Sustitución de WLAN + VLAN 802.1x con Mobility Express (ME) 8.2 e ISE 2.1

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Configurar Diagrama de la red Configuraciones Configuración en ME Declarar ME en ISE Crear un nuevo usuario en ISE Crear la regla de autenticación Crear la regla de autorización Configuración del dispositivo final Verificación Proceso de autenticación en ME Proceso de autenticación en ISE

Introducción

Este documento describe cómo configurar una WLAN (red de área local inalámbrica) con seguridad empresarial Wi-Fi Protected Access 2 (WPA2) con un controlador Mobility Express y un servidor externo Remote Authentication Dial-In User Service (RADIUS). Identity Service Engine (ISE) se utiliza como ejemplo de servidores RADIUS externos.

El protocolo de autenticación extensible (EAP) utilizado en esta guía es el protocolo de autenticación extensible protegido (PEAP). Además, el cliente se asigna a una VLAN específica (distinta de la asignada a la WLAN y a la predeterminada).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- 802.1x
- PEAP
- Autoridad de certificación (CA)
- Certificados

Componentes Utilizados

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

ME v8.2

ISE v2.1

Portátil Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Diagrama de la red



Configuraciones

Los pasos generales son:

- 1. Cree el identificador de conjunto de servicios (SSID) en ME y declare el servidor RADIUS (ISE en este ejemplo) en ME
- 2. Declarar ME en servidor RADIUS (ISE)
- 3. Crear la regla de autenticación en ISE
- 4. Crear la regla de autorización en ISE
- 5. Configurar el terminal

Configuración en ME

Para permitir la comunicación entre el servidor RADIUS y ME, es necesario registrar el servidor RADIUS en ME y viceversa. Este paso muestra cómo registrar el servidor RADIUS en ME.

Paso 1. Abra la GUI de ME y navegue hasta Wireless Settings (Parámetros inalámbricos) >

WLANs > Add new WLAN (WLAN > WLAN > Agregar nueva WLAN).



Paso 2. Seleccione un nombre para la WLAN.

Add N	ew WLAN		×
General	WLAN Security	VLAN & Firewall	QoS
	WLAN Id	3	•
	Profile Name *	me-ise	
	SSID *	me-ise	
	Admin State	Enabled	•
	Radio Policy	ALL	•
		📿 📿 Ap	ply 🛞 Cancel

Paso 3. Especifique la configuración de seguridad en la pestaña Seguridad WLAN.

Elija **WPA2 Enterprise**, para el servidor de autenticación elija **External RADIUS**. Haga clic en la opción edit (editar) para agregar la dirección IP de RADIUS y elegir una clave **secreta compartida**.



Add N	ew WLAN	×
General	WLAN Security	VLAN & Firewall QoS
Auther	Security ntication Server	WPA2 Enterprise • External Radius •
	Radius IP 🔺	Radius Port Shared Secret 1812 •••••••• e enter valid IPv4 address ••••••••
External R all WLANs	adius configuration a	applies to 🛛 📿 Apply 🛞 Cancel

<a.b.c.d> corresponde al servidor RADIUS.

Paso 4. Asigne una VLAN al SSID.

Si el SSID necesita ser asignado a la VLAN del AP, este paso puede ser omitido.

Para asignar los usuarios para este SSID a una VLAN específica (que no sea la VLAN de AP), habilite **Use VLAN Tagging** y asigne el **ID de VLAN** deseado.

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

Nota: Si se utiliza Etiquetado de VLAN, asegúrese de que el puerto de switch al que se conecta el punto de acceso esté configurado como puerto troncal y la VLAN de AP esté configurada como nativa.

Paso 5. Haga clic en Aplicar para finalizar la configuración.

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

Paso 6. Opcional, configure la WLAN para aceptar la invalidación de VLAN.

