Update von SSL/TLS-Zertifikat für bestehende Integrationen auf v6.7 SR1 (oder höher)

Paxton aktualisiert Net2 kontinuierlich, um ein hohes Maß an Cybersicherheit zu gewährleisten. Aus diesem Grund haben wir Änderungen am Zertifikatsverwaltungsprozess innerhalb der Software vorgenommen.

Bitte beachten Sie: Dies betrifft nur Integrationen, die unsere RESTful API verwenden, nicht aber Integrationen, die das SDK von Paxton Net2 nutzen. Für den Zugriff auf die lokale API über HTTPS ist ein SSL-Zertifikat erforderlich, um die sichere Verbindung herzustellen.

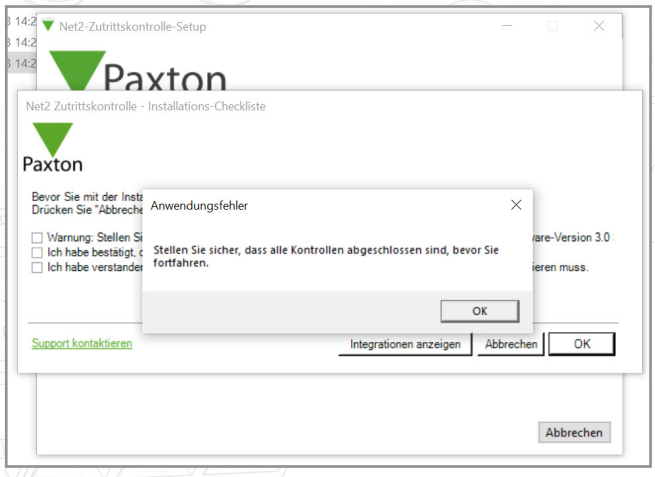
In unserer nächsten Version v6.7 SR1 müssen alle Integrationen ihre SSL-Zertifikate aktualisieren. Die Registerkarte „Zertifikatsmanager" wurde jetzt von der Seite localhost8080 entfernt und Paxton installiert nicht mehr automatisch ein SSL-Zertifikat im vertrauenswürdigen Stammverzeichnis.

Bitte stellen Sie sicher, dass Ihre Integration nur HTTPS verwendet, da HTTP nach dem Update auf v6.7 SR1 nicht mehr funktioniert.

Installieren eines selbstsignierten TLS-Zertifikats

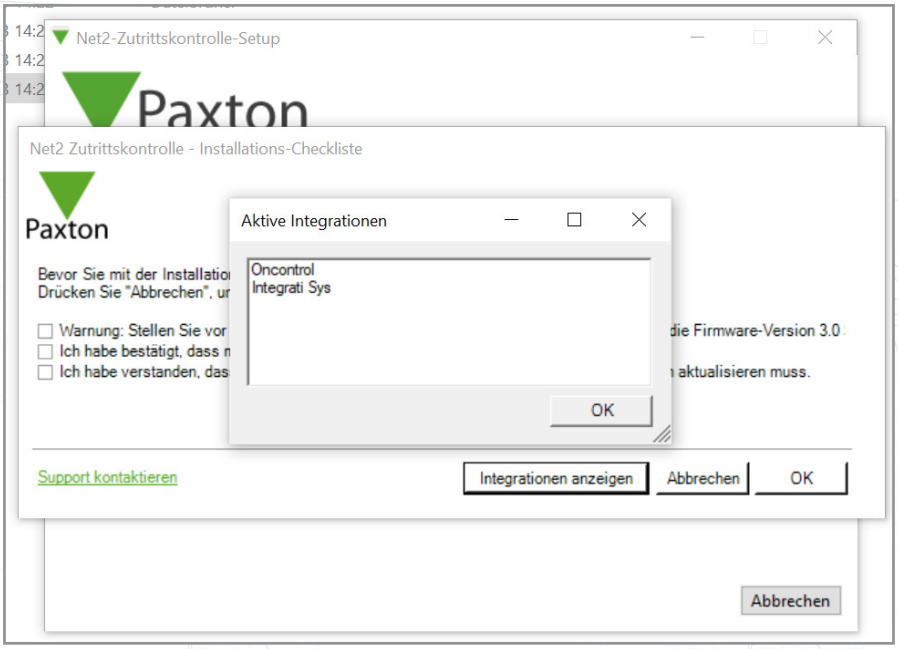
Damit eine Integration funktioniert und eine sichere Verbindung hergestellt werden kann, müssen Sie bei einem Update auf Net2 v6.7 SR1 oder höher ein selbstsigniertes TLS-Zertifikat installieren. Dieses sollte auf dem Server- und dem Client-Rechner installiert werden.

Vor der Aktualisierung von Net2 erhalten Sie die unten stehende Checkliste.

