Esempio di autenticazione EAP locale sul controller LAN wireless con EAP-FAST e configurazione del server LDAP

Sommario

Introduzione

Questo documento spiega come configurare EAP (Extensible Authentication Protocol) - Autenticazione flessibile tramite FAST (Secure Tunneling) Autenticazione EAP locale su un controller WLC. In questo documento viene inoltre spiegato come configurare il server LDAP (Lightweight Directory Access Protocol) come database back-end per il protocollo EAP locale in modo da recuperare le credenziali dell'utente e autenticarlo.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Cisco serie 4400 WLC con firmware 4.2
- Cisco Aironet serie 1232AG Lightweight Access Point (LAP)
- Server Microsoft Windows 2003 configurato come controller di dominio, server LDAP e server Autorità di certificazione.
- Cisco Aironet 802.11 a/b/g Client Adapter con firmware versione 4.2
- Cisco Aironet Desktop Utility (ADU) con firmware versione 4.2

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

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

L'autenticazione EAP locale sui controller LAN wireless è stata introdotta con Wireless LAN Controller versione 4.1.171.0.

EAP locale è un metodo di autenticazione che consente agli utenti e ai client wireless di essere autenticati localmente sul controller. È progettato per l'utilizzo in uffici remoti che desiderano mantenere la connettività ai client wireless quando il sistema back-end viene interrotto o il server di autenticazione esterno si blocca. Quando si abilita il protocollo EAP locale, il controller funge da server di autenticazione e da database degli utenti locali, pertanto rimuove la dipendenza da un server di autenticazione esterno. EAP locale recupera le credenziali utente dal database degli utenti locale o dal database backend LDAP per autenticare gli utenti. Local EAP supporta l'autenticazione LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2 e PEAPv1/GTC tra il controller e i client wireless.

EAP locale può utilizzare un server LDAP come database backend per recuperare le credenziali utente.

Un database backend LDAP consente al controller di eseguire una query su un server LDAP per ottenere le credenziali (nome utente e password) di un utente specifico. Queste credenziali vengono quindi utilizzate per autenticare l'utente.

Il database backend LDAP supporta i seguenti metodi EAP locali:

- EAP-FAST/GTC

- EAP-TLS
- PEAPv1/GTC.

Sono supportati anche LEAP, EAP-FAST/MSCHAPv2 e PEAPv0/MSCHAPv2, **ma solo se il server LDAP è configurato per restituire una password non crittografata**. Microsoft Active Directory, ad esempio, non è supportato perché non restituisce una password non crittografata. Se non è possibile configurare il server LDAP in modo che restituisca una password non crittografata, i protocolli LEAP, EAP-FAST/MSCHAPv2 e PEAPv0/MSCHAPv2 non sono supportati.

Nota: se sul controller sono configurati server RADIUS, il controller tenta di autenticare prima i client wireless utilizzando i server RADIUS. Il tentativo di eseguire EAP locale viene eseguito solo se non vengono trovati server RADIUS, a causa del timeout dei server RADIUS o della mancata configurazione di server RADIUS. Se sono configurati quattro server RADIUS, il controller tenta di autenticare il client con il primo server RADIUS, quindi con il secondo server RADIUS e infine con l'EAP locale. Se il client tenta di eseguire nuovamente l'autenticazione manualmente, il controller tenta di eseguire il terzo server RADIUS, quindi il quarto server RADIUS e infine l'EAP locale.

In questo esempio viene utilizzato EAP-FAST come metodo EAP locale sul WLC, che a sua volta è configurato per eseguire una query sul database backend LDAP per ottenere le credenziali utente di un client wireless.

Configurazione

In questo documento viene usato EAP-FAST con certificati sia sul lato client che sul lato server. A tale scopo, il programma di installazione utilizza il server **Microsoft Certificate Authority (CA)** per generare i certificati client e server.

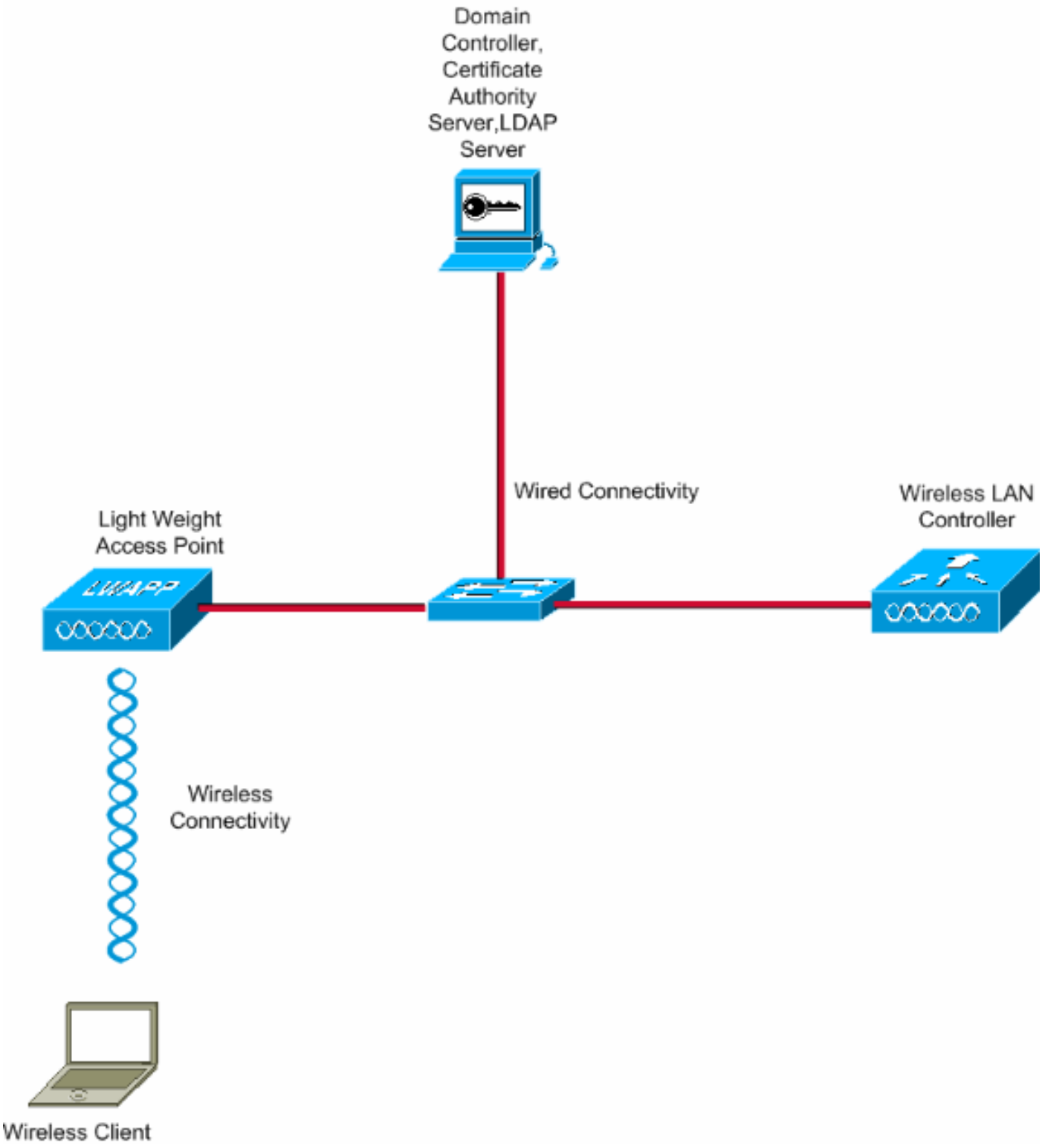
Le credenziali utente vengono archiviate nel server LDAP in modo che, dopo la convalida del certificato, il controller interroghi il server LDAP per recuperare le credenziali utente e autentichi il client wireless.

In questo documento si presume che queste configurazioni siano già presenti:

- Un LAP è registrato sul WLC. Per ulteriori informazioni sul processo di registrazione, fare riferimento a Registrazione di un Lightweight AP (LAP) su un Wireless LAN Controller (WLC).
- Un server DHCP è configurato per assegnare un indirizzo IP ai client wireless.
- Il server Microsoft Windows 2003 è configurato sia come controller di dominio che come server CA. In questo esempio viene utilizzato **wireless.com** come dominio.Per ulteriori informazioni sulla configurazione di un server Windows 2003 come controller di dominio, fare riferimento a Configurazione di Windows 2003 come controller di dominio.Per configurare il server Windows 2003 come server CA dell'organizzazione, consultare il documento sull'installazione e configurazione di Microsoft Windows 2003 Server come server CA dell'organizzazione (Enterprise).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Per implementare questa configurazione, completare i seguenti passaggi:

- Configurazione di EAP-FAST come metodo di autenticazione EAP locale sul WLC
- Configura server LDAP
- Configura client wireless

Configurazione di EAP-FAST come metodo di autenticazione EAP locale sul WLC

Come accennato in precedenza, in questo documento viene utilizzato il metodo di autenticazione EAP-FAST con certificati sia sul lato client che sul lato server. Il primo passaggio consiste nel scaricare e installare i certificati seguenti nel server (in questo caso WLC) e nel client.

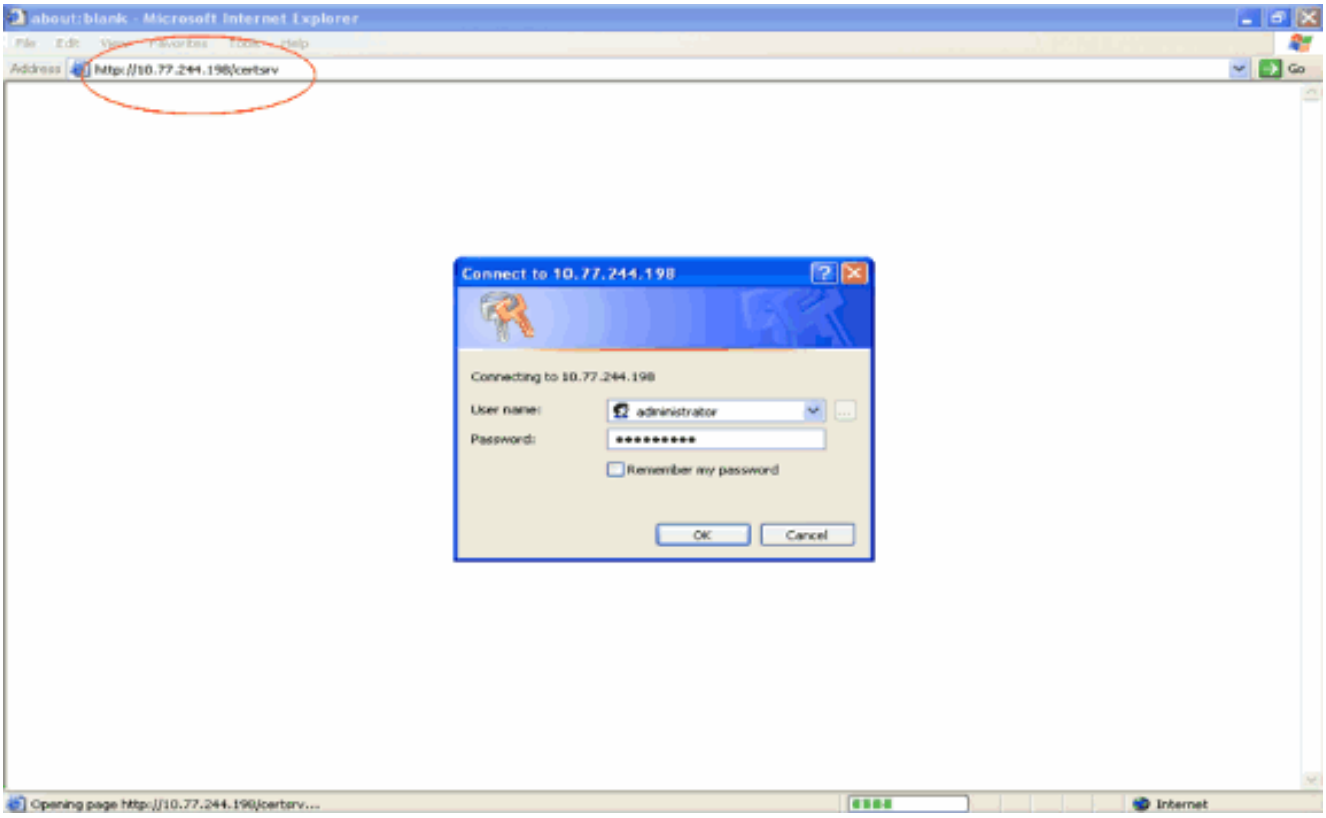
Il WLC e il client necessitano entrambi di questi certificati per essere scaricati dal server CA:

- Certificato dispositivo (uno per il WLC e uno per il client)
- Certificato radice dell'infrastruttura a chiave pubblica (PKI) per il WLC e certificato CA per il client

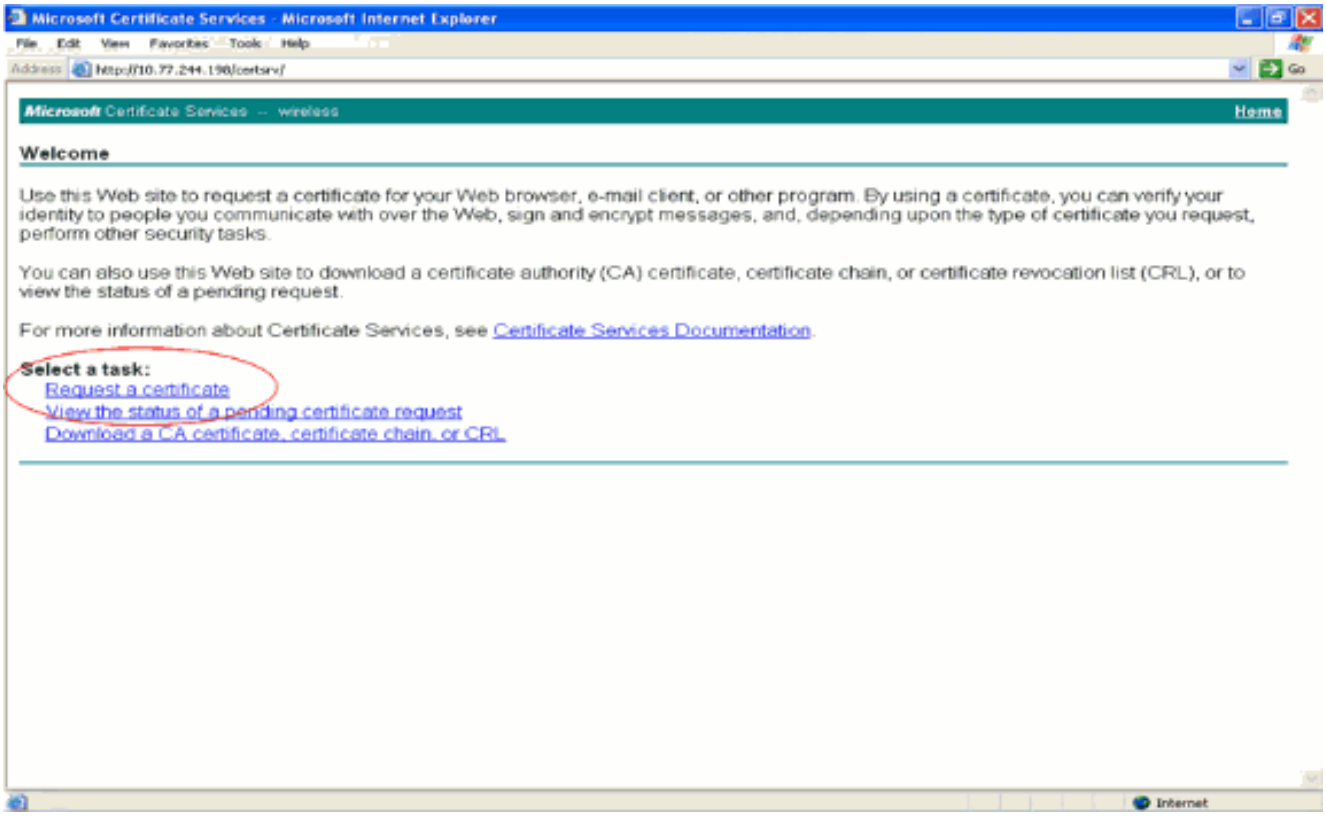
Genera un certificato dispositivo per il WLC

Eseguire questa procedura per generare un certificato del dispositivo per il WLC dal server CA. Questo certificato di dispositivo viene utilizzato dal WLC per l'autenticazione al client.

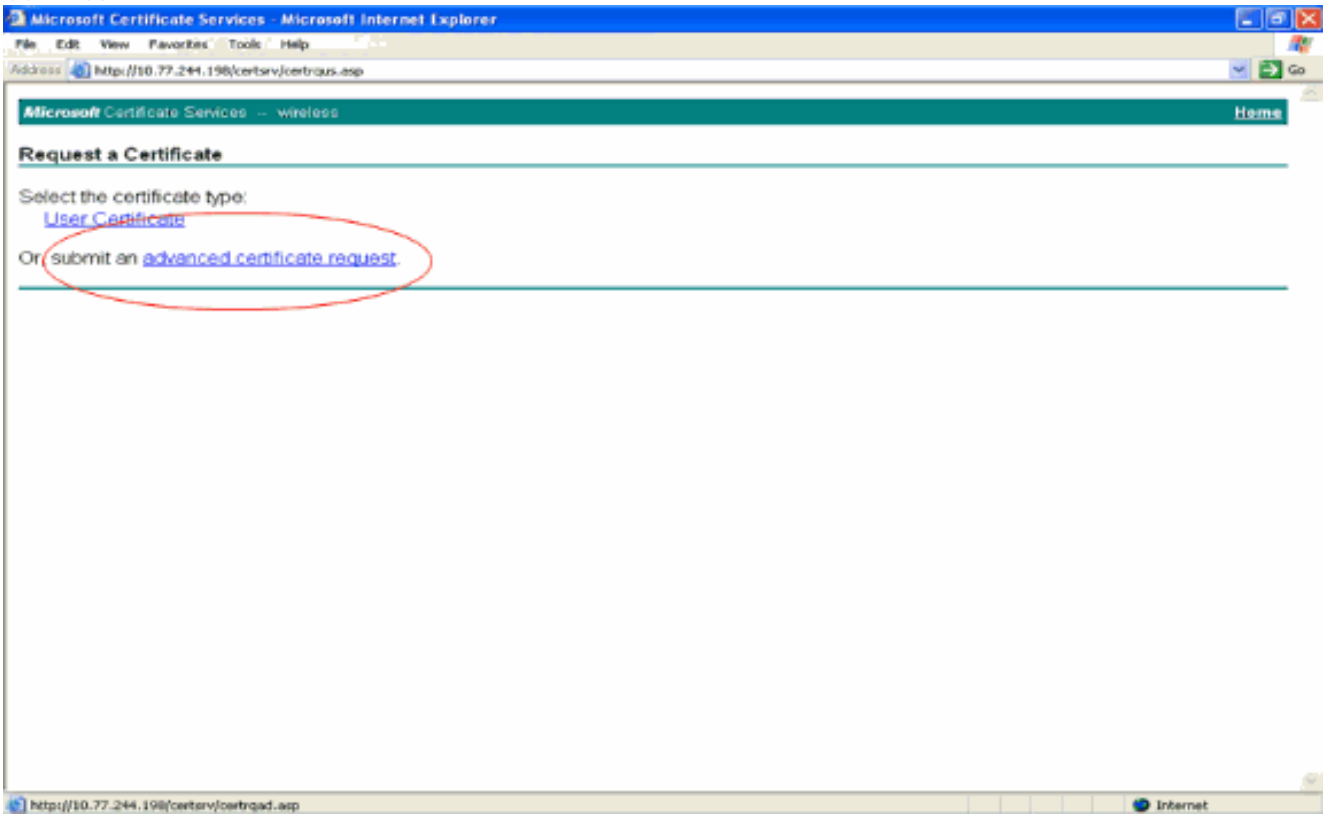
1. Visitare il sito Web all'indirizzo **http://<indirizzo IP del server CA>/certsrv** dal PC che dispone di una connessione di rete al server CA. Accedere come amministratore del server CA.



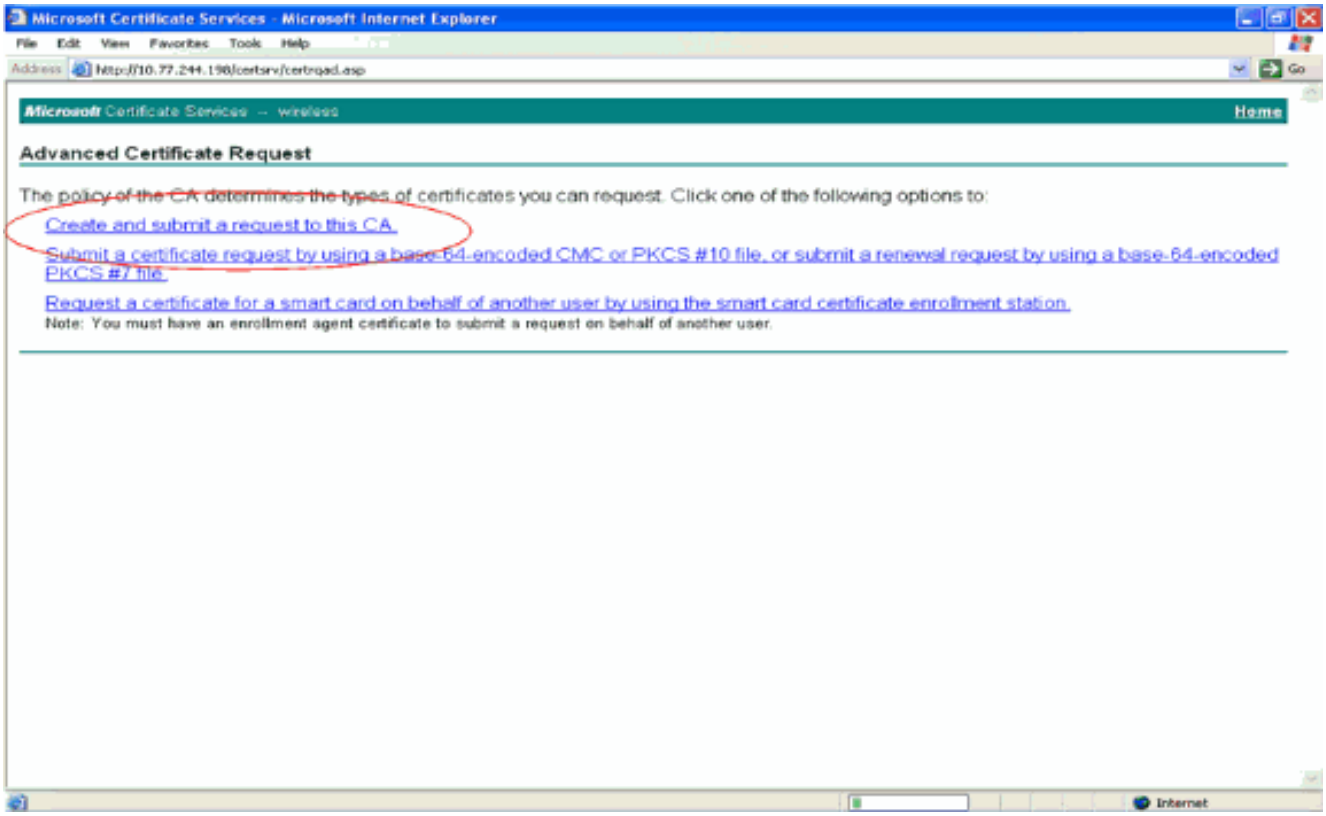
2. Selezionare **Richiedi certificato**.



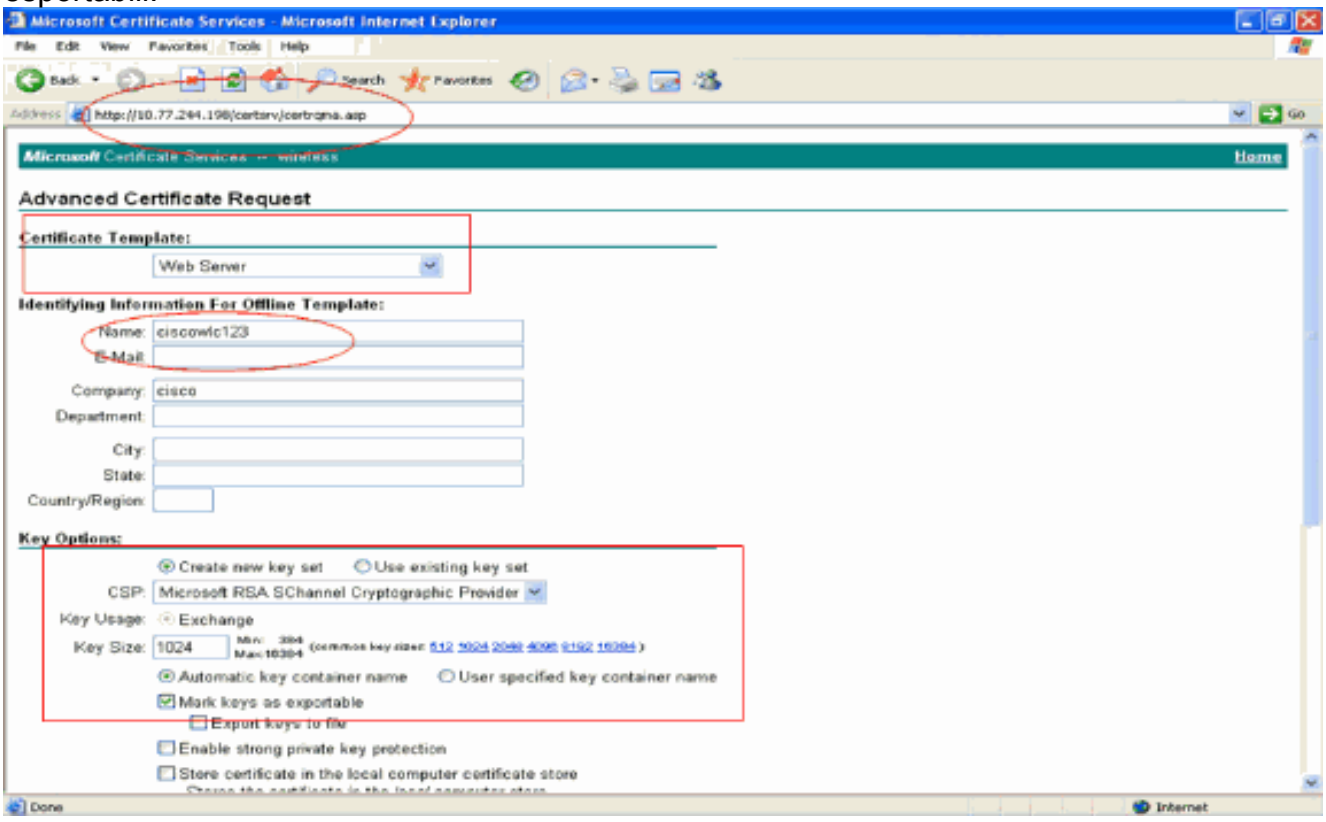
3. Nella pagina Richiedi un certificato fare clic su **Richiesta avanzata di certificati**.



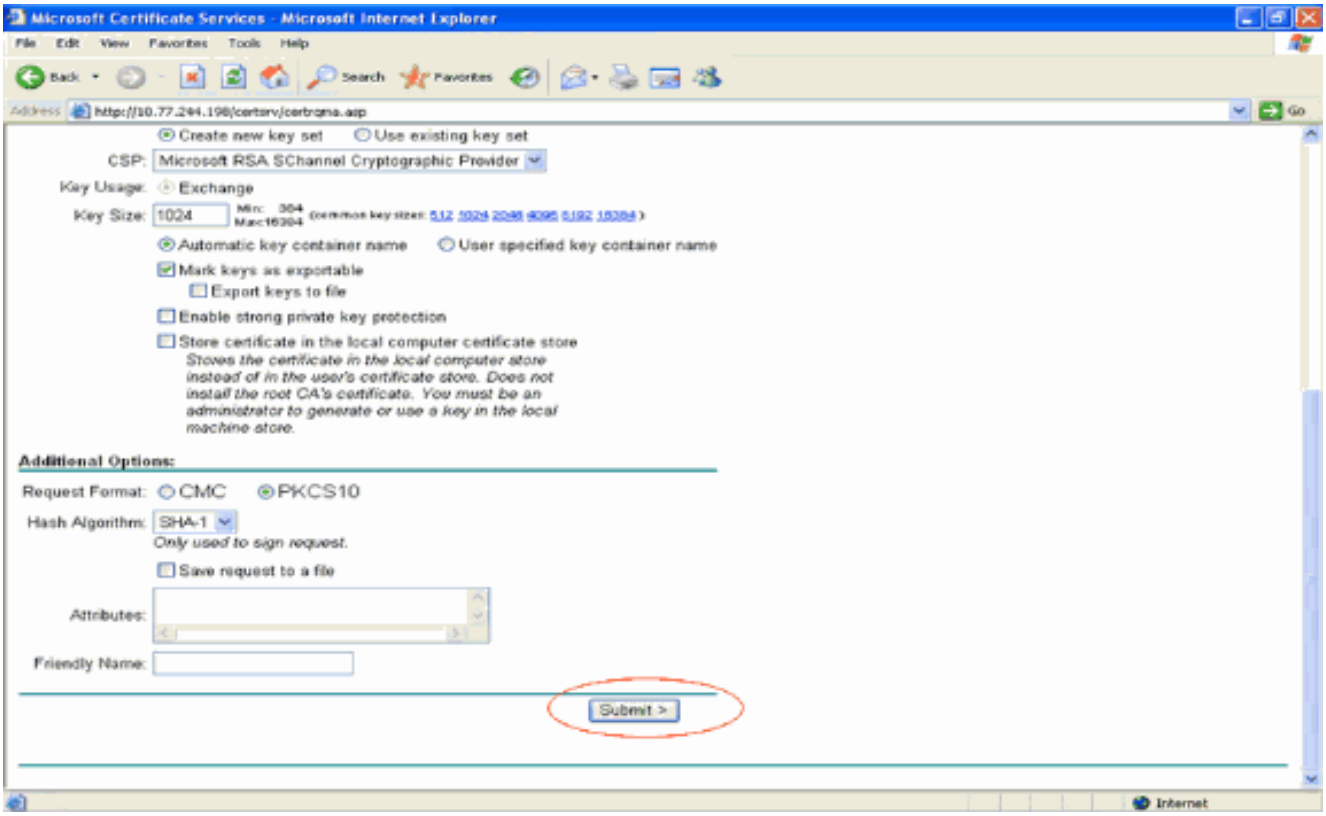
4. Nella pagina Richiesta avanzata di certificati fare clic su **Crea e invia una richiesta a questa CA**. Verrà visualizzato il modulo di richiesta avanzata dei certificati.



5. Nel modulo di richiesta avanzata del certificato scegliere **Server Web** come modello di certificato. Specificare quindi un nome per il certificato del dispositivo.In questo esempio viene utilizzato il nome del certificato ciscowlc123. Compilare le altre informazioni di identificazione in base alle proprie esigenze.
6. Nella sezione **Opzioni chiave** selezionare l'opzione **Contrassegna chiavi come esportabili**. A volte questa opzione è disattivata e non può essere attivata o disattivata se si sceglie un modello di server Web. In questi casi, scegliere **Indietro** dal menu del browser per tornare indietro di una pagina e tornare nuovamente a questa pagina. Questa volta dovrebbe essere disponibile l'opzione Contrassegna le chiavi come esportabili.

