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 <u>Cisco sulle convenzioni</u> 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:

 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.							SAVE C	u u Rau U FR	
CISC)), :0		<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY		C <u>O</u> MMANDS	HELP
Security		Local Net	Users >	New	l]	< Back	Apply
T AAA General		User Nam	e	eapuser2					
▼ RADIUS Authentic Accountin	cation	Password		•••••					
TACACS+		Confirm Pa	assword	•••••					
MAC Filterin Disabled Cli	sers Ig ients	Guest Use	r						
User Login A AP Policies	Policies	WLAN ID		1	*				
Ceneral		Descriptio	in	Employee u	iser local datab	ase			

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</p>

uludu cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	HErb
Security	Priority 0	rder > L	ocal-Auth				
General • RADIUS	User Cred	lentials					
Authentication Accounting * TACACS+ Authentication Accounting Authorization LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	LDAP	*	LOCAL	9 WR			-
Local EAP Profiles EAP-FAST Parameters Authentication Priority							

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**.

	MONITOR	WLANS		R WIREL	LESS SECU	RITY MAN	AGEMENT	COMMANDS	HEID	 			
	Local E	AP Profile	s								•	iew	Apply
	Profile N	iame	u	EAP	EAP-FAST		EAP-T	LS			1		
										1			
rs ty													
	TOD 141 414						100				Sage Co	nfiguration B	ng Logout Befre
Bow		s <u>c</u> oninoci	EK MINELESS	SECONTIL	MENNUEMENT	CTHANNED	HELP.						1
LOCI	II EAP' PTOT	ies > riew										< Back	Apply
Profi	le Name				EAP-test								

Per eseguire questa operazione, è possibile usare anche il comando **config local-auth eapprofile 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).					
.ili.ili. cisco	MONITOR WLANS CONTROLLER	WIRELESS SEC	URITY MUNAGEMENT	сонников нер	
Security	Local EAP Profiles				
Ceneral • RADOUS	Profile Name EAP-rest	R P	AP-PAST EAP-	n.s	
uluulu cisco	MONITOR WLANS CONTROLLER	wpeless :	ECURITY MENAGEMENT	г сомнимов неця	
Security	Local EAP Profiles > Edit				
	Profile Name			EAP-test	
+ RADEUS Authentication	LEAP			P	
Accounting • TACACS+	EAP-FAST			P	
Local Net Users MAC Filtering	EAP-TLS			P	
Disabled Clients User Login Policies AR Policies	Local Certificate Required			P Enabled	
* Local EAP	Client Certificate Required			E Enabled	
Profiles EAP-FAST Parameters	Certificate Issuer			Vendor x	
Authentication Priority Priority Order	Check against CA certificates			P Enabled	
Access Central Lists	Verify Certificate CN Identity			C Enabled	
IPSec Certs				E	
Wireless Protection Policies	Check Certificate Date Validity			Enabled	

Èinoltre 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.

1	MONITOR WLANS CONTROLLER WIRELESS SECURITY N	NUVAGEMENT COMMANDS HELP
	EAP-FAST Method Parameters	
	Server Key (in hex)	****
	Confirm Server Key	****
	Time to live for the PAC	10 days
	Authority ID (in hex)	426972636f
	Authority ID Information	Cisce A-ID
	Anonymous Provision	F Enabled

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:

،، ،،، ،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MONAGEMENT COMMANDS HE	p
WLANs	WLANs > Edit	
* WLANS WLANS	General Security QoS Advanced	
AF GOUDS YOAR	Select AAA servers below to override use of default servers on this WLAN Radius Servers Authentication Servers Accounting Servers Enabled	LDAP Servers Server 1 None Server 2 None
	Server 1 None None P Server 2 None None P	Server 3 None 💌
	Local EAP Authentication	
	Local EAP Authentication 🗜 Enabled EAP Profile Name EAP-test 🗷	

Èpossibile 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

7. 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.		
		Saye Configuration Ping Logout Refresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANA	SEMENT C <u>O</u> MMANDS HELP
WLANs	WLANs > Edit	< Back Apply
T WI ANS	General Security QoS Advanced	
WLANS AP Groups VLAN	Layer 2 Layer 3 AAA Servers	
	Laver 2 Security WPA+WPA2	
	MAC Filtering	
	WPA+WPA2 Parameters	
	WPA Policy	
	WPA Encryption 🔲 AES 🗹 TKJP	
	WPA2 Policy	
	WPAZ Encryption VAES TKJP	
	Auth Key Mgmt 802.1X Y	

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

8. 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
Configured on WLANs	1
Configured on WLANs	1
Configured on WLANs EAP Method configuration: EAP-FAST:	1
Configured on WLANS EAP Method configuration: EAP-FAST: More or (q)uit	1
Configured on WLANS EAP Method configuration: EAP-FAST: More or (q)uit Server key	1 <hidden></hidden>
Configured on WLANS EAP Method configuration: EAP-FAST: More or (q)uit Server key TTL for the PAC	1 <hidden> 10</hidden>
Configured on WLANS EAP Method configuration: EAP-FAST: More or (q)uit Server key TTL for the PAC Anonymous provision allowed	1 <hidden> 10 Yes</hidden>
Configured on WLANS EAP Method configuration: EAP-FAST: More or (q)uit Server key TTL for the PAC Anonymous provision allowed Authority ID	1 <hidden> 10 Yes 43697369f10000000000000000000</hidden>

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)
	Disabled
CCX - Aironetle Support	Enabled
CCX - Gratuitous ProbeResponse (GPR)	Disabled
	Disabled
Wired Protocol	None
More or (g)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 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

Èpossibile 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



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**

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**.

սիսիս							Sa⊻e Configur	ation <u>P</u> ing	Logout <u>R</u> efre
cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>- s</u> ecurity	MANAGEMENT	-C <u>O</u> MMANDS	не <u>г</u> р	
Commands	Upload fil	e from C	ontroller					Clear	Upload
Download File	File Type			PAC (Protects	ad Accass Cred	dential) 💌			
Reboot	User (Idei	ntity)		test1				/	
Reset to Factory Default Set Time	Validity (i	n days)		60					
	Password			•••••					
	Confirm P	assword		•••••					
	TFTP Serv	er							
	IP Addres	s		10.1.1.1					
	File Name			manual.pac					

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 ? Enter the PAC validity period (days) <validity> (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) ${\rm y}$ 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.



3. Controllare Servizi certificati.

ndows Components Wizard				
Windows Components You can add or remove comp	onents of Windows 2000.			
To add or remove a componer part of the component will be i Details.	nt, click the checkbox. A nstalled. To see what's in	shaded box means that only included in a component, 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	52MB		
Description: Installs a certifica public key securi	ation authority (CA) to issu ity applications.	e certificates for use with		
Total disk space required:	0.0 MB	Datala		
Space available on disk:	4205.9 MB	<u>U</u> etaiis		
	< <u>B</u> ack	: <u>N</u> ext > Cancel		
minare questo avviso prima di				
cedere:				
osoft Certificate Services	4			
After installing Certificate Services	the computer cannot be repar	ed and the computer cannot join or be remov		
from a domain. Do you want to cor	tinue?	and and the compater carried join of De remo-		

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

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.

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:

<u>C</u> ertificate database:		
C:\WINNT\system32\CertLog		Browse
Certificate database log:		
C:\WINNT\system32\CertLog		Bro <u>w</u> se
Store configuration information	a shared folder	
Shared folder: ~		Browse

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: Microsoft	t Certificate Services
<u>.</u>	Internet Information Services is running on this computer. You must stop this service before proceeding. Do you want to stop the service now?

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:

- Per generare il certificato da importare sul WLC, completare i seguenti passaggi:Visitare il sito Web all'indirizzo http://<serverlpAddr>/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.
- 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 <ciscol23> (Cisco Controller) >transfer download
filename tme2.pem

(Cisco Controller) >transfer download start

Mode.....TFTPData Type.....Vendor Dev CertTFTP Server IP....10.1.1.12TFTP Packet Timeout.....6TFTP Max Retries.....10TFTP 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:

- Per recuperare il certificato CA del fornitore, completare la procedura seguente:Visitare il sito Web all'indirizzo http://<serverlpAddr>/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.
- 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.II file di output è rootca.pem nel
 formato PEM.

```
3. Scaricare il certificato CA del fornitore:
  (Cisco Controller) >transfer download datatype eapcacert
  (Cisco Controller) >transfer download filename ?
             Enter filename up to 16 alphanumeric characters.
 <filename>
  (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.

ululu cisco	MONITOR MLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COMMANDS HELP
Security	Local EAP Profiles > Edit	
- AAA	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	P Enabled
* Local EAP	Client Certificate Required	Enabled
Profiles EAP-FAST Parameters	Certificate Issuer	Vendor 💌
Authentication Priority Priority Order	Check against CA certificates	P Enabled
Access Control Lists	Verify Certificate CN Identity	C Enabled
BrSec Certs Wireless Protection	Check Certificate Date Validity	C trabled

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:

Velcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certific will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and sepending upon the type of certificate you request.	ate, you more
Select a task: Retrieve the CA certificate or certificate revocation list Request a certificate Check on a pending certificate	
	lext >
Microsoft Certificate Services - tme	Home
Retrieve The CA Certificate Or Certificate Revocation List	
nstall this CA certification path to allow your computer to trust certificates issued from this certification authority.	
t is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, be CA certification path will be installed for you automatically.	cause the
CA Certificate: Current [tmie]	

DER encoded or OBase 64 encoded
 Download CA certificate
 Download CA certification path
 Download latest certificate revocation list

8. Fare clic su Scarica certificato

Microsoft Certificate Services - tme

Microsoft Certificate Services - 1me		<u>Home</u>
Retrieve The CA Certificate Or Certificate	e 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	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: CA Certificate: Current [tme]	Name: certnew.cer Type: Security Certificate, 798 bytes From: 10.1.1.12	
●DER encoded or ●Bar	Open Save Cancel	
Download CA certificate Download CA certification p Download latest certificate r	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. <u>What's the risk?</u>	

Certificate Import Wizard



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.

ate	< Back Next > Cance
Cer	cate Store rtificate stores are system areas where certificates are kept.
WH (Automatically select the certificate store based on the type of certificate
	C Place all certificates in the following store
	Certificate store: Browse



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



Internet Options 🛛 🛛 🔀
General Security Privacy Content Connections Programs Advanced
Content Advisor Ratings help you control the Internet content that can be viewed on this computer. Enable Settings
Certificates
Use certificates to positively identify yourself, certification authorities, and publishers.
Clear SSL State Certificates Publishers
Personal information
AutoComplete stores previous entries and suggests matches for you.
Microsoft Profile Assistant stores your My Profile
OK Cancel Apply

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

Issued To	1	Issued By	Expiratio	Friendly Name	1
🚟 Thawte Serv	/er CA	Thawte Server CA	12/31/2020	Thawte Server CA	
📇 Thawte Time	estampi	Thawte Timestamping	12/31/2020	Thawte Timesta	
tme		tme	2/28/2012	<none></none>	
UTN - DATA	Corp SGC	UTN - DATACorp SGC	6/24/2019	UTN - DATACorp	
UTN-USERFit	rst-Clie	UTN-USERFirst-Client	7/9/2019	UTN - USERFirst	
UTN-USERFit	rst-Har	UTN-USERFirst-Hardw	7/9/2019	UTN - USERFirst	
UTN-USERFi	rst-Net	UTN-USERFirst-Netwo	7/9/2019	UTN - USERFirst	••
UTN-USERFit	rst-Obj	UTN-USERFirst-Object	7/9/2019	UTN - USERFirst	
VeriSign Com	nmercia	VeriSign Commercial S	12/31/1999	VeriSign Commer	
Import	Export	Remove		Adva	nced
	Loporerri			- India	11000
Certificate intende	ed purpose	S			

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 tme	Home
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you a will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail depending upon the type of certificate you request.	acquire a certificate, you messages, and more
Select a task: O Retrieve the CA certificate or certificate revocation list	
 Request a certificate Check on a pending certificate 	
	Next >
Microsoft Certificate Services tme	Home
Choose Request Type	
Please select the type of request you would like to make:	
O User certificate request.	
 Advanced request 	
	Next >
Miemont Cartificata Sanácas Ima	Home
Advanced Certificate Requests	Interior
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the authority (CA) will determine the certificates that you can obtain.	e policy of the certification
 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

Certificate Temp	late:				
	User		~		
Key Options:					
CSP:	Microsoft Base Crypt	ographic l	Provider v1.0)	~
Key Usage:	O Exchange O Si	gnature	 Both 		
Key Size:	512 Min: 384 Max:1024 (ee	ommon key :	rizes: <u>512 102</u>	4)	
	 Create new key se Set the contain Use existing key s 	t nername :et			
	Enable strong priva	ate key pr	otection		
	Mark keys as expo Export keys to	ortable o file			
	Use local machine You must be an a a key in the local	store Idministra Machine	tor to gener store.	ate	
Additional Optio	ns:				
Hash Algorithm:	SHA-1 Only used to sign requ	vest.			
	Save request to a l	PKCS #10) file		

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.

Certificates	5				? 🔀
Intended pu	rpose:	<all></all>			~
Personal	Other Peop	le Intermediate Certificati	on Authorities Trust	ed Root Certification	< >
Issued 1	Го	Issued By	Expiratio	Friendly Name	
🕮 Admi	nistrator	tme	3/27/2008	<none></none>	
Import	Exp	ort Remove		Advan	
Certificate	intended p	urposes			
Encrypting	File Systen	n, Secure Email, Client Authe	entication		_
				View	
				Clo	se

EAP-TLS con Cisco Secure Services Client sul dispositivo client

Attenersi alla seguente procedura:

- 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.
- 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.

hoom (Data Socuritu
Access A	WEP
а в	X Open
ccx5 (2 accesses detected)	X Open
con	X Open
Con-eap	WEP WEP
001907351aa3 High Signal	WEP
guestnet (5 accesses detected)	😹 Open
guestnetwork	💢 Open
N-Rogue	🚈 WEP
secure-1 (3 accesses detected)	? Mixed
tme-test (5 accesses detected)	🖀 WPA
II trng1 (2 accesses detected)	1 WEP
III ungr (z accesses delected)	

- 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-

Authentication Methods: Turn Off Turn On Use Username as Identity Use 'Anonymous' as Identity Protocol EAP-MD5 EAP-MD5 EAP-MSCHAPv2 EAP-TLS Authentication Methods: Configure	User Credentials: C Use Machine Credentials C Use Single Sign on Credentials Request when needed Remember forever Remember for this session Remember for 5 minute

Network Profile	-			×
Network				
Name: con-eap	Network			_
🔽 Avai	lable to all users (publ	ic profile)		
T Auto	matically establish Ma	chine con	nection	
🔽 Auto	matically establish Us	er connec	tion	
V	Before user account	t (support:	s smartcard/password only)	
-Network Configur	ation Summary:			
Authentication:	EAP-TLS:			
C				\exists
Credentials:	Request when need	led and re	member for the session.	
			Modify	
Access Devices				
Access / SSID	Mode	Notes		_
con-eap	WPA2 Enterprise	5		
1				
Add	Modify Co	onfiguratio	n Remove	
Help			OK Cance	ы

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

Configure EAP Metho	d	
-EAP-TLS settings:		
Use Smartcard-base	d Client Certificates Only	
🔽 Validate Server Cert	ificate	
Allow Fast Session F	Resumption	
	•	
Help	OK	Cancel

 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.

Cisco Secure Services	Client	_O×
Client Administration Help		
Manage Adapters	hotuorko	
Trusted Servers 🔸	Manage Current User Trusted Servers	
Advanced Settings	Manage Machine / All Users Trusted Servers	Data Seci
Enable Client	ork Disconnected	
✓ Turn WiFi Radio On	Misconfigured Access (AutoCor	meeti GBI WP4
 Show System Tray 	Capable for: wep	
Close Window	Configured for: wpa2	
Connect	t Configure Remove. Status	Details
Manage Current User	Trusted Servers	
-Trusted Server Definition	Current Users:	
Dute Name	V-Ed-C M-L	
Add Server Bule	Validation Met	ielected
Add Server Hule	Hemove Selected Edit S	elected
Help		Close

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

•
7
tme
OK Cancel

Configurazione EAP-TLS completata.

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

😳 Cisco Secure Services Client
Client Administration Help
Create Networks Manage Networks Network A Image Network Enter Your Credentials Image Network Con Network Image Network Please enter your credentials for network, access con-eap
Username: Administrator
Connect Configure Remove Status

sco 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.

conneap Connected Authenticated (AutoConn WPA2 1:24:28.044 connection authentication stated using the logged in user's credentials. 1:24:28.074 Connection authentication stated using the logged in user's credentials. 1:24:28.074 Connection association stated using encryption mode AC_ENCR_AES AC_ASSOC_11:8021X 1:24:28.104 Connection association stated using encryption mode AC_ENCR_AES AC_ASSOC_11:8021X 1:24:28.104 Connection association succeeded. 1:24:28.295 Port state transition to AC_PORT_STATE_OUNECTING(AC_PORT_STATUS_B021x_ACQUIRED) 1:24:28.295 Port state transition to AC_PORT_STATE_AUTHENTICATING(AC_PORT_STATUS_8021x_ACQUIRED) 1:24:28.205 Identity has been requested from the network. 1:24:28.305 Identity has been requested using authentication type: EAP-TLS 1:24:28.305 The server has requested using authentication type: EAP-TLS 1:24:28.305 Port state transition to AC_PORT_STATE_AUTHENTICATED(AC_PORT_STATUS_GROUP_KEY) 1:24:28.305 Port state transition to AC_PORT_STATE_AUTHENTICATED(AC_PORT_STATUS_GROUP_KEY) 1:24:28.505 Port state transition to AC_PORT_STATE_AUTHENTICATED(AC_PORT_STATUS_GROUP_KEY) 1:24:28.505 Port state transition to AC_PORT_STATE_AUTHENTICATED(AC_PORT_STATUS_GROUP_KEY) 1:24:28.505	elected Acce	199	Status	Sec	unity
124:28.044 con-eap Network Connection requested from user context. 124:28.054 Connection authentication started using the logged in user's credentials. 124:28.074 Port state transition to AC_PORT_STATE_UNAUTHENTICATED(AC_PORT_STATUS_STARTED) 124:28.094 Connection association succeeded. 124:28.104 Connection association succeeded. 124:28.295 Port state transition to AC_PORT_STATE_CONNECTING(AC_PORT_STATUS_LINK_UP) 124:28.295 Port state transition to AC_PORT_STATE_AUTHENTICATING(AC_PORT_STATUS_8021x_ACQUIRED) 124:28.295 Port state transition to AC_PORT_STATE_AUTHENTICATING(AC_PORT_STATUS_8021x_ACQUIRED) 124:28.305 Identity has been requested from the network. 124:28.305 Identity has been sent to the network. 124:28.305 Identity has requested using authentication type: EAP-TLS 124:28.305 The cient has requested using authentication type: EAP-TLS 124:28.305 Port state transition to AC_PORT_STATE_AUTHENTICATED(AC_PORT_STATUS_GROUP_KEY) 124:28.505 Port state transition to AC_PORT_STATE_AUTHENTICATED(AC_PORT_STATUS_GROUP_KEY) 124:28.505 The authentication process has succeeded. 124:28.505 The following IP address has been assigned: 10.10.80.24.	con-eap		Connected: Authenticate	ed (AutoConn WPA	2
Clear	1:24:28.044 1:24:28.054 1:24:28.094 1:24:28.094 1:24:28.194 1:24:28.295 1:24:28.305 1:24:28.335 1:24:28.335 1:24:28.335 1:24:28.335 1:24:28.505 1:24:28.505 1:24:35.534	con-eap Network C Connection authenti Port state transition I Connection associati Connection associati Port state transition I Port state transition I Identity has been re- Identity has been re- Identity has been re- Identity has been se Authentication state The server has reque Validating the server. Port state transition I The authentication p The following IP ado	onnection requested from us ication started using the logg to AC_PORT_STATE_UNAL ion started using encryption in on succeeded. to AC_PORT_STATE_CONN to AC_PORT_STATE_AUTH quested from the network. int to the network. ed using method type EAP-TL ested using authentication type sted using authentication type to AC_PORT_STATE_AUTH process has succeeded. tress has been assigned: 10.	er context. ed in user's credential JTHENTICATED(AC_ node AC_ENCR_AES IECTING(AC_PORT_ IENTICATING(AC_PO S, level 0 pe: EAP-TLS e: EAP-TLS HENTICATED(AC_PO 10.80.24.	* PORT_STATUS_STARTED) AC_ASSOC_11i_8021X STATUS_LINK_UP) JRT_STATUS_8021x_ACQUIRED
			Clear		

Cisco Secure Services Client	
Create Networks Manage Networks	
Network 🛆	Status Data :
E- Con Network	Disconnected
con	No Adapter Available (Suspended) 🛛 🗕 🕅
- 🐑 con-eap Network	Connected: Authenticated
L	Connected: Authenticated (AutoConnect) 🗃 🛝
•	•
	Details
Disconnect Configure	Remove Status

onnection Status	
onnection Details WiFi [Details
Status:	Connected: Authenticated
Duration:	00:01:19
Network Profile:	con-eap Network
Network Adapter:	Cisco 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 Addr	ess: 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
Help	Close

Comandi debug

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> 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 enableO
- 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