Fondation Mérieux

LabBook

LabBook v3.6

Sécurisation du serveur

Comptes système, HTTPS, certificats et base de données

V3.1

Octobre 2026

Table des matières

1. À qui s'adresse ce guide....3
2. Changer le mot de passe de user_labbook....4
3. Passer LabBook en HTTPS....6
3.1 Générer le certificat sur le serveur....6
3.2 Installer le certificat dans Firefox (serveur Ubuntu)....7
3.3 Installer le certificat sur un poste Windows....11
3.4 Installer le certificat sur Android (LabBook Lite)....17
4. Changer l'utilisateur et le mot de passe MySQL....21
5. Autres bonnes pratiques de sécurité....23
6. Dépannage....24
Annexe — Historique du document....25

1. À qui s'adresse ce guide

Ce guide décrit les opérations de **sécurisation** à réaliser juste après l'installation du serveur (guide E1).

Public	Responsable informatique du laboratoire
Prérequis	Serveur LabBook installé ; accès à la console du serveur avec le compte administrateur système (`sigl` par défaut)
Durée	Environ 30 minutes, plus 5 minutes par poste client pour le certificat

Les quatre mesures de ce guide :

Mesure	Pourquoi	§
Changer le mot de passe de `user_labbook`	Ce compte donne accès aux supports de sauvegarde ; son mot de passe d'origine est connu de tous	2
Passer LabBook en **HTTPS**	Chiffrer les échanges entre les postes et le serveur (mots de passe, résultats)	3
Installer le **certificat** sur les postes et les tablettes	Supprimer l'alerte « connexion non sécurisée », obligatoire pour LabBook Lite	3.2 à 3.4
Changer l'utilisateur **MySQL**	Remplacer le compte par défaut `root` / `root` de la base de données	4

À savoir — les différents comptes Ne les confondez pas :

- `sigl` : administrateur du **système Ubuntu**, créé à l'installation.
- `user_labbook` : compte système qui donne accès aux **supports USB de sauvegarde**.
- `root` : administrateur de **l'application LabBook** (guide D1).
- le compte **MySQL** : utilisé par LabBook pour accéder à la base de données.

2. Changer le mot de passe de `user_labbook`

L'installation crée l'utilisateur système `user_labbook`, avec le mot de passe `user_labbook`. Ce compte permet d'accéder aux supports de sauvegarde branchés sur le serveur. Son mot de passe **doit être changé à la première connexion**.

1. Sur la console du serveur, connectez-vous en tant que `user_labbook`.
2. Saisissez le mot de passe actuel : `user_labbook`.
3. Saisissez une seconde fois le mot de passe actuel : `user_labbook.`
4. Saisissez le nouveau mot de passe, puis confirmez-le.

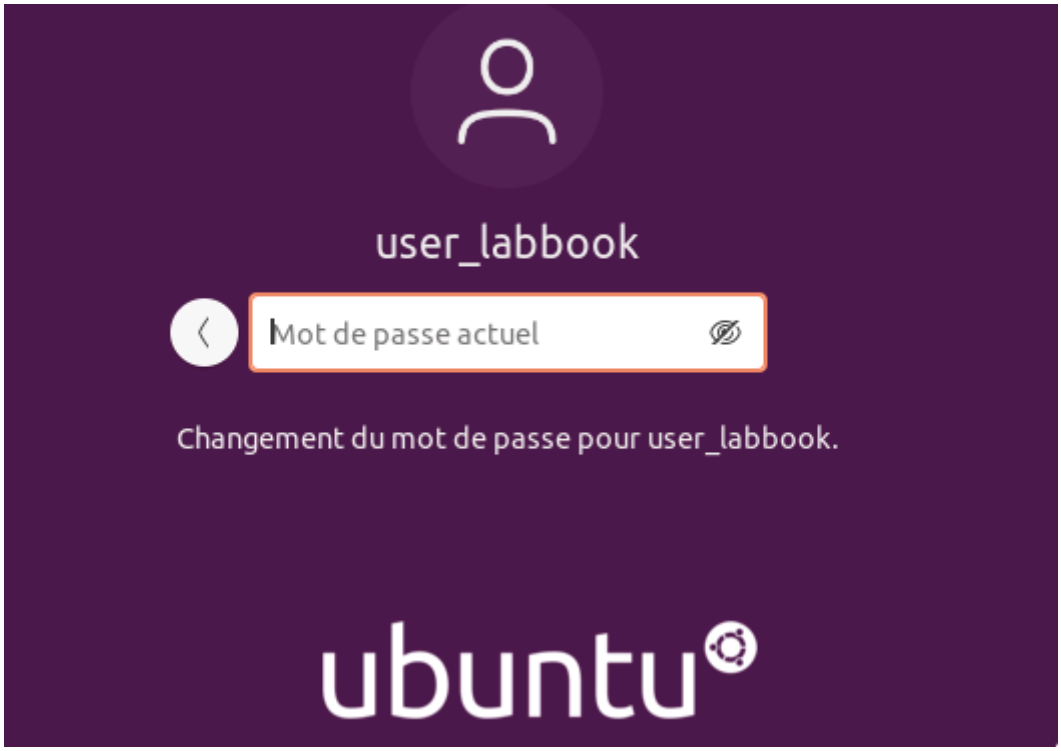

Figure 1 – Saisie du mot de passe actuel

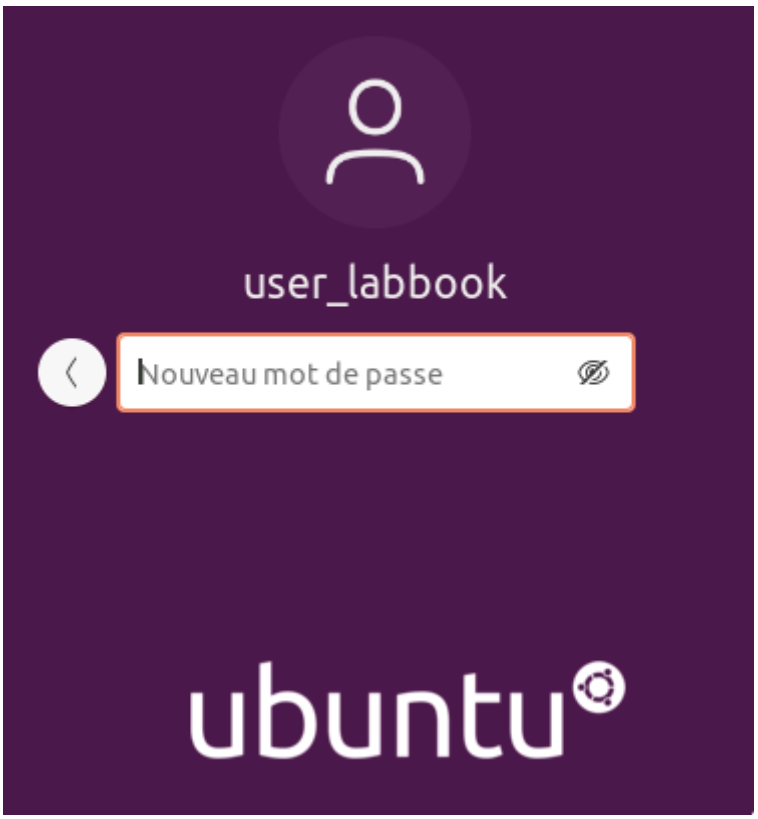

Figure 2 – Saisie du nouveau mot de passe

Attention : ce mot de passe est demandé pour **chaque action de sauvegarde ou de restauration** (guide E4). Notez-le dans le coffre-fort des mots de passe du laboratoire.

3. Passer LabBook en HTTPS

Par défaut, LabBook communique en **HTTP** : les échanges circulent en clair sur le réseau. En **HTTPS**, ils sont chiffrés. Le serveur LabBook joue alors le rôle d'**autorité de certification locale** (`LabBookLocalRootCA`).

3.1 Générer le certificat sur le serveur

Avant de commencer, fixez l'adresse IP du serveur (guide E3). Le certificat est lié à cette adresse : si elle change, il faut le régénérer.

