

MSPのUmbrellaの2段階検証の有効化と管理

内容

[はじめに](#)

[2段階認証の概要](#)

[2段階認証の有効化](#)

[有効にする手順](#)

[方法1: テキストメッセージを使用する](#)

[方法2: モバイルアプリを使用する](#)

[2段階認証によるログイン](#)

[2段階認証を無効にする](#)

[電話の紛失](#)

はじめに

このドキュメントでは、MSPのUmbrellaの2段階検証を有効、設定、および無効にする方法について説明します。

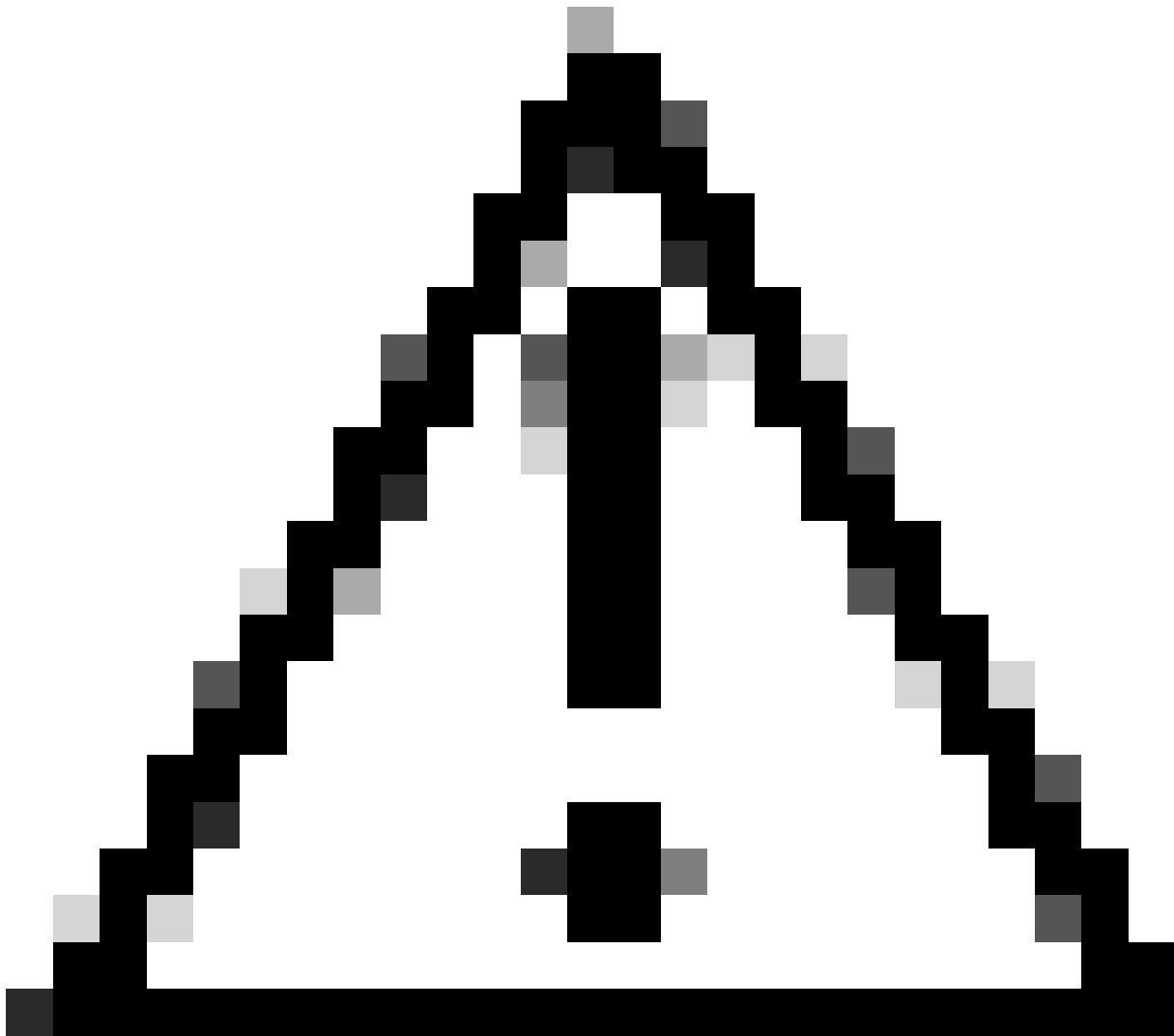
2段階認証の概要

2段階認証（2要素認証とも呼ばれます）では、2番目の認証要素が必要になるため、Umbrella for MSPのコンソールにセキュリティが追加されます。ユーザは、自分のパスワードとモバイルデバイスで生成されたセキュリティコードの両方を入力する必要があります。このプロセスにより、総当たり攻撃による不正アクセスが防止され、許可されたユーザだけがログインできるようになります。

