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

# Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Configureren **Netwerkdiagram** 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 (WAP2) Enterprise-beveiliging met een Mobility Expresscontroller 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

Netwerkdiagram



### 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 Ne	ew WLAN		×
General	WLAN Security	VLAN & Firewall	QoS
	WLAN Id	3	•
	Profile Name *	me-ise	
	SSID *	me-ise	
	Admin State	Enabled	•
	Radio Policy	ALL	•
		( ⊘ A	pply 🛞 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 N	ew WLAN	×
General	WLAN Security	VLAN & Firewall QoS
Authe	Security ntication Server	WPA2 Enterprise  • External Radius  •
<ul> <li>⊘</li> <li></li> <li>&lt;</li></ul>	Radius IP 🛦	Radius Port Shared Secret          1812       •••••••         e enter valid IPv4 address       •••••••
External F all WLANs	Radius configuration a	applies to 🛛 📿 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 all WLANs	n apply to 🛛 📿 Apply 🛞 Cancel

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.

Add New WLAN	×
General WLAN Security	VLAN & Firewall QoS
Use VLAN lagging	Yes
VLAN ID *	2400 🔻
Enable Firewall	No
VLAN and Firewall configuration all WLANs	n apply to 🛛 🖉 Apply 🛞 Cancel

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 uitgeven:

```
>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 > Netwerkapparaten > Toevoegen.** 

dialo Identity Serv	/ices Engine Hom	e 🔹 🕨 Context Visibility	♦ Operations	olicy Administration Worl
▶ System → Ident	tity Management 🛛 🖵 Net	vork Resources 🔹 🕨 Dev	ce Portal Management	pxGrid Services
✓ Network Devices	Network Device Groups	Network Device Profile	es External RADIUS Ser	vers RADIUS Server Sequences
	G			
Network devices		etwork Devices		
Default Device	/	'Edit 🕂 Add 🕞 Duplicat	e 🕵 Import 🎲 Export	Generate PAC XDelete

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 WLC-name
Description optional description
* IP Address: a.b.c.d / 32
* Device Profile 🛛 😹 Cisco 👻 🕀
Model Name wic-model
Software Version wic-software 👻
* Network Device Group
Device Type WLCs-2504 📀 Set To Default
WEGS Set to belaar
← RADIOS Authentication Settings
Enable Authentication Settings
Protocol RADIUS
* Shared Secret Show
Enable KeyWrap 🗌 👔
* Key Encryption Key Show
* Message Authenticator Code Key Show
Key Input Format 💿 ASCII 🔵 HEXADECIMAL
CoA Port 1700 Set To Default

Zie deze link voor meer informatie over Network Devices Group:

#### Een nieuwe gebruiker op ISE maken

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

diale Identity Services Engine	Home	Context Visibility	<ul> <li>Operations</li> </ul>	▶ Policy	<ul> <li>Administration</li> </ul>
► System	• Network F	Resources 🔹 🕨 Devi	ce Portal Managemer	nt pxGrid 8	System
▼Identities Groups External Iden	tity Sources	Identity Source Se	quences 🔹 🕨 Setting	s	Deployment Licensing
() Users	Networ	k Access Users			Certificates Logging Maintenance
Latest Manual Network Scan Res	🥖 Edit	🕂 Add 🔣 Change	Status 👻 🎲 Import	🚯 Export 👻	Upgrade Backup & Restor
	Stat	tus Name	•	Description	Admin Access
	🎲 Loa	ading			Settings
					Identity Managem
					Identities

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 Users List > New Network Access User	
Network Access User	
* Name user1	
Status 🛃 Enabled 👻	
Email	
<ul> <li>Passwords</li> </ul>	
Password Type: Internal Users 🔹	
Password	Re-Enter Passw
* Login Password	•••••
Enable Password	
<ul> <li>User Information</li> </ul>	
First Name	
Last Name	
- A construct Outlines	
Account Uptions	
Description	
Change password on next login	
<ul> <li>Account Disable Policy</li> </ul>	
Disable account if date exceeds 2017-01-21	
User Groups	
ALL_ACCOUNTS (default) 📀 🛶 🕂	
Submit Cancel	

#### 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.

aliatio cisco	Identity Services Engine	Home	▶ Context Visibility	▶ Operations	→ Policy	▶ Administration	• Work Centers	Li
Authe	entication Authorization	Profiling Pos	ture Client Provisio	ning 🔹 Policy El	ements			
ting the pr System > f	otocols that ISE should use t ∃ackup & Restore ≻ Policy Ex	o communicate v port Page	with the network device	es, and the identity	sources that it	should use for auther	tication.	
