

Configurar o TACACS+ com a interface Gigabit Ethernet 1 do ISE

Contents

[Introdução](#)

[Informações de Apoio](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração do Identity Services Engine para TACACS+](#)

[Configurar endereço IP para interface Gigabit Ethernet 1 no ISE](#)

[Ativar a administração de dispositivos no ISE](#)

[Adicionar um dispositivo de rede no ISE](#)

[Configurar conjuntos de comandos TACACS+](#)

[Configurar o perfil TACACS+](#)

[Configurar o perfil de autenticação e autorização TACACS+](#)

[Configurar usuários de acesso à rede para autenticação TACACS de NAD no ISE](#)

[Configurar roteador para TACACS+](#)

[Configurar o Cisco IOS Router para Autenticação e Autorização TACACS+](#)

[Configurar o switch para TACACS+](#)

[Configurar o switch para autenticação e autorização TACACS+](#)

[Verificação](#)

[Verificação do roteador](#)

[Verificação do Switch](#)

[Troubleshooting](#)

[Verificação do Dispositivo de Rede \(Switch\)](#)

[Verificação do Dispositivo de Rede \(Switch\)](#)

[Referência](#)

Introdução

Este documento descreve a configuração do ISE TACACS+ com a interface Gigabit Ethernet 1 onde o roteador e o switch funcionam como dispositivos de rede.

Informações de Apoio

O Cisco ISE suporta até 6 interfaces Ethernet. Ele pode ter apenas três ligações, ligação 0, ligação 1 e ligação 2. Você não pode alterar as interfaces que fazem parte de uma ligação ou

alterar a função da interface em uma ligação.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes tópicos:

- Conhecimento básico de rede
- Cisco Identity Service Engine

Componentes Utilizados

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

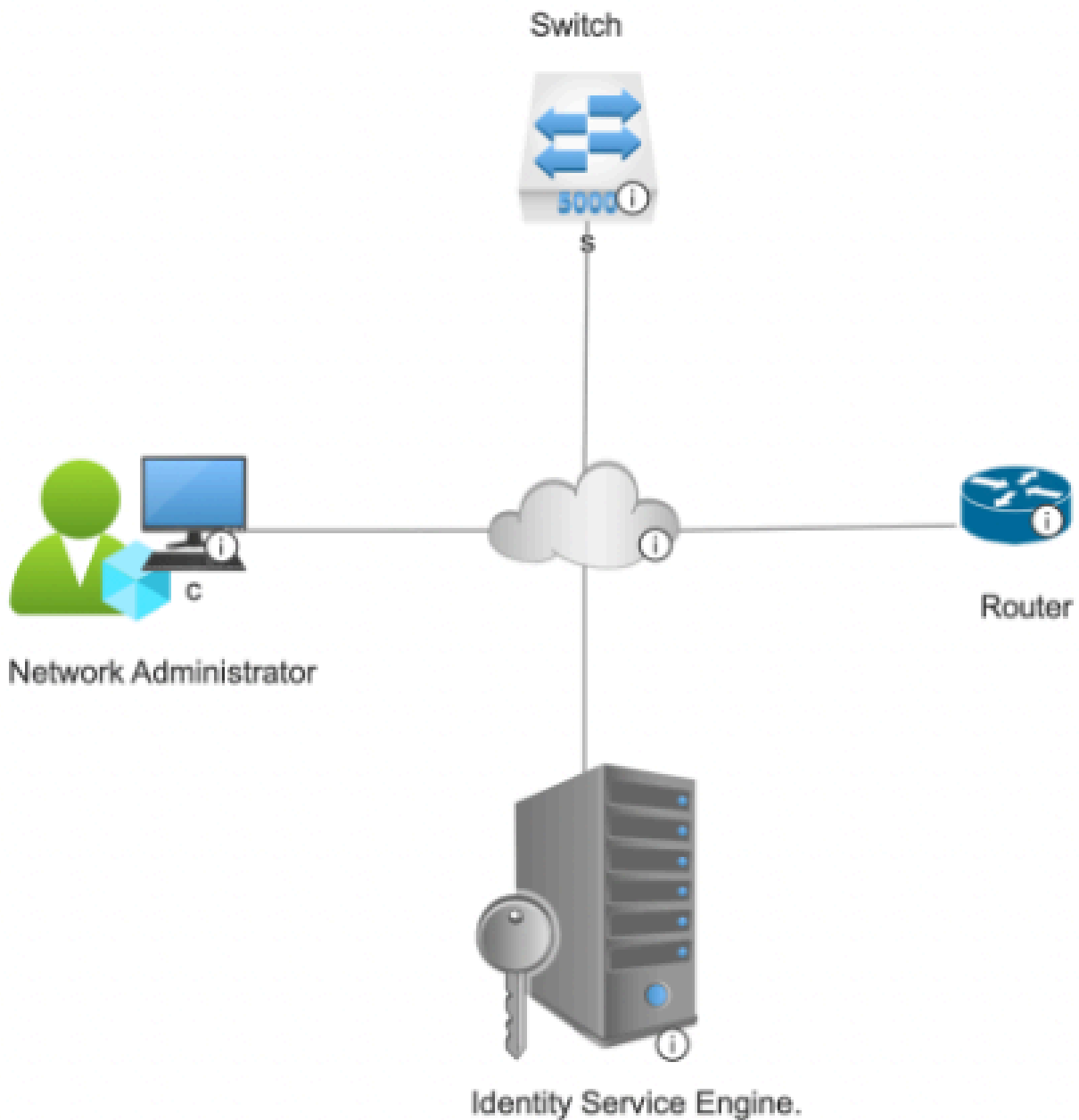
- Cisco Identity Service Engine v3.3
- Versão do Software Cisco IOS® 17.x
- Switch Cisco C9200.

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.

Configurar

O objetivo da configuração é: Configure Gigabit Ethernet 1 do ISE para TACACS+ e autentique o switch e o roteador com TACACS+ com ISE como servidor de autenticação.

Diagrama de Rede



Topologia de rede

Configuração do Identity Services Engine para TACACS+

Configurar endereço IP para interface Gigabit Ethernet 1 no ISE

1. Efetue login na CLI do nó PSN do ISE onde Device admin está habilitado e verifique as interfaces disponíveis usando o comando `show interface`:

```
honey/admin# show interface
```

```
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 100.233.1.1 netmask 255.255.255.0 broadcast 100.233.1.255
  inet6 fe80::8ca9:c4ff:fe1b:6827 prefixlen 64 scopeid 0x20<link>
  ether 8e:a9:c4:1b:68:27 txqueuelen 1000 (Ethernet)
  RX packets 629139 bytes 226044590 (215.5 MiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 674817 bytes 100272799 (95.6 MiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 100.233.1.2 netmask 255.255.255.0 broadcast 100.233.1.255
  inet6 fd00::1:8:1 prefixlen 112 scopeid 0x0<global>
  inet6 fe80::304a:47ff:fe59:264a prefixlen 64 scopeid 0x20<link>
  ether 32:4a:47:59:26:4a txqueuelen 1000 (Ethernet)
  RX packets 438392 bytes 363642766 (346.7 MiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 481076 bytes 369977760 (352.8 MiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
GigabitEthernet 0
```

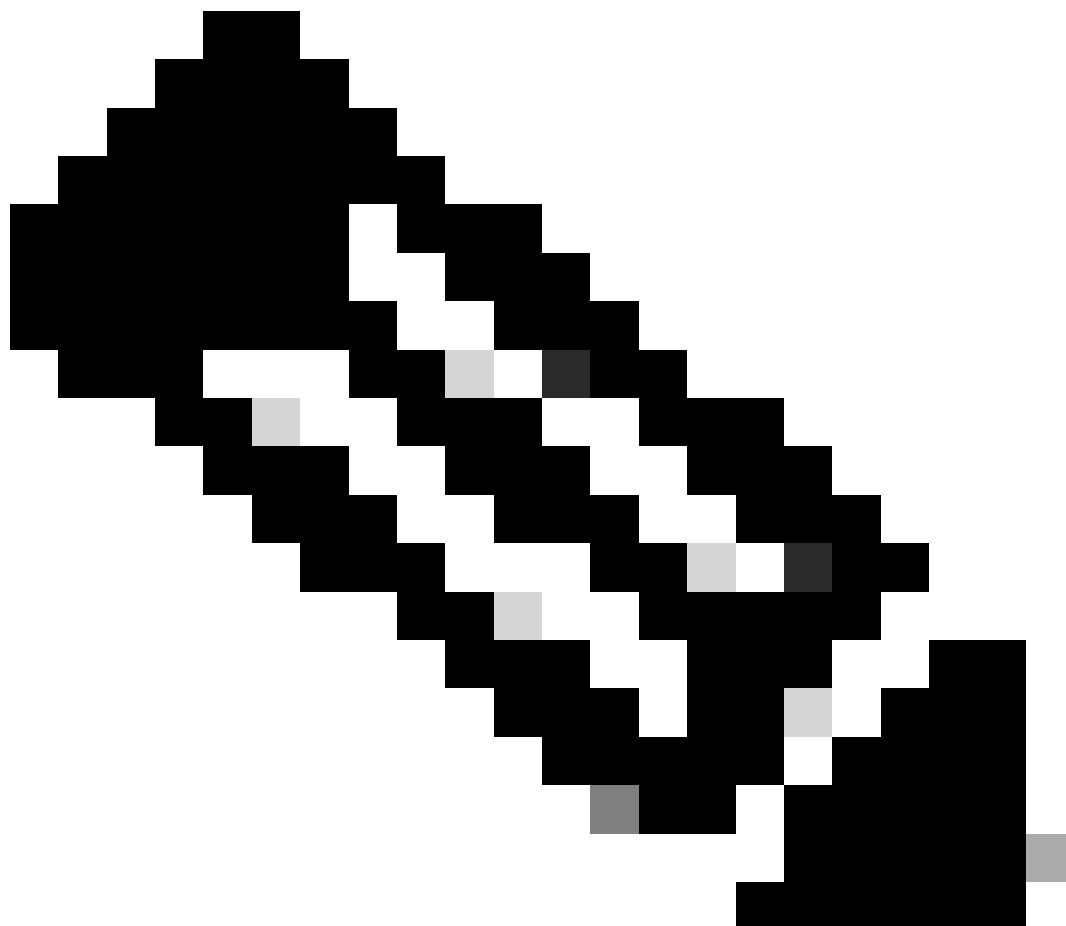
```
flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 10.100.20.13 netmask 255.255.255.0 broadcast 10.100.20.255
  inet6 fe80::250:56ff:fe8b:1b81 prefixlen 64 scopeid 0x20<link>
  ether 00:50:56:8b:1b:81 txqueuelen 1000 (Ethernet)
  RX packets 1271564 bytes 203676256 (194.2 MiB)
  RX errors 0 dropped 266 overruns 0 frame 0
  TX packets 76672 bytes 116577841 (111.1 MiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
GigabitEthernet 1
```

```
flags=4098<BROADCAST,MULTICAST> mtu 1500
  ether 00:50:56:8b:e1:af txqueuelen 1000 (Ethernet)
  RX packets 262 bytes 36180 (35.3 KiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 7 bytes 606 (606.0 B)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
GigabitEthernet 2
```

```
flags=4098<BROADCAST,MULTICAST> mtu 1500
  ether 00:50:56:8b:f8:5f txqueuelen 1000 (Ethernet)
  RX packets 268 bytes 36228 (35.3 KiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 6 bytes 516 (516.0 B)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



Note: Nessa configuração, apenas três interfaces são configuradas no ISE, com foco na interface Gigabit Ethernet 1. O mesmo procedimento pode ser aplicado para configurar o endereço IP para todas as interfaces. Por padrão, o ISE suporta até seis interfaces Gigabit Ethernet.

2. Na CLI do mesmo nó PSN, atribua um endereço IP à interface Gigabit Ethernet 1 usando estes comandos:

