



Solution Technique de 2FA

Dans le cas du projet pour le choix d'un nouvel équipement nomade et sécurisé, nous vous proposons de sécuriser l'équipement avec une solution d'authentification à deux facteurs qui permet l'accès sécurisé sous Windows à l'aide de token USB **Rohos Logon Key**

Rohos Logon Key

GodMod
La Clé USB n'est pas encore configurée.
Pour utiliser **USB token Bluetooth le téléphone comme USB clé** [Configurer les options...](#) [Aide...](#)

- Configurer une clé USB**
Configurer votre clé USB pour ouvrir une session Windows. Paramétrer un code PIN. [Setup smartphone](#)
- Configurer les options**
Changer l'écran d'accueil, choisir le comportement lorsqu'on enlève la clé USB, personnaliser le texte d'accueil.
- Setup OTP token**
You can setup Google Authenticator or Yubikey HOTP as a login method to your computer..
- Users and keys**
Manage the list of registered users and authentication devices.

Créé par **Tesline-Service** fondé en 2000 dans le but de répondre à la nécessité croissante pour les services IT dans l'Europe de l'Est. En 2003 il commence à développer la gamme de produits **Rohos** – la Sécurité des Données de l'Ordinateur et le logiciel de Contrôle d'Accès.

Rohos Logon Key transforme une simple clé de stockage USB en une clé d'accès sécurisé sous Windows.



Mieux sécuriser votre ordinateur:

- Remplacez le mot de passe simple sur lequel est basée votre authentification par un pass d'authentification USB matériel (clé de stockage USB ou carte mémoire)
- Utilisez un mot de passe complexe, sans avoir besoin de vous en rappeler
- L'authentification par clé USB est entièrement automatique et rapide!
- Le système est protégé par un mot de passe matériel, sans nécessité de le rentrer manuellement
- Authentification sécurisée à 2 facteurs: votre Clé USB + code PIN
- N'utilisez qu'une seule et unique clé USB pour accéder en toute sécurité à votre ordinateur familial, à votre PC portable et à votre PC de bureau
- Restriction de l'accès à l'ordinateur basée sur le facteur temps/Clé USB
- Windows est protégé, même en Mode Sans Échec
- En assignant un mot de passe à votre compte d'utilisateur; vous allez obtenir une meilleure protection en temps que l'ordinateur est mise en veille.

Aucun risque grâce aux dispositions qui suivent:

1. Logon de Secours, vous aide à accéder à votre système au cas où vous perdriez la clé USB où vous oublieriez le Code PIN
2. Code PIN pour protéger la Clé USB contre l'authentification non-autorisée (avec des tentatives d'entrer limitées)
3. Protection en Mode Sans Échec- ne permet pas à une personne mal-intentionnée à contourner la sécurité de la clé USB en chargeant Windows en Mode Sans Échec
4. Rohos utilise les principes de sécurisation des données approuvés par le NIST: le mot de passe n'est pas stocké en libre accès sur la Clé USB, la protection contre la copie de la Clé USB ne permet pas de créer des copies non autorisées. Toutes les données existantes sur la Clé sont chiffrées grâce à une clé AES de 256 bit.

La variété du Matériel:

- n'importe quelle clé de stockage USB
- les token USB /carte à puce Aladdin eToken PRO, Futako HiToken v22, Aktiv ruToken, uaToken, Crypto Identity 5,etc
- YubiKey et Swekey – token avec un mot de passe à usage unique
- Les clés USB avec lecteur d'empreintes digitales, par exemple: Transcend, Apacer, LG, TakeMS etc.
- Les PDA et téléphone portables Bluetooth
- Tag RFID



Avantages et inconvénients

Nous avons décidé de choisir **Rohos Logon Key** car nous lui trouvons énormément d'avantages :

- Multitude de solution d'authentification
- Large choix de configuration
- Facilité à mettre en oeuvre
- Pas besoin d'être connecter à internet

Le seul inconvénient :

- Cette solution est payante 75€ la licence pro qui permet 3 ordinateurs, nous avons donc besoin de 52 licences pro, avec une remise de 5% nous en avons pour un total de 3529,5€ HT.

