802.1x configureren - PEAP met FreeRadius en WLC 8.3

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Configureren **Netwerkdiagram** Installeer de httpd-server en MariaDB Installeer PHP 7 op CentOS 7 Installeer FreeRADIUS **FreeRADIUS** WLC als verificatie, autorisatie en accounting (AAA) client op FreeRADIUS FreeRADIUS-server als RADIUS-server op WLC **WLAN** Gebruikers aan gratis RADIUS-database toevoegen Certificaten op gratisRADIUS Apparaatconfiguratie FreeRADIUS-certificaat importeren WLAN-profiel maken Verifiëren Verificatieproces op WLC Problemen oplossen

Inleiding

In deze documenten wordt beschreven hoe u een Wireless Local Area Network (WLAN) kunt instellen met 802.1x security en Protected Extensible Authentication Protocol (PEAP) als Extensible Authentication Protocol (EAP). FreeRADIUS wordt gebruikt als de externe RADIUS-server (Dial-In User Service) (RADIUS).

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- Linux
- Vim-editor
- AireOS draadloze LAN-controllers (WLC's)

Opmerking: Dit document is bedoeld om de lezers een voorbeeld te geven over de configuratie die op een gratis RADIUS-server vereist is voor PEAP-MS-CHAPv2-verificatie. De gratisRADIUS-serverconfiguratie die in dit document wordt voorgesteld, is in het lab getest en bleek te werken zoals verwacht. Het Cisco Technical Assistance Center (TAC) ondersteunt de gratis RADIUS-serverconfiguratie niet.

Gebruikte componenten

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

- CentOS7 of Red Hat Enterprise Linux 7 (RHEL7) (Aanbevolen 1 GB RAM en minstens 20 GB HDD)
- WLC 5508 v8.3
- MariaDB (MySQL)
- FreeRADIUS
- PHP 7

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Netwerkdiagram



Installeer de httpd-server en MariaDB

Stap 1. Start deze opdrachten om httpd-server en MariaDB te installeren.

[root@tac-mxwireless ~]# yum -y update [root@tac-mxwireless ~]# yum -y groupinstall "Development Tools" [root@tac-mxwireless ~]# yum -y install httpd httpd-devel mariadb-server mariadb Stap 2. Start en schakel httpd (Apache) en Maria DB server in.

[root@tac-mxwireless ~]# systemctl enable httpd [root@tac-mxwireless ~]# systemctl start httpd [root@tac-mxwireless ~]# systemctl start mariadb [root@tac-mxwireless ~]# systemctl enable mariadb

Stap 3. Configureer de eerste instellingen van MariaDB om het te beveiligen.

[root@tac-mxwireless ~] #mysql_secure_installation

Opmerking: Draai alle delen van dit script. Het wordt aanbevolen voor alle MariaDB-servers in productiegebruik. Lees elke stap zorgvuldig door.

In order to log into MariaDB to secure it, we'll need the current password for the root user. If you've just installed MariaDB, and you haven't set the root password yet, the password will be blank, so you should just press enter here.

Enter current password for root (enter for none): OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB root user without the proper authorisation.

Set root password? [Y/n] Y New password: Re-enter new password: Password updated successfully! Reloading privilege tables. ... Success! By default, a MariaDB installation has an anonymous user, allowing anyone to log into MariaDB without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment. Remove anonymous users? [Y/n] y ... Success! Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network. Disallow root login remotely? [Y/n] y ... Success! By default, MariaDB comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment. Remove test database and access to it? [Y/n] y - Dropping test database... ... Success! - Removing privileges on test database... ... Success! Reloading the privilege tables will ensure that all changes made so far will take effect immediately. Reload privilege tables now? [Y/n] y ... Success! Cleaning up... All done! If you've completed all of the above steps, your MariaDB installation should now be secure. Thanks for using MariaDB! **Stap 4. Configureer database voor gratis RADIUS (gebruik hetzelfde wachtwoord in Stap 3)**.

