THALES

SafeNet eToken FIDO

GUIDE DE DEMARRAGE ET D'UTILISATION

Informations sur les documents

Nom du produit/Version	SafeNet eToken FIDO/Version 1
Date de sortie	21 mars 2025

Historique de la révision

Révision	Date	Raison
Rév. A	21 mars 2025	Première publication

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

TABLE DES MATIÈRES

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

CHAPITRE 1: Vue d'ensemble

Qu'est-ce que SafeNet eToken FIDO ?

SafeNet eToken FIDO est conçu pour les applications basées sur FIDO et offre une intégration parfaite avec une prise en charge native des environnements Microsoft et mobiles avec le connecteur USB-C.

La clé de sécurité embarque un applet FIDO conforme à la norme Fast IDentity Online 2.0 (FIDO2) et offrent un accès sans mot de passe aux applications cloud, aux services web et à toutes les applications et tous les services connectés à Azure AD.

L'authentification sans mot de passe remplace les mots de passe par d'autres méthodes d'identification qui améliorent les niveaux d'assurance et de commodité. Ce type d'authentification a gagné en popularité en raison des avantages considérables qu'il offre en facilitant l'expérience de connexion pour les utilisateurs et en surmontant les vulnérabilités inhérentes aux mots de passe textuels. Parmi ces avantages, citons la réduction des frictions, un niveau de sécurité plus élevé offert pour chaque application et l'élimination de l'ancien mot de passe.

CHAPITRE 2: Utilisation de FIDO 2.0 avec SafeNet eToken FIDO

Cette section décrit comment initialiser, enregistrer, authentifier et effectuer d'autres opérations avec la clé SafeNet eToken FIDO.

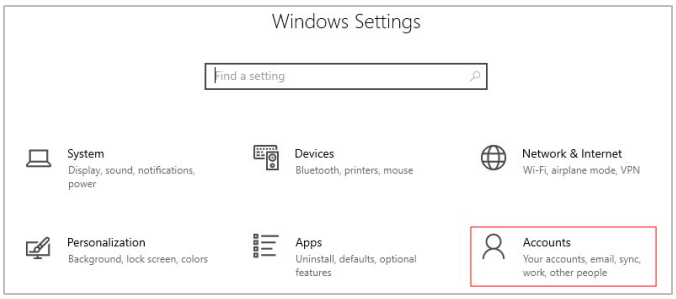
Initialisation

Pour initialiser un appareil, procédez comme suit :

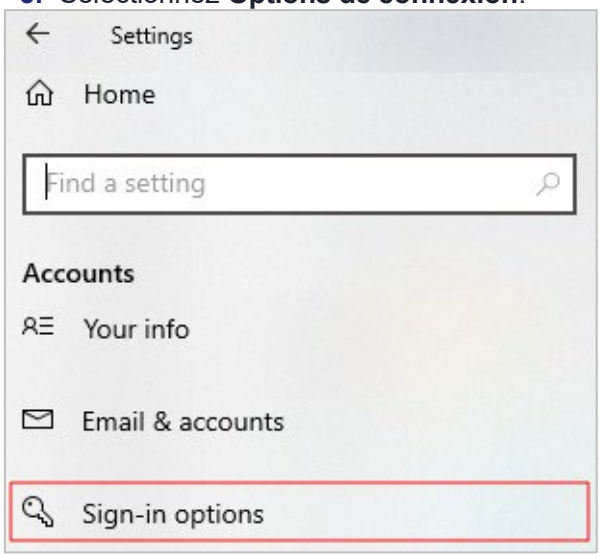
Ajouter un code PIN

Pour ajouter un code PIN à une clé de sécurité :

