



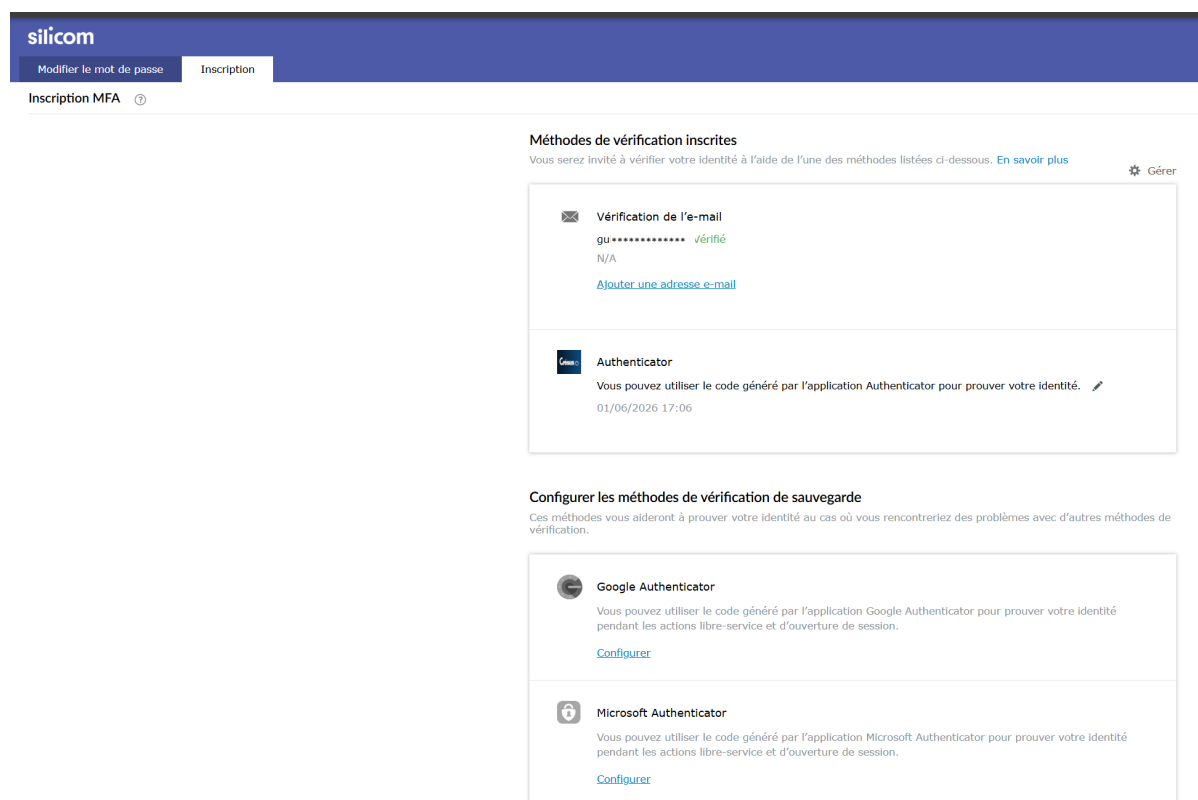
Crésus Cloud

3.1 - Gérer les codes de double authentication

3.1 - Gérer les codes de double authentication

Cette procédure décrit les étapes à suivre en cas de perte ou de remplacement d'un smartphone, ainsi que celles permettant à un collaborateur d'accéder au compte Cresus Cloud partagé.

- Accédez à la page mfa.komodo.ch, puis connectez-vous avec vos identifiants.
- Dans la page qui s'affiche, ouvrez l'onglet *Inscription* :

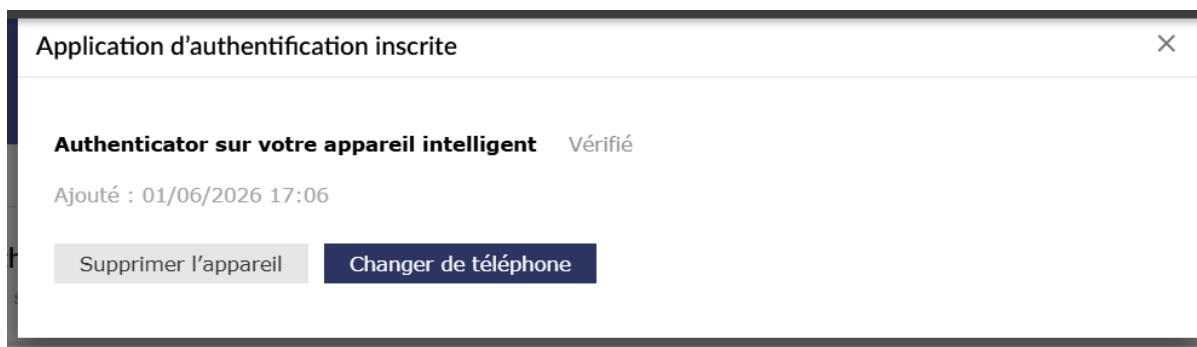


The screenshot shows the 'Inscription MFA' page on the silicom portal. It features a navigation bar with 'Modifier le mot de passe' and 'Inscription' tabs. The main content area is titled 'Méthodes de vérification inscrites' and lists two methods: 'Vérification de l'e-mail' (verified) and 'Authenticator'. Below this, there is a section for 'Configurer les méthodes de vérification de sauvegarde' with options for 'Google Authenticator' and 'Microsoft Authenticator'.

- Cliquez sur l'icône en forme de crayon située à côté de *Authenticator*.

Vous pouvez alors choisir entre les deux options suivantes :

- *Changer de téléphone* : permet de configurer l'authentification à deux facteurs sur un nouveau smartphone.
- *Supprimer l'appareil* : permet de supprimer l'appareil actuellement enregistré.



Si vous choisissez *Changer de téléphone*, un nouveau code QR permettant de configurer l'authentification à deux facteurs s'affiche.

Ouvrez l'application d'authentification (Authenticator) sur votre nouveau smartphone, puis scannez le code QR pour configurer l'accès.



Pour permettre à un collaborateur d'accéder au compte Cresus Cloud partagé, vous pouvez configurer une méthode d'authentification supplémentaire.

Suivez les instructions affichées à l'écran pour enregistrer cette méthode.