Configurazione di 802.1x - PEAP con FreeRadius e WLC 8.3

Sommario

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

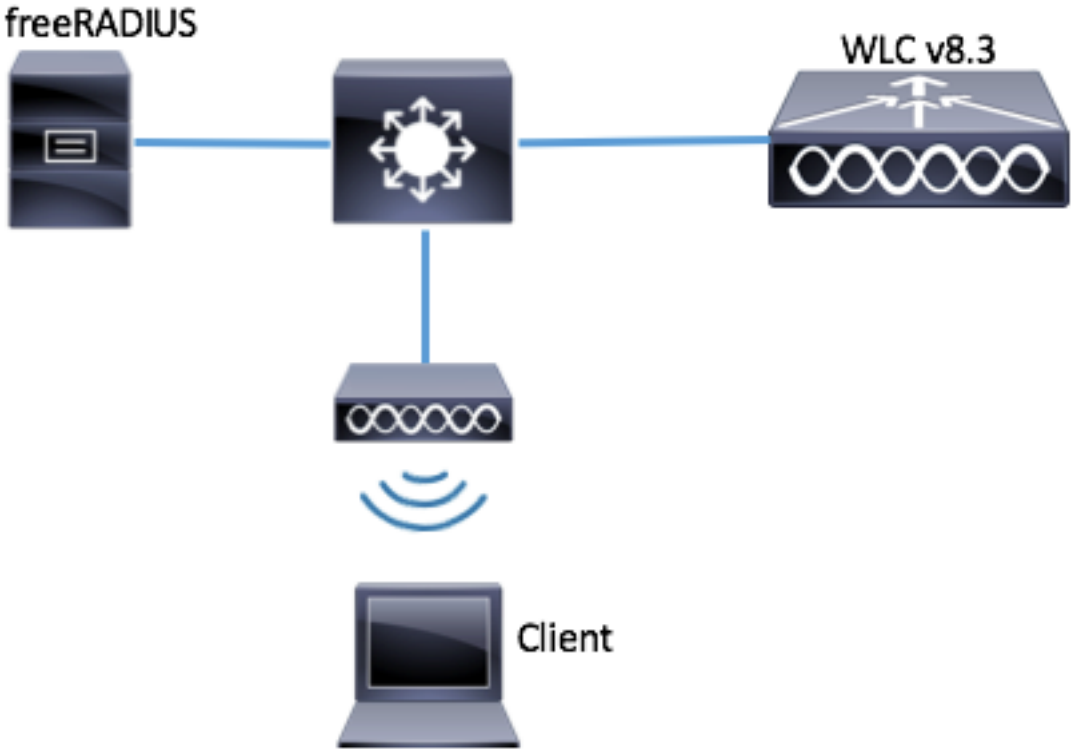
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 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

Passaggio 1. Eseguire questi comandi per installare PHP 7 su CentOS7.

```
[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 freeradius-
sqlite
```

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
```

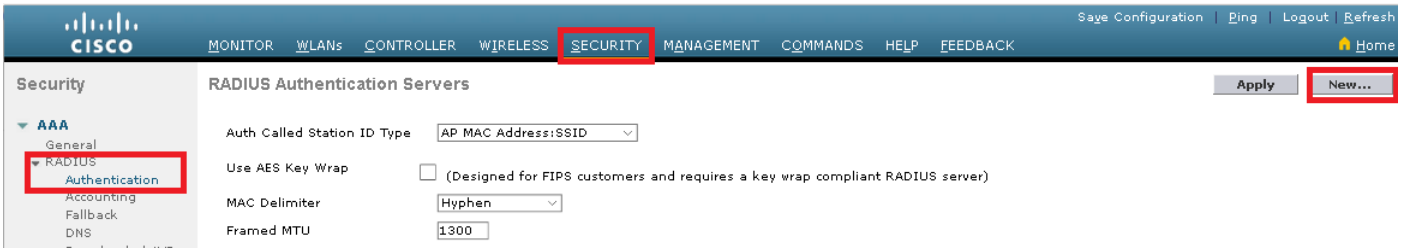
Passaggio 2. In basso, aggiungere l'indirizzo IP del controller e la chiave condivisa.

```
client{ secret = shortname = }
```

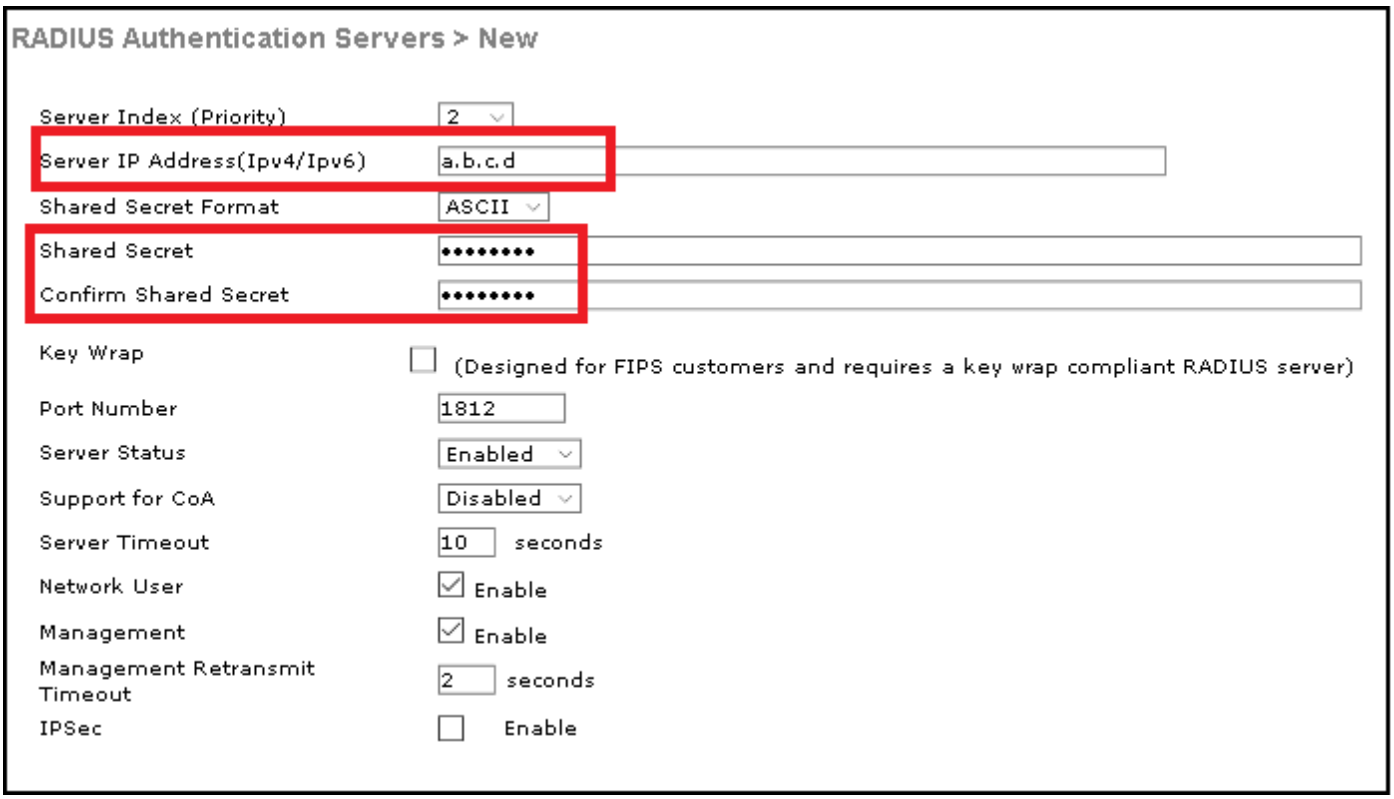
FreeRADIUS come server RADIUS su WLC

GUI:

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



Passaggio 2. Inserire le informazioni sul server RADIUS come illustrato nell'immagine.



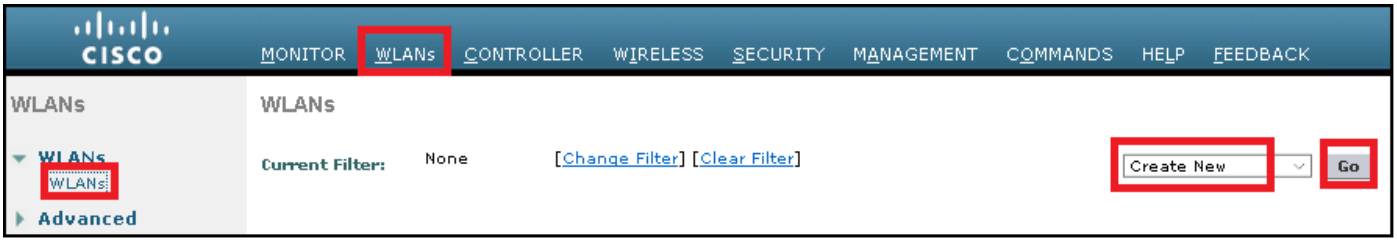
CLI:

```
> 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>
```

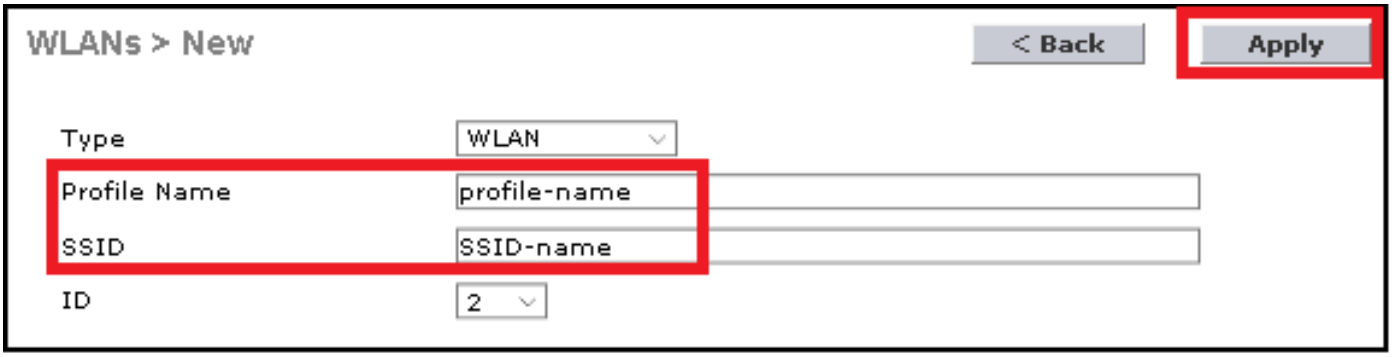
WLAN

GUI:

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



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



CLI:

```
> config wlan create <id> <profile-name> <ssid-name>
```

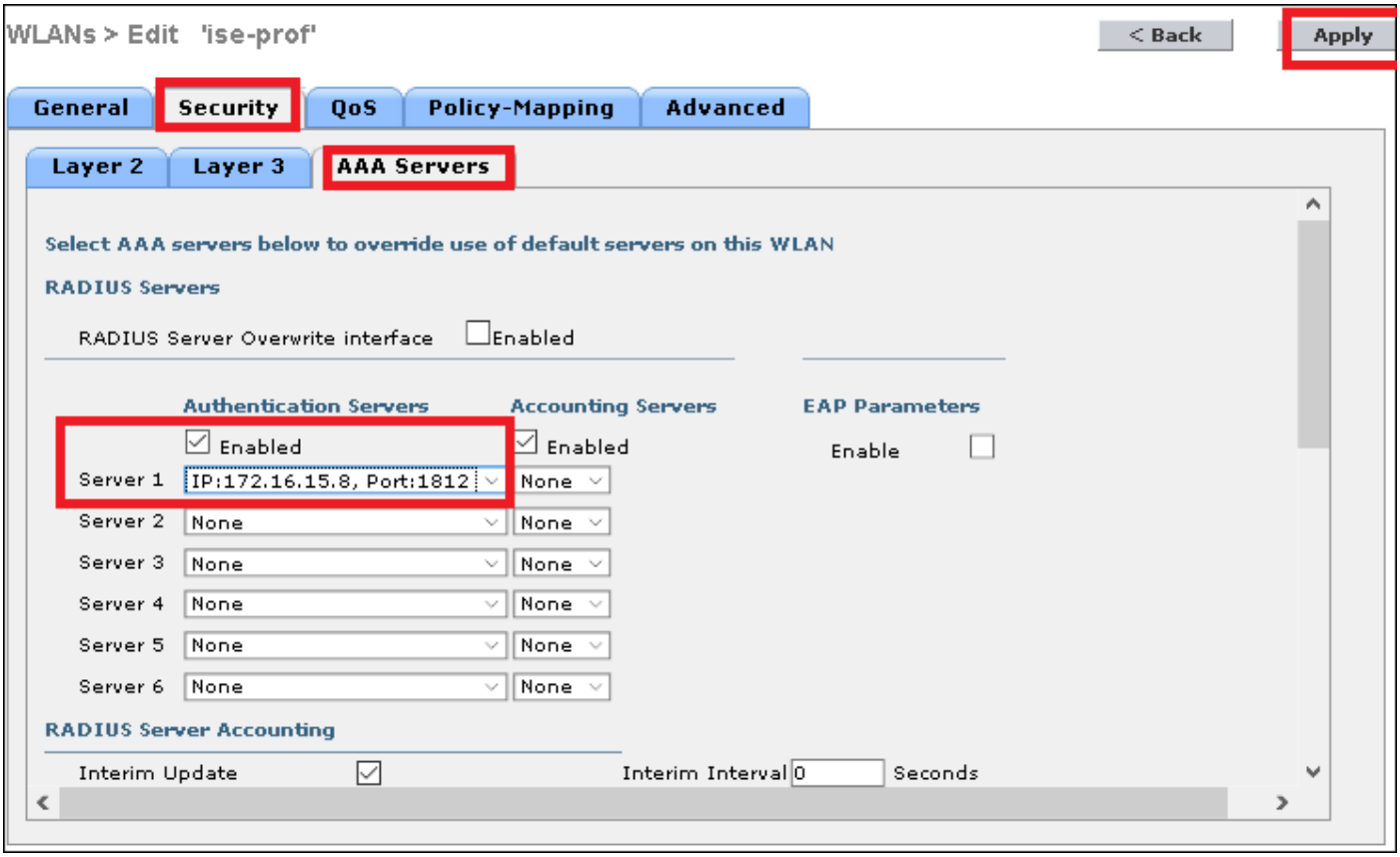
Passaggio 3. Assegnare il server RADIUS alla WLAN.

CLI:

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI:

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



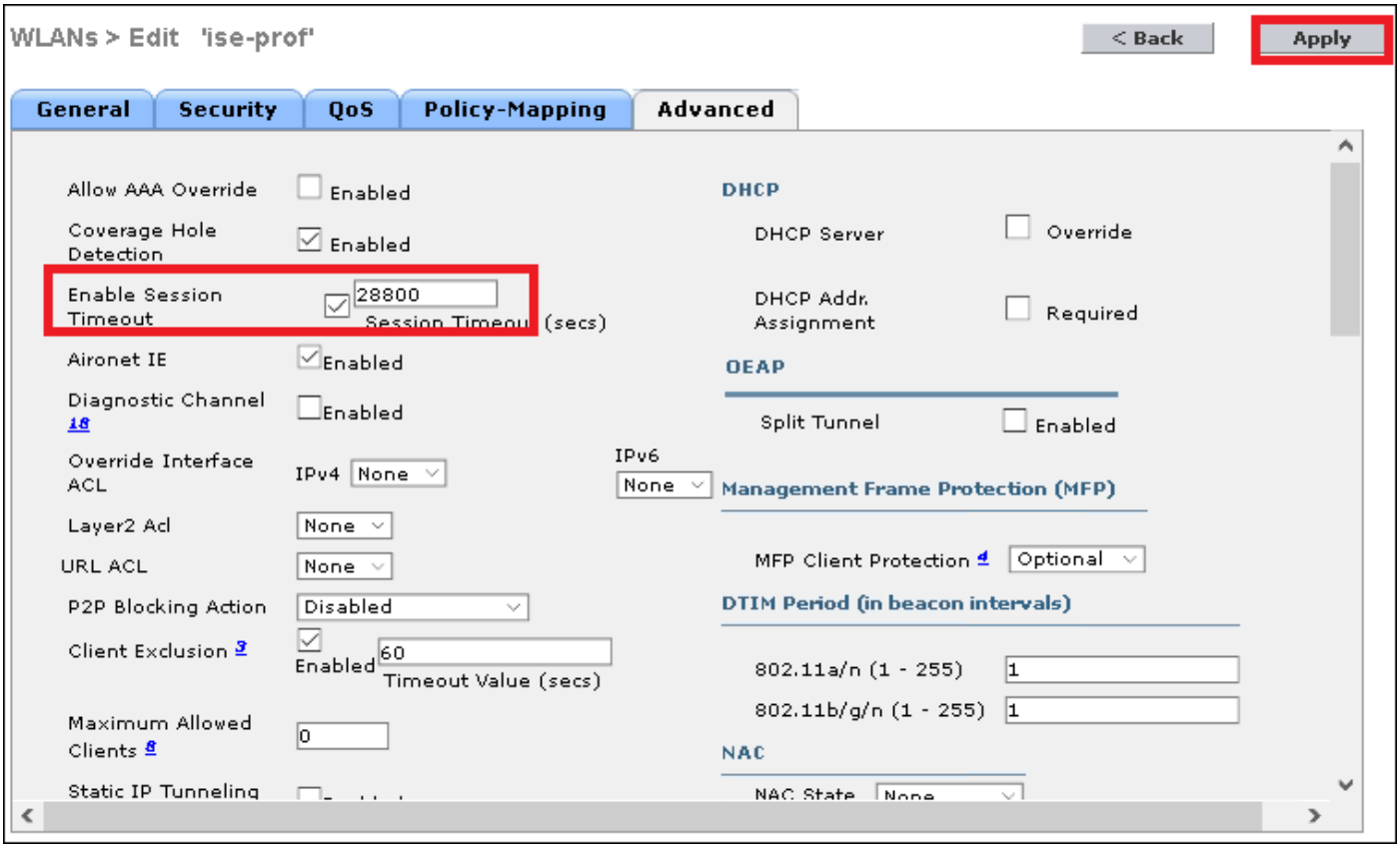
Passaggio 4. Se necessario, aumentare il tempo della sessione.

CLI:

```
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

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



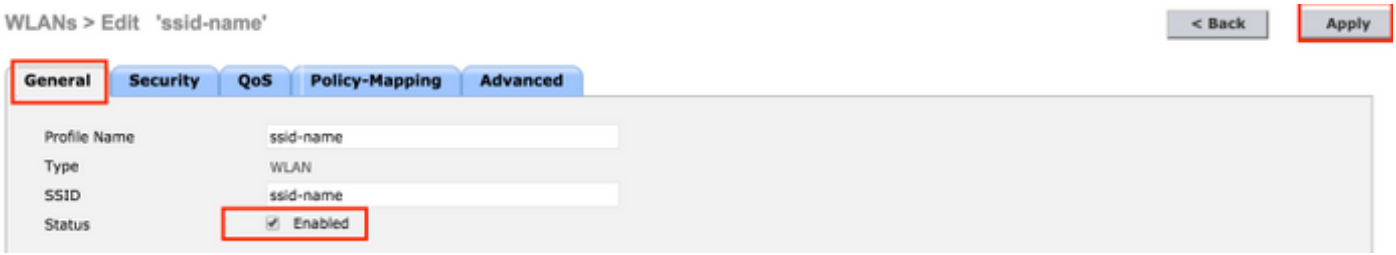
Passaggio 5. Abilitare la WLAN.

CLI:

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

GUI:

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



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**.

```
[root@tac-mxwireless ~]# nano /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
2. 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:

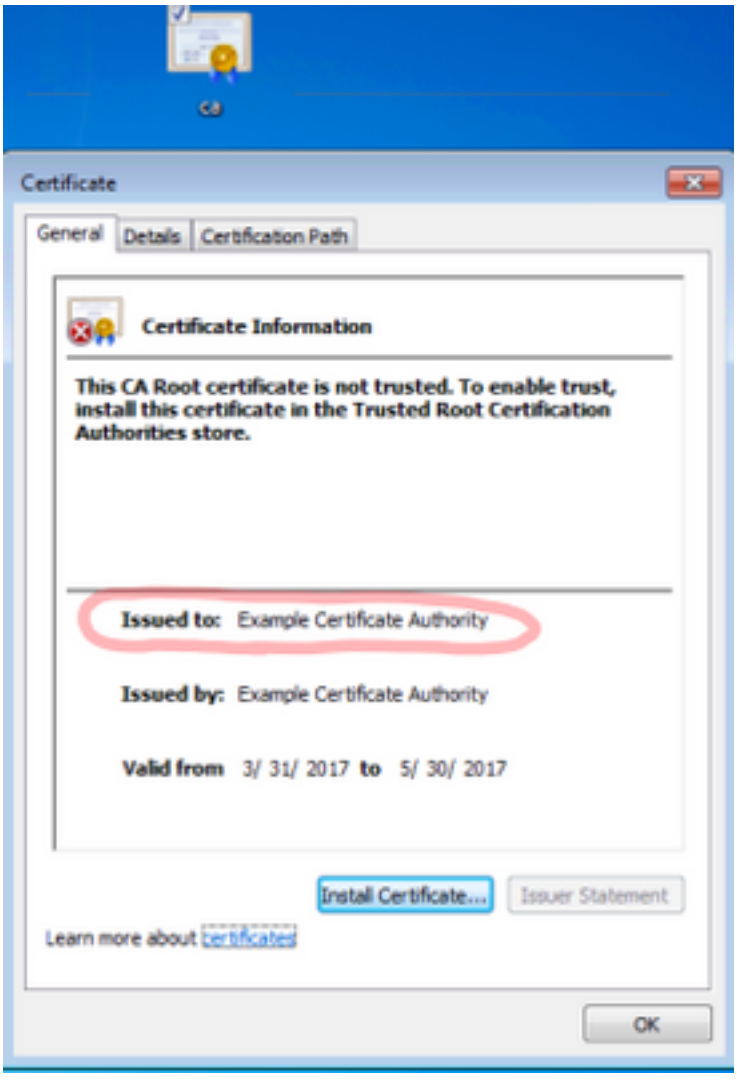
```
[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

