yubico

The key to trust

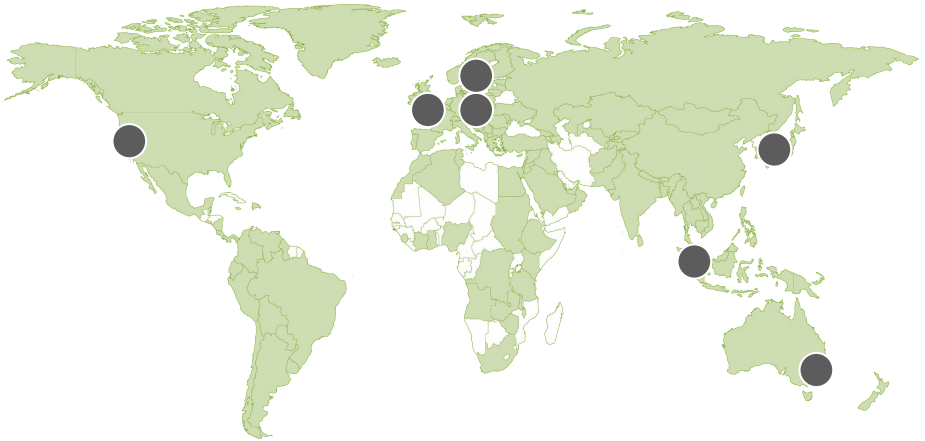
Partenariat CERTA

- **Activité pédagogique :** Équiper les classes/étudiants public ou privés sous contrat proposant le BTS Cybersécurité et Services Informatiques aux Organisations de YUBIKEYS pour réaliser des tests.
  - Réseau CERTA (https://www.reseaucerta.org)
  - Former les futurs administrateurs, RSSI, DSI
- **Population cible :** Étudiants et enseignants de 250 sections de BTS SIO réparties sur l'ensemble du territoire français et des DOM-TOM (lycées publics et privés sous contrat).
- **Session**: 4 sessions Webinaires + démos
- **Type de clés concernées:** YUBIKEYS 5C NFC (USBC) OU 5 NFC (USBA)
- Bénéficier de tarifs spécifiques « Education » via INMAC https://www.inmac-wstore.com/

Introduction

Yubico et la YubiKey

Yubico - acteur majeur de l'authentification forte

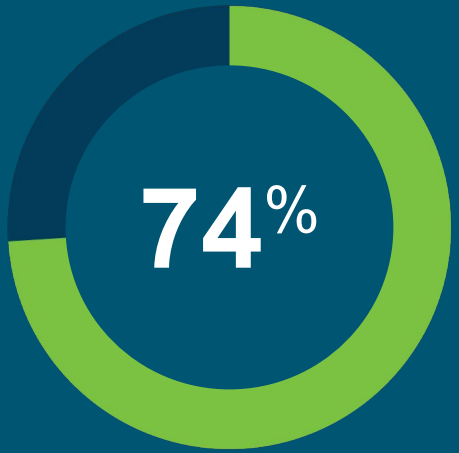


Clients Yubico

Bureaux Yubico

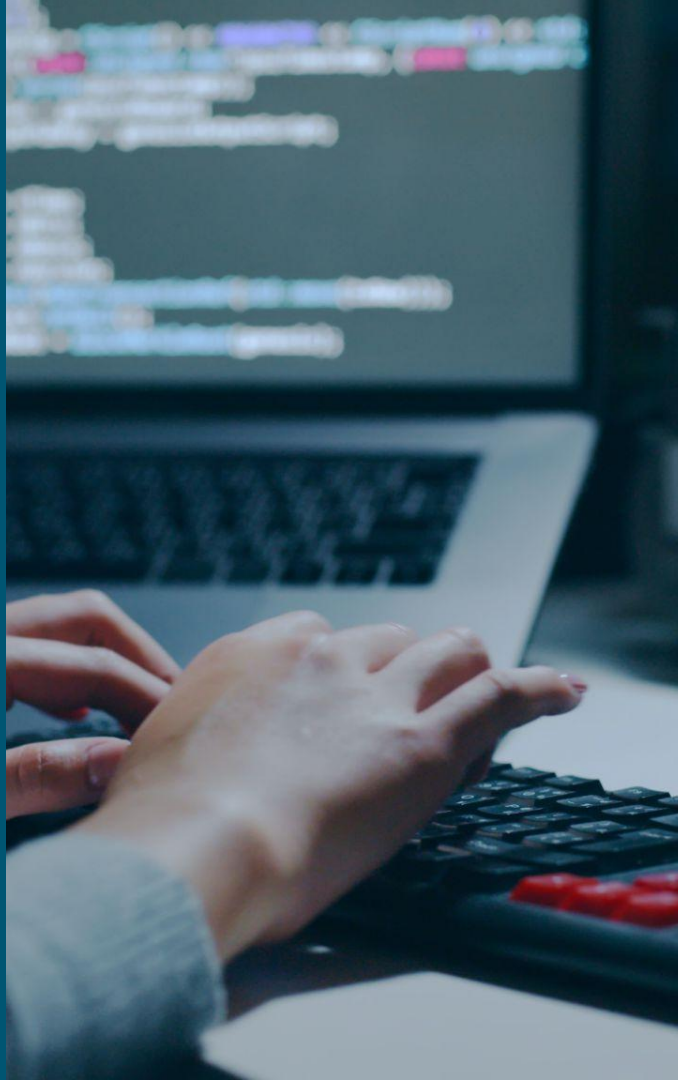
- Fondé en Suède en 2007
- 450 employés dans 10 pays
- 20M+ YubiKeys et + de 5000 entreprises équipées