1. Ouvrez un terminal sur le serveur et connectez-vous avec l'administrateur système (`sigl` par défaut).
2. Repérez l'adresse IP du serveur avec la commande `ifconfig`. Elle est en général de la forme `192.168.X.Y` ou `10.10.X.Y`.
3. Lancez le script :

```
sudo /home/util/https_labbook.sh localstore
```

4. Quand le script le demande, saisissez **l'adresse IP du serveur** sur le réseau local, par exemple `192.168.1.10`.

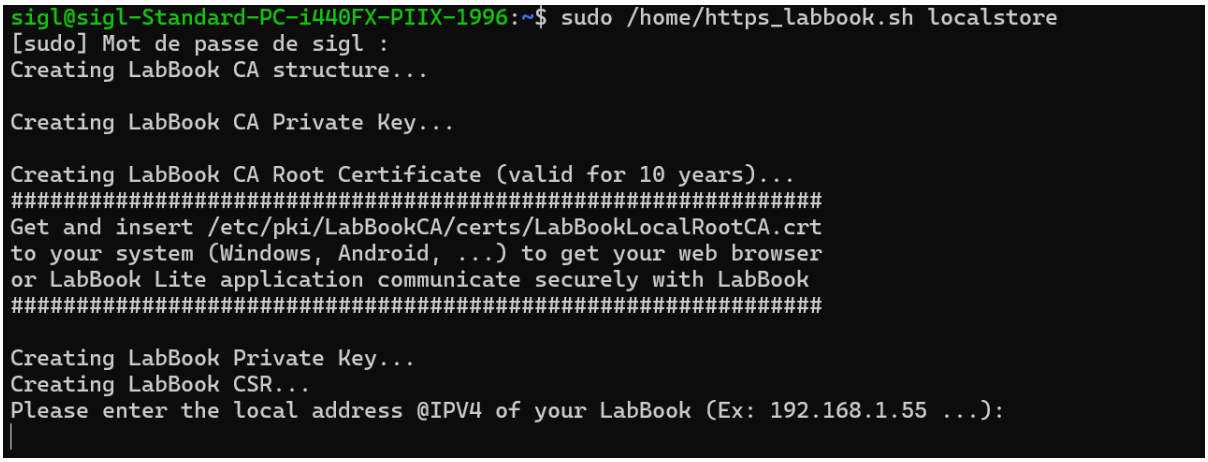

Figure 3 – Exécution du script https_labbook.sh

Attention — adresses à ne pas utiliser :

- `10.88.0.1` est réservée aux conteneurs ;
- `127.0.1.1` est l'adresse locale de la machine.

LabBook est ensuite accessible en `https://<adresse_IP>/sigl` (ex. `https://192.168.1.10/sigl`). Le fichier `LabBookLocalRootCA.crt` doit maintenant être installé **sur chaque navigateur ou appareil** qui accède à LabBook.

3.2 Installer le certificat dans Firefox (serveur Ubuntu)

1. Ouvrez LabBook dans Firefox. L'alerte *Warning: Potential Security Risk Ahead* s'affiche : c'est normal tant que le certificat n'est pas installé.
2. Cliquez sur **Advanced**, puis sur **View Certificate**.

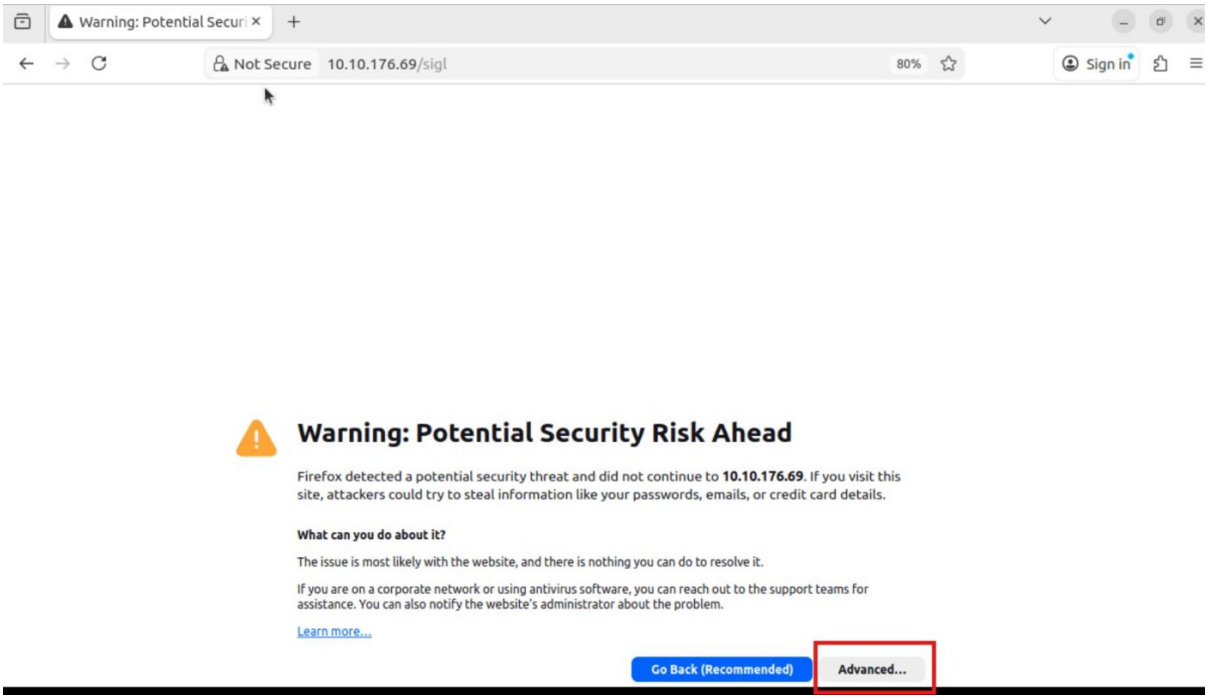

Figure 4 – Alerte de sécurité dans Firefox

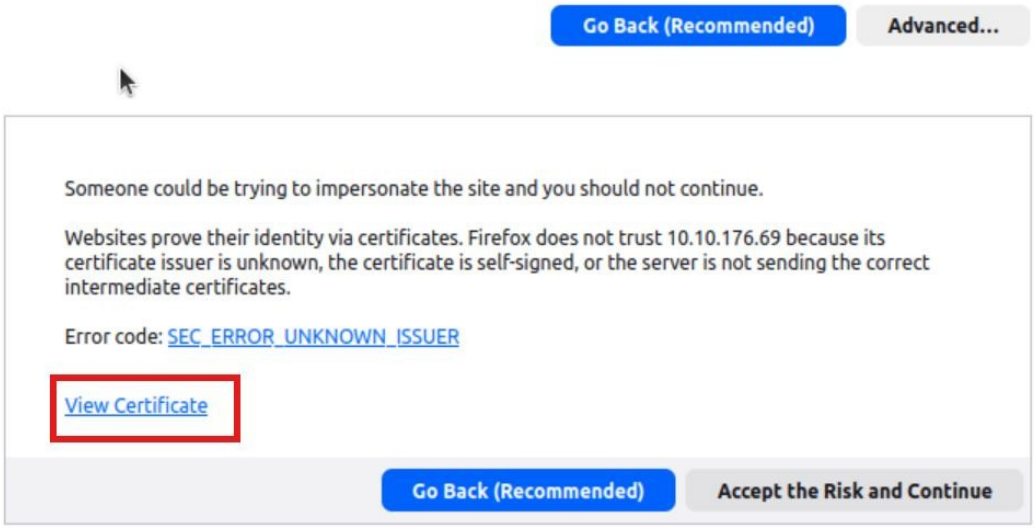

Figure 5 – Lien « View Certificate »

3. La page *Certificate* comporte deux onglets : l'adresse IP et **LabBookLocalRootCA**. Ouvrez l'onglet **LabBookLocalRootCA**.
4. Cliquez sur **PEM (cert)** pour télécharger le certificat.

