SSL/TLS Certificate Update for existing integrations to v6.7 SR1 (or above)

Paxton are continually updating Net2 to maintain high levels of cyber security and as such, we have made changes to the certificate management process within the software.

Please note: this will only affect integrations using our RESTful API and not integrations using Paxton Net2's SDK.
To access the local API via HTTPS an SSL certificate is required to create the secure connection.

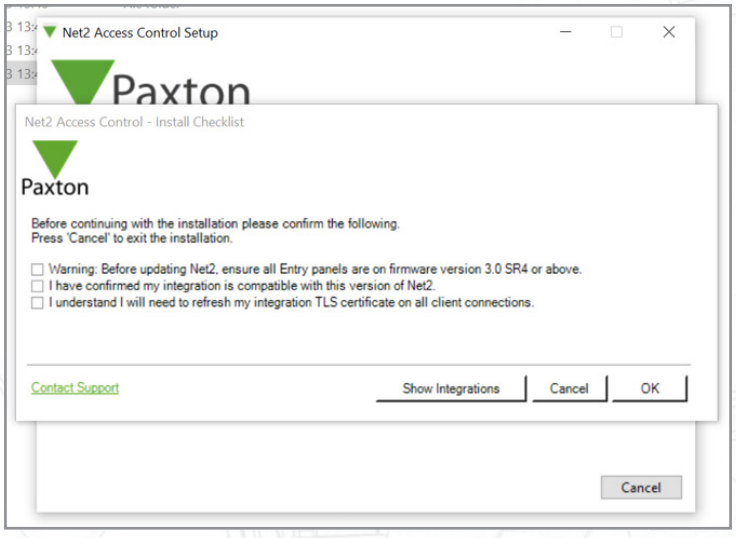
Within our next release v6.7 SR1, all integrations will need to have their SSL certificates updated. The certificate manager tab has now been removed from the localhost8080 page and Paxton no longer automatically install an SSL certificate to the trusted root folder.

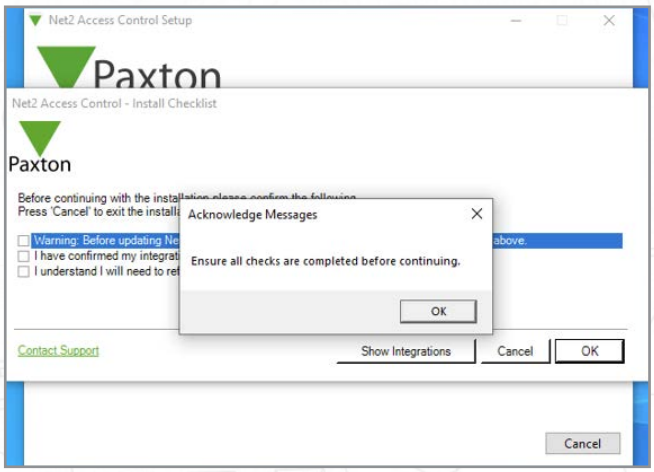
Please ensure your integration is using HTTPS only as HTTP will cease to operate on updating to v6.7 SR1.

Installing a self-signed TLS certificate

For an integration to function and have a secure connection, when updating to Net2 v6.7 SR1 or above, you will need to install a self-signed TLS certificate. This should be installed on the server and client machine.

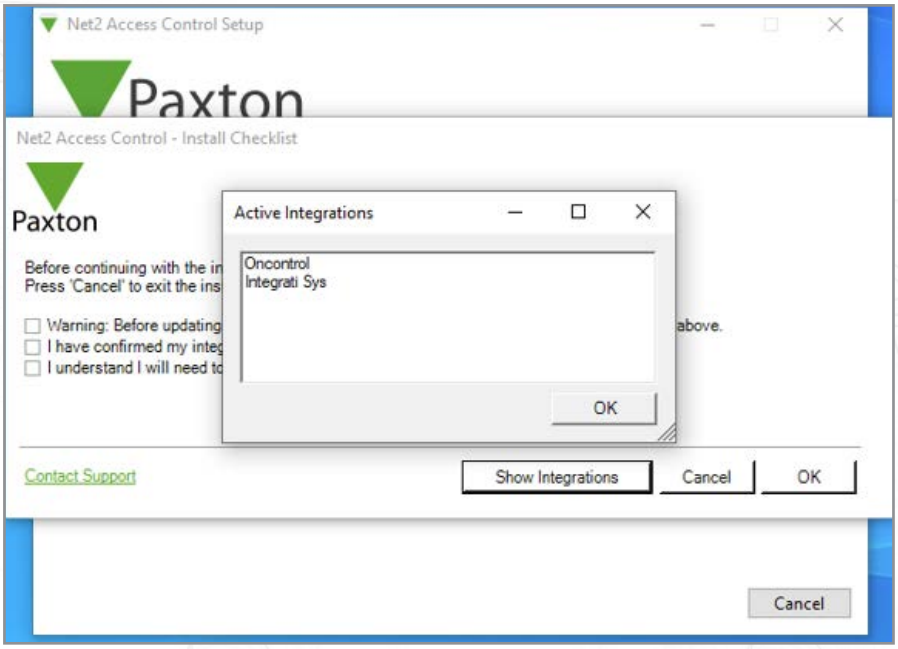
Before updating Net2 you will receive the below checklist.



