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

Contenido

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.

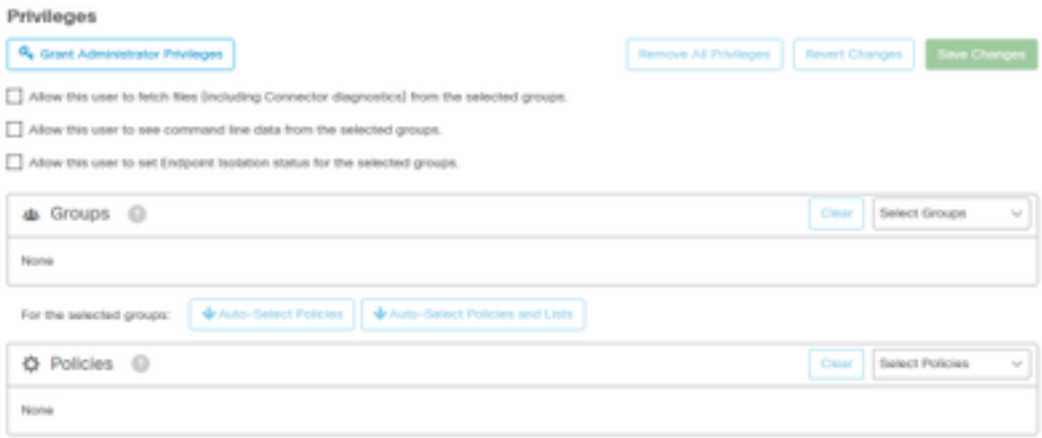
Autenticación de dos factores

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.

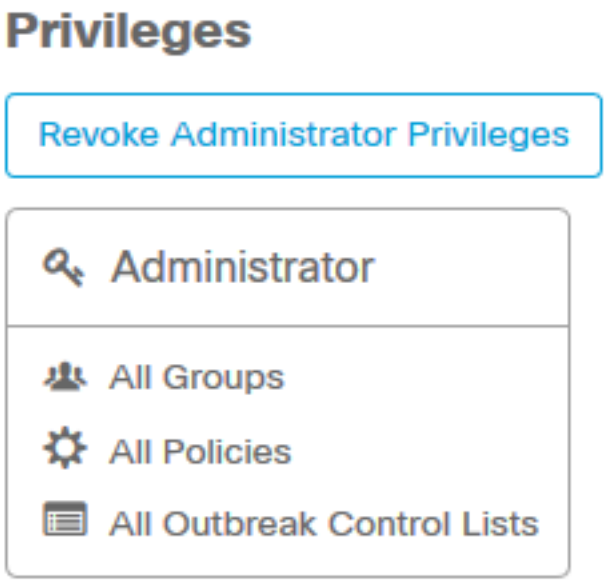
Configurar

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.



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.

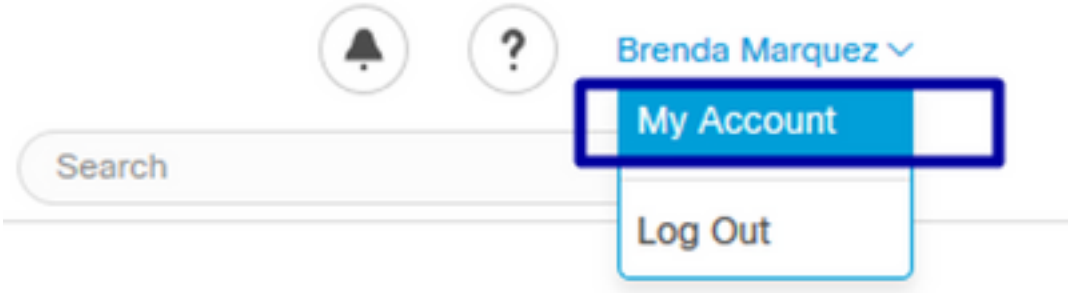


Nota: Cuando los permisos de usuario cambian algunos datos se almacenan en la memoria caché en los resultados de la búsqueda, de modo que el usuario pueda verlos durante un período de tiempo aunque ya no tenga acceso a un grupo. En la mayoría de los casos, la memoria caché se actualiza después de 5 minutos.