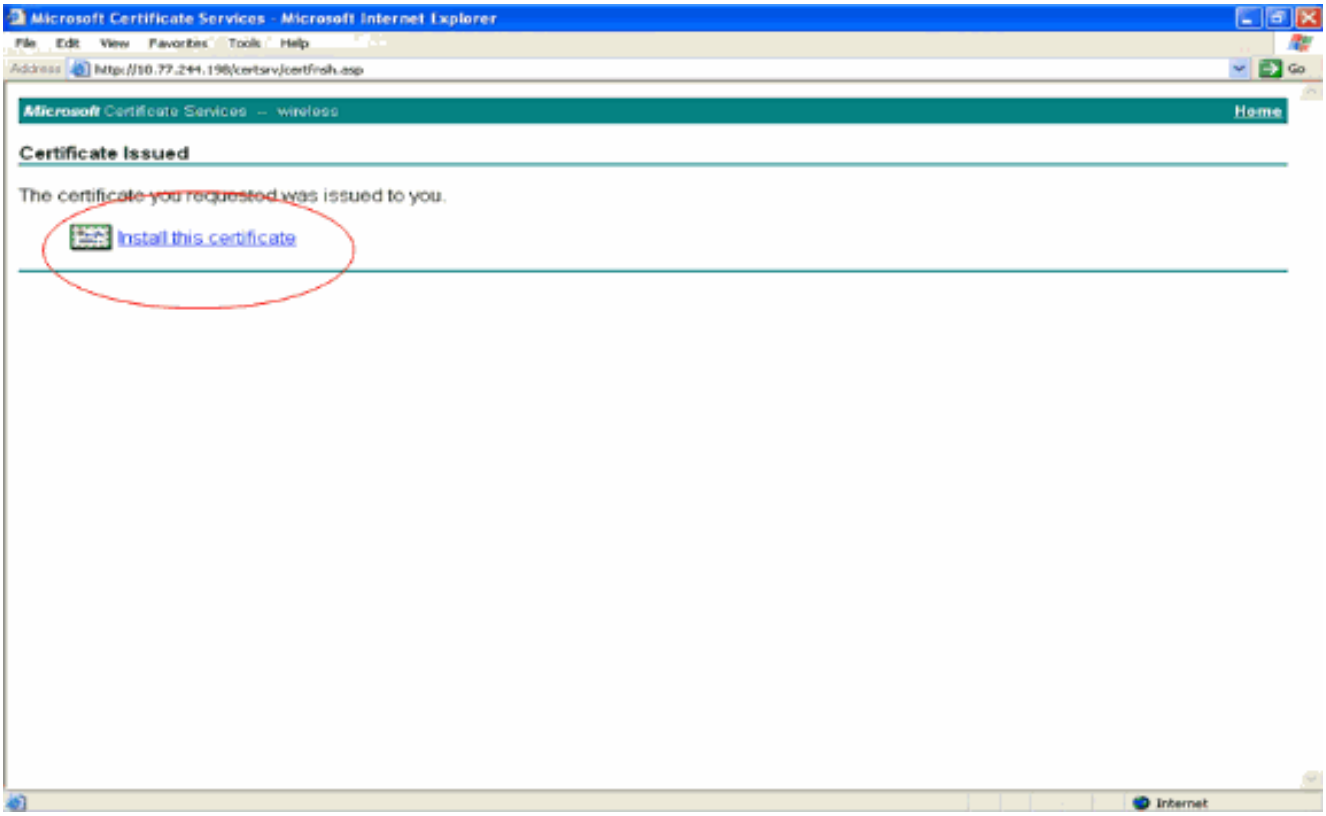


7. Configurare tutti gli altri campi necessari e fare clic su **Invia**.

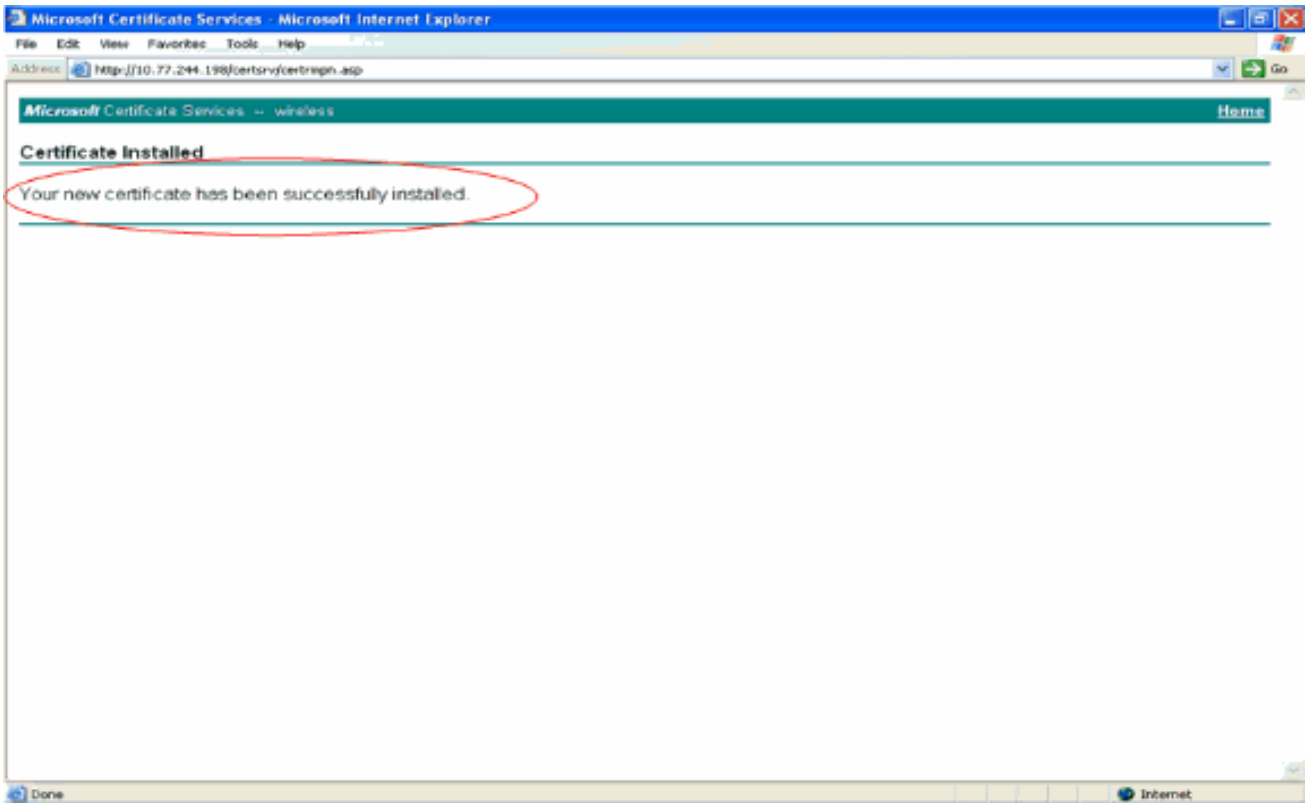


8. Fare clic su **Sì** nella finestra successiva per consentire il processo di richiesta del certificato.

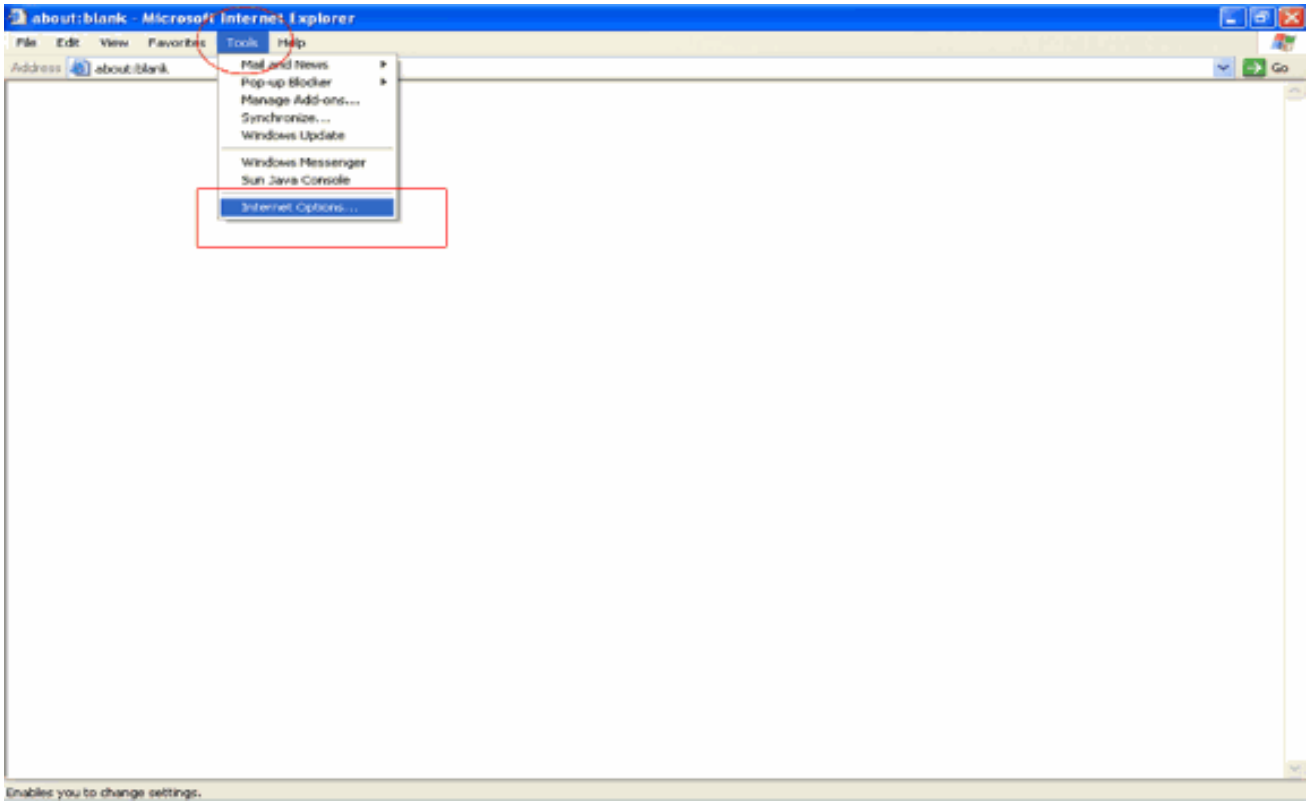
9. Viene visualizzata la finestra Certificato rilasciato che indica che il processo di richiesta del certificato è stato completato correttamente. Il passaggio successivo consiste nell'installare il certificato rilasciato nell'archivio certificati del PC. Fare clic su **Installa il certificato**.



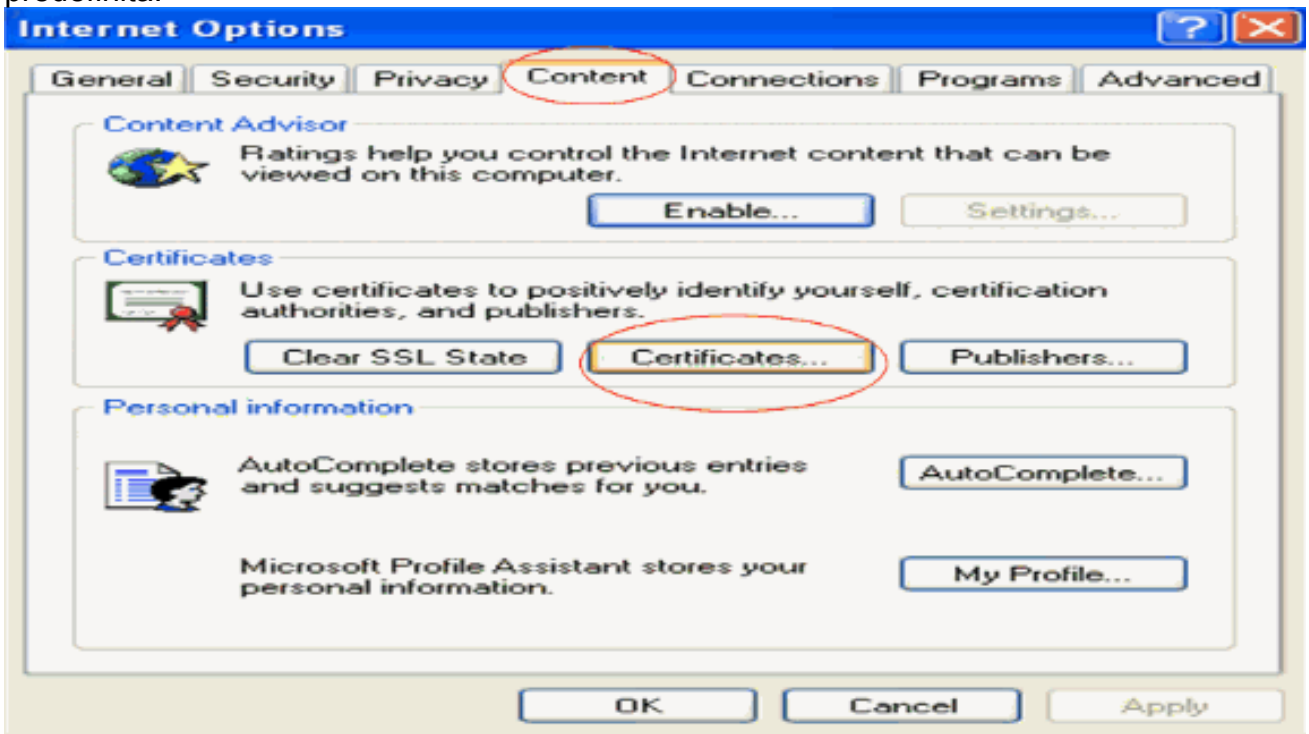
10. Il nuovo certificato è stato installato correttamente nel PC da cui la richiesta è stata generata nel server
    CA.



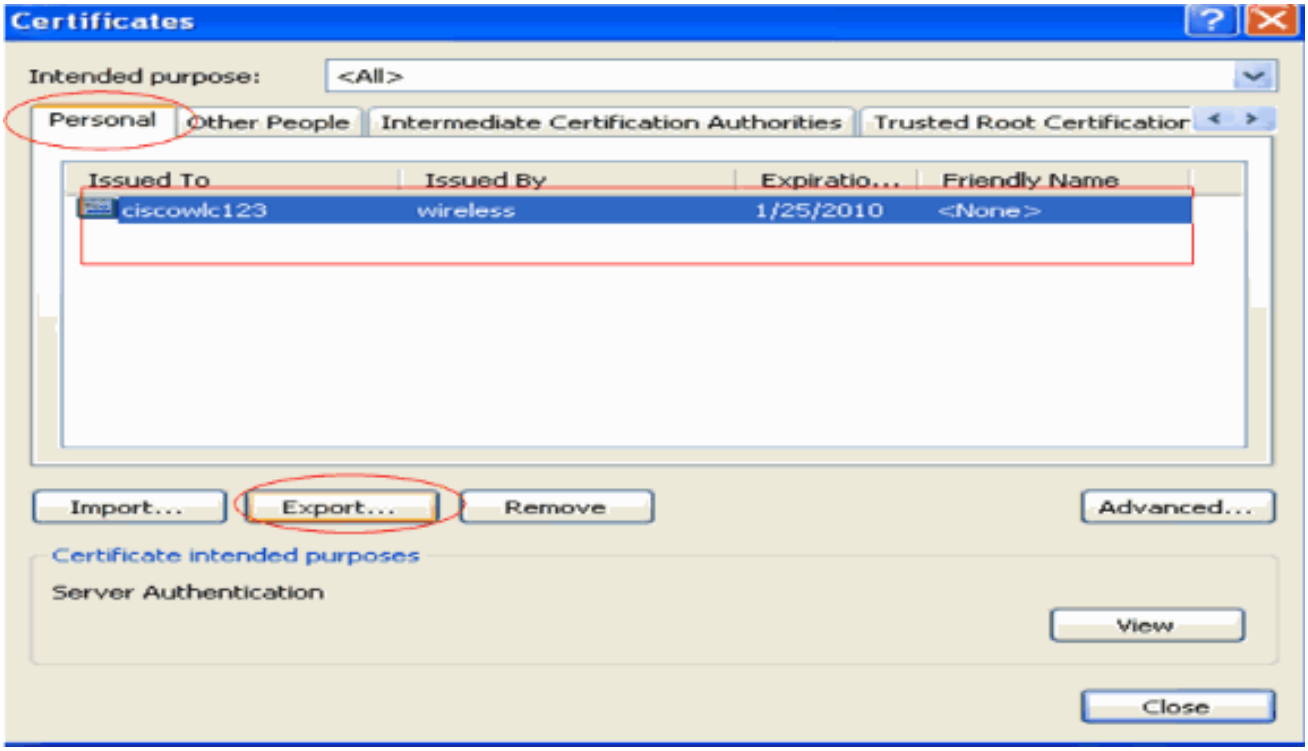
11. Il passaggio successivo consiste nell'esportare il certificato dall'archivio certificati al disco rigido come file. Questo file di certificato verrà utilizzato successivamente per scaricare il certificato nel WLC.Per esportare il certificato dall'archivio certificati, aprire il browser Internet Explorer, quindi fare clic su **Strumenti > Opzioni Internet**.



12. Fare clic su **Contenuto > Certificati** per accedere all'archivio certificati in cui i certificati sono installati per impostazione predefinita.

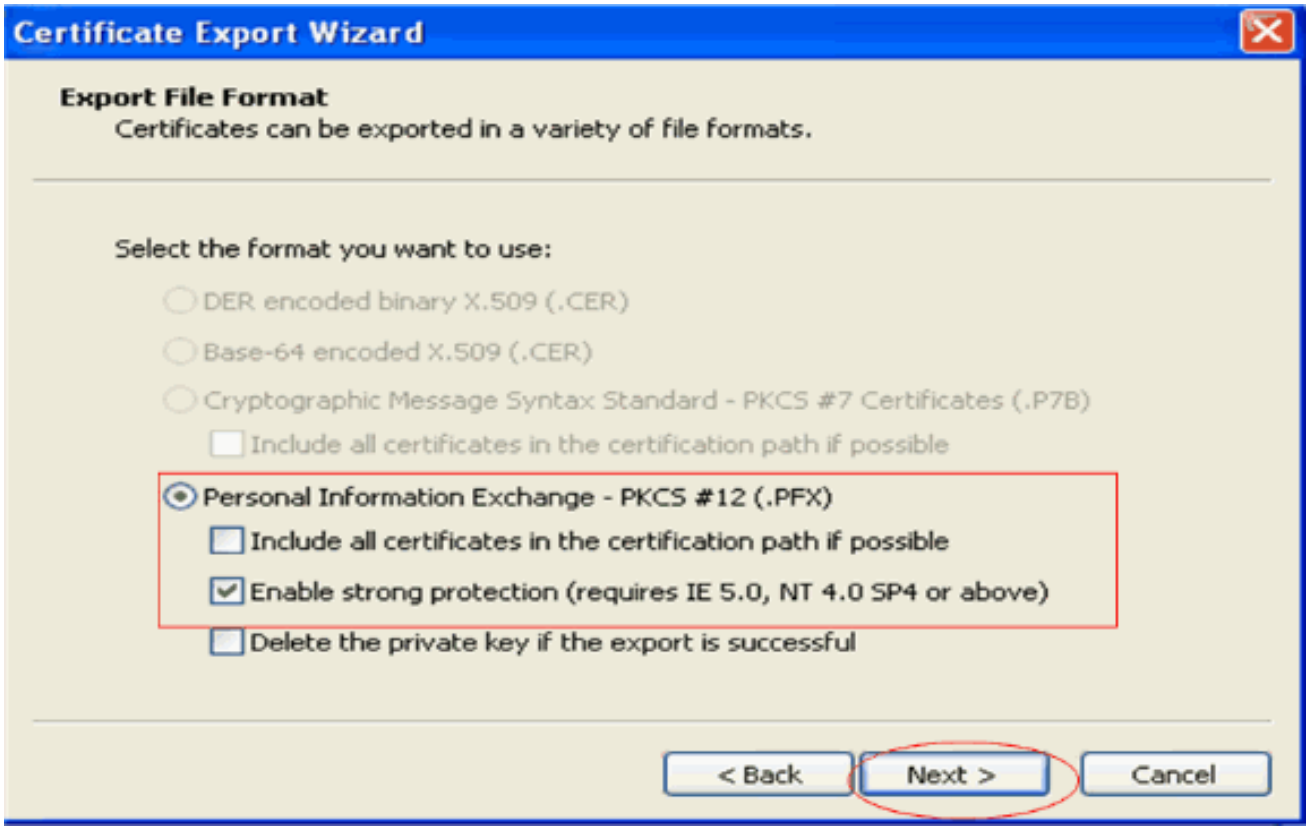


13. I certificati dei dispositivi vengono in genere installati nell'elenco dei certificati **personali**. In questo punto dovrebbe essere visualizzato il certificato appena installato. Selezionare il certificato e fare clic su **Esporta**.

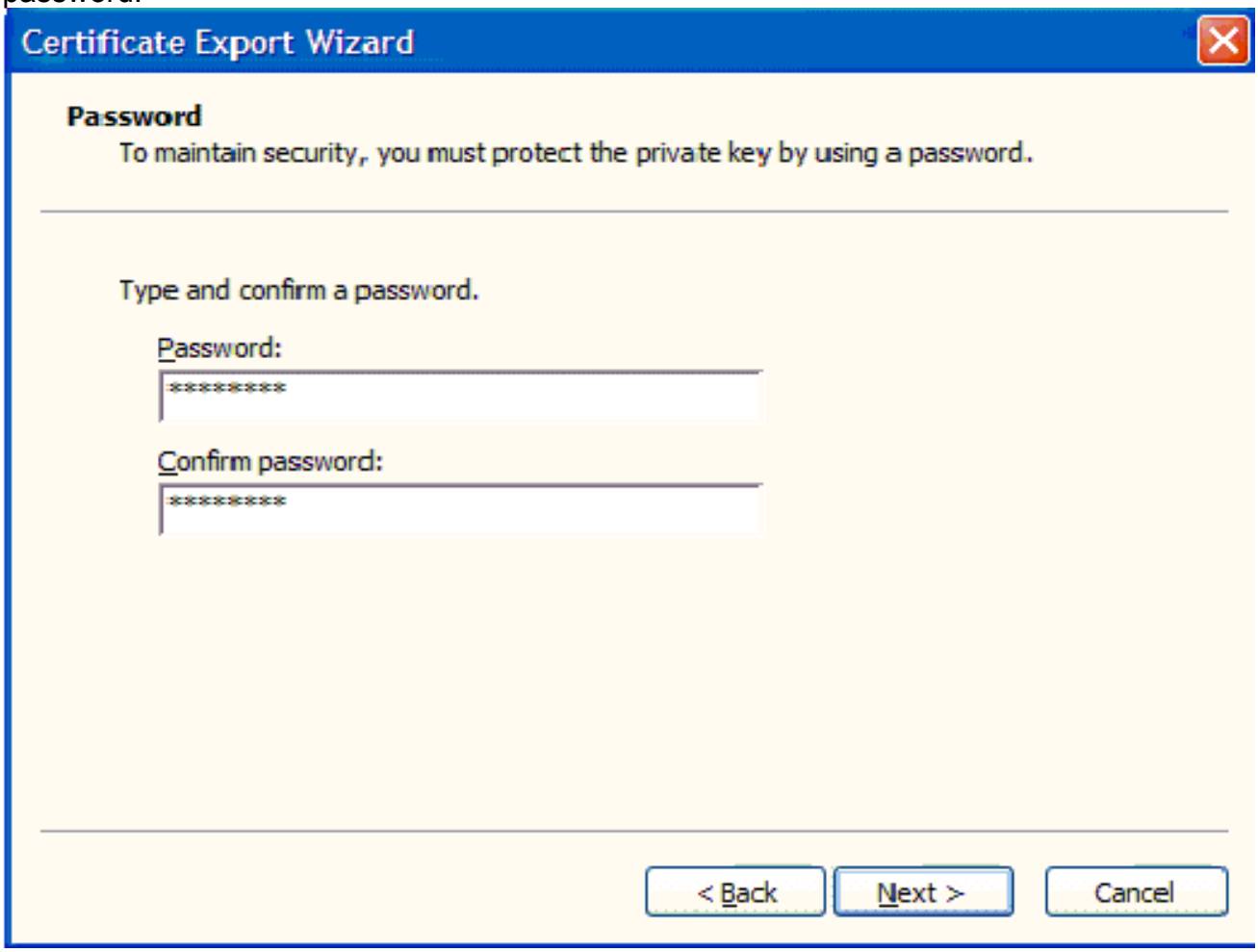


14. Fare clic su **Avanti** nelle seguenti finestre. Scegliere l'opzione **Sì, esporta la chiave privata** nella finestra **Esportazione guidata certificati**. Fare clic su **Next** (Avanti).

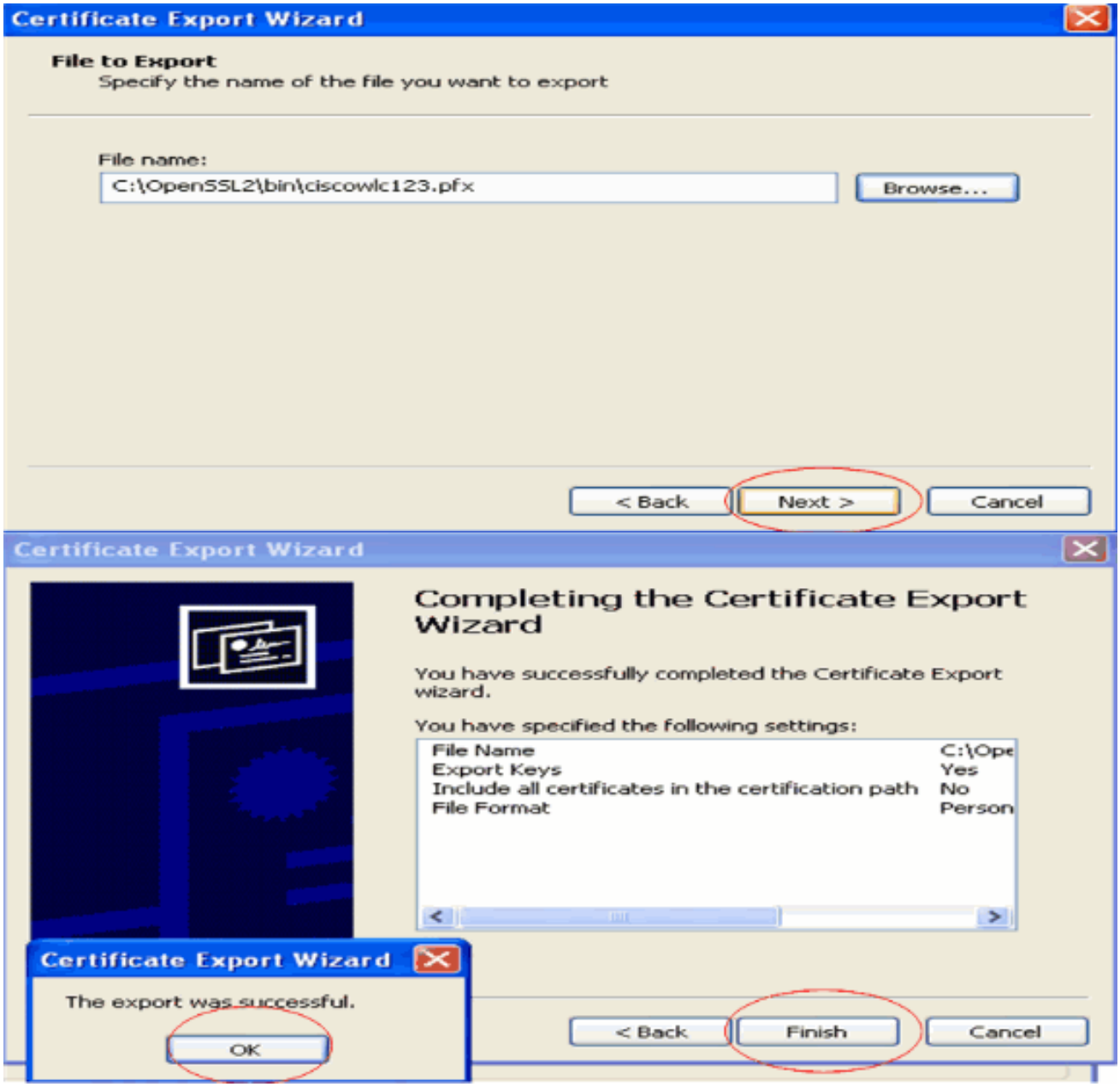
15. Scegliere il formato del file di esportazione come **.PFX** e scegliere l'opzione **Abilita protezione avanzata**. Fare clic su **Next** (Avanti).



16. Nella finestra Password, immettere una password. In questo esempio viene utilizzato **cisco** come
password.



17. Salvare il file del certificato (file PFX) sul disco rigido. Fare clic su **Avanti** e completare l'esportazione.



Download del certificato del dispositivo sul WLC

Ora che il certificato del dispositivo WLC è disponibile come file con estensione PFX, il passaggio successivo consiste nel scaricare il file sul controller. I WLC Cisco accettano certificati solo in formato .PEM. Pertanto, è innanzitutto necessario convertire il file in formato PFX o PKCS12 in un file PEM utilizzando il programma openSSL.

Convertire il certificato in formato PFX in formato PEM utilizzando il programma openSSL

Èpossibile copiare il certificato in qualsiasi PC in cui è installato openSSL per convertirlo in formato PEM. Immettere i seguenti comandi nel file Openssl.exe nella cartella bin del programma openSSL:

Nota: è possibile scaricare openSSL dal sito Web OpenSSL .

```
openssl>pkcs12 -in ciscowlc123.pfx -out ciscowlc123.pem
!--- ciscowlc123 is the name used in this example for the exported file. !--- You can specify
any name to your certificate file. Enter Import Password : cisco
```

```
!--- This is the same password that is mentioned in step 16 of the previous section. MAC
verified Ok Enter PEM Pass phrase : cisco
!--- Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM
pass phrase : cisco
```

Il file del certificato viene convertito nel formato PEM. Il passaggio successivo consiste nel scaricare il certificato del dispositivo in formato PEM sul WLC.

Nota: prima di questo, avete bisogno di un software server TFTP sul vostro PC da cui il file PEM sta per essere scaricato. Il PC deve essere connesso al WLC. Per il server TFTP devono essere specificate la directory corrente e la directory di base con la posizione in cui è memorizzato il file PEM.

Scaricare il certificato dispositivo in formato PEM convertito nel WLC

Questo esempio spiega il processo di download dalla CLI del WLC.

1. Accedere alla CLI del controller.
2. Immettere il comando **transfer download datatype eapdevcert**.
3. Immettere il comando **transfer download serverip** ***10.77.244.196***.10.77.244.196 è l'indirizzo IP del server TFTP.
4. Immettere il comando **transfer download filename** ***ciscowlc.pem***.ciscowlc123.pem è il nome del file utilizzato in questo esempio.
5. Immettere il comando **transfer download certpassword** per impostare la password per il certificato.
6. Immettere il comando **transfer download start** per visualizzare le impostazioni aggiornate.Quindi, rispondere **y** quando viene richiesto di confermare le impostazioni correnti e avviare il processo di download.Nell'esempio viene mostrato l'output del comando download:

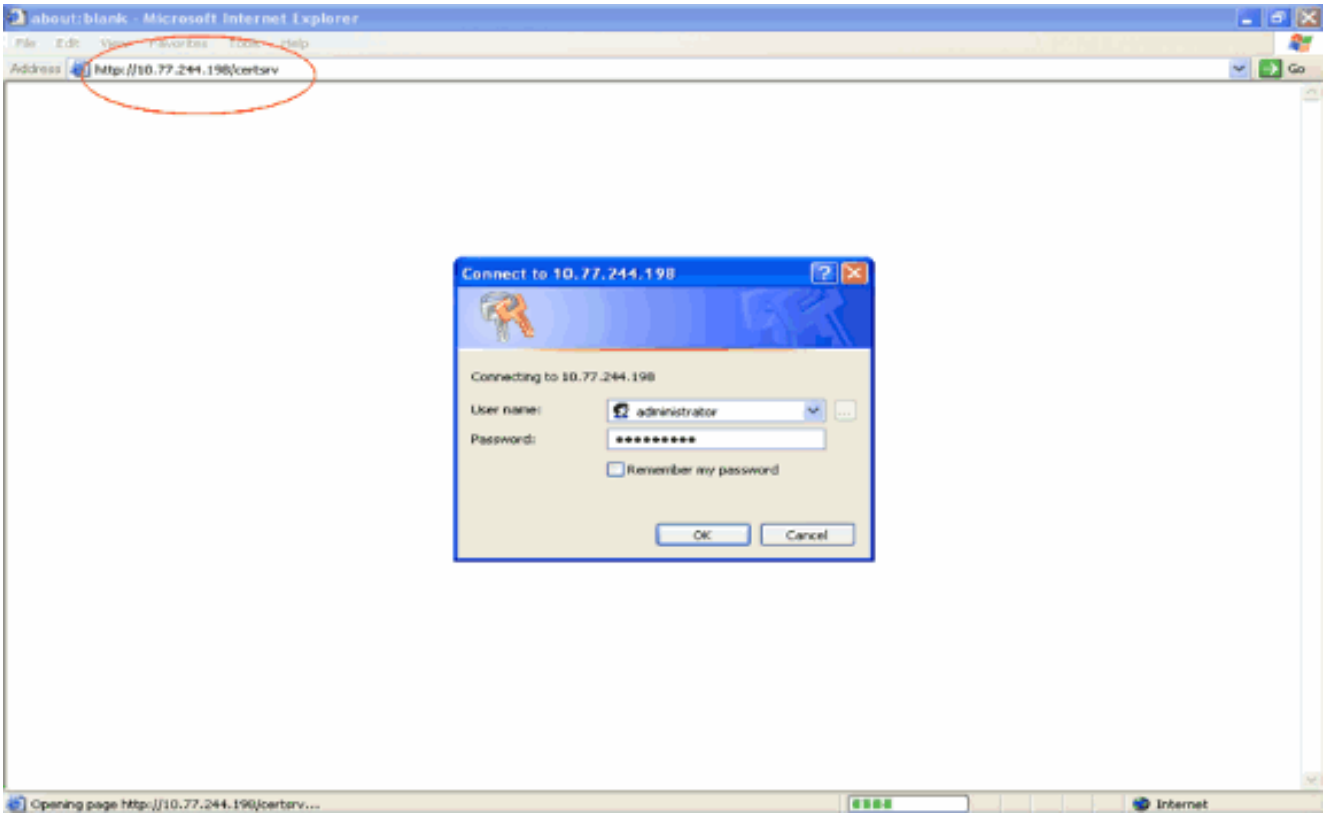
```
(Cisco Controller) >transfer download start

Mode............................................ TFTP
Data Type....................................... Vendor Dev Cert
TFTP Server IP.................................. 10.77.244.196
TFTP Packet Timeout............................. 6
TFTP Max Retries................................ 10
TFTP Path.......................................
TFTP Filename................................... ciscowlc.pem

This may take some time.
Are you sure you want to start? (y/N) y
TFTP EAP CA cert transfer starting.
Certificate installed.
Reboot the switch to use the new certificate.
Enter the reset system command to reboot the controller.
     The controller is now loaded with the device certificate.
```

7. Immettere il comando **reset system** per riavviare il controller. Il controller è ora caricato con il certificato del dispositivo.

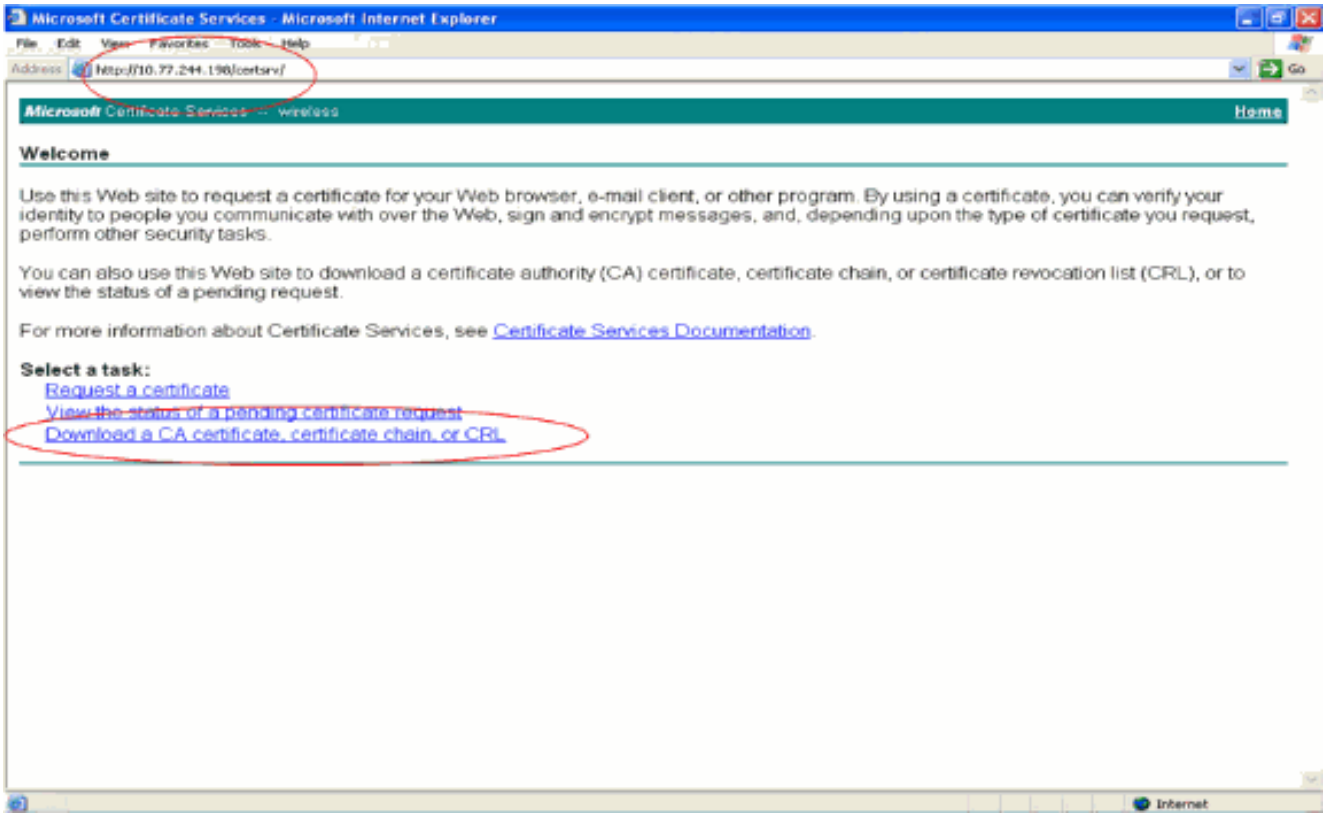
Installare il certificato radice di PKI nel WLC

Ora che il certificato del dispositivo è installato nel WLC, il passaggio successivo consiste nell'installare il certificato radice della PKI nel WLC dal server CA. Attenersi alla procedura seguente:

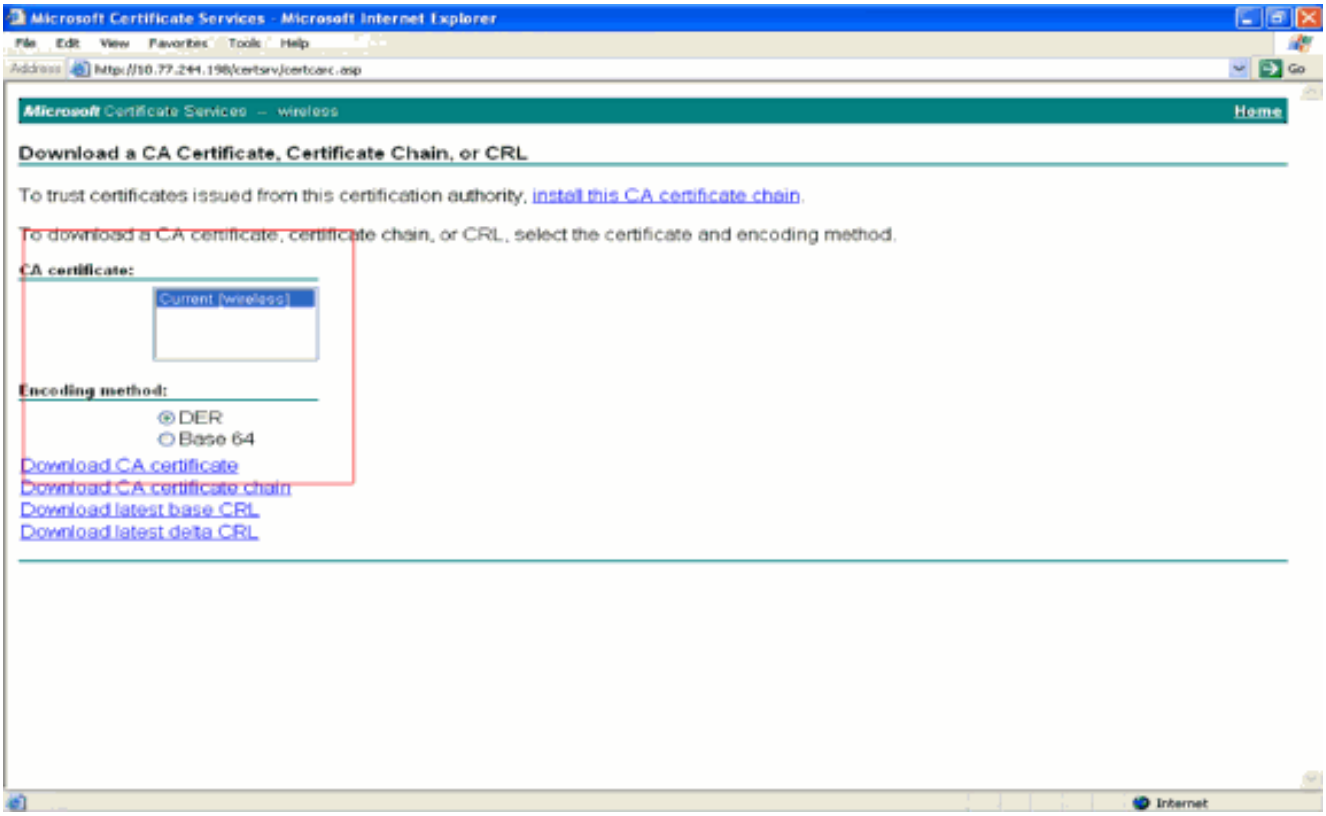
1. Visitare il sito Web all'indirizzo **http://<indirizzo IP del server CA>/certsrv** dal PC che dispone di una connessione di rete al server CA. Eseguire il login come amministratore del server CA.



