## Konfigurieren der 802.1X-Authentifizierung mit PEAP, ISE 2.1 und WLC 8.3

### Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Netzwerkdiagramm **Konfiguration RADIUS-Server auf WLC deklarieren** SSID erstellen WLC auf der ISE deklarieren Neuen Benutzer auf ISE erstellen Authentifizierungsregel erstellen Erstellen des Autorisierungsprofils Autorisierungsregel erstellen Konfiguration des Endgeräts Endgerätekonfiguration - ISE-selbstsigniertes Zertifikat installieren Endgerätekonfiguration - Erstellen Sie das WLAN-Profil. Überprüfung Authentifizierungsprozess auf WLC Authentifizierungsprozess auf der ISE Fehlerbehebung

### Einleitung

In diesem Dokument wird die Einrichtung eines Wireless Local Area Network (WLAN) mit 802.1x-Sicherheit und Virtual Local Area Network (VLAN) Override beschrieben.

### Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- 802.1x
- Protected Extensible Authentication Protocol (PEAP)
- Zertifizierungsstelle (CA)
- Zertifikate

#### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

• WLC Version 8.3.102.0

- Identity Service Engine (ISE) Version 2.1
- Windows 10-Laptop

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

### Hintergrundinformationen

Wenn Sie ein WLAN mit 802.1x-Sicherheit und VLAN einrichten, können Sie das Protected Extensible Authentication Protocol als Extensible Authentication Protocol (EAP) außer Kraft setzen.

### Konfigurieren

### Netzwerkdiagramm



#### Konfiguration

Die allgemeinen Schritte sind wie folgt:

- 1. Deklarieren Sie den RADIUS-Server auf dem WLC und umgekehrt, um die Kommunikation untereinander zu ermöglichen.
- 2. Erstellen Sie den Service Set Identifier (SSID) im WLC.

- 3. Erstellen Sie die Authentifizierungsregel auf der ISE.
- 4. Erstellen Sie das Autorisierungsprofil auf der ISE.
- 5. Erstellen Sie die Autorisierungsregel für die ISE.
- 6. Konfigurieren Sie den Endpunkt.

#### **RADIUS-Server auf WLC deklarieren**

Um die Kommunikation zwischen dem RADIUS-Server und dem WLC zu ermöglichen, müssen Sie den RADIUS-Server auf dem WLC registrieren und umgekehrt.

GUI:

Schritt 1: Öffnen Sie die grafische Benutzeroberfläche des WLC, und navigieren Sie zu **SECURITY** > **RADIUS** > **Authentication** > **New**, wie im Bild dargestellt.

،،ا،،،ا،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	RADIUS Authentication Servers
▼ AAA General	Auth Called Station ID Type AP MAC Address:SSID <->
<ul> <li>RADIUS Authentication</li> </ul>	Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Accounting Fallback	MAC Delimiter Hyphen V
DNS	Framed MTU 1300

Schritt 2: Geben Sie die Informationen zum RADIUS-Server wie im Bild dargestellt ein.

RADIUS Authentication Ser	vers > 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 for	·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> entspricht dem RADIUS-Server.

#### **SSID** erstellen

GUI:

Schritt 1: Öffnen Sie die grafische Benutzeroberfläche des WLC, und navigieren Sie zu **WLANs > Create New > Go** (WLANs > Neues erstellen > Gehe zu), wie im Bild dargestellt.



Schritt 2: Wählen Sie einen Namen für die SSID und das Profil aus, und klicken Sie dann wie im Bild dargestellt auf **Apply**.

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

CLI:

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

Schritt 3: Weisen Sie den RADIUS-Server dem WLAN zu.

CLI:

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

GUI:

Navigieren Sie zu **Security** > **AAA Servers**, und wählen Sie den gewünschten RADIUS-Server aus. Drücken Sie dann auf **Apply** (Anwenden), wie im Bild dargestellt.

