

Configurar a autenticação TACACS+ no switch Arista com ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração TACACS+ no ISE](#)

[Configurar o switch Arista](#)

[Etapa 1. Ativar a autenticação TACACS+](#)

[Etapa 2. Salvar a configuração](#)

[Verificar](#)

[Revisão do ISE](#)

[Troubleshooting](#)

[Problema 1](#)

[Possíveis causas](#)

[Problema 2](#)

[Possíveis causas](#)

[Solução](#)

Introdução

Este documento descreve como integrar o Cisco ISE TACACS+ com um switch Arista para AAA centralizado de acesso de administrador.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo Cisco ISE e TACACS+.
- Switches Arista

Componentes Utilizados

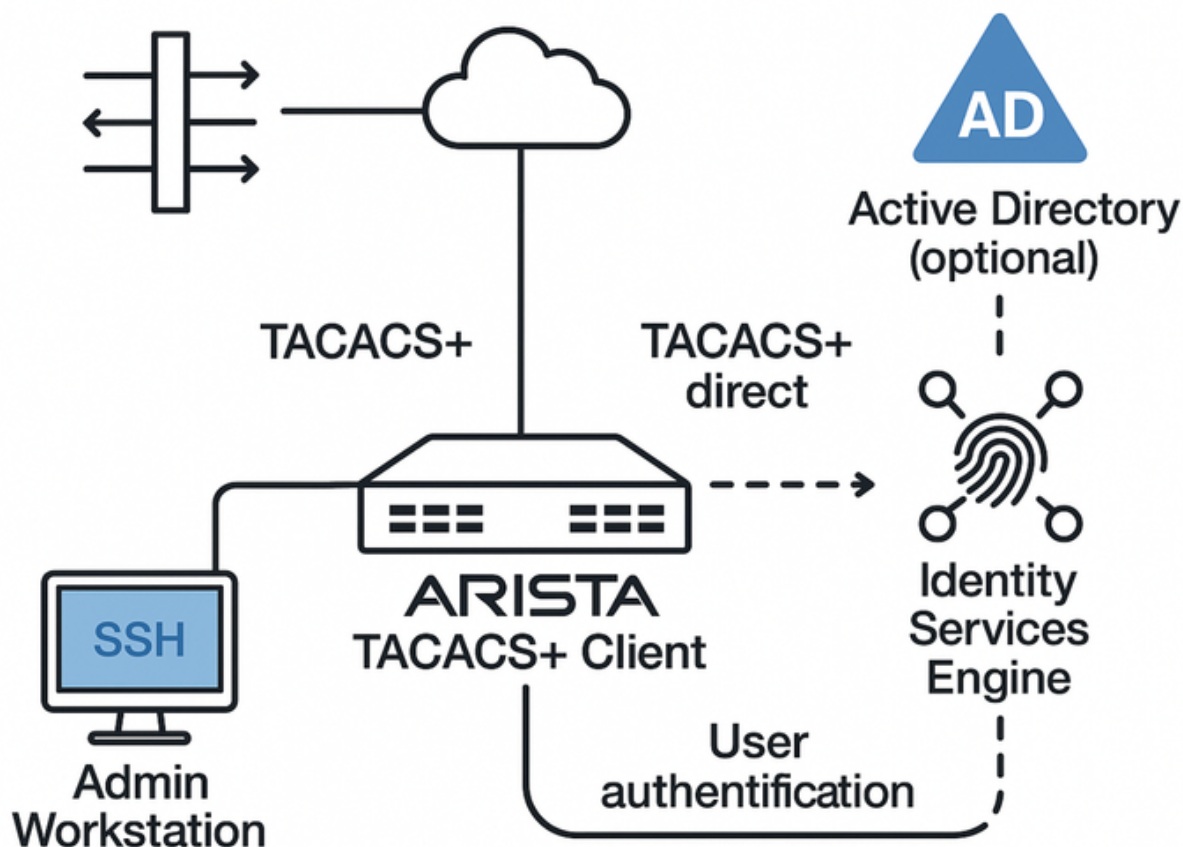
As informações neste documento são baseadas nestas versões de software e hardware:

- Versão da imagem do software do switch Arista: 4,33,2F
- 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