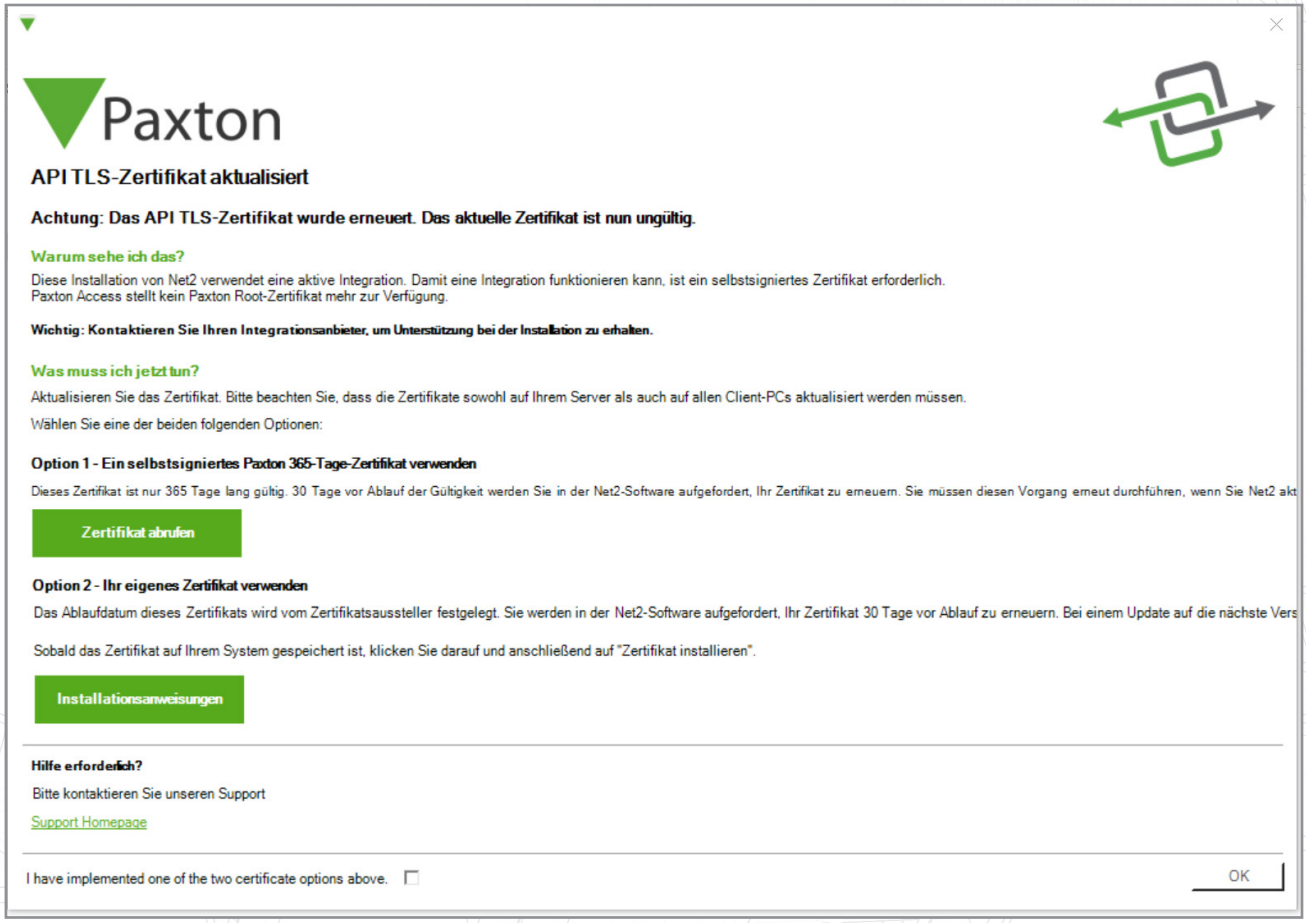


Kreuzen Sie alle Kästchen an und klicken Sie auf „Ok“, um fortzufahren.

Um die derzeit laufenden Integrationen zu überprüfen, klicken Sie auf „Integrationen anzeigen“.



Während der Aktualisierung wird der folgende Bildschirm angezeigt.



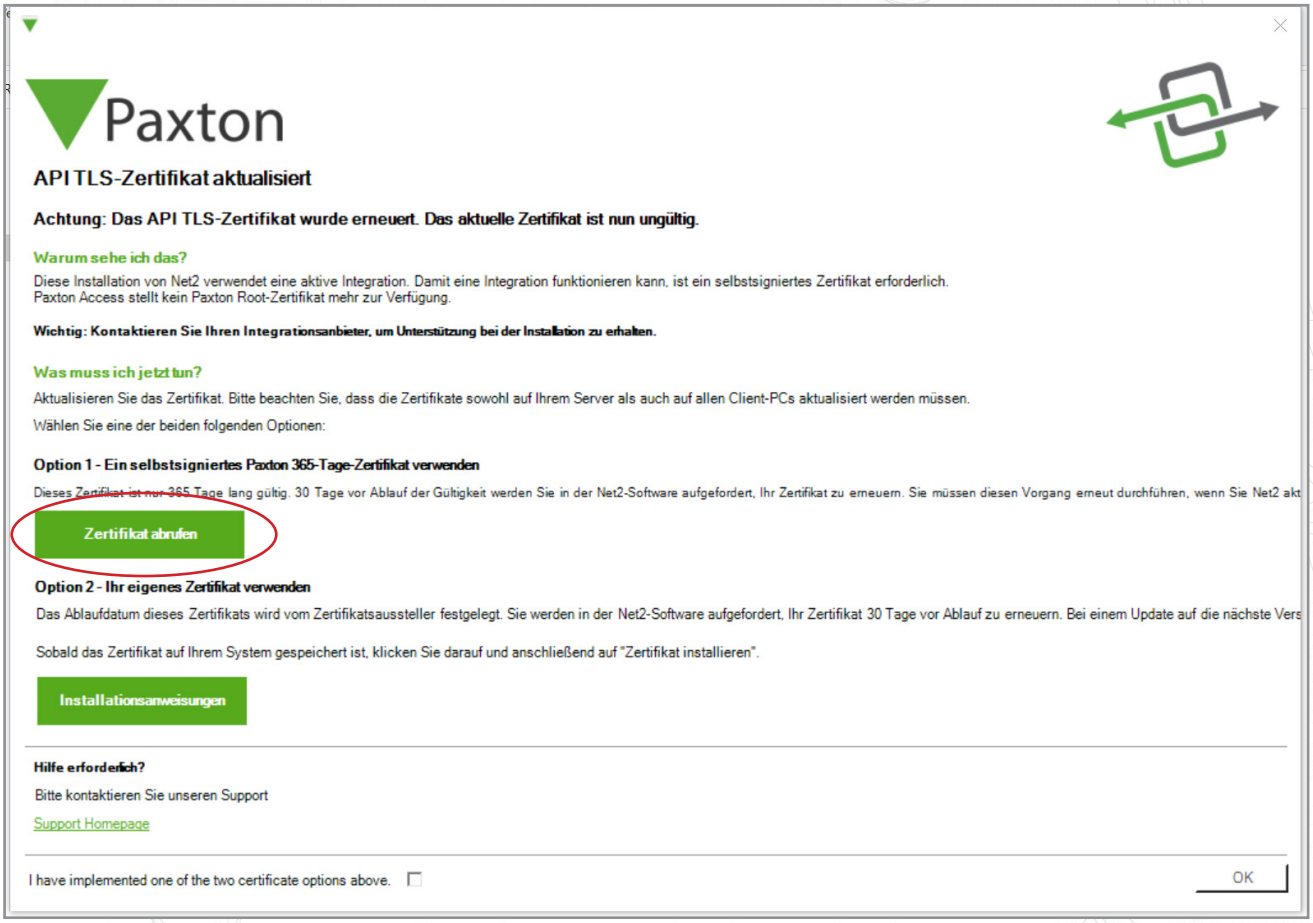
Bevor Sie die Installation von Net2 abschließen, müssen Sie eine der beiden angebotenen Zertifikatsoptionen auswählen und implementieren.

