

Configurar a administração de dispositivos TACACS+ em Palo Alto com ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Fluxo de autenticação](#)

[Configurar](#)

[Seção 1: Configurar o firewall Palo Alto para TACACS+](#)

[Seção 2: Configuração TACACS+ no ISE](#)

[Verificar](#)

[Revisão do ISE](#)

[Troubleshooting](#)

[TACACS: Pacote de solicitação TACACS+ inválido - Segredos compartilhados possivelmente incompatíveis](#)

[Problema](#)

[Possíveis causas](#)

[Solução](#)

Introdução

Este documento descreve a configuração TACACS+ em Palo Alto com o Cisco ISE.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo Cisco ISE e TACACS+.
- Firewall Palo Alto.

Componentes Utilizados

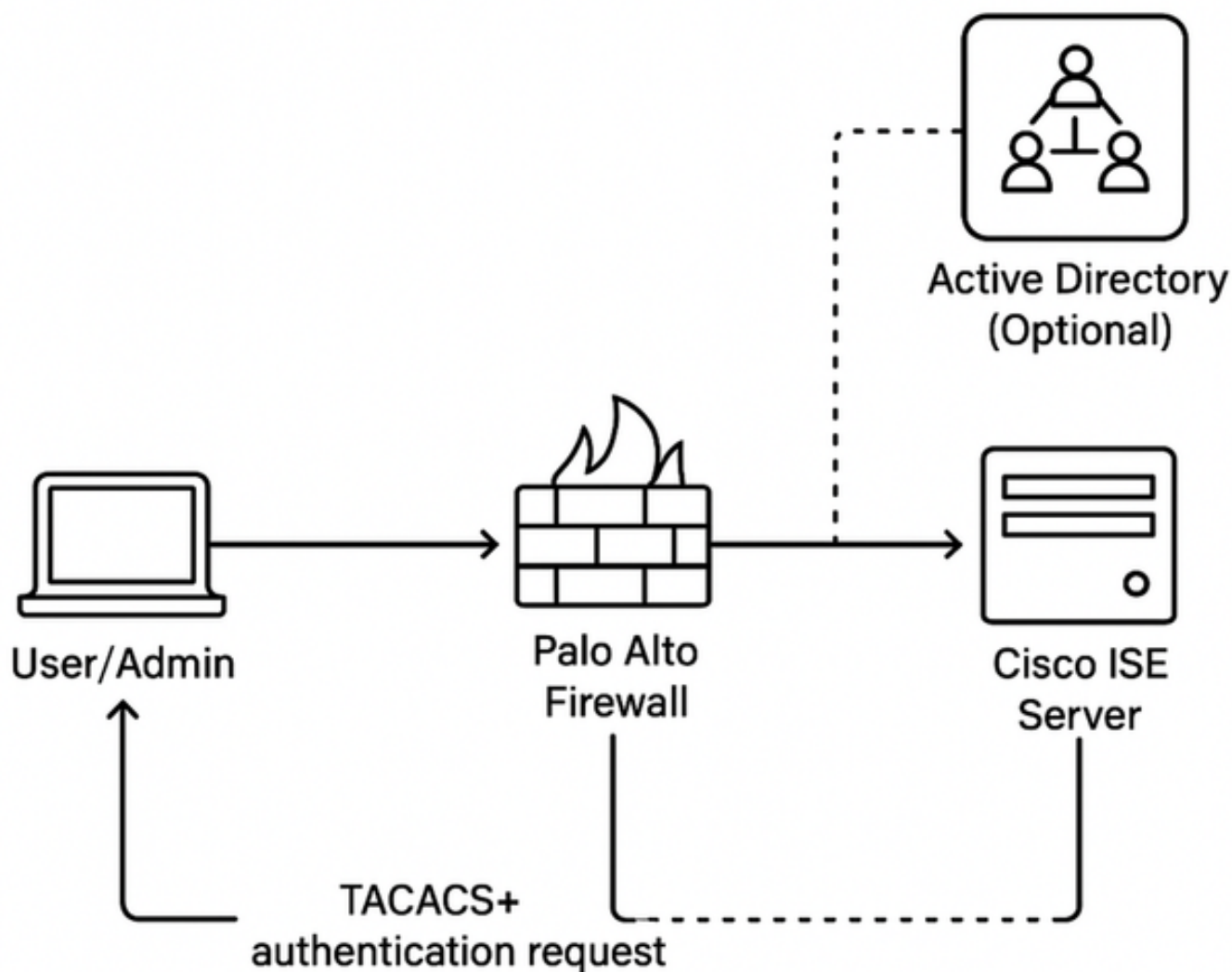
As informações neste documento são baseadas nestas versões de software e hardware:

- Palo Alto Firewall versão 10.1.0
- Cisco Identity Services Engine (ISE) versão 3.3 Patch 4

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de Rede



Fluxo de autenticação

1. O administrador faz login no firewall Palo Alto.
2. A Palo Alto envia uma solicitação de autenticação TACACS+ ao Cisco ISE.
3. Cisco ISE:
 - Se o AD estiver integrado, ele consultará o AD para autenticação e autorização.
 - Se não houver AD, ele usará repositórios ou políticas de identidade locais.
 - O Cisco ISE envia uma resposta de autorização para a Palo Alto com base nas políticas configuradas.
 - O administrador obtém acesso com o nível de privilégio apropriado.

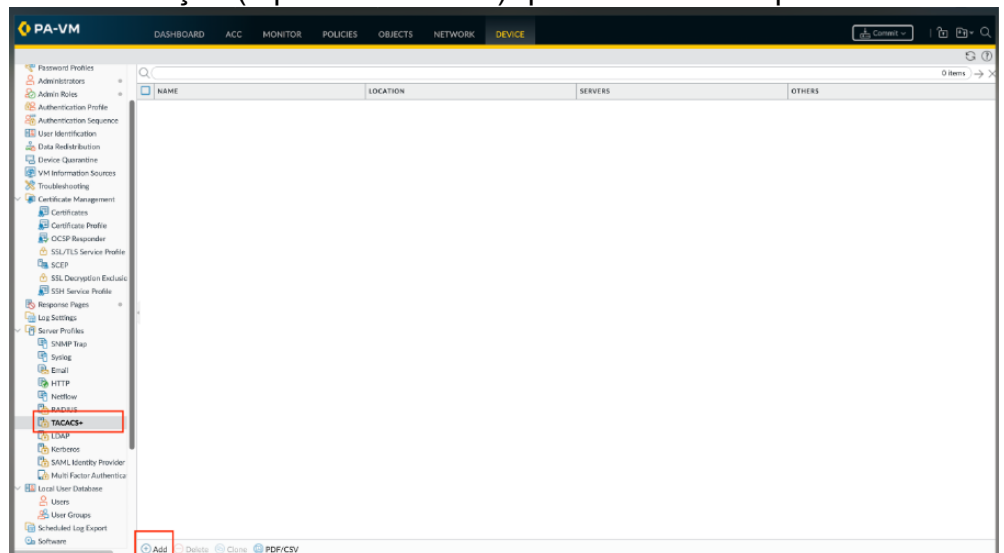
Configurar

Seção 1: Configurar o firewall Palo Alto para TACACS+

Etapa 1. Adicionar um perfil de servidor TACACS+.