ANs > Edit	t 'ise-prof'	< Back	Ар
eneral	Security QoS Policy-Mapping Advanced		
Layer 2	Layer 3 AAA Servers		
			^
elect AAA	servers below to override use of default servers on this WLAN		
ADIUS Ser	vers		
RADIUS S	Server Overwrite interface 🛛 Enabled		
	Authentication Servers Accounting Servers EAP Parameters		
	Enabled Enable Enable		
Server 1	Enabled     Enabled     Enabled       IP:172.16.15.8, Port:1812     None		
Server 1 Server 2	Enabled     Enabled     Enabled       IP:172.16.15.8, Port:1812     None        None     None		
Server 1 Server 2 Server 3	✓ Enabled       Enabled       Enable         IP:172.16.15.8, Port:1812       None ∨         None       None ∨         None       None ∨		1
Server 1 Server 2 Server 3 Server 4	✓ Enabled       Enabled       Enable         IP:172.16.15.8, Port:1812       None ∨         None       None ∨		
Server 1 Server 2 Server 3 Server 4 Server 5	✓ Enabled       Enabled       Enable         IP:172.16.15.8, Port:1812       None ∨         None       None ∨		1
Server 1 Server 2 Server 3 Server 4 Server 5 Server 6	✓ Enabled       Enabled       Enable         IP:172.16.15.8, Port:1812       None ∨         None       None ∨		
Server 1 Server 2 Server 3 Server 4 Server 5 Server 6 <b>RADIUS Ser</b>	Enabled Enabled Enabled   IP:172.16.15.8, Port:1812 None    None None    None None    None None    None None    None None    None None		
Server 1 Server 2 Server 3 Server 4 Server 5 Server 6 <b>RADIUS Ser</b>	Enabled Enabled Enabled   IP:172.16.15.8, Port:1812 None   None None		

Schritt 4: Aktivieren Sie **AAA-Außerkraftsetzung zulassen**, und erhöhen Sie optional das Sitzungs-Timeout.

CLI:

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

GUI:

Navigieren Sie zu WLANs > WLAN ID > Advanced, und aktivieren Sie Allow AAA Override. Geben Sie optional das Sitzungstimeout wie im Bild dargestellt an.

WLANs > Edit 'ise-p	rof		< Back	A
General Security	QoS Policy-Mapping	Advanced		
Allow AAA Override	Foshled	DHCP		Â
Coverage Hole Detection	✓ Enabled ✓ Enabled	DHCP Serve	er 🗌 Override	
Enable Session Timeout	Session Timeou (secs)	DHCP Addr. Assignmen	t Required	
Aironet IE	Enabled	OEAP		
Diagnostic Channel <u>18</u>	Enabled	Split Tunne	el 🗌 Enabled	
Override Interface ACL	IPv4 None 🗸	IPv6 None 💛 Management I	Frame Protection (MFP)	
Layer2 Ad	None 🗸			
URL ACL	None 🗸	MFP Client	Protection 🛃 Optional 🖂	
P2P Blocking Action	Disabled $\lor$	DTIM Period (i	in beacon intervals)	
Client Exclusion 💈	Enabled 60 Timeout Value (secs)	802.11a/n	(1 - 255) 1	
Maximum Allowed Clients <sup>g</sup>	0	802.11b/g/ NAC	'n (1 - 255) 1	
Static IP Tunneling	□	NAC State	None	>

Schritt 5: Aktivieren des WLAN

CLI:

> config wlan enable <wlan-id>

GUI:

Navigieren Sie zu **WLANs > WLAN ID > General (WLAN-ID > Allgemein**), und aktivieren Sie die SSID, wie im Bild dargestellt.

WLANs > E				< Back	Apply			
General	Security	QoS	Policy-Mapping	Advanced				
Profile Na Type SSID Status Security I	ame ise Wi ise Volicies [W (Mo	prof LAN ssid Enabled /PA2][Au odification	Ith (802.1X)] is done under security	tab will appear a	fter applying the	e changes.)	1	
Radio Po Interface Group(G) Multicast Feature Broadcas NAS-ID	licy All /Interface m Vlan t SSID no	anageme Enabled Enabled ne	∨ int ∨					

#### WLC auf der ISE deklarieren

Schritt 1: Öffnen Sie die ISE-Konsole, und navigieren Sie zu Administration > Network Resources > Network Devices > Add, wie im Bild dargestellt.

dialo Identity Services Engine	Home	▶ Context \	/isibility	<ul> <li>Operations</li> </ul>	Policy	★Administratio	n 🔸
<ul> <li>System</li> <li>Identity Management</li> </ul>	✓Netwo	rk Resources	Device	Portal Managemen	t pxGrid S	Services 🔹 🕨 Fee	d Service
✓Network Devices Network Device	Groups	Network Devic	e Profiles	External RADIUS	Servers	RADIUS Server S	equence
0	•						
Network devices	Net	work Devices	6				
Default Device	/ E	dit 🕂 Add 🖸	Duplicate	😰 Import 🚯 Exp	ort 👻 🙆 G	enerate PAC 🗙	Delete 👻

Schritt 2: Geben Sie die Werte ein.

