Configurar a Alteração de Autorização no Catalyst 1300 Usando a Interface de Usuário da Web

Objetivo

O objetivo deste artigo é mostrar como configurar a alteração de autorização (CoA) nos switches Catalyst 1300 usando a interface de usuário da Web (UI).

Dispositivos aplicáveis e versão de software

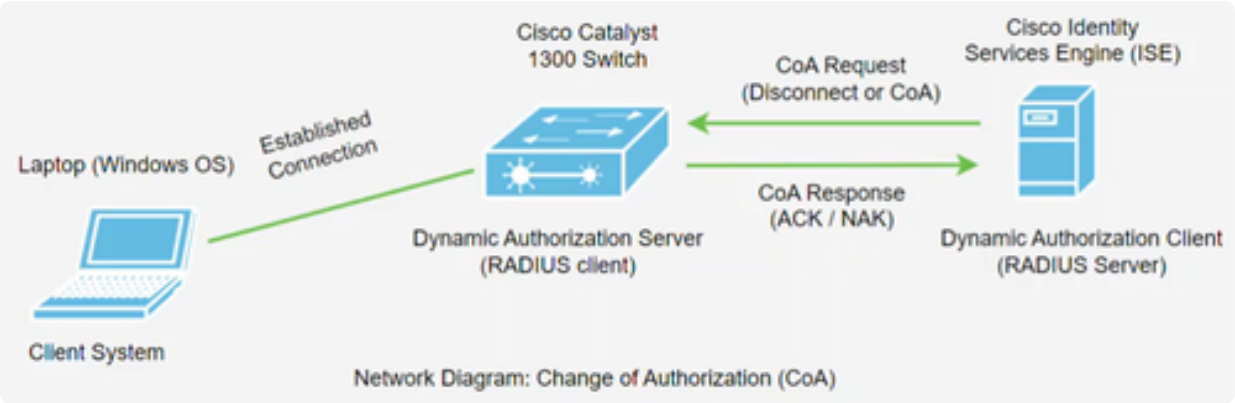
- Catalyst 1300 Switches |4.1.6.53

Introdução

Change of Authorization (CoA) é uma extensão do protocolo RADIUS, que permite alterar as propriedades de uma sessão de usuário de autenticação, autorização e relatório (AAA) ou dot1x após ser autenticada. Quando uma política para um usuário ou grupo em AAA muda, os administradores podem transmitir pacotes RADIUS CoA do servidor AAA, como um Cisco Identity Services Engine (ISE), para reinicializar a autenticação e aplicar a nova política.

O Cisco Identity Services Engine (ou ISE) é um mecanismo completo de controle de acesso baseado em rede e aplicação de políticas. Ele fornece análise e aplicação de segurança, serviços RADIUS e TACACS, distribuição de políticas e muito mais. O Cisco ISE é atualmente o único cliente de autorização dinâmica de CoA suportado para switches Catalyst 1300. Consulte o guia de administração do ISE para obter mais informações.

Este recurso requer comunicação entre o cliente de autorização dinâmica (servidor RADIUS) e o servidor de autorização dinâmica (switch Catalyst). Conforme visto no diagrama de rede abaixo, o Servidor de Autorização Dinâmico envia uma mensagem de desconexão ou CoA ao Servidor de Autorização Dinâmico e o switch fornece uma resposta.



O suporte a CoA foi adicionado aos switches Catalyst 1300 na versão 4.1.3.36 do firmware. Isso inclui suporte para desconectar usuários e alterar autorizações aplicáveis a uma sessão de usuário. O dispositivo oferece suporte às seguintes ações de CoA:

- Desconectar Sessão
- Desabilitar o comando CoA da porta do host
- comando CoA de porta de host de devolução
- Comando CoA Reauthenticate host

Para configurar o CoA usando a interface de linha de comando (CLI), consulte Configuração de Alteração de Autorização no Switch Catalyst 1300 usando CLI.

Table Of Contents

Configurando o cliente RADIUS Catalyst 1300 no ISE

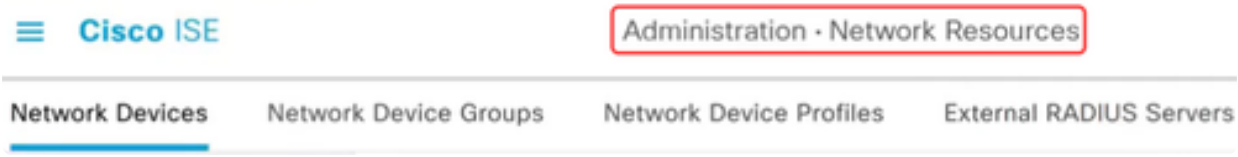
Neste exemplo, o servidor Cisco ISE versão 3.2 é usado. Para obter uma visão geral do ISE, consulte a página do produto Cisco Identity Services Engine.

> **Note:**
> CoA é suportado no ISE versão 2.7 e posterior.

Após implantar o servidor Cisco ISE, faça login para acessar a interface do usuário da Web.

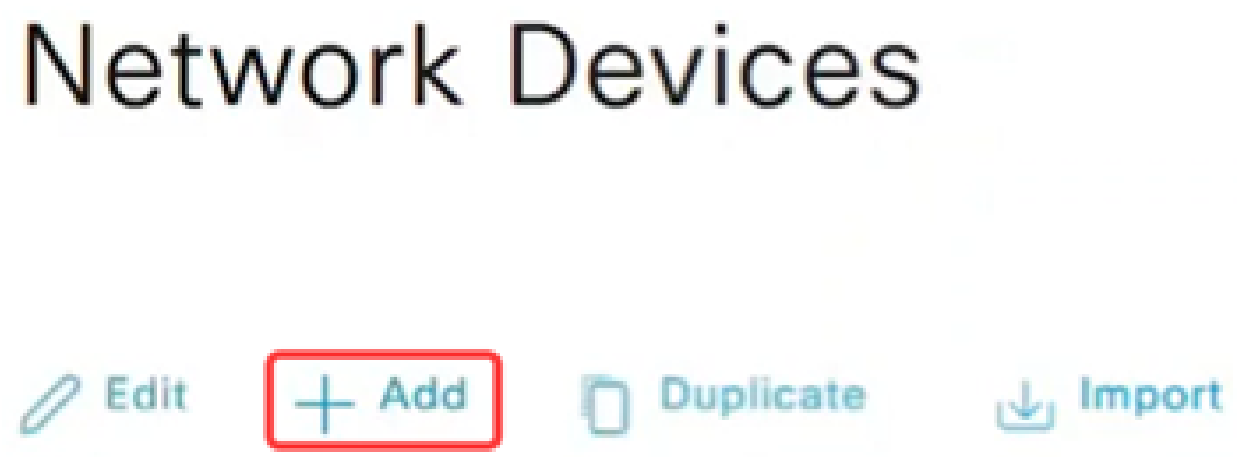
Passo 1

Para adicionar dispositivos de rede, navegue até o menu Administração > Recursos de rede.



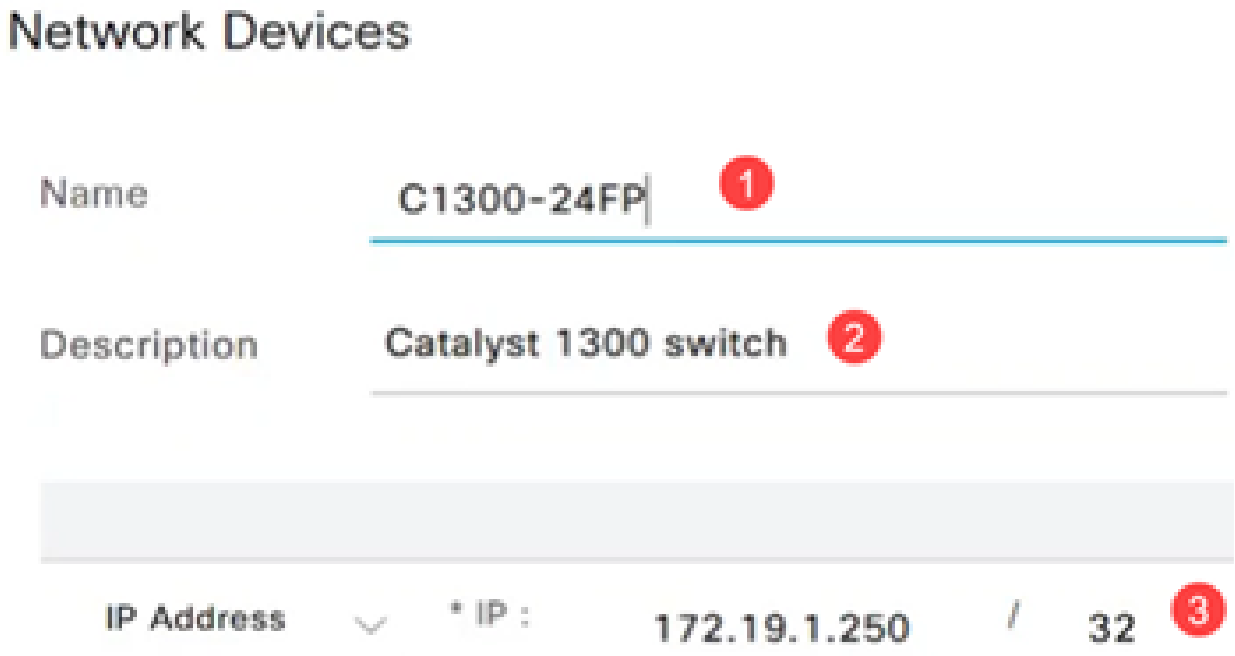
Passo 2

Clique no botão + Add.



Etapa 3

Insira o nome, a descrição e o endereço IP do switch Catalyst.

