

Activer et gérer la vérification en deux étapes pour Umbrella pour MSP

Table des matières

[Introduction](#)

[Présentation de la vérification en deux étapes](#)

[Activation de la vérification en deux étapes](#)

[Étapes d'activation](#)

[Méthode 1 : Utiliser les messages texte](#)

[Méthode 2 : Utiliser l'application mobile](#)

[Connexion avec vérification en deux étapes](#)

[Désactiver la vérification en deux étapes](#)

[Téléphone perdu](#)

Introduction

Ce document décrit comment activer, configurer et désactiver la vérification en deux étapes pour Umbrella pour MSP.

Présentation de la vérification en deux étapes

La vérification en deux étapes (également appelée authentification à deux facteurs) ajoute de la sécurité à la console Umbrella for MSPs en exigeant un second facteur d'authentification. Les utilisateurs doivent saisir leur mot de passe et un code de sécurité généré sur leur appareil mobile. Ce processus empêche les accès non autorisés par des attaques en force et garantit que seuls les utilisateurs autorisés peuvent se connecter.

La vérification en deux étapes peut également être activée pour les connexions de clients individuels dans le tableau de bord de chaque client.

Activation de la vérification en deux étapes

Avant de commencer, il est important que l'authentification en deux étapes soit désactivée par défaut et qu'elle soit activée pour le compte actuellement connecté.



Mise en garde : Vous ne pouvez activer la vérification en deux étapes que pour le compte actuellement connecté. Vous ne pouvez pas modifier les paramètres du compte d'un autre administrateur, mais vous pouvez afficher leur état.

Étapes d'activation

1. Accédez à MSP Settings > Admins.
2. Développez votre compte en cliquant sur son nom.
3. Cliquez sur Activer.

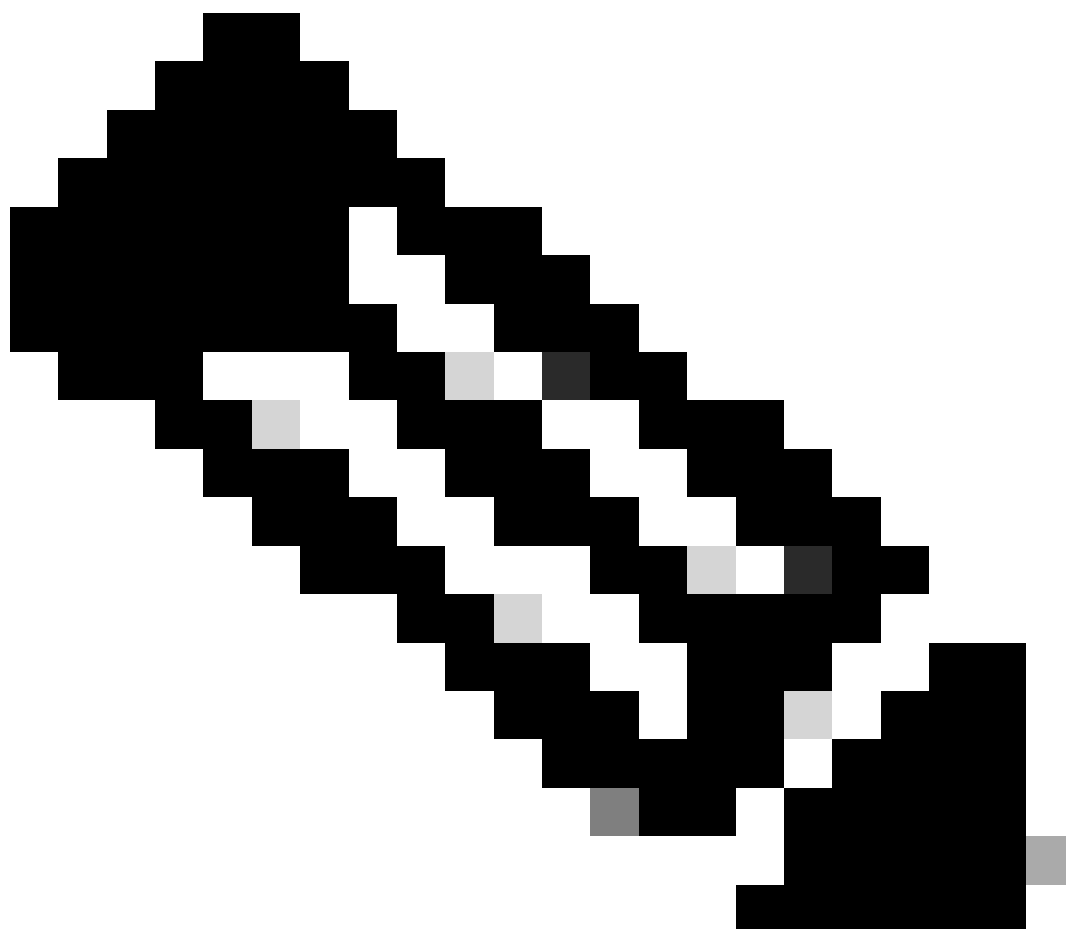
Vous devez sélectionner et vérifier votre méthode préférée pour recevoir les codes de sécurité :

