

Configurar login de administrador baseado em RADIUS no switch Arista

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Configurar](#)

[Configuração do Cisco ISE](#)

[Etapa 1. Obter o perfil do dispositivo de rede Arista para o Cisco ISE](#)

[Etapa 2. Adicionar um switch Arista como um dispositivo de rede](#)

[Etapa 3. Validar se o novo dispositivo é exibido em Dispositivos de rede](#)

[Etapa 4. Criar os Grupos de Identidade de Usuário Obrigatórios](#)

[Etapa 5. Definir um nome para o Grupo de Identidade do Usuário do Administrador](#)

[Etapa 6. Criar os Usuários Locais e Adicioná-los ao Grupo de Correspondentes](#)

[Etapa 7. Criar o Perfil de Autorização para o Usuário Admin](#)

[Etapa 8. Criar um conjunto de políticas que corresponda ao endereço IP do switch Arista](#)

[Etapa 9. Exibir o Novo Conjunto de Políticas](#)

[Configurando o switch Arista](#)

[Etapa 1. Ativar a autenticação RADIUS](#)

[Etapa 2. Salvar a configuração](#)

[Verificar](#)

[Revisão do ISE](#)

[Troubleshooting](#)

[Cenário 1. "5405 Solicitação RADIUS descartada"](#)

[Problema](#)

[Possíveis causas](#)

[Solução](#)

[Cenário 2: Falha do switch Arista no failover para backup do ISE PSN](#)

[Problema](#)

[Possíveis causas](#)

[Solução](#)

Introdução

Este documento descreve como configurar o Cisco Identity Services Engine (ISE) para autenticar logons de administrador em switches Arista usando o RADIUS.

Pré-requisitos

Requisitos

Antes de continuar, verifique se:

- O Cisco ISE (recomenda-se a versão 3.x) está instalado e operacional.
- Switch Arista executando EOS com suporte a RADIUS.
- Active Directory (AD) ou banco de dados de usuário interno configurado no ISE.

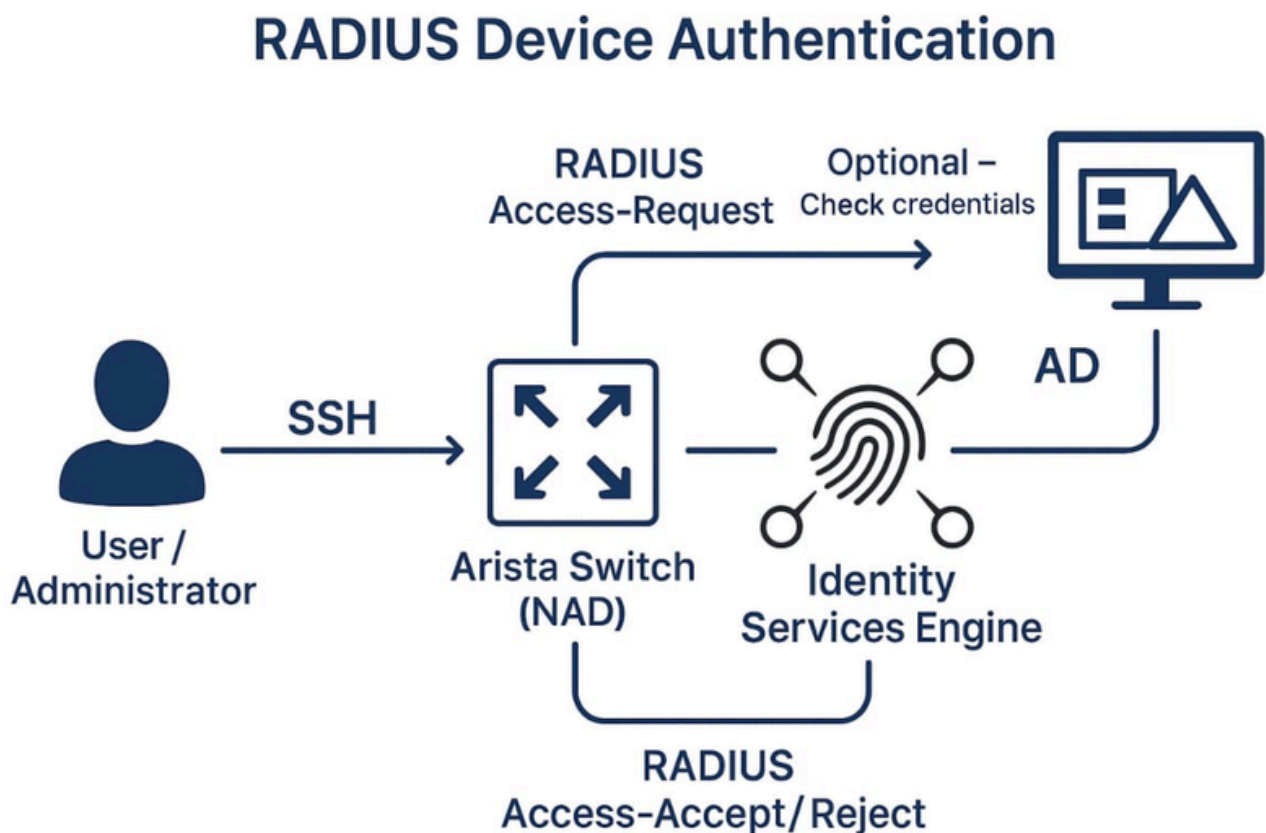
Componentes Utilizados

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



Este é um diagrama de rede que ilustra a autenticação de dispositivos baseados em RADIUS para um switch Arista usando o Cisco ISE, com o Active Directory (AD) como uma origem de

autenticação opcional.

O diagrama inclui:

- Switch Arista (atuando como o dispositivo de acesso à rede, NAD)
- Cisco ISE (atuando como servidor RADIUS)
- Active Directory (AD) [Opcional] (usado para verificação de identidade)
- Usuário/Administrador (que faz login via SSH)

Configurar

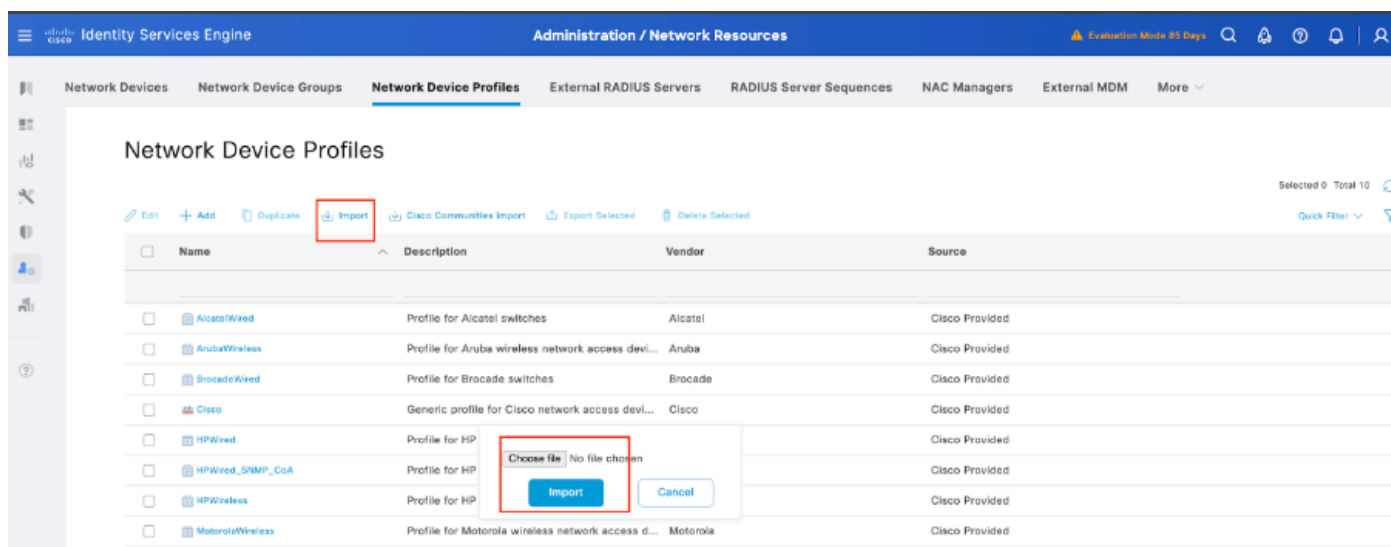
Configuração do Cisco ISE

Etapas 1. Obtendo o perfil de 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

