

Configuración de TACACS+ Device Administration en Palo Alto con ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Flujo de autenticación](#)

[Configurar](#)

[Sección 1: Configuración del firewall de Palo Alto para TACACS+](#)

[Sección 2: Configuración de TACACS+ en ISE](#)

[Verificación](#)

[Revisión de ISE](#)

[Resolución de problemas](#)

[TACACS: Paquete de solicitud TACACS+ no válido: posiblemente secretos compartidos no coincidentes](#)

[Problema](#)

[Posibles Causas](#)

[Solución](#)

Introducción

Este documento describe la configuración de TACACS+ en Palo Alto con Cisco ISE.

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ISE y protocolo TACACS+.
- Firewall de Palo Alto.

Componentes Utilizados

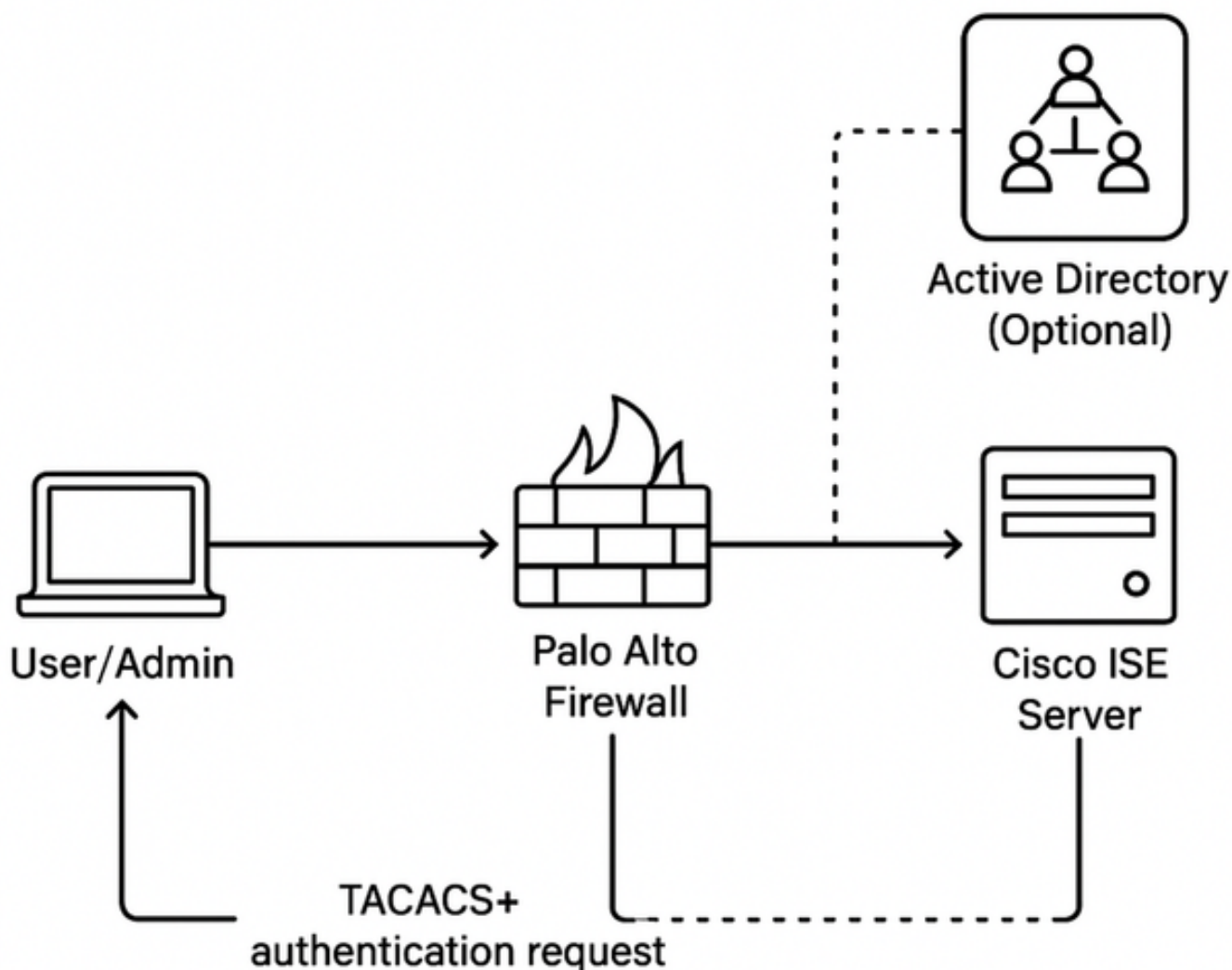
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Palo Alto Firewall versión 10.1.0
- Parche 4 de Cisco Identity Services Engine (ISE) versión 3.3

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.

Diagrama de la red



Flujo de autenticación

1. El administrador inicia sesión en el firewall de Palo Alto.
2. Palo Alto envía una solicitud de autenticación TACACS+ a Cisco ISE.
3. Cisco ISE:
 - Si AD está integrado, solicita autenticación y autorización a AD.
 - Si no hay AD, usa almacenes de identidad o políticas locales.
 - Cisco ISE envía una respuesta de autorización a Palo Alto en función de las políticas configuradas.
 - El administrador obtiene acceso con el nivel de privilegio adecuado.

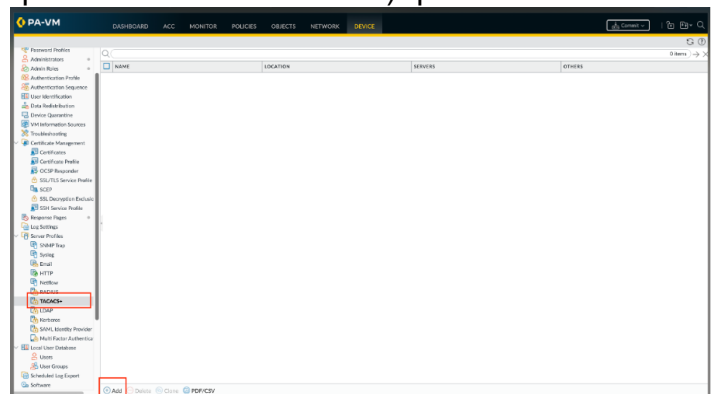
Configurar

Sección 1: Configuración de Palo Alto Firewall para TACACS+

Paso 1. Agregue un perfil de servidor TACACS+.

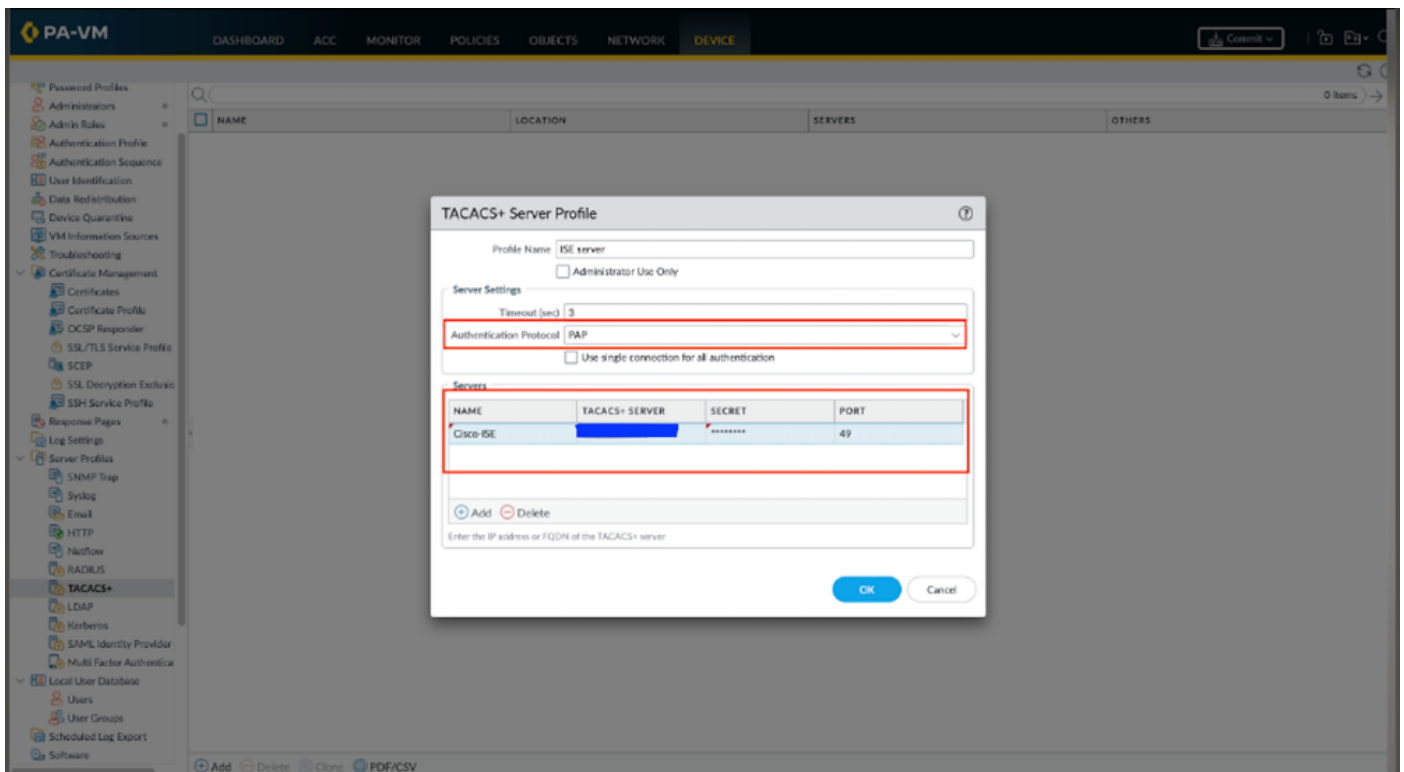
El perfil define cómo el firewall se conecta al servidor TACACS+.

