Habilitar y administrar la verificación en dos pasos de Umbrella para MSP

Contenido

Introducción

Descripción general de la verificación en dos pasos

Activación de la verificación en dos pasos

- Pasos que se deben habilitar
- Método 1: Usar mensajes de texto
- Método 2: Usar aplicación móvil

Inicio de sesión con verificación en dos pasos

Desactivar la verificación en dos pasos

Teléfono perdido

Introducción

Este documento describe cómo habilitar, configurar y deshabilitar la verificación de dos pasos para Umbrella para MSPs.

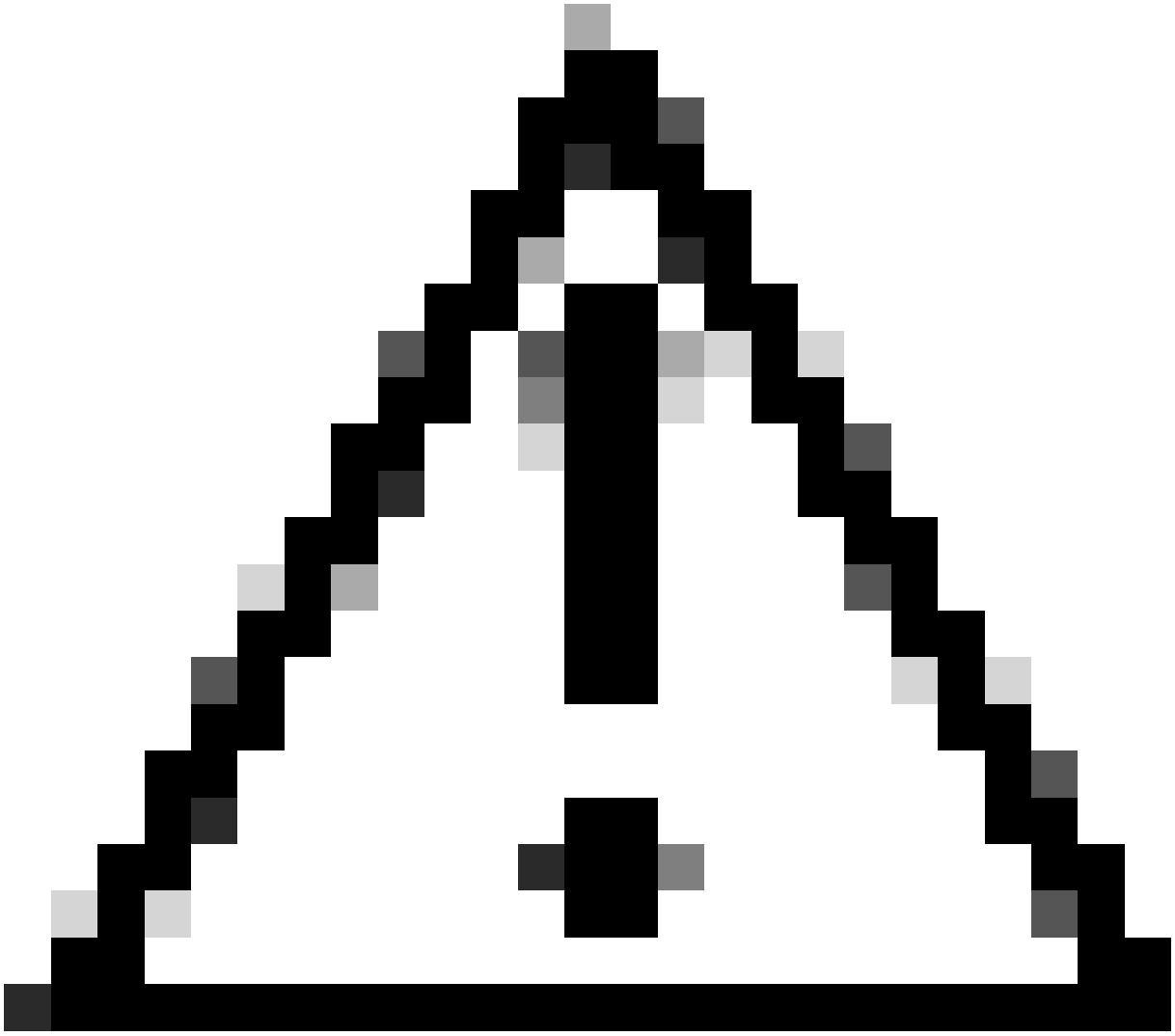
Descripción general de la verificación en dos pasos

