

# 802.1x WLAN + VLAN-voorrang met Mobility Express (ME) 8.2 en ISE 2.1

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Configuratie op ME](#)

[ME op ISE verklaren](#)

[Een nieuwe gebruiker op ISE maken](#)

[De verificatieregel maken](#)

[Maak de autorisatieregel](#)

[Configuratie van het eindapparaat](#)

[Verifiëren](#)

[Verificatieproces op ME](#)

[Verificatieproces op ISE](#)

## Inleiding

In deze documenten wordt beschreven hoe u een WLAN (Wireless Local Area Network) kunt instellen met Wi-Fi Protected Access 2 (WPA2) Enterprise-beveiliging met een Mobility Express-controller en een externe externe RADIUS-server (Remote Verificatie) bij gebruiker. Identity Services Engine (ISE) wordt gebruikt als voorbeeld van externe RADIUS-servers.

Het Extensible Authentication Protocol (EAP) dat in deze handleiding wordt gebruikt, is Protected Extensible Authentication Protocol (PEAP). Naast dat de client is toegewezen aan een specifiek VLAN (anders dan de client die is toegewezen aan de WLAN-standaard).

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- 802,1x
- PEAP
- Certificeringsinstantie (CA)
- Certificaten

## **Gebruikte componenten**

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

ME v8.2

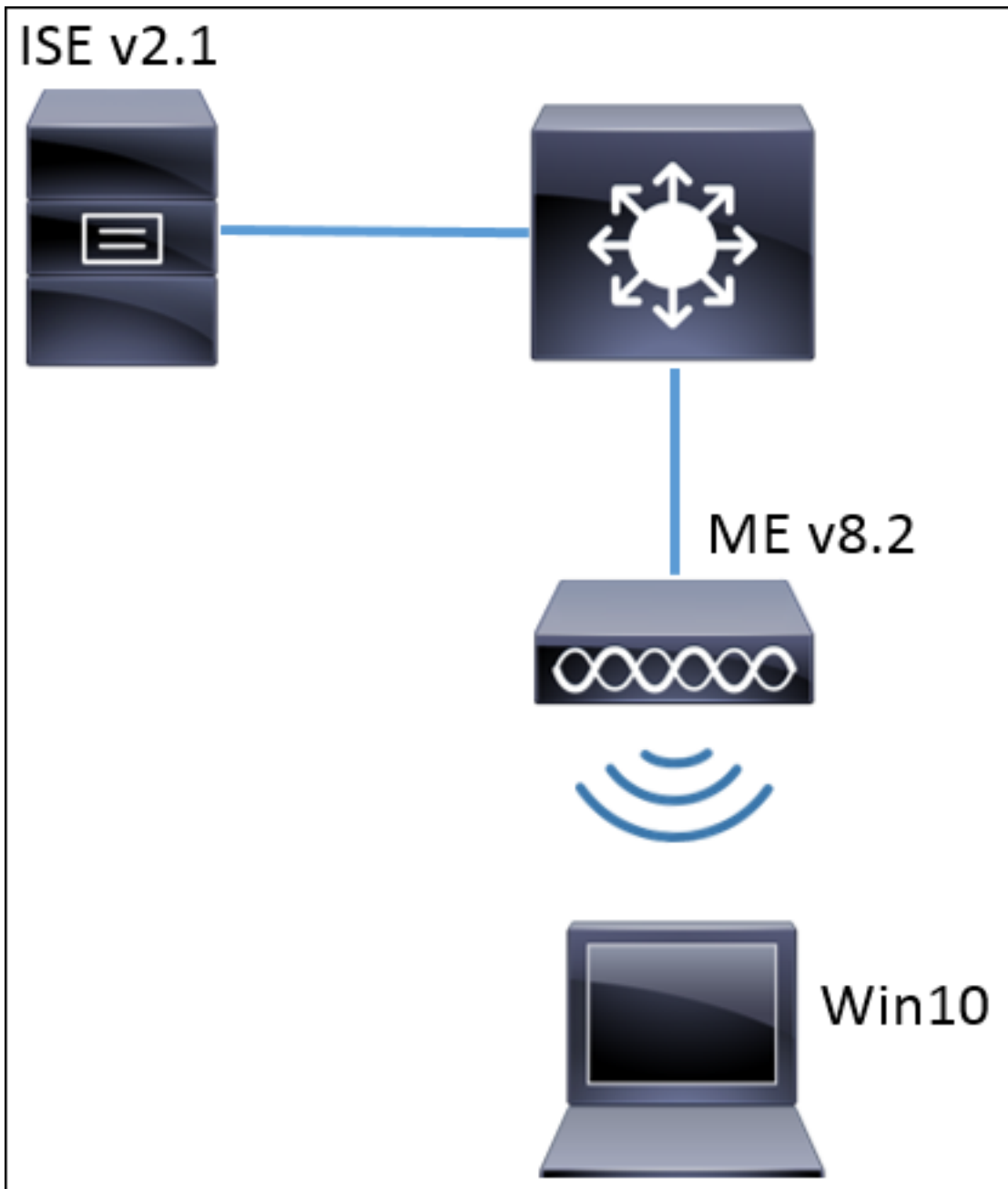
ISE v2.1

Windows 10-laptop

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**

### **Netwerkdigram**



### Configuraties

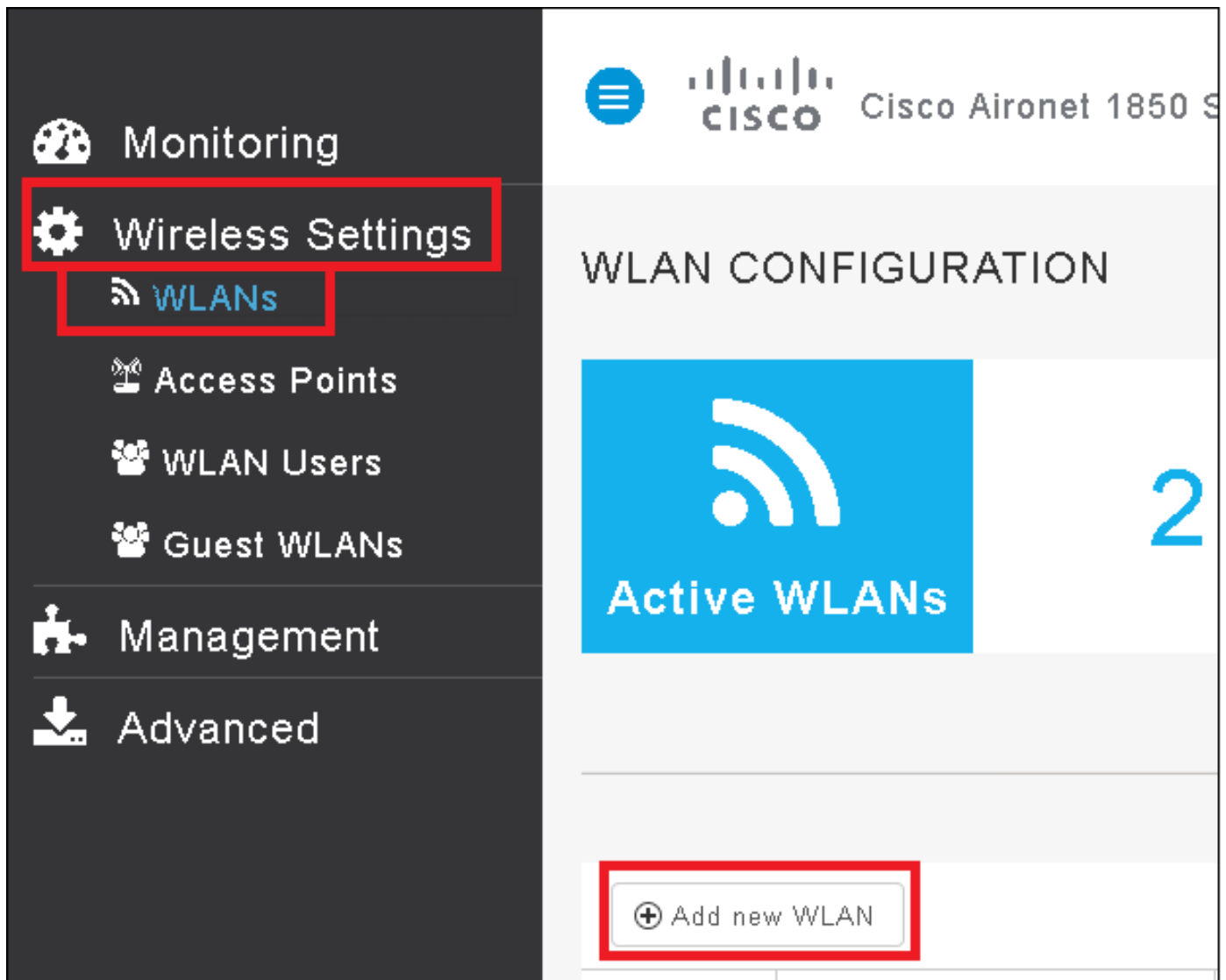
De algemene stappen zijn:

1. Maak de Service Set Identifier (SSID) in ME en verklaar RADIUS-server (ISE in dit voorbeeld) op ME
2. ME op RADIUS-server (ISE) verklaren
3. Maak de authenticatieregel op ISE
4. Maak de autorisatieregel op ISE
5. Het eindpunt configureren

### Configuratie op ME

Om communicatie tussen RADIUS-server en ME mogelijk te maken, moet de RADIUS-server op ME worden geregistreerd en vice versa. Deze stap laat zien hoe u RADIUS-server op ME kunt registreren.

Stap 1. Open de GUI van het menu en navigeer naar **Draadloze instellingen > WLAN's > Voeg nieuwe WLAN's toe**.



Stap 2. Selecteer een naam voor WLAN.

## Add New WLAN ✕

General **WLAN Security** VLAN & Firewall QoS

**WLAN Id** 3 ▼

**Profile Name \*** me-ise|

**SSID \*** me-ise

**Admin State** Enabled ▼

**Radio Policy** ALL ▼

✓ Apply ✕ Cancel

Stap 3. Specificeer de beveiligingsconfiguratie onder het tabblad **WLAN Security**.

Kies **WAP2 Enterprise**, voor verificatieserver kiest **Externe RADIUS**. Klik op de optie Bewerken om het IP-adres van de RADIUS toe te voegen en een **gedeelde** beveiligingstoets te kiezen.



# Add New WLAN



General WLAN Security VLAN & Firewall QoS

**Security** WPA2 Enterprise ▼

**Authentication Server** External Radius ▼

	Radius IP ▲	Radius Port	Shared Secret	
		1812	*****	▲
		1812	*****	▼

External Radius configuration applies to all WLANs

Apply

Cancel

Add New WLAN

General WLAN Security VLAN & Firewall QoS

Security WPA2 Enterprise

Authentication Server External Radius

Radius IP ▲ Radius Port Shared Secret

a.b.c.d 1812

⊙ ⊗

ⓘ Please enter valid IPv4 address

External Radius configuration applies to all WLANs

⊙ Apply ⊗ Cancel

<a.b.c.d> komt overeen met de RADIUS-server.

Stap 4. Pas een VLAN aan SSID toe.

Als SSID aan het VLAN van AP moet worden toegewezen kan deze stap worden overgeslagen.

Als u de gebruikers voor deze SSID aan een specifiek VLAN wilt toewijzen (anders dan VLAN van AP), schakelt u **VLAN-tagging** in en wijst u de gewenste **VLAN-id** toe.

