LACCESS
ZukoServices

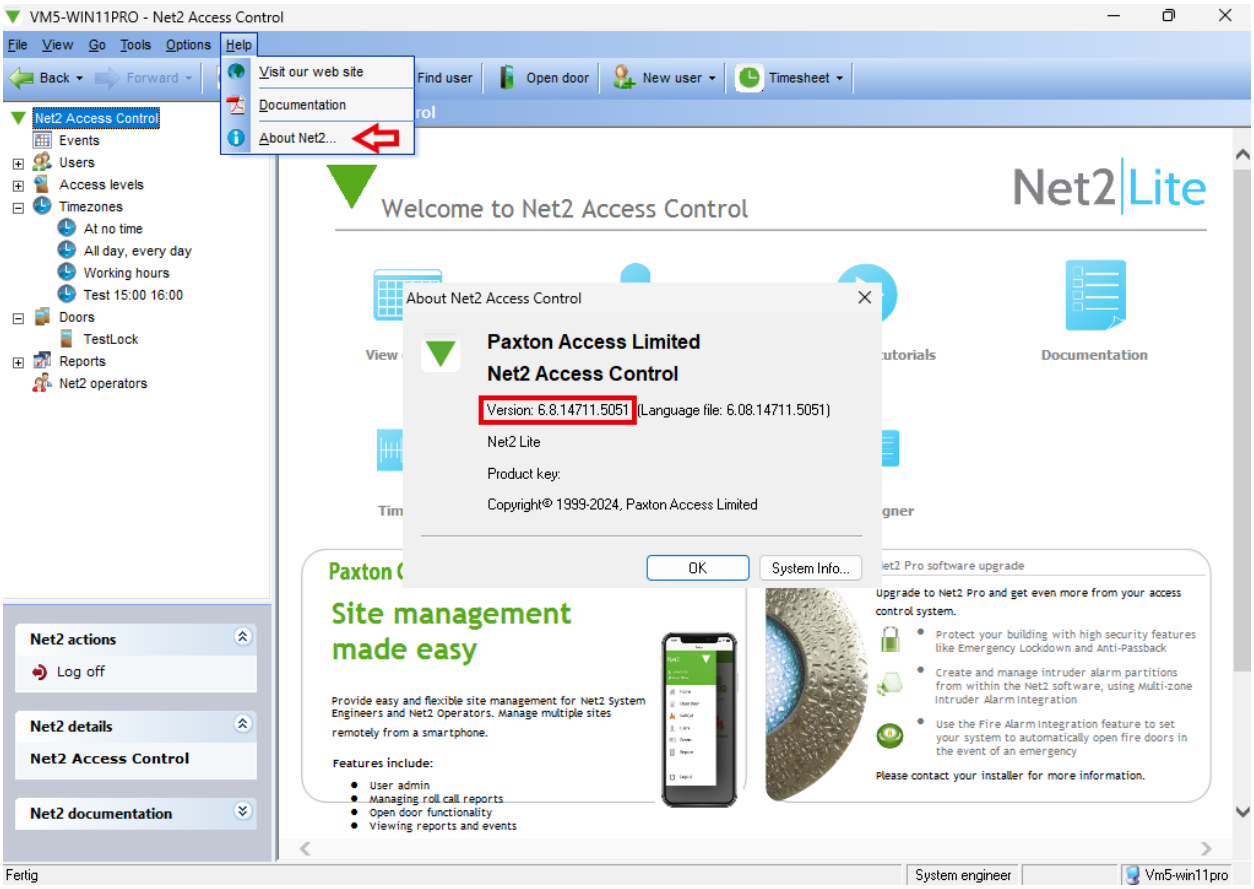
LACCESS GmbH S.Beckers
06.08.2025
V 1.81.0.0 (A.Moißl)

Table of contents

Paxton Net2 - Requirements

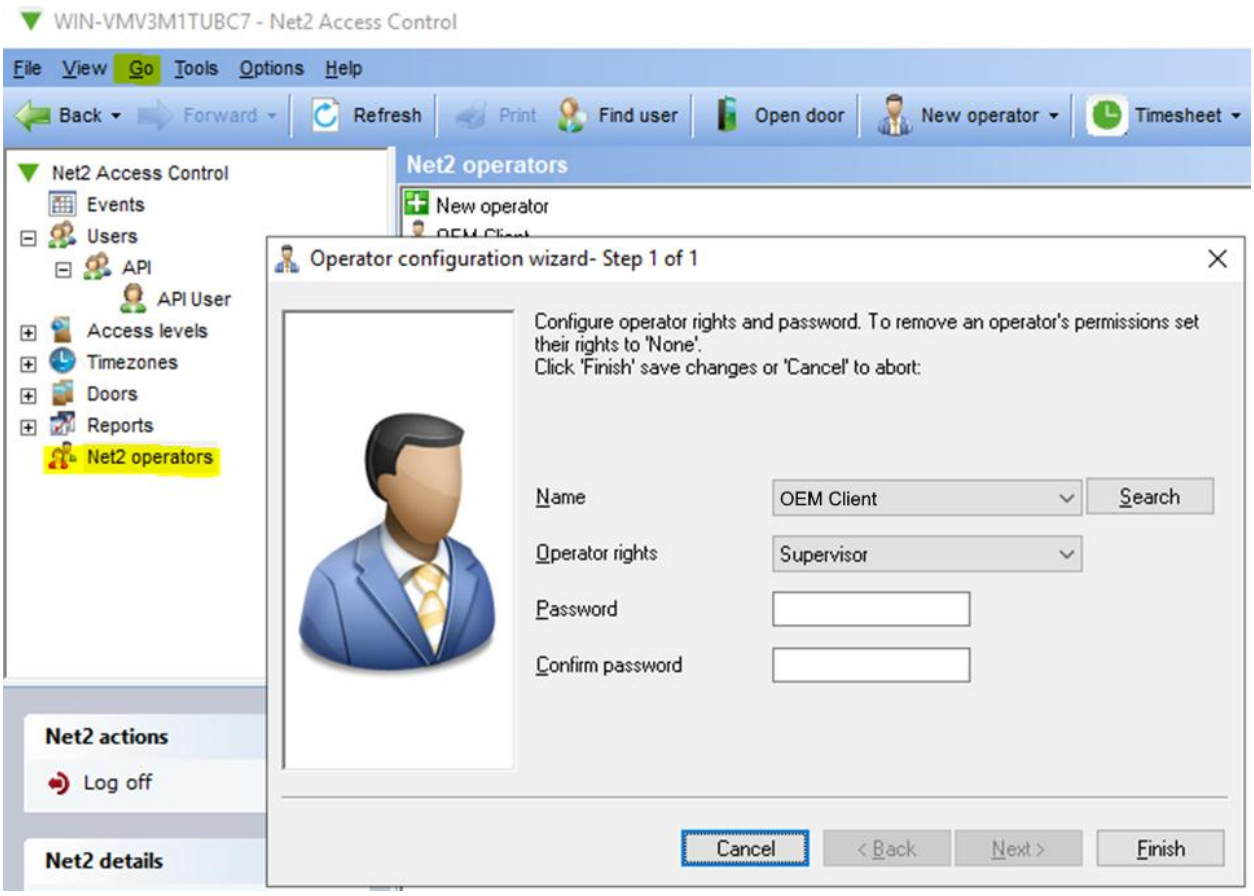
Check Version

Ensure that Paxton Net2 Access Control Software is already installed and contains version V6.8.14711.5051. To view the version number, start the Paxton Net2 software, click on "Help", and then select "About Net2...".



Net2 API User

Navigate to **“Net2 operators”**, double-click on the user **“OEM Client”**, set a password, and click **“Finish”**. This user is required later for LACCESS ZukoServices to access Paxton via the API. If you prefer to use a different Net2 operator, make sure he has the permission level **“all hours, all doors”**.



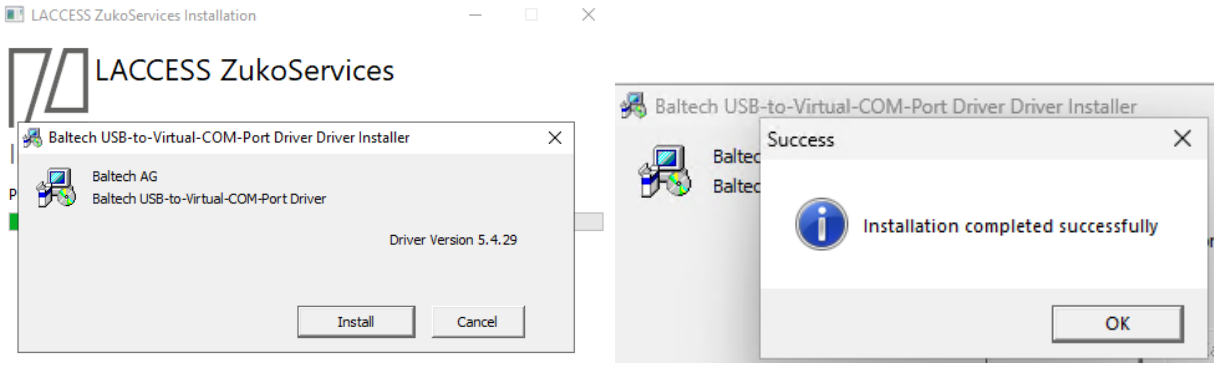
Now you can close Net2 Access Control.

ZukoServices Installation

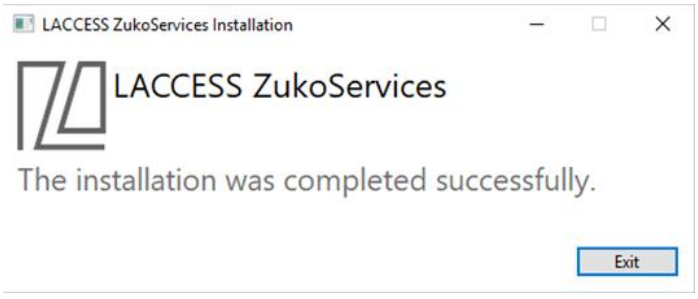
Start the file 'LACCESS_ZukoServices_Setup_EN_v1.81.0.0.exe' from the supplied USB stick and follow the instructions. The setup will install the ZukuServices software along with the following programs:

1. Grafa – Software for managing log entries
2. SQL Server 2022 Express – Database
3. SimonsVoss SmartIntego – Software for configuring SimonsVoss wireless online devices
4. SimonsVoss SmartIntego VCN – Software for configuring SimonsVoss VCN (Virtual Card Network) devices
5. Feig Discovery Reader – Tool for configuring Feig NFC readers
6. SimonsVoss OAM Tool – Tool for configuring the wireless online gateways

As soon as this dialog opens, please click **“Install”** and later **“OK”**.



The installation is now complete. Click **”Exit”**.



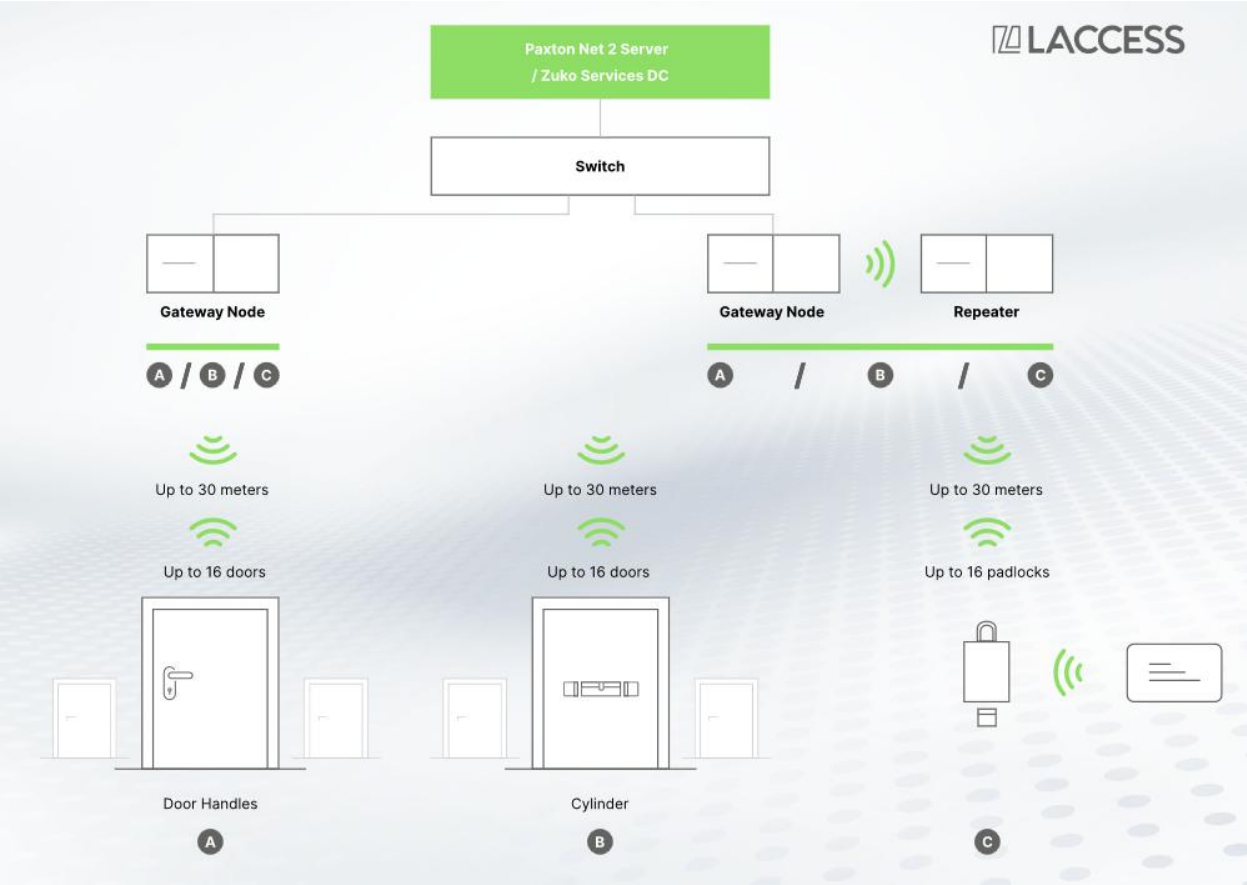
Please restart your Server.

