LACCESS
ZukoServices

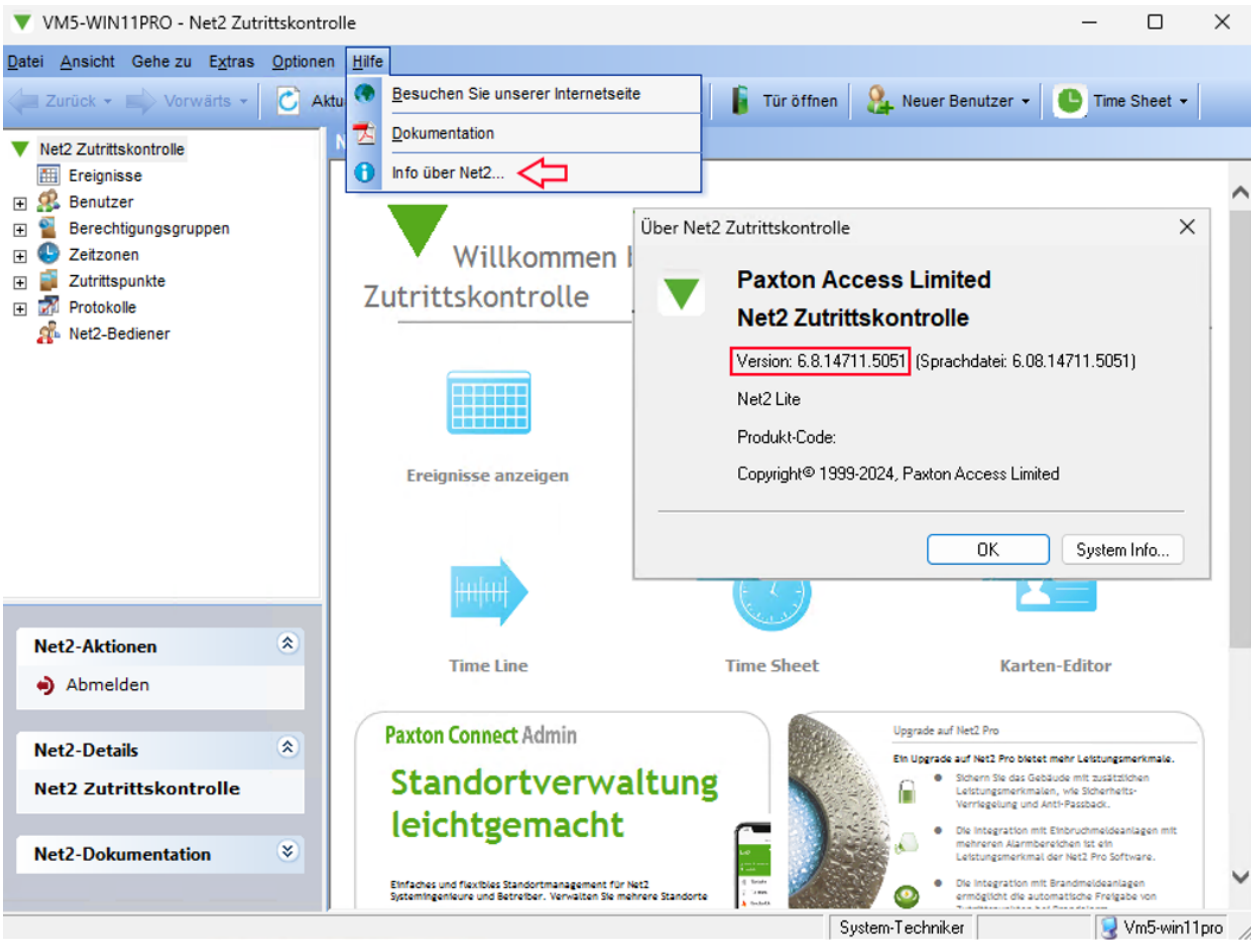
LACCESS GmbH S.Beckers
06.08.2025
V 1.81.0.0 (A.Moißl)

Inhaltsverzeichnis

Paxton Net2 – Voraussetzungen

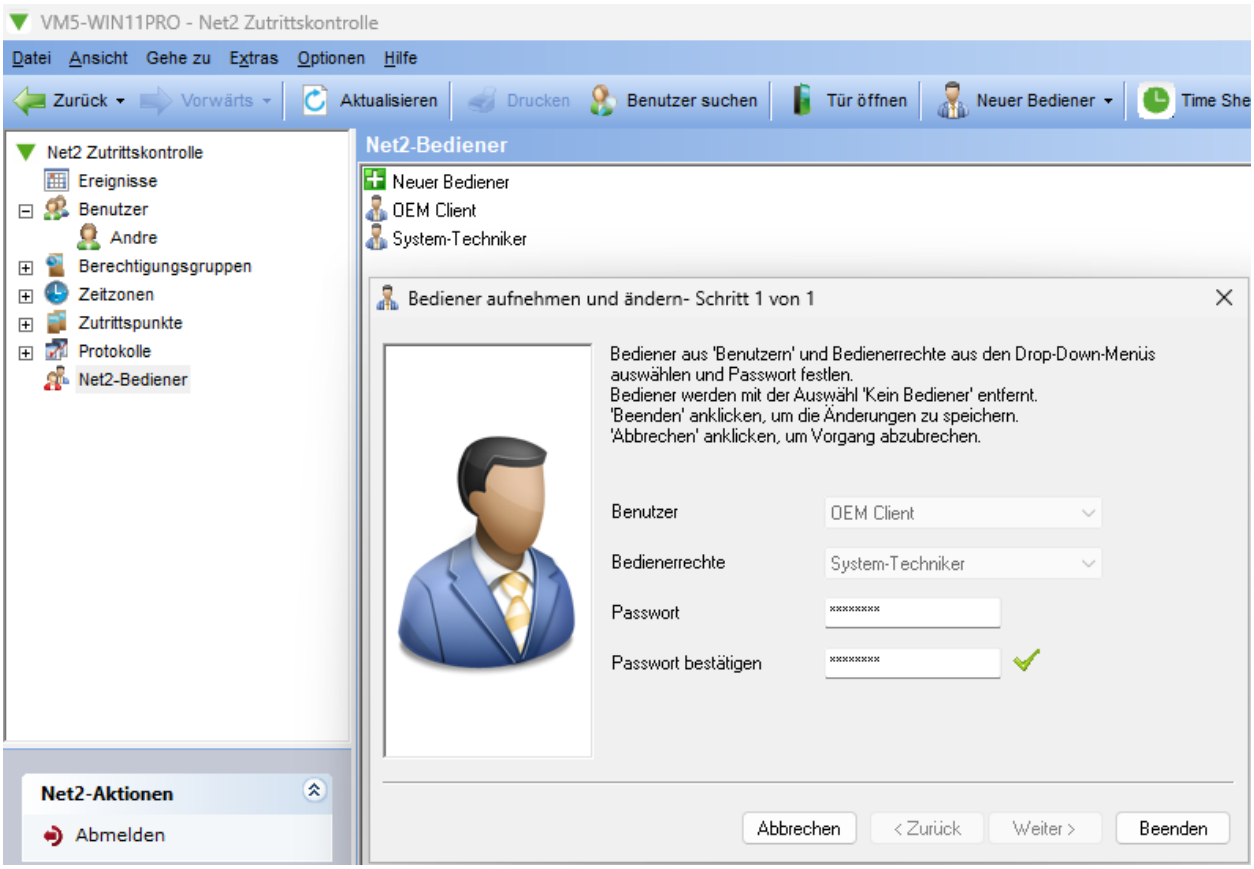
Versionsprüfung

Stellen Sie sicher, dass Paxton Net2 Access Control in Version V6.8.14711.5051 bereits installiert ist. Um die Versionsnummer anzuzeigen, starten Sie Paxton Net2, klicken auf „Hilfe“ und wählen anschließend „Info über Net2…“ aus.



Net2 API-Benutzer

Navigieren Sie zu **„Net2-Bediener“**, doppelklicken Sie auf den Benutzer „OEM Client“, legen Sie ein Passwort fest und klicken auf **„Beenden“**. Dieser Benutzer wird später benötigt, damit LACCESS ZukoServices über die API auf Paxton zugreifen kann. Wenn Sie lieber einen anderen Net2-Bediener verwenden möchten, stellen Sie sicher, dass dieser die Berechtigungsstufe „Jedereit an allen Zutrittspunkten“ besitzt.



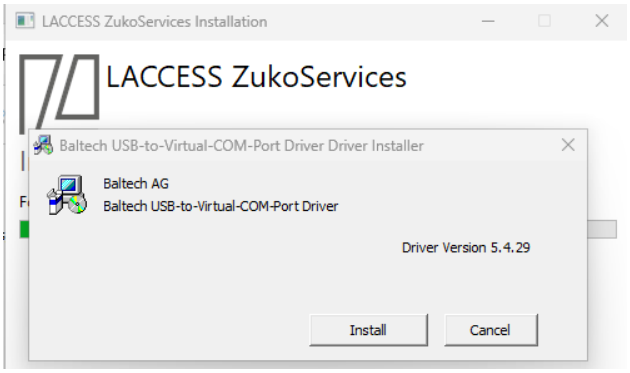
Jetzt können Sie die Net2 Access Control schließen.

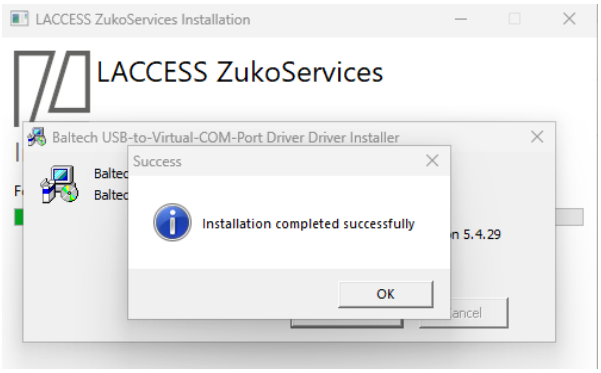
ZukoServices Installation

Starten Sie die Datei “LACCESS_ZukoServices_Setup_DE_v1.81.0.0.exe” vom mitgelieferten USB-Stick und folgen Sie den Anweisungen. Das Setup installiert neben der ZukoServices Software folgende Programme:

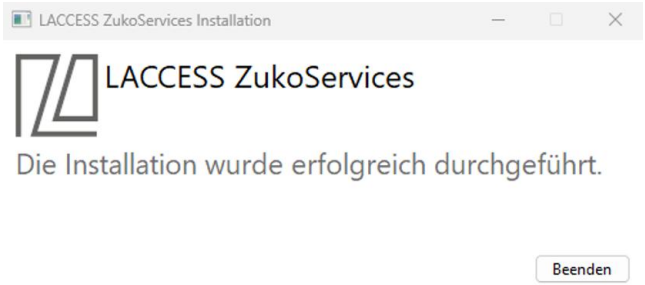
1. Grafana - Eine Software zur Verwaltung von Log Einträgen
2. SQL Express 2020 - Datenbank
3. SimonsVoss SmartIntego - Software zur Konfiguration von SimonsVoss Wireless Online Geräten
4. SimonsVoss SmartIntego VCN - Software zur Konfiguration von SimonsVoss VCN (Virtual Card Network) Geräten
5. Feig Discovery Reader - Tool zur Konfiguration von Feig NFC Readern
6. SimonsVoss OAM Tool - Tool zur Konfiguration der Wireless Online Gateways

Sobald dieses Dialogfenster erscheint, klicken Sie auf „Installieren“ und anschließend auf „OK“.





Die Installation ist nun abgeschlossen. Klicken Sie auf „Beenden“.



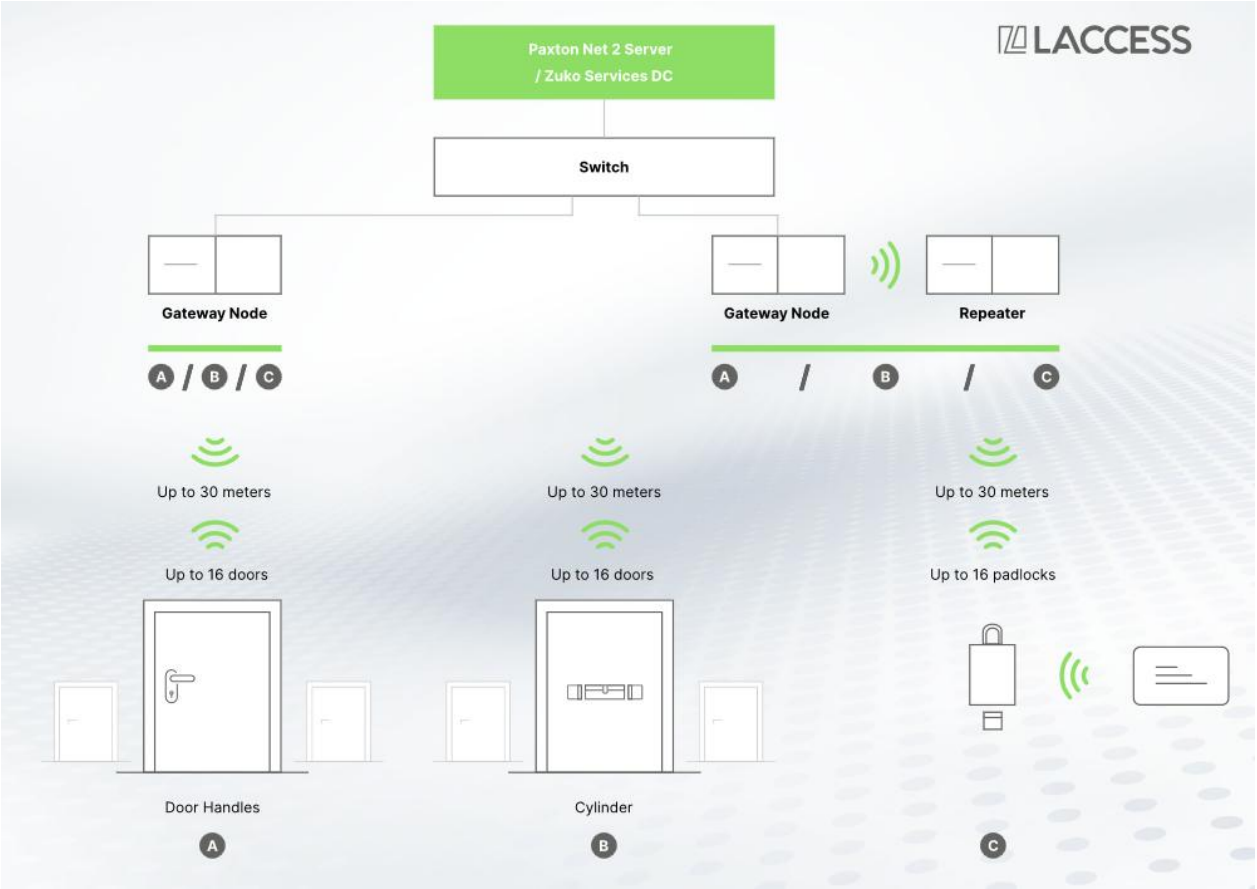
Bitte starten Sie nun Ihren Server neu.

