MISE A DISPOSITION DES NOUVEAUX EQUIPEMENTS AUX UTILISATEURS

Document qui explique la mise en place des nouveaux équipements informatiques

ASSURMER

Services informatiques

Version : 4.0

Service IT

22/03/2022

Yohan HALIMI

Kevin ORTIZ

DIFFUSION et VISAS

Diffusion			
Société / Entité	**Destinataires**	**Fonction**	**Diffusion**
Assurmer	Service IT	Procédure	Réseau

Visas			
Société / Entité	**Nom**	**Fonction**	**Signature**

SUIVI DES VERSIONS

Versions				
Version	**Date**	**Auteur**	**Raison**	**Nombre de pages**
V 8.0	14/12/2022	Kevin ORTIZ Yohan HALIMI	Solution de stockage	14

COORDONNEES

Contacts		
Nom	**E-mail**	**Téléphone**
Kevin ORTIZ	Kevin.ortiz@edu.esiee-it.fr	07.50.03.94.59
Yohan HALIMI	Yohan.Halimi@edu.esiee-it.fr	06.89.03.25.78

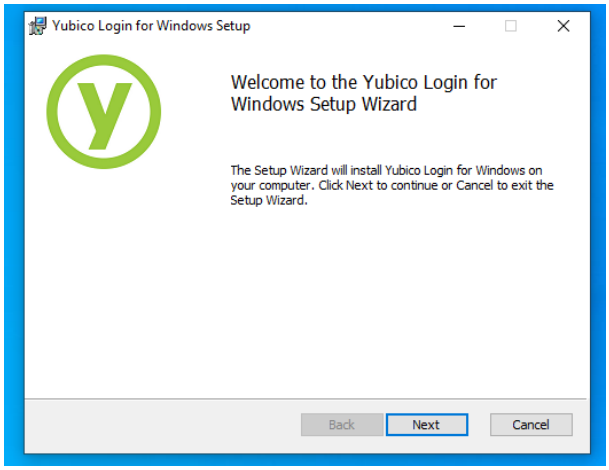
Table des matières

1 Système de double authentification avec Yubico :

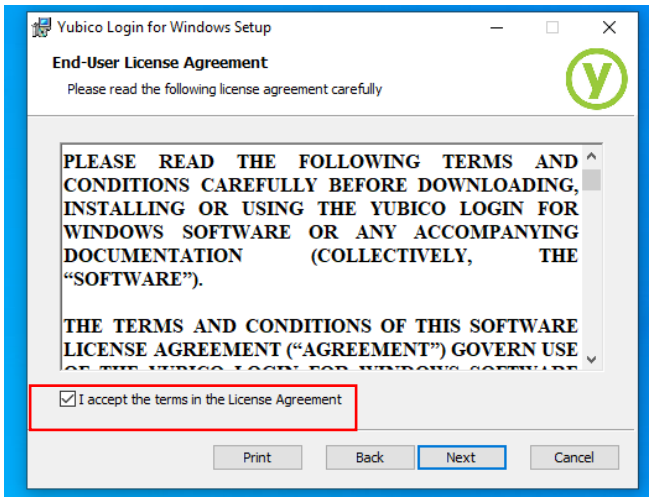
1.1 Installation du logiciel :

Avant d'installer le logiciel Yubico Login pour Windows, notez votre nom d'utilisateur et votre mot de passe Windows pour le compte local. La personne qui installera le logiciel doit avoir le nom d'utilisateur et le mot de passe Windows pour son compte. Sans ceux-ci, rien ne peut être configuré et le compte sera inaccessible.

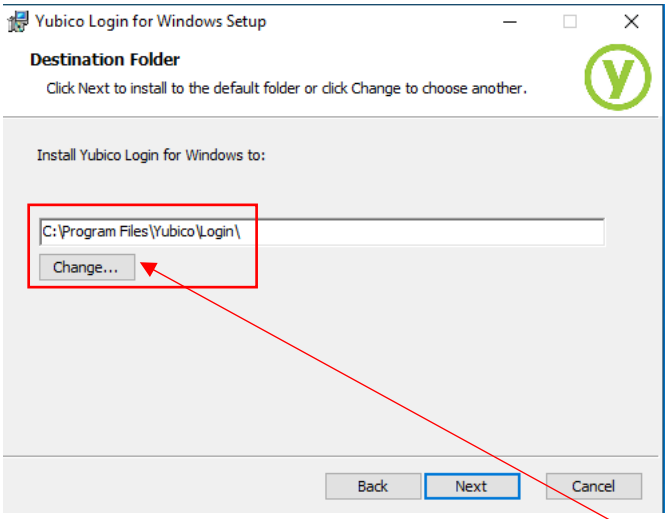
Puis double cliquez sur cet exécutable.



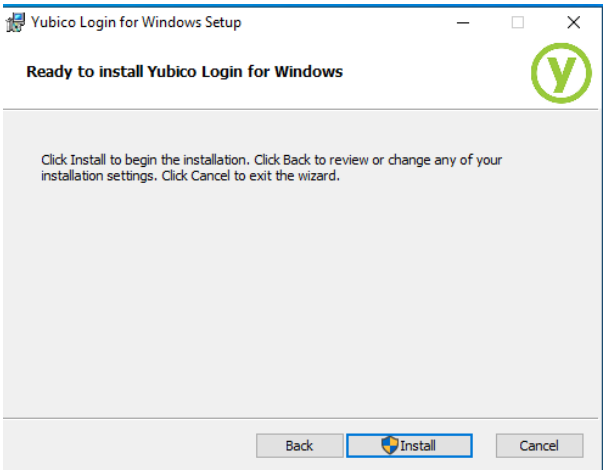
Cliquez sur Next



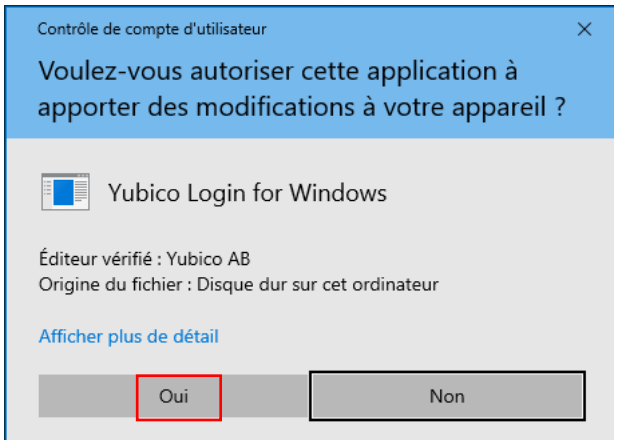
Cochez la case pour affirmer que l'on accepte les thermes de la licence puis après il faudra cliquer sur Next.



