

# Configurar a autenticação de dois fatores no console do ponto final seguro

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Controle de acesso](#)

[Autenticação de dois fatores](#)

[Configurar](#)

[Privilégios](#)

[Autenticação de dois fatores](#)

## Introduction

Este documento descreve o tipo de contas e as etapas para configurar a autenticação de dois fatores no Cisco Secure Endpoint Console.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Endpoint seguro
- Acesso ao console de endpoint seguro

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Secure Endpoint Console v5.4.20211013

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

### Controle de acesso

Há dois tipos de contas no Secure Endpoint Console: administradores e contas não privilegiadas

ou regulares. Ao criar um novo nome de usuário, você deve selecionar seu nível de privilégio, mas pode alterar seu nível de acesso a qualquer momento.

Os administradores têm controle total, podem exibir dados de qualquer grupo ou computador na organização e fazer alterações em grupos, políticas, listas e nomes de usuário.

**Note:** Um administrador pode rebaixar outro administrador em uma conta regular, mas não pode rebaixar a si mesmo.

Uma conta de usuário não privilegiada ou regular só pode exibir informações para grupos aos quais foi concedido acesso. Ao criar uma nova conta de usuário, você tem a opção de conceder privilégios de administrador a eles. Se você não conceder esses privilégios a eles, poderá selecionar os grupos, políticas e listas aos quais eles têm acesso.

## Autenticação de dois fatores

A Autenticação de dois fatores fornece uma camada adicional de segurança contra tentativas não autorizadas de acessar sua conta do Secure Endpoint Console.

# Configurar

## Privilégios

Se você for um administrador, para alterar permissões ou conceder privilégios de administrador, você poderá navegar para Contas > Usuários, selecionar a conta de usuário e escolher as permissões, veja esta imagem.

The screenshot shows the 'Privileges' configuration page. At the top, there is a search bar with the text 'Grant Administrator Privileges' and three buttons: 'Remove All Privileges', 'Revert Changes', and 'Save Changes'. Below this are three checkboxes with labels: 'Allow this user to fetch files (including Connector diagnostics) from the selected groups.', 'Allow this user to see command line data from the selected groups.', and 'Allow this user to set Endpoint Isolation status for the selected groups.' There are two main sections for selecting resources. The first is 'Groups', with a 'Clear' button and a 'Select Groups' dropdown menu. The second is 'Policies', with a 'Clear' button and a 'Select Policies' dropdown menu. Both sections currently show 'None' as the selected value. Below the 'Groups' section, there are two buttons: 'Auto-Select Policies' and 'Auto-Select Policies and Lists'.

Um administrador também pode revogar privilégios de administrador para outro administrador. Para fazer isso, você pode navegar para a conta de administrador para ver a opção, como mostrado na imagem.

## Privileges

Revoke Administrator Privileges

🔍 Administrator

👤 All Groups

⚙️ All Policies

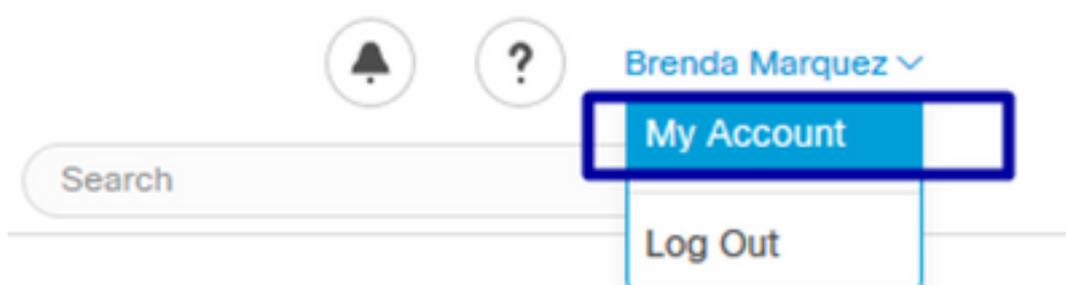
📄 All Outbreak Control Lists

**Note:** Quando as permissões do usuário alteram, alguns dados são armazenados em cache nos resultados da pesquisa para que o usuário ainda possa vê-los por um período de tempo, mesmo que não tenha mais acesso a um grupo. Na maioria dos casos, o cache é atualizado após 5 minutos.

