

# Configuração RADIUS com switches gerenciados Cisco 200/300 Series e Windows Server 2008

## Objetivo

O Serviço de Usuário de Discagem de Autorização Remota (RADIUS - Remote Authorization Dial-in User Service) oferece uma forma robusta de autenticação de usuários para permitir acesso a um serviço de rede. Portanto, os servidores RADIUS oferecem um controle de acesso centralizado, em que o administrador do servidor decide se um segmento específico é autenticado ou não usando o RADIUS. Este artigo explica as etapas gerais para estabelecer o RADIUS em um ambiente cliente/servidor, onde o cliente é representado pelo Switch gerenciado Cisco 200/300 Series e o servidor está executando um Windows Server 2008 com RADIUS habilitado.

## Dispositivos aplicáveis

- Switches gerenciados Cisco 200/300 Series

## Procedimento Passo a Passo

A configuração ocorre em duas partes. Primeiro temos que definir o switch como um cliente RADIUS, depois temos que definir o servidor adequadamente para RADIUS.

## Definindo RADIUS no switch

Etapa 1. No utilitário de configuração SG200/300 Series, escolha **Security > RADIUS**. A página *RADIUS* é aberta:

**RADIUS**

**Use Default Parameters**

IP Version:  Version 6  Version 4

Retries:  (Range: 1 - 10, Default: 3)

Timeout for Reply:  sec. (Range: 1 - 30, Default: 3)

Dead Time:  min. (Range: 0 - 2000, Default: 0)

Key String:  (0/128 ASCII Alphanumeric Characters Used)

**RADIUS Table**

<input type="checkbox"/>	Server	Priority	Key String	Timeout for Reply	Authentication Port	Retries	Dead Time	Usage Type
0 results found.								

Etapa 2. Insira as configurações de RADIUS padrão.

- Versão IP – Exibe a versão IP suportada.
- Repetições – Neste campo, informe o número de solicitações transmitidas que são enviadas ao servidor RADIUS antes de ocorrer uma falha.
- Tempo limite para resposta – Neste campo, insira o tempo, em segundos, que o switch espera por uma resposta do servidor RADIUS antes de tentar uma consulta novamente.
- Tempo inativo – Neste campo, insira o tempo em minutos que o switch espera antes de ignorar o servidor RADIUS.
- Key String – Neste campo, insira a string padrão usada para autenticação e criptografia entre o switch e o servidor RADIUS. A chave deve corresponder àquela configurada no servidor RADIUS.

Etapa 3. Clique em **Apply** para atualizar a configuração atual do switch com as configurações de RADIUS.



Etapa 4. Você precisa adicionar o servidor RADIUS ao switch. Clique em Add. A página *Adicionar servidor RADIUS* é aberta em uma nova janela:

A imagem mostra uma janela de configuração para adicionar um servidor RADIUS. O formulário contém os seguintes campos e opções:

- Server Definition:  By IP address  By name
- IP Version:  Version 6  Version 4
- IPv6 Address Type: Global
- Server IP Address/Name:
- Priority:  (Range: 0 - 65535)
- Key String:  Use Default  User Defined  (0/128 ASCII Alphanumeric Characters Used)
- Timeout for Reply:  Use Default  User Defined  sec. (Range: 1 - 30, Default: 3)
- Authentication Port:  (Range: 0 - 65535, Default: 1812)
- Retries:  Use Default  User Defined  (Range: 1 - 10, Default: 3)
- Dead Time:  Use Default  User Defined  min. (Range: 0 - 2000, Default: 0)
- Usage Type:  Login  802.1x  All

Na base da janela, há dois botões: 'Apply' e 'Close'.

Etapa 5. Insira os valores nos campos do servidor. Se quiser usar os valores padrão, selecione **Usar padrão** no campo desejado.