## Add New WLAN ✕

General   **WLAN Security**   VLAN & Firewall   QoS

**Use VLAN Tagging** Yes ▼

**VLAN ID \*** 2400 ▼

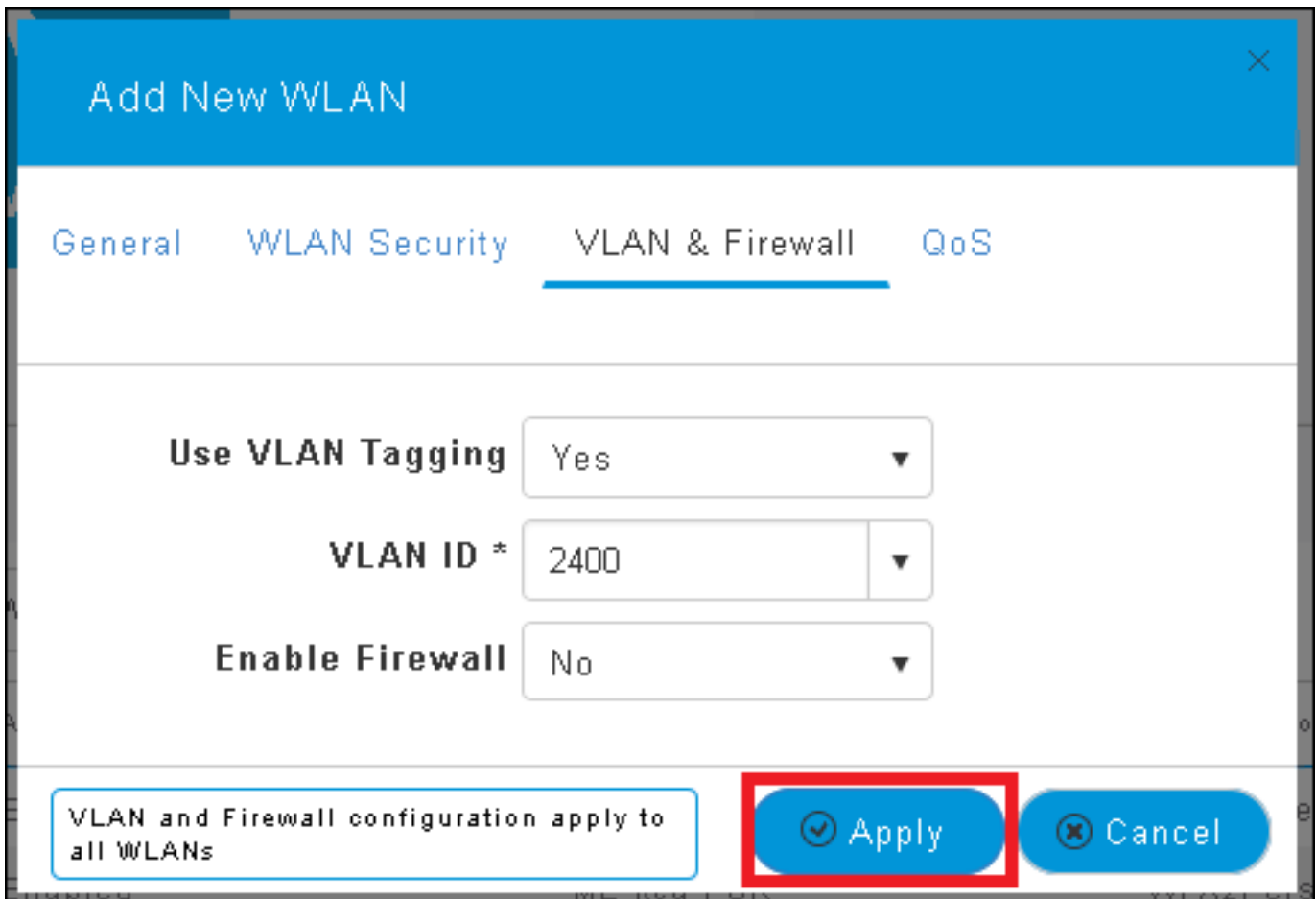
**Enable Firewall** No ▼

VLAN and Firewall configuration apply to all WLANs

Opmerking: Als VLAN-markering wordt gebruikt, zorg er dan voor dat de switchpoort waar het access point is aangesloten, is ingesteld als boomstampoort en dat AP VLAN als native VLAN is geconfigureerd.

Stap 5. Klik op **Toepassen** om de configuratie te voltooien.





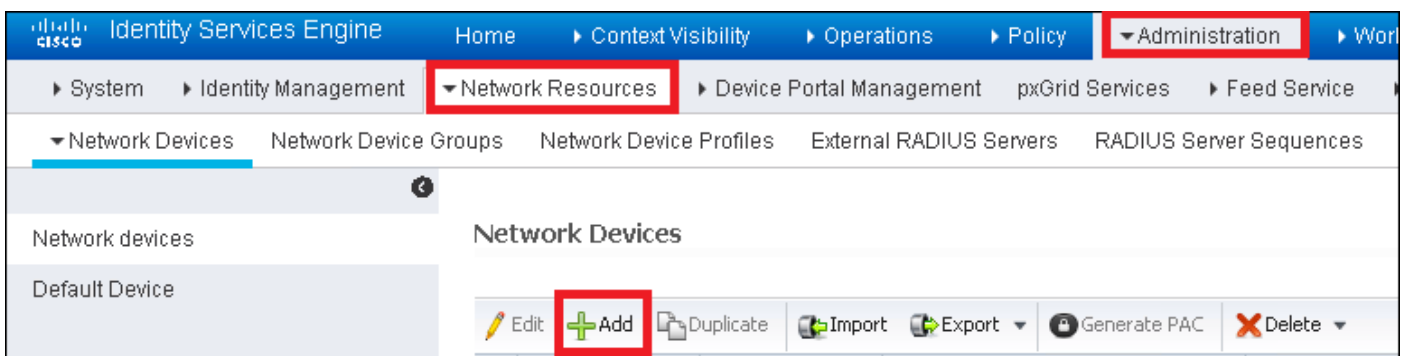
Stap 6. Optioneel: configureer de WLAN-functie om de VLAN-excuus te aanvaarden.

AAA-voorrang op WLAN inschakelen en de benodigde VLAN's toevoegen. U moet daarom een CLI-sessie openen naar de ME-beheerinterface en deze opdrachten uitvoeren:

```
>config wlan disable <wlan-id>  
>config wlan aaa-override enable <wlan-id>  
>config wlan enable <wlan-id>  
>config flexconnect group default-flexgroup vlan add <vlan-id>
```

**ME op ISE verklaren**

Stap 1. Open ISE-console en navigeer naar **Beheer > Netwerkbronnen > Netwerkkapitalen > Toevoegen**.



Stap 2. Voer de informatie in.

Optioneel kan er een modelnaam, softwareversie, beschrijving en toewijzen aan

netwerkapparaatgroepen op basis van apparaattypen, locaties of WLC's.

a.b.c.d. komt overeen met het IP-adres van de ME.

Network Devices List > New Network Device

### Network Devices

\* Name

Description

---

\* IP Address:  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Device Type

Location

WLCs

---

**RADIUS Authentication Settings**

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

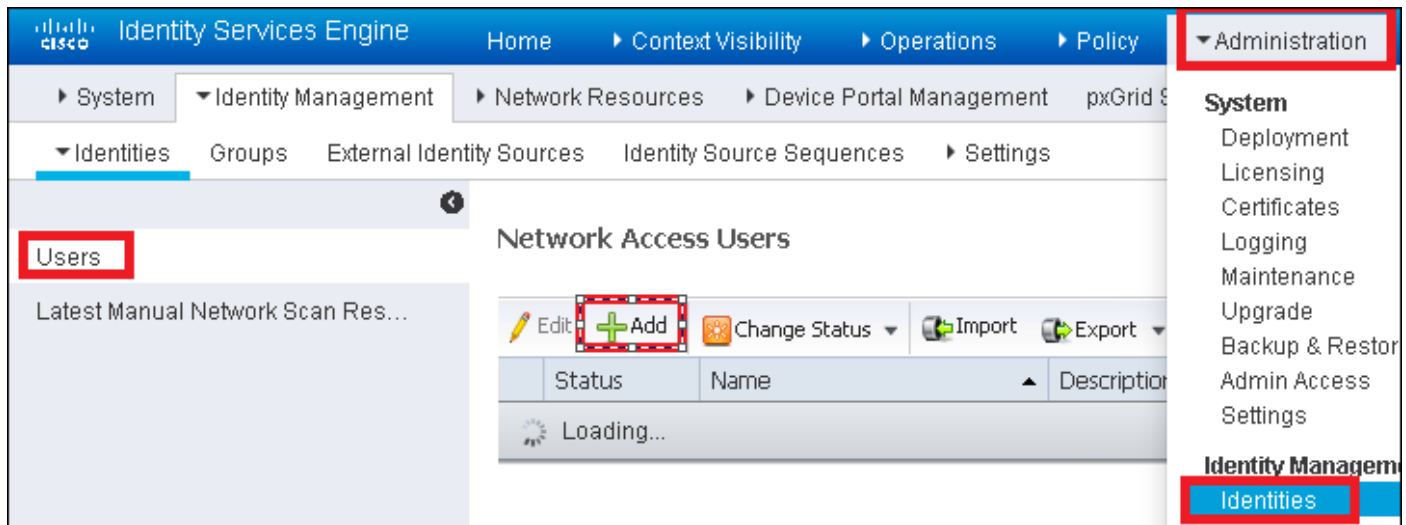
CoA Port

Zie deze link voor meer informatie over Network Devices Group:

## [ISE - Netwerkapparaatgroepen](#)

Een nieuwe gebruiker op ISE maken

Stap 1. navigeren naar **Administratie > identiteitsbeheer > Identiteiten > Gebruikers > Toevoegen.**



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation at the top reads: Home > Context Visibility > Operations > Policy > Administration. The 'Administration' menu is expanded, showing options like System, Identity Management, and Identities. The 'Identities' option is highlighted in blue. The main content area is titled 'Network Access Users' and features a toolbar with buttons for Edit, Add, Change Status, Import, and Export. The 'Add' button is highlighted with a red dashed box. Below the toolbar is a table with columns for Status, Name, and Description, which is currently loading.

Stap 2. Voer de informatie in.

In dit voorbeeld hoort deze gebruiker tot een groep die ALL\_ACCOUNTS heet, maar kan hij indien nodig worden aangepast.

▼ Network Access User

\* Name

Status  Enabled ▼

Email

▼ Passwords

Password Type:  ▼

Password

Re-Enter Passw

\* Login Password

Enable Password

▼ User Information

First Name

Last Name

▼ Account Options

Description

Change password on next login

▼ Account Disable Policy

Disable account if date exceeds

▼ User Groups

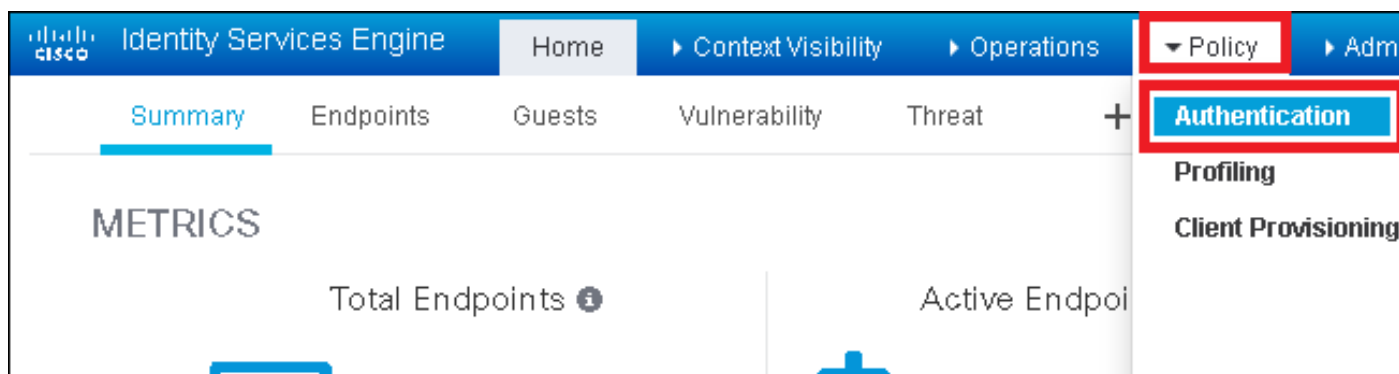
+

De verificatieregel maken

De verificatieregels worden gebruikt om te controleren of de aanmeldingsgegevens van de gebruikers juist zijn (Controleer of de gebruiker echt zegt wie het is) en om de verificatiemethoden