Hinweis: Wenn das Zertifikat während der Aktualisierung auf v6.7 SR1 nicht aktualisiert wird, funktioniert die Integration nicht länger.

Option 1: Ein selbstsigniertes Paxton 365-Tage-Zertifikat

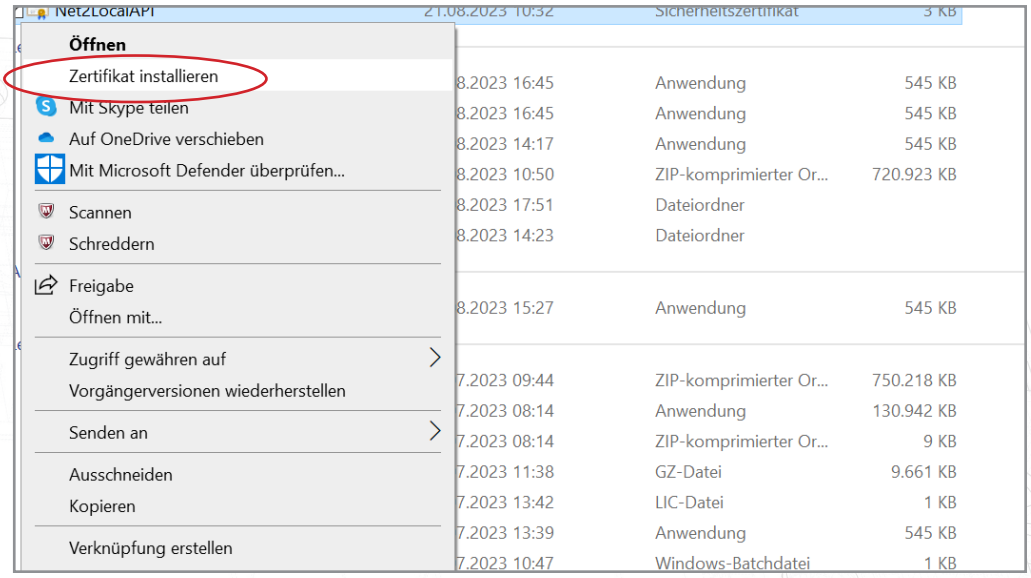
Dieses Zertifikat ist nur 365 Tage lang gültig. 30 Tage vor Ablauf der Gültigkeit werden Sie in der Net2-Software aufgefordert, Ihr Zertifikat zu erneuern. Sie müssen diesen Vorgang erneut durchführen, wenn Net2 aktualisiert wird.

1. Klicken Sie auf „Zertifikat abrufen“.

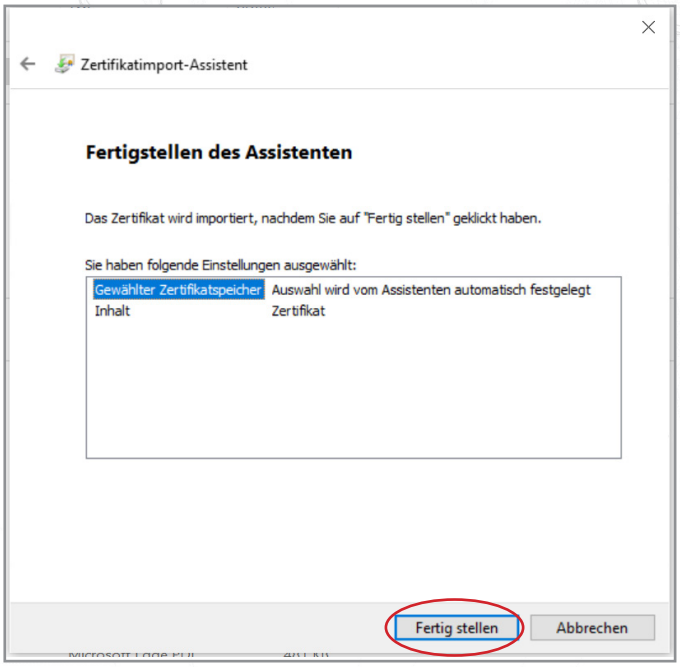


2. Das Zertifikat wird automatisch in den Ordner „Downloads“ installiert.

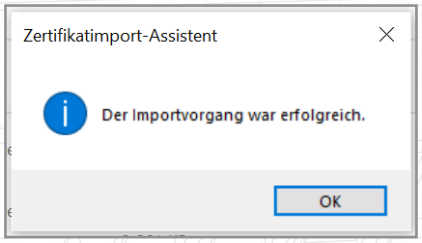
3. Öffnen Sie den Ordner „Downloads“.
4. Klicken Sie mit der rechten Maustaste auf das Zertifikat und dann auf „Zertifikat installieren“.



5. Wählen Sie die gewünschten Optionen innerhalb des Installationsprogramms.
6. Wenn Sie die Optionen ausgewählt haben, klicken Sie auf „Fertig stellen“.



