SmartIntego WO
Step by step

Manual

12.11.2021

SimonsVoss
technologies

Contents

1 General safety instructions

Signal word (ANSI Z535.6)	Possible immediate effects of non-compliance
DANGER	Death or serious injury (likely)
WARNING	Death or serious injury (possible, but unlikely)
CAUTION	Minor injury
IMPORTANT	Property damage or malfunction
NOTE	Low or none

WARNING

Blocked access

Access through a door may stay blocked due to incorrectly fitted and/or incorrectly programmed components. SimonsVoss Technologies GmbH is not liable for the consequences of blocked access such as access to injured or endangered persons, material damage or other damage!

Blocked access through manipulation of the product

If you change the product on your own, malfunctions can occur and access through a door can be blocked.

- Modify the product only when needed and only in the manner described in the documentation.

NOTE

Intended use

SmartIntego-products are designed exclusively for opening and closing doors and similar objects.

- Do not use SmartIntego products for any other purposes.

Qualifications required

The installation and commissioning requires specialized knowledge.

- Only trained personnel may install and commission the product.

Modifications or further technical developments cannot be excluded and may be implemented without notice.

The German language version is the original instruction manual. Other languages (drafting in the contract language) are translations of the original instructions.

Read and follow all installation, installation, and commissioning instructions. Pass these instructions and any maintenance instructions to the user.

2 Meaning of the text formatting

This documentation uses text formatting and design elements to facilitate understanding. The table explains the meaning of possible text formatting:

Example	button
☑ Example □ Example	checkbox
◉ Example	Option
[Example]	Tab
"Example"	Name of a displayed window
| Example |	Upper programme bar
Example	Entry in the expanded upper programme bar
Example	Context menu entry
▼ Example	Name of a drop-down menu
"Example"	Selection option in a drop-down menu
"Example"	Area
Example	Field
Example	Name of a (Windows) service
Example	Commands (e.g. Windows CMD commands)
`Example`	Database entry
[Example]	MobileKey type selection

3 SmartIntego Tech Kit

The SmartIntego Tech-Kit helps you to perform the initial operation and operate your SmartIntego locking system.

It contains:

- Configuration Software
- System description
- Step-by-step instructions
- Current firmware versions
- Manuals

Versioning

You can recognise the current version in the file name (year month, e.g. 20-01). You can find the latest version of the SmartIntego-TechKit in the partner section of the SmartIntego website (*https://www.smartintego.com/int/home/home*).

4 Planning a SmartIntego project

The successful implementation of your SmartIntego project requires detailed planning. This planning consists of several steps:

1. Check conditions on site (see*Check conditions on site [▸ 9]*).
2. Measure the doors (see *Measure doors [▸ 9]*).
3. Illuminate WaveNet (see *Illuminate WaveNet [▸ 12]*).
4. Order your SmartIntego components (see *Ordering components [▸ 16]*).
5. Plan your installation (see *Planning the installation process [▸ 16]*).

Other parameters may be important. However, this document is limited to the technical conditions of the SmartIntego components and their configuration.

4.1 Check conditions on site

Consider the following in the review:

Environment	SmartIntego components required
▪ Floor plans ▪ Different areas ▪ Fire safety regulations ▪ ESCAPE ROUTES ▪ Existing or planned cabling (network/RS-485) ▪ Power supply (external power supply or PoE) ▪ Restrictions due to design/architecture ▪ Concealed or visible installation of the infrastructure ▪ Uniform design for all locking devices (also mechanical) ▪ Special features in the IT environment ▪ Type of doors ▪ System functionalities	▪ Locking cylinder ▪ SmartHandles ▪ GatewayNodes (RS-485 or Ethernet) ▪ PIN code terminal ▪ Node IO

4.2 Measure doors

1. Measure each door in the project individually (values to be measured depend on the locking device type, see table).

2. Enter the results of the measurement directly in the SmartIntego-Order-Tool.

Measure the following values:

Locking cylinder	SmartHandle
Profile (European profile, Swiss round profile, ...) SmartIntego technology (WirelessOnline) Desired locking cylinder properties (see price list) CO (Comfort = One side permanently engaged mechanically) FD (freely rotating = knob with reader on both sides) AP2 (anti-panic version) HZ (Half cylinder) ... External dimensions Inside dimension	Profile (European profile, Swiss round profile, mechanical...) Desired mechanical overrideability (MO) SmartIntego technology (WirelessOnline) Desired properties of the SmartHandles (see price list) SI-S2 (SmartHandle AX) ... SH (SmartHandle 3062) ER (Escape and Return = time-controlled return function) WP (Weatherproof) DM (internal sensors) DM (external sensors) Door thickness Asymmetrical installation of the mortise lock (see SH manual) Spindle (Note the asymmetrical installation of the square on the SI:SmartHandle). Fastening Centres distance Version Handle design outside Handle design inside Surface (colour, finish) Options Cover (narrow or wide)

4.3 Illuminate WaveNet

Before ordering the components, measure the planned WaveNet in the building. Thorough, planned illumination ensures the following objectives (in contrast to the Pi-mal thumb method):

- Suitable locations for the GatewayNodes:
  - Interference-free connection to locking device (use reflections from walls, avoid radio shadows from door frames)
  - Fulfilled specifications of architects/builders regarding the visibility of the components
  - Compliant fire protection and escape route regulations
- Minimum number of GatewayNodes
- Use of existing cabling and thus
- Reduction of set-up costs

4.3.1 Components required

You need the following components to illuminate the planned WaveNet:

- BAMO.EU
  - Base power supply: 9V block battery or power supply (WN.POWER.SUPPLY.PPP)
  - Power supply of mobile station: 1/2AA battery (3.6 V_{DC})
- Telescopic rod or tripod

BAMO handset	Base station
Ready Signal Noise Error On 100% 90% 80% 70% 60% 50% 40% 30% 20% 10% SimonsVoss technologies	

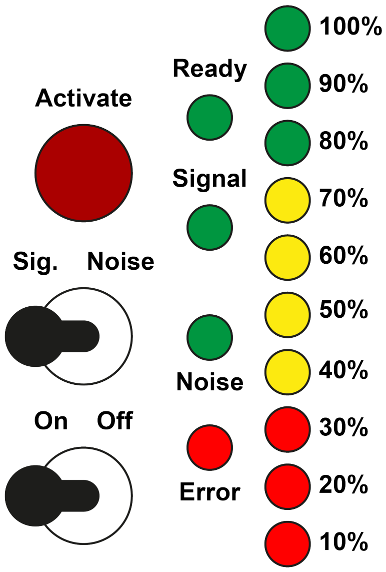
4.3.2 Measure test by test

Test the communication between the base and handset.

✓ Base and handset switched on.

- Perform a short distance measurement.

4.3.3 Operation:



NOTE

Falsification due to changed base station location

A changed location of the base station falsifies all measurement results obtained so far.

- Do not change the location of the base station until the measurements have been completed.

Preparation

✓ Base station and handset or accessories undamaged.

✓ Handset battery full (see Battery test and battery replacement).

1. Screw the antenna onto the base station.
2. Set up the base station at the planned location of the router node.
3. Align the base station so that the antenna is vertical.
4. Connect the base station to the power supply.
   ↳ The green LED inside the base station flashes.
5. Insert the battery into the mobile station.
6. Switch on the mobile device with the on/off toggle switch.
   ↳ All LEDs light up temporarily.
   ↳ Ready LED lights temporarily.
   ↳ Ready LED flashes.

↳ BAMO ready for operation.

If the error LED lights up permanently, there is a hardware defect.

Measurement

✓ BAMO ready for operation.

1. Go to the locking device whose WaveNet accessibility you want to test. In the process, close all doors between the base station and the locking device to be tested.
2. Set the Sig/Noise toggle switch to the **Sig** position (signal measurement).
3. Hold the handset with its arm extended next to the LockNode locking device.
4. Press the Activate button.
   - ↳ Signal strength is measured and displayed (see table).
   - ↳ Data packet transmission is measured and displayed (see table).
5. Repeat the signal strength measurement twice.
6. Set the Sig/Noise toggle switch to **Noise** (interference signal measurement).
7. Hold the handset with its arm extended next to the LockNode locking device.
8. Press the Activate button.
   - ↳ Interference signal strength is measured and displayed (see table).

Signal strength		Connection can be used (3060)	Connection can be used (SmartIntego)
100%-80%	Optimal	Yes	Yes
70%	Sufficient	Yes	Yes
60%	Sufficient	Yes	No
50%-40%	Sufficient	Yes	No
30%-10%	Too weak	No	No
No display	No connection	No	No

Data packet transmission		Connection can be used (3060)	Connection can be used (SmartIntego)
100%-80%	Good	Yes	Yes
70%-10%	Poor	No	No
No display	No connection	No	No

If one of the connections cannot be used, you have the following options:

- Repeat the measurement.
- Reduce the distance between the base station and the mobile station.

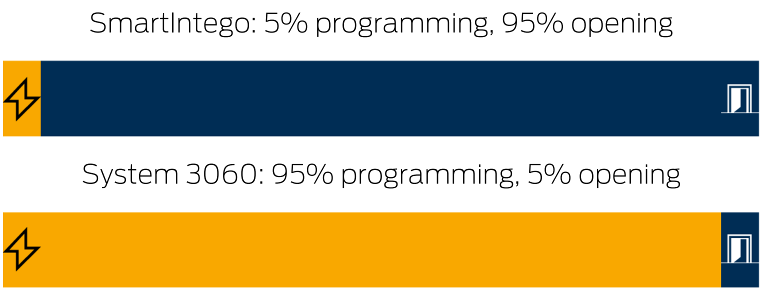
- Set up another RouterNode to improve coverage and also measure from its position.

Interference signal strength		Connection can be used (3060)	Connection can be used (SmartIntego)
No display	No interference signal	Yes	Yes
100%-10%	Interference signal	No	No

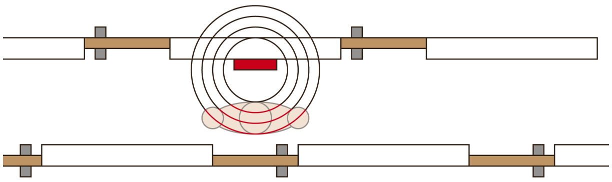
If an interference signal is detected during the interference signal measurement, another device transmits on the same or a similar frequency band. In this case, contact SimonsVoss Technologies GmbH.

Explanation of stricter SmartIntego values

The SmartIntego values are stricter due to how the system works. The use of communication is divided as follows:



When the door is opened, the cardholder often stands between the locking device and the gateway code and dampens the signal additionally:



4.3.4 Identify potential eye-catchers

Keep at least 1.5 m away from the following devices:

- Fluorescent lamps (electronic ballast)
- Illuminated pictograms (escape route signs)
- Air conditioners
- Access points (WLAN)

If you know that additional 868 MHz radio systems are within the reception range of your WaveNet, ask about the frequency used. Inform SimonsVoss Support of this frequency (see *Help and other information [▸ 172]*). Support will then recommend a radio channel which you can set up later in SmartIntego Manager.

Channel	Frequency
1	868.099915 MHz
2	868.0999151999512 MHz

(Channel spacing 199.951172 kHz). The frequencies used by potential interferers and the selected channel should be as far apart as possible. Please contact SimonsVoss Support if you have any questions (see *Help and other information [▸ 172]*).

These systems also typically used 868 MHz (list not exhaustive):

- Radio fire alarm systems
- Radio alarm systems
- Radio microphones
- Garage door controls with radio remote controls

4.4 Ordering components

- Use the SmartIntego ordering tool . This way you avoid wrong quantities and/or order codes. You can get the order tool in the partner area on *https://www.smartintego.com*.
- Please consider the delivery times.
- Make sure that the SmartIntego components you require are compatible with the integrator system. Integrators can integrate different types of SmartIntego components.

4.5 Planning the installation process

Commissioning of your SmartIntego system consists of two steps:

1. Establish infrastructure and
2. Add and programme locking devices.

You can perform these steps in different ways. Choosing the right route for you is influenced by:

- Required processes in the project
- Compatibility of your SmartIntego components with the integrator system
- Integrator system infrastructure

The scenarios described are examples. They serve as templates and can be individually adapted or redesigned.

NOTE

Functional test before installation

Before installing the lock in the door, a function test of the system (Lock, GatewayNode and Integrator System together) is strongly recommended. Without the function test, when installing the lock in the door, there is a risk that you may lock yourself out and no longer be able to open the door. Since the tests are individual for each integrator system, they are not explicitly mentioned in the following procedures.

4.5.1 TCP: Installation according to WaveNet illumination

Use this procedure to commission the system manually according to the results of the illumination (see *Illuminate WaveNet [▸ 12]*). This description applies to the preparation at the installer and installation at the customer's premises.

Preparing the installer

Your locking devices can remain collected in the box.

- ✓ Network cable available to connect each GatewayNode.
- ✓ If possible, all subsequent GatewayNodes are connected to a separate network.
- ✓ Final IP configuration known (obtain from end customer if necessary).
- ✓ SmartIntego components already delivered.
- ✓ Name list for the door known (obtain from end customer if necessary).
- ✓ Integrator system configured.

1. Label the components.
2. Set up the door name list (see *Creating, expanding and importing a name list [▸ 29]*).
3. Create the system documentation (see *Document system [▸ 35]*).
   The system documentation shows what has been installed where.
4. Connect the configuration PC to your GatewayNodes.
5. Configure your GatewayNodes (see *Configuring GatewayNodes (TCP) [▸ 54]*).
6. Create your SmartIntego project (see *Createing a SmartIntego project [▸ 39]*).
7. Set up your card configuration (see *Card configuration setup [▸ 43]*).
8. Set up SmartIntego Manager (see *Setting up SmartIntego Manager [▸ 83]*).

9. Add individual GatewayNodes (see *TCP: Add individual GatewayNodes [▸ 85]*).
10. Manually add several LockNodes (see *Add multiple LockNodes (Manual) [▸ 101]*) and add additional LockNodes manually (see *Add individual LockNodes [▸ 97]*).
11. If necessary, manage your locking devices in the SmartIntego tool (WO) (see *Managing locking devices in the SmartIntego tool (WO) [▸ 119]*).
12. Programme your locking devices (see *Programme hybrid locking devices [▸ 114]*).
13. Repeat steps 6, 7, 10, 11 and 13 for each GatewayNode.
14. After making changes, connect your SmartIntego locking system to the integrator system (see *Connecting SmartIntego to the integrator system [▸ 128]*).
15. Transfer the integrator whitelist to your locking devices.

Always compare your SmartIntego locking system with the integrator system after making changes.

Installation at the customer's site

✓ Completed installer sequence.

1. Set up the infrastructure for your locking system in the property.
2. Mount your GatewayNodes.
3. Hand out the cards (if not done yet).
4. Mount the locking devices in the object.

IMPORTANT

Discharging the batteries

Operation exclusively via the whitelist is only recommended temporarily. The locking devices do not issue battery warnings. You will not be informed about low batteries.

5. Check the WaveNet (see *Check WaveNet [▸ 121]*).
6. If necessary, change the assignment of LockNodes to the GatewayNodes (see *Automatically assign LockNodes [▸ 123]*).
7. After making changes, connect your SmartIntego locking system to the integrator system (see *Connecting SmartIntego to the integrator system [▸ 128]*).
8. Test the system.

4.5.2 TCP: On-site installation (automatic WaveNet configuration)

✓ Integrator system prepared.

✓ Cables and connections available.

✓ Assign IP addresses (TCP only).

✓ Customer informed about the process.

✓ SmartIntego components already delivered.

✓ Names of the doors are fixed.

1. Label the components.
2. Set up the door name list (see *Creating, expanding and importing a name list [▸ 29]*).
3. Create the system documentation (see *Document system [▸ 35]*).
   The system documentation shows what has been installed where.
4. Configure your GatewayNodes (see *Configuring GatewayNodes (TCP) [▸ 54]*).
5. Mount your GatewayNodes.
6. Install the SmartIntego tool (WO) (see *Install SmartIntego tool [▸ 37]*).
7. Create your SmartIntego project (see *Createing a SmartIntego project [▸ 39]*).
8. Set up your card configuration (see *Card configuration setup [▸ 43]*).
9. Mount your locking devices. Alternatively, you can also place your locking devices in front of the doors and install them after programming.

NOTE

Unprotected rooms and relocated locks

The locking devices can be opened with any card in non-programmed state. The rooms are only protected once the locking devices have been programmed.

Locking devices in front of the door can be relocated or escaped by third parties.

■ Inform all persons in the property that the position of the locking devices must not be changed and that no locking devices may be stolen

10. Set up SmartIntego Manager (see *Setting up SmartIntego Manager [▸ 83]*).
11. Add multiple GatewayNodes (IP range) (see *TCP: Add multiple GatewayNodes (IP range) [▸ 87]*).
12. Automatically add several LockNodes (see *Add multiple LockNodes (Automatic) [▸ 106]*) and add additional LockNodes manually if necessary (see *Add individual LockNodes [▸ 97]*).

13. If necessary, manage your locking devices in the SmartIntego tool (WO) (see *Managing locking devices in the SmartIntego tool (WO) [▸ 119]*).
14. Programme your locking devices (see *Programme hybrid locking devices [▸ 114]*).
15. Mount if necessary. Your locking devices that have not yet been installed.
16. After making changes, connect your SmartIntego locking system to the integrator system (see *Connecting SmartIntego to the integrator system [▸ 128]*).
17. Test the system.

Always compare your SmartIntego locking system with the integrator system after making changes.

4.5.3 TCP: On-site installation (manual WaveNet configuration)

- ✓ Integrator system prepared.
- ✓ Cables and connections available.
- ✓ Assign IP addresses (TCP only).
- ✓ Customer informed about the process.
- ✓ SmartIntego components already delivered.
- ✓ Names of the doors are fixed.

1. Label the components.
2. If necessary, set up the name list of the doors (see *Creating, expanding and importing a name list [▸ 29]*).
3. Create the system documentation (see *Document system [▸ 35]*).
   The system documentation shows what has been installed where.
4. Configure your GatewayNodes (see *Configuring GatewayNodes (TCP) [▸ 54]*).
5. Mount your GatewayNodes.
6. Install the SmartIntego tool (WO) (see *Install SmartIntego tool [▸ 37]*).
7. Create your SmartIntego project (see *Createing a SmartIntego project [▸ 39]*).
8. Set up your card configuration (see *Card configuration setup [▸ 43]*).
9. Mount your locking devices. Alternatively, you can also place your locking devices in front of the doors and install them after programming.

NOTE

Unprotected rooms and relocated locks

The locking devices can be opened with any card in non-programmed state. The rooms are only protected once the locking devices have been programmed.

Locking devices in front of the door can be relocated or escaped by third parties.

- Inform all persons in the property that the position of the locking devices must not be changed and that no locking devices may be stolen

10. Set up SmartIntego Manager (see *Setting up SmartIntego Manager [▸ 83]*).
11. Add multiple GatewayNodes (IP range) (see *TCP: Add multiple GatewayNodes (IP range) [▸ 87]*).
12. Add several LockNodes manually (see *Add multiple LockNodes (Manual) [▸ 101]*) and add additional LockNodes manually if necessary (see *Add individual LockNodes [▸ 97]*).
13. If necessary, manage your locking devices in the SmartIntego tool (WO) (see *Managing locking devices in the SmartIntego tool (WO) [▸ 119]*).
14. Programme your locking devices (see *Programme hybrid locking devices [▸ 114]*).
15. Mount if necessary. Your locking devices that have not yet been installed.
16. After making changes, connect your SmartIntego locking system to the integrator system (see *Connecting SmartIntego to the integrator system [▸ 128]*).
17. Test the system.

Always compare your SmartIntego locking system with the integrator system after making changes.

4.5.4 TCP: Prepared installation (construction site whitelist)

Sometimes it is necessary to install the locking devices on a construction site before the necessary infrastructure (power connections, IT equipment or integrator system) is available.

In this case, you can temporarily use your locking devices offline in advance until the network infrastructure is ready for use. To do so, release cards that can be used by construction site workers.

Preparing the installer

Your locking devices can remain collected in the box.

- ✓ Network switch present
  (preferably for all GatewayNodes and with PoE capability). Required for configuring all components in one run (TCP only).
- ✓ Network cable available to connect each GatewayNode.
- ✓ If possible, all subsequent GatewayNodes are connected to a separate network.
- ✓ Final IP configuration known (obtain from end customer if necessary).
- ✓ SmartIntego components already delivered.
- ✓ Name list for the door known (obtain from end customer if necessary).
- ✓ Cards available for the transition phase (MIFARE Classic or MIFARE DESFire).

1. Label the components.
2. Set up the door name list (see *Creating, expanding and importing a name list [▸ 29]*).
3. Create the system documentation (see *Document system [▸ 35]*).
   The system documentation shows what has been installed where.
4. Configure your GatewayNodes (see *Configuring GatewayNodes (TCP) [▸ 54]*).
5. Install the SmartIntego tool (WO) (see *Install SmartIntego tool [▸ 37]*).
6. Create your SmartIntego project (see *Createing a SmartIntego project [▸ 39]*).
7. Set up your card configuration (see *Card configuration setup [▸ 43]*).
8. Set up the construction site whitelist (see *Create, modify and delete construction site whitelist [▸ 41]*).
9. Set up SmartIntego Manager (see *Setting up SmartIntego Manager [▸ 83]*).
10. Add multiple GatewayNodes (IP range) (see *TCP: Add multiple GatewayNodes (IP range) [▸ 87]*).
11. Automatically add several LockNodes (see *Add multiple LockNodes (Automatic) [▸ 106]*) and add additional LockNodes manually if necessary (see *Add individual LockNodes [▸ 97]*).
12. If necessary, manage your locking devices in the SmartIntego tool (WO) (see *Managing locking devices in the SmartIntego tool (WO) [▸ 119]*).
13. Programme your locking devices (see *Programme hybrid locking devices [▸ 114]*).

Installation at the customer's site

1. Mount the locking devices in the object.
2. Hand out the cards (if not done yet).

NOTE

Updating the construction site whitelist

You can update the construction site whitelist with the SI tool and the SI.SmartCD.

IMPORTANT

Discharging the batteries

Operation exclusively via the whitelist is only recommended temporarily. The locking devices do not issue battery warnings. You will not be informed about low batteries.

3. Set up the infrastructure for your locking system in the property.
4. Mount your GatewayNodes.
5. Assign LockNodes to the actual GatewayNodes (see *Automatically assign LockNodes [▸ 123]*).
6. After making changes, connect your SmartIntego locking system to the integrator system (see *Connecting SmartIntego to the integrator system [▸ 128]*).
7. Test the system.
8. Delete the construction site whitelist (see *Delete the construction site whitelist [▸ 43]*).

Always compare your SmartIntego locking system with the integrator system after making changes.

4.5.5 TCP: Prepared installation (Integrator Whitelist)

Sometimes you have to install the locking devices beforehand, as you cannot store them during configuration.

In this case, you can temporarily use your locking devices offline in advance until the network infrastructure is ready for use. For this purpose, the integrator releases cards with its own whitelist which can be used at the locking devices.

Preparing the installer

Your locking devices can remain collected in the box.

- ✓ Network switch present
  (preferably for all GatewayNodes and with PoE capability). Required for configuring all components in one run (TCP only).
- ✓ Network cable available to connect each GatewayNode.
- ✓ If possible, all subsequent GatewayNodes are connected to a separate network.
- ✓ Final IP configuration known (obtain from end customer if necessary).
- ✓ SmartIntego components already delivered.
- ✓ Name list for the door known (obtain from end customer if necessary).
- ✓ Cards available for the transition phase (MIFARE Classic or MIFARE DESFire).
- ✓ Integrator system prepared.

1. Label the components.
2. Set up the door name list (see *Creating, expanding and importing a name list [▸ 29]*).
3. Create the system documentation (see *Document system [▸ 35]*).
   The system documentation shows what has been installed where.
4. Configure your GatewayNodes (see *Configuring GatewayNodes (TCP) [▸ 54]*).
5. Install the SmartIntego tool (WO) (see *Install SmartIntego tool [▸ 37]*).
6. Create your SmartIntego project (see *Createing a SmartIntego project [▸ 39]*).
7. Set up your card configuration (see *Card configuration setup [▸ 43]*).
8. Set up SmartIntego Manager (see *Setting up SmartIntego Manager [▸ 83]*).
9. Add multiple GatewayNodes (IP range) (see *TCP: Add multiple GatewayNodes (IP range) [▸ 87]*).
10. Automatically add several LockNodes (see *Add multiple LockNodes (Automatic) [▸ 106]*) and add additional LockNodes manually if necessary (see *Add individual LockNodes [▸ 97]*).
11. If necessary, manage your locking devices in the SmartIntego tool (WO) (see *Managing locking devices in the SmartIntego tool (WO) [▸ 119]*).
12. Programme your locking devices (see *Programme hybrid locking devices [▸ 114]*).
13. After making changes, connect your SmartIntego locking system to the integrator system (see *Connecting SmartIntego to the integrator system [▸ 128]*).
14. Transfer the Integrator Whitelist to your locking devices.

Installation at the customer's site

1. Set up the infrastructure for your locking system in the property.
2. Mount your GatewayNodes.
3. Mount the locking devices in the object.

IMPORTANT

Discharging the batteries

Operation exclusively via the whitelist is only recommended temporarily. The locking devices do not issue battery warnings. You will not be informed about low batteries.

4. Hand out the cards (if not done yet).
5. Assign LockNodes to the actual GatewayNodes (see *Automatically assign LockNodes [▸ 123]*).
6. After making changes, connect your SmartIntego locking system to the integrator system (see *Connecting SmartIntego to the integrator system [▸ 128]*).
7. Test the system.

Always compare your SmartIntego locking system with the integrator system after making changes.

4.5.6 RS-485: On-site installation (manual WaveNet configuration)

✓ Integrator system prepared.
✓ Cables and connections available.
✓ Customer informed about the process.
✓ SmartIntego components already delivered.
✓ Name list for the door known (obtain from end customer if necessary).

1. Label the components.
2. If necessary, set up the name list of the doors (see *Creating, expanding and importing a name list [▸ 29]*).
3. Create the system documentation (see *Document system [▸ 35]*).
   The system documentation shows what has been installed where.
4. Mount your GatewayNodes.
5. Install the SmartIntego tool (WO) (see *Install SmartIntego tool [▸ 37]*).
6. Set up your RS-485-ConfigNode (see *RS-485 ConfigNode [▸ 78]*).
7. Create your SmartIntego project (see *Createing a SmartIntego project [▸ 39]*).
8. Set up your card configuration (see *Card configuration setup [▸ 43]*).

9. Mount your locking devices. Alternatively, you can also place your locking devices in front of the doors and install them after programming.

NOTE

Unprotected rooms and relocated locks

The locking devices can be opened with any card in non-programmed state. The rooms are only protected once the locking devices have been programmed.

Locking devices in front of the door can be relocated or escaped by third parties.

- Inform all persons in the property that the position of the locking devices must not be changed and that no locking devices may be stolen

10. Set up SmartIntego Manager (see *Setting up SmartIntego Manager [▸ 83]*).
11. Add multiple RS-485 Gateway Nodes (see *RS-485: Add multiple GatewayNodes [▸ 94]*).
12. Manually add several LockNodes (see *Add multiple LockNodes (Manual) [▸ 101]*) and add additional LockNodes manually (see *Add individual LockNodes [▸ 97]*).
13. If necessary, manage your locking devices in the SmartIntego tool (WO) (see *Managing locking devices in the SmartIntego tool (WO) [▸ 119]*).
14. Programme your locking devices (see *Programme hybrid locking devices [▸ 114]*).
15. Mount if necessary. Your locking devices that have not yet been installed.
16. After making changes, connect your SmartIntego locking system to the integrator system (see *Connecting SmartIntego to the integrator system [▸ 128]*).
17. Test the system.

Always compare your SmartIntego locking system with the integrator system after making changes.

4.5.7 RS-485: Prepared installation (construction site whitelist)

Sometimes it is necessary to install the locking devices on a construction site before the necessary infrastructure (power connections, IT equipment or integrator system) is available.

In this case, you can temporarily use your locking devices offline in advance until the network infrastructure is ready for use. To do so, release cards that can be used by construction site workers.

Preparing the installer

Your locking devices can remain collected in the box.

- ✓ Network switch present
  (preferably for all GatewayNodes and with PoE capability). Required for configuring all components in one run (TCP only).
- ✓ Network cable available to connect each GatewayNode.
- ✓ If possible, all subsequent GatewayNodes are connected to a separate network.
- ✓ Final IP configuration known (obtain from end customer if necessary).
- ✓ SmartIntego components already delivered.
- ✓ Name list for the door known (obtain from end customer if necessary).
- ✓ Cards available for the transition phase (MIFARE Classic or MIFARE DESFire).

1. Label the components.
2. If necessary, set up the name list of the doors (see *Creating, expanding and importing a name list [▸ 29]*).
3. Create the system documentation (see *Document system [▸ 35]*).
   The system documentation shows what has been installed where.
4. Connect your GatewayNodes (cable segments as in the project).
5. Install the SmartIntego tool (WO) (see *Install SmartIntego tool [▸ 37]*).
6. Create your SmartIntego project (see *Createing a SmartIntego project [▸ 39]*).
7. Set up your card configuration (see *Card configuration setup [▸ 43]*).
8. Set up the construction site whitelist (see *Create, modify and delete construction site whitelist [▸ 41]*).
9. Set up SmartIntego Manager (see *Setting up SmartIntego Manager [▸ 83]*).
10. Add multiple RS-485 Gateway Nodes (see *RS-485: Add multiple GatewayNodes [▸ 94]*).
11. Manually add several LockNodes (see *Add multiple LockNodes (Manual) [▸ 101]*) and add additional LockNodes manually (see *Add individual LockNodes [▸ 97]*).
12. If necessary, import the door name list into SmartIntego Manager (see *Importing a door name list into SmartIntego Manager [▸ 34]*).
13. If necessary, manage your locking devices in the SmartIntego tool (WO) (see *Managing locking devices in the SmartIntego tool (WO) [▸ 119]*).
14. Programme your locking devices (see *Programme hybrid locking devices [▸ 114]*).
15. Repeat steps 10, 12, 13, 15 and 16 for each cable segment.

Installation at the customer's site

1. Mount the locking devices in the object.
2. Hand out the cards (if not done yet).

IMPORTANT

Discharging the batteries

Operation exclusively via the whitelist is only recommended temporarily. The locking devices do not issue battery warnings. You will not be informed about low batteries.

3. Set up the infrastructure for your locking system in the property.
4. Mount your GatewayNodes.
5. Check the WaveNet (see *Check WaveNet [▸ 121]*).
6. If necessary, relocate several locking devices (see *Relocate locking devices (assign to another GatewayNode) [▸ 143]*).
7. After making changes, connect your SmartIntego locking system to the integrator system (see *Connecting SmartIntego to the integrator system [▸ 128]*).
8. Test the system.
9. Delete the construction site whitelist (see *Delete the construction site whitelist [▸ 43]*).

Always compare your SmartIntego locking system with the integrator system after making changes.

5 Commissioning the SmartIntego project

There are several commissioning variants available (see *Planning the installation process [▸ 16]*) that require specific steps. The following chapters describe the individual steps described in detail.

5.1 Creating, expanding and importing a name list

5.1.1 Create door name list

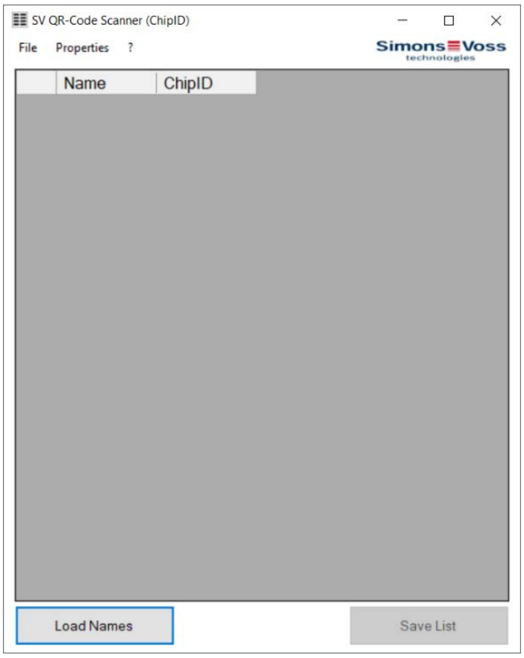
The door name list should be available as a text file (*.txt) in the following format:

```
GatewayNode_01
GatewayNode_02
GatewayNode_03
Cylinder_01
Cylinder_02
Cylinder_03
Cylinder_04
Cylinder_05
Cylinder_06
Cylinder_07
Cylinder_08
Cylinder_09
Cylinder_10
SmartHandle_01
Cylinder_12
```

Use the names of the corresponding doors instead of the terms GatewayNode, Cylinder and SmartHandle. The order of the list entries does not matter.

- ✓ SimonsVoss QR code scanner installed.
- ✓ SmartIntego components already delivered.
- ✓ Physical QR barcode scanner available (Datamatrix code capable, recommendation: Honeywell Voyager 1400g D2).
- ✓ Door name list of the doors and GatewayNodes to be equipped.

1. Open the SimonsVoss QR code scanner (chip ID).



2. Connect the QR barcode scanner.

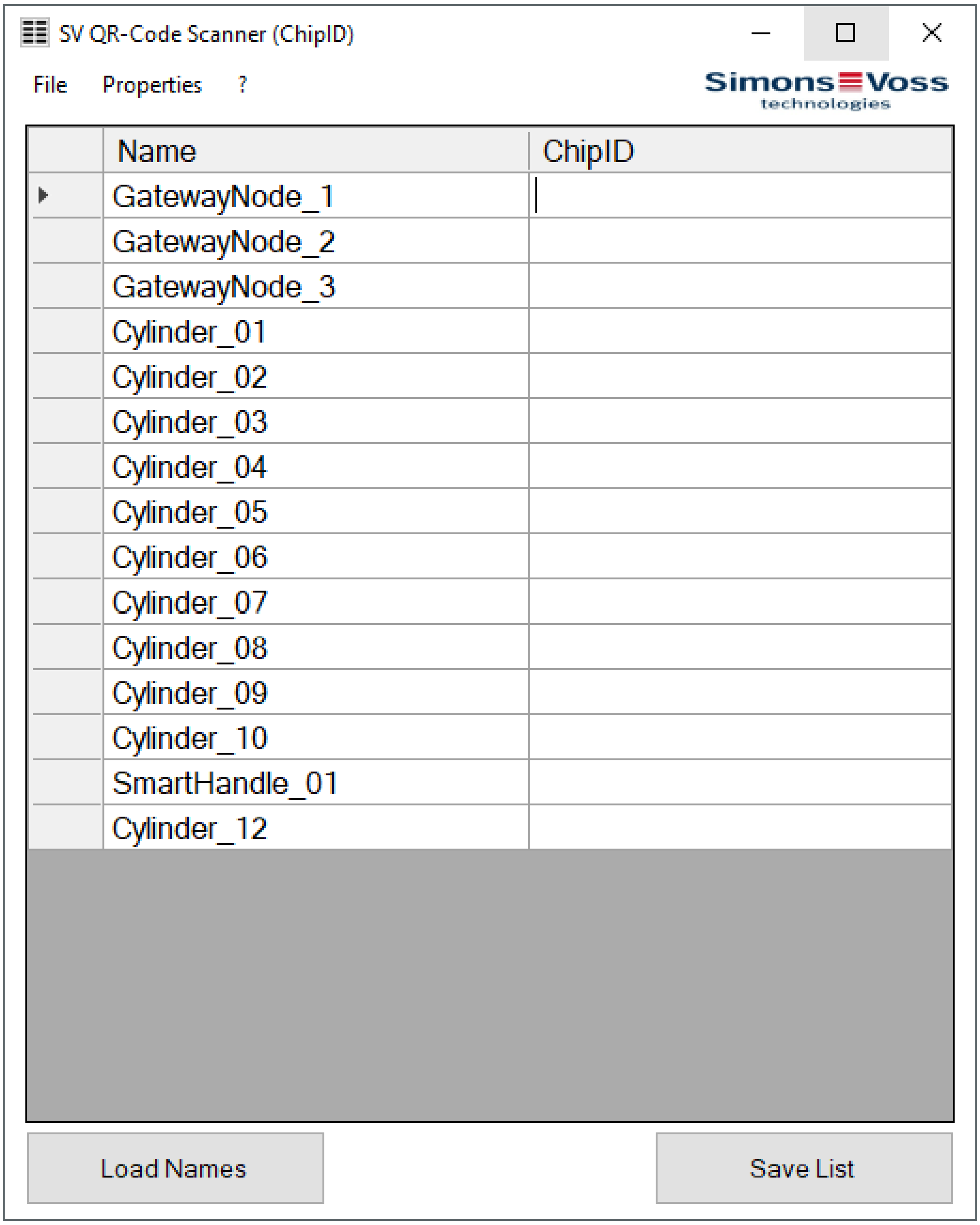
NOTE

QR barcode scanner settings

The SimonsVoss QR barcode scanner processes keyboard entries in a German keyboard layout (QWERTZ).

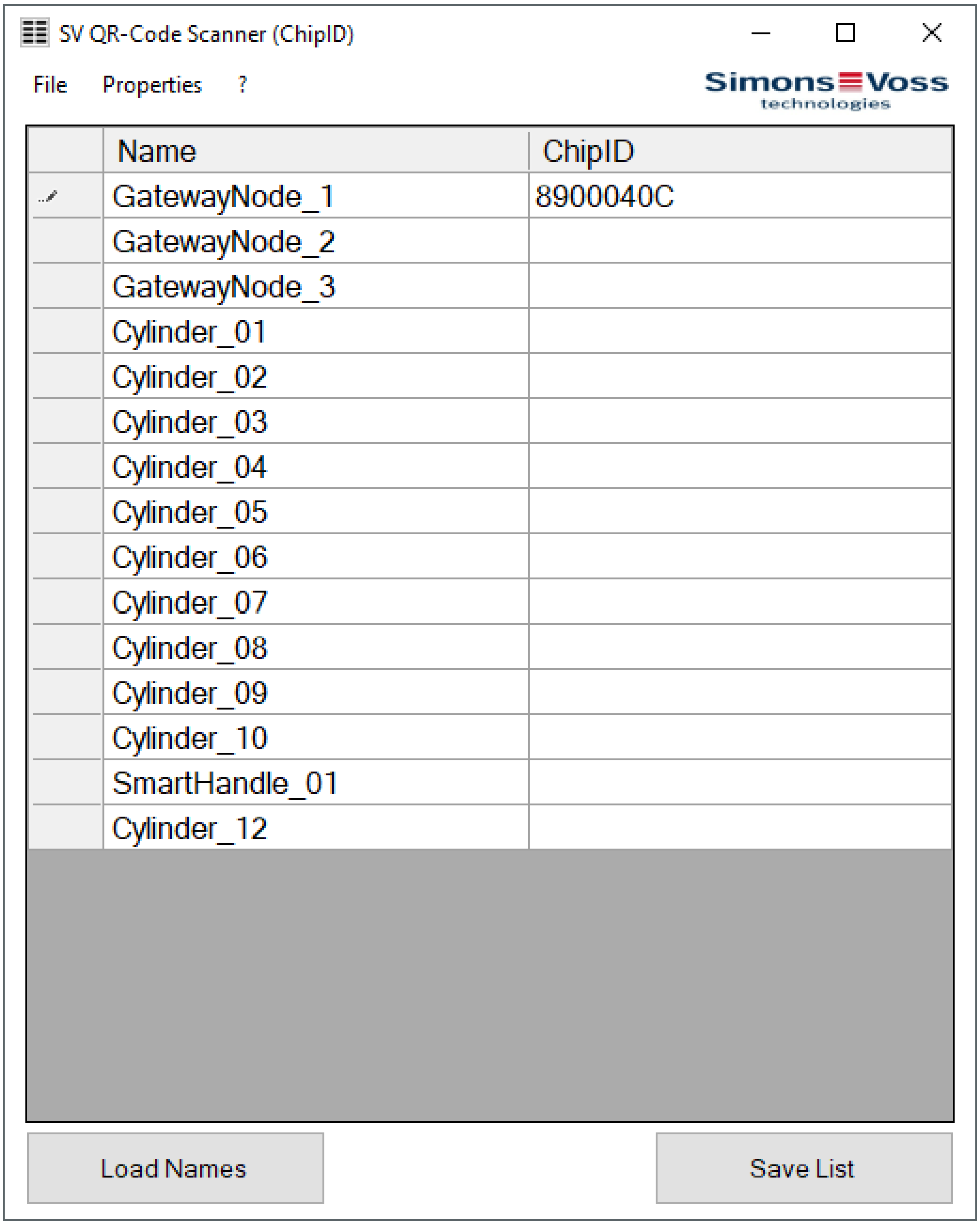
1. Set the QR barcode scanner as a keyboard (normally default setting).
2. Set the QR barcode scanner to the German keyboard layout (QWERTZ) (*Properties - Configuration*).

3. Click on the Load Names button.
   - ↳ The Explorer opens.
4. Navigate to your door name list.
5. Click on the button OK .
   - ↳ The Explorer closes.
   - ↳ Reading in door name list.



Name	ChipID
GatewayNode_1	
GatewayNode_2	
GatewayNode_3	
Cylinder_01	
Cylinder_02	
Cylinder_03	
Cylinder_04	
Cylinder_05	
Cylinder_06	
Cylinder_07	
Cylinder_08	
Cylinder_09	
Cylinder_10	
SmartHandle_01	
Cylinder_12	

6. Highlight the line or place the cursor in the chip ID cell.
7. Scan the code on the appropriate packaging.
   ↳ Entire code is read in.
8. Go to the next line.
   ↳ Previously scanned code is filtered down to chip ID.



Name	ChipID
GatewayNode_1	8900040C
GatewayNode_2	
GatewayNode_3	
Cylinder_01	
Cylinder_02	
Cylinder_03	
Cylinder_04	
Cylinder_05	
Cylinder_06	
Cylinder_07	
Cylinder_08	
Cylinder_09	
Cylinder_10	
SmartHandle_01	
Cylinder_12	

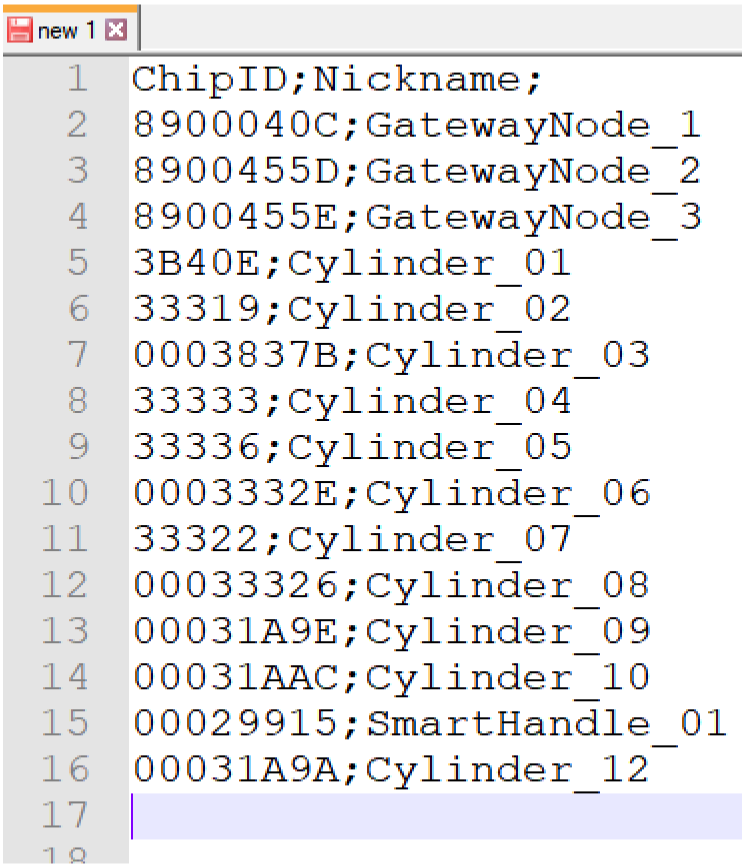
9. Scan further locking devices and GatewayNodes.
10. Click on the Save List button.
    ↳ The Explorer opens.
11. Navigate to an output directory of your choice.
12. Click on the button OK .
    ↳ The Explorer closes.

↳ The door name list with the chip IDs is saved (required later by SmartIntego Manager, see) *Importing a door name list into SmartIntego Manager [▸ 34]*.

5.1.2 Expand door name list

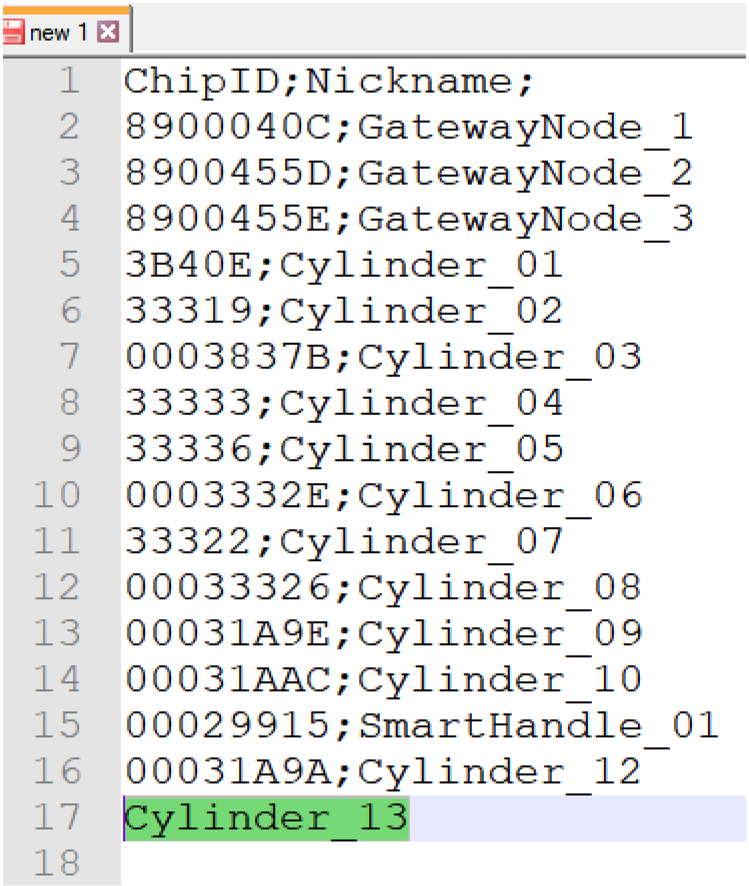
If you continue your SmartIntego project, you can expand the door name list.

1. Open the existing door name list with the chip IDs with a text editor.



```
ChipID;Nickname;
8900040C;GatewayNode_1
8900455D;GatewayNode_2
8900455E;GatewayNode_3
3B40E;Cylinder_01
33319;Cylinder_02
0003837B;Cylinder_03
33333;Cylinder_04
33336;Cylinder_05
0003332E;Cylinder_06
33322;Cylinder_07
00033326;Cylinder_08
00031A9E;Cylinder_09
00031AAC;Cylinder_10
00029915;SmartHandle_01
00031A9A;Cylinder_12
```

2. Add further entries.



```
ChipID;Nickname;
8900040C;GatewayNode_1
8900455D;GatewayNode_2
8900455E;GatewayNode_3
3B40E;Cylinder_01
33319;Cylinder_02
0003837B;Cylinder_03
33333;Cylinder_04
33336;Cylinder_05
0003332E;Cylinder_06
33322;Cylinder_07
00033326;Cylinder_08
00031A9E;Cylinder_09
00031AAC;Cylinder_10
00029915;SmartHandle_01
00031A9A;Cylinder_12
Cylinder_13

```

3. Save the door name list again as a text file (*.txt).
   ↳ Door name list supplemented with new components.
4. Import the door name list back into the SimonsVoss QR code scanner.
5. Scan the codes on the packaging of the newly added components.
6. Save the door name list.

↳ Door name list supplemented with new components and chip IDs.

5.1.3 Importing a door name list into SmartIntego Manager

You have created the door name list with the chip IDs with one of the three options:

- SimonsVoss QR code scanner (see *Create door name list [▸ 29]*)
- Integrator system
- Manual

Now import the door name list into SmartIntego Manager:

1. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.
2. Select the option ◉ Read list of nicknames.

3. Click on the button OK.
   - ↳ Window "Administration" closes.
   - ↳ The Explorer opens.
4. Navigate to your door name list with chip IDs.
5. Click on the button OK.
   - ↳ The Explorer closes.

↳ Door name list opened in SmartIntego Manager.

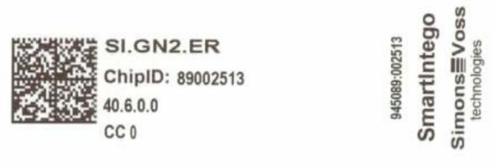
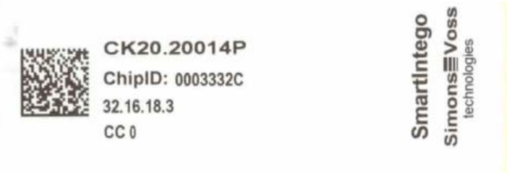
Components not yet created in SmartIntego Manager	Components already created in SmartIntego Manager
SmartIntego Manager uses the list as a basis when ◉ Update topology you add new SmartIntego components (see *Add GatewayNode [▸ 84]* and *Add multiple LockNodes (Automatic) [▸ 106]*).	SmartIntego Manager updates the names of SmartIntego components using the chip ID.

The list remains loaded in the background until you Exit exit SmartIntego Manager with the button.

5.2 Document system

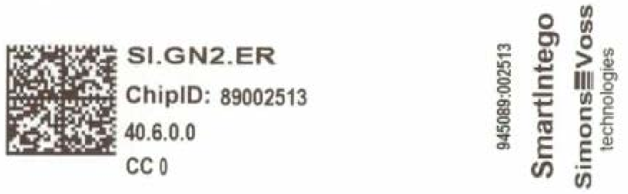
Operating a digital locking system without system documentation is not practical. System documentation (whether on paper or digitally) greatly facilitates subsequent maintenance and modification work.

The system documentation must contain the following information:

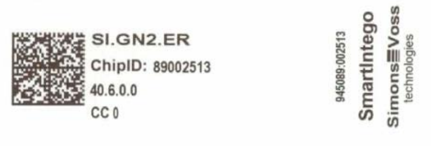
Component information	Installation information
Source: Data matrix code on the packaging or the supplied sticker	Source: Environment or infrastructure
GatewayNode:  SI.GN2.ER ChipID: 89002513 40.6.0.0 CC 0 945089-002513 SmartIntego SimonsVoss technologies Locking device:  CK20.20014P ChipID: 0003332C 32.16.18.3 CC 0 SmartIntego SimonsVoss technologies	

Component information	Installation information
■ Order code ■ Chip ID ■ PHI (Physical Hardware Identifier = serial number, only for locking devices) ■ Firmware version on delivery (LockNodes and, if necessary, locking devices) ■ MAC address (SI.GN.ER and SI.GN2.ER only) Optional but helpful: Deviations from the order code (e.g. subsequently modified cover for SmartHandles)	■ Locking devices: Door names (e.g. Office *Sam Sample*) ■ GatewayNode: DNS name or IP address and installation location (building plan)

The finished documentation can look like this:

GatewayNode Name/IP	GatewayNode Information
GatewayNode 1	 SI.GN2.ER ChipID: 89002513 40.6.0.0 CC 0 945089:002513 SmartIntego SimonsVoss technologies
GatewayNode 2	SI.GN2.ER ChipID: 89002513 40.6.0.0 CC 0 945089:002513 SmartIntego SimonsVoss technologies

Door name	GatewayNode nearby	Locking plan information
Door 1	GatewayNode 1	SI.GN2.ER ChipID: 89002513 40.6.0.0 CC 0 945089:002513 SmartIntego SimonsVoss technologies
Door 2	GatewayNode 2	SI.GN2.ER ChipID: 89002513 40.6.0.0 CC 0 945089:002513 SmartIntego SimonsVoss technologies

Door name	GatewayNode nearby	Locking plan information
Door 3	GatewayNode 3	 SI.GN2.ER ChipID: 89002513 40.6.0.0 CC 0 945089:002513 SmartIntego SimonsVoss technologies
...		

