

# Esempio di configurazione del server EAP locale della rete wireless unificata

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurare l'EAP locale sul controller Cisco Wireless LAN](#)

[Configurazione EAP locale](#)

[Autorità di certificazione Microsoft](#)

[Installazione](#)

[Installare il certificato nel controller LAN wireless Cisco](#)

[Installare il certificato del dispositivo sul controller LAN wireless](#)

[Scaricare un certificato CA del fornitore sul controller LAN wireless](#)

[Configurare il controller LAN wireless per l'utilizzo di EAP-TLS](#)

[Installare il certificato dell'autorità di certificazione sul dispositivo client](#)

[Scaricare e installare un certificato CA radice per il client](#)

[Generare un certificato client per un dispositivo client](#)

[EAP-TLS con Cisco Secure Services Client sul dispositivo client](#)

[Comandi debug](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritta la configurazione di un server EAP (Extensible Authentication Protocol) locale in un controller WLC Cisco per l'autenticazione di utenti wireless.

EAP locale è un metodo di autenticazione che consente agli utenti e ai client wireless di essere autenticati localmente. 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 EAP locale, il controller funge da server di autenticazione e da database degli utenti locali, rimuovendo così la dipendenza da un server di autenticazione esterno. EAP locale recupera le credenziali utente dal database degli utenti locale o dal database back-end LDAP (Lightweight Directory Access Protocol) per autenticare gli utenti. Local EAP supporta l'autenticazione Lightweight EAP (LEAP), EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) e EAP-Transport Layer Security (EAP-TLS) tra il controller e i client wireless.

Il server EAP locale non è disponibile se nel WLC è presente una configurazione globale del server RADIUS esterno. Tutte le richieste di autenticazione vengono inoltrate al RADIUS esterno

globale finché il server EAP locale non è disponibile. Se il WLC perde la connettività al server RADIUS esterno, il server EAP locale diventa attivo. In assenza di una configurazione globale del server RADIUS, il server EAP locale diventa immediatamente attivo. Il server EAP locale non può essere utilizzato per autenticare i client connessi ad altri WLC. In altre parole, un WLC non può inoltrare la propria richiesta EAP a un altro WLC per l'autenticazione. Ogni WLC deve avere il proprio server EAP locale e il proprio database.

**Nota:** utilizzare questi comandi per impedire al WLC di inviare richieste a un server RADIUS esterno.

```
config wlan disable
    config wlan radius_server auth disable
config wlan enable
```

Il server EAP locale supporta questi protocolli nella versione software 4.1.171.0 e successive:

- LEAP
- EAP-FAST (nome utente/password e certificati)
- EAP-TLS

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di come configurare i WLC e i Lightweight Access Point (LAP) per le operazioni di base
- Conoscenza dei metodi LWAPP (Lightweight Access Point Protocol) e di sicurezza wireless
- Conoscenze base dell'autenticazione EAP locale.

### Componenti usati

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

- Windows XP con scheda adattatore CB21AG e Cisco Secure Services Client versione 4.05
- Controller LAN wireless Cisco 4400 4.1.171.0
- Autorità di certificazione Microsoft sul server Windows 2000

### Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

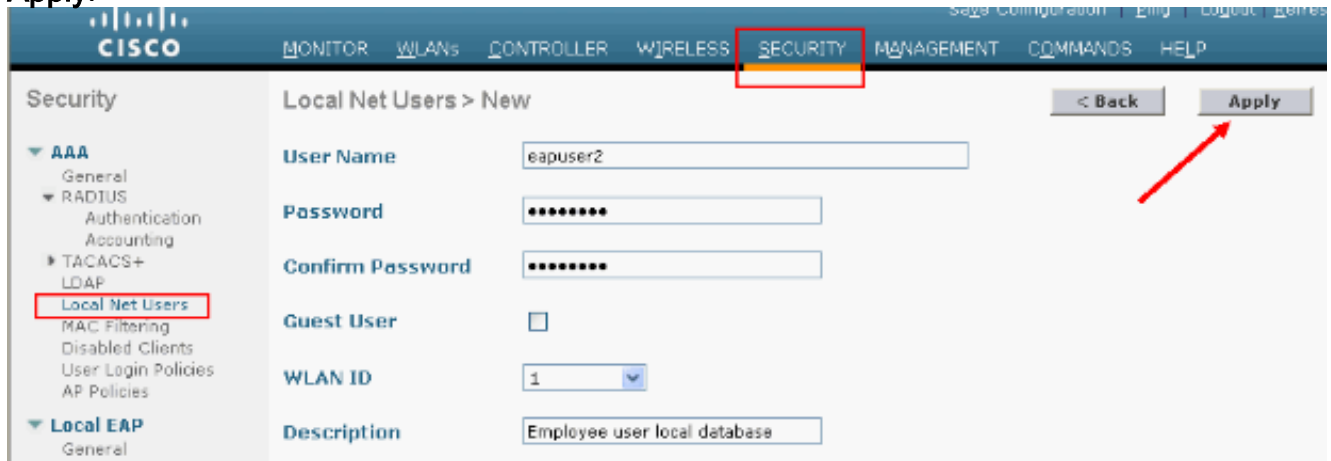
## Configurare l'EAP locale sul controller Cisco Wireless LAN

in questo documento si presume che la configurazione di base del WLC sia già stata completata.

## Configurazione EAP locale

Completare questa procedura per configurare il protocollo EAP locale:

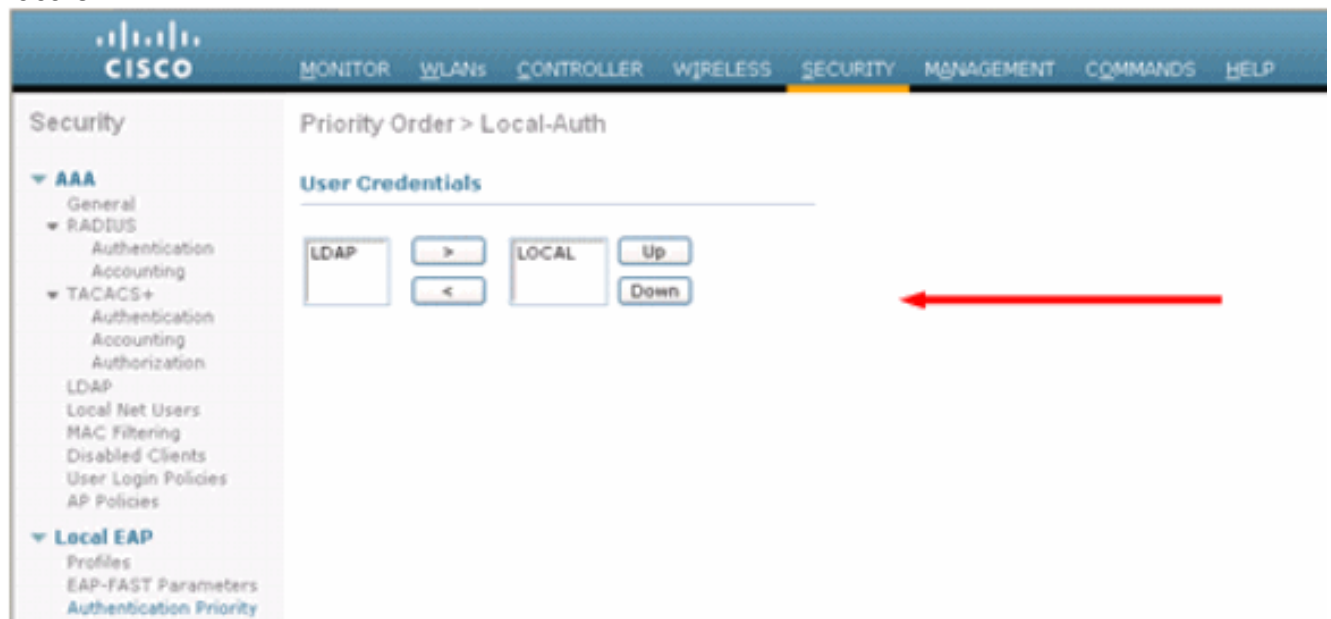
1. Aggiungere un utente di rete locale:Dalla GUI. Selezionare **Security > Local Net Users > New**, immettere il nome utente, la password, l'utente guest, l'ID WLAN e la descrizione, quindi fare clic su **Apply**.



Dalla CLI è possibile usare il comando **config netuser add <nomeutente> <password> <ID WLAN> <descrizione>** :Nota: questo comando è stato abbassato a una seconda riga per motivi di spazio.

```
(Cisco Controller) >config netuser add eapuser2 cisco123 1 Employee user local database
```

2. Specificare l'ordine di recupero delle credenziali utente.Dalla GUI, selezionare **Security > Local EAP > Authentication Priority** (Sicurezza > EAP locale > Priorità autenticazione). Quindi selezionare LDAP, fare clic sul pulsante "<" e fare clic su **Apply**. Le credenziali utente vengono inserite per prime nel database locale.

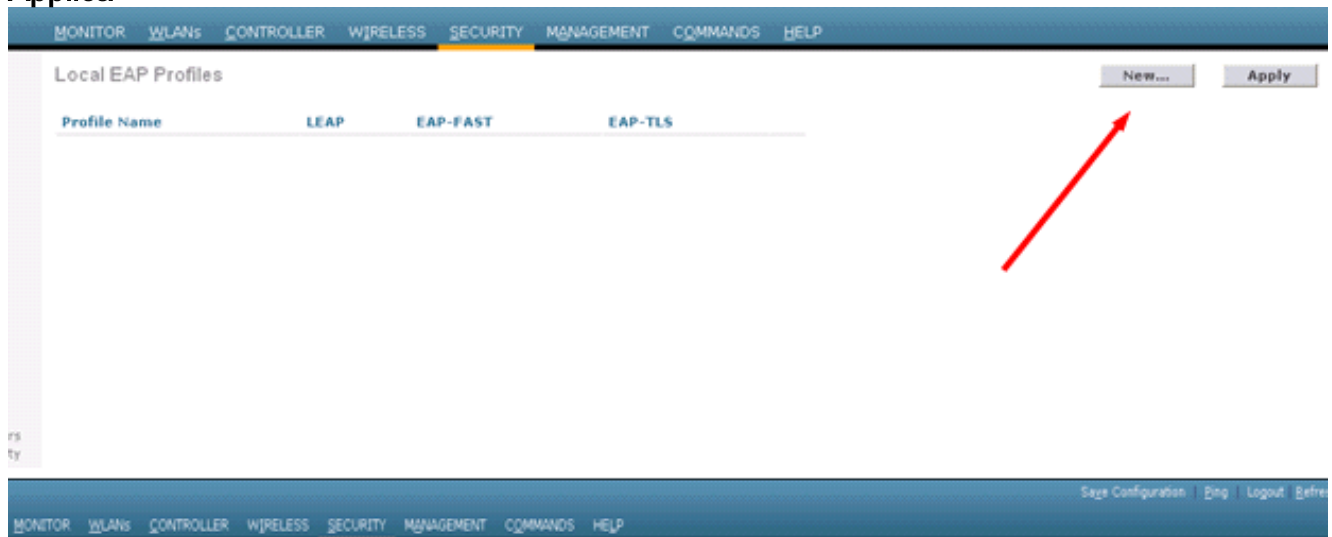


Dalla CLI:

```
(Cisco Controller) >config local-auth user-credentials local
```

3. Aggiungere un profilo EAP:Per eseguire questa operazione dalla GUI, selezionare **Security > Local EAP > Profiles** (Sicurezza > EAP locale > Profili), quindi fare clic su **New** (Nuovo).

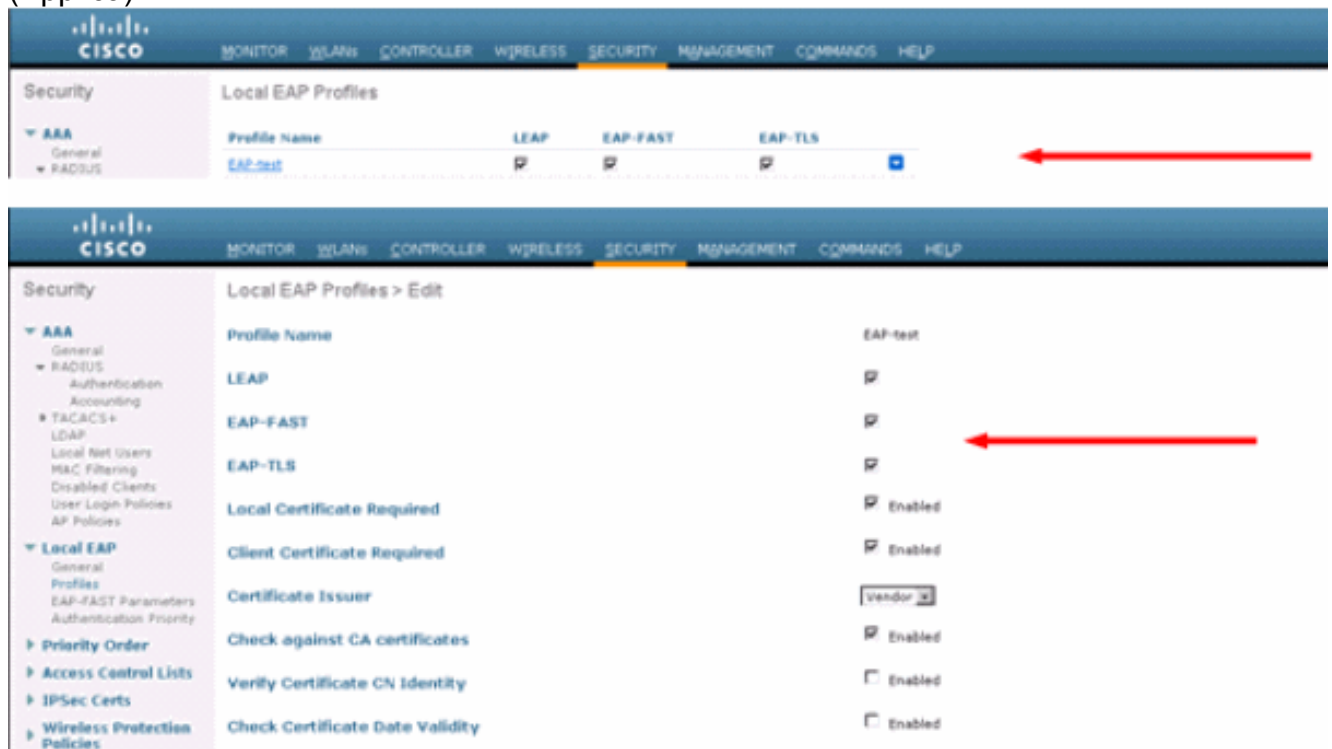
Quando viene visualizzata la nuova finestra, digitare il Nome profilo e fare clic su **Applica**.



