Mise à jour du certificat SSL/TLS pour les intégrations existantes vers la version 6.7 SR1 (ou supérieure)

Paxton met continuellement à jour Net2 afin de maintenir des niveaux élevés de cybersécurité et, à ce titre, nous avons apporté des modifications au processus de gestion des certificats au sein du logiciel.

Remarque : cela n'affectera que les intégrations utilisant notre API RESTful et non les intégrations utilisant le SDK de Paxton Net2. Pour accéder à l'API locale via HTTPS, un certificat SSL est requis afin de créer la connexion sécurisée.

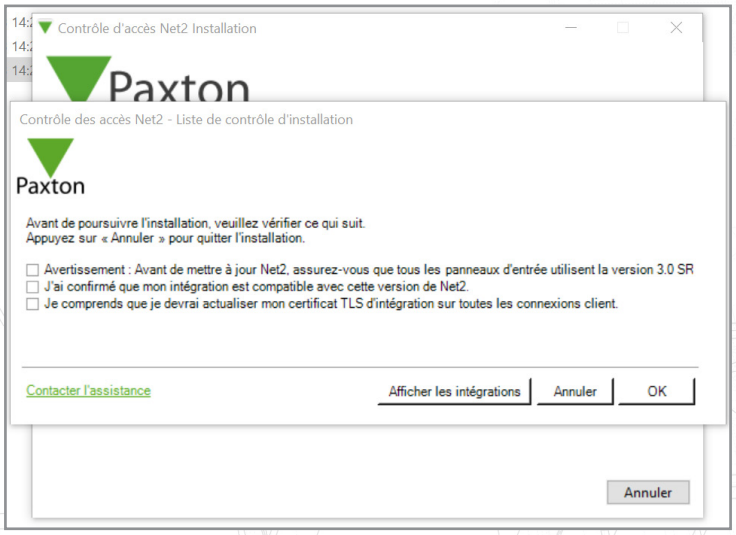
Dans notre prochaine version v6.7 SR1, toutes les intégrations devront mettre à jour leurs certificats SSL. L'onglet du gestionnaire de certificats a maintenant été supprimé de la page localhost8080 et Paxton n'installe plus automatiquement de certificat SSL dans le dossier racine sécurisé.

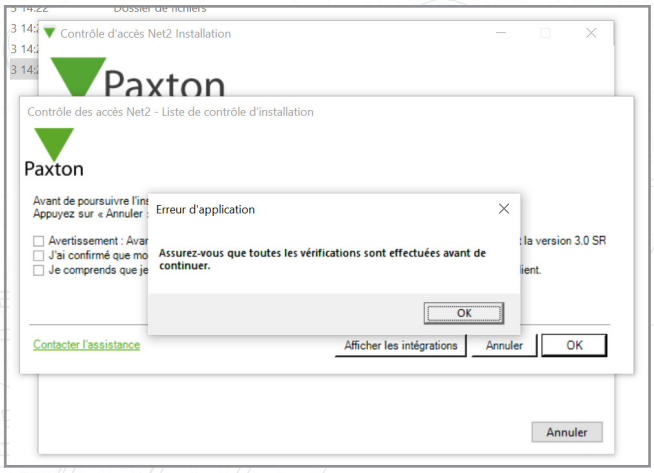
Assurez-vous que votre intégration utilise le protocole HTTPS uniquement, car le protocole HTTP cessera de fonctionner lors de la mise à jour vers la version 6.7 SR1.

Installation d'un certificat TLS auto-signé

Pour qu'une intégration fonctionne et dispose d'une connexion sécurisée, lors de la mise à jour vers Net2 v6.7 SR1 ou version ultérieure, vous devez installer un certificat TLS auto-signé. Il doit être installé sur le serveur et la machine cliente.

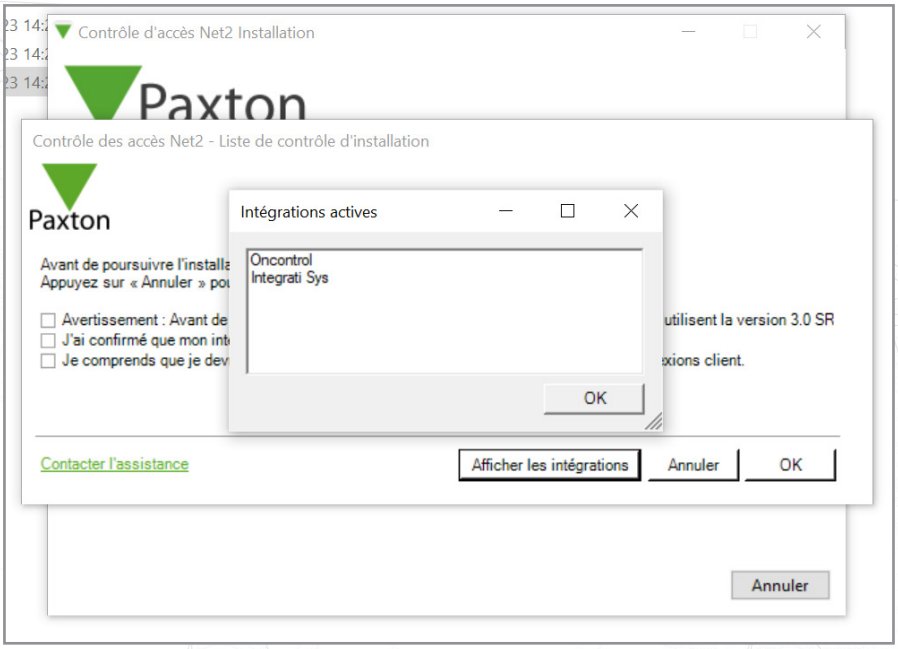
Avant de mettre à jour Net2, vous recevrez la liste de contrôle ci-dessous.