7. Das Zertifikat wird installiert und der Importassistent meldet „Der Import war erfolgreich“.
8. Klicken Sie auf „OK“.

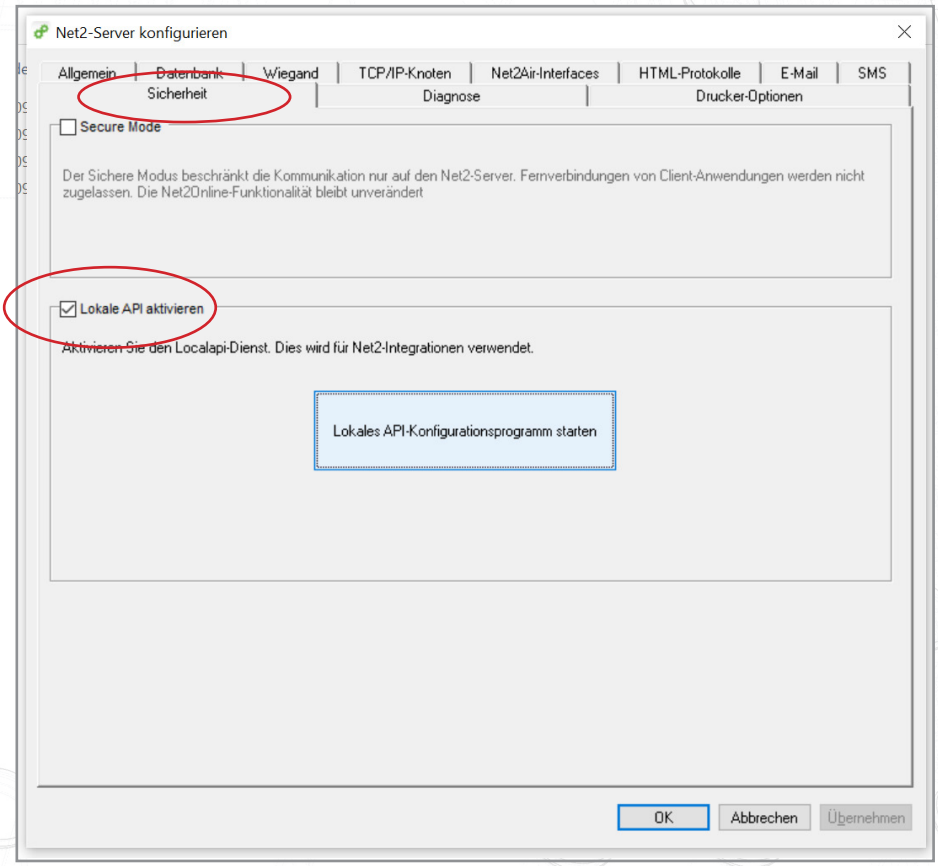


Die Aktualisierung ist nun abgeschlossen.

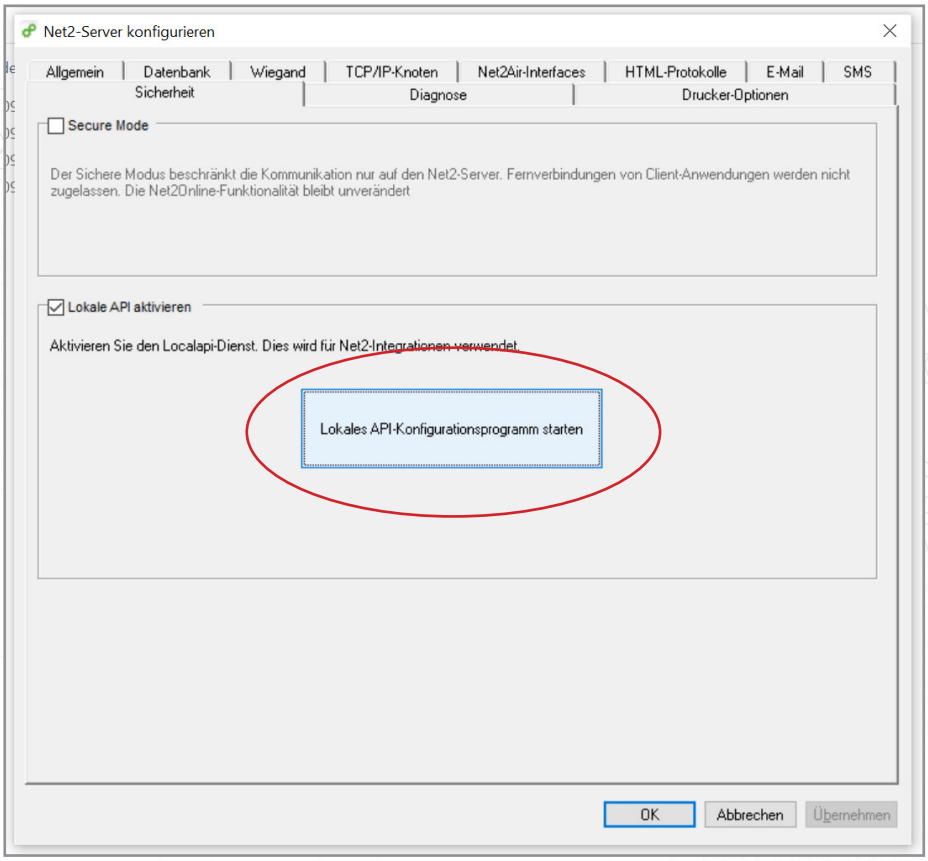
Option 2: Ihr eigenes Zertifikat importieren

Das Ablaufdatum dieses Zertifikats wird vom Zertifikatsaussteller festgelegt. Sie werden in der Net2-Software aufgefordert, Ihr Zertifikat 30 Tage vor Ablauf zu erneuern. Bei der Aktualisierung auf die nächste Version von Net2 müssen Sie dieses Zertifikat nicht aktualisieren.

1. Erstellen Sie Ihr eigenes Zertifikat mit einem TLS-Zertifikatsanbieter. Im Lieferumfang sollten ein Zertifikat und ein Schlüssel enthalten sein.
2. Aktualisieren Sie auf Net2 v6.7 SR1.
3. Suchen und öffnen Sie das Net2-Konfigurationsprogramm.
4. Navigieren Sie zur Registerkarte „Sicherheit".
5. Stellen Sie sicher, dass die lokale API aktiviert ist.

