# 802.1x konfigurieren - PEAP mit FreeRadius und WLC 8.3

# Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Netzwerkdiagramm Installieren von httpd Server und MariaDB Installieren von PHP 7 auf CentOS 7 Installation von FreeRADIUS **FreeRADIUS** WLC als AAA-Client (Authentication, Authorization, and Accounting) auf FreeRADIUS FreeRADIUS als RADIUS-Server auf WLC **WLAN** Hinzufügen von Benutzern zur freienRADIUS-Datenbank Zertifikate auf freeRADIUS Endgerätekonfiguration FreeRADIUS-Zertifikat importieren WLAN-Profil erstellen Überprüfen Authentifizierungsprozess in WLC Fehlerbehebung

# Einführung

In diesem Dokument wird beschrieben, wie Sie ein Wireless Local Area Network (WLAN) mit 802.1x-Sicherheit und Protected Extensible Authentication Protocol (PEAP) als Extensible Authentication Protocol (EAP) einrichten. FreeRADIUS wird als externer RADIUS-Server (Remote Authentication Dial-In User Service) verwendet.

# Voraussetzungen

#### Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- Linux
- Vim-Editor
- AireOS Wireless LAN Controller (WLCs)

**Hinweis**: Dieses Dokument soll den Lesern ein Beispiel für die Konfiguration geben, die auf einem freien RADIUS-Server für die PEAP-MS-CHAPv2-Authentifizierung erforderlich ist. Die in diesem Dokument vorgestellte Konfiguration des freeRADIUS-Servers wurde im Labor getestet und als erwartungsgemäß funktioniert. Das Cisco Technical Assistance Center (TAC) unterstützt keine freie RADIUS-Serverkonfiguration.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- CentOS7 oder Red Hat Enterprise Linux 7 (RHEL7) (empfohlen: 1 GB RAM und mindestens 20 GB HDD)
- WLC 5508 v8.3
- MariaDB (MySQL)
- FreeRADIUS
- PHP 7

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# Konfigurieren

#### Netzwerkdiagramm



Schritt 1: Führen Sie diese Befehle aus, um den httpd-Server und MariaDB zu installieren.

[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
Schritt 2: Starten und aktivieren Sie den HTTP- (Apache) und den MariaDB-Server.

[root@tac-mxwireless ~]# systemctl enable httpd [root@tac-mxwireless ~]# systemctl start httpd [root@tac-mxwireless ~]# systemctl start mariadb [root@tac-mxwireless ~]# systemctl enable mariadb Schritt 3: Konfigurieren Sie die anfänglichen MariaDB-Einstellungen, um diese zu sichern.

[root@tac-mxwireless ~] #mysql\_secure\_installation

**Hinweis**: Führen Sie alle Teile dieses Skripts aus. Es wird für alle MariaDB-Server empfohlen, die in der Produktion verwendet werden. Lesen Sie jeden Schritt sorgfältig durch.

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! Schritt 4: Konfigurieren Sie die Datenbank für freeRADIUS (verwenden Sie dasselbe Kennwort, das in Schritt 3 konfiguriert wurde).

[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

#### Installieren von PHP 7 auf CentOS 7

[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

#### Installation von FreeRADIUS

Schritt 1: Führen Sie diesen Befehl aus, um FreeRADIUS zu installieren.

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

Schritt 2: Machen Sie radius.service starte nach mariadb.service.

Führen Sie diesen Befehl aus:

[root@tac-mxwireless ~]# vim /etc/systemd/system/multi-user.target.wants/radiusd.service
Fügen Sie im Abschnitt [Einheit] einen Posten hinzu:

After=mariadb.service

Der Abschnitt [Einheit] muss wie folgt aussehen:

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

Schritt 3: Starten und aktivieren Sie fretilus, um beim Hochfahren zu starten.

[root@tac-mxwireless ~]# systemctl start radiusd.service [root@tac-mxwireless ~]# systemctl enable radiusd.service Schritt 4: Aktivieren Sie die Firewall aus Sicherheitsgründen.

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

Schritt 5: Fügen Sie der Standardzone permanente Regeln hinzu, um HTTP-, HTTPS- und Radius-Dienste zuzulassen.

[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius'
[root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success
Schritt 6: Laden Sie die Firewall neu, damit die Änderungen wirksam werden.

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

#### FreeRADIUS

Führen Sie die folgenden Schritte aus, um FreeRADIUS für die Verwendung von MariaDB zu konfigurieren.

