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

Contents

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

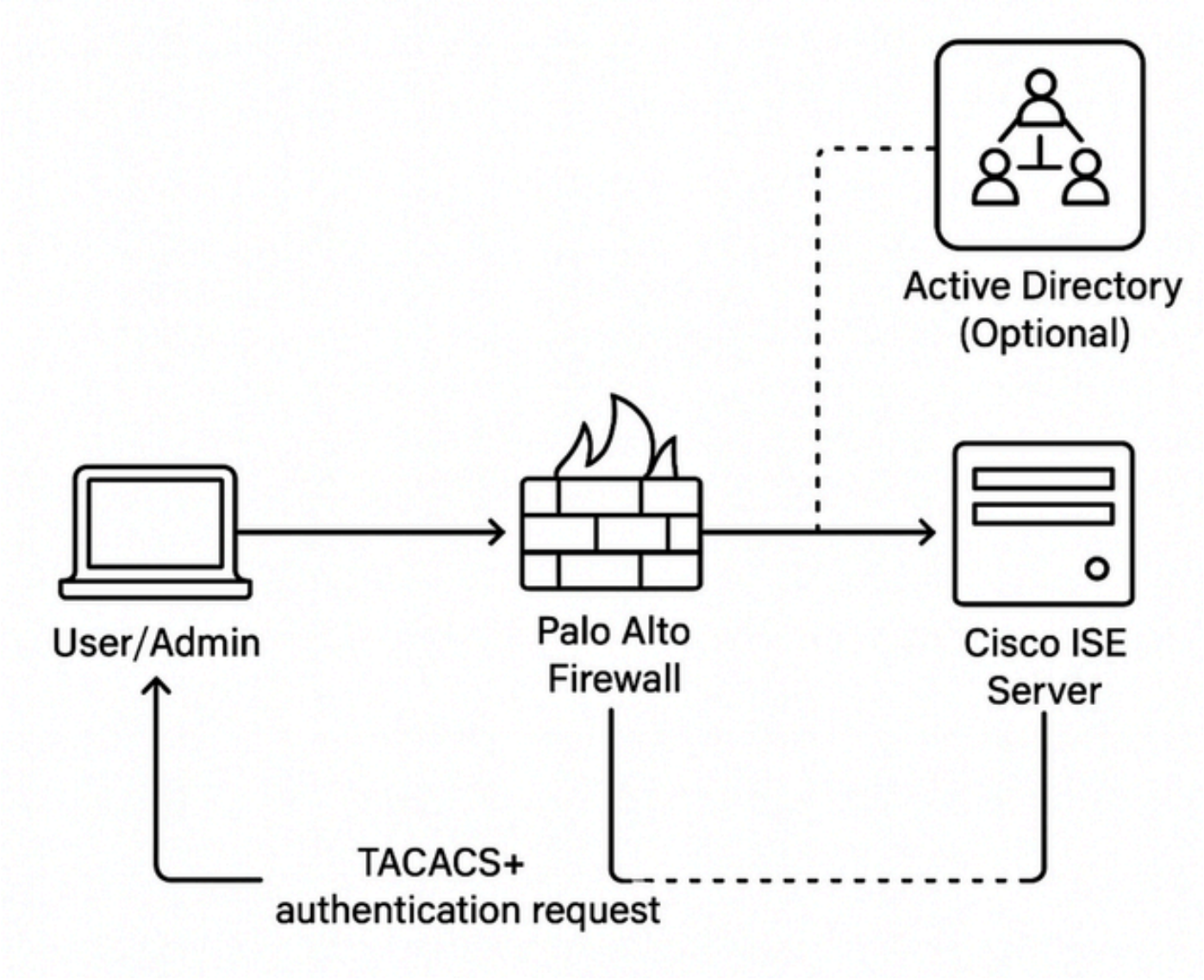
As informações neste documento são baseadas nestas versões de software e hardware:

- 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.

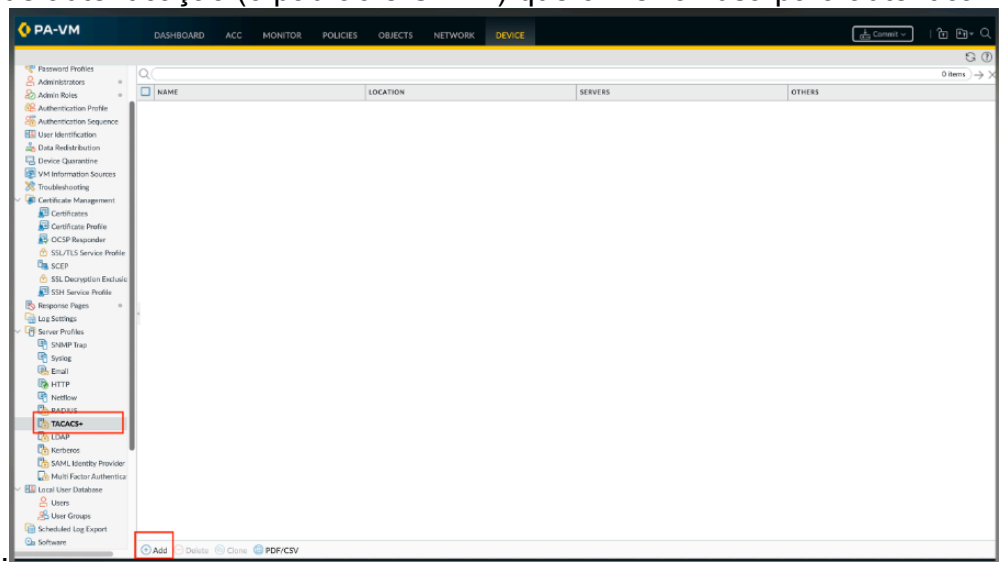
Configurar

Seção 1: Configurar o firewall Palo Alto para TACACS+

Etapa 1. Adicionar um perfil de servidor TACACS+.

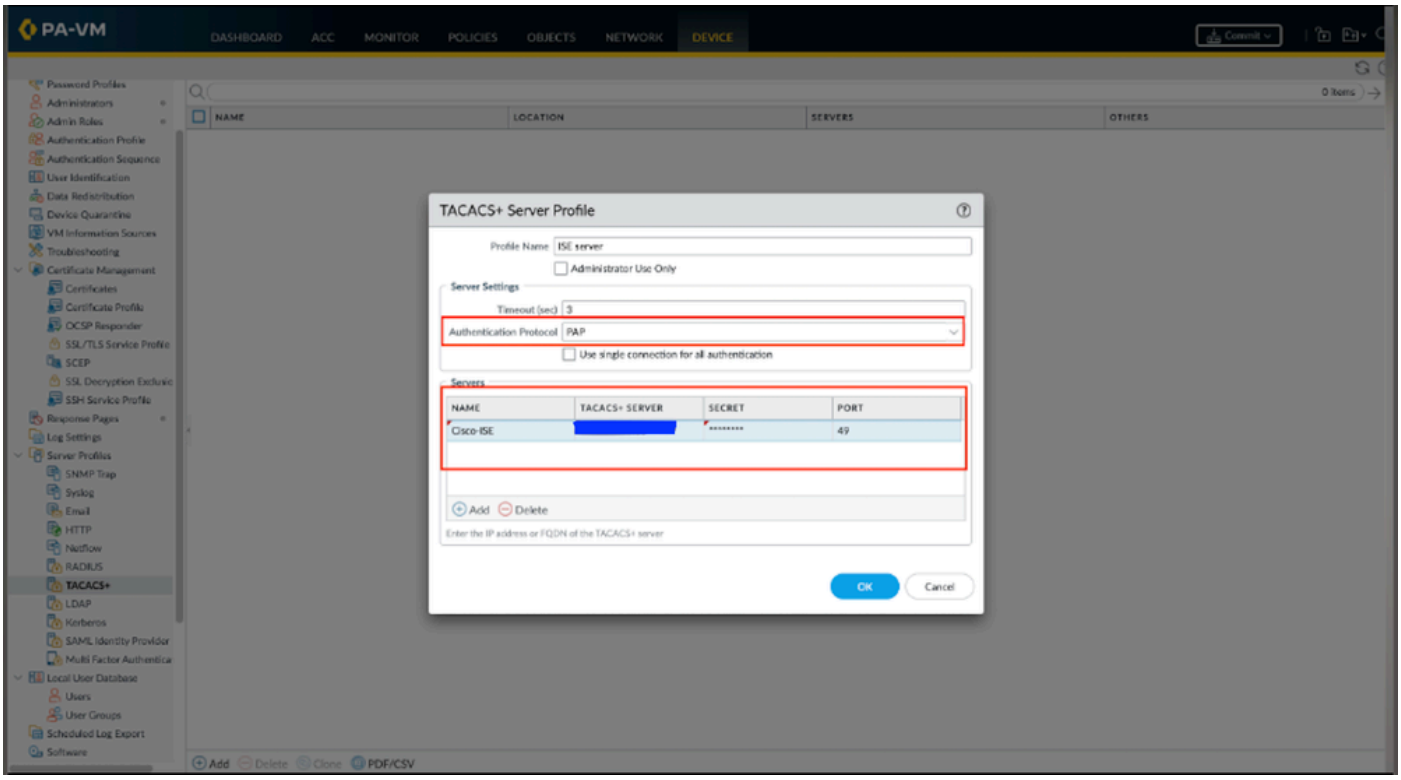
O perfil define como o firewall se conecta ao servidor TACACS+.

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.

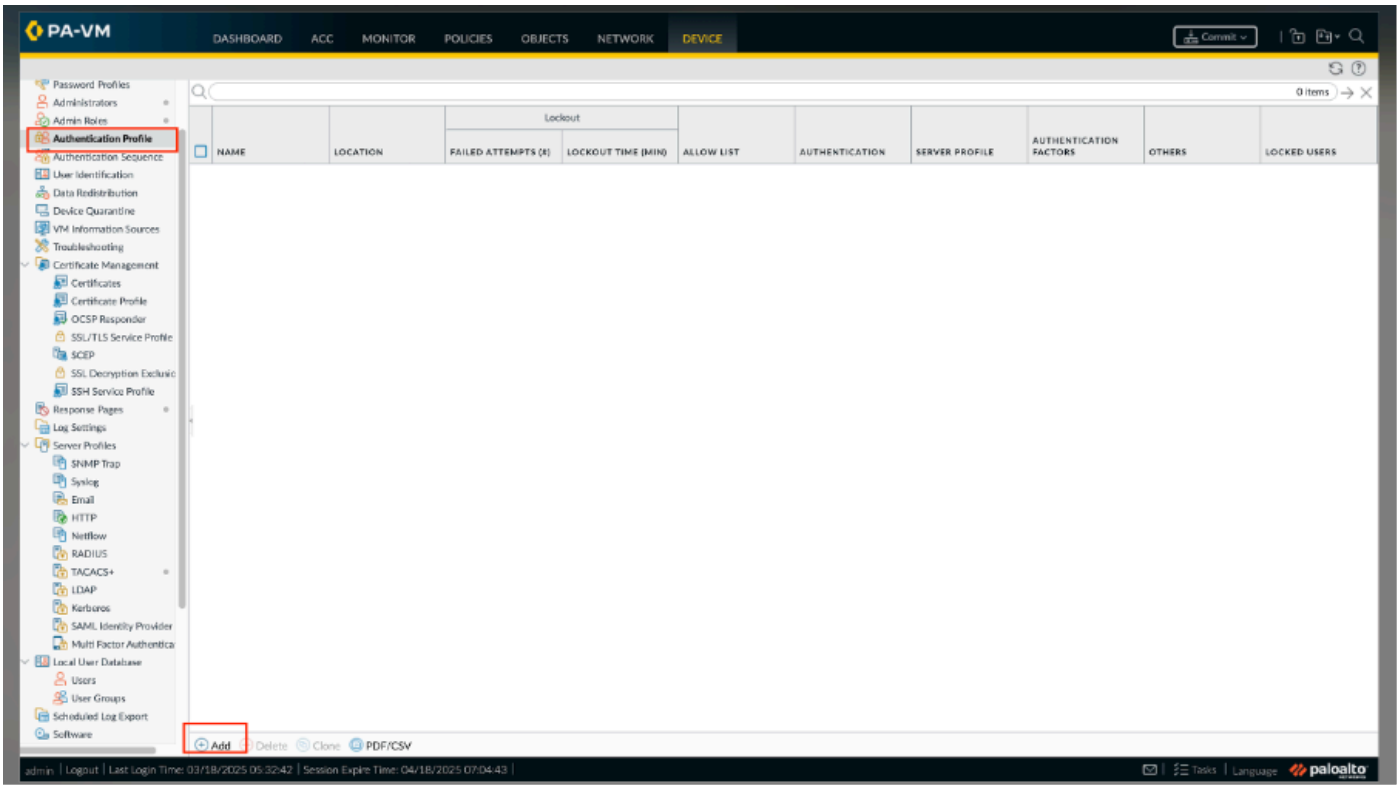
7. Clique em OK para salvar o perfil do servidor.

