# Sistema operativo ampliable FirePOWER (FXOS) 2.2: Autenticación/autorización de chasis para administración remota con ISE mediante TACACS+

# Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Diagrama de la red Configuraciones Configuración del chasis FXOS Configuración del servidor ISE Verificación Verificación de FXOS Chasis Verificación de ISE 2.0 Troubleshoot Información Relacionada

# Introducción

Este documento describe cómo configurar la autenticación y autorización TACACS+ para el chasis Firepower eXtensible Operating System (FXOS) a través de Identity Services Engine (ISE).

El chasis FXOS incluye las siguientes funciones de usuario:

- Administrador: complete el acceso de lectura y escritura a todo el sistema. La cuenta de administrador predeterminada tiene asignada esta función de forma predeterminada y no se puede cambiar.
- Sólo lectura: acceso de sólo lectura a la configuración del sistema sin privilegios para modificar el estado del sistema.
- Operaciones: acceso de lectura y escritura a la configuración de NTP, configuración de Smart Call Home para Smart Licensing y registros del sistema, incluidos los servidores y fallos de syslog. Lea el acceso al resto del sistema.
- AAA: acceso de lectura y escritura a usuarios, funciones y configuración AAA. Lea el acceso al resto del sistema.

A través de CLI, esto puede verse de la siguiente manera:

fpr4120-TAC-A /security\* # show role

Función:

Nombre de rol Priv

\_\_\_\_

aaa aaa

admin

operaciones

sólo lectura

Colaborado por Tony Remirez, Jose Soto, Ingenieros del TAC de Cisco.

# Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de Firepower eXtensible Operating System (FXOS)
- Conocimiento de la configuración de ISE
- La licencia de administración de dispositivos TACACS+ se requiere dentro de ISE

## **Componentes Utilizados**

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

- Cisco Firepower 4120 Security Appliance versión 2.2
- Cisco Identity Services Engine 2.2.0.470 virtual

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

El objetivo de la configuración es:

- Autentique a los usuarios que inician sesión en la GUI basada en Web y SSH de FXOS mediante ISE
- Autorice a los usuarios a iniciar sesión en la GUI basada en Web y SSH de FXOS según su función de usuario respectiva mediante ISE.
- Verifique el correcto funcionamiento de la autenticación y autorización en el FXOS mediante ISE



Network admin

## Configuraciones

Configuración del chasis FXOS

Creación de un proveedor TACACS+

Paso 1. Vaya a Configuración de plataforma > AAA.

Paso 2. Haga clic en la pestaña TACACS.

(	Overview	Interfaces	Logical	Devices	Secur	ity Engine	Platform Setting	gs			
	NTP			LDAP	RADIUS	TACACS					
	SSH										
	SNMP			Propertie	s						
	HTTPS			Timeout:	* 5	Secs					
	AAA				_						
	Syslog			TACACS	Providers						
	DNS									0	Add
	FIPS and C	Common Criteria		Hostna	me			Order	Port		
	Access List			mostina				0.001			

Paso 3. Para cada proveedor TACACS+ que desee agregar (hasta 16 proveedores).

3.1. En el área Proveedores TACACS, haga clic en Agregar.

3.2. Cuando se abra el cuadro de diálogo Agregar proveedor TACACS, introduzca los valores necesarios.

3.3. Haga clic en Aceptar para cerrar el cuadro de diálogo Agregar proveedor TACACS.

ĺ	Add TACACS Provider		?×	
	Hostname/FQDN(or IP Address):*	10.88.244.50		6
l	Order:*	lowest-available	] [	
I	Key:	•••••	Set:No	
l	Confirm Key:	••••••	]	
l	Port:*	49		
l	Timeout:*	5 Secs		
l		UK Can	icei	

## Paso 4. Click Save.

Overview Interfaces Logic	al Devices Security Engine Platform Setting	gs							
NTP	LDAP RADIUS TACACS								
SNMP	Properties								
HTTPS	Timeout:* 5 Secs	meout:* 5 Secs							
Syslog	TACACS Providers								
DNS				Add					
FIPS and Common Criteria	Hostname	Order	Port						
Access List	10.88.244.50	1	49	0					
	Save								

Paso 5. Vaya a System > User Management > Settings.

Paso 6. En Default Authentication , elija TACACS.