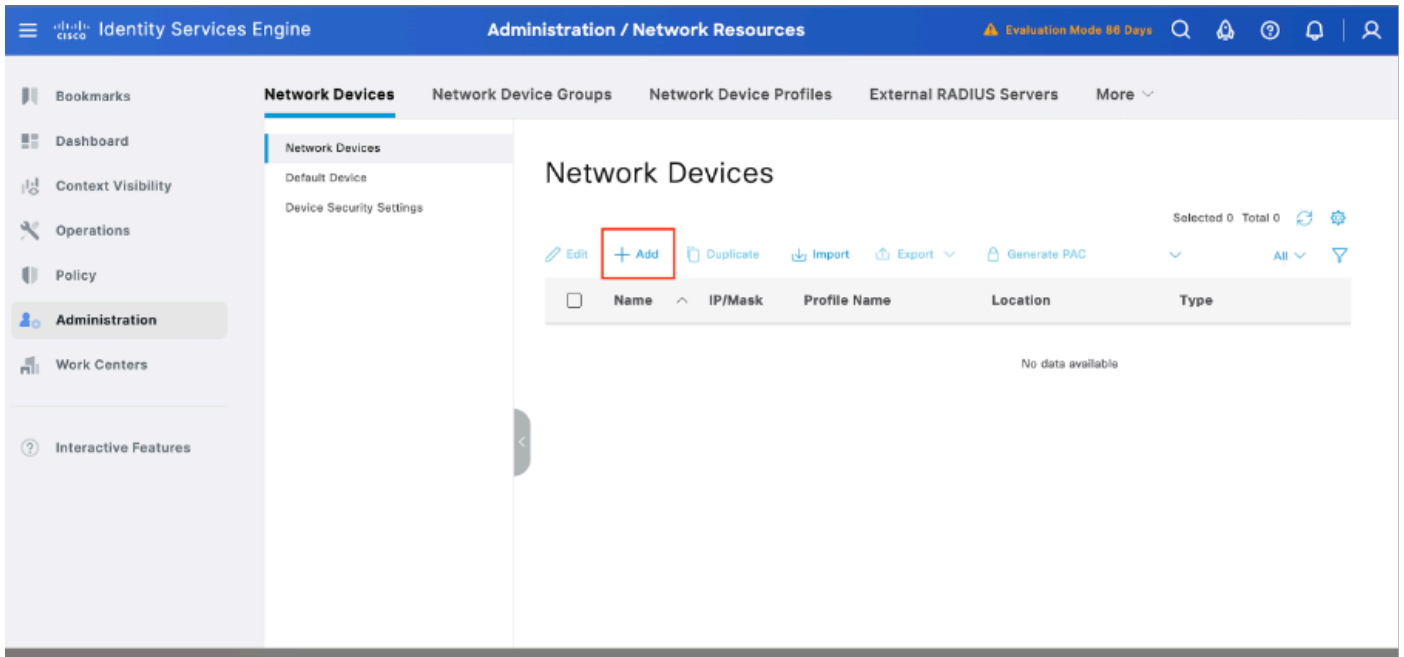
Estas são as etapas para importar o perfil Arista NAD para o Cisco ISE:

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 Import
 - Carregue o arquivo de perfil Arista NAD baixado.



Etapa 2. Adicionar o switch Arista como um dispositivo de rede

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



2. Clique em Adicionar e informe estes detalhes:

1. Nome: Arista-Switch
2. Endereço IP: <Switch-IP>
3. tipo de dispositivo: Escolha outro com fio
4. Perfil do dispositivo de rede: selecione AirstaCloudVisionWiFi.
5. Configurações de autenticação RADIUS:
 1. Habilitar autenticação RADIUS
 2. Insira o Shared Secret (deve corresponder à configuração do switch).

3. Clique em Salvar.

The screenshot shows the 'Network Devices' configuration page in the Cisco ISE Administration console. The breadcrumb trail is 'Administration / Network Resources'. The left sidebar shows 'Network Devices' as the active section. The main content area is titled 'Network Devices' and shows the configuration for a device named 'Arista_switch'. The configuration includes fields for Name, Description, IP Address (with a dropdown for IP and a value of 32), Device Profile (set to 'AristaCloudVisionWiFi'), Model Name, Software Version (set to '4-33-2F'), Network Device Group, Location (set to 'All Locations'), IPSEC (set to 'No'), and Device Type (set to 'All Device Types'). Below these fields, the 'RADIUS Authentication Settings' section is expanded, showing 'RADIUS UDP Settings' with 'Protocol' set to 'RADIUS' and a 'Shared Secret' field. A red box highlights the 'RADIUS Authentication Settings' section header.

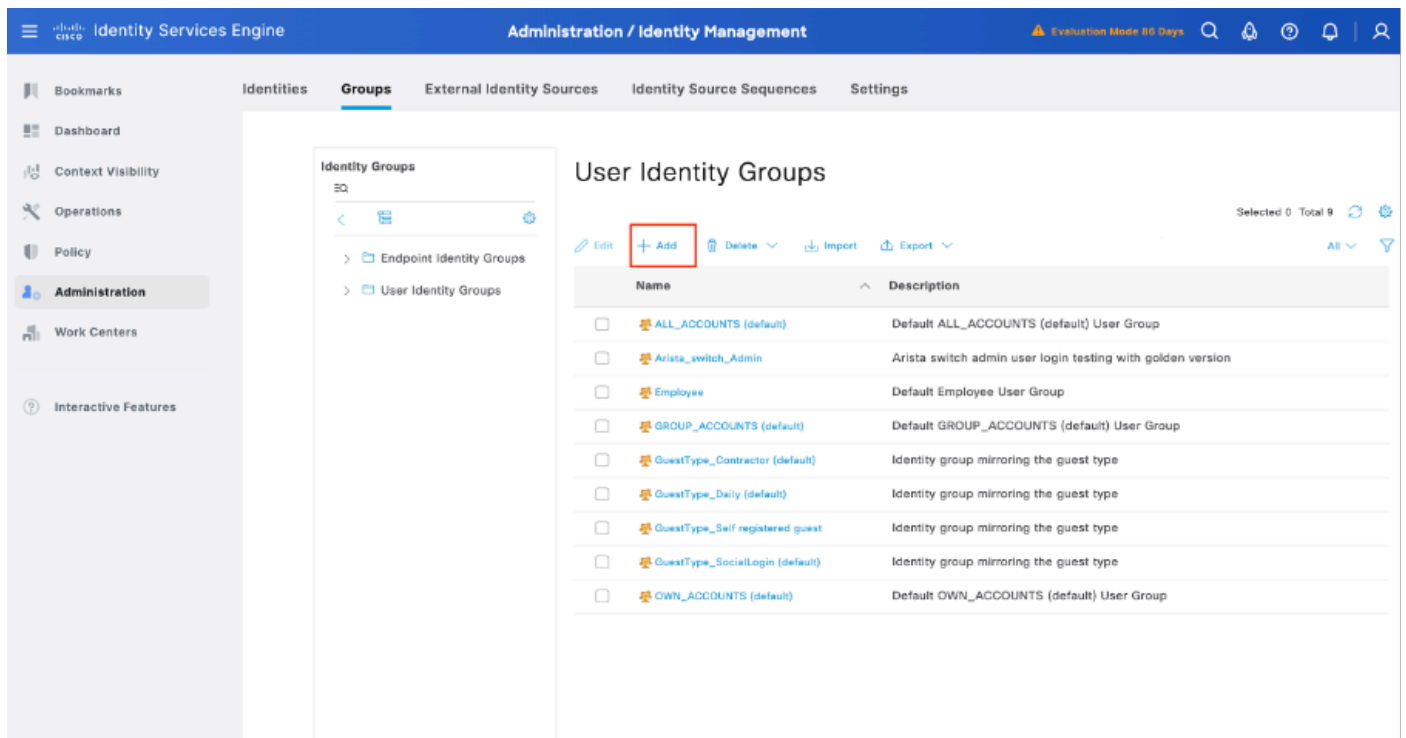
Etapa 3. Valide se o novo dispositivo é mostrado em Dispositivos de rede

The screenshot shows the 'Network Devices' list page in the Cisco ISE Administration console. The breadcrumb trail is 'Administration / Network Resources'. The left sidebar shows 'Network Devices' as the active section. The main content area is titled 'Network Devices' and shows a list of devices. A red box highlights the table containing the device 'Arista_switch'.

