Istruzioni di accesso alla piattaforma CGM STUDIO con MFA

L'autenticazione multifattoriale (MFA) è un metodo di autenticazione che richiede all'utente di fornire almeno due fattori di verifica per poter accedere all'applicazione CGM Studio.

Per la MFA su CGM Studio l'utente può scegliere tra tre (3) fattori di autenticazione dopo aver inserito username e password e cioè **SMS Code** o **Google Authentication Code**, oppure il fattore di sicurezza ultimo detto **Recovery code** che viene generato alla fine del primo processo di autenticazione.

Riepilogando, i fattori della MFA per CGM Studio sono i seguenti:
1) **Autenticazione tramite SMS**
2) **Autenticazione tramite App Google Authenticator**
3) **Recovery Code**

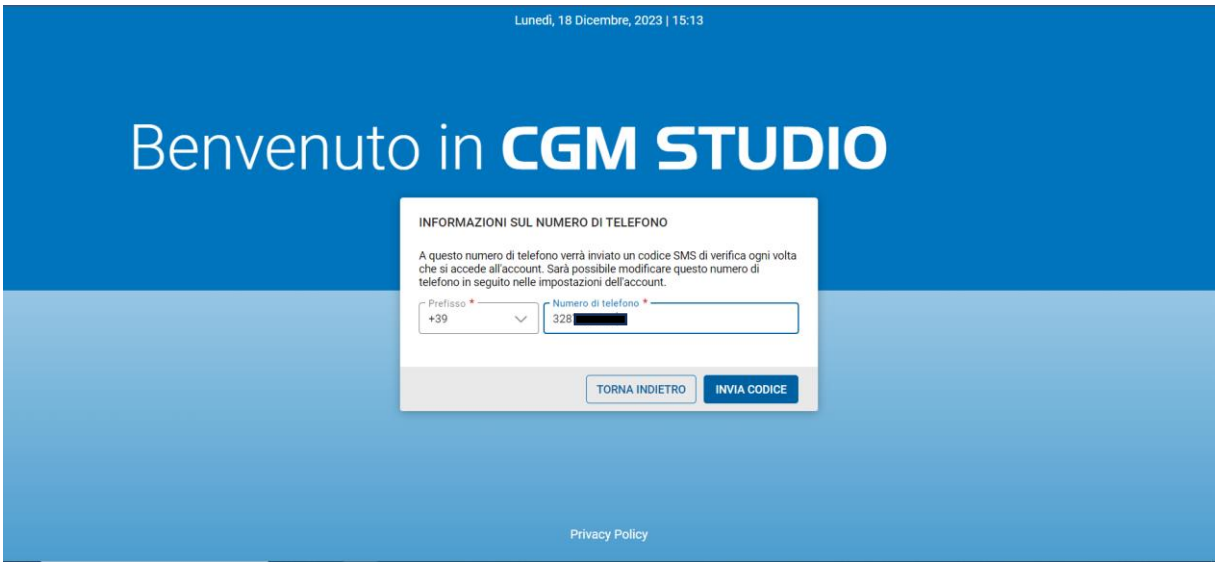
CONFIGURAZIONE AUTENTICAZIONE A DUE FATTORI CON SMS O APP GOOGLE AUTHENTICATOR

1

Inserite le proprie credenziali di accesso Username e Password, l'applicazione presenta una finestra nella quale viene proposta la configurazione di uno dei due metodi di autenticazione o di entrambi.

2

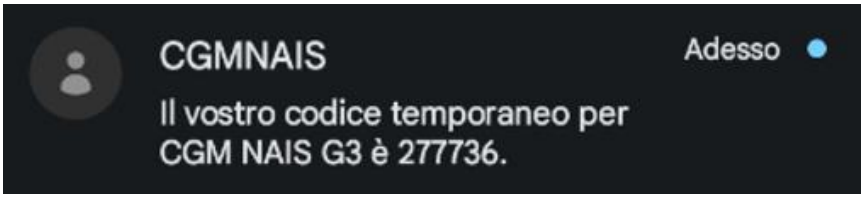
Una volta scelta l'opzione **Autenticazione tramite SMS**, viene visualizzata una finestra, dove è necessario inserire il proprio numero di cellulare e inviare il codice SMS di autenticazione



3

Dopo aver cliccato su INVIA CODICE, verrà visualizzata una finestra contenente 6 caselle in cui inserire il codice che giungerà in pochi istanti, via SMS, sul numero di cellulare indicato precedentemente.