SmartIntego Wireless Online

Components

The SimonsVoss Wireless Online System consists of following components:

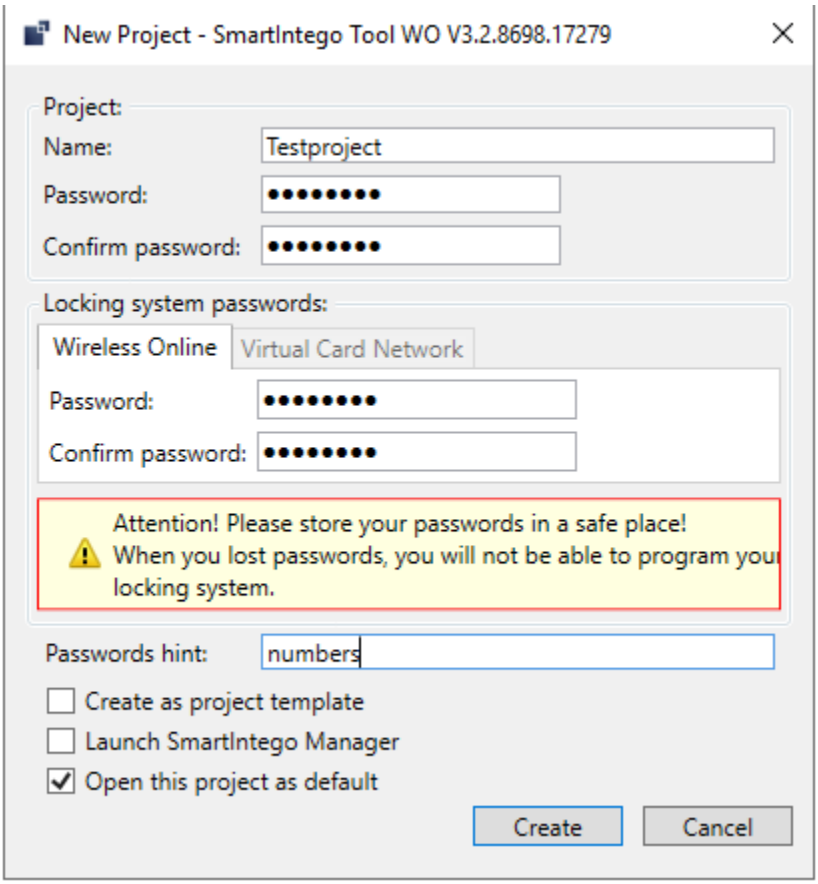
- Lock Node: Lock Nodes are buttons and cylinders installed on the doors.
- Gateway Node: This is a control unit that manages cylinders via a wireless connection. Cylinders report events to the gateway, and the gateway sends commands (e.g., open door) to the cylinders.
- ZukoServices: The Gateway Nodes send events to the ZukoServices system. ZukoServices processes these events and sends commands to the Gateway Nodes. A Gateway Node can manage up to 16 Lock Nodes.
- Paxton Net2: ZukoServices retrieves information for result evaluation from the access control system Paxton Net2. Among other things, it reads tokens, users, user groups, and access points.



Configuration

Create a new project

Gateway Nodes und Lock Nodes are configured through the SmartIntego software in a project file. To do this, open the SmartIntego program and create a new project.



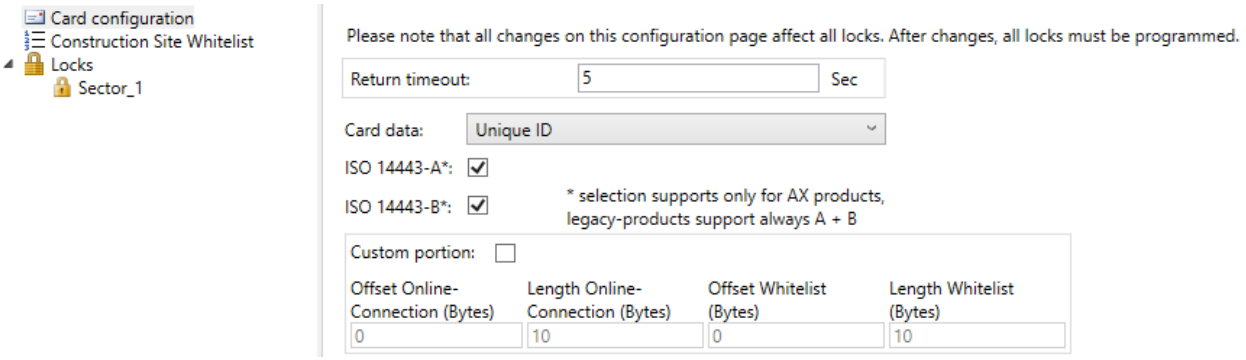
Name	Project name
Password	Password to open the project (The password must be at least (8 characters long and should include at least one uppercase letter, one lowercase letter, and either a number or a special character).

Confirm Password	Confirmation of the password
Wireless Online Password	This password is used to encrypt the Lock Nodes. It is also required to reset devices. The password must be at least 8 characters long and cannot be the same as the project password.
Wireless Online Confirm Password	Confirmation of the password
Passwords hint	Note on the passwords

Store passwords securely and reliably. Passwords cannot be reset. The loss of passwords will result in project files no longer being accessible and Lock Nodes being unusable!

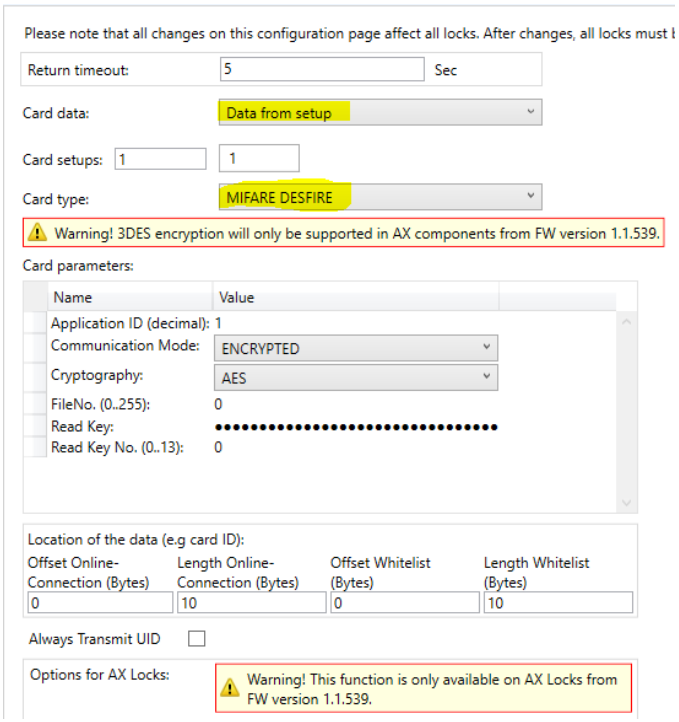
After confirming with "Create" the project opens. The settings under the „Card Configuration” section determine how the Lock Nodes read an NFC token. Under the “Card Data” section, it is specified whether the “Unique ID” or the encryption of a token should use “Data from setup”.

The setting for using the Unique ID (the default setting) is as follows:



(Optional) The setting for using the encryption of a token is as follows:

The settings for „Data from setup“ should be made by qualified personnel. All setting under „Card Configuration“ should be completed before creating the Gateway Nodes and Lock Nodes. If changes are made afterward, they must be reprogrammed on the Lock Node.



After you have decided on an option, save the project in a folder you can find again. The default folder path is C:\Users\Public\Documents\SimonsVoss\SmartIntego.

Adding a Gateway Node

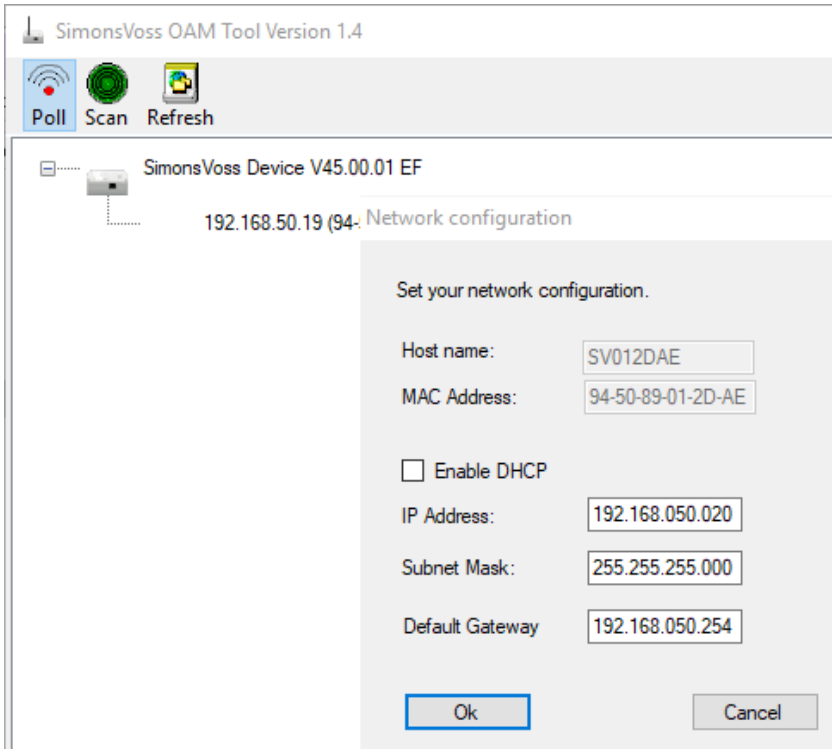
Setting up the Gateway Node

Mount the Gateway Node at a suitable location and connect it to a PoE switch.

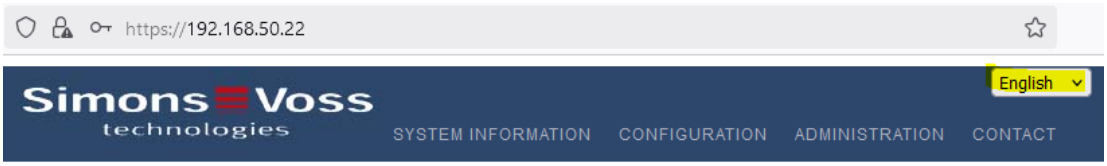
To ensure proper identification later, make a note of the ChipID, which can be found on the back of the respective Gateway Node.

Open the SimonsVoss OAM program. You can find it in the folder: C:\Program Files\LACCESS ZukoServices\SimonsVoss. Ensure that the Windows firewall is configured appropriately or turned off.

You will now see the discovered Gateway Nodes within the software. Right-click on the Gateway Node and select “Set IP”. Set the desired IP address.



The Gateway Node should be on the same network as the ZukoServices software. The Gateway Node is configured via a web interface. Find the IP address of the device and access it through your browser (e.g., https://192.168.178.10/). Depending on your browser, confirm certificate warnings with "Advanced" and "Continue to xxx (unsafe)" or similar. Log in with the default username: “SimonsVoss” and the password “SimonsVoss”.



