Aktivieren und Verwalten der zweistufigen Überprüfung für Umbrella für MSPs

Inhalt

Einleitung

Übersicht über die zweistufige Verifizierung

Aktivieren der zweistufigen Überprüfung

- Aktivierungsschritte
- Methode 1: Textnachrichten verwenden
- Methode 2: Mobile App verwenden

Anmeldung mit zweistufiger Überprüfung

Zweistufige Überprüfung deaktivieren

Verlorenes Telefon

Einleitung

In diesem Dokument wird beschrieben, wie die zweistufige Überprüfung für Umbrella für MSPs aktiviert, konfiguriert und deaktiviert wird.

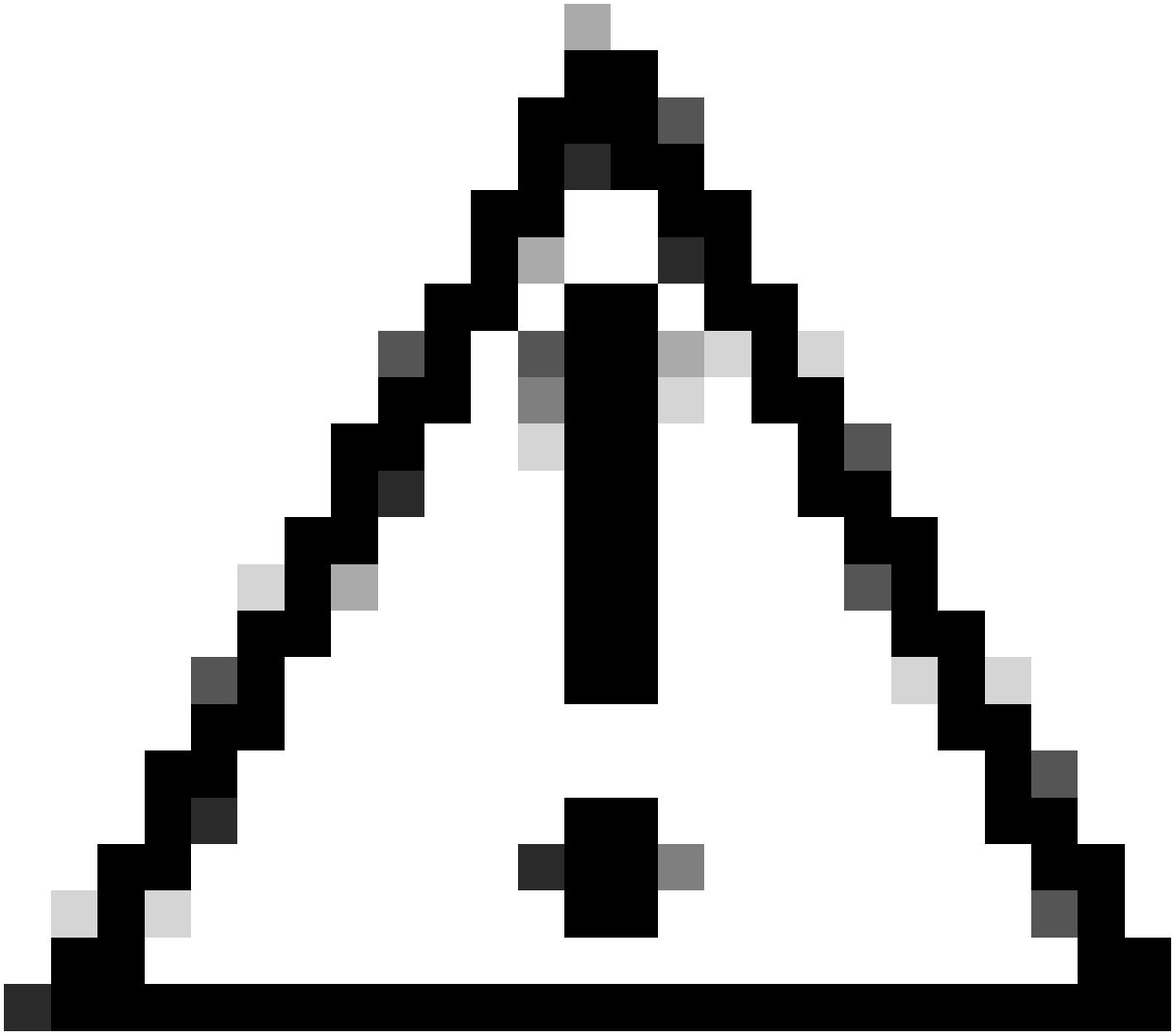
Übersicht über die zweistufige Verifizierung

