802.1x configureren - PEAP met FreeRadius en WLC 8.3

Inhoud

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

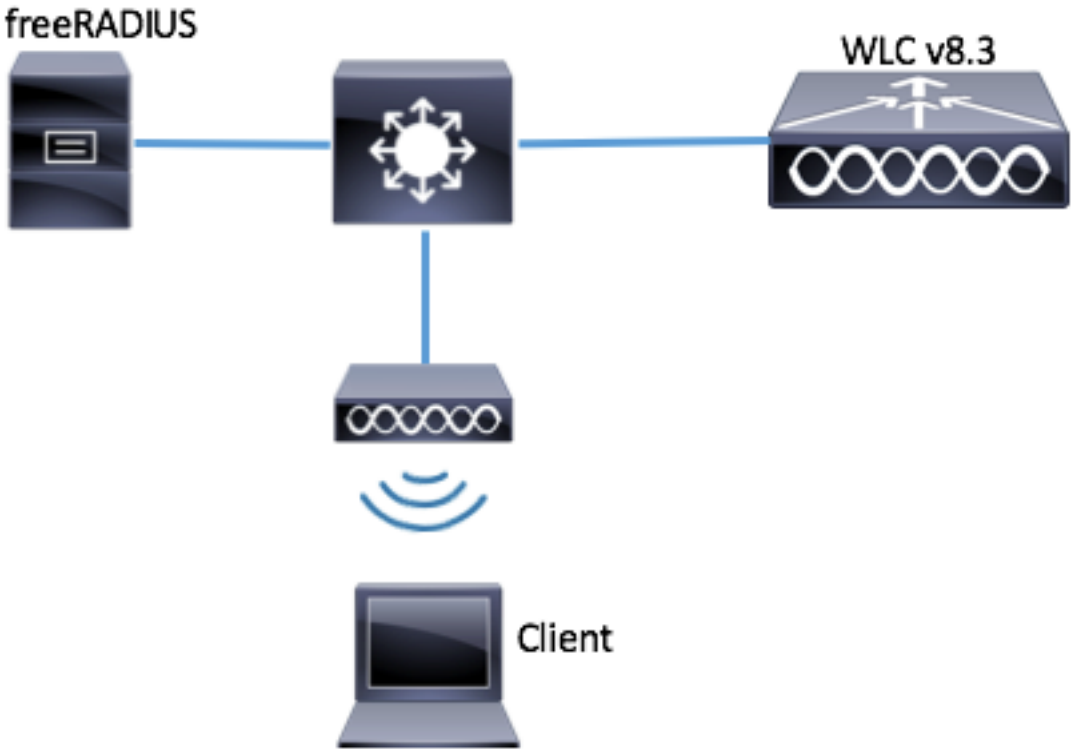
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- 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 freeradius-
sqlite
```

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/mods-
config/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
```

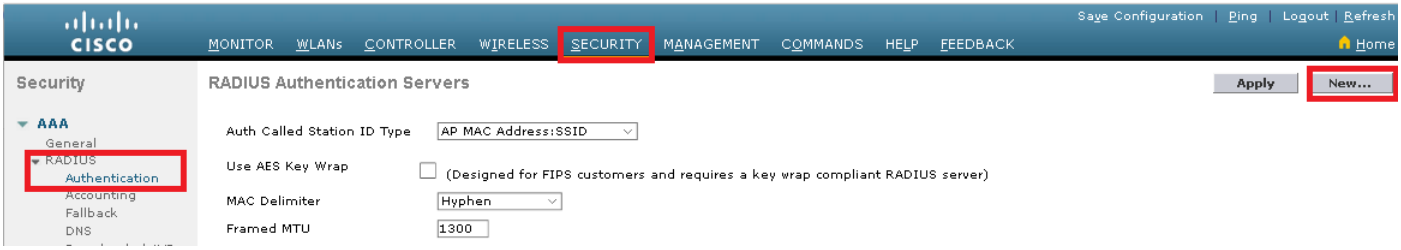
Stap 2. Onderaan voegt u uw ip-adres van de controller en de gedeelde toets toe.

```
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.

CLI:

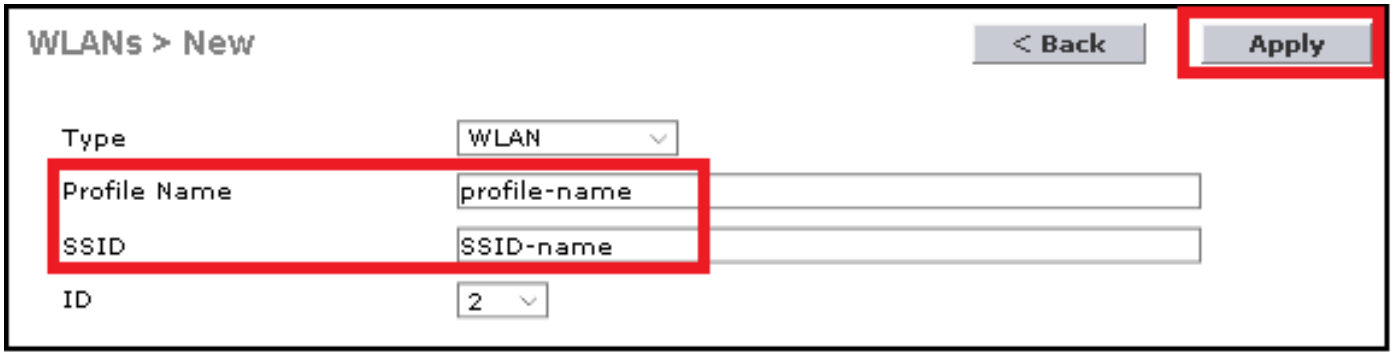
```
> config radius auth add <index> <radius-ip-address> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

WLAN

GUI:

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

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



CLI:

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

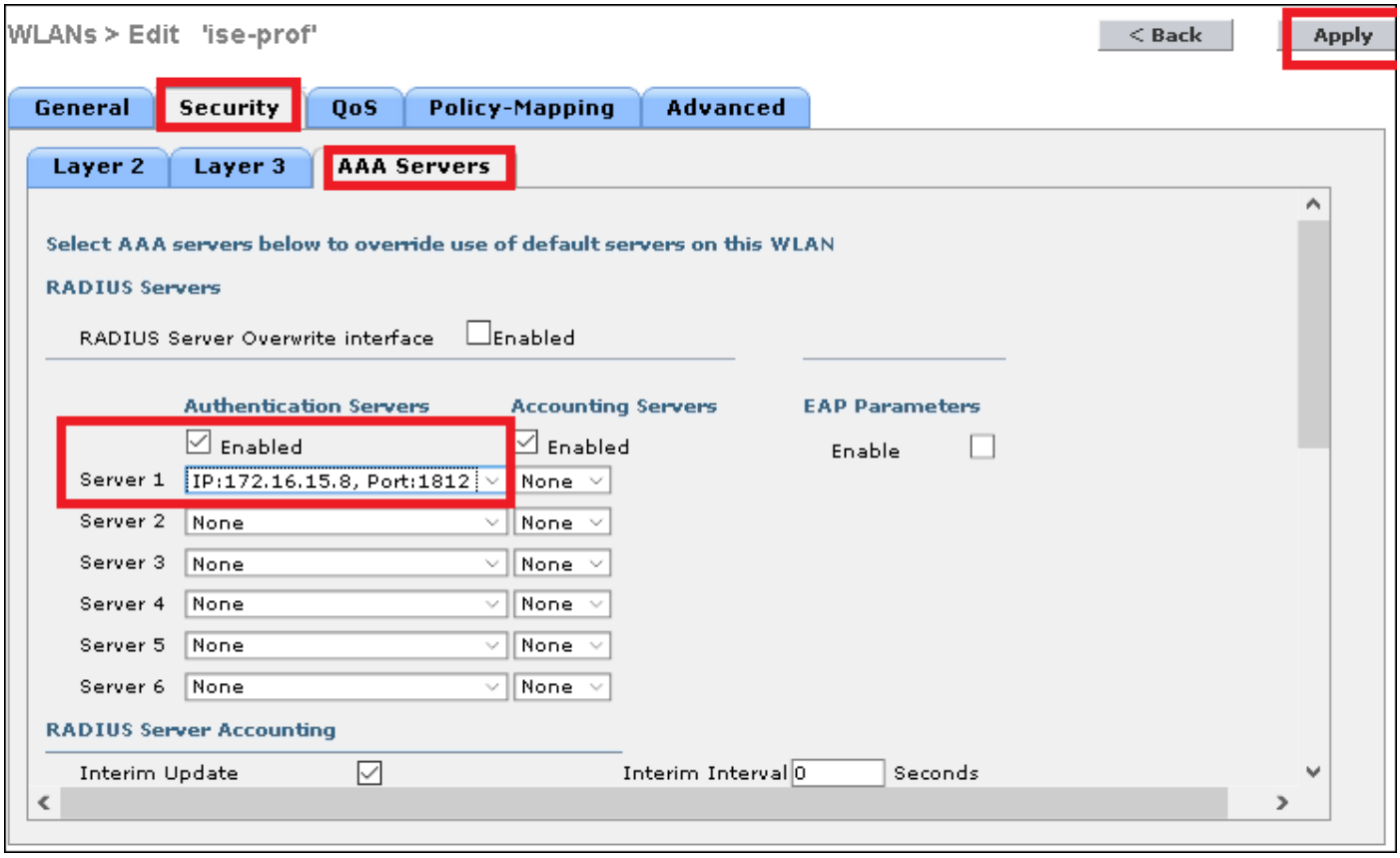
Stap 3. Pas de RADIUS-server aan WLAN aan.

CLI:

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

GUI:

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



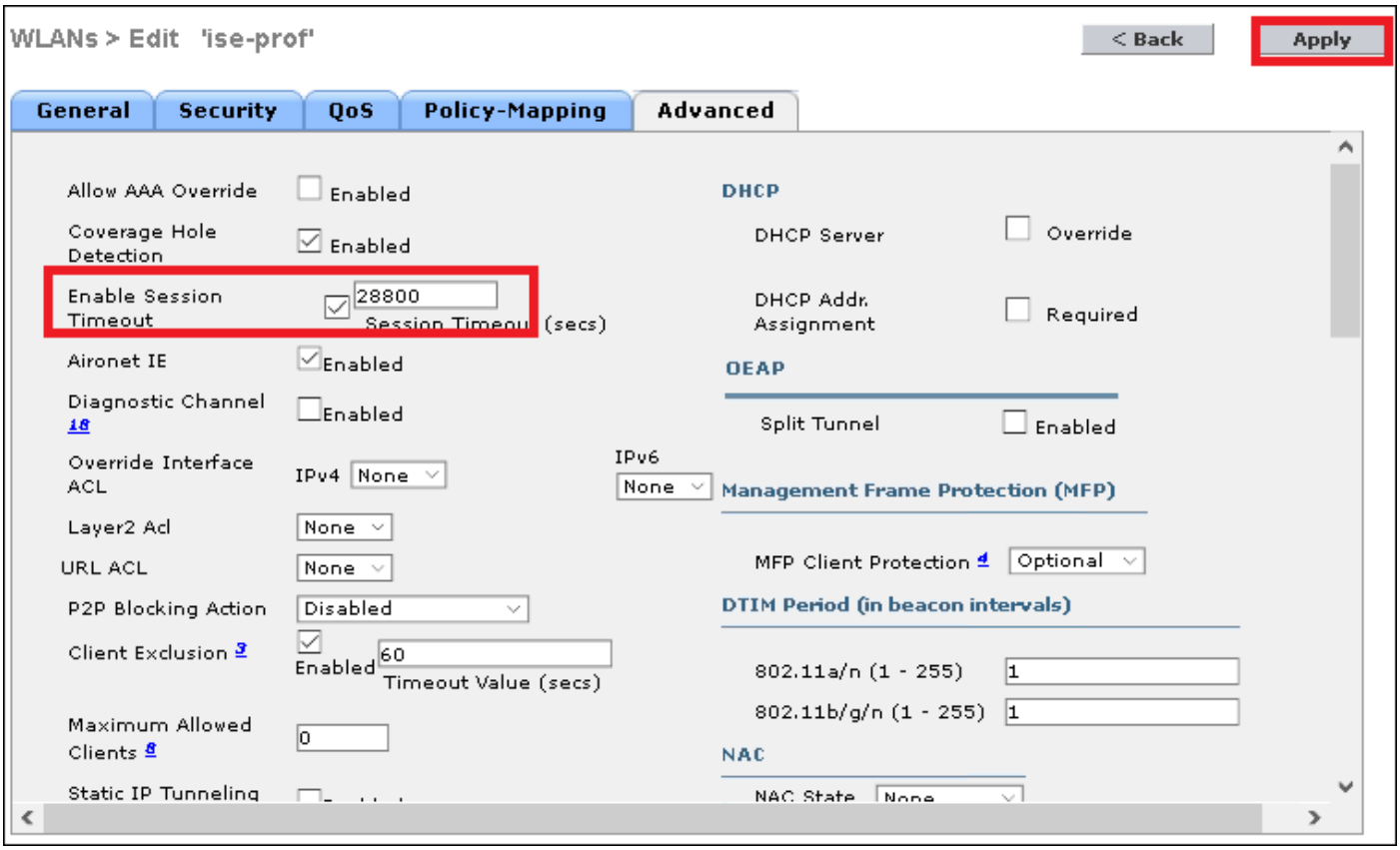
Stap 4. Verhoog optioneel de sessietijd.