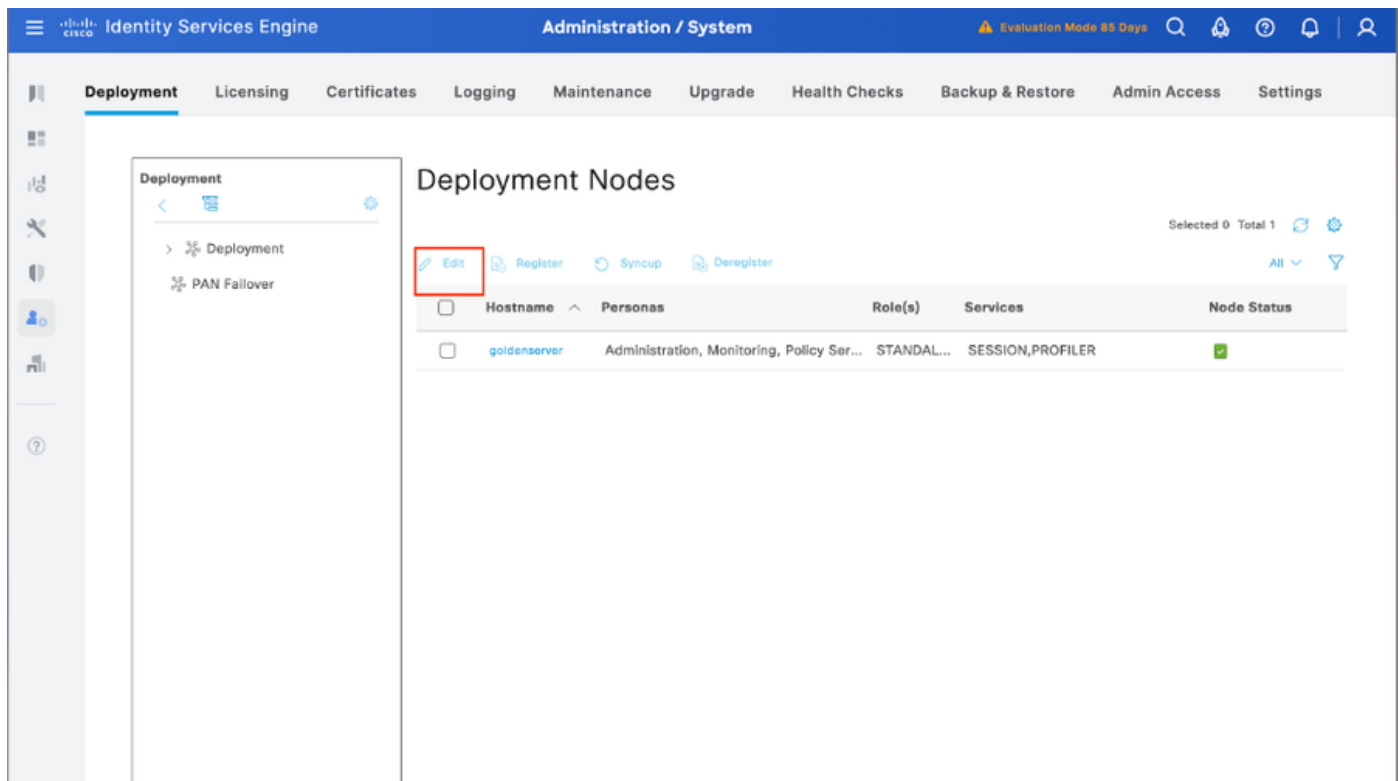


Configurações

Configuração TACACS+ no ISE

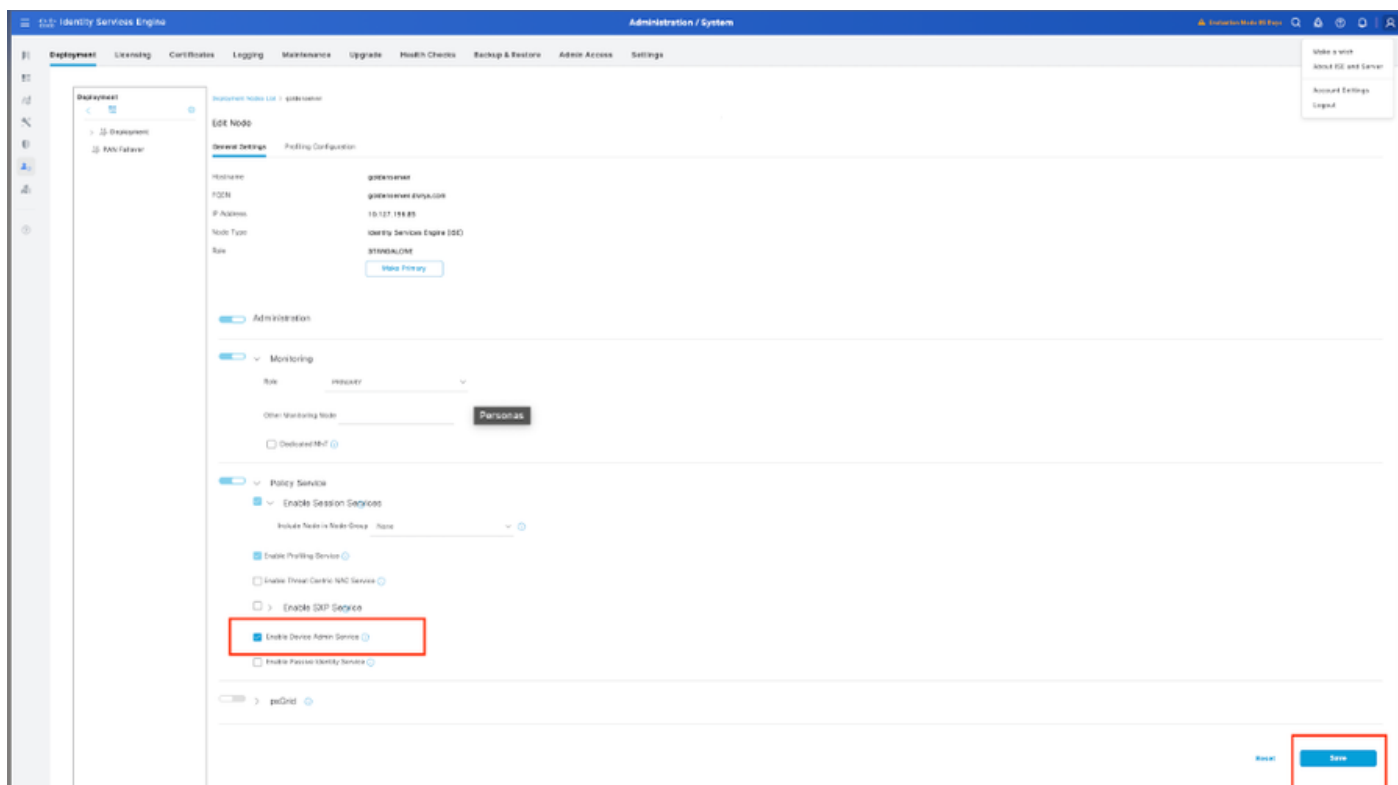
Etapa 1. A etapa inicial é verificar se o Cisco ISE tem os recursos necessários para lidar com a autenticação TACACS+. Para fazer isso, confirme se o Policy Service Node (PSN) desejado tem o recurso Device Admin Service habilitado.

Navegue até **Administration > System > Deployment**, selecione o nó apropriado onde o ISE processa a autenticação TACACS+ e clique em **Edit** 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.