2. Fare clic su **Scarica un certificato CA, una catena di certificati o un CRL**.



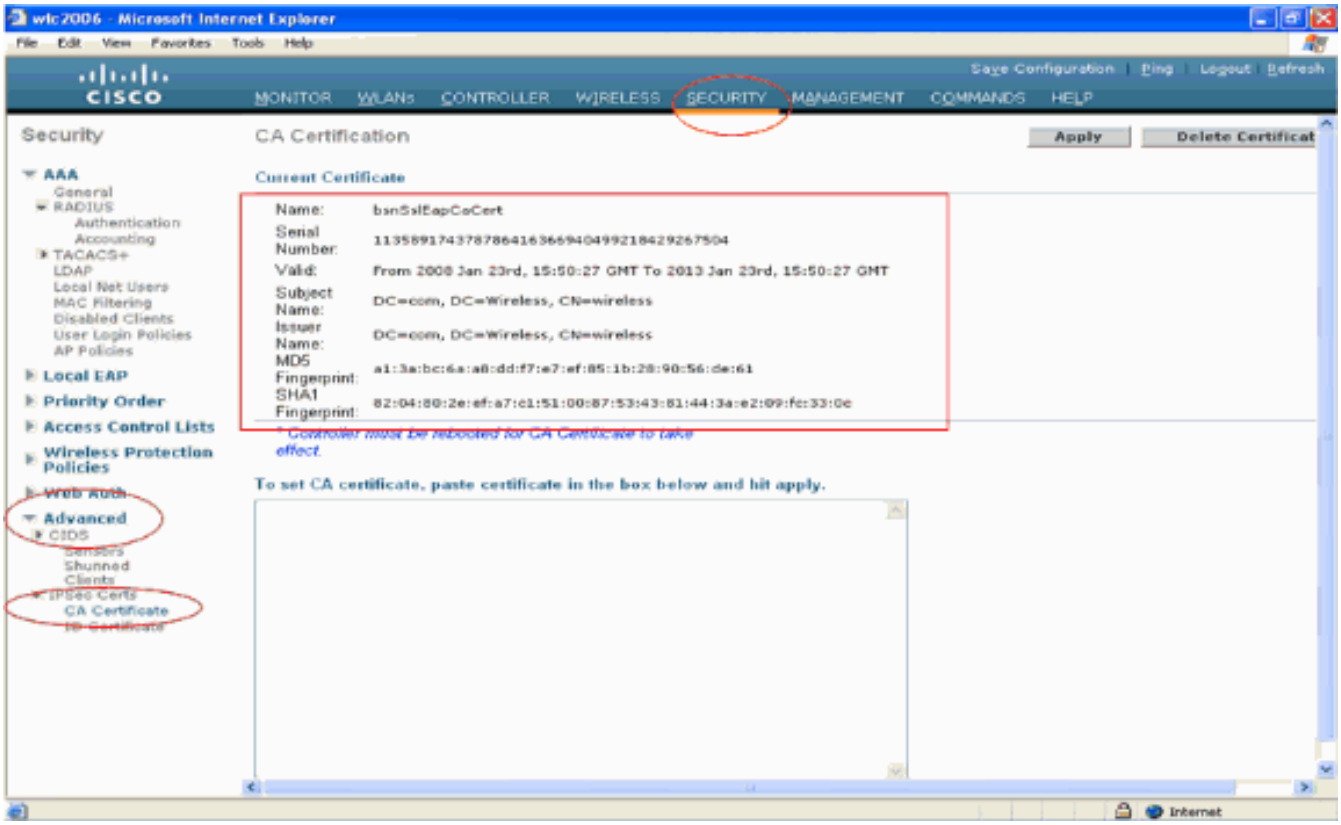
3. Nella pagina risultante è possibile visualizzare i certificati CA correnti disponibili nel server CA nella casella **Certificato CA**. Scegliere **DER** come metodo di codifica e fare clic su **Scarica certificato CA**.



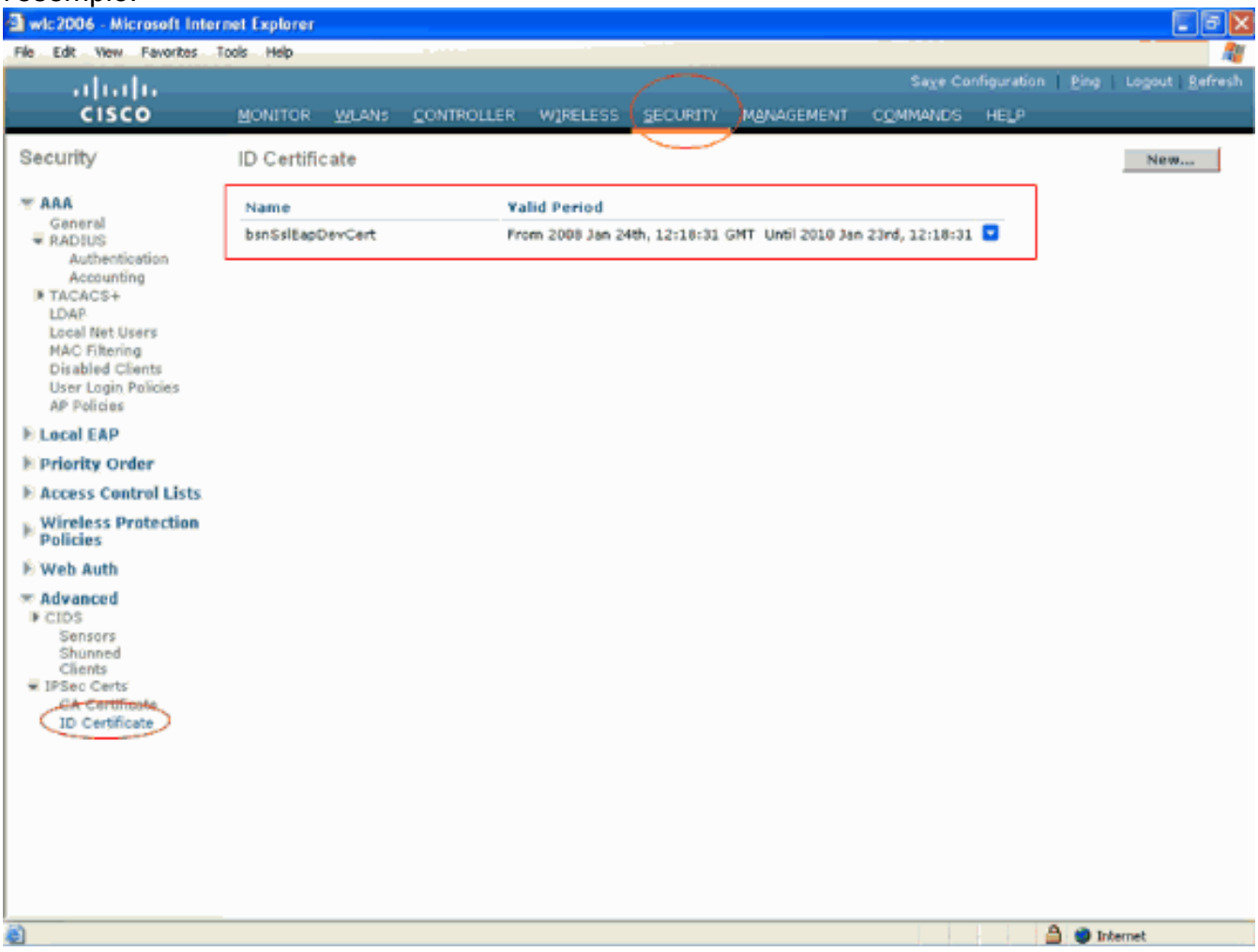
4. Salvare il certificato come file **.cer**. In questo esempio viene utilizzato **certnew.cer** come nome di file.
5. Il passaggio successivo consiste nel convertire il file con estensione cer in formato PEM e scaricarlo sul controller. Per eseguire questi passaggi, ripetere la stessa procedura descritta nella sezione Download del certificato del dispositivo sul WLC con le seguenti modifiche:I file "-in" e "-out" openSSL sono **certnew.cer** e **certnew.pem**.Inoltre, in questo processo non sono richieste passphrase PEM o password di importazione.Inoltre, il comando openSSL per convertire il file **.cer** nel file **.pem** è:**x509 -in *certnew.cer* -inform DER -out *certnew.pem* -outform PEM**Nel passaggio 2 della sezione Download del certificato di dispositivo in formato PEM convertito sul WLC, il comando per scaricare il certificato sul WLC è:(Cisco Controller)**>transfer download datatype eapcacert**Il file da scaricare sul WLC è **certnew.pem**.

Èpossibile verificare se i certificati sono installati sul WLC dall'interfaccia utente del controller come segue:

- Dall'interfaccia utente del WLC, fare clic su **Security** (Sicurezza). Nella pagina Protezione fare clic su **Avanzate > Certificati IPSec** nelle attività visualizzate a sinistra. Fare clic su **Certificato CA** per visualizzare il certificato CA installato. Di seguito è riportato l'esempio:



- Per verificare se il certificato del dispositivo è installato sul WLC, dall'interfaccia utente del WLC fare clic su **Security**. Nella pagina Protezione fare clic su **Avanzate > Certificati IPSec** nelle attività visualizzate a sinistra. Fare clic su **ID certificato** per visualizzare il certificato del dispositivo installato. Di seguito è riportato l'esempio:

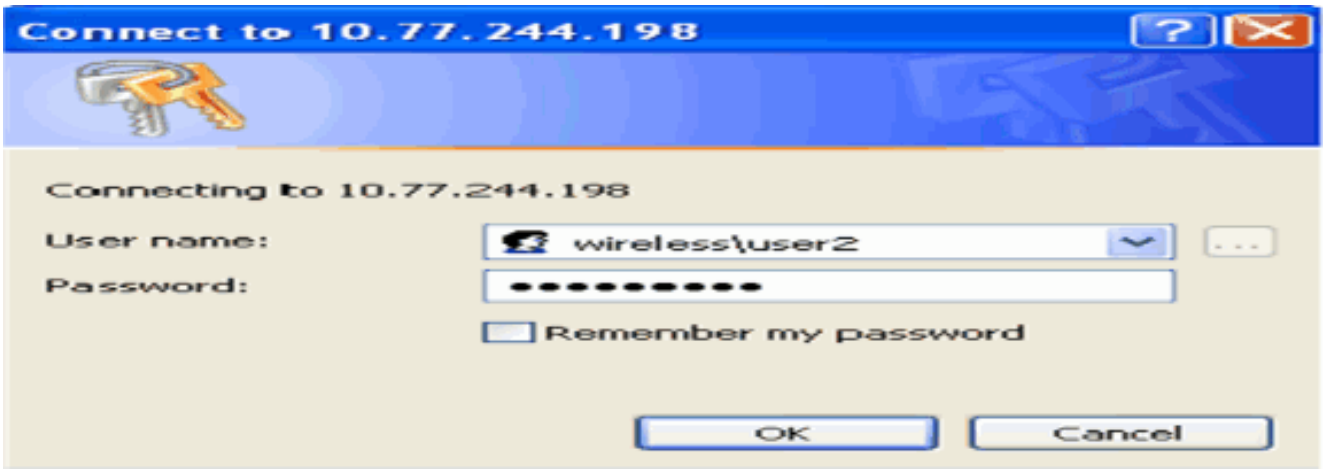


Genera un certificato dispositivo per il client

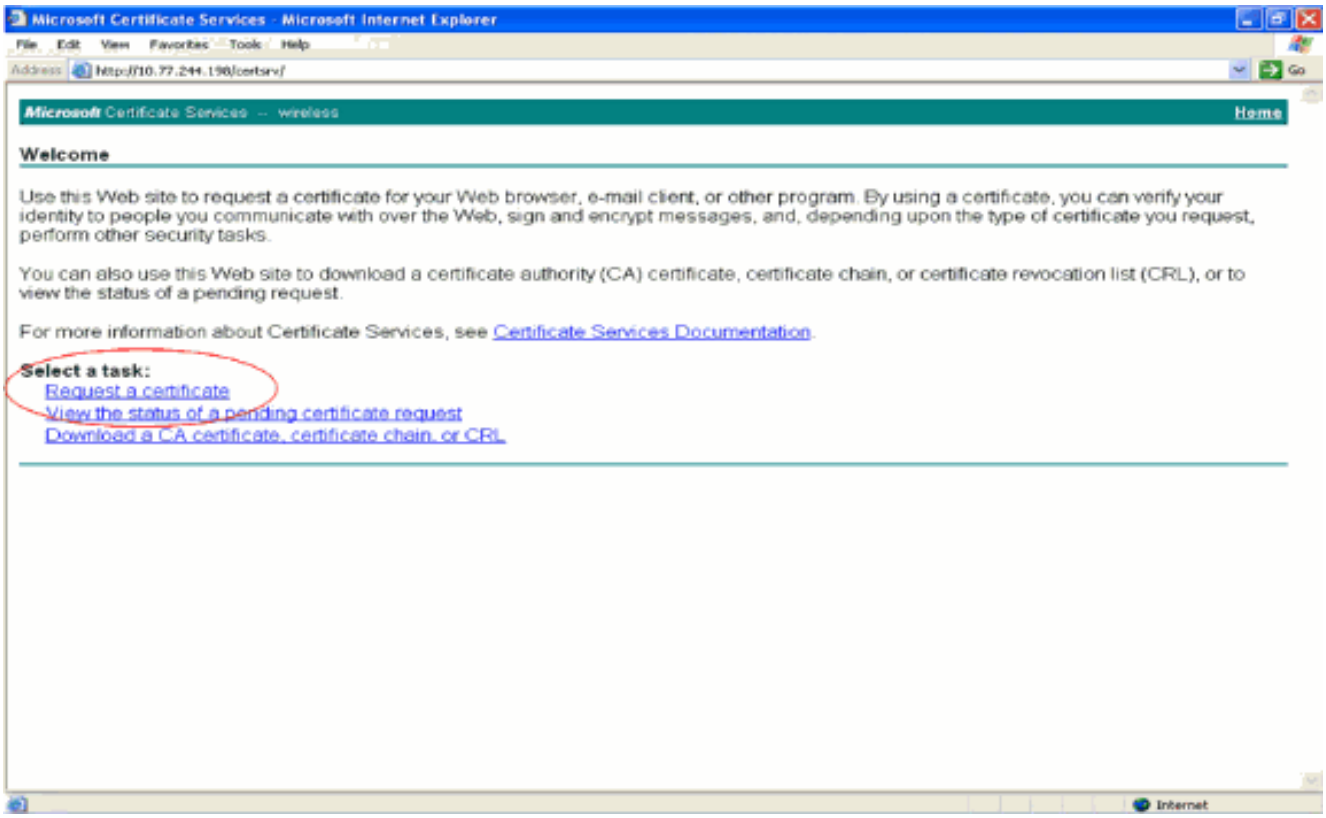
Ora che il certificato del dispositivo e il certificato della CA sono installati sul WLC, il passaggio successivo consiste nel generare questi certificati per il client.

Per generare il certificato del dispositivo per il client, eseguire la procedura seguente. Questo certificato verrà utilizzato dal client per l'autenticazione al WLC. In questo documento vengono illustrati i passaggi necessari per la generazione di certificati per il client Windows XP Professional.

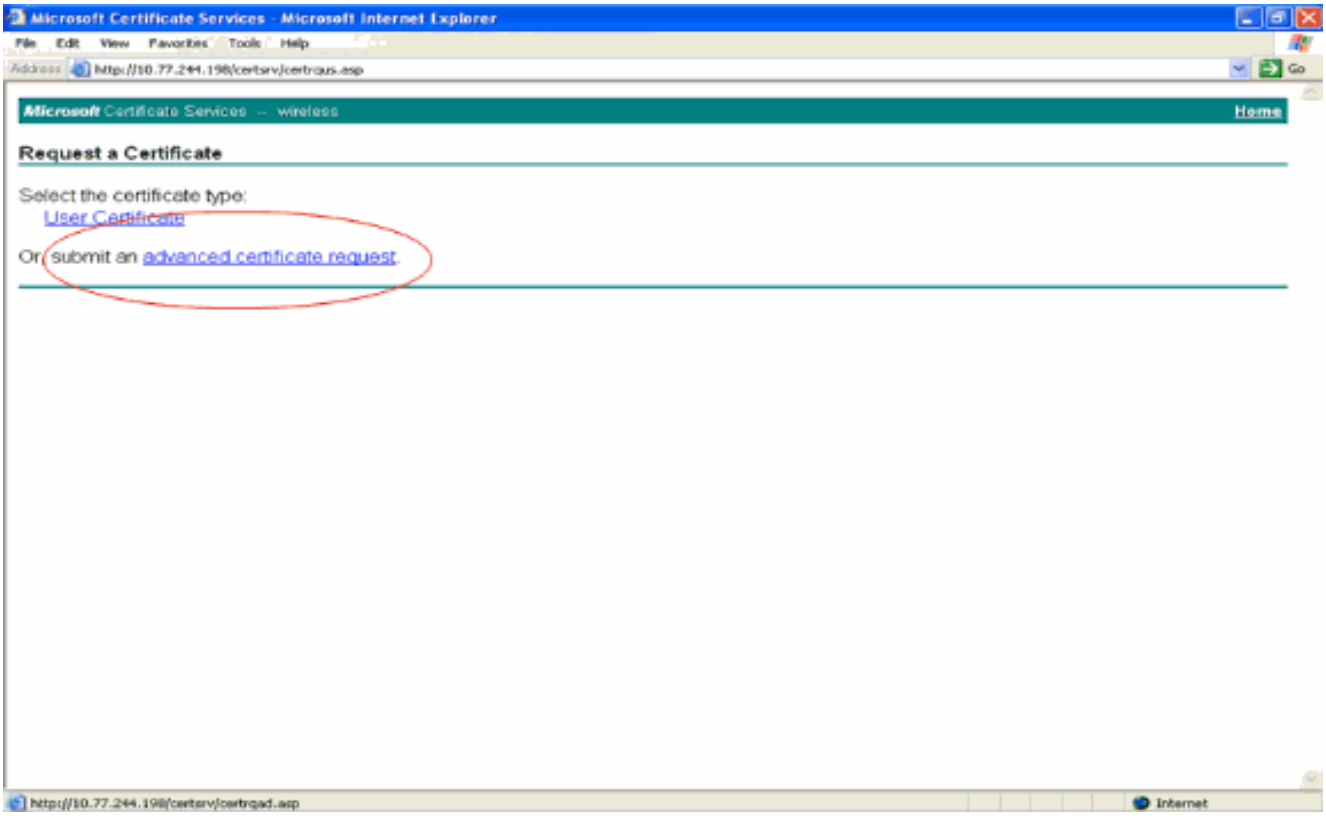
1. Visitare il sito Web all'indirizzo **http://<indirizzo IP del server CA>/certsrv** dal client che richiede l'installazione del certificato. Eseguire l'accesso come nome di dominio omeutente al server CA. Il nome utente deve corrispondere al nome dell'utente che utilizza questo computer XP e l'utente deve essere già configurato come parte dello stesso dominio del server
CA.



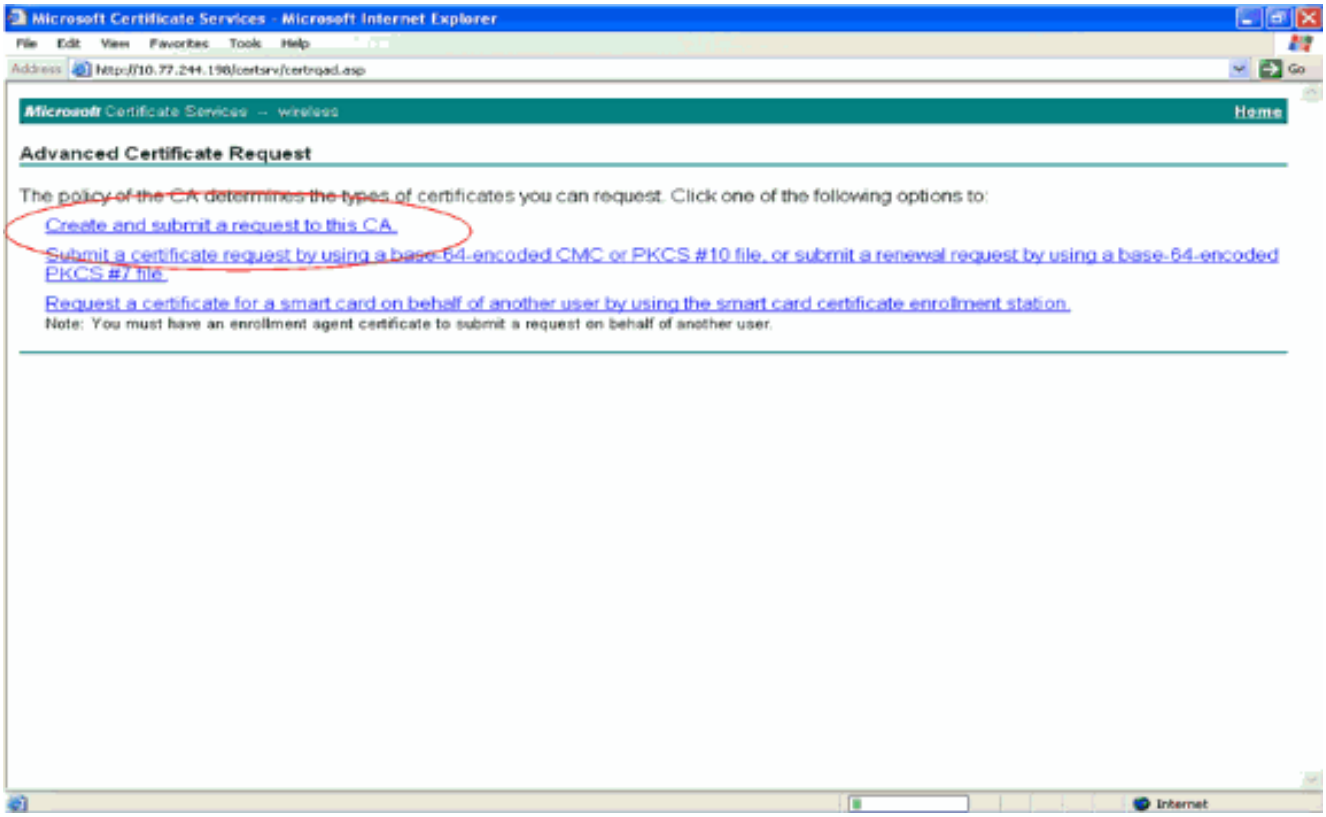
2. Selezionare **Richiedi certificato**.



3. Nella pagina Richiedi un certificato fare clic su **Richiesta avanzata di certificati**.

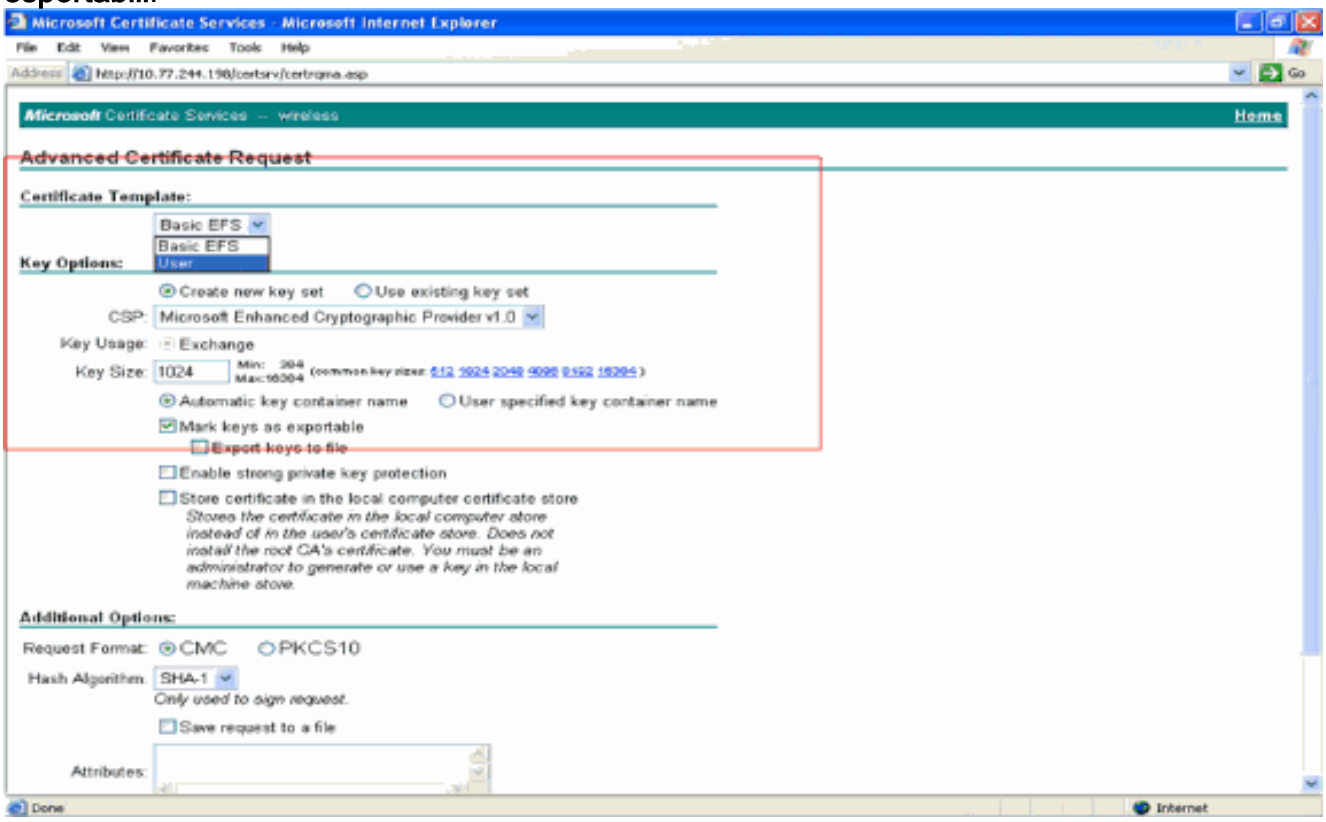


4. Nella pagina Richiesta avanzata di certificati fare clic su **Crea e invia una richiesta a questa CA**. Verrà visualizzato il modulo di richiesta del certificato avanzato.

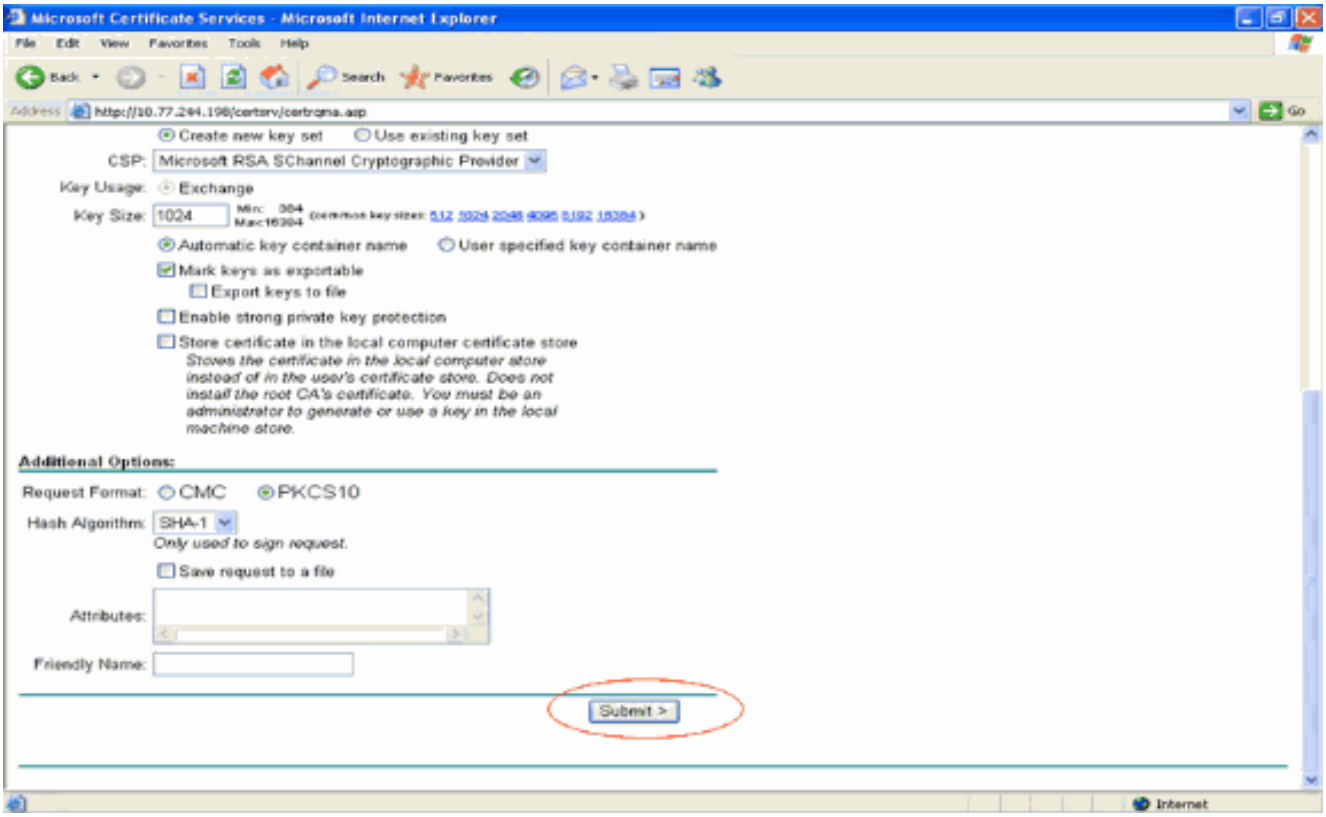


5. Nel modulo di richiesta avanzata del certificato scegliere **Utente** dal menu a discesa Modello di certificato.Nella sezione Opzioni chiave (Key options), selezionate i seguenti parametri:Immettere la Dimensione chiave nel campo Dimensione chiave. In questo esempio viene utilizzato **1024**.Selezionare l'opzione **Contrassegna le chiavi come**

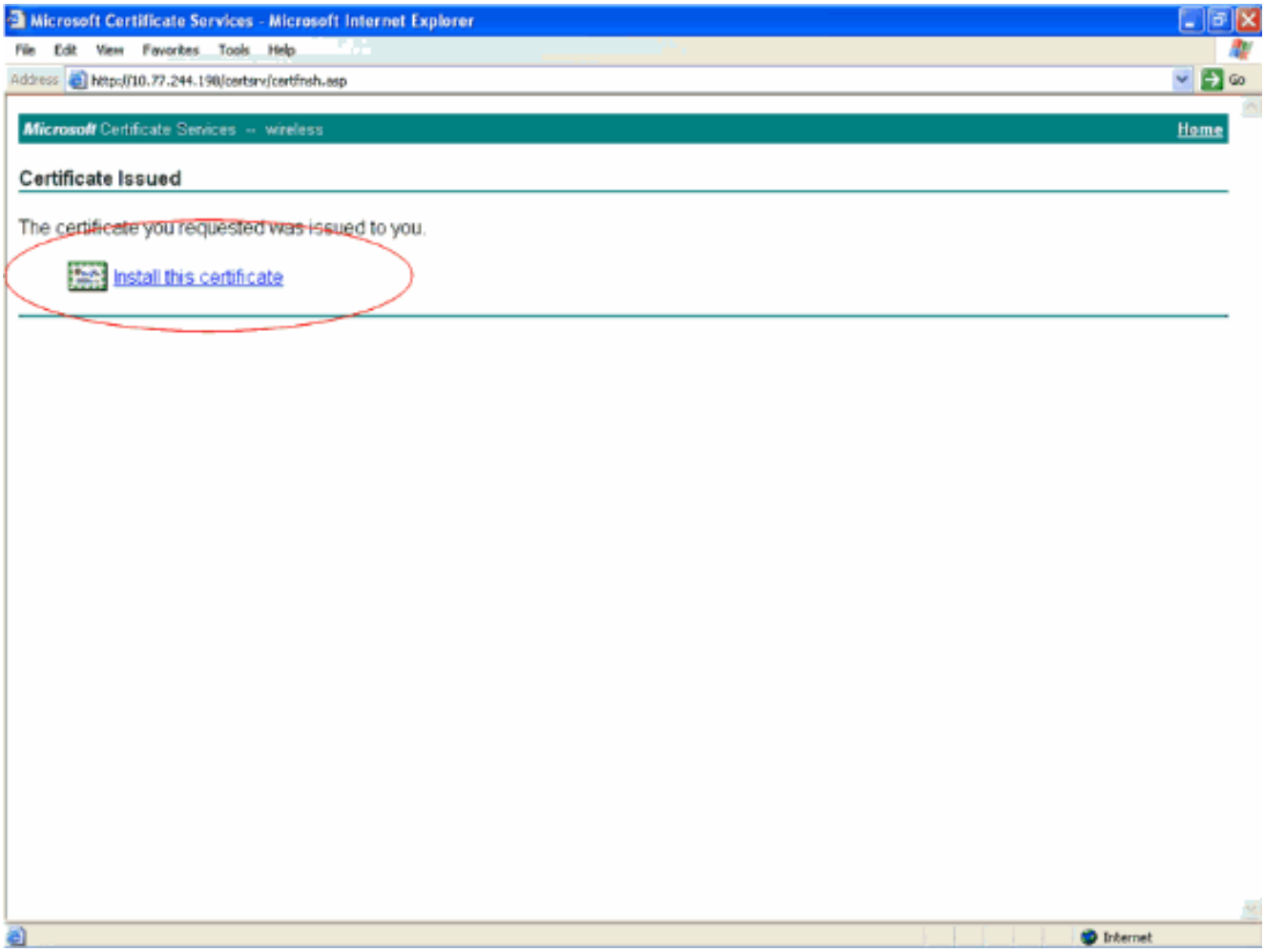
esportabili.