Les attaquants ne hackent pas, ils entrent avec des mots de passe

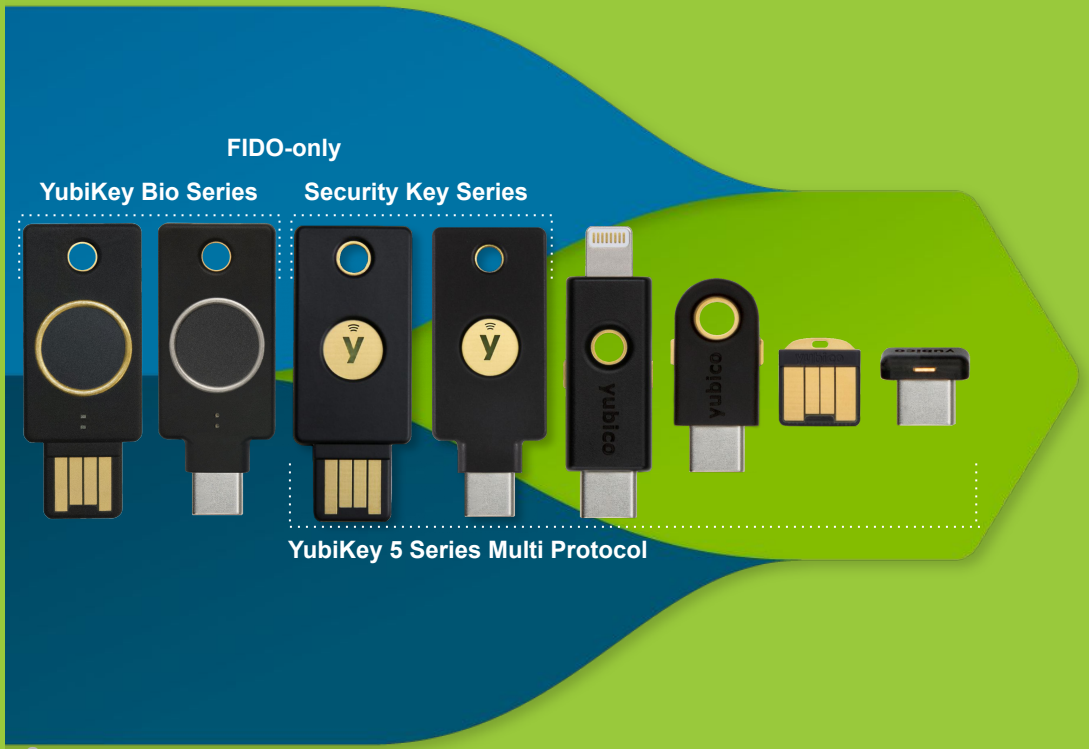


des brèches sont dues à des identifiants volés

Source: Verizon 2023 Data Breach Investigations Report



La YubiKey
Simple, Rapide, Fiable



Notre technologie est la manière la plus simple et conviviale de mettre en œuvre une MFA moderne, en préparant votre cadre de sécurité aux normes de sécurité de demain.

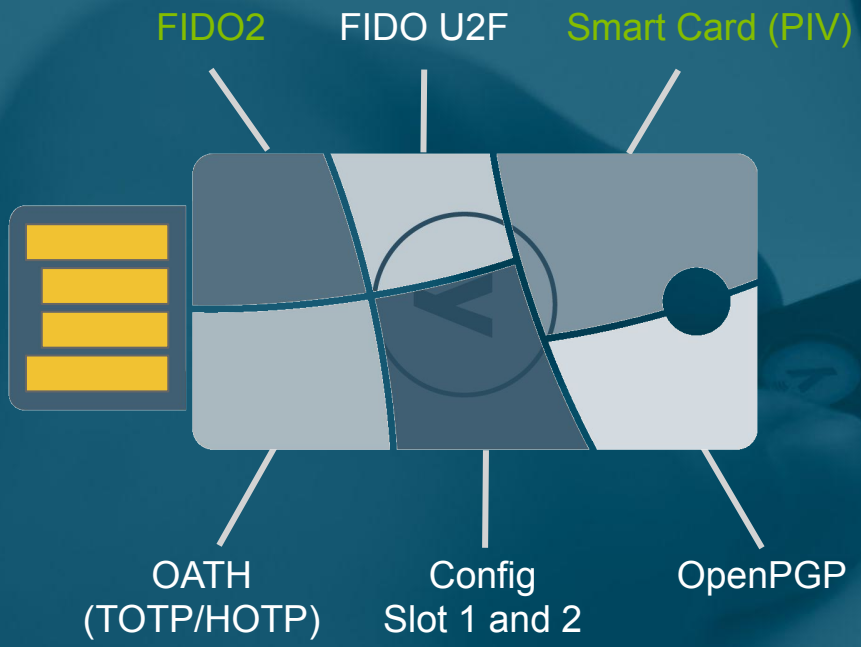
SÉCURITÉ DE PREMIÈRE CLASSE

Conçu pour mettre en œuvre des cadres de sécurité Zero Trust

PRÊT À L'EMPLOI

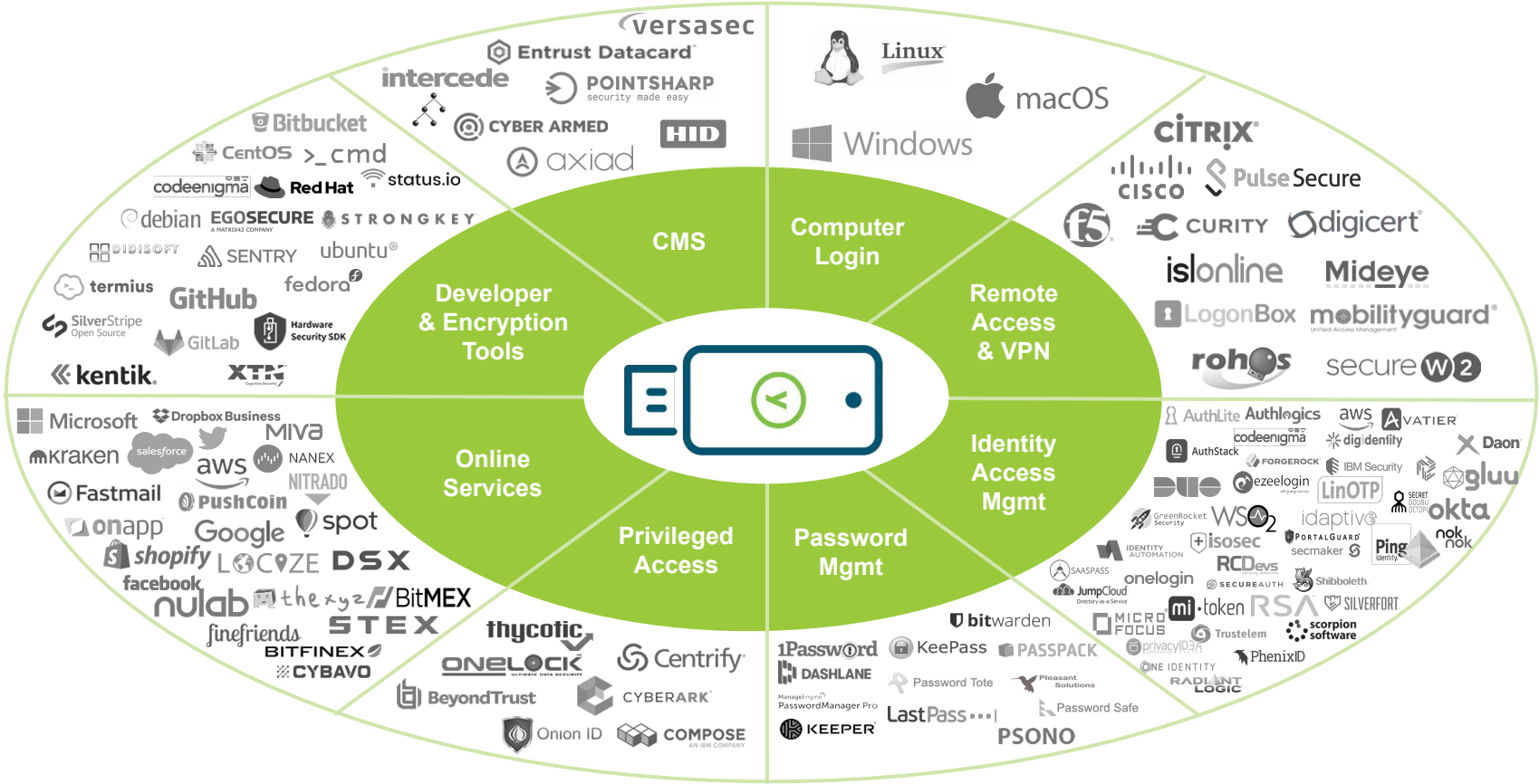
Contribue à maximiser la productivité de votre équipe tout en réduisant vos coûts informatiques