Habilite la anulación de AAA en la WLAN y agregue las VLAN necesarias. Para ello, deberá abrir una sesión CLI a la interfaz de administración de ME y ejecutar estos comandos:

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

Paso 1. Abra la consola ISE y navegue hasta Administration > Network Resources > Network Devices > Add.

dialo Identity Serv	vices Engine Home	e F Context Visibility	♦ Operations ♦ Po	licy -Administration - Worl
♦ System → Ident	tity Management 🛛 🕶 Netw	rork Resources 🔹 Devi	ce Portal Management p	(Grid Services) Feed Service)
✓ Network Devices	Network Device Groups	Network Device Profile	s External RADIUS Serve	ers RADIUS Server Sequences
	Ø			
Network devices	Ne	twork Devices		
Default Device	1	Edit 🕂 Add 🕞 Duplicat	e 🕵 Import 🚯 Export 👻	Generate PAC XDelete ▼

Paso 2. Introduzca la información.

Opcionalmente se puede especificar un nombre de modelo, una versión de software, una

descripción y asignar grupos de dispositivos de red basados en tipos de dispositivos, ubicación o WLC.

a.b.c.d corresponde a la dirección IP de ME.

Network Devices List > New Network Device Network Devices									
* Name WLC-name									
Description optional description									
* IP Address: a.b.c.d / 32									
* Device Profile 🛛 😹 Cisco 👻 🕀									
Model Name									
Soliware version wic-software 🍷									
* Network Device Group									
Device Type WLCs-2504 📀 Set To Default									
WILCS WILC									
WELCS VIEW Set To Default									
RADIUS Authentication Settings									
Enable Authentication Settings									
Protocol RADIUS									
* Shared Secret Show									
Enable KewWrap									
* Key Encryption Key									
* Message Authenticator Code Key									
Key Input Format ASCII HEXADECIMAL									
COA POR 1700 Set To Default									

Para obtener más información sobre los grupos de dispositivos de red, revise este enlace:

ISE - Grupos de dispositivos de red

Crear un nuevo usuario en ISE

Paso 1. Vaya a Administration > Identity Management > Identities > Users > Add.



Paso 2. Introduzca la información.

En este ejemplo, este usuario pertenece a un grupo denominado ALL_ACCOUNTS, pero se puede ajustar según sea necesario.

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

Crear la regla de autenticación

Las reglas de autenticación se utilizan para verificar si las credenciales de los usuarios son correctas (verifique si el usuario es realmente quien dice ser) y limitar los métodos de

autenticación que puede utilizar.

Paso 1. Navegar a Política > Autenticación.



Paso 2. Inserte una nueva regla de autenticación.

Para hacerlo, navegue hasta Política > Autenticación > Insertar nueva fila arriba/abajo.

al talla cisco	Identity Services Engin	e Home	▶ Context Visibility	Operations	→ Policy	► Administration	▶ Work Centers	L. L.	
Auth	entication Authorization	Profiling Pos	sture Client Provisio	ning 🔹 🕨 Policy Ele	ements				
ting the p System > ed	ing the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. ystem > Backup & Restore > Policy Export Page ed								
_Protocol	: If Wired_MAB OR Is and :use Internal Endpoi	ints						Insert new row above Insert new row below	
IC_Proto	: If Wired_802.1X OR cols and							Duplicate above Duplicate below Delete	

Paso 3. Introduzca la información necesaria

Este ejemplo de regla de autenticación permite todos los protocolos enumerados en la lista **Acceso de red predeterminado**, esto se aplica a la solicitud de autenticación para clientes Wireless 802.1x y con Called-Station-ID y termina con *ise-ssid*.

disclo Identity S	Services Engine	Home	Context Visibility	 Operations 	▼Policy	Administration	♦ Work Center	ers	
Authentication	Authorization	Profiling Postur	e Client Provision	ing 🔹 🕨 Policy Ele	ements				
Authentication	n Policy	alacting the protoco	le that ICE aboutd up	aa ta aammuuniaata	with the net	usely doubless, and the	identity equipage t	that it aboutd upon	for outbontion
For Policy Export (Policy Type	go to Administratic Simple ① Rule	in > System > Backu -Based	ip & Restore > Policy	Export Page	: with the field	vork devices, and the	identity sources t	natit should use	ior autrentica
		_							
	Rule name	: If	Wireless_802.1X	AND Select Attribu		low Protocols : Defa	ult Network Acce	ss 📀	and <u>—</u>
			Add All Con	iditions Below to L	ibrary				
-	Default	: (Js Wireless_80	2.1X 📀 A c	Description	atch 802.1X based a	uthentication req	juest AND) -
			♦ [Radius:Cal	ed-Sta 📀 🛛 End	ls With 👻 ise	ə-ssid	\bigcirc

