

ةكبش لل يلحمل EAP م داخ نيوكت لاثم ةدحوم لة يكلس الال

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[تكوين EAP المحلي على وحدة التحكم في شبكة LAN اللاسلكية من Cisco](#)

[تكوين EAP المحلي](#)

[هيئة شهادة Microsoft](#)

[التثبيت](#)

[تثبيت الشهادة في وحدة التحكم في شبكة LAN اللاسلكية من Cisco](#)

[تثبيت شهادة الجهاز على وحدة تحكم الشبكة المحلية اللاسلكية](#)

[تنزيل شهادة CA للمورد إلى وحدة التحكم في الشبكة المحلية اللاسلكية](#)

[قم بتكوين وحدة التحكم في الشبكة المحلية اللاسلكية لاستخدام EAP-TLS](#)

[تثبيت "شهادة المرجع المصدق" على "الجهاز العميل"](#)

[تنزيل شهادة مرجع مصدق جذري للعميل وتثبيتها](#)

[إنشاء شهادة عميل لجهاز عميل](#)

[EAP-TLS مع عميل Cisco Secure Services على جهاز العميل](#)

[أوامر التصحيح](#)

[معلومات ذات صلة](#)

المقدمة

يصف هذا المستند تكوين خادم بروتوكول المصادقة المتوسع المحلي (EAP) في وحدة تحكم شبكة LAN اللاسلكية (WLC) من Cisco لمصادقة المستخدمين اللاسلكيين.

EAP المحلي هو أسلوب مصادقة يسمح للمستخدمين والعملاء اللاسلكيين بالمصادقة محليا. وقد تم تصميمه للاستخدام في المكاتب البعيدة التي ترغب في الحفاظ على الاتصال بالعملاء اللاسلكيين عند تعطل النظام الطرفي الخلفي أو تعطل خادم المصادقة الخارجي. عندما تقوم بتمكين EAP المحلي، فإن وحدة التحكم تعمل كخادم المصادقة وقاعدة بيانات المستخدم المحلية، وبالتالي إزالة الاعتماد على خادم مصادقة خارجي. يسترجع EAP المحلي مسوغات المستخدم من قاعدة بيانات المستخدم المحلية أو قاعدة بيانات الطرف الخلفي لبروتوكول الوصول إلى الدليل الخفيف (LDAP) لمصادقة المستخدمين. يدعم EAP المحلي المصادقة خفيفة الوزن (EAP (LEAP والمصادقة المرنة EAP عبر الاتصال النفقي الآمن (EAP-FAST) ومصادقة تأمين طبقة النقل (EAP (EAP-TLS بين وحدة التحكم والعملاء اللاسلكيين.

لاحظ أن خادم EAP المحلي غير متوفر إذا كان هناك تكوين عالمي خارجي لخادم RADIUS في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). تتم إعادة توجيه جميع طلبات المصادقة إلى RADIUS الخارجي العام حتى يتوفر خادم EAP المحلي. إذا فقد عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الاتصال بخادم RADIUS الخارجي، يصبح خادم EAP المحلي نشطا. في حالة عدم تكوين خادم RADIUS العمومي، يصبح خادم EAP المحلي نشطا

فورا. لا يمكن استخدام خادم EAP المحلي لمصادقة العملاء، المتصلين بمجموعات WLC أخرى. بمعنى آخر، يتعذر على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إعادة توجيه طلب EAP الخاص به إلى عنصر تحكم في الشبكة المحلية اللاسلكية (WLC) آخر للمصادقة. يجب أن يكون لكل عنصر تحكم في الشبكة المحلية اللاسلكية (WLC) خادم EAP محلي خاص به وقاعدة بيانات فردية.

ملاحظة: أستخدم هذه الأوامر لمنع WLC من إرسال الطلبات إلى خادم RADIUS خارجي .

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

ويدعم خادم EAP المحلي هذه البروتوكولات في إصدار البرنامج 4.1.171.0 والإصدارات الأحدث:

- قفزة
- EAP-FAST (اسم المستخدم/كلمة المرور، والشهادات)
- EAP-TLS

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة كيفية تكوين نقاط الوصول في الوضع (Lightweight (LAPs) و WLCs للتشغيل الأساسي
- معرفة بروتوكول نقطة الوصول في الوضع (Lightweight (LWAPP) وطرائق الأمان اللاسلكية
- معرفة أساسية بمصادقة EAP المحلية.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Windows XP مع بطاقة مهأي CB21AG و Cisco Secure Services Client، الإصدار 4.05
- وحدة التحكم في شبكة LAN اللاسلكية Cisco 4400 4.1.171.0
- المرجع المصدق ل Microsoft على خادم Windows 2000

الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

تكوين EAP المحلي على وحدة التحكم في شبكة LAN اللاسلكية من Cisco

يفترض هذا وثيقة أن التشكيل أساسي من ال WLC أتمت بالفعل.

تكوين EAP المحلي

أتمت هذا steps in order to شكلت EAP محلي:

1. إضافة مستخدم صاف محلي: من واجهة المستخدم الرسومية. اختر تأمين < مستخدم الشبكة المحلية > جديد،

أدخل اسم المستخدم، كلمة المرور، مستخدم الضيف، معرف WLAN، والوصف، وانقر تطبيق.

من ال CLI أنت تستطيع استعملت ال `config netuser add <username> <password> <wlan id> <<description`

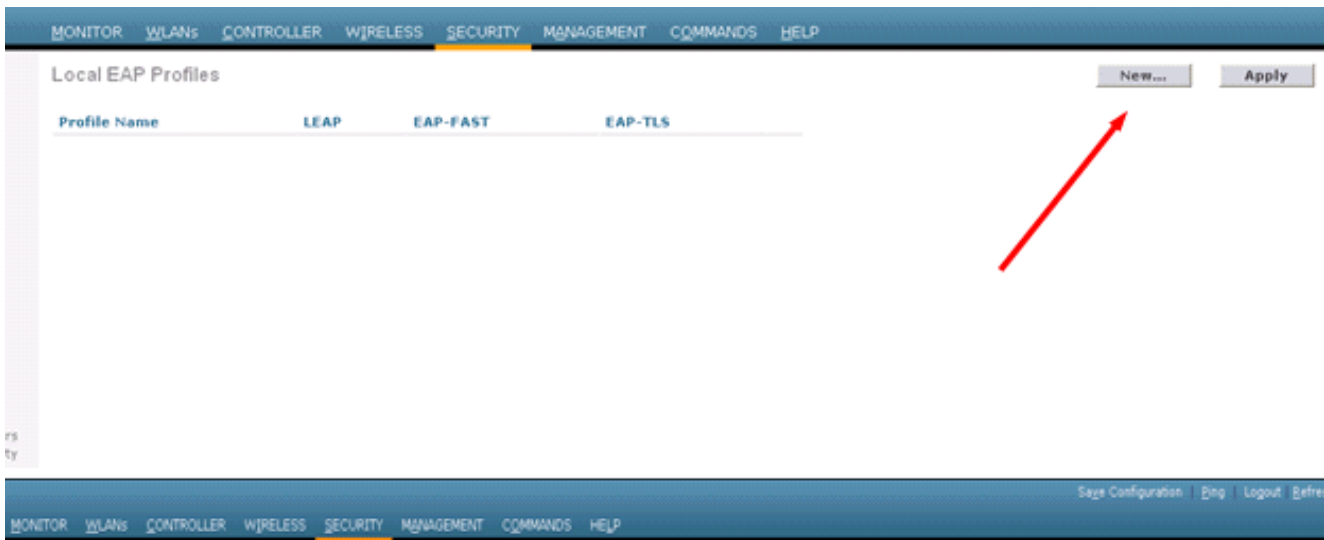
(Cisco Controller) `>config netuser add eapuser2 cisco123 1 Employee user local database)`

حدد أمر إسترجاع بيانات اعتماد المستخدم. من واجهة المستخدم الرسومية، اختر تأمين < EAP محلي > أولوية المصادقة. ثم حدد LDAP، وانقر زر ">" وانقر تطبيق. وهذا يضع بيانات اعتماد المستخدم في قاعدة البيانات المحلية أولاً.

من واجهة سطر الأوامر:

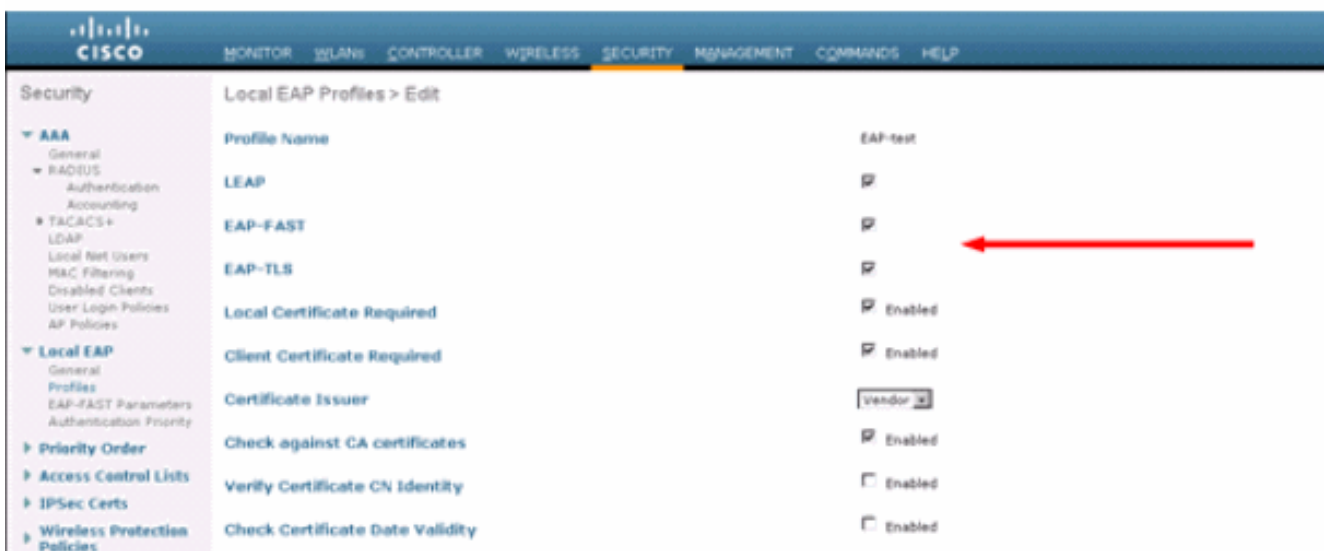
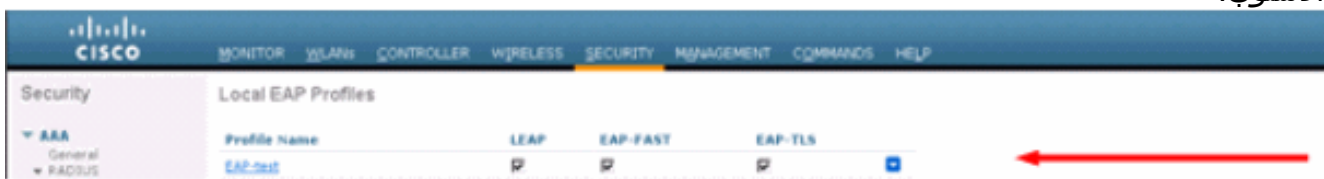
(Cisco Controller) `>config local-auth user-credentials local)`

3. إضافة توصيف EAP: اخترت in order to أتمت هذا من ال gui، أمن < محلي EAP > توصيفات وطققة جديد. عندما تظهر النافذة الجديدة، اكتب اسم ملف التخصيص وانقر تطبيق.



يمكنك أيضا القيام بذلك باستخدام أمر `config local-auth eap-profile add <profile-name>` في المثال الخاص بنا، يكون اسم التوصيف هو `EAP-test` (Cisco Controller) `>config local-auth eap-profile add EAP-test`.

