

Configurar o gerenciamento do DAC (Device Authorization Control, controle de autorização de dispositivo) por meio do SNA (Smart Network Application, aplicativo de rede inteligente)

Objetivo

O sistema Smart Network Application (SNA) exibe uma visão geral da topologia da rede, incluindo informações detalhadas de monitoramento de dispositivos e tráfego. A SNA permite visualizar e modificar configurações globalmente em todos os dispositivos suportados na rede.

A SNA tem um recurso conhecido como DAC (Device Authorization Control, Controle de Autorização de Dispositivos) que permite configurar uma lista de dispositivos de clientes autorizados na rede. O DAC ativa os recursos 802.1X em dispositivos SNA na rede e um RADIUS (Remote Authentication Dial-In User Service) ou RADIUS Host Server pode ser configurado em um dos dispositivos SNA. O DAC é feito através da autenticação Media Access Control (MAC).

Este artigo fornece instruções sobre como configurar o DAC Management através de SNA.

Dispositivos aplicáveis

- Sx350 Series
- SG350X Series
- Sx550X Series

Note: Os dispositivos da Sx250 Series podem fornecer informações SNA quando estão conectados à rede, mas a SNA não pode ser iniciada a partir desses dispositivos.

Versão de software

- 2.2.5.68

Fluxo de trabalho do DAC

Você pode configurar o gerenciamento de DAC através das seguintes etapas:

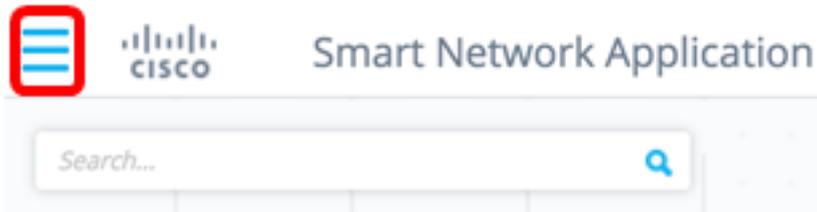
- [Ativar DAC](#)
- [Configurar servidor e clientes RADIUS](#)
- [Gerenciamento de lista DAC](#)

[Ativar DAC](#)

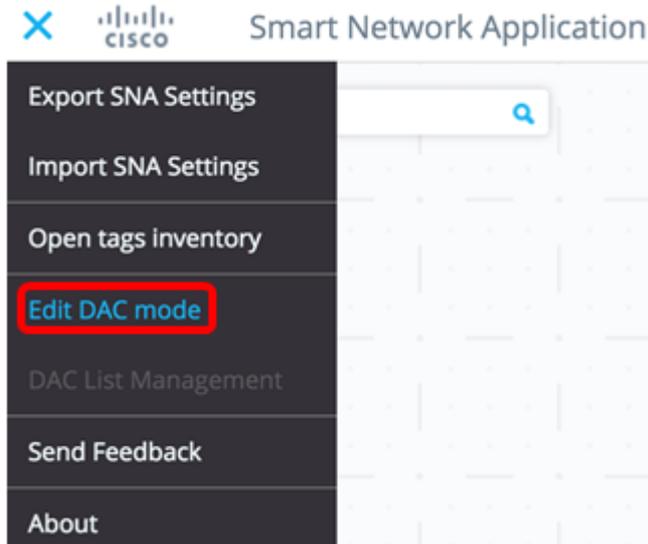
Para acessar e ativar o DAC, siga estas etapas:

Etapa 1. Clique no menu **Options** no canto superior esquerdo da página SNA para mostrar

as opções disponíveis.



Etapa 2. Escolha **Editar modo DAC**.



O modo de edição DAC está ativado. Você deve ver o quadro azul abaixo do mapa de topologia e o painel de controle na parte inferior da tela.



Etapa 3. (Opcional) Para sair do Modo de edição do DAC, clique no botão **Sair**.

[Configurar servidor e clientes RADIUS](#)

Etapa 1. Na exibição Topologia, escolha um dos dispositivos SNA e clique em seu menu **Opções**.



Etapa 2. Clique em **+ Definir como servidor DAC**.