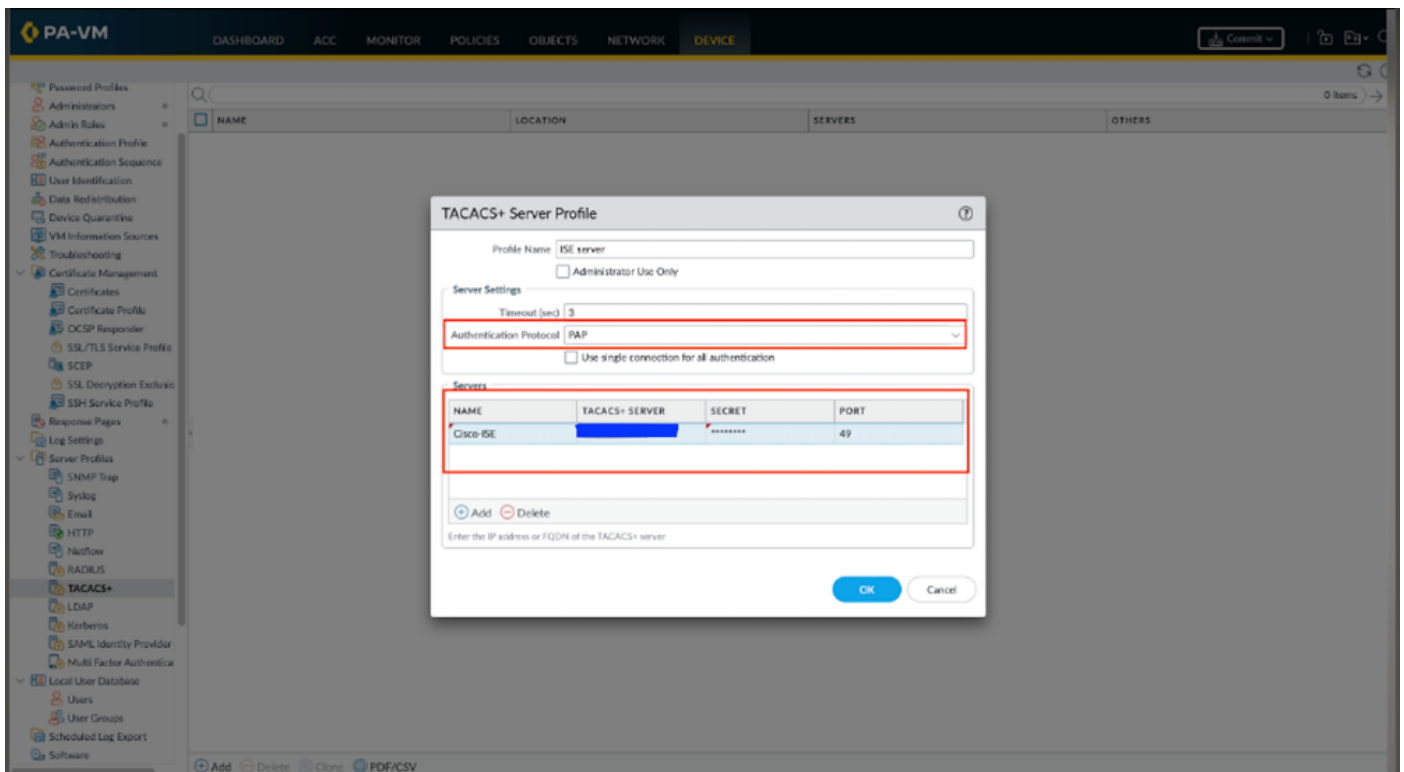
O perfil define como o firewall se conecta ao servidor TACACS+.

1. Selecione Device > Server Profiles > TACACS+ ou Panorama > Server Profiles > TACACS+ on Panorama e Add a profile.
2. Digite um Nome de perfil para identificar o perfil do servidor.
3. (Opcional) Selecione Somente para uso do administrador para restringir o acesso aos administradores.
4. Insira um intervalo de tempo limite em segundos após o qual uma solicitação de autenticação atinge o tempo limite (o padrão é 3; o intervalo é de 1 a 20).
5. Selecione o protocolo de autenticação (o padrão é CHAP) que o firewall usa para autenticar



no servidor TACACS+.

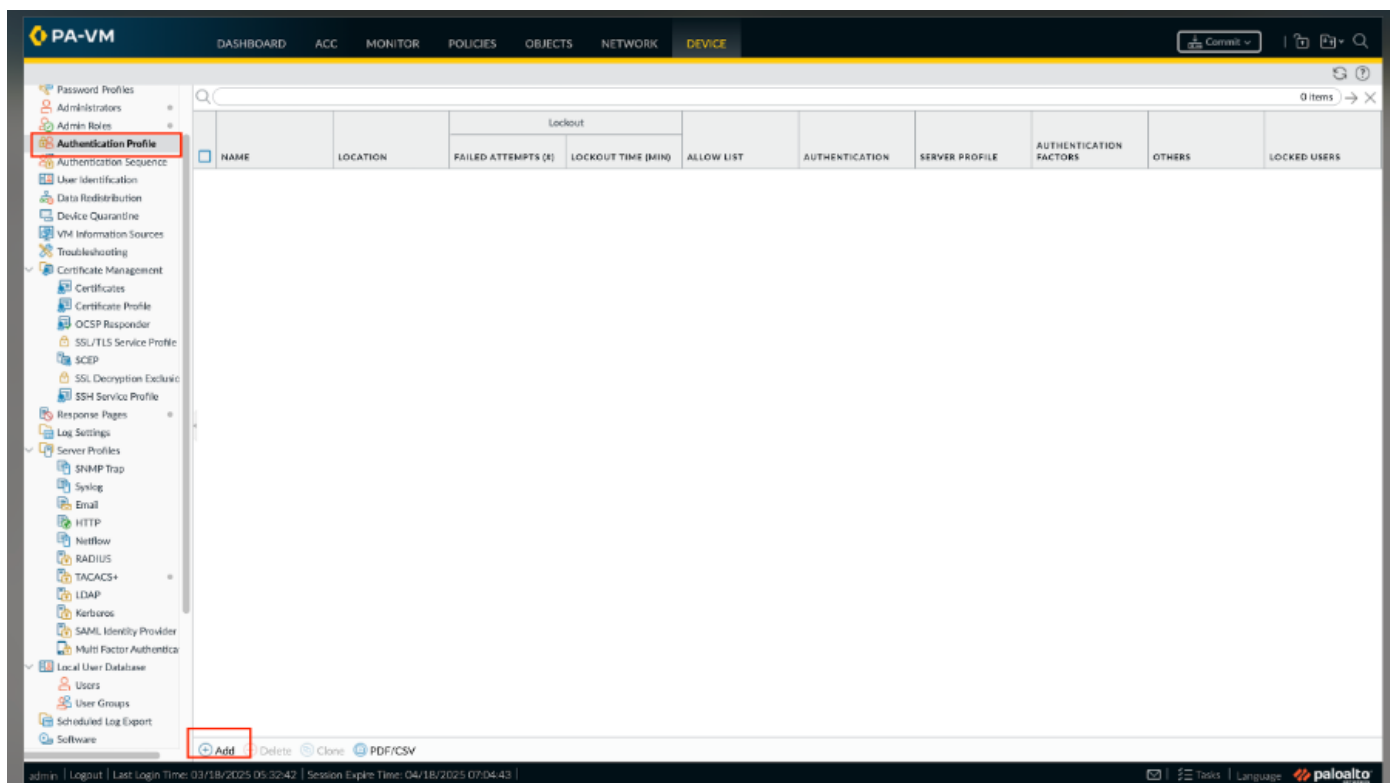
6. Adicione cada servidor TACACS+ e execute estas etapas:
 1. Um Nome para identificar o servidor.
 2. O endereço IP ou FQDN do servidor TACACS+. Se você usar um objeto de endereço FQDN para identificar o servidor e, subsequentemente, alterar o endereço, deverá confirmar a alteração para que o novo endereço do servidor entre em vigor.
 3. Um Segredo e Confirmar Segredo para criptografar nomes de usuário e senhas.
 4. A porta do servidor para solicitações de autenticação (o padrão é 49). Clique em OK para salvar o perfil do servidor.
7. Clique em OK para salvar o perfil do servidor.