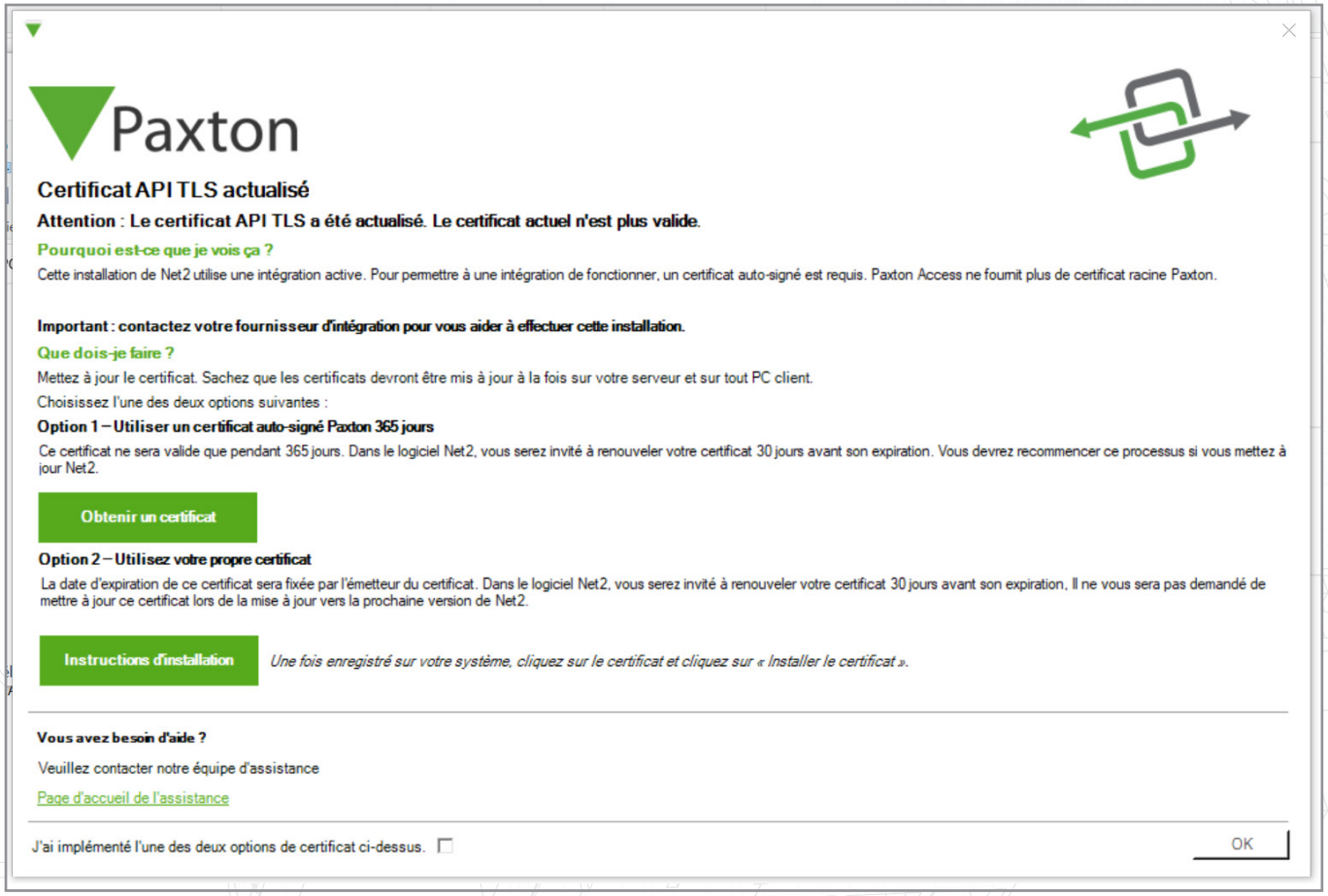


Cochez toutes les cases et cliquez sur « Ok » pour continuer.

Pour vérifier les intégrations en cours d'exécution, cliquez sur « Afficher les intégrations ».



Pendant que la mise à jour est en cours, l'écran suivant s'affiche.



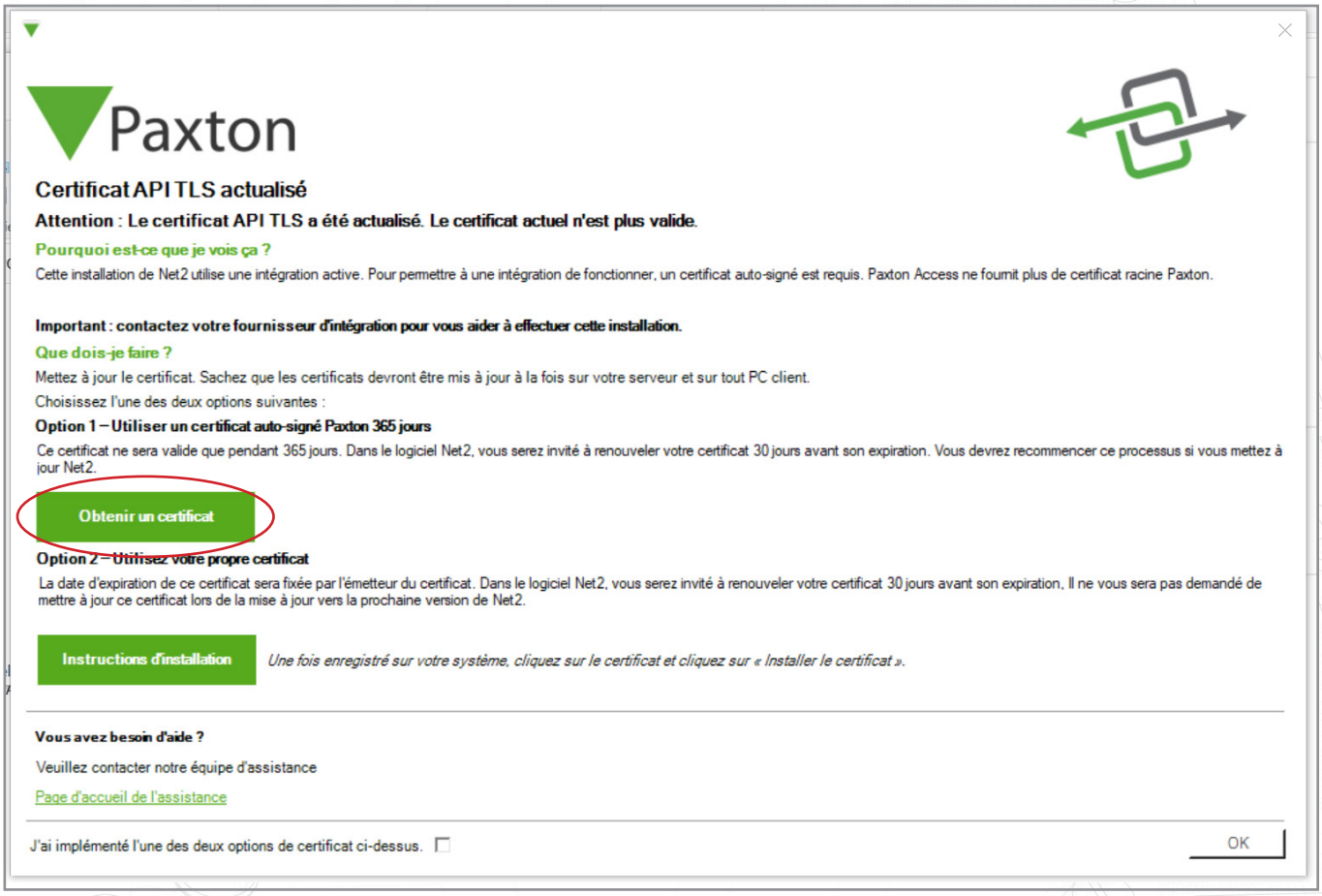
Avant de terminer l'installation de Net2, vous devrez choisir et implémenter l'une des deux options de certificat proposées.

