# Configurar RADIUS & TACACS+ para GUI & CLI Auth en WLC 9800

## Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configurar
Restricciones de usuario de sólo lectura
Configuración de la Autenticación RADIUS para el WLC
Configuración de ISE para RADIUS
Configuración de TACACS+ WLC
Configuración de ISE de TACACS+
Troubleshoot
Resolución de problemasAcceso RADIUS/TACACS+ CLI o GUI WLC a través de WLC CLI
Resolución de problemasWLC GUI o CLITACACS+ Acceso a través de la GUI de ISE

# Introducción

Este documento describe cómo configurar un Catalyst 9800 para la autenticación externa RADIUS o TACACS+.

### Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Modelo de configuración de Catalyst Wireless 9800
- Conceptos AAA, RADIUS y TACACS+

### **Componentes Utilizados**

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

- C9800-CL v17.9.2
- ISE 3.2.0

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 un usuario intenta acceder a la CLI o a la GUI del WLC, se le pide que ingrese un nombre de usuario y una contraseña. De forma predeterminada, estas credenciales se comparan con la base de datos local de usuarios, que está presente en el propio dispositivo. Alternativamente, el WLC se puede instruir para comparar las credenciales de entrada contra un servidor AAA remoto: el WLC puede hablar con el servidor con el uso de RADIUS o TACACS+.

# Configurar

### En este ejemplo, se configuran dos tipos de usuarios en el servidor AAA (ISE), respectivamente

adminuser, yhelpdeskuser. Estos usuarios forman parte de admin-group y de los helpdesk-group grupos respectivamente. Se espera que el usuario adminuser, parte deladmin-group, tenga acceso completo al WLC. Por otro lado, el helpdeskuser, parte del helpdesk-group, está destinado a ser concedido solamente privilegios del monitor al WLC. Por lo tanto, no hay acceso a la configuración.

Este artículo primero configura el WLC e ISE para la autenticación RADIUS y luego realiza lo mismo para TACACS+.

Restricciones de usuario de sólo lectura

Cuando se utiliza TACACS+ o RADIUS para la autenticación 9800 WebUI, existen estas restricciones:

- Los usuarios con nivel de privilegio 0 existen pero no tienen acceso a la GUI
- Los usuarios con niveles de privilegio 1-14 sólo pueden ver la ficha Monitor (esto equivale al nivel de privilegio de un usuario autenticado localmente de sólo lectura)
- Los usuarios con el nivel de privilegio 15 tienen acceso completo

No se admiten los usuarios con el nivel de privilegio 15 y un conjunto de comandos que sólo permite comandos específicos. El usuario todavía puede ejecutar los cambios de configuración a través de la interfaz de usuario Web

#### Configuración de la Autenticación RADIUS para el WLC

#### Paso 1. Declare el servidor RADIUS.

#### Desde la GUI:

En primer lugar, cree el servidor RADIUS de ISE en el WLC. Esto se puede hacer desde la pestaña Servers/Groups > RADIUS > Servers de la página GUI WLC accesible en https://<WLC-IP>/webui/#/aaa, o si navega a Configuration > Security > AAA, como se muestra en esta imagen.

Q Search Menu Items	Configuration • > Security	• > AAA				
bee Dashboard	+ AAA Wizard	Method List AAA Advanced				
Monitoring →	+ Add × Delete					
Configuration >	RADIUS	Servers Server Groups				
C Licensing	TACACS+	Name	▼ Address	Y Auth Port	Y Acct Port Y	
X Troubleshooting	LDAP	□ ISE-lab	10.48.39.134	1812	1813 1 - 1 of 1 items	
		For Radius Fallback to work, please mak	e sure the Dead Criteria and D	lead Time configuration exists on	the device	
Walk Me Through >						

Para agregar un servidor RADIUS en el WLC, haga clic en el botón Add enmarcado en rojo en la imagen. Se abrirá la ventana emergente que se muestra en la captura de pantalla.

Q Search Menu Items	Configuration • >	Security - > AAA				
	Create AAA Radius Server				×	
Dashboard	Name*	ISE-lab	Support for CoA (i)	ENABLED		
Monitoring	Server Address*	10.48.39.134	CoA Server Key Type	Clear Text 🔻	)	
Real Configuration	PAC Key	0	CoA Server Key (i)		]	
() Administration	Кеу Туре	Clear Text 👻	Confirm CoA Server Key		]	
C Licensing	Key* (i)		Automate Tester	0		T
X Troubleshooting	Confirm Key*					items to display
	Auth Port	1812				
	Acct Port	1813				
Walk Me Through >	Server Timeout (seconds)	1-1000				
	Retry Count	0-100				
	Capcel					
					Apply to Device	
	Cancel			I	Apply to Device	

En esta ventana emergente, debe proporcionar:

- El nombre del servidor (tenga en cuenta que no tiene que coincidir con el nombre del sistema de ISE)
- La dirección IP del servidor
- El secreto compartido entre el WLC y el servidor RADIUS

Se pueden configurar otros parámetros, como los puertos utilizados para la autenticación y la administración de cuentas, pero no son obligatorios y se dejan como predeterminados para esta documentación.

Desde CLI:

#### <#root>

WLC-9800(config)#radius server

#### ISE-lab

WLC-9800(config-radius-server)#address ipv4

10.48.39.134

auth-port 1812 acct-port 1813
WLC-9800(config-radius-server)#key

Ciscol23

Paso 2. Asigne el servidor RADIUS a un grupo de servidores.

#### Desde la GUI:

En caso de que tenga varios servidores RADIUS que se puedan utilizar para la autenticación, se recomienda asignar todos estos servidores al mismo grupo de servidores. El WLC se ocupa del balanceo de carga de las diferentes autenticaciones entre los servidores en el grupo de servidores. Los grupos de servidores RADIUS se configuran desde la Servers/Groups > RADIUS > Server Groups pestaña desde la misma página GUI que la mencionada en el Paso 1, como se muestra en la imagen.

Q Search Menu Items	Configuration • > Security	- > AAA			
Dashboard	+ AAA Wizard				
Monitoring →	+ Add × Delete	Method List AAA Advanced			
Configuration	RADIUS	Servers Server Groups			
© Licensing	TACACS+	Name	Y Server 1	Server 2	Server 3
X Troubleshooting	LDAP	RADIUS-Group	ISE-lab	N/A	N/A 1 - 1 of 1 items
Walk Me Through >					

En cuanto a la creación del servidor, aparece una ventana emergente al hacer clic en el botón Agregar (enmarcado en la imagen anterior), que se muestra aquí.

Q Search Menu Items	Configu	uration * > Security * > AAA Create AAA Radius Server (	Group	
Dashboard	+ 44	Name*	RADIUS-Group	
Monitoring	> Server	Group Type	RADIUS	
	>	MAC-Delimiter	none	
O Administration		MAC-Filtering	none	
C Licensing	TAC	Dead-Time (mins)	5	Server 3
Troubleshooting	LD/	Load Balance	DISABLED	No items to display
879 		Source Interface VLAN ID	1 🗸	
		Available Servers	Assigned Servers	
Walk Me Through 2			>     ISE-lab     A         A       >      ×         ×	
		Cancel		Apply to Device

En la ventana emergente, proporcione un nombre al grupo y mueva los servidores deseados a la lista Servidores asignados.

Desde CLI:

<#root>

.....

#### WLC-9800(config)# aaa group server radius

#### RADIUS-Group

WLC-9800(config-sg-radius)# server name

#### <u>ISE-lab</u>

\_

Paso 3. Cree un método de inicio de sesión de autenticación AAA que apunte al grupo de servidores RADIUS.

#### Desde la GUI:

Desde la página GUIhttps://<WLC-IP>/webui/#/aaa, navegue hasta la AAA Method List > Authentication pestaña y cree un método de autenticación como se muestra en esta imagen.



Como es habitual, cuando utiliza el botón Add (Agregar) para crear un método de autenticación, aparece una ventana emergente de configuración, similar a la que se muestra en esta imagen.