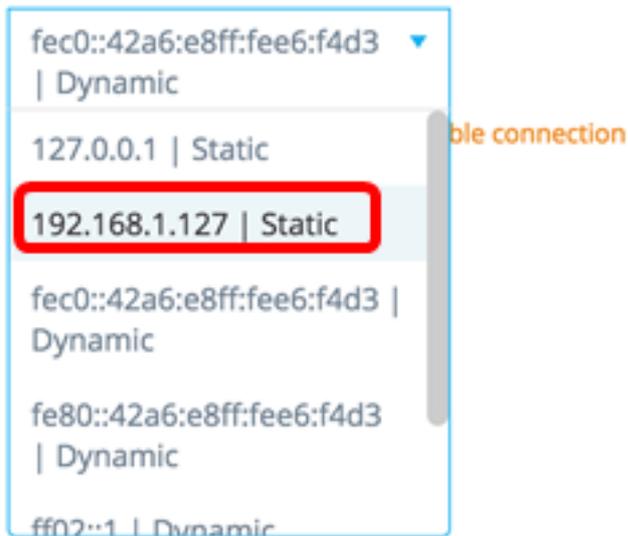
Etapa 3. Se o dispositivo tiver mais de um único endereço IP, escolha um desses endereços como o que será usado pelo DAC. Neste exemplo, 192.168.1.127 | O estático é escolhido.

< BACK

Select IP Address

switche6f4d3 / fec0::42a6:e8ff:fee6:f4d3

IP ADDRESS



fec0::42a6:e8ff:fee6:f4d3 | Dynamic

127.0.0.1 | Static unstable connection

192.168.1.127 | Static

fec0::42a6:e8ff:fee6:f4d3 | Dynamic

fe80::42a6:e8ff:fee6:f4d3 | Dynamic

ff02::1 | Dynamic

Note: A lista de endereços indica se a interface IP é estática ou dinâmica. Você será avisado de que a escolha de um IP dinâmico pode causar uma conexão instável.

Select IP Address

switche6f4d3 / fec0::42a6:e8ff:fee6:f4d3

IP ADDRESS



192.168.1.127 | Dynamic

⚠ Dynamic ip might cause an unstable connection

DONE

Etapa 4. Clique em Concluído.

< BACK

Select IP Address

switche6f4d3 / fec0::42a6:e8ff:fee6:f4d3

IP ADDRESS

192.168.1.127 |
Static

DONE

Note: Ao editar um servidor DAC existente, o endereço usado atualmente por seus clientes é pré-selecionado.

O servidor RADIUS do DAC é destacado continuamente na exibição Topologia.



Etapa 5. Escolha um dos dispositivos SNA e clique em seu menu Opções.

Note: Se nenhum cliente estiver selecionado, você não poderá aplicar as configurações.