OVERVIEW
WAVENET
CONNECTION

System Information: Overview

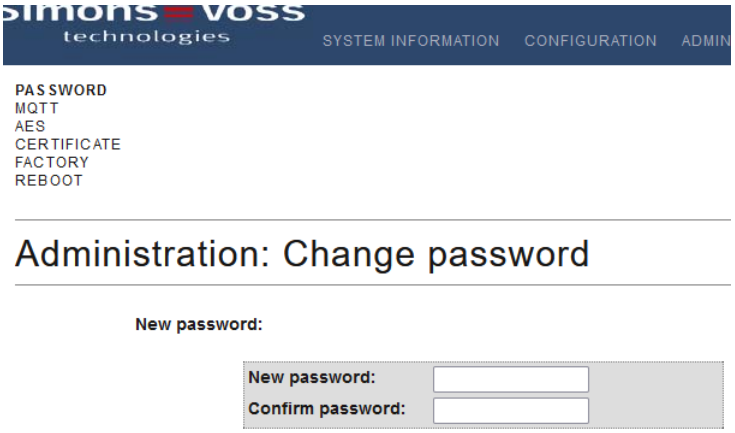
Version:

Firmware version:	45.00.01

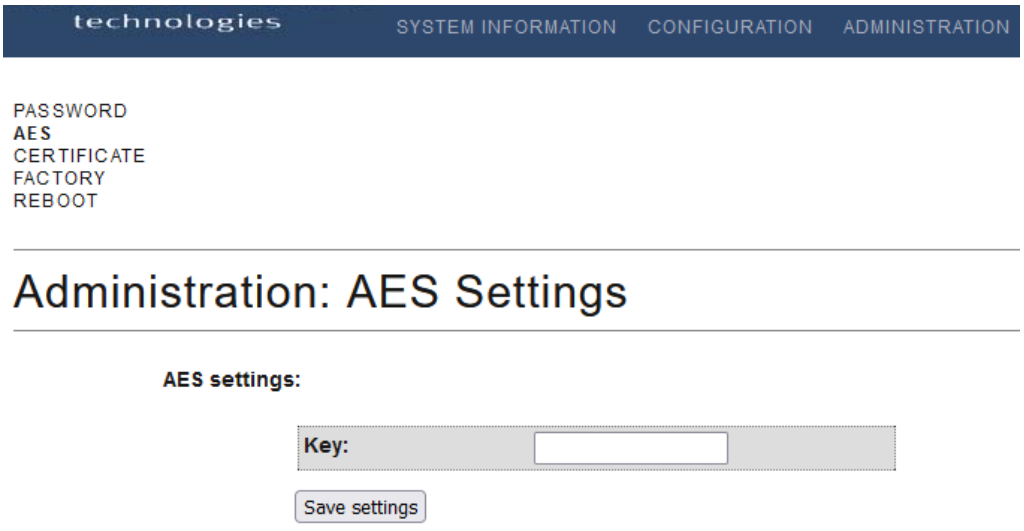
Basic network settings:

MAC Address:	94:50:89:01:2D:AE
Host Name:	SV012DAE
DHCP:	On
IP-Address:	192.168.50.22
Subnetmask:	255.255.255.0
Gateway:	192.168.50.254

Under the “Configuration” menu, you can make network settings. You should also change the default password. To do this, open the “Administration” menu.

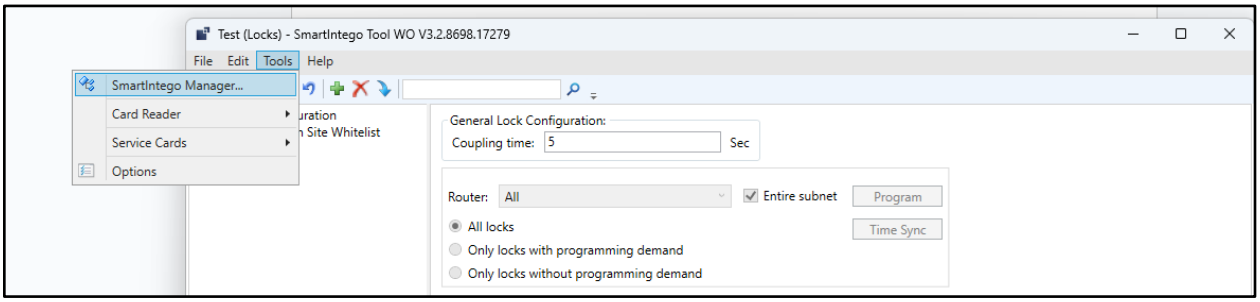


It is also recommended to set an AES password. This password encrypts the network communication between the Gateway Node and the ZukoServices software. To do this, open the menu “Administration” → “AES” and set a password.



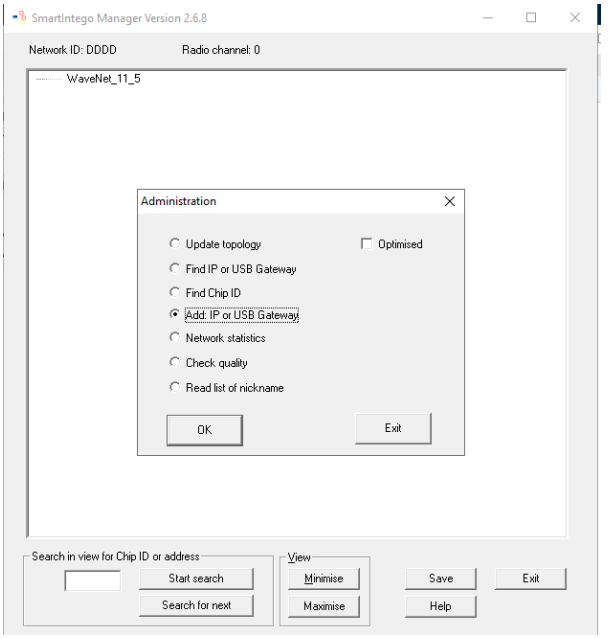
Integration into SmartIntego

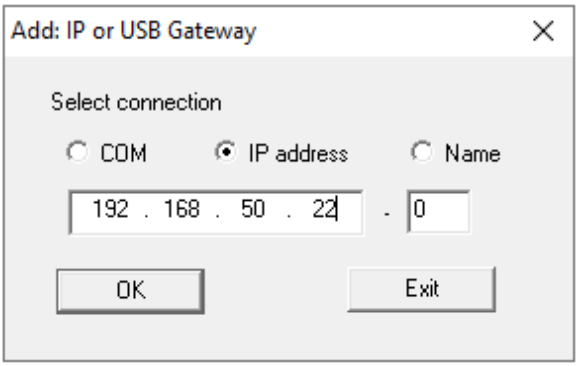
Switch into the program SmartIntego. Open the SmartIntego Manager at “Tools”→ “SmartIntego Manager”.

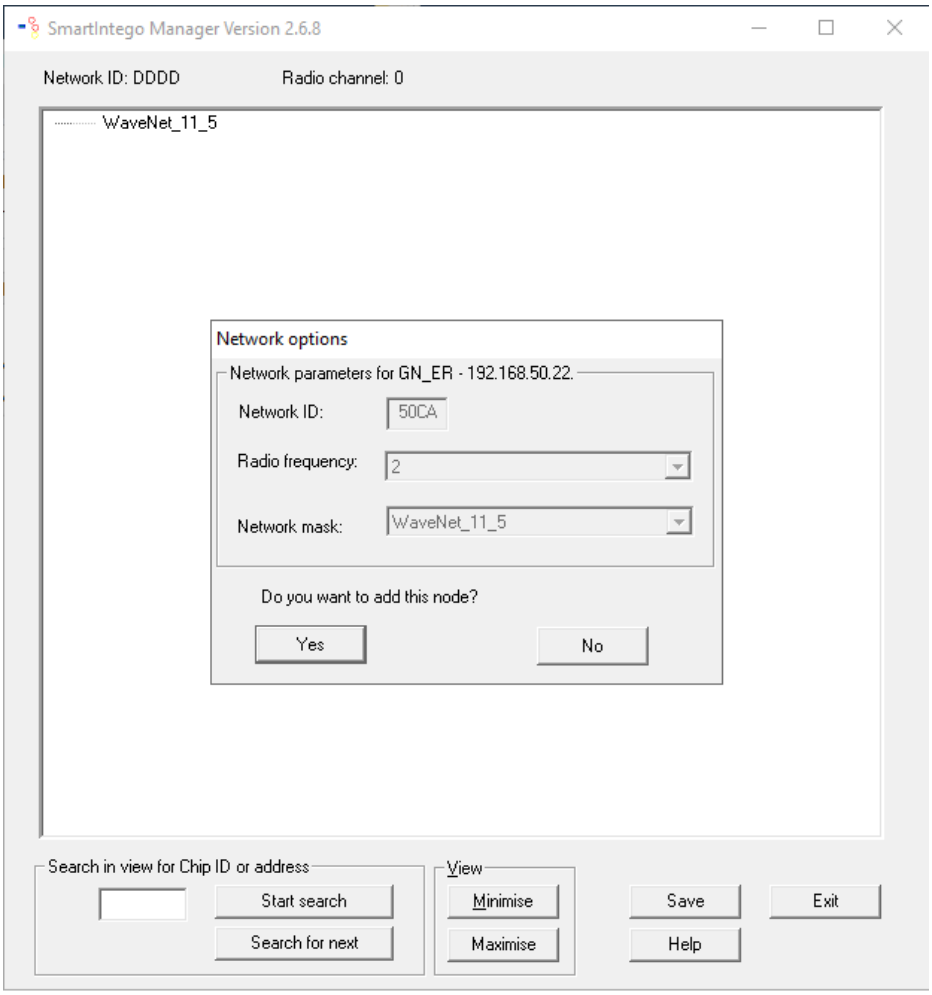


When opening it for the first time, set the WaveNet password. It can be a maximum of 8 characters long. You must not make a typing error, as it is only entered once.

Play it safe and close the SmartIntego Manager by clicking 'Exit', then restart it (“Tools”→ “SmartIntego Manager”) and enter the password again to ensure that the password has been set correctly without typos.

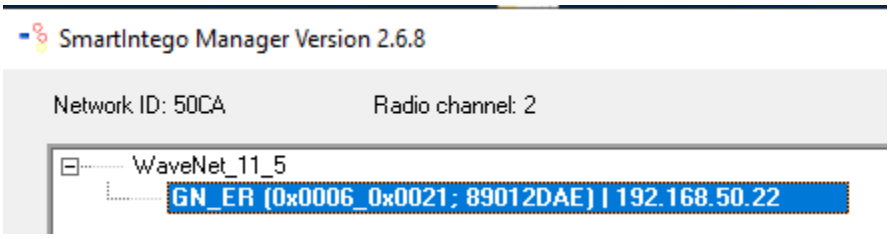
Then right-click on WaveNet. A dialog will appear where you can select “Add: IP or USB Gateway” and confirm by clicking “OK”.	

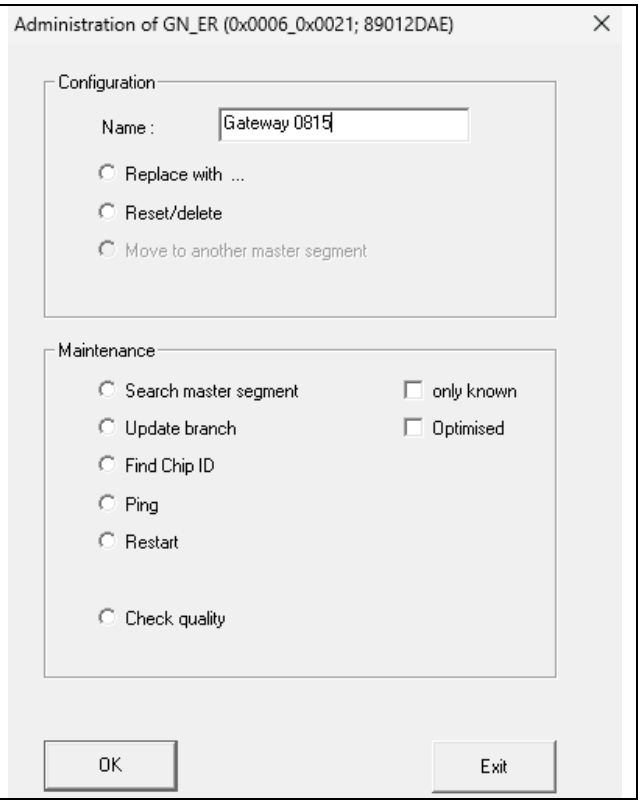
Enter the IP address of the device and confirm by clicking „OK“. By using the second number (-0), you can also set a range. This allows you to add multiple Gateway Nodes simultaneously.	



Press „Yes“.

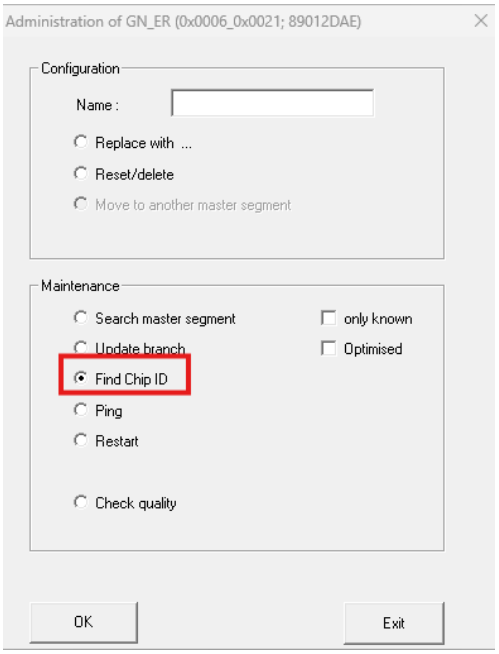
Afterwards, the Gateway Node will appear in the list. Make sure to save your entries!



Optionally, you can assign a name to the gateway. To do so, right-click the gateway, choose a name and click "OK".	

