

# Configurar a autenticação 802.1x nos switches Cisco Business 220 Series

## Objetivo

O objetivo deste artigo é mostrar a você como configurar a autenticação 802.1x nos switches inteligentes Cisco Business 220 Series.

## Dispositivos aplicáveis | Versão do firmware

- Série CBS220 ([Data Sheet](#)) | 2.0.0.17

## Introduction

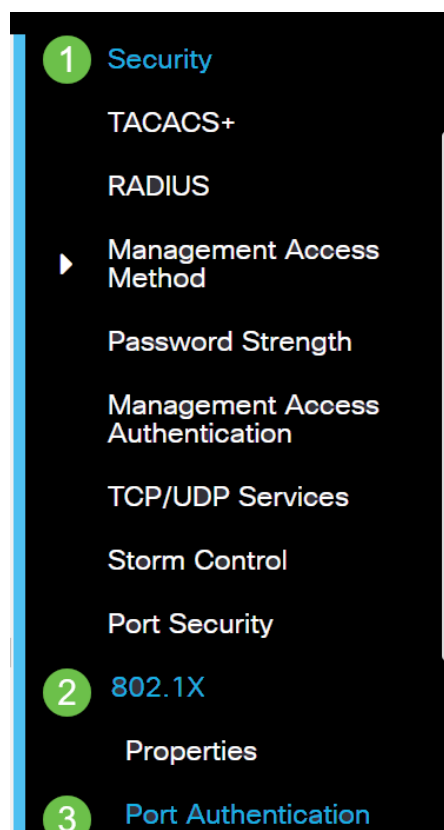
A autenticação de porta permite a configuração de parâmetros para cada porta. Como algumas alterações de configuração só são possíveis enquanto a porta está em um estado Force Authorized (Forçar autorização), como a autenticação do host, é recomendável alterar o controle de porta para Force Authorized (Forçar autorização) antes de fazer alterações. Quando a configuração estiver concluída, retorne o controle de porta ao seu estado anterior.

Uma porta com 802.1x definida nela não pode se tornar membro de um LAG. 802.1x e a segurança de porta não podem ser ativadas na mesma porta ao mesmo tempo. Se você habilitar a segurança de porta em uma interface, o controle administrativo de porta não poderá ser alterado para modo automático.

## Configurar a autenticação de porta

### Passo 1

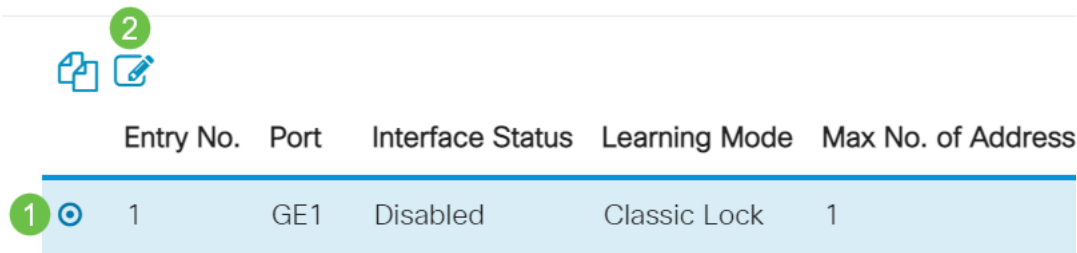
Faça login na interface de usuário da Web (UI) do switch e escolha **Security > 802.1x > Port Authentication**.



## Passo 2

Clique no botão de opção da porta que deseja configurar e clique no ícone de edição.

### Port Security Table



Entry No.	Port	Interface Status	Learning Mode	Max No. of Address
1	GE1	Disabled	Classic Lock	1

## Etapa 3

A janela *Edit Port Authentication* aparecerá. Na lista suspensa Interface, verifique se a porta especificada é a que você escolheu na Etapa 2. Caso contrário, clique na seta suspensa e escolha a porta direita.

### Edit Port Authentication

Interface:  Port GE1 ▾

## Passo 4

Escolha um botão de opção para o Controle de porta administrativo. Isso determinará o estado de autorização da porta. As opções são:

- **Desabilitado** — Desabilita 802.1x. Este é o estado padrão.
- **Force Unauthorized** — Nega o acesso à interface movendo a interface para o estado não autorizado. O switch não fornece serviços de autenticação ao cliente através da interface.
- **Auto** — Ativa a autenticação e autorização baseadas em portas no switch. A interface se move entre um estado autorizado ou não autorizado com base na troca de autenticação entre o switch e o cliente.
- **Force Authorized** — Autoriza a interface sem autenticação.