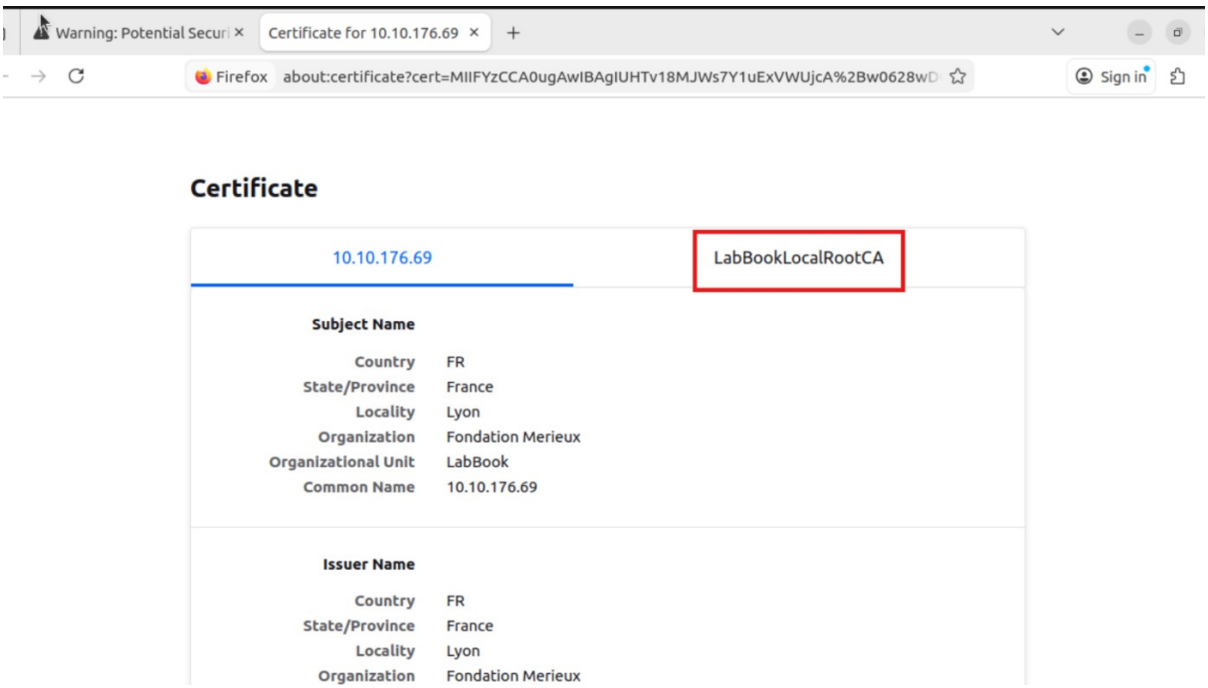

Figure 6 – Onglet LabBookLocalRootCA

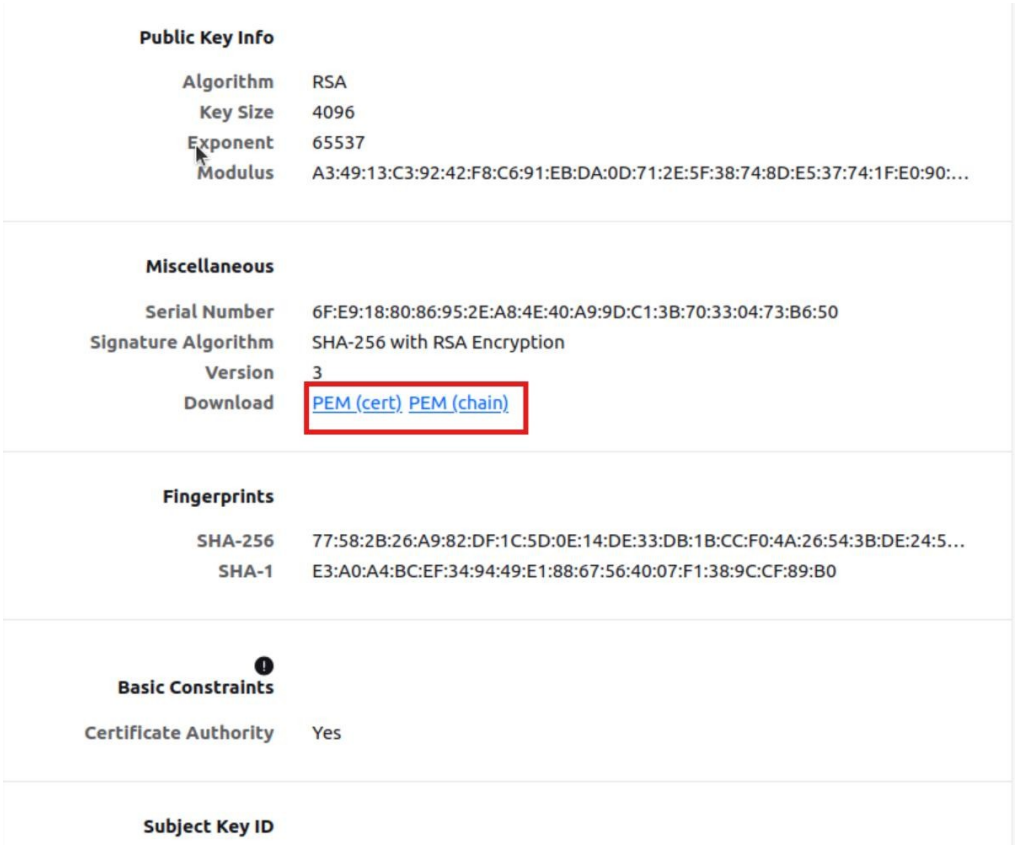

Figure 7 – Téléchargement au format PEM

5. Ouvrez les **Paramètres** de Firefox et tapez « certificat » dans la recherche. Cliquez sur **Afficher les certificats**.

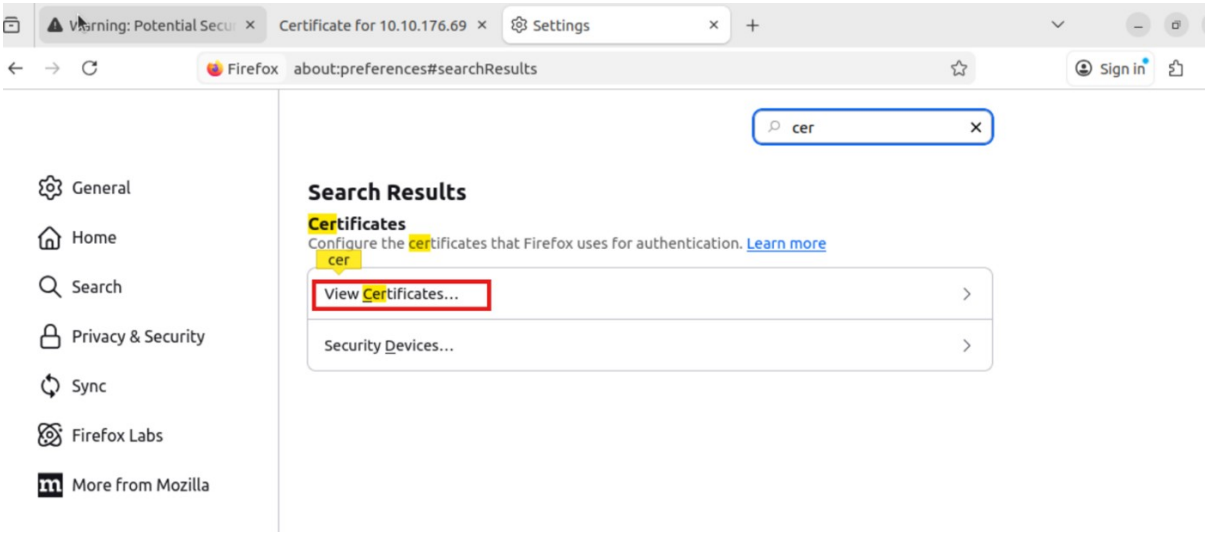

Figure 8 – Recherche « certificat » dans les paramètres

6. Dans l'onglet **Autorités**, cliquez sur **Importer** et sélectionnez le fichier téléchargé.
7. Cochez **Confirmer cette AC pour identifier des sites web** (*Trust this CA to identify websites*), puis **OK**.