_Protocol:	: If Wired_MAB <b>OR</b> s and :use Internal Endpoint	s					C	Insert new row above Insert new row below
IC_Protoc	: If Wired_802.1X <b>OR</b> ols and						_	Duplicate above Duplicate below Delete

### 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*.

dialo Identity S	Services Engine	Home	e ⊧C	ontext Visibility	<ul> <li>Operations</li> </ul>	▼Policy	Administration	▶ Work Ce	nters		
Authentication	Authorization	Profiling	Posture	Client Provisior	ning 🔹 🕨 Policy Ele	ements					
Authentication	1 Policy										
Define the Authen For Policy Export of Policy Type	tication Policy by s go to Administratio Simple	electing the p n > System > -Based	orotocols Backup &	that ISE should u & Restore ≻ Policy	se to communicata y Export Page	e with the netv	vork devices, and the	identity source	s that it shoul	ld use for	r authentica
										_	
	Rule name		: lf	Wireless_802.1>	(AND Select Attrib)	ute 🦳 Al	llow Protocols : Defa	ault Network Ac	cess	0	and <u>—</u>
				💾 Add All Cor	nditions Below to L	ibrary					
-	Default		: Us	Condition	Name	Description	atch 902 1V based a	uthentication r	oqued		*
						Radius:Cal	led-Sta 📀 🛛 End	ds With 👻	ise-ssid	(	2

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

Rule name : If Wi	reless_802.1X AND Radius:Call	It Network Access 📀 and .
Default : Use	Internal Users Identity Source Internal Users Options If authentication failed Reject  If user not found Reject  If process failed Drop  Y	Identity Source List
A .	Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or it is not possible to continue processing when authentication fails o If continue option is selected in these cases, requests will be reject	All_User_ID_Stores     Certificate_Request_Sequence     DenyAccess
A 		Guest Osers     Guest_Portal_Sequence     IdnetitySequence_JUST_Internal     Internal Endpoints     Internal Users

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

Rule name	: If Wireless_802.1X AND Radius:Cal 💠 Allow Protocols : Default Network Access 📀 and 🚃	Done
Default	: Use Internal Users 💠	Actions 👻
Save		

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.** 

es Engine	e Home	) ¢	ontext Visibility	<b>▶</b> 0	perations	▼Policy	Administration	► V	Vork Centers
norization	Profiling F	Posture	Client Provisioni	ng	Policy Ele	Authentic	ation		Authorization
						Profiling			Posture
Y						Client Pro	visioning		Policy Elements
Policy by co	Policy by configuring rules based on identity groups and/or other con								Dictionaries
dministratio	on > System >	Наскир &	& Restore > Policy	Expor	tPage				Conditions
olies	*								Results

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

altala cisco	Identity S	Services Engine	Home	Context Visibility	Operations	- Policy	Administration	Work Centers	License V
Authe	entication	Authorization Pro	ofiling Postur	e Client Provisioning	<ul> <li>Policy Eleme</li> </ul>	ents			
riguring ru	ules based o	on identity groups and	d/or other condi	tions. Drag and drop rul	les to change the	order.			
> System	> Backup &	Restore > Policy Exp	ort Page						
-									
		Conditions (ide	entity groups an	d other conditions)			Permissions		
									Insert New Rule Above
									Insert New Rule Below
									Duplicate Above

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*.

	Status	Rule Name	Co	nditions (identity groups and other conditions) Permissions	
1		NameAuthZrule		Any Condition(s) 💠 then AuthZ Pr	
	<b>~</b>	To d	if V	·	
	<b>~</b>	Menore as Tables (as) Defense	if Eð	ac Any Col - +	less Ac. 55
	<b>~</b>	Profiled Cisco Statical III a	if <b>C</b>	User Identity Groups	s
	<b>~</b>	Francis Mon Cheo P. Pixerak	if No	∽ <b>→ → →</b>	ગોરાટ્સ
	0	Compliant_Devices_Addr.co	if 🐴	et U GuestType_Daily (default) GuestType_Weekly (default)	
1	0	Employes, FAD THE	if M	firGuestType_Contractor (default)	NE
	0	Etipleves Ophoenting	if <mark>(</mark> 1	Incless_800.411 AND EAP-MSCHAPV2 : ALL_ACCOUNTS (default)	0025266
	-				

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*.