Interface:  Port GE1 ▾

Administrative Port Control:  Disabled  
 Force Authorized  
 Force Unauthorized  
 Auto

## Etapa 5 (opcional)

Escolha um botão de opção para a Atribuição de VLAN RADIUS. Isso ativará a atribuição de VLAN dinâmica na porta especificada. As opções são:

- **Desativado** — Ignora o resultado da autorização da VLAN e mantém a VLAN original do host.

Esta é a ação padrão.

- **Rejeitar** — Se a porta especificada receber uma informação de VLAN autorizada, ela usará essa informação. No entanto, se não houver nenhuma informação autorizada de VLAN, ela rejeitará o host e o tornará não autorizado.
- **Estático** — Se a porta especificada receber informações autorizadas de VLAN, ela usará as informações. No entanto, se não houver nenhuma informação autorizada de VLAN, ela manterá a VLAN original do host.

Se houver informações autorizadas de VLAN do RADIUS, mas a VLAN não for criada administrativamente no dispositivo em teste (DUT), a VLAN será criada automaticamente.

RADIUS VLAN Assignment:  Disabled  
 Reject  
 Static

**Dica rápida:** para que o recurso Atribuição dinâmica de VLAN funcione, o switch exige que os seguintes atributos de VLAN sejam enviados pelo servidor RADIUS:

- [64] Tunnel-Type = VLAN (tipo 13)
- [65] Tunnel-Medium-Type = 802 (tipo 6)
- [81] Tunnel-Private-Group-Id = VLAN ID

## Etapa 6 (Opcional)

Marque a caixa de seleção **Habilitar** para que a VLAN de convidado use uma VLAN de convidado para portas não autorizadas.

Guest VLAN:  Enable

## Etapa 7

Marque a caixa de seleção **Habilitar** para Autenticação periódica. Isso ativará as tentativas de reautenticação de porta após o Período de Reautenticação especificado.

Periodic Reauthentication:  Enable

## Passo 8

Insira um valor no campo *Período de reautenticação*. Esse é o tempo em segundos para reautenticar a porta.

Reauthentication Period: 3600

## Etapa 9 (Opcional)

Marque a caixa de seleção **Reautenticar agora** para habilitar a reautenticação imediata da porta.

O campo Estado do autenticador exibe o estado atual da autenticação.

Reauthenticate Now:  Enable

Authenticator State: Initialize

Se a porta não estiver no estado Forçar Autorizado ou Forçar Não Autorizado, ela estará no Modo Automático e o autenticador exibirá o estado da autenticação em andamento. Depois que a porta é autenticada, o estado é mostrado como Autenticado.

### Passo 10

No campo *Máximo de hosts*, insira o número máximo de hosts autenticados permitidos na porta específica. Esse valor só entra em vigor no modo de várias sessões.

Max Hosts: 256 (Range: 1 - 256, Default: 256)

### Passo 11

No campo *Quiet Period*, insira o número de segundos em que o switch permanece no estado silencioso após uma falha de troca de autenticação. Quando o switch está em um estado silencioso, isso significa que o switch não está ouvindo novas solicitações de autenticação do cliente.

Quiet Period: 60 sec (Range: 0 - 65535)

### Etapa 12

No campo *Reenviando EAP*, insira o número de segundos que o switch espera por uma resposta a uma solicitação ou quadro de identidade do EAP (Extensible Authentication Protocol) do requerente (cliente) antes de reenviar a solicitação.

Resending EAP: 30 (Range: 1 - 65535, Default: 30)

### Passo 13

No campo *Máximo de solicitações EAP*, insira o número máximo de solicitações EAP que podem ser enviadas. Se uma resposta não for recebida após o período definido (tempo limite do suplicante), o processo de autenticação será reiniciado.

Max EAP Requests: 2 (Range: 1 - 10, Default: 2)

### Passo 14


No campo *Timeout do requerente*, insira o número de segundos que faltam antes que as solicitações EAP sejam enviadas ao requerente.

Supplicant Timeout: 30 sec (Range: 1 - 65535, Default: 30)

### Etapa 15

No campo *Server Timeout*, insira o número de segundos que faltam antes que o switch reenvie

uma solicitação ao servidor de autenticação.

 Server Timeout:	30	sec (Range: 1 - 65535, Default:
---	----	---------------------------------

## Passo 16

Clique em Apply.

<input type="button" value="Apply"/>	<input type="button" value="Close"/>
--------------------------------------	--------------------------------------

Agora você deve ter configurado com êxito a autenticação 802.1x em seu switch.

Para obter mais configurações, consulte o [Guia de Administração dos Switches Cisco Business 220 Series](#).

Se quiser ver outros artigos, confira a [página de suporte do switch Cisco Business 220 Series](#)