

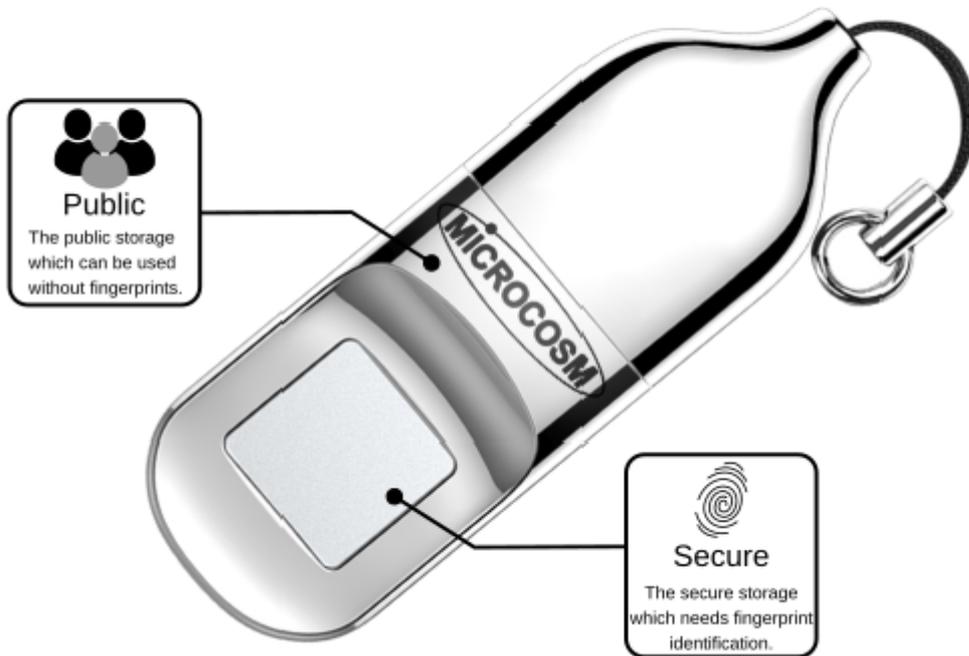
Clé USB Biométrique Guide de l'utilisateur

KORUM SECURE - 2024

Table des matières

1/ Introduction.....	2
2/ Aperçu.....	2
3/ Spécifications	3
4/ Logiciel de Gestion des Empreintes Digitales	3
5/ Enregistrement pour les Administrateurs	3
6/ Utilisation de la Clé USB Biométrique.....	5
7/ SUPPORT :.....	8

1/ Introduction



2/ Aperçu

Merci d'avoir acheté la Clé USB Biométrique.

Cet appareil combine la technologie d'identification biométrique et le stockage de données. Conçu pour ceux qui exigent un niveau élevé de protection des données, cet appareil protège les données sensibles contre tout accès non autorisé grâce à l'authentification par empreinte digitale.

Les données stockées dans la partition sécurisée sont protégées et ne peuvent être accessibles qu'après authentification d'une empreinte digitale enregistrée. Offrant à la fois commodité et sécurité, il évite de mémoriser des mots de passe et vous assure une tranquillité d'esprit.

3/ Spécifications

Interface	USB 2.0
Empreintes Digitales Stockées	jusqu'à 6 empreintes
Capacité	32GB
Systèmes Pris en Charge (Logiciel de Gestion)	Windows XP(SP3), Windows Vista, Windows 7, Windows 8, Windows 10 (64bit), Windows 11 (64bit)
Systèmes Pris en Charge (Clé USB)	Windows XP(SP3), Windows Vista, Windows 7, Windows 8, Windows 10 (64bit), Windows 11 (64bit), Linux, MacOS

4/ Logiciel de Gestion des Empreintes Digitales

Lors de la première utilisation de la Clé USB Biométrique, lancez l'application de gestion des empreintes digitales intégrée. Cette application permet de définir un mot de passe, d'enregistrer des empreintes digitales, de gérer les utilisateurs et de protéger vos données personnelles.

Étapes pour lancer l'application de gestion des empreintes digitales :