Overview Interfaces	logical Devices Security Engine Platform Settings			System Too	is Help fxosadmin
		Configuration	Licensing	Updates	User Management
Local Users Settings				_	
Default Authentication	TACACS v Local is failback authentication method				
Console Authentication	Local				
Remote User Settings Remote User Role Policy	C Assign Default Role 🔿 No-Login				

Creación de un proveedor TACACS+ mediante CLI

Paso 1. Para habilitar la autenticación TACACS, ejecute los siguientes comandos.

seguridad de alcance fpr4120-TAC-A#

## fpr4120-TAC-A /security # scope default-auth

fpr4120-TAC-A /security/default-auth # set realm tacacs

Paso 2. Utilice el comando show detail para verificar la configuración.

fpr4120-TAC-A /security/default-auth # show detail

Autenticación predeterminada:

Rango de administración: TACACS

Rango operativo: TACACS

Período de actualización de la sesión web(en segundos): 600

Tiempo de espera de sesión(en segundos) para sesiones web, ssh, telnet: 600

Tiempo de espera de sesión absoluto(en segundos) para sesiones web, ssh, telnet: 3600

Tiempo de espera de la sesión de la consola serie(en segundos): 600

Tiempo de espera de la sesión absoluta de la consola serie(en segundos): 3600

Grupo de servidores de autenticación de administrador:

Grupo de servidores de autenticación operativa:

Uso del segundo factor: No

Paso 3. Para configurar los parámetros del servidor TACACS, ejecute los siguientes comandos.

seguridad de alcance fpr4120-TAC-A#

fpr4120-TAC-A /security # scope tacacs

fpr4120-TAC-A /security/tacacs # ingrese server 10.88.244.50

fpr4120-TAC-A /security/tacacs/server # set descr "ACS Server"

fpr4120-TAC-A /security/tacacs/server\* # set key

Introduzca la clave: \*\*\*\*\*

Confirme la clave: \*\*\*\*\*

Paso 4. Utilice el comando show detail para verificar la configuración.

fpr4120-TAC-A /security/tacacs/server\* # show detail

Servidor TACACS+:

Nombre de host, FQDN o dirección IP: 10.88.244.50

Descr:

Pedido: 1

Puerto: 49

Clave: \*\*\*

timeout (tiempo de espera): 5

Configuración del servidor ISE

Adición de FXOS como recurso de red

Paso 1. Vaya a Administration > Network Resources > Network Devices.

Paso 2. Haga clic en Add (Agregar).



Paso 3. Introduzca los valores necesarios (Nombre, Dirección IP, Tipo de dispositivo y Activar TACACS+ y agregue la CLAVE), haga clic en **Enviar**.

dentity Services Engine	Home	<ul> <li>Context \</li> </ul>	Visibility	Policy	<ul> <li>Administration</li> </ul>	<ul> <li>Work Centers</li> </ul>		
System     Identity Management	- Network	k Resources	Device Portal Manager	nent pxGrid \$	Services    Feed Se	rvice	NAC	
Network Devices Network Device	Groups	Network Devic	e Profiles External RAD	IUS Servers	RADIUS Server Sequ	ences NAC Managers	External MDM	Location Services
(	3							
Network devices	Netwo	vork Devices List	( > FXOS					
Default Device	Heer	fork befield	• Name	EXOS				
Device Security Settings			Description					
		* IP Address:	10.83.180.6	/ 32				
			Device Profile	🗱 Cisco 👻 🕀	)			
			Model Name		Ţ			
			Software Version		Ţ			
	•	Network Devi	ce Group					
	C	Device Type	FXOS 📀	Set To Defaul	t			
		IPSEC	No 📀	Set To Defaul	t			
		Location	All Locations 📀	Set To Defaul	t			
		RADIUS A	uthentication Settings					
	✓	- TACACS A	uthentication Settings					
			Enable Single	Shared Secret Connect Mode	Legacy Cisco Der     TACACS Draft Co	Show Vice Single Connect	Support	
		SNMP Sett	tings					
		Advanced	TrustSec Settings					
	Save	Reset						

## Creación de grupos de identidad y usuarios

Paso 1. Vaya a Administration > Identity Management > Groups > User Identity Groups.

Paso 2.	Haga	clic en	Add	(Agregar)	).
---------	------	---------	-----	-----------	----

tiste Identity Services Engine Home	Context Visibility ► Operations ► Policy ► Admin	istration Vork Centers
► System	ources       Device Portal Management pxGrid Services	Feed Service     Threat Centric NAC
Identities Groups External Identity Sources Identity	dentity Source Sequences	
Identity Groups	User Identity Groups	
<u>ج</u>	user mentity croups	
<		
Endpoint Identity Groups	Name	Description
User Identity Groups	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
	Employee	Default Employee User Group
	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
	GuestType_Contractor (default)	Identity group mirroring the guest type
	GuestType_Daily (default)	Identity group mirroring the guest type
	GuestType_Weekly (default)	Identity group mirroring the guest type
	ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

Paso 3. Introduzca el valor para Name y haga clic en Submit.

den cisco	tity Services	Engine	Home	Context Visibility	<ul> <li>Operations</li> </ul>	Policy	<del>▼</del> Admi	nistration	Work Centers	
<ul> <li>System</li> </ul>	✓ Identity Ma	anagement	Network F	Resources + Devic	ce Portal Managemen	t pxGrid S	ervices	Feed Service	Threat Centric NAC	
Identities	Groups	External Ider	ntity Sources	Identity Source Se	quences + Setting	S				
Identity	y Groups	Groups ups	(م •	User Identity Gr Identity Gre Name Description Submit	roups > New User Id pup FXOS ADMIN Cancel	entity Group				