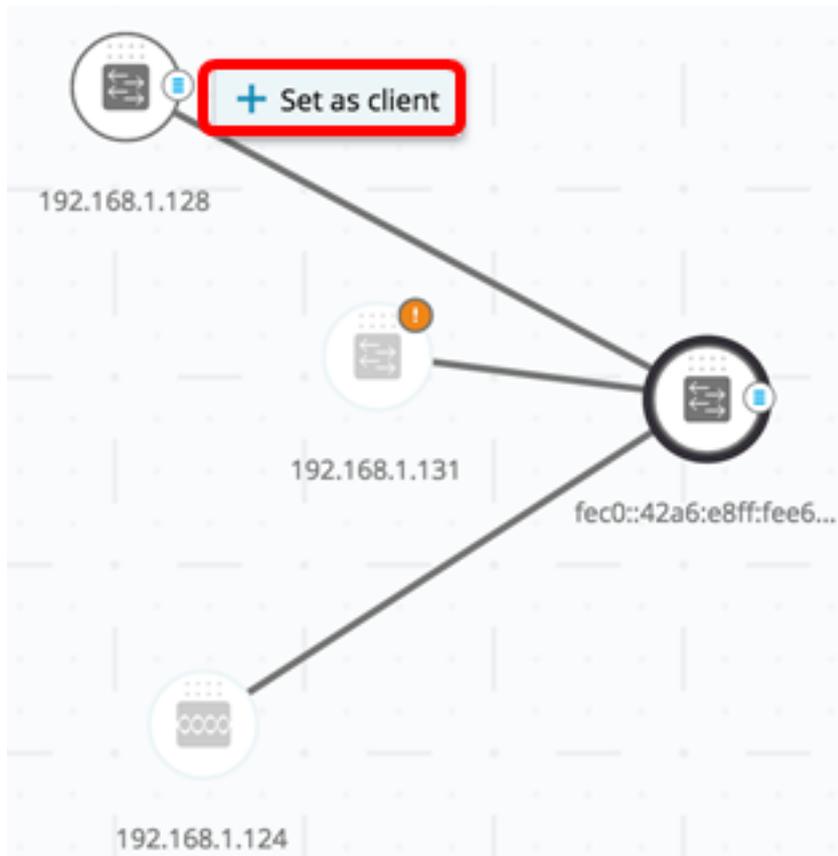


Se um switch já for um cliente do servidor RADIUS do DAC, seu endereço IP estará na tabela NAS do servidor RADIUS e o servidor RADIUS estiver configurado na tabela do servidor RADIUS com o tipo de uso 802.1X ou todos na prioridade 0. Este switch está pré-selecionado.

Se um cliente for escolhido, que já tem um servidor RADIUS configurado para 802.1X diferente do servidor selecionado anteriormente, você será notificado de que o procedimento interromperá a operação existente do servidor RADIUS.

Se um cliente for escolhido, com um servidor RADIUS configurado para 802.1X na prioridade 0 diferente do servidor selecionado anteriormente, uma mensagem de erro será exibida e o DAC não será configurado nesse cliente.

Etapa 6. Clique em + Definir como cliente.



Passo 7. Marque a caixa de seleção ou as caixas de seleção da porta ou portas do switch cliente para aplicar autenticações 802.1X.

Note: Neste exemplo, as portas GE1/1, GE1/2, GE1/3 e GE1/4 são verificadas.

