# Abilitare e gestire la verifica in due passaggi per Umbrella per MSP

## Sommario


Introduzione

Panoramica della verifica in due passaggi

Abilitazione della verifica in due passaggi

- Passi da abilitare
- Metodo 1: Usa SMS
- Metodo 2: Usa app mobile

Accesso con verifica in due passaggi

Disabilita verifica in due passaggi

Telefono perso


## Introduzione

In questo documento viene descritto come abilitare, configurare e disabilitare la verifica in due passaggi per Umbrella per MSP.

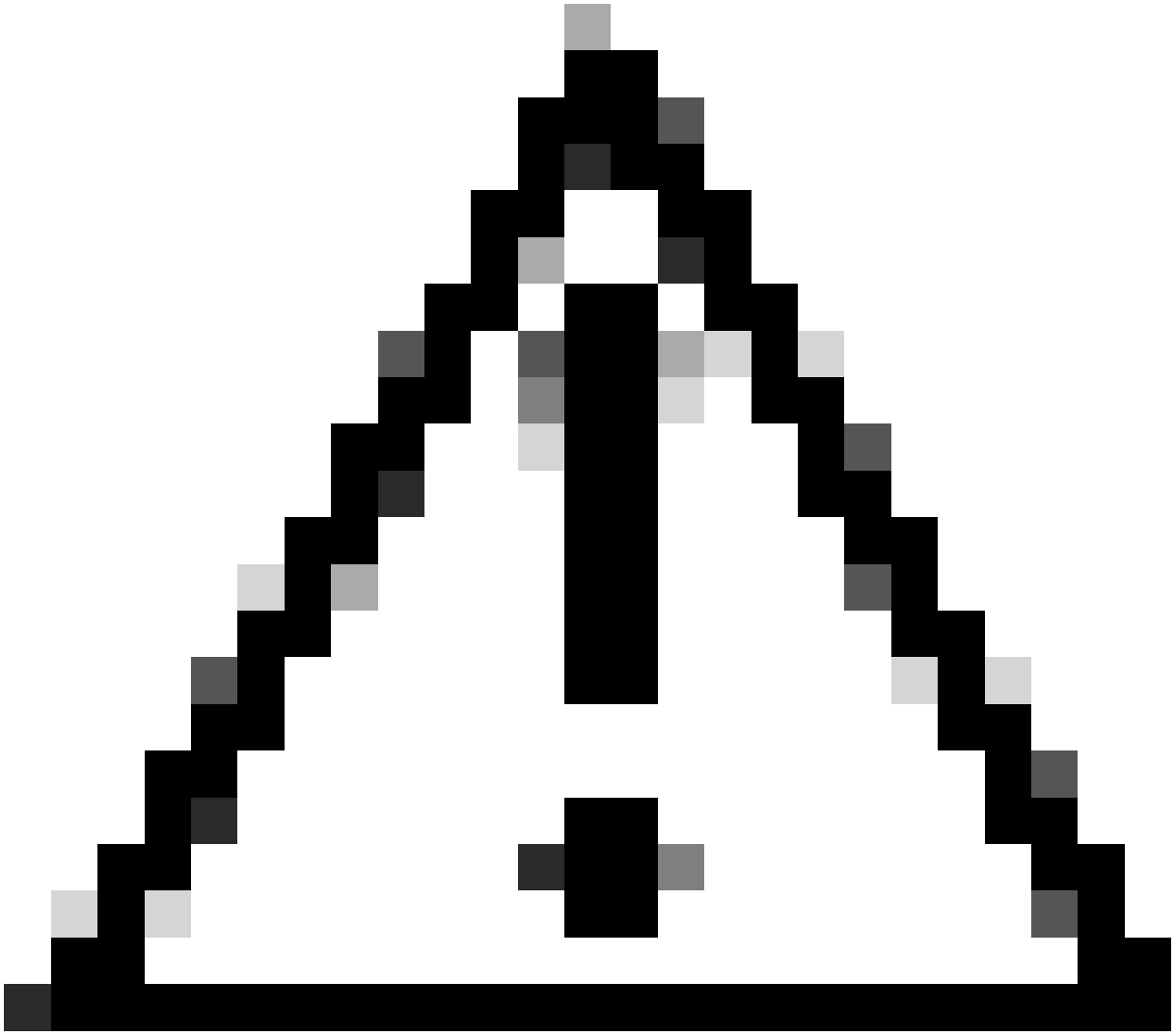
## Panoramica della verifica in due passaggi