Paso 4. Repita el paso 3 para todas las funciones de usuario necesarias.

dentity Services Engine Home	Context VIsibility → Operations → Policy      Ad	Iministration Vork Centers
► System	esources	Feed Service
Identities Groups External Identity Sources	Identity Source Sequences	
Identity Groups	User Identity Groups	
⟨= •   E •	/ Edit 🕂 Add 🗙 Delete 👻 🎲 Import 😭 Export	*
Endpoint Identity Groups	Name	Description
User Identity Groups	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
	Employee	Default Employee User Group
	🗌 💐 FXOS AAA	
	E A FXOS ADMIN	
	E PXOS OPER	
	FXOS Read Only	
		Diffult COOLD, ACCOUNTS (J-5-15) Unit Count

Paso 5. Vaya a Administration > Identity Management > Identity > Users.

Paso 6. Haga clic en Add (Agregar).

-Indentity Services Engine	Home ► Context Visibility ► Op	erations   Policy  Administration	► Work Centers								
System      Identity Management     Network Resources     Device Portal Management     pxGrid Services     Feed Service     Threat Centric NAC											
Identities Groups External Identity Sources Identity Source Sequences      Settings											
0											
Users	Users Network Access Users										
Latest Manual Network Scan Results	/ Edit 🕂 Add 🔯 Change Status	🛃 Import 🚯 Export 🗙 Delete 🖓	Duplicate								
	Status Name	<ul> <li>Description</li> </ul>	irst Name Last Name Email Address	User Identity Groups Admin							
			N	o data available							

Paso 7. Introduzca los valores necesarios (Nombre, Grupo de usuarios, Contraseña).

cisco	Identity Serv	vices Engi	ine	Home	► Context 1	Visibility	<ul> <li>Operations</li> </ul>	Policy	<b>▼</b> Adm	inistration	Work Ce	inters
<ul> <li>Syst</li> </ul>	em 🗸 Ideni	ity Manage	ement	Network	Resources	Device	Portal Managemen	t pxGrid	Services	Feed Se	rvice + Th	reat Centric NAC
- Ident	tities Group	os Exter	nal Identit	y Sources	Identity So	ource Sequ	ences	s				
			G	Matural		and link as the						
Users				Netwon	Access Use		ew Network Acces	s User				
Latest M	anual Networ	k Scan Res	sults	* Ne	LWORK ACCO	ess user						
				• Na	me fxosad	min						
				Sta	itus 🔽 Er	nabled 👻						
				En	nail							
				▼ P	asswords							
				Pa	ssword Type	Interna	al Users	Ŧ				
						Passwo	ord		Re-Enter	Password		
				•	ogin Passwo	rd •••••	••		•••••			Generate Password (
				En	able Passwo	rd						Generate Password ()
				ΨU	ser Inform	ation						
				Fin	st Name							
				La	st Name							
				- A	ccount Op	tions						
						Descri	intion					
				Ch								
					ange passing							
				▼ A	ccount Dis	able Poli	cy					
					Disable ac	count if dat	e exceeds 2018-	03-01		(797)	y-mm-dd)	
				- U	ser Groups	5						
				E	XOS ADMIN		<u> </u>					
				Subr	nit Canr	el						
				5401	Cuno							

Paso 8. Repita el paso 6 para todos los usuarios requeridos.

Identity Services Engine	Home + Conte	xt Visibility	Policy     Administration	on 🔹 Work Ce	nters							
System      ▼Identity Management	Network Resources	Device Portal Management	pxGrid Services + Fee	d Service + Thr	eat Centric NAC							
dentities Groups External Identity Sources Identity Source Sequences      Settings												
O Network Assess Users												
Users Network Access Users												
Latest Manual Network Scan Results	/ Edit 🕂 Add	🔀 Change Status 👻 🎼 Import	🕞 Export 👻 🗙 Delete 👻	Duplicate								
	Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin				
	Enabled	👤 fxosaaa					FXOS AAA					
	Enabled	👤 fxosadmin					FXOS ADMIN					
	🗌 🔽 Enabled	2 fxosoper	1 fxosoper									
	🗌 🛃 Enabled	9 fxosro					FXOS Read Only					

Creación del perfil de shell para cada rol de usuario

Paso 1. Navegue hasta Centros de trabajo > Administración de dispositivos > Elementos de políticas > Resultados > Perfiles TACACS y haga clic +AÑADIR.

