# Usar o RADIUS para administração de dispositivos com o Identity Services Engine

## Contents



## Introdução

Este documento descreve a compilação de atributos que vários produtos Cisco e não Cisco esperam receber de um servidor AAA como um Cisco ISE.

## Informações de Apoio

Produtos Cisco e não Cisco esperam receber uma compilação de atributos de um servidor de autenticação, autorização e contabilidade (AAA). Nesse caso, o servidor é um Cisco ISE e o ISE retornaria esses atributos junto com um Access-Accept como parte de um perfil de autorização (RADIUS).

Este documento fornece instruções passo a passo sobre como adicionar perfis de autorização de atributo personalizado e também contém uma lista de dispositivos e os atributos RADIUS que os dispositivos esperam ver retornados do servidor AAA. Todos os tópicos incluem exemplos.

A lista de atributos fornecida neste documento não é exaustiva nem autorizada e pode ser alterada a qualquer momento sem uma atualização deste documento.

A Administração de Dispositivos de um dispositivo de rede é geralmente obtida com o protocolo TACACS+, mas se o dispositivo de rede não suportar TACACS+ ou se o ISE não tiver uma licença de administração de dispositivos, isso também poderá ser feito com o RADIUS se o dispositivo de rede suportar a administração de dispositivos RADIUS. Alguns dispositivos suportam ambos os protocolos e cabe aos usuários decidir qual protocolo usar, mas o TACACS+ pode ser favorável, pois tem recursos como autorização de comandos e contabilidade de comandos.

# Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha o conhecimento destes:

- Cisco ISE como um servidor Radius na rede de interesse
- O fluxo de trabalho do protocolo Radius - RFC2865

## Componentes Utilizados

As informações neste documento são baseadas no Cisco Identity Services Engine (ISE) 3.x e versões posteriores do ISE.

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

Etapa 1. Criar os Atributos Específicos do Fornecedor (VSA)

Pode haver vários dicionários criados para cada um dos fornecedores, e atributos podem ser adicionados a cada um desses dicionários. Cada dicionário pode ter vários atributos que podem ser usados nos perfis de autorização. Cada atributo, em geral, define a função diferente da administração de dispositivos que um usuário pode obter ao fazer login no dispositivo de rede. No entanto, o atributo pode ter diferentes finalidades de operação ou configuração no dispositivo de rede.

O ISE vem com atributos predefinidos para alguns fornecedores. Se o fornecedor não estiver listado, ele poderá ser adicionado como um dicionário com atributos. Para alguns dispositivos de rede, os atributos são configuráveis e podem ser alterados para vários tipos de acesso. Se esse for o caso, o ISE precisa ser configurado com atributos que o dispositivo de rede espera para diferentes tipos de acesso.

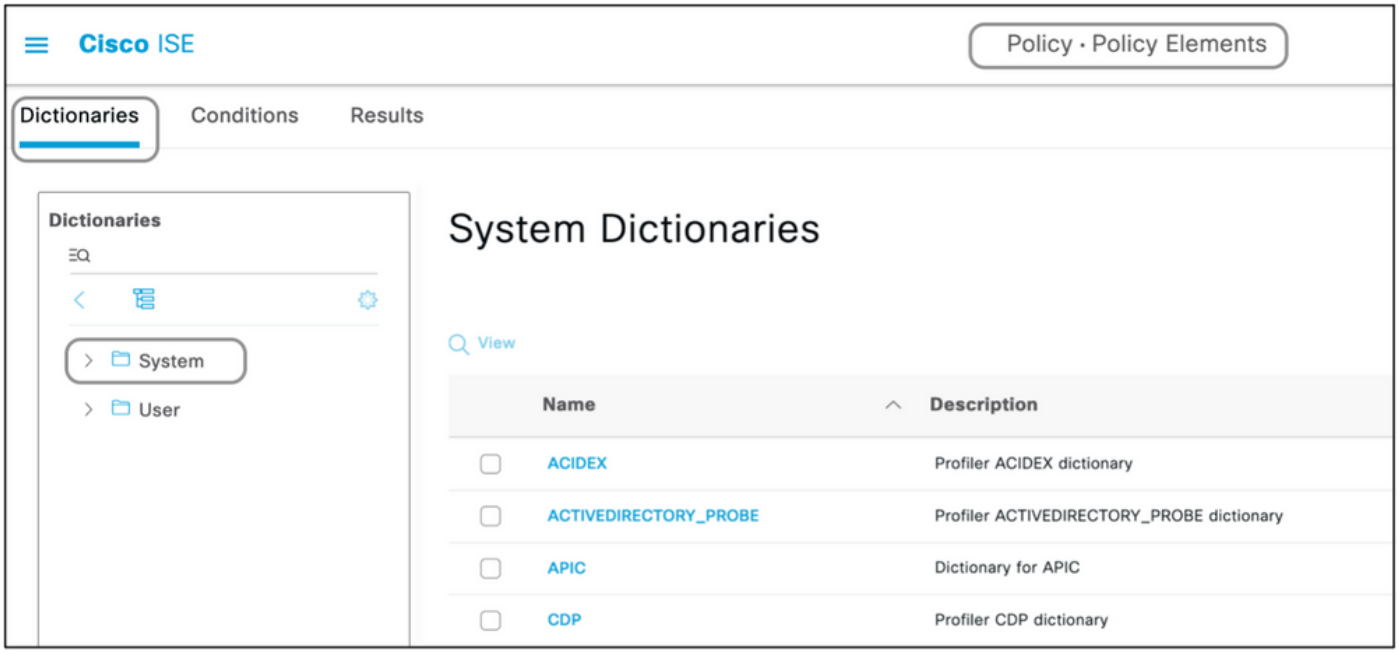
Os atributos que se espera enviar com um Radius Access-Accept são definidos como aqui:

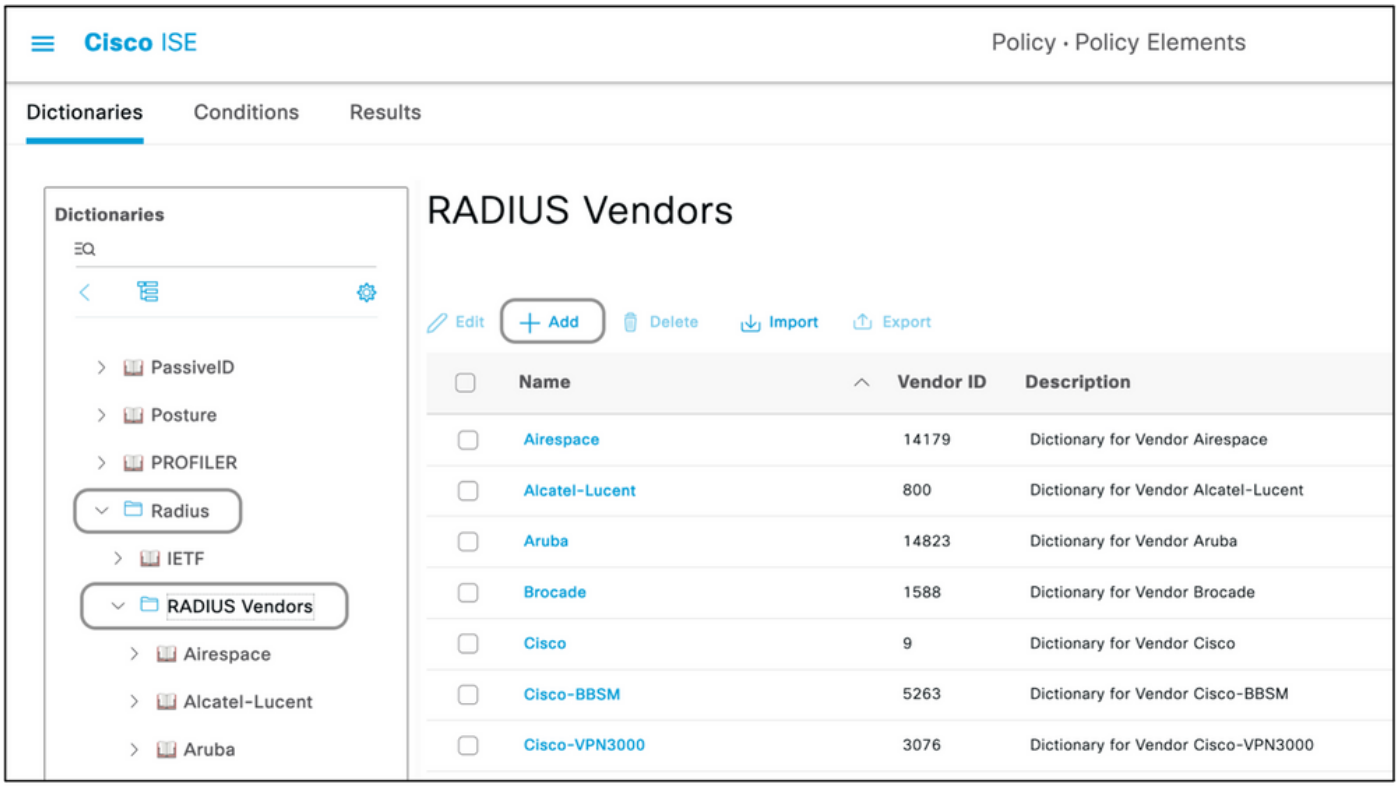
1. Navegue para Política > Elementos de política > Dicionários > Sistema > Radius > Fornecedores Radius > Adicionar.
2. O nome e as IDs de fornecedor devem ser inseridos e salvos.
3. Clique no Fornecedor Radius salvo e navegue para Atributos de dicionário.
4. Clique em Adicionar e preencha o Nome do Atributo, o Tipo de Dados, a Direção e a ID com distinção entre maiúsculas e minúsculas.
5. Salve o atributo.
6. Adicione outros Atributos na mesma página se houver vários Atributos a serem adicionados ao mesmo Dicionário.