Name	IP/Mask	Profile Name	Location	Type	Description
Arista_switch	[Redacted]	AristaCloudVisionWiFi	All Locations	All Device Types	Arista_switch for device login

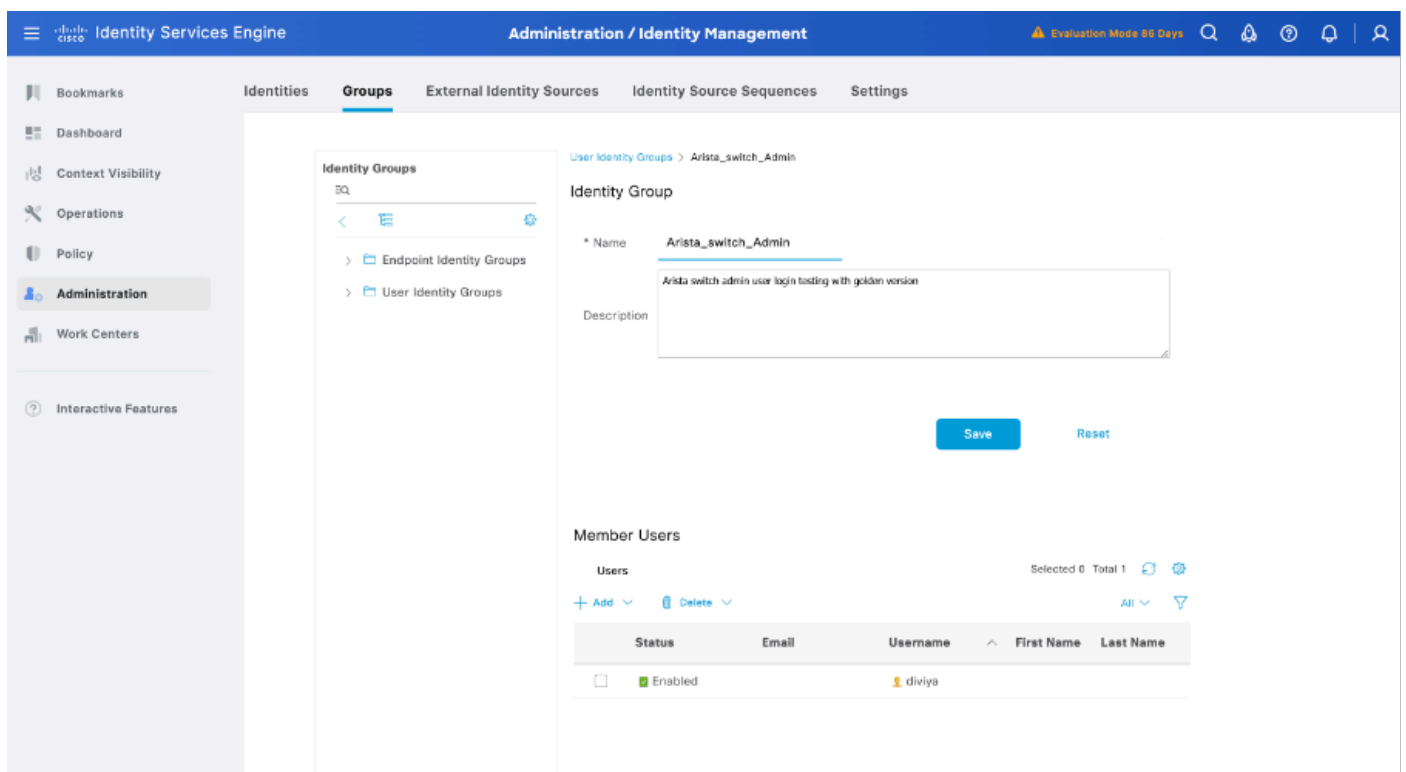
Etapa 4. Crie os grupos de identidade do usuário necessários

Navegue até Administração > Gerenciamento de identidades > Grupos > Grupos de identidades do usuário > + Adicionar:



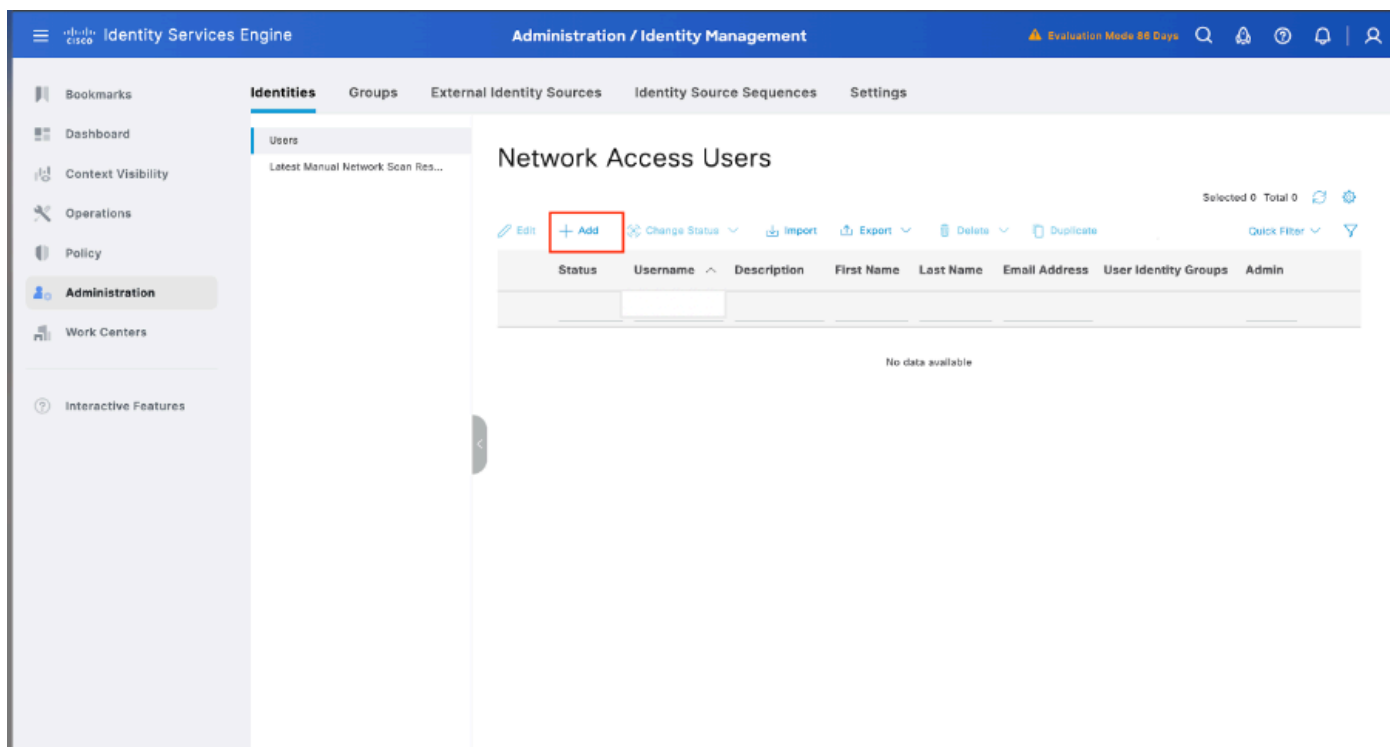
Etapa 5. Definir um nome para o Grupo de Identidade de Usuário Admin