-----BEGIN CERTIFICATE-----
MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb211d2hlcmUxFTAT
BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs
ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w
DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh
bXBsZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQG
A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B0OXLpeQFWjqolQOB9F
```

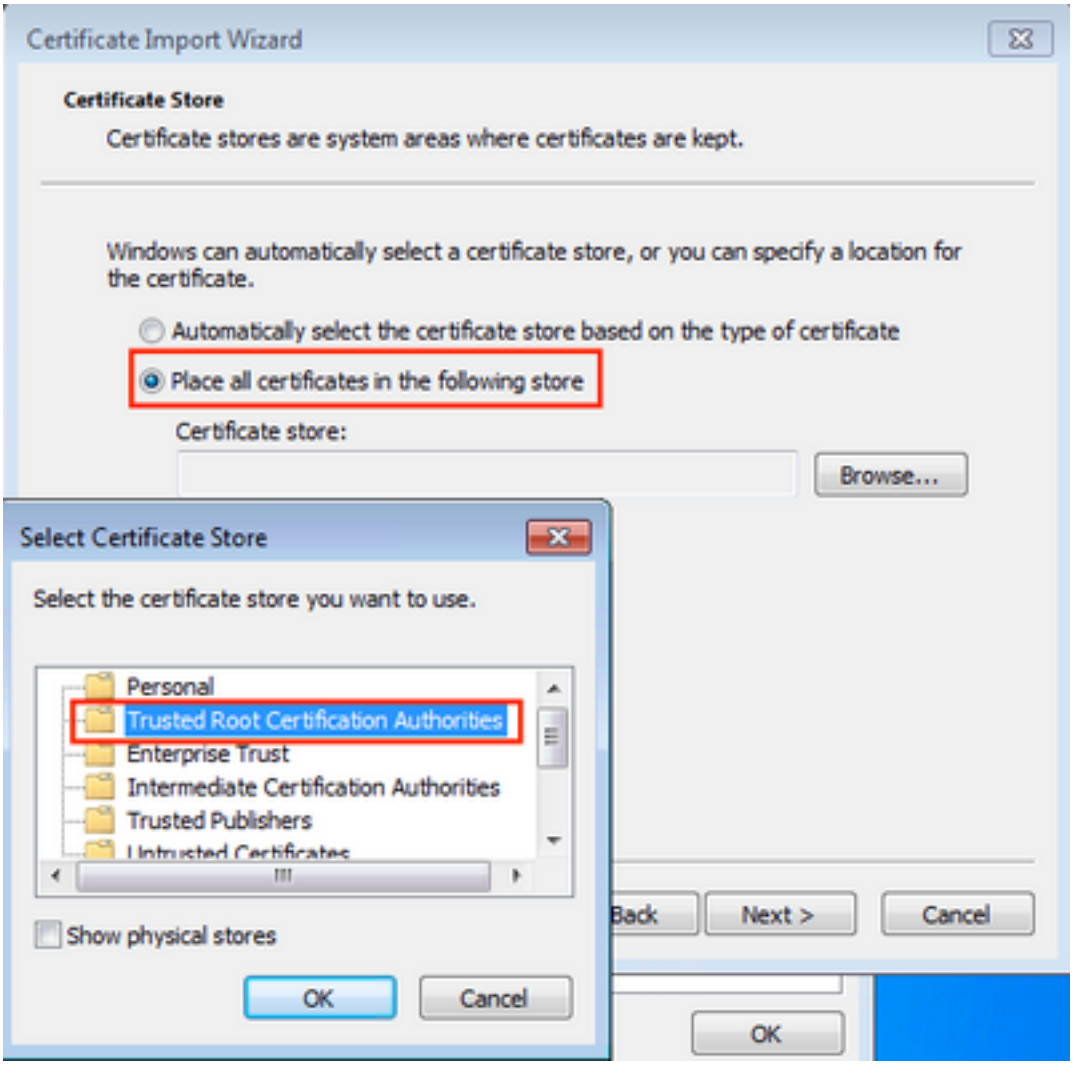
```
/8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyzI8sKi5H42GU
Eu6GDw1YJvhHn4rVC36OZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS
oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC
ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp
gwNNZ7X5US0FcjuuOtpJJ3hfQ8K6uXjEWPOkDE0DAnqp4/n9AgMBAAGjggE0MIIB
MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU
ysFNRZKpAlcFCEgwdOPVGV0waLGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD
VQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs
ZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQGA1UE
AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV
HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j
b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4
1wnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV
mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY
Z6cNjx8+aYQIcsRIyqA1IXMOBwIXo141TOmoODdgfX95lpoLwgktRLkvl7Y7owsz
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.

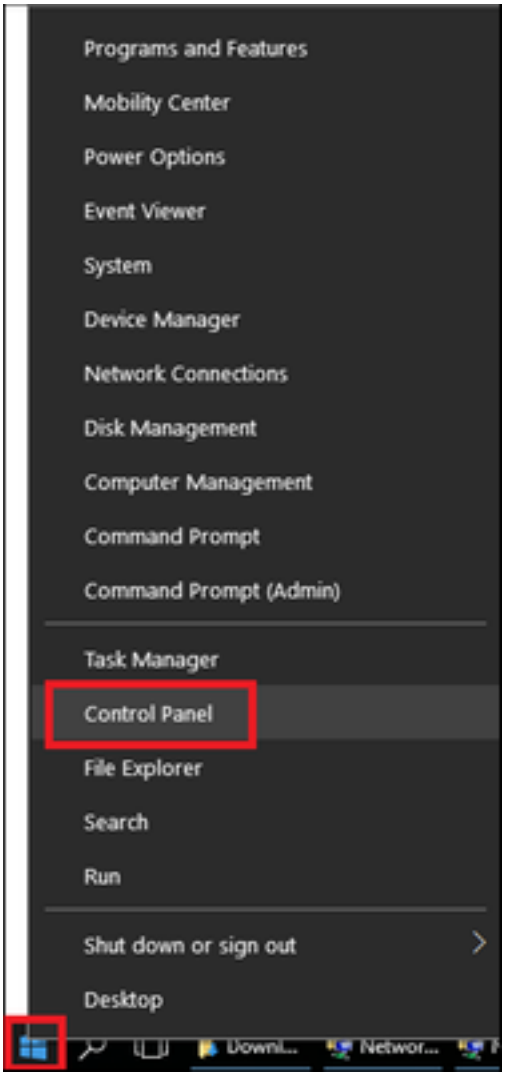


Passaggio 4. Installare il certificato nell'archivio **Autorità di certificazione radice attendibili**, come mostrato nell'immagine.