Q Search Menu Items	Configuration * > Security * > AAA				
Dashboard	+ AAA Wizard Quick Setup: AAA Authenti	ication			
Monitoring >	Method List Name*	radius-authe-method			
Configuration >	Type*	login 🔹			
O Administration	Group Type			Group?	Ground
C Licensing	Available Server Groups	Assigned Server Groups		N/A	N/A
X Troubleshooting	radius Idap tacacs+	>     RADIUS-Group           %	× × ×		
Walk Me Through >	ී Cancel		Apply to Device		

En esta ventana emergente, proporcione un nombre para el método. Elija Type como conexión y agregue el servidor de grupos creado en el paso anterior a la Assigned Server Groups lista. Con respecto al campo Tipo de grupo, son posibles varias configuraciones.

• Si elige el tipo de grupo como local, el WLC primero verifica si las credenciales del usuario existen localmente y después vuelve al grupo del servidor.

• Si elige el tipo de grupo como grupo y no marca la opción Volver a local, el WLC verifica solamente las credenciales del usuario contra el grupo del servidor.

• Si elige Group Type como grupo y marca la opción Fallback to local, el WLC verifica las credenciales del usuario contra el grupo del servidor y consulta la base de datos local solamente si el servidor no responde. Si el servidor envía un rechazo, el usuario se autenticará, aunque pueda existir en la base de datos local.

Desde CLI:

Si desea que las credenciales de usuario se comprueben con un grupo de servidores sólo si no se encuentran primero localmente, utilice:

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

local group

RADIUS-Group

Si desea que las credenciales de usuario se comprueben sólo con un grupo de servidores, utilice:

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

group

RADIUS-Group

Si desea que las credenciales de usuario se comprueben con un grupo de servidores y si esta última no responde con una entrada local, utilice:

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

group

RADIUS-Group

local

En este ejemplo de configuración, hay algunos usuarios que solo se crean localmente y algunos usuarios solo en el servidor ISE, por lo tanto, hacen uso de la primera opción.

Paso 4. Cree un método de ejecución de autorización AAA que apunte al grupo de servidores RADIUS.

#### Desde la GUI:

El usuario también debe estar autorizado para que se le conceda acceso. En la GUI Page Configuration > Security > AAA, vaya a la AAA Method List > Authorization ficha y cree un método de autorización como se muestra en esta imagen.



Creación del método de autorización

Una ventana emergente de configuración de método de autorización similar a la representada aparece cuando se agrega una nueva con el botón Add (Agregar).

Q Search Menu Items	Config	uration * > Security * > AAA			
Dashboard	+ 44	Quick Setup: AAA Authoriz	ation		
	> Server	Method List Name*	radius-autho-method		
	Aut	t Type*	exec v		
	Au	Group Type		▼ Group3 ▼	Group4
© Licensing	Ac	Authenticated Available Server Groups	Assigned Server Groups	N/A	N/A
💥 Troubleshooting		radius Idap tacacs+	RADIUS-Group <ul> <li></li></ul>		
		Cancel	Apply to Device		

En esta ventana emergente de configuración, proporcione un nombre para el método de autorización, elija el Tipo como exec y utilice el mismo orden de Tipo de grupo que el utilizado para el método de autenticación en el Paso 3.

#### Desde CLI:

En cuanto al método de autenticación, la autorización se asigna primero para comprobar los usuarios con las entradas locales y, a continuación, con las entradas de un grupo de servidores.

<#root>

WLC-9800(config)#aaa authorization exec

radius-autho-method

local group

RADIUS-Group

Paso 5. Asigne los métodos a las configuraciones HTTP y a las líneas VTY utilizadas para Telnet/SSH.

#### Desde la GUI:

Los métodos de autenticación y autorización creados se pueden utilizar para la conexión de usuario HTTP y/o Telnet/SSH, que se puede configurar desde la AAA Advanced > AAA Interface pestaña todavía desde la página WLC de GUI accesible en https://<WLC-IP>/webui/#/aaa, como se muestra en esta imagen:

Q Search Menu Items	Configuration * > Sec	urity * > AAA			
Dashboard	+ AAA Wizard				
	Servers / Groups A	AA Method List	anced		
	Global Config				🖺 Apply
O Administration	RADIUS Fallback		Authentication	Authorization	Accounting
C Licensing	Attribute List Name	Console	None 👻 💈	None 👻 💈	None 👻 🗹
	Device Authentication	VTY	radius-authe-method -	radius-autho-method 🗸 🛛	None 🔻 💈
9 <b>.</b> 0	AP Policy	НТТР	radius-authe-method 🗸 💈	radius-autho-method 🗸 💈	None 🔻 🗹
	Password Policy				
Walk Me Through >	AAA Interface				

CLI para autenticación GUI:

<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

radius-authe-method

WLC-9800(config)#ip http authentication aaa exec-authorization

radius-autho-method

CLI para autenticación Telnet/SSH:

<#root>

WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication

radius-authe-method

WLC-9800(config-line)#authorization exec

radius-autho-method

Tenga en cuenta que cuando se realizan cambios en las configuraciones HTTP, es mejor reiniciar los servicios HTTP y HTTPS. Esto se puede lograr con estos comandos:

WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-server WLC-9800(config)#ip http s

Configuración de ISE para RADIUS

Paso 1. Configure el WLC como un dispositivo de red para RADIUS.

Desde la GUI:

Para declarar el WLC utilizado en la sección anterior como un dispositivo de red para RADIUS en ISE, navegue hasta Administration > Network Ressources > Network Devices y abra la ficha Network devices (Dispositivos de red), como se muestra en la siguiente imagen.

<b>≡ Cisco</b> ISE		Administratio	n · Network Resources	5	A Evaluation	Mode 82 Days Q 🕜 🕫 🕸
Network Devices	Network Device Gro	ups Network Device Pr	ofiles External RAD	IUS Servers RADIUS	Server Sequences	More ~
Network Devices	Netw	work Devices				
Default Device Device Security Settings	Netv	VOIR Devices				Colored & Total 1 City
	🖉 Edit	+ Add Duplicate	j Import 🏦 Export 🗸	🖰 Generate PAC 🍵 Dele	te $\vee$	All V
		Name $\land$ IP/Mask	Profile Name	Location	Туре	Description
		WLC-9800 10.48.39.133	/32 🗰 Cisco 🕕	All Locations	All Device Types	

Para agregar un dispositivo de red, utilice el botón Add (Agregar), que abre el formulario de configuración del nuevo dispositivo de red.