Schritt 1: Importieren Sie das RADIUS-Datenbankschema, um die RADIUS-Datenbank zu füllen.

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

Schritt 2: Erstellen Sie unter **/etc/raddb/mods-enabled** einen Soft Link für Structured Query Language (SQL).

[root@tac-mxwireless ~]# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/ Schritt 3: Konfigurieren Sie das SQL-Modul /raddb/mods-available/sql, und ändern Sie die Datenbankverbindungsparameter in Ihre Umgebung.

[root@tac-mxwireless ~]# vim /etc/raddb/mods-available/sql
Der SQL-Abschnitt muss ähnlich aussehen.

sql {

```
driver = "rlm_sql_mysql"
dialect = "mysql"
```

# Connection info:

server = "localhost"

Schritt 4: Ändern Sie das Gruppenrecht von /etc/raddb/mods-enabled/sql in radiusd.

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

#### WLC als AAA-Client (Authentication, Authorization, Accounting) auf FreeRADIUS

Schritt 1: Bearbeiten Sie /etc/raddb/clients.conf, um den gemeinsamen Schlüssel für WLC festzulegen.

[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf Schritt 2: Fügen Sie unten die IP-Adresse des Controllers und den gemeinsamen Schlüssel hinzu.

client{ secret = shortname = }

Benutzeroberfläche:

Schritt 1: Öffnen Sie die GUI des WLC, und navigieren Sie zu SECURITY > RADIUS > Authentication > New (SICHERHEIT > RADIUS > Authentifizierung > Neu), wie im Bild gezeigt.

սիսիս		Sa <u>v</u> e Configuration   <u>P</u> ing   Logout   <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	<mark>A</mark> <u>H</u> ome
Security	RADIUS Authentication Servers	Apply New
▼ AAA General	Auth Called Station ID Type AP MAC Address:SSID 🗸	
<ul> <li>RADIUS Authentication</li> </ul>	Use AES Key Wrap 🛛 (Designed for FIPS customers and requires a key wrap compliant RADIUS server)	
Accounting Fallback	MAC Delimiter Hyphen V	
DNS	Framed MTU 1300	

#### Schritt 2: Füllen Sie die RADIUS-Serverinformationen aus, wie im Bild gezeigt.

RADIUS Authentication Servers > 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 fo	r 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:

۰.	/1				
>	config	radius	auth	enable <index></index>	
>	config	radius	auth	etransmit-timeout <index> <timeout-seco< th=""><th>nds&gt;</th></timeout-seco<></index>	nds>
>	config	radius	auth	lisable <index></index>	
>	config	radius	auth	dd <index> <radius-ip-address> 1812 asc</radius-ip-address></index>	ii <shared-key></shared-key>

#### WLAN

Benutzeroberfläche:

Schritt 1: Öffnen Sie die Benutzeroberfläche des WLC, und navigieren Sie zu WLANs > Create New > Goas (Neues > Ziel erstellen), wie im Bild gezeigt.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANS
<ul> <li>WLANS</li> <li>WLANS</li> <li>Advanced</li> </ul>	Current Filter: None [Change Filter] [Clear Filter] Create New Create New

Schritt 2: Wählen Sie einen Namen für den Service Set Identifier (SSID) und das Profil aus, und klicken Sie dann wie im Bild gezeigt auf Anwenden.

WLANs > New		< Back	Apply
Туре	WLAN ~		
Profile Name	profile-name		
SSID	SSID-name		
ID	2 ~		

CLI:

> config wlan create <id> <profile-name> <ssid-name>
Schritt 3: Weisen Sie dem WLAN den RADIUS-Server zu.

CLI:

> config wlan radius\_server auth add <wlan-id> <radius-index>
Benutzeroberfläche:

Navigieren Sie zu **Sicherheit > AAA-Server**, und wählen Sie den gewünschten RADIUS-Server aus. Klicken Sie anschließend wie im Bild auf **Apply**.

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		^
Enabled Enabled Enable		
Server 1 IP:172.16.15.8, Port:1812 🗸 None 🗸		
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 🗹 Interim Interval 🛛 Seconds	2	>

Schritt 4: Erhöhen Sie optional die Sitzungszeit.

CLI:

> config wlan session-timeout <wlan-id> <session-timeout-seconds>
Benutzeroberfläche:

Navigieren Sie zu **Erweitert > Sitzungs-Timeout aktivieren >** klicken Sie auf **Übernehmen**, wie im Bild gezeigt.