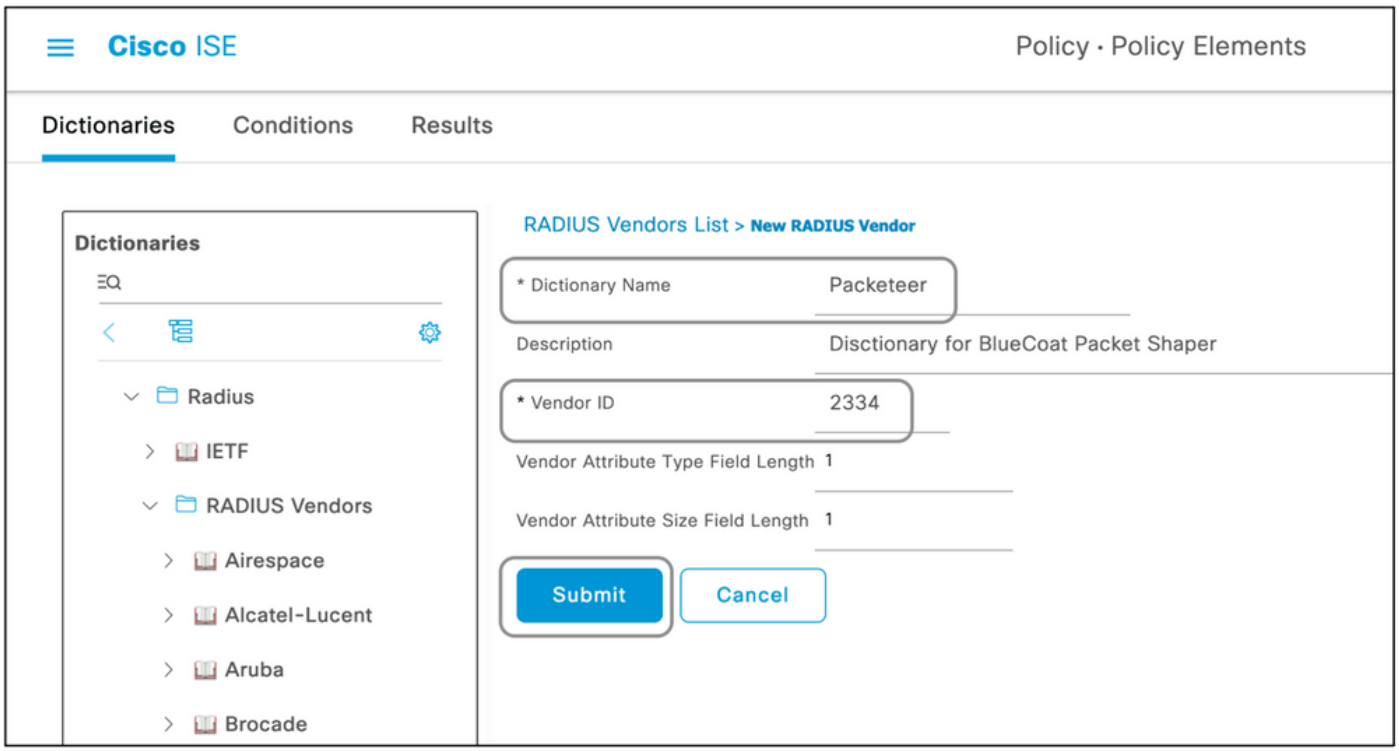
---

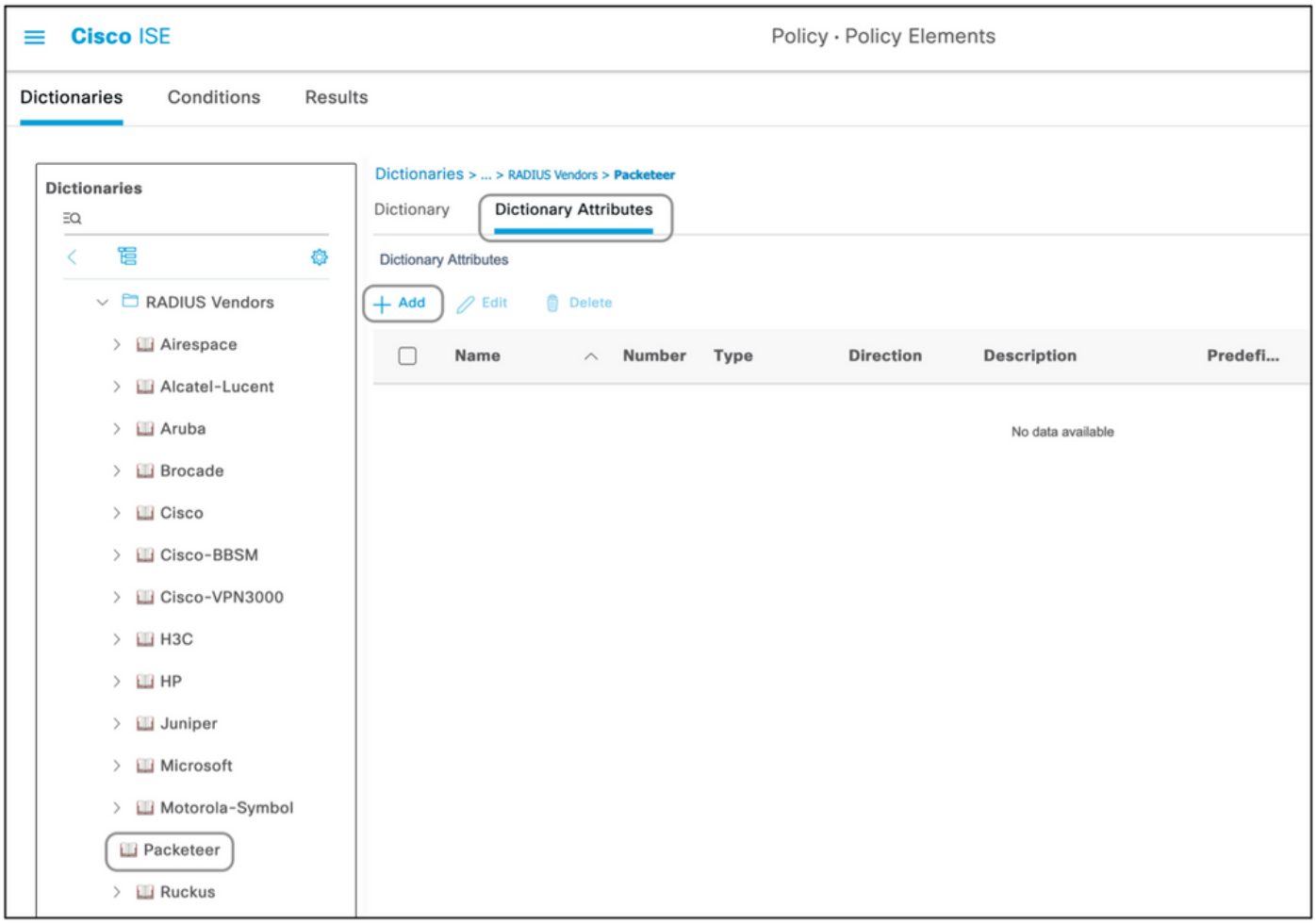
Observação: cada campo inserido como valor nesta seção deve ser fornecido pelo próprio fornecedor. Os sites do fornecedor podem ser visitados ou o suporte do fornecedor pode ser contatado caso eles não sejam conhecidos.

---




Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Dictionaries
PassiveID
Posture
PROFILER
Radius
IETF
RADIUS Vendors
Airespace
Alcatel-Lucent
Aruba
RADIUS Vendors
Edit
Add
Delete
Import
Export
Name
Vendor ID
Description
Airespace 14179 Dictionary for Vendor Airespace
Alcatel-Lucent 800 Dictionary for Vendor Alcatel-Lucent
Aruba 14823 Dictionary for Vendor Aruba
Brocade 1588 Dictionary for Vendor Brocade
Cisco 9 Dictionary for Vendor Cisco
Cisco-BBSM 5263 Dictionary for Vendor Cisco-BBSM
Cisco-VPN3000 3076 Dictionary for Vendor Cisco-VPN3000


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Dictionaries
Radius
IETF
RADIUS Vendors
Airespace
Alcatel-Lucent
Aruba
Brocade
RADIUS Vendors List > New RADIUS Vendor
* Dictionary Name Packeteer
Description Disctionary for BlueCoat Packet Shaper
* Vendor ID 2334
Vendor Attribute Type Field Length 1
Vendor Attribute Size Field Length 1
Submit
Cancel





Observação: nem todos os fornecedores exigem que um dicionário específico seja adicionado. Se o fornecedor puder usar os atributos radius definidos pelo IETF, que já existem no ISE, essa etapa poderá ser ignorada.

