Configuración de la autenticación 802.1X con PEAP, ISE 2.1 y WLC 8.3

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configurar
Diagrama de la red
Configuración
Declare el servidor RADIUS en el WLC
Crear SSID
Declarar WLC en ISE
Creación de un usuario nuevo en ISE
Crear regla de autenticación
Creación del perfil de autorización
Crear regla de autorización
Configuración del dispositivo final
Configuración del dispositivo final: instalación del certificado autofirmado de ISE
Configuración del dispositivo final: creación del perfil WLAN
Verificación
Proceso de autenticación en WLC
Proceso de autenticación en ISE
Troubleshoot

Introducción

En este documento se describe cómo configurar una red de área local inalámbrica (WLAN) con seguridad 802.1x e invalidación de la red de área local virtual (VLAN).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- 802.1x
- Protocolo de autenticación extensible protegido (PEAP)
- Entidad de certificación (CA)
- Certificados

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC v8.3.102.0
- Identity Service Engine (ISE) v2.1
- Portátil Windows 10

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cuando configura una WLAN con seguridad 802.1x y VLAN, puede reemplazar con el protocolo de autenticación extensible protegido como protocolo de autenticación extensible (EAP).

Configurar

Diagrama de la red



Configuración

Los pasos generales son:

- 1. Declare el servidor de RADIUS en el WLC y viceversa para permitir la comunicación entre sí.
- 2. Cree el identificador del conjunto de servicios (SSID) en el WLC.
- 3. Cree la regla de autenticación en ISE.
- 4. Cree el perfil de autorización en ISE.
- 5. Cree la regla de autorización en ISE.
- 6. Configure el terminal.

Declare el servidor RADIUS en el WLC

Para permitir la comunicación entre el servidor RADIUS y el WLC, usted necesita registrar el servidor RADIUS en el WLC y viceversa.

GUI:

Paso 1. Abra la GUI del WLC y navegue hasta SECURITY > RADIUS > Authentication > New como se muestra en la imagen.

սիսիս	and the second	Sa <u>v</u> e Configuration <u>P</u> ing Lo <u>g</u> out <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	n Home
Security	RADIUS Authentication Servers	Apply New
AAA General	Auth Called Station ID Type 🛛 AP MAC Address:SSID 🚽	
 RADIUS Authentication 	Use AES Key Wrap 🗌 (Designed for FIPS customers and requires a key wrap compliant RADIUS server)	
Accounting	MAC Delimiter Hyphen 🗸	
DNS	Framed MTU 1300	

Paso 2. Introduzca la información del servidor RADIUS como se muestra en la imagen.

RADIUS Authentication Se	rvers > 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 \vee	
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> corresponde al servidor RADIUS.

Crear SSID

GUI:

Paso 1. Abra la GUI del WLC y navegue hasta WLANs > Create New > Go como se muestra en la imagen.

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs
WLANS WLANS WLANS	Current Filter: None [Change Filter] [Clear Filter] Create New Create New Create New

Paso 2. Elija un nombre para el SSID y el perfil y, a continuación, haga clic en Apply como se muestra en la imagen.

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

CLI:

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

Paso 3. Asigne el servidor RADIUS a la WLAN.

CLI:

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

GUI:

Navegue hasta Security > AAA Servers y elija el servidor RADIUS deseado, luego presione Apply como se muestra en la imagen.

_	: 'ise-prot'	< Back	A
eneral	Security QoS Polic	y-Mapping Advanced	
ayer 2	Layer 3 AAA Servers		
			^
elect AAA :	servers below to override use	of default servers on this WLAN	
ADIUS Ser	vers		
RADTUS	Server Overwrite interface	Fnabled	
NADIOS 3			
	Authentication Servers	Accounting Servers EAP Parameters	
	🗹 Enabled	🗹 Enable 🗌	
Server 1	Enabled IP:172.16.15.8, Port:1812	✓ Enabled Enable None ✓	
Server 1 Server 2	 Enabled IP:172.16.15.8, Port:1812 None 	✓ Enabled Enable ✓ None ✓ ✓ None ✓	
Server 1 Server 2 Server 3	Enabled IP:172.16.15.8, Port:1812 None None	✓ Enabled Enable None ✓ None ✓ None ✓	
Server 1 Server 2 Server 3 Server 4	Enabled IP:172.16.15.8, Port:1812 None None None	Enabled Enable None None None None None None None	
Server 1 Server 2 Server 3 Server 4 Server 5	Enabled IP:172.16.15.8, Port:1812 None None None None	<pre>✓ Enabled Enable </pre> None ✓ None ✓ None ✓ None ✓ None ✓ None ✓	
Server 1 Server 2 Server 3 Server 4 Server 5 Server 6	Enabled IP:172.16.15.8, Port:1812 None None None None None None		
Server 1 Server 2 Server 3 Server 4 Server 5 Server 6	Enabled IP:172.16.15.8, Port:1812 None N	<pre>✓ Enabled Enable </pre> None ✓ None ✓ None ✓ None ✓ None ✓ None ✓ None ✓	
Server 1 Server 2 Server 3 Server 4 Server 5 Server 6 ADIUS Ser	Enabled IP:172.16.15.8, Port:1812 None N		

