

ACS seguro - NAR com clientes AAA para usuários e grupos de usuários

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Restrições de acesso à rede](#)

[Sobre as restrições de acesso à rede](#)

[Adicionar um NAR compartilhado](#)

[Editar um NAR compartilhado](#)

[Excluir um NAR compartilhado](#)

[Definir restrições de acesso à rede para um usuário](#)

[Definir restrições de acesso à rede para um grupo de usuários](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve como configurar as Restrições de Acesso de Rede (NAR) na versão 4.x do Cisco Secure Access Control Server (ACS) com clientes de AAA (inclui roteadores, PIX, ASA e controladores wireless) para Usuários e Grupos de usuários.

[Prerequisites](#)

[Requirements](#)

Este documento é criado com o pressuposto de que os clientes Cisco Secure ACS e AAA estão configurados e funcionam corretamente.

[Componentes Utilizados](#)

As informações neste documento são baseadas no Cisco Secure ACS 3.0 e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[Conventions](#)

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Restrições de acesso à rede

Esta seção descreve NARs e fornece instruções detalhadas para configurar e gerenciar NARs compartilhados.

Esta seção contém estes tópicos:

- [Sobre as restrições de acesso à rede](#)
- [Adicionar um NAR compartilhado](#)
- [Editar um NAR compartilhado](#)
- [Excluir um NAR compartilhado](#)

Sobre as restrições de acesso à rede

Um NAR é uma definição, que você faz no ACS, de condições adicionais que você deve atender antes que um usuário possa acessar a rede. O ACS aplica essas condições usando informações de atributos que seus clientes AAA enviam. Embora você possa configurar NARs de várias maneiras, todos se baseiam em informações de atributo correspondentes que um cliente AAA envia. Portanto, você deve entender o formato e o conteúdo dos atributos que seus clientes AAA enviam se quiser empregar NARs eficazes.

Quando você configura um NAR, você pode escolher se o filtro funciona de forma positiva ou negativa. Ou seja, no NAR você especifica se permite ou nega o acesso à rede, com base nas informações enviadas de clientes AAA quando comparadas às informações armazenadas no NAR. No entanto, se um NAR não encontrar informações suficientes para operar, o padrão será o acesso negado. Esta tabela mostra as seguintes condições:

	Baseado em IP	Não baseado em IP	Informações insuficientes
Permitir	Acesso concedido	Acesso negado	Acesso negado
Negar	Acesso negado	Acesso concedido	Acesso negado

O ACS suporta dois tipos de filtros NAR:

- **Filtros baseados em IP** — os filtros NAR baseados em IP limitam o acesso com base nos endereços IP do cliente do usuário final e do cliente AAA. Consulte a seção [Sobre filtros NAR baseados em IP](#) para obter mais informações.
- **Filtros não baseados em IP** — Os filtros NAR não baseados em IP limitam o acesso com base na simples comparação de cadeia de caracteres de um valor enviado do cliente AAA. O valor pode ser o número de identificação da linha chamadora (CLI), o número do serviço de identificação do número discado (DNIS), o endereço MAC ou outro valor originado do cliente. Para que esse tipo de NAR funcione, o valor na descrição do NAR deve corresponder exatamente ao que está sendo enviado do cliente, que inclui qualquer formato usado. Por exemplo, o número de telefone (217) 555-4534 não corresponde a 217-555-4534. Consulte a

seção [Sobre filtros NAR não baseados em IP](#) para obter mais informações.

Você pode definir um NAR para um usuário específico ou grupo de usuários e aplicá-lo a ele. Consulte as seções [Definir Restrições de Acesso à Rede para um Usuário](#) ou [Definir Restrições de Acesso à Rede para um Grupo de Usuários](#) para obter mais informações. No entanto, na seção Shared Profile Components do ACS, você pode criar e nomear um NAR compartilhado sem citar diretamente qualquer usuário ou grupo de usuários. Você dá ao NAR compartilhado um nome que pode ser referenciado em outras partes da interface da Web do ACS. Em seguida, quando você configurar usuários ou grupos de usuários, poderá selecionar nenhuma, uma ou várias restrições compartilhadas a serem aplicadas. Ao especificar a aplicação de vários NARs compartilhados a um usuário ou grupo de usuários, você escolhe um dos dois critérios de acesso:

- Todos os filtros selecionados devem permitir.
- Qualquer filtro selecionado deve permitir.