Per eseguire questa operazione, è possibile usare anche il comando **config local-auth eap-profile add <nome-profilo>** della CLI. Nell'esempio, il nome del profilo è *EAP-test*.

(Cisco Controller) >**config local-auth eap-profile add EAP-test**

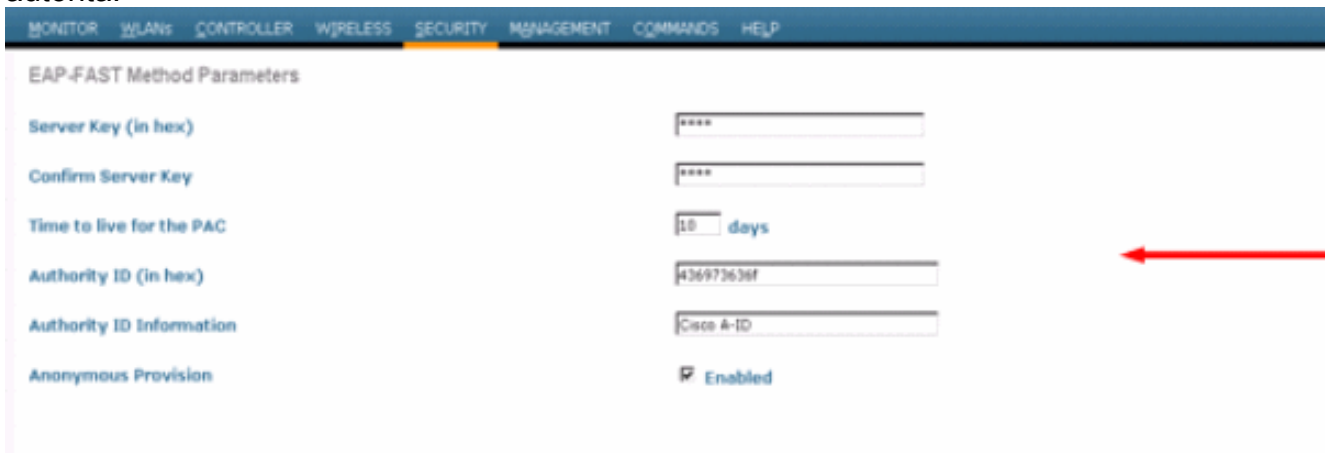
4. Aggiungere un metodo al profilo EAP. Dalla GUI, selezionare **Security > Local EAP > Profiles** (Sicurezza > EAP locale > Profili) e fare clic sul nome del profilo per cui si desidera aggiungere i metodi di autenticazione. In questo esempio vengono utilizzati LEAP, EAP-FAST e EAP-TLS. Per impostare i metodi, fare clic su **Apply** (Applica).



È inoltre possibile utilizzare il comando CLI **config local-auth eap-profile method add <nome-metodo> <nome-profilo>**. Nella configurazione di esempio vengono aggiunti tre metodi al test EAP del profilo. I metodi sono LEAP, EAP-FAST e EAP-TLS i cui nomi sono rispettivamente *leap*, *fast* e *tls*. Questo output mostra i comandi di configurazione della CLI:

```
(Cisco Controller) >config local-auth eap-profile method add leap EAP-test
(Cisco Controller) >config local-auth eap-profile method add fast EAP-test
(Cisco Controller) >config local-auth eap-profile method add tls EAP-test
```

5. Configurare i parametri del metodo EAP. Utilizzato solo per EAP-FAST. I parametri da configurare sono:**Chiave server (chiave server)** - Chiave server per crittografare/decrittografare le credenziali di accesso protette (PAC) (in esadecimale).**Durata (Time to Live) per PAC (pac-ttl)**: imposta la durata della PAC.**ID autorità (Authority-id)** - Imposta l'identificativo dell'autorità.**Provisioning anonimo (anon-provn)**: configura se il provisioning anonimo è consentito. L'opzione è abilitata per impostazione predefinita. Per la configurazione tramite la GUI, scegliere **Security > Local EAP > EAP-FAST Parameters** (Sicurezza > EAP locale > Parametri EAP-FAST) e immettere la chiave del server, la durata (TTL) della PAC, l'ID autorità (in esadecimale) e i valori delle informazioni sull'ID autorità.



The screenshot shows the 'EAP-FAST Method Parameters' configuration page in the Cisco GUI. The page has a navigation bar at the top with tabs: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, and HELP. The configuration fields are as follows:

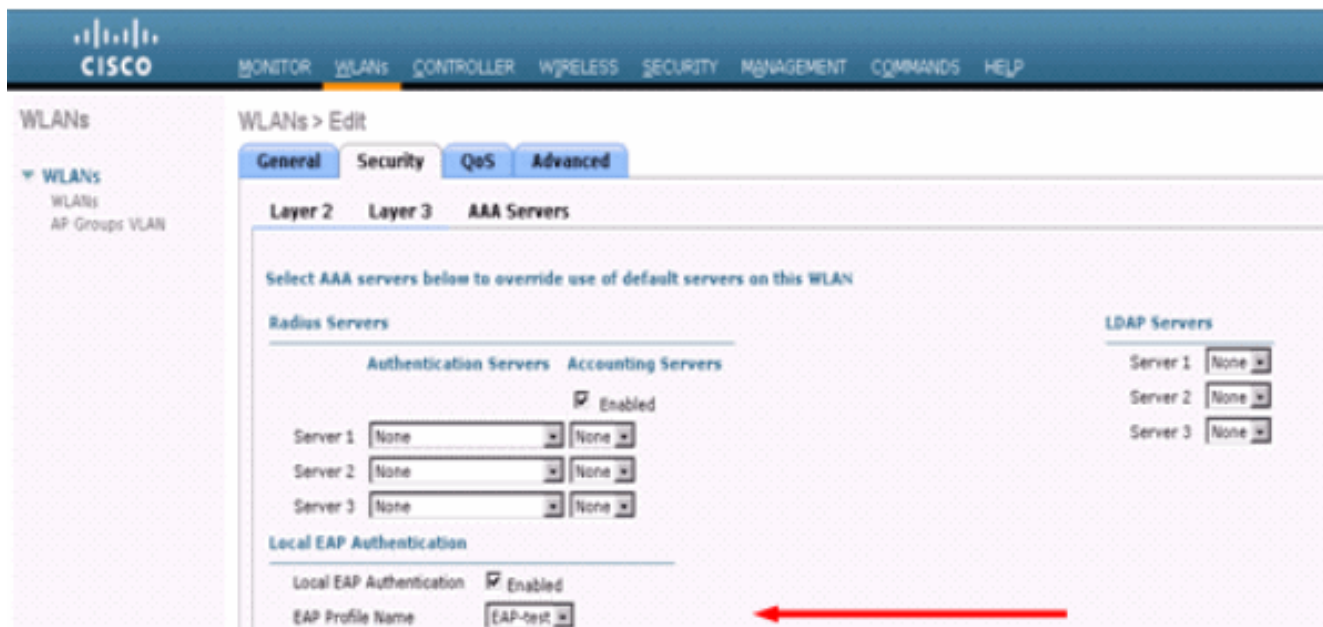
Field Name	Value
Server Key (in hex)	****
Confirm Server Key	****
Time to live for the PAC	10 days
Authority ID (in hex)	43697369f1
Authority ID Information	Cisco A-ID
Anonymous Provision	<input checked="" type="checkbox"/> Enabled

A red arrow points to the Authority ID field.

Di seguito sono riportati i comandi di configurazione CLI da utilizzare per impostare questi parametri per EAP-FAST:

```
(Cisco Controller) >config local-auth method fast server-key 12345678
(Cisco Controller) >config local-auth method fast authority-id 43697369f1 CiscoA-ID
(Cisco Controller) >config local-auth method fast pac-ttl 10
```

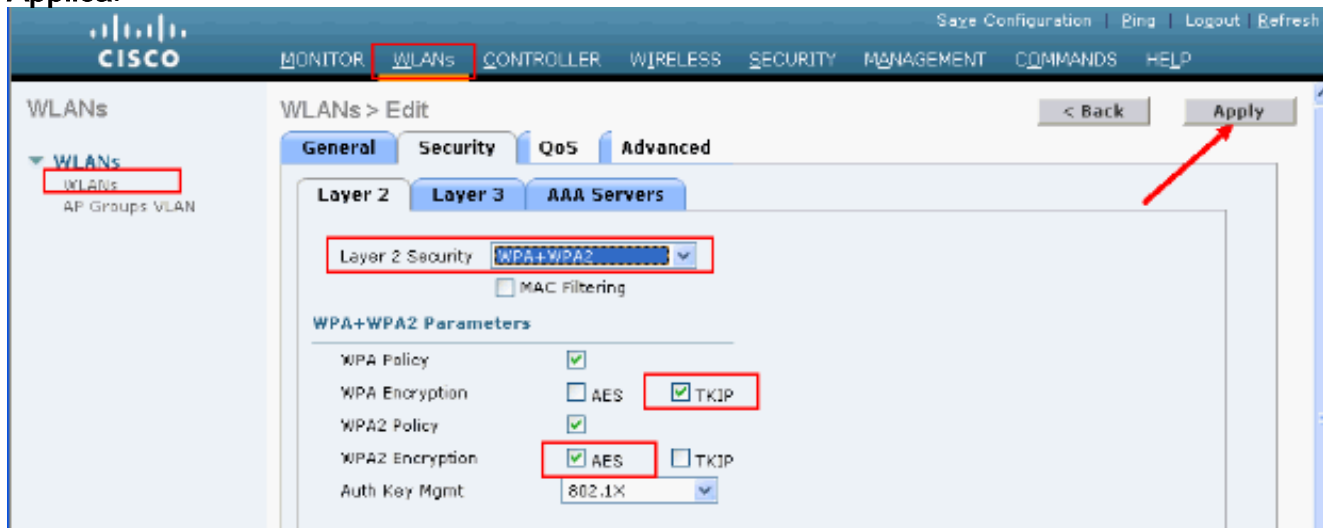
6. Abilita autenticazione locale per WLAN: Dalla GUI, selezionare **WLAN** dal menu in alto e selezionare la WLAN per cui configurare l'autenticazione locale. Viene visualizzata una nuova finestra. Selezionare la scheda **Security > AAA**. Controllare l'**autenticazione EAP locale** e selezionare il nome del profilo EAP corretto dal menu a discesa come mostrato nell'esempio seguente:



È possibile anche usare il comando di configurazione `config wlan local-auth enable <nome-profilo> <id-wlan>` della CLI, come mostrato di seguito:

```
(Cisco Controller) >config wlan local-auth enable EAP-test 1
```

- Impostare i parametri di sicurezza del layer 2. Dall'interfaccia GUI, nella finestra WLAN Edit (Modifica WLAN), selezionare **Security** > Layer 2 tab (Sicurezza > Layer 2), quindi selezionare **WPA+WPA2** dal menu a discesa Layer 2 Security (Sicurezza di Layer 2). Nella sezione Parametri WPA+WPA2, impostare la crittografia WPA su **TKIP** e la crittografia WPA2 **AES**. Quindi fare clic su **Applica**.



Dalla CLI, usare questi comandi:

```
(Cisco Controller) >config wlan security wpa enable 1
```

```
(Cisco Controller) >config wlan security wpa wpa1 ciphers tkip enable 1
```

```
(Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1
```

- Verificare la configurazione:

```
(Cisco Controller) >show local-auth config
```

User credentials database search order:

```
Primary ..... Local DB
```

Timer:

```
Active timeout ..... Undefined
```

Configured EAP profiles:

```

Name ..... EAP-test
Certificate issuer ..... cisco
Peer verification options:
  Check against CA certificates ..... Enabled
  Verify certificate CN identity ..... Disabled
  Check certificate date validity ..... Enabled
EAP-FAST configuration:
  Local certificate required ..... No
  Client certificate required ..... No
Enabled methods ..... leap fast tls
Configured on WLANs ..... 1

```

EAP Method configuration:

```

EAP-FAST:
--More-- or (q)uit
  Server key ..... <hidden>
  TTL for the PAC ..... 10
  Anonymous provision allowed ..... Yes
  Authority ID ..... 43697369f10000000000000000000000
  Authority Information ..... CiscoA-ID

```

Per visualizzare parametri specifici della wlan 1, usare il comando **show wlan <id wlan>**:

(Cisco Controller) **>show wlan 1**

```

WLAN Identifier..... 1
Profile Name..... austinlab
Network Name (SSID)..... austinlab
Status..... Disabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
Interface..... management
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
--More-- or (q)uit
IPv6 Support..... Disabled
Radio Policy..... All
Local EAP Authentication..... Enabled (Profile 'EAP-test')
Security

```

```

802.11 Authentication:..... Open System
Static WEP Keys..... Disabled
802.1X..... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Enabled
  WPA (SSN IE)..... Enabled
    TKIP Cipher..... Enabled
    AES Cipher..... Disabled
  WPA2 (RSN IE)..... Enabled
    TKIP Cipher..... Disabled
    AES Cipher..... Enabled

