# 802.1X-verificatie configureren met PEAP, ISE 2.1 en WLC 8.3

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Netwerkdiagram Configuratie RADIUS-server op WLC verklaren **SSID** maken WLC declareren op ISE Nieuwe gebruiker maken op ISE Verificatieregel maken Autorisatieprofiel maken Autorisatieregel aanmaken Configuratie van eindapparaat Configuratie van eindapparaat - Installeer ISE-zelfondertekend certificaat Configuratie van eindapparaat - Het WLAN-profiel maken Verifiëren Verificatieproces op WLC Verificatieproces op ISE Problemen oplossen

# Inleiding

Dit document beschrijft hoe u een Wireless Local Area Network (WLAN) kunt instellen met 802.1xbeveiliging en Virtual Local Area Network (VLAN)-opheffing.

# Voorwaarden

# Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- 802.1x
- Protected Extensible Verification Protocol (PEAP)
- Certificeringsinstantie (CA)
- Certificaten

### Gebruikte componenten

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

• WLC v8.3.102.0

- Identity Service Engine (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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Achtergrondinformatie

Wanneer u een WLAN met 802.1x-beveiliging en VLAN instelt, kunt u met Protected Extensible Verification Protocol (EAP) overschrijven.

# Configureren

# Netwerkdiagram



# Configuratie

De algemene stappen zijn:

- 1. Verklaar de Server van de RADIUS op WLC en vice versa om communicatie met elkaar toe te staan.
- 2. Maak de Service Set Identifier (SSID) aan in de WLC.
- 3. Maak de verificatieregel op ISE.
- 4. Maak het autorisatieprofiel op ISE.

- 5. Maak de autorisatieregel op ISE aan.
- 6. Configureer het eindpunt.

#### **RADIUS-server op WLC verklaren**

Om communicatie tussen RADIUS-server en WLC mogelijk te maken, moet u RADIUS-server op WLC registreren en omgekeerd.

GUI:

Stap 1. Open de GUI van de WLC en navigeer naar **SECURITY > RADIUS > Verificatie > Nieuw** zoals in de afbeelding.



Stap 2. Voer de RADIUS-serverinformatie in zoals in de afbeelding.

RADIUS Authentication Serv	ers > New	
Server Index (Priority)	2 ~	
Server IP Address(Ipv4/Ipv6)	a.b.c.d	
Shared Secret Format	ASCII 🗸	
Shared Secret	•••••	
Confirm Shared Secret	•••••	
Key Wrap	(Designed fo	r FIPS customers and requires a key wrap compliant RADIUS server;
Port Number	1812	
Server Status	Enabled $\sim$	
Support for CoA	Disabled $\vee$	
Server Timeout	10 seconds	
Network User	🗹 Enable	
Management	🗹 Enable	
Management Retransmit Timeout	2 seconds	
IPSec	Enable	

### CLI:

> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>

> config radius auth enable <index>

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

#### SSID maken

GUI:

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

،، ،،، ،، cısco	MONITOR	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE
WLANs	WLANs						
WLANs     WLANs     Advanced	Current Filter: No	ne [ <u>Cha</u>	nge Filter] [Cl	ear Filter]		[	Crea

Stap 2. Kies een naam voor de SSID en het profiel en klik vervolgens op Toepassen zoals in de afbeelding.

W	/LANs > New			]	< Back	Apply
	Туре	WLAN ~	_			
	Profile Name	profile-name				
	SSID	SSID-name				
	ID	2 ~	•			

CLI:

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

Stap 3. Wijs de RADIUS-server toe aan het WLAN.

CLI:

> config wlan radius\_server auth add <wlan-id> <radius-index>

GUI:

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

WLANs > Edit 'ise-prof'	< Back	Apply
General Security QoS Policy-Mapping Advanced		
Layer 2 Layer 3 AAA Servers		
Select AAA servers below to override use of default servers on this WLAN		^
RADIUS Servers		
RADIUS Server Overwrite interface		
Authentication Servers Accounting Servers EAP Parameters		
Enabled Enabled Enable		
Server 2 None V None V		
Server 3 None V None V		
Server 4 None V None V		
Server 5 None V None V		
Server 6 None V None V		
RADIUS Server Accounting		
Interim Update 🗹 Interim Interval 0 Seconds		~
	2	<b>&gt;</b>

