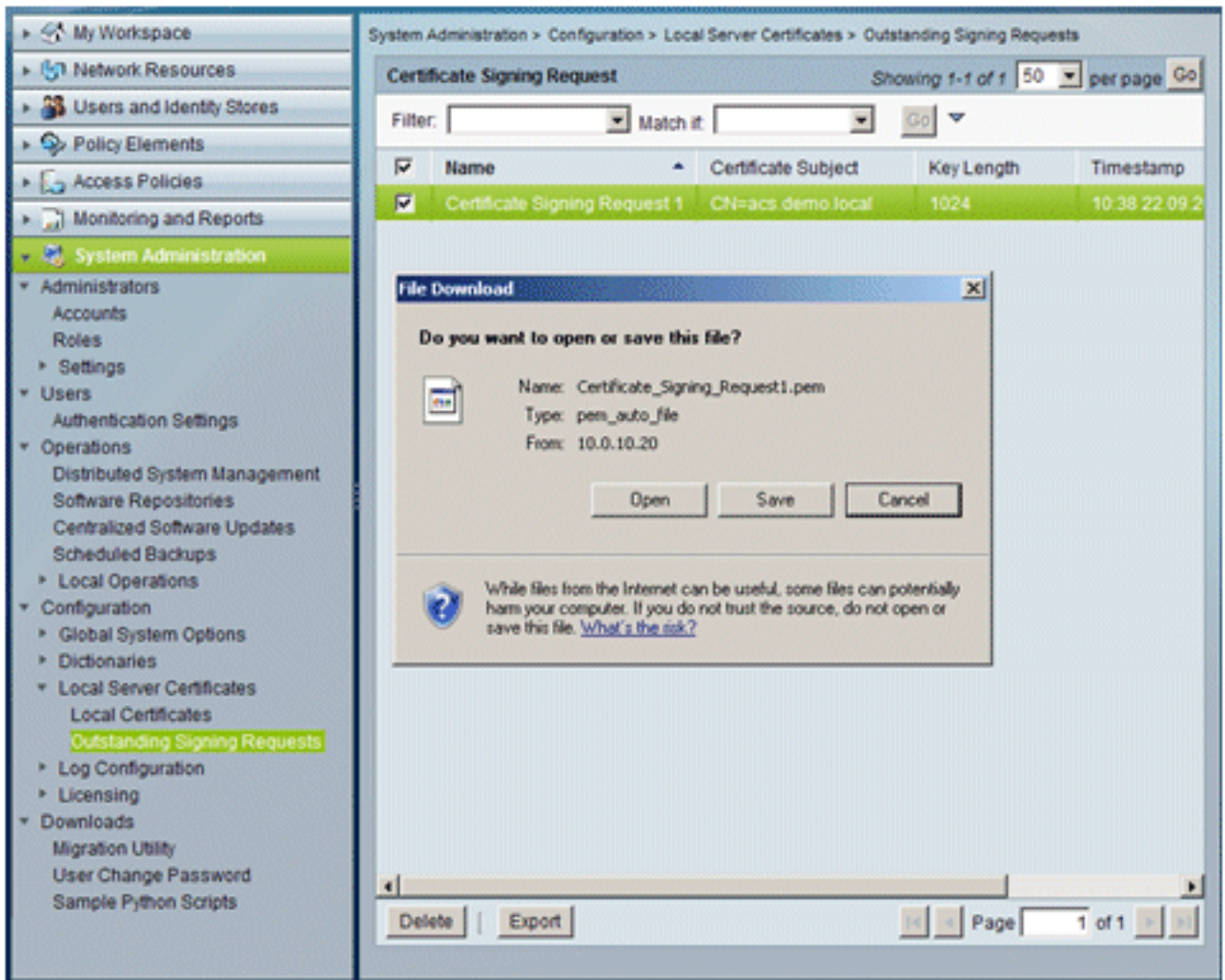
Filter: Match if: Go

<input type="checkbox"/>	Name	Certificate Subject	Key Length	Timestamp
<input type="checkbox"/>	Certificate Signing Request 1	CN=acs.demo.local	1024	10:38 22.09.2

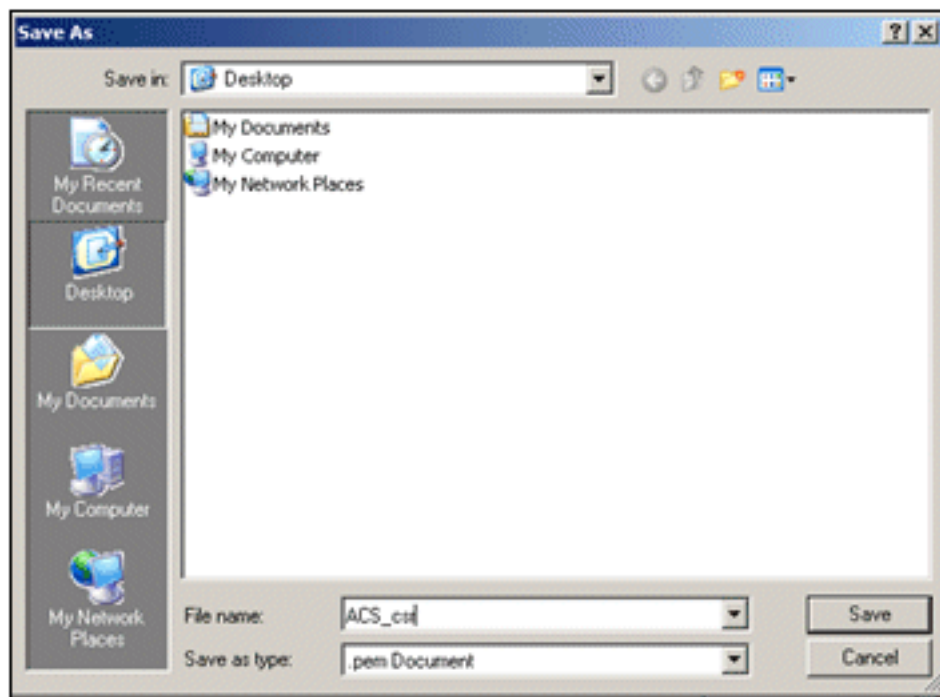
multiple row selection

Delete | Export Page 1 of 1

7. Scegliere la voce **Richiesta di firma del certificato** e fare clic su **Esporta**.



8. Salvare il file .pem del certificato ACS sul



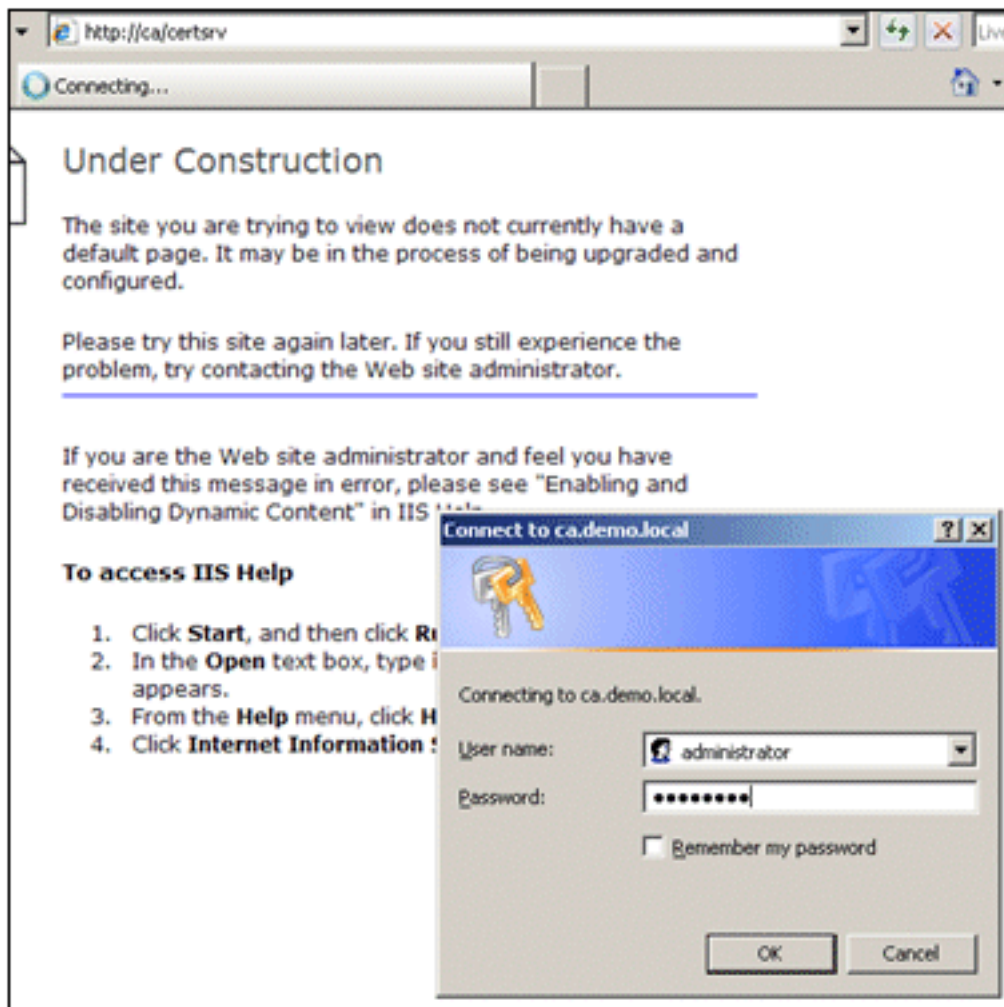
desktop.

## [Installare il certificato nel software ACS 5.1](#)

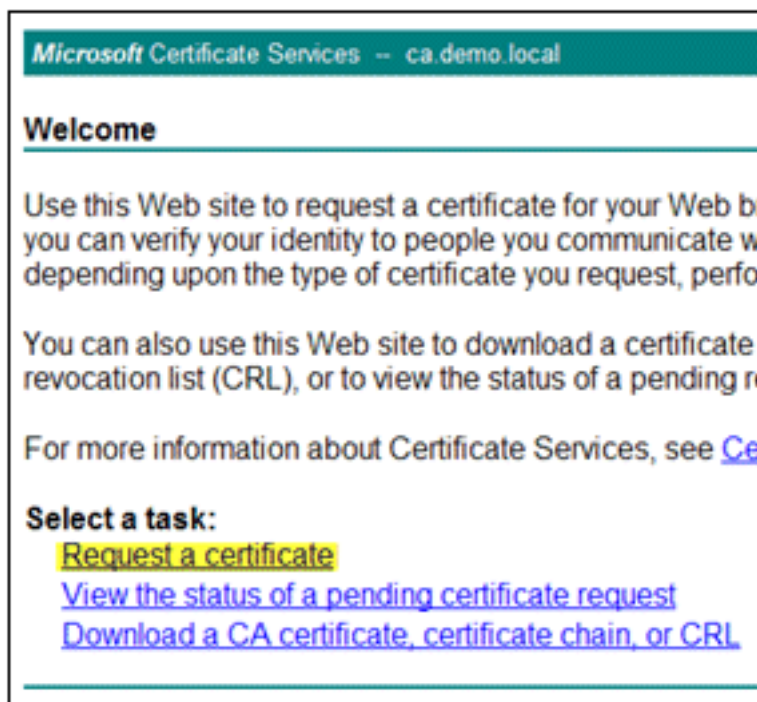
Attenersi alla procedura seguente:



1. Aprire un browser e connettersi all'URL del server CA <http://10.0.10.10/certsrv>.

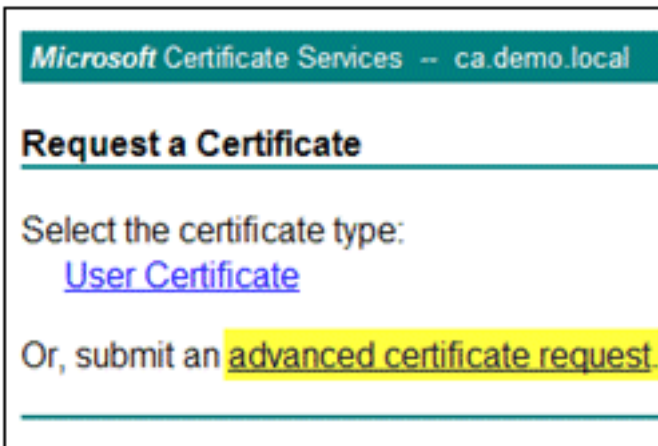


2. Verrà visualizzata la finestra Servizi certificati Microsoft. Scegliere **Richiedi**



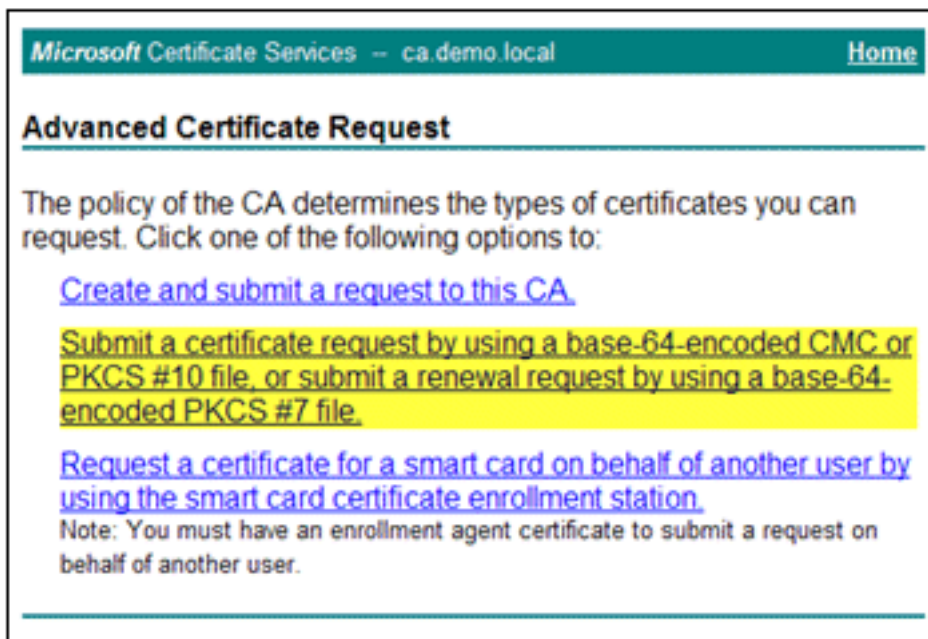
certificato.

3. Fare clic per inviare una **richiesta di certificato**



avanzata.

4. Nella richiesta avanzata, fare clic su **Invia una richiesta di certificato utilizzando una codifica**



in base 64...

5. Nel campo Richiesta salvata, se la protezione del browser lo consente, individuare il file di richiesta del certificato ACS precedente e

Microsoft Certificate Services -- ca.demo.local Home

---

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

[Browse for a file to insert.](#)

**Certificate Template:**

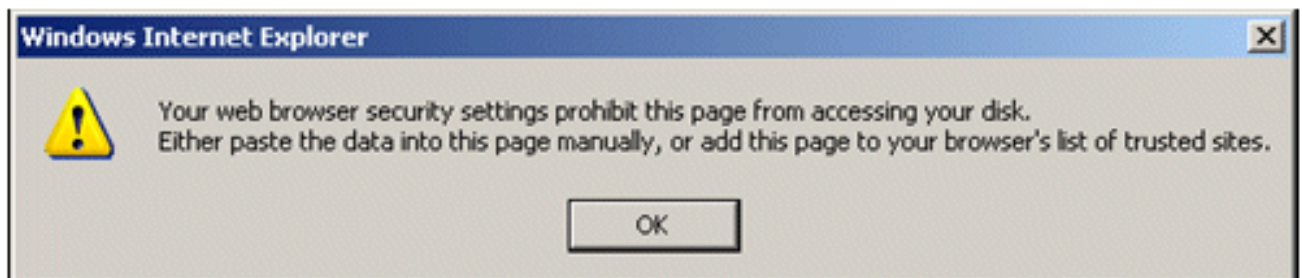
Administrator

**Additional Attributes:**

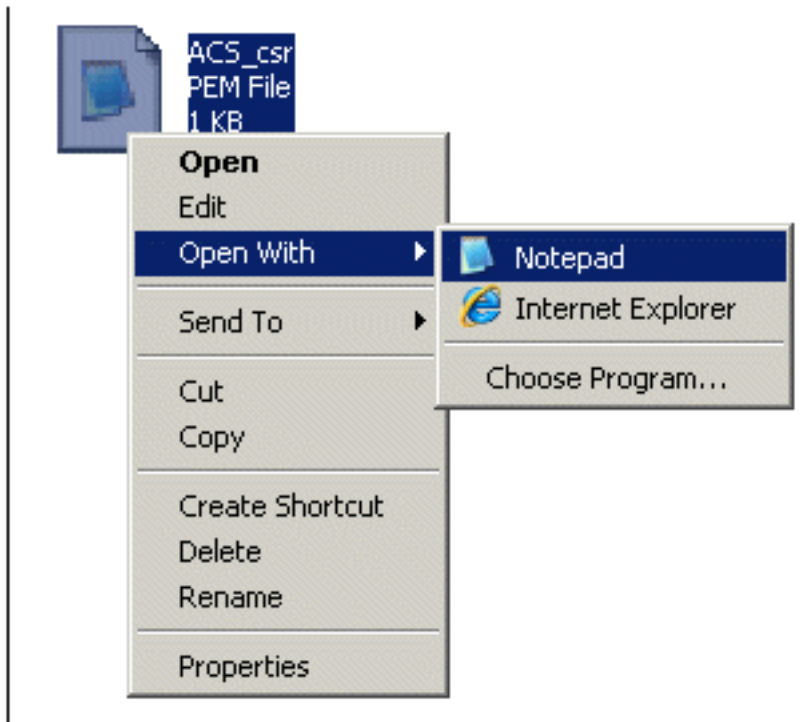
Attributes:

inserirlo.

6. Le impostazioni di protezione del browser potrebbero non consentire l'accesso al file su disco. In tal caso, fare clic su **OK** per eseguire un'operazione Incolla manuale.

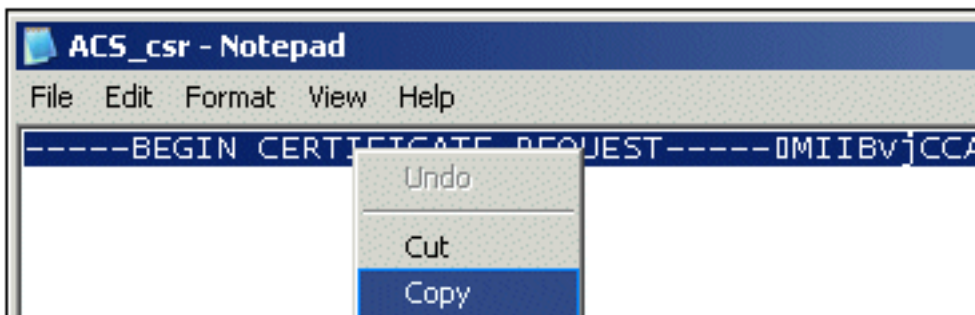


7. Individuare il file ACS \*.pem della precedente esportazione ACS. Aprire il file utilizzando un editor di testo, ad esempio Blocco



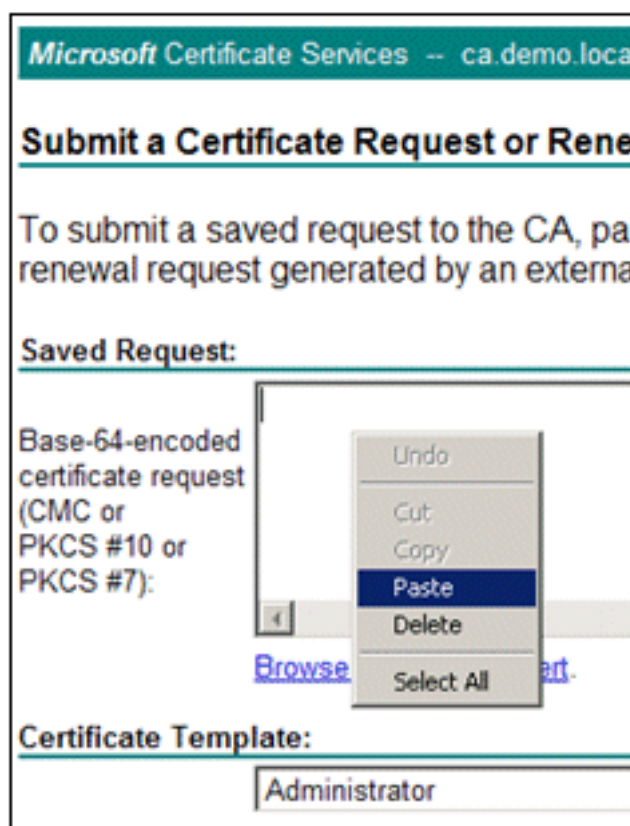
note.

8. Evidenziare l'intero contenuto del file e fare clic su



Copia.

9. Tornare alla finestra Richiesta certificato Microsoft. **Incollare** il contenuto copiato nel campo



Richiesta salvata.