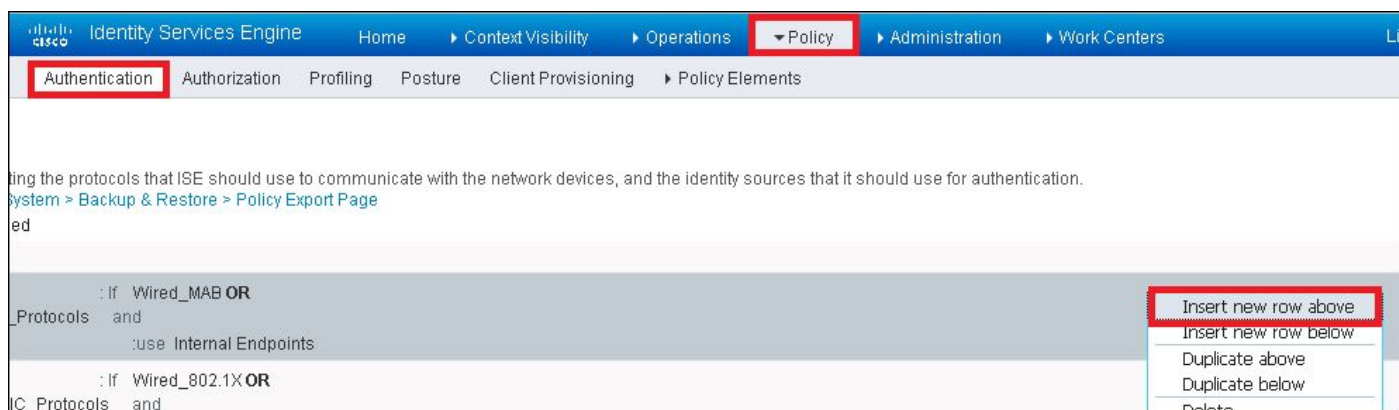
te beperken die door de gebruiker mogen worden gebruikt.

Stap 1. navigeren naar **Policy > Verificatie**.



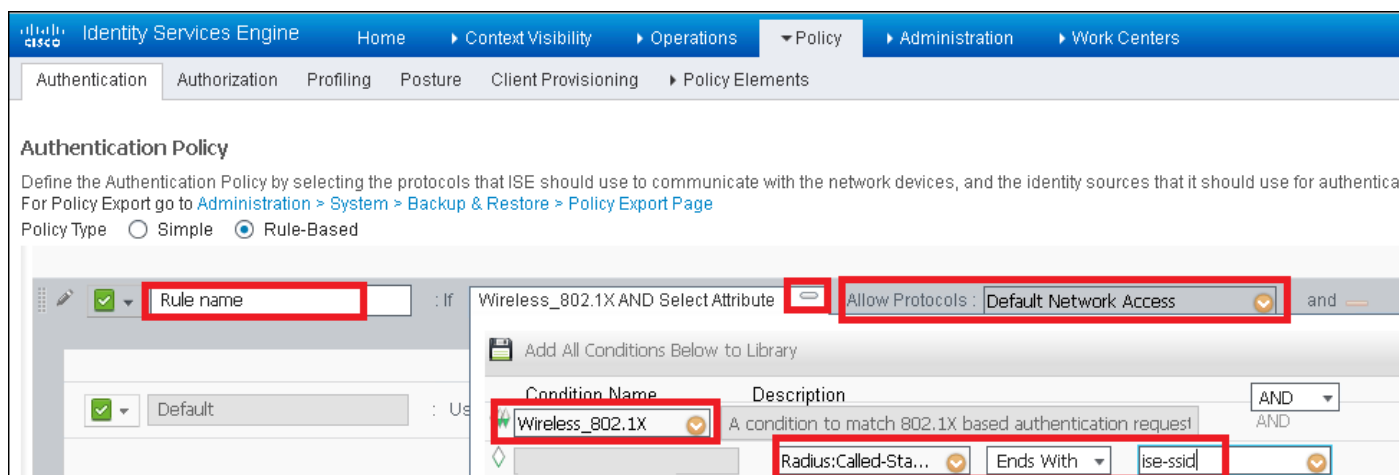
Stap 2. Plaats een nieuwe verificatieregel.

Om dit te doen navigeer naar **Policy > Verificatie > Nieuwe rij boven/onder invoegen**.

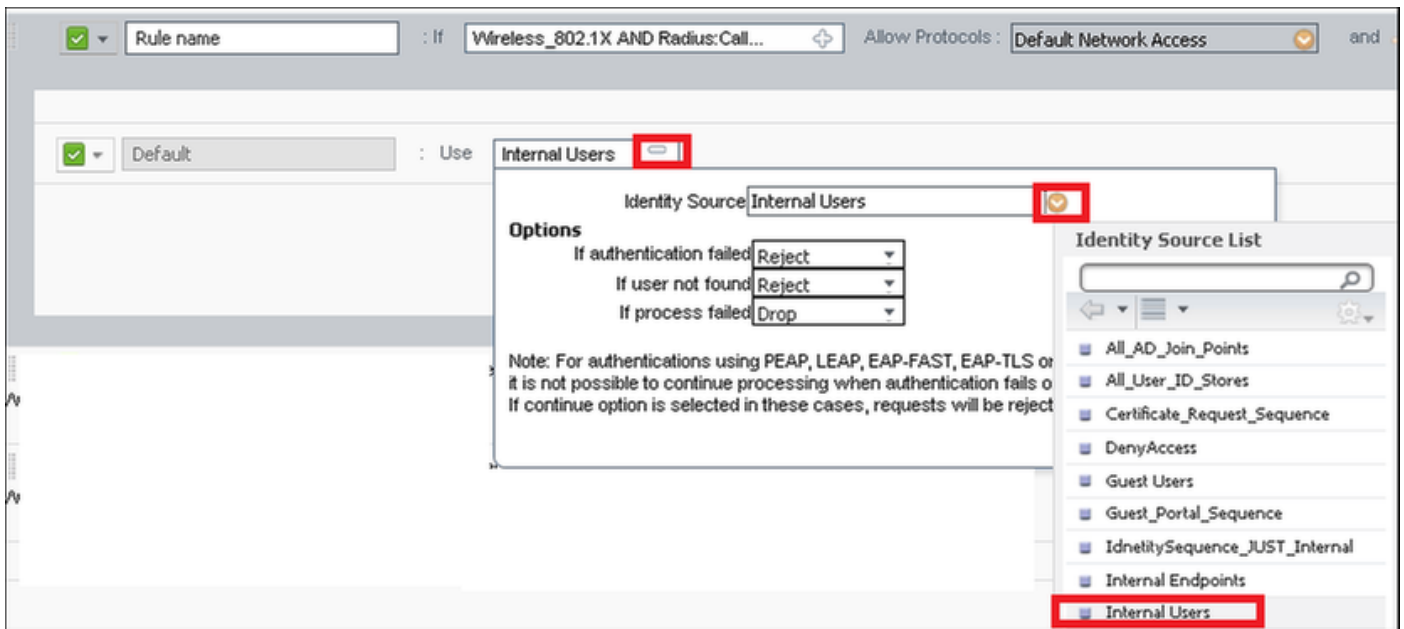


Stap 3. Voer de gewenste informatie in

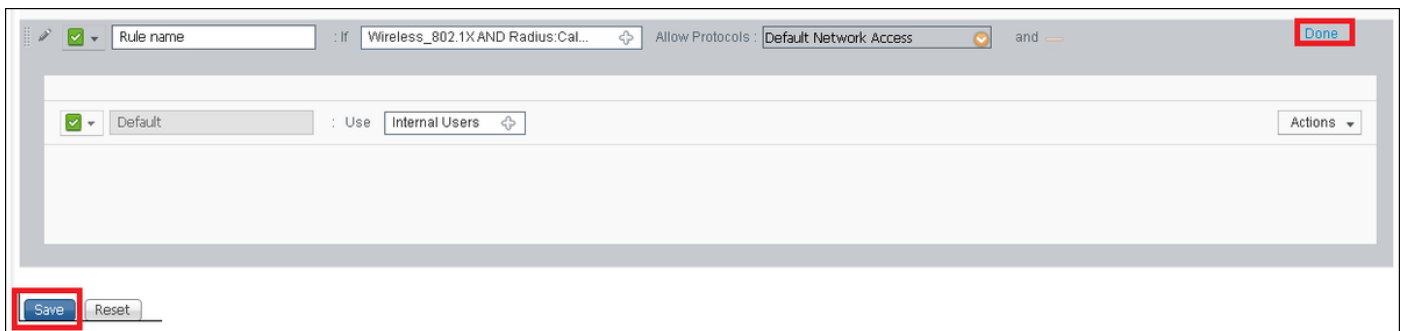
Dit voorbeeld van de authenticatieregel staat alle protocollen toe die onder de lijst van de **Standaardnetwerktoegang** staan, dit is van toepassing op de authenticatieaanvraag voor draadloze 802.1x-clients en met geroepen-station-ID en eindigt met *standaard-id*.



Kies ook de bron van de identiteit voor de klanten die deze authenticatieregel aanpast, in dit voorbeeld wordt het gebruikt *Interne gebruikers*



Klik na voltooiing van het programma op **Gereed** en **Opslaan**



Zie voor meer informatie over litiging van protocollen deze link:

[Toegestane protocolservice](#)

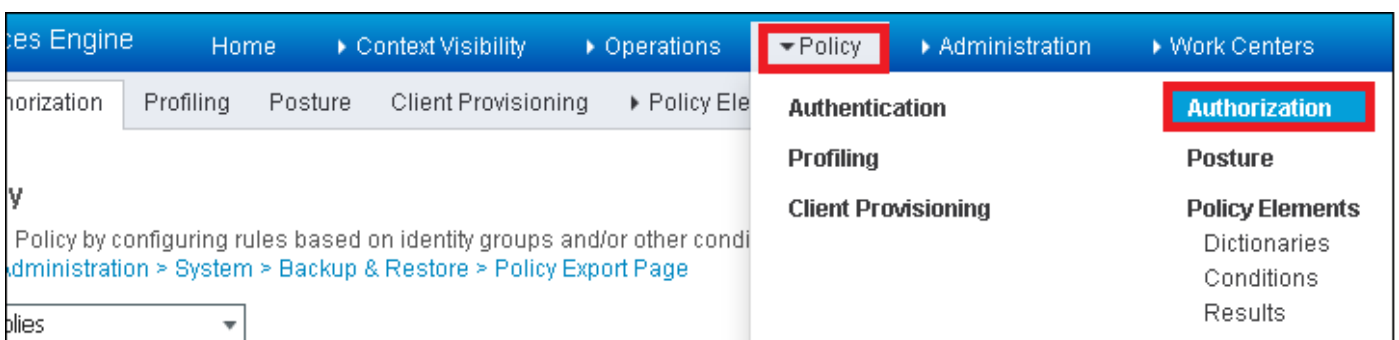
Zie voor meer informatie over identiteitsbronnen de volgende link:

[Een gebruikersidentiteitsgroep maken](#)

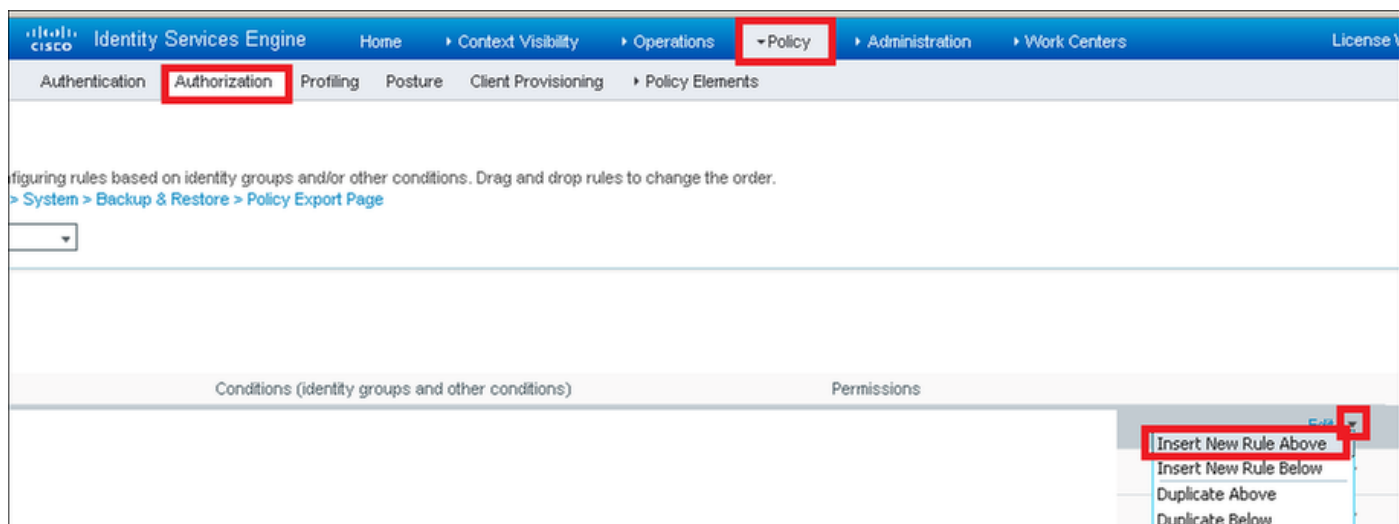
**Maak de autorisatieregel**

De machtigingsregel is degene die bepaalt of de cliënt al dan niet tot het netwerk mag toetreden

Stap 1. Navigeer naar **beleid > autorisatie**.