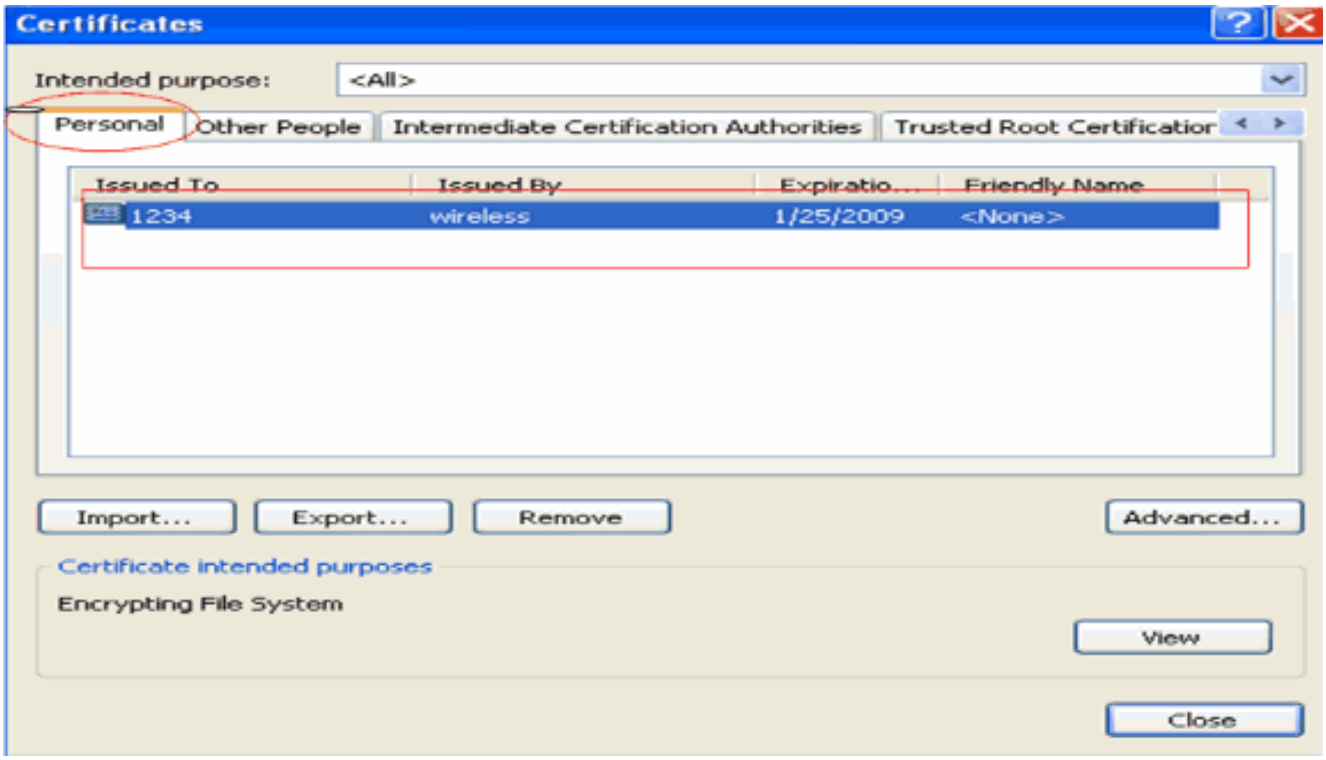
6. Configurare tutti gli altri campi necessari e fare clic su **Invia**.



7. Il certificato del dispositivo del client è ora generato in base alla richiesta. Fare clic su **Installa il certificato** per installarlo nell'archivio certificati.



8. Dovrebbe essere possibile trovare il certificato del dispositivo del client installato nell'elenco Certificati personali in **Strumenti > Opzioni Internet > Contenuto > Certificati** sul browser IE del
client.

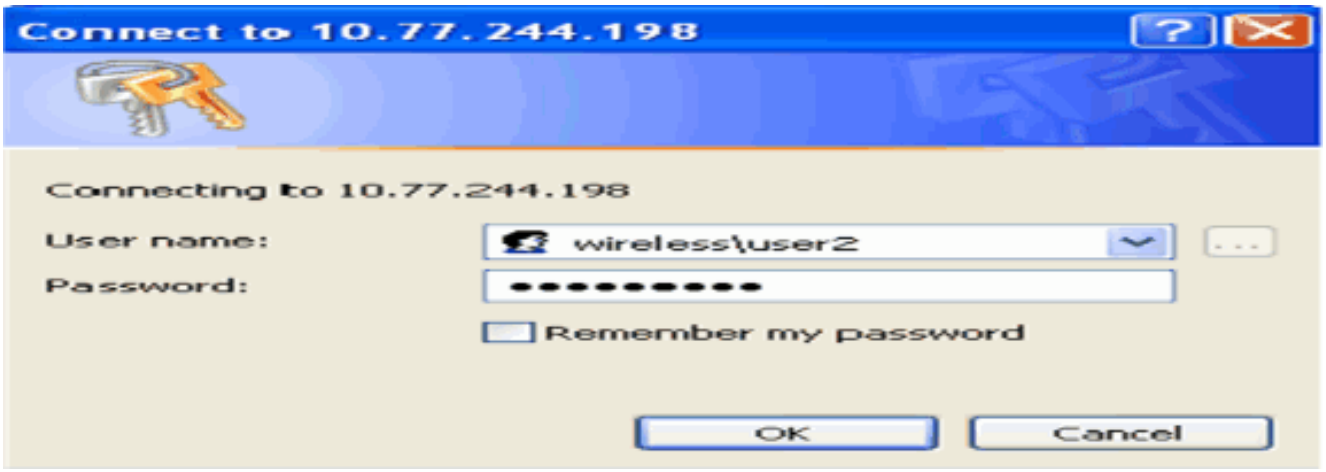


Il certificato del dispositivo per il client è installato nel client.

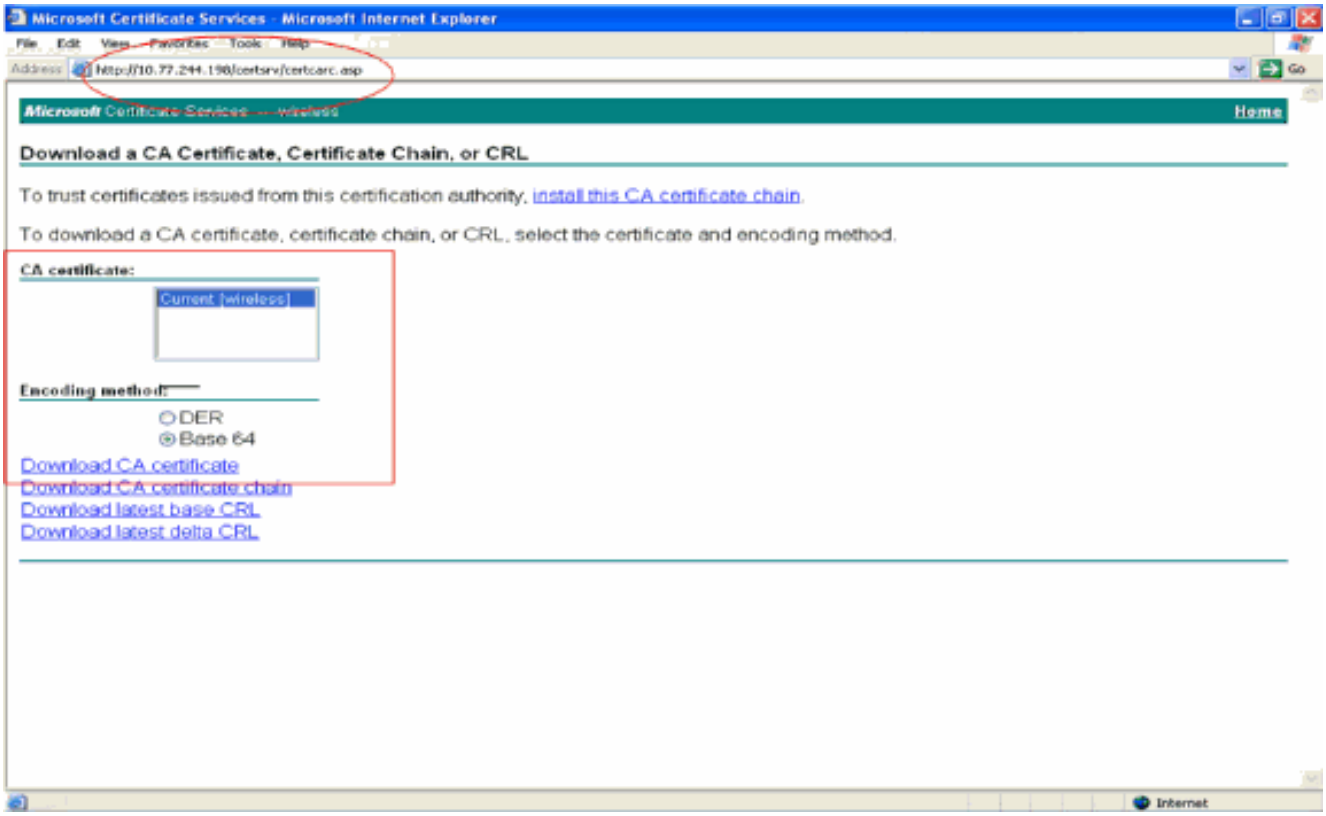
Genera il certificato CA radice per il client

Il passaggio successivo consiste nel generare il certificato CA per il client. Eseguire i seguenti passaggi dal PC client:

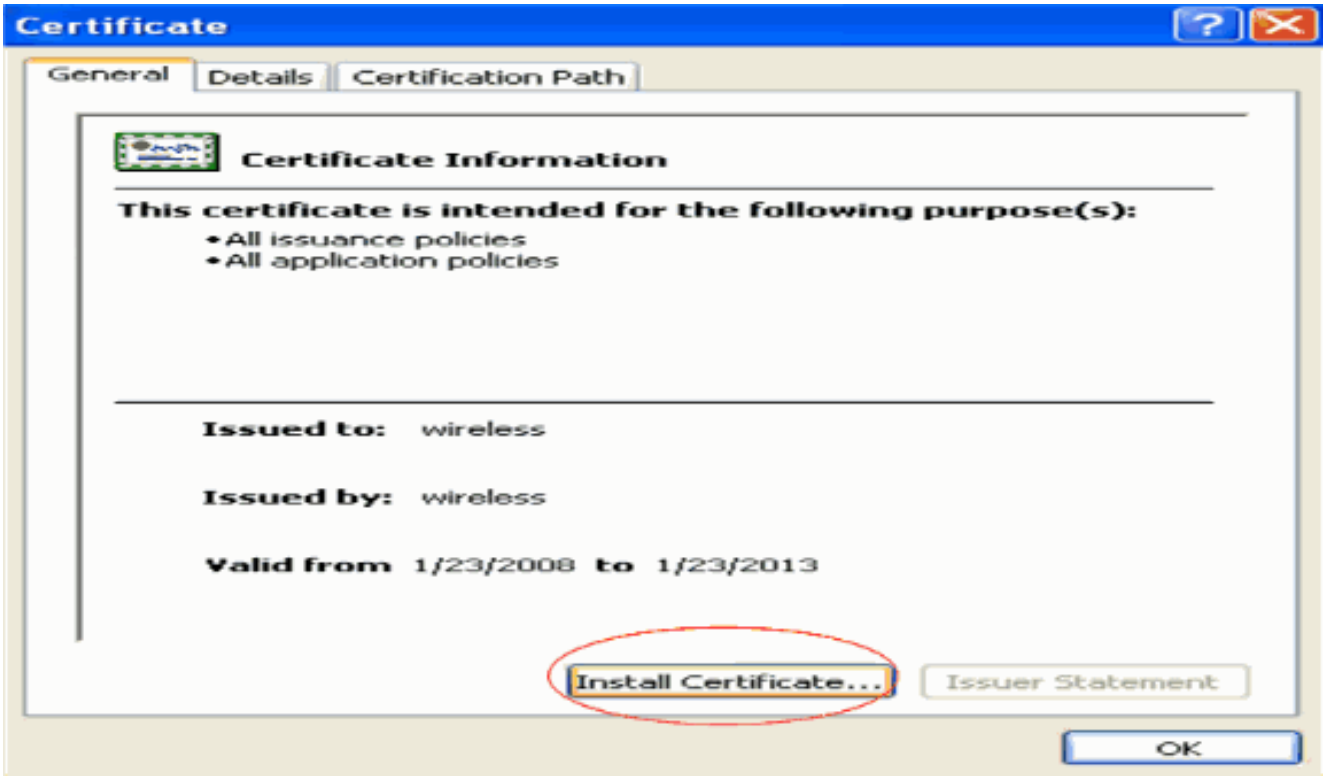
1. Visitare il sito Web all'indirizzo **http://<indirizzo IP del server CA>/certsrv** dal client che richiede l'installazione del certificato. Eseguire l'accesso come nome di dominio omeutente al server CA. Il nome utente deve corrispondere al nome dell'utente che utilizza questo computer XP e l'utente deve essere già configurato come parte dello stesso dominio del server
CA.



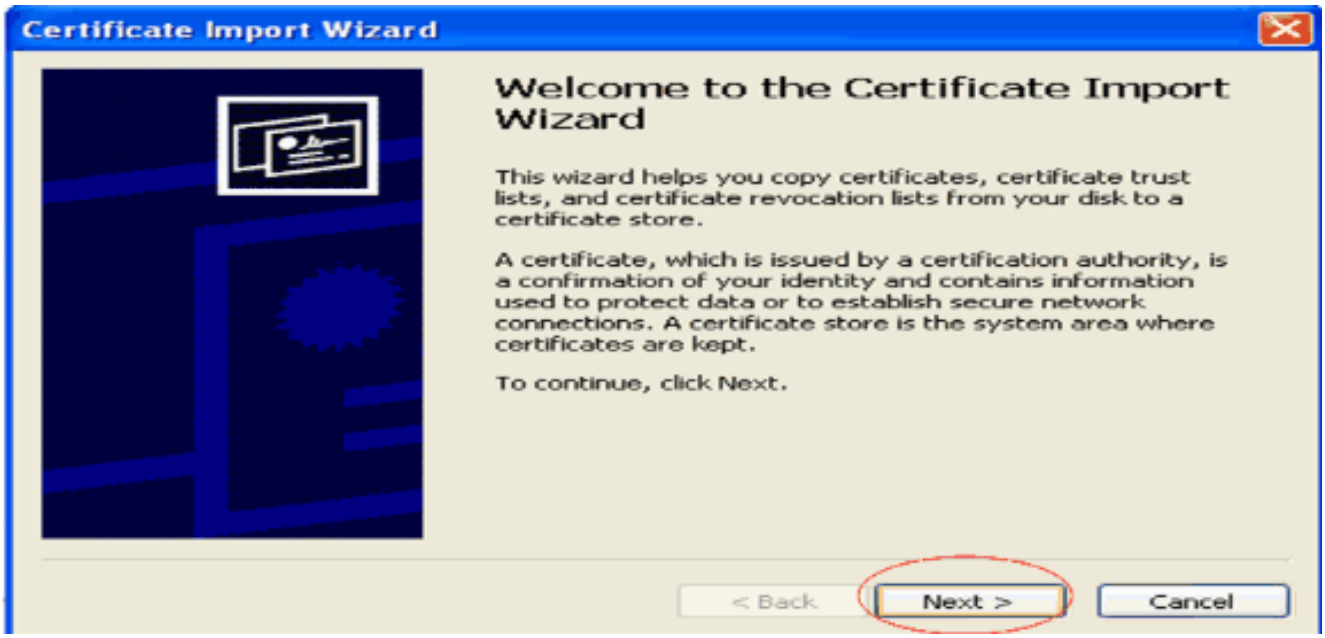
2. Nella pagina risultante è possibile visualizzare i certificati CA correnti disponibili nel server CA nella casella **Certificato CA**. Selezionate **Base 64** come metodo di codifica. Quindi, fare clic su **Scarica certificato CA** e salvare il file sul PC del client come file **.cer**. In questo esempio viene utilizzato **rootca.cer** come nome di
file.



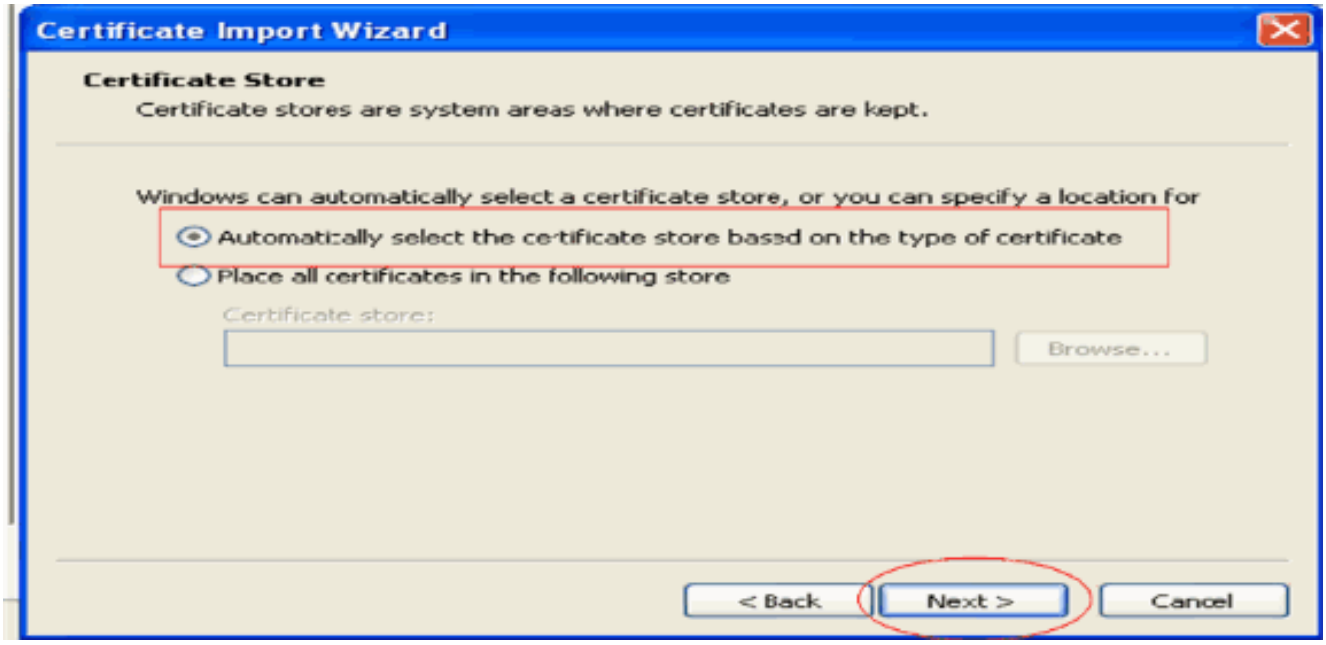
3. Installare quindi il certificato CA salvato in formato cer nell'archivio certificati del client. Fare doppio clic sul file rootca.cer e fare clic su **Installa certificato**.



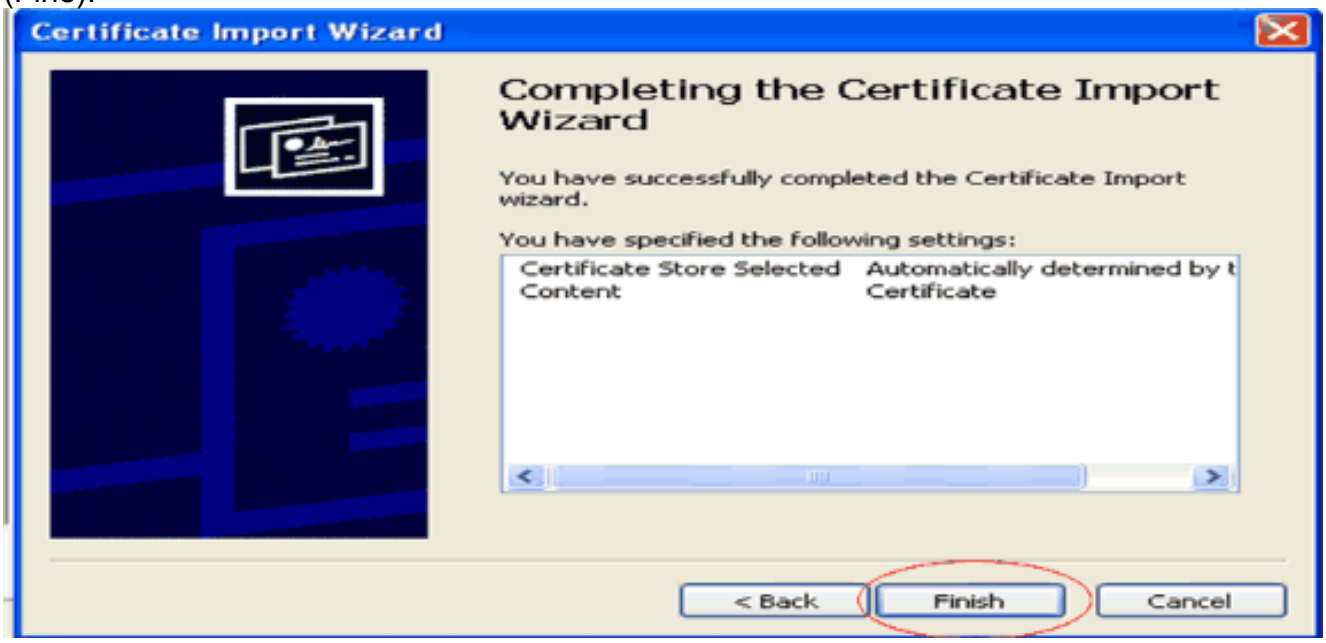
4. Fare clic su **Avanti** per importare il certificato dal disco rigido del client all'archivio certificati.



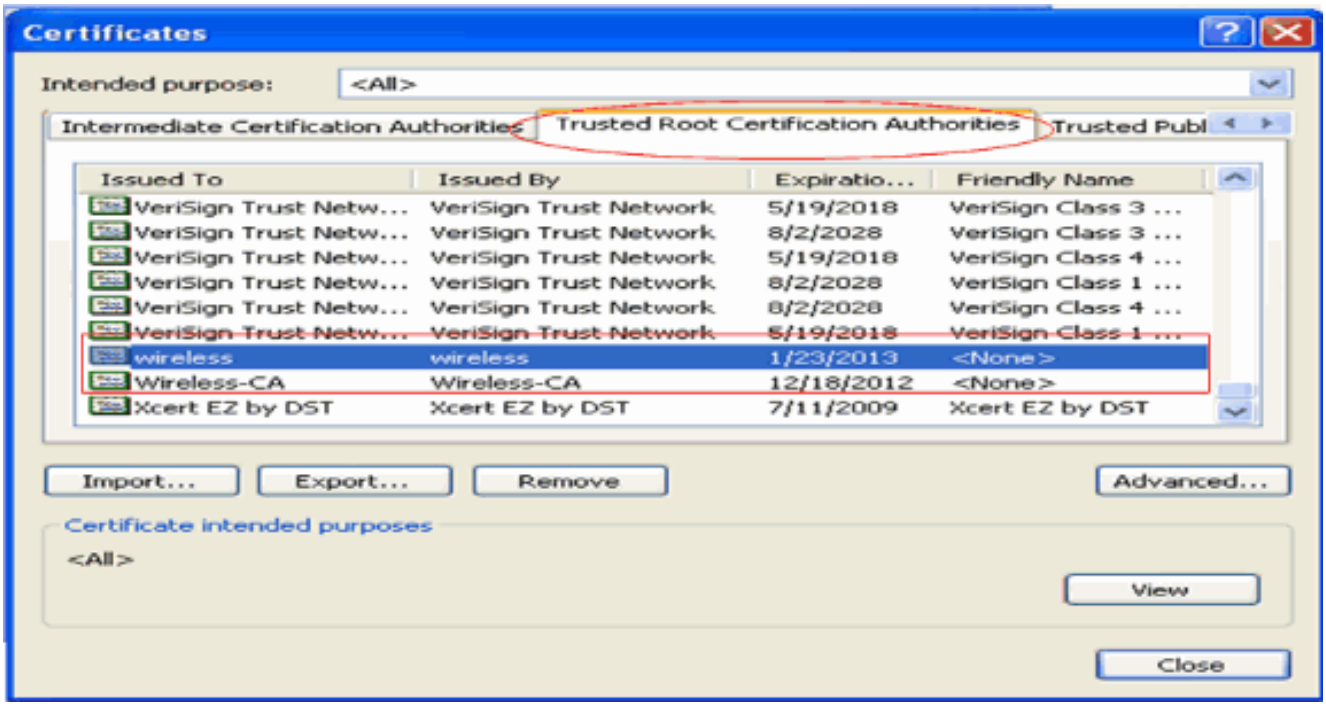
5. Scegliere **Seleziona automaticamente l'archivio certificati in base al tipo di certificato** e fare clic su
Avanti.



6. Per completare il processo di importazione, fare clic su **Finish** (Fine).



7. Per impostazione predefinita, i certificati CA vengono installati nell'elenco Autorità di certificazione radice attendibili nel browser IE del client in **Strumenti > Opzioni Internet > Contenuto > Certificati**. Di seguito è riportato l'esempio:

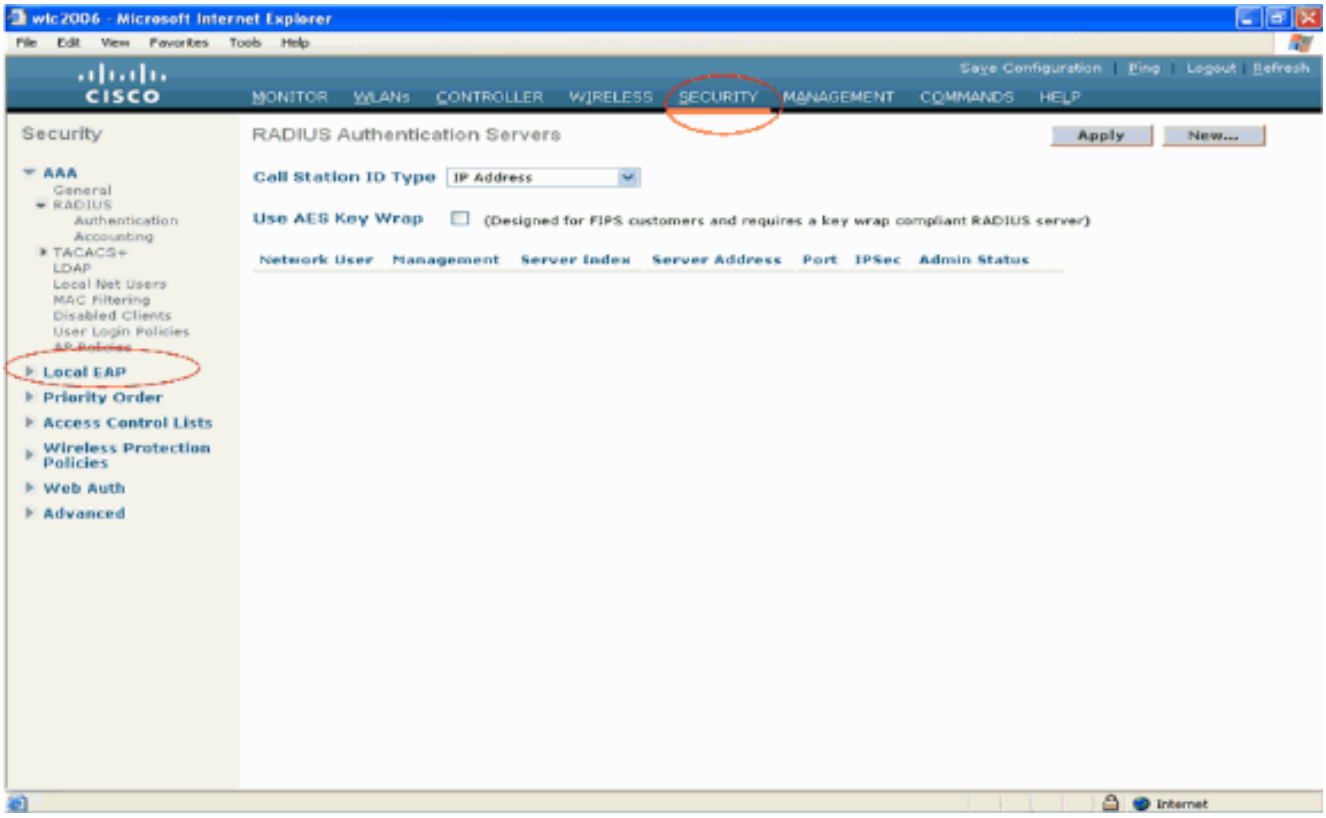


Tutti i certificati richiesti vengono installati sul WLC e sul client per l'autenticazione EAP locale EAP-FAST. Il passaggio successivo è configurare il WLC per l'autenticazione EAP locale.

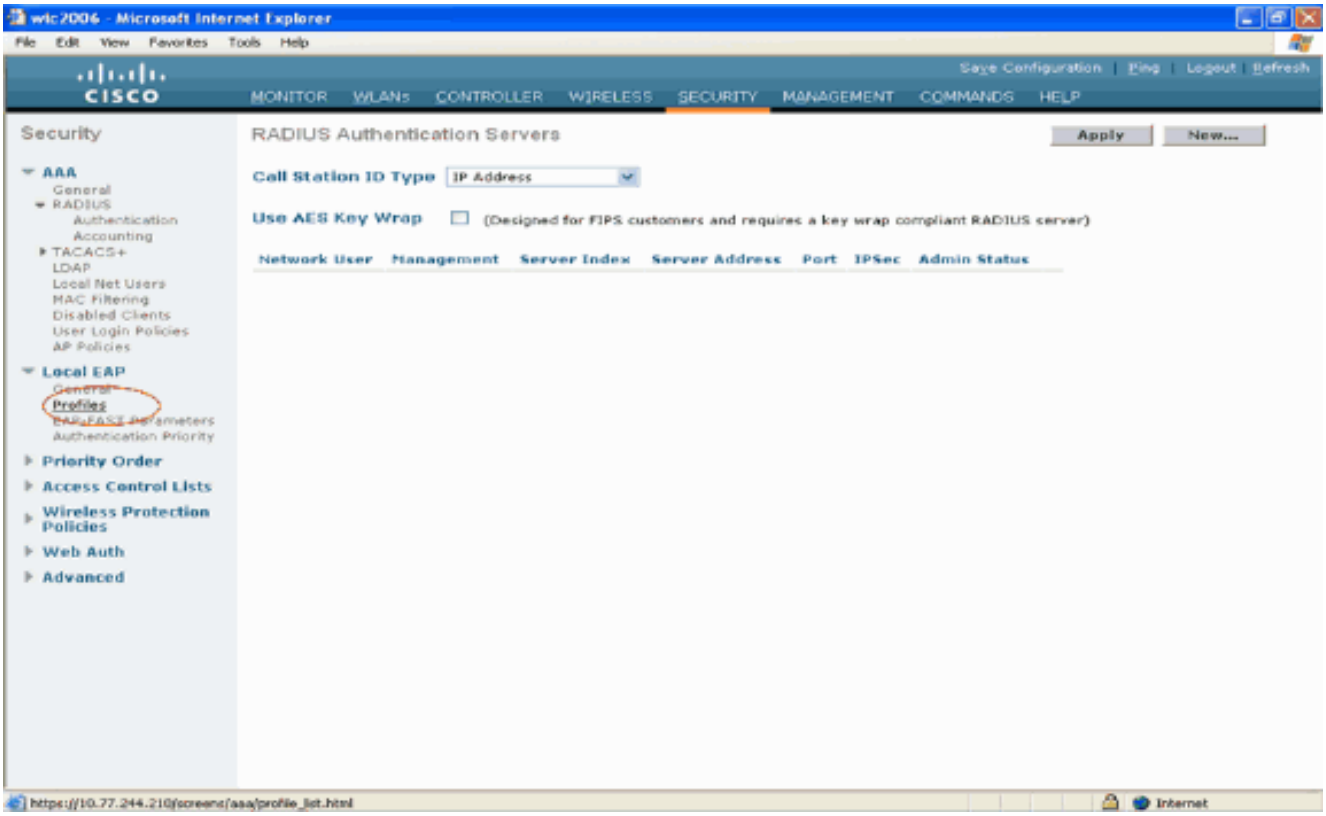
Configurazione di EAP locale sul WLC

Completare questa procedura dalla **modalità GUI** del **WLC** per configurare l'autenticazione EAP locale sul WLC:

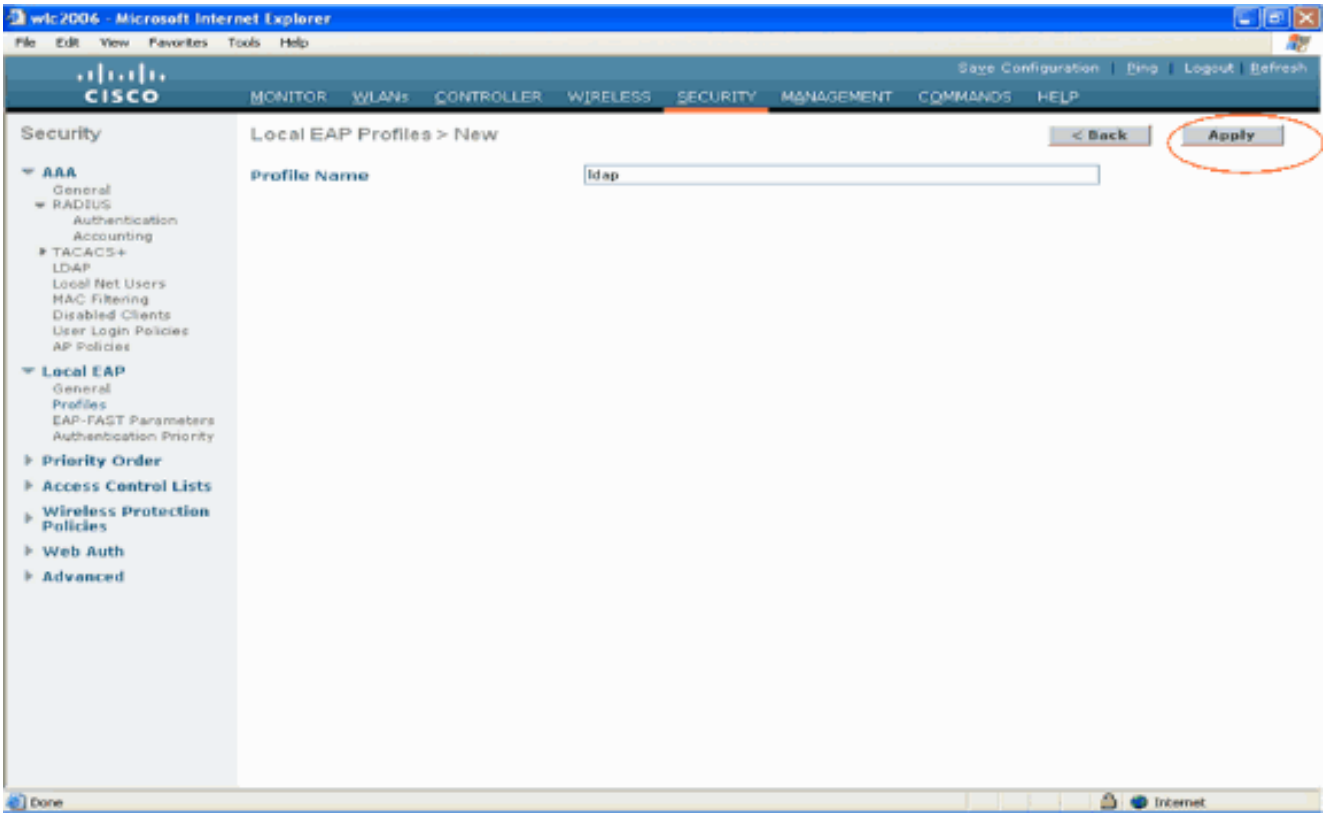
1. Fare clic su **Protezione > EAP locale**.



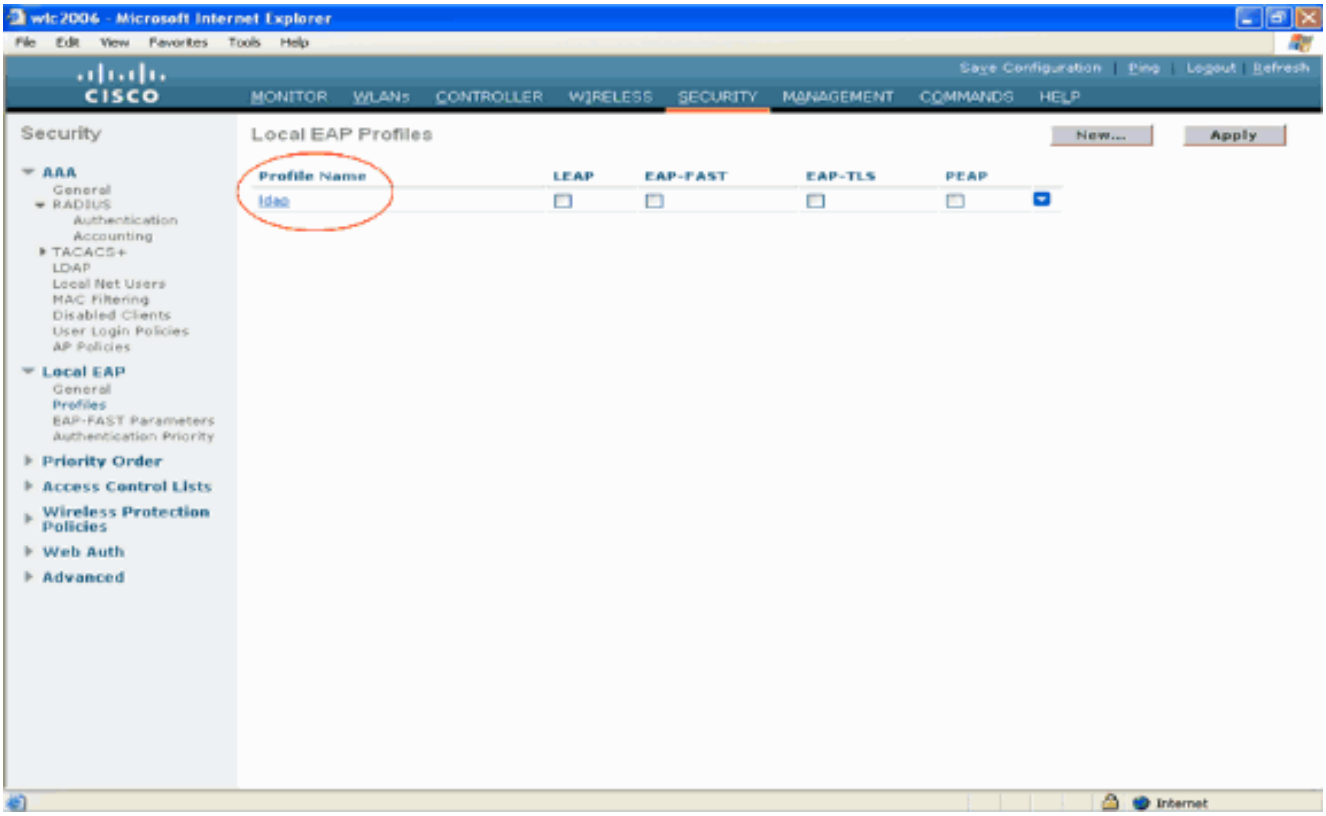
2. In EAP locale fare clic su **Profili** per configurare il profilo EAP locale.