10. Scegliere **ACS** come modello di certificato e fare clic su

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
YI2IAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUA...
-----END CERTIFICATE REQUEST-----
```

[Browse for a file to insert.](#)

**Certificate Template:**

ACS

**Additional Attributes:**

Attributes:

Submit >

Invia.

11. Una volta rilasciato il certificato, scegliere **Codifica Base 64** e fare clic su **Scarica**

Microsoft Certificate Services - ca demo.local

**Certificate Issued**

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

[Download certificate](#)

[Download certificate chain](#)

**File Download - Security Warning**

Do you want to open or save this file?

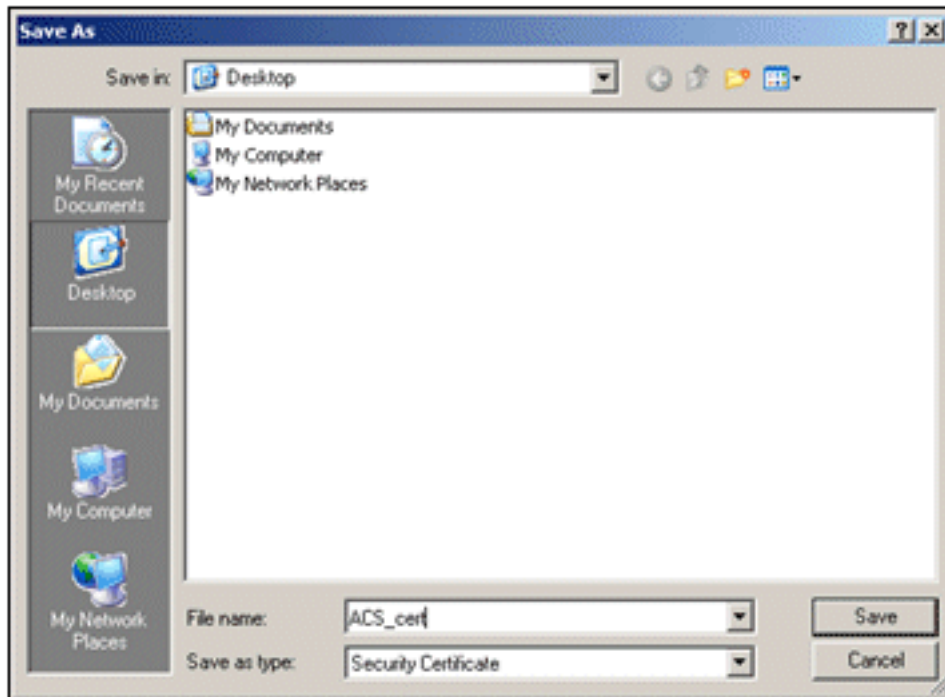
Name: certnew.cer  
Type: Security Certificate, 1.88KB  
From: ca

Open Save Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. [What's the risk?](#)

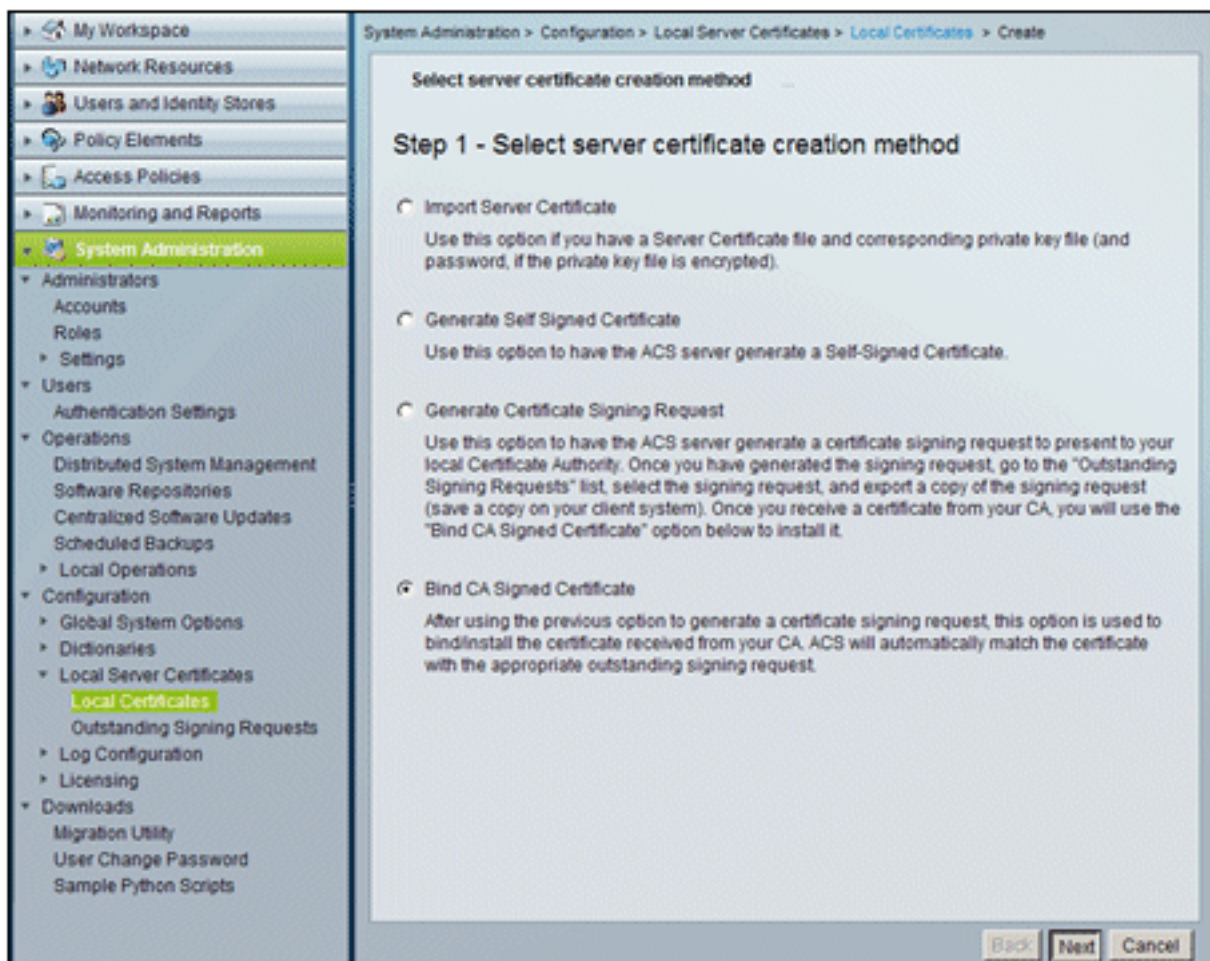
certificato.

12. Per salvare il certificato sul desktop, fare clic su **Save**

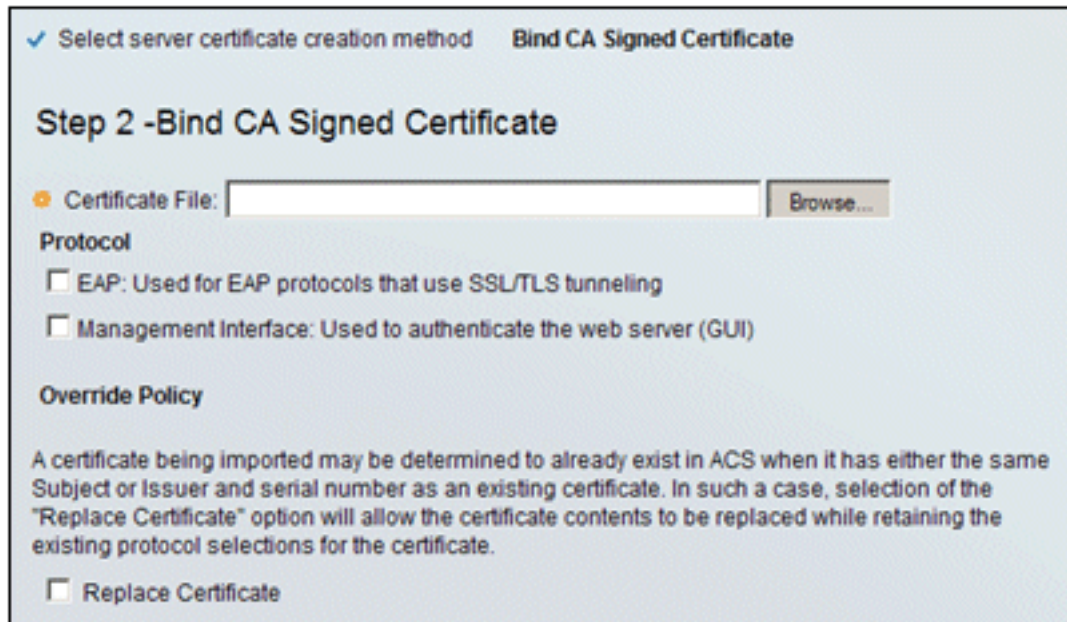


(Salva).

- Selezionare **ACS > System Administration > Configuration > Local Server Certificates** (ACS > Amministrazione sistema > Configurazione > Certificati server locale). Scegliere **Associa certificato firmato CA**, quindi fare clic su **Avanti**.

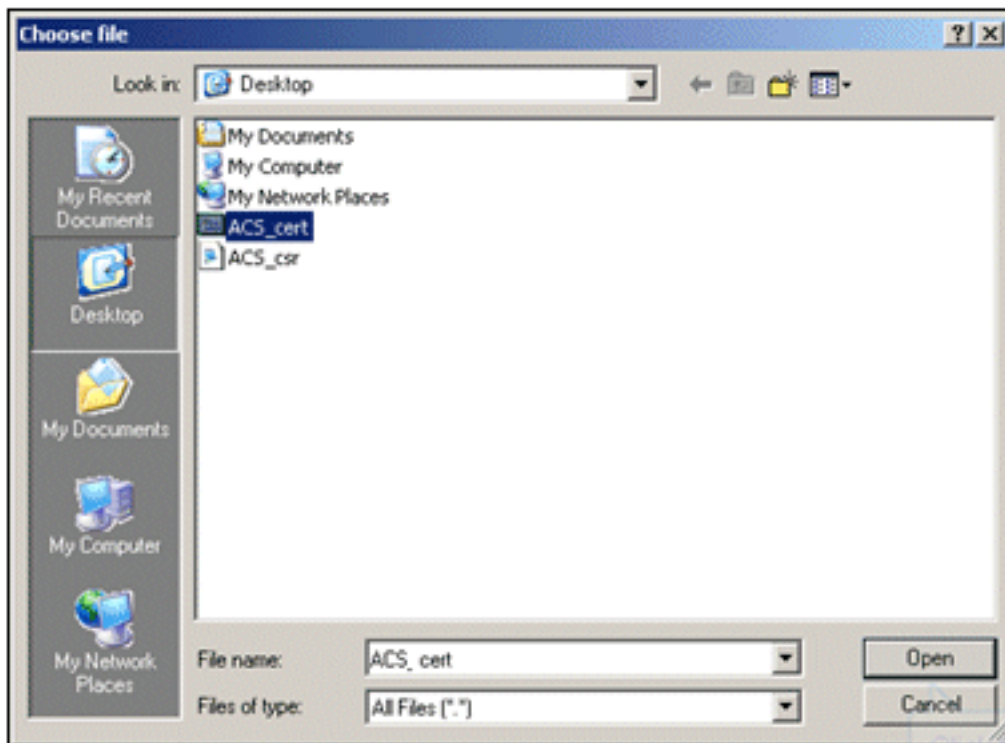


- Fare clic su **Sfoggia** e individuare il certificato



salvato.

15. Scegliere il certificato ACS emesso dal server CA e fare clic su



Apri.

16. Selezionare inoltre la casella Protocollo per **EAP** e fare clic su

System Administration > Configuration > Local Server Certificates > Local Certificates > Create

✓ Select server certificate creation method **Bind CA Signed Certificate**

### Step 2 -Bind CA Signed Certificate

Certificate File:

**Protocol**

EAP: Used for EAP protocols that use SSL/TLS tunneling  
 Management Interface: Used to authenticate the web server (GUI)

**Override Policy**

A certificate being imported may be determined to already exist in ACS when it has either the same Subject or Issuer and serial number as an existing certificate. In such a case, selection of the "Replace Certificate" option will allow the certificate contents to be replaced while retaining the existing protocol selections for the certificate.

Replace Certificate

Fine.

17. Il certificato ACS rilasciato dalla CA verrà visualizzato nel certificato locale ACS.

System Administration > Configuration > Local Server Certificates > Local Certificates

**Local Certificates** Showing 1-2 of 2

Filter:  Match if:

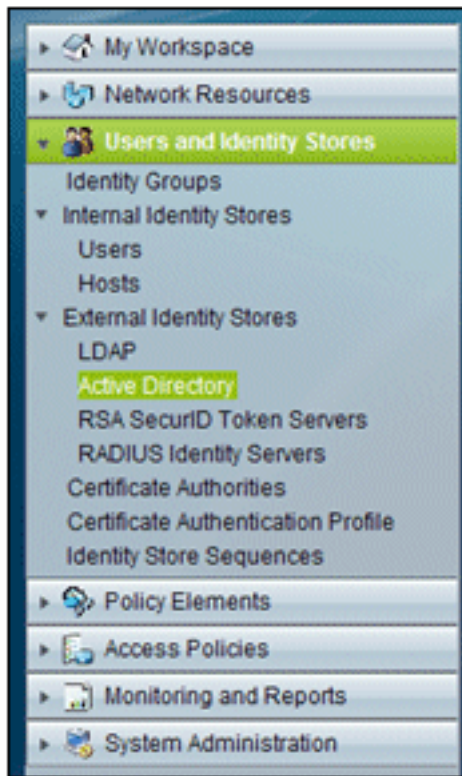
<input type="checkbox"/>	Friendly Name	Issued To	Issued By	Valid From
<input type="checkbox"/>	<a href="#">acs</a>	acs	acs	04:29 20.09.2010
<input checked="" type="checkbox"/>	<a href="#">acs.demo.local</a>	acs.demo.local	ca.demo.local	10:39 22.09.2010

## [Configura archivio identità ACS per Active Directory](#)

Attenersi alla procedura seguente:

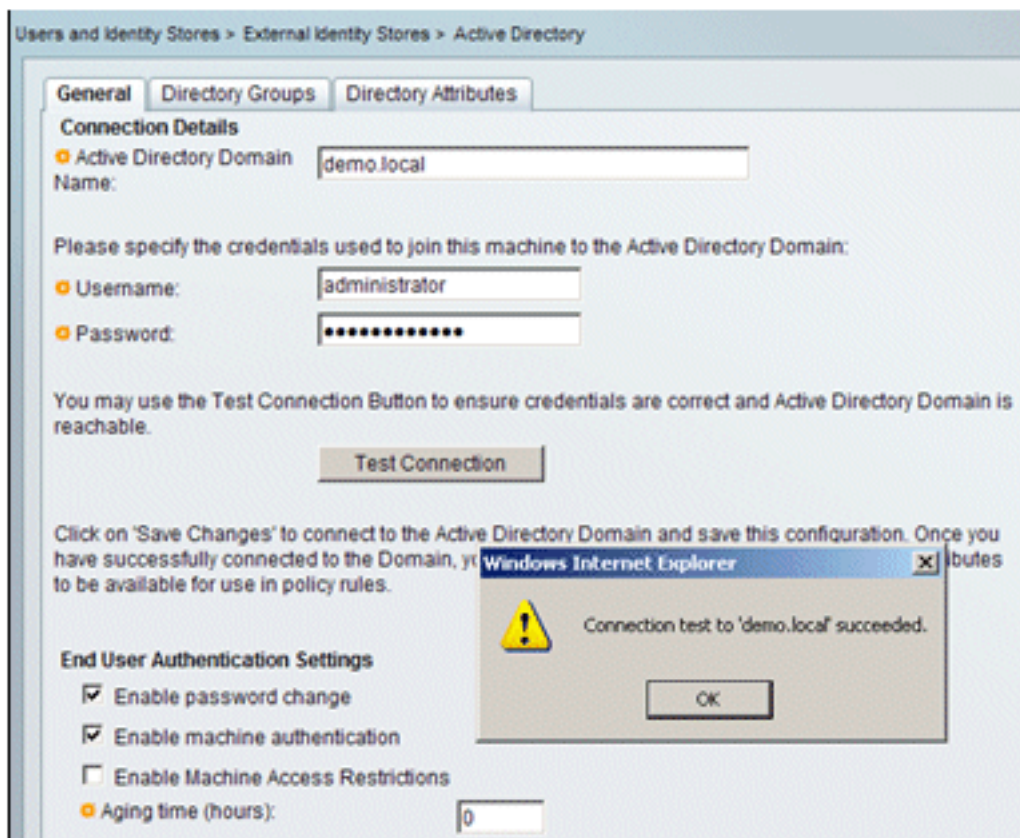
1. Connettersi ad ACS ed eseguire l'accesso con l'account Admin.
2. Passare a **Utenti e archivi identità > Archivi identità esterni > Active**





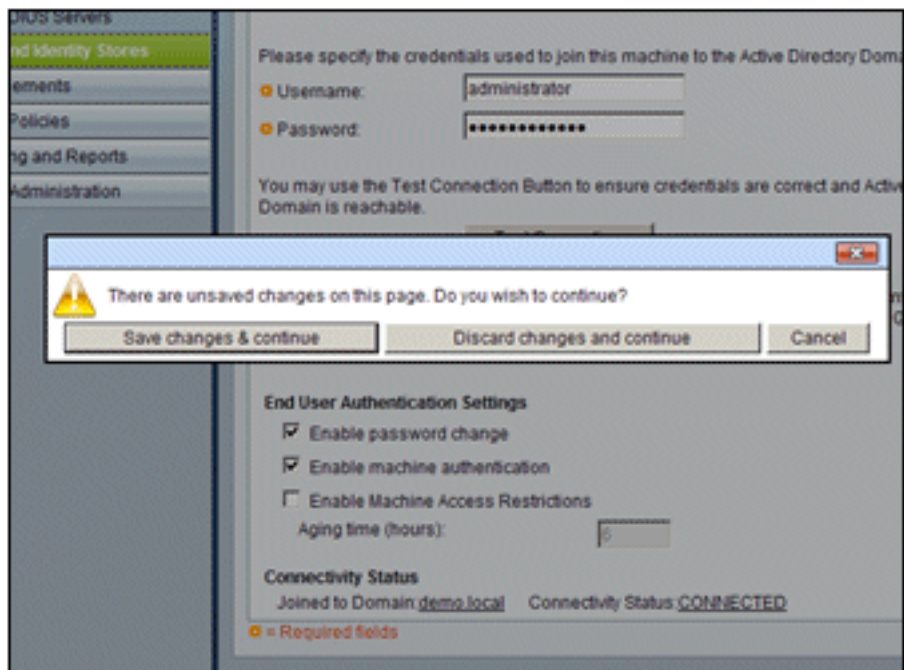
Directory.

3. Immettere il dominio Active Directory *demo.local*, immettere la password del server e fare clic su **Test connessione**. Per continuare, fare clic su



OK.

4. Fare clic su **Salva**



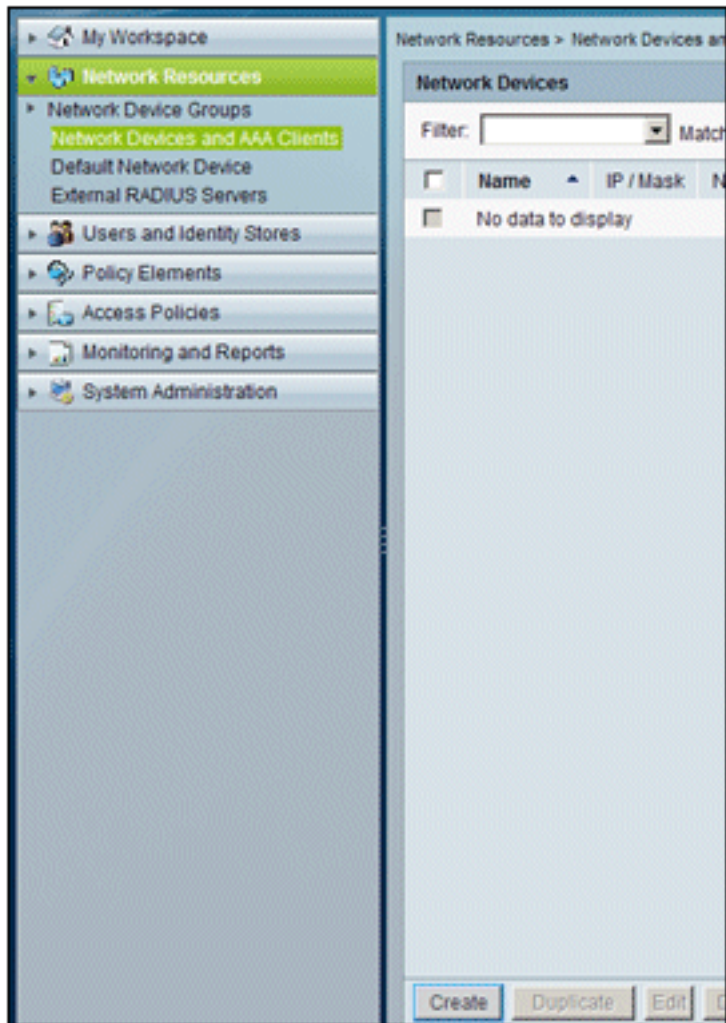
modifiche.

**Nota:** per ulteriori informazioni sulla procedura di integrazione di ACS 5.x, vedere [Esempio di integrazione con Microsoft Active Directory in ACS 5.x e versioni successive](#).

## Aggiunta di un controller ad ACS come client AAA

Attenersi alla procedura seguente:

1. Connettersi ad ACS e selezionare **Risorse di rete > Dispositivi di rete e client AAA**. Fare clic



su Crea.

2. Immettere quanto segue nei campi:  
Name - wlclP - 10.0.1.10  
Casella di controllo RADIUS -  
Selezionata  
Segreto condiviso -

Network Resources > Network Devices and AAA Clients > Create

Name:  Description:

Network Device Groups

Location:

Device Type:

IP Address

Single IP Address  IP Range (s)

IP:

Authentication Options

TACACS+

Shared Secret:

Single Connect Device

Legacy TACACS+ Single Connect Support

TACACS+ Draft Compliant Single Connect Support

RADIUS

Shared Secret:

TrustSec

Use Device ID for TrustSec Identification

Device ID:

Password:

= Required fields

cisco

3. Al termine, fare clic su **Invia**. Il controller verrà visualizzato come voce nell'elenco Periferiche di rete ACS.

Network Resources > Network Devices and AAA Clients

Network Devices Showing 1-1 of 1

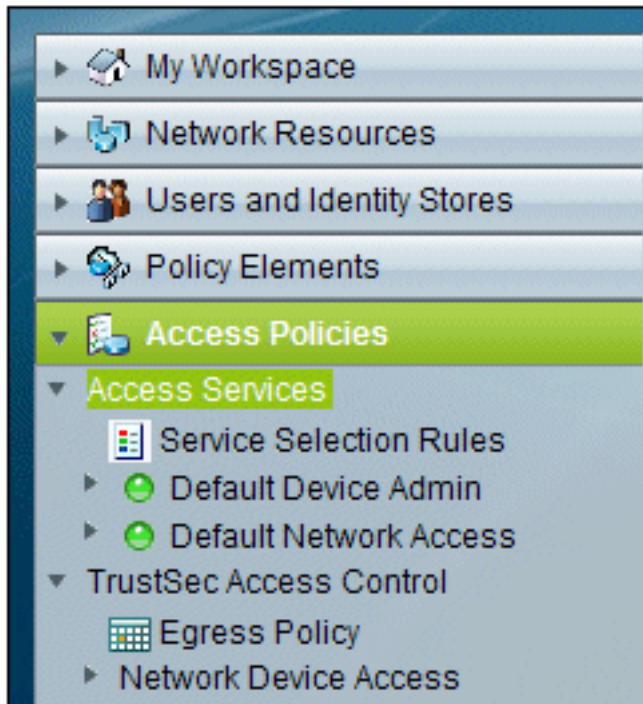
Filter:  Match if:

<input type="checkbox"/>	Name	IP / Mask	NDG:Location	NDG:Device Type
<input type="checkbox"/>	<a href="#">wlc</a>	10.0.1.10/32	All Locations	All Device Types

## [Configurazione dei criteri di accesso ACS per reti wireless](#)

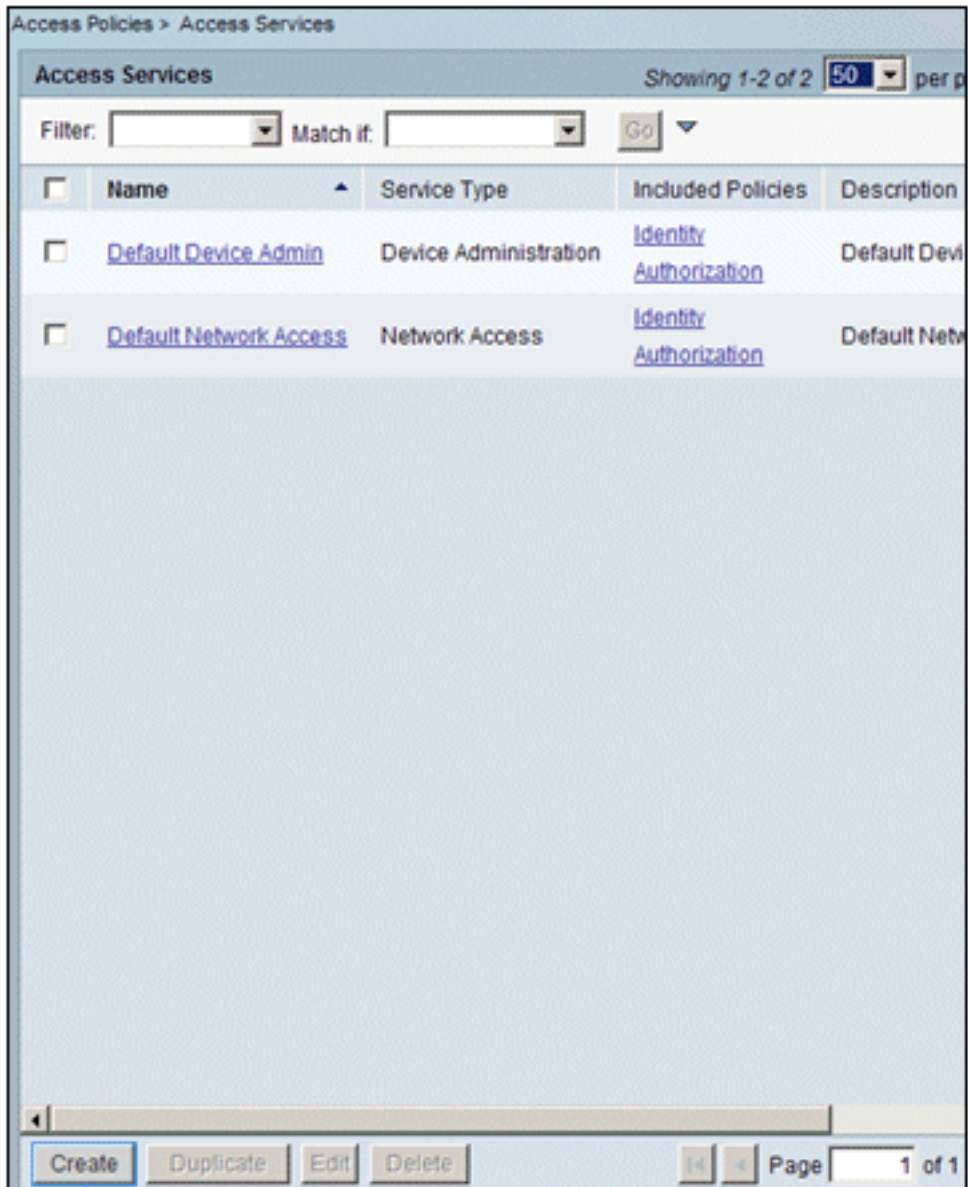
Attenersi alla procedura seguente:

1. In ACS, selezionare **Access Policies > Access Services** (Policy di accesso > Servizi di



accesso).

2. Nella finestra Servizi di Access fare clic su



Crea.

3. Creare un servizio di accesso e immettere un nome, ad esempio WirelessAD. Scegliere

Basato sul modello di servizio, quindi fare clic su

Access Policies > Access Services > Create

General Allowed Protocols

### Step 1 - General

General

Name:

Description:

Access Service Policy Structure

Based on service template

Based on existing service

User Selected Service Type

Seleziona.

4. Nella finestra di dialogo della pagina Web, scegliere **Accesso di rete - Semplice**. Fare clic su OK.

Cisco Secure ACS -- Webpage Dialog

Access Services Showing 1-4 c

Filter:  Match it:

Name	Service Type	Description
<input type="radio"/> Device Admin - Command Auth	Device Administration	