dentity Services Engine	Home   Context Visibility   Operations   Poli	icy ► Administration
Network Access     Guest Access	TrustSec      BYOD      Profiler      Posture      Device	e Administration    PassiveID
Overview      Identities     User Ident	ty Groups Ext Id Sources + Network Resources - Pol	licy Elements Device Admin Policy Sets Reports Settings
Conditions	TACACS Profiles 0 Selected	Rows/Page 4 - 1 3 / 1 > 1 Go 4 Total Rows
Network Conditions	S Refresh 🕂 Add Duplicate 🏛 Trash 🗸	© Edit Ţ Filter ▼ ♦ ▼
✓ Results	Name	Type Description
Allowed Protocols	U WLC ALL	WLC WLC ALL
TACACS Command Sets	U WLC MONITOR	WLC WLC MONITOR
TACACS Profiles	Deny All Shell Profile	Shell Deny All Shell Profile
	Default Shell Profile	Shell Default Shell Profile

## Paso 2. Introduzca los valores necesarios para el perfil TACACS

## 2.1. Introduzca el nombre.

TACACS Profiles > New	
TACACS Profile	
Name	FXOS_Admin_Profile
Description	
Task Attribute View Raw	View

2.2. En la FICHA Vista en RAW, configure el siguiente CISCO-AV-PAIR.

cisco-av-pair=shell:roles="admin"

#### TACACS Profiles > New

#### TACACS Profile

Name	FXOS_Admin_Profile
Description	
Task Attribute View Raw	View
Profile Attributes	
cisco-av-pair=shell:roles="admin"	
	Cancel Submit

2.3. Haga clic en Submit (Enviar).

#### TACACS Profiles > FXOS\_Admin\_Profile

TACACS Profile				
,	Name FXOS_Admin_Profile			
Descr	ription			
Task Attribute View	Raw View			
Common Tasks				
Common Task Type Shell	-			
Default Privilege		0	(Select 0 to 15)	
Maximum Privilege		0	(Select 0 to 15)	
C Access Control List	st	0		
Auto Command		0		
No Escape		0	(Select true or false)	
Timeout		0	Minutes (0-9999)	
Idle Time		0	Minutes (0-9999)	
Custom Attributes				
+ Add	dit			۸-
	Name	Value		

Paso 3. Repita el paso 2 para las restantes funciones de usuario utilizando los siguientes pares AV-Cisco.

shell:roles="admin"

C 🖻

Save

Cancel

#### cisco-av-pair=shell:roles="aaa"

cisco-av-pair=shell:roles="operaciones"

cisco-av-pair

## cisco-av-pair=shell:roles="sólo lectura"

**Custom Attributes** 

MANDATORY

+ A	dd 🍵 Trash 🕶 🖸 E	dit		۰.
	Туре	Name	Value	
	MANDATORY	cisco-av-pair	shell:roles="aaa"	C' 🗊
			Cance	I Save

#### **Custom Attributes**

+ Add	💼 Trash 👻 🖸 E	dit					¢-
🗆 Туре		Name		Value			
	DATORY	cisco-av-pair		shell:rol	es="operations"	<b>G</b> i	<b>D</b>
Custom Attr	ributes						0
+ Add	💼 Trash 👻 🖸 E	dit					۰.
🗆 Туре		Name		Value			
MAND	DATORY	cisco-av-pair		shell:role	s="read-only"	ß. U	i
0 Selected	S Profiles	Duplicate 🛱 Tra		Rows/	Page 8 1 0/1 > > 0	30 8 Tota	Rows
Refre	esn <b>-</b> Add	Duplicate III Ira	sn ▼	& Edit		Filter	ų.
	ame		Ту	pe	Description		
W	LC ALL		W	LC	WLC ALL		
W	LC MONITOR		W	LC	WLC MONITOR		
	eny All Shell Profil	e	S	hell	Deny All Shell Profile		
De	efault Shell Profile	•	S	hell	Default Shell Profile		
D F)	KOS_Admin_Profi	le	S	hell			
D F)	KOS_AAA_Shell		S	hell			
D F)	KOS_Operations_	Shell	S	hell			
- F)	KOS_ReadOnly_S	Shell	S	hell			

## Creación de la Política de Autorización TACACS

Paso 1. Vaya a Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos.

"Invite Identity Services Engine Home	Context Visibility     Operations     Policy     Administration     Work Centers	() Q 0 0 0
Network Access     Guest Access     TrustSec	BYOD + Profiler + Posture - Device Administration + PassiveID	Click here to do wireless setup and visibility setup Do not show this again.
Overview      Identities User Identity Groups	Ext Id Sources + Network Resources + Policy Elements Device Admin Policy Sets Reports Settings	
Policy Sets Search policy names & descriptions. Comparison of Policies A lat of al your policies Comparison of the options Bules across effer deployment Bules across effer deployment	Define the Picky Sets by configuring rules based on conditions. Dag and drop tells on the left hand side to change the order. For Picky Sport pairs Aname Satus Name Defined Tacase, Definid Regular Picky Server Sequence Picky Server Sequence Picky Server Sequence:	
Tacacs_Default	Authentication Policy	
Save Order Reset Order	Default Rule (If no match) : Allow Protocols : Default Device Admin and use : All_User_ID_Stores	Edt   •
	* Authorization Policy	
	Exceptions (0)	
	Standard	
	Status Rule Name Conditions (identity groups and other conditions) Command Sets Shell Profiles	
	Tacacs_Default if no matches, then Select Profile(8) Deny Al Shell Profile	Edit   •

Paso 2. Asegúrese de que la política de autenticación apunte a la base de datos de usuarios

internos o al almacén de identidades requerido.