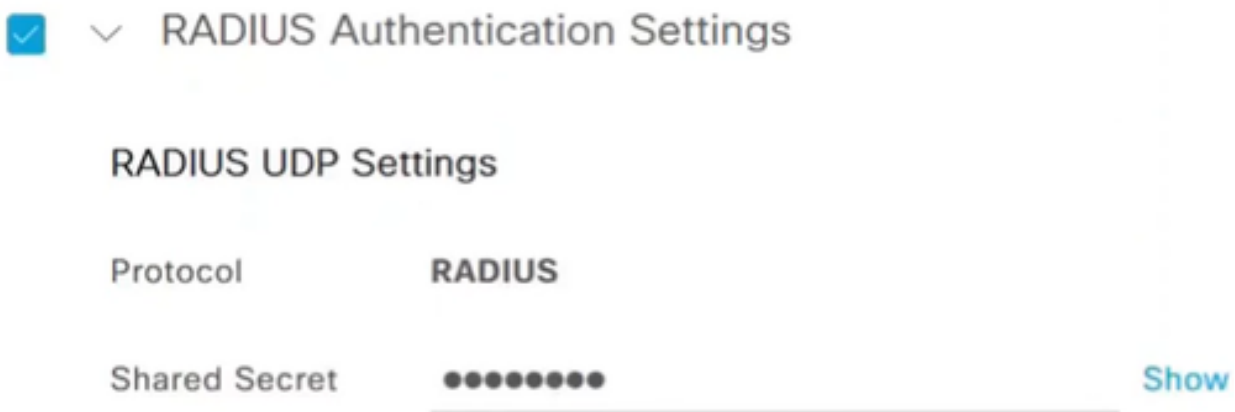


Passo 4

No menu suspenso Device Profile, selecione Cisco.

Etapa 5

Defina as configurações de autenticação RADIUS inserindo o segredo compartilhado.



Etapa 6

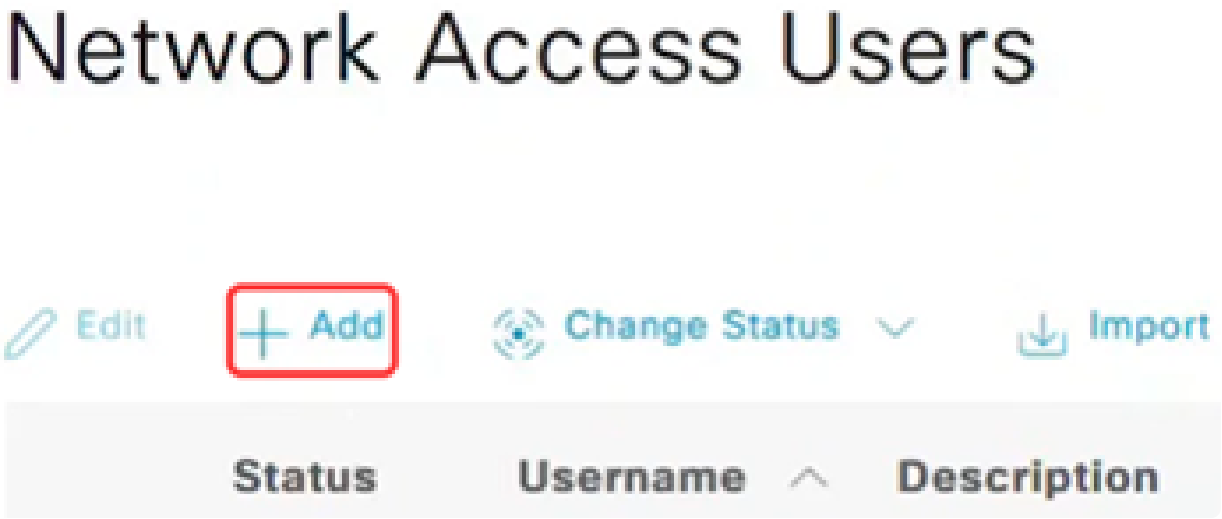
Insira o número da porta de CoA. A porta padrão é 1700.

Etapa 7

Em seguida, navegue até Administração > Gerenciamento de identidades e selecione Usuários de acesso à rede.

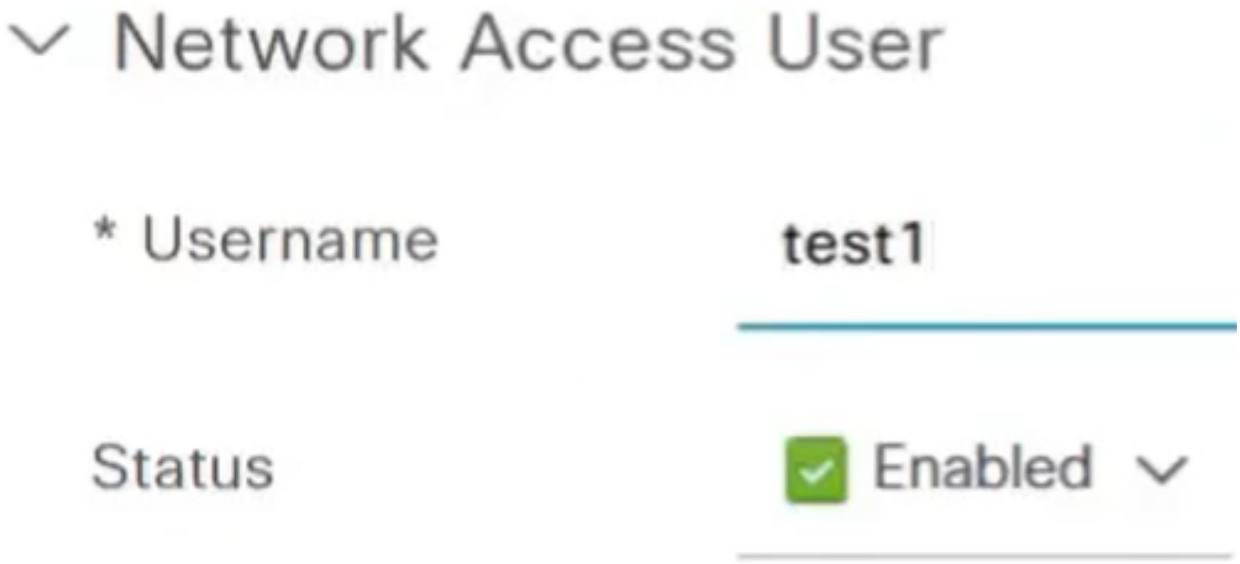
Passo 8

Para definir o nome de usuário e a senha, clique no símbolo +Add.



Passo 9

Insira o nome de usuário e a senha e clique em Save na parte inferior da página.



Configurações no Switch Catalyst 1300

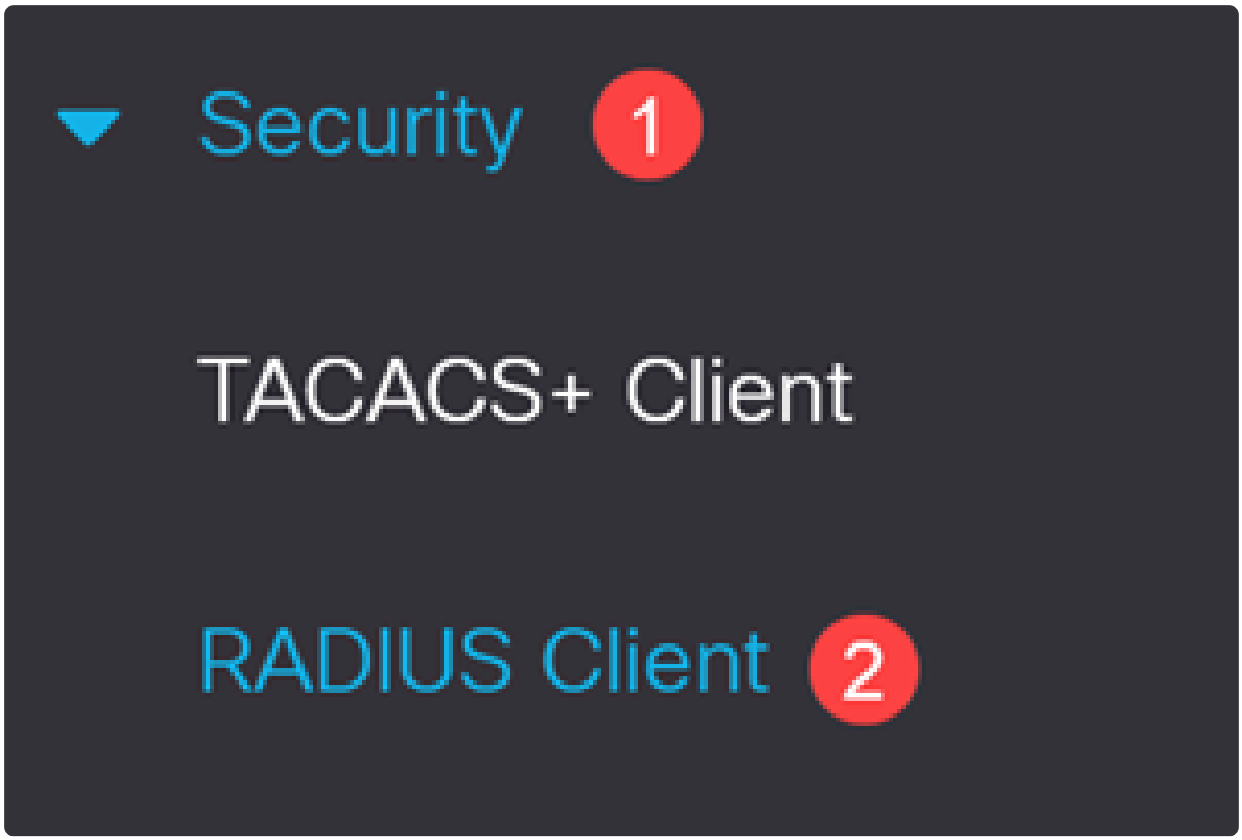
Passo 1

Faça login no switch Catalyst 1300 e selecione o modo Avançado. Neste exemplo, C1300-24FP-4X é usado.