Stap 4. AAA negeren en optioneel de sessietime-out inschakelen

CLI:

```
> config wlan aaa-override enable <wlan-id>
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

Navigeer naar WLANâ€<sup>TM</sup>s > WLAN-id > Geavanceerden schakel AAA-opheffing in. Specificeer optioneel de Session Time-out zoals in de afbeelding.

WLAN	Ns≻Edit 'ise-pro	of'		< Back
Ger	neral Security	QoS Policy-Mapping /	Advanced	
Г		Plan and a	0.000	^
ľ	allow AAA Override	Enabled	DHCP	
( [	Coverage Hole Detection	🗹 Enabled	DHCP Server	Override
1	Enable Session Timeout	Session Timeou (secs)	DHCP Addr. Assignment	Required
ļ	Aironet IE	Enabled	OEAP	
[ 	Diagnostic Channel 18	Enabled	Split Tunnel	Enabled
¢ ¢	Override Interface ACL	IPv4 None V Non	e 💛 Management Frame F	Protection (MFP)
ι	ayer2 Ad	None ~		
U	RL ACL	None ~	MFP Client Protecti	on 🛃 Optional 🗸
ţ	2P Blocking Action	Disabled 🗸	DTIM Period (in beaco	on intervals)
<	Client Exclusion 💈	Enabled Timeout Value (secs)	802.11a/n (1 - 25	5) 1
	Maximum Allowed Clients <sup>g</sup>	0	802.11b/g/n (1 - 2 NAC	255) 1
<	Static IP Tunneling	□	NAC State None	× ×

Stap 5. Schakel het WLAN in.

CLI:

> config wlan enable <wlan-id>

GUI:

Navigeer naar **WLAN's > WLAN-id > Algemeen**en schakel de SSID in zoals in het beeld.

WLANs > Edit 'ise-j	orof'		< Back	< Apply	
General Securit	y QoS	Policy-Mapping	Advanced		
Profile Name Type SSID Status Security Policies	ise-prof WLAN ise-ssid ☑ Enabled [WPA2][Ac (Modification	th(802.1X)] is done under security	tab will appear a	fter applying the changes.)	
Radio Policy Interface/Interface Group(G) Multicast Vlan Feature Broadcast SSID NAS-ID	All manageme Enabled Enabled none	 nt_⊻			

#### WLC declareren op ISE

Stap 1. Open de ISE-console en navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten > Toevoegen** zoals in de afbeelding.

elisco Identity Services E	Engine Home	) ► Context \	/isibility ► Operations		Policy	★Administ	tration
▶ System → Identity Man	nagement 🔽 Netwo	ork Resources	Device Portal N	lanagement	pxGrid S	ervices 🕨 🕨	Feed Service
✓Network Devices Network	work Device Groups	Network Devi	ce Profiles Exter	nal RADIUS Se	rvers F	RADIUS Serv	er Sequence
	G						
Network devices	Net	twork Devices	6				
Default Device							
	/	Edit 🕂 Add 🛱	Duplicate	ort 🚯 Export	• 🕲 Ge	enerate PAC	🗙 Delete 👻

Stap 2. Voer de waarden in.

Optioneel kan het een opgegeven Modelnaam, softwareversie, beschrijving zijn en netwerkapparaatgroepen toewijzen op basis van apparaattypen, locatie of WLC's.

a.b.c.d komt overeen met de WLC-interface die de gevraagde verificatie verstuurt. Standaard is het de beheerinterface zoals in het beeld.

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 wlc-model 🍸
Software Version wic-software 🍸
* Network Device Group
Device Type WLCs-2504 O Set To Default Location All Locations O Set To Default WLCs WLCs O Set To Default
RADIUS Authentication Settings
Enable Authentication Settings Protocol <b>RADIUS</b>
* 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

Voor meer informatie over Netwerkapparaatgroepen:

ISE - Apparaatgroepen voor netwerk

### Nieuwe gebruiker maken op ISE

Stap 1. Ga naar **Beheer > Identiteitsbeheer > Identiteiten > Gebruikers > Toevoegen** zoals in de afbeelding.

dialo Identi	ty Services Engin	e Home	▶ Context Visibility	Operations	▶ Policy	<ul> <li>Administration</li> </ul>
▶ System	▼Identity Managerr	nent 🕨 Network F	Resources 🔹 🕨 Device	e Portal Manageme	nt pxGrid 8	System
▼Identities	Groups Externa	al Identity Sources	Identity Source Seq	uences 🕨 Setting	gs	Deployment Licensing
Users		<b>G</b> Networ	rk Access Users			Certificates Logging Maintenance
Latest Manual	Network Scan Res.	·· 🦯 Edit	🕂 Add 🔢 Change St	atus 👻 🕵 Import	Export 🗸	Upgrade Backup & Restor
		Sta	tus Name	4	Description	Admin Access
		🍰 Lo:	ading			Settings
						Identity Managem
						Identities

Stap 2. Voer de informatie in.

In dit voorbeeld behoort deze gebruiker tot de groep ALL\_ACCOUNTANTS, maar hij kan naar behoefte worden aangepast, zoals in de afbeelding wordt getoond.

Network Access Users List > New Network Access User	
<ul> <li>Network Access User</li> </ul>	
* Name user1	
Status 🛃 Enabled 👻	
Email	
<ul> <li>Passwords</li> </ul>	
Password Type: Internal Users 🔹	
Password	Re-Enter Passw
* Login Password	•••••
Enable Password	
✓ User Information	
First Name	
Last Name	
<ul> <li>Account Options</li> </ul>	
Description	