<input type="radio"/> Device Admin - Simple	Device Administration	
<input type="radio"/> Network Access - MAC Authentication Bypass	Network Access	
<input checked="" type="radio"/> Network Access - Simple	Network Access	

5. Nella finestra di dialogo della pagina Web, scegliere **Accesso di rete - Semplice**. Fare clic su OK. Dopo aver selezionato il modello, fare clic su

Step 1 - General

General

Name:

Description:

Access Service Policy Structure

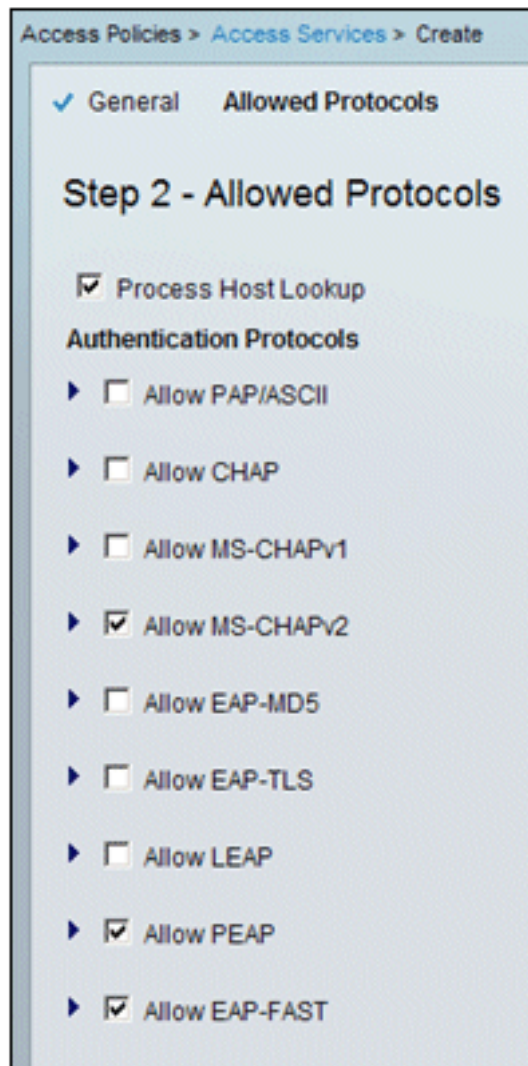
Based on service template

Based on existing service

User Selected Service Type

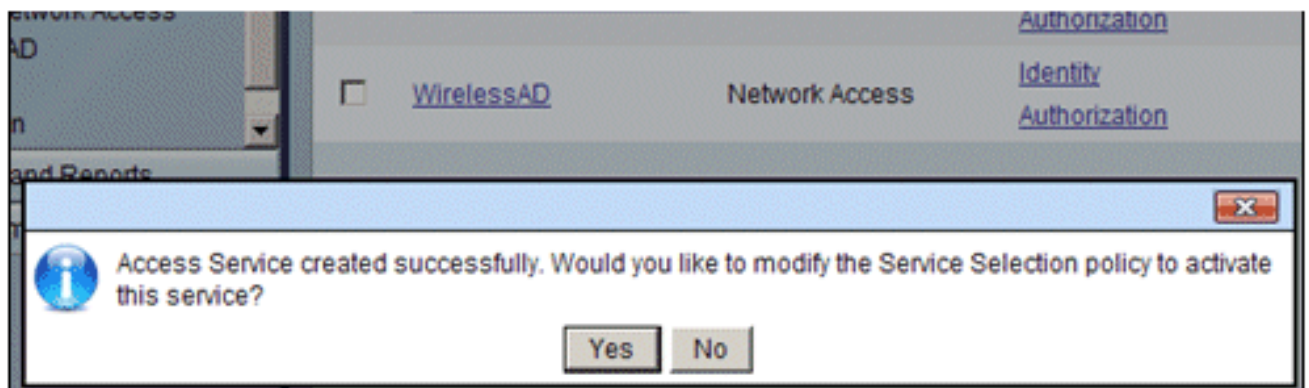
Avanti.

6. In Protocolli consentiti selezionare le caselle **Consenti MS-CHAPv2** e **Consenti PEAP**. Fare

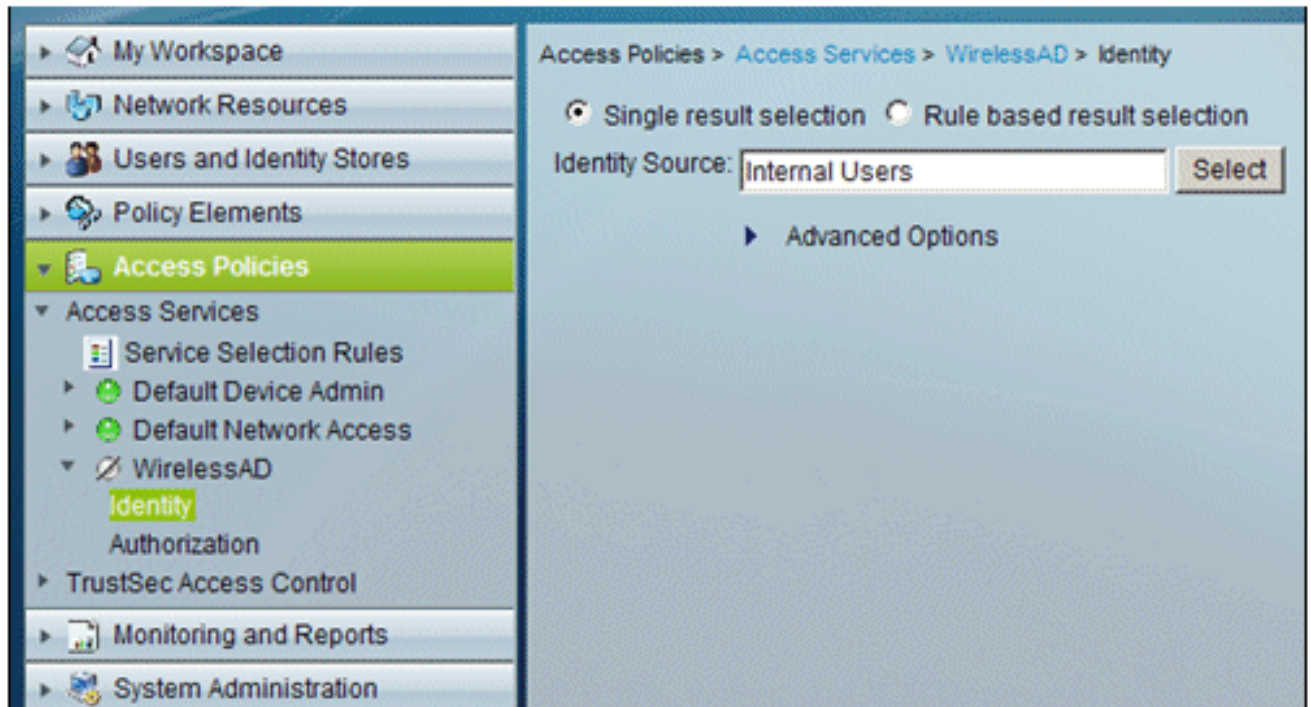


clic su **Finish** (Fine).

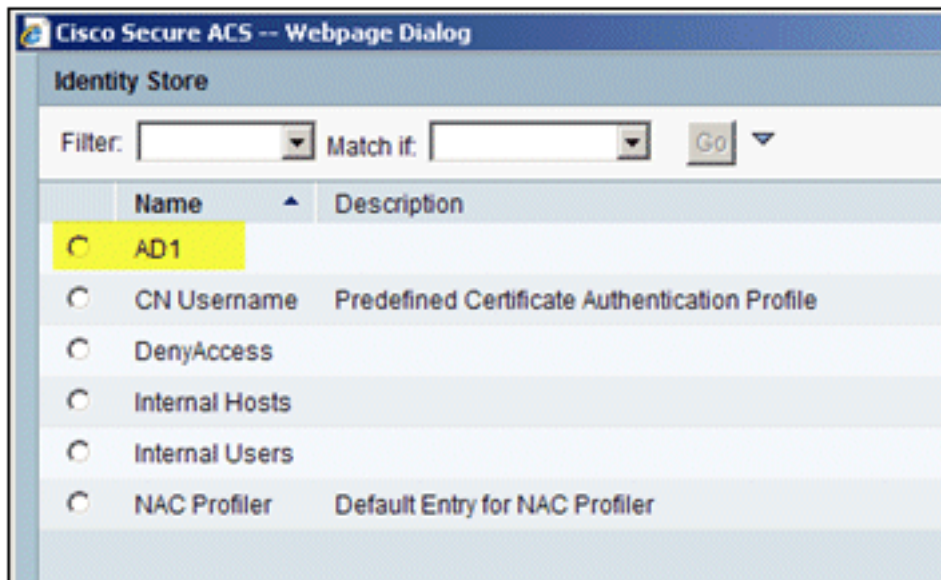
7. Quando ACS chiede di attivare il nuovo servizio, fare clic su **Sì**.



8. Nel nuovo servizio di accesso appena creato/attivato, espandere e scegliere **Identità**. Per Origine identità, fare clic su **Seleziona**.

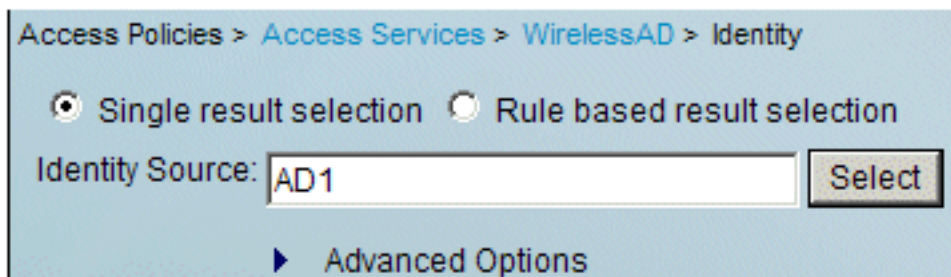


9. Scegliere **AD1** per Active Directory configurato in ACS, quindi fare clic su



OK.

10. Verificare che l'origine dell'identità sia **AD1** e fare clic su **Salva**



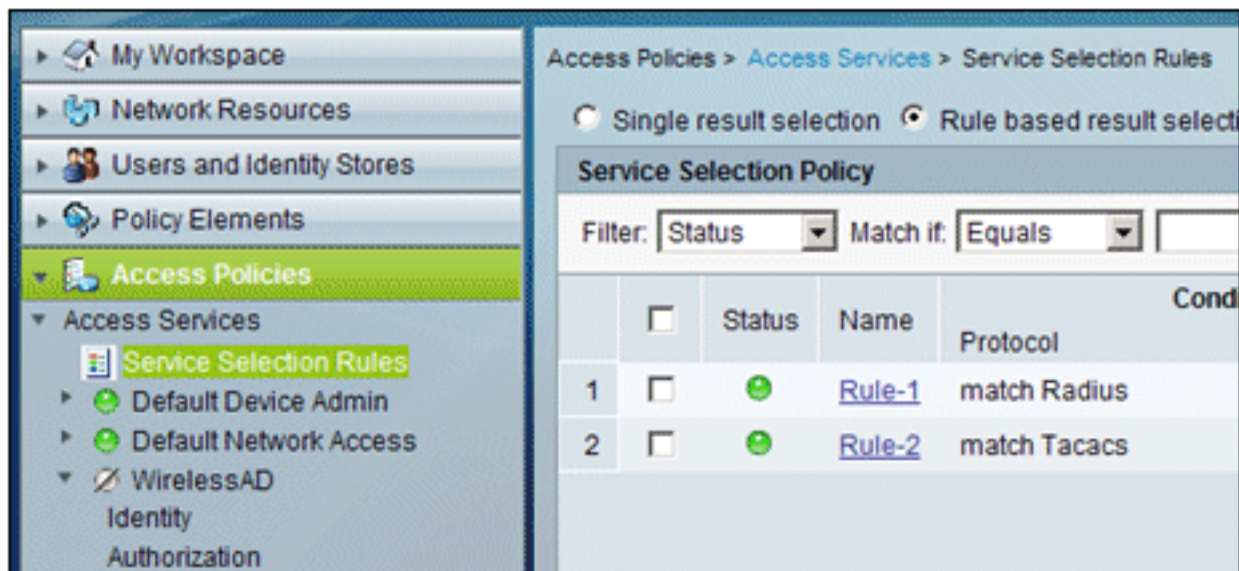
modifiche.

## [Crea regola di servizio e criterio di accesso ACS](#)

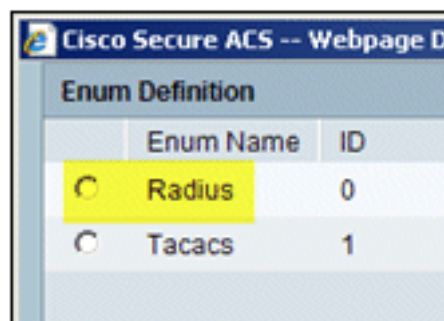
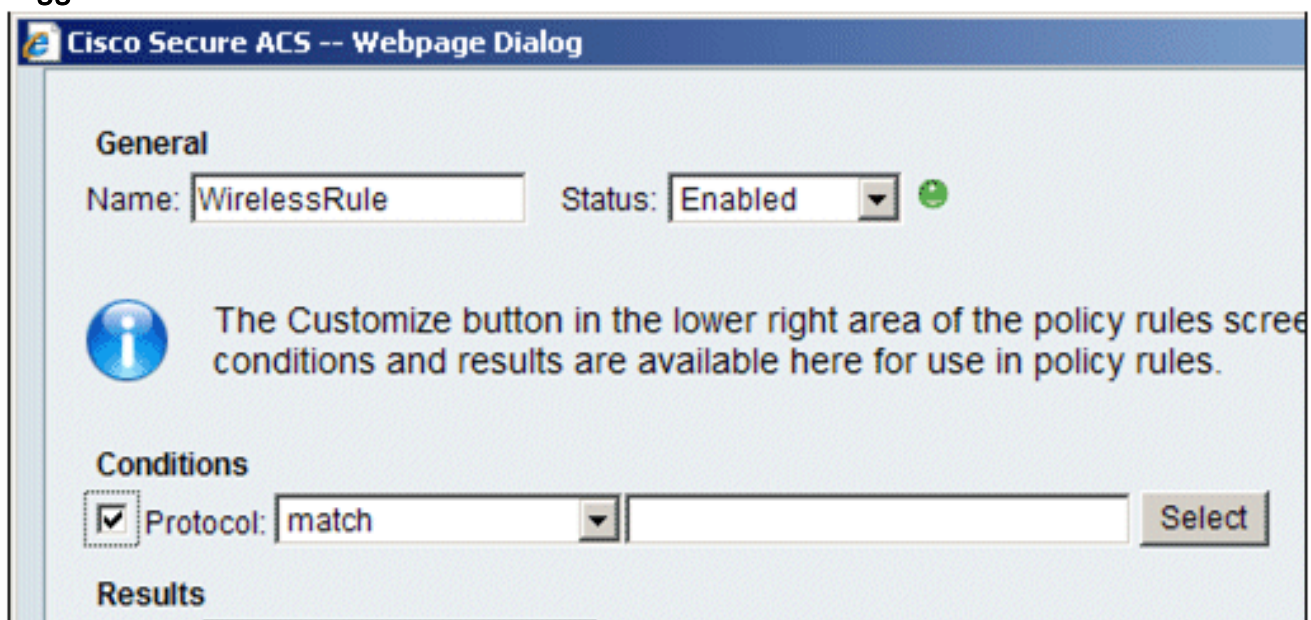
Attenersi alla procedura seguente:

1. Andare a **Criteri di accesso > Regole selezione servizio**.

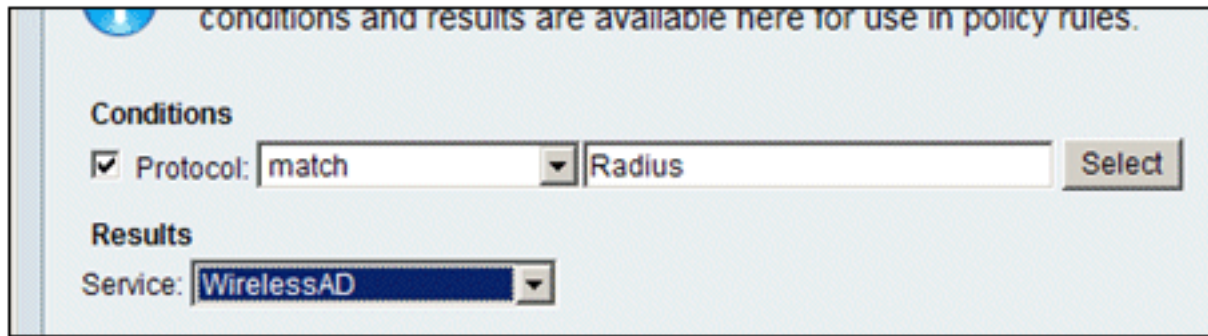




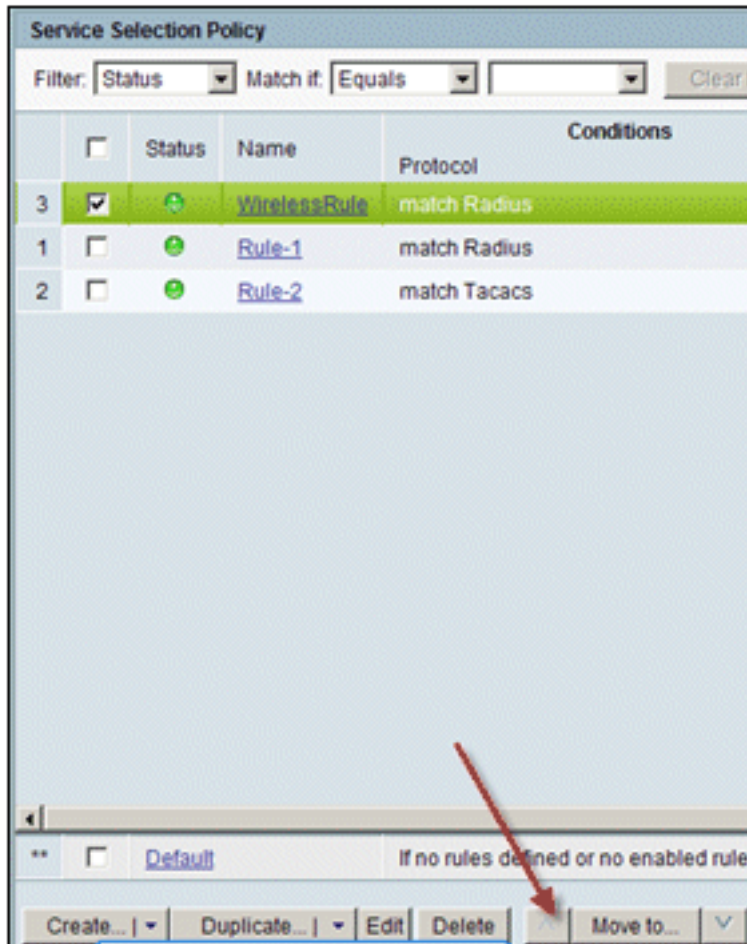
2. Fare clic su **Crea** nella finestra Criteri di selezione servizi. Assegnare un nome alla nuova regola, ad esempio *WirelessRule*. Selezionare la casella **Protocollo** per trovare una corrispondenza con **Raggio**.



3. Selezionate **Raggio (Radius)**, quindi fate clic su **OK**.  
 4. In Risultati, scegliere **WirelessAD** per Service (creato nel passaggio precedente).



5. Una volta creata la nuova regola wireless, scegliere e **spostare** questa regola all'inizio, che sarà la prima regola per identificare l'autenticazione radius wireless mediante Active



Directory.

## Configurazione CLIENT per PEAP con Windows Zero Touch

Nell'esempio, CLIENT è un computer che esegue Windows XP Professional con SP che funge da client wireless e ottiene l'accesso alle risorse della 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 procedura seguente:

1. Collegare il CLIENT al segmento della rete Intranet utilizzando un cavo Ethernet collegato all'hub.
2. In CLIENT, installare Windows XP Professional con SP2 come computer membro denominato CLIENT del dominio demo.local.

3. Installare Windows XP Professional con SP2. Per poter utilizzare il supporto PEAP, è necessario che sia installato. **Nota:** Windows Firewall viene attivato automaticamente in Windows XP Professional con SP2. Non disattivare il firewall.