Remarque : Si le certificat n'est pas mis à jour lors de la mise à jour vers la version 6.7 SR1, l'intégration cessera de fonctionner.

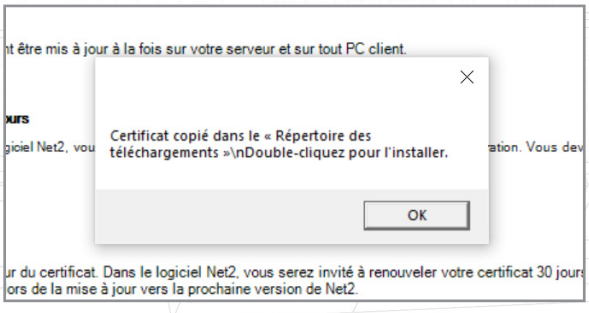
Option 1 : utiliser un certificat auto-signé Paxton de 365 jours

Ce certificat ne sera valide que pendant 365 jours. Dans le logiciel Net2, vous serez invité à renouveler votre certificat 30 jours avant son expiration. Vous devrez recommencer cette procédure si Net2 est mis à jour.

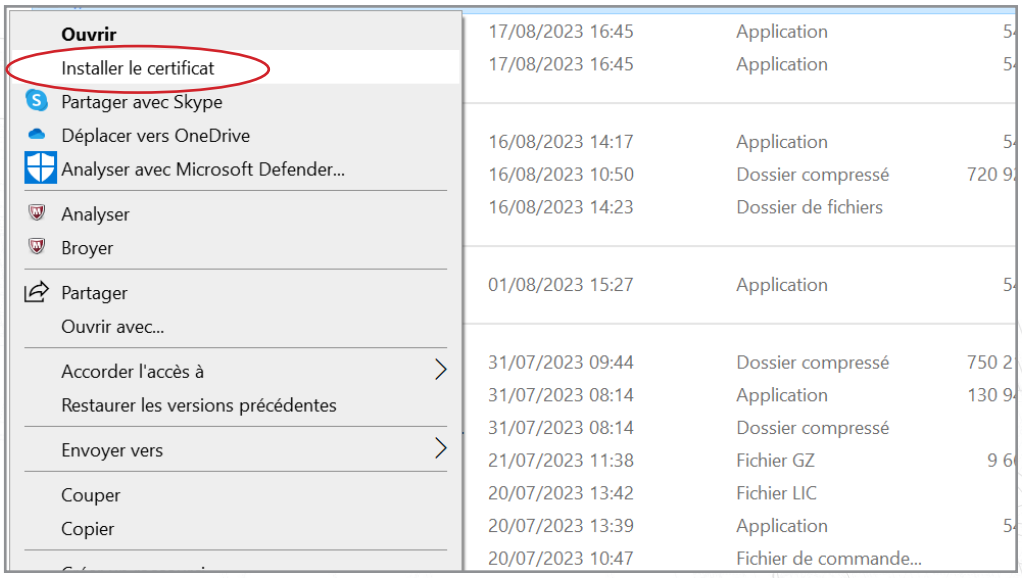
1. Cliquez sur « Obtenir un certificat ».



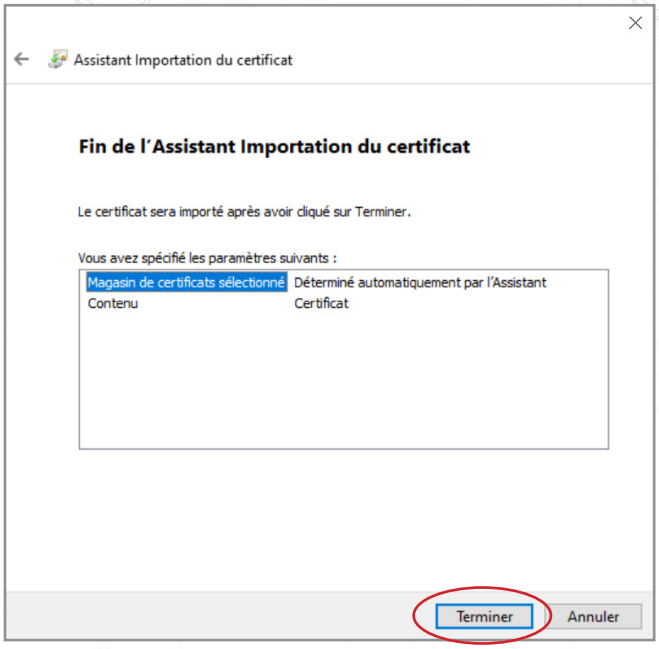
2. Le certificat sera automatiquement installé dans le dossier des téléchargements.