	Administration · Netw	ork Resources		A	Evaluation Mode 82 Days	Q	0	50	٩
Device Groups	Network Device Profiles	External RADIUS Se	ervers RAD	IUS Server Sequen	ices More $\vee$				
Network Devices List	> New Network Device								
Name	WLC-9800								
Description									
IP Address	* IP : 10.48.39.13	33 <sup>/</sup> 32 🕸							
Device Profile	atta Cisco	× ()							
Model Name		~							
Software Version	1	~							
Network Device	Group								
Location	All Locations	✓ Se	at To Default						
IPSEC	Is IPSEC Device	✓ Se	et To Default						
Device Type	All Device Types	∽ Se	et To Default						
🗹 🗸 RADIL	JS Authentication Setting	IS							
RADIUS I	JDP Settings								
Protocol	RADIUS								
Shared Se		s	show						
Use Se	econd Shared Secret 🕕								
	Second Shared Secret			Show					
CoA Port	1700	S	Set To Default						
RADIUS [	OTLS Settings 🕕								
	Required (i)								
Shared Se	cret radius/dtls	(	D						
	Device Groups  Network Devices List Network Devices Name Description  E Povice Profile Model Name Software Version Network Device Location IPSEC Device Type  V RADIUS RADIUS I Shared Se CoA Port RADIUS I Shared Se Shared Se	Administration - Network         Device Groups       Network Device Profiles         Network Devices List > New Network Device         Network Devices List > New Network Device         Name       WLC-9800         Description	Administration - Network Resources   Device Groups Network Device Profiles   External RADIUS Setings   Name WLC-9800   Description     Image: Inplace Profile   Image: Inplace Profi	Administration - Network Resources     RAD       Device Groups     Network Device Profiles     External RADIUS Servers     RAD       Network Devices     Network Devices     Network Devices     Network Devices       Name     WLC-9800	Administration - Network Resources     A       Device Groups     Network Device Profiles     External RADIUS Servers     RADIUS Server Sequent       Network Devices     Name	Administration - Network Resources RADIUS Server Sequences More ~  Petreors Devices List -> New Network Device Network Devices Network Devices  Network Devices  Network Devices  Network Devices  Network Devices  Network Device frolls  Device Prolite  Device Prolite  Device Prolite  Device Group  Location All Locations  V Set To Default  Device Type All Device Types V Set To Default  Device Type All Device Types Set To Default  CoA Port 1700 Set To Default  RADIUS DTLS Settings Device CoA Port 1700 Set To Default  CoA Port 170 Set To Default  C	Administration - Network Resources ADUS Servers RADIUS Server Sequences More  Pavice Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences More  Network Devices Lat > New Network Device  Network Device Uers	Administration - Network Resources RADIUS Server Sequences More >  Perice Groups Network Device Profiles External RADIUS Server RADIUS Server Sequences More >  Network Devices  Network Devices  Network Devices  Network Devices  Network Devices  Network Devices  Network Device Type: 10.48.39.133 / 32  Device Profile  Coico  All Locations  All Locations  All Device Types  All Device Types  All Device Types  Set To Default  Perice I RADIUS Authentication Settings  Protocol  RADIUS Authentication Settings  Protocol  RADIUS Authentication Settings  Protocol  RADIUS TLS Settings  Protocol  RADIUS  RADIUS TLS Settings  Protocol  RADIUS  RA	Administration - Network Resources ADUUS Server Sequences More            Device Groups         Network Device           Network Devices         Network Device           Network Devices         Network Device           Image: Server Sequences         More            Network Devices         Network Device           Network Devices         Network Devices           Image: Network Device         Network Devices           Device Profile         Image: Network Device           Image: Network Devices         Network Devices           Device Profile         Image: Network Device           Image: Network Device         Image: Network Device           Software Version         Image: Network Device           Network Device Group         Locations           Location         All Locations           Image: Network Device         Set To Default           IPSEC         Image: Network Device           Image: Network Device         Set To Default           IPSEC         RADIUS Authentication Settings           Protocol         RADIUS           Second Shared Secret         Second Shared Secret           Second Shared Secret         Set To Default           Device Type         Secret           Secret         Secret

En la nueva ventana, proporcione un nombre para el dispositivo de red y agregue su dirección IP. Elija los ajustes de autenticación de RADIUS y configure el mismo secreto compartido de RADIUS que el que se utiliza en el WLC.

Paso 2. Cree un resultado de autorización para devolver el privilegio.

#### Desde la GUI:

Para tener derechos de acceso de administrador, el adminuser necesita tener un nivel de privilegio de 15, que permite acceder al intérprete de comandos exec. Por otro lado, el helpdeskuser no necesita acceso al shell exec prompt y, por lo tanto, se puede asignar con un nivel de privilegio inferior a 15. Para asignar el nivel de privilegio adecuado a los usuarios, se pueden utilizar perfiles de autorización. Estos se pueden configurar desde la ISE GUI Page Policy > Policy Elements > Results, en la pestaña Authorization > Authorization Profiles que se muestra en la siguiente imagen.

≡ Cisco ISE			Policy	Policy Elements	A Evaluation Mode 82 Days Q 🔿 👼	0 ¢
Dictionaries Cor	nditions	Results				
Authentication Authorization Authorization Profiles Downloadable ACLs	>	Star For Policy	+ Add Duplicate	Zation Profiles - System > Backup & Restore > Policy Expo Delete	oort Page Selected 0 Total 11 ♀ All ∨	\$ 7
Profiling	>		Name	Profile	∧ Description	
Posture	>		9800-admin-priv	🗰 Cisco 👔		
Client Provisioning	>		9800-helpdesk-priv	🚓 Cisco 🧃		
			Block_Wireless_Access	🗱 Cisco 🕧	Default profile used to block wireless devices. Ensure	e ti
			Cisco_IP_Phones	🗰 Cisco 🧻	Default profile used for Cisco Phones.	
			Cisco_Temporal_Onboard	🚓 Cisco 🧃	Onboard the device with Cisco temporal agent	
			Cisco_WebAuth	🗰 Cisco  (i)	Default Profile used to redirect users to the CWA por	rtal
			NSP_Onboard	🗰 Cisco 🧃	Onboard the device with Native Supplicant Provisioni	ing
			Non_Cisco_IP_Phones	att Cisco 🕦	Default Profile used for Non Cisco Phones.	
			UDN	🗰 Cisco 🧻	Default profile used for UDN.	
			DenyAccess		Default Profile with access type as Access-Reject	
		-				

Para configurar un nuevo perfil de autorización, utilice el botón Agregar, que abre el formulario de configuración del nuevo perfil de autorización. Este formulario debe ser especialmente similar a este para configurar el perfil que se asigna a adminuser.

=	Cieco	ISE
_	CISCU	1 JL

Policy · Policy Elements

Dictionaries Conditions	Results
Authentication >	Authorization Profiles > New Authorization Profile
Authorization $\sim$	Authorization Profile
Authorization Profiles	* Name 9800-admin-priv
Downloadable ACLs	
Profiling >	Description
Posture >	* Access Type ACCESS_ACCEPT ~
Client Provisioning >	Network Device Profile 📾 Cisco 🗸 🕀
	Service Template
	Track Movement
	Agentless Posture
	Passive Identity Tracking 🗌 🕕
	> Common Tasks
	✓ Advanced Attributes Settings
	ii Cisco:cisco-av-pair v shell:priv-lvl=15 v - +
	✓ Attributes Details
	Access Type = ACCESS_ACCEPT clsco-av-pair = shell:priv-tvl=15
	Submit Cancel

La configuración mostró el nivel de privilegio de concesiones 15 a cualquier usuario al que esté asociado. Como se ha mencionado anteriormente, este es el comportamiento esperado para el adminuser que se crea durante el paso siguiente. Sin embargo, el helpdeskuser debe tener un nivel de privilegio inferior y, por lo tanto, debe crearse un segundo elemento de política.

El elemento de directiva para el helpdeskuser es similar al creado justo encima, excepto que la cadena shell:priv-lvl=15 debe cambiarse a shell:priv-lvl=X y reemplazar X con el nivel de privilegio deseado. En este ejemplo, se utiliza 1.

Paso 3. Cree grupos de usuarios en ISE.

Desde la GUI:

Los grupos de usuarios de ISE se crean en la ficha Grupos de identidades de usuario de Administration > Identity Management > Groups GUI Page, que se muestra en la captura de pantalla.

■ Cisco ISE		Administration · Identity Manag	gement	▲ Evaluation Mode 82 Days Q (	0 59	)
Identities Groups External Ide	ntity Sour	es Identity Source Sequences	Settings			
Identity Groups EQ C TE © D Endpoint Identity Groups	Use	r Identity Groups + Add 🔋 Delete 🗸 🅁 Import	▲ Export ∨	Selected 0 Total 1	0 <i>C</i> All ~	@ 又
> 🗂 User Identity Groups		Name ~	Description			
		A helpdesk-group	This is the group containing all users with read	d-only privileges.		
		😤 admin-group	This is the group containing all users with adm	ninistrator privileges.		
		MOWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group	p		
		A GuestType_Weekly (default)	Identity group mirroring the guest type			
		SuestType_SocialLogin (default)	Identity group mirroring the guest type			
		SuestType_Daily (default)	Identity group mirroring the guest type			
		SuestType_Contractor (default)	Identity group mirroring the guest type			
		Market GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Gro	oup		
		A Employee	Default Employee User Group			
		ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group			

Para crear un nuevo usuario, utilice el botón Agregar, que abre el formulario de configuración del nuevo grupo de identidades de usuario como se muestra.

=	Cisc	O ISE		4	Administration · Identity Man	agement			A Evaluation Mode 82 Days	Q	0	P	٩
Ide	ntities	Groups	External Ide	entity Sources	Identity Source Sequences	Settings							
1	dentity (	Groups Endpoint Iden User Identity (	¢ tity Groups Groups	User Identity Grou Identity Grou * Name Description	ups > New User Identity Group JP admin-group This is the group containing all users with ad	ministrator privileges.	Submit	Cancel					

Proporcione el nombre del grupo que se ha creado. Cree los dos grupos de usuarios mencionados anteriormente, a saber, admin-group y helpdesk-group.

