

Configurar a Autenticação Externa no Catalyst Center usando o Windows Server

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Política de Função do Administrador](#)

[Política de Função de Observador.](#)

[Habilitar autenticação externa](#)

[Verificar](#)

Introdução

Este documento descreve como configurar a Autenticação Externa no Cisco DNA Center usando o Servidor de Políticas de Rede (NPS) no Windows Server como RADIUS.

Pré-requisitos

Requisitos

Conhecimento básico sobre:

- Usuários e funções do Cisco DNA Center
- Servidor de Diretivas de Rede, RADIUS e Active Directory do Windows Server

Componentes Utilizados

- Cisco DNA Center 2.3.5.x
- Microsoft Windows Server Versão 2019 atuando como Controlador de Domínio, Servidor DNS, NPS e Active Directory

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.



Observação: o Cisco Technical Assistance Center (TAC) não fornece suporte técnico ao Microsoft Windows Server. Se você tiver problemas com a configuração do Microsoft Windows Server, entre em contato com o Suporte da Microsoft para obter assistência técnica.

Configurar

Política de Função do Administrador

1. Clique no menu Iniciar do Windows e procure NPS. Em seguida, selecione Servidor de Diretivas de Rede:

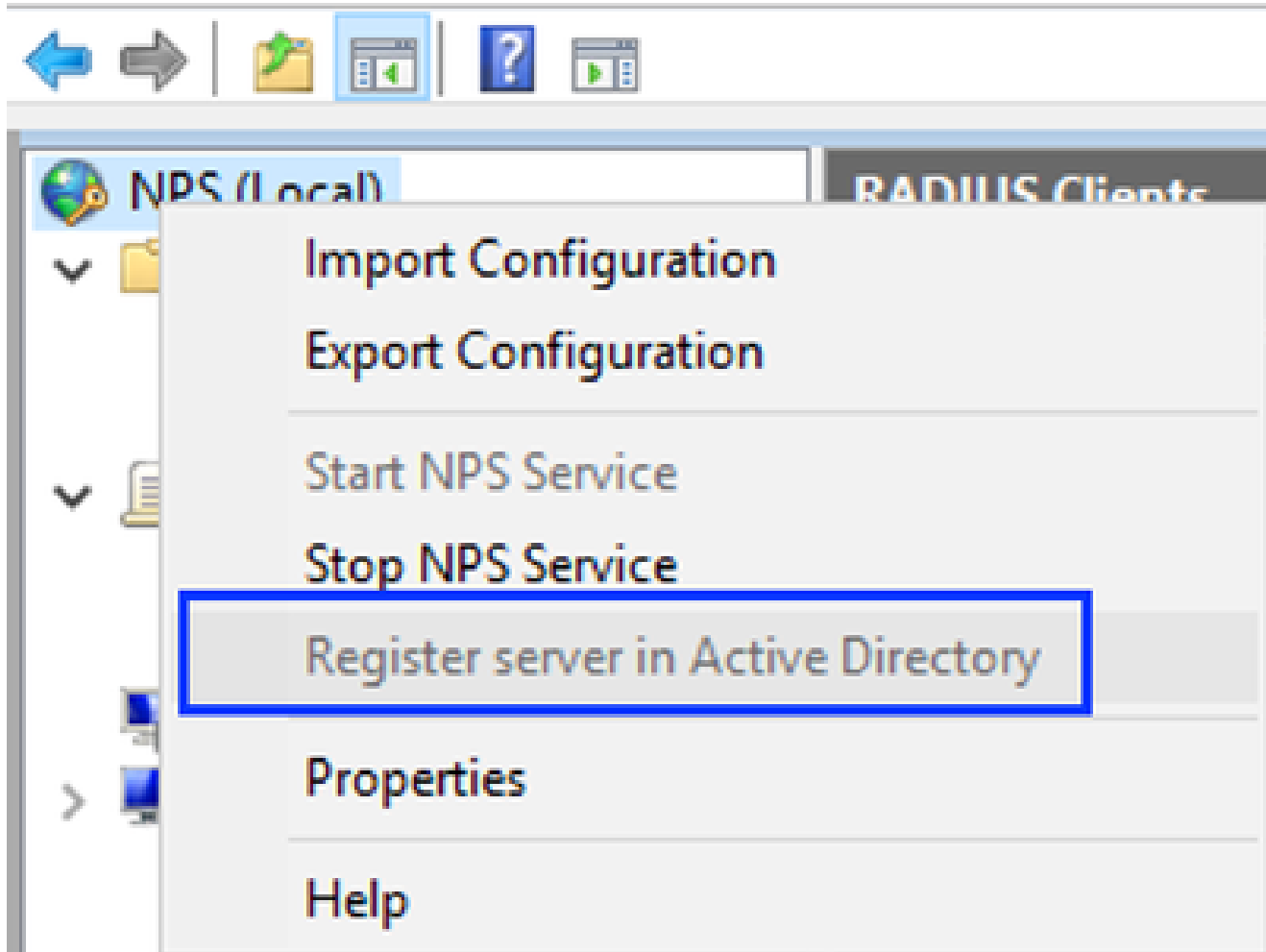


Network Policy Server

Desktop app

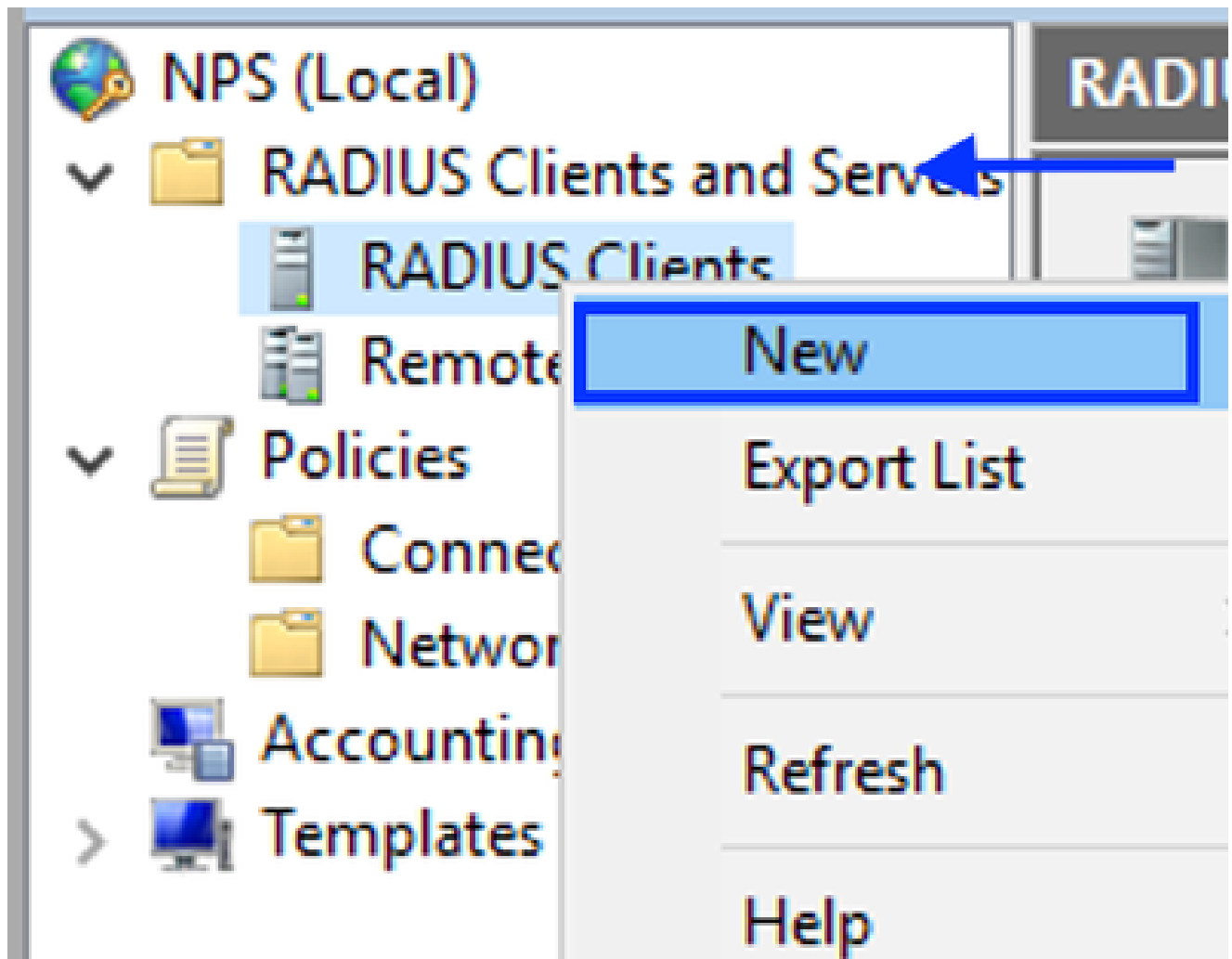
Network Policy Server

File Action View Help



Serviço de Política de Rede do Windows

3. Clique duas vezes em OK.
4. Expanda Clientes e servidores RADIUS, clique com o botão direito do mouse em Clientes RADIUS e selecione Novo:



Adicionar cliente RADIUS

5. Insira o Nome amigável, o endereço IP de gerenciamento do Cisco DNA Center e um segredo compartilhado (isso pode ser usado posteriormente):

DNAC Properties X

Settings **Advanced**

Enable this RADIUS client

Select an existing template:

Name and Address

Friendly name:
DNAC

Address (IP or DNS):
10.88.244.160 Verify...

Shared Secret

Select an existing Shared Secrets template:
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual Generate

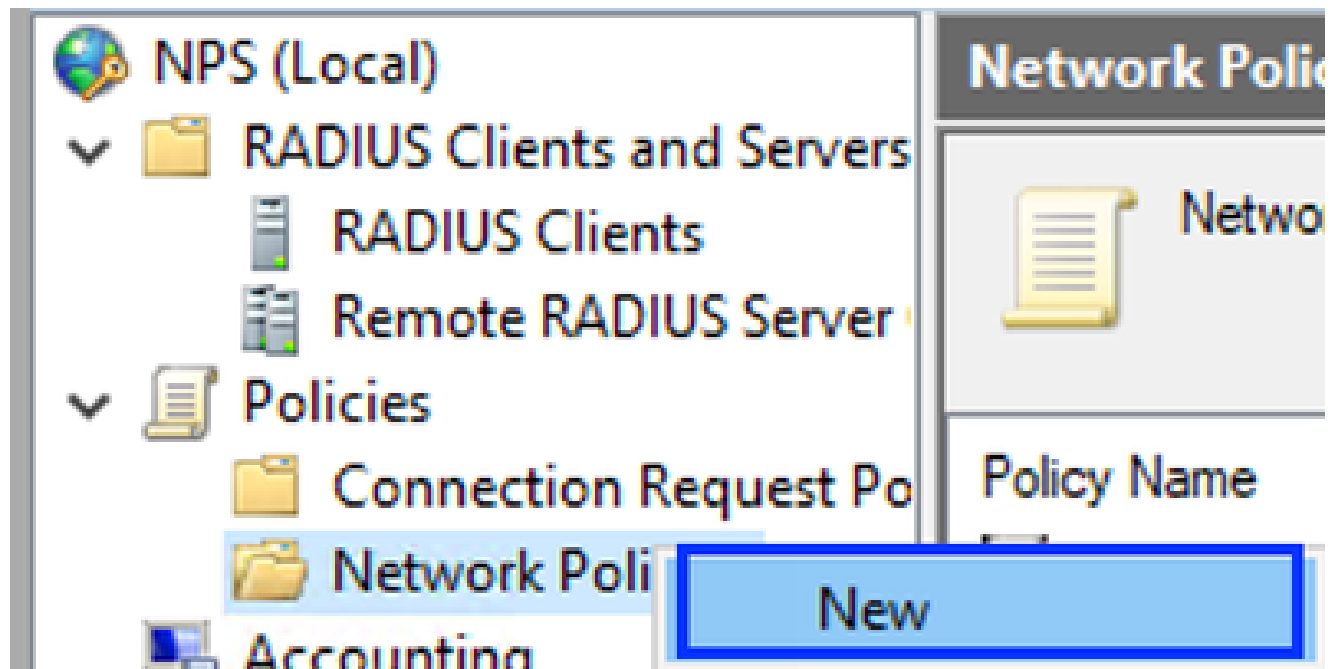
Shared secret:
●●●●●●●●

Confirm shared secret:
●●●●●●●●

OK Cancel Apply

Configuração do cliente Radius

6. Clique em OK para salvá-lo.
7. Expanda Políticas, clique com o botão direito do mouse em Network Policies e selecione New:



Adicionar Nova Diretiva de Rede

8. Insira um nome de política para a regra e clique em Avançar:



Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

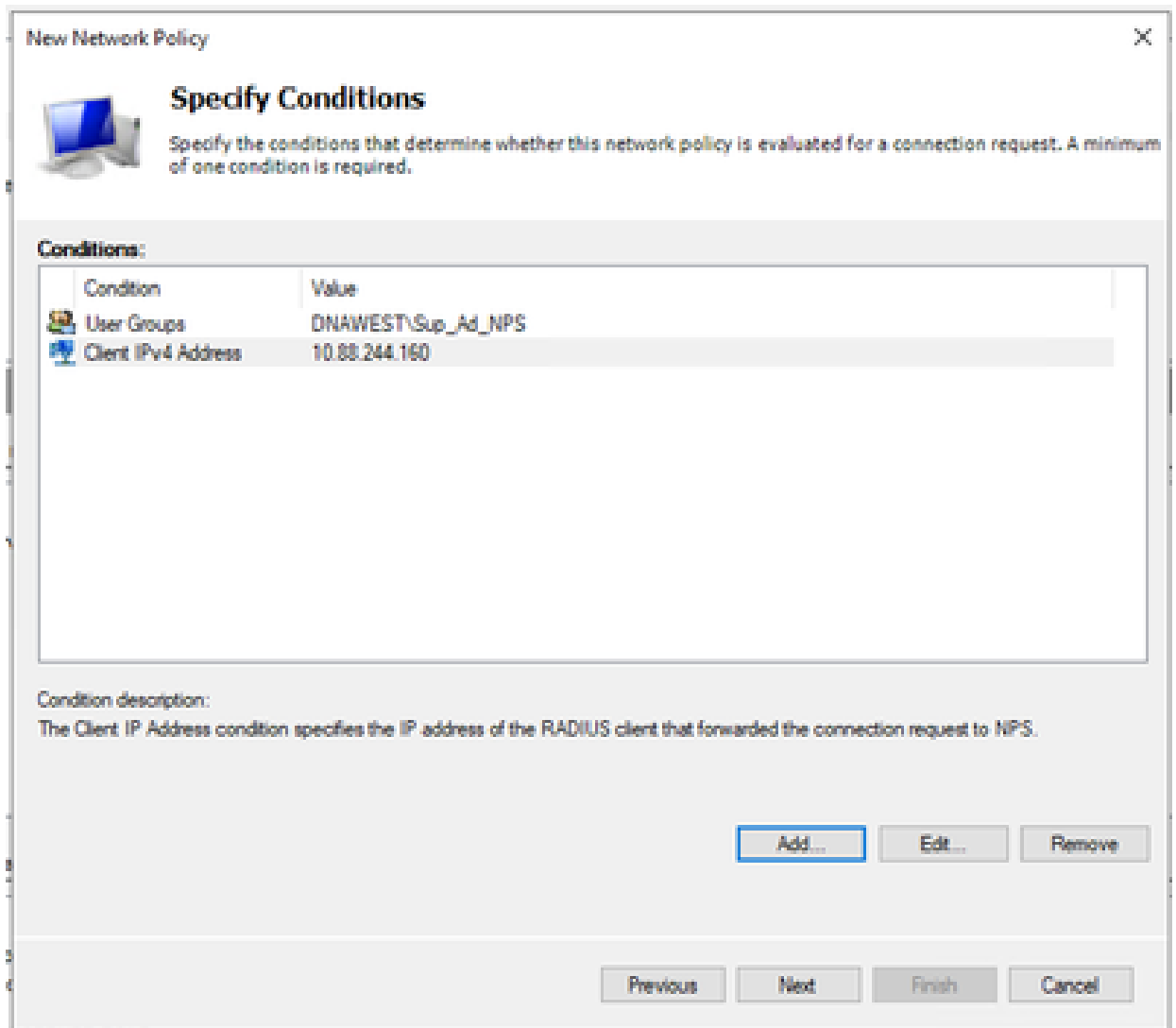
Type of network access server:

Vendor specific:

Nome da política

9. Para permitir um grupo de domínio específico, adicione estas duas condições e clique em Avançar:


- Grupo de usuários - Adicione seu grupo de domínio que pode ter uma função de administrador no Cisco DNA Center (para este exemplo, o grupo Sup_Ad_NPS é usado).
- ClientIPv4Address - Adicione seu endereço IP de gerenciamento do Cisco DNA Center.



Condições da política

10. Selecione Acesso concedido e clique em Avançar:

New Network Policy ✕



Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

Access granted
Grant access if client connection attempts match the conditions of this policy.

Access denied
Deny access if client connection attempts match the conditions of this policy.

Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

Usar Acesso Concedido

11. Selecione Somente Autenticação sem criptografia (PAP, SPAP):



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up

Move Down

Add...

Edit...

Remove

Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
 - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method.

Previous

Next

Finish

Cancel

Selecione Autenticação não criptografada

12. Selecione Avançar já que os valores padrão são usados:



Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.

If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints

- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

Disconnect after the maximum idle time

1

Previous

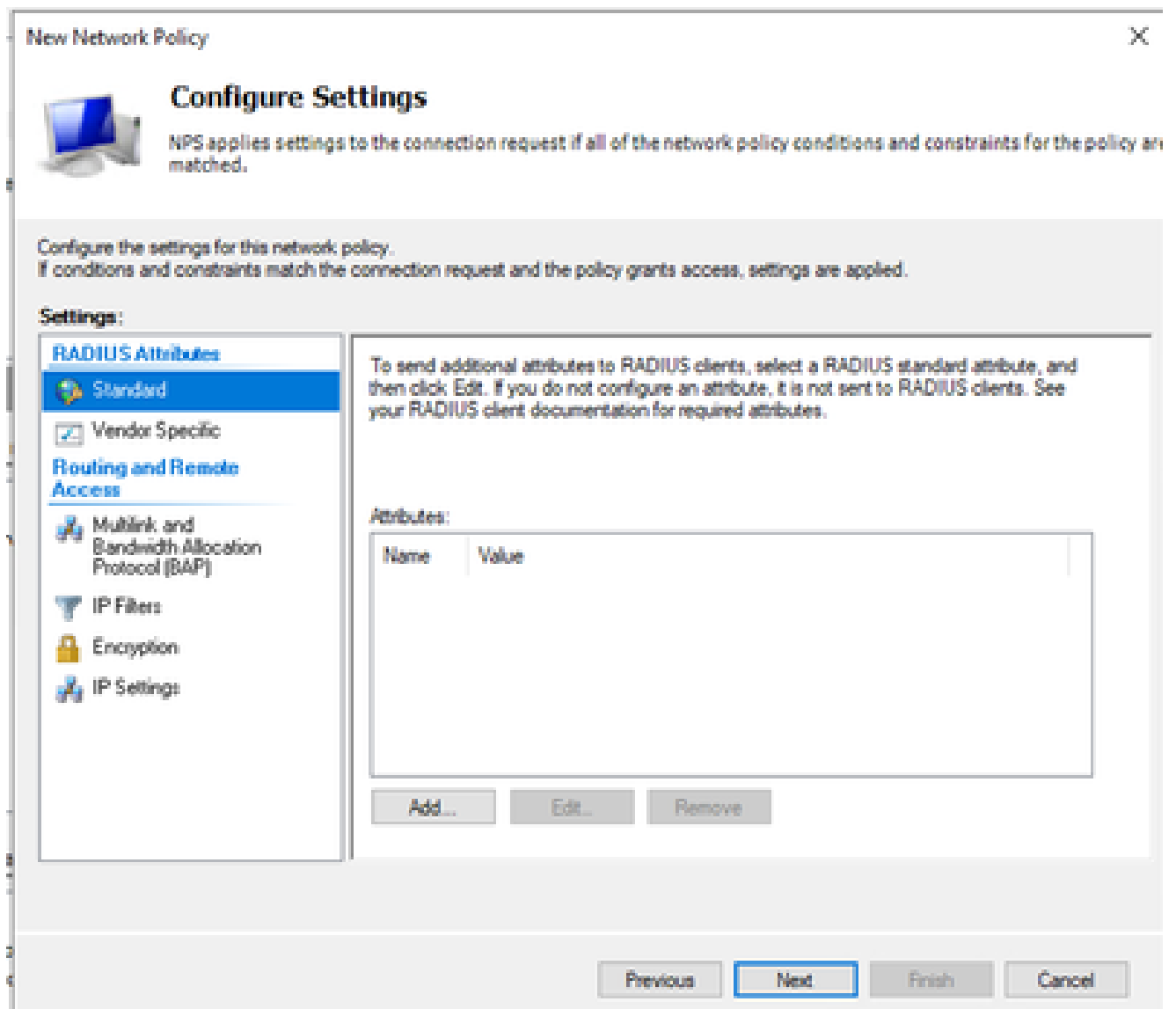
Next

Finish

Cancel

Janela Configurar Restrição

13. Remover atributos padrão:



Definir atributos a serem usados

14. Em Atributos RADIUS, selecione Específico do fornecedor e, em seguida, clique em Adicionar, selecione Cisco como um fornecedor e clique em Adicionar:

Add Vendor Specific Attribute



To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor:

Disco

Attributes:

| Name | Vendor |
|---------------|--------|
| Cisco-AV-Pair | Cisco |

Description:

Specifies the Cisco AV Pair VSA.