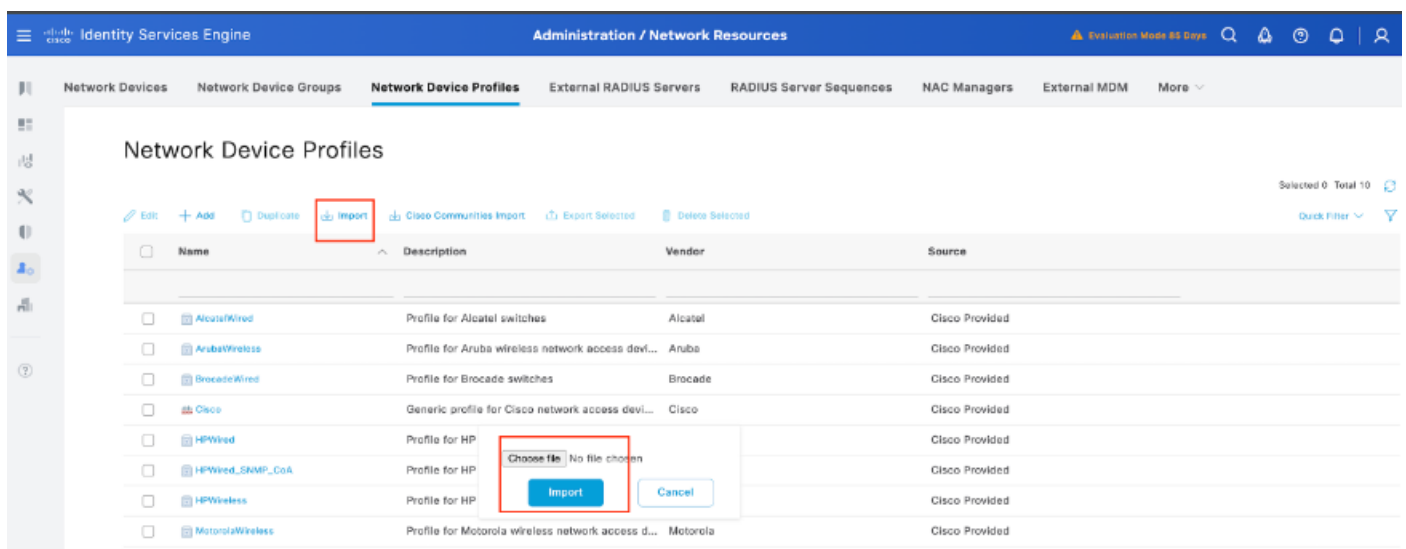


Etapa 3. Obter o perfil do dispositivo de rede Arista para o Cisco ISE.

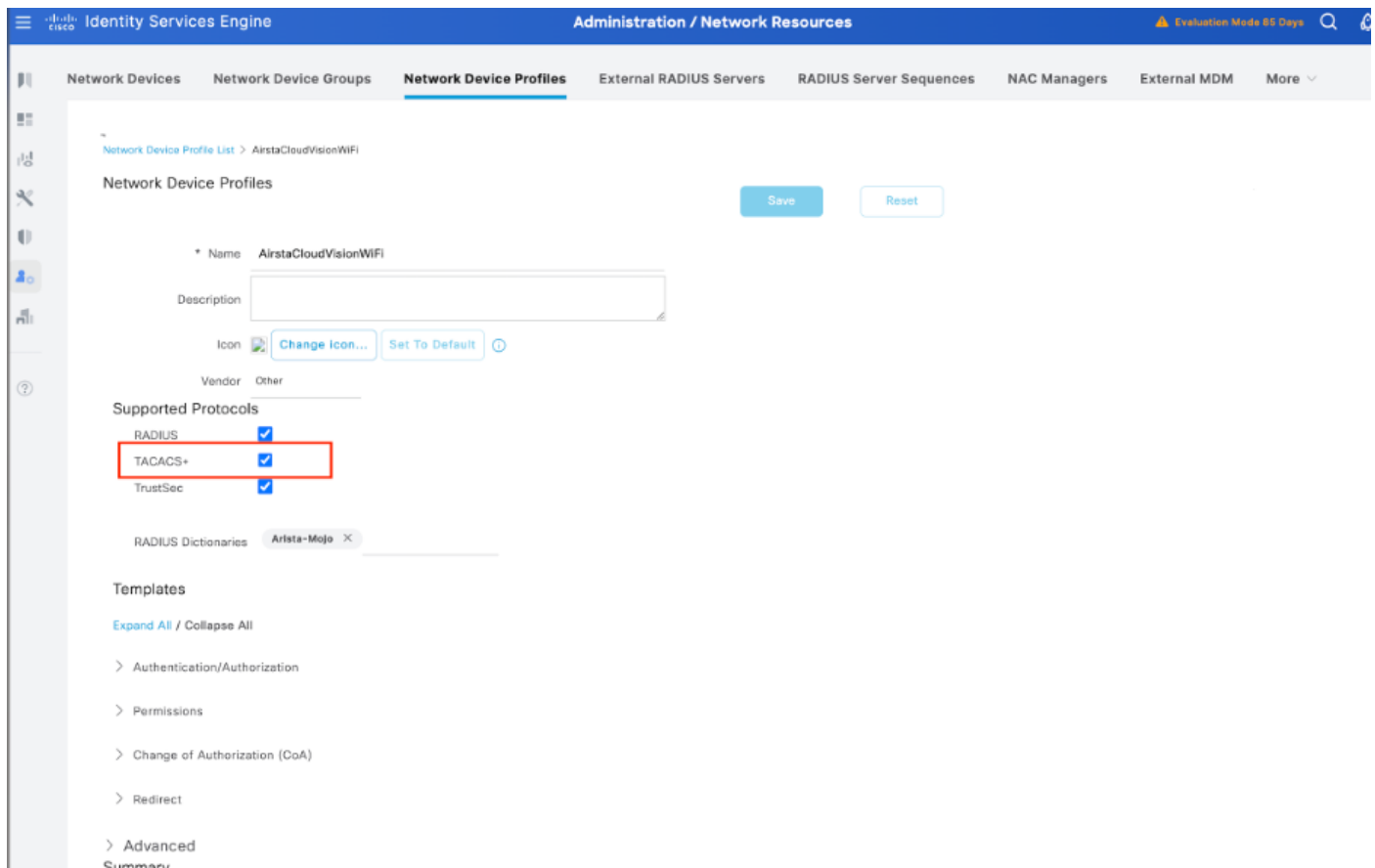
A Comunidade Cisco compartilhou um perfil NAD dedicado para dispositivos Arista. Esse perfil, juntamente com os arquivos de dicionário necessários, pode ser encontrado no artigo [Arista CloudVision WiFi Dictionary e NAD Profile for ISE Integration](#). O download e a importação desse perfil para a configuração do ISE facilita uma integração mais tranquila

Etapas para importar o perfil Arista NAD para o Cisco ISE:

1. Faça o download do perfil:
 - Obtenha o perfil Arista NAD no link da Comunidade Cisco fornecido acima.
[Comunidade Cisco](#)
2. Acesse o Cisco ISE:
 - Faça login no console administrativo do Cisco ISE
3. Importar o perfil NAD:
 - Navegue até Administration > Network Resources > Network Device Profiles.
 - Clique no botão Importar
 - Carregue o arquivo de perfil Arista NAD baixado.