< BACK

DONE

Select Client Ports

switche6fa9f / 192.168.1.128

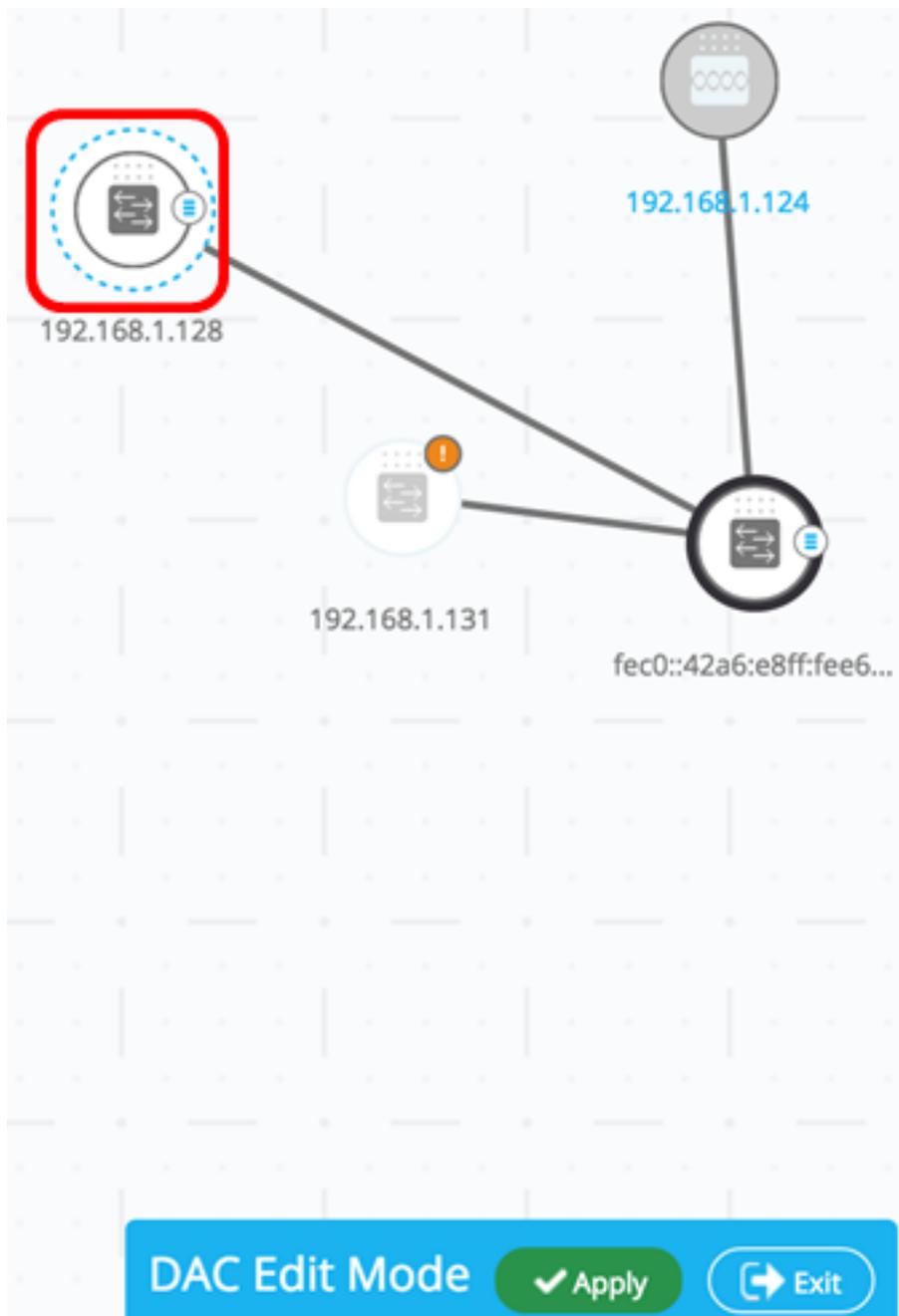
★ Select Recommended

<input type="checkbox"/>	PORT	SWITCHPORT MODE	DESCRIPTION	RECOMMENDED
<input checked="" type="checkbox"/>	GE1/1	trunk		
<input checked="" type="checkbox"/>	GE1/2	access		★
<input checked="" type="checkbox"/>	GE1/3	access		★
<input checked="" type="checkbox"/>	GE1/4	access		★
<input type="checkbox"/>	GE1/5	trunk		★

Note: A SNA recomenda uma lista de todas as portas de borda ou todas as portas que não se sabe estarem conectadas a outros switches ou nuvens.

Etapa 8. (Opcional) Clique no botão **Select Recommended (Selecionar recomendado)** para verificar todas as portas recomendadas.

Etapa 9. Clique em Concluído. O cliente RADIUS do DAC é destacado em azul tracejado na exibição Topologia.



Etapa 10. Clique em **Apply** para salvar as alterações.

Etapa 11. Digite uma sequência de caracteres que será usada pelo servidor DAC RADIUS com todos os seus clientes na rede.

Apply

STEP 1 - Insert Keysting » STEP 2 - Review Changes » STEP 3 - Apply Changes

i Please notice: you must enter a manual keysting or choose the auto generated option

Manual Auto Generated

Cisco1234|

Note: Neste exemplo, Cisco1234 é usado.

Etapa 12. (Opcional) Alterne o botão para **Gerado automaticamente** para usar uma sequência de caracteres de chave autogerada.

Apply

STEP 1 - Insert Keystring » STEP 2 - Review Changes » STEP 3 - Apply Changes

i Please notice: you must enter a manual keystring or choose the auto generated option

Manual Auto Generated

An auto generated Keystring will be created by the system

Etapa 13. Clique em **Continuar** no canto superior direito da página.

CONTINUE

Etapa 14. Revise as alterações e clique em **APLICAR ALTERAÇÕES**.

Apply

STEP 1 - Insert Keystring » STEP 2 - Review Changes » STEP 3 - Apply Changes

APPLY CHANGES

Save to Startup configuration

SWITCH	ACTIONS
switche6f4d3 fec0:42a6:e8ff:fee6:f4d3	Set radius server fec0:42a6:e8ff:fee6:f4d3
switche6fa9f 192.168.1.128	Add radius client 192.168.1.128 to server fec0:42a6:e8ff:fee6:f4d3
switche6fa9f 192.168.1.128	Set radius client for 192.168.1.128

Etapa 15. (Opcional) Desmarque a caixa de seleção **Salvar na configuração de inicialização** se não desejar salvar as configurações no arquivo de configuração.

APPLY CHANGES

Save to startup configuration

Etapa 16. (Opcional) Se estiver usando uma conta Somente leitura, talvez seja solicitado que você insira suas credenciais para continuar. Digite a senha no campo *Senha* e clique em **ENVIAR**.