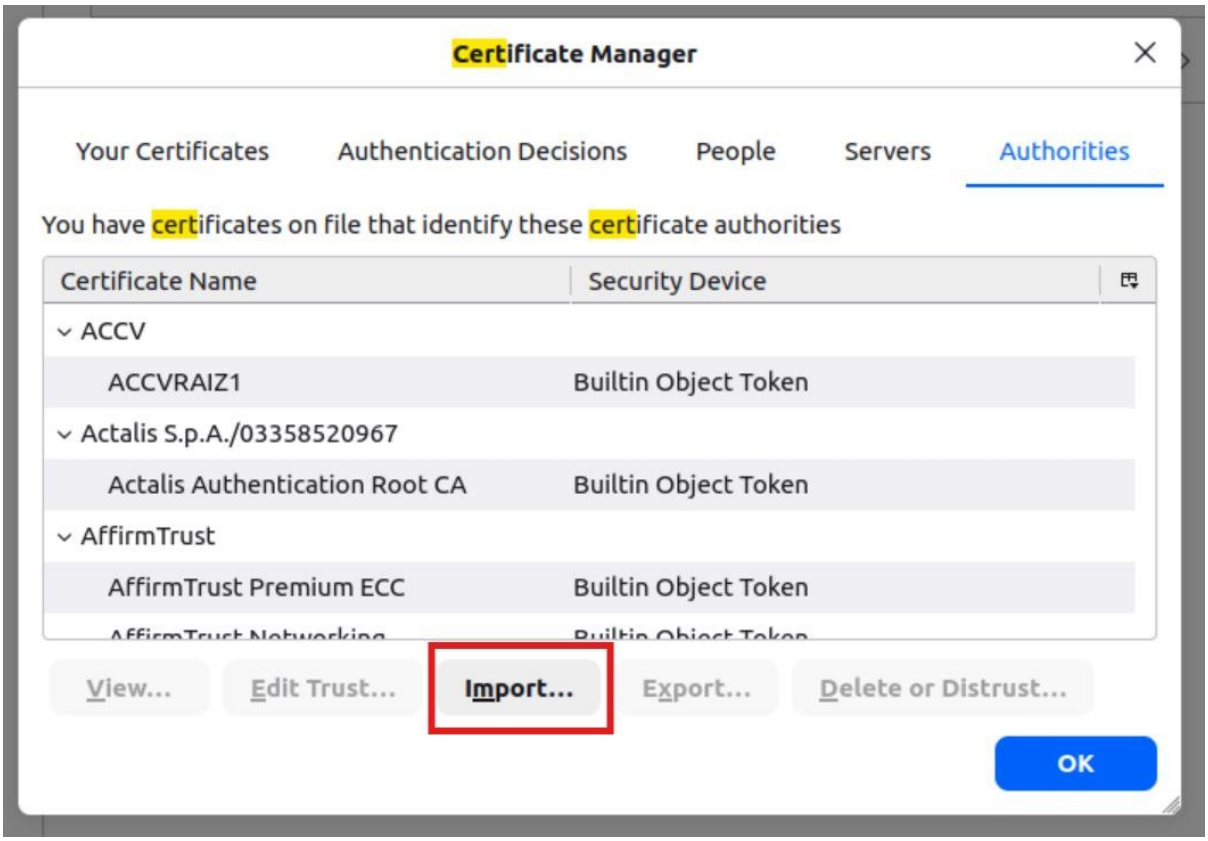

Figure 9 – Importer le certificat

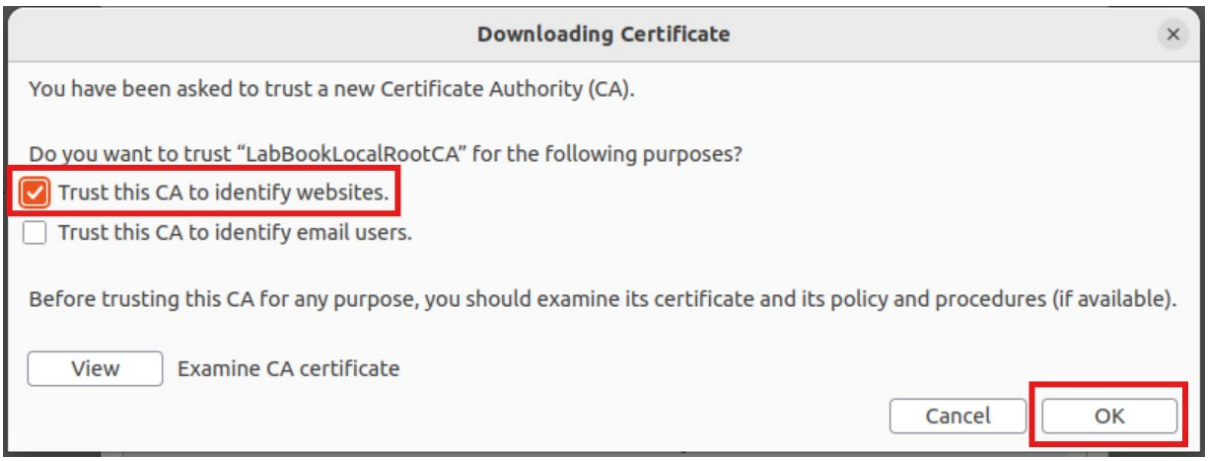

Figure 10 – Confiance accordée pour les sites web

8. Vérifiez que **LabBookLocalRootCA** apparaît sous *Fondation Mérieux*. Rechargez LabBook : un **cadenas** remplace l'alerte.

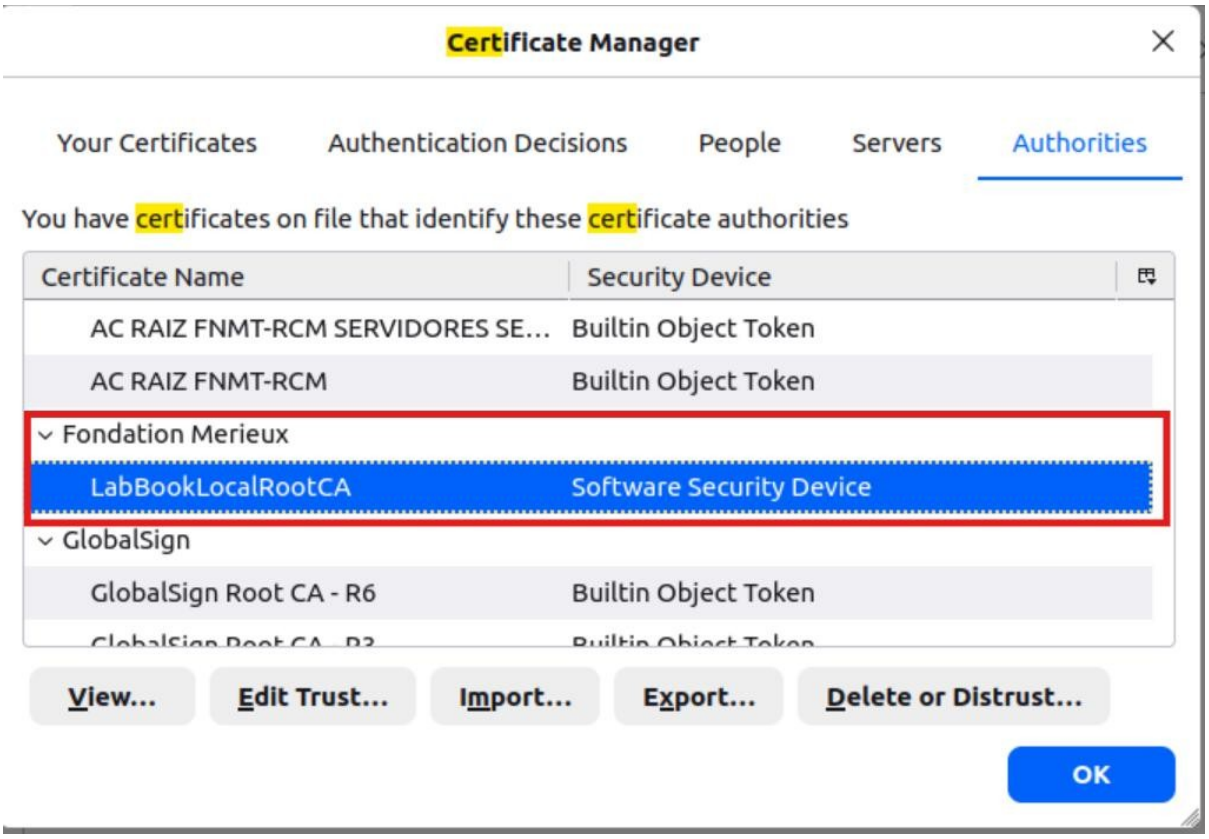

Figure 11 – Certificat ajouté

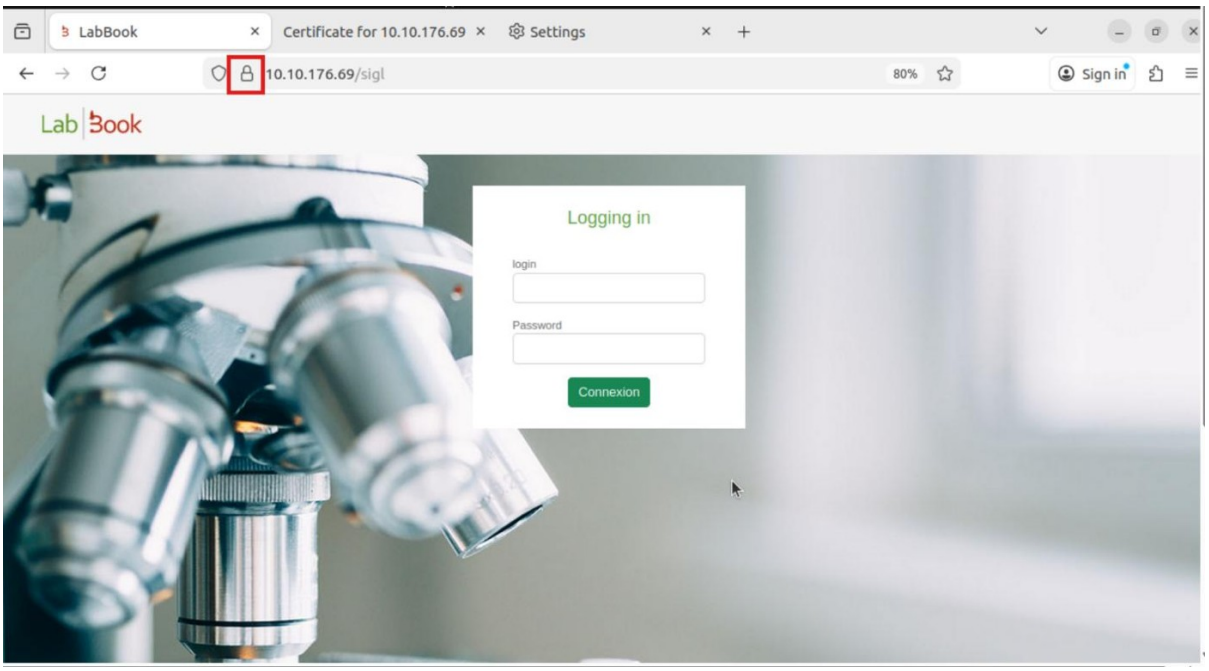

Figure 12 – Connexion sécurisée (cadenas)

3.3 Installer le certificat sur un poste Windows

Cette procédure installe le certificat **pour tout le système Windows** : Chrome et Edge l'utilisent automatiquement.

1. Copiez le fichier `LabBookLocalRootCA.crt` du serveur vers le poste, par exemple avec une clé USB.
2. Avant l'installation, Chrome affiche *Votre connexion n'est pas privée*.