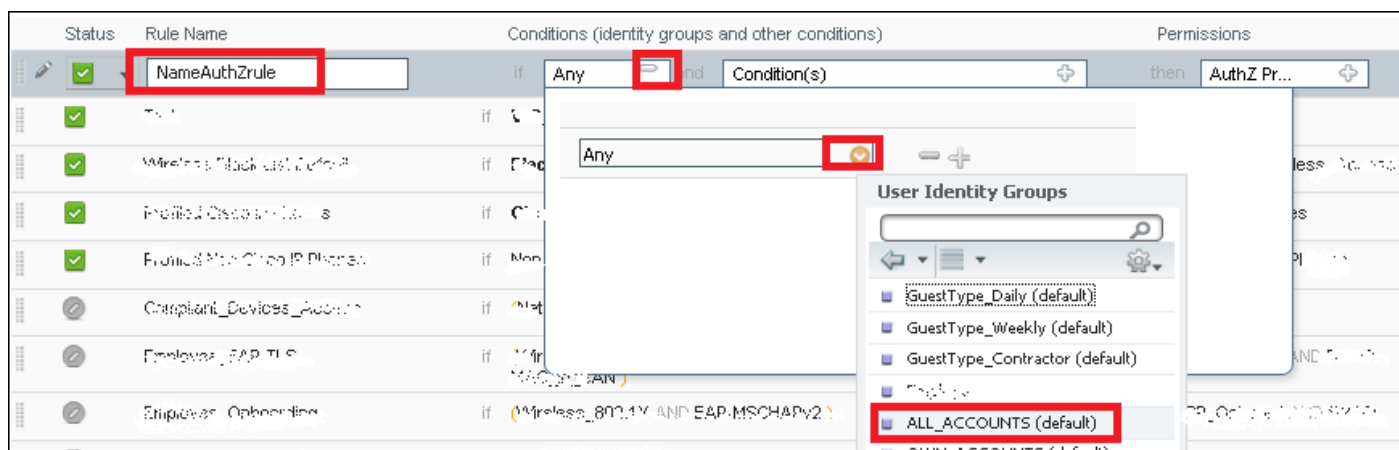


Stap 2. Plaats een nieuwe regel. Navigeren in op **beleid > autorisatie > Nieuwe regel** hierboven/hieronder invoegen.

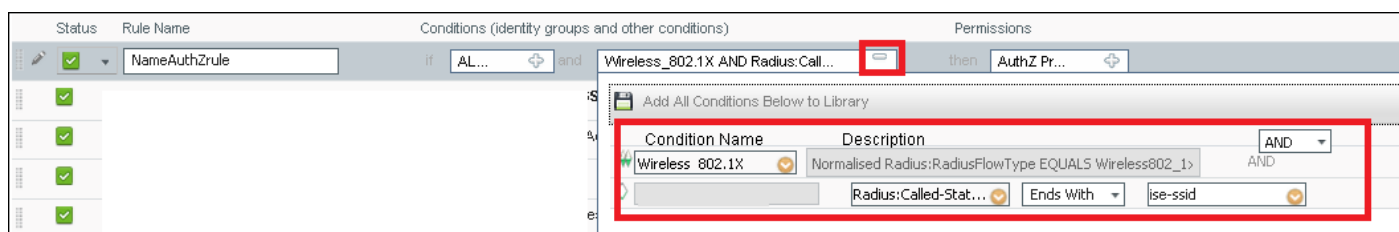


Stap 3. Voer de informatie in.

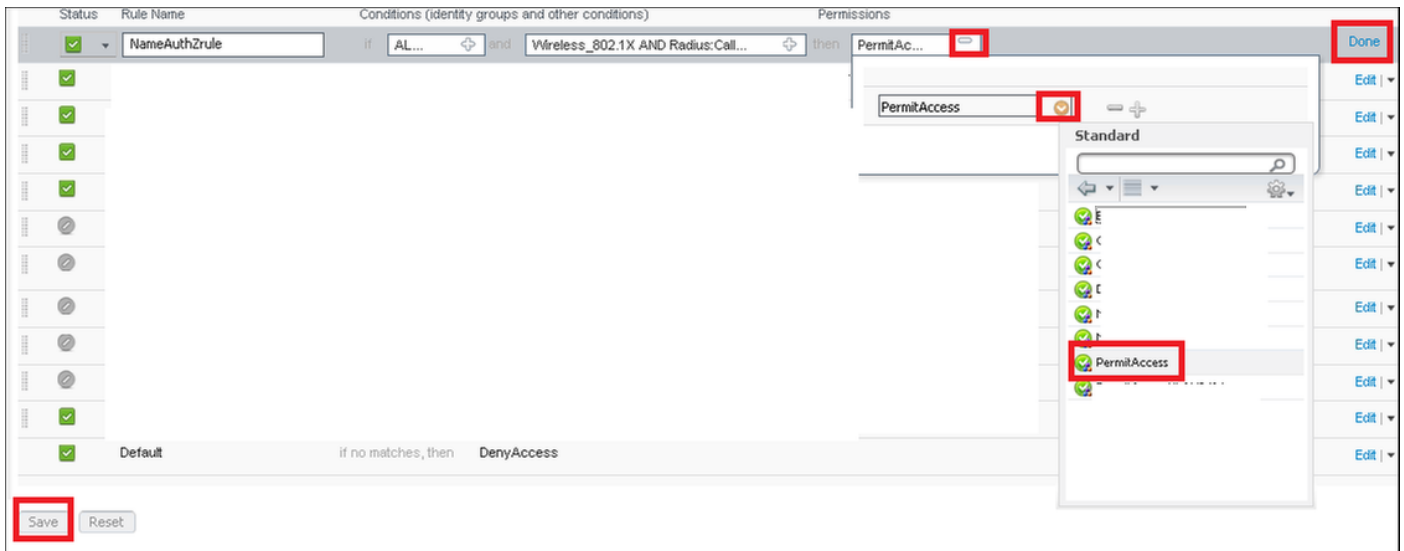
Kies eerst een naam voor de regel en de identiteitsgroepen waar de gebruiker is opgeslagen. In dit voorbeeld wordt de gebruiker opgeslagen in groep **ALL\_ACCOUNTS**.



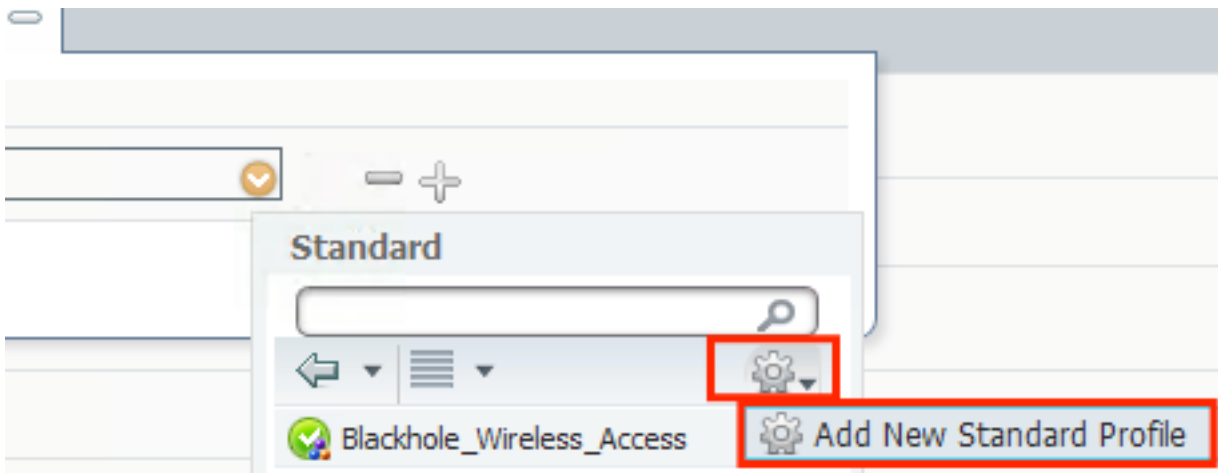
Daarna worden andere voorwaarden gekozen waardoor de vergunningsprocedure onder deze regel valt. In dit voorbeeld bereikt het vergunningsproces deze regel als het 802.1x Wireless gebruikt en het station ID eindigt met *ise-ssid*.



Kies ten slotte het autorisatieprofiel waarmee de klanten zich bij het netwerk kunnen aansluiten, klik op **Gereed** en **Opslaan**.



Optioneel maakt u een nieuw autorisatieprofiel dat de draadloze client aan een ander VLAN zal toewijzen:



Voer de informatie in:



**Add New Standard Profile**

**Authorization Profile**

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

---

**Common Tasks**

DAACL Name

ACL (Filter-ID)

VLAN

Voice Domain Permission

---

**Advanced Attributes Settings**

Select an item  =

---

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
Tunnel-Private-Group-ID = 1:van-id  
Tunnel-Type = 1:13  
Tunnel-Medium-Type = 1:6

## Configuratie van het eindapparaat

Configureer een Windows 10-laptop met het oog op de aansluiting op een SSID met 802.1x-verificatie met behulp van PEAP/MS-CHAPv2 (Microsoft versie van het Challenge-Handshake Authentication Protocol, versie 2).

In dit configuratievoorbeeld gebruikt ISE zijn zelfgetekende certificaat om de authenticatie uit te voeren.

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

1. Installeer het zelf ondertekende certificaat op de machine om ISE-server te valideren en te vertrouwen om de verificatie te voltooien
2. omzeilen de validatie van de RADIUS-server en vertrouwen op elke RADIUS-server die gebruikt wordt om de verificatie uit te voeren (niet aanbevolen, omdat dit een beveiligingsprobleem kan worden)

De configuratie voor deze opties wordt uitgelegd op de [configuratie van het eindapparaat - Maak het WLAN-profiel - Stap 7](#).

## End-of-support configuratie - Installeer ISE-zichzelf getekend certificaat

Stap 1. Exporteren van zelf ondertekend certificaat van ISE.

Meld u aan bij ISE en navigeer naar **Administratie > Systeem > Certificaten > Systeemcertificaten**.

Selecteer vervolgens het certificaat dat wordt gebruikt voor **EAP-verificatie** en klik op **Exporteren**.