SmartIntego Wireless Online

Komponenten

Das SimonsVoss Wireless Online System besteht aus folgenden Komponenten:

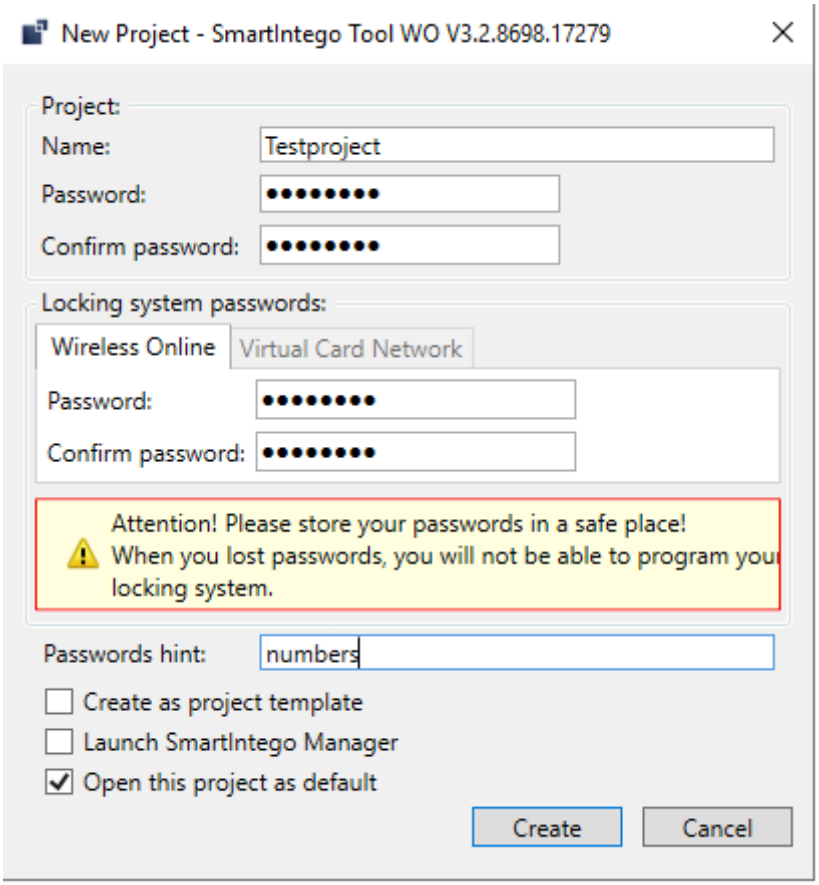
- Lock Node: Lock Nodes sind Drücker und Zylinder, die an den Türen verbaut werden.
- Gateway Node: Hierbei handelt es sich um ein Steuergerät, welches Zylinder über die Funkstrecke steuert. Zylinder melden Ereignisse an das Gateway, das Gateway sendet Befehle (z.B. Tür öffnen) an die Zylinder.
- ZukoServices: Die Gateway Nodes senden Events an das ZukoServices System. ZukoServices wertet diese Ereignisse aus und sendet Befehle an das Gateway Node. Eine Gateway Node kann bis zu 16 Lock Nodes bedienen.
- Paxton Net2: ZukoServices bezieht Informationen zur Ergebnisauswertung aus dem Zutrittskontrollsystem Paxton Net2. Es werden u.a. Token, Benutzer, Benutzergruppen und Zutrittspunkte ausgelesen.



Konfiguration

Projekt erstellen

Gateway Nodes und Lock Nodes werden über die SmartIntego Software in einer Projektdatei konfiguriert. Öffnen Sie dafür das Programm SmartIntego und legen Sie ein neues Projekt an.



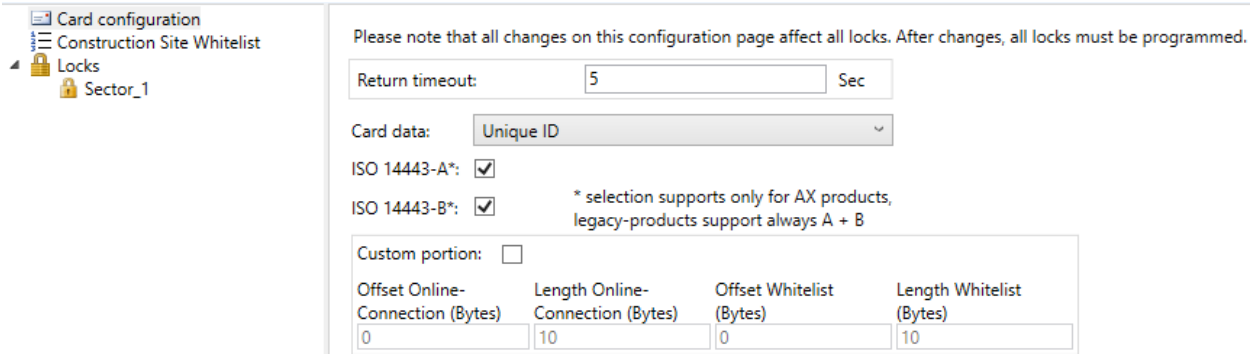
Name	Name des Projektes
Password	Passwort zum Öffnen des Projektes (das Passwort muss mindestens 8 Stellen haben und sollte einen Groß- und einen Kleinbuchstaben sowie eine Zahl oder Sonderzeichen beinhalten).

Confirm Password	Bestätigung des Passworts
Wireless Online Password	Mit diesem Passwort werden die Lock Nodes verschlüsselt. Mit diesem Passwort ist es möglich, Geräte zurückzusetzen. Das Passwort muss mindestens 8 Stellen haben und darf nicht identisch mit dem Projektpasswort sein.
Wireless Online Confirm Password	Bestätigung des Passworts
Passwords hint	Passworthinweis

Bewahren Sie Passwörter zuverlässig und sicher auf. Passwörter können nicht zurückgesetzt werden. Der Verlust der Passwörter führt dazu, dass Projektdateien nicht mehr geöffnet werden und Lock Nodes nicht mehr verwendet werden können!

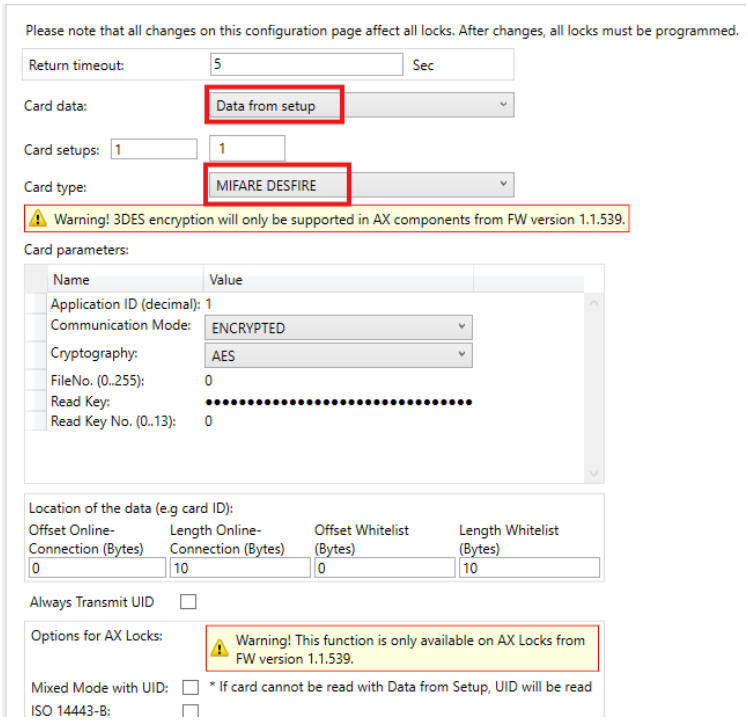
Nach der Erstellung des Projekts mit einem Klick auf „Create“, wird dieses geöffnet. Die Einstellungen unter dem Punkt „Card Configuration“ bestimmen, wie die Lock Nodes einen NFC-Token lesen. Unter dem Punkt „Card Data“ wird festgelegt, ob die Unique ID oder die Verschlüsselung eines Tokens “Data from setup” verwendet werden soll.

Die Einstellung für die Verwendung der Unique ID sieht wie folgt aus:



(Optional) Die Einstellungen für die Verwendung der Tokenverschlüsselung sehen wie folgt aus:

Die Einstellungen der „Data from setup“-Option sollten von fachkundigen Personen vorgenommen werden. Alle Einstellungen der „Card Configuration“ sollten vor der Anlage der Gateway Nodes und Lock Nodes vorgenommen werden. Werden Änderungen nachträglich vorgenommen, müssen diese auf den Lock Nodes neu programmiert werden.



Nachdem Sie sich für eine Option entschieden haben, speichern Sie das Projekt in einem Ordner, den Sie wiederfinden. Der Standard-Ablageort lautet: C:\Benutzer\Öffentlich\Öffentliche Dokumente\SimonsVoss\SmartIntego.

Hinzufügen einer Gateway Node

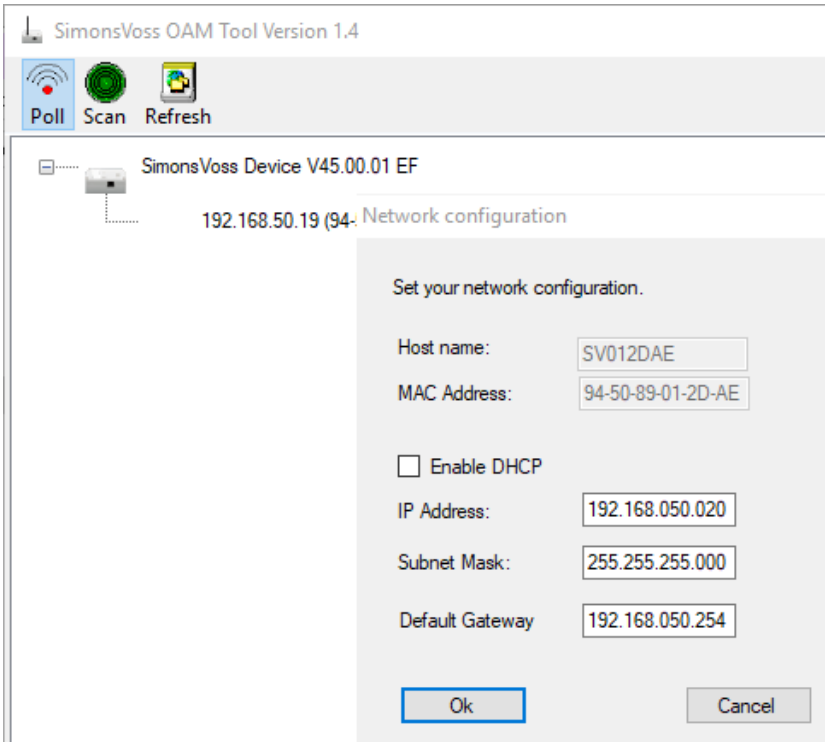
Einrichtung der Gateway Node

Montieren Sie die Gateway Node an einem geeigneten Ort und schließen Sie diese an einen PoE Switch an.

Damit Sie die Nodes später zuordnen können, sollten Sie sich die ChipID notieren. Diese finden Sie auf der Rückseite der entsprechenden Gateway Node.

Öffnen Sie das Programm SimonsVoss OAM. Dieses finden Sie im Ordner C:\Program Files\LACCESS ZukoServices\SimonsVoss. Bitte achten Sie darauf, dass die Windows Firewall entsprechend konfiguriert oder ausgeschaltet ist.

Sie finden nun innerhalb der Software die gefundenen Gateway Nodes. Klicken Sie mit der rechten Maustaste auf die Gateway Node und gehen Sie auf **„Set IP“**. Stellen Sie nun die gewünschte IP Adresse ein.



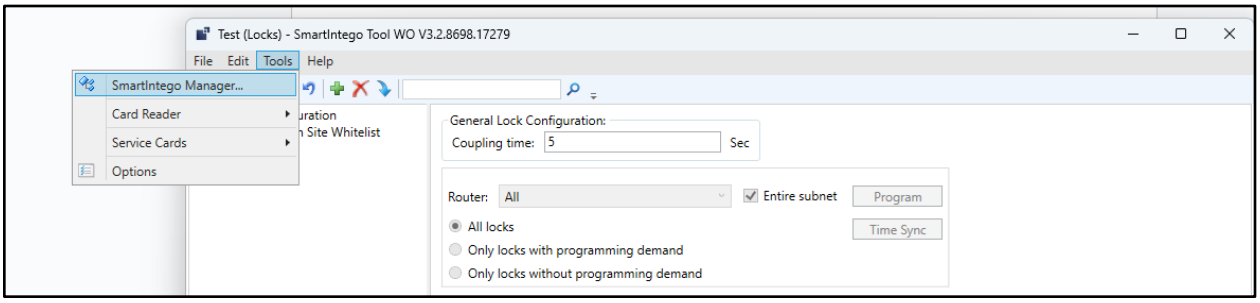
Die Gateway Node sollte bestenfalls im gleichen Netzwerk sein wie die ZukoServices Software. Die Gateway Node wird über eine Weboberfläche konfiguriert. Ermitteln Sie die IP-Adresse des Gerätes und rufen Sie diese über den Browser auf (z.B. https://192.168.178.10). Je nach verwendetem Browser bestätigen Sie Zertifikatswarnungen mit „Erweitert“ und „Weiter zu xxx (unsicher)“ oder einer ähnlichen Option. Melden Sie sich mit dem Standard Benutzer “**SimonsVoss**” und dem Passwort “**SimonsVoss**” an.