Optional können ein bestimmter Modellname, eine bestimmte Softwareversion, eine Beschreibung sowie die Zuweisung von Netzwerkgerätegruppen basierend auf Gerätetypen, Standort oder WLCs angegeben werden.

a.b.c.d entspricht der WLC-Schnittstelle, die die angeforderte Authentifizierung sendet. Standardmäßig ist dies die Management-Schnittstelle, wie im Bild dargestellt.

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 wlc-software 🍸
* Network Device Group
Device Type       WLCs-2504       Set To Default         Location       All Locations       Set To Default         WLCs       WLCs       Set To Default
RADIUS Authentication Settings
Enable Authentication Settings
* 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

Weitere Informationen zu Netzwerk-Gerätegruppen:

ISE – Netzwerkgerätegruppen

#### Neuen Benutzer auf ISE erstellen

Schritt 1: Navigieren Sie zu Administration > Identity Management > Identities > Users > Add (Administration > Identitätsmanagement > Identitäten > Benutzer > Hinzufügen), wie in der Abbildung dargestellt.

diado Identity Services Engine	Home	▶ Context Visibility	Operations	Policy	<ul> <li>Administration</li> </ul>
System	▶ Network F	Resources 🕨 Device	Portal Managemer	nt pxGrid 8	System
▼Identities Groups External Identi	ity Sources	Identity Source Sequ	Jences 🕨 🕨 Setting	IS	Deployment Licensing
C Users	Networ	k Access Users			Certificates Logging Maintenance
Latest Manual Network Scan Res	🥖 Edit	🕂 Add 🔣 🔛 Change St	atus 👻 💽 Import	🕞 Export 👻	Upgrade Backup & Restor
	Stat	tus Name	-	Description	Admin Access
	🎲 Loa	ading			Settings
					Identity Managem Identities

Schritt 2: Geben Sie die Informationen ein.

In diesem Beispiel gehört dieser Benutzer zu einer Gruppe mit dem Namen ALL\_ACCOUNTS, kann jedoch nach Bedarf angepasst werden, wie im Bild gezeigt.

Network Access Users List > New Network Access User	
<ul> <li>Network Access User</li> </ul>	
*Name user1	
Status 🛃 Enabled 👻	
Email	
▼ Passwords	
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	
▼ User Groups	
📕 ALL_ACCOUNTS (default) 🛛 💿 🔶 🕂	
Submit Cancel	

#### Authentifizierungsregel erstellen

Authentifizierungsregeln werden verwendet, um zu überprüfen, ob die Anmeldeinformationen der Benutzer korrekt sind (überprüfen Sie, ob der Benutzer wirklich der ist, für den er sich ausgibt), und um die Authentifizierungsmethoden einzuschränken, die von ihm verwendet werden dürfen.

Schritt 1: Navigieren Sie zu **Policy > Authentication (Richtlinie > Authentifizierung**), wie im Bild dargestellt.



Schritt 2: Fügen Sie eine neue Authentifizierungsregel wie im Bild dargestellt ein.

altalia cisco	Identity	Services Engine	e Home	e 🕨 Conte	et Visibility	Operations	→Policy	Administration	
Auth	entication	Authorization	Profiling	Posture Cli	ent Provisionin	g 🔹 🕨 Policy El	ements		
ting the p System > ed	rotocols tł Backup &	nat ISE should use Restore > Policy E	to communic: xport Page	ate with the net	twork devices, a	and the identity	sources that it	t should use for authe	enticat
_Protocol	: If VVi Is and :us	red_MAB <b>OR</b> se Internal Endpoir	nts						
IC_Proto	: If Wi cols an	red_802.1X <b>OR</b> d							

Schritt 3: Geben Sie die Werte ein.

