SSL/TLS Certificate implementation for new integrations installs

Overview

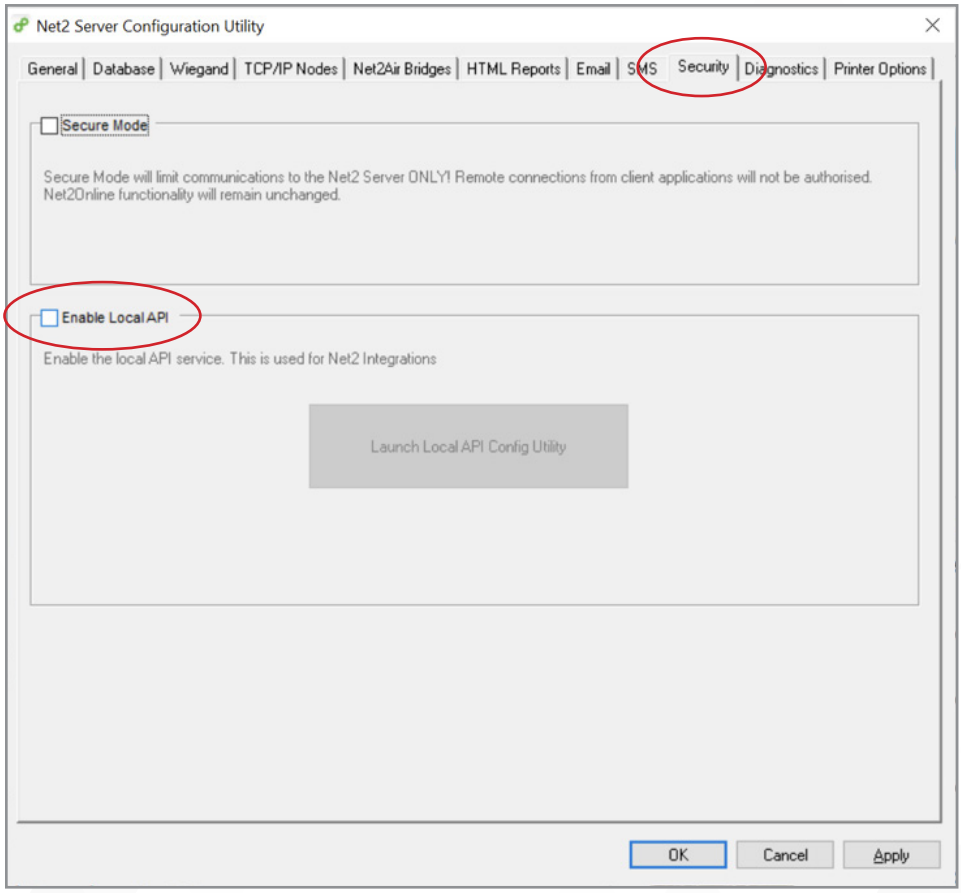
For an API integration to function and have a secure connection, when installing an integration, you will need to install a self-signed TLS certificate. This should be installed on the server and client machine.

Enabling the API connection

Please note: On all Net2 versions from Net2 6.6 v6 the API service will need to be enabled.

1. Open the configuration utility.
2. Click on security tab.
3. Tick '**Enable LocalAPI**'.

The services will now restart and connection to the API is enabled.