1. Sur votre ordinateur Windows, sélectionnez **Démarrer**> **Paramètres**.
2. Sélectionnez **Comptes**.

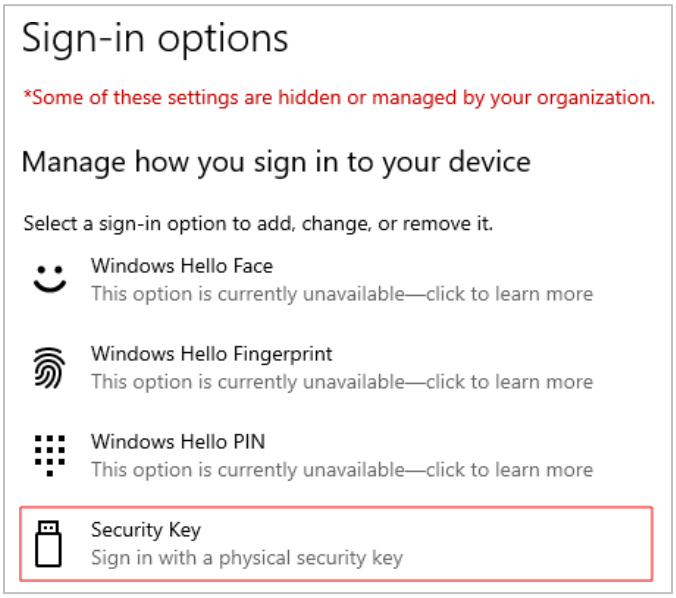


3. Sélectionnez **Options de connexion**.

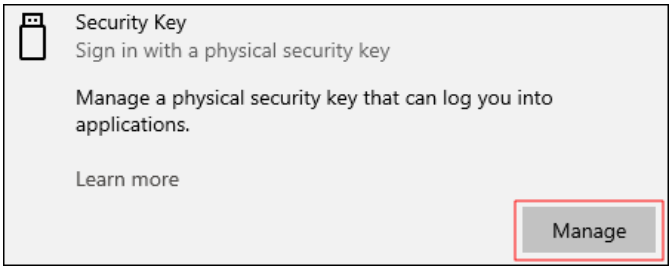


Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

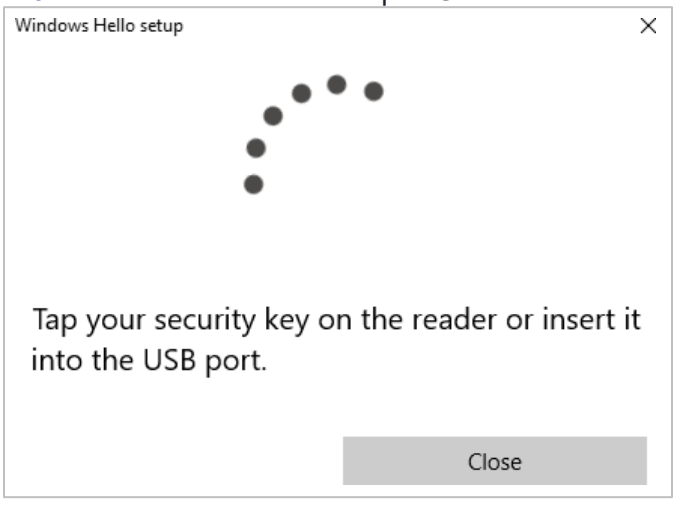
4. Sélectionnez **Clé de sécurité.**



5. Sélectionnez **Gérer**.



6. Insérez votre clé dans le port USB.

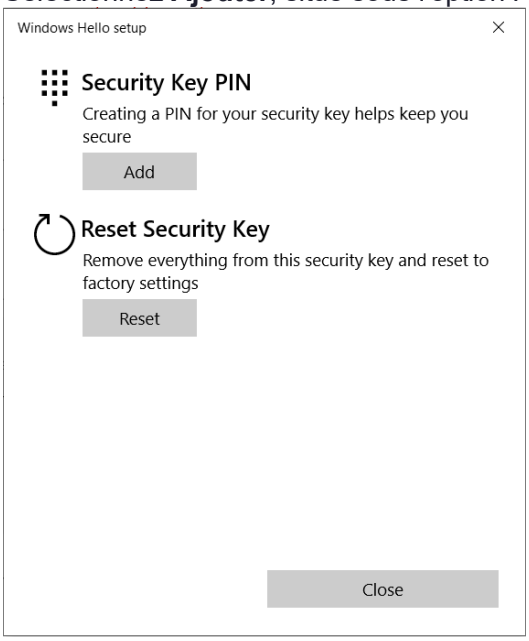


Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

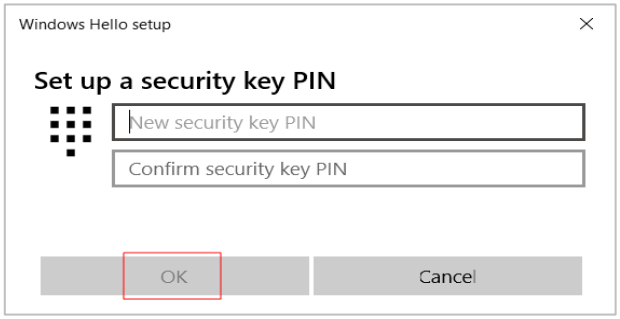
1. Insérer la clé de sécurité dans le port USB.

2. Tapez sur la clé lorsque le voyant est allumé

7. Sélectionnez **Ajouter**, situé sous l'option PIN de la clé de sécurité.



8. Saisissez un code PIN pour la clé de sécurité, puis saisissez-le à nouveau dans les champs prévus à cet effet.
9. Sélectionnez **OK**.



Avant de pouvoir utiliser la clé, vous devez l'enregistrer sur le site web protégé auquel vous souhaitez accéder.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

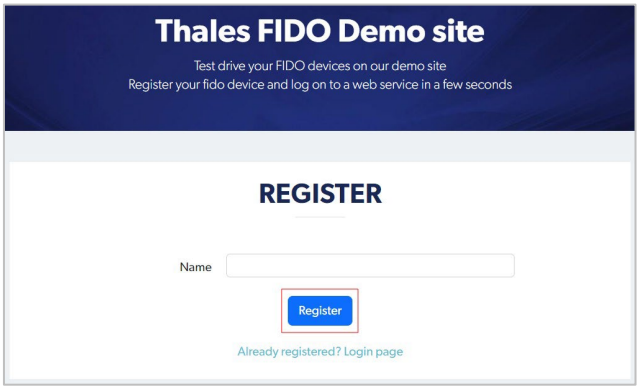
CHAPITRE 3: Inscription

Pour enregistrer une clé:

1. Voir : https://fido.demo.gemalto.com/. (Uniquement disponible en anglais)

> **REMARQUE** Ce site est utilisé à titre d'exemple uniquement. Pour vous authentifier à l'aide d'une méthode compatible FIDO sur un site web pris en charge, reportez-vous à la section d'aide du site concerné pour obtenir des instructions détaillées.

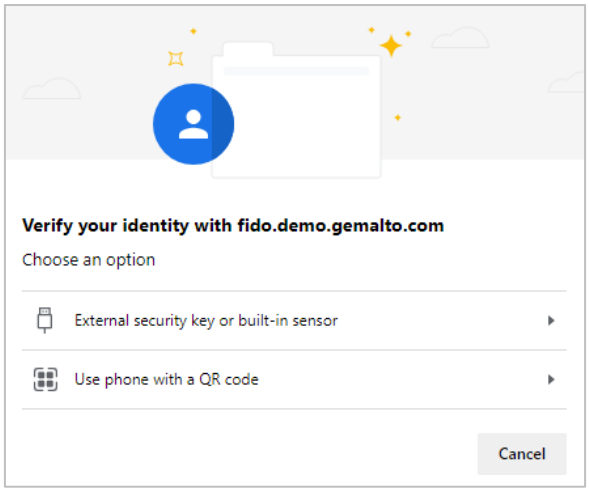
2. Sélectionnez "**S'inscrire maintenant"**.
3. Saisissez votre nom dans le champ prévu à cet effet, puis sélectionnez **S'inscrire.**



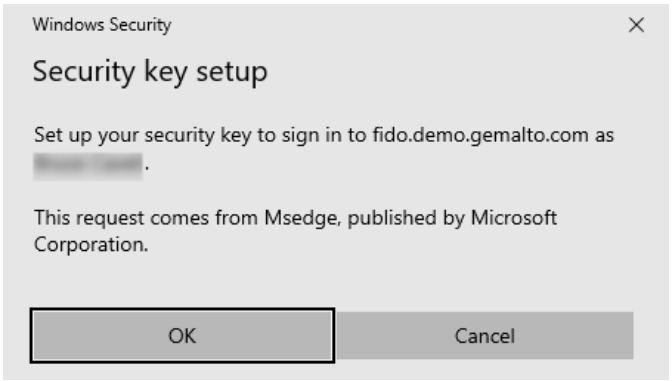
- Sélectionnez **Clé de sécurité externe ou capteur intégré**.

> **REMARQUE** L'option **Utiliser un téléphone avec un code QR** n'est pas prise en charge par ce produit.

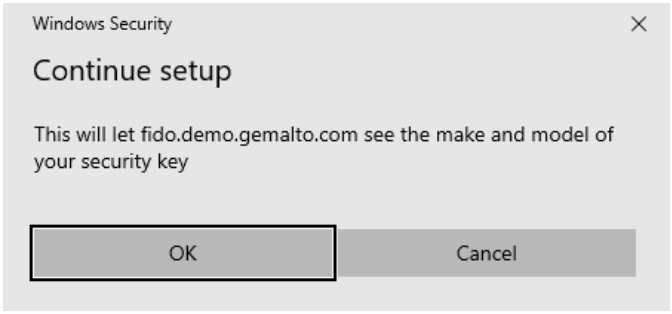
Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés



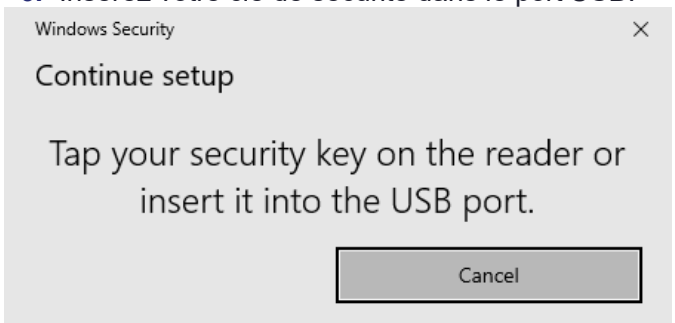
4. Sélectionnez **OK**.