Diese Authentifizierungsregel lässt alle Protokolle zu, die in der Liste "Standard-Netzwerkzugriff" aufgeführt sind. Dies gilt für die Authentifizierungsanforderung für Wireless-802.1x-Clients mit Called-Station-ID und endet mit ise-ssid, wie im Bild gezeigt.

dialo Identity	Services Engine	B Home	▸ Context Visibility	Operations	▼Policy	► Administra	ation 🕨
Authentication	Authorization	Profiling Pos	ture Client Provisio	ning 🔹 🕨 Policy Ele	ements		
Authenticatio	n Policy ntication Policy by	selecting the prote	ocols that ISE should u	ise to communicate	e with the netv	vork devices, an	id the identity
Policy Type	Simple 💿 Rul	e-Based	ckup & Restore > Point	y Export Page			
<ul> <li>Image: A set of the set of the</li></ul>	Rule name		: If Wireless_802.1	X AND Select Attrib	ute 😐 Al	llow Protocols :	Default Net
			Add All Co	nditions Below to L	ibrary		
<b></b>	Default		: Us Condition	Name	Description	-+ 000 1V	
				J2.1X 💟 AC	Padiuc(Call	aton 802, IX ba	Sed authent
			× [		Raulus;Call	eu-sta 💟	Enus With

Wählen Sie außerdem die Identitätsquelle für die Clients aus, die dieser Authentifizierungsregel entsprechen. In diesem Beispiel wird die Identitätsquellenliste für interne Benutzer verwendet, wie im Bild dargestellt.

Rule name : If W	freless_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	Identity Source List
~	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	<ul> <li>All_AD_Join_Points</li> <li>All_User_ID_Stores</li> <li>Certificate_Request_</li> </ul>
~		<ul> <li>DenyAccess</li> <li>Guest Users</li> <li>Guest_Portal_Seque</li> <li>IdnetitySequence_J</li> </ul>
		<ul> <li>Internal Endpoints</li> <li>Internal Users</li> </ul>

Klicken Sie abschließend auf Fertig und Speichern, wie im Bild dargestellt.

🖉 🖉 🖌 Rule name	: If Wretess_002.1X AND Radius Cal	Done
🖉 🔹 Default	: Use Internat Users 🔿	Actions +
		_
Seve Resot		

Weitere Informationen zu Identitätsquellen finden Sie unter diesem Link:

Benutzeridentitätsgruppe erstellen

#### Erstellen des Autorisierungsprofils

Das Autorisierungsprofil bestimmt, ob Sie Zugriff auf das Netzwerk haben. Push-Zugriffskontrolllisten (ACLs), VLAN-Übersteuerung oder andere Parameter. Das in diesem Beispiel gezeigte Autorisierungsprofil sendet eine Bestätigung für den Zugang an Sie und weist VLAN 2404 zu.

Schritt 1: Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse**, wie im Bild dargestellt.



Schritt 2: Hinzufügen eines neuen Autorisierungsprofils Navigieren Sie zu **Autorisierung** > **Autorisierungsprofile** > **Hinzufügen**, wie im Bild dargestellt.

ditation Identity Services	s Engine 🛛 🖡	Home 🔸	Context Visibility	• Operations
Authentication Authoriz	ation Profiling	Posture	Client Provisioning	→Policy Elements
Dictionaries + Condition	is <b>≁</b> Results			
Authentication	G	Standa For Policy	ird Authorization	n <b>Profiles</b> stration > System > Ba
<ul> <li>Authorization</li> </ul>				
Authorization Profiles		/ Edit		e XDelete
Downloadable &CLs		Nan	ne	

Schritt 3: Geben Sie die im Bild angezeigten Werte ein.

Authorization Profiles > New Authori Authorization Drofile	zation Profile	
* Name PermitA	ccessVLAN2404	
Description		
* Access Type ACCESS	ACCEPT	
Network Device Profile 🏼 🎎 Cisc	·• • •	
Service Template		
Track Movement 🛛 🗊		
Passive Identity Tracking 🛛 👔		
Common Tasks  ACL (Fitter-ID)		
. ,		
VLAN	Tag ID 0	Edit Tag ID/Name 2404
VLAN	Tag ID 0	Edit Tag ID/Name 2404
VLAN Voice Domain Permission NAch Redirection (C)A/A_MDM	Tag ID 0	Edit Tag ID/Name 2404
VLAN Voice Domain Permission Voice Domain Permission Voice Domain Permission Advanced Attributes Sett	Tag ID <b>0</b> אופס מסט או	Edit Tag ID/Name 2404
VLAN Voice Domain Permission Voice Domain Permission Voice Domain Permission Advanced Attributes Sett Select an item	Tag ID 0	Edit Tag ID/Name 2404
<ul> <li>VLAN</li> <li>Voice Domain Permission</li> <li>VAlab Redirection (CARA_MDM)</li> <li>Advanced Attributes Sett</li> <li>Select an item</li> <li>Select an item</li> </ul>	Tag ID 0 NISD CODY (2) tings 	Edit Tag ID/Name 2404
<ul> <li>VLAN</li> <li>Voice Domain Permission</li> <li>Voice Domain Perm</li></ul>	Tag ID 0	Edit Tag ID/Name 2404

#### Autorisierungsregel erstellen

Die Autorisierungsregel bestimmt, welche Berechtigungen (welches Autorisierungsprofil) auf Sie angewendet werden.

