

yubico

The key to trust

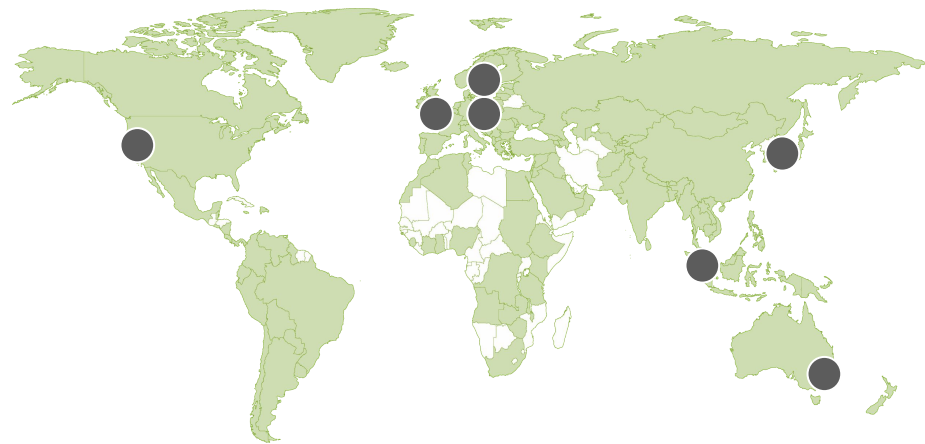
Partenariat CERTA

- **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)
- Bénéficiaire 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

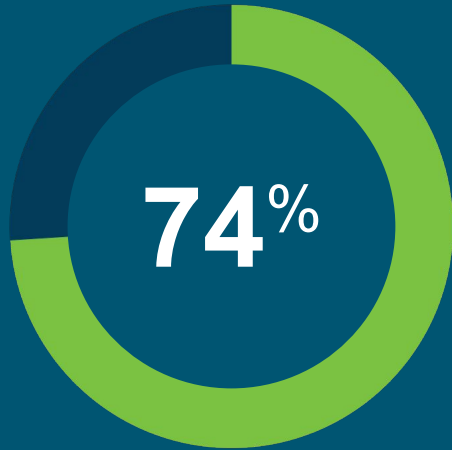


- Fondé en Suède en 2007
- 450 employés dans 10 pays
- 20M+ YubiKeys et + de 5000 entreprises équipées