Etapa 2. Criar um Perfil de Dispositivo de Rede

Esta seção não é obrigatória. Um perfil de dispositivo de rede ajuda a segregar o tipo de dispositivo de rede que é adicionado e criar perfis de autorização apropriados para eles. Assim como os dicionários radius, o ISE tem alguns perfis predefinidos que podem ser usados. Se ainda não estiver presente, um novo perfil de dispositivo pode ser criado.

Este é o procedimento para adicionar um perfil de rede:

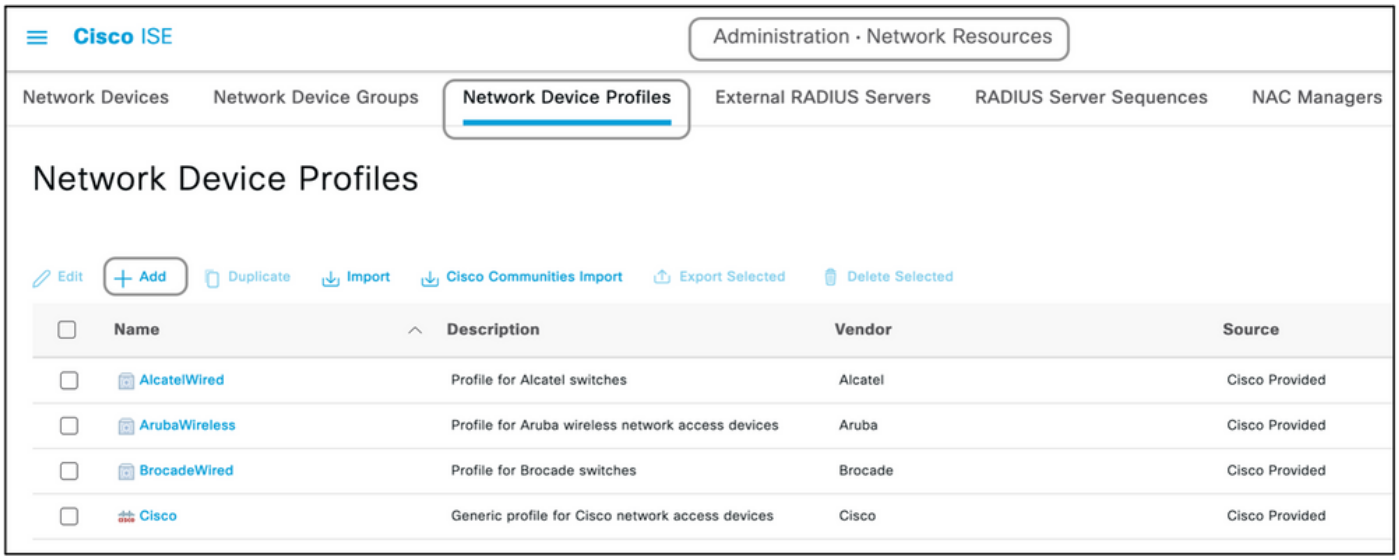
1. Navegue até Administração > Recursos de rede > Perfis de dispositivo de rede > Adicionar.

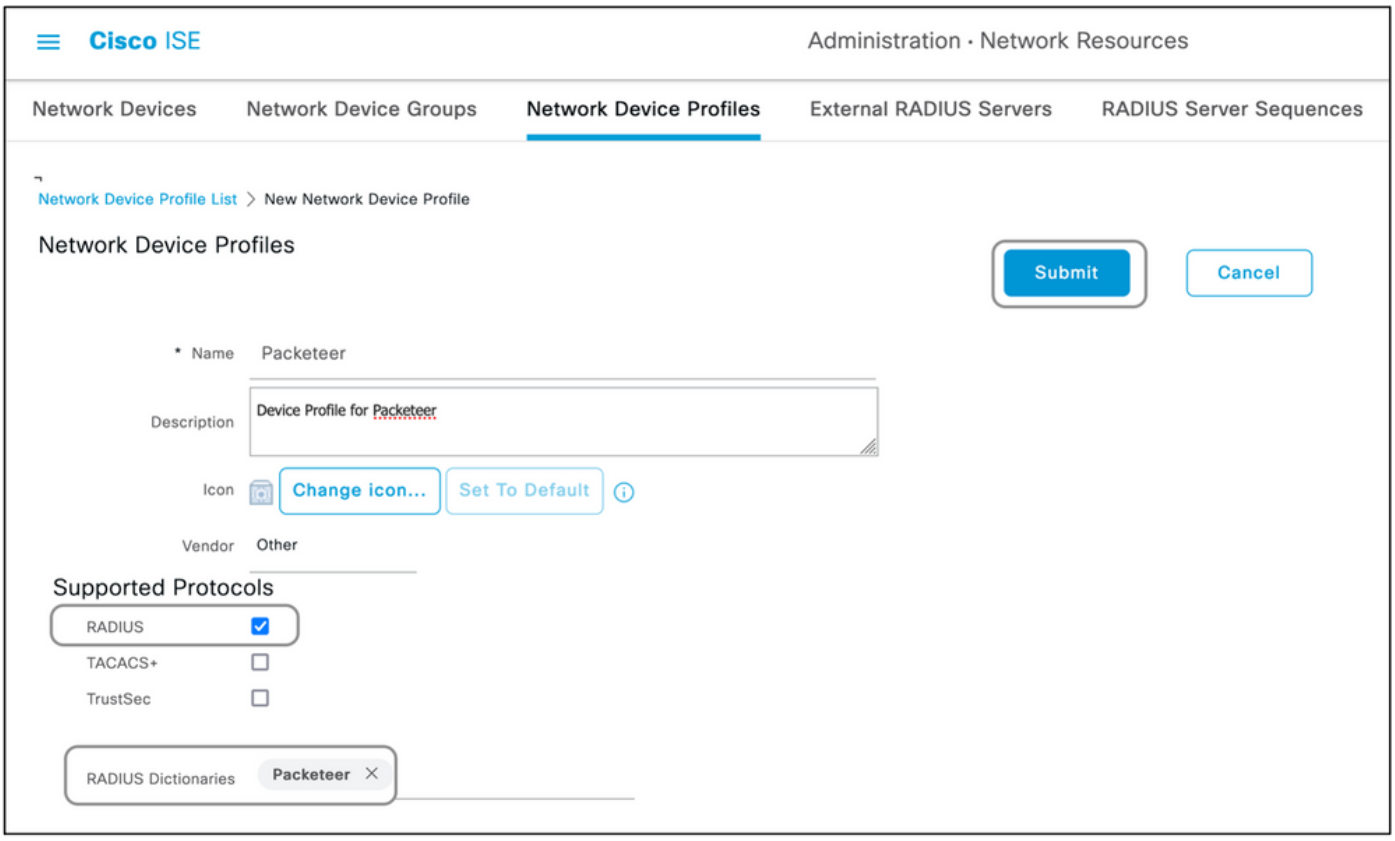
2. Dê um nome e marque a caixa de seleção para RADIUS.

3. Em RADIUS Dictionaries, selecione o dicionário criado na seção anterior.

4. Se vários dicionários foram criados para o mesmo tipo de dispositivo, todos eles poderão ser selecionados em Dicionários RADIUS.

5. Salve o perfil.






Etapa 3. Adicionar o dispositivo de rede no ISE

O dispositivo de rede no qual a administração do dispositivo é obtida deve ser adicionado no ISE junto com uma chave que é definida no dispositivo de rede. No dispositivo de rede, o ISE é adicionado como um servidor AAA radius com essa chave.

Este é o procedimento para adicionar um dispositivo no ISE:

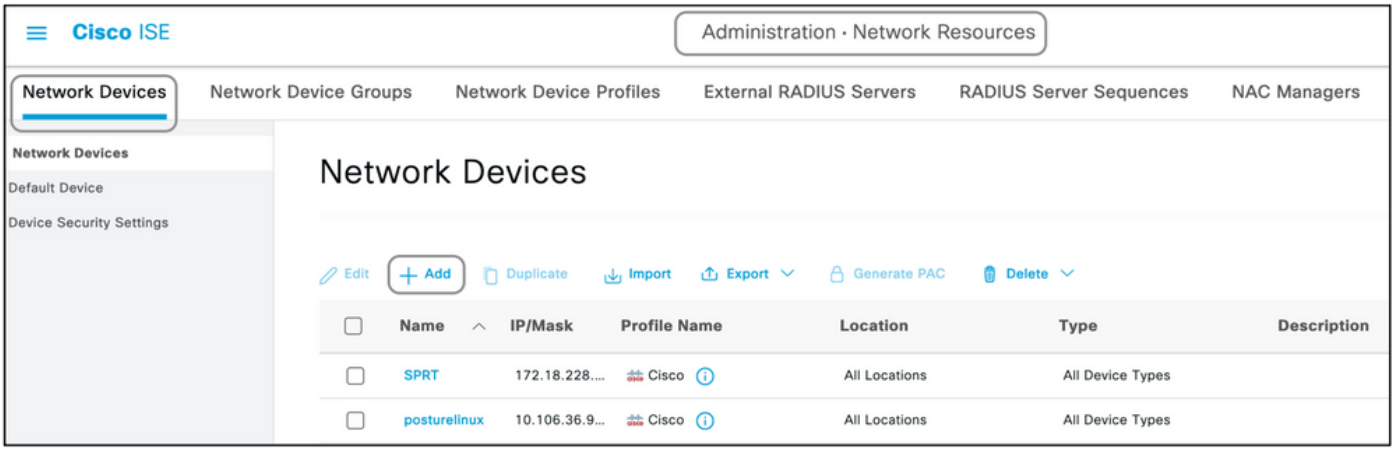
1. Navegue até Administração > Recursos de rede > Dispositivos de rede > Adicionar.