La verifica in due passaggi (nota anche come autenticazione a due fattori) aggiunge sicurezza alla console Umbrella per MSP richiedendo un secondo fattore di autenticazione. Gli utenti devono immettere sia la password che un codice di protezione generato sul dispositivo mobile. Questo processo impedisce l'accesso non autorizzato tramite attacchi brute-force e garantisce che solo gli utenti autorizzati possano eseguire l'accesso.

È inoltre possibile abilitare la verifica in due passaggi per i singoli accessi client all'interno del dashboard di ogni client.

## Abilitazione della verifica in due passaggi

Prima di iniziare, è importante che l'autenticazione in due passaggi sia disabilitata per impostazione predefinita e che sia abilitata per l'account attualmente connesso.



Attenzione: È possibile abilitare la verifica in due passaggi solo per l'account attualmente connesso. Non è possibile modificare l'impostazione di un altro account amministratore, ma è possibile visualizzarne lo stato.

## Passi da abilitare

1. Passare a Impostazioni MSP > Amministratori.
2. Espandere la voce dell'account facendo clic sul nome dell'account.
3. Fare clic su Attiva.

È necessario selezionare e verificare il metodo preferito per ricevere i codici di sicurezza:

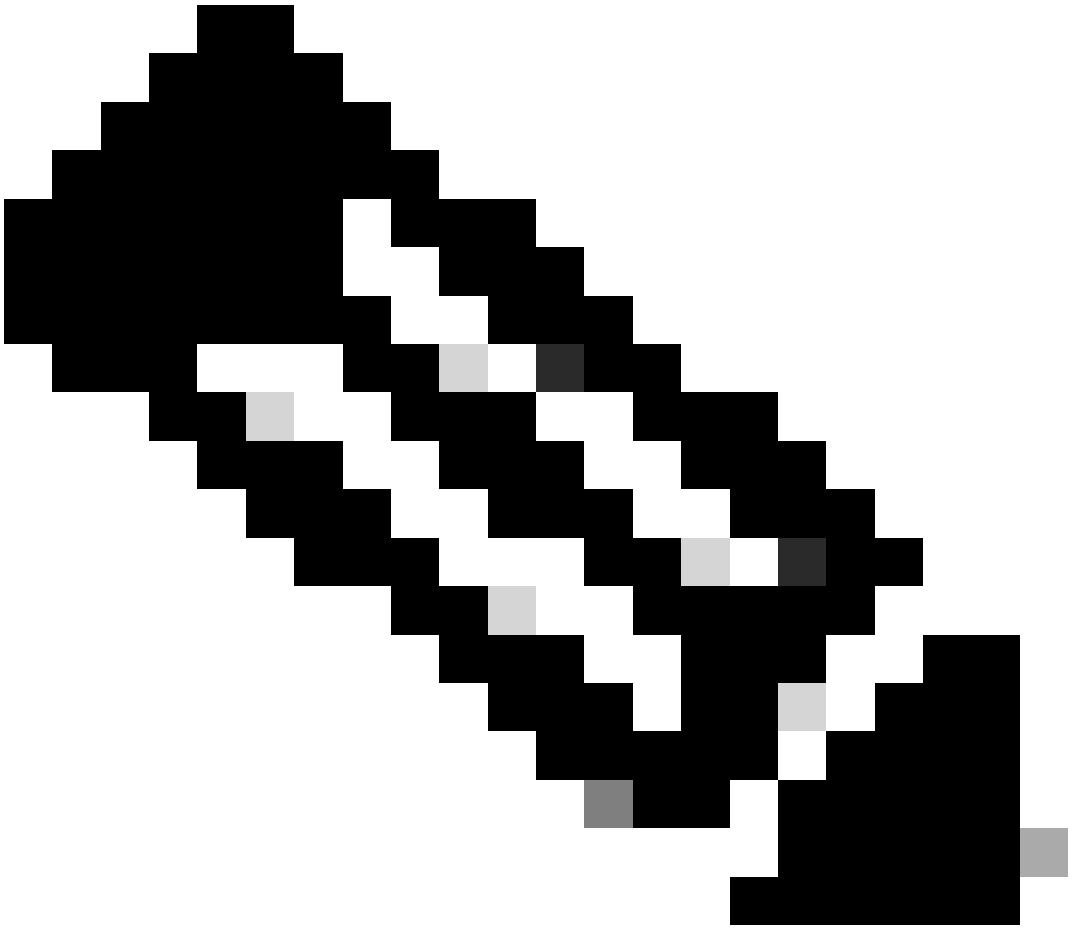
- SMS
- App mobile (app Autenticatore, ad esempio Google Authenticator)