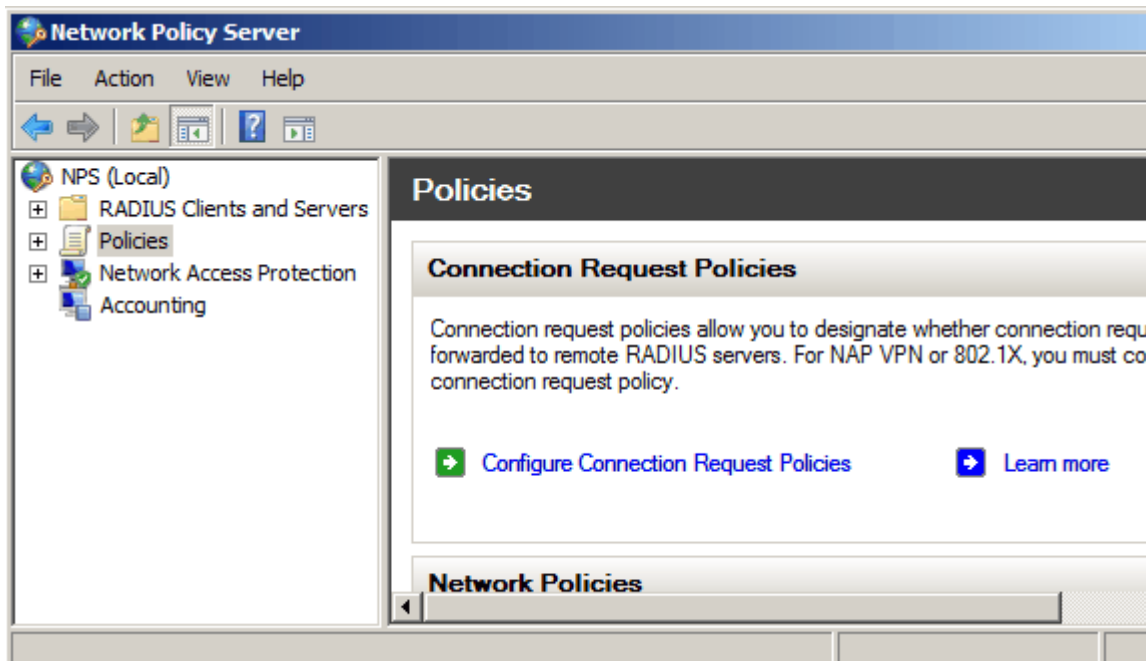
- Definição do servidor – Neste campo, você especifica como se conectar ao servidor, por endereço IP ou pelo nome do servidor.
- Versão do IP – Se o servidor for identificado pelo endereço IP, selecione o endereço IPv4 ou IPv6.

- Tipo de endereço IPv6 – Este campo exibe o tipo Global do endereço IPv6.
- Server IP Address/Name (Endereço IP/Nome do servidor) – nesse campo, insira o endereço IP ou o nome de domínio do servidor RADIUS.
- Prioridade – Nesse campo, insira a prioridade do servidor. Se mais de um servidor estiver configurado, o switch tentará se conectar a cada servidor de acordo com esse valor de prioridade.
- Key String – Neste campo, insira a string padrão usada para autenticação e criptografia entre o switch e o servidor RADIUS. A chave deve corresponder àquela configurada no servidor RADIUS.
- Tempo limite para resposta – Neste campo, insira o tempo, em segundos, que o switch espera por uma resposta do servidor RADIUS antes de tentar uma consulta novamente.
- Porta de autenticação – Nesse campo, insira o número da porta UDP definido para o servidor RADIUS para solicitações de autenticação.
- Repetições – Neste campo, informe o número de solicitações transmitidas que são enviadas ao servidor RADIUS antes de ocorrer uma falha.
- Tempo inativo – Neste campo, insira o tempo em minutos que o switch espera antes de ignorar o servidor RADIUS.
- Tipo de uso – Neste campo, insira o tipo de autenticação do servidor RADIUS. Há três opções:
  - Login – O servidor RADIUS autentica os usuários que desejam administrar o switch.
  - 802.1X – O servidor RADIUS é usado para a autenticação 802.1X.
  - Todos – O servidor RADIUS é usado para as autenticações Login e 802.1X.

