Unified Wireless Network Local EAP Server Configuration Example

Document ID: 91628

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Configure Local EAP on the Cisco Wireless LAN Controller
Local EAP Configuration
Microsoft Certification Authority
Installation
Install the Certificate in the Cisco Wireless LAN Controller
Install the Device Certificate on the Wireless LAN Controller
Download a Vendor CA Certificate to the Wireless LAN Controller
Configure the Wireless LAN Controller to use EAP-TLS
Install the Certificate Authority Certificate on the Client Device
Download and Install a Root CA Certificate for the Client
Generate a Client Certificate for a Client Device
EAP-TLS with Cisco Secure Services Client on the Client Device
Debug Commands
Related Information
Introduction

This document describes the configuration of a local Extensible Authentication Protocol (EAP) server in a Cisco Wireless LAN Controller (WLC) for the authentication of wireless users.

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the back–end system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, thereby removing dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the Lightweight Directory Access Protocol (LDAP) back–end database to authenticate users. Local EAP supports Lightweight EAP (LEAP), EAP–Flexible Authentication via Secure Tunneling (EAP–FAST), and EAP–Transport Layer Security (EAP–TLS) authentication between the controller and wireless clients.

Note that the local EAP server is not available if there is a global external RADIUS server configuration in the WLC. All authentication requests are forwarded to the global external RADIUS until the Local EAP Server is available. If the WLC looses connectivity to the external RADIUS server, then the local EAP server becomes active. If there is no global RADIUS server configuration, the local EAP server becomes immediately active. The local EAP server cannot be used to authenticate clients, which are connected to other WLCs. In other words, one WLC cannot forward its EAP request to another WLC for authentication. Every WLC should have its own local EAP server and individual database.

Note: Use these commands in order to stop WLC from sending requests to an external radius server .

The local EAP server supports these protocols in 4.1.171.0 software release and later:

- LEAP
- EAP-FAST (both username/password, and certificates)
- EAP-TLS

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of how to configure WLCs and lightweight access points (LAPs) for basic operation
- Knowledge of Lightweight Access Point Protocol (LWAPP) and wireless security methods
- Basic knowledge of local EAP authentication.

Components Used

The information in this document is based on these software and hardware versions:

- Windows XP with CB21AG Adapter Card and Cisco Secure Services Client Version 4.05
- Cisco 4400 Wireless LAN Controller 4.1.171.0
- Microsoft Certification Authority on Windows 2000 server

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configure Local EAP on the Cisco Wireless LAN Controller

This document assumes that the basic configuration of the WLC is already completed.

Local EAP Configuration

Complete these steps in order to configure Local EAP:

1. Add a local net user:

From the GUI. choose **Security > Local Net Users > New**, enter the User Name, Password, Guest User, WLAN ID, and Description and click **Apply**.

111111				Se⊼e Ci	ouniðrsanon í Fu	nd I coñfinar i Weives
cisco	MONITOR WLANS	<u>C</u> ONTROLLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Security	Local Net Users > I	New		1	< Back	Apply
T AAA General	User Name	eapuser2				
 RADIUS Authentication Accounting 	Password	******			1	
▶ TACACS+ LDAP	Confirm Password					
Local Net Users MAC Filtering Disabled Clients	Guest User					
User Login Policies AP Policies	WLAN ID	1				
Local EAP General	Description	Employee user local data	9958			

From the CLI you can use the **config netuser add** *<username> <password> <WLAN id> <description>* command:

Note: This command has been brought down to a second line due to spatial reasons.

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

2. Specify the user credential retrieval order.

From the GUI, choose **Security** > **Local EAP** > **Authentication Priority**. Then select LDAP, click the "<" button and click **Apply**. This puts the user credentials in the local database first.

	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	HEID
Security	Priority 0)rder > L	ocal-Auth				
- AAA General	User Cred	lentials					
 RADIUS Authentication Accounting TACACS+ Authentication Accounting Authorization LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies 	LDAP	> <	LOCAL U	9 #n			 -
▼ Local EAP Profiles EAP-FAST Parameters Authentication Priority							

From the CLI:

(Cisco Controller) >config local-auth user-credentials local 3. Add an EAP profile:

In order to do this from the GUI, choose **Security** > **Local EAP** > **Profiles** and click **New**. When the new window appears, type the Profile Name and click **Apply**.



You can also do this using the CLI command **config local–auth eap–profile add** *<profile–name>*. In our example, the profile name is *EAP–test*.

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

4. Add a method to the EAP profile.

From the GUI choose **Security** > **Local EAP** > **Profiles** and click on the profile name for which you want to add the authentication methods. This example uses LEAP, EAP–FAST, and EAP–TLS. Click **Apply** in order to set the methods.

 cisco	MONITOR MLANS		WIRELESS	SECURITY	нулькемент	сомилос	HELP
Security	Local EAP Profile	15					
- AAA General - RADOUS	Profile Name EAP-test		LEAP P	EAP-FAST P	P EAP-	n.s	3
.ili.ili. cisco	HONITOR WLAN	CONTROLLER	WIRELESS	s geouran	Management	соммию	5 HELP
Security	Local EAP Profi	les > Edit					
	Profile Name					EAP	test.
= RADEUS Authentication	LEAP					P	
Accounting * TACACS+	EAP-FAST					P	
Local Net Users MAC Filtering	EAP-TLS					D.	
Disabled Clients User Login Policies	Local Certificate	Required				R	nabled
* Local EAP	Client Certificate	Required				R	nabled
Profiles EAP-FAST Parameters	Certificate Issue	-				Ven	lor 💌
Authentication Priority Priority Order	Check against C/	A certificates				R	nabled
+ Access Centrol Lists	Verify Certificate	CN Identity					nabled
IPSec Certs	reiny certainan					-	
Wireless Protection Policies	Check Certificate	Date Validity				C (nabled

You can also use the CLI command **config local–auth eap–profile method add** *<method–name> <profile–name>*. In our example configuration we add three methods to the profile EAP–test. The methods are LEAP, EAP–FAST, and EAP–TLS whose method names are *leap, fast,* and *tls* respectively. This output shows the CLI configuration commands:

```
(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. Configure the parameters of the EAP method. This is only used for EAP–FAST. The parameters to be configured are:
 - Server Key (server-key) Server key to encrypt/decrypt Protected Access Credentials (PACs) (in hexadecimal).
 - ◆ Time to Live for PAC (pac-ttl) Sets the Time to Live for the PAC.
 - ♦ Authority ID (authority-id) Sets the authority identifier.
 - Annonymous Provision (anon-provn) Configures whether anonymous provision is allowed. This is enabled by default.

For configuration through the GUI, choose **Security > Local EAP > EAP–FAST Parameters** and enter the Server key, Time to live for the PAC, authority ID (in hex), and Authority ID Information values.

MONITOR WLANS CONTROLLER WIRELESS SECURITY	NAVAGEMENT COMMINIOS HELP
EAP-FAST Method Parameters	
Server Key (in hex)	
Confirm Server Key	
Time to live for the PAC	10 days
Authority ID (in hex)	436973636f
Authority ID Information	Cisce A-ID
Anonymous Provision	E Enabled

These are the CLI configuration commands to use in order to set these parameters for 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. Enable local authentication per WLAN:

From the GUI choose **WLANs** on the top menu and select the WLAN for which you want to configure local authentication. A new window appears. Click the **Security** > **AAA** tabs. Check **Local EAP authentication** and select the right EAP Profile Name from the pull–down menu as this example shows:

uludu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs	WLANs > Edit	
♥ WLANS WLANS AP Groups VLAN	General Security QoS Advanced Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use of default servers on this WLAN Radius Servers Authentication Servers	LDAP Servers Server 1 None
	Enabled Server 1 None None None None Server 3 None None None None None None None None	Server 3 None 💌
	Local EAP Authentication P Enabled EAP Profile Name EAP-test	

You can also issue the CLI **config wlan local–auth enable** *<profile–name> <wlan–id>* configuration command as shown here:

(Cisco Controller) >config wlan local-auth enable EAP-test 1 7. Set the Layer 2 Security parameters.

From the GUI interface, in the WLAN Edit window go to the **Security > Layer 2** tabs and chose **WPA+WPA2** from the Layer 2 Security pull–down menu. Under the WPA+WPA2 Parameters section, set the WPA Encryption to **TKIP** and WPA2 Encryption **AES**. Then click **Apply**.

ւլորը cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGE	Sage Configuration Bing Logout <u>R</u> efresh MENT C <u>O</u> MMANDS HELP
WLANS WLANS WLANS AP Groups VLAN	WLANs > Edit General Security QoS Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security WDA+WIDAE00000000 V MAC Filtering WPA+WPA2 Parameters WPA Policy WPA2 Policy V WPA2 Policy V WPA2 Encryption AES TKIP Auth Key Mgmt 802.1X V	< Back Apply

From the CLI, use these commands:

(Cisco Controller) >config wlan security wpa enable 1 (Cisco Controller) >config wlan security wpa wpal ciphers tkip enable 1 (Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1 8. Verify the configuration:

```
(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 Information CiscoA-ID

You can see specific parameters of wlan 1 with the **show wlan** *<wlan id>* command:

(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

ССКМ		Disabled	
CKIP		Disabled	
IP Security		Disabled	
IP Security Passthru		Disabled	
Web Based Authenticatior	1	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 prote	ection	Enabled	
	(Global	Infrastructure 1	MFP Disabled)
Client MFP		Optional	
Tkip MIC Countermeasure	Hold-down Timer	60	
Mobility Anchor List			
WLAN ID IP Address	Status		

There are other local authentication parameters that can be configured, in particular the active timeout timer. This timer configures the period during which local EAP is used after all RADIUS servers have failed.

From the GUI, choose **Security > Local EAP > General** and set the time value. Then click **Apply**.

սիսիս						onfiguration <u>P</u>	ing Logout <u>R</u> efres
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Security AAA General RADIUS Authentication Aesounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Lagin Policies AP Policies Prod FAP General	General Local Auth Active * The timeout period a used after all Radius S	Timeout [±] (in so uring which Local i ervers are failed	ecs) EAP will always	60]		Αρρίγ

From the CLI, issue these commands:

```
(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
```

You can verify the value to which this timer is set up when you issue the **show local–auth config** command.

```
(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. If you need to generate and load the manual PAC, you can use either the GUI or the CLI.

From the GUI, select **COMMANDS** from the top menu and chose **Upload File** from the list in the right–hand side. Select **PAC** (**Protected Access Credential**) from the File Type pull–down menu. Enter all the parameters and click on **Upload**.

ahaha							_Sa⊻e Configura	ition <u>P</u> ing	Logout <u>R</u> efres
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	не <u>ц</u> р	
Commands	Upload file	from C	ontroller					Clear	Upload
Download File	File Type			PAC (Protecte	ed Access Cred	lential) 💌			
Reboot	User (Iden	tity)		test1					
Reset to Factory Default Set Time	Validity (in	days)		60					
	Password			•••••					
	Confirm Pa	ssword		•••••					
	TFTP Serve	HP							
	IP Address			10.1.1.1					
	File Path			1					
	File Name			manual.pac					

From the CLI, enter these commands:

(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)</validity>
(Cisco Controller) >transfer upload pac test1 60 ?
<pre><password> Enter a password to protect the PAC</password></pre>
(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.TFTPTFTP Server IP.10.1.1.1TFTP Path./TFTP Filename.manual.paceData Type.PACPAC User.test1PAC Validity.60 daysPAC Password.ciscol23
Are you sure you want to start? (y/N) y PAC transfer starting. File transfer operation completed successfully.

Microsoft Certification Authority

In order to use EAP–FAST version 2 and EAP–TLS authentication, the WLC and all the client devices must have a valid certificate and must also know the public certificate of the Certification Authority.

Installation

If the Windows 2000 Server does not already have Certification Authority services installed, you need to install it.

Complete these steps in order to activate the Microsoft Certification Authority on a Windows 2000 Server:

1. From the Control Panel, choose Add/Remove Programs. :



2. Select Add/Remove Windows Components on the left side.



3. Check Certificate Services.

∀indows Components You can add or remove comp	onents of Windows	2000.	
To add or remove a compone part of the component will be i Details.	nt, click the checkb nstalled. To see wh	x. A shaded box r at's included in a c	neans that only omponent, click
Components:			
🖉 📻 Accessories and Utiliti	es		12.1 MB 🔺
🗔 📴 Certificate Services			1.4 MB
Indexing Service			0.0 MB
🗹 🍓 Internet Information Se	ervices (IIS)		21.6 MB
Management and Mor	nitorina Tools		5.2 MB
Description: Installs a certifica public key secur	ation authority (CA) to ity applications.	issue certificates I	for use with
Total disk space required:	0.0 MB		Details
Space available on disk:	4205.9 MB		Decens

Review this warning before you proceed:

Microsoft	: Certificate Servio	es	R	×
⚠	After installing Cerl from a domain. Do	tificate Services, the computer can you want to continue?	not be renamed and th	e computer cannot join or be removed
		<u>Y</u> es	No	

4. Select which type of Certification Authority you want to install. In order to create a simple stand–alone authority, select **Stand–alone root CA**.

Certification Authority types:	Description:	
Enterprise root CA Enterprise subordinate CA Stand-alone root CA Stand-alone subordinate CA	The most trusted CA in a CA hierarchy. Does not require Active Directory.	*
Advanced options		

5. Enter the necessary information about the Certification Authority. This information creates a self–signed certificate for your Certification Authority. Remember the CA name that you use.

The Certification Authority stores the certificates in a database. This example uses the default setup proposed by Microsoft:

C:\WINNT\system32\CertLog Certificate database log:	Browse
Certificate database log:	
C. WINN I Vsystem32 VCenLog	BIOMse
Store configuration information a s Shared folder:	hared folder
1	- STOLLA

6. Microsoft Certification Authority services use the IIS Microsoft Web Server in order to create and manage client and server certificates. It needs to restart the IIS service for this:



The Microsoft Windows 2000 Server now installs the new service. You need to have your Windows 2000 Server installation CD in order to install new Windows Components.

The Certification Authority is now installed.

Install the Certificate in the Cisco Wireless LAN Controller

In order to use EAP–FAST version 2 and EAP–TLS on the local EAP server of a Cisco Wireless LAN Controller, follow these three steps:

- 1. Install the device certificate on the Wireless LAN Controller.
- 2. Download a Vendor CA Certificate to the Wireless LAN Controller.
- 3. Configure the Wireless LAN Controller to use EAP-TLS.

Note that in the example shown in this document, the Access Control Server (ACS) is installed on the same host as the Microsoft Active Directory and Microsoft Certification Authority, but the configuration should be the same if the ACS server is on a different server.

Install the Device Certificate on the Wireless LAN Controller

Complete these steps:

- 1. Complete these steps in order to generate the certificate to import to the WLC:
 - a. Go to http://<serverIpAddr>/certsrv.
 - b. Choose Request a Certificate and click Next.
 - c. Choose Advanced Request and click Next.
 - d. Choose Submit a certificate request to this CA using a form and click Next.
 - e. Choose **Web server** for Certificate Template and enter the relevant information. Then mark the keys as **exportable**.
 - f. You now receive a certificate that you need to install in your machine.
- 2. Complete these steps in order to retrieve the certificate from the PC:
 - a. Open an Internet Explorer browser and choose **Tools > Internet Options > Content**.
 - b. Click Certificates.
 - c. Select the newly installed certificate from the pull-down menu.
 - d. Click Export.
 - e. Click **Next** twice and choose **Yes export the private key**. This format is the PKCS#12 (.PFX format).
 - f. Choose Enable strong protection.
 - g. Type a password.
 - h. Save it in a file <tme2.pfx>.
- 3. Copy the certificate in the PKCS#12 format to any computer where you have Openssl installed in order to convert it to PEM format.

!--- The command to be given, -in <inputfilename>. 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. Download the converted PEM format device certificate onto the 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. Once rebooted, check the certificate. (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

Download a Vendor CA Certificate to the Wireless LAN Controller

Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT

Complete these steps:

1. Complete these steps in order to retrieve the Vendor CA Certificate:

- a. Go to http://<serverIpAddr>/certsrv.
- b. Choose Retrieve the CA Certificate and click Next.
- c. Choose the CA Certificate.
- d. Click **DER encoded**.
- e. Click on Download CA certificate and save the certificate as rootca.cer.
- 2. Convert the Vendor CA from DER format into PEM format with the **openssl x509 in rootca.cer –inform DER – out rootca.pem – outform PEM** command.

The output file is rootca.pem in the PEM format. 3. Download the Vendor CA Certificate:

> (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.

Configure the Wireless LAN Controller to use EAP-TLS

Complete these steps:

From the GUI, choose **Security > Local EAP > Profiles**, choose the profile and check for these settings:

- Local Certificate Required is enabled.
- Client Certificate Required is enabled.
- Certificate Issuer is Vendor.
- Check against CA certificates is enabled.

li.ili. cisco	HONETOR MLANS CONTROLLER WERELESS	SECURITY MUNACEMENT COMMANDS HELP
Security	Local EAP Profiles > Edit	
	Profile Name	EAP-test
▼ RADIUS Authentication	LEAP	P
TACACS+ LDAP	EAP-FAST	P
Local Net Users MAC Filtering	EAP-TLS	P
Disabled Clients User Login Policies AP Policies	Local Certificate Required	E Enabled
* Local EAP	Client Certificate Required	R Enabled
Profiles EAP-FAST Parameters	Certificate Issuer	Vendor x
Authentication Priority Priority Order	Check against CA certificates	P Enabled
* Access Control Lists	Verify Certificate CN Identity	Inabled
IPSec Certs		
Wireless Protection Policies	Check Certificate Date Validity	C Enabled

Install the Certificate Authority Certificate on the Client Device

Download and Install a Root CA Certificate for the Client

The client must obtain a root CA Certificate from a Certification Authority server. There are several methods you can use to obtain a client certificate and install it on the Windows XP machine. In order to acquire a valid certificate, the Windows XP user has to be logged in using their user ID and must have a network connection.

A web browser on the Windows XP client and a wired connection to the network were used to obtain a client certificate from the private root Certification Authority server. This procedure is used to obtain the client certificate from a Microsoft Certification Authority server:

- 1. Use a web browser on the client and point the browser to the Certification Authority server. In order to do this, enter **http://IP-address-of-Root-CA/certsrv**.
- 2. Log in using **Domain_Name\user_name**. You must log in using the username of the individual who is to use the XP client.
- 3. On the Welcome window, choose **Retrieve a CA certificate** and click **Next**.
- 4. Select Base64 Encoding and Download CA certificate.
- 5. On the Certificate Issued window, click Install this certificate and click Next.
- 6. Choose Automatically select the certificate store and click Next, for successful Import message.
- 7. Connect to the Certification Authority for retrieving the Certificate Authority certificate:

Microsoft Certificate Services - tme	Home
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt y depending upon the type of certificate you request.	Once you acquire a certificate, you your e-mail messages, and more
Select a task: © Retrieve the CA certificate or certificate revocation list © Request a certificate © Check on a pending certificate	
	Next >
Microsoft Certificate Services - tme	Hom
Microsoft Certificate Services - tme Retrieve The CA Certificate Or Certificate Revocation List	Hom
Microsoft Certificate Services - trme Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification auth	Hon nority.
Microsoft Certificate Services - tree Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification auth It is not necessary to manually install the CA certification path if you request and install a certificate from thi CA certification path will be installed for you automatically.	Horn nority. is certification authority, because the
Microsoft Certificate Services - true Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification auth It is not necessary to manually install the CA certification path if you request and install a certificate from thi CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Current [ime]	Hor nority. s certification authority, because th
Microsoft Certificate Services - tree Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification auth It is not necessary to manually install the CA certification path if you request and install a certificate from thi CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Ourrorst true OER encoded or OBase 64 encoded Download CA certificate	Horn nority.
Microsoft Certificate Services - tme Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification auth It is not necessary to manually install the CA certification path if you request and install a certificate from thi CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Current [tme] © DER encoded or © Base 64 encoded Download CA certificate Download CA certificate Download CA certificate Download CA certification path	Hom nority. Is certification authority, because the

8. Click Download CA certificate.

Microsoft Certificate Ser

Microsoft Certificate Services tme	Microsoft Certificate Services tme Hom			
Retrieve The CA Certificate Or Certificate Revocation List				
Install this CA certification path to allow your	computer to trust certificates issued from this certification	n authority.		
It is not necessary to manually install the CA	File Download - Security Warning	this certification authority, because the		
CA certification path will be installed for you	Do you want to open or save this file?			
Choose file to download:	Name: certnew.cer			
Contra inte	Fion: 10.1.1.12			
	Open Save Cancel			
⊙DER encoded or ⊙Bar Developed CA continents				
Download CA certification p	While files from the Internet can be useful, this file type can			
Download latest certificate r	 apen or save this software. What's the sisk? 			

	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 Import Wizard		×
Certificate Store Certificate stores are sy	/stem areas where certificates are kept.	
Windows can automatic	ally select a certificate store, or you can specify a location for	
Automatically sel	ect the certificate store based on the type of certificate	
C Place all certifical	tes in the following store	
Certificate store:		
	Browse	
	Carcel	-
	Calcel	

×



9. In order to check that the Certification Authority certificate is correctly installed, open Internet Explorer and choose **Tools > Internet Options > Content > Certificates**.

Microsoft Certificate Service	es - M	icrosoft Internet Exploi
File Edit View Favorites	Tools	Help
Back Section Back Section Sectio	Mail Pop- Man Syno Wino	and News -up Blocker age Add-ons chronize dows Update
Retrieve The CA Cer	Wind Crea IBM	dows Messenger ate Mobile Favorite Java Console

Internet Options
General Security Privace Content Gonnections Programs Advanced Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Content Advisor Image: Cont
Certificates Use certificates to positively identify yourself, certification authorities, and publishers. Clear SSL State Certificates Publishers
Personal information AutoComplete stores previous entries AutoComplete AutoComplete
Microsoft Profile Assistant stores your My Profile
OK Cancel Apply

In Trusted Root Certification Authority, you should see your newly installed Certification Authority:

Certificates				? ×
Intended purpose:	<all></all>			~
Intermediate Certificati	on Authorities Trusted Root C	ertification Auth	norities Trusted Pub	
Issued To	Issued By	Expiratio	Friendly Name	~
Thawte Server Co	A Thawte Server CA pi Thawte Timestamping tme SGC UTN - DATACorp SGC UTN-USEP Einst-Client	12/31/2020 12/31/2020 2/28/2012 6/24/2019 7/9/2019	Thawte Server CA Thawte Timesta <none> UTN - DATACorp</none>	
UTN-USERFirst-H	ar UTN-USERFirst-Hardw et UTN-USERFirst-Netwo bj UTN-USERFirst-Object	7/9/2019 7/9/2019 7/9/2019 7/9/2019	UTN - USERFirst UTN - USERFirst UTN - USERFirst	
Import Expo	ort Remove	12/31/1999	Advan	 ced
Certificate intended pu <all></all>	rposes		View	
			Clo	se

Generate a Client Certificate for a Client Device

The client must obtain a certificate from a Certification Authority server for the WLC to authenticate a WLAN EAP–TLS client. There are several methods that you can use in order to obtain a client certificate and install it on the Windows XP machine. In order to acquire a valid certificate, the Windows XP user has to be logged in using their user ID and must have a network connection (either a wired connection or a WLAN connection with 802.1x security disabled).

A web browser on the Windows XP client and a wired connection to the network are used to obtain a client certificate from the private root Certification Authority server. This procedure is used to obtain the client certificate from a Microsoft Certification Authority server:

- 1. Use a web browser on the client and point the browser to the Certification Authority server. In order to do this, enter **http://IP-address-of-Root-CA/certsrv**.
- 2. Log in using **Domain_Name\user_name**. You must log in using the username of the individual who uses the XP client. (The username gets embedded into the client certificate.)
- 3. On the Welcome window, choose **Request a certificate** and click **Next**.
- 4. Choose Advanced request and click Next.
- 5. Choose Submit a certificate request to this CA using a form and click Next.
- 6. On the Advanced Certificate Request form, choose the Certificate Template as **User**, specify the Key Size as **1024** and click **Submit**.
- 7. On the Certificate Issued window, click **Install this certificate**. This results in the successful installation of a client certificate on the Windows XP client.

/elcome	
ou use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acc Il be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail me spending upon the type of certificate you request.	quire a certificate, you essages, and more
elect a task: © Retrieve the CA certificate or certificate revocation list	
 Request a certificate Check on a pending certificate 	
	Next >
ficrosoft Certificate Services tme	Hom
hoose Request Type	
lease select the type of request you would like to make:	
D User certificate request.	
D Advanced request	
	Next >
Microsoft Certificate Services tme	Hom
Idvanced Certificate Requests	
fou can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the p authority (CA) will determine the certificates that you can obtain.	policy of the certificatio
 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 	IPKCS#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. Select Client Authentication Certificate.

Microsoft Certific	ate Services tme
Advanced Ce	rtificate Request
Certificate Temp	late:
	User
Key Options:	
CSP:	Microsoft Base Cryptographic Provider v1.0
Key Usage:	○ Exchange ○ Signature ④ Both
Key Size:	512 Min: 384 (common key sizes: <u>512 1024</u>) Max: 1024
	 Create new key set Set the container name Use existing key set Enable strong private key protection
	Export keys to file
	Use local machine store You must be an administrator to generate a key in the local machine store.
Additional Optio	ns:
Hash Algorithm:	SHA-1 Only used to sign request.
	Save request to a PKCS #10 file
Attrihuteo.	6

The client certificate is now created.

9. In order to check that the certificate is installed, go to Internet Explorer and choose **Tools > Internet Options > Content > Certificates**. In the Personal tab, you should see the certificate.

Ce	rtificate	15					?	X
Ъ	ntended pu	urpose:	<all></all>					*
	Personal	Other Peop	le Intermediate Certif	ication Authoritie	Trus	ted Root Certific	atior <	>
	Issued	То	Issued By	Expira	itio	Friendly Name		
	Adm	inistrator	tme	3[27]2	008	<none></none>		
ſ	Import	. Exp	ort Remove	7		Ad	vanced.	_
	Certificate	e intended p						
	Encryptin	g File System	, Secure Email, Client A	uthentication				
						v	iew	J
						_	Close	
							0000	

EAP-TLS with Cisco Secure Services Client on the Client Device

Complete these steps:

1. The WLC, by default, broadcasts the SSID, so it is shown in the Create Networks list of scanned SSIDs. In order to create a Network Profile, you can click the SSID in the list (Enterprise) and click **Create Network**.

If the WLAN infrastructure is configured with broadcast SSID disabled, you must manually add the SSID. In order to do this, click **Add** under Access Devices and manually enter the appropriate SSID (for example, Enterprise). Configure active probe behavior for the client. That is, where the client actively probes for its configured SSID. Specify **Actively search for this access device** after you enter the SSID on the Add Access Device window.

Note: The port settings do not permit enterprise modes (802.1X) if the EAP authentication settings are not first configured for the profile.

2. Click **Create Network** in order to launch the Network Profile window, which permits you to associate the chosen (or configured) SSID with an authentication mechanism. Assign a descriptive name for the profile.

Note: Multiple WLAN security types and/or SSIDs can be associated under this authentication profile.

Access	Data Security	
II aruba-ap-config-in-the-clear (2 accesses	dete m WEF	
II cov5 (2 accesses detected)	X Open	
	X Open	
con-eap	NEP	
001907351aa3 High Signal	WEP	
guestnet (5 accesses detected)	💢 Open	
guestnetwork	💢 Open	
N-Rogue	🚡 WEP	
👔 secure-1 (3 accesses detected)	?🗎 Mixed	
III tme-test (5 accesses detected)	🔒 WPA	
III trng1 (2 accesses detected)	1 WEP	

- 3. Turn on authentication and check the EAP–TLS method. Then click **Configure** in order to configure EAP–TLS properties.
- 4. Under Network Configuration Summary, click **Modify** in order to configure the EAP / credentials settings.
- 5. Specify **Turn On Authentication**, choose **EAP–TLS** under Protocol, and choose **Username** as the Identity.

6. Specify **Use Single Sign on Credentials** to use log on credentials for network authentication. Click **Configure** to set up EAP–TLS parameters.

Tomone Toon oop	Network			
Authentication Metho	nde:			
C Turn Off			C Use Machine Creden	tials
Turn On			C Use Single Sign on C	redentials
Use Userna	me as Identity		Request when needed	ed
C Use Anonyr	mous' as Identity		 Remember for 	ever
Protocol	^		C Remember for	this session
EAP-MD5			C Remember for	5 minutes
EAP-MSCHA	APv2			
FAP-TLS				
FAST				
🔲 GTC	- C	onfigure		
Help			OK	Cancel
			-	
				×
Network Name: con-eap Ne	itwork			×
Network Name: con-eap Ne I Availabl	twork le to all users (public	; profile)		×
Network Name: Con-eap Ne V Availabl	twork le to all users (public tically establish Mac	profile)	 on	×
Network Name: Con-eap Ne Valabl Availabl Automa V Automa	twork le to all users (public tically establish Mac tically establish Use efore user account	: profile) :hine connection r connection (supports smar	on tcard/password only)	×
Network Name: Con-eap Ne Vavailabl Availabl Automa Vatuoma Vatuoma Network Configuratio	itwork le to all users (public tically establish Mac tically establish Use efore user account	: profile) :hine connection r connection (supports smar	on tcard/password only)	×
Network Name: Con-eap Ne V Availabl Automa V Automa V B Network Configuratio Authentication: E/	itwork le to all users (public tically establish Mac tically establish Use efore user account on Summary:	: profile) :hine connection r connection (supports smar	on tcard/password only)	×
Network Name: con-eap Ne Vavalabl Automa V Automa V Automa V B Network Configuratio Authentication: E/ Credentials: R	twork le to all users (public tically establish Mac tically establish Use efore user account on Summary: AP-TLS; equest when neede	: profile) :hine connection r connection (supports smar (supports and rememb	on tcard/password only) er for the session.	×
Network Name: Con-eap Ne Vavailabl Automa V Automa V Automa V B Network Configuratio Authentication: Credentials: R	twork le to all users (public tically establish Mac tically establish Use efore user account on Summary: AP-TLS; equest when needs	: profile) :hine connection (supports smar : : : : : : : : : : : : :	on tcard/password only) er for the session.	×
Network Name: Con-eap Ne Vavailabl Automa V Automa V Automa V B Network Configuratio Authentication: E/ Credentials: R	itwork le to all users (public tically establish Mac tically establish Use efore user account on Summary: AP-TLS; equest when neede	: profile) :hine connection (supports smar :d and rememb	on tcard/password only) er for the session.	×
Network Name: con-eap Ne Variable Automa V Automa V Automa V Automa V B Network Configuratio Authentication: E/ Credentials: R	twork le to all users (public tically establish Mac tically establish Use efore user account on Summary: AP-TLS; equest when neede	: profile) shine connection (supports smar ed and rememb	on tcard/password only) er for the session.	×
Network Name: con-eap Ne Vavailabl Automa V Availabl Automa V Automa V Automa V B Network Configuratio Authentication: E/ Credentials: R Access Devices Access / SSID con-eap	twork le to all users (public tically establish Mac tically establish Use efore user account on Summary: AP-TLS; equest when neede	: profile) :hine connection (supports smar ed and rememb	on tcard/password only) er for the session.	×
Network Name: Con-eap Ne Availabl Automa V Automa V Automa V Automa V B Network Configuratio Authentication: E/ Credentials: R Access Devices Access / SSID con-eap	twork le to all users (public tically establish Mac tically establish Use efore user account on Summary: AP-TLS; equest when neede Mode WPA2 Enterprise	: profile) :hine connection (supports smar ed and rememb	on teard/password only) er for the session.	×
Network Name: con-eap Ne Vavaiabl Automa V Avaiabl Automa V Automa V Automa Automa Automa Automa Automa Automa V Automa Automa Automa Automa V Automa Automa V Automa Automa V Automa Automa V Automa V Automa Automa V Automa V Aut	twork le to all users (public tically establish Mac tically establish Use efore user account on Summary: AP-TLS; equest when neede Mode WPA2 Enterprise	: profile) :hine connection (supports smar : :d and rememb	on tcard/password only) er for the session.	×
Network Name: Con-eap Ne Valable Automa V Automa V Automa V Automa V B Network Configuratio Authentication: E Credentials: R Access Devices Access / SSID con-eap	twork le to all users (public tically establish Mac tically establish Use efore user account on Summary: AP-TLS; equest when neede Mode WPA2 Enterprise	: profile) :hine connection (supports smar ed and rememb	on tcard/password only) er for the session.	×

Help

7. In order to have a secured EAP–TLS configuration you need to check the RADIUS server certificate. In order to do this, check **Validate Server Certificate**.

Cancel

0K

Configure EAP Method	I	×
-EAP-TLS settings:		
Use Smartcard-based	Client Certificates Only	
Validate Server Certifi	cate	
JV Allow Fast Session Re	esumption	
Hala 1	04	Canad
неір		Cancel

8. In order to validate the RADIUS server certificate, you need to give Cisco Secure Services Client information in order to accept only the right certificate. Choose **Client > Trusted Servers > Manage Current User Trusted Servers**.

()	isco Secure Services	Client	_ 🗆 🗵
Clie	nt Administration Help		
	Manage Adapters		
	Trusted Servers 🔹 🕨	Manage Current User Trusted Servers	1
	Advanced Settings	Manage Machine / All Users Trusted Servers	Data Seci
> >	Enable Client Turn WiFi Radio On	ork Disconnected	
-	Show System Trav	Misconfigured Access (AutoConn	ect) 🔐 WPA
-	Close Window	Capable for: wep Configured for: woa2	
	د		Þ
			Details
	Connec	t Configure Remove Status	

Rule Name	Validation Method	

9. Give a name for the rule and check the name of the server certificate.

()) Trusted Server	×
Trusted Server	
Rule name: WLC-Config	
Validation method: Certificate	_
Match ANY Certificate Validation Rule: Subject Alternative Name Exactly matches Subject/Common Name Exactly matches	▼ tme
Help	OK Cancel

The EAP-TLS configuration is finished.

10. Connect to the Wireless network profile. The Cisco Secure Services Client asks for the user login:

Cisco Secure Services Client
Client Administration Help
Create Networks Manage Networks
Network
Image: Second Reference Image: Second Reference
Username: Administrator
Send Cancel
I
Details
Connect Configure Remove Status

The Cisco Secure Services Client receives the server certificate and checks it (with the rule configured and the Certification Authority installed). It then asks for the certificate to use for the user.

11. After the client authenticates, choose **SSID** under the Profile in the Manage Networks tab and click **Status** to query connection details.

The Connection Details window provides information on the client device, connection status and statistics, and authentication method. The WiFi Details tab provides details on the 802.11 connection status, which includes the RSSI, 802.11 channel, and authentication/encryption.

	199	Status		Security
con-eap		Connected: Authenticated	(AutoConn	WPA2
1:24:28.044 1:24:28.054 1:24:28.074 1:24:28.074 1:24:28.074 1:24:28.074 1:24:28.074 1:24:28.075 1:24:28.05 1:24:28.305 1:24:28.305 1:24:28.305 1:24:28.505 1:24:28.505 1:24:28.505	con-eap Network Co Connection authentic Port state transition to Connection association Connection association Port state transition to Port state transition to Identity has been required Identity has been required Authentication started The server has requered Validating the server. Port state transition to The authentication pri The following IP addre	nnection requested from user ation started using the logged AC_PORT_STATE_UNAUT in started using encryption mo in succeeded. AC_PORT_STATE_CONNE AC_PORT_STATE_AUTHE uested from the network. It to the network. It using method type EAP-TLS sted using authentication type ted using authentication type ted using authentication type AC_PORT_STATE_AUTHE occess has succeeded. ess has been assigned: 10.10	context. in user's cred HENTICATED de AC_ENCR CTING(AC_P(NTICATING(A :: EAP-TLS :: EAP-TLS :: EAP-TLS NTICATED(A0 0.80.24.	entials.)(AC_PORT_STATUS_STARTED) _AES AC_ASSOC_111_8021X DRT_STATUS_LINK_UP) IC_PORT_STATUS_8021x_ACQUIRED

CO Cisco Secure Services Client	
Client Administration Help	
Create Networks Manage Networks	
Network 🛆	Status Data :
E- Con Network	Disconnected
💷 💥 con	No Adapter Available (Suspended) 🛛 🗕 🛛
E- 🎨 con-eap Network	Connected: Authenticated
L	Connected: Authenticated (AutoConnect) 🗃 🔪
Disconnect Configure	Details Remove Status
	//

onnection Status	
onnection Details WiFi Detai	ls
Status:	Connected: Authenticated
Duration:	00:01:19
Network Profile:	con-eap Network
Cise Network Adapter:	co Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:	00-40-96-A6-D6-F6
Access Device:	con-eap
Access Device MAC Address:	00-19-07-35-1A-AC
Transmitted packets:	346
Received packets:	3
Speed:	54.0 Mbps
Authentication Method:	EAP-TLS
Authentication Server:	tme2 (trusted)
IP Address:	10.10.80.24
Heb	Close

Debug Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use debug commands.

These debug commands can be employed at the WLC to monitor progress of the authentication exchange:

- debug aaa events enable
- debug aaa detail enable
- debug dot1x events enable
- debug dot1x states enable
- debug aaa local-auth eap events enable

OR

• debug aaa all enable

Related Information

- Cisco Wireless LAN Controller Configuration Guide, Release 4.1
- WLAN Technology Support
- Technical Support & Documentation Cisco Systems

Contacts & Feedback | Help | Site Map

© 2013 – 2014 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: May 31, 2007

Document ID: 91628