

Wireless Gateway 90 40

Technical Manual
9040-K5



Contents

1	About this document	4
1.1	Validity	4
1.2	Target group	4
1.3	Contents and purpose	4
1.4	Additional documentation	4
1.5	Availability of additional documentation	4
1.6	Orientation in the document	5
1.7	Abbreviations/Definition of terms	5
1.8	Warnings	5
1.8.1	Hazard categories	5
1.8.2	Symbols	5
1.9	Notes	6
2	Basic safety instructions	7
2.1	Designated use	7
2.2	Qualification of persons	7
2.3	Assembly and installation	7
2.4	Accessories and spare parts	7
2.5	Service and maintenance	7
2.6	Data protection and privacy and IT security	8
3	Product description	9
3.1	Overview	9
3.2	Technical data	10
3.2.1	Interfaces	10
3.2.2	Power supply	10
3.2.3	Data retention	11
3.2.4	Ambient Conditions	11
3.2.5	Dimensions and weight	11
3.3	Conformity	12
3.4	Identification label	12
3.5	Open Source information	13
3.6	Accessories	14
3.6.1	Plug-in power supply	14
3.6.2	Wireless extender	14
3.6.3	Wireless USB stick	14
4	Construction and function	15
4.1	Device construction	15
4.2	LEDs	16
4.2.1	Meaning of LEDs on the front	16
4.2.2	Meaning of LEDs at Ethernet socket	17
4.3	System connection	17
5	Installation	18
5.1	Installation requirements	18
5.1.1	General	18
5.1.2	Installation location	18
5.2	Connecting the device	19
5.3	Wall mounting	20
6	Commissioning	21
6.1	Commissioning process	21
6.2	Service interface	23
6.2.1	Log in	23
6.2.2	Overview of service functions	24
6.2.3	Home	25

6.2.4	Wireless commissioning	26
6.2.5	Wireless components	27
6.2.6	Wireless extender	30
6.2.7	Events	31
6.2.8	Ethernet network	32
6.2.9	Wireless network	33
6.2.10	Diagnosis	34
6.2.11	Certificate	35
6.2.12	Import	35
6.2.13	Export	36
6.2.14	Password	37
6.2.15	About device	37
7	Maintenance	41
7.1	Restoring factory settings	41
7.1.1	Procedure	41
7.1.2	Effects on wireless components	41
7.1.3	Effects on wireless extender	41
7.1.4	Effects on the host system	41
7.2	System time	42
8	Packaging/return	43
8.1	Complete devices	43
8.2	Electronic component assemblies	43
8.3	Labelling	44
9	Disposal	45
10	Appendix	46
10.1	Commissioning wireless extender	46
	Key word directory	48

1 About this document

1.1 Validity

This document describes the product:

Product designation:	Wireless gateway 90 40
Firmware:	From 04.11.x onwards
Article number:	04045056
Product code:	9040-K5
Model:	MGW211-KAB7
Manufacturer:	Develco Products Tangen 6 8200 Aarhus N, Denmark

This document describes all product variants and all optional accessories and functions. Options are subject to a charge and are thus only available if they have been purchased. Additional accessories and functions may not be available on the date of publishing of the document and may only be available for purchase at a later point in time.

1.2 Target group

This document is intended for skilled personnel only.

1.3 Contents and purpose

Contents are limited to the assembly, installation, commissioning and basic operation of the product.

1.4 Additional documentation

- Planning Guideline Wireless
Information on planning of wireless systems

1.5 Availability of additional documentation

Additional documentation is available on the dormakaba extranet.

You will need a user account to access the extranet. A user account can be created directly. Detailed information about this is available on the homepage.

dormakaba extranet
<http://www.dormakaba.com/extranet-emea-en>



1.6 Orientation in the document

This document contains the following features to help find specific topics:

- The table of contents at the beginning of the document offers an overview of all topics.
- The header contains the associated main section.
- Cross references indicate the number of the chapter in which additional information can be found in each case. Example [▶ 5.7].
- An index in alphabetical order is given at the end of the document.

1.7 Abbreviations/Definition of terms

In order to make it easier to read the document, the following brief descriptions have been used:

Abbreviation/term	Description
wireless gateway	• Wireless Gateway 90 40
wireless extender	• Wireless Extender 90 41
wireless component	• evolo component, with the wireless option e.g. c-lever pro, digital cylinder • Remote reader 91 15 with extension module 90 43

1.8 Warnings

Warnings containing information/instructions and prohibitions designed to prevent personal injury or damage are specially marked.

Please pay attention to warnings! They are intended to help avoid accidents and prevent injury and damage.

1.8.1 Hazard categories

Warnings are divided into the following categories:



CAUTION

Low risk

Indicates a possibly dangerous situation which may lead to minor physical injury.



NOTICE

Important information on the correct use of the product.

Failure to comply with these instructions could lead to malfunctions. It is possible to damage the product.

1.8.2 Symbols

Symbols with the following meaning are used for warnings, depending on the source of danger.



General hazard



Danger of damage to electronic components from electrostatic discharge

1.9 Notes

Notes are indicated by an info symbol.



Tips and useful information.

These help you make the best use of the product and its functions.

2 Basic safety instructions

Read and observe this document before using the device to avoid any injury to persons or damage to property.

The manufacturer is not liable for damages caused by improper handling or incorrect installation.

2.1 Designated use

This device is intended for data transfer between an access control system and door components via radio.

Guidelines for meeting the requirements pertaining to intended use:

- Only use the components and assemblies approved by dormakaba.
- Follow the guidelines stated in this document.

Any other use is considered improper use.

2.2 Qualification of persons

The operations described in this document must only be carried out by skilled personnel. The skilled personnel must be trained and authorised by dormakaba.

The skilled personnel have suitable technical training and experience with the technology used. The skilled personnel are responsible for adhering to the conditions stated by the manufacturer and the applicable provisions and standards.

2.3 Assembly and installation

- The device may get damaged during transport or due to incorrect storage.
 - Check the device for visible damage.
 - Do not commission a damaged device.
- The installation location must meet the climatic and technical conditions of the manufacturer.

2.4 Accessories and spare parts

- Only use the components and assemblies approved by dormakaba.
- Follow the electrical specifications (voltage/power consumption).

2.5 Service and maintenance

- Retrofits and modifications are not permissible on the device.

2.6 Data protection and privacy and IT security

The device must be configured for safe operation.

Unauthorised access to the device and the system is possible without further security settings.

Security risks

- Violation of data protection and privacy through unauthorised access to person-related data.
- Unauthorised access
- Tampering/system failure

Recommended measures

- Device:
 - Keep the firmware current.
 - Before decommissioning: Reset the device to factory settings.
- Browser:
 - Activate secure encryption.
 - Do not save passwords in the browser.
 - Delete the history before closing the browser.
- System software:
 - Activate encrypted communication.
 - Switch off network ports that are not required.
 - Import the current patches.



The recommended actions are only relevant for connecting the dormakaba wireless gateway to the exivo system. We make no claim that the information is complete and up to date.

The facility operator of the system must ensure the protection of person-related data and IT security in their entire organisation by taking suitable measures.

3 Product description

3.1 Overview

The wireless gateway 90 40 acts as an interface between the host system and wireless components.

The wireless gateway supports the connection of up to 16 wireless components via its IEEE 802.15.4-compliant radio interface. 8 wireless extenders can be used per wireless gateway to extend the radio range.

A 10BASE-T/100BASE-TX Ethernet interface is available for communicating with the host system.

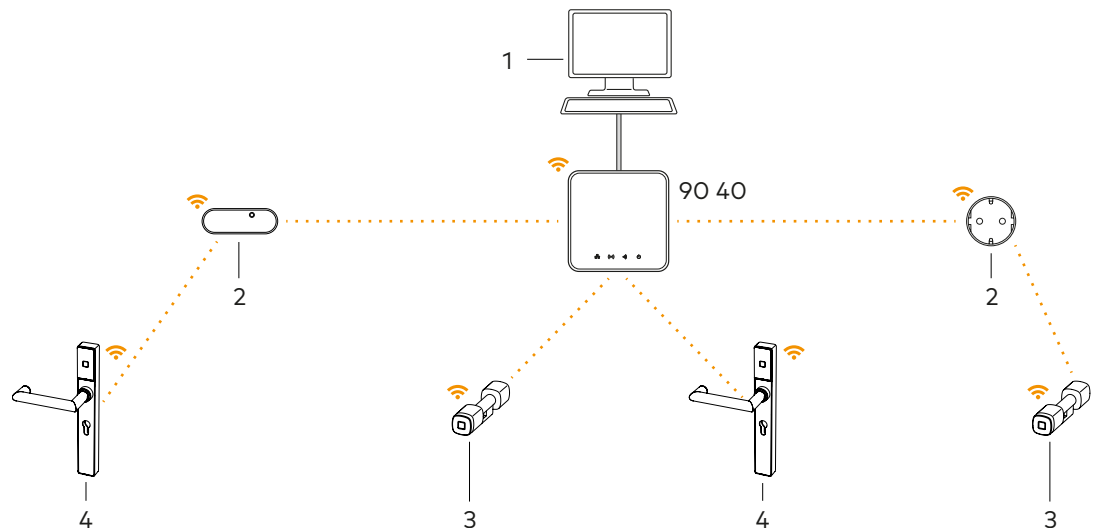
The device can be powered via Power over Ethernet (PoE) or via an external power supply.

The device has a status display and buttons.

The wireless gateway is installed indoors.

Topology

The graphic illustrates how the wireless gateway is integrated into a dormakaba system with wireless components and wireless extenders.