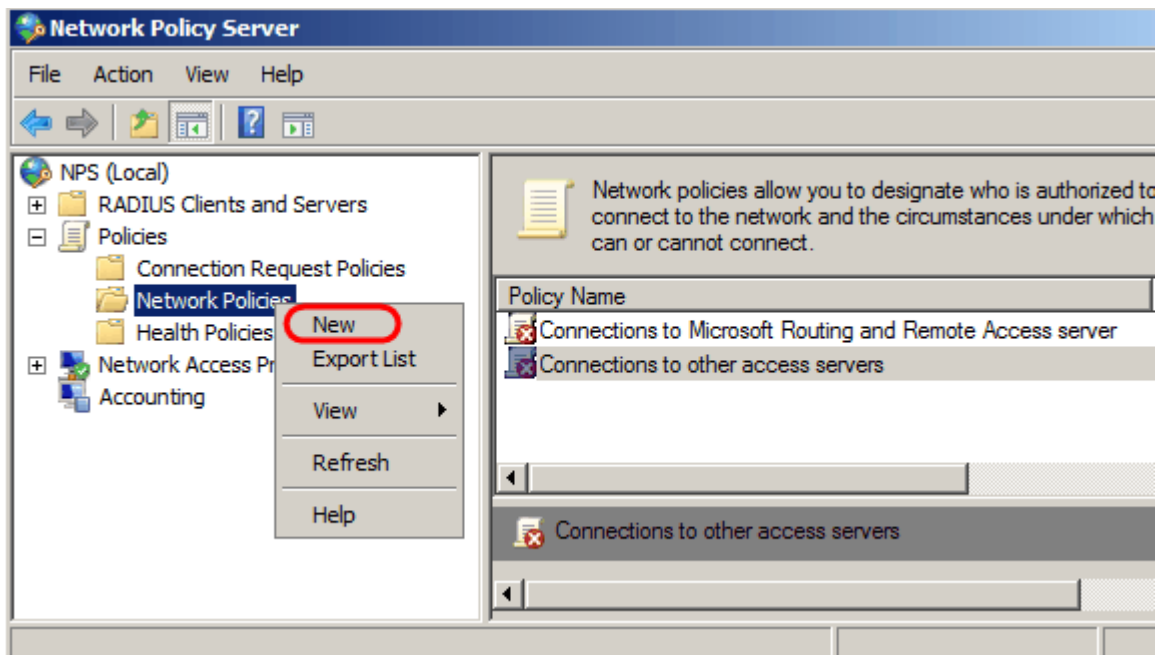
Etapa 6. Clique em **Apply** para adicionar a definição do servidor à configuração atual do switch.

## Configurando o Windows Server 2008 para RADIUS

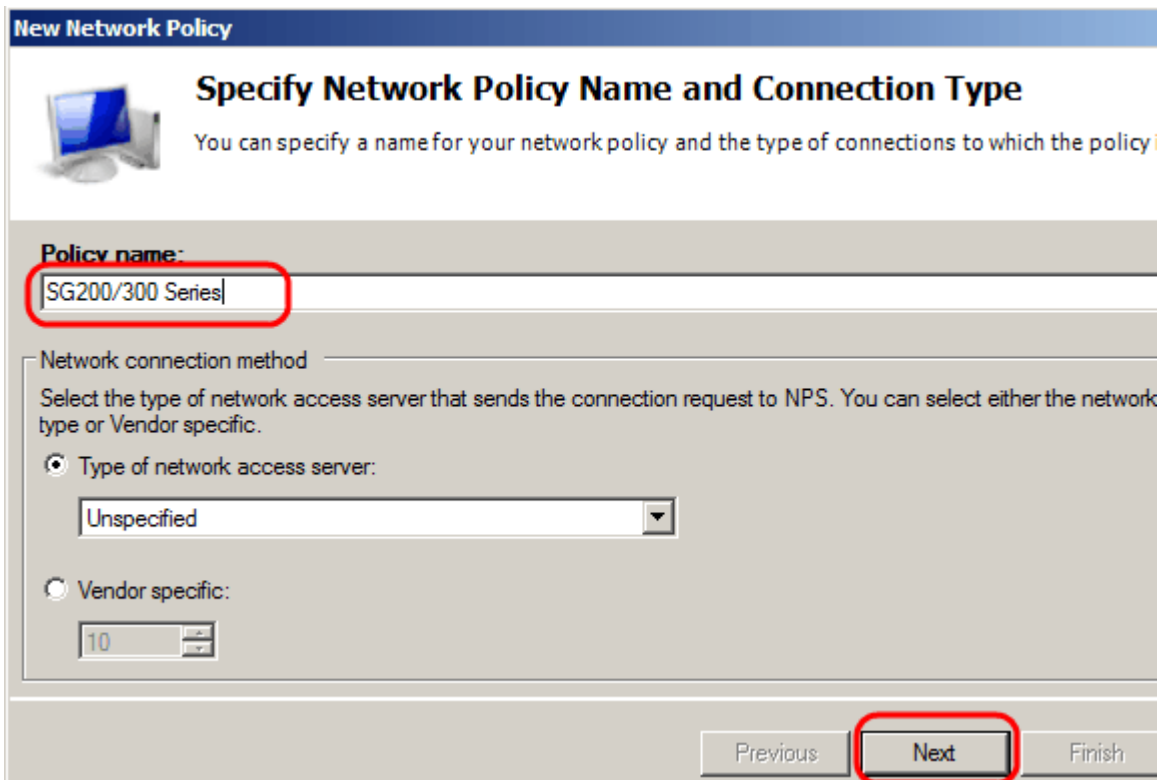
Etapa 1. Na máquina Windows Server 2008, escolha **Start > Administrative tools > Network Policy Server**. A janela *Servidor de Políticas de Rede* é aberta:



Etapa 2. Para ativar o servidor RADIUS para um segmento específico da rede, você precisa criar uma nova política de rede. Para criar uma nova diretiva de rede, escolha **Policies > Network Policy**, clique com o botão direito do mouse e selecione **New**. A janela *Nova Diretiva de Rede* é aberta:



Etapa 3. No campo Policy Name (Nome da política), insira o nome da nova política. Clique em Next.



Etapa 4. Você precisa especificar as condições desta política. Há duas condições necessárias: a que segmento de usuários o servidor RADIUS será implementado e o método usado para conectar a esse segmento. Clique em **Adicionar** para adicionar essas condições.

## New Network Policy



### Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection of one condition is required.

**Conditions:**

Condition	Value
-----------	-------

Condition description:

Etapa 5. Em Grupos, há três opções: Grupos do Windows, Grupos de máquinas e Grupos de usuários. escolha o grupo de acordo com a configuração da rede e clique em **Adicionar**. Uma nova janela é aberta de acordo com o grupo selecionado. Clique em **Add Groups**.

**Select condition**

Select a condition, and then click Add.

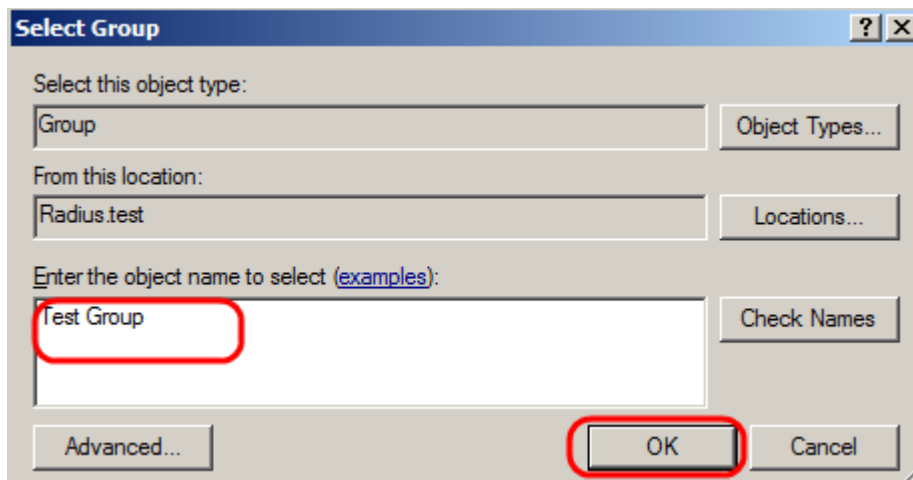
Groups

- Windows Groups**  
The Windows Groups condition specifies that the connecting user or computer must belong to one of the s
- Machine Groups**  
The Machine Groups condition specifies that the connecting computer must belong to one of the selected
- User Groups**  
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