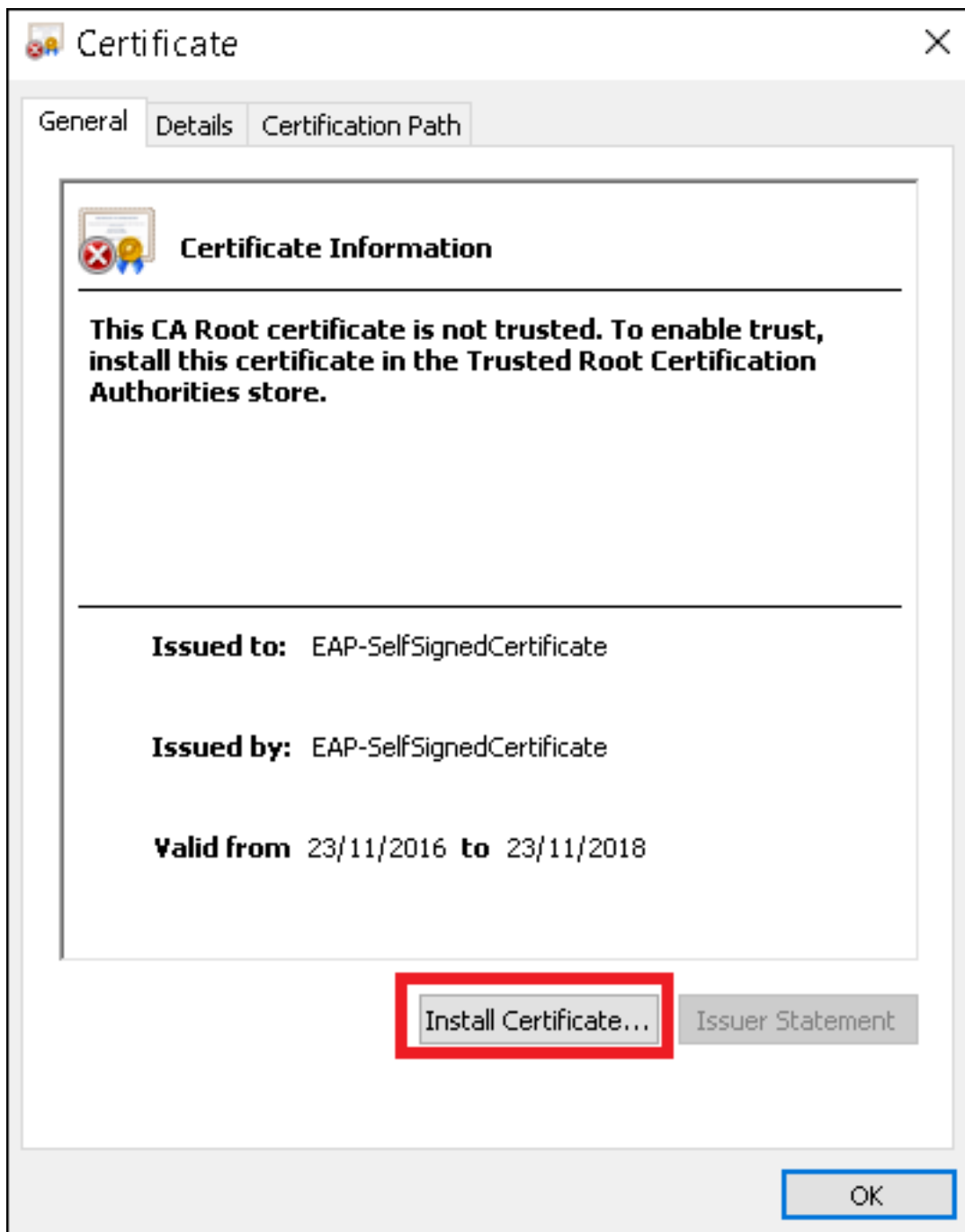
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes 'System', 'Administration', and 'Certificates'. The main area displays 'System Certificates' with a warning icon and the text: 'For disaster recovery it is recommended to export certificate ar'. Below this, there are buttons for 'Edit', 'Generate Self Signed Certificate', 'Import', 'Export', and 'Delete'. A table of certificates is shown with columns for 'Friendly Name', 'Used By', and 'Portal group tag'. One certificate is selected, with a checkbox checked and the text 'EAP Authentication' visible.

Sla het certificaat op de gewenste locatie op. Dit certificaat is geïnstalleerd in Windows.

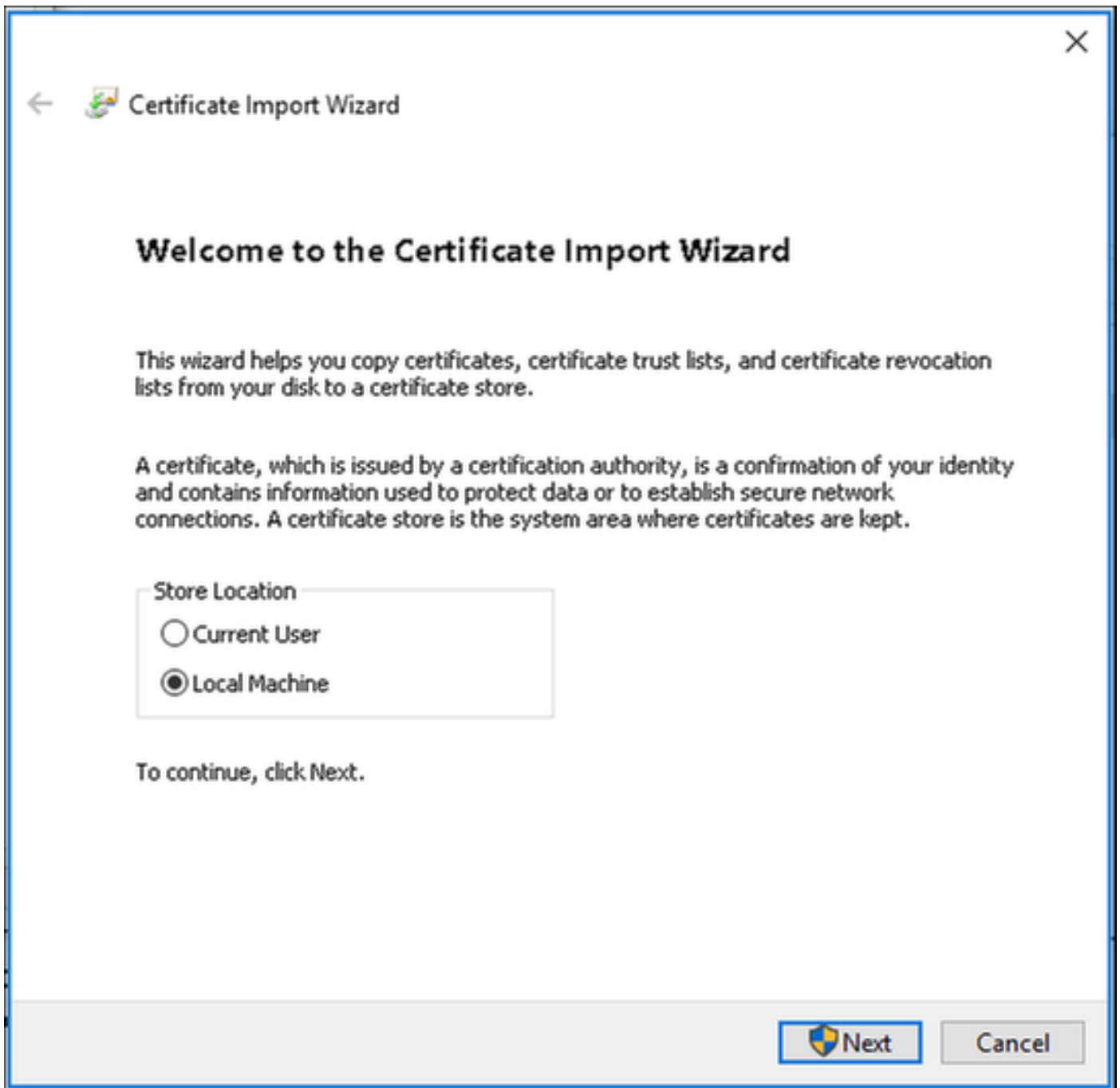
The screenshot shows the 'Export Certificate' dialog box in the ISE console. The title is 'Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001''. There are two radio button options: 'Export Certificate Only' (selected) and 'Export Certificate and Private Key'. Below these are input fields for '\*Private Key Password' and '\*Confirm Password'. A warning message is displayed at the bottom: 'Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.' At the bottom right, there are 'Export' and 'Cancel' buttons.

Stap 2. Installeer het certificaat in het Windows-apparaat.

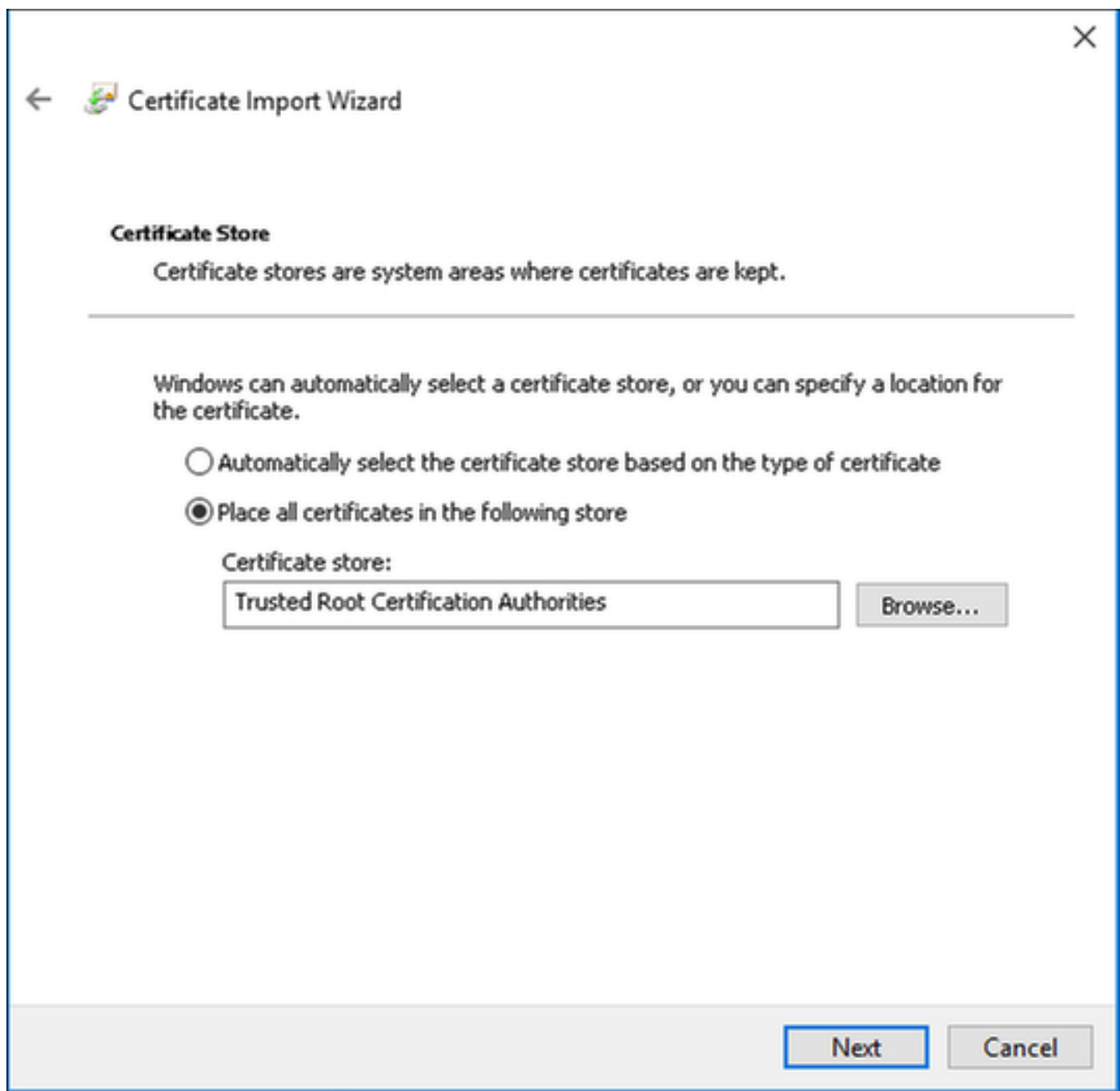
Kopieer het certificaat dat voor het eerst naar de Windows-machine is geëxporteerd, wijzig de uitbreiding van het bestand van .pem naar .crt nadat u op deze dubbelklik en selecteer **Installeer Certificaat....**