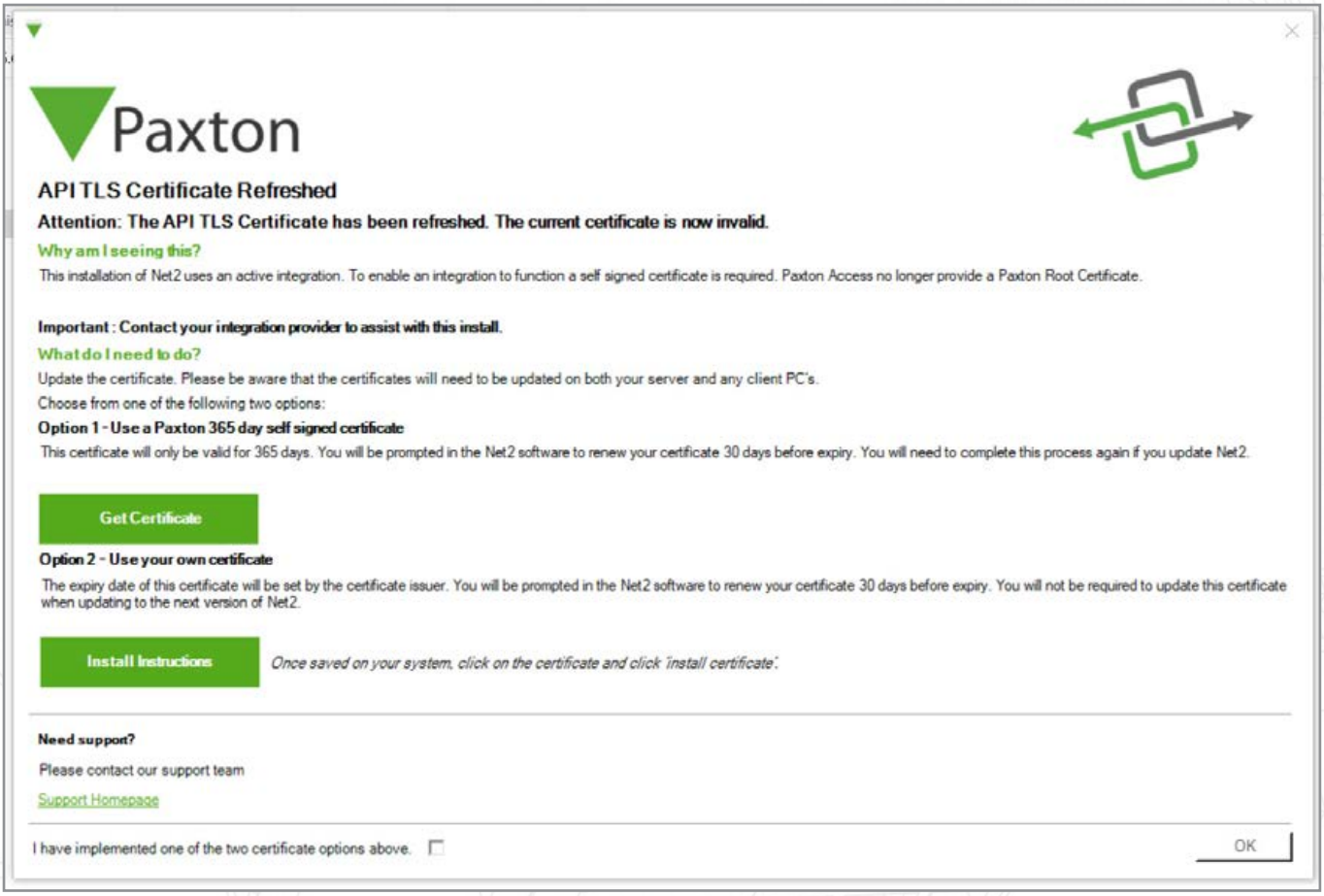


Tick all boxes and click 'Ok' to continue.

To check the integrations that are currently running, click 'Show integrations'.



Whilst the update is taking place the following screen will pop-up.



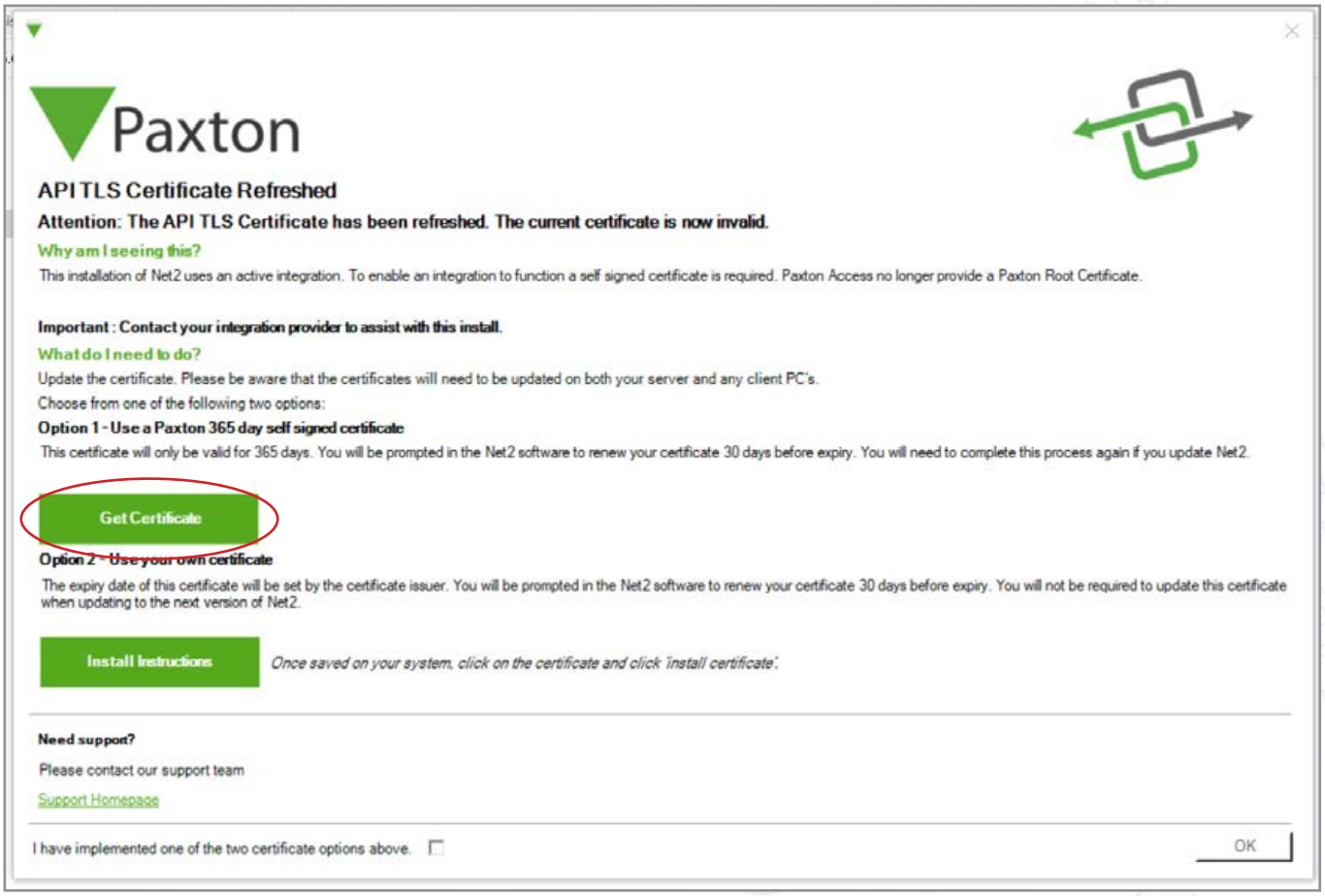
Before completing the install of Net2, you will be required to choose and implement one of the two certificate options that are offered.