各クライアントのダッシュボード内で個々のクライアントログインに対して2段階認証を有効にすることもできます。

2段階認証の有効化

を開始する前に、2段階認証がデフォルトで無効になっており、現在ログインしているアカウントに対して有効になっている必要があります。



注意:2段階認証を有効にできるのは、現在ログインしているアカウントに対してだけです。別の管理者のアカウントの設定は変更できませんが、そのステータスは表示できます。

有効にする手順

1. MSP Settings > Adminsの順に移動します。
2. アカウント名をクリックして、アカウントエントリを展開します。
3. Enableをクリックします。

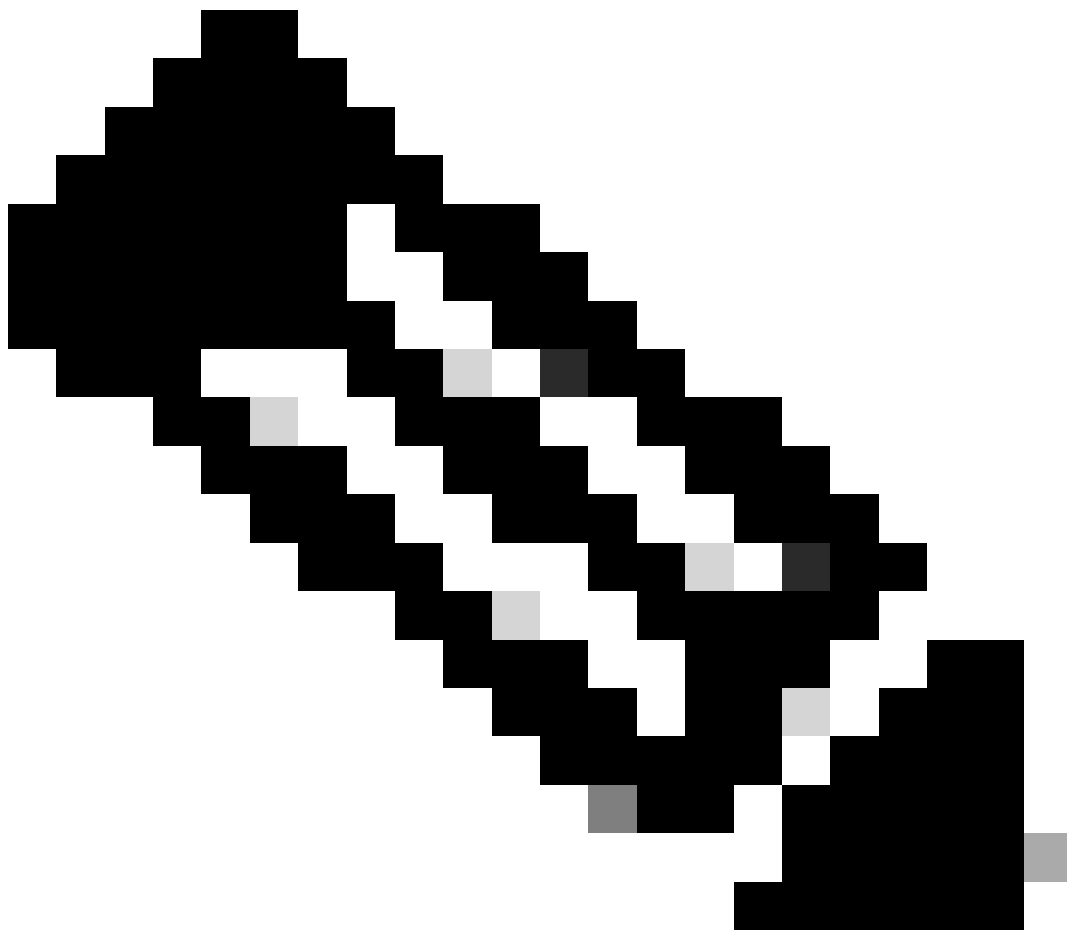
セキュリティコードを受け取るには、希望する方法を選択して確認する必要があります。