5. Sélectionnez **OK**.

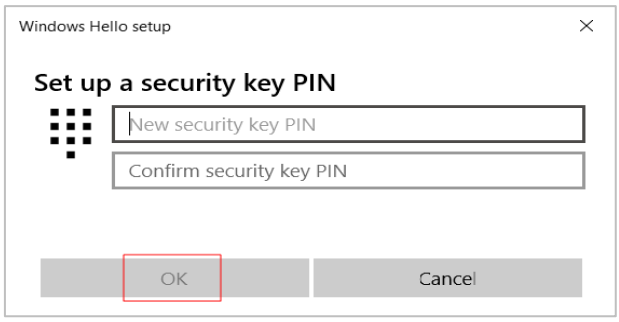


6. Insérez votre clé de sécurité dans le port USB.



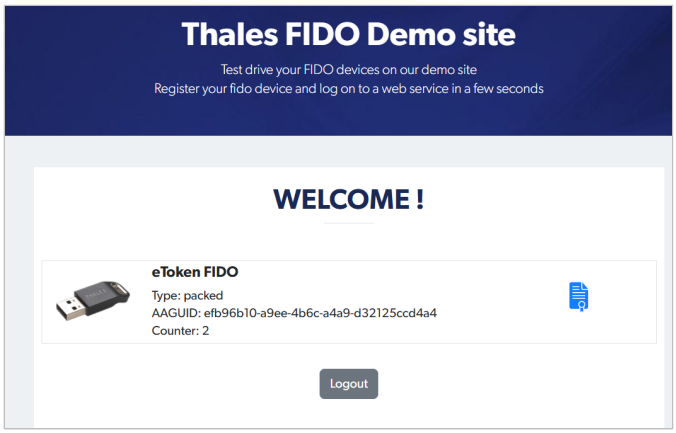
Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

7. Insérer le code PIN



8. Effleurer la clé de sécurité une fois qu'elle est demandée

L'écran de bienvenue s'affiche et votre clé est maintenant accessible.



Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

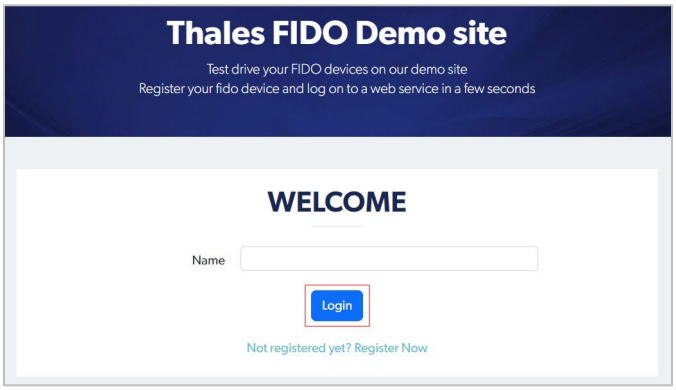
CHAPITRE 4: Authentification

Pour s'authentifier auprès d'un appareil :

1. Allez sur: https://fido.demo.gemalto.com/.

> **REMARQUE** Ce site est utilisé à titre d'exemple uniquement. Pour vous authentifier à l'aide d'une méthode compatible FIDO sur un site web pris en charge, reportez-vous à la section d'aide du site pour obtenir des instructions détaillées.

2. Saisissez le nom que vous avez utilisé lors de l'"Initialisation", puis sélectionnez **Connexion**.



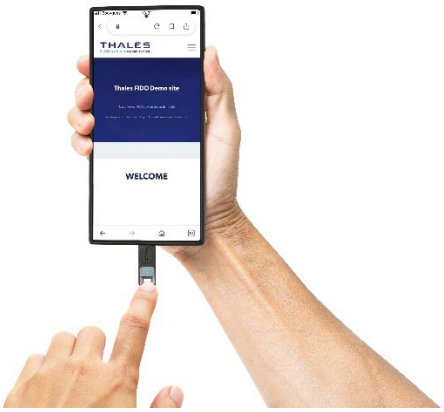
Une fenêtre contextuelle de sécurité Windows s'affiche pour authentifier l'utilisateur.

3. Insérez votre appareil dans le port USB.

4. Insérer le code PIN
5. Effleurez la clé de sécurité une fois qu'elle est demandée.

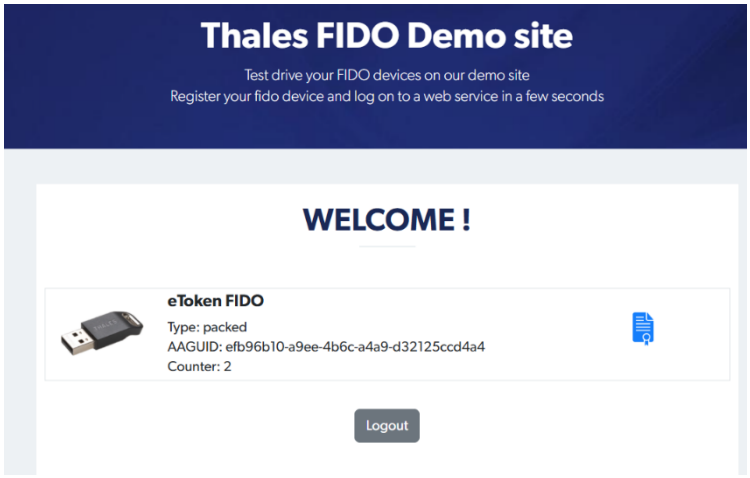
Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

Sur un PC, appuyez sur la clé de sécurité lorsqu'elle est insérée pour terminer l'authentification.



Sur un appareil mobile, appuyez sur la clé de sécurité lorsqu'il est connecté pour terminer l'authentification.

Vous avez maintenant accès au site.



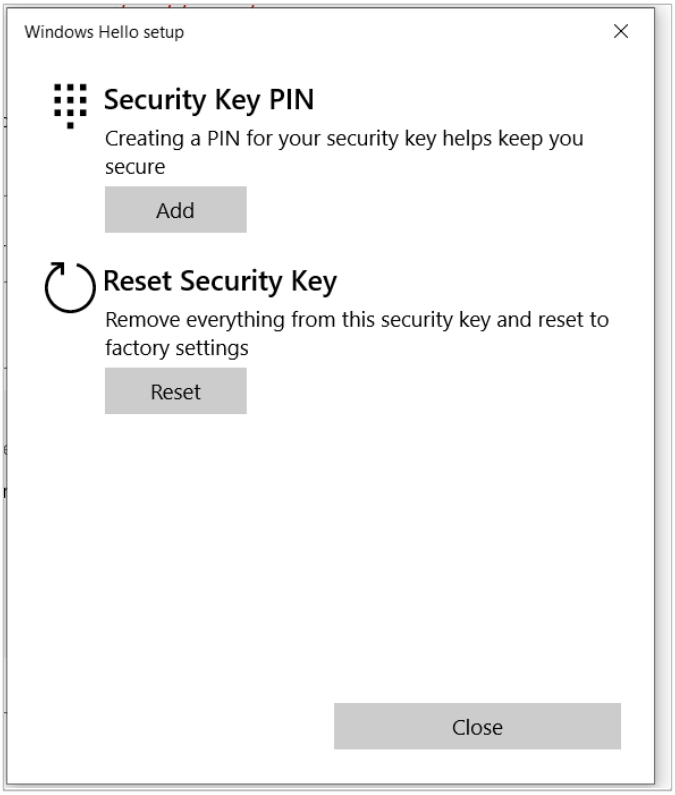
Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