CLI:

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

GUI:

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



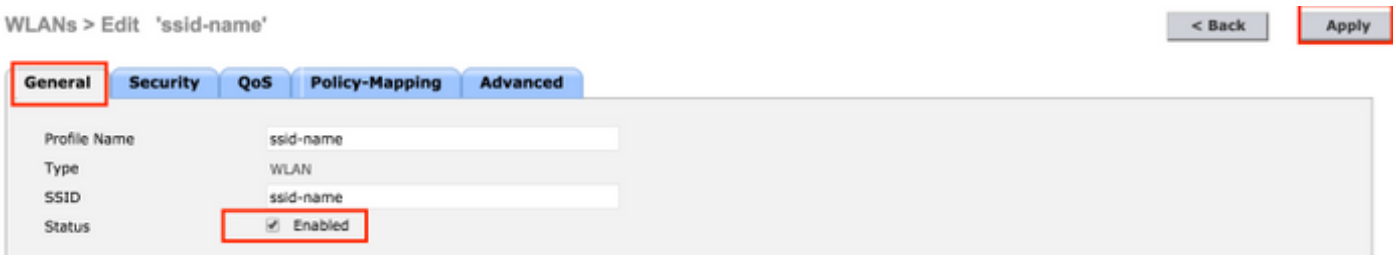
Stap 5. Schakel het WLAN in.

CLI:

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

GUI:

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



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 802.1x-verificatie 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
2. 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:

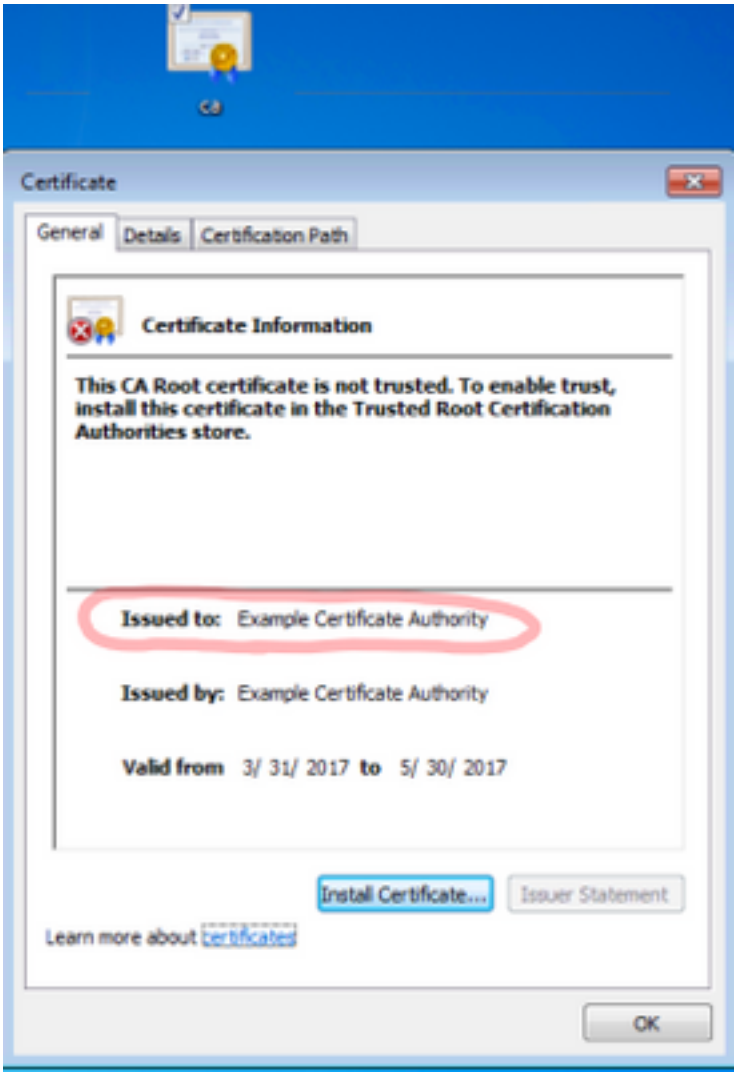
```
[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

-----BEGIN CERTIFICATE-----
MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb21ld2hlcmUxFTAT
```