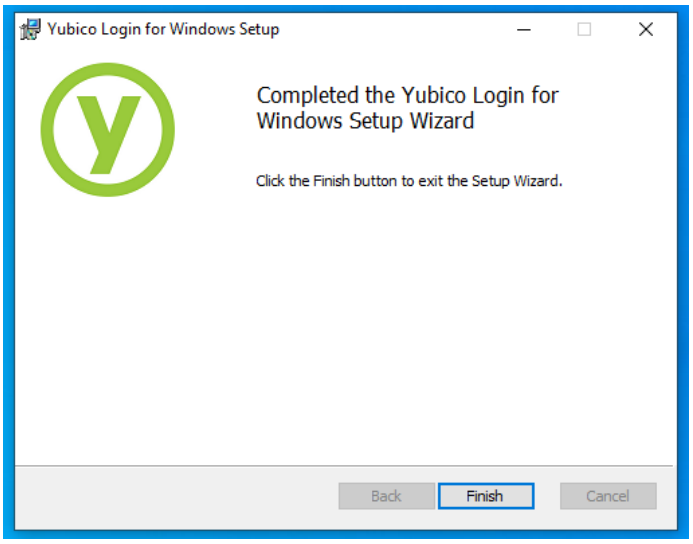
Une fois arrivé ici on vous demande de choisir où vous voulez installer le logiciel, vous pouvez le laisser par défaut comme sur la photo ou sinon vous pouvez cliquer sur change et choisir l'emplacement que vous voulez lui attribuer. Après, il faut cliquer sur Next.



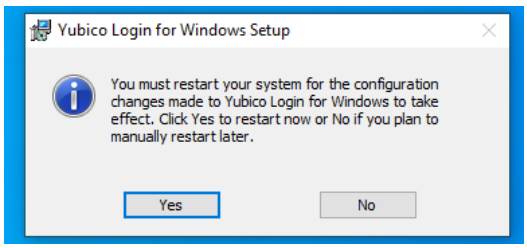
Une fois arrivé ici, veuillez cliquer sur install pour confirmer les choix que vous avez faits précédemment et débuter l'installation.



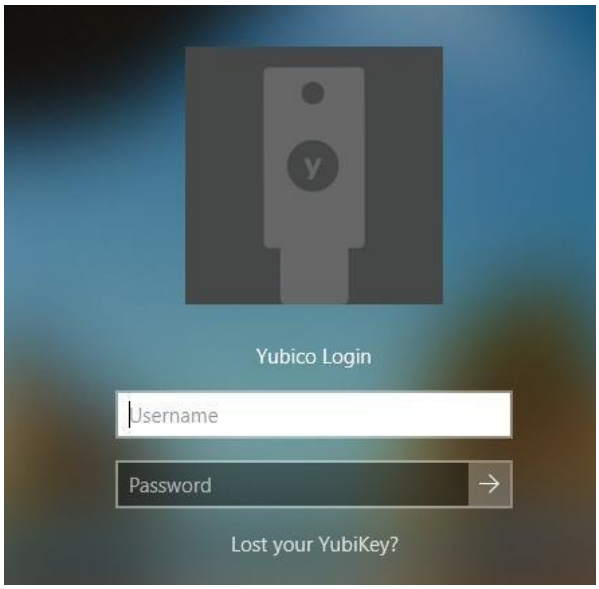
Ici Windows vous demande de confirmer le droit au logiciel Yubico et d'apporter des modifications à votre poste et pour s'installer. Veuillez donc cliquer sur oui.