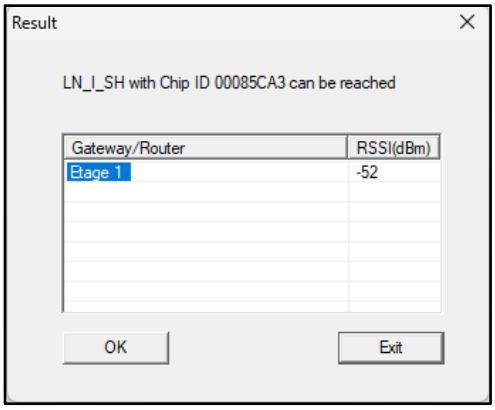
Adding a Lock Node (Cylinder)

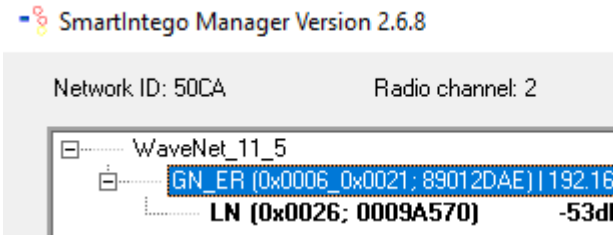
Open the SmartIntego Manager at “Tools“ → “SmartIntego Manager”. A Gateway Node should already have been added. Right-click on the entry of the Gateway Node and select “Find Chip ID”. Click in “OK”.



Enter the Chip ID of the Lock Node. You can find this on the packaging of the device. It consists of 8 alphanumeric characters. Click “Start” to begin the search for the Lock Node and wait a moment.

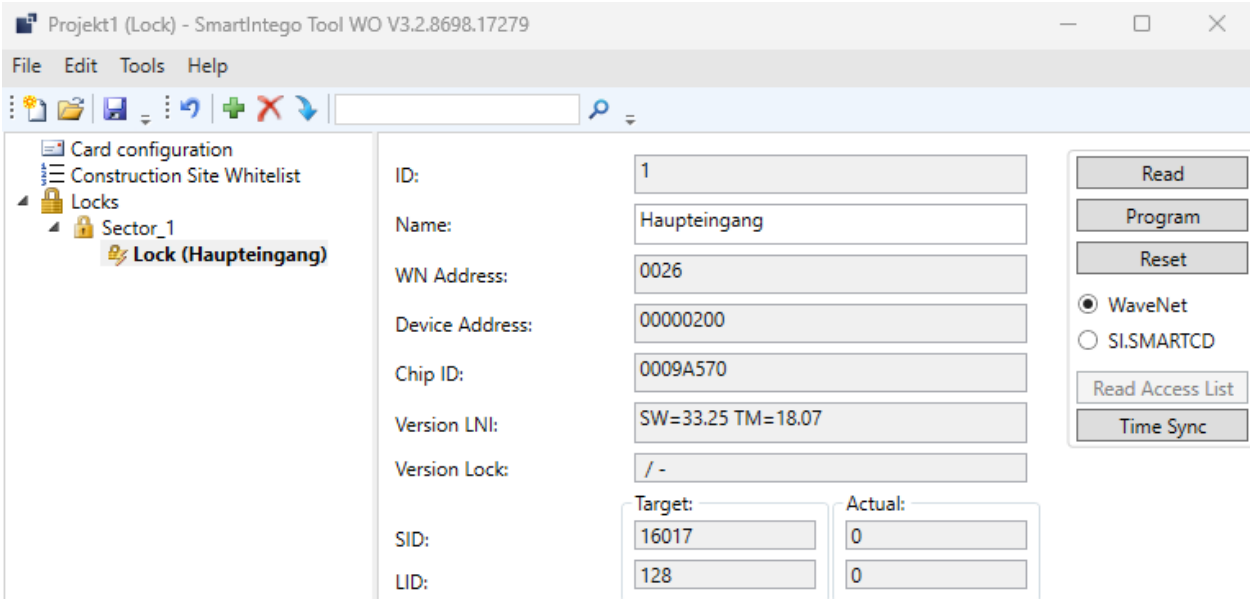
If a Gateway node finds the cylinder, it will appear in the list. Select the Gateway node with the highest signal strength (dBm). So the value that is closer to zero. Pay attention to the dBm value. It should not be lower than -85. If the value is lower than -85, you need to either reposition the Gateway Node, use a signal amplifier antenna, or install another Gateway Node. As an example, a value like -60 dBm is good.





Save your changes and then close the SmartIntego Manager.

Next, assign a name to the cylinder. This name should be descriptive and will later be used in Paxton Net2 as well.



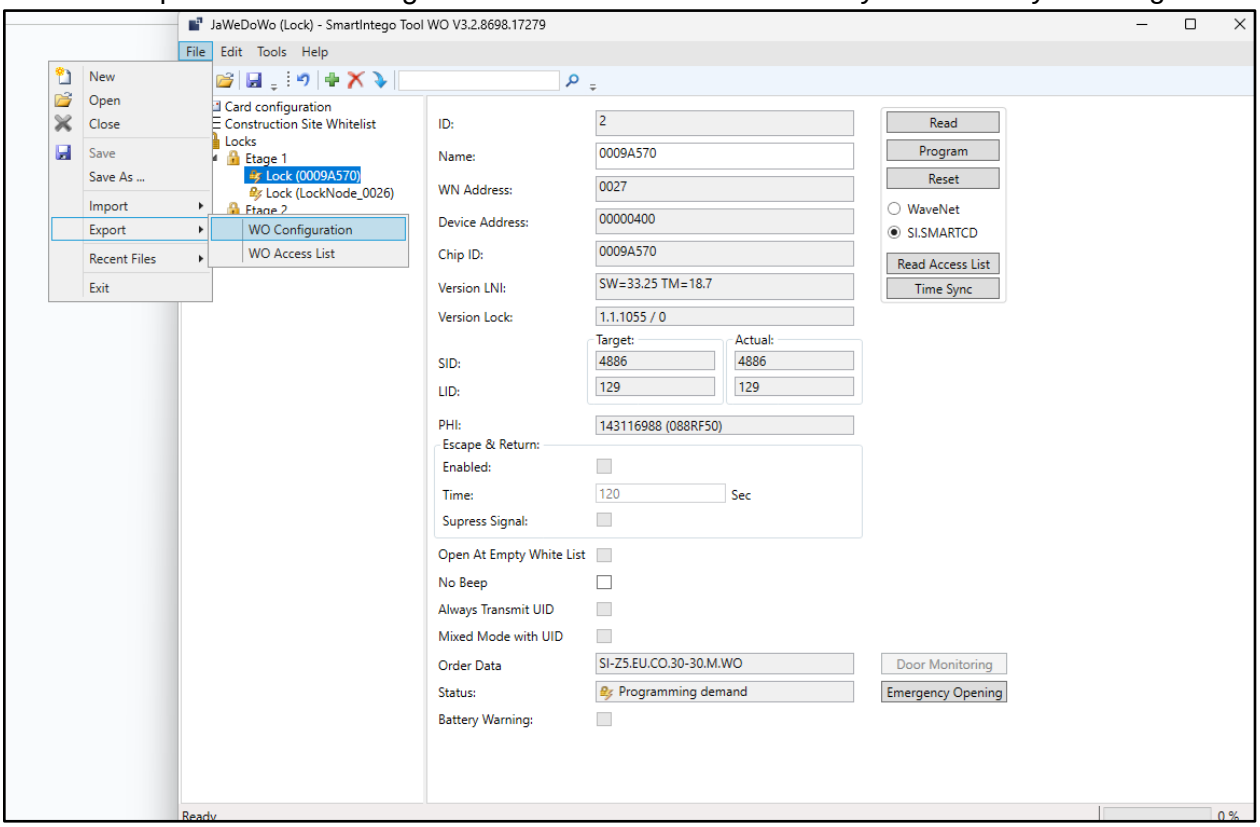
Finally, click „Program“ to transfer the configurations to the cylinder.
Skipping this step may cause the cylinder to behave incorrectly and potentially lead to high energy consumption. Programming via WaveNet can take up to 4 minutes.

Repeat this process for each cylinder and each Gateway.

Save the project again. You can optionally back it up to a secure location.

After all cylinders have been created, you must export the configuration so that you can transfer it to ZukoServices.

To export the SmartIntego project as a CSV file, follow these steps:
“File” → “Export” → “WO Configuration”. Save the CSV file where you can easily find it again.



You have now completed the setup of the SimonsVoss components in the SimonsVoss SmartIntego software. The configuration of the ZuKoServices will follow next.

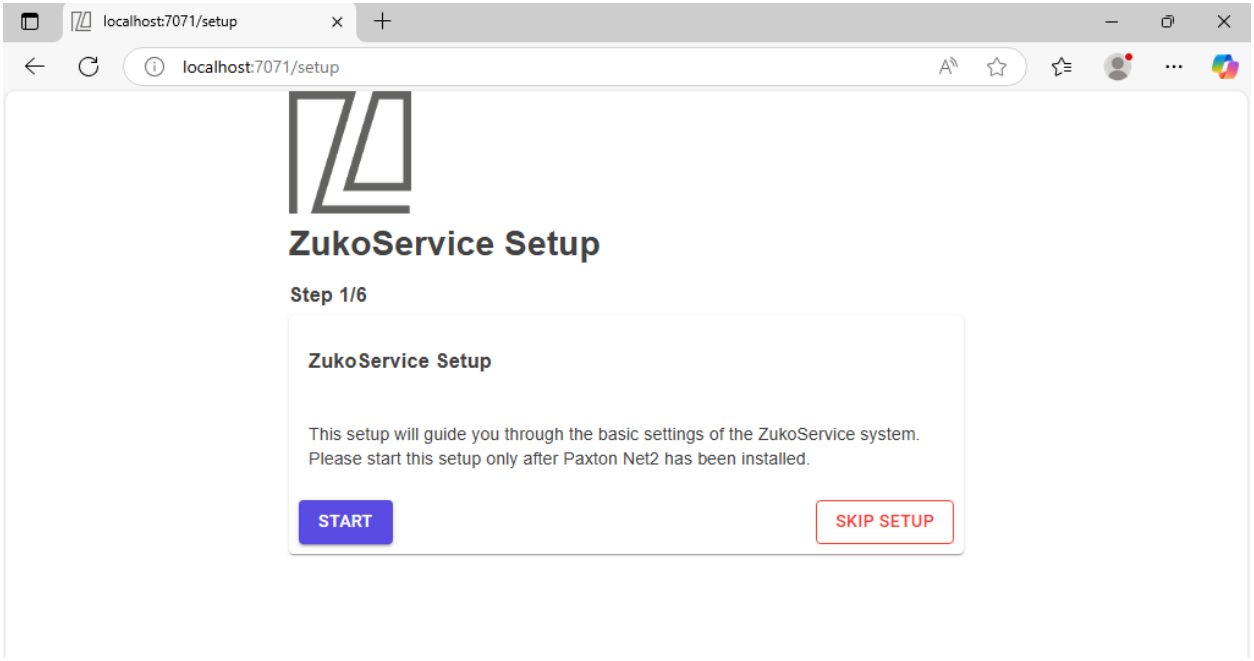
ZukoServices Initial Setup

Now you can access the ZukoServices portal at the URL http://localhost:7071. The default login credentials are as follows:

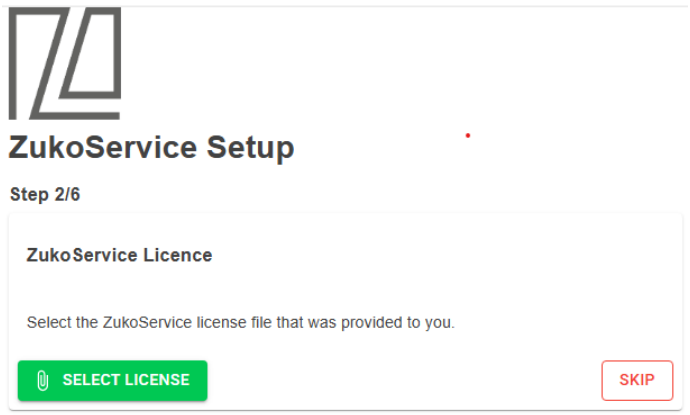
Username: admin

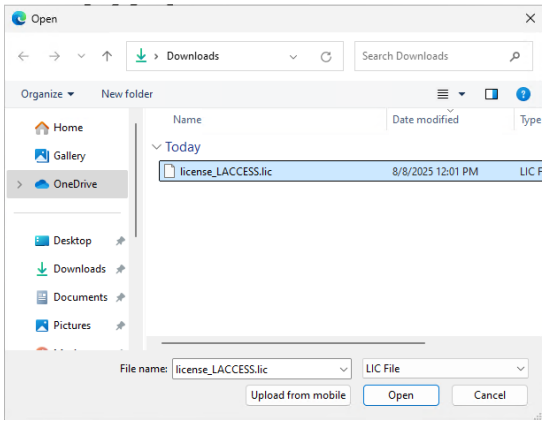
Password: admin

Upon first use of the ZukoServices Portal, a setup wizard will launch. Please follow the on-screen instructions. Click “Start”.