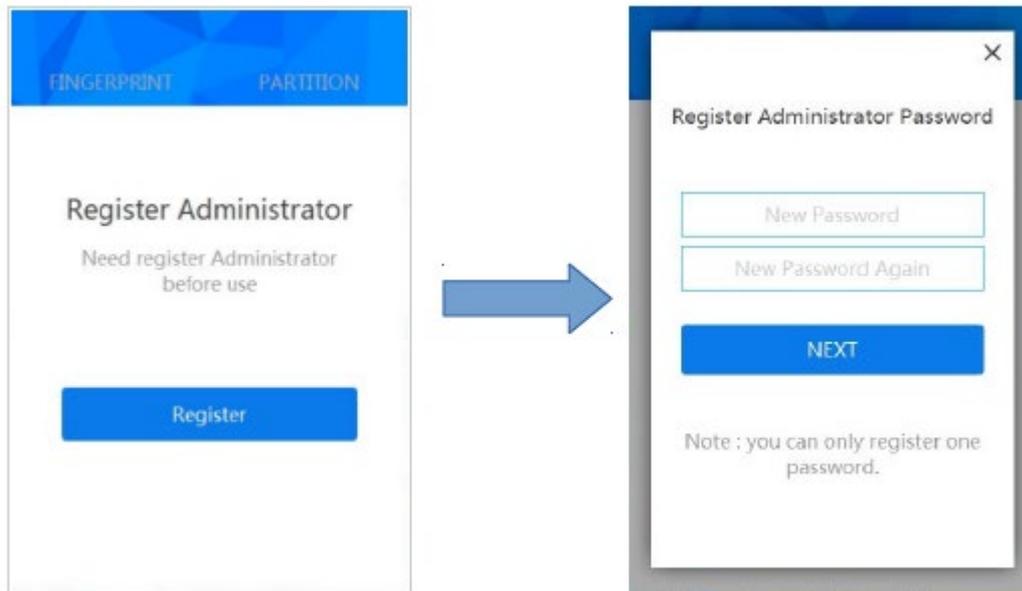
1. Connectez la Clé USB Biométrique à un port USB disponible sur votre ordinateur.
2. Cliquez sur le lecteur CD nommé "MICROCOSM" dans la liste des lecteurs de votre ordinateur.
3. Double-cliquez sur "FingerprintTool.exe" pour lancer l'application de gestion.

5/ Enregistrement pour les Administrateurs

Pour créer des comptes et enregistrer des empreintes digitales pour les utilisateurs généraux, vous devez préalablement enregistrer un compte administrateur.

Définir un Mot de Passe pour l'Administrateur :

1. Cliquez sur REGISTER à l'écran d'accueil.
2. Choisissez un mot de passe administrateur en le saisissant deux fois.
3. Cliquez sur NEXT.



Enregistrer une Empreinte Digitale pour l'Administrateur :



1. Saisissez le nom de l'administrateur, puis cliquez sur NEXT.
2. Cliquez sur NEXT.
3. Enregistrez votre empreinte digitale en suivant les instructions affichées dans l'application. Vous pouvez redémarrer l'enregistrement de l'empreinte en cliquant sur "Re-entry".

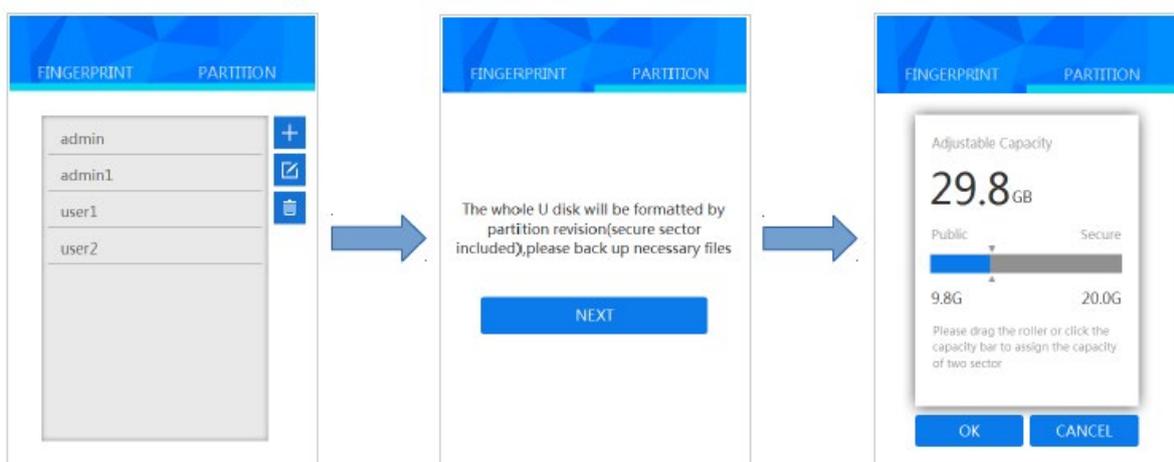
Remarque : Nous vous suggérons de légèrement changer l'angle de votre doigt à chaque tentative pour permettre au système de stocker les données de la pulpe, des côtés et du bout de votre doigt. Répétez cette étape 6 fois jusqu'à ce que l'enregistrement de votre empreinte soit complet.