Paso 4. Cree usuarios en ISE.

Desde la GUI:

Los usuarios de ISE se crean en la ficha Users of the Administration > Identity Management > Identities GUI Page (Usuarios de), que se muestra en la captura de pantalla.

≡ Cisco ISE	Administration - Identity Management	🛕 Evaluation Mode 82 Days 📿 ⊘ 🕫 🅸
Identities Groups External Identity Sources	Identity Source Sequences Settings	
Users Network Scan Res	ccess Users	
🖉 Edit 🕇 Add	🛞 Change Status 🗸 🕁 Import 🛧 Export 🗸 👩 Delete 🗸 🚺 Duplica	Selected 0 Total 2 🔁 🔕
Status	Username $\land$ Description First Name Last Name Email Addres	s User Identity Groups Admin
🗌 🛛 🖸 Enabled	2 adminuser	admin-group
🗌 🛛 🖸 Enabled	2 helpdeskus	helpdesk-group

Para crear un nuevo usuario, utilice el botón Add (Agregar) para abrir el nuevo formulario de configuración de usuario de acceso a la red, como se muestra.

■ Cisco ISE	Administration · Identity Management	🛕 Evaluation Mode 82 Days Q 🔿 🖓
Identities Groups Ex	xternal Identity Sources Identity Source Sequences Settings	
sers atest Manual Network Scan Res	Network Access Users List > New Network Access User	
	✓ Network Access User	
	* Username adminuser	
	Status Zenabled V	
	Account Name Alias	
	Email	
	✓ Passwords	
	Password Type: Internal Users V	
	Password Lifetime: With Expiration Password will expire in <b>60 days</b> Never Expires Password Re-Enter Password	
	* Login Password ·····	Generate Password (i)
	Enable Password	Generate Password ()
	> User Information	
	> Account Options	
	Account Dirable Policy	
	/ Account Disable Policy	
	<ul> <li>V User Groups</li> </ul>	

Proporcione las credenciales a los usuarios, a saber, su nombre de usuario y contraseña, que son los que se utilizan para autenticar en el WLC. Además, asegúrese de que el estado del usuario es Enabled. Por último, agregue el usuario a su grupo relacionado, que se ha creado en el paso 4, con el menú desplegable Grupos de usuarios al final del formulario.

Cree los dos usuarios mencionados anteriormente, a saber, el adminuser y helpdeskuser.

Paso 5. Autentique a los usuarios.

#### Desde la GUI:

En esta situación, la política de autenticación de los conjuntos de políticas predeterminados de ISE, que ya está preconfigurada, permite el acceso a la red predeterminado. Este conjunto de políticas se puede ver en la páginaPolicy > Policy Sets de la GUI de ISE, como se muestra en esta imagen. Por lo tanto, no hay necesidad de cambiarlo.

≡	Cisco IS	E		Policy · Policy Sets	· · · · · · · · · · · · · · · · · · ·	Levaluation Mode 82 Days	0 7	0 ¢
Poli	cy Sets→	Default			Reset	Reset Policyset Hitcounts	Sa	ve
	Status Po	blicy Set Name De	escripti	tion Conditions		Allowed Protocols / Server Se	quence	Hits
	Q Search							
	0	Default	Default	t policy set		Default Network Access 🛛	a ∼+	0
$\sim$	Authenticatio	n Policy (3)						
(	+ Status	Rule Name	Cond	ditions	Use	н	its Acti	ions
	Q Search							
				. Wired_MAB	Internal En	dpoints 🛛 🗸		
		MAB	OR	E Wireless_MAB	> Option:	5	₽ <u>₹</u> Ç	3
				Wired_802.1X	All_User_I	D_Stores 🛛 🗸		
	0	Dot1X	OR	Wireless_802.1X	> Option:	ŝ	• {ô	\$
Г			-		All_User_I	D_Stores 🛛 🗸	-	٦
	ø	Default			> Option	5	¢} ø	3

#### Paso 6. Autorizar a los usuarios.

#### Desde la GUI:

Una vez que el intento de inicio de sesión supera la política de autenticación, debe estar autorizado e ISE debe devolver el perfil de autorización creado anteriormente (aceptación de permiso, junto con el nivel de privilegio).

En este ejemplo, los intentos de inicio de sesión se filtran en función de la dirección IP del dispositivo (que es la dirección IP del WLC) y distinguen el nivel de privilegio que se otorgará en función del grupo al que pertenece un usuario. Otro enfoque válido es filtrar los usuarios en función de sus nombres de usuario, ya que cada grupo solo contiene un usuario en este ejemplo.

E			Policy · Policy S	Sets		🔺 Ev	raluation Mode 82 Days	Q (2)	9
Default						Reset	set Policyset Hitcounts		Save
licy Set Name	Descript	ion	Conditions			Allow	ved Protocols / Serve	Seque	nce H
Default	Default	policy :	et			Defa	ult Network Access	× ~	+ 19
Policy (3)									
Policy - Local Exception	S								
Policy - Global Exception	ns (2)								
				Results					
Rule Name	Cond	litions		Profiles		Security Groups		Hits	Actio
		₽	Network Access-Device IP Address EQUALS 10.48.39.133	0000 beledesk astron		Coloct from lice			~
9800 Helpdesk Osers	AND	8	InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	9800-neipdesk-priv ×	+	Select from list		ľ	£Č3
9900 Admin Linera		₽	Network Access-Device IP Address EQUALS 10.48.39.133		~ +	Select from list			527
Soco Admin Osers	-	0	InternalUser-IdentityGroup EQUALS User Identity	Sood-admin-priv X					202
	Default IICY Set Name Default Default Default Policy (3) Policy - Local Exception Policy - Global Exception Rule Name 9800 Helpdesk Users 9800 Helpdesk Users	Default     Descript       Ilcy Set Name     Descript       Default     Default       Default     Default       Policy (3)     Policy - Local Exceptions       Policy - Global Exceptions (2)     Image: Condition of the second se	Icy Set Name     Description       Iley Set Name     Default       Default     Default policy s       Default     Default policy s       Policy (3)     Policy - Local Exceptions (2)       Policy - Global Exceptions (2)     Image: Conditions       Rule Name     Conditions       9800 Helpdesk Users     AND       9800 Admin Lisers     AND	Default       Description       Conditions         Icy Set Name       Description       Conditions         Default       Default policy set       Image: Conditions         Policy (3)       Policy - Local Exceptions (2)       Image: Conditions         Policy - Global Exceptions (2)       Image: Conditions       Image: Conditions         B800 Helpdesk Users       AND       Image: Condition Conditions         B800 Helpdesk Users       AND       Image: Condition Condition Conditions         B800 Helpdesk Users       AND       Image: Condition Condition Condition Conditions	Default       Description       Conditions         Default       Default policy set       Image: Conditions         Default       Default policy set       Image: Conditions         Policy (3)       Policy - Local Exceptions       Image: Conditions         Policy - Global Exceptions (2)       Image: Conditions       Image: Conditions         Policy - Global Exceptions (2)       Image: Conditions       Image: Conditions         Performance       Image: Conditions       Image: Conditions       Image: Conditions         Performance       Image: Conditions       Image: Conditions       Image: Conditions       Image: Conditions         Performance       Image: Conditions       Image: Conditions       Image: Conditions       Image: Conditions       Image: Conditions         Performance       Image: Conditions       Image: Conditions       Image: Conditions       Image: Conditions       Image: Conditions         Performance       Image: Conditions       Image: Conditions       Image: Conditions       Image: Conditions       Image: Conditions         Performance       Image: Conditions       Image: Conditions       Image: Conditions       Image: Conditions       Image: Conditions         Performance       Image: Conditions       Image: Conditions       Image: Conditions       Image: Conditions	Default       Description       Conditions         Default       Default policy set	Default     Reset     Reset       Ilcy Set Name     Description     Conditions     Allow       Default     Default policy set     Default     Default       Policy (3)     Policy - Local Exceptions     Policy - Global Exceptions (2)     Results       Rule Name     Conditions     Profiles     Security Groups       9800 Helipdesk Users     AND     Retwork Access-Device IP Address     9800-helipdesk-priv × · · +     Select from list       9800 helipdesk Users     AND     Retwork Access-Device IP Address     9800-helipdesk-priv × · · +     Select from list	Default       Reset       Reset Policyset Hitcounts         Itery Set Name       Description       Conditions       Allowed Protocols / Server         Default       Default policy set       Default Network Access       Default Network Access         Default       Default policy set       Default Network Access       Default Network Access         Policy (3)       Policy - Local Exceptions (2)       Results       Policy (3)         Rule Name       Conditions       Results       Security Groups         9800 Helpdesk Users       AND       Retwork Access Device IP Address EQUALS 10.48.39.133 R EQUALS 10.48.39.133       9800-helpdesk-priv × · +       Select from list · · +         9800 Admin Liners       AND       Retwork Access Device IP Address EQUALS 10.48.39.133       9800-admin-priv × · +       Select from list · · · +	Default       Reset       Reset <threset< th=""> <t< td=""></t<></threset<>