-  Wireless device
-  Wireless communication

- 1 Parent system
- 2 Wireless extender
- 3 Wireless component (digital cylinder)
- 4 Wireless component (c-lever pro)

3.2 Technical data

3.2.1 Interfaces

Ethernet

- 10/100 Mbit/s
- PoE as per IEEE802.3af
- Connector type: 8P8C (RJ45)

Wireless

- Radio interface, as per IEEE802.15.4, for connecting evolo components that are equipped with the wireless option
- Frequency: 2.4–2.4855 GHz
- Number of channels: 16
- Transmitting power
 - EU: +12 dBm
 - US: +18 dBm
- Receiver sensitivity: –101 dBm
- Data rate: 250 kbit/s
- Range: max. 30 metres (depending on the local conditions)

USB

- USB 2.0 (type A) for additional connectivity

3.2.2 Power supply

- **PoE**
PoE as per IEEE802.3af
- Optional with **plug-in power supply** (9 V DC)

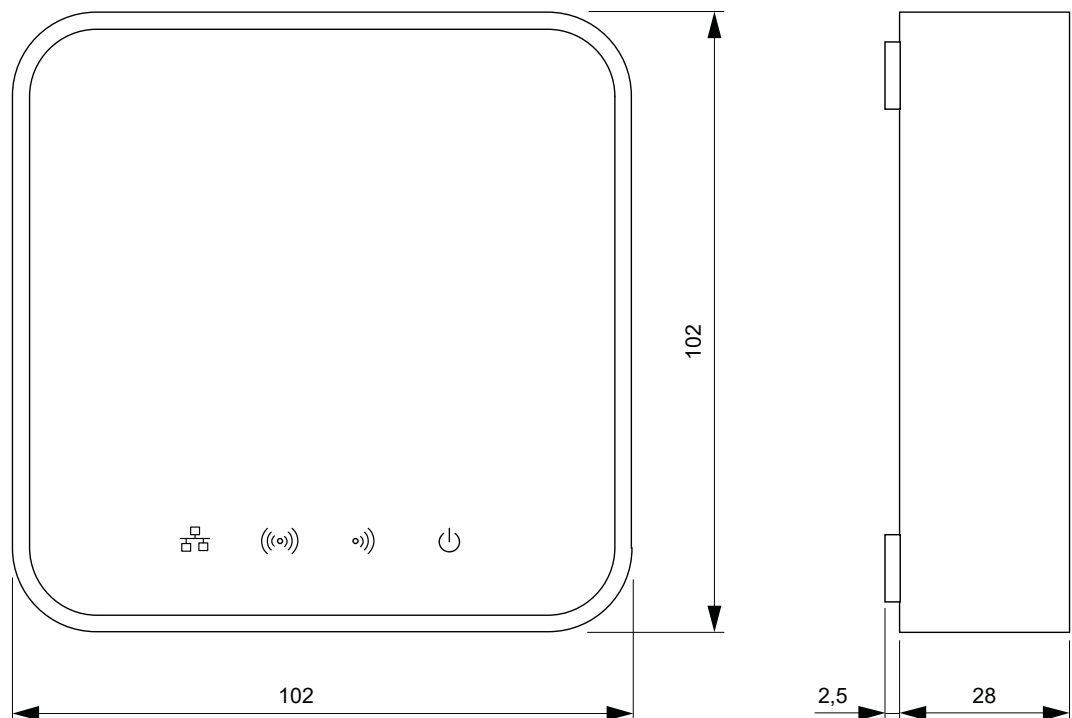
3.2.3 Data retention

The configuration data for the wireless gateway itself and for the connected wireless devices is located in a non-volatile memory and will be retained should there be a disruption to the power supply.

3.2.4 Ambient Conditions

- Class of protection: IP20
- Relative humidity: 5%–85%; non-condensing
- Operating temperature: 0 °C to +50 °C
- Use: in interior spaces

3.2.5 Dimensions and weight



- Dimensions in millimetres
- Weight: approx. 140 g

3.3 Conformity

Information about conformity is available in the quick guide.

Responsible manufacturer:

Develco Products
Tangen 6
8200 Aarhus N, Denmark

<https://www.develcoproducts.com/>



3.4 Identification label

The nameplate is situated on the rear of the device.

The identification label has the following:

- 1 Manufacturer
- 2 Article number
- 3 Product code
- 4 ZigBee: wireless MAC address
- 5 Ethernet: MAC address
- 6 Installation code (do not use)
- 7 Serial number
- 8 Model
- 9 QR code, contains:
 - Serial number (7)
 - Ethernet: MAC address (5)
 - Installation code (6)
 - Model (8)
 - ZigBee: wireless MAC address (4)
- 10 Approval marks



Do not use the installation code stated on the identification label.

Instead use the installation code generated from the system software.

3.5 Open Source information

The firmware contains packages that are subject to open source licenses.

dormakaba provides the following legal information for each firmware version:

- List of the open source packages
 - Name and version of the packages
 - Name and version of the licenses
- Detailed information on the individual packages
 - Detailed license texts
 - Information on copyright

The legal information can be accessed via the following ways:

- dormakaba extranet
 - The firmware and the legal information are packed in a ZIP file.
- Accessing the device via browser/console program

Disclaimer

In accordance with the conditions of the open source licences, dormakaba points out that the developers of packages have excluded any liability and warranty for the packages and their properties. The details are available in the respective licence conditions.

By pointing out this exclusion of liability, dormakaba exclusively fulfils the licence conditions of the packages. Legal and contractual claims against dormakaba are not affected by this exclusion of liability.

3.6 Accessories

3.6.1 Plug-in power supply

Plug-in power supply for supplying power to a compatible wireless gateway.

Technical data

- Input voltage: 100–240 V 50/60 Hz
- Output voltage: 9 V DC
- Output current: max. 2 A
- Coaxial connector 3.5/1.35

Pin assignment:



Compatibility

- 9240-K5 (only MGW211–KAB7)
- 9240-K7
- 9242-K7

- IEC/EN/UL/CSA 62368-1-certified

Order number: 04049253 (DE, VIS)

3.6.2 Wireless extender

If the wireless quality between a **wireless gateway** and a **wireless component** is not optimum, it can be improved using a **wireless extender**.

- Wireless extender 90 41, Schuko
The extender is plugged into a Schuko plug socket.
Order number: 04047513 (DE, VIS); 2030012709 (AT, HER)
- Wireless extender 90 41, cable
The extender is connected to the mains voltage through a permanent power supply.
Order number: 04047514 (DE, VIS); 2030012703 (AT, HER)

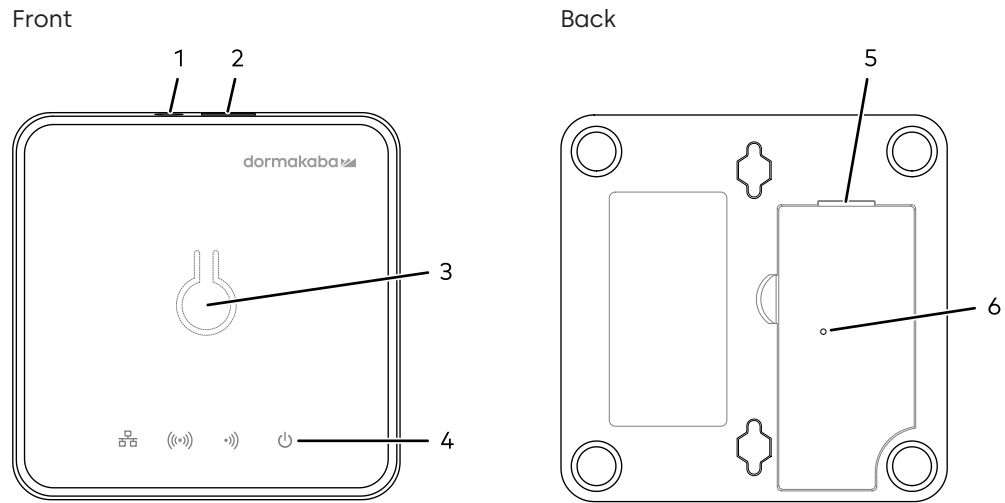
3.6.3 Wireless USB stick

The wireless USB stick is used along with the wireless site survey tool for range measurements.

Order number: 04046400

4 Construction and function

4.1 Device construction



- 1 Power supply input
- 2 Ethernet Interface
- 3 Range measurement button (not visible)
- 4 LED status display
- 5 USB interface (Type A)
- 6 Reset button

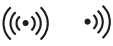
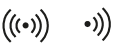
4.2 LEDs

4.2.1 Meaning of LEDs on the front

The 4 LEDs on the front signal the status of the device.

System start

The system is started in several phases and is signalled as follows.

LED	Status	Phase	After approx.
  	On	Bootloader starting up	0 s
  	Off	Barrel is being loaded	10 s
	Flashing 2x	Operating system starting up	20 s
	Flashing 1x	Operating system running Application starting up	40 s
	On (30 s) Off (1 s)	Application running System start completed	4 min

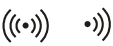
Operation

When in operation, the LEDs signal the status of the IP address, wireless components, and software.

LED	Status	Meaning
	Off	IP address is not assigned
	On	IP address is assigned
	Flashing	Default IP address is active (172.16.99.98)
	Off	Reserved for future function
	Off	No wireless component is connected to the wireless gateway
	On	At least one wireless component is connected to the wireless gateway
	Flashes slowly	Wireless commissioning active
	Flashes rapidly	Range measurement active
	Flashes 2x (10 s)	Range measurement could not be started
	On or off	Software error
	On (30 s) Off (1 s)	Software running System start completed

After pressing the reset button

The reset to factory settings takes place in several phases and is signalled as follows.

LED	Status	Phase
	Flickers	Reset triggered
	Flashing 2x	Barrel is being shut down
  	On	Bootloader starting up System start, see above

4.2.2 Meaning of LEDs at Ethernet socket

The 2 LEDs at the Ethernet socket indicate the status of the Ethernet interface.