Ici, cliquer sur finish pour terminer l'installation

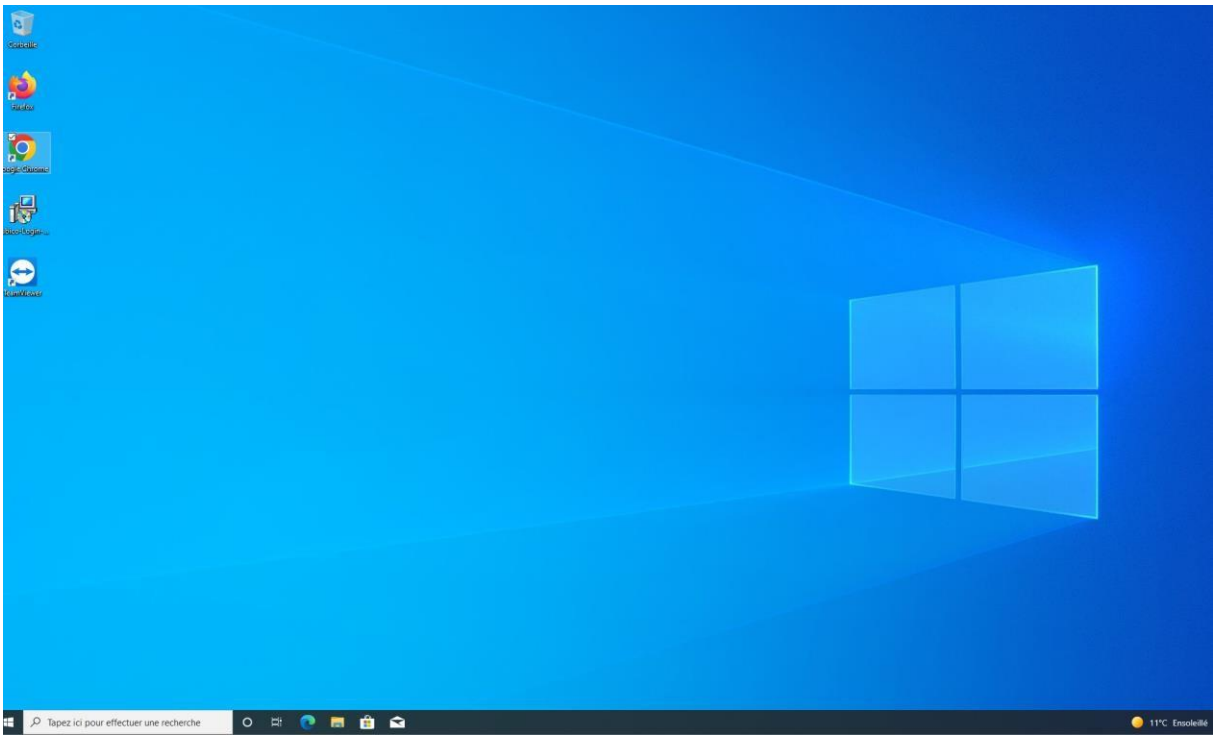


Un message va s'afficher vous demandant de redémarrer votre poste. En cliquant sur yes celui-ci va redémarrer automatiquement.

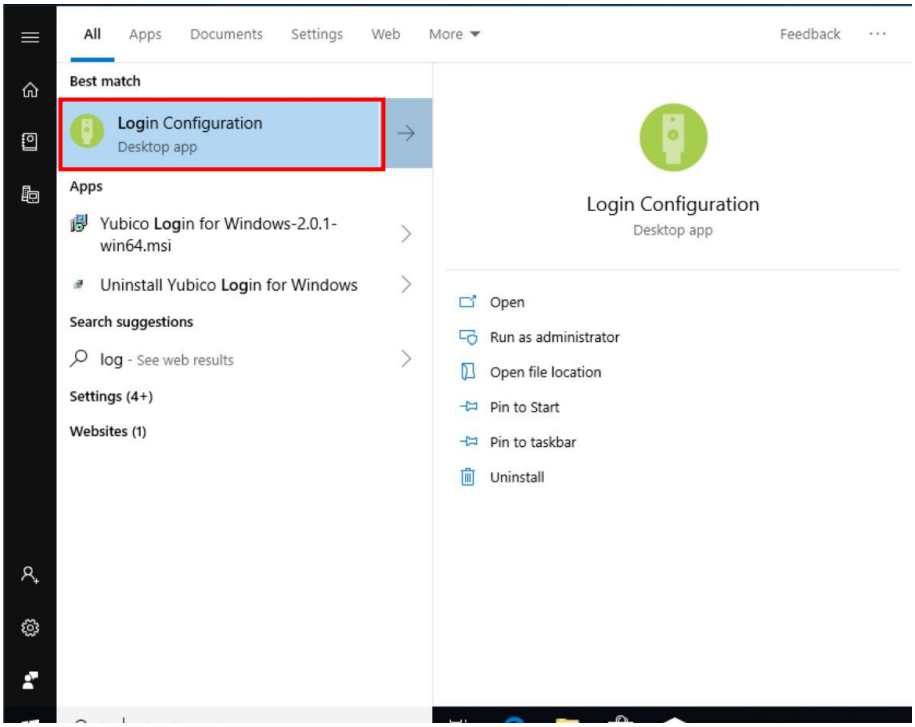


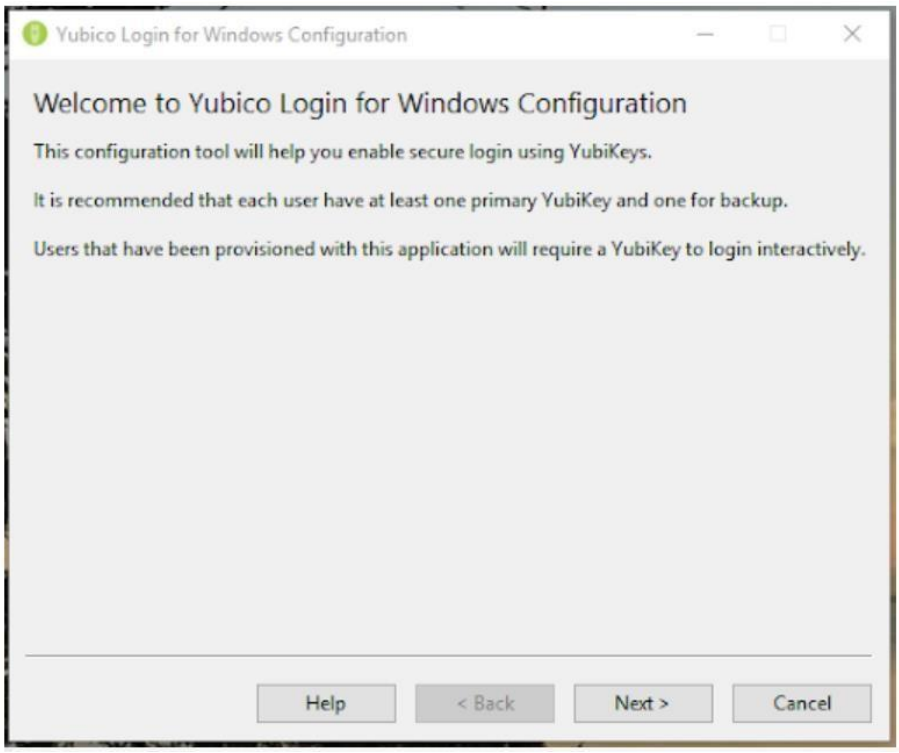
Une fois que votre poste soit redémarré comme vous pouvez le voir l'interface a changé. Il vous faut saisir le nom ainsi que le mot de passe du poste que vous avez retenu en début de procédure.