Upgrade Access Permission X



SESSION IS IN READ ONLY MODE
Enter your password to upgrade permission and continue

Username:

cisco

Password:

SUBMIT

Etapa 17. A coluna Status deve conter caixas de seleção verdes que confirmam a aplicação bem-sucedida das alterações. Clique em Concluído.

Apply

STEP 1 - Insert Keystring » STEP 2 - Review Changes » STEP 3 - Apply Changes

DONE

Save to startup configuration

SWITCH	ACTIONS	STATUS
switch6f6d3 fec0:42a6:e8ff:fee6:f4d3	Set radius server fec0:42a6:e8ff:fee6:f4d3	<input checked="" type="checkbox"/> Set radius server fec0:42a6:e8ff:fee6:f4d3 succeed...
switch6fa9f 192.168.1.128	Add radius client 192.168.1.128 to server fec0:42a6:e8ff:fee6:f4d3	<input checked="" type="checkbox"/> Add DAC client 192.168.1.128 to server fec0:42a6:...
switch6fa9f 192.168.1.128	Set radius client for 192.168.1.128	<input checked="" type="checkbox"/> DAC configuration for client 192.168.1.128 succeed...

Depois que o DAC é configurado, um alerta é exibido sempre que um novo dispositivo não bloqueado é rejeitado na rede por meio de um servidor RADIUS habilitado para DAC. Você será solicitado a adicionar esse dispositivo à lista de permissões de dispositivos autorizados ou enviá-lo a uma lista de bloqueio para que você não seja alertado novamente.

Ao informar o usuário do novo dispositivo, a SNA fornece o endereço MAC do dispositivo e a porta que o dispositivo tentou acessar a rede.

Se um evento de rejeição for recebido de um dispositivo que não é um servidor DAC RADIUS, a mensagem será ignorada e todas as mensagens adicionais desse dispositivo para os próximos 20 minutos serão ignoradas. Após 20 minutos, a SNA verifica novamente se o dispositivo é um servidor DAC RADIUS. Se um usuário for adicionado à lista de permissões, o dispositivo será adicionado ao grupo DAC de todos os servidores DAC. Quando essa configuração for salva, você poderá escolher se deseja salvar essa configuração imediatamente na configuração de inicialização do servidor. Essa opção é selecionada por padrão.

Até que um dispositivo seja adicionado à lista de permissões, ele não terá permissão de acesso à rede. Você pode visualizar e alterar as listas de permissão e bloqueio a qualquer momento, desde que um servidor DAC RADIUS esteja definido e acessível. Para configurar o DAC List Management, vá para [DAC List Management](#).

Ao aplicar as configurações de DAC, você recebe um relatório listando ações que serão aplicadas aos dispositivos participantes. Depois de aprovar as alterações, você pode decidir se as configurações devem ser copiadas para o arquivo de configuração de inicialização dos dispositivos configurados. Finalmente, aplique as configurações.

O relatório exibe avisos se algumas etapas do processo de configuração do DAC forem perdidas, juntamente com o status das ações como tratadas pelos dispositivos.

Campo	Valor	Comentários
Dispositivo	Os identificadores do dispositivo (nome do host ou endereço IP)	
Ação	<p>Ações possíveis para o servidor DAC:</p> <ul style="list-style-type: none"> • Habilitar servidor RADIUS • Desativar servidor RADIUS • Atualizar lista de clientes • Criar grupo de servidores RADIUS • Excluir grupo de servidores RADIUS <p>Possíveis ações para o cliente DAC:</p> <ul style="list-style-type: none"> • Adicionar conexão de servidor RADIUS • Atualizar conexão do servidor RADIUS • Remover conexão de servidor RADIUS • Atualize as configurações do 802.1x • Atualizar configurações de autenticação da interface • Atualizar configurações de host e sessão da interface 	<p>É possível (e provável) que várias ações apareçam para cada dispositivo. Cada ação pode ter seu próprio status.</p>
Avisos	<p>Os possíveis avisos para o servidor DAC incluem:</p> <ul style="list-style-type: none"> • A interface IP selecionada é dinâmica. <p>Os possíveis avisos para clientes DAC incluem:</p> <ul style="list-style-type: none"> • O dispositivo já é um cliente de um servidor RADIUS diferente. • Nenhuma porta 	<p>Os avisos também contêm links para as seções do CAD onde podem ser endereçados. As alterações podem ser aplicadas quando os avisos estiverem presentes.</p>

	selecionada.	
Status	<ul style="list-style-type: none"> • Pendente • Sucesso • Falha 	Quando o status é uma falha, a mensagem de erro é exibida para a ação.