NOTE

Update deviating configuration according to topology (optimised)

If you ● Update topology use the function ☑ SI-Manager Update topology: Optimised [offen] with the checkbox, SmartIntego Manager links the LockNodes in the locking devices with the GatewayNodes that are most easily accessible.

The real configuration may then differ.

- In this case, use the exported WO configuration file (ConfigData.csv) from the SmartIntego tool.

5.3 Install SmartIntego tool

Install the SmartIntego tool (WO) on a PC or laptop with USB connection.

✓ Administrator rights available.

1. Run `the SmartIntego_setup_X_X_WO.exe` file.
2. Follow the instructions.
   ↳ Install SmartIntego tool (WO).
   ↳ SmartIntego Manager installed.
   ↳ Driver for SI.SmartCD installed.
3. After installation, connect the SI.SmartCD programming device.
4. Open any existing project file.

The card configuration for the locking devices must be fully loaded. When programming the first locking device, connect the programming device (SI.SmartCD) to a USB port on the PC. The locking device itself is programmed via WaveNet.

You can also use the SmartIntego tool (WO) later without a local programming device (e.g. on a virtual server).

NOTE

Descriptions in this document

The descriptions in this document refer to SmartIntego tool (WO) version 3.0 or higher.

- Use the latest version of the SmartIntego tool (WO).

5.4 Update SmartIntego tool (WO)

Uninstalling the old version is not necessary. Create a backup (see *Create backup [▸ 170]*) and update older versions of the SmartIntego tool (WHO):

✓ Administrator rights available.

1. Run `the SmartIntego_setup_X_X_WO.exe` file.
2. Follow the instructions.
   ↳ Install SmartIntego tool (WO).
   ↳ SmartIntego Manager installed.
   ↳ Driver for SI.SmartCD installed.
3. After installation, connect the SI.SmartCD programming device.
4. Open any existing project file.

5.4.1 Changes to SI-Tool 3.0

- Support for the SI.SmartHandle AX
- Changes to the interface for card configuration (see *Card configuration setup [▸ 43]*)
- Change to the coupling time for the locking devices (whitelist, see *Set coupling duration [▸ 53]*)
- Internal improvements
- Bug fixes

NOTE

CSV export for integrator systems after update

After an update from version 2.1 to version 3.0, the SmartIntego Manager must be started once before you export CSV files.

Change to the card configuration

The update changes DESFire card configuration in existing projects:

- Increase the maximum file size to 8192 bytes
- Changing the file type to standard

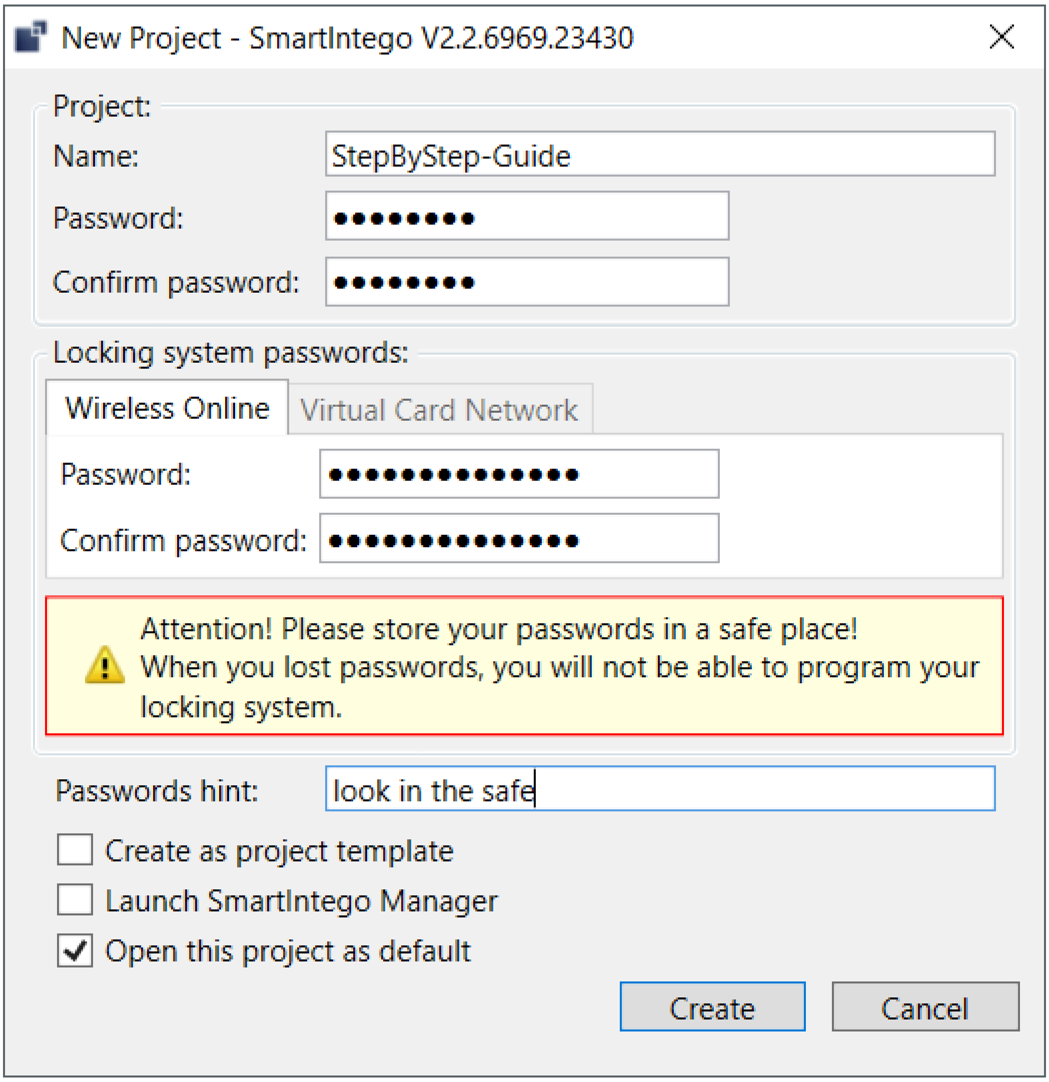
Each locking device can thus read files with up to 8192 bytes. This change creates a unique non-critical programming requirement for all locking devices. Perform programming either immediately after the update or later (see *Programme locking device [▸ 112]*).

5.4.2 Changes to SI-Tool 3.1

- Support for the SI Digital Cylinder AX

5.5 Createing a SmartIntego project

1. Open the SmartIntego tool (WO).
2. Via | File | select the entry New.
   ↳ The view for creating a new project opens.



New Project - SmartIntego V2.2.6969.23430

Project:

Name: StepByStep-Guide

Password: ●●●●●●●●

Confirm password: ●●●●●●●●

Locking system passwords:

Password: ●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●

Attention! Please store your passwords in a safe place! When you lost passwords, you will not be able to program your locking system.

Passwords hint: look in the safe

□ Create as project template

□ Launch SmartIntego Manager

☑ Open this project as default

3. Enter a project name.
4. Assign a login password (project password).
5. Change to the "[SI-Tool - Projekt erstellen: Wireless online [offen]]" tab.

6. Assign a locking system password.

NOTE

Loss of passwords

Your passwords are the basis for managing your locking system. Lost or publicly known passwords are a serious security risk and/or lead to loss of control over the system.

1. Make a note of your passwords.
2. Store your passwords in a safe place.

7. Provide a password hint.
8. Click on the Create button.
   ↳ The Explorer opens.
9. Select an output folder for your project file.
10. Click on the button Save.
    ↳ The Explorer closes.

↳ The project is created (*.ikp).

NOTE

Multiple project files for an integration project

Using a separate project file for each hardware controller of the integrator system significantly increases the administrative effort for the installer.

1. SimonsVoss advises against this type of administration.
2. If necessary, ensure that the integrator system supports the use of multiple project files.

Loss of the project file (*.ikp)

If the project file is lost despite a backed up environment and backup, you will no longer be able to continue working with the existing project.

1. Reset the locking devices with the locking system password.
2. If necessary, reset the LockNodes with a hardware reset.
3. If necessary, reset the GatewayNodes with a hardware reset.
4. Then reprogram the entire locking system.

5.6 Create, modify and delete construction site whitelist

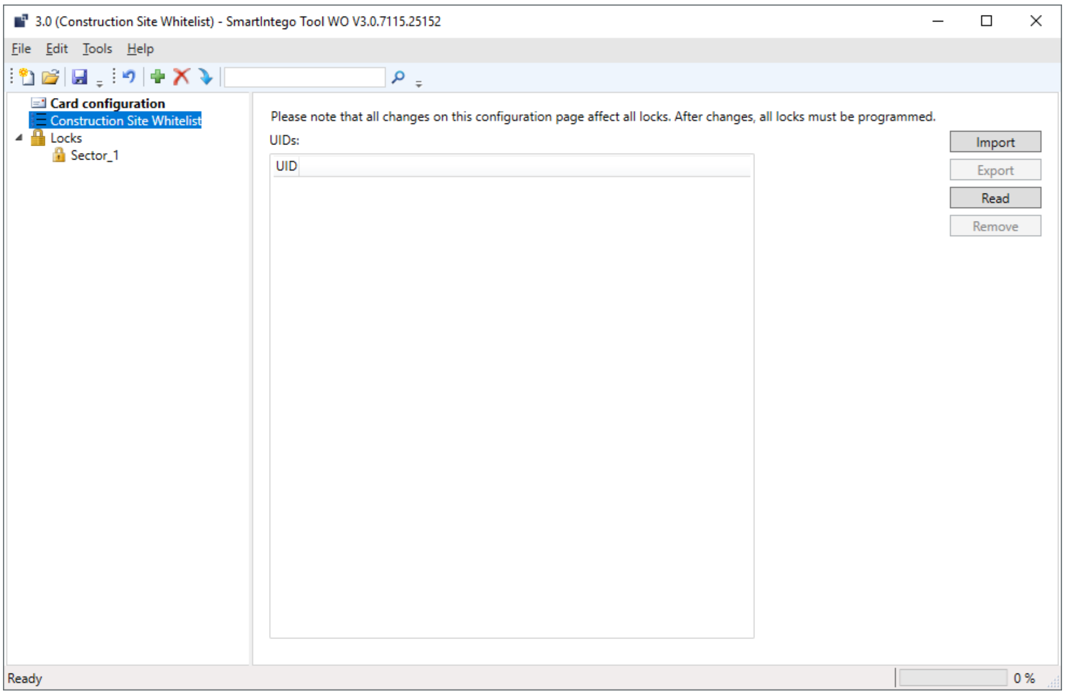
5.6.1 Create construction site whitelist

Reading individual cards

✓ SmartIntego-Tool (WO) opened.

✓ Programming device (SI.SmartCD) connected.

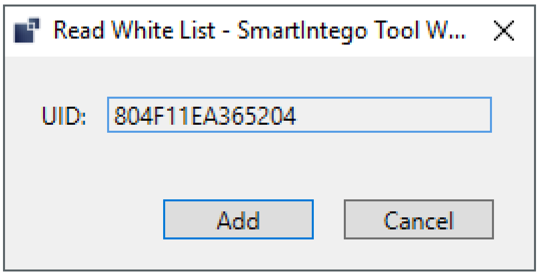
1. In the navigation bar, select the entry | Construction Site Whitelist |.
   ↳ Administration of the construction site whitelist opens.



3.0 (Construction Site Whitelist) - SmartIntego Tool WO V3.0.7115.25152

Please note that all changes on this configuration page affect all locks. After changes, all locks must be programmed.

2. Place the card on the programming device (SI.SmartCD).
3. Click on the Read button.
   ↳ The window "Read White List" opens.

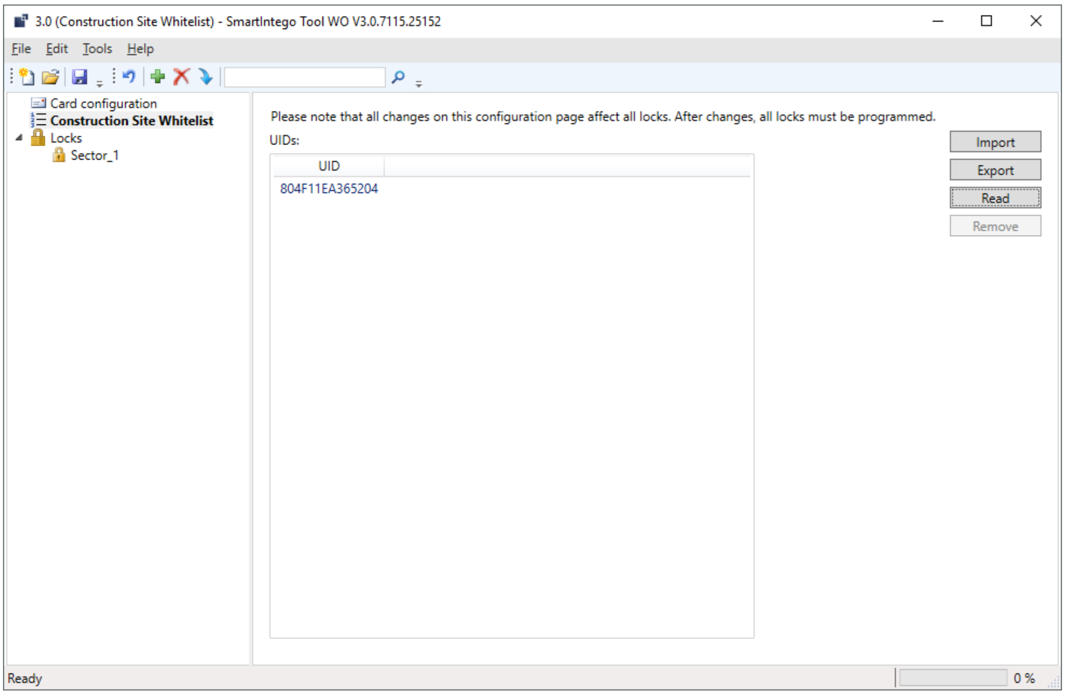


Read White List - SmartIntego Tool W...

UID: 804F11EA365204

4. Click on the Add button.

↳ Card read is added to construction site whitelist.



3.0 (Construction Site Whitelist) - SmartIntego Tool WO V3.0.7115.25152

Please note that all changes on this configuration page affect all locks. After changes, all locks must be programmed.

UIDs:

UID
804F11EA365204

Import entire list

Alternatively, you can import a list with the UIDs of the cards. The file must have the extension *.uid and look like this (first line UID, the following lines the UIDs of the cards):

```
UID
BD70855B
804F11EA2A3704
804F11EA2A3204
804F11EA2A5C04
```

1. Click on the Import button.
   ↳ The Explorer opens.
2. Navigate to your UID file.
3. Click on the button OK.
   ↳ The Explorer closes.

↳ List with cards is added to construction site whitelist.

NOTE

Incompatibility of cards

When reading in the cards, no check for ISO 14443-A or ISO 14443-B is performed.

- Check that the boards are compatible with the settings in Card Configuration.

5.6.2 Change the construction site whitelist

Individual cards can be added and deleted using the buttons Read and Remove.

If you import a list, all previous entries are deleted and the UIDs of the imported list are used.

5.6.3 Delete the construction site whitelist

✓ SmartIntego-Tool (WO) opened.

1. Highlight the construction site whitelists to be deleted in the navigation pane (multiple selection: Ctrl+mouse click or Shift+mouse click).
2. Click on the Remove button.
3. Programme all locking devices (see *Programme locking device [▸ 112]*).

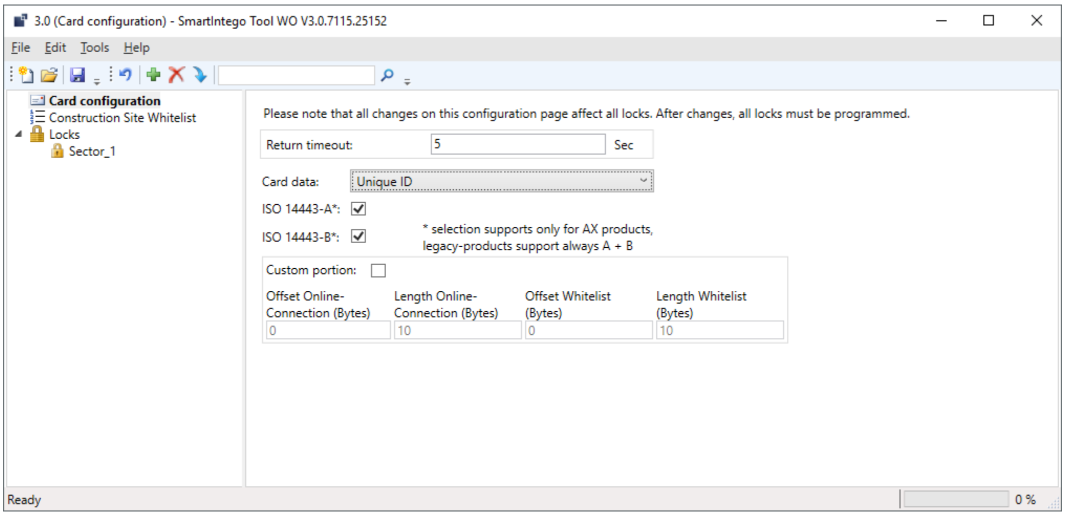
↳ Construction site whitelist is deleted.

5.7 Card configuration setup

✓ SmartIntego-Tool (WO) opened.

1. On the navigation bar, select the entry Card Configuration.
2. Set the return timeout value for all locking devices (default value: 5 seconds; note the integrator's specifications when changing the value).

   ↳ Return timeout value set


3.0 (Card configuration) - SmartIntego Tool WO V3.0.7115.25152
File
Edit
Tools
Help
Card configuration
Construction Site Whitelist
Locks
Sector_1
Ready
0 %

Please note that all changes on this configuration page affect all locks. After changes, all locks must be programmed.

Return timeout: 5 Sec

Card data: Unique ID

ISO 14443-A*: ☑

ISO 14443-B*: ☑

* selection supports only for AX products, legacy-products support always A + B

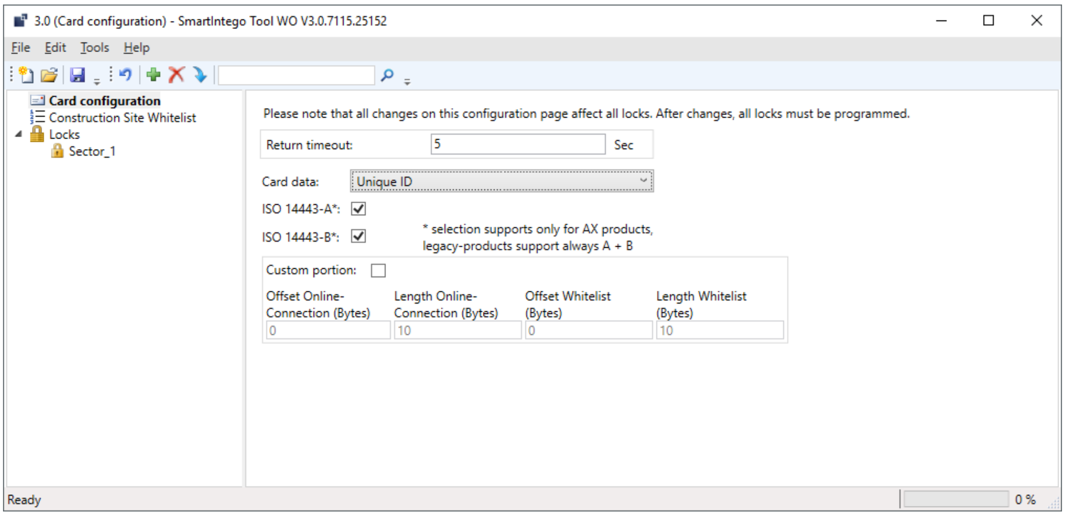
Custom portion: ☐

Offset Online-Connection (Bytes)	Length Online-Connection (Bytes)	Offset Whitelist (Bytes)	Length Whitelist (Bytes)
0	10	0	10

5.7.1 Unique ID mode

✓ Card Configuration selected.

1. From the drop-down menu ▼ **Card data**, select the entry "SI-Tool: Card data - Unique ID [offen]".


3.0 (Card configuration) - SmartIntego Tool WO V3.0.7115.25152
File
Edit
Tools
Help
Card configuration
Construction Site Whitelist
Locks
Sector_1
Ready
0 %

Please note that all changes on this configuration page affect all locks. After changes, all locks must be programmed.

Return timeout: 5 Sec

Card data: Unique ID

ISO 14443-A*: ☑

ISO 14443-B*: ☑

* selection supports only for AX products, legacy-products support always A + B

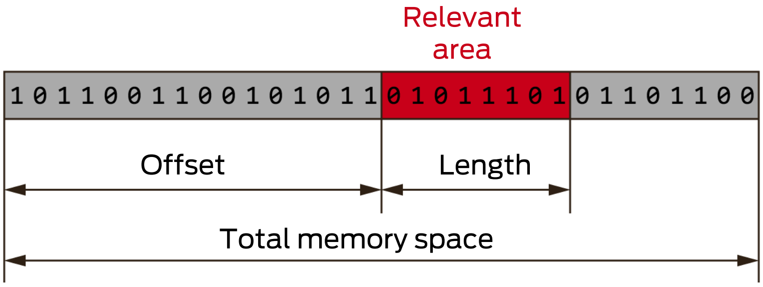
Custom portion: □

Offset Online-Connection (Bytes)	Length Online-Connection (Bytes)	Offset Whitelist (Bytes)	Length Whitelist (Bytes)
0	10	0	10

2. If necessary: In the area, "SI-Tool: Kartenkonfiguration - Custom portion [offen]" specify which data of the UID should be used (see table). These settings are specified by the integrator (see also *Entering card data [▸ 48]*).
3. Assign a password (see *Protecting card configuration [▸ 49]*).
   ↳ Unintentional changes excluded.

In the area, "SI-Tool: Kartenkonfiguration - Custom portion [offen]" you specify which contiguous bytes of the identification number should be read out from the locking device. Normally, the entire identification number is evaluated; restrictions are specified by the card manufacturer or the integrator.

SI-Tool: Kartenkonfiguration - Offset Online Connection (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Length Online Connection (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Offset Whitelist (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Length Whitelist (Bytes) [offen]
■ Specifies from which byte the identification number is read. ■ Use for online access	■ Specifies how many bytes of the identification number are read. ■ Use for online access	■ Specifies from which byte the identification number is read. ■ Use for whitelist access	■ Specifies how many bytes of the identification number are read. ■ Use for whitelist access

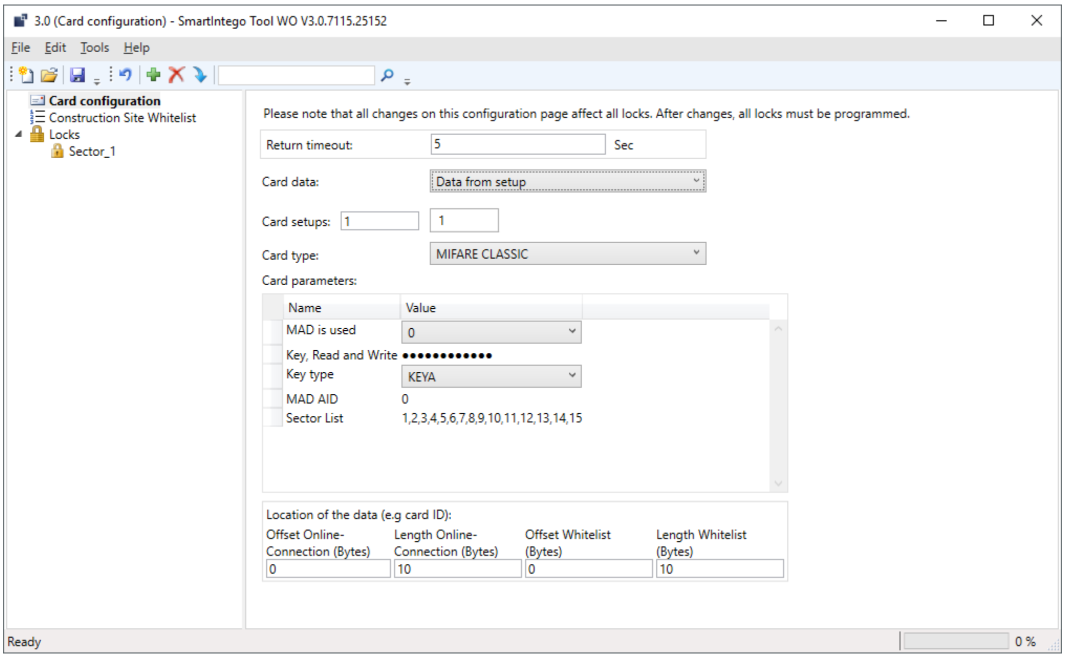


The exact parameters can be found in the documentation of your integrator system.

5.7.2 Card data usage mode: MIFARE Classic

- ✓ SmartIntego-Tool (WO) opened.
- ✓ Card Configuration selected.

1. From the drop-down menu ▼ **Card data**, select"SI-Tool: Card data - Data from Setup [offen]".
2. Specify the number of card configurations (*card setups*) used in the system (up to 5).
3. In the dropdown menu ▼ **Card type** select the entry "SI-Tool: Card type - MIFARE Classic [offen]".


3.0 (Card configuration) - SmartIntego Tool WO V3.0.7115.25152
File
Edit
Tools
Help
Card configuration
Construction Site Whitelist
Locks
Sector_1

Please note that all changes on this configuration page affect all locks. After changes, all locks must be programmed.

Return timeout: 5 Sec

Card data: Data from setup

Card setups: 1 1

Card type: MIFARE CLASSIC

Card parameters:

Name	Value
MAD is used	0
Key, Read and Write	••••••••••••
Key type	KEYA
MAD AID	0
Sector List	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

Location of the data (e.g card ID):

Offset Online-Connection (Bytes)	Length Online-Connection (Bytes)	Offset Whitelist (Bytes)	Length Whitelist (Bytes)
0	10	0	10

Ready 0 %

4. Enter the card parameters in the area "SI-Tool: Kartenkonfiguration - Card parameters [offen]" in order to be able to read the card data. These settings are specified by the integrator (see also*Entering card data [▸ 48]*).

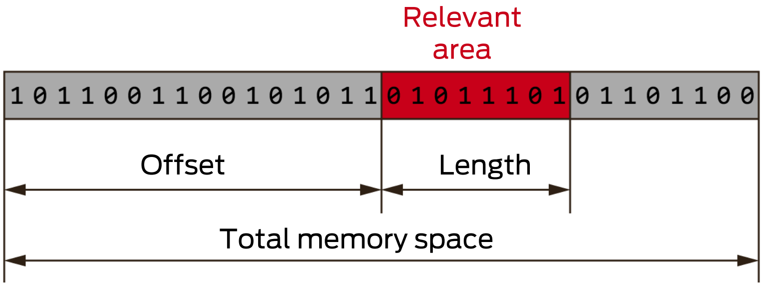
5. In the section, "SI-Tool: Kartenmanagement - LOcation if the data (e.g. card ID) [offen]" specify where the data is located on the card (see table). These settings are specified by the integrator.
6. Repeat steps 3, 4 and 5 for all cards with other MIFARE Classic data records.
7. Assign a password (see *Protecting card configuration [▸ 49]*).
   ↳ Unintentional changes excluded.

Data to be entered:

- MAD or sector based
- Readkey to read the data (read and write keys are sometimes the same)
- Selection of key (A or B)
- MAD AID: If "MAD is used" = 1
- Sector List: If "MAD is used" = 0 (sector in which the ID of the card is located)

The locking device should not read out the entire data record of the card. It only requires a number (max. 32 bytes) that uniquely identifies the card. In the area "SI-Tool: Kartenmanagement - LOcation if the data (e.g. card ID) [offen]" you specify which related data should be read out from the locking device.

SI-Tool: Kartenkonfiguration - Offset Online Connection (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Length Online Connection (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Offset Whitelist (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Length Whitelist (Bytes) [offen]
Specifies from which byte the data is read. Use for online access	Specifies how many bytes of the data are read. Use for online access	Specifies from which byte the data is read. Use for whitelist access	Specifies how many bytes of the data are read. Use for whitelist access

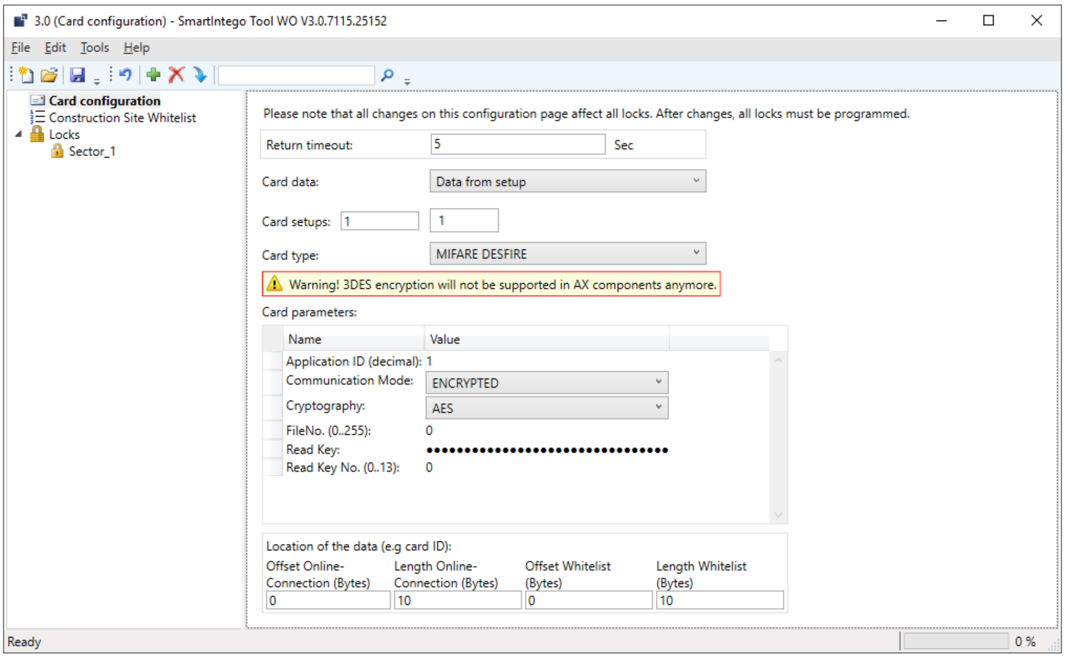


The exact parameters can be found in the documentation of your integrator system.

5.7.3 Card data usage mode: MIFARE DESFire

✓ Card Configuration selected.

1. From the drop-down menu ▼ **Card data**, select"SI-Tool: Card data - Data from Setup [offen]".
2. Specify the number of card configurations (*card setups*) used in the system (up to 5).
3. In the dropdown menu ▼ **Card type** select the entry "SI-Tool: Card type - MIFARE DESFire [offen]".


3.0 (Card configuration) - SmartIntego Tool WO V3.0.7115.25152
File
Edit
Tools
Help
Card configuration
Construction Site Whitelist
Locks
Sector_1
Ready
0 %

Please note that all changes on this configuration page affect all locks. After changes, all locks must be programmed.

Return timeout: 5 Sec

Card data: Data from setup

Card setups: 1 1

Card type: MIFARE DESFIRE

⚠ Warning! 3DES encryption will not be supported in AX components anymore.

Card parameters:

Name	Value
Application ID (decimal):	1
Communication Mode:	ENCRYPTED
Cryptography:	AES
FileNo. (0..255):	0
Read Key:	••••••••••••••••••••••••••••••••
Read Key No. (0..13):	0

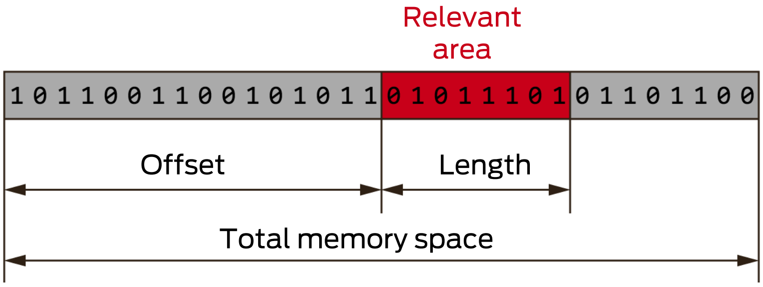
Location of the data (e.g card ID):

Offset Online-Connection (Bytes)	Length Online-Connection (Bytes)	Offset Whitelist (Bytes)	Length Whitelist (Bytes)
0	10	0	10

4. Enter the card parameters in the area "SI-Tool: Kartenkonfiguration - Card parameters [offen]" to access the card in a read-only manner (these settings are specified by the integrator (see also *Entering card data [▸ 48]*)).
5. In the section, "SI-Tool: Kartenmanagement - LOcation if the data (e.g. card ID) [offen]" specify where the data is located on the card (see table). These settings are specified by the integrator.
6. Repeat steps 3, 4 and 5 for all cards with other MIFARE Classic card records.
7. Assign a password (see *Protecting card configuration [▸ 49]*).
   ↳ Unintentional changes excluded.

The locking device should not read out the entire data record of the card. It only requires a number (max. 32 bytes) that uniquely identifies the card. In the area "SI-Tool: Kartenmanagement - LOcation if the data (e.g. card ID) [offen]" you specify which related data should be read out from the locking device.

SI-Tool: Kartenkonfiguration - Offset Online Connection (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Length Online Connection (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Offset Whitelist (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Length Whitelist (Bytes) [offen]
- Specifies from which byte the data is read. - Use for online access	- Specifies how many bytes of the data are read. - Use for online access	- Specifies from which byte the data is read. - Use for whitelist access	- Specifies how many bytes of the data are read. - Use for whitelist access



The exact parameters can be found in the documentation of your integrator system.

5.7.4 Entering card data

Access to the card data is generally provided by the integrator or the cardholder. Your SmartIntego locking devices only need a small part of the data on the card to identify them (settings in ▼ Card data -"SI-Tool: Card data - Data from Setup [offen]").

The data (in particular the application ID) is always entered in decimal notation in the SmartIntego
tool: 0 1 2 3 4 5 6 7 8 9

Other manufacturers often use a hexadecimal notation:
0 1 2 3 4 5 6 7 8 9 A B C D E F

You must convert the data from hexadecimal to decimal to be able to enter the data in the SmartIntego tool.

The special feature of this hexadecimal notation is that it can be read in both directions. The reading direction is specified in the card configuration. The result of the conversion to decimal notation depends on the reading direction. There are two read types:

- MSByte first (Most Significant Byte first): Highest byte first, corresponds to reading direction from left to right
- LSByte first (Least Significant Byte first): Lowest byte first, corresponds to reading direction from right to left

Example

Example								
Hex	A4BC							
Hex split	MSByte first				LSByte first			
	A	4	B	C	B	C	A	4
	10*4096	4*256	11*16	12*1	11*4096	12*256	10*16	4*1
Decimal split	40960	1024	176	12	45056	3072	160	4
Decimal	42172				48292			

5.7.5 Protecting card configuration

Protect your card configuration with a password to prevent unintentional changes.

NOTE

Loss of passwords

Your passwords are the basis for managing your locking system. Lost or publicly known passwords are a serious security risk and/or lead to loss of control over the system.

1. Make a note of your passwords.
2. Store your passwords in a safe place.

1. Via | Tools | call up the entry Options and Project.
2. In the area "SI-Tools: Tools Options Project - Passwords [offen]", switch to tab [SI-Tools: Tools Options Project Passwords - Card configuration [offen]].
3. Enter the desired passwords.

↳ Card configuration saved.

5.8 Creating and loading a template for card configurations

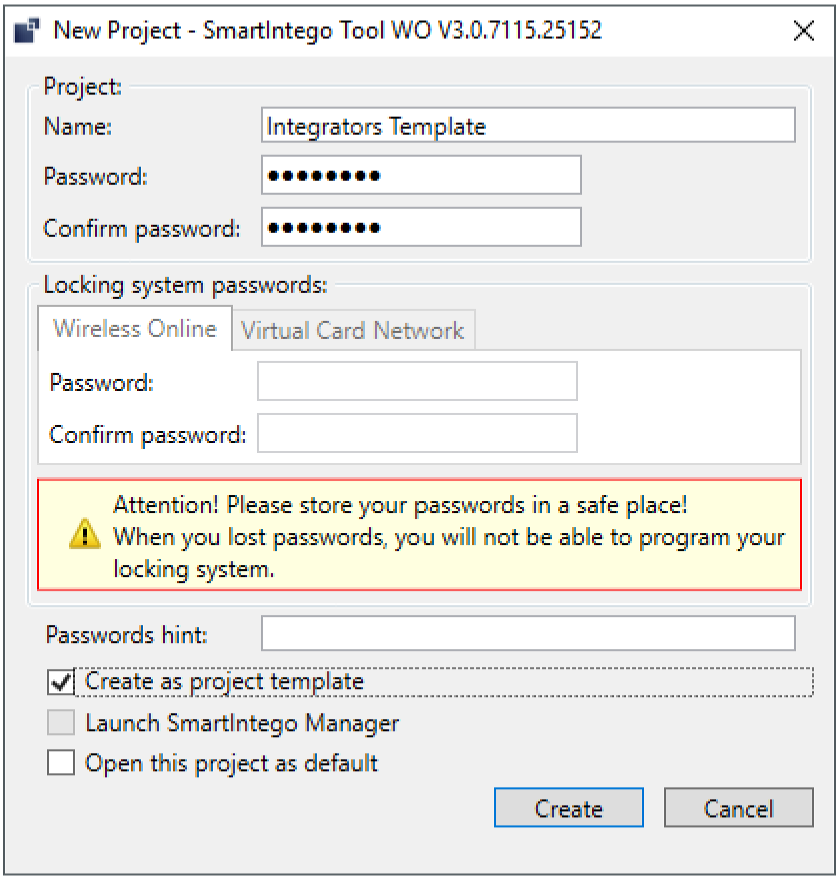
Integrators who have a global access key for their card data cannot disclose it.

However, these integrators can make it easier for installers to commission the project by creating a template file using the SmartIntego tool. This template file only contains the card configuration.

The installer can then load this template file on a project-specific basis. The card data in it can be processed, but cannot be viewed.

5.8.1 Create template (integrator)

1. Open the SmartIntego tool.
2. Via | File | select the entry New.
3. Give the template a name.
4. Assign a project password to the template.
5. Activate the checkbox ☑ SI-Tool: Create as project template [offen].



New Project - SmartIntego Tool WO V3.0.7115.25152

Project:

Name: Integrators Template

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

Locking system passwords:

Wireless Online | Virtual Card Network

Password:

Confirm password:

Attention! Please store your passwords in a safe place!
When you lost passwords, you will not be able to program your locking system.

Passwords hint:

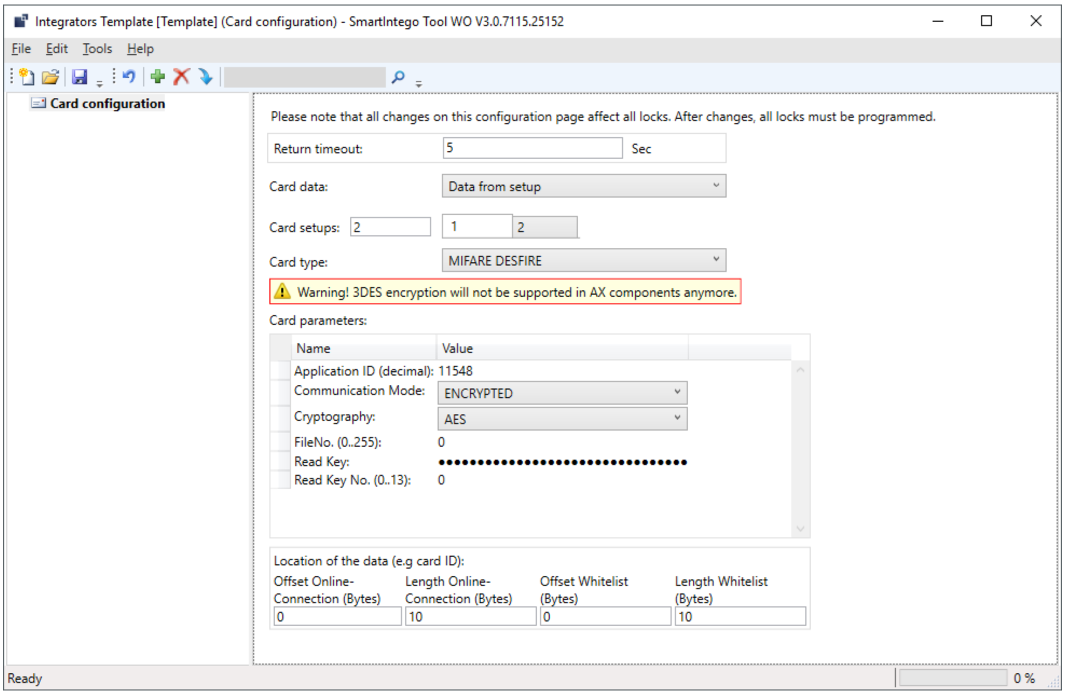
☑ Create as project template

☐ Launch SmartIntego Manager

☐ Open this project as default

6. Click on the Create button.

7. Set the card configuration(s) (see *Card configuration setup [▸ 43]*).



Integrators Template [Template] (Card configuration) - SmartIntego Tool WO V3.0.7115.25152

Please note that all changes on this configuration page affect all locks. After changes, all locks must be programmed.

Return timeout: 5 Sec

Card data: Data from setup

Card setups: 2 | 1 | 2

Card type: MIFARE DESFIRE

⚠ Warning! 3DES encryption will not be supported in AX components anymore.

Card parameters:

Name	Value
Application ID (decimal):	11548
Communication Mode:	ENCRYPTED
Cryptography:	AES
FileNo. (0..255):	0
Read Key:	••••••••••••••••••••••••••••••••
Read Key No. (0..13):	0

Location of the data (e.g card ID):

Offset Online-Connection (Bytes)	Length Online-Connection (Bytes)	Offset Whitelist (Bytes)	Length Whitelist (Bytes)
0	10	0	10

Ready 0 %

8. Secure the card configuration with a password to prevent accidental changes (see *Protecting card configuration [▸ 49]*).

NOTE

Loss of passwords

Your passwords are the basis for managing your locking system. Lost or publicly known passwords are a serious security risk and/or lead to loss of control over the system.

1. Make a note of your passwords.
2. Store your passwords in a safe place.

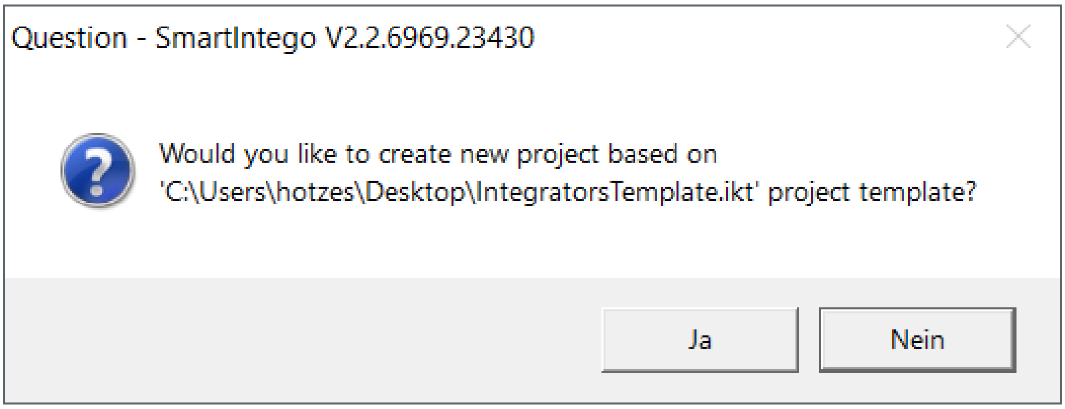
9. Save the template file as a * .ikt file.

↳ Template file is created. The card data is encrypted in the * .ikt file and cannot be viewed.

5.8.2 Load template (installer)

1. Open the SmartIntego tool.
2. Via | File | select the entry Open.
   ↳ The Explorer opens.
3. Navigate to your template file (*.ikt).
4. Click on the button OK.
   ↳ The Explorer closes.

5. Log in with the integrator's password.
   ↳ Programming window opens.



Question - SmartIntego V2.2.6969.23430

Would you like to create new project based on 'C:\Users\hotzes\Desktop\IntegratorsTemplate.ikt' project template?

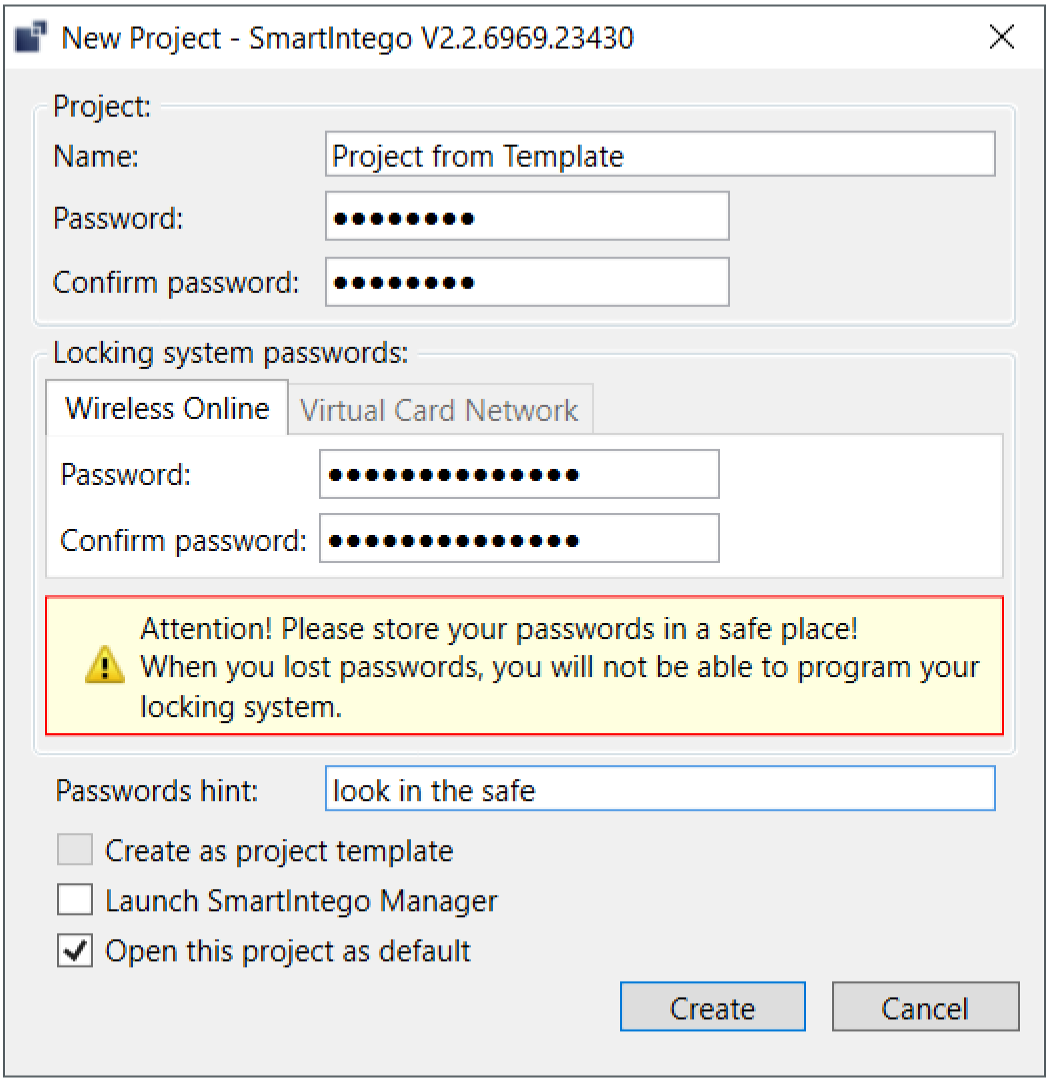
6. Confirm the query with Yes.
   ↳ The prompt closes.
7. Enter a project name.
8. Assign a login password (project password).
9. Assign a locking system password.

NOTE

Loss of passwords

Your passwords are the basis for managing your locking system. Lost or publicly known passwords are a serious security risk and/or lead to loss of control over the system.

1. Make a note of your passwords.
2. Store your passwords in a safe place.



New Project - SmartIntego V2.2.6969.23430

Project:

Name: Project from Template

Password: ••••••••

Confirm password: ••••••••

Locking system passwords:

Password: ••••••••••••••

Confirm password: ••••••••••••••

Attention! Please store your passwords in a safe place!
When you lost passwords, you will not be able to program your locking system.

Passwords hint: look in the safe

□ Create as project template

□ Launch SmartIntego Manager

☑ Open this project as default

10. Click on the Create button.
11. | File | Use the entry to select Save.
12. Save the project file (*.ikp) in an output folder of your choice.

↳ Project created based on template.

5.9 Set coupling duration

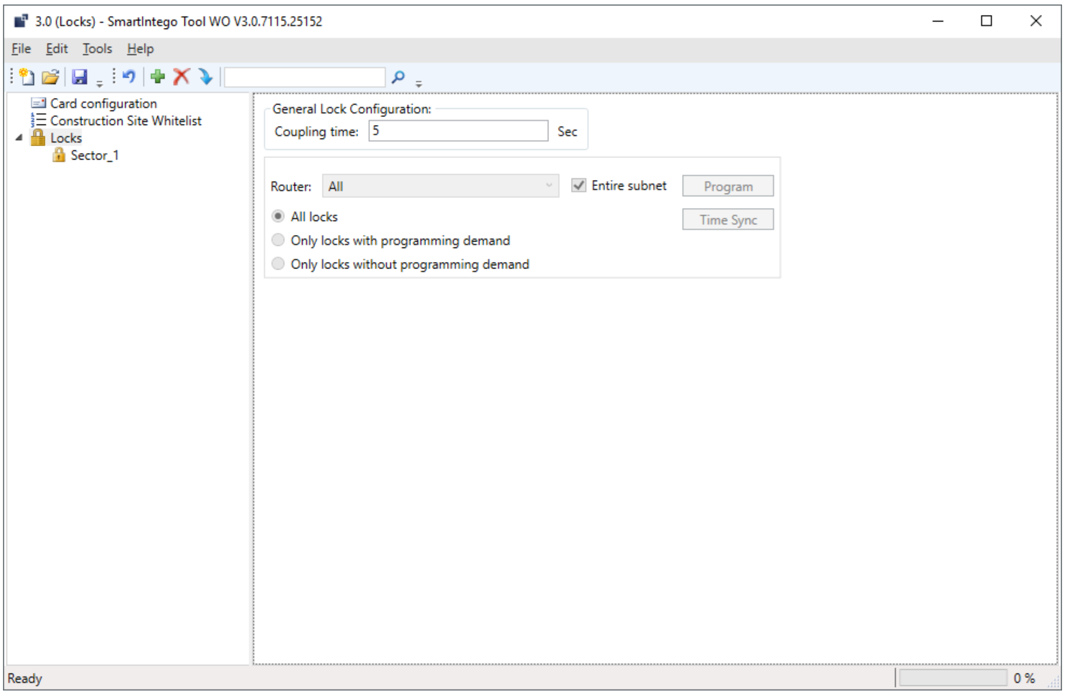
In the case of an online opening (short-term activation), the integrator system generally determines the duration of engagement.

If the integrator system does not determine the duration or the locking device uses the whitelist to open, the locking device itself decides the duration of the engagement.

You can determine this duration yourself from version 3.0 of the SmartIntego tool (WO) (previously always five seconds).

✓ SmartIntego-Tool (WO) opened.