1.1 Configuration du logiciel :



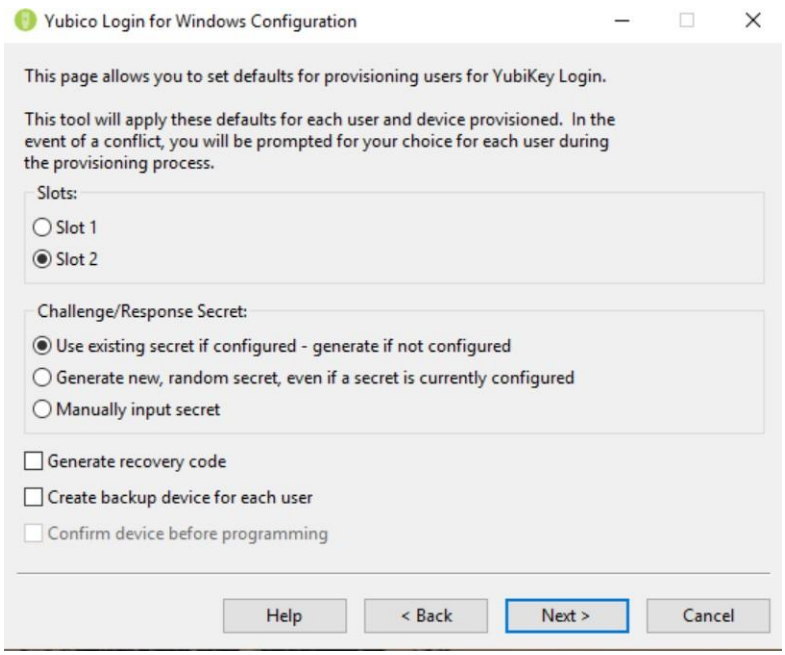
Une fois votre poste redémarré, taper Login Configuration dans le menu démarrer puis rechercher l'application suivante :

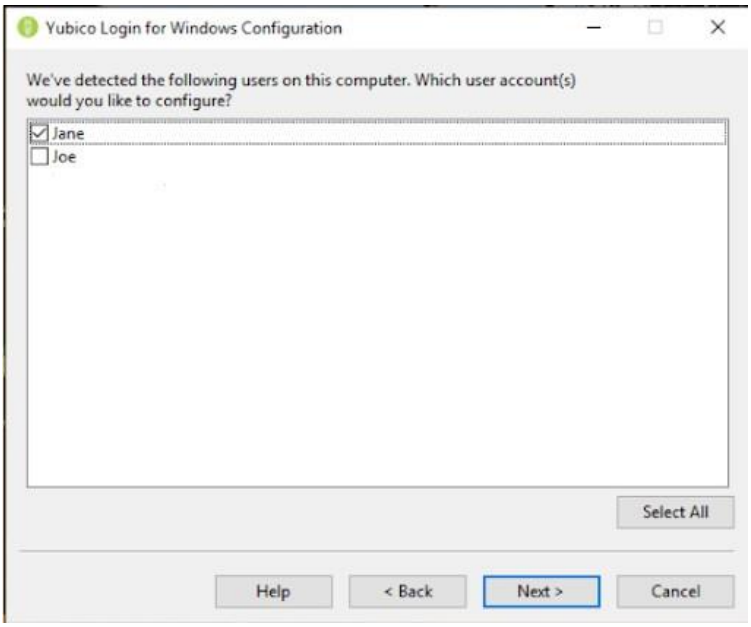




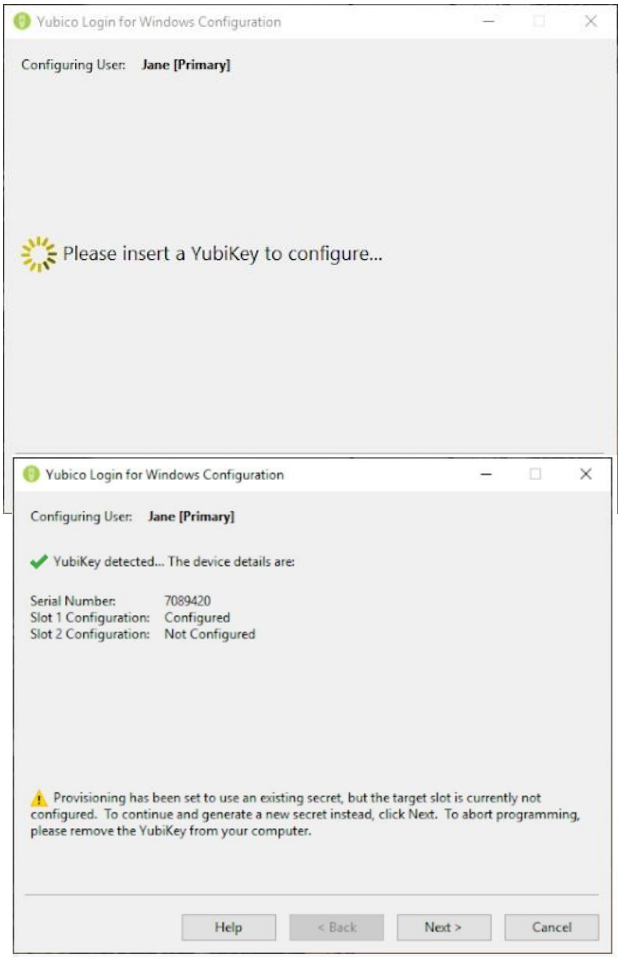
Une fois ici veuillez cliquer sur next

Puis inscrivez les mêmes paramètres que sur la capture d'écran ci-dessous :