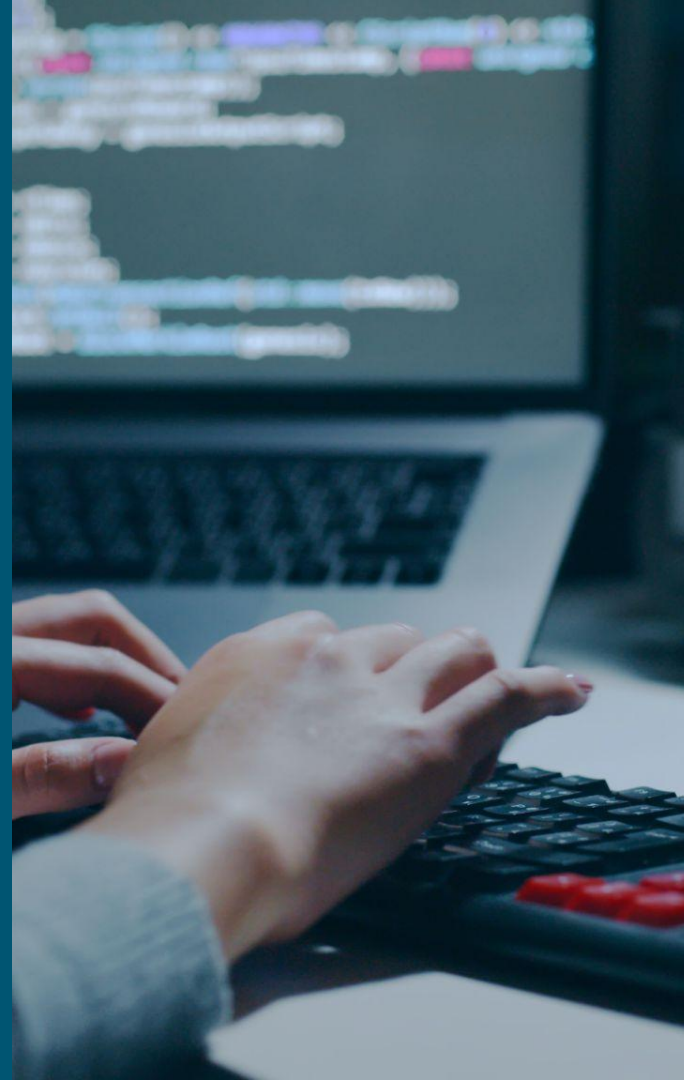


yubico

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



des brèches sont dues à des identifiants volés



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

FIDO-only

YubiKey Bio Series

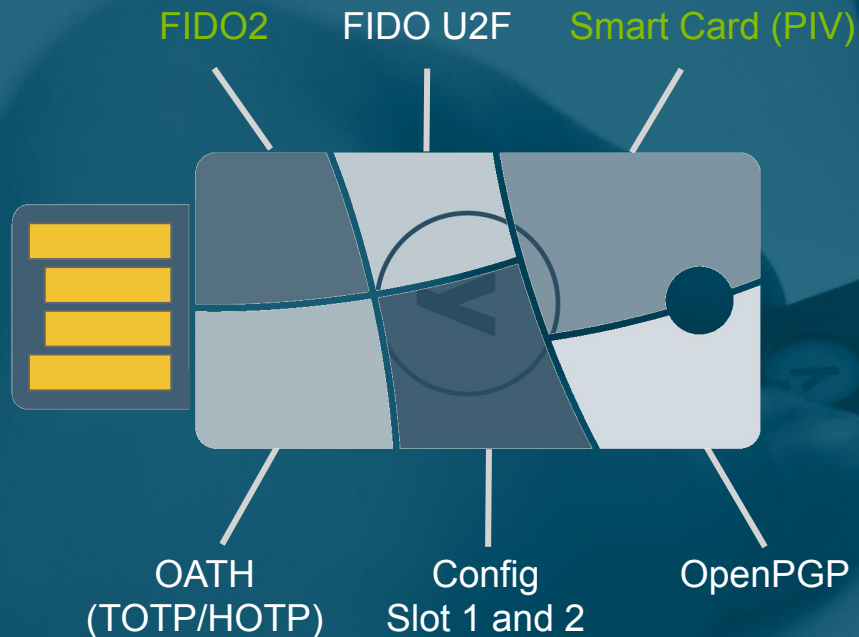