1. In the navigation area, select the entry SI-Tool Navigationsbereich: Locks [offen].



3.0 (Locks) - SmartIntego Tool WO V3.0.7115.25152

General Lock Configuration:

Coupling time: 5 Sec

Router: All ☑ Entire subnet

● All locks

○ Only locks with programming demand

○ Only locks without programming demand

Ready 0 %

2. Specify for SI-Tool Navigationsbereich: Locks - Coupling time [offen] a value between 2 and 25 seconds.
3. Programme your locking devices (see *Programme hybrid locking devices [▸ 114]*).

↳ Locking device internal coupling duration set.

5.10 Configuring GatewayNodes (TCP)

5.10.1 Search GatewayNode

On delivery, the GatewayNodes expect a DHCP server in the network to assign them an IP address. If there is no DHCP server on the network, GatewayNodes assign default credentials.

You receive the device with the following factory configuration:

IP address	192.168.100.100 (if no DHCP server is found)
Subnet mask	255.255.0.0
User name	SimonsVoss
Password	SimonsVoss

The configuration PC and the GatewayNode must be on the same network, otherwise the configuration PC cannot access the GatewayNode.

You can access the GatewayNode via the web interface. To do this, enter `https://192.168.100.100` (or the IP address of your GatewayNode) in a browser of your choice. If you do not know the IP address, you can determine the IP address with the OAM tool.

NOTE

Unauthorised access with standard access data

The standard access data can be viewed freely. Unauthorised persons cannot change the access authorisations, but they can change the network configuration. You will then no longer be able to reach the device via the network and will have to reset it.

Some browsers do not transmit spaces at the beginning of the password.

1. Change the default password.
2. Do not start or end the password with spaces.

5.10.2 OAM tool

The OAM tool can:

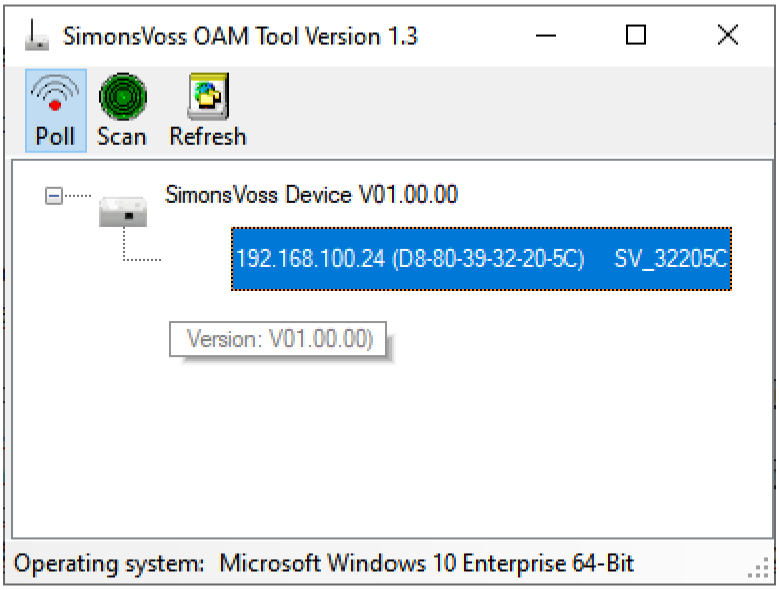
- change the IP settings of a GatewayNode
- open the configuration website of a GatewayNode
- open HTTPS configuration website of a GatewayNode (required for AES encryption settings)
- update firmware of a GN2

The following chapters describe the procedure in more detail. Some of them are written for RouterNode 2 (System 3060). The procedure for GatewayNode 2 is the same.

To ensure secure operation in the IT infrastructure, it is necessary that some settings are made directly via the configuration website of the GatewayNodes (see Configuration TCP GatewayNodes).

5.10.2.1 Determining and setting the IP address

With the Operation, Administration and Maintenance Tool (OAM tool) you can both read and set the IP address. The OAM tool is available free of charge in the download area of the SimonsVoss website (*https://www.simons-voss.com*). You do not need to install the OAM tool.


SimonsVoss OAM Tool Version 1.3

SimonsVoss Device V01.00.00

192.168.100.24 (D8-80-39-32-20-5C) SV_32205C

Version: V01.00.00)

Operating system: Microsoft Windows 10 Enterprise 64-Bit

IMPORTANT

Unauthorised changing of the IP address

The OAM tool is freely accessible. The OAM tool can be misused by unauthorized persons to change the IP address of your RouterNodes, GatewayNodes or SmartBridges.

- Block changing the IP address in the OAM Tool via the browser interface (see *Browser interface [▸ 60]*).

NOTE

Unauthorised access with standard access data

The standard access data can be viewed freely. Unauthorised persons cannot change the access authorisations, but they can change the network configuration. You will then no longer be able to reach the device via the network and will have to reset it.

Some browsers do not transmit spaces at the beginning of the password.

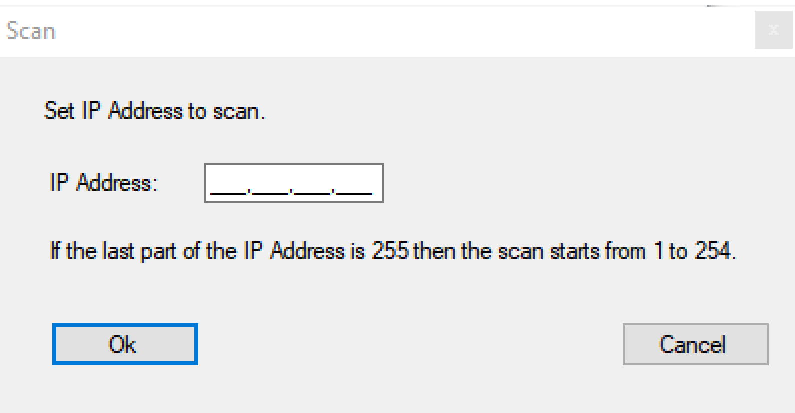
1. Change the default password.
2. Do not start or end the password with spaces.

Determining the IP

The procedure is described for RouterNodes. Follow the same procedure for SmartIntego GatewayNodes and MobileKey SmartBridges.

- ✓ OAM tool available and unpacked.
- ✓ RouterNode connected to the network.
- ✓ Subnet known.

1. Double-click on the executable file to start the OAM tool.
   ↳ OAM Tool opens.
2. Click on the button Scan.
   ↳ The window "Scan" opens.



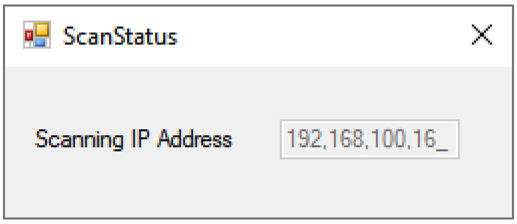
Scan

Set IP Address to scan.

IP Address: ___.___.___.___

If the last part of the IP Address is 255 then the scan starts from 1 to 254.

3. Enter a known IP address of a device in the WaveNet network (other or new devices are also found. If you do not know an IP address, use the following IP address: 192.168.100.255 - may differ depending on the subnet).
4. Click on the OK button.
   ↳ The "Scan" window closes.
   ↳ The OAM tool scans the address range.



ScanStatus

Scanning IP Address 192.168.100.16_

↳ The OAM tool displays found devices in the list.

You can choose: DHCP server or static IP. You can also make the settings described below in the browser interface (see *Browser interface [▸ 60]*).

The procedure is described for RouterNodes. Follow the same procedure for SmartIntego GatewayNodes and MobileKey SmartBridges.

Setting IP for DHCP operation (default)

If you use a DHCP server, the IP address is determined by a DHCP server.

- ✓ OAM tool available and unpacked.
- ✓ RouterNode connected to the network.

1. Double-click on the executable file to start the OAM tool.
   - ↳ The OAM tool opens.
2. Click on the button Refresh.
   - ↳ IP address of the RouterNode updated.
3. Open the context menu by right-clicking on the entry of the IP address of the RouterNode.

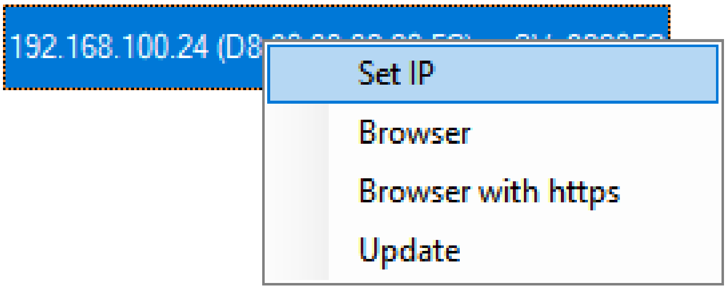
NOTE

Compare MAC

If you select the wrong RouterNode, you could assign the same IP address multiple times.

- Compare the MAC address of the entry with the label on your RouterNode.

4. Click on the entry Set IP.



   - ↳ The window "Network configuration" opens.
5. Make sure that the checkbox ☑ Enable DHCP is activated.
6. If no address reservation on the DHCP server is provided for this RouterNode, make a note of the *host name* (e.g. SV_32205C). You will need it later during configuration in the WaveNet Manager (see Add RouterNode to WaveNet).
7. Click on the OK button.
   - ↳ The window "Network configuration" closes.
   - ↳ RouterNode will restart.
8. Close the information window about the restart.
9. Close the OAM tool.

↳ DHCP operation is set.

Set IP for operation with static IP address

If you are not using a DHCP server, the IP address is the factory default. In this case you must change the IP address, otherwise several router nodes will have the same IP (namely the factory IP) and will not be able to communicate.

✓ OAM tool available and unpacked.

✓ RouterNode connected to the network.

1. Double-click on the executable file to start the OAM tool.
   ↳ The OAM tool opens.
2. Click on the button Refresh.
   ↳ IP address of the RouterNode updated.
3. Open the context menu by right-clicking on the entry of the IP address of the RouterNode.

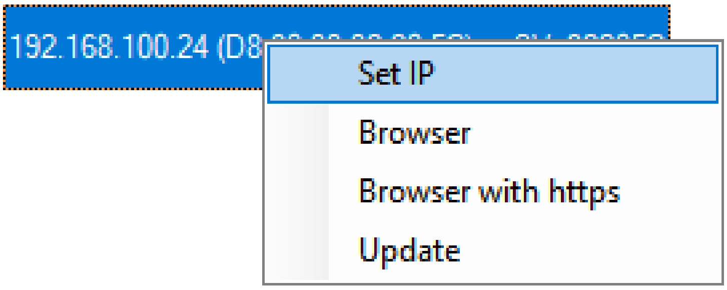
NOTE

Compare MAC

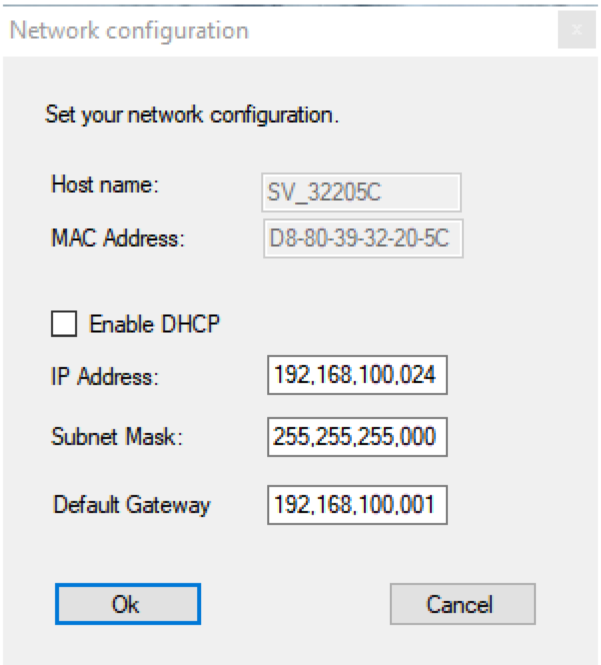
If you select the wrong RouterNode, you could assign the same IP address multiple times.

- Compare the MAC address of the entry with the label on your RouterNode.

4. Click on the entry Set IP.



   ↳ The window "Network configuration" opens.



Network configuration

Set your network configuration.

Host name: SV_32205C

MAC Address: D8-80-39-32-20-5C

□ Enable DHCP

IP Address: 192.168.100.024

Subnet Mask: 255.255.255.000

Default Gateway 192.168.100.001

5. Deactivate the checkbox □ Enable DHCP.
6. Enter a new IP address, if necessary.
7. Click on the OK button.
   - ↳ The "Network configuration" window closes.
   - ↳ RouterNode will restart.
8. Close the information window about the restart.
9. Close the OAM tool.

↳ IP address is set.

5.10.2.2 Browser interface

You can use the Ethernet interface in the browser to configure the following for RouterNodes, GatewayNodes and SmartBridges:

- Allow changes using the OAM tool
- Password for the web interface
- IP address/DHCP mode
- Opening and closing the SMTP port

Launching

You receive the device with the following factory configuration:

IP address	192.168.100.100 (if no DHCP server is found)
Subnet mask	255.255.0.0
User name	SimonsVoss
Password	SimonsVoss

The procedure is described for RouterNodes. Use the same procedure for SmartIntego GatewayNodes and MobileKey SmartBridges.

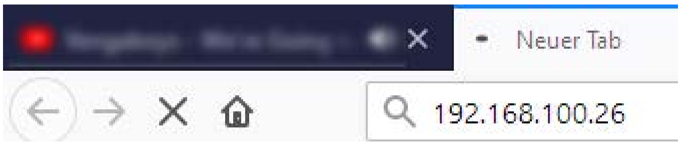
Change the default password after you launch for the first time.

✓ RouterNode IP known (see *Determining and setting the IP address [▸ 55]*).

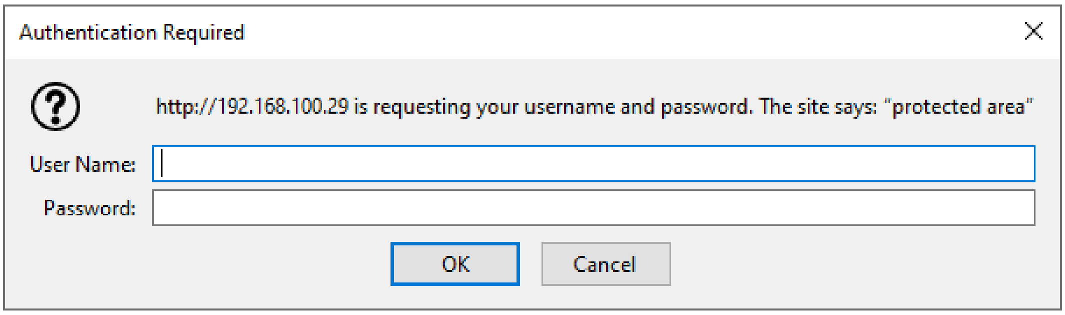
✓ Browser open.

✓ User credentials known for the browser interface (name and password).

1. Enter the IP address in your browser's address field.



2. Press the Enter key to confirm.
   ↳ The "Authentication required" window will open.


Authentication Required

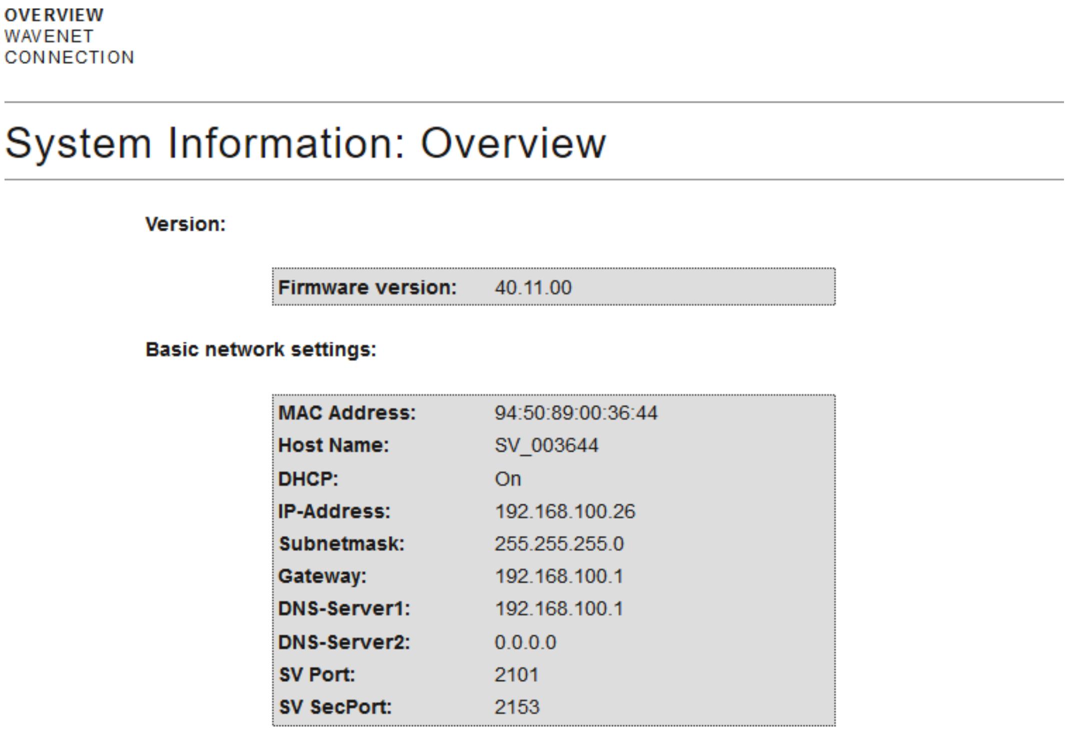
http://192.168.100.29 is requesting your username and password. The site says: "protected area"

User Name:

Password:

3. Enter the login credentials.
4. Click on the OK button.

↳ The browser interface system overview is visible.



System Information: Overview

Version:

Firmware version:	40.11.00

Basic network settings:

MAC Address:	94:50:89:00:36:44
Host Name:	SV_003644
DHCP:	On
IP-Address:	192.168.100.26
Subnetmask:	255.255.255.0
Gateway:	192.168.100.1
DNS-Server1:	192.168.100.1
DNS-Server2:	0.0.0.0
SV Port:	2101
SV SecPort:	2153

NOTE

Web interface can no longer be used with the default password with firmware 40.12 and above

The browser interface remains blocked in firmware version 40.12 or above until the default password has been changed.

- Change the default password.

↳ Browser interface is unblocked and settings can be changed.

NOTE

Unauthorised access with standard access data

The standard access data can be viewed freely. Unauthorised persons cannot change the access authorisations, but they can change the network configuration. You will then no longer be able to reach the device via the network and will have to reset it.

Some browsers do not transmit spaces at the beginning of the password.

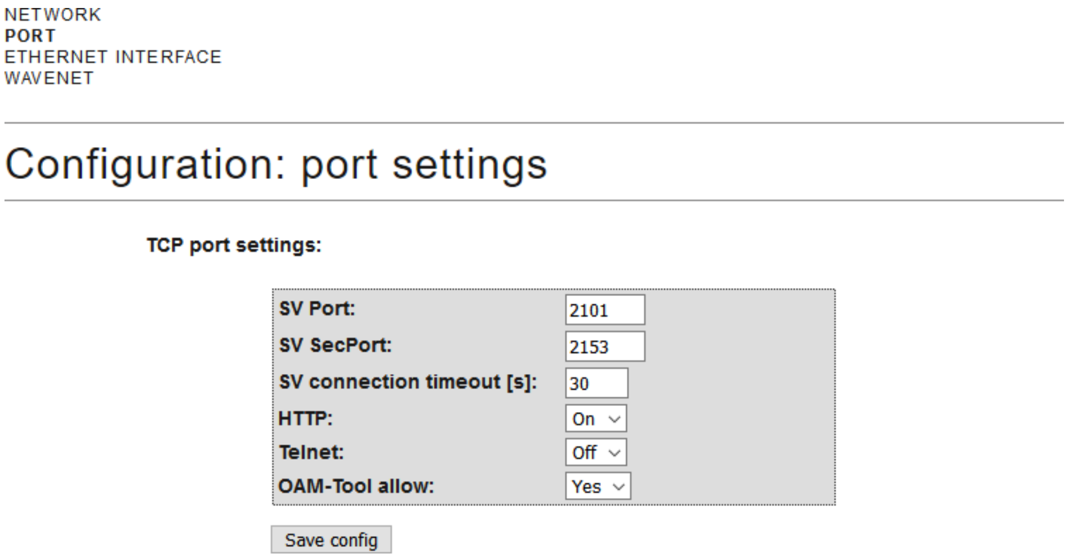
1. Change the default password.
2. Do not start or end the password with spaces.

Blocking/enable change to the IP address using the OAM tool

If you do not enable the ▼ OAM-Tool allow, you will not be able to use the OAM tool to perform updates.

✓ Browser interface opened.

1. Open the [PORT] tab using | CONFIGURATION |.
   ↳ You will see an overview of the TCP port settings for RouterNode 2.



Configuration: port settings

TCP port settings:

SV Port:	2101
SV SecPort:	2153
SV connection timeout [s]:	30
HTTP:	On
Telnet:	Off
OAM-Tool allow:	Yes

2. Select the option "Yes" (enable the OAM tool to change the IP) or the option "No" (block change to the IP by the OAM tool) from the ▼ OAM-Tool allow drop-down menu.
3. Click on the button Save.

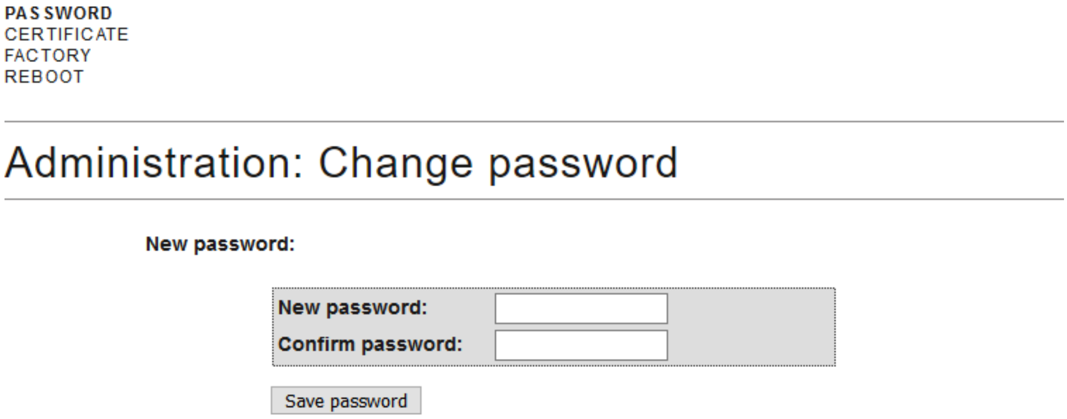
↳ Changing the IP address using the OAM tool is locked/allowed.

Change password

Some browsers do not register any spaces included at the start of a password, so do not begin your password with spaces.

✓ Browser interface opened.

1. Open the [PASSWORD] tab using | ADMINISTRATION |.



Administration: Change password

New password:

New password:	
Confirm password:	

2. Enter your new password.
3. Repeat your new password.

4. Click on the Save password button.

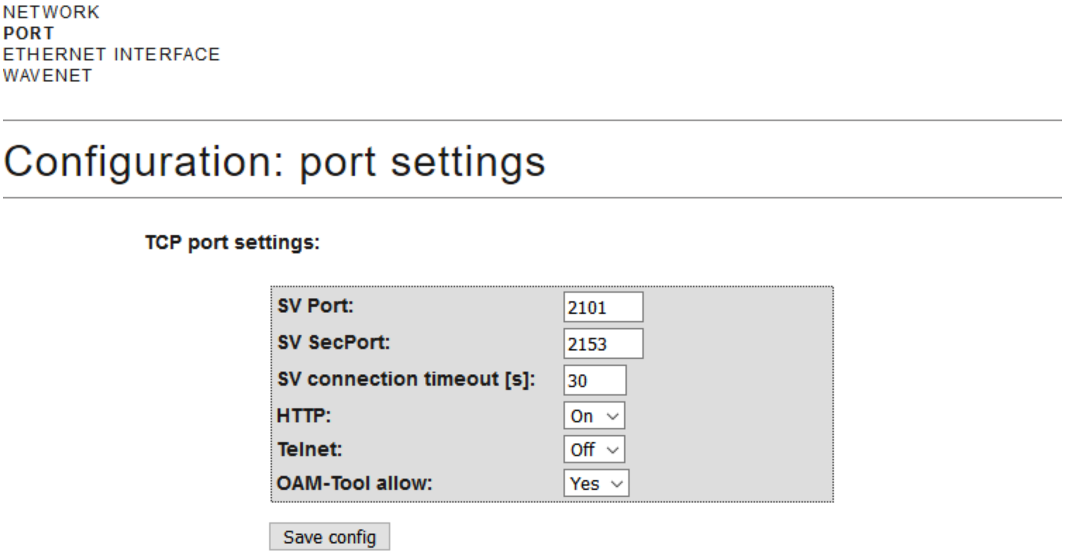
↳ Password is now changed.

Opening and closing the SMTP port

The SMTP port is open ex works and after each reset. As a general rule, ports that are not required should be closed. If you close the SMTP port, the OAM tool will no longer find RouterNode 2.

✓ Browser interface opened.

1. Open the [PORT] tab using | CONFIGURATION |.
   ↳ You will see an overview of the TCP port settings for RouterNode 2.



Configuration: port settings

TCP port settings:

SV Port:	2101
SV SecPort:	2153
SV connection timeout [s]:	30
HTTP:	On
Telnet:	Off
OAM-Tool allow:	Yes

2. Select the "Yes" option (open SMTP port) or the "No" option (close SMTP port) from the ▼ SMTP Port drop-down menu.
3. Click on the button Save.

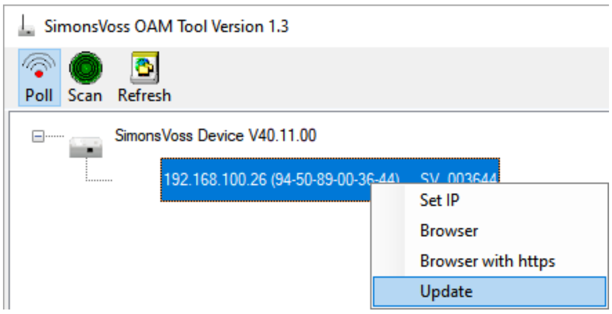
↳ The SMTP port is open or closed.

5.10.2.3 Updating firmware

Newer firmware versions improve your products and may also enable new features (see Firmware information).

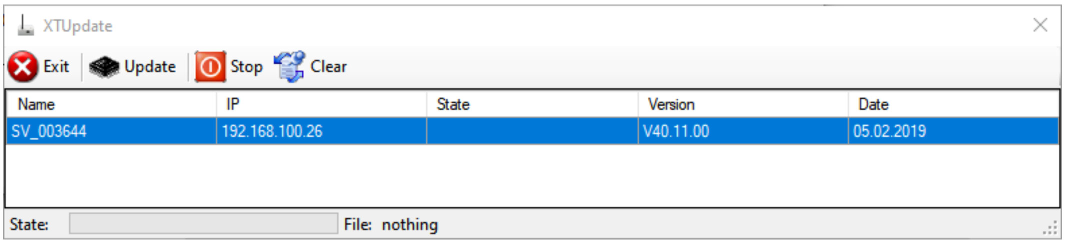
RouterNodes with Ethernet connection

You can update the firmware yourself by using the Operation, Administration and Maintenance Tool (OAM tool) (only RN2). The OAM tool is available free of charge in the download area on the SimonsVoss website (*https://www.simons-voss.com*). You do not need to install the OAM tool.


SimonsVoss OAM Tool Version 1.3
Poll
Scan
Refresh
SimonsVoss Device V40.11.00
192.168.100.26 (94-50-89-00-36-44) SV_003644
Set IP
Browser
Browser with https
Update

- ✓ Latest version of the OAM tool opened (see *Determining and setting the IP address [▸ 55]*).
- ✓ RouterNode listed (see *Determining and setting the IP address [▸ 55]*).
- ✓ Change of IP allowed via the OAM tool (see *Browser interface [▸ 60]*).
- ✓ Current firmware of RouterNode 40.1X or higher.
- ✓ RouterNode type RN2
- ✓ Firmware file (.REL) available (contact your dealer or system partner)

1. Right-click on the entry of the RouterNode you want to update to open the context menu.
2. Select the entry Update.
   ↳ Window "XTUpdate" with a RouterNode list opens.



Name	IP	State	Version	Date
SV_003644	192.168.100.26		V40.11.00	05.02.2019

State: File: nothing

NOTE

Updating multiple RouterNodes

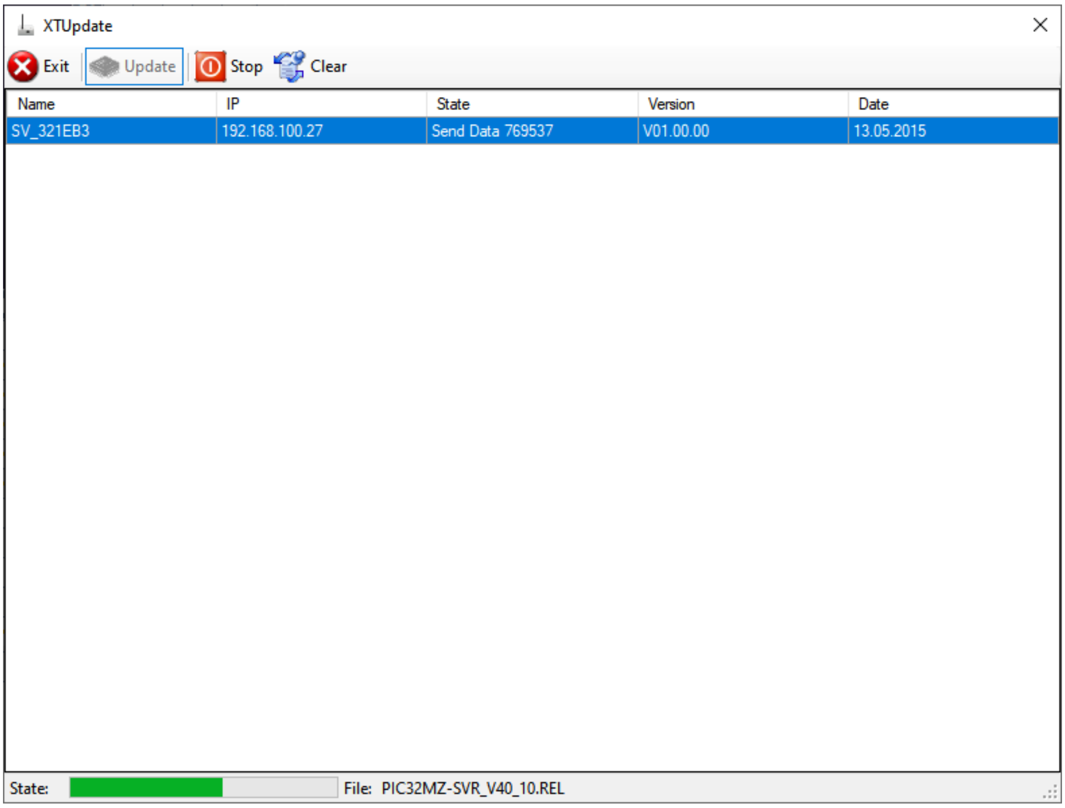
The OAM tool stays open. You can add more entries to the update list in the "XTUpdate" window.

1. Select another RouterNode in the OAM tool.
2. Select the entry Update aus.
   ↳ RouterNode is added to the update list in the "XTUpdate" window.
3. Repeat the steps until all RouterNodes you want to update are in the update list.

↳ RouterNodes are added to the update list in the "XTUpdate" window.

3. Make sure that the RouterNodes you want to update are highlighted.
4. Click on the button Update.
   ↳ Explorer window opens.
5. Navigate to the location of the firmware file.

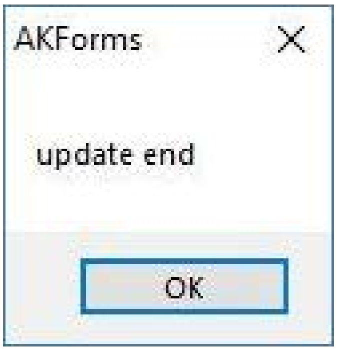
6. Highlight the firmware file.
7. Click on the button Open.
   ↳ The Explorer window closes.
   ↳ The firmware of the RouterNodes is updated.



Name	IP	State	Version	Date
SV_321EB3	192.168.100.27	Send Data 769537	V01.00.00	13.05.2015

State: File: PIC32MZ-SVR_V40_10.REL

↳ The window "AKForms" opens.



update end

8. Click on the OK button.
   ↳ The "AKForms" window closes.
9. Click on the button Exit.
   ↳ The "XTUpdate" window closes.

↳ The firmware of the RouterNodes is updated.

5.10.3 Open configuration page

The procedure is described for RouterNodes. Use the same procedure for SmartIntego GatewayNodes and MobileKey SmartBridges.

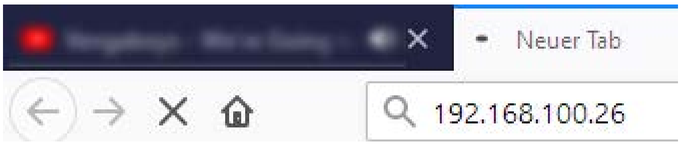
Change the default password after you launch for the first time.

✓ RouterNode IP known (see *Determining and setting the IP address [▸ 55]*).

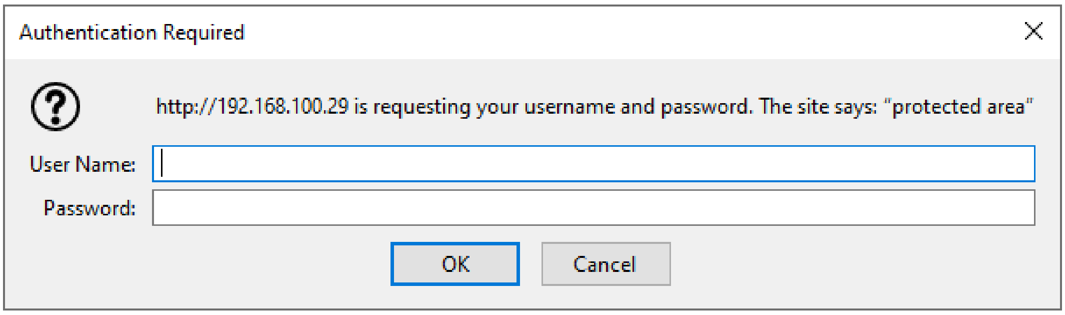
✓ Browser open.

✓ User credentials known for the browser interface (name and password).

1. Enter the IP address in your browser's address field.



2. Press the Enter key to confirm.
   ↳ The "Authentication required" window will open.



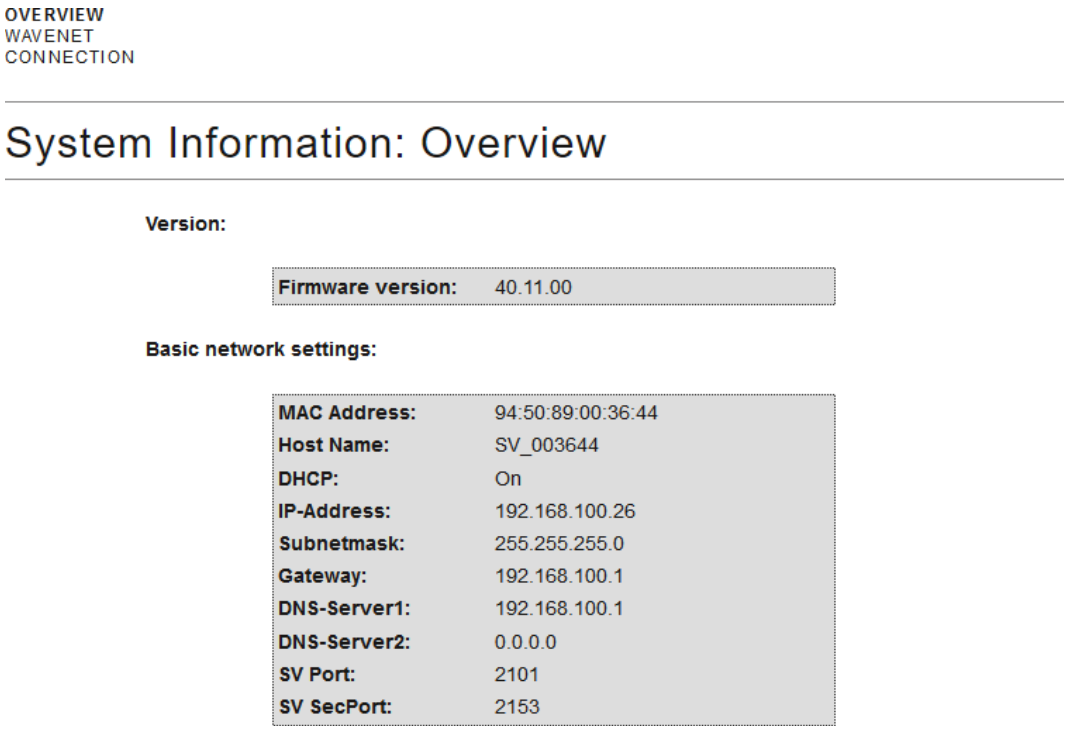
http://192.168.100.29 is requesting your username and password. The site says: "protected area"

User Name:

Password:

3. Enter the login credentials.
4. Click on the OK button.

↳ The browser interface system overview is visible.



System Information: Overview

Version:

Firmware version:	40.11.00

Basic network settings:

MAC Address:	94:50:89:00:36:44
Host Name:	SV_003644
DHCP:	On
IP-Address:	192.168.100.26
Subnetmask:	255.255.255.0
Gateway:	192.168.100.1
DNS-Server1:	192.168.100.1
DNS-Server2:	0.0.0.0
SV Port:	2101
SV SecPort:	2153

NOTE

Web interface can no longer be used with the default password with firmware 40.12 and above

The browser interface remains blocked in firmware version 40.12 or above until the default password has been changed.

- Change the default password.

↳ Browser interface is unblocked and settings can be changed.

5.10.4 Assign IP address

You can assign the IP address statically or have it defined by a DHCP server.

Define the setting either via the configuration page (see *Open configuration page [▸ 67]*) or with the OAM tool:

You can choose: DHCP server or static IP. You can also make the settings described below in the browser interface (see *Browser interface [▸ 60]*).

The procedure is described for RouterNodes. Follow the same procedure for SmartIntego GatewayNodes and MobileKey SmartBridges.

Setting IP for DHCP operation (default)

If you use a DHCP server, the IP address is determined by a DHCP server.

✓ OAM tool available and unpacked.

✓ RouterNode connected to the network.

1. Double-click on the executable file to start the OAM tool.
   ↳ The OAM tool opens.
2. Click on the button Refresh.
   ↳ IP address of the RouterNode updated.
3. Open the context menu by right-clicking on the entry of the IP address of the RouterNode.

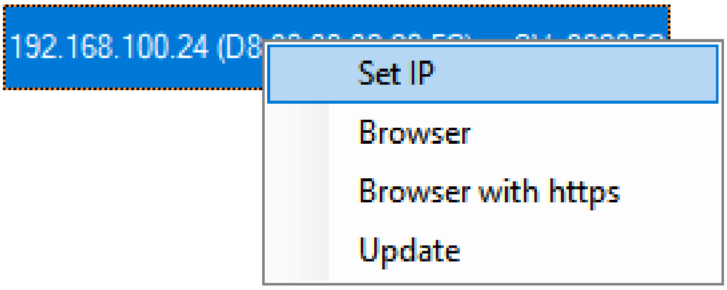
NOTE

Compare MAC

If you select the wrong RouterNode, you could assign the same IP address multiple times.

- Compare the MAC address of the entry with the label on your RouterNode.

4. Click on the entry Set IP.



   ↳ The window "Network configuration" opens.
5. Make sure that the checkbox ☑ Enable DHCP is activated.
6. If no address reservation on the DHCP server is provided for this RouterNode, make a note of the *host name* (e.g. SV_32205C). You will need it later during configuration in the WaveNet Manager (see Add RouterNode to WaveNet).
7. Click on the OK button.
   ↳ The window "Network configuration" closes.
   ↳ RouterNode will restart.
8. Close the information window about the restart.
9. Close the OAM tool.

↳ DHCP operation is set.

Set IP for operation with static IP address

If you are not using a DHCP server, the IP address is the factory default. In this case you must change the IP address, otherwise several router nodes will have the same IP (namely the factory IP) and will not be able to communicate.

✓ OAM tool available and unpacked.

✓ RouterNode connected to the network.

1. Double-click on the executable file to start the OAM tool.
   ↳ The OAM tool opens.
2. Click on the button Refresh.
   ↳ IP address of the RouterNode updated.
3. Open the context menu by right-clicking on the entry of the IP address of the RouterNode.

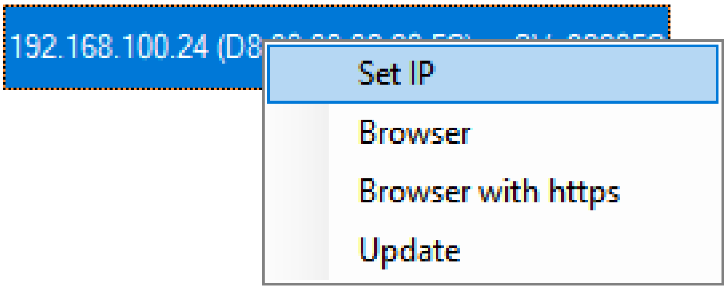
NOTE

Compare MAC

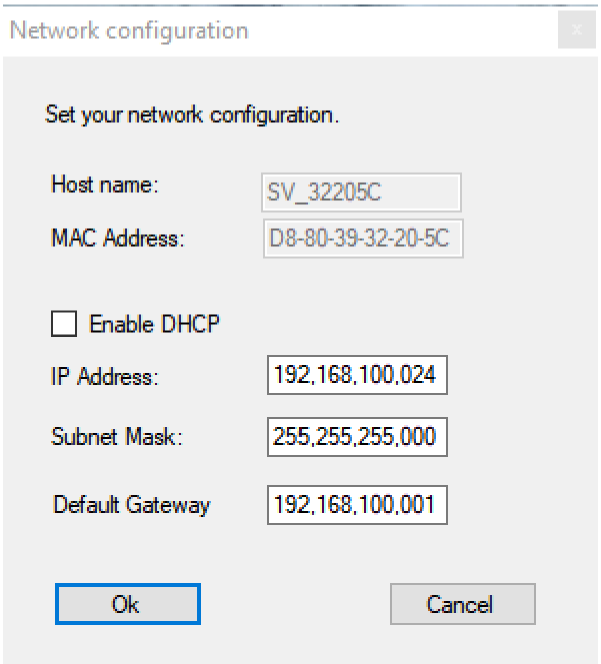
If you select the wrong RouterNode, you could assign the same IP address multiple times.

- Compare the MAC address of the entry with the label on your RouterNode.

4. Click on the entry Set IP.



↳ The window "Network configuration" opens.



Network configuration

Set your network configuration.

Host name: SV_32205C

MAC Address: D8-80-39-32-20-5C

☐ Enable DHCP

IP Address: 192,168,100,024

Subnet Mask: 255,255,255,000

Default Gateway 192,168,100,001

5. Deactivate the checkbox ☐ Enable DHCP.
6. Enter a new IP address, if necessary.
7. Click on the OK button.
   - ↳ The "Network configuration" window closes.
   - ↳ RouterNode will restart.
8. Close the information window about the restart.
9. Close the OAM tool.

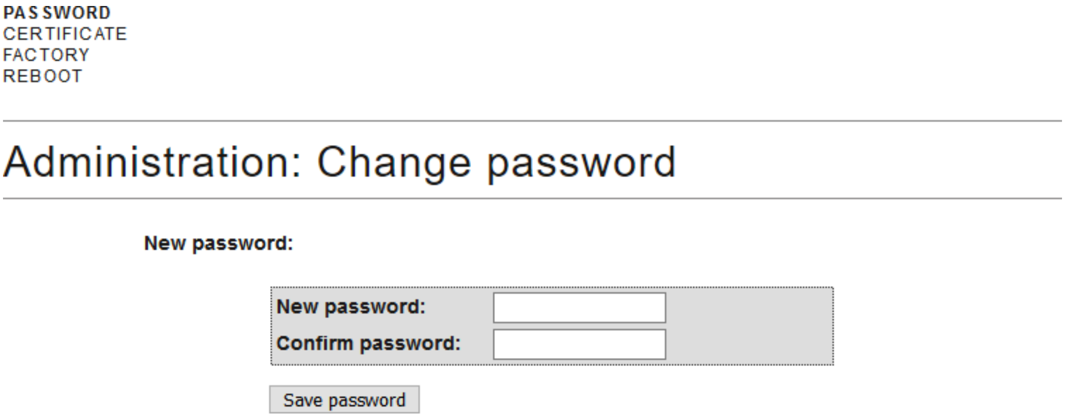
↳ IP address is set.

5.10.5 Change the password of the configuration website

Some browsers do not register any spaces included at the start of a password, so do not begin your password with spaces.

✓ Browser interface opened.

1. Open the [PASSWORD] tab using | ADMINISTRATION |.



Administration: Change password

New password:

New password:

Confirm password:

2. Enter your new password.

3. Repeat your new password.
4. Click on the Save password button.

↳ Password is now changed.

NOTE

Loss of passwords

Your passwords are the basis for managing your locking system. Lost or publicly known passwords are a serious security risk and/or lead to loss of control over the system.

1. Make a note of your passwords.
2. Store your passwords in a safe place.

5.10.6 Set GatewayNode encryption

Also refer to the integrator system documentation.

AES

✓ Configuration page with HTTPS opened in front of the IP address (also see *Open configuration page [▸ 67]*).

1. Select | ADMINISTRATION |.
2. Enter for RN2-Web: Verschlüsselung - AES [offen] your AES keys (only visible for https connection).
3. Enter your AES key in the integrator system.

TLS

✓ Configuration page opened (see *Open configuration page [▸ 67]*).

1. Select | ADMINISTRATION |.
2. Open the menu item RN2-Web: Verschlüsselung - TLS [offen].
3. Import your certificates into the GatewayNode.
4. If necessary, change the RN2-Web: Verschlüsselung - SV SecPort [offen] with | CONFIGURATION |, Port and RN2-Web: Verschlüsselung - SV SecPort [offen].
5. Import your certificates into integrator system.

5.10.7 About IEEE802.1X

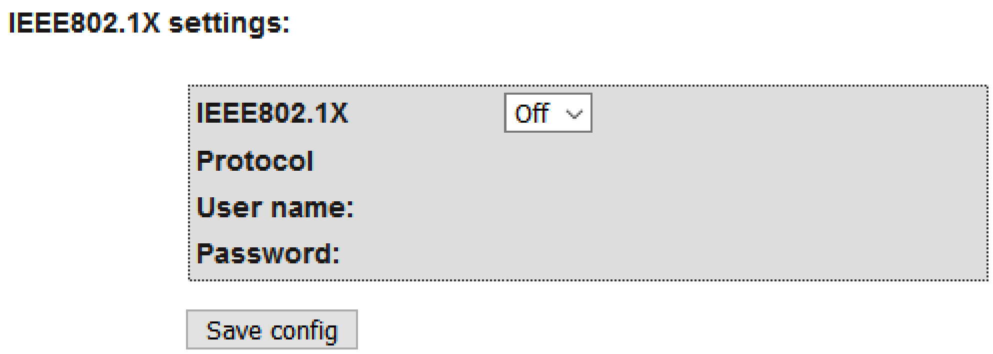
Some managed IT environments require external components to authenticate on the network, typically using IEEE802.1X.

You access the IEEE802.1X settings of the GatewayNode as follows:

✓ Configuration page opened (see *Open configuration page [▸ 67]*).

✓ Information on settings known (ask the system's IT administrator).

1. Via | CONFIGURATION | select the entry ETHERNET INTERFACE.
   ↳ The configuration interface opens.



IEEE802.1X settings:

IEEE802.1X	Off
Protocol	
User name:	
Password:	

2. Make the settings in the "IEEE802.1X settings" section.
3. Click on the Save button.

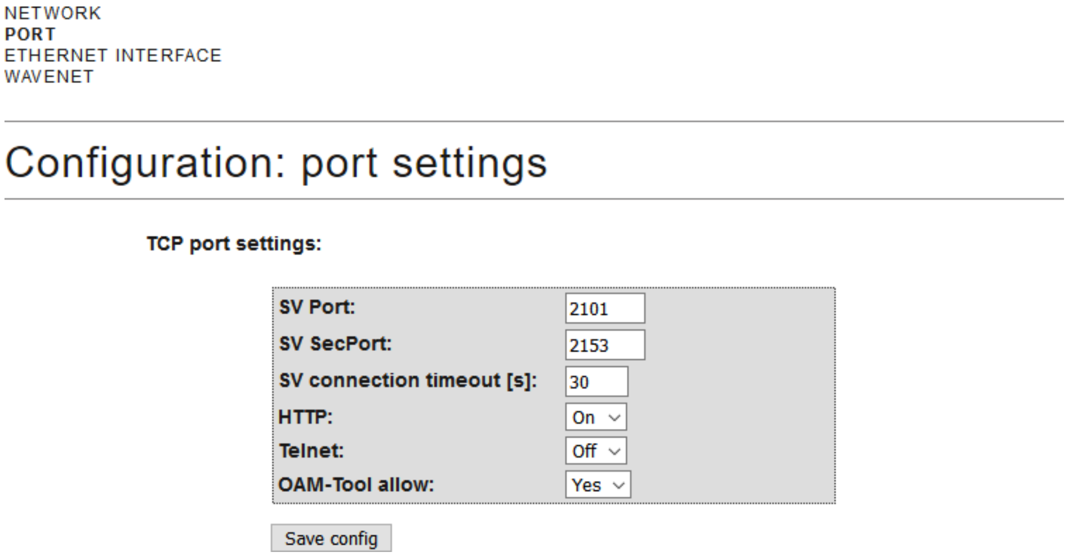
5.10.8 Disable Telnet Access

In some managed IT environments Telnet must be switched off. Telnet is disabled by default from firmware version 40.10.

You can activate and deactivate Telnet manually:

✓ Configuration page opened (see *Open configuration page [▸ 67]*).

1. Via | CONFIGURATION | select the entry Port.
   ↳ The configuration interface opens.



Configuration: port settings

TCP port settings:

SV Port:	2101
SV SecPort:	2153
SV connection timeout [s]:	30
HTTP:	On
Telnet:	Off
OAM-Tool allow:	Yes

2. From the drop-down menu , select the entry ▼ EintragDropDown"Off" or "On".
3. Click on the Save button.

5.10.9 Disable HTTP access (unencrypted)

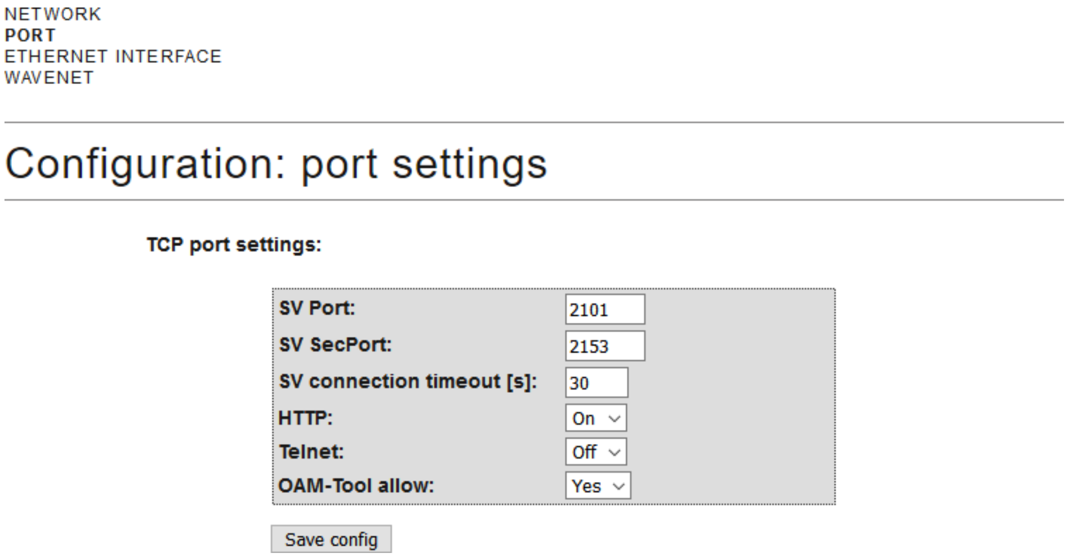
The GatewayNodes configuration page can be displayed both unencrypted (http) and encrypted (https) at the factory.