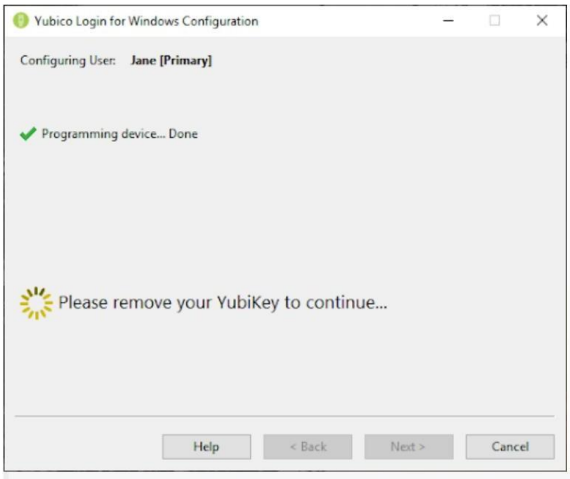




Sur la page ci-dessus, sélectionnez les comptes d'utilisateurs à provisionner pendant l'exécution actuelle de Yubico Login pour Windows en cochant la case à côté du nom d'utilisateur, puis cliquez sur Next. La page Configuration de l'utilisateur s'affiche comme illustré ci-dessous.



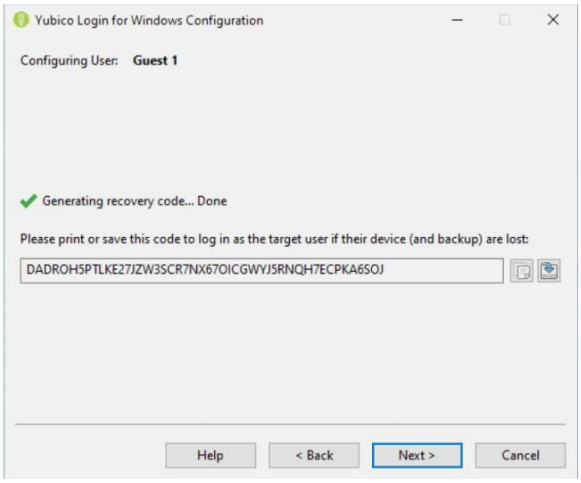
Une fois la programmation terminée pour un compte utilisateur, ce compte n'est plus accessible sans la YubiKey correspondante. Vous êtes invité à supprimer la YubiKey que vous venez de configurer et le processus de provisionnement passe automatiquement à la prochaine combinaison compte d'utilisateur/YubiKey, comme indiqué dans la capture d'écran ci-dessous.



Une fois chose faite, il faudra générer les codes de récupération :

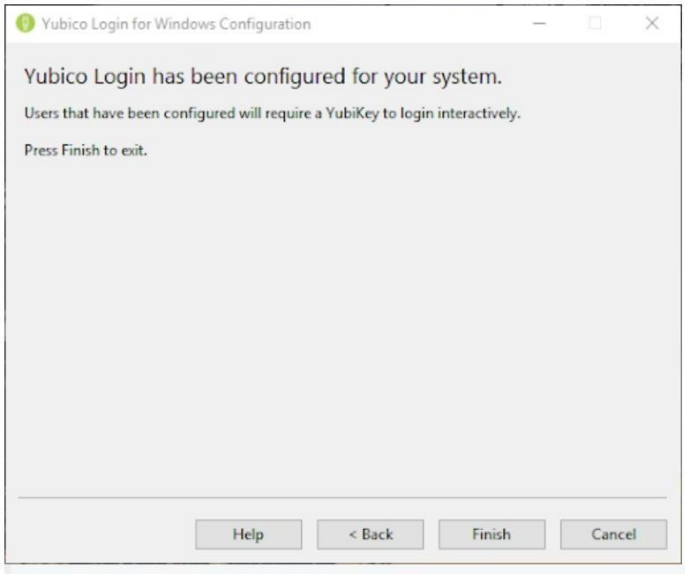
Lors de la définition des paramètres du flux d'approvisionnement comme décrit dans Spécifier la configuration ci-dessus, vous pouvez déterminer si des codes de récupération peuvent être créés pour les utilisateurs YubiKey. Le code de récupération est une longue chaîne.

Sur la page Code de récupération, générez et définissez un code de récupération pour l'utilisateur sélectionné. Une fois cela fait, les boutons **Copier** et **Enregistrer** à droite du champ du code de récupération deviennent disponibles, comme le montre la capture d'écran ci-dessous :



N’oubliez pas de bien conserver le code. Puis cliquez sur Next.

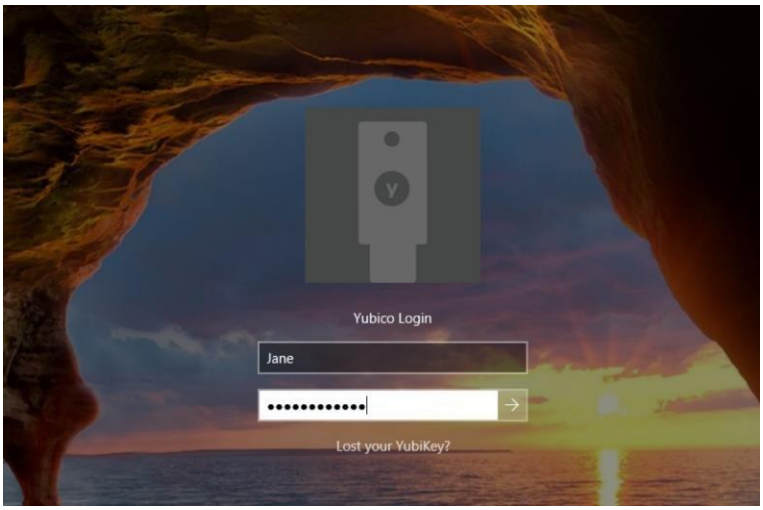
Lorsque vous avez configuré le dernier utilisateur, le processus de provisionnement affiche la page Terminé comme illustré dans la capture d'écran ci-dessous.