Security Key Series



YubiKey 5 Series Multi Protocol

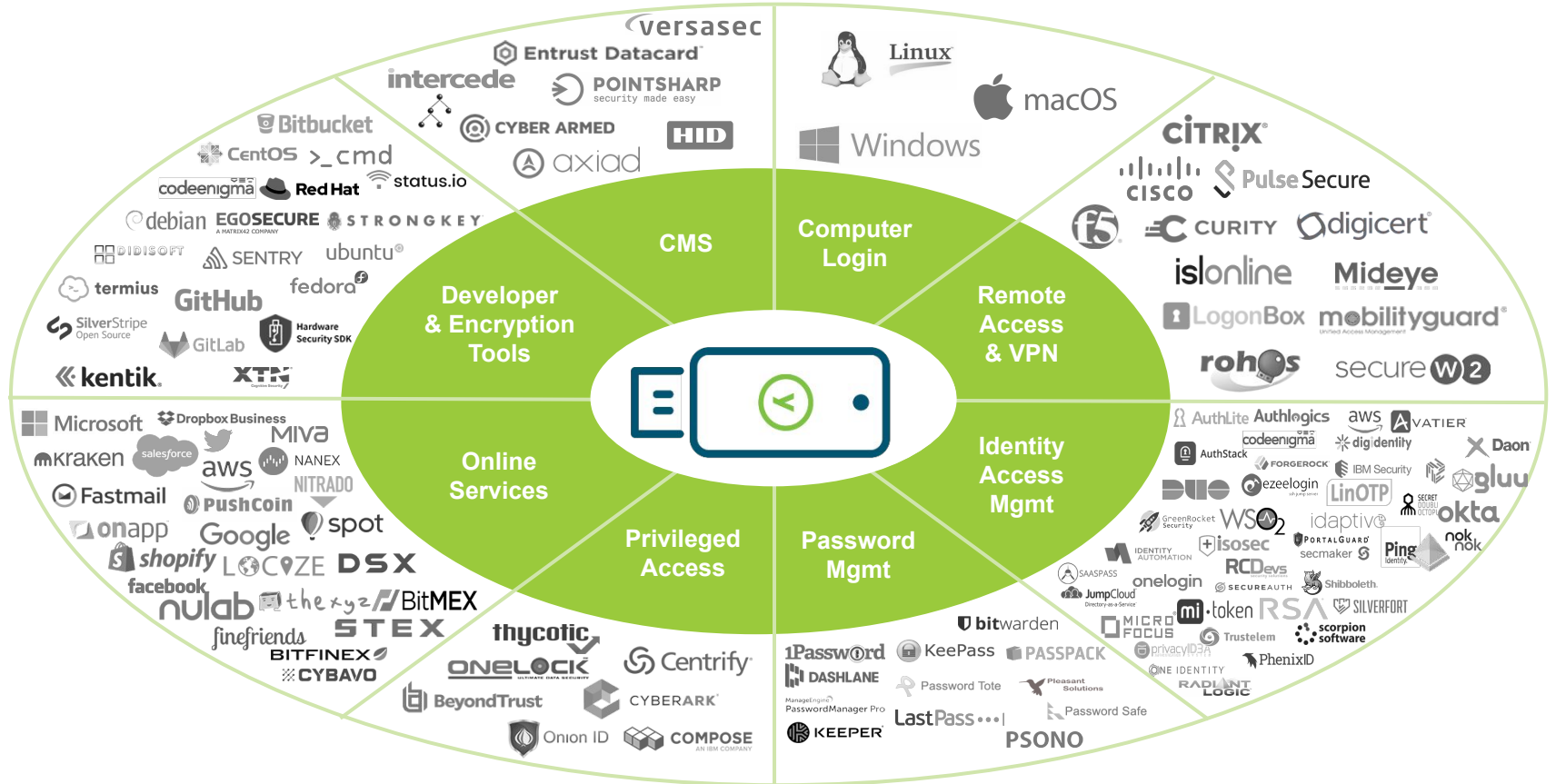


La YubiKey



- 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

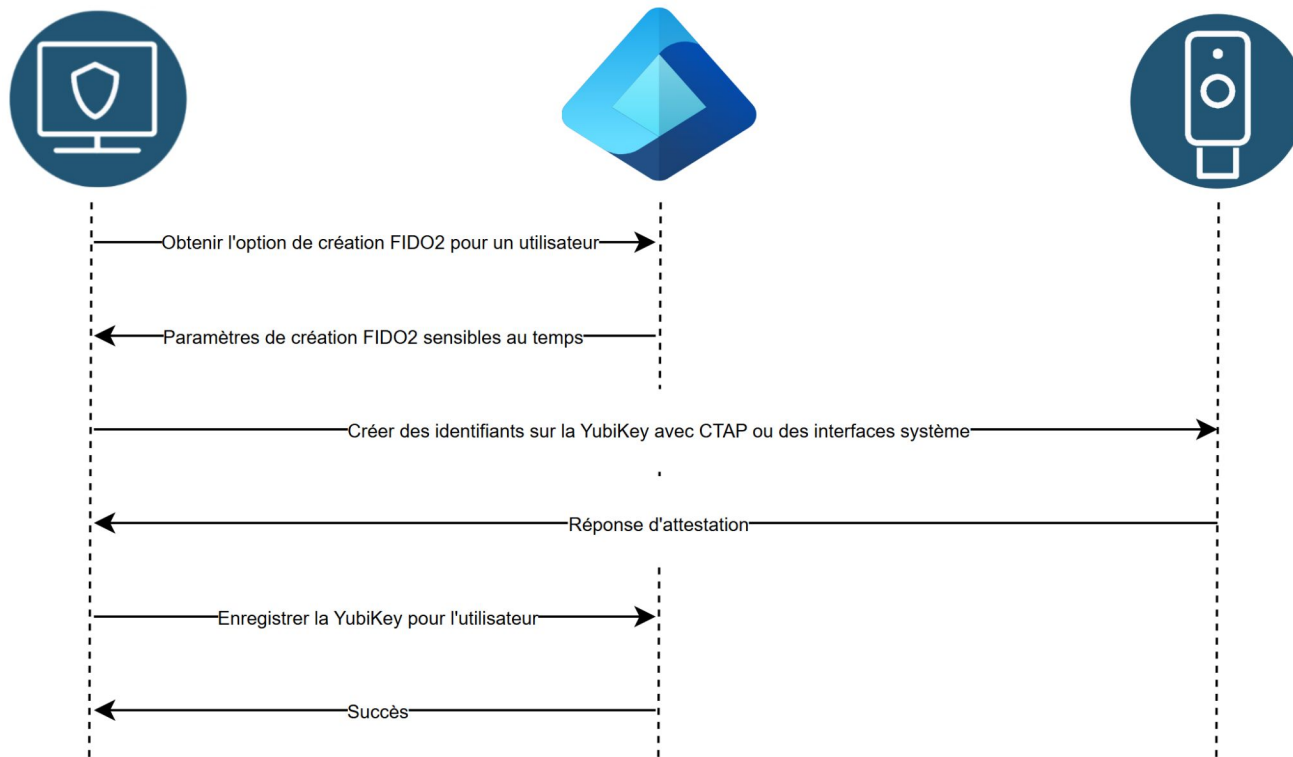
L'utilisateur demande accès à un service ou application.

