Configuratievoorbeeld voor Unified Wireless Network Local EAP-server

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten **Conventies** Local EAP op Cisco draadloze LAN-controller configureren Local EAP-configuratie Microsoft certificeringsinstantie Installatie Installeer het certificaat in de Cisco draadloze LAN-controller Installeer het apparaatcertificaat op de draadloze LAN-controller Download een leveranciercertificaat aan de draadloze LAN-controller Configureer de draadloze LAN-controller voor het gebruik van EAP-TLS Installeer het certificaatcertificaat op het clientapparaat. Download en Installeer een Root CA-certificaat voor de client Een clientcertificaat genereren voor een clientapparaat EAP-TLS met Cisco Secure Services-client op het clientapparaat Opdrachten debug Gerelateerde informatie

Inleiding

Dit document beschrijft de configuratie van een lokale MAP-server (Extensible Authentication Protocol) in een Cisco Wireless LAN Controller (WLC) voor de verificatie van draadloze gebruikers.

Plaatselijke MAP is een authenticatiemethode die het mogelijk maakt dat gebruikers en draadloze klanten lokaal worden geauthentiseerd. Het is ontworpen voor gebruik in afgelegen kantoren die verbindingen willen onderhouden met draadloze klanten wanneer het back-end systeem verstoord raakt of de externe authenticatieserver daalt. Wanneer u lokale EAP toelaat, dient de controller als de authenticatieserver en de lokale gebruikersdatabase, waarmee de afhankelijkheid van een externe verificatieserver wordt verwijderd. Plaatselijke MAP haalt gebruikersaanmeldingsgegevens uit de lokale gebruikersdatabase of de Lichtgewicht Directory Access Protocol (LDAP) back-end database om gebruikers echt te maken. Lokale EAP ondersteunt lichtgewicht EAP (LEAP), EAP-Flexibele verificatie via Secure Tunneling (EAP-FAST) en EAP-Transport Layer Security (EAP-TLS)-verificatie tussen de controller en draadloze klanten.

Merk op dat de lokale EAP-server niet beschikbaar is als er een globale externe RADIUS-

serverconfiguratie in de WLC is. Alle verificatieverzoeken worden naar de globale externe RADIUS doorgestuurd totdat de lokale MAP-server beschikbaar is. Als de WLC de connectiviteit op de externe RADIUS-server verliest, wordt de lokale EAP-server actief. Als er geen algemene RADIUS-serverconfiguratie is, wordt de lokale EAP-server onmiddellijk actief. De lokale EAPserver kan niet gebruikt worden om cliënten te authentiseren, die verbonden zijn met andere WLC's. Met andere woorden, het ene WLC kan zijn EAP-verzoek niet aan een andere WLC doorsturen voor authenticatie. Elke WLC zou zijn eigen lokale EAP server en individuele database moeten hebben.

Opmerking: gebruik deze opdrachten om te voorkomen dat WLC verzoeken naar een externe straal server verstuurt.

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

De lokale EAP-server ondersteunt deze protocollen in 4.1.171.0 softwarerelease en later:

- LEAP
- EAP-FAST (zowel gebruikersnaam/wachtwoord als certificaten)
- EAP-TLS

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van het configureren van WLC's en lichtgewicht access points (LAP's) voor gebruik als basiseenheid
- Kennis van Lichtgewicht Access Point Protocol (LWAPP) en draadloze beveiligingsmethoden
- Basiskennis van lokale MAP-authenticatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Windows XP met CB21AG adapterkaart en Cisco Secure Services client versie 4.0
- Cisco 4400 draadloze LAN-controller 4.1.17.0
- Microsoft Certified Authority op Windows 2000-server

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> meer informatie over documentconventies.

Local EAP op Cisco draadloze LAN-controller configureren

Dit document gaat ervan uit dat de basisconfiguratie van de WLC al is voltooid.

Local EAP-configuratie

Voltooi deze stappen om lokale MAP te configureren:

 Voeg een lokale netgebruiker toe:Kies in de GUI. Beveiliging > Lokale Net-gebruikers > Nieuw, voer de gebruikersnaam, het wachtwoord, de gastgebruiker, WLAN-id en de beschrijving in en klik op

loepassen.				Set U	III III CAUUU - PI	
cisco	MONITOR WLANS (ONTROLLER WIRELESS	SECURITY		C <u>O</u> MMANDS	HELP
Security	Local Net Users > N	lew			< Back	Apply
General	User Name	eapuser2				
 RADIUS Authentication 	Password	•••••				
TACACS+ LDAP	Confirm Password	•••••				
Local Net Users MAC Filtering Disabled Clients	Guest User					
User Login Policies AP Policies	WLAN ID	1				
Local EAP General	Description	Employee user local datab	ase			

Vanuit de CLI kunt u het configuratieset gebruiken om

<gebruikersnaam><wachtwoord><WLAN id><beschrijving>opdracht toe te

voegen:Opmerking: deze opdracht is vanwege ruimtelijke redenen naar een tweede regel teruggebracht.

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

 Specificeer de terugwinningsvolgorde voor gebruikersinterface.Kies in de GUI Security > Local EAP > Accounting Priority. Selecteer LDAP en klik op "<" en klik op Toepassen. Hiermee worden de gebruikersreferenties in de lokale database eerst gezet

uluilu cisco	MONITOR	<u>W</u> LANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	HErb
Security	Priority 0)rder > L	ocal-Auth				
- AAA General	User Cred	lentials					
 Authentication Accounting TACACS+ Authentication Accounting Authorization LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies 	LDAP	~	LOCAL	P HT			-
Local EAP Profiles EAP-FAST Parameters Authentication Priority							

Van de CLI:

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

3. Een MAP-profiel toevoegen:Om dit vanuit de GUI te doen, kiest u **Beveiliging > Local EAP > Profiles** en klikt u op **New**. Wanneer het nieuwe venster verschijnt, typt u de Profile Name en

klikt u op Toepassen

1000	4000												
Мо	NITOR	<u>W</u> LANS		WIRE	LESS <u>S</u> ECU	RITY MAN	AGEMENT	COMMANDS	HEID	 			
Lo	cal EAP	Profiles									New		Apply
Pr	ofile Nar	ne	u	AP	EAP-FAST	r	EAP-T	LS			1		
										/			
rs ty													
											Sage Configuration	Bng	Logout Befre
BONLOK	WLANS	CONTROLLER	WINELESS	SECONTRY	MANANEMENT	COMMANDS	HELP						
Local EA	P Profiles	; > New									< 84	ock	Apply
Profile Na	me				EAP-test								

U kunt dit ook doen door de CLI-opdracht **configuratie van de lokale auth-eap-profile add** <profile-name> te gebruiken. In ons voorbeeld is de profielnaam een *EAP-test*. (Cisco Controller) >config local-auth eap-profile add *EAP-test*

4. Voeg een methode toe aan het MAP-profiel.Kies in de GUI Security > Local EAP > Profiles en klik op de profielnaam waarvoor u de authenticatiemethoden wilt toevoegen. In dit voorbeeld wordt gebruik gemaakt van LEAP, EAP-FAST en EAP-TLS. Klik op Toepassen om de methoden in te

stellen.
CISCO MONITOR MLANI CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security Local EAP Profiles
* AAA Profile Name LEAP EAP-FAST EAP-TLS General * PADDUS EAP-Cest E E E
CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security Local EAP Profiles > Edit
* AAA Profile Name EAP-test
PLADIUS Authoritication ELEAP
Accounting P TACACS+ EAP-FAST
Laced Net Users EAP-TLS
Disabled Clients User Login Policies AP Policies Local Certificate Required P Enabled
* Local EAP Client Certificate Required F Enabled
Profiles EAP-FAST Parameters Certificate Issuer Vendor V
Authentication Priority Priority Order Check against CA certificates P Enabled
Access Central Lists Verity Certificate CN Identity Enabled
▶ IPSec Certs

U kunt ook de CLI opdracht **mede-configuratie van de lokale auth-eap-profile methode** gebruiken **om** *<methode-name><profile-name>* toe te voegen. In onze voorbeeldconfiguratie voegen we drie methoden toe aan de MAP-profieltest. De methoden zijn LEAP, EAP-FAST en EAP-TLS, waarvan de methodenamen respectievelijk *springen* en *hoog* zijn. Deze uitvoer toont de CLI configuratieopdrachten:

(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. Configureer de parameters van de MAP-methode. Dit wordt alleen gebruikt voor EAP-FAST. De parameters die moeten worden ingesteld zijn:Server Key (server-key)-serversleutel om beschermde toegangsaanmeldingsgegevens (PAC's) te versleutelen/decrypteren (in hexadecimaal).Tijd om te leven voor PAC (pac-tl) Hiermee wordt de tijd ingesteld om te leven voor de PAC.Bevoegde autoriteit-id —Hiermee stelt u de autoriteit-identificator in.Anonymous Voorziening (anon-provn) - vormt of anonieme bepaling wordt toegestaan. Dit is standaard ingeschakeld.Voor configuratie via de GUI, kies Beveiliging > Lokaal MAP > EAP-FAST-parameters en voer de servertoets, de tijd om voor de PAC te leven, autoriteit-ID (in hex) en de waarde van de autoriteit-ID

 1.							
MONITOR	<u>₩</u> LANs	CONTROLLER	WIRELESS	SECURITY	MENAGEMENT	COMMANDS	s HELP
EAP-FAS	T Metho	d Parameters					
Server Ke	y (in hex	0				****	
Confirm S	erver Ke	Y				****	
Time to liv	e for the	PAC				10	days
Authority	1D (in he	»()				436973	1726364
Authority	ID Inform	nation				Cisco A	e A-ID
Anonymo	us Provis	lion				R En	Enabled

Dit zijn de CLI-configuratieopdrachten die moeten worden gebruikt om deze parameters voor EAP-FAST in te stellen:

(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 verificatie per WLAN inschakelen:Kies in de GUI WLAN's in het bovenste menu en selecteer de WLAN's waarvoor u lokale verificatie wilt configureren. Er verschijnt een nieuw venster. Klik op de tabbladen Security > AAA. Controleer lokale MAP-verificatie en selecteer de juiste MAP-profielnaam in het keuzemenu zoals in dit voorbeeld wordt weergegeven:

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

U kunt ook het CLI **Config-***lokaal*-auth uitgeven **om***<profiel-naam><WLAN-id>* configuratieopdracht zoals hieronder wordt getoond, uit te geven: (Cisco Controller) >**config wlan local-auth enable EAP-test 1**

7. Stel Layer 2 security parameters in.Vanuit de GUI-interface gaat in het venster WLANbewerking naar de tabbladen Security > Layer 2 en kiest u WAP+WAP2 uit het keuzemenu Layer 2 Security. Stel onder het gedeelte WAP+WAP2-parameters de WAP-encryptie in op TKIP en WAP2-encryptie AES. Klik vervolgens op

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMEN	e Configuration Ping Logout <u>R</u> efree VT C <u>O</u> MMANDS HELP
WLANS	WLANs > Edit General Security Qos Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security Mac Filtering WPA+WPA2 Parameters MAC Filtering WPA Policy V WPA Encryption AES TKIP WPA2 Policy V WPA2 Encryption AES TKIP Auth Key Mgmt 802.1× V	< Back Apply

(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. Controleer de configuratie:

(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
	lean fast tis
Enabled methods	icap labe elb
Enabled methods Configured on WLANs	1
Enabled methods	1
Enabled methods Configured on WLANS EAP Method configuration: EAP-FAST:	1
Enabled methods Configured on WLANS EAP Method configuration: EAP-FAST: More or (q)uit	1
Enabled methods Configured on WLANS EAP Method configuration: EAP-FAST: More or (q)uit Server key	<pre>loop last ths 1 <hidden></hidden></pre>
Enabled methods Configured on WLANS EAP Method configuration: EAP-FAST: More or (q)uit Server key TTL for the PAC	<pre>chidden> 10</pre>
Enabled methods Configured on WLANS EAP Method configuration: EAP-FAST: More or (q)uit Server key TTL for the PAC Anonymous provision allowed	<hidden> 10 Yes</hidden>
Enabled methods Configured on WLANS EAP Method configuration: EAP-FAST: More or (q)uit Server key TTL for the PAC Anonymous provision allowed Authority ID	<pre>chidden> 10 Yes 43697369f1000000000000000000000000000000000000</pre>
Enabled methods Configured on WLANS EAP Method configuration: EAP-FAST: More or (q)uit Server key TTL for the PAC Anonymous provision allowed Authority ID Authority Information	<hidden> 10 Yes 43697369f1000000000000000000000000000000000000</hidden>

U kunt specifieke parameters van VLAN 1 zien met de opdracht Show WLAN *<wlan>*: (Cisco Controller) *>show wlan 1*

WLAN Identifier	1
Profile Name	austinlab
Network Name (SSID)	austinlab
Status	Disabled
MAC Filtering	Disabled
Broadcast SSID	Enabled
AAA Policy Override	Disabled
Number of Active Clients	0
Exclusionlist Timeout	60 seconds
Session Timeout	1800 seconds
Interface	management
WLAN ACL	unconfigured
DHCP Server	Default
DHCP Address Assignment Required	Disabled
Quality of Service	Silver (best effort)
WMM	Disabled
CCX - AironetIe Support	Enabled
CCX - Gratuitous ProbeResponse (GPR)	Disabled
Dot11-Phone Mode (7920)	Disabled
Wired Protocol	None
More or (q)uit	
IPv6 Support	Disabled
Radio Policy	All
Local EAP Authentication	Enabled (Profile 'EAP-test')
Security	
802.11 Authentication:	Open System
Static WEP Keys	Disabled
802.1X	Disabled
Wi-Fi Protected Access (WPA/WPA2)	Enabled
WPA (SSN IE)	Enabled
TKIP Cipher	Enabled
AES Cipher	Disabled
WPA2 (RSN IE)	Enabled
TKIP Cipher	Disabled
AES Cipher	Enabled
	Auth Key Management
802.1x	Enabled
PSK	
	Disabled
ССКМ	Disabled 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

Toepassen.

Er zijn andere lokale authenticatieparameters die kunnen worden geconfigureerd, in het bijzonder de actieve time-out timer. Deze timer vormt de periode waarin lokale EAP wordt gebruikt nadat alle RADIUS-servers zijn mislukt.Kies in de GUI, **Security > Local EAP > General** en stel de tijdwaarde in. Klik vervolgens op

սիսիս							onfiguration [<u>P</u> ing Logout <u>R</u> efree
cisco		<u>W</u> LANs		W <u>I</u> RELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
CISCO Security AAA General RADIUS Authentication Accounting TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies	General Local Auti	<u>W</u> LANS h Active ' It period di li Radius Se	CONTROLLER Timeout ¹ (in se uring which Local a revers are failed	wireless ecs) EAP will always	60 60		COMMANDS	Apply
User Lagin Policies AP Policies Ceneral Profilies								

Geef deze opdrachten vanuit CLI uit:

(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

U kunt de waarde verifiëren waaraan deze timer is ingesteld wanneer u het opdracht **lokaalauth** configuratie afgeeft.

(Cisco Controller) >show local-auth config User credentials database search order: Primary Local DB Timer: Active timeout 60 Configured EAP profiles: Name EAP-test ... Skip Als u de handleiding voor PAC wilt genereren en laden, kunt u de

9. Als u de handleiding voor PAC wilt genereren en laden, kunt u de GUI of de CLI gebruiken.Selecteer in de GUI de optie **OPDRACHTEN** in het bovenste menu en kies de

optie Bestand uploaden in de lijst aan de rechterkant. Selecteer PAC (Protected Access Credentials) in het keuzemenu van het bestandstype. Voer alle parameters in en klik op Upload.

սիսիս								ation <u>P</u> ing	Logout <u>R</u> efres
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	не <u>т</u> р	
Commands	Upload file	from C	ontroller					Clear	Upload
Download File	File Type			PAC (Protects	ed Access Cred	dential) 💌			
Reboot	User (Iden	tity)		test1				^	
Reset to Factory Default Set Time	Validity (in	days)		60]				
	Password			•••••					
	Confirm Pa	ssword		•••••					
	TFTP Serve	er i i i							
	IP Address File Path			10.1.1.1					
								1	

Voer vanuit CLI deze opdrachten in:

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

username	Enter the user	(identity) of th	le PAC
(Cisco Cont	roller) > transf	er upload pac tes	t1 ?
<validity></validity>	Enter the PAG	C validity period	l (days)
(Cisco Contr	oller) > transfe :	r upload pac test	1 60 ?
<password></password>	Enter a pass	word to protect t	he PAC
(Cisco Cont:	roller) > transf	er upload pac tes	t1 60 cisco123
(Cisco Contro	oller) > transfe :	r upload serverip	0 10.1.1.1
(Cisco Contro	oller) > transfe :	r upload filename	manual.pac
(Cisco Contro	oller) > transfe :	r upload start	
Mode TFTP Server TFTP Path TFTP Filenam Data Type PAC User PAC Validity PAC Password	IP		TFTP 10.1.1.1 / manual.pac PAC test1 60 days cisco123
Are you sure PAC transfer File transfe	you want to stand starting. r operation com	art? (y/N) y pleted successful	ly.

Microsoft certificeringsinstantie

Om de MAP-FAST versie 2 en MAP-TLS-authenticatie te kunnen gebruiken, moeten de WLC en alle clientapparaten over een geldig certificaat beschikken en tevens het publieke certificaat van de certificeringsinstantie kennen.

Installatie

Als de Windows 2000 Server niet reeds de diensten van de certificeringsinstantie geïnstalleerd heeft, moet u het installeren.

Voltooi deze stappen om de Microsoft certificeringsinstantie in te schakelen op een Windows 2000-server:

1. Kies in het Configuratiescherm de optie Software.



2. Selecteer Windows-componenten aan de linkerkant toevoegen of



3. Controleer de certificaatservices.

ndows Components You can add or remove comp	oonents of Windows 2000	D.
To add or remove a compone part of the component will be Details.	ent, click the checkbox. A installed. To see what's i	A shaded box means that only included in a component, click
Components:		
🗷 📻 Accessories and Utilit	ies	12.1 MB 🔺
🗔 📴 Certificate Services		1.4 MB
Indexing Service		0.0 MB
Internet Information S	ervices (IIS)	21.6 MB
Management and Mo	nitorina Tools	5.2 MB
Description: Installs a certific public key secu	ation authority (CA) to iss rity applications.	ue certificates for use with
Total disk space required:	0.0 MB	Detaile
Space available on disk:	4205.9 MB	
	(Pao	k Next> Car

Microsoft	Certificate Se	rvices		R	×
⚠	After installing from a domain.	Certificate Servi Do you want to	ces, the computer cann o continue?	ot be renamed and th	ne computer cannot join or be removed
			Yes	No	

4. Selecteer welk type certificeringsinstantie u wilt installeren. Om een eenvoudig op zichzelf staand gezag te creëren, selecteert u **Afstand-alone wortel CA**.

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

5. Voer de nodige informatie in over de certificeringsinstantie. Deze informatie creëert een zelfondertekend certificaat voor uw certificeringsinstantie. Onthoud de CA-naam die u gebruikt.De certificeringsinstantie slaat de certificaten op in een database. In dit voorbeeld wordt de standaardinstelling gebruikt die door Microsoft is voorgesteld:

	Browse
	Bro <u>w</u> se
ared rolder	Browse
	ared folder

6. De diensten van de certificeringsinstantie van Microsoft gebruiken de server van het ISIS Microsoft om client- en servercertificaten te creëren en te beheren. De IS-dienst moet hiervoor opnieuw worden

Microsof	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

De Microsoft Windows 2000 Server installeert nu de nieuwe service. U hebt uw installatie-cd voor Windows 2000-servers nodig om nieuwe Windows-onderdelen te installeren.De certificeringsinstantie is nu geïnstalleerd.

Installeer het certificaat in de Cisco draadloze LAN-controller

Om EAP-FAST versie 2 en EAP-TLS op de lokale MAP server van een Cisco draadloze LAN controller te gebruiken, volgt u deze drie stappen:

- 1. Installeer het apparaatcertificaat op de draadloze LAN-controller.
- 2. Download een leveranciercertificaat aan de draadloze LAN-controller.
- 3. Configureer de draadloze LAN-controller voor het gebruik van EAP-TLS.

Merk op dat in het voorbeeld in dit document, de Access Control Server (ACS) op dezelfde host is geïnstalleerd als de Microsoft Active Directory en Microsoft Cerfication Authority, maar de configuratie dient hetzelfde te zijn als de ACS-server op een andere server is.

Installeer het apparaatcertificaat op de draadloze LAN-controller

Voer de volgende stappen uit:

- 1. Voltooi deze stappen om het certificaat voor invoer in de WLC te genereren:Ga naar http://<serverlpAddress>/certsrv.Kies een certificaat aanvragen en klik op Volgende.Klik op Geavanceerde aanvraag en klik op Volgende.Kies een certificaataanvraag bij deze CA indienen met behulp van een formulier en klik op Volgende.Kies webserver voor certificaatsjabloon en voer de relevante informatie in. Merk de sleutels vervolgens op als uitvoerbaar.U ontvangt nu een certificaat dat u in uw machine moet installeren.
- 2. Voltooi deze stappen om het certificaat van de pc terug te halen:Open een browser van Internet Explorer en kies Gereedschappen > Internet-opties > Content.Klik op Certificaten.Selecteer het nieuwe geïnstalleerde certificaat in het keuzemenu.Klik op Exporteren.Klik tweemaal op Volgende en kies Ja exporteren de privé-toets. Dit formaat is het PKCS#12 (PFX-formaat).Kies sterke bescherming inschakelen.Typ een wachtwoord.Opslaan in een bestand <tme2.pfx>.
- 3. Kopieer het certificaat in de PKCS#12-indeling naar een computer waarop u OpenSSL hebt geïnstalleerd, zodat het naar PEM-indeling wordt geconverteerd.

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. Download het geconverteerde PEM-formaat certificaat op de WLC. (Cisco Controller) >transfer download datatype eapdevcert

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

(Cisco Controller) >transfer download start

Mode.....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. Controleer het certificaat zodra u het hebt herstart.

(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

Download een leveranciercertificaat aan de draadloze LAN-controller

Voer de volgende stappen uit:

- Voltooi deze stappen om het CA-certificaat van de verkoper terug te halen:Ga naar http://<serverlpAddress>/certsrv.Kies Ophalen het CA-certificaat en klik op Volgende.Kies het CA-certificaat.Klik op DER gecodeerd.Klik op CA-certificaat downloaden en het certificaat opslaan als rootca.cer.
- De verkoper CA van het DER-formaat converteren naar het PEM-formaat met de openssl x509-in rootca.cer -informeert DER-out rootca.pem -buiten PEM-opdracht.Het uitvoerbestand is rootca.pem in de PEM-indeling.
- 3. Download het CA-certificaat van verkoper: (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.

Configureer de draadloze LAN-controller voor het gebruik van EAP-TLS

Voer de volgende stappen uit:

Kies in de GUI, Security > Local EAP > Profiles, kies het profiel en controleer op deze instellingen:

- · Lokaal certificaat vereist is ingeschakeld.
- · Clientcertificaat vereist is ingeschakeld.
- Certificaat-uitgever is verkoper.
- Controleer tegen CA-certificaten is ingeschakeld.

ululu cisco	MONITOR MUNIC 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	R trabled
Profiles EAP-FAST Parameters	Certificate Issuer	Vendor 💌
Authentication Priority F Priority Order	Check against CA certificates	P Enabled
	Verify Certificate CN Identity	C Enabled
IPSec Certs		E como
Wireless Protection Policies	Check Certificate Date Validity	C/ Enabled

Installeer het certificaatcertificaat op het clientapparaat.

Download en Installeer een Root CA-certificaat voor de client

De client moet een basiscertificaat van CA van een server van de certificeringsinstantie verkrijgen. Er zijn meerdere methoden die u kunt gebruiken om een client-certificaat te verkrijgen en het in de Windows XP-machine te installeren. Om een geldig certificaat te kunnen verkrijgen, moet de Windows XP-gebruiker zijn aangemeld bij het gebruik van zijn gebruikersidentificatie en moet er een netwerkverbinding zijn.

Een webbrowser op de Windows XP client en een bekabelde verbinding met het netwerk werden gebruikt om een client certificaat te verkrijgen van de server van de Private root Certified Authority. Deze procedure wordt gebruikt om het client-certificaat te verkrijgen van een server van de Microsoft certificeringsinstantie:

- 1. Gebruik een webbrowser op de client en plaats de browser naar de server van de certificeringsinstantie. Voer hiervoor http://IP-address-of-Root-CA/certsrv in.
- 2. Meld u aan bij gebruik van **Domain_Name\user_name**. U moet inloggen met behulp van de gebruikersnaam van het individu dat de XP-client moet gebruiken.
- 3. Kies in het venster Welcome een CA-certificaat ophalen en klik op Next.
- 4. Selecteer Base64 Encoding en Download CA certificaat.
- 5. Klik in het venster certificaatuitgifte op Installeer dit certificaat en klik op Volgende.
- 6. Kies **Automatisch de certificaatopslag selecteren** en klik op **Volgende**, voor een succesvol importbericht.
- 7. Connect met de certificeringsinstantie voor het opvragen van het certificaat van de certificeringsinstantie:

Microso	& Certificat	e Service	is tme

Welcome

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

Select a task:

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

Microsoft Certificate Services - tme

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow your computer to trust certificates issued from this certification authority.

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

Choose file to download:



8. Klik op CA-certificaat

downloaden.

Microsoft Certificate Services -- tme

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow your computer to trust certificates issued from this certification 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?	
CA Certificate: Current [tme]	Name: certnew.cer Type: Security Certificate, 798 bytes Fiorix 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. What's the sisk?	



Hom

Home

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. Om te controleren of het certificaat van de certificeringsinstantie correct is geïnstalleerd, opent u Internet Explorer en kiest u **Gereedschappen > Internet-opties > Content >**



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

Bij Trusted Root-certificeringsinstantie dient u uw nieuwe geïnstalleerde certificeringsinstantie te raadplegen:

nver CA nesta ACorp
ACorp
ACorp
ACorp
RFirst
RFirst
RFirst
RFirst
ommer
Advance
Muvance

Een clientcertificaat genereren voor een clientapparaat

De client moet een certificaat van een server van de certificeringsinstantie verkrijgen voor de WLC om een WLAN EAP-TLS-client te authenticeren. Er zijn meerdere methoden die u kunt gebruiken om een client-certificaat te verkrijgen en het in de Windows XP-machine te installeren. Om een geldig certificaat te kunnen verkrijgen, moet de Windows XP-gebruiker zijn aangemeld bij het gebruik van zijn gebruikersidentificatie en moet hij een netwerkverbinding hebben (een bekabelde verbinding of een WLAN-verbinding met een 802.1x-beveiliging uitgeschakeld).

Een webbrowser op de Windows XP client en een bekabelde verbinding met het netwerk worden gebruikt om een client certificaat te verkrijgen van de server van de Private root Certified Authority. Deze procedure wordt gebruikt om het client-certificaat te verkrijgen van een server van de Microsoft certificeringsinstantie:

- 1. Gebruik een webbrowser op de client en plaats de browser naar de server van de certificeringsinstantie. Voer hiervoor http://IP-address-of-Root-CA/certsrv in.
- 2. Meld u aan bij gebruik van **Domain_Name\user_name**. U moet inloggen met behulp van de gebruikersnaam van het individu dat de XP-client gebruikt. (De gebruikersnaam wordt in het client-certificaat opgenomen.)
- 3. Kies in het venster Welcome een certificaat aanvragen en klik op Volgende.
- 4. Kies Geavanceerde aanvraag en klik op Volgende.

- 5. Kies een certificaataanvraag bij deze CA indienen met behulp van een formulier en klik op Volgende.
- 6. Kies in het formulier Geavanceerd certificaataanvraag de sjabloon als **gebruiker**, specificeer de grootte van het certificaat als **1024** en klik op **Indienen**.
- 7. Klik in het venster certificaatafgifte op **Installeer dit certificaat**. Dit resulteert in de succesvolle installatie van een client certificaat op de Windows XP-

client. Microsoft Certificate Services -- trme 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 Request a certificate 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 -- tme Home Advanced Certificate Requests You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain

Submit a certificate request to this CA using a form.

Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station. You must have an enrollment agent certificate to submit a request for another user.

Next >

8. Selecteer Clientverificatiecertificaat.

Microsoft Certifi	cate Services tme		
Advanced Ce	rtificate Request		
Certificate Tem	late:		
	User		
Key Options:			
CSP:	Microsoft Base Cryptographic Provider v1.0	~	
Key Usage:	○ Exchange ○ Signature ● Both		
Key Size:	512 Min: 384 (common key sizes: 512 1024) Max:1024		
	 Create new key set Set the container name Use existing key set 		
	Enable strong private key protection		
	Mark keys as exportable		
	Use local machine store You must be an administrator to generate a key in the local machine store.		
Additional Optic	ns:		
Hash Algorithm:	SHA-1 Only used to sign request.		
	Save request to a PKCS #10 file		
Attributeo.			

certificaat is nu gemaakt.

9. Om te controleren of het certificaat is geïnstalleerd, gaat u naar Internet Explorer en kiest u Gereedschappen > Internet-opties > Content > Certificaten. In het tabblad Persoonlijk kunt u het certificaat bekijken.

Certificates				? 🛛
Intended purp	pose:	<all></all>		~
Personal (Other Peop	le Intermediate Certificatio	n Authorities Trusted	Root Certification
Issued To	0	Issued By	Expiratio Fri	endly Name
🕮 Admin	istrator	tme	3/27/2008 <n< td=""><td>one></td></n<>	one>
Import Certificate in Encrypting f	Exp ntended p File Systen	ort Remove	ntication	Advanced View

EAP-TLS met Cisco Secure Services-client op het clientapparaat

Voer de volgende stappen uit:

- De WLC zendt standaard de SSID uit, dus wordt deze weergegeven in de lijst Netwerk maken van gescande SSID's. U kunt een netwerkprofiel maken door op SSID in de lijst (Enterprise) te klikken en op Netwerk maken te klikken. Als de WLAN-infrastructuur is geconfigureerd met SSID dat wordt uitgeschakeld, moet u handmatig de SSID toevoegen. Om dit te doen, klik op Add onder Access Devices en voer handmatig de juiste SSID's (bijvoorbeeld Enterprise) in. Configureer actief probe gedrag voor de client. Dat is, waar de klant actief voor zijn gevormd SSID probeert. Specificeer actief zoekactie naar dit toegangsapparaat nadat u SSID in het venster Toevoegen toegangsapparaat hebt ingevoerd.Opmerking: de poortinstellingen staan geen bedrijfsmodi toe (802.1X) indien de MAP-echtheidsinstellingen niet voor het profiel zijn ingesteld.
- 2. Klik op Netwerk maken om het venster Network Profile te starten, dat u toestaat om de gekozen (of geconfigureerde) SSID te associëren met een verificatiemechanisme. Geef een beschrijvende naam voor het profiel toe. Opmerking: Meerdere WLAN-beveiligingstypen en/of SSID's kunnen bij dit verificatieprofiel worden

gekoppeld. **Cisco Secure Services Client** - 0 × Client Administration Help Create Networks Manage Networks Access Data Security 👔 aruba-ap-config-in-the-clear (2 accesses dete... 🚈 WEP 🐹 Open il b Ccx5 (2 accesses detected) Open Open con аl аl 001907351aa3 High Signal WEP guestnet (5 accesses detected) 💥 Open guestnetwork Open N-Rogue WEP secure-1 (3 accesses detected) Mixed Itme-test (5 accesses detected) WPA III trng1 (2 accesses detected) WEP Create Network

- 3. Schakel de authenticatie in en controleer de EAP-TLS-methode. Klik vervolgens op **Configureren** om de EAP-TLS-eigenschappen te configureren.
- 4. Klik onder Samenvatting van de Netwerkconfiguratie op **Wijzigen** om de instellingen EAP / geloofsbrieven te configureren.
- 5. Specificeer Inschakelen-verificatie, kies EAP-TLS onder Protocol en kies Gebruikersnaam als Identity.
- 6. Specificeer **Gebruik Single Sign on Credentials** om logaanmeldingsgegevens voor netwerkverificatie te gebruiken. Klik op **Configureren** om de EAP-TLS-parameters in te stellen.

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	Network			
🔽 Avai	able to all users (pub	lic profile)		
T Auto	matically establish M	achine con	nection	
🔽 Auto	matically establish U	ser connect	ion	
	Before user accourt	nt (supports	smartcard/password or	nly)
-Network Configur	ation Summary:			
Authentication	FAP-TLS:			
- 1	EA 160,			
Credentials:	Request when nee	ded and rer	nember for the session.	
			Modi	fy
Access Devices		, ,		
Access / SSID	Mode	Notes		
con-eap	WPA2 Enterpris	e		
Add	Modify C	onfiguration	Remove	
Help			ок са	ancel

7. Om een beveiligde EAP-TLS-configuratie te hebben, moet u het RADIUS-servercertificaat controleren. Controleer hiervoor **het servercertificaat**

ed Client Ce tificate Resumption	rtificates Or		
ed Client Ce tificate Resumption	rtificates Or	nly	
tificate Resumption			
Resumption			
	OK .	Ca	nce
		OK	OK Ca

 Om het RADIUS-servercertificaat te valideren, moet u Cisco Secure Services Clientinformatie geven om alleen het juiste certificaat te aanvaarden. Kies client > Vertrouwde servers > Huidige op gebruikers vertrouwde servers beheren.

Cisco Secure Services	Client	_O×
Client Administration Help		
Manage Adapters	A Maturation	
Trusted Servers 🔸	Manage Current User Trusted Servers	1
Advanced Settings	Manage Machine / All Users Trusted Servers	Data Seci
✓ Enable Client	ork Disconnected	
✓ Turn WiFi Radio On	Misconfigured Access (AutoCom	
 Show System Tray 	Canable for: wen	
Close Window	Configured for: wpa2	
Connect	Configure Remove Status	Details
Manage Current User	Trusted Servers	//
-Trusted Server Definition -	- Current Users:	
Bule Name	Validation Meth	od
Add Server Bule	Bemove Selected	lected
	Edit Se	
Help		Close

9. Geef een naam voor de regel en controleer de naam van het

servercertificaat.

Trusted Server	
Trusted Server	
Rule name: WLC-Config	
Validation method: Certificate	•
Match ANY Certificate Validation Rule:	
Subject/Common Name Exactly matches	tme
L	
Help	OK Cancel

De configuratie van het MAP-TLS is voltooid.

10. Sluit aan op het draadloze netwerkprofiel. De Cisco Secure Services Client vraagt om inloggen van de gebruiker:

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

e Cisco Secure Services Client ontvangt het servercertificaat en controleert dit (met de regel ingesteld en de certificeringsinstantie geïnstalleerd). Vervolgens wordt gevraagd het certificaat te gebruiken voor de gebruiker.

11. Nadat de client voor authenticatie is geselecteerd, kiest u SSID onder het profiel in het tabblad Oplossingen beheren en klikt u op Status om verbindingsdetails te vragen.Het venster Connection Details geeft informatie over het clientapparaat, de verbindingsstatus en de statistieken en de verificatiemethode. Het tabblad WiFi biedt details over de 802.11verbindingsstatus, waaronder RSSI, 802.11-kanaal en

verificatie/encryptie.

Selected Acce	855	Status		Security
con-eap		Connected: Authenti	cated (AutoConn	WPA2
11:24:28.044 11:24:28.054 11:24:28.074 11:24:28.094 11:24:28.094 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 Connection auth Port state transiti Connection assoc Connection assoc Port state transiti Port state transiti Identity has been Authentication st The server has re Validating the ser Port state transiti The authenticati The following IP	Connection requested from entication started using the k on to AC_PORT_STATE_UN siation started using encryptic siation succeeded. on to AC_PORT_STATE_AL on to AC_PORT_STATE_AL in requested from the network. a sent to the network	Auser context. Augged in user's cred AUTHENTICATED in mode AC_ENCR, INNECTING(AC_P(ITHENTICATING(A 	entials. DIAC_PORT_STATUS_STARTED) _AES AC_ASSOC_11i_8021X DRT_STATUS_LINK_UP) DC_PORT_STATUS_8021x_ACQUIRED)
		Ck	sar	

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

nnection Details WiFi D	etails
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 Addre	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	Class

Opdrachten debug

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg <u>Belangrijke informatie over debug Commands</u> voordat u **debug**opdrachten gebruikt.

Deze debug opdrachten kunnen bij de WLC worden gebruikt om de voortgang van de authenticatie-uitwisseling te bewaken:

- debug aaaaaathedingen activeren
- u kunt gegevens debug a
- debug dot1x gebeurtenissen in staat stellen

- debug dot1x-staten
- debug a local-auth-gebeurtenissen activerenOF
- debug a allen activeren

Gerelateerde informatie

- Configuratie-gids voor Cisco draadloze LAN-controllers, release 4.1
- <u>WLAN-technologieondersteuning</u>
- Technische ondersteuning en documentatie Cisco Systems