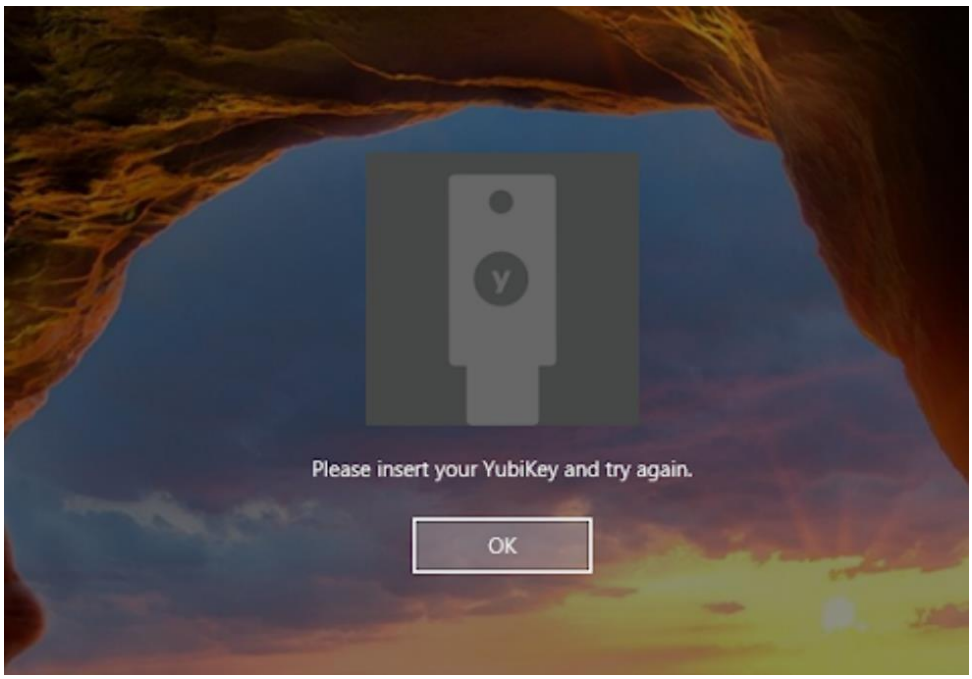
Il faudra donner à chaque utilisateur son code de récupération. Les utilisateurs finaux doivent enregistrer leur code de récupération dans un emplacement sûr, accessible lorsqu'ils ne peuvent pas se connecter.

1.1 Démonstration sur le poste d'un utilisateur :

Lorsque le compte d'utilisateur local a été configuré pour exiger une YubiKey, l'utilisateur est authentifié par le fournisseur d'informations d'identification Yubico au lieu du fournisseur d'informations d'identification Windows par défaut. L'utilisateur est invité à insérer sa YubiKey. Ensuite, l'écran de connexion Yubico s'affiche. L'utilisateur entre son nom d'utilisateur et son mot de passe.

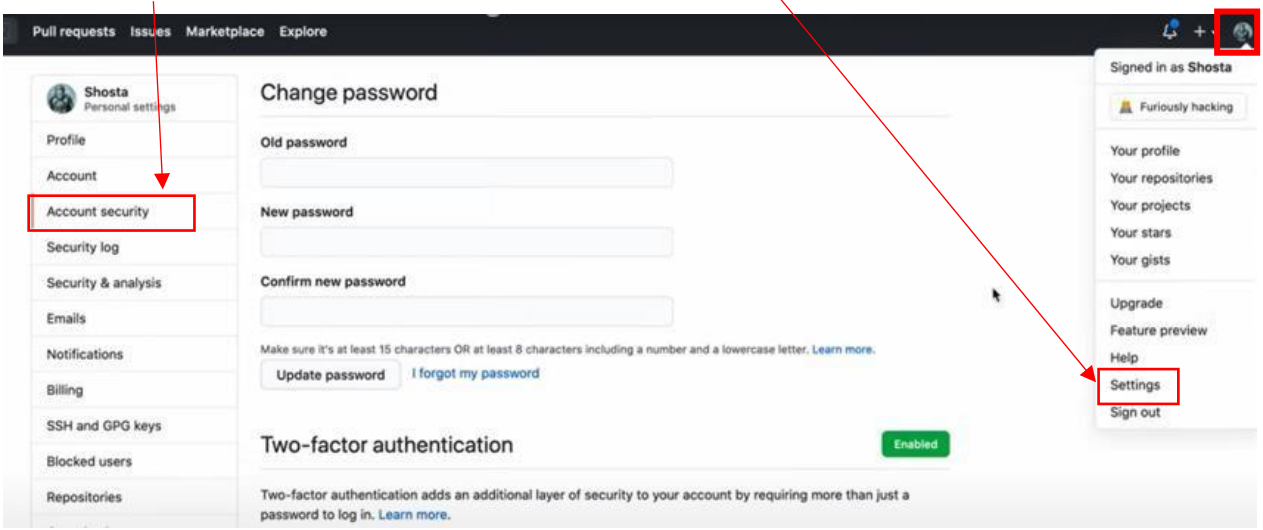


Lorsque l'utilisateur final se connecte, il doit insérer la YubiKey correcte dans un port USB de son système. Si l'utilisateur final saisit son nom d'utilisateur et son mot de passe sans insérer la YubiKey correcte, l'authentification échouera et l'utilisateur recevra un message d'erreur tel que celui illustré dans la capture d'écran suivante :