Note: If the certificate is not updated whilst updating to v6.7 SR1, the integration will cease to function.

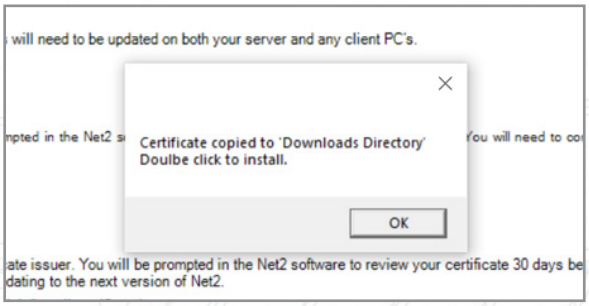
Option 1: Use Paxton 365-day self-signed certificate

This certificate will only be valid for 365 days. You will be prompted in the Net2 software to renew your certificate 30 days before expiry. You will need to do this process again if Net2 is updated.

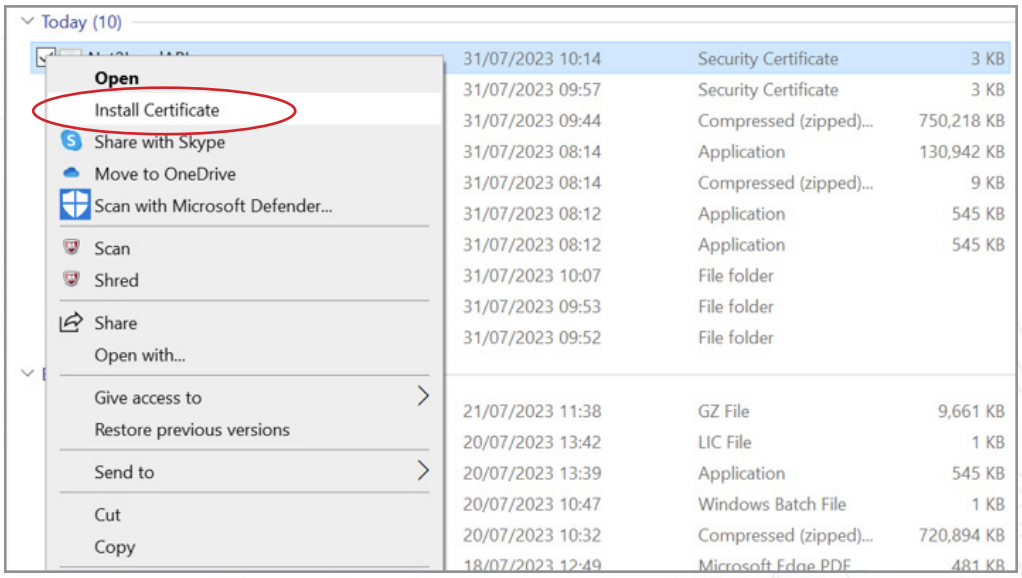
1. Click on 'Get certificate'.



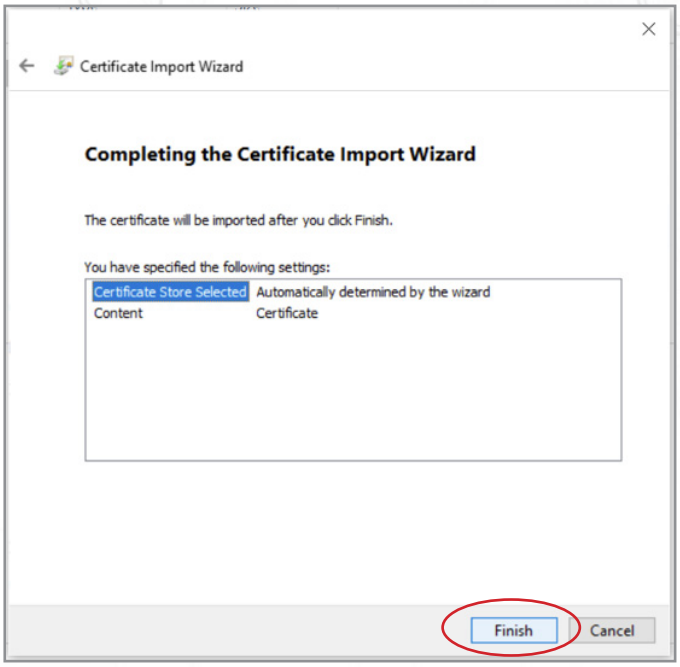
2. The certificate will automatically install in the downloads folder.



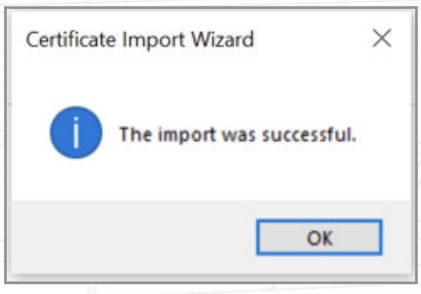
3. Navigate to the downloads folder.
4. Right click on the certificate and click 'Install certificate'.