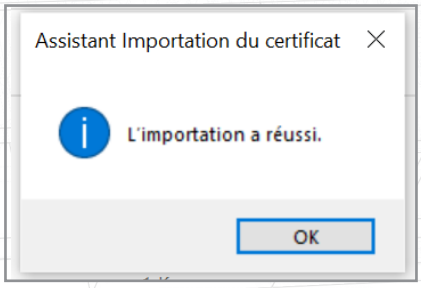
3. Accédez au dossier des téléchargements.
4. Cliquez avec le bouton droit sur le certificat, puis cliquez sur « Installer le certificat ».



5. Choisissez les options que vous souhaitez dans le programme d'installation.
6. Une fois les options choisies, cliquez sur « Terminer ».



7. Le certificat sera installé et l'assistant d'importation indiquera « L'importation a réussi ».
8. Cliquez sur « OK ».

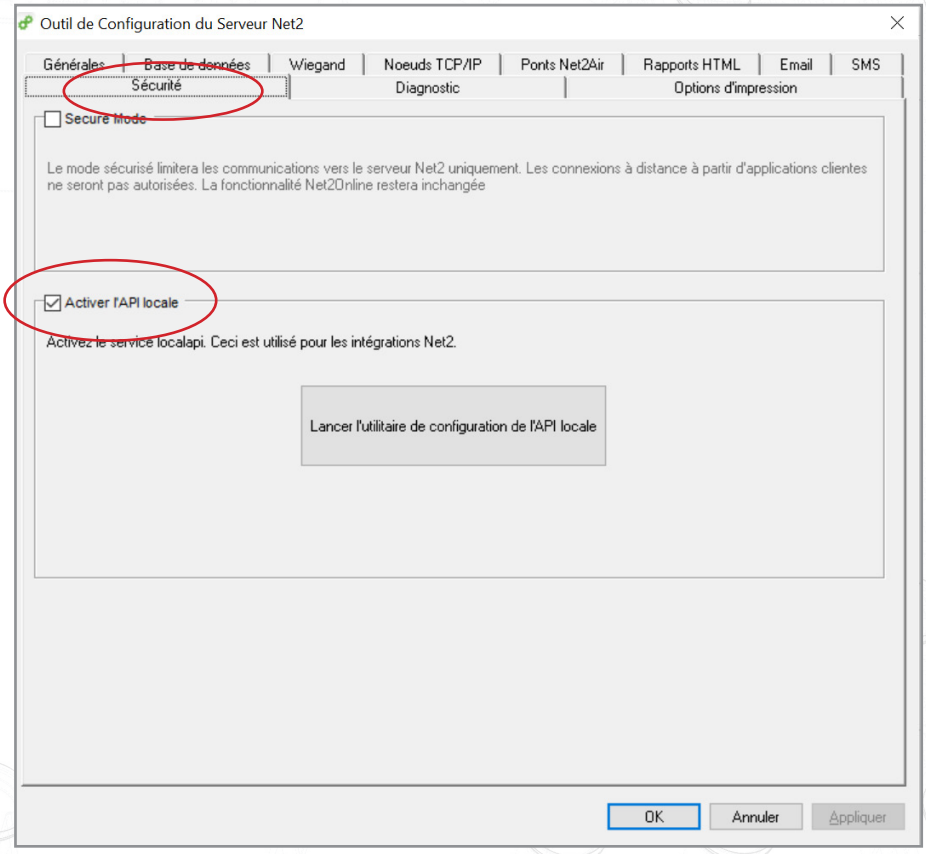


La mise à jour est maintenant terminée.

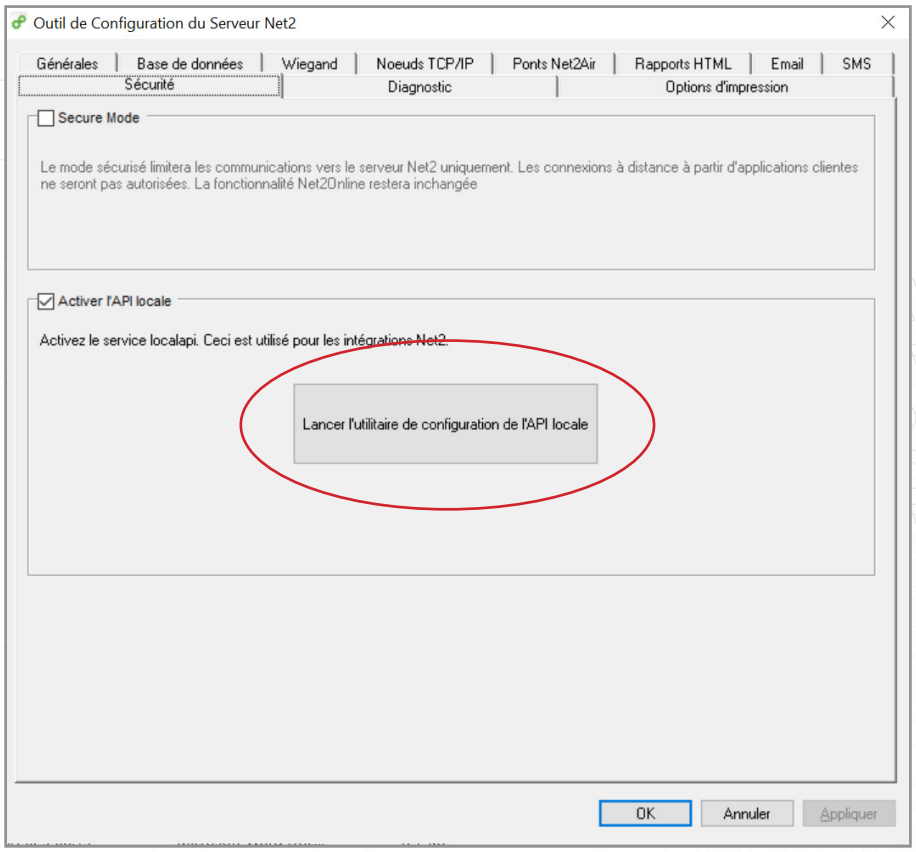
Option 2 : Importez votre propre certificat

La date d'expiration de ce certificat sera fixée par l'émetteur du certificat. Dans le logiciel Net2, vous serez invité à renouveler votre certificat 30 jours avant son expiration. Il ne vous sera pas demandé de mettre à jour ce certificat lors de la mise à jour vers la prochaine version de Net2.