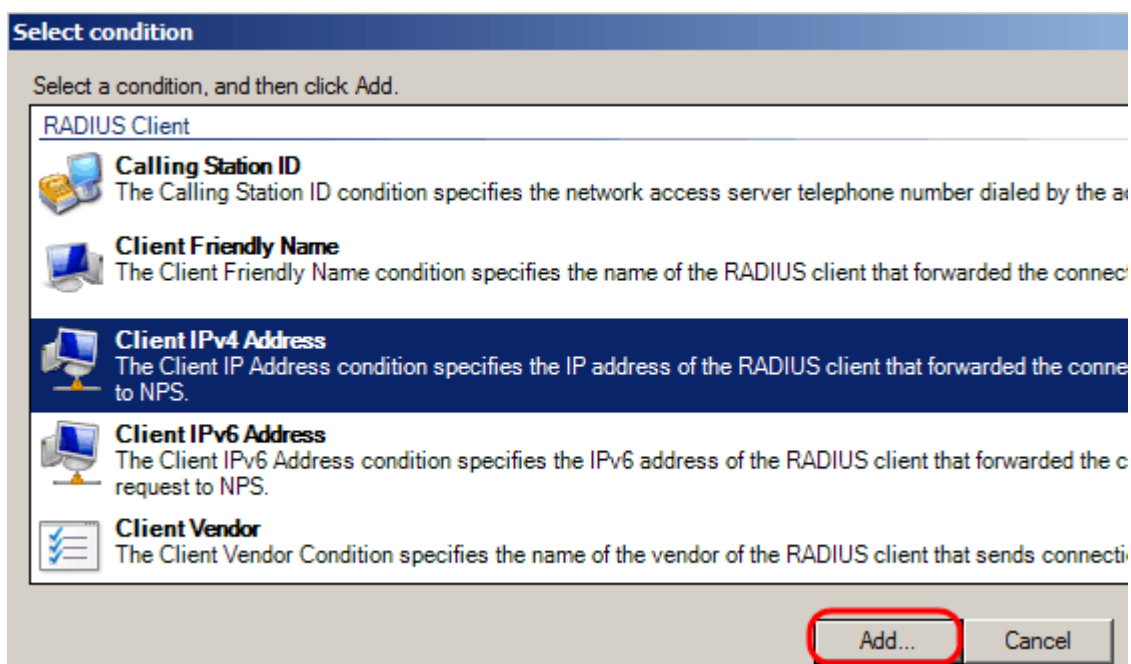
HCAP

- Location Groups**  
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) locatio required to match this policy. The HCAP protocol is used for communication between NPS and some third network access servers (NASs). See your NAS documentation before using this condition.
- HCAP User Groups**

Etapa 6. Selecione o tipo de objeto, o local e insira o nome do objeto. Clique em **Ok** e, em seguida, clique em **Ok**. Clique em **Adicionar** para adicionar a próxima condição.



Passo 7. Em RADIUS Client, selecione escolha IPv4 Address como o método para conectar o servidor aos clientes RADIUS, que, nesse caso, serão o endereço IP do switch. Clique em Add.



Etapa 8. Insira o endereço IP correspondente e clique em **Ok**. Uma lista com as condições adicionadas é exibida. Clique em **Next**.

Etapa 9. Na página Especificar Permissão de Acesso, selecione **Acesso Concedido**. Clique em Next.

**New Network Policy**

### Specify Access Permission

Configure whether you want to grant network access or deny network access if the 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

Etapa 10. Na página de autenticação, defina o método de autenticação mais adequado à sua rede. Clique em Next.

**New Network Policy**

### Configure Authentication Methods

Configure one or more authentication methods required for the connection request authentication, you must configure an EAP type. If you deploy NAP with 802.1X or Protected EAP in connection request policy, which overrides network policy authentication.

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

**EAP Types:**

[Empty list box] 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.
- Perform machine health check only