- テキストメッセージ(SMS)
- モバイルアプリ([Google Authenticator](#)などの認証アプリ)

選択した方法に基づいて手順を実行します。

方法1：テキストメッセージを使用する

1. 「テキストメッセージを使用」を選択し、「続行」をクリックします。
 2. 国コードと市外局番を含む電話番号を入力し、Continueをクリックします。
 3. SMSで6桁のコードを受信します。
 4. MSPのパスワードと6桁のコードのUmbrellaを入力し、Enable 2-step verificationをクリックします。
 5. 提供された緊急復旧コードを保存します。モバイルデバイスやパスワードから切り離して、安全に保存します。
 6. Doneをクリックします。
-



注：ログインするたびに、テキストメッセージによるセキュリティコードが送信されます。セキュリティコードは30秒後に期限切れになります。必要に応じて、ログイン画面でResend Codeを使用します。

また、SMSにGoogle Voiceを使用することをお勧めします。Gmailアカウントに誰かがアクセスすると、攻撃者がパスワードのリセット機能を使用して、ワンタイムパスワード

を受信する可能性があるためです。

方法2：モバイルアプリを使用する

1. モバイルデバイスに認証アプリケーション([Google Authenticator](#)など)をダウンロードしてインストールします。
2. Use mobile app and Continueを選択します。
3. 認証アプリを使用してQRコードをスキャンします。新しいトークンを追加してバーコードをスキャンします次に、QRコードをスキャンするように求められます。
4. 右下の+をクリックし、次にScan Barcodeをクリックして、新しいトークンを追加します。
5. 生成された6桁のコードとUmbrella for MSPのパスワードを入力し、Enable Two-Step Verificationをクリックします。
6. 提供された緊急復旧コードを保存します。モバイルデバイスやパスワードから切り離して、安全に保存します。セキュリティは、パスワードとセキュリティコードが分離されている場合にのみ有効です。
7. Doneをクリックします。