La YubiKey



- Interfaces: USB and NFC
- Slots:
  - YubiOTP
  - Challenge-Response
  - OATH-HOTP
  - Static Password
- Custom Configuration
  - Complexité du code PIN
  - Taille minimale du code PIN
  - Enterprise Attestation
  - Randomisation code PIN/PUK
  - …

Compatible avec plus de 1000 applications



La YubiKey et Microsoft

Comment utiliser la YubiKey avec O365 / Entra ID

Compatibilité YubiKey vs O365C

OATH-TOTP

Yubico Authenticator

CBA

Authentification basée sur un certificat

FIDO2

Authentification sans mdp avec une clé de sécurité

YubiKey & FIDO2

Enregistrement

Association d’un passkey (identifiant FIDO2) à un compte utilisateur.

Le passkey est l’objet qui est enregistré dans la YubiKey.

Opération est faite **une fois** par service / applications / compte.

Avec Microsoft, cela peut être fait par l’utilisateur ou par un administrateur (API Graph)

Authentification

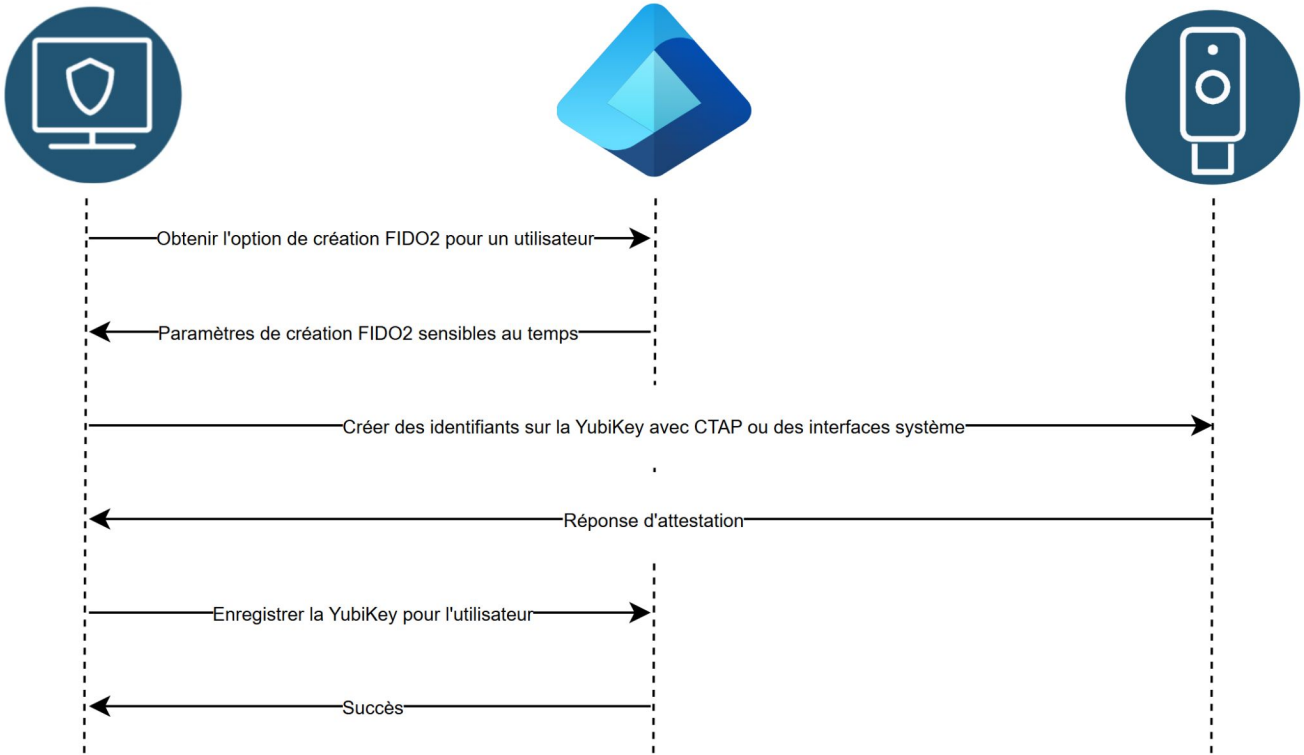
L’utilisateur demande accès à un service ou application.

Avec FIDO2, l’authentification se passe sans login et sans mots de passe.

Opération est faite à chaque fois que l’utilisateur doit s’authentifier

Microsoft FIDO2 Enregistrement “on-behalf”

GET /users/{user-id}/authentication/fido2Methods/creationOptions(challengeTimeoutInMinutes={challengeTimeoutInMinutes})



Enrôlement “on-behalf” - La solution Yubico

YubiEnroll

(Outil Téléchargeable; N'importe quel nombre d'utilisateurs)

Réaffectation des clés possible / programmation faite par vous

Accélérer le processus informatique

À petite échelle

Enrôlement sur site

Outil en ligne de commande

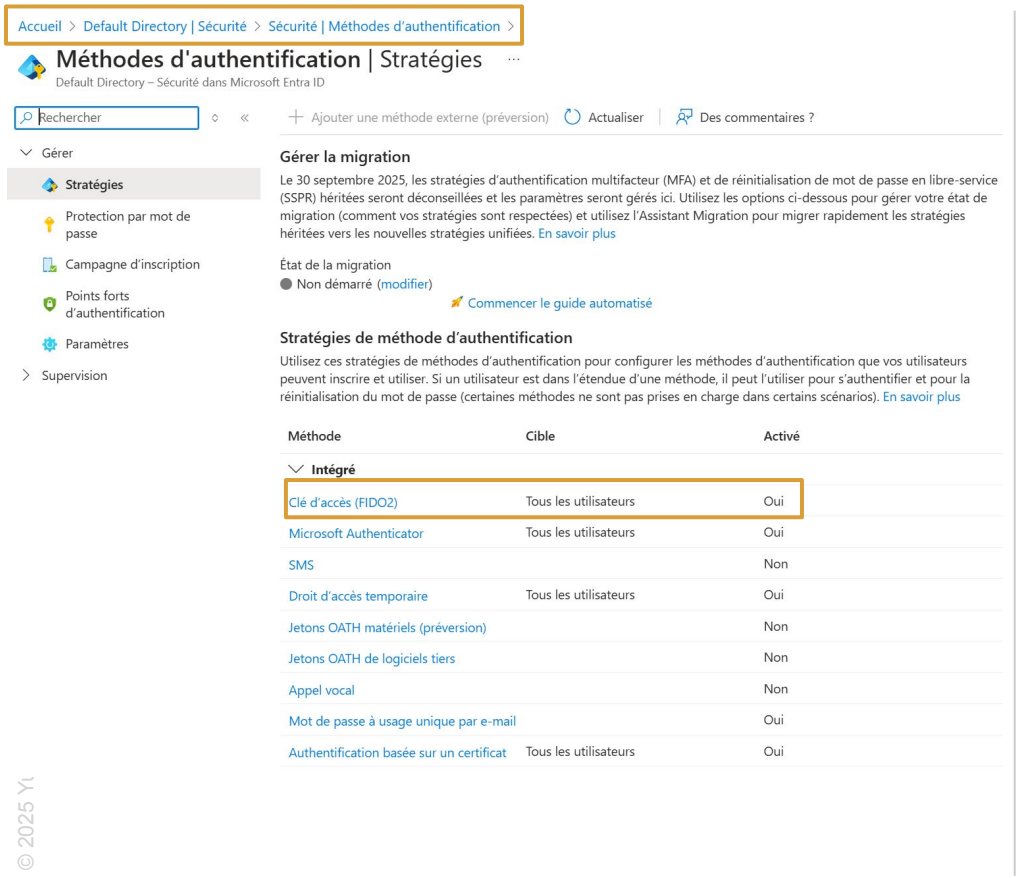
(Accès en avant-première limité)