LED	Status	Meaning
Yellow	Off	No network link
	On	Network link
Green	On	No data transfer
	On/flashing	Data transfer

4.3 System connection

The wireless gateway acts as an interface between the host system and evolo components equipped with the wireless option. The wireless gateway does not manage access control itself. It receives the relevant configuration for the connected wireless components from the host system and transfers this information to the wireless components.

Data exchange with the host system takes place via Ethernet, whilst data exchange with the wireless components takes place via radio.

Service functions such as network settings, firmware updates and certain wireless commissioning functions can be performed via the inbuilt service interface.

5 Installation

5.1 Installation requirements

5.1.1 General

Careful installation is essential in order to ensure the smooth functioning of the device. Therefore, the following installation instructions must be strictly adhered to.

5.1.2 Installation location

- The wireless gateway is designed for wall mounting. Alternatively, it is possible to simply place the device on the rubber feet. During wall mounting, it must be observed that the network and power cable on the top of the device have sufficient space.
- Only install the device in tamper-proof interiors.
- Do not install the device in metal cabinets or in environments that restrict radio performance.

Electromagnetic fields

Do not install the device in the vicinity of strong electromagnetic fields caused, for example, by switched-mode power supplies, electric power lines, phase control etc.

5.1.2.1 Determining the installation location

Before assembling the wireless gateway, ensure that the wireless components can be reached wirelessly.

Range measurement



The range measurement does not function together with wireless extenders. Range measurement mode will not be available if (a) one or more wireless components are already connected to the secured wireless network of the wireless gateway or (b) a user is logged in to the service interface of the wireless gateway.

This function provides the basis for deciding whether

- The device can be assembled in this location.
- The wireless network needs to be extended using wireless extenders.

Activating range measurement mode:

1. Press button (3) on the wireless gateway. [▶ 4.1](#)
 - ⇒ The device will indicate whether the range measurement started successfully. [▶ 4.2.1](#)
2. Hold the wireless test medium in front of the wireless component.
 - ⇒ The wireless component will indicate the reception quality by flashing.

Deactivating range measurement mode:

1. Press button (3) on the wireless gateway. [▶ 4.1](#)
2. Hold the wireless test medium in front of the wireless component.
 - ⇒ Range measurement mode is finished.

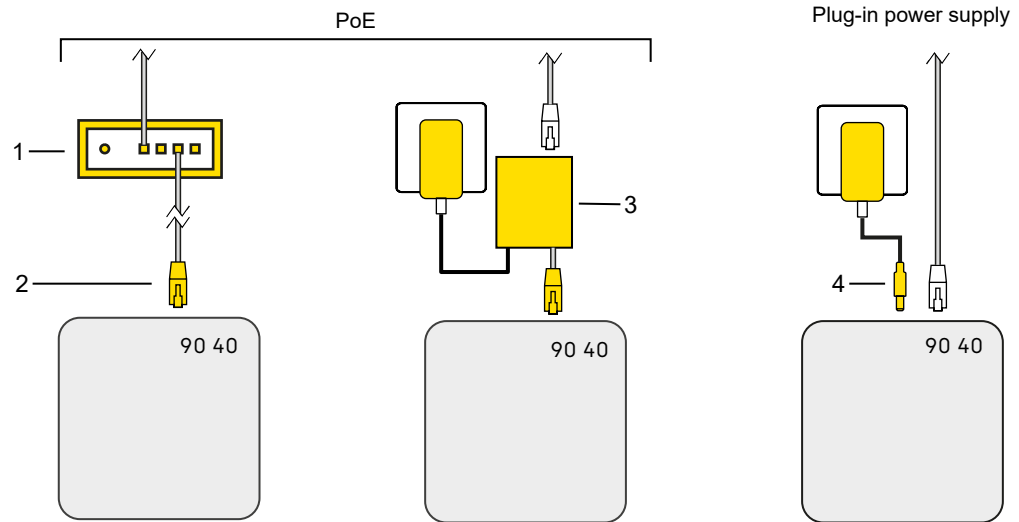
After a timeout, the wireless gateway and wireless components automatically exit range measurement mode.

Wireless site survey tool

The tool offers further options for measuring the range. See the quick guide for the wireless site survey tool and the wireless planning guideline.

5.2 Connecting the device

Depending on the power supply, connect the device as follows.



- 1 PoE switch
- 2 Network cable
- 3 PoE injector
- 4 Plug-in power supply (available as accessories, see Plug-in power supply [▶ 3.6.1](#))



To avoid damage to the device, never supply power to the device simultaneously via PoE and plug-in power supply.

Power supply via PoE

- ✓ PoE switch or PoE injector is available.
- 1. Plug the network cable into the Ethernet socket of the device.
- ⇒ The device is connected.

Power supply via plug-in power supply

- ✓ Plug-in power supply is available.
- 1. Plug the network cable into the Ethernet socket of the device.
- 2. Plug the coaxial connector into the low-voltage socket of the device.
- ⇒ The device is connected.

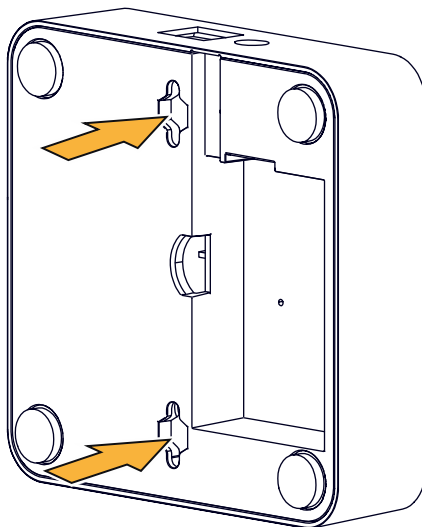
5.3 Wall mounting



Before the wall mounting, ensure that the wireless components can be reached wirelessly
[\[► 5.1.2.1\]](#).

Two slots are provided on the back of the device for fastening (see arrows).
The housing is to be fastened to the wall with the appropriate fastening material (screws/
dowels).

For wall mounting, it should be taken into consideration that the network cable and, if
necessary, the power supply lead have enough space on the top of the device.



6 Commissioning

6.1 Commissioning process

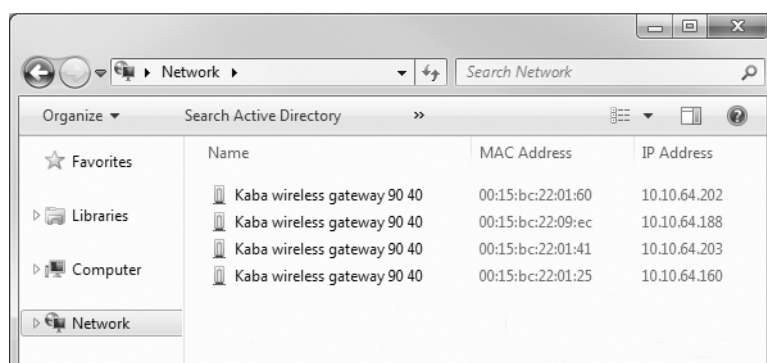
The first step in commissioning the wireless gateway involves localising the device in the Ethernet network.

UPnP

The wireless gateway supports the querying of network information via standard universal Plug and Play (UPnP). In order that a wireless gateway on the Ethernet network can be detected on a PC, support for UPnP on the PC is a requirement.

Windows displays UPnP devices on a network in Windows Explorer and supports direct access to the devices.

For a better overview, set the view of the network devices to Details in Explorer and add the MAC address and IP address columns.



When using multiple wireless gateways, use the Ethernet MAC addresses (EUI-48) to distinguish the devices on the network. The EUI-48 can be found on the nameplate.



- 1 ZigBee MAC address (EUI-64)
- 2 Ethernet MAC address (EUI-48)

Localisation via UPnP

- ✓ The network is equipped with an accessible DHCP server.
 - 1. Connect the gateway to the network and switch on.
 - 2. Localise the wireless gateway as a UPnP device in the computer's network environment.
 - 3. Search for the localised device's IP address.
- ⇒ The device can be found in the Ethernet network using the IP address.

Localisation via USB stick

Alternatively, the wireless gateway can write its IP address onto a USB stick in a text file.

- ✓ The network is equipped with an accessible DHCP server.
 - ✓ The USB stick is formatted in FAT32 format.
1. Insert the USB stick into the USB interface on the wireless gateway.
 2. Connect the wireless gateway to the network and switch on.
 3. After approx. 4 minutes, remove the USB stick if the Power LED signals that the boot process is complete.
- ⇒ The text file 'network_<MAC-address>.conf' containing the IP address in Classless Inter-Domain Routing (CIDR) format will be located in the USB stick's root directory:

Notation in accordance with CIDR: 172.16.99.98/16

corresponds to:	172.16.99.98	255.255.0.0
	IP address	Subnet mask



It is best to address the wireless gateway via a DHCP server. When doing so, ensure that the device always receives the same IP address (dynamic assignment: endless lease or manual assignment: linked to the MAC address) so that communication with the host system is maintained.

Default IP address 172.16.99.98

If no DHCP server is available in the network or the DHCP server does not reply, the device will assign itself the default IP address [▶ 6.2.8](#).

Changing the network settings

The second step is optional, and involves the allocation of a fixed IP address to the wireless gateway:

1. Enter the following into a browser's address field: `https://<IP address>`
2. Log in to the device with the following details: User: admin / Password: admin
3. Carry out changes [▶ 6.2.8](#).

This completes the process of commissioning the wireless gateway itself. Additional steps required, such as the wireless commissioning of wireless components, are carried out via the host system.

Some changes can also be made via the wireless gateway's service interface [▶ 6.2](#).