4. إضافة أسلوب إلى ملف تعريف EAP. من واجهة المستخدم الرسومية اختر **تأمين < EAP محلي > توصيفات** وانقر على اسم التوصيف الذي تريد إضافة أساليب المصادقة له. يستخدم هذا المثال LEAP و EAP-FAST و EAP-TLS. طقطقة يطبق in order to ثبت الأسلوب.



يمكنك أيضا استخدام أمر `config local-auth eap-profile method add <profile> <method-name>` في مثال التكوين الخاص بنا نضيف ثلاث طرق إلى اختبار EAP لملف التعريف. وهذه الأساليب هي LEAP و EAP-FAST و EAP-TLS التي أسماء أساليبها هي LEAP و FAST و TLS على التوالي. يبدي هذا إنتاج ال CLI تشكيل أمر:

```
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)
```

قم بتكوين معلمات أسلوب EAP. لا يستخدم هذا إلا مع EAP-FAST. المعلمات التي سيتم تكوينها هي: مفتاح الخادم (مفتاح الخادم) — مفتاح الخادم لتشفير/فك تشفير مسوغات الوصول المحمي (PACs) (بالسداسي العشري). مدة البقاء ل (PAC-TTL) (PAC) - يحدد وقت عيش PAC. معرف السلطة (معرف السلطة) — يحدد معرف السلطة. الحكم المسمى (anon-provn) - يحدد ما إذا كان الحكم المغفل مسموحا به. مكنت هذا افتراضيا. للتكوين من خلال واجهة المستخدم الرسومية، أختار التأمين < EAP محلي > معلمات EAP-FAST وأدخل مفتاح الخادم، ووقت للعيش من أجل مسوغ الوصول المحمي (PAC)، ومعرف السلطة (hex)، وقيم معلومات معرف المرجع.

هذه هي أوامر تكوين CLI التي يجب استخدامها لتعيين هذه المعلمات ل 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. تمكين المصادقة المحلية لكل شبكة محلية لاسلكية: من واجهة المستخدم الرسومية (GUI) أختار شبكات WLAN من القائمة العليا وحدد شبكة WLAN التي تريد تكوين المصادقة المحلية لها. تظهر نافذة جديدة. انقر فوق التأمين < تبويات AAA. تحقق من مصادقة EAP المحلية وحدد اسم ملف تعريف EAP الأيمن من القائمة المنسدلة كما يوضح هذا المثال:

يمكنك أيضا إصدار أمر التكوين `config wlan local-auth enable <profile-name> <wlan-id>` كما هو موضح هنا:

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

7. ضبط معاملات أمان الطبقة 2 من واجهة المستخدم الرسومية، في نافذة تحرير الشبكة المحلية اللاسلكية (WLAN)، انتقل إلى التأمين < علامات تبويب الطبقة 2 واختر WPA+WPA2 من القائمة المنسدلة تأمين الطبقة 2. تحت قسم معاملات WPA+WPA2، اضبط تشفير WPA على TKIP و WPA2 تشفير AES. ثم انقر فوق تطبيق.



من ال CLI، استعملت هذا أمر:

```
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)
```

8. التحقق من التكوين:

```
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
```

يمكنك رؤية معاملات معينة من الشبكة المحلية اللاسلكية (WLAN) رقم 1 باستخدام الأمر `show wlan <wlan id`

```
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

```

```

Authentication:..... Open System 802.11
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

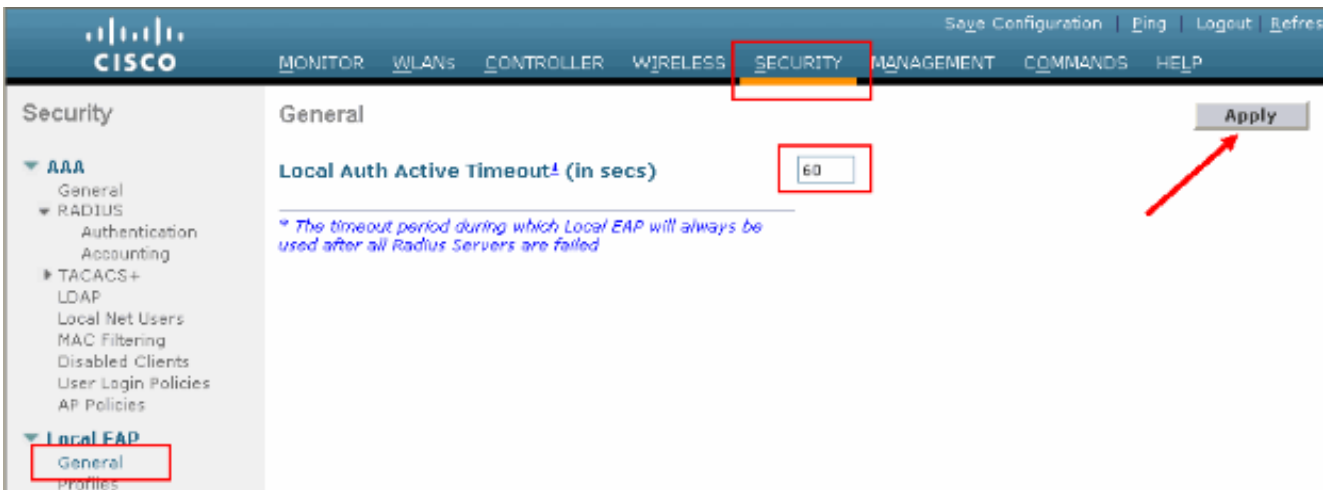
```

```

Mobility Anchor List
WLAN ID IP Address Status

```

هناك معلومات مصادقة محلية أخرى يمكن تكوينها، وخاصة مؤقت المهلة النشطة. يقوم هذا المؤقت بتكوين الفترة التي يتم خلالها استخدام EAP المحلي بعد فشل جميع خوادم RADIUS. من واجهة المستخدم الرسومية، اخترت أمن <EAP محلي> عام وعينت الوقت قيمة. ثم انقر فوق تطبيق.



من ال CLI، أصدرت هذا أمر:

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

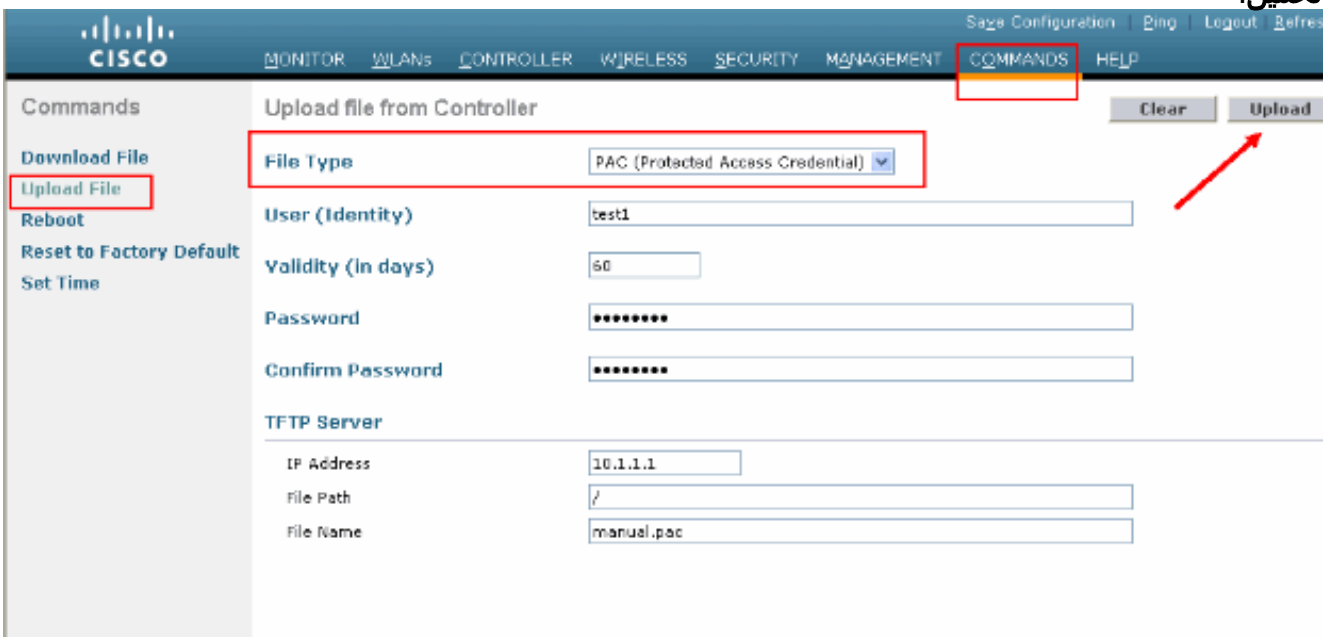
يمكنك التحقق من القيمة التي تم إعداد هذا المؤقت لها عند إصدار الأمر `show local-auth config`.
 (Cisco Controller) >`show local-auth config`)

```
:User credentials database search order
Primary ..... Local DB

:Timer
Active timeout ..... 60

:Configured EAP profiles
Name ..... EAP-test
Skip ...
```

9. إذا احتجت إلى إنشاء مسوغ الوصول المحمي اليدوي وتحميله، فيمكنك استخدام واجهة المستخدم الرسومية (GUI) أو واجهة سطر الأوامر (CLI). من واجهة المستخدم الرسومية، حدد الأوامر من القائمة العليا واختر تحميل الملف من القائمة في الجانب الأيمن. حدد PAC (مسوغات الوصول المحمي) من القائمة المنسدلة نوع الملف. أدخل كافة المعلمات وانقر فوق تحميل.



من واجهة سطر الأوامر (CLI)، أدخل الأوامر التالية:

```
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

```

هيئة شهادة Microsoft

من أجل إستخدام مصادقة EAP-FAST الإصدار 2 و EAP-TLS، يجب أن يكون لدى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وجميع أجهزة العميل شهادة صالحة ويجب أن تعرف أيضا الشهادة العامة الخاصة بالمرجع المصدق.

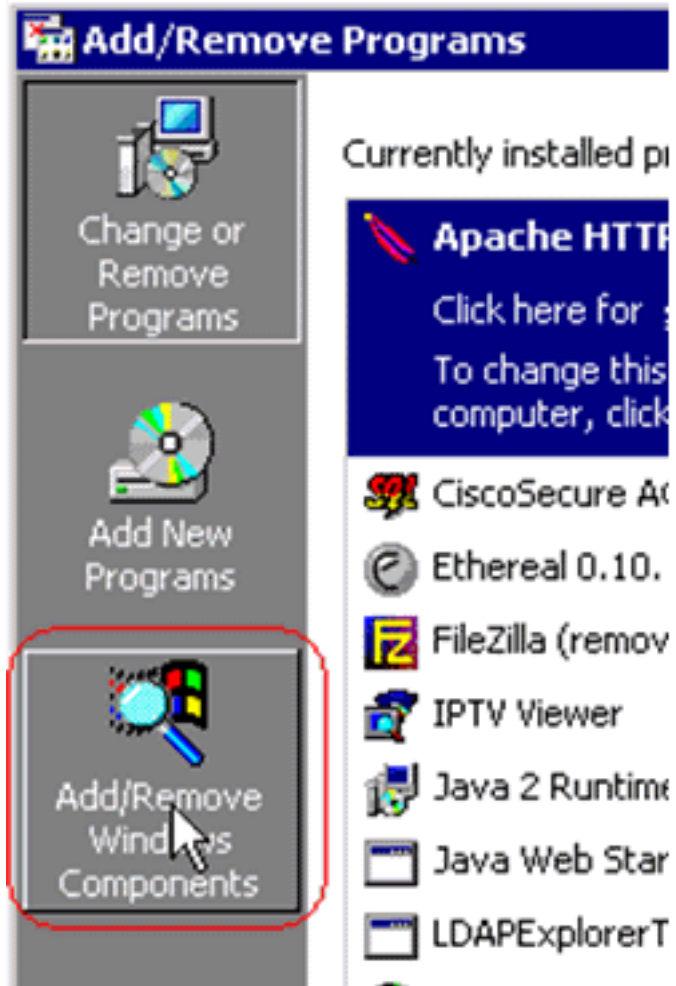
التثبيت

إذا لم يكن Windows 2000 Server مثبتا عليه خدمات المرجع المصدق، يجب تثبيته.
أكمل الخطوات التالية لتنشيط "مرجع مصدق Microsoft" على خادم Windows 2000:

1. من لوحة التحكم، أختار إضافة/إزالة برامج.