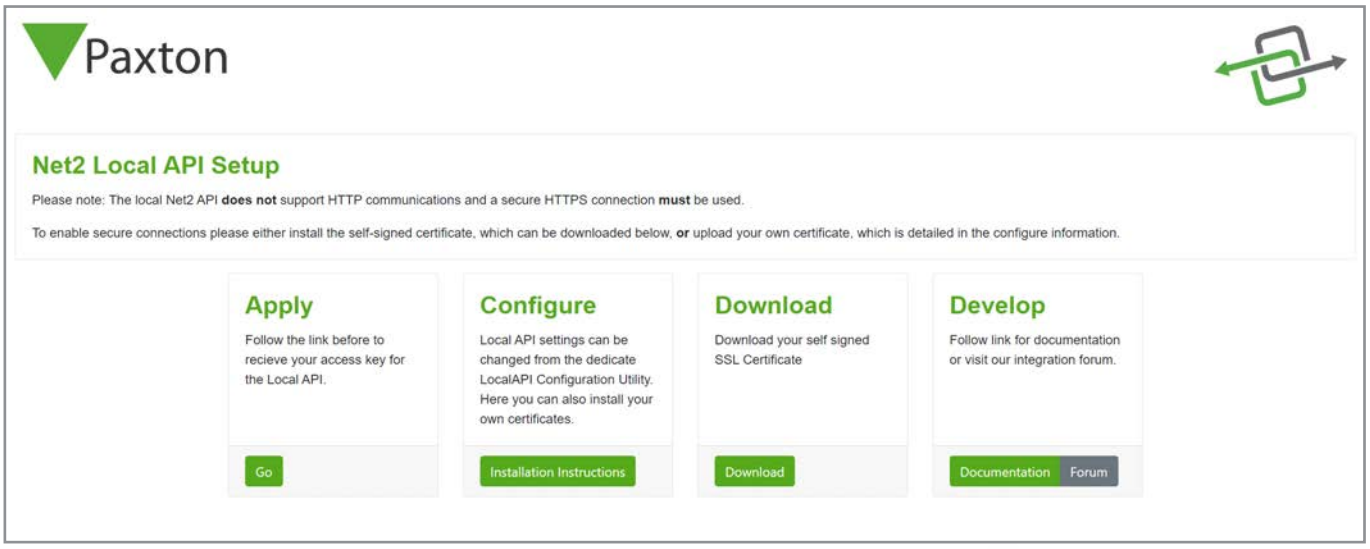


Installing the self-signed TLS certificate

Paxton have provided two options for the certificate install. To view these options, navigate to: https://localhost:8443/setup.html

Note: The API connection must be enabled before accessing this URL

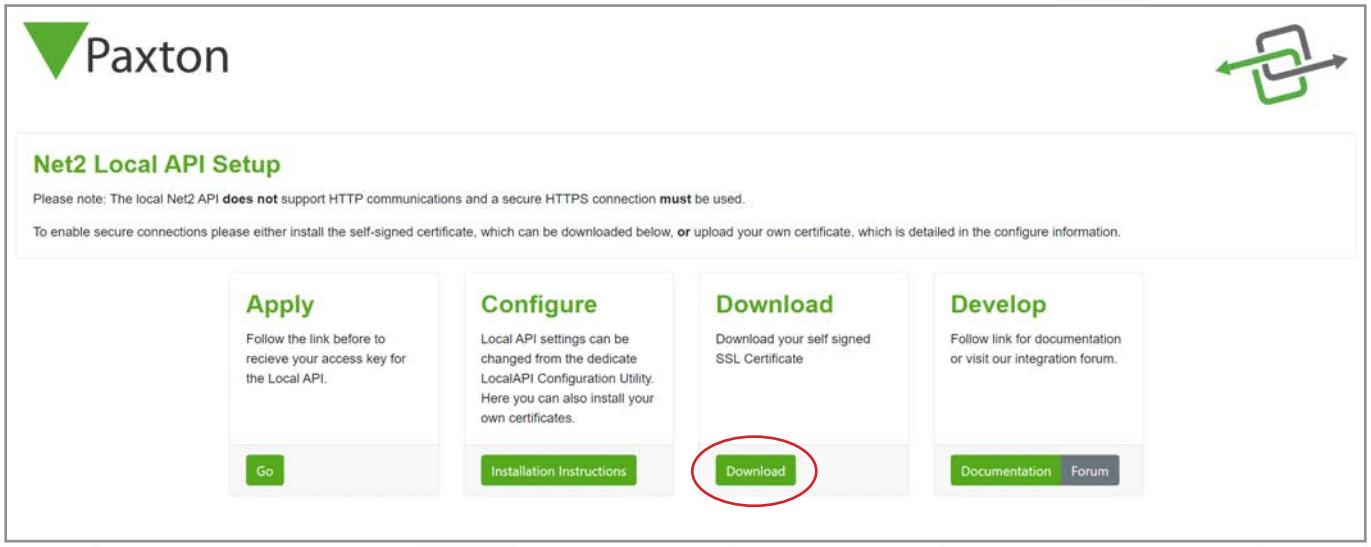
You will now see the following webpage displayed.