Etapa 2. Atribuir o perfil de servidor TACACS+ a um perfil de autenticação.

O perfil de autenticação define as configurações de autenticação que são comuns a um conjunto de usuários.

1. Selecione Device > Authentication Profile e Add um perfil.
 1. Digite um nome para identificar o perfil
 2. Defina o Tipo como TACACS+.
 3. Selecione o Server Profile que você configurou.
 4. Selecione Recuperar grupo de usuários do TACACS+ para coletar informações do grupo de usuários dos VSAs definidos no servidor TACACS+.



Authentication Profile

Name

Cisco-AAA-Auth Profile

Authentication

Factors

Advanced

Type

TACACS+

Server Profile

ISE server

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

O firewall corresponde às informações do grupo usando os grupos especificados na Lista de permissões do perfil de autenticação.

1. Selecione Advanced e, na lista de permissões, Add os usuários e grupos que podem se autenticar com este perfil de autenticação.
2. Clique em OK para salvar o perfil de autenticação.

Authentication Profile

Name Cisco-AAA-Auth Profile

Authentication | Factors | **Advanced**

Allow List

☐	ALLOW LIST
☒	all

+ Add - Delete

Account Lockout

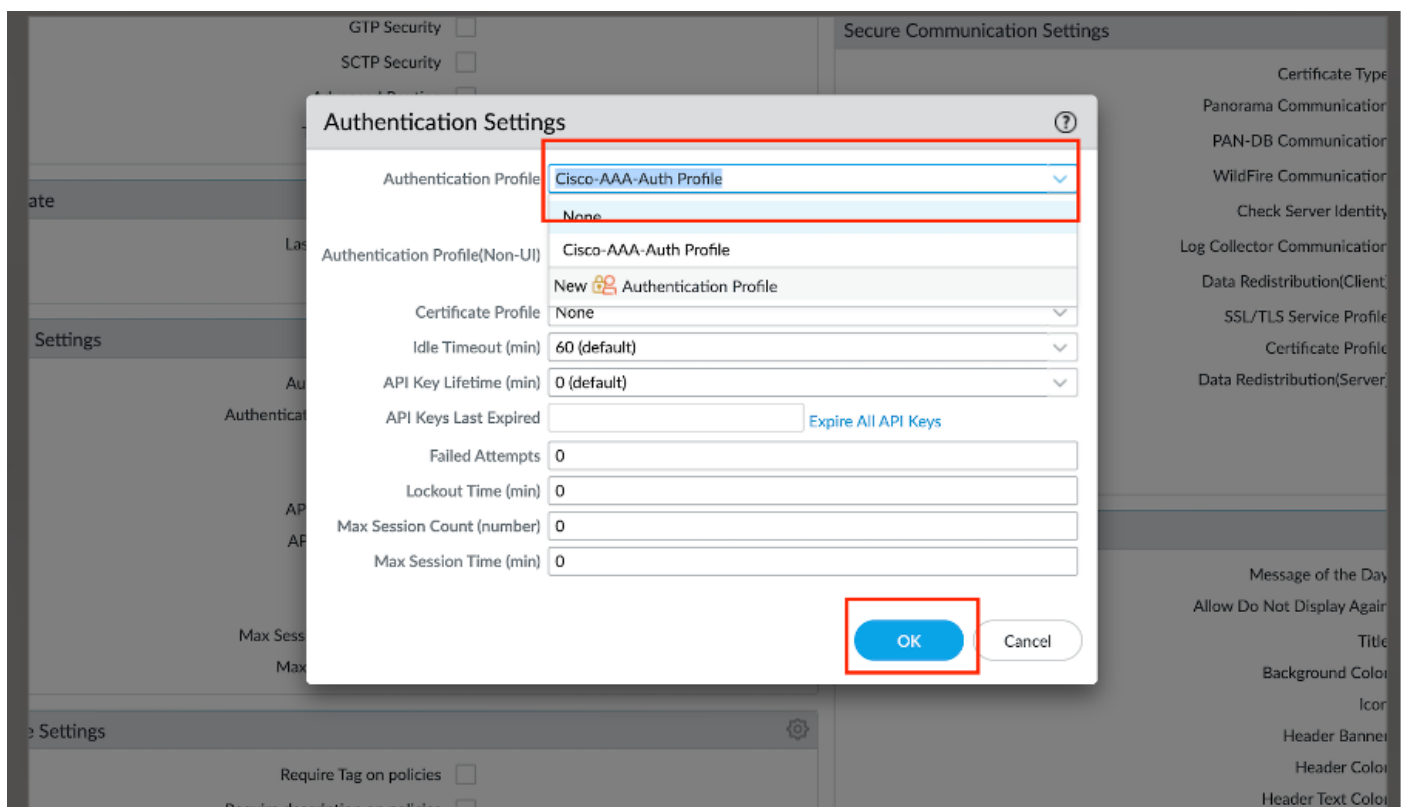
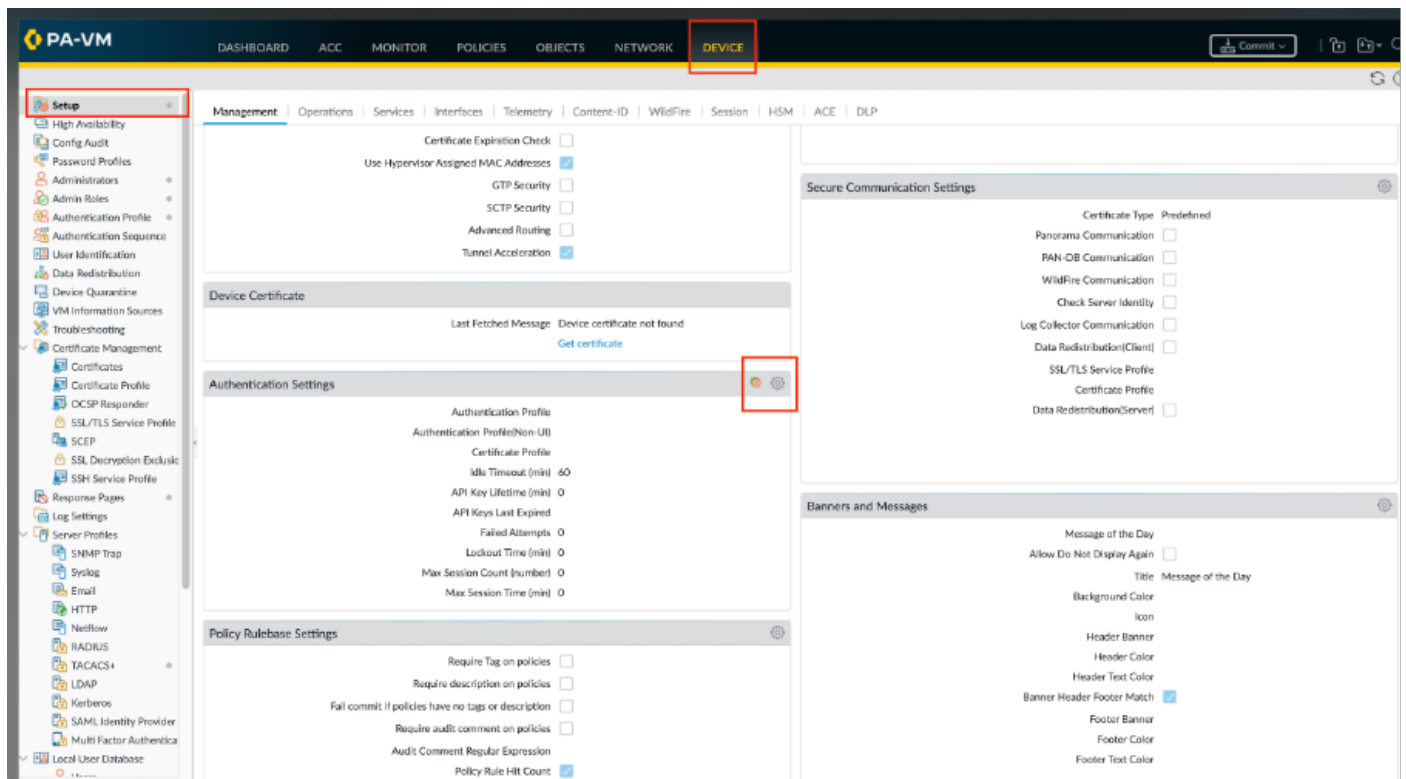
Failed Attempts [0 - 10]