WL	.ANs > Edit 'ise-p	rof			SBack	Apply
	General Security	y QoS Policy-Mapping	g Adva	inced		
	Allow AAA Override	Enabled		DHCP	_	
	Coverage Hole Detection	🗹 Enabled		DHCP Server	Override	
	Enable Session Timeout	Session Timeou (secs	)	DHCP Addr. Assignment	Required	
	Aironet IE	Enabled		OEAP		
	Diagnostic Channel <u>18</u>	Enabled		Split Tunnel	Enabled	
	Override Interface ACL	IPv4 None 🗡	IPv6 None ∨	Management Frame	e Protection (MFP)	
	Layer2 Ad	None V				
	URL ACL	None 🗸		MFP Client Prote	ction 🖣 Optional 🗸	
	P2P Blocking Action	Disabled $\vee$		DTIM Period (in bea	acon intervals)	
	Client Exclusion ²	Enabled Timeout Value (secs)		802.11a/n (1 - 2	255) 1	
	Maximum Allowed Clients <sup>g</sup>	0		802.11b/g/n (1 · NAC	- 255) 1	
<	Static IP Tunneling	□		NAC State Non	•	>

Schritt 5: Aktivieren Sie das WLAN.

CLI:

> config wlan enable <wlan-id>
Benutzeroberfläche:

Navigieren Sie zu **Allgemein > Status > Aktivieren > Klicken Sie auf Übernehmen**, wie im Bild gezeigt.

ANs > Edit 'ssid-na	me'	< Back
eneral Security	QoS Policy-Mapping Advanced	
Profile Name	ssid-name	
Туре	WLAN	
SSID	ssid-name	
Status		

#### Hinzufügen von Benutzern zur freienRADIUS-Datenbank

Standardmäßig verwenden Clients PEAP-Protokolle. FreeRadius unterstützt jedoch andere Methoden (nicht in diesem Handbuch behandelt).

Schritt 1: Bearbeiten Sie die Datei /etc/raddb/users.

Beispiel ist user1 der Benutzername und Cisco123 das Kennwort.

user1 Cleartext-Password := <Cisco123> Schritt 3: Starten Sie FreeRadius neu.

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

#### Zertifikate auf freeRADIUS

FreeRADIUS ist mit einem standardmäßigen Zertifikat der Zertifizierungsstelle (Certificate Authoritiy, CA) und einem Gerätezertifikat ausgestattet, das im Pfad /etc/raddb/certs gespeichert ist. Der Name dieser Zertifikate lautet ca.pem und server.pem. server.pem ist das Zertifikat, das Clients erhalten, während sie den Authentifizierungsprozess durchlaufen. Wenn Sie ein anderes Zertifikat für die EAP-Authentifizierung zuweisen müssen, können Sie diese einfach löschen und die neuen Zertifikate im gleichen Pfad mit diesem exakten Namen speichern.

#### Endgerätekonfiguration

Konfigurieren Sie einen Laptop-Windows-Computer für die Verbindung mit einer SSID mit 802.1x-Authentifizierung und PEAP/MS-CHAP (Microsoft-Version des Challenge-Handshake Authentication Protocol) Version 2.

Zum Erstellen des WLAN-Profils auf dem Windows-Computer gibt es zwei Optionen:

- 1. Installieren Sie das selbstsignierte Zertifikat auf dem Computer, um den FreeRADIUS-Server zu validieren und zu vertrauen, um die Authentifizierung abzuschließen.
- Umgehen Sie die Validierung des RADIUS-Servers, und vertrauen Sie jedem RADIUS-Server, der zur Durchführung der Authentifizierung verwendet wird (nicht empfohlen, da dies zu einem Sicherheitsproblem werden kann). Die Konfiguration dieser Optionen wird in der Endgerätekonfiguration - WLAN-Profil erstellen - erläutert.

#### FreeRADIUS-Zertifikat importieren

Wenn Sie die auf freeRADIUS installierten Standardzertifikate verwenden, führen Sie die folgenden Schritte aus, um das EAP-Zertifikat vom freeRADIUS-Server in das Endgerät zu importieren.