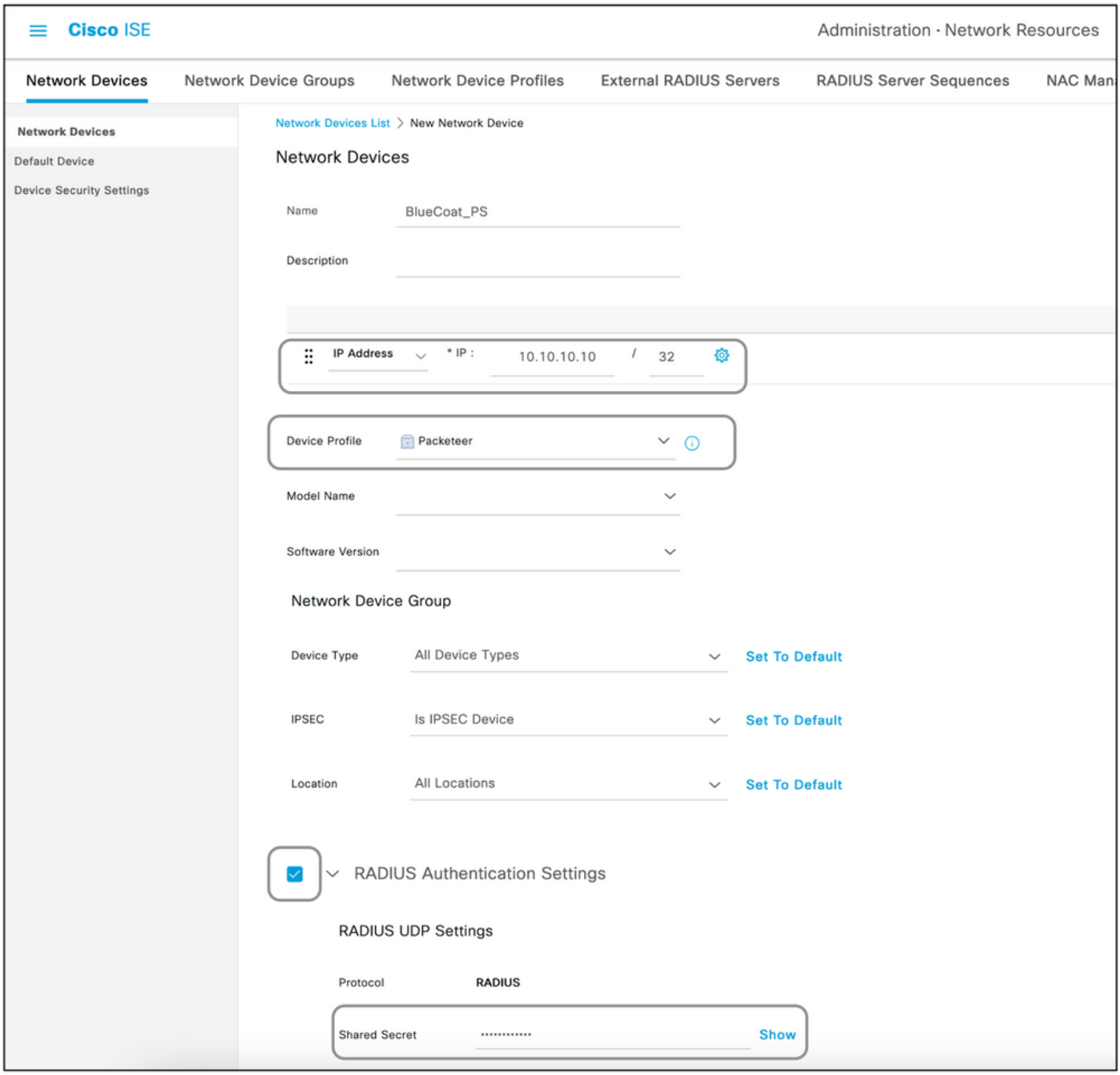
2. Dê um nome e o endereço IP.

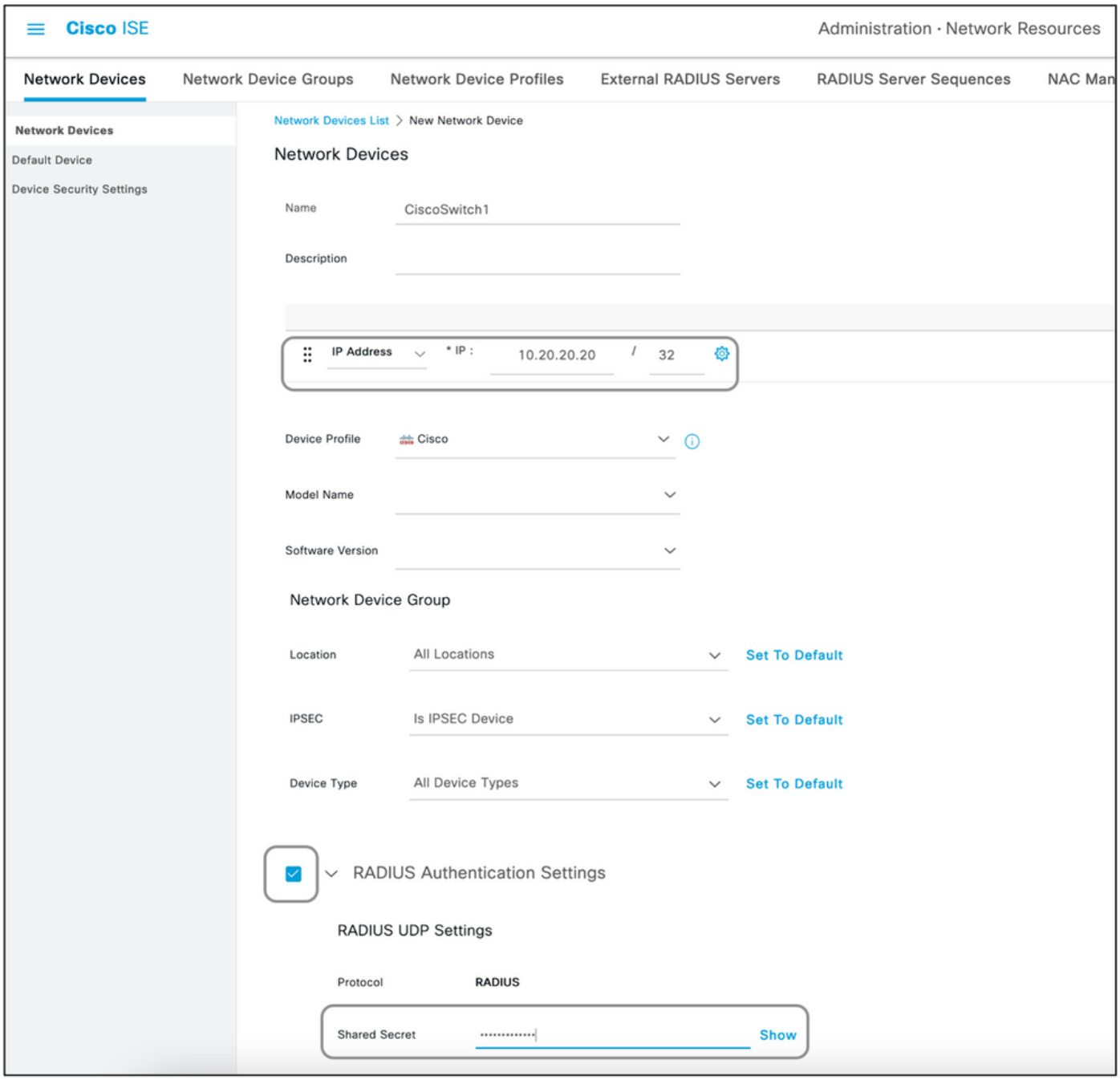
3. O perfil do dispositivo pode ser escolhido na lista suspensa para ser aquele definido na seção anterior. Se um perfil não tiver sido criado, o Cisco padrão poderá ser usado como está.