Lockout Time (min) 0

OK Cancel

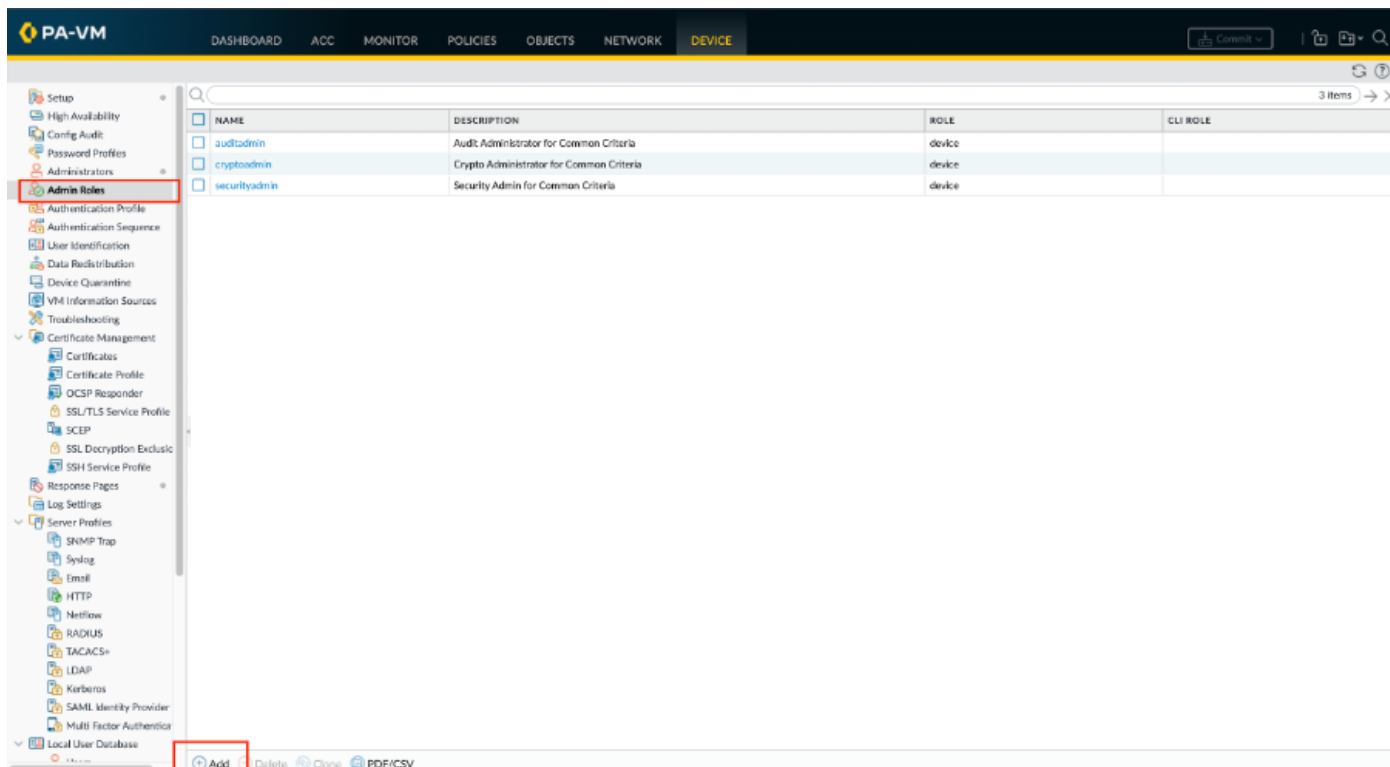
Etapa 3. Configurar o firewall para usar o perfil de autenticação para todos os administradores.

1. Selecione Device > Setup > Management e edite as Authentication Settings.
2. Selecione o perfil de autenticação que você configurou e clique em OK.

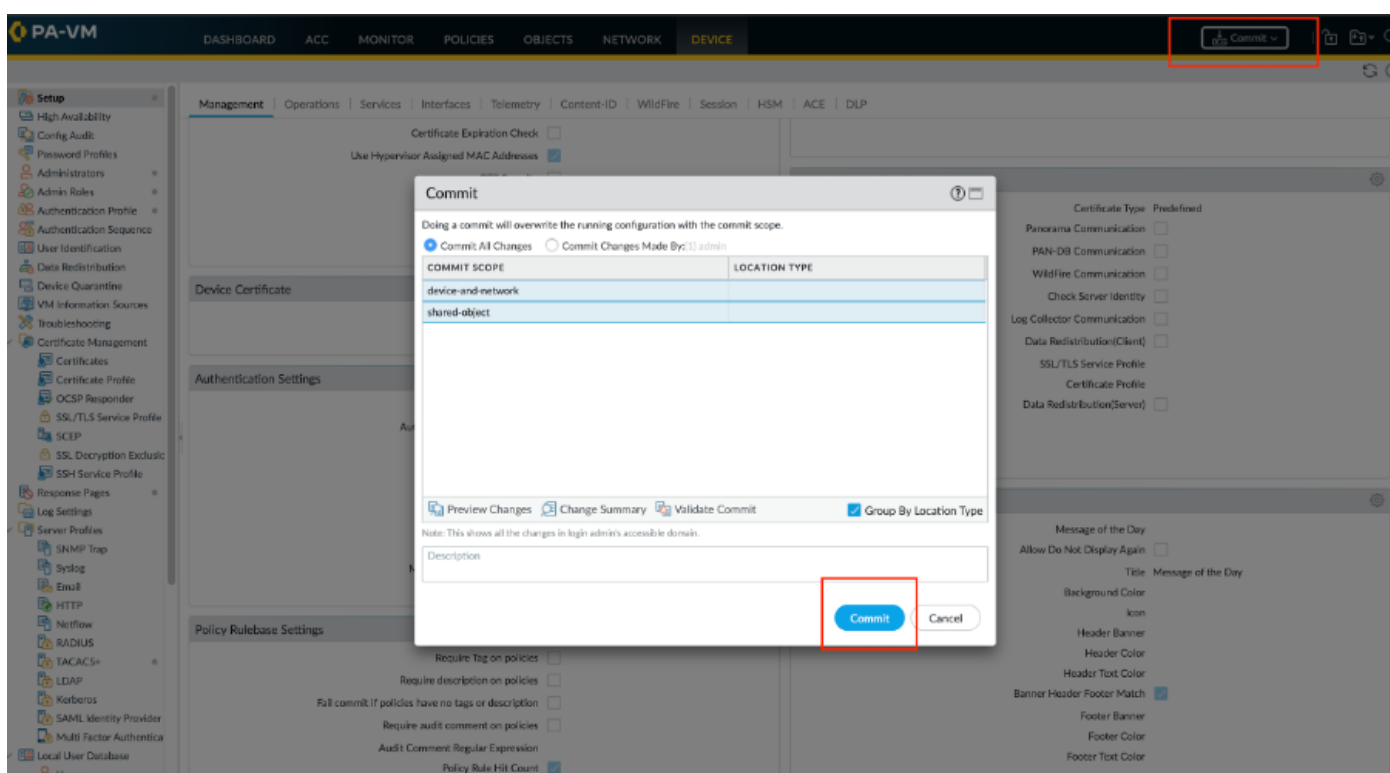


Etapa 4. Configurar um Perfil de Função do Administrador.