Some managed IT environments only allow encrypted connections to components.

You can therefore activate and deactivate the unencrypted connection manually:

✓ Configuration page opened (see *Open configuration page [▸ 67]*).

1. Via | CONFIGURATION | select the entry Port .
   ↳ The configuration interface opens.



Configuration: port settings

TCP port settings:

SV Port:	2101
SV SecPort:	2153
SV connection timeout [s]:	30
HTTP:	On
Telnet:	Off
OAM-Tool allow:	Yes

2. From the drop-down menu ▼ **HTTP**, select the entry "Off" or "On".
3. Click on the Save button.

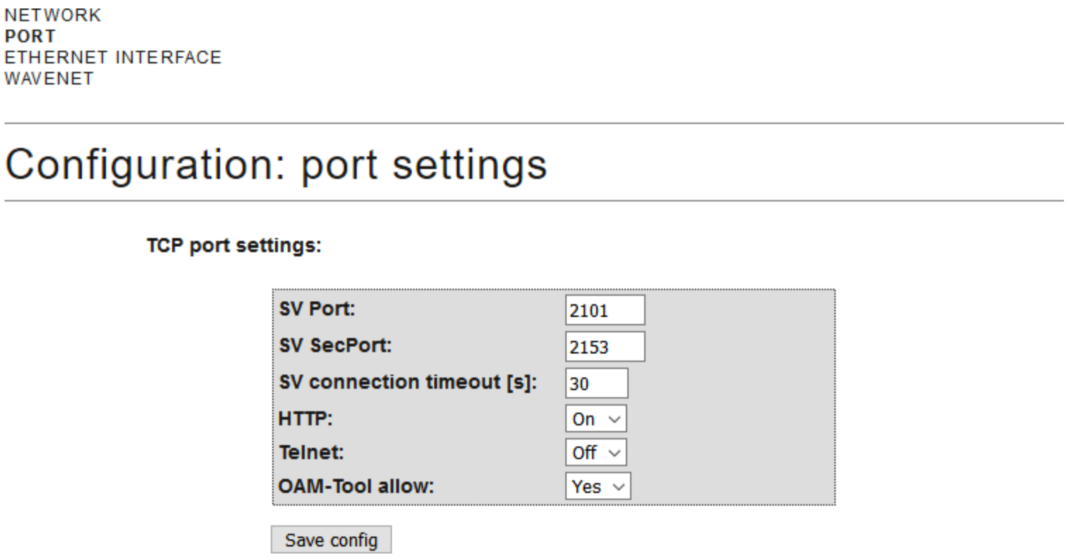
5.10.10 Disable OAM tool access

Access with the OAM tool is not password protected. Disabling OAM Tool access prevents unauthorized users from changing network settings or firmware with the OAM tool.

If you do not enable the ▼ **OAM-Tool allow**, you will not be able to use the OAM tool to perform updates.

✓ Browser interface opened.

1. Open the [PORT] tab using | CONFIGURATION |.
   ↳ You will see an overview of the TCP port settings for RouterNode 2.



NETWORK
PORT
ETHERNET INTERFACE
WAVENET

Configuration: port settings

TCP port settings:

SV Port:	2101
SV SecPort:	2153
SV connection timeout [s]:	30
HTTP:	On
Telnet:	Off
OAM-Tool allow:	Yes

2. Select the option "Yes" (enable the OAM tool to change the IP) or the option "No" (block change to the IP by the OAM tool) from the ▼ OAM-Tool allow drop-down menu.
3. Click on the button Save.

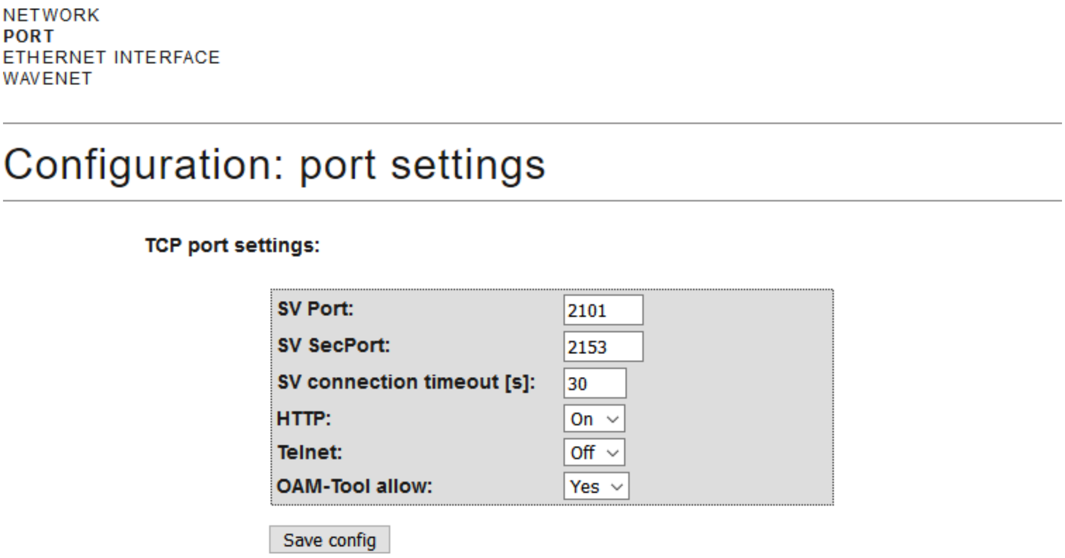
↳ Changing the IP address using the OAM tool is locked/allowed.

5.10.11 TCP Keep Alive (set timeout)

The TCP connection between the integrator system and GatewayNode is automatically terminated after 30 seconds of inactivity. However, the integrator system must maintain the connection. For this purpose, the integrator system sends a monitoring command to the GatewayNodes every 15 s to 25 s. If the integrator deviates from this value, the timeout value in the GatewayNodes must be extended (see also the integrator system documentation):

✓ Configuration page opened (see *Open configuration page [▸ 67]*).

1. Via | CONFIGURATION | select the entry Port.
   ↳ The configuration area opens.



NETWORK
PORT
ETHERNET INTERFACE
WAVENET

Configuration: port settings

TCP port settings:

SV Port:	2101
SV SecPort:	2153
SV connection timeout [s]:	30
HTTP:	On
Telnet:	Off
OAM-Tool allow:	Yes

2. Enter the desired timeout "SV connection timeout [s]" value in the field.
3. Click on the button Save.

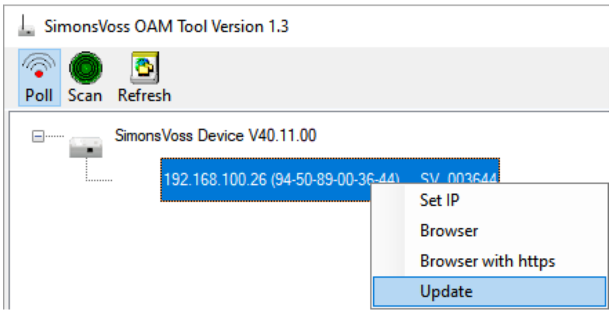
The GatewayNode can also attempt to maintain the connection itself after 27 s to 30 s. In this case, enter 0 as the timeout value. In contrast to handling by the integrator system, the GatewayNode has no error handling in this case and does not send notifications of success/failure.

5.10.12 Update GatewayNode

GatewayNodes with Ethernet connection

- A firmware update takes about a minute.
- A firmware update does not change the configuration.
- During the firmware update, the GatewayNode is not available for the integrator system.

You can update the firmware yourself using the Operations, Administration and Maintenance tool (OAM tool) (GN2 only). The OAM tool is available free of charge in the download area on the SimonsVoss website (*https://www.simons-voss.com*). You do not need to install the OAM tool.



SimonsVoss OAM Tool Version 1.3

SimonsVoss Device V40.11.00

192.168.100.26 (94-50-89-00-36-44) SV_003644

✓ Latest version of OAM tool opened (see *Search GatewayNode [▸ 54]*).

✓ GatewayNode (see *Search GatewayNode [▸ 54]*).

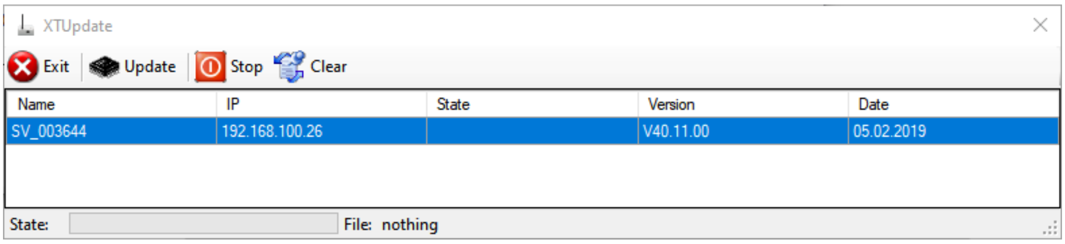
✓ Change of IP allowed via OAM tool (see *Disable OAM tool access [▸ 74]*).

✓ Current firmware of RouterNode 40.1X or later.

✓ GatewayNode type GN2

✓ Firmware file (.REL) available (included in your SI-TechKit).

1. Right-click the entry of the GatewayNode you want to update to open the context menu.
2. Select the entry Update.
   ↳ A window "XTUpdate" with a GatewayNode list opens.



Name	IP	State	Version	Date
SV_003644	192.168.100.26		V40.11.00	05.02.2019

State: File: nothing

NOTE

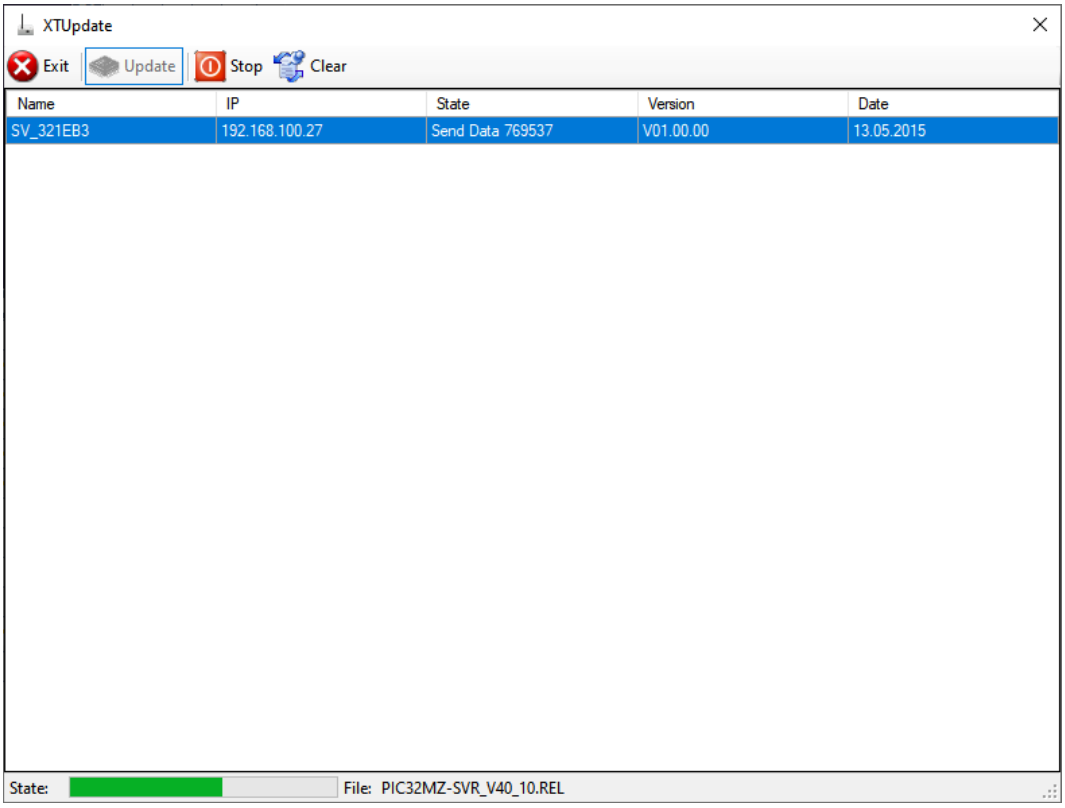
Updating multiple GatewayNodes

The OAM tool remains open. You can add further entries to the update list in the window "XTUpdate".

1. Select another GatewayNode in the OAM tool.
2. Select the entry Update.
   ↳ GatewayNode is added to the update list in the window "XTUpdate".
3. Repeat the steps until all GatewayNodes you want to update are in the update list.

↳ GatewayNodes are added to the update list in the window "XTUpdate".

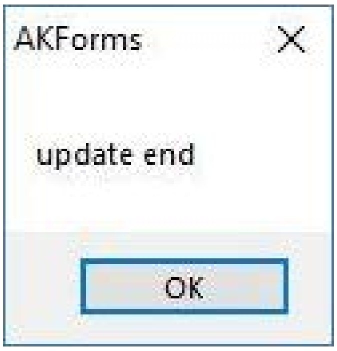
3. Make sure that the GatewayNodes you want to update are highlighted.
4. Click on the Update button.
   ↳ The Explorer window opens.
5. Navigate to the firmware file location.
6. Select the firmware file.
7. Click on the Open button.
   ↳ Explorer window closes.
   ↳ Updating firmware of GatewayNodes.



Name	IP	State	Version	Date
SV_321EB3	192.168.100.27	Send Data 769537	V01.00.00	13.05.2015

State: File: PIC32MZ-SVR_V40_10.REL

↳ The window "AKForms" opens.



update end

8. Click on the OK button.
   ↳ Window "AKForms" closes.
9. Click on the Exit button.
   ↳ Window "XTUpdate" closes.

↳ The firmware of the GatewayNodes is updated.

5.11 RS-485 ConfigNode

5.11.1 Configure RS-485 ConfigNode

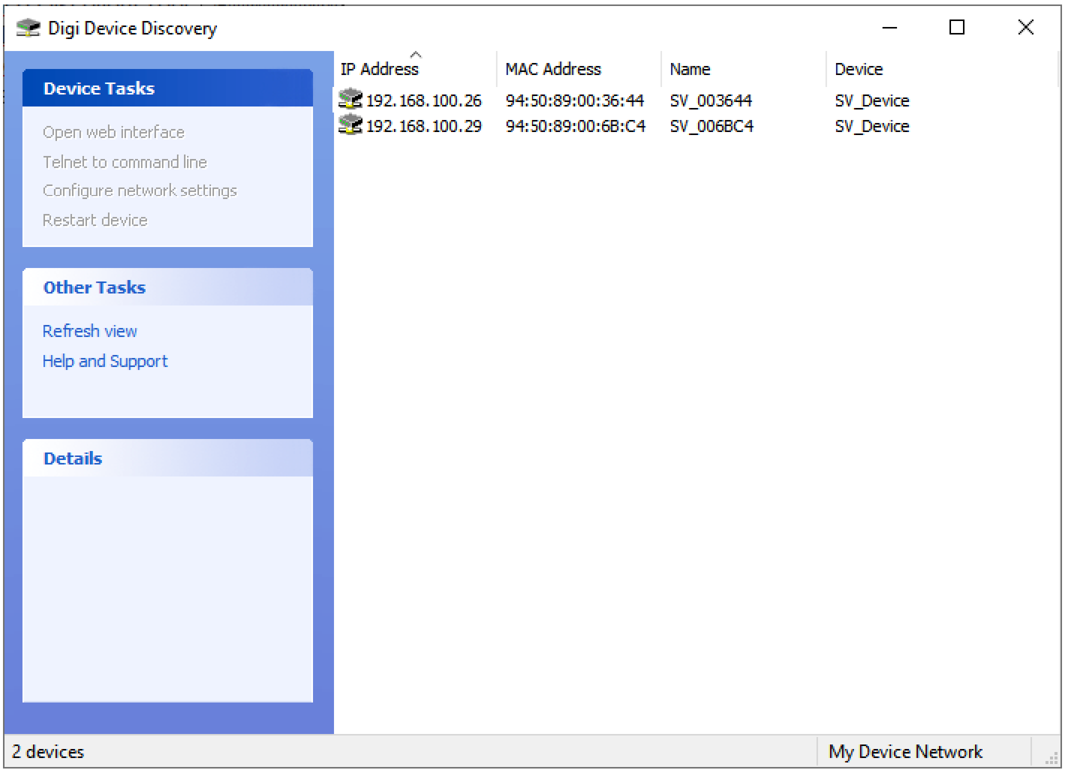
There is no need to pre-configure your RS-485 GatewayNodes.

Only assign a free IP address to the ConfigNode. You can assign this IP address statically or have it defined by a DHCP server. If there is no DHCP server, the component uses the default IP address: 169.254.X.X.

Find ConfigNode

You can find your ConfigNode with the Digi Device Discovery Tool:

1. Launch the Digi Device Discovery Tool.
2. Connect ConfigNode to your computer.
3. Start the Digi Device Discovery Tool.
   ↳ Digi Device Discovery Tool.

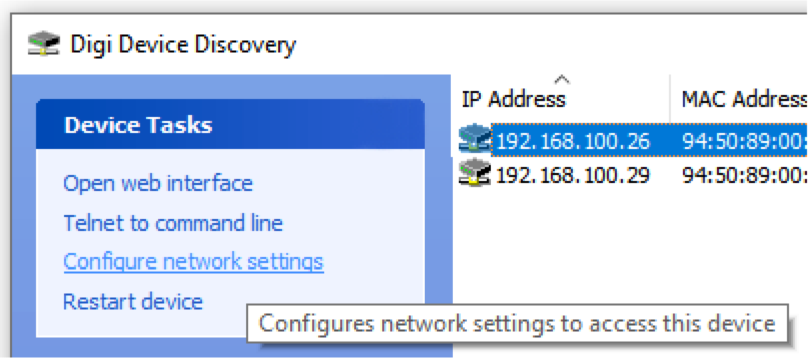


IP Address	MAC Address	Name	Device
192.168.100.26	94:50:89:00:36:44	SV_003644	SV_Device
192.168.100.29	94:50:89:00:6B:C4	SV_006BC4	SV_Device

2 devices

My Device Network

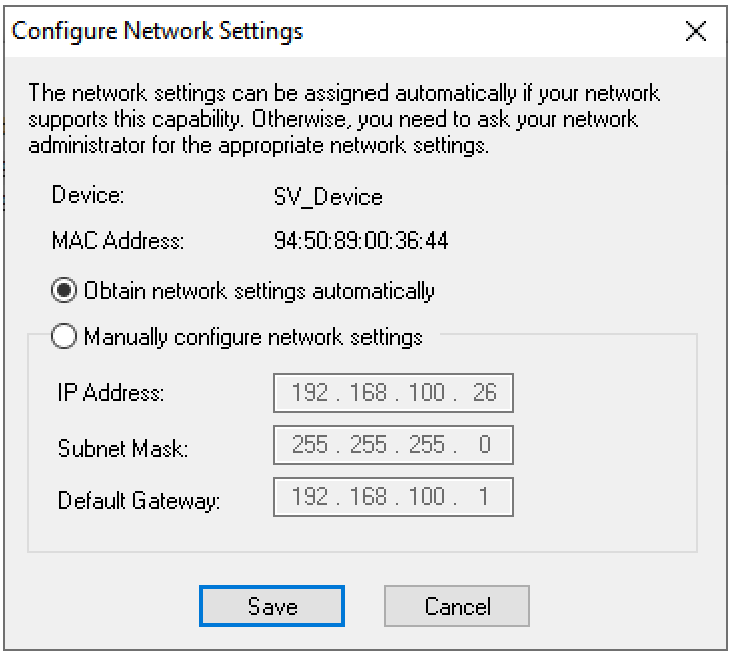
4. Highlight the entry of your component.
5. Click on the Configure network settings button.



IP Address	MAC Address
192.168.100.26	94:50:89:00:
192.168.100.29	94:50:89:00:

Configures network settings to access this device

↳ The "DDD Tool: Configure network settings" window opens.



Configure Network Settings

The network settings can be assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate network settings.

Device: SV_Device

MAC Address: 94:50:89:00:36:44

● Obtain network settings automatically

○ Manually configure network settings

IP Address: 192 . 168 . 100 . 26

Subnet Mask: 255 . 255 . 255 . 0

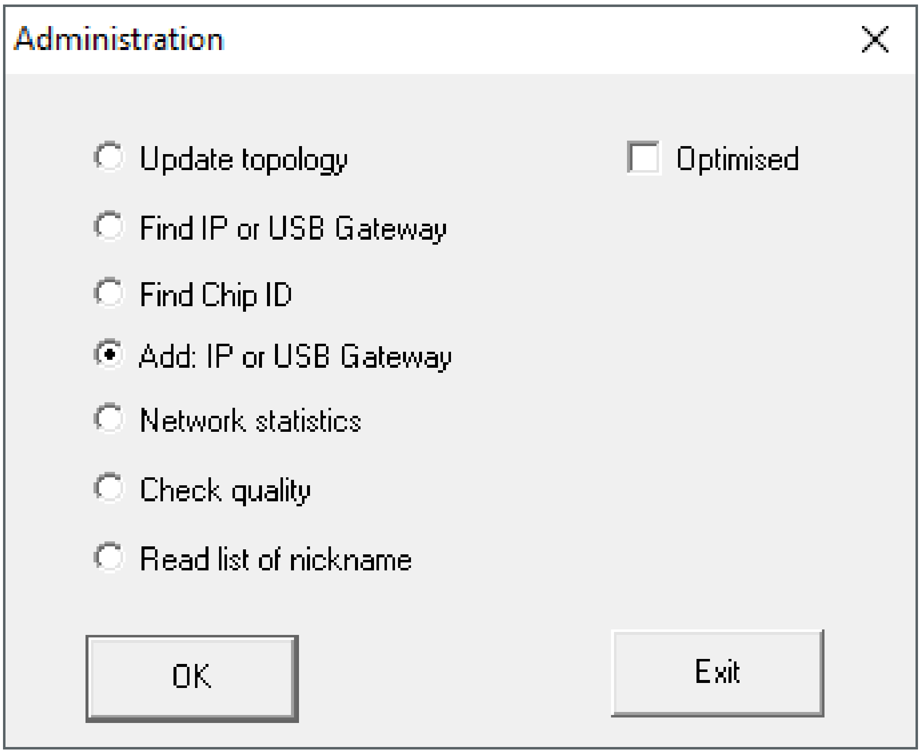
Default Gateway: 192 . 168 . 100 . 1

6. Specify the IP settings.
7. Click on the button Save.

Add ConfigNode

✓ SmartIntego Manager opened.

1. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.



Administration

○ Update topology

□ Optimised

○ Find IP or USB Gateway

○ Find Chip ID

● Add: IP or USB Gateway

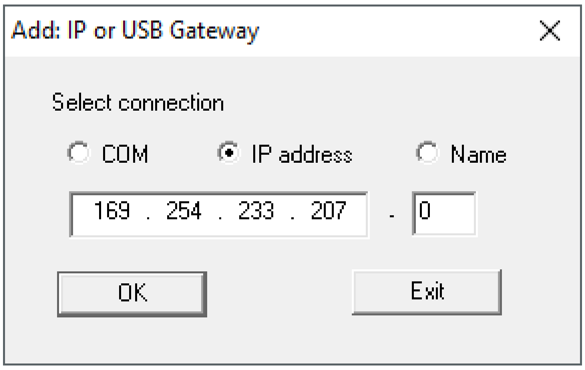
○ Network statistics

○ Check quality

○ Read list of nickname

2. Select the ● Add IP or USB gateway option.

3. Click on the button OK.
   - ↳ Window "Administration" closes.
   - ↳ The window "Add IP or USB Gateway" opens.



Add: IP or USB Gateway

Select connection

○ COM ● IP address ○ Name

169 . 254 . 233 . 207 - 0

4. Select the option ● IP address.
5. Enter the IP address you have identified (example: Start-IP 169.254.233.207, end-IP: 0).
6. Click on the button OK.

↳ ConfigNode is added.

5.11.2 Configure RS-485 ConfigNode for another project

NOTE

Reset ConfigNode for new projects

Configured ConfigNodes can cause problems in new projects.

- Reset ConfigNode as described before using it in a new project.

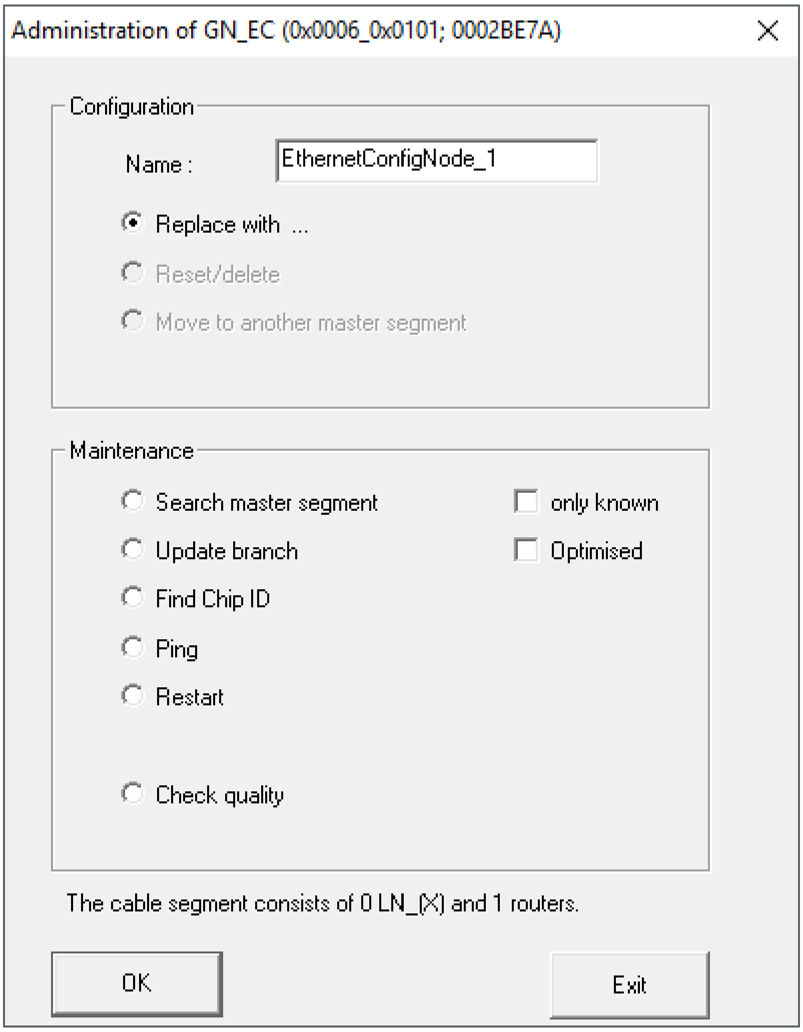
1. Reset the WaveNet settings of the ConfigNode (hardware reset, see *Resetting the WaveNet/network configuration of the GatewayNode [▸ 167]*).
2. Connect ConfigNode to a new project.
3. Determine/set the IP address (see *Search GatewayNode [▸ 54]* and *Assign IP address [▸ 68]*).
4. Add the ConfigNode with SmartIntego Manager (see *Configure RS-485 ConfigNode [▸ 78]*).

5.11.3 Use RS-485 ConfigNode in various projects

✓ SmartIntego Manager opened (see *Setting up SmartIntego Manager [▸ 83]*).

1. Reset the WaveNet settings of the ConfigNode (hardware reset, see *Resetting the WaveNet/network configuration of the GatewayNode [▸ 167]*).

2. Connect the ConfigNode in the second project.
3. Determine the IP address (see *Search GatewayNode [▸ 54]*).
4. In SmartIntego Manager, right-click the ConfigNode entry.
   ↳ The window "Administration" opens.



Administration of GN_EC (0x0006_0x0101; 0002BE7A)

Configuration

Name : EthernetConfigNode_1

● Replace with ...
○ Reset/delete
○ Move to another master segment

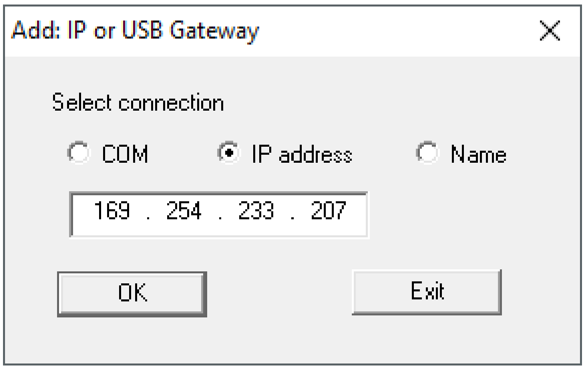
Maintenance

○ Search master segment □ only known
○ Update branch □ Optimised
○ Find Chip ID
○ Ping
○ Restart

○ Check quality

The cable segment consists of 0 LN_(X) and 1 routers.

5. Select the option ● Replace with.
6. Click on the button OK.
   ↳ The window "Add IP or USB Gateway" opens.



Add: IP or USB Gateway

Select connection

○ COM ● IP address ○ Name

169 . 254 . 233 . 207

7. Enter the IP address determined for the ConfigNode.

8. Click on the button OK.
   - ↳ Window "Add IP or USB Gateway" closes.
   - ↳ ConfigNode is described with the data of the project.

↳ ConfigNode set up for second project.

5.12 Setting up SmartIntego Manager

You program the WaveNet configuration of the components using SmartIntego Manager.

IMPORTANT

Password assignment at first start

You can only assign the password when you first start the WaveNet Manager. If you do not assign a password when you first start the WaveNet Manager, you will not be able to assign a password afterwards. The password is then empty.

- Assign a password the first time you start the WaveNet Manager.

✓ TCP/RS-485 configuration of GatewayNodes completed.

1. Assign a WaveNet password at the first start. (This password protects the WaveNet configuration of all SmartIntego components).

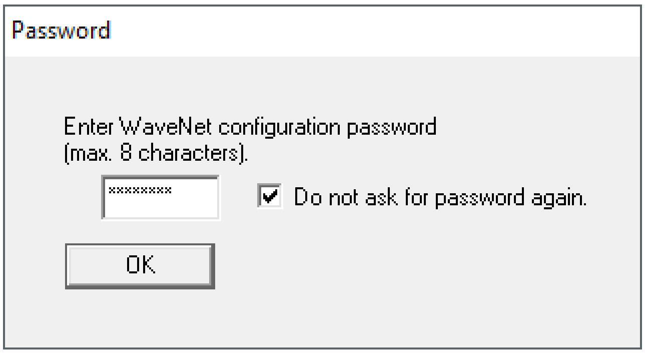
NOTE

Loss of passwords

Your passwords are the basis for managing your locking system. Lost or publicly known passwords are a serious security risk and/or lead to loss of control over the system.

1. Make a note of your passwords.
2. Store your passwords in a safe place.

2. If you no longer wish to be asked for the password in the future, activate the checkbox ☑ Do not ask for password again.



Password

Enter WaveNet configuration password (max. 8 characters).

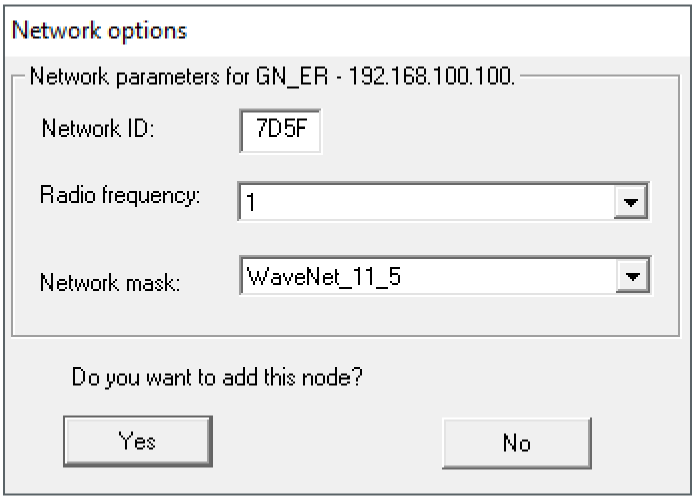
****

☑ Do not ask for password again.

5.13 WaveNet global settings

You define three parameters when you add the first GatewayNode to your project:

1. Network ID (must be individual for each project)
2. Radio frequency (frequency 1 and 2 can be selected)
3. Network mask (general recommendation: 11_5 = 11 bit and 5 bit, other settings are possible.)



Network options

Network parameters for GN_ER - 192.168.100.100.

Network ID: 7D5F

Radio frequency: 1

Network mask: WaveNet_11_5

Do you want to add this node?

NOTE

GatewayNodes already configured

GatewayNodes that have already been configured already have a network ID. Therefore, the Network ID field is greyed out.

- Reset previously configured GatewayNodes (see *Reset components [▸ 156]*).

5.14 Add GatewayNode

You can add GatewayNodes individually or collectively:

- Enter an IP address
- Enter a host name

Requests to host names are forwarded through a DNS server. If this DNS server is not reachable, you will not reach your GatewayNodes. They are (additionally) dependent on a functioning DNS server. Avoid this dependency by adding your GatewayNodes via the IP address. If IT or the integrator system dictates adding via host names, add your GatewayNodes via host names as required.

Always choose one of the two variants: Either add all TCP GatewayNodes over IP addresses or all TCP GatewayNodes over host names. Mixed configurations greatly increase support efforts.

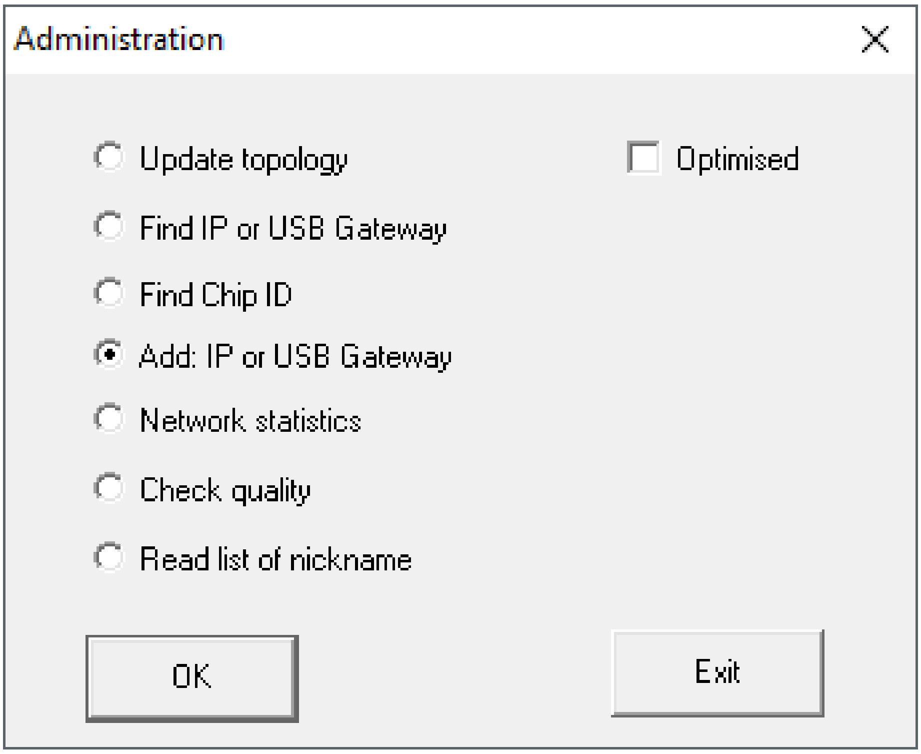
5.14.1 TCP: Add individual GatewayNodes

✓ GatewayNode powered and connected.

✓ TCP configuration completed (see *Configuring GatewayNodes (TCP) [▸ 54]*).

✓ SmartIntego Manager opened.

1. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.



Administration

○ Update topology

□ Optimised

○ Find IP or USB Gateway

○ Find Chip ID

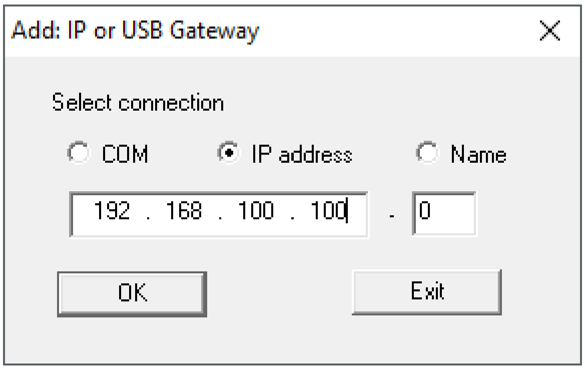
● Add: IP or USB Gateway

○ Network statistics

○ Check quality

○ Read list of nickname

2. Select the option ● Add IP or USB gateway.
3. Click on the button OK.
   ↳ Window "Administration" closes.
   ↳ The window "Add IP or USB Gateway" opens.



192 . 168 . 100 . 100 . 0

4. Enter the IP address (example: 192.168.100.100, End IP: 0).
5. Click on the button OK.
   - ↳ Window "Add IP or USB Gateway" closes.
6. Right-click the entry of the new GatewayNode.

NOTE

Name assignment by name list

If you are using a name list (*Creating, expanding and importing a name list [▸ 29]* see), you no longer need to name the GatewayNodes.

   - ↳ The window "Administration" opens.
7. Specify the name of your GatewayNode.
8. Click on the button OK.
   - ↳ Window "Administration" closes.
9. Click on the button Save.
   - ↳ SmartIntego Manager contacts the GatewayNode.
   - ↳ SmartIntego Manager assigns GatewayNode device address.
   - ↳ SmartIntego Manager saves routing table in the GatewayNode.

NOTE

Data loss due to improper termination

The data is not transferred to the SmartIntego tool (WO) until the SmartIntego Manager is properly ended. After saving, the files are permanently saved in the * ikp file in the SmartIntego tool (WO).

1. Click on the Save button.
2. Close SmartIntego Manager correctly using the button Exit.

5.14.2 TCP: Add multiple GatewayNodes (IP range)

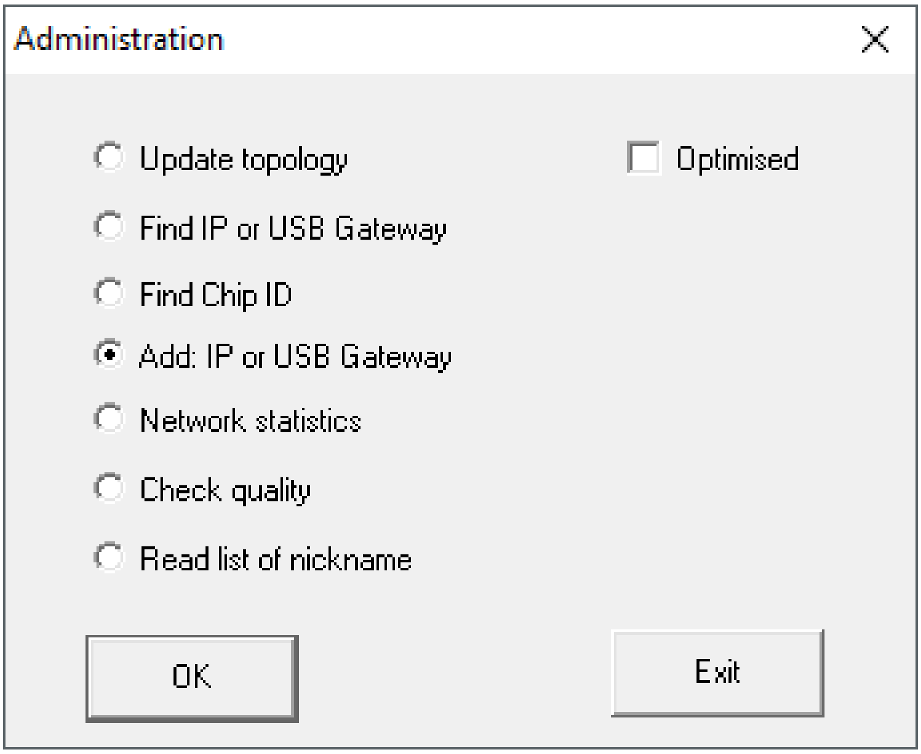
✓ All GatewayNodes powered and mounted.

✓ TCP configuration completed (see *Configuring GatewayNodes (TCP) [▸ 54]*).
Unreachable IP addresses are skipped.

✓ Start IP address of the range must be physically reachable.

✓ SmartIntego Manager opened.

1. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.



Administration

○ Update topology

○ Find IP or USB Gateway

○ Find Chip ID

● Add: IP or USB Gateway

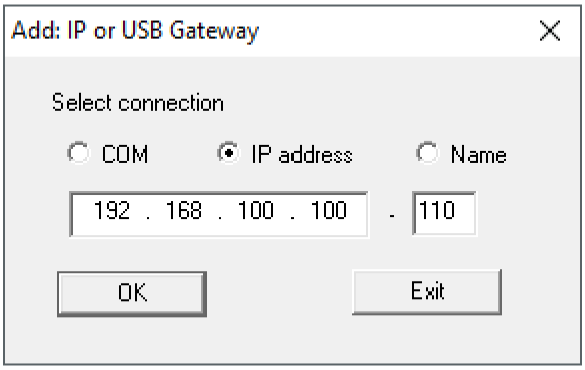
○ Network statistics

○ Check quality

○ Read list of nickname

□ Optimised

2. Select the option ● Add IP or USB gateway.
3. Click on the button OK.
   ↳ Window "Administration" closes.
   ↳ The window "Add IP or USB Gateway" opens.



Add: IP or USB Gateway

Select connection

○ COM ● IP address ○ Name

192 . 168 . 100 . 100 - 110

4. Specify the start IP address of the IP range and the last digit of the end IP (example: Start-IP: 192.168.100.100, End IP: 192,168,100,110).
5. Click on the button OK.
   ↳ Window "Add IP or USB Gateway" closes.
6. Right-click the entry of the new GatewayNode.

NOTE

Name assignment by name list

If you are using a name list (*Creating, expanding and importing a name list [▸ 29]* see), you no longer need to name the GatewayNodes.

   ↳ The window "Administration" opens.

7. Select the option ● Set name.
8. Click on the button OK.
   ↳ Window "Administration" closes.
   ↳ The window for naming opens.
9. Specify the name of your GatewayNode.
10. Click on the button Save.
    ↳ Name assignment window closes.
    ↳ SmartIntego Manager contacts the GatewayNode.
    ↳ SmartIntego Manager assigns GatewayNode device address.
    ↳ SmartIntego Manager saves routing table in the GatewayNode.
11. If necessary, repeat the designation for the other GatewayNodes.

NOTE

Data loss due to improper termination

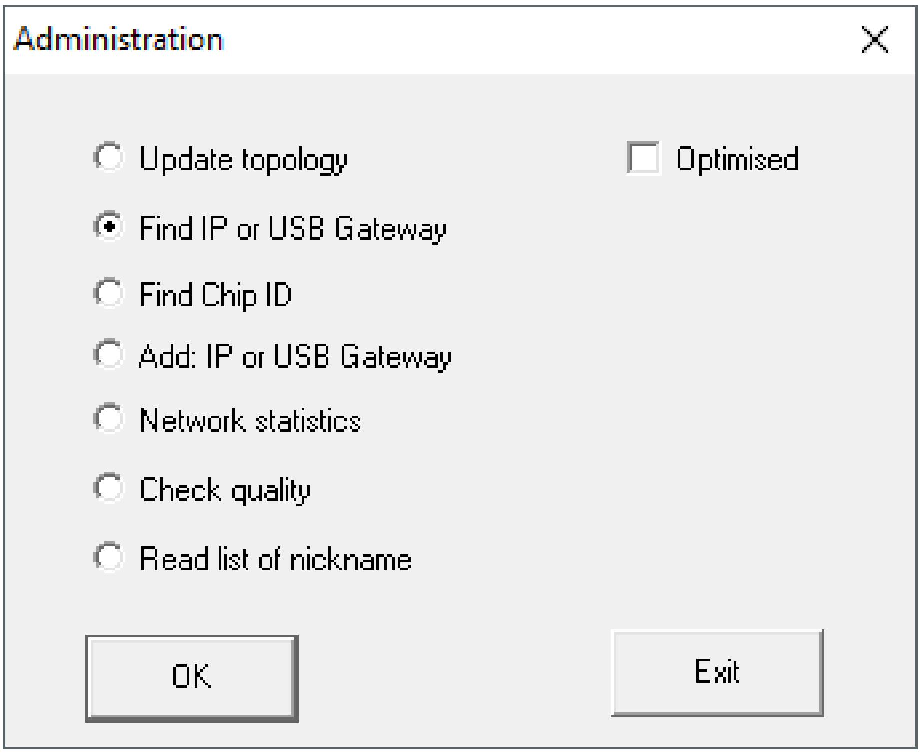
The data is not transferred to the SmartIntego tool (WO) until the SmartIntego Manager is properly ended. After saving, the files are permanently saved in the * ikp file in the SmartIntego tool (WO).

1. Click on the Save button.
2. Close SmartIntego Manager correctly using the button Exit.

5.14.3 TCP: Add multiple GatewayNodes (Broadcast)

- ✓ All GatewayNodes powered and mounted.
- ✓ TCP configuration completed (see *Configuring GatewayNodes (TCP) [▸ 54]*).
- ✓ Configuration PC and all GatewayNodes on the same (IP)subnet.
- ✓ SmartIntego Manager opened.

1. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.



Administration

○ Update topology

● Find IP or USB Gateway

○ Find Chip ID

○ Add: IP or USB Gateway

○ Network statistics

○ Check quality

○ Read list of nickname

□ Optimised

2. Select the option ● Find IP or USB gateway.
3. Click on the button OK.
   - ↳ Window "Administration" closes.
   - ↳ SmartIntego Manager searches for reachable GatewayNodes.
   - ↳ SmartIntego Manager adds all accessible GatewayNodes.
4. Right-click the entry of the new GatewayNode.

NOTE

Name assignment by name list

If you are using a name list (*Creating, expanding and importing a name list [▸ 29]* see), you no longer need to name the GatewayNodes.

   - ↳ The window "Administration" opens.
5. Specify the name of your GatewayNode.
6. Click on the button OK.
   - ↳ Window "Administration" closes.
7. Click on the button Save.
   - ↳ SmartIntego Manager contacts the GatewayNode.
   - ↳ SmartIntego Manager assigns GatewayNode device address.
   - ↳ SmartIntego Manager saves routing table in the GatewayNode.

NOTE

Data loss due to improper termination

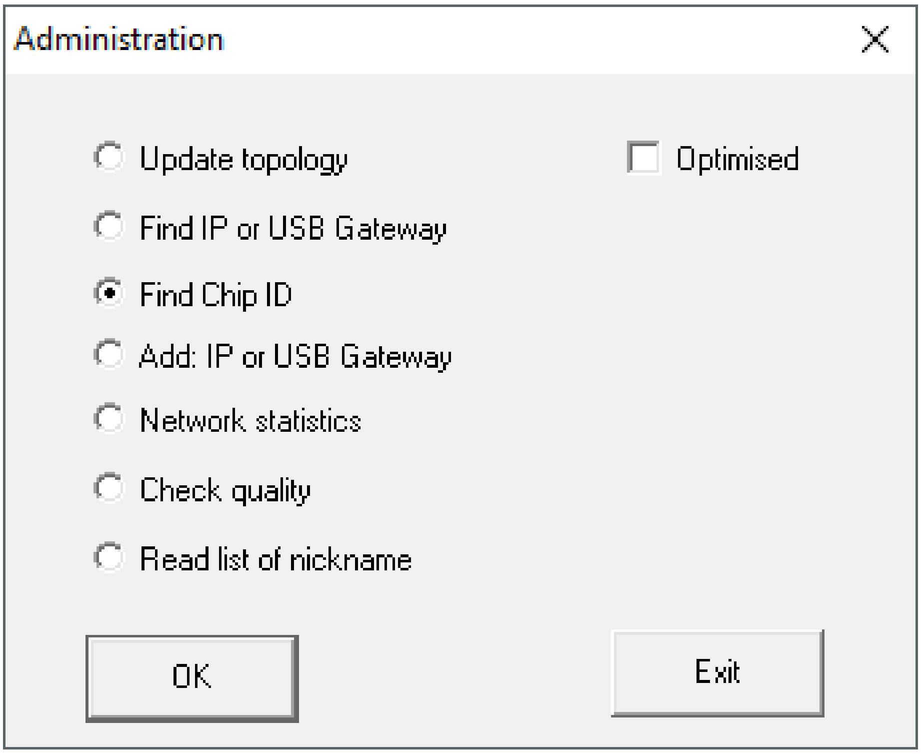
The data is not transferred to the SmartIntego tool (WO) until the SmartIntego Manager is properly ended. After saving, the files are permanently saved in the * ikp file in the SmartIntego tool (WO).

1. Click on the Save button.
2. Close SmartIntego Manager correctly using the button Exit .

5.14.4 TCP/RS-485: Add Radio Radio Gateway Node

- ✓ SI.GN.R connected to WN.POWER.SUPPLY.PPP.
- ✓ SI.GN.R.
- ✓ SmartIntego Manager opened.

1. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.

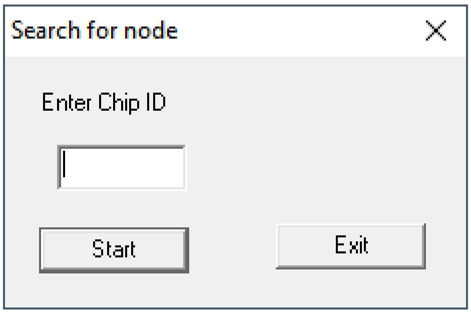


Administration

○ Update topology
○ Find IP or USB Gateway
● Find Chip ID
○ Add: IP or USB Gateway
○ Network statistics
○ Check quality
○ Read list of nickname

□ Optimised

2. Select the option ● Find Chip ID.
3. Click on the button OK .
   ↳ Window "Administration" closes.
   ↳ The window "Search for node" opens.



4. Enter the chip ID of the SI.GN.R without leading zeros (label or type plate).
5. Click on the Start button.
   - ↳ Window "Search for node" closes.
   - ↳ SmartIntego Manager searches for chip ID.
   - ↳ SmartIntego Manager displays search results with RSSI values. (RSSI values indicate the accessibility of the existing GatewayNodes.)
6. Select the GatewayNode to which you want to add the GatewayNode Radio (usually the one with the best accessibility).
7. Click on the button OK.
   - ↳ Search results are closed.
8. Right-click the entry of the new GatewayNode.

NOTE

Name assignment by name list

If you are using a name list (*Creating, expanding and importing a name list [▸ 29]* see), you no longer need to name the GatewayNodes.

   - ↳ The window "Administration" opens.
9. Specify the name of your GatewayNode.
10. Click on the button OK.
    - ↳ Window "Administration" closes.
11. Click on the button Save.
    - ↳ SmartIntego Manager contacts the GatewayNode.
    - ↳ SmartIntego Manager assigns GatewayNode device address.
    - ↳ SmartIntego Manager saves routing table in the GatewayNode.
12. If necessary, repeat the designation for the other GatewayNodes.
13. If necessary, add further locking devices to the new segment.
14. Click on the button Save.
    - ↳ SmartIntego Manager contacts the GatewayNode.
    - ↳ SmartIntego Manager assigns GatewayNode device address.
    - ↳ SmartIntego Manager saves routing table in the GatewayNode.