Você deve entender a ordem de precedência relacionada aos diferentes tipos de NARs. Esta é a ordem da filtragem NAR:

1. NAR compartilhado no nível do usuário
2. NAR compartilhado no nível do grupo
3. NAR não compartilhado no nível do usuário
4. NAR não compartilhado no nível do grupo

Você também deve entender que a **negação de acesso em qualquer nível tem precedência sobre as configurações em outro nível que não negam o acesso**. Essa é a única exceção no ACS à regra que as configurações de nível de usuário substituem as configurações de nível de grupo. Por exemplo, um usuário específico pode não ter restrições de NAR no nível do usuário que se aplicam. No entanto, se esse usuário pertencer a um grupo restrito por um NAR compartilhado ou não compartilhado, o usuário terá o acesso negado.

Os NARs compartilhados são mantidos no banco de dados interno do ACS. Você pode usar os recursos de backup e restauração do ACS para fazer backup e restaurá-los. Você também pode replicar os NARs compartilhados, juntamente com outras configurações, para ACSs secundários.

[Sobre os filtros NAR baseados em IP](#)

Para filtros NAR baseados em IP, o ACS usa os atributos como mostrado, o que depende do protocolo AAA da solicitação de autenticação:

- **Se você estiver usando TACACS+**—O campo `rem_addr` do corpo do pacote de início TACACS+ é usado. **Observação:** quando uma solicitação de autenticação é encaminhada por proxy para um ACS, todos os NARs para solicitações TACACS+ são aplicados ao endereço IP do servidor AAA de encaminhamento, não ao endereço IP do cliente AAA de origem.
- **Se você estiver usando o RADIUS IETF** — A `call-station-id` (atributo 31) deve ser usada. **Observação:** os filtros NAR baseados em IP funcionam somente se o ACS receber o atributo Radius Calling-Station-Id (31). A Calling-Station-Id (31) deve conter um endereço IP válido. Caso contrário, cairá sobre as regras do DNIS.

Os clientes AAA que não fornecem informações de endereço IP suficientes (por exemplo, alguns tipos de firewall) não suportam a funcionalidade NAR completa.

Outros atributos para restrições **baseadas em IP**, por protocolo, incluem os campos NAR conforme mostrado:

- **Se você estiver usando TACACS+** — Os campos NAR no ACS usam estes valores:**AAA client** —O `NAS-IP-address` é extraído do endereço de origem no soquete entre o ACS e o cliente TACACS+.**Porta** —O campo da porta é retirado do corpo do pacote de início TACACS+.

[Sobre os filtros NAR não baseados em IP](#)

Um filtro NAR não baseado em IP (ou seja, um filtro NAR baseado em DNIS/CLI) é uma lista de locais de chamada ou ponto de acesso permitidos ou negados que você pode usar para restringir um cliente AAA quando você não tem uma conexão baseada em IP estabelecida. O recurso NAR não baseado em IP geralmente usa o número CLI e o número DNIS.

No entanto, quando você digita um endereço IP no lugar da CLI, você pode usar o filtro não baseado em IP; mesmo quando o cliente AAA não usa uma versão do software Cisco IOS® que suporta CLI ou DNIS. Em outra exceção à inserção de uma CLI, você pode inserir um endereço MAC para permitir ou negar acesso. Por exemplo, quando você estiver usando um cliente Cisco Aironet AAA. Da mesma forma, você pode digitar o endereço MAC do AP Cisco Aironet no lugar do DNIS. O formato do que você especifica na caixa CLI—CLI, endereço IP ou endereço MAC—deve corresponder ao formato do que você recebe do seu cliente AAA. Você pode determinar esse formato a partir do seu Registro de Contabilidade RADIUS.