6/ Utilisation de la Clé USB Biométrique

Accès à la Partition Sécurisée :

1. Connectez la Clé USB Biométrique à un port USB disponible sur votre ordinateur.
2. Une lumière bleue clignotera. Placez votre doigt (celui enregistré) sur le capteur d'empreinte avec une pression légère et uniforme. Une fois l'empreinte authentifiée, la partition sécurisée apparaîtra dans la liste des lecteurs de votre ordinateur et vous pourrez accéder aux données stockées.

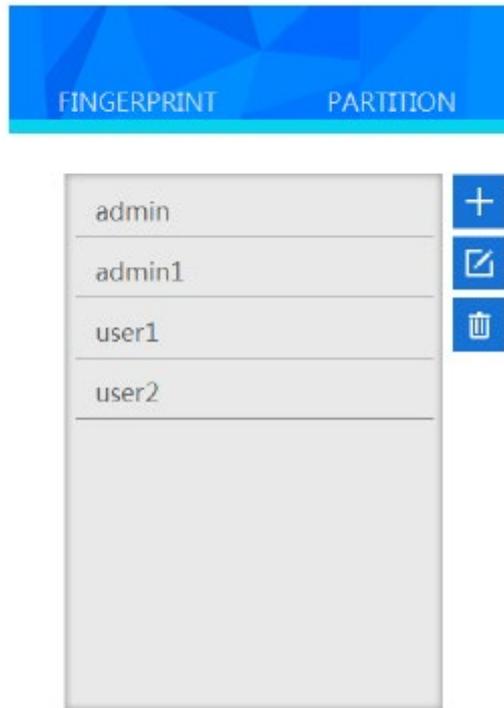
Partitionnement :



1. Lancez l'application FingerprintTool.exe, utilisez l'empreinte administrateur pour l'authentification, puis cliquez sur l'onglet "PARTITION".
2. Cliquez sur NEXT.
3. Ajustez la capacité des partitions publique et sécurisée avec la souris. Cliquez sur "OK" pour confirmer l'ajustement. Déconnectez puis reconnectez l'appareil après avoir modifié les partitions.

Gestion des Comptes Admin et Utilisateurs :

- Ajouter une nouvelle empreinte .
- Changer le mot de passe et l'empreinte du compte sélectionné .
- Supprimer le compte sélectionné (Note : Conservez au moins une empreinte de l'administrateur) .



Gestion des Mots de Passe :



1. Cliquez sur "Password Verification" dans la fenêtre d'authentification par empreinte.
2. Cliquez sur "Forget Password" dans la fenêtre d'authentification par mot de passe.
3. Saisissez un nouveau mot de passe.
4. Cliquez sur NEXT et utilisez l'empreinte administrateur pour terminer le paramétrage.

FAQ

- Pourquoi la clé USB n'est-elle pas reconnue ?

Retirez et reconnectez la clé USB. La clé est sans pilote elle fonctionne sans aucune installation

- Pourquoi ne puis-je pas accéder à la partition sécurisée après avoir placé mon doigt sur le capteur d'empreinte ?

Votre empreinte peut ne pas être lue si votre doigt est trop humide ou s'il y a des débris sur votre doigt ou le capteur. Nettoyez et séchez votre doigt et le capteur. Reconnectez la clé USB si cela ne fonctionne toujours pas.

- Pourquoi la clé USB n'a-t-elle que 10GB de capacité ?

La capacité disponible de la clé USB de 32GB est de 29,6GB. La capacité par défaut de la partition publique est de 10GB. Vous pouvez modifier la taille des partitions via l'application de gestion. Veuillez consulter la section Partitionnement de ce guide.

- La clé USB biométrique fonctionne-t-elle via USB OTG sur un smartphone ?

Seule la partition publique est accessible via OTG sur un smartphone compatible.

- Pourquoi ne puis-je pas enregistrer des fichiers de plus de 4GB sur la clé USB ?

Le format initial de la clé USB biométrique est FAT32, vous devez la formater en exFAT pour stocker des fichiers de plus de 4GB.

- Quels sont les systèmes compatibles avec l'application d'empreintes digitales ?

Veuillez consulter la section Spécifications de ce guide.

- Quel est le principe de cryptage de la clé USB ?

Le cryptage AES256 est utilisé et les données des empreintes sont sauvegardées avec un UID exclusif produit par le FPIC. Comme la méthode de calcul des données d'empreintes et des empreintes est séparée, les données de la partition sécurisée seront perdues si la clé USB est démontée de force.

- Combien de fois peut-on entrer un mot de passe administrateur incorrect ?

Si l'utilisateur entre un mot de passe incorrect plus de 254 fois de suite, l'appareil détruira toutes les données stockées.

7/ SUPPORT :

Si vous avez besoin d'assistance pour l'utilisation de nos produits, n'hésitez pas à nous contacter au contact@korum-secure.fr