1. Créez votre propre certificat à l'aide d'un fournisseur de certificats TLS. Dans le cadre du package, vous devez disposer d'un certificat et d'une clé.
2. Effectuez la mise à jour vers Net2 v6.7 SR1.
3. Recherchez et ouvrez l'utilitaire de configuration Net2.
4. Accédez à l'onglet « Sécurité ».
5. Assurez-vous que l'API locale est activée.

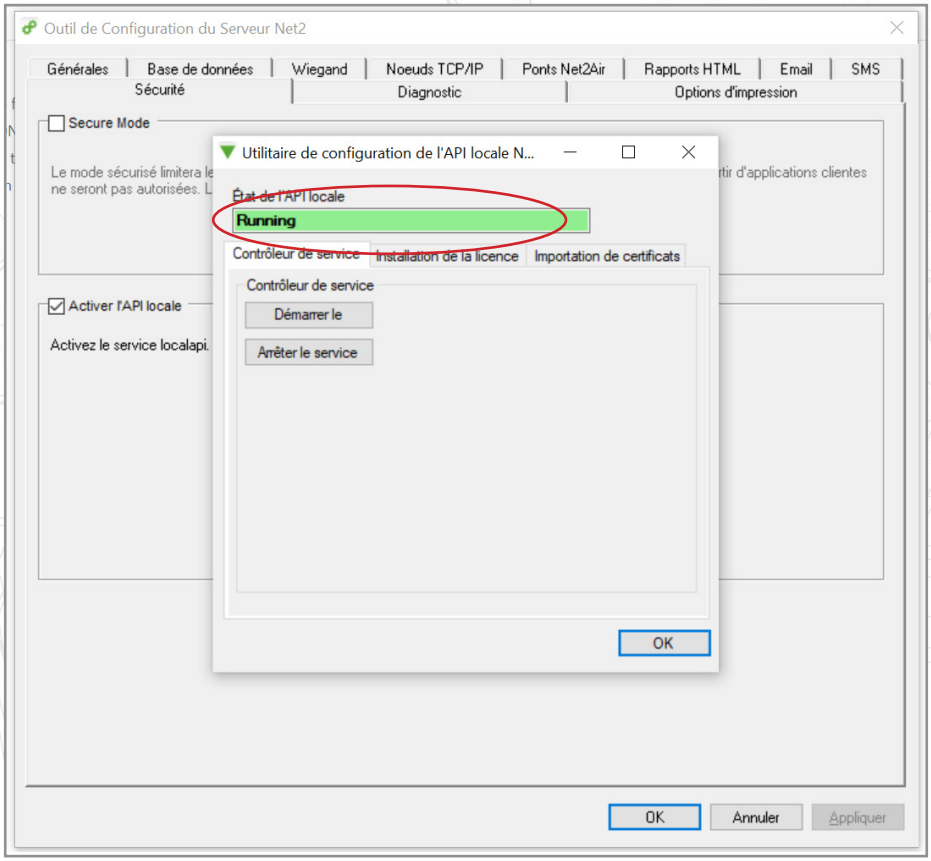


6. Cliquez sur « Lancer l'utilitaire de configuration de l'API ».

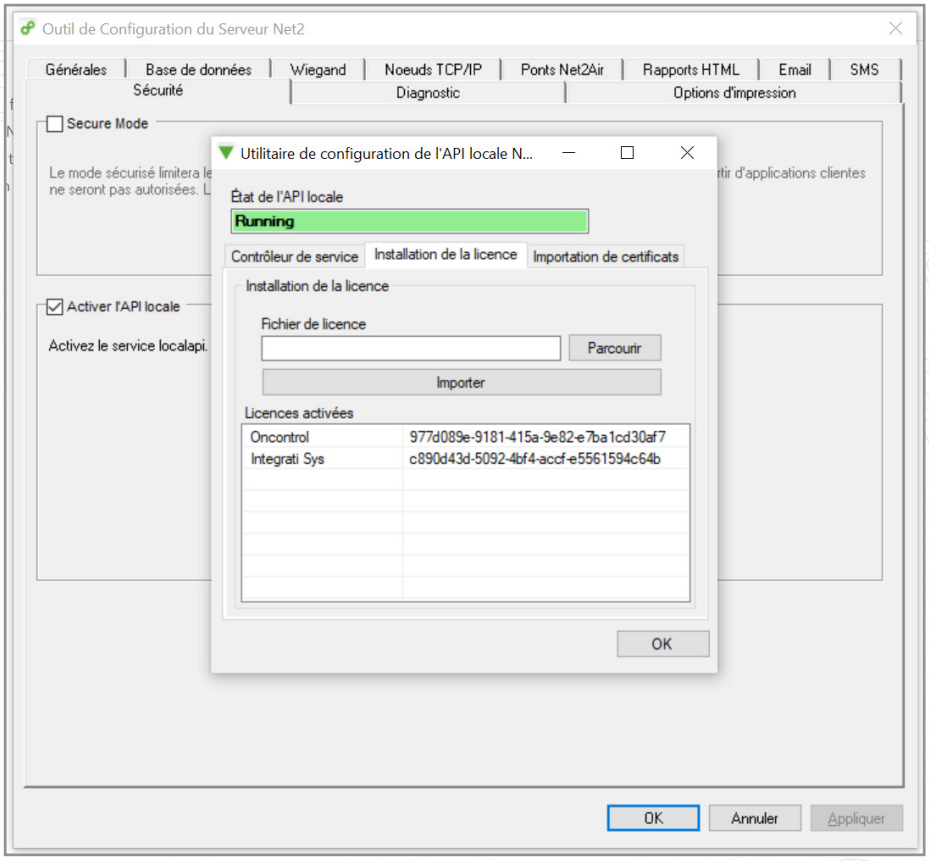


7. L'utilitaire de configuration de l'API locale sera lancé.

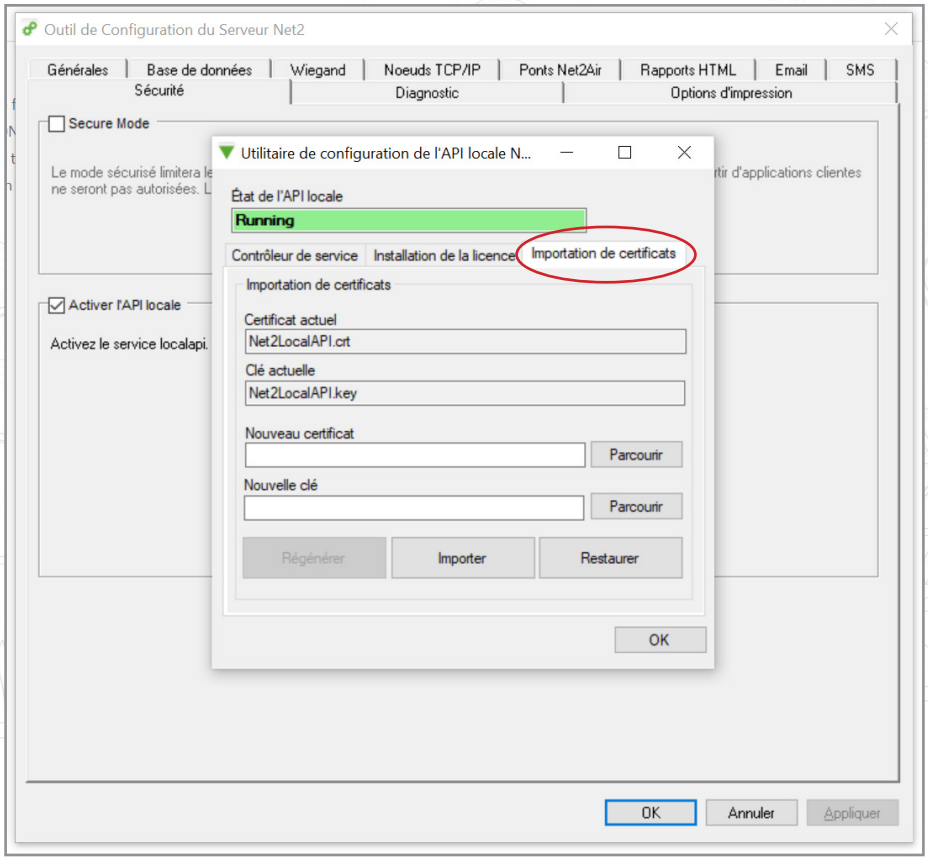
L'état de l'API locale doit indiquer « En cours d'exécution ».



Comme le système dispose d'une intégration en cours d'exécution, vous n'aurez pas besoin d'importer de licence. L'onglet Importateur de licences affiche toutes les licences d'API actuellement utilisées.