6.2 Service interface

To change the settings outside of a host system, there is a service interface on the device. Access is via the device's network connection, either directly or over the network. For a direct connection, an Ethernet crossover cable (crossed RJ-45 cable) or an Ethernet patch cable can be used 1:1 (Auto MDIX).

The service interface can be accessed via a PC by entering the device's IP address into your browser's address field.

HTTPS is activated on the wireless gateway as standard. Communication between the web server (wireless gateway) and the web browser (computer) is encrypted. Enter the following accordingly:

https://<IP address> **Example** https://172.16.99.97

If the wireless gateway's IP address is unknown, it can be determined via UPnP or written on to a USB stick [▶ 6.1](#).



On first access, the browser may warn that the certificate is unknown. In this case you must confirm that the page is trustworthy and can be displayed.

IT security Configure the browser so that the history is deleted after exiting. Do not open any other websites with the browser while accessing the service interface. Log out from the service interface and close the browser before accessing other websites.

6.2.1 Log in

After calling up the service interface, a user name and password will be requested.

The following users are stored as standard:

User	Password	Authorization
admin	admin	Write permission
reader	kabagateway	Restricted read permission

IT security It is essential that the passwords of the standard users are changed. [▶ 6.2.14](#)
Protect the changed passwords against access by third parties.

6.2.2 Overview of service functions

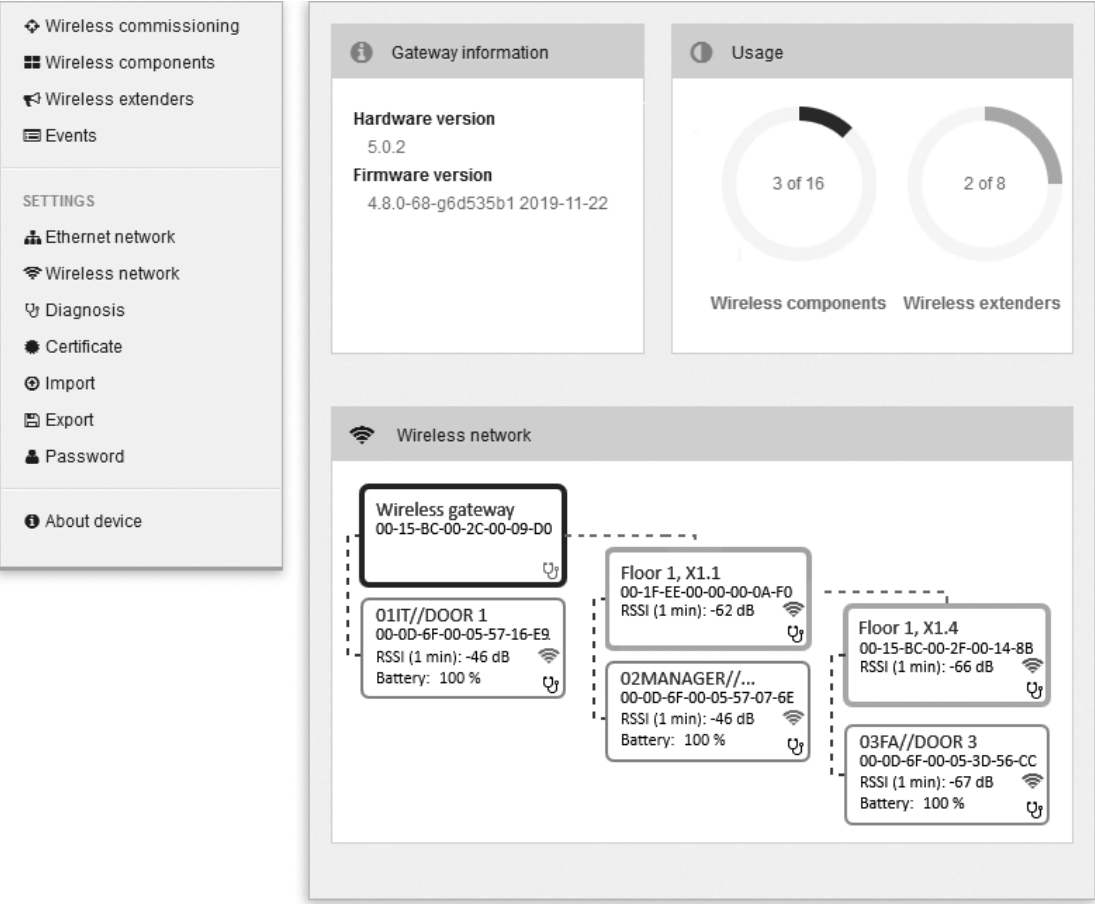
Menu	Description	
Homepage	Gateway information	Details of hardware and firmware version
	Usage	Number of connected wireless devices (wireless components, wireless extenders)
	Wireless network	Illustrated overview of connected wireless devices. Display of topology and connection quality if Diagnosis is activated.
Wireless Commissioning	Starting wireless commissioning to connect to wireless devices: - Wireless components (with installation code) - Wireless extenders (with HA Security)	
Wireless components	Details of wireless components already connected to the wireless gateway Editing functions are also available: Details > Identify, Edit, Disconnect	
Wireless extender	Details of the wireless extenders already connected to the wireless gateway Editing functions are also available: Details > Edit, Disconnect	
Events	Information on events (only for specialist personnel)	

Settings	Description	
Ethernet network	Settings for communication via the Ethernet network	
Wireless network	Settings for communication via the wireless network	
Diagnosis	Starting the wireless network diagnosis	
Certificate	Importing SSL certificates	
Import	Importing firmware to update wireless components	
Export	Download protocol files	
Password	Change passwords for the users admin and reader	
About the gateway	Gateway information	Information on the device's hardware and firmware and the wireless MAC address (EUI-64)
	System update	Importing firmware to update the wireless gateway
	Restart	Trigger restart
	Factory defaults	Trigger restoration of factory defaults

6.2.3 Home

Function call: **Homepage**

The homepage provides information about the wireless gateway and the connected wireless devices. The screenshot shows a device with connected wireless devices: three wireless components and two wireless extenders.



The information is grouped:

Gateway information	Hardware and firmware version of the device
Usage	Number of connected wireless devices
Wireless network	Illustrated overview of connected wireless devices

The dashed lines indicate the topology of the wireless network:

- "01IT/Door 1" is directly connected to the wireless gateway.
- "02Manager/Door 2" is connected to the wireless gateway via the wireless extender "Floor 1, X1.1".
- "03FA/Door 3" is connected to the wireless gateway via the wireless extenders "Floor 1, X1.1" and "Floor 1, X1.4".



Prerequisite for the display of topology and connection quality: Diagnosis is activated
[▶ 6.2.10\]](#)

6.2.4 Wireless commissioning

Wireless commissioning means connecting devices with the wireless gateway's secured radio network. Wireless devices, like wireless components and wireless extenders, must be commissioned in this way in order to guarantee the secure exchange of data between wireless components and the wireless gateway as an interface to the host system.

- **Wireless components (with installation code)**
The installation code generated by the host system is required by the wireless gateway and wireless components. Wireless commissioning is not possible without the host system.
- **Wireless extender (with HA Security)**
Commission wireless extender according to the Home Automation (HA) standard.

IT security Deactivate the wireless commissioning for the extender as soon as the desired extender is connected, in order to give potential attackers as little time as possible to connect their own extender.

Wireless commissioning process

Carry out wireless commissioning in the following sequence:

- 1 Wireless extenders (if present)
- 2 Wireless components

6.2.4.1 Carrying out wireless commissioning

Function call: **Menu > Wireless commissioning**

- ✓ The installation code [▶ 6.2.9](#) is transferred to the wireless gateway.
 - ✓ The installation code is transferred to the wireless components.
This is not required for wireless extenders.
 - ✓ Accessibility via radio [▶ 5.1.2.1](#) is ensured.
 - ✓ Wireless commissioning of the wireless extender (if present) or the wireless components is activated.
1. Choose **Wireless components (with installation code)**,
or
choose **Wireless extenders (with HA Security)** [▶ 10.1](#).
 2. Optionally adjust the **timeout (minutes)**, the time within which the wireless gateway remains open for connections.
 3. Activate **Wireless commissioning**.
⇒ The device searches for wireless components or wireless extenders.

Wireless commissioning

☒ Wireless components (with installation code)
☐ Wireless extenders (with HA Security)

Timeout (minutes)

Wireless commissioning **ON** (0 hours 29 minutes 55 seconds)

Searching...

4. Wait until the wireless component or the wireless extender is displayed under **Available devices**, i. e. is connected.
5. Deactivate **Wireless commissioning**.

- ⇒ The wireless component or the wireless extender is connected to the secure wireless network.

Wireless commissioning

☒ Wireless components (with installation code)
 ☐ Wireless extenders (with HA Security)

Timeout (minutes)

Wireless commissioning ☐ OFF

Type	Wireless MAC address	Wireless address	GUID address	Status
C-Lever	00-0D-6F-00-05-57-16-A1	0x8912	7878cff9-4a19-5d7b-93c5-1cd211970518	PERMIT NOTIFIED

6.2.5 Wireless components

Function call: **Menu > Wireless components**

In addition to displaying information about the connected wireless components, updates to the wireless component's firmware can be started via radio.

Available components										
Name	Compatibility	Wireless MAC address	Wireless-address	GUID address	Signal (RSSI)	Battery	Status	Actions	Update Selected	
01TITIDOOOR 1	✓	00-0D-6F-00-05-57-16-A1	0x4D85	8d3659d1-3c86-0048-b9d7-3dab5cd4e809	-42 dB	100%	INITIALISED	Details	BCLP42.34TAF → BCLP42.34TAF	
02MANAGERIDOOOR 2	✓	00-0D-6F-00-05-57-07-6E	0xB333	011386e-22f6-4a4a-8b76-0f248c2bfc32	-76 dB	100%	INITIALISED	Details	BDC42.34TAF → BDC42.34TAF	
										Update Selected

Name

A name chosen by the user for a wireless component, can also be assigned via the service interface [▶ 6.2.5.1](#).

