

**DRAFT**

**User Manual**

**Online Option**

# Copyrights

*The information in this document is subject to change at the sole discretion of ASSA ABLOY without notice.*

*Any use, operation or repair in contravention of this document is at your own risk. ASSA ABLOY does not assume any responsibility for incidental or consequential damages arising from the use of this manual.*

*All information and drawings in this document are the property of ASSA ABLOY. Unauthorized use and reproduction is prohibited.*

*VingCard and Elsafe are registered trademarks of ASSA ABLOY.*

# Table of contents

|                                              |           |
|----------------------------------------------|-----------|
| <b>FCC and ISED (IC) statements.....</b>     | <b>6</b>  |
| FCC statements .....                         | 6         |
| ISED (IC) statements .....                   | 7         |
| OEM responsibilities .....                   | 7         |
| End product labeling .....                   | 8         |
| <b>1. Introduction.....</b>                  | <b>9</b>  |
| 1.1 ZigBee standard .....                    | 10        |
| 1.2 Server .....                             | 10        |
| 1.3 Gateway .....                            | 10        |
| 1.3.1 Without DHCP server .....              | 11        |
| 1.4 Router .....                             | 12        |
| 1.5 Endnode .....                            | 12        |
| 1.6 Lock .....                               | 12        |
| 1.7 Permit joining/Forbid joining .....      | 12        |
| 1.8 Discovery .....                          | 13        |
| 1.9 Orphan join .....                        | 13        |
| 1.10 SysMon and the client .....             | 13        |
| 1.11 Link quality .....                      | 15        |
| 1.12 Abbreviations .....                     | 15        |
| <b>2. Installing the option.....</b>         | <b>16</b> |
| <b>3. Installing online devices.....</b>     | <b>17</b> |
| 3.1 Installing a server .....                | 18        |
| 3.1.1 TL Concentrator .....                  | 18        |
| 3.1.1.1 TL Concentrator setup.....           | 19        |
| 3.1.1.2 TL Concentrator monitor.....         | 19        |
| 3.2 Installing a gateway .....               | 20        |
| 3.3 Adding routers to a gateway .....        | 22        |
| 3.4 Adding endnodes to a router .....        | 25        |
| 3.5 Using routers as repeaters .....         | 26        |
| 3.6 Adding locks to gateways .....           | 27        |
| 3.7 Forcing parents .....                    | 27        |
| 3.8 Right-click menus in SysMon .....        | 28        |
| 3.8.1 Right-click menu choices for GWs ..... | 29        |
| 3.8.2 Right-click menu choices for RTs ..... | 32        |
| 3.8.3 Right-click menu choices for ENs ..... | 33        |
| <b>4. Online settings in the client.....</b> | <b>34</b> |

|                                                                                   |           |
|-----------------------------------------------------------------------------------|-----------|
| 4.1 Setting up door parameters in a hotel system .....                            | 34        |
| 4.1.1 Door ajar alarm .....                                                       | 34        |
| 4.1.2 Status .....                                                                | 35        |
| 4.1.2.1 Intruder status.....                                                      | 35        |
| 4.1.2.2 Offline status.....                                                       | 35        |
| 4.1.3 Miscellaneous .....                                                         | 36        |
| 4.1.4 Alarms .....                                                                | 37        |
| 4.1.5 Safes .....                                                                 | 38        |
| 4.2 Setting up door parameters in an access control system .....                  | 38        |
| 4.3 Setting up operator templates in a hotel system .....                         | 39        |
| 4.4 Setting up operator templates in an access control system .....               | 40        |
| 4.5 Preventing invalid staff card usage (only applicable for hotel systems) ..... | 41        |
| <b>5. Issuing a ZigBee configuration card.....</b>                                | <b>42</b> |
| <b>6. System operation.....</b>                                                   | <b>43</b> |
| 6.1 Events .....                                                                  | 43        |
| 6.1.1 Acknowledge .....                                                           | 43        |
| 6.1.2 Retransmission .....                                                        | 43        |
| 6.1.3 Fallback .....                                                              | 43        |
| 6.2 Online functionality .....                                                    | 43        |
| 6.2.1 Commands .....                                                              | 44        |
| 6.2.1.1 Buffered commands.....                                                    | 44        |
| 6.2.2 Alarm list .....                                                            | 44        |
| 6.2.3 Endnode list .....                                                          | 45        |
| 6.2.4 Router list .....                                                           | 46        |
| 6.2.5 Gateway list .....                                                          | 47        |
| 6.3 Setting in construction mode .....                                            | 47        |
| <b>7. Commissioning.....</b>                                                      | <b>48</b> |
| 7.1 Printing a status report .....                                                | 48        |
| 7.2 Pinging a door .....                                                          | 49        |
| 7.3 Checking online status with card .....                                        | 50        |
| <b>8. Power loss and hardware failure.....</b>                                    | <b>51</b> |
| 8.1 Lock electronics .....                                                        | 51        |
| 8.2 Endnode .....                                                                 | 51        |
| 8.3 Router .....                                                                  | 52        |
| 8.4 Gateway .....                                                                 | 53        |
| 8.5 Server .....                                                                  | 53        |
| <b>9. Redundancy and recovery.....</b>                                            | <b>54</b> |
| 9.1 Communication channel .....                                                   | 54        |
| 9.1.1 Automatic channel change .....                                              | 55        |
| 9.2 Recovery .....                                                                | 55        |
| 9.2.1 Polling .....                                                               | 55        |