Unter dem Menüpunkt “Konfiguration” haben Sie die Möglichkeit weitere Netzwerkeinstellungen vorzunehmen. Sie sollten außerdem das Standardpasswort ändern. Öffnen Sie dazu den Menüpunkt “Administration”.

Es ist außerdem empfehlenswert ein AES Passwort zu vergeben. Dieses Passwort verschlüsselt die Netzwerkkommunikation zwischen dem Gateway Node und der ZukoServices Software. Öffnen Sie dazu den Menüpunkt “Administration” → “AES” und vergeben Sie ein Passwort.

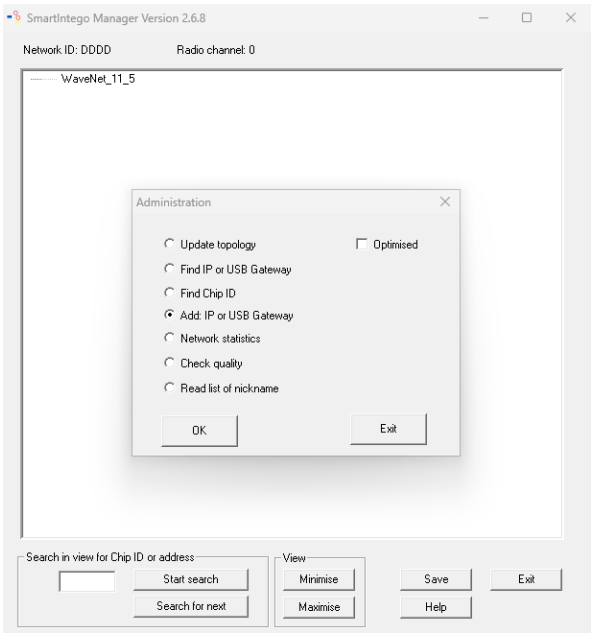
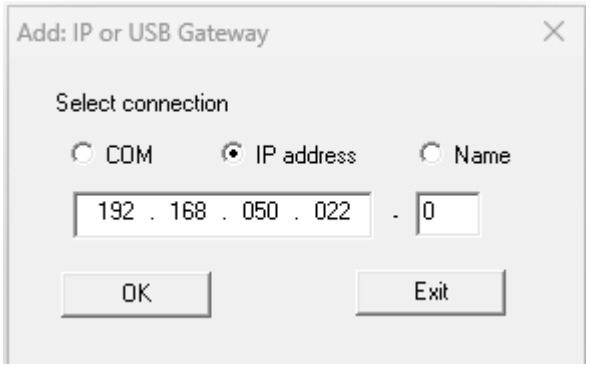
Einbindung in SmartIntego

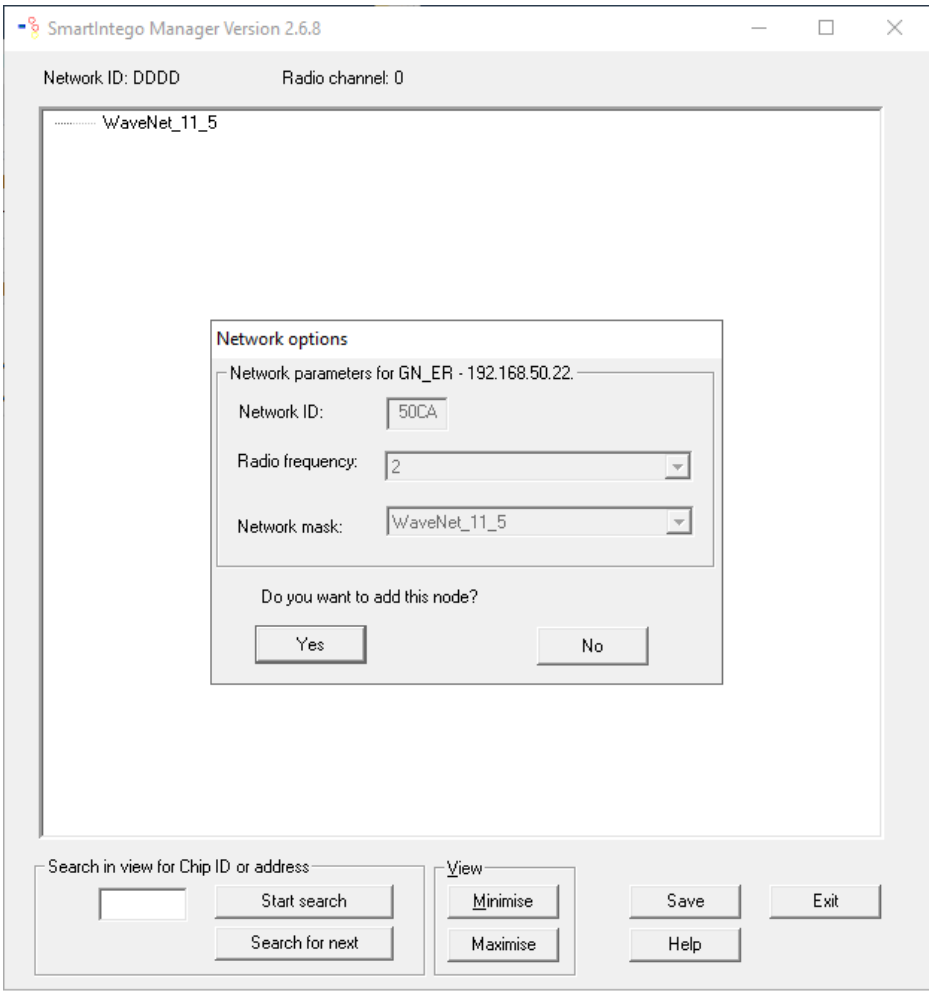
Wechseln Sie in das Programm SmartIntego. Öffnen Sie den SmartIntego Manager unter “Tools”→ “Smartart Intego Manager”.



Wenn Sie es zum ersten Mal öffnen, legen Sie das WaveNet-Passwort fest. Es darf maximal 8 Zeichen lang sein. Sie dürfen sich nicht vertippen, da es nur einmal eingegeben wird.

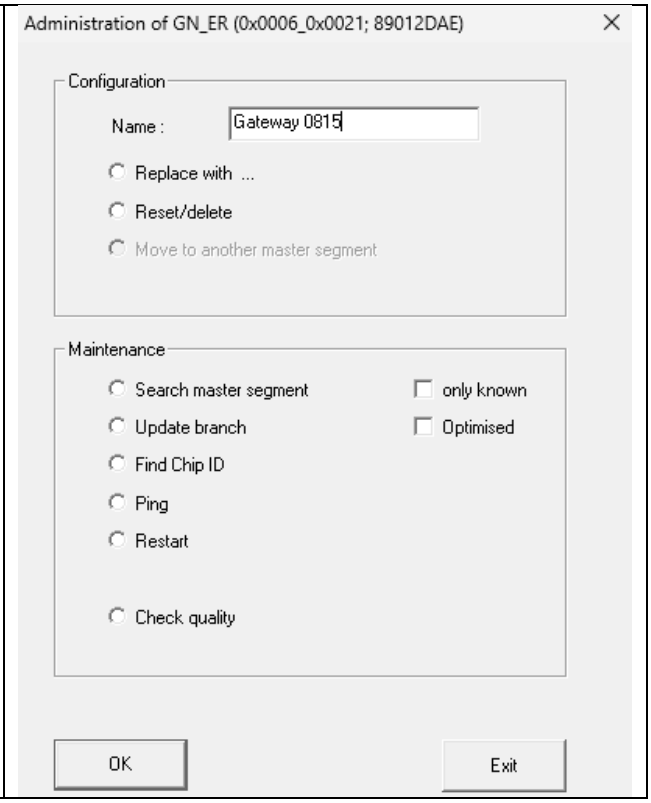
Gehen Sie auf Nummer sicher und schließen Sie den SmartIntego Manager mit **„Exit“**. Starten Sie ihn anschließend neu („Tools“ → „SmartIntego Manager“) und geben Sie das Passwort erneut ein, um sicherzustellen, dass es korrekt und ohne Tippfehler gesetzt wurde.

Klicken Sie im Anschluss mit der rechten Maustaste auf WaveNet. Es erscheint ein Dialog, in dem Sie “Add: IP or USB Gateway” wählen und mit “OK” bestätigen.	
Geben Sie die IP-Adresse des Gerätes ein und bestätigen Sie mit “OK”. Mit der zweiten Zahl (-0) können Sie auch eine Range einstellen. Hiermit können Sie mehrere Gateway Nodes gleichzeitig hinzufügen.	



Drücken Sie anschließend auf “Yes”.

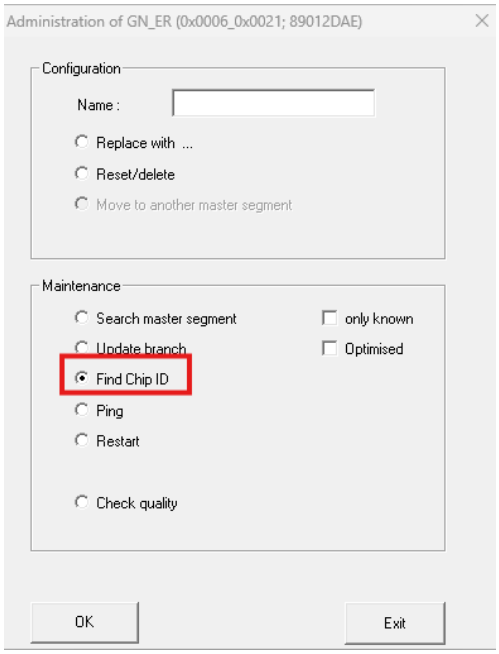
Im Anschluss erscheint das Gateway Node in der Auflistung. Speichern Sie Ihre Eingaben!

Optional können Sie dem Gateway einen Namen zuweisen. Klicken Sie dazu mit der rechten Maustaste auf das Gateway, geben einen Namen ein und klicken auf „OK“.	

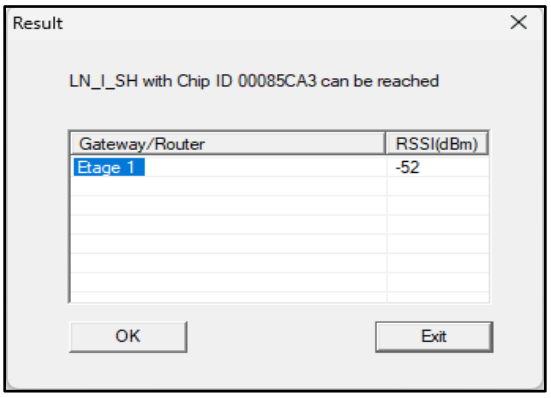
Hinzufügen einer Lock Node (Zylinder)

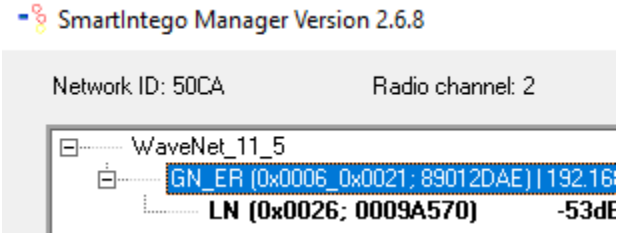
Öffnen Sie den SmartIntego Manager unter “Tools“ → “SmartIntego Manager”. Es sollte bereits ein Gateway Node hinzugefügt worden sein. Klicken Sie mit der rechten Maustaste auf den Eintrag der Gateway Node und wählen Sie den Punkt “Find Chip ID”.

Geben Sie die Chip ID der Lock-Node ein. Diese finden Sie auf der Verpackung des Gerätes. Diese besteht aus 8 alphanumerischen Zeichen. Drücken Sie auf “Start”, um die Suche nach der Lock Node zu beginnen und warten einen Moment.