```
hostnameofise#configure t
```

```
hostnameofise/admin(config)#interface Gigabit Ethernet 1
```

```
hostnameofise/admin(config-GigabitEthernet-1)# <endereço ip> <máscara de rede de sub-rede>
```

% A alteração do endereço IP pode fazer com que os serviços do ise sejam reiniciados

Continuar com a alteração do endereço IP?

Prosseguir? [sim,não] sim

3. Executar a etapa 2 faz com que os serviços de nó do ISE sejam reiniciados. Para verificar o status dos serviços do ISE, execute o comando `show application status ise` e verifique se o status dos serviços está em execução, de acordo com esta captura de tela:

```
honey/admin#show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	1739169
Database Server	running	102 PROCESSES
Application Server	running	1755746
Profiler Database	running	1746379
ISE Indexing Engine	running	1757121
AD Connector	running	1759148
M&T Session Database	running	1752122
M&T Log Processor	running	1755926
Certificate Authority Service	running	1759026
EST Service	running	1786647
SXP Engine Service	disabled	
TC-NAC Service	disabled	
PassiveID WMI Service	disabled	
PassiveID Syslog Service	disabled	
PassiveID API Service	disabled	
PassiveID Agent Service	disabled	
PassiveID Endpoint Service	disabled	
PassiveID SPAN Service	disabled	
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	
ISE Messaging Service	running	1743222
ISE API Gateway Database Service	running	1745409
ISE API Gateway Service	running	1750887
ISE pxGrid Direct Service	running	1874179
Segmentation Policy Service	disabled	
REST Auth Service	disabled	
SSE Connector	disabled	
Hermes (pxGrid Cloud Agent)	disabled	
McTrust (Meraki Sync Service)	disabled	
ISE Node Exporter	running	1760519
ISE Prometheus Service	running	1762540
ISE Grafana Service	running	1765779
ISE MNT LogAnalytics Elasticsearch	running	1768218
ISE Logstash Service	running	1773207
ISE Kibana Service	running	1774914
ISE Native IPsec Service	running	1779658
MFC Profiler	running	1932013

Verificação do status do serviço do ISE

4. Verifique o endereço IP da interface Gig1 usando o comando `show interface`:

V


```

honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.106.20.1 netmask 255.255.255.0 broadcast 10.106.20.255
    inet6 fe80::8ca9:c4ff:fe1b:6827 prefixlen 64 scopeid 0x20<link>
    ether 8e:a9:c4:1b:68:27 txqueuelen 1000 (Ethernet)
    RX packets 633876 bytes 228753800 (218.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 680052 bytes 102100762 (97.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.106.20.1 netmask 255.255.255.0 broadcast 10.106.20.255
    inet6 fd00::1:8:1 prefixlen 112 scopeid 0x0<global>
    inet6 fe80::304a:47ff:fe59:264a prefixlen 64 scopeid 0x20<link>
    ether 32:4a:47:59:26:4a txqueuelen 1000 (Ethernet)
    RX packets 503576 bytes 516105026 (492.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 595701 bytes 383404526 (365.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

GigabitEthernet 0
    flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.106.20.56 netmask 255.255.255.0 broadcast 10.106.20.255
    inet6 fe80::250:56ff:fe8b:1b81 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:8b:1b:81 txqueuelen 1000 (Ethernet)
    RX packets 1387052 bytes 213478717 (203.5 MiB)
    RX errors 0 dropped 266 overruns 0 frame 0
    TX packets 136494 bytes 261900250 (249.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

GigabitEthernet 1
    flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.106.20.56 netmask 255.255.255.0 broadcast 10.106.20.255
    inet6 fe80::250:56ff:fe8b:e1af prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:8b:e1:af txqueuelen 1000 (Ethernet)
    RX packets 5165 bytes 1072036 (1.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 2260 (2.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Verificação do endereço IP da interface ISE Gig2 a partir do CLI

5. Verifique a permissão da porta 49 no nó ISE usando o comando show ports | inc 49 comando:

```

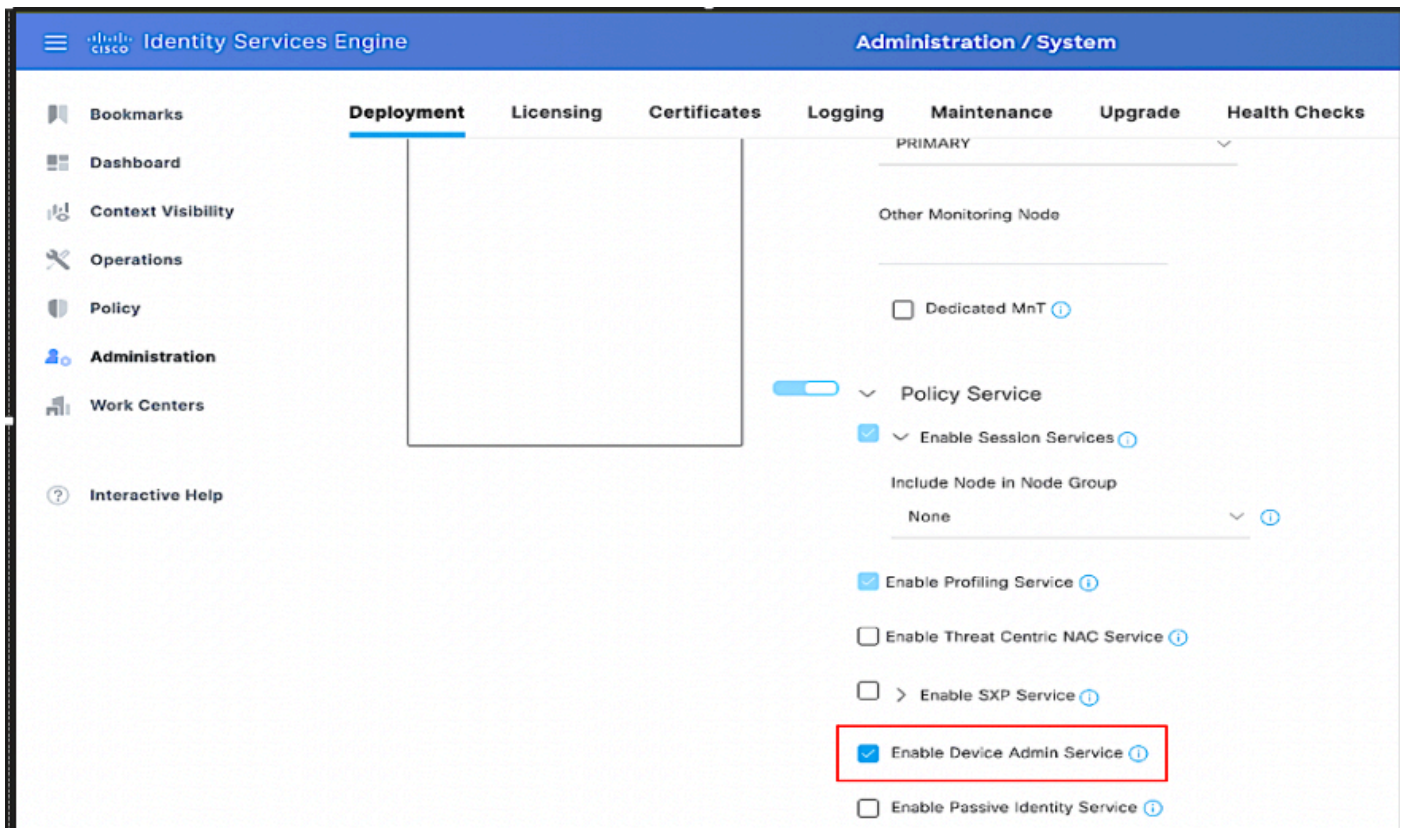
honey/admin#show ports | include 49
    tcp: 127.0.0.1:8888, 169.254.4.1:49, 169.254.2.1:49, 10.106.20.1:49, 10.106.20.56:49,

```

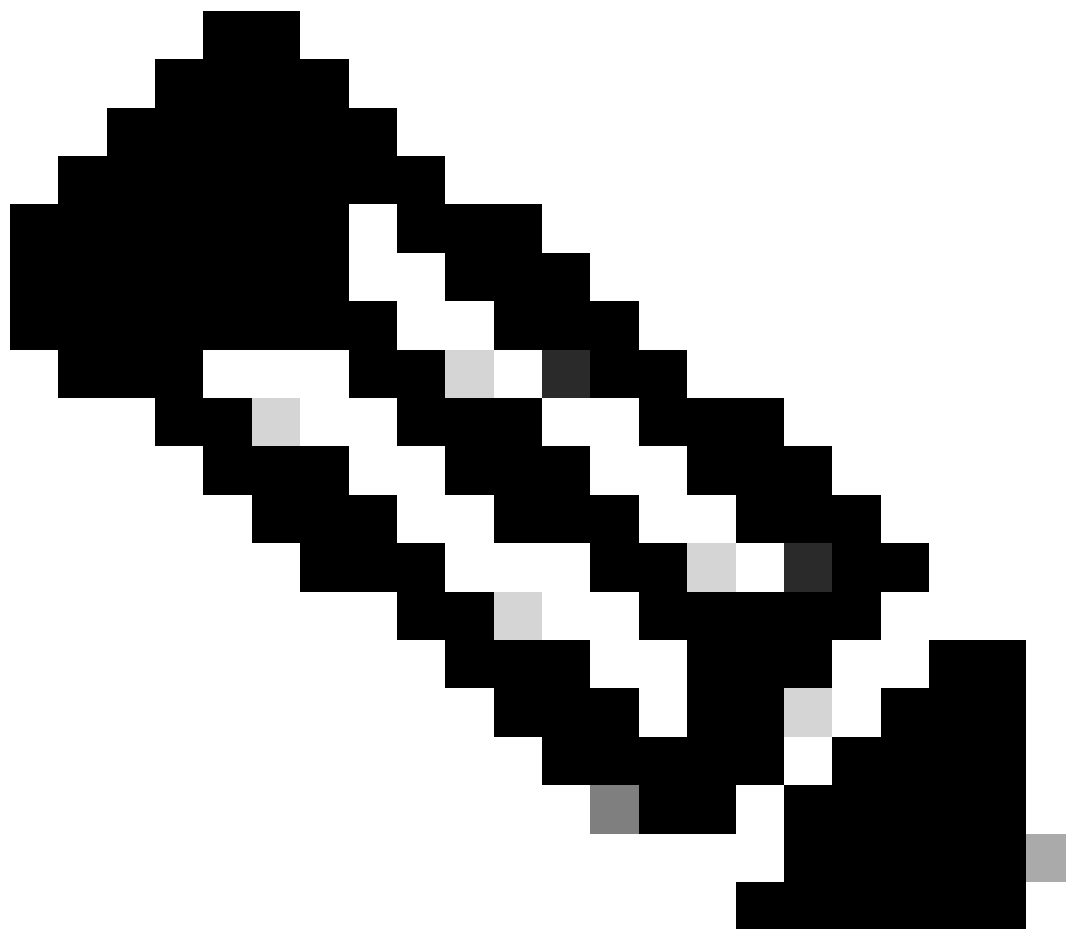
verificação da autorização do porto 49 no ISE

Ativar a administração de dispositivos no ISE

Navegue para GUI do ISE > Administração > Implantação > Selecione o nó PSN e marque Ativar serviço de administração de dispositivo:



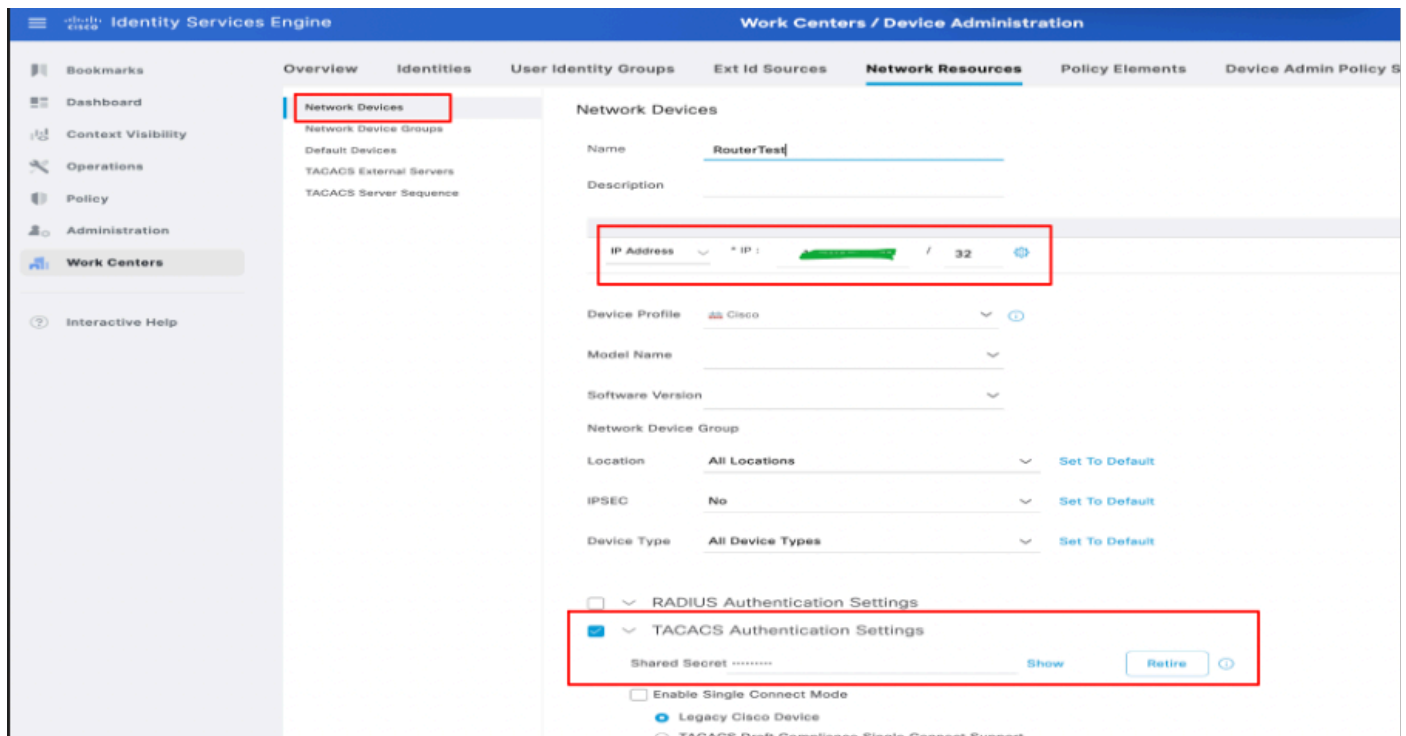
Ativação do serviço de administração de dispositivos no ISE



Note: Para ativar o serviço Device Admin, é necessária uma Licença de Administração do Dispositivo.

Adicionar um dispositivo de rede no ISE

1. Navegue até Centros de trabalho > Administração de dispositivos > Recursos de rede > Dispositivos de rede. Clique em Add. Forneça Nome, Endereço IP. Marque a caixa de seleção TACACS+ Authentication Settings e forneça a chave Shared Secret.



Configuração do dispositivo de rede no ISE

2. Siga o procedimento acima para adicionar todos os dispositivos de rede necessários para a autenticação TACACS.

Configurar conjuntos de comandos TACACS+

Dois conjuntos de comandos estão configurados para esta demonstração:

`Permit_all_commands`, é atribuído ao administrador de usuário e permite todos os comandos no dispositivo.

`permit_show_commands`, é atribuído a um usuário e permite apenas comandos show

1. Navegue até Centros de trabalho > Administração de dispositivo > Resultados de política > Conjuntos de comandos TACACS. Clique em Adicionar. Forneça o nome `PermitAllCommands` e escolha a caixa de seleção Permitir qualquer comando que não esteja listada. Clique em Submit.

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring TACACS Command Sets. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Help. The main content area is titled 'TACACS Command Sets' and includes sections for 'Conditions', 'Network Conditions', 'Results', 'Allowed Protocols', and 'TACACS Profiles'. The 'Results' section is expanded, showing a 'Name' field with the value 'Permit_all_commands' and a 'Description' field with the text 'This allows all the commands which are not listed in the below list.' Below these fields is a 'Commands' section with a checkbox labeled 'Permit any command that is not listed below' which is checked. At the bottom, there is a table with columns 'Grant', 'Command', and 'Arguments', and a message 'No data found.'

Configuração de conjuntos de comandos no ISE