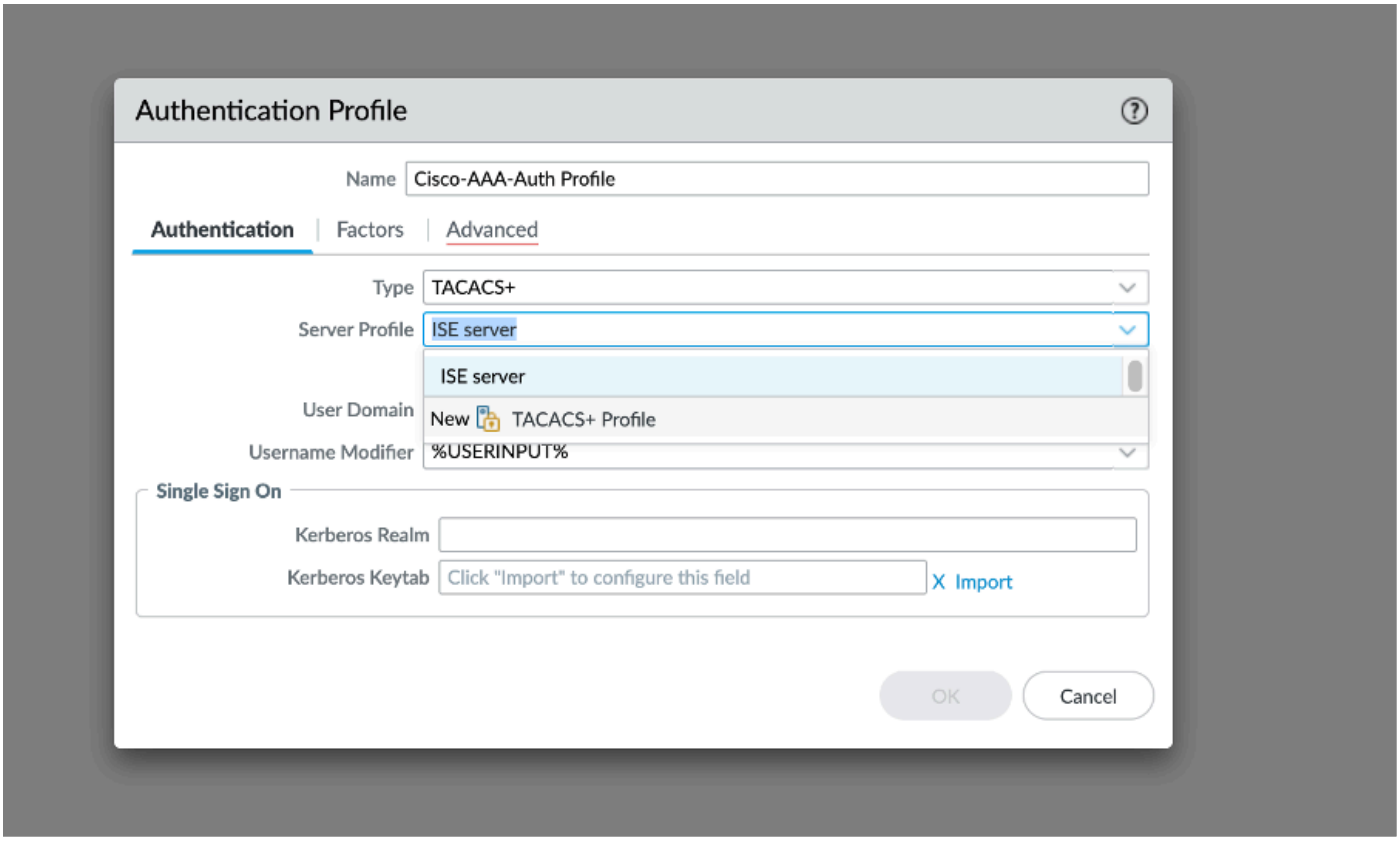


Etapa 2. Atribuir o perfil de servidor TACACS+ a um perfil de autenticação.

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

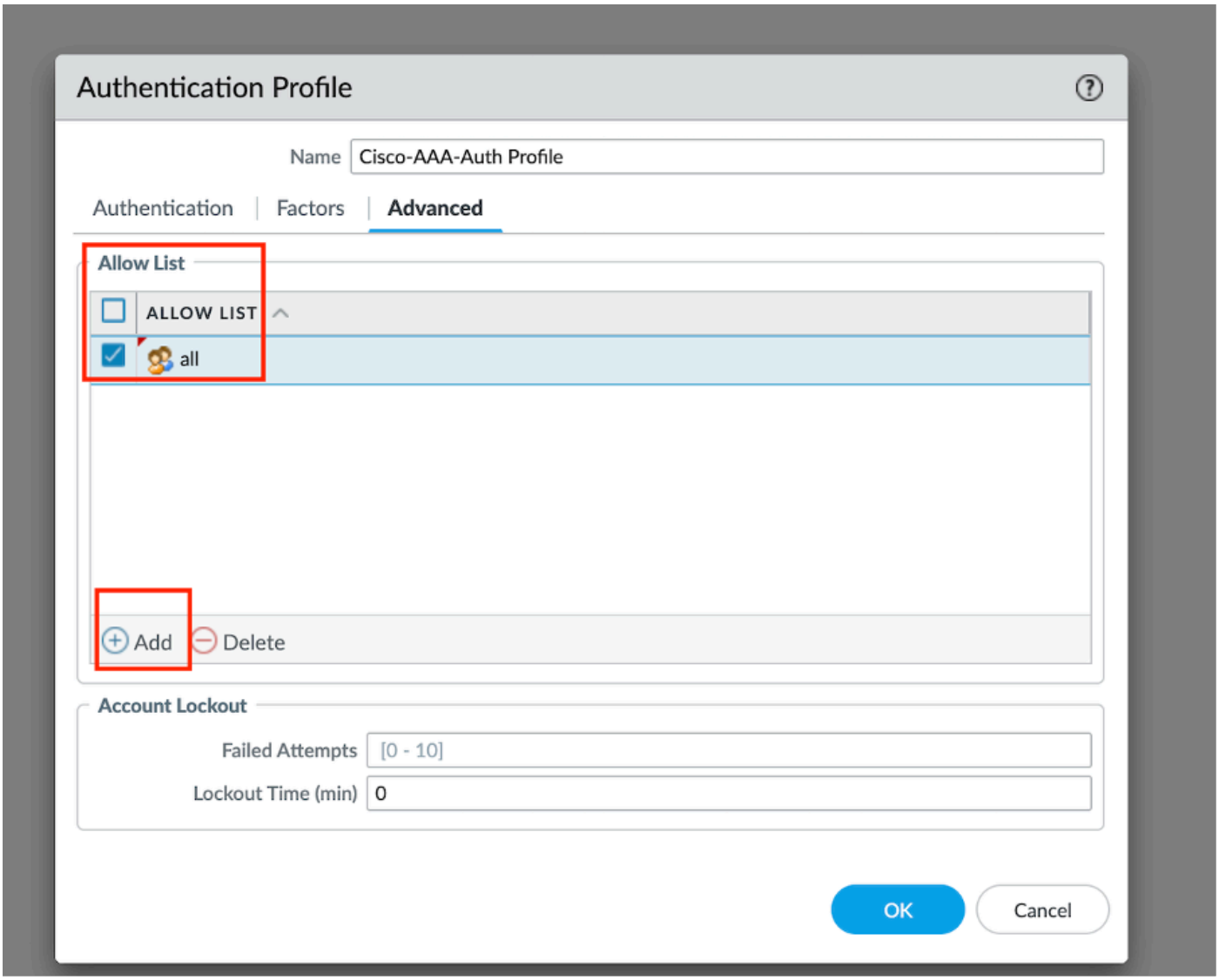
1. Selecione Device > Authentication Profile e Add um perfil.
    1. Digite um nome para identificar o perfil
    2. Defina o Tipo como TACACS+.
    3. Selecione o Server Profile que você configurou.
    4. Selecione Recuperar grupo de usuários do TACACS+ para coletar informações do grupo de usuários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





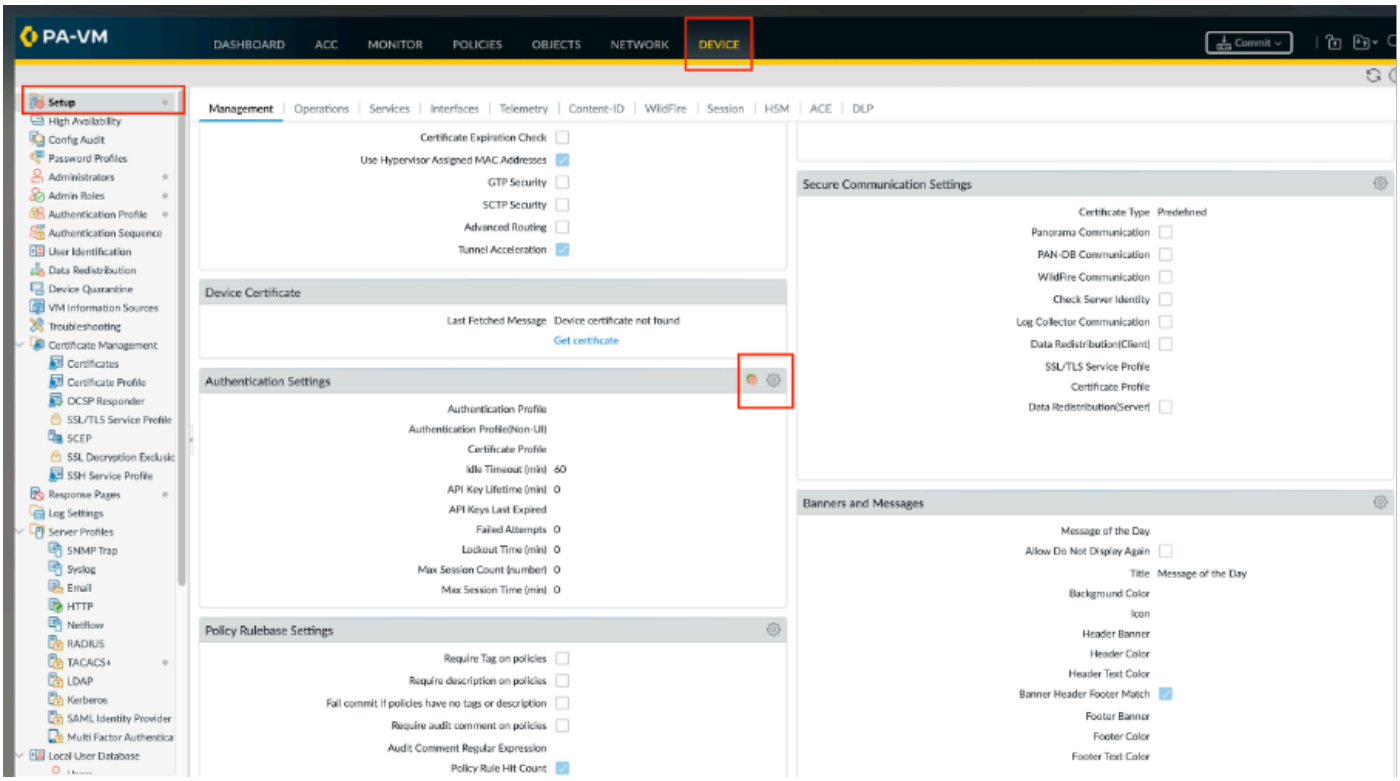
O firewall corresponde às informações do grupo usando os grupos especificados na Lista de permissões do perfil de autenticação.

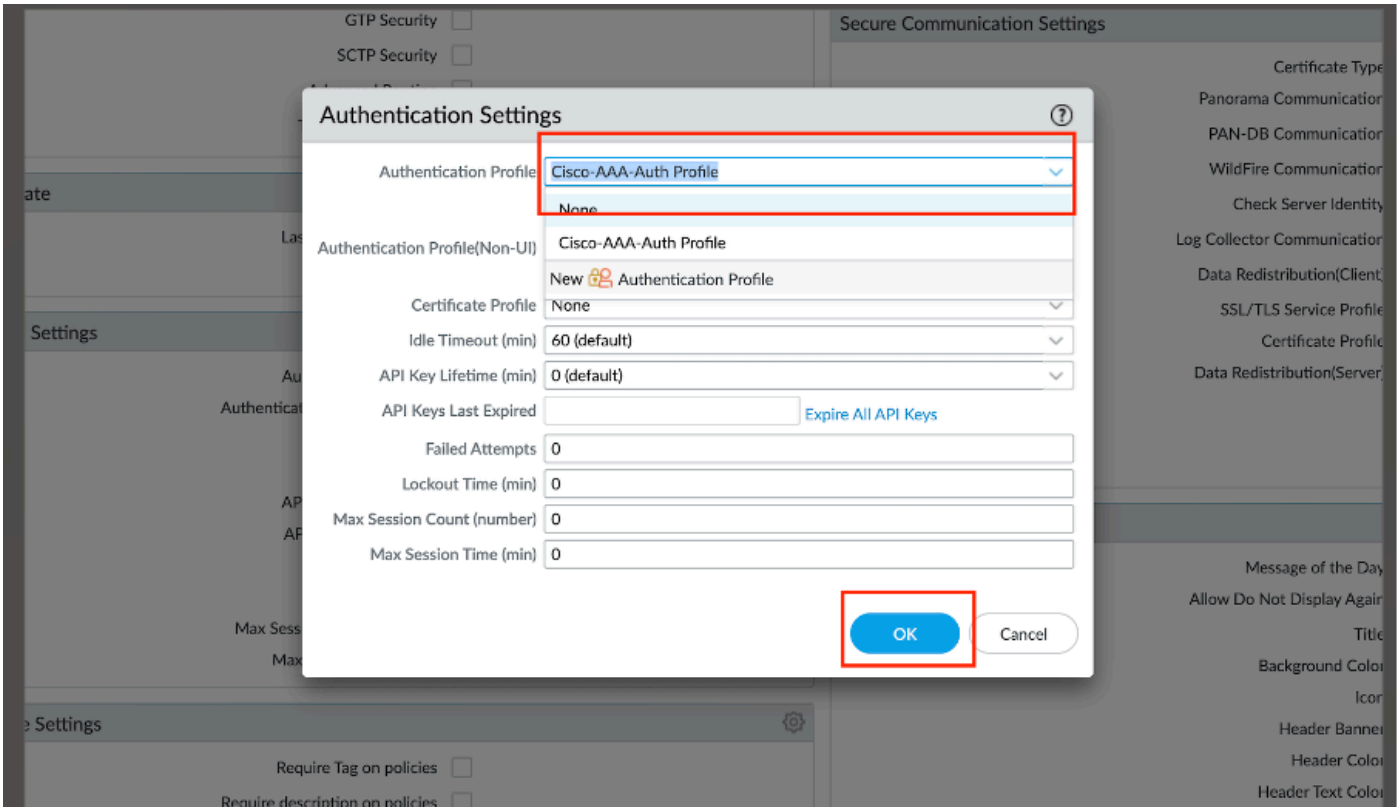
1. Selecione Advanced e, na lista de permissões, Add os usuários e grupos que podem se autenticar com este perfil de autenticação.
2. Clique em OK para salvar o perfil de autenticação.