¥	Authenti	cation Policy		
	<b>_</b>	Default Rule (If no match)	: Allow Protocols : Default Device Admin and use : All_User_ID_Stores	

Paso 3. Haga clic en la flecha situada al final de la política de autorización predeterminada y haga clic en insertar regla anterior.

Authorization Policy				
Exceptions (0)				
Standard				
Status Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles	
Tacacs_Default	If no matches, then Select Profile(s) Deny All Shell I	Profile		Entit Ly

Paso 4. Introduzca los valores de la regla con los parámetros necesarios:

- 4.1. 'Nombre de la regla Regla de administración FXOS.
- 4.2. Condiciones.

Si: El grupo de identidad de usuario es FXOS ADMIN

Status Rule Name	Conditions (identity groups and other conditions) Command Sets	Shell Profiles
FXOS Admin Rule	if Any 🗢 and Condition(s) 💠 then Comman 🤇	and Select a Shell Profile
Tacacs_Default	if no ma	
	User Identity Groups	
		Q
	• • = •	÷
	EXOS AAA	
	GuestType_Weekly (defaulter)	ult)
	OWN_ACCOUNTS (default	t)
	GROUP_ACCOUNTS (defa	ault)
	FXOS ADMIN	
	FXOS OPER	
	Employee	
	GuestType_Daily (default)	)
	GuestType_Contractor (della contractor)	efault)
Cours Dearth	FXOS Read Only	
Save	ALL_ACCOUNTS (default)	

Y dispositivo: El tipo de dispositivo es igual a todos los tipos de dispositivo #FXOS

Conditions (identity group	and other conditions) Command	Sets Shell Profiles			
if FX 💠 and	DEVICE:Devi 🗢 then Comman	select a Shell Profile	$\odot$		
to matches, then Select	Add All Conditions Below to Library				-
	Condition Name Desc	ription VICE:Device Ty 📀 Equals 👻	All Device Types# 📀	]	ŵ <b>.</b>
				( ↓ ↓ ■ •	হ ©-
				All Device Types	
				All Device Types#FXOS	
				🚞 AD	>
				DEVICE	>
				InternalUser	>
				Network Access	>
				Network Condition	>
				TACACS	>

Perfil de shell: FXOS\_Admin\_Profile

Shell Profile
(م
🖉 🖛 🗐 🔹 🚳 🖓 🖓
🥁 Default Shell Profile
😪 Deny All Shell Profile
Generation FXOS_AAA_Shell
KOS_Admin_Profile
Generations_Shell
FXOS_ReadOnly_Shell
Se WLC ALL
WLC MONITOR

Paso 5. Haga clic en Done (Listo).

Exce	eptions (0)		
Stand	lard		
5	status Rule Name	Conditions (identity groups and other conditions) Command Sets Shell Profiles	
P 🛃	<ul> <li>FXOS Admin Rule</li> </ul>	If FX $\diamondsuit$ and DEVICE:Devi $\diamondsuit$ than Select an item $\diamondsuit$ and FXOS_Admin_Profile	Done
	<ul> <li>Tacacs_Default</li> </ul>	If no matches, then Select Profile (s) Deny Al Shell Profile	Edit   🕶
Save	Reset		

Paso 6. Repita los pasos 3 y 4 para las funciones de usuario restantes y, cuando haya terminado, haga clic en **GUARDAR**.