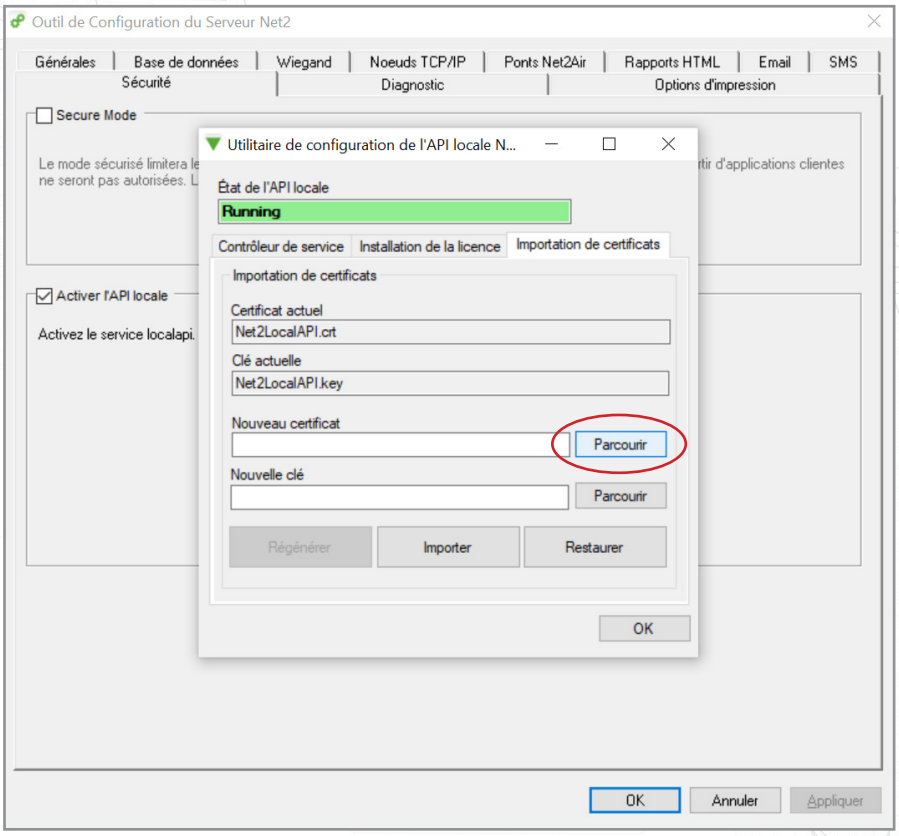


8. Accédez à l'onglet « Importateur de certificats ».

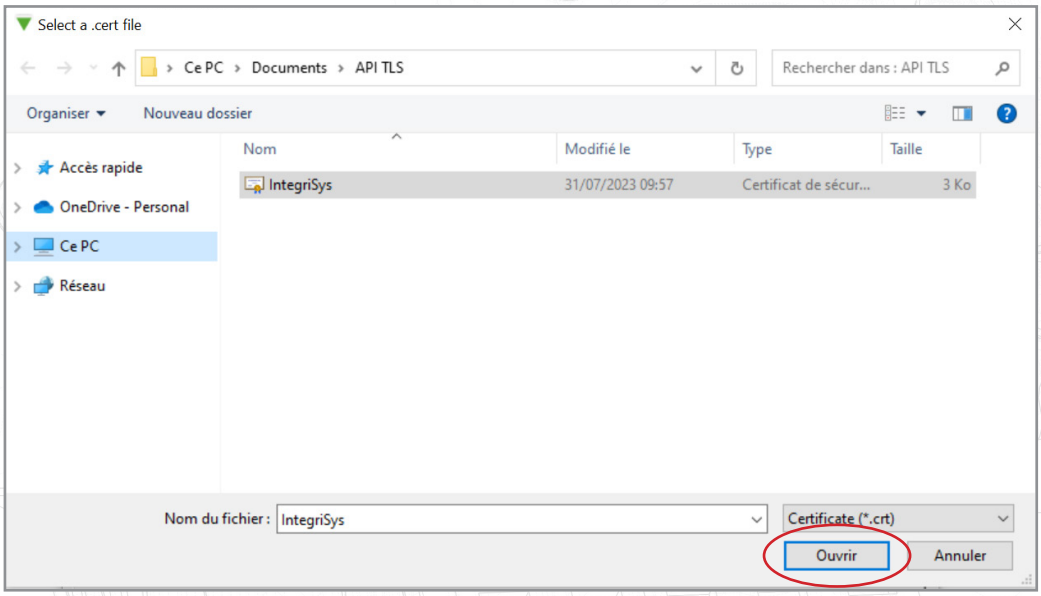


Remarque : L'importateur de licences affichera les licences existantes pour toute intégration en cours d'exécution sur la machine.