## Autenticação de dois fatores

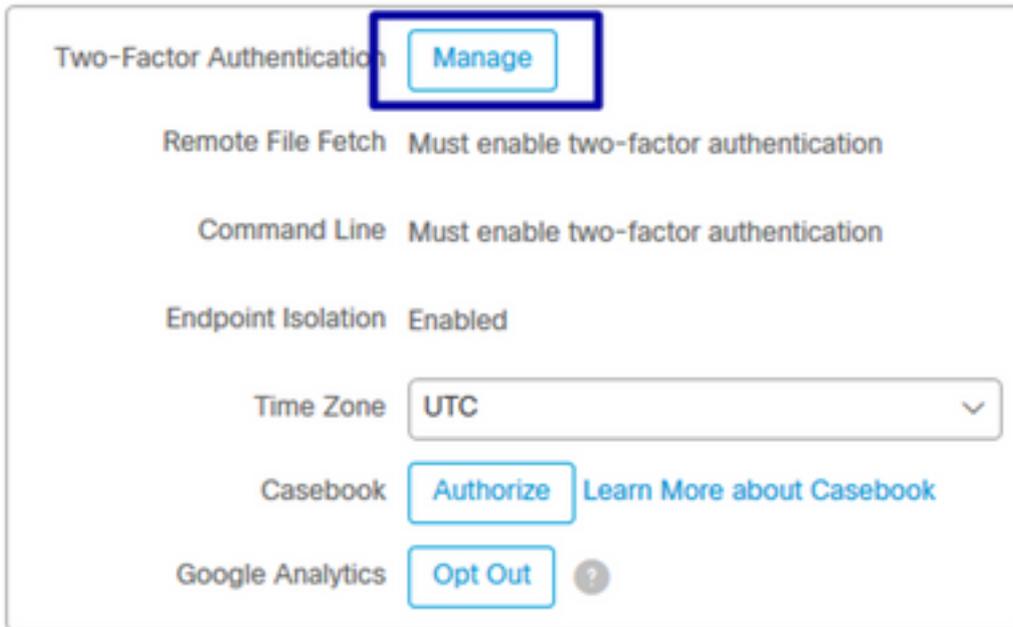
Este recurso permite que você aplique a autenticação com uma solicitação de acesso externo. Para configurar isso, siga este procedimento:

**Etapa 1.** Navegue até Minha conta na parte superior direita do Secure Endpoint Console como na imagem.



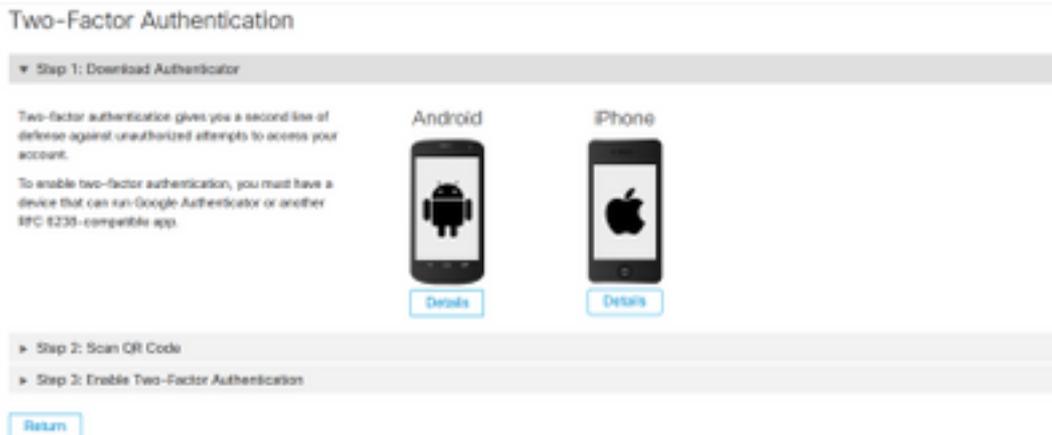
**Etapa 2.** Na seção Configurações, selecione Gerenciar para ver um guia direto com três etapas necessárias para ativar esse recurso, como mostrado na imagem.