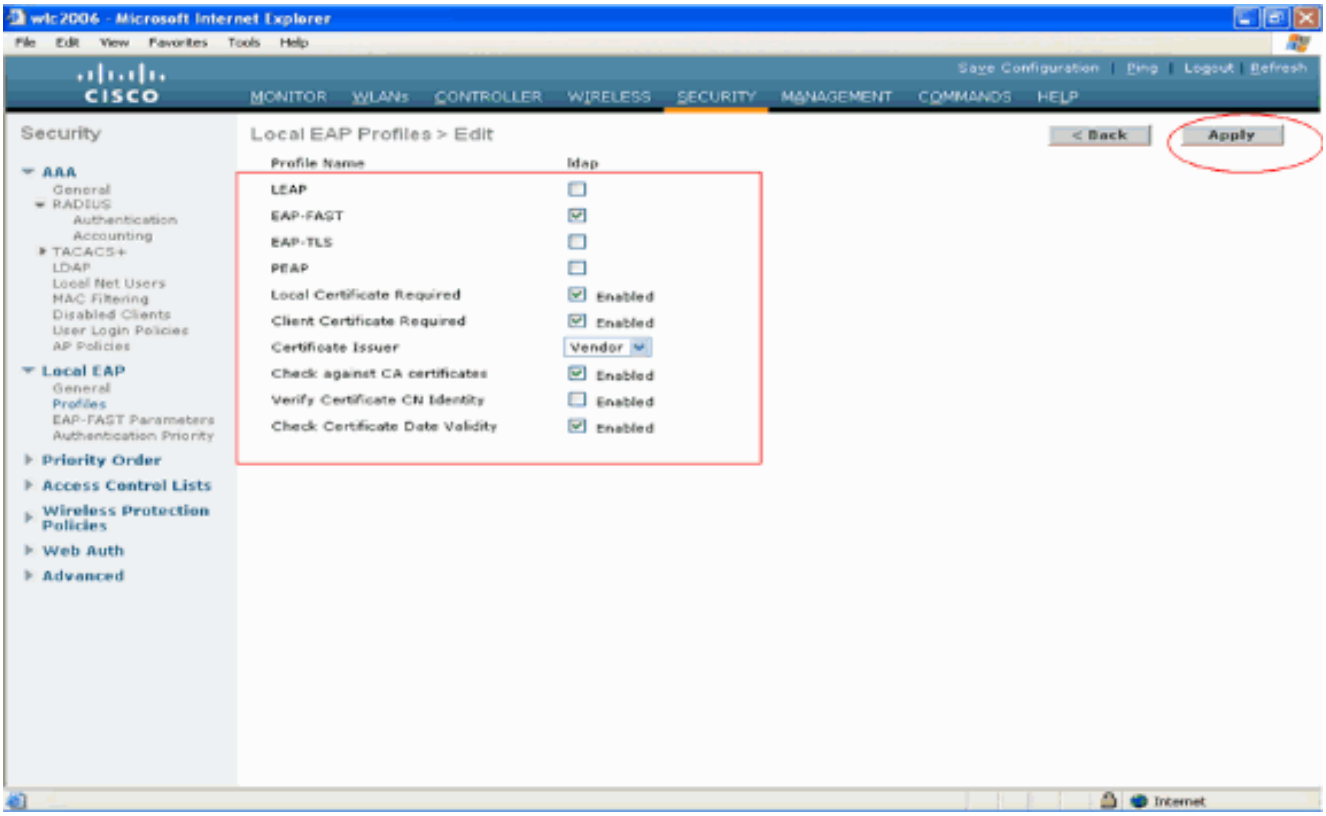
3. Per creare un nuovo profilo EAP locale, fare clic su **New** (Nuovo).
4. Configurare un nome per il profilo e fare clic su **Applica**. In questo esempio, il nome del profilo è **ldap**. In questo modo è possibile accedere ai profili EAP locali creati sul WLC.



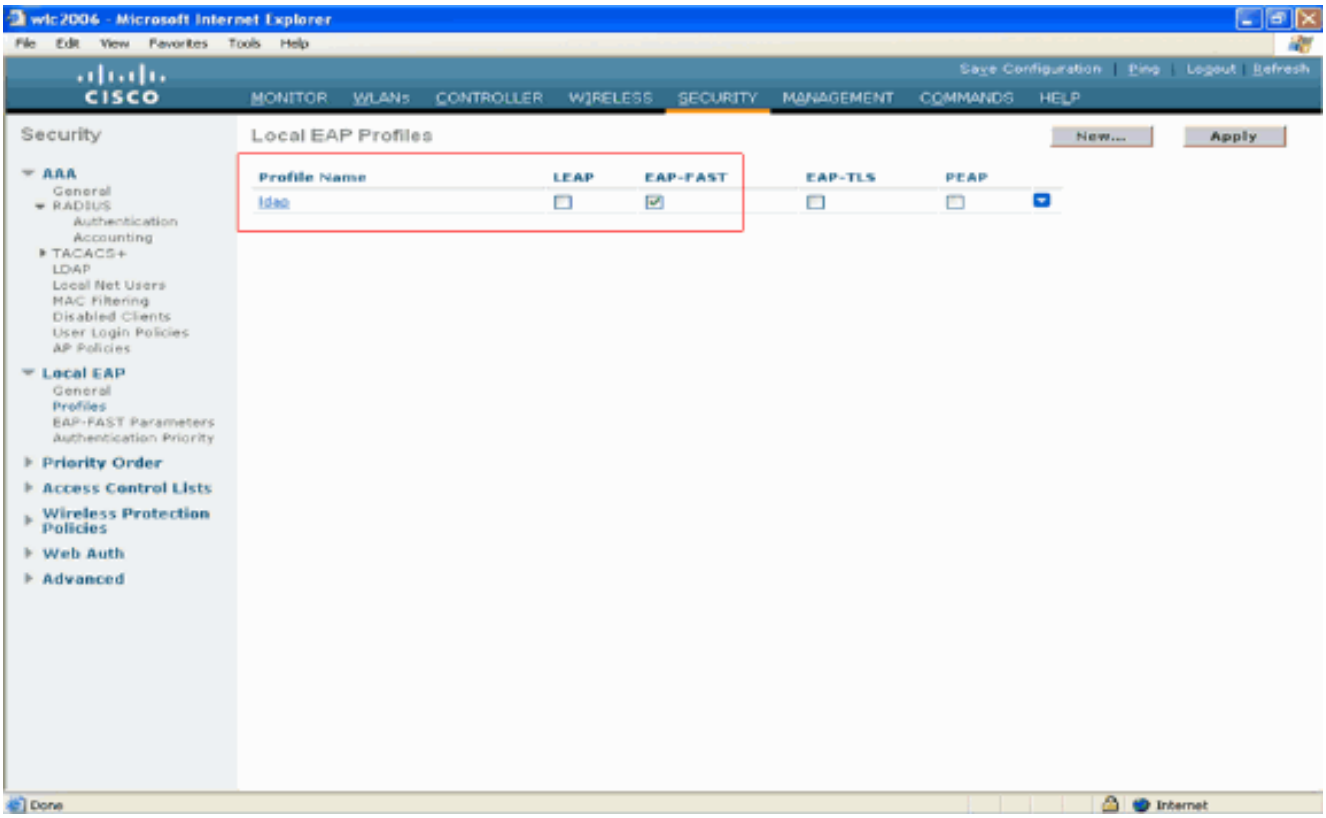
5. Fare clic sul profilo **ldap** appena creato, che viene visualizzato nel campo Nome profilo della pagina Profili EAP locali. Viene visualizzata la pagina **Profili EAP locali > Modifica**.



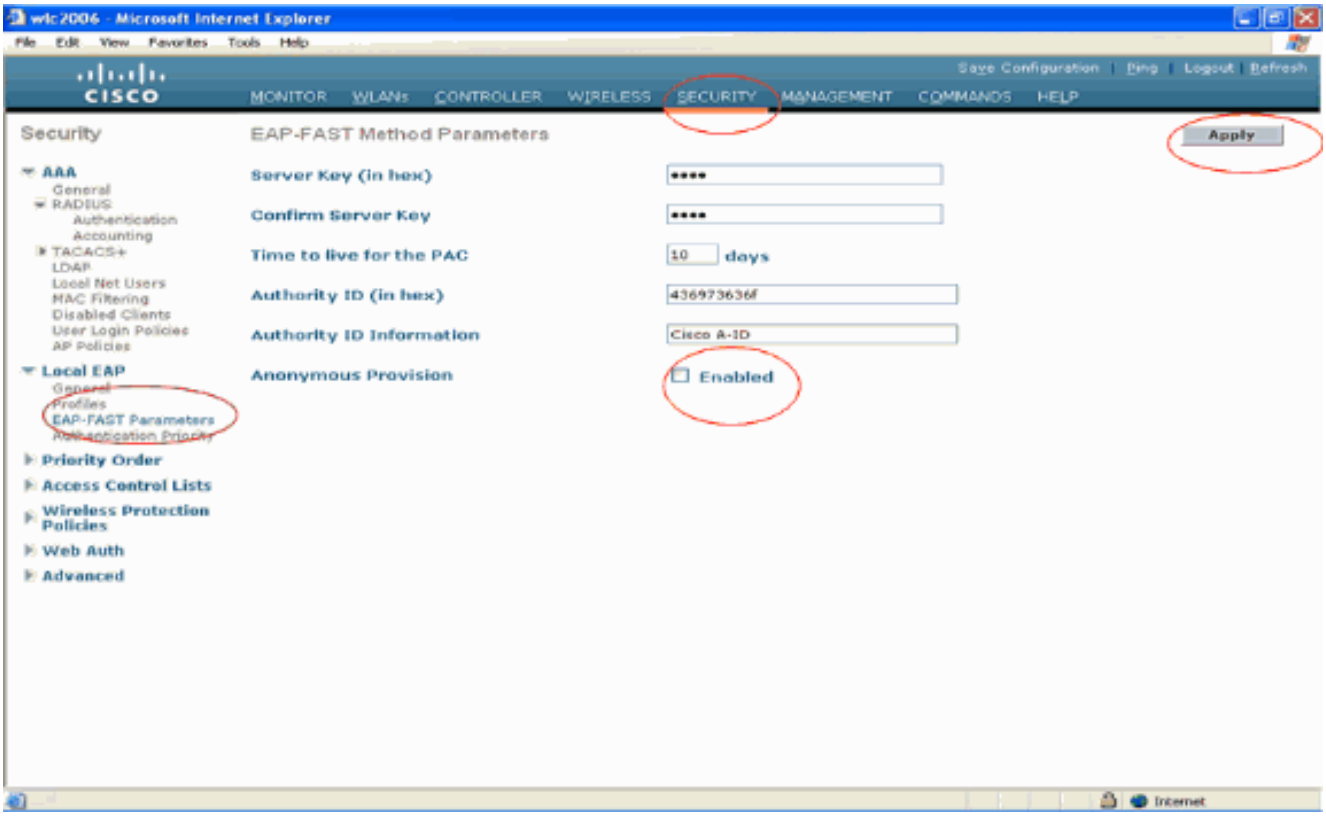
6. Configurare i parametri specifici del profilo nella pagina **Profili EAP locali > Modifica**.Scegliere **EAP-FAST** come metodo di autenticazione EAP locale.Selezionare le caselle di controllo **Certificato locale richiesto** e **Certificato client richiesto**.Selezionare **Fornitore** come Autorità di certificazione perché il documento utilizza un server CA di terze parti.Selezionare la casella di controllo accanto a **Controlla rispetto ai certificati CA** per consentire la convalida del certificato in ingresso dal client rispetto ai certificati CA sul controller.Se si desidera che il nome comune (CN) nel certificato in ingresso venga convalidato rispetto al CN dei certificati CA nel controller, selezionare la casella di controllo **Verifica identità CN certificato**. L'impostazione predefinita è disattivata. Per consentire al controller di verificare che il certificato del dispositivo in ingresso sia ancora valido e non sia scaduto, selezionare la casella di controllo **Controlla validità data certificato**.**Nota:** la validità della data del certificato viene verificata in base all'ora UTC (GMT) corrente configurata sul controller. La differenza di fuso orario viene ignorata.Fare clic su **Apply** (Applica).



7. Il profilo EAP locale con autenticazione EAP-FAST viene ora creato sul WLC.



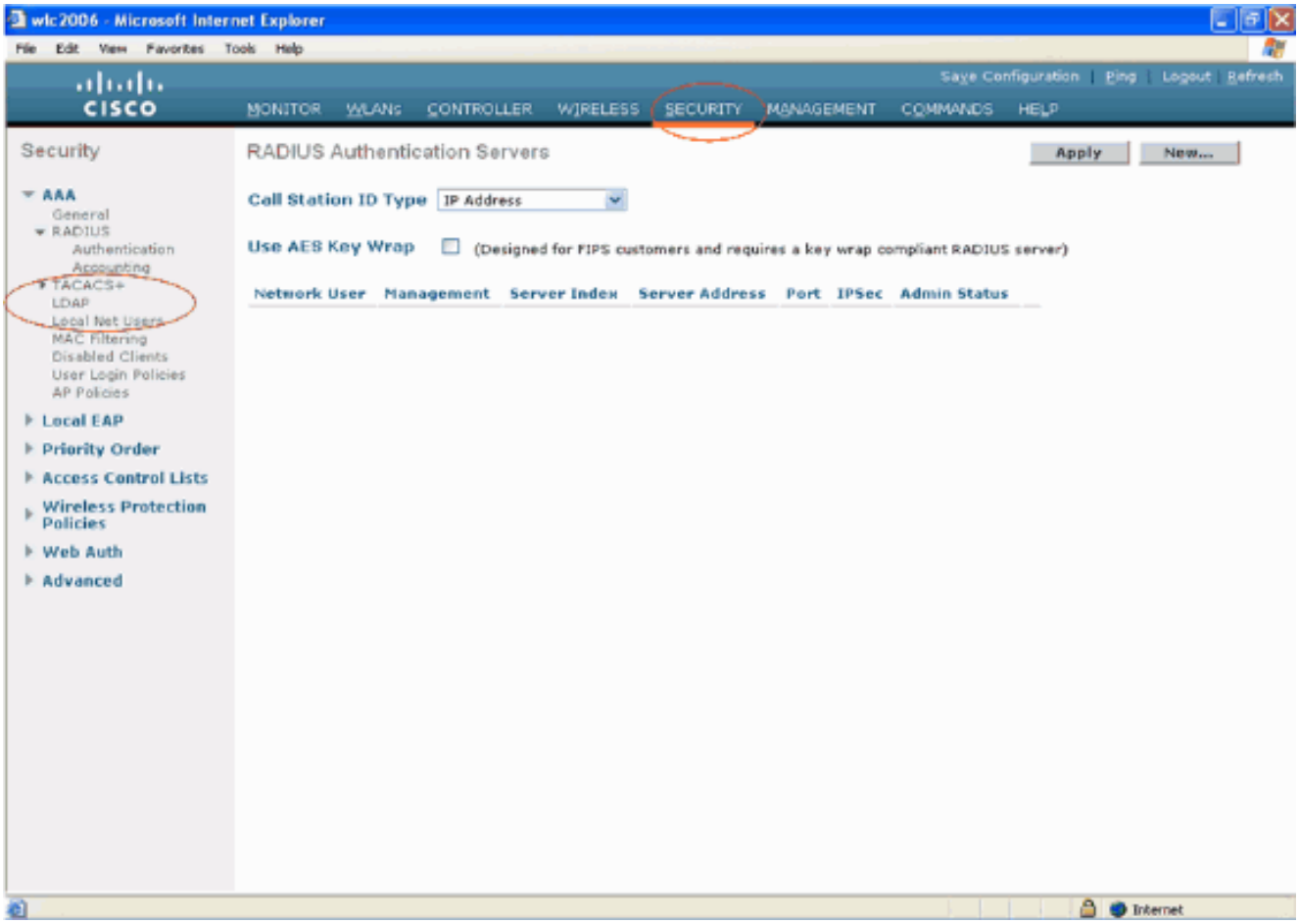
8. Il passaggio successivo è la configurazione di parametri specifici di EAP-FAST sul WLC. Nella pagina Sicurezza WLC, fare clic su **EAP locale > Parametri EAP-FAST** per passare alla pagina Parametri del metodo EAP-FAST.Deselezionare la casella di controllo **Provisioning anonimo** in quanto in questo esempio viene spiegato come utilizzare i certificati EAP-FAST. Mantenere tutti gli altri parametri ai valori predefiniti. Fare clic su **Apply** (Applica).



Configura WLC con dettagli del server LDAP

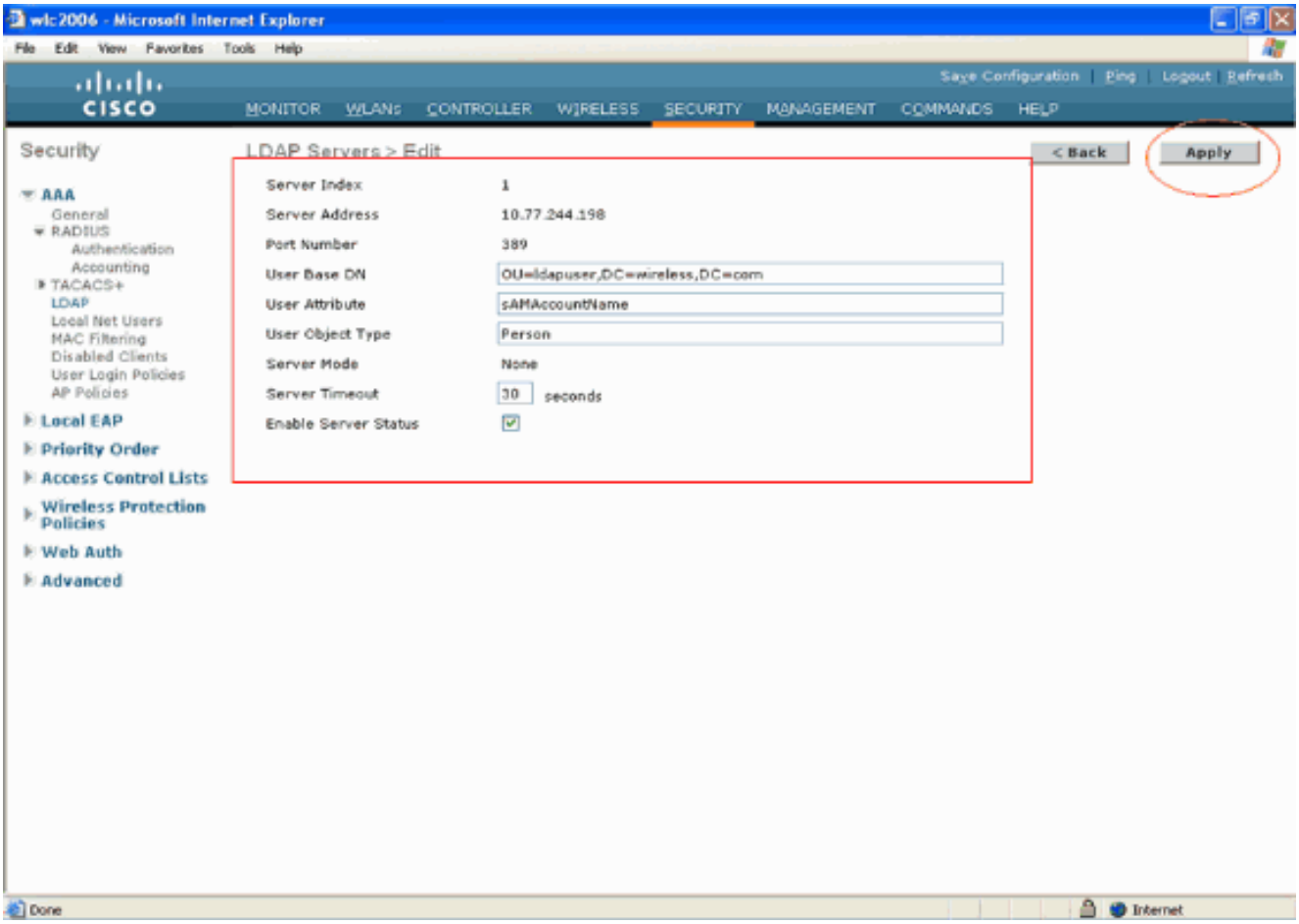
Ora che il WLC è stato configurato con il profilo EAP locale e le informazioni correlate, il passaggio successivo è configurare il WLC con i dettagli del server LDAP. Completare questi passaggi sul WLC:

1. Nella pagina **Sicurezza** del WLC, selezionare **AAA > LDAP** dal riquadro attività a sinistra per passare alla pagina di configurazione del server LDAP. Per aggiungere un server LDAP, fare clic su **Nuovo**. Viene visualizzata la pagina **Server LDAP > Nuovo**.



2. Nella pagina Server LDAP: Modifica, specificare i dettagli del server LDAP, ad esempio l'indirizzo IP del server LDAP, il numero di porta, lo stato Abilita server e così via.Scegliere un numero dalla casella a discesa **Indice server (priorità)** per specificare l'ordine di priorità di questo server in relazione agli altri server LDAP configurati. È possibile configurare fino a diciassette server. Se il controller non riesce a raggiungere il primo server, proverà con il secondo nell'elenco e così via.Immettere l'indirizzo IP del server LDAP nel campo **Indirizzo IP server**.Immettere il numero della porta TCP del server LDAP nel campo **Numero porta**. L'intervallo valido è compreso tra 1 e 65535 e il valore predefinito è **389**.Nel campo **DN base utente**, immettere il nome distinto (DN) della sottostruttura nel server LDAP che contiene un elenco di tutti gli utenti. Ad esempio, ou=unità organizzativa, ou=unità organizzativa successiva e o=corporation.com. Se la struttura contenente gli utenti è il DN di base, immettere o=corporation.com o dc=corporation, dc=com.In questo esempio, l'utente si trova nell'unità organizzativa **ldapuser** che a sua volta viene creata come parte del dominio **Wireless.com**.Il DN di base dell'utente deve puntare al percorso completo in cui si trovano le informazioni utente (credenziali utente in base al metodo di autenticazione EAP-FAST). In questo esempio, l'utente si trova nel DN di base OU=ldapuser, DC=Wireless, DC=com.Per ulteriori informazioni sull'unità organizzativa e sulla configurazione degli utenti, vedere la sezione Creazione di utenti sul controller di dominio in questo documento.Nel campo **Attributo utente**, immettere il nome dell'attributo nel record utente che contiene il nome utente.Nel campo **Tipo oggetto utente**, immettere il valore dell'attributo objectType LDAP che identifica il record come utente. I record utente dispongono spesso di diversi valori per l'attributo objectType, alcuni dei quali sono univoci per l'utente e altri sono condivisi con altri tipi di oggetto.**Nota:** è possibile ottenere il valore di questi due campi dal server delle directory con l'utilità browser LDAP, inclusa negli strumenti di supporto di Windows 2003. **Questo strumento del browser LDAP Microsoft è denominato LDP.** Con l'aiuto di questo strumento, è possibile conoscere i campi DN base utente, Attributo utente e Tipo oggetto

utente di questo particolare utente. Per informazioni dettagliate sull'utilizzo di LDP per conoscere questi attributi specifici dell'utente, vedere la sezione Utilizzo di LDP per identificare gli attributi utente in questo documento.Selezionare **Protetto** dall'elenco a discesa Modalità server se si desidera che tutte le transazioni LDAP utilizzino un tunnel TLS sicuro. In caso contrario, scegliere **Nessuno**, che è l'impostazione predefinita.Nel campo **Timeout server**, immettere il numero di secondi che devono intercorrere tra le ritrasmissioni. L'intervallo valido è compreso tra 2 e 30 secondi e il valore predefinito è 2 secondi.Selezionare la casella di controllo **Abilita stato server** per abilitare il server LDAP oppure deselezionarla per disabilitarlo. Il valore predefinito è disattivato.Fare clic su **Applica** per eseguire il commit delle modifiche.Di seguito è riportato un esempio già configurato con queste
informazioni:

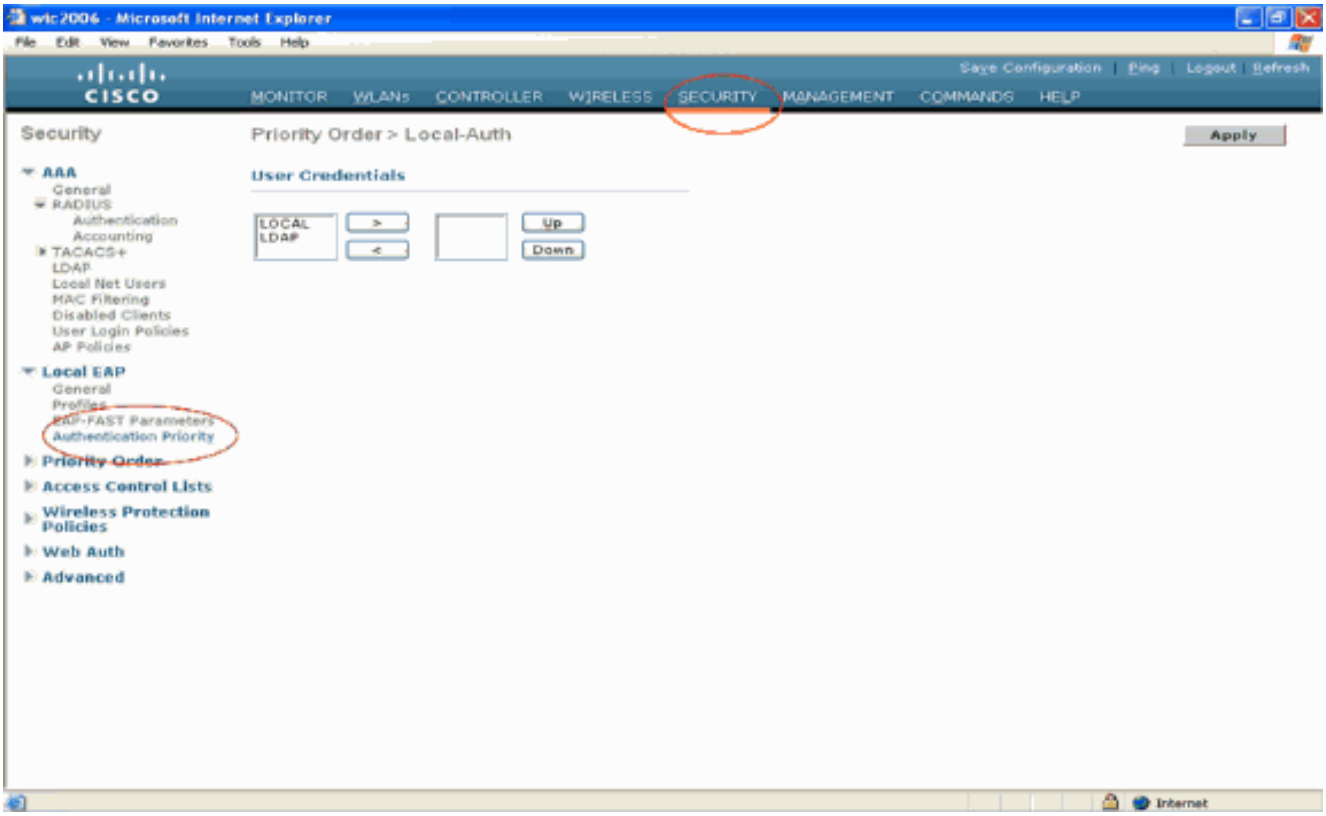


Ora che i dettagli sul server LDAP sono stati configurati sul WLC, il passo successivo consiste nel configurare LDAP come database backend di priorità in modo che il WLC cerchi innanzitutto le credenziali utente nel database LDAP anziché in qualsiasi altro database.

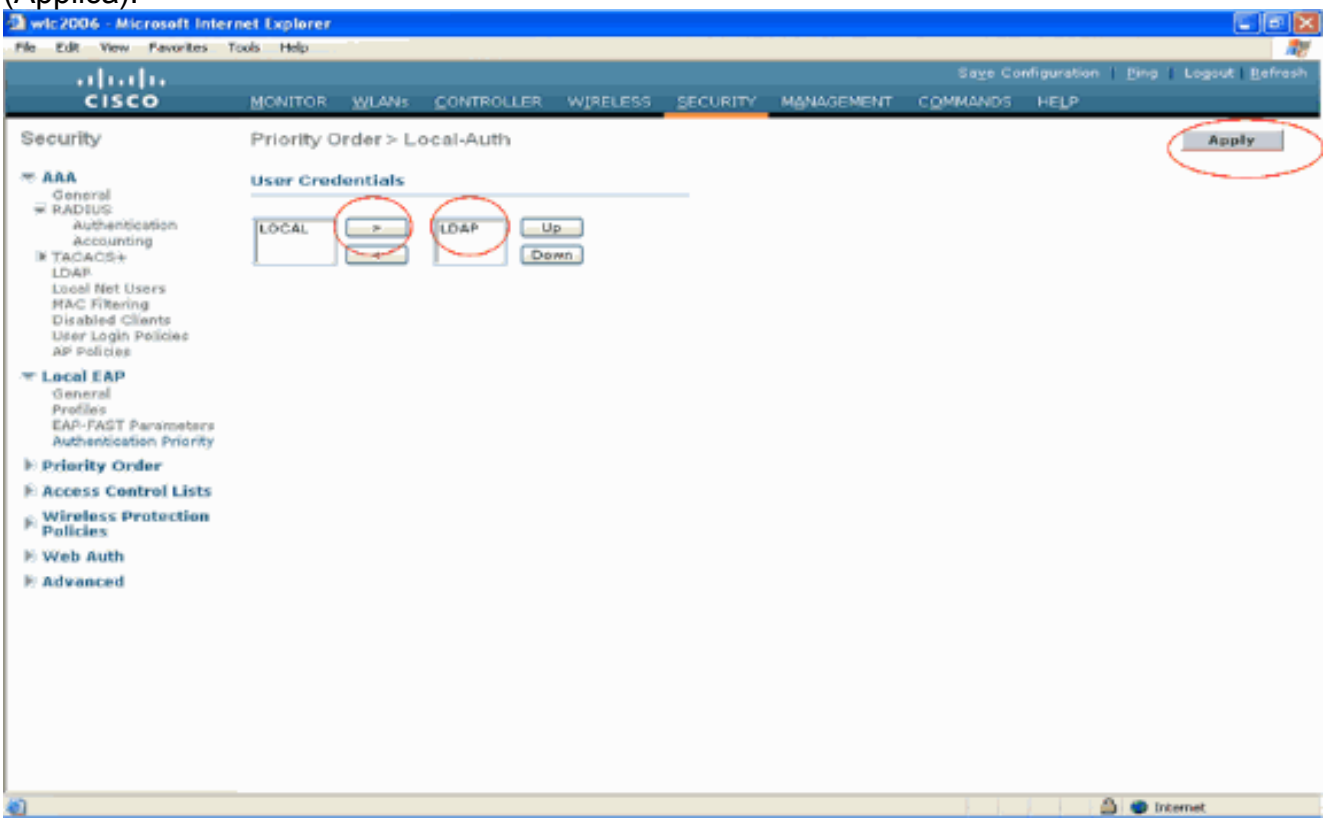
Configurare LDAP come database backend di priorità

Completare questi passaggi sul WLC per configurare LDAP come database backend di priorità:

1. Nella pagina Protezione, fare clic su **EAP locale > Priorità di autenticazione**. Nella pagina Ordine di priorità > Autenticazione locale è possibile trovare due database (Locale e LDAP) in grado di memorizzare le credenziali dell'utente.Per impostare LDAP come database con priorità, scegliere **LDAP** dalla casella di sinistra delle credenziali utente e fare clic sul pulsante **>** per spostare LDAP nella casella di destra dell'ordine di
priorità.



2. Questo esempio mostra chiaramente che LDAP è selezionato nella casella laterale sinistra e che il pulsante **>** è selezionato. Di conseguenza, LDAP viene spostato nella casella sul lato destro che decide la priorità. Il database LDAP viene scelto come database con priorità di autenticazione.Fare clic su **Apply**
(Applica).



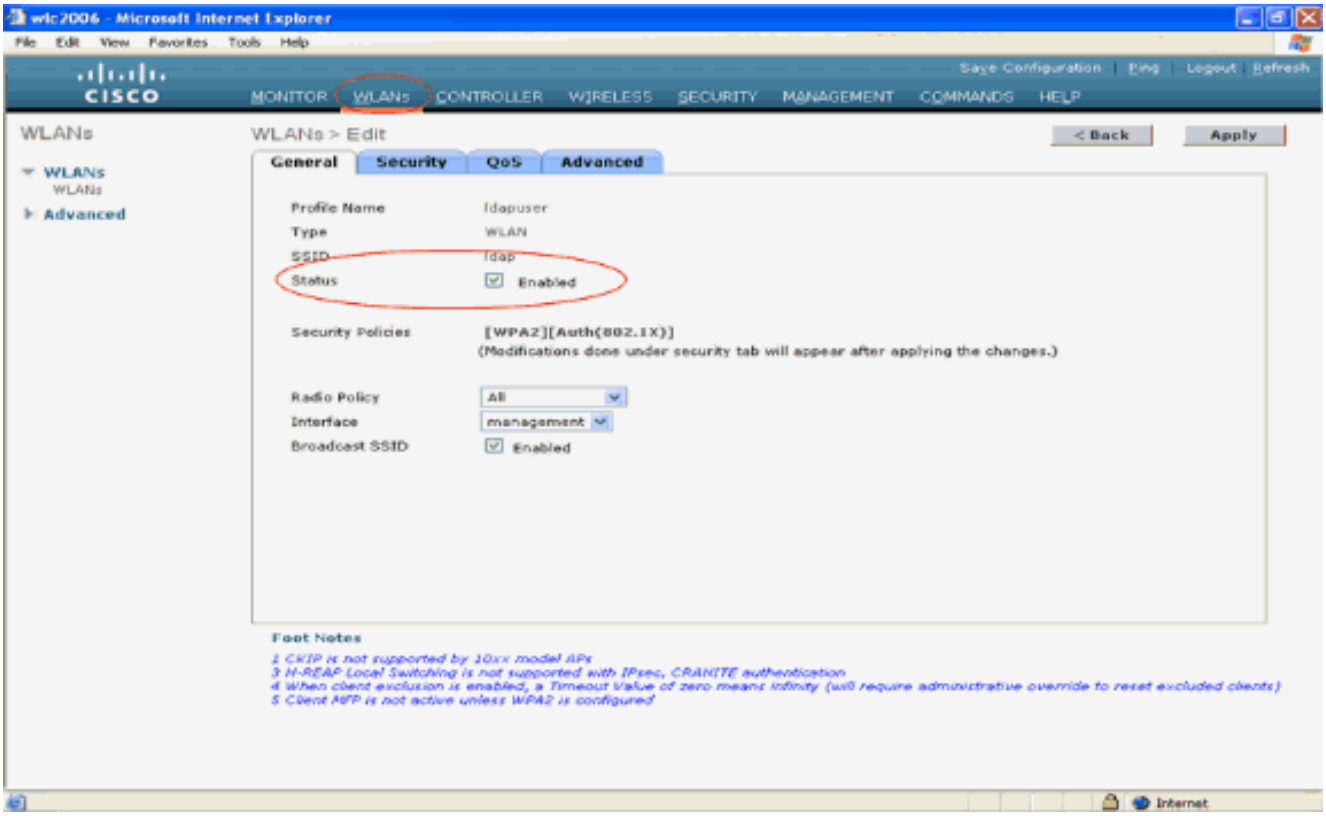
Nota: se sia LDAP che LOCAL vengono visualizzati nella casella Credenziali utente di destra con LDAP nella parte superiore e LOCAL nella parte inferiore, Local EAP tenta di autenticare i client utilizzando il database backend LDAP e esegue il failover al database utente locale se i server LDAP non sono raggiungibili. Se l'utente non viene trovato, il tentativo di autenticazione verrà rifiutato. Se LOCAL si trova nella parte superiore, EAP locale tenta di

eseguire l'autenticazione utilizzando solo il database degli utenti locale. Non esegue il failover nel database back-end LDAP.