[root@tac-mxwireless ~]# mysql -u root -p -e "CREATE DATABASE radius" [root@tac-mxwireless ~]# mysql -u root -p -e "show databases" [root@tac-mxwireless ~]# mysql -u root -p MariaDB [(none)]> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "radiuspassword"; MariaDB [(none)]> FLUSH PRIVILEGES; MariaDB [(none)]> \q Bye

Installeer PHP 7 op CentOS 7

Stap 1. Start deze opdrachten om PHP 7 op CentOS7 te installeren.

```
[root@tac-mxwireless ~]# cd ~
[root@tac-mxwireless ~]# curl 'https://setup.ius.io/' -o setup-ius.sh
[root@tac-mxwireless ~]# sudo bash setup-ius.sh
[root@tac-mxwireless ~]# sudo yum remove php-cli mod_php php-common
[root@tac-mxwireless ~]# sudo yum -y install mod_php70u php70u-cli php70u-mysqlnd php70u-devel
php70u-gd php70u-mcrypt php70u-mbstring php70u-xml php70u-pear
[root@tac-mxwireless ~]# sudo apachectl restart
```

Installeer FreeRADIUS

Stap 1. Start deze opdracht om FreeRADIUS te installeren.

[root@tac-mxwireless ~]# yum -y install freeradius freeradius-utils freeradius-mysql freeradiussqlite

Stap 2. Maak straal.de dienst start na mariadb.service.

Start deze opdracht:

[root@tac-mxwireless ~]# vim /etc/systemd/system/multi-user.target.wants/radiusd.service Voeg een regel toe in sectie[Eenheid]:

After=mariadb.service [Eenheid] moet er zo uitzien:

[Unit] Description=FreeRADIUS high performance RADIUS server. After=syslog.target network.target After=mariadb.service

Stap 3. Start en schakel freeradius in bij het opstarten.

[root@tac-mxwireless ~]# systemctl start radiusd.service [root@tac-mxwireless ~]# systemctl enable radiusd.service Stap 4. Schakel de beveiliging in.

[root@tac-mxwireless ~]# systemctl enable firewalld [root@tac-mxwireless ~]# systemctl start firewalld [root@tac-mxwireless ~]# systemctl status firewalld

Stap 5. Voeg permanente regels toe aan standaardzone om http, https en Straal diensten toe te staan.

[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius'
[root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success
Stap 6. Wasblok voor wijzigingen opnieuw laden.

[root@tac-mxwireless ~]# firewall-cmd --reload

FreeRADIUS

Om FreeRADIUS te configureren en MariaDB te gebruiken, volgt u deze stappen.

Stap 1. Importeer het RADIUS-databases om de RADIUS-database te vullen.

[root@tac-mxwireless ~]# mysql -u root -p radius < /etc/raddb/modsconfig/sql/main/mysql/schema.sql

Stap 2. Maak een zachte link voor Structured Search Query Language (SQL) onder /etc/raddb/mods-enabled.

[root@tac-mxwireless ~]# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/ Stap 3. Configureer de SQL-module/raddb/mods-available/sql en wijzig de parameters voor de databases met de juiste omgeving.

[root@tac-mxwireless ~]# vim /etc/raddb/mods-available/sql SQL moet er op lijken.

sql {

driver = "rlm_sql_mysql"
dialect = "mysql"

Connection info:

server = "localhost"

```
port = 3306
login = "radius"
password = "radpass" # Database table configuration for everything except Oracle radius_db =
"radius" } # Set to 'yes' to read radius clients from the database ('nas' table) # Clients will
ONLY be read on server startup. read_clients = yes # Table to keep radius client info
client_table = "nas"
```

Stap 4. Verander het groepsrecht van enz/raddb/mods-enabled/sql naar straling.

[root@tac-mxwireless ~]# chgrp -h radiusd /etc/raddb/mods-enabled/sql

WLC als client voor verificatie, autorisatie en accounting (AAA) op FreeRADIUS

Stap 1. Bewerk /etc/raddb/clients.conf om de gedeelde toets voor WLC in te stellen.