Os atributos para restrições baseadas em DNIS/CLI, por protocolo, incluem os campos NAR conforme mostrado:

- **Se você estiver usando TACACS+** — Os campos NAR listados empregam estes valores:**AAA client** —O `NAS-IP-address` é extraído do endereço de origem no soquete entre o ACS e o cliente TACACS+.**Porta**—O campo `porta` no corpo do pacote de início TACACS+ é usado.**CLI** —O campo `rem-addr` no corpo do pacote de início TACACS+ é usado.**DNIS**—O campo `rem-addr` retirado do corpo do pacote de início TACACS+ é usado. Nos casos em que os dados `rem-addr` começam com a barra (/), o campo DNIS contém os dados `rem-addr` sem a barra (/).**Observação:** quando uma solicitação de autenticação é encaminhada por proxy para um ACS, todos os NARs para solicitações TACACS+ são aplicados ao endereço IP do servidor AAA de encaminhamento, não ao endereço IP do cliente AAA de origem.
- **Se você estiver usando RADIUS** — Os campos NAR listados usam estes valores:**AAA client** —O `NAS-IP-address` (atributo 4) ou, se `NAS-IP-address` não existir, `NAS-identifier` (atributo RADIUS 32) é usado.**Porta** —A `porta NAS` (atributo 5) ou, se a porta NAS não existir, `NAS-port-ID` (atributo 87) é usado.**CLI** — A `call-station-ID` (atributo 31) é usada.**DNIS**—O `called-station-ID` (atributo 30) é usado.

Ao especificar um NAR, você pode usar um asterisco (*) como curinga para qualquer valor ou como parte de qualquer valor para estabelecer um intervalo. Todos os valores ou condições em uma descrição NAR devem ser atendidos para que o NAR restrinja o acesso. Isso significa que os valores contêm um AND booleano.

[Adicionar um NAR compartilhado](#)

Você pode criar um NAR compartilhado que contém muitas restrições de acesso. Embora a interface da Web do ACS não aplique limites ao número de restrições de acesso em um NAR compartilhado ou ao comprimento de cada restrição de acesso, você deve seguir estes limites:

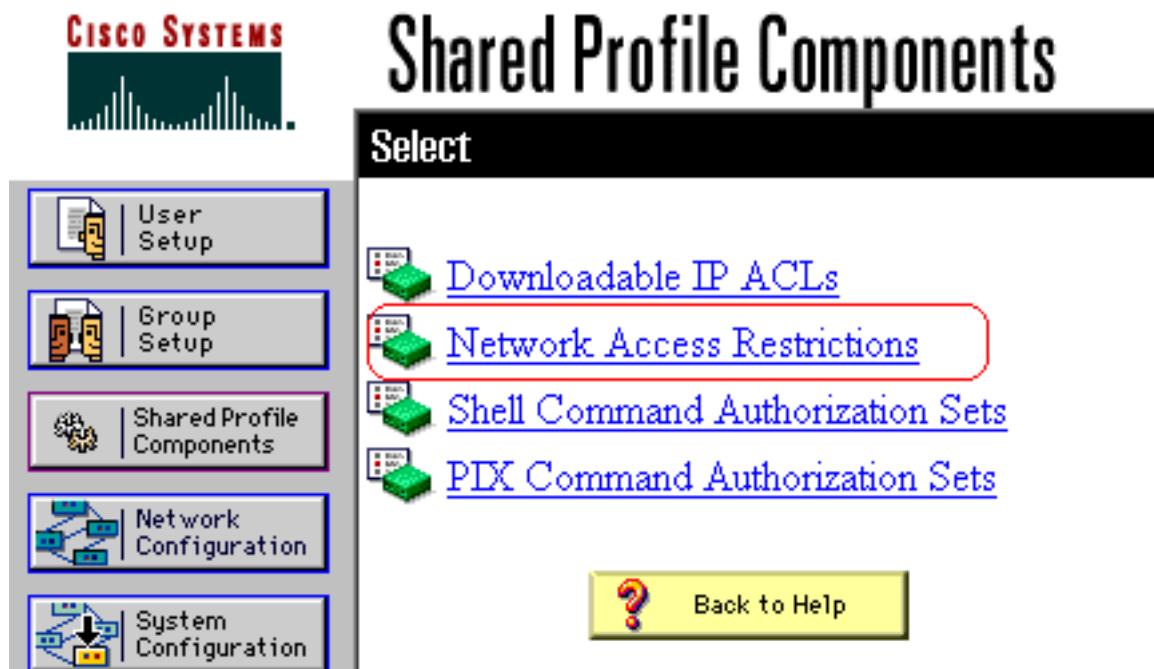
- A combinação de campos para cada item de linha não pode exceder 1024 caracteres.