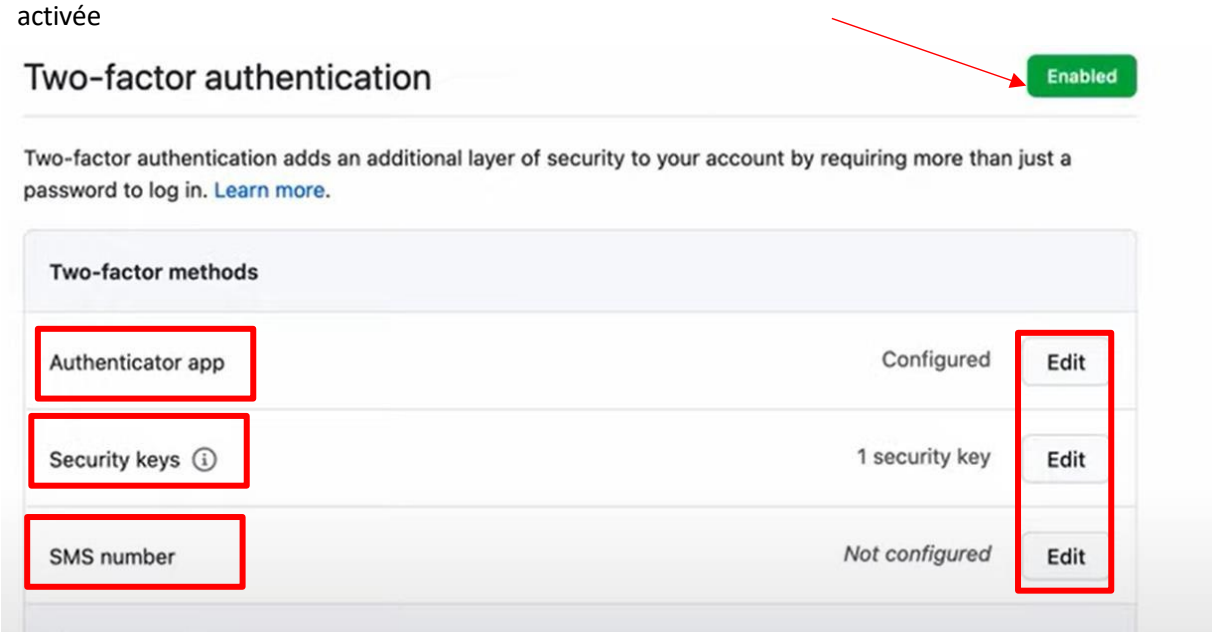


1.1 Activation du système de double authentification :

Connectez-vous sur l'application puis rendez-vous dans les settings (paramètres), puis cliquez sur account security



Ensuite il faudra activer le mode double authentification en cliquant ici si la case n'est pas déjà activée



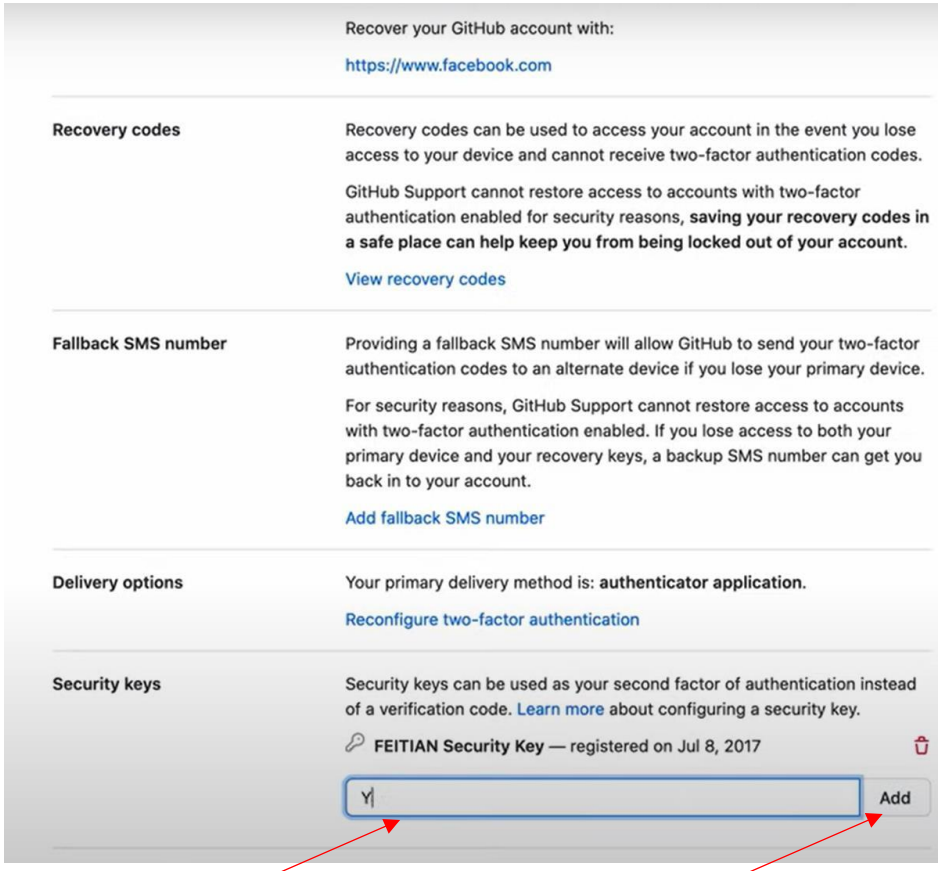
Puis en fonction du type de double authentification que vous voulez cliquez sur l'un des 3 modes pour
pouvoir ajouter une clé.