Clique em Submit para salvar a configuração:

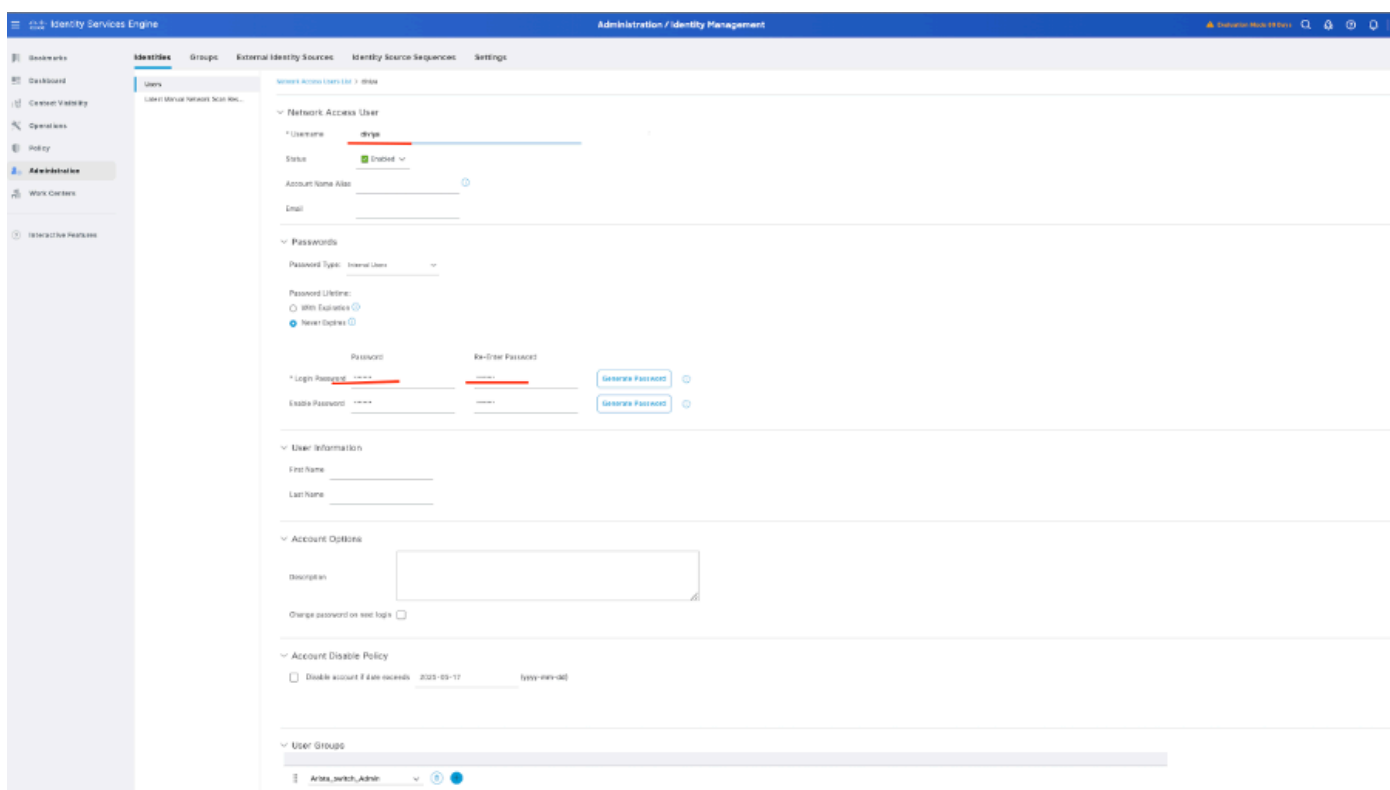


Etapa 6. Criar os Usuários Locais e Adicioná-los ao Grupo de Correspondentes

Navegue até Administração > Gerenciamento de identidades > Identidades > + Adicionar:



6.1. Adicione o usuário com direitos de Administrador. Defina um nome, uma senha e atribua-a a Arista_switch_Admin, role para baixo e clique em Enviar para salvar as alterações.

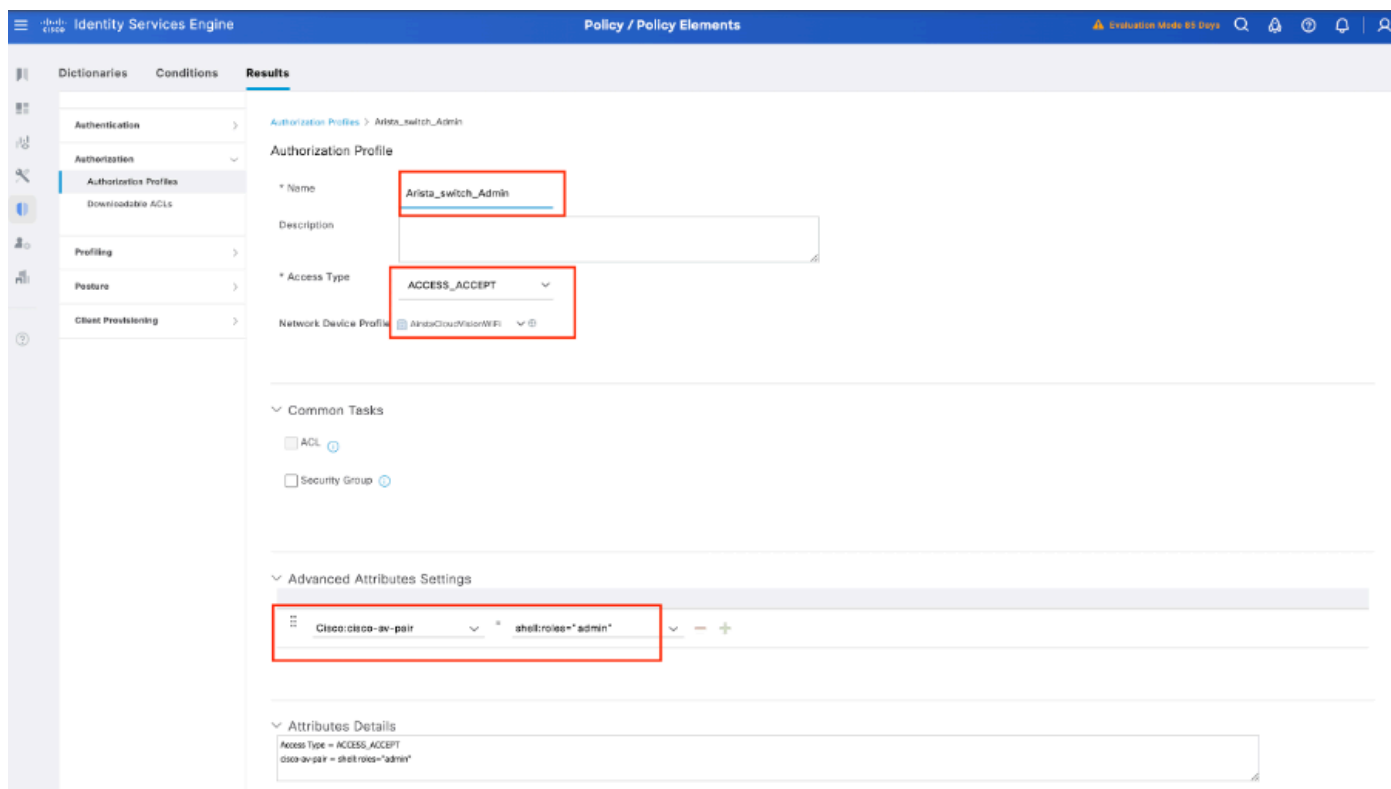


Passo 7. Criar o perfil de autorização para o usuário administrador

Navegue até Política > Elementos de política > Resultados > Autorização > Perfis de autorização > +Adicionar.