Compatibility

Indicates whether the firmware version of a connected wireless component is compatible with the firmware version of the wireless gateway.

- ✓ = Compatible
No need for action.
- ! = Unknown, e. g. after a firmware update
Solution: Select **Identify** for the affected wireless component.
Function call: **Menu > Wireless components > Details > Identify**
- ⚡ = Incompatible
Solution: Update the firmware of the wireless component, see section "Carry out an update to wireless component's firmware" [▶ 6.2.5.1](#).

Wireless MAC address

The wireless MAC address (EUI-64) is a unique hardware address for a wireless network adapter.

Wireless address

The unique network address within a wireless network.

GUID address

The GUID address (Globally Unique Identifier) is a generated identifier for unique identification in a wireless system.

Signal (RSSI)

The RSSI value (Received Signal Strength Indicator) is the signal strength at which the wireless component receives data packages from its parent device (wireless gateway or extender).

Prerequisites for the display:

- Diagnosis is activated [▶ 6.2.10](#)
- Application version of the wireless component : ≥ 42.34

Battery

Battery charge status.

Status

The Status column indicates the wireless commissioning phase of a wireless component.

Status	Meaning
Unpermitted	The wireless component is connected but not yet confirmed by the host system.
Permitted	The host system has confirmed the wireless component.
Permit notified	The wireless component has received the confirmation notification.
Initialised	The host system has transferred the access configuration to the wireless component.

Actions

Additional functions are available under **Details** for further commissioning of the wireless components [▶ 6.2.5.1](#).

Update selected

In the overview, the device displays

- the firmware version imported to the wireless gateway for wireless components.
- the firmware version currently installed on the connected wireless components.

Carry out an update to wireless components' firmware:

- ✓ The battery's charge status is sufficient for the updating process.
 - ✓ The wireless components to be updated can be accessed via radio.
 - ✓ The diagnosis function is inactivated during the update process [▶ 6.2.10](#).
 - ✓ The firmware for the wireless component has been imported to the wireless gateway [▶ 6.2.12](#).
1. Choose the wireless components to be updated.
 2. Choose **Update selected**.
 - ⇒ The firmware will be transmitted via radio to the selected wireless components. It can take up to 60 minutes for the firmware to be transferred.
 - ⇒ The service interface reports whether the update was successful.

6.2.5.1 Details

Function call: **Menu > Wireless components > Details**

In addition to displaying information about the selected wireless components such as addresses, battery status, signal quality and firmware versions, updates to the wireless component's firmware can be started via radio. The **Reconnect**, **Identify**, **Edit** and **Disconnect** functions can also be called up.

Wireless component: 01IT//DOOR 1

Reconnect

Identify

Edit

Disconnect

Device information

Name

01IT//DOOR 1

Compatibility

✓

Type

C-Lever Pro

Wireless MAC address

00-0D-6F-00-12-0D-E9-C5

Wireless address

0x3692

GUID address

00000000-0000-0000-0000-000001100501

Status

INITIALISED

Battery

Type

AA

Status

100 %

from

28.11.2019, 12:18:23

Signal

RSSI

-42 dB

Firmware

Application version

BCLP42.34TAD

Wireless version

EvoLo 01.0603

Legic chipset information

4.2.0.0

Update

Available update

• BCLP42.34TAD

Update

Reconnect

Function call: **Menu > Wireless components > Details > Reconnect**

Manually reconnect the wireless component.

Wireless components automatically search for the parent device (wireless gateway or extender) with the best signal quality in greater intervals. If e.g. a wireless extender has been added, the connection to this wireless extender is immediately triggered.

Identify

Function call: **Menu > Wireless components > Details > Identify**

The function triggers signals (LED and acoustic signal generator) on the selected wireless component for 30 seconds. This clearly identifies the wireless components.

Edit

Function call: **Menu > Wireless components > Details > Edit**

Identified wireless components can be given a name to link them to a fixed installation location. The changed name, e.g. 'server room', is displayed in the wireless gateway's service interface and transmitted to the wireless components.



The host system can overwrite the name specified in the wireless gateway, if the wireless gateway is registered and configured in the system.

Disconnect

Function call: **Menu > Wireless components > Details > Disconnect**

This function disconnects the selected component from the secured wireless network.

Effects on wireless components

Disconnecting wireless components from the secured wireless network does not reset their settings. At these control points, access control continues in the same status as before disconnection.

Firmware update of wireless components

See section Update selected [▶ 6.2.5](#).

6.2.6 Wireless extender

Function call: **Menu > Wireless extenders**

Details of the wireless extenders connected to the secure wireless network.

Wireless extenders				
Available extenders				
Name	Wireless MAC address	Wireless address	RSSI	Actions
Floor 1, X1.4	00-15-BC-00-37-00-06-93	0x5A44	-67 dB 	Details
Floor 1, X1.1	00-15-BC-00-2F-00-0F-5D	0xA170	-62 dB 	Details

The overview displays some information about the wireless extenders:

Name

A name chosen by the user for a wireless extender, can also be assigned via the service interface [▶ 6.2.6.1](#).

Wireless MAC address

The wireless MAC address (EUI-64) is a unique hardware address for a wireless network adapter.

Wireless address

The unique network address within a wireless network.

RSSI

The RSSI value (Received Signal Strength Indicator) is the signal strength at which the wireless extender receives data packages from its parent device (wireless gateway or extender). Prerequisite for the display: Diagnosis is activated [▶ 6.2.10](#)

Actions

Additional functions are available under **Details** for further commissioning of the wireless extenders [▶ 6.2.6.1](#).

6.2.6.1 Details

Function call: **Menu > Wireless extenders > Details**

In addition to displaying information about the selected wireless extender on wireless address, manufacturer and version of the wireless extender and signal quality, the **Edit**, **Request version** and **Disconnect** functions are available.

Edit

Function call: **Menu > Wireless extenders > Details > Edit**

Identified wireless extenders can be given a name to link them to a fixed installation location. The name, e.g. 'Floor 1, X1.4', is displayed in the wireless gateway's service interface.



The host system can overwrite the name specified in the wireless gateway, if the wireless gateway is registered and configured in the system.

Request version

Function call: **Menu > Wireless extenders > Details > Request version**

Manually request the wireless extender version.

The extender version is requested automatically only in the case of wireless commissioning. After updating the wireless gateway firmware, you can request the extender version again as the gateway loses this information.

Disconnect

Function call: **Menu > Wireless extenders > Details > Disconnect**

The function disconnects the wireless extender from the secure wireless network.

6.2.7 Events

Function call: **Menu > Events**

Information on events (only for specialist personnel).

Events									
Available events									Refresh
Counter	Timestamp	Priority	Source	Groups	Log level	Message Id	Message	Parameters	
1227	Sat Sep 26 19:54:29 GMT 2015	NORMAL	GATEWAY_EVENT	100, 101	(5) NOTICE	12	Process completed with Success	- final_event: true - transaction_number: 34	
1226	Sat Sep 26 19:54:25 GMT 2015	NORMAL	GATEWAY_EVENT	100, 101	(5) NOTICE	12	Process completed with Success	- final_event: true - transaction_number: 36	
1225	Sat Sep 26 19:49:27 GMT 2015	NORMAL	GATEWAY_EVENT	100, 101	(5) NOTICE	12	Process completed with Success	- final_event: true - transaction_number: 30	
1224	Sat Sep 26 19:49:25 GMT 2015	NORMAL	GATEWAY_EVENT	100, 101	(5) NOTICE	12	Process completed with Success	- final_event: true - transaction_number: 32	
1223	Sat Sep 26 19:44:24 GMT 2015	NORMAL	GATEWAY_EVENT	100, 101	(5) NOTICE	12	Process completed with Success	- final_event: true - transaction_number: 26	
1222	Sat Sep 26 19:44:20 GMT 2015	NORMAL	GATEWAY_EVENT	100, 101	(5) NOTICE	12	Process completed with Success	- final_event: true - transaction_number: 28	
1221	Sat Sep 26 19:39:22 GMT 2015	NORMAL	GATEWAY_EVENT	100, 101	(5) NOTICE	12	Process completed with Success	- final_event: true - transaction_number: 22	

6.2.8 Ethernet network

Function call: **Settings > Ethernet network**

Ethernet Network

MAC address 00:15:BC:22:01:34

UPnP ☒ ON

DHCP ☒ ON

IP address

Subnetmask 24 (255.255.255.0)

Default gateway

DNS address 1

TLS 1.2 and later ☒ ON

Save changes

UPnP

In its factory state, Universal Plug and Play (UPnP) is activated for easy localisation in the Ethernet network.

Deactivate UPnP by turning the UPnP switch to **Off**.

Assigning a fixed IP address

In its factory state, DHCP is activated.

1. Deactivate DHCP by turning the DHCP switch to **Off**.
2. Enter the desired address in the **IP address** field.
3. Under **Subnet** mask, select a network mask.
4. Under **Standard gateway** you have the option to enter the IP address of the Ethernet gateway, which enables communication with the host system if the devices are not located in the same network segment.
5. Under **DNS address**, you have the option of entering the IP address of a DNS server.
6. Select **Save**.

Get IP address from the DHCP server

1. Activate DHCP by turning the DHCP switch to **On**.
2. Select **Save**.

Default IP address 172.16.99.98

To guarantee the accessibility of the wireless gateway, the device reverts to its default IP address if there is no DHCP server in the network or if the DHCP server does not respond. The device signals [▶ 4.2.1](#) the activation of the default IP address.