5. Choose the options that you want within the installer.
6. Once the options have been chosen click 'Finish'.



7. The certificate will install and import wizard will state 'The import was successful'.
8. Click 'Ok'.

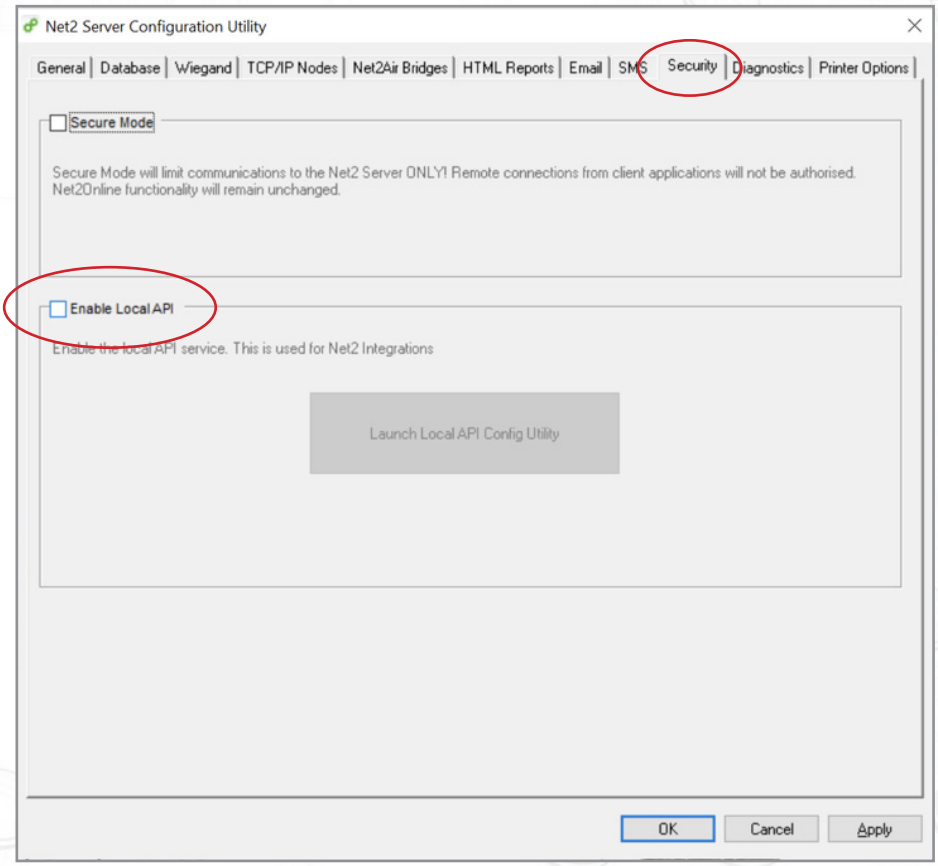


The update is now complete.

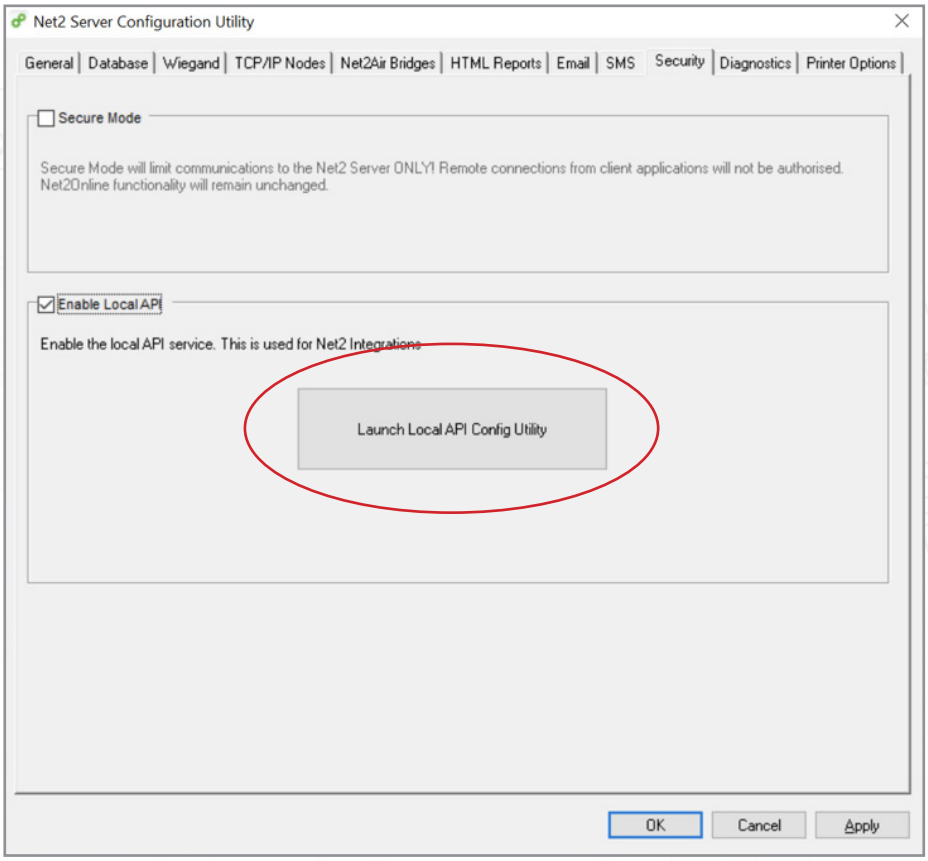
Option 2: Import your own certificate

The expiry date of this certificate will be set by the certificate issuer. You will be prompted in the Net2 software to renew your certificate 30 days before expiry. You will not be required to update this certificate when updating to the next version of Net2.

1. Create your own certificate using a TLS certificate provider. As part of the package, you should have a certificate and a key.
2. Update to Net2 v6.7 SR1.
3. Search and open the Net2 configuration utility.
4. Navigate to the 'Security' tab.
5. Ensure the local API is enabled.