Esempio di SMS contenente codice temporaneo di autenticazione



4

Inserito il codice corretto, sarà possibile procedere con il Login oppure configurare l'ulteriore fattore di autenticazione tramite **App Google Authenticator**.

Per configurare la modalità di autenticazione tramite Applicazione **Google Authenticator**, sarà necessario:

- scaricare e installare l'applicazione sul proprio dispositivo mobile
- aprire l'applicazione
- cliccare sull'icona **+**
- scansionare il codice QR proposto o inserire i codici di autenticazione proposti.

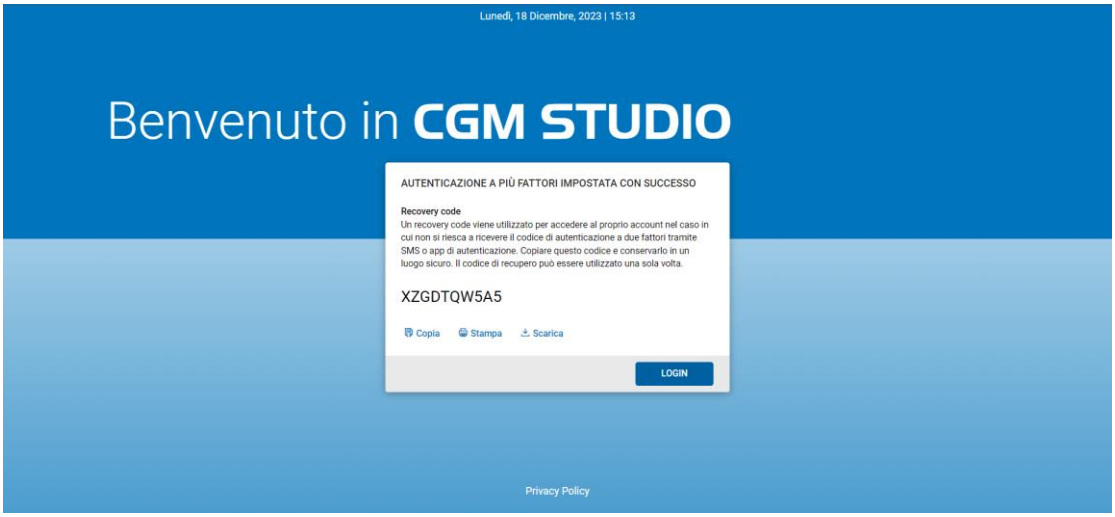
Verrà generato un codice dall'applicazione **Google Authenticator** che sarà necessario inserire nelle caselle proposte a video.

RECOVERY CODE

Dopo aver configurato uno o entrambi i fattori di autenticazione, il sistema ne fornisce un terzo automaticamente: **Recovery code**.