|                                                                     |           |
|---------------------------------------------------------------------|-----------|
| 9.2.2 Fallback .....                                                | 55        |
| <b>Appendix A: Online devices .....</b>                             | <b>56</b> |
| Gateway .....                                                       | 56        |
| Router .....                                                        | 57        |
| <b>Appendix B: Mounting of gateway and router.....</b>              | <b>58</b> |
| <b>Appendix C: Example configurations.....</b>                      | <b>59</b> |
| <b>Appendix D: Web interface for gateway.....</b>                   | <b>61</b> |
| <b>Appendix E: Reset of gateway .....</b>                           | <b>62</b> |
| <b>Appendix F: Gateway boot-up.....</b>                             | <b>63</b> |
| <b>Appendix G: More about how the gateway finds the server.....</b> | <b>65</b> |
| Commissioning of gateways .....                                     | 66        |
| Single server - commissioning of gateways with DNS .....            | 66        |
| Multiple servers - commissioning of gateways with DNS .....         | 66        |
| Commissioning of gateways without DNS .....                         | 67        |
| Switching to backup server .....                                    | 67        |
| Single server - switching to backup server with DNS .....           | 67        |
| Multiple servers - switching to backup server with DNS .....        | 67        |
| Switching to backup server without DNS .....                        | 67        |
| <b>Appendix H: Firmware upgrade.....</b>                            | <b>68</b> |

# FCC and ISED (IC) statements

## ***FCC (Federal Communications Commission) statements***

These devices comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) these devices may not cause harmful interference, and
- (2) these devices must accept any interference received, including interference that may cause undesired operation.

**Important note:** To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20 cm between the radiator and your body. Use only the supplied antenna.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

These transmitters must not be co-located or operating in conjunction with any other antennas or transmitters.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

**Note:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The concerned end product must be labeled to say 'Contains FCC ID: Y7V-683081150C1'.

The concerned end product must be labeled to say 'Contains FCC ID: WYV-EN110'.

The concerned end product must be labeled to say 'Contains FCC ID: WYV-EN055'.

The concerned end product must be labeled to say 'FCC ID: Y7V-683081067C1'.

The concerned end product must be labeled to say 'Contains FCC ID: WYV-RT067'.

The concerned end product must be labeled to say 'FCC ID: Y7V-683081066C1'.

The concerned end product must be labeled to say 'FCC ID: Y7V-GW683081066'.

## **ISED (IC) statements**

These devices comply with Industry Canada licence-exempt RSS standard CAN ICES-3 (B)/NMB-3(B) B. Operation is subject to the following two conditions:

- (1) these devices may not cause interference, and
- (2) these devices must accept any interference, including interference that may cause undesired operation of the devices.