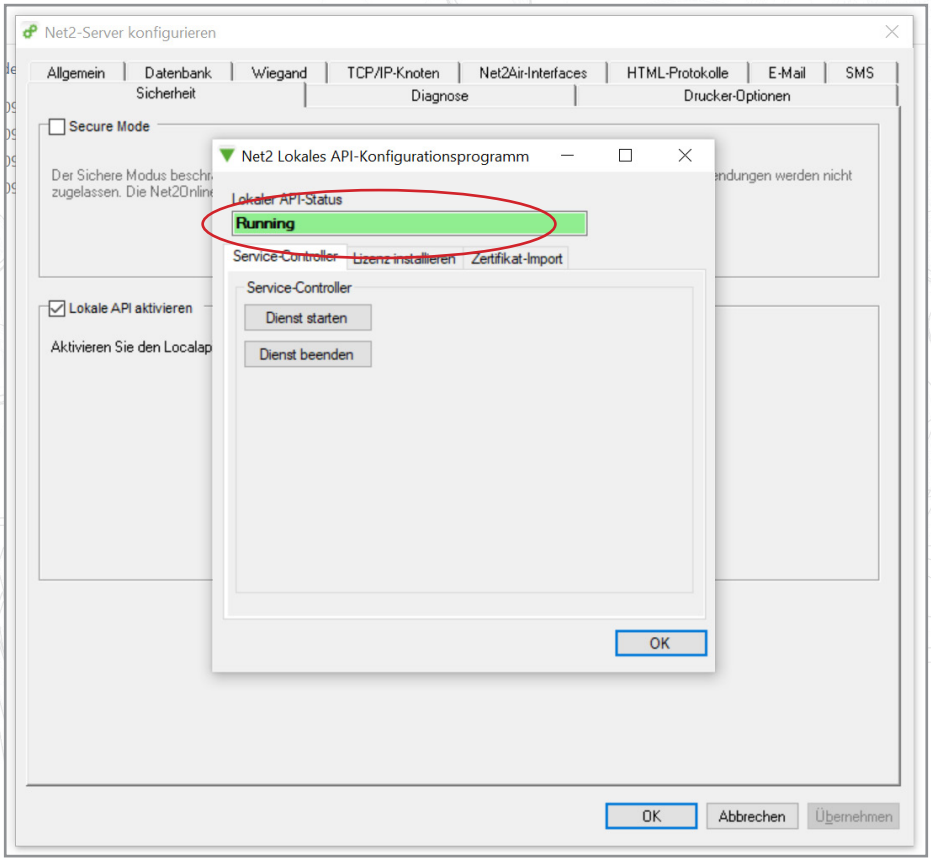


6. Klicken Sie auf „API-Konfigurationsdienstprogramm starten“.

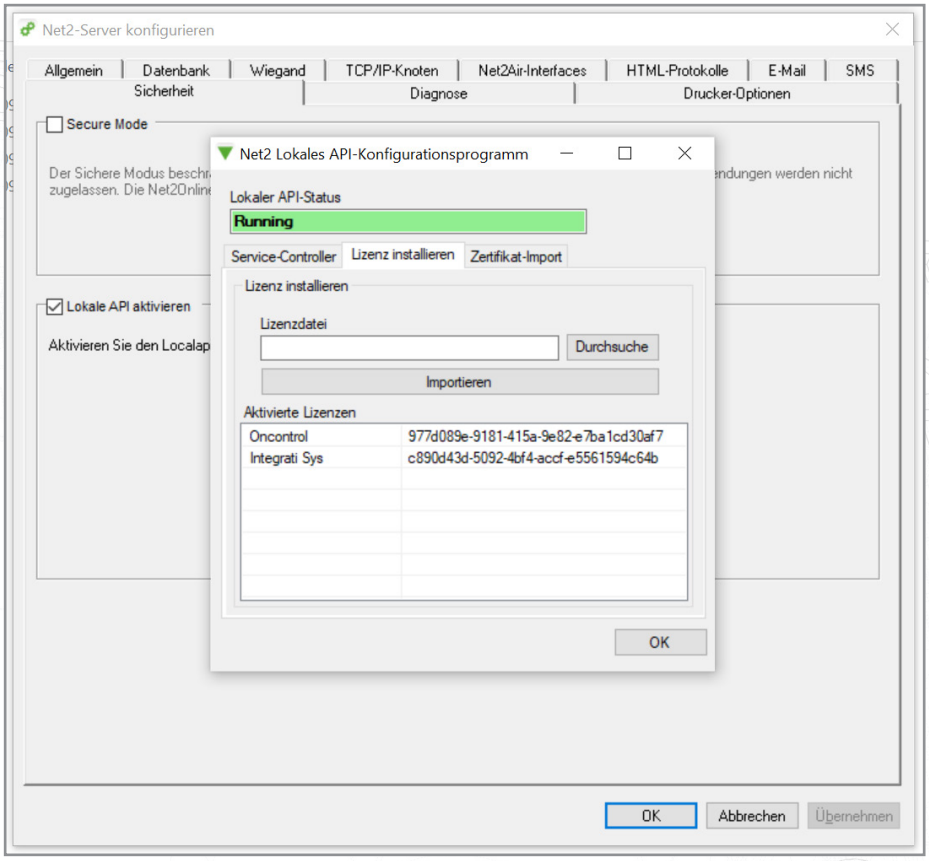


7. Das Dienstprogramm für die lokale API-Konfiguration wird gestartet.

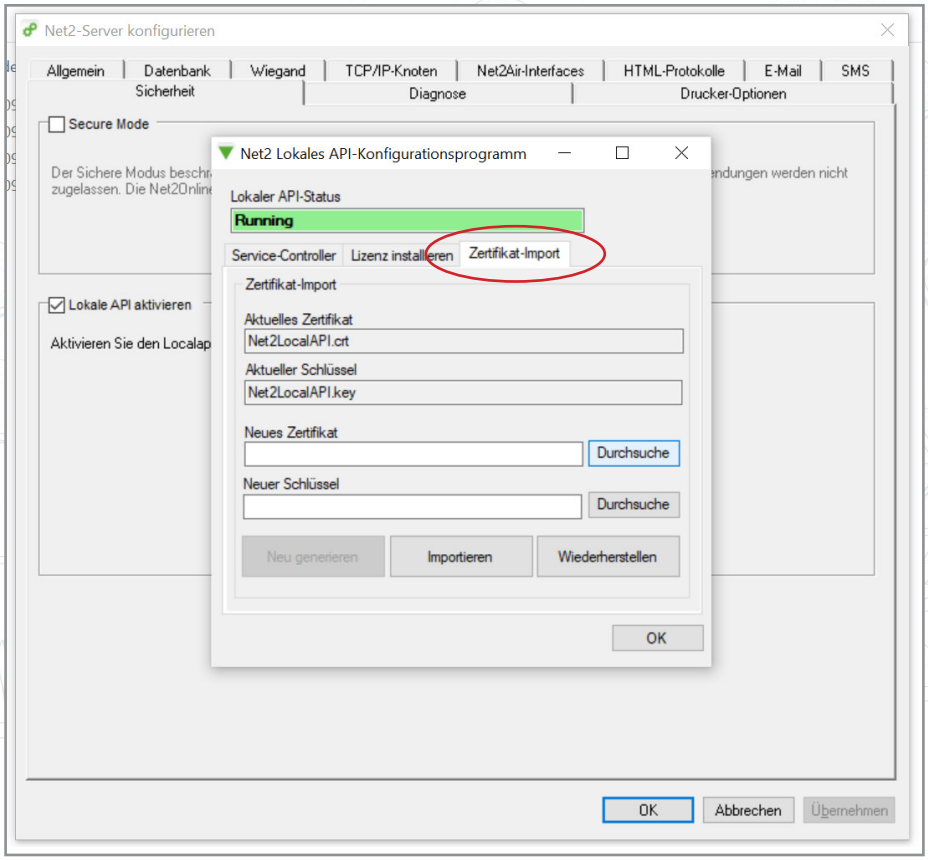
Der Status der lokalen API sollte „Läuft“ anzeigen.



Da das System über eine laufende Integration verfügt, ist es nicht erforderlich, eine