```

Auth Key Management

```

802.1x..... Enabled
PSK..... Disabled

```

```

CCKM..... Disabled
CKIP ..... Disabled
IP Security..... Disabled
IP Security Passthru..... Disabled
Web Based Authentication..... Disabled
--More-- or (q)uit
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Auto Anchor..... Disabled
Cranite Passthru..... Disabled
Fortress Passthru..... Disabled
H-REAP Local Switching..... Disabled
Infrastructure MFP protection..... Enabled
                                (Global Infrastructure MFP Disabled)
Client MFP..... Optional
Tkip MIC Countermeasure Hold-down Timer..... 60

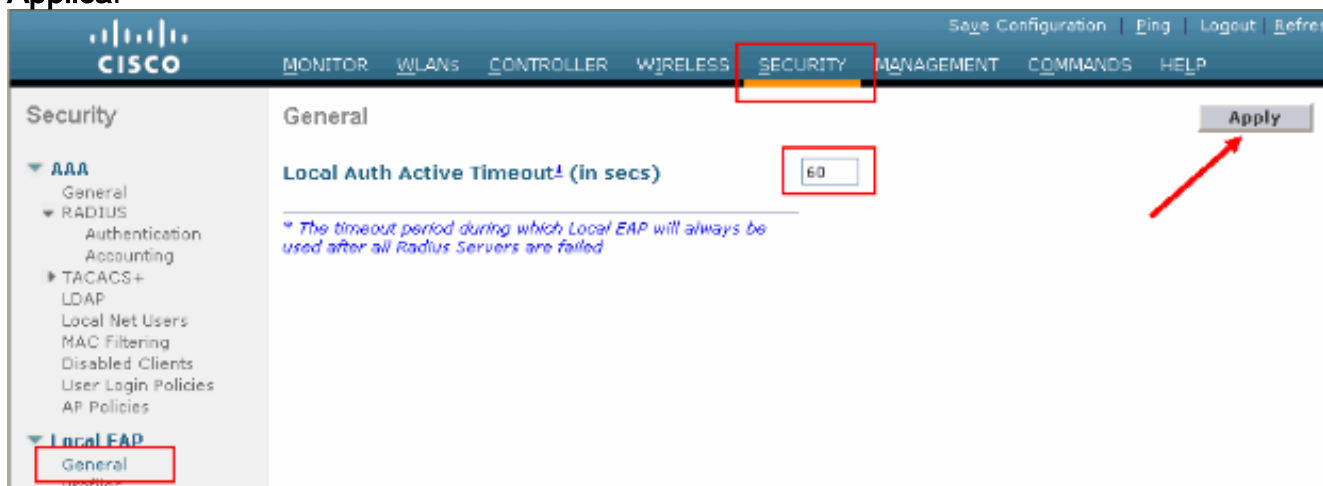
```

```

Mobility Anchor List
WLAN ID      IP Address      Status

```

È possibile configurare altri parametri di autenticazione locale, in particolare il timer di timeout attivo. Questo timer configura il periodo di utilizzo dell'EAP locale dopo un errore di tutti i server RADIUS. Dalla GUI, selezionare **Security > Local EAP > General (Sicurezza > EAP locale > Generale)**, quindi impostare il valore dell'ora. Quindi fare clic su **Applica**.



Dalla CLI, usare questi comandi:

```

(Cisco Controller) >config local-auth active-timeout ?
<1 to 3600> Enter the timeout period for the Local EAP to remain active,
in seconds.
(Cisco Controller) >config local-auth active-timeout 60

```

Per verificare il valore su cui è impostato il timer, usare il comando **show local-auth config**.

```

(Cisco Controller) >show local-auth config

```

User credentials database search order:

```

Primary ..... Local DB

```

**Timer:**

```

Active timeout ..... 60

```

Configured EAP profiles:

```

Name ..... EAP-test
... Skip

```

- Per generare e caricare la PAC manuale, è possibile usare la GUI o la CLI. Dalla GUI, selezionare **COMMANDS** dal menu in alto e selezionare **Upload File** dall'elenco a destra. Selezionare **PAC (Protected Access Credential)** dal menu a discesa Tipo file. Immettere tutti



i parametri e fare clic su Upload.

Dalla CLI, immettere questi comandi:

```
(Cisco Controller) >transfer upload datatype pac
(Cisco Controller) >transfer upload pac ?
```

username      Enter the user (identity) of the PAC

```
(Cisco Controller) >transfer upload pac test1 ?
```

<validity>      Enter the PAC validity period (days)

```
(Cisco Controller) >transfer upload pac test1 60 ?
```

<password>      Enter a password to protect the PAC

```
(Cisco Controller) >transfer upload pac test1 60 cisco123
```

```
(Cisco Controller) >transfer upload serverip 10.1.1.1
```

```
(Cisco Controller) >transfer upload filename manual.pac
```

```
(Cisco Controller) >transfer upload start
```

```
Mode..... TFTP
TFTP Server IP..... 10.1.1.1
TFTP Path..... /
TFTP Filename..... manual.pac
Data Type..... PAC
PAC User..... test1
PAC Validity..... 60 days
PAC Password..... cisco123
```

Are you sure you want to start? (y/N) y

PAC transfer starting.

File transfer operation completed successfully.

## [Autorità di certificazione Microsoft](#)

Per utilizzare l'autenticazione EAP-FAST versione 2 e EAP-TLS, il WLC e tutti i dispositivi client

devono disporre di un certificato valido e devono inoltre conoscere il certificato pubblico dell'Autorità di certificazione.

## Installazione

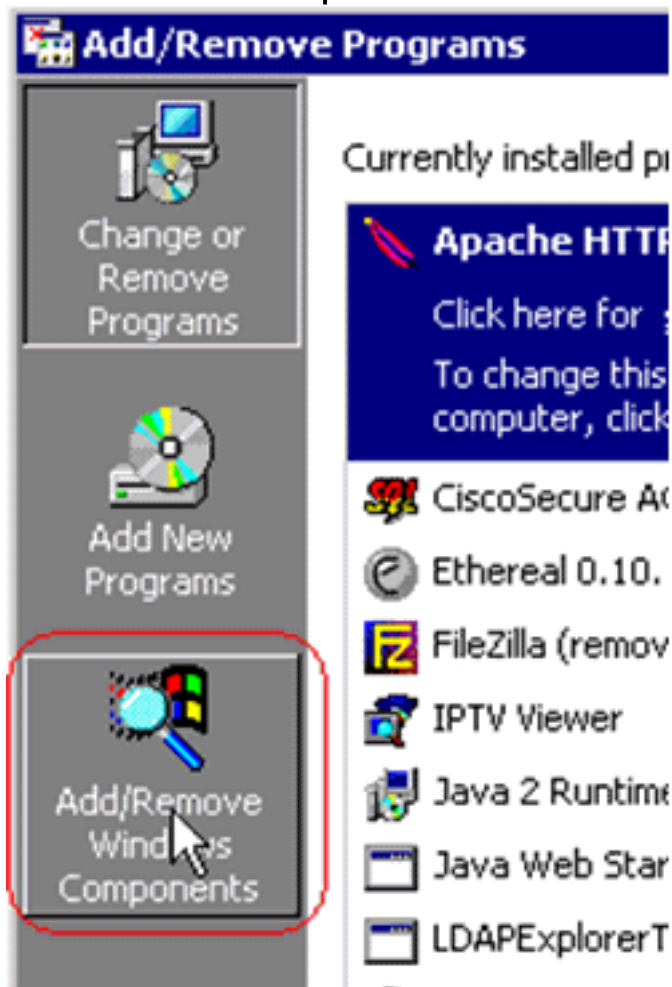
Se in Windows 2000 Server non sono già installati i servizi Autorità di certificazione, è necessario installarli.

Completare questa procedura per attivare l'Autorità di certificazione Microsoft su un server Windows 2000:

1. Dal Pannello di controllo, scegliere **Installazione applicazioni**.



2. Selezionare **Installazione componenti di Windows** sul lato

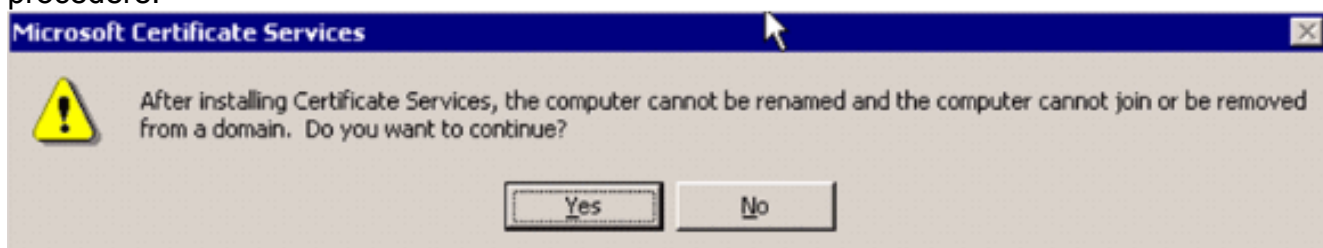


sinistro.

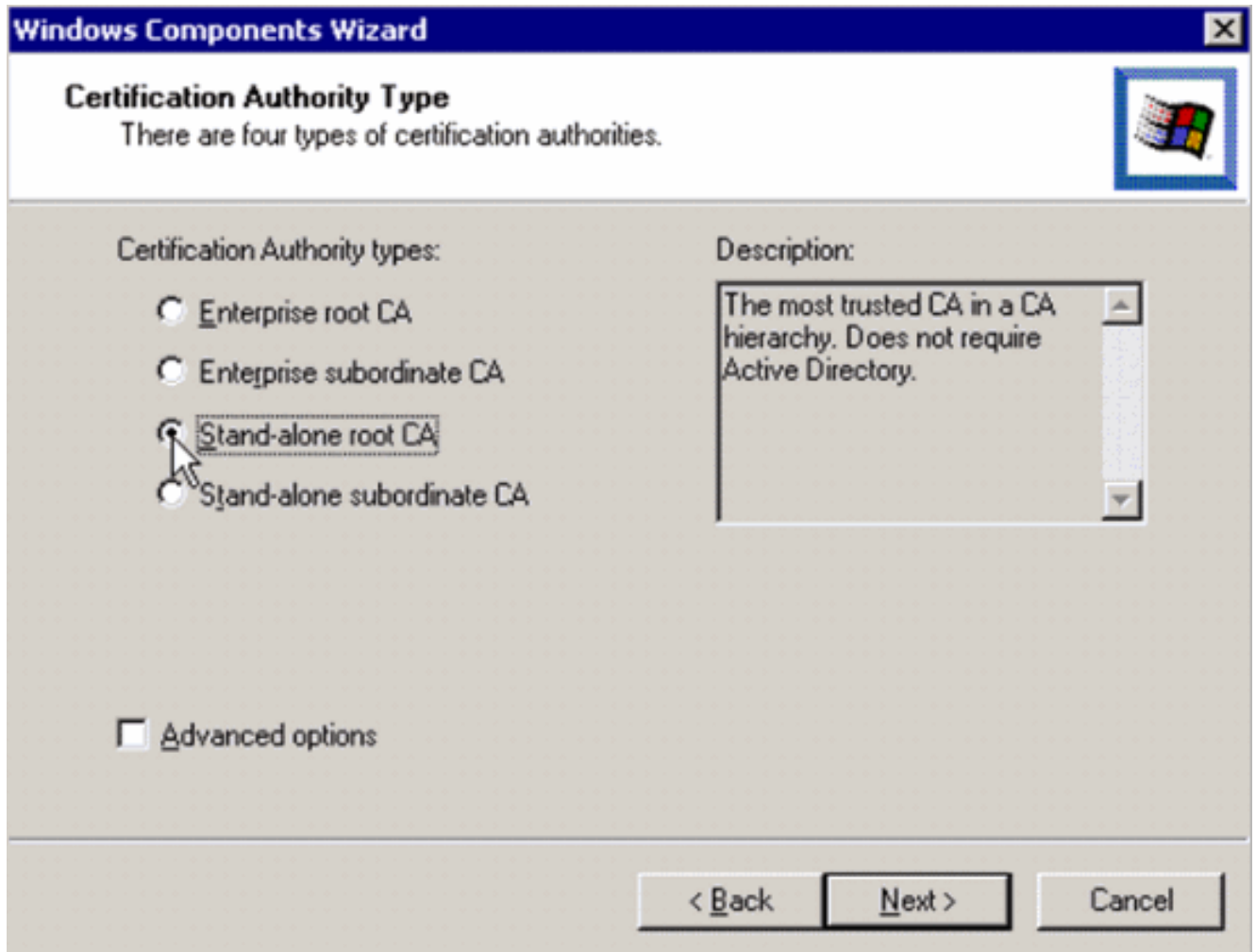
3. Controllare **Servizi certificati**.



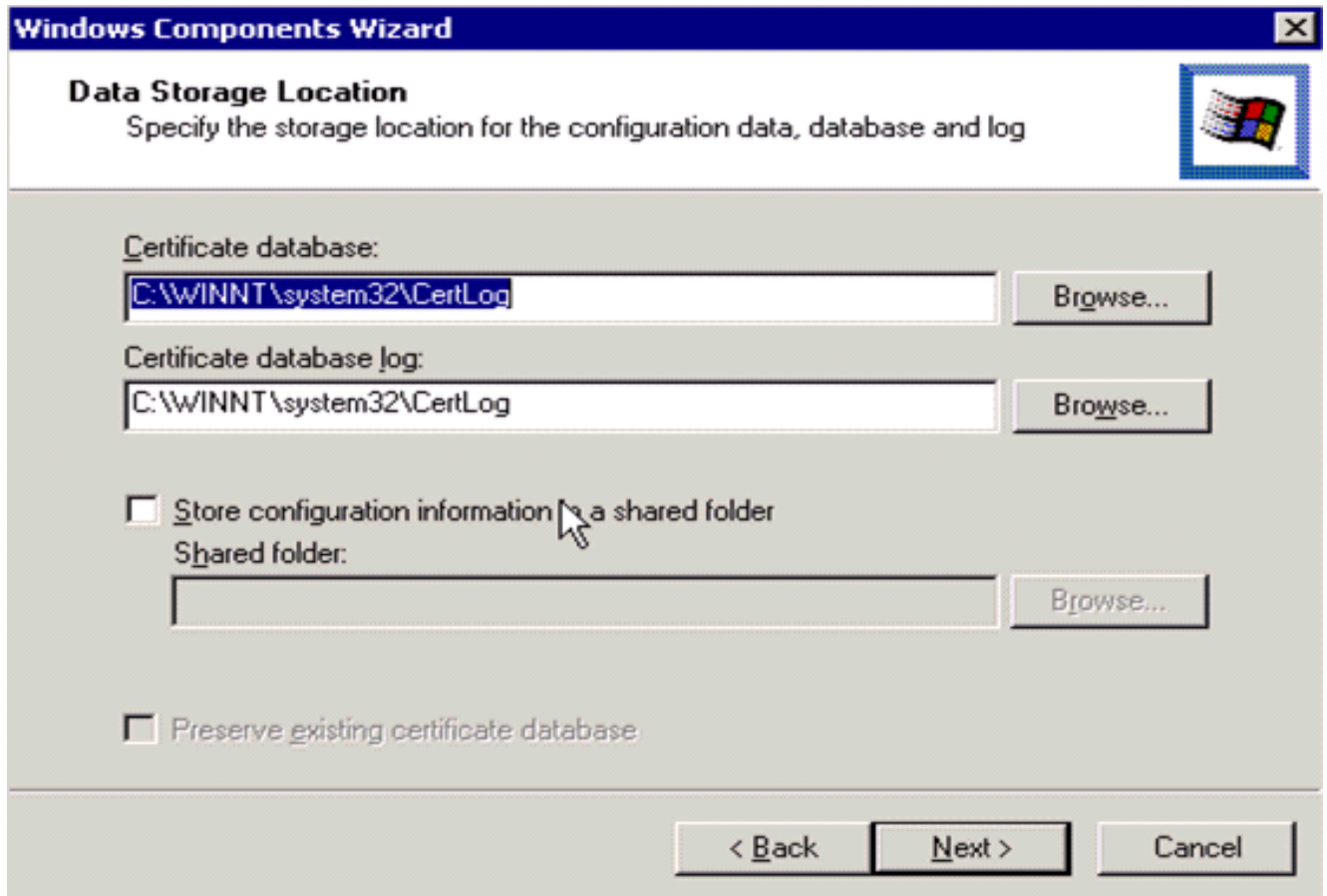
Esaminare questo avviso prima di procedere:



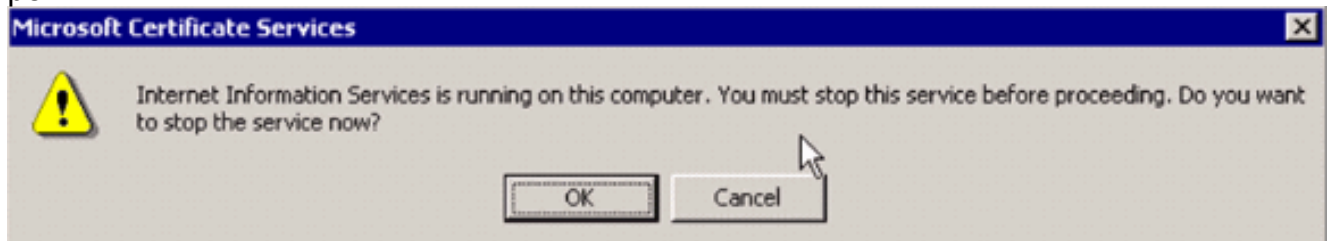
4. Selezionare il tipo di Autorità di certificazione da installare. Per creare un'autorità autonoma semplice, selezionare **CA radice autonoma (Standalone)**.



5. Immettere le informazioni necessarie sull'Autorità di certificazione. Questa informazione consente di creare un certificato autofirmato per l'Autorità di certificazione. Ricordare il nome della CA utilizzato. L'Autorità di certificazione archivia i certificati in un database. In questo esempio viene utilizzata l'impostazione predefinita proposta da Microsoft:



6. I servizi Autorità di certificazione Microsoft utilizzano il server Web Microsoft IIS per creare e gestire certificati client e server. È necessario riavviare il servizio IIS per:



Il nuovo servizio verrà ora installato da Microsoft Windows 2000 Server. Per installare i nuovi componenti di Windows, è necessario disporre del CD di installazione di Windows 2000 Server. L'Autorità di certificazione è ora installata.

## [Installare il certificato nel controller LAN wireless Cisco](#)

Per utilizzare EAP-FAST versione 2 e EAP-TLS sul server EAP locale di un controller LAN wireless Cisco, attenersi alla seguente procedura:

1. [Installare il certificato del dispositivo sul controller LAN wireless.](#)
2. [Scaricare un certificato CA del fornitore nel controller LAN wireless.](#)
3. [Configurare il controller LAN wireless per l'utilizzo di EAP-TLS.](#)

Si noti che nell'esempio riportato in questo documento Access Control Server (ACS) viene installato sullo stesso host in cui si trovano Microsoft Active Directory e Microsoft Certification Authority, ma la configurazione deve essere la stessa se il server ACS si trova su un server diverso.

## Installare il certificato del dispositivo sul controller LAN wireless

Attenersi alla seguente procedura:

1. Per generare il certificato da importare sul WLC, completare i seguenti passaggi: Visitare il sito Web all'indirizzo **http://<serverIpAddr>/certsrv**. Scegliere **Richiedi certificato** e fare clic su **Avanti**. Scegliere **Richiesta avanzata** e fare clic su **Avanti**. Scegliere **Invia una richiesta di certificato a questa CA utilizzando un modulo** e fare clic su **Avanti**. Scegliere **Server Web** per Modello di certificato e immettere le informazioni appropriate. Contrassegnare quindi le chiavi come **esportabili**. A questo punto si riceve un certificato da installare nel computer.
2. Per recuperare il certificato dal PC, completare i seguenti passaggi: Aprire un browser Internet Explorer e scegliere **Strumenti > Opzioni Internet > Contenuto**. Fare clic su **Certificati**. Selezionare il certificato appena installato dal menu a discesa. Fare clic su **Esporta**. Fare clic su **Avanti** due volte e scegliere **Sì per esportare la chiave privata**. Questo formato è PKCS#12 (formato .PFX). Scegliere **Abilita protezione avanzata**. Digitare una password. Salvarlo in un file <time2.pfx>.
3. Copiare il certificato nel formato PKCS#12 in qualsiasi computer in cui è installato Openssl per convertirlo nel formato PEM.

```
openssl pkcs12 -in tme2.pfx -out tme2.pem
```

```
!--- The command to be given, -in Enter Import Password: !--- Enter the password given previously, from step 2g. MAC verified OK Enter PEM pass phrase: !--- Enter a phrase. Verifying - Enter PEM pass phrase:
```

4. Scaricare il certificato del dispositivo in formato PEM convertito nel WLC.

```
(Cisco Controller) >transfer download datatype eapdevcert
```

```
(Cisco Controller) >transfer download certpassword password
```

```
!--- From step 3. Setting password to <cisco123> (Cisco Controller) >transfer download filename tme2.pem
```

```
(Cisco Controller) >transfer download start
```

```
Mode..... TFTP
Data Type..... Vendor Dev Cert
TFTP Server IP..... 10.1.1.12
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... /
TFTP Filename..... tme2.pem
```

```
This may take some time.
```

```
Are you sure you want to start? (y/N) y
```

```
TFTP EAP Dev cert transfer starting.
```

```
Certificate installed.
```

```
Reboot the switch to use new certificate.
```

5. Una volta riavviato, controllare il certificato.

```
(Cisco Controller) >show local-auth certificates
```

```
Certificates available for Local EAP authentication:
```

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

```
CA certificate:
```

```
Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
```

```
Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
```

```
Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT
```

```
Device certificate:
```

Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme2  
Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme  
Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT

## [Scaricare un certificato CA del fornitore sul controller LAN wireless](#)

Attenersi alla seguente procedura:

1. Per recuperare il certificato CA del fornitore, completare la procedura seguente: Visitare il sito Web all'indirizzo <http://<serverIpAddr>/certsrv>. Scegliere **Recupera il certificato CA** e fare clic su **Avanti**. Scegliere il certificato CA. Fare clic su **Codificato DER**. Fare clic su **Scarica certificato CA** e salvare il certificato come **rootca.cer**.
2. Convertire la CA del fornitore dal formato DER al formato PEM con il comando **openssl x509 -in rootca.cer -inform DER -out rootca.pem -outform PEM**. Il file di output è **rootca.pem** nel formato PEM.
3. Scaricare il certificato CA del fornitore:

```
(Cisco Controller) >transfer download datatype eapcert
```

```
(Cisco Controller) >transfer download filename ?
```

```
<filename>      Enter filename up to 16 alphanumeric characters.
```

```
(Cisco Controller) >transfer download filename rootca.pem
```

```
(Cisco Controller) >transfer download start ?
```

```
(Cisco Controller) >transfer download start
```

```
Mode..... TFTP
Data Type..... Vendor CA Cert
TFTP Server IP..... 10.1.1.12
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... /
TFTP Filename..... rootca.pem
```

```
This may take some time.
```

```
Are you sure you want to start? (y/N) y
```

```
TFTP EAP CA cert transfer starting.
```

```
Certificate installed.
```

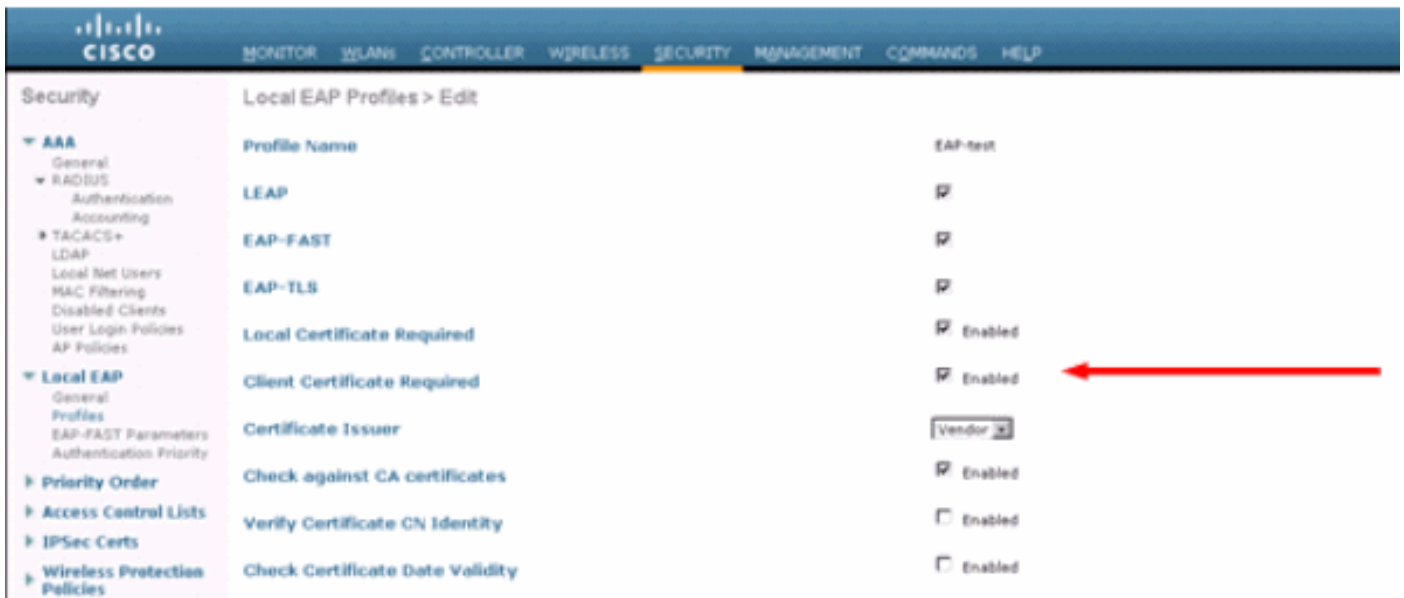
```
Reboot the switch to use new certificate.
```

## [Configurare il controller LAN wireless per l'utilizzo di EAP-TLS](#)

Attenersi alla seguente procedura:

Dalla GUI, selezionare **Security > Local EAP > Profiles**, scegliere il profilo e controllare le seguenti impostazioni:

- Il certificato locale obbligatorio è abilitato.
- Il certificato client richiesto è abilitato.
- L'autorità di certificazione è il fornitore.
- Il controllo dei certificati CA è abilitato.



## [Installare il certificato dell'autorità di certificazione sul dispositivo client](#)

### [Scaricare e installare un certificato CA radice per il client](#)

Il client deve ottenere un certificato CA radice da un server Autorità di certificazione. Esistono diversi metodi per ottenere un certificato client e installarlo nel computer Windows XP. Per ottenere un certificato valido, è necessario che l'utente di Windows XP abbia eseguito l'accesso utilizzando il proprio ID utente e che disponga di una connessione di rete.

Per ottenere un certificato client dal server dell'Autorità di certificazione principale privato, sono stati utilizzati un browser Web nel client Windows XP e una connessione cablata alla rete. Questa procedura viene utilizzata per ottenere il certificato client da un server Microsoft Certification Authority:

1. Utilizzare un browser Web nel client e puntare il browser al server Autorità di certificazione. A tale scopo, immettere **http://IP-address-of-Root-CA/certsrv**.
2. Accedere utilizzando **Nome\_dominio\nome\_utente**. È necessario eseguire l'accesso utilizzando il nome utente della persona che utilizzerà il client XP.
3. Nella finestra iniziale scegliere **Recupera certificato CA** e fare clic su **Avanti**.
4. Selezionare **Codifica Base64** e **Scarica certificato CA**.
5. Nella finestra Certificato rilasciato fare clic su **Installa il certificato** e quindi su **Avanti**.
6. Scegliere **Seleziona automaticamente l'archivio certificati** e fare clic su **Avanti**, per visualizzare il messaggio di importazione.
7. Connettersi all'Autorità di certificazione per recuperare il certificato dell'Autorità di certificazione:



## Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

### Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

Next >

## Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

### Choose file to download:

CA Certificate:

DER encoded or  Base 64 encoded

[Download CA certificate](#)

[Download CA certification path](#)

[Download latest certificate revocation list](#)

## 8. Fare clic su Scarica certificato CA.

## Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

### Choose file to download:

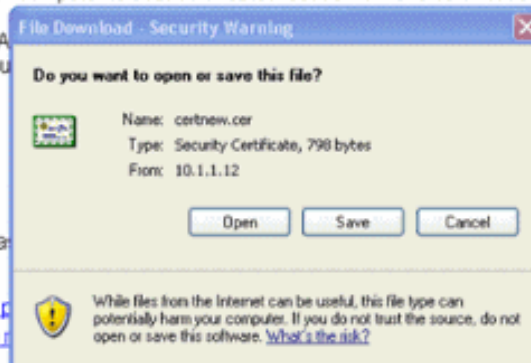
CA Certificate:

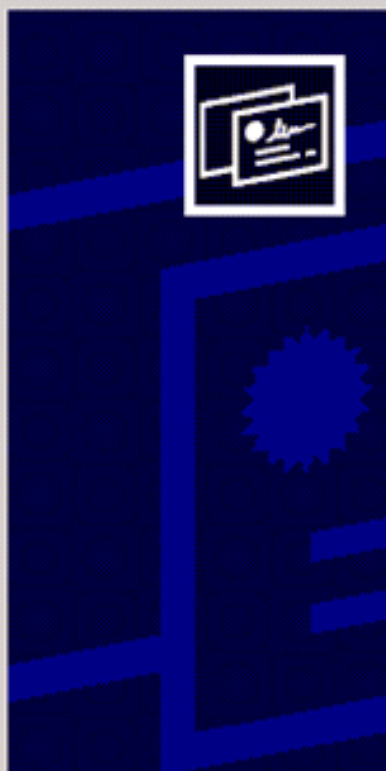
DER encoded or  Base 64 encoded

[Download CA certificate](#)

[Download CA certification path](#)

[Download latest certificate revocation list](#)





## Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

&lt; Back

Next &gt;

Cancel

### Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

- Automatically select the certificate store based on the type of certificate
- Place all certificates in the following store

Certificate store:

Browse...