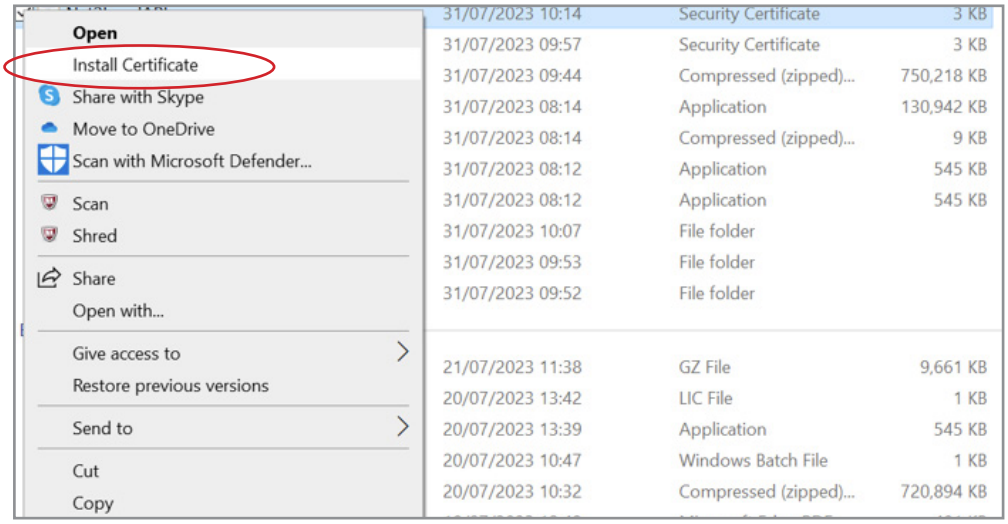
Option 1: Use Paxton 365-day self-signed certificate

This certificate will only be valide 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.

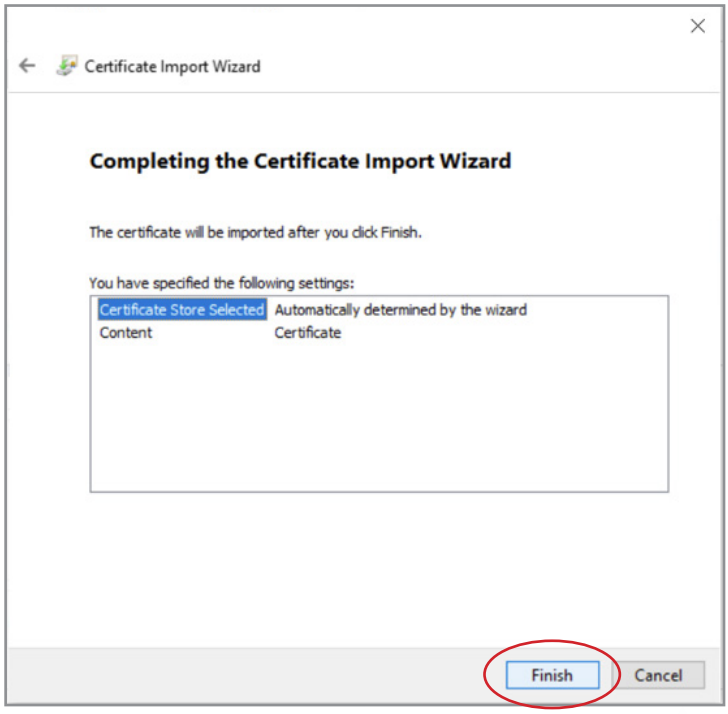
1. Click on '**Download**'.