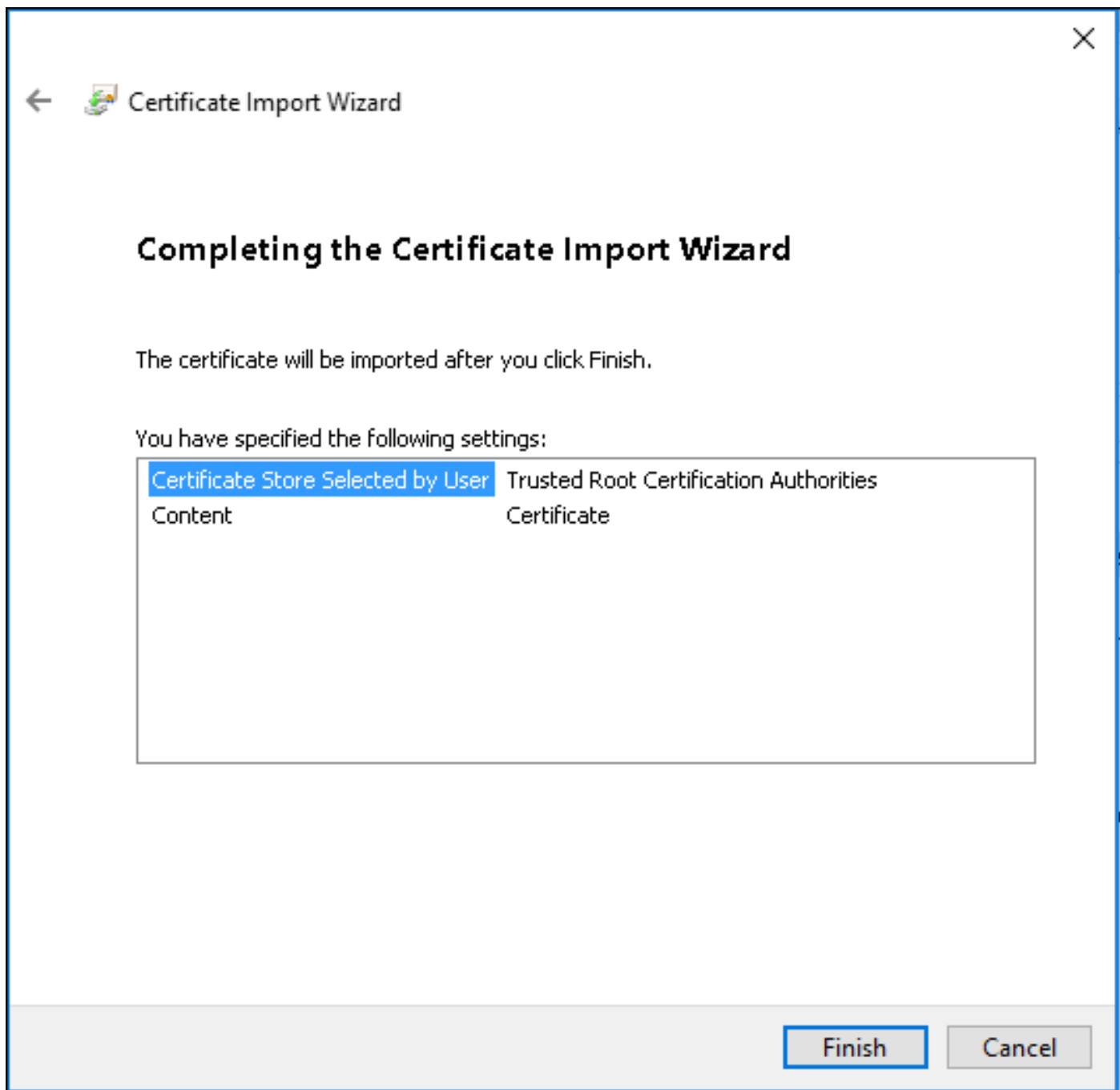
Kies om het in **Lokale machine** te installeren, en klik op **Volgende**.



Selecteer **Plaats alle certificaten in de volgende winkel** en blader vervolgens en kies **Trusted Root Certified-autoriteiten**. Klik vervolgens op **Volgende**.



Klik vervolgens op **Voltoeien**.



Klik aan het einde op **Ja** om de installatie van het certificaat te bevestigen.

## Security Warning



You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Thumbprint (sha1): 011A193D 70C7713D 0204E3D0 4759215D  
4294213C

### Warning:

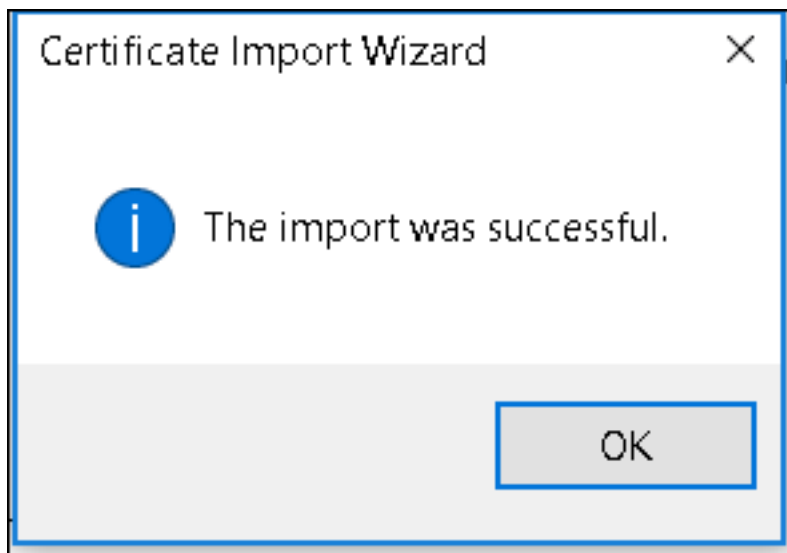
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes

No

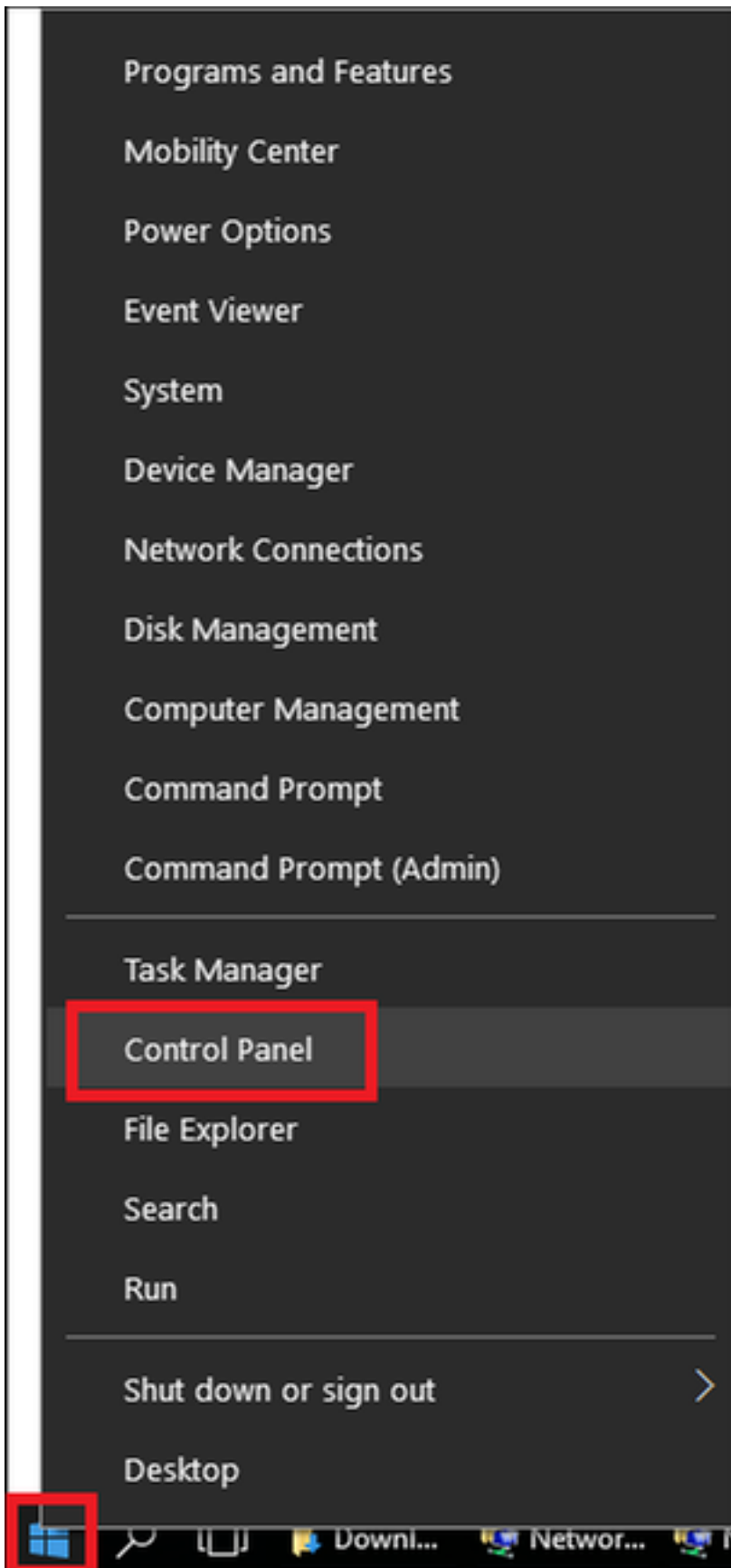
Klik tot slot op OK.



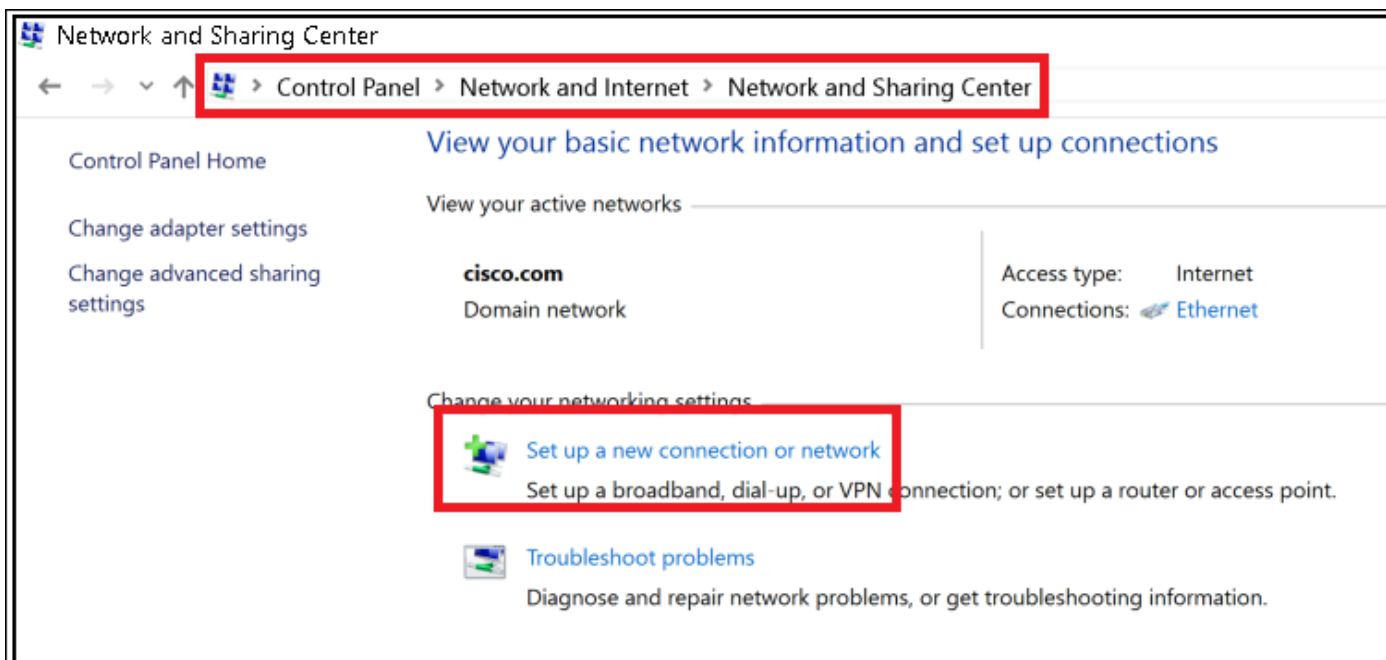
End-of-support configuratie - maakt WLAN-profiel