Gerenciamento de lista DAC

Depois de adicionar dispositivos clientes e selecionar quais de suas portas serão autenticadas, todos os dispositivos não autenticados detectados nessas portas serão adicionados à lista de dispositivos não autenticados.

O DAC suporta as seguintes listas de dispositivos:

- Allow List (Permitir lista) — Contém a lista de todos os clientes que podem ser autenticados.
- Bloquear lista — **Contém** a lista de clientes que nunca devem ser autenticados.

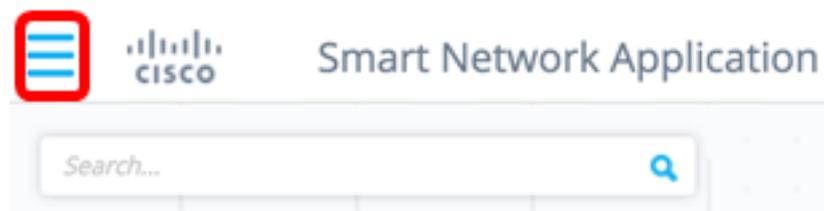
Se você deseja que os dispositivos e suas portas sejam autenticados, eles devem ser adicionados às listas de permissão. Se você não deseja que eles sejam autenticados, nenhuma ação é necessária, pois eles serão adicionados à lista de bloqueio por padrão.

[Consulte o glossário para obter mais informações.](#)

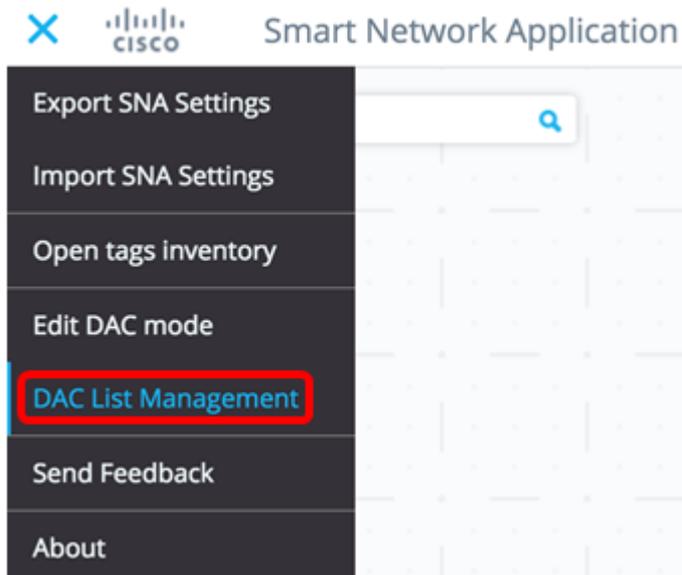
Adicionar dispositivos à lista Permitir ou Bloquear

Para adicionar dispositivos à lista de permissão ou bloqueio, siga estas etapas:

Etapa 1. Clique no menu **Options** no canto superior esquerdo da página SNA para mostrar as opções disponíveis.

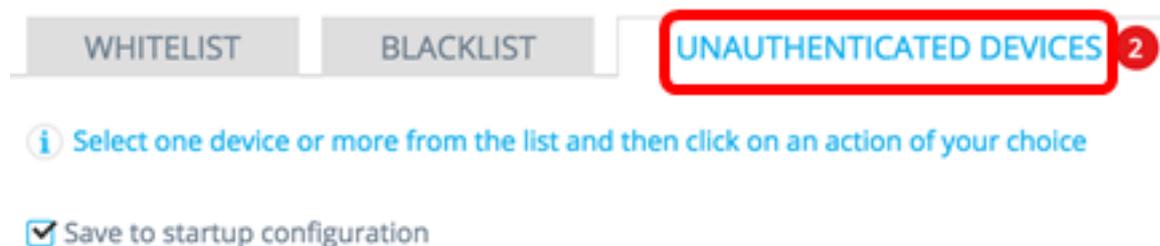


Etapa 2. Escolha **DAC List Management**.



Etapa 3. Clique na guia **DISPOSITIVOS NÃO AUTENTICADOS**. Esta página exibirá a lista de todos os dispositivos não autenticados.