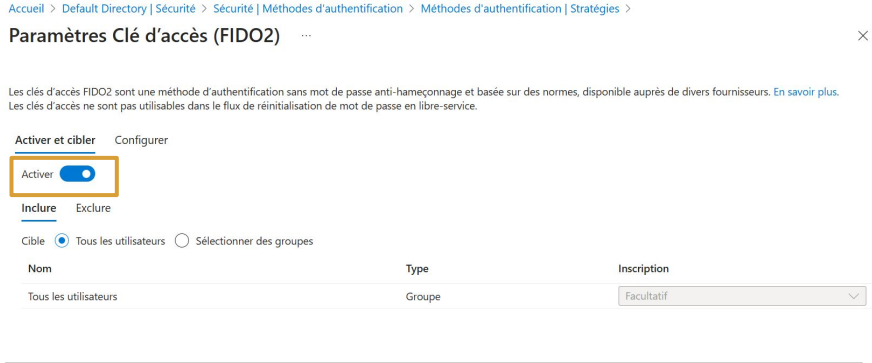
```
PS C:\Users\Renato.Antues> yubienroll
Usage: yubienroll.exe [OPTIONS] COMMAND [ARGS]...

Options:
  -l, --log-level [ERROR|WARNING|INFO|DEBUG|TRAFFIC]
                                  enable logging at given verbosity level
  --log-file FILE
  -v, --version                   show version information about the app
  -h, --help                      show this message and exit

Commands:
  credentials  manage FIDO credentials for users
  login        authenticate to the active provider
  logout       logout from the active provider
  profiles     manage enrollmment profiles
  providers    manage authentication settings for identity providers
  status       show which provider is active, and its authentication status
  users        search for users
PS C:\Users\Renato.Antues>
```