Procedere con i passaggi in base al metodo scelto.

## Metodo 1: Usa SMS

1. Selezionare Utilizza messaggi di testo e fare clic su Continua.
2. Immetti il tuo numero di telefono, compresi il prefisso nazionale e l'indicativo di località, quindi fai clic su Continua.
3. Ricevi un codice a sei cifre tramite SMS.
4. Immettere la password Umbrella for MSP e il codice a sei cifre, quindi fare clic su Abilita verifica in due passaggi.
5. Salvare il codice di recupero di emergenza fornito. Archiviarlo in modo sicuro, separato dal dispositivo mobile e dalle password.
6. Fate clic su Fine (Done).

---



Nota: Riceverai un codice di protezione per gli SMS ogni volta che accedi. I codici di sicurezza scadono dopo 30 secondi. Se necessario, utilizzare Resend Code nella schermata di accesso.

Suggeriamo anche di usare Google Voice per l'SMS, perché se qualcuno ottiene

---

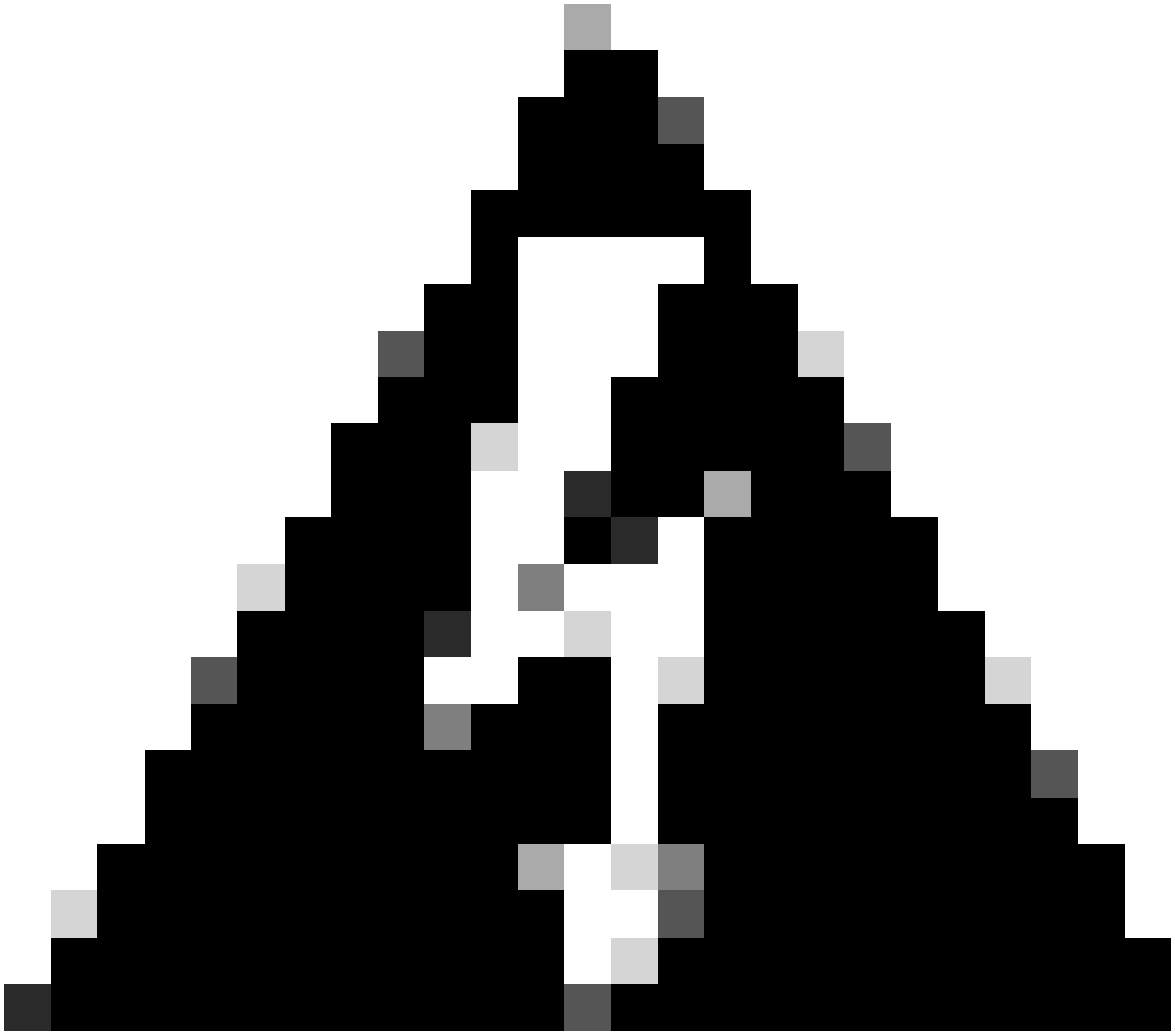
l'accesso al tuo account Gmail, l'aggressore può usare la funzione di reimpostazione password e anche ricevere password monouso.

---

## Metodo 2: Usa app mobile

1. Scaricare e installare un'app di autenticazione, ad esempio Google Authenticator, nel dispositivo mobile.
2. Selezionare Usa app per dispositivi mobili e fare clic su Continua.
3. Analizza il codice a matrice utilizzando l'app di autenticazione. Aggiungere un nuovo token e digitalizzare il codice a barre Viene quindi richiesto di digitalizzare un codice a matrice.
4. Aggiungere un nuovo token facendo clic sul segno + in basso a destra, quindi su Digitalizza codice a barre.
5. Immettere il codice a sei cifre generato e la password Umbrella for MSP, quindi fare clic su Abilita verifica in due passaggi.
6. Salvare il codice di recupero di emergenza fornito. Archiviarlo in modo sicuro, separato dal dispositivo mobile e dalle password. La protezione è efficace solo se la password e i codici di protezione sono separati.
7. Fate clic su Fine (Done).