## Installare la scheda di rete wireless

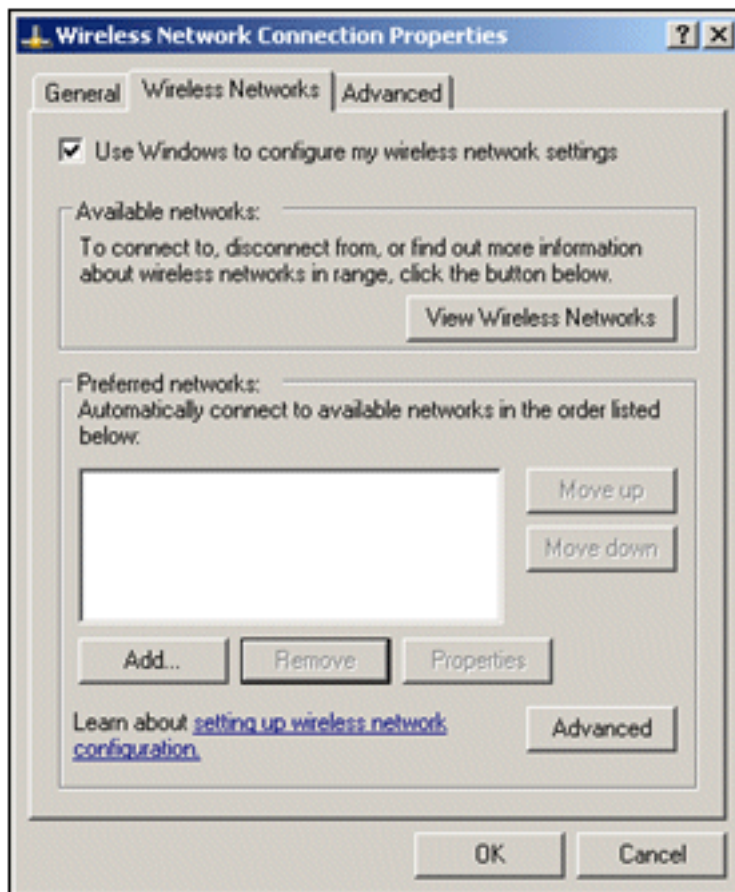
Attenersi alla procedura seguente:

1. Arrestare il computer CLIENT.
2. Disconnettere il computer CLIENT dal segmento di rete Intranet.
3. Riavviare il computer CLIENT, quindi accedere utilizzando l'account di amministratore locale.
4. Installare la scheda di rete wireless. **Nota:** non installare il software di configurazione del produttore per la scheda di rete wireless. Installare i driver della scheda di rete wireless utilizzando l'Installazione guidata hardware. Inoltre, quando richiesto, fornire il CD fornito dal produttore o un disco con i driver aggiornati da utilizzare con Windows XP Professional con SP2.

## Configurazione della connessione di rete wireless

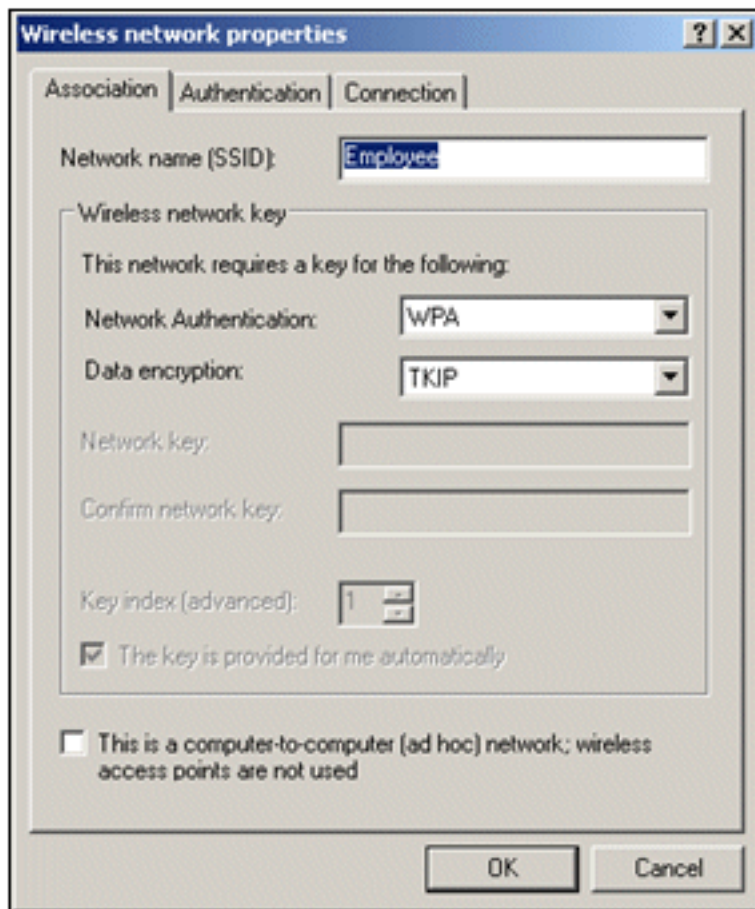
Attenersi alla procedura seguente:

1. Disconnettersi e quindi accedere utilizzando l'account **WirelessUser** nel dominio **demo.local**.
2. Scegliere **Start > Pannello di controllo**, fare doppio clic su **Connessioni di rete**, 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 **Usa Windows per configurare le impostazioni della rete wireless** sia



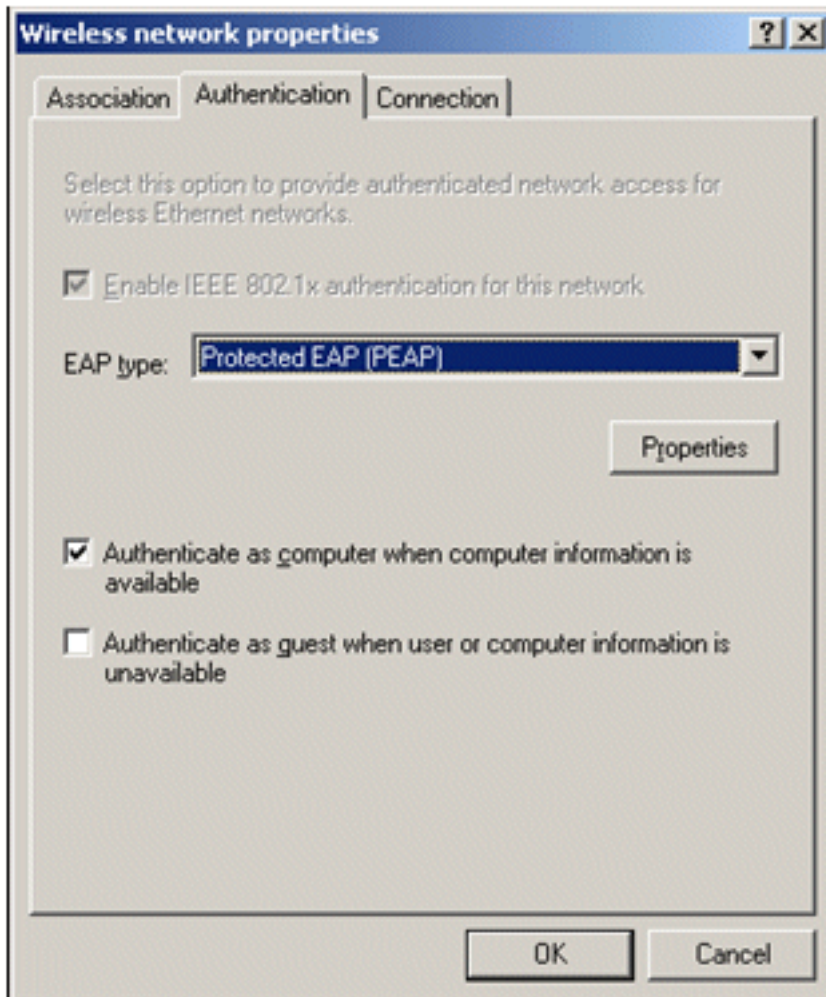
selezionato.

4. Fare clic su **Add**.
5. Nella scheda Associazione, immettere *Dipendente* nel campo Nome rete (SSID).
6. Scegliere **WPA** per Autenticazione di rete e verificare che la crittografia dei dati sia impostata



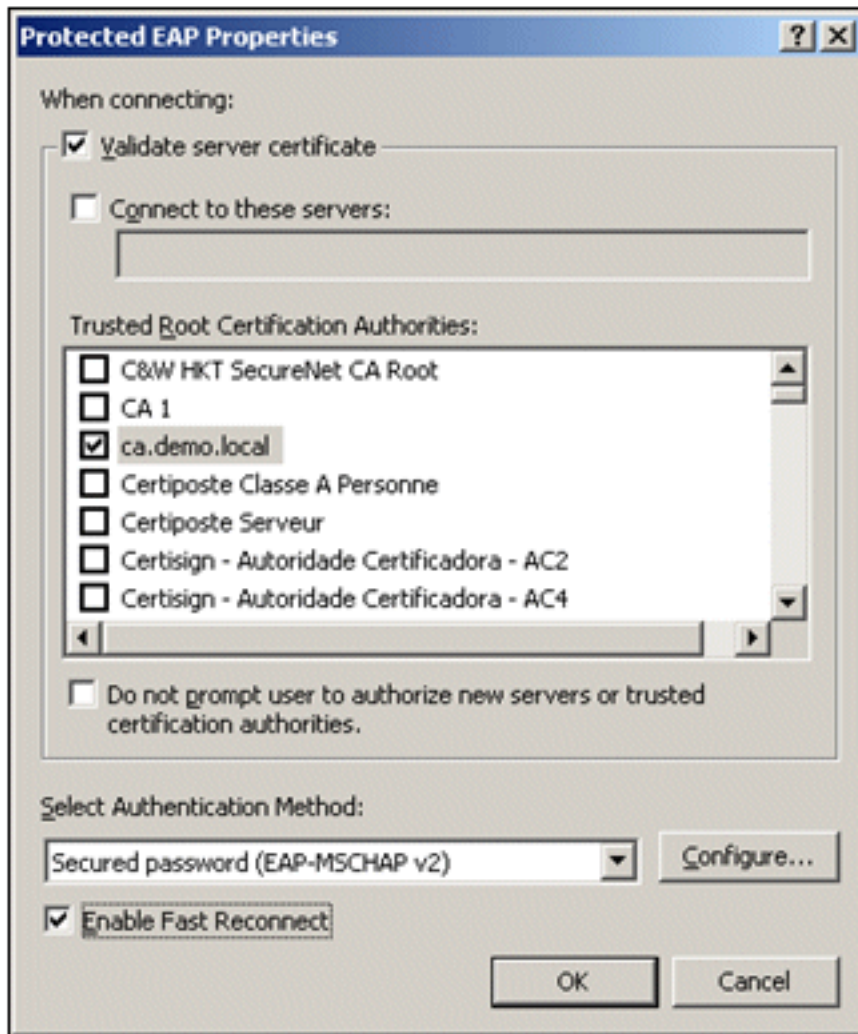
su TKIP.

7. Fare clic sulla scheda **Autenticazione**.
8. Verificare che il tipo EAP sia configurato per l'utilizzo di **PEAP (Protected EAP)**. In caso contrario, sceglierlo 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 **Autentica come computer quando sono disponibili informazioni sul**



computer.

10. Fare clic su **Proprietà**.
11. Poiché PEAP prevede l'autenticazione del server da parte del client, verificare che il **certificato Convalida server** sia selezionato. Verificare inoltre che l'autorità di certificazione che ha rilasciato il certificato ACS sia selezionata nel menu Autorità di certificazione radice attendibili.
12. Scegliere **Password protetta (EAP-MSCHAP v2)** in Metodo di autenticazione in quanto viene utilizzata per l'autenticazione



interna.

13. Verificare che la casella di controllo **Abilita riconnessione rapida** sia selezionata. Quindi, fare clic su **OK** tre volte.
14. Fare clic con il pulsante destro del mouse sull'icona della connessione di rete wireless in systray e quindi scegliere **Visualizza reti wireless disponibili**.
15. Fare clic sulla rete wireless Employee e quindi su **Connetti**. Il client wireless visualizzerà **Connesso** se la connessione viene stabilita correttamente.

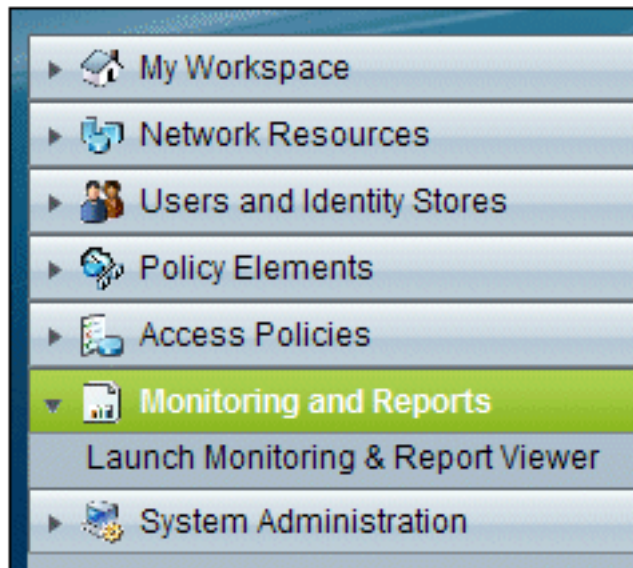


16. Al termine dell'autenticazione, controllare la configurazione TCP/IP per la scheda di rete wireless utilizzando Connessioni di rete. Deve avere un intervallo di indirizzi compreso tra 10.0.20.100 e 10.0.20.200 dall'ambito DHCP o dall'ambito creato per i client wireless CorpNet.