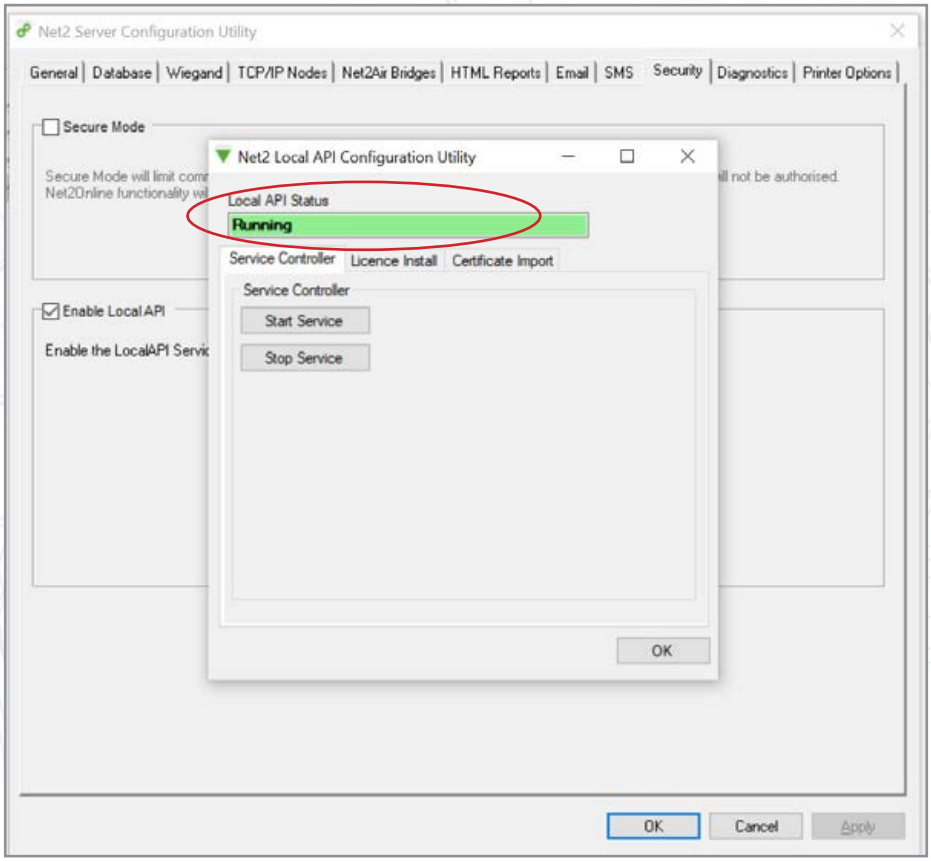


6. Click 'Launch API Config Utility'.

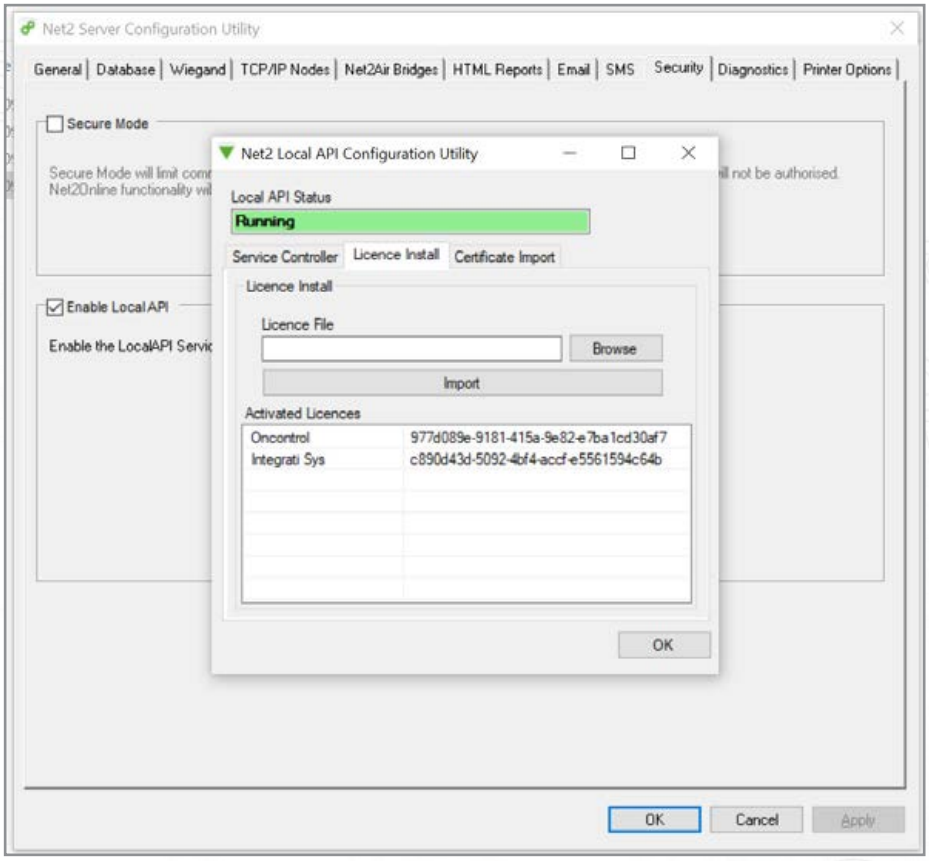


7. The Local API Config Utility will launch.

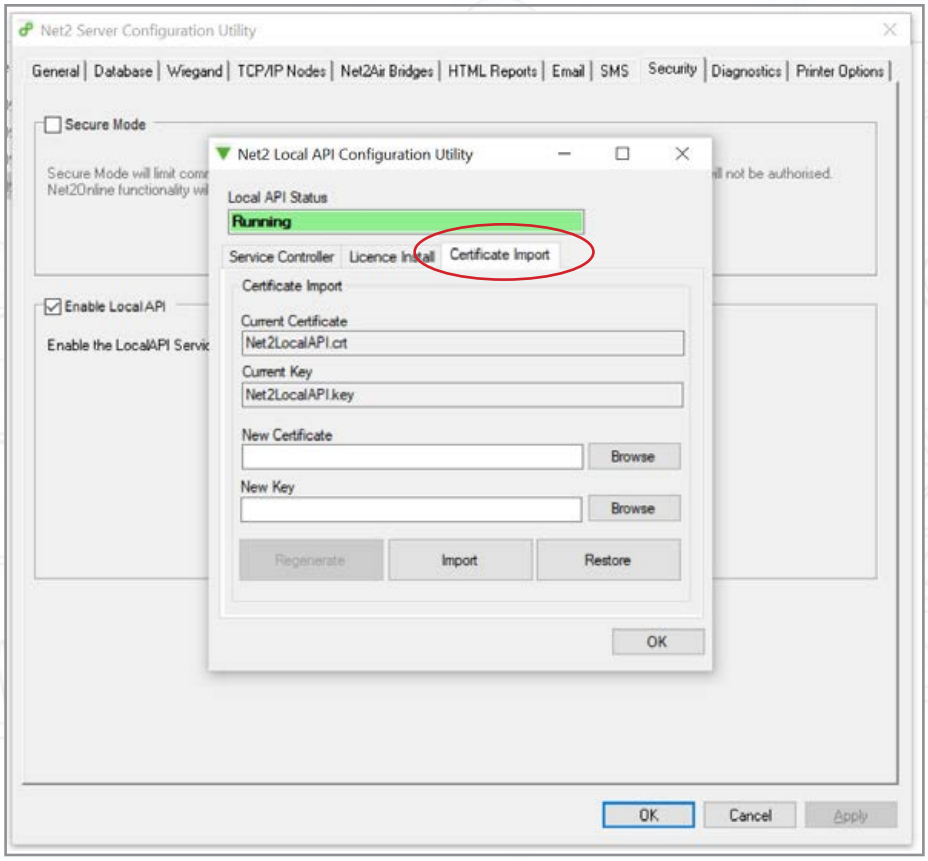
The Local API status should state 'Running'.



As the system has an integration running you will not be required to import a licence. The licence importer tab will show any API licences that are currently being used.

