

Configuración de la Autenticación de Dos Factores en la Consola de Extremo Seguro

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Control de acceso](#)

[Autenticación de dos factores](#)

[Configurar](#)

[Privilegios](#)

[Autenticación de dos factores](#)

Introducción

Este documento describe el tipo de cuentas y los pasos para configurar la Autenticación de Dos Factores en Cisco Secure Endpoint Console.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Terminal seguro
- Acceso a la consola de terminales seguros

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Consola de terminal seguro 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Control de acceso

Hay dos tipos de cuentas en Secure Endpoint Console: administradores y cuentas normales o no privilegiadas. Al crear un nuevo nombre de usuario, debe seleccionar su nivel de privilegio, pero puede cambiar su nivel de acceso en cualquier momento.

Los administradores tienen un control completo, pueden ver los datos de cualquier grupo o equipo de la organización y realizar cambios en grupos, políticas, listas y nombres de usuario.

Nota: Un administrador puede degradar a otro administrador a una cuenta normal pero no puede degradarse a sí mismo.

Una cuenta de usuario normal o sin privilegios solo puede ver información de los grupos a los que se les ha concedido acceso. Al crear una nueva cuenta de usuario, puede elegir entre concederles privilegios de administrador. Si no les concede esos privilegios, puede seleccionar a qué grupos, políticas y listas tienen acceso.

Autenticación de dos factores

La autenticación de dos factores proporciona una capa adicional de seguridad contra los intentos no autorizados de acceder a su cuenta de consola de terminales seguros.

Configurar

Privilegios

Si es administrador, para cambiar permisos o conceder privilegios de administrador, puede navegar hasta Cuentas > Usuarios seleccionar la cuenta de usuario y elegir los permisos, consulte esta imagen.

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 location status for the selected groups.' There are two main sections for selecting resources. The first is 'Groups', which has a 'Clear' button and a 'Select Groups' dropdown menu. The second is 'Policies', which has a 'Clear' button and a 'Select Policies' dropdown menu. Both sections currently show 'None' as the selected value. There are also two buttons for auto-selecting policies: 'Auto-Select Policies' and 'Auto-Select Policies and Lists'.

Un administrador también puede revocar los privilegios de administrador a otro administrador, para ello puede navegar a la cuenta de administrador para ver la opción, como se muestra en la imagen.

Privileges

Revoke Administrator Privileges

🔍 Administrator

👤 All Groups

⚙️ All Policies

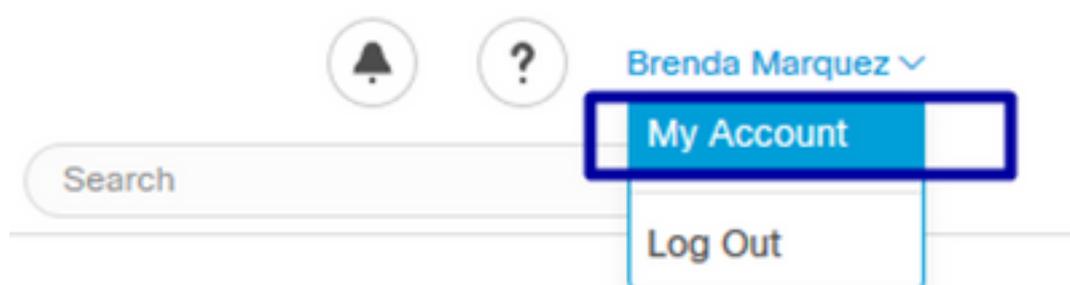
📄 All Outbreak Control Lists

Nota: Cuando los permisos de usuario cambian algunos datos se almacenan en la memoria caché en los resultados de la búsqueda, de modo que el usuario pueda verlos durante un período de tiempo aunque ya no tenga acceso a un grupo. En la mayoría de los casos, la memoria caché se actualiza después de 5 minutos.