17. Per verificare la funzionalità, aprire un browser e selezionare **http://10.0.10.10** (o l'indirizzo IP del server CA).

# Risoluzione dei problemi di autenticazione wireless con ACS

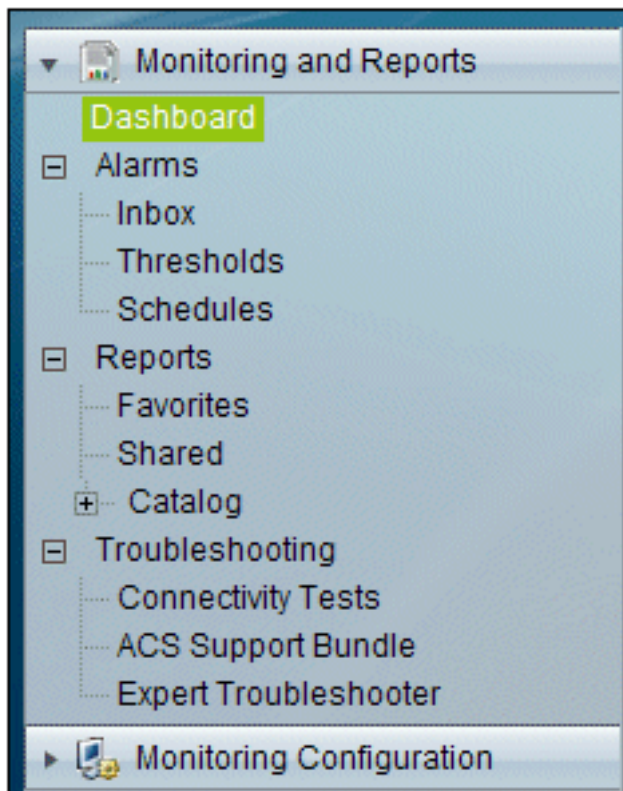
Attenersi alla procedura seguente:

1. Selezionare ACS > **Monitoraggio e report**, quindi fare clic su **Avvia Visualizzatore**



**monitoraggio e report.**

2. Viene visualizzata una finestra ACS separata. Fare clic su



**Dashboard.**

3. Nella sezione Report preferiti fare clic su **Autenticazioni - RADIUS -**

My Favorite Reports	
Favorite Name	Report Name
<a href="#">ACS - Configuration Audit - Today</a>	ACS Instance>ACS_Configuration_Audit
<a href="#">ACS - System Errors - Today</a>	ACS Instance>ACS_System_Diagnostics
<a href="#">Authentications - RADIUS - Today</a>	AAA Protocol>RADIUS_Authentication

Oggi.

4. In un registro tutte le autenticazioni RADIUS vengono visualizzate come Superate o Non riuscite. All'interno di una voce registrata, fare clic sull'**icona della lente di ingrandimento** nella colonna Dettagli.

AAA Protocol > RADIUS Authentication						
Authentication Status : Pass or Fail						
Date : September 22, 2010 ( <a href="#">Last 30 Minutes</a>   <a href="#">Last Hour</a>   <a href="#">Last 12 Hours</a>   <a href="#">Today</a>   <a href="#">Yesterday</a>   <a href="#">Last 7 Days</a>   <a href="#">Last 30 Days</a> )						
Generated on September 22, 2010 5:51:34 PM PDT						
<a href="#">Reload</a>						
✔ =Pass   ✘ =Fail   🔍 =Click for details   🖱️ =Mouse over item for additional information						
Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Authentication Method
Sep 22, 10 5:51:17.843 PM	✔		<a href="#">🔍</a>	wirelessuser	00-21-5c-69-9a-39 WirelessAD	PEAP (EAP-MSCHAPv2)

5. Nel campo Dettagli autenticazione RADIUS vengono fornite molte informazioni sui tentativi



AAA Protocol > RADIUS Authentication Detail	
ACS session ID :	acs/74551189/31
Date :	September 22, 2010
Generated on September 22, 2010 5:52:16 PM PDT	
Authentication Summary	
Logged At:	September 22, 2010 5:51:17.843 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	wirelessuser
MAC/IP Address:	00-21-5c-69-9a-39
Network Device:	wlc : 10.0.1.10 :
Access Service:	WirelessAD
Identity Store:	AD1
Authorization Profiles:	Permit Access
CTS Security Group:	
Authentication Method:	PEAP(EAP-MSCHAPv2)

registrati.

6. Il conteggio riscontri del servizio ACS può fornire una panoramica dei tentativi corrispondenti alle regole create in ACS. Selezionare **ACS > Access Policies > Access Services**, quindi fare clic su **Service Selection Rules** (Regole di selezione

Results	Hit Count
Service	
WirelessAD	33
Default Network Access	0

servizi).