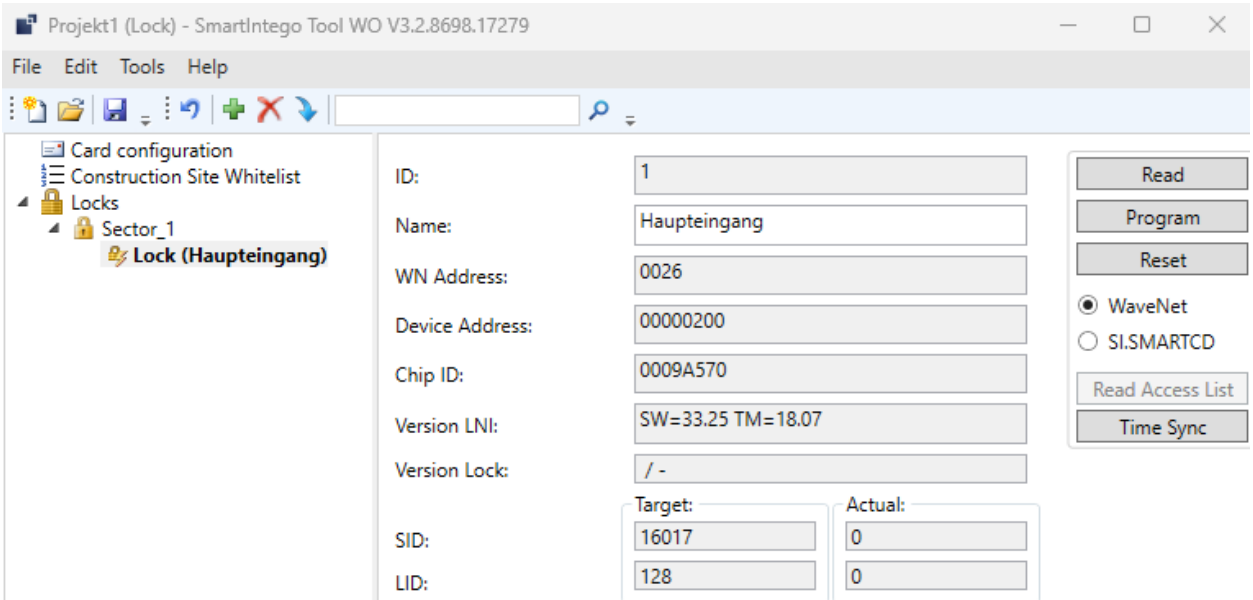
Findet ein Gateway Node den Zylinder, erscheint dieser in der Auflistung. Wählen Sie die Gateway Node, mit der besten Empfangsqualität (dBm). Also der Wert, der näher an 0 liegt. Der Wert sollte nicht niedriger als -85 sein. Für den Fall, dass der Wert niedriger als -85 ist, müssen Sie entweder das nächstgelegene Gateway Node anders platzieren, eine Verstärker-Antenne benutzen oder eine weitere Gateway Node installieren. Beispiel: Ein Wert von -60 dBm ist gut.





Speichern Sie die Änderungen und schließen Sie im Anschluss den SmartIntego Manager.

Im Anschluss vergeben Sie einen Namen für den Zylinder. Dieser Name sollte aussagekräftig sein und wird später in Paxton Net2 ebenfalls verwendet.



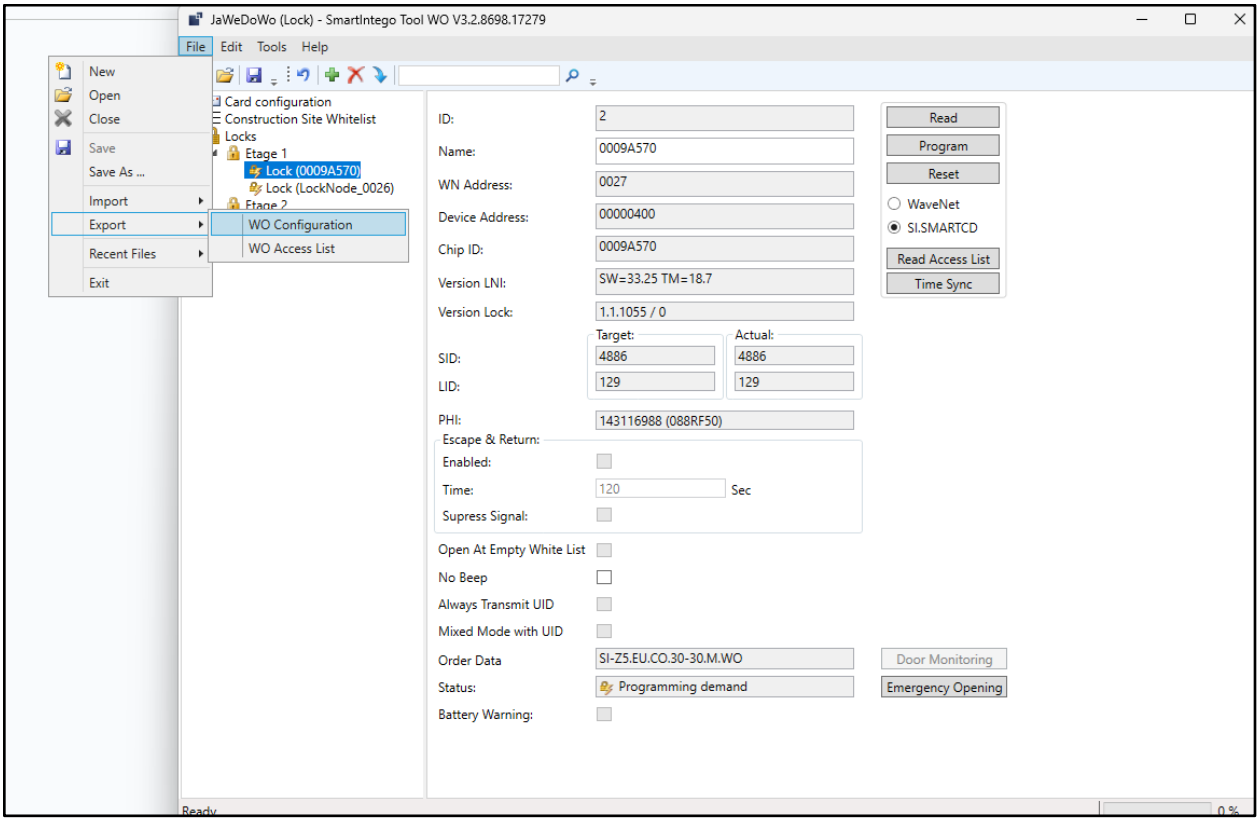
Zum Schluss klicken Sie auf “Program”, um die Konfigurationen auf den Zylinder zu übertragen. Wird dieser Schritt übergangen, führt dies zu einem Fehlverhalten des Zylinders und ggf. zu hohem Energieverbrauch. Das Programmieren über das WaveNet kann bis zu 4 Minuten dauern.

Wiederholen Sie den Vorgang für jeden Zylinder und jedes Gateway.

Speichern Sie das Projekt erneut. Optional können Sie es an einem sicheren Ort sichern.

Nachdem alle Zylinder erstellt wurden, müssen Sie die Konfiguration exportieren, damit Sie sie in ZukoServices übertragen können.

Exportieren Sie das Smart Intego Projekt als CSV-Datei. Gehen Sie hierzu über den Reiter “File” → “Export” → “WO Configuration”. Sichern Sie die CSV-Datei an einen Ort, wo Sie sie gut wiederfinden können.



Sie haben nun die Einrichtung der SimonsVoss-Komponenten in der SimonsVoss SmartIntego-Software abgeschlossen. Als Nächstes folgt die Konfiguration der ZuKoServices.

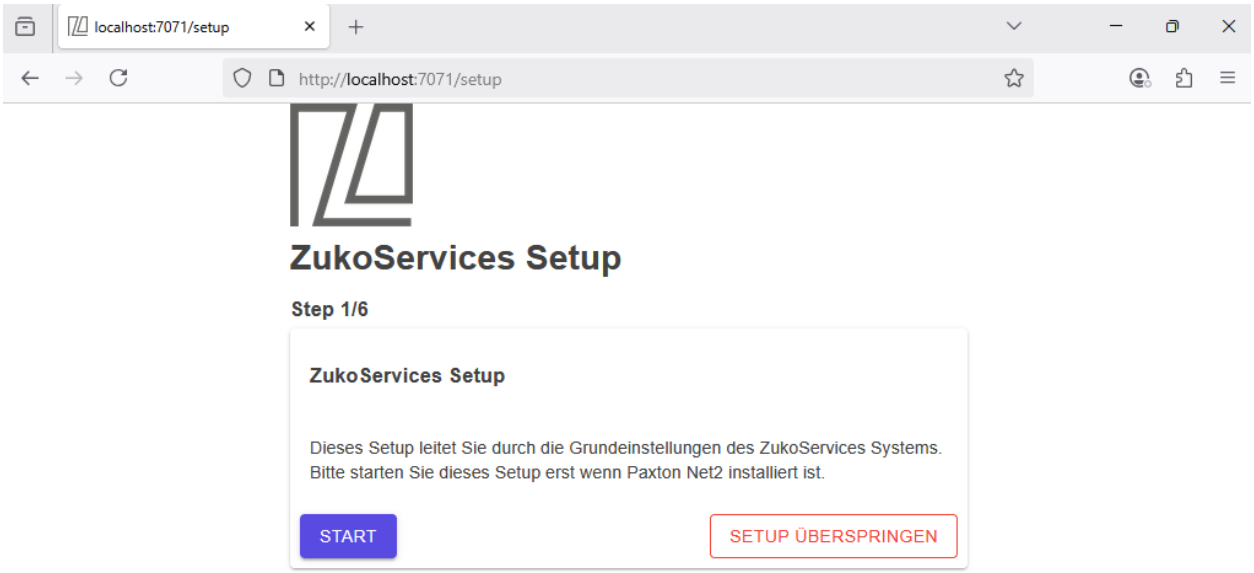
ZukoServices Ersteinrichtung

Nach erfolgreicher Installation finden Sie das ZukoServices Portal unter der URL http://localhost:7071. Die Standard Login Daten lauten:

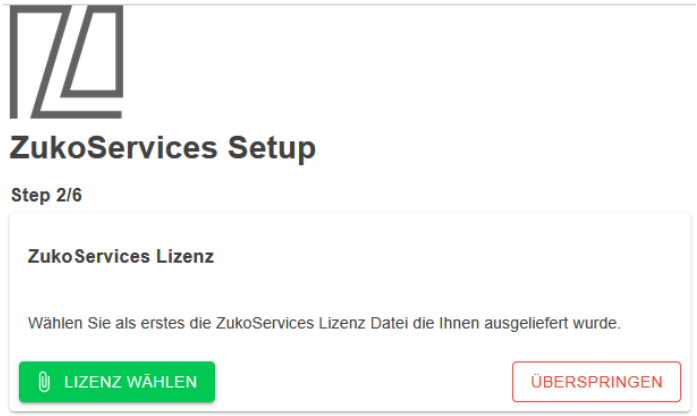
Benutzer: admin

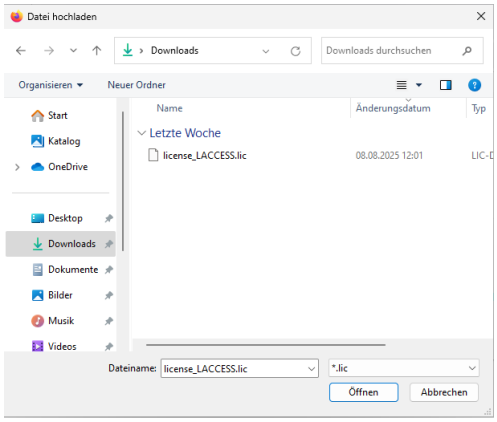
Passwort: admin

Beim ersten Start des ZukoServices-Portals wird ein Einrichtungsassistent gestartet. Bitte folgen Sie den Anweisungen auf dem Bildschirm. Klicken Sie auf „Start“.

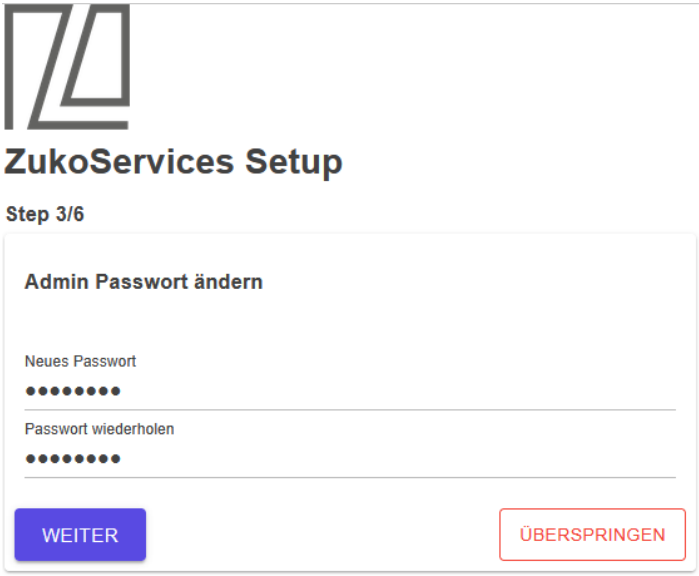


Um die Software zu lizenzieren, klicken Sie auf **„Lizenz auswählen“** und wählen Sie die von uns bereitgestellte Lizenzdatei aus.

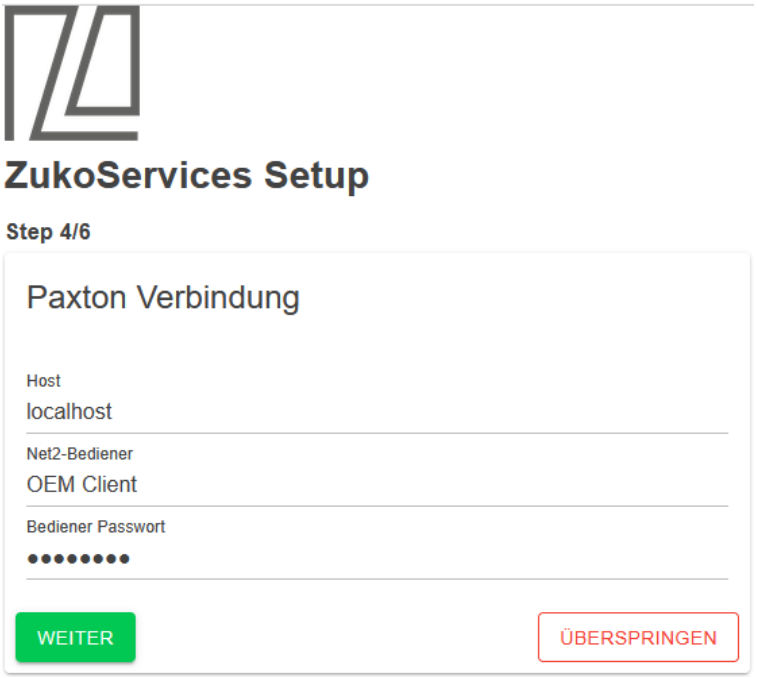




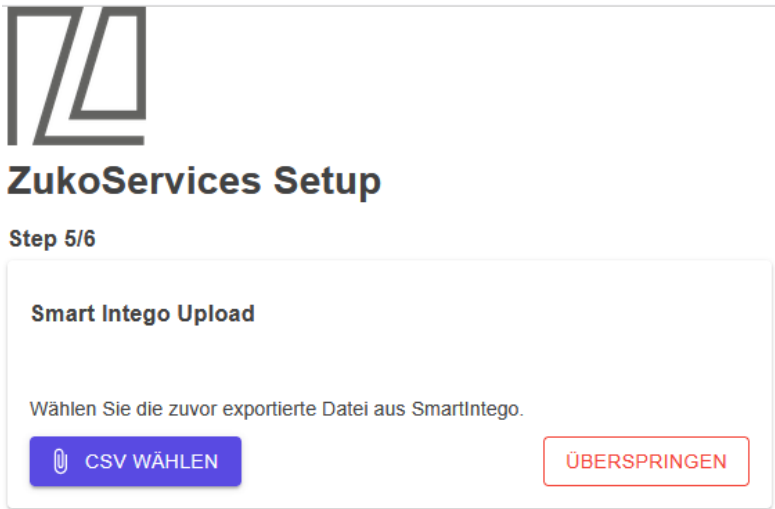
Es wird dringend empfohlen, das Standardpasswort zu ändern. Geben Sie das neue Passwort zweimal ein und klicken Sie auf **„Weiter“**. Notieren Sie dieses Passwort an einem sicheren Ort.