CHAPITRE 5: Réinitialisation

****AVERTISSEMENT** Il s'agit d'une procédure destructrice. Toutes les données et informations d'identification créées précédemment avec la clé de sécurité seront perdues.**

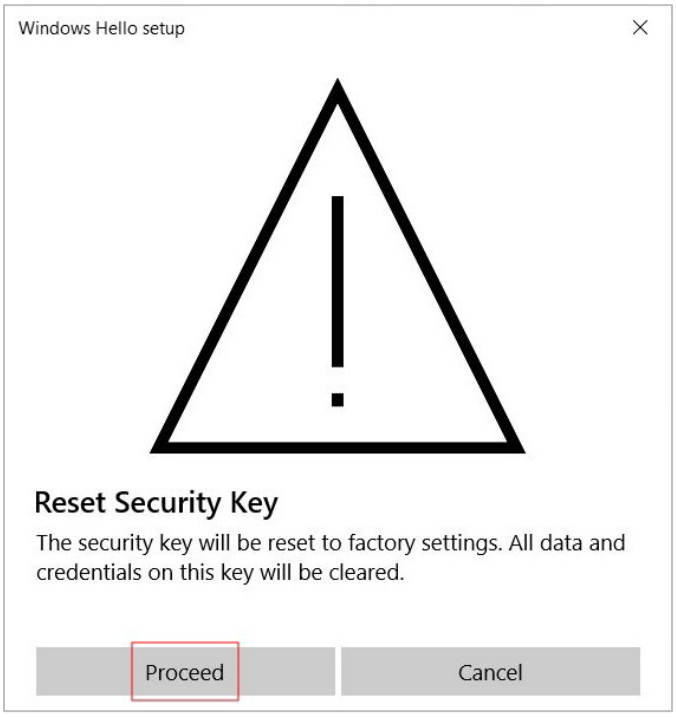
Pour réinitialiser un appareil :

1. Effectuer les étapes 1 à 4 de la section "Initialisation de l'appareil".
2. Sélectionnez **Réinitialiser**.

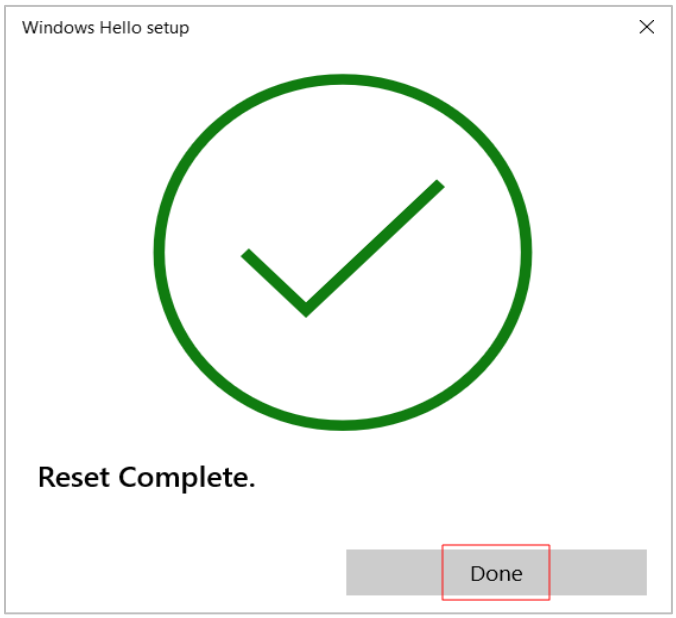


Un message avertit de la nécessité de réinitialiser les paramètres d'usine.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

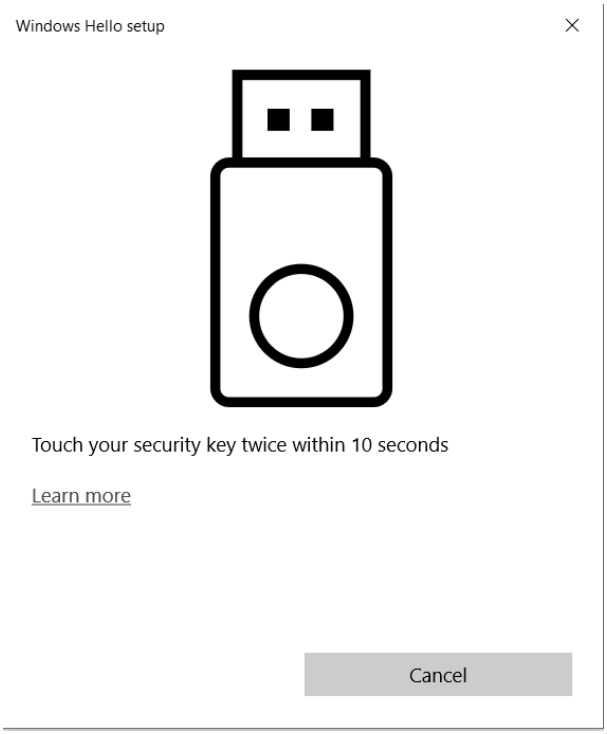


3. Sélectionner **Poursuivre**



4. Retirez et insérez votre clé de sécurité dans le port
5. Pour terminer l'opération de réinitialisation, touchez deux fois la clé une fois que cela est demandé.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés



6. Sélectionnez **Terminé**.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

CHAPITRE 6: FIDO sur un compte Microsoft 365

Cette section décrit comment initialiser, enregistrer et authentifier eToken FIDO sur un compte Microsoft 365.

Initialisation

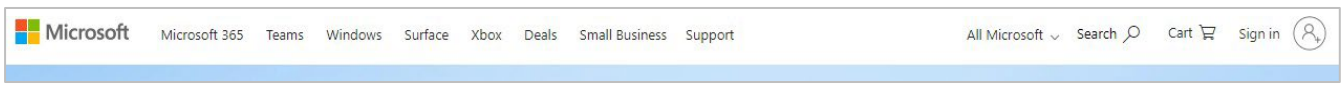
Pour initialiser un appareil :

1. Ajouter un code PIN à un appareil, voir "Ajouter un code PIN" .

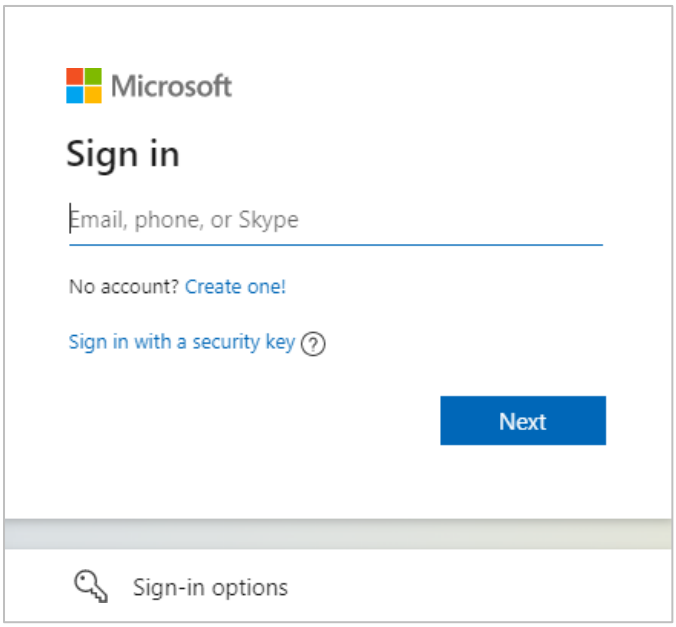
Pour enregistrer un appareil sur Microsoft :