Les présents appareils sont conformes aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- (1) les appareils ne doivent pas produire de brouillage, et
- (2) l'utilisateur des appareils doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

**Important note:** To comply with Industry Canada RF radiation exposure limits for general population, the antennas used for these transmitters must be installed such that a minimum separation distance of 20 cm is maintained between the radiator (antenna) and all persons at all times and must not be co-located or operating in conjunction with any other antenna or transmitter.

Under Industry Canada regulations, these radio transmitters may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

These radio transmitters IC9514A-683081150C1, IC8231A-EN110, IC8231A-EN055, IC8231A-RT067, IC9514A-683081067C1, IC9514A-683081066C1 and IC9514A-683081066 have been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with these devices.

| Name/Model         | Gain    | Impedance |
|--------------------|---------|-----------|
| Inverted F-antenna | 3.0 dBi | 50 ohm    |

The term "IC" before the equipment certification number only signifies that the Industry Canada technical specifications were met.

Le terme "IC" devant le numéro de certification signifie seulement que les spécifications techniques Industrie Canada ont été respectées.

## **OEM responsibilities**

The endnode module has been certified for integration into products only by OEM integrators under the following conditions:

1. The antenna must be installed such that a minimum separation distance of 20cm is maintained between the radiator (antenna) and all persons at all times.
2. The transmitter module must not be co-located or operating in conjunction with any other antenna or transmitter.

As long as the two conditions above are met, further transmitter testing will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with these modules installed (e.g., digital device emissions, PC peripheral requirements, etc.).

**Important note:** In the event that these conditions can not be met (for certain configurations or co-location with another transmitter), then Industry Canada certification is no longer considered valid and the IC Certification Number can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end products (including the transmitter) and obtaining a separate Industry Canada authorization.

## **End product labeling**

The endnode module is labeled with its own IC Certification Number. If the IC Certification Number is not visible when a module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module. In that case, the final end product must be labeled in a visible area with the following:

'Contains IC: 8231A-EN110'

'Contains IC: 8231A-EN055'

The OEM of the respective module must only use the approved antenna listed above, which have been certified with this module. The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module or change RF related parameters in the user's manual of the end products.

