

Habilitar e gerenciar a verificação em duas etapas do Umbrella para MSPs

Contents

[Introdução](#)

[Visão geral da verificação em duas etapas](#)

[Ativando a verificação em duas etapas](#)

[Etapas para ativar](#)

[Método 1: Usar mensagens de texto](#)

[Método 2: Usar aplicativo móvel](#)

[Fazendo login com verificação em duas etapas](#)

[Desabilitar Verificação em Duas Etapas](#)

[Telefone perdido](#)

Introdução

Este documento descreve como habilitar, configurar e desabilitar a verificação em duas etapas do Umbrella para MSPs.

Visão geral da verificação em duas etapas

A verificação em duas etapas (também conhecida como autenticação de dois fatores) adiciona segurança ao console do Umbrella for MSPs, exigindo um segundo fator de autenticação. Os usuários devem inserir a senha e um código de segurança gerado no dispositivo móvel. Esse processo impede o acesso não autorizado por meio de ataques de força bruta e garante que apenas usuários autorizados possam fazer login.

A verificação em duas etapas também pode ser habilitada para logons de clientes individuais no painel de cada cliente.

Ativando a verificação em duas etapas

Antes de começar, é importante que a autenticação em duas etapas esteja desabilitada por padrão e deva ser habilitada para a conta atualmente conectada.



Caution: Você só pode habilitar a verificação em duas etapas para a conta atualmente conectada. Você não pode alterar a configuração da conta de outro administrador, mas pode exibir seu status.

Etapas para ativar

1. Navegue para Configurações de MSP > Administradores.
2. Expanda sua entrada de conta clicando no nome da conta.
3. Clique em Habilitar.

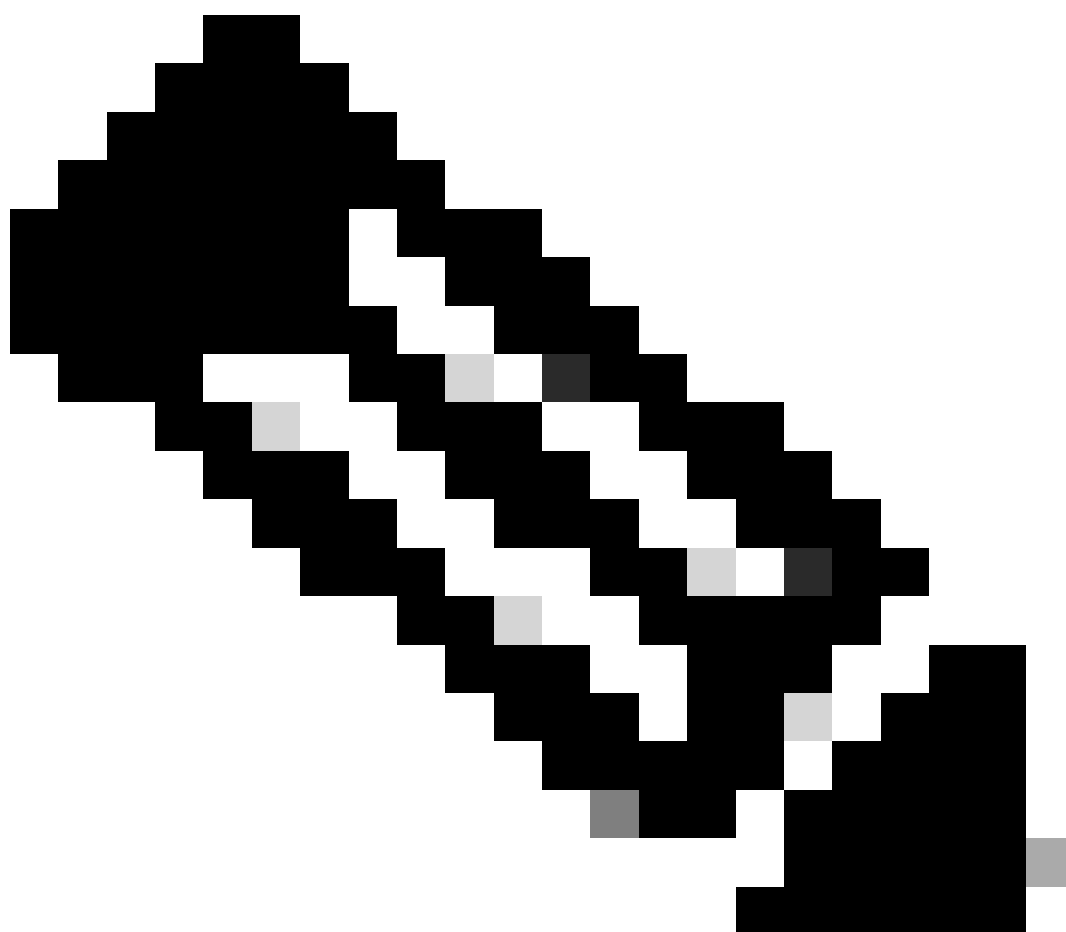
Você deve selecionar e verificar seu método preferido para receber códigos de segurança:

- Mensagem de texto (SMS)
- Aplicativo móvel (aplicativo autenticador, como [Google Authenticator](#))

Continue com as etapas com base no método escolhido.

Método 1: Usar mensagens de texto

1. Selecione Usar mensagens de texto e clique em Continuar.
 2. Insira seu número de telefone, incluindo códigos de país e de área, e clique em Continuar.
 3. Receber um código de seis dígitos via SMS.
 4. Insira a senha do Umbrella for MSPs e o código de seis dígitos e clique em Habilitar verificação em duas etapas.
 5. Salve o código de recuperação de emergência fornecido. Armazene-o com segurança, separado de seu dispositivo móvel e senhas.
 6. Clique em Concluído.
-



Note: Você recebe um código de segurança de mensagem de texto toda vez que faz login. Os códigos de segurança expiram após 30 segundos. Se necessário, use Reenviar código na tela de login.

Também sugerimos o uso do Google Voice para o SMS, porque se alguém obtiver acesso à sua conta do Gmail, o invasor poderá usar o recurso de redefinição de senha e

também receber senhas ocasionais.

Método 2: Usar aplicativo móvel

1. Baixe e instale um aplicativo de autenticação (como o [Google Authenticator](#)) em seu dispositivo móvel.
2. Selecione Usar aplicativo móvel e clique em Continuar.
3. Examine o código QR usando seu aplicativo de autenticação. Adicionar um novo token e digitalizar o código de barras. Você será solicitado a digitalizar um código QR.
4. Adicione um novo token clicando no + no canto inferior direito e em Scan Barcode.
5. Insira o código de seis dígitos gerado e sua senha do Umbrella for MSPs e clique em Enable Two-Step Verification.
6. Salve o código de recuperação de emergência fornecido. Armazene-o com segurança, separado de seu dispositivo móvel e senhas. A segurança só será efetiva se a senha e os códigos de segurança forem separados.
7. Clique em Concluído.

Depois de habilitado, o aplicativo de autenticação gera um novo código a cada 30 segundos para fazer login.



aviso: Verifique se a hora do seu dispositivo móvel está sincronizada corretamente. A hora incorreta do dispositivo pode causar falhas de verificação de código.

Fazendo login com verificação em duas etapas

Depois de digitar sua senha, insira o código de segurança recebido por meio do aplicativo móvel ou SMS. A tela de verificação é exibida após o login inicial.



Note: Se você não receber códigos SMS, o provedor de SMS (Twilio) pode estar com problemas. Verifique se há atualizações no [Twilio Status](#).

Desabilitar Verificação em Duas Etapas

Se você não quiser mais usar a verificação em duas etapas:

1. Navegue até Configuration > System Settings > Accounts.
2. Selecione sua conta e clique em Disable para obter a autenticação em duas etapas.
3. Em seguida, você recebe um novo código de segurança único e é solicitado a inseri-lo uma última vez para confirmar sua solicitação.

Telefone perdido

Se você tiver perdido seu telefone (ou tablet) e não quiser mais usar a verificação em duas

etapas, clique em Perdeu seu telefone? ao fazer login. Isso o leva a uma área onde você pode inserir seu código de recuperação de emergência e desativar o software. Como lembrete, o código de recuperação de emergência foi o código fornecido após a configuração inicial para o SMS e o aplicativo móvel.

Se você perder tanto o seu dispositivo, bem como o código de recuperação de emergência, o suporte requer informações adicionais para ajudá-lo com uma redefinição de conta.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.