Schritt 1: Navigieren Sie zu **Policy > Authorization (Richtlinie > Autorisierung)**, wie im Bild dargestellt.

es Engine	e Home 🔸	Context Visibility	Operations	→ Policy → Ad	dministration	
horization	Profiling Posture	Client Provisioning	Policy Ele	Authentication	Authorization	
				Profiling	Posture	
Y				Client Provisioni	ing Policy Elements	s
Policy by c	onfiguring rules base	d on identity groups and		Dictionaries		
dministrati	on > System > Backup	o & Restore > Policy Exp	ort Page		Conditions	
olies	•				Results	

Schritt 2: Fügt eine neue Regel wie im Bild dargestellt ein.

cisco	Identity	Services Engi	ne H	Home	Context Visibility	♦ Operations	→Policy	Administration	• Work Centers
Auther	ntication	Authorization	Profiling	Posture	e Client Provisioning	) • Policy Eleme	nts		
ifiguring ru > System >	les based ∘ Backup ∂	on identity group: & Restore > Policy	s and/or oti / Export Pa	her conditi ge	ons. Drag and drop ru	lles to change the	order.		
		Conditions	s (identity <u>c</u>	groups and	l other conditions)			Permissions	

Schritt 3: Geben Sie die Werte ein.

Wählen Sie zunächst einen Namen für die Regel und die Identitätsgruppe aus, in der der Benutzer gespeichert ist (ALL\_ACCOUNTS), wie im Bild gezeigt.

	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 License	if	C'ac Any	
		Profile 2 Cisco ser Loreis	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
	-				

Wählen Sie anschließend andere Bedingungen aus, die dazu führen, dass der Autorisierungsprozess in diese Regel fällt. In diesem Beispiel trifft der Autorisierungsprozess diese Regel, wenn er 802.1x Wireless verwendet und die angerufene Stations-ID mit ise-ssid endet, wie im Bild gezeigt.

	Status	Rule Name	Conditions (identity groups and other condi	tions)	Permissions
P	-	NameAuthZrule	if AL 💠 and Wireless_802	.1X AND Radius:Call	then AuthZ F
			S 💾 Add All	Conditions Below to Library	/
			مر <sup>1</sup> Condit	ion Name De:	scription
1	<b>~</b>		Wireless	802.1X ONORMALISE	ed Radius:RadiusFlowType E
1	<b>~</b>		e:		

Wählen Sie abschließend das Autorisierungsprofil aus, das Ihnen zugewiesen ist und auf diese Regel trifft. Klicken Sie auf **Fertig** und **Speichern**, wie im Bild dargestellt.

		Status	Rule Name	Co	onditions (ident	ity group:	s and other conditions)		Permi	ssions	_
	ø	<b>–</b> •	NameAuthZrule	if	AL	💠 and	Wireless_802.1X AND Radius:Call	¢	then	AuthZ Pr	-
1		<b>~</b>									
1		<ul> <li>Image: A set of the set of the</li></ul>								Select an it	em
1		<b>~</b>									
		~									
1		0									
1		0									
_		-									_
1		0									
1		0									
1		0									
1											
		<b>~</b>	Default	if no r	matches, then	Deny.	Access				
	5av	e Re:	et								

#### Konfiguration des Endgeräts

Konfigurieren Sie einen Windows 10-Laptop-Computer für die Verbindung mit einer SSID mit 802.1x-Authentifizierung und PEAP/MS-CHAPv2 (Microsoft-Version des Challenge-Handshake-Authentifizierungsprotokolls) Version 2.

In diesem Konfigurationsbeispiel verwendet die ISE ein selbstsigniertes Zertifikat für die Authentifizierung.