## [Autenticazione PEAP non riuscita con server ACS](#)

Quando il client non esegue l'autenticazione PEAP con un server ACS, verificare se è possibile trovare il messaggio di errore *NAS duplicated authentication try* (Tentativo di autenticazione duplicata NAS) nell'opzione **Failed TRIES** (Tentativi non riusciti) del menu **Report and Activity (Report e attività)** di ACS.

È possibile che questo messaggio di errore venga visualizzato quando Microsoft Windows XP SP2 è installato nel computer client e Windows XP SP2 esegue l'autenticazione in un server di terze parti diverso da un server Microsoft IAS. In particolare, il server Cisco RADIUS (ACS) utilizza un metodo diverso per calcolare l'ID EAP-TLV (Extensible Authentication Protocol Type:Length:Value format) rispetto al metodo utilizzato da Windows XP. Microsoft ha identificato questo problema

come difetto nel supplicant di XP SP2.

Per un aggiornamento rapido, contattare Microsoft e fare riferimento all'articolo [Autenticazione PEAP non riuscita quando ci si connette a un server RADIUS di terze parti](#) . Il problema di base è che sul lato client, con l'utilità Windows, l'opzione di riconnessione rapida è disabilitata per impostazione predefinita per PEAP. Tuttavia, questa opzione è attivata per impostazione predefinita sul lato server (ACS). Per risolvere il problema, deselezionare l'opzione Riconnessione rapida sul server ACS (in Opzioni globali di sistema). In alternativa, è possibile abilitare l'opzione di riconnessione rapida sul lato client per risolvere il problema.

Per abilitare la riconnessione rapida sul client che esegue Windows XP con l'utilità Windows, eseguire la procedura seguente:

1. Selezionare **Start > Impostazioni > Pannello di controllo**.
2. Fare doppio clic sull'icona **Connessioni di rete**.
3. Fare clic con il pulsante destro del mouse sull'icona **Connessione rete senza fili** e quindi scegliere **Proprietà**.
4. Fare clic sulla scheda **Reti wireless**.
5. Scegliere l'opzione **Usa Windows per configurare le impostazioni della rete wireless** per consentire a Windows di configurare la scheda client.
6. Se è già stato configurato un SSID, sceglierlo e fare clic su **Proprietà**. In caso contrario, fare clic su **New** (Nuovo) per aggiungere una nuova WLAN.
7. Immettere il SSID nella scheda Associazione. Verificare che Autenticazione di rete sia **Aperta** e che Crittografia dati sia impostata su **WEP**.
8. Fare clic su **Autenticazione**.
9. Selezionare l'opzione **Abilita autenticazione IEEE 802.1x per questa rete**.
10. Selezionate **PEAP** come tipo EAP, quindi fate clic su **Proprietà (Properties)**.
11. Scegliere l'opzione **Abilita riconnessione rapida** nella parte inferiore della pagina.

## [Informazioni correlate](#)

- [PEAP in Unified Wireless Networks con ACS 4.0 e Windows 2003](#)
- [Esempio di configurazione di Cisco Wireless LAN Controller \(WLC\) e Cisco ACS 5.x \(TACACS+\) per l'autenticazione Web](#)
- [Guida all'installazione e all'aggiornamento di Cisco Secure Access Control System 5.1](#)
- [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).