Schritt 1: Laden Sie das Zertifikat von FreeRadius herunter:

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

----BEGIN CERTIFICATE----

MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEw1Tb21ld2hlcmUxFTAT BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X DTE3MDMzMTExMTIxN1oXDTE3MDUzMDExMTIxN1owgZMxCzAJBgNVBAYTAkZSMQ8w DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3 DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B00XLpeQFWjqolQOB9F /8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyzI8sKi5H42GU Eu6GDw1YJvhHn4rVC36OZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp qwNNZ7X5US0FcjuuOtpJJ3hf08K6uXjEWPOkDE0DAnqp4/n9AqMBAAGjqqE0MIIB MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU ysFNRZKpAlcFCEgwdOPVGV0waLGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD VQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs ZSBJbmMuMSAwHqYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQGA1UE  ${\tt AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV} a {\tt AxMdRXhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV} a {\tt AxMdRXhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV} a {\tt AxMdRXhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV} a {\tt AxMdRXhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV a {\tt AxMdRXhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV a {\tt AxMdRXhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV a {\tt AxMdRXhbA}A {\tt AxMdRXhbXBA} a {\tt AxMdRXhbA}A {\tt AxMdRA} {\tt AxMdRXhbA}A {\tt AxMdRA} {\tt AxMdRA}$ HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4 1wnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY Z6cNjx8+aYQIcsRIyqA11XMOBwIXo141TOmoODdgfX951poLwgktRLkv17Y7owsz ChYDO++H7Iewsxx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbBOxqkLiFJ5+GFbfLh a0HBHZWhTKvffbr62mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO RUvDhfE=

----END CERTIFICATE----

Schritt 2: Kopieren Sie die Ausgabe des vorherigen Schritts, fügen Sie sie in eine Textdatei ein, und ändern Sie die Erweiterung in .crt.

Schritt 3: Doppelklicken Sie auf die Datei, und wählen Sie **Zertifikat installieren aus...** wie im Bild gezeigt.



Schritt 4: Installieren Sie das Zertifikat im Speicher **der vertrauenswürdigen Stammzertifizierungsstellen**, wie im Bild gezeigt.

Certificate Import Wizard	8				
Certificate Store Certificate stores are system areas where certificates are kept.					
Windows can automatically select a certificate store, or you can specify a location for the 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 Show physical stores Back	< Next > Cancel				
OK Cancel	ОК				

#### WLAN-Profil erstellen

Schritt 1: Klicken Sie mit der rechten Maustaste auf das Symbol Start, und wählen Sie **Systemsteuerung** aus, wie im Bild gezeigt.

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
👔 אין

Schritt 2: Navigieren Sie zu Netzwerk und Internet > Netzwerk- und Freigabecenter> klicken Sie auf Neue Verbindung oder neues Netzwerk einrichten, wie im Bild gezeigt.



Schritt 3: Wählen Sie **Manuelle Verbindung mit einem Wireless-Netzwerk** aus, und klicken Sie im Bild auf Nextas.

	-		×
🔶 👙 Set Up a Connection or Network			
Choose a connection option			
Connect to the Internet Set up a broadband or dial-up connection to the Internet.			1
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.			
Set up a dial-up or VPN connection to your workplace.			
	Next	Can	cel

Schritt 4: Geben Sie die Informationen mit dem Namen der SSID und des Sicherheitstyps WPA2-Enterprise ein, und klicken Sie auf **Weiter**, wie im Bild gezeigt.

			-		×
÷	Manually connect to a	wireless network			
	Enter information f	or the wireless network you want to add			
	Network name:	SSID-name			
	Security type:	WPA2-Enterprise ~			
	Encryption type:	AES			
	Security Key.	Hide character	5		
	Start this connection	on automatically			
	Connect even if the Warning: If you set	e network is not broadcasting ect this option, your computer's privacy might be at risk			
		N	ext	Can	cel

Schritt 5: Wählen Sie **Verbindungseinstellungen ändern**, um die Konfiguration des WLAN-Profils wie im Bild gezeigt anzupassen.

	-		$\times$
<ul> <li>Manually connect to a wireless network</li> </ul>			
Successfully added ise-ssid			
-> Change connection settings			
Open the connection properties so that I can change the settings.			
		Cle	
		Cic	S.C.

Schritt 6: Navigieren Sie zur Registerkarte **Sicherheit**, und klicken Sie auf **Einstellungen** wie im Bild gezeigt.

ise-ssid Wireless Ne	etwork Properties			×
Connection Security				
Security type:	WPA2-Enterprise		$\sim$	
Encryption type:	AES		$\sim$	
Choose a network au	thentication method:			
Microsoft: Protected	EAP (PEAP) $\sim$	Settin	igs	
Remember my cro time I'm logged o	edentials for this connec n	tion each:		
Advanced settings	5			
		ОК	Ca	ncel

Schritt 7: Wählen Sie aus, ob der RADIUS-Server validiert wurde.