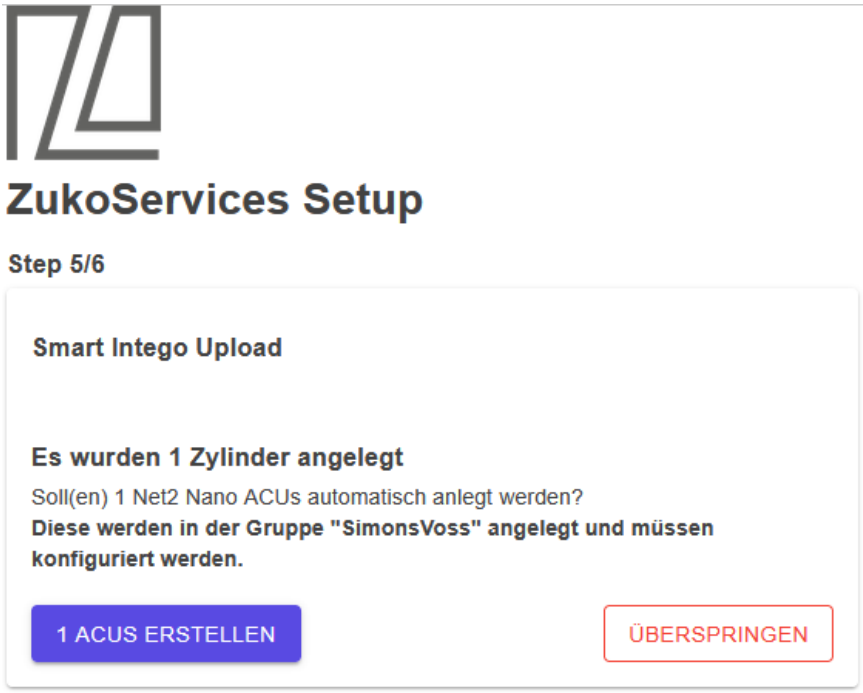
Damit ZukoServices funktioniert, muss eine Verbindung zur Paxton Net2 API hergestellt werden. Geben Sie hier das Passwort des API-Benutzers ein, das Sie zuvor im Abschnitt „Net2 API-Benutzer“ der Dokumentation festgelegt haben.



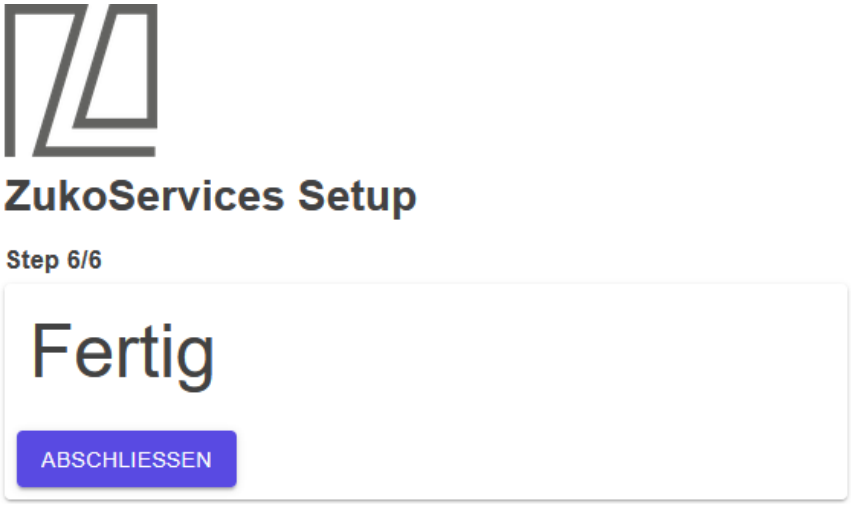
Klicken Sie auf „CSV wählen“ und geben Sie die zuvor aus SmartIntego exportierte Datei an.



Klicken Sie auf „x ACUs erstellen“, um leere Paxton Net2 Zutrittspunkt-Objekte für alle SimonsVoss-Zylinder zu erstellen, die in SmartIntego konfiguriert wurden.



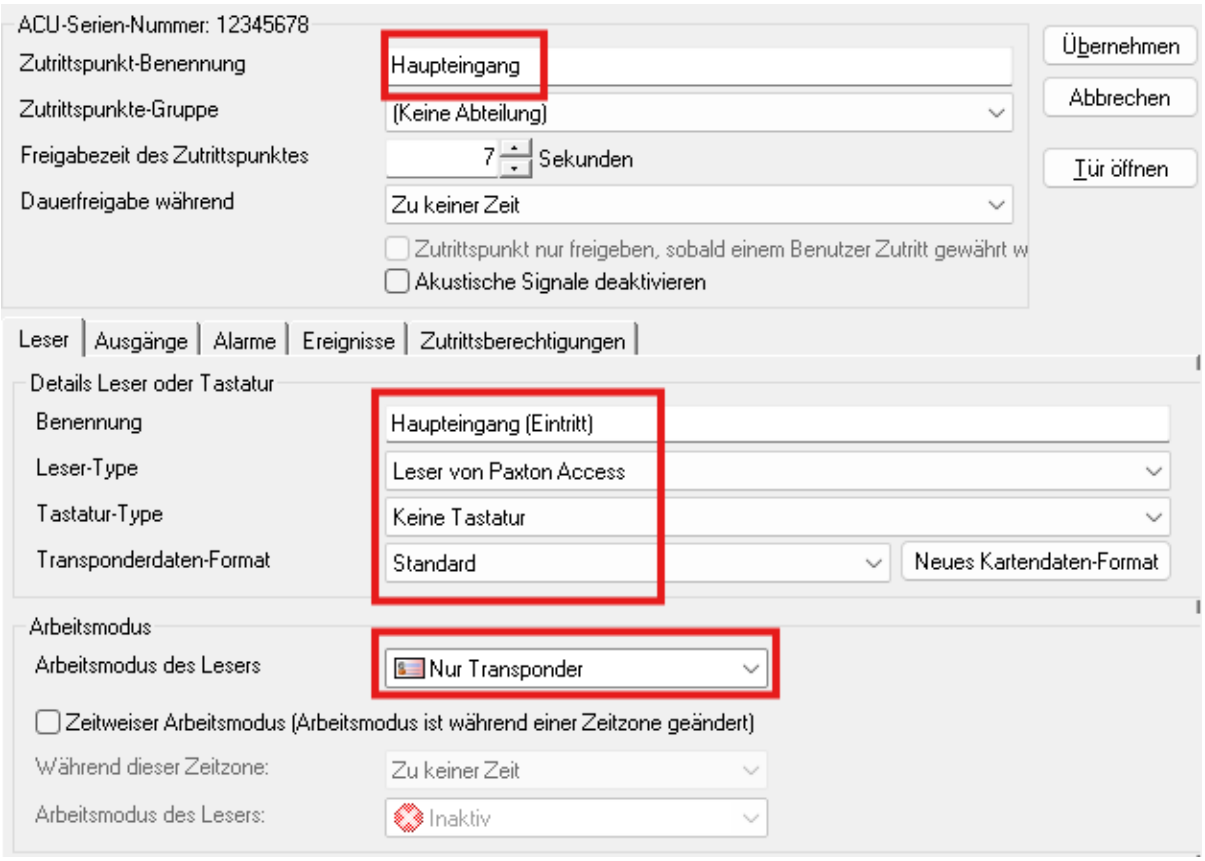
Nun ist die Ersteinrichtungsassistent der ZukoServices abgeschlossen.



Wechseln Sie zu Paxton Net2 Access Control → Zutrittspunkte. Für jeden SimonsVoss-Zylinder wurde nun ein leeres Tür-Objekt erstellt. Die Verknüpfung mit den ZuKo Services erfolgt über den Namen des Paxton Net2 Zutrittslesers und den Namen des SimonsVoss-Zylinders. Doppelklicken Sie auf eines der ACUs mit dem Namenspräfix „ACU“, gefolgt von der fiktiven 8-stelligen Zahl (z. B. „ACU 42818939“). Ändern Sie die frei wählbare Bezeichnung des

Zugangspunkts. Für eine bessere Übersicht können Sie denselben Namen verwenden, der in Smart Intego Wireless Online angegeben wurde.

Stellen Sie sicher, dass die Benennung des Lesers der Bezeichnung des Zylinders in SmartIntego entspricht. Achten Sie außerdem darauf, dass der „Leser-Type“ und der „Arbeitsmodus des Lesers“ korrekt konfiguriert sind.



Klicken Sie auf **“Übernehmen”**.

Wiederholen Sie die Schritte für jeden SimonsVoss Zylinder, indem Sie jedes Mal ein vorhandenes leeres ACU Objekt verwenden.

System Konfiguration

Die Konfiguration von ZukoServices wird über die Weboberfläche durchgeführt. Melden Sie sich dazu am System an:

URL: http://localhost:7071

Benutzer: admin

Passwort: admin

Bedienung

Ereignisse

Ereignisse können nun sowohl in der Net2 Access Control Software als auch auf der Weboberfläche der ZukoServices (http://localhost:7071) aufgerufen werden.
Hier finden Sie jede Kommunikation zwischen ZukoServices und den Online Zylindern.

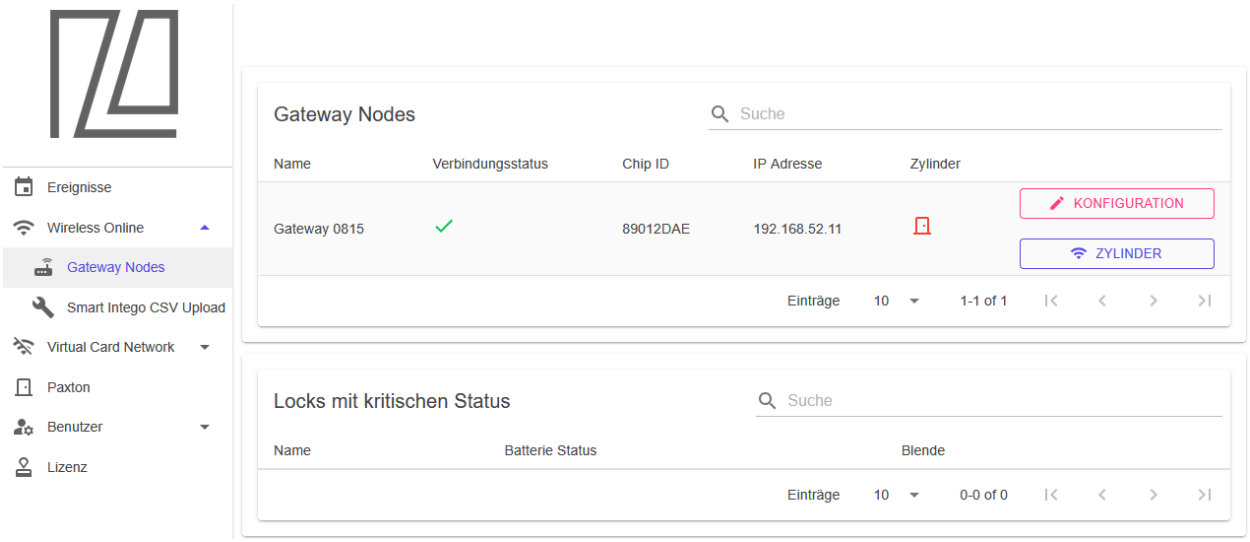
Wenn Sie in Paxton keine Ereignisse sehen können, starten Sie bitte den Computer neu oder starten Sie alle LACCESS-Dienste manuell.

Folgende Ereignisse werden in ZukoServices erfasst:

Construction Site Whitelist gelöscht	Die Smart Intego Software bietet die Möglichkeit, Whitelist-Einträge zu verwalten. Diese Einträge werden beim Systemstart von ZukoServices gelöscht.
Status Abfrage	ZukoServices fragt täglich den Status der Zylinder und der Gateways ab.
Dauerfreigabe durch Benutzer	Ein Zylinder wurde dauerhaft durch einen Benutzer freigegeben.
Kurzzeitfreigabe	Ein Zylinder wurde kurzzeitig durch einen Benutzer freigegeben.
Zutritt verweigert	Der Zutritt wurde durch das ZukoServices System verweigert.
Zutritt gewährt	Der Zutritt wurde durch das ZukoServices System gewährt.