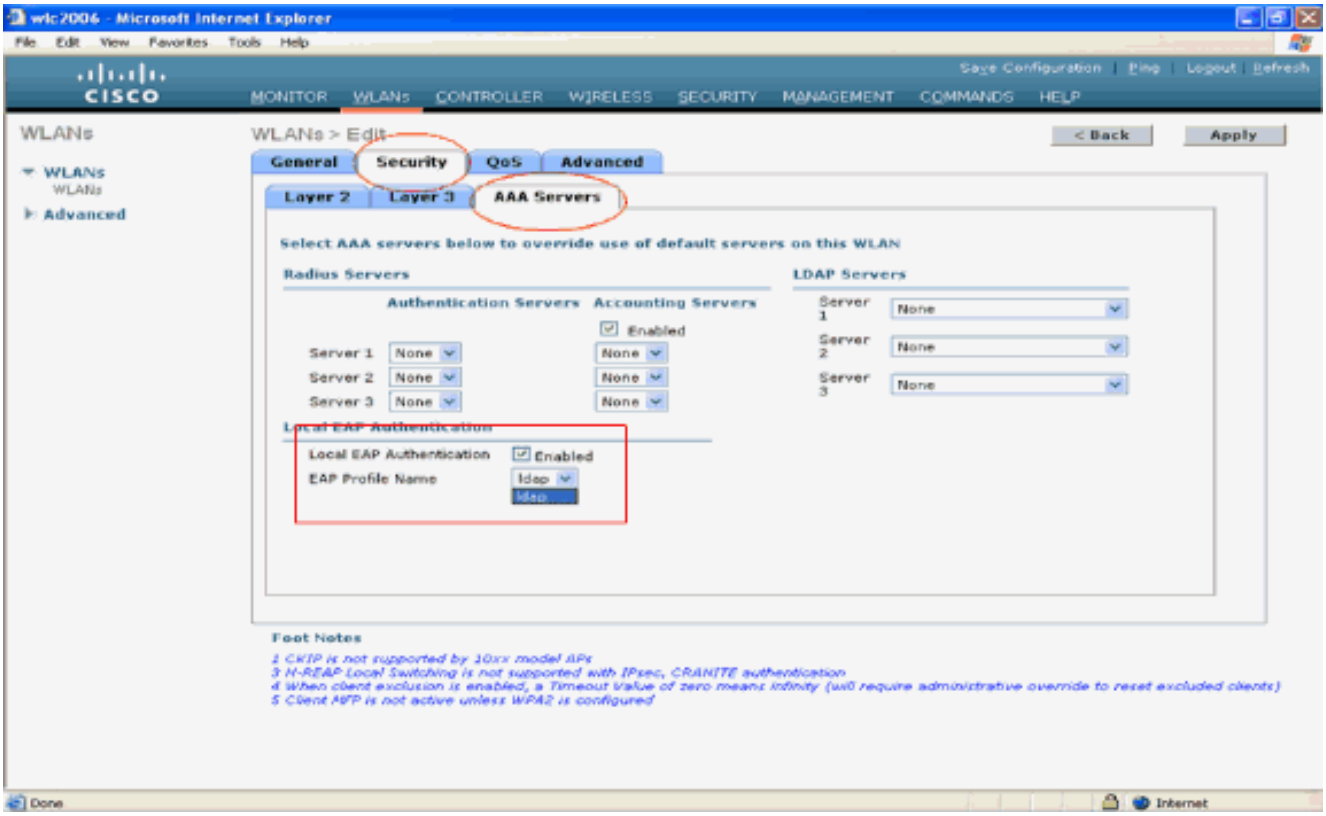
Configurazione della WLAN sul WLC con autenticazione EAP locale

L'ultimo passaggio del WLC è configurare una WLAN che utilizza l'EAP locale come metodo di autenticazione con LDAP come database backend. Attenersi alla procedura seguente:

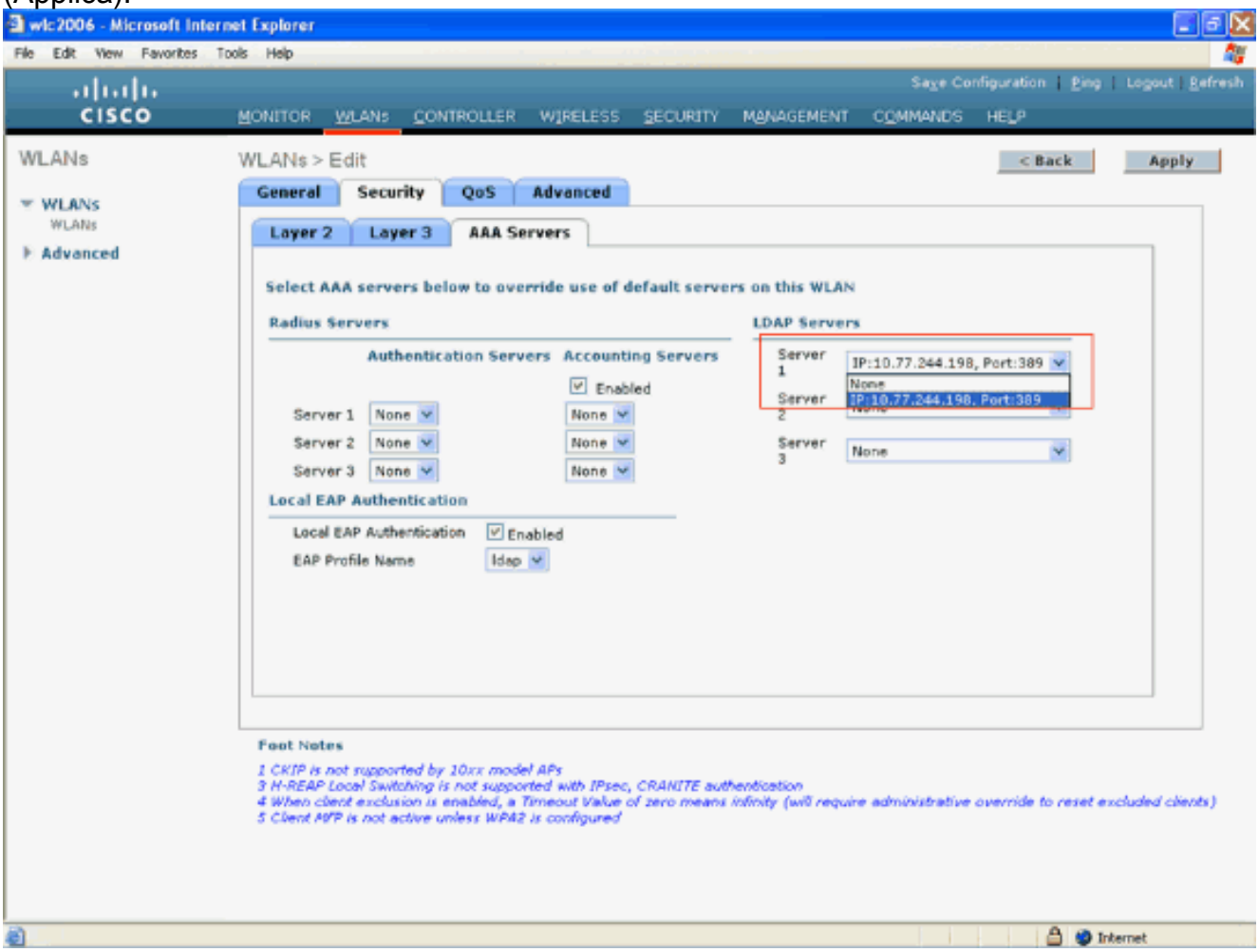
1. Dal menu principale del controller, fare clic su **WLAN** per passare alla pagina di configurazione delle WLAN. Per creare una nuova WLAN, nella pagina WLAN fare clic su **New** (Nuova). In questo esempio viene creato un nuovo **LDAP** WLAN.Fare clic su **Apply** (Applica). Il passaggio successivo consiste nel configurare i parametri WLAN nella pagina WLAN > Edit (Modifica).
2. Nella pagina di modifica della WLAN, abilitare lo stato della WLAN. Configurare tutti gli altri parametri
necessari.



3. Per configurare i parametri relativi alla sicurezza per la WLAN, fare clic su **Sicurezza**. In questo esempio viene utilizzata la sicurezza di layer 2 come 802.1x con WEP dinamico a 104 bit.**Nota:** questo documento utilizza 802.1x con l'esempio di WEP dinamico. Si consiglia di utilizzare metodi di autenticazione più sicuri, ad esempio WPA/ WPA2.
4. Nella pagina Configurazione della sicurezza WLAN, fare clic **sulla** scheda **Server AAA**. Nella pagina Server AAA, abilitare il metodo di autenticazione EAP locale e scegliere **ldap** dall'elenco a discesa corrispondente al parametro Nome profilo EAP. Questo è il profilo EAP locale creato in questo
esempio.

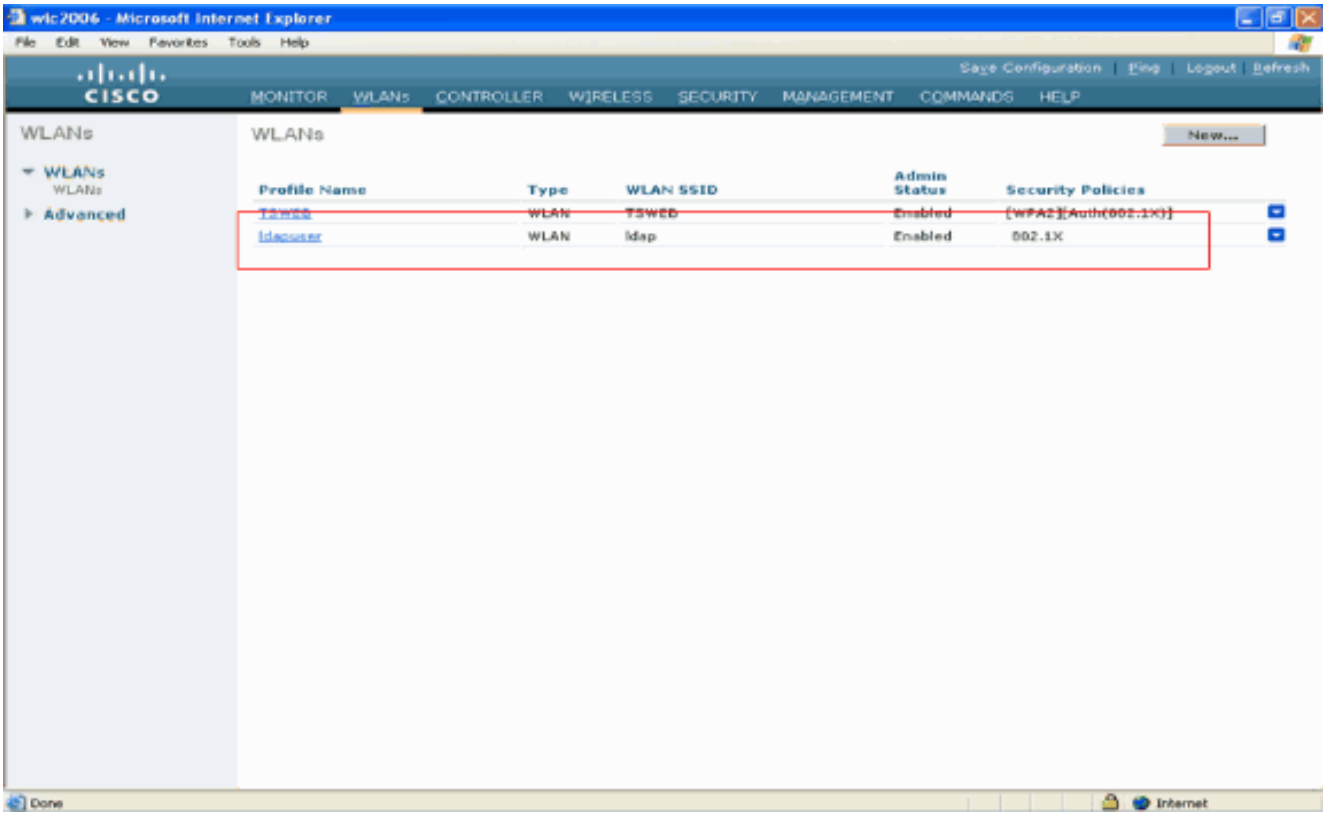


5. Selezionare il server LDAP (precedentemente configurato sul WLC) dalla casella a discesa. Verificare che il server LDAP sia raggiungibile dal WLC.Fare clic su **Apply** (Applica).



6. Il nuovo ldap WLAN è stato configurato sul WLC. Questa WLAN autentica i client con l'autenticazione EAP locale (in questo caso EAP-FAST) ed esegue query su un database

backend LDAP per la convalida delle credenziali client.



Configura server LDAP

Ora che il protocollo EAP locale è stato configurato sul WLC, il passaggio successivo consiste nel configurare il server LDAP che funge da database back-end per autenticare i client wireless al completamento della convalida del certificato.

Il primo passo nella configurazione del server LDAP consiste nel creare un database utenti sul server LDAP in modo che il WLC possa eseguire query su questo database per autenticare l'utente.

Creazione di utenti nel controller di dominio

In questo esempio viene creato un nuovo **ldapuser** dell'unità organizzativa e l'utente **user2** viene creato in questa unità organizzativa. Configurando l'utente per l'accesso LDAP, il WLC può eseguire query in questo database LDAP per l'autenticazione utente.

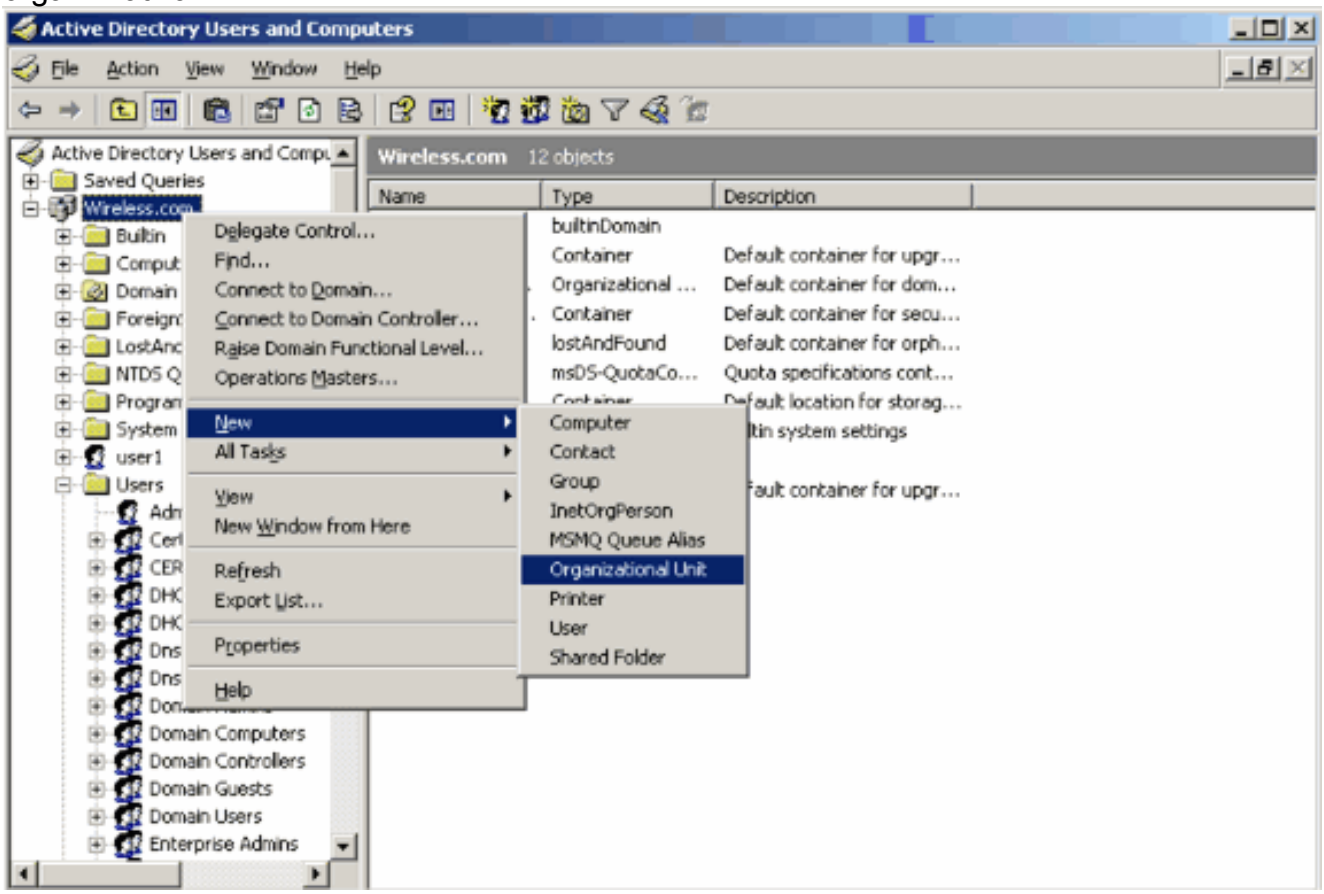
Il dominio utilizzato in questo esempio è **wireless.com**.

Creazione di un database utenti in un'unità organizzativa

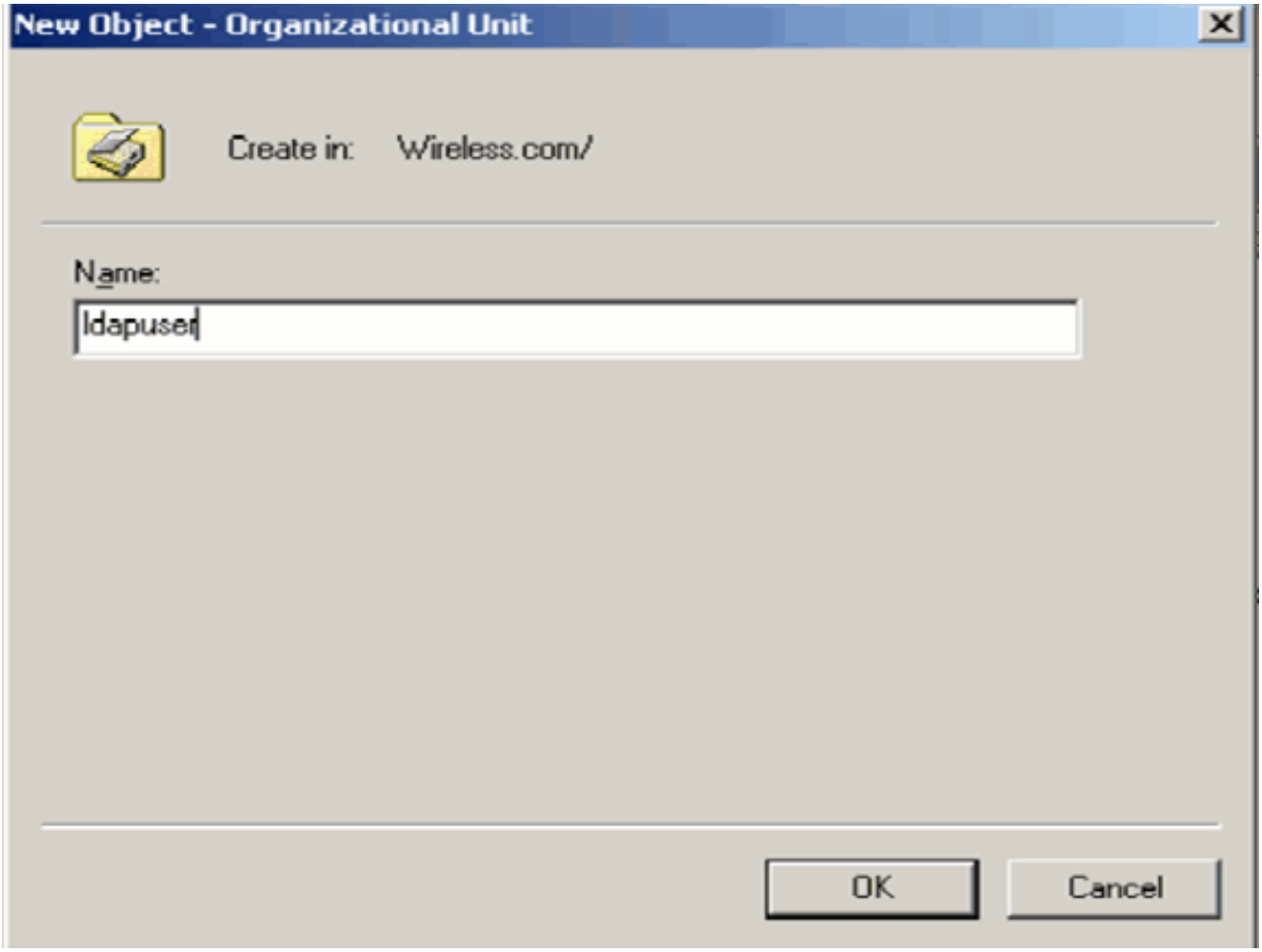
In questa sezione viene illustrato come creare una nuova unità organizzativa nel dominio e creare un nuovo utente in questa unità organizzativa.

1. Nel controller di dominio fare clic su **Start > Programmi > Strumenti di amministrazione > Utenti e computer di Active Directory** per avviare la console di gestione **Utenti e computer di Active Directory**.

2. Fare clic con il pulsante destro del mouse sul nome di dominio (wireless.com, in questo esempio), quindi selezionare **Nuovo > Unità organizzativa** dal menu di scelta rapida per creare una nuova unità organizzativa.

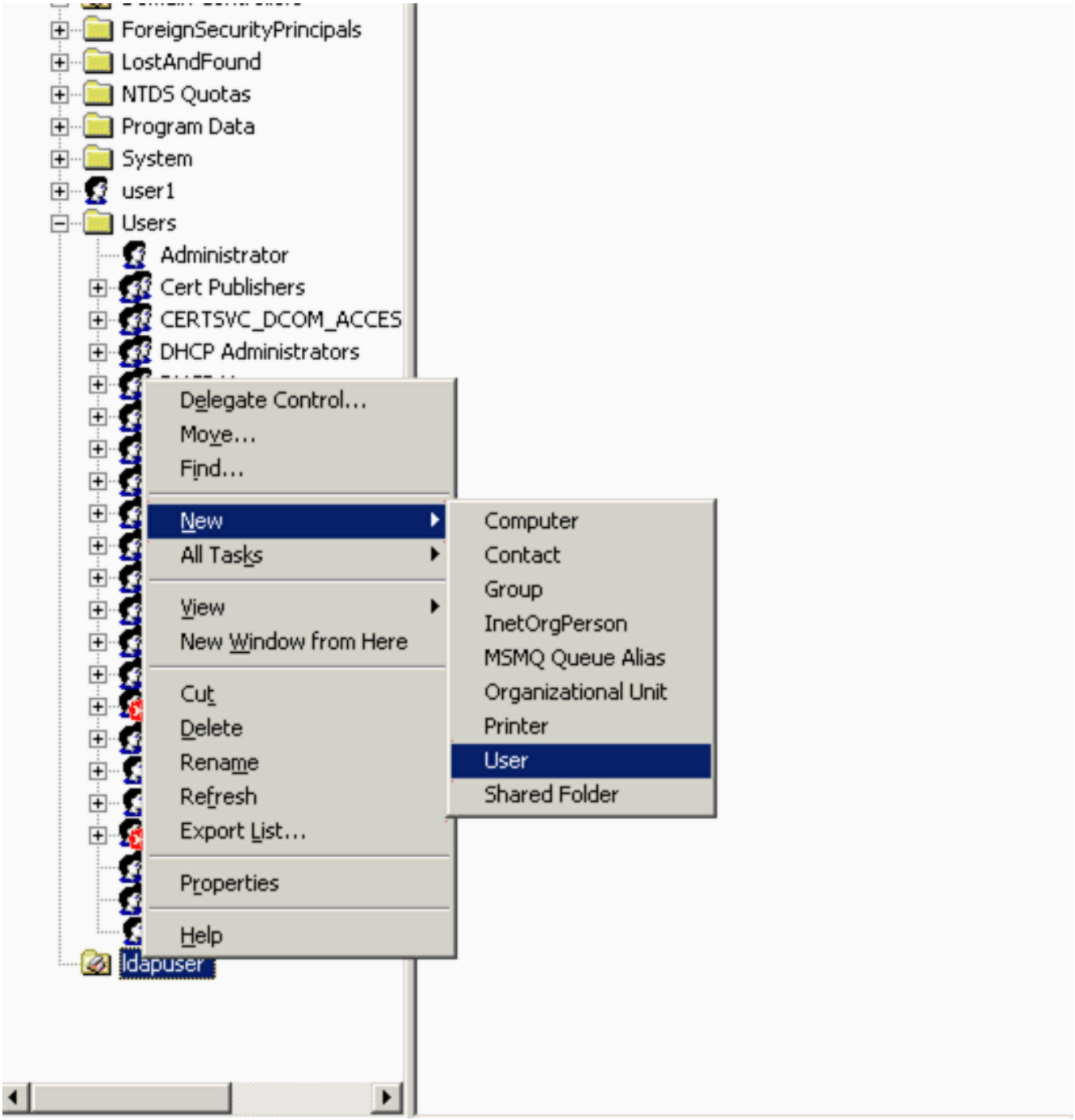


3. Assegnare un nome all'unità organizzativa e fare clic su **OK**.

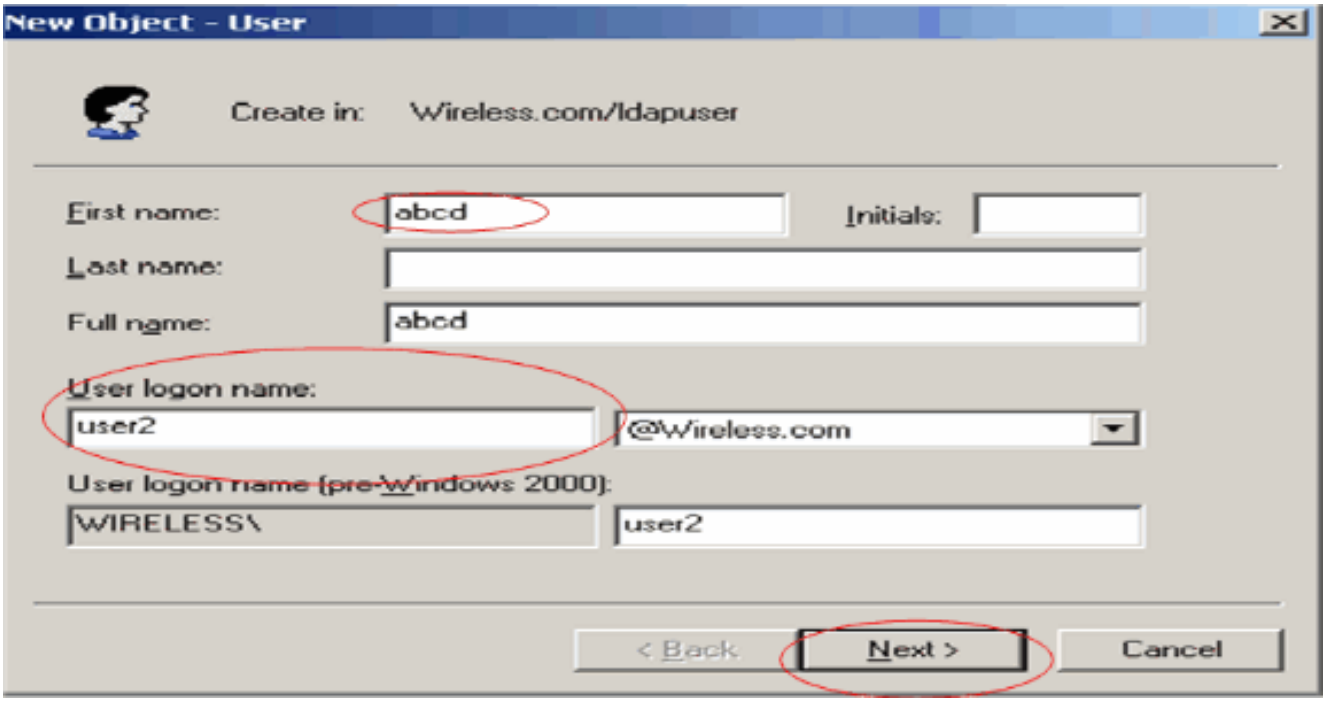


Ora che il nuovo **ldapuser** dell'unità organizzativa è stato creato sul server LDAP, il passaggio successivo consiste nel creare l'utente **user2** in questa unità organizzativa. A tale scopo, effettuare i seguenti passaggi:

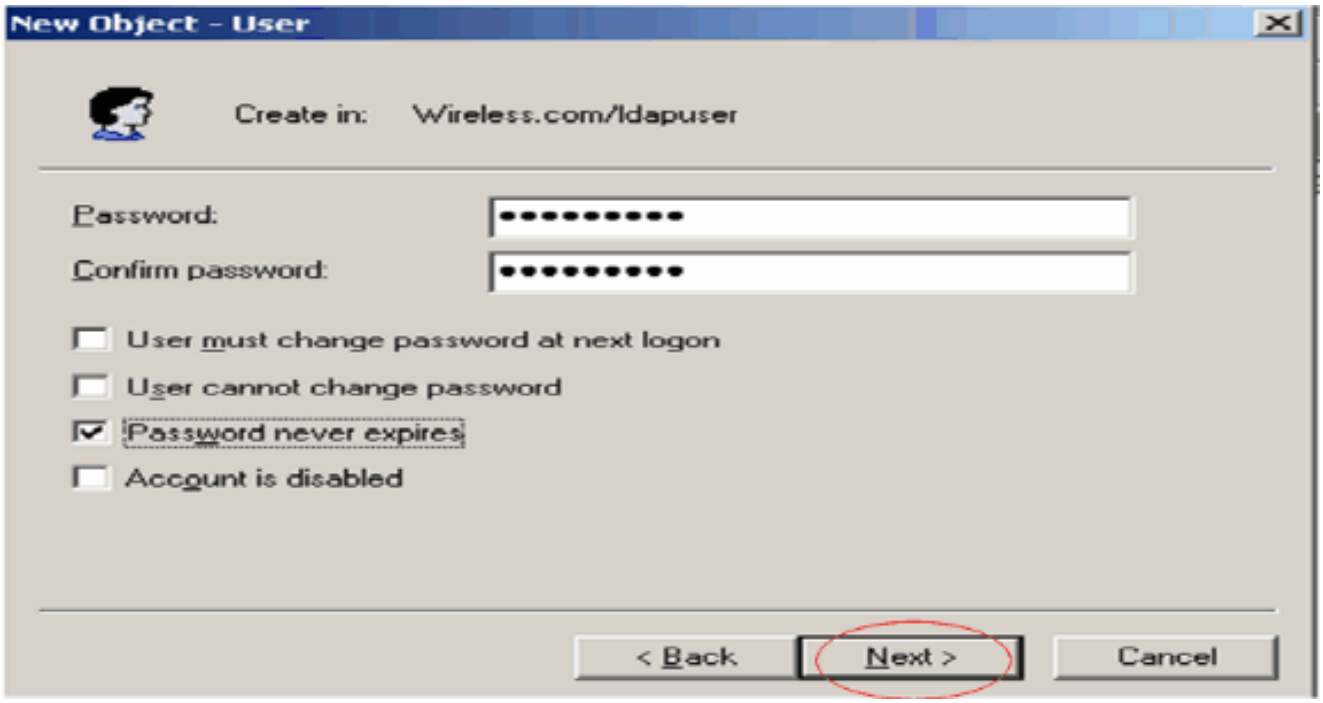
1. Fare clic con il pulsante destro del mouse sulla nuova unità organizzativa. Per creare un nuovo utente, selezionare **Nuovo > Utente** dai menu di scelta rapida risultanti.



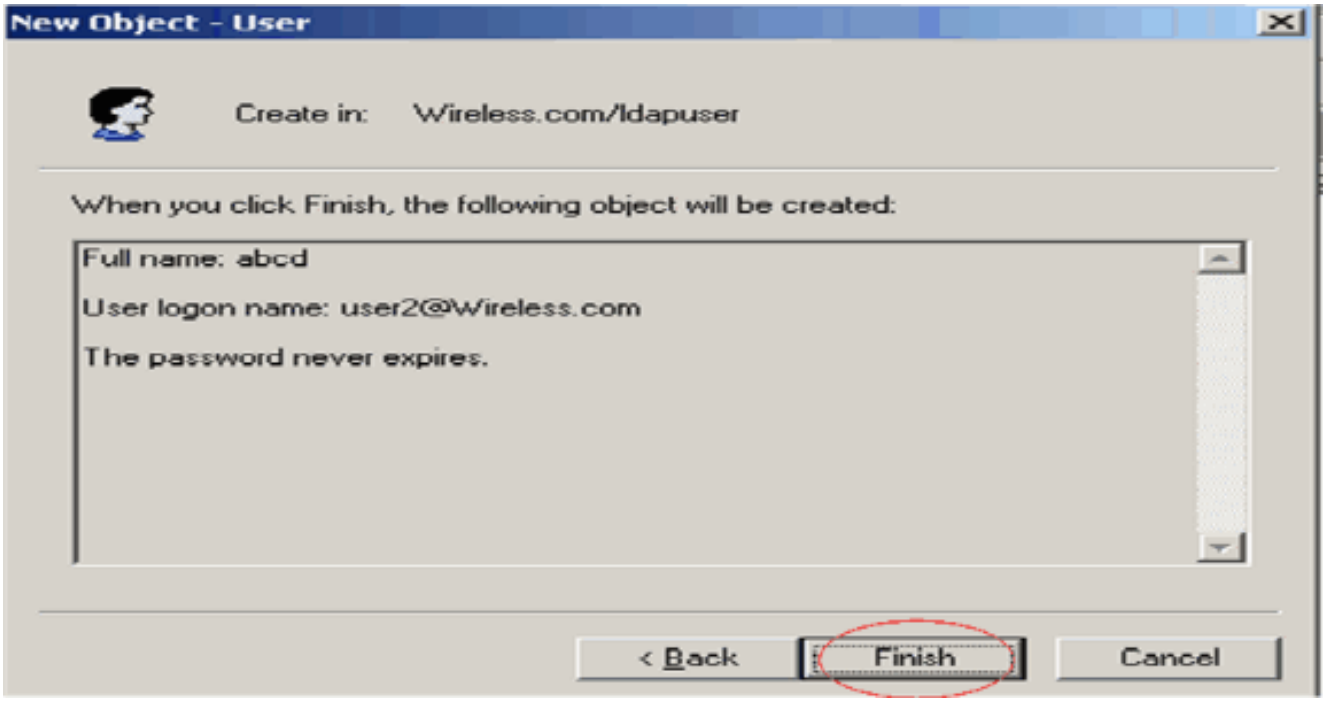
2. Nella pagina Impostazione utente, compilare i campi obbligatori come illustrato in questo esempio. In questo esempio, il nome di accesso dell'utente è **user2**.Questo è il nome utente che verrà verificato nel database LDAP per l'autenticazione del client. In questo esempio vengono utilizzati il nome e il cognome **abcd**. Fare clic su **Next**
(Avanti).



3. Immettere una password e confermarla. Selezionare l'opzione **Nessuna scadenza password** e fare clic su **Avanti**.



4. Fare clic su Finish (Fine).Un nuovo utente **user2** viene creato nell'**utente LDAP** dell'unità organizzativa. Credenziali utente:nome utente: **user2**password: **notebook123**



Dopo aver creato l'utente in un'unità organizzativa, il passaggio successivo consiste nel configurare l'utente per l'accesso LDAP.