Change password on next login	
✓ Account Disable Policy	
Disable account if date exceeds 2017-01-21	
Viser Groups	
🗛 🕹 🕹 🖡	
Submit Cancel	

### Verificatieregel maken

Verificatieregels worden gebruikt om te verifiëren of de referenties van de gebruikers correct zijn (verifiëren of de gebruiker echt is wie ze zeggen dat ze zijn) en beperken de verificatiemethoden die door hem mogen worden gebruikt.

Stap 1. Navigeer naar **Beleid > Verificatie** zoals in de afbeelding.



Stap 2. Plaats een nieuwe verificatieregel zoals in de afbeelding.

altalla cisco	Identity	Services Engine	e Home	e 🕨 Conte	ext Visibility	▶ Operations	→ Policy	Administration	
Auth	entication	Authorization	Profiling	Posture C	lient Provisionir	ng 🕨 Policy E	Elements		
ting the pi System > I ed	rotocols tł Backup &	nat ISE should use Restore > Policy E	to communic: xport Page	ate with the n	etwork devices,	and the identity	/ sources that if	t should use for authe	enticat
_Protocol	:lf Wi s and :us	red_MAB <b>OR</b> e Internal Endpoir	its						
IC_Proto	: If Wi cols an	red_802.1X <b>OR</b> d							

Stap 3. Voer de waarden in.

Deze verificatieregel staat alle protocollen toe die worden vermeld in de lijst Standaard netwerktoegang. Dit is van toepassing op het verificatieverzoek voor draadloze 802.1x-clients, en met Call-Station-ID, en eindigt met een stijgende lijn zoals in de afbeelding.

aliado - Identity S	ervices Engine	e Home	► Co	ontext Visibility	▶ Opera	tions	▼Policy	► Administr	ation 🕨	١
Authentication	Authorization	Profiling Po	osture	Client Provisio	ning 🕨 Po	olicy Elen	nents			
Authentication Define the Authen For Policy Export <u>o</u>	I Policy lication Policy by to Administration	selecting the pro on > System > B	otocols tř lackup &	hat ISE should u Restore > Polic	se to comm y Export Pag	iunicate v	with the netv	work devices, ar	nd the identi	ity
Policy Type 🔿 🤅	3imple 💿 Rule	e-Based								
🦉 🗹 🗸	Rule name		∶lf V	Wireless_802.1)	X AND Selec	t Attribut	e 😐 A	llow Protocols :	Default Ne	et
				💾 Add All Co	nditions Belo	ow to Lib	rary			
	Default		· Us	Condition	Name	D	escription			
	/ ordene			Wireless_80	)2.1X 🔇	A cor	ndition to m	hatch 802.1X ba	ased authen	it
				0			Radius:Cal	led-Sta 📀	Ends Wit	h

Kies ook de identiteitsbron voor de clients die aan deze verificatieregel voldoen. In dit voorbeeld wordt de bronlijst van interne gebruikers gebruikt zoals in de afbeelding wordt getoond.

Rule name : If Wireless_802.1X AND Radius:Call 💠 Allow Protocols : Defau	It Network Access
Default : Use Internal Users	
Options         If authentication failed         Reject         If user not found         Reject         If process failed         Drop         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         Av	Identity Source Lis
	Internal Users

Als u klaar bent, klikt u op Gereed en Opslaan zoals in de afbeelding.

🖉 🖌 Rule name : If Wretess_002.1XAND Radius Cal	Done
🖉 🕶 Default : Use Internal Users 🔷	Actions +
	_
Resot	

Zie voor meer informatie over Identiteitsbronnen deze link:

Een gebruikersgroep maken

### Autorisatieprofiel maken

Het autorisatieprofiel bepaalt of u al dan niet toegang hebt tot het netwerk. Druk op ACLâ€<sup>TM</sup>s (Access Control Lists), VLAN-overschrijving of een andere parameter. Het in dit voorbeeld getoonde autorisatieprofiel stuurt een toegangsgoedkeuring naar u en wijst VLAN 2404 toe.

Stap 1. Navigeer naar **Beleid > Beleidselementen > Resultaten** zoals in de afbeelding.



Stap 2. Voeg een nieuw autorisatieprofiel toe. Navigeer naar **autorisatie > autorisatieprofielen > Toevoegen** zoals in de afbeelding.

ditolin Identity Services	Engine H	Home 🔸	Context Visibility	Operations
Authentication Authoriz	ation Profiling	Posture	Client Provisioning	→Policy Elements
Dictionaries + Condition	s <b>≁</b> Results			
	G			
<ul> <li>Authentication</li> </ul>		Standa For Policy	rd Authorization Export go to Adminis	n <b>Profiles</b> tration > System > Ba
<ul> <li>Authorization</li> </ul>		_		
Authorization Profiles		/ Edit	+Add Duplicate	e 🗙 Delete
Downloadable ACLs		Narr	ie	

Stap 3. Voer de waarden in zoals in de afbeelding.

Authorization Profiles > New Authoriz Authorization Profile	ation Profile	
* Name PermitAc	cessVLAN2404	
Description		
* Access Type ACCESS	ACCEPT	
Network Device Profile 🔐 Cisco	<b>▼</b> ⊕	
Service Template		
Track Movement 🛛 👔		
Passive Identity Tracking 🛛 👔		
Common Tasks		