# 1. Introduction

CENTRAL ELECTRONIC LOCKING SYSTEM  
USING RADIO FREQUENCY (RF) COMMUNICATION

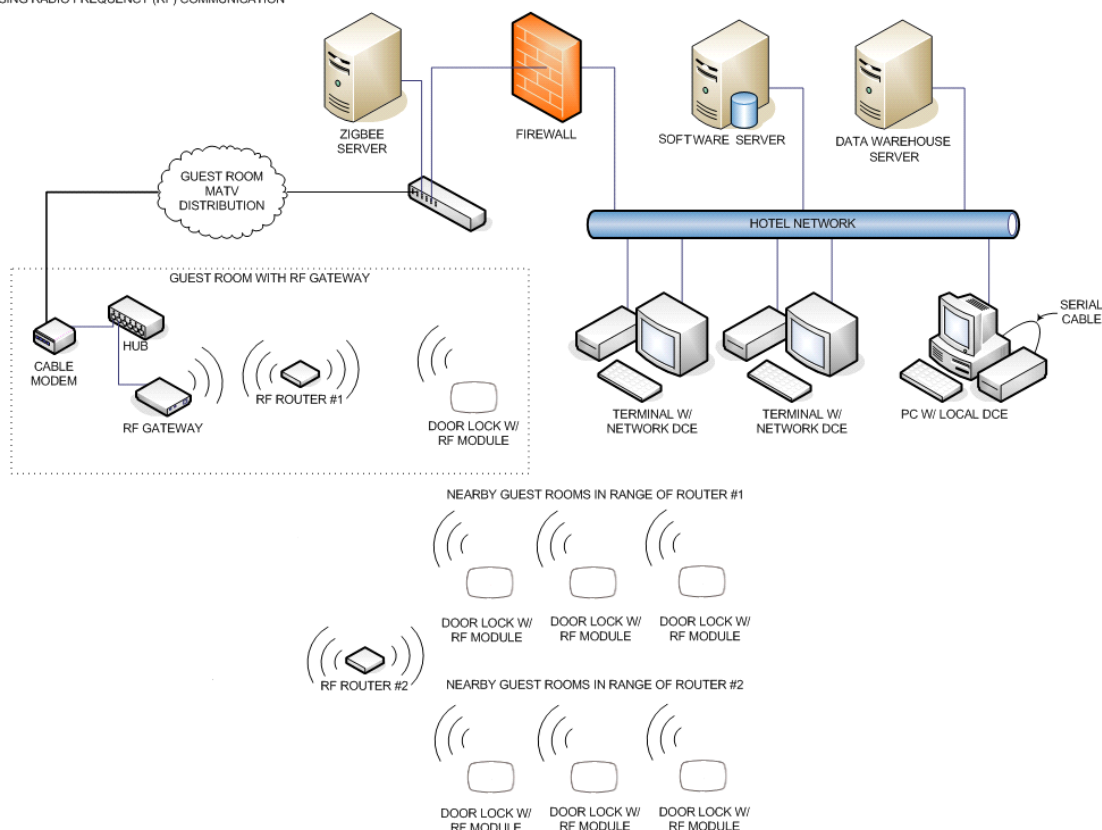


Figure 1: Example of online configuration. Several other configurations are possible; see [Appendix C](#) for some examples.

With the online option, the locks can both send and retrieve information. Commands can be sent from the front desk (hotel systems)/company reception (access control systems) to the lock. e.g., in hotel systems a guest can change rooms without needing to go to the reception. Events are directly sent to the application server.

This chapter describes the online network topology all the way from the server to the lock. Commands sent from the server to a lock will pass through the items in the order they are mentioned. Answers will pass through the same items but in the opposite direction.

**Note:** The most information in this manual is common for hotel systems and access control systems. In some cases there are however specific sections, which is clearly stated in the heading.

**Note:** Some online functions require the *Online advanced* option; see the section about options in the client user manual for details.

### 1.1 ZigBee standard

The online option is based on the ZigBee standard, a standard for transmission of data via radio. The ZigBee devices have low power consumption and the standard is aimed at control applications with relatively low data rate. Below are some basic facts for the standard:

- based on IEEE 802.15.4 (Open ISM 2.4GHz band; *ISM* = industrial, scientific and medical)
- 16 channels spread spectrum (DSSS, *Direct Sequence Spread Spectrum*)
- 250kbit/s (~2kbit/s @ 1% duty-cycle)
- consists of a virtually unlimited number of small networks (PANs, *personal area networks*)

### 1.2 Server

The server is the manager of the whole network for a property. It can manage a virtually unlimited number of gateways. All commands sent from the server are encrypted.

### 1.3 Gateway

The gateways connect to the server via TCP/IP and automatically adjusts to 10 or 100 Mbit/s networks. The gateway starts by retrieving an IP address via DHCP (*Dynamic Host Configuration Protocol*) and then automatically finds the server.

**Note:** The DHCP protocol is specified according to the standard *RFC 2131*.

**Note:** A ping is sent to each gateway once an hour. The statistics is evaluated once a day. An alarm is triggered if more than one per cent of the pings fail. The statistics is shown in the **System Settings** report in the client.

If DHCP has previously been turned off manually, it can be enabled again by clicking the **Set** button in the **Online Network** dialog of SysMon (*System Monitor*) and choosing **Turn on DHCP in gateway**. See [section 1.10](#) for more information about SysMon.

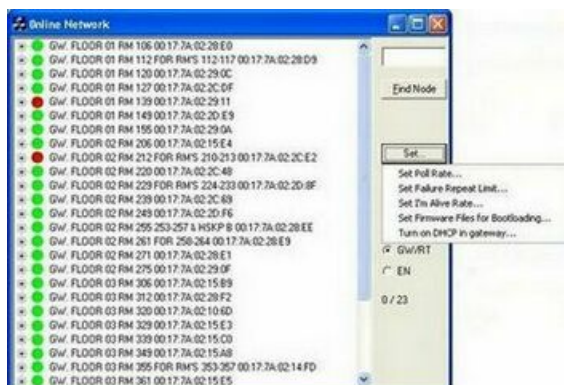


Figure 2

The dialog **Enter MAC address** will be shown; fill it in and click **OK**.