> Note:
> O suporte a CoA foi adicionado aos switches Catalyst 1300 na versão 4.1.3.36 do firmware.

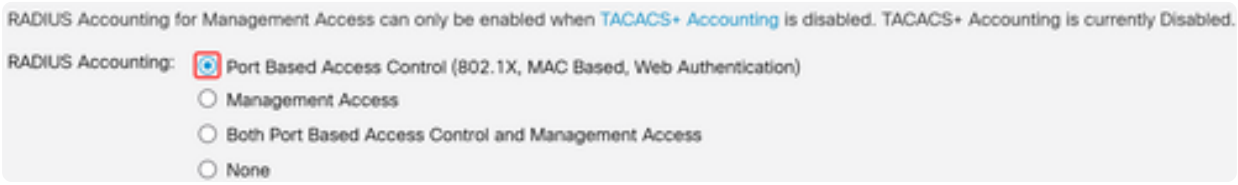
Passo 2

Navegue até Segurança > Cliente RADIUS no painel de navegação.



Etapa 3

Defina Contabilização RADIUS como Controle de Acesso Baseado em Porta.



Passo 4

Para adicionar o servidor ISE, role para baixo até a tabela RADIUS e clique no ícone de mais.

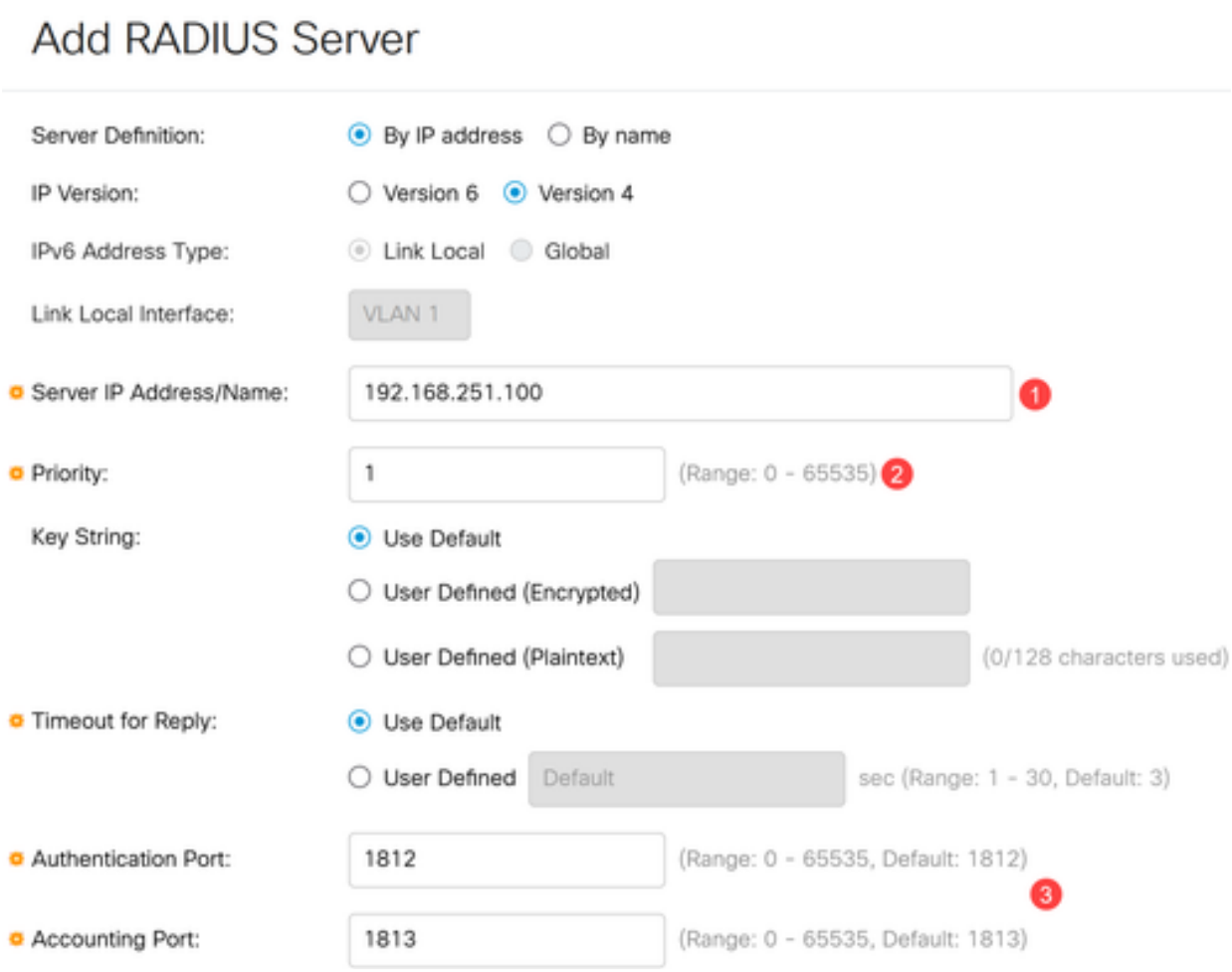
Etapa 5

Defina as configurações do servidor RADIUS.

- Selecione Server Definition. Neste exemplo, Por endereço IP está selecionado. Insira o endereço IP no campo Server IP Address/Name.
- Defina uma prioridade de RADIUS.

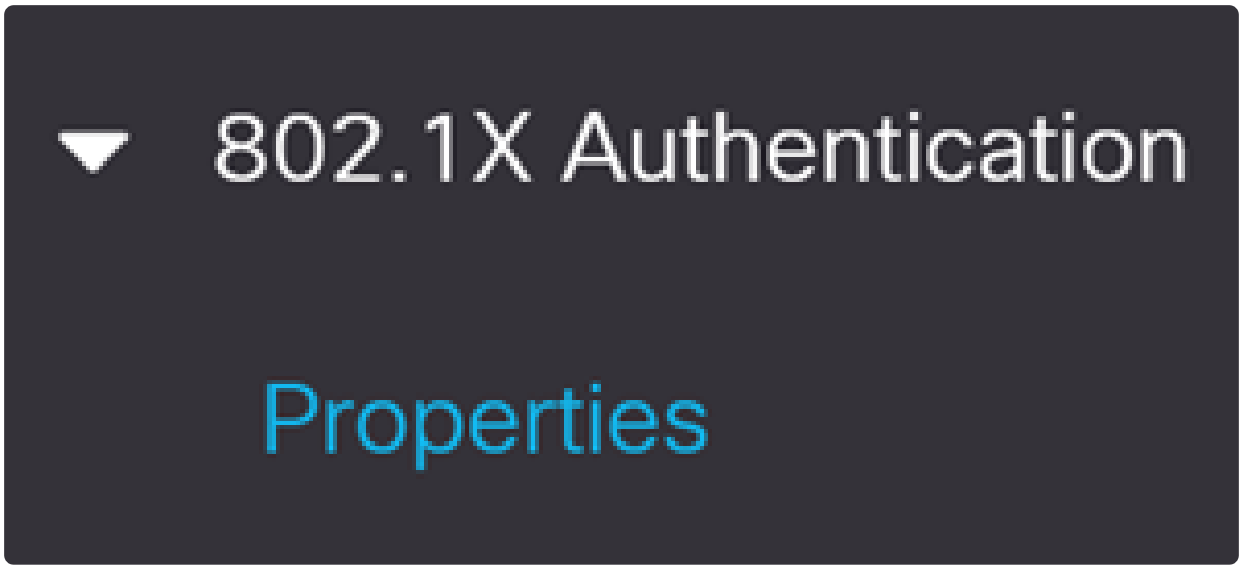
- As portas de autenticação e contabilização são definidas como o padrão.
- O tipo de uso é 802.1x.

Clique em Apply.



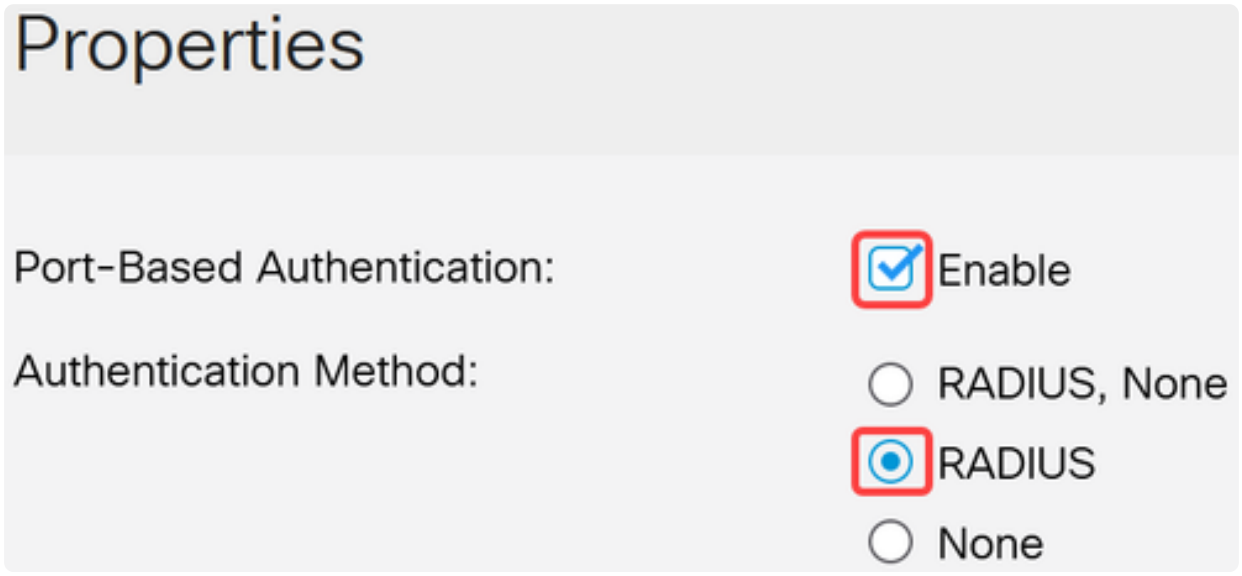
Etapa 6

Para configurar a autenticação 802.1x, navegue para o menu Security > 802.1X Authentication > Properties.