Defina um nome para o perfil de autorização, deixe Tipo de acesso como ACCESS_ACCEPT e

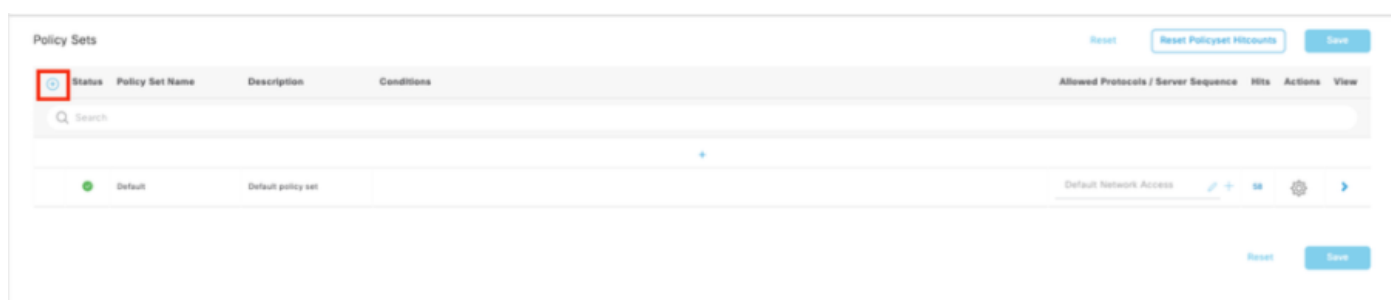
em Configurações avançadas de atributos adicione cisco-av-pair=shell:roles="admin" com e clique em Enviar.



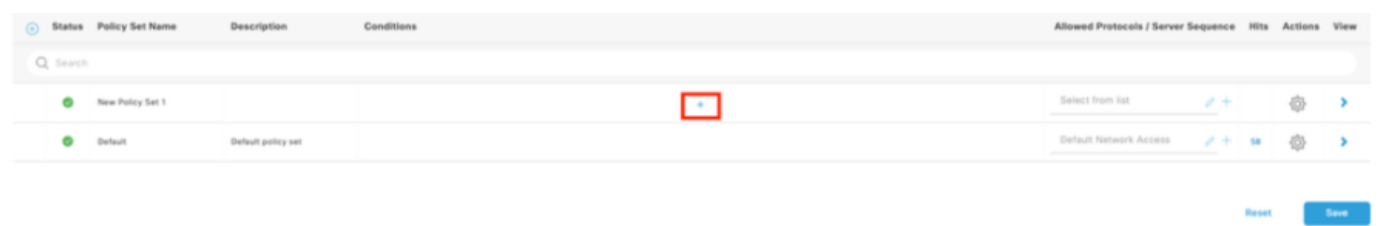
Etapa 8. Crie um conjunto de políticas correspondente ao endereço IP do switch Arista

Isso evita que outros dispositivos concedam acesso aos usuários.

Navegue até Policy > Policy Sets > Add icon sign no canto superior esquerdo.

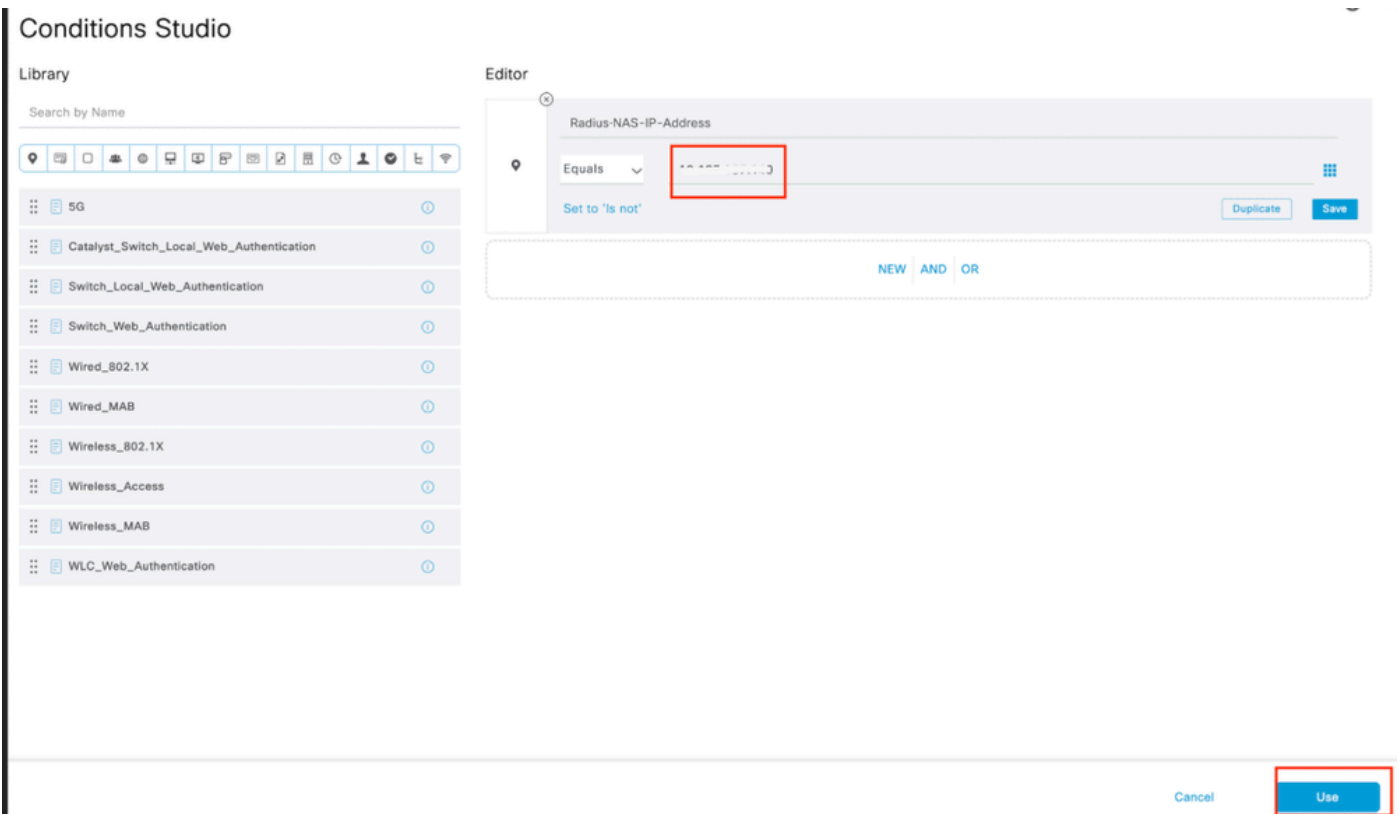
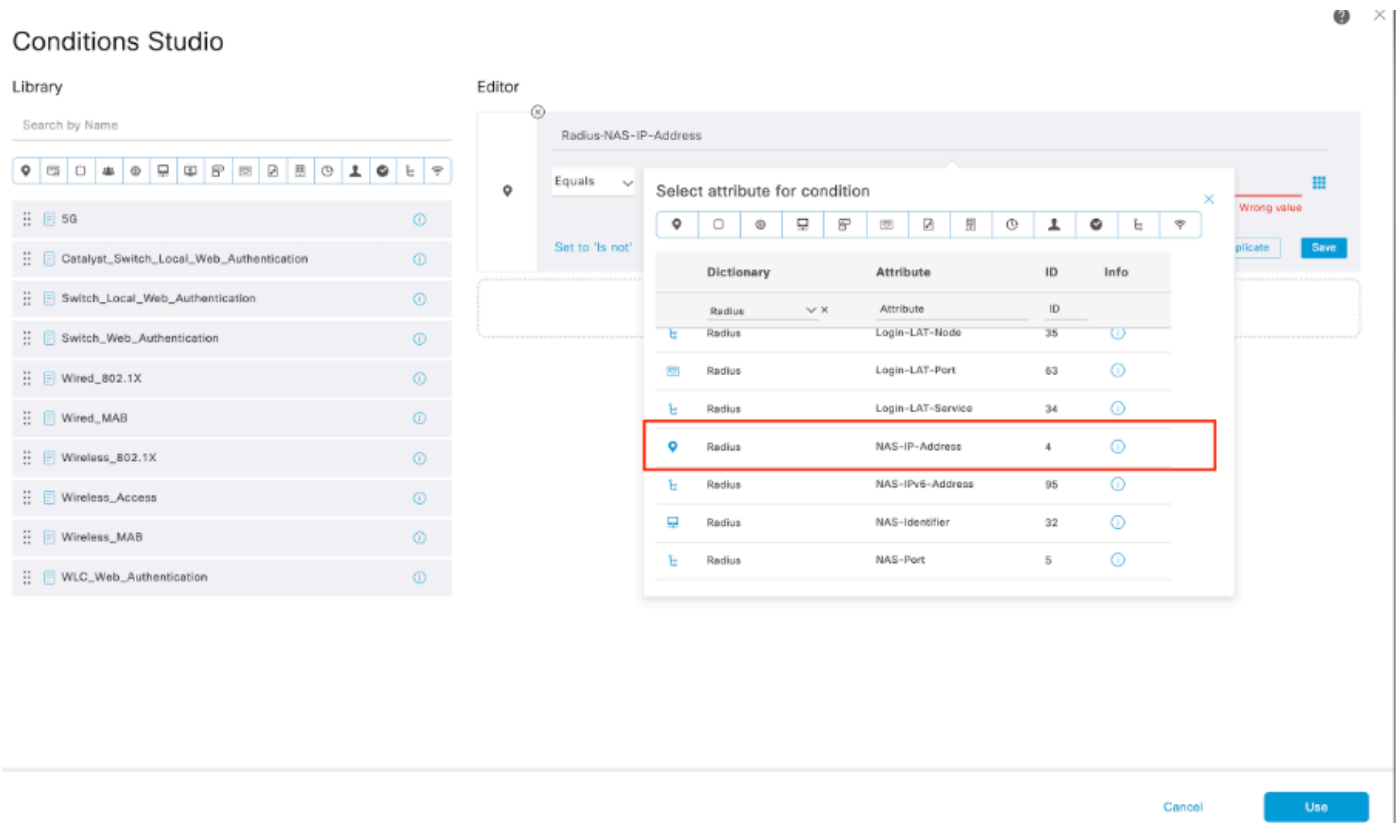