Lizenz zu importieren. Auf der Registerkarte „Lizenzimport“ werden alle API-Lizenzen angezeigt, die derzeit verwendet werden.

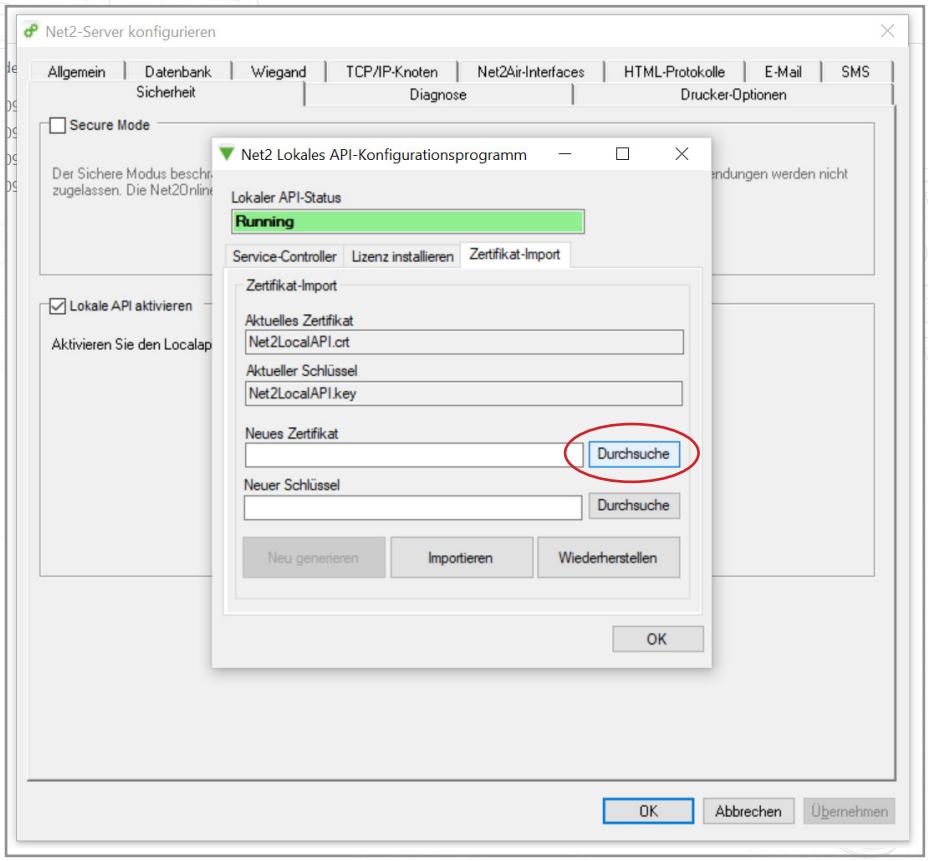


8. Navigieren Sie zur Registerkarte „Zertifikatsimporteur“.

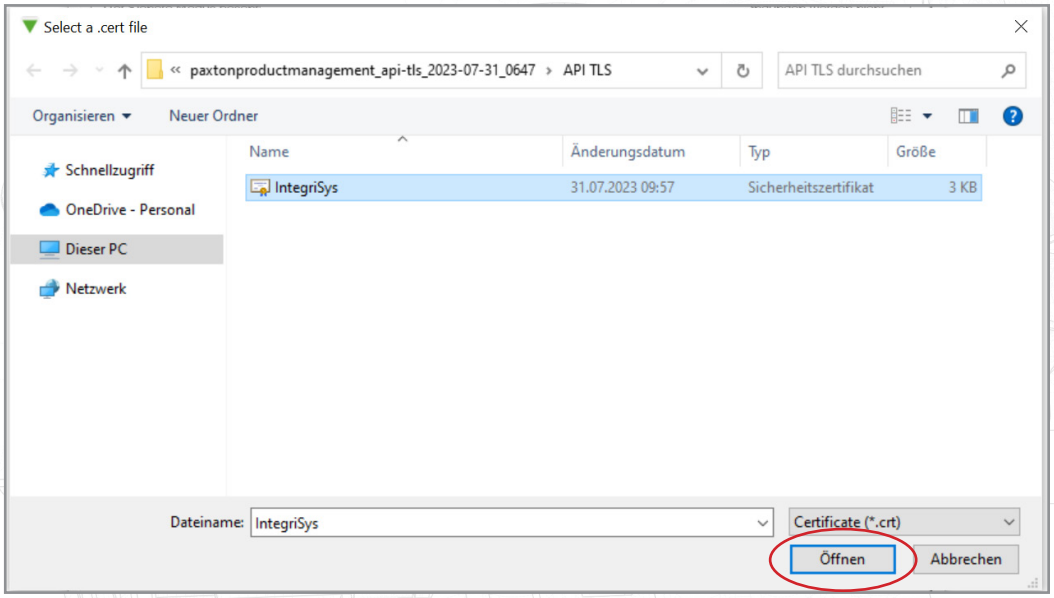


Hinweis: Der Lizenzimporteur zeigt die vorhandenen Lizenzen für alle auf dem Rechner laufenden Integrationen an.