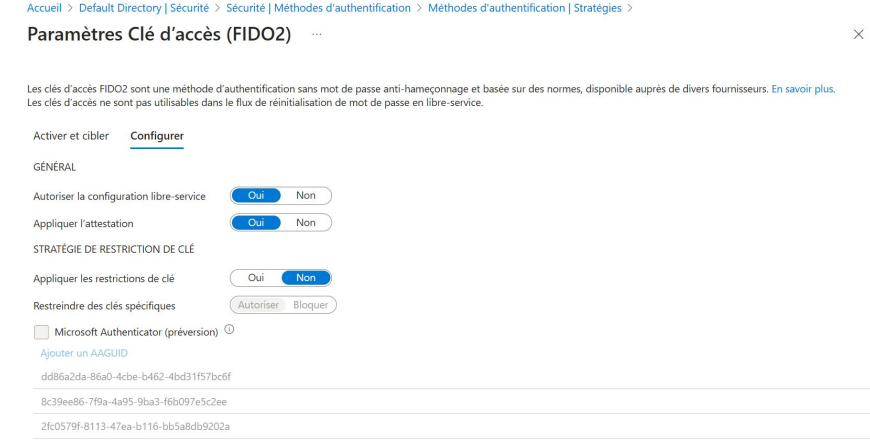
Entra ID - Admin

Pré-requis et configurations du tenant

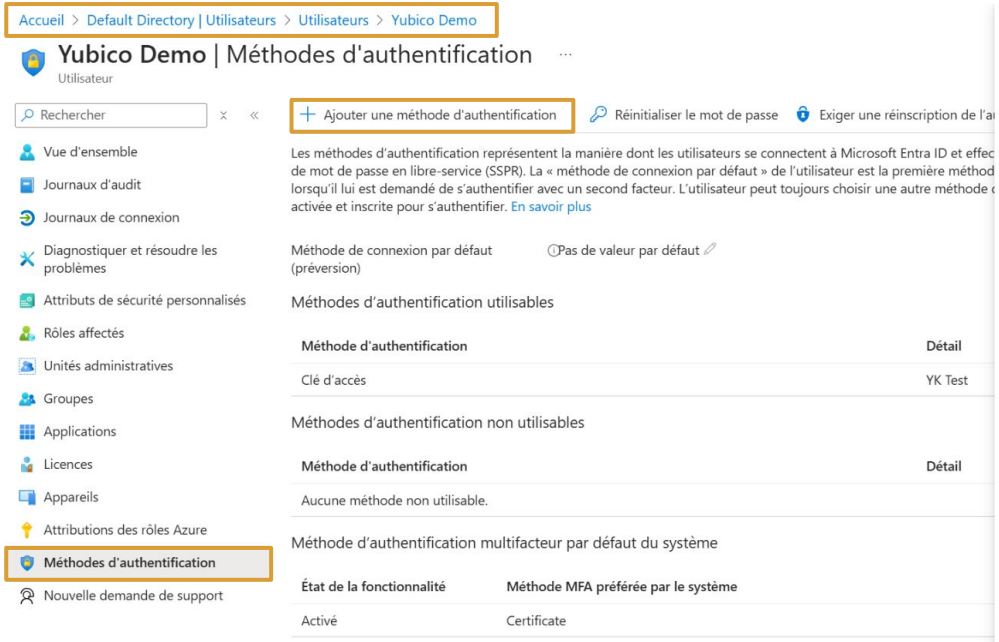
Activation du protocole FIDO2

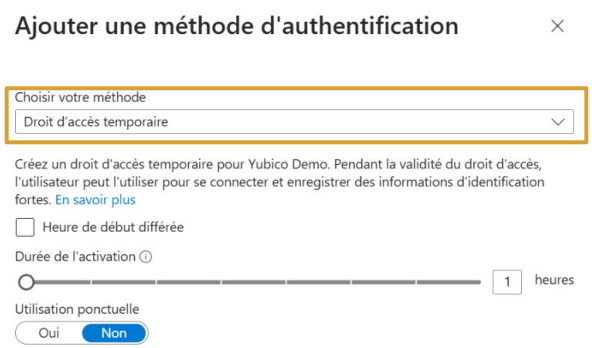


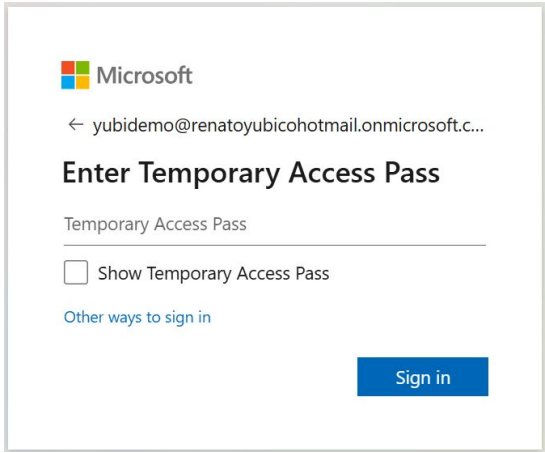




Droit d’Accès Temporaire



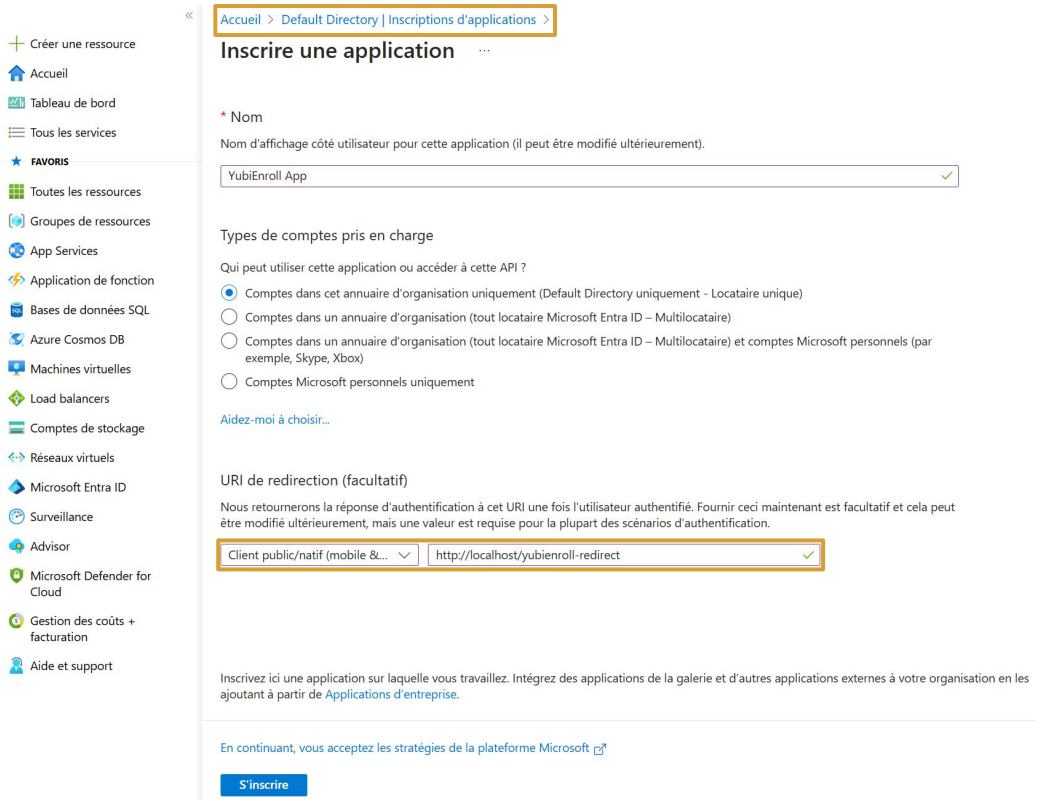




YubiEnroll - Inscription d’application

Création de l’application

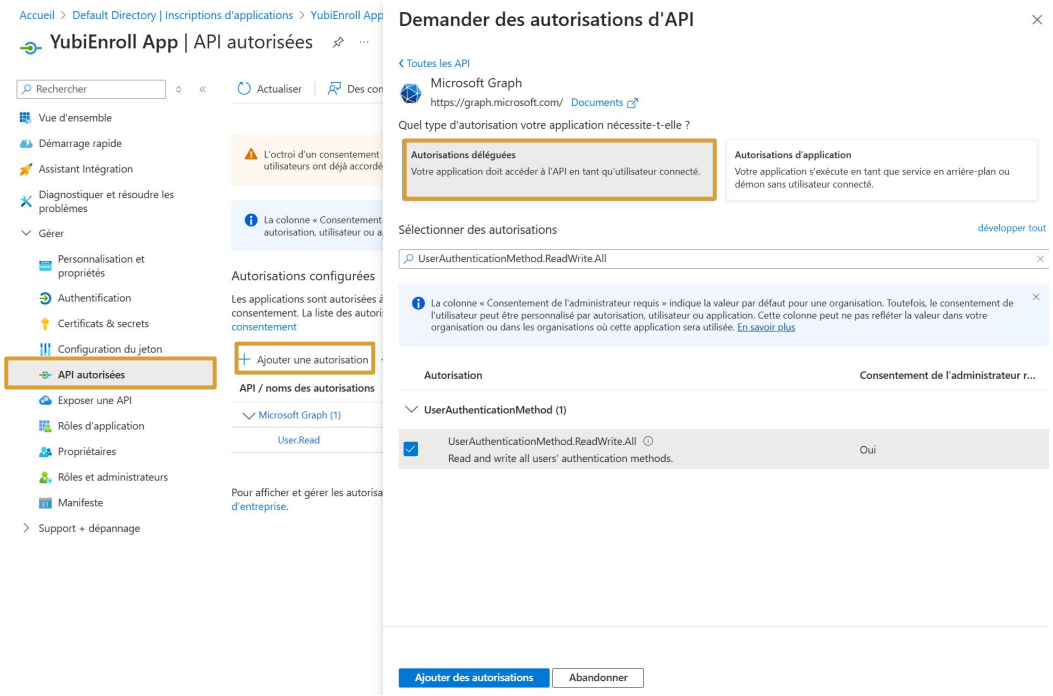
- Rendez-vous sur le lien : https://portal.azure.com
- Allez sur “*Entra ID > Gérer > Inscriptions d'applications*” et cliquez sur l’option “*Nouvelle Inscription*”
- Saisissez le nom de l’application, choisissez l’option “*Client public/natif (mobile et bureau)*” et saisissez l’URI de redirection (cet URI est l'adresse où Entra ID redirige le client - YubiEnroll - et envoie des jetons de sécurité après authentification)
- Cliquez sur “*S’inscrire*”