Además, elija el origen de identidad para los clientes que coincidan con esta regla de autenticación, en este ejemplo se utiliza *Usuarios internos*

Rule name : If Wir	eless_802.1X AND Radius:Call 💠 Allow Protocols : Defau	It Network Access 📀 and .
Default : Use	Internal Users Identity Source Internal Users Options If authentication failed Reject If user not found Reject If process failed Drop 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	Identity Source List
*		DenyAccess Guest Users Guest_Portal_Sequence IdnetitySequence_JUST_Internal Internal Endpoints Internal Users

Cuando haya terminado, haga clic en Finalizado y Guardar

Rule name	If Wireless_802.1X AND Radius:Cal I Allow Protocols : Default Network Access	o and
🛛 🗸 Default	: Use Internal Users 💠	Actions 👻
Save		

Para obtener más información sobre las políticas de permisos de protocolos, consulte este enlace:

Servicio de protocolos permitidos

Para obtener más información sobre las fuentes de identidad, consulte este enlace:

Crear un grupo de identidad de usuario

Crear la regla de autorización

La regla de autorización es la encargada de determinar si el cliente puede o no unirse a la red

Paso 1. Vaya a Política > Autorización.

es Engine	Home) ♦ C	ontext Visibility	Þ	Operations	▼Policy	 Administration 	۰V	Vork Centers
horization	Profiling Po	osture	Client Provision	ing	Policy Ele	Authentic	ation		Authorization
						Profiling			Posture
V Policy by co dministratio plies	onfiguring rules on > System > E	based) Jackup (on identity groups & Restore ≻ Policy	and/ Expo	'or other condi ort Page	Client Pro	ovisioning		Policy Elements Dictionaries Conditions Results

Paso 2. Inserte una nueva regla. Vaya a **Política > Autorización > Insertar Nueva Regla Arriba/Abajo.**

ditalia cisco	Identity Servi	ces Engine	Home	Context Visibility	Operations	* Policy	Administration	Work Centers	License V
Authe	entication Autr	orization Pro	ofiling Postur	e Client Provisioning	Policy Eleme	ents			
figuring ru	les based on ide	ntity groups and	i/or other condi	tions. Drag and drop ru	les to change the	order.			
> System	> Backup & Rest	ore > Policy Exp	ort Page						
*									
		Conditions (ide	ntity groups an	d other conditions)			Permissions		
									Incert New Dule Above
									Insert New Rule Below
									Duplicate Above Duplicate Below

Paso 3. Introduzca la información.

Primero elija un nombre para la regla y los grupos de identidad donde se almacena el usuario. En este ejemplo, el usuario se almacena en el grupo *ALL_ACCOUNTS*.

	Status	Rule Name	Соп	ditions (identity groups and other conditions)	Permissions	
1		NameAuthZrule		Any Pland Condition(s)	then AuthZ Pr	. ¢
	~	75.5	f Vi			
	~	Minetes Thank and deep a	f Ela	Any Ol -+		less Acuma
		Profiled Ciscolary Lauris	f Ci	User Identity Groups	C	s
	~	Francis Mon Cheo (R.Phones	f Nor	↓	•	ગણ્યુલ
	0	Compliant_Devices_Authors	f (the	GuestType_Daily(default) GuestType_Weekly(default)		
	0	Employes JEAP THE	f (114 184	GuestType_Contractor (default)		NE
1	0	Employee Ophoending	f (031	EAP-MSCHAPV2 ALL_ACCOUNTS (default)	07_05/2×1	0.0.9200
	-					

Después de eso, elija otras condiciones que hacen que el proceso de autorización caiga en esta regla. En este ejemplo, el proceso de autorización llega a esta regla si utiliza 802.1x Wireless y se denomina ID de estación termina con *ise-ssid*.