VLAN	Tag ID 0	Edit Tag ID/Name 2404
Voice Domain Permission		
Alah Redirection (CIAIA - MDM -	NED CDDY (1)	
✓ Advanced Attributes Setti	ngs	
Select an item	📀 =	⊘ +
Select an item  Attributes Details  Access Type = ACCESS_ACCEPT Tunnel-Private-Group-ID = NaN:240 Tunnel-Ince = NicNic240	S =	<b>&gt;</b> +

### Autorisatieregel aanmaken

De autorisatieregel is degene die bepaalt welke permissies (welk autorisatieprofiel) op u worden toegepast.

Stap 1. Navigeer naar **Beleid > Autorisatie** zoals in de afbeelding.

es Engine	e Hon	ne ⊧C	ontext Visibility	Operations	→ Policy	Administration	▶ Work Centers		
norization	Profiling	Posture	Client Provisioning	Policy Ele	Authentica	ntion	Authorization		
					Profiling		Posture		
Y					Client Prov	risioning	Policy Elements		
Policy by c	onfiguring ru	les based	on identity groups an	d/or other condi			Dictionaries		
dministratio	on > System		Conditions						
olies	lies								

Stap 2. Plaats een nieuwe regel zoals in de afbeelding.

dicolu cisco	Identity	Services Engi	ne H	Home	<ul> <li>Context Visibility</li> </ul>	▸ Operations	→Policy	Administration	• Work Centers
Authe	ntication	Authorization	Profiling	Posture	Client Provisioning	Policy Eleme	nts		
diauripa ri	iles hased	op identity groups	e and (or ot)	her conditi	ons. Drag and drop ru	les to change the i	order		
> System	> Backup (	& Restore > Policy	Export Pa	ige	ons. Drag and drop ru	ies to change the			
*									
		Conditions	s (identity <u>o</u>	groups and	other conditions)			Permissions	

Stap 3. Voer de waarden in.

Selecteer eerst een naam voor de regel en de identiteitsgroep waarin de gebruiker is opgeslagen (ALL\_ACCOUNT), zoals in de afbeelding.

	Status	Rule Name		Conditions (identity groups and other conditions)	Permis
1		NameAuthZrule		if Any Pland Condition(s)	then
	2	That .	if	<u></u>	
	<b>~</b>	Minetes Stuck as Lactors	if	C'ac Any	
		Profile 2 Cisco s - Louis	if	C :	
	<u>~</u>	Franks Pro Creo & Pixtrax	if	Non	<u>نې</u>
	0	Compliant_Devices_Auchtin	if	GuestType_Daily (default)	
	0	Employee, FAP THE	if	GuestType_Weekly (default) GuestType_Contractor (default)	ult)
	0	Shipleyes Ophoenline	if	MARCHARY AND EAR-MSCHARY2 )	-9
	-				

Selecteer vervolgens andere voorwaarden waardoor het autorisatieproces onder deze regel valt. In dit voorbeeld, het vergunningsproces raakt deze regel als het draadloze 802.1x en zijn geroepen station ID eindigt met ise-side zoals getoond in het beeld gebruikt.

	Status	Rule Name	Conditions (identity groups	and other conditions)	Permissions
Ø	-	NameAuthZrule	if AL 💠 and	Wireless_802.1X AND Radius:Call	then AuthZ P
1	<b>2</b>			S 💾 Add All Conditions Below to Librar	У
			1	Condition Name De	escription
1				Wireless 802.1X 📀 Normali	sed Radius:RadiusFlowType E
1	<u>~</u>				

Selecteer tot slot het autorisatieprofiel dat aan u is toegewezen en dat deze regel raakt. Klik op **Gereed** en **Opslaan** zoals in de afbeelding.

	Status	R	ule Name	Con	ditions (identit	ty groups	and other conditions)	Permi	ssions
Η,	1	•	NameAuthZrule		AL (	🗘 and	Wireless_802.1X AND Radius:Call	> then	AuthZ Pr
1	2								
1									Select an item
	~								
	0								
	0								
	0								
1	0								
	Ø								
1	0								
	<b>~</b>	D	efault	if no m	atches, then	DenyA	ccess		
	_								
Sa	ave R	leset							

#### Configuratie van eindapparaat

Configureer een laptop Windows 10-machine om verbinding te maken met een SSID met 802.1x-verificatie en PEAP/MS-CHAPv2 (Microsoft-versie van het Challenge-Handshake-verificatieprotocol) versie 2.

In dit configuratievoorbeeld gebruikt ISE zijn zelfondertekende certificaat om de verificatie uit te voeren.

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

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

De configuratie van deze opties wordt toegelicht in de instructies voor de configuratie van het eindapparaat -

Het WLAN-profiel maken - Stap 7.

### Configuratie van eindapparaat - Installeer ISE-zelfondertekend certificaat

Stap 1. Zelfondertekend certificaat voor uitvoer.

Log in op ISE en navigeer naar **Beheer > Systeem > Certificaten > Systeemcertificaten**.

Kies vervolgens het certificaat dat wordt gebruikt voor **EAP-verificatie** en klik op **Exporteren** zoals in de afbeelding.

dentity Services Engin	e Home 🔸	Context Visibility	• Operations	Policy      Adminis	stration 🔹 🕨 Work
	ent 🔹 Network Resou	urces I Device I	Portal Management	pxGrid Services	Feed Service 🔹 🖡