Requirements for activation of the default IP address

- Device is in DHCP mode
- Network cable is plugged into the device and a network link [▶ 4.2.2](#) is produced

Boot process

If the DHCP server is not accessible during the boot process, the device will assign itself the default IP address.

Normal operation

If the DHCP server is no longer accessible in normal operation, the device can assign itself the default IP address. This depends on the configuration of the DHCP server, e.g. the lease duration.

Deactivating the default IP address

- Switch off the device and switch it on again as soon as the DHCP server is accessible again. The IP address assigned by the DHCP server will be restored.
- Assign the device a fixed IP address [\[► 6.2.8\]](#)

TLS

In its factory state, TLS 1.2 is inactivated. This means that the encryption protocols TLS 1.0 and TLS 1.1 are activated. In this way, the communication with a host system that does not support TLS 1.2 is ensured.

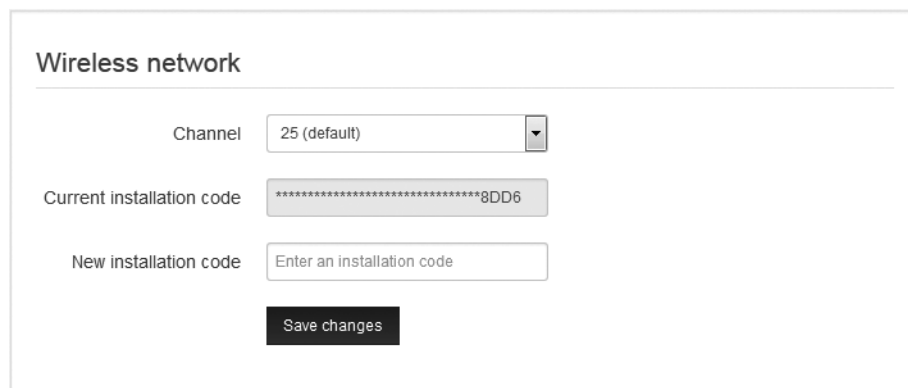
IT security We strongly advise you to activate **TLS 1.2 and later** to securely encrypt the communication if the host system supports it. Inactivate it only if the host system does not support it.

Also see about this

 Commissioning process [\[► 21\]](#)

6.2.9 Wireless network

Function call: **Settings > Wireless network**



Wireless network

Channel

Current installation code

New installation code

Save changes

Channel

Option of changing the ZigBee channel over which the wireless gateway communicates with the connected wireless devices.

Changing the channel

1. Under **Channel**, select a ZigBee channel.
2. Select **Save**.

⇒ The device communicates over the newly selected channel. Connected wireless devices automatically transfer over to the new channel within approx. six minutes.

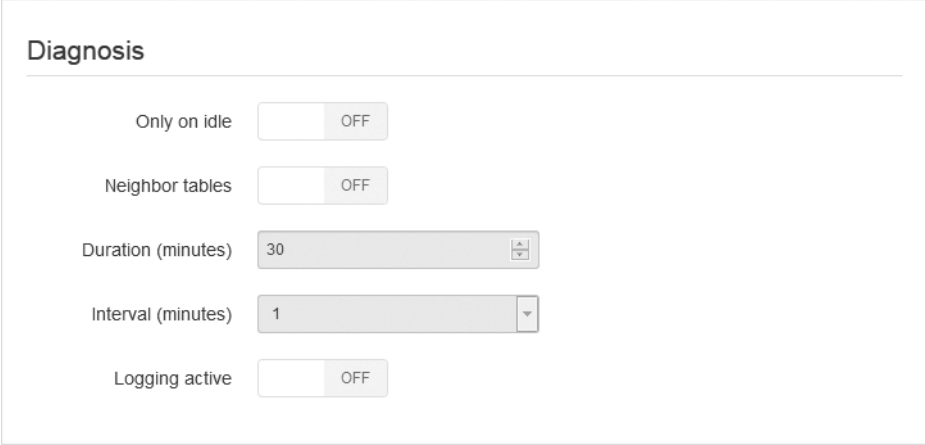
Installation code

The service interface masks the active installation code, as the code is used to encrypt the radio communication. The installation code is generated by the host system and transmitted to the wireless gateway.

The installation code can be manually entered in the field **New installation code**.

6.2.10 Diagnosis

Function call: **Settings > Diagnosis**



Diagnosis

Only on idle ☐ OFF

Neighbor tables ☐ OFF

Duration (minutes) 30

Interval (minutes) 1

Logging active ☐ OFF

The diagnosis is inactivated by default as the function shortens the service life of the batteries of wireless components.

The wireless gateway carries out the following functions if the diagnosis is activated:

- The device shows the wireless network topology on the homepage [▶ 6.2.3](#).
- The device shows the signal strength (RSSI) for wireless extenders and wireless components.
- The device writes log files for analysing the wireless network [▶ 6.2.13](#) for the specified duration.

Only on idle

If activated, the wireless gateway does not carry out the diagnosis process if the device is used by another process.

Activate if the diagnosis should run for a long period.

Neighbor tables

If activated, the wireless gateway also records information about neighbors of wireless extenders (mesh network) in addition to the quality of connection to wireless components and wireless extenders.

Important in analysing wireless extenders (mesh network).

Requirement: Use of multiple wireless extenders that reach each other.

Duration

Choose the period for diagnosis (max. 999,999,999 minutes ~ 1,900 years).

Interval

Choose the regular time interval in which the device requests diagnosis data.

Logging active

Activate diagnosis by turning the switch to **On**.

Requirement: The wireless gateway has the current system time [▶ 7.2](#).

6.2.11 Certificate

Function call: **Settings > Certificate**

HTTPS is activated as standard to ensure secure communication via the Ethernet interface of the wireless gateway. Both direct communication with the service interface of the wireless gateway and communication by the host system with the wireless gateway are encrypted.

The SSL certificate integrated in its factory state can be replaced:

- with a certificate from a certifying body
- with a self-signed certificate.

Possible import formats:

Format	Coding	File name extension
X509	PKCS12	.p12 .pfx
	JKS	.jks

Uploading a certificate

- ✓ The certificate is <10 KB.
 - ✓ The certificate file contains no more than one private key.
 - ✓ The certificate can be password-protected.
 - ✓ If the private key is password-protected, then the certificate file must be protected with the same password.
1. Select **Browse** and navigate to the certificate.
 2. If the certificate is password-protected, enter the password.
 3. Select **Upload**.
 - ⇒ The certificate is uploaded to the wireless gateway.
 4. Select **Activate certificate**.
 5. Select **Activate** again in the next dialogue window.
 - ⇒ The wireless gateway's web server will restart.
 6. Call up the service interface (IP address) again in the browser.
 - ⇒ The uploaded certificate secures the communication with the wireless gateway (service interface and interface to the host system).



Once a different certificate has been activated, the standard certificate can only be reset by restoring the factory settings [▶ 7.1](#).

6.2.12 Import

Function call: **Settings > Import**

Import of firmware for update of connected wireless components.

The wireless gateway saves a firmware version for each type of wireless component, such as the c-lever and digital cylinder.

Update the firmware of wireless components

If the firmware was imported to the wireless gateway, carry out an update for each wireless component [▶ 6.2.5](#) under **Menu > Wireless components > Details**.

6.2.13 Export

Function call: **Settings > Export**

Log files for analysis (only for specialist personnel).

Export			
Available files			
Filename	Size	Last modified	Actions
java0.log.0	14 KB	Tue Sep 17 16:36:14 GMT 2019	Download
java0.log.1	244 KB	Tue Sep 17 16:18:57 GMT 2019	Download
messages	195 KB	Mon Sep 16 14:12:13 GMT 2019	Download
messages.0	200 KB	Tue Aug 13 19:22:02 GMT 2019	Download
messages.1	200 KB	Wed Aug 07 17:31:32 GMT 2019	Download
upgradeserver.log	388 bytes	Fri Sep 13 09:02:06 GMT 2019	Download
upgradeserver.log.1	937 bytes	Fri Sep 06 13:54:40 GMT 2019	Download
watchtower.log	33 KB	Tue Sep 17 07:20:57 GMT 2019	Download
zigbee_neighbortable.csv.0	4 MB	Tue Sep 17 16:34:59 GMT 2019	Download
zigbee_neighbortable.csv.1	12 MB	Mon Sep 16 16:08:01 GMT 2019	Download
zigbee_networkdiagnosis.csv.0	8 MB	Tue Sep 17 16:35:00 GMT 2019	Download
zigbee_networkdiagnosis.csv.1	12 MB	Thu Sep 12 21:39:15 GMT 2019	Download

To export data, select **Download** for the required log file.

The log files contain entries on the areas:

- **Java: Device application**
When a file is full, the device writes in the other log file.
After a restart, the device always writes in the java0.log1 file.
- **Messages: Linux kernel**
When a file is full, the device writes in the other log file.
- **Upgrade server: Update of the ZigBee chip**
After a restart, the device always writes in the other log file.
- **Watchtower: Monitoring the processes on the device**
The device always writes in the one log file.
- **ZigBee neighbor table: Wireless extender neighbors (mesh network)** [▶ 6.2.10](#)
When a file is full, the device writes in the other log file.
- **ZigBee network diagnosis: Quality of connection to wireless extenders and components (including parent device)** [▶ 6.2.10](#)
When a file is full, the device writes in the other log file.

6.2.14 Password

Function call: **Settings > Password**

Change password

User:

Current password:

New password:

Confirm new password:

IT security It is essential that the passwords of the standard users are changed. [▶ 6.2.1](#)
Protect the changed passwords against access by third parties.

Communication between the host system and the wireless gateway is also password-protected. This password is separate from the passwords for users of the wireless gateway service interface.



