Configurazione di 802.1x - PEAP con FreeRadius e WLC 8.3

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Configurazione Esempio di rete Installare il server httpd e MariaDB Installare PHP 7 su CentOS 7 Installa FreeRADIUS **FreeRADIUS** WLC as Authentication, Authorization, and Accounting (AAA) Client su FreeRADIUS FreeRADIUS come server RADIUS su WLC **WLAN** Aggiungi utenti al database freeRADIUS Certificati su freeRADIUS Fine configurazione dispositivo Importa certificato FreeRADIUS Crea profilo WLAN Verifica Processo di autenticazione su WLC Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare una rete WLAN (Wireless Local Area Network) con sicurezza 802.1x e PEAP (Protected Extensible Authentication Protocol) come EAP (Extensible Authentication Protocol). FreeRADIUS viene utilizzato come server RADIUS (Remote Authentication Dial-In User Service) esterno.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Linux
- Editor Vim
- Controller LAN wireless (WLC) AireOS

Nota: questo documento ha lo scopo di fornire ai lettori un esempio della configurazione richiesta su un server freeRADIUS per l'autenticazione PEAP-MS-CHAPv2. La configurazione del server freeRADIUS esposta in questo documento è stata testata in laboratorio e ha dimostrato di funzionare come previsto. Il Cisco Technical Assistance Center (TAC) non supporta la configurazione del server RADIUS gratuito.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CentOS7 o Red Hat Enterprise Linux 7 (RHEL7) (si consiglia 1 GB di RAM e almeno 20 GB di disco rigido)
- WLC 5508 v8.3
- MariaDB (MySQL)
- FreeRADIUS
- PHP 7

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Installare il server httpd e MariaDB

Passaggio 1. Eseguire questi comandi per installare il server httpd e MariaDB.

[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 Passaggio 2. Avviare e abilitare httpd (Apache) e il server MariaDB.

[root@tac-mxwireless ~]# systemctl enable httpd [root@tac-mxwireless ~]# systemctl start httpd [root@tac-mxwireless ~]# systemctl start mariadb [root@tac-mxwireless ~]# systemctl enable mariadb
Passaggio 3. Configurare le impostazioni iniziali di MariaDB per proteggerlo.

[root@tac-mxwireless ~] #mysql_secure_installation

Nota: Esegue tutte le parti di questo script. È consigliato per tutti i server MariaDB in produzione. Leggere attentamente ogni passaggio.

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! Passaggio 4. Configurare il database per freeRADIUS (utilizzare la stessa password configurata nel passaggio 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

Installare PHP 7 su 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

Installa FreeRADIUS

Passaggio 1. Eseguire questo comando per installare FreeRADIUS.

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

Passaggio 2. Impostare l'avvio di radius.service dopo mariadb.service.

Eseguire questo comando:

[root@tac-mxwireless ~]# vim /etc/systemd/system/multi-user.target.wants/radiusd.service
Aggiungere una riga nella sezione [unit]:

After=mariadb.service

La sezione [Unit] deve avere il seguente aspetto:

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

Passaggio 3. Avviare e abilitare freeradius all'avvio.

[root@tac-mxwireless ~]# systemctl start radiusd.service [root@tac-mxwireless ~]# systemctl enable radiusd.service Passaggio 4. Abilitare il firewall per la sicurezza.

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

Passaggio 5. Aggiungere regole permanenti alla zona predefinita per consentire i servizi http, https e radius.

[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius'
[root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success
Passaggio 6. Ricaricare il firewall per rendere effettive le modifiche.

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

FreeRADIUS

Per configurare FreeRADIUS per l'utilizzo di MariaDB, eseguire la procedura seguente.

Passaggio 1. Importare lo schema del database RADIUS per popolare il database RADIUS.

```
[root@tac-mxwireless ~]# mysql -u root -p radius < /etc/raddb/mods-
config/sql/main/mysql/schema.sql
Passaggio 2. Creare un collegamento soft per Structured Query Language (SQL) in
/etc/raddb/mods-enabled.
```

[root@tac-mxwireless ~]# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/ Passaggio 3. Configurare il modulo SQL /raddb/mods-available/sql e modificare i parametri di connessione al database per adattare l'ambiente.

[root@tac-mxwireless ~]# vim /etc/raddb/mods-available/sql La sezione SQL deve essere simile a questa.