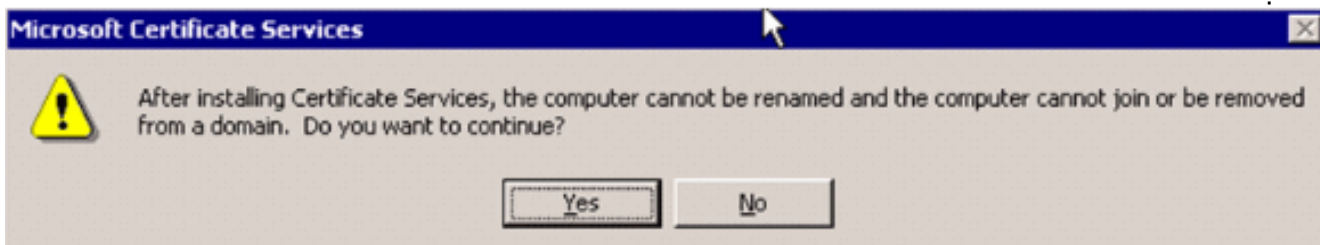
2. حدد إضافة/إزالة مكونات Windows على الجانب



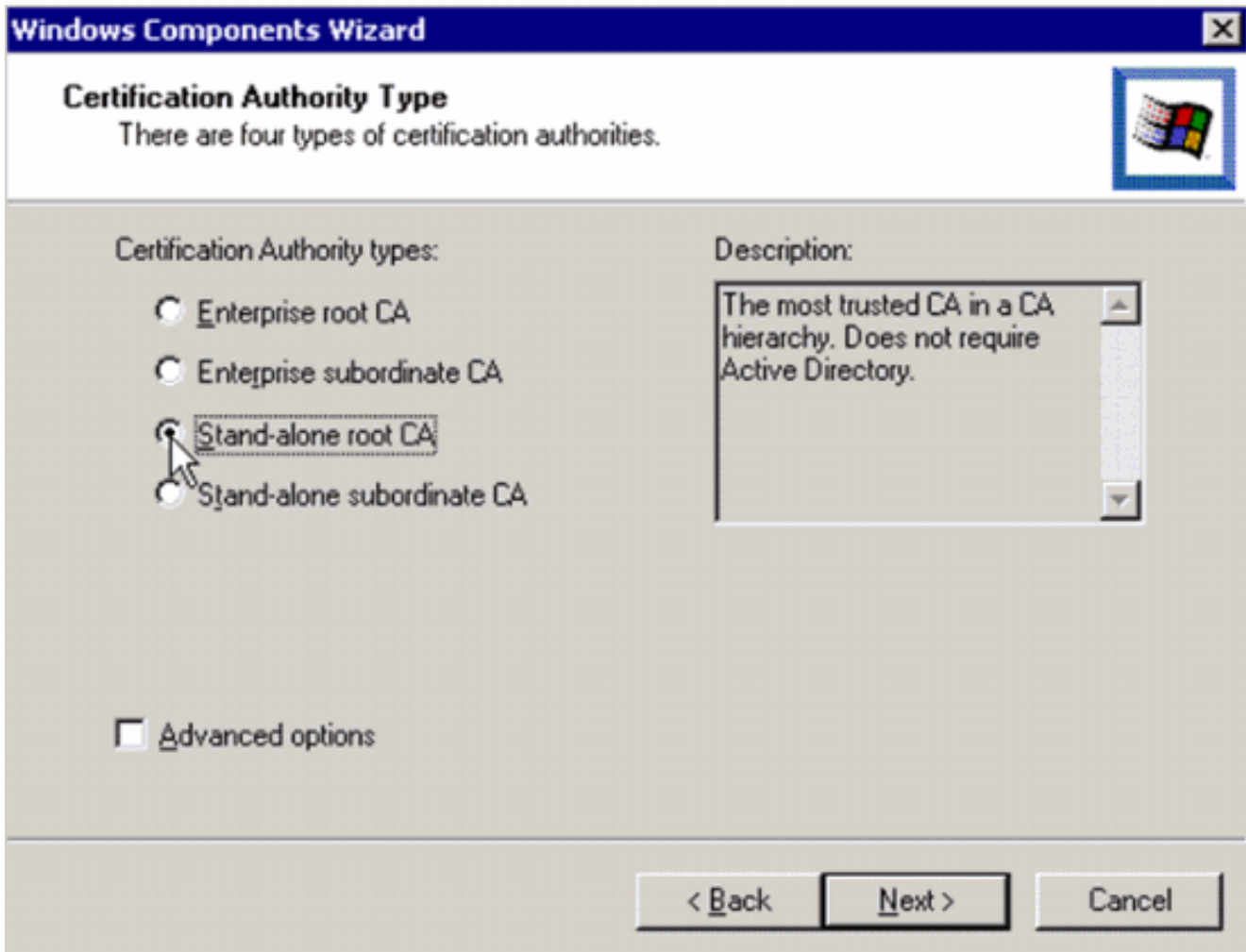
الأيسر.
3. تحقق من خدمات
الشهادات.



راجع هذا التحذير قبل المتابعة:



4. حدد نوع المرجع المصدق الذي تريد تثبيته. من أجل إنشاء مرجع مستقل بسيط، حدد المرجع المصدق CA الجذري المستقل.



5. إدخال المعلومات الضرورية حول المرجع المصدق. تنشئ هذه المعلومات شهادة موقعة ذاتيا للمرجع المصدق الخاص بك. تذكر اسم المرجع المصدق الذي تستخدمه. يخزن المرجع المصدق الشهادات في قاعدة بيانات. يستخدم هذا المثال الإعداد الافتراضي المقترح من قبل Microsoft:

Windows Components Wizard

Data Storage Location
Specify the storage location for the configuration data, database and log

Certificate database:
C:\WINNT\system32\CertLog Browse...

Certificate database log:
C:\WINNT\system32\CertLog Browse...

Store configuration information in a shared folder
Shared folder:
Browse...

Preserve existing certificate database

< Back Next > Cancel

6. تستخدم خدمات مصدقة Microsoft خادم ويب IIS من أجل إنشاء شهادات العميل والخادم وإدارتها. يجب إعادة تشغيل خدمة IIS لهذا الغرض:

Microsoft Certificate Services

Internet Information Services is running on this computer. You must stop this service before proceeding. Do you want to stop the service now?

OK Cancel

يقوم Microsoft Windows 2000 Server الآن بتثبيت الخدمة الجديدة. يجب أن يكون لديك القرص المضغوط الخاص بتثبيت Windows 2000 Server لتثبيت مكونات Windows الجديدة. تم تثبيت "المرجع المصدق" الآن.

تثبيت الشهادة في وحدة التحكم في شبكة LAN اللاسلكية من Cisco

لاستخدام EAP-FAST الإصدار 2 و EAP-TLS على خادم EAP المحلي لوحدة تحكم الشبكة المحلية اللاسلكية من Cisco، اتبع الخطوات الثلاث التالية:

1. [قم بتثبيت شهادة الجهاز على وحدة تحكم الشبكة المحلية اللاسلكية.](#)
 2. [قم بتنزيل شهادة CA للمورد إلى وحدة التحكم في الشبكة المحلية اللاسلكية.](#)
 3. [قم بتكوين وحدة التحكم في الشبكة المحلية اللاسلكية لاستخدام EAP-TLS.](#)
- لاحظ أنه في المثال الموضح في هذا المستند، يتم تثبيت "خادم التحكم في الوصول" (ACS) على نفس المضيف الخاص بـ Microsoft Active Directory و Microsoft Certificate Authority، ولكن يجب أن يكون التكوين هو نفسه إذا كان خادم ACS على خادم مختلف.

[تثبيت شهادة الجهاز على وحدة تحكم الشبكة المحلية اللاسلكية](#)

1. . أتمت هذا steps in order to خلقت الشهادة أن يستورد إلى ال WLC: انتقل إلى `http://<serverAddr>/certsrv`. اختر طلب شهادة وانقر التالي. اخترت طلب متقدم وطققة بعد ذلك. اختر إرسال طلب شهادة إلى المرجع المصدق هذا باستخدام نموذج وانقر فوق التالي. اختر خادم ويب لقالب الشهادة وأدخل المعلومات ذات الصلة. ثم وضع علامة قابلة للتصدير على المفاتيح. تتلقى الآن شهادة تحتاج إلى تثبيتها في جهازك.

2. أتمت هذا steps in order to إستردت الشهادة من pc: افتح مستعرض Internet Explorer واختر أدوات < خيارات الإنترنت < المحتوى. انقر على شهادات. حدد الشهادة المثبتة حديثًا من القائمة المنسدلة. طقطقة يصدر. طقطقت بعد ذلك مرتين واخترت نعم يصدر المفتاح الخاص. هذا التنسيق هو (.PFX) PKCS#12 (تنسيق). اختر تمكين الحماية القوية. اكتب كلمة مرور. احفظه في ملف < tme2.pfx >.

3. انسخ الشهادة بتنسيق PKCS#12 إلى أي حاسب حيث يكون OpenSSL مثبتًا لتحويلها إلى تنسيق 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. قم بتنزيل شهادة جهاز تنسيق PEM المحولة على عنصر التحكم في الشبكة المحلية اللاسلكية (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. بعد إعادة التشغيل، تحقق من الشهادة.

```
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
```

[تنزيل شهادة CA للمورد إلى وحدة التحكم في الشبكة المحلية اللاسلكية](#)

1. أتمت هذا steps in order to إستردت البائع ca شهادة: انتقل إلى `http://<serverAddr>/certsrv`. أخترت `يسترد` ال CA شهادة وطققة بعد ذلك. أختار شهادة المرجع المصدق. انقر فوق DER المررمز. انقر على تنزيل شهادة CA واحفظ الشهادة على هيئة `rootca.cer`.

2. قم بتحويل المرجع المصدق للمورد من تنسيق DER إلى تنسيق PEM باستخدام الأمر `openssl x509 -in rootca.cer -out rootca.pem -information der - PEM` خارج PEM أمر. ملف المخرجات هو `rootca.pem` بتنسيق PEM.

3. تنزيل شهادة المرجع المصدق للمورد:

```
Cisco Controller) >transfer download datatype eapcacert)

? 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
```

قم بتكوين وحدة التحكم في الشبكة المحلية اللاسلكية لاستخدام EAP-TLS

أكمل الخطوات التالية:

من واجهة المستخدم الرسومية، أختار تأمين < EAP محلي > توصيفات، أختار التوصيف وفحص لهذه الإعدادات:

- تم تمكين الشهادة المحلية المطلوبة.
- تم تمكين شهادة العميل المطلوبة.
- مصدر الشهادة هو المورد.
- تم تمكين الفحص مقابل شهادات المرجع المصدق.