Mise en oeuvre

Dans notre cas nous n'utilisons pas toutes les solutions que propose **Rohos Logon Key**

Nous configurons pour la solution d'**authentification à deux facteurs** :

- User+Mot de passe et clé de sécurité USB
- et
- User+Mot de passe et un One-Time password



Administrateur

Installation des solutions 2FA

Création de la clé de sécurité

Aller dans “Configurer une clé USB”

Rohos Logon Key

GodMod
La Clé USB n'est pas encore configurée.
Pour utiliser **USB token Bluetooth le téléphone comme USB clé** [Configurer les options...](#) [Aide...](#)

- Configurer une clé USB**
Configurer votre clé USB pour ouvrir une session Windows. Paramétrer un code PIN. [Setup smartphone](#)
- Configurer les options**
Changer l'écran d'accueil, choisir le comportement lorsqu'on enlève la clé USB, personnaliser le texte d'accueil.
- Setup OTP token**
You can setup Google Authenticator or Yubikey HOTP as a login method to your computer..
- Users and keys**
Manage the list of registered users and authentication devices.

Choisissez “USB flash drive” si il n’est pas de base, puis “Sélection de l’Utilisateur”

Configurer la clé USB

Vous voulez configurer votre clé USB comme une clé d'accès matérielle? votre ordinateur. Lorsque vous voudrez ouvrir votre session Windows, il vous faudra insérer cette clé USB.

Utilisateur: **GodMod**, [Sélection de l'Utilisateur...](#)

Vous pouvez choisir le type périphérique de la Clé USB pour l'utiliser en Rohos:

USB flash drive

Le volume USB **D:** a été détecté [\[Choisir...\]](#)

Veuillez entrer votre mot de passe de session Windows:

Installer le code PIN Pour protéger votre clé USB de toute utilisation non autorisée. Une clé USB sera bloquée après 3 essais sans succès. [Débloquer une clé USB...](#)



Sélectionner “Avancé...”.

Sélectionnez un utilisateur

Sélectionnez le type de cet objet :

un utilisateur

Types d'objets...

À partir de cet emplacement :

DESKTOP-37IV5AD

Emplacements...

Entrez le nom de l'objet à sélectionner (exemples) :

Vérifier les noms

Avancé... OK Annuler

Puis sélectionnez votre utilisateur qui aura la 2FA et faites “OK”.

Sélectionnez un utilisateur

Sélectionnez le type de cet objet :

un utilisateur

Types d'objets...

À partir de cet emplacement :

DESKTOP-37IV5AD

Emplacements...

Requêtes communes

Nom : Commence par

Description : Commence par

Comptes désactivés

Mot de passe sans date d'expiration

Nombre de jours depuis la dernière session :

Colonnes...

Rechercher

Arrêter

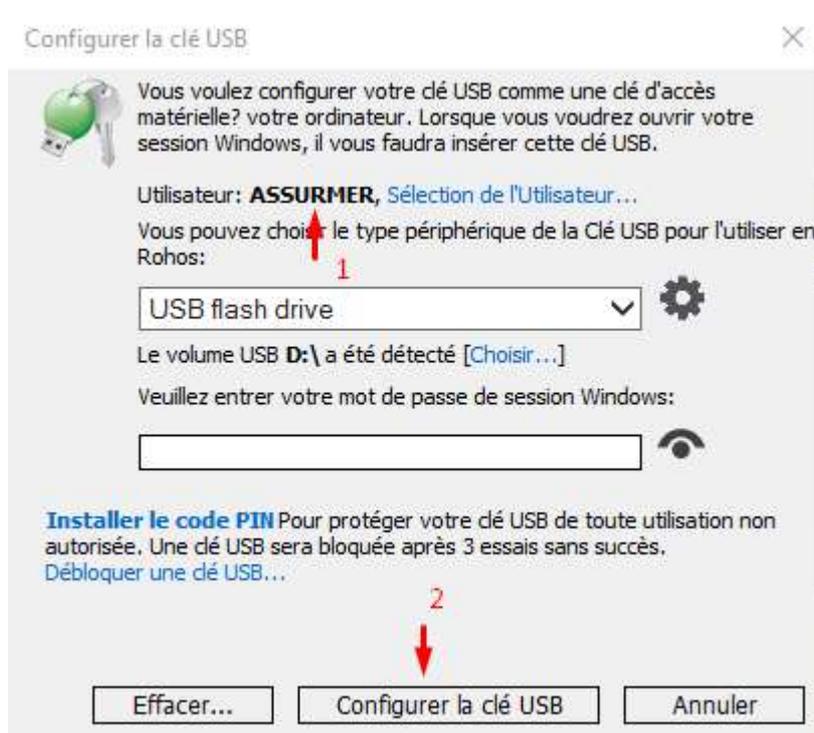
Résultats de la recherche :