Resetting to factory settings resets all passwords to the factory-set passwords. [▶ 7.1](#)

6.2.15 About device

Function call: **Settings > About the gateway**

About device

Gateway information

Wireless MAC address
00-15-BC-00-2C-00-6F-26

Hardware version
5.0.2

Firmware version
4.8.0-68-g6d535b1 2019-11-22

Kernel version
Linux 4.4.187

OS version
1.3.3273-1.3.30-dormakaba20191114

ZigBee Version
3.12.13

System update

A downgrade from version 4.4.1 to an older Version is not possible

In addition to displaying information on the wireless gateway's hardware and firmware, the following options are available here: restart, factory reset, firmware update.

6.2.15.1 Restart

Trigger the restart of the device by selecting **Restart**, or disconnect the device from the power supply.

Effects of the restart

- Duration of up to 10 minutes.
- The restart does not change settings and data on the wireless gateway. It is not necessary to repeat the wireless commissioning process.
- During the restart, the access control is continued at connected access points.



The internal clock of the device is reset if the device has been disconnected from the power supply. Ensure correctness of the system time with the help of the host system. [▶ 7.2\]](#)

6.2.15.2 Factory reset

Trigger a factory reset of the device by selecting **Factory defaults**, or the reset button on the back of the device.

For effects of a factory reset, see paragraph Restoring factory settings [▶ 7.1\]](#).

6.2.15.3 Firmware update

IT security Protect the image file of the wireless gateway firmware against access by third parties.

Launch updates to the wireless gateway's firmware

1. Select **Browse file** and navigate to the wireless gateway's firmware.
 2. Select **Open**.
 3. Select **Update**.
- ⇒ The firmware is loaded onto the wireless gateway and the device restarts with the updated firmware.



Firmware Version 4.1.1

Proceed in 2 stages when updating from a gateway firmware before version 4.4.1 to a version after version 4.4.1.

Stage 1: Upgrade to firmware version 4.1.1. Observe the section "Instruction for the firmware update" in the Product Information for version 4.1.1.

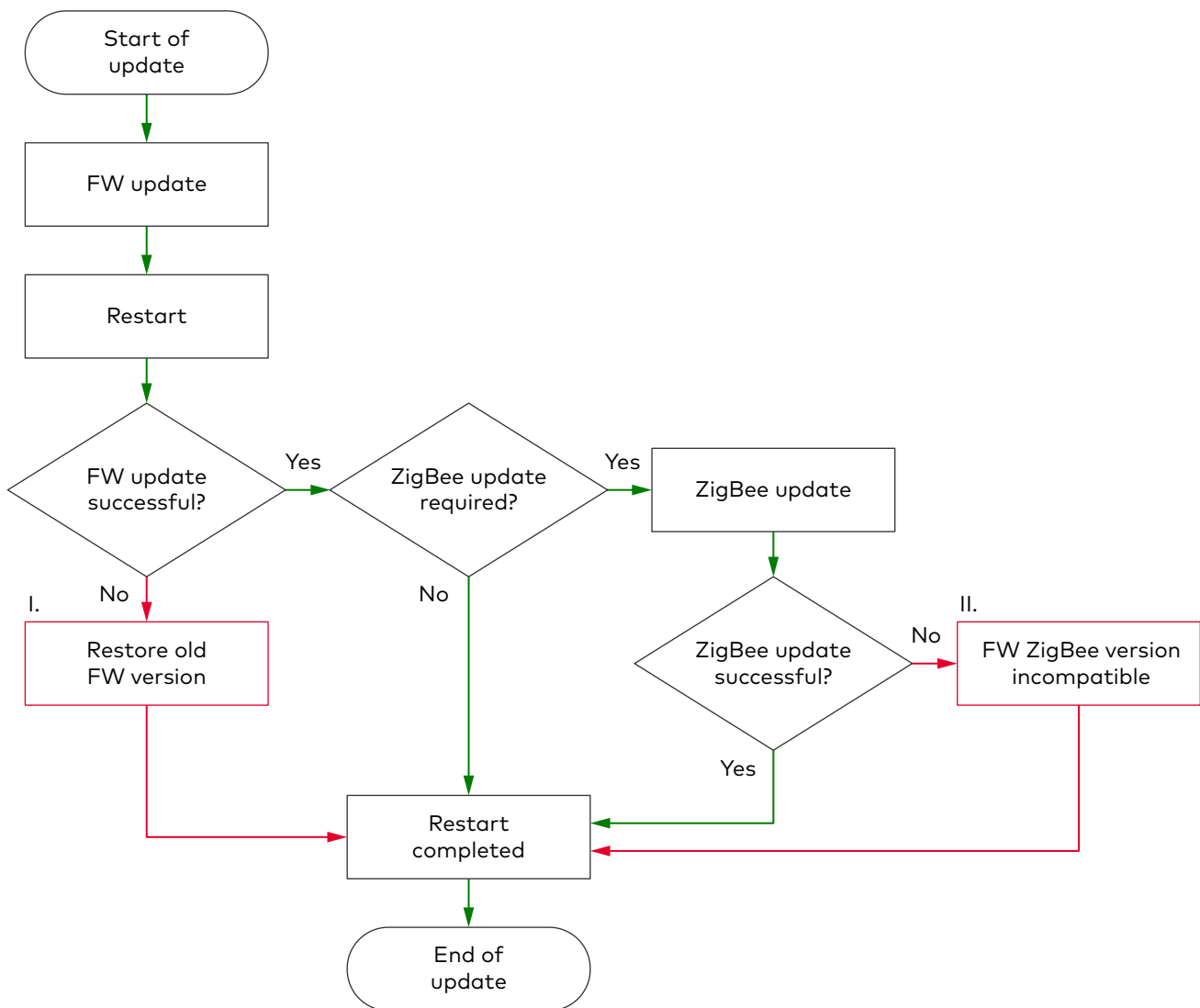
Stage 2: Update to the later firmware version.

Effects of the update

- The update does not change settings and data on the wireless gateway. It is not necessary to repeat the wireless commissioning process.
- During the update, the access control is continued at connected access points.

Update process

The flowchart shows the process of the firmware update on the wireless gateway.



Errors can occur in 2 phases of the workflow.

I. The device restores the initial condition if the firmware update fails.

Measures

- Restart firmware update.
- Contact Support if the update fails again.

II. In case of a partially failed update, the device is only functional to a limited extent. The updated device firmware is not compatible with the ZigBee firmware version that is not updated. The ZigBee function of the device is deactivated in this case.

Measures

Perform these steps until the device is again fully functional.

- Download log files for analysis purpose [▶ 6.2.13](#).
- Restart (via the service interface) [▶ 6.2.15](#).
ZigBee update now successful?
- Restart (disconnect device from the power supply)
ZigBee update now successful?
- Carry out factory reset [▶ 7.1](#).
ZigBee update now successful? If yes, carry out commissioning.

- Carry out downgrade of the device firmware [▶ 6.2.15.4](#) and commissioning. The device is fully functional with the old firmware version. Contact Support to initiate further steps.
- Send device in for repair [▶ 8](#).

6.2.15.4 Firmware downgrade

The device supports the installation of firmware versions for the wireless gateway which are older than the installed firmware version.

Downgrading the firmware version will restore the device's factory defaults.

The wireless commissioning process will need to be carried out again.

The connection to the host system, the wireless components and, if necessary, the wireless extenders, needs to be re-established [▶ 7.1.2](#).



A downgrade of the firmware for the wireless gateway may only be performed in consultation with Support.



Firmware version 4.1.1

A downgrade to wireless gateway firmware older than version 4.1.1 is not possible if the firmware version 4.1.1 or a subsequent version up to 4.7 is installed on the device.



Firmware version 4.8.1

A downgrade to wireless gateway firmware older than version 4.8.1 is not possible if the firmware version 4.8.1 or a subsequent version is installed on the device.

7 Maintenance

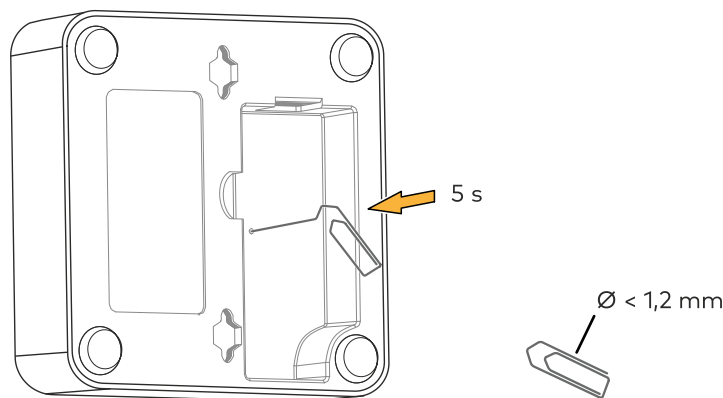
7.1 Restoring factory settings

In Wireless Gateway 90 42, the factory reset is triggered when the gateway is deleted in exivo (partner and client application).

7.1.1 Procedure

Trigger a factory reset of the device via the service interface [▶ 6.2.15](#) or the Reset button at the back of the device.

- ✓ The back of the device is accessible.
 - ✓ The device is connected to the power.
 - ✓ Use a paper clip or similar with a maximum diameter of 1.2 mm.
1. Press the Reset button on the back of the device for five seconds.
 - ⇒ The power LED will flash for approx. five seconds. [▶ 4.2.1](#)
 - ⇒ The wireless gateway will restart and load the factory defaults.



7.1.2 Effects on wireless components

- The settings on connected wireless components are not reset by restoring the factory settings on the wireless gateway. At these control points, access control continues in the same status as before resetting the device.
- The wireless components can no longer find the wireless gateway after the reset. The wireless commissioning must be carried out again to include the wireless components back into the secured wireless network. First carry out an INI reset and then connect the wireless components again.
- To reset the settings of the wireless components in a similar manner, proceed as per the installation instructions of the wireless component.