- O NAR compartilhado não pode ter mais de 16 KB de caracteres. O número de itens de linha suportados depende do comprimento de cada item de linha. Por exemplo, se você criar um NAR baseado em CLI/DNIS em que os nomes dos clientes AAA são 10 caracteres, os números de porta são 5 caracteres, as entradas CLI são 15 caracteres e as entradas DNIS são 20 caracteres, você pode adicionar 450 itens de linha antes de atingir o limite de 16 KB.

Nota: Antes de definir um NAR, certifique-se de que estabeleceu os elementos que pretende utilizar nesse NAR. Portanto, você deve ter especificado todos os NAFs e NDGs e definido todos os clientes AAA relevantes, antes de fazer deles parte da definição de NAR. Consulte a seção [Sobre restrições de acesso à rede](#) para obter mais informações.

Conclua estes passos para adicionar um NAR compartilhado:

1. Na barra Navegação, clique em **Shared Profile Components**. A janela Shared Profile Components (Componentes do perfil compartilhado) é




exibida.

2. Clique em **Network Access Restrictions (Restrições de acesso à**



Shared Profile Components

Select

Network Access Restrictions 

Name	Description
None Defined	

Add Cancel

rede).

3. Clique em Add. A janela Network Access Restriction (Restrição de acesso à rede) é exibida.

Shared Profile Components

Network Access Restriction

Name:

Description:

Define IP-based access restrictions

Table Defines:

AAA Client	Port	Src IP Address
<input type="text"/>		

AAA Client:

Port:

Src IP Address:

Define CLI/DNIS-based access restrictions

Table Defines:

AAA Client	Port	CLI	DNIS
<input type="text"/>			

- Na caixa Nome, digite um nome para o novo NAR compartilhado. **Observação:** o nome pode conter até 31 caracteres. Espaços à esquerda e à direita não são permitidos. Os nomes não podem conter estes caracteres: colchete esquerdo ([), colchete direito (]), vírgula (,) ou barra (/).
- Na caixa Descrição, digite uma descrição do novo NAR compartilhado. A descrição pode ter até 30.000 caracteres.
- Se você quiser permitir ou negar o acesso com base no endereçamento IP: Marque a caixa de seleção **Definir descrições de acesso baseadas em IP**. Para especificar se você está listando endereços permitidos ou negados, na lista Definições da tabela, selecione o valor aplicável. Selecione ou insira as informações aplicáveis em cada uma destas caixas: **Cliente AAA** — Selecione **Todos os clientes AAA**, ou o nome do NDG, ou do NAF ou do cliente AAA individual, ao qual o acesso é permitido ou negado. **Port** — Digite o número da porta à qual

deseja permitir ou negar acesso. Você pode usar o asterisco (*) como curinga para permitir ou negar acesso a todas as portas no cliente AAA selecionado. **Endereço IP Src** — Insira o endereço IP para filtrar ao executar restrições de acesso. Você pode usar o asterisco (*) como curinga para especificar todos os endereços IP. **Observação:** o número total de caracteres na lista de clientes AAA e nas caixas Port e Src IP Address não deve exceder 1024. Embora o ACS aceite mais de 1024 caracteres quando você adiciona um NAR, não é possível editar o NAR e o ACS não pode aplicá-lo com precisão aos usuários. Clique em **Enter**. As informações de cliente, porta e endereço AAA aparecem como um item de linha na tabela. Repita as etapas c e d para inserir itens de linha baseados em IP adicionais.