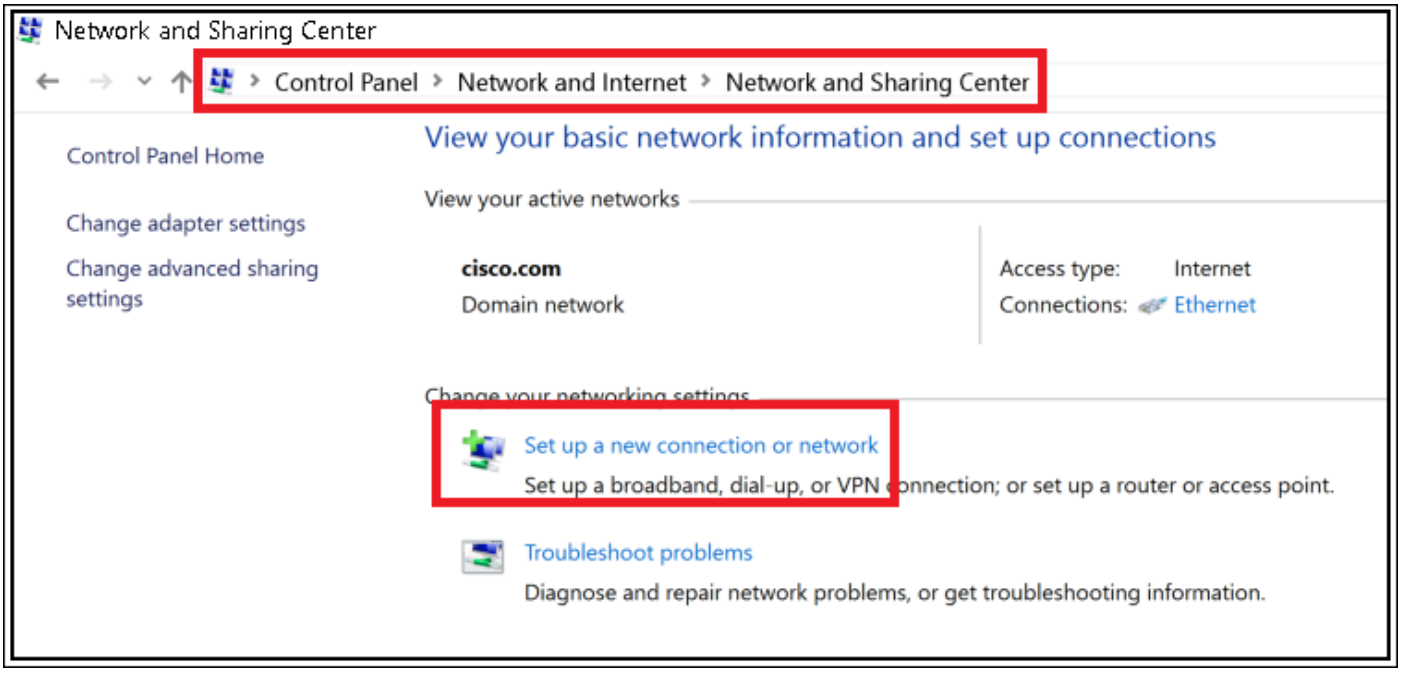


Crea profilo WLAN

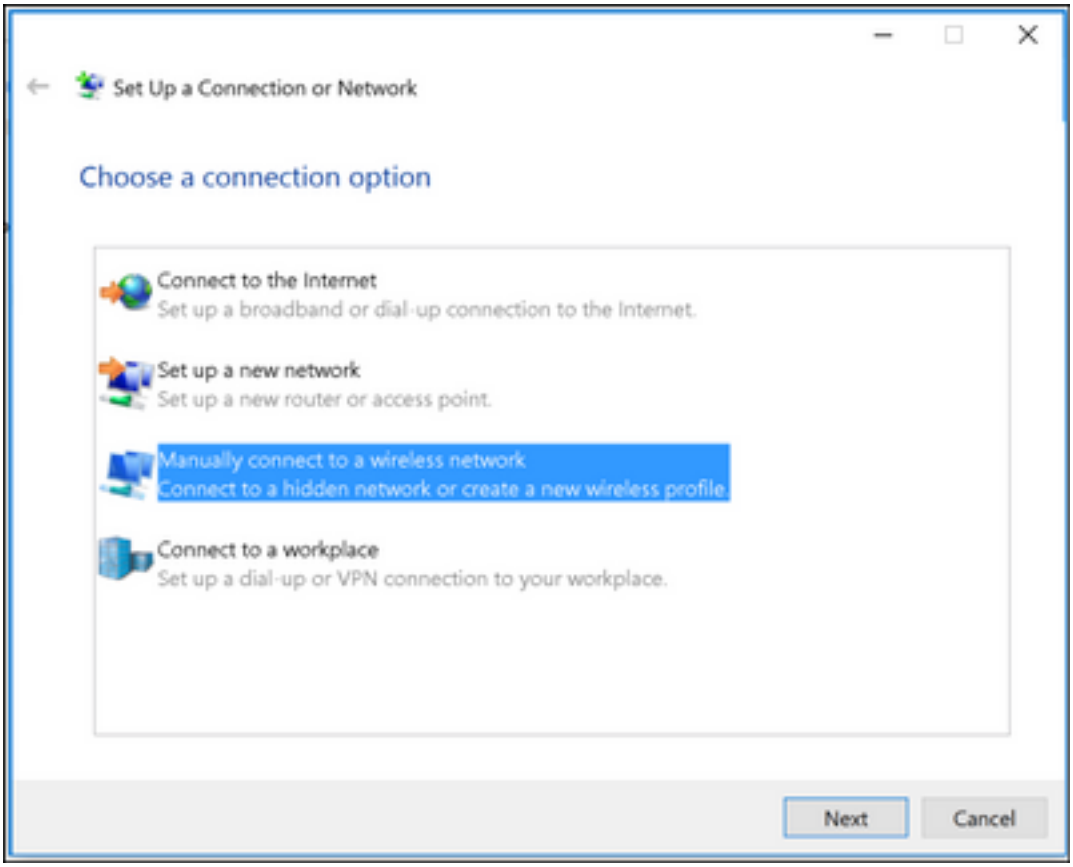
Passaggio 1. Fare clic con il pulsante destro del mouse sull'icona Start e selezionare **Pannello di controllo** come mostrato nell'immagine.



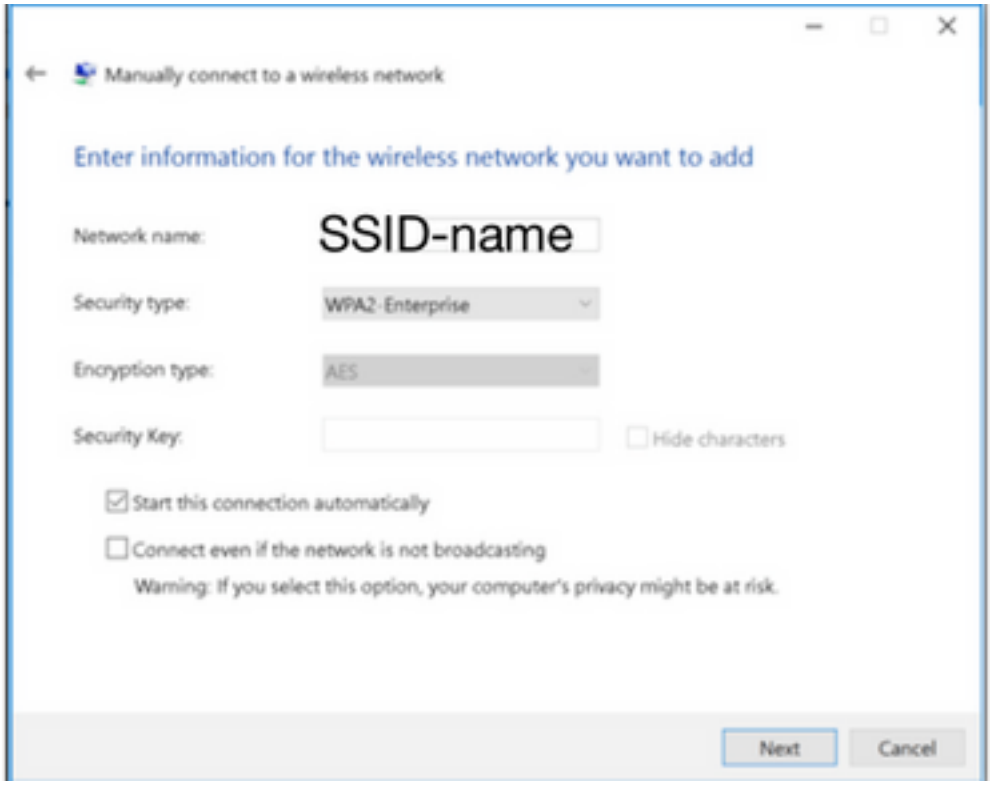
Passaggio 2. Selezionare **Rete e Internet > Centro connessioni di rete e condivisione> fare clic su Configura nuova connessione o rete** come mostrato nell'immagine.