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

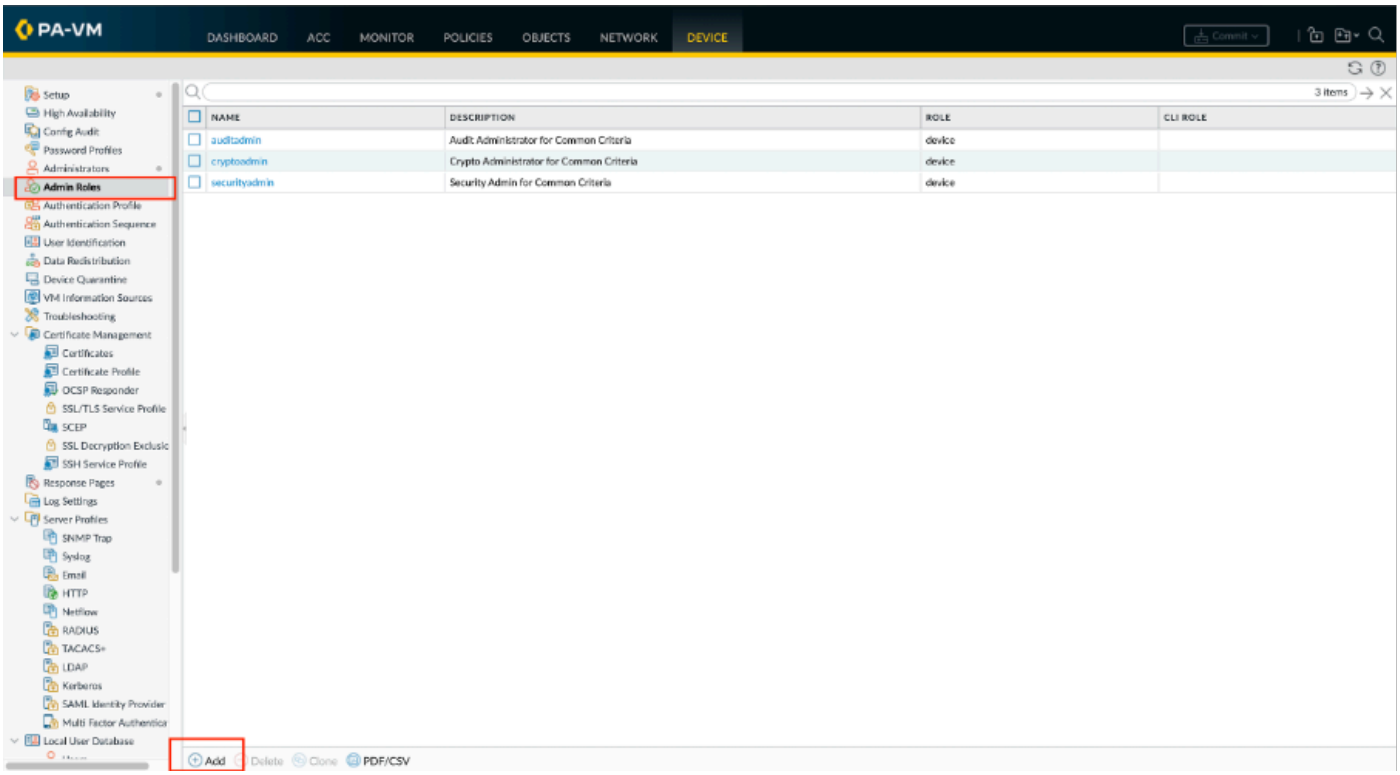
1. Selecione Device > Setup > Management e edite as Authentication Settings.
2. Selecione o perfil de autenticação que você configurou e clique em OK.



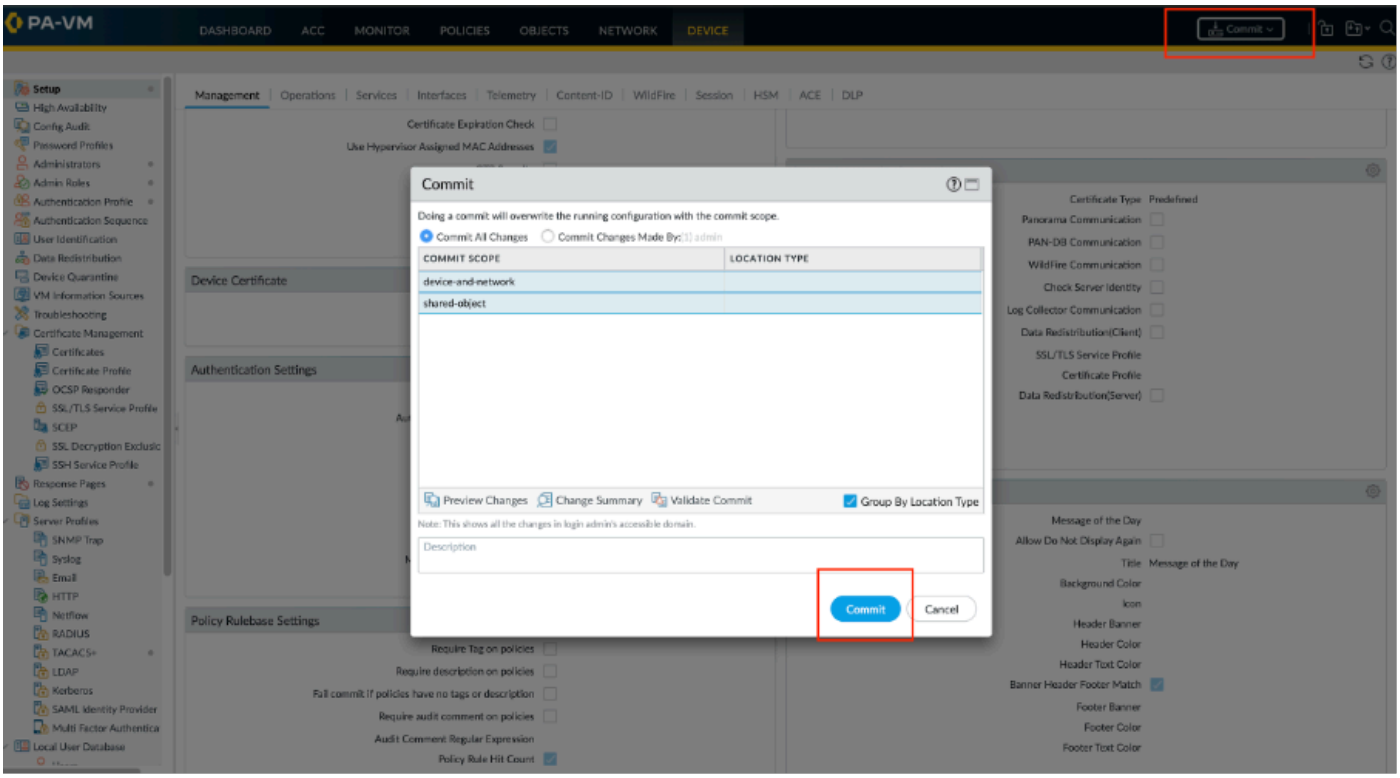


Etapa 4. Configurar um Perfil de Função do Administrador.

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



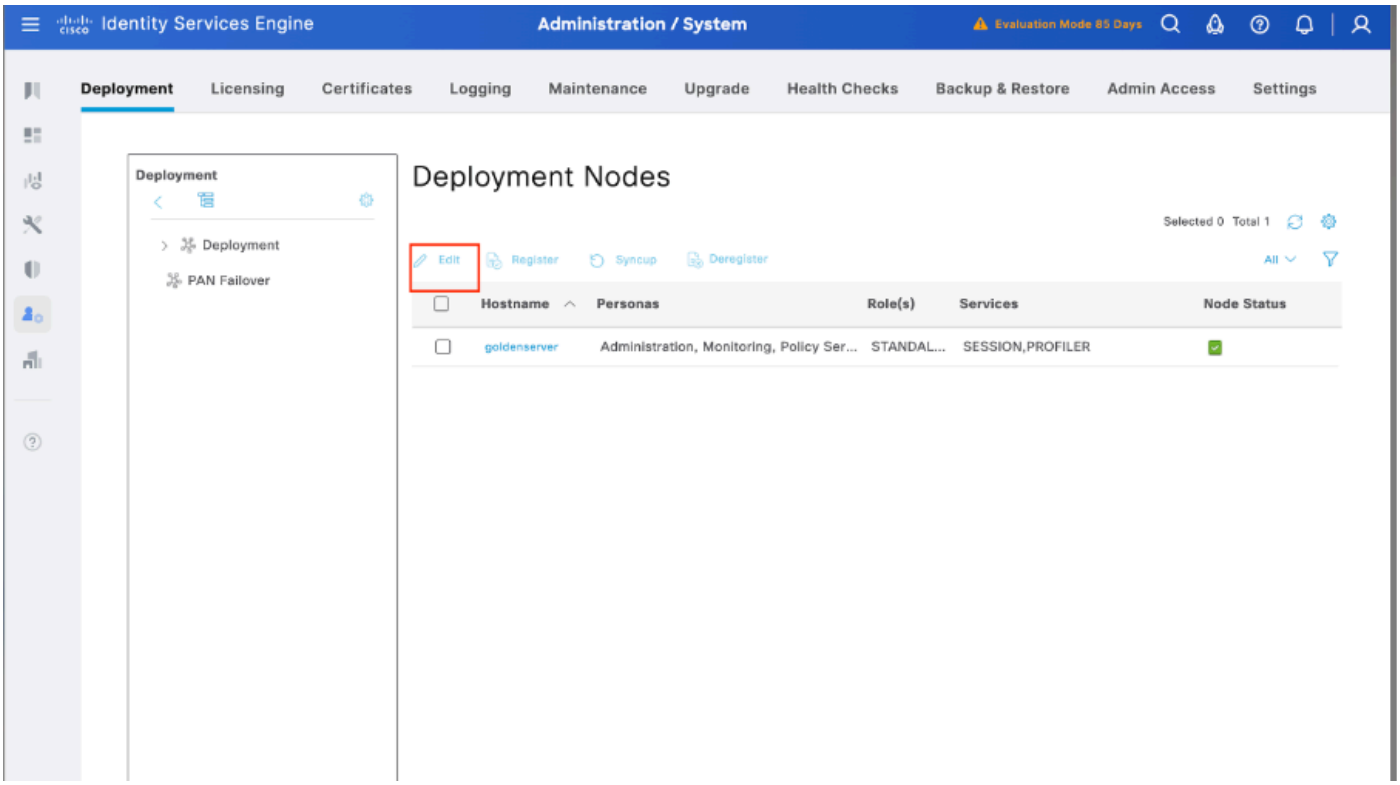
Etapa 5. Confirme suas alterações para ativá-las no firewall.



