Maker Produkte Version 5
Authentification forte

1.

L'activation de l'authentification forte augmente la sécurité de votre logiciel. En plus de votre mot de passe, vous avez besoin d'un code généré par Authenticator-App sur votre smartphone.

Apps prises en charge :

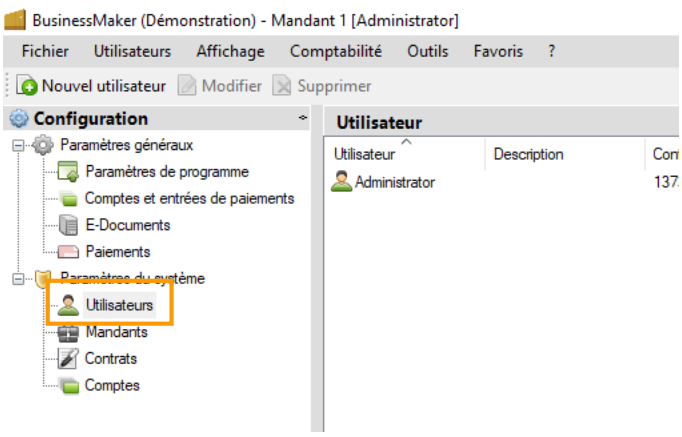
- Google Authenticator
- Microsoft Authenticator

2.

Pour activer l'authentification forte, cliquez sur:
Fichier – Configuration – Utilisateur

A droite vous avez tous les noms d'utilisateur.

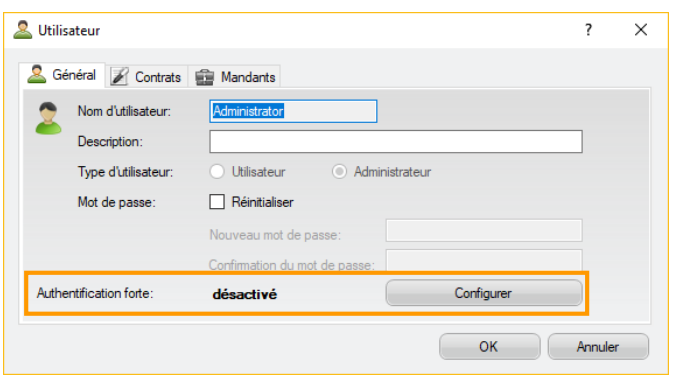
Sélectionnez l'utilisateur approprié pour lequel l'authentification forte doit être activée.



3.

Dans la boîte de dialogue utilisateur, vous trouverez l'option Authentification forte avec le statut « Désactivé ».

Cliquez sur « Configurer ».

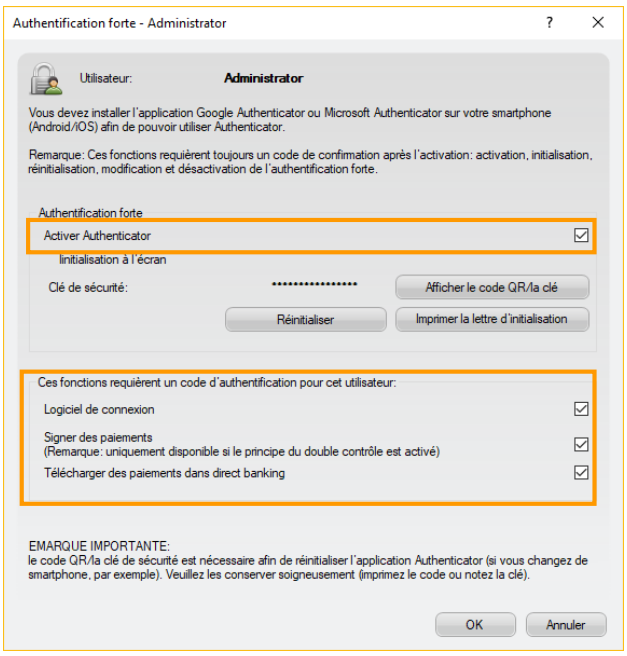


Maker Produkte Version 5
Authentification forte

4.