Paso 4. Habilite Allow AAA Override y opcionalmente aumente el tiempo de espera de la sesión

CLI:

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

GUI:

Navegue hasta WLANs > WLAN ID > Advanced y habilite Allow AAA Override. Opcionalmente, especifique el tiempo de espera de sesión como se muestra en la imagen.

WLANs > Edit 'ise-pr	of			Sack	
General Security	QoS Policy-Mapping	Advanced			
					^
Allow AAA Override	🗹 Enabled	DHCP			
Coverage Hole Detection	🗹 Enabled	DHC	P Server	Override	
Enable Session Timeout	Session Timeou (secs)	DHC Assi	P Addr. ignment	Required	
Aironet IE	Enabled	OEAP			
Diagnostic Channel	Enabled	Spli	it Tunnel	Enabled	
Override Interface ACL	IPv4 None 🗹	IPv6 None 😪 Manage	ement Frame Prote	action (MFP)	
Layer2 Ad	None \vee				
URL ACL	None 🗸	MFP	Client Protection 4	Optional 🗸	
P2P Blocking Action	Disabled \lor	DTIM P	eriod (in beacon in	tervals)	
Client Exclusion 💈	Enabled 60 Timeout Value (secs)	802	.11a/n (1 - 255)	1	
Maximum Allowed Clients 🗳	0	802. NAC	.11b/g/n (1 - 255)	1	
Static IP Tunneling	□	NAC	State None	$\overline{\mathbf{v}}$	> ×

Paso 5. Active la WLAN.

CLI:

> config wlan enable <wlan-id>

GUI:

Navegue hasta WLANs > WLAN ID > General y habilite el SSID como se muestra en la imagen.

WLANs>Edit 'ise-p	rof	< Back	Apply
General Securit	y QoS Policy-Mapping Advanced		
Profile Name Type SSID Status	ise-prof WLAN ise-ssid Imabled		
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)	I	
Radio Policy	All		
Interface/Interface Group(G)	management 🗸		
Multicast Vlan Feature	Enabled		
Broadcast SSID	Enabled		
NAS-ID	none		

Declarar WLC en ISE

Paso 1. Abra la consola de ISE y navegue hasta Administration > Network Resources > Network Devices > Add como se muestra en la imagen.

Home	♦ Context V	/isibility	Operation	is ▶Pol	icy 🗸 Adm	inistration	► Worl
✓ Netwo	ork Resources	Device P	ortal Manag	ement px	Grid Services	▶ Feed Se	ervice (
e Groups	Network Devic	e Profiles:	External R/	ADIUS Serve	rs RADIUS	Server Sequ	ences
9							
Net	work Devices	6					
/ E	idit 🕂 Add 🕞	Duplicate	👍 Import (🏠 Export 👻	Generate P/	AC XDele	ete 🔻
	Home Netwo	Home Context V Network Resources G Network Devices C Edit + Add C	Home Context Visibility Network Resources Device Profiles Network Devices Letter L	Home Context Visibility Operation Network Resources Device Portal Manage Groups Network Device Profiles External R# Network Devices Legit Add Duplicate Import Import 	Home Context Visibility Operations Pol Network Resources Device Portal Management px See Groups Network Device Profiles External RADIUS Serve Network Devices Network Devices Edit Add Duplicate Import Export Export 	Home Context Visibility Operations Policy ~Adm Network Resources Device Portal Management pxGrid Services RADIUS Retwork Device Profiles External RADIUS Servers RADIUS Network Devices Network Devices Edit Add Duplicate Import Export < Generate Profiles Generate Profiles Add Duplicate Import Export < Generate Profiles Generate Profiles External RADIUS Response Respons	Home Context Visibility Operations Policy Administration Network Resources Device Portal Management pxGrid Services Feed Services RADIUS Server Sequities RADIUS Server Sequities Network Devices Network Devices Left Add Duplicate Import Export Generate PAC Device Context Visibility Operations Policy Add Duplicate Export Operations Context PAC Device Device Portal Management Policy Add Add Policy Policy