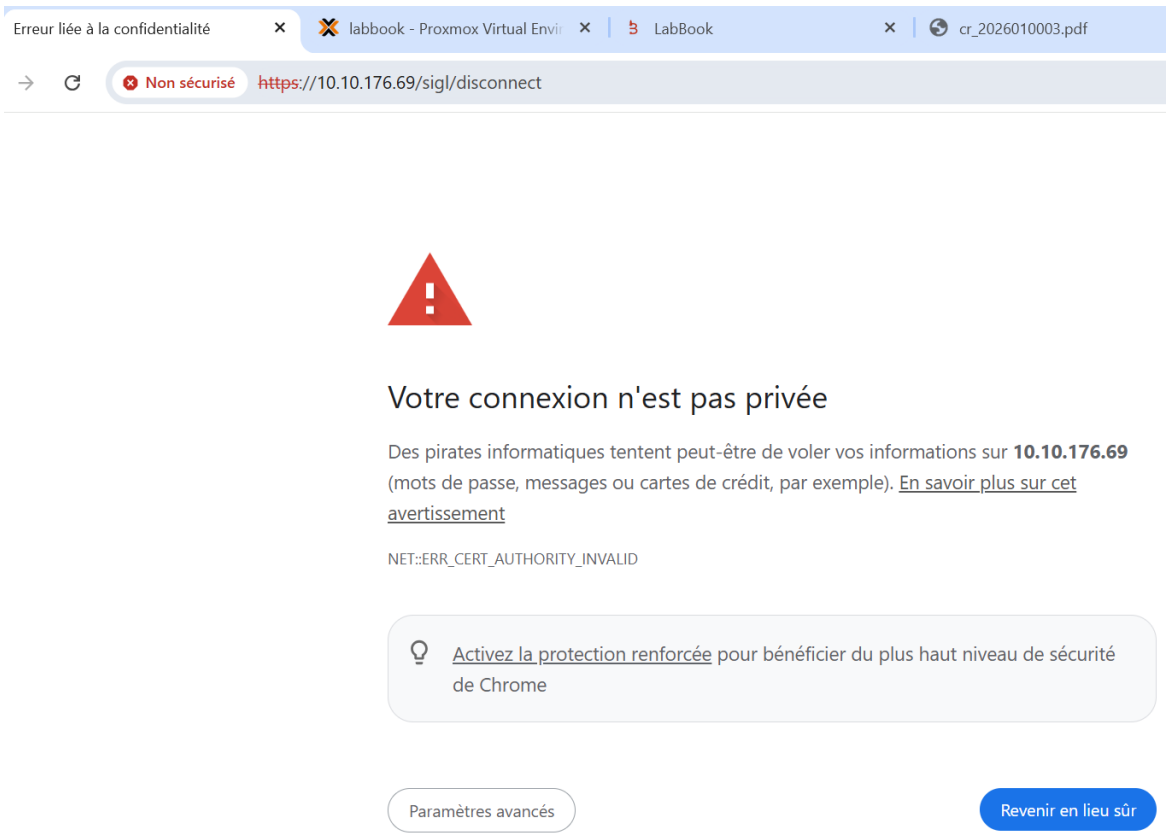

Figure 13 – Alerte avant installation du certificat

3. Double-cliquez sur le fichier `.crt`, puis cliquez sur **Installer un certificat**.

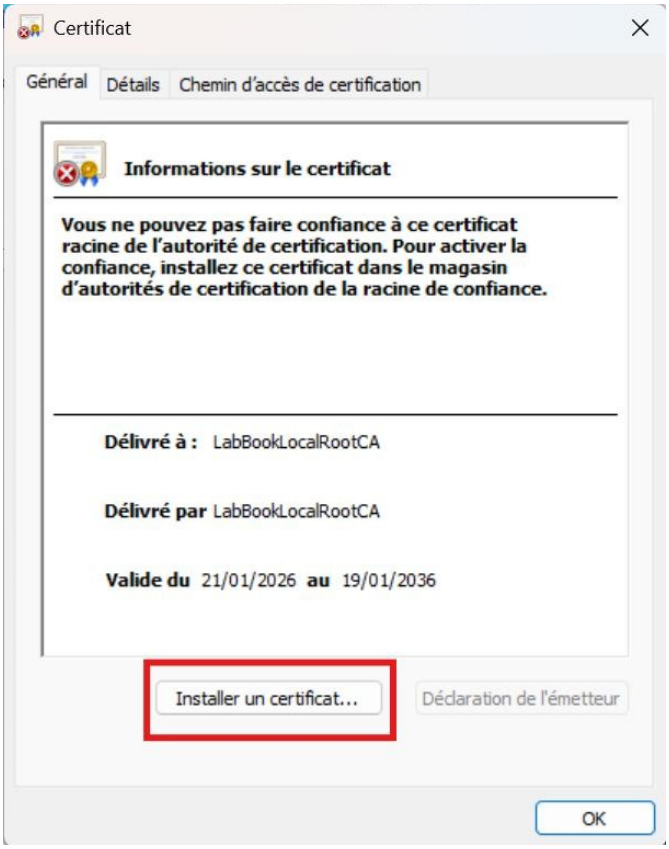

Figure 14 – Fenêtre du certificat

4. Choisissez **Ordinateur local**, puis **Suivant**.

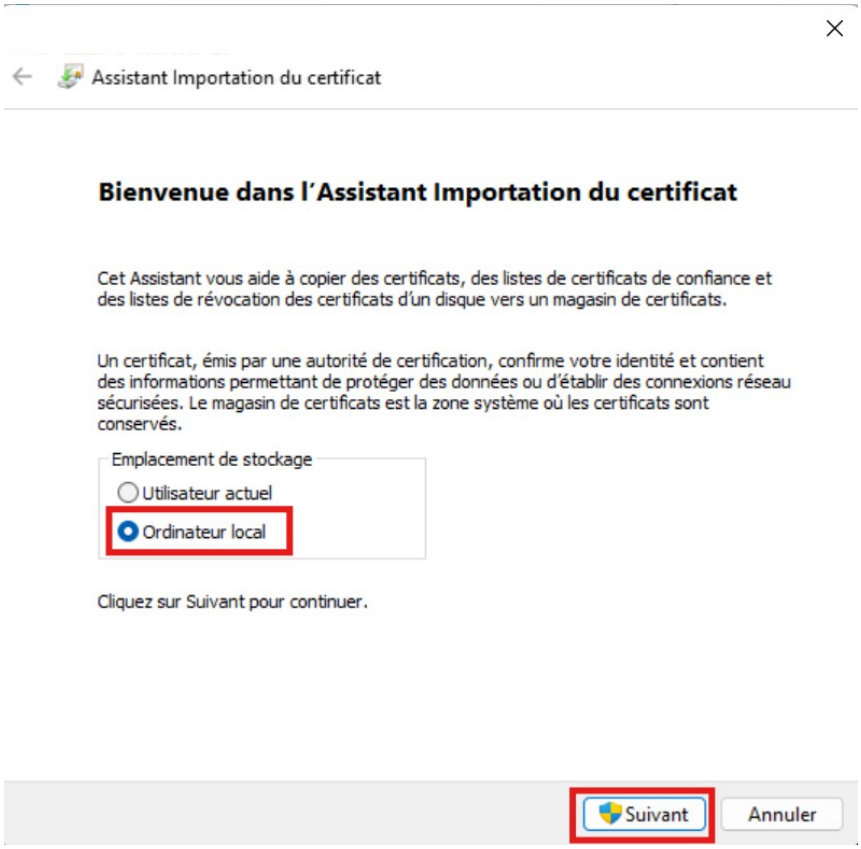

Figure 15 – Emplacement : Ordinateur local

5. Choisissez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur **Parcourir**.

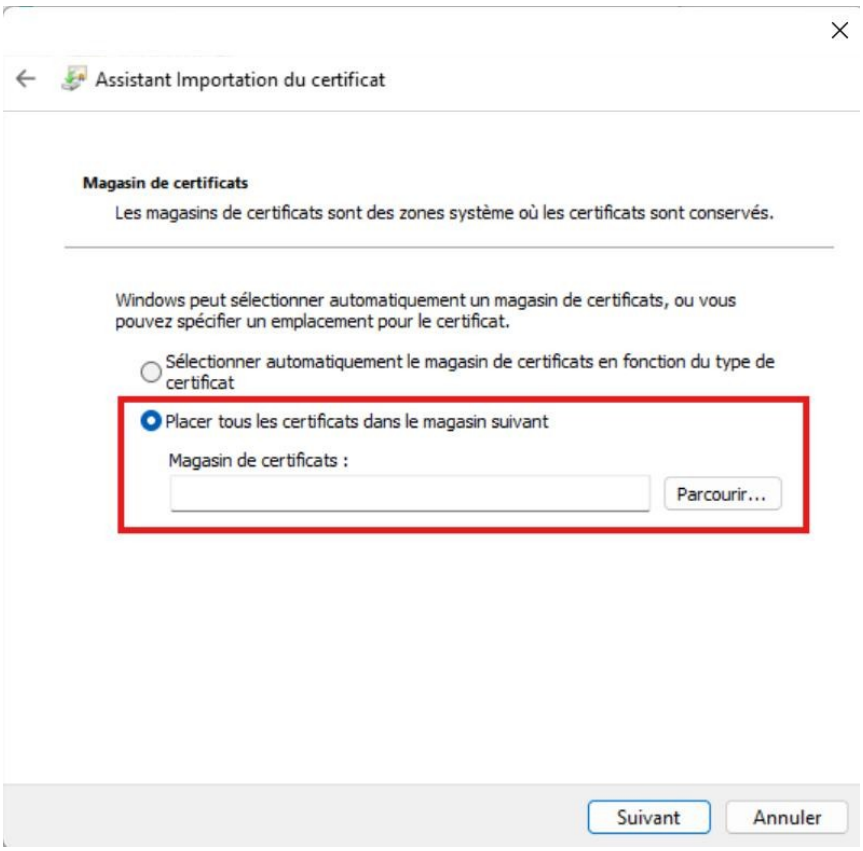

Figure 16 – Choisir le magasin

6. Sélectionnez **Autorités de certification racines de confiance**, puis **OK** et **Suivant**.

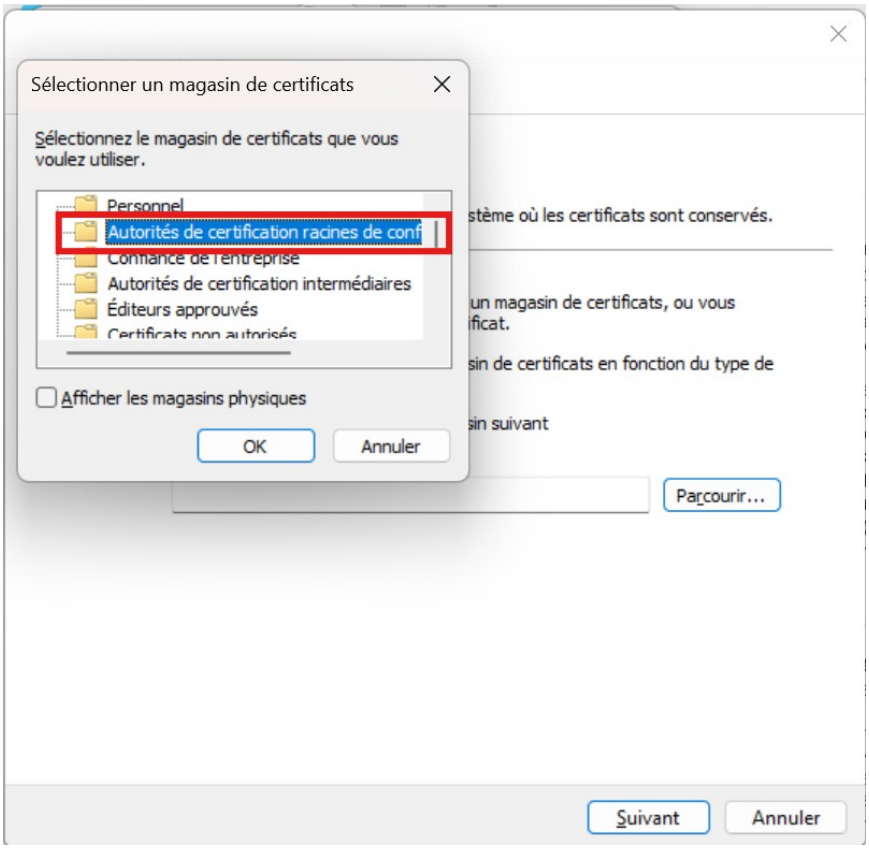

Figure 17 – Magasin « Autorités de certification racines de confiance »