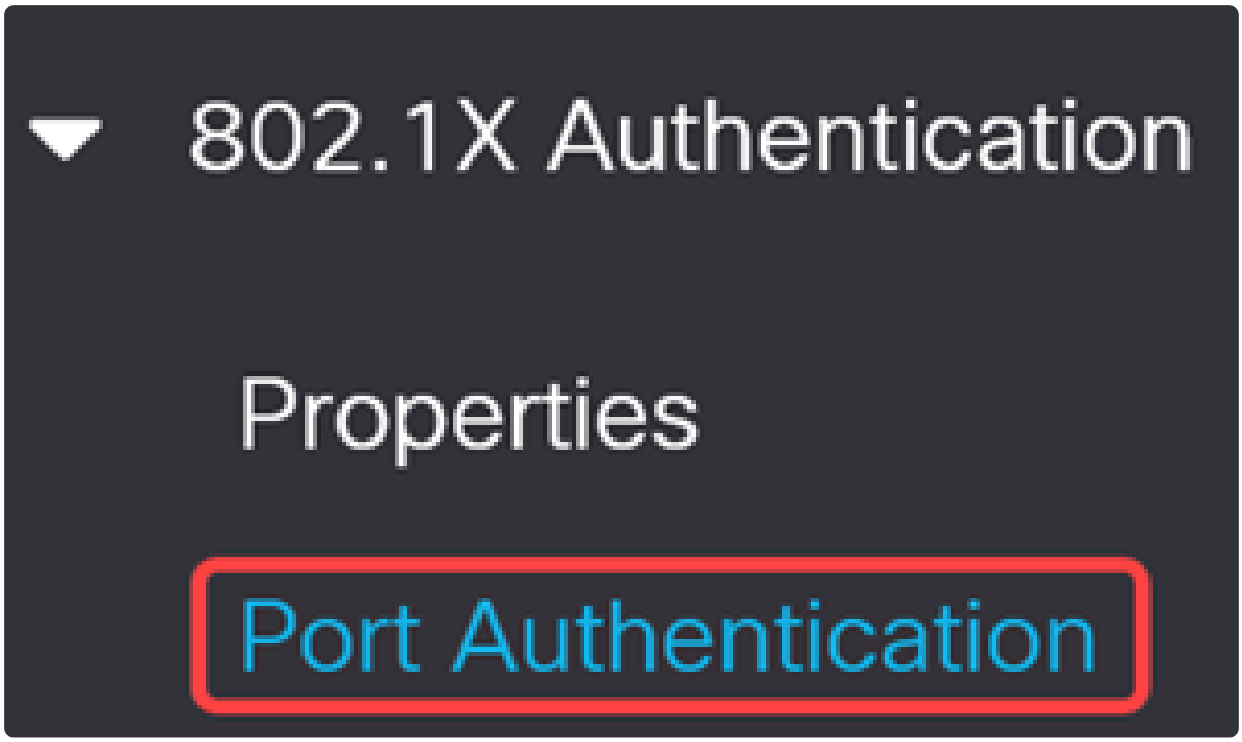
Etapa 7

Certifique-se de que a Autenticação Baseada em Porta esteja habilitada e que o Método de Autenticação esteja definido como RADIUS.



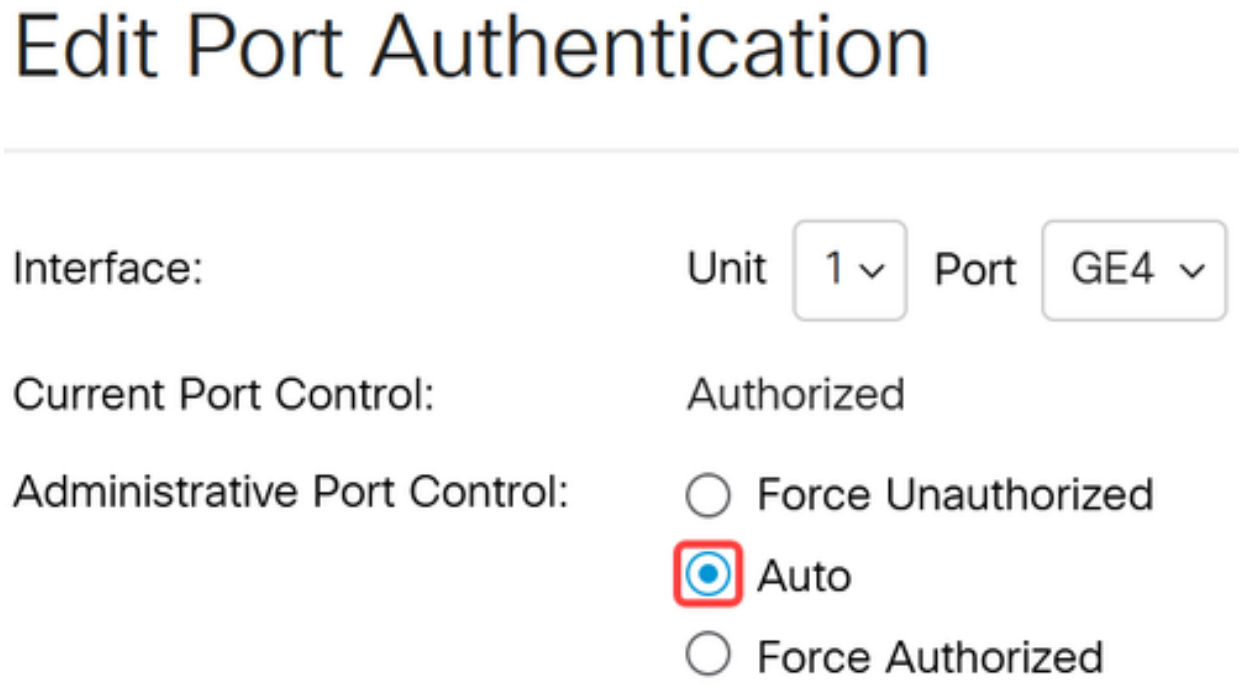
Passo 8

Navegue até o menu Autenticação de porta, selecione a porta desejada e clique em editar.



Passo 9

Para Administrative Port Control, selecione a opção Auto que alternará a porta entre o estado autorizado e não autorizado com base na resposta RADIUS.

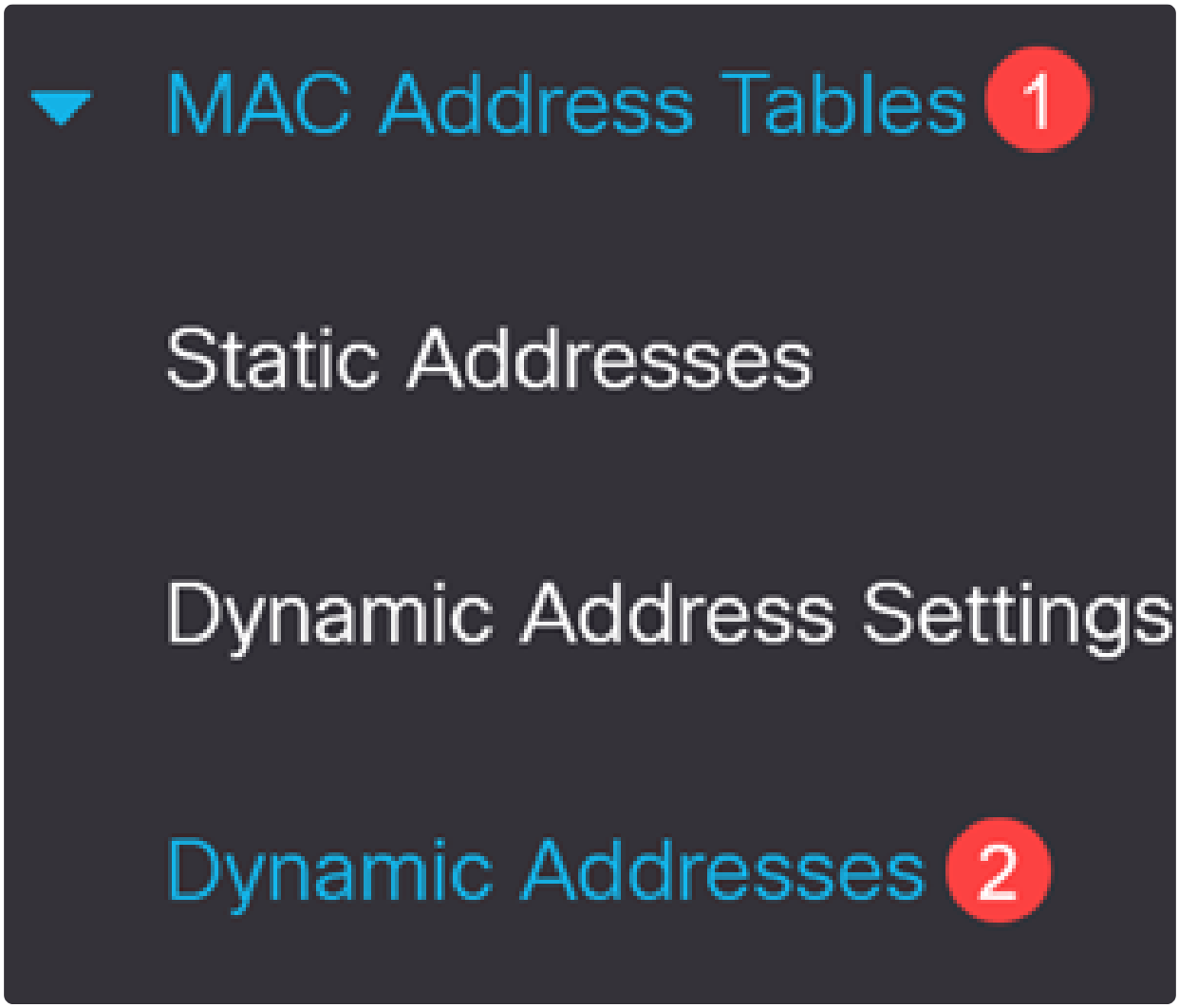


Passo 10

Habilite a autenticação baseada em 802.1x e clique em Aplicar.