Add...

Close

Adicionar par AV da Cisco

15. Clique em Add, escreva Role=SUPER-ADMIN-ROLE e clique em OK duas vezes:



Configure Settings

NPS applies settings to the connection request if **all** of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.

If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

Standard

Vendor Specific

Routing and Remote Access

Multilink and Bandwidth Allocation Protocol (BAP)

IP Filters

Encryption

IP Settings

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

| Name | Vendor | Value |
|---------------|--------|-----------------------|
| Cisco-AV-Pair | Cisco | Role=SUPER-ADMIN-ROLE |

Add...

Edit...

Remove

Previous

Next

Finish

Cancel

Atributo Cisco AV-Pair adicionado

16. Selecione Close e, em seguida, Next.

17. Revise suas configurações de política e selecione Concluir para salvá-las.



Completing New Network Policy

You have successfully created the following network policy:

DNAC-Admin-Policy

Policy conditions:

| Condition | Value |
|---------------------|--------------------|
| User Groups | DNAWEST\Sup_Ad_NPS |
| Client IPv4 Address | 10.88.244.160 |

Policy settings:

| Condition | Value |
|--------------------------------|----------------------------------|
| Authentication Method | Encryption authentication (CHAP) |
| Access Permission | Grant Access |
| Ignore User Dial-In Properties | False |
| Cisco-AV-Pair | Role=SUPER-ADMIN-ROLE |

To close this wizard, click Finish.

Previous

Next

Finish

Cancel

Resumo da política

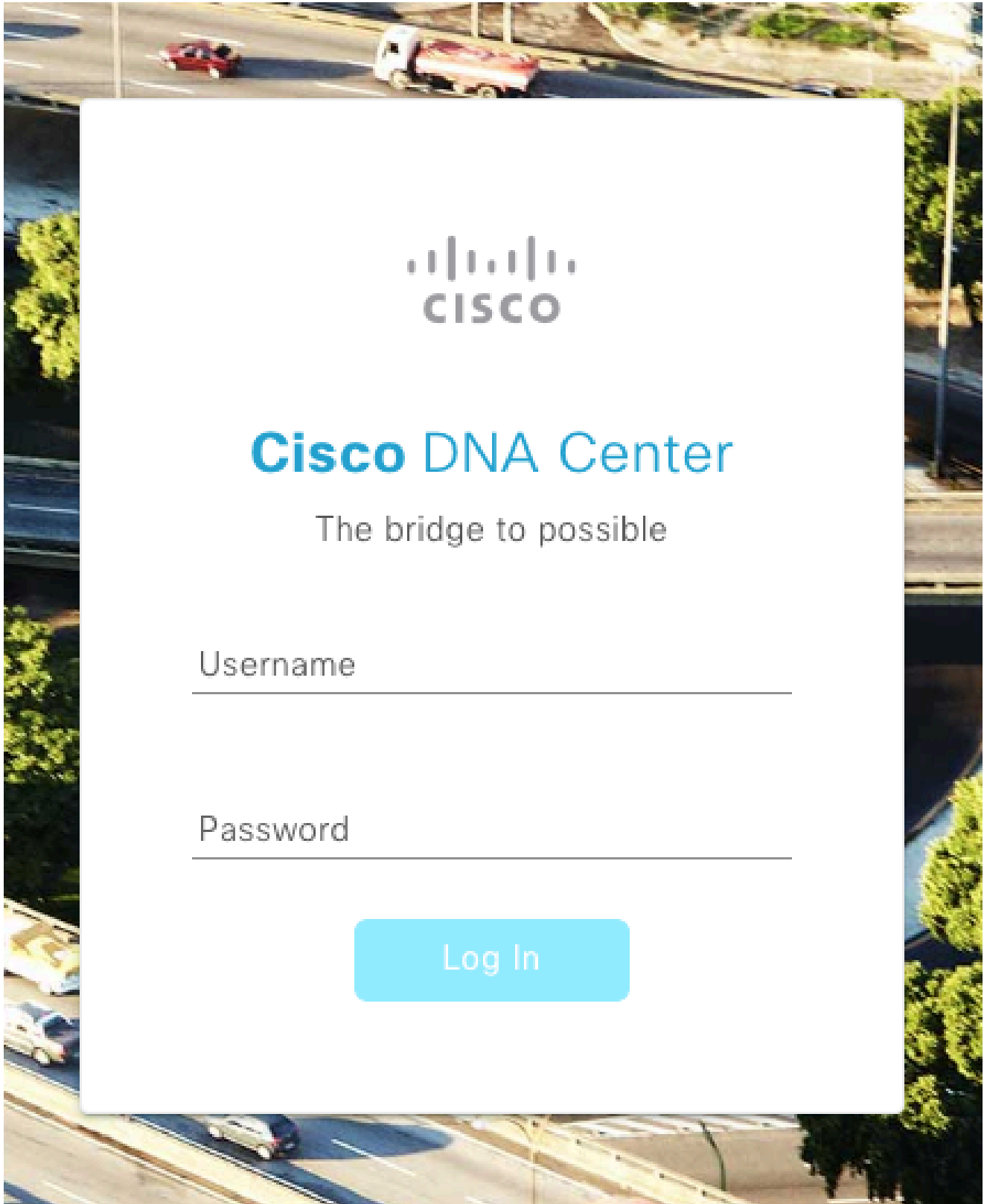
Política de Função de Observador.