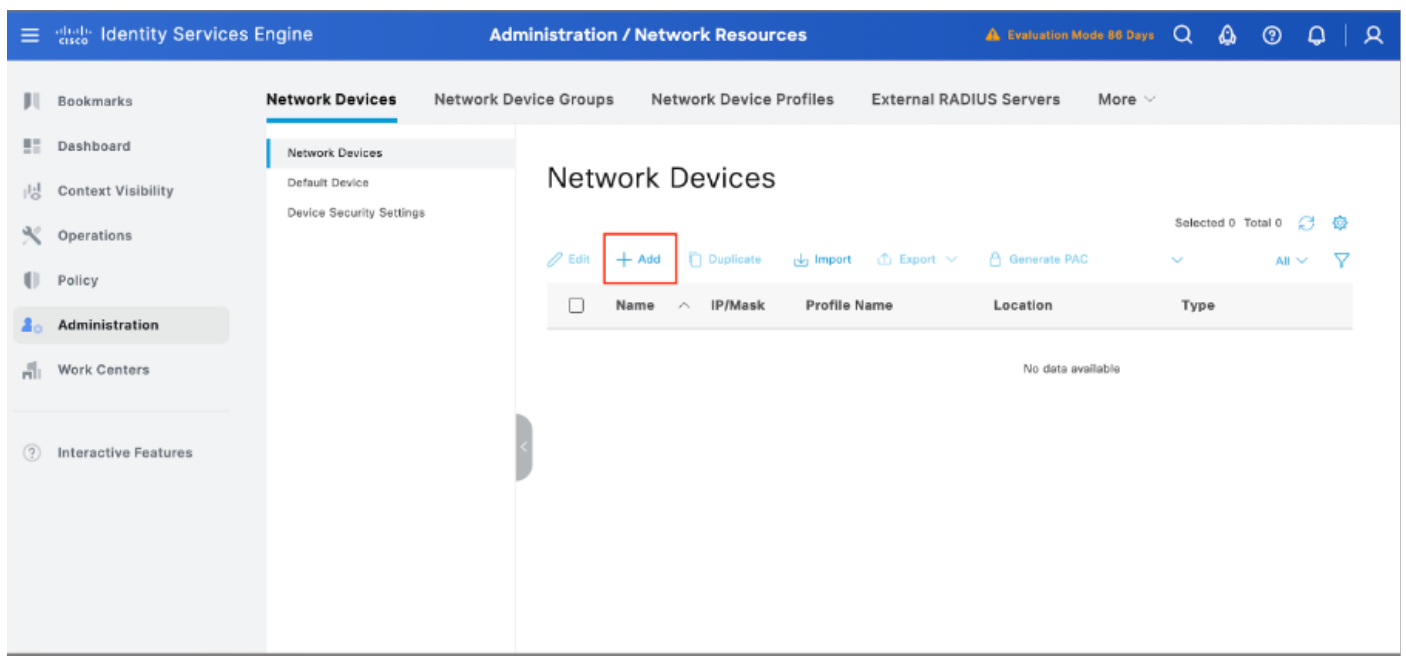


Após a conclusão do upload, navegue para a opção Edit e ative o TACACS+ como um protocolo suportado.



Passo 2: Adicione o switch Arista como um dispositivo de rede.

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



2.Clique em Adicionar e insira estes detalhes:

- Endereço IP: <Switch-IP>
- tipo de dispositivo: Escolha outro com fio
- Perfil do dispositivo de rede: selecione AristaCloudVisionWiFi.

- Configurações de autenticação RADIUS:
 - Ative a autenticação RADIUS.
 - Insira o Shared Secret (deve corresponder à configuração do switch).

3. Clique em Salvar:

The screenshot shows the 'Administration / Network Resources' page in the Cisco ISE console. The 'Network Devices' tab is selected. The configuration for 'Arista_switch' is displayed. The 'Name' field is highlighted with a red box. Below it, the 'Description' is 'Arista_switch for device login TACACS and'. The 'IP Address' is set to '32'. The 'Device Profile' is 'AristaCloudVisionWiFi'. The 'Model Name' and 'Software Version' are both set to '4-33-2F'. The 'Network Device Group' is 'All Locations'. The 'Location' is 'All Locations'. The 'IPSEC' is 'No'. The 'Device Type' is 'All Device Types'. The 'RADIUS Authentication Settings' section is expanded, and the 'Protocol' is set to 'RADIUS'. The 'Shared Secret' field is highlighted with a red box. The 'Use Second Shared Secret' checkbox is unchecked.

Etapa 3. Validar o novo dispositivo é mostrado em Dispositivos de rede:

The screenshot shows the 'Network Devices' list in the Cisco ISE console. The table below is a representation of the data shown in the screenshot. The 'Arista_switch' device is highlighted with a red box.

Name	IP/Mask	Profile Name	Location	Type	Description
Arista_switch	32	AristaCloudVisionWiFi	All Locations	All Device Types	Arista_switch f

Etapa 4. Configurar o perfil TACACS.

Crie um perfil TACACS, navegue até o menu Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Perfis TACACS e selecione Adicionar:

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 'TACACS Profiles' and displays a table of existing profiles. A red box highlights the 'Add' button in the top left corner of the table.

Name	Type	Description
Arista Profile Admin	Shell	
Default Shell Profile	Shell	Default Shell Profile
Deny All Shell Profile	Shell	Deny All Shell Profile
TAC_PROFILE_PRIV15	Shell	
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR

Insira um Nome, marque a caixa de seleção Privilégio Padrão e defina o valor como 15. Além disso, selecione Privilégio Máximo, defina seu valor como 15 e clique em Enviar:

The screenshot shows the configuration page for the 'TAC_PROFILE_PRIV15' TACACS Profile. The 'Name' field is filled with 'TAC_PROFILE_PRIV15'. The 'Description' field is empty. The 'Task Attribute View' tab is selected, showing a list of common tasks. A red box highlights the 'Default Privilege' and 'Maximum Privilege' fields, both set to 15.

Common Task Type	Value	Unit
Default Privilege	15	(Select 0 to 15)
Maximum Privilege	15	(Select 0 to 15)
Access Control List		
Auto Command		
No Escape		(Select true or false)
Timeout	60	Minutes (0-9999)
Idle Time	15	Minutes (0-9999)

Etapa 5. Crie um Device Admin Policy Set a ser usado para seu Arista Switch, navegue para o menu Work Centers > Device Administration > Device Admin Policy Sets, em seguida, de um conjunto de políticas existente selecione o ícone de engrenagem para, em seguida, selecione Insert new row above.

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

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Arista Switch Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	27		
+	Default	Tacacs Default policy set		Default Device Admin			

Insert new row above
Insert new row below
Duplicate above
Duplicate below
Delete

Save

Etapa 6. Nomeie este novo Conjunto de políticas, adicione condições dependendo das características das autenticações TACACS+ que estão em andamento no switch Arista e selecione Allowed Protocols > Default Device Admin, salve sua configuração.