Selecione Device > Admin Roles e clique em Add. Insira um Nome para identificar a função.



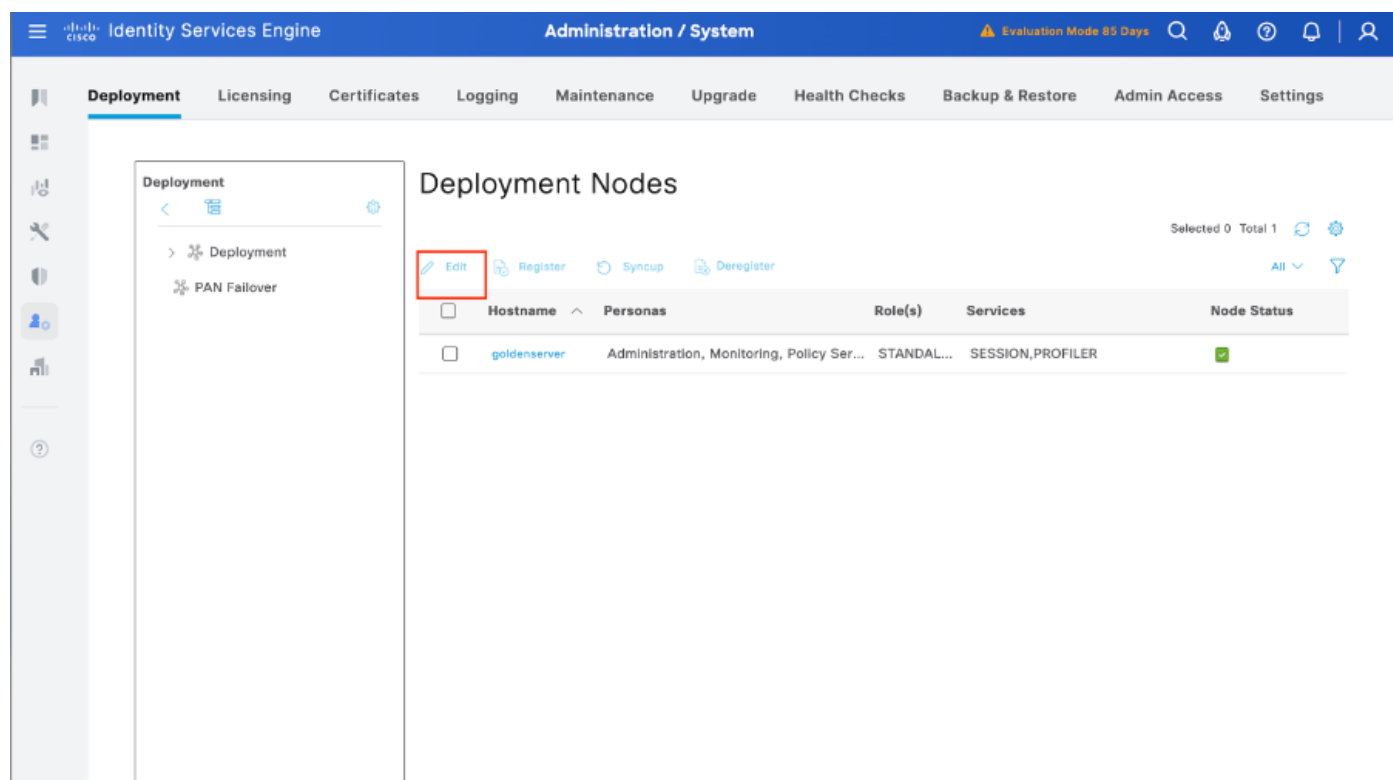
Etapa 5. Confirme suas alterações para ativá-las no firewall.



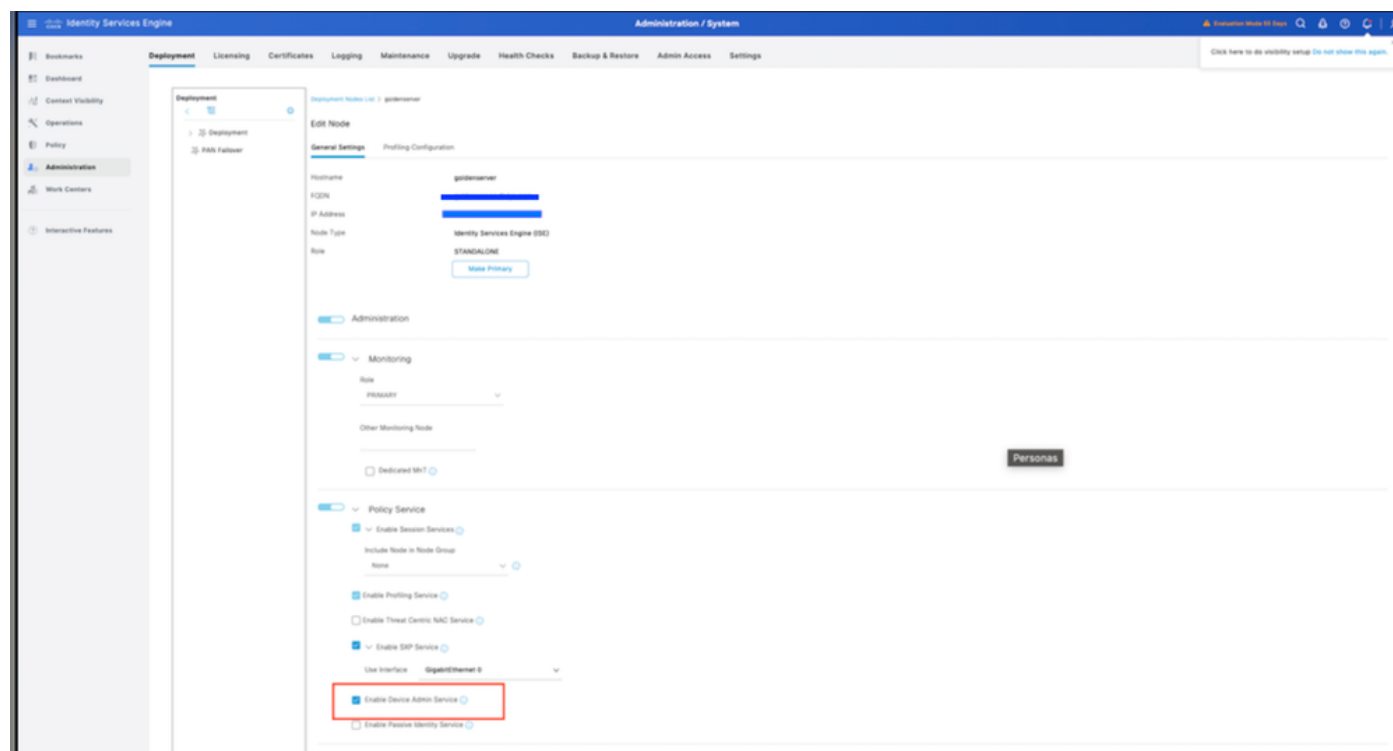
Seção 2: Configuração TACACS+ no ISE

Etapa 1. A etapa inicial é verificar se o Cisco ISE tem os recursos necessários para lidar com a autenticação TACACS+. Para fazer isso, confirme se o Policy Service Node (PSN) desejado tem o recurso Device Admin Service habilitado. Navegue para Administração > Sistema > Implantação, selecione o nó apropriado onde o ISE processa a autenticação TACACS+ e clique

em Editar para revisar sua configuração.



