

Configure Two-Factor Authentication in the Secure Endpoint Console

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Access Control](#)

[Two-Factor Authentication](#)

[Configure](#)

[Privileges](#)

[Two-Factor Authentication](#)

Introduction

This document describes the type of accounts and the steps to configure Two-Factor Authentication in the Cisco Secure Endpoint Console.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Endpoint
- Access to the Secure Endpoint Console

Components Used

The information in this document is based on these software and hardware versions:

- 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. If your network is live, ensure that you understand the potential impact of any command.


Background Information

Access Control

There are two types of accounts in the Secure Endpoint Console: administrators and unprivileged or regular accounts. When you create a new username you must select their privilege level, but you can change their

access level at any time.

Administrators have full control, can view data from any group or computer in the organization and make changes to groups, policies, lists and usernames.

 **Note:** An administrator can demote another administrator to a regular account but cannot demote themselves.

An unprivileged or regular user account can only view information for groups they have been given access to. When you create a new user account, you have the choice of whether to grant them administrator privileges. If you do not grant them those privileges, you can select which groups, policies and lists they have access to.

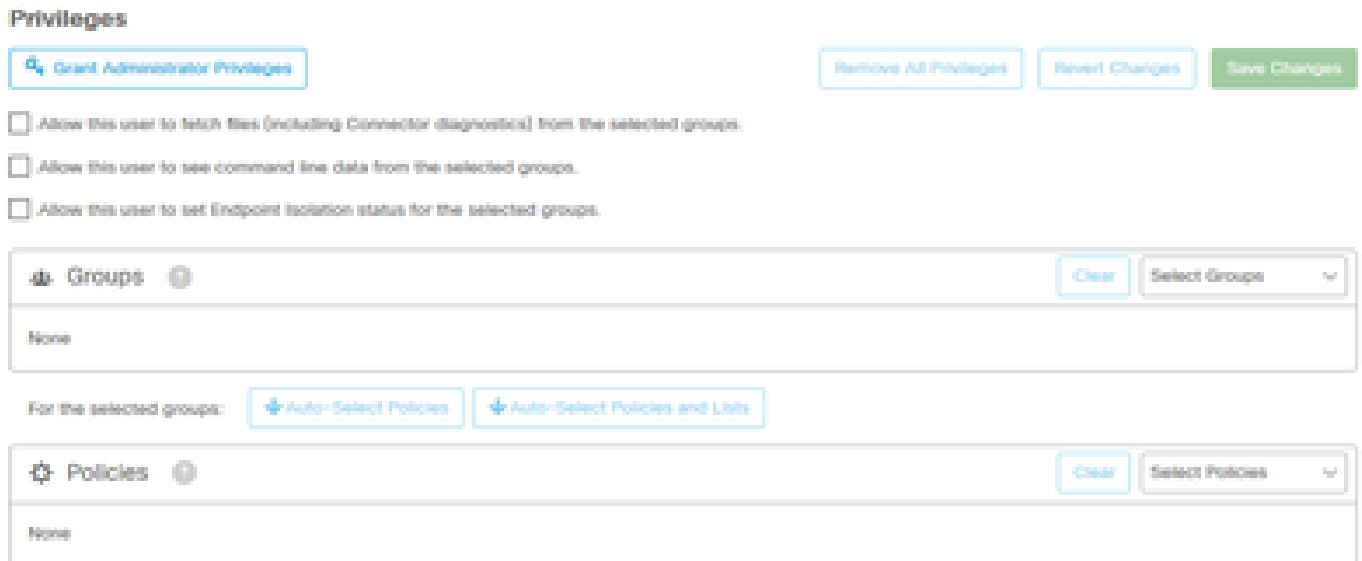
Two-Factor Authentication

Two-Factor Authentication provides an additional layer of security against unauthorized attempts to access your Secure Endpoint Console account.

Configure

Privileges

If you are an administrator, in order to change permissions or grant administrator privileges, you can navigate to Accounts > Users select the user account and choose the permissions, see this image.



Privileges

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.

Allow this user to set Endpoint Isolation status for the selected groups.

Groups

None

For the selected groups:

Policies


None

An administrator also can revoke administrator privileges to another administrator, to do this you can navigate to the administrator account to see the option, as shown in the image.

Privileges


Revoke Administrator Privileges

 Administrator

 All Groups

 All Policies

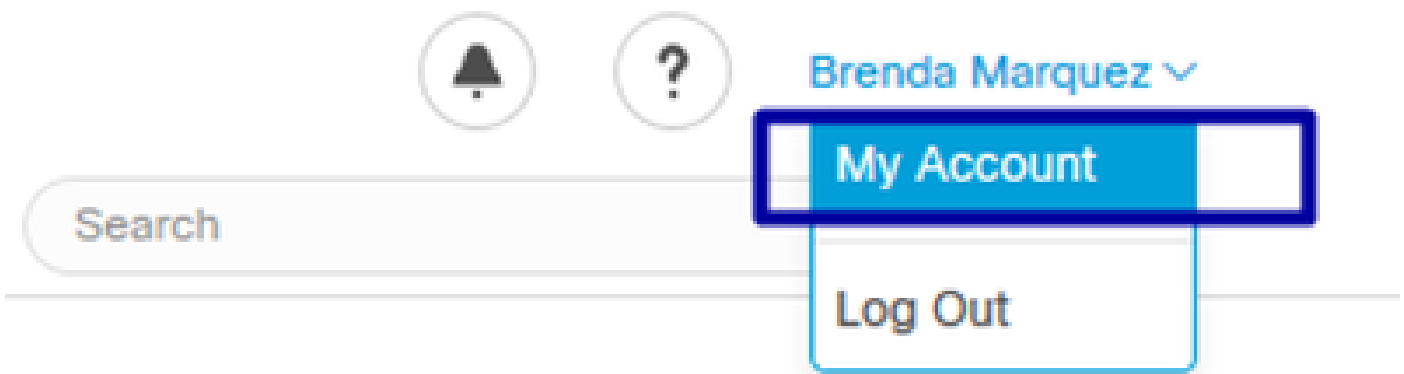
 All Outbreak Control Lists

 **Note:** When user permissions change some data is cached in Search results so a user is still able to see it for a period of time even though they no longer have access to a group. In most cases, the cache is refreshed after 5 minutes.