8.1 Uma nova linha é colocada na parte superior de seus conjuntos de políticas. Clique no ícone Adicionar para configurar uma nova condição.



8.2 Adicione uma condição superior para o atributo RADIUS NAS-IP-Address que corresponda ao

endereço IP do switch Arista e clique em Use.



8.3 Depois de concluir, clique em Salvar:

Identity Services Engine

Policy / Policy Sets

Evaluation Mode 88 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

Policy Sets

Reset

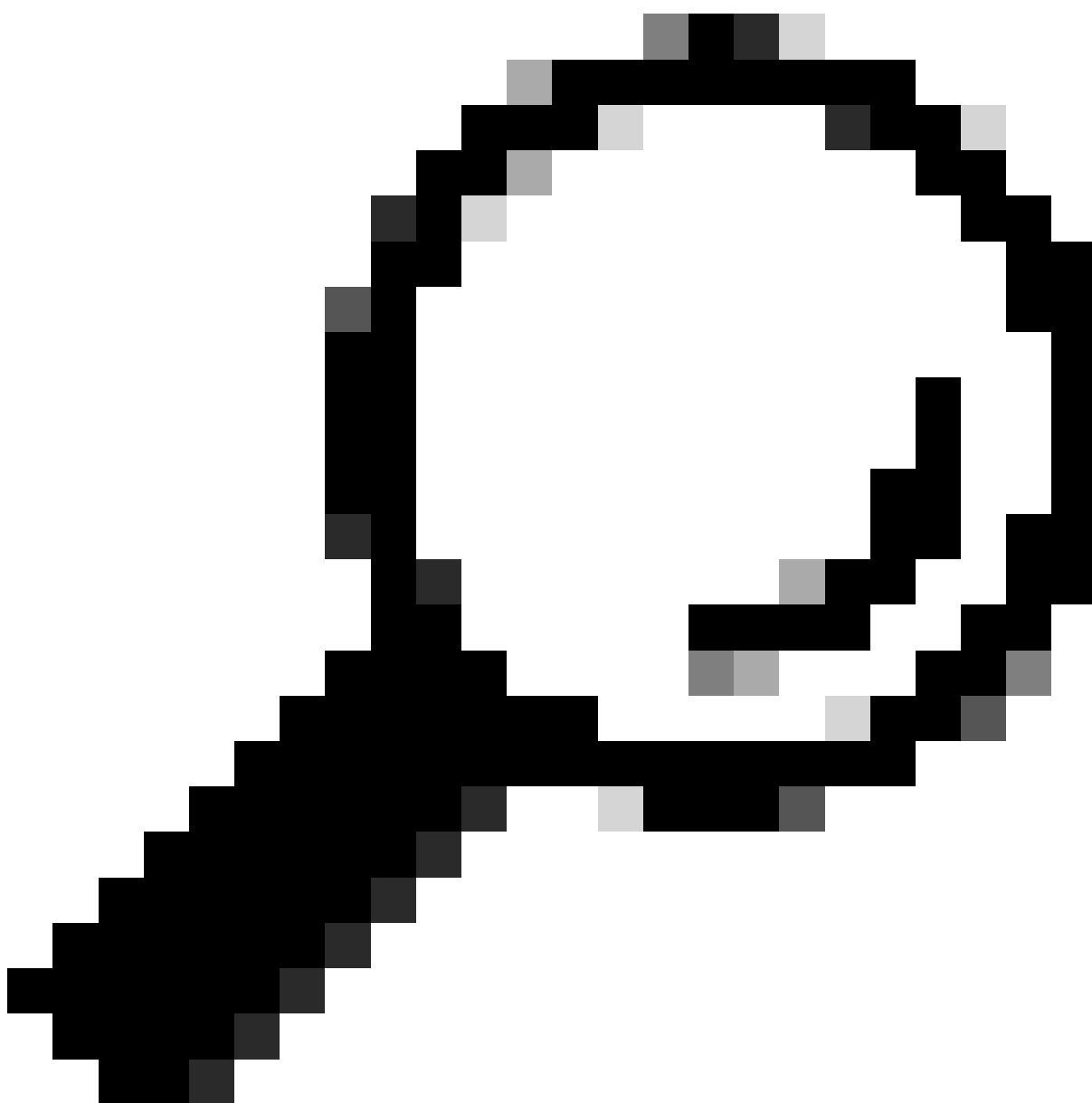
Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Arista_switch_radius login		Radius NAS-IP-Address EQUALS	Default Network Access	26		
✓	Wired		DEVICE-Device Type EQUALS All Device Types	Default Network Access	3		
✓	Default	Default policy set		Default Network Access	0		

Reset

Save



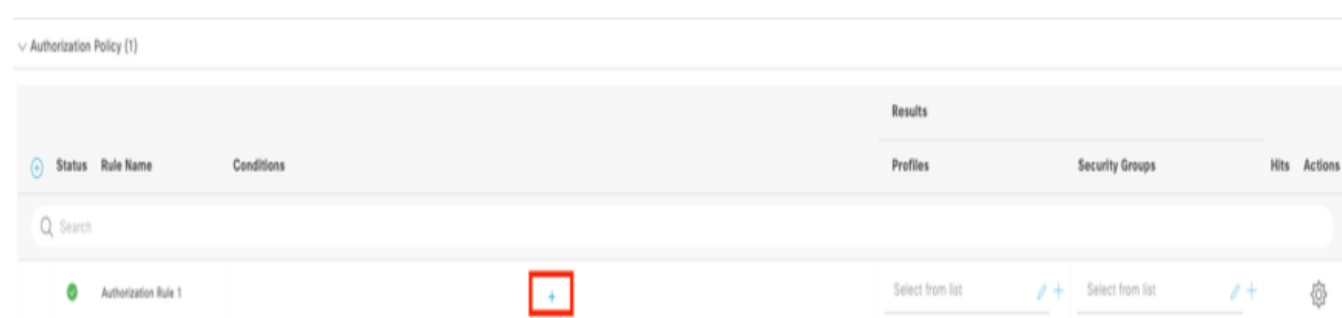
Tip: Para este exercício, permitimos a lista de Protocolos de acesso à rede padrão. Você pode criar uma nova lista e restringi-la conforme necessário.