Passo 11

Você precisará do endereço MAC do dispositivo na porta. A operação de CoA no ISE será aplicada a esse endereço MAC. Neste exemplo, é a porta 9. Para obtê-la, navegue até MAC Address Tables > Dynamic Addresses.

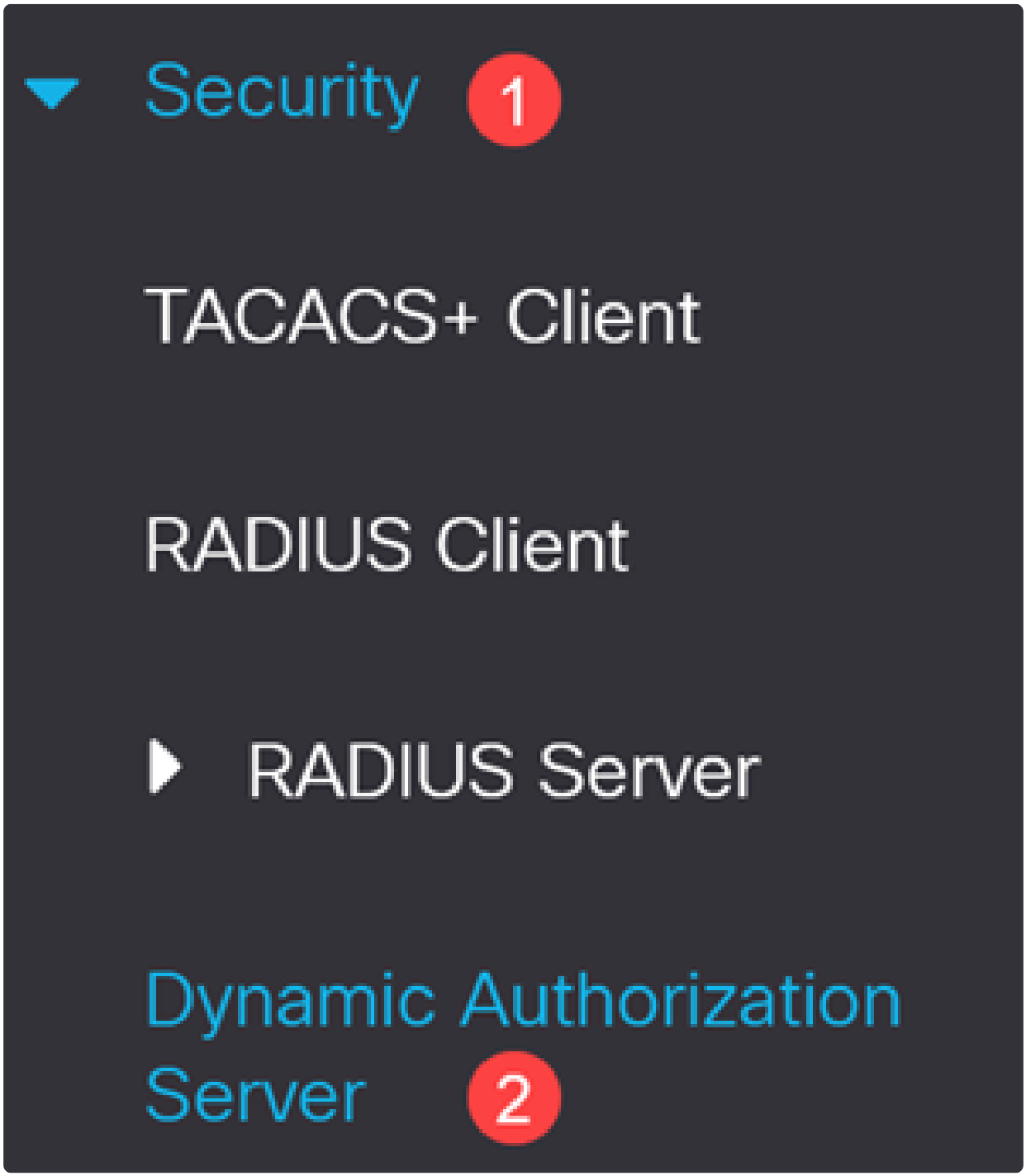


Etapa 12

Role até a porta e observe o endereço MAC.

Passo 13

Navegue até Segurança > Servidor de autorização dinâmica.

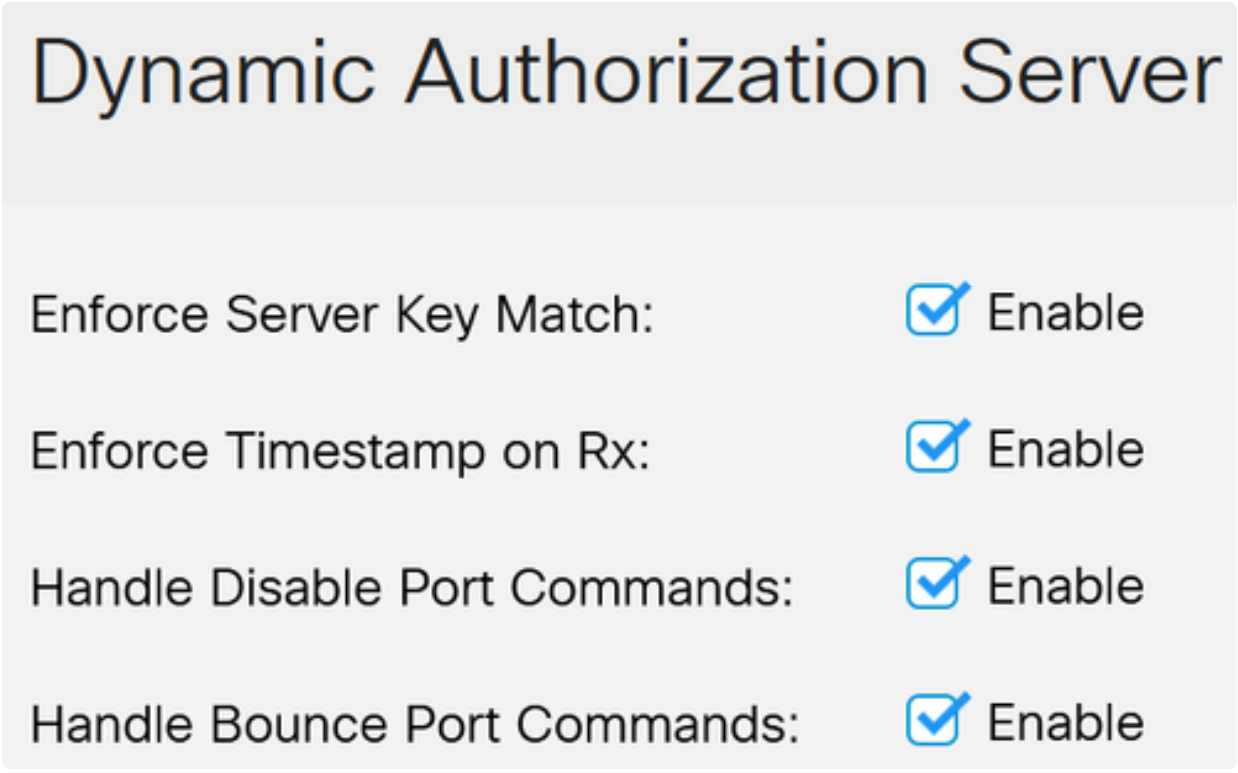


Passo 14

Habilite o seguinte:

- Aplicar Correspondência de Chave do Servidor

- Impor Carimbo de Data/Hora em Rx
- Comandos Handle Disable Port
- Tratar Comandos de Porta de Devolução

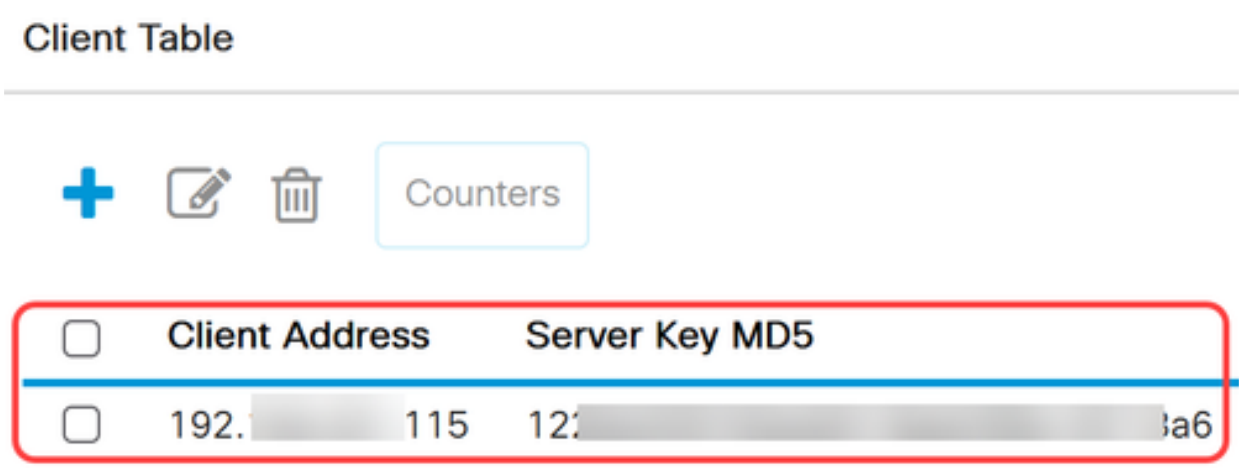


Etapa 15

Deixe a porta UDP com o valor padrão de 1700.