Um das WLAN-Profil auf dem Windows-Computer zu erstellen, gibt es zwei Optionen:

- 1. Installieren Sie das selbstsignierte Zertifikat auf dem Computer, um es zu validieren, und vertrauen Sie dem ISE-Server, um die Authentifizierung abzuschließen.
- 2. Umgehen Sie die Validierung des RADIUS-Servers, und vertrauen Sie allen RADIUS-Servern, die für die Authentifizierung verwendet werden (nicht empfohlen, da dies zu einem Sicherheitsproblem werden kann).

Die Konfiguration dieser Optionen wird unter Endgerätekonfiguration - Erstellen des WLAN-Profils - Schritt 7 erläutert.

#### Endgerätekonfiguration - ISE-selbstsigniertes Zertifikat installieren

Schritt 1: Selbstsigniertes Zertifikat exportieren

Melden Sie sich bei der ISE an, und navigieren Sie zu Administration > System > Certificates > System Certificates.

Wählen Sie dann das für die **EAP-Authentifizierung** verwendete Zertifikat aus, und klicken Sie wie im Bild dargestellt auf **Exportieren**.

<ul> <li>System          <ul> <li>Identity Management              <ul> <li>Network Resources              <ul> <li>Device Portal Management pxGrid Services                  </li> <li>Feed Service                  </li> <li>Licensing                      <ul> <li>Certificates                      <ul> <li>Logging                      <ul> <li>Maintenance Upgrade Backup &amp; Restore                            <ul> <li>Admin Access                               </li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul>
Deployment Licensing  Certificates   Logging   Maintenance  Upgrade  Backup & Restore  Admin Access <b>Certificate Management</b> Overview      Overview  Overview  Delete  Edit Fiendly Name Used By Portel group teg
G         • Certificate Management       System Certificates       A For disaster recovery it is recommended to export certificate a         Overview       ✓ Edit       Generate Self Signed Certificate       Import       Export       X Delete         Outer Outer de Vir. de       Eriepdly Name       Used By       Portel group teg
Certificate Management     System Certificates A For disaster recovery it is recommended to export certificate a     Overview     Certificate Self Signed Certificate     Friendly Name     Used By     Portal group teg
Overview / Edit - Generate Self Signed Certificate - Import Export Delete
Eriendly Name Liead By Portal around an
System Certificates Prenary Name Used By Portal gloup tag
Endpoint Certificates
Trusted Certificates       EAP-SelfSignedCertificate#E         Image: Application Certificate Ce

Speichern Sie das Zertifikat am erforderlichen Speicherort. Dieses Zertifikat muss auf dem Windows-Computer installiert werden, wie im Bild dargestellt.

Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001'	8
<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 ke	у.
	:el

Schritt 2: Installieren Sie das Zertifikat auf dem Windows-Computer.

Kopieren Sie das von ISE exportierte Zertifikat in den Windows-Computer, ändern Sie die Dateierweiterung von .pem in .crt, und doppelklicken Sie danach, um sie wie im Bild gezeigt zu installieren.

🐱 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	
OK	5

Schritt 3: Wählen Sie Install it in Local Machine (Lokaler Computer) aus, und klicken Sie auf Next (Weiter), wie im Bild dargestellt.

<ul> <li>&amp; Certificate Import Wizard</li> </ul>	×
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 contain information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	, I
Store Location	
O Current User	
Local Machine	
To continue, click Next.	
Sheat Car	ncel

Schritt 4: Wählen Sie Alle Zertifikate in diesem Speicher platzieren, dann die Option Vertrauenswürdige Stammzertifizierungsstellen durchsuchen und auswählen. Klicken Sie anschließend auf Weiter, wie im Bild gezeigt.

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. 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	Certificate Store	a an hÉachas an back	
Windows can automatically select a certificate store, or you can specify a location for 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	Certificate stores are system areas when	e certificates are kept.	
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	Windows can automatically select a certil the certificate.	ficate store, or you can specify a lo	ocation for
Place all certificates in the following store Certificate store: Trusted Root Certification Authorities     Browse	O Automatically select the certificate	store based on the type of certific	cate
Certificate store: Trusted Root Certification Authorities Browse	Place all certificates in the following	g store	
Trusted Root Certification Authorities Browse	Certificate store:		
	Trusted Root Certification Author	rities Br	owse

Schritt 5: Klicken Sie dann auf Fertig stellen, wie im Bild dargestellt.