Figure 3

The gateway contains functionality for coordination of a PAN (*Personal Area Network*). The PAN is a wireless network that communicates on the 2.4GHz band. The gateway allows routers (see [section 1.4](#)) and endnodes (see [section 1.5](#)) to join the PAN and assigns network addresses. Each ZigBee node has a unique 64-bit IEEE address similar to Mac addresses used in TCP/IP.

- The gateway chooses which of the 16 channels in the 2.4GHz band the nodes in the PAN should use.
- The gateway is powered either over Ethernet or by a power adapter.
- The total number of gateways is virtually unlimited.
- The maximum theoretical limit of endnodes per PAN is high, but a practical limit is some hundred. In most cases, only some ten to 20 endnodes will be connected to each gateway. However, this can change due to the building construction, materialwise etc.
- The gateway can have either five routers or 15 endnodes connected as direct descendants.

See [Appendix A](#) for more information about the gateway, including a detailed picture.

See [Appendix B](#) for preferred way of mounting the gateway.

See [Appendix C](#) for configuration examples.

### 1.3.1 Without DHCP server

1. The IP address on the gateway will change to an IP address in the range 169.254.1.0 – 169.254.254.255; this IP address range is based on the *zero config* standard.
2. Have a web browser available, to reach a web interface where the gateway parameters can be changed. Follow the steps below:
  - Press the **F** button on the gateway for a short while (see in [Appendix A](#) where the button is located). The status LED on top of the gateway will blink yellow.
  - Use *Wireshark* to find out the *zero config* IP address of the gateway.
  - Enter the *zero config* IP address in the web browser (<http://ipaddress>) to reach the web interface (**ZigBee Gateway Setup** page) where the desired changes can be made. **Note:** See [Appendix D](#) e.g. screenshot and more details about the web interface. **Note:** For a reset to factory default values, press and hold the **F** button while powering up the gateway.

## 1.4 Router

A router acts either as a repeater for range extension, or as a parent for endnodes. It will also act as a buffer for messages sent to endnodes connected to the router.

- Routers are externally powered.
- The router can have either five routers or 15 endnodes connected as direct descendants.
- There can be a maximum of five hops down the gateway; i.e. gateway – router – router – router – router – endnode. This limits the physical coverage of a PAN. ***Important:* Even though it is possible to have five hops, it is recommended to have maximum three hops, i.e. gateway - router - router - endnode. The link quality index (LQI) should be at least 30%.** See [section 1.11](#) for more information about the LQI.

See [Appendix A](#) for more information about the router, including a detailed picture.

See [Appendix B](#) for preferred way of mounting the router.

See [Appendix C](#) for configuration examples.

## 1.5 Endnode

An endnode is built into each lock. It is optimized for low power consumption.

The parent router will act as a buffer for commands from the server. A command sent from the server to a lock will be sent from the gateway to the lock's parent router. The command will be sent through the routers that may be located between the gateway and the lock's parent router. Any message sent from the lock will be passed on to the server through the parent router, any intermediate routers and the gateway. Messages from the lock are sent instantly. The total number of endnodes is virtually unlimited.

## 1.6 Lock

The locks are the destination for commands and the source of events.

## 1.7 Permit joining/Forbid joining

In order to prevent nodes from joining randomly, 'permit joining' can for each PAN only be made at one router or its 'parent gateway' at a time. When a node is to be joined to the PAN, 'permit joining' must be made at the router or gateway that shall be its parent. When the node has joined, 'forbid joining' should be made at the parent. 'Forbid joining' will automatically be made on the parent after 15 minutes in case it is forgotten. ***Note:*** It is only possible to make 'permit joining' at one RT per PAN at a time. If you make 'permit joining' at one RT and then at another RT in the same PAN, the first RT will automatically make 'forbid joining'.

The commands for 'permit joining' and 'forbid joining' are sent from SysMon. The 'permit joining'/'forbid joining' states of routers can also be toggled by pressing the **F1** button. The LED on the router indicates 'permit joining' by fast blinking; short blink every 0.5 seconds. 'Forbid joining' is indicated by slow blinking; short blink every two seconds. See [Appendix A](#) for a router picture with buttons, LED etc.