Standard         Standard         Status       Rule Name       Conditions (identity groups and other conditions)       Command Sets       Shell Profiles         Image: Status       FXOS Admin Rule       If       FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS       then       Select an item       FXOS_Admin_Profile         Image: Status       FXOS AAA Rule       If       FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS       then       Select Profile(s)       FXOS_AAA_Shell         Image: Status       FXOS Operations Rule       If       FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS       then       Select Profile(s)       FXOS_Operations_Shell         Image: Status       FXOS Read Only Rule       Image: Status Equation FXOS       then       Select Profile(s)       FXOS_ReadOnly_Shell	Authorization Policy		
Status       Rule Name       Conditions (identity groups and other conditions)       Command Sets       Shell Profiles         Image: Status       FXOS Admin Rule       If       FXOS ADMIN AND DEVICE:Device Type       then       Select an item       FXOS_Admin_Profile         Image: Status       FXOS AAA Rule       If       FXOS AAA AND DEVICE:Device Type       then       Select Profile(s)       FXOS_AAA_Shell         Image: Status       FXOS Operations Rule       If       FXOS OPER AND DEVICE:Device Type       then       Select Profile(s)       FXOS_Operations_Shell         Image: Status       FXOS Read Only Rule       If       FXOS Read Only AND DEVICE:Device Type       then       Select Profile(s)       FXOS_Operations_Shell	Exceptions (0) Standard		
Image: Select Profile(s)       FXOS AAA Rule       If       FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS       then       Select Profile(s)       FXOS_AAA_Shell         Image: Select Profile(s)       FXOS Operations Rule       If       FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS       then       Select Profile(s)       FXOS_Operations_Shell         Image: Select Profile(s)       FXOS Read Only Rule       If       FXOS Read Only AND DEVICE:Device Type       then       Select Profile(s)       FXOS_ReadOnly_Shell	Status Rule Name V V FXOS Admin Rule	Conditions (identity groups and other conditions) Command Sets Shell Profiles if FXOS ADMIN AND DEVICE:Device Type then Select an item FXOS_Admin_Profile EQUALS All Device Types#FXOS	
Image: State Stat	FXOS AAA Rule	if FXOS AAA AND DEVICE:Device Type then Select Profile(s) FXOS_AAA_Shell EQUALS All Device Types#FXOS	
FXOS Read Only Rule If FXOS Read Only AND DEVICE:Device Type then Select Profile(s) FXOS_ReadOnly_Shell	FXOS Operations Rule	if FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS then Select Profile(s) FXOS_Operations_Shell	
EQUALS AII DEVICE Types#FAOS	FXOS Read Only Rule	If FXOS Read Only AND DEVICE:Device Type then Select Profile(s) FXOS_ReadOnly_Shell EQUALS All Device Types#FXOS	
Tacacs_Default If no matches, then Select Profile(s) Deny All Shell Profile	Tacacs_Default	if no matches, then Select Profile(s) Deny All Shell Profile	



# Verificación

Ahora puede probar cada usuario y verificar la función de usuario asignada.

## Verificación de FXOS Chasis

1. Telnet o SSH al chasis FXOS e inicie sesión con cualquiera de los usuarios creados en ISE.

Nombre de usuario: fxosadmin

Contraseña

fpr4120-TAC-A# scope security

fpr4120-TAC-A /security # show remote-user detail

Usuario remoto fxosaaa:

Descripción:

Funciones de usuario:

Nombre: aaa

Nombre: sólo lectura

Usuario remoto fxosadmin:

Descripción:

Funciones de usuario:

Nombre: admin

Nombre: sólo lectura

Fxosoper Usuario remoto:

Descripción:

Funciones de usuario:

Nombre: operaciones

Nombre: sólo lectura

Usuario remoto fxosro:

Descripción:

Funciones de usuario:

Nombre: sólo lectura

Según el nombre de usuario introducido, la cli del chasis FXOS sólo mostrará los comandos autorizados para el rol de usuario asignado.

Admin User Role (Función de usuario de administrador).

fpr4120-TAC-A /security #?

Reconocimiento

clear-user-sessions Clear User Sessions

Crear objetos administrados

eliminar objetos administrados

inhabilitar servicios

enable Habilita servicios

introducir un objeto administrado

scope Cambia el modo actual

establecer valores de propiedad

show Show system information

finalizar sesiones cimc activas

fpr4120-TAC-A# connect fxos

fpr4120-TAC-A (fxos)# debug aaa-requests

fpr4120-TAC-A (fxos)#

Función de usuario de sólo lectura.

fpr4120-TAC-A /security #?

scope Cambia el modo actual

establecer valores de propiedad

show Show system information

fpr4120-TAC-A# connect fxos

fpr4120-TAC-A (fxos)# debug aaa-requests

% Permiso denegado para la función

2. Busque la dirección IP del chasis FXOS e inicie sesión con cualquiera de los usuarios creados en ISE.

Admin User Role (Función de usuario de administrador).

Overview Interfaces Lo	gical	Devices	Secur	ity Engine	Platform	Setting	5					
NTP		LDAP	RADIUS	TACACS								
SSH SNMP HTTPS		Propertie Timeout:	s :* 5	Secs								
Syslog DNS		TACACS	Providers					Add TACACS Provi	der		ĩ×	Add
FIPS and Common Criteria Access List		Hostna	ime			(	rder	Hostname/FQDN(or IP Ac	ddress):*		]	
		10.88.2	44.50			1		Order:*		lowest-available		<i>d</i>
								Key:			Set:No	
								Confirm Key:			]	
								Port:*		49		
								Timeout:*		5 Secs		
										ок	ancel	
		Save	Cancel									

Función de usuario de sólo lectura.

ven	view Interfaces	Logical I	Devices Security E	ngine Platform Settings			
NTP			LDAP RADIUS	circis 🛛			
558	9		Properties				
HTT	PS .		Timeout:* 5	Secs			
Sys	og		TACACS Providers				
ON	and Common Criteria						Q A66
Aco	iss List		Hostname	On	der	Pert	
			10.88.244.50	1		49	9,8

Nota: Observe que el botón ADD está atenuado.