1. Seleccione Device > Server Profiles > TACACS+ or Panorama > Server Profiles > TACACS+ en Panorama y Add a profile.
2. Introduzca un nombre de perfil para identificar el perfil de servidor.
3. (Opcional) Seleccione Administrator Use Only para restringir el acceso a los administradores.
4. Introduzca un intervalo de tiempo de espera en segundos tras el cual se agotará el tiempo de espera de una solicitud de autenticación (el valor predeterminado es 3; es de 1 a 20).
5. Seleccione el protocolo de autenticación (el predeterminado es CHAP) que el firewall utiliza



para autenticarse en el servidor TACACS+.

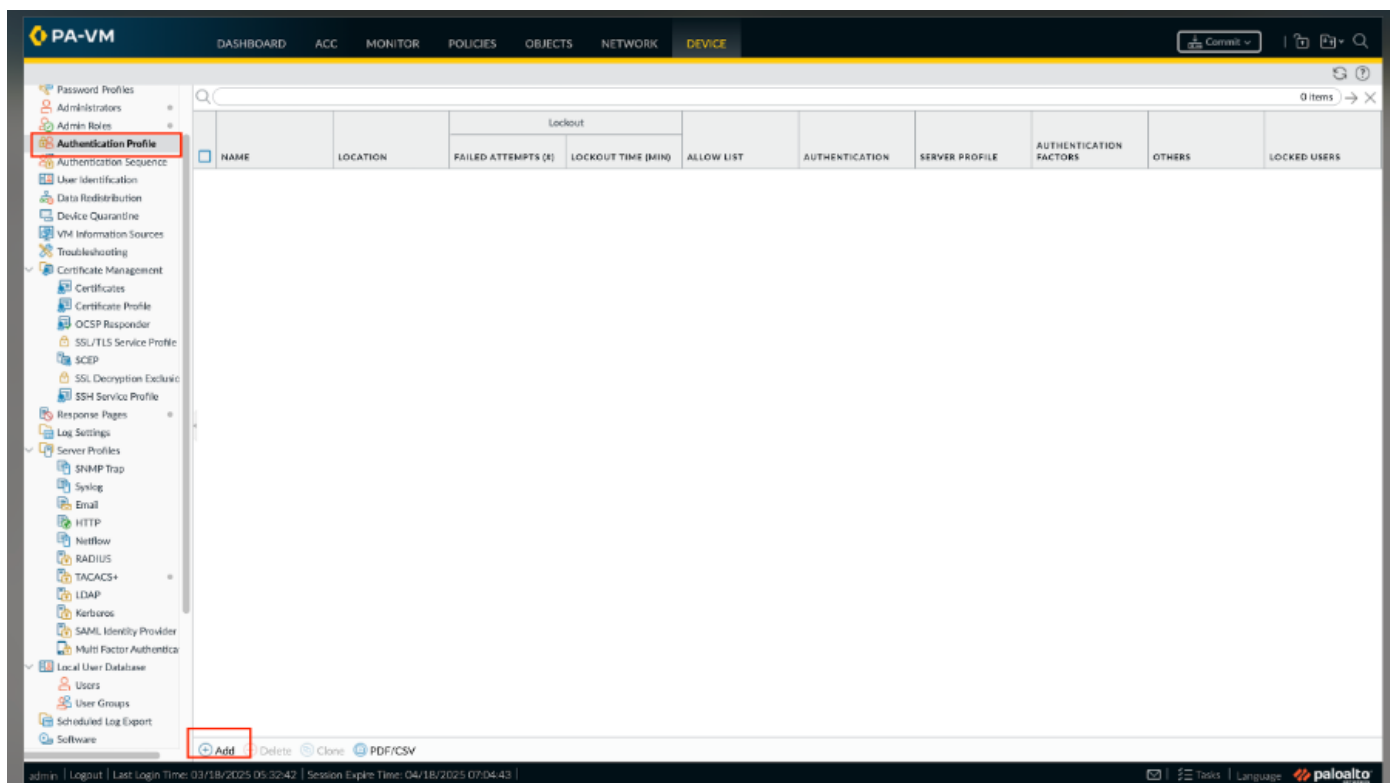
6. Agregue cada servidor TACACS+ y realice estos pasos:
 1. Un Nombre para identificar el servidor.
 2. La dirección IP o FQDN del servidor TACACS+. Si utiliza un objeto de dirección FQDN para identificar el servidor y posteriormente cambia la dirección, debe confirmar el cambio para que la nueva dirección del servidor surta efecto.
 3. Secreto y Confirmar secreto para cifrar nombres de usuario y contraseñas.
 4. El puerto del servidor para las solicitudes de autenticación (el valor predeterminado es 49). Haga clic en Aceptar para guardar el perfil de servidor.
7. Haga clic en Aceptar para guardar el perfil de servidor.



Paso 2. Asigne el perfil de servidor TACACS+ a un perfil de autenticación.

El perfil de autenticación define las opciones de autenticación que son comunes a un conjunto de usuarios.

1. Seleccione Device > Authentication Profile y Add a profile.
 1. Introduzca un nombre para identificar el perfil
 2. Establezca el Tipo en TACACS+.
 3. Seleccione el perfil de servidor que ha configurado.
 4. Seleccione Recuperar grupo de usuarios de TACACS+ para recopilar información de grupo de usuarios de VSA definidos en el servidor TACACS+.



Authentication Profile

Name: Cisco-AAA-Auth Profile

Authentication | Factors | Advanced

Type: TACACS+

Server Profile: ISE server

User Domain: New TACACS+ Profile

Username Modifier: %USERINPUT%

Single Sign On

Kerberos Realm:

Kerberos Keytab: Click "Import" to configure this field [X Import](#)

OK Cancel

El firewall hace coincidir la información del grupo mediante los grupos especificados en la Lista de permitidos del perfil de autenticación.

1. Seleccione Advanced y en la Lista de permitidos, Add los usuarios y grupos que pueden autenticarse con este perfil de autenticación.
2. Haga clic en Aceptar para guardar el perfil de autenticación.

Authentication Profile ?

