Vade-mecum connexion au bureau virtuel (Université d'Aix-Marseille) V1.1.1

Document en ligne : www.mickael-martin-nevot.com

1 Généralités

Le bureau virtuel, aussi appeler *Virtual Desktop Infrastructure* (VDI), *Desktop as a Service* (DaaS) ou encore bureau en tant que service ou bureau virtuel hébergé correspond à l'externalisation d'une infrastructure de bureau virtuel auprès d'un fournisseur de services.

L'Université d'Aix-Marseille (AMU) offre un accès à un bureau virtuel, y compris à distance. Ce document présente comment permettre son utilisation.

La configuration présentée doit être réalisée au sein d'une machine connectée à un réseau informatique d'AMU.

2 Activation de l'authentification forte

Connectez-vous à l'environnement numérique de travail (ENT), et exécuter le **service d'authentification forte**, ou d'activation du mfa (pour authentification multifacteurs en anglais).

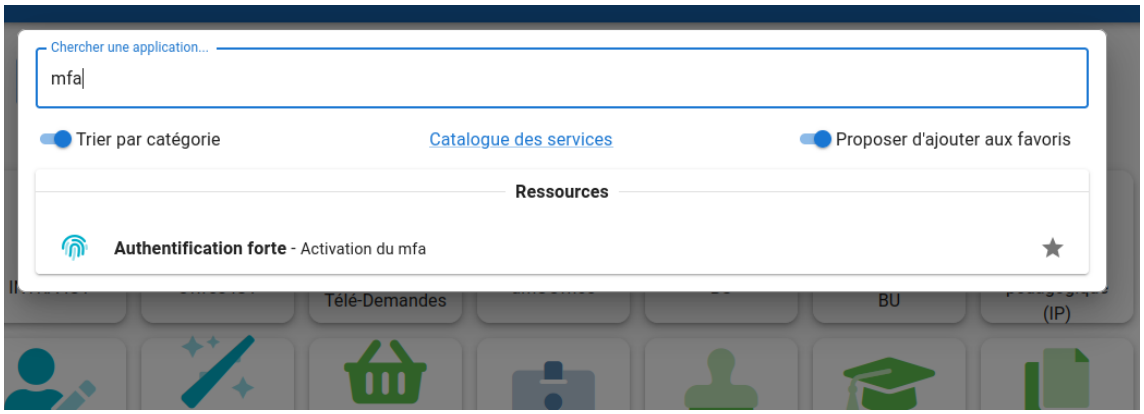

Figure 1 – Authentification forte – Activation du mfa

2.1 Installation de l'extension du navigateur Web

L'exécution du service d'authentification forte ouvre un nouvel onglet proposant une procédure de sécurisation des accès en deux étapes :

1. **Installez l'extension TrustBuilder Backup** sur le navigateur Web, puis certifiez l'avoir fait en cochant la case à cocher correspondante.
2. **Activez votre navigateur Web** (cela fonctionnera aussi avec d'autres une fois toute la procédure terminée avec succès) avec TrustBuilder, en fournissant une phrase de vérification de la légitimité de votre authentification, un code PIN et en cliquant sur `Valider`.