Pour activer l'authentification forte, cochez la case appropriée.

Sélectionnez ci-dessous les options correspondantes que vous souhaitez sécuriser en plus (pour PayMaker Home, seule la première option est disponible). Respectez les consignes de sécurité.



5.

Afficher le code QR / la clé :

Avec cette option, vous pouvez afficher le code QR.

Imprimer la lettre d'initialisation :

Vous pouvez imprimer ici la lettre d'initialisation qui a été créée lors de la configuration aussi souvent que vous le souhaitez.

Réinitialiser:

A partir du bouton «Réinitialiser», le code QR / la clé en cours sera renouvelé et l'initialisation doit avoir lieu à nouveau.

6.

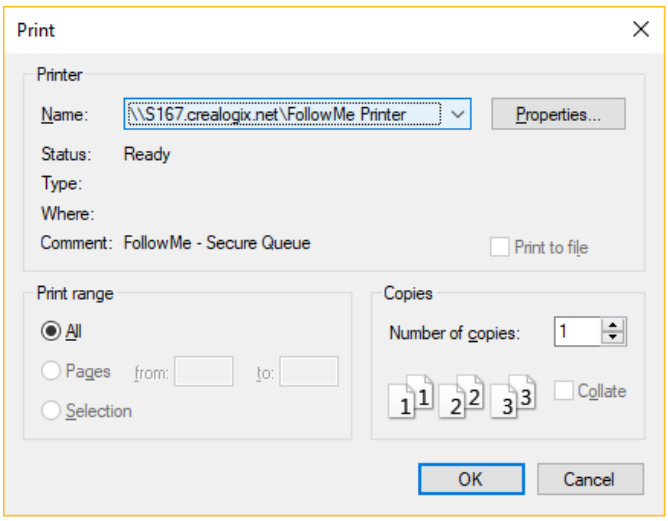
Confirmez votre sélection aux points 4. et 5. avec "OK".

Veuillez scanner le code QR avec Google Authenticator et après entrer le code généré par l'Authenticator pour terminer l'initialisation de l'authentification à deux facteurs.

7.

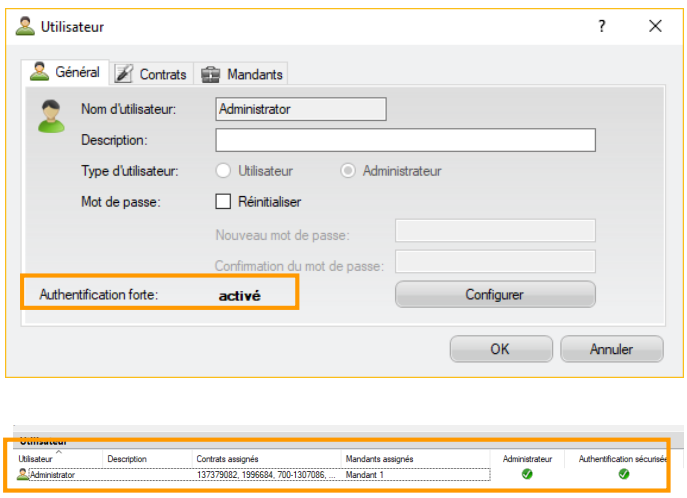
Une fois l'initialisation réussie, il vous sera demandé d'imprimer la lettre d'initialisation. Pour des raisons de sécurité, ce processus d'impression ne peut pas être exécuté à l'aide d'une imprimante virtuelle ou sauvegardé (par exp: en PDF, etc..), mais uniquement à l'aide d'une imprimante physique.

Cette lettre d'initialisation est nécessaire en cas de perte du smartphone ou pour la récupération lors de la désinstallation et réinstallation de l'application.



8.

Une fois l'authentification forte est terminée avec succès, l'état d'authentification forte est « activé » dans la boîte de dialogue de l'utilisateur.



9.

Si l'option "Login Software" est activée, vous serez invité à entrer le code d'authentification lors de la prochaine connexion dans le logiciel.

Pour ce faire, ouvrez votre application d'authentification et entrez le code qui y est affiché.