Name

Authentication | Factors | **Advanced**

Allow List

☐	ALLOW LIST ^
☒	 all

☒ **Add** ☐ **Delete**

Account Lockout

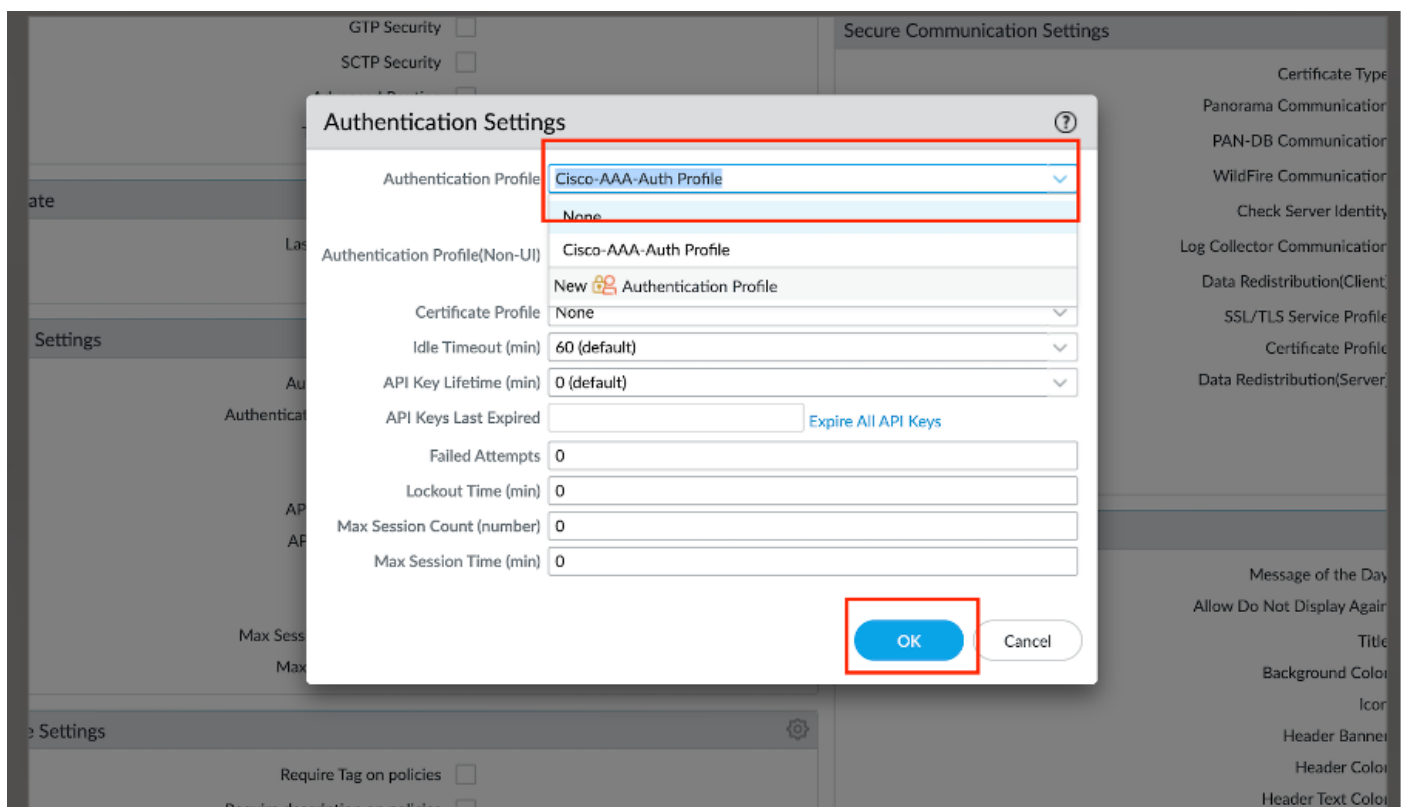
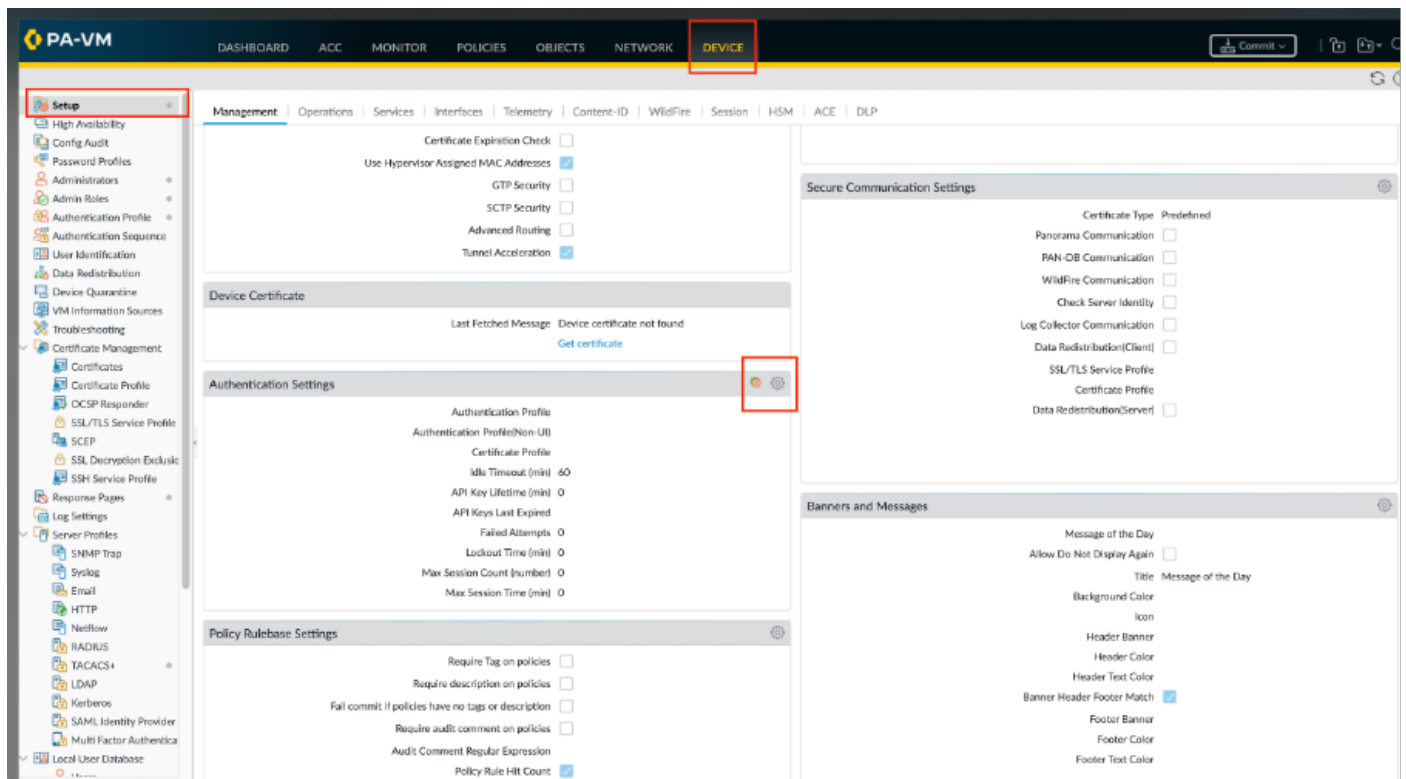
Failed Attempts

Lockout Time (min)

OK **Cancel**

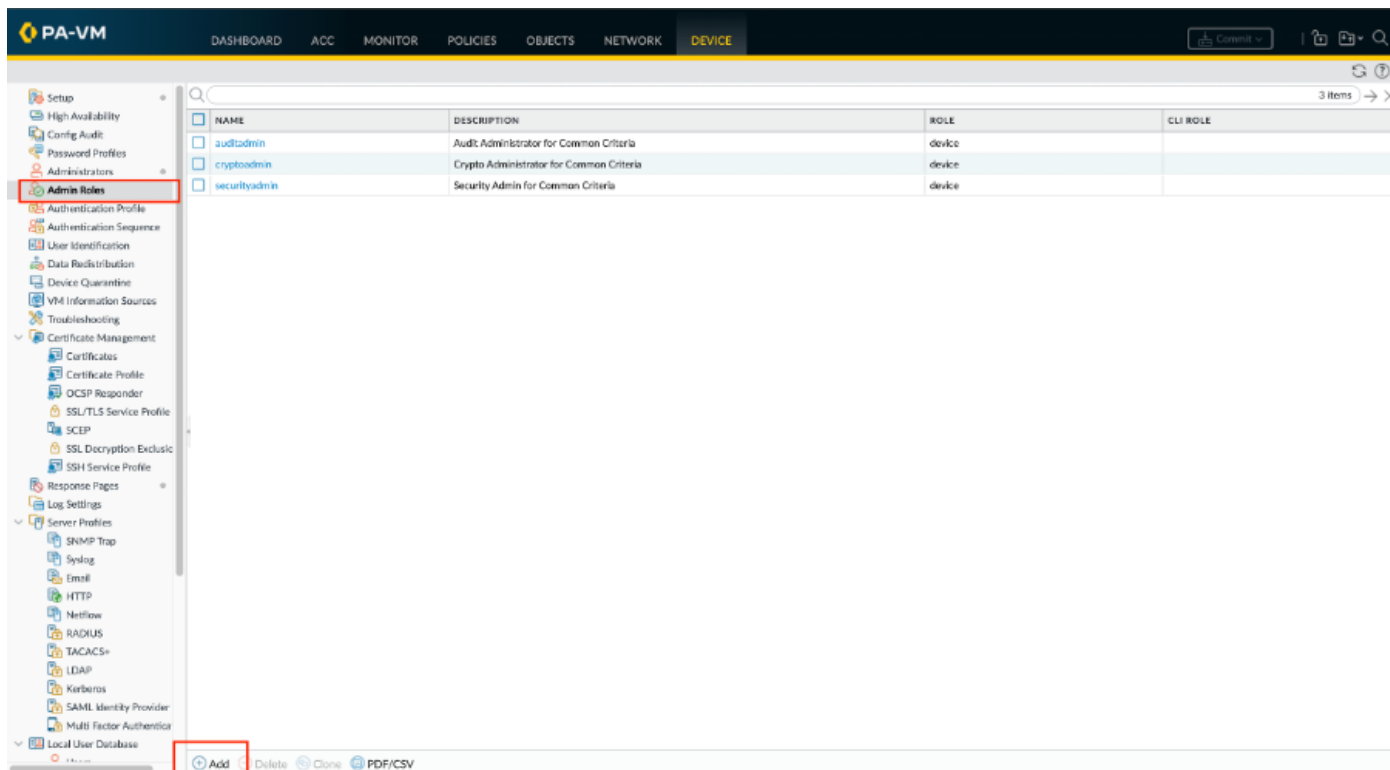
Paso 3. Configure el firewall para utilizar el perfil de autenticación para todos los administradores.