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

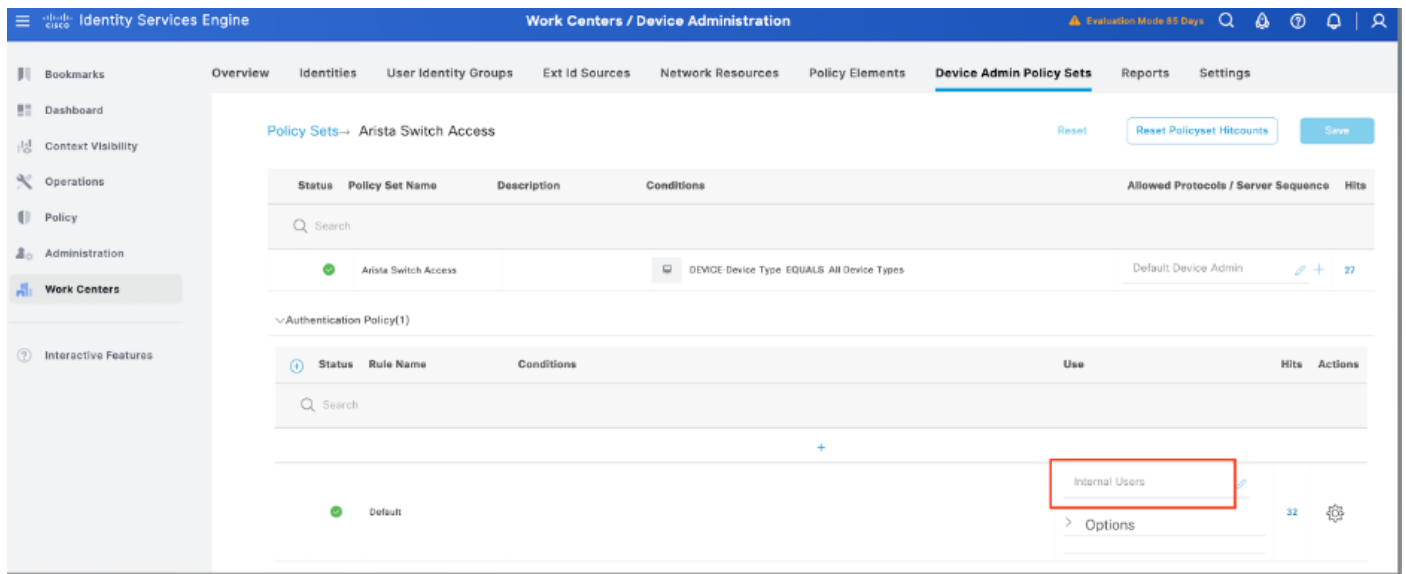
Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Arista Switch Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	27		
+	Default	Tacacs Default policy set					

Allowed Protocols
Default Device Admin
Default Network Access

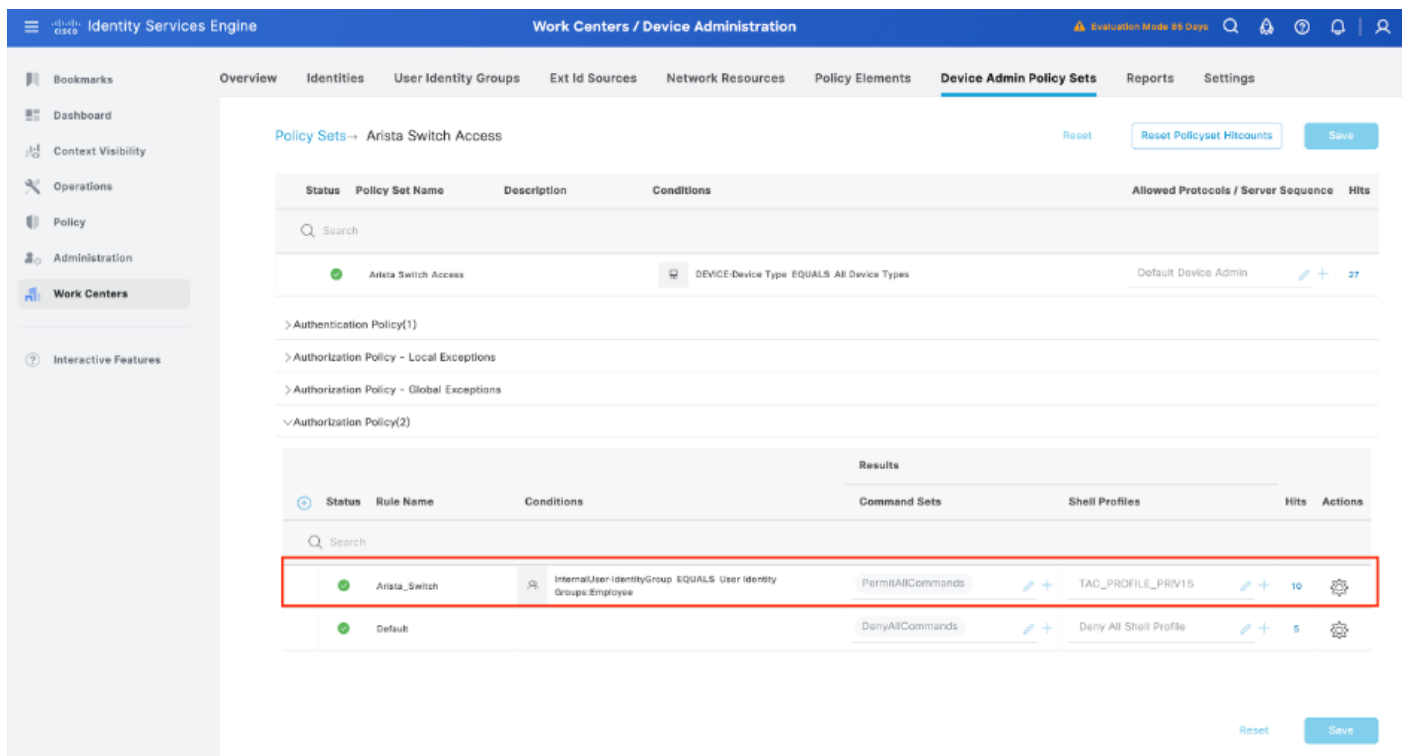
Save

Etapa 7. Selecione na opção > view e, em seguida, na seção Authentication Policy, selecione a fonte de identidade externa que o Cisco ISE usa para consultar o nome de usuário e as credenciais para autenticação no switch Arista. Neste exemplo, as credenciais correspondem a Usuários internos armazenados no ISE.



Etapa 8. Role para baixo até a seção chamada Authorization Policy to Default policy, selecione o ícone de engrenagem e insira uma regra acima.