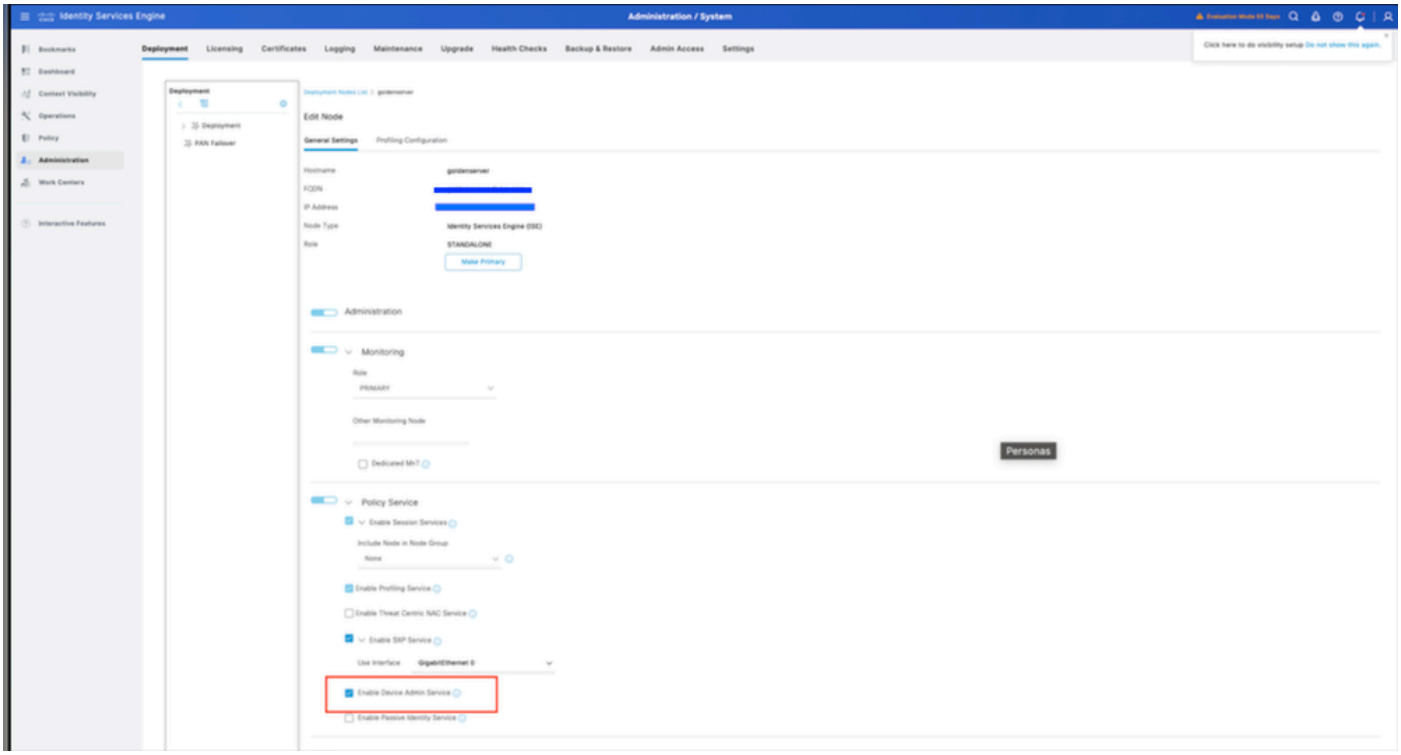
Seção 2: Configuração TACACS+ no ISE

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.

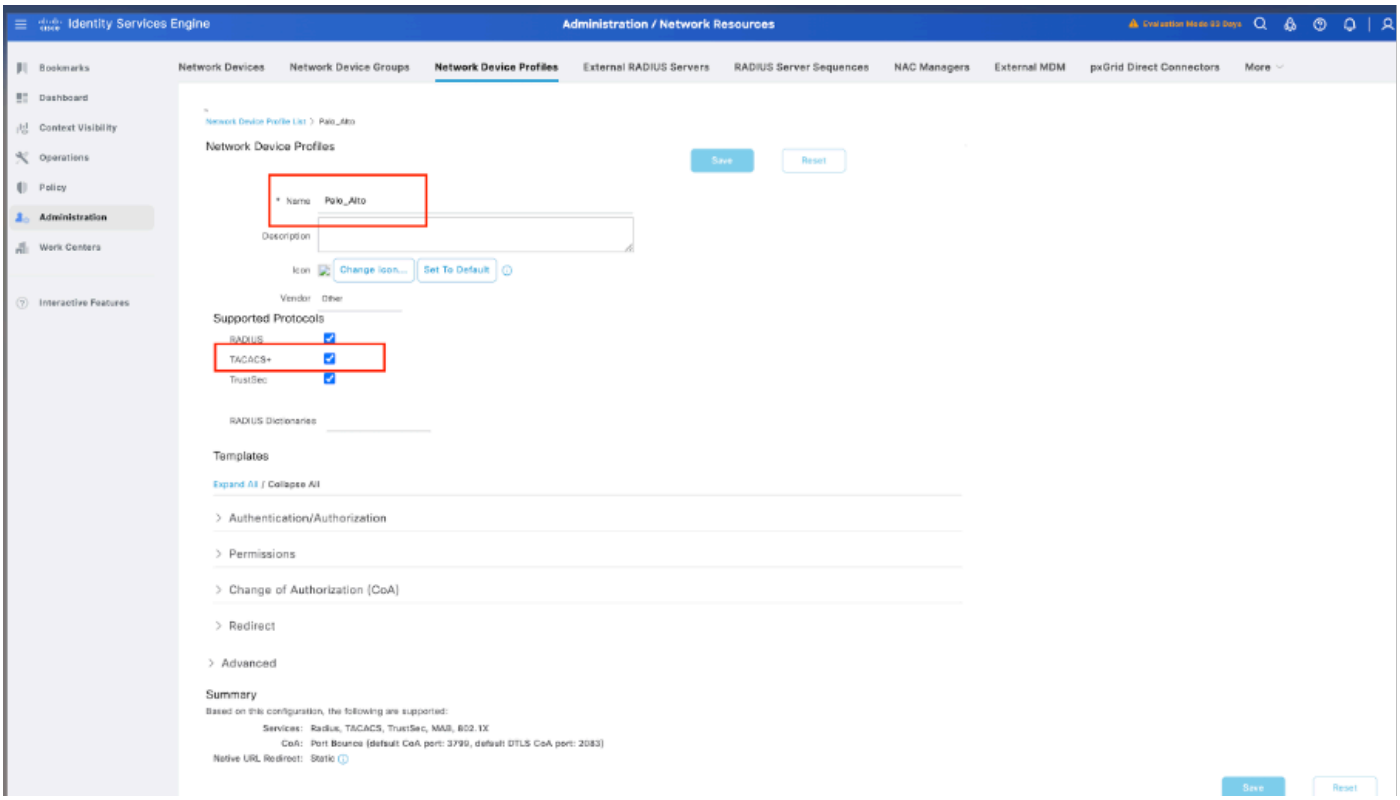


Etapa 2. Role para baixo para localizar o recurso Device Administration Service. Observe que a habilitação desse recurso exige que a persona do Serviço de política esteja ativa no nó, junto com as licenças TACACS+ disponíveis na implantação. Marque a caixa de seleção para ativar o recurso e salve a configuração.



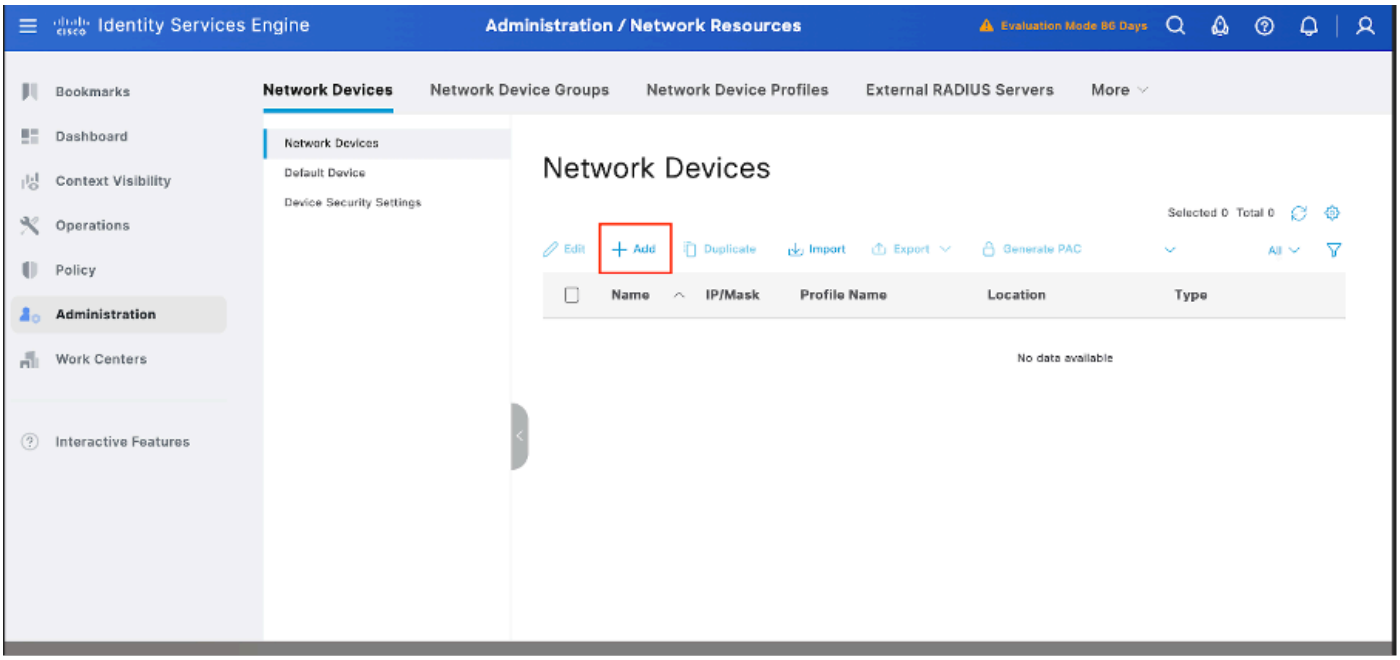
Etapa 3. Configurar o perfil do dispositivo de rede Palo Alto para o Cisco ISE.

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.



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

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



2. Clique em Adicionar e informe estes detalhes:

Nome: Palo-Alto

Endereço IP: <IP Palo-Alto>

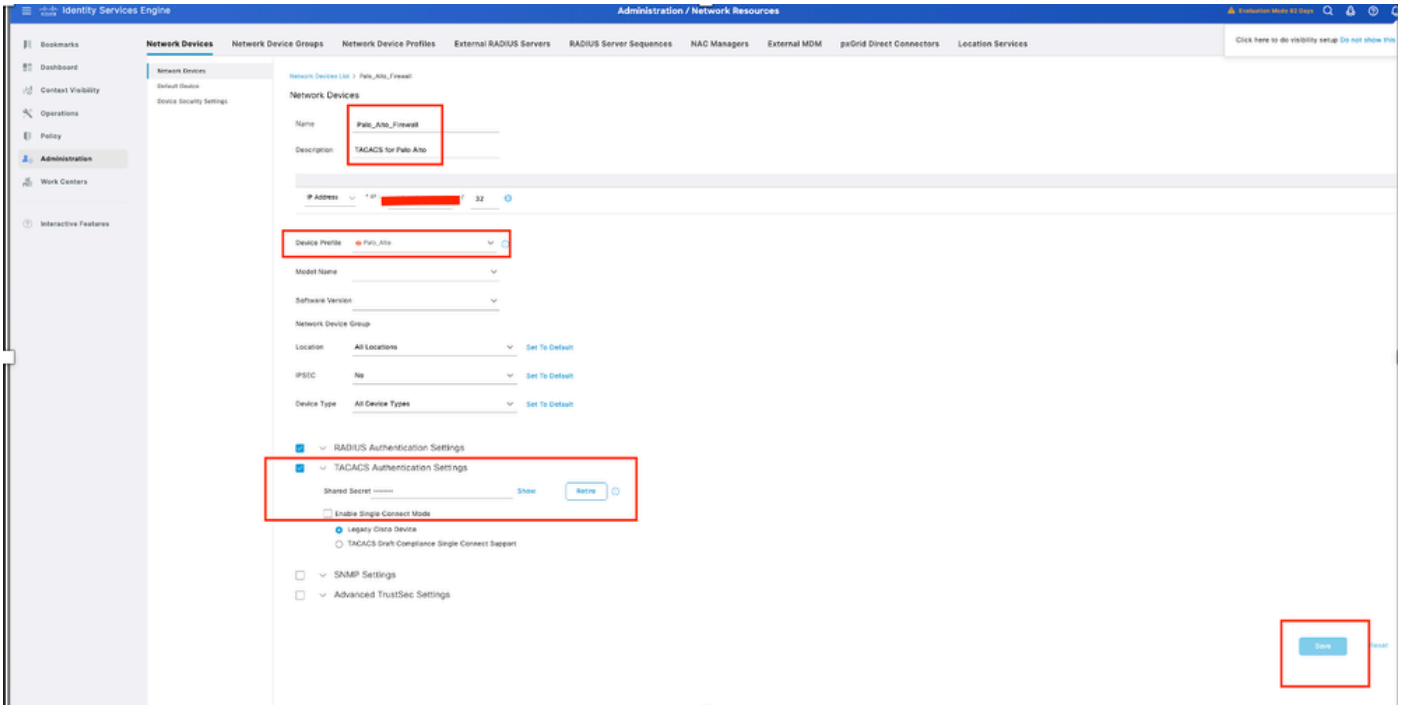
Perfil do dispositivo de rede: selecione Palo Alto

Configurações de autenticação TACACS:

Habilitar autenticação TACACS+

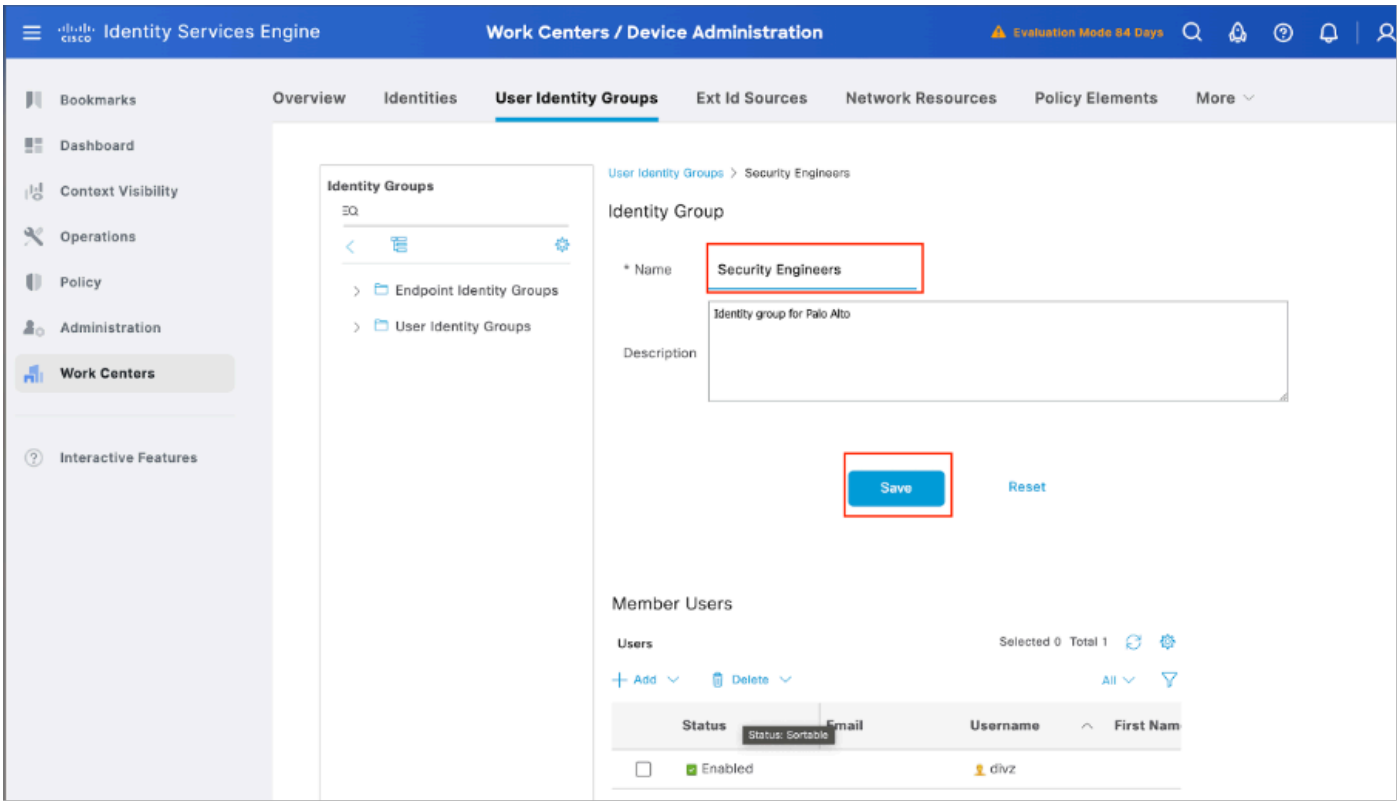
Insira o segredo compartilhado (deve corresponder à configuração da Palo Alto)

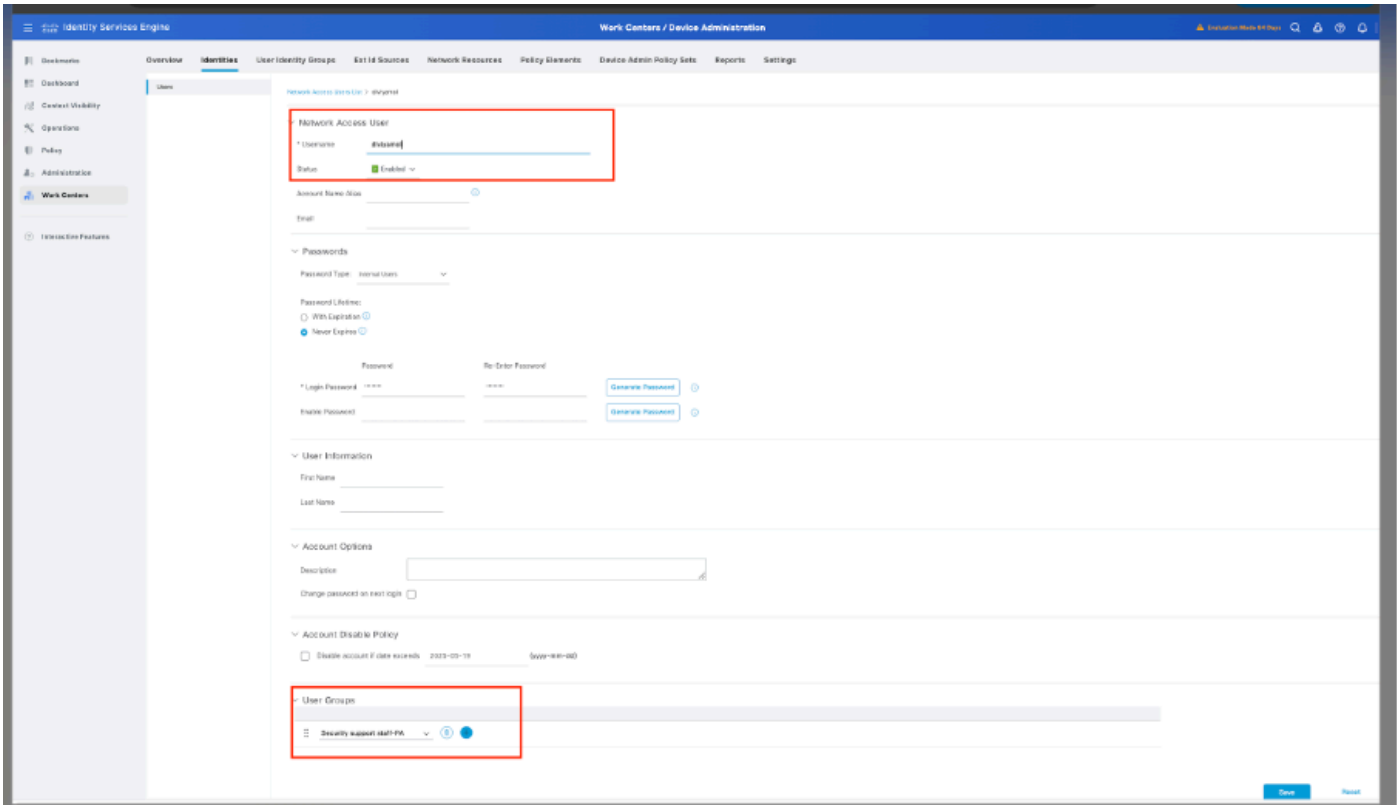
Click Save.

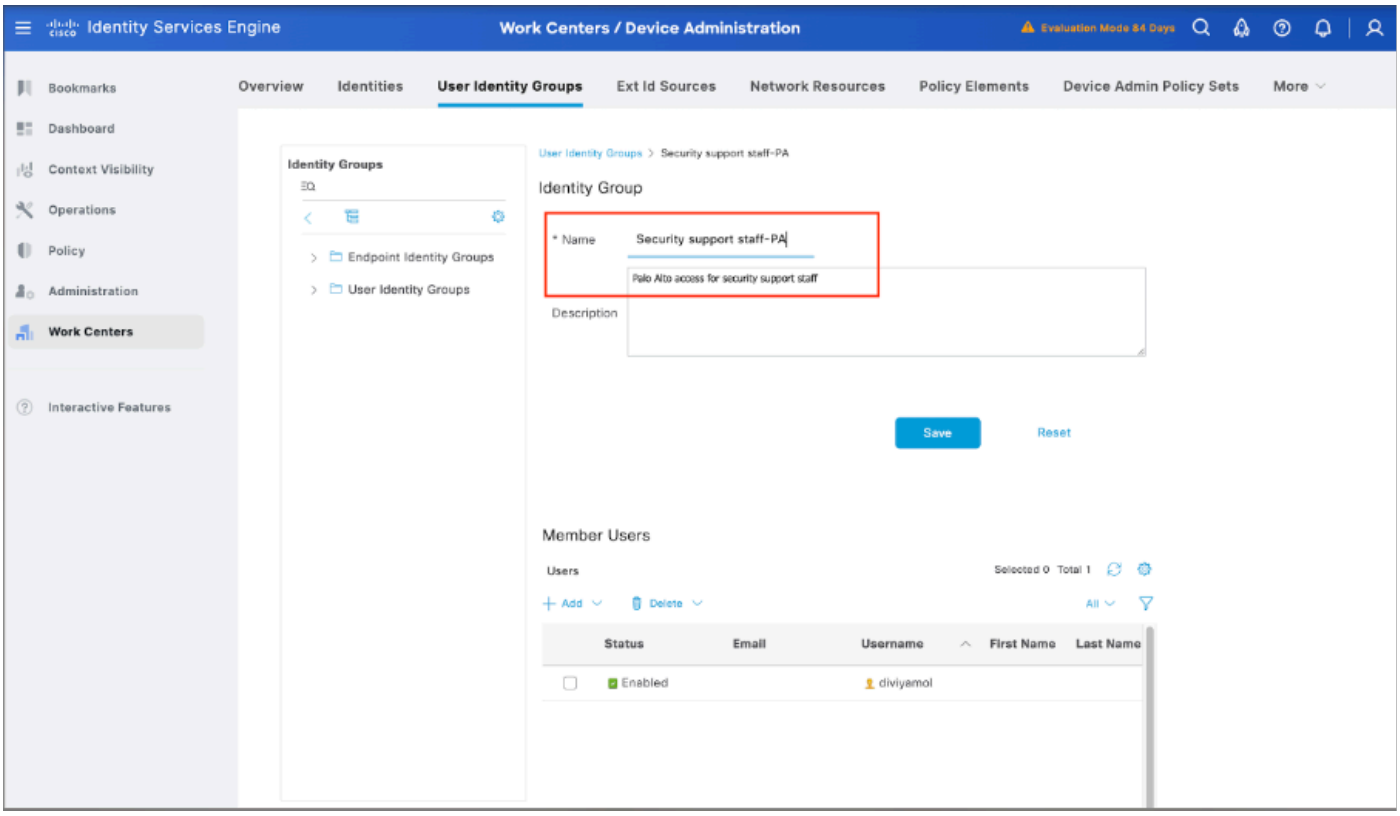


Etapa 5. Criar Grupos de Identidades de Usuário.

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 84 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
Endpoint Identity Groups
User Identity Groups
User Identity Groups > Security Engineers
Identity Group
* Name
Security Engineers
Description
Identity group for Palo Alto
Save
Reset
Member Users
Users
Selected 0 Total 1
Add
Delete
All
Status
Email
Username
First Nam
Status: Sortable
Enabled
divz