Two-Factor Authentication

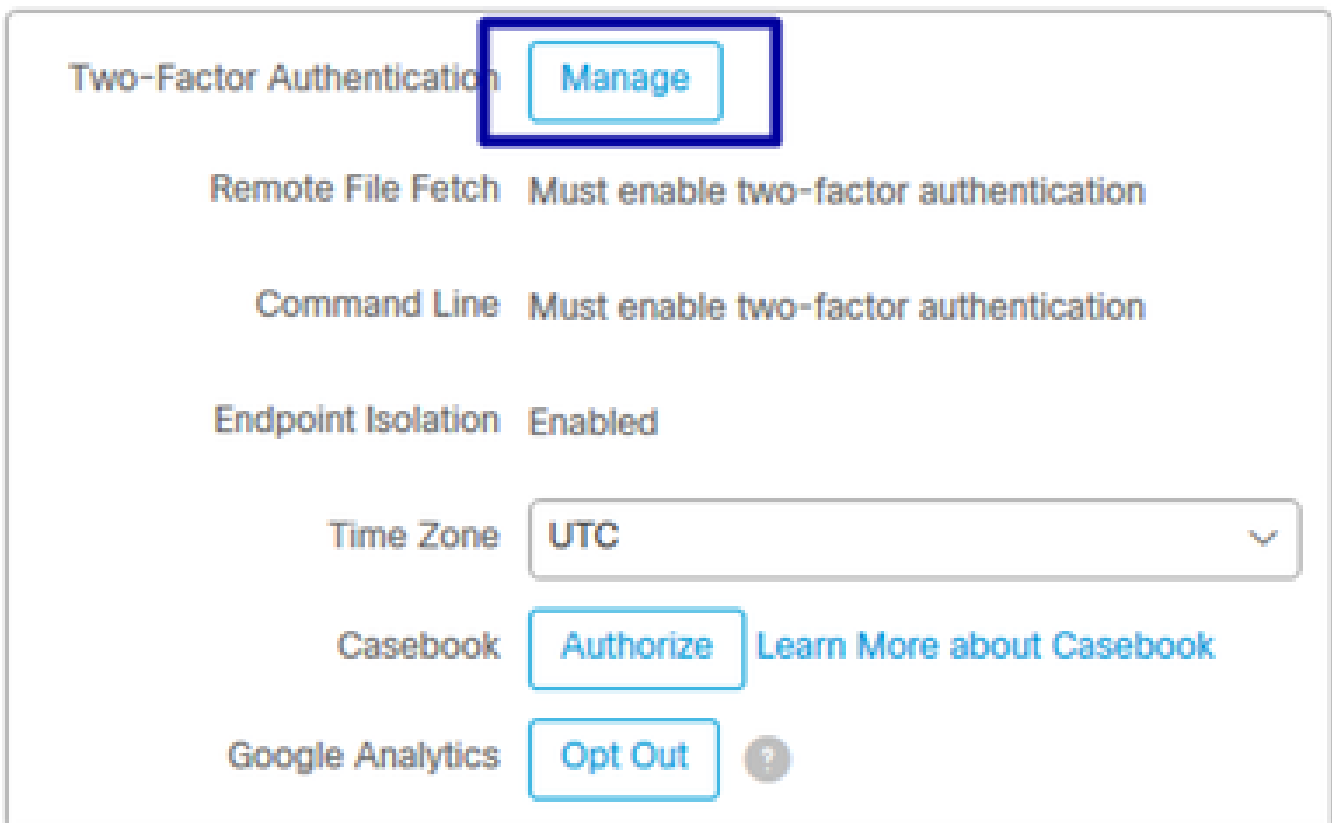
This feature allows you to enforce the authentication with an external access request. In order to configure this, follow this procedure:

Step 1. Navigate to My Account at the right top of the Secure Endpoint Console as in this image.



Step 2. In the Settings section select Manage, in order to see a straightforward guide with three steps needed to enable this feature, as shown in the image.

Settings



Step 3. There are three quick steps:

a) Download authenticator, which you can obtain for Android or iPhone that can run Google Authenticator. Select Details on any of the cell phones to generate a QR code that redirects you to the download page. See this image.

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) Scan QR code, select on Generate QR code, it that has to be scanned by Google Authenticator as shown in this image.

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) Enable Two-Factor authenticator, open your authenticator application in your cellular phone and enter the verification code. Select Enable to finish this process, as shown in the image.

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

Step 4. Once it is done, it gives you some backup codes. Select **Copy** to clipboard in order to save them, see the image as an example.


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

- 5c8a4c86
- 220ea7d6
- 7f1aeb53
- a4f59f0c
- 21e33ced
- 1e3d73b1
- 42e2e109
- f56f3fde
- 7426ed5f
- 28a7ab11

Copy to clipboard

 **Note:** Each backup code can only be used one time. After you have used all your backup codes you must return to this page in order to generate new codes.

For further reference, you can consult the [Secure Endpoint User Guide](#).

Additionally, you can watch the [Accounts and Enable Two-Factor Authentication](#) video.