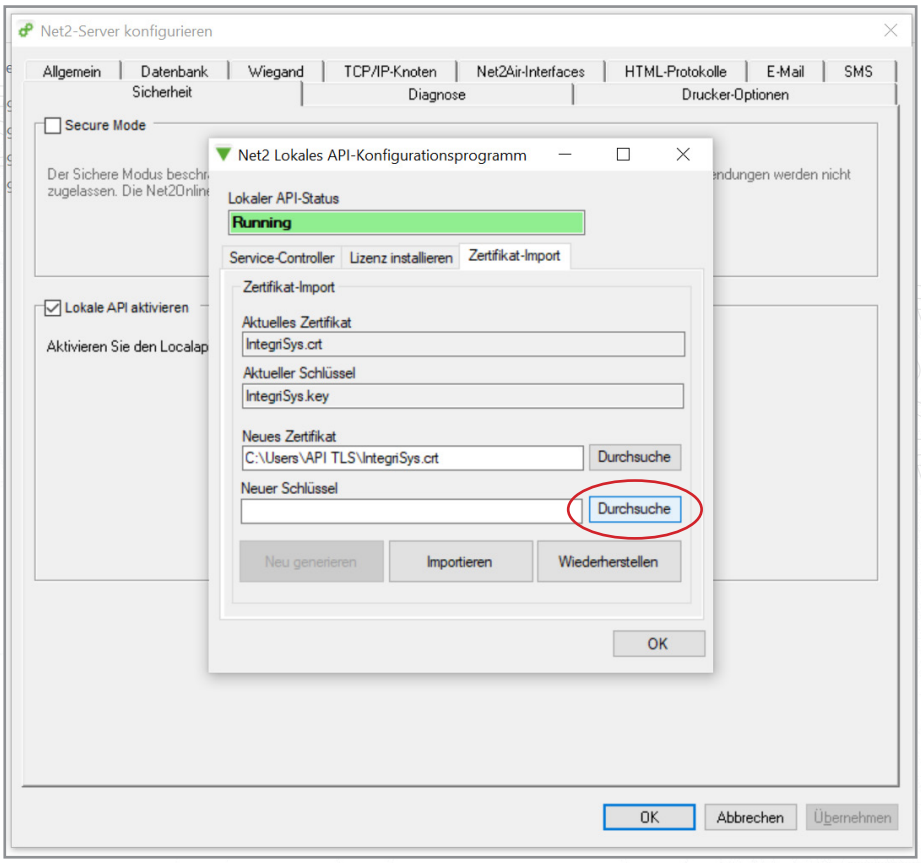
9. Klicken Sie auf „Durchsuchen“ für ein neues Zertifikat.



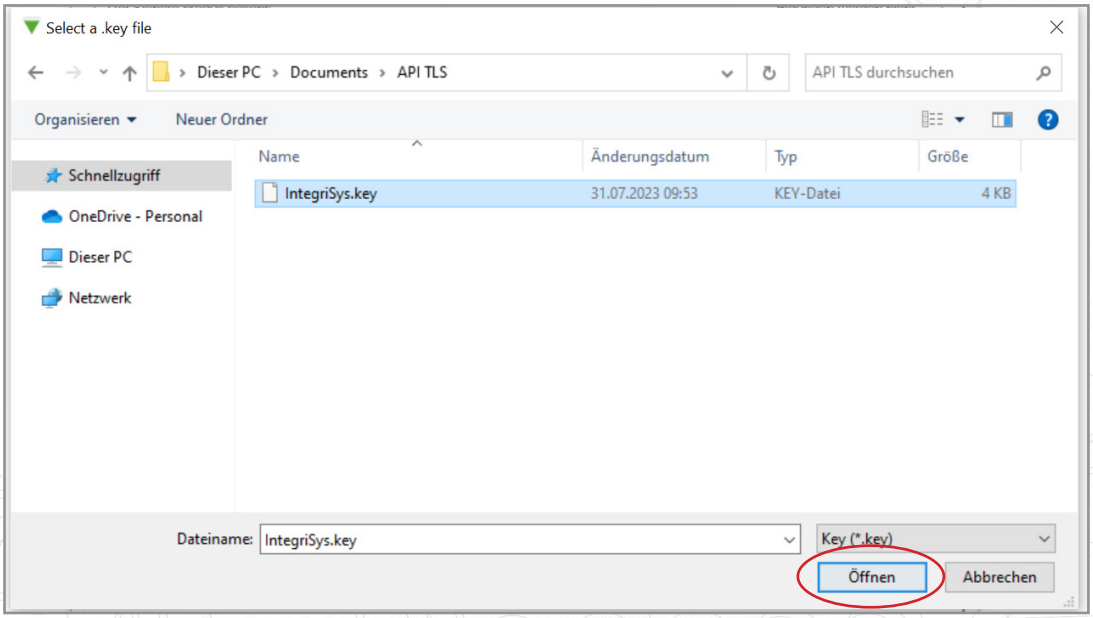
10. Suchen Sie das Zertifikat und klicken Sie auf „Öffnen“.