2. Navegue até Centros de Trabalho > Administração de Dispositivo > Resultados de Política > Conjuntos de Comandos TACACS. Clique em Adicionar. Forneça o Nome PermitShowCommands, clique em Adicionar, e, finalmente, em permitir show e sair. Por padrão, se os argumentos forem deixados em branco, todos os argumentos serão incluídos. Clique em Submit.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Device Administration'. The left sidebar contains various navigation options, with 'Work Centers' selected. The main content area is titled 'Policy Elements' and shows the configuration for a 'TACACS Command Set' named 'permit_show_commands'. The 'Name' field is set to 'permit_show_commands'. The 'Description' field contains the text: 'Only commands which are added in the below list are allowed.' The 'Commands' section has a checkbox labeled 'Permit any command that is not listed below' which is unchecked. Below this, there is a table with columns 'Grant', 'Command', and 'Arguments'. The table contains three rows: 'PERMIT', 'exit', and 'Config'; 'DENY', 'Config'; and 'PERMIT', 'show'. Each row has a checkbox in the 'Grant' column and a blue pencil icon in the 'Arguments' column. The table is highlighted with a red box.

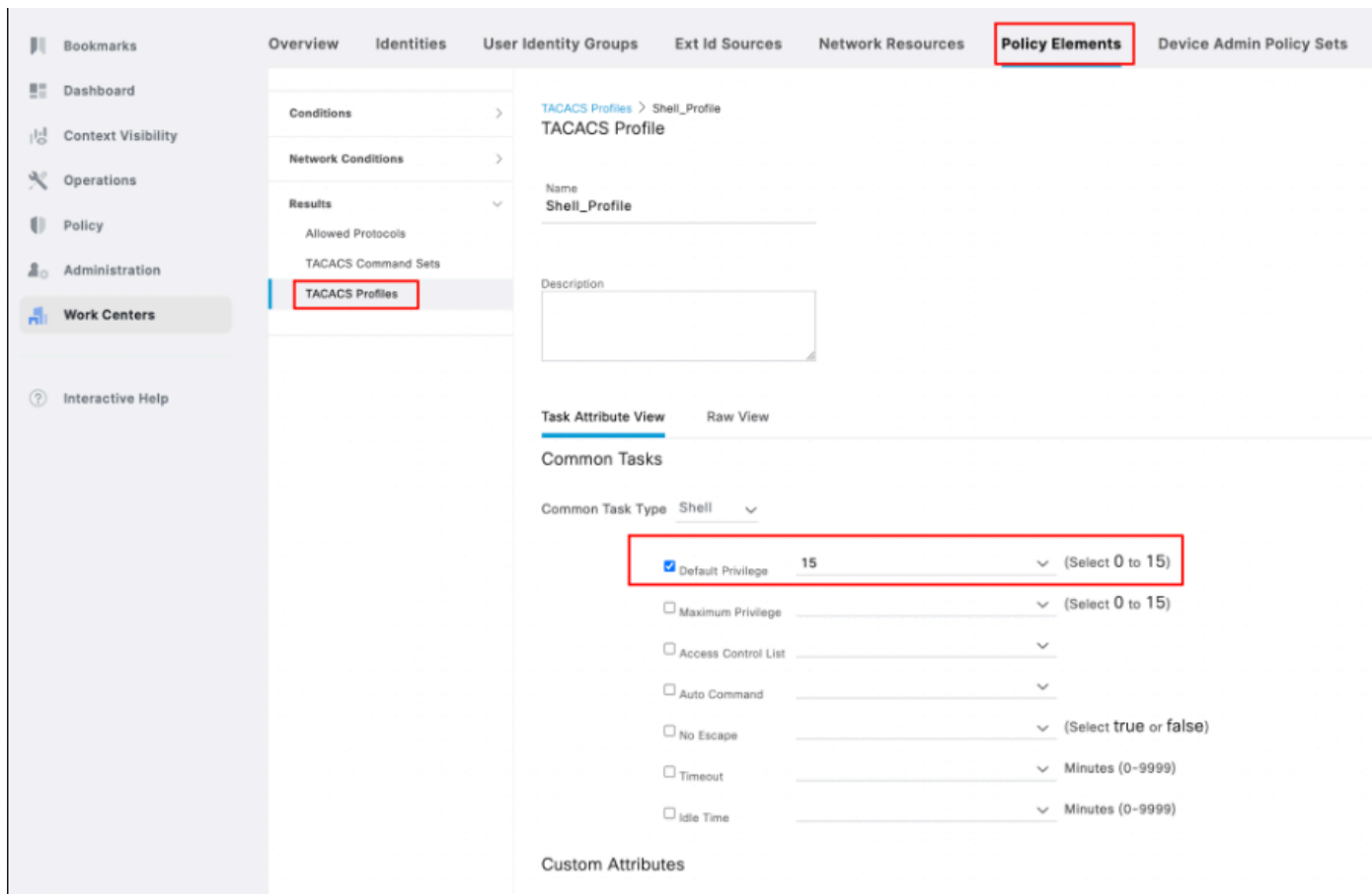
Grant	Command	Arguments
☐	PERMIT	exit
☐	DENY	Config
☐	PERMIT	show

Configuração de permit_show_commands no ISE

Configurar o perfil TACACS+

Um único perfil TACACS+ é configurado e a autorização de comando é realizada através de conjuntos de comandos.

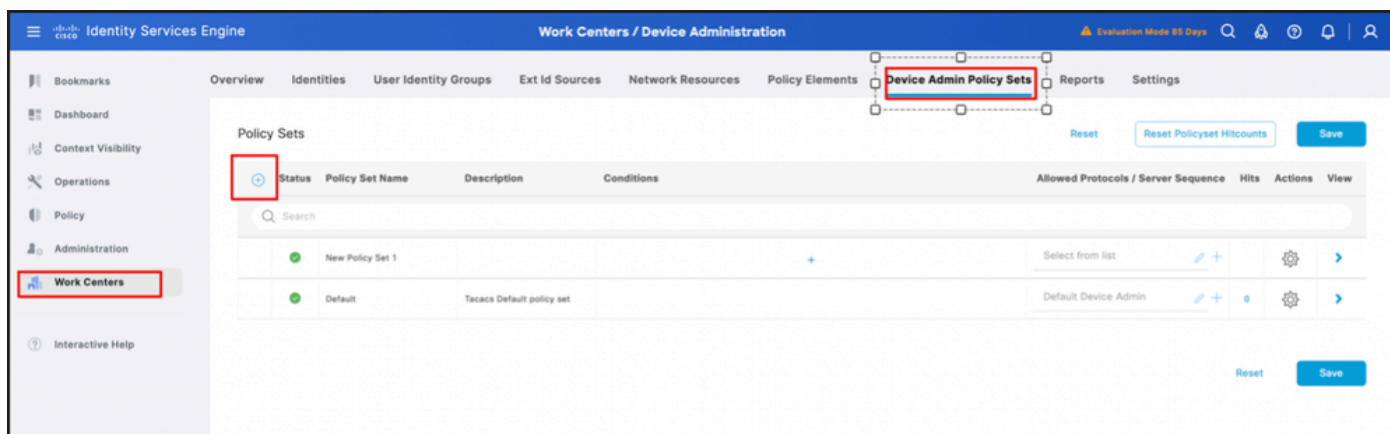
Para configurar um perfil TACACS+, navegue para Centros de trabalho > Administração de dispositivo > Resultados de política > Perfis TACACS. Clique em Add, forneça um nome para o Perfil Shell, marque a caixa de seleção Default Privilege e insira o valor 15. Finalmente, clique em Submit.



Configuração do perfil TACACS no ISE

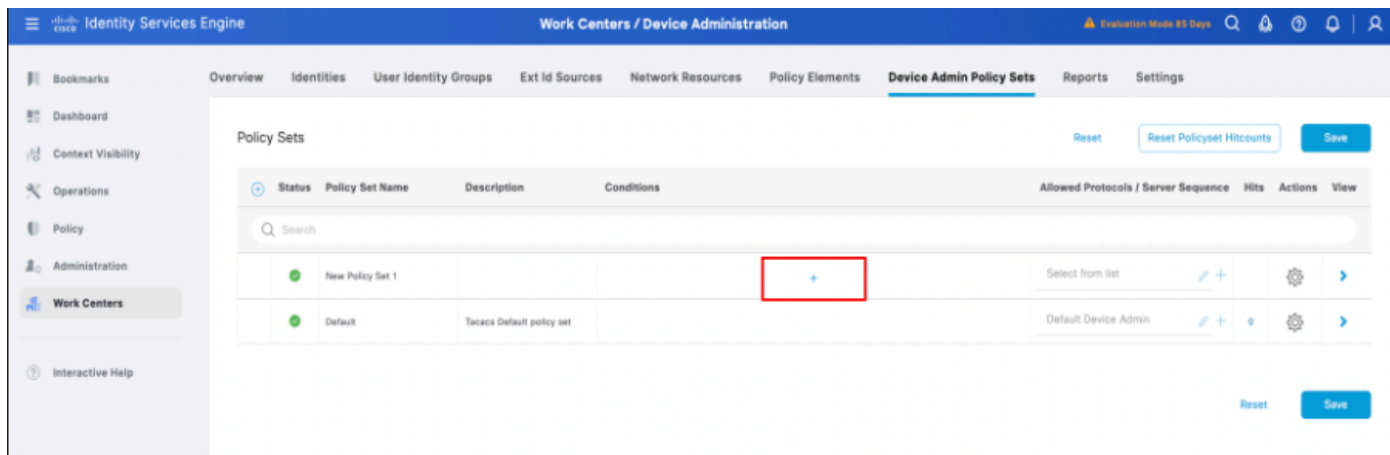
Configurar o perfil de autenticação e autorização TACACS+

1. Faça login na GUI do ISE PAN -> Administração -> Centros de trabalho -> Administração de dispositivos -> Conjuntos de políticas de administração de dispositivos. Clique no ícone + (sinal de adição) para criar uma nova regra. Nesse caso, o conjunto de políticas é nomeado como Novo conjunto de políticas 1.



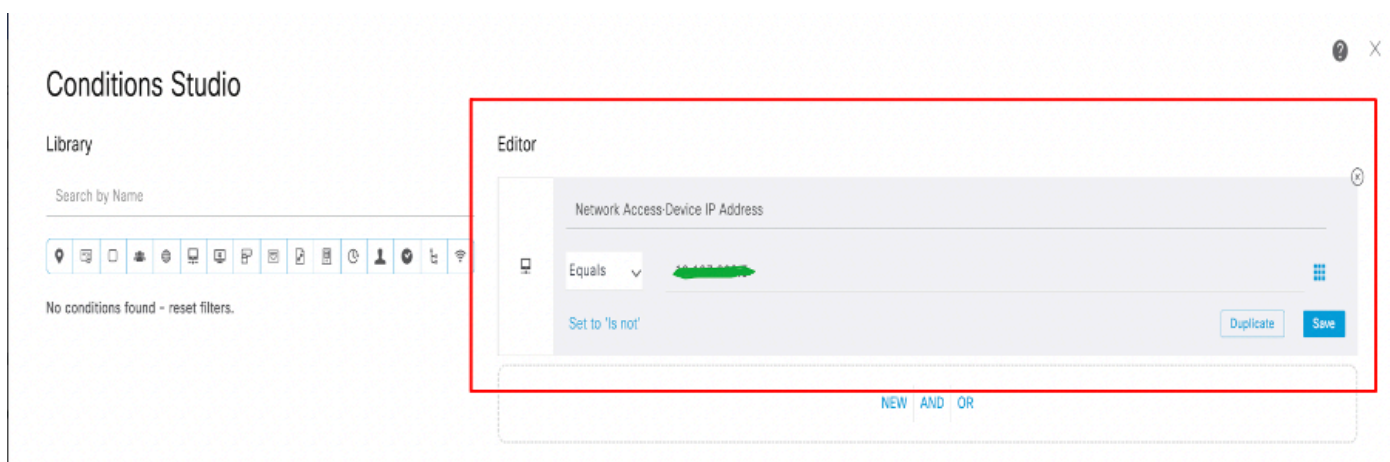
Configuração da política definida no ISE

2. Antes de salvar o conjunto de políticas, é necessário configurar as condições, como mostrado nesta captura de tela. Clique no ícone + (sinal de adição) para configurar as condições do conjunto de políticas.

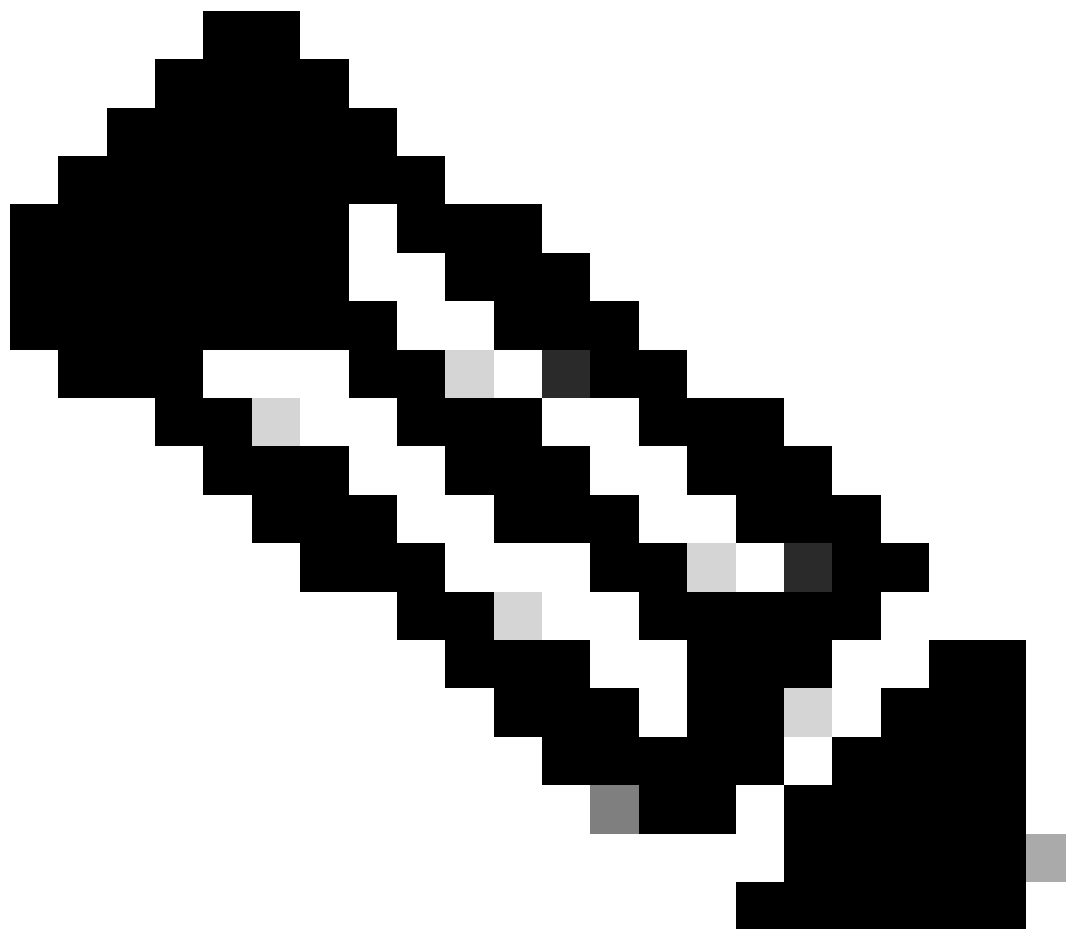


Configuração das condições do conjunto de políticas no ISE

3. Depois de clicar no ícone + (mais) como mencionado na etapa 2, a caixa de diálogo condições estúdio se abre. Aqui, configure as condições necessárias. Salve a condição com as condições novas ou existentes, role. Clique em use.