Deployment Licensing -Cer	tificates + Logging	Maintenance	Upgrade Backu	ip & Restore 💿 🕨 Admi	in Access 🔹 🕨 Settir
	0				
<ul> <li>Certificate Management</li> </ul>	System C	ertificates 🛕	For disaster recover	ry it is recommended to	export certificate ar
Overview	🥖 Edit	🕂 Generate Self	Signed Certificate	🕂 Import 💽 Exp	ort 🗙 Delete
System Certificates	Frie	ndly Name	Used By	Portal group	tag I
Endpoint Certificates	▼ 012120				
Trusted Certificates	EAP AP-1	-SelfSignedCertific SelfSignedCertifica	ate#E te#00 EAP Authent	ication	EAI
OCSD Client Brofile					

Sla het certificaat op de gewenste locatie op. Dat certificaat moet op de Windows-machine worden geïnstalleerd zoals in het beeld wordt weergegeven.

Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001'					
	• Export Certificate Only				
	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.				
	Export				

Stap 2. Installeer het certificaat in de Windows-machine.

Kopieer het certificaat dat uit ISE naar de Windows-machine is geëxporteerd, wijzig de extensie van het bestand van .pem naar .crt en dubbelklik daarna om het te installeren zoals in de afbeelding.

🐱 Certificate	×
General Details Certification Path	
Certificate Information 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	
Valid from 23/11/2016 to 23/11/2018	
Install Certificate Issuer Statement	
ОК	

Stap 3. Selecteer de optie in Lokale machine installeren en klik op Volgende zoals in de afbeelding.

Stap 4. Selecteer Alle certificaten in deze winkel plaatsen, blader en selecteer vervolgens Trusted Root Certification Authorities. Klik vervolgens op Volgende zoals in de afbeelding.

Certificate S	lore				
Certifica	ke stores are sys	tem areas where	certificates are	kept.	
Window the cert	s can automatical ficate.	ly select a certifi	cate store, or yo	u can specif	iy a location for
OA	utomatically selec	t the certificate	store based on t	he type of c	ertificate
	lace all certificates	s in the following	store		
0	ertificate store:				
[	Trusted Root Cer	tification Author	ties		Browse

Stap 5. Klik vervolgens op **Voltooien** zoals in de afbeelding.

← 😺 Certificate Import Wizard	×
Completing the Certificate Import Wizard	
The certificate will be imported after you click Finish.	
You have specified the following settings:	
Certificate Store Selected by User Trusted Root Certification Authorities Content Certificate	
Finish	Cancel

Stap 6. Bevestig de installatie van het certificaat. Klik op **Ja** zoals in de afbeelding.



Stap 7. Klik tot slot op **OK** zoals in de afbeelding.

Certificate Import Wizard	×
The import was successful.	
ОК	

### Configuratie van eindapparaat - Het WLAN-profiel maken

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

	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
Ľ	👔 א אין אין אין אין אין אין אין אין אין א

Stap 2. Navigeer naar **Netwerk en Internet**, navigeer vervolgens naar **Netwerkcentrum** en klik op **Een nieuwe verbinding of netwerk instellen** zoals in de afbeelding.



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

	-		×
<ul> <li>Set Up a Connection or Network</li> </ul>			
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.			
Connect to a hidden network or create a new wireless profile.			
Connect to a workplace Set up a dial-up or VEN connection to your workplace			
and up a sear up of an in community point manipulate.			
	Next	Can	cel

Stap 4. Voer de informatie in met de naam van de SSID en het beveiligingstype WPA2-Enterprise en klik op **Volgende** zoals in de afbeelding.

			-		×
÷	🐓 Manually connect to a	wireless network			
	Enter information fo	or the wireless network you want to add			
	Network name:	ise-ssid			
	Security type:	WPA2-Enterprise ~			
	Encryption type:	AES V			
	Security Key:	Hide character			
	Start this connectio	n automatically			
	Connect even if the	network is not broadcasting			
	Warning: If you seld	ect this option, your computer's privacy might be at risk.			
		Ne	xt	Can	cel

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



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

ise-ssid Wireless Ne	twork Properties			×
Connection Security				
Security type:	WPA2-Enterprise		$\sim$	
Encryption type:	AES		$\sim$	
Choose a network aut	thentication method:			
Microsoft: Protected	EAP (PEAP) 🗸 🗸	Settin	igs	
Remember my cre	edentials for this conne	ction each		