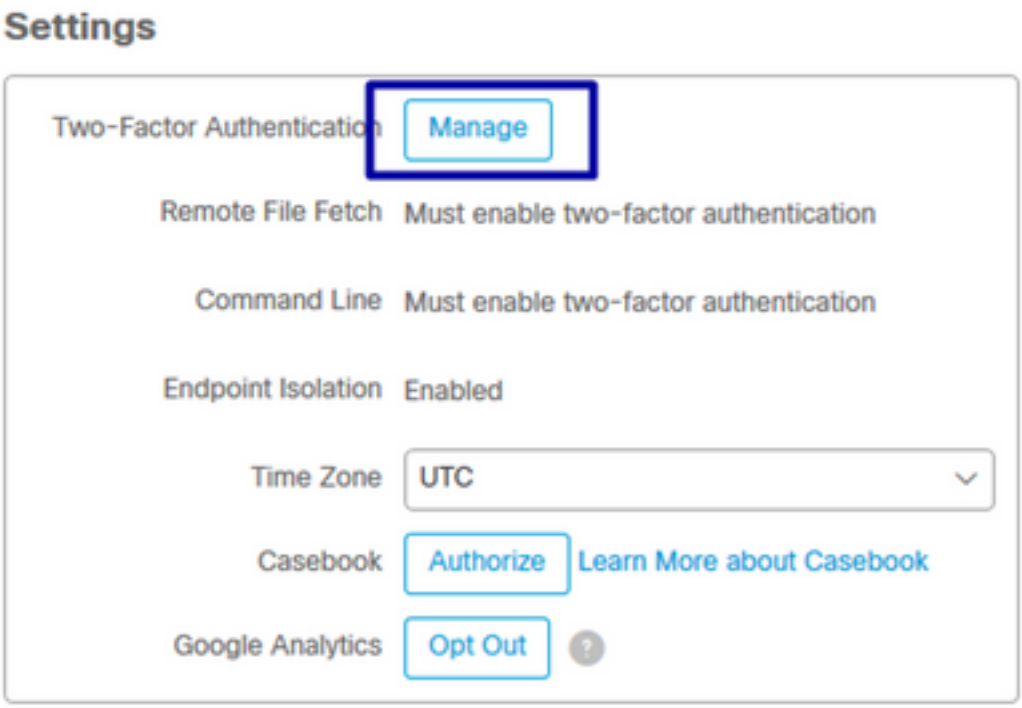
Autenticación de dos factores

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.

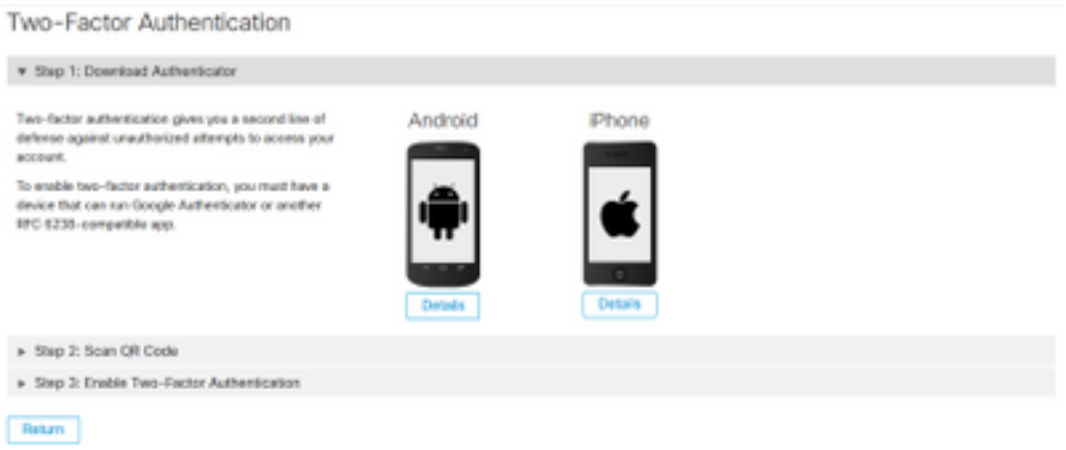


Paso 2. En la sección Settings (Configuración), seleccione Manage (Administrar) para ver una guía sencilla con tres pasos necesarios para habilitar esta función, como se muestra en la imagen.