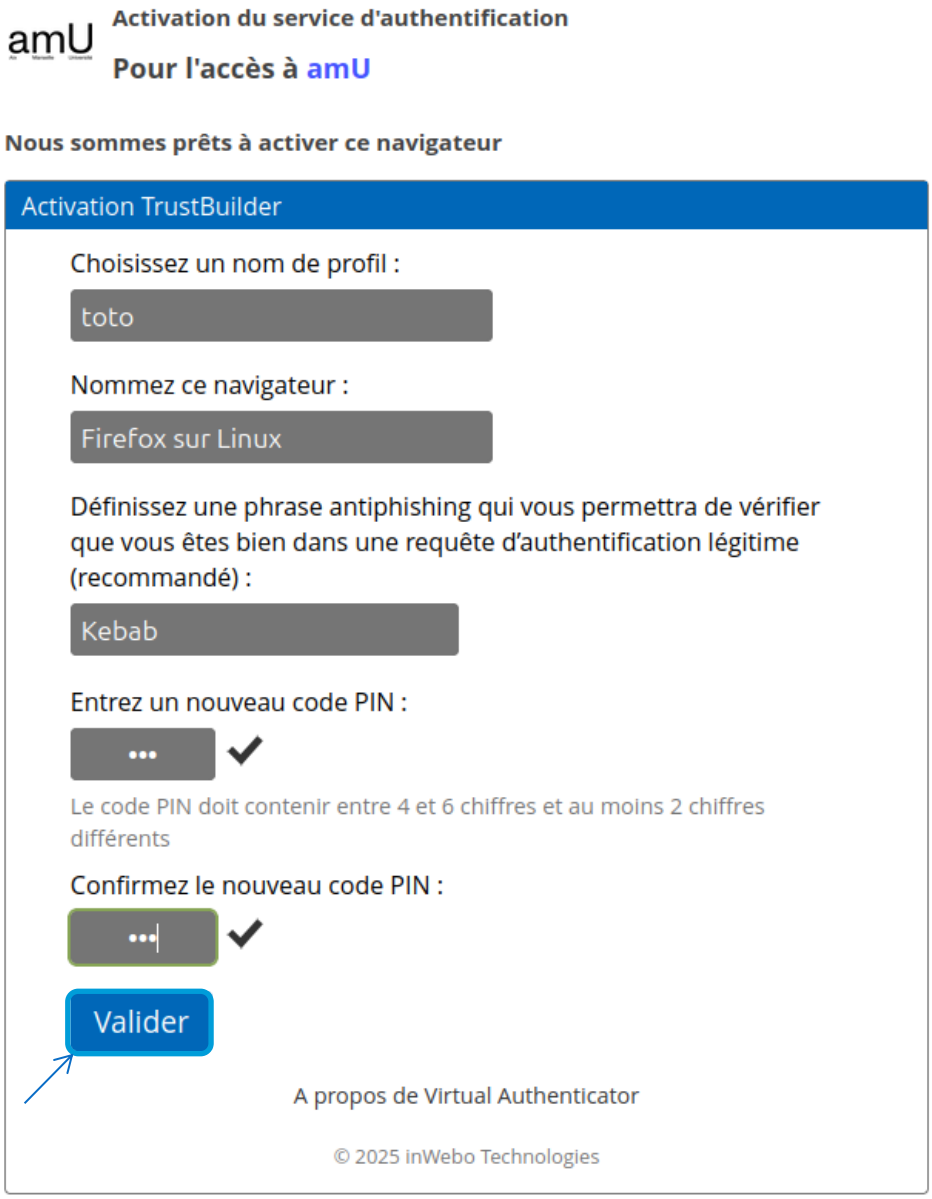

Figure 2 – Activation (de Virtual Authenticator) de TrustBuilder

Vous devez alors obtenir une confirmation d'activation du navigateur Web.

Cliquez alors sur `Activer Authenticator`.

Figure 3 – Confirmation de l'activation du navigateur

2.2 Installation de l'application mobile

Téléchargez et **installer l'application TrustBuilder** ou inWebo Authenticator sur votre *smartphone* possédant un système d'exploitation Android ou iOS.

Lancez l'application et **scannez le code QR** ou saisissez le code d'activation affiché sur la page Web de l'Authenticator.

Cliquez alors sur `J'ai terminé`.