1. Seleccione Device > Setup > Management y edite los ajustes de autenticación.
2. Seleccione el perfil de autenticación que configuró y haga clic en Aceptar.

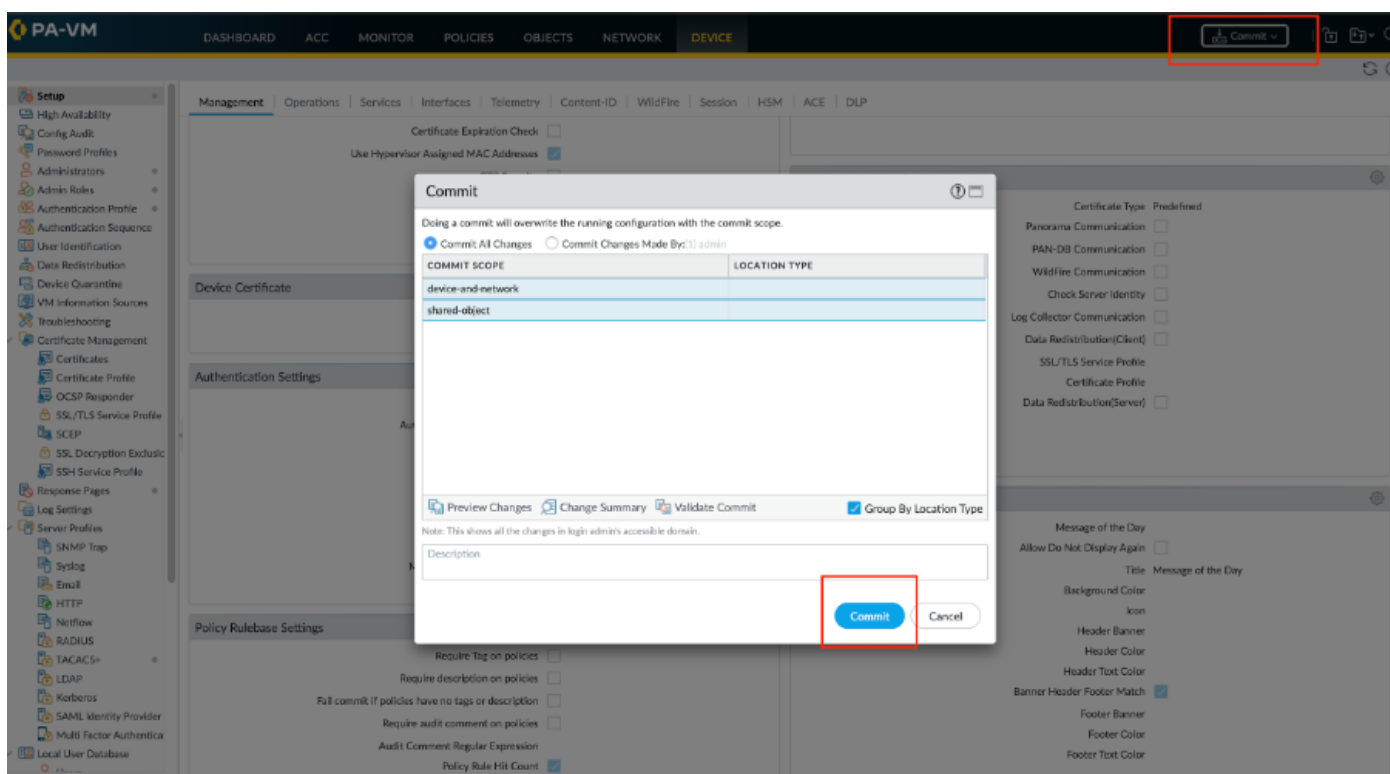


Paso 4. Configure un perfil de rol de administrador.

Seleccione Device > Admin Roles y haga clic en Add. Introduzca un nombre para identificar el rol.



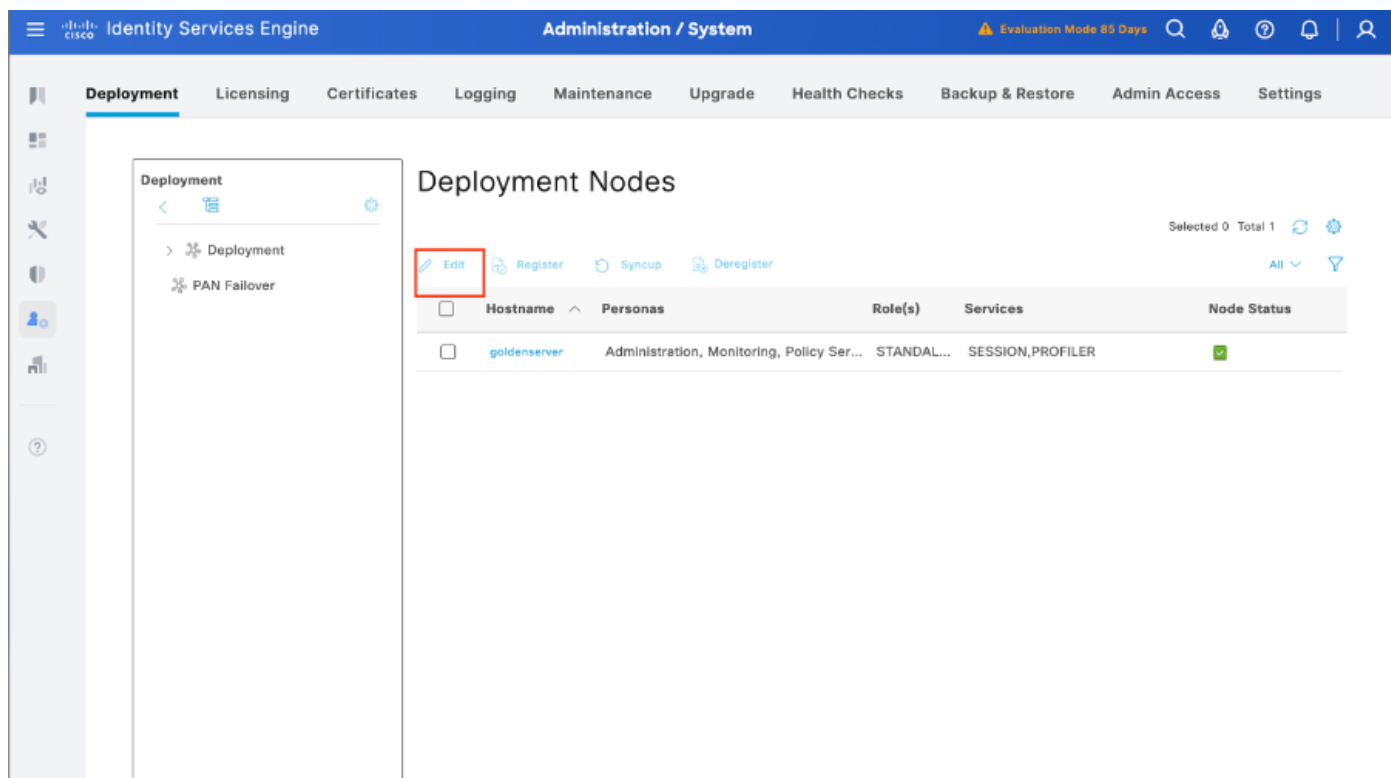
Paso 5. Realice los cambios para activarlos en el firewall.