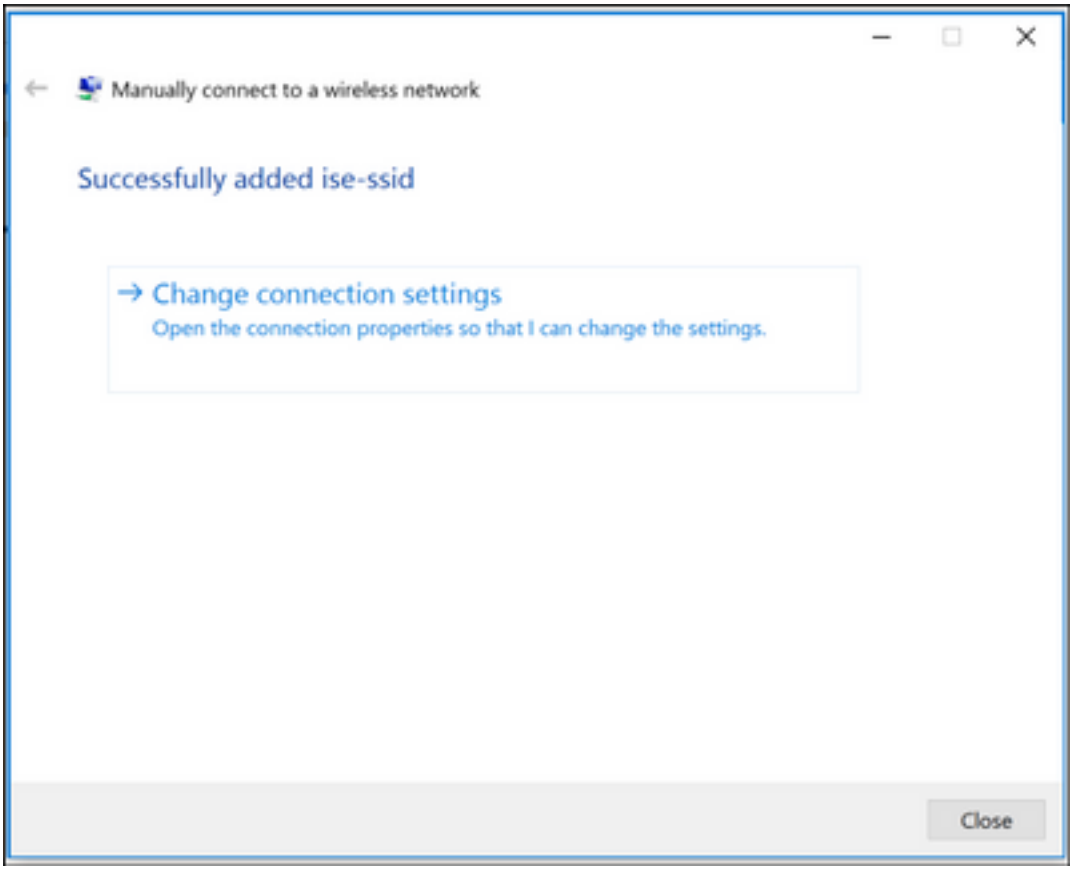
Passaggio 3. Selezionare **Connetti manualmente a una rete wireless** e fare clic su Avanti come mostrato nell'immagine.



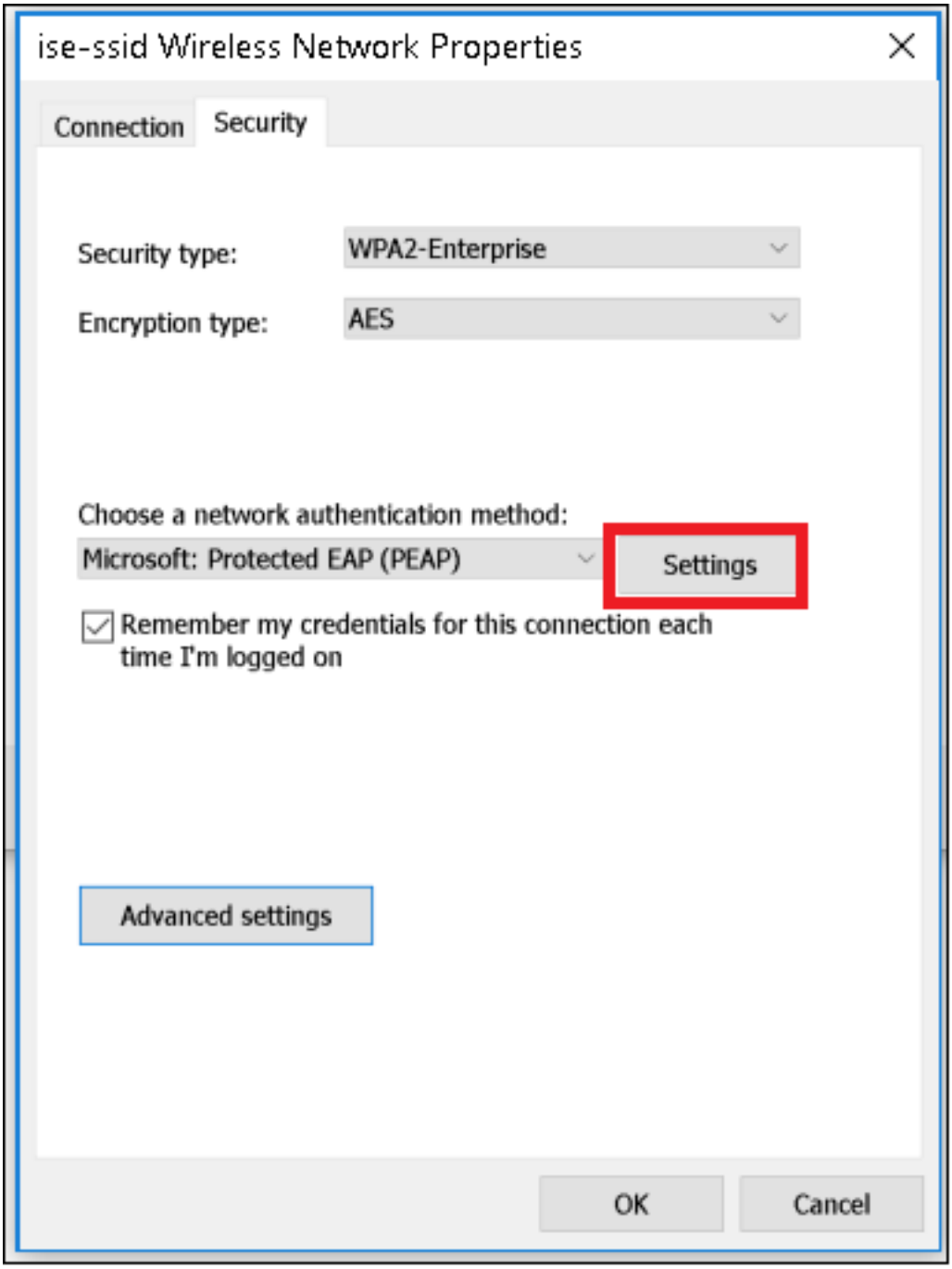
Passaggio 4. Immettere le informazioni con il nome del SSID e il tipo di protezione WPA2-Enterprise e fare clic su **Avanti** come mostrato nell'immagine.