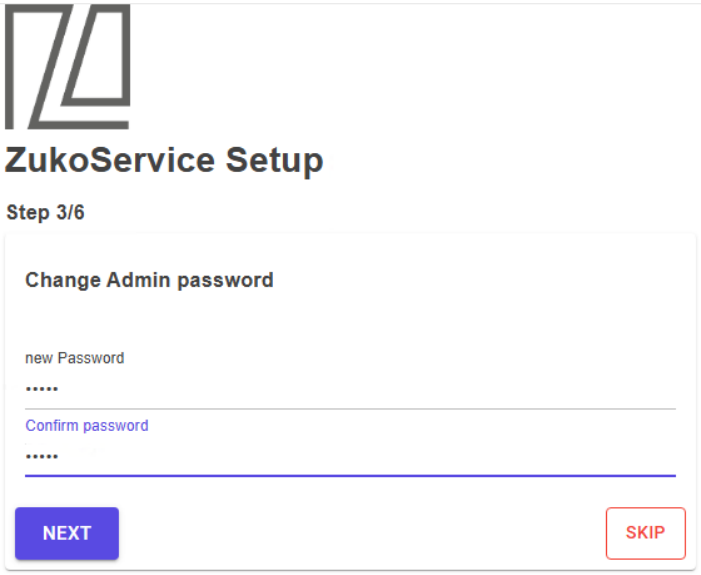


To license the software, click **“Select License”** and choose the license file we have provided to you.

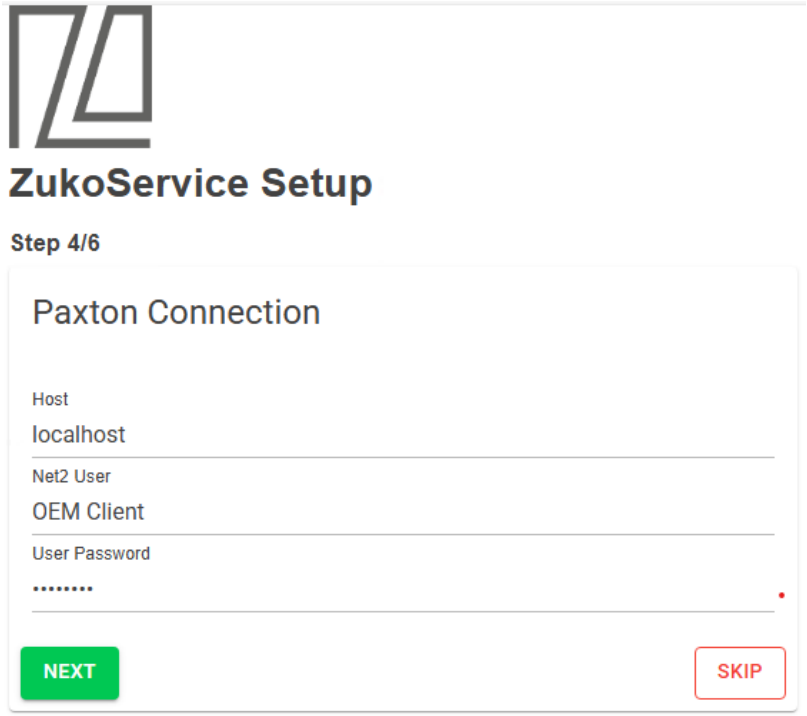




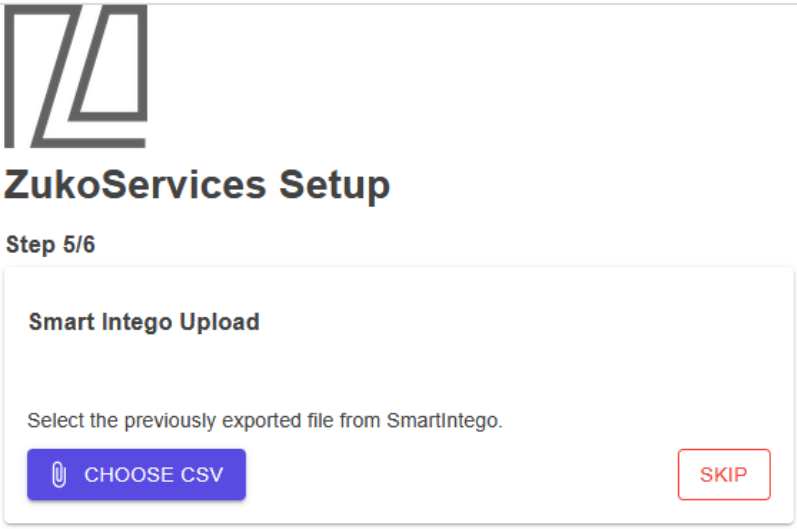
It is recommended to change the default password. Enter the new password twice and click **"Next"**. Make a note of this password in a safe place.



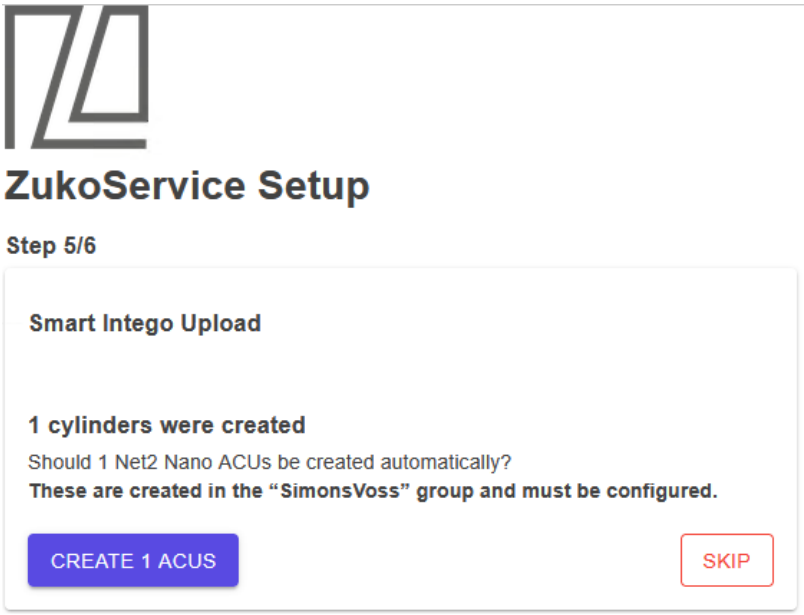
For ZukoServices to function, a connection to the Paxton Net2 API must be established. Enter here the password of the API user that you previously set under the **“Net2 API User”** section of the documentation.



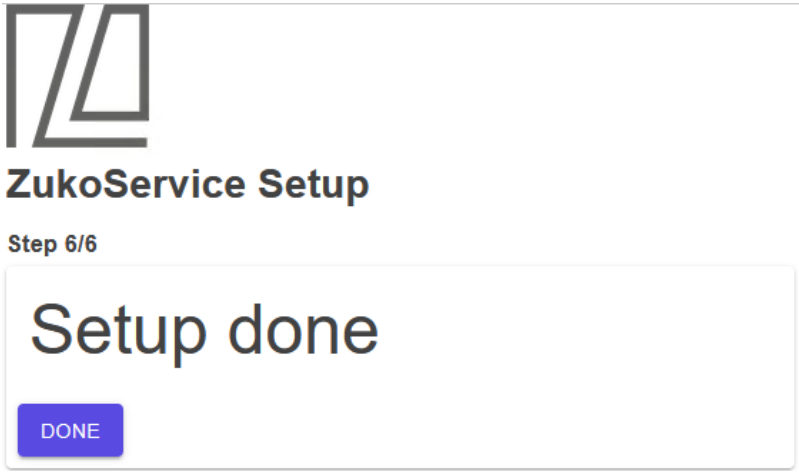
Select “Choose CSV” and specify the previously exported file from SmartIntego.



Click “Create x ACUs” to create empty Paxton Net2 door objects for any SimonsVoss cylinder you have configured in SmartIntego.

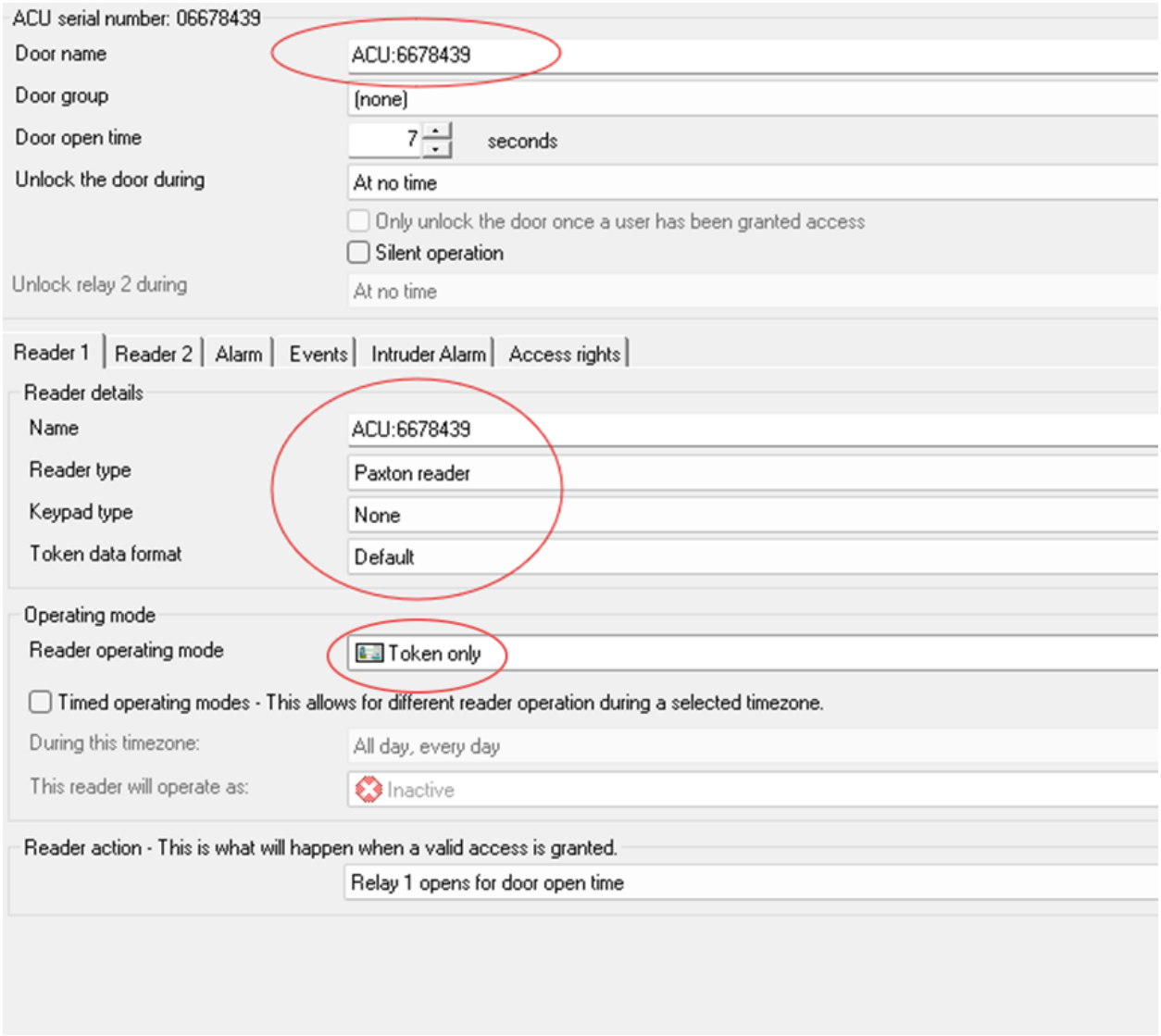


Now you have finished the initial ZukoServices Setup.



Switch to Paxton Net2 Access Control → Doors. An empty door object has now been created for each SimonsVoss cylinder. The linking to ZuKo Services is done via the Paxton Net2 access reader name and the SimonsVoss cylinder name.
Double-click one of the ACUs with the name prefix "ACU" followed by the fictitious 8-digit number (e.g. "ACU 42818939"). Change the freely selectable Access point naming. For a better overview, you can use the same name that was specified in Smart Intego Wireless Online.

Make sure that the reader´s name corresponds to the naming of the cylinder in SmartIntego. Additionally, ensure that the “reader type” and “operating mode” are configured correctly.



Click **„Apply“**.

Repeat this for each SimonsVoss cylinder, selecting one of the empty ACU objects each time.

System Configuration

The configuration of ZukoServices is carried out via the web interface. To begin, log in to the system again:

URL: http://localhost:7071

Username: admin

Password: admin

Operation

Events

Events can now be accessed both in the Net2 Access Control Software and on the ZukoServices web interface. Here, you will find all communications between ZukoServices and the online cylinders.