NOTE

Data loss due to improper termination

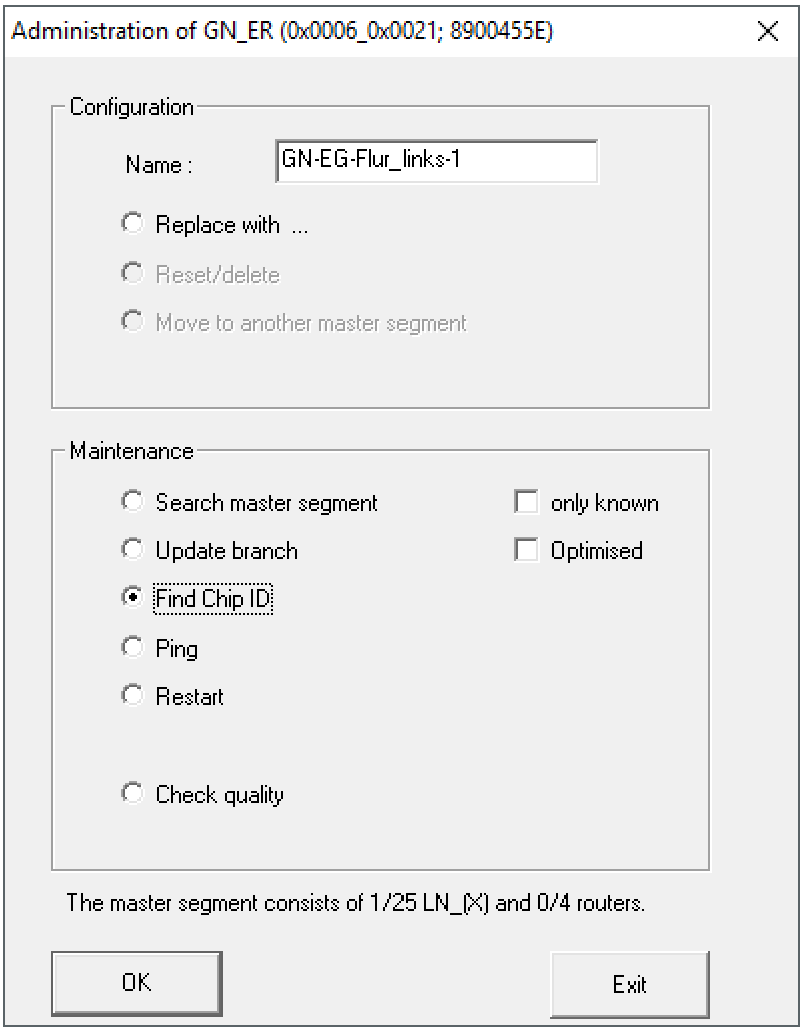
The data is not transferred to the SmartIntego tool (WO) until the SmartIntego Manager is properly ended. After saving, the files are permanently saved in the * ikp file in the SmartIntego tool (WO).

1. Click on the Save button.
2. Close SmartIntego Manager correctly using the button Exit.

5.14.5 RS-485: Add individual GatewayNodes

- ✓ GatewayNode powered and connected.
- ✓ RS-485 configured (see *RS-485 ConfigNode [▸ 78]*).
- ✓ ConfigNode configured (see *RS-485 ConfigNode [▸ 78]*).
- ✓ SmartIntego Manager opened.

1. Click with the right mouse button on the ConfigNode entry.
   ↳ The window "Administration" opens.



Administration of GN_ER (0x0006_0x0021; 8900455E)

Configuration

Name : GN-EG-Flur_links-1

○ Replace with ...

○ Reset/delete

○ Move to another master segment

Maintenance

○ Search master segment □ only known

○ Update branch □ Optimised

● Find Chip ID

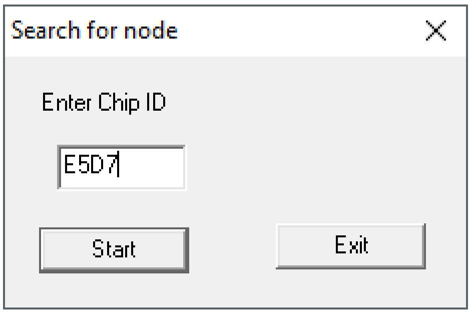
○ Ping

○ Restart

○ Check quality

The master segment consists of 1/25 LN_(X) and 0/4 routers.

2. Select the option ◉ Find Chip ID.
3. Click on the button OK.
   - ↳ Window "Administration" closes.
   - ↳ The window "Search for node" opens.



E5D7

4. Enter the chip ID without leading zeros (example: E5D7).
5. Click on the Start button.
   - ↳ Window "Search for node" closes.
   - ↳ SmartIntego Manager searches for chip ID.
6. Right-click the entry of the new GatewayNode.

NOTE

Name assignment by name list

If you are using a name list (*Creating, expanding and importing a name list [▸ 29]* see), you no longer need to name the GatewayNodes.

   - ↳ The window "Administration" opens.
7. Specify the name of your GatewayNode.
8. Click on the button OK.
   - ↳ Window "Administration" closes.
9. Click on the button Save.
   - ↳ SmartIntego Manager contacts the GatewayNode.
   - ↳ SmartIntego Manager assigns GatewayNode device address.
   - ↳ SmartIntego Manager saves routing table in the GatewayNode.
10. Click on the button Save.

NOTE

Data loss due to improper termination

The data is not transferred to the SmartIntego tool (WO) until the SmartIntego Manager is properly ended. After saving, the files are permanently saved in the * ikp file in the SmartIntego tool (WO).

1. Click on the Save button.
2. Close SmartIntego Manager correctly using the button Exit.

5.14.6 RS-485: Add multiple GatewayNodes

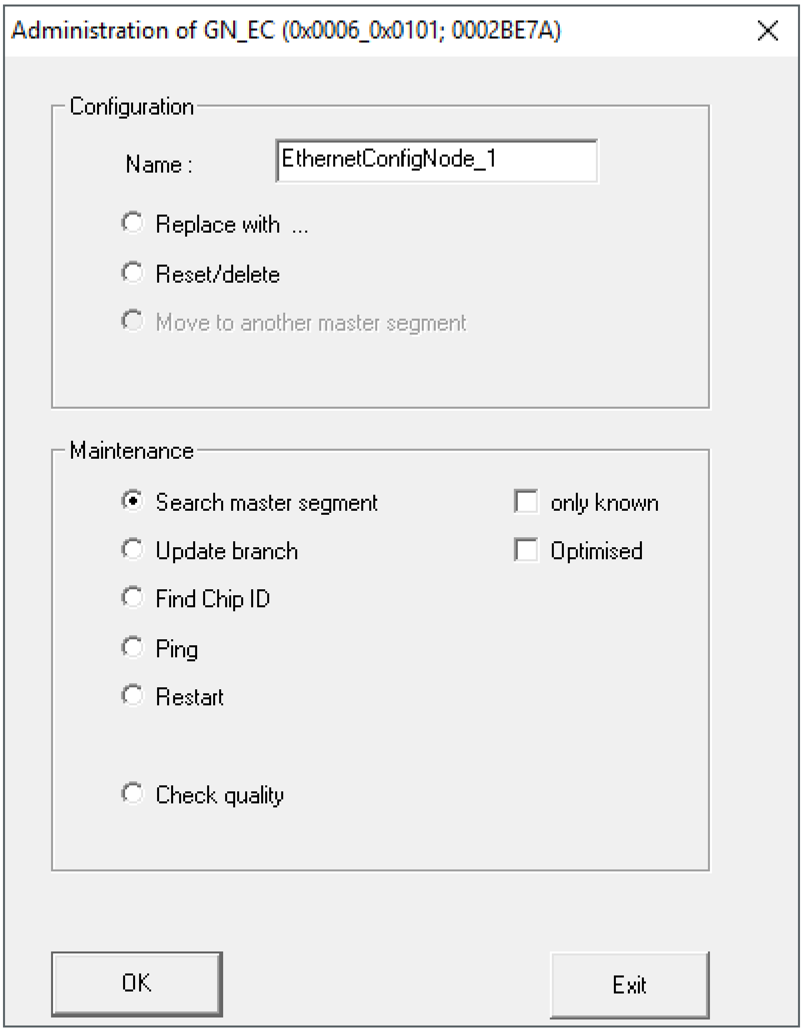
✓ All GatewayNodes powered and mounted.

✓ RS-485 configured (see *RS-485 ConfigNode [▸ 78]*)

✓ SmartIntego Manager opened.

1. Right-click the ConfigNode entry.

   ↳ The window "Administration" opens.



Administration of GN_EC (0x0006_0x0101; 0002BE7A)

Configuration

Name : EthernetConfigNode_1

○ Replace with ...

○ Reset/delete

○ Move to another master segment

Maintenance

● Search master segment □ only known

○ Update branch □ Optimised

○ Find Chip ID

○ Ping

○ Restart

○ Check quality

2. Select the option ◉ Search master segment.
3. Click on the button OK.

   ↳ Window "Administration" closes.

   ↳ SmartIntego Manager searches master segment.

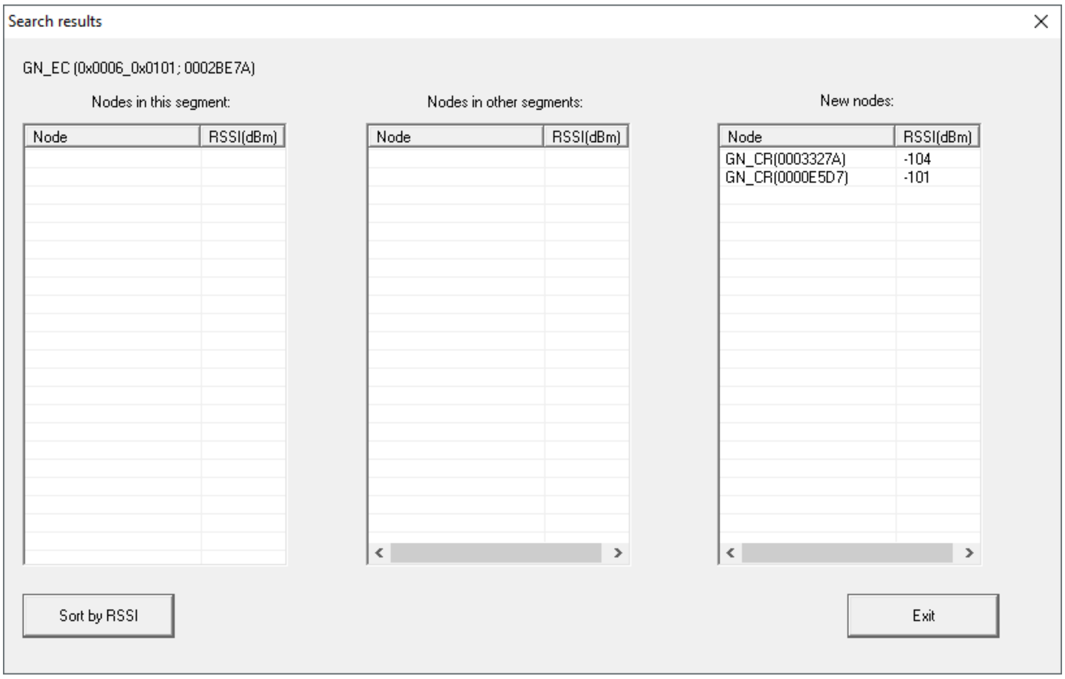
   ↳ The window "Search results" opens.

   Column "Nodes in this segment" → GatewayNodes assigned to the current ConfigNode

   in the column "Nodes in other segments" → GatewayNodes assigned to other ConfigNodes in

   the column "New Nodes" → GatewayNodes assigned without assigning

RSSI value of all columns refers to the connection from the current ConfigNode to the GatewayNodes. Values > -100 dBm are normal for wired components.


Search results

GN_EC (0x0006_0x0101; 0002BE7A)

Nodes in this segment:

Node	RSSI(dBm)

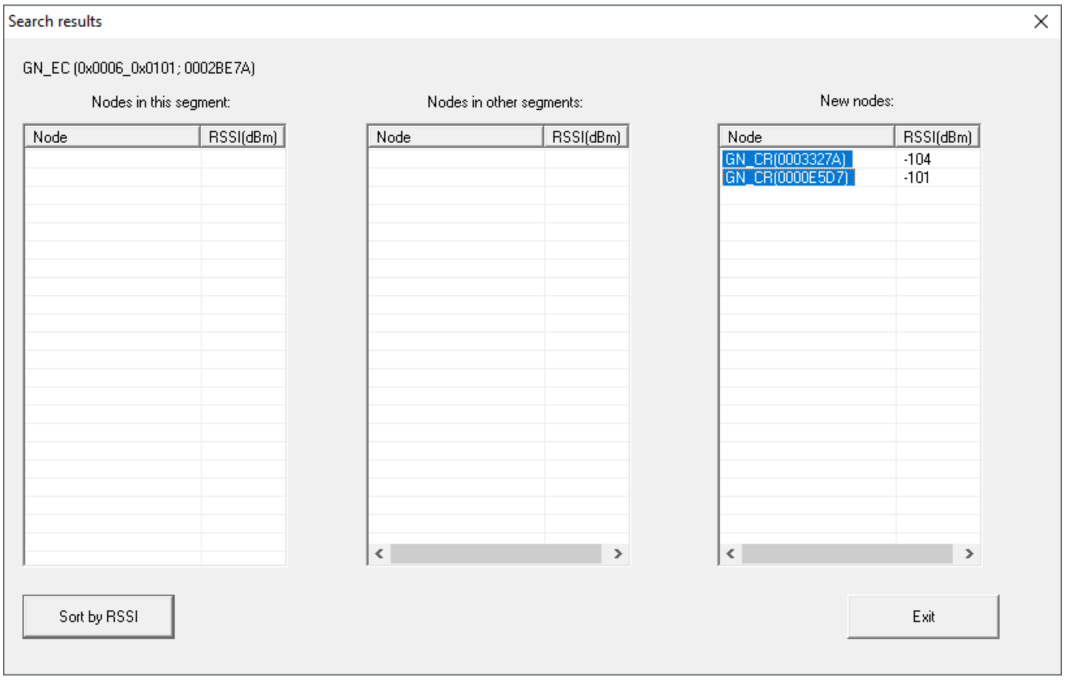
Nodes in other segments:

Node	RSSI(dBm)

New nodes:

Node	RSSI(dBm)
GN_CR(0003327A)	-104
GN_CR(0000E5D7)	-101

4. Select the new GatewayNodes you want to add to the current segment (Ctrl+ Mouse selection).


Search results

GN_EC (0x0006_0x0101; 0002BE7A)

Nodes in this segment:

Node	RSSI(dBm)

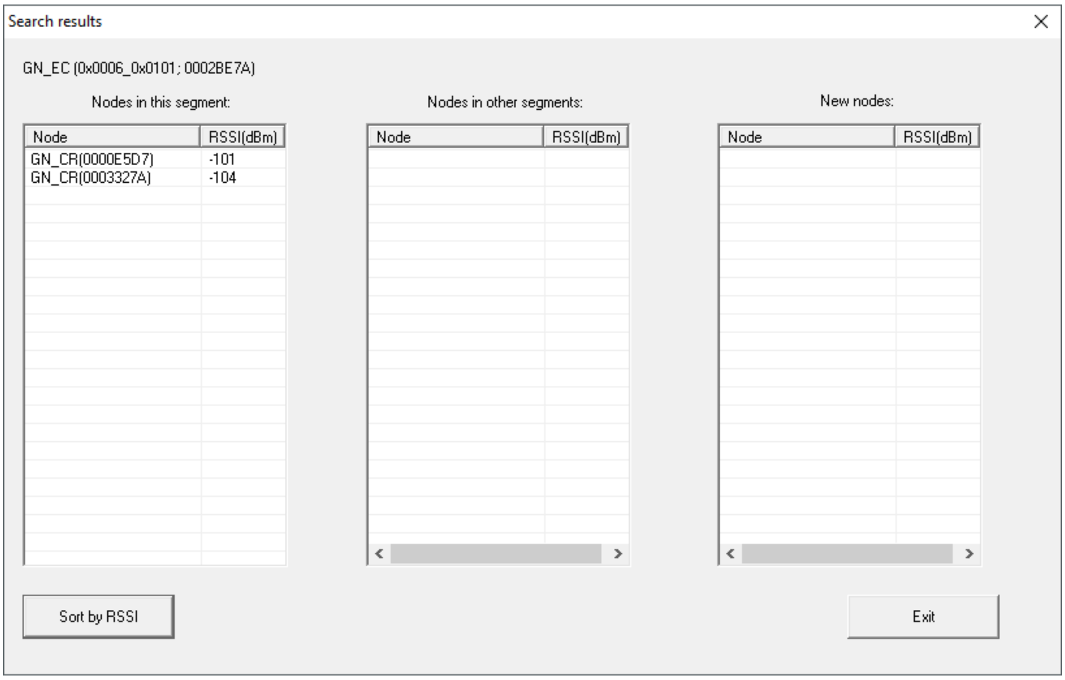
Nodes in other segments:

Node	RSSI(dBm)

New nodes:

Node	RSSI(dBm)
GN_CR(0003327A)	-104
GN_CR(0000E5D7)	-101

5. Drag and drop the GatewayNodes into the Nodes in this segment column.



GN_EC (0x0006_0x0101; 0002BE7A)

Nodes in this segment:

Node	RSSI(dBm)
GN_CR(0000E5D7)	-101
GN_CR(0003327A)	-104

Nodes in other segments:

Node	RSSI(dBm)

New nodes:

Node	RSSI(dBm)

6. Click on the Exit button.
   - ↳ Window "Search results" closes.
7. Right-click the entry of the new GatewayNode.

NOTE

Name assignment by name list

If you are using a name list (*Creating, expanding and importing a name list [▸ 29]* see), you no longer need to name the GatewayNodes.

- ↳ The window "Administration" opens.

8. Specify the name of your GatewayNode.
9. Click on the button OK.
   - ↳ Window "Administration" closes.
10. Click on the button Save.
    - ↳ SmartIntego Manager contacts the GatewayNode.
    - ↳ SmartIntego Manager assigns GatewayNode device address.
    - ↳ SmartIntego Manager saves routing table in the GatewayNode.
11. If necessary, repeat the designation for the other GatewayNodes.
12. If necessary, add further locking devices to the new segment.
13. Click on the button Save.
    - ↳ SmartIntego Manager contacts the GatewayNode.
    - ↳ SmartIntego Manager assigns GatewayNode device address.
    - ↳ SmartIntego Manager saves routing table in the GatewayNode.

14. Click on the button Save.

NOTE

Data loss due to improper termination

The data is not transferred to the SmartIntego tool (WO) until the SmartIntego Manager is properly ended. After saving, the files are permanently saved in the * ikp file in the SmartIntego tool (WO).

1. Click on the Save button.
2. Close SmartIntego Manager correctly using the button Exit.

5.15 Add LockNodes

NOTE

Electronics for SI Digital Cylinder AX with reader on both sides

In the version with a reader on both sides, the SI Digital Cylinder AX is equipped with an electronic reader thumb-turn on the outside and an electronic reader thumb-turn on the inside. Both thumb-turns are independent of each other.

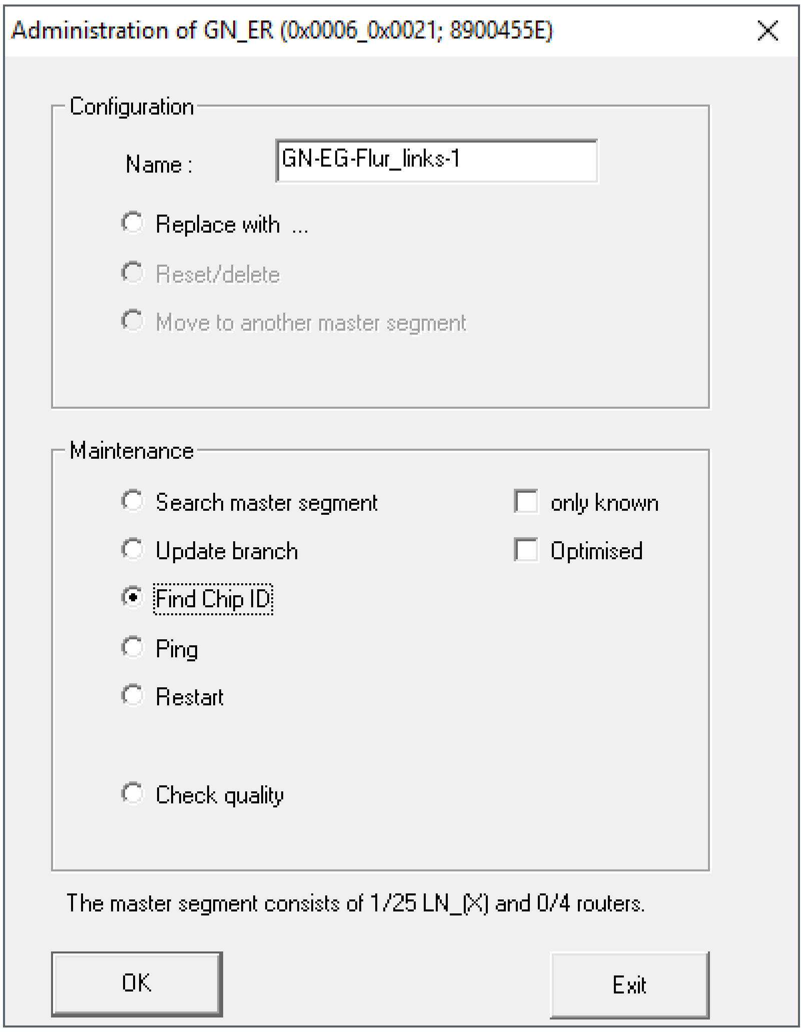
1. Create and configure the two electronic reader thumb-turns separately.
2. Program the two electronic reader thumb-turns separately.

5.15.1 Add individual LockNodes

✓ LockNode reachable from at least one GatewayNode.

✓ SmartIntego Manager opened.

1. Right-click on the GatewayNode with which you want to search for the LockNode.
   ↳ The window "Administration" opens.



Administration of GN_ER (0x0006_0x0021; 8900455E)

Configuration

Name : GN-EG-Flur_links-1

○ Replace with ...

○ Reset/delete

○ Move to another master segment

Maintenance

○ Search master segment □ only known

○ Update branch □ Optimised

● Find Chip ID

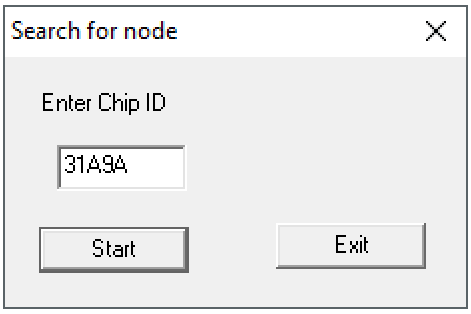
○ Ping

○ Restart

○ Check quality

The master segment consists of 1/25 LN_(X) and 0/4 routers.

2. Select the option ● Find Chip ID.
3. Click on the button OK.
   - ↳ Window "Administration" closes.
   - ↳ The window "Search for node" opens.

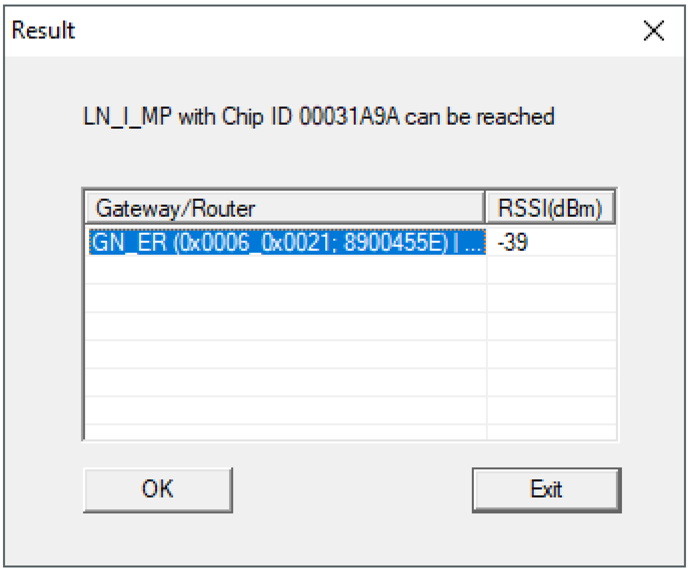


Search for node

Enter Chip ID

31A9A

4. Enter the chip ID without leading zeros (see LockNode, LockNode packaging or supplied sticker).
5. Click on the Start button.
   - ↳ Window "Search for node" closes.
   - ↳ Reset is being performed.
   - ↳ The window "Results" opens.



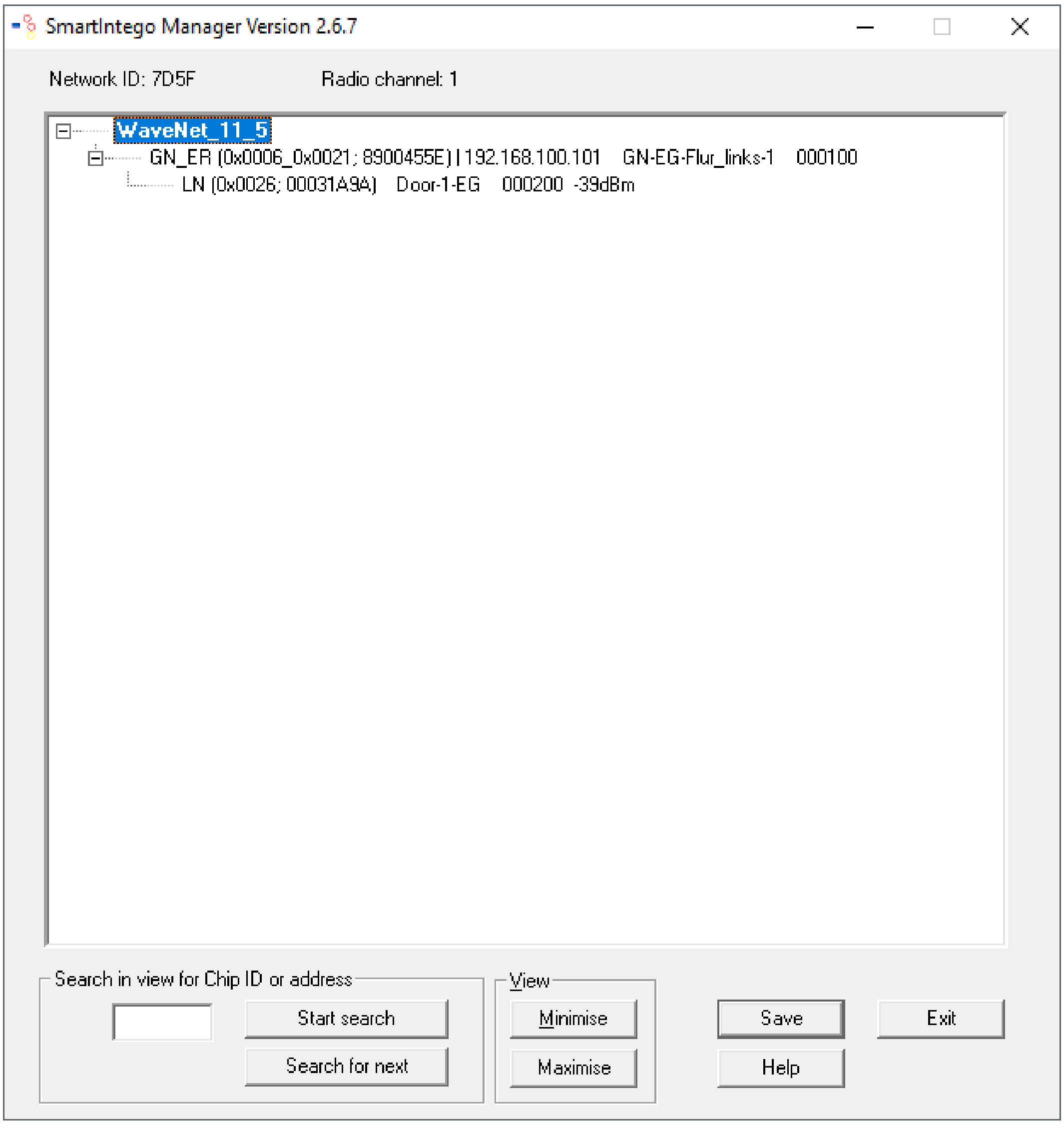
LN_I_MP with Chip ID 00031A9A can be reached

Gateway/Router	RSSI(dBm)
GN_ER (0x0006_0x0021; 8900455E) I ...	-39

6. Select the entry of the GatewayNode.
7. Click on the button OK.
   ↳ Window "Results" closes.
8. Right-click the entry of the new LockNode.
   ↳ The window "Administration" opens.
9. Enter a name (alternative: list of names for updating the names, see)*Creating, expanding and importing a name list [▸ 29]*.
10. Click on the button OK.
    ↳ Window "Administration" closes.

↳ LockNode is added.

View after import



SmartIntego Manager Version 2.6.7

Network ID: 7D5F   Radio channel: 1

```
WaveNet_11_5
  GN_ER (0x0006_0x0021; 8900455E) | 192.168.100.101   GN-EG-Flur_links-1   000100
    LN (0x0026; 00031A9A)   Door-1-EG   000200  -39dBm
```

SmartIntego Manager shows you the following information for the locking device:

- WaveNet address
- Chip ID
- Name
- Device Address
- Last RSSI value measured by SmartIntego Manager in dBm

Import to SmartIntego Tool (WO)

1. Click on the button Save.
2. Click on the Exit button.

↳ Transfer and save values in SmartIntego tool (WO).

NOTE

Data loss due to improper termination

The data is not transferred to the SmartIntego tool (WO) until the SmartIntego Manager is properly ended. After saving, the files are permanently saved in the * ikp file in the SmartIntego tool (WO).

1. Click on the Save button.
2. Close SmartIntego Manager correctly using the button Exit .

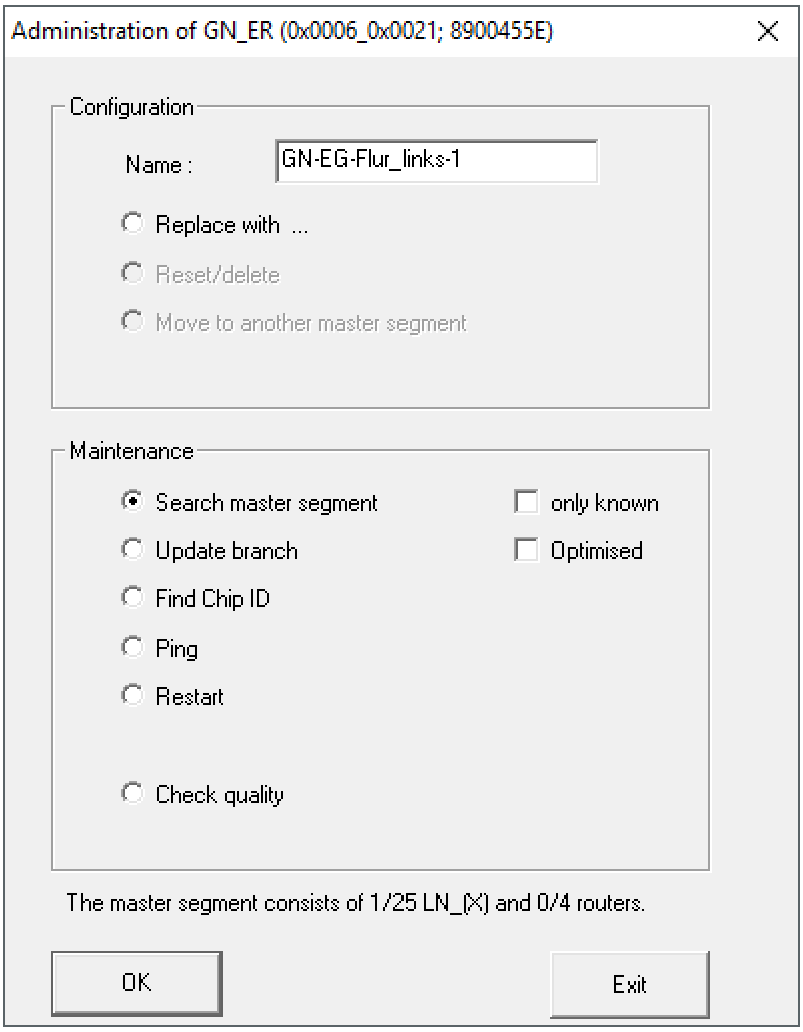
5.15.2 Add multiple LockNodes (Manual)

Finding LockNodes

✓ LockNodes accessible from at least one GatewayNode.

✓ SmartIntego Manager opened.

1. Right-click on the GatewayNode with which you want to search for the LockNodes.
   ↳ The window "Administration" opens.



Administration of GN_ER (0x0006_0x0021; 8900455E)

Configuration

Name : GN-EG-Flur_links-1

○ Replace with ...

○ Reset/delete

○ Move to another master segment

Maintenance

● Search master segment

○ Update branch

○ Find Chip ID

○ Ping

○ Restart

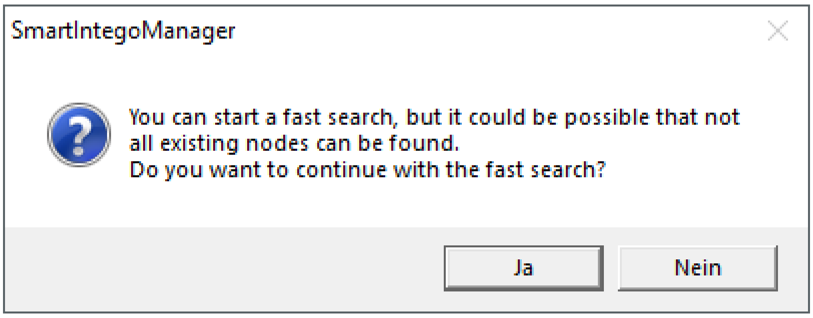
○ Check quality

□ only known

□ Optimised

The master segment consists of 1/25 LN_(X) and 0/4 routers.

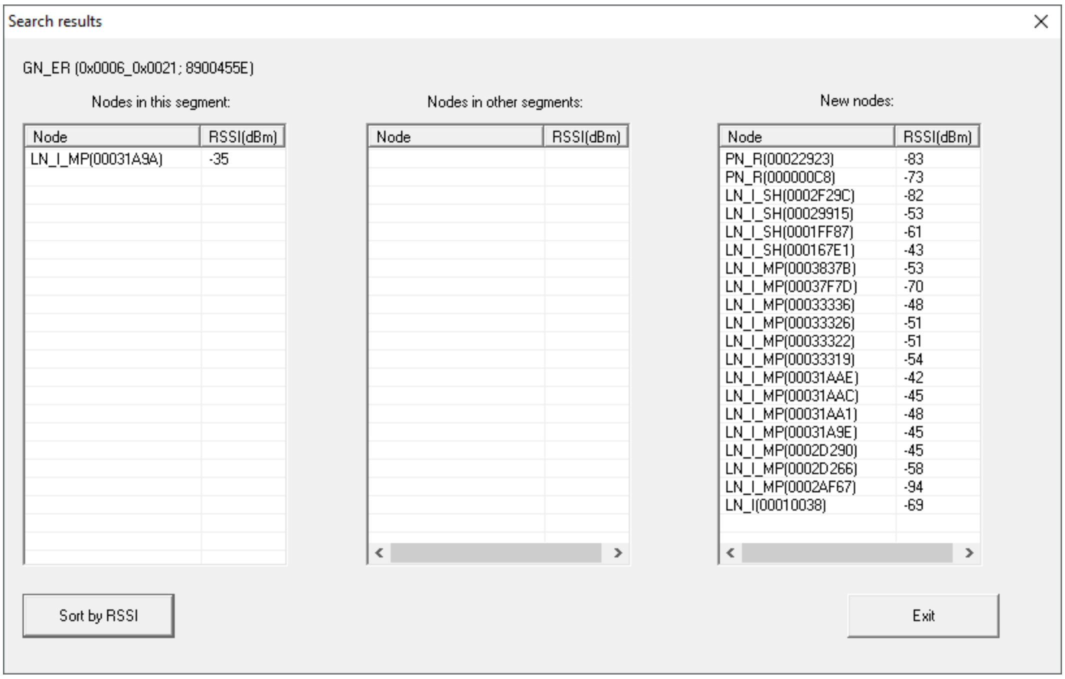
2. Select the option ◉ Search master segment.
3. Click on the button OK .
   ↳ Window "Administration" closes.
   ↳ The window for selecting between quick and intensive search opens.


SmartIntegoManager

You can start a fast search, but it could be possible that not all existing nodes can be found.
Do you want to continue with the fast search?

4. Click on the button Yes to perform a quick search or click on the button No to perform an intensive search.
   ↳ Searching for new and known LockNodes. (Known LockNodes are already assigned to other segments.)
   ↳ The window "Search results" opens.

Display of search results


Search results

GN_ER (0x0006_0x0021; 8900455E)

Nodes in this segment:

Node	RSSI(dBm)
LN_I_MP(00031A9A)	-35

Nodes in other segments:

Node	RSSI(dBm)

New nodes:

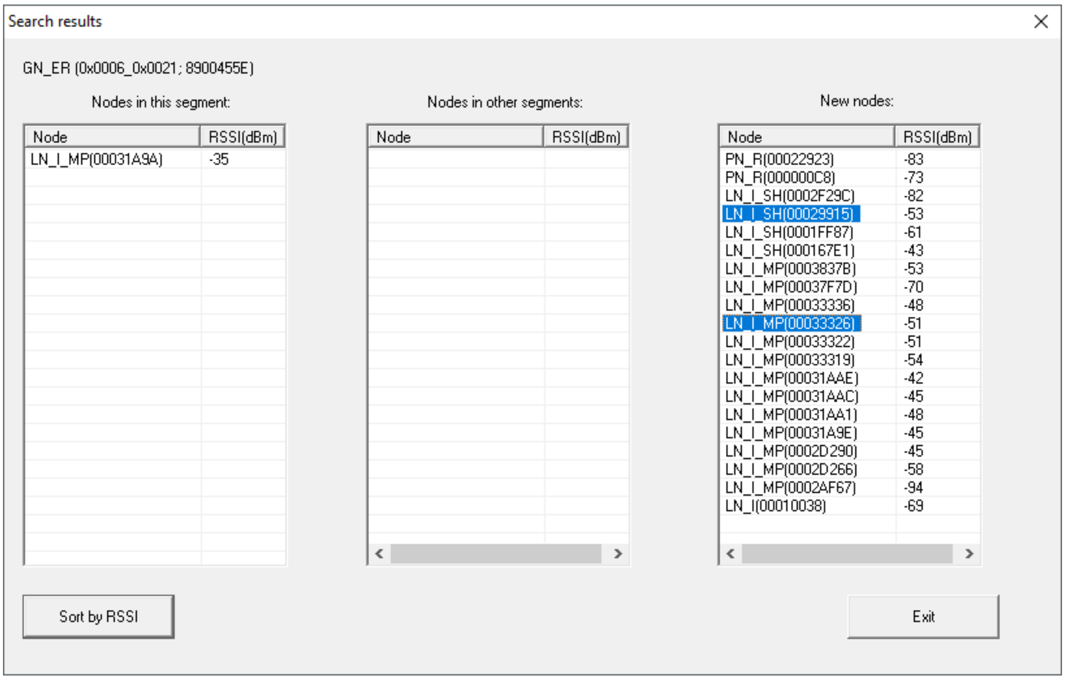
Node	RSSI(dBm)
PN_R(00022923)	-83
PN_R(000000C8)	-73
LN_I_SH(0002F29C)	-82
LN_I_SH(00029915)	-53
LN_I_SH(0001FF87)	-61
LN_I_SH(000167E1)	-43
LN_I_MP(0003837B)	-53
LN_I_MP(00037F7D)	-70
LN_I_MP(00033336)	-48
LN_I_MP(00033326)	-51
LN_I_MP(00033322)	-51
LN_I_MP(00033319)	-54
LN_I_MP(00031AAE)	-42
LN_I_MP(00031AAC)	-45
LN_I_MP(00031AA1)	-48
LN_I_MP(00031A9E)	-45
LN_I_MP(0002D290)	-45
LN_I_MP(0002D266)	-58
LN_I_MP(0002AF67)	-94
LN_I(00010038)	-69

Column	Meaning
Nodes in this segment	These LockNodes are assigned to the current GatewayNode.
Nodes in other segments	These LockNodes are assigned to another GatewayNode in this WaveNet.

Column	Meaning
New nodes	These LockNodes are not yet assigned to a GatewayNode.
RSSI value	The value displayed refers to the connection quality from the current GatewayNode to the respective LockNodes.

Add LockNodes

1. Mark the new LockNodes that you want to add (Ctrl + selection with the mouse).
   ↳ LockNodes are selected.



GN_ER (0x0006_0x0021; 8900455E)

Nodes in this segment:

Node	RSSI(dBm)
LN_I_MP(00031A9A)	-35

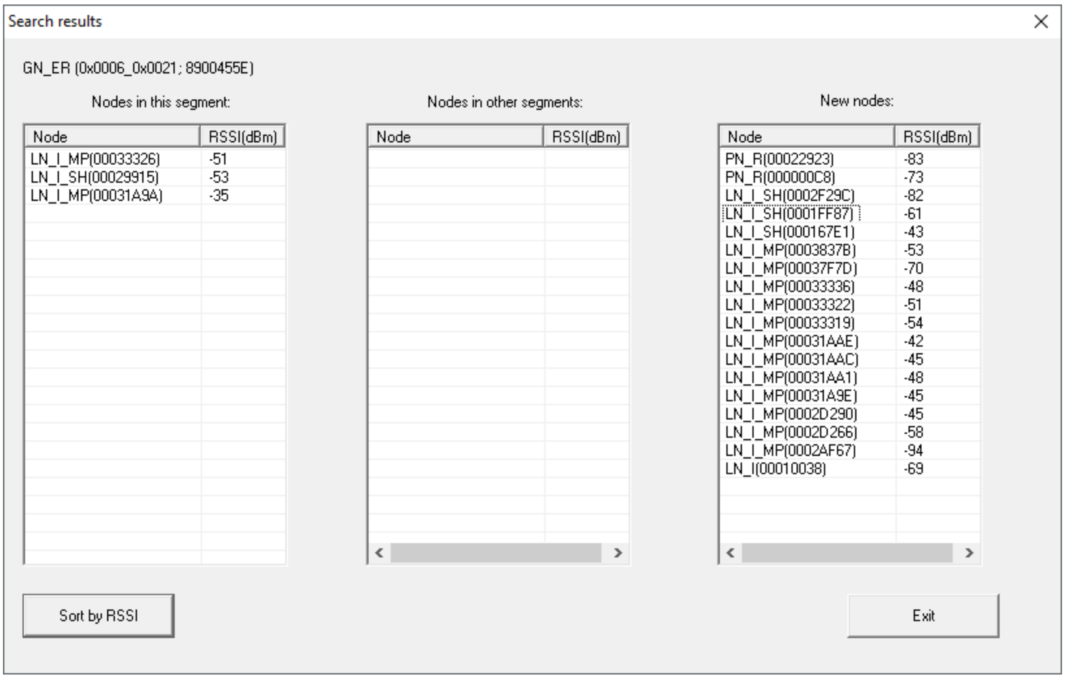
Nodes in other segments:

Node	RSSI(dBm)

New nodes:

Node	RSSI(dBm)
PN_R(00022923)	-83
PN_R(000000C8)	-73
LN_I_SH(0002F29C)	-82
LN_I_SH(00029915)	-53
LN_I_SH(0001FF87)	-61
LN_I_SH(000167E1)	-43
LN_I_MP(0003837B)	-53
LN_I_MP(00037F7D)	-70
LN_I_MP(00033336)	-48
LN_I_MP(00033326)	-51
LN_I_MP(00033322)	-51
LN_I_MP(00033319)	-54
LN_I_MP(00031AAE)	-42
LN_I_MP(00031AAC)	-45
LN_I_MP(00031AA1)	-48
LN_I_MP(00031A9E)	-45
LN_I_MP(0002D290)	-45
LN_I_MP(0002D266)	-58
LN_I_MP(0002AF67)	-94
LN_I(00010038)	-69

2. Drag the LockNodes to the "Nodes in this segment" column.
   ↳ LockNodes are located in the "Nodes in this segment" column.



Search results

GN_ER (0x0006_0x0021; 8900455E)

Nodes in this segment:

Node	RSSI(dBm)
LN_I_MP(00033326)	-51
LN_I_SH(00029915)	-53
LN_I_MP(00031A9A)	-35

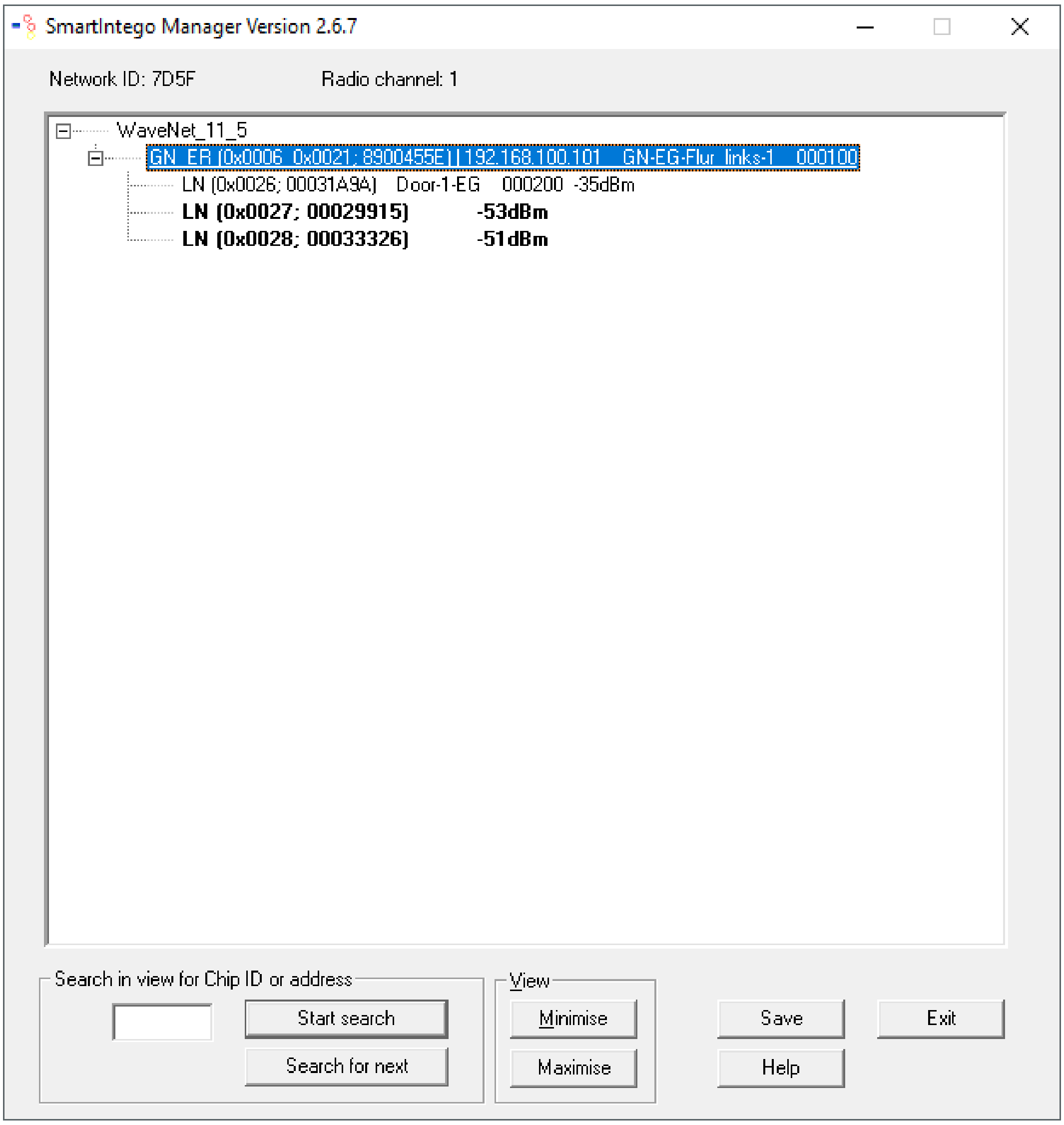
Nodes in other segments:

Node	RSSI(dBm)

New nodes:

Node	RSSI(dBm)
PN_R(00022923)	-83
PN_R(000000C8)	-73
LN_I_SH(0002F29C)	-82
LN_I_SH(0001FF87)	-61
LN_I_SH(000167E1)	-43
LN_I_MP(0003837B)	-53
LN_I_MP(00037F7D)	-70
LN_I_MP(00033336)	-48
LN_I_MP(00033322)	-51
LN_I_MP(00033319)	-54
LN_I_MP(00031AAE)	-42
LN_I_MP(00031AAC)	-45
LN_I_MP(00031AA1)	-48
LN_I_MP(00031A9E)	-45
LN_I_MP(0002D290)	-45
LN_I_MP(0002D266)	-58
LN_I_MP(0002AF67)	-94
LN_I(00010038)	-69

3. Click on the Exit button.
   - ↳ Window "Search results" closes.
   - ↳ LockNodes are displayed in SmartIntego Manager.


SmartIntego Manager Version 2.6.7
Search in view for Chip ID or address
Start search
Search for next
View
Minimise
Maximise
Save
Help
Exit

```
Network ID: 7D5F          Radio channel: 1

WaveNet_11_5
  GN ER (0x0006 0x0021; 8900455E)||192.168.100.101   GN-EG-Flur links-1   000100
    LN (0x0026; 00031A9A)   Door-1-EG   000200  -35dBm
    LN (0x0027; 00029915)          -53dBm
    LN (0x0028; 00033326)          -51dBm
```

4. Enter a name (alternative: list of names for updating the names, see) *Creating, expanding and importing a name list [▸ 29]*.

↳ LockNodes are added.

View after import

SmartIntego Manager shows you the following information for the locking device:

- WaveNet address
- Chip ID
- Name
- Device Address
- Last RSSI value measured by SmartIntego Manager in dBm

Import to SmartIntego Tool (WO)

1. Click on the button Save.

2. Click on the Exit button.

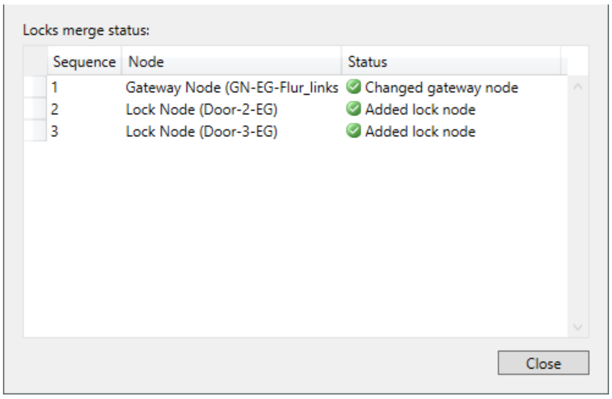
↳ Transfer and save values in SmartIntego tool (WO).

NOTE

Data loss due to improper termination

The data is not transferred to the SmartIntego tool (WO) until the SmartIntego Manager is properly ended. After saving, the files are permanently saved in the * ikp file in the SmartIntego tool (WO).

