

## Guida all'attivazione della 2FA per l'accesso al Pannello di Controllo di Hosting Solutions

Dal 12 novembre 2024 è obbligatorio aver attivato l'autenticazione a due fattori (2FA) per accedere al nostro Pannello di Controllo.

L'autenticazione a due fattori consiste in un sistema di 'autenticazione forte' che utilizza **contemporaneamente due metodi di autenticazione**: nel nostro caso questi due metodi consistono nell'autenticazione **tramite credenziali** (utente e password) e nell'autenticazione **tramite password OTP** (One Time Password).


Dal 12 novembre, quindi, se non è stata attivata la **2FA**, l'accesso al **Pannello di Controllo** sarà condizionato all'attivazione della autenticazione a due fattori.

Una volta effettuato il login, quindi, l'utente si troverà davanti ad una schermata che mostra un **QRCode** e un **codice alfanumerico** come in figura.

Autenticazione a 2 fattori

L'autenticazione a 2 Fattori è implementata tramite Google Authenticator, una app gratuita di Google. Installare sul proprio dispositivo l'app **Google Authenticator** e fare la scansione del seguente QRCode (oppure inserire manualmente il codice), dopodiché clicca sul pulsante Continua

Alternativamente sarà possibile ottenere il codice OTP tramite mail, una volta cliccato sul pulsante Continua



oppure inserisci manualmente

ABCD12DEFG34HILM

Continua

Per completare la procedura di attivazione della 2FA esistono due diverse modalità.

## QR Code o codice alfanumerico

Per questo sistema di autenticazione serve uno **smartphone** su cui è stata installata l'app **Google Authenticator** (o applicazione equivalente): una volta aperta l'app scansionare il QRCode mostrato nella schermata oppure, in alternativa, inserire il codice alfanumerico sottostante.

Se si usa Google Authenticator, aprire l'app e fare tap sull'icona **+** posta in basso a destra, quindi fare tap sulla voce **“Scansiona un codice QR”** oppure **“inserisci codice”**: nel primo caso si attiverà automaticamente la fotocamera (previa autorizzazione) per inquadrare il QRCode; nel secondo caso si dovrà inserire manualmente il codice alfanumerico mostrato nella stessa schermata.

Se l'operazione andrà a buon fine, **Google Authenticator** mostrerà un **codice OTP a sei cifre** che ha una validità di qualche decina di secondi e che quindi potrà essere utilizzato entro questo tempo di validità come secondo fattore di autenticazione per accedere al Pannello di Controllo. Se il codice scade, è sufficiente inserire il codice OTP generato successivamente, visto che l'app genera codici OTP in ciclo continuo.

## Ricevi OTP via email

In questa modalità, il **codice OTP viene trasmesso via email**. Per attivarlo è necessario fare clic su **“Ricevi OTP via Mail”**, presente nel form di inserimento dell'OTP, come in figura. Utilizzando questo comando, il codice OTP verrà inviato alla **casella mail di contatto dell'utente che sta effettuando l'accesso al Pannello di Controllo**.

Autenticazione a 2 fattori

Inserisci codice OTP

☐ Ricorda questo browser

Continua

Ricevi OTP Via Mail

UserCP

GroupCP

## Salvataggio dell'autenticazione

Per non dover inserire l'**OTP** ogni volta che ci si collega dallo stesso browser è sufficiente fare clic sulla casella **Ricorda questo browser** (vedi figura) prima di cliccare su **Continua**. Da quel momento, gli accessi successivi **attraverso lo stesso browser** potranno essere effettuati utilizzando esclusivamente le credenziali, senza l'OTP.

Se si utilizza più browser, anche su dispositivi diversi, per accedere al Pannello di Controllo, sarà necessario spuntare la casella per ciascun browser al momento dell'accesso