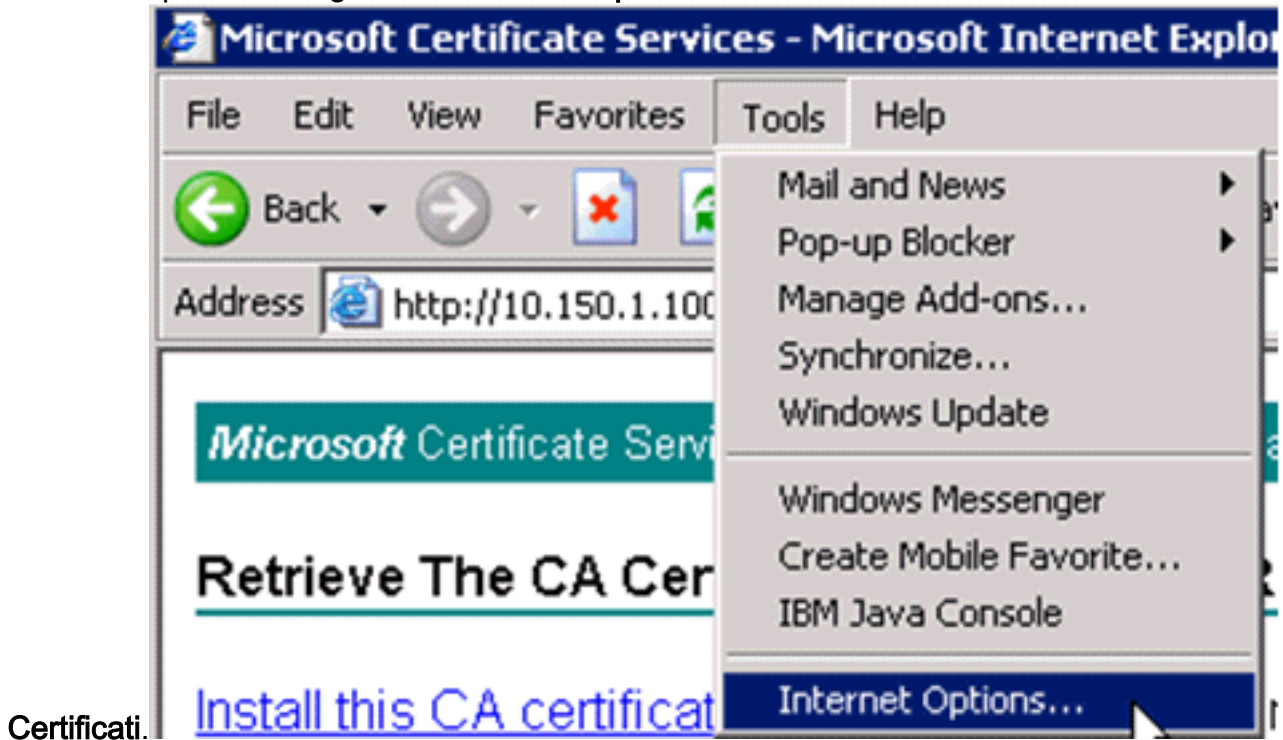
&lt; Back

Next &gt;

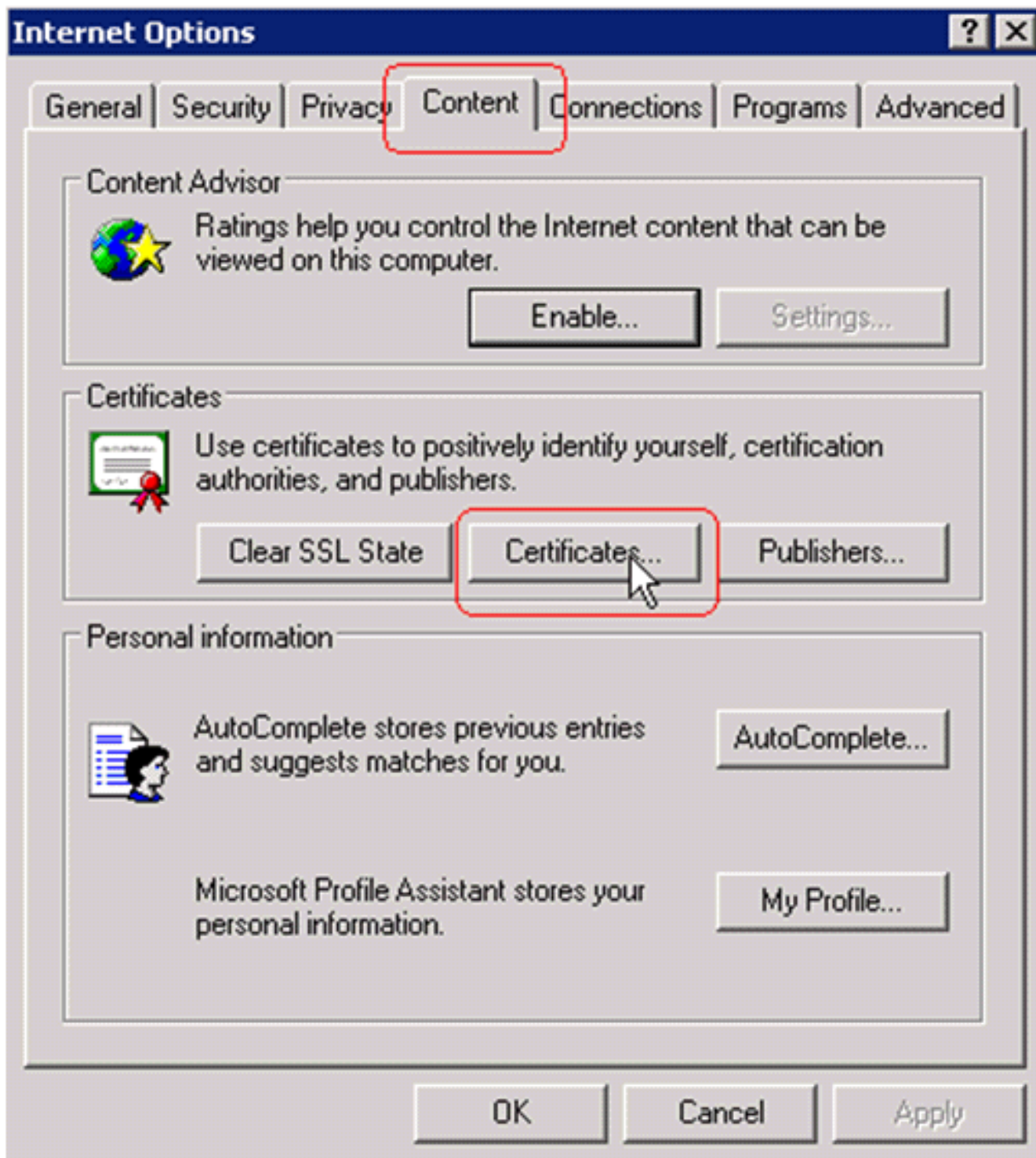
Cancel



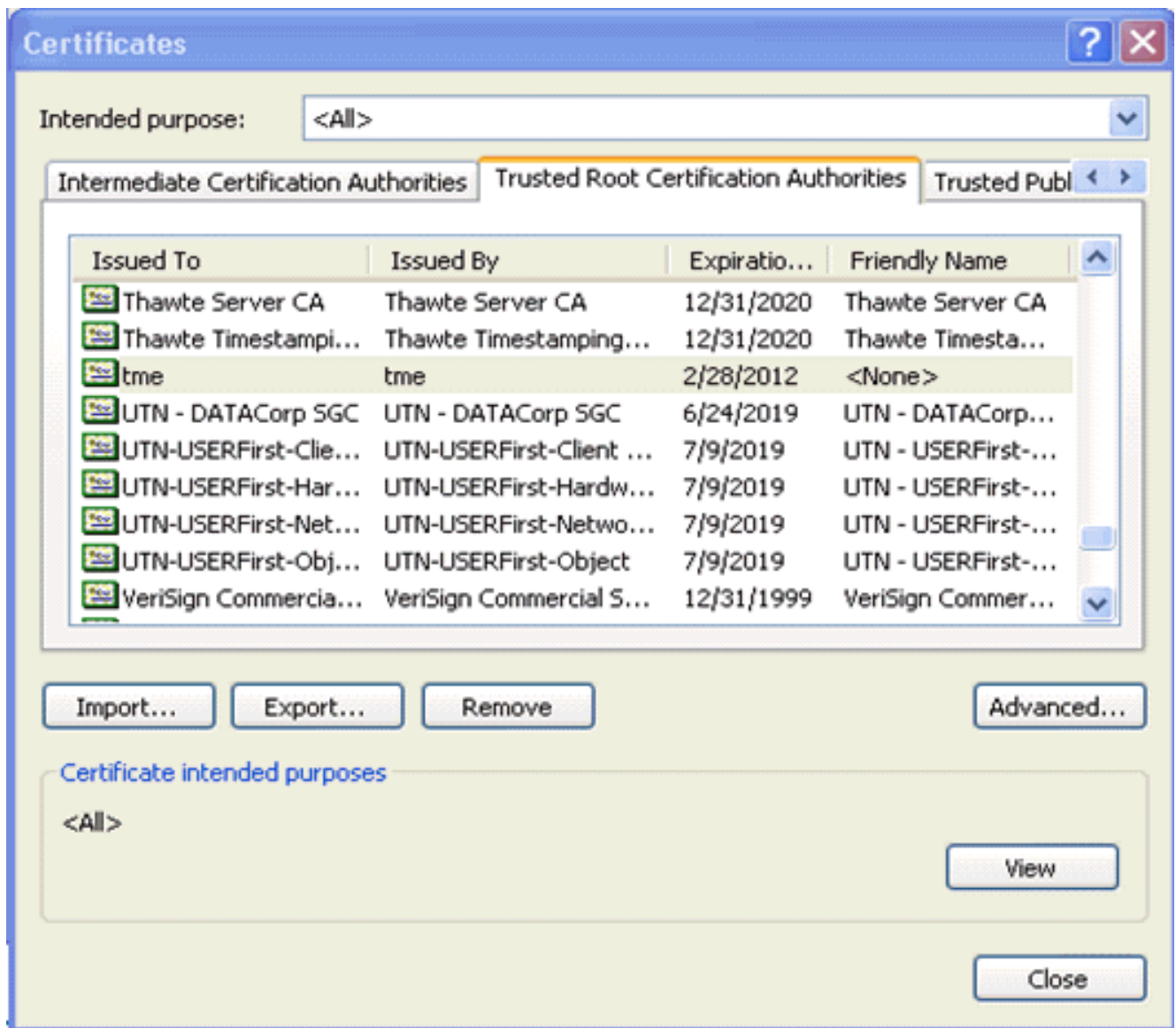
9. Per verificare che il certificato dell'Autorità di certificazione sia installato correttamente, aprire Internet Explorer e scegliere **Strumenti > Opzioni Internet > Contenuto >**



Certificati.



In Autorità di certificazione principale attendibile dovrebbe essere visualizzata la nuova Autorità di certificazione installata:



## Generare un certificato client per un dispositivo client

Per autenticare un client WLAN EAP-TLS, il client deve ottenere un certificato da un server dell'Autorità di certificazione per il WLC. Per ottenere un certificato client e installarlo nel computer Windows XP è possibile utilizzare diversi metodi. Per ottenere un certificato valido, è necessario che l'utente di Windows XP abbia eseguito l'accesso utilizzando il proprio ID utente e che disponga di una connessione di rete (connessione cablata o WLAN con protezione 802.1x disattivata).

Per ottenere un certificato client dal server dell'Autorità di certificazione principale privato, vengono utilizzati un browser Web sul client Windows XP e una connessione cablata alla rete. Questa procedura viene utilizzata per ottenere il certificato client da un server Microsoft Certification Authority:

1. Utilizzare un browser Web nel client e puntare il browser al server Autorità di certificazione. A tale scopo, immettere **http://IP-address-of-Root-CA/certsrv**.
2. Accedere utilizzando **Nome\_dominio\nome\_utente**. È necessario eseguire l'accesso utilizzando il nome utente della persona che utilizza il client XP. Il nome utente viene incorporato nel certificato client.
3. Nella finestra iniziale scegliere **Richiedi certificato** e fare clic su **Avanti**.
4. Scegliere **Richiesta avanzata** e fare clic su **Avanti**.

5. Scegliere **Invia una richiesta di certificato a questa CA utilizzando un modulo** e fare clic su **Avanti**.
6. Nel modulo Richiesta avanzata di certificati scegliere il modello di certificato come **utente**, specificare la dimensione della chiave come **1024** e fare clic su **Invia**.
7. Nella finestra Certificato rilasciato fare clic su **Installa il certificato**. In questo modo l'installazione di un certificato client nel client Windows XP è riuscita.