ume i m logged o	1			
Advanced settings	<b>;</b>			
		OK	Cano	el

Stap 7. Selecteer deze optie als RADIUS-server al dan niet is gevalideerd.

Indien ja, **controleer de serveridentiteit door het certificaat te valideren** en van **Trusted Root Certification Authorities:** list selecteer het zelfondertekende certificaat van ISE.

Daarna selecteert u **Configureren** en uitschakelen **Automatisch mijn Windows-aanmeldingsnaam en wachtwoord gebruiken...** en klikt u vervolgens op **OK** zoals in de afbeeldingen.

Protected EAP Properties	Х
When connecting:	
✓ Verify the server's identity by validating the certificate	
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):	
Trusted Root Certification Authorities:	
Digitize & Octobellines and Digitize & Octobellines and Discourse and the second se	^
In the product of the measurement of the transmission of the product of the transmission of the product of t	
EAD-SelfSignedCertificate	
E. L. Markenski, Extension in New York (1997) [1] K. L. L. K. S.	
Constraint Clabele	~
Notifications before connecting:	_
Tell user if the server name or root certificate isn't specified	~
Select Authentication Method:	
Secured password (EAP-MSCHAP v2) Configure	e
C Enable Fast Reconnect	
Disconnect if server does not present cryptobinding TLV	
Enable Identity Privacy	
OK Cance	3I
EAD MSCHADy2 Properties	
When connecting:	
Automatically use my Windows logon name and password (and domain if any).	

Stap 8. Configureer de gebruikersreferenties.

Cancel

ОK

Terug naar 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 te verifiëren zoals in de afbeeldingen.

ise-ssid Wireless Ne	twork Properties		×
Connection Security			
Security type:	WPA2-Enterprise		$\sim$
Encryption type:	AES		$\sim$
Choose a network au	thentication method:		
Microsoft: Protected	EAP (PEAP) 🗸 🗸	Setting	ps
Remember my cro time I'm logged o	edentials for this connect n	ion each	
Advanced settings	•		
		ОК	Cancel

02.1X settings 802.11 settings	dvanced settings		3
Specify authentication mode: User authentication  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	02.1X settings 802.11 settings		
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	Specify authentication mode:		_
Delete credentials for all users     Enable single sign on for this network     @ Perform immediately before user logon     Perform immediately after user logon     Maximum delary (seconds):     10     Allow additional dialogs to be displayed during single     sign on     This network uses separate virtual LANs for machine     and user authentication	User authentication	Save cre	dentials
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	Delete credentials for all users		
Perform immediately before user logon     Perform immediately after user logon Maximum delay (seconds):     10     10     Allow additional dialogs to be displayed during single     sign on     This network uses separate virtual LANs for machine     and user authentication	Enable single sign on for this network		
Perform immediately after user logon Maximum delay (seconds):     10     1	Perform immediately before user	logon	
Maximum delay (seconds):	<ul> <li>Perform immediately after user log</li> </ul>	gon	
Allow additional dialogs to be displayed during single sign on     This network uses separate virtual LANs for machine and user authentication	Maximum delay (seconds):	10	-
This network uses separate virtual LANs for machine and user authentication	Allow additional dialogs to be disp sign on	layed during s	ingle
and user addrend.attorn	This network uses separate virtual	LANs for mac	thine
	and user automication		
		OK	Cancel
OV Course		UN	Cancel

Windows Secur	rity	×
Save creder Saving your cre when you're no	tials dentials allows your computer to connect to the network t logged on (for example, to download updates).	
ahaha cisco	user1	
	OK Cancel	

# Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

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

#### Verificatieproces op WLC

Voer de volgende opdrachten uit om het verificatieproces voor een specifieke gebruiker te bewaken:

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

Voorbeeld van een succesvolle verificatie (een of andere uitvoer is weggelaten):

<#root>

\*apfMsConnTask\_1: Nov 24 04:30:44.317:

e4:b3:18:7c:30:58 Processing assoc-req station:e4:b3:18:7c:30:58 AP:00:c8:8b:26:2c:d0-00