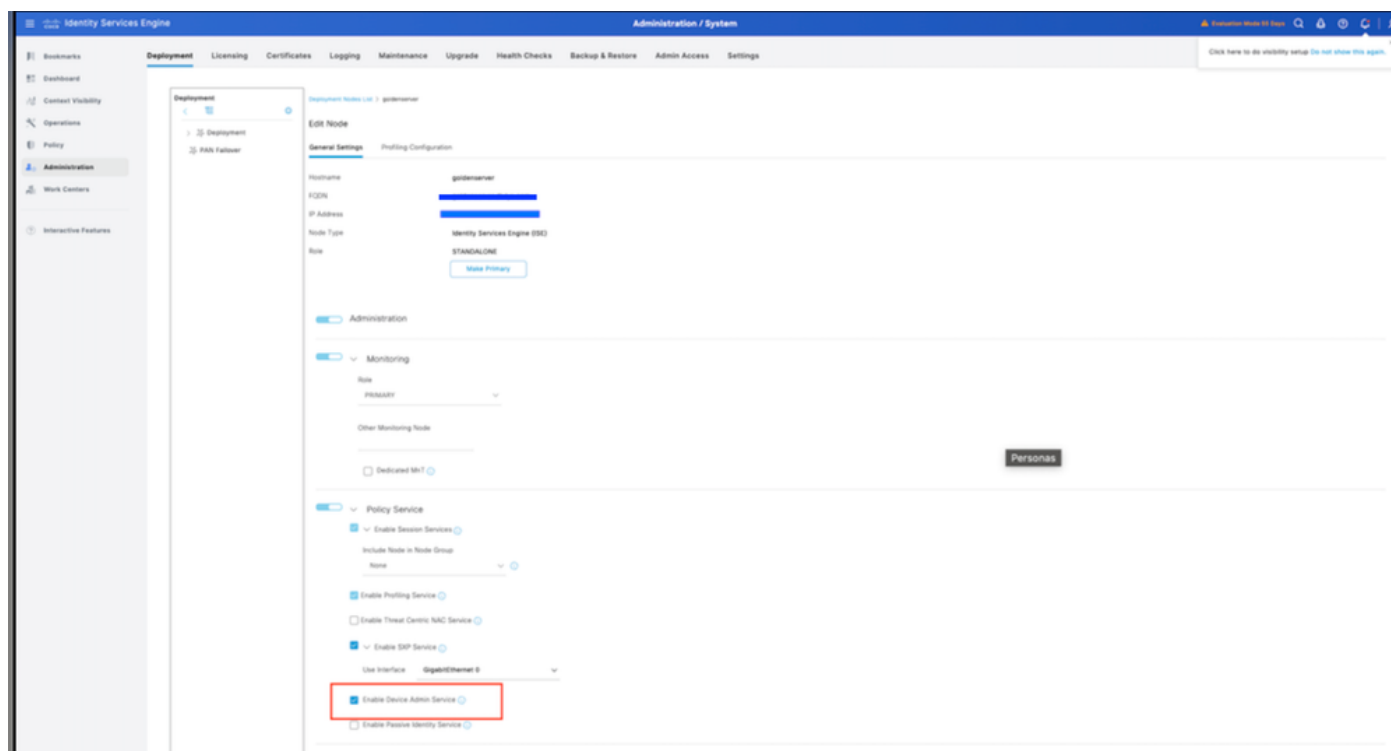
Sección 2: Configuración de TACACS+ en ISE

Paso 1. El paso inicial es verificar si Cisco ISE cuenta con las capacidades necesarias para gestionar la autenticación TACACS+. Para ello, confirme que el nodo de servicios de directivas (PSN) deseado tiene activada la función Device Admin Service. Vaya a Administration > System > Deployment, seleccione el nodo adecuado donde ISE procesa la autenticación TACACS+ y haga

clic en Edit para revisar su configuración.



Paso 2. Desplácese hacia abajo para localizar la función Device Administration Service. Tenga en cuenta que para activar esta función es necesario que el usuario del servicio de políticas esté activo en el nodo, junto con las licencias TACACS+ disponibles en la implementación. Seleccione la casilla de verificación para activar la función y, a continuación, guarde la configuración.



Paso 3. Configuración del perfil de dispositivo de red de Palo Alto para Cisco ISE.

Vaya a Administration > Network Resources > Network device profile. Haga clic en Agregar y mencione el nombre (Palo Alto) y habilite TACACS+ en los protocolos soportados.

Identity Services Engine Administration / Network Resources

Network Device Profiles

Name: Palo_Alto

Description:

Icon: Change icon... Set To Default

Vendor: Other

Supported Protocols:

- ☒ RADIUS
- ☒ TACACS+
- ☒ TrustSec

RADIUS Dictionary:

Templates:

- Expand All / Collapse All
- Authentication/Authorization
- Permissions
- Change of Authorization (CoA)
- Redirect
- Advanced

Summary

Based on this configuration, the following are supported:

- Services: Radius, TACACS, TrustSec, MAB, RADIUS
- CoA: Port Bounce (default CoA port: 3799, default DTLS CoA port: 2083)
- Native URL Redirect: Static

Save Reset

Paso 4. Agregue Palo Alto como dispositivo de red.

1. Vaya a Administración > Recursos de red > Dispositivos de red > +Agregar.

Identity Services Engine Administration / Network Resources

Network Devices

Network Devices

Default Device

Device Security Settings

Network Devices

Selected 0 Total 0

Edit + Add Duplicate Import Export Generate PAC

Name	IP/Mask	Profile Name	Location	Type
No data available				

2. Haga clic en Agregar e ingrese estos detalles:

Nombre: Palo Alto

IP Address: <IP de Palo-Alto>

Perfil de dispositivo de red: select Palo Alto

Configuración de autenticación TACACS:

Habilitar autenticación TACACS+

Introduzca la clave secreta compartida (debe coincidir con la configuración de Palo Alto)

Click Save.

The screenshot displays the 'Network Devices' configuration page in the Palo Alto Networks Identity Services Engine (ISE) interface. The page is titled 'Administration / Network Resources'. The left sidebar shows the navigation menu with 'Administration' selected. The main content area shows the configuration for a device named 'Palo_Alto_Firewall'. The 'Device Profile' is set to 'Palo_Alto'. The 'TACACS Authentication Settings' section is expanded, showing the 'Shared Secret' field with a 'Show' button and a 'Retire' button. The 'Save' button is located at the bottom right of the page.

Paso 5. Crear grupos de identidad de usuarios.

Navegue hasta Centros de trabajo > Administración de dispositivos > Grupos de identidades de usuario, luego haga clic en Agregar y especifique el nombre para el grupo de usuarios.

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 94 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

More

Identity Groups

EQ

< > ⚙

> Endpoint Identity Groups

> User Identity Groups

User Identity Groups > Security Engineers

Identity Group

* Name Security Engineers

Identity group for Palo Alto

Description

Save Reset

Member Users

Users

Selected 0 Total 1

+ Add - Delete

All

Status: Sortable

Email Username First Nam

Enabled divz

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 94 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Settings