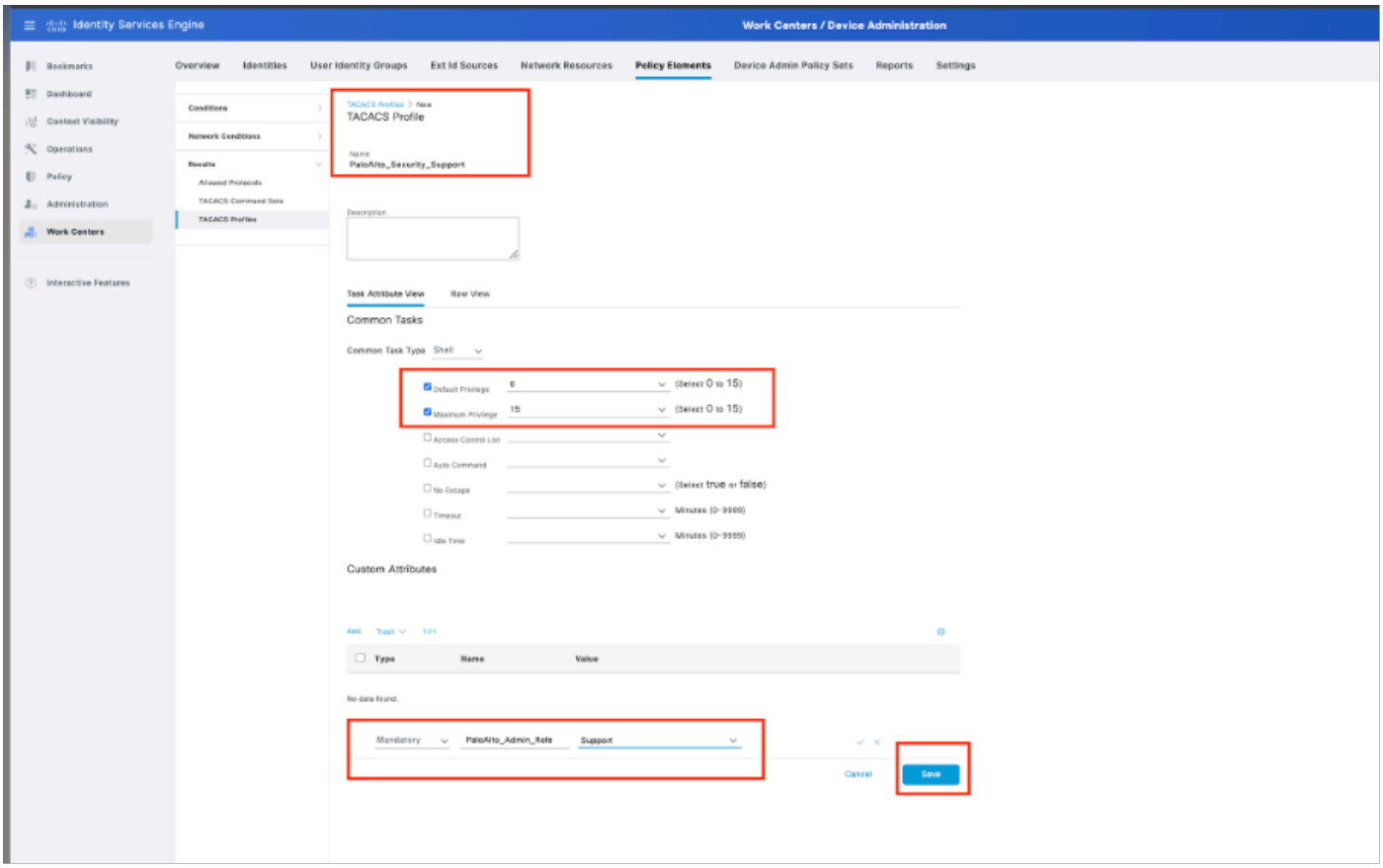

Identity Services Engine
Work Centers / Device Administration
Network Access User
Passwords
User Information
Account Options
Account Disable Policy
User Groups

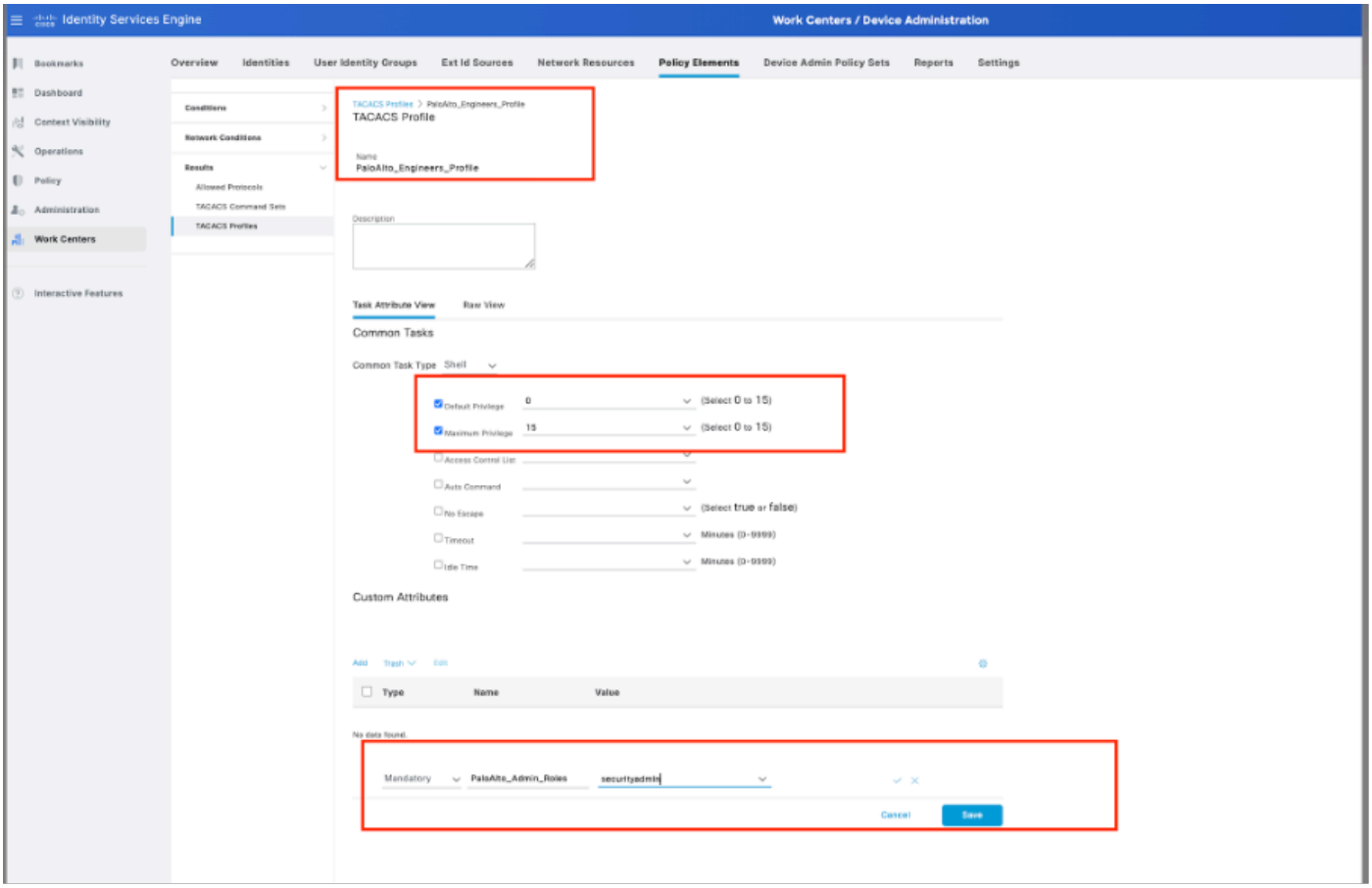


Etapa 6. Configurar Um Perfil TACACS.

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.





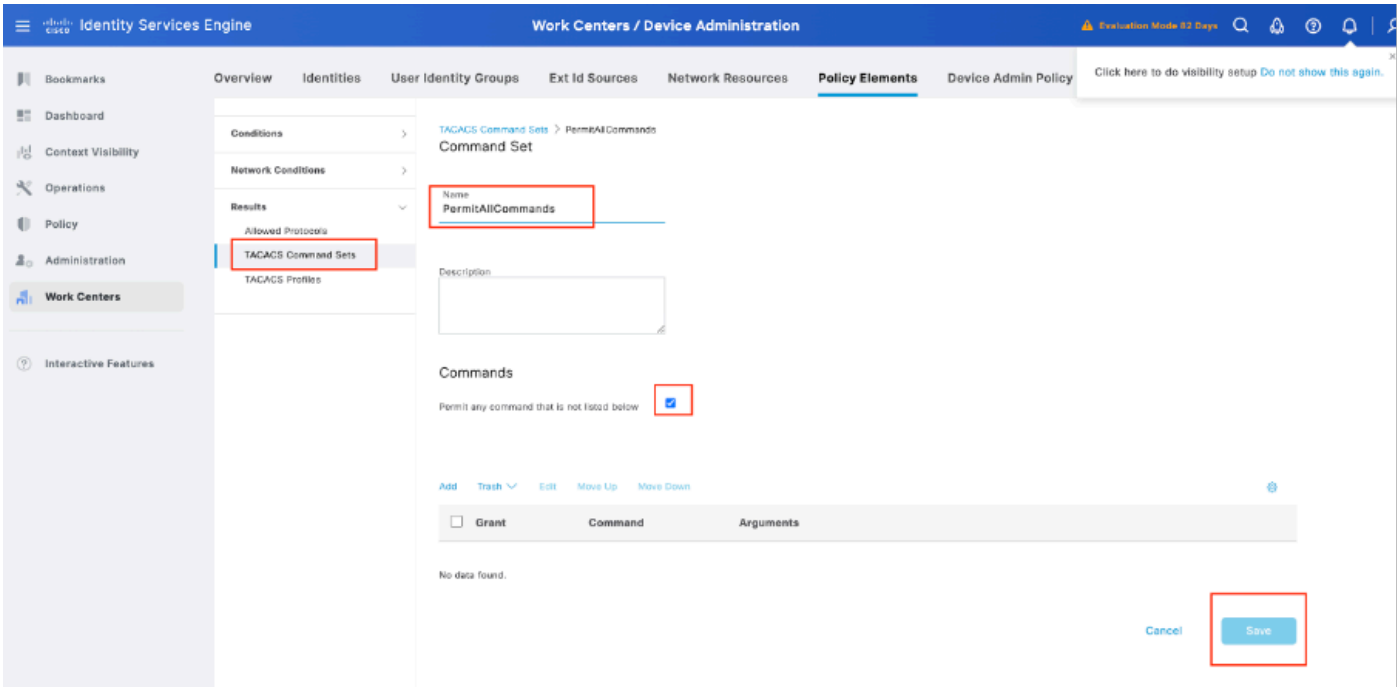
Etapa 6. Configurar conjuntos de comandos TACACS.

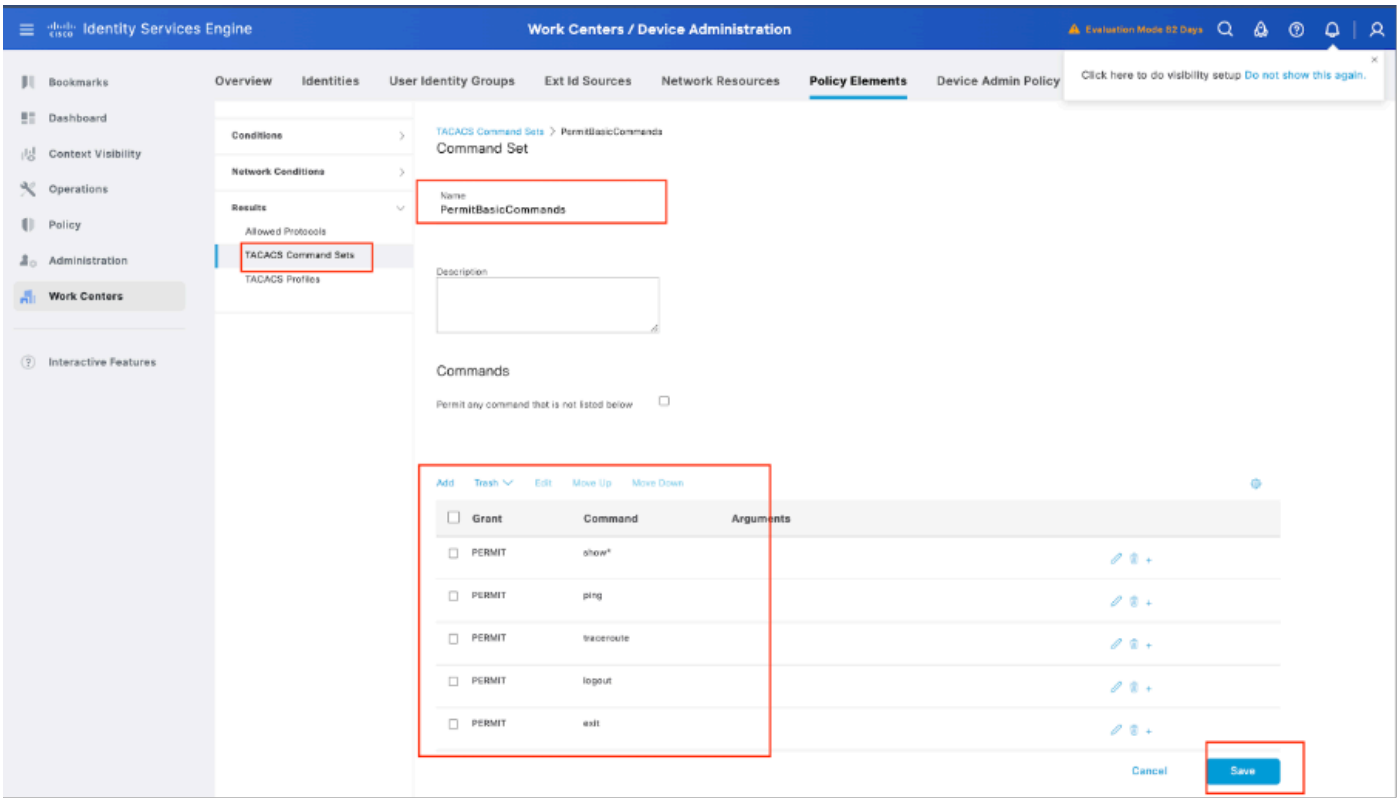
Agora, é hora de configurar quais comandos os usuários podem usar. Como você pode conceder

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.