Después de que este paso se haya completado, las credenciales configuradas para adminuser y helpdesk usuario se pueden utilizar para autenticar en el WLC vía la GUI o a través de Telnet/SSH.

Configuración de TACACS+ WLC

Paso 1. Declare el servidor TACACS+.

Desde la GUI:

En primer lugar, cree el ISE del servidor Tacacs+ en el WLC. Esto se puede hacer desde la pestaña Servers/Groups > TACACS+ > Servers de la página GUI WLC accesible en el <u>https://<WLC-IP>/webui/#/aaa.</u> o si navega a Configuration > Security > AAA, como se muestra en esta imagen.

Reset

Cisco Catalyst	t 9800-CL Wireless Controller	Welcome admin & 🕷 🔹 🛕	🖺 🏟 🖗 📿 Search APs	and Clients Q
Q. Search Menu Items     Image: Configuration items       Image: Configuration items     Image: Configuration items       Image: Configuration items     Image: Configuration items	Configuration * > Security * > AAA + AAA Wizard Servers / Groups AAA Method List + Add × Delete RADIUS Servers	t AAA Advanced Server Groups		
<ul> <li>Licensing</li> <li>Troubleshooting</li> </ul>	LDAP	Name	Server Address 10.48.39.134	Y         Port         Y           49         1 - 1 of 1 items
Walk Me Through 3				

Para agregar un servidor TACACS en el WLC, haga clic en el botón Add enmarcado en rojo en la imagen de arriba. Se abrirá la ventana emergente representada.

Cisco Cisco	o Cata	alyst 9800-CL	Wireless Controll	er Welcome admin		irch APs and Clients
				Last login 12/07/2022 14:14:33		
Q Search Menu Items		Configuration •	Security * > AA	A		
Dashboard		+ AAA Wizard	Create AAA Tacad	cs Server		
Monitoring	>	Servers / Grou	Name*	ISE-lab		
	>	+ Add	Server Address*	10.48.39.134		
O Administration	>	RADIUS	Кеу Туре	Clear Text 🗸		
C Licensing		TACACS+	Key*			T Port
K Troubleshooting		LDAP	Confirm Key*			No items to display
			Port	49		
			Server Timeout (seconds)	1-1000		
waik Me Inrough 3			Cancel		Apply to Device	

Cuando se abra la ventana emergente, proporcione el nombre del servidor (no tiene que coincidir con el nombre del sistema ISE), su dirección IP, la clave compartida, el puerto utilizado y el tiempo de espera.

En esta ventana emergente, debe proporcionar:

• El nombre del servidor (tenga en cuenta que no tiene que coincidir con el nombre del sistema de ISE)

- La dirección IP del servidor
- El secreto compartido entre el WLC y el servidor TACACS+

Se pueden configurar otros parámetros, como los puertos utilizados para la autenticación y la contabilidad, pero estos no son obligatorios y se dejan como predeterminados para esta documentación.

Desde CLI:

<#root>

WLC-9800(config)#tacacs server

ISE-lab

WLC-9800(config-server-tacacs)#address ipv4

10.48.39.134

WLC-9800(config-server-tacacs)#key

Cisco123

Paso 2. Asigne el servidor TACACS+ a un grupo de servidores. Desde la GUI:

En caso de que tenga varios servidores TACACS+ que se puedan utilizar para la autenticación, se recomienda asignar todos estos servidores al mismo grupo de servidores. El WLC entonces se ocupa del balanceo de carga de las diferentes autenticaciones entre los servidores en el grupo de servidores. Los grupos de servidores TACACS+ se configuran desde la Servers/Groups > TACACS > Server Groups pestaña desde la misma página de GUI que la mencionada en el Paso 1, que se muestra en la imagen.

Cisco Cataly	st 9800-CL Wireless Controlle	Welcome acimin Last login 12/07/2022 14:14:43	* * & B * *	Search APs and Clients	Q Feedback x <sup>A</sup> (*
Q. Search Menu Items         Image: Dashboard         Image: Omitoring         Image: Omitoring	Configuration • > Security • > AAV • AAA Wizard Servers / Groups AAA Method Li • Add × Delete RADIUS Servers	st AAA Advanced			
<ul> <li>Licensing</li> <li>Troubleshooting</li> </ul>	LDAP	Name TACACS-Group	' Server 1 ISE-lab	Server 2 N/A	Server 3 N/A 1 - 1 of 1 items:
Walk Me Through 3					

En cuanto a la creación del servidor, aparece una ventana emergente al hacer clic en el botón Agregar enmarcado en la imagen anterior, que se representa en la imagen.

Cisco Cata	ilyst 9800-CL Wireless Controller		🌣 🙋 😧 🎜 Search APs an	d Clients Q
Q. Search Manu Items	Configuration * > Security * > AAA + AAA Wizard Server Create AAA Tacacs Server	r Group		
Configuration > Configuration	Name*       RAI     Group Type       7A     Available Servers	TACACS-Group TACACS Assigned Servers ISE-lab C P C	X X X	Server 3 No items to display
Walk Me Through >	Cancel		Apply to Device	

En la ventana emergente, asigne un nombre al grupo y mueva los servidores deseados a la lista Servidores asignados.

Desde CLI:

WLC-9800(config)#aaa group server tacacs+

#### TACACS-Group

WLC-9800(config-sg-tacacs+)#server name

#### ISE-lab

Paso 3. Cree un método de registro de autenticación AAA que apunte al grupo de servidores TACACS+.

#### Desde la GUI:

En la página GUIhttps://<WLC-IP>/webui/#/aaa, vaya a la AAA Method List > Authentication ficha y cree un método de autenticación como se muestra en la imagen.



Como es habitual, cuando utiliza el botón Add (Agregar) para crear un método de autenticación, aparece una ventana emergente de configuración, similar a la que se muestra en esta imagen.

Cisco Cata	alyst 9800-CL Wireless Controller		Search APs and C	ients Q
Q. Search Manu Items       Image       Dashboard       Image       Monitoring       Image       Configuration	Configuration * > Security * > AAA AAA Au Au Au Type* Configuration * > Security * > AAA Au Au Au Au Au Au Au	tication tacacs-authe-method login	×	
<ul> <li>Administration &gt;</li> <li>Licensing</li> <li>Troubleshooting</li> </ul>	Aut Group Type Act Available Server Groups radius Idap tacacs + RADIUS-Group	local   Assigned Server Groups  TACACS-Group  ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	r ~ × ×	Group3 ▼ Group4 ▼ N/A N/A N/A N/A 1 - 2 of 2 items
Walk Me Through >	Cancel		Apply to Device	

En esta ventana emergente, proporcione un nombre para el método, elija Tipo como login y agregue el servidor de grupos creado en el paso anterior a la lista Grupos de servidores asignados. Con respecto al campo Tipo de grupo, son posibles varias configuraciones.