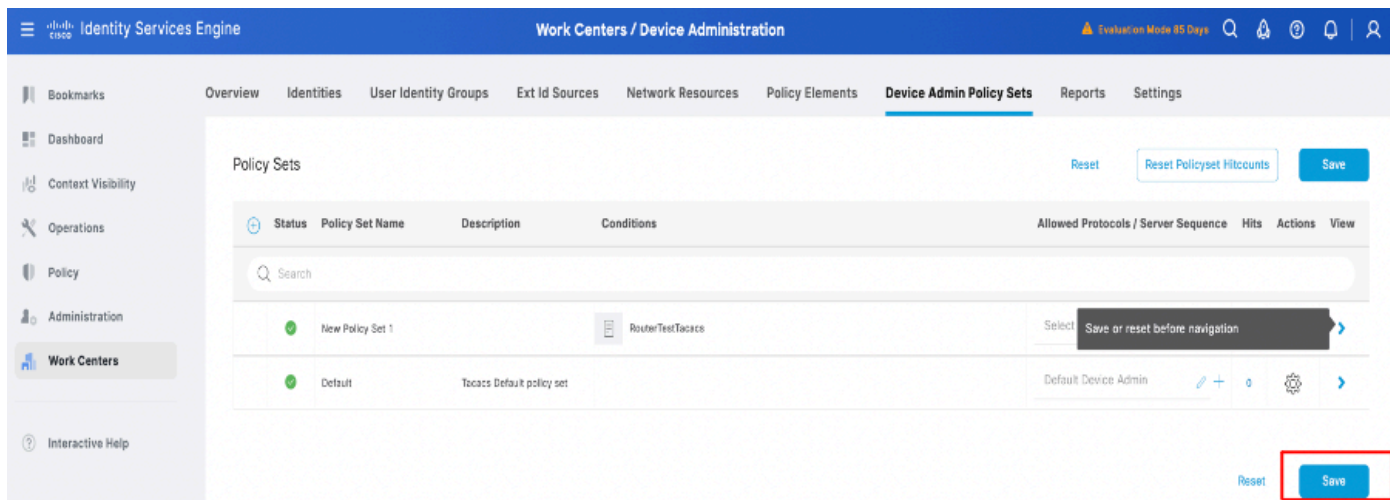


Configuração das condições do conjunto de políticas no ISE



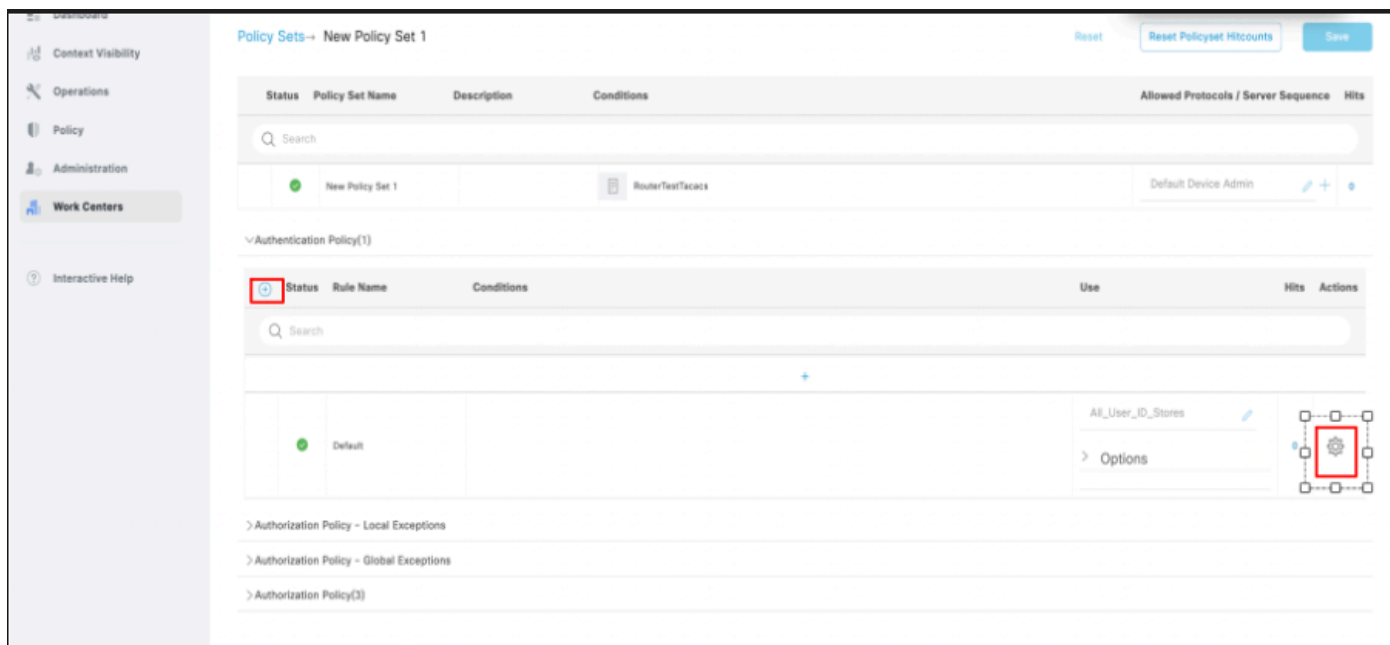
Note: Para esta documentação, as condições são combinadas com o IP do dispositivo de rede. No entanto, as condições podem variar de acordo com os requisitos de implantação.

4. Depois que as condições forem configuradas e salvas, configure os protocolos permitidos como Default device admin. Salve o conjunto de políticas criado clicando na opção Save .

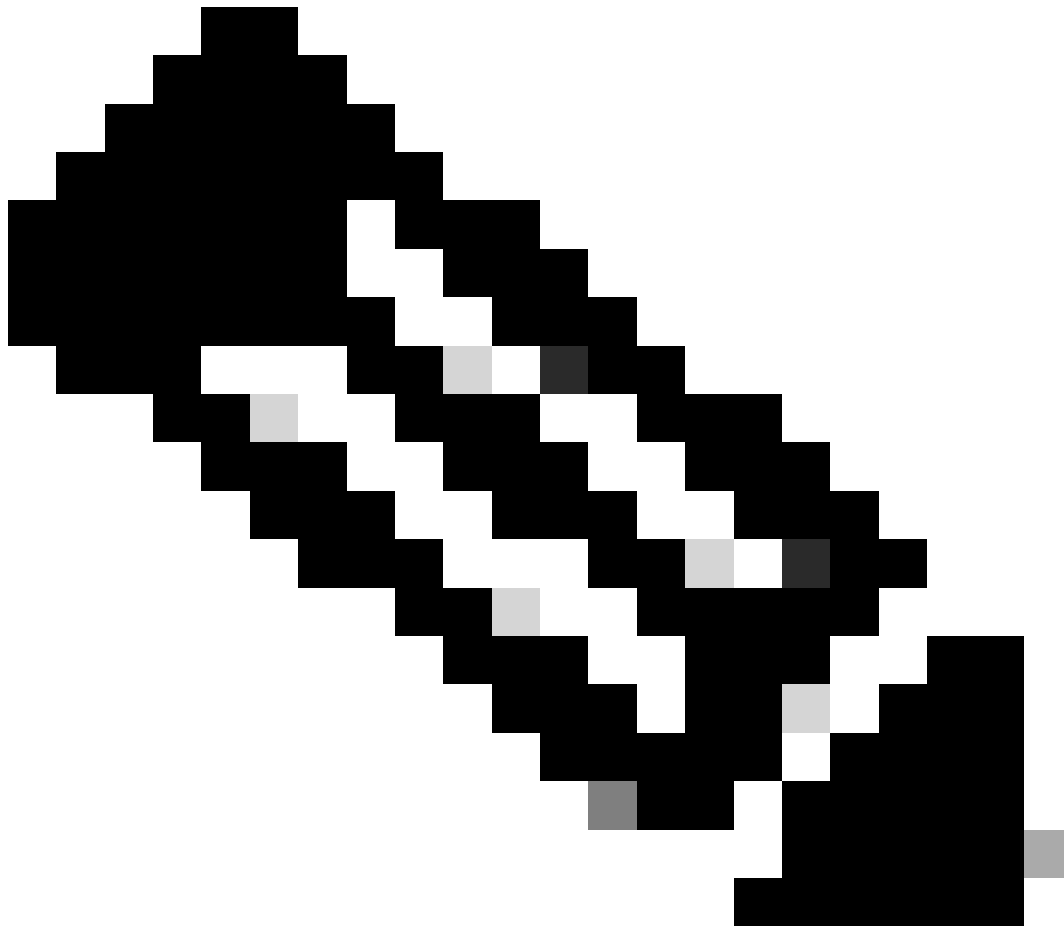


Confirmação da configuração do conjunto de políticas.

5. Expanda o Novo conjunto de políticas -> Política de autenticação (1) -> Crie uma nova política de autenticação clicando no ícone + (mais) ou clicando no ícone de engrenagem e Inserir nova linha acima.



Configuração da Política de Autenticação no conjunto de políticas.



Note: Para esta demonstração, a política de autenticação padrão definida com All_User_ID_Stores é usada. No entanto, o uso dos repositórios de Identidade é personalizável de acordo com os requisitos de implantação.

6. Expanda o Novo Conjunto de Políticas -> Política de Autorização (1). Clique no ícone + (sinal de adição) ou no ícone de engrenagem. Em seguida, insira a nova linha acima para criar uma política de autorização.

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

Status Policy Set Name Description Conditions Allowed Protocols / Server Sequence Hits

Search

New Policy Set 1 RouterTestTacacs Default Device Admin 0

> Authentication Policy(1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

> Authorization Policy(1)

Status Rule Name Conditions Results Command Sets Shell Profiles Hits Actions

Search

Default DenyAllCommands Deny All Shell Profile 0

Insert new row above

Reset Save

Configuração da Política de Autorização

7. Configure a Política de Autorização com condições, conjuntos de comandos e perfil de shell mapeados para as políticas de autorização.

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

Status Policy Set Name Description Conditions Allowed Protocols / Server Sequence Hits

Search

New Policy Set 1 RouterTestTacacs Default Device Admin 0

> Authentication Policy(1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

> Authorization Policy(3)

Status Rule Name Conditions Results Command Sets Shell Profiles Hits Actions

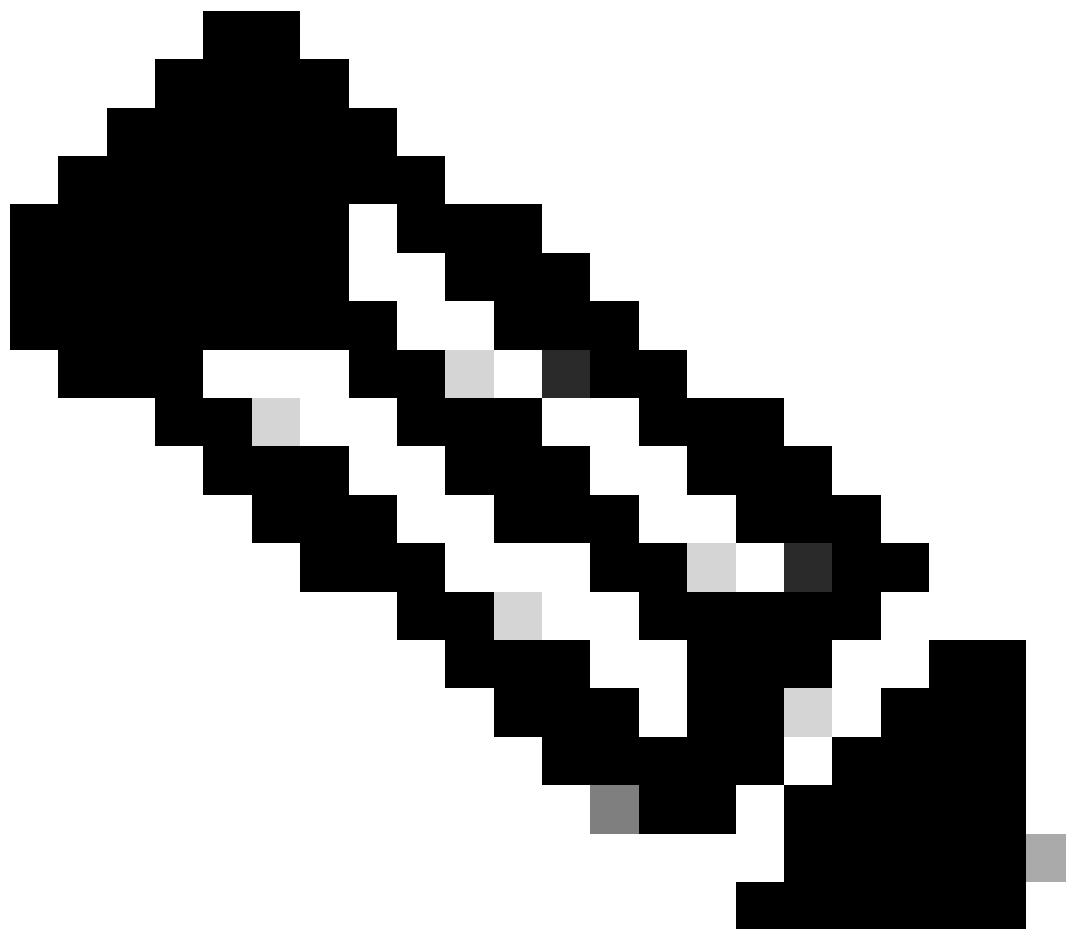
Search

Router_Auth RouterTestAuthz Permit_all_commands Shell_Profile 0

Router_Auth_Showcommand RouterTestAuthz permit_show_commands Shell_Profile 0

Default DenyAllCommands Deny All Shell Profile 0