Paso 2. Introduzca los valores.

Opcionalmente, puede ser un nombre de modelo especificado, versión de software, descripción y asignar grupos de dispositivos de red basados en tipos de dispositivos, ubicación o WLC.

a.b.c.d corresponde a la interfaz WLC que envía la autenticación solicitada. De forma predeterminada, se trata de la interfaz de administración tal y como se muestra en la imagen.

Network Devices List > New Network Device Network Devices
* Name WLC-name
Description optional description
*IP Address: a.b.c.d / 32
* Device Profile 👾 Cisco 👻 🕀
Model Name wic-model
Software Version 🛛 🔤 😴
* Network Device Group
Leastion Wills-2504
All Locations 💟 Set To Default
WLCs 📀 Set To Default
✓ RADIUS Authentication Settings
Enable Authoritation Cottings
Protocol RADIUS
* Shared Secret
Enable Keylöran
* Key Encryption Key
t Massage Authoritiester Carda Kar
* Message Authenticator Code Key Show
Key Input Format ASCII HEXADECIMAL
CoA Port 1700 Set To Default

Para obtener más información sobre los grupos de dispositivos de red:

Creación de un usuario nuevo en ISE

Paso 1. Vaya a Administración > Administración de identidades > Identidades > Usuarios > Agregar como se muestra en la imagen.

dialo Identity Services Engine	Home 🔸 C	ontext Visibility	Operations	Policy	 Administration
▶ System ▼Identity Management	Network Reso	urces 🕨 Devic	e Portal Manageme	nt pxGrid 8	System
◄Identities Groups External Iden	tity Sources Ide	entity Source Sec	juences 🔹 🕨 Setting	js	Deployment Licensing
C Users	Certificates Logging Maintenance				
Latest Manual Network Scan Res	/ Edit + Ad	d 🔢 Change S	itatus 🔻 😭 Import	Export -	Upgrade Backup & Restor Admin Access
	Cading			Beschpabl	Settings
					Identity Managem

Paso 2. Introduzca la información.

En este ejemplo, este usuario pertenece a un grupo denominado ALL_ACCOUNTS, pero se puede ajustar según sea necesario, como se muestra en la imagen.

Network Access Users	List > New Networ	k Access User			
Network Access	User				
* Name user1					
Status 🗾 Enable	d 💌				
Email					
 Passwords 					
Password Type:	Internal Users	٣			
	Password		Re-Enter Passw		
* Login Password	•••••		•••••		
Enable Password					
👻 User Informati	on				
First Name					
Last Name					
Account Optio	ns				
	Description				
Change password	on next login 🛛				
Account Disable Policy					
Disable accourt	nt if date exceeds	2017-01-21			

2. Omita la validación del servidor RADIUS y confíe en cualquier servidor RADIUS utilizado para realizar la autenticación (no se recomienda, ya que puede convertirse en un problema de seguridad).

La configuración de estas opciones se explica en Configuración del dispositivo final: creación del perfil WLAN, paso 7.

Configuración del dispositivo final: instalación del certificado autofirmado de ISE

Paso 1. Exportar certificado autofirmado.

Inicie sesión en ISE y navegue hasta Administration > System > Certificates > System Certificates.

A continuación, elija el certificado utilizado para la autenticación EAP y haga clic en Exportar como se muestra en la imagen.



Guarde el certificado en la ubicación necesaria. Ese certificado debe estar instalado en el equipo con Windows como se muestra en la imagen.

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	y.
Export Canc	el

Paso 2. Instale el certificado en el equipo con Windows.

Copie el certificado exportado desde ISE en el equipo de Windows, cambie la extensión del archivo de .pem a .crt y, después, haga doble clic para instalarlo, como se muestra en la imagen.