Etapa 2. Role para baixo para localizar o recurso Device Administration Service. Observe que a habilitação desse recurso exige que a persona do Serviço de política esteja ativa no nó, junto com as licenças TACACS+ disponíveis na implantação. Marque a caixa de seleção para ativar o recurso e salve a configuração.



Etapa 3. Configurar o perfil do dispositivo de rede Palo Alto para o Cisco ISE.

Navegue até Administração > Recursos de rede > Perfil do dispositivo de rede. Clique em Add e mencione o nome (Palo Alto) e ative o TACACS+ nos protocolos suportados.

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, 802.1X

CoA: Port Bounce (default CoA port: 3799, default DTLS CoA port: 2083)

Native URL Redirect: [Static](#)

Etapa 4. Adicionar a Palo Alto como um dispositivo de rede.

1. Navegue até Administração > Recursos de rede > Dispositivos de rede > +Adicionar.

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. Clique em Adicionar e informe estes detalhes:

Nome: Palo-Alto

Endereço IP: <IP Palo-Alto>

Perfil do dispositivo de rede: selecione Palo Alto

Configurações de autenticação TACACS:

Habilitar autenticação TACACS+

Insira o segredo compartilhado (deve corresponder à configuração da Palo Alto)

Click Save.

The screenshot displays the 'Administration / Network Resources' section of the Palo Alto Networks Identity Services Engine (ISE) interface. The 'Network Devices' tab is selected, and the configuration for a device named 'Palo_Alto_Firewall' is shown. The 'Device Profile' is set to 'Palo_Alto'. The 'TACACS Authentication Settings' section is expanded, revealing a 'Shared Secret' field and a 'Retire' button. A 'Save' button is located at the bottom right of the configuration area.

Etapa 5. Criar Grupos de Identidades de Usuário.

Navegue até Centros de trabalho > Administração de dispositivo > Grupos de identidade de usuário e clique em Adicionar e especifique o nome do grupo de usuários.

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 > divznet

Network Access User

* Username divznet

Status Enabled

Account Name divz

Email

Passwords

Password Type Internal Users

Password Lifetime

With Expiration Never Expires

Password

Re-Enter Password

* Login Password

Enable Password

Generate Password

Generate Password

User Information

First Name

Last Name

Account Options

Description

Change password on next login

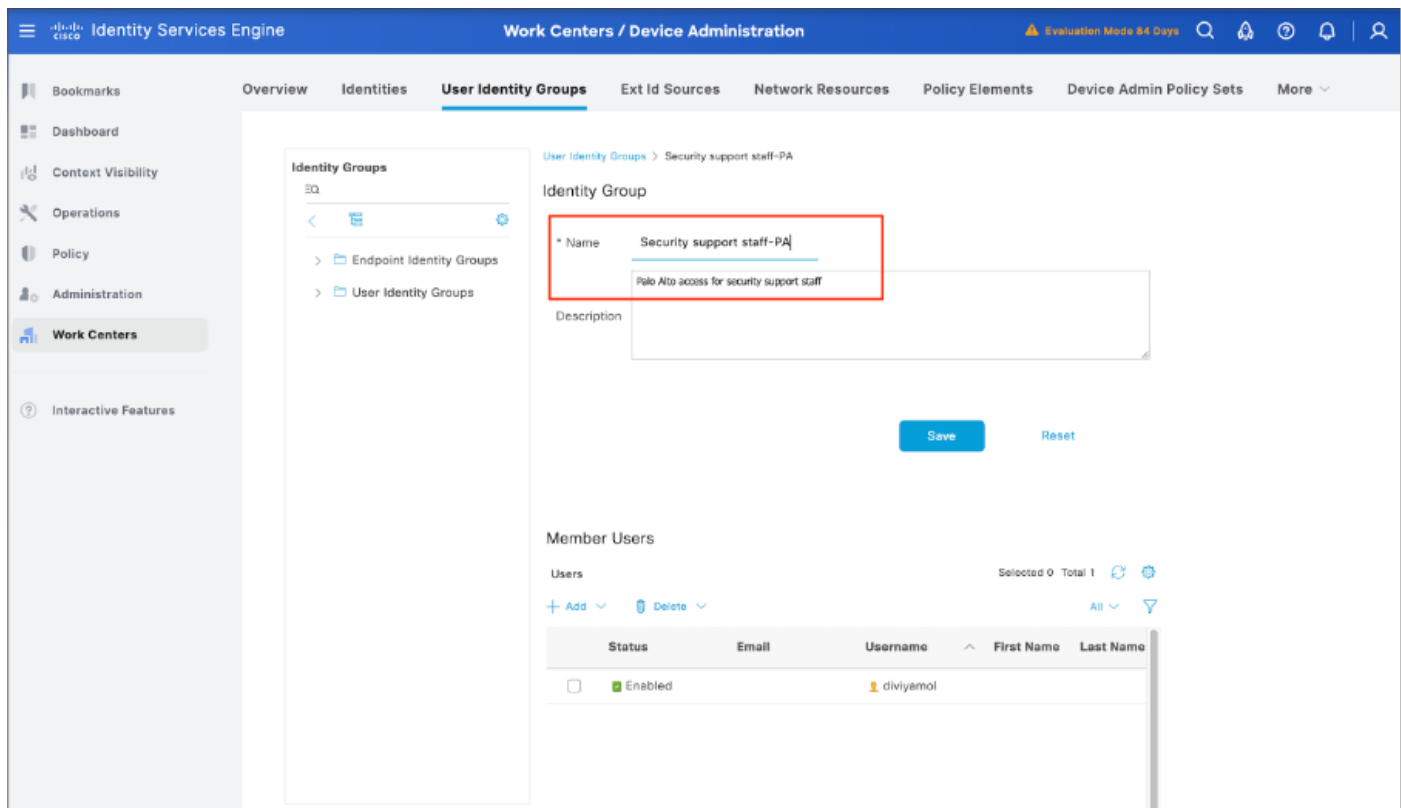
Account Disable Policy

Disable account if date exceeds 2023-03-19

Group name divz

User Groups

Security support idm-PK



Etapa 6. Configurar Um Perfil TACACS.

O próximo passo é configurar um Perfil TACACS, que é onde você pode configurar definições como Nível de Privilégio e timeout. Navegue até Centros de trabalho > Administração de dispositivos -> Elementos de política -> Resultados -> Perfis TACACS.

Clique em Add para criar um novo perfil TACACS. Dê um bom nome ao 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

Etapa 6. Configurar conjuntos de comandos TACACS.

Agora, é hora de configurar quais comandos os usuários podem usar. Como você pode conceder

a ambos os casos de uso o nível de privilégio 15, que dá acesso a todos os comandos disponíveis, use os conjuntos de comandos TACACS para limitar quais comandos podem ser usados.

Navegue até Centros de trabalho > Administração de dispositivos > Elementos de política > Resultados -> Conjuntos de comandos TACACS. Clique em Add para criar um novo conjunto de comandos TACACS e nomeá-lo PermitAllCommands. Aplique este conjunto de comandos TACACS para obter suporte de segurança.