- Message texte (SMS)
- Application mobile (application Authenticator, telle que [Google Authenticator](#))

Suivez les étapes en fonction de la méthode que vous avez choisie.

Méthode 1 : Utiliser les messages texte

1. Sélectionnez Utiliser les messages texte et cliquez sur Continuer.
 2. Saisissez votre numéro de téléphone, y compris les indicatifs régionaux et nationaux, puis cliquez sur Continuer.
 3. Recevez un code à six chiffres par SMS.
 4. Saisissez le mot de passe Umbrella for MSPs et le code à six chiffres, puis cliquez sur Activer la vérification en deux étapes.
 5. Enregistrez le code de récupération d'urgence fourni. Stockez-le en toute sécurité, indépendamment de votre appareil mobile et de vos mots de passe.
 6. Cliquez sur Terminé.
-



Remarque : Vous recevez un code de sécurité pour les messages texte chaque fois que vous vous connectez. Les codes de sécurité expirent après 30 secondes. Si nécessaire, utilisez Renvoyer le code sur l'écran de connexion.

Nous suggérons également d'utiliser Google Voice pour les SMS, car si quelqu'un accède

à votre compte Gmail, le pirate peut utiliser la fonction de réinitialisation de mot de passe et recevoir également des mots de passe à usage unique.

Méthode 2 : Utiliser l'application mobile

1. Téléchargez et installez une application d'authentification (telle que [Google Authenticator](#)) sur votre appareil mobile.
2. Sélectionnez Utiliser l'application mobile et cliquez sur Continuer.
3. Scannez le code QR à l'aide de votre application d'authentification. Ajouter un nouveau jeton et scanner le code barre Vous êtes alors invité à scanner un code QR.
4. Ajoutez un nouveau jeton en cliquant sur le signe + en bas à droite, puis sur Scan Barcode.
5. Entrez le code à six chiffres généré et votre mot de passe Umbrella for MSPs, puis cliquez sur Activer la vérification en deux étapes.
6. Enregistrez le code de récupération d'urgence fourni. Stockez-le en toute sécurité, indépendamment de votre appareil mobile et de vos mots de passe. La sécurité n'est efficace que si le mot de passe et les codes de sécurité sont séparés.
7. Cliquez sur Terminé.

Une fois activée, l'application d'authentification génère un nouveau code toutes les 30 secondes pour la connexion.



Avertissement : Assurez-vous que l'heure de votre appareil mobile est correctement synchronisée. Une heure incorrecte du périphérique peut entraîner des échecs de vérification du code.

Connexion avec vérification en deux étapes

Après avoir saisi votre mot de passe, saisissez le code de sécurité reçu via l'application mobile ou SMS. L'écran de vérification s'affiche après votre connexion initiale.



Remarque : Si vous ne recevez pas de codes SMS, le fournisseur de SMS (Twilio) peut rencontrer des problèmes. Vérifiez [Twilio Status](#) pour les mises à jour.

Désactiver la vérification en deux étapes

Si vous ne souhaitez plus utiliser la vérification en deux étapes :

1. Accédez à Configuration > System Settings > Accounts.
2. Sélectionnez votre compte, puis cliquez sur Désactiver pour l'authentification en deux étapes.
3. Un nouveau code de sécurité à usage unique vous est ensuite envoyé, puis vous êtes invité à le saisir une dernière fois pour confirmer votre demande.

Téléphone perdu

Si vous avez perdu votre téléphone (ou votre tablette) et ne souhaitez plus utiliser la vérification en deux étapes, cliquez sur Perdu votre téléphone ? lors de la connexion. Cela vous amène à une zone où vous pouvez entrer votre code de récupération d'urgence et désactiver le logiciel. Pour rappel, le code de récupération d'urgence était le code fourni après la configuration initiale pour SMS et l'application mobile.

Si vous perdez votre périphérique et le code de récupération d'urgence, l'assistance nécessite des informations supplémentaires pour vous aider à réinitialiser votre compte.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.