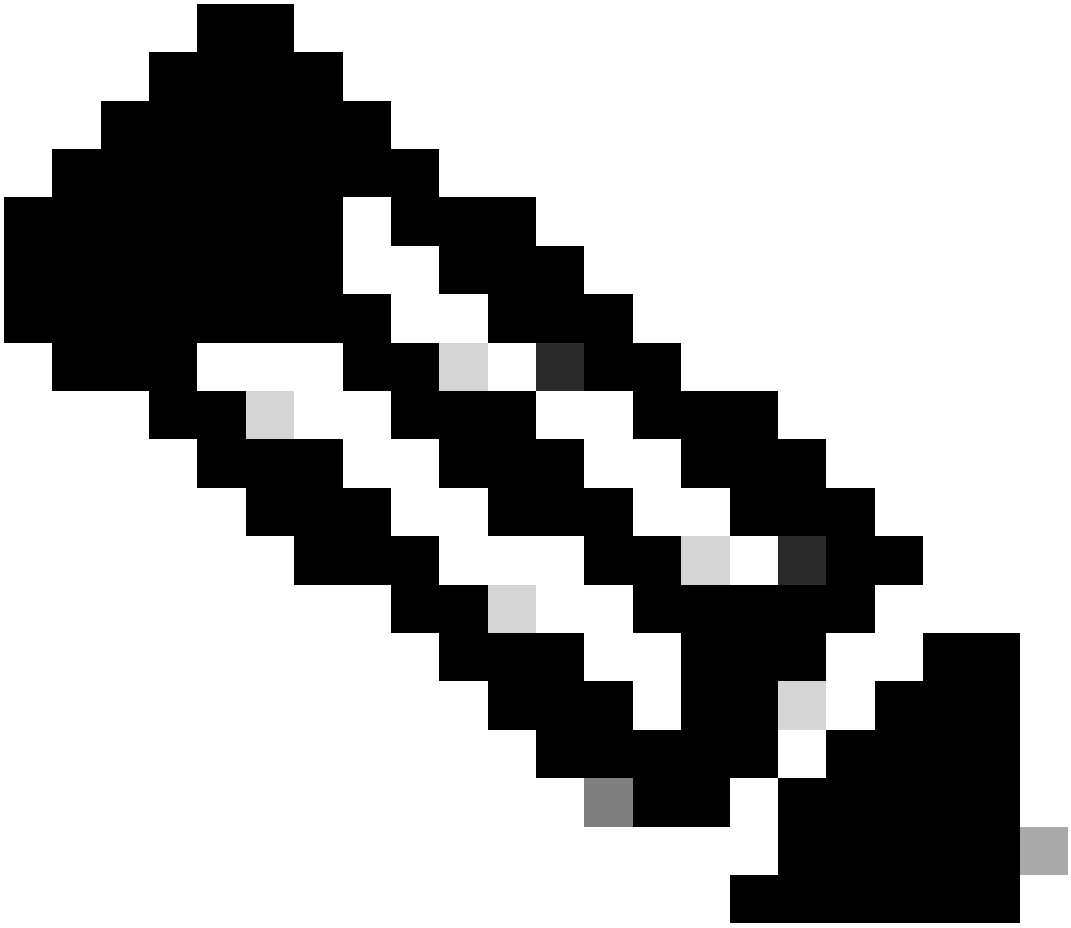
Una volta abilitata, l'app di autenticazione genera un nuovo codice ogni 30 secondi per l'accesso.



Avviso: Verificare che il dispositivo mobile sia sincronizzato correttamente con l'ora. L'ora errata del dispositivo può causare errori di verifica del codice.

## Accesso con verifica in due passaggi

Dopo aver immesso la password, immetti il codice di sicurezza ricevuto tramite l'app per dispositivi mobili o l'SMS. La schermata di verifica viene visualizzata dopo il login iniziale.



Nota: Se non si ricevono i codici SMS, il provider SMS (Twilio) potrebbe riscontrare dei problemi. Controlla lo stato di Twilio per gli aggiornamenti.

## Disabilita verifica in due passaggi

Se non desideri più utilizzare la verifica in due passaggi:

1. Passare a Configurazione > Impostazioni di sistema > Account.
2. Selezionare l'account e fare clic su Disabilita per l'autenticazione in due passaggi.
3. Ti verrà quindi inviato un nuovo codice di sicurezza occasionale e ti verrà chiesto di immetterlo un'ultima volta per confermare la richiesta.

## Telefono perso

Se hai perso il telefono (o il tablet) e non desideri più utilizzare la verifica in due passaggi, fai clic

su Hai perso il telefono? al momento dell'accesso. In questo modo si arriva in un'area in cui è possibile immettere il codice di ripristino di emergenza e disattivare il software. Come promemoria, il codice di recupero di emergenza è stato il codice fornito dopo la configurazione iniziale sia per SMS che per l'app mobile.

Se si perde sia il dispositivo che il codice di recupero di emergenza, il supporto richiede ulteriori informazioni per la reimpostazione dell'account.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).