	Status	Rule Name	Conditions (identity groups	and other conditions)	Permissions	
P	~ •	NameAuthZrule	if 🛛 AL 💠 and	Wireless_802.1X AND Radius:Call	😑 then AuthZ Pr 💠	
	2		1	Add All Conditions Below to Library	/	
			٥	Condition Name Des	scription	AND -
	~			Wireless 802.1X 💟 Normalise	ed Radius:RadiusFlowType EQUALS Wireless802_1> adius:Called-Stat	AND
1	<u>~</u>		e			

Finalmente elija el perfil de autorización que permite a los clientes unirse a la red, haga clic en **Finalizado** y **Guardar**.

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

Opcionalmente, cree un nuevo perfil de autorización que asigne al cliente inalámbrico a una VLAN diferente:

•		
(o	
	Standard	
	↓ ■ ↓	ý; ↓
	🚱 Blackhole_Wireless_Access	🎡 Add New Standard Profile

Introduzca la información:

Add New Standard Pro	file		1
Authorization Profile		í	ì.,
* Name	e name-of-profile		
Description			
* Access Type	access_accept		
Network Device Profile	the Cisco 🔹 🕀		
Service Template			
Track Movement			
Passive Identity Tracking	9 D 0		
▼ Common Tasks			
DACL Name		^	
		- 84	
ACL (Filter-ID)			
_			
🗹 VLAN	Tag ID 1 Edit Tag IDName Van-id		
Voice Domain Perm	nission		
		Ŷ	
 Advanced Attribut 	tes Settings		
Select an item			
 Attributes Details 			
Access Type = ACCESS Tunnel-Private-Group-ID Tunnel-Type = 1:13 Tunnel-Medium-Type =	LACEPT D = 1:vbn-id 1:f6		
americanite type -			
C		>	
		Save	ance

Configuración del dispositivo final

Configure un portátil Windows 10 para conectarse a un SSID con autenticación 802.1x mediante PEAP/MS-CHAPv2 (versión de Microsoft del Protocolo de autenticación por desafío mutuo versión 2).

En este ejemplo de configuración, ISE utiliza su certificado autofirmado para realizar la autenticación.

Para crear el perfil WLAN en el equipo de Windows hay dos opciones:

- 1. Instale el certificado autofirmado en el equipo para validar y confiar en el servidor ISE para completar la autenticación
- 2. Omitir la validación del servidor RADIUS y confiar en cualquier servidor RADIUS utilizado para realizar la autenticación (no recomendado, ya que puede convertirse en un problema de seguridad)

La configuración para estas opciones se explica en <u>End device configuration - Create the WLAN</u> <u>Profile - Step 7</u>.

Configuración del dispositivo final: instalación del certificado autofirmado de ISE

Paso 1. Exportar certificado autofirmado de ISE.

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

A continuación, seleccione el certificado utilizado para la **autenticación EAP** y haga clic en **Exportar.**

ില്ലാം Identity Services Eng	gine Home ⊧o	Context Visibility	Operations	Policy + Adr	ninistration 🔹 🕨 Work
	ment 🔹 Network Resou	irces 🔹 🕨 Device F	Portal Management	pxGrid Services	+ Feed Service + F
Deployment Licensing -	Certificates + Logging	 Maintenance 	Upgrade Backup	& Restore 🔹 🕨 A	dmin Access 🔹 🕨 Settir
	G				
 Certificate Management 	System C	ertificates 🛕	For disaster recovery	it is recommended	to export certificate ar
Overview	💋 Edit	🕂 Generate Self :	Signed Certificate	🔓 Import 💽 🗟	Export 🛛 🗙 Delete
System Certificates	Frier	ndly Name	Used By	Portal gro	up tag
Endpoint Certificates	▼ <1212E			_	
Trusted Certificates	AP-S	-SelfSignedCertifica SelfSignedCertifical	ate#E te#00 EAP Authentic	ation	EAI
OCSD Client Brofile					

Guarde el certificado en la ubicación necesaria. Este certificado está instalado en el equipo de Windows.