7.1.3 Effects on wireless extender

- Wireless extenders are disconnected from the wireless gateway by restoring the factory settings on the wireless gateway. Carry out wireless commissioning again to include the wireless extenders back in the secured wireless network.

7.1.4 Effects on the host system

- The settings of the parent system are not reset by restoring the factory settings on the wireless gateway.

- In order to re-establish a connection with the reset wireless gateway, carry out the commissioning again. [▶ 6.1](#)

7.2 System time

The wireless gateway receives the system time from the host system and forwards it to the connected wireless components. The availability of the host system is a requirement for ensuring the long-term accuracy of the system time for the wireless gateway and the wireless components.

After disconnecting from the mains, the gateway requires up-to-date time information. In the event that the host system cannot be reached, the wireless gateway does not have access to valid time information. Wireless components do not accept invalid time information but operate to their internal clock until the wireless gateway has received up-to-date time information and has transferred it by radio.



In the event of a power failure, it must be ensured that the wireless gateway is receiving time information from the host system.

8 Packaging/return

Improperly packed assemblies and devices may incur costs due to damage during transport.

Please observe the following instructions when shipping dormakaba products.

dormakaba is not liable for damage to products caused by inadequate packaging.

8.1 Complete devices

The original packaging is specially made for the device. It provides optimum protection against transport damage.



Always use the original packaging to return the device!

If this is not possible, you must provide packaging which will prevent any damage to the device.

- Use a sturdy, thick-walled transport case or a box. The transport case should be large enough to allow 8–10 cm clearance between the unit and container wall.
- Wrap device in a suitable foil or place in a bag.
- Pad heavily around the device with foam padding or air bags, for example. The device must not be able to move around within the packaging.
- Use dust-free, environmentally friendly fill material.

8.2 Electronic component assemblies



Store, transport and ship ESD-sensitive electronic component assemblies such as PCBs and readers in packaging with suitable ESD protection. Electronic component assemblies must be packed at ESD-protected workstations. This should be carried out by persons who are familiar with and comply with general ESD protection regulations.

Electronic component assemblies must be returned in packaging with sufficient ESD protection to

- make warranty claims in the event of malfunctions of any type.
- Delivery of replacements for electronic PCBs and components in replacement procedure.

Electronic components shipped in packaging without adequate ESD protection will not be analysed or repaired to maintain a high quality standard; they will be taken directly to disposal instead.

8.3 Labelling

Including all returns paperwork and labelling the package correctly enables us to process your case quickly. Please ensure that a delivery note is enclosed in each package. The delivery note should contain the following information:

- Number of devices or components in each package.
- Article numbers, serial numbers, designations, order number.
- Address of your company/contact person.
- Reason for return, e.g. repair exchange.
- Accurate description of fault.

Returns from countries outside the EU also require a customs invoice with an accurate customs value and customs tariff number.

9 Disposal



The device is indicated with the adjacent symbol which means prohibition of its disposal as household waste.

The device's integral components must be separated before they are taken for recycling or disposal. Old and used devices contain valuable recyclable materials which must be recycled. Toxic and hazardous components may cause long-term damage to the environment if you dispose of them incorrectly.

The facility operators are obliged to return electrical and electronic devices to their manufacturer, point of purchase or designated public collection points at the end of their service life.

Disposal in Germany:

dormakaba EAD GmbH will take responsibility for correct disposal of supplied goods once they are no longer in use as per statutory regulations (ElektroG in Germany). The owner of the used electrical appliance bears any costs incurred for transport to the manufacturer's plant.

Disposal in Switzerland:

The device is to be returned to an electrical appliance return point as per the Regulation on Returning, Taking Back and Disposing of Electrical and Electronic Equipment (VREG).

In the EU, electrical appliances should be taken for disposal in accordance with the country's respective disposal and environmental guidelines.

Deletion of personal data

The owner/operator is responsible for deleting their personal data.



Dispose of packaging in an environmentally responsible fashion.

The packaging materials are recyclable. Do not dispose of packaging in the household waste; take it to a recycling point instead.

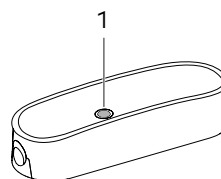
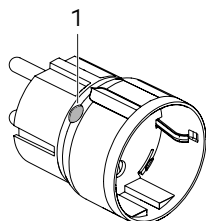
10 Appendix

10.1 Commissioning wireless extender

Commissioning of the wireless extenders is carried out solely via the wireless gateway service interface. Host systems from dormakaba do not show wireless extenders and do not support their commissioning.

Wireless extender 90 41

This section solely describes the commissioning of the wireless extender 90 41. See manufacturer's documentation for further information.



- 1 LED status indicator and push button (transmission of electricity on/off and reset)

Commissioning wireless extender 90 41

Activate wireless commissioning on the wireless gateway and wireless extender to connect the extender to the secured wireless network of the gateway.



Always activate wireless commissioning only on one wireless gateway so that a wireless extender does not connect to a different wireless gateway than desired.

1. Navigate to **Menu > Wireless commissioning** in the gateway service interface and activate **Wireless extenders (with HA Security)**.

Wireless commissioning

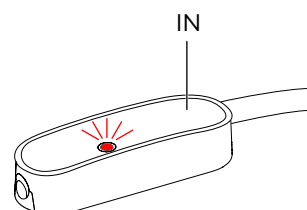
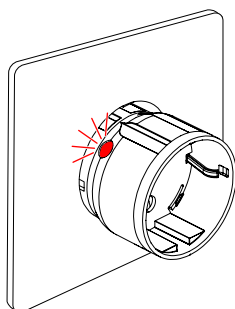
☐ Wireless components (with installation code)
 ☒ Wireless extenders (with HA Security)

Timeout (minutes)

Wireless commissioning ☒ ON (0 hours 29 minutes 53 seconds)

Searching...

2. Supply the extender with power or press the push button until the status LED flashes red.



- ⇒ A flashing extender status LED means that the extender is searching for an open and accessible wireless network.
The status LED stops flashing as soon as the extender is connected to the gateway.
3. Deactivate **Wireless commissioning** at the wireless gateway as soon as the extender is listed under **Available devices**.

Wireless commissioning

☐ Wireless components (with installation code)
☒ Wireless extenders (with HA Security)

Timeout (minutes)

Wireless commissioning ☐ OFF

Type	Wireless MAC address	Wireless address	Status
Extender	00-0D-6F-00-0B-BD-4A-A7	0x16F3	

- ⇒ The gateway and the extender are now connected.
The gateway service interface displays the extender on the **Homepage** and under **Wireless extenders**.

IT security Activate wireless commissioning for wireless extenders for as short a time as possible. Attackers could try to connect their own extender.

Assign name

Function call: **Menu > Wireless extenders > Details > Edit**
 or: **Homepage > Symbol Wireless extender > Edit**

Optionally assign a name to the extender in the gateway service interface in order, for example, to set the installation location.

Wireless extender: Floor 1, X1.1

[Edit](#) [Request version](#) [Disconnect](#)

Device information	Firmware	Signal
Name Floor 1, X1.1 Type Extender Wireless MAC address 00-15-BC-00-2F-00-0F-CE Wireless address 0xF580	Manufacturer Name Develco Products A/S Primary Software Version 3.12.8 Primary Hardware Version 2.0.1	RSSI -42 dB

Key word directory

A		
Ambient conditions	11	
Ambient temperature	11	
C		
Commissioning	21	
Commissioning wireless extender 90 41	46	
Compatibility	27	
D		
Default IP address	22, 32	
DHCP	32	
Dimensions	11	
Disconnect	30, 31	
Disconnect wireless components	30	
Disconnect wireless extender	31	
Disposal	45	
Downgrade the wireless gateway's firmware	40	
E		
Electromagnetic fields	18	
Errors during firmware update	39	
Ethernet LEDs	17	
F		
Factory reset	38	
Fastening	20	
Firmware update of wireless components	28, 30	
Firmware version 4.1.1	40	
Firmware Version 4.4.1	38	
Firmware version 4.8.1	40	
Fixed IP address	32	
I		
Identification	12	
Identification label	12	
Identify	29	
Identify wireless components	29	
Installation code	12, 26	
IP address	21	
IT security	23, 26, 33, 37, 38, 47	
L		
LED status display	16	
Localising	21	
Log in	23	
M		
Measuring the range	18	
N		
Network (Ethernet)	21	
P		
Packaging	43	
Power over Ethernet (PoE)	10	
R		
Radio interface	10	
Range measurement	14, 18	
Reconnect	29	
Reset	38	
Reset factory defaults	38	
Reset signalling	16	
Restart	38	
Return shipment	43	
RSSI value	28, 30	
S		
Service interface	23	
Signal strength	28	
Signalling	16	
Status LEDs	16	
System time	42	
T		
Time server	42	
TLS	33	
Topology	9, 25	
Transmitting power	10	
U		
Update the firmware of wireless components	35	
Update the wireless gateway's firmware	38	
Updating the firmware of wireless components	28, 30	
UPnP	21, 32	
USB stick	22	
W		
Wall mounting	20	
WEEE guideline	45	
Weight	11	
Wireless commissioning	26	
Wireless commissioning extender 90 41	46	

Wireless components' firmware update	35
Wireless extender	14
Wireless gateway firmware downgrade	40
Wireless gateway firmware update	38
Wireless site survey tool	14, 18
Wireless USB stick	14

Notes

[illegible]

04045088 - 02/2023
Copyright © dormakaba 2023



www.dormakaba.com

dormakaba Deutschland GmbH
Albertstraße 3
78056 Villingen-Schwenningen
Germany
T: +49 7720 603-0
www.dormakaba.com
Company headquarters: Ennepetal