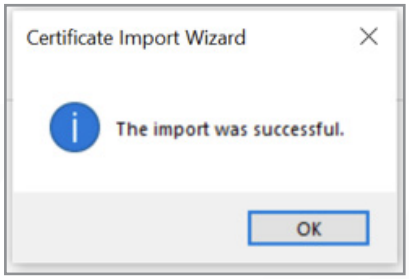
2. The certificate will automatically install in the downloads folder.
3. Navigate to downloads folder.
4. Right click on the certificate.
5. Click '**Install certificate**'.



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



8. Certificate will install and import wizard will state, '**The import was successful**'.
9. Click '**Ok**'.

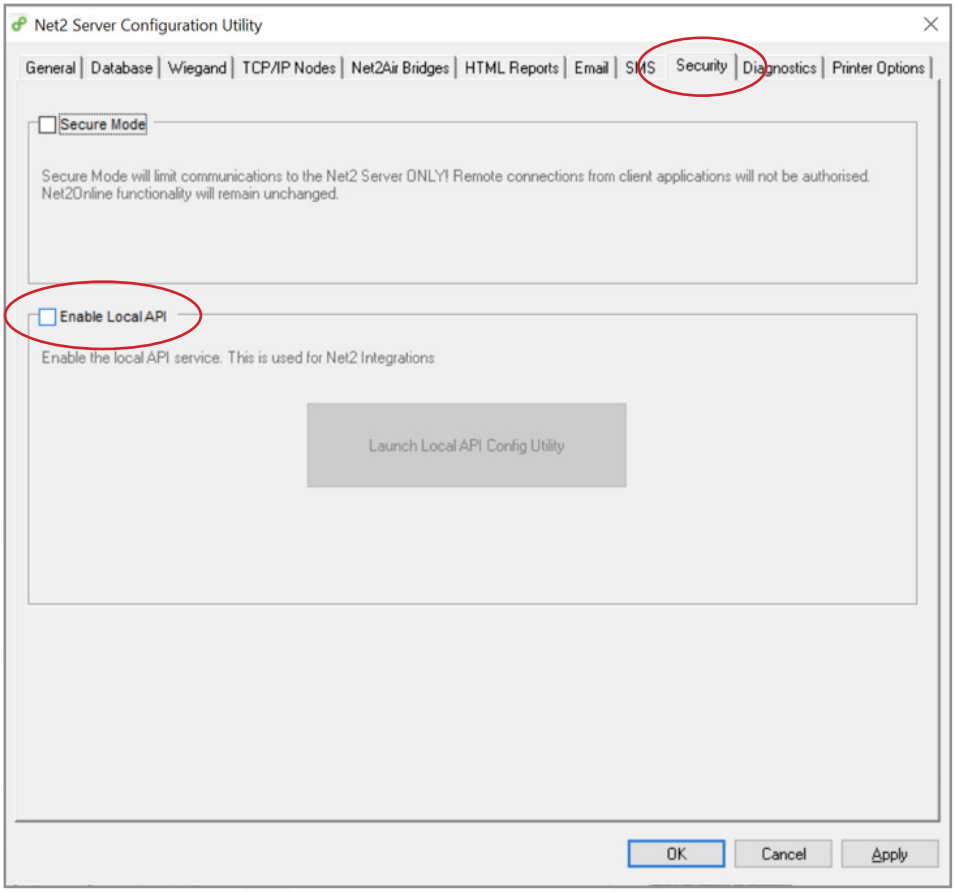


The implementation is now complete.