Nom	Dossier
Administrateur	DESKTOP-37IV...
ASSURMER	DESKTOP-37IV...
DefaultAccount	DESKTOP-37IV...
GodMod	DESKTOP-37IV...
Invité	DESKTOP-37IV...
WDAGUtilityA...	DESKTOP-37IV...

OK Annuler



Assurez vous de bien avoir votre utilisateur, puis “Configurer la clé USB”





Création de la clé One-Time Password

Aller dans “Setup OTP token”

Sélectionner votre utilisateur et cocher “Google Authenticator TOTP” puis cliquer sur “Display QR code” cela va ouvrir un page web avec un QR code, faites “Ctrl+S” pour sauvegarder et sauvegarder la à la racine de la clé USB de l'utilisateur, puis “Setup OTP Token”.



Configuration

Aller dans “Configurer les options”

Sélectionner comme ceci puis ”ok”

Nous en avons fini pour la partie Administrateur.



Utilisateur

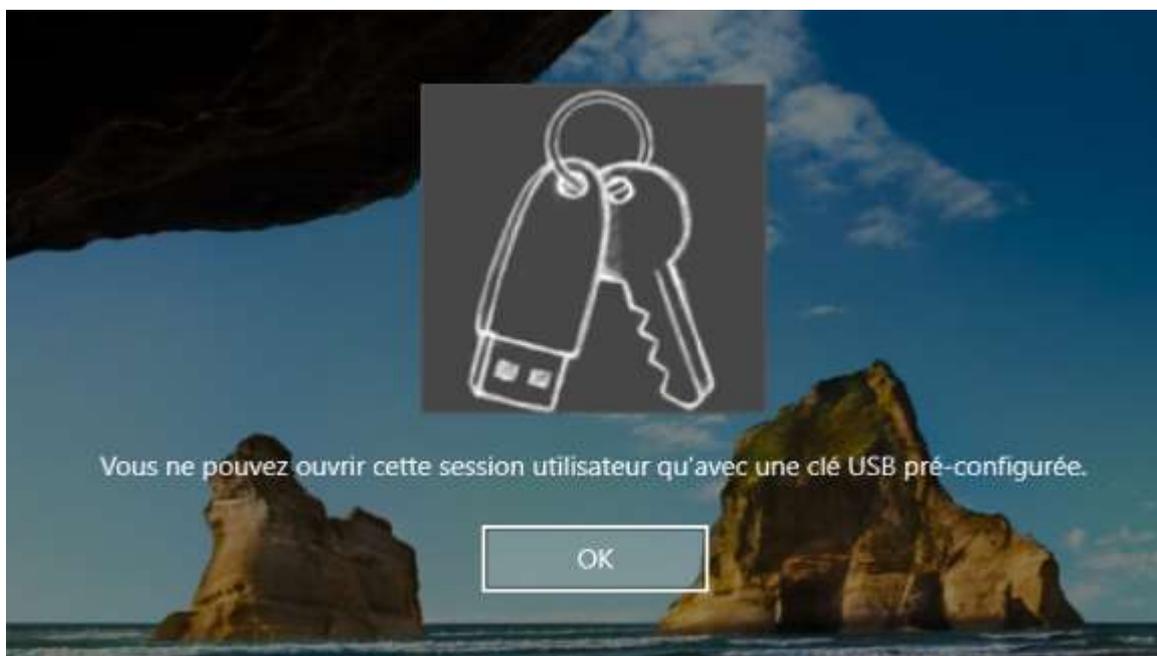
Utilisation des solutions 2FA

Première utilisation

L'utilisateur devra à la première connexion, insérer la clé de sécurité pour pouvoir accéder à la création de son mot de passe (une gpo à été créée pour avoir un mot de passe minimal de 12 caractères et avoir au moins 3 des 4 entre caractères majuscules, minuscule, chiffre, spécial);

A screenshot of a login interface. It features three input fields stacked vertically. The top field is labeled 'User Name' and is empty. The middle field is labeled 'Password' and has a right-pointing arrow icon on its right side. The bottom field is labeled 'OTP' and is empty. The background of the form is a dark, blurred image of a beach and ocean.