Microsoft Certificate Services -- time [Home](#)

---

**Welcome**

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

**Select a task:**

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate


[Next >](#)

Microsoft Certificate Services -- time [Home](#)

---

**Choose Request Type**

Please select the type of request you would like to make:

- User certificate request  

- Advanced request

[Next >](#)

Microsoft Certificate Services -- time [Home](#)

---

**Advanced Certificate Requests**

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.  
*You must have an enrollment agent certificate to submit a request for another user.*

[Next >](#)

8. Selezionare **Certificato di autenticazione**

## Advanced Certificate Request

### Certificate Template:

User

### Key Options:

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage:  Exchange  Signature  Both

Key Size: 512 Min: 384 Max: 1024 (common key sizes: 512 1024)

- Create new key set
  - Set the container name
- Use existing key set
- Enable strong private key protection
- Mark keys as exportable
  - Export keys to file
- Use local machine store

*You must be an administrator to generate a key in the local machine store.*

### Additional Options:

Hash Algorithm: SHA-1

*Only used to sign request.*

Save request to a PKCS #10 file

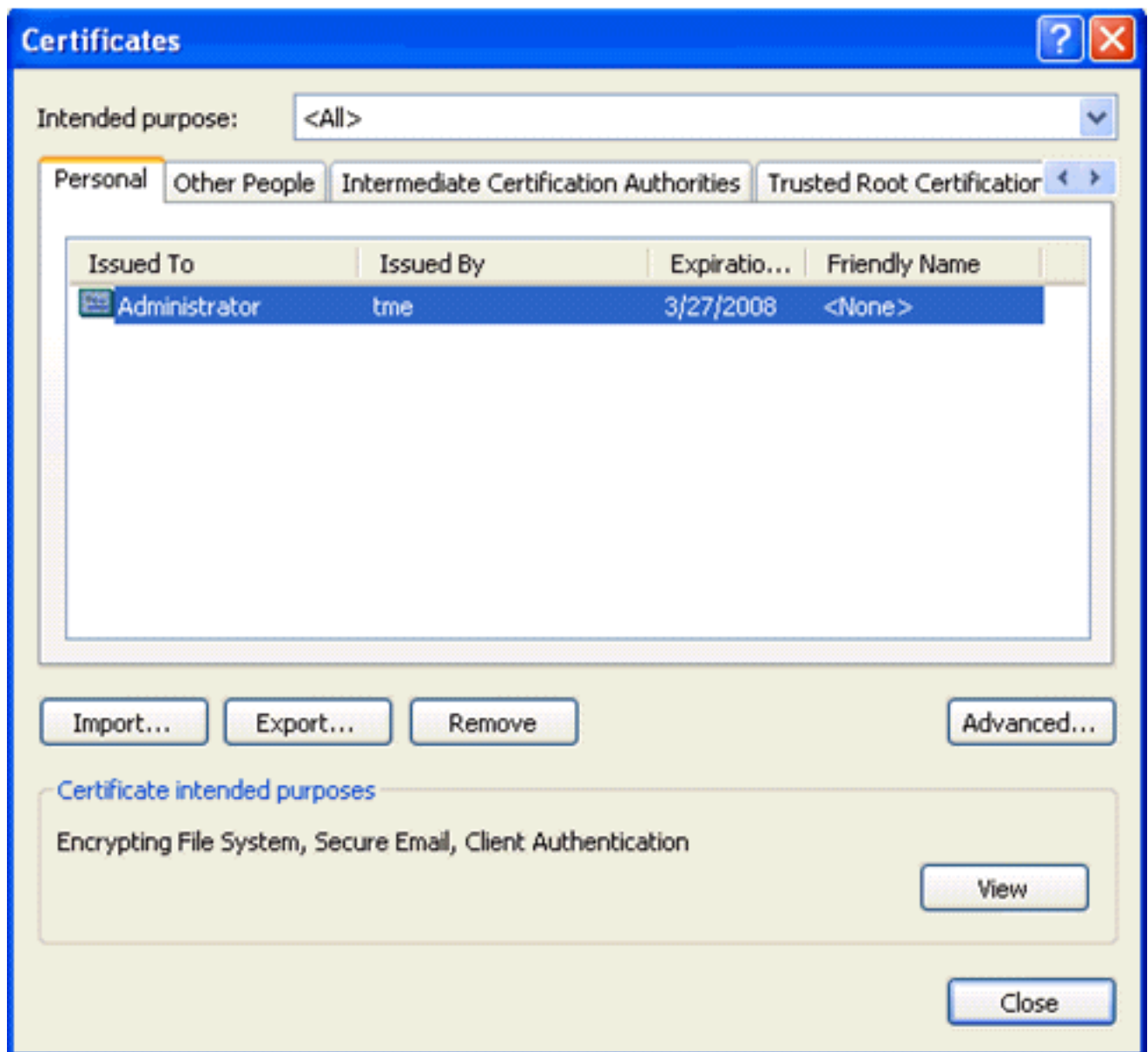
Attributes:

client.

II

certificato client è stato creato.

9. Per verificare che il certificato sia installato, andare in Internet Explorer e scegliere **Strumenti > Opzioni Internet > Contenuto > Certificati**. Nella scheda Personale dovrebbe essere visualizzato il certificato.



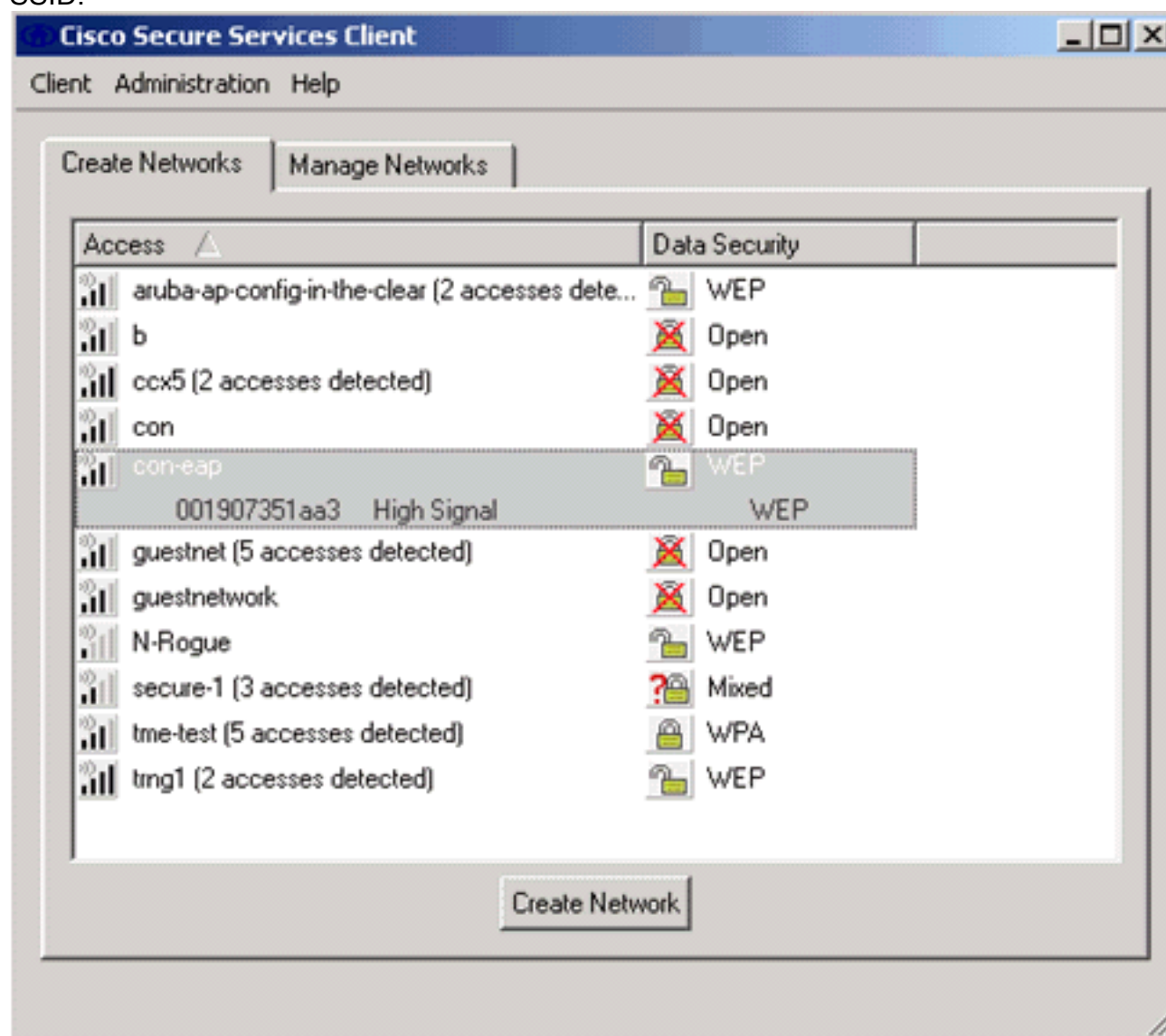
## EAP-TLS con Cisco Secure Services Client sul dispositivo client

Attenersi alla seguente procedura:

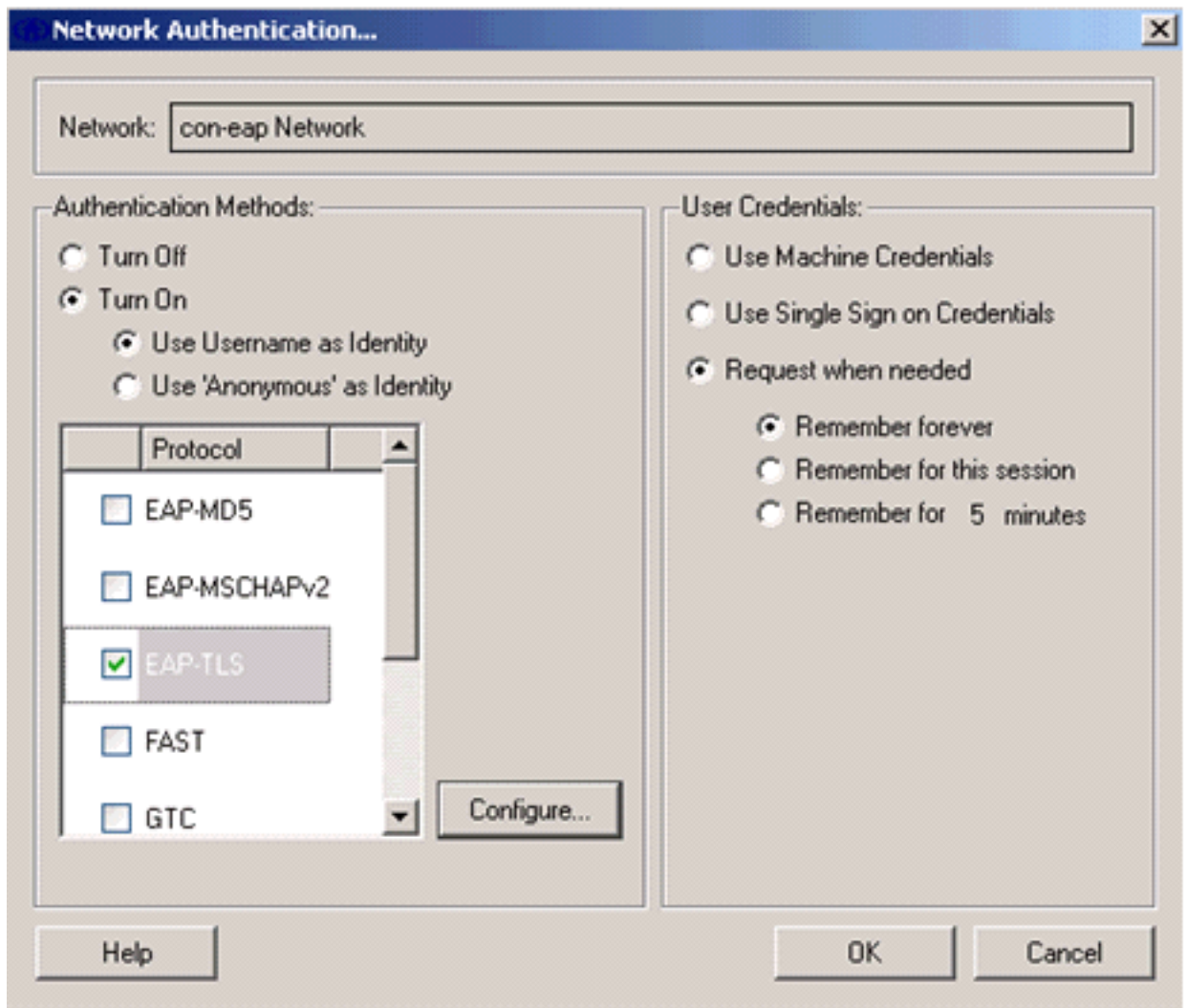
1. Per impostazione predefinita, il WLC trasmette l'SSID, quindi viene visualizzato nell'elenco Crea reti degli SSID analizzati. Per creare un profilo di rete, è possibile fare clic sul SSID nella lista (Enterprise) e fare clic su **Crea rete**. Se l'infrastruttura WLAN è configurata con SSID broadcast disabilitato, è necessario aggiungere manualmente l'SSID. A tale scopo, fare clic su **Add** (Aggiungi) in Access Devices (Dispositivi di accesso) e immettere manualmente il SSID appropriato (ad esempio, Enterprise). Configurare il comportamento probe attivo per il client. In questo caso, il client verifica attivamente il proprio SSID configurato. Specificare **Ricercare attivamente la periferica di accesso** dopo aver immesso il SSID nella finestra Aggiungi periferica di accesso. **Nota:** le impostazioni della porta non consentono le modalità enterprise (802.1X) se le impostazioni di autenticazione EAP non sono configurate per il profilo.
2. Fare clic su **Create Network** (Crea rete) per aprire la finestra Network Profile (Profilo di rete), in cui è possibile associare l'SSID scelto (o configurato) a un meccanismo di autenticazione. Assegnare un nome descrittivo per il profilo. **Nota:** sotto questo profilo di autenticazione è