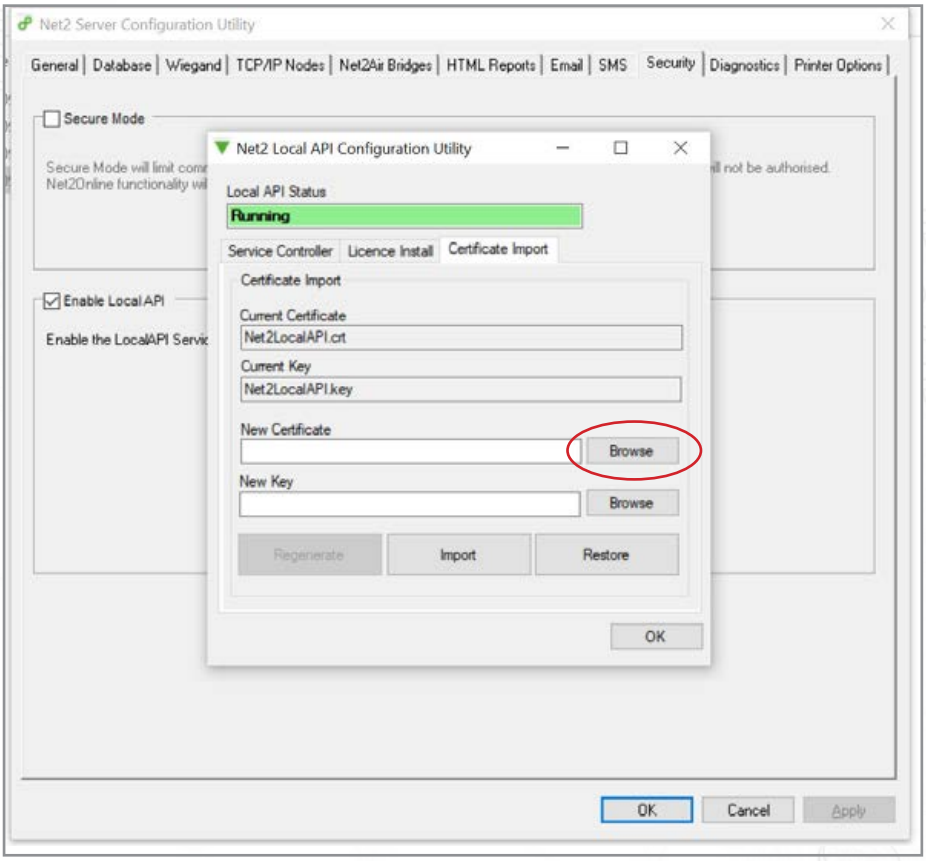


8. Navigate to 'Certficate Importer' tab.

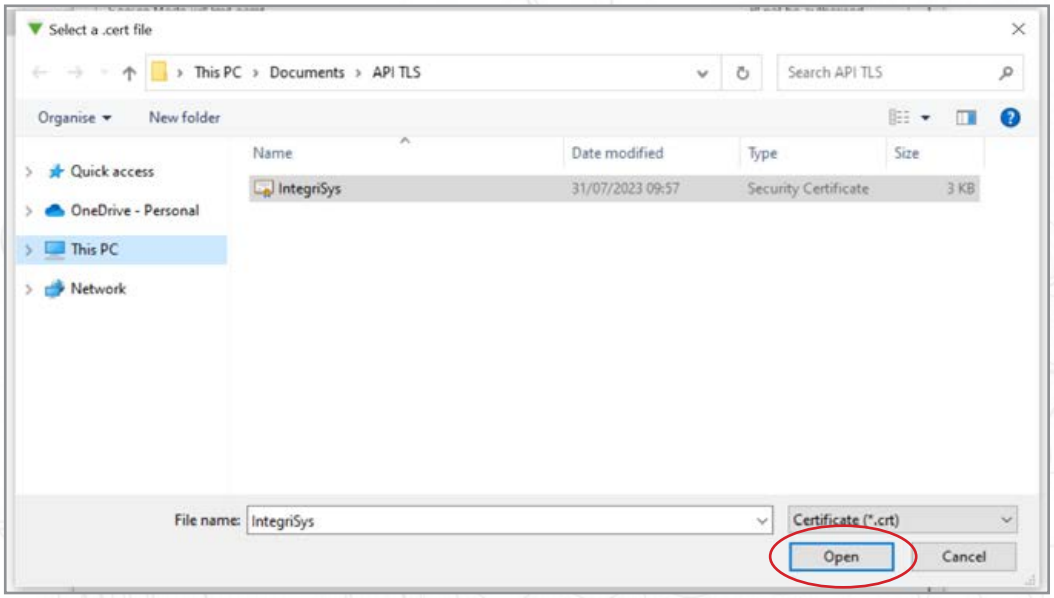


Note: Licence Importer will show the existing licences for any integration