Etapa 9. Nomeie a nova Regra de Autorização, adicione condições referentes ao usuário que já está autenticado como membro do grupo e, na seção Perfis de shell adicione o perfil TACACS que você configurou anteriormente, salve a configuração.



Configurar o switch Arista

Etapa 1. Ativar a autenticação TACACS+

Faça login no switch Arista e entre no modo de configuração:

configurar

```
!  
tacacs-server host <ISE-IP> key <TACACS-SECRET>  
  
!  
aaa group server tacacs+ ISE_TACACS  
    server <ISE-IP>  
  
!  
aaa authentication login default group ISE_TACACS local  
aaa authorization exec default group ISE_TACACS local  
aaa accounting commands 15 default start-stop group ISE_TACACS  
  
!
```

Fim

Etapa 2. Salvar a configuração

Para persistir a configuração nas reinicializações:

```
# write memory  
  
OU  
  
# copy running-config startup-config
```

Verificar

Revisão do ISE

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

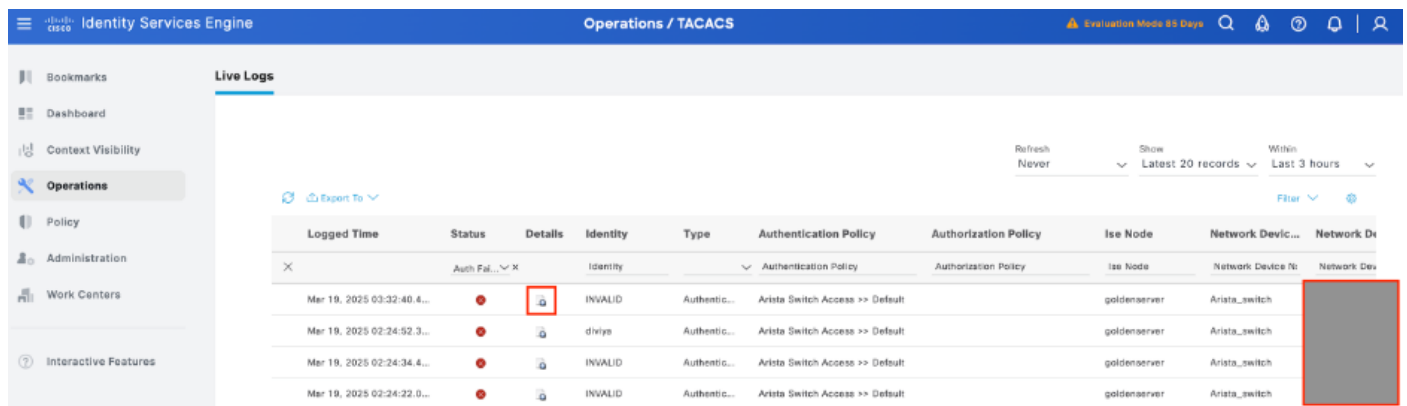
- GUI: Verifique se você tem o nó listado com o serviço DEVICE ADMIN em > Sistema > Implantação.
- CLI: Execute o comando `show ports | include 49` para confirmar que há conexões na porta TCP que pertencem ao TACACS+

```
goldenserver/admin#show ports | include 49
```

```
tcp: 
```

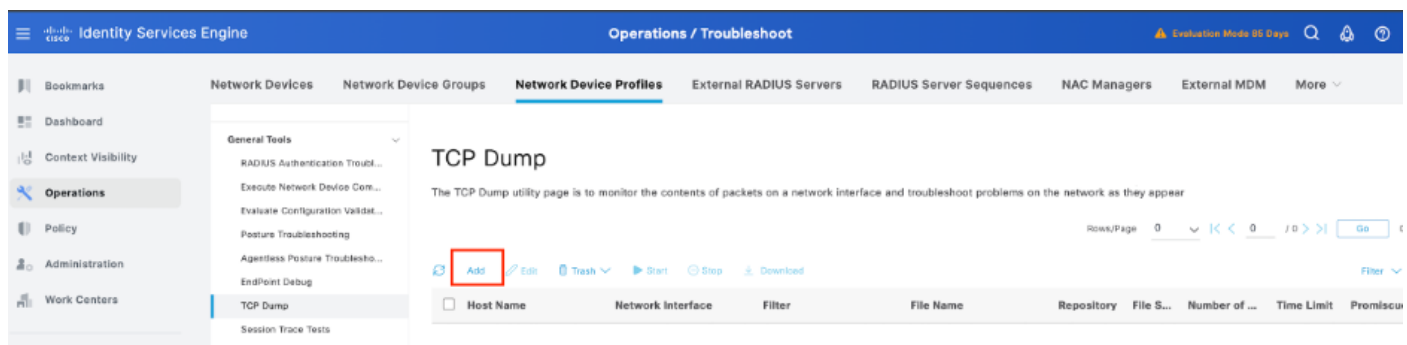
Etapa 2. Confirme se há registros em tempo real referentes a tentativas de autenticação

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	Isr Node	Network Device...	Network De
Mar 19, 2025 03:32:40.4...	Auth Fail...	X	INVALID	Authentic...	Arista Switch Access >> Default	Authorization Policy	goldenserver	Arista_switch	Network Dev
Mar 19, 2025 02:24:52.3...			diviya	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	
Mar 19, 2025 02:24:34.4...			INVALID	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	
Mar 19, 2025 02:24:22.0...			INVALID	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	

Etapa 3. Caso você não veja nenhum LiveLog, continue para capturar um pacote. Navegue até o menu Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump , selecione Add:



General Tools

- RADIUS Authentication Troub...
- Execute Network Device Com...
- Evaluate Configuration Validat...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- Endpoint Debug
- TCP Dump
- Session Trace Tests