1. Click on the Save button.
2. Close SmartIntego Manager correctly using the button Exit.

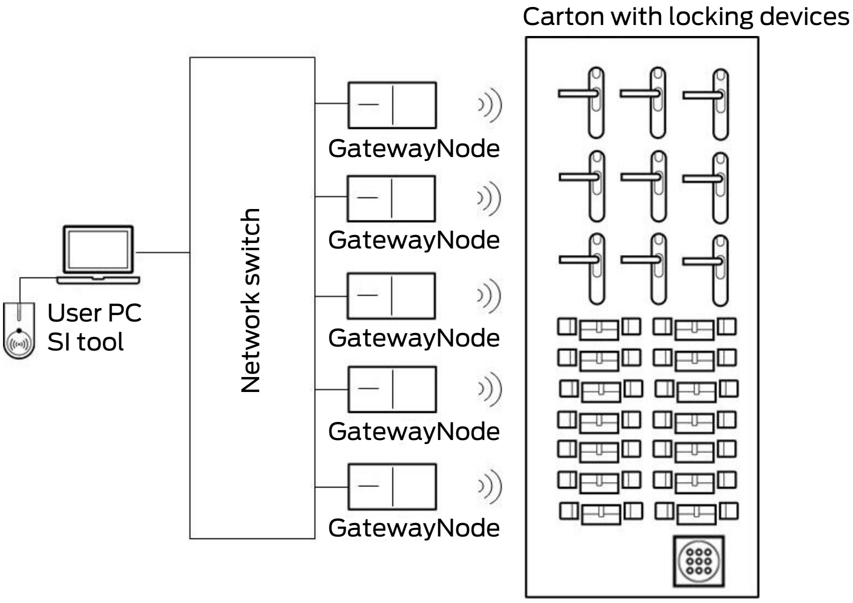


Locks merge status:

Sequence	Node	Status
1	Gateway Node (GN-EG-Flur_links	✓ Changed gateway node
2	Lock Node (Door-2-EG)	✓ Added lock node
3	Lock Node (Door-3-EG)	✓ Added lock node

5.15.3 Add multiple LockNodes (Automatic)

You do not have to remove the locking devices from the boxes. This setup can be carried out by the installer.



Hardware required:

- QR scanner with DataMatrix support (for name list creation)

- Network switch (ideally with PoE) to connect multiple GatewayNodes
- Separate network setup from other IT networks

NOTE

Procedure does not replace assignment to GatewayNodes

This procedure is only used to assign and programme LockNodes in locking devices to the system as quickly and efficiently as possible. The assignment takes place later (see *Automatically assign LockNodes [▸ 123]*).

NOTE

Not suitable for RS-485 systems

This procedure is not suitable for RS-485 systems.

NOTE

Limitation to LockNodes for the project with name list

Using the name list is optional. Without a name list, however, all LockNodes within reach are added to the system. This also applies to LockNodes which are to be used in other projects (and which for example are stored in the same warehouse at the installer).

- Use the name list.

✓ TCP configuration completed, ideally with the final IP address association (see *Configuring GatewayNodes (TCP) [▸ 54]*).

✓ Locking devices labelled and scanned (see *Creating, expanding and importing a name list [▸ 29]*).

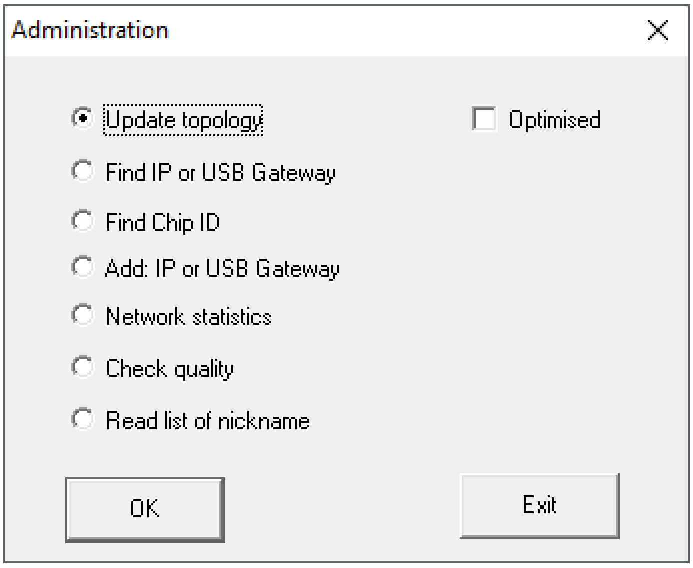
✓ Name list created (see *Creating, expanding and importing a name list [▸ 29]*).

✓ Locking devices with LockNodes can be accessed via connected GatewayNodes.

✓ SmartIntego Manager opened.

1. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.
2. Select the option ◉ Read list of nicknames.
3. Click on the button OK.
   ↳ Window "Administration" closes.
4. Select the name list.

5. Import the name list.
   - ↳ All chip IDs in SmartIntego Manager are checked and updated with the assigned name from the name list.
   - ↳ Name list remains loaded in the background during the entire session. All newly found GatewayNodes and LockNodes are automatically named.
6. Right-click on the navigation root (WaveNet_XX_X).
   - ↳ The window "Administration" opens.



Administration

● Update topology

○ Find IP or USB Gateway

○ Find Chip ID

○ Add: IP or USB Gateway

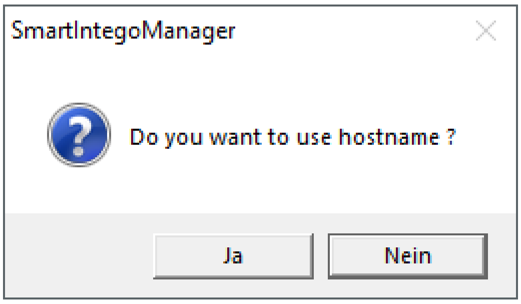
○ Network statistics

○ Check quality

○ Read list of nickname

□ Optimised

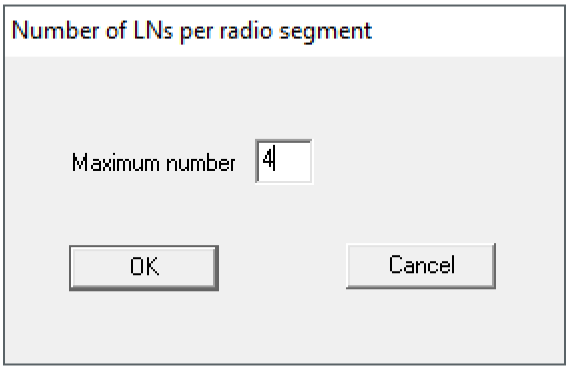
7. Select the option ● Update topology.
8. Click on the button OK.
   - ↳ Window "Administration" closes.
   - ↳ Query opens for host names.



SmartIntegoManager

Do you want to use hostname ?

9. Reject the use of host names (whenever possible, always work with the IP address to reduce dependency on DNS servers).
   - ↳ Query for host name closes.
   - ↳ The window for specifying the maximum number of LockNodes per GatewayNode opens.



Number of LNs per radio segment

Maximum number 4

10. Specify the maximum number of LockNodes per GatewayNode.

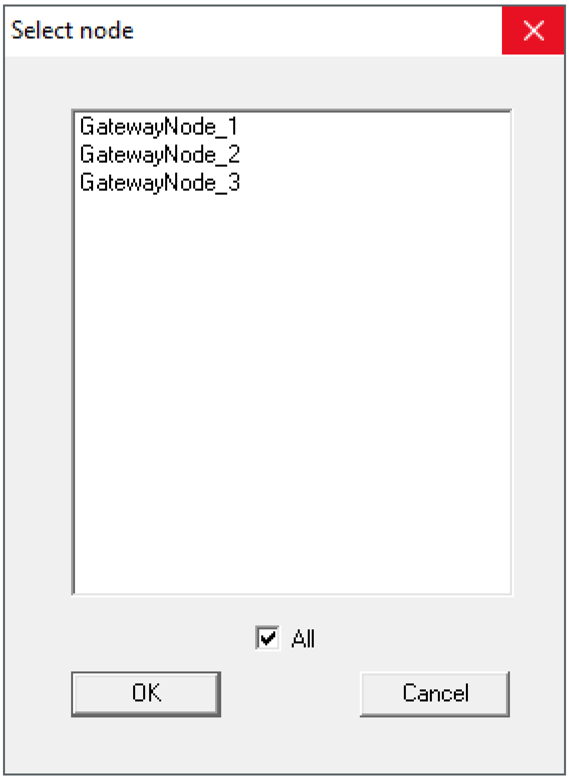
NOTE

Information on specifying the maximum number of LockNodes per gateway

The number of LockNodes supported can be limited by the integrator system. This particularly applies to integrator systems with hardware controllers (limitation of the number of locking devices per controller).

1. In this step, specify 50% of the maximum locking devices supported by the integrator system.
   - ↳ This leaves capacities free for later moving the LockNodes to the GatewayNodes.
2. In this example, the integrator system supports eight LockNodes per GatewayNode. Therefore, the number is limited to four LockNodes per GatewayNode.

11. Click on the button OK .
   - ↳ Window for specifying the maximum number of LockNodes per GatewayNode closes.
   - ↳ The window "Select node" opens.


Select node

GatewayNode_1
GatewayNode_2
GatewayNode_3

☑ All

12. Select all connected GatewayNodes.

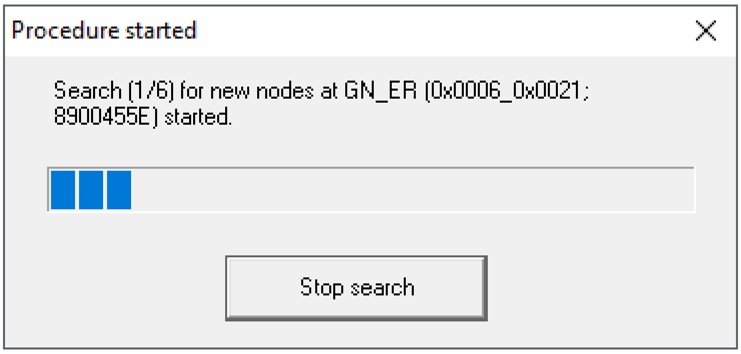
NOTE

Multiple Pass Allocation

Sometimes it is not possible to connect all GatewayNodes at the same time. However, the assignment should take place at all GatewayNodes.

1. Stake out the previous GatewayNodes.
2. Instead, connect the unassigned GatewayNodes.
3. Select the connected GatewayNodes.
4. Repeat the run.
   ↳ Run again shows all GatewayNodes found.
5. Select only GatewayNodes that are not yet added or configured.

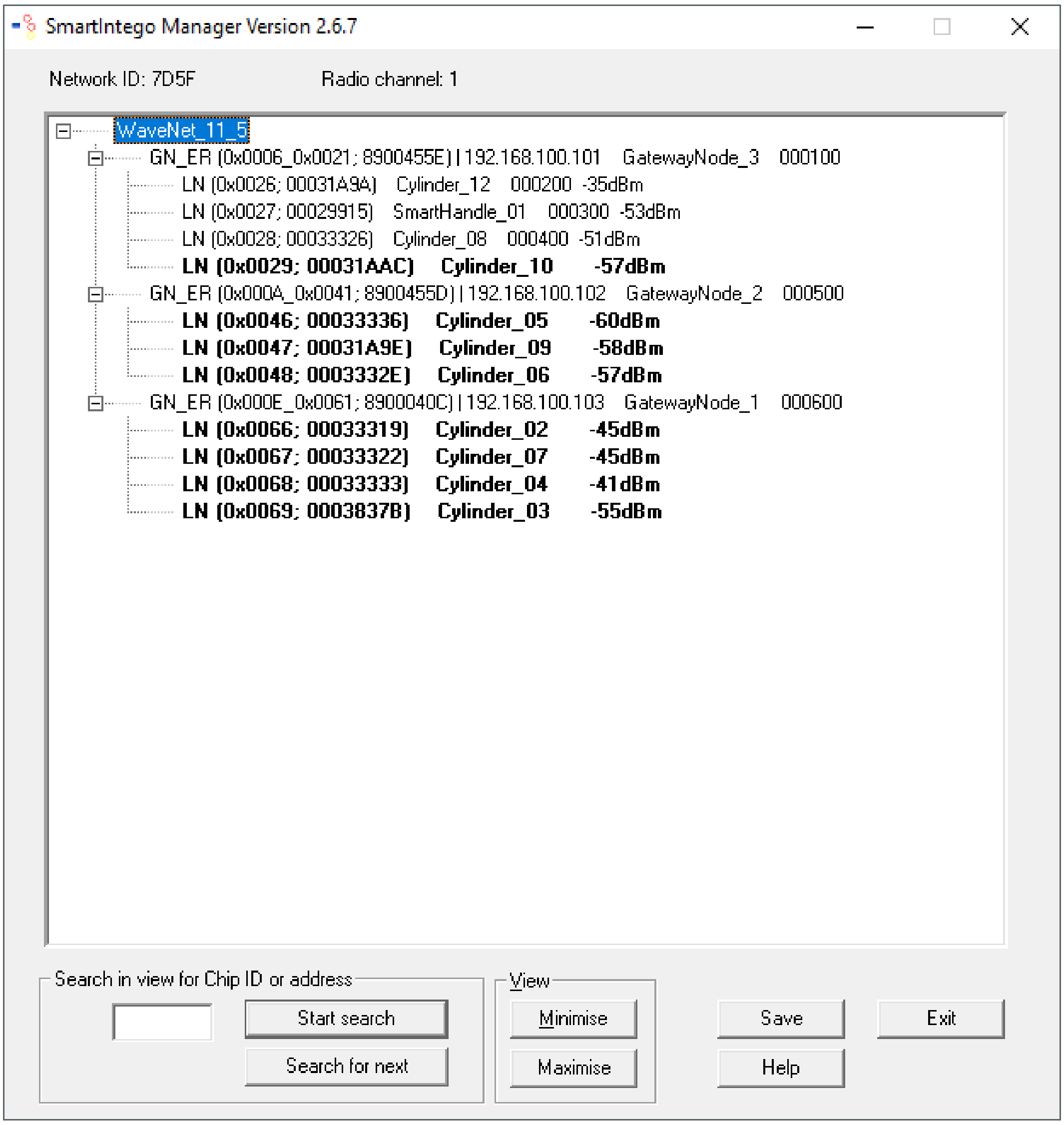
13. Click on the button OK.
    ↳ LockNodes are searched for and added using the name list (duration: approximately two minutes per GatewayNode).



Procedure started

Search (1/6) for new nodes at GN_ER (0x0006_0x0021; 8900455E) started.

↳ Added LockNodes are displayed in Smartntego Manager.



SmartIntego Manager Version 2.6.7

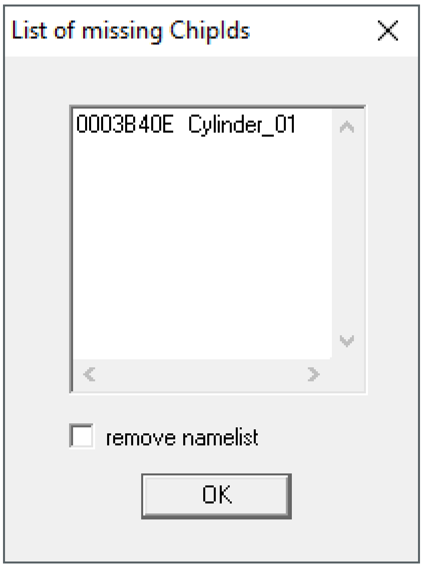
Network ID: 7D5F   Radio channel: 1

```
WaveNet_11_5
  GN_ER (0x0006_0x0021; 8900455E) | 192.168.100.101   GatewayNode_3   000100
    LN (0x0026; 00031A9A)   Cylinder_12   000200  -35dBm
    LN (0x0027; 00029915)   SmartHandle_01   000300  -53dBm
    LN (0x0028; 00033326)   Cylinder_08   000400  -51dBm
    LN (0x0029; 00031AAC)   Cylinder_10      -57dBm
  GN_ER (0x000A_0x0041; 8900455D) | 192.168.100.102   GatewayNode_2   000500
    LN (0x0046; 00033336)   Cylinder_05      -60dBm
    LN (0x0047; 00031A9E)   Cylinder_09      -58dBm
    LN (0x0048; 0003332E)   Cylinder_06      -57dBm
  GN_ER (0x000E_0x0061; 8900040C) | 192.168.100.103   GatewayNode_1   000600
    LN (0x0066; 00033319)   Cylinder_02      -45dBm
    LN (0x0067; 00033322)   Cylinder_07      -45dBm
    LN (0x0068; 00033333)   Cylinder_04      -41dBm
    LN (0x0069; 0003837B)   Cylinder_03      -55dBm
```

14. Click on the button Save.

Add unattached or unallocated LockNodes later

It is possible that LockNodes from the name list have not been reached or not assigned:



Manually add these LockNodes with one of the two options:

- Rerun: *Add multiple LockNodes (Automatic) [▸ 106]*
- Add individually: *Add individual LockNodes [▸ 97]*

In the example, the LockNodes was incorrectly in the name list for illustration purposes.

SmartIntego Manager shows you the following information for the locking device:

- WaveNet address
- Chip ID
- Name
- Device Address
- Last RSSI value measured by SmartIntego Manager in dBm

NOTE

Data loss due to improper termination

The data is not transferred to the SmartIntego tool (WO) until the SmartIntego Manager is properly ended. After saving, the files are permanently saved in the * ikp file in the SmartIntego tool (WO).

1. Click on the Save button.
2. Close SmartIntego Manager correctly using the button Exit.

5.16 Programme locking device

- You have successfully set up the infrastructure for locking devices with SmartIntego Manager.

- You have imported the data into the SmartIntego tool.
- Locking devices were automatically created by the import.

Then, program the locking devices.

Locking devices that have undergone changes, such as

- newly added locking devices or
- Locking devices with changed configuration

are selected with a yellow lightning symbol ⚡. This flash indicates that the locking device requires programming, but it has not yet been written to the locking device.

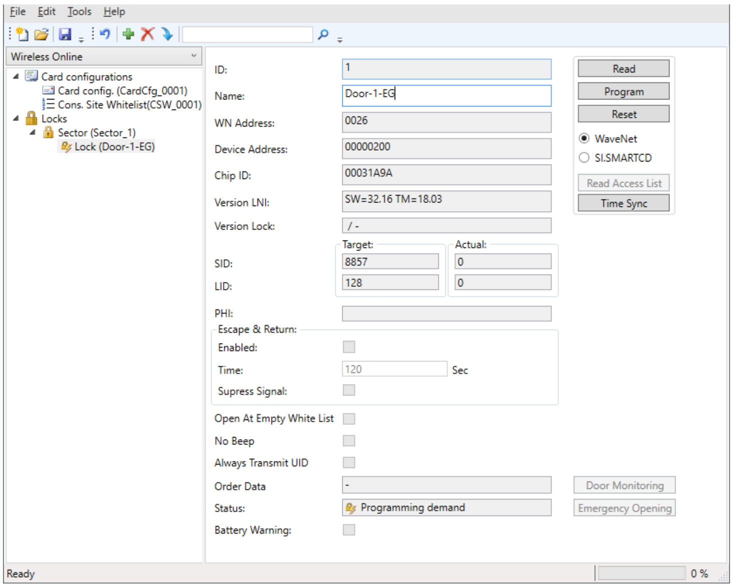
NOTE

Electronics for SI Digital Cylinder AX with reader on both sides

In the version with a reader on both sides, the SI Digital Cylinder AX is equipped with an electronic reader thumb-turn on the outside and an electronic reader thumb-turn on the inside. Both thumb-turns are independent of each other.

1. Create and configure the two electronic reader thumb-turns separately.
2. Program the two electronic reader thumb-turns separately.

5.16.1 Programme hybrid locking devices



ID: 1
Name: Door-1-EG
WN Address: 0026
Device Address: 00000200
Chip ID: 00031A9A
Version LNI: SW=32.16 TM=18.03
Version Lock: / -

	Target:	Actual:
SID:	8857	0
LID:	128	0

PHI:
Escape & Return:
Enabled: ☐
Time: 120 Sec
Supress Signal: ☐
Open At Empty White List ☐
No Beep ☐
Always Transmit UID ☐
Order Data -
Status: Programming demand
Battery Warning: ☐

● WaveNet
○ SI.SMARTCD

✓ SmartIntego-Tool (WO) opened.

✓ When programming the first locking device in the system: SI.SmartCD connected.

1. Select the locking device in the navigation area.

2. Click on the Program button.
   - ↳ Programming via WaveNet starts.
   - ↳ Duration of programming: 45 seconds (locking cylinder) or 80 seconds (SmartHandle).

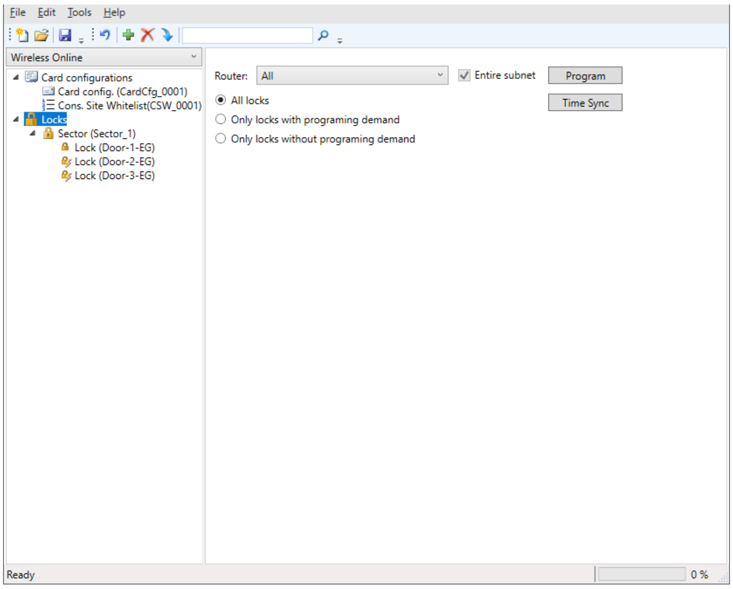
↳ Pthe locking device is programmed.

The SI.SmartCD cannot be used for initial programming, but must be connected.

5.16.2 Programme hybrid locking devices

Select the locking devices tab in the navigation area. You can configure programming tasks for the locking devices in the drop-down menu ▼ Router:

- "SI-Tool: Mehrere programmieren "Alle Schließungen" [offen]"
- "SI-Tool: Mehrere programmieren "Alle Schließungen an einem bestimmten Gateway/Router" [offen]"
- "SI-Tool: Mehrere programmieren "Schließungen mit Programmierbedarf" [offen]"
- "SI-Tool: Mehrere programmieren "Schließungen ohne Programmierbedarf" [offen]"



Router: All
☑ Entire subnet
● All locks
○ Only locks with programing demand
○ Only locks without programing demand

✓ SmartIntego-Tool (WO) opened.

✓ When programming the first locking device in the system: SI.SmartCD connected.

1. Select the locking devices tab in the navigation area.
2. Select which locking devices you want to programme from the drop-down menu ▼ Router.

3. Click on the Program button.
   - ↳ Programming via WaveNet starts.
   - ↳ Duration of programming: 45 seconds (locking cylinder) or 80 seconds (SmartHandle).
   - ↳ Locking devices are programmed in succession.

↳ Locking devices are programmed.

The SI.SmartCD cannot be used for initial programming, but must be connected.

Do not perform any major updates (e.g. major whitelist update) through the integrator system during programming.

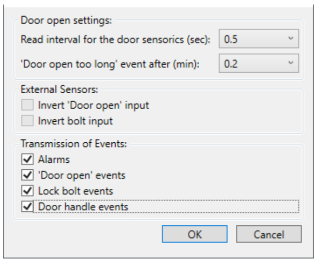
5.17 SmartHandle: Configure DoorMonitoring

- You have successfully set up the infrastructure for locking with SmartIntego Manager.
- You have imported the data into the SmartIntego tool.
- Locking devices were automatically created by the import.

The SmartIntego tool (WO) does not yet recognise the locking device as a DoorMonitoring locking device. Perform the detection using one of these methods:

- Read out the locking device (button Read).
- Programme the locking device (button Program).

The DoorMonitoring settings are then active.



Door open settings:

Read interval for the door sensorics (sec): 0.5

'Door open too long' event after (min): 0.2

External Sensors:

□ Invert 'Door open' input

□ Invert bolt input

Transmission of Events:

☑ Alarms

☑ 'Door open' events

☑ Lock bolt events

☑ Door handle events

1. Open the DoorMonitoring settings.
2. Set DoorMonitoring according to the integrator's specifications.
3. Click on the button OK.
4. Click on the Program button.

↳ DoorMonitoring is configured.

5.18 SmartHandle: Configure Escape&Return

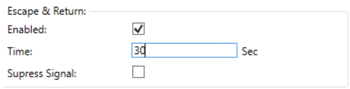
All SmartHandles with sensors or ER options also support the escape and return function.

- You have successfully set up the infrastructure for locking with SmartIntego Manager.
- You have imported the data into the SmartIntego tool.
- Locking devices were automatically created by the import.

The SmartIntego tool (WO) does not yet recognise the locking device as an escape-and-return locking device. Perform the detection using one of these methods:

- Read out the locking device (button Read).
- Programme the locking device (button Program).

Escape and return settings will then be active.



Escape & Return:
Enabled: ☑
Time: 30 Sec
Supress Signal: □

☑ SI-EscapeReturn: Enabled [offen]	Activates/deactivates the escape and return function.
SI-EscapeReturn: Time [offen]	Specifies the duration of engagement (30 s to 240 s). SmartHandle beeps continuously during this time.
□ SI-EscapeReturn: Suppress Signal [offen]	Disables beeping during engage time.

NOTE

Escape & Return: Legal situation

The Escape & Return Timeout can be between 30 s and 240 s. The use and configuration of Escape & Return may be subject to legal regulations (e.g. Norway).

- Inform yourself in advance about legal regulations.

Save the escape and return settings in the locking device by programming the locking device with the button Program.

The user can disengage the locking device manually (and thus cancel the escape and return function) by holding their card in front of the card reader of the locking device for two seconds.

5.19 Configure PIN code keypad

- ✓ Master PIN (see *Changing the master PIN [▸ 117]*).
- ✓ Pin length configured (see *Determining the PIN length [▸ 118]*).
- ✓ SmartIntego Manager opened.

1. Right-click on the navigation root (WaveNet_XX_X).
   - ↳ The window "Administration" opens.
2. Select one of the options: ◉ Find Chip ID, ◉ Search master segment or ◉ Update topology.
3. Click on the button OK.
   - ↳ Window "Administration" closes.
4. Follow the instructions to set up the PIN code keypad.

↳ PIN code keypad configured.

The PIN code keypad is a WaveNet component only. It therefore does not need to be programmed in the SmartIntego tool (WO).

5.19.1 Changing the master PIN

You only need to carry out this step if no new Master PIN has been programmed yet. You cannot start any configurations until you change the Master PIN. The Master PIN can be changed at any time. No programming is required to make a change. The Master PIN is unable to open any locks.

NOTE

Enter the numbers consecutively. The SmartIntego PIN code keypad only signals the pressing of the keys, but not completion of the individual steps in the process.

1. Enter 000 0 (SI firmware from 31.14.16.12: Press the first 0 approx. 2s → flashes 2x orange).
2. Enter the default or old Master PIN (default: 123 456 78).
   - ↳ SmartIntego PIN code keypad beeps and flashes green briefly twice.
3. Enter the new Master PIN.
   - ↳ The new Master PIN must consist of 8 digits and must not start with 0.
4. Enter the new Master PIN again.

↳ SmartIntego PIN code keypad beeps and flashes green briefly twice.

↳ The Master PIN has been successfully changed.

IMPORTANT

Master PIN loss

The Master PIN is an essential, integral part of the security concept. No more administrative changes can be made to the device if the Master PIN is lost.

1. Keep the Master PIN in a safe place.
2. Make the Master PIN visible for authorized persons at any time.

5.19.2 Determining the PIN length

The User PIN may be between 1 and 9 digits long; 8 digits is the standard configuration.

1. Enter 0 (SI firmware from 31.14.16.12: Press 0 approx. 2s → flashes 2x orange).
2. Enter the Master PIN.
   ↳ SmartIntego PIN code keypad beeps and flashes green briefly twice.
3. Enter the length of the User PIN – e.g. 4 for a 4-digit User PIN.

↳ SmartIntego PIN code keypad beeps and flashes green briefly twice.

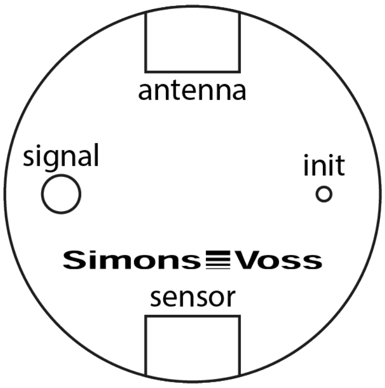
↳ The User PIN length has been successfully changed.

5.19.3 Programming

The SmartIntego PIN code keypad is programmed in the MobileKey web app (*https://app.my-mobilekey.com*) or for SmartIntego products in the SmartIntego manager and in the integrator system.

5.20 Configure Node IO

1. Connect the sensor cable (WN.LN.SENSOR.CABLE) to the SmartIntego Node IO (socket "Sensor").



2. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.

3. Select one of the options: ◉ Find Chip ID, ◉ Search master segment or ◉ Update topology.
4. Click on the button OK.
   ↳ Window "Administration" closes.
5. Follow the instructions to set up SmartIntego Node IO.

↳ SmartIntego Node IO configured.

SmartIntego Node IO is a WaveNet component only. It therefore does not need to be programmed in the SmartIntego tool (WO).

Please refer to the integrator documentation for the exact connection assignment of the sensor cable.

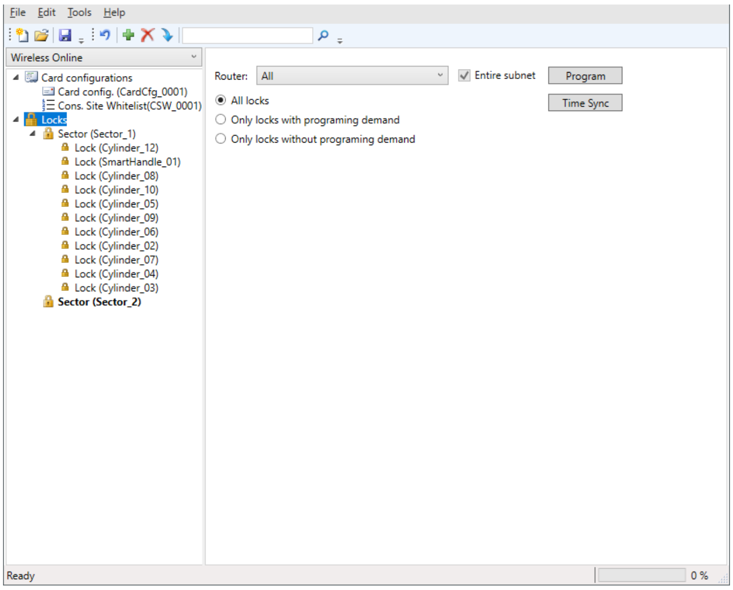
5.21 Managing locking devices in the SmartIntego tool (WO)

Managing many locking devices in the SmartIntego tool (WO) becomes easier if you group them into sectors. For example, you can combine all locking devices of a floor in a building into one sector.

Create sector

✓ SmartIntego-Tool (WO) opened.

1. In the navigation tree, mark the entry for the locking devices.
2. Click the green Plus icon ✚.
   ↳ Sector is created.



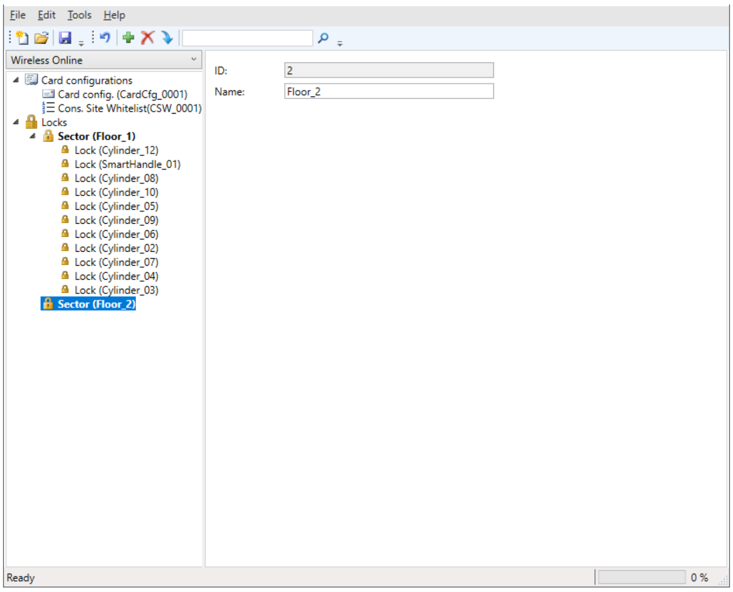
- Card configurations
  - Card config. (CardCfg_0001)
  - Cons. Site Whitelist(CSW_0001)
- Locks
  - Sector (Sector_1)
    - Lock (Cylinder_12)
    - Lock (SmartHandle_01)
    - Lock (Cylinder_08)
    - Lock (Cylinder_10)
    - Lock (Cylinder_05)
    - Lock (Cylinder_09)
    - Lock (Cylinder_06)
    - Lock (Cylinder_02)
    - Lock (Cylinder_07)
    - Lock (Cylinder_04)
    - Lock (Cylinder_03)
  - **Sector (Sector_2)**

Router: All ☑ Entire subnet

● All locks
○ Only locks with programing demand
○ Only locks without programing demand

3. Select the entry of the newly created sector.

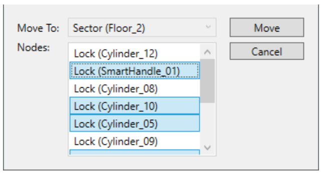
4. Give the sector a name in the settings.



ID: 2

Name: Floor_2

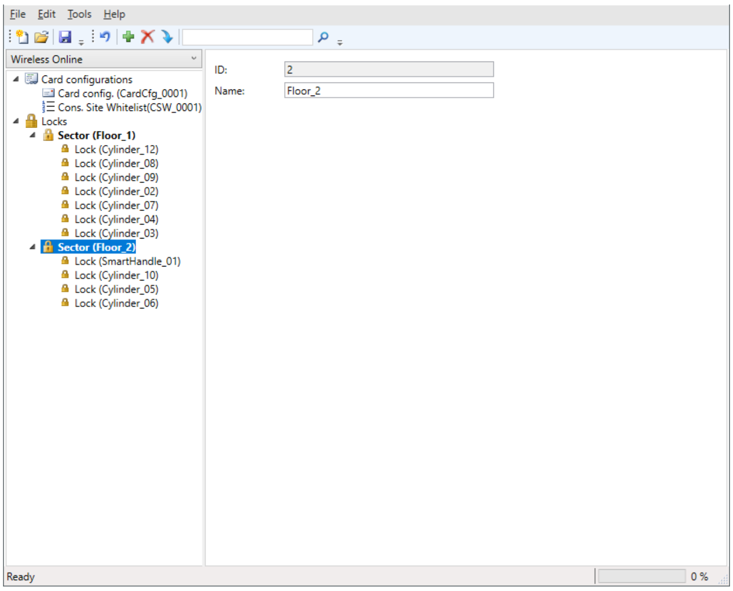
5. Drag and drop locking devices to the sector entry in the navigation tree.
   ↳ Programming window opens.



Move To: Sector (Floor_2)

Nodes:
Lock (Cylinder_12)
Lock (SmartHandle_01)
Lock (Cylinder_08)
Lock (Cylinder_10)
Lock (Cylinder_05)
Lock (Cylinder_09)

6. Click on the button Move
   ↳ The prompt closes.
   ↳ Locking devices are moved to the sector.



ID: 2

Name: Floor_2

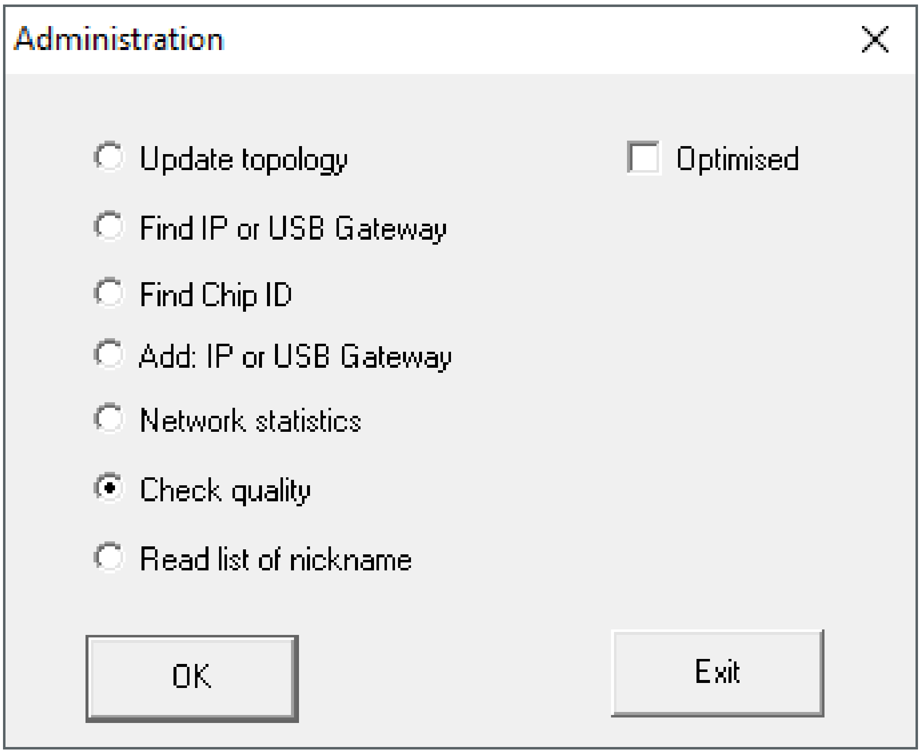
7. If necessary, drag further locking devices to the entry of the sector.

8. Click on the save button.

5.22 Check WaveNet

✓ SmartIntego Manager opened.

1. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.



Administration

○ Update topology

○ Find IP or USB Gateway

○ Find Chip ID

○ Add: IP or USB Gateway

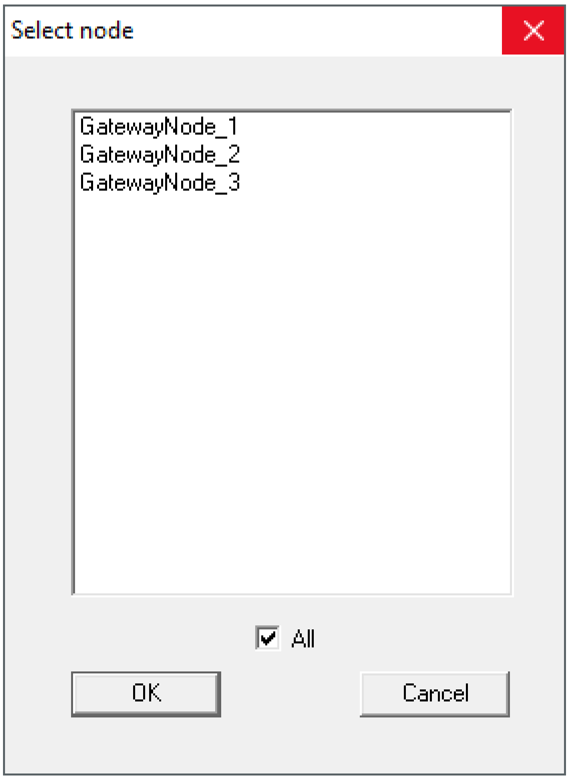
○ Network statistics

● Check quality

○ Read list of nickname

□ Optimised

2. Select the option ● Check quality.
3. Click on the button OK.
   ↳ Window "Administration" closes.
   ↳ The window "Select node" opens.



4. Highlight the GatewayNodes you want to check.
5. Click on the button OK.
   - ↳ Window "Select node" closes.
   - ↳ RSSI values are performed for each LockNode of the GatewayNodes.
   - ↳ Values in the SmartIntego Manager tree view are updated.
6. Click on the button Save.
7. Click on the Exit button.

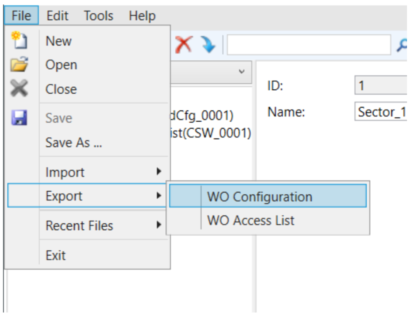
↳ Values are stored in the SmartIntego tool (WO).

Exporting measurement results

You can export the measurement results with the configuration file.

✓ SmartIntego-Tool (WO) opened.

1. Via | File | and Export open the entry SI-Tool: File, Export - WO Configuration [offen].



2. Export the configuration file.

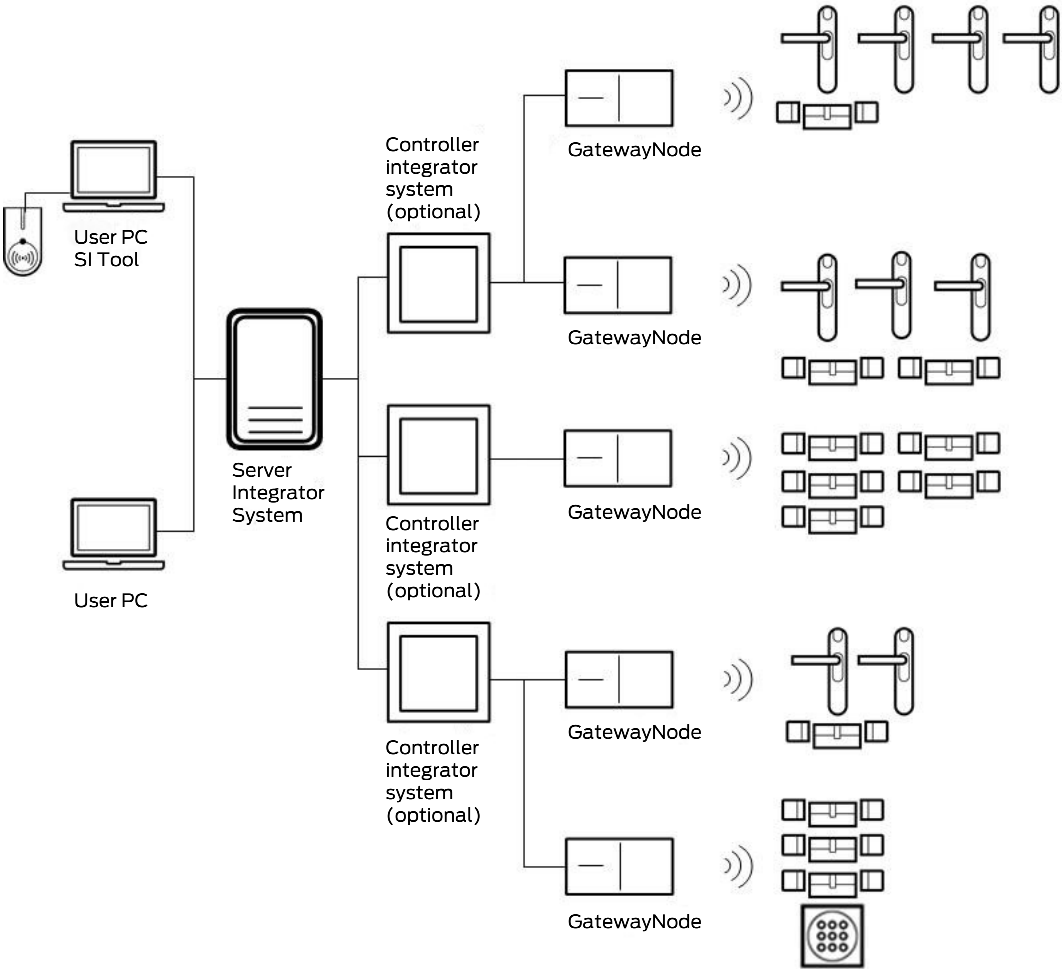
5.23 Automatically assign LockNodes

The assignment of LockNodes must be adapted in the following cases:

- Prepared commissioning at the observer (see *Add multiple LockNodes (Automatic) [▸ 106]*)
- structural changes in the property (change in radio characteristics)

To ensure the best possible reception, assign the GatewayNodes automatically.

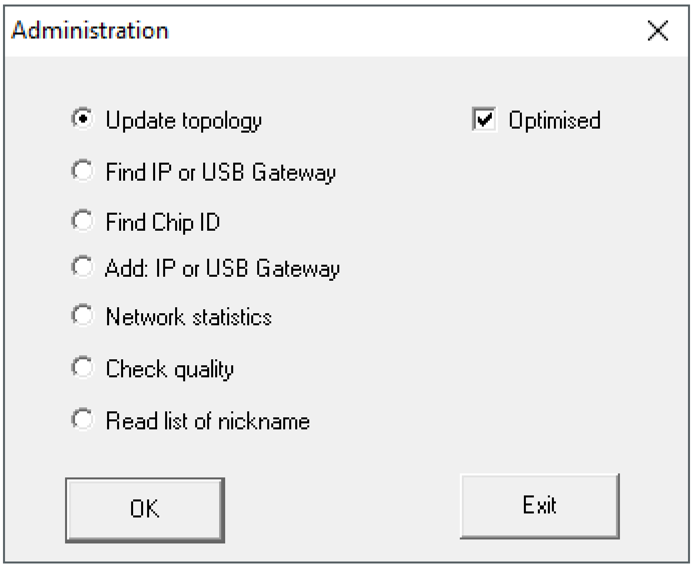
Create a whitelist beforehand (see *Create, modify and delete construction site whitelist [▸ 41]*) and store it on the locking devices.


Controller integrator system (optional)
GatewayNode
User PC
SI Tool
GatewayNode
Server Integrator System
GatewayNode
Controller integrator system (optional)
User PC
GatewayNode
Controller integrator system (optional)
GatewayNode

- ✓ Doors closed.
- ✓ No moving obstacles between the locking device and GatewayNodes.
- ✓ SmartIntego Manager opened.

1. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.
2. Select the option ◉ Read list of nicknames.

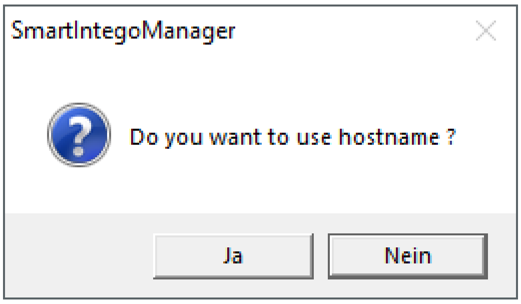
3. Click on the button OK.
   ↳ Window "Administration" closes.
4. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.


Administration

● Update topology
○ Find IP or USB Gateway
○ Find Chip ID
○ Add: IP or USB Gateway
○ Network statistics
○ Check quality
○ Read list of nickname

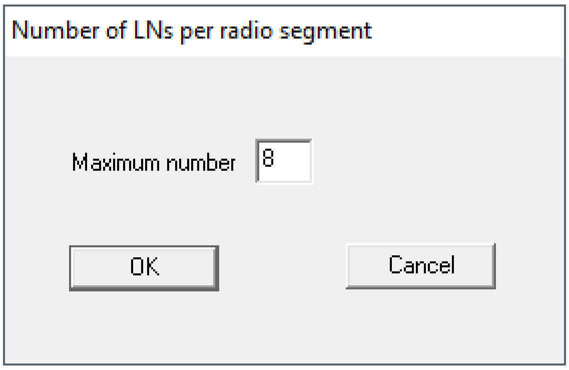
☑ Optimised

5. Select the option ● Update topology.
6. Activate the checkbox ☑ SI-Manager Update topology: Optimised [offen].
7. Click on the button OK.
   ↳ Window "Administration" closes.
   ↳ Query opens for host names.


SmartIntegoManager

Do you want to use hostname ?

8. Reject the use of host names (Wherever possible, always work with the IP address to reduce dependency on DNS servers).
   ↳ Query for host name closes.
   ↳ The window for specifying the maximum number of LockNodes per GatewayNode opens.



Number of LNs per radio segment

Maximum number 8

9. Specify the maximum number of LockNodes per GatewayNode.

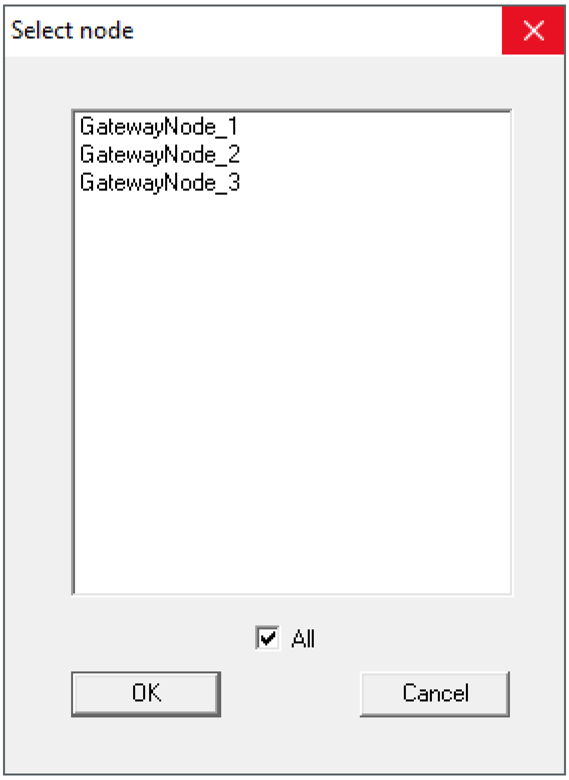
NOTE

Information on specifying the maximum number of LockNodes per gateway

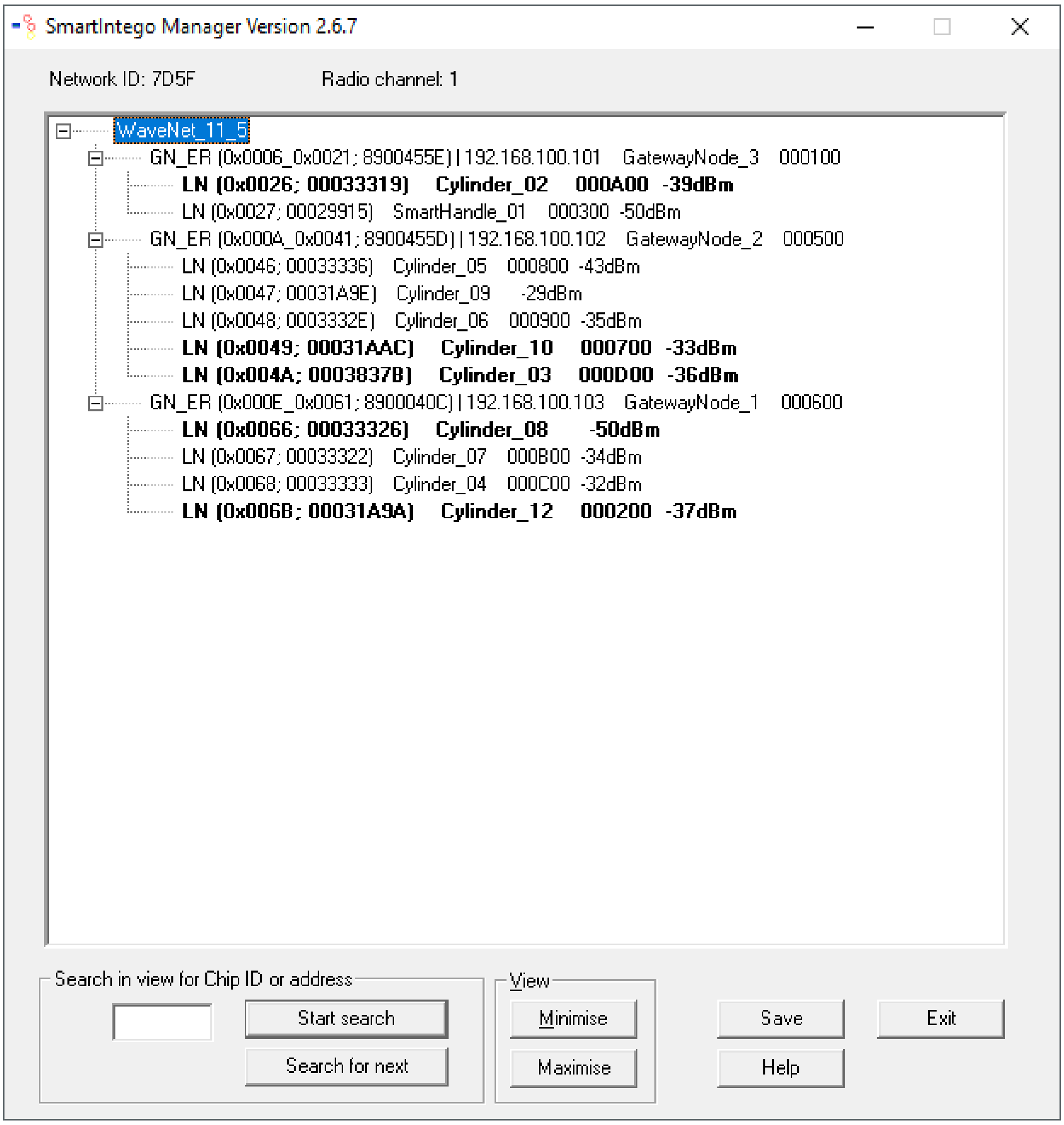
The number of LockNodes supported can be limited by the integrator system. This particularly applies to integrator systems with hardware controllers (limitation of the number of locking devices per controller).