La verificación en dos pasos (también conocida como autenticación de dos factores) agrega seguridad a la consola de Umbrella para MSPs al requerir un segundo factor de autenticación. Los usuarios deben introducir su contraseña y un código de seguridad generado en su dispositivo móvil. Este proceso evita el acceso no autorizado a través de ataques de fuerza bruta y garantiza que solo los usuarios autorizados puedan iniciar sesión.

La verificación en dos pasos también se puede habilitar para los inicios de sesión de clientes individuales dentro del panel de cada cliente.

Activación de la verificación en dos pasos

Antes de comenzar, es importante que la autenticación en dos pasos esté deshabilitada de forma predeterminada y debe habilitarse para la cuenta que está conectada actualmente.



Precaución: Solo puede habilitar la verificación en dos pasos para la cuenta actualmente conectada. No puede cambiar la configuración de la cuenta de otro administrador, pero puede ver su estado.

Pasos que se deben habilitar

1. Vaya a Configuración MSP > Administradores.
2. Amplíe la entrada de cuenta haciendo clic en el nombre de la cuenta.
3. Haga clic en Activar.

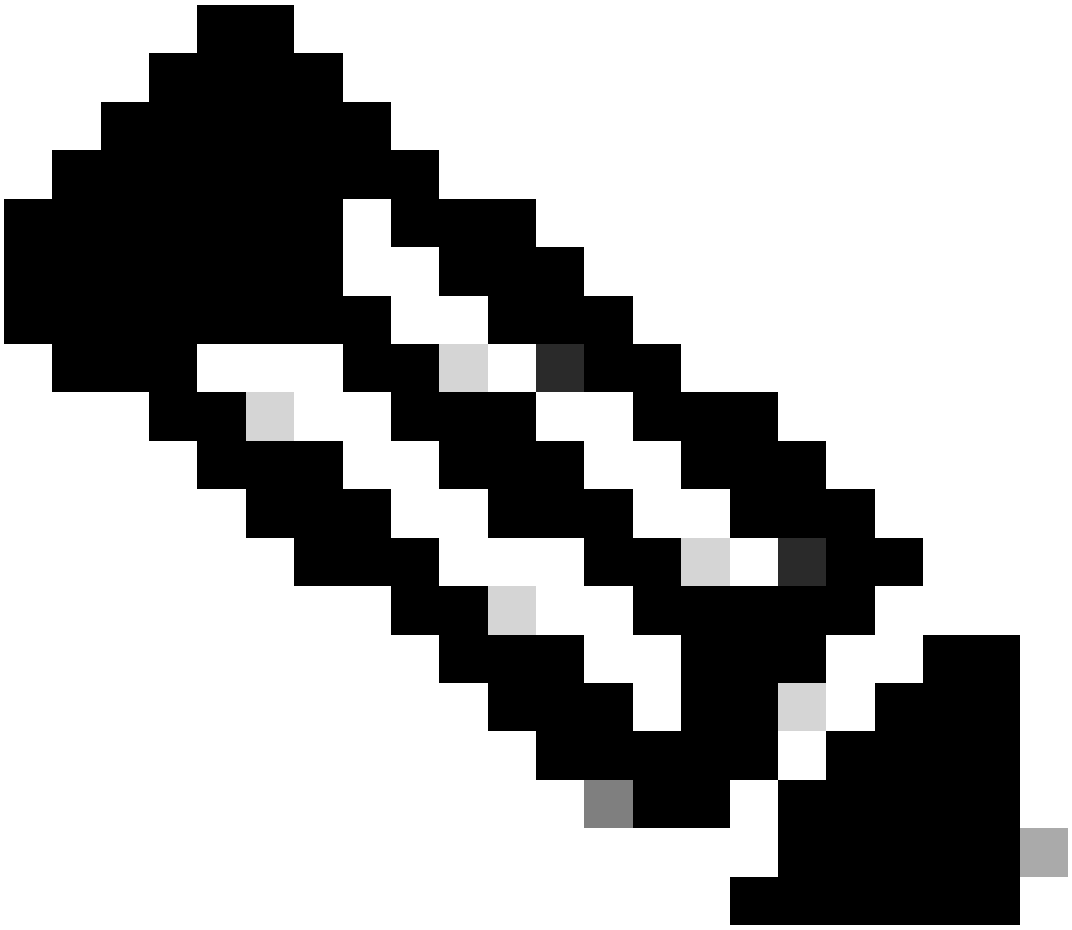
Debe seleccionar y verificar el método que prefiera para recibir los códigos de seguridad:

- Mensaje de texto (SMS)
- Aplicación móvil (aplicación de autenticación, como Google Authenticator)

Continúe con los pasos según el método que haya elegido.

Método 1: Usar mensajes de texto

1. SeleccioneUsar mensajes de texto y haga clic en Continuar.
2. Introduzca su número de teléfono, incluidos los códigos de país y de área y, a continuación, haga clic en Continuar.
3. Recibe un código de seis dígitos por SMS.
4. Introduzca la contraseña de Umbrella for MSPs y el código de seis dígitos y, a continuación, haga clic en Activar verificación en dos pasos.
5. Guarde el código de recuperación de emergencia proporcionado. Almacénelo de forma segura, separado de su dispositivo móvil y contraseñas.
6. Haga clic en Finalizado.



Nota: Recibirá un código de seguridad de mensaje de texto cada vez que inicie sesión. Los códigos de seguridad caducan después de 30 segundos. Si es necesario, utilice Reenviar código en la pantalla de inicio de sesión.

También recomendamos usar Google Voice para el SMS, porque si alguien obtiene

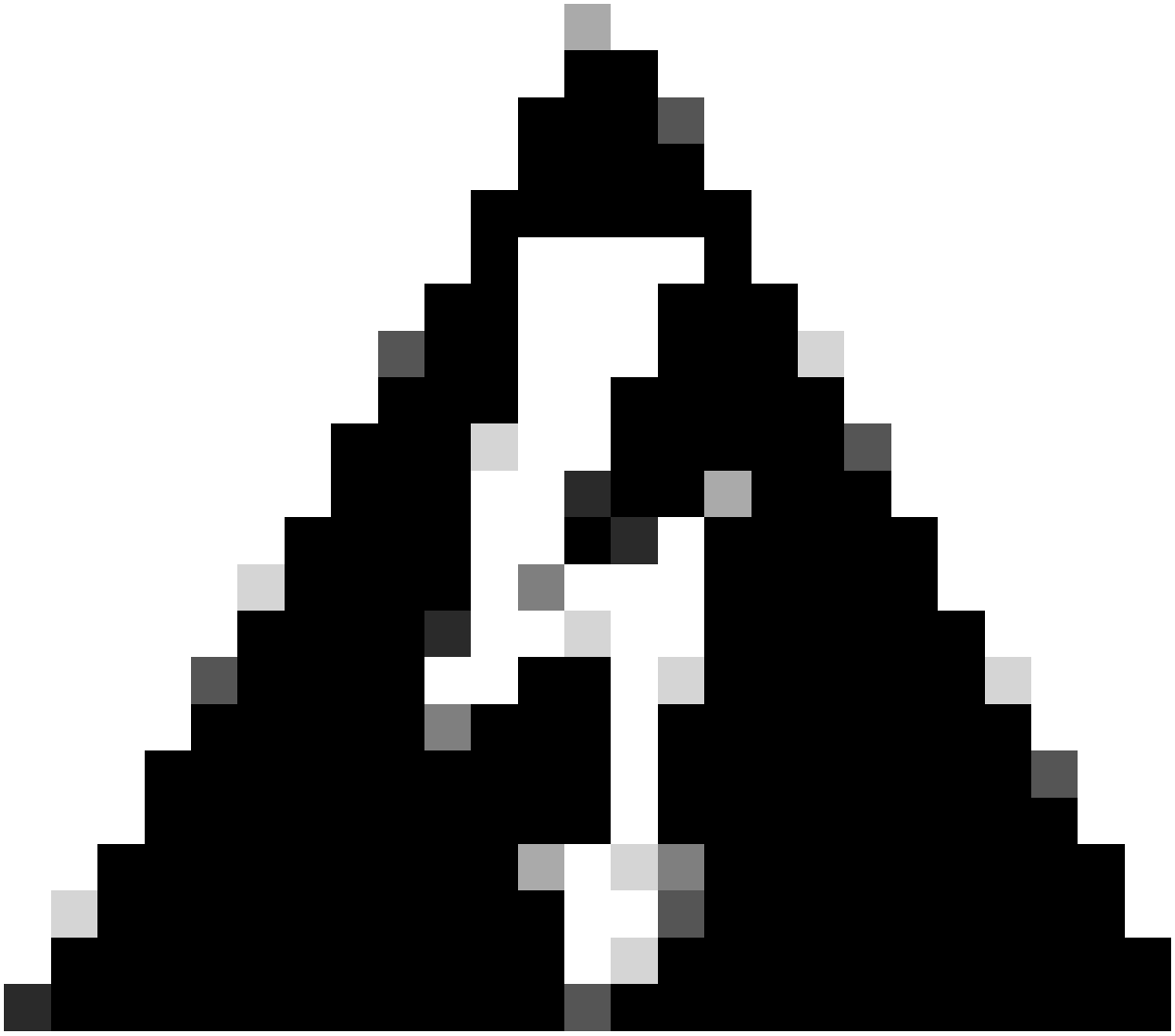
---

acceso a tu cuenta de Gmail, el atacante puede usar la función de restablecimiento de contraseña y también recibir contraseñas de un solo uso.

Método 2: Usar aplicación móvil

1. Descargue e instale una aplicación de autenticación (como Google Authenticator) en su dispositivo móvil.
2. Seleccione Utilizar aplicación móvil y haga clic en Continuar.
3. Escanee el código QR con su aplicación de autenticación. Agregue un nuevo token y escanee el código de barras. Luego, se le pedirá que escanee un código QR.
4. Agregue un nuevo token haciendo clic en el símbolo + de la parte inferior derecha y, a continuación, en Escanear código de barras.
5. Ingrese el código de seis dígitos generado y su contraseña de Umbrella for MSPs, luego haga clic en Enable Two-Step Verification.
6. Guarde el código de recuperación de emergencia proporcionado. Almacénelo de forma segura, separado de su dispositivo móvil y contraseñas. La seguridad sólo es eficaz si la contraseña y los códigos de seguridad son independientes.
7. Haga clic en Finalizado.