Scénario 1

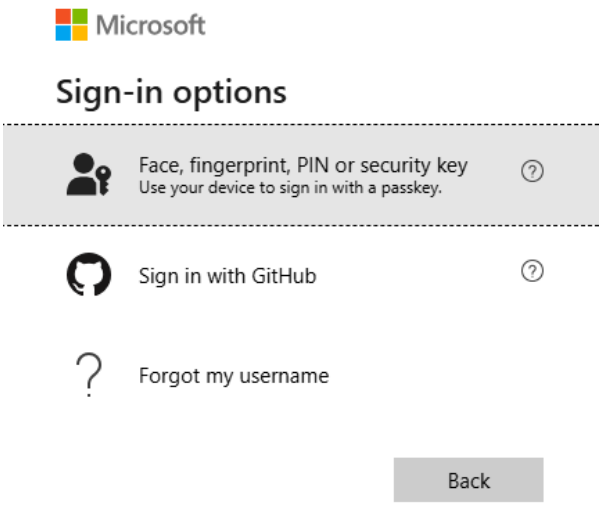
1. Allez sur https://www.microsoft.com et sélectionnez **Sign in** en haut à droite de la page.



2. Sélectionnez l'option de connexion que vous préférez .

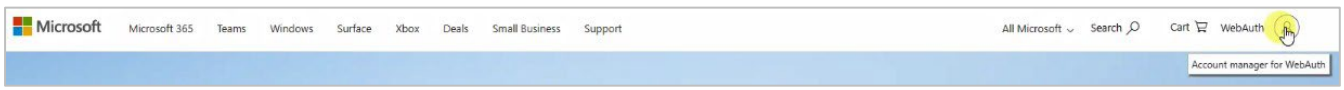


Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

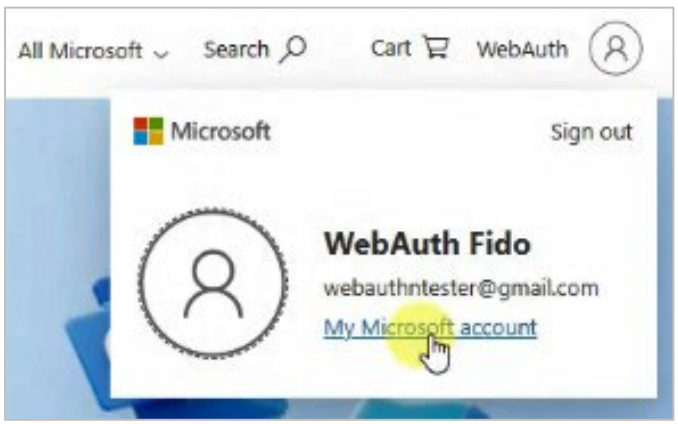


Scénario 2

1. Allez sur https://www.microsoft.com et sélectionnez **WebAuth** en haut à droite de la page.



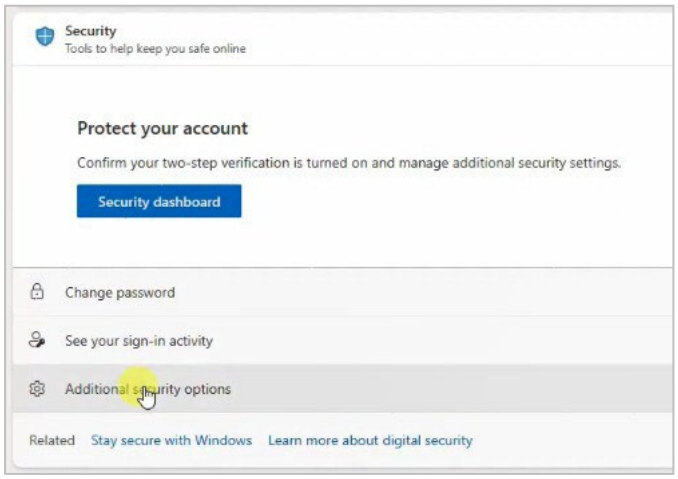
2. Sélectionnez **Mon compte Microsoft**.



3. Sélectionnez **Sécurité**.

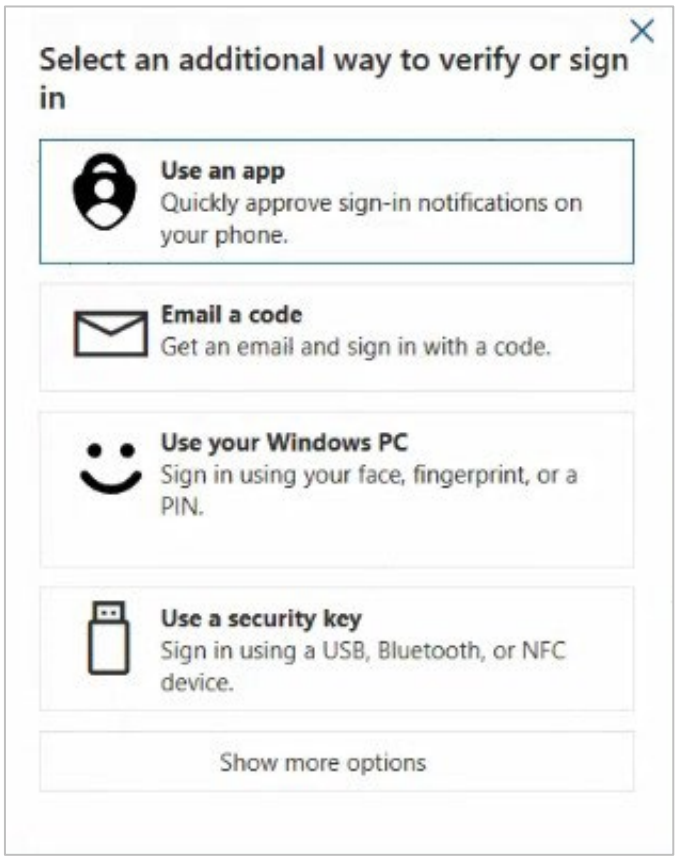
4. Sélectionnez **Options de sécurité supplémentaires**.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés



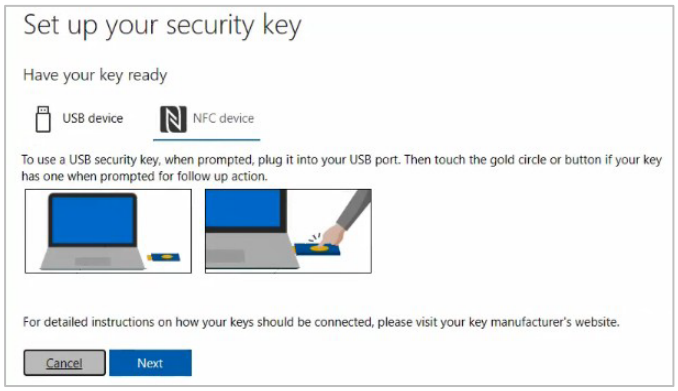
5. Sélectionnez **Ajouter une nouvelle méthode de connexion ou de vérification.**

6. Sélectionnez **Utiliser une clé de sécurité**.



7. Sélectionnez le **périphérique USB**, puis cliquez sur **Suivant**.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

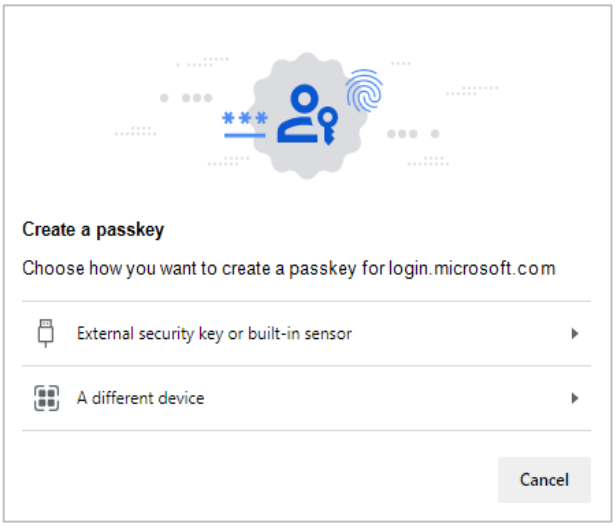


L'écran suivant s'affiche en arrière-plan pendant la procédure de configuration.

8. **Sélectionnez Clé de sécurité externe ou capteur intégré.**

> **NOTE** Cette option ne s'affiche que si vous ne fournissez pas la clé de sécurité dans le délai imparti. Cela peut se produire si, par exemple, vous ne disposez pas d'un lecteur de carte à puce.

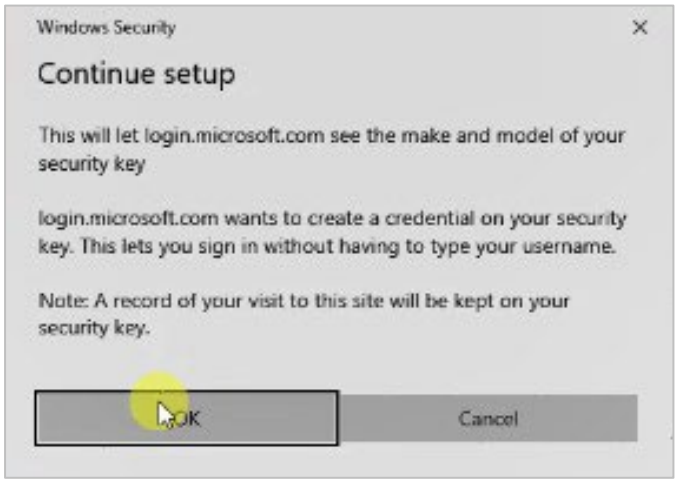
Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés



9. Sélectionnez **OK**.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

10. Sélectionnez **OK**.



11. Insérez votre clé de sécurité dans le port USB.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

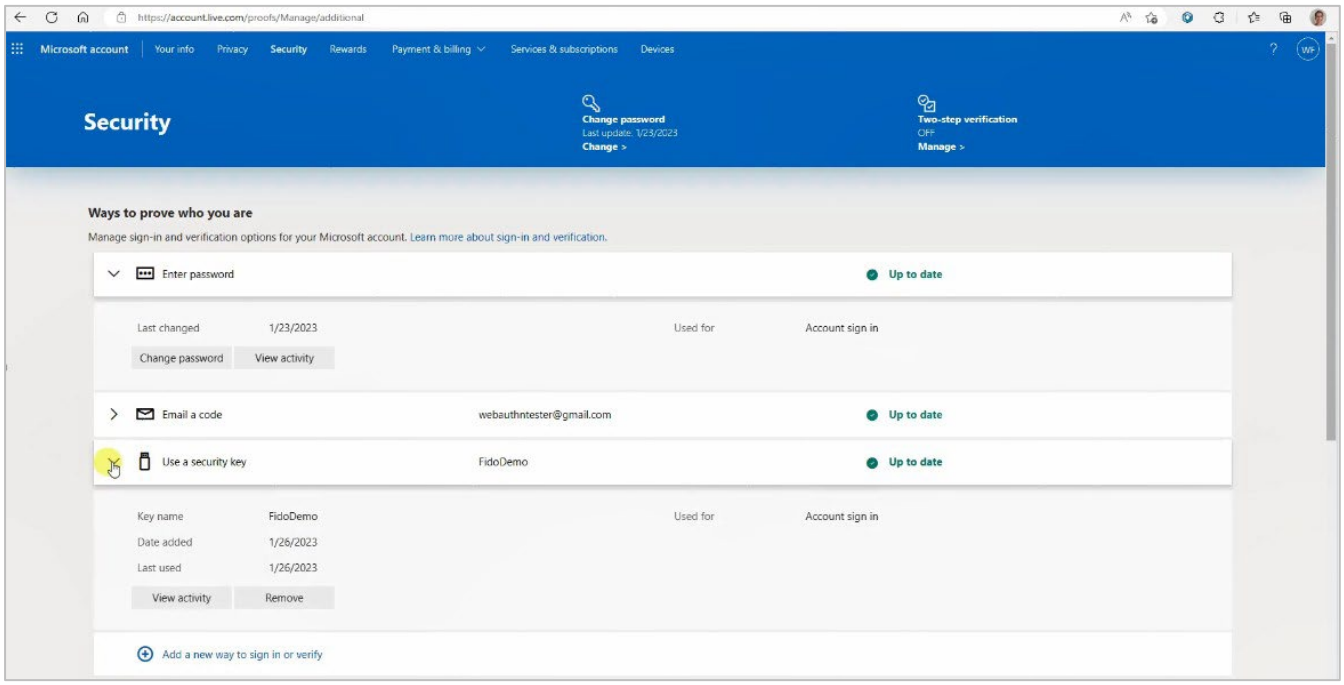
12. Saisissez un nom pour votre clé de sécurité, puis sélectionnez **Suivant.**

13. Sélectionnez **Compris**

Vous pouvez maintenant utiliser votre clé de sécurité pour vous connecter.

Votre clé de sécurité est répertoriée, comme le montre la capture d'écran suivante.