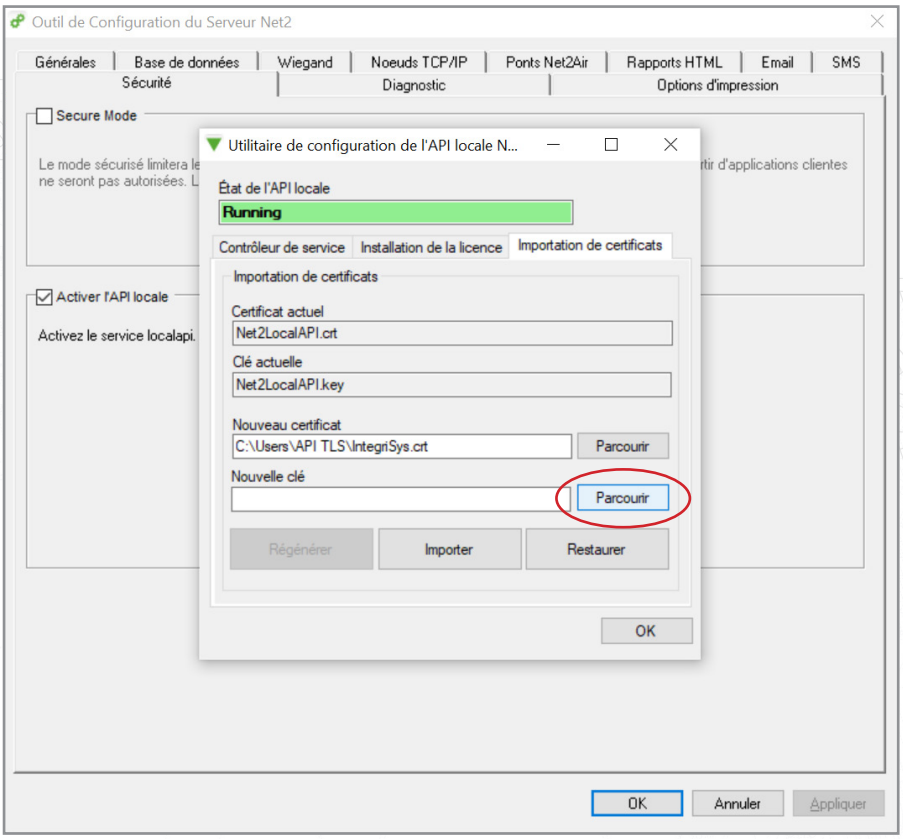
9. Cliquez sur « Parcourir » pour trouver un nouveau certificat.



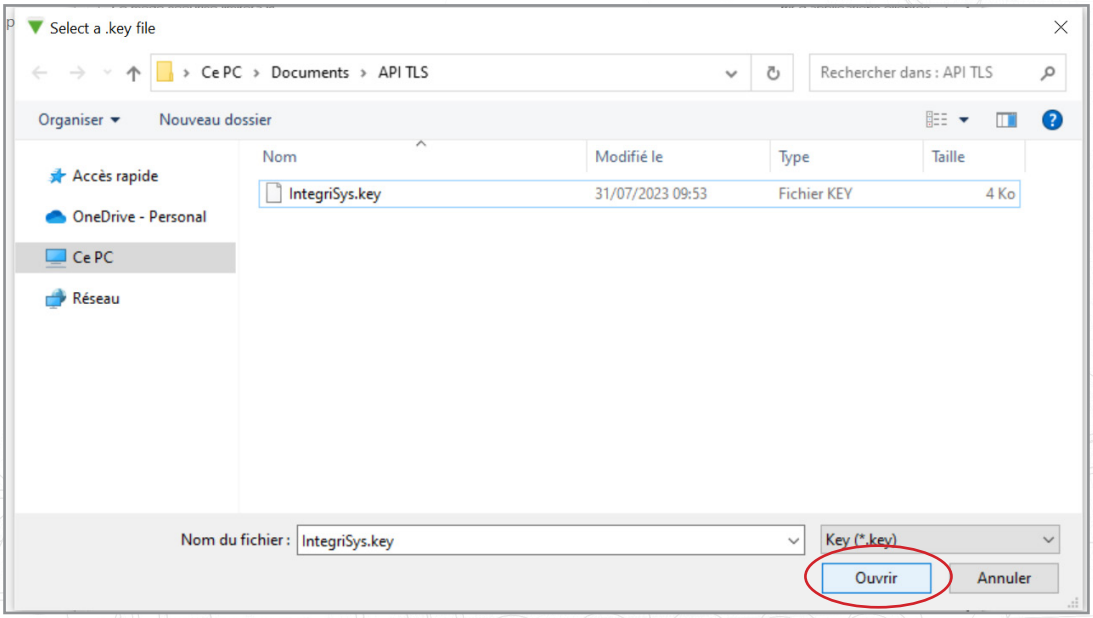
10. Localisez le certificat et cliquez sur « Ouvrir ».