The screenshot shows the Cisco Security Management Center (SMC) interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP. The left sidebar shows a tree view with categories like AAA, RADIUS, TACACS+, Local EAP, Priority Order, Access Control Lists, IPSec Certs, and Wireless Protection Policies. The main content area is titled 'Local EAP Profiles > Edit'. It displays a configuration table for a profile named 'EAP-test'. The table has three columns: 'Profile Name', 'LEAP', and 'EAP-FAST'. Below this, there are several settings with checkboxes and a dropdown menu:

Profile Name	LEAP	EAP-FAST
EAP-test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Local Certificate Required	<input checked="" type="checkbox"/>	Enabled
Client Certificate Required	<input checked="" type="checkbox"/>	Enabled
Certificate Issuer	Vendor	
Check against CA certificates	<input checked="" type="checkbox"/>	Enabled
Verify Certificate CN Identity	<input type="checkbox"/>	Enabled
Check Certificate Date Validity	<input type="checkbox"/>	Enabled

تثبيت "شهادة المرجع المصدق" على "الجهاز العميل"

تنزيل شهادة مرجع مصدق جذري للعميل وتثبيتها

يجب أن يحصل العميل على شهادة مرجع مصدق الجذر من خادم مرجع مصدق. هناك عدة طرق يمكنك استخدامها للحصول على شهادة عميل وتثبيتها على جهاز Windows XP. للحصول على شهادة صالحة، يجب تسجيل دخول مستخدم Windows XP باستخدام معرف المستخدم الخاص به ويجب أن يكون لديه اتصال شبكة.

تم استخدام مستعرض ويب على عميل Windows XP واتصال سلكي بالشبكة للحصول على شهادة عميل من خادم المرجع المصدق الجذر الخاص. يستخدم هذا الإجراء للحصول على شهادة العميل من خادم مرجع مصدق من Microsoft:

1. استخدم مستعرض ويب على العميل وقم بتوجيه المستعرض إلى خادم المرجع المصدق. للقيام بذلك، أدخل <http://IP-address-of-Root-CA/certsrv>.
2. سجل الدخول باستخدام `Domain_name\user_name`. يجب عليك تسجيل الدخول باستخدام اسم المستخدم الخاص بالشخص المراد استخدام عميل XP.
3. في نافذة الترحيب، اختر إسترجاع شهادة CA وانقر بعد ذلك.
4. حدد ترميز Base64 وتنزيل شهادة CA.
5. في الإطار "تم إصدار الشهادة"، انقر على تثبيت هذه الشهادة وانقر على التالي.
6. اختر تحديد مخزن الشهادات تلقائياً وانقر فوق التالي، لرسالة إستيراد ناجحة.
7. الاتصال بالمرجع المصدق لاسترداد شهادة المرجع المصدق:

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. انقر على تنزيل شهادة المرجع المصدق.

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:

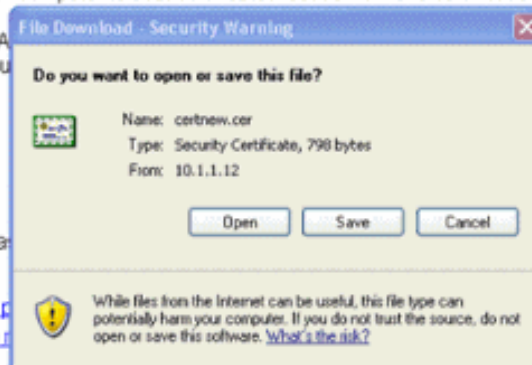
CA Certificate:

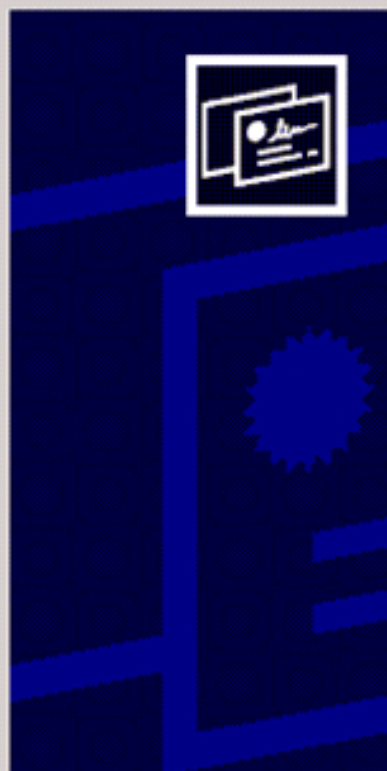
DER encoded or Base 64 encoded

[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.

< Back

Next >

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...