DAC List Management



Note: Como alternativa, você pode clicar no ícone DAC List Management System no canto superior direito da página SNA.



Etapa 4. (Opcional) Marque a caixa de seleção ao lado do endereço MAC do dispositivo ou dispositivos que deseja adicionar à lista de permissões e clique em **Adicionar à lista de permissões**.

DAC List Management

WHITELIST

BLACKLIST

UNAUTHENTICATED DEVICES **2**

 Select one device or more from the list and then click on an action of your choice

Save to startup configuration

Add to Whitelist

Add to Blacklist

Dismiss

<input type="checkbox"/>	MAC ADDRESS	CONNECTING SWITCH	CONNECTING PORT	LAST SEEN	STATUS
<input checked="" type="checkbox"/>	0C:27:24:1F:47:A8	192.168.1.128	gi1/0/3	November 22nd 2016, 12:11:01 pm	Pending
<input type="checkbox"/>	0C:27:24:1F:47:A9	192.168.1.128	gi1/0/3	November 22nd 2016, 12:08:11 pm	Pending

Etapa 5. (Opcional) Marque a caixa de seleção ao lado do endereço MAC do dispositivo ou dispositivos que deseja adicionar à lista de bloqueio e clique em **Adicionar à lista de bloqueio**.

DAC List Management

WHITELIST

BLACKLIST

UNAUTHENTICATED DEVICES **1**

 Select one device or more from the list and then click on an action of your choice

Save to startup configuration

Add to Whitelist

Add to Blacklist

Dismiss

<input type="checkbox"/>	MAC ADDRESS	CONNECTING SWITCH	CONNECTING PORT	LAST SEEN	STATUS
<input checked="" type="checkbox"/>	0C:27:24:1F:47:A9	192.168.1.128	gi1/0/3	November 22nd 2016, 12:15:12 pm	Pending
<input type="checkbox"/>	0C:27:24:1F:47:A8	192.168.1.128	gi1/0/3	November 22nd 2016, 12:15:01 pm	 success

Etapa 6. (Opcional) Marque a caixa de seleção ao lado do endereço MAC do dispositivo ou dispositivos que deseja descartar e clique em **Dispensar**.

DAC List Management

WHITELIST BLACKLIST **UNAUTHENTICATED DEVICES** 1

i Select one device or more from the list and then click on an action of your choice

Save to startup configuration

Add to Whitelist Add to Blacklist Dismiss

<input checked="" type="checkbox"/>	MAC ADDRESS	CONNECTING SWITCH	CONNECTING PORT	LAST SEEN	STATUS
<input checked="" type="checkbox"/>	00:41:D2:A0:FA:20	192.168.1.128	gi1/0/5	November 22nd 2016, 12:34:14 pm	Pending

Note: Todos os pacotes que entram nas portas do dispositivo são autenticados no servidor RADIUS.

Agora você deve ter adicionado um dispositivo à lista Permitir ou Bloquear.

Gerenciar dispositivos na lista Permitir ou na lista Bloquear

Para gerenciar as listas de permissão ou bloqueio, clique na guia **PERMITIR LISTA** ou **BLOQUEAR**.

DAC List Management

WHITELIST **BLACKLIST** UNAUTHENTICATED DEVICES

i Select one device or more from the list and then click on an action of your choice

Save to startup configuration

Add Device

Remove from list Move to Whitelist **ADD +**

<input type="checkbox"/>	MAC ADDRESS	SEARCH	LAST SEEN
<input type="checkbox"/>	00:41:D2:A0:FA:20	<input type="text" value="Search Device"/>	

Você pode executar as seguintes tarefas nestas páginas:

- Remover da lista — Esta ação remove o dispositivo ou dispositivos escolhidos da lista.
- Mover para a lista Bloquear ou Mover para a lista Permitir — Esta ação move o dispositivo ou

dispositivos escolhidos para a lista especificada.

- Adicionar um dispositivo — Esta ação adiciona um dispositivo à lista de bloqueio ou permissão inserindo seu endereço MAC e clicando no botão **ADD+**.
- Pesquisar um dispositivo usando o endereço MAC — Insira um endereço MAC e clique no **Busca**  botão.

Agora você deve ter gerenciado os dispositivos na lista do DAC.