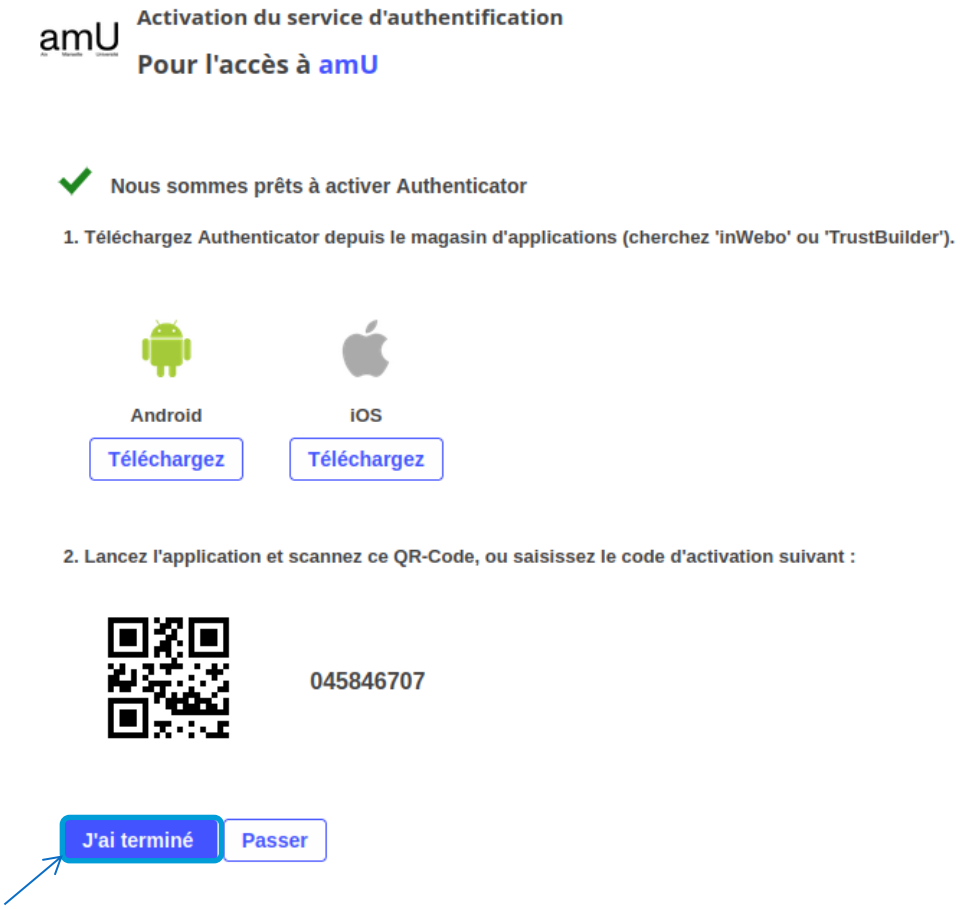

Figure 4 – Activation du service d'authentification à l'aide d'une application mobile

3 Accéder au bureau virtuel

3.1 Portail d'authentification

Après avoir vérifié l'activation de votre authentification forte, accédez au **portail d'authentification** d'AMU avec l'URL (n'utilisez pas les sites sécurisés proposés par défaut) : https://labtech.univ-amu.fr/portal/webclient.

Cliquez sur `Autres options de connexion`.