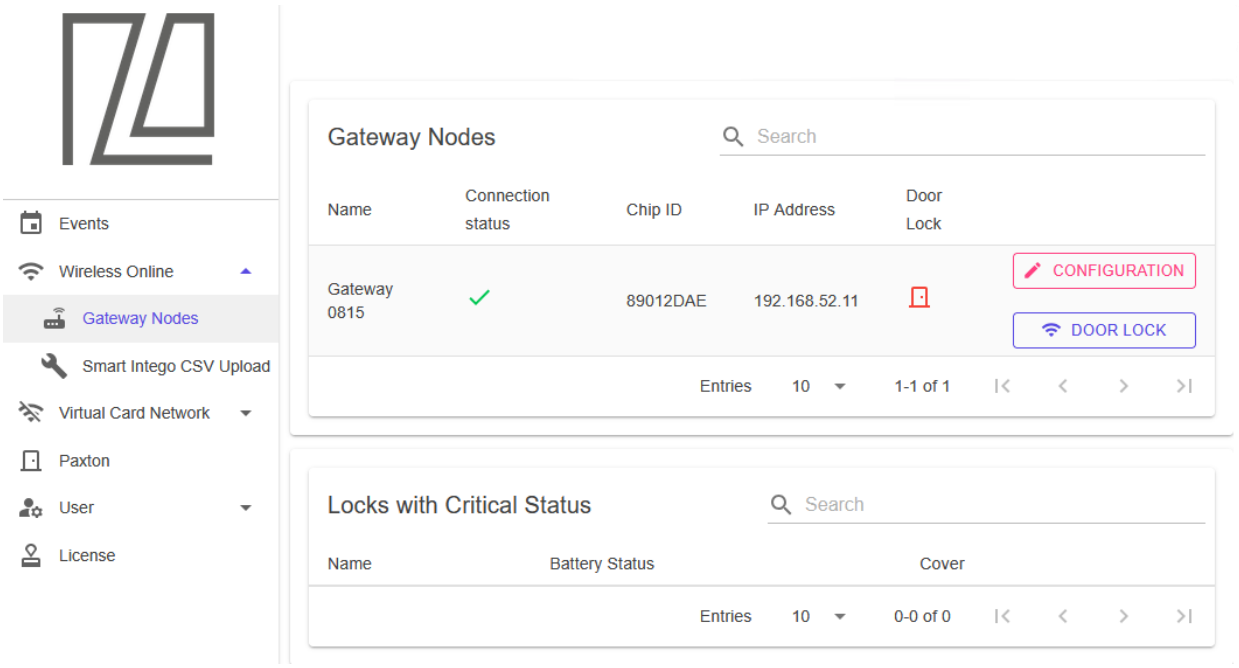
If you can't see any events in Paxton, please restart the computer or manual all LACCESS Services.

The following events are recorded in ZukoServices:

Deleted construction Site Whitelist	The SmartIntego Software provides the option to manage whitelist entries. These entries are deleted during the system startup of ZukoServices.
Status inquiry	ZukoServices queries the status of the cylinders and gateways on a daily basis.
Permanent access granted by user	A cylinder has been permanently unlocked by a user
Temporary access granted	A cylinder has been temporary unlocked by a user.
Access denied	The Access has been denied by ZukoServices System
Access granted	The Access has been allowed by ZukoServices System

Gateway Nodes and Cylinders

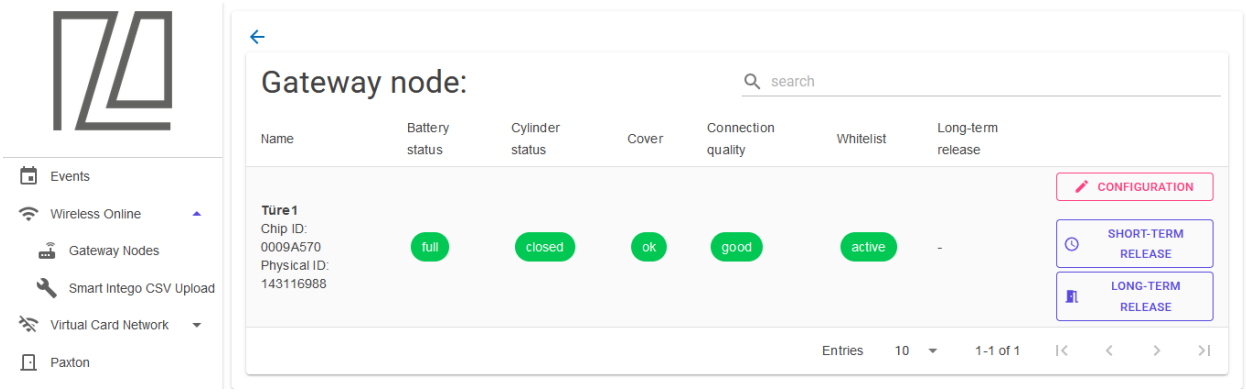
All imported Gateway Nodes are located at ZukoServices web interface (http://localhost:7071) menu “Wireless Online” → “Gateway Nodes”. In the overview, you will find relevant data for the Gateways as well as the connected cylinders.



Name	Gateway Node name
Connection status 	Indicates whether a Gateway Node is reachable over the network. If there is no connection, the current cylinder status cannot be determined and displayed. Maybe you must set the AES password described later in the documentation (see Gateway Configuration - AES Encryption).
Chip ID	The Chip ID is used to uniquely identify a Gateway Node.
IP address	Shows the assigned IP address of a Gateway Node
Door lock	Here, all cylinders assigned to the Gateway Node are listed. The status of a cylinder is

	marked in green or red. A „grey“ status indicates that the Gateway Node is not reachable, and the status cannot be determined. The status of a cylinder is actively queried. The cylinder transmits its status with every event it sends to the Gateway Node. This approach helps extend the battery life of the cylinder.

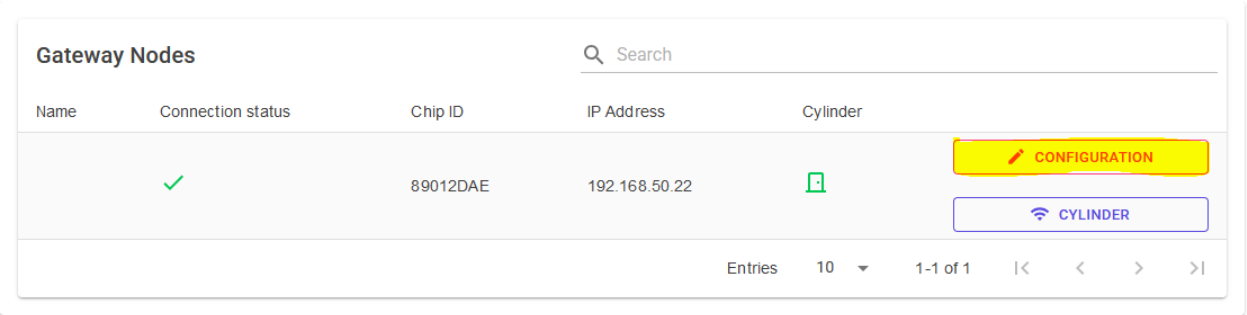
Click on the "Door lock" button for additional settings and details.
The cylinder view allows for both temporary and permanent unlocking of a cylinder.



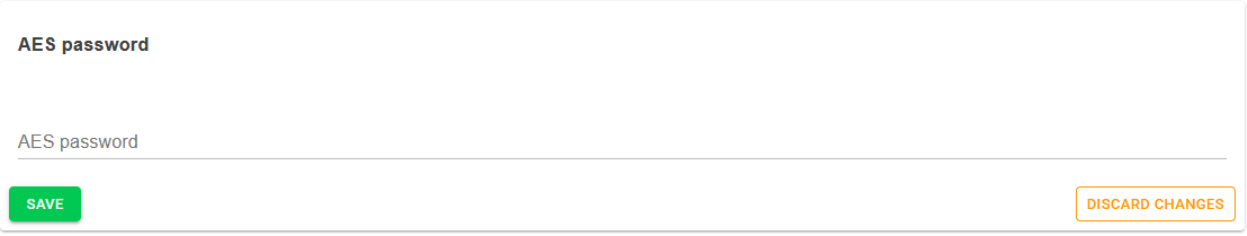
The configuration view of the cylinders shows the current whitelist written to a cylinder and allows you to disable this list (not recommended).
Additionally, you can activate cylinder monitoring at this point. This monitoring should only be used in exceptional cases, as it significantly increases energy consumption.

Gateway Configuration - AES Encryption

Under the "Gateway Nodes" menu of the ZukoServices web interface (http://localhost:7071), click the "Configuration" button to open the settings of a Gateway Node. Here, you have the option to enter a defined AES password. This password is used to decrypt network communication between the Gateway Node and the ZukoServices system.



Enter the AES password that you assigned in the SimonsVoss Gateway configuration (see chapter: Setting up the Gateway Node) and save your entry.



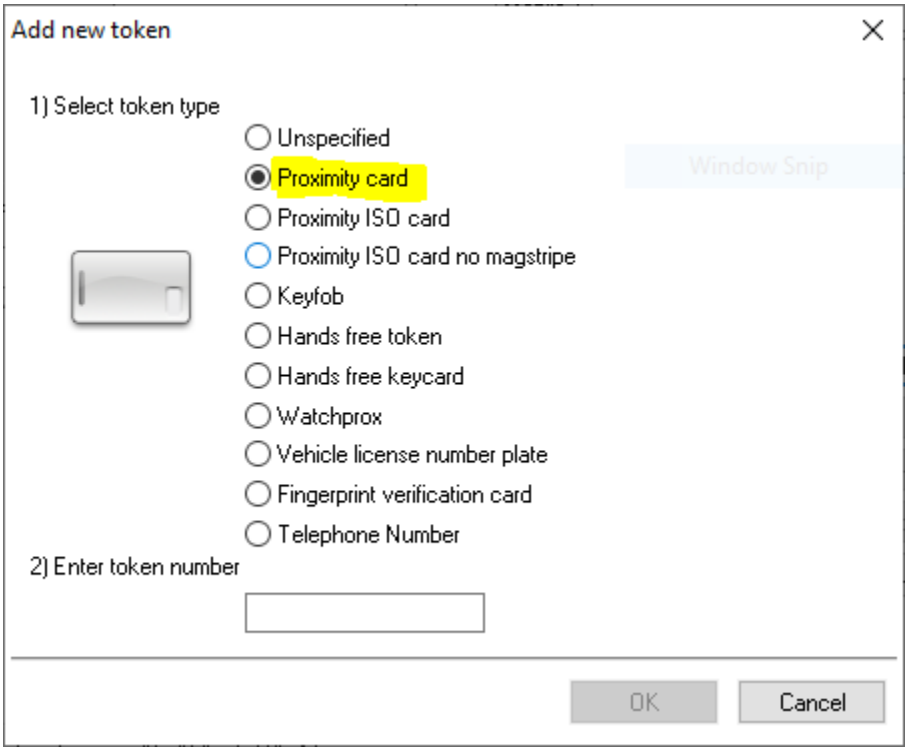
Whitelist

Simons Voss AX cylinders offer the security mechanism of a whitelist. This is a list of tokens written to the cylinders, ensuring they can open the doors in the event of a system failure or reboot. This ensures that access to certain doors is always available.

Whitelist entries are imported from Paxton Net2 Access Control. For a user to receive whitelist access, their token must be defined as a **"Proximity card"**, and they must have access rights to the door.

It is recommended that only a selected group of people be granted whitelist access.

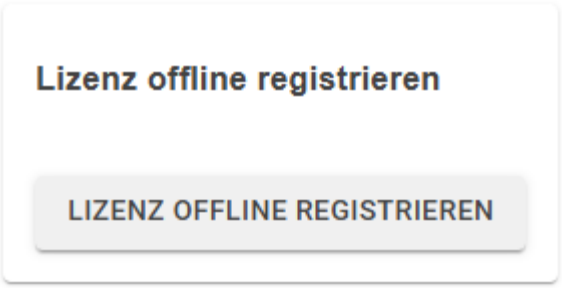
If tokens have already been defined as **"Proximity card"** in the past, change the token type to, for example, **"Proximity ISO card"** or another type. This will only affect the displayed icon at this point.



Complete Licensing

After the configuration, the system must be registered. This will link the SimonsVoss Gateway Nodes and Feig readers to your license.

Click the "Register License Online" button in the ZukoServices web interface (http://localhost:7071) under “License” to complete the registration. This process can only be done once. If the SimonsVoss or Feig hardware has been changed and the license is no longer valid, please contact support at (+49)0221 – 4744270).



If the system does not have internet access, click the "Register License Offline" button. A file will be generated and downloaded.

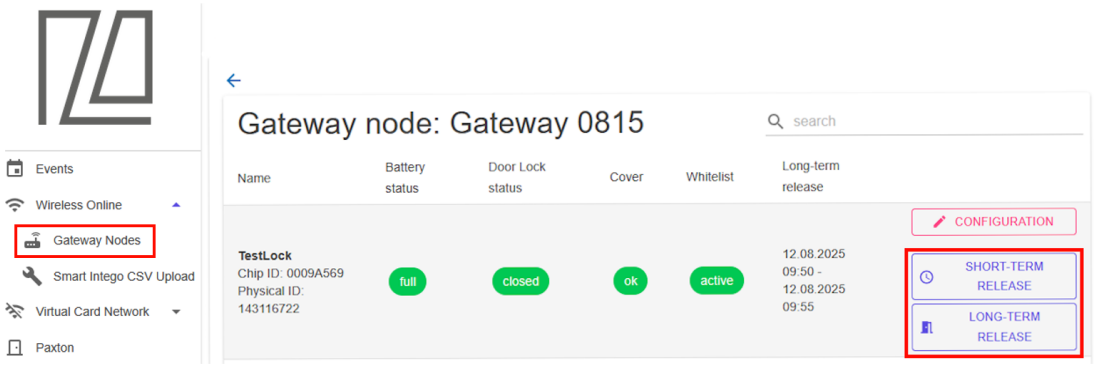
This file can be validated and registered by support. Send the file to support (support@laccess.de), and they will send you a registered license file. This file can then be uploaded via the license upload feature.

Long- and Short-Term Release

There are different ways to define a release.