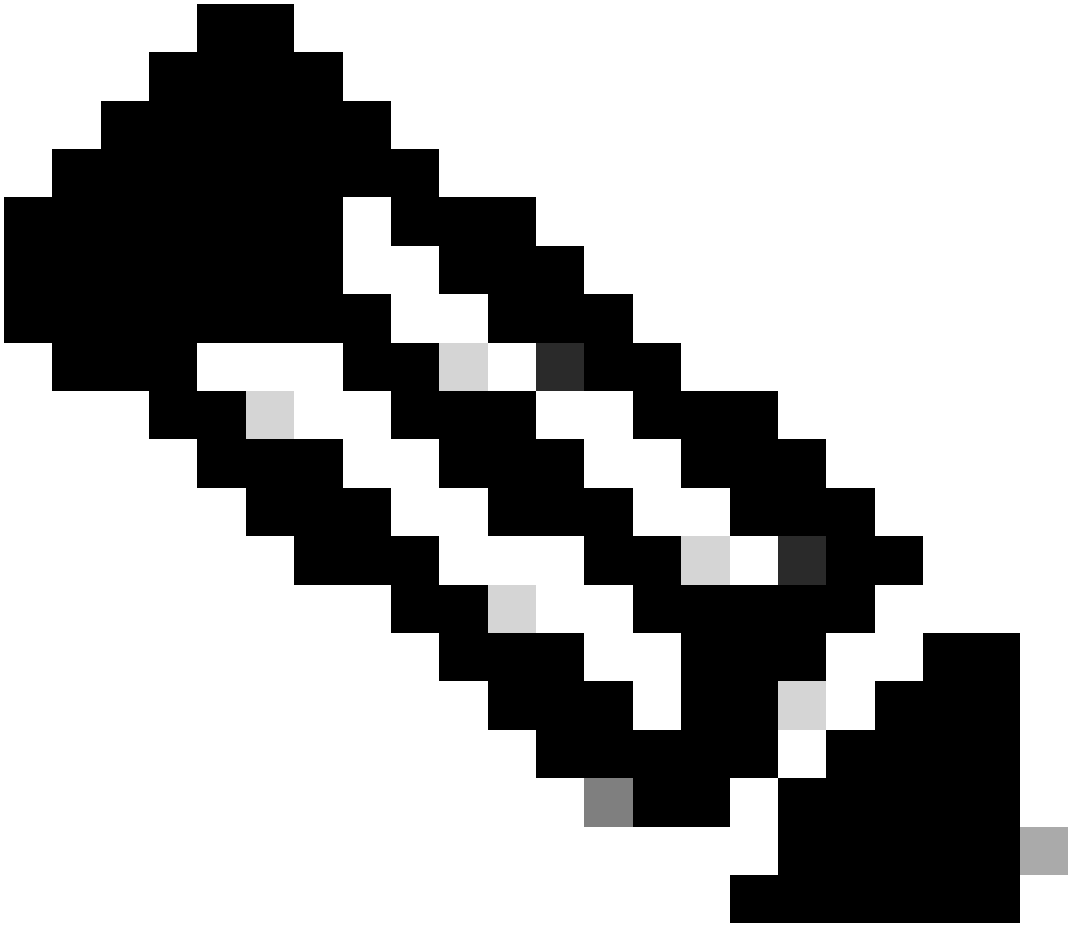
Una vez habilitada, la aplicación de autenticación genera un nuevo código cada 30 segundos para iniciar sesión.



Advertencia: Asegúrese de que la hora del dispositivo móvil esté sincronizada correctamente. La hora incorrecta del dispositivo puede provocar errores de verificación de código.

Inicio de sesión con verificación en dos pasos

Después de introducir su contraseña, introduzca el código de seguridad recibido a través de la aplicación móvil o SMS. La pantalla de verificación se muestra después del inicio de sesión inicial.



Nota: Si no recibe códigos SMS, el proveedor de SMS (Twilio) podría estar experimentando problemas. Consulte Estado de Twilio para obtener actualizaciones.

Desactivar la verificación en dos pasos

Si ya no desea utilizar la verificación en dos pasos:

1. Vaya a Configuración > Configuración del sistema > Cuentas.
2. Seleccione su cuenta y luego haga clic en Disable para la autenticación de dos pasos.
3. A continuación, se le envía un nuevo código de seguridad único y se le solicita que lo introduzca por última vez para confirmar su solicitud.

Teléfono perdido

Si ha perdido el teléfono (o tablet) y ya no desea utilizar la verificación en dos pasos, haga clic en

¿Perdió el teléfono? al iniciar sesión. Esto lo lleva a un área donde puede ingresar su código de recuperación de emergencia y deshabilitar el software. Como recordatorio, el código de recuperación de emergencia fue el código proporcionado después de la configuración inicial tanto para SMS como para la aplicación móvil.

Si pierde tanto su dispositivo como el código de recuperación de emergencia, el soporte técnico requiere información adicional para ayudarlo con el restablecimiento de la cuenta.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).