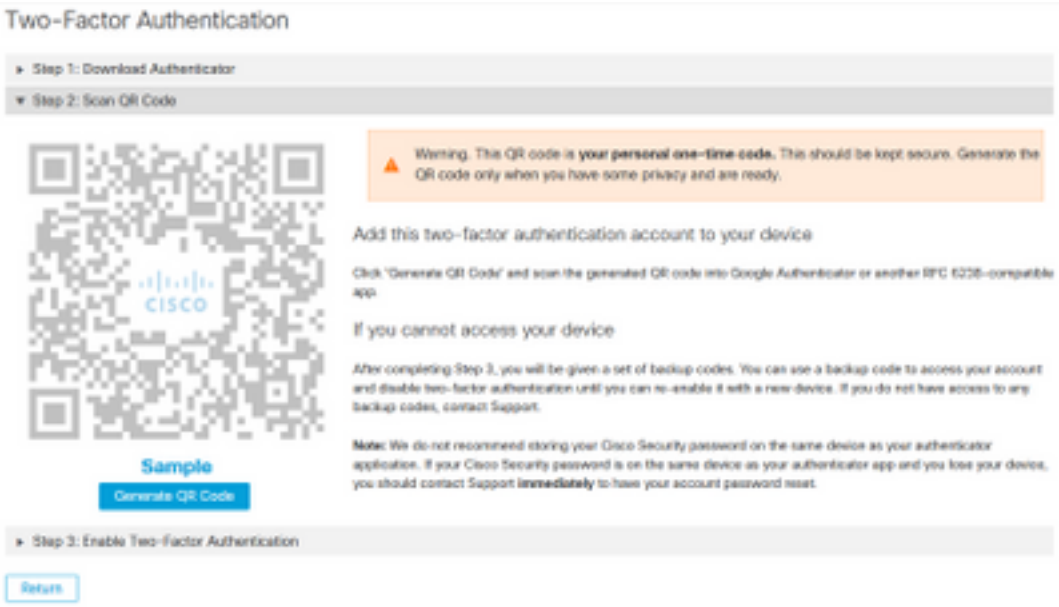


Paso 3. Hay tres pasos rápidos:

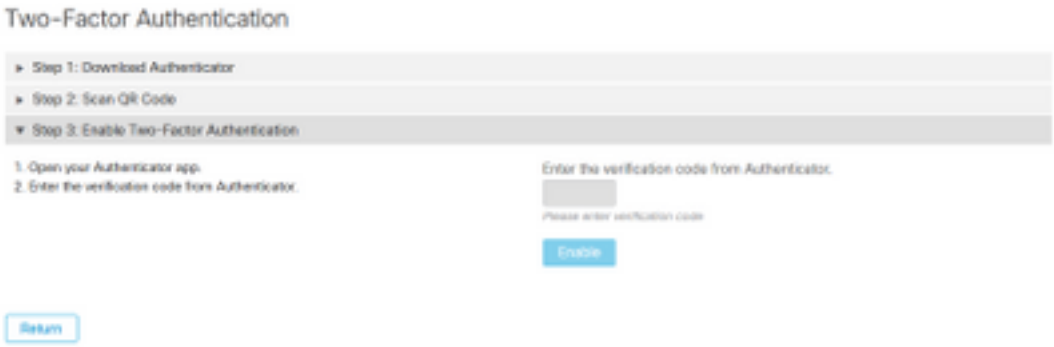
a) Descargar autenticador, que puede obtener para Android o iPhone que pueden ejecutar Google Authenticator. Seleccione Detalles en cualquiera de los teléfonos móviles para generar un código QR que le redirija a la página de descarga. Vea esta imagen.



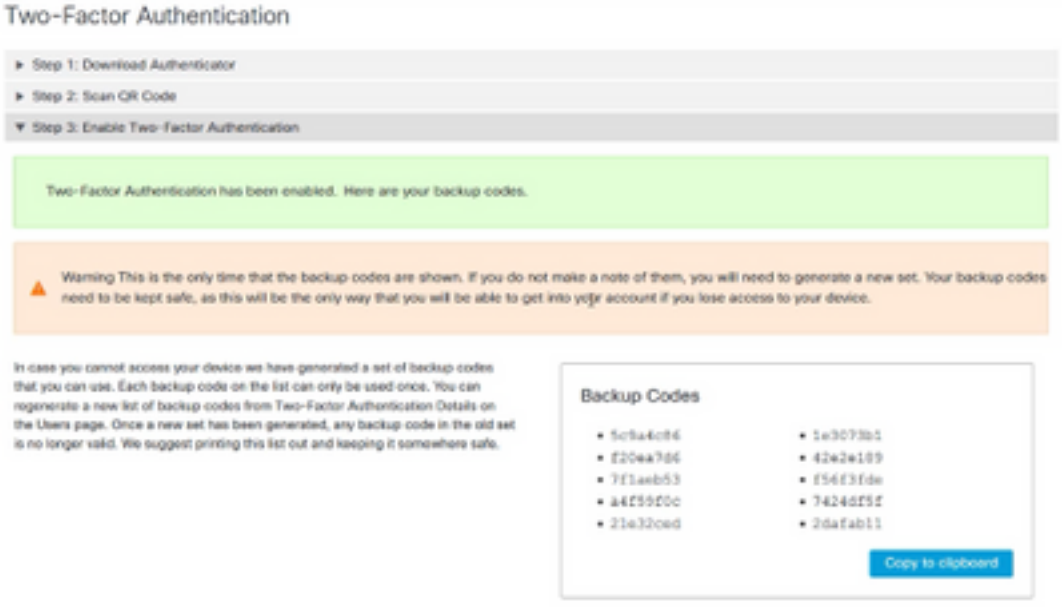
b) Escanee el código QR, seleccione Generar código QR, que debe ser analizado por Google Authenticator como se muestra en esta imagen.



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.



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



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.