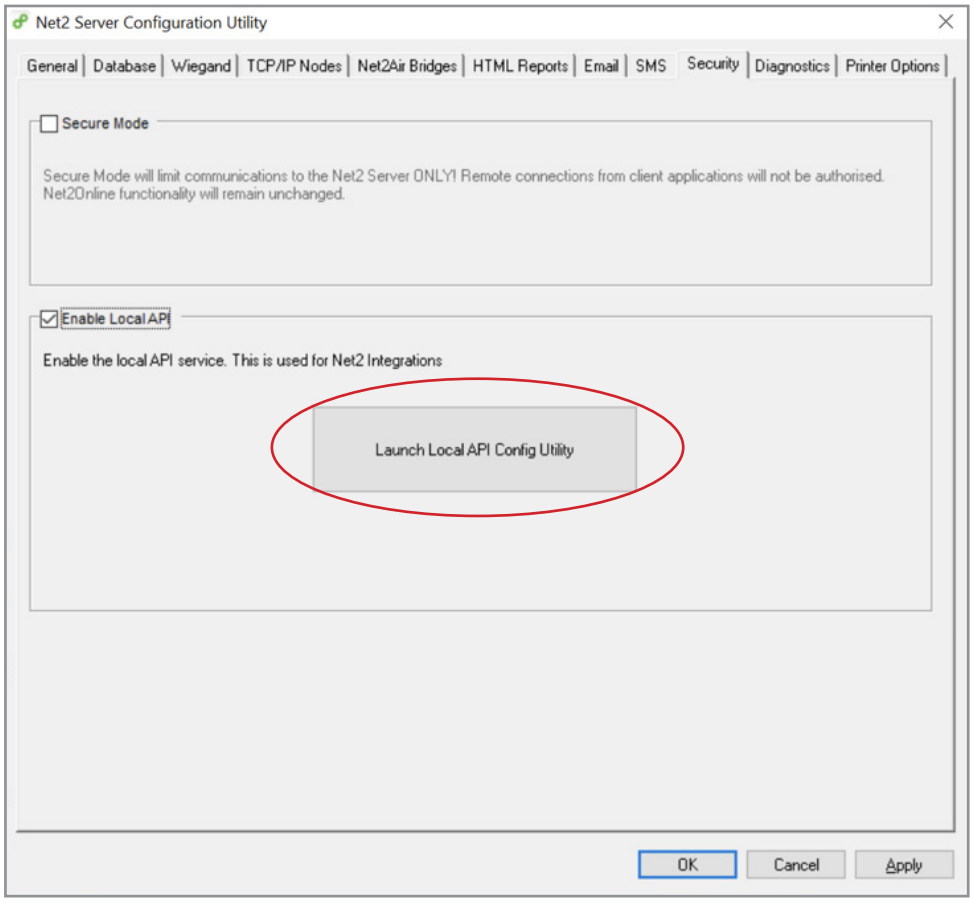
Option 2: Import your own certificate

This 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 receive a certificate and key.
2. Ensure you are on Net2 6.7 SR1 (or above).
3. Search and open the Net2 configuration utility.
4. Navigate to '**Security**' tab.