Configuração completa da política de autorização no ISE

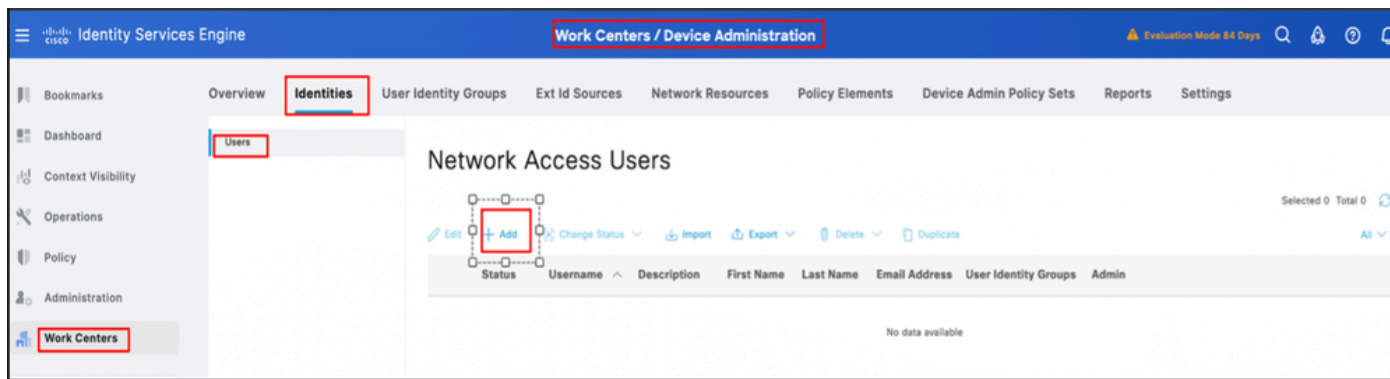


Note: As condições configuradas são de acordo com o ambiente de laboratório e podem ser configuradas de acordo com os requisitos de implantação.

8. Siga as 6 primeiras etapas para configurar os conjuntos de políticas para switch ou qualquer outro dispositivo de rede usado para TACACS+.

Configurar usuários de acesso à rede para autenticação TACACS de NAD no ISE

1. Navegue até Workcenters -> Device Administration -> Identities -> Users (Centros de trabalho -> Administração de dispositivos -> Identidades -> Usuários). Clique no ícone +(plus) para criar um novo usuário.



Configurar usuários de acesso à rede no ISE

2. Forneça para expandir os detalhes de Nome de usuário e Senha, mapeie o usuário para um Grupo de Identidade de Usuário (opcional) e clique em Enviar.

Network Access Users List > router

Network Access User

* Username: router

Status: Enabled

Account Name Alias:

Email:

Passwords

Password Type: Internal Users

Password Lifetime: With Expiration (60 days)

Never Expires

Password:

Re-Enter Password:

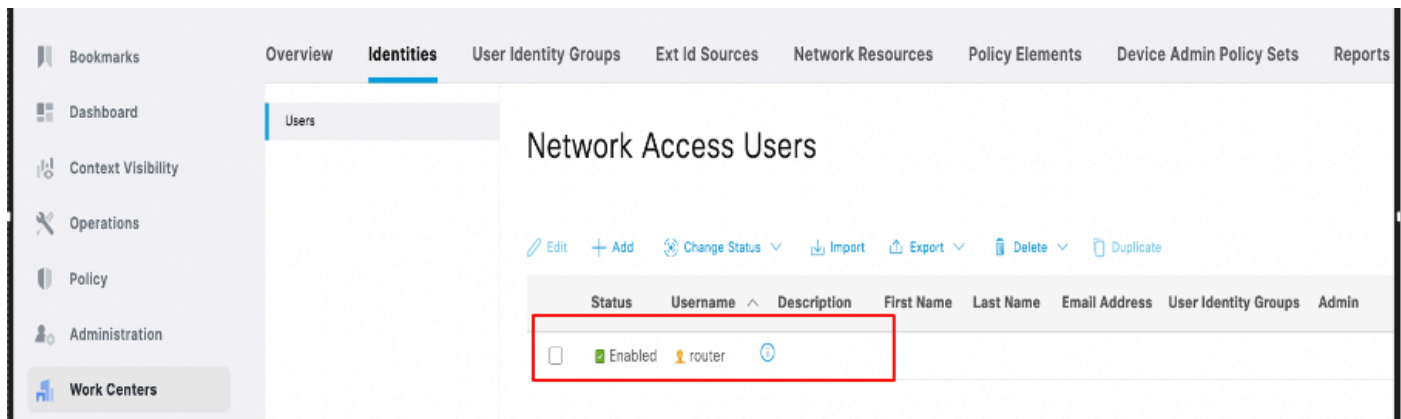
* Login Password:

Enable Password:

Generate Password

Configurar usuários de acesso à rede - Continuar

3. Depois de submeter a configuração de nome de usuário em Centros de Trabalho -> Identities -> Usuários -> Usuários de Acesso à Rede , o usuário é visivelmente configurado e ativado.



Confirmação da configuração do usuário de acesso à rede.

Configurar roteador para TACACS+

Configurar o Cisco IOS Router para Autenticação e Autorização TACACS+

1. Faça login na CLI do Roteador e execute esses comandos para configurar o TACACS no Roteador.

ASR1001-X(config)#aaa novo modelo — comando necessário para ativar aaa no NAD

ASR1001-X(config)#aaa id de sessão comum. —comando necessário para ativar aaa no NAD.

ASR1001-X(config)#aaa autenticação login padrão grupo tacacs+ local

ASR1001-X(config)#aaa authorization exec default group tacacs+

ASR1001-X(config)#aaa autorização lista de rede1 grupo tacacs+

ASR1001-X(config)#tacacs servidor ise1

ASR1001-X(config-server-tacacs)#address ipv4 <endereço IP do servidor TACACS > . —
Endereço IP da interface ISE G1.

ASR1001-X(config-server-tacacs)#key XXXXX

ASR1001-X(config)# aaa group server tacacs+ isegroup

ASR1001-X(config-sg-tacacs+)#server name ise1

ASR1001-X(config-sg-tacacs+)#ip vrf forwarding Mgmt-intf

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet0

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet1

ASR1001-X(config)#exit

2. Após salvar as configurações TACACS+ do roteador, verifique a configuração TACACS+

usando o comando show run aaa.