1. In this step, specify the maximum locking devices supported by the integrator system (use the limit when reallocating).
2. In this example, the integrator system supports eight LockNodes per GatewayNode. Therefore, the number is limited to eight LockNodes per GatewayNode when assigned.

10. Click on the button OK.
    - ↳ Window for specifying the maximum number of LockNodes per GatewayNode closes.
    - ↳ The window "Select node" opens.



11. Highlight all GatewayNodes with which you want to address LockNodes (usually all).
12. Click on the button OK.
    - ↳ Window "Select node" closes.
    - ↳ Allocation is changed based on measured RSSI value.
    - ↳ Device address remains the same.
    - ↳ Duration: Approximately two minutes per GatewayNode.
    - ↳ Modified assignment is displayed in SmartIntego Manager.


SmartIntego Manager Version 2.6.7

Network ID: 7D5F   Radio channel: 1

```
WaveNet_11_5
  GN_ER (0x0006_0x0021; 8900455E) | 192.168.100.101   GatewayNode_3   000100
    LN (0x0026; 00033319)   Cylinder_02   000A00  -39dBm
    LN (0x0027; 00029915)   SmartHandle_01   000300  -50dBm
  GN_ER (0x000A_0x0041; 8900455D) | 192.168.100.102   GatewayNode_2   000500
    LN (0x0046; 00033336)   Cylinder_05   000800  -43dBm
    LN (0x0047; 00031A9E)   Cylinder_09     -29dBm
    LN (0x0048; 0003332E)   Cylinder_06   000900  -35dBm
    LN (0x0049; 00031AAC)   Cylinder_10   000700  -33dBm
    LN (0x004A; 0003837B)   Cylinder_03   000D00  -36dBm
  GN_ER (0x000E_0x0061; 8900040C) | 192.168.100.103   GatewayNode_1   000600
    LN (0x0066; 00033326)   Cylinder_08     -50dBm
    LN (0x0067; 00033322)   Cylinder_07   000B00  -34dBm
    LN (0x0068; 00033333)   Cylinder_04   000C00  -32dBm
    LN (0x006B; 00031A9A)   Cylinder_12   000200  -37dBm
```

13. Click on the button Save.
    ↳ The data record is saved.
14. Click on the Exit button.

↳ Assignment has been accepted.

NOTE

Manual configuration if CSV import of the configuration file is missing

Some integrator systems do not support CSV import of the configuration file.

- Configure manually in the integrator system (considerable effort).

NOTE

Different procedure for Mercury components

Mercury GatewayNodes will change the device address (LockNodes) when moving.

5.24 Connecting SmartIntego to the integrator system

All SmartIntego components set up are configured with individual data in the system.

This data must be communicated to the integrator system after each change to the SmartIntego components. The most important data for the integrator system and communication are:

- Device address (all components)
- Device address for locking devices with two card readers
- IP address (TCP GatewayNodes)
- Segment address (RS-485-GatewayNode)
- Locking device connection to the GatewayNode
- Unique hardware number
    - Locking devices: PHI
    - GatewayNodes and LockNodes: Chip ID

You can also transfer additional information to the integrator system:

- Configuration
- Locking device status
- Quality of connection (based on last data packet)
- ...

Please refer to the integrator system documentation for the required information.

NOTE

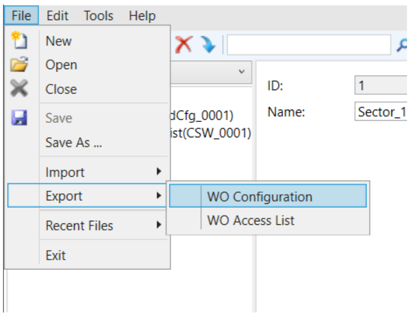
CSV export for integrator systems after update

After an update from version 2.1 to version 3.0, the SmartIntego Manager must be started once before you export CSV files.

You can export all information together as a CSV file:

✓ SmartIntego-Tool (WO) opened.

1. Via | File | and Export open the entry SI-Tool: File, Export - WO Configuration [offen].



2. Export the configuration file.

Integration into the integrator system can be different (import or manual transfer). In any case, you must prevent deviations from the actual configuration. This could have different effects:

- Opening of wrong doors
- Incorrect authorisations
- Double doors (double configuration in integrator system)
- Doors that no longer open
- ...

6 Maintain SmartIntego project and correct errors

6.1 Read access list (whitelist accesses)

The integrator system records the access list for SmartIntego locking devices.

If the integrator system fails, the locking devices use the integrator whitelist stored on the locking device (see *TCP: Prepared installation (Integrator Whitelist) [▸ 23]*). Access based on this whitelist is stored in a rolling (automatically overwritten) access list with a maximum of 1,000 entries (WO Legacy 250).

NOTE

Shared access list for cylinders with reader on both sides

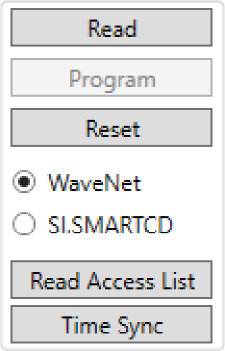
Cylinders reading from both sides create a common access list for both readers.

6.1.1 Read access list via WaveNet

✓ SmartIntego-Tool (WO) opened.

✓ Locking device reachable via WaveNet.

1. Click on the locking device entry in the navigation area.
2. Select the option ● WaveNet in the settings.



3. Click on the Read Access List button.
   ↳ Access list for the locking device is read out via WaveNet.
4. Export the access list via | File |, Export and WO Access List.

↳ Access list is exported as CSV file.

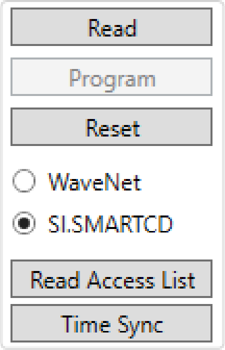
6.1.2 Read access list via programming device

✓ SmartIntego-Tool (WO) opened.

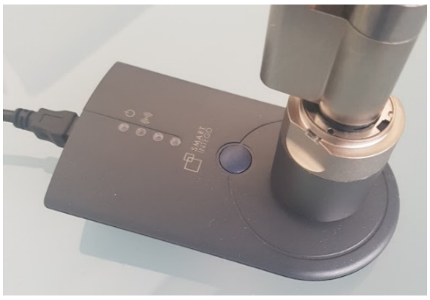
✓ Programming device connected.

1. Click on the locking device entry in the navigation area.

2. In the settings, select ◉ SI.SmartCD



3. Position the programming device on the locking device (example: locking cylinder).



4. Click on the Read Access List button.
5. Export the access list via | File |, Export and WO Access List.

↳ Access list is exported as CSV file.

6.2 Time in the locking device

Each programming resets the time of the locking devices. The clock in the locking devices can deviate from the real time by up to 15 minutes for technical reasons. With SmartIntego this has an effect on the:

- access lists (times of logged accesses differ)
- Start times of the battery measurement (Regularly between midnight and four o'clock)

Update the time of all locking devices annually. Once you synchronise the time of the locking devices, the locking devices will receive the time of the computer from which the synchronisation with the SmartIntego tool originates.

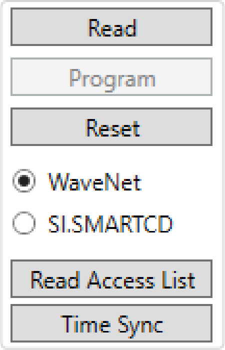
6.2.1 Setting the time on a single locking device

✓ SmartIntego-Tool (WO) opened.

✓ Locking device reachable via WaveNet.

1. Click on the locking device entry in the navigation area.

2. In the settings, click the button Time Sync.



● WaveNet

○ SI.SMARTCD

   ↳ Time is synchronized via WaveNet (approx. 10 seconds).

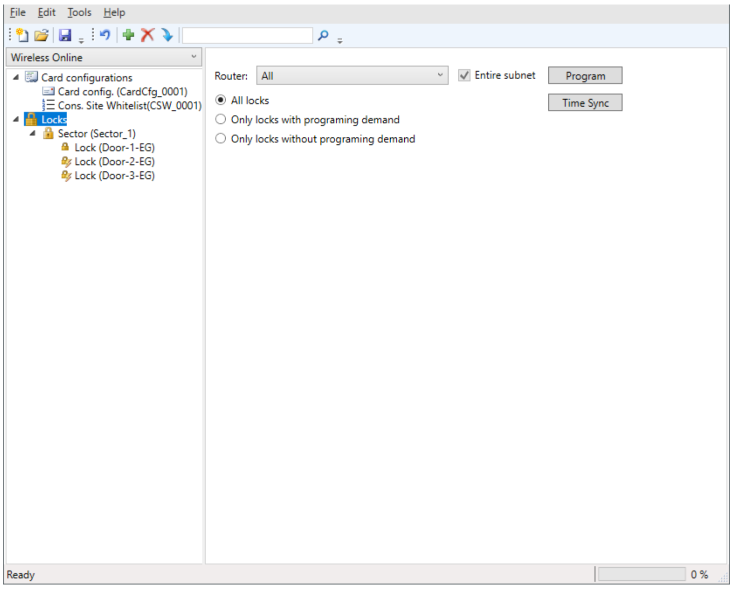
↳ Time is synchronized.

6.2.2 Setting the time on several locking devices

✓ SmartIntego-Tool (WO) opened.

✓ Locking devices can be accessed via WaveNet.

1. Click on the entry of a sector or root node of all locking devices in the navigation area.
2. In the drop-down menu, ▼ **Router** select whether you want to synchronise the locking devices of all GatewayNodes or only the locking devices of a specific GatewayNodes.
3. Use the options ◉ SI-Tool: Mehrere programmieren "Alle Schließungen" [offen], ◉ SI-Tool: Mehrere programmieren "Schließungen mit Programmierbedarf" [offen] or ◉ SI-Tool: Mehrere programmieren "Schließungen ohne Programmierbedarf" [offen] to specify which locking devices of the GatewayNode you want to synchronise.



Router: All

☑ Entire subnet

● All locks

○ Only locks with programing demand

○ Only locks without programing demand

4. Click on the Time Sync button.
   ↳ Time is synchronized via WaveNet (approx. 10 seconds locking device).

↳ Time is synchronized.

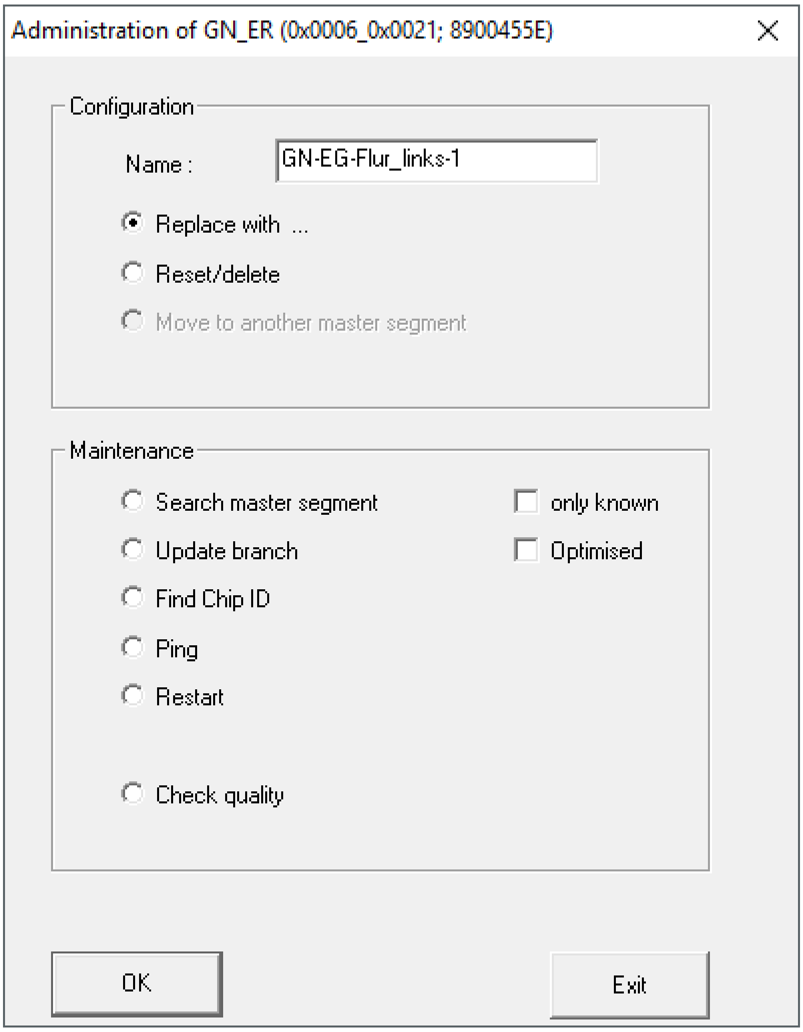
6.3 Change DNS name or IP address of a GatewayNode

To do this, first change the DNS name or IP address via the configuration website of the GatewayNode (see *Open configuration page [▸ 67]*. Resolving host names requires a functioning DNS server and creates an additional dependency. Therefore, avoid host names.

Then replace the GatewayNode with the same GatewayNode with the new IP address or host name:

✓ SmartIntego Manager opened.

1. Right-click on the entry of the corresponding GatewayNode.
   ↳ The window "Administration" opens.



Administration of GN_ER (0x0006_0x0021; 8900455E)

Configuration

Name : GN-EG-Flur_links-1

● Replace with ...

○ Reset/delete

○ Move to another master segment

Maintenance

○ Search master segment □ only known

○ Update branch □ Optimised

○ Find Chip ID

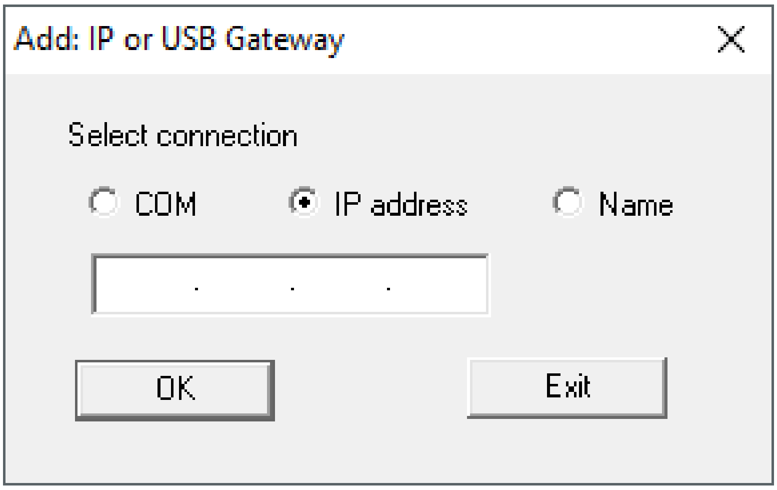
○ Ping

○ Restart

○ Check quality

2. Select the option ● Replace with

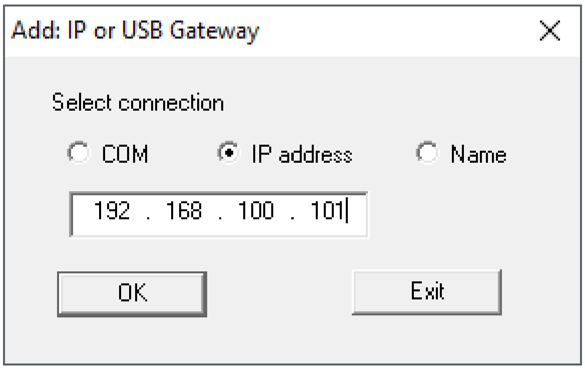
3. Click on the button OK.
   - ↳ Window "Administration" closes.
   - ↳ The window "Add IP or USB Gateway" opens.


Add: IP or USB Gateway

Select connection

○ COM ● IP address ○ Name

4. Select the option ● IP address or ● Name.
5. Enter the new IP or host name.


Add: IP or USB Gateway

Select connection

○ COM ● IP address ○ Name

192 . 168 . 100 . 101

6. Click on the button OK.
   - ↳ Window "Add IP or USB Gateway" closes.
   - ↳ IP address or host name of the GatewayNode replaced.
   - ↳ GatewayNode displayed in overview with new IP address or host name.
7. Click on the button Save.
8. Click on the Exit button.

↳ Configuration saved with new IP address or host name.

6.4 Rename GatewayNode

You can name all GatewayNodes with another name in addition to the host name.

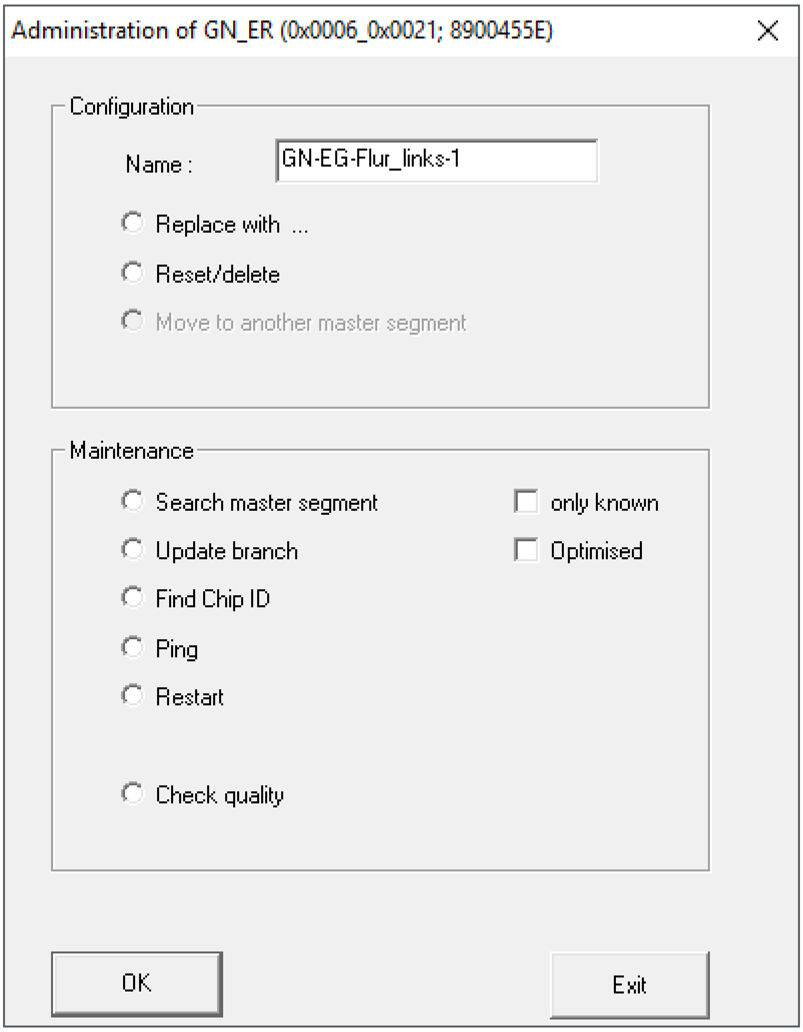
For example, a location name such as `GatewayNode-EG-Flur_links-1` would be conceivable.

This name is displayed in the SI Manager and, if necessary, in the integrator system.

6.4.1 Renaming an individual GatewayNode

- ✓ SmartIntego Manager opened.
- ✓ GatewayNode.

1. Right-click the entry of the GatewayNode.
   ↳ The window "Administration" opens.



Administration of GN_ER (0x0006_0x0021; 8900455E)

Configuration

Name : GN-EG-Flur_links-1

○ Replace with ...

○ Reset/delete

○ Move to another master segment

Maintenance

○ Search master segment □ only known

○ Update branch □ Optimised

○ Find Chip ID

○ Ping

○ Restart

○ Check quality

2. Specify a new name for the GatewayNode.
3. Click on the button OK.
   ↳ Window "Administration" closes.
   ↳ GatewayNode displayed in overview with new name.
4. Click on the button Save.

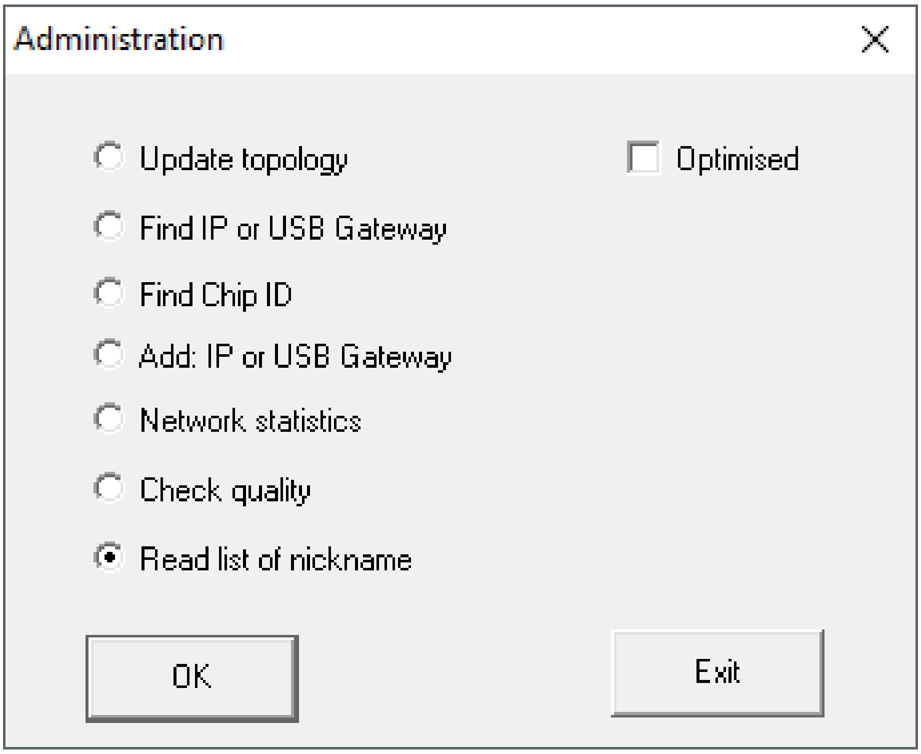
↳ GatewayNode is renamed.

6.4.2 Rename multiple GatewayNodes

You can also rename multiple GatewayNodes at the same time. To do this, import the name list (see also *Creating, expanding and importing a name list [▸ 29]*).

✓ SmartIntego Manager opened.

1. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.



Administration

○ Update topology □ Optimised

○ Find IP or USB Gateway

○ Find Chip ID

○ Add: IP or USB Gateway

○ Network statistics

○ Check quality

● Read list of nickname

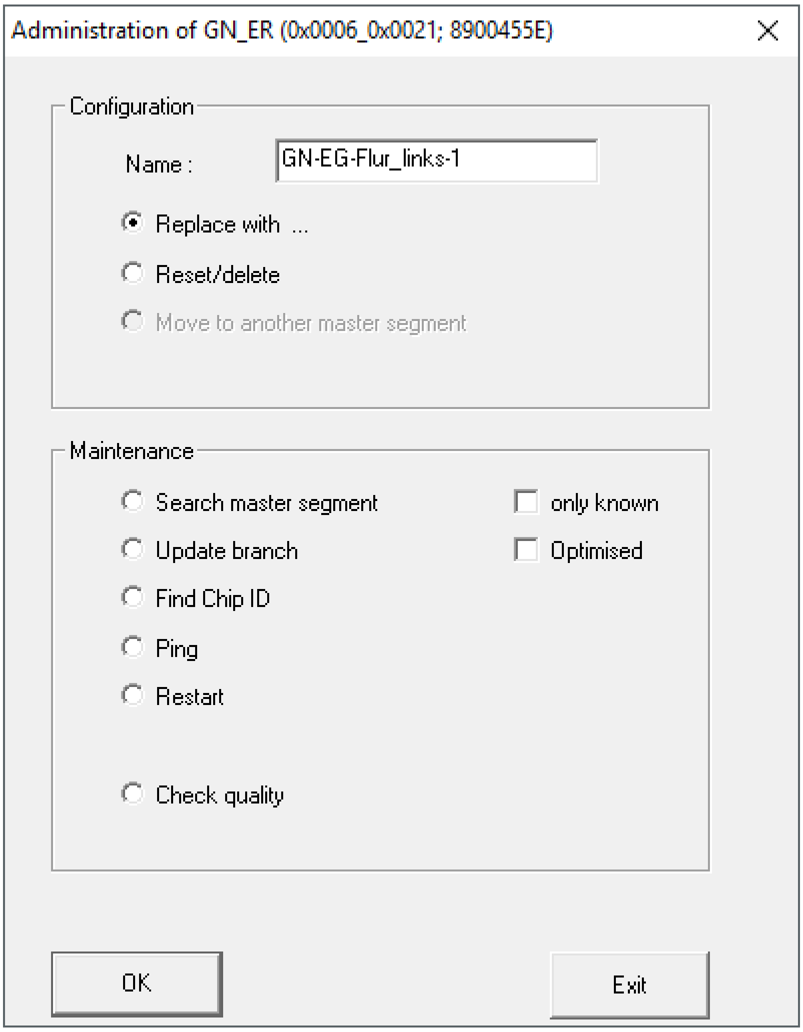
2. Select the option ● Read list of nicknames.
3. Click on the button OK.
   ↳ The window for selecting the list opens.
4. Select the list.
5. Import the list.
   ↳ The window for selecting the list closes.
   ↳ All chip IDs in SmartIntego Manager are checked and updated with the assigned name from the name list.
6. Click on the button Save.

↳ GatewayNodes renamed.

6.5 Replace GatewayNode

- ✓ SmartIntego Manager opened.
- ✓ New GatewayNode connected.
- ✓ TCP/RS-485 configuration completed (see *Configuring GatewayNodes (TCP) [▸ 54]* or *RS-485 ConfigNode [▸ 78]*).

1. Click with the right mouse button on the ConfigNode entry.
   ↳ The window "Administration" opens.



Administration of GN_ER (0x0006_0x0021; 8900455E)

Configuration

Name : GN-EG-Flur_links-1

● Replace with ...

○ Reset/delete

○ Move to another master segment

Maintenance

○ Search master segment □ only known

○ Update branch □ Optimised

○ Find Chip ID

○ Ping

○ Restart

○ Check quality

2. Select the option ● Replace with.
3. Click on the button OK.
   ↳ The window for entering the new IP address or host name opens.
4. Specify the new IP address or host name of the GatewayNode.
5. Click on the button OK.
   ↳ Window for entering the new IP address or host name closes.
6. Click on the button Save.
7. Click on the Exit button.

↳ GatewayNode replaced.

If necessary, reset the old GatewayNode via hardware reset (see *Resetting components with hardware reset [▸ 160]*)

6.6 Replace defective locking device

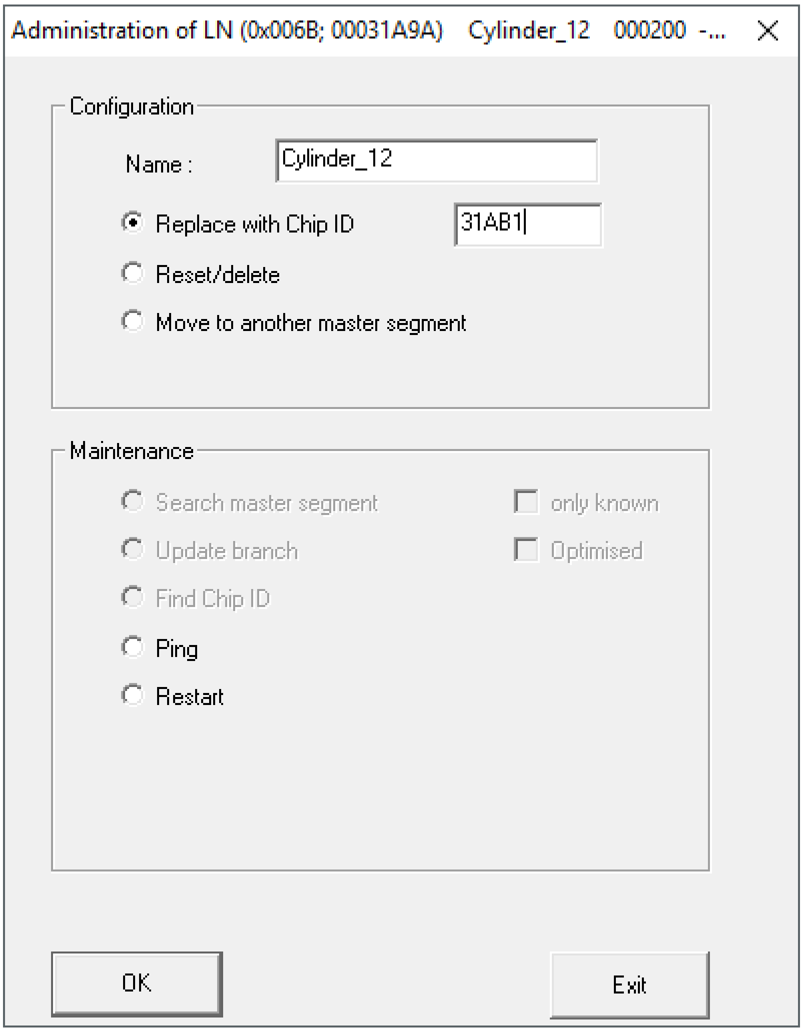
Proceed as described if your locking device is mechanically or electronically defective. For information on replacing an intact locking device with another model, see *Replace intact locking device [▸ 139]*.

✓ SmartIntego Manager opened.

✓ SmartIntego-Tool (WO) opened.

1. Replace the defective locking device on the door physically.
2. Remove the batteries of the faulty locking device (see quick guide or locking device manual).
3. Right-click on the entry for the defective locking device.

   ↳ The window "Administration" opens.



Administration of LN (0x006B; 00031A9A) Cylinder_12 000200 -... ✕

Configuration

Name : Cylinder_12

● Replace with Chip ID 31AB1

○ Reset/delete

○ Move to another master segment

Maintenance

○ Search master segment □ only known

○ Update branch □ Optimised

○ Find Chip ID

○ Ping

○ Restart

OK Exit

4. Select the option ● Replace with Chip ID.
5. Enter the chip ID of the new locking device (overwrite old chip ID).

   ↳ Window "Administration" closes.

   ↳ LockNode is being reconfigured.

6. Confirm the message with OK.
7. Click on the button Save.
8. Click on the Exit button.
9. Programme the new locking device in the SmartIntego tool (WO) (see *Programme locking device [▸ 112]*).

↳ Defective locking device replaced.

Further procedure at RMA

Reset the locking device with the SI.SmartCD:

1. Use the SmartIntego tool (WO) to create a new, empty * .ikp file to reset.
2. Insert the batteries into the locking device.
3. Read out the locking device via | Tools |, Card Reader and Read unknown lock.
   ↳ Locking device is read out.
   ↳ The window with read-out values opens.
4. Click on the Reset button.
   ↳ Window with read-out values closes.
5. Enter the locking system password.
   ↳ The locking device is reset.
6. Remove the batteries of the faulty locking device again.
7. Update the name list if necessary (see *Creating, expanding and importing a name list [▸ 29]*).

↳ Locking device prepared for RMA.

6.7 Replace intact locking device

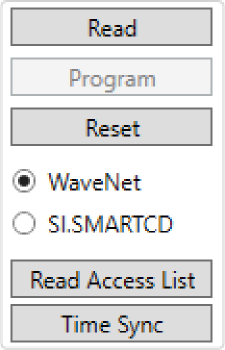
Proceed as described if you want to replace an intact locking device with another locking device (e.g. a SmartHandle instead of a locking cylinder).

✓ SmartIntego-Tool (WO) opened.

✓ New and old locking device within reach of a GatewayNode.

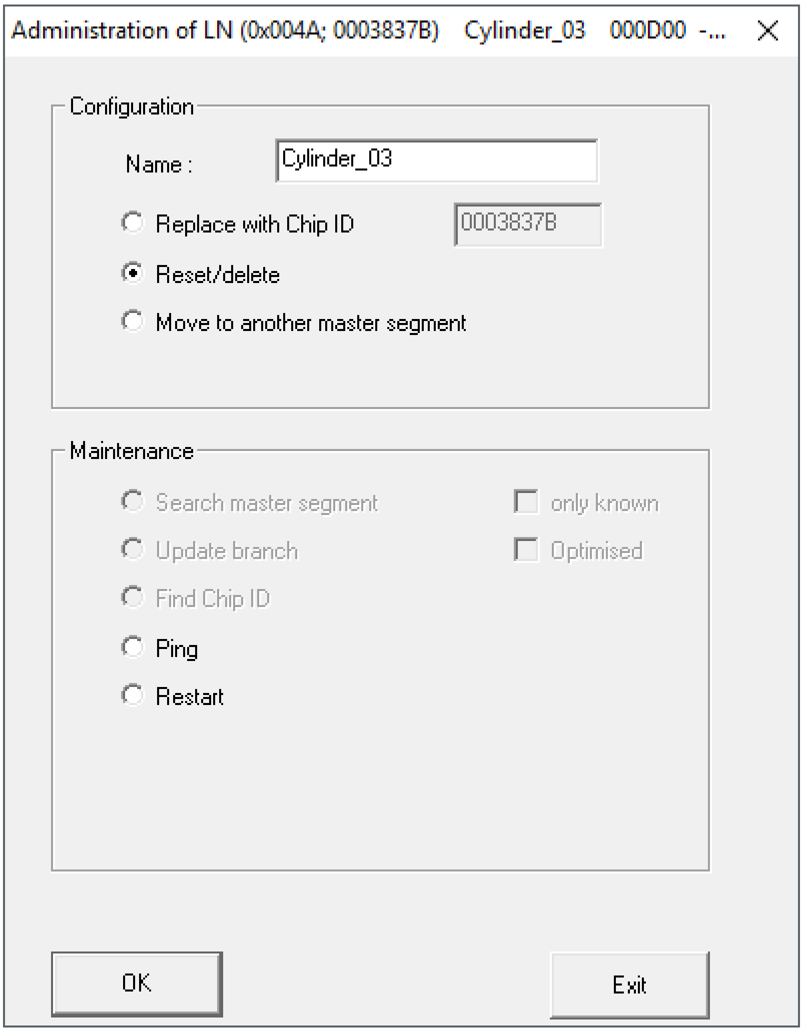
1. In the navigation area, click the entry for the locking device you want to replace.

2. Select the option ● WaveNet in the settings.



● WaveNet
○ SI.SMARTCD

3. Click on the Reset button.
   ↳ The locking device is reset.
4. Open SmartIntego Manager.
5. Right-click the entry of the locking device you want to replace.
   ↳ The window "Administration" opens.



Administration of LN (0x004A; 0003837B) Cylinder_03 000D00 -...

Configuration

Name : Cylinder_03

○ Replace with Chip ID 0003837B

● Reset/delete

○ Move to another master segment

Maintenance

○ Search master segment □ only known

○ Update branch □ Optimised

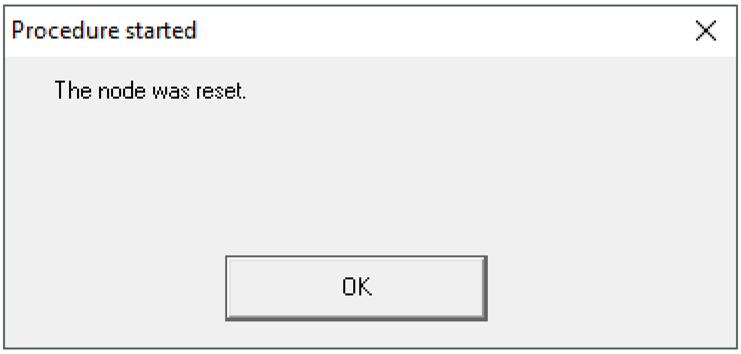
○ Find Chip ID

○ Ping

○ Restart

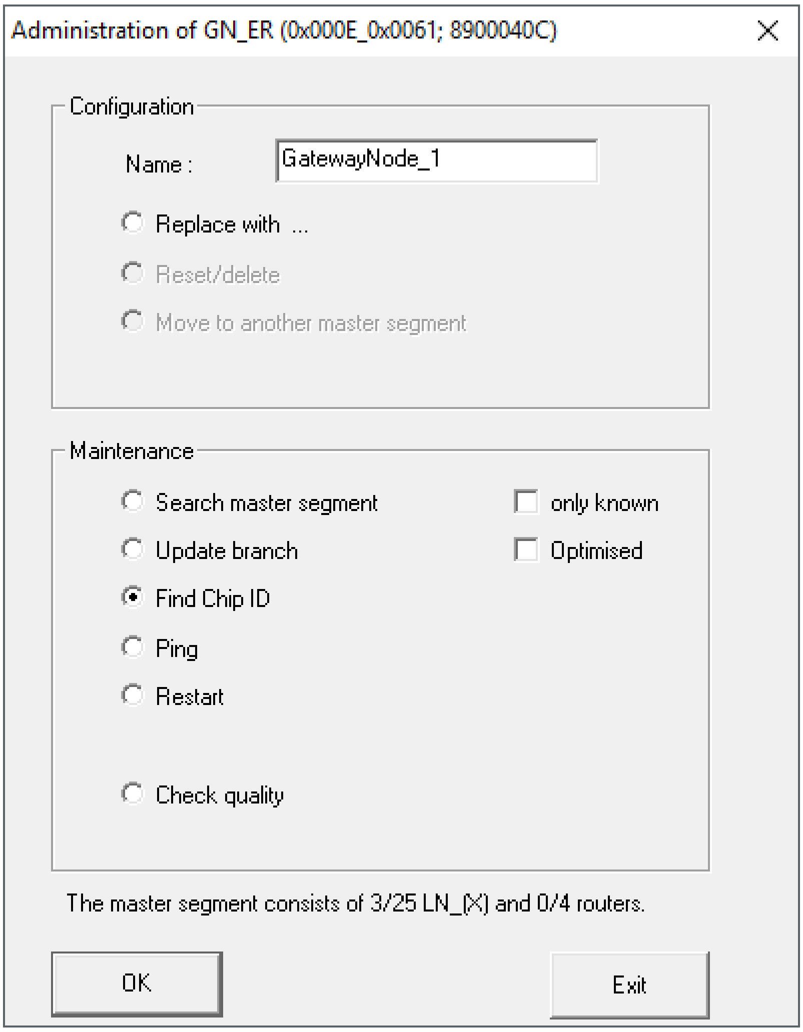
6. Select the option ● Reset/delete.

7. Click on the button OK.
   - ↳ Window "Administration" closes.
   - ↳ The window "Procedure started" opens.


Procedure started

The node was reset.

8. Click on the button OK.
   - ↳ Window "Procedure started" closes.
9. Right-click the entry of the GatewayNode in which the locking device was located.
   - ↳ The window "Administration" opens.


Administration of GN_ER (0x000E_0x0061; 8900040C)

Configuration

Name : GatewayNode_1

○ Replace with ...

○ Reset/delete

○ Move to another master segment

Maintenance

○ Search master segment □ only known

○ Update branch □ Optimised

● Find Chip ID

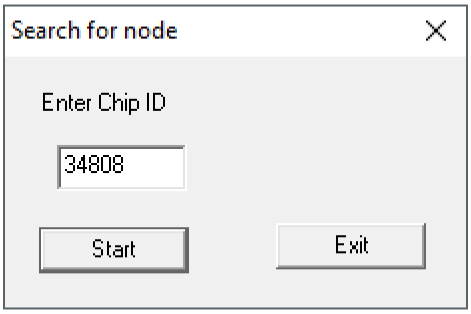
○ Ping

○ Restart

○ Check quality

The master segment consists of 3/25 LN_(X) and 0/4 routers.

10. Select the option ◉ Find Chip ID.
11. Click on the button OK.
    - ↳ Window "Administration" closes.
    - ↳ The window "Search for node" opens.

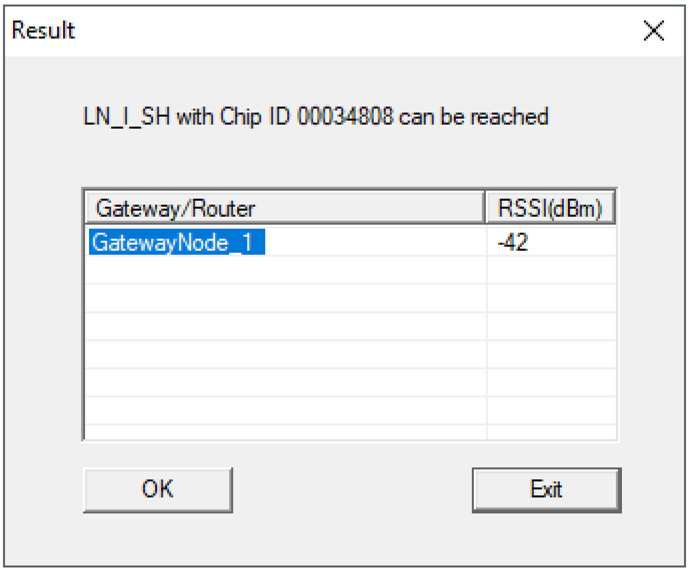


Search for node

Enter Chip ID

34808

12. Enter the chip ID of the new locking device.
13. Click on the Start button.
    - ↳ Window "Search for node" closes.
    - ↳ SmartIntego Manager searches for chip ID.
    - ↳ The window "Results" opens.



Result

LN_I_SH with Chip ID 00034808 can be reached

Gateway/Router	RSSI(dBm)
GatewayNode_1	-42

14. Select the entry of the GatewayNode.
15. Click on the button OK.
    - ↳ Window "Results" closes.
    - ↳ Locking device is displayed in SmartIntego Manager.
16. Click on the button Save.
17. Update the name list if necessary (see *Creating, expanding and importing a name list [▸ 29]*).
18. Click on the Exit button.

19. Program the new locking device in the SmartIntego tool (see *Programme locking device [▸ 112]*).
    ↳ Locking device has been replaced.

NOTE

New locking device with new device address

This is a new locking device with a new device address.

6.8 Relocate locking devices (assign to another GatewayNode)

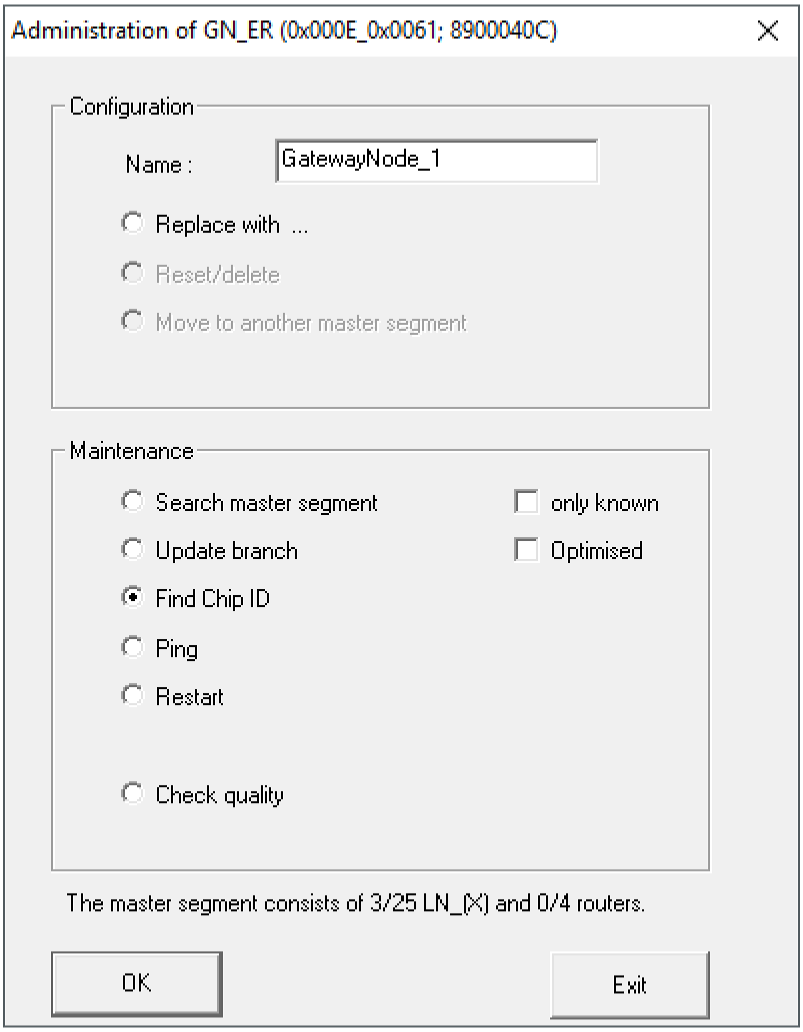
The environment of your SmartIntego project can change (e.g. new walls). You may therefore need to relocate your locking devices (i.e. assign them to another GatewayNode).

6.8.1 Move individual locking device

✓ SmartIntego Manager opened.

✓ Locking device reachable from new GatewayNode.

1. Right-click the entry of the GatewayNode to which you want to relocate the locking device.
   ↳ The window "Administration" opens.



Administration of GN_ER (0x000E_0x0061; 8900040C)

Configuration

Name : GatewayNode_1

○ Replace with ...

○ Reset/delete

○ Move to another master segment

Maintenance

○ Search master segment

○ Update branch

● Find Chip ID

○ Ping

○ Restart

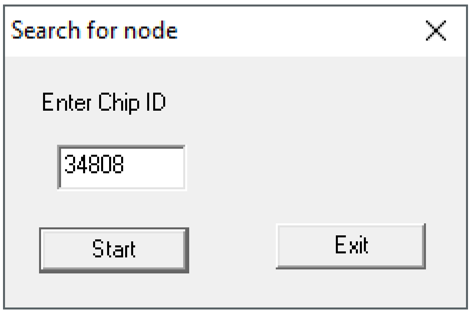
○ Check quality

□ only known

□ Optimised

The master segment consists of 3/25 LN_(X) and 0/4 routers.

2. Select the option ● Find Chip ID.
3. Click on the button OK .
   - ↳ Window "Administration" closes.
   - ↳ The window "Search for node" opens.



Search for node

Enter Chip ID

34808

4. Enter the LockNode chip ID without leading zeros.
5. Click on the Start button.
   - ↳ Window "Search for node" closes.
   - ↳ SmartIntego Manager searches for LockNode.
   - ↳ Window "Search results" opens with RSSI values.

6. Select the GatewayNode to which you want to move the locking device (usually the GatewayNode with the best RSSI value).
7. Click on the button OK.
   - ↳ Window "Search results" closes.
   - ↳ Note on resetting after relocation opens.
8. Confirm the notification message.
   - ↳ Note on resetting after relocation closes.
   - ↳ LockNode is reset.
   - ↳ Locking device is displayed for the new GatewayNode.
9. Click on the button Save.
10. Click on the Exit button.

↳ Locking device has relocated.

NOTE

Different procedure for Mercury components

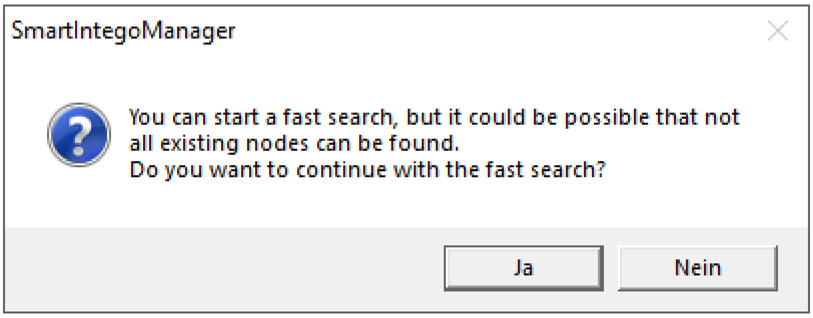
Mercury GatewayNodes will change the device address (LockNodes) when moving.

6.8.2 Moving several locking devices

✓ SmartIntego Manager opened.

✓ Locking devices of new GatewayNode.

1. Right-click the entry of the GatewayNode to which you want to relocate the locking device.
   - ↳ The window "Administration" opens.
2. Select the option ● Search master segment.
3. Click on the button OK.
   - ↳ Window "Administration" closes.
   - ↳ The window for selecting between quick and intensive search opens.



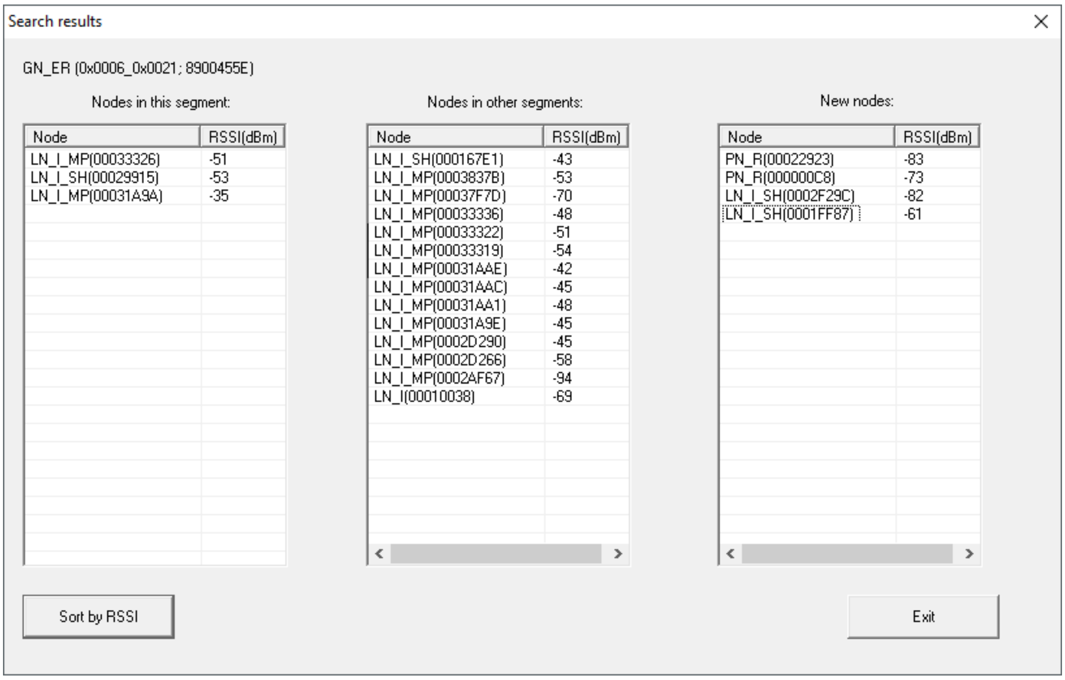
SmartIntegoManager

You can start a fast search, but it could be possible that not all existing nodes can be found.
Do you want to continue with the fast search?

4. Click on the button Yes to perform a quick search or click on the button No to perform an intensive search.
   - ↳ Searching for new and known LockNodes. (Known LockNodes are already assigned to other segments.)

↳ The window "Search results" opens.