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"
```

Passaggio 4. Modificare il diritto di gruppo di /etc/raddb/mods-enabled/sql in radiusd.

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

WLC come client di autenticazione, autorizzazione e accounting (AAA) su FreeRADIUS

Passaggio 1. Modificare /etc/raddb/clients.conf per impostare la chiave condivisa per WLC.

[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf Passaggio 2. In basso, aggiungere l'indirizzo IP del controller e la chiave condivisa.

client{ secret = shortname = }

FreeRADIUS come server RADIUS su WLC

GUI:

Passaggio 1. Aprire la GUI del WLC e selezionare **SECURITY > RADIUS > Authentication > New** (SICUREZZA > RADIUS > Autenticazione > Nuovo), come mostrato nell'immagine.

| սիսիս | | Sa <u>v</u> e Configuration <u>P</u> ing Lo <u>g</u> out <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 🛛 🗛 MAC Address:SSID 🚽 | |
| RADIUS Authentication | Use AES Key Wrap 🗌 (Designed for FIPS customers and requires a key wrap compliant RADIUS server) | |
| Accounting | MAC Delimiter Hyphen V | |
| DNS | Framed MTU 1300 | |

| Let a subscript the first succession in the | · · · · · · · · · · · · · · · · · · · | and a life in a second second second |
|---|---------------------------------------|--------------------------------------|
| Inserire le informazion | COME IIIIISTRATO | nell'immadine |
| | | non miniaquito. |
| | | |

| 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 fo | r FIPS customers and requires a key wrap compliant RADIUS server) |
| Port Number | 1812 | |
| Server Status | Enabled \sim | |
| Support for CoA | Disabled ${\scriptstyle \lor}$ | |
| Server Timeout | 10 seconds | 5 |
| 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>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>

WLAN

GUI:

Passaggio 1. Aprire la GUI del WLC e selezionare **WLAN > Create New >** Go (WLAN) come mostrato nell'immagine.

| cisco | MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK |
|--|--|
| WLANs | WLANS |
| WLANS WLANS Advanced | Current Filter: None [Change Filter] [Clear Filter] Create New Create New |

Passaggio 2. Scegliere un nome per l'SSID (Service Set Identifier) e il profilo, quindi fare clic su Applica come mostrato nell'immagine.

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

CLI:

> config wlan create <id> <profile-name> <ssid-name>
Passaggio 3. Assegnare il server RADIUS alla WLAN.

CLI:

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

Passare a **Sicurezza > Server AAA** e scegliere il server RADIUS desiderato, quindi fare clic su **Applica** come mostrato nell'immagine.

| 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 | | |
| | | |
| Authentication Servers Accounting Servers EAP Parameters | | |
| Enabled Enabled Enable | | |
| Server 1 [19:172.16.15.8, 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 Interim Interval Seconds | | ~ |
| < | 2 | > |
| | | |

Passaggio 4. Se necessario, aumentare il tempo della sessione.

CLI:

| > | config | wlan | session-timeout | <wlan-id></wlan-id> | <session-timeout-seconds></session-timeout-seconds> |
|---|--------|------|-----------------|---------------------|---|
| G | iUI: | | | | |

Selezionare **Avanzate > Abilita timeout sessione >** fare clic su **Applica** come mostrato nell'immagine.

| 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 ^g | 0 | | 802.11b/g/n (1 · NAC | - 255) 1 | |
| < | Static IP Tunneling | □ | | NAC State Non | • | > |

Passaggio 5. Abilitare la WLAN.

CLI:

```
> config wlan enable <wlan-id>
GUI:
```

Passare a Generale > Stato > Selezione abilitata > Fare clic su Applica come mostrato nell'immagine.

| /LANs > Edit 'ssid-na | me' | < Back |
|-----------------------|-----------------------------|--------|
| General Security | QoS Policy-Mapping Advanced | |
| | | |
| Profile Name | ssid-name | |
| Туре | WLAN | |
| SSID | ssid-name | |
| Status | ✓ Enabled | |

Aggiungi utenti al database freeRADIUS

Per impostazione predefinita i client utilizzano i protocolli PEAP, tuttavia freeRadius supporta altri metodi (non descritti in questa guida).

Passaggio 1. Modificare il file /etc/raddb/users.

Passaggio 2. Nella parte inferiore del file aggiungere le informazioni relative agli utenti.

Nell'esempio, user1 è il nome utente e Cisco123 la password.

user1 Cleartext-Password := <Cisco123> Passaggio 3. Riavviare FreeRadius.

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

Certificati su freeRADIUS

FreeRADIUS viene fornito con un certificato CA (Certification Authority) predefinito e un certificato di dispositivo archiviati nel percorso /etc/raddb/certs. I nomi di questi certificati sono ca.pem e server.pem. server.pem è il certificato ricevuto dai client durante il processo di autenticazione. Se è necessario assegnare un certificato diverso per l'autenticazione EAP, è sufficiente eliminarlo e salvare i nuovi certificati nello stesso percorso con lo stesso esatto nome.

Fine configurazione dispositivo

Configurare un computer portatile Windows per la connessione a un SSID con autenticazione 802.1x e PEAP/MS-CHAP (versione Microsoft del protocollo di autenticazione Challenge-Handshake) versione 2.

Per creare il profilo WLAN sul computer Windows, sono disponibili due opzioni:

- 1. Installare il certificato autofirmato nel computer per convalidare e considerare attendibile il server freeRADIUS per completare l'autenticazione
- Ignorare la convalida del server RADIUS e considerare attendibile qualsiasi server RADIUS utilizzato per eseguire l'autenticazione (scelta non consigliata, in quanto può diventare un problema di sicurezza). La configurazione di queste opzioni è spiegata in Configurazione del dispositivo terminale - Creazione del profilo WLAN.

Importa certificato FreeRADIUS

Se si utilizzano i certificati predefiniti installati in freeRADIUS, eseguire la procedura seguente per importare il certificato EAP dal server freeRADIUS nel dispositivo terminale.

Passaggio 1. Ottenere il certificato da FreeRadius:

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

----BEGIN CERTIFICATE----

MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEw1Tb21ld2hlcmUxFTAT BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh bXBsZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkB1eGFtcGxlLmNvbTEmMCQG A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3 DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B00XLpeQFWjqo1Q0B9F

| /8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyz18sKi5H42GU |
|--|
| ${\tt Eu6GDw1YJvhHn4rVC360ZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvC0S5QGn4X1elRS}$ |
| oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC |
| ay 6 dt G55 YQOH x Kasw H7/HJkLs K WhS4 Ym X LgJ X Cee Jqooqr + TEwy CDEa Fai X835 Jp Sin State Stat |
| gwNNZ7X5US0FcjuuOtpJJ3hfQ8K6uXjEWPOkDE0DAnqp4/n9AgMBAAGjggE0MIIB |
| ${\tt MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU}$ |
| ys FNRZKpAlcFCEgwdOPVGV0 wa LGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD |
| $\verbVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs$ |
| $\verb ZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQGA1UE $ |
| ${\tt AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV}$ |
| ${\tt HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j}$ |
| $b \verb+20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4$ |
| 1wnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV |
| mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY |
| Z6cNjx8+aYQIcsRIyqA1IXMOBwIXo141TOmoODdgfX951poLwgktRLkv17Y7owsz |
| ChYDO++H7Iewsxx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbBOxgkLiFJ5+GFbfLh |
| a0HBHZWhTKvffbr62mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO |
| RUvDhfE= |
| END CERTIFICATE |

Passaggio 2. Copiare e incollare l'output del passaggio precedente in un file di testo e modificare l'estensione in .crt

Passaggio 3. Fare doppio clic sul file e selezionare **Installa certificato...** come mostrato nell'immagine.



Passaggio 4. Installare il certificato nell'archivio Autorità di certificazione radice attendibili, come mostrato nell'immagine.

| 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. Automatically select the certificate store ba | 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 Show physical stores | Back Next > Cancel |
| OK Cancel | ОК |

Crea profilo WLAN

Passaggio 1. Fare clic con il pulsante destro del mouse sull'icona Start e selezionare **Pannello di controllo** come mostrato nell'immagine.

| | 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 |
| 1 | 👔 א נון 🖡 DownL 💇 Networ 👳 ו |

Passaggio 2. Selezionare Rete e Internet > Centro connessioni di rete e condivisione> fare clic su Configura nuova connessione o rete come mostrato nell'immagine.