← 🖉 Certificate Import Wizard	×
Completing the Certificate Import Wizard	
The certificate will be imported after you click Finish.	
You have specified the following settings:	
Centrificate Store Selected by User Content Centrification Authonities	
Finish Ca	ncel

Schritt 6: Bestätigen Sie die Installation des Zertifikats. Klicken Sie wie in der Abbildung dargestellt auf Ja.



Schritt 7. Klicken Sie abschließend auf OK, wie im Bild gezeigt.



#### Endgerätekonfiguration - Erstellen Sie das WLAN-Profil.

Schritt 1: Klicken Sie mit der rechten Maustaste auf das Symbol **Start**, und wählen Sie **Systemsteuerung** wie im Bild dargestellt aus.

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	
📒 🔜 UownL., 👽 Networ., ۹	

Schritt 2: Navigieren Sie zu **Netzwerk und Internet**, navigieren Sie anschließend zum **Netzwerk- und Freigabecenter**, und klicken Sie auf **Neue Verbindung oder neues Netzwerk einrichten**, wie im Bild dargestellt.

👙 Network and Sharing Center					
🔶 🚽 🗠 🛧 😫 > Control Par	el > Network and Internet > Network and Sharing	Center			
Control Panel Home View your basic network information and set up connections					
Change adapter settings	Change adapter settings				
Change advanced sharing settings	cisco.com Access type: Internet Domain network Connections: 40° Ethernet				
	Channe your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN opnec Troubleshoot problems Diagnose and repair network problems, or g	ction; or set up a router or access point. get troubleshooting information.			

Schritt 3: Wählen Sie **Manuell mit einem Wireless-Netzwerk verbinden aus**, und klicken Sie auf **Weiter**, wie im Bild gezeigt.

	-		×
Choose a connection option			
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.			
N	ort	Can	cel

Schritt 4: Geben Sie die Informationen mit dem Namen der SSID und dem Sicherheitstyp WPA2-Enterprise ein, und klicken Sie auf **Weiter**, wie im Bild dargestellt.

			-		×
+	🐓 Manually connect to a	wireless network			
	Enter information f	or the wireless network you want to a	dd		
	Network name:	ise-ssid			
	Security type:	WPA2-Enterprise ~			
	Encryption type:	AES			
	Security Key:	Hide chi	aracters		
	Start this connection	in automatically			
	Connect even if the	e network is not broadcasting			
	Warning: If you sel	ect this option, your computer's privacy might be	at risk.		
			Next	Cano	el

Schritt 5: Wählen Sie **Verbindungseinstellungen ändern** aus, um die Konfiguration des WLAN-Profils wie im Bild dargestellt anzupassen.



Schritt 6: Navigieren Sie zur Registerkarte **Sicherheit**, und klicken Sie auf **Einstellungen**, wie im Bild dargestellt.

ise-ssid Wireless Ne	twork Properties			×
Connection Security				
Security type:	WPA2-Enterprise		$\sim$	
Encryption type:	AES		$\sim$	
Choose a network aut	hentication method:			
Microsoft: Protected	EAP (PEAP) 🗸 🗸	Settin	gs	
Remember my cre	dentials for this conne	ction each		
time I'm logged o	n			
Advanced settings				
-				
		OK	Cano	el

Schritt 7. Wählen Sie aus, ob der RADIUS-Server validiert ist oder nicht.

Wenn ja, aktivieren Sie **Überprüfen der Serveridentität durch Validieren des Zertifikats** und von **Trusted Root Certification Authorities:** list wählen Sie das selbstsignierte Zertifikat von ISE aus.

Wählen Sie anschließend **Konfigurieren** und Deaktivieren **Automatisch meinen Windows-Anmeldenamen und mein Kennwort verwenden...**, und klicken Sie dann auf **OK**, wie in den Bildern dargestellt.

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:	
□ Egg00: A Cleft à laise dan □ Egg00: A Cleft Assachte e à Court da	^
EAP-SelfSignedCertificate	
E mathematic Cathering and Barton and Cathering (1997)	
Construct Clabels	~
Notifications before connecting:	
Tell user if the server name or root certificate isn't specified	$\sim$
Select Authentication Method:	
Secured password (EAP-MSCHAP v2) Configur	e
C Enable Fast Reconnect	
Disconnect if server does not present cryptobinding TLV	
Enable Identity Privacy	
OK Cance	el
EAP MSCHAPv2 Properties X	
When connecting:	
Automatically use my Windows logon name and password (and domain if any).	