```
thread:1a5cc288
```

\*apfMsConnTask\_1: Nov 24 04:30:44.317: e4:b3:18:7c:30:58 Reassociation received from mobile on BSSID 00: \*apfMsConnTask\_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mobile \*apfMsConnTask\_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying site-specific Local Bridging override \*apfMsConnTask\_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Local Bridging Interface Policy for st \*apfMsConnTask\_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 RSN Capabilities: 60 \*apfMsConnTask 1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Marking Mobile as non-

e4:b3:18:7c:30:58 Received 802.11i 802.1X key management suite, enabling dot1x Authentication

11w Capable

```
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Received RSN IE with 1 PMKIDs from mobile e4:b3
*apfMsConnTask_1: Nov 24 04:30:44.319: Received PMKID: (16)
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Searching for PMKID in MSCB PMKID cache for mot
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 No valid PMKID found in the MSCB PMKID cache for
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 START (0) Initializing policy
*apfMsConnTask_1: Nov 24 04:30:44.319:
```

e4:b3:18:7c:30:58 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

\*apfMsConnTask\_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 AUTHCHECK (2) Change state to 8021X\_REQD (3) last state AUTHCHECK (2)

\*apfMsConnTask\_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 8021X\_REQD (3) Plumbed mobile LWAPP rul \*apfMsConnTask\_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfMsAssoStateInc \*apfMsConnTask\_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2 (apf\_policy.c:437) Changing stat \*apfMsConnTask\_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2:session timeout forstation e4:b3 \*apfMsConnTask\_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Stopping deletion of Mobile Station: (callerId: \*apfMsConnTask\_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Func: apfPemAddUser2, Ms Timeout = 0, Session T \*apfMsConnTask\_1: Nov 24 04:30:44.320: e4:b3:18:7c:30:58 Sending Assoc Response to station on BSSID 00:c \*spamApTask2: Nov 24 04:30:44.323: e4:b3:18:7c:30:58 Received ADD\_MOBILE ack - Initiating 1x to STA e4:b \*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58

Sent dot1x auth initiate message for mobile e4:b3:18:7c:30:58

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 reauth\_sm state transition 0 ---> 1 for mob

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 EAP-PARAM Debug - eap-params for Wlan-Id :2
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Disable re-auth, use PMK lifetime.
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:58
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.326:

e4:b3:18:7c:30:58 Sending EAP-Request/Identity to mobile e4:b3:18:7c:30:58 (EAP Id 1)

\*Dot1x\_NW\_MsqTask\_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:7 \*Dot1x\_NW\_MsqTask\_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received Identity Response (count=1) from mo \*Dot1x\_NW\_MsqTask\_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Resetting reauth count 1 to 0 for mobile e4 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 EAP State update from Connecting to Authent: \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mol \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18:7 \*Dot1x\_NW\_MsqTask\_0: Nov 24 04:30:44.386: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b3 \*Dot1x NW MsgTask 0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Entering Backend Auth Reg state (id=215) for \*Dot1x NW MsgTask 0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 WARNING: updated EAP-Identifier 1 ===> 215 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b3 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mol \*Dot1x\_NW\_MsqTask\_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:7 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAP Response from mobile e4:b3:18:7 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Resetting reauth count 0 to 0 for mobile e4 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mol \*Dot1x NW MsgTask 0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b3 \*Dot1x\_NW\_MsqTask\_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=216) for \*Dot1x NW MsgTask 0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b3 \*Dot1x NW MsgTask 0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for re

•

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Processing Access-Accept for mobile e4:b3:18:7c:30:58

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 acl from 255 to 255 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 Flex acl from 65535 to 65 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Username entry (user1) created for mobile, length = 253

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Found an interface name: 'vlan2404' corresponds to interface name received: vlan2404

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 override for default ap group, marking intg \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mok \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Re-applying interface policy for client \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 apfApplyWlanPolicy: Apply WLAN Policy over F \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531:

#### e4:b3:18:7c:30:58 Inserting AAA Override struct for mobile

MAC: e4:b3:18:7c:30:58, source 4 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying override policy from source Overric \*Dot1x\_NW\_MsgTask\_0: Nov 24

04:30:44.531: e4:b3:18:7c:30:58 Found an interface name: 'vlan2404' corresponds to interface name receive