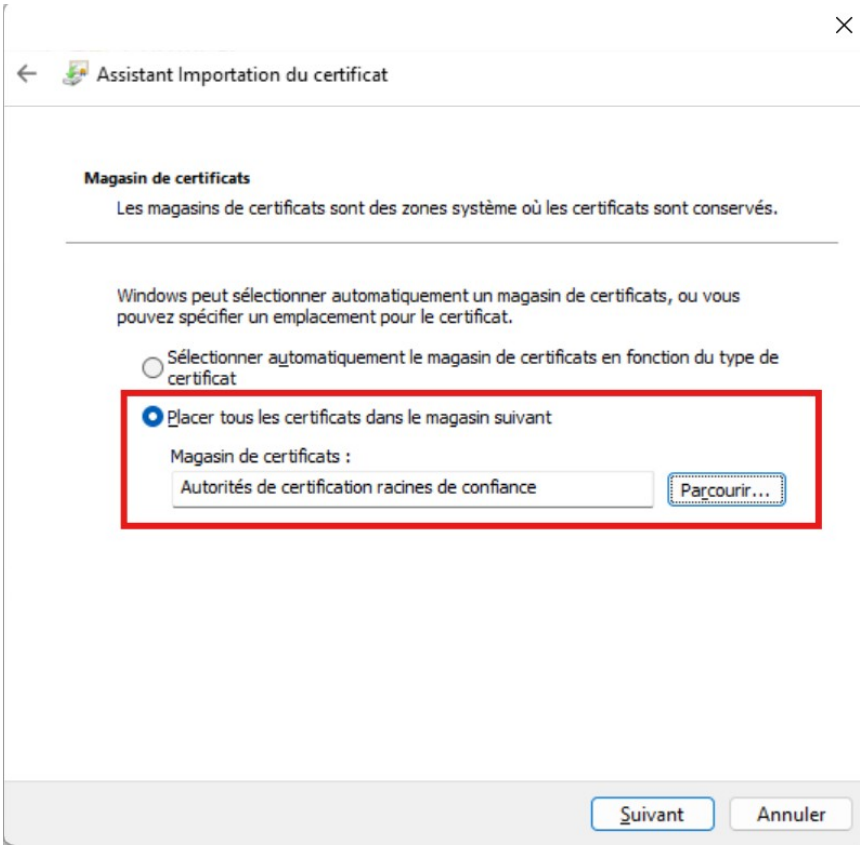

Figure 18 – Magasin sélectionné

7. Cliquez sur **Terminer**. Un message confirme que l'importation a réussi.

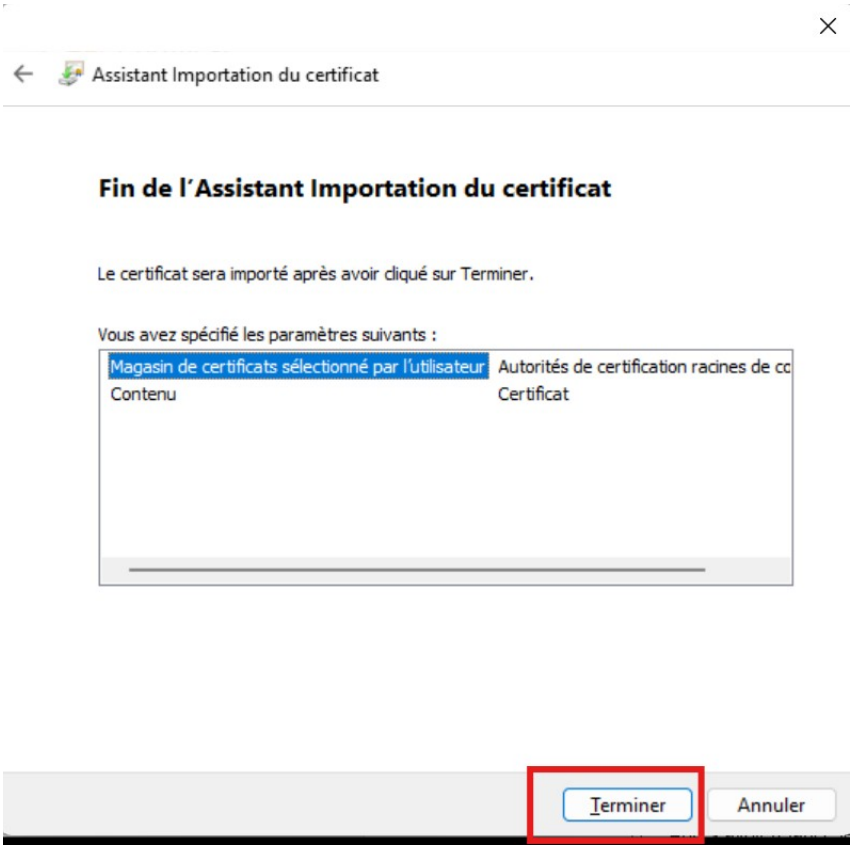

Figure 19 – Fin de l'assistant

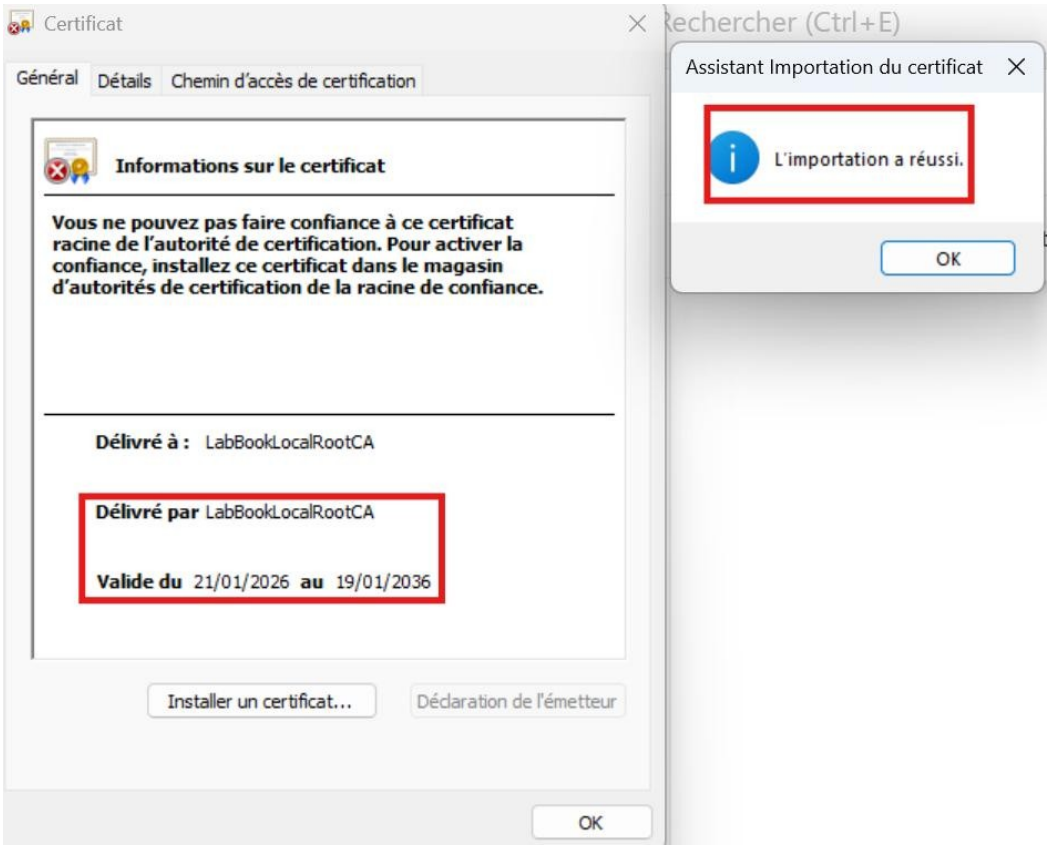

Figure 20 – Importation réussie

8. Relancez le navigateur et ouvrez LabBook en `https://`. Le message de sécurité a disparu.

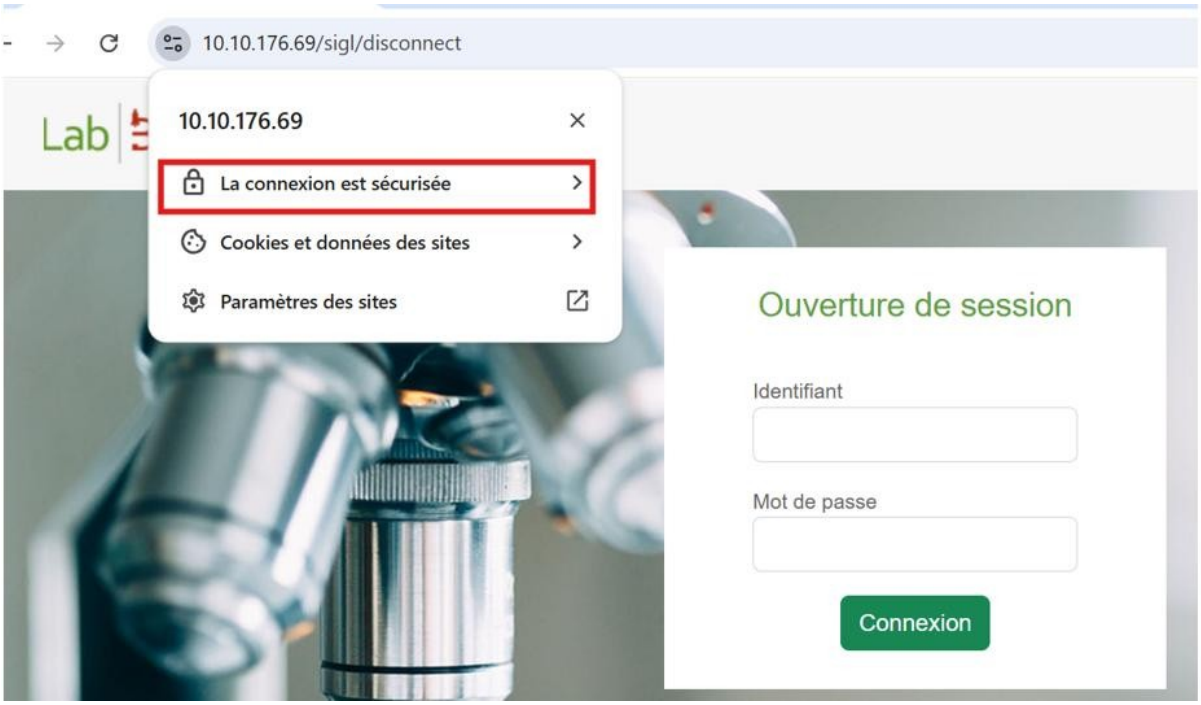

Figure 21 – Connexion sécurisée sous Windows

Conseil : préparez une clé USB contenant le fichier `LabBookLocalRootCA.crt` et une copie de ce paragraphe. L'installation sur chaque poste ne prend alors que quelques minutes.

3.4 Installer le certificat sur Android (LabBook Lite)

