

在安全终端控制台中配置双因素身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[访问控制](#)

[双因素身份验证](#)

[配置](#)

[权限](#)

[双因素身份验证](#)

简介

本文档介绍帐户类型以及在思科安全终端控制台中配置双因素身份验证的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全终端
- 访问安全终端控制台

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全终端控制台v5.4.20211013

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

访问控制

安全终端控制台中有两种帐户类型：管理员和非特权或常规帐户。创建新用户时，必须选择其权限级别，但可以随时更改其访问级别。

管理员拥有完全控制权，可以查看组织中任何组或计算机的数据，并对组、策略、列表和用户名进行更改。

注意：管理员可以将其他管理员降级到常规帐户，但无法降级自己。

非特权或常规用户帐户只能查看其有权访问的组的信息。创建新用户帐户时，可以选择是否授予他们管理员权限。如果不授予他们这些权限，则可以选择他们有权访问的组、策略和列表。

双因素身份验证

双因素身份验证提供额外的安全层，防止未经授权尝试访问您的安全终端控制台帐户。

配置

权限

如果您是管理员，为了更改权限或授予管理员权限，您可以导航至“帐户”>“用户”选择用户帐户并选择权限，请参阅此图像。

The screenshot shows a 'Privileges' configuration page. At the top, there is a search bar with 'Grant Administrator Privileges' and three buttons: 'Remove All Privileges', 'Revert Changes', and 'Save Changes'. Below this are three checkboxes for permissions: '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 groups and policies. The 'Groups' section has a search bar, a 'Clear' button, and a 'Select Groups' dropdown menu. Below it are two buttons: 'Auto-Select Policies' and 'Auto-Select Policies and Lists'. The 'Policies' section has a search bar, a 'Clear' button, and a 'Select Policies' dropdown menu.

管理员还可以撤销对其他管理员的管理员权限，为此，您可以导航到管理员帐户查看选项，如图所示。

Privileges

Revoke Administrator Privileges

Administrator

All Groups

All Policies

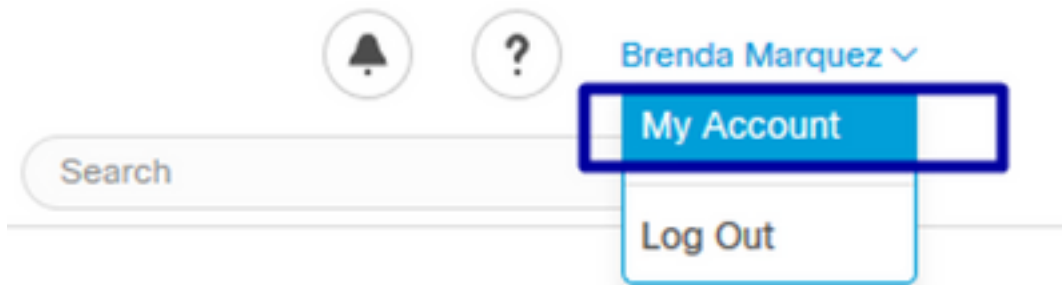
All Outbreak Control Lists

注意：当用户权限更改时，搜索结果中会缓存某些数据，因此即使用户不再具有组访问权限，用户仍能在一段时间内查看这些数据。在大多数情况下，缓存在5分钟后刷新。

双因素身份验证

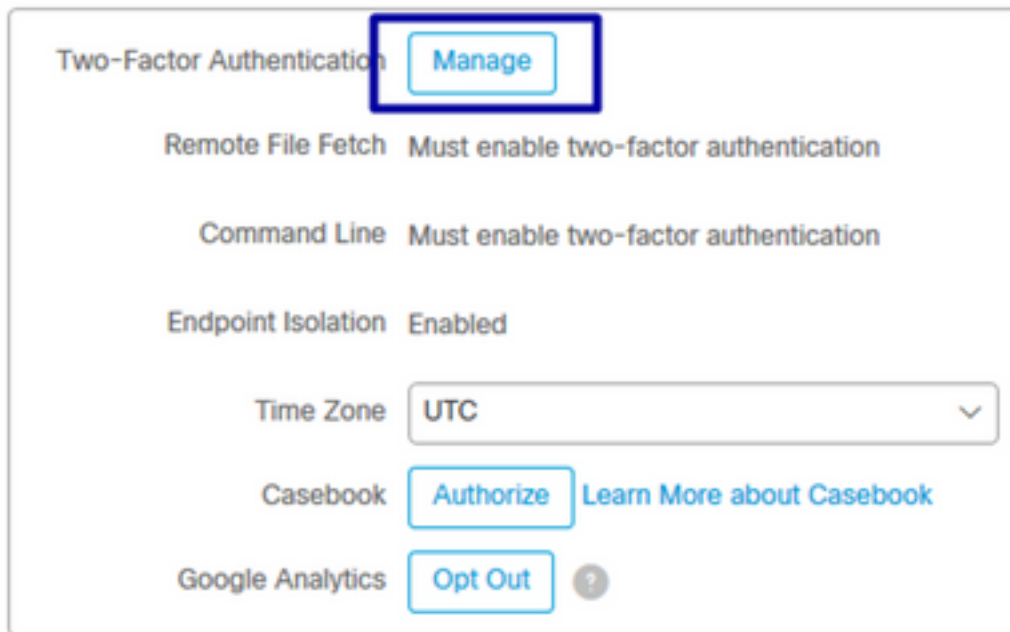
此功能允许您使用外部访问请求实施身份验证。要配置此项，请按照以下步骤操作：

步骤1.如此图中所示，导航至安全终端控制台右上方的“我的帐户”。



第2步。在“设置”部分，选择“管理”，以便查看直观的指南，其中包含启用此功能所需的三个步骤，如图所示。

Settings



步骤3.有三个快速步骤：

a) 下载身份验证器，您可以为运行Google Authenticator的Android或iPhone获取该身份验证器。在任何手机上选择Details以生成将您重定向到下载页面的QR代码。查看此图像。

Two-Factor Authentication

▼ Step 1: Download Authenticator

Two-factor authentication gives you a second line of defense against unauthorized attempts to access your account.

To enable two-factor authentication, you must have a device that can run Google Authenticator or another RFC 6238-compatible app.

Android



Details

iPhone



Details

► Step 2: Scan QR Code

► Step 3: Enable Two-Factor Authentication

Return

b)扫描QR代码，在生成QR代码(Generate QR code)上选择，该代码必须由Google身份验证器扫描，如此图像所示。

Two-Factor Authentication

► Step 1: Download Authenticator

▼ Step 2: Scan QR Code



Sample

Generate 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 3, 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.

► Step 3: Enable Two-Factor Authentication

Return

c)启用双因素身份验证器，在手机中打开身份验证器应用并输入验证代码。如图所示，选择启用完成此过程。

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

步骤4。完成后，它会提供一些备份代码。选择“复制到剪贴板”以保存它们，请以图像为例查看。

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
- 21e32ced
- 1e3073b1
- 42e2e189
- f54f3fde
- 7424df5f
- 3dafab11

Copy to clipboard

注意：每个备份代码只能使用一次。使用所有备份代码后，必须返回此页才能生成新代码。

有关进一步的参考，请参阅《[安全终端用户指南](#)》。

此外，您还可以观看“[帐户](#)”和“[启用双因素身份验证](#)”视频。