### **1.8 Discovery**

*Discovery* is the process when a node shall join a PAN. It starts by the node broadcasting a discovery message. Any plausible parent will answer and the node will join the one on which "permit joining" has been made, provided that it is within range.

Routers make discovery when given a reset while the **F1** button is being pressed; see [Appendix A](#) for a router picture with buttons.

An endnode makes discovery when a *Discovery card* is presented at the lock; see [chapter 5 Issuing a ZigBee configuration card](#). When the card is presented, the lock will chirp once and/or show a green LED signal (depending on lock model). If the endnode in the lock is busy at the moment, there will instead be a tick sound and/or a very short green LED signal. In this case, make a new try by presenting the Discovery card at the lock again.

### **1.9 Orphan join**

As it can take up to three hours for the endnodes to get online after recovery from a power cut, there is an *Orphan Join card* that will initiate an orphan join when presented at a lock; see [chapter 5 Issuing a ZigBee configuration card](#). When the card is presented at the lock, the lock will chirp once and/or show a green LED signal (depending on lock model). If the endnode in the lock is busy at the moment, there will instead be a tick sound and/or a very short green LED signal. In this case, make a new try by presenting the Orphan Join card at the lock again.

### **1.10 SysMon and the client**

The System Monitor (*SysMon*; found in the folder where the server software has been installed) is used for managing the online network. In SysMon all connected gateways, routers, endnodes etc are shown. Depending on what operator template that the logged on operator belongs to, the operator is authorized to perform different operations in SysMon.

**Note:** If the distributor is going to log on to SysMon, *system manager* must be logged on first.

To set up SysMon authorities:

1. Double click on **Operator templates** under the **Lists** tab in the navigation window of the client.
2. Mark an existing operator template and click **Properties**, or click **Add** to create a new operator template.
3. In the **Operator Template Details** dialog, click **SysMon** in the left pane.
4. Mark the applicable checkboxes for operations that operators belonging to the template should be allowed to perform in SysMon.
5. If an existing operator template was updated with SysMon information, click **Update** and **Close**. If a new operator template was created, enter applicable information for the operator template under the other panes **General**, **Database** etc and then click **Save** and **Close**.

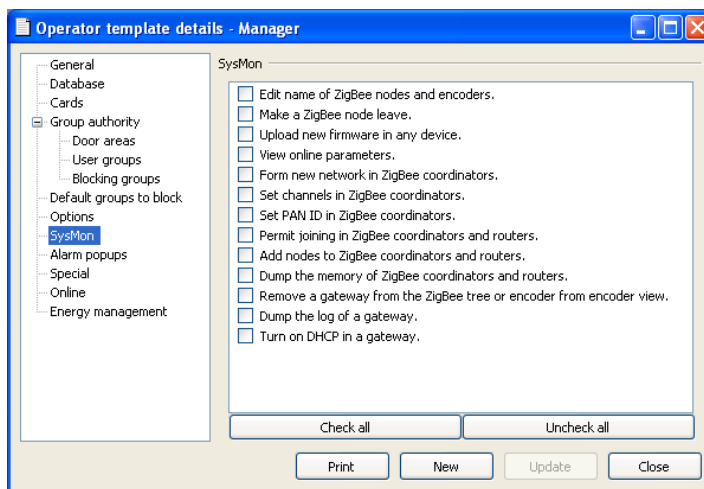


Figure 4

Online settings and commands are made in the client.

If a dialog in the client should be refreshed due to online changes, this is shown with a \* in the dialog caption. Click the **Refresh** button in the dialog.

Different operator templates can be given different authorities for online commands; see sections [4.3 Set up operator templates in a hotel system](#) and [4.4 Set up operator templates in an access control system](#) respectively.

For online settings, see [chapter 4 Online settings in the client](#).

For online commands, see the user manual for the client (the sections about online commands for a door and about commands under the **Online** tab).

For supervision of the system, see chapters [6 System operation](#) and [7 Commissioning](#).