1. Clique no menu Iniciar do Windows e procure NPS. Em seguida, selecione Network Policy Server.
2. No painel de navegação à esquerda, clique com o botão direito do mouse na opção NPS (Local) e selecione Register server in Active Directory.
3. Clique duas vezes em OK.
4. Expanda Clientes e servidores RADIUS, clique com o botão direito do mouse em Clientes RADIUS e selecione Novo.
5. Insira um Nome amigável, o endereço IP de gerenciamento do Cisco DNA Center e um segredo compartilhado (isso pode ser usado posteriormente).
6. Clique em OK para salvá-lo.

7. Expanda Policies, clique com o botão direito do mouse em Network Policies e selecione New.
8. Insira um nome de política para a regra e clique em Avançar.
9. Para permitir um grupo de domínio específico, você precisa adicionar essas duas condições e selecionar Próximo.
 - Grupo de usuários - Adicione seu grupo de domínio para atribuir uma função de observador no Cisco DNA Center (neste exemplo, o grupo Observer_NPS é usado).
 - ClientIPv4Address - Adicione seu IP de gerenciamento do Cisco DNA Center.
10. Selecione Acesso concedido e, em seguida, Próximo.
11. Selecione Somente Autenticação não criptografada (PAP, SPAP).
12. Selecione Avançar já que os valores padrão são usados.
13. Remova os atributos Standard.
14. Em RADIUS Attributes, selecione Vendor Specific e, em seguida, clique em Add, selecione Cisco como um fornecedor e clique em Add.
15. Selecione Add, write ROLE=OBSERVER-ROLE e OK duas vezes.
16. Selecione Fechar e Avançar.
17. Revise suas configurações de política e selecione Concluir para salvá-las.

Habilitar autenticação externa

1. Abra a interface gráfica do usuário (GUI) do Cisco DNA Center em um navegador da Web e faça login usando uma conta privilegiada de administrador:



Página de login do Cisco DNA Center

2. Navegue até Menu > Sistema > Configuração > Servidores de autenticação e política e selecione Adicionar > AAA:

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[+ Add ^](#) [↑ Export](#)

| AAA | Protocol |
|-----|------------------------|
| ISE | 4.189 RADIUS_TACACS |

Adicionar Windows Server

3. Digite o endereço IP do Windows Server e o segredo compartilhado usados nas etapas anteriores e clique em Salvar:

Add AAA server



Server IP Address*

10.88.244.148

Shared Secret*

.....|

[SHOW](#)



Advanced Settings

Cancel

Save

4. Valide se o status do Windows Server é Ativo:

10.88.244.148

RADIUS

AAA

ACTIVE



Resumo do Windows Server

5. Navegue até Menu > Sistema > Usuários e funções > Autenticação externa e selecione seu servidor AAA:

▼ AAA Server(s)

Primary AAA Server

IP Address

10.88.244.148

Shared Secret

[Info](#)

[View Advanced Settings](#)