1. Authenticator app :

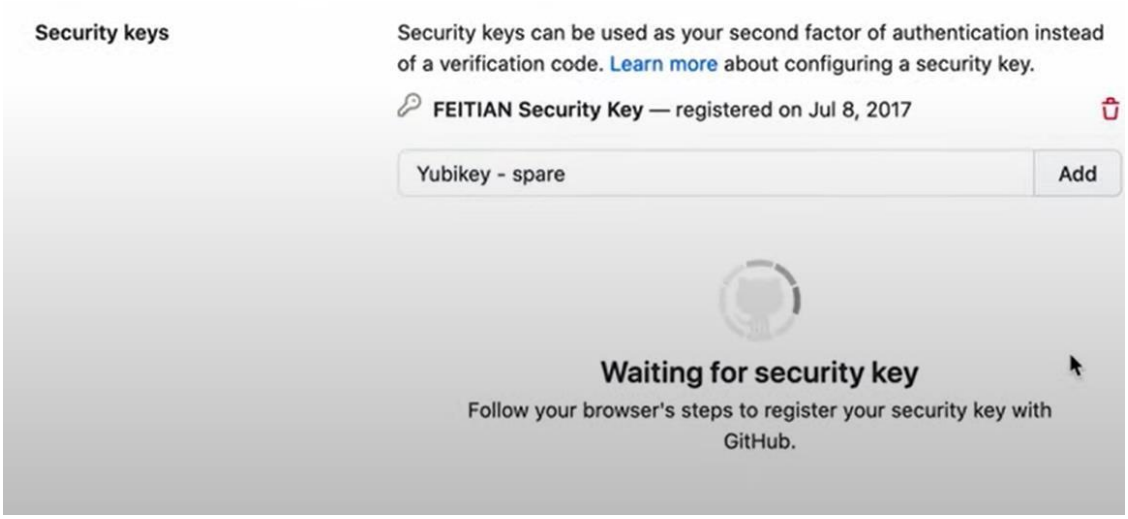
Correspond à une application d'authentification que l'on a sur son smartphone par exemple google authenticator. A ce moment, en cliquant sur Edit un QR code va s'afficher, il faudra le scanner avec votre smartphone pour pouvoir ajouter une clé.

1. Security keys :

Correspond à la configuration d'une nouvelle clé USB.



Vous lui attribuez un nom ici puis cliqué sur add



Ensuite, l'ordinateur va rechercher si une clé est connectée au poste. C'est à ce moment où il vous faudra brancher la clé que vous voulez ajouter.

Puis vous devrez cliquer sur le bouton se trouvant sur la clé en question

Comme vous pouvez le voir, la clé a bien été ajoutée. Vous pouvez la déconnecter de l'ordinateur.

Pour supprimer la clé il, vous suffira juste de cliquer sur l'icône de la poubelle

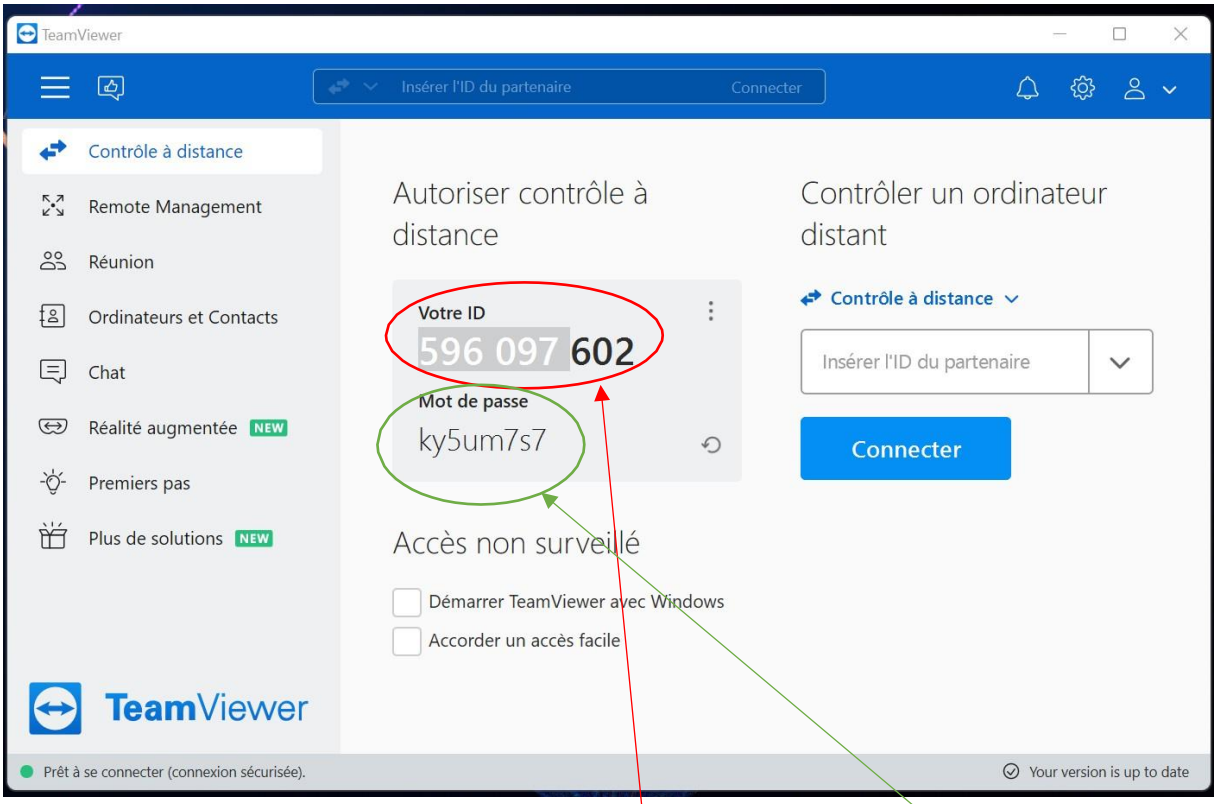
1. SMS number :

Concernant la 3ème option il vous suffit de cliquer sur edit puis d'enregistrer votre numéro de téléphone pour qu'au moment de la connexion le logiciel vous envoie un SMS avec un mot de passe unique qui généralement est valable durant une courte durée.

1 Assistance client via TeamViewer :

En cas d'incident, ou de demande de service après nous avoir joint via téléphone nous vous demanderons d'ouvrir sur votre bureau le logiciel TeamViewer en double cliquant dessus :

Après cela, une nouvelle page apparaitra :



Après ça il vous suffira de nous donner votre identifiant ainsi que votre mot de passe à usage unique, cela va nous permettre de prendre