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 enrollment 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

Accueil > Default Directory | Sécurité > Sécurité | Méthodes d'authentification >

Méthodes d'authentification | Stratégies

Default Directory – Sécurité dans Microsoft Entra ID

Rechercher

Gérer la migration

Le 30 septembre 2025, les stratégies d'authentification multifactor (MFA) et de réinitialisation de mot de passe en libre-service (SSPR) héritées seront déconseillées et les paramètres seront gérés ici. Utilisez les options ci-dessous pour gérer votre état de migration (comment vos stratégies sont respectées) et utilisez l'Assistant Migration pour migrer rapidement les stratégies héritées vers les nouvelles stratégies unifiées. [En savoir plus](#)

État de la migration

Non démarré ([modifier](#))

[Commencer le guide automatisé](#)

Stratégies de méthode d'authentification

Utilisez ces stratégies de méthodes d'authentification pour configurer les méthodes d'authentification que vos utilisateurs peuvent inscrire et utiliser. Si un utilisateur est dans l'étendue d'une méthode, il peut l'utiliser pour s'authentifier et pour la réinitialisation du mot de passe (certaines méthodes ne sont pas prises en charge dans certains scénarios). [En savoir plus](#)

Méthode	Cible	Activé
Intégré		
Clé d'accès (FIDO2)	Tous les utilisateurs	Oui
Microsoft Authenticator	Tous les utilisateurs	Oui
SMS		Non
Droit d'accès temporaire	Tous les utilisateurs	Oui
Jetons OATH matériels (préversion)		Non
Jetons OATH de logiciels tiers		Non
Appel vocal		Non
Mot de passe à usage unique par e-mail		Oui
Authentification basée sur un certificat	Tous les utilisateurs	Oui

Accueil > Default Directory | Sécurité > Sécurité | Méthodes d'authentification > Méthodes d'authentification | Stratégies >

Paramètres Clé d'accès (FIDO2)

Les clés d'accès FIDO2 sont une méthode d'authentification sans mot de passe anti-hameçonnage et basée sur des normes, disponible auprès de divers fournisseurs. [En savoir plus](#). Les clés d'accès ne sont pas utilisables dans le flux de réinitialisation de mot de passe en libre-service.

Activer et cibler Configurer

Activer

Inclure Exclure

Cible Tous les utilisateurs Sélectionner des groupes

Nom	Type	Inscription
Tous les utilisateurs	Groupe	Facultatif

Accueil > Default Directory | Sécurité > Sécurité | Méthodes d'authentification > Méthodes d'authentification | Stratégies >

Paramètres Clé d'accès (FIDO2)

Les clés d'accès FIDO2 sont une méthode d'authentification sans mot de passe anti-hameçonnage et basée sur des normes, disponible auprès de divers fournisseurs. [En savoir plus](#). Les clés d'accès ne sont pas utilisables dans le flux de réinitialisation de mot de passe en libre-service.

Activer et cibler Configurer

GÉNÉRAL

Autoriser la configuration libre-service Oui Non

Appliquer l'attestation Oui Non

STRATÉGIE DE RESTRICTION DE CLÉ

Appliquer les restrictions de clé Oui Non

Restreindre des clés spécifiques Autoriser Bloquer

Microsoft Authenticator (préversion) ⓘ

Ajouter un AAGUID

dd86a2da-86a0-4cbe-b462-4bd31f7bc6f

8c39ee86-7f9a-4a95-9ba3-f6b097e5c2ee

2fc0579f-8113-47ea-b116-bb5a8db9202a

Droit d'Accès Temporaire

Accueil > Default Directory | Utilisateurs > Utilisateurs > Yubico Demo

Yubico Demo | Méthodes d'authentification

Rechercher

+ Ajouter une méthode d'authentification

Réinitialiser le mot de passe Exiger une réinscription de l'a

- Vue d'ensemble
- Journaux d'audit
- Journaux de connexion
- Diagnostiquer et résoudre les problèmes
- Attributs de sécurité personnalisés
- Rôles affectés
- Unités administratives
- Groupes
- Applications
- Licences
- Appareils
- Attributions des rôles Azure
- Méthodes d'authentification**
- Nouvelle demande de support