[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf
Stap 2. Onderaan voegt u uw ip-adres van de controller en de gedeelde toets toe.

client{ secret = shortname = }

FreeRADIUS-server als RADIUS-server op WLC

GUI:

Stap 1. Open de GUI van de WLC en navigeer naar **BEVEILIGING > RADIUS > Verificatie > Nieuw** zoals in de afbeelding.



Stap 2. Vul de RADIUS-serverinformatie in zoals in de afbeelding.

RADIUS Authentication Serv	vers > New	
Server Index (Priority)	2 ~	
Server IP Address(Ipv4/Ipv6)	a.b.c.d	
Shared Secret Format	ASCII 🗸	•
Shared Secret	•••••	
Confirm Shared Secret	•••••	
Key Wrap	(Designed for	FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812	
Server Status	Enabled \sim	
Support for CoA	Disabled \vee	
Server Timeout	10 seconds	
Network User	🗹 Enable	
Management	🗹 Enable	
Management Retransmit Timeout	2 seconds	
IPSec	Enable	

CLI:

>	config	radius	auth	add <index> <radius-ip-address> 1812 ascii <shared-key></shared-key></radius-ip-address></index>
>	config	radius	auth	disable <index></index>
>	config	radius	auth	retransmit-timeout <index> <timeout-seconds></timeout-seconds></index>
>	config	radius	auth	enable <index></index>

WLAN

GUI:

Stap 1. Open de GUI van de WLC en navigeer naar **WLAN's > Nieuw >** Gebieden in de afbeelding.

،، ،،، ،، cısco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK	
WLANs	WLANs									
WLANS WLANS WLANS	Current Filt	ter: Not	ne [<u>Cha</u>	nge Filter] [Cl	<u>ear Filter]</u>			Create N	lew 🗸 Go]

Stap 2. Kies een naam voor de Service Set Identifier (SSID) en het profiel en klik vervolgens op Toepassen in de afbeelding.

W	/LANs > New			< Back	Apply
	Туре	WLAN V	_		
	Profile Name	profile-name			
	SSID	SSID-name			
	ID	2 ~			

CLI:

> config wlan create <id> <profile-name> <ssid-name>
Stap 3. Pas de RADIUS-server aan WLAN aan.

CLI:

> config wlan radius_server auth add <wlan-id> <radius-index> $\ensuremath{\mathsf{GUI}}$:

Navigeer naar **Security > AAA-servers** en kies de gewenste RADIUS-server en klik vervolgens op **Toepassen** zoals in de afbeelding.

WLANs > Edit 'ise-prof'	< Back	Apply
General Security QoS Policy-Mapping Advanced		
Layer 2 Layer 3 AAA Servers		
		^
Select AAA servers below to override use of default servers on this WLAN		
RADIUS Servers		
RADIUS Server Overwrite interface Enabled		
Authentication Servers Accounting Servers EAP Parameters		
✓ Enabled ✓ Enabled Enable		
Server 1 IP:172.16.15.8, Port:1812 V None V		
Server 2 None V None V		
Server 3 None V None V		
Server 4 None V None V		
Server 5 None V None V		
Server 6 None V None V		
RADIUS Server Accounting		
Interim Update		~
<	2	,

Stap 4. Verhoog optioneel de sessietijd.

CLI:

> config wlan session-timeout <wlan-id> <session-timeout-seconds> $\ensuremath{\mathsf{GUI}}$:

Navigeren in op **Geavanceerd > Time-out sessie inschakelen >** klik op **Toepassen** zoals in de afbeelding.

WLANs > E	dit 'ise-pro	of'						< Back	Арр	oly
General	Security	QoS	Policy-Mapping	Adva	nced					
Allow AA	A Override	Enabled	I		DHCP					
Coverag Detectio	e Hole n	🗹 Enabled	I		DHC	P Server		Override		
Enable S Timeout	ession	⊠ 2880 Sest	0 sion Timeou (secs)		DHC Assig	P Addr. 9nment		Required		
Aironet 1	E	⊡ _{Enabled}			OEAP					
Diagnos [.] <u>18</u>	tic Channel	Enabled			Split	: Tunnel	□ E	nabled		
Override ACL	Interface	IPv4 None	[Pv6 None ∨	Manage	ment Frame	e Protection	(MFP)		
Layer2 A URL ACL	kcl	None ~			MFP	Client Prote	ction 🛃 🛛 Op	tional 🗸		
P2P Bloc	king Action	Disabled	~		DTIM P	eriod (in bea	icon interva	ls)		
Client E>	⊲clusion ²	⊠ Enabled ⁶⁰ Tir	meout Value (secs)		802.	11a/n (1 - 2	255) 1]	
Maximu Clients 🕯	m Allowed	0			802. NAC	11b/g/n (1 ·	- 255) 1			
Static IP	Tunneling	m			NAC	State Non	• ~		>	~