Falls ja, aktivieren Sie Verifizieren der Serveridentität durch Validieren des Zertifikats und von vertrauenswürdigen Stammzertifizierungsstellen: wählen Sie das selbstsignierte Zertifikat von freeRADIUS aus.

Wählen Sie anschließend **Configure** and disable **Automatisch use my Windows logon name and password...**, und klicken Sie dann wie in den Bildern gezeigt auf **OK**.

Protected EAP Properties	×
When connecting:	
Verify the server's identity by validating the certificate	
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):	
Trusted Root Certification Authorities:	
Degoto & Oktob topo da	^
Lag = 1.5 Strandon de 1.5	
Example Certification Authority	
Contract Dopt Contribution for the	
E. a. March Letterinder in NOT Step (1971)	
	~
Notifications before connecting:	
Tell user if the server name or root certificate isn't specified	~
Select Authentication Method:	
Secured password (EAP-MSCHAP v2) Configu	re
Enable Fast Reconnect	
Disconnect if server does not present cryptobinding TLV	
Enable Identity Privacy	
OK Cano	el
EAP MSCHAPv2 Properties X	
When connecting:	
Automatically use my Windows logon name and password (and domain if any).	

Schritt 8: Konfigurieren Sie die Benutzeranmeldeinformationen.

Cancel

οк

Wenn Sie wieder zur Registerkarte Sicherheit zurückkehren, wählen Sie **Erweiterte Einstellungen aus**, geben Sie den Authentifizierungsmodus als **Benutzerauthentifizierung** an, und speichern Sie die Anmeldeinformationen, die auf freeRADIUS konfiguriert wurden, um den Benutzer zu authentifizieren, wie in den Bildern gezeigt.

ise-ssid Wireless Ne	twork Propert	ies		×
Connection Security				
Security type:	WPA2-Enterprise		$\sim$	
Encryption type:	AES		$\sim$	
Choose a network au	thentication metho	d:		
Microsoft: Protected	EAP (PEAP)	✓ Se	ttings	
Remember my cro time I'm logged o	edentials for this co n	onnection eac	:h	
Advanced cetting				
Advanced secongs	,			
		OK	Can	cel

.1X settings 80	02.11 settings			
Specify auth	entication mode:			
User auther	itication	Y Save o	redentials	
Delete cr	edentials for all use	rs		
Enable single	e sign on for this ne	twork		
Perform	immediately before	user logon		
O Perform	immediately after u	ser logon		
Maximum d	elay (seconds):	10	*	
Allow ad sign on	ditional dialogs to b	e displayed during	single	
This network	vork uses separate	virtual LANs for ma	chine	
		OK	Cancel	
		OK	Cancel	
ndows Sea	urity	OK	Cancel	
ndows Sec	urity	ОК	Cancel	
ndows Sec ave crede	urity	OK	Cancel	
ndows Sec ave crede aving your cr	urity entials redentials allow	OK vs your compt	Cancel uter to conn	ect to the n
ndows Sec ave crede aving your cr hen you're r	urity entials redentials allow rot logged on (	ok vs your compt (for example, 1	Cancel uter to connecto download	ect to the n d updates).
ndows Sec ave crede aving your cr hen you're r	urity entials edentials allow iot logged on (	OK vs your compt (for example, t	Cancel uter to conne to download	ect to the n d updates).
ndows Sec ave crede aving your co hen you're r	urity entials redentials allow rot logged on (	OK vs your compt (for example, t	Cancel uter to conne to download	ect to the n
ndows Sect ave crede aving your co hen you're n	urity entials redentials allow tot logged on ( user1	OK vs your compt (for example, t	Cancel uter to conne to download	ect to the n d updates).
ndows Sect ave crede aving your cr hen you're r	urity entials redentials allow not logged on ( user1	OK vs your compt (for example, f	Cancel uter to conne to download	ect to the n

# Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

OK

 $\times$ 

Cancel

### Authentifizierungsprozess in WLC

Führen Sie die folgenden Befehle aus, um den Authentifizierungsprozess für einen bestimmten Benutzer zu überwachen:

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

Mit dem Wireless Debuganalyzer-Tool können Sie Debug-Clientausgaben leicht lesen:

Wireless-Debug-Analyzer

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.