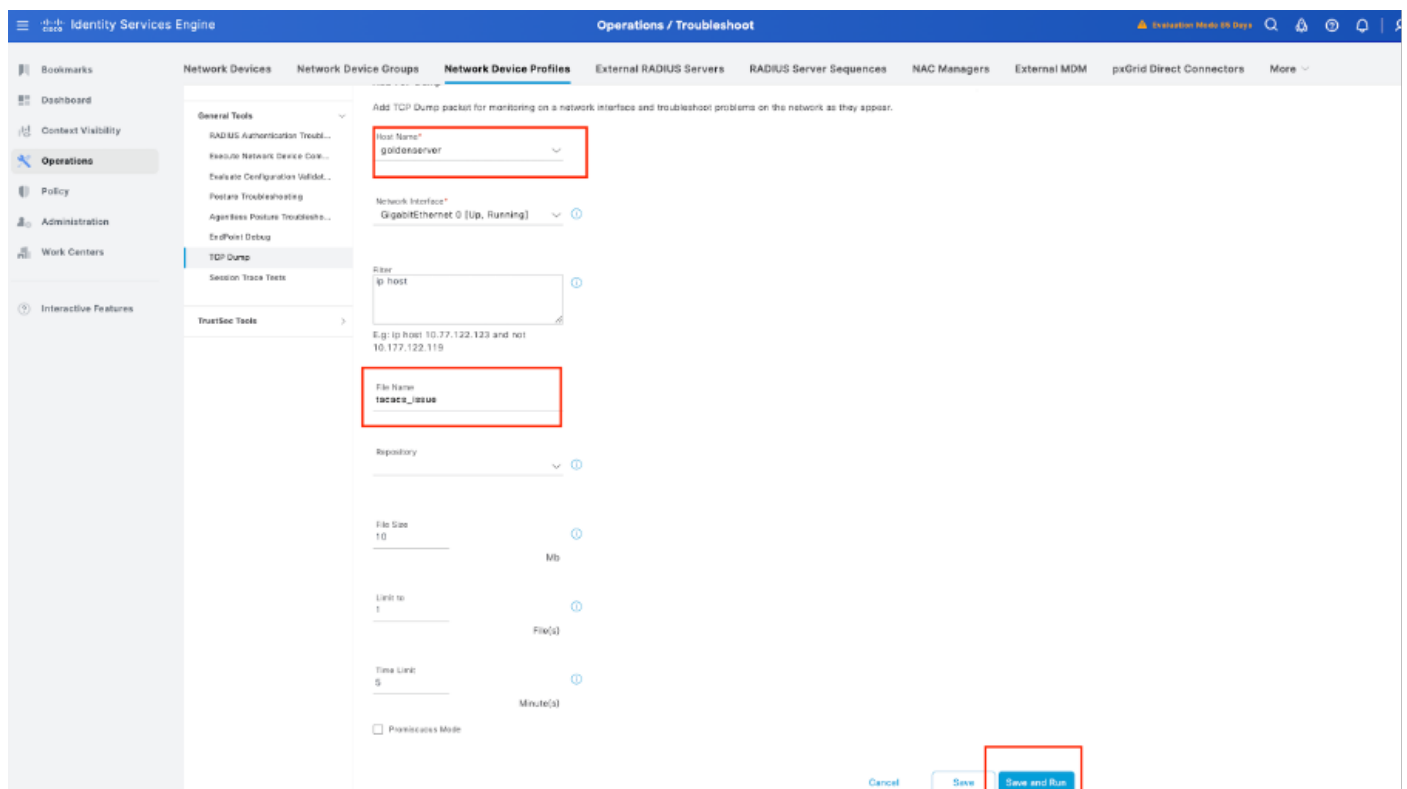
TCP Dump

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 >> Go

Add Edit Trash Start Stop Download

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



General Tools

- RADIUS Authentication Troub...
- Execute Network Device Com...
- Evaluate Configuration Validat...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- Endpoint Debug
- TCP Dump
- Session Trace Tests

TCP Dump

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 tacacs_issue

Repository

File Size 10 Mb

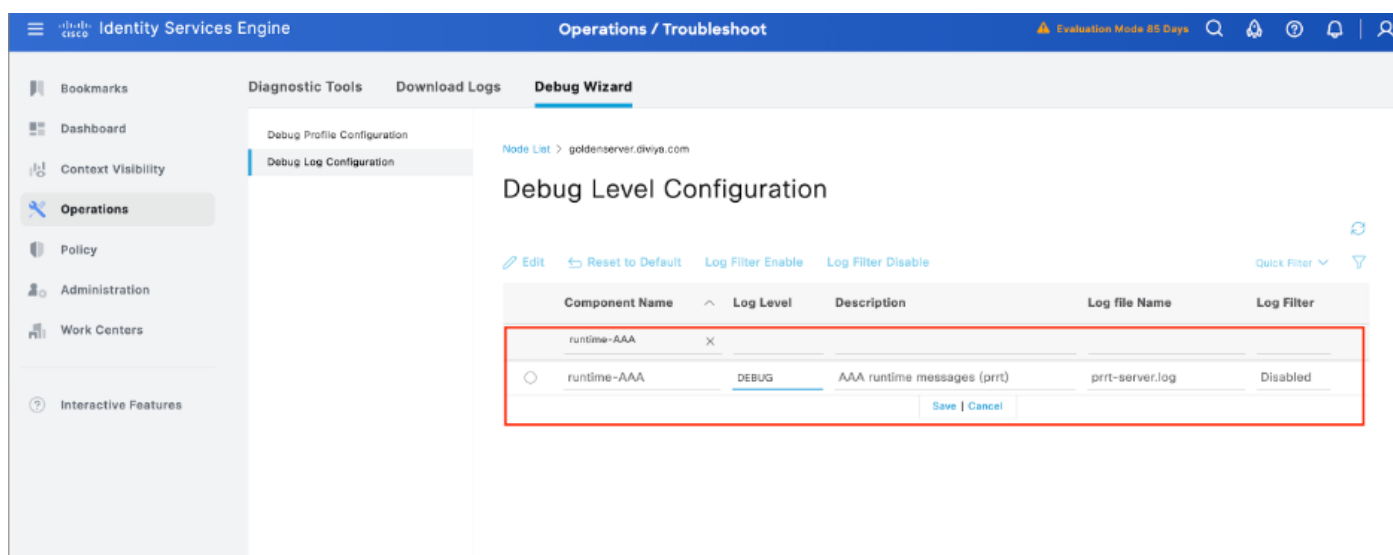
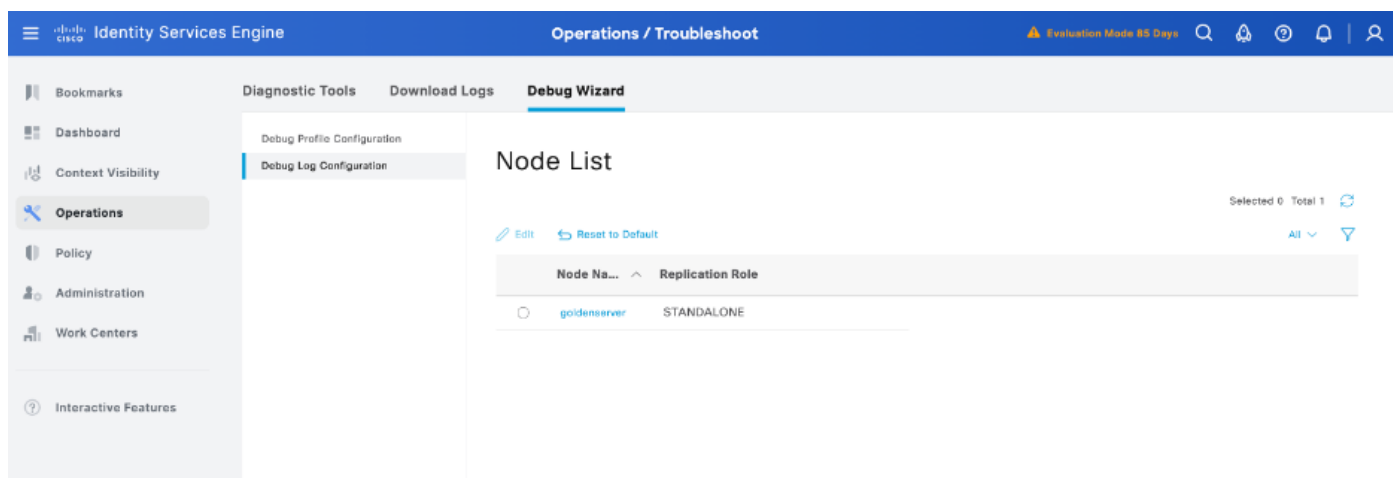
Limit to 1 File(s)