```
ASR1001-X#show run aaa
```

```
!
```

```
aaa authentication login default group isegroup local
```

```
aaa authorization exec default group isegroup
```

```
aaa authorization network list1 group isegroup
```

```
username admin password 0 XXXXXXXX
```

```
!
```

```
servidor tacacs ise1
```

```
address ipv4 <endereço IP do servidor TACACS>
```

```
chave XXXXX
```

```
!
```

```
!
```

```
aaa group server tacacs+ isegroup
```

```
nome do servidor ise1
```

```
ip vrf forwarding Mgmt-intf
```

```
ip tacacs source-interface GigabitEthernet1
```

```
!
```

```
!
```

```
!
```

```
aaa new-model
```

```
aaa session-id common
```

```
!
```

```
!
```

Configurar o switch para TACACS+

Configurar o switch para autenticação e autorização TACACS+

1. Faça login na CLI do switch e execute esses comandos para configurar o TACACS no switch.

```
C9200L-48P-4X#configure t
```

Enter configuration commands, one per line. Finalize with CNTL/Z.

```
C9200L-48P-4X(config)#aaa novo modelo. — comando necessário para ativar aaa no NAD
```

```
C9200L-48P-4X(config)#aaa session-id comum. — comando necessário para ativar aaa no NAD.
```

```
C9200L-48P-4X(config)#aaa autenticação logon padrão grupo isegroup local
```

```
Grupo isegroup padrão do C9200L-48P-4X(config)#aaa authorization exec
```

```
C9200L-48P-4X(config)#aaa autorização network list1 grupo isegroup
```

```
Servidor C9200L-48P-4X(config)#tacacs ise1
```

```
C9200L-48P-4X(config-server-tacacs)#address ipv4 <endereço IP do servidor TACACS> —  
Endereço IP da interface G1 do ISE.
```

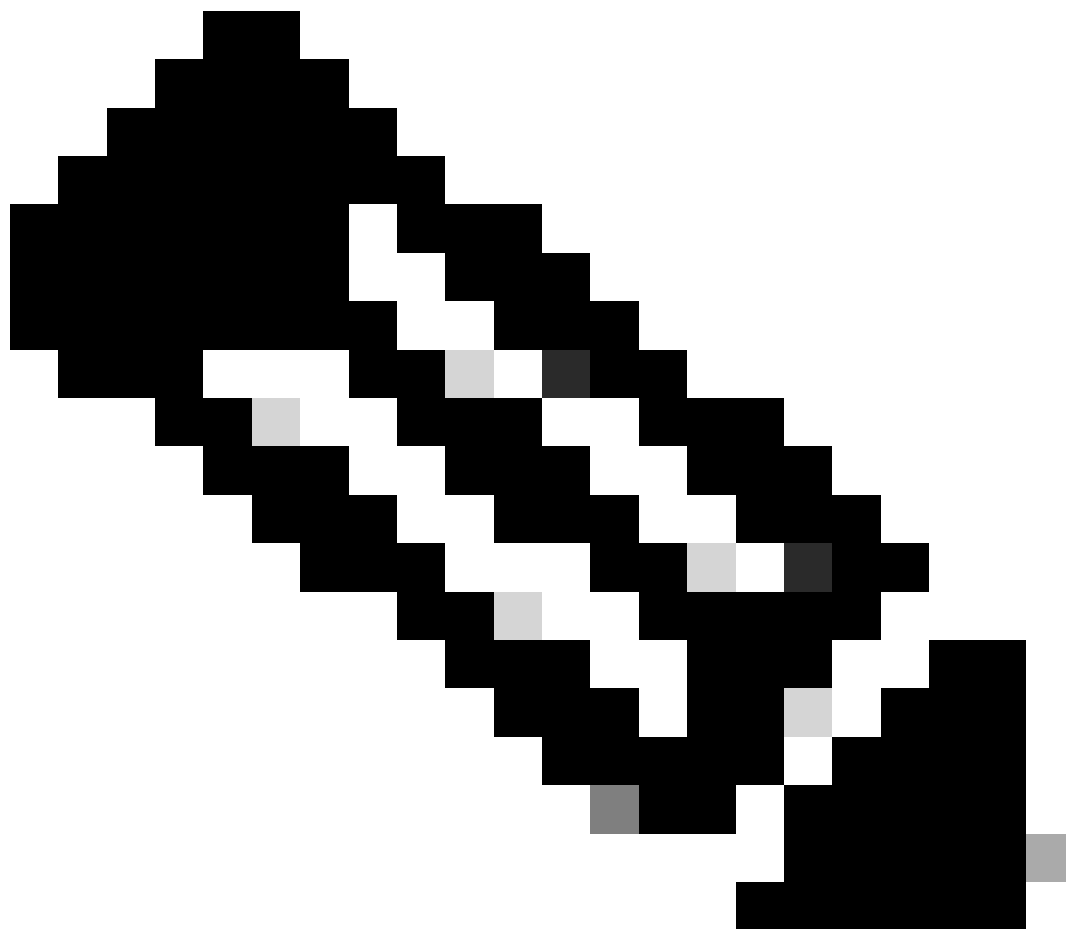
```
C9200L-48P-4X(config-server-tacacs)#key XXXXX
```

```
Servidor de grupo C9200L-48P-4X(config)#aaa tacacs+ isegroup
```

```
C9200L-48P-4X(config-sg-tacacs+)#server name ise1
```

```
C9200L-48P-4X(config)#exit
```

```
C9200L-48P-4X#wr mem
```



Note: Na configuração NAD TACACS+, tacacs+ é o grupo que pode ser personalizado de acordo com os requisitos de implantação.

2. Após salvar as configurações TACACS+ do switch, verifique a configuração TACACS+ usando o comando `show run aaa`.