Die zweistufige Verifizierung (auch als Zwei-Faktor-Authentifizierung bezeichnet) erhöht die Sicherheit der Umbrella for MSPs-Konsole, da ein zweiter Authentifizierungsfaktor erforderlich ist. Die Benutzer müssen sowohl ihr Kennwort als auch einen auf ihrem Mobilgerät generierten Sicherheitscode eingeben. Dieser Prozess verhindert nicht autorisierte Zugriffe durch Brute-Force-Angriffe und stellt sicher, dass sich nur autorisierte Benutzer anmelden können.

Die zweistufige Überprüfung kann auch für individuelle Client-Anmeldungen im Dashboard jedes Clients aktiviert werden.

Aktivieren der zweistufigen Überprüfung

Bevor Sie beginnen, ist es wichtig, dass die Zwei-Schritt-Authentifizierung standardmäßig deaktiviert ist und für das Konto aktiviert werden muss, das derzeit angemeldet ist.



Vorsicht: Sie können nur die zweistufige Verifizierung für das aktuell angemeldete Konto aktivieren. Sie können die Einstellung für ein anderes Administratorkonto nicht ändern, aber Sie können deren Status anzeigen.

Aktivierungsschritte

1. Navigieren Sie zuMSP Settings > Admins.
2. Erweitern Sie Ihren Kontoeintrag, indem Sie auf den Kontonamen klicken.
3. Klicken Sie auf Aktivieren.

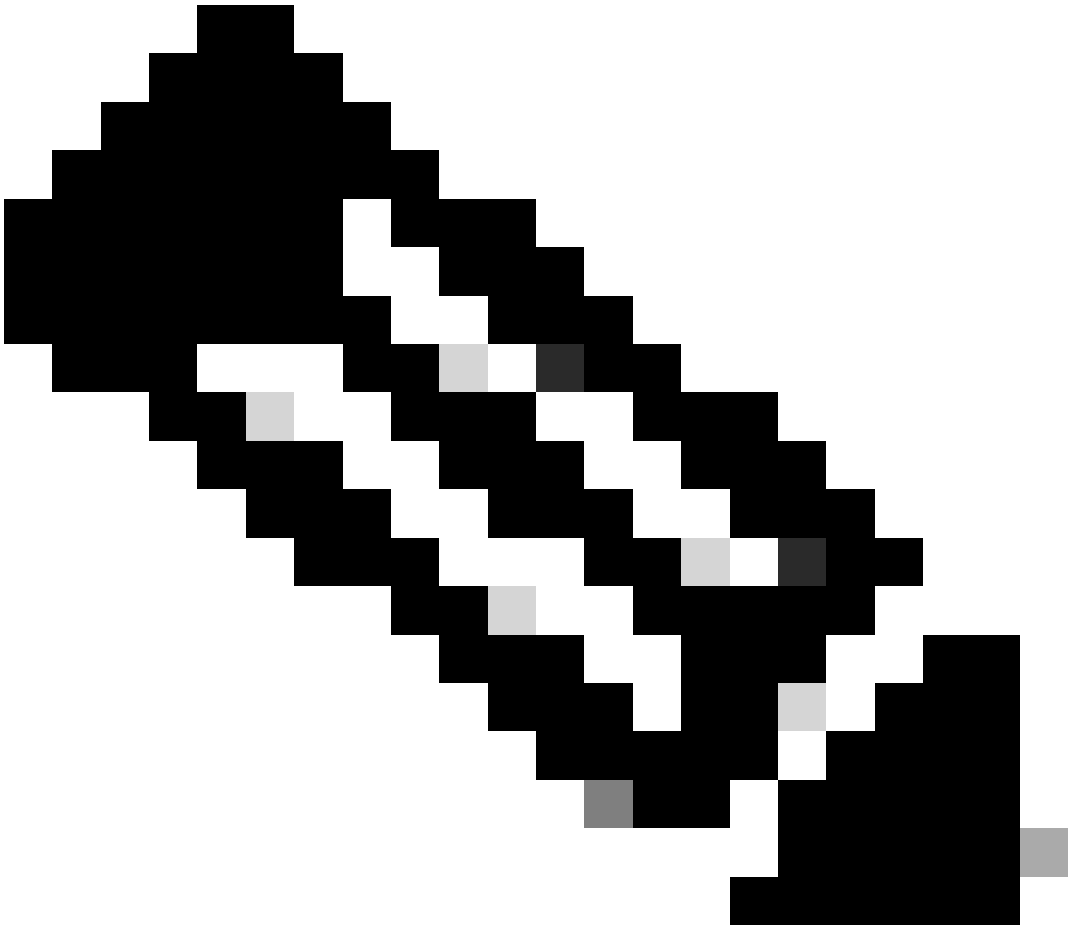
Sie müssen Ihre bevorzugte Methode auswählen und überprüfen, um Sicherheitscodes zu erhalten:

- Textnachricht (SMS)
- Mobile App (Authentifizierer-App wie Google Authenticator)

Fahren Sie mit den Schritten basierend auf der von Ihnen gewählten Methode fort.

Methode 1: Textnachrichten verwenden

1. Wählen Sie Textnachrichten verwenden aus, und klicken Sie auf Weiter.
2. Geben Sie Ihre Telefonnummer, einschließlich Land und Vorwahl, ein, und klicken Sie dann auf Weiter.
3. Sechsstelliger Code per SMS
4. Geben Sie Ihr Umbrella for MSPs-Kennwort und den sechsstelligen Code ein, und klicken Sie dann auf Zweistufenüberprüfung aktivieren.
5. Speichern Sie den angegebenen Notfallwiederherstellungscode. Sichere Speicherung, unabhängig von Mobilgerät und Passwörtern
6. Klicken Sie auf Fertig.



Anmerkung: Bei jeder Anmeldung erhalten Sie einen Sicherheitscode für die Textnachricht. Sicherheitscodes laufen nach 30 Sekunden ab. Verwenden Sie ggf. Code erneut auf dem Anmeldebildschirm.

Wir empfehlen auch, Google Voice für die SMS zu verwenden, denn wenn jemand Zugriff

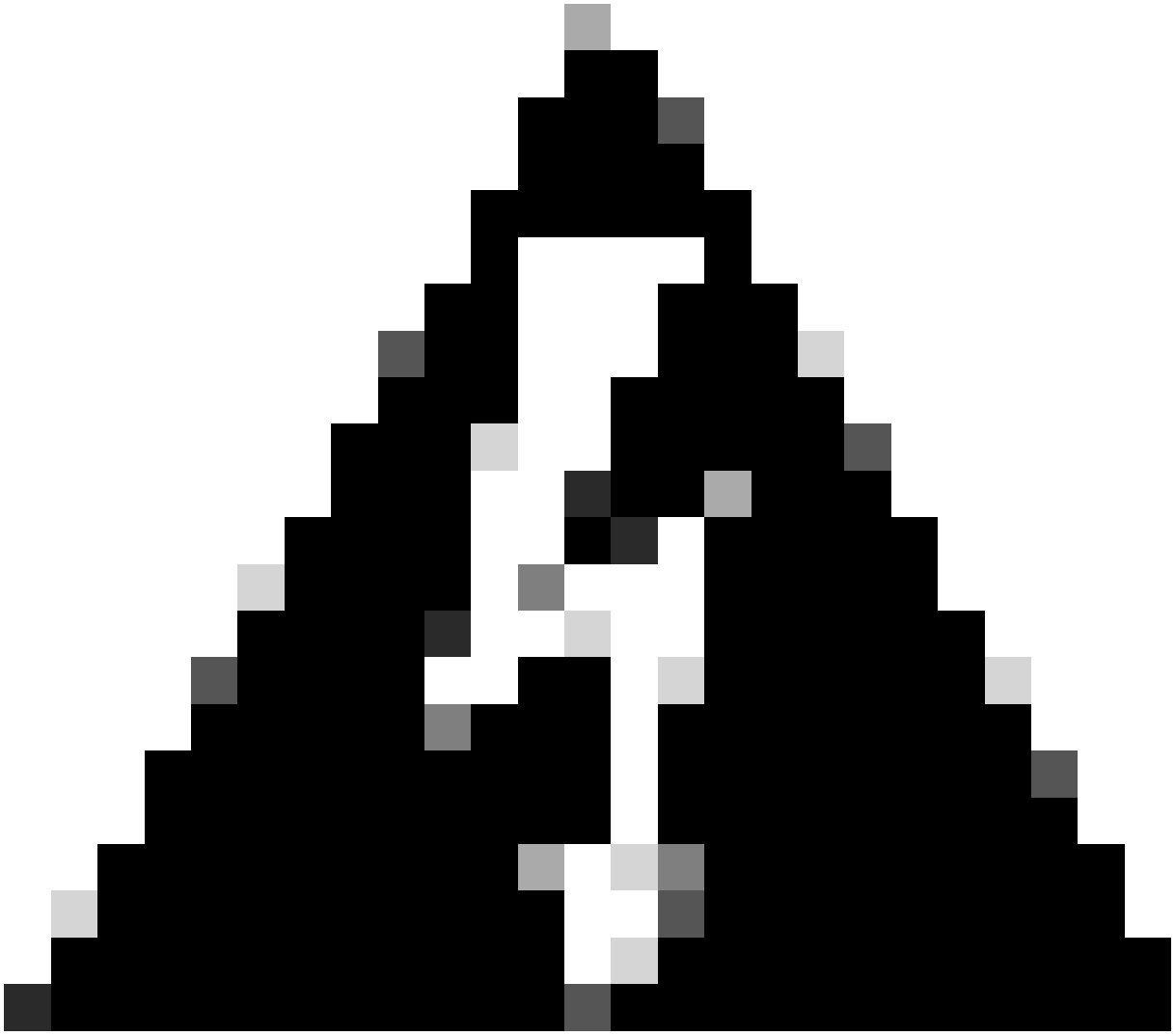
---

auf Ihr Gmail-Konto erhält, kann der Angreifer die Kennwortrücksetzfunktion verwenden und auch einmalige Kennwörter erhalten.

Methode 2: Mobile App verwenden

1. Laden Sie eine Authentifizierungs-App (z. B. Google Authenticator) auf Ihr Mobilgerät herunter, und installieren Sie sie.
2. Wählen Sie die Option Mobile App verwenden, und klicken Sie auf Weiter.
3. Scannen Sie den QR-Code mit Ihrer Authentifizierungs-App. Fügen Sie ein neues Token hinzu, und scannen Sie den Barcode. Anschließend werden Sie aufgefordert, einen QR-Code zu scannen.
4. Fügen Sie ein neues Token hinzu, indem Sie unten rechts auf + und dann auf Barcode scannen klicken.
5. Geben Sie den generierten sechsstelligen Code und Ihr Umbrella for MSPs-Kennwort ein, und klicken Sie dann auf Enable Two-Step Verification.
6. Speichern Sie den angegebenen Notfallwiederherstellungscode. Sichere Speicherung, unabhängig von Mobilgerät und Passwörtern Sicherheit ist nur wirksam, wenn das Passwort und die Sicherheitscodes getrennt sind.
7. Klicken Sie auf Fertig.