Stap 5. Schakel het WLAN in.

CLI:

> config wlan enable <wlan-id>
GUI:

Navigeren in op Algemeen > Status > Ingeschakeld > Klik op Toepassen zoals in de afbeelding.

Ns > Edit 'ssid-n	ame'	< Back
neral Security	QoS Policy-Mapping Advanced	
Profile Name	ssid-name	
Туре	WLAN	
SSID	ssid-name	
Status	✓ Enabled	

Gebruikers aan gratis RADIUS-database toevoegen

Standaard klanten gebruiken PEAP-protocollen, maar freeRadius ondersteunt andere methoden (die niet in deze gids worden behandeld).

Stap 1. Bewerk het bestand/enz/raddb/gebruikers.

[root@tac-mxwireless ~] # nano /etc/raddb/users

Stap 2. Onder in het bestand voegt u de gebruikersinformatie toe. In dit voorbeeld is **user1** de gebruikersnaam en **Cisco123** het wachtwoord.

user1 Cleartext-Password := <Cisco123>

Stap 3. Start FreeRadius opnieuw.

[root@tac-mxwireless ~]# systemctl restart radiusd.service

Certificaten op gratisRADIUS

FreeRADIUS wordt geleverd met een CA-certificaat (standaard certificeringsinstantie) en een apparaatcertificaat dat is opgeslagen in het pad/etc/raddb/certs. De naam van deze certificaten is ca.pem en server.pem. server.pem is het certificaat dat klanten ontvangen terwijl ze door het authenticatieproces gaan . Als u een ander certificaat voor MAP-verificatie moet toewijzen, kunt u deze eenvoudigweg verwijderen en de nieuwe certificaten in hetzelfde pad met exact dezelfde naam opslaan.

Apparaatconfiguratie

Configureer een laptop van Windows om verbinding te maken met een SSID met 802.1xverificatie en PEAP/MS-CHAP (Microsoft versie van het Challenge-Handshake Authentication Protocol) versie 2.

Om het WLAN-profiel op de Windows-machine te maken, zijn er twee opties:

- 1. Installeer het zelf-ondertekende certificaat op de machine om de gratis RADIUS-server te valideren en te vertrouwen teneinde de verificatie te voltooien
- Bypass de validatie van de RADIUS-server en trust elke RADIUS-server die gebruikt wordt om de verificatie uit te voeren (niet aanbevolen, omdat deze een beveiligingsprobleem kan worden). De configuratie voor deze opties wordt uitgelegd op de configuratie van het Eindapparaat - Maak het WLAN-profiel.

FreeRADIUS-certificaat importeren

Als u de standaardcertificaten gebruikt die op freeRADIUS zijn geïnstalleerd, volgt u deze stappen om het EAP-certificaat van de gratis RADIUS-server in het eindapparaat te importeren.

Stap 1. Haal het graf van FreeRadius:

[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

----BEGIN CERTIFICATE-----

MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb21ld2hlcmUxFTAT BqNVBAoTDEV4YW1wbGUqSW5jLjEqMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydG1maWNhdGUgQXV0aG9yaXR5MB4X DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3 DQEBAQUAA4IBDwAwqqEKAoIBAQC0vJ53NN7J9vhpKhcB3B00XLpeQFWjqolQOB9F /8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyz18sKi5H42GU Eu6GDw1YJvhHn4rVC36OZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp gwNNZ7X5US0FcjuuOtpJJ3hfQ8K6uXjEWPOkDE0DAnqp4/n9AgMBAAGjggE0MIIB MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU ysFNRZKpAlcFCEgwdOPVGV0waLGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD VQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs ZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGx1LmNvbTEmMCQGA1UE AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADqqEBACsPR2jiOFXnTsK4 1wnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY Z6cNjx8+aYQIcsRIyqA11XMOBwIXo141TOmoODdgfX951poLwgktRLkv17Y7owsz ChYDO++H7Iewsxx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbBOxgkLiFJ5+GFbfLh a0HBHZWhTKvffbr62mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO RUvDhfE=