Gateway Nodes und Zylinder

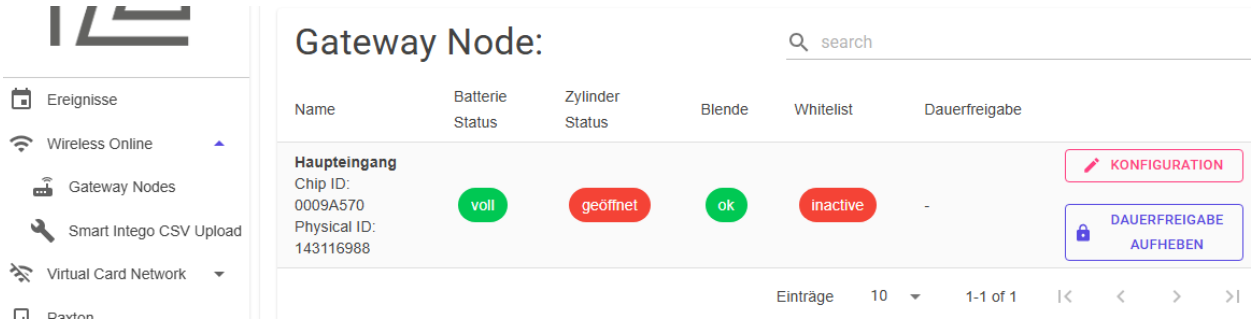
Unter dem Menüpunkt “Wireless Online” → “Gateway Nodes” der ZukoServices Weboberfläche (http://localhost:7071) befinden sich alle importierten Gateway Nodes. In der Übersicht finden Sie relevante Daten der Gateways sowie der verbundenen Zylinder.



Name	Name der Gateway Node
Verbindungsstatus 	Zeigt an, ob ein Gateway Node über das Netzwerk erreichbar ist. Sollte keine Verbindung bestehen, kann der aktuelle Zylinder Status nicht ermittelt und angezeigt werden. Wenn hier ein Fehler angezeigt wird, müssen Sie möglicherweise das AES-Passwort festlegen, was später in der Dokumentation beschrieben wird (siehe Gateway-Konfiguration – AES-Verschlüsselung).
Chip ID	Die Chip ID dient zur eindeutigen Identifizieren einer Gateway Node.
IP Adresse	Zeigt die vergebene IP Adresse der Gateway Node
Zylinder	Hier werden alle Zylinder aufgelistet, die der Gateway Node zugeordnet sind. Der Status eines Zylinders wird als grün oder rot markiert. Der Status “grau” signalisiert, dass die Gateway Node nicht erreichbar ist und der Status nicht ermittelt werden kann. Der Status eines Zylinders wird nicht aktiv abgefragt.

	Der Zylinder übermittelt den Status bei jedem Ereignis, das er an die Gateway Node sendet. Dieses Verfahren trägt zur längeren Batterielaufzeit des Zylinders bei.

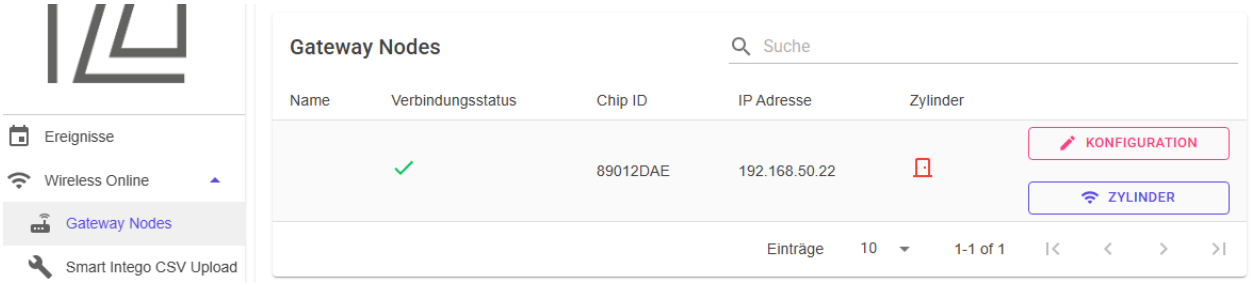
Klicken Sie auf den Button “Zylinder” für weitere Einstellungen und Details.
Die Zylinder-Ansicht ermöglicht die Kurz- und Dauerfreigabe eines Zylinders.



Die Konfigurations-Ansicht der Zylinder zeigt die aktuell geschriebene Whitelist eines Zylinders und ermöglicht die Deaktivierung dieser Liste (nicht empfohlen).
Des Weiteren lässt sich an dieser Stelle eine Zylinderüberwachung aktivieren. Diese Überwachung sollte nur in Ausnahmen verwendet werden, da sie den Energieverbrauch deutlich erhöht.

Gateway Konfiguration - AES Verschlüsselung

Unter dem Menüpunkt “Gateway Nodes” der ZukoServices Weboberfläche (http://localhost:7071) wählen Sie den Button "Konfiguration", um die Einstellungen einer Gateway Node zu öffnen. Sie haben an dieser Stelle die Möglichkeit, ein AES-Passwort einzutragen. Dieses Passwort wird verwendet, um die Netzwerkkommunikation zwischen dem Gateway Node und dem ZukoServices System zu entschlüsseln.



Tragen Sie das AES-Passwort ein, das Sie in der SimonsVoss Gateway Konfiguration vergeben haben (siehe Kapitel: Einrichtung der Gateway Node) und speichern Sie Ihre Eingabe.

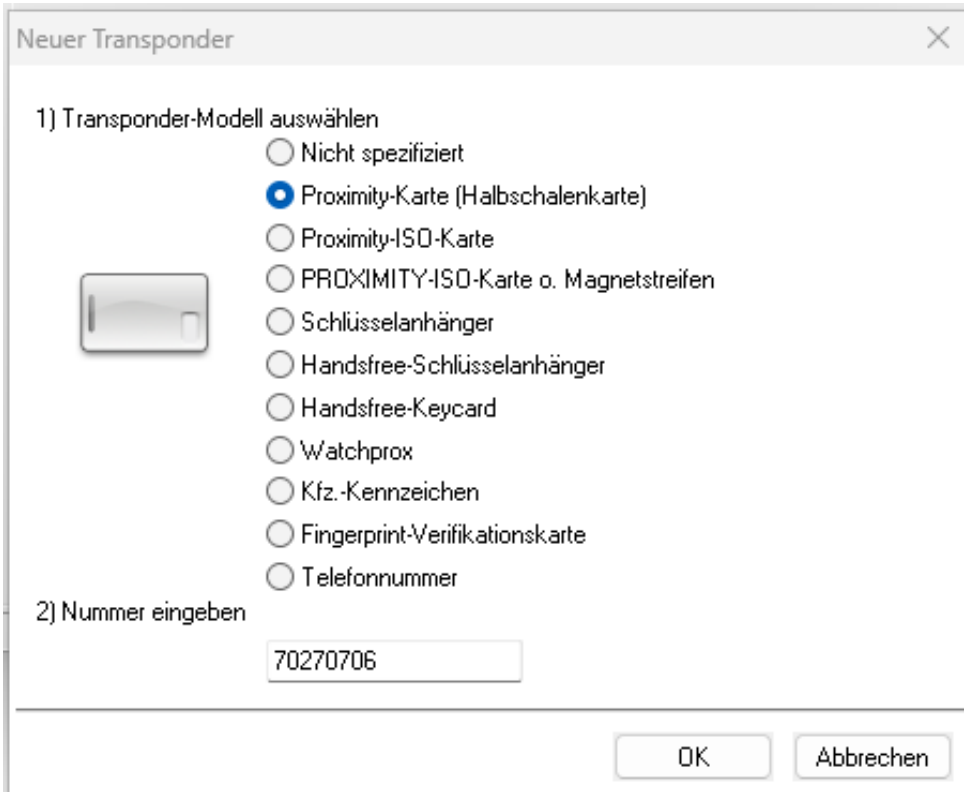
Whitelist

Simons Voss AX Zylinder bieten den Sicherheitsmechanismus einer Whitelist. Dabei handelt es sich um eine Liste von Tokens, die auf den Zylindern geschrieben werden und somit auch bei einem Systemausfall /-neustart zutrittsberechtigt sind. Dadurch wird sichergestellt, dass zu jederzeit Zugang zu bestimmten Türen existiert.

Whitelist-Einträge werden aus Paxton Net2 Access Control importiert. Damit ein Benutzer Whitelist-Zugriff erhält, muss sein Token als **„Proximity-Karte (Halbschalenkarte)“** definiert sein und er muss Zutrittsrechte für die Tür besitzen.

Es wird empfohlen, dass nur eine ausgewählte Personengruppe Whitelist-Zugriff erhält.

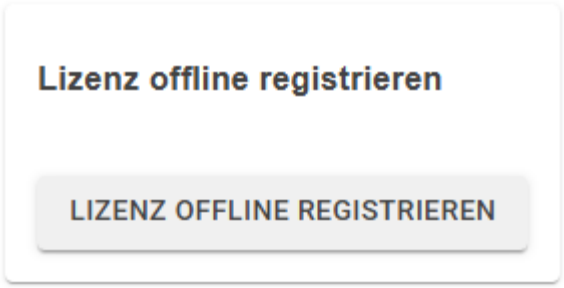
Falls Token in der Vergangenheit bereits als **„Proximity-Karte (Halbschalenkarte)“** definiert wurden, ändern Sie den Tokentyp beispielsweise in **„Proximity-ISO-Karte“** oder einen anderen Typ. Dies wirkt sich an dieser Stelle nur auf das angezeigte Symbol aus.



Lizenzierung abschließen

Im Anschluss der Konfiguration muss das System registriert werden. Dadurch werden die SimonsVoss Gateway Nodes und Feig Reader mit Ihrer Lizenz verknüpft.

Klicken Sie in der Weboberfläche der ZukoServices (http://localhost:7071) den Button “Lizenz online registrieren”, um die Registrierung abzuschließen. Dieser Vorgang kann nur einmal vorgenommen werden. Wurde die SimonsVoss oder Feig -Hardware geändert und ist die Lizenz somit nicht mehr gültig, wenden Sie sich an den Support (Tel.: (+49)0221 - 4744270).



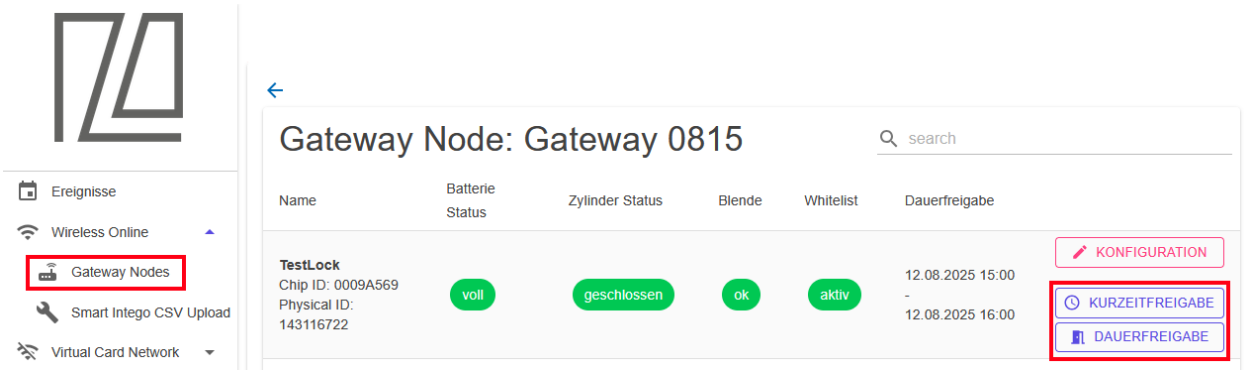
Sollte das System über keinen Internetzugang verfügen, klicken Sie den Button “Lizenz offline registrieren”. Es wird eine Datei generiert und heruntergeladen.

Diese kann durch den Support validiert und registriert werden. Senden Sie die Datei an den Support (support@laccess.de), dieser wird Ihnen eine registrierte Lizenz-Datei zusenden. Diese kann über den Lizenz-Upload eingespielt werden.

Kurzeitfreigabe / Dauerfreigabe

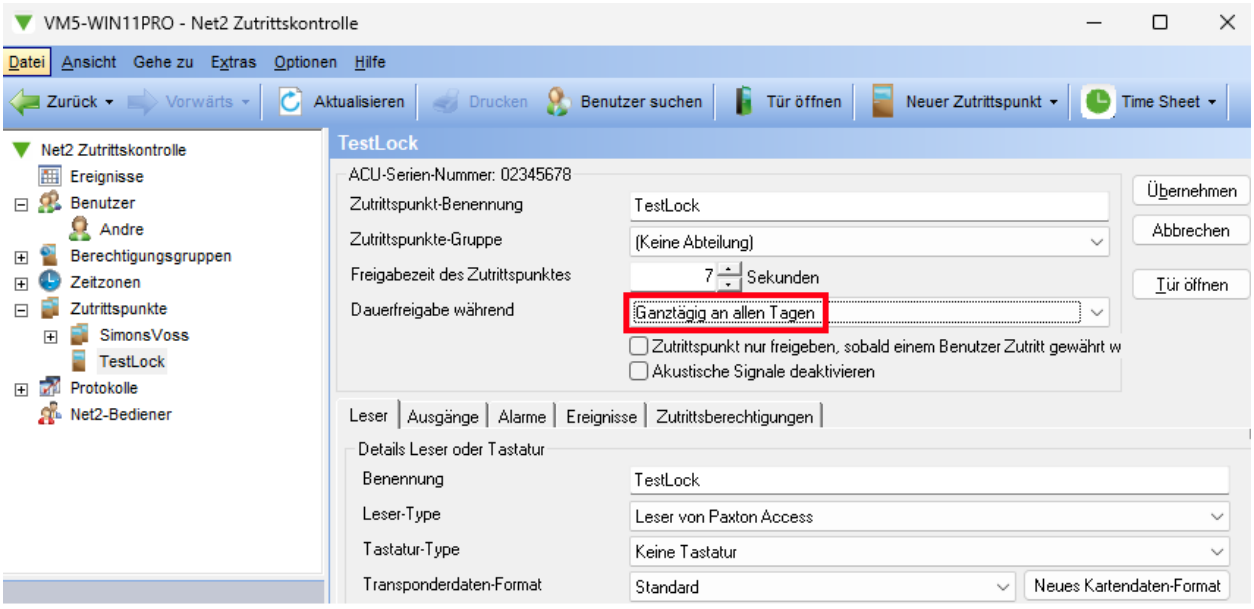
Es gibt verschiedene Möglichkeiten, eine Freigabe zu definieren.