4. Verifique As Configurações De Autenticação Radius.

5. Insira a chave secreta compartilhada e salve o dispositivo.


Cisco ISE
Administration · Network Resources
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
Network Devices
Default Device
Device Security Settings
Network Devices
Edit
Add
Duplicate
Import
Export
Generate PAC
Delete
Name
IP/Mask
Profile Name
Location
Type
Description
SPRT
172.18.228....
Cisco
All Locations
All Device Types
posturelinux
10.106.36.9...
Cisco
All Locations
All Device Types


Cisco ISE
Administration · Network Resources
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Man
Network Devices
Default Device
Device Security Settings
Network Devices List > New Network Device
Network Devices
Name
BlueCoat_PS
Description
IP Address
* IP :
10.10.10.10
/
32
Device Profile
Packeteer
Model Name
Software Version
Network Device Group
Device Type
All Device Types
Set To Default
IPSEC
Is IPSEC Device
Set To Default
Location
All Locations
Set To Default
RADIUS Authentication Settings
RADIUS UDP Settings
Protocol
RADIUS
Shared Secret
Show



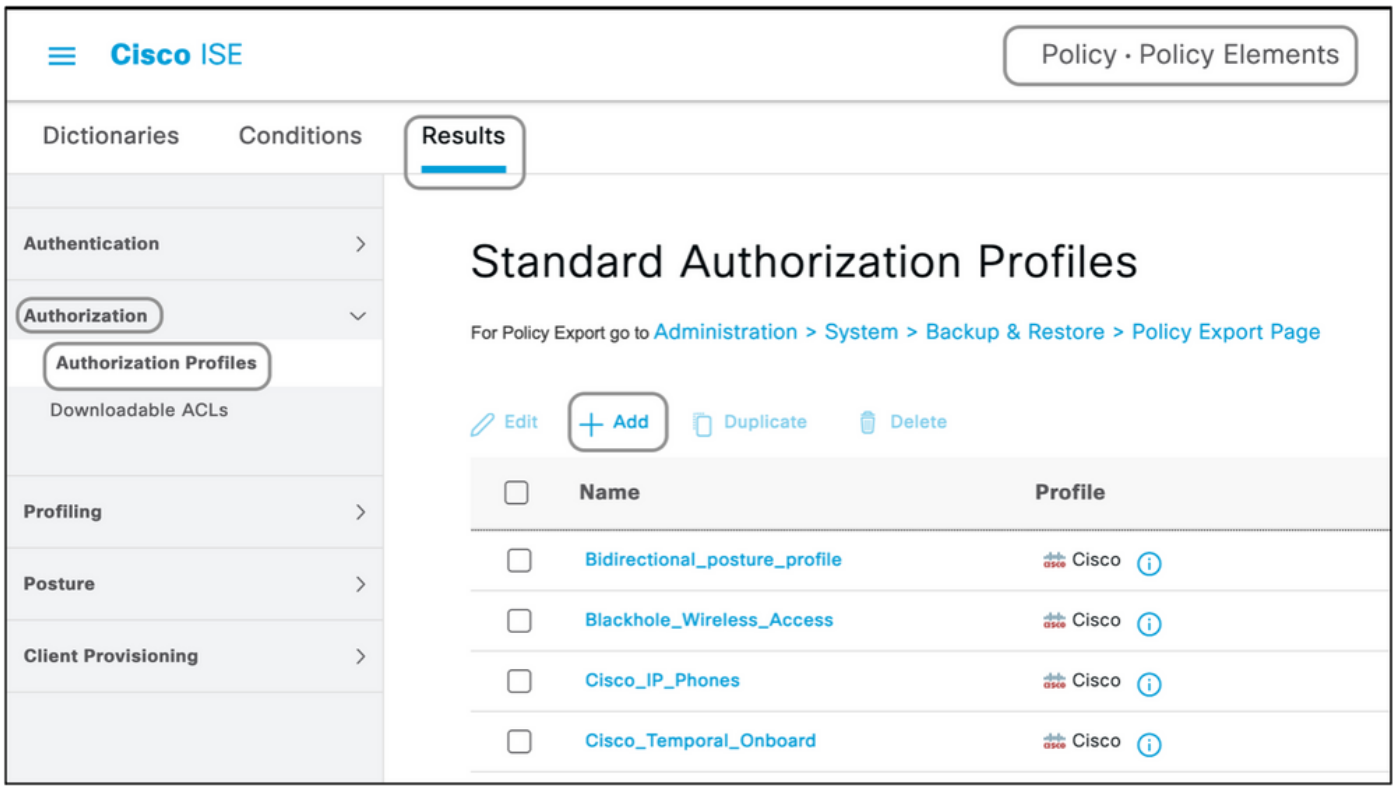

Etapa 4. Criar perfis de autorização

O resultado final que é enviado do ISE como um Access-Accept ou Access-Reject é definido em um perfil de autorização. Cada perfil de autorização pode enviar atributos adicionais que o dispositivo de rede espera.

Este é o procedimento para criar um perfil de autorização:

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

2. Em Perfis de autorização padrão, clique em Adicionar.




Os tipos de perfis que podem ser adicionados são Access-Accept e Access-Reject.

Criar um perfil de aceitação de acesso

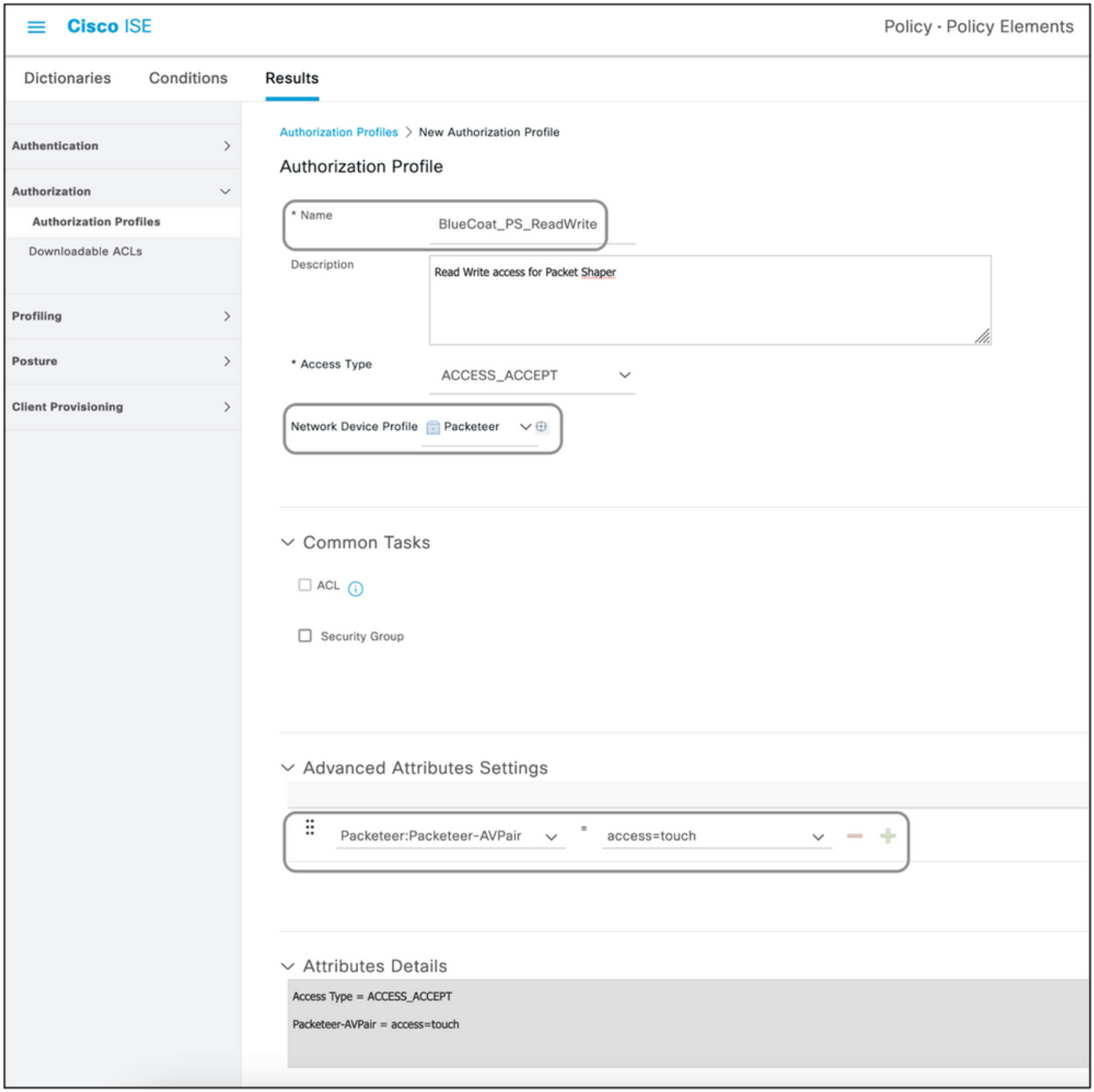
Esse perfil é usado para algum tipo de acesso ao dispositivo de rede. Esse perfil pode ter vários atributos passados junto com ele. Aqui estão as etapas:

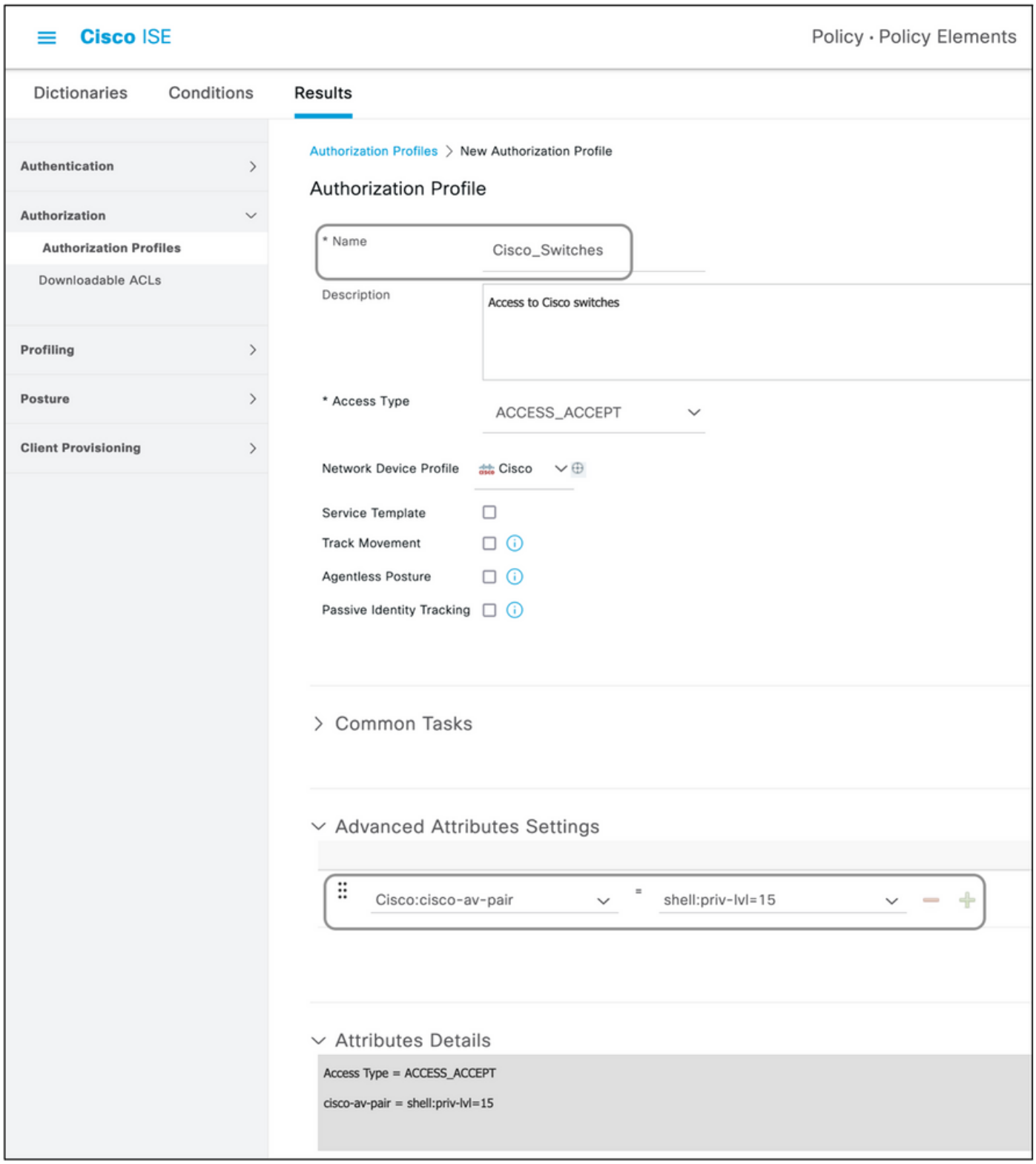
1. Dê um nome sensato e escolha Tipo de acesso para ser Aceitar-acesso.
2. Escolha o perfil do dispositivo de rede que foi criado em uma das seções anteriores. Se nenhum perfil tiver sido criado, o Cisco padrão poderá ser usado.
3. Com diferentes tipos de perfis escolhidos, a página aqui limita as opções de configuração.
4. Em Advanced Attributes Settings, escolha o dicionário e o atributo aplicável (LHS).
5. Atribua um valor (RHS) ao atributo no menu suspenso, se disponível, ou digite o valor esperado.
6. Se houver mais atributos a serem enviados como parte do mesmo resultado, clique no ícone + e repita as etapas 4 e 5.

Crie vários perfis de autorização para cada um dos resultados/funções/autorizações que o ISE deve enviar.

---

Nota: Os atributos consolidados podem ser verificados no campo Detalhes do Atributo.


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Profiling
Posture
Client Provisioning
Authorization Profiles > New Authorization Profile
Authorization Profile
* Name
BlueCoat_PS_ReadWrite
Description
Read Write access for Packet Shaper
* Access Type
ACCESS_ACCEPT
Network Device Profile
Packeteer
Common Tasks
ACL
Security Group
Advanced Attributes Settings
Packeteer:Packeteer-AVPair
=
access=touch
Attributes Details
Access Type = ACCESS_ACCEPT
Packeteer-AVPair = access=touch




Criar um Perfil de Rejeição de Acesso

Esse perfil é usado para enviar uma rejeição para a administração do dispositivo, mas ainda pode ser usado para enviar atributos junto com ele. Isso é usado para enviar um pacote Access-Reject Radius. As etapas permanecem as mesmas, exceto a etapa um, em que Access-Reject deve ser escolhido em vez de Access-Accept para o Tipo de acesso.

Etapa 5. Criar um conjunto de políticas

Os conjuntos de políticas no ISE são avaliados de cima para baixo e o primeiro que satisfaz a condição definida nos conjuntos de políticas é responsável pela resposta do ISE ao pacote de Solicitação de Acesso Radius enviado pelo dispositivo de rede. A Cisco recomenda um conjunto de políticas exclusivo para cada tipo de dispositivo. A condição para avaliar a autenticação e a autorização do usuário acontece na avaliação. Se o ISE tiver origens de identidade externas, ele poderá ser usado para o tipo de autorização.

Um conjunto de políticas típico é criado desta maneira:

1. Navegue até Política > Conjuntos de políticas > +.

2. Renomeie o Novo conjunto de políticas 1.

3. Defina a condição como exclusiva para este dispositivo.

4. Expanda o conjunto de políticas.

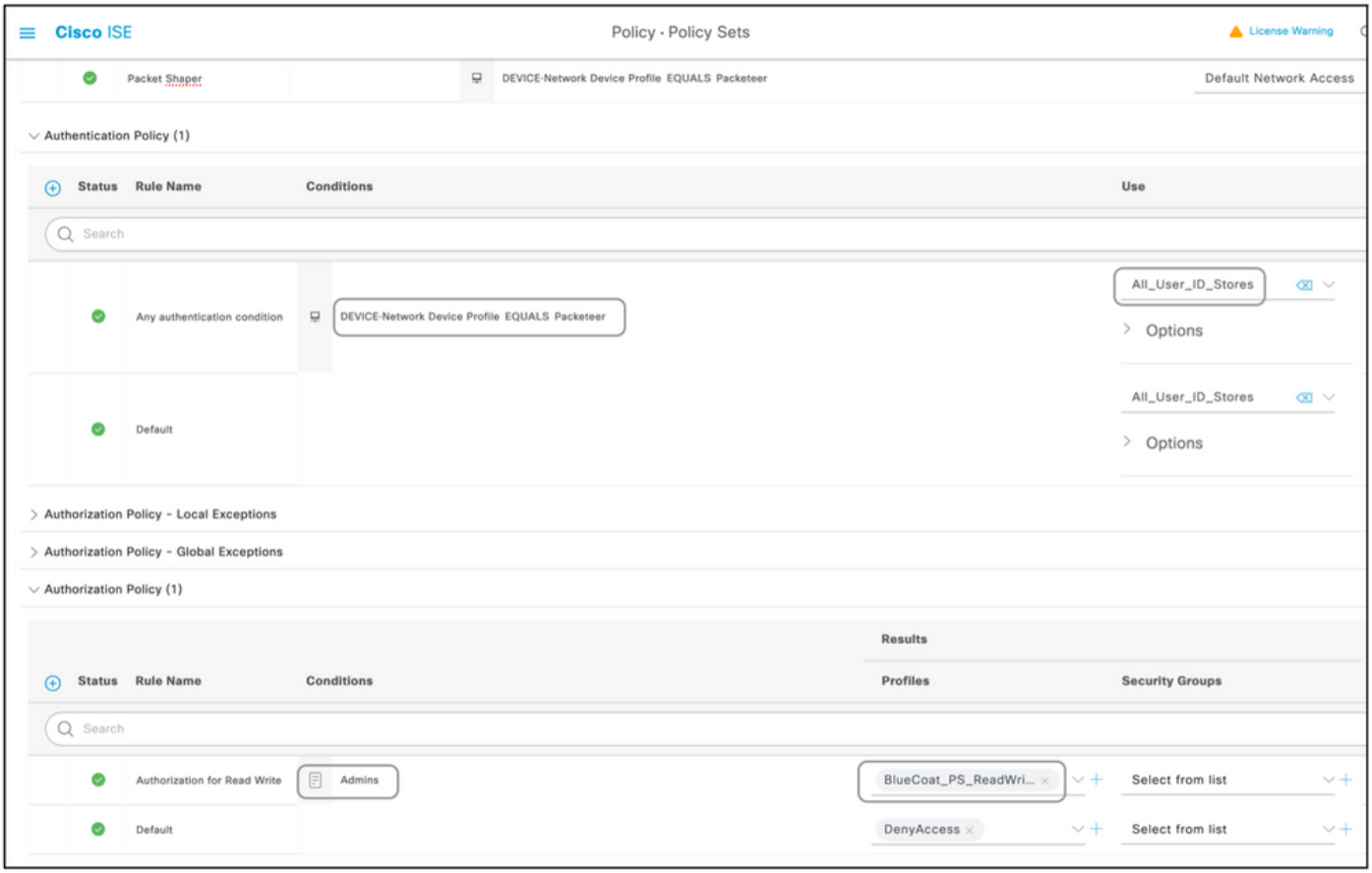
5. Expanda Authentication Policy para definir uma regra de autenticação. A origem externa ou os usuários internos são exemplos que podem ser usados como uma sequência de origem de identidade contra a qual o ISE verificaria o usuário.