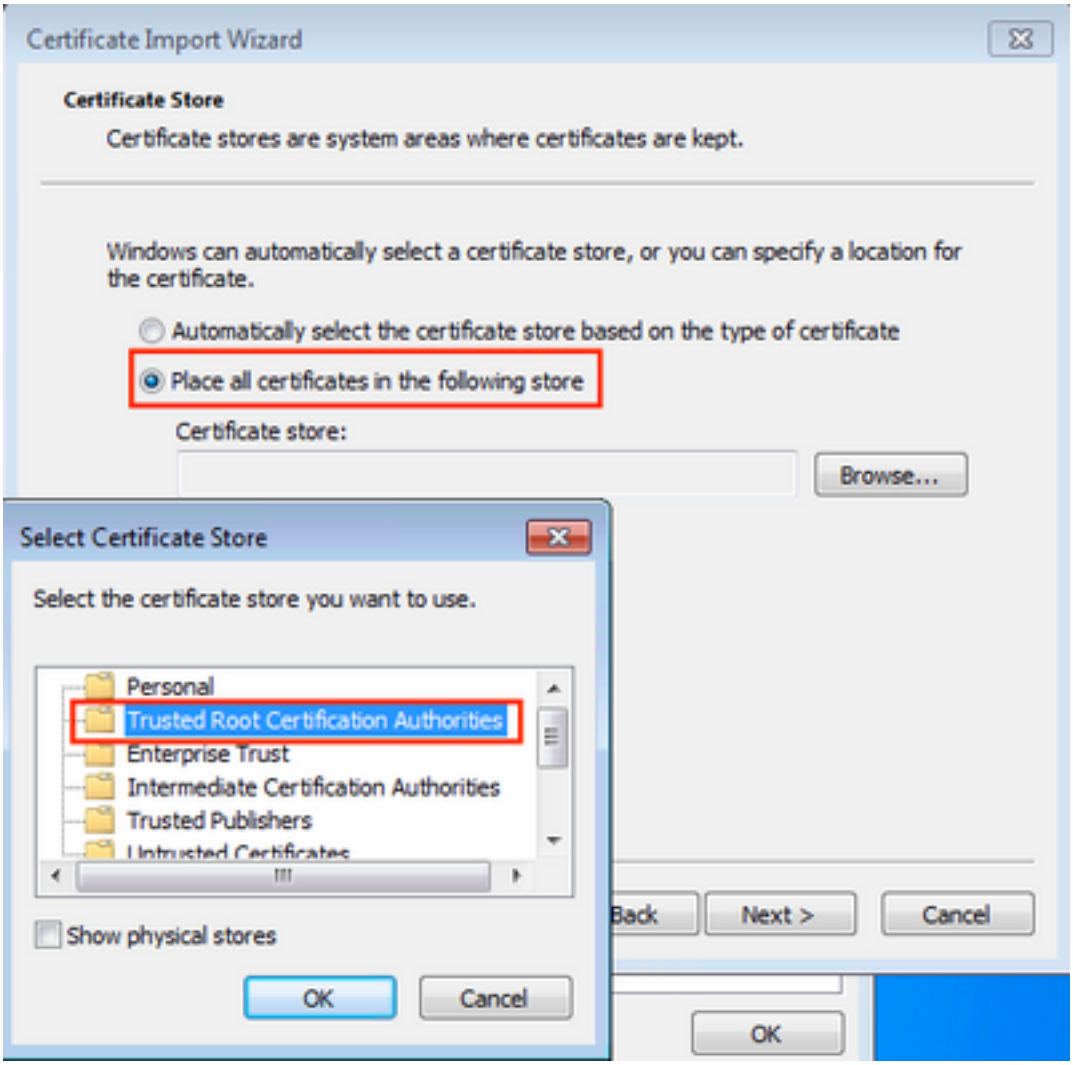
```
BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs
ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w
DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh
bXBsZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQG
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-----
```


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.

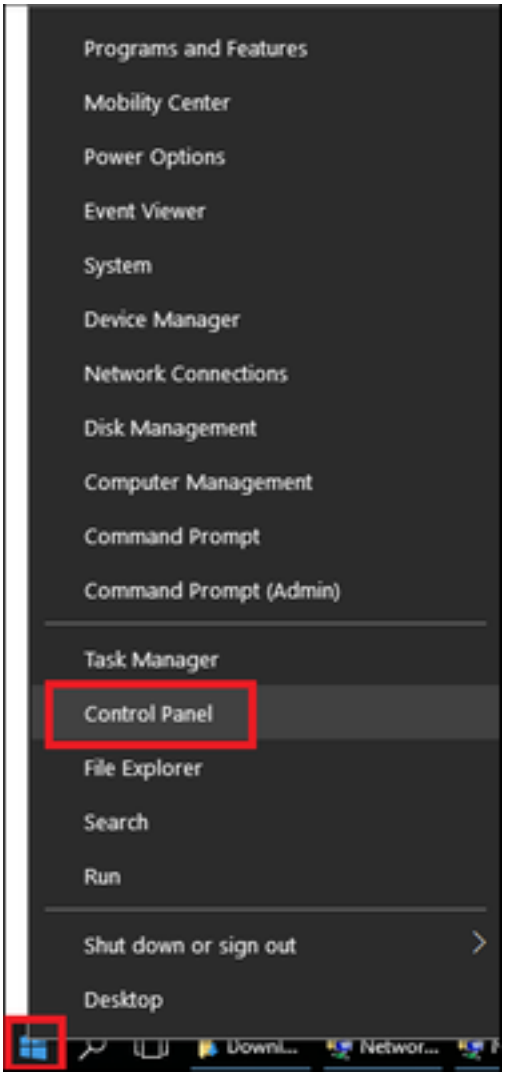


Stap 4. Installeer het certificaat in de winkel **Trusted Root-certificeringsinstanties** zoals in de afbeelding.