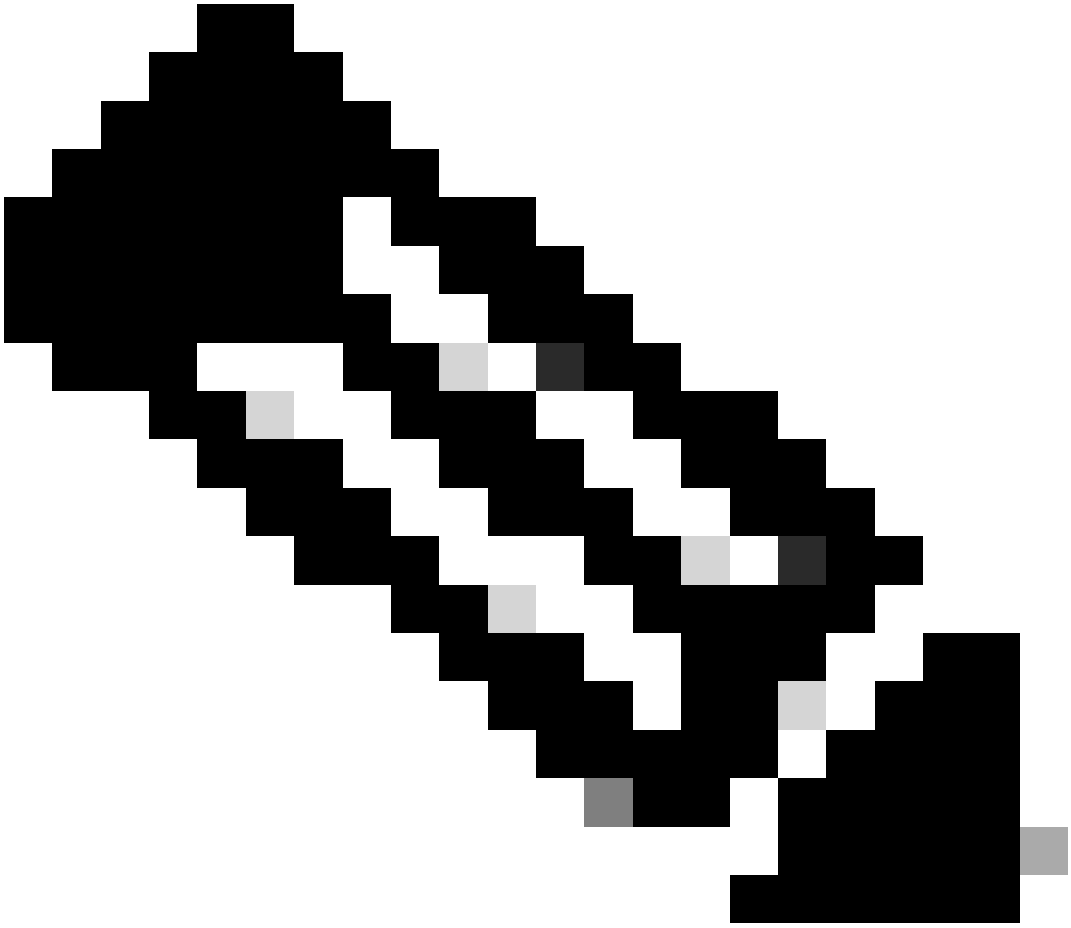
Nach der Aktivierung generiert die Authentifizierungs-App alle 30 Sekunden einen neuen Code für die Anmeldung.



Warnung: Stellen Sie sicher, dass Ihr Mobilgerät die Uhrzeit richtig synchronisiert. Falsche Gerätezeit kann Fehler bei der Codeüberprüfung verursachen.

Anmeldung mit zweistufiger Überprüfung

Geben Sie nach Eingabe Ihres Kennworts den Sicherheitscode ein, den Sie über die mobile App oder SMS erhalten haben. Der Verifizierungsbildschirm wird nach der erstmaligen Anmeldung angezeigt.



Anmerkung: Wenn Sie keine SMS-Codes erhalten, kann es beim SMS-Anbieter (Twilio) zu Problemen kommen. Überprüfen Sie den Twilio-Status auf Aktualisierungen.

Zweistufige Überprüfung deaktivieren

Wenn Sie die zweistufige Verifizierung nicht mehr verwenden möchten:

1. Navigieren Sie zu Konfiguration > Systemeinstellungen > Konten.
2. Wählen Sie Ihr Konto aus, und klicken Sie dann auf Deaktivieren, um die Authentifizierung in zwei Schritten durchzuführen.
3. Sie erhalten dann einen neuen einmaligen Sicherheitscode und werden aufgefordert, diesen ein letztes Mal einzugeben, um Ihre Anfrage zu bestätigen.

Verlorenes Telefon

Wenn Sie Ihr Telefon (oder Tablet) verloren haben und die zweistufige Verifizierung nicht mehr verwenden möchten, klicken Sie auf Telefon verloren? bei der Anmeldung. Dadurch gelangen Sie in einen Bereich, in dem Sie Ihren Notfallwiederherstellungscode eingeben und die Software deaktivieren können. Zur Erinnerung: Der Notfallwiederherstellungscode ist der Code, der nach der Ersteinrichtung sowohl für SMS als auch für die mobile App bereitgestellt wurde.

Wenn Sie sowohl Ihr Gerät als auch den Notfallwiederherstellungscode verlieren, benötigt der Support zusätzliche Informationen, um Ihnen bei einer Zurücksetzung Ihres Kontos behilflich zu sein.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.