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

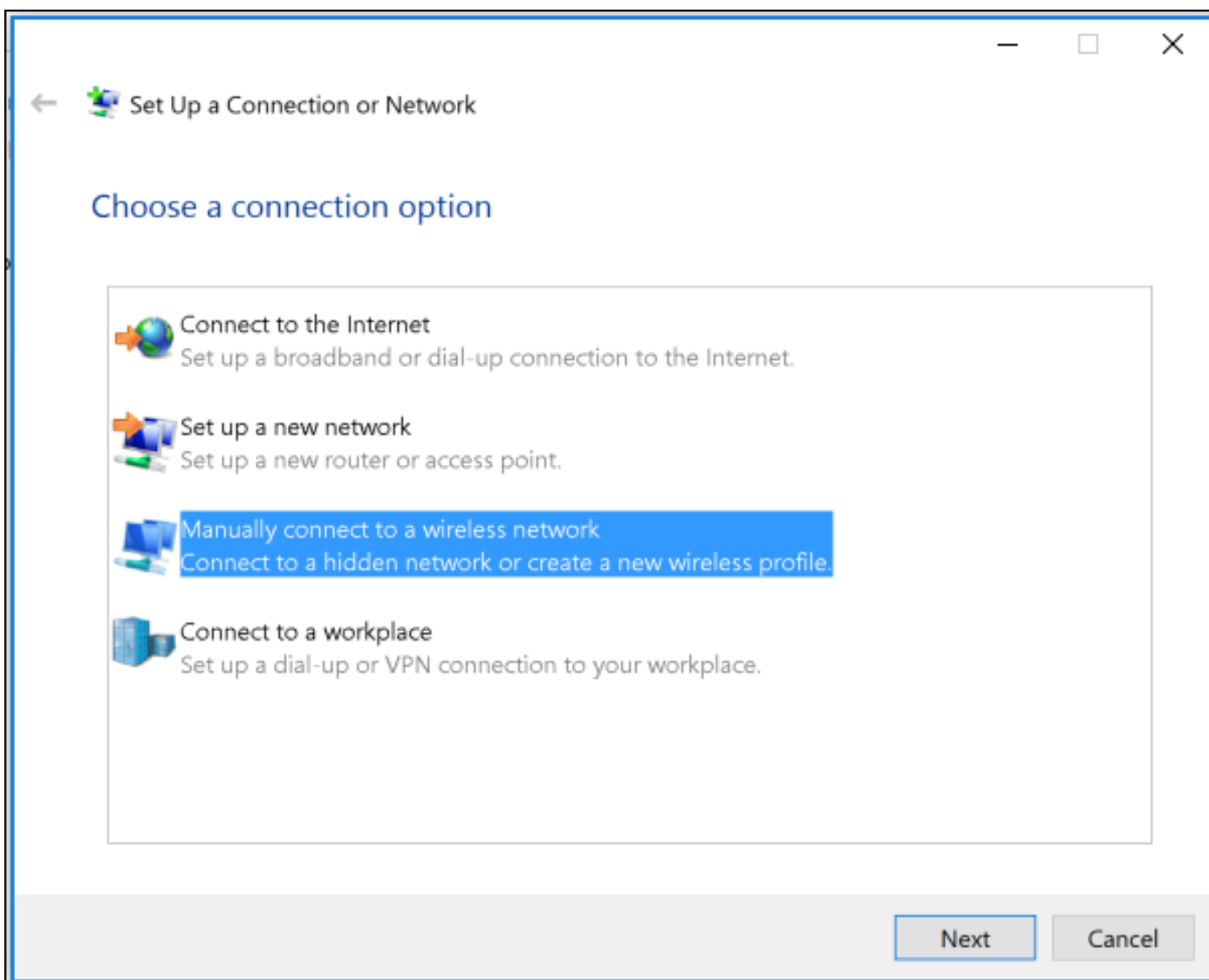




Stap 2. Navigeer naar **Netwerk en Internet** en vervolgens naar **Netwerk- en Sharing Center** en klik op **Stel een nieuwe verbinding of een netwerk in**.



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



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

← Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

Security Key:   Hide characters

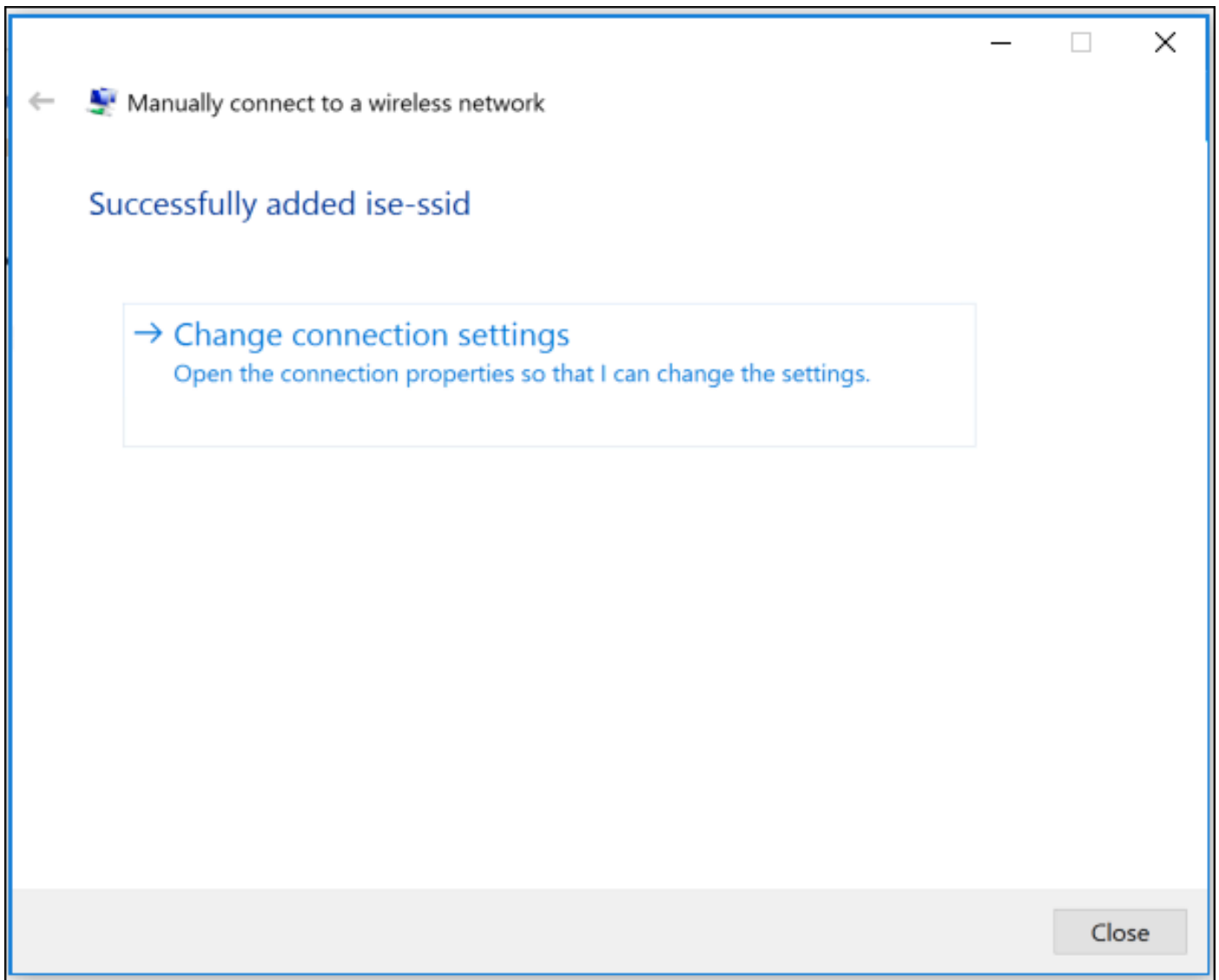
Start this connection automatically

Connect even if the network is not broadcasting

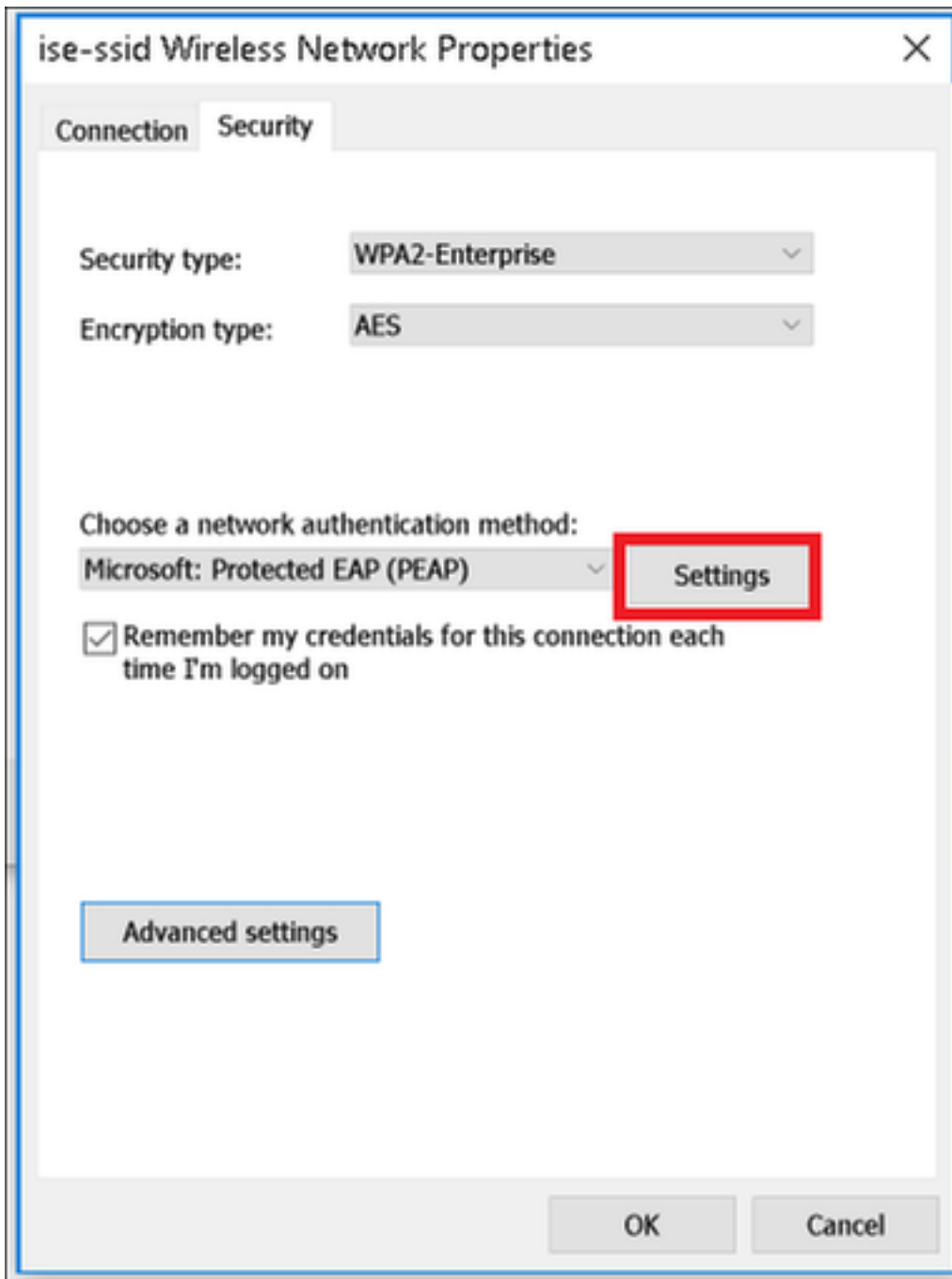
Warning: If you select this option, your computer's privacy might be at risk.