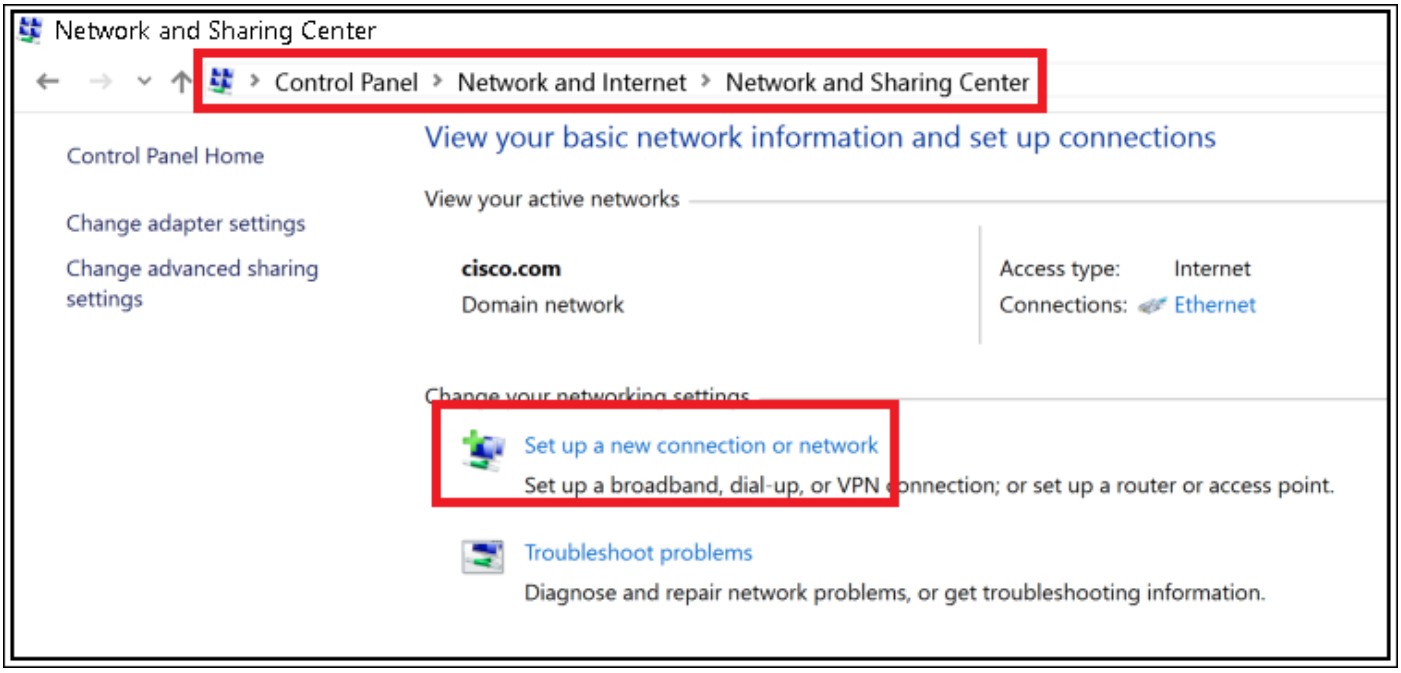


WLAN-profiel maken

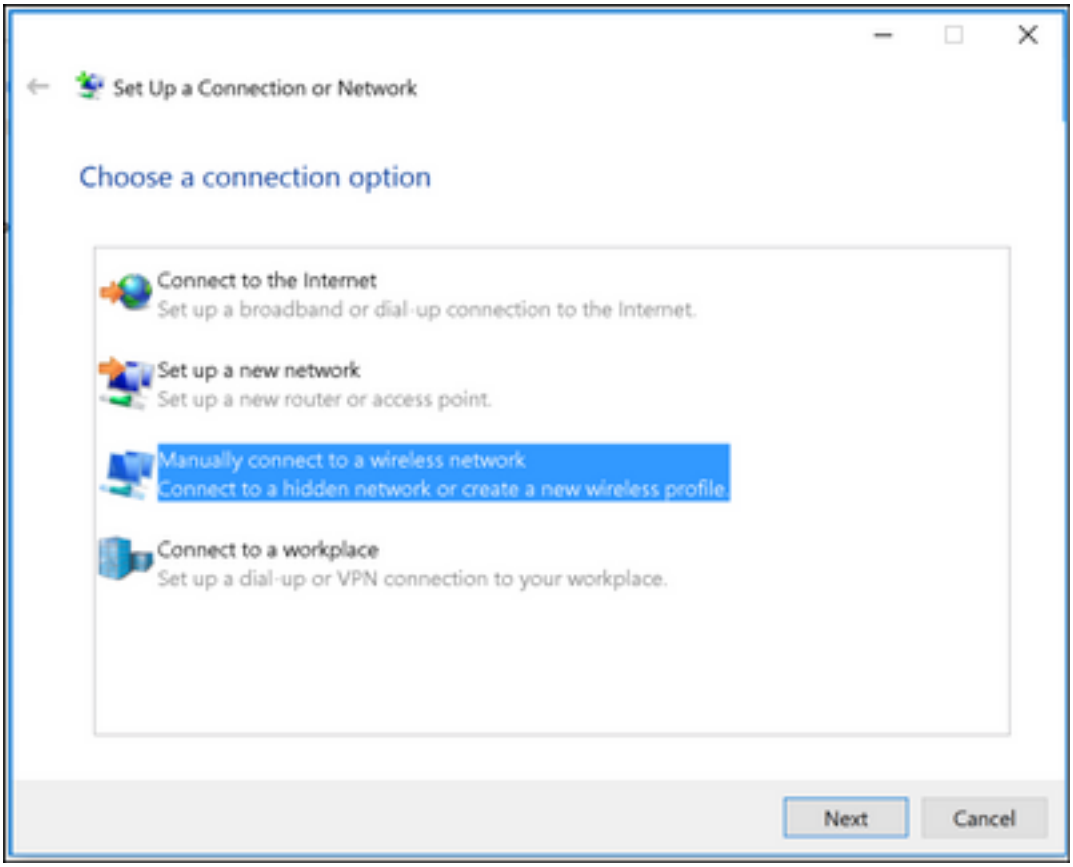
Stap 1. Klik met de rechtermuisknop op het pictogram Start en selecteer **het bedieningspaneel** zoals in de afbeelding.



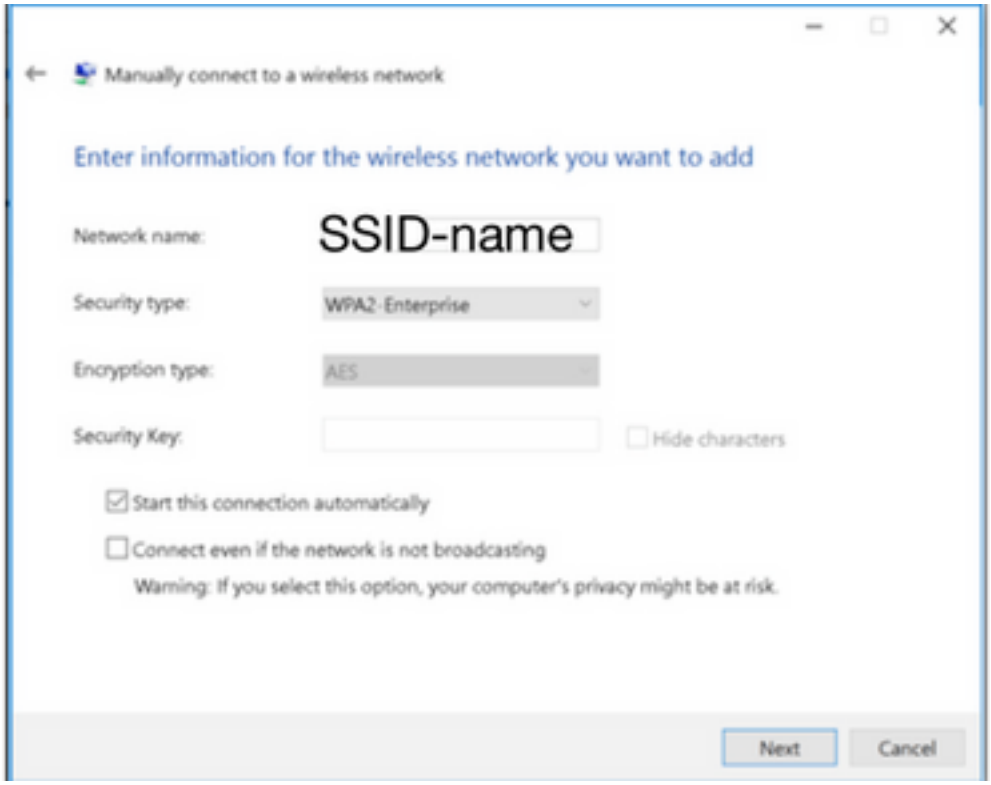
Stap 2. Navigeer naar **Netwerk en internet > Netwerk- en Sharing Center> klik op Een nieuwe verbinding of een netwerk** instellen zoals in de afbeelding.