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



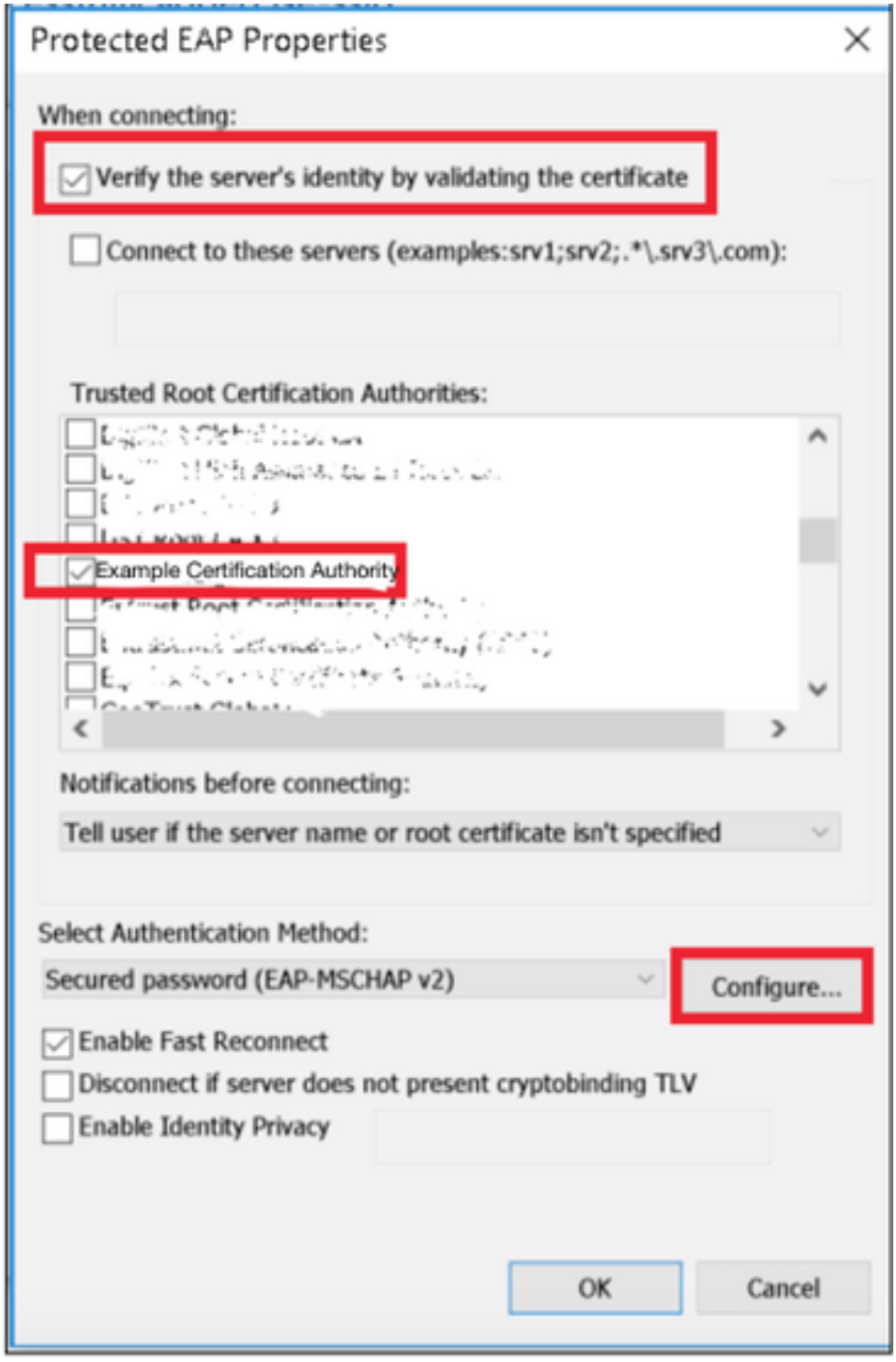
Passaggio 6. Passare alla scheda **Sicurezza** e fare clic su **Impostazioni**, come mostrato nell'immagine.

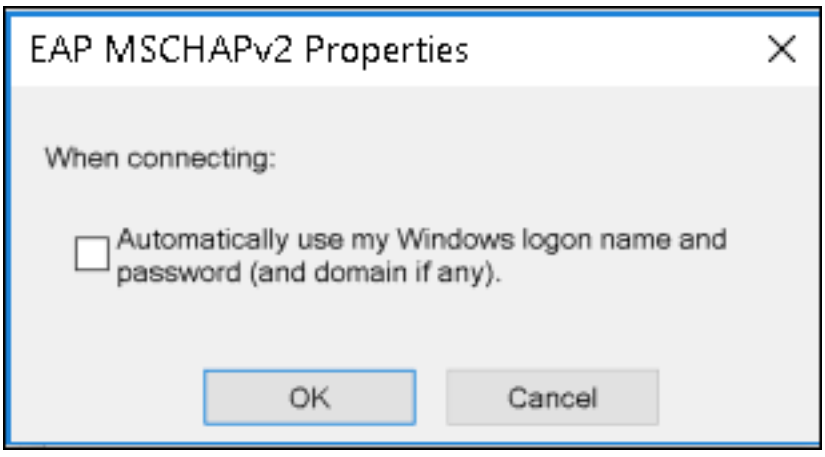


Passaggio 7. Scegliere se il server RADIUS è convalidato o meno.

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.