6. A política de autenticação está definida. A política pode ser salva neste ponto.

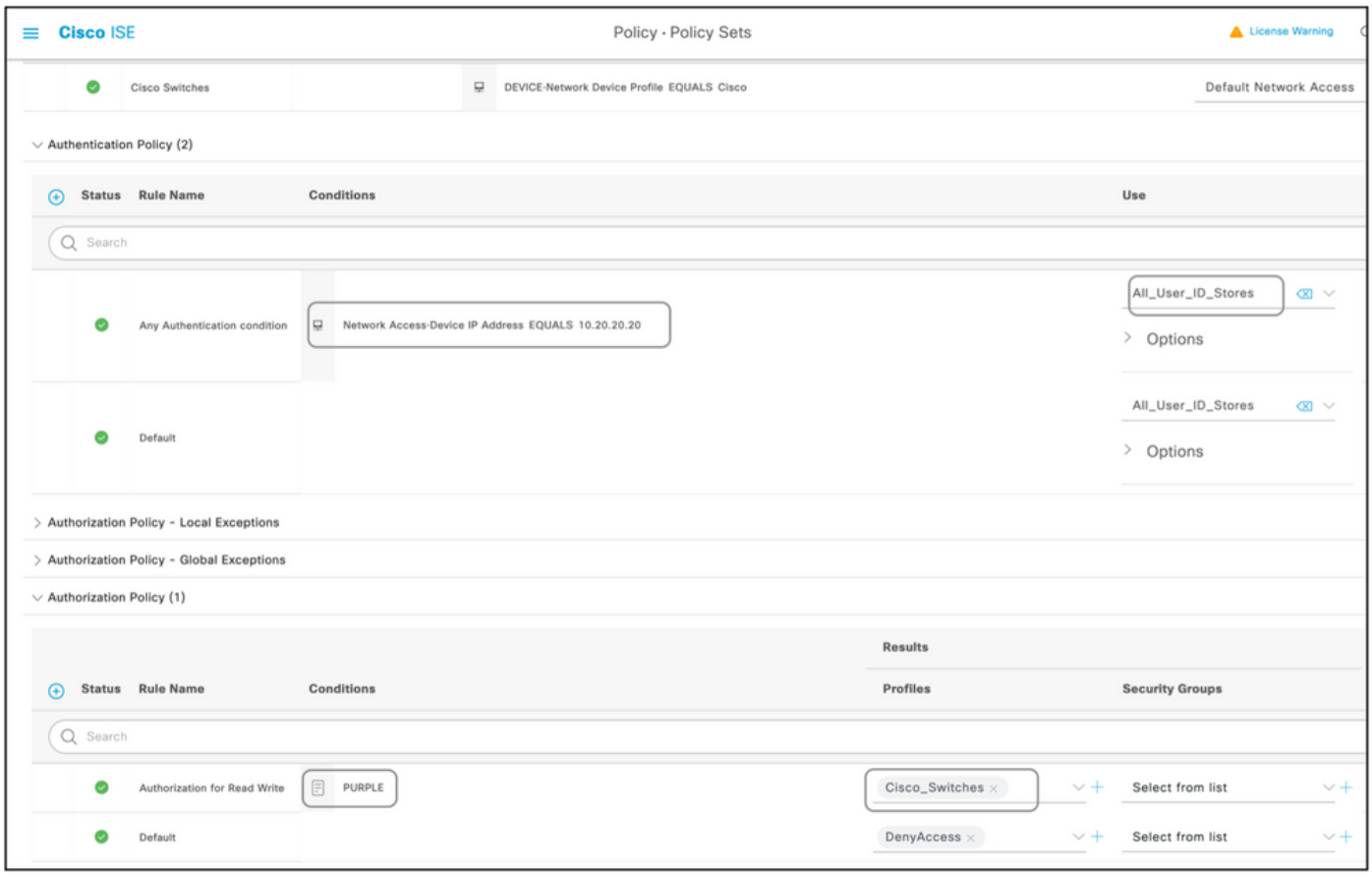
7. Expanda a Diretiva de Autorização para adicionar as condições de autorização para os usuários. Um exemplo é verificar um determinado grupo do AD ou grupo de identidade interno do ISE. Nomeie a regra da mesma forma.

8. O resultado da regra de autorização pode ser selecionado na lista suspensa.

9. Criar várias regras de autorização para diferentes tipos de acesso suportados pelo fornecedor.



Cisco ISE
Policy - Policy Sets
License Warning
Packet Shaper
DEVICE-Network Device Profile EQUALS Packeteer
Default Network Access
Authentication Policy (1)
Status
Rule Name
Conditions
Use
Search
Any authentication condition
DEVICE-Network Device Profile EQUALS Packeteer
All_User_ID_Stores
Options
Default
All_User_ID_Stores
Options
Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions
Authorization Policy (1)
Results
Status
Rule Name
Conditions
Profiles
Security Groups
Search
Authorization for Read Write
Admins
BlueCoat_PS_ReadWri...
Select from list
Default
DenyAccess
Select from list


Cisco ISE
Policy - Policy Sets
License Warning
Policy Sets
Reset
Reset Policyset Hitcounts
Save
Status
Policy Set Name
Description
Conditions
Allowed Protocols / Server Sequence
Hits
Actions
View
Search
Cisco Switches
DEVICE-Network Device Profile EQUALS Cisco
Default Network Access
0




# Lista de Dispositivos

Qualquer dispositivo que suporte a administração de dispositivos com Radius pode ser adicionado no ISE com algumas modificações em todas as etapas mencionadas na seção anterior. Portanto, este documento tem uma lista de dispositivos que funcionam com as informações fornecidas nesta seção. A lista de atributos e valores fornecida neste documento não é exaustiva nem autoritativa e pode ser alterada a qualquer momento sem uma atualização deste documento. Consulte os sites do fornecedor e o suporte do fornecedor para validação.

## Roteadores de serviços agregados (ASR)

Não é necessário criar dicionários e VSAs separados para isso, pois ele usa pares Cisco AV que já estão presentes no ISE.

Atributo(s): cisco-av-pair

Valor(es): shell:tasks="#<nome-da-função>,<permissão>:<processo>"

Uso: define os valores de <role-name>para o nome de uma função definida localmente no roteador. A hierarquia de funções pode ser descrita em termos de uma árvore, onde o role#rootis no topo da árvore e o role#leafadiciona comandos adicionais. Essas duas funções podem ser combinadas e passadas de volta se:shell:tasks="#root,#leaf".

As permissões também podem ser passadas de volta em uma base de processo individual, para que um usuário possa receber privilégios de leitura, gravação e execução para determinados

processos. Por exemplo, para conceder a um usuário privilégios de leitura e gravação para o processo BGP, defina o valor como:shell:tasks="#root,rw:bgp". A ordem dos atributos não importa; o resultado é o mesmo se o valor estiver definido como shell:tasks="#root,rw:bgp"ou toshell:tasks="rw:bgp,#root".

Exemplo: Adicione o Atributo a um Perfil de Autorização.

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-Cisco | Cisco-av-pair | Série | shell:tasks="#root,#leaf,rwx:bgp,r:ospf" |

## Switches Cisco IOS® e Cisco IOS® XE

Não é necessário criar dicionários e VSAs separados para isso, pois ele usa atributos RADIUS que já estão presentes no ISE.

Atributo(s):cisco-av-pair

Valor(es):shell:priv-lvl=<level>

Uso: define os valores de<nível>para os números que são basicamente o número de privilégios a serem enviados. Normalmente, se 15 é enviado, significa leitura-gravação, se 7 é enviado significa somente leitura.

Exemplo: Adicione o Atributo a um Perfil de Autorização.

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-Cisco | Cisco-av-pair | Série | shell:priv-lvl=15 |

## Formatador de Pacotes BlueCoat

Atributo(s):Packet-AVPair

Valor(es):access=<level>

Uso:<level>é o nível de acesso a ser concedido. O acesso de toque equivale a leitura-gravação, enquanto o acesso de aparência equivale a somente leitura.