YubiEnroll - Inscription d’application

Configuration des droits

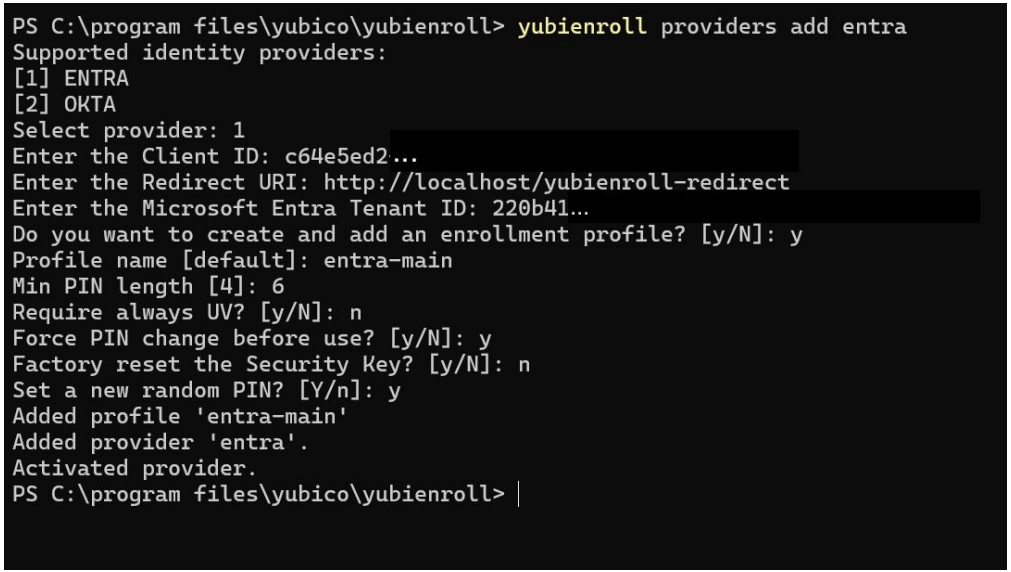
- Rendez-vous sur le lien : https://portal.azure.com
- Une fois que l’application soit inscrite, cliquez sur le lien “*API autorisée*” pour ajouter les droits dont YubiEnroll a besoin
- Cliquez sur l’option “*Ajouter une autorisation*” et choisissez l’option “*Microsoft Graph*”
- Sélectionnez l’option “*Autorisations déléguées*”
- Cherchez et sélectionnez les options “**User.ReadBasic.All**” et “**UserAuthenticationMethod.ReadWrite.All**”
- Cliquez sur “*Ajouter des autorisations*”



YubiEnroll - Connexion à Entra ID

Ajout d'un "provider"

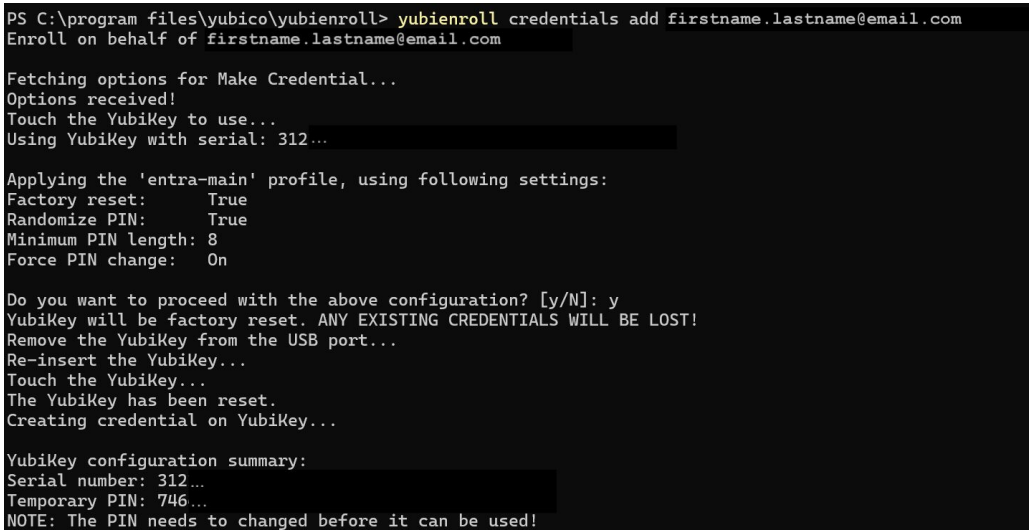
- Rendez-vous sur le lien : https://portal.azure.com
- Allez sur "*Entra ID > Gérer > Inscriptions d'applications*"*autorisée*" et cliquez sur l'application que vous avez créé pour YubiEnroll
- Notez les valeurs de l'**ID d'application (client)** et l'**ID de l'annuaire (locataire)**
- Ouvrez une fenêtre Powershell et allez sur le dossier où l'outil YubiEnroll est installé
- Exécutez la commande "*yubienroll providers add entra*" pour connecter l'outil au tenant Entra ID
- Si vous sélectionnez d'ajouter un profil en ce moment, l'outil vous demandera les options à appliquer sur la YubiKey lors de l'enregistrement des identifiants avec ce tenant Entra ID



YubiEnroll - Enregistrement d’une YubiKey

Associer une YubiKey à un compte

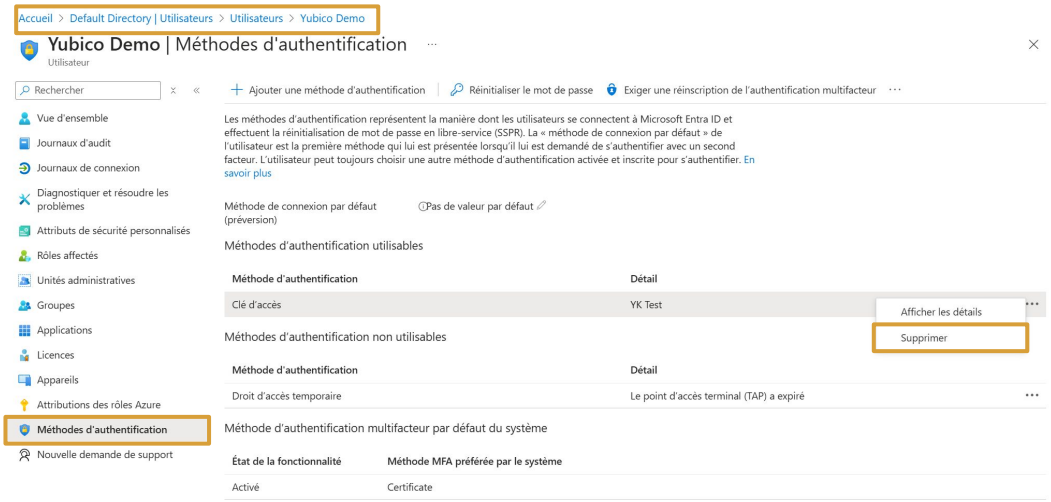
- Ouvrez une fenêtre Powershell et allez sur le dossier où l’outil YubiEnroll est installé
- Exécutez la commande “*yubienroll login*” pour s’authentifier auprès d’Entra ID (sélectionnez l’option ENTRA)
- Exécutez la commande “*yubienroll credentials add <user login>*” pour enregistrer une YubiKey au compte utilisateur