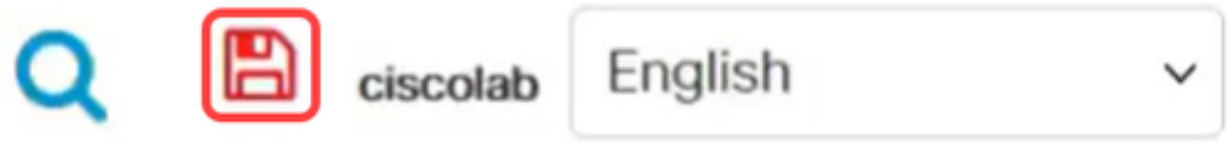
Passo 16

Em Client Table, verifique se o servidor ISE foi adicionado com a chave de servidor correta. Clique em Apply.



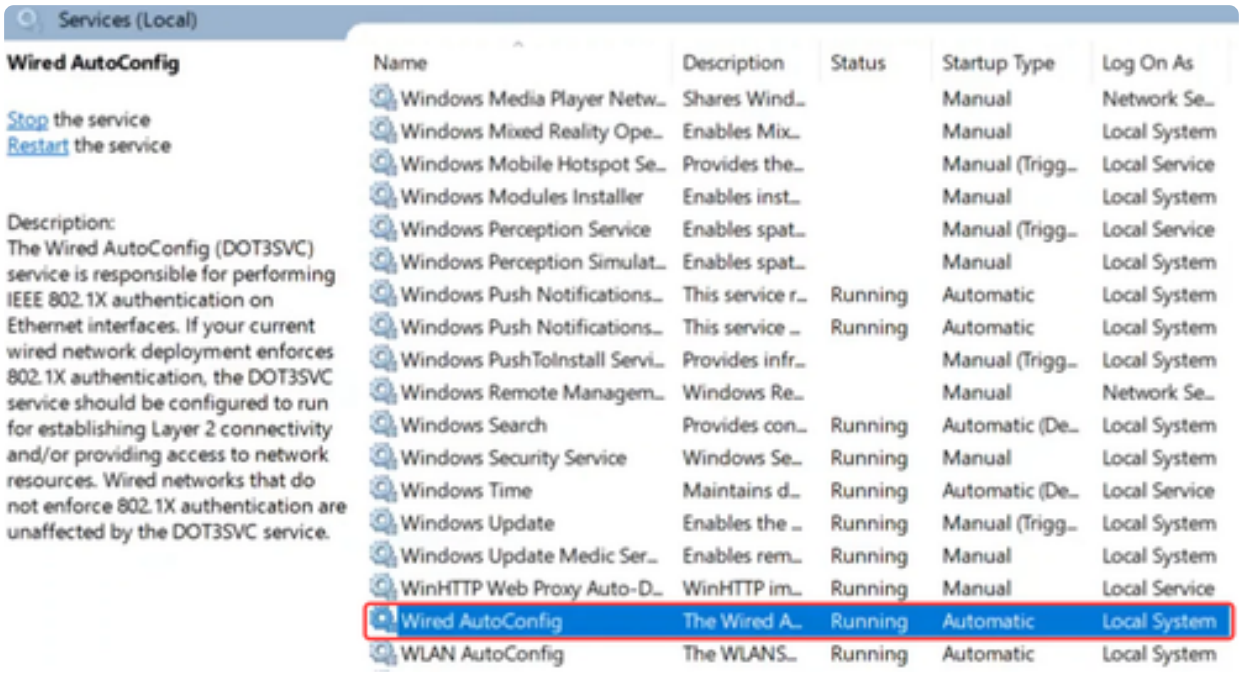
Etapa 17

Clique no ícone Save vermelho piscando para salvar as configurações.



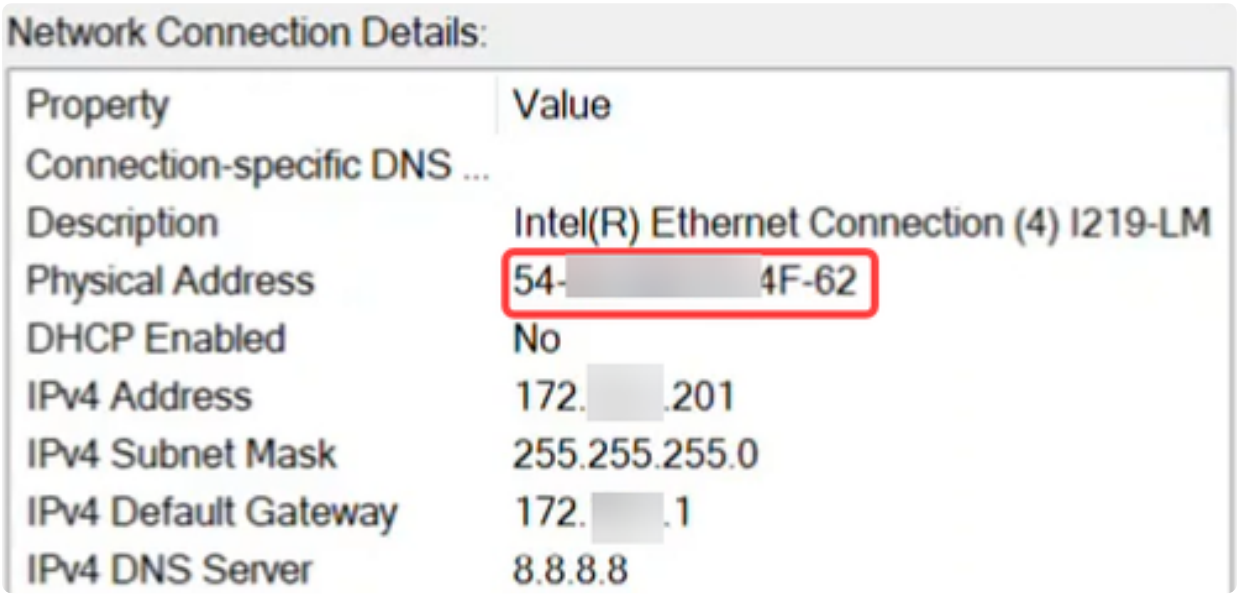
Etapa 18

No laptop do cliente conectado à porta 9, verifique se o serviço Wired AutoConfig está habilitado para a autenticação 802.1 X.



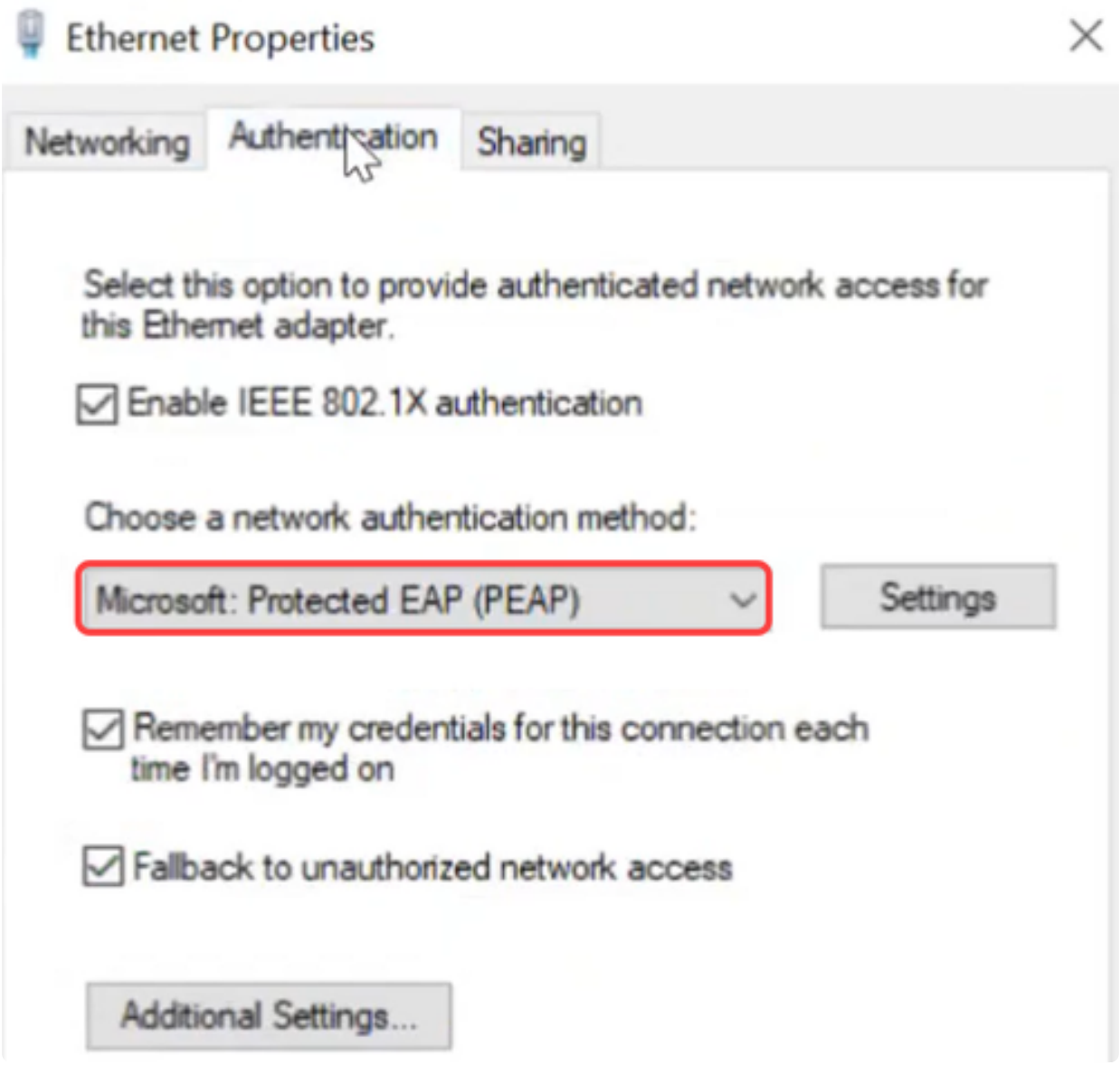
Etapa 19

Nas configurações do adaptador Ethernet, verifique se o endereço MAC corresponde.