Autenticación de dos factores

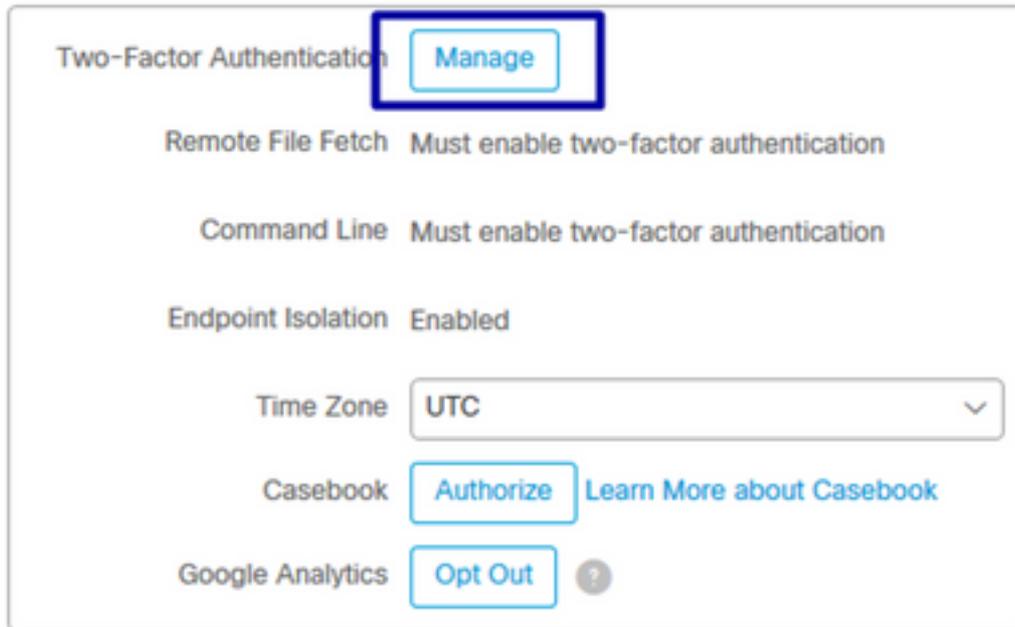
Esta función permite aplicar la autenticación con una solicitud de acceso externa. Para configurar esto, siga este procedimiento:

Paso 1. Vaya a Mi cuenta en la parte superior derecha de la Consola de terminal seguro, como en esta imagen.



Paso 2. En la sección Settings (Configuración), seleccione Manage (Administrar) para ver una guía sencilla con tres pasos necesarios para habilitar esta función, como se muestra en la imagen.

Settings



Two-Factor Authentication [Manage](#)

Remote File Fetch Must enable two-factor authentication

Command Line Must enable two-factor authentication

Endpoint Isolation Enabled

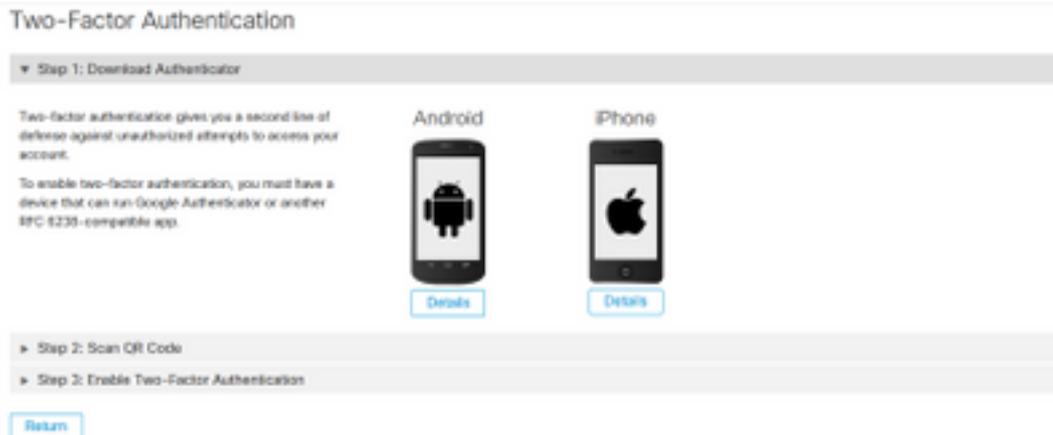
Time Zone

Casebook [Authorize](#) [Learn More about Casebook](#)

Google Analytics [Opt Out](#) 

Paso 3. Hay tres pasos rápidos:

a) Descargar autenticador, que puede obtener para Android o iPhone que pueden ejecutar Google Authenticator. Seleccione Detalles en cualquiera de los teléfonos móviles para generar un código QR que le redirija a la página de descarga. Vea esta imagen.



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) Escanee el código QR, seleccione Generar código QR, que debe ser analizado por Google Authenticator como se muestra en esta imagen.

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) Habilite el autenticador de dos factores, abra la aplicación de autenticación en su teléfono móvil e introduzca el código de verificación. Seleccione Enable (Activar) para finalizar este proceso, como se muestra en la imagen.

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

Paso 4. Una vez hecho, le proporciona algunos códigos de respaldo. Seleccione **Copiar** al portapapeles para guardarlos, vea la imagen como ejemplo.

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

- 5c9a4c086
- f20ea706
- 7f1aeb53
- a4f50f0c
- 21e32ced
- 1e307301
- 42e2e109
- f56f3fde
- 7424df5f
- 2dafab11

Copy to clipboard

Nota: Cada código de copia de seguridad sólo se puede utilizar una vez. Después de haber utilizado todos los códigos de copia de seguridad, debe volver a esta página para generar

nuevos códigos.

Para obtener más información, consulte la [Guía del usuario de terminales seguros](#).

Además, puede ver el video [Cuentas y Habilitar autenticación de dos factores](#).