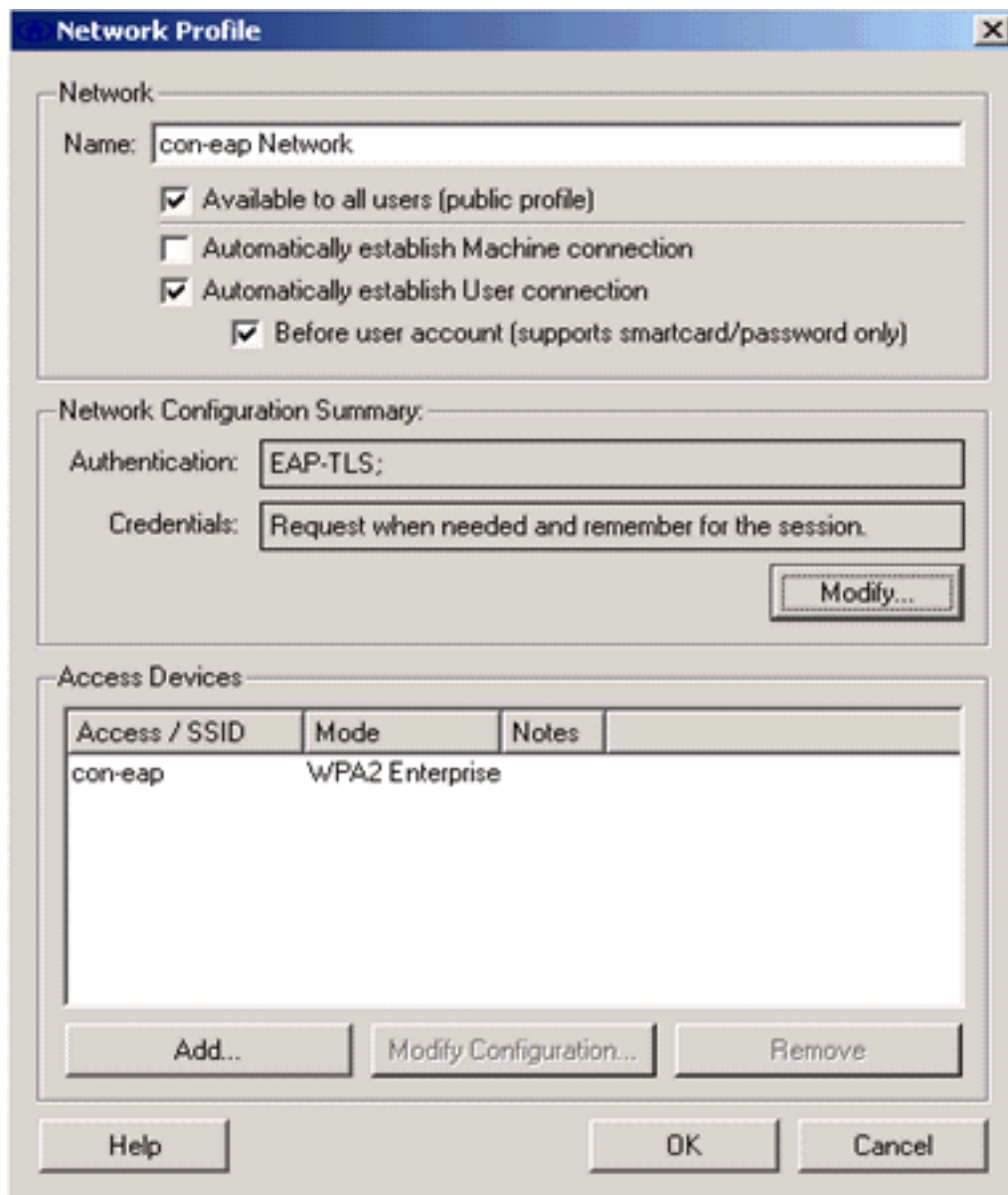
possibile associare più tipi di sicurezza WLAN e/o SSID.



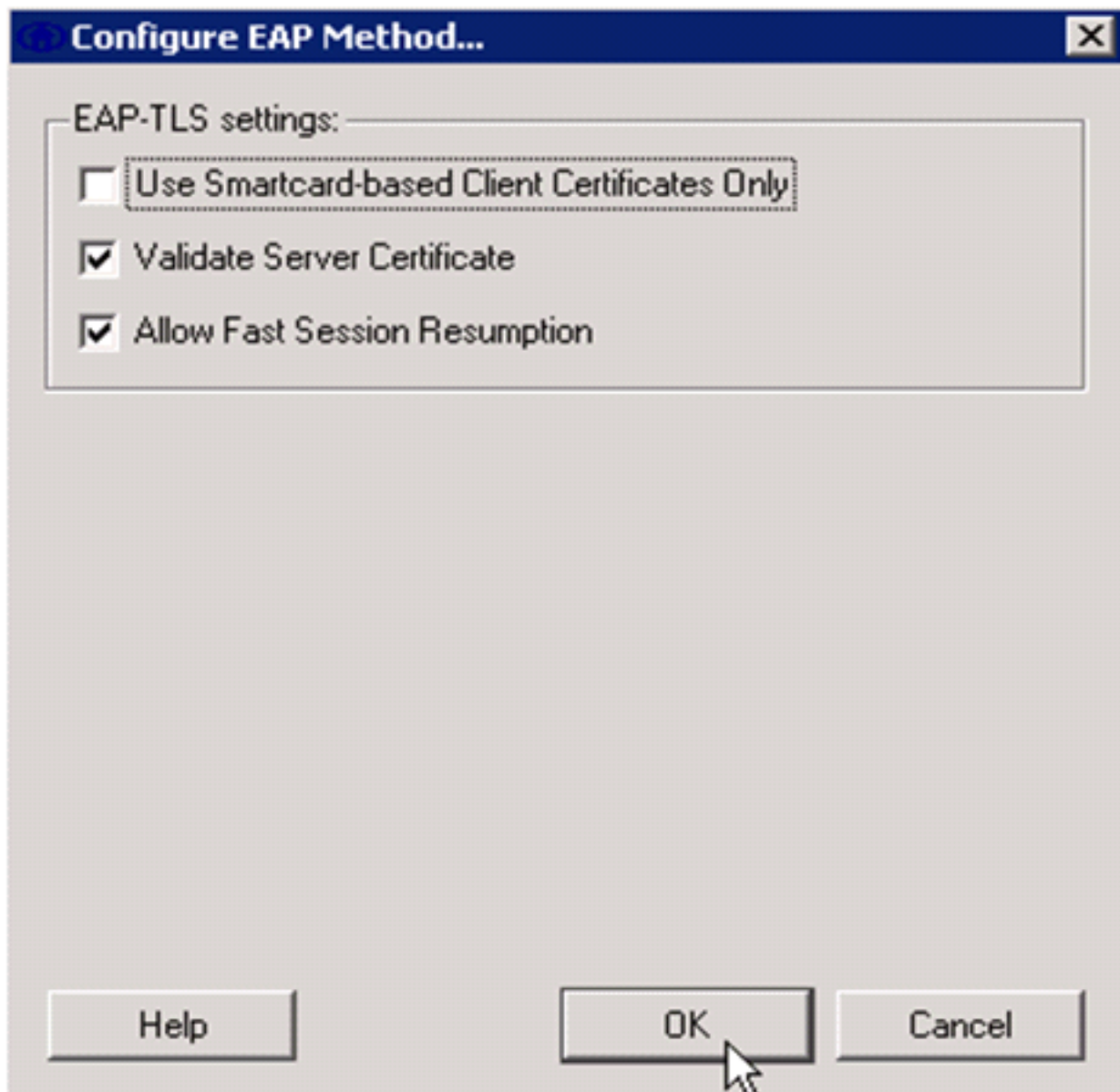
3. Attivare l'autenticazione e controllare il metodo EAP-TLS. Quindi, fare clic su **Configure** (Configura) per configurare le proprietà EAP-TLS.
4. In Riepilogo configurazione di rete fare clic su **Modifica** per configurare le impostazioni EAP / credenziali.
5. Specificare **Turn On Authentication** (Attiva autenticazione), scegliere **EAP-TLS** in Protocol (Protocollo), quindi selezionare **Username** come Identity (Nome utente).
6. Specificare **Usa credenziali Single Sign-On** per utilizzare le credenziali di accesso per l'autenticazione di rete. Fare clic su **Configure** (Configura) per impostare i parametri EAP-



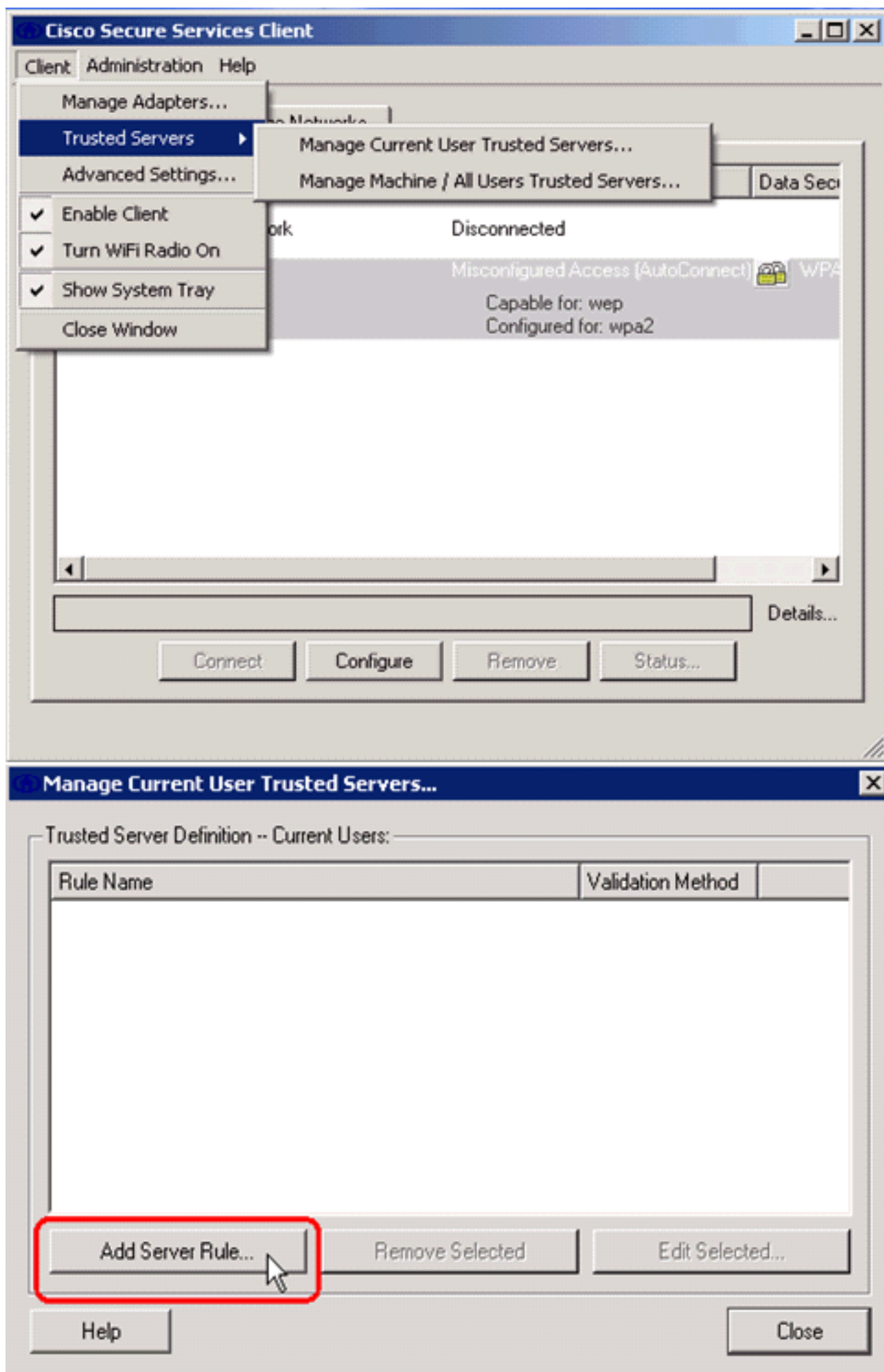
TLS.



7. Per ottenere una configurazione EAP-TLS protetta, è necessario controllare il certificato del server RADIUS. A tale scopo, selezionare **Convalida certificato server**.

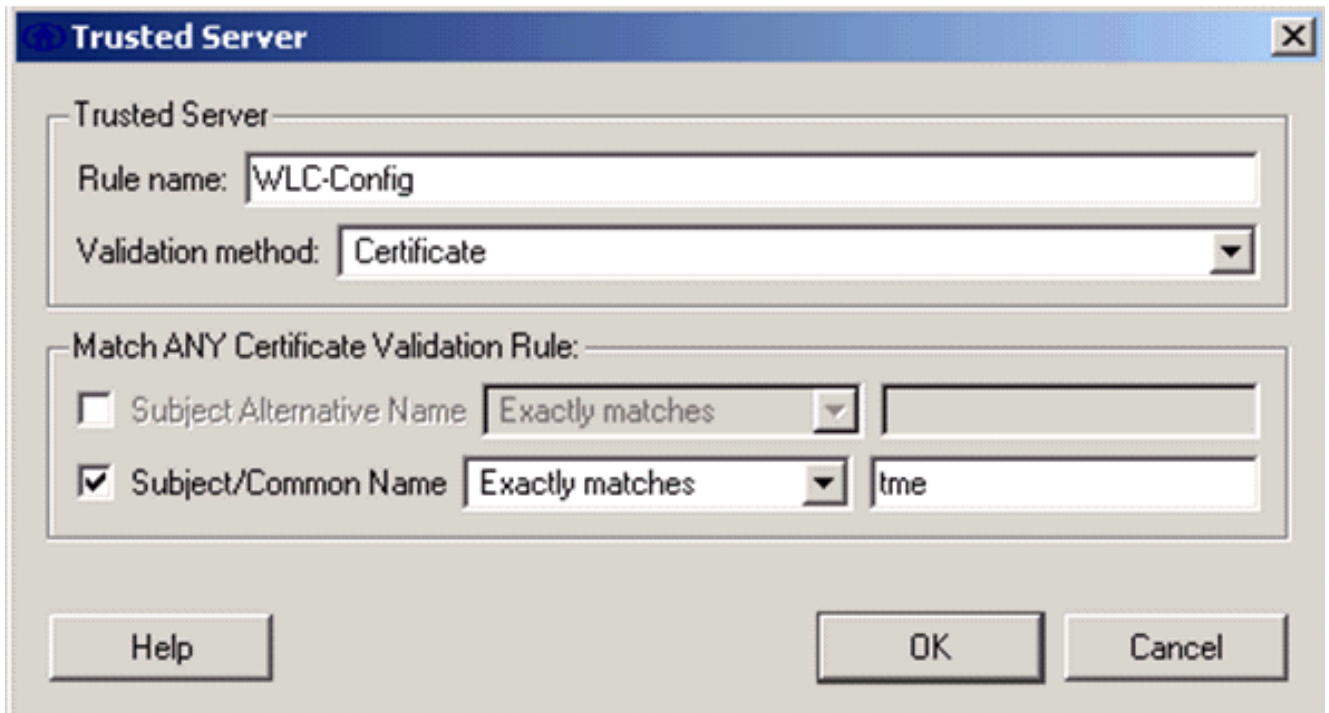


8. Per convalidare il certificato del server RADIUS, è necessario fornire a Cisco Secure Services Client le informazioni necessarie per accettare solo il certificato corretto. Scegliere **Client > Server trusted > Gestisci server trusted utente corrente**.