Révocation d’une YubiKey perdue - Admin

Révocation

- Rendez-vous sur le lien : https://portal.azure.com
- Allez sur “*Entra ID > Gérer > Utilisateurs*” et cliquez sur l’utilisateur pour lequel vous voulez supprimer la YubiKey
- Sur le menu à gauche, cliquez sur l’option “Méthodes d’authentification”
- Identifiez la clé perdue sur la liste de méthodes d’authentification et cliquez sur le “...” à la fin de la ligne
- Cliquez sur “*Supprimer*”



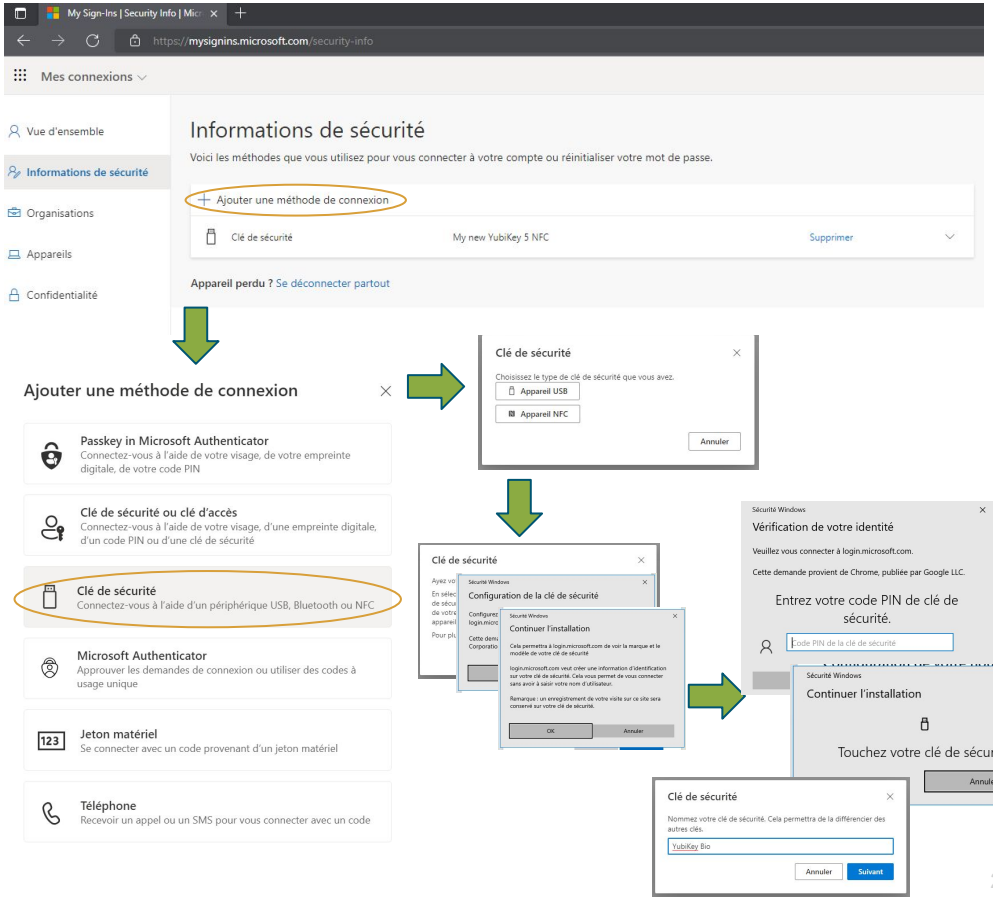
Entra ID - Utilisateur

Comment utiliser la YubiKey

YubiKey - Configuration du compte utilisateur

Enregistrer la YubiKey

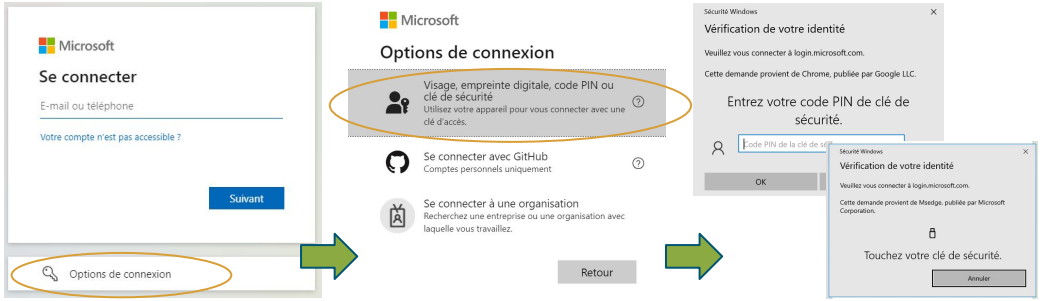
- Rendez-vous sur le lien : https://aka.ms/mfasetup
- Authentifiez vous avec la méthode que vous avez aujourd'hui (vous pouvez demander un passe d'accès temporaire à votre administrateur de système)
- Cliquez sur l'option "*Ajouter une méthode de connexion*"
- Cliquez sur l'option "*Clé de sécurité*"
- Cliquez sur l'option "Appareil USB" et confirmez tous les messages montrés par le navigateur
- Saisissez votre code PIN et touchez votre YubiKey (pour la YubiKey Bio vous n'avez qu'à toucher la clé)
- Nommez votre clé de sécurité et confirmez le dernier message

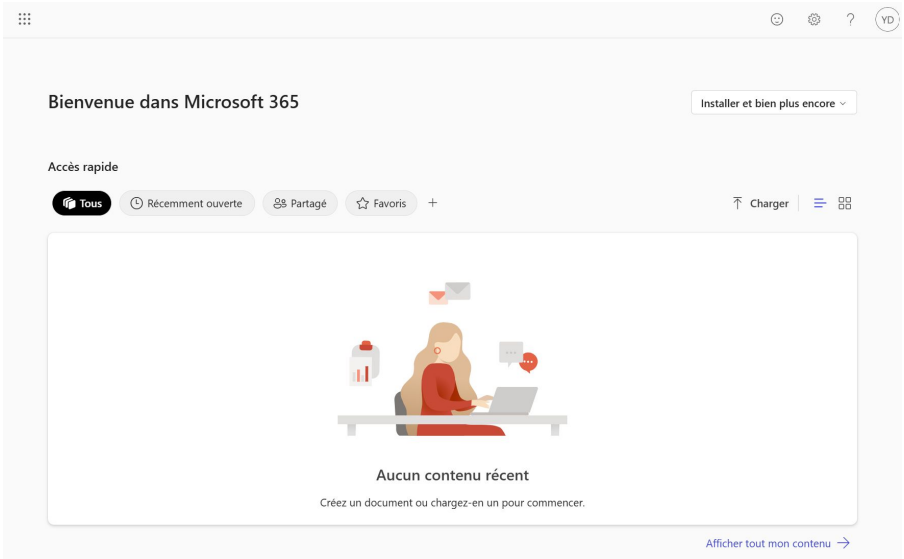


Connexion O365 avec la YubiKey

Authentification

- Rendez-vous sur le lien : https://www.office.com
- Sur la mire de connexion, cliquez sur l'option "*Options de connexion*"
- Choisissez l'option "*Visage, empreinte digitale, code PIN ou **clé de sécurité***"
- Saisissez votre code PIN et touchez votre YubiKey (pour la YubiKey Bio vous n'avez qu'à toucher la clé)
- Choisissez si vous voulez rester connecté ou pas