Configurare l'utente per l'accesso LDAP

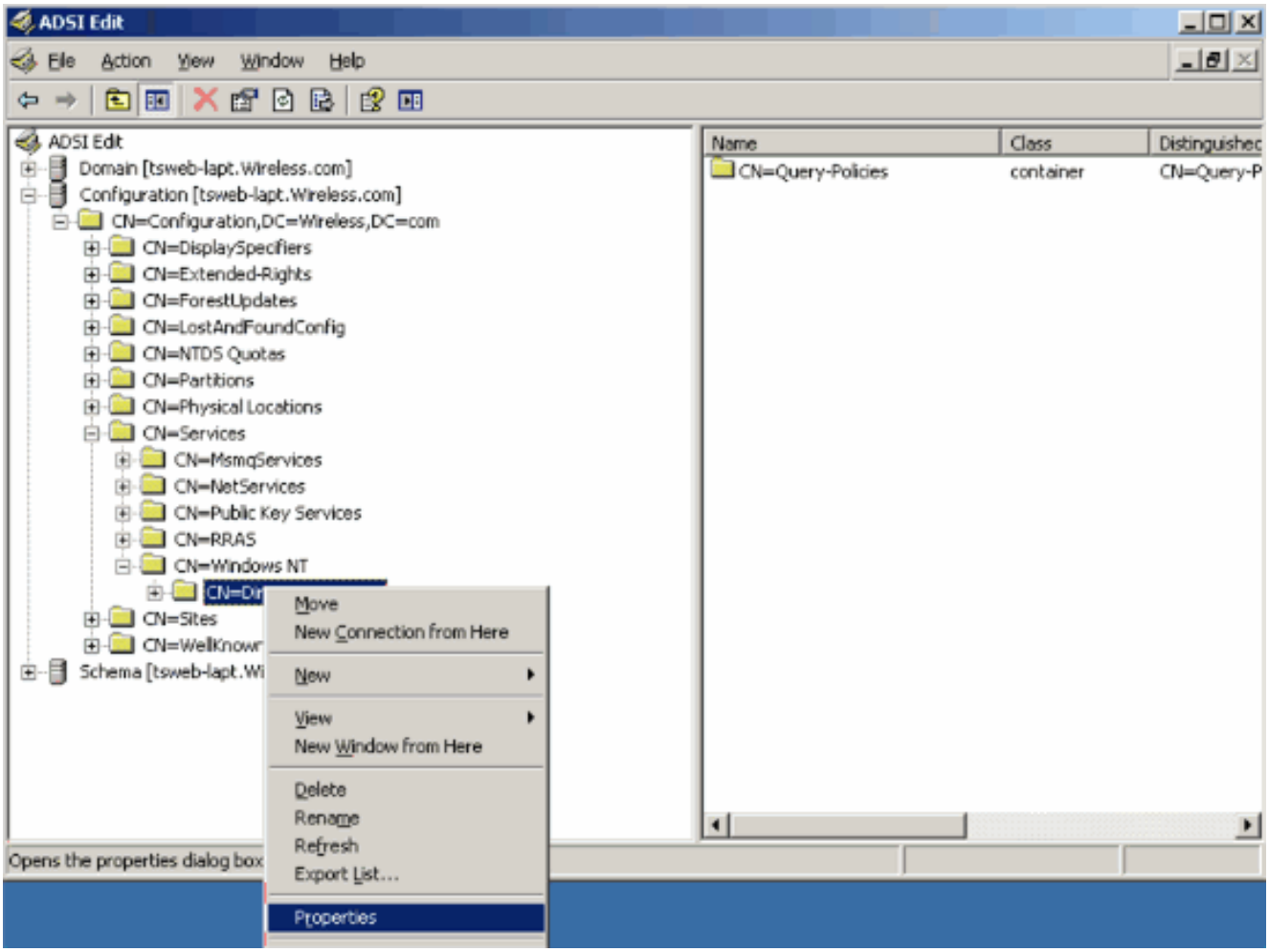
Eseguire la procedura descritta in questa sezione per configurare un utente per l'accesso LDAP.

Attivare la funzione di binding anonimo su Windows 2003 Server

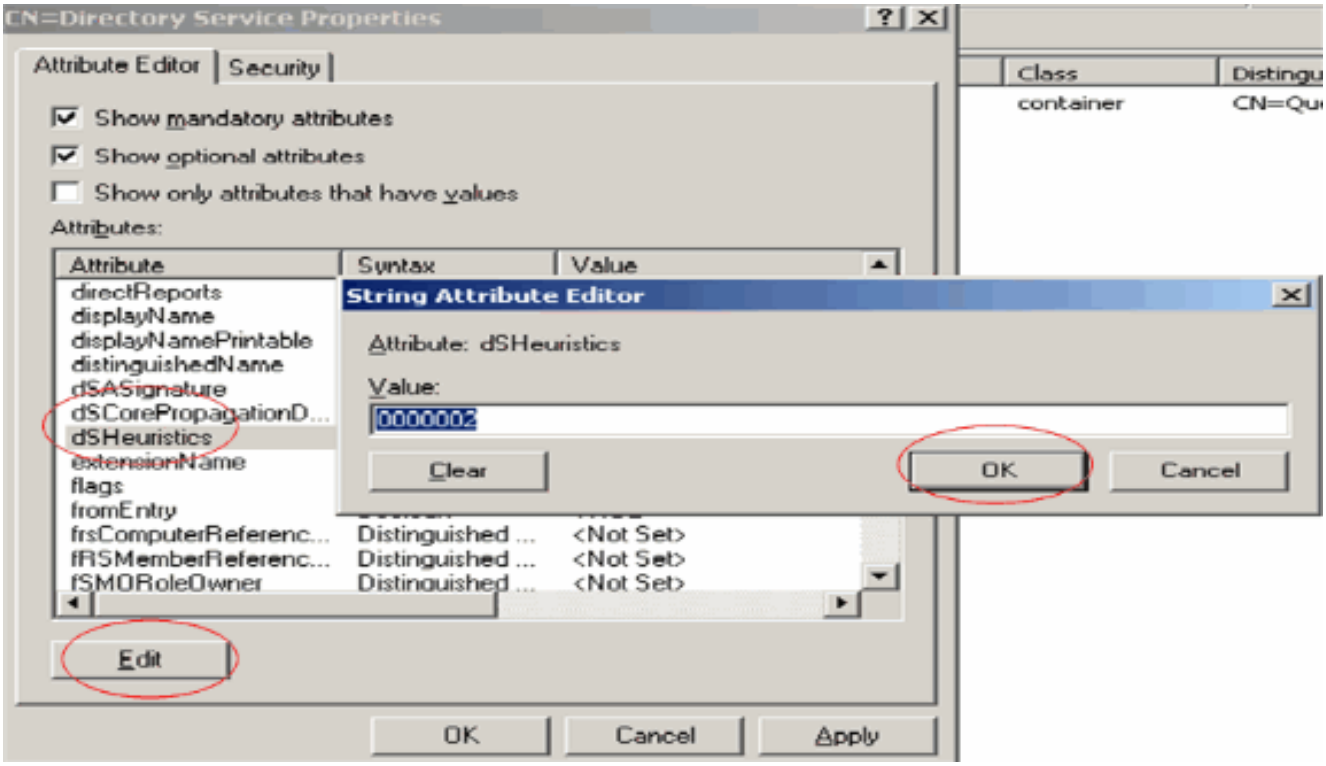
Affinché le applicazioni di terze parti possano accedere a Windows 2003 AD sul server LDAP, è necessario attivare la funzione di binding anonimo su Windows 2003. Per impostazione predefinita, le operazioni LDAP anonime non sono consentite nei controller di dominio di Windows 2003.

Per abilitare la funzione di binding anonimo, effettuare le operazioni riportate di seguito.

1. Avviare lo strumento di **modifica ADSI** dalla posizione Start > Esegui > Tipo: **ADSI Edit.msc**. Questo strumento fa parte degli strumenti di supporto di Windows 2003.
2. Nella finestra Modifica ADSI, espandere il dominio radice (Configuration [tsweb-lapt.Wireless.com]).Espandere **CN=Servizi > CN=Windows NT > CN=Servizio directory**. Fare clic con il pulsante destro del mouse sul contenitore **CN=Directory Service** e selezionare **proprietà** dal menu di scelta rapida.



3. Nella finestra **CN=Directory Service Properties**, fare clic sull'attributo **dsHeuristics** sotto il campo Attribute e scegliere **Modifica**. Nella finestra **Editor attributi stringa** di questo attributo, immettere il valore **0000002**, quindi fare clic su **Applica** e **OK**. La funzionalità di binding anonimo è attivata nel server Windows 2003.**Nota:** l'ultimo (settimo) carattere controlla il modo in cui è possibile eseguire l'associazione al servizio LDAP. "0" o nessun settimo carattere indica che le operazioni LDAP anonime sono disabilitate. **Se si imposta il settimo carattere su "2", viene attivata la funzione di associazione anonima.**

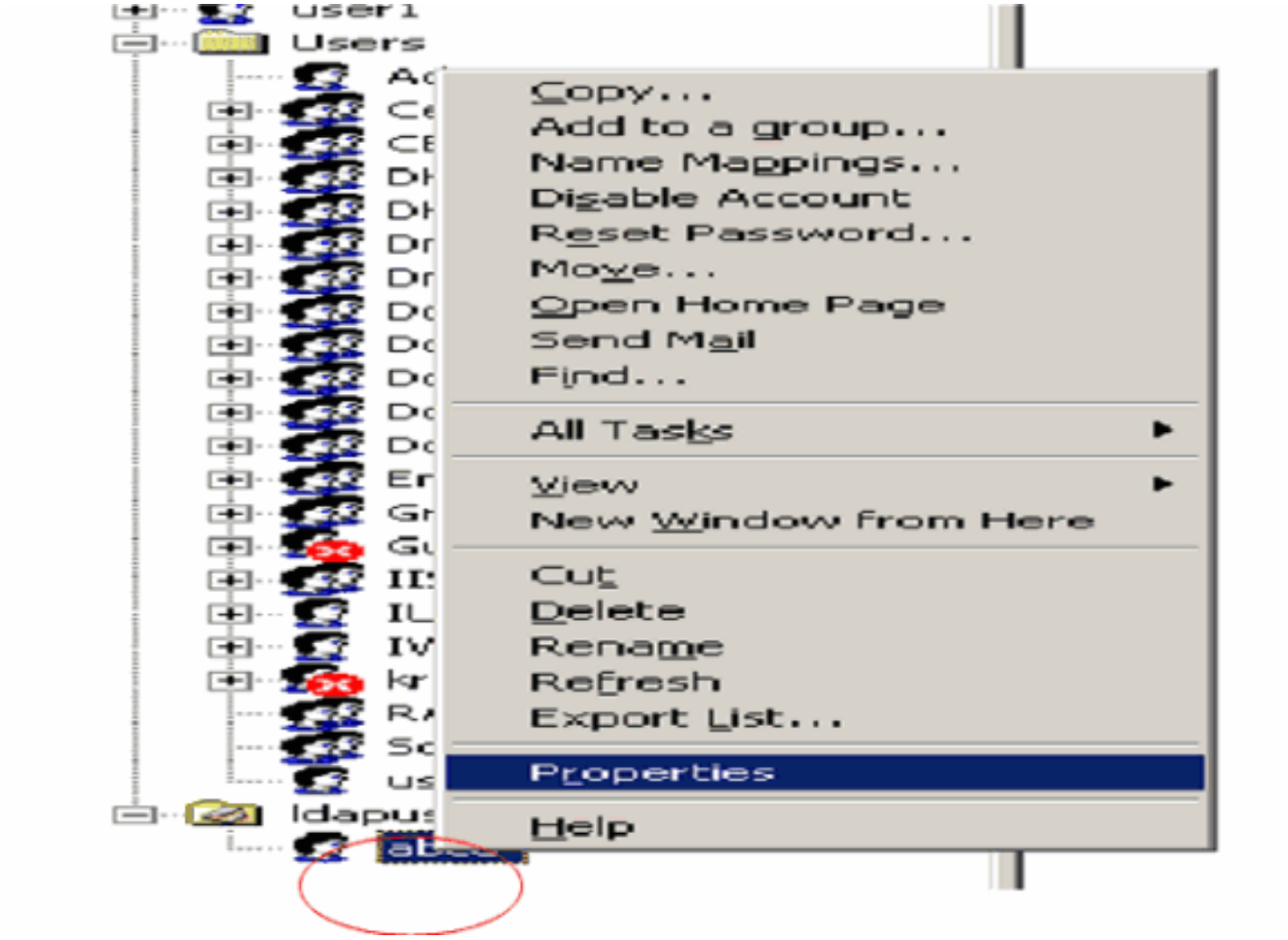


Nota: se questo attributo contiene già un valore, assicurarsi di modificare solo il settimo carattere da sinistra. Questo è l'unico carattere da modificare per abilitare le associazioni anonime. Ad esempio, se il valore corrente è "0010000", sarà necessario modificarlo in "0010002". Se il valore corrente è inferiore a sette caratteri, sarà necessario inserire degli zeri nelle posizioni non utilizzate: "001" diventerà "0010002".

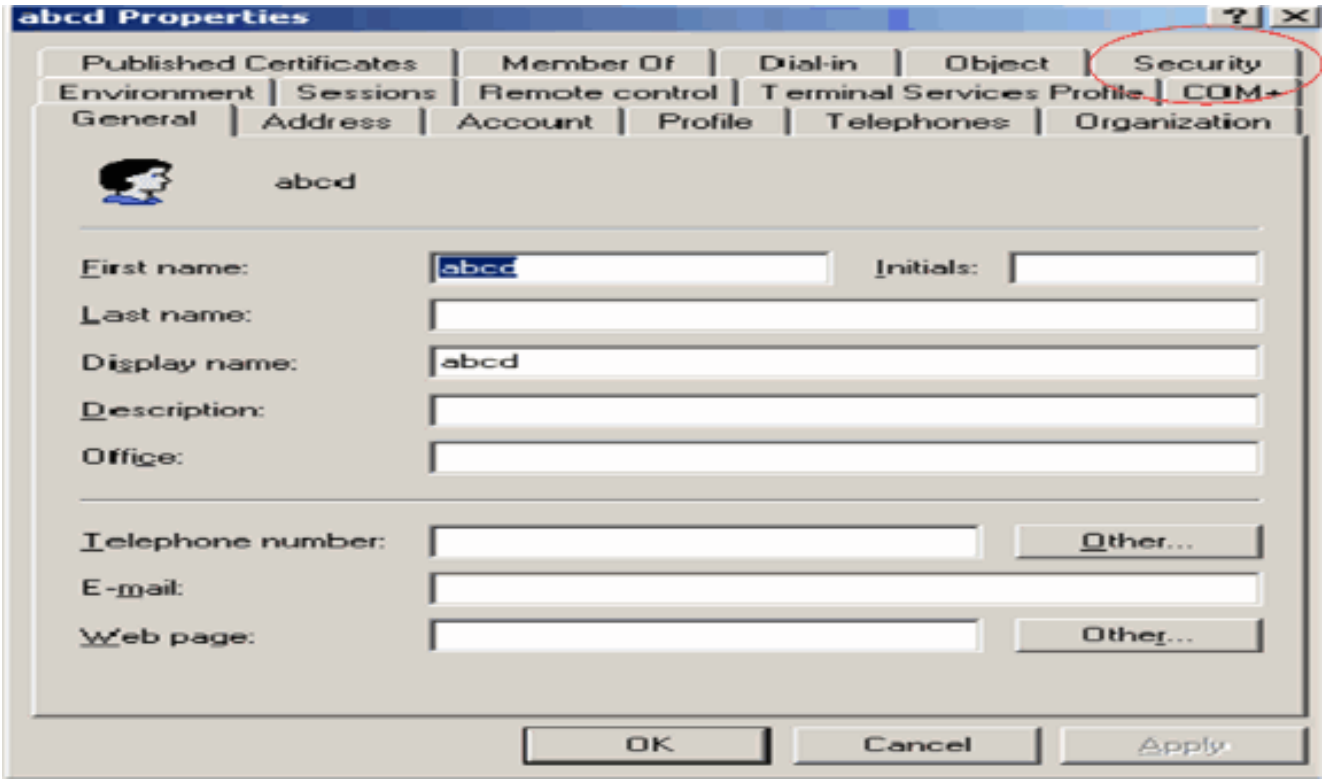
Concessione dell'accesso ANONIMO all'utente "user2"

Il passaggio successivo consiste nel concedere l'accesso **ANONIMO** all'utente **user2**. A tale scopo, completare i seguenti passaggi:

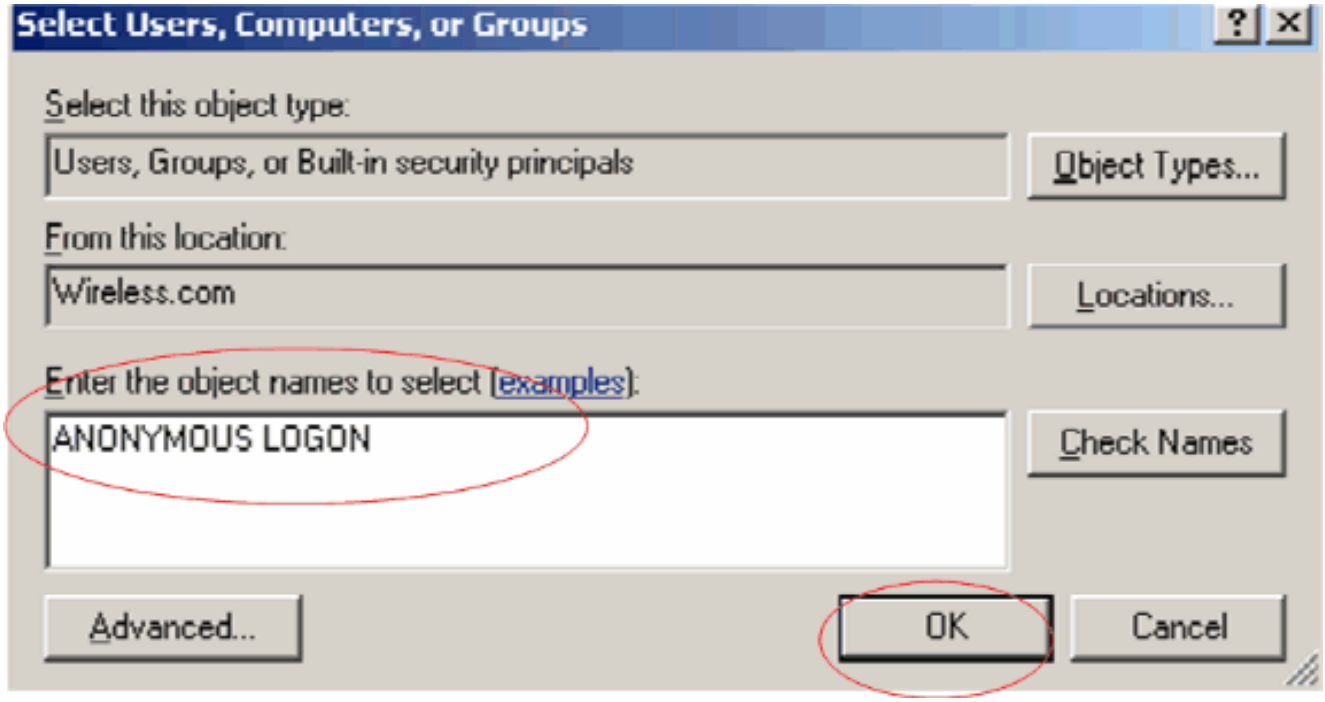
1. Aprire **Utenti** e **computer di Active Directory**.
2. Accertarsi che l'opzione **Visualizza funzioni avanzate** sia selezionata.
3. Individuare l'utente **user2** e fare clic con il pulsante destro del mouse su di esso. Selezionare **Proprietà** dal menu di scelta rapida. Questo utente è identificato dal nome "abcd".



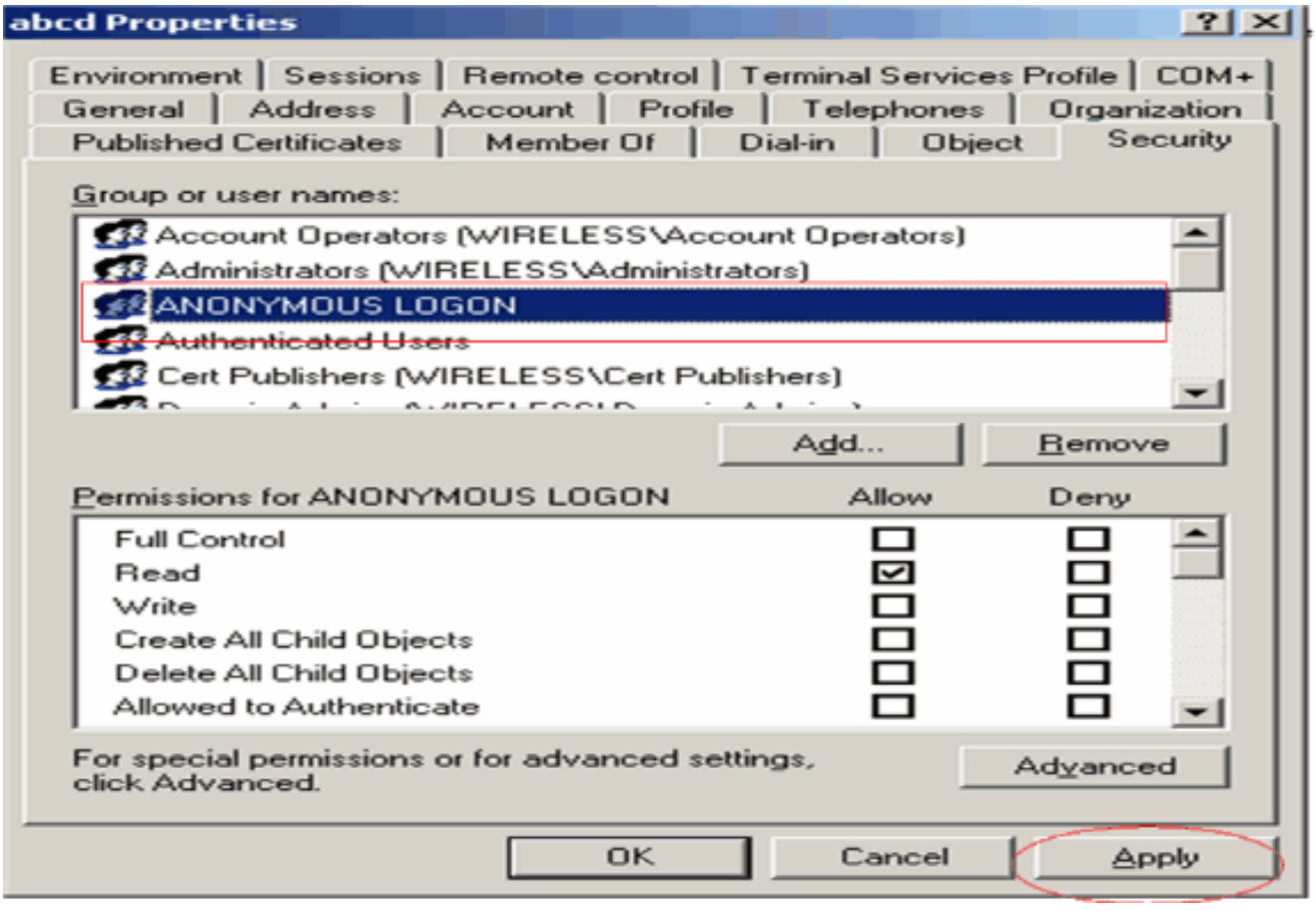
4. Passare alla sezione **Protezione** nella finestra Proprietà - Abcd.



5. Fare clic su **Add** nella finestra risultante.
6. Immettere **ACCESSO ANONIMO** nella casella **Immettere i nomi degli oggetti da selezionare** e confermare la finestra di dialogo.



7. Nell'ACL, si noterà che **ANONYMOUS LOGON** ha accesso ad alcuni set di proprietà dell'utente. Fare clic su **OK**. Accesso ANONIMO concesso all'utente.

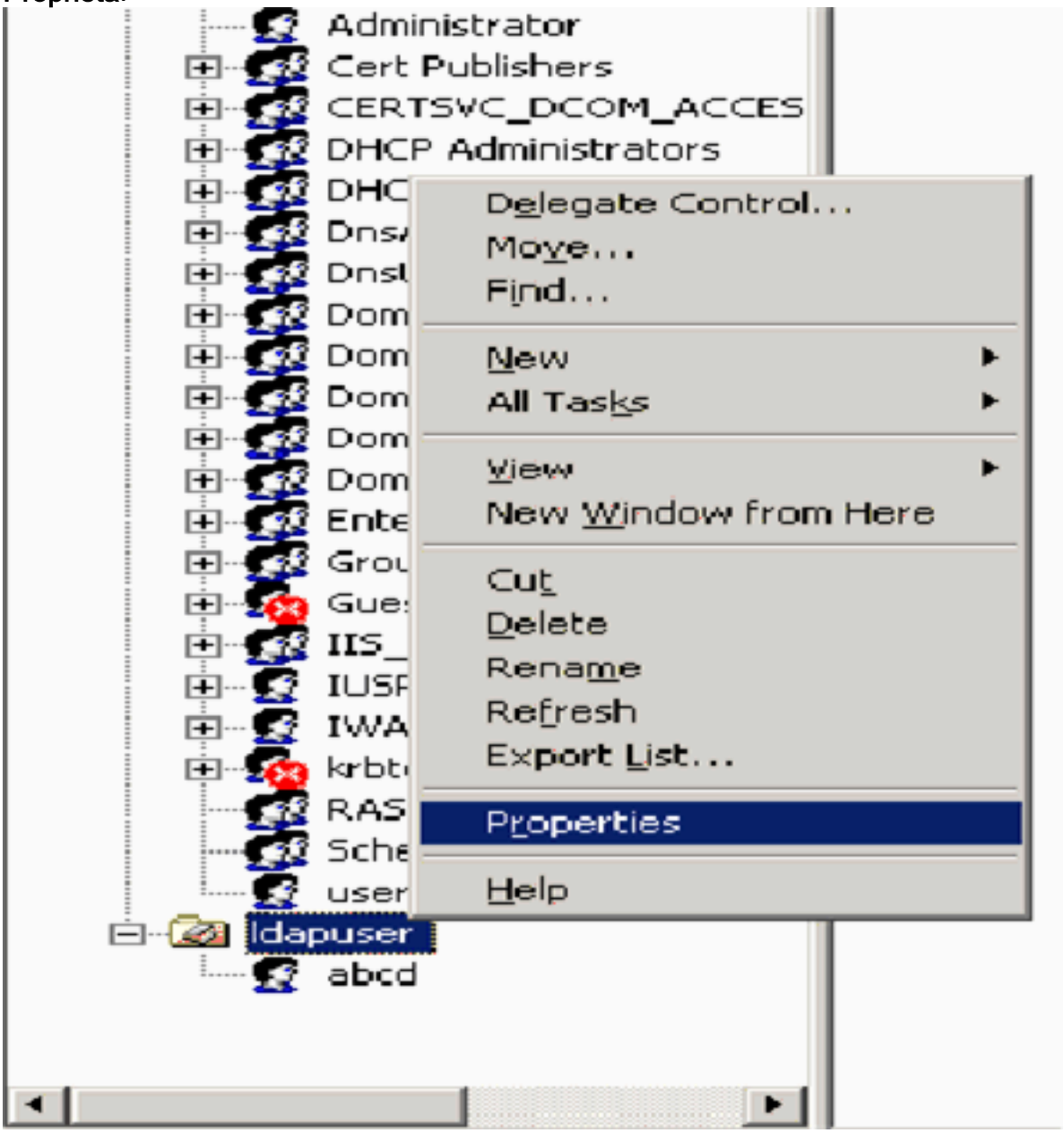


Concessione dell'autorizzazione Contenuto elenco per l'unità organizzativa

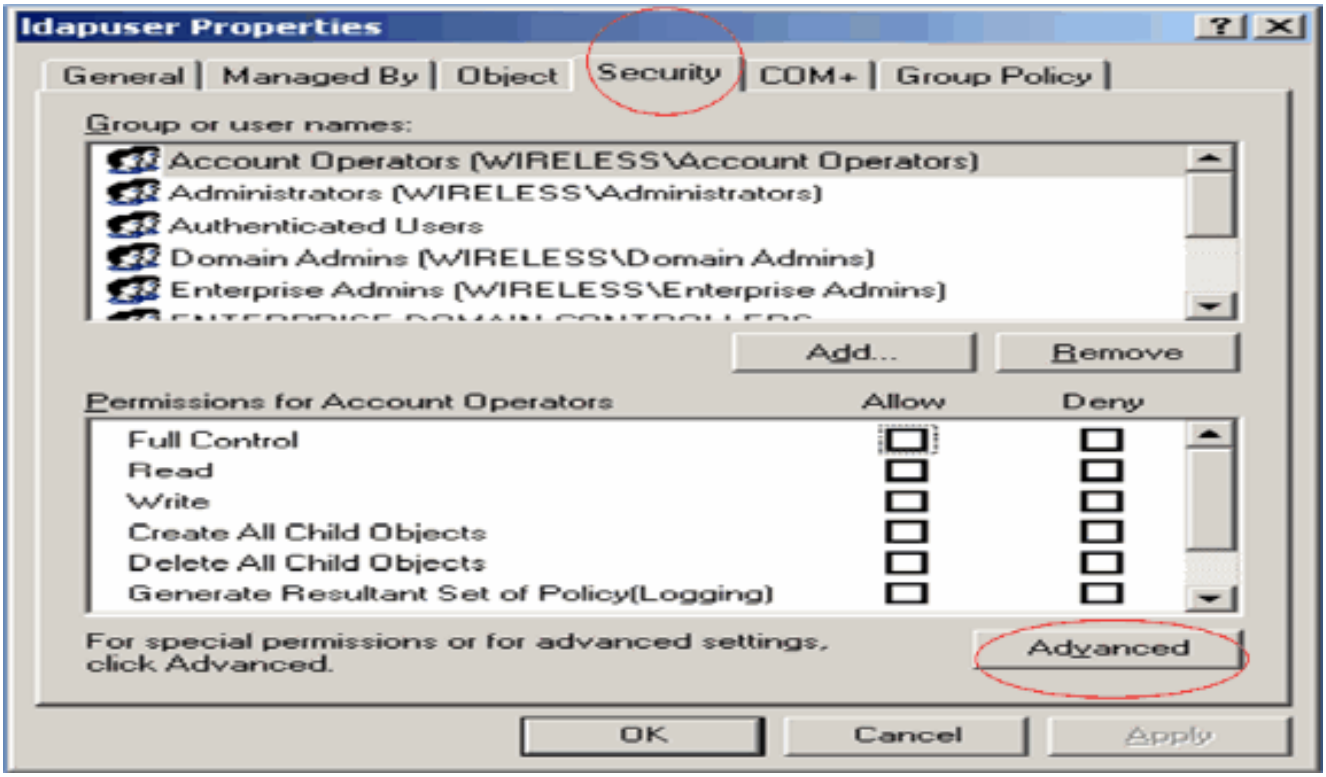
Il passaggio successivo consiste nel concedere almeno l'autorizzazione **Elenco contenuti** all'**ACCESSO ANONIMO** nell'unità organizzativa in cui si trova l'utente. In questo esempio, "user2" si trova sull'unità organizzativa "ldapuser". A tale scopo, completare i seguenti passaggi:

1. In Utenti e computer di Active Directory fare clic con il pulsante destro del mouse sul

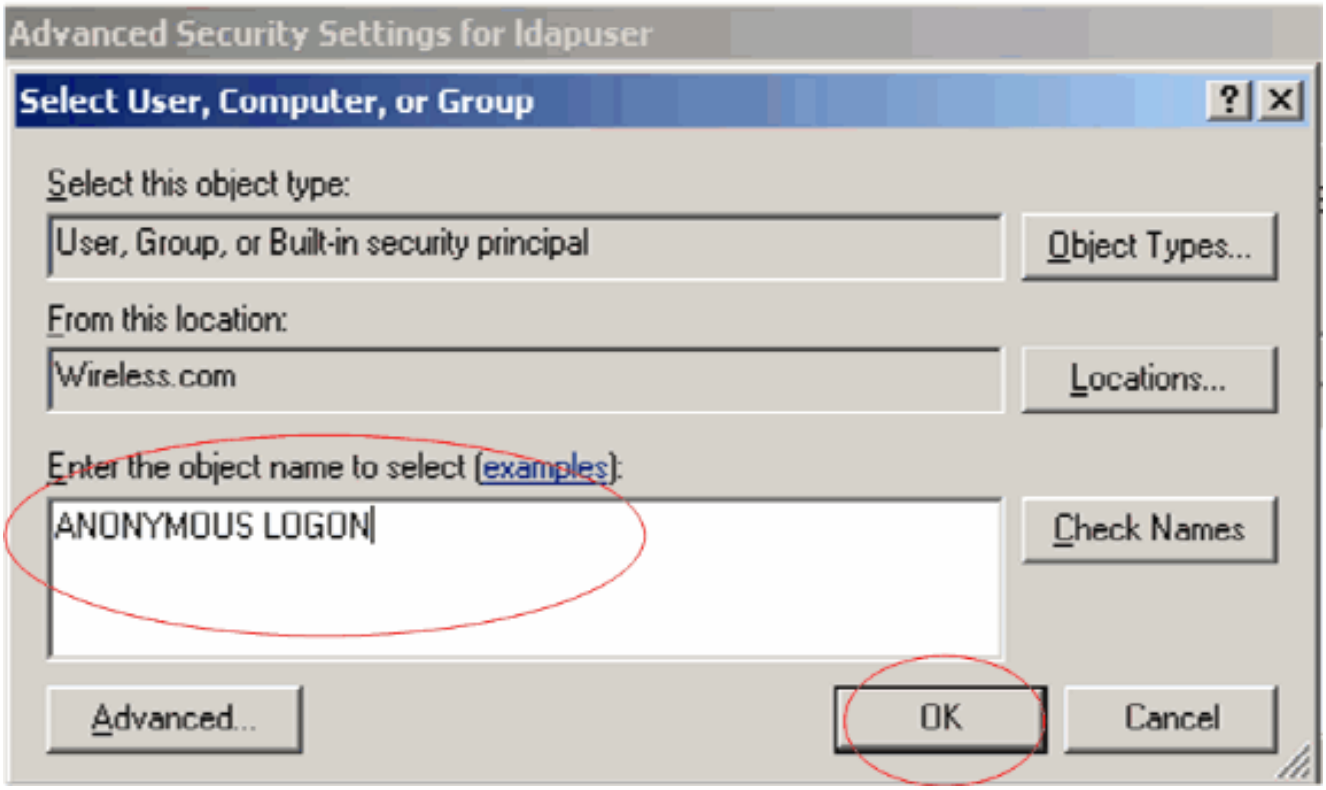
ldapuser dell'unità organizzativa e scegliere **Proprietà**.



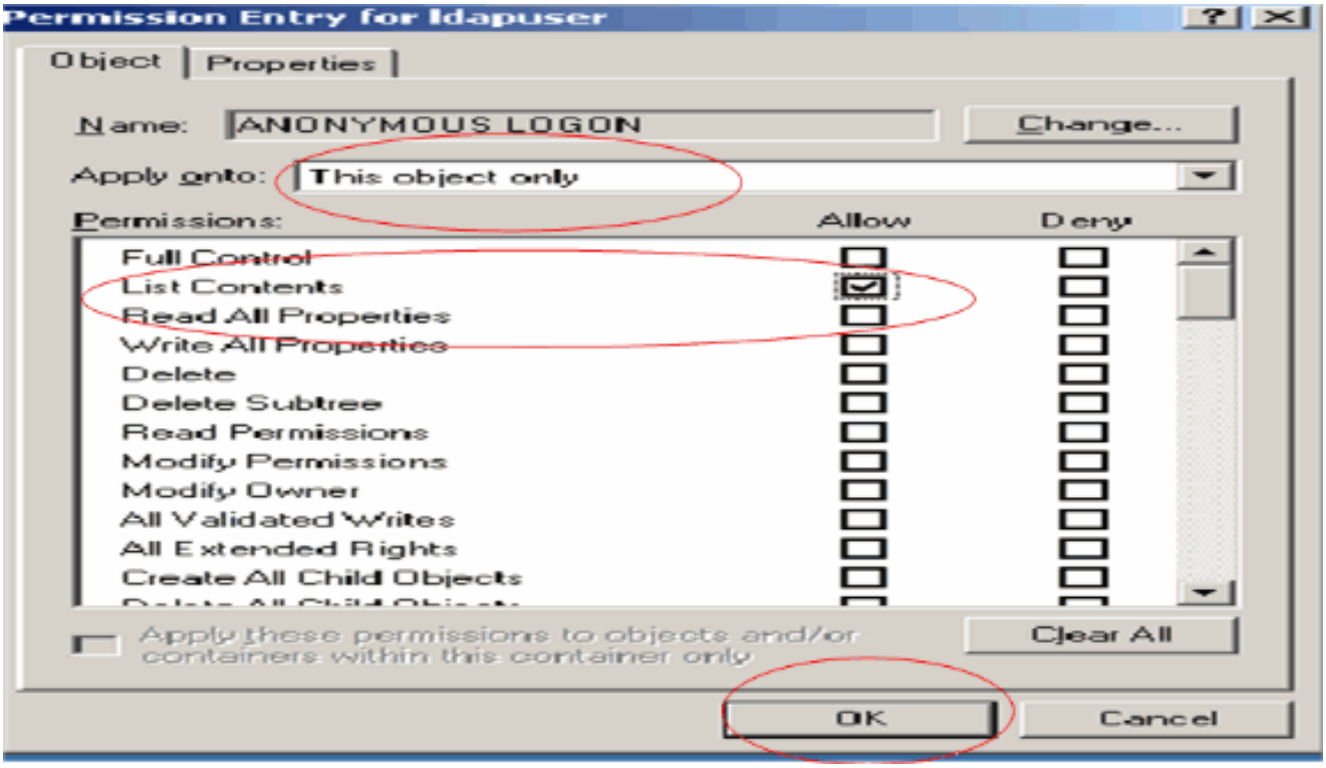
2. Fare clic su **Protezione** e quindi su **Avanzate**.