that is running on the machine.

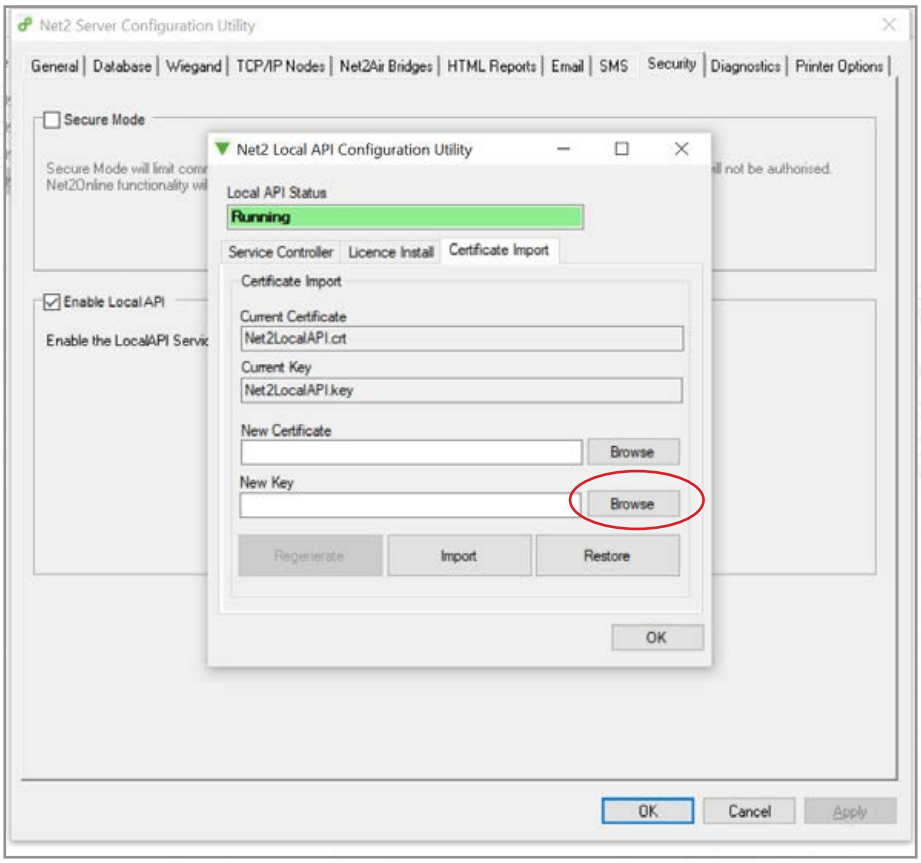
9. Click 'Browse' for New Certificate.



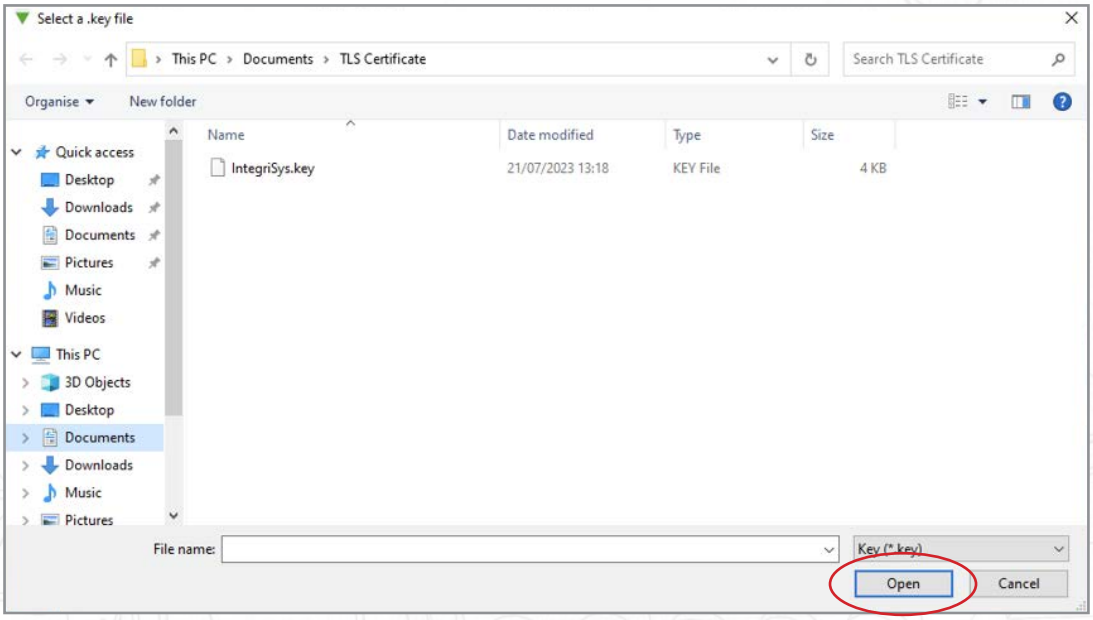
10. Locate the certificate and click 'Open'.