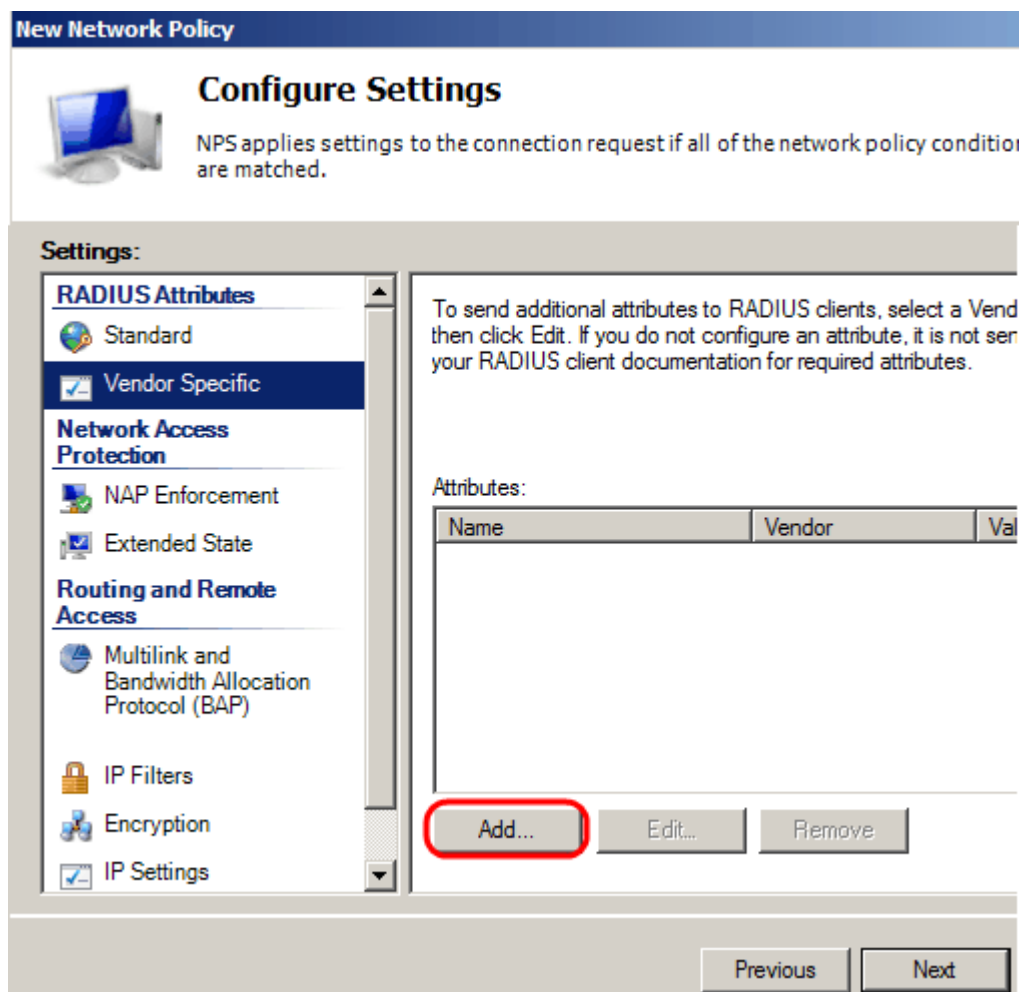
Previous Next

Etapa 11. Na janela Configurar Restrições, use os valores padrão. Clique em Next.

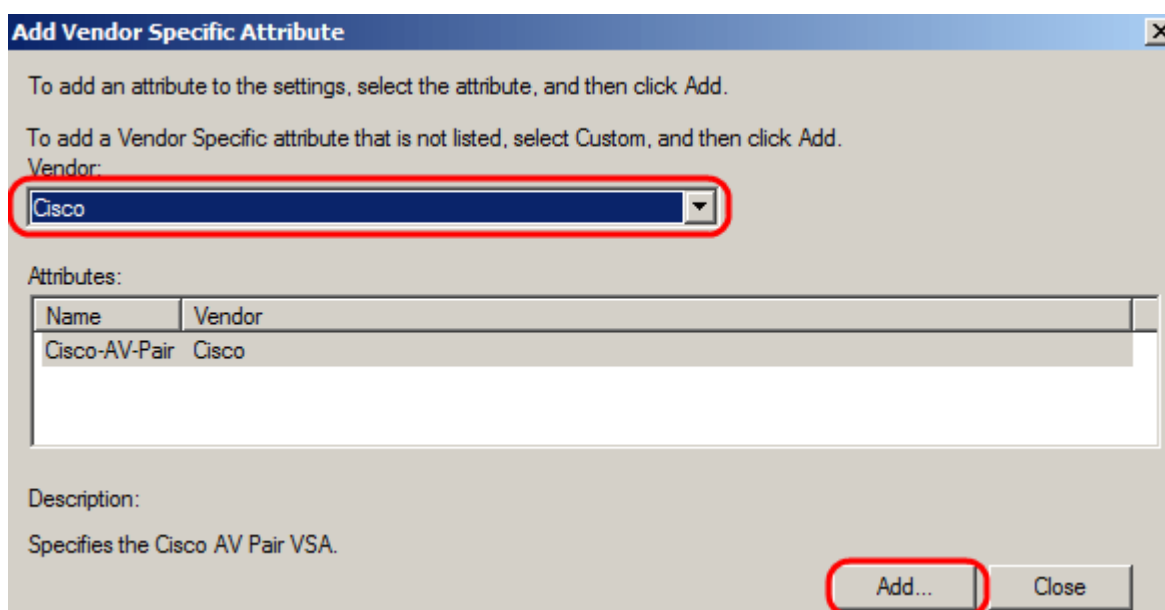
Etapa 12. Na página Configurar configurações, em Atributos RADIUS, clique em **Específico do**