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying Interface(vlan2404) policy on Mobil \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Re-applying interface policy for client \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Setting re-auth timeout to 0 seconds, got fr \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Creating a PKC PMKID Cache entry for station \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Resetting MSCB PMK Cache Entry 0 for station \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding BSSID 00:c8:8b:26:2c:d1 to PMKID cach \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: New PMKID: (16) \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 unsetting PmkIdValidatedByAp \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Updating AAA Overrides from local for static \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding Audit session ID payload in Mobility \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 0 PMK-update groupcast messages sent \*Dot1x\_NW\_MsqTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 PMK sent to mobility group \*Dot1x NW MsgTask 0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Disabling re-auth since PMK lifetime can tal \*Dot1x\_NW\_MsqTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Sending EAP-Success to mobile e4:b3:18:7c:30 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Freeing AAACB from Dot1xCB as AAA auth is do \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 key Desc Version FT - 0 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Found an cache entry for BSSID 00:c8:8b:26:2 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: Including PMKID in M1 (16) \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: M1 - Key Data: (22) \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: [0000] dd 14 00 0f ac 04 cc 3a 3d 26 80 17 8b f1 2d c5 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: [0016] cd fd a0 8a c4 39 \*Dot1x NW MsgTask 0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Starting key exchange to mobile e4:b3:18:7c:30:58, data packets will be dropped

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for re \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Entering Backend Auth Success state (id=223) \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Received Auth Success while in Authenticatin \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Received Auth Success while in Authenticatin \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 key Desc Version FT - 0 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.547:

e4:b3:18:7c:30:58 Received EAPOL-key in PTK\_START state (message 2) from mobile

e4:b3:18:7c:30:58

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Successfully computed PTK from PMK!!!
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Received valid MIC in EAPOL Key Message M2!!
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Not Flex client. Do not distribute PMK Key of
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Key Desc Version FT - 0
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.00
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for re
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30:58 Foot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30:58 Foot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30:58 Foot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30:58 Foot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30:58 Key Desc Version FT - 0
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555:

e4:b3:18:7c:30:58 Received EAPOL-key in PTKINITNEGOTIATING state (message 4)

from mobile e4:b3:18:7c:30:58
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Freeing EAP Retransmit Bufer for mobile e4:k
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMs1xStateInc
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqCntInc
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc

e4:b3:18:7c:30:58 0.0.0.0 8021X\_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X\_REQD (3)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                              Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                                Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                                Client Vlan Ip: 172.16.0.134, Vlan mask
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                                Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                                Virtual Ip: 10.10.10.10
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                                ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                              Building VlanIpPayload.
*Dot1x_NW_MsqTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code gosCap 00
*Dot1x NW MsgTask 0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LV
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556:
e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6677
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 00:c8:8b:26:2c:d0, slot 0, interface = 1, QOS = 0
 IPv4 ACL ID = 255, IPv
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed r
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successfully Plumbed PTK session Keysfor mol
*spamApTask2: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP (
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update reque
 Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.3
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) State Update from Mobility
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6315, Adv
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
  IPv4 ACL ID = 255,
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobil
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 Sent an XID frame
*dtlArpTask: Nov 24 04:30:47.932: e4:b3:18:7c:30:58 Static IP client associated to interface vlan2404 wh
*dtlArpTask: Nov 24 04:30:47.933: e4:b3:18:7c:30:58 apfMsRunStateInc
*dtlArpTask: Nov 24 04:30:47.933:
e4:b3:18:7c:30:58 172.16.0.151 DHCP_REQD (7) Change state to RUN (20)
last state DHCP_REQD (7)
```

Voor een eenvoudige manier om te lezen debug client outputs, gebruik de draadloze debug analyzer tool:

Wireless Debug Analyzer

### Verificatieproces op ISE

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

Klik voor meer informatie op **Details** om een meer gedetailleerd verificatieproces te zien, zoals in de afbeelding.

- al C	sete Ident	ity Service	s Engine	Home	In Context Visibility	ity -Operation	s Policy I	Administration	+ Work Centers
	▼RADIUS	TC-NAC Li	ve Logs	▶ TACACS	Reports + Troubl	eshoot 🕨 Adapti	ve Network Control		
L	Live Logs	Live Sessio	ons						
		ħ	Misconfigured Supplicants			nfigured Networl Devices O	RADIUS Drops 🖲		Client Stopp
								R	efresh Never
	C Refresh	n 🗢 Reset Repeat Counts 🛛 🛃 Export To 👻							
	Time	e Sta	Details	Ide	Endpoint ID	Endpoint	Authentication P	Policy	Authorization Policy
	No	1	ò	user1	08:74:02:77:13:45	Apple-Device	Default >> Rule nam	ne >> Default	Default >> NameAuthZr

# Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar om deze configuratie problemen op te lossen.

### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.