	Status	Rule Name	Conditions (identity groups a	nd other conditions)	Permissions	
🖉	-	NameAuthZrule	if AL 💠 and	Wireless_802.1X AND Radius:Call	😑 then AuthZ Pr 💠	
1			s	💾 Add All Conditions Below to Librar	у	
	<b>~</b>		۵,	Condition Name De	scription	AND -
	<b>~</b>			Wireless 802.1X 💟 Normalis	ed Radius:RadiusFlowType EQUALS Wireless802_1>	AND
	<u>~</u>		e:			¥

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

	Status	Rule Name	Conditions (identity	groups and other conditions)	Perm	nissions		
	<b>-</b>	NameAuthZrule	if AL <	and Wireless_802.1X AND Radius:Call	💠 then	PermitAc		Done
1	~					·		Edit   🕶
1						PermitAccess		Edit   🕶
1							Standard	Edit   •
1	~							Edit   🕶
1	0						C E	Edit   🕶
1	0							Edit   🕶
-	0						2 C	5-00 I
	0						1	Eat
1	0						PermitAccess	Edit   🕶
1	0							Edit   🕶
1								Edit   +
	<b>~</b>	Default	if no matches, then	DenyAccess				Edit   🕶
	_							
Sa	ve Res	set						

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

•		
(	> -+	
	Standard	
	⟨= •  ≡ •	<u>िं</u> द्र
	😪 Blackhole_Wireless_Access	🎡 Add New Standard Profile

Voer de informatie in:

Add New Standard Prof	file		
Authorization Profile		í	
* Name	Iname-of-profile		
Description			
* Access Type	a ACCESS_ACCEPT T		
Network Device Profile	the Cisco 🔻 🕀		
Service Template			
Track Movement	ut ⊡⊕		
Passive Identity Tracking	9 D <i>0</i>		
▼ Common Tasks			
		^	
EI DAGE Name		- 54	
ACL (Filter-ID)			
🗹 VLAN	Tag ID 1 Edit Tag ID/Name van-id		
U voice Domain Permi	lission	~	
<ul> <li>Advanced Attribut</li> </ul>	ites Settinos		
Select an item			
▼ Attributes Details			
Access Type = ACCESS_ Tunnel-Private-Group-ID	)_ACCEPT D = 1:v/an-id		
Tunnel-Type = 1:13 Tunnel-Medium-Type =	1.6		
C		>	
		Save	Ince

#### Configuratie van het eindapparaat

Configureer een Windows 10-laptop met het oog op de aansluiting op een SSID met 802.1xverificatie 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 <u>configuratie van het eindapparaat - Maak</u> <u>het WLAN-profiel - Stap 7</u>.

#### 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.



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

Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001'	×
<ul> <li>Export Certificate Only</li> </ul>	
Export Certificate and Private Key	
*Private Key Password	
*Confirm Password	
Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key	ey.
Export Can	.cel

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...** 

08	Certificate	×				
Ge	General Details Certification Path					
	Certificate Information	1				
	This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.					
	Issued to: EAP-SelfSignedCertificate					
	Issued by: EAP-SelfSignedCertificate					
	<b>Valid from</b> 23/11/2016 <b>to</b> 23/11/2018					
	Install Certificate Issuer Statement					
	OK					

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

🔶 😸 Certificate Import Wizard	^
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Store Location Current User Local Machine	
To continue, click Next.	
Next Cance	1

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

←	🚰 Certificate Import Wizard	^			
	Certificate Store Certificate stores are system areas where certificates are kept.				
	Windows can automatically select a certificate store, or you can specify a location for the certificate.				
	O Automatically select the certificate store based on the type of certificate				
	Place all certificates in the following store				
	Certificate store:				
	Trusted Root Certification Authorities Browse				
	Next Canc	el			

V

Klik vervolgens op Voltooien.

← 🔮	Certificate Import Wizard		^
	Completing the Certific	ate Import Wizard	
	The certificate will be imported after y	/ou click Finish.	
	You have specified the following setti	ngs:	
	Certificate Store Selected by User	Trusted Root Certification Authorities	
	Content	Certificate	
		Finish Cance	el

 $\sim$ 

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:

### 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?



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.

	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									
I	ال العام 👳 Networ 🧐 کر									

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.** 

🔩 Network and Sharing Center									
🔶 🚽 🔨 🛧 💐 🔪 Control Pan	el > Network and Internet > Network and Sharing C	enter							
Control Panel Home View your basic network information and set up connections									
Change adapter settings	View your active networks								
Change advanced sharing settings	<b>cisco.com</b> Domain network	Access type: Internet Connections: <i>«</i> Ethernet							
	Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN connection Troubleshoot problems Diagnose and repair network problems, or get	on; or set up a router or access point. t troubleshooting information.							

