Enable and Manage Two-Step Verification for Umbrella for MSPs

Contents

Introduction

This document describes how to enable, configure, and disable two-step verification for Umbrella for MSPs.

Overview of Two-Step Verification

Two-step verification (also known as two-factor authentication) adds security to the Umbrella for MSPs console by requiring a second authentication factor. Users must enter both their password and a security code generated on their mobile device. This process prevents unauthorized access through brute-force attacks and ensures only authorized users can log in.

Two-step verification can also be enabled for individual client logins within the dashboard of each client.

Enabling Two-Step Verification

Before you start, it is important that two-step authentication is disabled by default and must be enabled for hte account currently logged in.

⚠

Caution: You can only enable two-step verification for the account currently logged in. You cannot change the setting for another administrator’s account, but you can view their status.

Steps to Enable

1. Navigate to**MSP Settings** > **Admins**.
2. Expand your account entry by clicking the account name.
3. Click**Enable**.

You must select and verify your preferred method to receive security codes:

- Text message (SMS)
- Mobile app (Authenticator app, such as Google Authenticator)

Proceed with the steps based on your chosen method.

Method 1: Use Text Messages

1. Select**Use text messages**and click**Continue**.

2. Enter your phone number, including country and area codes, then click**Continue**.
3. Receive a six-digit code via SMS.
4. Enter your Umbrella for MSPs password and the six-digit code, then click**Enable two-step verification**.
5. Save the emergency recovery code provided. Store it securely, separate from your mobile device and passwords.
6. Click**Done**.

Note: You receive a text message security code each time you log in. Security codes expire after 30 seconds. If necessary, use **Resend Code** on the login screen.

We also suggest using Google Voice for the SMS, because if someone gains access to your Gmail account, the attacker can use the reset password feature and also receive one-time passwords.

Method 2: Use Mobile App

1. Download and install an authentication app (such as Google Authenticator) on your mobile device.
2. Select**Use mobile app**and click**Continue**.
3. Scan the QR code using your authentication app. Add a new token and scan the barcode You are

then asked to scan a QR code.

4. Add a new token by clicking the **+** in the lower right then **Scan Barcode**.
5. Enter the generated six-digit code and your Umbrella for MSPs password, then click**Enable Two-Step Verification**.
6. Save the emergency recovery code provided. Store it securely, separate from your mobile device and passwords. Security is only effective if the password and the security codes are separate.
7. Click**Done**.

Once enabled, the authentication app generates a new code every 30 seconds for logging in.

> **Warning**: Ensure your mobile device is time synchronized correctly. Incorrect device time can cause code verification failures.

Logging in with Two-Step Verification

After entering your password, enter the security code received via the mobile app or SMS. The verification screen displays after your initial login.

Note: If you do not receive SMS codes, the SMS provider (Twilio) could be experiencing issues. Check Twilio Status for updates.

Disable Two-Step Verification

If you no longer wish to use two-step verification:

1. Navigate to **Configuration** > **System Settings** > **Accounts**.
2. Select your account and then click **Disable** for two-step authentication.
3. You are then sent a new one-time security code and then asked to enter it one last time to confirm your request.

Lost Phone

If you have lost your phone (or tablet) and no longer wish to use two-step verification, click **Lost your phone?** when logging in. This takes you to an area where you can enter your emergency recovery code and disable the software. As a reminder, the emergency recovery code was the code provided after the initial setup for both SMS and the mobile app.

If you lose both of your device as well as the emergency recovery code, support requires additional information to assist you with an account reset.