ZukoServices

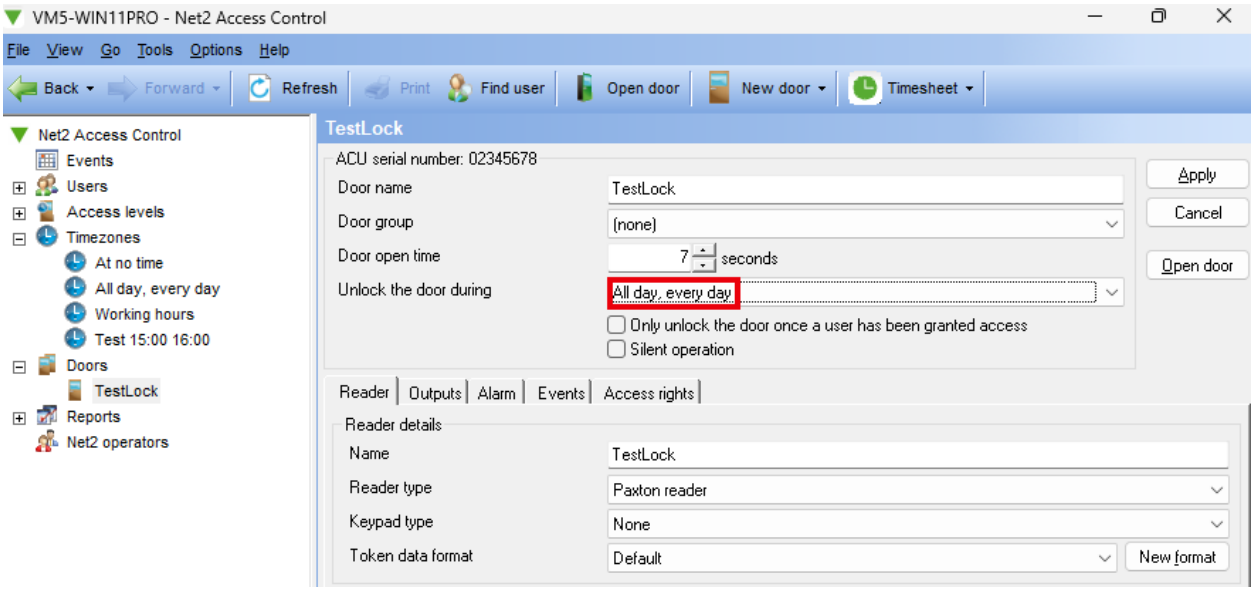
In the ZukoServices interface, in the cylinder view below the gateway overview, you can initiate a short-term release. The cylinder will then open immediately for 4 seconds and then close again. In the same location, you can also initiate a long-term release. The cylinder will open immediately and remain open until the long-term release is cancelled there.



Paxton Net2

The long-term release option in Paxton is also supported. Once the release is configured, the SimonsVoss cylinder will automatically open for the specified period of time and then close again.

Note: Please note that the start date of the defined time zone must be in the future. For example, if the default time zone “All day, every day,” this will not occur again until 00:00. The accuracy is to the minute.



Reset a Lock Node (Cylinder)

To reset a Lock Node that has already been created in the project, please follow these steps:

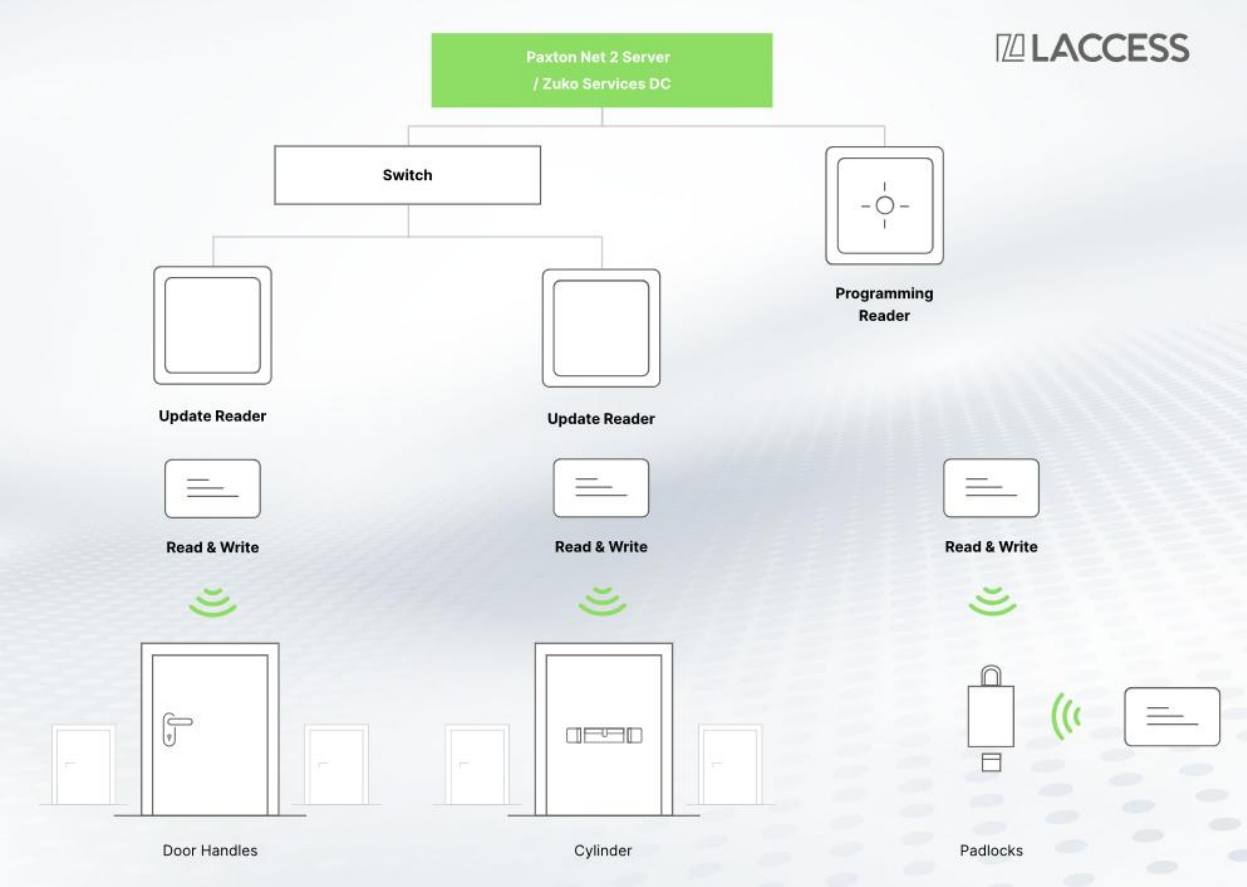
1. Open the SmartIntego WO Software and click on the corresponding cylinder or fitting that you want to reset.
2. Then, perform the reset via WaveNet.

To ensure that cylinder is completely reseted and contains no data, proceed as follows:

3. Navigate to the „tools“ menu in the SmartIntego WO Software and select „SmartIntego Manager“
4. Enter the password and right-click on the desired Lock Node
5. Select „Reset/delete“ to fully reset the cylinder.

SmartIntego Virtual Card Network

The SmartIntego Virtual Card Network communicates without a network connection. Data exchange between the ZukoServices system and the offline cylinders occurs through writing and reading the tokens. The system consists of the following components:

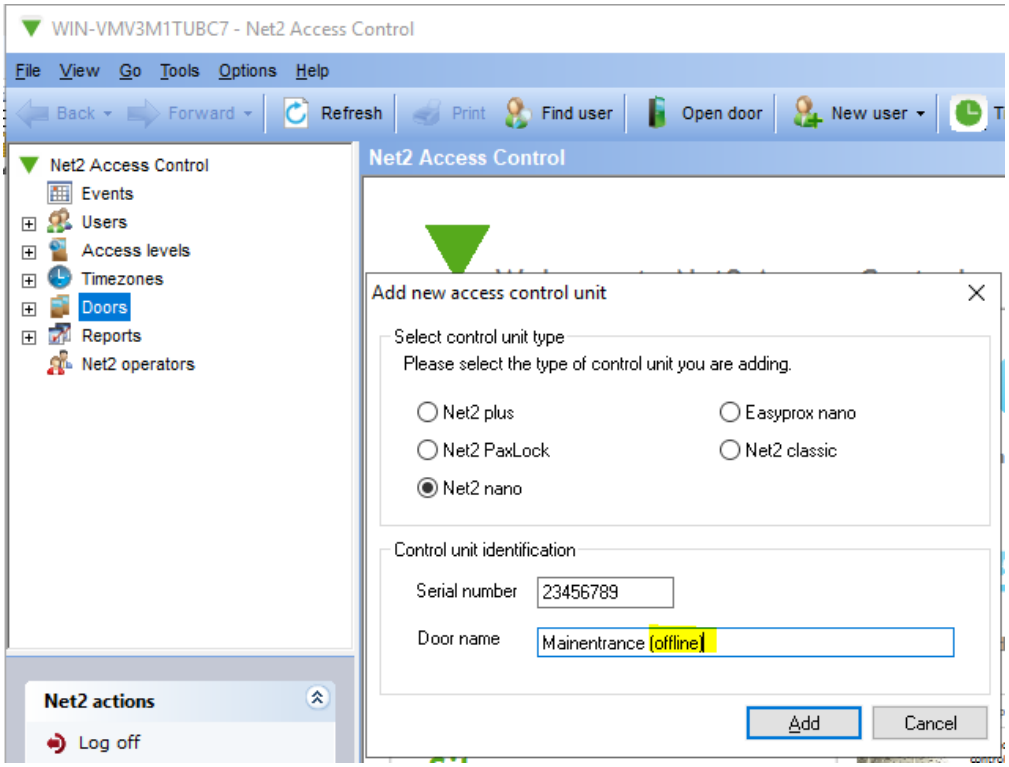


Update Reader	The update reader is usually located at the entrance of a premises, allowing each visitor to scan their personal token there. This enables the system to write to and read from the token.
Program Reader	Each token in the system must be initially programmed.
SimonsVoss offline cylinder	The offline cylinders are programmed once. The programming determines which access zone they belong to.
ZukoServices	ZukoServices provides tools for reading and writing tokens. It also offers support for programming the cylinders.

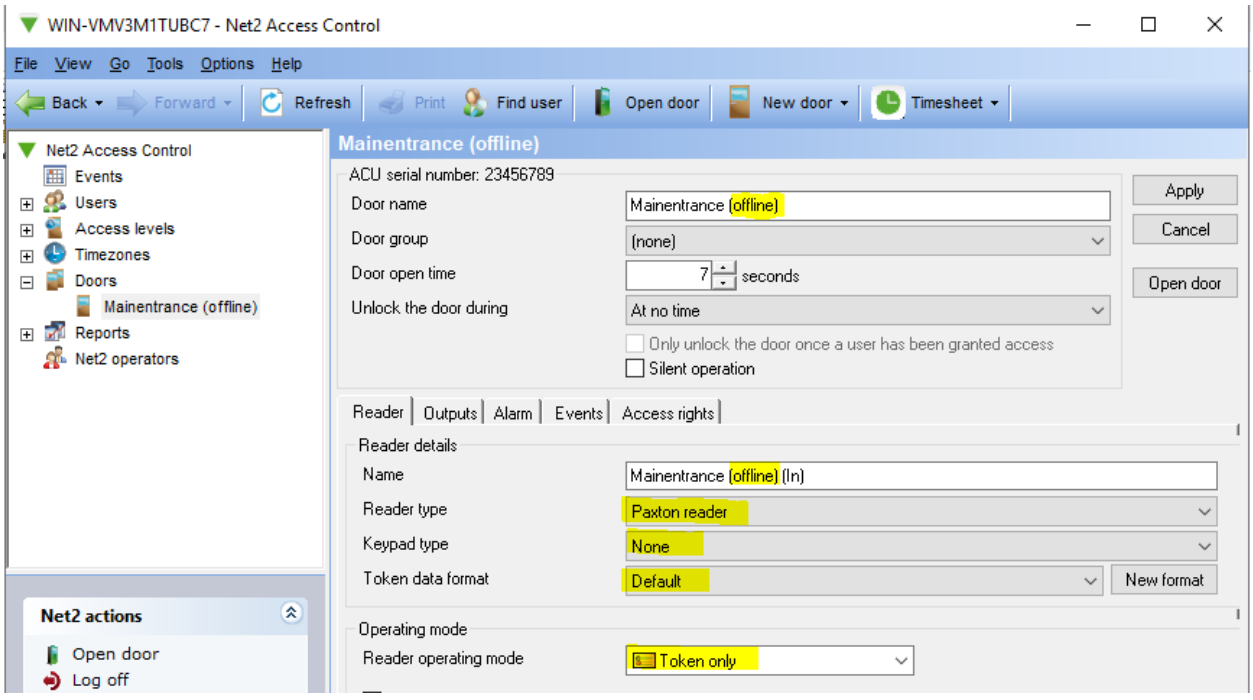
AX Cylinder Programming

First, create your SimonsVoss offline cylinders as ACU access points in the Paxton Net2 Access Control software. To do this, right-click on "Doors" and select "Add new access control unit."