ZukoServices
In der ZukoServices-Oberfläche können Sie in der Zylinderansicht unterhalb der Gateway-Übersicht eine Kurzzeitfreigabe aktivieren. Der Zylinder öffnet sich dann sofort für 4 Sekunden und schließt sich anschließend wieder. An derselben Stelle können Sie auch eine Dauerfreigabe aktivieren. Der Zylinder öffnet sich dann sofort und bleibt so lange geöffnet, bis die Dauerfreigabe dort wieder aufgehoben wird.



Paxton Net2
Auch die Dauerfreigabe-Option in Paxton wird unterstützt. Sobald die Freigabe konfiguriert wurde, öffnet sich der SimonsVoss-Zylinder automatisch für den festgelegten Zeitraum und schließt sich danach wieder.

Hinweis: Bitte beachten Sie, dass das Startdatum der definierten Zeitzone in der Zukunft liegen muss. Wird zum Beispiel die Standardzeitzone „Ganztägig an allen Tagen“ verwendet, wird der Zylinder erst um 00:00 Uhr geöffnet. Die Genauigkeit beträgt eine Minute.



Resetten einer Lock Node (Zylinder)

Um eine bereits im Projekt angelegte Lock Node zurückzusetzen, gehen Sie bitte wie folgt vor:

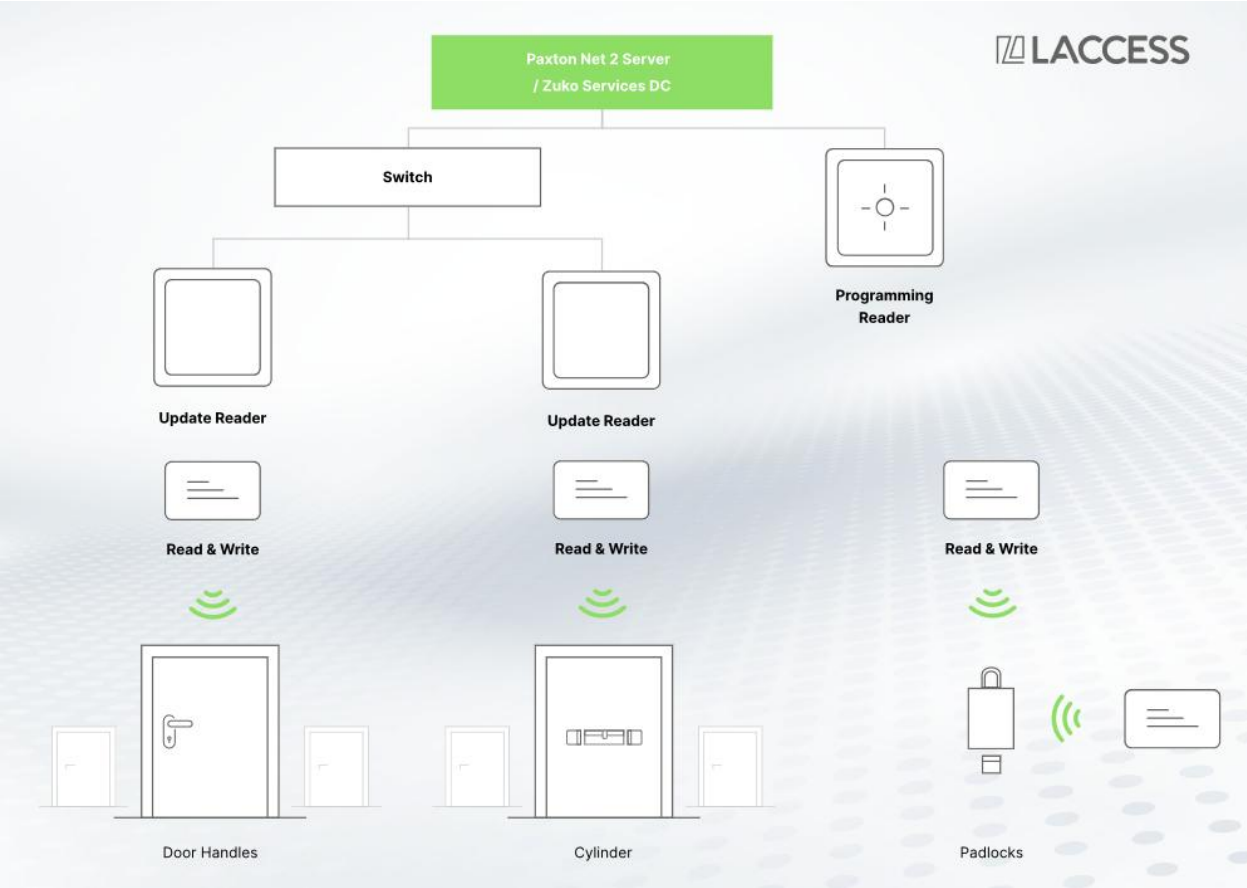
1. Öffnen Sie die SmartIntego WO Software und klicken Sie auf den entsprechenden Zylinder oder Beschlag, den Sie zurücksetzen möchten.
2. Führen Sie anschließend den Reset über das WaveNet durch.

Um sicherzustellen, dass der Zylinder vollständig zurückgesetzt ist und keine Daten mehr enthält, gehen Sie wie folgt weiter vor:

3. Navigieren Sie in der SmartIntego WO Software zum Menüpunkt “Tools” und wählen Sie “SmartIntego Manager”.
4. Geben Sie das Passwort ein und klicken Sie mit der rechten Maustaste auf die gewünschte Lock Node.
5. Wählen Sie “Reset/delete” aus, um den Zylinder vollständig zu resetten.

SmartIntego Virtual Card Network

Das SmartIntego Virtual Card Network kommuniziert ohne eine Netzwerkverbindung. Der Datenaustausch zwischen ZukoServices System und den offline Zylindern geschieht über das Schreiben und Lesen der Tokens. Das System besteht aus folgenden Komponenten:

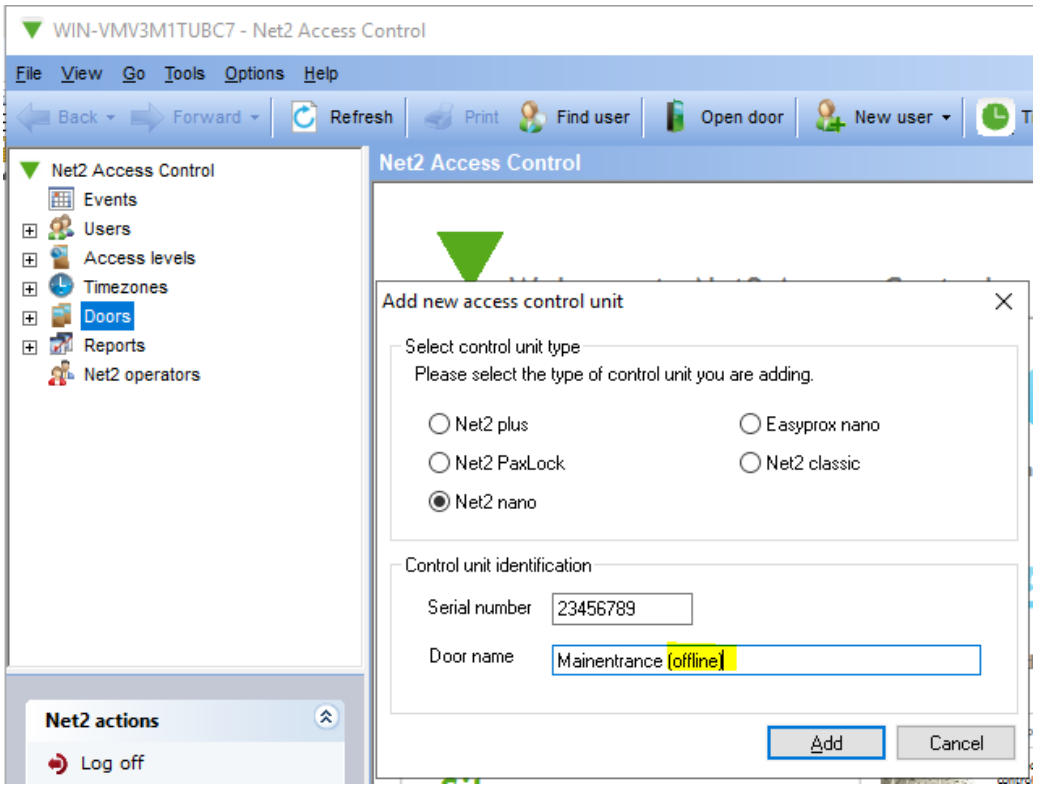


Update Reader	Der Update Reader befindet sich i.d.R. am Eingang eines Geländes, sodass jeder Besucher seinen persönlichen Token dort scannt. Das System kann so diesen Token beschreiben und auslesen.
Program Reader	Jeder Token des Systems muss initial programmiert werden.
SimonsVoss offline Zylinder	Die offline Zylinder werden einmalig programmiert. Es wird durch die Programmierung bestimmt, welcher Zutrittszone sie unterliegen.
ZukoServices	ZukoServices bietet Tools, um Tokens zu Lesen und zu schreiben. Außerdem bietet es Unterstützung bei der Programmierung der Zylinder.

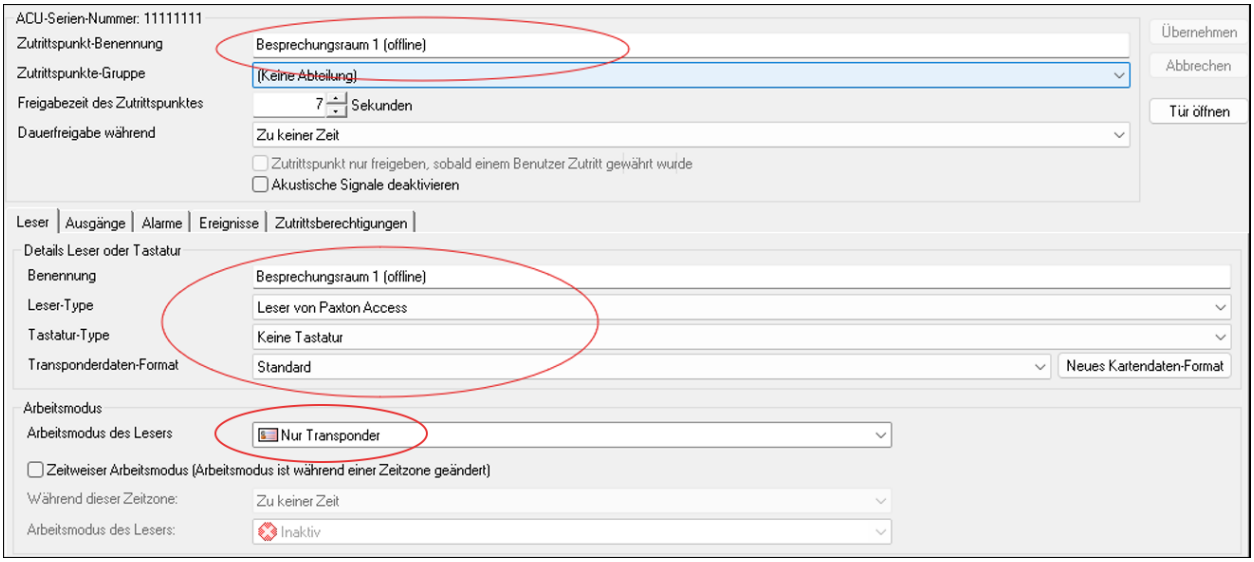
AX Zylinder Programmierung

Legen Sie als erstes Ihre SimonsVoss Offline Zylinder in Paxton Net2 Access Controll Software als ACU Zutrittspunkt an. Hierzu mit der rechten Maustaste auf “Zutrittspunkte” und “Neue ACU hinzufügen”.

ACU Type	Net2 Nano
Seriennummer	Fiktive 8-stellige Nummer, die noch von keiner anderen ACU verwendet wird (z.B. 12345678).
Zutrittspunkt-Benennung	Schreiben Sie “offline” und eine frei wählbare schlagkräftige Benennung

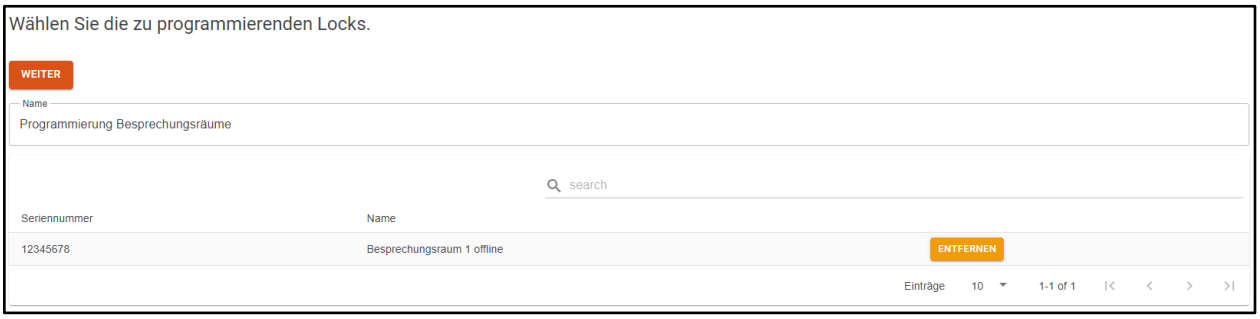


Editieren Sie die ACU in dem Sie mit Doppelklick auf den jeweiligen Zylinder gehen. Achten Sie darauf, dass die Benennung des Lesers das Codewort “offline” beinhaltet, z.B. „Besprechungsraum (offline)“. Es sollte außerdem der Leser-Type und der Arbeitsmodus konfiguriert werden:



Wechseln Sie im Anschluss zum ZukoServicess Web-Portal (http://localhost:7071) und navigieren Sie zum Menüpunkt “Virtual Card Network” → “Smart Intego VCN”.