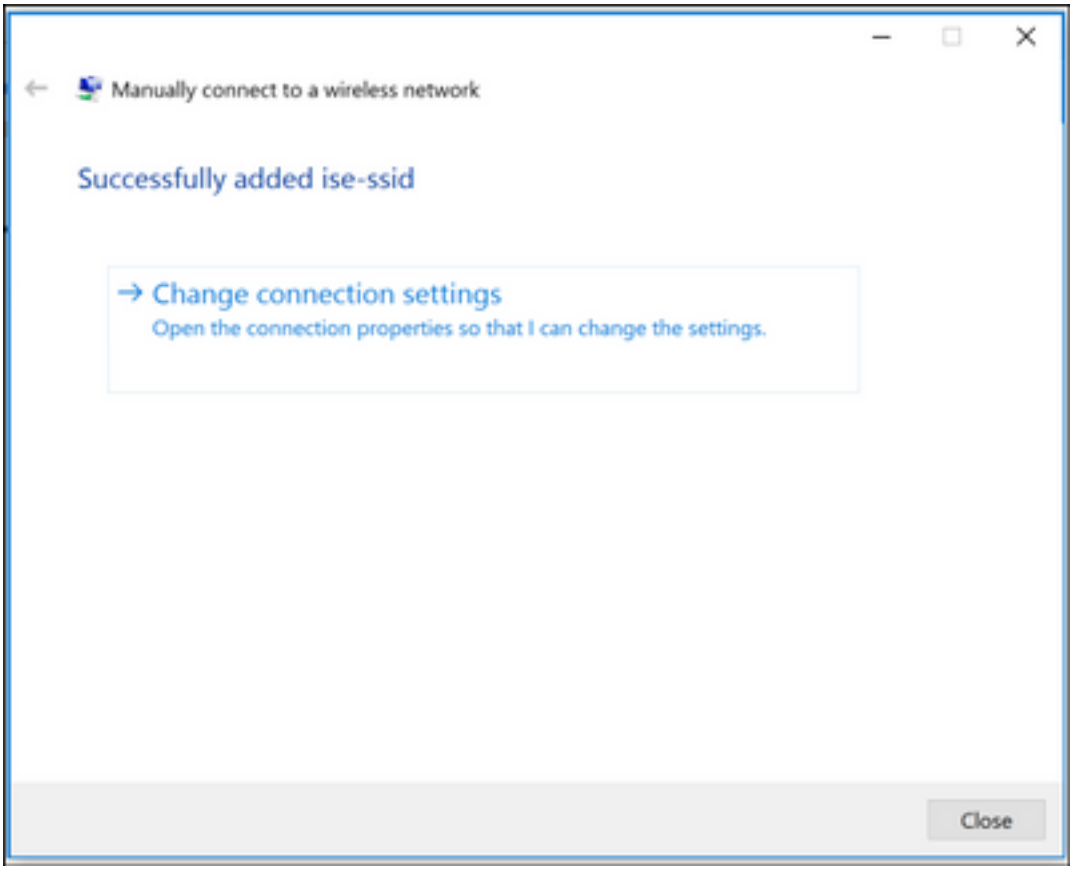
Stap 3. Selecteer **Handmatig verbinding maken met een draadloos netwerk** en klik op Volgende zoals in de afbeelding.



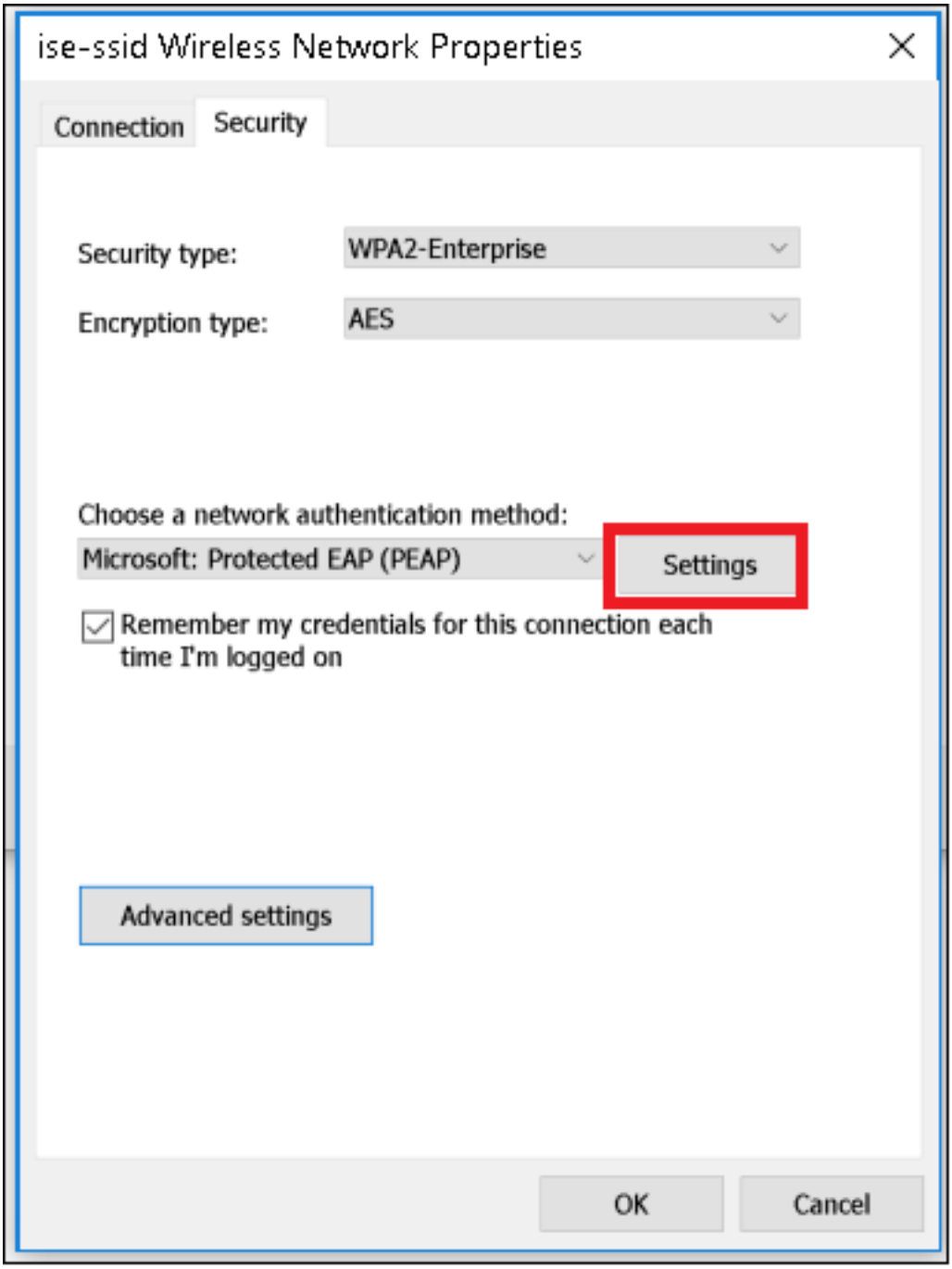
Stap 4. Voer de informatie in met de naam van de SSID en het beveiligingstype WAP2-Enterprise en klik op **Volgende** zoals in de afbeelding.