Etapa 20

Clique no botão Properties em Ethernet settings e, na guia Authentication, certifique-se de que as caixas de seleção estejam ativadas. Além disso, verifique se o método de autenticação é Protected EAP (PEAP).



Etapa 21

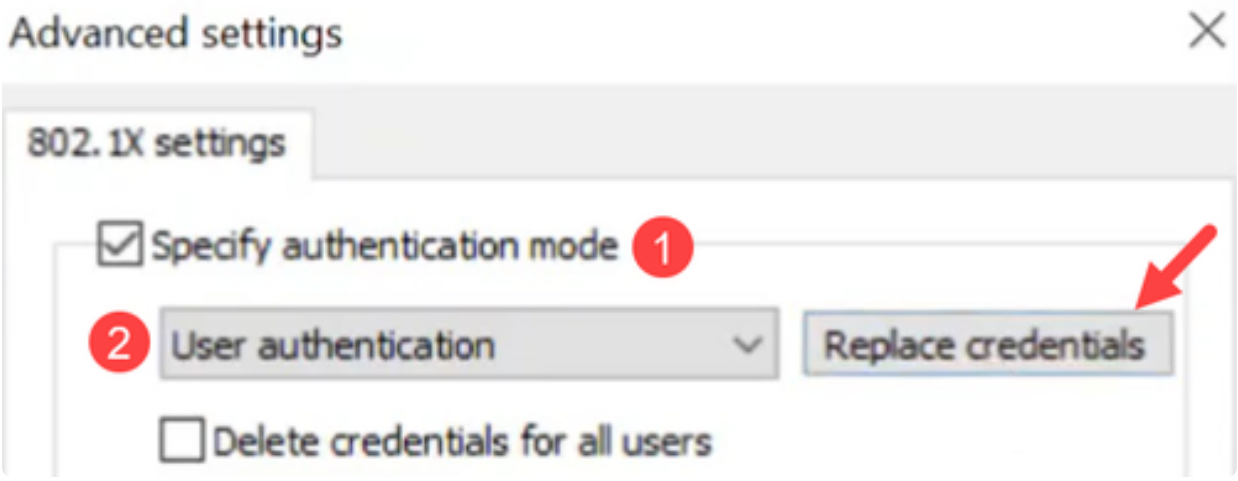
Clique no botão Settings para verificar se a caixa de seleção ao lado de Verify the server's identity by validating the certificate está desmarcada.

Etapa 22

A caixa Enable Fast Reconnect deve estar marcada.

Etapa 23

Em Additional settings (Configurações adicionais), certifique-se de que Specify authentication mode esteja habilitado e que User authentication esteja selecionado no menu suspenso. Você pode salvar as credenciais criadas no ISE ou substituí-las usando o botão Substituir credenciais.



Operação de CoA

Antes de iniciar a operação de CoA, habilite a captura de pacotes no switch.

Passo 1

No PuTTY, efetue login no switch Catalyst e especifique o tamanho do buffer e o modo de captura usando o comando monitor capture cap1 buffer size 20 circular.

Passo 2

Especifique o plano de controle como ambos usando o comando monitor capture cap1 control-plane both.

Etapa 3

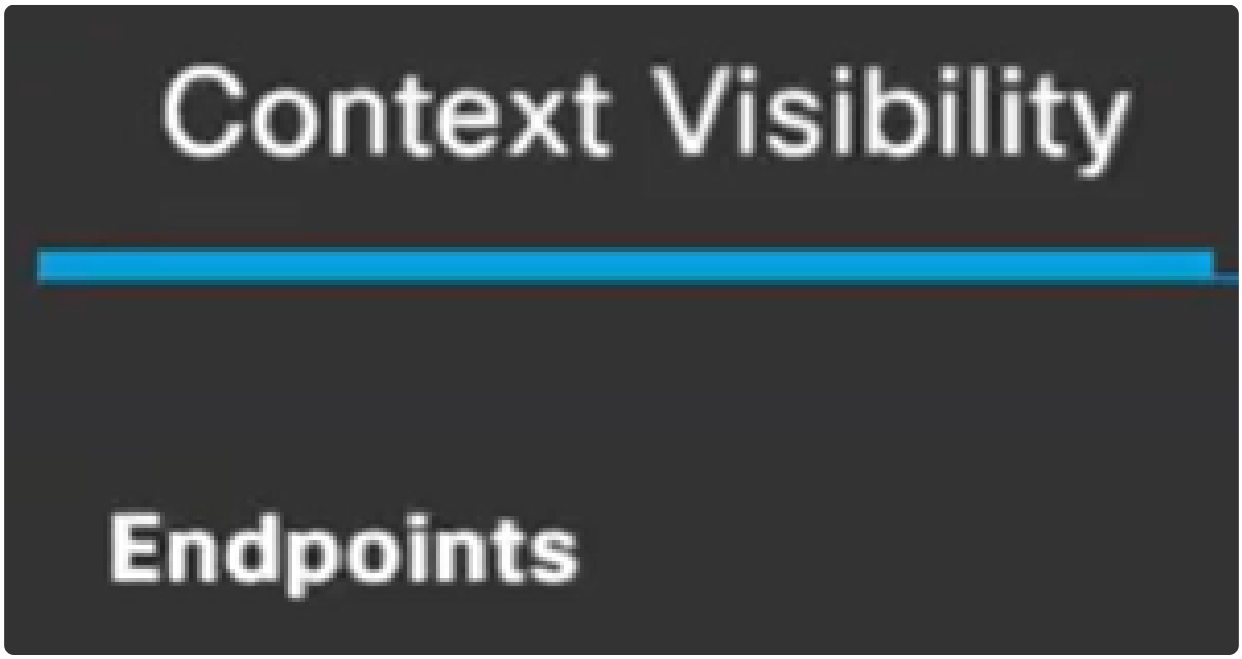
Insira os critérios de correspondência como qualquer um. O comando para isso será monitor capture cap1 match any.

Passo 4

Inicie a captura do pacote.

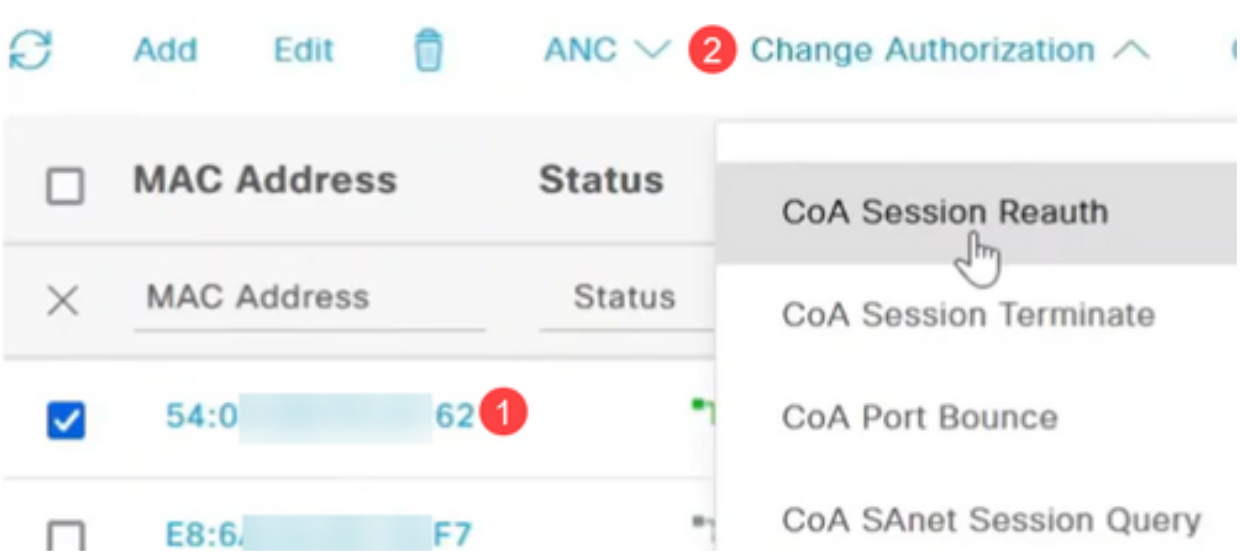
Etapa 5

Na interface do ISE, navegue até a opção Endpoints em Visibilidade de contexto.



Etapa 6

Escolha o endereço MAC e selecione a operação CoA no menu suspenso Alteração de autorização. Neste exemplo, CoA Session Reauth está selecionado. Isso força a reautenticação na porta, enviando um pacote CoA com um comando reauthenticate.