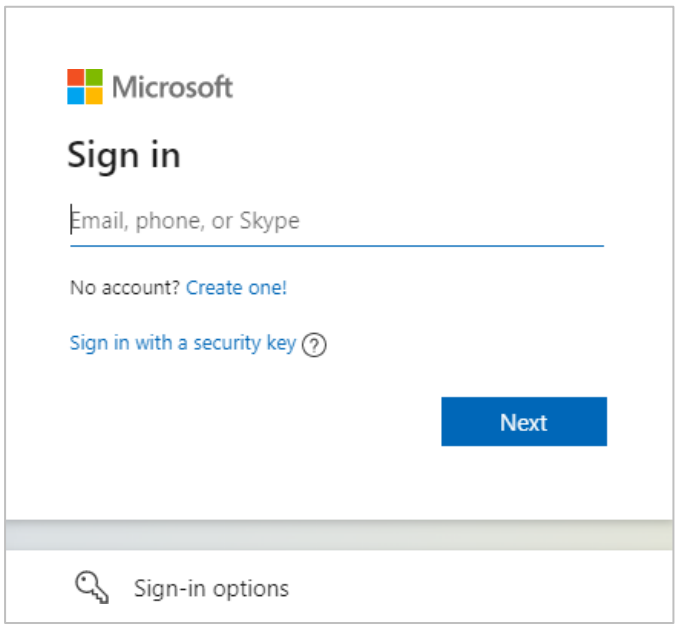
Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés



Authentification avec une clé

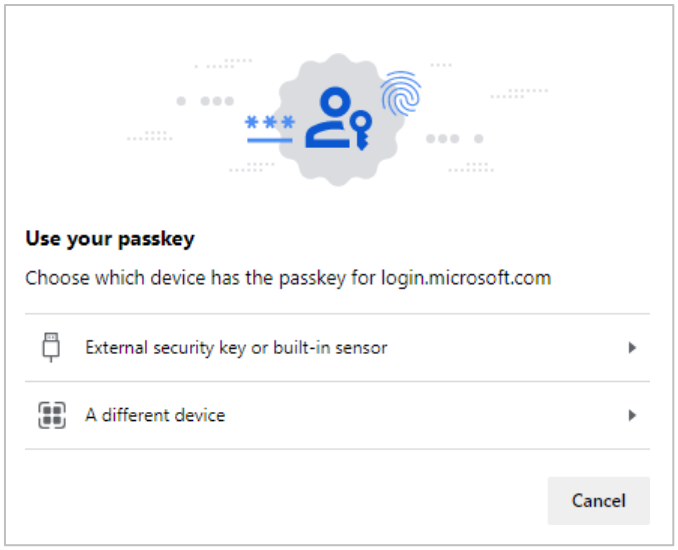
Pour s'authentifier avec un appareil sur un site Microsoft :

1. Allez sur le site de Microsoft et sélectionnez **Se connecter avec clé de sécurité**.



2. Sélectionnez **Clé de sécurité externe ou capteur intégré**.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés



3. Insérez votre clé dans le port USB.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

4. Sélectionnez votre préférence de connexion.

Vous avez maintenant accès au site web de Microsoft.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

CHAPITRE 7: FIDO sur Android

Cette section décrit comment initialiser, enregistrer, authentifier et effectuer d'autres opérations sur le SafeNet eToken FIDO sur Android.

Au préalable, assurez-vous que l'application FIDO Key Manager" (FKM") est installée sur votre appareil Android.

Initialisation

Effectuez les étapes suivantes pour initialiser un eToken FIDO :

Ajouter un code PIN

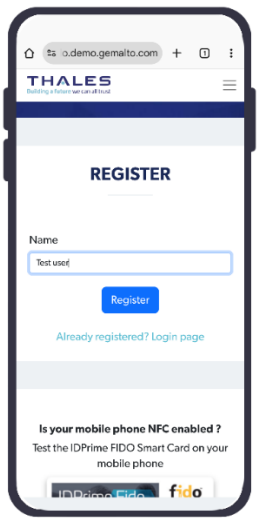
Pour ajouter un code PIN, veuillez suivre les étapes détaillées de la section Gestion des codes PIN.

Pour enregistrer un appareil :

1. Voir : https://fido.demo.gemalto.com/.

> **NOTE** Ce site est utilisé à titre d'exemple uniquement.

2. Sélectionnez "**S'inscrire maintenant"**.
3. Saisissez votre nom dans le champ prévu à cet effet, puis sélectionnez **S'inscrire.**



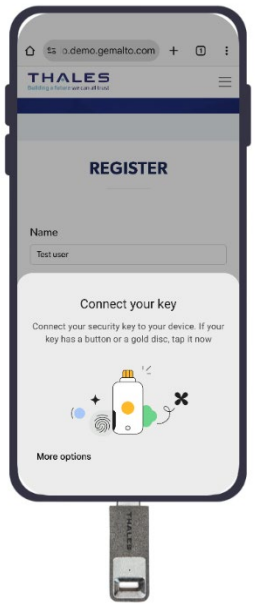
- Sélectionnez **Clé de sécurité externe ou capteur intégré**.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

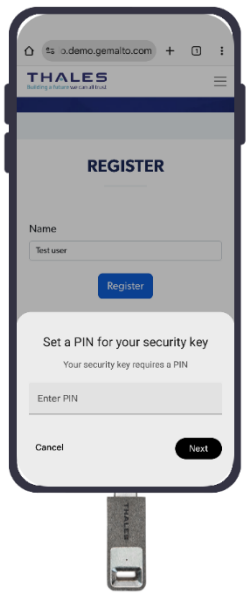
NOTE Cette option ne s'affiche que si vous ne fournissez pas la clé de sécurité dans le délai imparti. Cela peut se produire si, par exemple, vous ne disposez pas d'un lecteur de carte à puce.

REMARQUE L'option **Utiliser un téléphone avec un code QR** n'est pas prise en charge par ce produit.

4. Insérez votre clé.

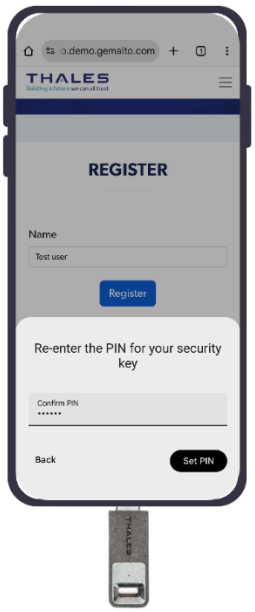


5. Définir le code PIN.

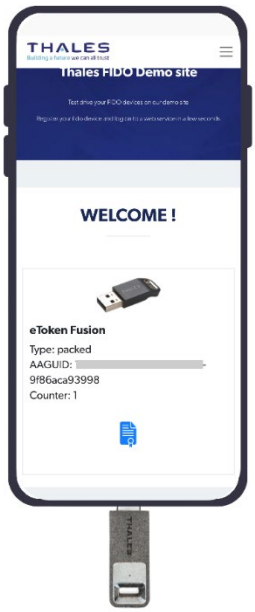


Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

6. Saisir à nouveau le code PIN



7. L'écran de bienvenue s'affiche et votre clé est maintenant accessible.

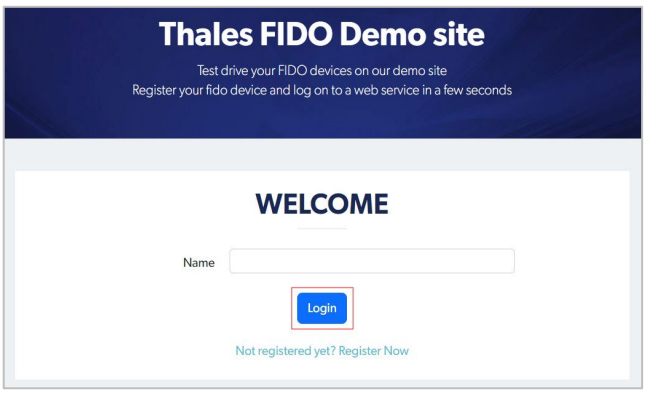


Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

Authentification avec un appareil

REMARQUE Ce site est utilisé à titre d'exemple uniquement. Pour vous authentifier à l'aide d'une méthode compatible FIDO sur un site web pris en charge, reportez-vous à la section d'aide du site pour obtenir des instructions détaillées.