Hier finden Sie eine Liste von erstellten Programmieraufgaben. Klicken Sie auf "Neue Datei erstellen”. Wählen Sie einen Namen für die neue Programmieraufgabe. Dieser Name dient nur der späteren Wiederfindung. In dieser Ansicht werden alle offline Zylinder aufgelistet, die in Paxton Net2 Access Control mit dem Schlagwort “offline” erstellt wurden. Klicken Sie "Hinzufügen" für jedes Schloss, welches programmiert werden soll. Im Anschluss klicken Sie auf “Weiter”.



In der zweiten Ansicht haben Sie die möglichkeit zu wählen welche Programmierung Sie mittels Smart CD vornehmen möchten:

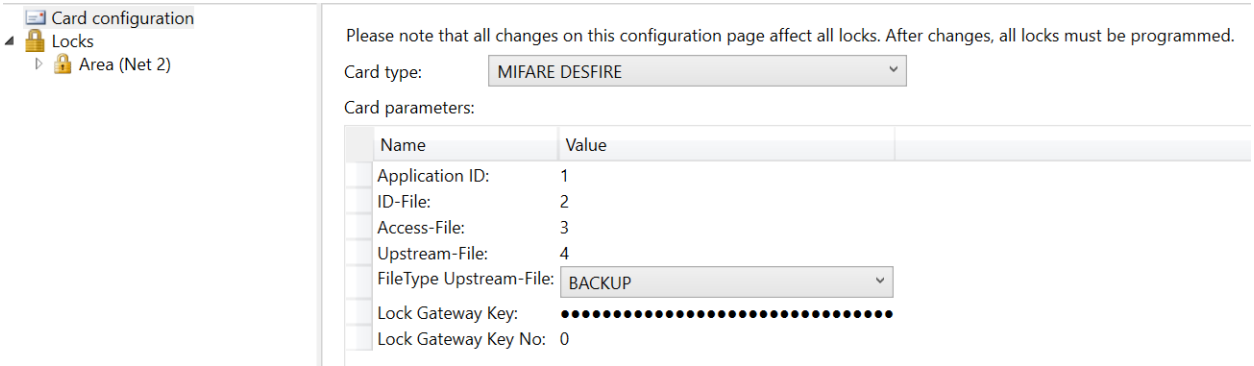
Zurücksetzen	Bereits programmierte Zylinder können zurückgesetzt werden, um diese zu ersetzen oder neu zu programmieren.
Programmieren	Um einen Zylinder zu programmieren, wählen Sie diesen Punkt. Durch eine Programmierung werden auf dem Zylinder Zutrittspunkte und Zeitprofile geschrieben. Sollten Sie Zeitprofile oder Berechtigungsgruppen in Paxton Net2 Access Control ändern, ist eine Neuprogrammierung der betroffenen Zylinder notwendig. Zur Neuprogrammierung wählen Sie den Punkt “Zurücksetzen” und “Programmierung”.
Uhrzeit konfigurieren	Die Uhrzeit der Zylinder sollte jährlich geupdatet werden, um sicherzustellen, dass die Uhrzeit richtig synchronisiert ist.
Zugangsdaten auslesen	SmartIntego bietet die Möglichkeit, Zylinder auszulesen und Zugänge einzusehen.
Notfallöffnung	SmartIntego bietet die Möglichkeit, die Zylinderschließung zu aktivieren und eine Tür zu öffnen.

Klicken Sie auf “Datei erstellen", um den Vorgang zu beenden. Wählen Sie den Download-Button, um die Datei herunterzuladen.

Öffnen Sie das Programm “SmartIntego VCN” und legen Sie ein neues Projekt an:

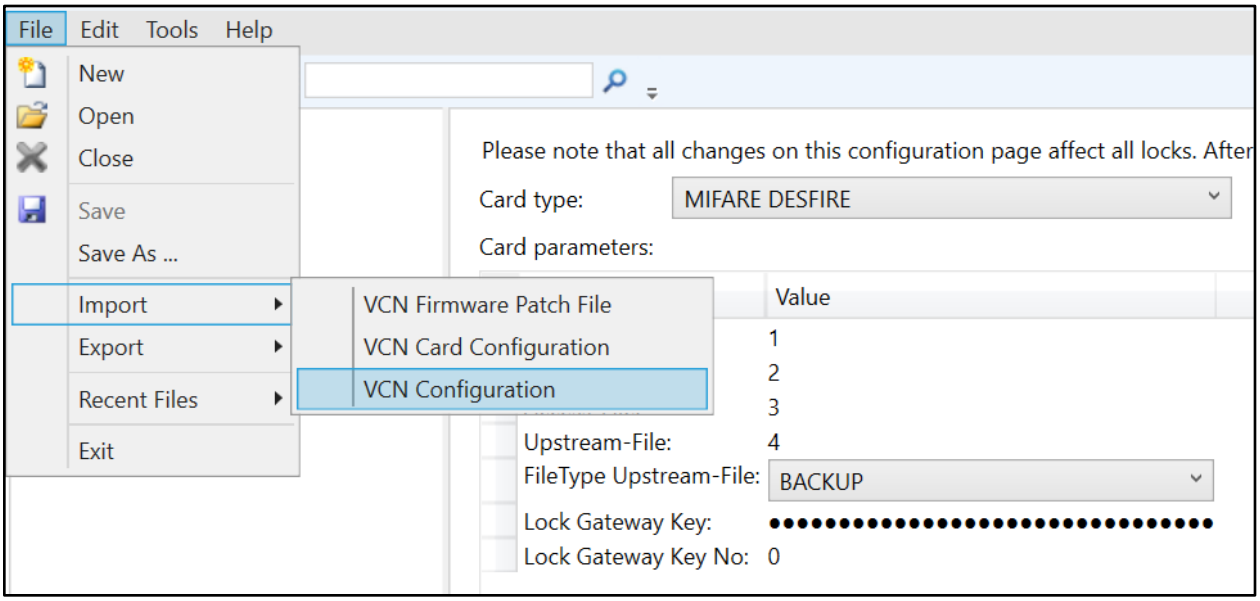
Name	Name des Projektes
Password	Passwort zum Öffnen des Projektes (Das Passwort muss mindestens 8 Stellen haben, einen Groß- und einen Kleinbuchstaben sowie eine Zahl oder Sonderzeichen beinhalten)
Confirm Password	Passwort Bestätigung
Virtual Card Network Password	Mit diesem Passwort werden die Lock Nodes verschlüsselt. Mit diesem Passwort ist es möglich, Geräte zurückzusetzen. Das Passwort muss mindestens 8 Stellen haben und darf nicht identisch mit dem Projektpasswort sein.
Virtual Card Network Confirm Password	Passwort Bestätigung
Passwords hint	Hinweis auf die Passwörter

Konfigurieren Sie zuerst die “Card configuration”:



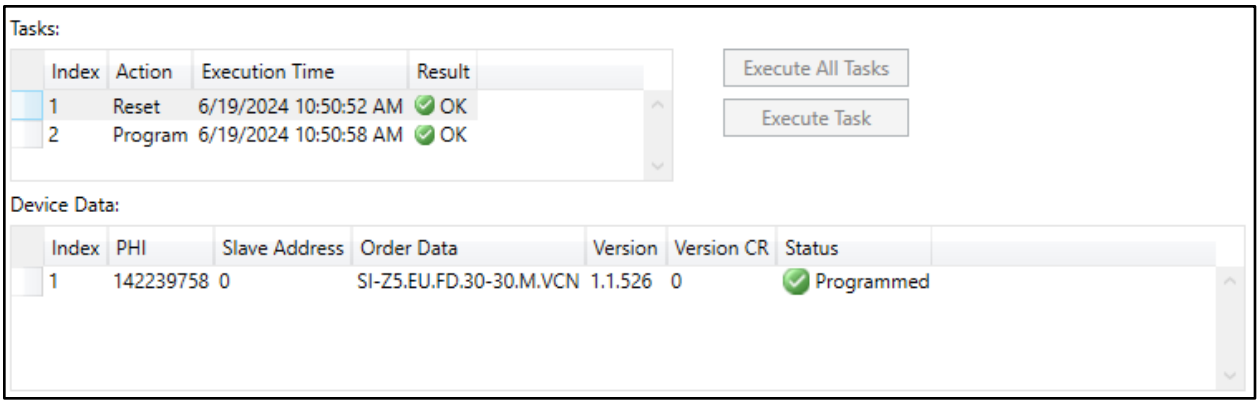
Die Felder sind frei wählbar und abhängig von Ihrer Token Programmierung. Das Feld “Lock Gateway Key No.” sollte in jedem Fall den Wert “0” haben. Aktuell werden jedoch nur “Card Type” → “MIFARE DESFIRE” und “FileType Upstream-File” → “BACKUP” unterstützt. Der Lock Gateway Key muss 32 Hex Characters haben und wird nicht automatisch vergeben. Kreiere einen Gateway Key bestehend aus den Zahlen von 0-9 und Buchstaben von a-f. Speichern Sie Ihre Eingabe!

Als nächstes wird die zuvor generierte Datei aus ZukoServices importiert. Gehen Sie hierzu über den Reiter “File” → “Import” → “VCN Configuration”:



Sie finden jetzt alle zuvor in Paxton Net2 Access Control angelegten und durch ZukoServices exportierten offline Zylinder in der SmartIntego VCN Baumstruktur.

Schließen Sie das SmartIntego SmartCD Programmiergerät an Ihren PC an, klicken Sie auf einen Zylinder der Baumstruktur, halten Sie den Zylinder an das Programmiergerät und klicken Sie auf “Execute All Tasks”.



Wiederholen Sie den Vorgang für jeden offline Zylinder, den Sie programmieren möchten.

Token-Programmierung

Karten Konfiguration

Richten Sie zuerst die Karten Konfiguration in ZukoServices ein. Öffnen Sie dazu ZukoServices im Browser (http://localhost:7071) und navigieren Sie nach “Virtual Card Network” → “Karten Konfiguration”. Übernehmen Sie die Eingaben aus SmartIntego VCN und speichern Sie die Einstellungen.

NFC Leser

Verbinden Sie einen Feig OBID RFID-Leser mit Ihrem Netzwerk und konfigurieren Sie ihn mithilfe der Reader Discovery Software. Achten Sie darauf, dass die Windows Firewall entsprechend konfiguriert oder ausgestellt ist. Wenn Sie den Leser in der Software sehen, klicken Sie diesen mit der rechten Maustaste an und wählen Sie “Setup Network Configuration”. Wenn Sie die Parameter ändern möchten, wählen Sie als erstes “change” aus. Der Leser muss sich im gleichen Netz wie die ZukoServices Software befinden. Wenn Sie mit den Netzwerkeinstellungen fertig sind, drücken Sie Ok.

Sie benötigen einen RFID-Leser zur Programmierung der Token und einen zweiten Leser als Update-Leser.

Öffnen Sie im Anschluss ZukoServices im Browser (http://localhost:7071) → “Virtual Card Network” → “NFC Leser”. Fügen Sie einen “Programmierungs-Leser” und einen “Update-Leser” neu hinzu (siehe Auswahlfeld “Typ”). Hierzu ist die Eingabe der zuvor in der Reader Discovery Software für die jeweiligen Leser vergebene IP-Adresse zwingend erforderlich. Speichern Sie Ihre Eingabe.

Token

Wechseln Sie in ZukoServices nach “Virtual Card Network” → “Token” → “Token erstellen” und wählen Sie einen Programmierungs-Leser, der für Sie erreichbar ist. Sie haben die Wahl zwischen folgenden Token Typen:

Zutritts-Token	Standard Token für normale Benutzer. Es werden Zutrittsberechtigungen und Zeitprofile aus Net2 übernommen. Der Token muss regelmäßig an einem Update NFC Leser geupdatet werden, damit er seine Gültigkeit behält.
Toggle-Token	Dieser Token öffnet oder schließt eine Tür dauerhaft. Es werden Zutrittsberechtigungen und Zeitprofile aus Net2 übernommen. Der Token muss regelmäßig an einem Update NFC Leser geupdatet werden, damit er

	seine Gültigkeit behält.
Blocklist-Token	Der Block List-Token kann keine Türen öffnen. Er wird nur verwendet, um Informationen, wie die Sperrung bestimmter Tokens, an verschiedene Zylinder zu verteilen. Er sollte vor Verwendung am Update Reader aktualisiert werden.
Notfall-Token	Der Notfall-Token kann jeden Zylinder permanent öffnen. Er wird nicht vom Update-Reader geändert und hat kein Ablaufdatum.

Drücken Sie den Button “Token Programmieren” und präsentieren Sie dem NFC-Leser solange einen Token, bis der Prozess abgeschlossen ist.

Token Vorlage

Sie können weitere Token-Einstellungen unter “Virtual Card Network” → “Karten Konfiguration” im Abschnitt Token Vorlagen vornehmen.

Transponder Gültigkeit in Stunden (Updateinterval)	Geben Sie hier die Anzahl der Stunden an, die ein Token gültig sein soll. Nach Ablauf dieser Zeit muss der Token am Update NFC-Leser aktualisiert werden. Dieser Mechanismus garantiert Ihnen, dass verlorene Token zeitnah nicht mehr verwendet werden können.
Blocklist Dauer in Wochen	Geben Sie die Anzahl von Wochen an, die ein Blocklist Eintrag auf einem Zylinder gespeichert werden soll. Wird in Net2 ein Token als verloren markiert, wird der Token für diese Zeit auf dem Zylinder als verloren und inaktiv gespeichert.

Logs

Zylinder

Unter dem Menüpunkt “Virtual Card Network” → “Zylinder” finden Sie alle offline Zylinder, von denen bereits Informationen gesammelt wurden. Sie können den Batteriestatus der Zylinder einsehen, sowie die Zutritte zu diesem Zylinder.