Display of search results



Search results

GN_ER (0x0006_0x0021; 8900455E)

Nodes in this segment:

Node	RSSI(dBm)
LN_I_MP(00033326)	-51
LN_I_SH(00029915)	-53
LN_I_MP(00031A9A)	-35

Nodes in other segments:

Node	RSSI(dBm)
LN_I_SH(000167E1)	-43
LN_I_MP(0003837B)	-53
LN_I_MP(00037F7D)	-70
LN_I_MP(00033336)	-48
LN_I_MP(00033322)	-51
LN_I_MP(00033319)	-54
LN_I_MP(00031AAE)	-42
LN_I_MP(00031AAC)	-45
LN_I_MP(00031AA1)	-48
LN_I_MP(00031A9E)	-45
LN_I_MP(0002D290)	-45
LN_I_MP(0002D266)	-58
LN_I_MP(0002AF67)	-94
LN_I(00010038)	-69

New nodes:

Node	RSSI(dBm)
PN_R(00022923)	-83
PN_R(000000C8)	-73
LN_I_SH(0002F29C)	-82
LN_I_SH(0001FF87)	-61

Column	Meaning
Nodes in this segment	These LockNodes are assigned to the current GatewayNode.
Nodes in other segments	These LockNodes are assigned to another GatewayNode in this WaveNet.
New nodes	These LockNodes are not yet assigned to a GatewayNode.
RSSI value	The value displayed refers to the connection quality from the current GatewayNode to the respective LockNodes.

Relocate locking devices

1. Highlight the LockNodes in the "Nodes in other segments" column (Ctrl key and selection with the mouse).
2. Drag and drop the selection into the "Nodes in this segment" column.
3. Click on the Exit button.
   - ↳ Window "Search results" closes.
   - ↳ Locking devices are displayed for the new GatewayNode.
4. Click on the button Save.
5. Click on the Exit button.

↳ Locking devices have relocated.

NOTE

Manual configuration if CSV import of the configuration file is missing

Some integrator systems do not support CSV import of the configuration file.

- Configure manually in the integrator system (considerable effort).

NOTE

Different procedure for Mercury components

Mercury GatewayNodes will change the device address (LockNodes) when moving.

6.8.3 Restructuring the system

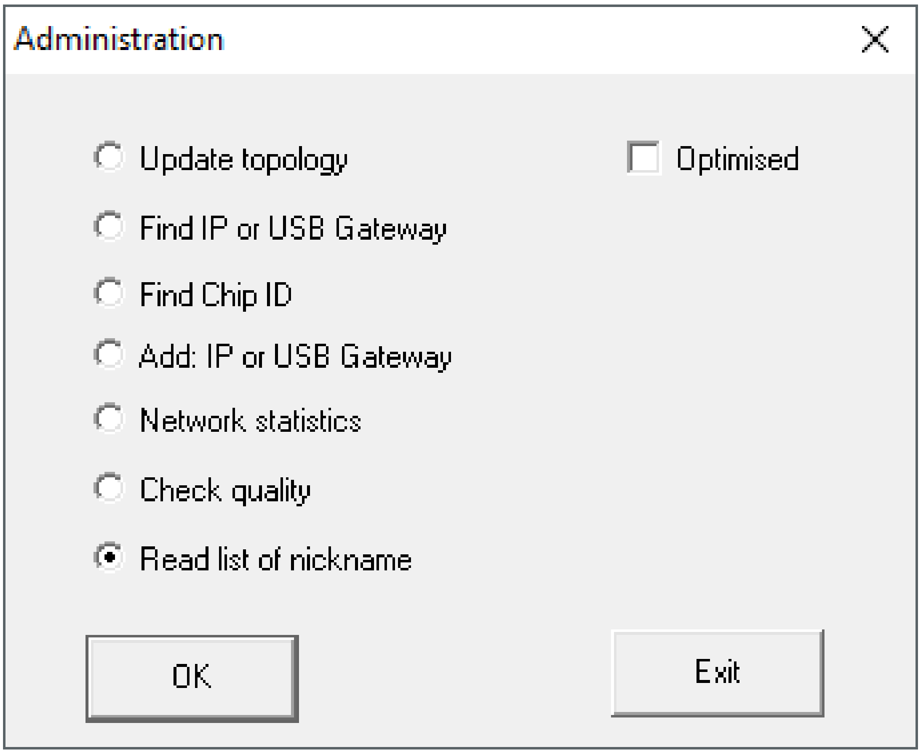
✓ SmartIntego Manager opened.

✓ Doors closed.

✓ No moving obstacles between locking devices and GatewayNodes.

1. Right-click on the navigation root (WaveNet_XX_X).

   ↳ The window "Administration" opens.



Administration

○ Update topology

□ Optimised

○ Find IP or USB Gateway

○ Find Chip ID

○ Add: IP or USB Gateway

○ Network statistics

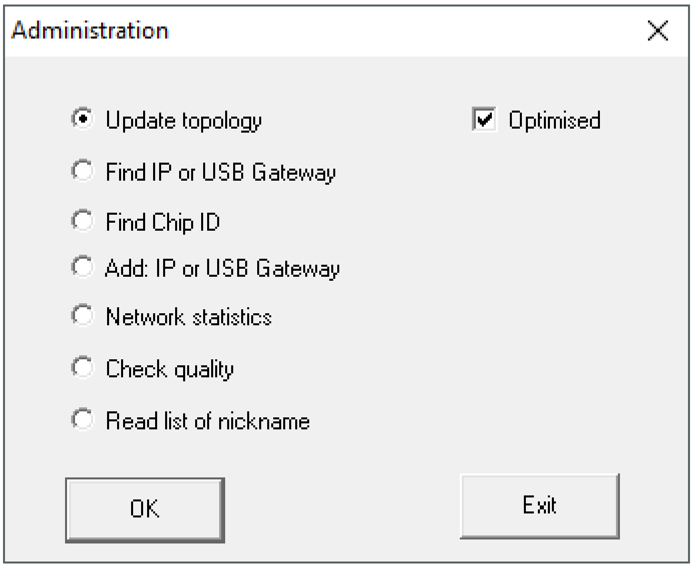
○ Check quality

● Read list of nickname

2. Select the option ● Read list of nicknames.
3. Click on the button OK.

   ↳ Window "Administration" closes.

4. Select the name list.
5. Import the name list.
6. Right-click on the navigation root (WaveNet_XX_X).
   ↳ The window "Administration" opens.



Administration

● Update topology

☑ Optimised

○ Find IP or USB Gateway

○ Find Chip ID

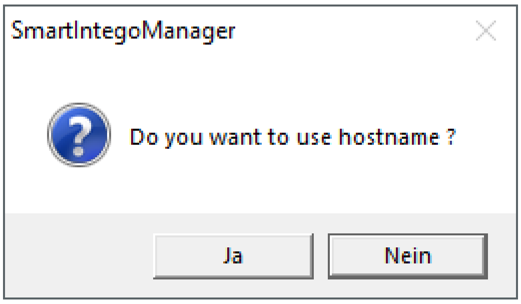
○ Add: IP or USB Gateway

○ Network statistics

○ Check quality

○ Read list of nickname

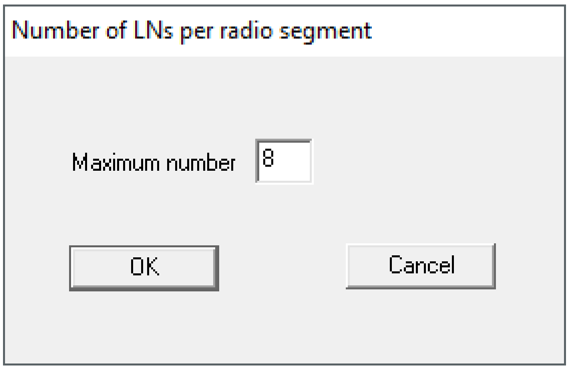
7. Select the option ● Update topology.
8. Activate the checkbox ☑ SI-Manager Update topology: Optimised [offen].
9. Click on the button OK.
   ↳ Window "Administration" closes.
   ↳ Query opens for host names.



SmartIntegoManager

Do you want to use hostname ?

10. Reject the use of host names (Wherever possible, always work with the IP address to reduce dependency on DNS servers).
    ↳ Query for host name closes.
    ↳ The window for specifying the maximum number of LockNodes per GatewayNode opens.



Number of LNs per radio segment

Maximum number 8

11. Specify the maximum number of LockNodes per GatewayNode.

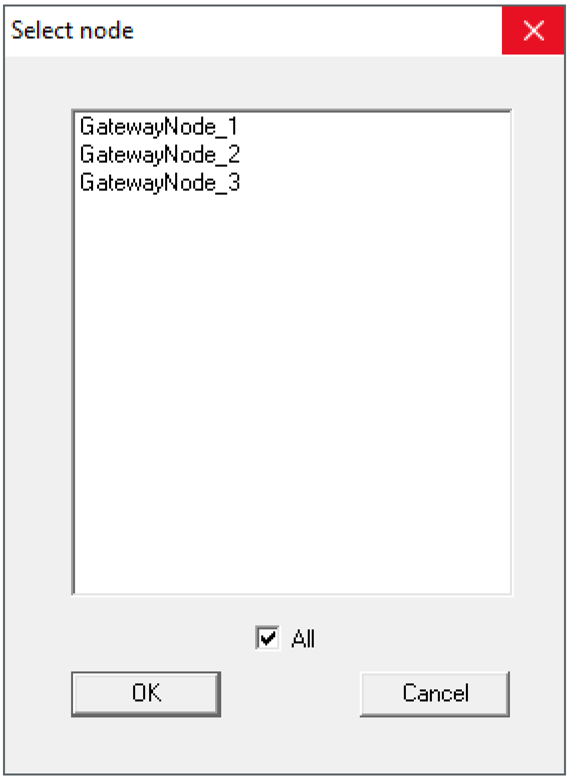
NOTE

Information on specifying the maximum number of LockNodes per gateway

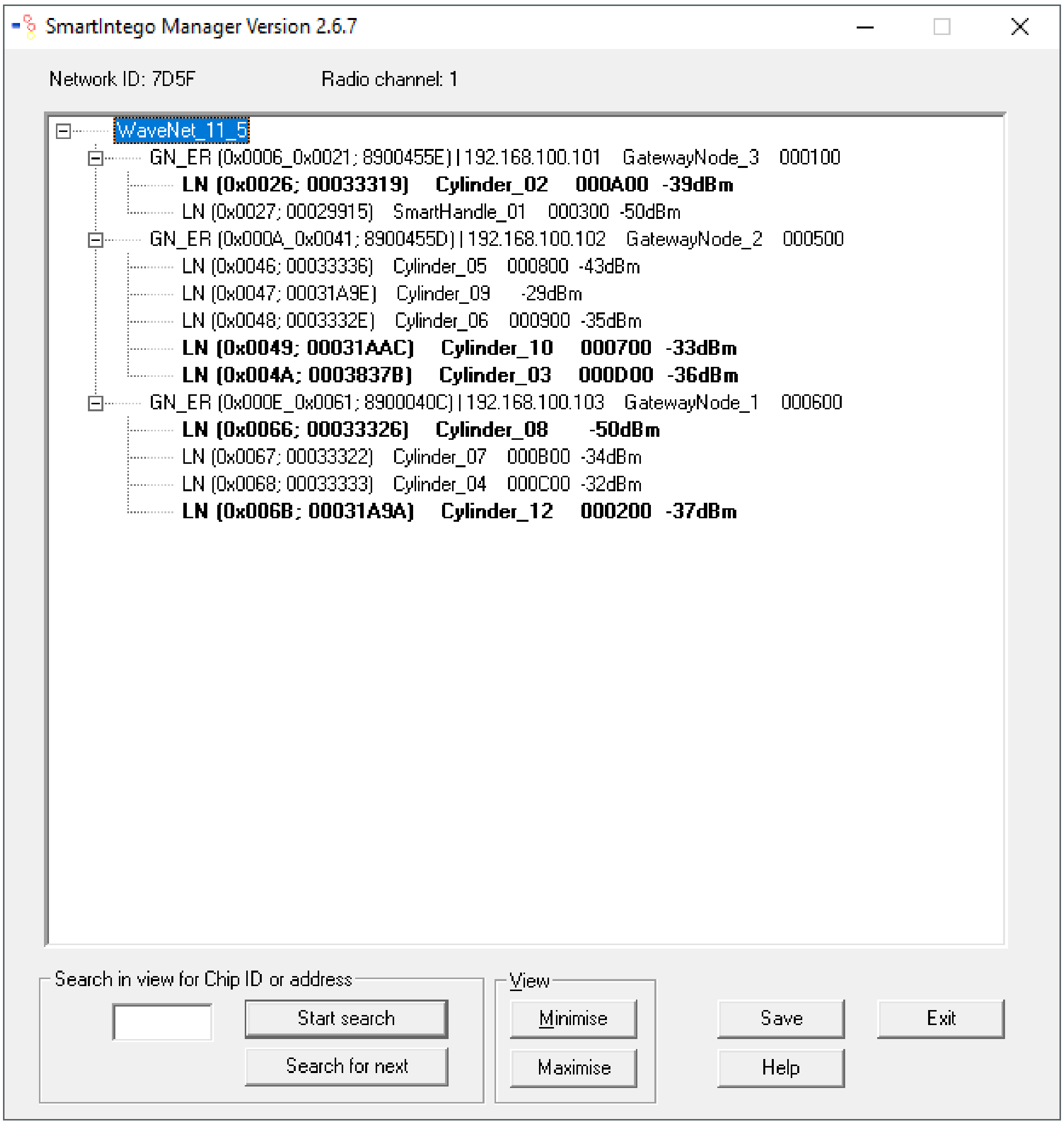
The number of LockNodes supported can be limited by the integrator system. This particularly applies to integrator systems with hardware controllers (limitation of the number of locking devices per controller).

1. In this step, specify the maximum locking devices supported by the integrator system (use the limit when reallocating).
2. In this example, the integrator system supports eight LockNodes per GatewayNode. Therefore, the number is limited to eight LockNodes per GatewayNode when assigned.

12. Click on the button OK.
    - ↳ Window for specifying the maximum number of LockNodes per GatewayNode closes.
    - ↳ The window "Select node" opens.



13. Highlight all GatewayNodes with which you want to address LockNodes (usually all).
14. Click on the button OK.
    - ↳ Window "Select node" closes.
    - ↳ Allocation is changed based on measured RSSI value.
    - ↳ Device address remains the same.
    - ↳ Duration: Approximately two minutes per GatewayNode.
    - ↳ Modified assignment is displayed in SmartIntego Manager.



SmartIntego Manager Version 2.6.7

Network ID: 7D5F Radio channel: 1

```
WaveNet_11_5
    GN_ER (0x0006_0x0021; 8900455E) | 192.168.100.101   GatewayNode_3   000100
        LN (0x0026; 00033319)   Cylinder_02   000A00  -39dBm
        LN (0x0027; 00029915)   SmartHandle_01   000300  -50dBm
    GN_ER (0x000A_0x0041; 8900455D) | 192.168.100.102   GatewayNode_2   000500
        LN (0x0046; 00033336)   Cylinder_05   000800  -43dBm
        LN (0x0047; 00031A9E)   Cylinder_09      -29dBm
        LN (0x0048; 0003332E)   Cylinder_06   000900  -35dBm
        LN (0x0049; 00031AAC)   Cylinder_10   000700  -33dBm
        LN (0x004A; 0003837B)   Cylinder_03   000D00  -36dBm
    GN_ER (0x000E_0x0061; 8900040C) | 192.168.100.103   GatewayNode_1   000600
        LN (0x0066; 00033326)   Cylinder_08      -50dBm
        LN (0x0067; 00033322)   Cylinder_07   000B00  -34dBm
        LN (0x0068; 00033333)   Cylinder_04   000C00  -32dBm
        LN (0x006B; 00031A9A)   Cylinder_12   000200  -37dBm
```

15. Click on the button Save.
    - ↳ The data record is saved.
16. Click on the Exit button.

↳ Assignment has been accepted.

NOTE

Manual configuration if CSV import of the configuration file is missing

Some integrator systems do not support CSV import of the configuration file.

- Configure manually in the integrator system (considerable effort).

NOTE

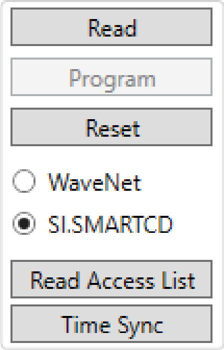
Different procedure for Mercury components

Mercury GatewayNodes will change the device address (LockNodes) when moving.

6.9 Carry out emergency opening

✓ SmartIntego-Tool (WO) opened.

1. In the navigation area, click the entry for the locking device you want to open.
   ↳ Locking device properties open.



2. Select the option ● SI.SmartCD.
3. Position the programming device on the locking device (example: locking cylinder).

4. Click on the Emergency Opening button.
   ↳ SmartIntego tool performs emergency opening.

↳ The locking device engages briefly (duration depends on the normal engagement time, see *Set coupling duration [▸ 53]*).

NOTE

Emergency opening for cylinders on both sides

An emergency opening on a cylinder with a reader on both sides only engages the master reader head (black ring behind the thumb-turn).

6.10 Battery change and battery replacement card

Battery warnings are displayed in the integrator system or on the locking device itself.

6.10.1 Creating a battery replacement card

You can start battery measurements manually with a battery replacement card.

It can be used independently of the SmartIntego project.

You no longer need a battery replacement card for AX locking devices.

✓ Empty MIFARE Classic card available (memory capacity not relevant).

✓ SmartIntego-Tool (WO) opened.

1. Place the battery replacement card on the SI.SmartCD.
2. Create the battery replacement card using | Tools |, Service Cards and Create Battery Over Change Card.
3. Follow the instructions.

6.10.2 Battery replacement

1. Open the locking device.
2. Change the battery as described in the quick guide or in the manual. (Remove the old batteries and insert the new batteries).
3. Hold the battery replacement card in front of the locking device (no longer necessary for AX).
   ↳ Battery measurement is performed manually immediately.
   ↳ Integrator system no longer receives false battery warnings.
4. Test the function of the lock with any authorised identification medium.

↳ Battery replaced.

You can also temporarily engage the locking device with an emergency opening using the SmartIntego tool (incl. the project file) and the SI.SmartCD. This type of emergency opening requires less energy and can still function even if the card reader of the locking device no longer functions due to low batteries.

6.11 Engage locking device in the event of a network failure

If the network fails or the integrator system cannot be reached, the locking device uses the integrator whitelist (see *TCP: Prepared installation (Integrator Whitelist) [▸ 23]*).

The cards of the integrator whitelist can be stored individually on the locking device.

■ Hold the card in front of the lock.

   ↳ Locking device reads card (blue LED).

   ↳ Locking device attempts to reach integrator system. If there is no response after a predefined time (= return timeout, see *TCP Keep Alive (set timeout) [▸ 75]*), the whitelist is used.

↳ Locking device engages for five seconds if the card is included in the whitelist.

NOTE

Restricted functions for whitelist access

A card that is granted access by the whitelist cannot use the following functions: Long-term opening, OfficeMode and schedules.

6.12 Disengage locking device in the event of a network failure

If the network fails or the integrator system cannot be reached, the locking device uses the integrator whitelist (see *TCP: Prepared installation (Integrator Whitelist) [▸ 23]*).

The cards of the integrator whitelist can be stored individually on the locking device.

If the locking device is currently engaged, it can be disengaged with a card stored on the whitelist.

■ Hold the card in front of the lock.

   ↳ Locking device reads card (blue LED).

   ↳ Locking device attempts to reach integrator system. If there is no response after a predefined time, the whitelist is used.

   ↳ Locking device engages if the card is included in the whitelist.

   ↳ Locking device reads card again after two seconds (blue LED).

↳ Locking device disengages.

NOTE

The construction site whitelist not suitable for disengaging in the event of a network failure

The construction site whitelist is designed to allow access to the rooms during the construction phase. Cards which are only included in the construction site whitelist cannot disengage the locking devices in the event of a network failure.

■ Use the integrator whitelist (see *TCP: Prepared installation (Integrator Whitelist) [▸ 23]*).

6.13 Creating and using WaveNet test cards

You can use a WaveNet test card to identify possible impairments in radio communication between GatewayNode and locking device.

6.13.1 Create WaveNet test card

✓ Empty MIFARE Classic card available (memory capacity not relevant).

✓ SmartIntego-Tool (WO) opened.

1. Create the WaveNet test card using | Tools |, Service Cards and Create WaveNet Test Card.
2. Follow the instructions.

6.13.2 Use WaveNet test card

- Hold the WaveNet test card to the locking device you wish to test.
  ↳ Locking device sends test signal to the GatewayNode.

↳ Feedback successful: Locking device beeps/flashes blue four times.
No response: The locking device is timed out and flashes red once.

6.14 Programming with the local programming device

NOTE

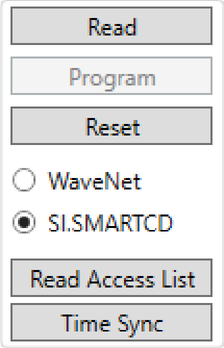
Initial programming via WaveNet

The SI.SmartCD cannot carry out initial programming.

- Programme your new locking devices via WaveNet (see *Programme locking device [▸ 112]*).

✓ SmartIntego-Tool (WO) opened.

1. In the navigation area, click the entry for the locking device.
   ↳ Locking device properties open.
2. Select the option ◉ SI.SmartCD.



3. Position the programming device on the locking device (example: locking cylinder).

4. Click on the Program button.
   ↳ Locking device is programmed.
5. Hold the programming wand in place until programming is complete.

↳ Locking device is programmed.

6.15 Reset components

Follow the order when resetting the components, otherwise the components may be damaged. Always reset components completely.

IMPORTANT

Damage caused by reset

Incomplete resetting or incorrect reset procedure can damage the components.

1. Always reset the components completely.
2. First reset the locking devices.
3. Then reset the LockNodes of the locking devices.
4. Finally, reset the connected GatewayNode.

Resetting the components is not saved in SmartIntego Manager during hardware reset. For this reason, always reset via the software and only in an emergency via the hardware reset.

6.15.1 Resetting components with SmartIntego software

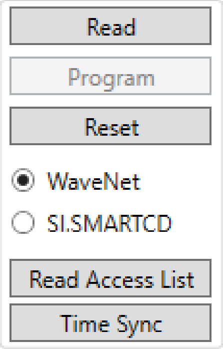
6.15.1.1 Re-set locking device

This step only resets the locking device. The LockNode remains reachable via WaveNet. Then reset the LockNode (see *Resetting the LockNode [▸ 158]*).

About WaveNet

✓ SmartIntego-Tool (WO) opened.

1. Click on the locking device entry in the navigation area.
   ↳ Locking device properties open.



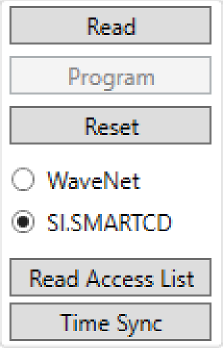
2. Select the option ● WaveNet.
3. Click on the Reset button.
   ↳ The locking device is reset.

↳ Locking device reset.

With SI.SmartCD

✓ SmartIntego-Tool (WO) opened.

1. Click on the locking device entry in the navigation area.
   ↳ Locking device properties open.



2. Select the option ● SI.SmartCD.
3. Click on the Reset button.
   ↳ The locking device is reset.

↳ Locking device reset.

6.15.1.2 Resetting the LockNode

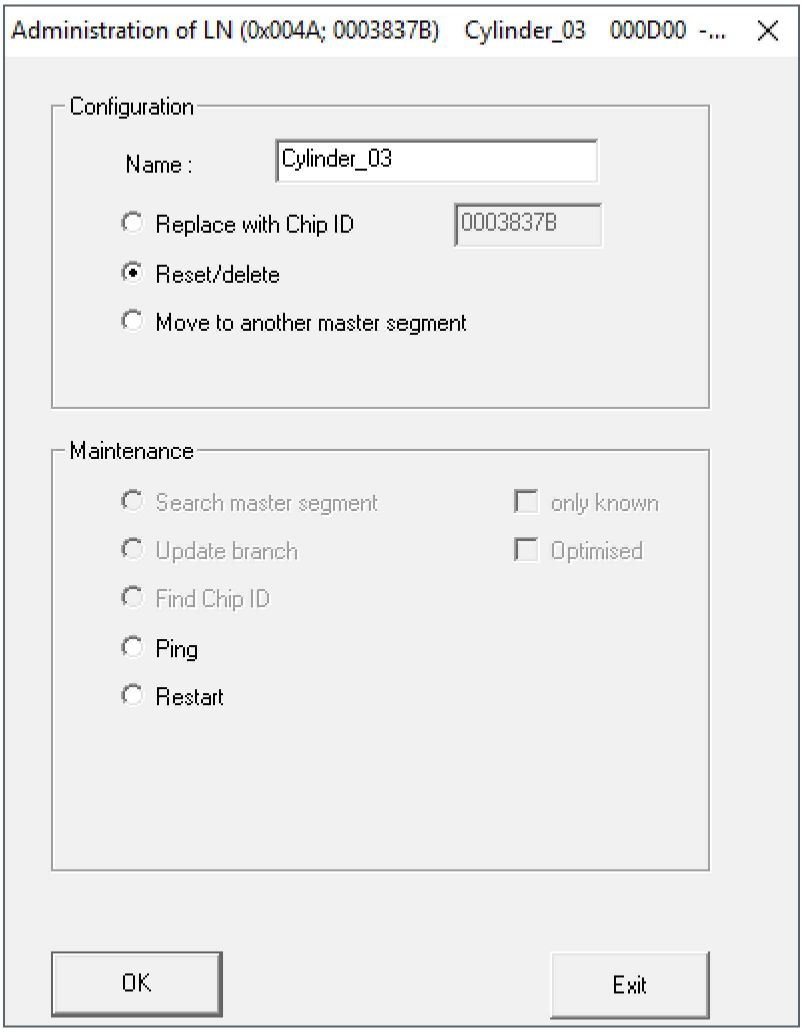
✓ SmartIntego Manager opened.

✓ Locking device reset (see *Re-set locking device [▸ 156]*).

✓ Locking device reachable via GatewayNode.

1. In SmartIntego Manager, right-click the LockNode entry.

   ↳ The window "Administration" opens.



Administration of LN (0x004A; 0003837B) Cylinder_03 000D00 -...

Configuration

Name : Cylinder_03

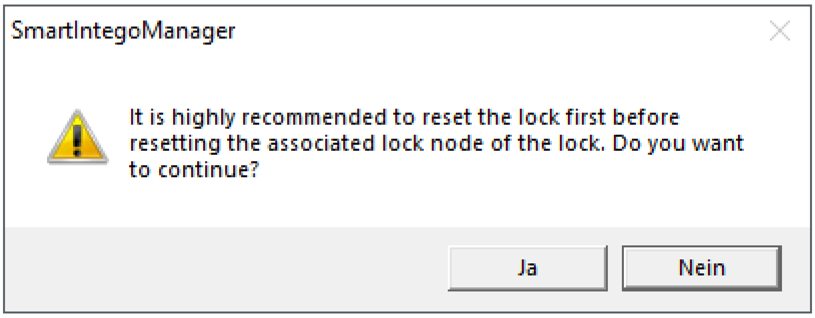
○ Replace with Chip ID 0003837B

● Reset/delete

○ Move to another master segment

2. Select the option ● Reset/delete.
3. Click on the button OK.

   ↳ Warning message appears.



SmartIntegoManager

It is highly recommended to reset the lock first before resetting the associated lock node of the lock. Do you want to continue?

4. Confirm the warning message.
   ↳ LockNode is reset.
5. Click on the button Save.
6. Click on the Exit button.
   ↳ SmartIntego Manager closes.

↳ LockNode is reset.

After the locking device and LockNode have been successfully reset, the locking device can be used in another project.

6.15.1.3 Resetting GatewayNode

The reset consists of two parts:

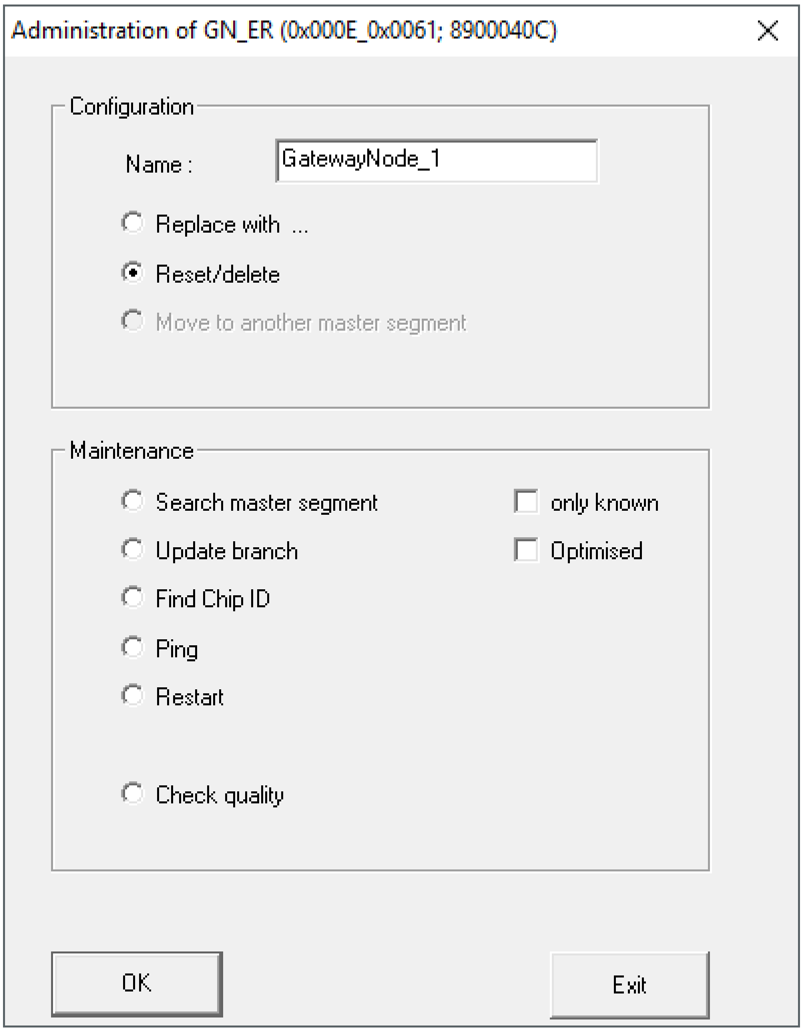
1. Reset WaveNet configuration
2. Reset IP configuration

✓ LockNode no longer connected to GatewayNode.
(Reset locking devices and LockNodes, see *Re-set locking device [▸ 156]* and *Resetting the LockNode [▸ 158]*)
Alternatively, move, see *Relocate locking devices (assign to another GatewayNode) [▸ 143]*.

✓ GatewayNode can be reached by SmartIntego Manager.

✓ SmartIntego Manager opened.

1. Right-click the entry of the GatewayNode that you want to reset.
   ↳ The window "Administration" opens.



Administration of GN_ER (0x000E_0x0061; 8900040C)

Configuration

Name : GatewayNode_1

○ Replace with ...

● Reset/delete

○ Move to another master segment

Maintenance

○ Search master segment □ only known

○ Update branch □ Optimised

○ Find Chip ID

○ Ping

○ Restart

○ Check quality

2. Select the option ◉ Reset/delete.
3. Click on the button OK.
   ↳ Window "Administration" closes.
4. Click on the button Save.
5. Click on the Exit button.
6. Open the Gateway Node configuration website (see *Open configuration page [▸ 67]*).
7. Reset the TCP settings of the GatewayNode there via | ADMINISTRATION | and [FACTORY].

↳ GatewayNode reset.

6.15.2 Resetting components with hardware reset

If you can no longer reset the components with SmartIntego Manager (see *Resetting components with SmartIntego software [▸ 156]*), you must use the hardware reset.

Possible causes:

- The data of a component has been deleted in the SmartIntego tool (WO) without deleting the component in the SmartIntego tool (WO). This means that the SmartIntego tool (WO) can no longer reach the component.
- The SmartIntego tool (WO) configuration file (*.ikp) no longer exists.
- The existing data status deviates from the real project in both cases. The system attempts to address components that no longer exist with the existing addressing. You must correct the deviation yourself.
- Reset the components in the following order:

1. LockNode
2. Locking device
3. GatewayNode (after resetting all connected LockNodes and locking devices, see *Resetting the WaveNet/network configuration of the GatewayNode [▸ 167]*)
4. Depending on the situation, you must deviate from this sequence.

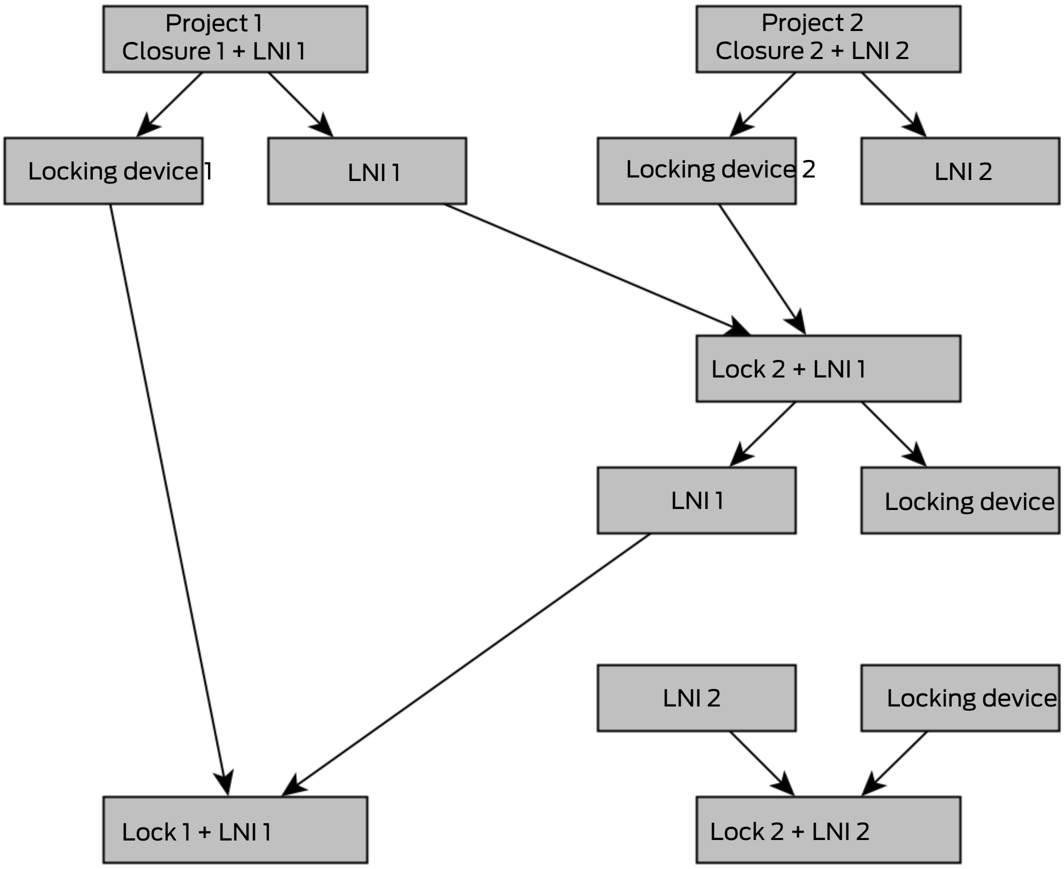
The procedure differs depending on the status of the locking device in which the LockNode is installed.

- Programmed LockNode in programmed locking device (see *Resetting the programmed LockNode and programmed locking device [▸ 162]*).
- Programmed LockNode in non-programmed locking device (see *Resetting the programmed LockNode and non-programmed locking device [▸ 164]*).

LockNodes are reset as soon as they are installed in a programmed locking device in which a previously programmed LockNode was already installed.

6.15.2.1 Resetting the programmed LockNode and programmed locking device

Resetting the LockNode



- ✓ SmartIntego-Tool (WO) opened.
- ✓ Second locking device of the same type available.
- ✓ GatewayNode available.
- ✓ SI.SmartCD available.

1. Create a second project with a different SID in the SmartIntego tool (WO) (see *Createing a SmartIntego project [▸ 39]*).
2. Add the GatewayNode to this project (see *Add GatewayNode [▸ 84]*).
3. Add the second locking device (see *Add LockNodes [▸ 97]*).
4. Program the LockNode of the second locking device and the second locking device (see *Programme locking device [▸ 112]*).
   ↳ Second system set up.
5. Remove the LockNode from the old locking device (see quick guide or manual).
6. Remove the LockNode from the second locking device (see quick guide or manual).
7. Install the LockNode of the old locking device in the second locking device.
   ↳ The locking device beeps and flashes red four times.
8. Remove the LockNode of the old locking device from the second locking device.

9. Reinstall the LockNode of the old locking device into the old locking device.
   - ↳ The locking device beeps and flashes red four times.

↳ LockNode is reset.

↳ Then reset the second locking device, LockNode and GatewayNode with SmartIntego Manager and the SmartIntego tool (WO) if necessary.

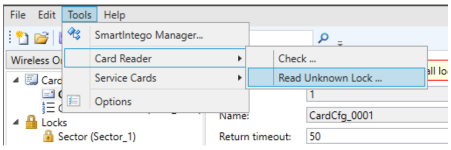
Re-set locking device

✓ SmartIntego-Tool (WO) opened.

✓ LockNode reset as described.

1. Position the programming device on the locking device (example: locking cylinder).

2. Read the locking device using | Tools | Card Reader and Read unknown lock.

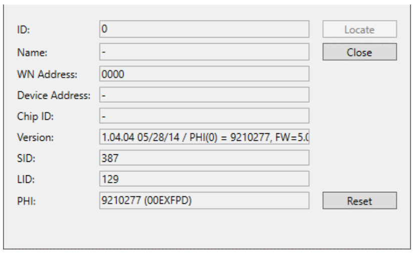


1

Name: CardCfg_0001

Return timeout: 50

   - ↳ Summary of the read locking device is displayed.



ID: 0

Name: -

WN Address: 0000

Device Address: -

Chip ID: -

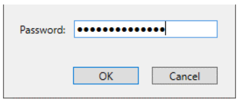
Version: 1.04.04 05/28/14 / PHI(0) = 9210277, FW=5.(

SID: 387

LID: 129

PHI: 9210277 (00EXFPD)

3. Click on the Reset button
   - ↳ Locking system password is queried.



Password: ••••••••••••••

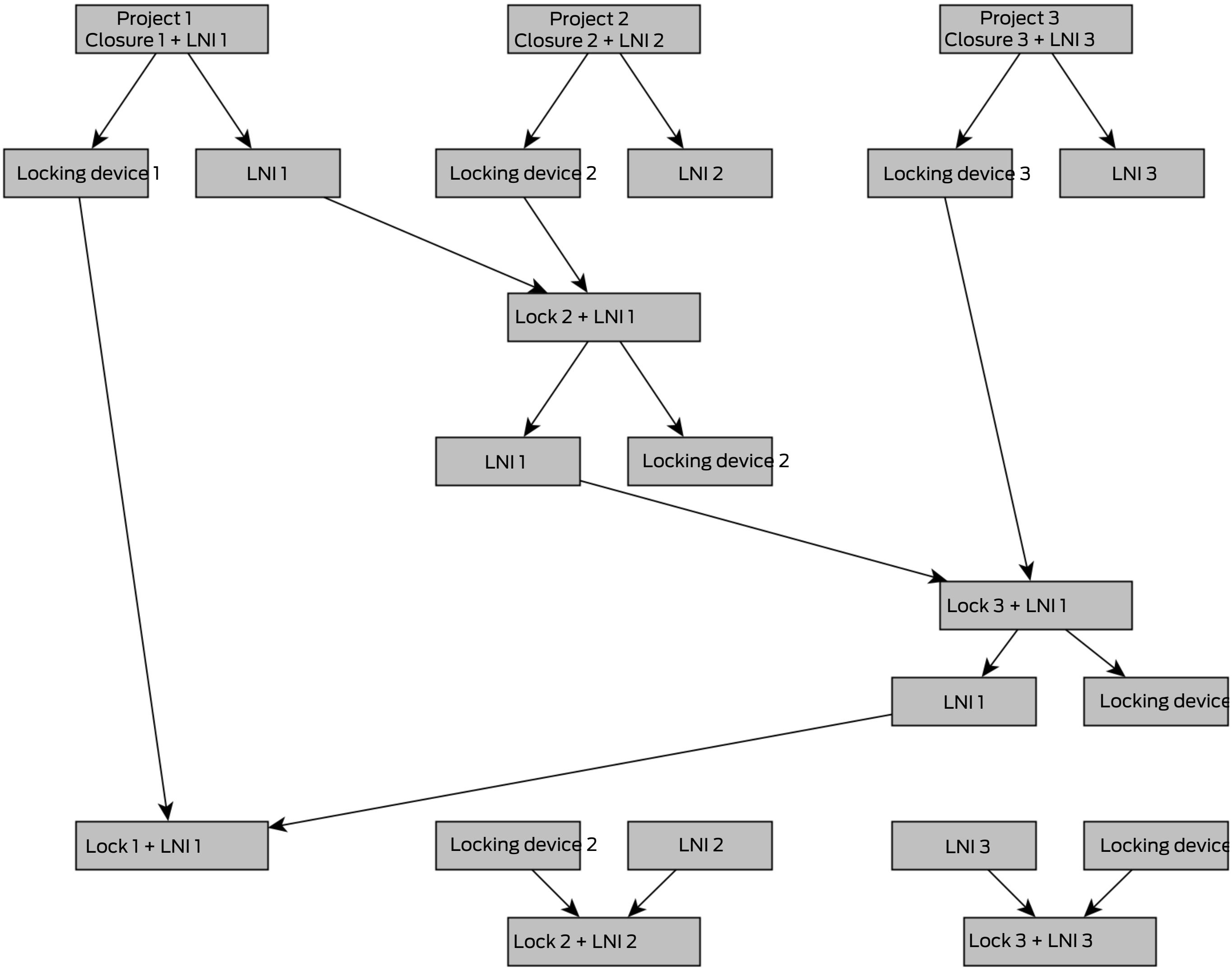
4. Enter the locking system password.

5. Click on the button OK.
   ↳ The locking device is reset.

↳ Locking device and LockNode reset.

6.15.2.2 Resetting the programmed LockNode and non-programmed locking device

Resetting the LockNode



✓ SmartIntego-Tool (WO) opened.

✓ Two additional locking devices of the same type available.

✓ Two GatewayNodes available.

✓ SI.SmartCD available.

1. In the SmartIntego tool (WO) l, create a second project with a different SID (see *Createing a SmartIntego project [▸ 39]*).
2. Add a GatewayNode to this project (see *Add GatewayNode [▸ 84]*).
3. Add the second locking device (see *Add LockNodes [▸ 97]*).

4. Program the LockNode of the second locking device and the second locking device (see *Programme locking device [▸ 112]*).
   ↳ Second system set up.
5. In the SmartIntego tool (WO) l, create a third project with a different SID (see *Createing a SmartIntego project [▸ 39]*).
6. Add the second GatewayNode to this project (see *Add GatewayNode [▸ 84]*).
7. Add the third locking device (see *Add LockNodes [▸ 97]*).
8. Programme the LockNode of the third locking device and the third locking device (see *Programme locking device [▸ 112]*).
   ↳ Third system set up.
9. Remove the LockNodes from all locking devices (see quick guide or manual).
10. Install the LockNode of the old locking device in the second locking device.
    ↳ The locking device beeps and flashes red four times.
11. Remove the LockNode of the old locking device from the second locking device.
12. Install the LockNode of the old locking device in the third locking device.
    ↳ The locking device beeps and flashes red four times.
13. Remove the LockNode of the old locking device from the third locking device.
14. Reinstall the LockNode of the old locking device into the old locking device.
    ↳ The locking device beeps and flashes red four times.
15. Reinstall the LockNodes of the second and third locking devices in the original locking devices.

↳ LockNode is reset.

↳ Then reset the second and third locking devices, LockNodes and GatewayNode with SmartIntego Manager and the SmartIntego tool (WO) l if necessary.

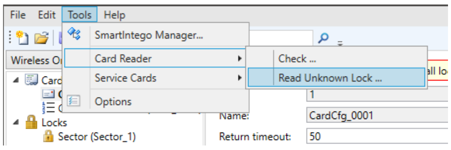
Re-set locking device

✓ SmartIntego-Tool (WO) opened.

✓ LockNode reset as described.

1. Position the programming device on the locking device (example: locking cylinder).

2. Read the locking device using | Tools | Card Reader and Read unknown lock.

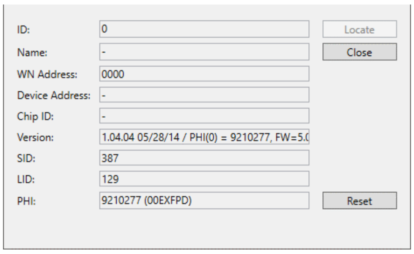


1

Name: CardCfg_0001

Return timeout: 50

↳ Summary of the read locking device is displayed.



ID: 0

Name: -

WN Address: 0000

Device Address: -

Chip ID: -

Version: 1.04.04 05/28/14 / PHI(0) = 9210277, FW=5.(

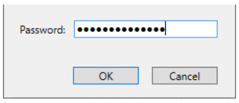
SID: 387

LID: 129

PHI: 9210277 (00EXFPD)

3. Click on the button Reset

↳ Locking system password is queried.



Password: ••••••••••••••

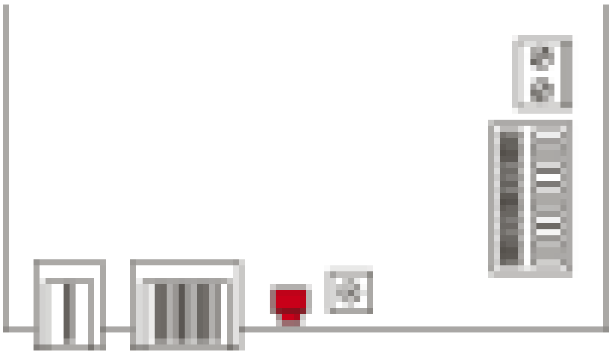
4. Enter the locking system password.
5. Click on the button OK.

↳ The locking device is reset.

↳ Locking device and LockNode reset.

6.15.2.3 Resetting the WaveNet/network configuration of the GatewayNode

If problems occur or you want to reset the component to the initial state, you can reset the component with the reset button (alternative: Reset via configuration page, see *Open configuration page [▸ 67]*: | CONFIGURATION | WAVENET and . Reset).



Make a distinction between them:

- Reset SmartIntego configuration: Reset all SmartIntego settings.
- Reset network configuration: Reset all network settings (IP address, DHCP settings, host name).

NOTE

IP address recovery

If the IP address is assigned by a DHCP server (default setting), the DHCP server assigns the IP address again directly after resetting (depending on settings of the DHCP server).

Reset the SmartIntego configuration

1. Disconnect the power supply (round plug or network cable for PoE).
2. Wait 20 seconds.
3. Press and hold the reset button.
4. Reconnect the power supply (round plug or network cable for PoE).
5. Release the reset button after one second.
   ↳ Component flashes green again (see Signalling).

↳ SmartIntego configuration is reset.

Reset network configuration

1. Disconnect the power supply (round plug or network cable for PoE).
2. Wait 20 seconds.
3. Press and hold the reset button.
4. Reconnect the power supply (round plug or network cable for PoE).

5. Release the reset button after five seconds.
   ↳ Component flashes green again (see Signalling).

↳ Network configuration is reset.

NOTE

Unauthorised access with standard access data

The standard access data can be viewed freely. Unauthorised persons cannot change the access authorisations, but they can change the network configuration. You will then no longer be able to reach the device via the network and will have to reset it.

Some browsers do not transmit spaces at the beginning of the password.

1. Change the default password.
2. Do not start or end the password with spaces.

You receive the component with the following factory configuration:

IP address	192168100100
User name	SimonsVoss
Password	SimonsVoss

The IP address of your device on your network can be determined using the free OAM tool (*https://www.simons-voss.com/de/downloads/software-downloads.html*). Please refer to the manual for more information.

6.15.3 Hardware reset of external LockNodes

You can reset WaveNet Manager-enabled LockNodes (recognisable by WN**M** in the article number):

1. Disconnect the LockNode from the power supply or remove the batteries.
2. Wait for about 20 seconds.
3. Press and hold the Init button.
4. Reconnect the power supply or replace the batteries.
   ↳ LED lights up constantly red.
5. Release the Init button while the LED is constantly red.

↳ All WaveNet information in the LockNode is deleted.

You can re-integrate the LockNode into your WaveNet (see WaveNet manual).

The SmartIntego variant (SI.N.IO) can only be reset in the SmartIntego Manager.

6.15.4 PIN code keypad

6.15.4.1 Set to storage mode

NOTE

If the SmartIntego PIN code keypad is to be used in a different system, the SmartIntego PIN code keypad not only needs to be deleted in the configuration view, but also set to storage mode.

The SmartIntego PIN code keypad can be reset to storage mode. This process also deletes all network settings.

NOTE

Enter the numbers consecutively. The SmartIntego PIN code keypad only signals the pressing of the keys, but not completion of the individual steps in the process.

1. Enter 000 00 (SI firmware from 31.14.16.12: Press the first 0 approx. 2s → flashes 2x orange).
2. Enter the Master PIN.

↳ SmartIntego PIN code keypad beeps and flashes green briefly twice.

↳ Storage mode set.

NOTE

If the SmartIntego PIN code keypad is already in storage mode, it cannot be set to storage mode again. In such a case, the process will be interrupted with a red flashing light and beeping for a long time.

6.16 Create and restore backup

Regular backups reduce the workload if the project file is lost, damaged or otherwise unusable.

The backup of the SmartIntego system is a copy of the project file (*.ikp). This file contains relevant hardware configuration data, e.g:

- Passwords
- Card configurations
- Locking device information from the last XML import
- Lock information from the last readout of the locking device

It is protected with the project password.

6.16.1 Create backup

After each use of the SmartIntego tool, copy the project file (*.ikp) to a secure location and protect it from loss.

Your IT department will help you develop a backup strategy.

6.16.2 Restore backup

If problems occur with the project file, you can import an existing backup.

The backup file is protected with the project password. You still need the project password to restore/edit the project file.

✓ Backup file available (see *Create backup [▸ 170]*).

1. Copy the last backup file known as working to your working directory.
2. Open the backup file with the SmartIntego tool.
3. Enter the project password.

↳ Configuration loaded at backup time.

NOTE

Restoring old versions

The hardware configuration in old backup files may differ from the current hardware configuration.

1. You still need the project password to recover/edit the project file.
2. If necessary, correct existing differences manually.

NOTE

Loss of the project file (*.ikp)

If the project file is lost despite a backed up environment and backup, you will no longer be able to continue working with the existing project.

1. Reset the locking devices with the locking system password.
2. If necessary, reset the LockNodes with a hardware reset.
3. If necessary, reset the GatewayNodes with a hardware reset.
4. Then reprogram the entire locking system.

7 Changelog

Versions	Changes	Chapter
01.00	FIRST RELEASE	...
01.01	Preparation AX	*Replace defective locking device [▸ 138]*
01.02	Several preparations for AX	Documents
01.03	Several preparations for AX	Documents
01.04	Internal Bugfixing	Documents
	New chapter	*Create and restore backup [▸ 169]*

8 Help and other information

Information material/documents

You will find detailed information on operation and configuration and other documents on the website:

www.smartintego.com/int/home/infocenter/documentation

Software and drivers

Software and drivers can be found on the website:

www.simons-voss.com/en/service/software-downloads.html

Declarations of conformity

You will find declarations of conformity and other certificates on the website:

www.simons-voss.com/en/certificates.html

Hotline

Our hotline will be happy to help you (landline, costs depend on provider):

+49 (0) 89 / 99 228 333

Email

You may prefer to send us an email.

si-support-simonsvoss@allegion.com

FAQs

You will find information and help in the FAQ section:

faq.simons-voss.com/otrs/public.pl

Address

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Germany

This is SimonsVoss

SimonsVoss, the pioneer in remote-controlled, cable-free locking technology provides system solutions with a wide range of products for SOHOs, SMEs, major companies and public institutions. SimonsVoss locking systems combine intelligent functionality, high quality and award-winning design Made in Germany.

As an innovative system provider, SimonsVoss focuses on scalable systems, high security, reliable components, powerful software and simple operation. As such, SimonsVoss is regarded as a technology leader in digital locking systems.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide (www.allegion.com).

Made in Germany

SimonsVoss is truly committed to Germany as a manufacturing location: all products are developed and produced exclusively in Germany.

ALLEGION™

SimonsVoss technologies

Made in Germany