Les méthodes d'authentification représentent la manière dont les utilisateurs se connectent à Microsoft Entra ID et effectuent le mot de passe en libre-service (SSPR). La « méthode de connexion par défaut » de l'utilisateur est la première méthode lorsqu'il lui est demandé de s'authentifier avec un second facteur. L'utilisateur peut toujours choisir une autre méthode de connexion activée et inscrite pour s'authentifier. [En savoir plus](#)

Méthode de connexion par défaut (préversion) Pas de valeur par défaut

Méthodes d'authentification utilisables

Méthode d'authentification	Détail
Clé d'accès	YK Test

Méthodes d'authentification non utilisables

Méthode d'authentification	Détail
Aucune méthode non utilisable.	

Méthode d'authentification multifacteur par défaut du système

État de la fonctionnalité	Méthode MFA préférée par le système
Activé	Certificat

Ajouter une méthode d'authentification

Choisir votre méthode

Droit d'accès temporaire

Créez un droit d'accès temporaire pour Yubico Demo. Pendant la validité du droit d'accès, l'utilisateur peut l'utiliser pour se connecter et enregistrer des informations d'identification fortes. [En savoir plus](#)

Heure de début différée

Durée de l'activation

1 heures

Utilisation ponctuelle

Oui Non



< yubidemo@renatoyubicohotmail.onmicrosoft.c...

Enter Temporary Access Pass

Temporary Access Pass

Show Temporary Access Pass

[Other ways to sign in](#)

Sign in

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”

« Accueil > Default Directory | Inscriptions d'applications >

Inscrire une application

* Nom
Nom d'affichage côté utilisateur pour cette application (il peut être modifié ultérieurement).

YubiEnroll App ✓

Types de comptes pris en charge

Qui peut utiliser cette application ou accéder à cette API ?

- Comptes dans cet annuaire d'organisation uniquement (Default Directory uniquement - Locataire unique)
- Comptes dans un annuaire d'organisation (tout locataire Microsoft Entra ID – Multilocataire)
- Comptes dans un annuaire d'organisation (tout locataire Microsoft Entra ID – Multilocataire) et comptes Microsoft personnels (par exemple, Skype, Xbox)
- Comptes Microsoft personnels uniquement

Aidez-moi à choisir...

URI de redirection (facultatif)

Nous retournerons la réponse d'authentification à cet URI une fois l'utilisateur authentifié. Fournir ceci maintenant est facultatif et cela peut être modifié ultérieurement, mais une valeur est requise pour la plupart des scénarios d'authentification.

Client public/natif (mobile &... http://localhost/yubiroll-redirect ✓

Inscrivez ici une application sur laquelle vous travaillez. Intégrez des applications de la galerie et d'autres applications externes à votre organisation en les ajoutant à partir de Applications d'entreprise.

En continuant, vous acceptez les stratégies de la plateforme Microsoft ☑

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"
- 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"

Accueil > Default Directory | Inscriptions d'applications > YubiEnroll App

YubiEnroll App | API autorisées

Rechercher Actualiser Des con

- Vue d'ensemble
- Démarrage rapide
- Assistant Intégration
- Diagnostiquer et résoudre les problèmes
- Gérer
 - Personnalisation et propriétés
 - Authentification
 - Certificats & secrets
 - Configuration du jeton
 - API autorisées**
 - Exposer une API
 - Rôles d'application
 - Propriétaires
 - Rôles et administrateurs
 - Manifeste

L'octroi d'un consentement utilisateurs ont déjà accordé

La colonne « Consentement autorisation, utilisateur ou application »

Autorisations configurées

Les applications sont autorisées à consentement. La liste des autorisations

+ Ajouter une autorisation

API / noms des autorisations

API / noms des autorisations
Microsoft Graph (1)
User.Read

Pour afficher et gérer les autorisations d'entreprise.

> Support + dépannage

Demander des autorisations d'API

Toutes les API

Microsoft Graph
<https://graph.microsoft.com/ Documents>

Quel type d'autorisation votre application nécessite-t-elle ?

Autorisations déléguées
Votre application doit accéder à l'API en tant qu'utilisateur connecté.

Autorisations d'application
Votre application s'exécute en tant que service en arrière-plan ou démon sans utilisateur connecté.