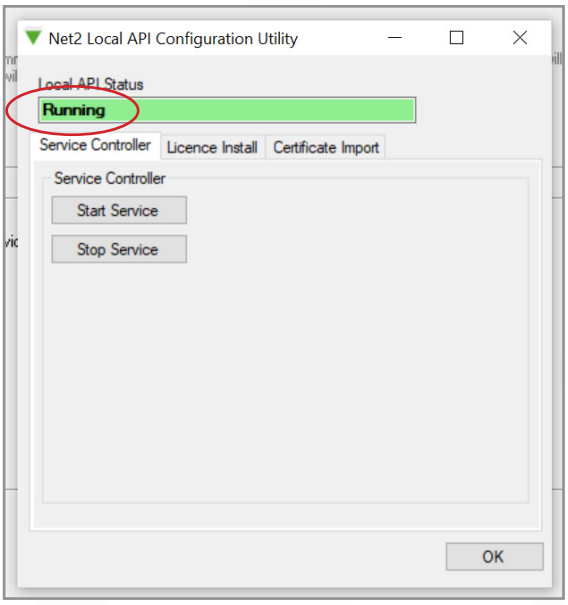


5. Click '**Launch Local API Config Utility**'.



6. The Local API Config Utility will launch.

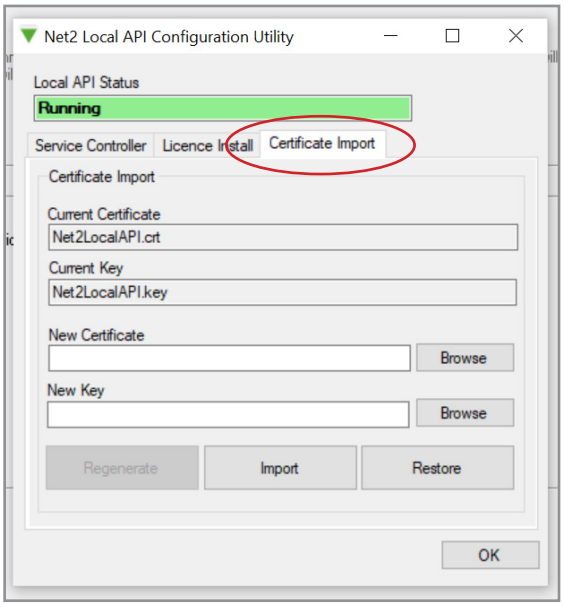
The Local API status should state '**Running**'.



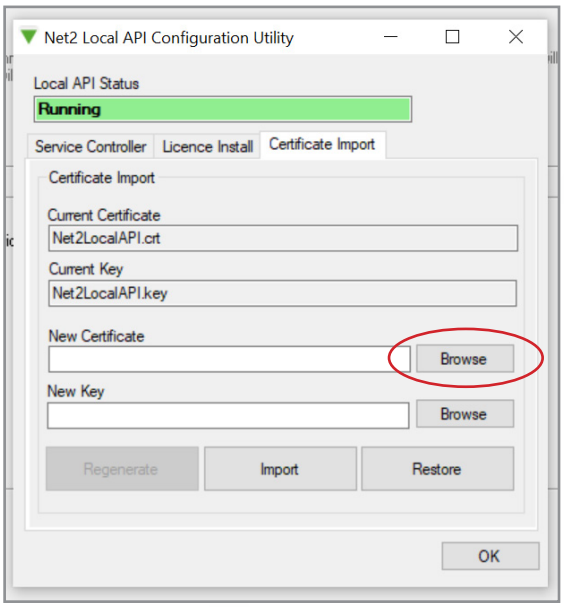
As the system does not have an integration running, there will be no licences under the licence importer tab. Please contact your integration partner for an API licence.