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

		_		×
🗧 🔶 Set Up a Connection or Network				
Choose a connection option				
Connect to the Internet Set up a broadband or dial-up connection to the Internet.				
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.				
				1
	Ne	ext	Can	cel

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 v	vireless network				
	Enter information fo	r the wireless network you	want to add			
	Network name:	ise-ssid				
	Security type:	WPA2-Enterprise ~				
	Encryption type:	AES				
	Security Key:		Hide characte	rs		
	Start this connection	automatically				
	Connect even if the	network is not broadcasting				
	Warning: If you seled	t this option, your computer's priva	acy might be at risk	-		
			N	ext	Cano	el

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

	—		×
<ul> <li>Manually connect to a wireless network</li> </ul>			
Successfully added ise-ssid			
→ Change connection settings Open the connection properties so that I can change the settings.			
		ch	
		Clo	se

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

ise-ssid Wireless Ne	twork Properties		×
Connection Security			
Security type:	WPA2-Enterprise	~	r
Encryption type:	AES	×	r
Choose a network au	thentication method:		
Microsoft: Protected	EAP (PEAP) 🛛 🗸	Settings	
Remember my cro time I'm logged o	edentials for this connec n	tion each	- I
	_		
Advanced settings	÷		
		ОК	Cancel

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**.

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:									
Eggille & Clobel Lines an     Eggille & Clobel Lines an     Eggille & Clobel Assessment and the exclusion     Eggille Assessment and an     Eggille Assessment and an	^								
EAP-SelfSignedCertificate									
<ul> <li>Fortunet Royal Configuration, M. Status, C. S. S.</li> <li>L. M. Schultz Configuration of Configuration, Status, Configuration, Configuratio, Configuration, Configuration, Configuration, Configuratio</li></ul>	~								
< >									
Notifications before connecting:									
Tell user if the server name or root certificate isn't specified	~								
Select Authentication Method:	_								
Secured password (EAP-MSCHAP v2) Configu	re								
C Enable Fast Reconnect									
Disconnect if server does not present cryptobinding TLV									
Enable Identity Privacy									
OK Cano	el								

EAP MSCHAPv2 Properties							
When connecting:							
Automatically use my Windows logon name and password (and domain if any).							
OK Cancel							

## 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.

ise-ssid Wireless Ne	twork Properties		×
Connection Security			
Security type:	WPA2-Enterprise		~
Encryption type:	AES		$\sim$
Choose a network au	thentication method:		
Microsoft: Protected	EAP (PEAP)	Setting	js
Remember my cro	edentials for this connecti	on each	
une i n logged o			
the second section of the second se			
Advanced settings	<b>)</b>		
	(	ОК	Cancel

Advanced sett	ings		×
802.1X settings	802.11 settings		
Specify a	uthentication mode:		
User aut	hentication $$	Save credent	tials
Delete	e credentials for all users		
Enable si	ngle sign on for this network		
Perfo	rm immediately before user log	ion	
O Perfo	rm immediately after user logo	n	
Maximun	n delay (seconds):	10	*
Allow sign o	additional dialogs to be display on	ed during single	
This r and u	network uses separate virtual L ser authentication	ANs for machine	
		ОК	Cancel

Windows Secu	rity	×
Save creder Saving your cre when you're no	ntials edentials allows your computer to connect to the network ot logged on (for example, to download updates).	¢
uluulu cisco	user1	
	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-reg
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 \*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 \*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 Of ..... \*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\_MsqTask\_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 00.00.00.00.00.00.00.00.01 \*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.

dinin cisco	Identit	y Service:	s Engine	Home	♦ Context Visit	ility <del>-</del> Opera	tions	• Policy	▶ Administrat	tion 🔸	Work Centers		License
▼RA	DIUS	TC-NAC Liv	e Logs	+ TACACS	Reports + Trou	oleshoot 🕨 Ad	laptive N	Network Contro	bl				
Live	Logs	Live Sessio	ns										
		Μ	lisconfigu	ored Supplic	ants Misc	onfigured Netw Devices 👁	rork	RØ	ADIUS Drops (	Defrech	Client Stop	ed Respondin 4	ng Repea
C Refresh ● Reset Repeat Counts													
	Time	Sta	Details	lde	Endpoint ID	Endpoint	. Au	uthentication	Policy	Autho	orization Polic	y Author	zation Profiles
	No	1	Q	user1	08:74:02:77:13:4	5 Apple-Device	e De	efault >> Rule n	ame ≻> Default	: Defaul	lt >> NameAuthZr	rule PermitA	ccess

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