A única coisa que você precisa configurar neste conjunto de comandos TACACS é marcar a caixa para Permitir qualquer comando que não esteja listado abaixo.

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 titled 'Policy Elements' and shows the configuration for a 'TACACS Command Set' named 'PermitAllCommands'. The 'Name' field is highlighted with a red box. The 'Description' field is empty. The 'Commands' section has a checkbox labeled 'Permit any command that is not listed below' which is checked and highlighted with a red box. Below this, there is a table with columns 'Grant', 'Command', and 'Arguments'. The table is currently empty, showing 'No data found.' At the bottom right, there are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted by a red box.

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 > TACACS Command Sets > PermitAllCommands

Command Set

Name: PermitAllCommands

Description:

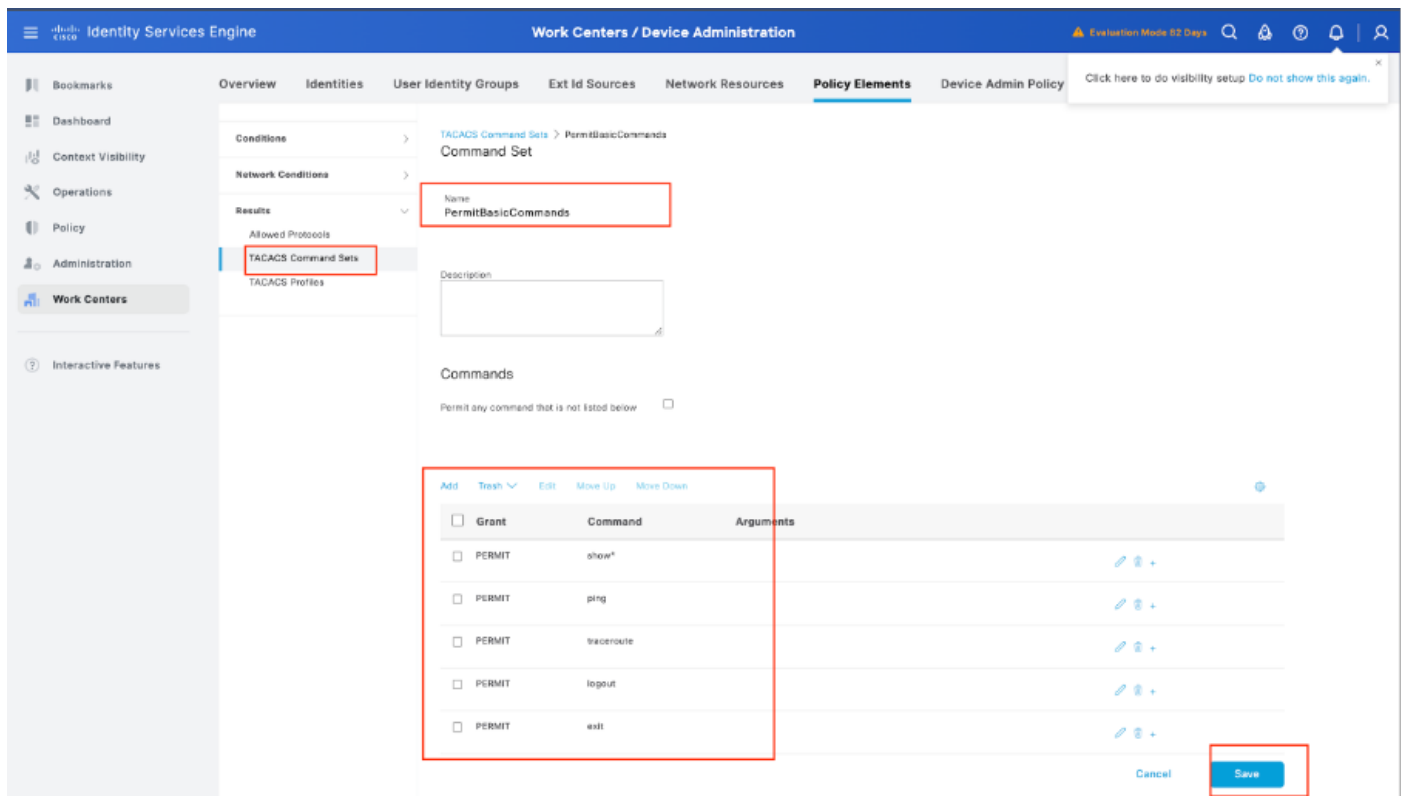
Commands

Permit any command that is not listed below ☒

Add Trash Edit Move Up Move Down

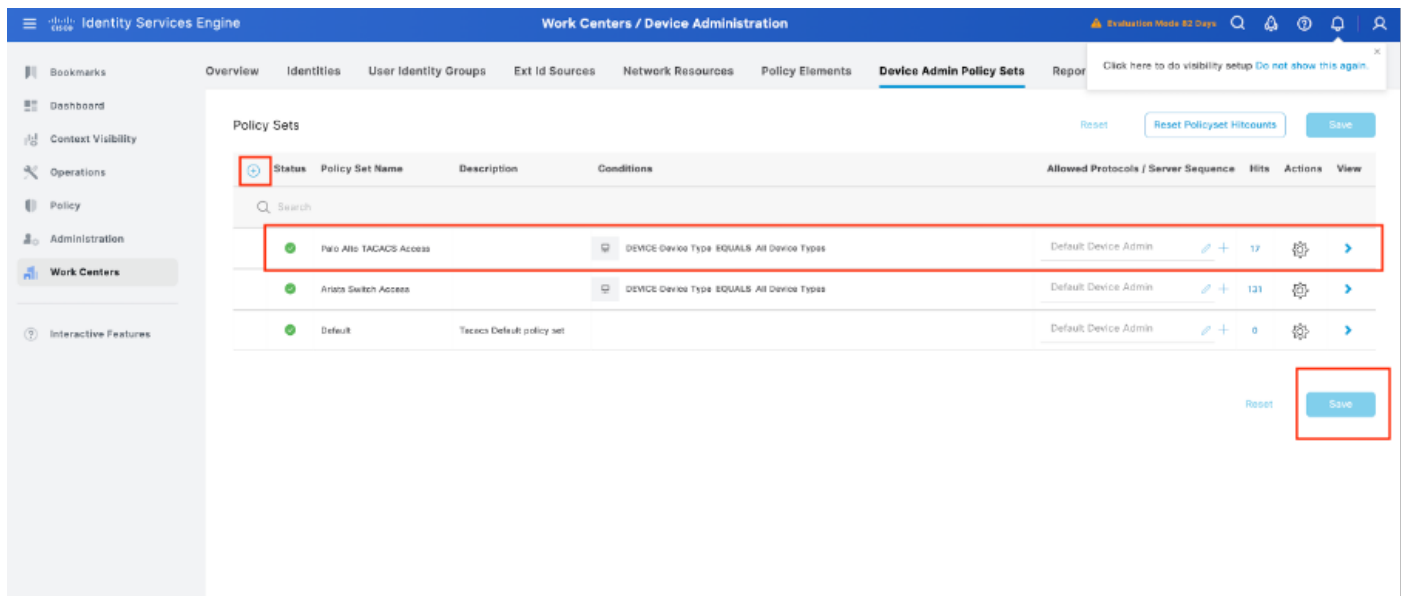
Grant	Command	Arguments
No data found.		

Cancel Save



Etapa 7. Crie um Device Admin Policy Set a ser usado para seu Palo Alto, Navegue no menu Work Centers > Device Administration > Device Admin Policy Sets, Clique no ícone Add +.

Etapa 8. Nomeie este novo Conjunto de políticas, adicione condições dependendo das características das autenticações TACACS+ que estão em andamento no Firewall Palo Alto e selecione como Allowed Protocols > Default Device Admin. Salve sua configuração.