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	εy.
Export	cel

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

Copie el certificado exportado antes en el equipo de Windows, cambie la extensión del archivo de .pem a .crt, después de hacer doble clic en él y seleccione **Instalar certificado...**.

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

Elija instalarlo en Local Machine y luego haga clic en Next.

🔶 😸 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	
Local Machine	
To continue, click Next.	
Sext Cance	I

Seleccione Colocar todos los certificados en el siguiente almacén y, a continuación, busque y elija Autoridades de certificación raíz de confianza. Después de eso, haga clic en Next.

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

 \sim

A continuación, haga clic en Finalizar.

🗲 🛭 🛃 Certificate Import Wizard	^
Completing the Certificate Import Wizard	
The certificate will be imported after you click Finish.	
You have specified the following settings:	
Certificate Store Selected by User Trusted Root Certification Authorities Content Certificate	
Finish Can	cel

 \sim

Al final, haga clic en Yes para confirmar la instalación del certificado.

Security Warning



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?



Por último, haga clic en Aceptar.



Configuración del dispositivo final: creación del perfil WLAN

Paso 1. Haga clic con el botón derecho del ratón en el icono Inicio y seleccione Panel de control.

	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
ł	ען א Downl א Networ א א א א א א א א א א א א א א א א א א

Paso 2. Navegue hasta Red e Internet y luego Centro de Red y Uso Compartido y haga clic en Configurar una nueva conexión o red.

💐 Network and Sharing Center									
←> -> -> 🛧 💐 > Control Par	nel > Network and Internet > Network and	Sharing Center							
Control Panel Home	View your basic network informat	View your basic network information and set up connections							
Change adapter settings	View your active networks								
Change advanced sharing settings	cisco.com Domain network	Access type: Internet Connections: <i>Iternet</i>							
	Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VP Troubleshoot problems Diagnose and repair network problems	rk Noonnection; or set up a router or access point. lems, or get troubleshooting information.							

Paso 3. Seleccione Manually connect to a wireless network y haga clic en Next.

	_		×
🔶 🛬 Set Up a Connection or Network			
Choose a connection option			
Connect to the Internet			
Set up a broadband or dial-up connection to the Internet.			
👷 Set up a new network			
Set up a new router or access point.			
Manually connect to a wireless network			
Connect to a hidden network or create a new wireless profile.			
Connect to a workplace			
Set up a dial-up or VPN connection to your workplace.			
	Next	Can	cel

Paso 4. Introduzca la información con el nombre del SSID y el tipo de seguridad WPA2-Enterprise y haga clic en **Siguiente**.

				—		×
←	💐 Manually connect to a v	vireless network				
	Enter information for	r the wireless network	you want to add			
	Network name:	ise-ssid				
	Security type:	WPA2-Enterprise	\sim			
	Encryption type:	AES	\sim			
	Security Key:		Hide charac	ters		
	Start this connection	automatically				
	Connect even if the r	network is not broadcasting				
	Warning: If you seled	t this option, your computer's	privacy might be at ri	sk.		
				Next	Cano	cel

Paso 5. Seleccione **Cambiar configuración de conexión** para personalizar la configuración del perfil WLAN.

		—		×
~	💐 Manually connect to a wireless network			
	Successfully added ise-ssid			
	\rightarrow Change connection settings			
	Open the connection properties so that I can change the settings.			
			Clo	5.A
			CIU	50

Paso 6. Vaya a la ficha **Seguridad** y haga clic en **Configuración.**

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)	Settin	gs	
Remember my cre time I'm logged o	edentials for this connec n	tion each		
Advanced settings	;			
	_			
		ОК	Can	cel

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

Si la respuesta es afirmativa, habilite Verificar la identidad del servidor validando el certificado y de Autoridades de certificación raíz de confianza: seleccione el certificado autofirmado de ISE.