Next Cancel

Stap 5. Selecteer **Wijzig de verbindinginstellingen** om de configuratie van het WLAN-profiel aan te passen.



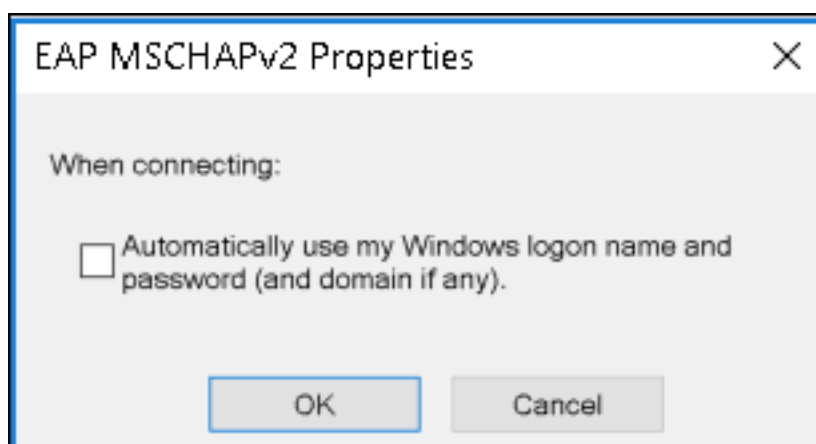
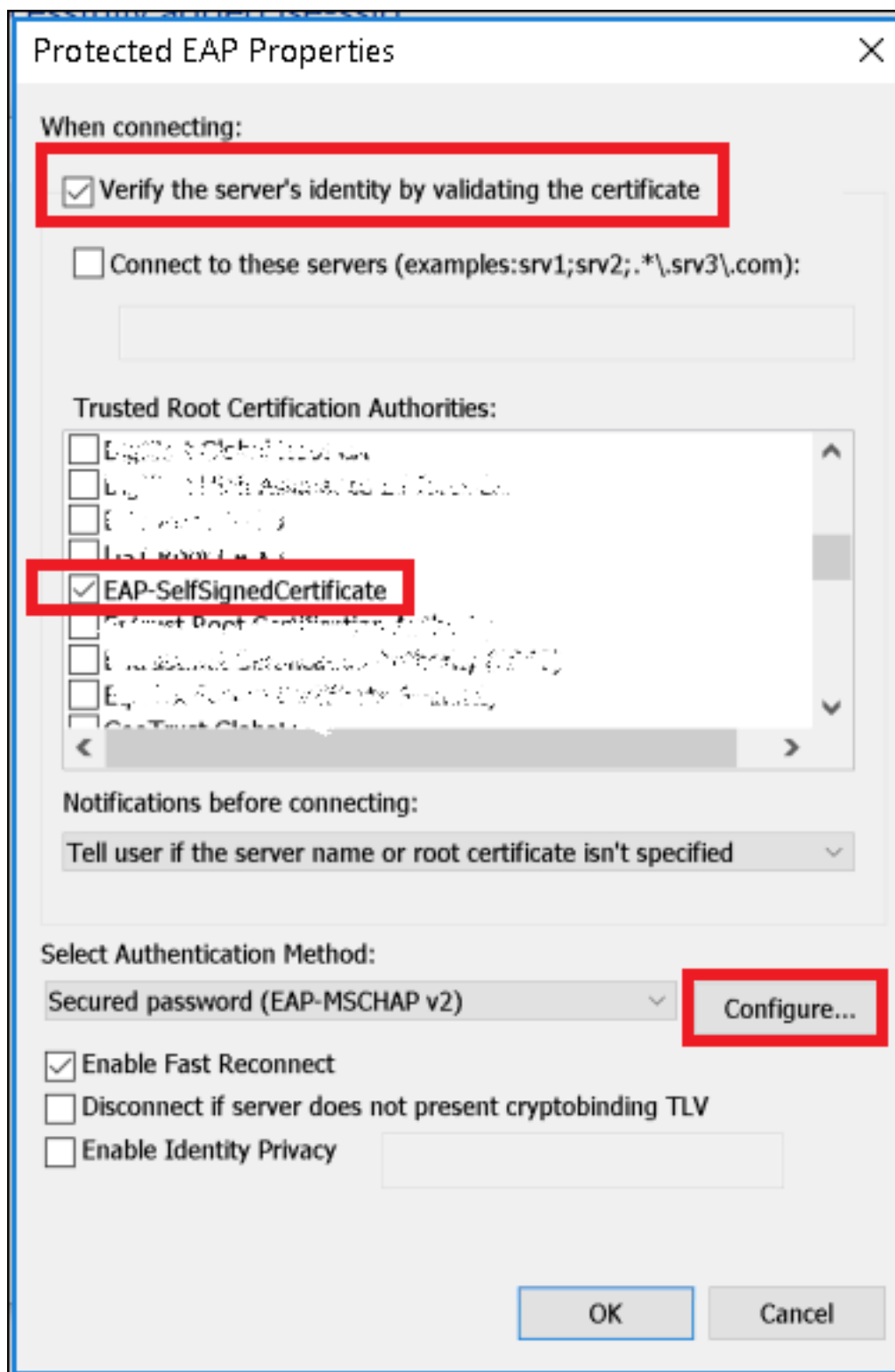
Stap 6. Navigeer naar het tabblad **Security** en klik op **Instellingen**.



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

Indien ja, schakelt u **de identiteit van de server in door het certificaat te valideren** en van de **Trusted Root-certificeringsinstanties**: selecteer de lijst met de zelf ondertekende ISE-certificaten.

Nadat u **Mijn Windows**-aanmelding en wachtwoord hebt **ingesteld** en uitgeschakeld, **gebruikt u** automatisch **OK**.



## Stap 8. Configureer de gebruikersreferenties

Als u weer terug bent op het tabblad **Beveiliging**, selecteert u **Geavanceerde instellingen**, specificeert u de verificatiemodus als **gebruikersverificatie** en slaat u de referenties op die op ISE zijn ingesteld om de gebruiker voor authentiek te verklaren.



## Advanced settings



802.1X settings

802.11 settings

Specify authentication mode:

User authentication

Save credentials

Delete credentials for all users

Enable single sign on for this network

Perform immediately before user logon

Perform immediately after user logon

Maximum delay (seconds):

10

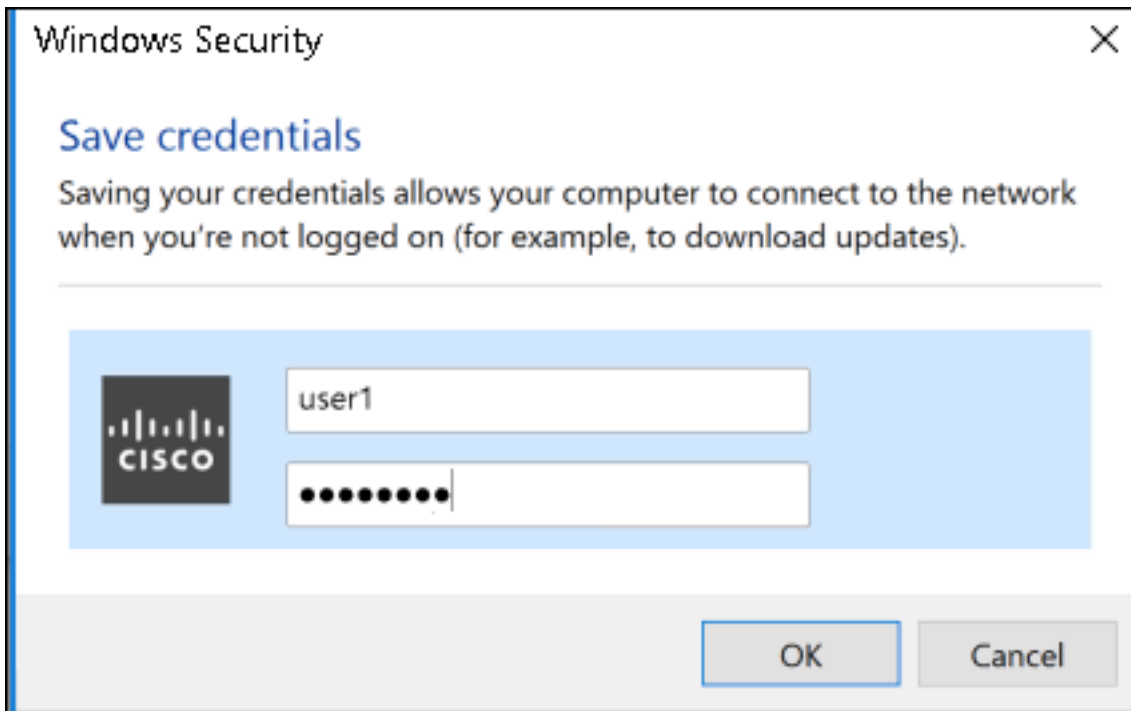
Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

OK

Cancel





## Verifiëren

De verificatiestroom kan vanuit WLC of ISE-perspectief worden geverifieerd.

### Verificatieproces op ME

Start deze opdracht om het verificatieproces voor een specifieke gebruiker te controleren:

```
> debug client <mac-add-client>
```

Voorbeeld van een succesvolle authenticatie (sommige output is weggelaten):

```
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Processing assoc-req  
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80  
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on  
BSSID 38:ed:18:c6:7b:4d AP 1852-4  
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging  
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'  
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface  
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'  
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific  
apfMsAccessVlan = 2400  
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed  
later from AAA after L2 Auth  
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management  
suite, enabling dot1x Authentication  
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 START (0) Change state to  
AUTHCHECK (2) last state START (0)  
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to  
8021X_REQD (3) last state AUTHCHECK (2)  
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on
```

**AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client**

\*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is 0

\*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId: 48)

\*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0

\*apfMsConnTask\_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3**

\*apfMsConnTask\_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1**

\*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth\_sm state transition 0 ---> 1 for mobile 08:74:02:77:13:45 at 1x\_reauth\_sm.c:47

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3 is disabled - applying Global eap timers and retries

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Connecting state

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: **08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1)**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45**

.

.

.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for station 08:74:02:77:13:45 (RSN 2)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cache at index 0 for station 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: New PMKID: (16)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility handoff

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can take care of same.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:13:45 (EAP Id 70)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: Including PMKID in M1 (16)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: M1 - Key Data: (22)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: **08:74:02:77:13:45 Starting key exchange to mobile**

08:74:02:77:13:45, data packets will be dropped

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile

08:74:02:77:13:45

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70) for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticating state for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Authenticated state

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-key in PTK\_START state (message 2) from mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!!

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!!!!

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0.....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 .....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f .....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 ....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45

state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 8021X\_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X\_REQD (3)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce :

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload:

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 255.255.255.224

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name:

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP\_REQD (7) last state L2AUTHCOMPLETE (4)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7)

pemAdvanceState2 6623, Adding TMP rule

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7) Adding Fast Path rule

type = Airespace AP - Learn IP address

```

on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role
update request from Unassociated to Local
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
6261, Adding TMP rule
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast
Path rule
type = Airespace AP - Learn IP address
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255,
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug:
regType=1 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller
apf_ms.c:3593)
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.841: 08:74:02:77:13:45 172.16.0.16 DHCP_REQD (7) Change state
to RUN (20) last state DHCP_REQD (7)

```

Voor een makkelijke manier om debug client-uitgangen te lezen, gebruikt u het gereedschap *Draadloze debug-analyzer*.

## [Draadloze debug Analyzer](#)

### Verificatieproces op ISE

Navigeer naar **operaties > RADIUS > Live Logs** om te zien welk authenticatiebeleid, autorisatiebeleid en autorisatieprofiel aan de gebruiker is toegewezen.

Time	Sta...	Details	Ide...	Endpoint ID	Endpoint ...	Authentication Policy	Authorization Policy	Authorization Profiles
No...			user1	08:74:02:77:13:45	Apple-Device	Default >> Rule name >> Default	Default >> NameAuthZrule	PermitAccess

Voor meer informatie klik op **Details** om een gedetailleerder authenticatieproces te zien.