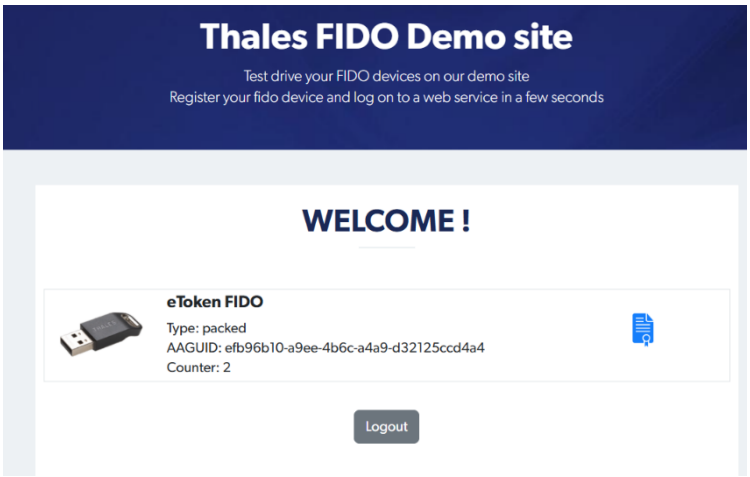
1. Voir : https://fido.demo.gemalto.com/.
2. Saisissez le nom que vous avez utilisé lors de l'inscription, puis sélectionnez **Connexion**.



Une fenêtre contextuelle de sécurité Windows s'affiche pour authentifier l'utilisateur.

3. Insérez votre appareil dans le port USB-C de votre mobile.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés



Vous avez maintenant accès au site.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

CHAPITRE 8: Spécifications techniques

Caractéristiques du produit

CARACTERISTIQUES	DESCRIPTION
MEMOIRE	52K
NORMES	Assistance en matière d'API et de normes : > FIDO 2.0 et U2F
SYSTEMES D'EXPLOITATION	> FIDO : pris en charge par Windows 10 et d'autres systèmes d'exploitation compatibles FIDO. > PKI : Windows Server 2008/R2, Windows Server 2012 et 2012 R2, Windows 7, Windows 8 > Windows 10, Windows 11, Mac OS, Linux
DIMENSIONS	> USB-A : 16mm*8mm*40.5mm > USB-C : 12mm*6,5mm*38mm
TEMPERATURE DE FONCTIONNEMENT	0° C à 70° C (32° F à 158° F)
TEMPERATURES DE STOCKAGE	De -40° C à 85° C (de -40° F à 185° F)
TAUX D'HUMIDITE	0-100% sans condensation
CERTIFICATION DE RESISTANCE A L'EAU	IP X7 - IEC 529
CONNECTEUR USB	> USB type A et USB type C supporte USB 1.1 et 2.0 (pleine vitesse)
ENVELOPPE	Plastique moulé dur, inviolable
MEMOIRE CONSERVATION DES DONNEES	Au moins 10 ans
REECRITURE DES CELLULES DE LA MEMOIRE	Au moins 500 000
COMPATIBILITE	Comptes Microsoft Azure Active Directory
CERTIFICATIONS	> Certification U2F (USB), version 1.1

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

	> FIDO2 niveau 1, version 2.0 > CC EAL5+ certifié selon EN 419211 partie 2 à partie 6 (correspondant au PP QSCD) > Conformité à : - ANSSI - eIDAS pour la signature électronique
ATR	- 3B FF 96 00 00 81 31 FE 43 80 31 80 65 B0 85 59 56 FB 12 01 78 82 90 00 88
NOM DU PRODUIT	SafeNet eToken FIDO
VERSION MASQUE	G286
VERSION DE L'APPLET	> FIDO 2.0.2.B > IDPrime Java Applet 4.4.2.a
PIN	PIN par défaut : "0000"

Fonctionnalité tactile

Pour utiliser la fonctionnalité du sens du toucher, procédez comme suit :

> La détection de présence est requise dans le cadre de l'authentification FIDO.

> La surface de détection de présence est présente au dos du clé.

> La surface de détection de présence ne doit être que touchée et NON pressée.

> La LED du SafeNet eToken FIDO s'allume et s'éteint en attendant de détecter la présence d’un être humain. Lorsque la surface de détection de présence est touchée :

- le voyant reste allumé sur SafeNet eToken FIDO

- la LED s'éteint sur SafeNet eToken FIDO

Exemple d'utilisation du sens du toucher :

L'image ci-dessous représente le SafeNet eToken Fusion :

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

L'image ci-dessous représente le SafeNet eToken FIDO :

Comportement des diodes électroluminescentes de l'appareil

Le tableau ci-dessous décrit les différents modes de LED de l'appareil :

MODE LED	DESCRIPTION
DESACTIVER	L'appareil n'est pas connecté à l'ordinateur ou le port USB est suspendu.
ALLUMER	L'appareil est connecté à l'ordinateur et prêt à fonctionner.
FONDU ENTRANT / FONDU SORTANT	Le dispositif attend la détection de la présence humaine. Cette fonction est déclenchée par le micrologiciel lors de l'analyse des données utiles CTAP2 afin de détecter si la présence de l'utilisateur est requise pour des commandes spécifiques. L'utilisateur doit toucher le dispositif dans un délai prédéfini (30 secondes), sinon la demande CTAP2 est rejetée.
CLIGNER DES YEUX	Défaillance de l'appareil. Le voyant de l'appareil clignote selon un schéma prédéfini. Contactez le support.

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

Contactez l’assistance

Si vous rencontrez un problème lors de l'installation, de l'enregistrement ou de l'utilisation de ce produit, veuillez consulter la documentation ci-dessus avant de contacter le service d'assistance.

Si vous ne parvenez pas à résoudre le problème, contactez l'équipe d'escalade du support de SAS à l'adresse électronique suivante : dl_sassupportescalationteam@thalesgroup.com

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés

CHAPITRE 9: Activez vos clés Fido dans SafeNet Trusted Access

Qu'est-ce que SafeNet Trusted Access et comment l'utiliser ?

SafeNet Trusted Access offre un accès sécurisé et simple à toutes les applications gérées par l'entreprise grâce à une authentification transparente sans mot de passe.

Découvrez comment activer l'authentification FIDO avec votre clé de sécurité dans SafeNet Trusted Access.

Découvrez comment les utilisateurs finaux peuvent auto-approvisionner SafeNet eToken Fusion ou eToken FIDO dans SafeNet Trusted Access.

S'INSCRIRE À UN ESSAI GRATUIT POUR STA

Mars 2025, Copyright© 2025 Groupe Thales. Tous droits réservés