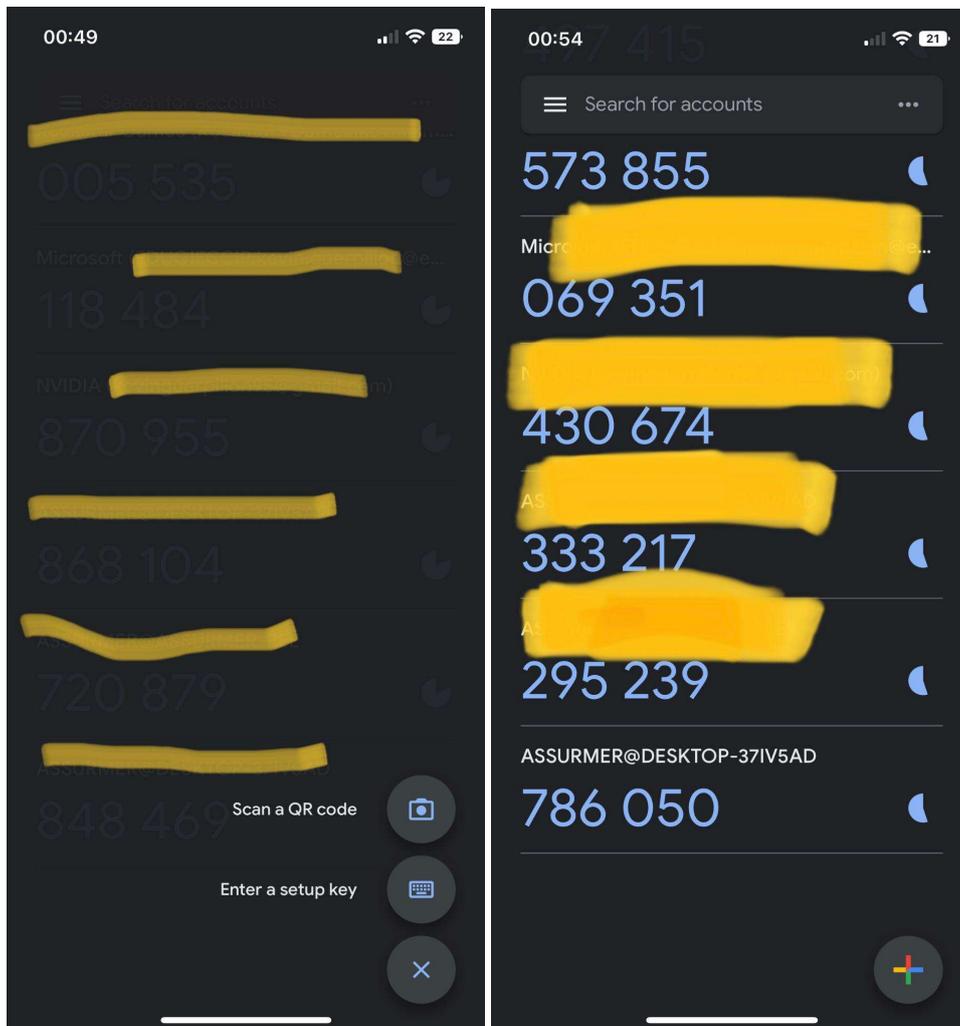
Si la clé de sécurité n'est pas insérée ce message d'erreur s'affichera





Configurer le One-Time Password sur son smartphone

L'utilisateur devra installer une application d'OTP Authenticator de son choix, et scanner le QR code qui est à la racine de la clé de sécurité.





Conclusion

Maintenant que tout est configuré, l'utilisateur à le choix soit il se connecte grâce à

Son nom utilisateur + mot de passe + la clé de sécurité

ou

Son nom utilisateur + mot de passe + OTP

A screenshot of a login interface. It features three input fields stacked vertically. The top field is labeled 'User Name' and is empty. The middle field is labeled 'Password' and contains a right-pointing arrow icon. The bottom field is labeled 'OTP' and is empty. The background of the form is a blurred image of a beach with waves.