Sélectionner des autorisations [développer tout](#)

UserAuthenticationMethod.ReadWrite.All

La colonne « Consentement de l'administrateur requis » indique la valeur par défaut pour une organisation. Toutefois, le consentement de l'utilisateur peut être personnalisé par autorisation, utilisateur ou application. Cette colonne peut ne pas refléter la valeur dans votre organisation ou dans les organisations où cette application sera utilisée. [En savoir plus](#)

Autorisation	Consentement de l'administrateur r...
UserAuthenticationMethod (1)	
<input checked="" type="checkbox"/> UserAuthenticationMethod.ReadWrite.All Read and write all users' authentication methods.	Oui

Ajouter des autorisations Abandonner

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

```
PS C:\program files\yubico\yubienroll> yubienroll providers add entra
Supported identity providers:
[1] ENTRA
[2] OKTA
Select provider: 1
Enter the Client ID: c64e5ed2...
Enter the Redirect URI: http://localhost/yubienroll-redirect
Enter the Microsoft Entra Tenant ID: 220b41...
Do you want to create and add an enrollment profile? [y/N]: y
Profile name [default]: entra-main
Min PIN length [4]: 6
Require always UV? [y/N]: n
Force PIN change before use? [y/N]: y
Factory reset the Security Key? [y/N]: n
Set a new random PIN? [Y/n]: y
Added profile 'entra-main'
Added provider 'entra'.
Activated provider.
PS C:\program files\yubico\yubienroll> |
```

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

```
PS C:\program files\yubico\yubienroll> yubienroll credentials add firstname.lastname@email.com
Enroll on behalf of firstname.lastname@email.com

Fetching options for Make Credential...
Options received!
Touch the YubiKey to use...
Using YubiKey with serial: 312...

Applying the 'entra-main' profile, using following settings:
Factory reset:      True
Randomize PIN:     True
Minimum PIN length: 8
Force PIN change:  On

Do you want to proceed with the above configuration? [y/N]: y
YubiKey will be factory reset. ANY EXISTING CREDENTIALS WILL BE LOST!
Remove the YubiKey from the USB port...
Re-insert the YubiKey...
Touch the YubiKey...
The YubiKey has been reset.
Creating credential on YubiKey...

YubiKey configuration summary:
Serial number: 312...
Temporary PIN: 746...
NOTE: The PIN needs to be changed before it can be used!
```

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”

Accueil > Default Directory | Utilisateurs > Utilisateurs > Yubico Demo

Yubico Demo | Méthodes d'authentification

Utilisateur

Rechercher

+ Ajouter une méthode d'authentification | Réinitialiser le mot de passe | Exiger une réinscription de l'authentification multifacteur

Les méthodes d'authentification représentent la manière dont les utilisateurs se connectent à Microsoft Entra ID et effectuent la réinitialisation de mot de passe en libre-service (SSPR). La « méthode de connexion par défaut » de l'utilisateur est la première méthode qui lui est présentée lorsqu'il lui est demandé de s'authentifier avec un second facteur. L'utilisateur peut toujours choisir une autre méthode d'authentification activée et inscrite pour s'authentifier. En savoir plus

Méthode de connexion par défaut Pas de valeur par défaut

Méthodes d'authentification utilisables

Méthode d'authentification	Détail	
Clé d'accès	YK Test	Afficher les détails

Méthodes d'authentification non utilisables

Méthode d'authentification	Détail	
Droit d'accès temporaire	Le point d'accès terminal (TAP) a expiré	