- Si elige el tipo de grupo como local, el WLC primero verifica si las credenciales del usuario existen localmente y después vuelve al grupo del servidor.
- Si elige el tipo de grupo como grupo y no marca la opción Volver a local, el WLC verifica solamente las credenciales del usuario contra el grupo del servidor.
- Si elige Group Type como grupo y marca la opción Fallback to local, el WLC verifica las credenciales del usuario contra el grupo del servidor y consulta la base de datos local solamente si el servidor no responde. Si el servidor envía un rechazo, el usuario se autenticará, aunque pueda existir en la base de datos local.

#### Desde CLI:

Si desea que las credenciales de usuario se comprueben con un grupo de servidores sólo si no se encuentran primero localmente, utilice:

<#root>

WLC-9800(config)#aaa authentication login

local group

TACACS-Group

Si desea que las credenciales de usuario sólo se comprueben con un grupo de servidores, utilice:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

Si desea que las credenciales de usuario se comprueben con un grupo de servidores y si esta última no responde con una entrada local, utilice:

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

local

En esta configuración de ejemplo, hay algunos usuarios que solo se crean localmente y otros usuarios solo en el servidor ISE, por lo tanto, hacen uso de la primera opción.

Paso 4. Cree un método exec de autorización AAA que apunte al grupo de servidores TACACS+. Desde la GUI:

El usuario también tiene que estar autorizado para que se le conceda acceso. En la página GUIConfiguration > Security > AAA, vaya a la AAA Method List > Authorization ficha y cree un método de autorización como se muestra en la imagen.

Cisco Cata	alyst 9800–CL Wireless (	Controller Welcome	admin /2022 14:14:43	<b>* A</b> B	* 1 0 3	Search APs and Clie	ents Q	Feedback	× (+
Q. Search Menu Items	Configuration - > Security + AAA Wizard	· · > AAA							
Monitoring     Solution	Authentication	Hethod List AAA A	Advanced						
<ul> <li>Administration &gt;</li> <li>Licensing</li> </ul>	Accounting	Name <b>Y</b> default radius-autho- method	Type <b>T</b> exec exec	Group Type <b>Y</b> local local	Group1 T N/A RADIUS-Group	Group2 <b>T</b>	Group3 <b>Y</b> N/A N/A	Group4 N/A N/A	Ŧ
X Troubleshooting		C tacacs-autho- method	exec	local	TACACS-Group	N/A I	N/A	N/A 1 - 3 of 3 item	15
Walk Me Through >									

Una ventana emergente de configuración de método de autorización similar a la representada aparece cuando se agrega una nueva con el botón Add (Agregar).

Cisco Catalyst 9800-CL Wire	less Controller				
	Welcome ad Last login 12/07/202	Imin 🛛 💣 🗞 🛕 🖺	🌣 🔯 🕜 🎜 Search APs	and Clients Q	🛛 Feedback 🖉 🦨 🕞
Q Search Menu Items	ecurity * > AAA				
+ Ar Quick Setu	p: AAA Authorization		×		
Server Method List	Name* tacacs-auti	no-method			
Monitoring     Type*	exec	▼ i			
Configuration > Aut Group Type	local	•			
Administration > Authenticate	ed 🛛			▼ Group3 ▼	Group4
C Licensing Act Available Set	ver Groups	Assigned Server Groups	]	N/A	N/A
radius Me Troubleshooting	>	TACACS-Group	Ā	N/A	N/A
RADIUS-G	oup				1 - 2 of 2 items
	«		×		
Walk Me Through >				-	
leoned C	]		Apply to Device		

En esta ventana emergente de configuración, proporcione un nombre para el método de autorización, elija Type as exec y utilice el mismo orden de Group Type que el utilizado para el método de autenticación en el paso anterior.

Desde CLI:

<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

local group

TACACS-Group

Paso 5. Asigne los métodos a las configuraciones HTTP y a las líneas VTY utilizadas para Telnet/SSH.

#### Desde la GUI:

Los métodos de autenticación y autorización creados se pueden utilizar para la conexión de usuario HTTP y/o Telnet/SSH, que se puede configurar desde la AAA Advanced > AAA Interface ficha todavía desde la página WLC de GUI accesible en https://<WLC-IP>/webui/#/aaa, como se muestra en la imagen.

Cisco Cata	lyst 9800-CL Wireless Controlle	Welcome <i>admin</i> Last login 12/07/2022 14:14:43	A 7 A	8 🗘 🔅	Search APs and Clients	Q Feedback x <sup>A</sup>
Q. Search Menu Items	Configuration • > Security • > AAA + AAA Wizard					
Monitoring > Configuration >	Servers / Groups AAA Method Lis	AAA Advanced				Apply
Administration     Administration     Licensing     Troubleshooting	Attribute List Name Console Device VTY Authentication VTY		Authentication None tacacs-authe-metho	• Ø d• Ø	Authorization None	Accounting None  None  None  X
Walk Me Through 5	AP Policy Password Policy AAA Interface	L				

#### Desde CLI:

Para la autenticación GUI:

<#root>

#### WLC-9800(config)#ip http authentication aaa login-authentication

tacacs-authe-method

WLC-9800(config)#ip http authentication aaa exec-authorization

tacacs-autho-method

Para autenticación Telnet/SSH:

<#root>

# WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication

tacacs-authe-method

WLC-9800(config-line)#authorization exec

tacacs-autho-method

Tenga en cuenta que cuando se realizan cambios en las configuraciones HTTP, es mejor reiniciar los servicios HTTP y HTTPS. Esto se puede lograr con estos comandos.

WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-server

#### Configuración de ISE de TACACS+

Paso 1. Configure el WLC como un dispositivo de red para TACACS+.

#### Desde la GUI:

Para declarar el WLC utilizado en la sección anterior como un dispositivo de red para RADIUS en ISE, navegue hasta Administration > Network Resources > Network Devices y abra la ficha Network devices (Dispositivos de red), como se muestra en esta imagen.

≡ Cisco ISE		Administration · Netw	vork Resources	🔺 Evalua	ation Mode 82 Days 🔍 🧑 🕫 🔅
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	More $ \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! $
Network Devices	Network	< Devices			
Device Security Settings	🖉 Edit + Ac	dd 📋 Duplicate 🕁 Import	🗅 Export 🗸 👌 Generate PAC	Delete 🗸	Selected 1 Total 1 🧭 🗔
	Name	e 🗠 IP/Mask Profile N	lame Location	Туре	Description
	WLC-	9800 10.48.39 🗰 Cisco	All Locations	All Device Types	

En este ejemplo, el WLC ya se ha agregado para la autenticación RADIUS (consulte el Paso 1 de la sección <u>Configuración de RADIUS ISE</u>). Por lo tanto, su configuración simplemente necesita ser modificada para configurar la autenticación TACACS, que se puede hacer cuando usted elige el WLC en la lista de dispositivos de red y hace clic en el botón Edit. Esto abre el formulario de configuración del dispositivo de red como se muestra en esta imagen.

≡ Cisco ISE		Administration • Netw	🛕 Evalu	ation Mode 82 Days Q	0	P	٩	
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	More $\sim$			
Network Devices	Genera	al Settings						
Default Device	Enal	ble KeyWrap 🥠						
Device Security Settings	Key	Encryption Key	Sho	w				
	Mes Auti Key	esage henticator Code	Sho	w				
	Key	Input Format ASCII () HEXADECIMAL						
		CACS Authentication Settin	gs					
	Shared	Secret	Show					
	Enal	ble Single Connect Mode						
	•	Legacy Cisco Device						
	0	TACACS Draft Compliance Single	Connect Support					
		MP Settings						
	🗌 🗸 Adv	anced TrustSec Settings						

Una vez que se haya abierto la nueva ventana, desplácese hacia abajo hasta la sección Configuración de autenticación TACACS, habilite estas configuraciones y agregue el secreto compartido ingresado durante el Paso 1 de la sección <u>Configuración de TACACS+ WLC</u>.

Paso 2. Active la función Device Admin para el nodo.



**Nota**: para utilizar ISE como servidor TACACS+, debe disponer de un paquete de licencias Device Administration y una licencia Base o Mobility.

#### Desde la GUI:

Una vez instaladas las licencias Device Administration, debe habilitar la función Device Admin para el nodo para poder utilizar ISE como servidor TACACS+. Para ello, edite la configuración del nodo de implementación de ISE utilizado, que se encuentra en Administrator > Deployment, y haga clic en su nombre o hágalo con la ayuda del Edit botón.