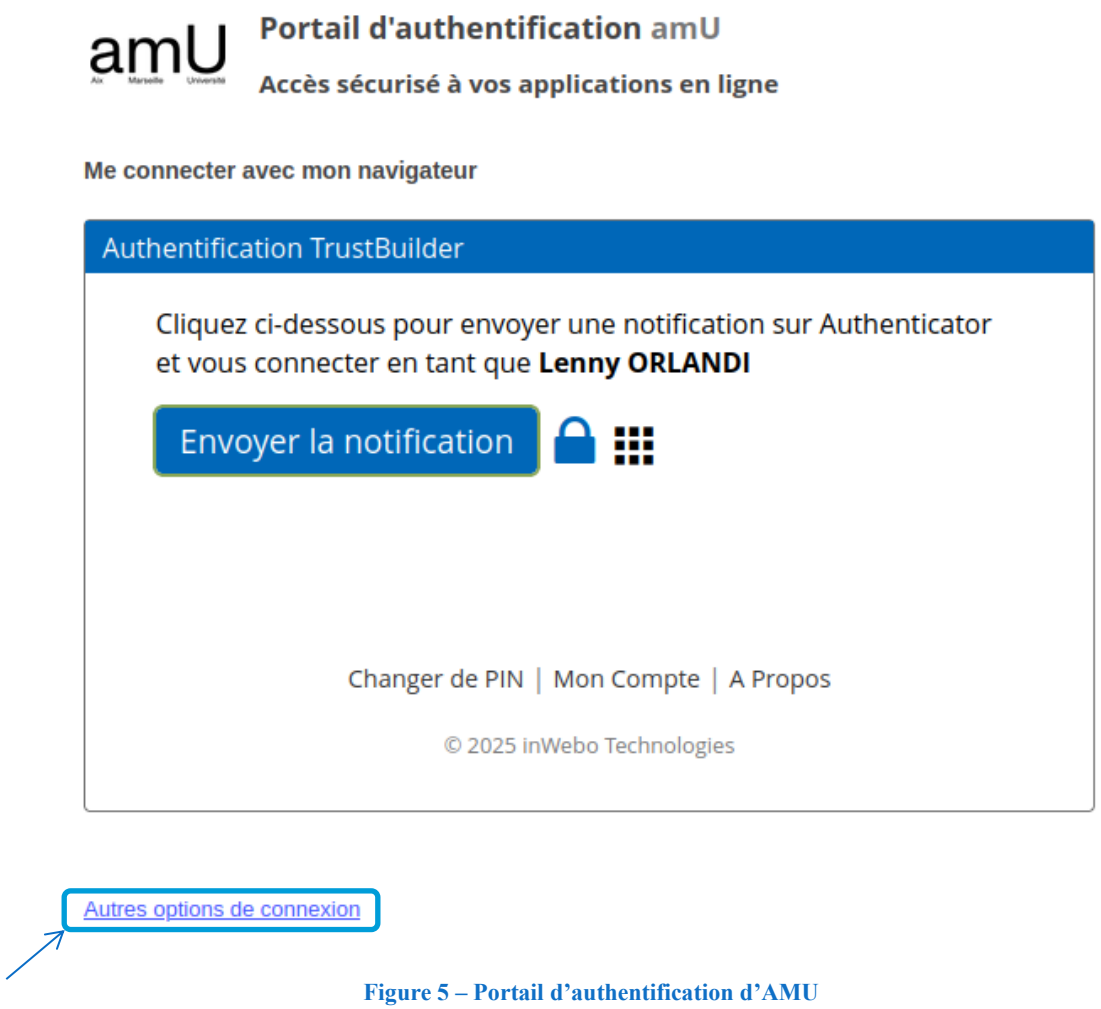

Figure 5 – Portail d'authentification d'AMU

Connectez-vous ensuite en saisissant un **code à usage unique (OTP)** généré par l'application Authenticator de votre *smartphone* (après avoir vérifié que votre identifiant était bien renseigné) et en cliquant sur `OK`.

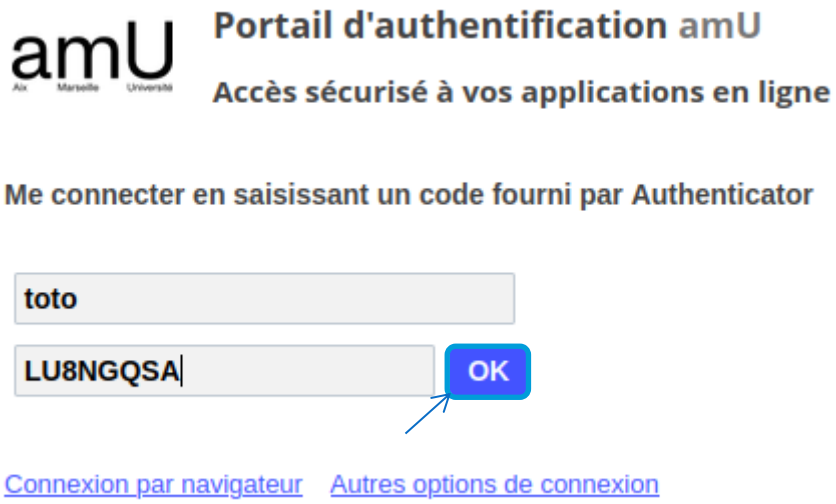

Figure 6 – Connexion au portail d'authentification d'AMU par code à usage unique (OTP)