## Settings



**Etapa 3.** Há três etapas rápidas:

a) Faça o download do autenticador, que você pode obter para Android ou iPhone que pode executar o Google Authenticator. Selecione Detalhes em qualquer um dos telefones celulares para gerar um código QR que o redireciona para a página de download. Veja esta imagem.



b) Digitalize o código QR, selecione Gerar código QR, que deve ser digitalizado pelo Google Authenticator, como mostrado nesta imagem.

## Two-Factor Authentication

► Step 1: Download Authenticator

▼ Step 2: Scan QR Code



**Warning:** This QR code is your **personal one-time code**. This should be kept secure. Generate the QR code only when you have some privacy and are ready.

Add this two-factor authentication account to your device

Click "Generate QR Code" and scan the generated QR code into Google Authenticator or another RFC 6238-compatible app.

If you cannot access your device

After completing Step 2, you will be given a set of backup codes. You can use a backup code to access your account and disable two-factor authentication until you can re-enable it with a new device. If you do not have access to any backup codes, contact Support.

**Note:** We do not recommend storing your Cisco Security password on the same device as your authenticator application. If your Cisco Security password is on the same device as your authenticator app and you lose your device, you should contact Support **immediately** to have your account password reset.

[Sample](#)  
[Generate QR Code](#)

► Step 3: Enable Two-Factor Authentication

[Return](#)

c) Ative o autenticador de dois fatores, abra o aplicativo autenticador no celular e digite o código de verificação. Selecione Habilitar para concluir este processo, como mostrado na imagem.

## Two-Factor Authentication

► Step 1: Download Authenticator

► Step 2: Scan QR Code

▼ Step 3: Enable Two-Factor Authentication

1. Open your Authenticator app.
2. Enter the verification code from Authenticator.

Enter the verification code from Authenticator.

Please enter verification code

[Enable](#)

[Return](#)

**Etapa 4.** Depois de concluído, ele fornece alguns códigos de backup. Selecione **Copiar** para a área de transferência para salvá-los, veja a imagem como um exemplo.

## Two-Factor Authentication

► Step 1: Download Authenticator

► Step 2: Scan QR Code

▼ Step 3: Enable Two-Factor Authentication

Two-Factor Authentication has been enabled. Here are your backup codes.

**Warning:** This is the only time that the backup codes are shown. If you do not make a note of them, you will need to generate a new set. Your backup codes need to be kept safe, as this will be the only way that you will be able to get into your account if you lose access to your device.

In case you cannot access your device we have generated a set of backup codes that you can use. Each backup code on the list can only be used once. You can regenerate a new list of backup codes from Two-Factor Authentication Details on the Users page. Once a new set has been generated, any backup code in the old set is no longer valid. We suggest printing this list out and keeping it somewhere safe.

**Backup Codes**

- 5c9a4c84
- f20ea786
- 7f1aeb53
- a4f59f0c
- 21a32ced
- 1e3073b1
- 42e2e189
- f54f3fde
- 7424df5f
- 3dafab11

[Copy to clipboard](#)

**Note:** Cada código de backup só pode ser usado uma vez. Depois de usar todos os códigos de backup, você deve retornar a esta página para gerar novos códigos.

Para obter mais referências, consulte o [Guia do usuário do Secure Endpoint](#).

Além disso, você pode assistir ao vídeo [Contas e Ativar a Autenticação de Dois Fatores](#).