-----END CERTIFICATE-----Stap 2. Kopieer en plak de uitvoer van de vorige stap naar een tekstbestand en wijzig de extensie naar .crt

Stap 3. Dubbelklik op het bestand en selecteer **installatieprogramma...** zoals in de afbeelding wordt weergegeven.

Certificate
General Details Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: Example Certificate Authority
Issued by: Example Certificate Authority
Valid from 3/ 31/ 2017 to 5/ 30/ 2017
Install Certificate Issuer Statement
ок

Stap 4. Installeer het certificaat in de winkel **Trusted Root-certificeringsinstanties** zoals in de afbeelding.

Certificate Import Wizard	8
Certificate Store Certificate stores are system areas where certific	ates are kept.
Windows can automatically select a certificate sto the certificate.	re, or you can specify a location for used on the type of certificate
Place all certificates in the following store	
Certificate store:	Browse
Select Certificate Store	
Select the certificate store you want to use.	
Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Intrusted Certificates Intrusted Cert	Back Next > Cancel
OK Cancel	ОК

WLAN-profiel maken

Stap 1. Klik met de rechtermuisknop op het pictogram Start en selecteer **het bedieningspaneel** zoals in de afbeelding.

Programs and Features
Mobility Center
Power Options
Event Viewer
System
Device Manager
Network Connections
Disk Management
Computer Management
Command Prompt
Command Prompt (Admin)
Task Manager
Control Panel
File Explorer
Search
Run
Shut down or sign out
Desktop
🏭 ア に」」 🖡 Downl 🦉 Networ 🦅

Stap 2. Navigeer naar Netwerk en internet > Netwerk- en Sharing Center> klik op Een nieuwe verbinding of een netwerk instellen zoals in de afbeelding.

😫 Network and Sharing Center							
🔶 🚽 🗸 🛧 💆 > Control Pa	🗧 🔿 🗸 🛧 💐 > Control Panel > Network and Internet > Network and Sharing Center						
Control Panel Home View your basic network information and set up connections							
Change adapter settings							
Change advanced sharing settings	cisco.com Domain network	Access type: Internet Connections: <i>Iternet</i>					
	Change your networking settings Set up a new connection or net Set up a broadband, dial-up, or Troubleshoot problems Diagnose and repair network provide	work VPN connection; or set up a router or access point. roblems, or get troubleshooting information.					

Stap 3. Selecteer **Handmatig verbinding maken met een draadloos netwerk** en klik op Volgende zoals in de afbeelding.

	-		×
🔶 🛬 Set Up a Connection or Network			
Choose a connection option			
Set up a broadband or dial-up connection to the Internet.			
Set up a new network			
Set up a new router or access point.			
Manually connect to a wireless network Connect to a hidden network or create a new wireless profile.			
Connect to a workplace			
Set up a dial-up or VPN connection to your workplace.			
			_
	Next	Can	cel

Stap 4. Voer de informatie in met de naam van de SSID en het beveiligingstype WAP2-Enterprise en klik op **Volgende** zoals in de afbeelding.

÷	Se Manually connect to	a wireless network		-		×
	Enter information	or the wireless network you want to	add			
	Network name:	SSID-name				
	Security type:	WPA2-Enterprise ~				
	Encryption type:	AES				
	Security Key:	Hide o	characters			
	Start this connecti	on automatically				
	Connect even if th Warning: If you se	e network is not broadcasting lect this option, your computer's privacy might b	ve at risk.			
			Nex	t	Can	cel

Stap 5. Selecteer **Wijzig de verbindingsinstellingen** om de configuratie van het WLAN-profiel aan te passen zoals in de afbeelding.