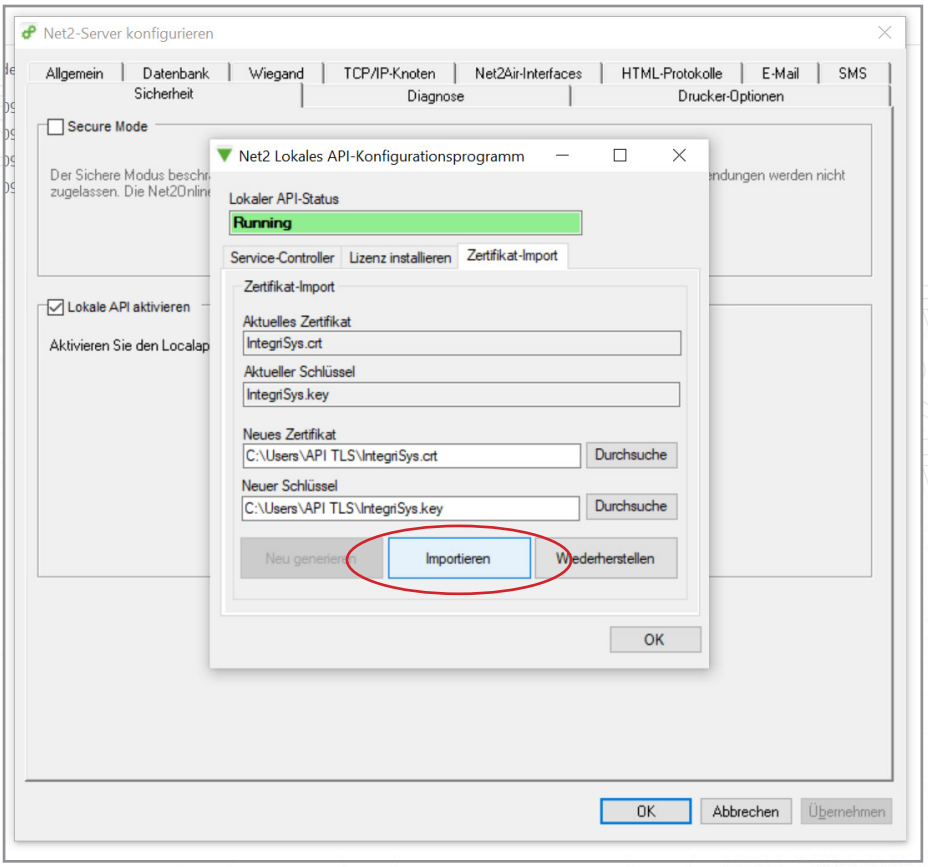
11. Klicken Sie auf „Durchsuchen“ für einen neuen Schlüssel.



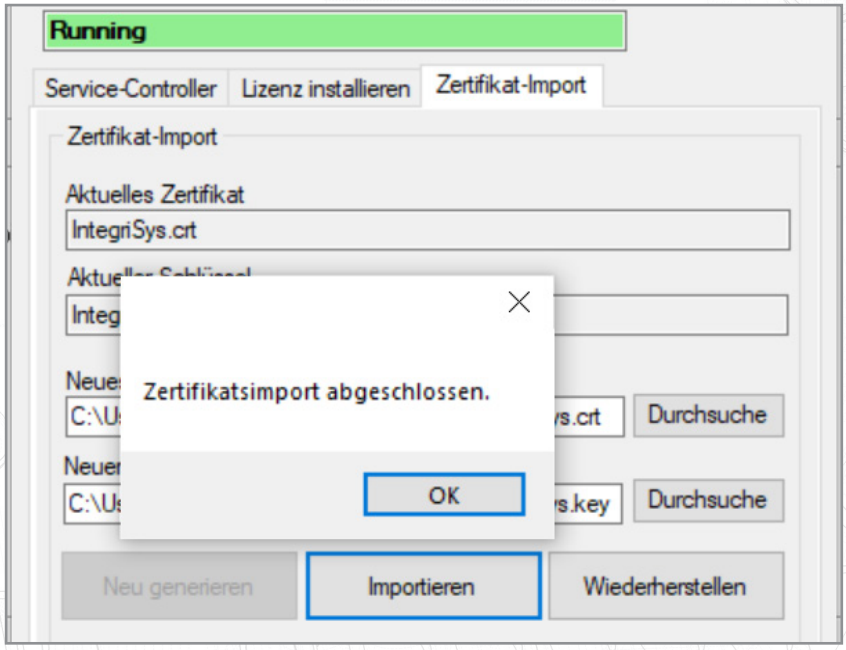
12. Suchen Sie den Schlüssel und klicken Sie auf „Öffnen“.



13. Klicken Sie nun auf „Importieren“.



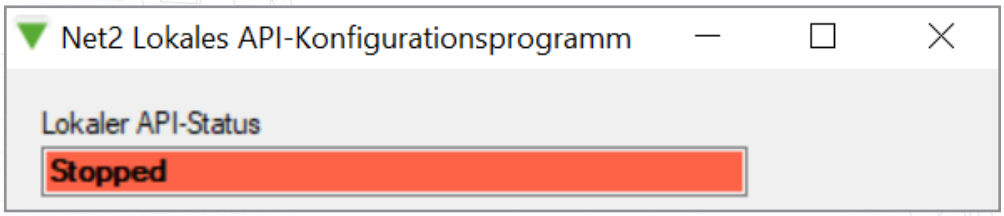
Der Import wird abgeschlossen.



Das aktuelle Zertifikat und der aktuelle Schlüssel werden aktualisiert.

Die Aktualisierung ist nun abgeschlossen.

Hinweis: Wenn sich der Status des Dienstes nach dem Import Ihres Zertifikats und Schlüssels auf „Angehalten“ ändert, überprüfen Sie das Ngnix-Fehlerprotokoll unter C:\Program Files (x86)\Paxton Access\Access Control\nginx\logs



Option 3: Zugriff auf die Anweisungen, wenn die API/TLS-Pop-up-Warnung nicht mehr angezeigt wird

1. Stellen Sie sicher, dass Ihre API-Verbindung aktiviert ist.
2. Öffnen Sie https://localhost:8080/setup.html
3. Klicken Sie auf „Download“, um selbstsignierte 365-Tage SSL-Zertifikate herunterzuladen.
4. Klicken Sie auf „Installationsanweisungen“, um einen Link zu den Installationsanweisungen zu erhalten.