3.2 Lancement du bureau virtuel

Connectez-vous à votre **compte numérique AMU** avec votre nom d'utilisateur et votre mot de passe (en utilisant le domaine SALSA) en cliquant sur `Connexion`.

Figure 7 – Connexion numérique AMU

3.3 Choix de l'infrastructure

Il ne vous reste plus qu'à cliquer sur **l'infrastructure Horizon** de votre choix. De manière générale, `LUNIX (Linux pour TOUS)` est conseillé.

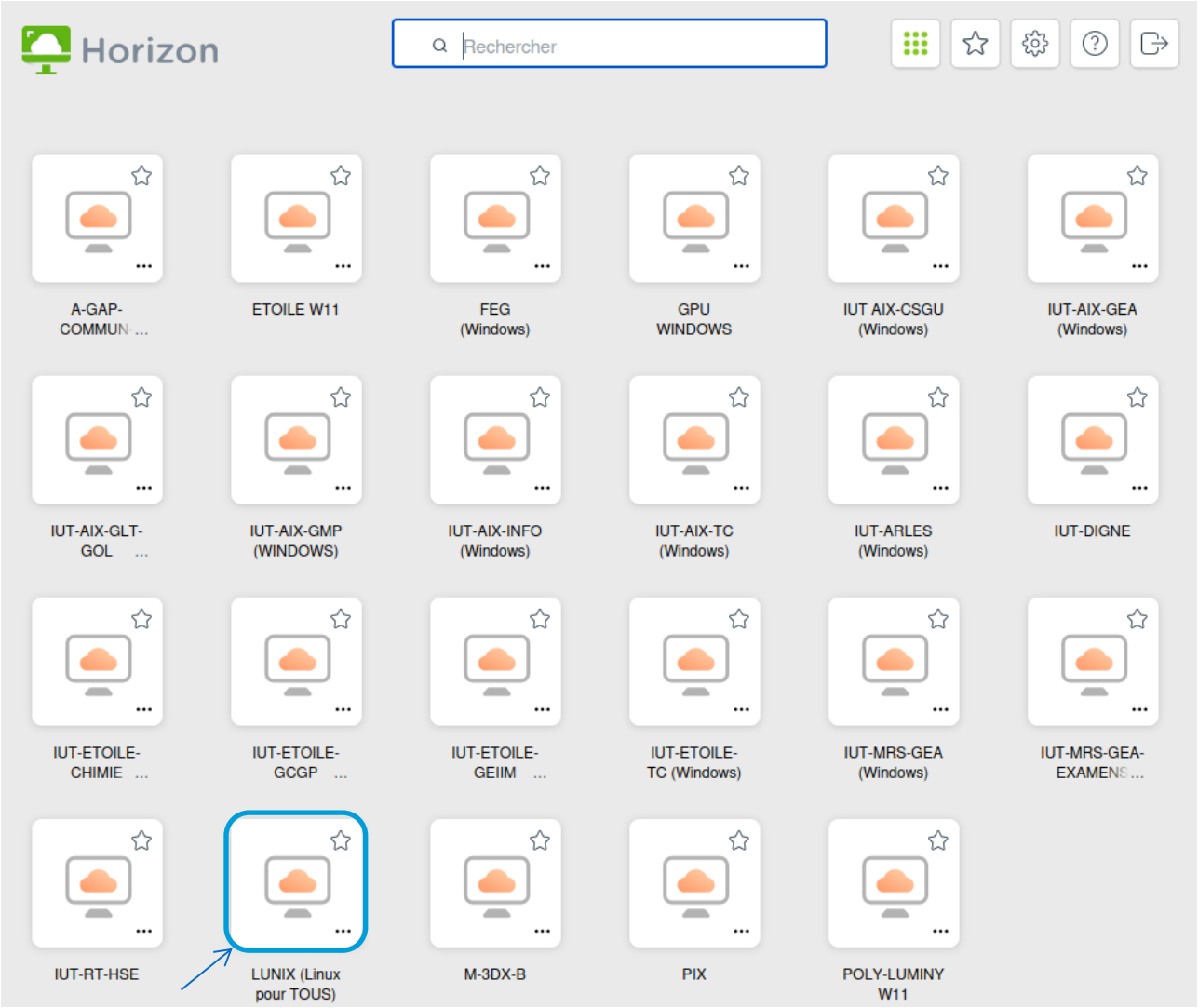

Figure 8 – Choix de l'infrastructure Horizon

4 En savoir plus