- Se você quiser permitir ou negar o acesso com base no local ou valores de chamada diferentes de endereços IP: Marque a caixa de seleção **Definir restrições de acesso baseadas em CLI/DNIS**. Para especificar se você está listando locais permitidos ou negados na lista de definições de tabela, selecione o valor aplicável. Para especificar os clientes aos quais este NAR se aplica, selecione um destes valores na lista de clientes AAA: O nome da NDGO nome do cliente AAA específico Todos os clientes AAA **Dica:** somente os NDGs que você já configurou estão listados. Para especificar as informações sobre as quais esse NAR deve filtrar, insira valores nessas caixas, conforme aplicável: **Dica:** você pode digitar um asterisco (*) como curinga para especificar **tudo** como um valor. **Port** — Digite o número da porta na qual filtrar. **CLI** — Digite o número CLI no qual filtrar. Você também pode usar esta caixa para restringir o acesso com base em valores diferentes de CLIs, como um endereço IP ou endereço MAC. Consulte a seção [Sobre restrições de acesso à rede](#) para obter mais informações. **DNIS** — Digite o número discado em para o qual filtrar. **Observação:** o número total de caracteres nas caixas Cliente AAA e Porta, CLI e DNIS não deve exceder 1024. Embora o ACS aceite mais de 1024 caracteres quando você adiciona um NAR, não é possível editar o NAR e o ACS não pode aplicá-lo com precisão aos usuários. Clique em **Enter**. As informações que especificam o item de linha NAR aparecem na tabela. Repita as etapas de c a e para inserir itens de linha NAR não baseados em IP adicionais. Clique em **Submit** para salvar a definição de NAR compartilhada. O ACS salva o NAR compartilhado e o lista na tabela **Network Access Restrictions (Restrições de acesso à rede)**.

[Editar um NAR compartilhado](#)

Conclua estes passos para editar um NAR compartilhado:

- Na barra Navegação, clique em **Shared Profile Components**. A janela Shared Profile Components (Componentes do perfil compartilhado) é exibida.
- Clique em **Network Access Restrictions (Restrições de acesso à rede)**. A tabela Network Access Restrictions (Restrições de acesso à rede) é exibida.
- Na coluna Nome, clique no NAR compartilhado que deseja editar. A janela Restrição de acesso à rede é exibida e exibe informações sobre o NAR selecionado.
- Edite o Nome ou a Descrição do NAR, conforme aplicável. A descrição pode ter até 30.000 caracteres.
- Para editar um item de linha na tabela de restrições de acesso com base em IP: Clique duas vezes no item de linha que deseja editar. As informações do item de linha são removidas da tabela e gravadas nas caixas abaixo da tabela. Edite as informações, conforme necessário. **Observação:** o número total de caracteres na lista de clientes AAA e nas caixas Port and Src IP Address não deve exceder 1024. Embora o ACS possa aceitar mais de 1024 caracteres quando você adiciona um NAR, não é possível editar um NAR e o ACS não pode

aplicá-lo com precisão aos usuários. Clique em **Enter**. As informações editadas para este item de linha são gravadas na tabela de restrições de acesso com base em IP.

6. Para remover um item de linha da tabela de restrições de acesso com base em IP: Selecione o item de linha. Na tabela, clique em **Remove**. O item de linha é removido da tabela de restrições de acesso com base em IP.
7. Para editar um item de linha na tabela de restrições de acesso CLI/DNIS: Clique duas vezes no item de linha que deseja editar. As informações do item de linha são removidas da tabela e gravadas nas caixas abaixo da tabela. Edite as informações, conforme necessário. **Observação:** o número total de caracteres nas caixas Cliente AAA e Porta, CLI e DNIS não deve exceder 1024. Embora o ACS possa aceitar mais de 1024 caracteres quando você adiciona um NAR, não é possível editar um NAR e o ACS não pode aplicá-lo com precisão aos usuários. Clique em **Enter**. As informações editadas para este item de linha são gravadas na tabela de restrições de acesso CLI/DNIS.
8. Para remover um item de linha da tabela de restrições de acesso CLI/DNIS: Selecione o item de linha. Na tabela, clique em **Remove**. O item de linha é removido da tabela de restrições de acesso CLI/DNIS.
9. Clique em **Submit** para salvar as alterações feitas. O ACS reinicia o filtro com as novas informações, que entram em vigor imediatamente.