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



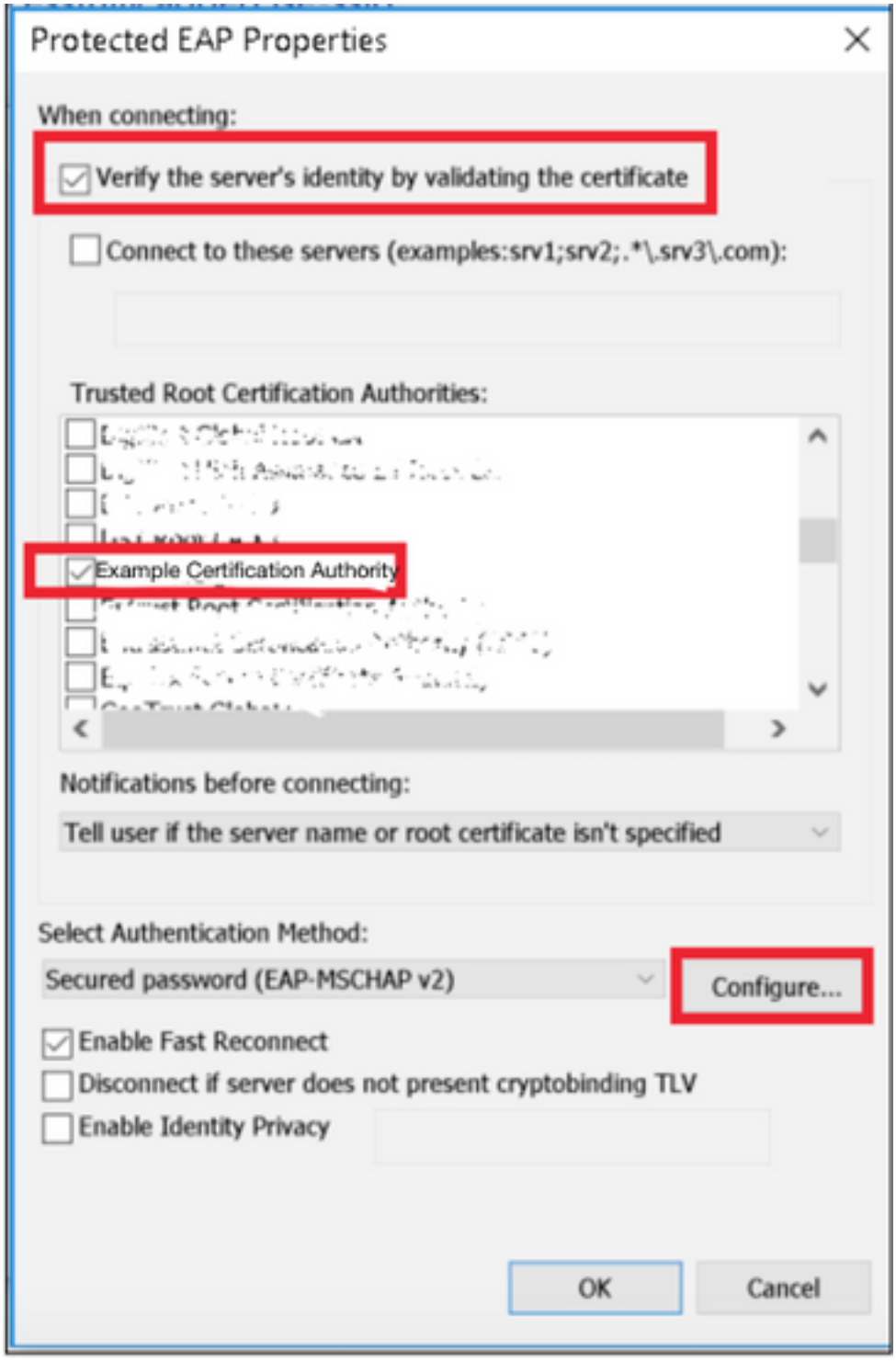
Stap 6. Navigeer naar het tabblad **Security** en klik op **Instellingen** zoals in de afbeelding.