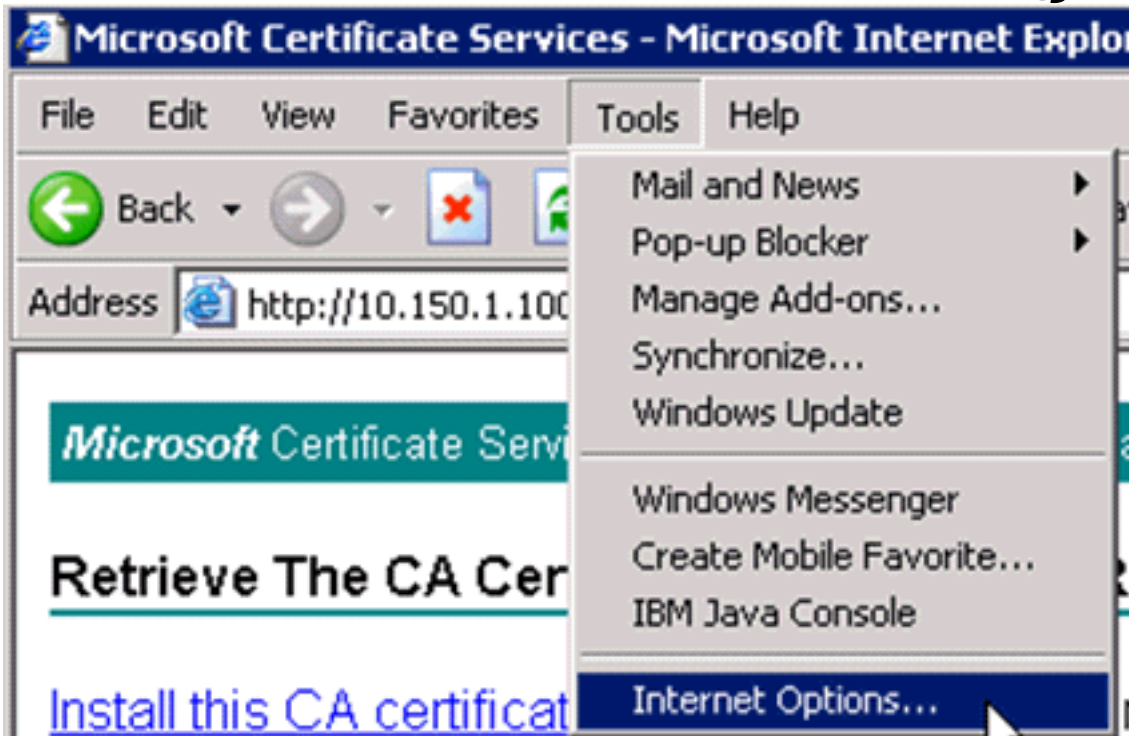
< Back

Next >

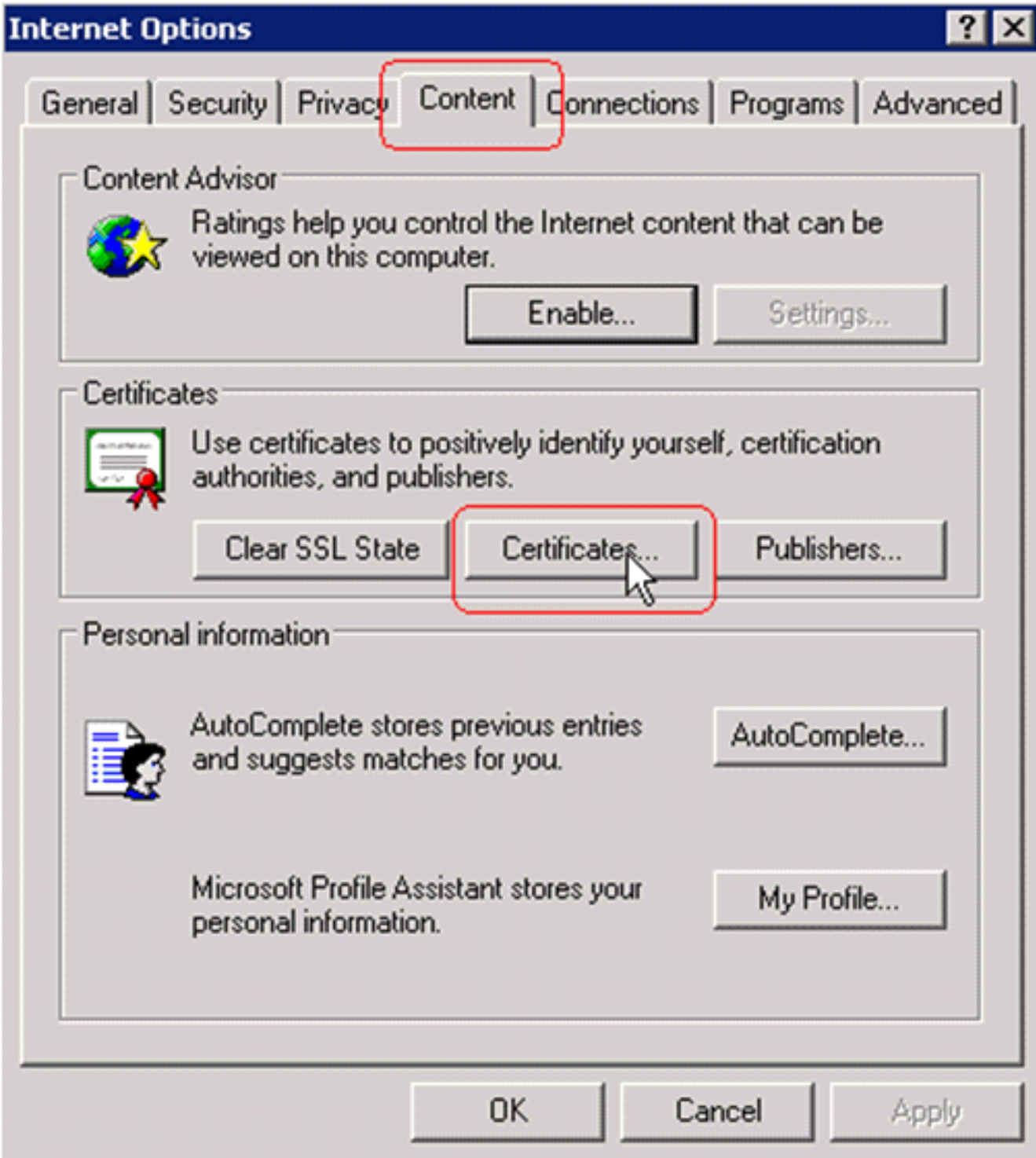
Cancel



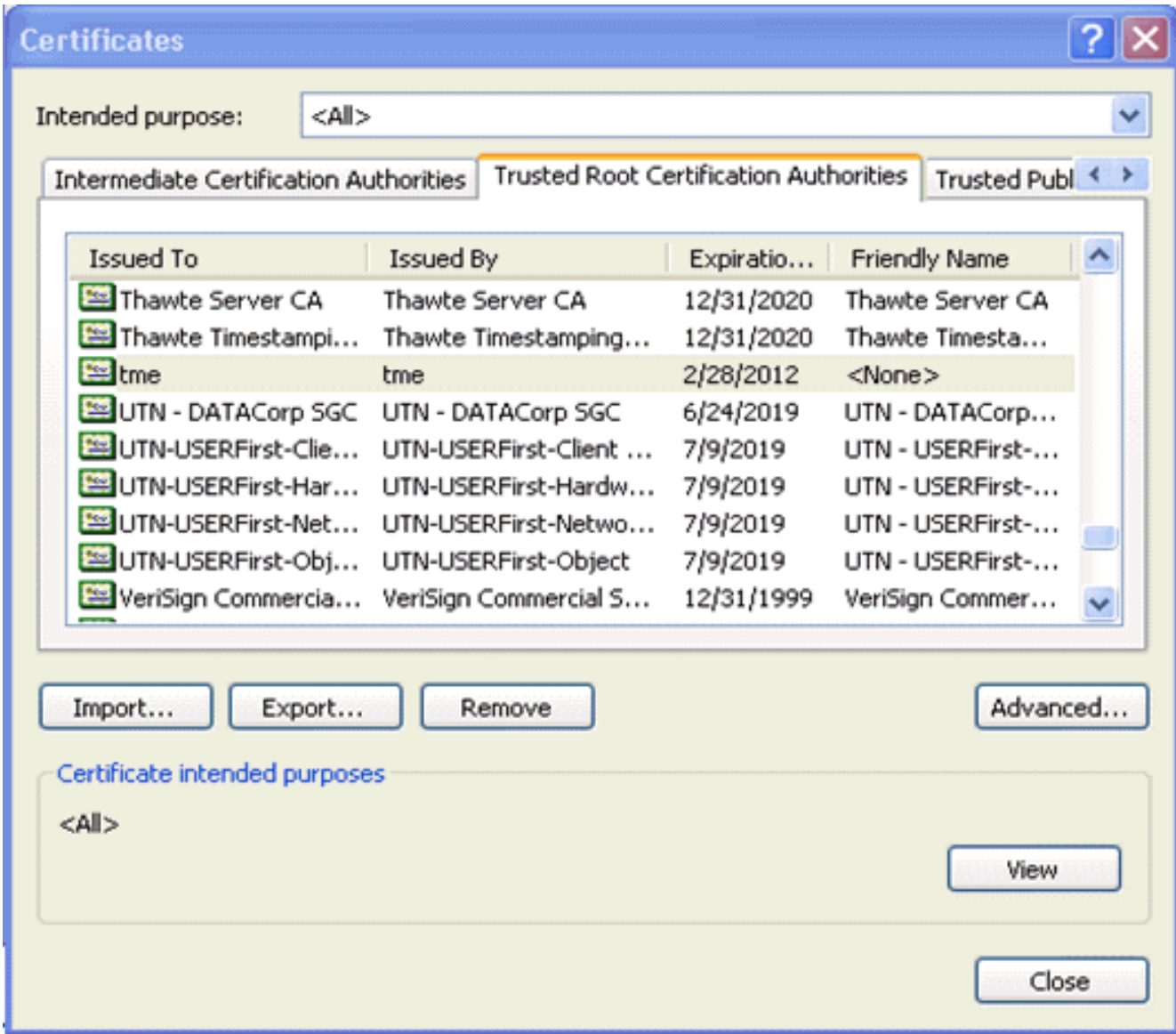
9. للتحقق من أن شهادة المرجع المصدق مثبتة بشكل صحيح، افتح Internet Explorer واختر أدوات > خيارات الإنترنت > المحتوى >



الشهادات.



في هيئة شهادة الجذر الموثوق فيها، يجب أن ترى هيئة شهادة النظام التي تم تثبيتها حديثاً:



إنشاء شهادة عميل لجهاز عميل

يجب على العميل الحصول على شهادة من خادم مرجع مصدق لمركز التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة عميل WLAN EAP-TLS. هناك العديد من الطرق التي يمكنك استخدامها للحصول على شهادة عميل وتثبيتها على جهاز Windows XP. للحصول على شهادة صالحة، يجب تسجيل دخول مستخدم Windows XP باستخدام معرف المستخدم الخاص به ويجب أن يكون لديه اتصال شبكة (إما اتصال سلكي أو اتصال WLAN مع تعطيل أمان 802.1x).

يتم استخدام مستعرض ويب على عميل Windows XP واتصال سلكي بالشبكة للحصول على شهادة عميل من خادم المرجع المصدق الجذر الخاص. يستخدم هذا الإجراء للحصول على شهادة العميل من خادم مرجع مصدق من Microsoft:

1. أستخدم مستعرض ويب على العميل وقم بتوجيه المستعرض إلى خادم المرجع المصدق. للقيام بذلك، أدخل <http://IP-address-of-Root-CA/certsrv>.
2. سجل الدخول باستخدام `Domain_name\user_name`. يجب تسجيل الدخول باستخدام اسم المستخدم الخاص بالشخص الذي يستخدم عميل XP. (يتم تضمين اسم المستخدم في شهادة العميل).
3. في نافذة الترحيب، أختار طلب شهادة وانقر بعد ذلك.
4. أختارت متقدم طلب وطققة بعد ذلك.
5. أختار إرسال طلب شهادة إلى المرجع المصدق هذا باستخدام نموذج وانقر فوق التالي.
6. في نموذج طلب الشهادة المتقدمة، أختار "قالب الشهادة" كمستخدم، وحدد حجم المفتاح على هيئة 1024 وانقر

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 >](#)

Choose Request Type

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

- User certificate request

- Advanced request

[Next >](#)

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 >](#)

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:

تم إنشاء

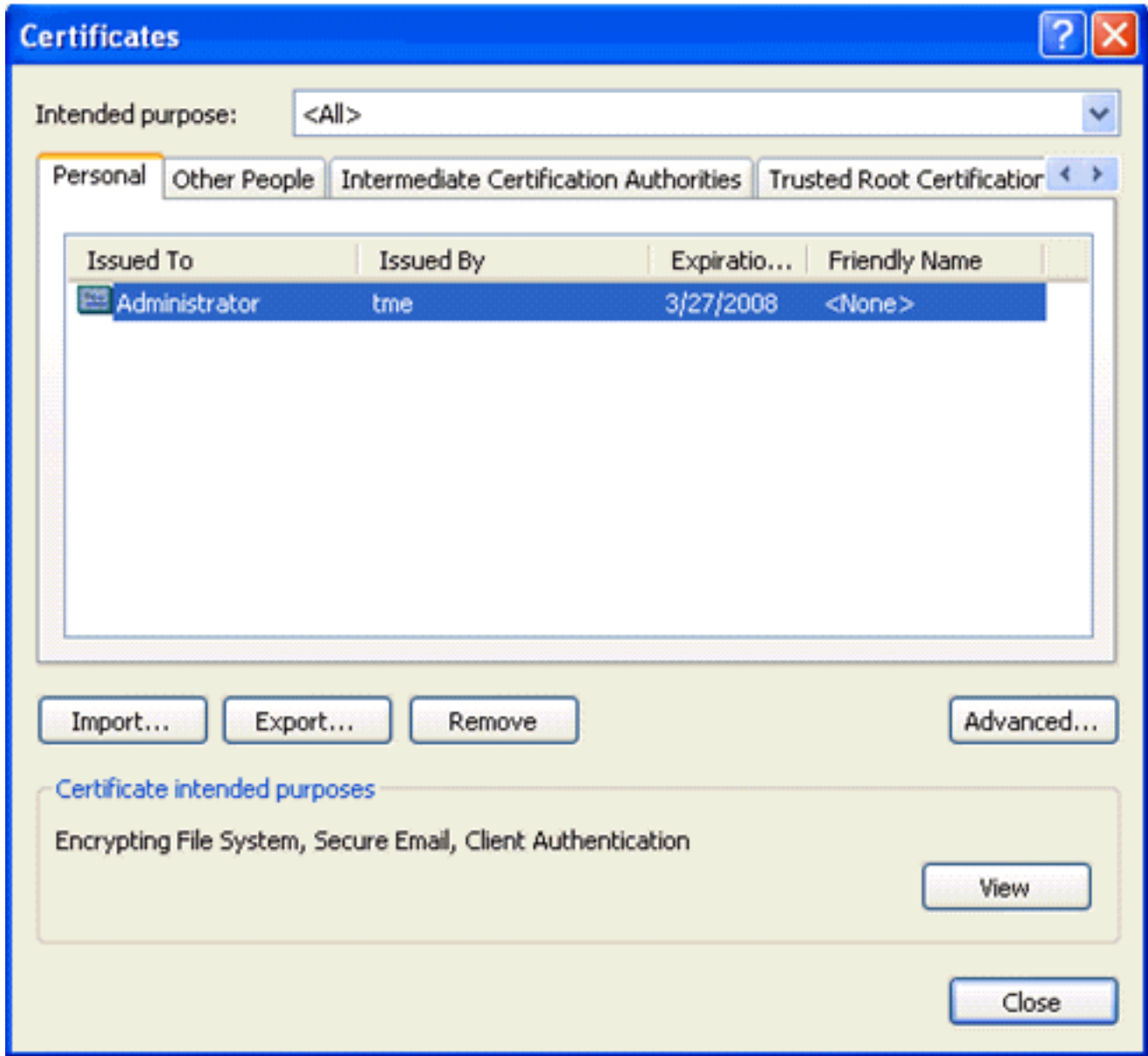
العميل.

شهادة العميل الآن.

9. للتحقق من تثبيت الشهادة، انتقل إلى Internet Explorer واختر أدوات < خيارات الإنترنت < المحتوى <

الشهادات. في علامة التبويب "شخصي"، يجب أن ترى

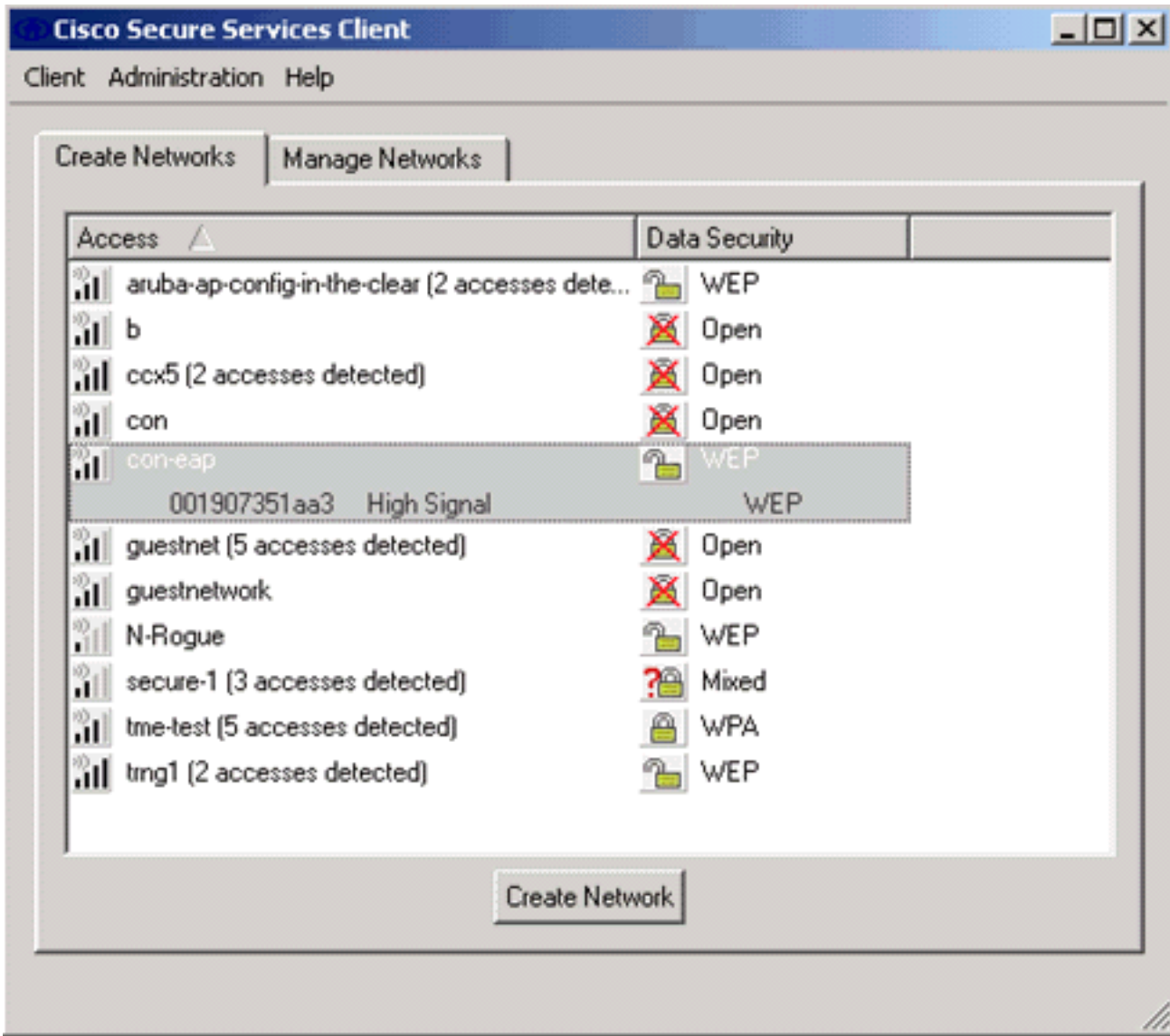
الشهادة.