Excluir um NAR compartilhado

Observação: certifique-se de remover a associação de um NAR compartilhado a qualquer usuário ou grupo antes de excluir esse NAR.

Conclua estes passos para excluir um NAR compartilhado:

1. Na barra Navegação, clique em **Shared Profile Components**. A janela Shared Profile Components (Componentes do perfil compartilhado) é exibida.
2. Clique em **Network Access Restrictions (Restrições de acesso à rede)**.
3. Clique no nome do NAR compartilhado que deseja excluir. A janela Restrição de acesso à rede é exibida e exibe informações sobre o NAR selecionado.
4. Na parte inferior da janela, clique em **Excluir**. Uma caixa de diálogo avisa que você está prestes a excluir um NAR compartilhado.
5. Clique em **OK** para confirmar que deseja excluir o NAR compartilhado. O NAR compartilhado selecionado é excluído.

Definir restrições de acesso à rede para um usuário

Use a tabela Restrições de acesso à rede na área Configurações avançadas de configuração do usuário para definir NARs de três maneiras:

- Aplicar NARs compartilhados existentes por nome.
- Defina restrições de acesso baseadas em IP para permitir ou negar o acesso do usuário a um cliente AAA especificado ou a portas especificadas em um cliente AAA quando uma conexão IP tiver sido estabelecida.
- Defina restrições de acesso baseadas em CLI/DNIS para permitir ou negar o acesso do usuário com base na CLI/DNIS usada. **Observação:** você também pode usar a área de restrições de acesso baseada em CLI/DNIS para especificar outros valores. Consulte a seção

[Restrições de Acesso à Rede](#) para obter mais informações.

Normalmente, você define (compartilhados) NARs na seção Componentes compartilhados para que possa aplicar essas restrições a mais de um grupo ou usuário. Consulte a seção [Adicionar um NAR compartilhado](#) para obter mais informações. Você deve ter selecionado a caixa de seleção **Restrições de Acesso à Rede no Nível do Usuário** na página Opções Avançadas da seção Configuração da Interface para que esse conjunto de opções apareça na interface da Web.

No entanto, você também pode usar o ACS para definir e aplicar um NAR para um único usuário na seção User Setup. Você deve ter ativado a configuração **User-Level Network Access Restrictions** na página Advanced Options da seção Interface Configuration para opções de filtro baseadas em IP de usuário único e opções de filtro baseadas em CLI/DNIS de usuário único para aparecerem na interface da Web.

Observação: quando uma solicitação de autenticação é encaminhada por proxy para um ACS, todos os NARs para solicitações do Terminal Access Controller Access Control System (TACACS+) são aplicados ao endereço IP do servidor AAA de encaminhamento, não ao endereço IP do cliente AAA de origem.

Quando você cria restrições de acesso por usuário, o ACS não impõe limites ao número de restrições de acesso e não impõe um limite ao comprimento de cada restrição de acesso. No entanto, há limites rigorosos:

- A combinação de campos para cada item de linha não pode exceder 1024 caracteres.
- O NAR compartilhado não pode ter mais de 16 KB de caracteres. O número de itens de linha suportados depende do comprimento de cada item de linha. Por exemplo, se você criar um NAR baseado em CLI/DNIS em que os nomes dos clientes AAA são 10 caracteres, os números de porta são 5 caracteres, as entradas CLI são 15 caracteres e as entradas DNIS são 20 caracteres, você pode adicionar 450 itens de linha antes de atingir o limite de 16 KB.

Conclua estes passos para definir NARs para um usuário:

1. Execute as etapas de 1 a 3 de [Adicionar uma conta de usuário básica](#). A janela User Setup Edit é aberta. O nome de usuário adicionado ou editado é exibido na parte superior da janela.