Méthode d'authentification multifacteur par défaut du système

État de la fonctionnalité	Méthode MFA préférée par le système
Activé	Certificate

Nouvelle demande de support

Entra ID - Utilisateur

Comment utiliser la YubiKey

YubiKey - Configuration du compte utilisateur

Enregistrer la YubiKey

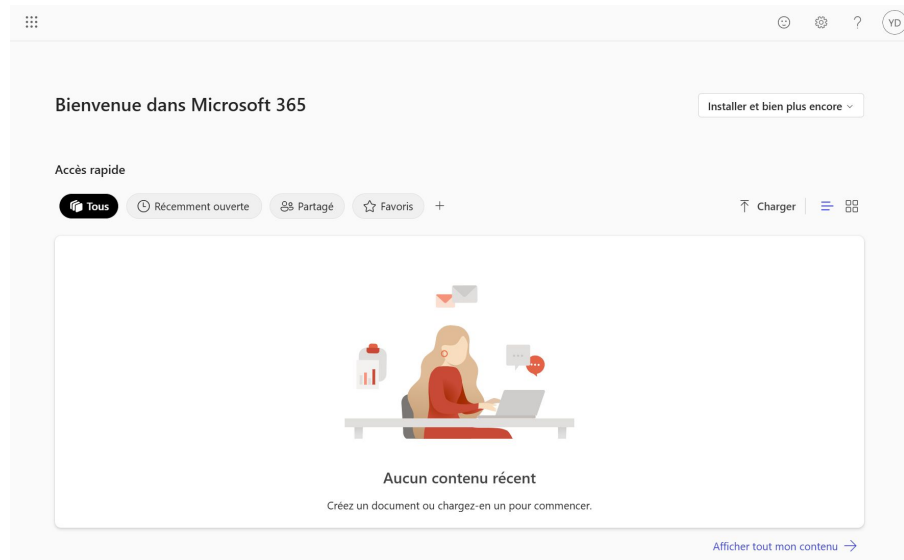
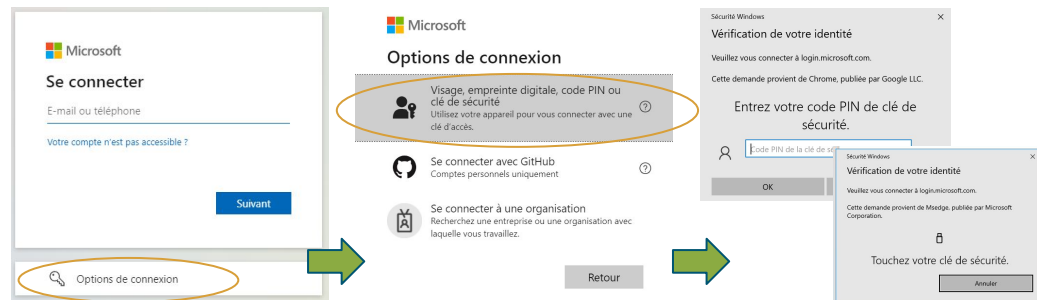
- Rendez-vous sur le lien : <https://aka.ms/mfasetup>
- Authentifiez vous avec la méthode que vous avez aujourd'hui (vous pouvez demander un passe d'accès temporaire à votre administrateur de système)
- Cliquez sur l'option "Ajouter une méthode de connexion"
- Cliquez sur l'option "Clé de sécurité"
- 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

The image shows a sequence of screenshots illustrating the configuration of a YubiKey on a Microsoft account. The main browser window is titled "My Sign-Ins | Security Info | Microsoft" and shows the "Informations de sécurité" page. A red circle highlights the "+ Ajouter une méthode de connexion" button. Below this, a list of connection methods is shown, with "Clé de sécurité" selected and circled in red. To the right, a "Clé de sécurité" dialog box prompts the user to choose between "Appareil USB" and "Appareil NFC". Below that, a "Sécurité Windows" dialog box asks for the PIN of the security key. Further down, another "Clé de sécurité" dialog box prompts the user to name the key, with "YubiKey Bio" entered in the text field. The final dialog box shows the "Suivant" (Next) button highlighted.

Connexion O365 avec la YubiKey

Authentification

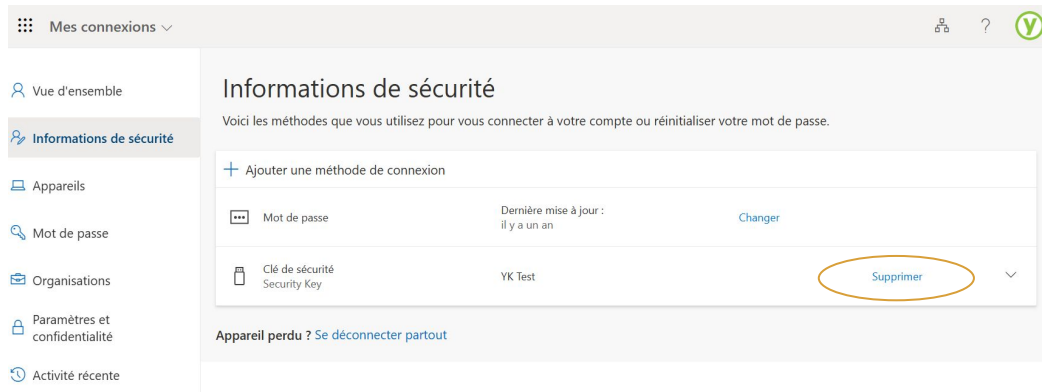
- Rendez-vous sur le lien : <https://www.office.com>
- Sur la mire de connexion, cliquez sur l'option "Options de connexion"
- Choisissez l'option "Visage, empreinte digitale, code PIN ou clé de sécurité"
- Saisissez votre code PIN et touchez votre YubiKey (pour la YubiKey Bio vous n'avez qu'à toucher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