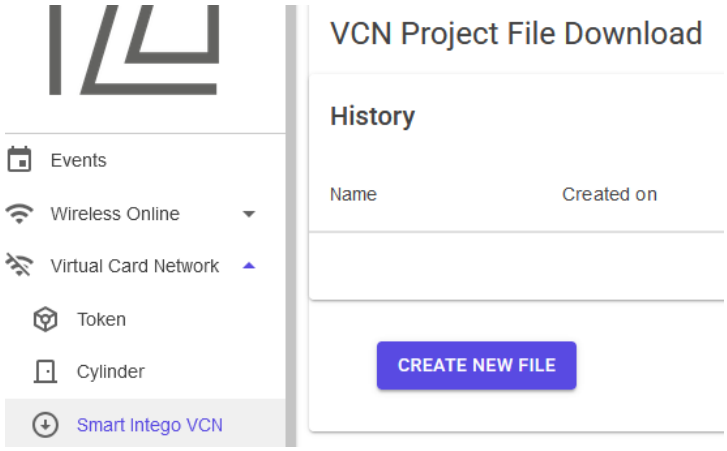
ACU Type	Net2 Nano
Serial Number	Enter a fictitious 8-digit number that has not been used by any other ACU (e.g., 12345678).
Access Point Naming	Write "offline" and choose a descriptive, memorable name for the access point.



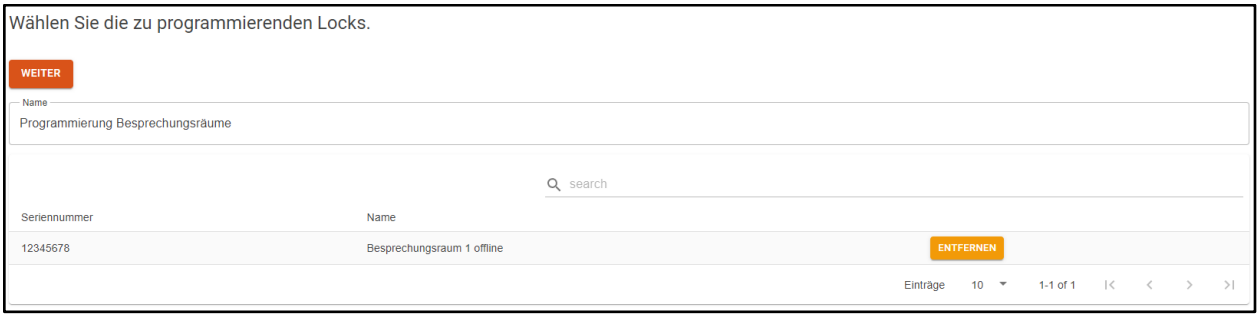
Edit the ACU by double-clicking on the respective cylinder. Make sure that the name of the reader includes the code word "offline", e.g., "Meeting Room (offline)". Additionally, configure the reader details and operating mode:



Next, go to the ZukoServices Web Portal (http://localhost:7071) and navigate to the menu item "Virtual Card Network" → "Smart Intego VCN".



Here, you'll find a list of created programming tasks. Click on "Create New File". Choose a name for the new programming task. This name is for later identification. In this view, all offline cylinders that have been created in Paxton Net2 Access Control with the keyword "offline" will be listed. Click "Add" for each lock that needs to be programmed. Then, click "Next".



In the second view, you have the option to choose which programming you would like to perform using Smart CD:

Reset	Already programmed cylinders can be reset in order to replace them or reprogram them.
Programming	To program a cylinder, select this option. During programming, access points and time profiles are written to the cylinder. If you change time profiles or access groups in Paxton Net2 Access Control, a reprogramming of the affected cylinders is required. To reprogram, select the "Reset" option and then "Programming."
Configure Time	The time of the cylinders should be updated annually to ensure that the time is correctly synchronized.
Read Access Data	SmartIntego offers the ability to read cylinders and view access logs.
Emergency Opening	SmartIntego provides the ability to activate the cylinder lock and open a door.

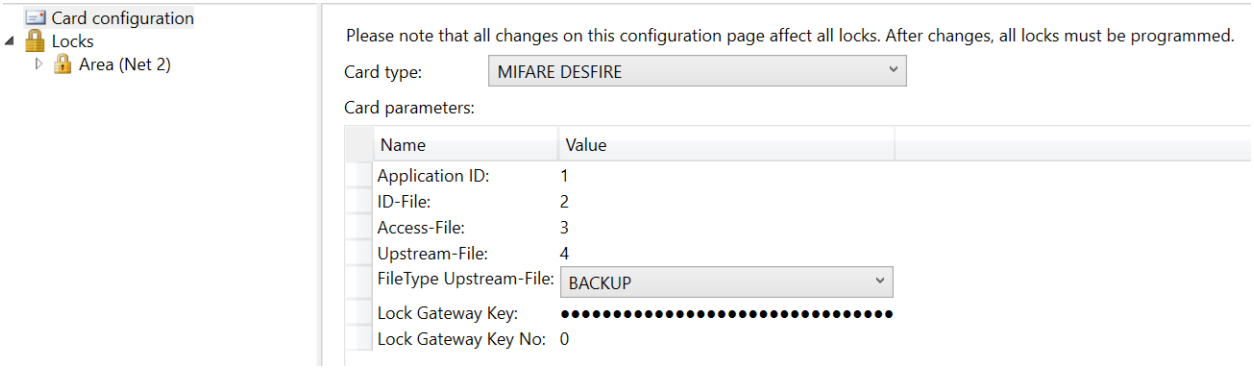
Click on "Create File" to complete the process. Select the download button to download the file.

Open the program "SmartIntego VCN" and create a new project:

Name	Name of the project
Password	Password to open the project (The password must be at least 8 characters long, contain both an uppercase and a lowercase letter, and include a number or special character).
Confirm Password	Confirm password
Virtual Card Network Password	This password encrypts the Lock Nodes. With this password, it is possible to reset devices. The password must be at least 8 characters long and cannot be identical to the project password.

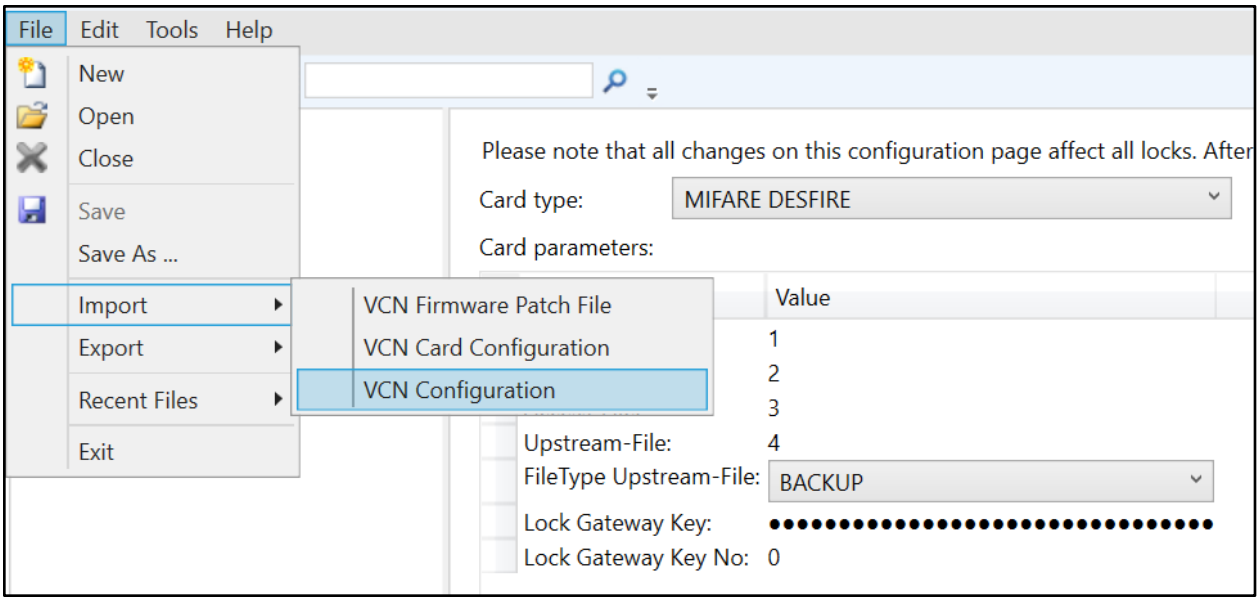
Virtual Card Network Confirm Password	Confirm password
Passwords hint	Note on passwords

First configure the “Card configuration”:



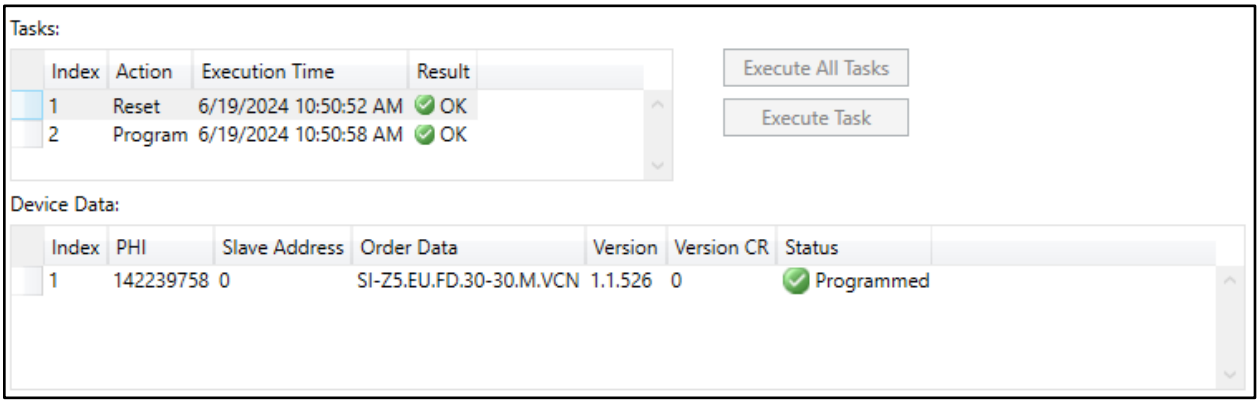
The fields are freely selectable and depend on your token programming. The field "Lock Gateway Key No." should always have the value "0". Currently, only "Card Type" → "MIFARE DESFIRE" and "FileType Upstream-File" → "BACKUP" are supported. The Lock Gateway Key must be 32 hexadecimal characters long and is not automatically generated. Create a Gateway Key using numbers 0-9 and letters a-f. Save your input!

Next, import the previously generated file from ZukoServices. To do this, go to the tab "File" → "Import" → "VCN Configuration".



You will now find all the offline cylinders that were previously created in Paxton Net2 Access Control and exported through ZukoServices in the SmartIntego VCN tree structure.

Connect the SmartIntego SmartCD programmer to your PC, click on a cylinder in the tree structure, hold the cylinder against the programmer, and click on "Execute All Tasks".



Repeat the process for each offline cylinder that you wish to program.

Token Programming

Card Configuration

First, set up the card configuration in ZukoServices. To do this, open ZukoServices in the browser (http://localhost:7071) and navigate to "Virtual Card Network" → "Card Configuration." Apply the settings from SmartIntego VCN and save the configuration.

NFC Reader

Connect a Feig OBID RFID reader to your network and configure it using the Reader Discovery Software. Ensure that the Windows Firewall is appropriately configured or turned off. When you see the reader in the software, right-click on it and select "Setup Network Configuration." If you want to change the parameters, first select "change." The reader must be on the same network as the ZukoServices software. Once you're done with the network settings, click OK.

You will need one RFID reader for programming the tokens and a second reader as an update reader.

Next, open ZukoServices in the browser (http://localhost:7071) → "Virtual Card Network" → "NFC Readers." Add a "Programming Reader" and an "Update Reader" (see the "Type" dropdown). You will need to enter the IP addresses assigned to the respective readers in the Reader Discovery Software. Save your entries.

Token

Switch to ZukoServices, go to "Virtual Card Network" → "Token" → "Create Token," and select a programming reader that is accessible to you. You have the following token types to choose from:

Access-Token	Standard token for regular users. Access permissions and time profiles from Net2 are applied. The token must be regularly updated at an NFC update reader to maintain its validity..
Toggle-Token	This token permanently opens or closes a door. Access permissions and time profiles from Net2 are applied. The token must be regularly updated at an NFC update reader to maintain its validity.
Blocklist-Token	The blocklist token cannot open doors. It is only used to distribute information, such as the blocking of specific tokens, to various cylinders. It should be updated at the update reader before use.
Emergency-Token	The emergency token can permanently open any cylinder. It is not modified by the update reader and has no expiration date.

Press the "Program Token" button and present a token to the NFC reader until the process is complete.

Token template

You can make additional token settings under "Virtual Card Network" → "Card Configuration" in the "Token Templates" section.

Transponder validity in hours (update interval)	Enter the number of hours for which a token should be valid. After this time expires, the token must be updated at the NFC update reader. This mechanism ensures that lost tokens can no longer be used in a timely manner.
Blocklist duration in weeks	Enter the number of weeks a blocklist entry should be stored on a cylinder. If a token is marked as lost in Net2, it will be recorded as lost and inactive on the cylinder for this duration.

Logs

Cylinder

Under the menu item “Virtual Card Network” → “Cylinder,“ you can find all offline cylinders for which information has already been collected. You can view the battery status of the cylinders as well as the access events for each cylinder.