#### Verificación de ISE 2.0

1. Navegue hasta **Operaciones > Enlace TACACS.** Debería poder ver intentos exitosos y fallidos.

-th-sh- cited Identity Services Engine Home + Context Visibility -Operations + Policy + Administration + Work Centers									o o		
RADIUS Threat-Centric NAC Live Logs      TACACS      Trubieshoot      Adaptive Network Control Reports     Chick base to do windless solution and visibility solution Control											
Live Logs											o ayan.
	Refresh Never • Show Latest 20 records • Within									Last 3 hour	s •
C Refresh 💆 Exp	ort To 🕶									¥ Filter •	0-
Logged Time		Status	Details	Username	Туре	Authentication Policy	Authorization Policy	Failure Reason	Matched Comma	Shell Profile	D
×			·	Username	-	Authentication Policy	Authorization Policy	Failure Reason	Matched Command S	Shell Profile	
Jan 17, 2018 08:	7:23.272 PM	<b>1</b>	ò	fxosadmin	Authorization		Tacacs_Default >> FXOS Admin Rule			FXOS_Admir	n_Profile
Jan 17, 2018 08:	7:22.852 PM	<b>2</b>	0	fxosadmin	Authentication	Tacacs_Default >> Default >> Default					
Jan 17, 2018 08:	7:10.829 PM	•	0	fxosadmin	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared			
Jan 17, 2018 08:	7:01.069 PM	2		fxosro	Authorization		Tacacs_Default >> FXOS Read Only			FXOS_Read	Only_S
Jan 17, 2018 08:	7:00.825 PM	<b>2</b>	0	fxosro	Authentication	Tacacs_Default >> Default >> Default					
Jan 17, 2018 08:	6:50.888 PM	•	0	fxosro	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared			

# Troubleshoot

Para depurar la autenticación y autorización AAA, ejecute los siguientes comandos en el cli FXOS.

fpr4120-TAC-A# connect fxos

fpr4120-TAC-A (fxos)# debug aaa-requests

fpr4120-TAC-A (fxos)# debug aaa event

fpr4120-TAC-A (fxos)# debug aaa errors

#### fpr4120-TAC-A (fxos)# plazo mon

Después de un intento de autenticación exitoso, verá el siguiente resultado.

2018 17 ene 15:46:40.305247 aaa: aaa\_req\_process para autenticación. session no 0

2018 17 ene 15:46:40.305262 aaa: aaa\_req\_process: Solicitud AAA general de appln: login appln\_subtype: predeterminado

2018 17 ene 15:46:40.305271 aaa: try\_next\_aaa\_method

2018 17 ene 15:46:40.305285 aaa: total de métodos configurados es 1, el índice actual que se probará es 0

2018 17 ene 15:46:40.305294 aaa: handle\_req\_using\_method

2018 17 ene 15:46:40.305301 aaa: AAA\_METHOD\_SERVER\_GROUP

2018 17 ene 15:46:40.305308 aaa: aaa\_sg\_method\_handler group = tacacs

2018 17 ene 15:46:40.305315 aaa: Uso de sg\_protocol que se pasa a esta función

2018 17 ene 15:46:40.305324 aaa: Envío de una solicitud al servicio TACACS

2018 17 ene 15:46:40.305384 aaa: Grupo de métodos configurado correctamente

2018 17 ene 15:46:40.554631 aaa: aaa\_process\_fd\_set

2018 17 ene 15:46:40.555229 aaa: aaa\_process\_fd\_set: mtscallback en aaa\_q

2018 17 ene 15:46:40.555817 aaa: mts\_message\_response\_handler: una respuesta mts

2018 17 ene 15:46:40.556387 aaa: prot\_daemon\_reponse\_handler

2018 17 ene 15:46:40.557042 aaa: sesión: 0x8dfd68c eliminado de la tabla de sesiones 0

2018 17 ene 15:46:40.557059 aaa: is\_aaa\_resp\_status\_éxito status = 1

2018 17 ene 15:46:40.557066 aaa: is\_aaa\_resp\_status\_éxito es VERDADERO

2018 17 ene 15:46:40.557075 aaa: aaa\_send\_client\_response para autenticación. session->indicadores=21. aaa\_resp->indicadores=0.

2018 17 ene 15:46:40.557083 aaa: AAA\_REQ\_FLAG\_NORMAL

2018 17 ene 15:46:40.557106 aaa: mts\_send\_response satisfactoria

2018 17 ene 15:46:40.557364 aaa: aaa\_req\_process para autorización. session no 0

2018 17 ene 15:46:40.557378 aaa: aaa\_req\_process llamado con contexto desde appln: login appln\_subtype: default authen\_type:2, authen\_method: 0

2018 17 ene 15:46:40.557386 aaa: aaa\_send\_req\_using\_context

2018 17 ene 15:46:40.557394 aaa: aaa\_sg\_method\_handler group = (nulo)

2018 17 ene 15:46:40.557401 aaa: Uso de sg\_protocol que se pasa a esta función

2018 17 ene 15:46:40.557408 aaa: solicitud AAA dirigida o basada en el contexto(excepción: no es una solicitud de relay). No aceptará copia de una solicitud

2018 17 ene 15:46:40.557415 aaa: Envío de una solicitud al servicio TACACS

2018 17 ene 15:46:40.801732 aaa: aaa\_send\_client\_response para autorización. session->indicadores=9. aaa\_resp->indicadores=0.