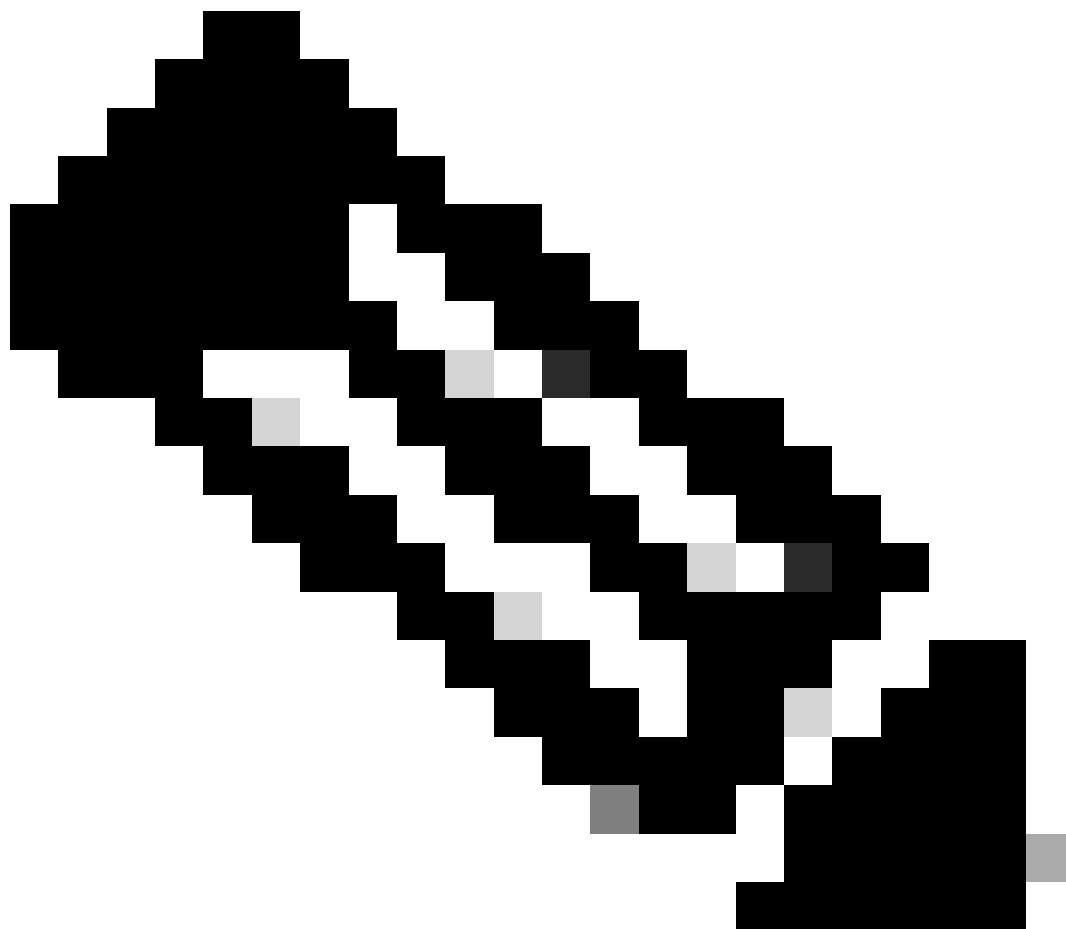
認証アプリを有効にすると、ログイン用の新しいコードが30秒ごとに生成されます。



警告：モバイルデバイスの時刻が正しく同期されていることを確認してください。デバイスの時刻が正しくないと、コード検証エラーが発生する可能性があります。

2段階認証によるログイン

パスワードを入力したら、モバイルアプリまたはSMSで受信したセキュリティコードを入力します。最初のログイン後に検証画面が表示されます。



注:SMSコードを受信しない場合、SMSプロバイダー(Twilio)で問題が発生している可能性があります。アップデートについては[Twilioステータス](#)を確認します。

2段階認証を無効にする

2段階認証を使用しない場合は、次の手順を実行します。

1. Configuration > System Settings > Accountsの順に選択します。
2. 2段階認証の場合は、アカウントを選択して、Disableをクリックします。
3. その後、新しいワンタイムセキュリティコードが送信され、要求を確認するために最後にもう1回そのコードを入力するよう求められます。

電話の紛失

電話（またはタブレット）を紛失し、2段階認証を使用しなくなった場合は、ログイン時にLost

your phone?をクリックします。これにより、緊急復旧コードを入力してソフトウェアを無効にできるエリアに移動します。この緊急リカバリコードは、SMSとモバイルアプリの両方の初期設定の後に提供されたコードです。

デバイスと緊急復旧コードの両方を紛失した場合は、アカウントのリセットに役立つ追加情報が必要です。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。