Passaggio 3. Selezionare **Connetti manualmente a una rete wireless** e fare clic su Avanti come mostrato nell'immagine.

| | - | | × |
|---|------|-----|-----|
| 🔶 🛬 Set Up a Connection or Network | | | |
| | | | |
| Choose a connection option | | | |
| Connect to the Internet | | | 1 |
| 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 |

Passaggio 4. Immettere le informazioni con il nome del SSID e il tipo di protezione WPA2-Enterprise e fare clic su **Avanti** come mostrato nell'immagine.

| ~ | Se 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 V | | | |
| | Security Key: | Hide characte | rs | | |
| | Start this connection | on automatically | | | |
| | Connect even if th Warning: If you se | e network is not broadcasting lect this option, your computer's privacy might be at risk | ł. | | |
| | | N | lext | Can | cel |

Passaggio 5. Selezionare **Change connection settings** (Cambia impostazioni di connessione) per personalizzare la configurazione del profilo WLAN, come mostrato nell'immagine.

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

Passaggio 6. Passare alla scheda **Sicurezza** e fare clic su **Impostazioni**, come mostrato nell'immagine.

| ise-ssid Wireless Ne | twork Properties | | | × |
|--------------------------------------|--------------------------------|-----------|--------|----|
| Connection Security | | | | |
| | | | | |
| Security type: | WPA2-Enterprise | | \sim | |
| Encryption type: | AES | | \sim | |
| | | | | |
| | | | | |
| Choose a network au | thentication method: | | _ | |
| Microsoft: Protected | EAP (PEAP) 🛛 🗸 | Settin | gs | |
| Remember my cre time I'm logged o | edentials for this connec n | tion each | | |
| | | | | |
| | | | | |
| | | | | |
| Advanced settings | i | | | |
| | | | | |
| | | | | |
| | | | | |
| | | OK | Cano | el |

Passaggio 7. Scegliere se il server RADIUS è convalidato o meno.

In caso affermativo, abilitare Verifica dell'identità del server convalidando il certificato e da Autorità di certificazione radice attendibili: selezionare il certificato autofirmato di freeRADIUS.

Quindi selezionare **Configure** and disable **Automatically use my Windows logon name and password...**, quindi fare clic su **OK** come mostrato nelle immagini.

| 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: | _ |
| Diggline & Olefred Linder dat Diggline & Olefred Linder dat Diggline & State Association of States dat | ^ |
| Example Certification Authority | |
| La debande Cationadera a Metteria (CECC) La Cation de Catione Serviciones Serviciones | ~ |
| | |
| Tell user if the server name or root certificate isn't specified | ~ |
| Select Authentication Method: | |
| Secured password (EAP-MSCHAP v2) Configur | 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). | |

Passaggio 8. Configurare le credenziali utente.

Cancel

ΟK

Tornando alla scheda Protezione, selezionare **Impostazioni avanzate**, specificare la modalità di autenticazione come **Autenticazione utente** e salvare le credenziali configurate su freeRADIUS per autenticare l'utente, come mostrato nelle immagini.

| ise-ssid Wireless Ne | twork Propert | ies | | | × |
|--------------------------------------|-----------------------|----------|---------|------------|------|
| Connection Security | | | | | |
| | | | | | |
| Security type: | WPA2-Enterprise | | | \sim | |
| Encryption type: | AES | | | \sim | |
| | | | | | |
| | | | | | |
| Choose a network aut | thentication metho | d: | | | |
| Microsoft: Protected | EAP (PEAP) | \sim | Setting | <u>g</u> s | |
| Remember my cre time I'm logged o | edentials for this co | nnection | each | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Advanced settings | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | [| OK | (| Car | ncel |

| Advanced setting | gs | | × | |
|----------------------|--|------------------|----------|-------------------|
| 802.1X settings 80 | 02.11 settings | | | |
| Specify auth | entication mode: | | | |
| User auther | ntication ~ | Save creder | ntials | |
| Delete cr | redentials for all users | | _ | |
| Enable single | e sign on for this network | | | |
| Perform | immediately before user lo | gon | | |
| O Perform | immediately after user log | on | | |
| Maximum d | elay (seconds): | 10 | * | |
| Allow ad sign on | ditional dialogs to be displa | yed during singl | le | |
| This net and user | vork uses separate virtual l authentication | ANs for machin | e | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | OK | Cancel | |
| | | | | 1 |
| | | | | |
| Windows Sec | urity | | | |
| | | | | |
| Save crede | entials | | | |
| Saving your c | redentials allows you | ur computer | to conne | ct to the network |
| when you're r | not logged on (for e | kample, to d | lownload | updates). |
| | | | | |
| | | | | |
| | user1 | | | |
| ahaha | userr | | | |
| cisco | | | | |
| | | | | |
| | | | | |
| | | | | |

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

OK

×

Cancel

Processo di autenticazione su WLC

Per monitorare il processo di autenticazione per un utente specifico, eseguire i comandi seguenti:

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

Per leggere facilmente gli output dei client di debug, usare lo strumento Wireless debug analyzer:

Wireless Debug Analyzer

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.