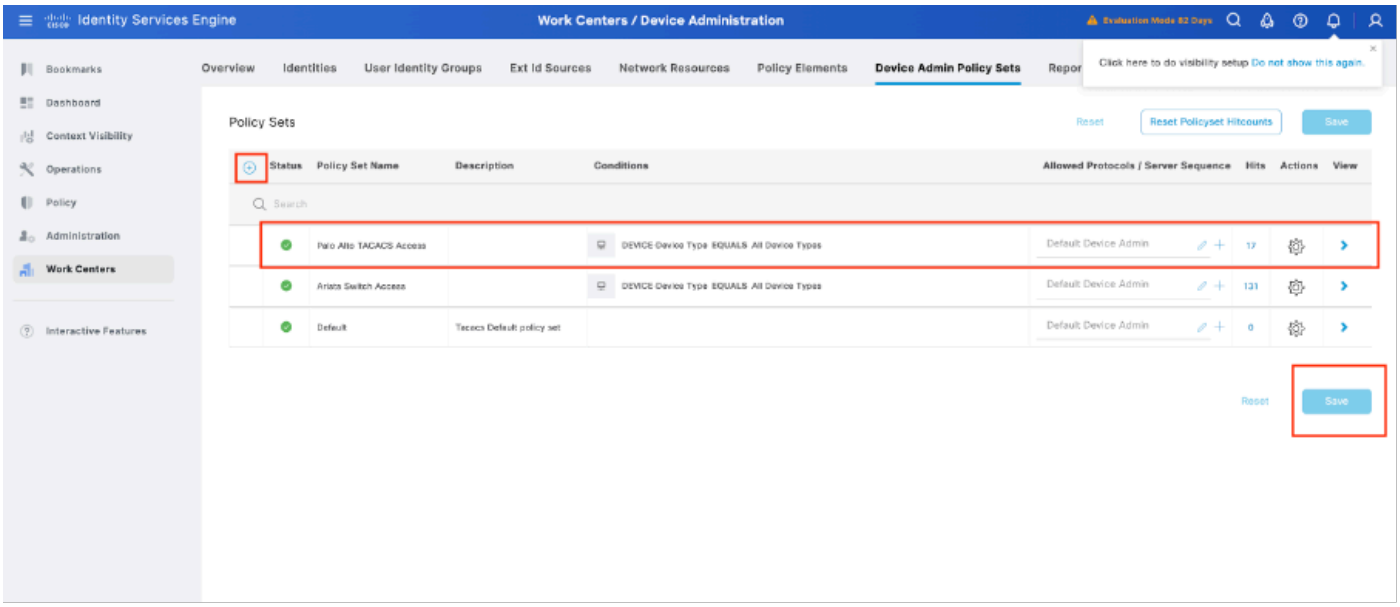
A única coisa que você precisa configurar neste conjunto de comandos TACACS é marcar a caixa para Permitir qualquer comando que não esteja listado abaixo.



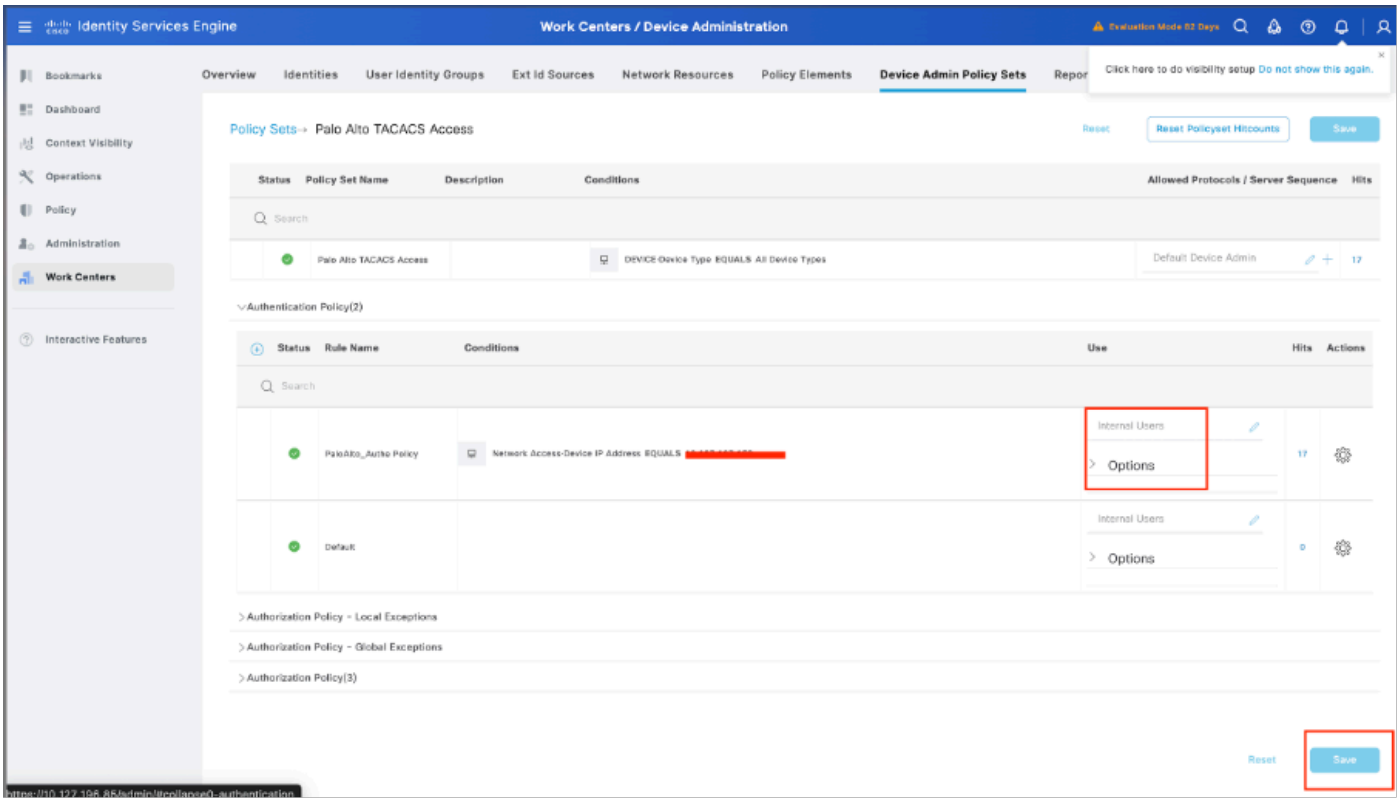


Etapa 7. Crie um Device Admin Policy Set a ser usado para seu Palo Alto, Navegue no menu Work Centers > Device Administration > Device Admin Policy Sets, Clique no ícone Add +.

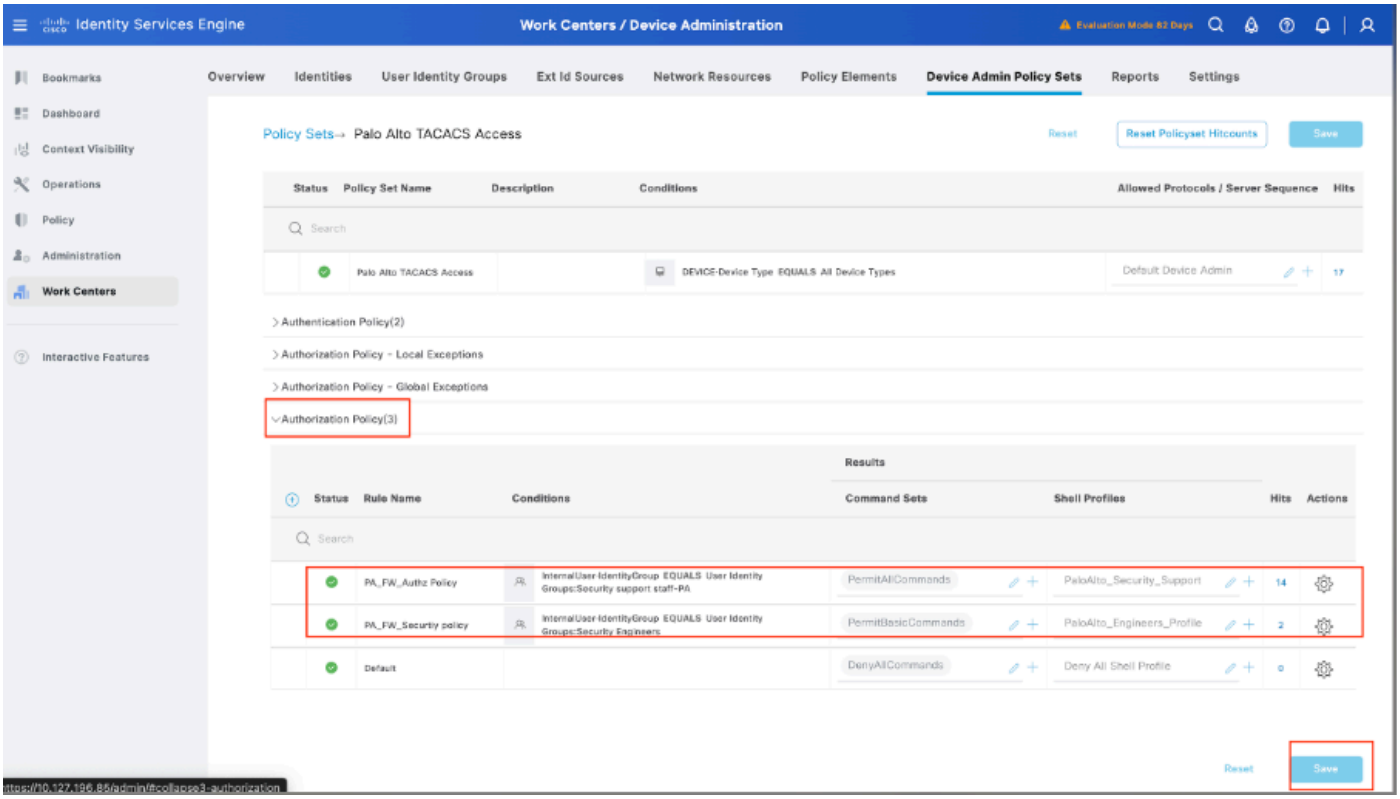
Etapa 8. Nomeie este novo Conjunto de políticas, adicione condições dependendo das características das autenticações TACACS+ que estão em andamento no Firewall Palo Alto e selecione como Allowed Protocols > Default Device Admin. Salve sua configuração.



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.



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.



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

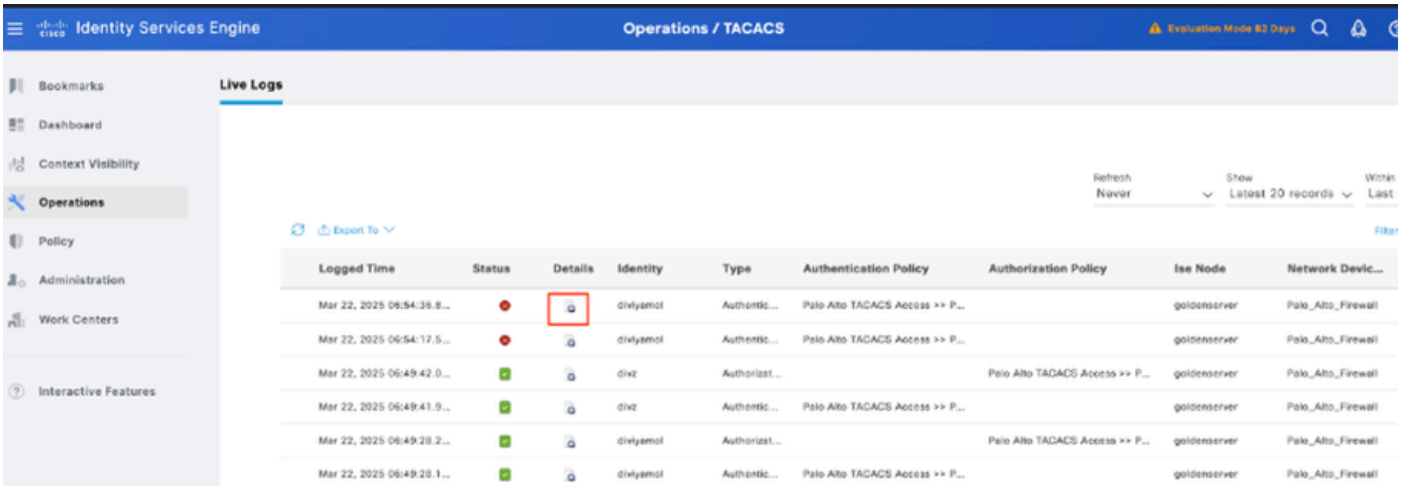
Etapa 1. Revise se se a capacidade de serviço TACACS+ está em execução, isso pode ser verificado em:

- 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+

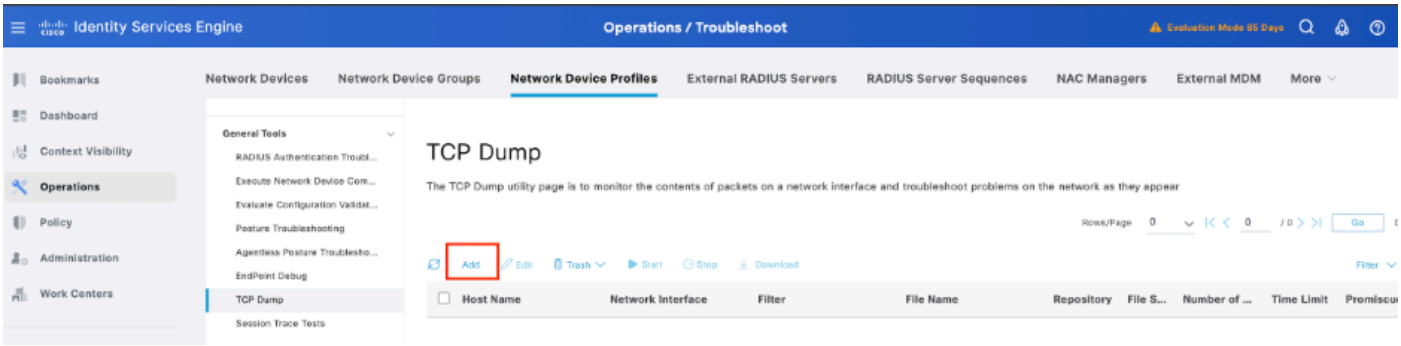
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