7. Navigate to '**Certificate Import**' tab.

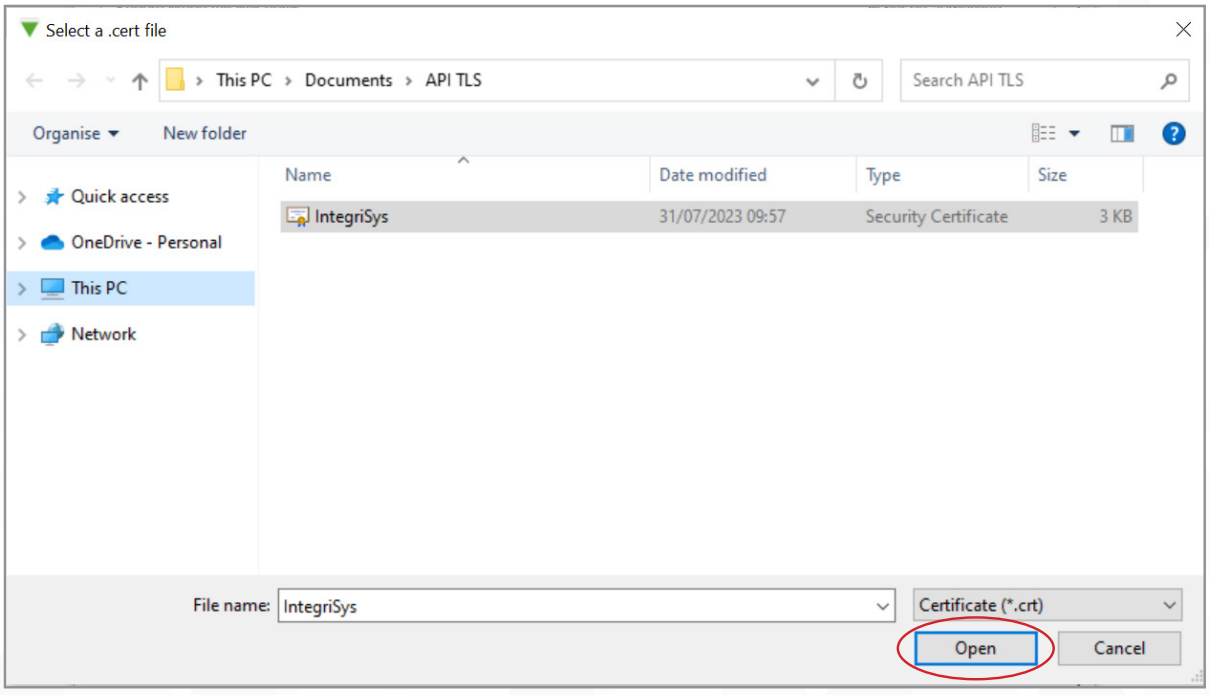
Note: Licence importer will show the existing licences for any integration that is running on the machine.



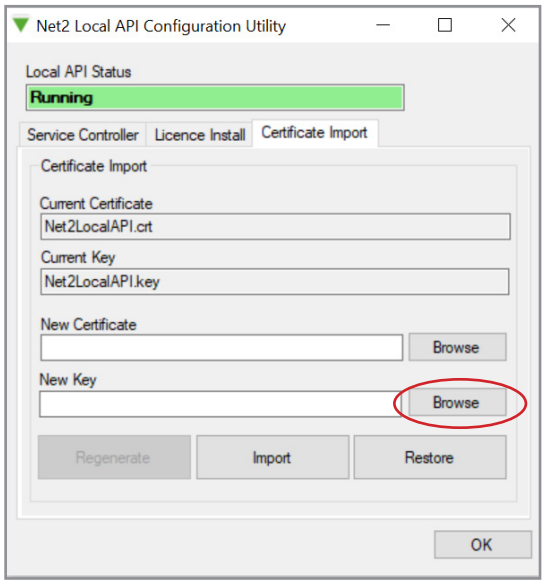
8. Click '**Browse**' for New certificate.