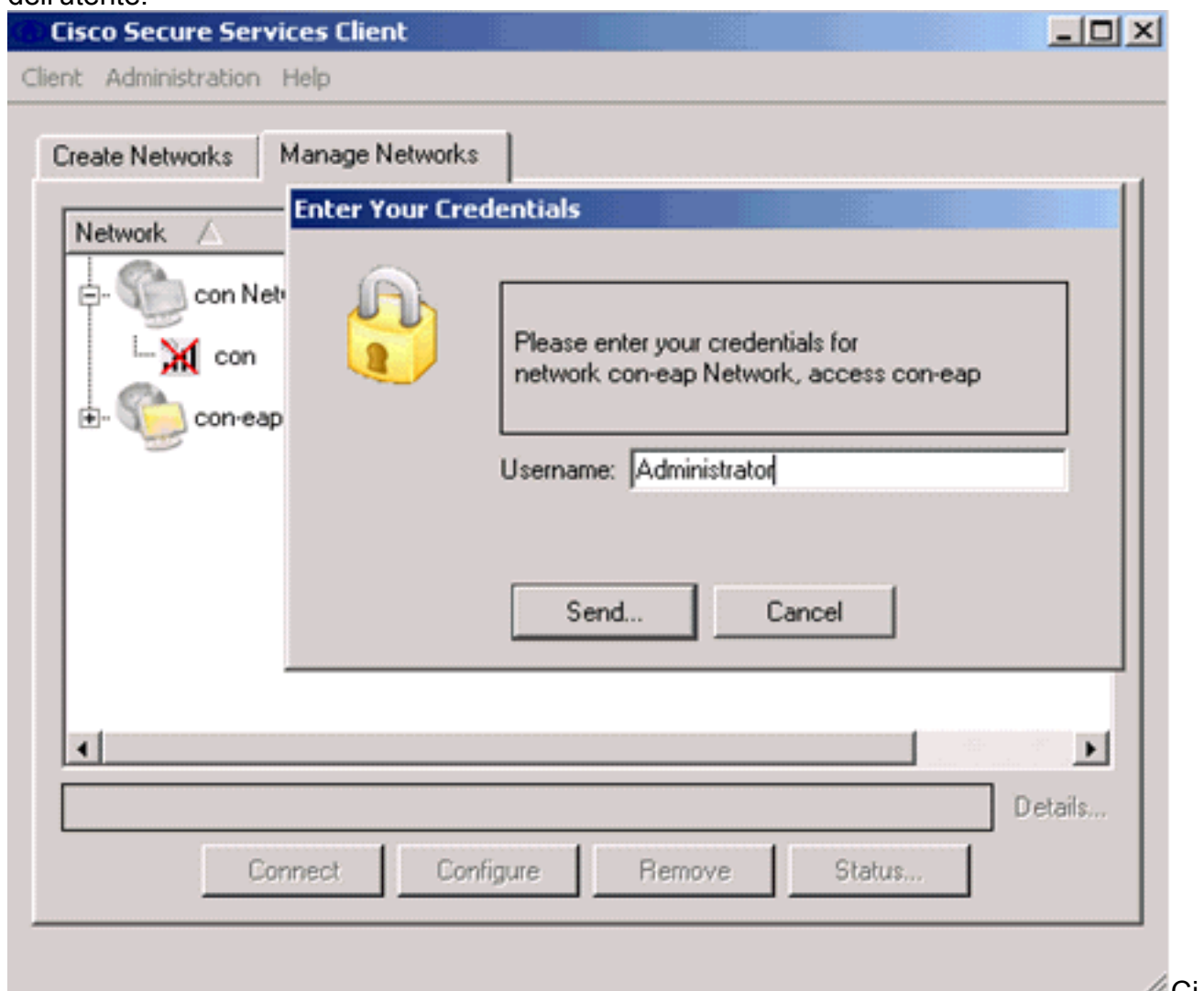
9. Assegnare un nome alla regola e controllare il nome del certificato del

server.



Configurazione EAP-TLS completata.

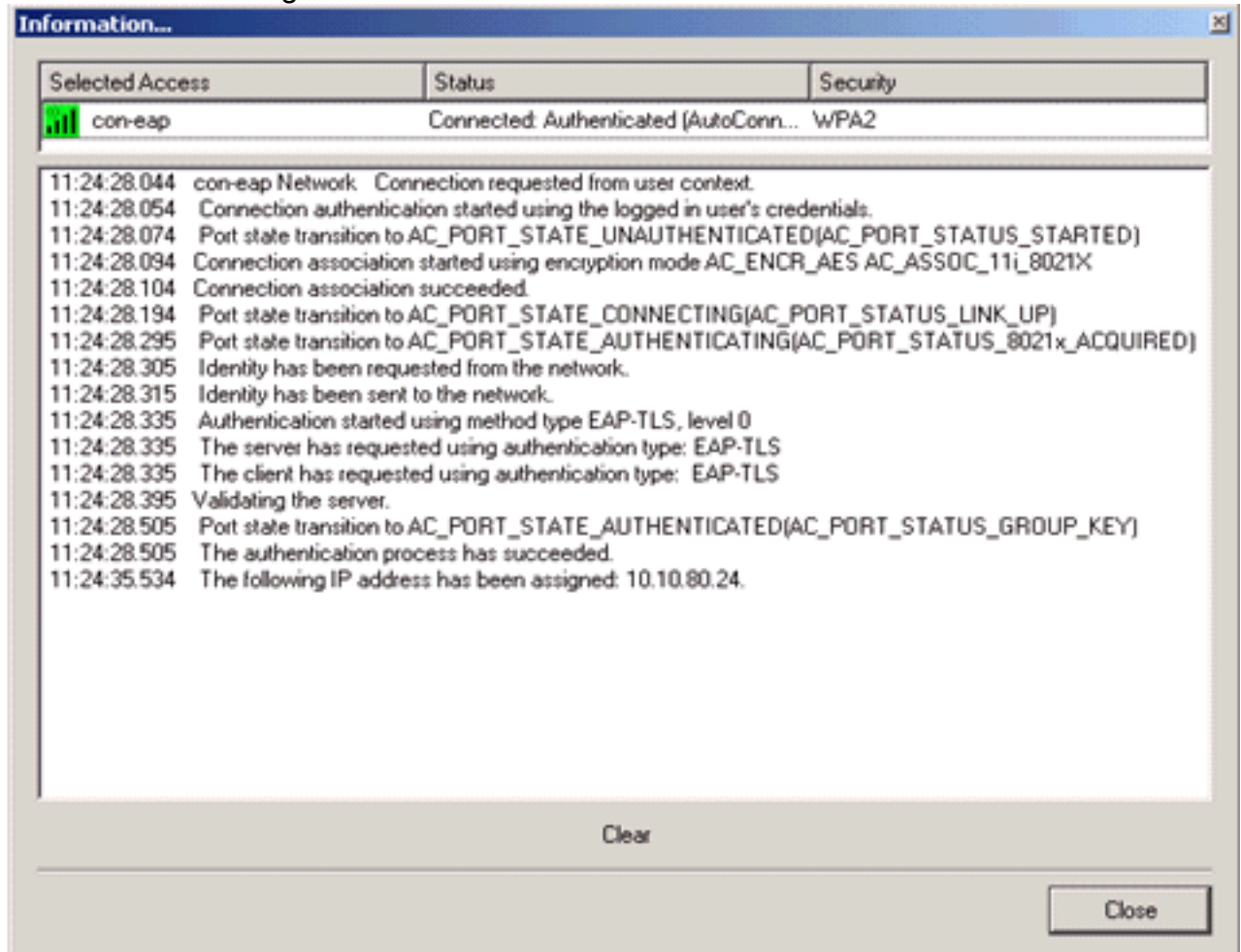
10. Connettersi al profilo della rete wireless. Cisco Secure Services Client richiede l'accesso dell'utente:



Cisco Secure Services Client riceve il certificato del server e lo controlla (con la regola







configurata e l'Autorità di certificazione installata). Viene quindi richiesto il certificato da utilizzare per l'utente.

11. Una volta eseguita l'autenticazione del client, scegliere **SSID** in Profilo nella scheda Gestisci reti e fare clic su **Stato** per eseguire una query sui dettagli della connessione. La finestra Dettagli connessione fornisce informazioni sulla periferica client, sullo stato e sulle statistiche della connessione e sul metodo di autenticazione. La scheda Dettagli WiFi fornisce dettagli sullo stato della connessione 802.11, che include RSSI, il canale 802.11 e autenticazione/crittografia.



Create Networks

Manage Networks

Network	Status	Data
 con Network	Disconnected	
 con	No Adapter Available (Suspended)	
 con-eap Network	Connected: Authenticated	
 con-eap	Connected: Authenticated (AutoConnect)	

 Details...

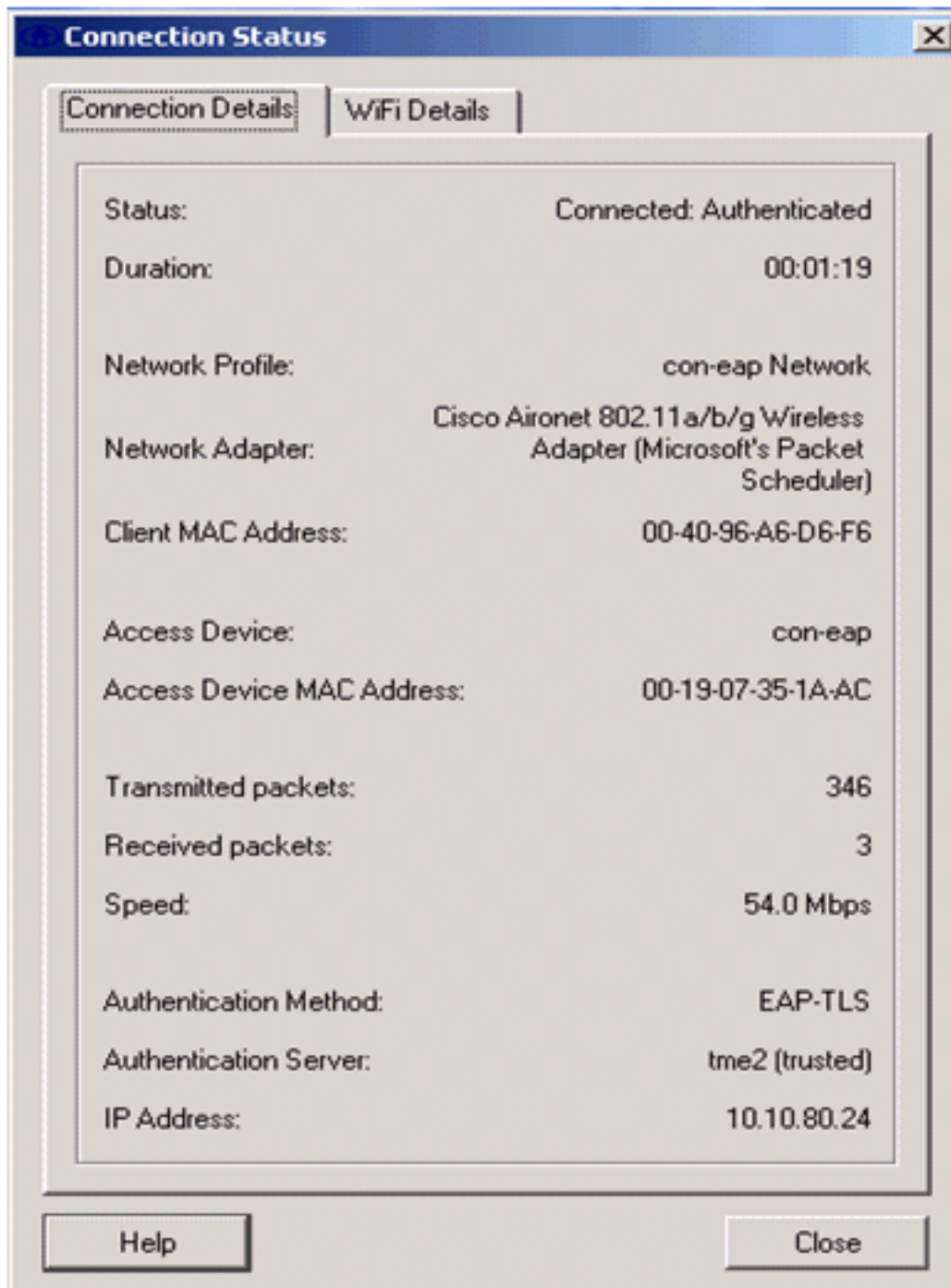
Disconnect

Configure

Remove

Status...





## [Comandi debug](#)

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

**Nota:** consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di **debug**.

I seguenti comandi di debug possono essere utilizzati sul WLC per monitorare l'avanzamento dello scambio di autenticazione:

- **debug aaa events enable**
- **abilitazione dettagli debug aaa**
- **debug dot1x events enable**

- debug dot1x stati enable
- debug aaa local-auth eap events enable
- debug aaa all enable

## Informazioni correlate

- [Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.1](#)
- [Supporto della tecnologia WLAN](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)