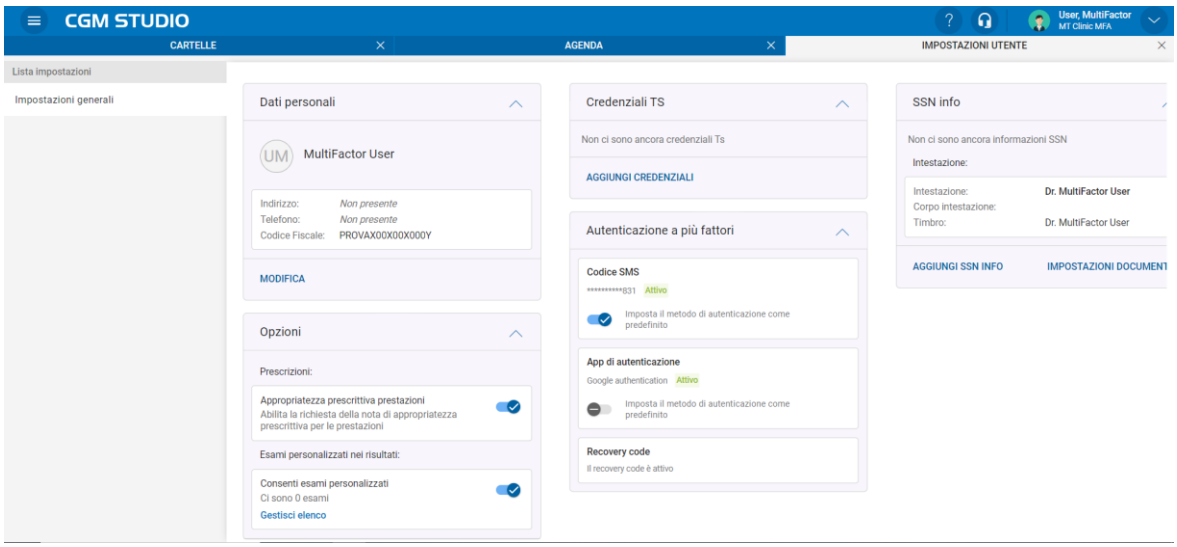
Il **Recovery code** viene generato una sola volta e può essere ugualmente utilizzato una sola volta nell'eventualità in cui non si abbia la possibilità di loggarsi utilizzando i fattori di autenticazione come **Autenticazione tramite SMS** o **Autenticazione tramite App Google Authenticator**.

Sarà possibile stamparlo, copiarlo o scaricarlo per non perderlo mai e utilizzarlo in caso di necessità.