The screenshot shows the 'Mes connexions' (My connections) page in a Microsoft account interface. The left sidebar contains navigation options: 'Vue d'ensemble', 'Informations de sécurité' (selected), 'Appareils', 'Mot de passe', 'Organisations', 'Paramètres et confidentialité', and 'Activité récente'. The main content area is titled 'Informations de sécurité' and includes the text 'Voici les méthodes que vous utilisez pour vous connecter à votre compte ou réinitialiser votre mot de passe.' Below this, there is a section '+ Ajouter une méthode de connexion' containing a table of security methods:

Méthode	Dernière mise à jour :	Action
Mot de passe	il y a un an	Changer
Clé de sécurité Security Key	YK Test	Supprimer

The 'Supprimer' button for the Security Key is circled in orange. Below the table, there is a link: 'Appareil perdu ? Se déconnecter partout'.

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



Clé de sécurité

Connexion avec une clé de sécurité physique

Gérez une clé de sécurité physique qui peut vous connecter aux applications.

[En savoir plus](#)

Gérer



Code PIN de la clé de sécurité

La création d'un code PIN pour votre clé de sécurité contribue à votre protection


Modifier

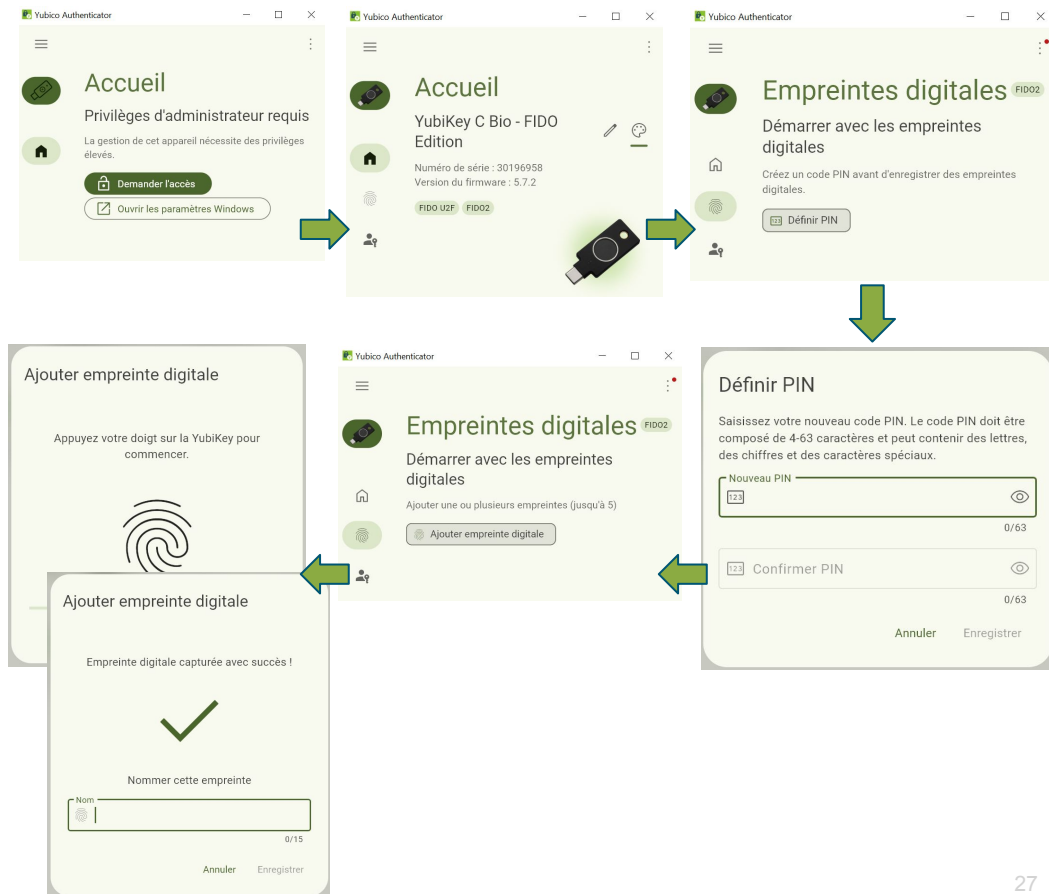
Modifier le code PIN de votre clé de sécurité



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