Update

Windows Server como servidor AAA

6. Digite Cisco-AVPair como o atributo AAA e clique em Update:

▼ AAA Attribute

AAA Attribute

Cisco-AVPair

Reset to Default

Update

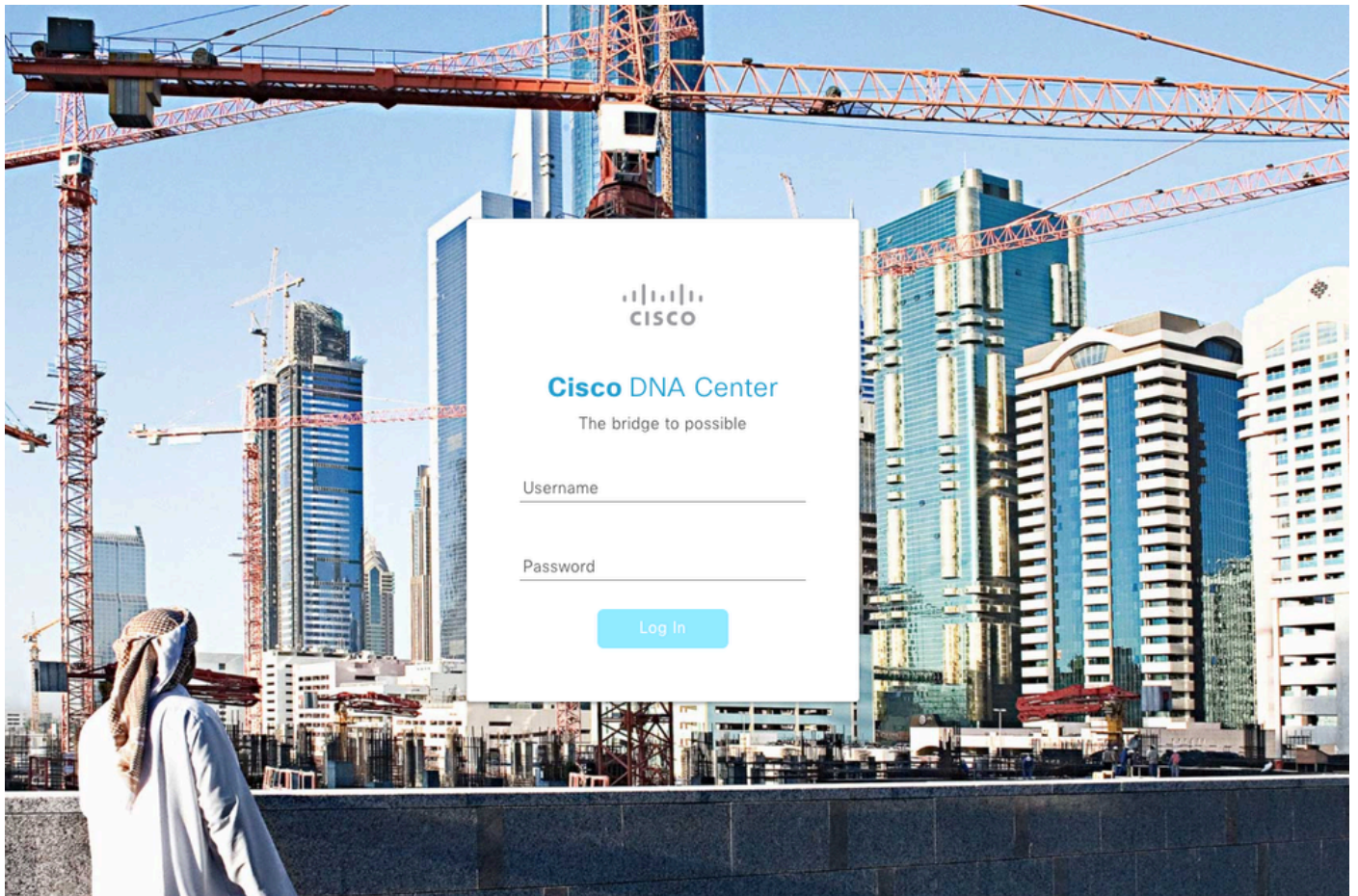
Par AV em usuário externo

7. Clique na caixa de seleção Enable External User para habilitar a Autenticação externa:

Enable External User 

Verificar

Você pode abrir a Interface gráfica do usuário (GUI) do Cisco DNA Center em um navegador da Web e fazer logon com um usuário externo configurado no Windows Server para confirmar que é possível fazer logon com êxito usando a autenticação externa.



Página de login do Cisco DNA Center

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.