Sertificate >	×
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	

Paso 3. Seleccione instalarlo en Local Machine y haga clic en Next como se muestra en la

imagen.

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

Paso 4. Seleccione Colocar todos los certificados en este almacén, busque y seleccione Entidades emisoras raíz de confianza. Después, haga clic en Next como se muestra en la imagen.

÷	Sertificate Import Wizard	×
	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	
	Next Canc	el

Paso 5. A continuación, haga clic en Finish como se muestra en la imagen.

← 🛛 & Certificate Import Wizard		×
Completing the Certifi	cate Import Wizard	
The certificate will be imported after	you click Finish.	
You have specified the following set	tings:	
Certificate Store Selected by User	Trusted Root Certification Authorities	
Content	Certificate	
	Finish Cance	

Paso 6. Confirme la instalación del certificado. Haga clic en Yes como se muestra en la imagen.

Security 1	Warning	×
	You are about to install a certificate from a certification authority (CA) claiming to represent: EAP-SelfSignedCertificate Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:	
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk. Do you want to install this certificate?	
	Yes No	

Paso 7. Finalmente, haga clic en OK como se muestra en la imagen.



Configuración del dispositivo final: creación del perfil WLAN

Paso 1. Haga clic con el botón derecho en el icono Start y seleccione Control Panel como se muestra en la imagen.

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

All a second as a second



Paso 3. Seleccione Manually connect to a wireless network, y haga clic en Next como se muestra en la imagen.

				х
🔶 💈 Set Up a	Connection or Network			
Choose a	connection option			
- Con	ect to the internet			
- 5450	p a broadband or dial-up connection to the internet.			
Set u	ip a new network			
	gramew rooter or access porn.			
A Man	ually connect to a wireless network sect to a hidden network or create a new wireless profile.			
Set u	p a dial-up or VPN connection to your workplace.			
		Next	Cano	el

Paso 4. Introduzca la información con el nombre del SSID y el tipo de seguridad WPA2-Enterprise y haga clic en Next, como se muestra en la imagen.

			-		×
4	🐓 Manually connect to a v	vireless network			
	Enter information fo	r the wireless network you want to add			
	Network name:	ise-ssid			
	Security type:	WPA2-Enterprise			
	Encryption type:	AES			
	Security Key:	Hide character	6		
	Start this connection	automatically			
	Connect even if the	network is not broadcasting			
	Warning: If you sele	ct this option, your computer's privacy might be at risk.			
		Ne	pet	Can	cel

Paso 5. Seleccione Change connection settings para personalizar la configuración del perfil WLAN como se muestra en la imagen.



Paso 6. Navegue hasta la pestaña Security y haga clic en Settings como se muestra en la imagen.

ise-ssid Wireless Ne	etwork Properties			×
Connection Security				
Security type:	WPA2-Enterprise		\sim	
Encryption type:	AES		\sim	
Choose a network aut	thentication method:			
Microsoft: Protected	EAP (PEAP) 🛛 🗸	Settin	gs	
Remember my cre	edentials for this connec	tion each		
time I'm logged o	n			
Advanced settings	5			
		OK	C	
		UK	Cance	21

Paso 7. Seleccione si el servidor RADIUS está validado o no.

En caso afirmativo, active Verificar la identidad del servidor validando el certificado y en la lista Entidades de certificación raíz de confianza: seleccione el certificado autofirmado de ISE.

Después seleccione Configure y desactive Automatically use my Windows logon name and password..., y haga clic en OK como se muestra en las imágenes.

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:	
 Equila V Cichai Interna. Equila 1985: Assessments infinite dat. Entrance infinite 	
EAP-SelfSignedCertificate	
End Advanced international over the control of the start of the s	
Notifications before connecting:	
Tell user if the server name or root certificate isn't specified $\qquad \qquad \qquad$	
Select Authentication Method:	
Secured password (EAP-MSCHAP v2) Configure.	
Enable Fast Reconnect	
Disconnect if server does not present cryptobinding TLV	
Enable Identity Privacy	
OK Cancel	

Una vez que vuelva a la pestaña Security, seleccione Advanced settings, especifique el modo de autenticación como User authentication y guarde las credenciales que se configuraron en ISE para autenticar al usuario como se muestra en las imágenes.