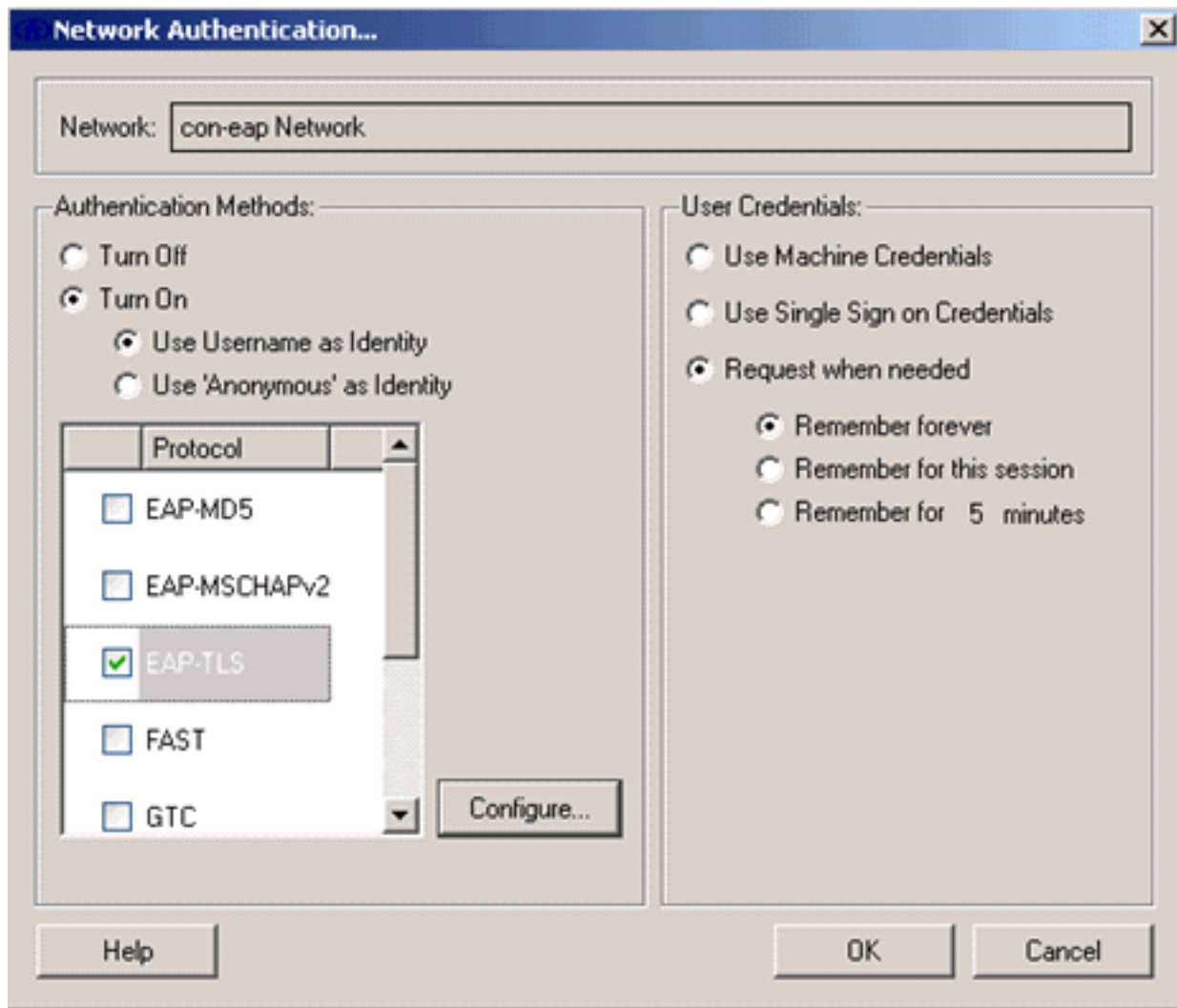
EAP-TLS مع عميل Cisco Secure Services على جهاز العميل

أكمل الخطوات التالية:

1. تقوم وحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، بشكل افتراضي، ببيث SSID، لذلك يتم عرضه في قائمة إنشاء شبكات من SSIDs الممسوحة ضوئياً. لإنشاء توصيف شبكة يمكنك النقر على SSID في القائمة (مشروع) والنقر على **إنشاء شبكة**. إذا تم تكوين البنية الأساسية للشبكة المحلية اللاسلكية (WLAN) مع تعطيل Broadcast SSID، فيجب عليك إضافة SSID يدوياً. للقيام بذلك، انقر فوق **إضافة** ضمن أجهزة الوصول وأدخل معرف SSID المناسب يدوياً (على سبيل المثال، Enterprise). تكوين سلوك الاستكشاف النشط للعميل. وهذا هو المكان الذي يبحث فيه العميل بنشاط عن SSID المكون الخاص به. حدد **البحث النشط عن جهاز الوصول** هذا بعد إدخال SSID في إطار إضافة جهاز الوصول. **ملاحظة:** لا تسمح إعدادات المنفذ بأوضاع المؤسسات (802.1X) إذا لم تكن إعدادات مصادقة EAP مكونة لأول مرة للتوصيف.
2. انقر على **إنشاء شبكة** لتشغيل إطار ملف تعريف الشبكة، والذي يسمح لك بإقران SSID الذي تم إختياره (أو تكوينه) بألية مصادقة. قم بتعيين اسم وصفي لملف التعريف. **ملاحظة:** يمكن إقران أنواع أمان متعددة لشبكة WLAN و/أو SSIDs ضمن ملف تعريف المصادقة هذا.



3. قم بتشغيل المصادقة وفحص أسلوب EAP-TLS. ثم انقر على تكوين لتكوين خصائص EAP-TLS.
4. تحت تشكيل خلاصة، انقر على تعديل in order to شكلت ال EAP / مسوغات عملية إعداد.
5. حدد تشغيل المصادقة، واختر EAP-TLS ضمن البروتوكول، واختر اسم المستخدم كهوية.
6. حدد استخدام بيانات اعتماد تسجيل الدخول الأحادي لاستخدام بيانات اعتماد تسجيل الدخول لمصادقة الشبكة.
انقر على تكوين لإعداد معلمات EAP-



.TLS

Network Profile [X]

Network:

Name:

Available to all users (public profile)

Automatically establish Machine connection

Automatically establish User connection

Before user account (supports smartcard/password only)

Network Configuration Summary:

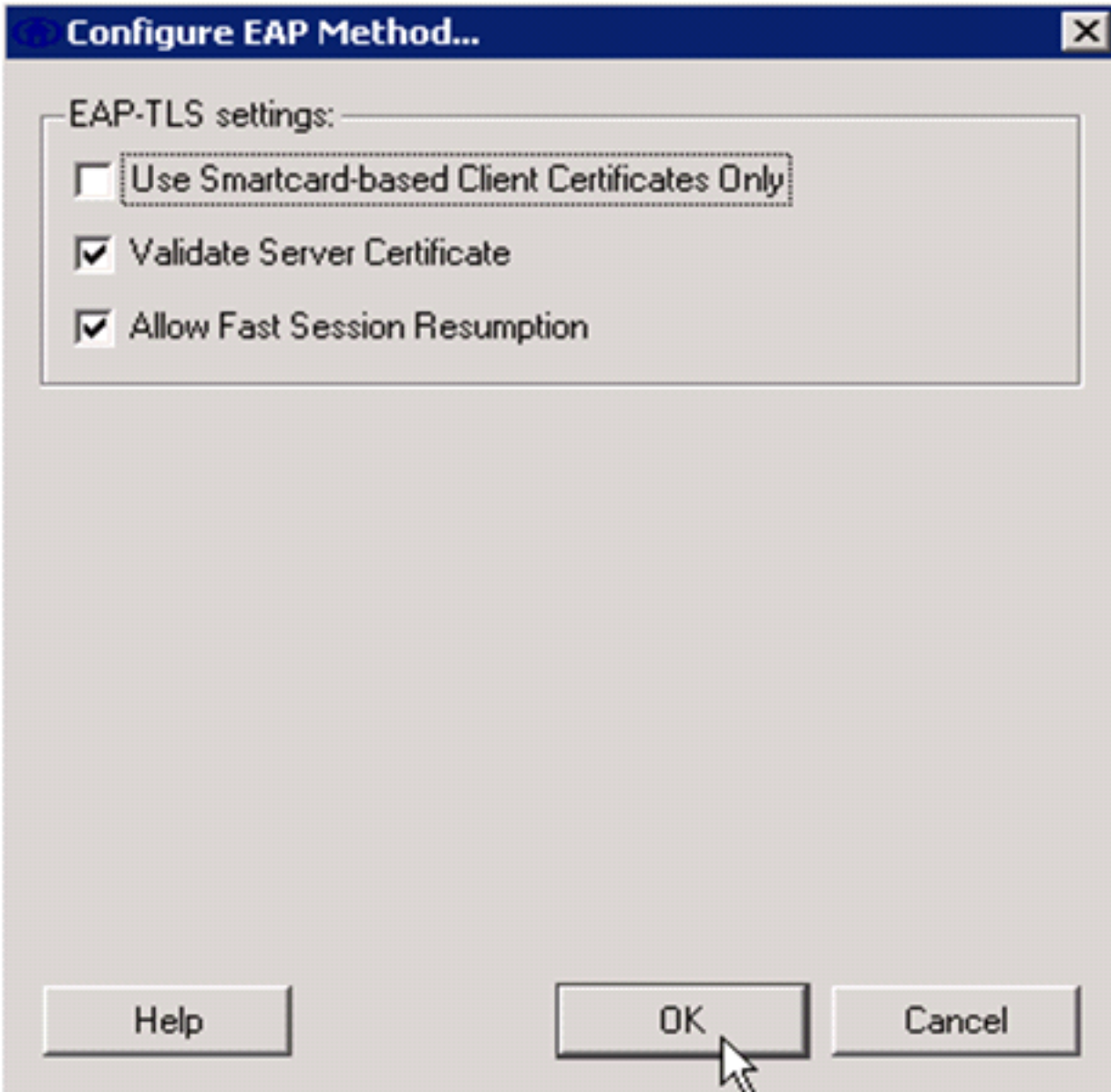
Authentication:

Credentials:

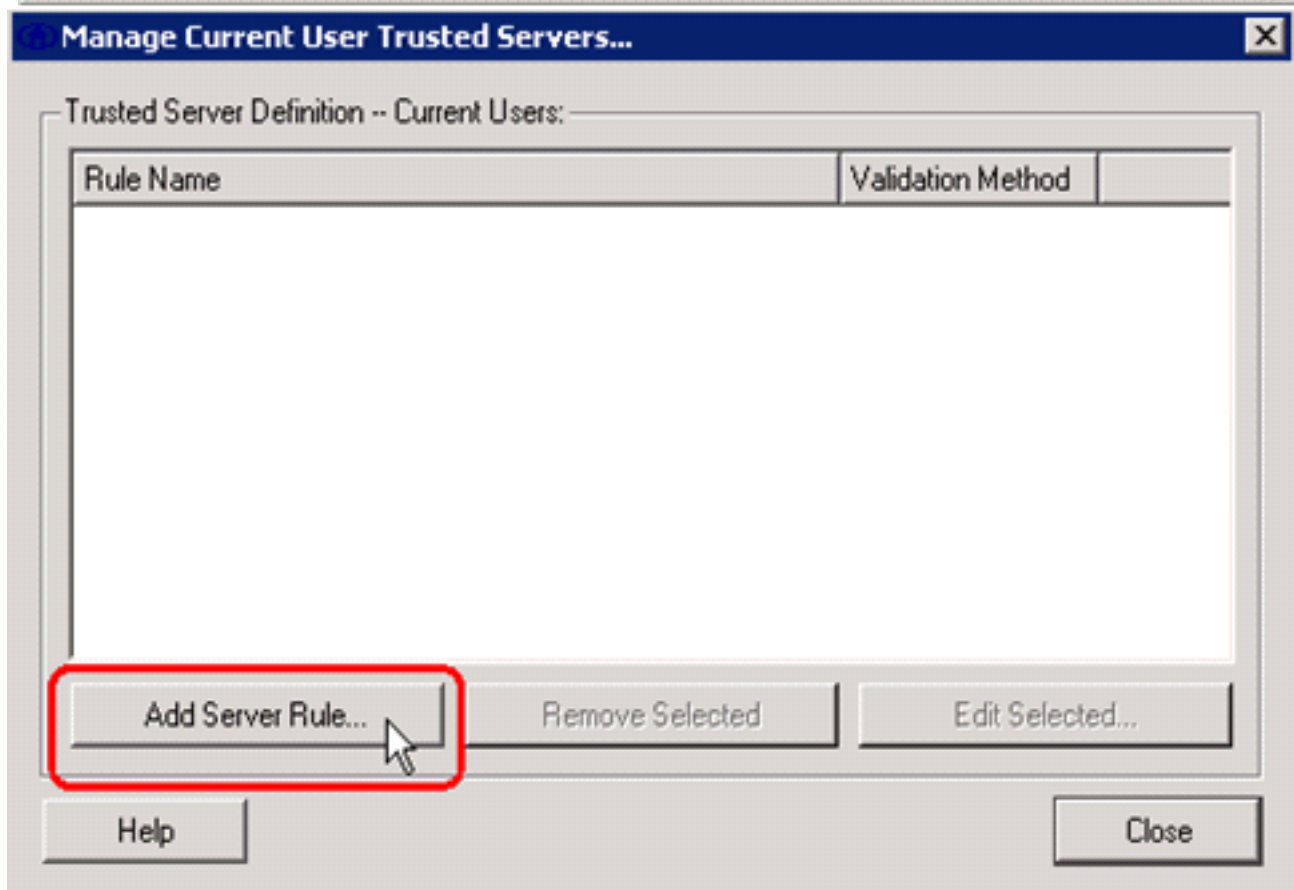
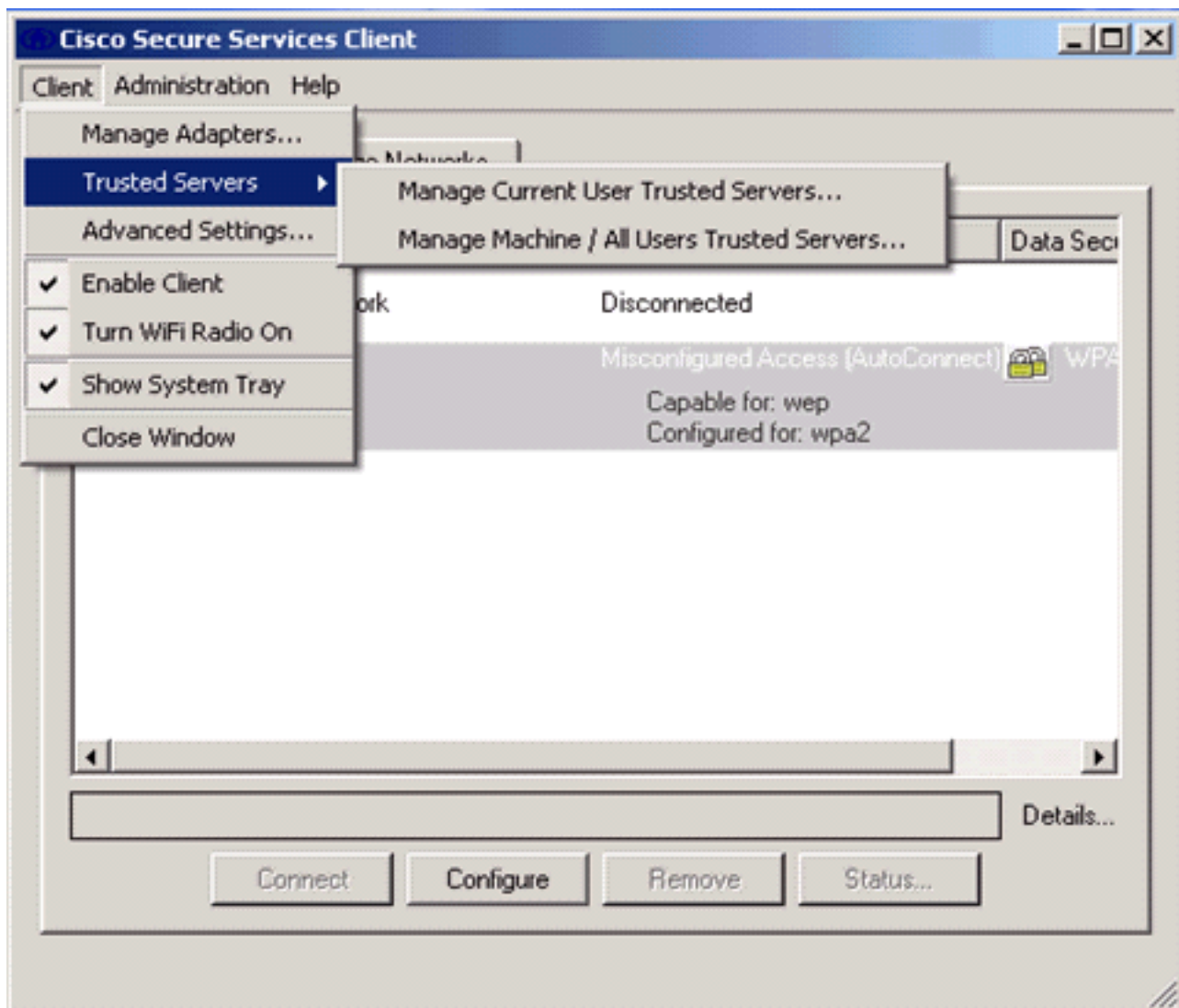
Access Devices

Access / SSID	Mode	Notes
con-eap	WPA2 Enterprise	

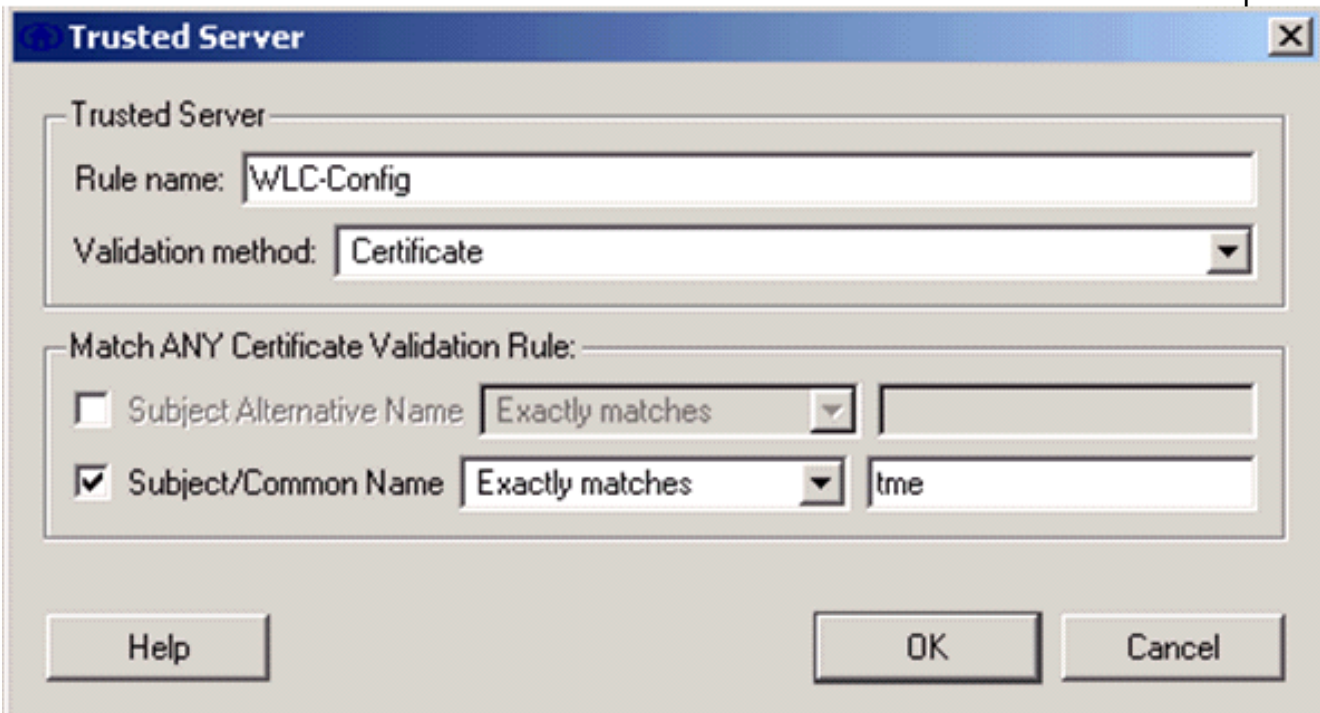
7. للحصول على تكوين EAP-TLS آمن يلزمك التحقق من شهادة خادم RADIUS. للقيام بذلك، تحقق من التحقق من شهادة