Network Access Service > diverz

Network Access User

* Username divz

Status Enabled

Account Name/Id

Email

Passwords

Password Type Internal Users

Password Lifetime

With Expiration Never Expires

Password

Re-Enter Password

Generate Password

Enable Password

Generate Password

User Information

First Name

Last Name

Account Options

Description

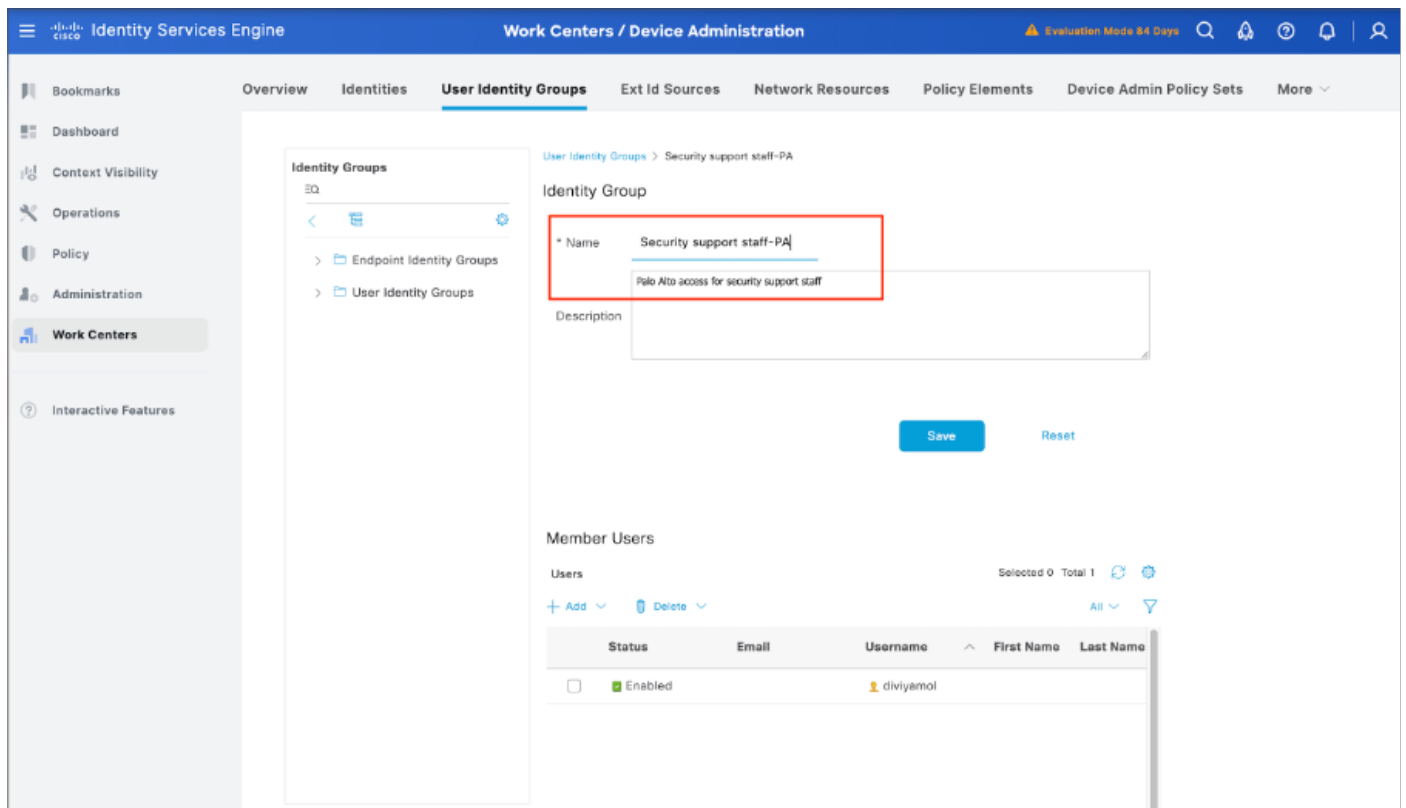
Change password on next sign

Account Disable Policy

Disable account if date exceeds 2023-03-19

User Groups

Security support staff PK



Paso 6. Configure Un Perfil TACACS.

Lo siguiente que debe hacer es configurar un perfil TACACS, que es donde puede configurar parámetros como el nivel de privilegio y el tiempo de espera. Vaya a Centros de trabajo > Administración de dispositivos -> Elementos de política -> Resultados -> Perfiles TACACS.

Haga clic en Agregar para crear un nuevo perfil TACACS. Dé un buen nombre al perfil.

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets Reports Settings

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

Conditions TACACS Profiles > New TACACS Profile

Network Conditions

Results Name PaloAlto_Security_Support

Allowed Protocols TACACS Command Sets TACACS Profiles

Description

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

Default Privilege 0 (Select 0 to 15)

Maximum Privilege 15 (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout Minutes (0-9999)

Idle Time Minutes (0-9999)

Custom Attributes

Add Type Value

No data found.

Mandatory PaloAlto_Admin_Role Support

Cancel Save

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets Reports Settings

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

Conditions TACACS Profiles > PaloAlto_Engineers_Profile TACACS Profile

Network Conditions

Results Name PaloAlto_Engineers_Profile

Allowed Protocols TACACS Command Sets TACACS Profiles

Description

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

Default Privilege 0 (Select 0 to 15)

Maximum Privilege 15 (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout Minutes (0-9999)

Idle Time Minutes (0-9999)

Custom Attributes

Add Type Value

No data found.

Mandatory PaloAlto_Admin_Role securityadmin

Cancel Save

Paso 6. Configure los Conjuntos de Comandos TACACS.

Ahora, es el momento de configurar qué comandos pueden utilizar los usuarios. Dado que puede

otorgar a ambos casos de uso el Nivel de Privilegio 15, que da acceso a todos los comandos disponibles, utilice los Conjuntos de Comandos TACACS para limitar los comandos que se pueden utilizar.

Vaya a Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados - > Conjuntos de comandos TACACS. Haga clic en Agregar para crear un nuevo conjunto de comandos TACACS y denominarlo PermitAllCommands. Aplique este conjunto de comandos TACACS para el soporte de seguridad.

Lo único que necesita configurar en este conjunto de comandos TACACS es marcar la casilla Permit any command that is not listed below.

The screenshot displays the Identity Services Engine (ISE) interface, specifically the 'Work Centers / Device Administration' section. The left sidebar shows the navigation menu with 'Work Centers' selected. The main content area is divided into several tabs: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, and Device Admin Policy. The 'Policy Elements' tab is active, and the 'TACACS Command Sets' section is highlighted in the left sidebar. The 'PermitAllCommands' command set is being configured. The 'Name' field is set to 'PermitAllCommands'. The 'Description' field is empty. The 'Commands' section has the checkbox 'Permit any command that is not listed below' checked. The 'Add' button is visible. The 'Grant' checkbox is unchecked. The 'Command' and 'Arguments' columns are empty. The 'No data found.' message is displayed. The 'Save' button is highlighted in the bottom right corner.

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy

Click here to do visibility setup Do not show this again.

Conditions

Network Conditions

Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Command Sets > PermitAllCommands

Command Set

Name: PermitAllCommands

Description:

Commands

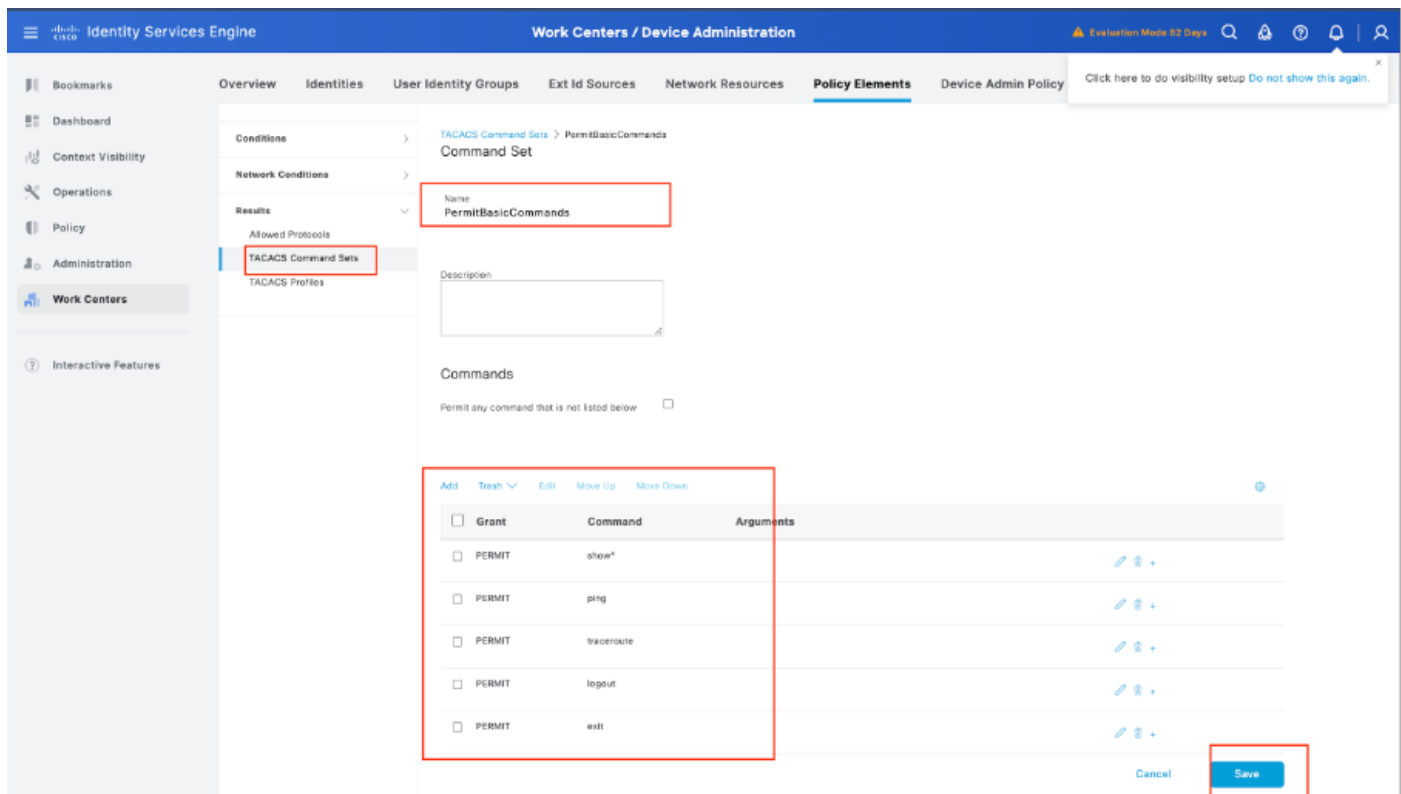
Permit any command that is not listed below ☒