User Setup

Advanced Settings

Network Access Restrictions (NAR) ?

Shared Network Access Restrictions

Only Allow network access when

- All selected NARs result in permit
- Any one selected NAR results in permit

NARs

testnar

>>

->

<-

<<

Selected NARs

View IP NAR

View CLI/DNIS NAR

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations

AAA Client	Port	Address

remove

AAA Client

All AAA Clients

Port

Address

Submit

Delete

Cancel

2. Para aplicar um NAR compartilhado configurado anteriormente a este usuário:**Observação:** para aplicar um NAR compartilhado, você deve configurá-lo em Network Access Restrictions (Restrições de acesso à rede) na seção Shared Profile Components (Componentes de perfil compartilhados). Consulte a seção [Adicionar um NAR compartilhado](#) para obter mais informações. Marque a caixa de seleção **Somente permitir acesso à rede quando**. Para especificar se um ou todos os NARs compartilhados devem ser aplicados para que o usuário

tenha permissão de acesso, selecione um, conforme aplicável: Todos os NARS selecionados resultam em permit. Qualquer NAR selecionado resulta em permitir. Selecione um nome de NAR compartilhado na lista NARs e clique em → (botão de seta para a direita) para mover o nome para a lista de NARs selecionados. **Dica:** para visualizar os detalhes do servidor dos NARs compartilhados que você selecionou para aplicar, clique em **Exibir NAR IP** ou em **Exibir CLID/DNIS NAR**, conforme aplicável.

3. Para definir e aplicar um NAR, para esse usuário específico, que permita ou negue o acesso desse usuário com base no endereço IP ou no endereço IP e na porta: **Observação:** você deve definir a maioria dos NARs na seção Componentes compartilhados para que possa aplicá-los a mais de um grupo ou usuário. Consulte a seção [Adicionar um NAR compartilhado](#) para obter mais informações. Na tabela Restrições de acesso à rede, em Restrições de acesso à rede definidas por usuário, marque a caixa de seleção **Definir restrições de acesso baseadas em IP**. Para especificar se a listagem subsequente especifica endereços IP permitidos ou negados, na lista Definições da tabela, escolha um: **Chamada/locais de ponto de acesso permitidos** **Chamada negada/Locais de ponto de acesso** Selecione ou insira as informações nessas caixas: **AAA Client**—Selecione **All AAA Clients**, ou o nome de um grupo de dispositivos de rede (NDG), ou o nome do cliente AAA individual, ao qual permitir ou negar acesso. **Port**—Digite o número da porta para a qual permitir ou negar acesso. Você pode usar o asterisco (*) como curinga para permitir ou negar acesso a todas as portas no cliente AAA selecionado. **Endereço**—Insira o endereço IP ou endereços a serem usados ao executar restrições de acesso. Você pode usar o asterisco (*) como curinga. **Observação:** o número total de caracteres na lista de clientes AAA e nas caixas Port e Src IP Address não deve exceder 1024. Embora o ACS aceite mais de 1024 caracteres quando você adiciona um NAR, não é possível editar o NAR e o ACS não pode aplicá-lo com precisão aos usuários. Clique em **Enter**. As informações especificadas de cliente AAA, porta e endereço aparecem na tabela acima da lista de clientes AAA.
4. Para permitir ou negar acesso a esse usuário com base no local ou valores de chamada diferentes de um endereço IP estabelecido: Marque a caixa de seleção **Definir restrições de acesso baseadas em CLI/DNIS**. Para especificar se a listagem subsequente especifica valores permitidos ou negados, na lista Definições da tabela, escolha um: **Chamada/locais de ponto de acesso permitidos** **Chamada negada/Locais de ponto de acesso** Preencha as caixas conforme mostrado: **Observação:** você deve fazer uma entrada em cada caixa. Você pode usar o asterisco (*) como curinga para todo ou parte de um valor. O formato que você usa deve corresponder ao formato da string que você recebe do seu cliente AAA. Você pode determinar esse formato a partir do seu Registro de Contabilidade RADIUS. **AAA Client**—Selecione **All AAA Clients**, ou o nome do NDG, ou o nome do cliente AAA individual, ao qual permitir ou negar acesso. **PORT**—Digite o número da porta à qual permitir ou negar acesso. Você pode usar o asterisco (*) como curinga para permitir ou negar acesso a todas as portas. **CLI**—Digite o número CLI ao qual permitir ou negar acesso. Você pode usar o asterisco (*) como curinga para permitir ou negar o acesso com base em parte do número. **Dica:** use a entrada CLI se quiser restringir o acesso com base em outros valores, como um endereço MAC do Cisco Aironet Client. Consulte a seção [Sobre restrições de acesso à rede](#) para obter mais informações. **DNIS**—Digite o número DNIS ao qual permitir ou negar acesso. Use esta entrada para restringir o acesso com base no número no qual o usuário discará. Você pode usar o asterisco (*) como curinga para permitir ou negar o acesso com base em parte do número. **Dica:** use a seleção de DNIS se quiser restringir o acesso com base em outros valores, como um endereço MAC de AP Cisco Aironet. Consulte a seção [Sobre restrições de acesso à rede](#) para obter mais