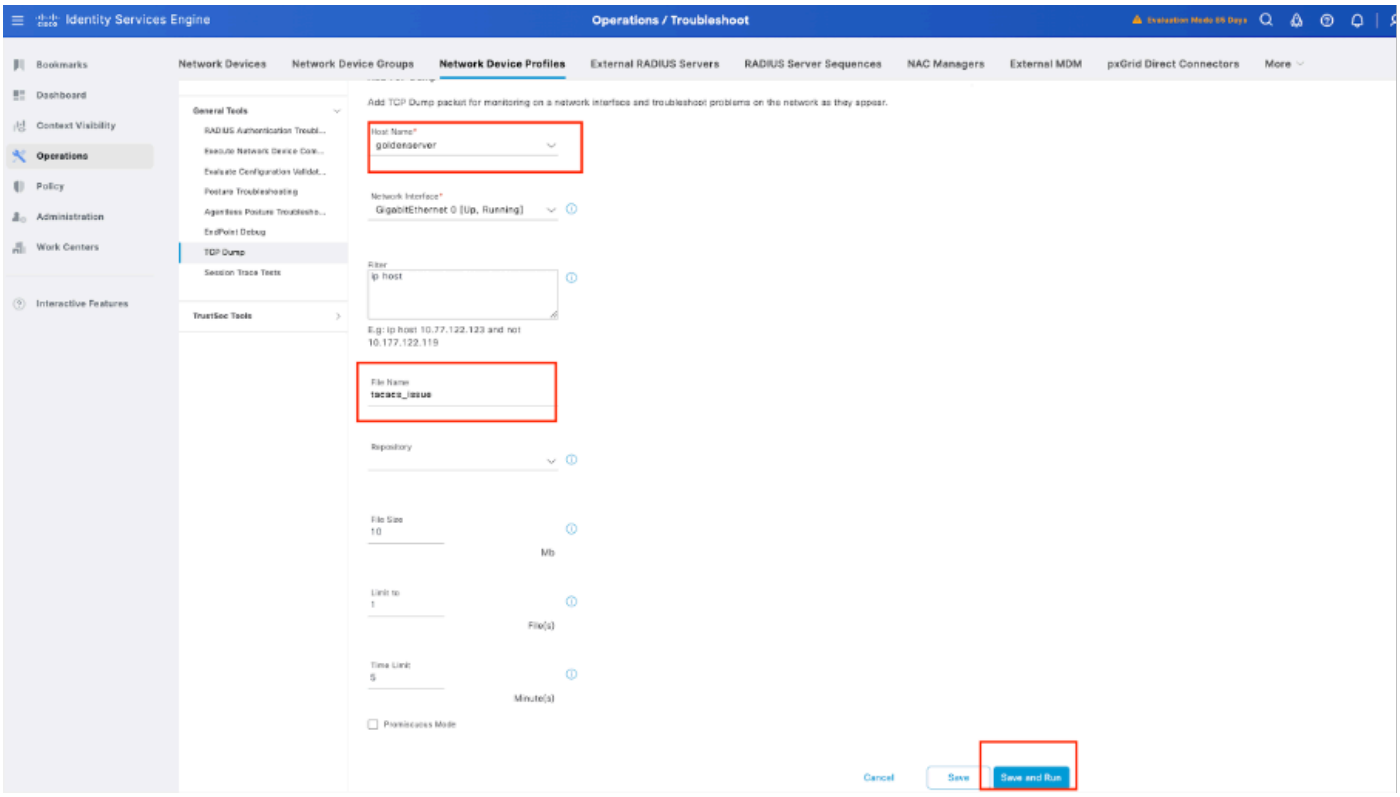
Etapa 2. Confirme se há registros em tempo real referentes a tentativas de autenticação TACACS+ : isso pode ser verificado no menu Operations -> TACACS -> Live logs.

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

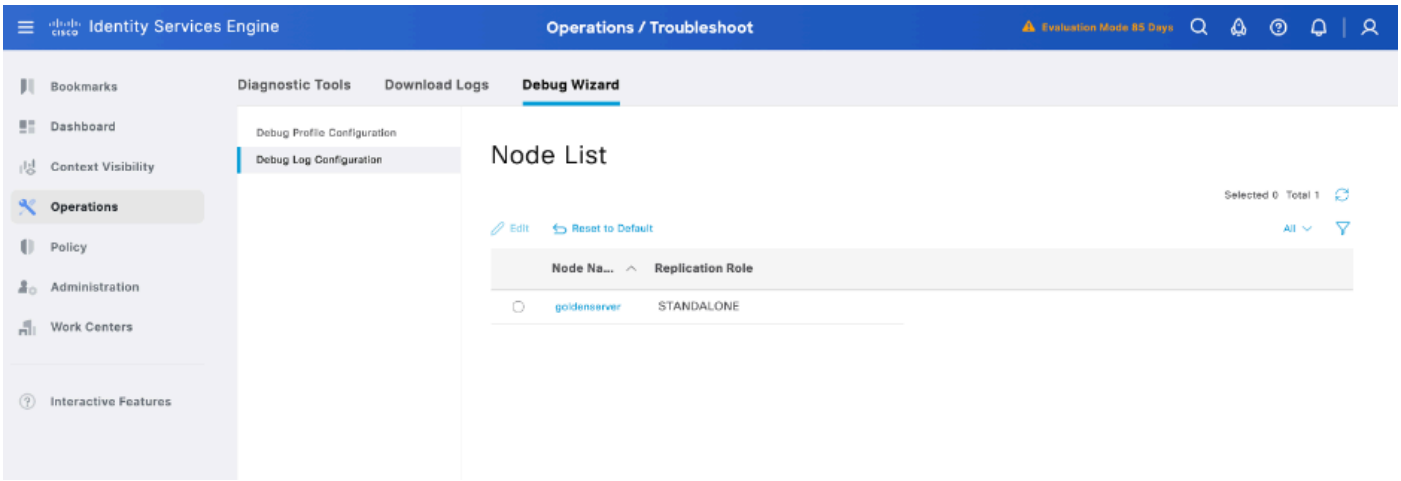


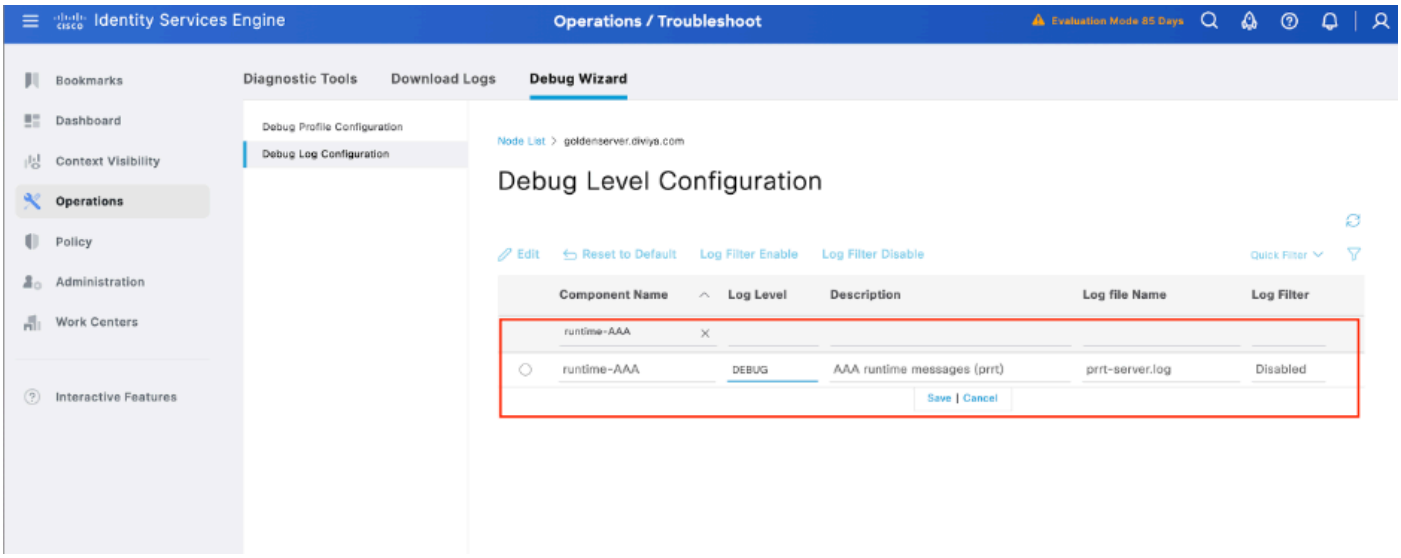
Etapa 3. Caso você não veja nenhum registro em tempo real, continue para fazer uma captura de pacote, navegue até o menu Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump e selecione Add.





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 .





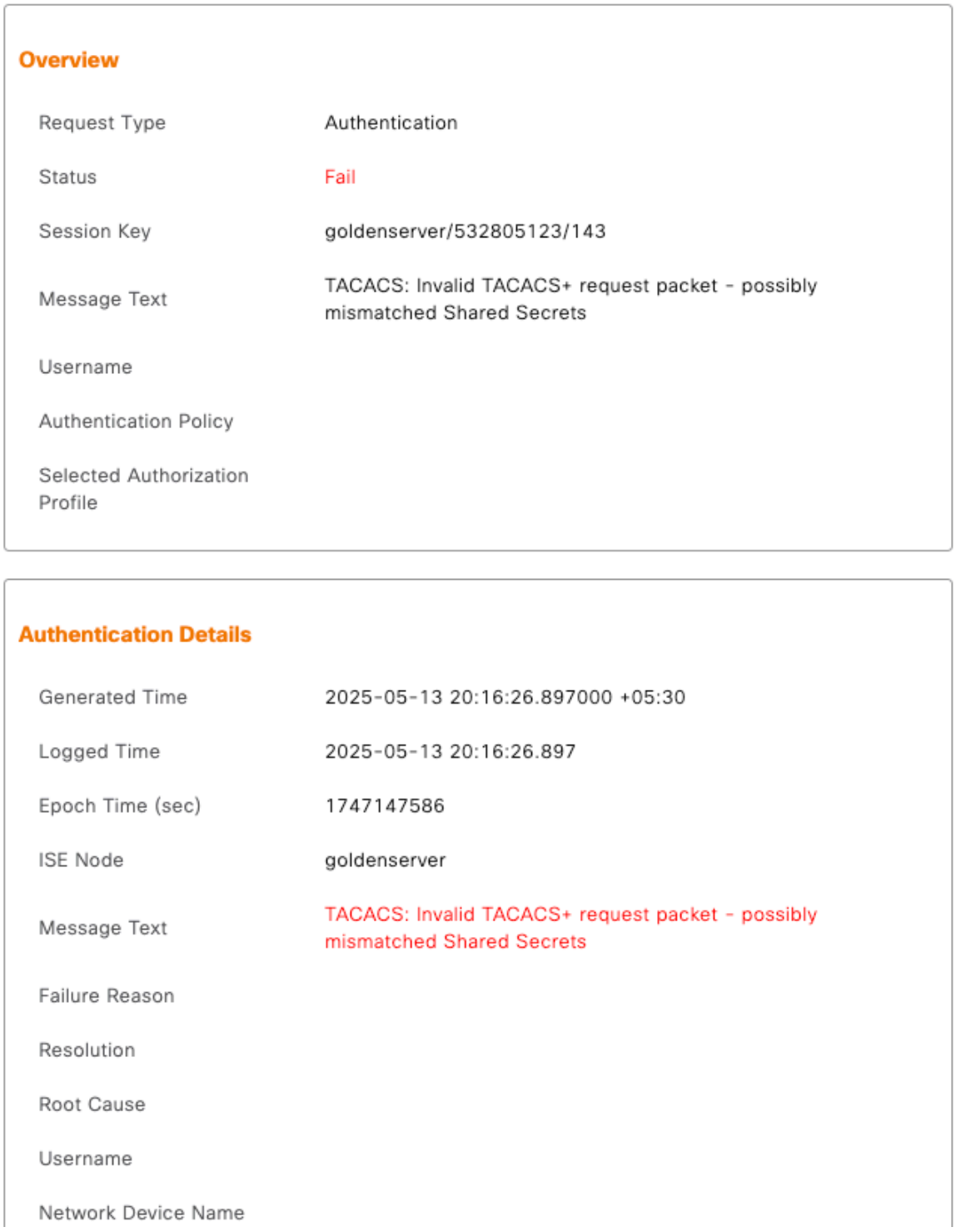
Identifique o componente runtime-AAA, defina seu nível de registro como debug, reproduza o problema e analise os registros para investigação adicional.

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.