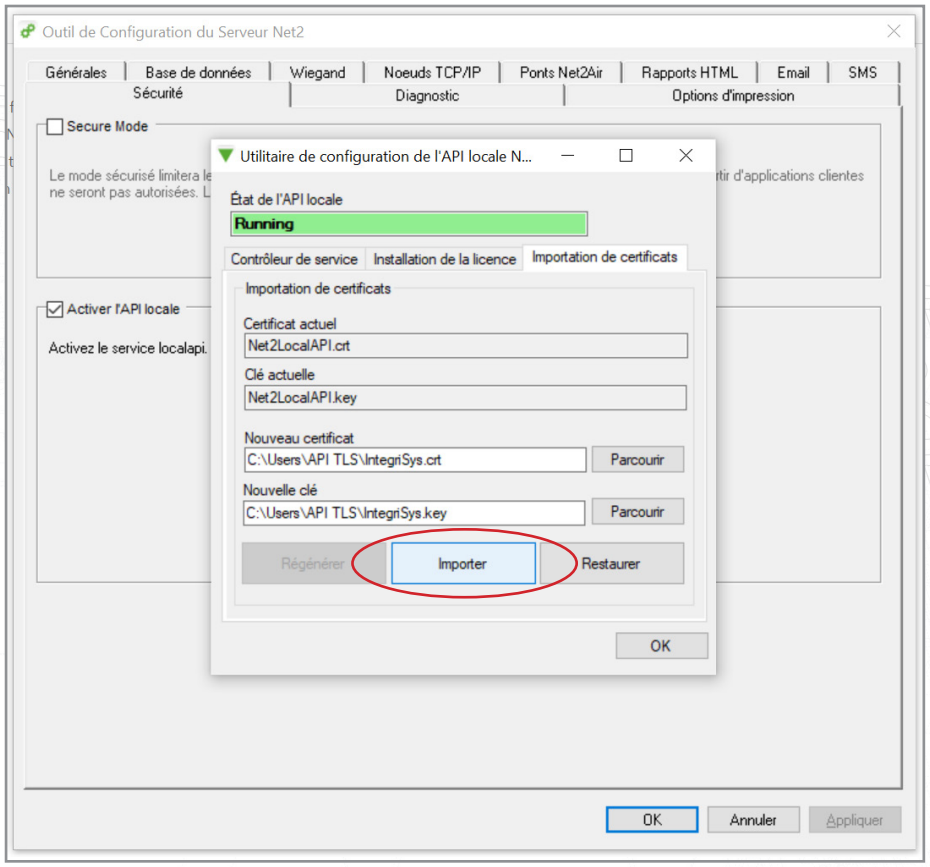
11. Cliquez sur « Parcourir » pour obtenir une nouvelle clé.



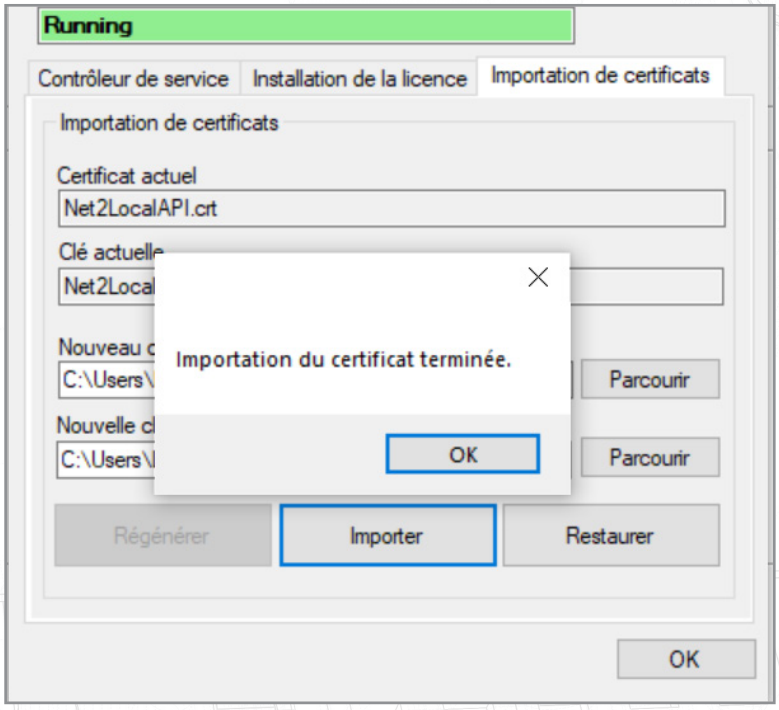
12. Localisez la clé et cliquez sur « Ouvrir ».



13. Cliquez maintenant sur « Importer ».



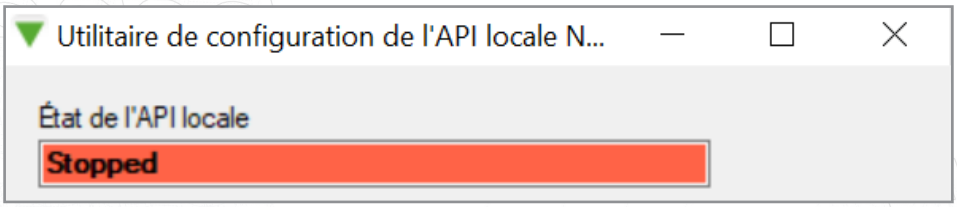
L'importation sera terminée.



Le certificat actuel et la clé actuelle seront mis à jour.

La mise à jour est maintenant terminée.

Remarque : Si l'état du service devient « Arrêté » après l'importation de votre certificat et de votre clé, consultez le journal des erreurs Ngnix situé dans C:\Program Files (x86)\Paxton Access\Access Control\nginx\logs



Option 3 : Comment accéder aux instructions si l'avertissement contextuel API/TLS a été quitté

1. Assurez-vous que votre connexion API est activée.
2. Accédez à https://localhost:8080/setup.html
3. Cliquez sur « Télécharger » pour télécharger le certificat SSL auto-signé 365.
4. Cliquez sur « Instructions d'installation » pour obtenir un lien vers les instructions d'installation.