LabBook Lite exige le HTTPS et le certificat. Sans eux, la tablette ne peut ni récupérer sa configuration ni envoyer ses données.

1. Copiez `LabBookLocalRootCA.crt` sur la tablette ou le téléphone.
2. Ouvrez **Paramètres** et tapez « certificat » dans la recherche.
3. Choisissez **Installer un certificat**, puis **Certificat CA**.
4. Sélectionnez le fichier `LabBookLocalRootCA.crt` et confirmez avec **Installer quand même**.

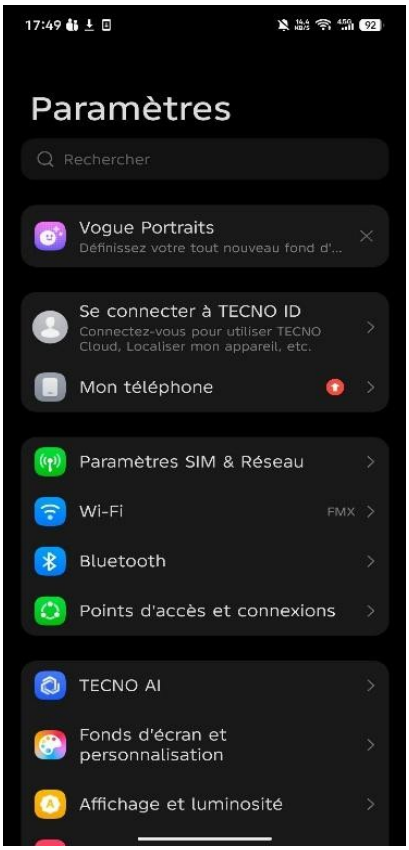

Figure 22 – Paramètres Android



Figure 23 – Recherche « certificat »

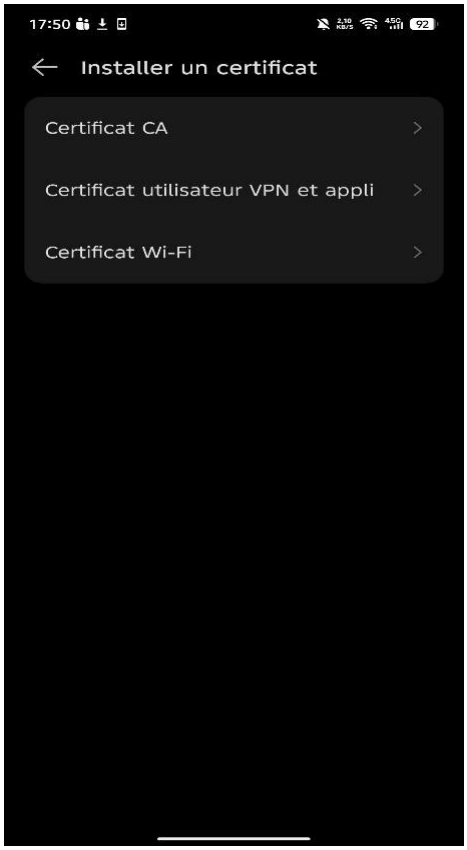

Figure 24 – Choix « Certificat CA »

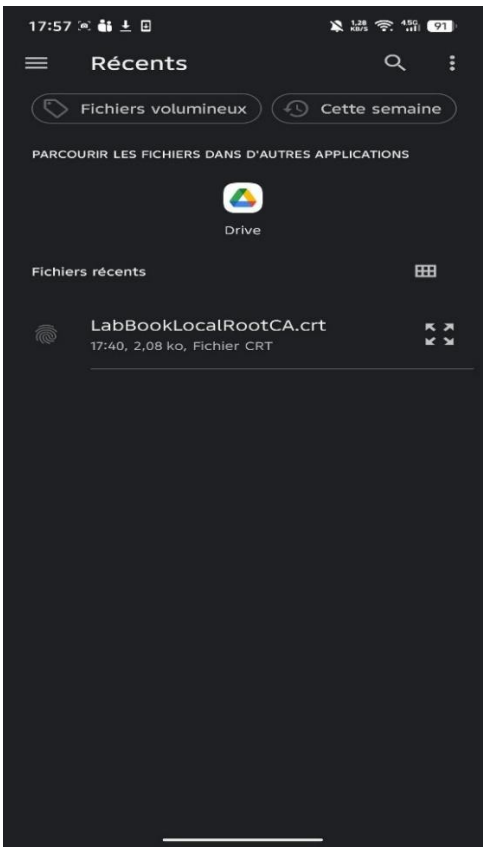

Figure 25 – Sélection du fichier



Figure 26 – Avertissement : « Installer quand même »