Add Trash Edit Move Up Move Down

☐ Grant Command Arguments

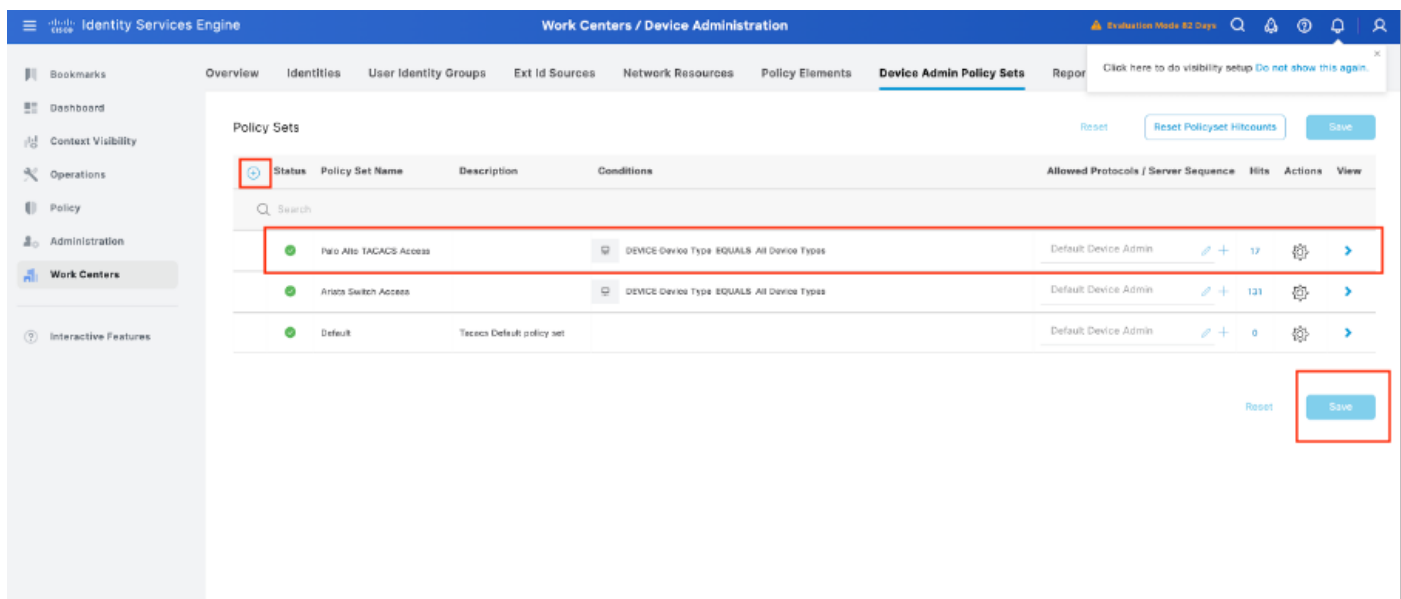
No data found.

Cancel Save



Paso 7. Cree un conjunto de políticas de administración de dispositivos para utilizarlo en Palo Alto. Navegue por el menú Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos, y haga clic en el icono Agregar +.

Paso 8. Dé un nombre a este nuevo conjunto de políticas, agregue condiciones en función de las características de las autenticaciones TACACS+ que se estén realizando desde el firewall de Palo Alto y seleccione Protocolos permitidos > Administrador de dispositivos predeterminado. Guarde la configuración.



Paso 9. Seleccione la opción > view y, a continuación, en la sección Authentication Policy (Política de autenticación), seleccione el origen de identidad externo que Cisco ISE utiliza para consultar el nombre de usuario y las credenciales para la autenticación en el firewall de Palo Alto. En este

ejemplo, las credenciales corresponden a los usuarios internos almacenados en ISE.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area is titled 'Work Centers / Device Administration' and shows the 'Policy Sets' section. Under 'Policy Sets', there is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. The table lists 'Palo Alto TACACS Access'. Below this, the 'Authentication Policy(2)' section is expanded, showing a table with columns: Status, Rule Name, Conditions, Use, Hits, and Actions. Two policies are listed: 'PaloAlto_Auth Policy' and 'Default'. The 'PaloAlto_Auth Policy' is selected, and its 'Options' are visible, showing 'Internal Users' and 'Options'. The 'Save' button is highlighted with a red box.

Paso 10. Desplácese hacia abajo hasta la sección denominada Authorization Policy (Directiva de autorización) hasta la directiva Default (Predeterminada), seleccione el icono de engranaje y, a continuación, inserte una regla arriba.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area is titled 'Work Centers / Device Administration' and shows the 'Policy Sets' section. Under 'Policy Sets', there is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. The table lists 'Palo Alto TACACS Access'. Below this, the 'Authorization Policy' section is expanded, showing a table with columns: Status, Rule Name, Conditions, Command Sets, Shell Profiles, Hits, and Actions. Three policies are listed: 'PA_FW_Auth Policy', 'PA_FW_Security policy', and 'Default'. The 'PA_FW_Auth Policy' is selected, and its 'Options' are visible, showing 'InternalUsers IdentityGroup EQUALS User Identity Group:Security support staff-PA' and 'Options'. The 'Save' button is highlighted with a red box.

Paso 11. Asigne un nombre a la nueva regla de autorización, agregue condiciones relativas al usuario que ya se ha autenticado como miembro del grupo y, en la sección Perfiles de shell,

agregue el perfil TACACS que configuró anteriormente y guarde la configuración.

Verificación

Revisión de ISE

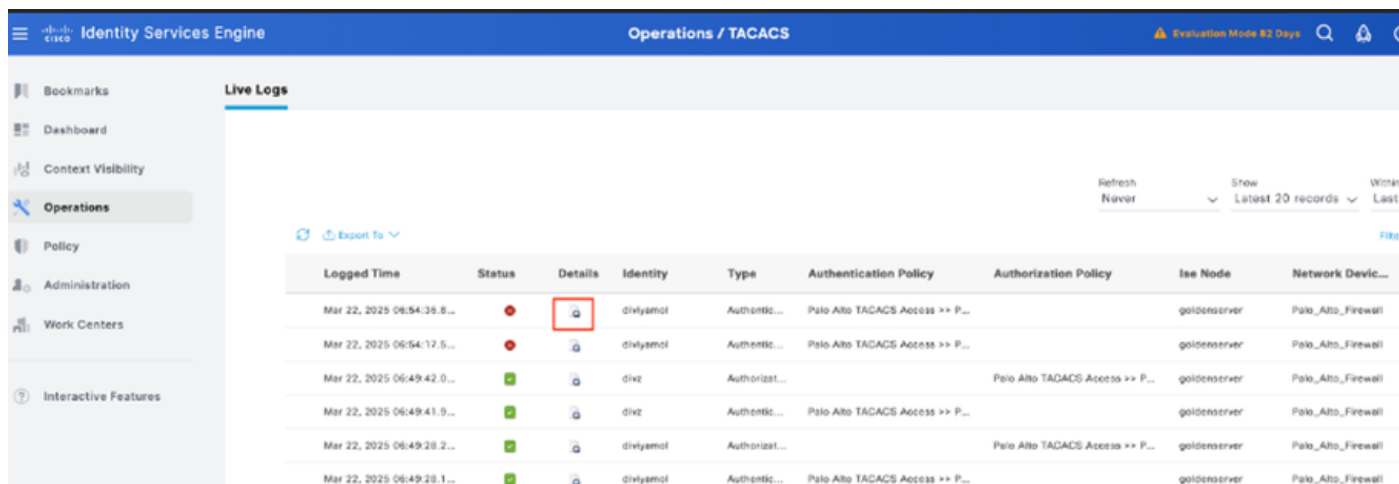
Paso 1. Revise si la capacidad de servicio de TACACS+ se está ejecutando, esto se puede registrar:

- GUI: Revise si el nodo aparece con el servicio DEVICE ADMIN en Administration -> System -> Deployment.
- CLI: Ejecute el comando show ports | incluir 49 para confirmar que hay conexiones en el puerto TCP que pertenecen a TACACS+

```
goldenserver/admin#show ports | include 49
tcp: [REDACTED]
```