3. Fare clic su **Add**. Nella finestra di dialogo visualizzata immettere **ACCESSO ANONIMO**.



4. Riconosci il dialogo. Verrà aperta una nuova finestra di dialogo.
5. Nella casella di riepilogo a discesa **Applica a** selezionare **Solo questo oggetto** e selezionare la casella di controllo Consenti **contenuto elenco**.

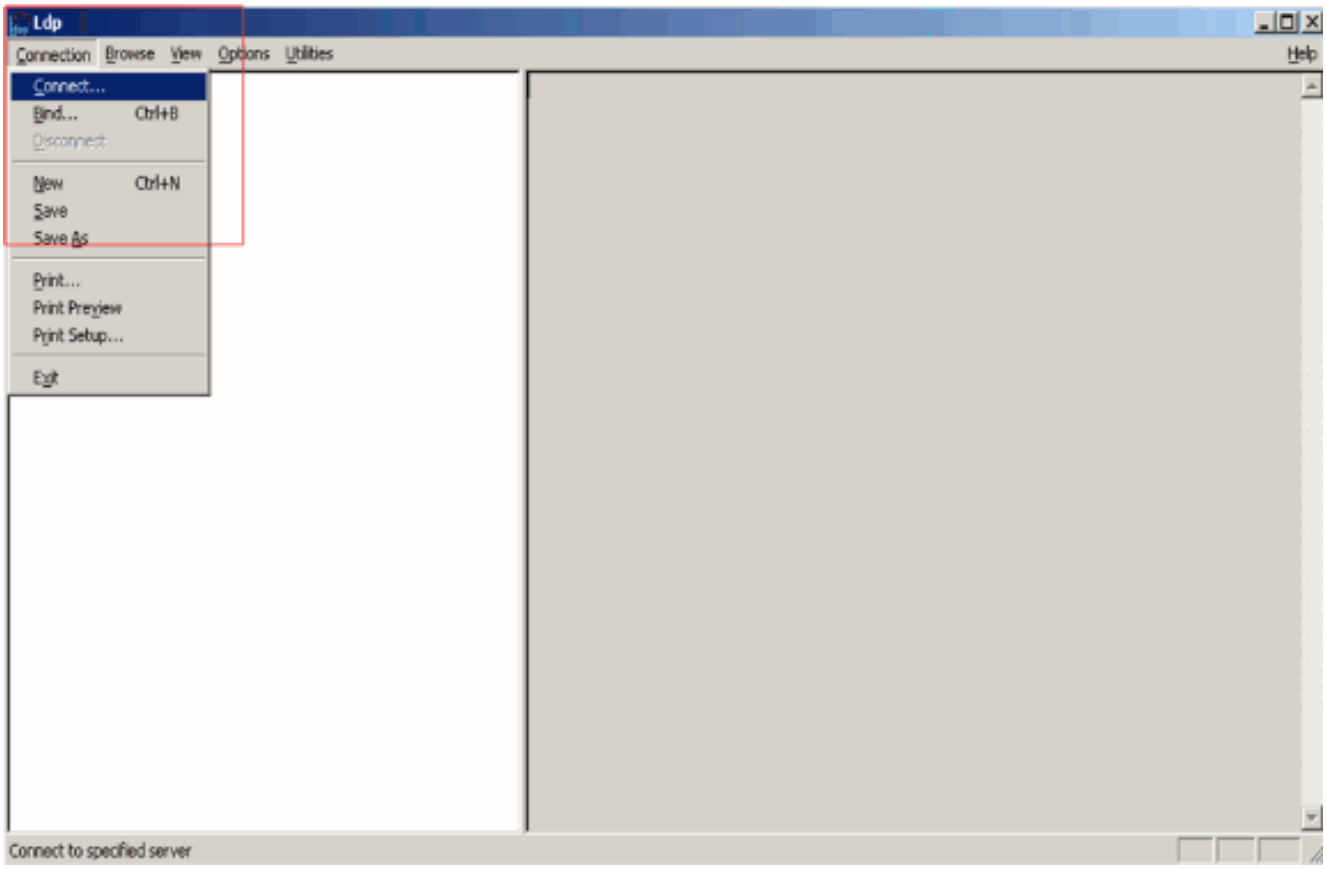


Utilizzo di LDP per identificare gli attributi utente

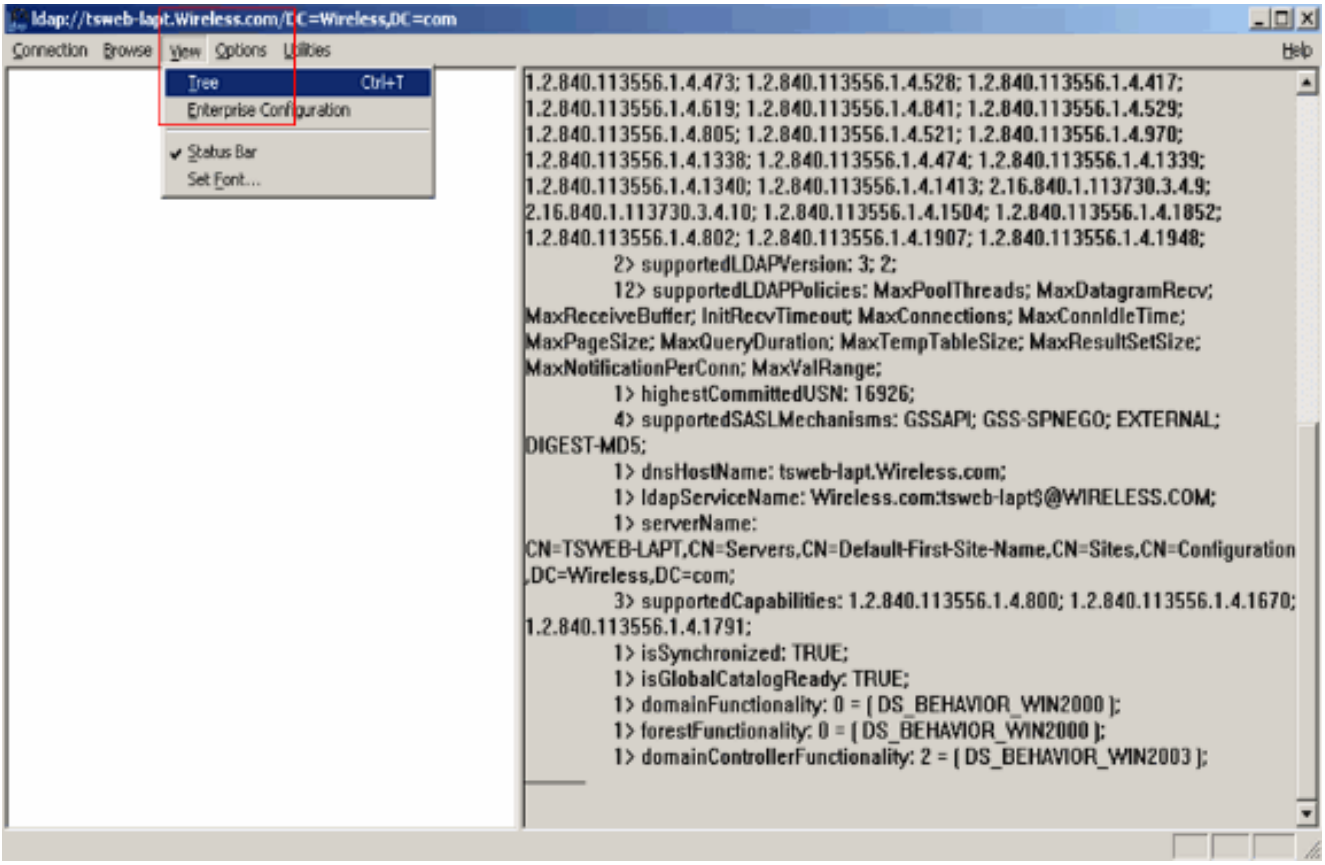
Questo strumento GUI è un client LDAP che consente agli utenti di eseguire operazioni (come la connessione, il binding, la ricerca, la modifica, l'aggiunta e l'eliminazione) su qualsiasi directory compatibile con LDAP, come Active Directory. LDP viene utilizzato per visualizzare gli oggetti archiviati in Active Directory insieme ai relativi metadati, ad esempio i descrittori di protezione e i metadati di replica.

Lo strumento LDP GUI è incluso quando si installano gli strumenti di supporto di Windows Server 2003 dal CD del prodotto. In questa sezione viene illustrato l'utilizzo dell'utilità LDP per identificare gli attributi specifici associati all'utente **user2**. Alcuni di questi attributi vengono utilizzati per compilare i parametri di configurazione del server LDAP sul WLC, ad esempio il tipo di attributo utente e il tipo di oggetto utente.

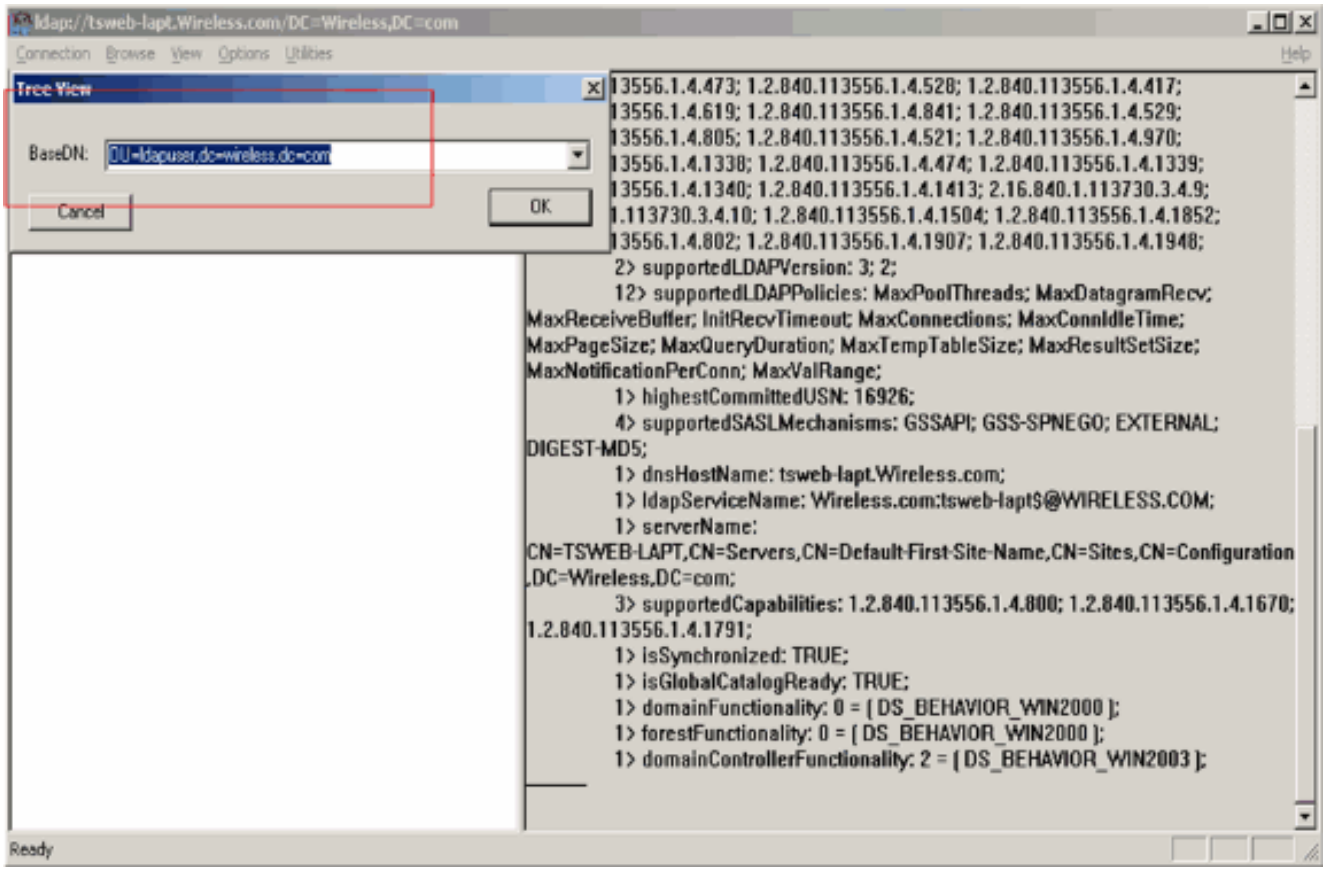
1. Sul server Windows 2003 (anche sullo stesso server LDAP), fare clic su **Start > Esegui** e immettere **LDP** per accedere al browser LDP.
2. Nella finestra principale di LDP, fare clic su **Connessione > Connetti** e connettersi al server LDAP immettendo l'indirizzo IP del server
   LDAP.



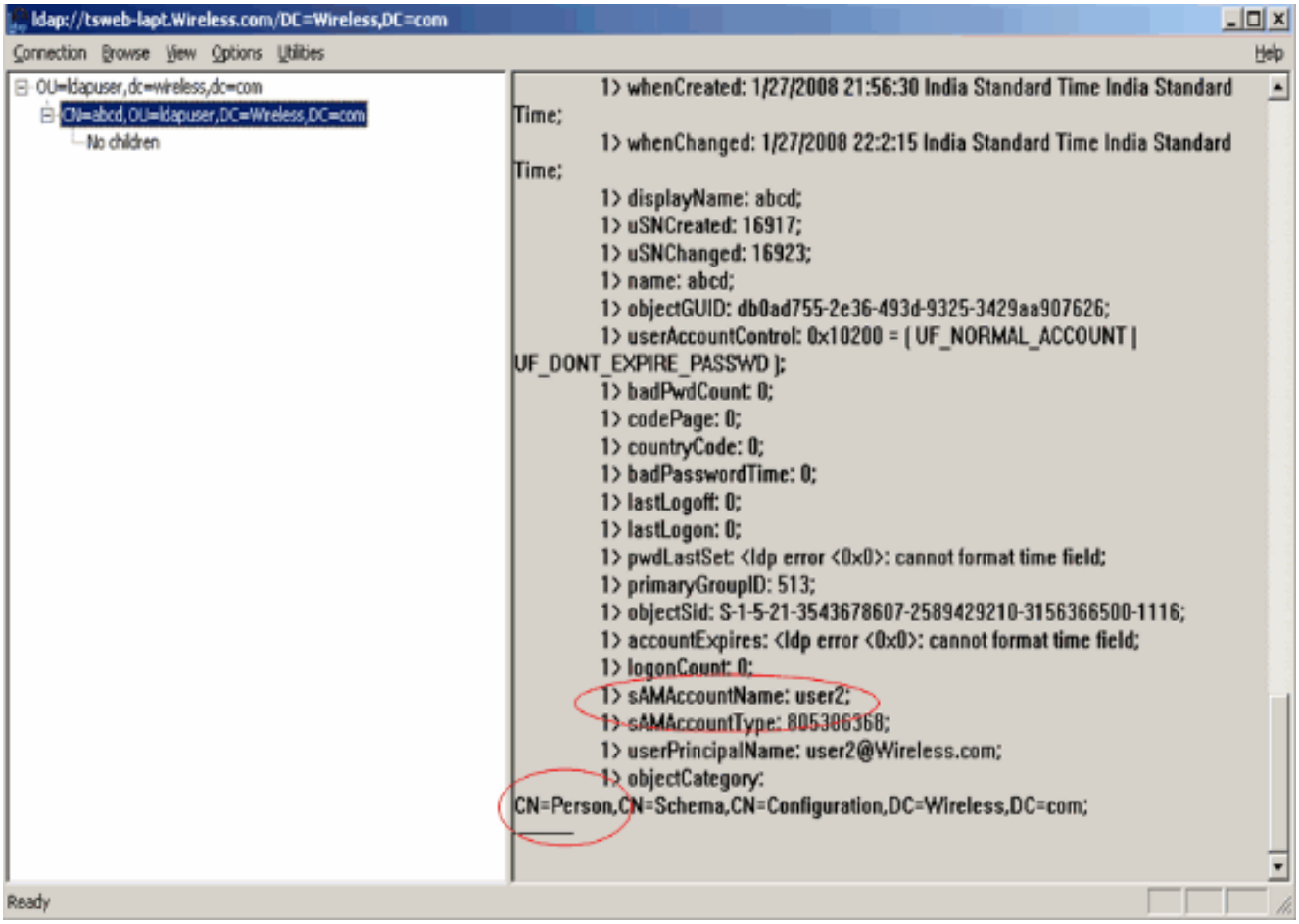
3. Una volta connessi al server LDAP, selezionare **Visualizza** dal menu principale e fare clic su **Albero**.



4. Nella finestra Visualizzazione struttura risultante, immettere il nome distinto di base dell'utente. In questo esempio, **l'utente 2 si trova nell'unità organizzativa "ldapuser" nel dominio Wireless.com**. Il nome di dominio di base per l'utente **user2** è **OU=ldapuser, dc=wireless, dc=com**. Fare clic su
OK.



5. Sul lato sinistro del browser LDP viene visualizzata l'intera struttura sotto il nome di dominio di base specificato (**OU=ldapuser, dc=wireless, dc=com**). Espandere la struttura ad albero per individuare l'utente **user2**. Questo utente può essere identificato con il valore CN che rappresenta il nome dell'utente. Nell'esempio, questo valore è **CN=abcd**. Fare doppio clic su **CN=abcd**. Nel riquadro a destra del browser LDP, **LDP visualizzerà tutti gli attributi associati all'utente 2**. Questo esempio spiega questo
passo:



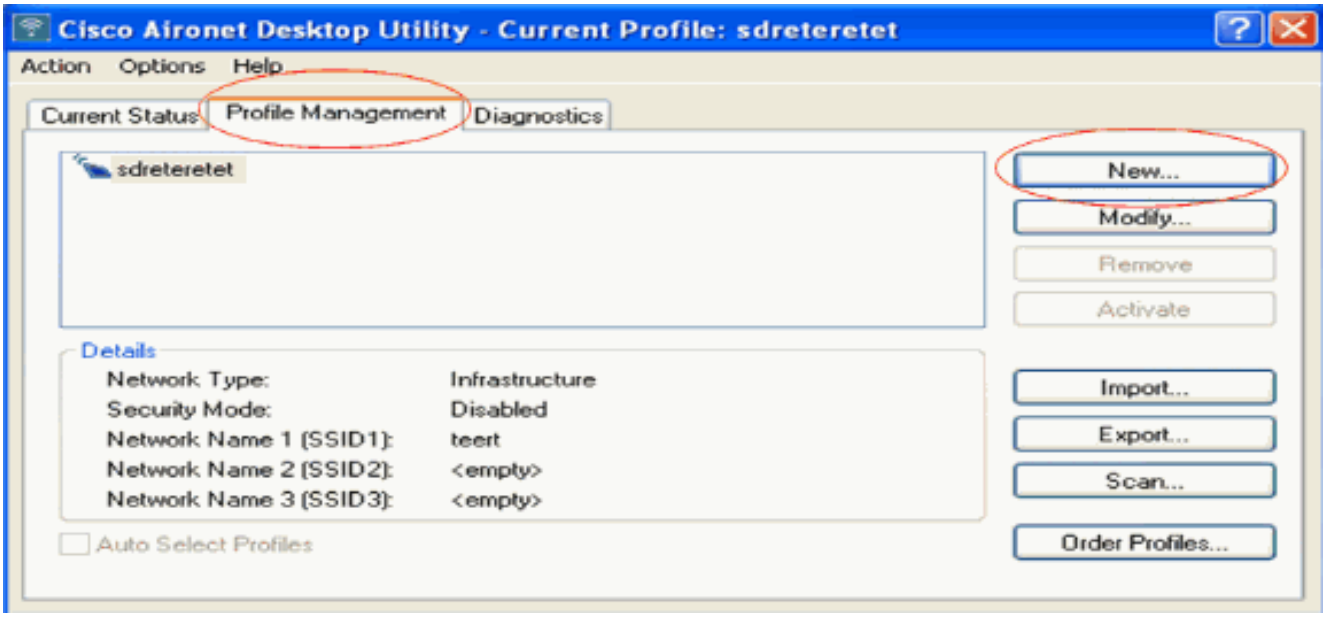
In questo esempio, osservare i campi circondati a destra.

6. Come indicato nella sezione Configurazione WLC con dettagli del server LDAP di questo documento, nel campo **Attributo utente** immettere il nome dell'attributo nel record utente che contiene il nome utente.Da questo output LDP, è possibile vedere che **sAMAccountName** è un attributo che contiene il nome utente "user2". Pertanto, immettere l'attributo **sAMAccountName** che corrisponde al campo **Attributo utente** sul WLC.
7. Nel campo **Tipo oggetto utente**, immettere il valore dell'attributo objectType LDAP che identifica il record come utente. I record utente dispongono spesso di diversi valori per l'attributo objectType, alcuni dei quali sono univoci per l'utente e altri sono condivisi con altri tipi di oggetto.Nell'output LDP, **CN=Person** è un valore che identifica il record come utente. Pertanto, specificare **Person** come attributo **User Object Type** sul WLC.

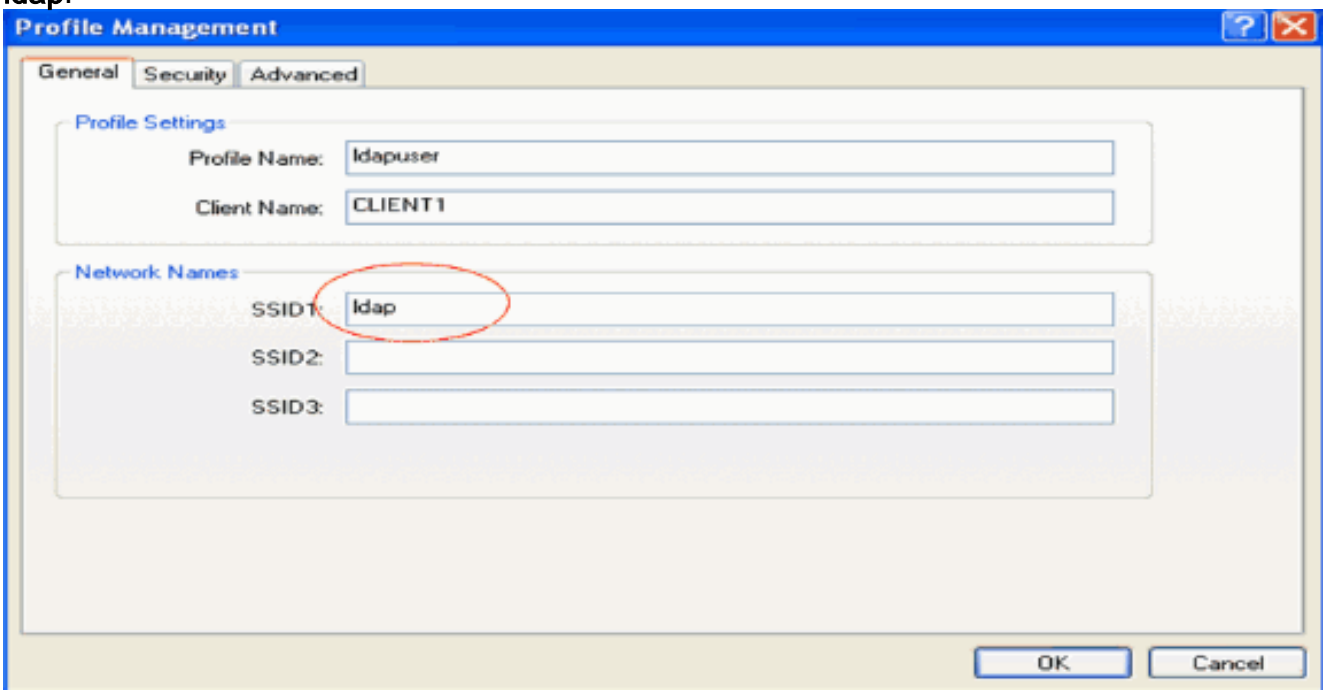
Configura client wireless

L'ultimo passaggio consiste nel configurare il client wireless per l'autenticazione EAP-FAST con certificati client e server. A tale scopo, completare i seguenti passaggi:

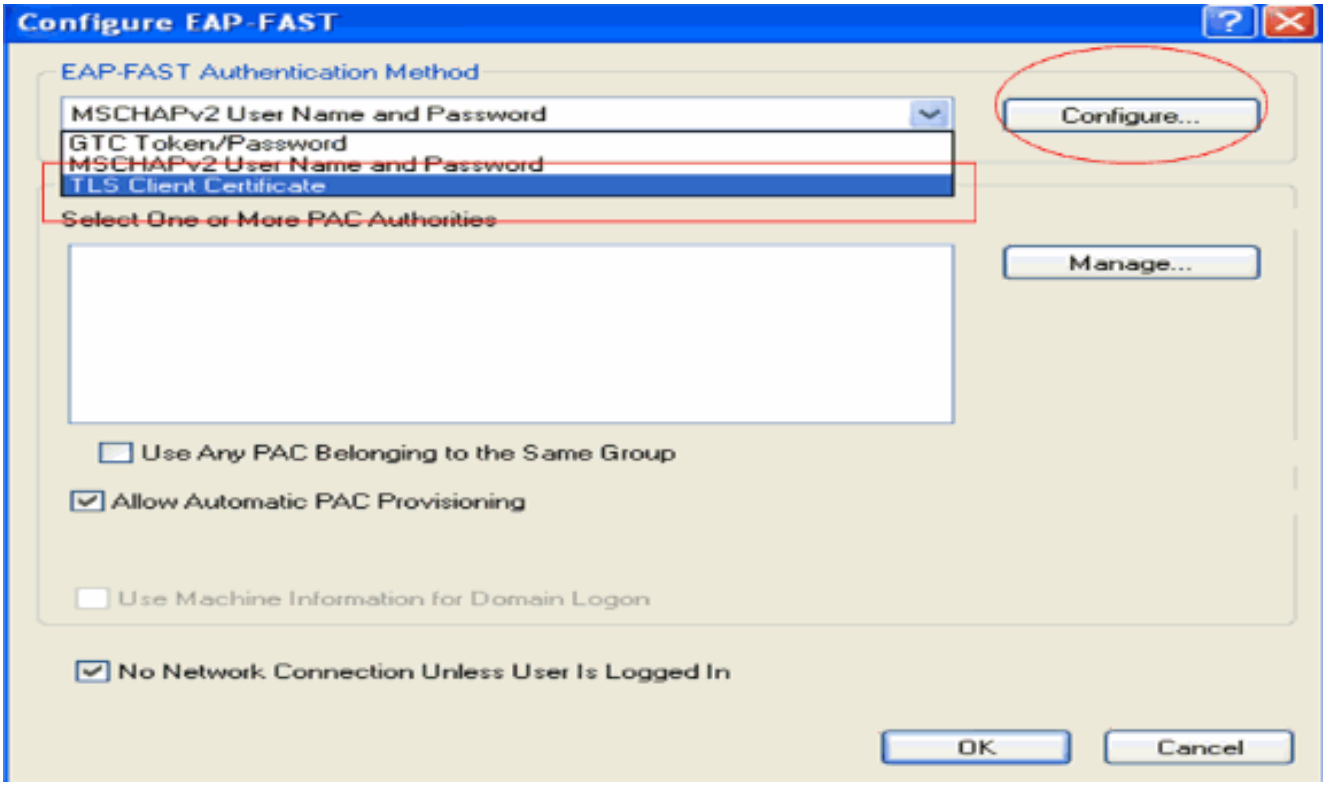
1. Avviare **Cisco Aironet Desktop Utility** (ADU). Per creare un nuovo profilo client wireless, nella finestra principale di ADU fare clic su **Gestione profili >**
Nuovo.



2. Specificare un nome di profilo e assegnare un nome SSID a questo profilo. Questo nome SSID deve essere lo stesso configurato sul WLC. In questo esempio, il nome SSID è **ldap**.



3. Fare clic sulla scheda **Security** (Protezione) e scegliere **802.1x/EAP** come protezione di livello 2. Scegliere **EAP-FAST** come metodo EAP e fare clic su **Configura**.
4. Nella pagina di configurazione di EAP-FAST, scegliere **Certificato client TLS** dall'elenco a discesa Metodo di autenticazione EAP-FAST e fare clic su **Configura**.



5. Nella finestra Configurazione certificato client TLS:Selezionare la casella di controllo **Convalida identità server** e selezionare il certificato CA installato nel client (illustrato nella sezione Generazione del certificato CA radice per il client di questo documento) come Autorità di certificazione radice attendibile.Selezionare il certificato del dispositivo installato sul client (come illustrato nella sezione Generazione di un certificato del dispositivo per il client di questo documento) come certificato del client.Fare clic su **OK**.Questo esempio spiega questo
passo:

Viene creato il profilo client wireless.

Verifica

Per verificare che la configurazione funzioni correttamente, attenersi alla seguente procedura.

1. Attivare il SSID **ldap** sull'ADU.

2. Fare clic su **Sì** o **OK** come richiesto nelle finestre successive. Per avere successo nell'ADU, dovrebbe essere possibile visualizzare tutti i passaggi dell'autenticazione client e dell'associazione.

Per verificare che la configurazione funzioni correttamente, consultare questa sezione. Usare la modalità CLI del WLC.

- Per verificare se il WLC è in grado di comunicare con il server LDAP e individuare l'utente, specificare il comando **debug aaa ldap enable** dalla CLI del WLC. In questo esempio viene illustrato un processo LDAP di comunicazione riuscito:**Nota:** parte dell'output di questa sezione è stato spostato su altre righe per motivi di spazio.(Cisco Controller) **>debug aaa ldap enable**

```
Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514
Sun Jan 27 09:23:46 2008:       Callback.....................................0x8
344900
Sun Jan 27 09:23:46 2008:       protocolType.................................0x0
0100002
Sun Jan 27 09:23:46 2008:       proxyState...................................00:
40:96:AC:E6:57-00:00
Sun Jan 27 09:23:46 2008:       Packet contains 2 AVPs (not shown)
Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED
Sun Jan 27 09:23:46 2008: LDAP server 1 now active
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser,DC=wireless,
DC=com, pattern=(&(objectclass=Person)(sAMAccountName=user2))
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: Returned msg type 0x64
Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called lcapi_query base="OU=ldapus
er,DC=wireless,DC=com" type="Person" attr="sAMAccountName" user="user2" (rc = 0
- Success)
Sun Jan 27 09:23:46 2008: LDAP ATTR> dn = CN=abcd,OU=ldapuser,DC=Wireless,DC=com
 (size 38)
Sun Jan 27 09:23:46 2008: Handling LDAP response Success
```

  Dalle informazioni evidenziate in questo output di debug, è chiaro che il WLC esegue una query sul server LDAP con gli attributi utente specificati sul WLC e che il processo LDAP ha esito positivo.
- Per verificare se l'autenticazione EAP locale ha esito positivo, specificare il comando **debug aaa local-auth eap method events enable** dalla CLI del WLC. Di seguito è riportato un esempio:(Cisco Controller) **>debug aaa local-auth eap method events enable**

```
Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: New context
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: Allocated new EAP-FAST context
(handle = 0x22000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Received Identity

Sun Jan 27 09:38:28 2008: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV
(436973636f000000000000000000000000)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start

Sun Jan 27 09:38:29 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b
```

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

**Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Start**

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
TLS_DHE_RSA_AES_128_CBC_SHA proposed...

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s):

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite:

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello

**Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 1 ...**

**Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 1 complete**

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello

Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack

.....

.....

.....

**Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Sent provisioning Server Hello**

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Certificate handshake

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Successfully validated received certificate

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID:
"EAP-FAST I-ID" from Peer Cert

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Key Exchange handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 2 ...

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 2 complete.

Sun **Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:**
Reading Client Certificate Verify handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Sign certificate verify succeeded (compare)

.....

.....

.....

.....
.

- Anche il comando **debug aaa local-auth db enable** è molto utile. Di seguito è riportato un esempio:(Cisco Controller) **>debug aaa local-auth db enable**

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: EAP: Received an auth request

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Creating new context

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Local auth profile name for context 'ldapuser'

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Created new context eap session handle fb000007

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 2) to EAP subsys

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP) Sending user credential
request username 'user2' to LDAP

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found context matching MAC address - 8

.....

.....

.....

.....

```
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 12) to EAP subsys

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) received keys waiting for success

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Processing keys success
```

- Per visualizzare i certificati installati nel WLC da utilizzare per l'autenticazione locale, usare il comando **show local-auth certificates** dalla CLI del WLC. Di seguito è riportato un esempio:(Cisco Controller) **>mostra certificati di autenticazione locale**

```
Certificates available for Local EAP authentication:



Certificate issuer ............................. vendor

  CA certificate:

    Subject: DC=com, DC=Wireless, CN=wireless

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

  Device certificate:

    Subject: O=cisco, CN=ciscowlc123

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT



Certificate issuer ............................. cisco

  CA certificate:

    Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

     Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

      Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

   Device certificate:

              Not installed.
```

- Per visualizzare la configurazione dell'autenticazione locale sul WLC dalla modalità CLI, usare il comando **show local-auth config**. Di seguito è riportato un esempio:(Cisco Controller) **>show local-auth config**

```
User credentials database search order:
```

```
    Primary ..................................... LDAP


Timer:

    Active timeout ............................. 300


Configured EAP profiles:

    Name ........................................ ldapuser

      Certificate issuer ....................... vendor

      Peer verification options:

        Check against CA certificates ........... Enabled

        Verify certificate CN identity .......... Disabled

        Check certificate date validity ......... Disabled

      EAP-FAST configuration:

        Local certificate required .............. Yes

        Client certificate required ............. Yes

      Enabled methods ........................... fast

      Configured on WLANs ....................... 2


EAP Method configuration:

    EAP-FAST:
--More-- or (q)uit

      Server key ................................ <hidden>

      TTL for the PAC ........................... 10

      Anonymous provision allowed ............... No

      ........................................

      ........................................

      Authority Information ..................... Cisco A-ID
```

Risoluzione dei problemi

Per risolvere i problemi relativi alla configurazione, è possibile utilizzare i seguenti comandi:

- **debug aaa local-auth eap method events enable**
- **debug aaa all enable**

- abilitazione pacchetto debug dot1x

Informazioni correlate

- Esempio di autenticazione EAP-FAST con i controller LAN wireless e la configurazione del server RADIUS esterno
- PEAP in Unified Wireless Networks con Microsoft Internet Authentication Service (IAS)
- Esempio di configurazione del mapping delle VLAN dinamiche con WLC basati su ACS ad Active Directory
- Guida alla configurazione di Cisco Wireless LAN Controller - Configurazione delle soluzioni di sicurezza
- Guida alla configurazione di Cisco Wireless LAN Controller - Gestione del software e delle configurazioni dei controller
- Esempio di configurazione dell'autenticazione EAP con i controller WLAN (WLC)
- Domande frequenti sul design e le caratteristiche del controller WLC (Wireless LAN Controller)
- Cisco Secure Services Client con autenticazione EAP-FAST
- Domande frequenti sui Wireless LAN Controller (WLC)
- Domande frequenti sui controller WLC (Wireless LAN Controller) e sui messaggi di sistema
- 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).