	-		\times
 Manually connect to a wireless network 			
Successfully added ise-ssid			
→ Change connection settings Open the connection properties so that I can change the settings			
open the connection properties so that i can change the settings.			
		Clo	se

Stap 6. Navigeer naar het tabblad **Security** en klik op **Instellingen** zoals in de afbeelding.

ise-ssid Wireless Ne	twork Properties			×
Connection Security				
Security type:	WPA2-Enterprise		\sim	
Encryption type:	AES		\sim	
Choose a network aut	hentication method:		_	
Microsoft: Protected I	Microsoft: Protected EAP (PEAP) Settings			
Remember my cre time I'm logged or	dentials for this conne 1	ction each		
Advanced settings				
		ОК	Car	ncel

Stap 7. Kies of de RADIUS-server al dan niet gevalideerd is.

Zo ja, schakelt u **de identiteit van de server in door het certificaat te valideren** en van de **Trusted Root-certificeringsinstanties:** Selecteer het zelf-ondertekende certificaat van FreeRADIUS.

Nadat u **mijn bestandsnaam en wachtwoord voor** aanmelding **door Windows automatisch instellen** en uitschakelen **gebruikt...** klikt u vervolgens op **OK** zoals in de afbeeldingen wordt weergegeven.

Protected EAP Properties	\times				
When connecting:					
Verify the server's identity by validating the certificate					
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):					
Trusted Root Certification Authorities:					
Eggille & Cleftel Inner an Eugille 19 Still Associated and Inner als Eugille 19 Still Associated and Inner als Eugline and the second associated and the second associated	^				
Example Certification Authority					
	~				
Notifications before connecting: Tell user if the server name or root certificate isn't specified	~				
Select Authentication Method:					
Secured password (EAP-MSCHAP v2) Configure	e				
Disconnect if server does not present cryptobinding TLV					
Enable Identity Privacy					
OK Cance					
OK Cance	<u> </u>				
EAP MSCHAPv2 Properties ×					
When connecting:					

Stap 8. Configureer de gebruikersreferenties.

ΟK

Automatically use my Windows logon name and password (and domain if any).

Cancel

Als u weer terug bent op het tabblad Security, selecteert u **Geavanceerde instellingen**, specificeert u de verificatiemodus als **gebruikersverificatie** en slaat u de aanmeldingsgegevens op die in gratisRADIUS zijn ingesteld om de gebruiker voor authentiek te verklaren, zoals in de afbeeldingen wordt weergegeven.

ise-ssid Wireless Ne	twork Propertie	s		×		
Connection Security						
Security type:	WPA2-Enterprise		\sim			
Encryption type:	AES		\sim			
Choose a network au	thentication method:					
Microsoft: Protected	EAP (PEAP)	✓ Settin	ngs			
Remember my cro time I'm logged o	Remember my credentials for this connection each time I'm logged on					
Advanced settings						
		ОК	Cano	el		

Advanced settings		×
802.1X settings 802.11 settings		
Specify authentication mode:		
User authentication	Save cr	edentials
Delete credentials for all users		
Enable single sign on for this netw	ork	
Perform immediately before us	ser logon	
O Perform immediately after use	r logon	
Maximum delay (seconds):	10	*
Allow additional dialogs to be o sign on	displayed during	single
 This network uses separate vir and user authentication 	tual LANs for ma	chine
	OK	Cancel
Windows Security		
Save credentials		
Saving your crodentials allows	VOUR COMPANY	tor to correc

when you're not logged on (for example, to download updates).	

 \times

ahaha	user1		
cisco	•••••••		
		OK	Cancel

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Verificatieproces op WLC

Start de volgende opdrachten om het verificatieproces voor een bepaalde gebruiker te controleren:

> debug client <mac-add-client> > debug dot1x event enable > debug dot1x aaa enable

Gebruik het gereedschap Draadloze debug-analyzer voor een makkelijke manier om debugclientuitgangen te lezen:

Draadloze debug Analyzer

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.