≡ Cisco ISE		Administration · System	4	A Evaluation Mode 82 Days Q ⑦ ヮ゚゚゚ の
Deployment Licensing	Certificates Logging	Maintenance Upgrade	Health Checks Backup & Restore	Admin Access Settings
Deployment < 1월 > 2월 Deployment 3월 PAN Failover		ent Nodes ter Syncup & Deregister a ^ Personas Administration, Monitor	Role(s) Services	Selected 0 Total 1 2 All V V Node Status PROFILER

Una vez abierta la ventana de configuración del nodo, verifique la opción Enable Device Admin Service bajo la sección Policy Service, como se muestra en esta imagen.

≡ Cisco ISE	Administration · System	🛕 Evaluation Mode 82 Days Q 🕜 🔎
Deployment Licensing Certifi	ates Logging Maintenance Upgrade Health Checks	Backup & Restore Admin Access Settings
Deployment       Image: Second system       Image: Second system       Image: Second system       Image: Second system	Administration - System       ▲ counter Nees 200 Q       Q       Admin Access       Settings         Certificates       Logging       Maintenance       Upgrade       Health Checks       Backup & Restore       Admin Access       Settings         Certificates       Logging       Maintenance       Upgrade       Health Checks       Backup & Restore       Admin Access       Settings         Certificates       Logging       Profiling Configuration       Image: Settings       Profiling Configuration         Hostmann       Set       FODN       Sections Certificates       Image: Settings         IP Address       10.48.39.134       Node Type       Image: Statings       Image: Statings         Role       STANDACORE       Maintenance       Image: Statings       Image: Statings       Image: Statings         IP Address       10.48.39.134       Node Type       Image: Statings       Image: Statings       Image: Statings       Image: Statings         IP Address       Description Node       Image: Statings       <	
	Role     STANDALONE       Administration       Monitoring       Role     PRIMARY       Other Monitoring Node	~
	<ul> <li>Dedicated MnT ()</li> <li>Policy Service</li> <li>Enable Session Services ()</li> <li>Include Node in Node Group None</li> <li>Enable Profiling Service ()</li> <li>Enable Threat Centric NAC Service ()</li> <li>Enable SXP Service ()</li> <li>Enable Device Admin Service ()</li> <li>Enable Passive Identity Service ()</li> </ul>	~ 0
	> pxtirid (j)	Reset Save

Paso 3. Cree perfiles TACACS para devolver el privilegio.

#### Desde la GUI:

Para tener derechos de acceso de administrador, el adminuser necesita tener un nivel de privilegio de 15, que permite acceder al intérprete de comandos exec. Por otro lado, el helpdeskuser no necesita acceso al shell exec prompt y, por lo tanto, se puede asignar con un nivel de privilegio inferior a 15. Para asignar el nivel de privilegio adecuado a los usuarios, se pueden utilizar perfiles de autorización. Se pueden configurar desde la página de la GUI de ISEWork Centers > Device Administration > Policy Elements, en la pestaña Results > TACACS Profiles que se muestra en la siguiente imagen.

≡ Cisco ISE		Work Centers · Device Administration     ups   Ext ld Sources   Network Resources   Policy Elements   Device Admin Policy Sets   More ×        CS Profiles     Nore ×     Policy Elements     Rows/Page   6   >  < 1   0   6   Total Rows     Policy Elements     Policy Elements     Rows/Page   6   >  < 1     Policy Elements     Rows/Page   6   >  < 1   00   6   Total Rows     Policy Elements     Policy Elements     Rows/Page   6   >  < 1   00   6   Total Rows     Policy Elements     Policy Elements  <		
E Cisco ISE       Work Centers • Device Administration       ▲ Extent Mode 82 Degs       Q       Q         Overview       Identities       User Identity Groups       Ext Id Sources       Network Resources       Policy Elements       Device Admin Policy Sets       More ~         Conditions       Smart Conditions       TACACS Profiles	ork Resources Policy Elements Device Admin Policy Sets More ~			
E Cisco ISE     Work Centers - Device Administration     Overview     Identities     User Identity Groups   Ext Id Sources   Network Resource   Dilcy Elements   Device Admin Policy Sets   Mere ~     Image: 1   Image: 1 </th				
Network Conditions	> 2 Add Dup	icate Trash 🗸 Edit		Filter 🗸 🕲
Results	∨ □ Name	,	Туре	Description
Allowed Protocols TACACS Command Sets	Default Shell	Profile \$	Shell	Default Shell Profile
TACACS Profiles	Deny All She	Il Profile S	Shell	Deny All Shell Profile
	IOS Admin	5	Shell	Assigned to each user in the group admin-group
	IOS Helpdesi	k S	Shell	Assigned to each user in the group helpdesk-group
	U WLC ALL	1	WLC	WLC ALL
	WLC MONITO	DR N	WLC	WLC MONITOR

Para configurar un nuevo perfil TACACS, utilice el botón Add (Agregar), que abre el nuevo formulario de configuración del perfil similar al que se muestra en la imagen. Este formulario debe tener un aspecto especial para configurar el perfil que se asigna al adminuser (es decir, con el nivel 15 de privilegios de shell).

	DISE		Work Centers ·	Device Administration		A Evaluation Mode	82 Days Q	0	~9 \$
Overview	Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	More $\vee$		
Conditions		> TACACS Profiles > 100 TACACS Profile	S Admin						
Network Conditio	ns	>		-					
Results Allowed Protoc	ols	V IOS Admin							
TACACS Comm	hand Sets	Description							
TACACS Profile	is	Assigned to each admin-group	user in the group						
		Task Attribute View	Raw View						
		Common Tasks							
		Common Tasks							
		Common Task Type	Shell 🗸						
		6	Default Privilege	15	✓ (Select 0)	to 15)			
				15	✓ (Select 0)	to 15)			
		Ľ	Maximum Privilege		(0000000				
			Access Control List		~				
		-	Auto Command		~				
		(	No Escape		✓ (Select true	ue or false)			
			Timeout		V Minutes (0	-9999)			
			Idle Time		✓ Minutes (0	-9999)			
		Custom Attribut	es						
		Add Trash 🗸 🛛	Edit					0	
		🗆 Туре	Name	Value					
		No data found.							
						Са	ncel	Save	

Repita la operación para el helpdesk perfil. Para este último, el privilegio predeterminado, así como el privilegio máximo, se establecen en 1.

Paso 4. Cree grupos de usuarios en ISE.

Esto es lo mismo que se presentó en el paso 3 de la sección Configuración de RADIUS ISE de este documento.

Paso 5. Cree los usuarios en ISE.

Esto es lo mismo que se presenta en el Paso 4 de la sección Configuración de RADIUS ISE de este documento.

Paso 6. Cree un conjunto de directivas de administración de dispositivos.

#### Desde la GUI:

~ .

En cuanto al acceso RADIUS, una vez que se crean los usuarios, sus políticas de autenticación y autorización todavía deben definirse en ISE para otorgarles los derechos de acceso adecuados. La autenticación TACACS utiliza conjuntos de políticas de administración de dispositivos para ese fin, que se pueden configurar desde el Work Centers > Device Administration > Device Admin Policy Sets GUI Page como se muestra.