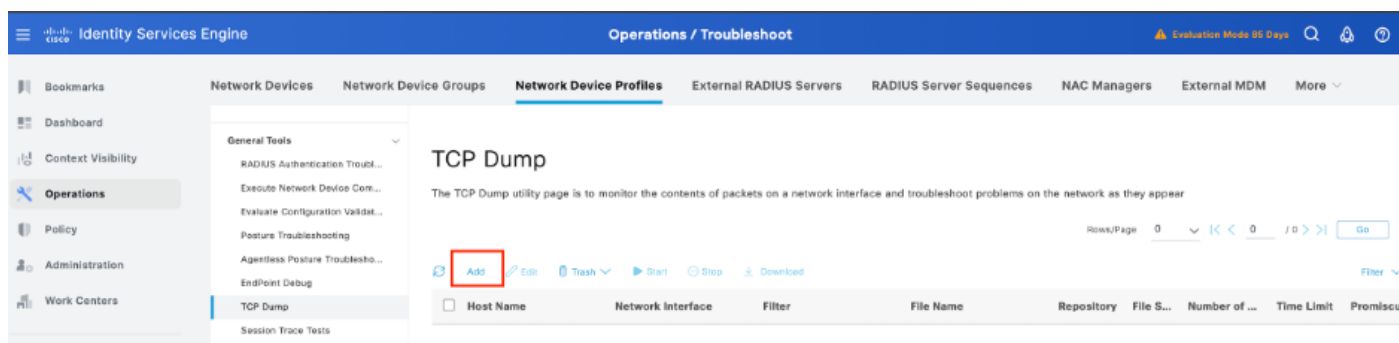
Paso 2. Confirme si hay registros en vivo relacionados con intentos de autenticación TACACS+ : esto se puede verificar en el menú Operations -> TACACS -> Live logs.

Dependiendo del motivo del fallo, puede ajustar la configuración o abordar la causa del fallo.



Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device
Mar 22, 2025 06:54:38.8...	Failed	[REDACTED]	diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:54:17.5...	Failed	[REDACTED]	diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:42.0...	Success	[REDACTED]	divi	Authorizat...		Palo Alto TACACS Access >> P...	goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:41.9...	Success	[REDACTED]	divi	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:28.2...	Success	[REDACTED]	diviyamol	Authorizat...		Palo Alto TACACS Access >> P...	goldenserver	Palo_Alto_Firewall
Mar 22, 2025 06:49:28.1...	Success	[REDACTED]	diviyamol	Authentic...	Palo Alto TACACS Access >> P...		goldenserver	Palo_Alto_Firewall

Paso 3. En caso de que no vea ningún registro en vivo, continúe con la captura de paquetes y navegue hasta el menú Operaciones > Solución de problemas > Herramientas de diagnóstico > Herramientas generales > Volcado TCP , seleccione Agregar.



Host Name	Network Interface	Filter	File Name	Repository	File S...	Number of ...	Time Limit	Promiscu
-----------	-------------------	--------	-----------	------------	-----------	---------------	------------	----------

Identity Services Engine Operations / Troubleshoot Evaluation Mode 85 Days

Network Devices Network Device Groups **Network Device Profiles** External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM pxGrid Direct Connectors More

General Tools

RADIUS Authentication Troubleshooting

Resolve Network Device Configuration Validation

Posture Troubleshooting

Agentless Posture Troubleshooting

Endpoint Debug

TCP Dump

Session Trace Tests

TrustSec Tools

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name* goldenserver

Network Interface* GigabitEthernet 0 [Up, Running]

Filter ip host

E.g: ip host 10.77.122.123 and not 10.177.122.119

File Name tcpdump_issue

Repository

File Size 10 Mb

Limit to 1 File(s)

Time Limit 5 Minute(s)

☐ Periodic Mode

Cancel Save Save and Run

Paso 4. Habilite el componente runtime-AAA en debug dentro de PSN desde donde se realiza la autenticación en Operaciones > Troubleshooting > Debug Wizard > Debug log configuration, seleccione el nodo PSN , luego seleccione next en el botón de edición .

Identity Services Engine Operations / Troubleshoot Evaluation Mode 85 Days

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration

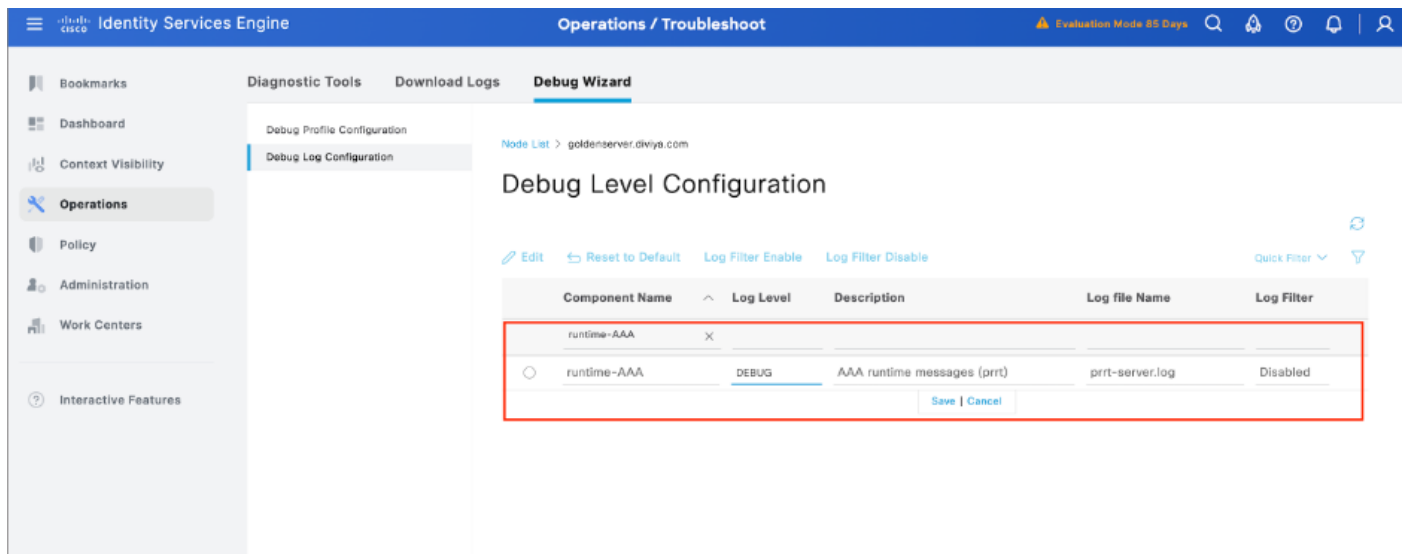
Debug Log Configuration

Node List

Selected 0 Total 1

Edit Reset to Default

Node Na...	Replication Role
goldenserver	STANDALONE



Identifique el componente runtime-AAA, establezca su nivel de registro en debug, reproduzca el problema y analice los registros para una investigación adicional.

Resolución de problemas

TACACS: Paquete de solicitud TACACS+ no válido: posiblemente secretos compartidos no coincidentes

Problema

La autenticación TACACS+ entre Cisco ISE y el firewall de Palo Alto (o cualquier dispositivo de red) falla con el mensaje de error:

"Paquete de solicitud TACACS+ no válido; posiblemente secretos compartidos no coincidentes"

Overview

Request Type	Authentication
Status	Fail
Session Key	goldenserver/532805123/143
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Username	
Authentication Policy	
Selected Authorization Profile	

Authentication Details

Generated Time	2025-05-13 20:16:26.897000 +05:30
Logged Time	2025-05-13 20:16:26.897
Epoch Time (sec)	1747147586
ISE Node	goldenserver
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Failure Reason	
Resolution	
Root Cause	
Username	
Network Device Name	

Esto evita los intentos de inicio de sesión administrativos exitosos y puede afectar el control de acceso del dispositivo a través de la autenticación centralizada.

Posibles Causas

- Una discordancia en el secreto compartido configurado en Cisco ISE y el firewall o dispositivo de red de Palo Alto.
- Configuración incorrecta del servidor TACACS+ en el dispositivo (como dirección IP, puerto o protocolo incorrecto).

Solución

Hay varias posibles soluciones para este problema:

1. Compruebe la clave secreta compartida:

- En Cisco ISE:
Vaya a Administration > Network Resources > Network Devices , seleccione el dispositivo afectado y confirme el secreto compartido.
- En el firewall de Palo Alto:
Vaya a Device > Server Profiles > TACACS+, y asegúrese de que el secreto compartido coincida exactamente, incluyendo mayúsculas y minúsculas y caracteres especiales.

2. Compruebe la configuración del servidor TACACS+:

- Asegúrese de que la dirección IP y el puerto correctos (el predeterminado es el 49) de Cisco ISE están configurados en el perfil TACACS+ del firewall.
- Confirme que el tipo de protocolo es TACACS+ (no RADIUS).

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).