Crie um dicionário conforme mostrado neste documento com estes valores:

- Nome: Packet
- ID do fornecedor: 2334
- Tamanho do campo Tamanho do fornecedor: 1
- Tamanho do campo Tipo de fornecedor: 1

Insira os detalhes do atributo:

- Atributo:Packet-AVPair
- Descrição: usado para especificar o nível de acesso
- ID do Atributo do Fornecedor: 1
- Direção: OUT
- Várias Permitidas: Falso
- Permitir marcação: desmarcada
- Tipo de Atributo: String

Exemplo: Adicione o Atributo a um Perfil de Autorização (para acesso somente leitura).

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-Packet | Pacote-AVPair | Série | access=look |

Exemplo: Adicione o Atributo a um Perfil de Autorização (para acesso leitura-gravação).

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-Packet | Pacote-AVPair | Série | access=touch |

## Servidor proxy BlueCoat (AV/SG)

Atributo(s): Blue-Coat-Authorization

Valor(es): <level>

Uso:<level>é o nível de acesso a ser concedido. 0 significa sem acesso, 1 significa acesso somente leitura, enquanto 2 significa acesso leitura-gravação. O atributo Blue-Coat-Authorization é o responsável pelo nível de acesso.

Crie um dicionário conforme mostrado neste documento com estes valores:

- Nome: BlueCoat
- ID do fornecedor: 14501
- Tamanho do campo Tamanho do fornecedor: 1
- Tamanho do campo Tipo de fornecedor: 1

Insira os detalhes do atributo:

- Atributo: Blue-Coat-Group
- ID do Atributo do Fornecedor: 1
- Direção: BOTH
- Várias Permitidas: Falso
- Permitir marcação: desmarcada
- Tipo de Atributo: Inteiro Não Assinado 32 (UINT32)

Insira os detalhes do segundo atributo:

- Atributo: Blue-Coat-Authorization

- Descrição: usado para especificar o nível de acesso
- ID do Atributo do Fornecedor: 2
- Direção: BOTH
- Várias Permitidas: Falso
- Permitir marcação: desmarcada
- Tipo de Atributo: Inteiro Não Assinado 32 (UINT32)

Exemplo: Adicione o Atributo a um Perfil de Autorização (sem acesso).

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-BlueCoat | Blue-Coat-Group | UINT32 | 0 |

Exemplo: Adicione o Atributo a um Perfil de Autorização (para acesso somente leitura).

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-BlueCoat | Blue-Coat-Group | UINT32 | 1 |

Exemplo: Adicione o Atributo a um Perfil de Autorização (para acesso leitura-gravação).

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-BlueCoat | Blue-Coat-Group | UINT32 | 2 |

## Switches Brocade

Não é necessário criar dicionários e VSAs separados para isso, pois ele usa atributos RADIUS que já estão presentes no ISE.

Atributo(s): Tunnel-Private-Group-ID

Valor(es):U:<VLAN1>; T:<VLAN2>

Uso:Defina<VLAN1>para o valor da VLAN de dados. Defina<VLAN2>para o valor da VLAN de voz. Neste exemplo, a VLAN de dados é a VLAN 10 e a VLAN de voz é a VLAN 21.

Exemplo: Adicione o Atributo a um Perfil de Autorização.

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-IETF | Tunnel-Private-Group-ID | Cadeia de Caracteres Marcada | U:10;T:21 |

## Infoblox

Atributo(s):Infoblox-Group-Info

Valor(es):<group-name>

Uso:<group-name>é o nome do grupo com os privilégios que o usuário recebe. Este grupo deve ser configurado no dispositivo Infoblox. Neste exemplo de configuração, o nome do grupo é Meu grupo.

Crie um dicionário conforme mostrado neste documento com estes valores:

- Nome: Infoblox
- ID do fornecedor: 7779
- Tamanho do campo Tamanho do fornecedor: 1
- Tamanho do campo Tipo de fornecedor: 1

Insira os detalhes do atributo:

- Atributo:Infoblox-Group-Info
- ID do Atributo do Fornecedor: 009
- Direção: OUT
- Várias Permitidas: Falso
- Permitir marcação: desmarcada
- Tipo de Atributo: String

Exemplo: Adicione o Atributo a um Perfil de Autorização.

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-Blox | Infoblox-Group-Info | Série | MeuGrupo |

## Cisco Firepower Management Center

Não é necessário criar dicionários e VSAs separados para isso, pois ele usa atributos RADIUS que já estão presentes no ISE.

Atributo(s):cisco-av-pair

Valor(es): Class-[25]=<função>

Uso: define os valores de <role>para os nomes das funções localmente definidas no FMC. Crie várias funções, como administrador e usuário somente leitura no FMC e atribua os valores aos atributos no ISE a serem recebidos pelo FMC da mesma forma.

Exemplo: Adicione o Atributo a um Perfil de Autorização.

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-Cisco | Cisco-av-pair | Série | Classe-[25]=NetAdmins |

## Switches Nexus

Não é necessário criar dicionários e VSAs separados para isso, pois ele usa atributos RADIUS que já estão presentes no ISE.

Atributo(s):cisco-av-pair

Valor(es):shell:roles="<função1> <função2>"

Uso: define os valores de<role1>e<role2>para os nomes das funções localmente definidas no switch. Quando várias funções forem criadas, separe-as com um caractere de espaço. Quando várias funções são passadas de volta do servidor AAA para o switch Nexus, o resultado é que o usuário tem acesso aos comandos definidos pela união das três funções.

As funções internas são definidas emConfigurar contas de usuário e RBAC.

Exemplo: Adicione o Atributo a um Perfil de Autorização.

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-Cisco | Cisco-av-pair | Série | shell:roles="rede-admin vdc-admin operador-vdc" |

## Controlador de LAN sem fio (WLC)

Não é necessário criar dicionários e VSAs separados para isso, pois ele usa atributos RADIUS que já estão presentes no ISE.

Atributo(s):Service-Type

Valor(es):Administrativo (6) / Prompt NAS (7)

Uso: Para conceder ao usuário acesso de leitura/gravação à controladora Wireless LAN (WLC), o valor deve ser Administrative; para acesso somente leitura, o valor deve ser NAS-Prompt.

Para obter detalhes, consulte Exemplo de Configuração de Autenticação de Servidor RADIUS de Usuários de Gerenciamento em Controladoras Wireless LAN (WLC)

Exemplo: Adicione o Atributo a um Perfil de Autorização (para acesso somente leitura).

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-IETF | Tipo de serviço | Enumeração | Prompt do NAS |

Exemplo: Adicione o Atributo a um Perfil de Autorização (para acesso leitura-gravação).

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-IETF | Tipo de serviço | Enumeração | Administrativo |

## Gerenciador de rede do data center (DCNM)

O DCNM deve ser reiniciado após a alteração do método de autenticação. Caso contrário, ele pode atribuir privilégio de operador de rede em vez de administrador de rede.

Não é necessário criar dicionários e VSAs separados para isso, pois ele usa atributos RADIUS que já estão presentes no ISE.

Atributo(s):cisco-av-pair

Valor(es):shell:roles=<função>

| Função DCNM | RADIUS Cisco-AV-Pair |
|---|---|
| Usuário | shell:funções = "operador de rede" |
| Administrador | shell:funções = "administrador de rede" |

## Códigode áudio

Atributo(s): ACL-Auth-Level

Valor(es): ACL-Auth-Level = "<inteiro>"

Uso:<integer>é o nível de acesso a ser concedido. Um valor do atributo ACL-Auth-Level com o nome ACL-Auth-UserLevel de 50 para o usuário, um valor do atributo ACL-Auth-Level com o nome ACL-Auth-AdminLevel de valor 100 para admin e valor de ACL-Auth-Level com o nome ACL-Auth-SecurityAdminLevel de valor 200 para security admin. Os nomes podem ser ignorados e os valores dos atributos podem ser fornecidos diretamente como valor para o par AV avançado do perfil de autorização.

Crie um dicionário conforme mostrado neste documento com estes valores:

- Nome: AudioCodes
- ID do fornecedor: 5003
- Tamanho do campo Tamanho do fornecedor: 1
- Tamanho do campo Tipo de fornecedor: 1

Insira os detalhes do atributo:

- Atributo: ACL-Auth-Level
- Descrição: usado para especificar o nível de acesso
- ID do atributo do fornecedor: 35
- Direção: OUT
- Várias Permitidas: Falso
- Permitir marcação: desmarcada
- Tipo de Atributo: Inteiro

Exemplo: Adicione o Atributo a um Perfil de Autorização (para usuário).

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-Códigos de áudio | ACL-Auth-Level | Número inteiro | 50 |

Exemplo: adicione o atributo a um perfil de autorização (para admin).

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-Códigos de áudio | ACL-Auth-Level | Número inteiro | 100 |

Exemplo: adicione o atributo a um perfil de autorização (para admin de segurança).

| Tipo de dicionário | Atributo RADIUS | Tipo de Atributo | Valor do Atributo |
|---|---|---|---|
| RADIUS-Códigos de áudio | ACL-Auth-Level | Número inteiro | 200 |

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.