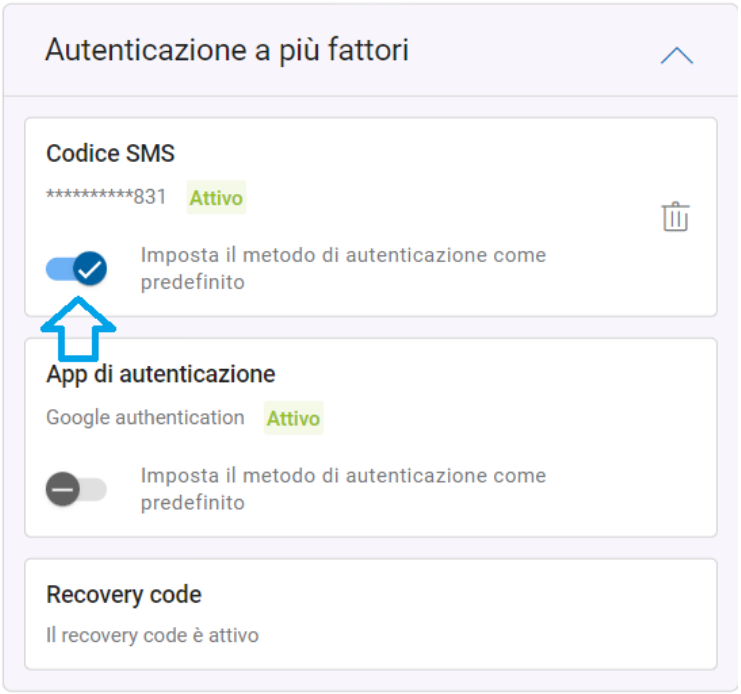


GESTIONE PERSONALIZZAZIONE IMPOSTAZIONI DI AUTENTICAZIONE

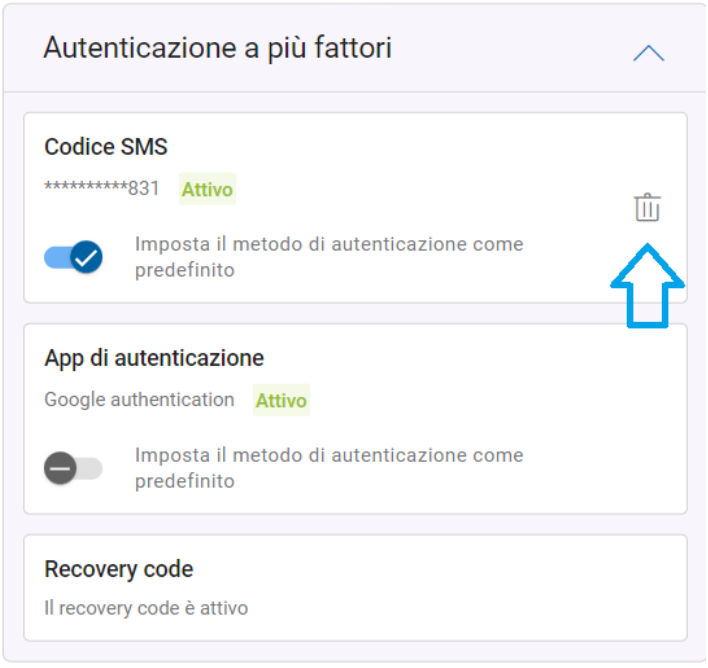
Una volta effettuato il login, sarà possibile gestire le impostazioni relative all'Autenticazione a più fattori dalla sezione delle **Impostazioni Utente**.



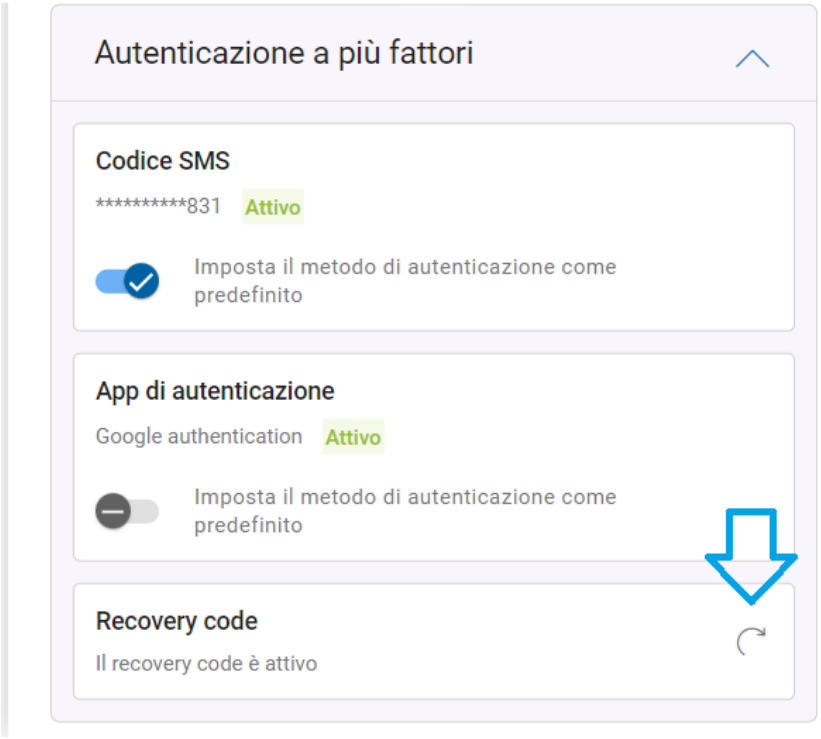
Nel caso in cui entrambi i fattori di autenticazione siano stati abilitati, si potrà scegliere quale dei due utilizzare come predefinito.



Sarà inoltre possibile eliminare uno dei due fattori (solo se sono stati preventivamente abilitati entrambi), dopo aver cliccato sull'icona del cestino in corrispondenza del fattore da eliminare e dopo aver confermato le proprie credenziali di accesso username e password.



Sempre nella sezione delle impostazioni, sarà possibile generare un nuovo **Recovery code** nel caso sia stato smarrito o il precedente non sia più utilizzabile (previa conferma delle proprie credenziali di accesso username e password).



Una volta effettuato il login e aver utilizzato l'autenticazione a due fattori per la prima volta, il sistema non richiederà più l'inserimento del secondo fattore fino a quando riterrà il device, sul quale si sta effettuando l'accesso, come totalmente sicuro (trust access) oppure fino a quando non si renderà necessario autenticarsi nuovamente con l'autenticazione a due fattori secondo le tempistiche previste dal servizio di autenticazione stesso.