Etapa 9. Exibir o novo conjunto de políticas

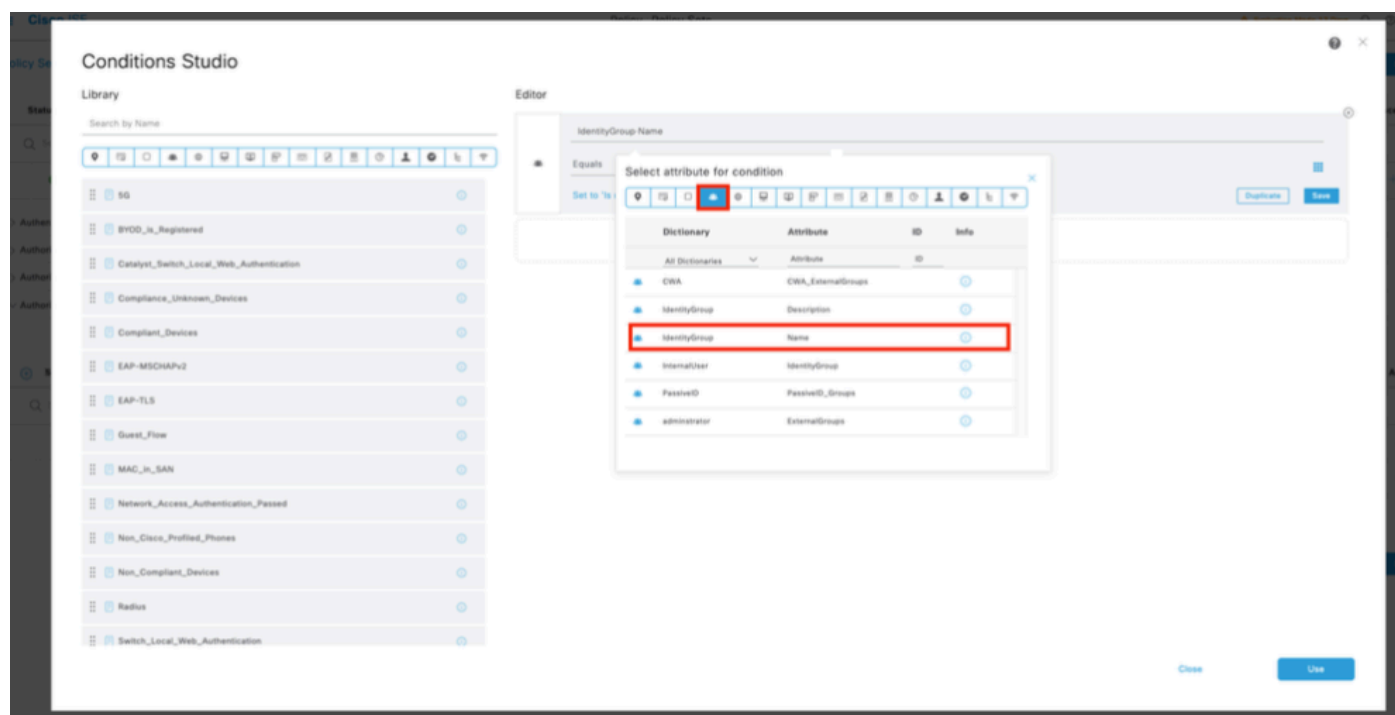
Clique no ícone > localizado no final da linha:



9.1 Expanda o menu Authorization Policy e clique em (+) para adicionar uma nova condição.



9.2 Defina as condições para corresponder o Grupo de Identidade do Dicionário com o Nome do Atributo Igual a Grupos de Identidade do Usuário: Arista_switch_Admin (o nome do grupo criado na Etapa 7) e clique em Usar.



Conditions Studio

Library

Search by Name

5G	
BYOD_is_Registered	
Catalyst_Switch_Local_Web_Authentication	
Compliance_Unknown_Devices	
Compliant_Devices	
EAP-MSCHAPv2	
EAP-TLS	
Guest_Flow	
MAC_in_SAN	
Network_Access_Authentication_Passed	
Non_Cisco_Profiled_Phones	
Non_Compliant_Devices	
Switch_Local_Web_Authentication	
Switch_Web_Authentication	

Editor

IdentityGroup-Name

Equals User Identity Groups:Arista_switch_Admin

Set to 'Is not'

Duplicate Save

NEW AND OR

Cancel

Use

9.3 Valide se a nova condição está configurada na política de autorização e adicione um perfil de usuário em Perfis:

Authorization Policy(2)

				Results			
Status	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
Search							
✓	Arista_Radius_login	IdentityGroup-Name EQUALS User Identity Groups:Arista_switch_Admin		Arista_switch_Admin	Select from list	9	⚙️
✓	Default			DenyAccess	Select from list	0	⚙️

Reset

Save

Configurando o switch Arista

Etapa 1. Ativar a autenticação RADIUS

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

configurar

!

radius-server host <ISE-IP> key <RADIUS-SECRET>

radius-server timeout 5

radius-server retransmit 3

radius-server deadtime 30

!

aaa group server radius ISE

server <ISE-IP>

!

aaa authentication login default group ISE local

aaa authorization exec default group ISE local

aaa accounting exec default start-stop group ISE

aaa accounting commands 15 default start-stop group ISE

aaa accounting system default start-stop group ISE

!

fim

Etapa 2. Salvar a configuração

Para manter as configurações nas reinicializações:

memória de gravação

or

copy running-config startup-config

Verificar

Revisão do ISE

1. Tente fazer login no Arista Switch usando as novas credenciais Radius:

1.1 Navegue até Operations > Radius > Live logs.

1.2 As informações exibidas mostram se um usuário efetuou login com êxito.

Identity Services Engine Operations / RADIUS

Evaluation Mode 60 Days

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

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0 Repeat Counter 5

Refresh Never Show Latest 20 records Within Last 3 hours

Reset Repeat Counts Export To

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization...	Authoriz...
Mar 18, 2025 07:08:22.0...			4	diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 07:08:21.9...			1	diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 07:08:21.9...				diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 07:08:21.9...				diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...