Etapa 7

Volte para o terminal PuTTY para verificar se a operação de CoA foi bem-sucedida.

```
Started capture point : capl
Cat1300-1#04-Jul-2024 20:49:45 %SEC-W-COAREAUTHSESSN: 802.1x re-authentication initiated for host 5
4:    62 by CoA Request "reauthenticate"
```

Passo 8

Se você selecionar CoA Session Terminate, ele enviará uma solicitação de desconexão com um comando terminate com base em uma solicitação administrativa.

```
Cat1300-1#04-Jul-2024 20:50:02 %SEC-W-PORTUNAUTHORIZED: Port gil/0/9 is unAuthorized
04-Jul-2024 20:50:02 %SEC-W-COADISCSESSN: 802.1x session for host 54:    :62 on interface gi
1/0/9 has been terminated by Disconnect-Request. Authenticator state on the Interface will be re-in
itialized
04-Jul-2024 20:50:02 %SEC-I-PORTAUTHORIZED: Port gil/0/9 is Authorized
```

Passo 9

A opção CoA Port Bounce enviará um pacote de solicitação de CoA com um comando bounce host port, desativando e reativando a porta no switch. O adaptador de rede fica off-line por 10 segundos e não é autorizado. Ele retornará on-line, se tornará autorizado e poderá encaminhar pacotes.

```
Cat1300-1#04-Jul-2024 20:50:21 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:          :62
04-Jul-2024 20:50:21 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:34 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:34 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:50:36 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:39 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:39 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized

Cat1300-1#04-Jul-2024 20:50:45 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

Passo 10

O término da sessão de CoA com devolução de porta encerrará a sessão existente, devolverá a porta por 10 segundos e se tornará não autorizado. Em seguida, ele volta a ficar on-line, torna-se autorizado e pode encaminhar pacotes.

```
Cat1300-1#04-Jul-2024 20:51:04 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:          :62
04-Jul-2024 20:51:04 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:51:22 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:51:22 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:51:22 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized
04-Jul-2024 20:51:29 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

Passo 11

O encerramento da sessão de CoA com o encerramento da porta encerrará a sessão e encerrará administrativamente a porta.

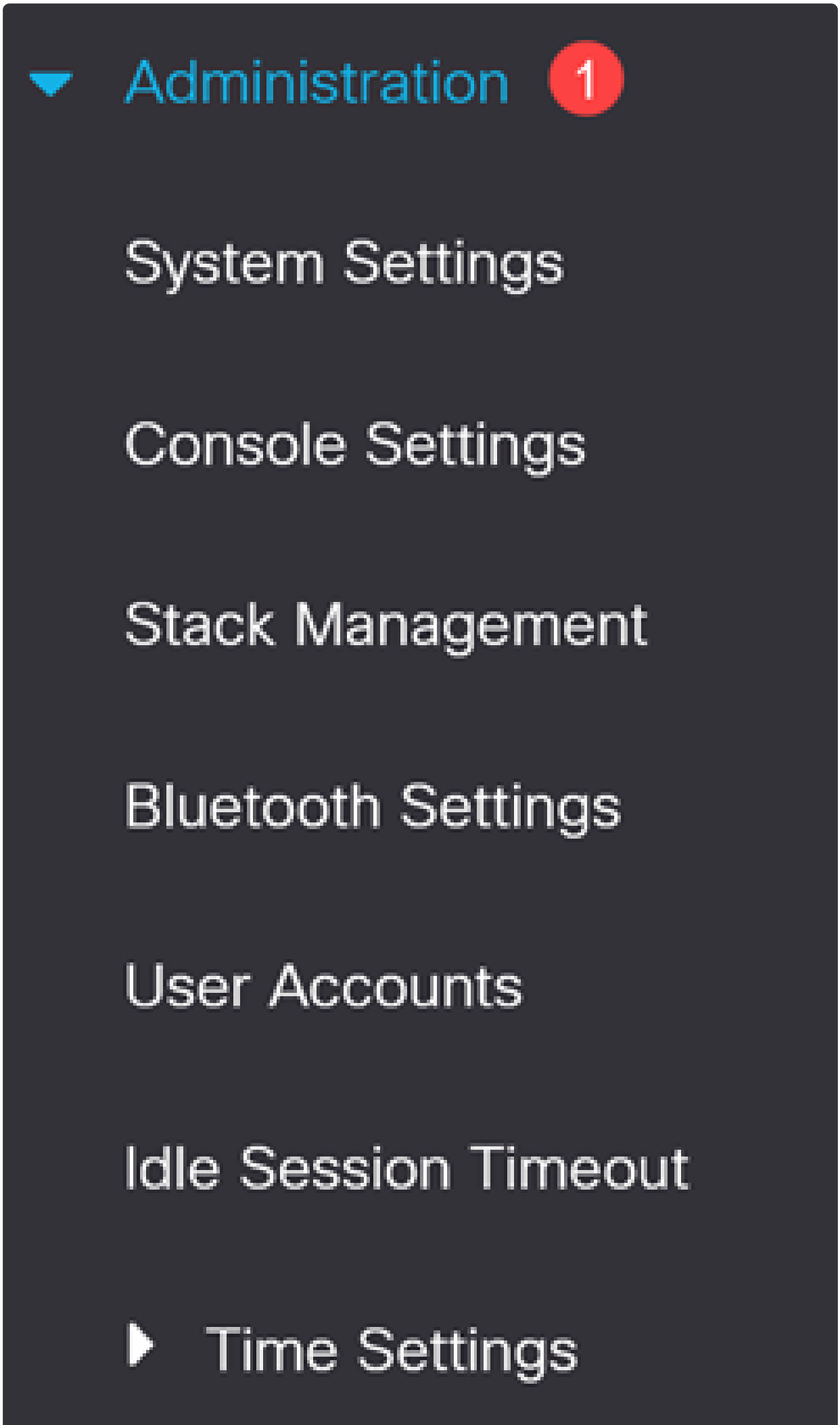
```
Cat1300-1#04-Jul-2024 20:51:47 %SEC-W-COADISPORT: Interface gi1/0/9 suspended by CoA Request "disab
le host port" for host 54:          :62
04-Jul-2024 20:51:47 %LINK-W-Down:  gi1/0/9
```

Etapa 12

Para interromper a captura de pacotes, use o comando monitor capture cap1 stop.

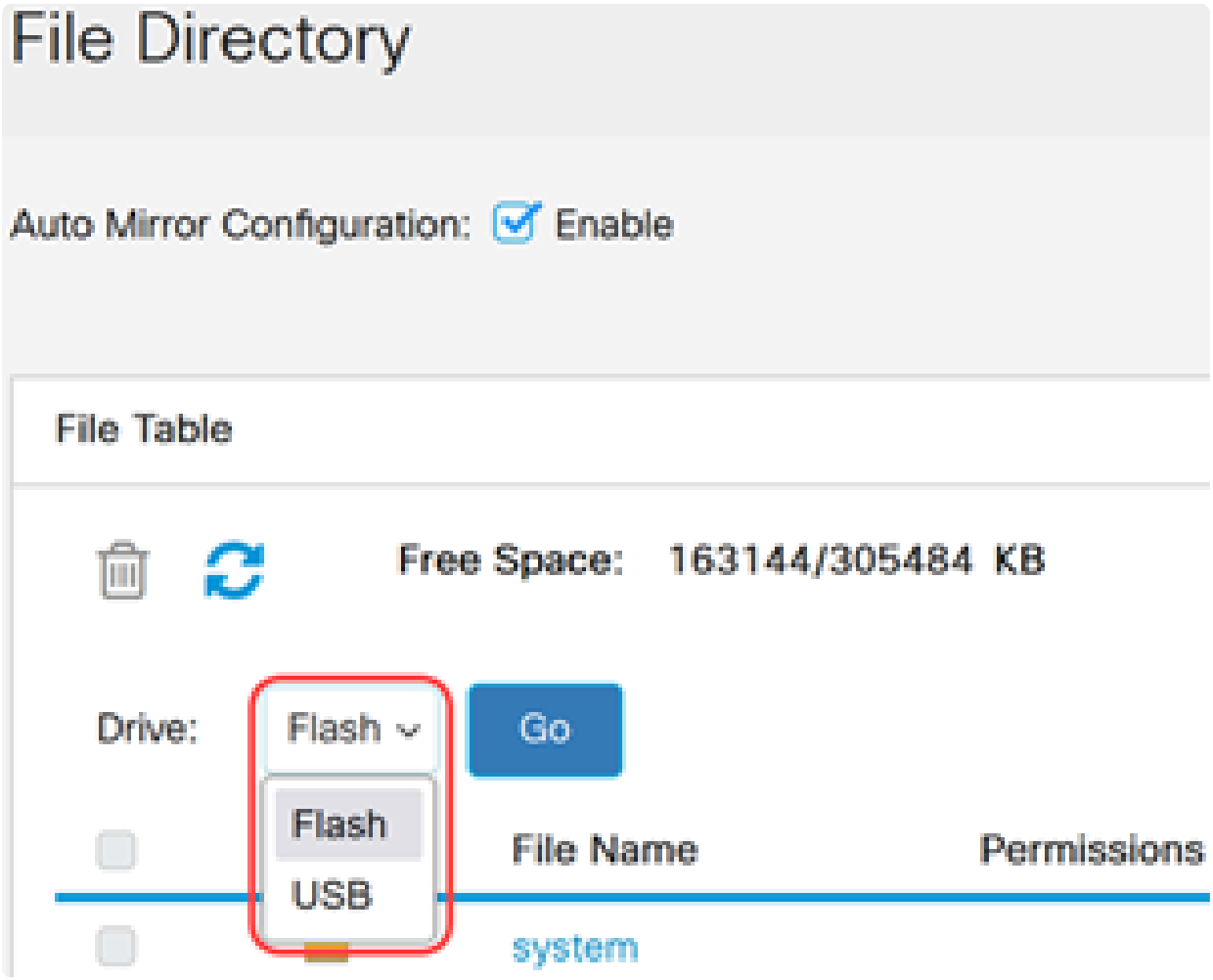
Passo 13

Para copiar os arquivos, navegue até Administração > Gerenciamento de arquivos > Diretório de arquivos.


Administration
1
System Settings
Console Settings
Stack Management
Bluetooth Settings
User Accounts
Idle Session Timeout
Time Settings

Passo 14

A Flash padrão está disponível. Como alternativa, você pode selecionar USB no menu suspenso Drive.



Conclusão

Agora você sabe tudo sobre o ISE e como configurar o CoA nos switches da série Catalyst 1300.

Para obter mais informações, confira o vídeo abaixo.

Exibir um vídeo relacionado a este artigo...

Clique aqui para ver outras palestras técnicas da Cisco

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.