Después de seleccionar **Configurar** y deshabilitar **Usar automáticamente mi nombre de inicio de sesión y contraseña de Windows...**, luego haga clic en **Aceptar**

Protected EAP Properties	×								
When connecting:									
Verify the server's identity by validating the certificate									
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):									
Trusted Root Certification Authorities:									
Eggille & Clobel Lines an Eggille & Clobel Lines an Eggille & Clobel Assessment and the exclusion Eggille Assessment and an Eggille Assessment and an	^								
EAP-SelfSignedCertificate									
 Fortunet Royal Configuration, M. Status, C. S. S. L. M. Schultz Configuration of Configuration, Status, Configuration, Configuratio, Configuration, Configuration, Configuration, Configuratio	~								
< >									
Notifications before connecting:									
Tell user if the server name or root certificate isn't specified	~								
Select Authentication Method:	_								
Secured password (EAP-MSCHAP v2) Configu	re								
C Enable Fast Reconnect									
Disconnect if server does not present cryptobinding TLV									
Enable Identity Privacy									
OK Cano	el								

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

Una vez que vuelva a la ficha **Seguridad**, seleccione **Configuración avanzada**, especifique el modo de autenticación como **Autenticación de usuario** y guarde las credenciales configuradas en ISE para autenticar al usuario.

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

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

Windows Secu	irity	×
Save crede Saving your cre when you're ne	ntials edentials allows your computer to connect to the network ot logged on (for example, to download updates).	k
ւլիւվի cisco	user1	
	OK Cancel	

Verificación

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

Proceso de autenticación en ME

Ejecute este comando para supervisar el proceso de autenticación para un usuario específico:

> debug client <mac-add-client>
Ejemplo de una autenticación correcta (se ha omitido alguna salida):

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

AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client *apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is *apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId: 48) *apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3 *apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1 *spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth_sm state transition 0 ---> 1 for mobile 08:74:02:77:13:45 at 1x_reauth_sm.c:47 *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3 is disabled - applying Global eap timers and retries *Dot1x NW MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime. *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800 *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Connecting state *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1) *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: 08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: 08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253 *Dot1x NW MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for station 08:74:02:77:13:45 (RSN 2) *Dot1x NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cache at index 0 for station 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: New PMKID: (16) *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility handoff *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent *Dot1x NW MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can take care of same. *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:13:45 (EAP Id 70) *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: Including PMKID in M1 (16) *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: M1 - Key Data: (22) *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Starting key exchange to mobile

08:74:02:77:13:45, data packets will be dropped *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45 state INITPMK (message 1), replay counter 00.00.00.00.00.00.00 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70) for mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticating state for mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Authenticated state *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-key in PTK_START state (message 2) from mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!! *Dot1x NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!!!!! *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0..... *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 Of *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 *Dot1x NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45 *Dot1x_NW_MsqTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45 state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.00.01 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45 *Dot1x NW MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3) *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce : *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload: *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 255.255.255.224 *Dot1x NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload. *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name: *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change

state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6623, Adding TMP rule *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule

type = Airespace AP - Learn IP address

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

Para obtener una manera fácil de leer los resultados de debug client, utilice la herramienta *Wireless debug analyzer*.

Analizador de depuración inalámbrica

Proceso de autenticación en ISE

Navegue hasta **Operaciones > RADIUS > Registros en directo** para ver qué política de autenticación, política de autorización y perfil de autorización se asignan al usuario.

atoto Iden	tity Services E	ngine	Home	♦ Context V	'isibility 🔫	Operations	Policy P	Administration	• Work Centers		License
▼RADIUS	TC-NAC Live Lo	ogs (TACACS	Reports + Tr	roubleshoot	▶ Adaptive N	Network Control				
Live Logs	Live Sessions										
	Misc	onfigur	ed Supplic	ants Mi	isconfigured Devices	Network O	RADIU	JS Drops 🛛	Client Stoppe	ed Responding 4 Show	Repea
C Refresh ● Reset Repeat Counts A Export To -											
Tim	e Sta De	etails	Ide	Endpoint ID	Endpo	int Au	uthentication Po	olicy	Authorization Policy	Authoriza	tion Profiles
No	0	ò	user1	08:74:02:77:13	3:45 Apple-E	evice De	efault >> Rule name	e >> Default	Default >> NameAuthZrul	e PermitAcce	:85

Para obtener más información, haga clic en **Detalles** para ver un proceso de autenticación más detallado.