Schritt 8: Konfigurieren Sie die Anmeldeinformationen des Benutzers.

Cancel

ОK

Wenn Sie wieder zur Registerkarte **Sicherheit** zurückkehren, wählen Sie **Erweiterte Einstellungen aus,** geben Sie den Authentifizierungsmodus als Benutzerauthentifizierung an, und **speichern Sie** die auf der ISE konfigurierten Anmeldeinformationen, um den Benutzer wie in den Abbildern dargestellt zu authentifizieren.

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

vanced settings		
2.1X settings 802.11 settings		
Specify authentication mode:		
User authentication	Save cr	edentials
Delete credentials for all users		
Enable single sign on for this network		
Perform immediately before user	logon	
<ul> <li>Perform immediately after user lo</li> </ul>	gon	
Maximum delay (seconds):	10	-
Allow additional dialogs to be disp sign on	alayed during s	single
This network uses separate virtua	I LANs for ma	chine
	OK	Cancel

Windows Secu	rity	×
Save creder	ntials	
Saving your cre when you're no	dentials allows your computer to connect to the netw togged on (for example, to download updates).	ork
	user1	
_		
	OK Can	:el

# Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Der Authentifizierungsfluss kann aus WLC- oder ISE-Sicht verifiziert werden.

#### Authentifizierungsprozess auf WLC

Führen Sie die folgenden Befehle aus, um den Authentifizierungsprozess für einen bestimmten Benutzer zu überwachen:

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

Beispiel für eine erfolgreiche Authentifizierung (einige Ausgaben wurden ausgelassen):

<#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 Successful transmission of LWAPP Add-Mobile to AP @ \*spamApTask2: Nov 24 04:30:44.325: 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 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 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\_MsgTask\_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\_MsqTask\_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18:7 \*Dot1x NW MsgTask 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 Req 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\_MsqTask\_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mol \*Dot1x\_NW\_MsgTask\_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 MsgTask 0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Reg 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 fi \*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 Stopping reauth timeout for e4:b3:18:7c:30:5 \*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\_MsqTask\_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) [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: \*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\_MsqTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 0 PMK-update groupcast messages sent \*Dot1x NW MsgTask 0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 PMK sent to mobility group \*Dot1x\_NW\_MsqTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Disabling re-auth since PMK lifetime can tal \*Dot1x\_NW\_MsgTask\_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 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:3 \*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 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 00.00.00.00.00.00.00.00.01
\*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 Received EAPOL-Key from mobile e4:b3:18:7c:30:58
\*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
\*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
\*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
\*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
\*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 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 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 Virtual Ip: 10.10.10.10 \*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 \*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\_MsgTask\_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code qosCap 00 \*Dot1x\_NW\_MsqTask\_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LN \*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)

Eine einfache Möglichkeit zum Lesen von Debug-Client-Ausgaben bietet das Wireless Debug Analyzer-Tool:

Wireless-Debug-Analyzer

#### Authentifizierungsprozess auf der ISE

Navigieren Sie zu **Operations > RADIUS > Live Logs**, um festzustellen, welche Authentifizierungsrichtlinie, Autorisierungsrichtlinie und welches Autorisierungsprofil dem Benutzer zugewiesen wurde.

Für weitere Informationen klicken Sie auf **Details**, um einen detaillierteren Authentifizierungsprozess anzuzeigen, wie im Bild dargestellt.

- 1	tata Ident	ity Service	s Engine	e Home	+ Context Visibili	ty + Operation	ns Policy	<ul> <li>Administration</li> </ul>	• Work Centers
	▼RADIUS	TC-NAC Li	ve Logs	+ TACACS	Reports + Trouble	eshoot 🕨 Adapt	ive Network Contro	ol	
L	Live Logs	Live Sessio	ons						
		Misconfigur		ured Supplic	ants Misco	Misconfigured Network Devices 🛛		ADIUS Drops 🛛	Client Stop
								R	efresh Never
	C Refresh	● Rese	t Repeat C	ounts 🛛 💆 E	Export To 🕶				
	Time	e Sta	Details	Ide	Endpoint ID	Endpoint	Authentication	) Policy	Authorization Policy
	No	1	Q	user1	08:74:02:77:13:45	Apple-Device	Default >> Rule name >> Default		Default >> NameAuthZr

## Fehlerbehebung

Es sind derzeit keine spezifischen Informationen zur Fehlerbehebung für diese Konfiguration verfügbar.

#### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.