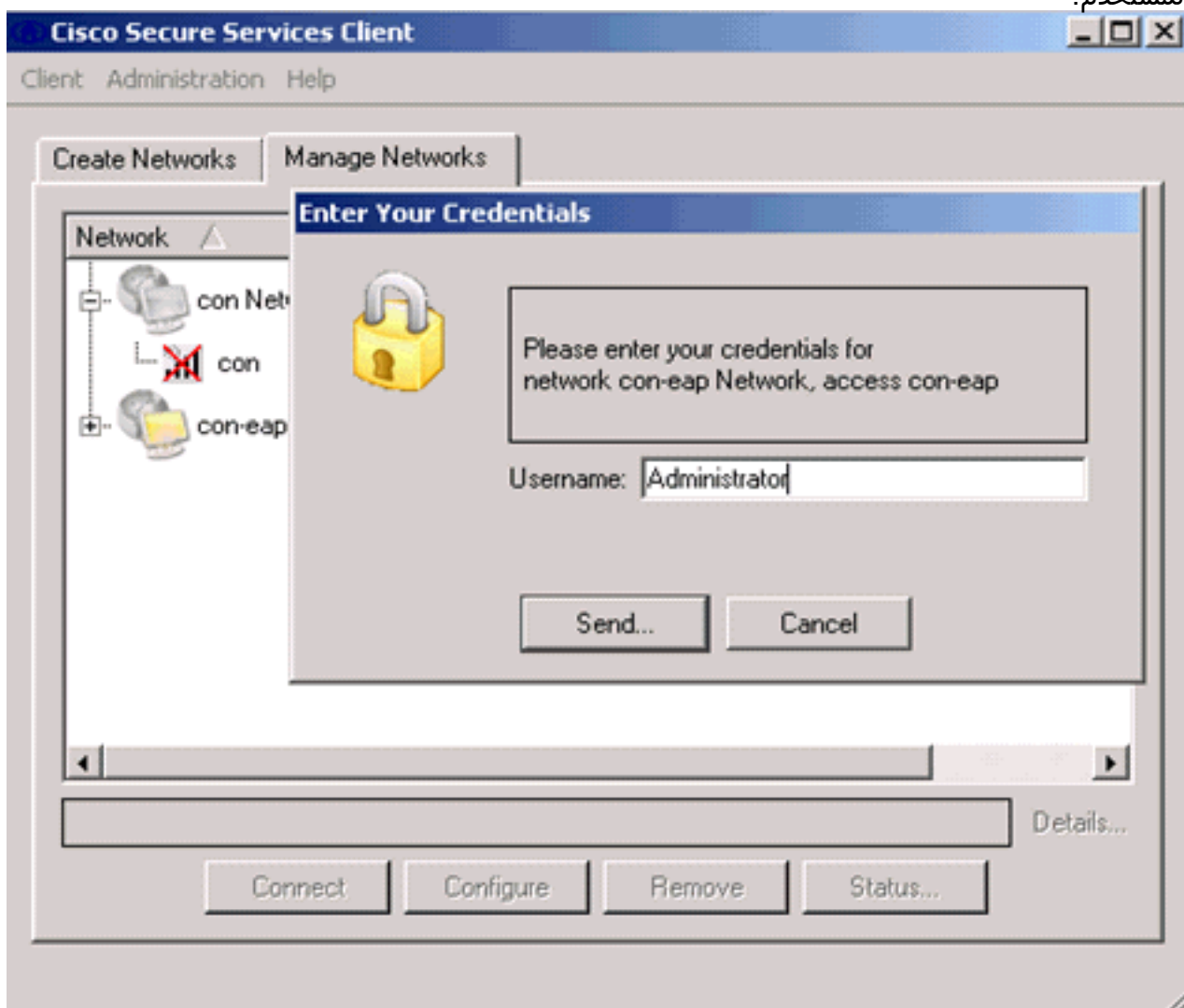
الخادم.
8. للتحقق من صحة شهادة خادم RADIUS، يلزمك منح معلومات Cisco Secure Services Client لقبول الشهادة الصحيحة فقط. اختر عميل < خوادم موثوق بها > إدارة الخوادم الموثوق بها للمستخدم الحالي.



9. قم بتسمية القاعدة وتحقق من اسم شهادة

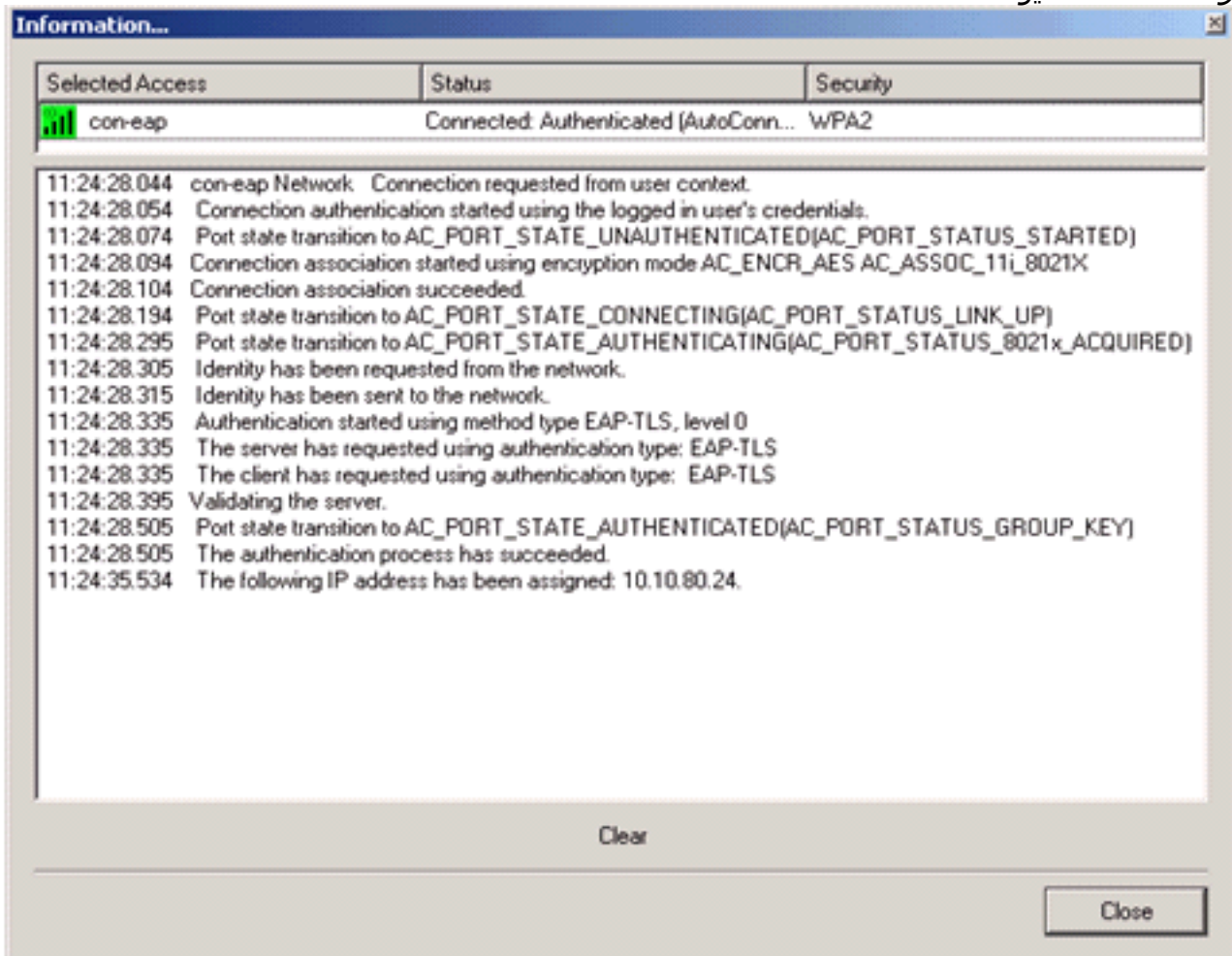


10. انتهى تكوين EAP-TLS .
 10. التوصليل بتوصيف الشبكة اللاسلكية. يطلب Cisco Secure Services Client تسجيل دخول المستخدم:









ستقبل Cisco Secure Services Client شهادة الخادم ويتحقق منها (مع تكوين القاعدة وثبيت المرجع

المصدق). ثم يطلب استخدام الشهادة للمستخدم.
11. بعد مصادقة العميل، أختَر SSID ضمن ملف التعريف في علامة التبويب إدارة الشبكات وانقر فوق الحالة للاستعلام عن تفاصيل الاتصال. يوفر إطار تفاصيل الاتصال معلومات عن جهاز العميل وحالة الاتصال وإحصاءاته وطريقة المصادقة. توفر علامة تبويب تفاصيل WiFi تفاصيل عن حالة توصيل 802.11 الذي يتضمن RSSI والقناة 802.11 والمصادقة/التشفير.

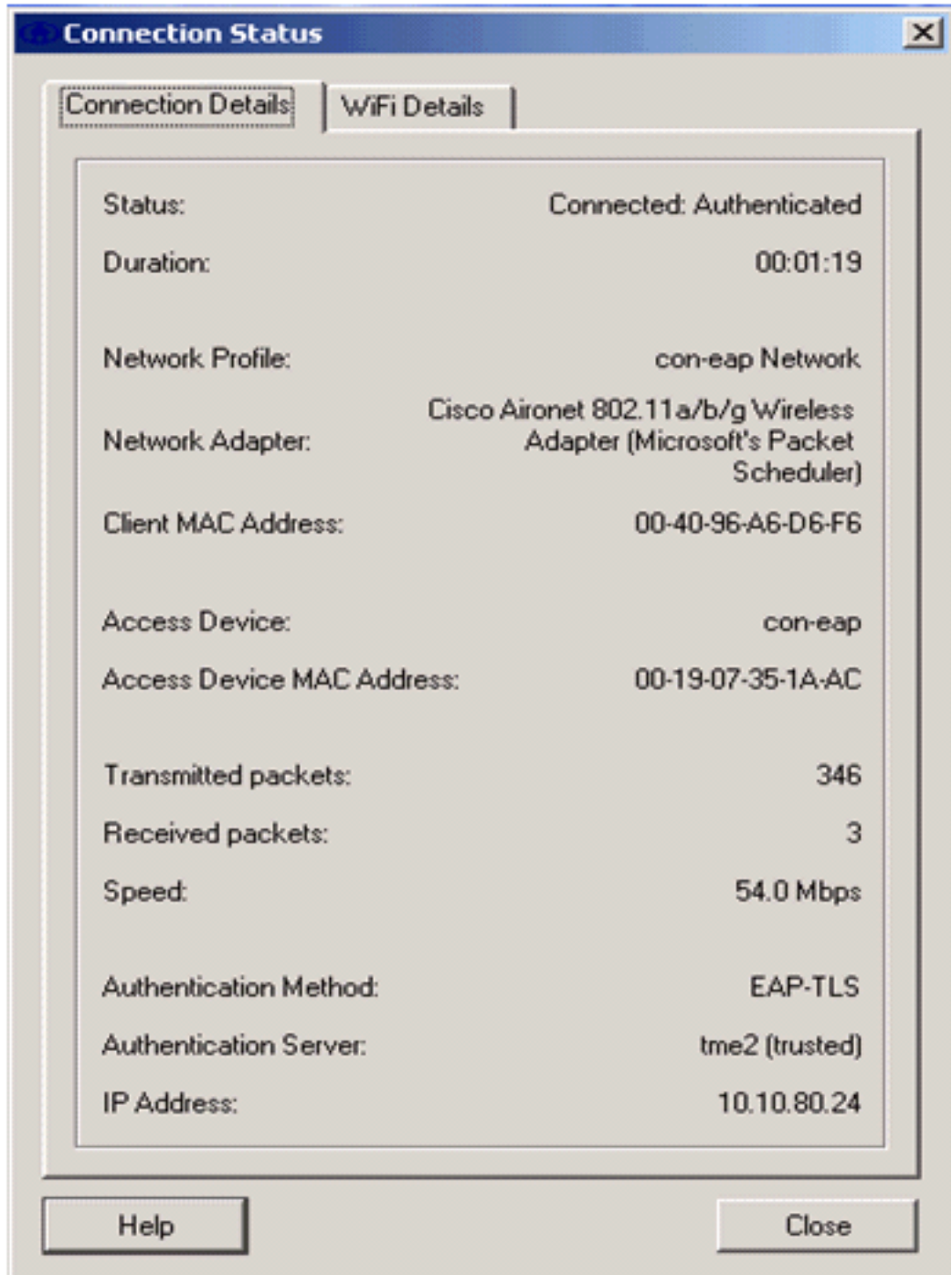


Create Networks Manage Networks

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...



أوامر التصحيح

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر `show`.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل استخدام أوامر `debug`.

يمكن استخدام أوامر تصحيح الأخطاء هذه في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمراقبة تقدم تبادل المصادقة:

- `debug aaa events enable`
- `enable debug aaa detail`
- `debug dot1x` حدث يمكن
- `enable debug dot1x` الحالات

- debug aaa local-auth eap events enable أو
- debug aaa all enable

معلومات ذات صلة

- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco، الإصدار 4.1
- دعم تقنية WLAN
- الدعم التقني والمستندات - Cisco Systems

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل
ىل ةل
(رفوتم طبارل) ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل