Unified Wireless Network Local EAP-Server -Konfigurationsbeispiel

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren des lokalen EAP auf dem Cisco Wireless LAN Controller Lokale EAP-Konfiguration Microsoft-Zertifizierungsstelle Installation Installieren des Zertifikats im Cisco Wireless LAN Controller Installieren Sie das Gerätezertifikat auf dem Wireless LAN-Controller. Laden Sie ein Zertifikat der Anbieterzertifizierungsstelle auf den Wireless LAN Controller herunter. Konfigurieren des Wireless LAN-Controllers für die Verwendung von EAP-TLS Installieren des Zertifikats der Zertifizierungsstelle auf dem Client-Gerät Herunterladen und Installieren eines Zertifikats der Stammzertifizierungsstelle für den Client Generieren eines Clientzertifikats für ein Clientgerät EAP-TLS mit Cisco Secure Services Client auf Client-Gerät Debugbefehle Zugehörige Informationen

Einleitung

Dieses Dokument beschreibt die Konfiguration eines lokalen EAP-Servers (Extensible Authentication Protocol) in einem Cisco Wireless LAN Controller (WLC) für die Authentifizierung von Wireless-Benutzern.

Lokaler EAP ist eine Authentifizierungsmethode, mit der Benutzer und Wireless-Clients lokal authentifiziert werden können. Sie ist für die Verwendung in Außenstellen ausgelegt, die die Verbindung zu Wireless-Clients aufrechterhalten möchten, wenn das Back-End-System ausfällt oder der externe Authentifizierungsserver ausfällt. Wenn Sie lokalen EAP aktivieren, fungiert der Controller als Authentifizierungsserver und als lokale Benutzerdatenbank. Dadurch entfällt die Abhängigkeit von einem externen Authentifizierungsserver. Der lokale EAP ruft Benutzeranmeldeinformationen aus der lokalen Benutzerdatenbank oder der Backend-Datenbank des Lightweight Directory Access Protocol (LDAP) ab, um Benutzer zu authentifizieren. Lokaler EAP unterstützt Lightweight EAP (LEAP), EAP-Flexible Authentifizierung zwischen Controller und Wireless Clients.

Beachten Sie, dass der lokale EAP-Server nicht verfügbar ist, wenn der WLC eine globale externe RADIUS-Serverkonfiguration enthält. Alle Authentifizierungsanforderungen werden an den globalen externen RADIUS weitergeleitet, bis der lokale EAP-Server verfügbar ist. Wenn der WLC die Verbindung zum externen RADIUS-Server verliert, wird der lokale EAP-Server aktiviert. Wenn keine globale RADIUS-Serverkonfiguration vorliegt, wird der lokale EAP-Server sofort aktiviert. Der lokale EAP-Server kann nicht zur Authentifizierung von Clients verwendet werden, die mit anderen WLCs verbunden sind. Anders ausgedrückt: Ein WLC kann seine EAP-Anforderung zur Authentifizierung nicht an einen anderen WLC weiterleiten. Jeder WLC muss über einen eigenen lokalen EAP-Server und eine eigene Datenbank verfügen.

Hinweis: Verwenden Sie diese Befehle, um zu verhindern, dass WLC Anfragen an einen externen Radius-Server sendet.

```
config wlan disable
config wlan radius_server auth disable
config wlan enable
Der lokalo EAP Server unterstützt diese Protokollo ab Version 4.1.171.0
```

Der lokale EAP-Server unterstützt diese Protokolle ab Version 4.1.171.0:

- LEBEN
- EAP-FAST (Benutzername/Kennwort und Zertifikate)
- EAP-TLS

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse der Konfiguration von WLCs und Lightweight Access Points (LAPs) für den Basisbetrieb
- Kenntnis der LWAPP- (Lightweight Access Point Protocol) und Wireless-Sicherheitsmethoden
- Grundkenntnisse der lokalen EAP-Authentifizierung.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Windows XP mit CB21AG Adapterkarte und Cisco Secure Services Client Version 4.05
- Cisco Wireless LAN Controller 4.1.171.0 der Serie 4400
- Microsoft-Zertifizierungsstelle für Windows 2000-Server

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions (Technische Tipps von Cisco zu Konventionen).</u>

Konfigurieren des lokalen EAP auf dem Cisco Wireless LAN

Controller

In diesem Dokument wird davon ausgegangen, dass die grundlegende Konfiguration des WLC bereits abgeschlossen ist.

Lokale EAP-Konfiguration

Gehen Sie wie folgt vor, um den lokalen EAP zu konfigurieren:

 Hinzufügen eines lokalen Netzbenutzers: Über die GUI. wählen Sie Security > Local Net Users > New aus, geben Sie den Benutzernamen, das Kennwort, den Gastbenutzer, die WLAN-ID und die Beschreibung ein, und klicken Sie auf

Apply.				Save Li	n n an	
CISCO	MONITOR WLANS C	ONTROLLER WIRELES	S <u>S</u> ECURITY		C <u>O</u> MMANDS	HELP
Security	Local Net Users > Ne	W		J	< Back	Apply
Ceneral	User Name	eapuser2				
 RADIUS Authentication Accounting 	Password	•••••				
▶ TACACS+ LDAP	Confirm Password	•••••				
MAC Filtering Disabled Clients	Guest User					
User Login Policies AP Policies	WLAN ID	1 💌				
Local EAP General	Description	Employee user local da	tabase			

Über die CLI können Sie den Befehl **config netuser add** *<username> <password> <WLAN ID> <description>* verwenden:Hinweis: Dieser Befehl wurde aus räumlichen Gründen auf eine zweite Zeile herabgesetzt.

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

2. Geben Sie die Bestellung zum Abrufen von Benutzeranmeldeinformationen an.Wählen Sie in der GUI Security > Local EAP > Authentication Priority (Sicherheit > Lokaler EAP > Authentifizierungspriorität). Wählen Sie dann LDAP aus, klicken Sie auf die Schaltfläche "<" und dann auf Übernehmen. Dadurch werden die Benutzeranmeldeinformationen zuerst in die lokale Datenbank eingegeben.</p>

ululu cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	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 HR				-
▼ Local EAP Profiles EAP-FAST Parameters Authentication Priority								

Uber die CLI:

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

EAP-Profil hinzufügen:Wählen Sie dazu in der GUI Security > Local EAP > Profiles
 (Sicherheit > Lokaler EAP > Profile) aus, und klicken Sie auf New (Neu). Wenn das neue
 Fenster angezeigt wird, geben Sie den Profilnamen ein, und klicken Sie auf
 Übernehmen.

	MONITOR	<u>W</u> LANs		WIREL	ESS SECU	rity Manu	AGEMENT	COMMANDS	HERb	 							
	Local EA	P Profiles											New	t		Apply	r
	Profile Na	me	u	AP	EAP-FAST	r	EAP-T	LS					1				
												/					
											/						
											/						
rs ty																	
												Say	e Confiqu	ration	Bing	Logout	Befre
MONE	for <u>w</u> lans	CONTROLLE	R WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP										
Loca	I EAP Profile	ts > New											1	< Back		App	ly
Profil	e Name				EAP-test												

Sie können dies auch mit dem CLI-Befehl **config local-auth eap-profile add** *profile-name> tun.* In unserem Beispiel lautet der Profilname *EAP-test.* (Cisco Controller) >**config local-auth eap-profile add** *EAP-test*

 4. Fügen Sie dem EAP-Profil eine Methode hinzu.Wählen Sie in der GUI Security > Local EAP
 > Profiles aus, und klicken Sie auf den Profilnamen, für den Sie die Authentifizierungsmethoden hinzufügen möchten. In diesem Beispiel werden LEAP, EAP-FAST und EAP-TLS verwendet. Klicken Sie auf Apply, um die Methoden festzulegen.



Sie können auch den CLI-Befehl **config local-auth eap-profile method add** *<method-name> <profile-name>* verwenden. In unserer Beispielkonfiguration fügen wir dem Profil-EAP-Test drei Methoden hinzu. Die Methoden sind LEAP, EAP-FAST und EAP-TLS, deren Methodennamen *Sprung, Fast* und *TLS* sind. Diese Ausgabe zeigt die CLI-Konfigurationsbefehle:

(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. Konfigurieren Sie die Parameter der EAP-Methode. Dies wird nur für EAP-FAST verwendet. Die zu konfigurierenden Parameter sind: Server Key (Server-Key) - Serverschlüssel zum Verschlüsseln/Entschlüsseln von PACs (Protected Access Credentials) (hexadezimal). Time to Live for PAC (pac-ttl): Legt die Zeit bis zum Live-Betrieb für die PAC fest. Authority ID (Authority-ID) (Autoritäts-ID) - Legt die Autoritätskennung fest. Annonymous Provivision (anon-provn): Konfiguriert, ob anonyme Rückstellungen zulässig sind. Dies ist standardmäßig aktiviert. Wählen Sie für die Konfiguration über die GUI Security > Local EAP > EAP-FAST Parameters (Sicherheit > Lokaler EAP > EAP-FAST-Parameter), und geben Sie den Serverschlüssel, Time to live für die PAC, Authority ID (in Hex) und Authority ID Information (Informationen zur Behörde-ID)

ein.		
MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COMMAND	YS HELP
EAP-FAST Method Parameters		
Server Key (in hex)	***	
Confirm Server Key		
Time to live for the PAC	10	days
Authority ID (in hex)	436	9736364
Authority ID Information	Cisc	ie A-ID
Anonymous Provision	R	Enabled

Dies sind die CLI-Konfigurationsbefehle zum Festlegen der folgenden Parameter für 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. Lokale Authentifizierung pro WLAN aktivieren:Wählen Sie in der GUI im oberen Menü WLANs aus, und wählen Sie das WLAN aus, für das Sie die lokale Authentifizierung konfigurieren möchten. Ein neues Fenster wird angezeigt. Klicken Sie auf die Registerkarten Security > AAA. Überprüfen Sie die lokale EAP-Authentifizierung, und wählen Sie im Pulldown-Menü den richtigen EAP-Profilnamen aus, wie in diesem Beispiel aczoigt:

,ı ı.ı ı. cısco	MONETOR 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	
	Radius Servers	LDAP Servers
	Authentication Servers Accounting Servers	Server 1 None K
	Server 1 None Server 2 None None Server 3 None Local EAP Authentication	Server 3 None 💌
	Local EAP Authentication 🖗 Enabled EAP Profile Name EAP-test 🗐	-

Sie können auch den Konfigurationsbefehl CLI config wlan local-auth enable *<profile-name> <wlan-id>* wie folgt ausgeben:

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

7. Legen Sie die Layer-2-Sicherheitsparameter fest.Gehen Sie in der GUI-Oberfläche im Fenster WLAN Edit (WLAN-Bearbeitung) zu den Registerkarten Security > Layer 2 und wählen Sie WPA+WPA2 aus dem Pulldown-Menü Layer 2 Security (Layer-2-Sicherheit). Legen Sie im Abschnitt WPA+WPA2-Parameter die WPA-Verschlüsselung auf TKIP und WPA2 Encryption AES fest. Klicken Sie anschließend auf Übernehmen.



Number of Active Clients..... 0 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 - Aironetle Support..... Enabled CCX - Gratuitous ProbeResponse (GPR)..... Disabled Dot11-Phone Mode (7920)..... Disabled Wired Protocol..... None --More-- or (q)uit IPv6 Support..... Disabled Radio Policy..... All Local EAP Authentication..... Enabled (Profile 'EAP-test') Security 802.11 Authentication:..... Open System Static WEP Keys..... Disabled 802.1X..... Disabled Wi-Fi Protected Access (WPA/WPA2)..... Enabled WPA (SSN IE)..... Enabled TKIP Cipher..... Enabled AES Cipher..... Disabled WPA2 (RSN IE)..... Enabled TKIP Cipher..... Disabled AES Cipher..... Enabled Auth Key Management 802.1x.... Enabled PSK..... Disabled CCKM..... Disabled CKIP Disabled IP Security..... Disabled IP Security Passthru..... Disabled Web Based Authentication..... Disabled --More-- or (q)uit Web-Passthrough..... Disabled Conditional Web Redirect..... Disabled Auto Anchor..... Disabled Cranite Passthru..... Disabled Fortress Passthru..... Disabled H-REAP Local Switching..... Disabled Infrastructure MFP protection..... Enabled (Global Infrastructure MFP Disabled) Client MFP..... Optional Tkip MIC Countermeasure Hold-down Timer..... 60

Mobility Anchor List WLAN ID IP Address

Status

Es gibt weitere lokale Authentifizierungsparameter, die konfiguriert werden können, insbesondere den aktiven Timeout-Timer. Dieser Timer konfiguriert den Zeitraum, in dem lokales EAP verwendet wird, nachdem alle RADIUS-Server ausgefallen sind.Wählen Sie in der GUI Security > Local EAP > General (Sicherheit > Lokaler EAP > Allgemein) aus, und legen Sie den Zeitwert fest. Klicken Sie anschließend auf Übernehmen.



Führen Sie über die CLI die folgenden Befehle aus:

```
(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
```

Sie können den Wert, für den dieser Timer eingerichtet ist, überprüfen, wenn Sie den Befehl show local-auth config ausführen.

(Cisco Controller) >show local-auth config

9. Wenn Sie die manuelle PAC erstellen und laden müssen, können Sie entweder die GUI oder die CLI verwenden.Wählen Sie in der GUI COMMANDS im oberen Menü aus und wählen Sie Upload File aus der Liste rechts. Wählen Sie PAC (Protected Access Credential) aus dem Dropdown-Menü Dateityp aus. Geben Sie alle Parameter ein und klicken Sie auf Hochladen.

ահահո							Sa⊻e Configur	ation <u>P</u> ing	Logout <u>R</u> efres	
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	COMMANDS	не <u>г</u> р		
Commands	Upload file	e from C	Controller					Clear	Upload	
Download File	File Type			PAC (Protect	ed Access Crea	dential) 💌				
Reboot	User (Identity)			test1	test1					
Reset to Factory Default Set Time	Validity (in days)			60						
	Password			•••••						
	Confirm Pa	nssword		•••••						
	TETP Serve	ər								
	IP Address	5		10.1.1.1						
	File Path			/						
	File Name			manual.pac						

Geben Sie in der CLI die folgenden Befehle ein:

(Cisco Controller) >transfer upload datatype pac (Cisco Controller) >transfer upload pac ? Enter the user (identity) of the PAC username (Cisco Controller) >transfer upload pac test1 ? Enter the PAC validity period (days) <validity> (Cisco Controller) >transfer upload pac test1 60 ? Enter a password to protect the PAC <password> (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..... ciscol23 Are you sure you want to start? (y/N) ${\rm y}$ PAC transfer starting. File transfer operation completed successfully.

Microsoft-Zertifizierungsstelle

Um die EAP-FAST Version 2 und die EAP-TLS-Authentifizierung zu verwenden, müssen der WLC und alle Client-Geräte über ein gültiges Zertifikat verfügen und das öffentliche Zertifikat der Zertifizierungsstelle kennen.

Installation

Wenn auf dem Windows 2000-Server noch keine Zertifizierungsstellen installiert sind, müssen Sie diese installieren.

Gehen Sie wie folgt vor, um die Microsoft Certification Authority auf einem Windows 2000-Server zu aktivieren:

1. Wählen Sie in der Systemsteuerung Software aus.



2. Wählen Sie links Windows-Komponenten hinzufügen/entfernen



3. Aktivieren Sie **Zertifizierungsdienste**.

You can add or remove components of Windows 2000. To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, clic Details. Components: Image: Certificate Services Image: Cerificate Services Imag	ndows Components				
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, clic Details. Components: Components: Cettificate Services 12.1 MB Cettificate Services 14.4 MB Components 12.1 MB 14.4 MB	You can add or remove comp	onents of Windows 2	2000.		4
Components: I2.1 MB Image: Certificate Services 1.4 MB Image: Certificate Services 0.0 MB Image: Internet Information Services (IIS) 21.6 MB Image: Internet Information Services (IIS) 52 MB Description: Installs a certification authority (CA) to issue certificates for use with public key security applications. 52 MB Total disk space required: 0.0 MB Details Space available on disk: 4205.9 MB Image: Imag	To add or remove a componer part of the component will be in Details.	nt, click the checkbo nstalled. To see wh	ox. A shaded at's included	l box means that in a component,	only click
Image: Certificate Services 1.4 MB Image: Certificate Services 0.0 MB Image: Internet Information Services (IIS) 21.6 MB Image: Internet Information Services (IIS) 20.0 MB Image: Internet Information Services (IIS) 0.0 MB Image: Internet Information Services (IIS) 0.0 MB Image: Internet Information Services (IIS)	Components:				
Image: Certificate Services 1.4 MB Image: Internet Information Services (IIS) 21.6 MB Image: Internet Information Services (IIS) 21.6 MB Image: Internet Information Services (IIS) 52 MB Description: Installs a certification authority (CA) to issue certificates for use with public key security applications. Total disk space required: 0.0 MB Space available on disk: 4205.9 MB Image:	🗷 📻 Accessories and Utiliti	es		12.1 M	B 🔺
Internet Information Services (IIS) Internet Information Services (IIS) Internet Information Services (IIS) Management and Monitoring Tools Source Services (IIS) Source Servic	📑 😫 Certificate Services			1.4 M	в
Internet Information Services (IIS) 21.6 MB Management and Monitoring Tools 5.2 MB Description: Installs a certification authority (CA) to issue certificates for use with public key security applications. Total disk space required: 0.0 MB Space available on disk: 4205.9 MB Qetails Utern Sie diese Warnung, bevor Sie	Indexing Service			0.0 M	В
Image: Management and Monitoring Tools 5.2 MB Description: Installs a certification authority (CA) to issue certificates for use with public key security applications. Total disk space required: 0.0 MB Space available on disk: 4205.9 MB Image: Certification of the security of the secure of the securety of the security of the secu	Mainternet Information Se	ervices (IIS)		21.6 M	в
Description: Installs a certification authority (CA) to issue certificates for use with public key security applications. Total disk space required: 0.0 MB Details Space available on disk: 4205.9 MB < Back	Management and Mor	aloo Tools		5.2 M	R 💌
Total disk space required: 0.0 MB Space available on disk: 4205.9 MB < Back	Description: Installs a certifica public key securi	ation authority (CA) to ity applications.	o issue certific	cates for use with	t.
Space available on disk: 4205.9 MB	Total disk space required:	0.0 MB		Detai	h
<u>k Back</u> <u>Next</u> > üfen Sie diese Warnung, bevor Sie	Space available on disk:	4205.9 MB			5
üfen Sie diese Warnung, bevor Sie en		<	<u>B</u> ack	<u>N</u> ext >	Can
en.	ifen Sie diese Warnung, be	vor Sie			
	en:				

		· · · · · · · · · · · · · · · · · · ·	
⚠	After installing Certificate Services, the co from a domain. Do you want to continue?	mputer cannot be renamed and	I the computer cannot join or be removed
		Yes No	

4. Wählen Sie die Zertifizierungsstelle aus, die Sie installieren möchten. Um eine einfache eigenständige Autorität zu erstellen, wählen Sie die **eigenständige Stammzertifizierungsstelle aus**.

There are rour types of certification author	nico.	
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.	4
Advanced options		

5. Geben Sie die erforderlichen Informationen zur Zertifizierungsstelle ein. Mit diesen Informationen wird ein selbstsigniertes Zertifikat für Ihre Zertifizierungsstelle erstellt. Beachten Sie den Namen der CA, den Sie verwenden.Die Zertifizierungsstelle speichert die Zertifikate in einer Datenbank. In diesem Beispiel wird die von Microsoft vorgeschlagene Standardeinrichtung verwendet:

Certificate database:		
C:\WINNT\system32\CertLog		Browse
Certificate database log:		
C:\WINNT\system32\CertLog		Bro <u>w</u> se
Store configuration information	No a shared folder	
Store configuration information Shared folder:	n 🏹 a shared folder	Biowse
Store configuration information Shared folder:	n 泽 a shared folder	BIowse

 Microsoft Certification Authority-Dienste verwenden den IIS Microsoft Web Server, um Clientund Serverzertifikate zu erstellen und zu verwalten. Der IIS-Dienst muss f
ür diesen Vorgang neu gestartet worden:

Microsoft	t Certificate Services
⚠	Internet Information Services is running on this computer. You must stop this service before proceeding. Do you want to stop the service now?
	OK Cancel

Der Microsoft Windows 2000 Server installiert den neuen Dienst jetzt. Sie benötigen Ihre Windows 2000 Server-Installations-CD, um neue Windows-Komponenten installieren zu können.Die Zertifizierungsstelle ist jetzt installiert.

Installieren des Zertifikats im Cisco Wireless LAN Controller

Um EAP-FAST Version 2 und EAP-TLS auf dem lokalen EAP-Server eines Cisco Wireless LAN Controllers zu verwenden, gehen Sie wie folgt vor:

- 1. Installieren Sie das Gerätezertifikat auf dem Wireless LAN Controller.
- 2. Laden Sie ein Zertifikat der Anbieterzertifizierungsstelle auf den Wireless LAN Controller herunter.
- 3. Konfigurieren Sie den Wireless LAN Controller für die Verwendung von EAP-TLS.

Beachten Sie, dass im Beispiel in diesem Dokument der Access Control Server (ACS) auf demselben Host wie Microsoft Active Directory und die Microsoft Certification Authority installiert ist. Die Konfiguration sollte jedoch identisch sein, wenn sich der ACS-Server auf einem anderen

Server befindet.

Installieren Sie das Gerätezertifikat auf dem Wireless LAN-Controller.

Führen Sie diese Schritte aus:

- 1. . Gehen Sie wie folgt vor, um das Zertifikat für den Import in den WLC zu generieren:Gehen Sie zu http://<serverlpAddr>/certsrv.Wählen Sie Zertifikat anfordern aus, und klicken Sie auf Weiter.Wählen Sie Erweiterte Anforderung aus, und klicken Sie auf Weiter.Wählen Sie eine Zertifikatsanforderung an diese Zertifizierungsstelle mithilfe eines Formulars senden aus, und klicken Sie auf Weiter.Wählen Sie Webserver für Zertifikatsvorlage aus, und geben Sie die entsprechenden Informationen ein. Markieren Sie dann die Tasten als exportierbar.Sie erhalten nun ein Zertifikat, das Sie auf Ihrem Computer installieren müssen.
- 2. Gehen Sie wie folgt vor, um das Zertifikat vom PC abzurufen:Öffnen Sie einen Internet Explorer-Browser, und wählen Sie Extras > Internetoptionen > Inhalt aus.Klicken Sie auf Zertifikate.Wählen Sie das neu installierte Zertifikat aus dem Dropdown-Menü aus.Klicken Sie auf Exportieren.Klicken Sie zweimal auf Weiter und wählen Sie Yes export the private key (Privater Schlüssel exportieren). Dieses Format ist PKCS#12 (PFX-Format).Wählen Sie Starken Schutz aktivieren aus.Geben Sie ein Kennwort ein.Speichern Sie die Datei in einer Datei <tme2.pfx>.
- 3. Kopieren Sie das Zertifikat im PKCS#12-Format auf einen Computer, auf dem Sie OpenSSL installiert haben, um es in das PEM-Format zu konvertieren.

!--- 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. Laden Sie das konvertierte Gerätezertifikat im PEM-Format auf den WLC herunter. (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.....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. Überprüfen Sie nach dem Neustart das Zertifikat. (Cisco Controller) >show local-auth certificates

Certificates available for Local EAP authentication:

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=tme 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

Laden Sie ein Zertifikat der Anbieterzertifizierungsstelle auf den Wireless LAN Controller herunter.

Führen Sie diese Schritte aus:

- Gehen Sie wie folgt vor, um das Zertifizierungsstellenzertifikat des Anbieters abzurufen:Gehen Sie zu http://<serverlpAddr>/certsrv.Wählen Sie Zertifikat abrufen aus, und klicken Sie auf Weiter.Wählen Sie das CA-Zertifikat aus.Klicken Sie auf DER codiert.Klicken Sie auf Zertifizierungsstellenzertifikat herunterladen und speichern Sie das Zertifikat als rootca.cer.
- Konvertieren Sie die Anbieter-CA aus dem DER-Format in das PEM-Format mit dem Befehl openssl x509 -in rootca.cer -notify DER -out rootca.pem -out PEM.Die Ausgabedatei ist rootca.pem im PEM-Format.
- 3. Laden Sie das Zertifizierungsstellenzertifikat des Anbieters herunter: (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 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.

Konfigurieren des Wireless LAN-Controllers für die Verwendung von EAP-TLS

Führen Sie diese Schritte aus:

Wählen Sie in der GUI **Security > Local EAP > Profiles**, wählen Sie das Profil aus, und prüfen Sie, ob diese Einstellungen vorhanden sind:

- Lokales Zertifikat erforderlich ist aktiviert.
- Client-Zertifikat erforderlich ist aktiviert.
- Zertifikataussteller ist Anbieter.
- Der Abgleich mit Zertifizierungsstellenzertifikaten ist aktiviert.

ı. cısco	MONITOR MLANI CONTROLLER WIRELESS S	ECURITY MANAGEMENT COMMANDS HELP
Security	Local EAP Profiles > Edit	
* AAA General	Profile Name	EAP-test
■ RADBUS Authentication	LEAP	P
* TACACS+ LDAP	EAP-FAST	P
Local Net Users MAC Filtering	EAP-TLS	P
User Login Policies AP Policies	Local Certificate Required	E Enabled
* Local EAP General	Client Certificate Required	R Enabled
Profiles EAP-FAST Parameters	Certificate Issuer	Vendor 🗵
Priority Order	Check against CA certificates	P Enabled
▶ Access Control Lists	Verify Certificate CN Identity	C Enabled
IPSec Certs Wireless Protection Policies	Check Certificate Date Validity	C trabled

Installieren des Zertifikats der Zertifizierungsstelle auf dem Client-Gerät

Herunterladen und Installieren eines Zertifikats der Stammzertifizierungsstelle für den Client

Der Client muss ein Root-Zertifizierungsstellenzertifikat von einem Zertifizierungsstellen-Server beziehen. Es gibt mehrere Methoden, mit denen Sie ein Clientzertifikat abrufen und auf dem Windows XP-Computer installieren können. Um ein gültiges Zertifikat zu erhalten, muss der Windows XP-Benutzer mit seiner Benutzer-ID angemeldet sein und über eine Netzwerkverbindung verfügen.

Ein Webbrowser auf dem Windows XP-Client und eine kabelgebundene Verbindung zum Netzwerk wurden verwendet, um ein Client-Zertifikat vom privaten Root Certification Authority-Server zu erhalten. Dieses Verfahren wird verwendet, um das Clientzertifikat von einem Microsoft Certification Authority-Server zu erhalten:

- 1. Verwenden Sie einen Webbrowser auf dem Client, und verweisen Sie den Browser auf den Zertifizierungsstellen-Server. Geben Sie dazu http://IP-address-of-Root-CA/certsrv ein.
- 2. Melden Sie sich mit **Domain_Name\user_name an**. Sie müssen sich mit dem Benutzernamen der Person anmelden, die den XP-Client verwenden soll.
- 3. Wählen Sie im Welcome-Fenster die Option **Retrieve a CA certificate (Zertifikat der Zertifizierungsstelle abrufen) aus,** und klicken Sie auf **Next (Weiter)**.
- 4. Wählen Sie Base64 Encoding und Download CA Certificate aus.
- 5. Klicken Sie im Fenster Zertifikat ausgegeben auf **Dieses Zertifikat installieren** und dann auf **Weiter**.
- 6. Wählen Sie Automatisch den Zertifikatsspeicher aus, und klicken Sie auf Weiter, um eine erfolgreiche Importmeldung zu erhalten.