2. Para obter o status de falha, revise os detalhes da sessão:

Identity Services Engine Operations / RADIUS

Evaluation Mode 60 Days

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0 Repeat Counter 6

Refresh Never Show Latest 20 records Within Last 3 hours

Reset Repeat Counts Export To

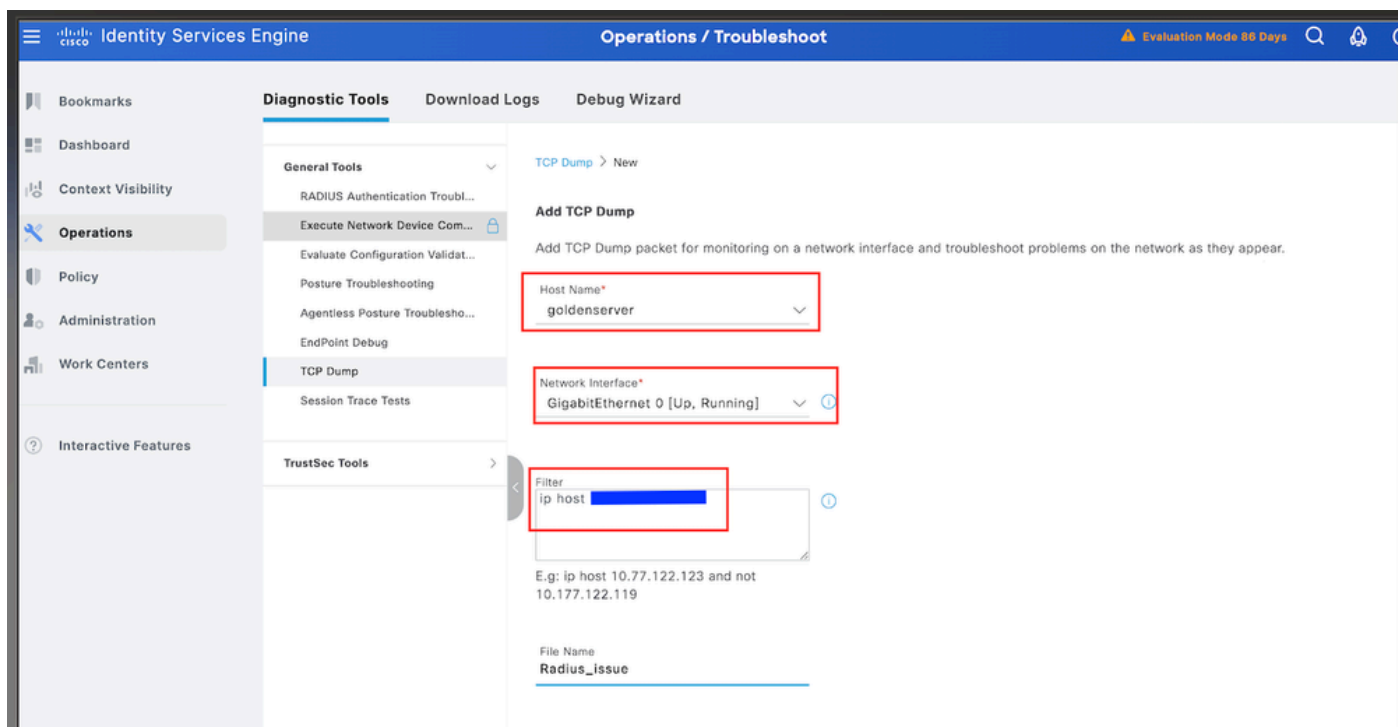
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization...	Authoriz...
Mar 18, 2025 05:57:12.4...	Auth Failed			diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 05:57:02.5...				diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 05:56:16.3...				diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 05:56:08.0...				diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...

3. Para solicitações que não aparecem nos logs do Radius Live , revise se a solicitação UDP está alcançando o nó ISE por meio de uma captura de pacote.

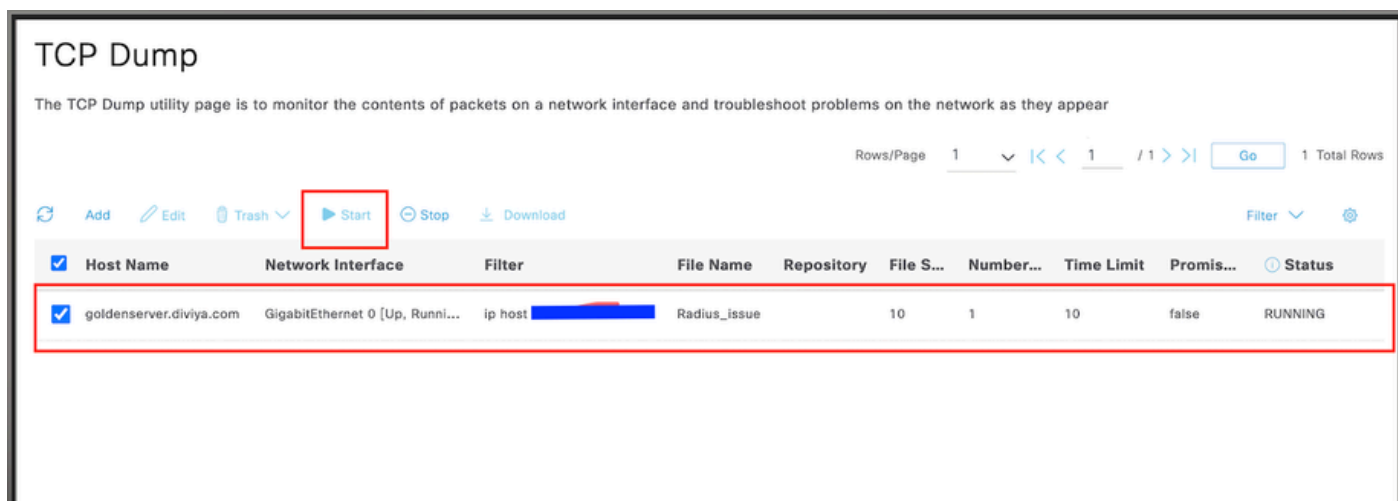
3.1. Navegue até Operations > Troubleshoot > Diagnostic Tools > TCP dump.

3.2. Adicione uma nova captura e faça o download do arquivo em sua máquina local para verificar se os pacotes UDP estão chegando ao nó ISE.

3.3. Preencha as informações solicitadas, role para baixo e clique em Salvar.



3.4. Selecione e inicie a captura.



3.5. Tente fazer login no switch Arista enquanto a captura do ISE estiver em execução.

3.6. Pare o TCP Dump no ISE e baixe o arquivo para uma máquina local.

3.7. Analisar a saída do tráfego.

Saída esperada:

Pacote No1. Solicitação do Switch Arista ao servidor ISE através da porta 1812 (RADIUS).

Pacote No2. Resposta do servidor ISE aceitando a solicitação inicial.

No.	Time	Source	Destination	Protocol	Length	Info
1	2025-03-18 07:16:26.147865			RADIUS	126	Access-Request id=141
2	2025-03-18 07:16:26.247483			RADIUS	181	Access-Accept id=141
3	2025-03-18 07:16:26.322942			RADIUS	213	Accounting-Request id=142
4	2025-03-18 07:16:26.342623			RADIUS	62	Accounting-Response id=142

Troubleshooting

Cenário 1. "5405 Solicitação RADIUS descartada"

Problema

Este cenário envolve a identificação e solução de problemas de um erro "5405 RADIUS Request drops" com a razão "11007 Could not locate Network Device or AAA Client" no Cisco ISE quando um dispositivo de rede (como um switch Arista) tenta autenticar.

Possíveis causas

- O Cisco Identity Services Engine (ISE) não pode identificar o switch Arista porque seu endereço IP não está listado entre os dispositivos de rede conhecidos.
- A solicitação RADIUS vem de um endereço IP que o ISE não reconhece como um dispositivo de rede válido ou cliente AAA.
- Pode haver uma incompatibilidade na configuração entre o switch e o ISE (como um IP incorreto ou segredo compartilhado).

Solução

- Adicione o switch à lista do Cisco ISE de dispositivos de rede com o endereço IP correto.
- Verifique se o endereço IP e o segredo compartilhado configurados no ISE correspondem exatamente ao que está definido no switch.
- Uma vez corrigida, a solicitação RADIUS deve ser reconhecida e processada corretamente.

Cenário 2: Falha do switch Arista no failover para backup do ISE PSN

Problema

Um switch Arista é configurado para usar o Cisco ISE para autenticação RADIUS. Quando o Nó de serviço de política (PSN) principal do ISE se torna indisponível, o switch não executa

automaticamente o failover para um PSN de backup. Como resultado, os registros de autenticação só aparecem na PSN principal do ISE, e não há registros da PSN secundária/de backup quando a principal está inativa.

Possíveis causas

- A configuração do servidor RADIUS do switch Arista aponta apenas para o nó principal do ISE, portanto, os servidores de backup não são usados.
- A prioridade do servidor RADIUS não está definida corretamente ou o IP do ISE de backup está ausente da configuração.
- As configurações de tempo limite e retransmissão no switch estão definidas muito baixas, impedindo o retorno bem-sucedido à PSN de backup.
- O switch usa um FQDN para o PSN, mas a resolução DNS não retorna todos os registros A, fazendo com que apenas o servidor primário seja contatado.

Solução

- Verifique se vários IPs PSN do ISE foram inseridos na configuração do grupo de servidores RADIUS do switch. Isso permite que o switch use a PSN do ISE de backup se o principal estiver inacessível.

Exemplo de configuração:

```
radius-server host <ISE1-IP> key <secret>
```

```
radius-server host <ISE2-IP> key <secret>
```

- Verifique se os valores de prioridade, tempo limite e retransmissão do servidor RADIUS estão configurados corretamente para failover confiável.
- Se estiver usando FQDNs, verifique as configurações e a resolução DNS para garantir que todos os endereços IP PSN sejam retornados e usados pelo switch.

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.