Etapa 9. Selecione na opção > exibir e, em seguida, na seção Authentication Policy (Política de autenticação), selecione a fonte de identidade externa que o Cisco ISE usa para consultar o nome de usuário e as credenciais para autenticação no Palo Alto Firewall. Neste exemplo, as credenciais correspondem a Usuários internos armazenados no ISE.

Identity Services Engine Work Centers / Device Administration

Policy Sets → Palo Alto TACACS Access

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Palo Alto TACACS Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	17

Authentication Policy(2)

Status	Rule Name	Conditions	Use	Hits	Actions
●	PaloAlto_Authz Policy	Network Access-Device IP Address EQUALS [REDACTED]	Internal Users Options	17	⚙️
●	Default		Internal Users Options	0	⚙️

Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions
Authorization Policy(3)

Reset Save

Etapa 10. Role para baixo até a seção chamada Política de autorização até a política padrão, selecione o ícone de engrenagem e insira uma regra acima.

Identity Services Engine Work Centers / Device Administration

Policy Sets → Palo Alto TACACS Access

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Palo Alto TACACS Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	17

Authorization Policy(3)

Status	Rule Name	Conditions	Results	Command Sets	Shell Profiles	Hits	Actions
●	PA_FW_Authz Policy	InternalUser IdentityGroup EQUALS User Identity Groups:Security support staff-PA	PermitAllCommands	PermitAllCommands	PaloAlto_Security_Support	14	⚙️
●	PA_FW_Security policy	InternalUser IdentityGroup EQUALS User Identity Groups:Security Engineers	PermitBasicCommands	PermitBasicCommands	PaloAlto_Engineers_Profile	2	⚙️
●	Default		DenyAllCommands	DenyAllCommands	Deny All Shell Profile	0	⚙️

Reset Save

Etapa 11. Nomeie a nova Regra de autorização, adicione condições referentes ao usuário que já está autenticado como membro do grupo e, na seção Perfis do shell, adicione o perfil TACACS que você configurou anteriormente e salve a configuração.

Verificar

Revisão do ISE

Etapa 1. Revise se se a capacidade de serviço TACACS+ está em execução, isso pode ser verificado em:

- GUI: Verifique se você tem o nó listado com o serviço DEVICE ADMIN em Administração -> Sistema -> Implantação.
- CLI: Execute o comando show ports | incluir 49 para confirmar que há conexões na porta TCP que pertencem ao TACACS+

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

Etapa 2. Confirme se há registros em tempo real referentes a tentativas de autenticação TACACS+ : isso pode ser verificado no menu Operations -> TACACS -> Live logs.

Dependendo do motivo da falha, você pode ajustar sua configuração ou tratar da causa da falha.

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

Etapa 3. Caso você não veja nenhum registro em tempo real, continue para fazer uma captura de pacote, navegue até o menu Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump e selecione Add.

TCP Dump

The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

Rows/Page 0 < 0 / 0 > Go

Add Edit Trash Start Stop Download

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

Evaluate 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)

☐ Periodically Mode

Cancel Save Save and Run

Etapa 4. Ative o componente runtime-AAA na depuração dentro do PSN de onde a autenticação está sendo executada em Operações > Solução de problemas > Assistente de depuração > Configuração do log de depuração, selecione o nó PSN e, em seguida, selecione avançar no botão de edição .

Identity Services Engine Operations / Troubleshoot Evaluation Mode 85 Days

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration

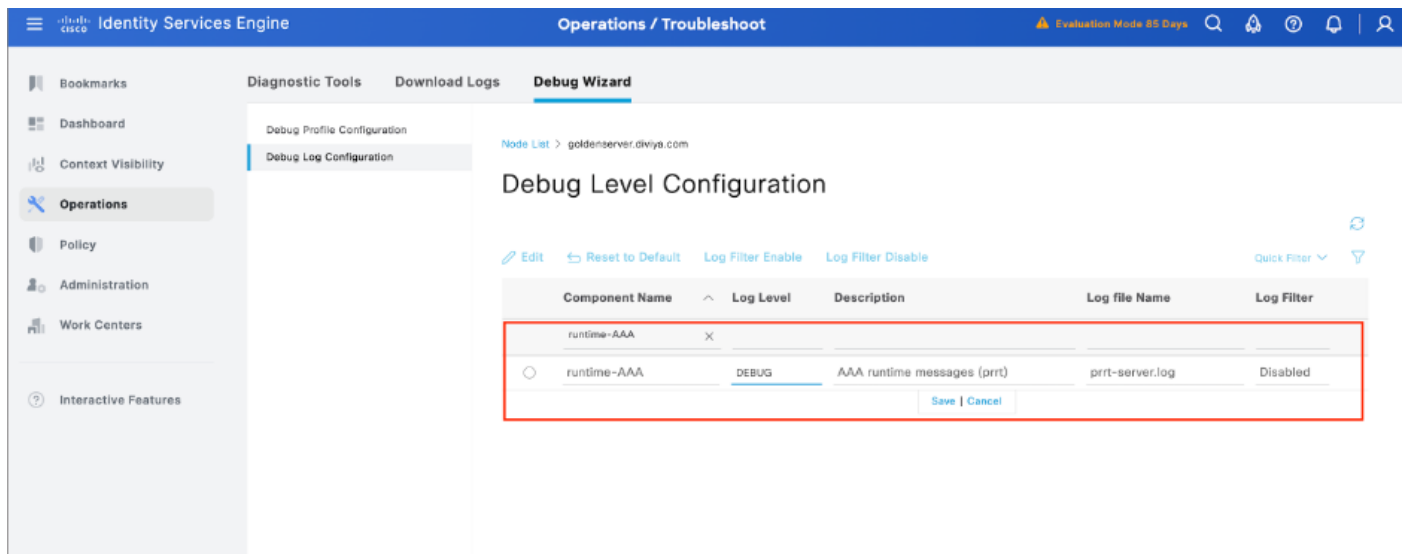
Debug Log Configuration

Node List

Selected 0 Total 1

Edit Reset to Default

Node Na...	Replication Role
goldenserver	STANDALONE



Troubleshooting

TACACS: Pacote de solicitação TACACS+ inválido - Segredos compartilhados possivelmente incompatíveis

Problema

A autenticação TACACS+ entre o Cisco ISE e o firewall Palo Alto (ou qualquer dispositivo de rede) falha com a mensagem de erro:

"Pacote de solicitação TACACS+ inválido - segredos compartilhados possivelmente incompatíveis"

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	

Isso impede tentativas de login administrativo bem-sucedidas e pode afetar o controle de acesso do dispositivo através da autenticação centralizada.

Possíveis causas

- Uma incompatibilidade no segredo compartilhado configurado no Cisco ISE e no firewall ou dispositivo de rede da Palo Alto.
- Configuração incorreta do servidor TACACS+ no dispositivo (como endereço IP, porta ou protocolo incorretos).

Solução

Há várias soluções possíveis para esse problema:

1. Verifique o segredo compartilhado:

- No Cisco ISE:
Navegue para Administração > Recursos de rede > Dispositivos de rede, selecione o dispositivo afetado e confirme o segredo compartilhado.
- No firewall da Palo Alto:
Vá para Device > Server Profiles > TACACS+ e verifique se o segredo compartilhado corresponde exatamente, incluindo maiúsculas e minúsculas e caracteres especiais.

2. Verificar Configurações do Servidor TACACS+:

- Verifique se o endereço IP e a porta corretos (o padrão é 49) do Cisco ISE estão configurados no perfil TACACS+ do firewall.
- Confirme se o tipo de protocolo é TACACS+ (não RADIUS).

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.