■ Cisco ISE	Work Centers · Device Administration	🛕 Evaluation Mode 82 Days Q 💮 🕫
Overview Identities User Identity Grou	ps Ext Id Sources Network Resources P	Policy Elements Device Admin Policy Sets More ~
Policy Sets		Reset Policyset Hitcounts Save
Status Policy Set Name Desc	ription Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q Search		
WLC TACACS Authentication	P Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin $\boxtimes \checkmark + 0$ $ correct corr$
Default Tacac	s Default policy set	Default Device Admin $\textcircled{\ } \lor +$ 0 $\textcircled{\ } \textcircled{\ } \r{\ } \checkmark$
		Reset Save

Para crear un conjunto de directivas de administración de dispositivos, utilice el botón agregar enmarcado en rojo en la imagen anterior. De este modo, se agrega un elemento a la lista de conjuntos de directivas. Proporcione un nombre para el conjunto recién creado, una condición bajo la cual debe aplicarse y la Secuencia Protocolos/Servidor Permitidos (aquí, Default Device Adminbasta). Utilice el Save botón para finalizar la adición del conjunto de políticas y utilice la punta de flecha de su derecha para acceder a su página de configuración, tal y como aparece en la representada.

erview Id	entities User Identit	y Groups	Ext Id Sources	Network Res	sources	Policy Elements	Dev	vice Admin Policy Se	ts More	~	
licy Sets→							_		_		
	WLC TACACS Authen	tication					Res	et Reset Policy	set Hitcounts		Save
Status Po	licy Set Name I	Description	Conditio	ons				Allowed Prote	ocols / Server	Sequer	ice H
Q Search	WLC TACACS Authentication			Network Access-I	Device IP Addres	s EQUALS 10.48.39	.133	Default Dev	ice Admin	≪ ≫	+ 0
<sup>7</sup> Authenticatior	Policy (1)										
+ Status	Rule Name	Conditions	5				Us	e		Hits	Action
Q Search											
					+						
							A	II_User_ID_Stores	$\propto$ $\sim$		
0	Default						>	Options		0	ŝ
Authorization	Policy - Local Exceptions										
Authorization	Policy - Global Exceptions										
				R	esults						
Status	Rule Name	Conditions	5	C	ommand Sets		Sh	ell Profiles		Hits	Action
Q Search											
0	Helpdesk users authorization	A Intern Identi	alUser-IdentityGroup EQU ty Groups:helpdesk-group	ALS User A	llowAllComma	inds $ imes$ $\sim$	+ 10	OS Helpdesk	∞ ~+	0	ŝ
0	Admin users authorization	A Intern Identi	alUser-IdentityGroup EQU ty Groups:admin-group	ALS User	llowAllComma	inds $\times$ $\checkmark$	+	OS Admin	<u> </u>	0	ŝ
	Default			D	enyAllComma	nds $ imes$ $\sim$	+ 0	eny All Shell Profile	∞ ~+	0	<u></u>

El conjunto de políticas específico 'WLC TACACS Authentication' en este ejemplo filtra las solicitudes con la dirección IP igual a la dirección IP del WLC C9800 de ejemplo.

Como política de autenticación, se ha dejado la regla predeterminada porque satisface las necesidades del caso de uso. Se han establecido dos reglas de autorización:

• La primera se activa cuando el usuario pertenece al grupo definido admin-group. Permite todos los comandos (mediante la regla predeterminada Permit\_all) y asigna el privilegio 15 (mediante el perfil TACACS definidoIOS\_Admin ).

• El segundo se activa cuando el usuario pertenece al grupo definido helpdesk-group. Permite todos los comandos (a través de la Permit\_all regla predeterminada) y asigna el privilegio 1 (a través del perfil TACACS definidoIOS\_Helpdesk).

autenticar en el WLC vía la GUI o con Telnet/SSH.

Troubleshoot

Si su servidor RADIUS espera que se envíe el atributo RADIUS del tipo de servicio, puede agregar en el WLC :

```
radius-server attribute 6 on-for-login-auth
```

Resolución de problemas de WLC GUI o CLI RADIUS/TACACS+ acceso a través de WLC CLI

Para resolver problemas del acceso TACACS+ a la GUI o CLI del WLC, ejecute el debug tacacs comando, junto con el monitor de terminal uno y vea la salida en vivo cuando se realiza un intento de inicio de sesión.

Por ejemplo, un inicio de sesión correcto seguido de un cierre de sesión del adminuser usuario genera este resultado.

<#root>

WLC-9800#

terminal monitor

WLC-9800#

debug tacacs

TACACS access control debugging is on WLC-9800# Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro

Se puede ver en estos registros que el servidor TACACS+ devuelve el privilegio correcto (que es AV priv-lvl=15).

Cuando realiza la autenticación RADIUS, se muestra una salida de depuración similar, que concierne al tráfico RADIUS.

Los comandos debug aaa authentication y debug aaa authorization en su lugar, muestran qué lista de métodos es elegida por el WLC cuando el

usuario intenta iniciar sesión.

#### Resolución de problemas de WLC GUI o CLI TACACS+ Access a través de ISE GUI

Desde la página Operations > TACACS > Live Logs, se puede ver cada autenticación de usuario realizada con TACACS+ hasta las últimas 24 horas. Para ampliar los detalles de una autorización o autenticación TACACS+, utilice el botón Detalles relacionado con este evento.

	Cisco ISE			Ope	rations · TACACS	]	4	Evaluation Mode 82 Day	rs Q	0	P	0
/e L	ogs											
ß	① Export To ∨					Refresh Never	~	Show Latest 20 records	Witi La	nin st 3 hor ilter 🗸	urs @	
	Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authori	zation Policy	lse M	lode		
×			~	Identity	~	Authentication Policy	Authoriz	ation Policy	Ise M	lode		
	Dec 08, 2022 06:51:46.1	2	à	helpdeskuser	Authorization		WLC TAC	CACS Authentication >	ise			
	Dec 08, 2022 06:51:46.0		o	helpdeskuser	Authentication	WLC TACACS Authentication	•		ise			
	Dec 08, 2022 06:38:38.2	2	ò	adminuser	Authorization		WLC TAC	CACS Authentication >	ise			
	Dec 08, 2022 06:38:38.1		à	adminuser	Authentication	WLC TACACS Authentication	<b>.</b>		ise			
	Dec 08, 2022 06:34:54.0		ò	adminuser	Authorization		WLC TAC	CACS Authentication >	ise			3
	Dec 08, 2022 06:34:53.9		ò	adminuser	Authentication	WLC TACACS Authentication	•		ise			
ast	Updated: Thu Dec 08 202	2 12:57:09	GMT+0100 (C	entral European	Standard Time)				Re	cords §	Showr	

Cuando se expande, un intento de autenticación correcto para el helpdeskuser se ve así:

#### Cisco ISE

Overview	
Request Type	Authentication
Status	Pass
Session Key	ise/459637517/243
Message Text	Passed-Authentication: Authentication succeeded
Username	helpdeskuser
Authentication Policy	WLC TACACS Authentication >> Default
Selected Authorization Profile	IOS Helpdesk

#### **Authentication Details**

Generated Time	2022-12-08 06:51:46.077000 -05:00
Logged Time	2022-12-08 06:51:46.077
Epoch Time (sec)	1670500306
ISE Node	ise
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdeskuser
Network Device Name	WLC-9800
Network Device Name Network Device IP	WLC-9800 10.48.39.133
Network Device Name Network Device IP Network Device Groups	WLC-9800 10.48.39.133 IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Network Device Name Network Device IP Network Device Groups Device Type	WLC-9800 10.48.39.133 IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types Device Type#All Device Types
Network Device Name Network Device IP Network Device Groups Device Type Location	WLC-9800 10.48.39.133 IPSEC#IIs IPSEC Device#No,Location#All Locations,Device Type#All Device Types Device Type#All Device Types Location#All Locations
Network Device Name Network Device IP Network Device Groups Device Type Location Device Port	WLC-9800 10.48.39.133 IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types Device Type#All Device Types Location#All Locations tty5

#### Steps

13013	Received TACACS+ Authentication START Request
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Network Access.Device IP Address
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore
24212	Found User in Internal Users IDStore
13045	TACACS+ will use the password prompt from global TACACS+ configuration
13015	Returned TACACS+ Authentication Reply
13014	Received TACACS+ Authentication CONTINUE Request (
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore
24212	Found User in Internal Users IDStore
22037	Authentication Passed
15036	Evaluating Authorization Policy
15048	Queried PIP - Network Access.UserName
15048	Queried PIP - InternalUser.IdentityGroup
13015	Returned TACACS+ Authentication Reply

A partir de esto, puede ver que el usuario helpdeskuser se ha autenticado correctamente en el dispositivo de red WLC-9800 con la ayuda de la política de autenticación WLC TACACS Authentication > Default. Además, el perfil de autorización IOS Helpdesk se ha asignado a este usuario y se le ha concedido el nivel de privilegio 1.

### 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).