```
C9200L-48P#show run aaa
```

```
!
```

```
aaa authentication login default group isegroup local
```

```
aaa authorization exec default group isegroup
```

```
aaa authorization network list1 group isegroup
```

```
username admin password 0 XXXXX
```

!

!

servidor tacacs ise1

address ipv4 <endereço IP do servidor TACACS>

chave XXXXX

!

!

aaa group server tacacs+ isegroup

nome do servidor ise1

!

!

!

aaa new-model

aaa session-id common

!

!

Verificação

Verificação do roteador

Na CLI do roteador, verifique a autenticação de TACACS+ contra ISE com interface Gigabit Ethernet 1 usando o comando `test aaa group tacacsgroupname username password new`.

Este é um exemplo de saída do Roteador & ISE:

Verificação da porta 49 do roteador:

ASR1001-X#telnet ISE Gig 1 interface IP 49

Tentando o IP da interface Glg 1 do ISE, 49... Abrir

ASR1001-X#test aaa group isegroup router XXXX novo

Enviando senha

Usuário autenticado com êxito

ATRIBUTOS DO USUÁRIO

username 0 "router"

reply-message 0 "Senha:"

Para a verificação do ISE, faça login na GUI -> Operations -> TACACS live logs e, em seguida, filtre com o IP do roteador no campo Network Device Details .

Overview

Request Type	Authentication
Status	Pass
Session Key	honey/530520237/15
Message Text	Passed-Authentication: Authentication succeeded
Username	router
Authentication Policy	New Policy Set 1 >> Default
Selected Authorization Profile	Shell_Profile

Authentication Details

Generated Time	2025-03-06 05:52:51.374000 +00:00
Logged Time	2025-03-06 05:52:51.374
Epoch Time (sec)	1741240371
ISE Node	honey
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	router
Network Device Name	RouterTest
Network Device IP	
Network Device Groups	IPSEC#Is IPSEC Device#No_Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	

Steps

13013

Received TACACS+ Authentication START Request

15049

Evaluating Policy Group (Step latency=2ms)

15008

Evaluating Service Selection Policy (Step latency=0ms)

15048

Queried PIP - Network Access.Device IP Address (Step latency=4ms)

15041

Evaluating Identity Policy (Step latency=14ms)

22072

Selected identity source sequence - All_User_ID_Stores (Step latency=6ms)

15013

Selected Identity Source - Internal Users (Step latency=1ms)

24210

Looking up User in Internal Users IDStore (Step latency=0ms)

24212

Found User in Internal Users IDStore (Step latency=80ms)

13045

TACACS+ will use the password prompt from global TACACS+ configuration (Step latency=1ms)

13015

Returned TACACS+ Authentication Reply (Step latency=0ms)

13014

Received TACACS+ Authentication CONTINUE Request (Step latency=3ms)

15041

Evaluating Identity Policy (Step latency=3ms)

22072

Selected identity source sequence - All_User_ID_Stores (Step latency=6ms)

15013

Selected Identity Source - Internal Users (Step latency=1ms)

24210

Looking up User in Internal Users IDStore (Step latency=0ms)

24212

Found User in Internal Users IDStore (Step latency=11ms)

22037

Authentication Passed (Step latency=1ms)

15036

Evaluating Authorization Policy (Step latency=2ms)

13015

Returned TACACS+ Authentication Reply (Step latency=11ms)

Registros ao vivo TACACS do ISE - Verificação do roteador.

Verificação do Switch

Na CLI do switch, verifique a autenticação do TACACS+ em relação ao ISE com a interface Gigabit Ethernet 1 usando o comando test aaa group tacacsgruppname username password newn:

Aqui está um exemplo de saída do switch e do ISE.

Verificação da porta 49 do switch:

C9200L-48P# telnet ISE Gig1 interface IP 49

Tentando o IP da interface ISE Gig1, 49... Abrir

C9200L-48P#test aaa group isegroup switch XXXX new

Enviando senha

Usuário autenticado com êxito

ATRIBUTOS DO USUÁRIO

username 0 "switch"

reply-message 0 "Senha:"

Para a verificação do ISE, faça login na GUI -> Operations -> TACACS live logs e, em seguida, filtre com o switch IP no campo Network Device Details .

The screenshot displays the Cisco ISE GUI with the 'Overview' and 'Authentication Details' sections on the left and a 'Steps' log on the right. Red boxes highlight specific fields in the Overview and Authentication Details sections.

Overview

Request Type	Authentication
Status	Pass
Session Key	honey/530520237/11
Message Text	Passed-Authentication: Authentication succeeded
Username	switch
Authentication Policy	New Policy Set 2 >> Default
Selected Authorization Profile	Shell_Profile

Authentication Details

Generated Time	2025-03-06 04:10:15.551000 +00:00
Logged Time	2025-03-06 04:10:15.551
Epoch Time (sec)	1741234215
ISE Node	honey
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	switch
Network Device Name	Switch
Network Device IP	[REDACTED]
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	

Steps

- 13013 Received TACACS+ Authentication START Request
- 15049 Evaluating Policy Group (Step latency=8ms)
- 15008 Evaluating Service Selection Policy (Step latency=0ms)
- 15048 Queried PIP - Network Access.Device IP Address (Step latency=11ms)
- 15041 Evaluating Identity Policy (Step latency=9ms)
- 22072 Selected identity source sequence - All_User_ID_Stores (Step latency=17ms)
- 15013 Selected Identity Source - Internal Users (Step latency=1ms)
- 24210 Looking up User in Internal Users IDStore (Step latency=1ms)
- 24212 Found User in Internal Users IDStore (Step latency=69ms)
- 13045 TACACS+ will use the password prompt from global TACACS+ configuration (Step latency=0ms)
- 13015 Returned TACACS+ Authentication Reply (Step latency=1ms)
- 13014 Received TACACS+ Authentication CONTINUE Request (Step latency=7ms)
- 15041 Evaluating Identity Policy (Step latency=6ms)
- 22072 Selected identity source sequence - All_User_ID_Stores (Step latency=22ms)
- 15013 Selected Identity Source - Internal Users (Step latency=1ms)
- 24210 Looking up User in Internal Users IDStore (Step latency=36ms)
- 24212 Found User in Internal Users IDStore (Step latency=16ms)
- 22037 Authentication Passed (Step latency=0ms)
- 15036 Evaluating Authorization Policy (Step latency=1ms)
- 13015 Returned TACACS+ Authentication Reply (Step latency=36ms)

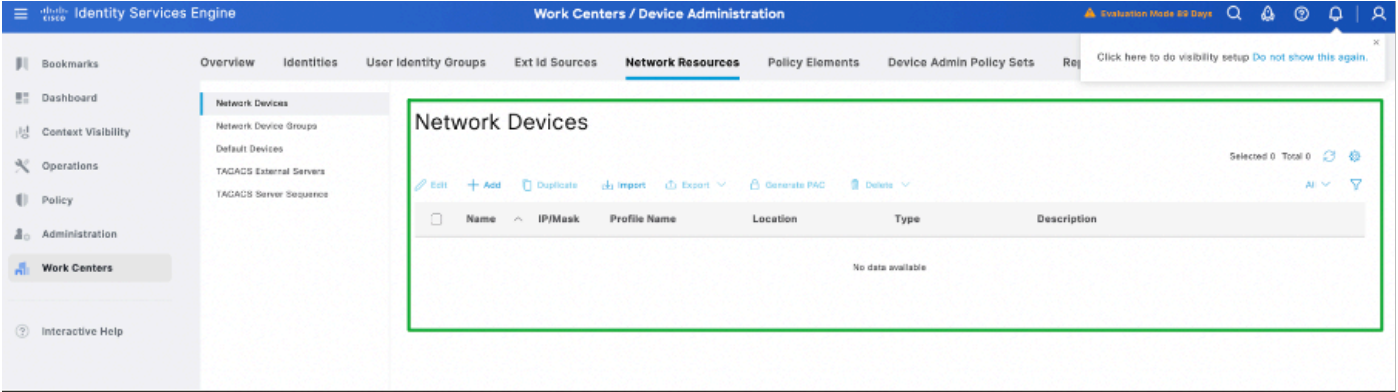
Registros ao vivo TACACS do ISE - Verificação de switch.

Troubleshooting

Esta seção discute alguns dos problemas comuns encontrados relacionados às autenticações TACACS+.

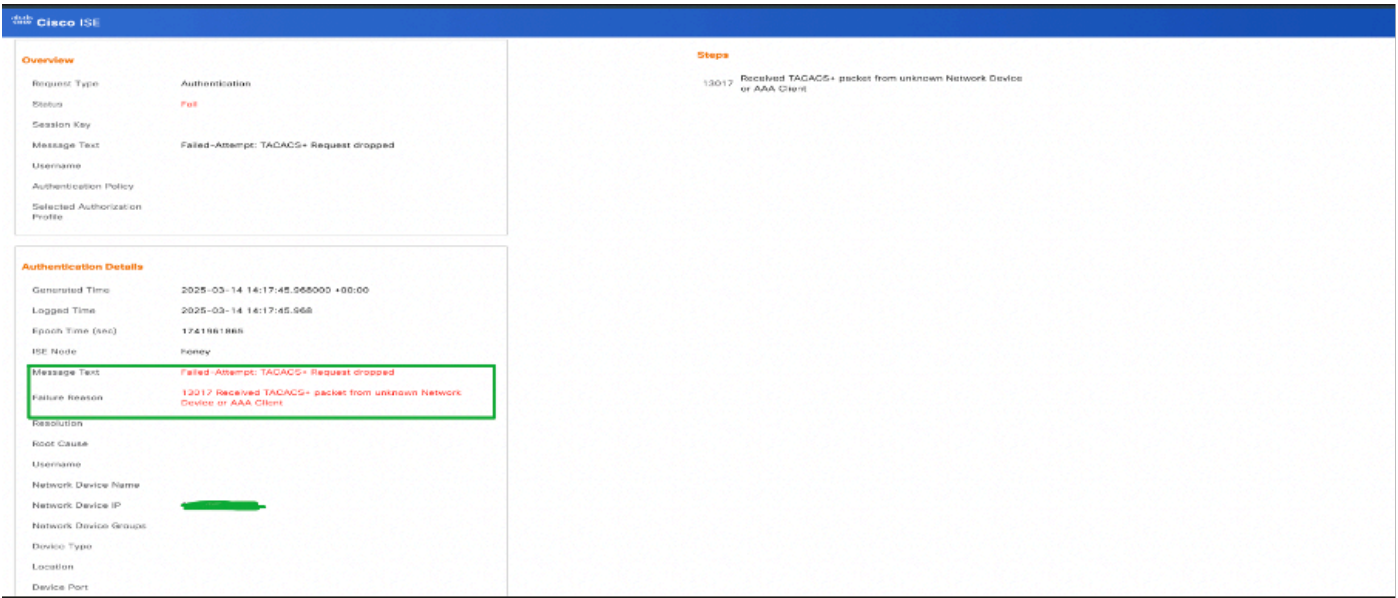
Cenário 1: A autenticação TACACS+ falha com "Erro: 13017 pacote TACACS+ recebido de dispositivo de rede desconhecido ou cliente AAA".

Esse cenário ocorre quando o dispositivo de rede não é adicionado como recursos de rede no ISE. Como mostrado nesta captura de tela, o switch não é adicionado aos recursos de rede do ISE.



Cenário de solução de problemas - Os dispositivos de rede não são adicionados ao ISE.

Agora, quando você testa a autenticação do switch/dispositivo de rede, o pacote alcança o ISE como esperado. No entanto, a autenticação falha com o erro "Erro : 13017 pacote TACACS+ recebido de dispositivo de rede desconhecido ou cliente AAA" como mostrado nesta captura de tela:



Registros em tempo real TACACS - falha quando o dispositivo de rede não é adicionado ao ISE.

Verificação do Dispositivo de Rede (Switch)

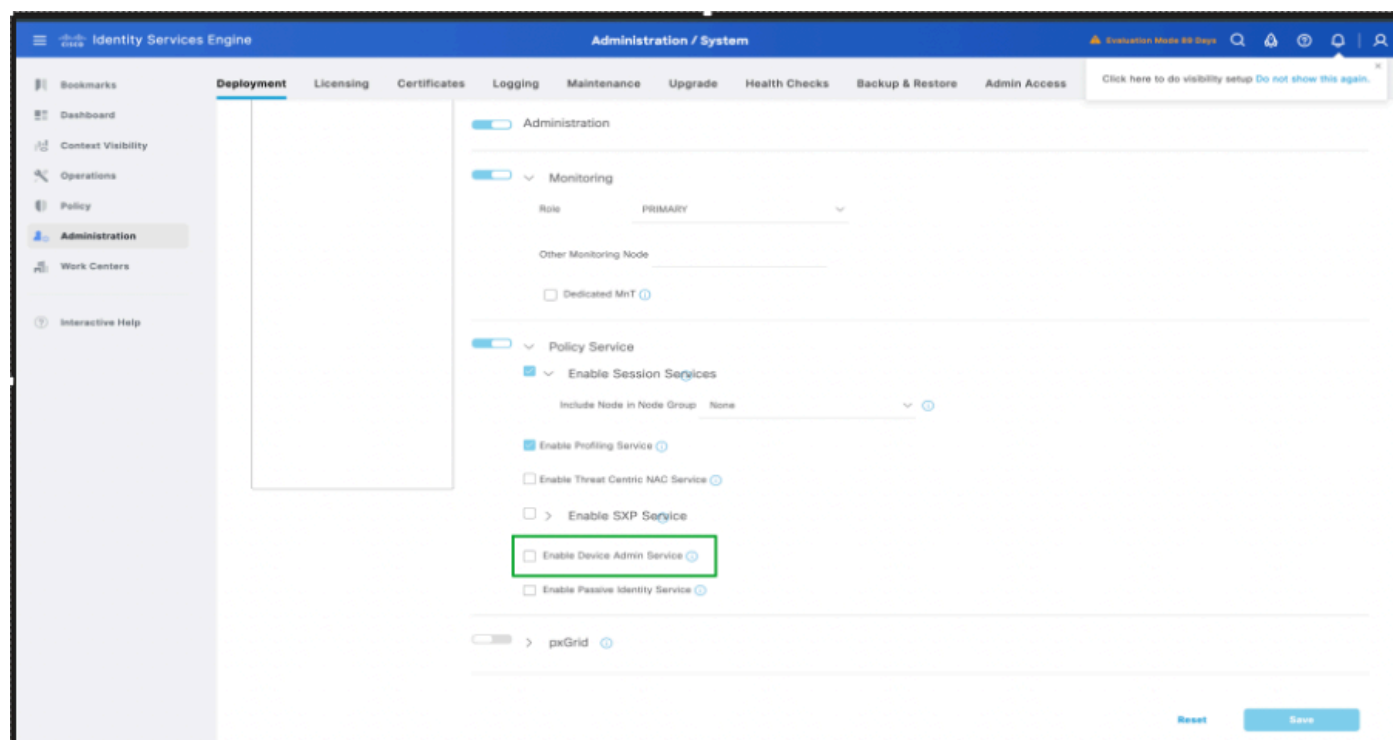
Switch#test aaa group isegroup switch XXXXXX novo
Usuário rejeitado

Solução: Verifique se o switch / Roteador / Dispositivo de rede foi adicionado como o Dispositivo de rede no ISE. Se o dispositivo não for adicionado, adicione-o à lista de dispositivos de rede do ISE.

Cenário 2: O ISE descarta o pacote TACACS+ silenciosamente sem nenhuma informação.

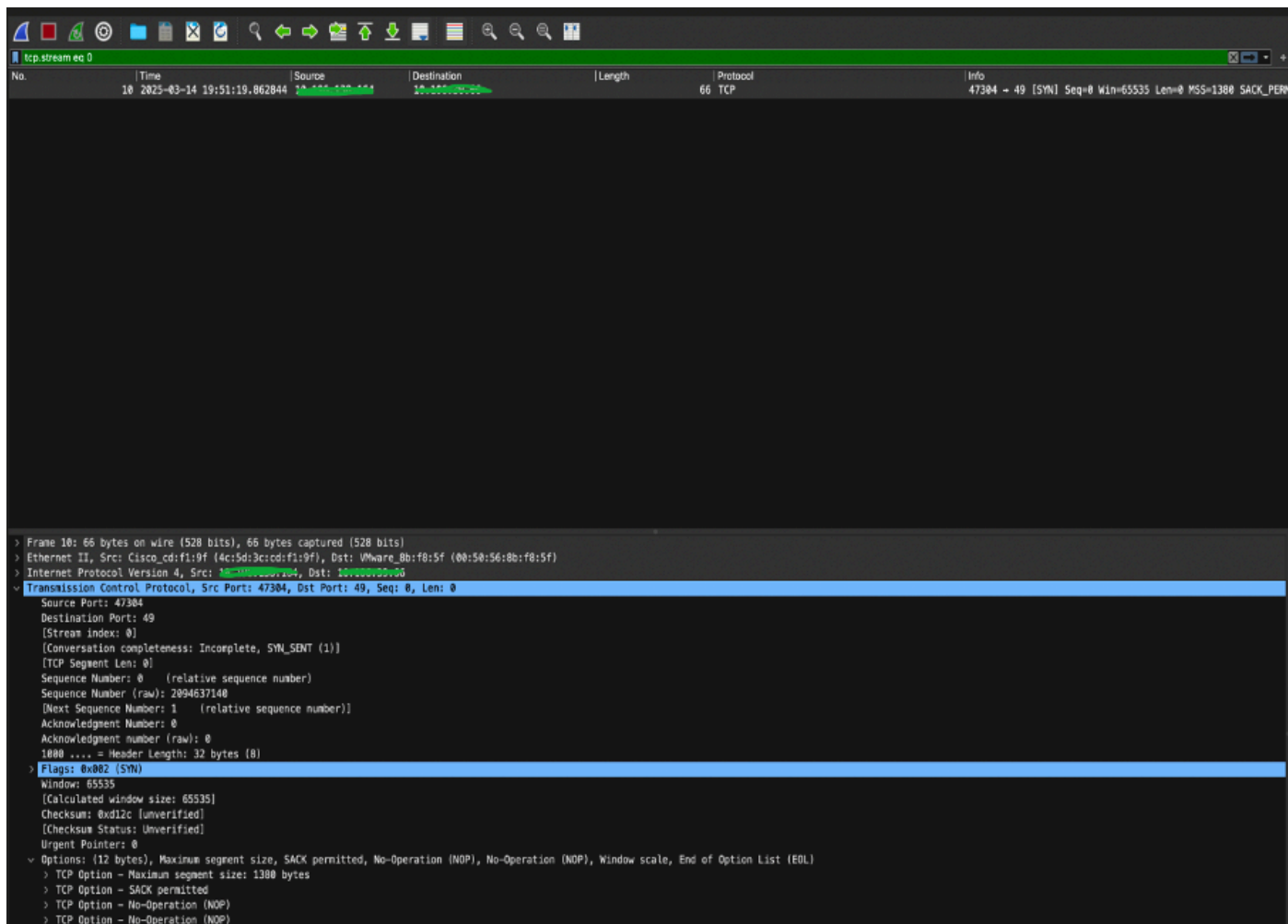
Este cenário ocorre quando o Device Administration Service está desabilitado no ISE. Neste cenário, o ISE descarta o pacote e nenhum registro ativo é visto, mesmo que a autenticação esteja sendo iniciada do dispositivo de rede que é adicionado aos recursos de rede do ISE.

Como mostrado nesta captura de tela, a Administração de dispositivos está desabilitada no ISE.



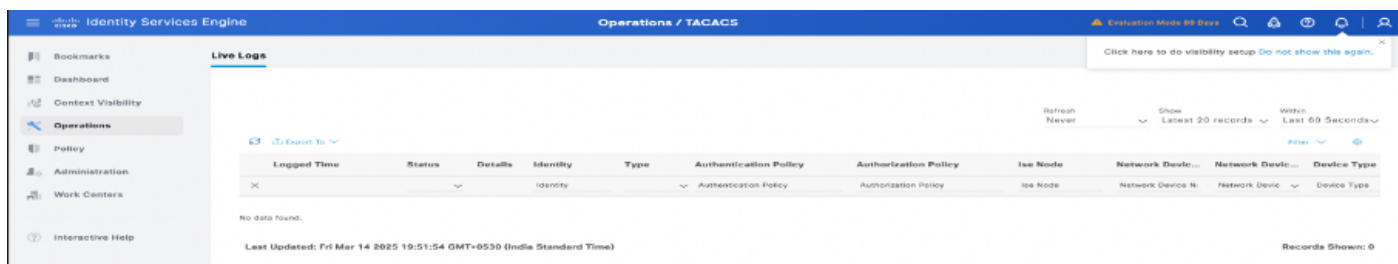
Cenário, a administração do dispositivo não está habilitada no ISE.

Quando um usuário inicia a autenticação a partir do dispositivo de rede, o ISE silenciosamente descarta os pacotes sem nenhuma informação nos registros em tempo real e o ISE não responde ao pacote Syn enviado pelo dispositivo de rede para concluir o processo de autenticação TACACS. Consulte esta captura de tela:



ISE descartando pacotes silenciosamente durante TACACS

O ISE não mostra nenhum registro ativo durante a autenticação.



Nenhum registro TACACS ativo - Verificação do ISE

Verificação do Dispositivo de Rede (Switch)

Switch#

Switch#test aaa group isegroup switch XXXX novo

Usuário rejeitado

Switch#

*14 de mar 13:54:28.144: T+: Versão 192 (0xC0), tipo 1, seq 1, criptografia 1, SC 0

*14 de mar 13:54:28.144: T+: session_id 10158877 (0x9B031D), dlen 14 (0xE)

*14 de mar 13:54:28.144: T+: texto:AUTHTEN/START, priv_lvl:15 ação:LOGIN ascii

*14 de mar 13:54:28.144: T+: svc:LOGIN user_len:6 port_len:0 (0x0) raddr_len:0 (0x0) data_len:0

*14 de mar 13:54:28.144: T+: usuário: switch

*14 de mar 13:54:28.144: T+: porta:

*14 de mar 13:54:28.144: T+: rem_addr:

*14 de mar 13:54:28.144: T+: dados:

*14 de mar 13:54:28.144: T+: Encerrar pacote

Solução: Habilite a administração de dispositivos no ISE.

Referência

- [Solucionar problemas de autenticação TACACS](#)
- [Guia do Administrador do Cisco Identity Services Engine, Versão 3.3](#)
- [VRF para servidores TACACS](#)

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.