fornecedor e em **Adicionar**.

**Observação:** o restante das configurações desta página são definidas com seus valores padrão. Você só precisa cuidar das configurações específicas do fornecedor.

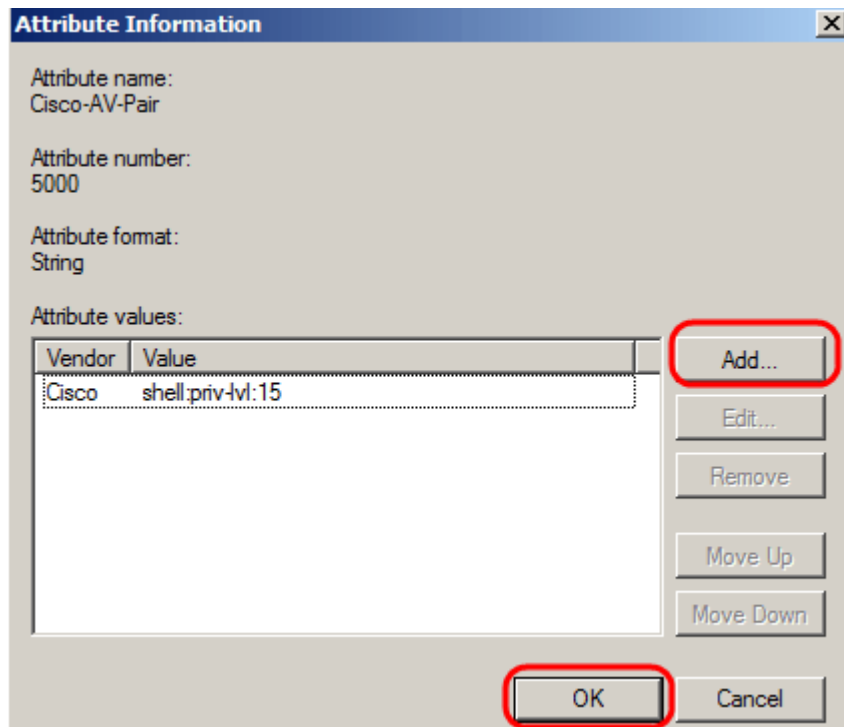


Em Fornecedor, Selecione **Cisco**. Clique em Add. A janela *Informações do Atributo* é aberta.



Na janela Informações do atributo, clique em **Adicionar** e insira o valor shell:priv-lvl:15. Click **OK**.





**Nota:** Este é o valor atribuído pela Cisco para que o servidor RADIUS conceda acesso ao utilitário de configuração de switch baseado na Web.

Clique em **Ok** para fechar a janela Informações do atributo e, em seguida, clique em **Fechar** para fechar a janela Adicionar atributo específico do fornecedor. Clique em Next.

Etapa 13. Um resumo das configurações para esta política é mostrado. Clique em **Finish**. A política de rede é criada.



## Completing New Network Policy

You have successfully created the following network policy:

### SG200/300 Series

#### Policy conditions:

Condition	Value
Windows Groups	RADIUS\Test Group
Client IPv4 Address	192.168.1.10

#### Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OF
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Previous

Next

Finish

## 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.