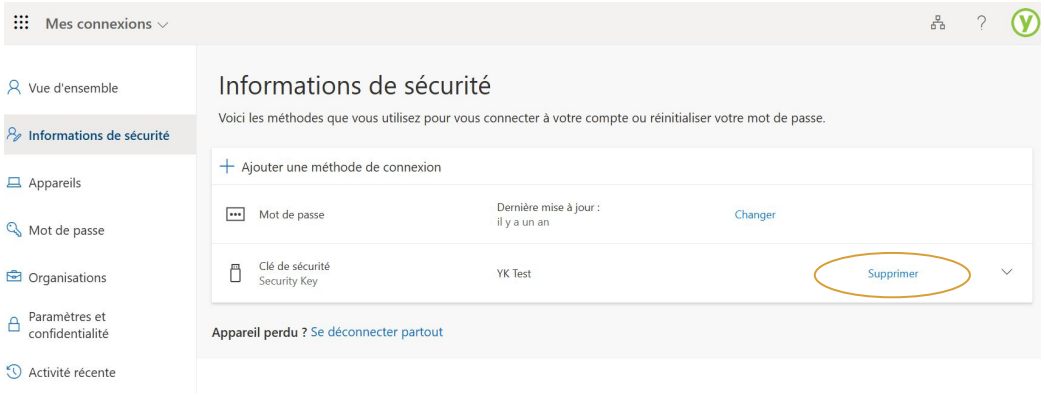




Révocation d’une YubiKey perdue - Utilisateur

Révocation

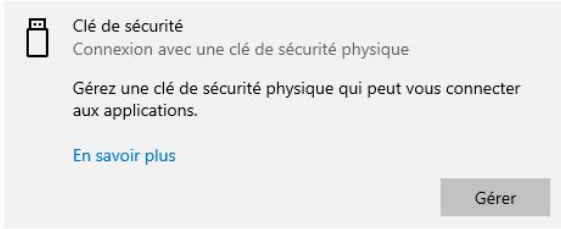
- Rendez-vous sur le lien : https://aka.ms/mfasetup
- Authentifiez vous avec la méthode que vous avez aujourd’hui (vous pouvez demander un passe d’accès temporaire à votre administrateur de système)
- Identifiez la clé perdue sur la liste de méthodes d’authentification
- Cliquez sur le lien “*Supprimer*”



Changement du code PIN

Pas à Pas

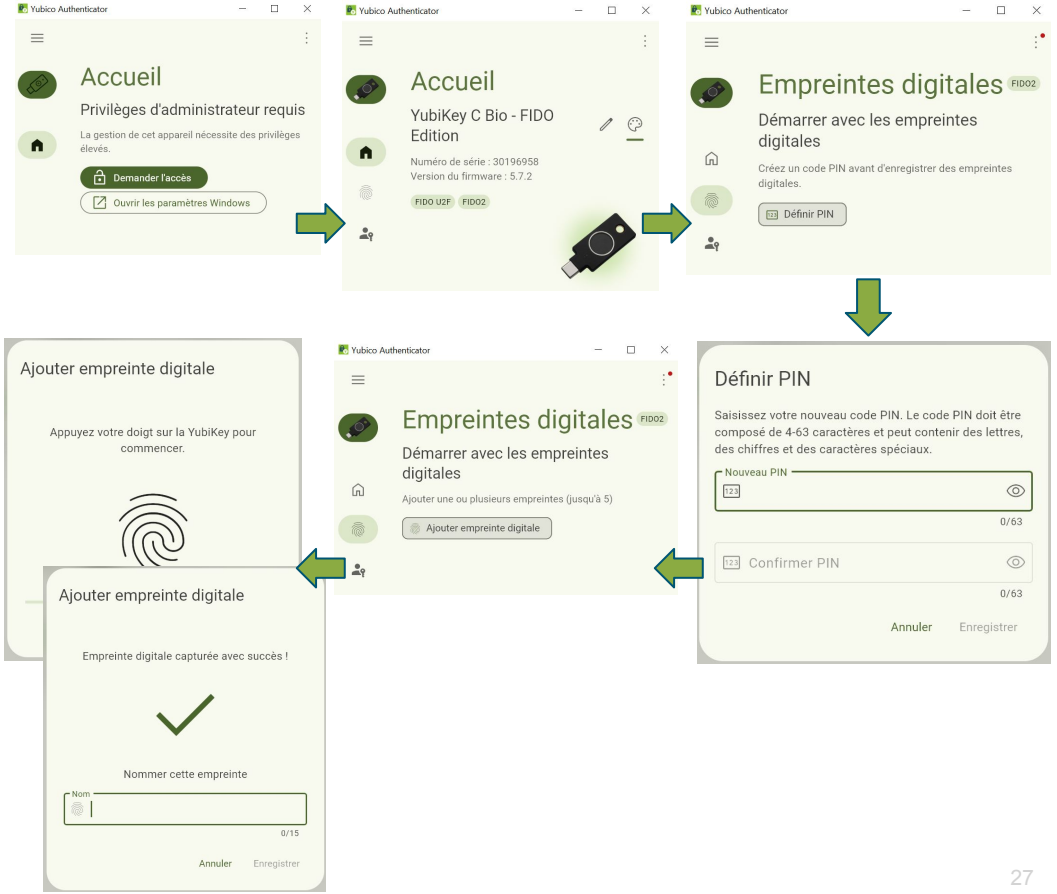
- Insérez la YubiKey dans le port USB
- Démarrer > Paramètres > Options de connexion > Clé de sécurité > Gérer
- Touchez la clé
- Sous l'option "Code PIN de la clé de sécurité", cliquez sur le bouton "Modifier"
- Saisissez le code PIN actuel
- Saisissez le nouveau code PIN (et confirmez-le). Le PIN doit avoir entre 4 et 63 caractères
- La fenêtre de configuration se fermera sans confirmer la modification



Yubico Authenticator

Configuration de la YubiKey

- **Attention** : sur Windows, vous avez besoin d'être administrateur du PC pour pouvoir gérer la YubiKey avec l'application Yubico Authenticator
- Télécharger l'application Yubico Authenticator sur le lien : https://www.yubico.com/products/yubico-authenticator/
- Lancez l'application Yubico Authenticator et cliquez sur le bouton "*Demander l'accès*" (cela va élever le privilège de l'application)
- Cliquez sur le bouton
- Cliquez sur l'option "*Définir PIN*"
- Saisissez le code PIN puis cliquez sur le bouton "Save". Le PIN doit avoir entre 4 et 63 caractères
- Cliquez sur le bouton "*Ajouter empreinte digitale*"
- Appuyez plusieurs fois sur le lecteur d'empreinte sur la YubiKey Bio, donnez un nom à l'empreinte puis cliquez sur "Save"



Démo

Prochaines sessions:

Jeudi 27 Mars 2025 18h00 - 19h00
Ouverture de session Windows en FIDO2 + Démo

Date à définir
Ouverture de session Smart Card + Démo

yubico