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 E	EAP (PEAP) 🛛 🗸	Setting	ps.	
Remember my cre time I'm logged or	dentials for this connect	tion each		
Advanced settings				
		ок	Cano	el

Advanced settings	×
802.1X settings 802.11 settings	
Specify authentication mode:	
User authentication Save credentials	
Delete credentials for all users	
Enable single sign on for this network	
Perform immediately before user logon	
 Perform immediately after user logon 	
Maximum delay (seconds): 10 *	
Allow additional dialogs to be displayed during single sign on	
This network uses separate virtual LANs for machine and user authentication	
OK Cano	el

Windows Security

Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

ahaha	user1		
cisco	•••••••		
		ОК	Cancel

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

El flujo de autenticación se puede verificar desde la perspectiva de WLC o ISE.

Proceso de autenticación en WLC

Ejecute los siguientes comandos para monitorear el proceso de autenticación para un usuario específico:

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

Ejemplo de una autenticación exitosa (se omitieron algunos resultados):

<#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

 \times

*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 Mobil *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 s *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 none4: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:b *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 mo *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 No valid PMKID found in the MSCB PMKID cache f *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 ru *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 sta *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2:session timeout forstation e4:b *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 *apfMsConnTask_1: Nov 24 04:30:44.320: e4:b3:18:7c:30:58 Sending Assoc Response to station on BSSID 00:

*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:
*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 rea *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 rea *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: *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 int *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_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received Identity Response (count=1) from m
*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 int
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.386: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=215) fo
*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:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAP Response from mobile e4:b3:18:
*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 mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=216) fo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b
```

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r

*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 6
*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 Mo *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 *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 Overri *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 Mobi *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 f *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 rea *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: *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Creating a PKC PMKID Cache entry for statio *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Resetting MSCB PMK Cache Entry 0 for statio *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 cac *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 stati *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_MsgTask_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 ta *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:3 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Freeing AAACB from Dot1xCB as AAA auth is d *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: *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

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r *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 Authenticati *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 int *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: *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

```
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Successfully computed PTK from PMK!!!
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Received valid MIC in EAPOL Key Message M2!
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Not Flex client. Do not distribute PMK Key
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:1
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Ignoring invalid EAPOL-Key from mobile e4:b3:18:7c:
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Reusing invalid EAPOL-Key from mobile e4:b3:18:7c:
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_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: *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_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code qosCap 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 L
*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) 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
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successfully Plumbed PTK session Keysfor mo
*spamApTask2: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require
*apfReceiveTask: Nov 2

```
Peer = 0.0.0.0, 0ld 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 Mobilit;
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6315, Ad
*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) 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 mobi
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 Static IP client associated to interface vlan2404 w
*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)
```

Para una manera fácil de leer los resultados del cliente de depuración, utilice la herramienta Wireless debug analyzer:

Analizador de depuración de errores inalámbrico

Proceso de autenticación en ISE

Navegue hasta Operaciones > RADIUS > Live Logs para ver qué política de autenticación, política de autorización y perfil de autorización se asignó al usuario.

Para obtener más información, haga clic en Details para ver un proceso de autenticación más detallado como se muestra en la imagen.

cisco	Identi	ty Service	s Engine	Home	♦ Context Vi	isibility	•Operations	Policy	• Administrati	tion → V	Vork Centers		License
▼RA	DIUS	TC-NAC Liv	ve Logs	+ TACACS	Reports + Tr	oubleshoot	 Adaptive 	Network Contro	d				
Live I	Logs	Live Sessio	ons										
	Misconfigured Supplicants		ants Mi	Misconfigured Network Devices 🖲		RADIUS Drops 🛛		•	Client Stopped Responding		g Repea		
										Refresh	Never	Show	Latest 20 records
C Refresh ● Reset Repeat Counts A Export To -													
	Time	Sta	Details	Ide	Endpoint ID	Endp	ooint A	uthentication	Policy	Author	rization Policy	y Authoriz	ation Profiles
	No	1	ò	user1	08:74:02:77:13	3:45 Apple	-Device D	efault ≻≻ Rule n	ame ≻> Default	Default	>> NameAuthZr	rule PermitAc	cessVLAN2404

Troubleshoot

Actualmente, no hay información específica disponible sobre cómo solucionar los problemas de esta configuración.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).