informações. **Observação:** o número total de caracteres nas caixas Cliente AAA e **Porta**, **CLI** e **DNIS** não deve exceder 1024. Embora o ACS aceite mais de 1024 caracteres quando você adiciona um NAR, não é possível editar o NAR e o ACS não pode aplicá-lo com precisão aos usuários. Clique em **Enter**. As informações que especificam o cliente AAA, a porta, a CLI e o DNIS aparecem na tabela acima da lista de clientes AAA.

5. Se você tiver terminado de configurar as opções da conta de usuário, clique em **Enviar** para gravar as opções.

[Definir restrições de acesso à rede para um grupo de usuários](#)

Use a tabela Network Access Restrictions (Restrições de Acesso à Rede) na Group Setup (Configuração do Grupo) para aplicar NARs de três maneiras distintas:

- Aplicar NARs compartilhados existentes por nome.
- Definir restrições de acesso a grupos baseados em IP para permitir ou negar acesso a um cliente AAA especificado ou a portas especificadas em um cliente AAA quando uma conexão IP tiver sido estabelecida.
- Defina NARs de grupos baseados em CLI/DNIS para permitir ou negar acesso ao número CLI ou ao número DNIS usado, ou ambos. **Observação:** você também pode usar a área de restrições de acesso baseada em CLI/DNIS para especificar outros valores. Consulte a seção [Sobre restrições de acesso à rede](#) para obter mais informações.

Normalmente, você define (compartilhado) NARs na seção Componentes compartilhados para que essas restrições possam se aplicar a mais de um grupo ou usuário. Consulte a seção [Adicionar um NAR compartilhado](#) para obter mais informações. Você deve marcar a caixa de seleção **Group-Level Shared Network Access Restriction** na página **Advanced Options** da seção Interface Configuration para que essas opções apareçam na interface da Web ACS.

No entanto, você também pode usar o ACS para definir e aplicar um NAR para um único grupo na seção **Configuração do grupo**. Você deve verificar a configuração **Group-Level Network Access Restriction** na página Advanced Options (Opções avançadas) da seção Interface Configuration (Configuração de interface) para ver as opções de filtro baseadas em IP de grupo único e as opções de filtro baseadas em CLI/DNIS de grupo único a serem exibidas na interface da Web ACS.

Observação: quando uma solicitação de autenticação é encaminhada por proxy para um servidor ACS, todos os NARs para solicitações RADIUS são aplicados ao endereço IP do servidor AAA de encaminhamento, não ao endereço IP do cliente AAA de origem.

Conclua estes passos para definir NARs para um grupo de usuários:

1. Na barra de navegação, clique em **Group Setup**. A janela Seleção de configuração de grupo é aberta.
2. Na lista Grupo, selecione um grupo e clique em **Editar configurações**. O nome do grupo é exibido na parte superior da janela Configurações do grupo.