7. Stellen Sie eine Verbindung zur Zertifizierungsstelle her, um das Zertifikat der Zertifizierungsstelle

abzurufen:

Microsoft Certificate Service	is – trie Her
Velcome	
ou use this web site to fill be able to securely in lepending upon the type	request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you dentify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more e of certificate you request.
Relect a task: Retrieve the CA can Request a certification Check on a pendir	ertificate or certificate revocation list ate ng certificate
	Next >
Miemona Carlifesta Sanies	ao _ teora
Microsoft Certificate Service	es – tme Har
Microsoft Certificate Service Retrieve The CA Certif	es – tme Hor ficate Or Certificate Revocation List
Microsoft Certificate Service Retrieve The CA Certif Install this CA certification	ticate Or Certificate Revocation List
Microsoft Certificate Service Retrieve The CA Certification Install this CA certification is not necessary to mai CA certification path will	Iter - tme Here Ricate Or Certificate Revocation List In path to allow your computer to trust certificates issued from this certification authority. nually install the CA certification path if you request and install a certificate from this certification authority, because the be installed for you automatically.
Microsoft Certificate Senic Retrieve The CA Certification Install this CA certification is not necessary to ma CA certification path will Choose file to downlo CA Certificate:	tion path to allow your computer to trust certificates issued from this certification authority. nually install the CA certification path if you request and install a certificate from this certification authority, because th be installed for you automatically. ad: me
Wicrosoft Certificate Service Retrieve The CA Certification Install this CA certification is not necessary to ma CA certification path will Choose file to downlo CA Certificate:	Har Har Ricate Or Certificate Revocation List In path to allow your computer to trust certificates issued from this certification authority. nually install the CA certification path if you request and install a certificate from this certification authority, because the be installed for you automatically. ad: meetered encoded Or Or Base 64 encoded
Microsoft Certificate Service Retrieve The CA Certification Install this CA certification t is not necessary to ma CA certification path will Choose file to downlo CA Certificate:	Iter Iter Incate Or Certificate Revocation List Iter In path to allow your computer to trust certificates issued from this certification authority. Iter nually install the CA certification path if you request and install a certificate from this certification authority, because the be installed for you automatically. Iter ad: Iter Iter encoded or O Base 64 encoded Iter Iter id CA certificate Iter Iter

8. Klicken Sie auf Zertifizierungsstellenzertifikat

herunterladen.

Microsoft Certificate Services tme Hon						
Retrieve The CA Certificate Or Certificate Revocation List						
Install this CA certification path to allow your	computer to trust certificates issued from this certification	authority.				
It is not necessary to manually install the CA	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 [tmo]	Name: certnew.cer Type: Security Certificate, 798 bytes From: 10.1.1.12					
⊙DER encoded or ○Ba	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. What's the risk?					

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. Um zu überprüfen, ob das Zertifikat der Zertifizierungsstelle korrekt installiert ist, öffnen Sie Internet Explorer und wählen Extras > Internetoptionen > Inhalt > Zertifikate



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 AutoComplete AutoComplete
Microsoft Profile Assistant stores your My Profile
OK Cancel Apply

In der Trusted Root Certification Authority sollten Sie Ihre neu installierte Zertifizierungsstelle sehen:

Issued To	Issued	Ву	Expiratio	Friendly N	Name
🔤 Thawte Server	CA Thawte	Server CA	12/31/2020	Thawte Se	erver CA
Thawte Timesta	mpi Thawte	Timestamping	12/31/2020	Thawte Ti	imesta
tme	tme		2/28/2012	<none></none>	
UTN - DATACon	p SGC UTN - D	ATACorp SGC	6/24/2019	UTN - DAT	TACorp
UTN-USERFirst-	Clie UTN-USI	ERFirst-Client	7/9/2019	UTN - USE	RFirst
UTN-USERFirst-	Har UTN-US	ERFirst-Hardw	7/9/2019	UTN - USE	ERFirst
UTN-USERFirst-	Net UTN-US	ERFirst-Netwo	7/9/2019	UTN - USE	RFirst
UTN-USERFirst-	Obj UTN-USI	ERFirst-Object	7/9/2019	UTN - USE	RFirst
VeriSign Comme	rcia VeriSign	Commercial S	12/31/1999	VeriSign C	iommer
Import Ex	port R	emove			Advance
		Centove			Marano
ertificate intended p	ourposes				

Generieren eines Clientzertifikats für ein Clientgerät

Der Client muss ein Zertifikat von einem Zertifizierungsstellen-Server für den WLC erhalten, um einen WLAN EAP-TLS-Client zu authentifizieren. Es gibt mehrere Methoden, mit denen Sie ein Clientzertifikat abrufen und auf dem Windows XP-Computer installieren können. Um ein gültiges Zertifikat zu erwerben, muss der Windows XP-Benutzer mit seiner Benutzer-ID angemeldet sein und über eine Netzwerkverbindung verfügen (entweder eine kabelgebundene Verbindung oder eine WLAN-Verbindung mit 802.1x-Sicherheit deaktiviert).

Ein Webbrowser auf dem Windows XP-Client und eine kabelgebundene Verbindung zum Netzwerk werden verwendet, um ein Client-Zertifikat vom privaten Root Certification Authority-Server zu erhalten. Dieses Verfahren wird verwendet, um das Clientzertifikat von einem Microsoft Certification Authority-Server zu erhalten:

- 1. Verwenden Sie einen Webbrowser auf dem Client, und verweisen Sie den Browser auf den Zertifizierungsstellen-Server. Geben Sie dazu **http://IP-address-of-Root-CA/certsrv** ein.
- 2. Melden Sie sich mit **Domain_Name\user_name an**. Sie müssen sich mit dem Benutzernamen der Person anmelden, die den XP-Client verwendet. (Der Benutzername wird in das Clientzertifikat eingebettet.)
- 3. Wählen Sie im Willkommensfenster Zertifikat anfordern aus und klicken Sie auf Weiter.
- 4. Wählen Sie Erweiterte Anforderung aus, und klicken Sie auf Weiter.

- 5. Wählen Sie eine Zertifikatsanforderung an diese Zertifizierungsstelle mithilfe eines Formulars senden aus, und klicken Sie auf Weiter.
- 6. Wählen Sie im Formular Erweiterte Zertifikatsanforderung die Zertifikatsvorlage als **Benutzer aus**, geben Sie die Schlüsselgröße als **1024** an, und klicken Sie auf **Senden**.
- Klicken Sie im Fenster Zertifikat ausgegeben auf Dieses Zertifikat installieren. Dies führt zur erfolgreichen Installation eines Clientzertifikats auf dem Windows XP-Client.

Client.
Microsoft Certificate Services true Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task: O Retrieve the CA certificate or certificate revocation list O Request a certificate O Check on a pending certificate
Next >
Microsoft Certificate Services tme Hom
Choose Request Type
Please select the type of request you would like to make:
User certificate request
 Advanced request
Next >
Microsoft Certificate Services Ime
Advanced Certificate Requests
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.
Submit a certificate request to this CA using a form.
Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
 Desurate a cartificate for a smart card on babalf of another user using the Smart Card Excellment Station

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. Wählen Sie Client Authentication Certificate

Certificate Temp	late:
	User
Key Options:	
CSP:	Microsoft Base Cryptographic Provider v1.0
Key Usage:	○Exchange ○Signature ④Both
Key Size:	512 Min: 384 (common key sizes: 512 1024) Max: 1024
	Oreate new key set
	Set the container name
	Enable strong private key protection
	Made keye as expectable
	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
	× 1
Attributeo:	

Clientzertifikat wurde jetzt erstellt.

9. Um zu überprüfen, ob das Zertifikat installiert ist, gehen Sie zu Internet Explorer, und wählen Sie Extras > Internetoptionen > Inhalt > Zertifikate aus. Auf der Registerkarte Personal sollte das Zertifikat angezeigt

werden.

Certificates				?	×
Intended purpo	ose:	<all></all>			*
Personal Ot	her Peopl	e Intermediate Certificat	ion Authorities Truste	ed Root Certification 🔨	>
Issued To		Issued By	Expiratio	Friendly Name	
Adminis	trator	tme	3/27/2008 <	<none></none>	
Import Certificate int Encrypting Fil	Expo tended pu le System,	ort Remove rposes , Secure Email, Client Auth	entication	Advanced View	
				Close	

EAP-TLS mit Cisco Secure Services Client auf Client-Gerät

Führen Sie diese Schritte aus:

- 1. Der WLC sendet die SSID standardmäßig, sodass sie in der Liste "Create Networks" (Netzwerke erstellen) der gescannten SSIDs angezeigt wird. Um ein Netzwerkprofil zu erstellen, können Sie auf die SSID in der Liste (Enterprise) klicken und auf Netzwerk erstellen. Wenn die WLAN-Infrastruktur so konfiguriert ist, dass die Broadcast-SSID deaktiviert ist, müssen Sie die SSID manuell hinzufügen. Klicken Sie dazu unter Zugriffsgeräte auf Hinzufügen und geben Sie manuell die entsprechende SSID ein (z. B. Enterprise). Konfigurieren Sie das aktive Testverhalten für den Client. In diesem Fall sucht der Client aktiv nach seiner konfigurierten SSID. Geben Sie Aktiv nach diesem Zugriffsgerät suchen an, nachdem Sie die SSID im Fenster Zugriffsgerät hinzufügen eingegeben haben.Hinweis: Die Porteinstellungen lassen keine Enterprise-Modi (802.1X) zu, wenn die EAP-Authentifizierungseinstellungen nicht zuerst für das Profil konfiguriert wurden.
- 2. Klicken Sie auf **Create Network (Netzwerk erstellen**), um das Fenster Network Profile (Netzwerkprofil) zu öffnen, in dem Sie die ausgewählte (oder konfigurierte) SSID einem Authentifizierungsmechanismus zuordnen können. Weisen Sie dem Profil einen

beschreibenden Namen zu. **Hinweis:** Mehrere WLAN-Sicherheitstypen und/oder SSIDs können diesem Authentifizierungsprofil zugeordnet

werden.

ACC	xess 🛆	Dat	a Security	
ăll 0.1	aruba-ap-config-in-the-clear (2 accesses dete	1	WEP	
àЦ о.т		<u>×</u>	Upen	
ăll	ccx5 [2 accesses detected]	Ä	Upen	
ăl.	con	×	Open	
al	001907351aa3 High Signal	<u>"</u>	WEP	
ål	guestnet (5 accesses detected)	X	Open	
зII	guestnetwork	X	Open	
11	N-Rogue	2	WEP	
21	secure-1 (3 accesses detected)	?8	Mixed	
ål.	tme-test (5 accesses detected)	8	WPA	
21	trng1 (2 accesses detected)	2	WEP	

- 3. Aktivieren Sie die Authentifizierung, und überprüfen Sie die EAP-TLS-Methode. Klicken Sie anschließend auf Konfigurieren, um die EAP-TLS-Eigenschaften zu konfigurieren.
- 4. Klicken Sie unter "Übersicht über die Netzwerkkonfiguration" auf Ändern, um die EAP-/Anmeldeinformationseinstellungen zu konfigurieren.
- 5. Geben Sie **Authentifizierung einschalten**, wählen Sie **EAP-TLS** unter Protokoll aus, und wählen Sie **Benutzername** als Identität aus.
- 6. Geben Sie Single Sign on Credentials (Single-Sign-on-Anmeldeinformationen verwenden, um Anmeldeinformationen f
 ür die Netzwerkauthentifizierung zu verwenden. Klicken Sie auf Konfigurieren, um EAP-TLS-Parameter einzurichten.

Network Authentication	×
Network Authentication Network: con-eap Network Authentication Methods:	User Credentials: C Use Machine Credentials Use Single Sign on Credentials Request when needed Remember forever Remember for this session Remember for 5 minutes
EAP-TLS FAST GTC Configure	
Help	OK Cancel

Network Profile	-				×		
Network							
Name: con-eap	Name: con-eap Network						
🔽 Ava	Available to all users (public profile)						
T Auto	Automatically establish Machine connection						
🔽 Auto	matically establish l	Jser connec	tion				
l.	Before user acco	unt (support	s smartcard	/password only)			
-Network Configu	ation Summary:						
Authentication	EAP-TLS:				٦		
Cradanijale	Request when pe	adad and ra	mambar for	the session	-		
Credenidais.	Inequest when he	eded and le	member for	une session.			
				Modify]		
Access / SSID	Mode	Notes			-		
con-eap	WPA2 Enterpr	ise			-		
1	1		1				
Add	Modify	Configuratio	n	Remove			
Hab		ſ	OK	Cancel	1		
neip		_	UK				

7. Um eine gesicherte EAP-TLS-Konfiguration zu erhalten, müssen Sie das RADIUS-Serverzertifikat überprüfen. Aktivieren Sie dazu die Option **Serverzertifikat** validieren.

Configure EAP Metho	d	×
-EAP-TLS settings:		
Use Smartcard-base	d Client Certificates Only	
🔽 Validate Server Certi	ficate	
Allow Fast Session R	lesumption	
Help	ПК	Cancel
		Canoor

 Um das RADIUS-Serverzertifikat zu validieren, müssen Sie den Cisco Secure Services Client angeben, damit nur das richtige Zertifikat akzeptiert werden kann. Wählen Sie Client > Trusted Servers (Client > vertrauenswürdige Server) > Manage Current User Trusted Servers (Aktuelle vertrauenswürdige Server verwalten).

Cisco Secure Services	Client	
Client Administration Help		
Manage Adapters	hatuatia	
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 (AutoCo	nnect) 🙉 WP4
 Show System Tray 	Capable for: wep	
Close Window	Configured for: wpa2	
Connec	t Configure Remove Status	Details
Mapage Current User	Trusted Servers	
Trusted Server Definition	Current Users:	A
Bule Name	Validation Me	thod
Add Server Bule	Bemove Selected	Selected
Help		Close

9. Geben Sie einen Namen für die Regel ein, und überprüfen Sie den Namen des

Serverzertifikats.

		2
Trusted Server		
Rule name: WLC-Config		
Validation method: Certificate		•
Match ANY Certificate Validation Rule: Subject Alternative Name Exactly matches	<u> </u>	
Subject/Common Name Exactly matches	tme	

Die EAP-TLS-Konfiguration ist abgeschlossen.

10. Stellen Sie eine Verbindung zum Wireless-Netzwerkprofil her. Der Cisco Secure Services Client bittet um

Anmeldung:	

Cisco Secure Services Client Client Administration Help	
Create Networks Manage Network	Credentials Please enter your credentials for network con-eap Network, access con-eap Username: Administrator Send Cancel
Connect	Details Configure Remove Status

er Cisco Secure Services Client empfängt das Serverzertifikat und überprüft es (mit konfigurierter Regel und installierter Zertifizierungsstelle). Anschließend wird die Verwendung des Zertifikats für den Benutzer angefordert.

11. Nachdem der Client sich authentifiziert hat, wählen Sie auf der Registerkarte "Netzwerke verwalten" unter SSID aus, und klicken Sie auf Status, um Verbindungsdetails abzufragen.Das Fenster Verbindungsdetails enthält Informationen zum Client-Gerät, zum Verbindungsstatus, zu Statistiken und zur Authentifizierungsmethode. Die Registerkarte WiFi Details enthält Details zum Verbindungsstatus für 802.11, einschließlich RSSI, 802.11-Kanal sowie

×

Authentifizierung/Verschlüsselung.

Information...

Selected Acce	888	Status	Security
con-eap		Connected: Authenticated (AutoC	onn WPA2
11:24:28.044 11:24:28.054 11:24:28.074 11:24:28.094 11:24:28.104 11:24:28.194 11:24:28.305 11:24:28.305 11:24:28.335 11:24:28.335 11:24:28.335 11:24:28.395 11:24:28.505 11:24:28.505 11:24:35.534	con-eap Network Con Connection authentical Port state transition to A Connection association Port state transition to A Port state transition to A Identity has been reque Identity has been reque Identity has been sent to Authentication started o The server has request Validating the server. Port state transition to A The authentication proo The following IP addres	nection requested from user context ion started using the logged in user IC_PORT_STATE_UNAUTHENTIC started using encryption mode AC_1 succeeded. IC_PORT_STATE_CONNECTING IC_PORT_STATE_AUTHENTICAT isted from the network. Ising method type EAP-TLS, level 0 ed using authentication type: EAP-1 id using authentication type: EAP-1 IC_PORT_STATE_AUTHENTICAT tests has succeeded. Is has been assigned: 10.10.80.24.	t 's credentials. CATED(AC_PORT_STATUS_STARTED) ENCR_AES AC_ASSOC_11i_8021X (AC_PORT_STATUS_LINK_UP) TING(AC_PORT_STATUS_8021x_ACQUIRED)) TLS TLS TED(AC_PORT_STATUS_GROUP_KEY)
		Clear	
			Close

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 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

Debugbefehle

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie <u>vor der</u> Verwendung von **Debug-**Befehlen die <u>Informationen</u> zu <u>Debug-</u><u>Befehlen</u>.

Diese Debug-Befehle können am WLC verwendet werden, um den Fortschritt des Authentifizierungsaustauschs zu überwachen:

- debug aaa events enable
- debuggen aaa detail enable
- debug dot1x-Ereignisse aktivieren

- debug dot1x status enable
- debuaa local-auth eap events enableODER
- debug aaa all enable

Zugehörige Informationen

- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.1
- Unterstützung von WLAN-Technologie
- Technischer Support und Dokumentation für Cisco Systeme