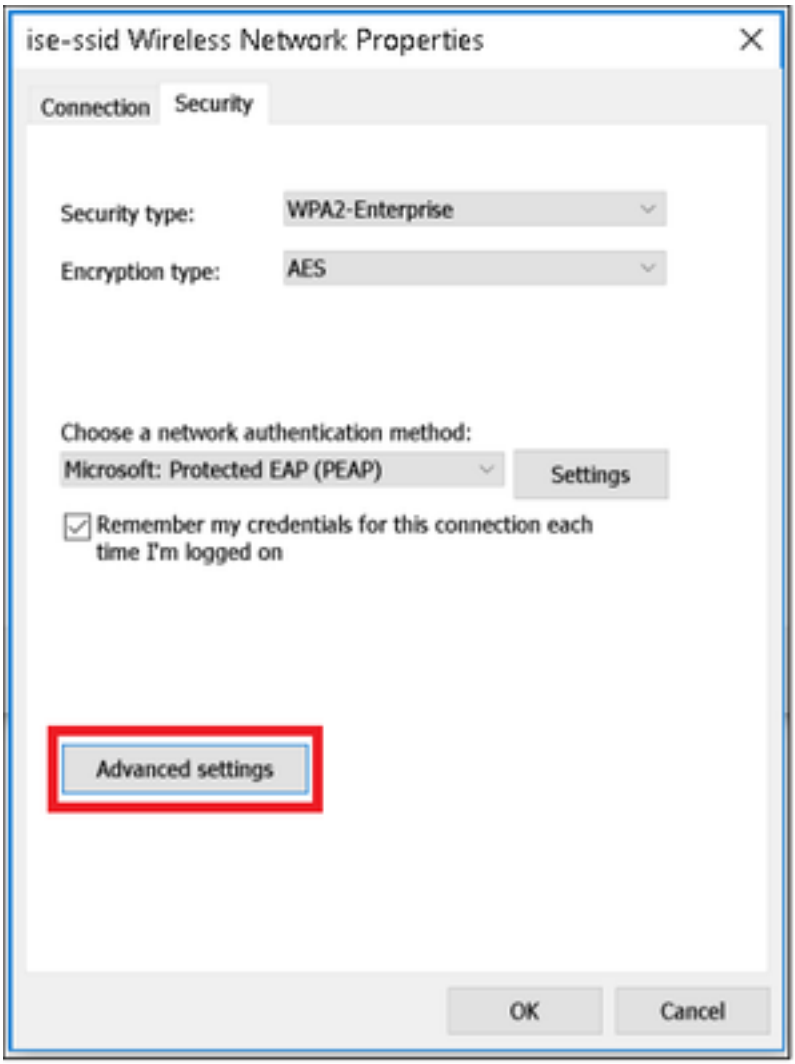
Quindi selezionare **Configure** and disable **Automatically use my Windows logon name and password...**, quindi fare clic su **OK** come mostrato nelle immagini.

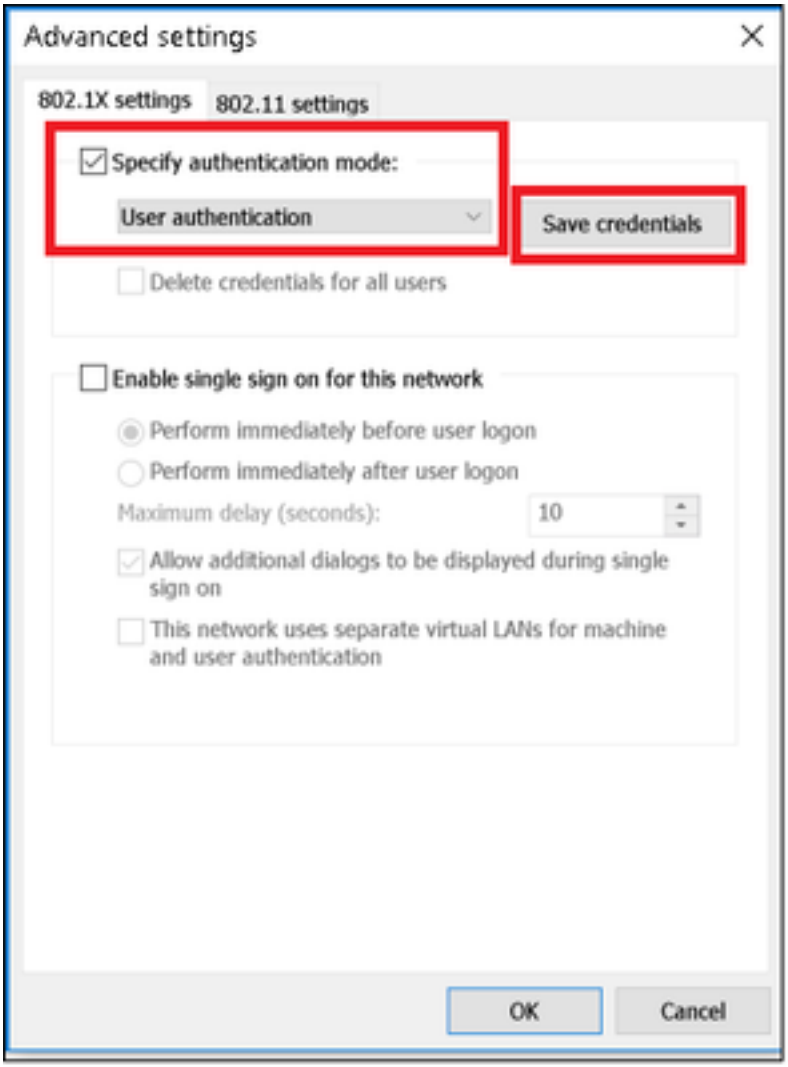


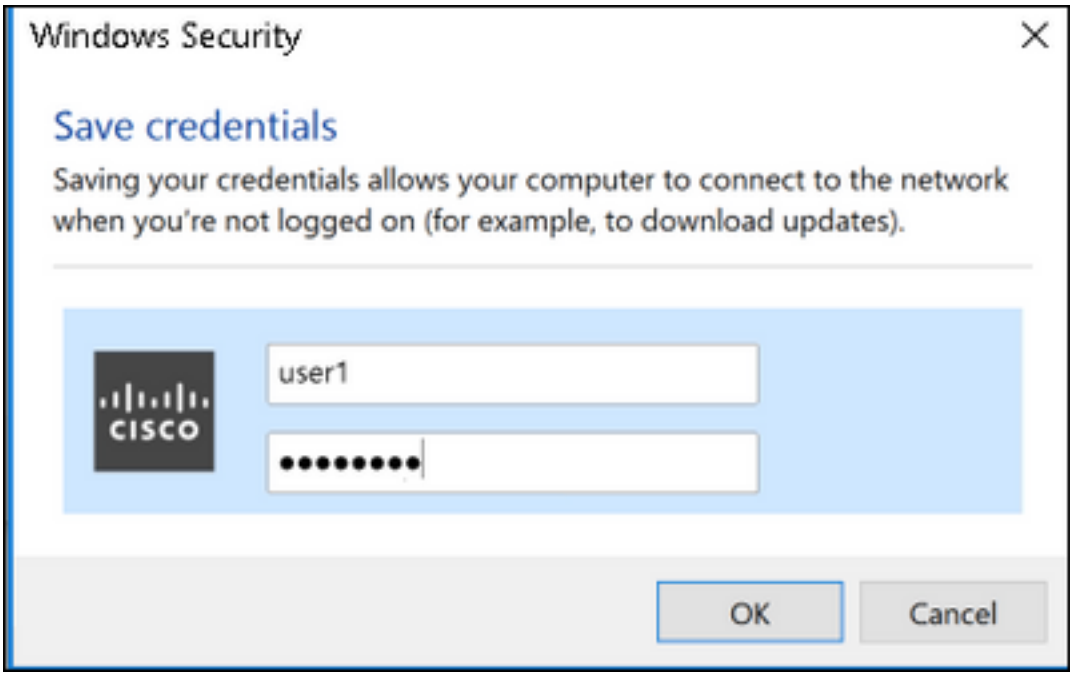


Passaggio 8. Configurare le credenziali utente.

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.







Verifica

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

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.