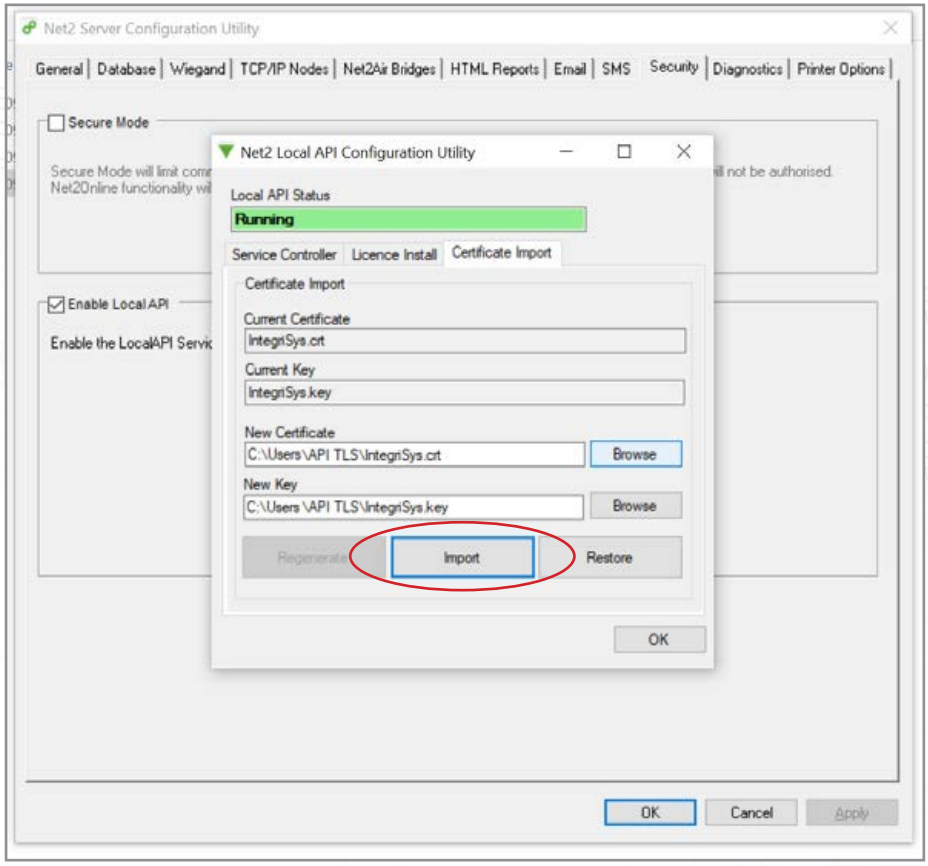
11. Click 'Browse' for New Key.



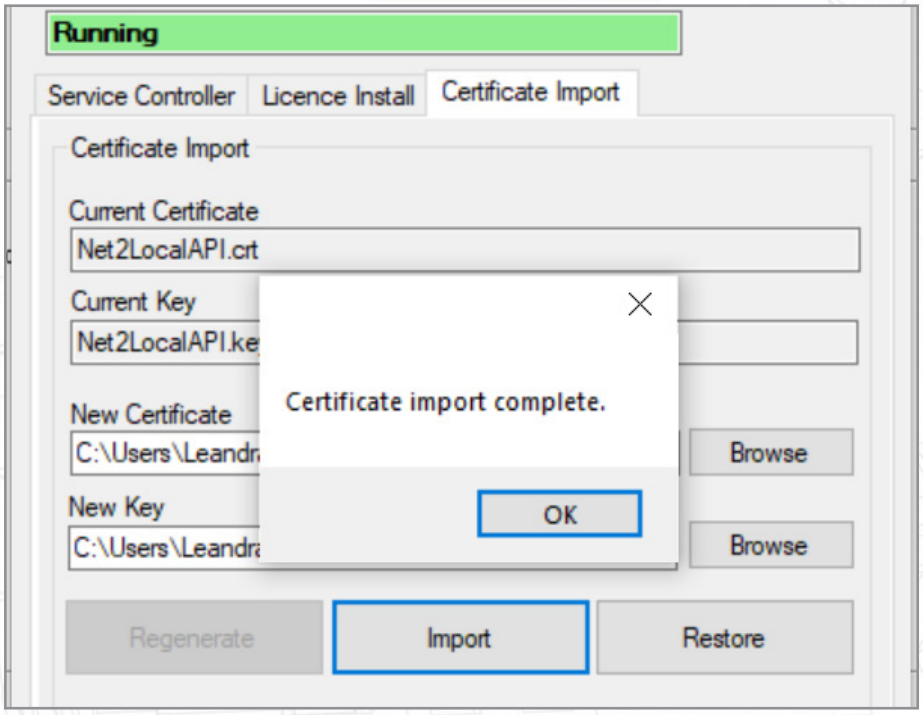
12. Locate the Key and click 'Open'.



13. Now click 'Import'.



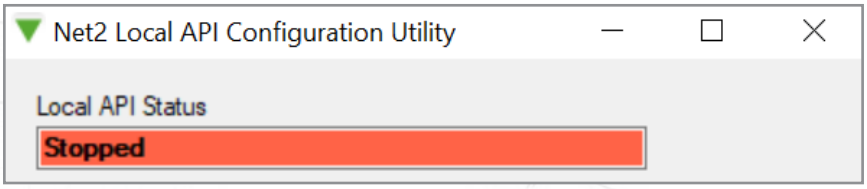
The import will complete.



The current certificate and current key will be updated.

The update is now complete.

Note: If the service status changes to stopped following the import of your certificate and key, check the Ngnix error log located at C:\Program Files (x86)\Paxton Access\Access Control\nginx\logs



Option 3: How to access the instructions if the API/TLS pop-up warning has been exited

1. Ensure your API connection has been enabled.
2. Navigate to https://localhost:8080/setup.html
3. Click 'Download' to download 365 self-signed SSL certificate.
4. Click 'Install instructions' for a link to the install instructions.