5. Vérifiez la présence du certificat : **Certificats de confiance › Utilisateur**.

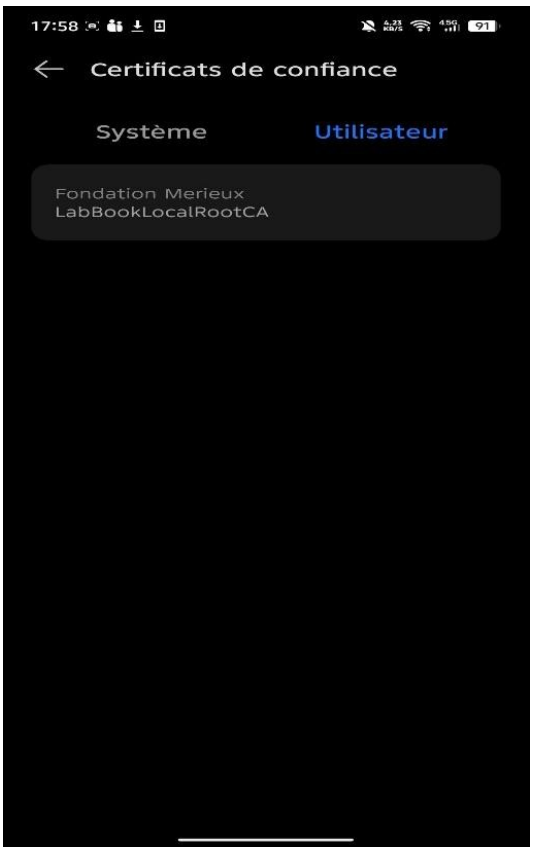

Figure 27 – Certificat visible dans l'onglet Utilisateur

Les intitulés exacts varient selon la marque et la version d'Android.

4. Changer l'utilisateur et le mot de passe MySQL

Par défaut, LabBook se connecte à sa base MySQL avec le compte `root` / `root`. Le script `mysql_change_user.sh` crée un nouveau compte et **désactive** le compte par défaut.

1. Ouvrez un terminal et connectez-vous avec l'administrateur système (`sigl`).
2. Lancez :

```
sudo /home/util/mysql_change_user.sh
```

3. Saisissez le **nouvel utilisateur** MySQL (ex. `labbook`), puis son **mot de passe**.

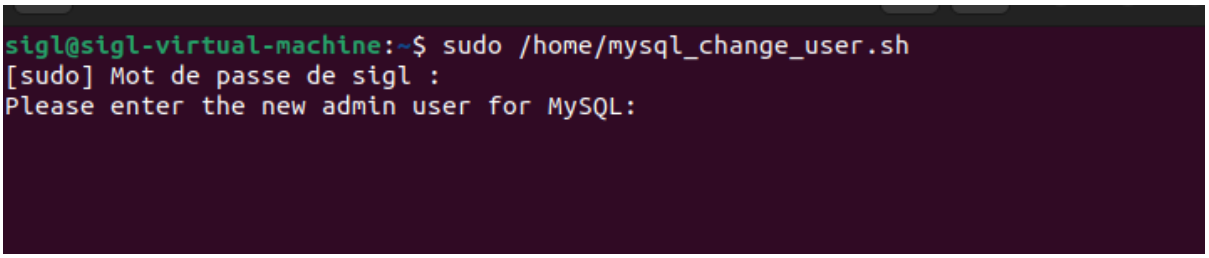

Figure 28 – Lancement du script

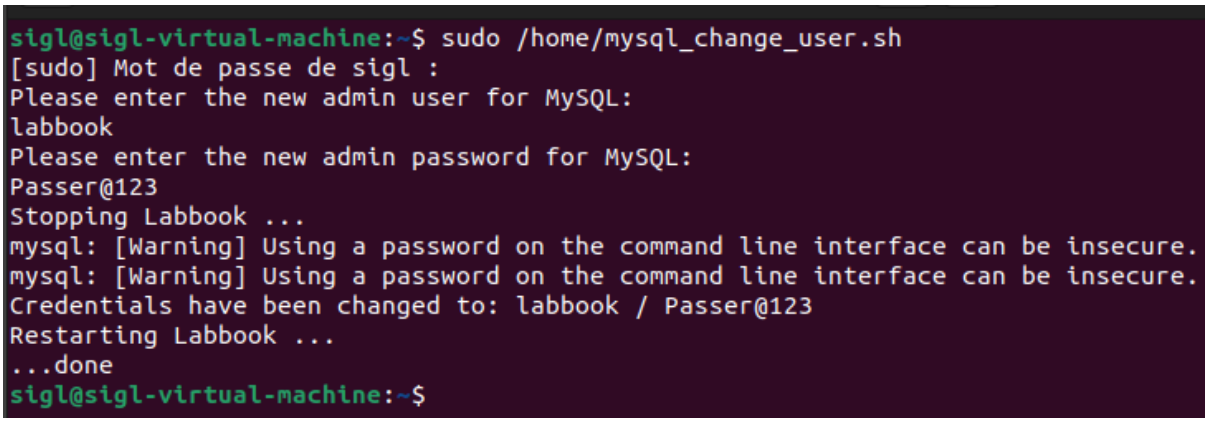

Figure 29 – Saisie du nouvel utilisateur et redémarrage de LabBook

Le script :

- crée le nouveau compte avec tous les droits sur la base ;
- désactive `root` / `root` ;
- relance le service LabBook, dont les conteneurs utilisent désormais les nouveaux identifiants.

Pour vérifier, dans MySQL, la commande `select User, Host from mysql.user;` doit lister le nouvel utilisateur.

```
mysql> show users
    -> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near 'users
' at line 1
mysql> select User,Host from mysql.user;
+------------------+-----------+
| User             | Host      |
+------------------+-----------+
| labbook          | 10.88.%.% |
| root             | 10.88.%.% |
| debian-sys-maint | localhost |
| labbook          | localhost |
| mysql.infoschema | localhost |
| mysql.session    | localhost |
| mysql.sys        | localhost |
| root             | localhost |
+------------------+-----------+
8 rows in set (0,00 sec)
```

Figure 30 – Vérification des utilisateurs MySQL

À savoir : vous pouvez relancer le script autant de fois que nécessaire.

- La première fois, `root` / `root` est bloqué.
- Les fois suivantes, les identifiants précédents sont **supprimés**.

Notez le compte MySQL en vigueur dans le coffre-fort des mots de passe.

5. Autres bonnes pratiques de sécurité

Mesure	Détail
Accès physique	Serveur dans une pièce fermée, peu fréquentée, ventilée, branché sur un onduleur
Mots de passe	Changez tous les mots de passe par défaut : `root` de l'application, `user_labbook`, MySQL, compte système. Conservez-les dans un coffre-fort
Comptes utilisateurs	Un compte nominatif par personne ; désactivez les comptes des personnes parties (guide D1, § 5.3)
Déconnexion automatique	Réglez une durée d'inactivité courte (guide D1, § 3.2)
Journal d'audit	Laissez-le activé et consultez-le régulièrement (guide D1, § 11.1)
Réseau	Pas d'accès depuis Internet ; réseau local du laboratoire uniquement
Pare-feu	N'ouvrez que les ports nécessaires. Par exemple, pour un automate relié par LabBook Connect : `sudo ufw allow 12345/tcp` (guide E5)
Sauvegardes	Chiffrées, testées régulièrement, copie conservée hors du bâtiment (guide E4)

6. Dépannage

Problème	Solution
L'alerte de sécurité reste affichée après l'installation du certificat	Vérifiez que vous ouvrez LabBook avec **la même adresse IP** que celle saisie dans le script. Relancez le navigateur
L'adresse IP du serveur a changé	Fixez l'IP (guide E3), relancez `https_labbook.sh`, puis réinstallez le nouveau certificat sur les postes
LabBook Lite n'arrive pas à récupérer sa configuration	Vérifiez l'URL en `https://`, la présence du certificat sur l'appareil et le réseau Wi-Fi
LabBook ne démarre plus après le changement MySQL	Relancez `mysql_change_user.sh` et vérifiez les identifiants saisis

Annexe — Historique du document

Version	Date	LabBook	Modifications
3.1	10/2026	3.6.28	Scripts regroupés dans /home/util : nouveaux chemins de https_labbook.sh et mysql_change_user.sh
3.0	10/2026	3.6.28	Nouveau guide, issu des chapitres 3 et 4 du manuel d'installation. Ajouts : tableau des comptes, bonnes pratiques, dépannage