2018 17 ene 15:46:40.801740 aaa: AAA\_REQ\_FLAG\_NORMAL

2018 17 ene 15:46:40.801761 aaa: mts\_send\_response satisfactoria

2018 17 ene 15:46:40.848932 aaa: ANTIGUO OPCODE: accounting\_interina\_update

2018 17 ene 15:46:40.848943 aaa: aaa\_create\_local\_acct\_req: user=, session\_id=, log=usuario agregado:fxosadmin a la función:admin

2018 17 ene 15:46:40.848963 aaa: aaa\_req\_process para contabilidad. session no 0

2018 17 ene 15:46:40.848972 aaa: La referencia de solicitud MTS es NULL. solicitud LOCAL

2018 17 ene 15:46:40.848982 aaa: Configuración de AAA\_REQ\_RESPONSE\_NOT\_NEEDED

2018 17 ene 15:46:40.848992 aaa: aaa\_req\_process: Solicitud AAA general de appln: appln\_subtype predeterminado: predeterminado

2018 17 ene 15:46:40.849002 aaa: try\_next\_aaa\_method

2018 17 ene 15:46:40.849022 aaa: no hay métodos configurados para el valor predeterminado

2018 17 ene 15:46:40.849032 aaa: no hay configuración disponible para esta solicitud

2018 17 ene 15:46:40.849043 aaa: try\_fallback\_method

2018 17 ene 15:46:40.849053 aaa: handle\_req\_using\_method

2018 17 ene 15:46:40.849063 aaa: local\_method\_handler

2018 17 ene 15:46:40.849073 aaa: aaa\_local\_accounting\_msg

2018 17 ene 15:46:40.849085 aaa: actualización::usuario agregado:fxosadmin a la función:admin

Después de un intento fallido de autenticación, verá el siguiente resultado.

2018 17 ene 15:46:17.836271 aaa: aaa\_req\_process para autenticación. session no 0

2018 17 ene 15:46:17.836616 aaa: aaa\_req\_process: Solicitud AAA general de appln: login appln\_subtype: predeterminado

2018 17 ene 15:46:17.837063 aaa: try\_next\_aaa\_method

2018 17 ene 15:46:17.837416 aaa: total de métodos configurados es 1, el índice actual que se probará es 0

2018 17 ene 15:46:17.837766 aaa: handle\_req\_using\_method

2018 17 ene 15:46:17.838103 aaa: AAA\_METHOD\_SERVER\_GROUP

2018 17 ene 15:46:17.838477 aaa: aaa\_sg\_method\_handler group = tacacs

2018 17 ene 15:46:17.838826 aaa: Uso de sg\_protocol que se pasa a esta función

2018 17 ene 15:46:17.839167 aaa: Envío de una solicitud al servicio TACACS

2018 17 ene 15:46:17.840225 aaa: Grupo de métodos configurado correctamente

2018 17 ene 15:46:18.043710 aaa: is\_aaa\_resp\_status\_éxito status = 2

2018 17 ene 15:46:18.044048 aaa: is\_aaa\_resp\_status\_éxito es VERDADERO

2018 17 ene 15:46:18.044395 aaa: aaa\_send\_client\_response para autenticación. session->indicadores=21. aaa\_resp->indicadores=0.

2018 17 ene 15:46:18.044733 aaa: AAA\_REQ\_FLAG\_NORMAL

2018 17 ene 15:46:18.045096 aaa: mts\_send\_response satisfactoria

2018 17 ene 15:46:18.045677 aaa: aaa\_cleanup\_session

2018 17 ene 15:46:18.045689 aaa: mts\_drop of request msg

2018 17 ene 15:46:18.045699 aaa: aaa\_req debe ser liberado.

2018 17 ene 15:46:18.045715 aaa: aaa\_process\_fd\_set

2018 17 ene 15:46:18.045722 aaa: aaa\_process\_fd\_set: mtscallback en aaa\_q

2018 17 ene 15:46:18.045732 aaa: aaa\_enable\_info\_config: mensaje de error GET\_REQ for aaa login

2018 17 ene 15:46:18.045738 aaa: devuelve el valor devuelto de la operación de configuración:elemento de seguridad desconocido

## Información Relacionada

El comando Ethanalyzer en FX-OS cli solicitará una contraseña cuando la autenticación TACACS/RADIUS esté habilitada. Este comportamiento es causado por un error.

ID de la falla: <u>CSCvg87518</u>