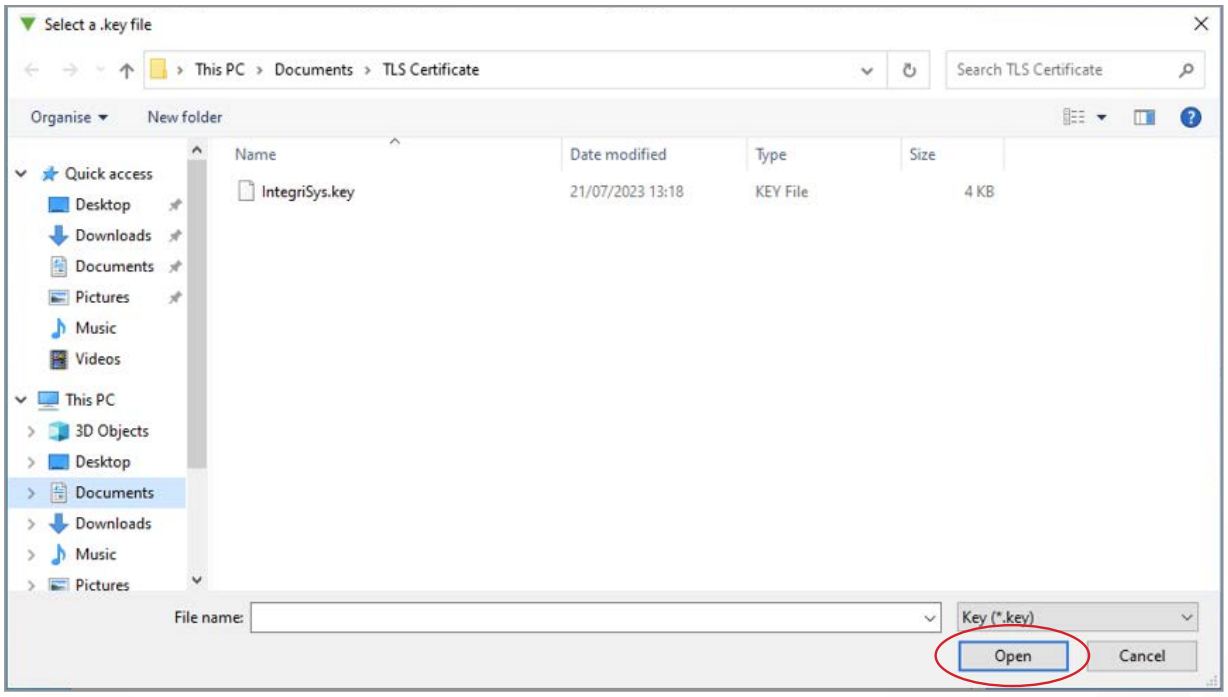
9. Locate the certificate and click '**Open**'.



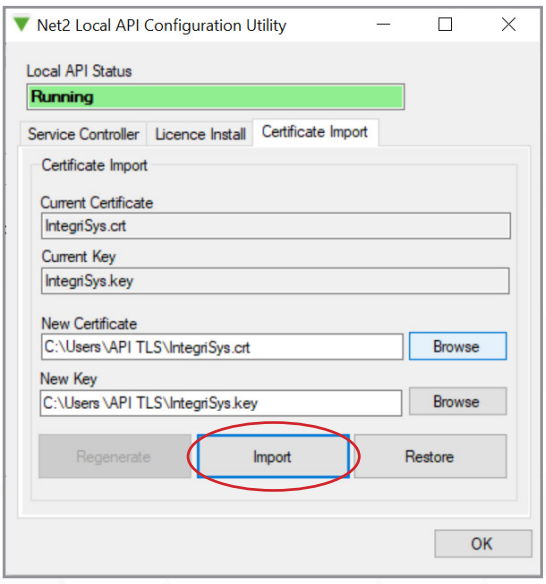
10. Click '**Browse**' for New Key.



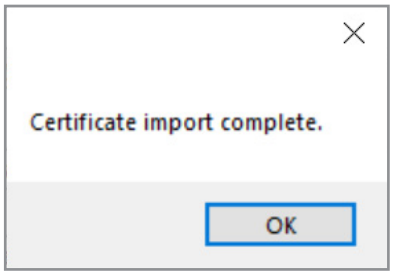
11. Locate the key and click '**Open**'.



12. Now click '**Import**'.



The import will complete.



The current certificate and current key will be updated.

The implementation is now complete.

Note: If the service status changes to '**Stopped**' following the import of your certificate and key, check the Nginx error log located at:

C:\Program Files (x86)\Paxton Access\Access Control\nginx\logs.

Within the logs you will be able to view where the error is.