Time Limit 5 Minute(s)

☐ Promiscuous 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 o botão Editar:



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

Troubleshooting

Problema 1

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

"13036 perfil de shell selecionado é DenyAccess"

Overview		Steps	
Request Type	Authentication	13013	Received TACACS+ Authentication START Request
Status	Fail	15049	Evaluating Policy Group (🔴 Step latency=1ms)
Session Key	goldenserver/541265148/80	15008	Evaluating Service Selection Policy (🔴 Step latency=0ms)
Message Text	Failed-Attempt: Authentication failed	15048	Queried PIP - DEVICE.Device Type (🔴 Step latency=2ms)
Username	diviya	15041	Evaluating Identity Policy (🔴 Step latency=3ms)
Authentication Policy	Arista SW_TACACS >> Arista SW_TACACS Auth	15048	Queried PIP - Network Access.Protocol (🔴 Step latency=2ms)
Selected Authorization Profile	Deny All Shell Profile	15013	Selected Identity Source - Internal Users (🔴 Step latency=2ms)
Authentication Details		24210	Looking up User in Internal Users IDStore (🔴 Step latency=0ms)
Generated Time	2025-07-27 16:06:30.094000 +05:30	24212	Found User in Internal Users IDStore (🔴 Step latency=37ms)
Logged Time	2025-07-27 16:06:30.094	13045	TACACS+ will use the password prompt from global TACACS+ configuration (🔴 Step latency=0ms)
Epoch Time (sec)	1753612590	13015	Returned TACACS+ Authentication Reply (🔴 Step latency=0ms)
ISE Node	goldenserver	13014	Received TACACS+ Authentication CONTINUE Request (🔴 Step latency=68ms)
Message Text	Failed-Attempt: Authentication failed	15041	Evaluating Identity Policy (🔴 Step latency=0ms)
Failure Reason	13036 Selected Shell Profile is DenyAccess	15013	Selected Identity Source - Internal Users (🔴 Step latency=4ms)
Resolution	Check whether the Device Administration Authorization Policy rules are correct	24210	Looking up User in Internal Users IDStore (🔴 Step latency=0ms)
Root Cause	Selected Shell Profile fails for this request	24212	Found User in Internal Users IDStore (🔴 Step latency=7ms)
Username	diviya	22037	Authentication Passed (🔴 Step latency=0ms)
		15036	Evaluating Authorization Policy (🔴 Step latency=0ms)
		15048	Queried PIP - Network Access.UserName (🔴 Step latency=4ms)

O erro "13036 perfil de shell selecionado é DenyAccess" no Cisco ISE geralmente significa que, durante uma tentativa de administração de dispositivo TACACS+, a política de autorização correspondeu a um perfil de shell definido como DenyAccess. Geralmente, isso não é resultado de um perfil de shell configurado incorretamente em si, mas indica que nenhuma das regras de autorização configuradas correspondeu aos atributos de usuário de entrada (como associação de grupo, tipo de dispositivo ou local). Como resultado, o ISE volta para uma regra padrão ou uma regra de negação explícita, resultando no acesso negado.

Possíveis causas

- Revise as regras da política de autorização no ISE. Confirme se o usuário ou dispositivo corresponde à regra correta que atribui o perfil de shell desejado, como um que permita acesso apropriado.
- Verifique se o AD ou o mapeamento do grupo de usuários interno está correto e se as condições da política, como associação do grupo de usuários, tipo de dispositivo e protocolo, estão especificadas com precisão.
- Use os logs ao vivo do ISE e os detalhes da tentativa com falha para ver exatamente qual regra é correspondida e por quê.

Problema 2

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

"13017 pacote TACACS+ recebido de dispositivo de rede desconhecido ou cliente AAA"



Overview

Request Type	Authentication
Status	Fail
Session Key	
Message Text	Failed-Attempt: TACACS+ Request dropped
Username	
Authentication Policy	
Selected Authorization Profile	

Authentication Details

Generated Time	2025-07-27 17:50:17.705000 +05:30
Logged Time	2025-07-27 17:50:17.705
Epoch Time (sec)	1753618817
ISE Node	goldenserver
Message Text	Failed-Attempt: TACACS+ Request dropped
Failure Reason	13017 Received TACACS+ packet from unknown Network Device or AAA Client
Resolution	
Root Cause	
Username	

Steps

13017 Received TACACS+ packet from unknown Network Device or AAA Client

Possíveis causas

- O motivo mais comum é que o endereço IP do switch não é adicionado como um dispositivo de rede no ISE (em Administração > Recursos de rede > Dispositivos de rede).
- Certifique-se de que o endereço IP ou intervalo corresponda exatamente ao IP de origem que está sendo usado pelo switch Arista para enviar pacotes TACACS+.
- Se o switch usar uma interface de gerenciamento, verifique se o IP exato (não apenas uma sub-rede/intervalo) foi adicionado ao ISE.

Solução

- Vá para Administração > Recursos de rede > Dispositivos de rede na GUI do ISE.
- Verifique se o endereço IP de origem exato no switch Arista está usando para comunicação TACACS+ (geralmente o IP da interface de gerenciamento).
- Especifique o segredo compartilhado (ele deve corresponder ao que está definido no switch Arista).

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.