Une page d'accompagnement dédiée est disponible dans la documentation utilisateur dynamique **(DUD)**, accessible via l'environnement numérique de travail (ENT) d'AMU.

Vous y trouverez :

- des informations plus détaillées sur le fonctionnement de l'authentification forte ou l'accès au bureau virtuel ;
- une foire aux questions (FAQ) et les contacts utiles en cas de besoin.

Figure 9 – Documentation utilisateur dynamique d'AMU

Pour y accéder, cliquez sur **Authentification forte pour le VDI**.

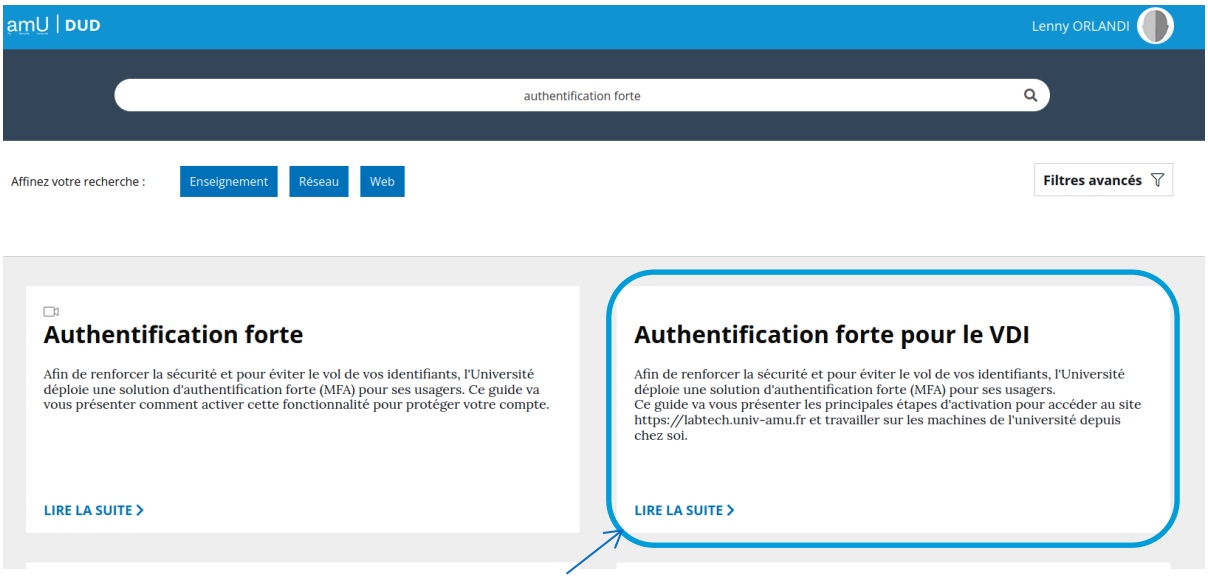

Figure 10 – Authentification forte pour le VDI