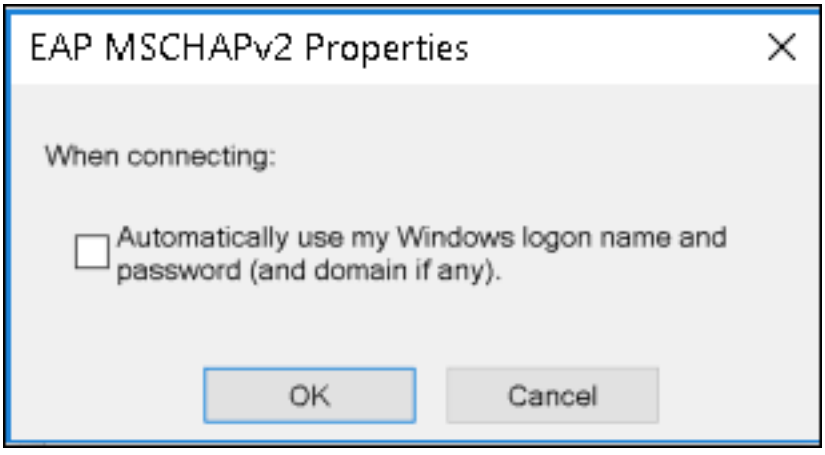


Stap 7. Kies of de RADIUS-server al dan niet gevalideerd is.

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.

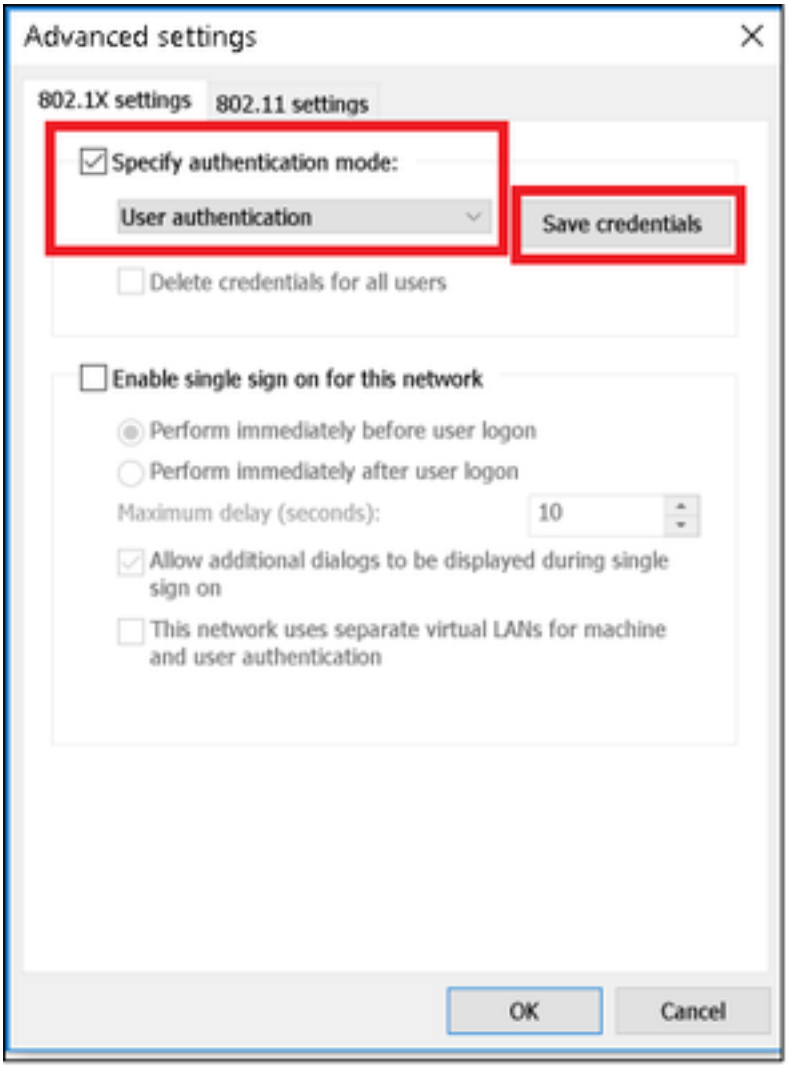
Nadat u **mijn bestandsnaam en wachtwoord voor** aanmelding **door Windows automatisch instellen** en uitschakelen **gebruikt...** klikt u vervolgens op **OK** zoals in de afbeeldingen wordt weergegeven.

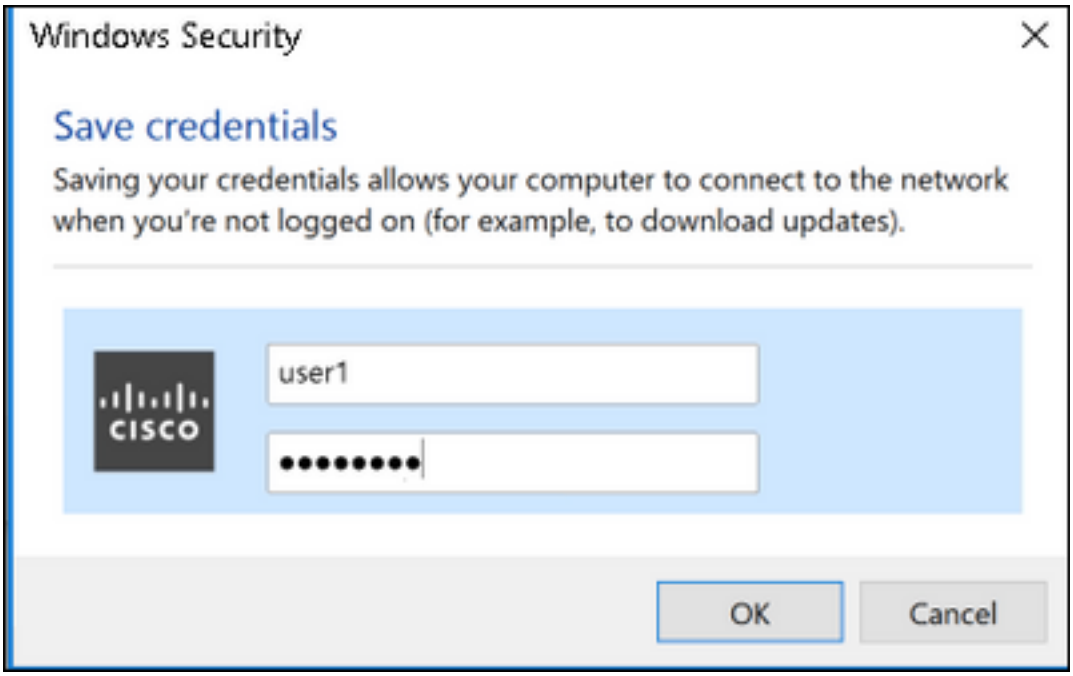




Stap 8. Configureer de gebruikersreferenties.

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.





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 debug-clientuitgangen te lezen:

Draadloze debug Analyzer

Problemen oplossen

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