### 1.11 Link quality

The *Link Quality Index* (LQI) is an average percentage that should not be below 30%. It is displayed when the mouse hovers over a node in the SysMon **Online Network** view; see example in the screenshot below. See [section 3.2 Installing a gateway](#) for information about how to log on to SysMon and find the **Online Network** view.

**Note:** The LQI value which is shown when the mouse hovers over a node is not an instantaneous value but an average; the last instantaneous value, with timestamp, is however shown within parantheses after the average. To get an instantaneous value of the LQI, right click on a router or endnode in the SysMon **Online Network** view and choose **Get User Description**.

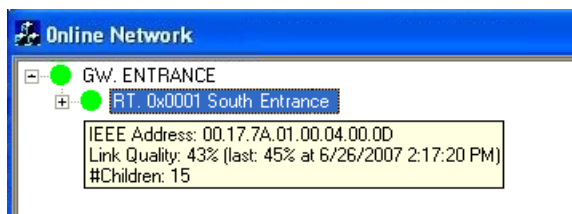


Figure 5

The LQI is valid for the link between the node and its parent.

If the LQI is below 30%, the dot in front of the node in SysMon is yellow; see example in Figure 6.



Figure 6

If the LQI is below 15%, the dot in front of the node in SysMon is red; see example in Figure 7.



Figure 7

### 1.12 Abbreviations

In the rest of this user manual, the following abbreviations are used:

GW = gateway  
RT = router  
EN = endnode  
PAN = personal area network

## 2. Installing the option

If the option has been ordered together with the software, it is included in the license code and will be set in the software when the license code is entered.

If the option should be added to the system at a later occasion, when the license code has already been entered and system ID is therefore set, an option code is used instead. Several software options can be included in one option code. An operator with the authority to handle option codes must be logged on. Normally, options are set by the system manager or the distributor.

When ordering the option, the system code must be communicated to the ordering department:

1. Double click on **System settings** under the **Reports** tab in the navigation window to find the system code. **System settings** is available even if you are not logged on.
2. Communicate your system code to the order department; see order acknowledgement for phone number and e-mail address. The system code can also be entered in the *Ordering web page* when making the order.

To install the option:

1. When you have got your option code, go to **Tools/Option code**.
2. Enter the option code and click **Apply**.

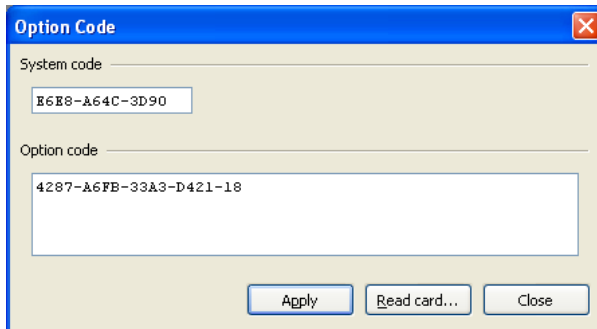


Figure 8

### 3. Installing online devices

The online devices were designed to allow for maximum flexibility during installation. There are no particular location specifications as long as the devices are within reasonable range of each other and good radio communication can be attained. Generally, the range is however around 20 metres or through a wall. The range of the devices depends to large extent on the building material(s) in the surroundings. As much effort as possible should be made to securely install each device in a location where it will be dry, cool, and undisturbed, yet still maintain good radio contact with its parent or children.

**Important:** The ZigBee communication can be disturbed by e.g. Wi-Fi networks; always make sure to have as long distances as is physically possible between ZigBee devices and other radio equipment. If this still causes problems at a site, automatic channel change can be enabled. See more information about automatic channel change in [section 9.1.1](#).

This section will discuss the installation methods for each device in the system as well as options for forcing devices to connect to specific parent devices.

Software requirement:

- Hotel system: version 1.9.0 or later
- Access control system: version 1.6.0 or later

### 3.1 Installing a server

- The application server must be connected to the same network that the GW devices will be connected to.
  - The application server must have the online option installed; see [chapter 2](#) for details.
1. Before you install the first GW device, you must add a ZigBee gateway to the device list in the software (double click on **Devices** under the **Lists** tab in the navigation window and click **Add** to add a new device) using the following parameters:

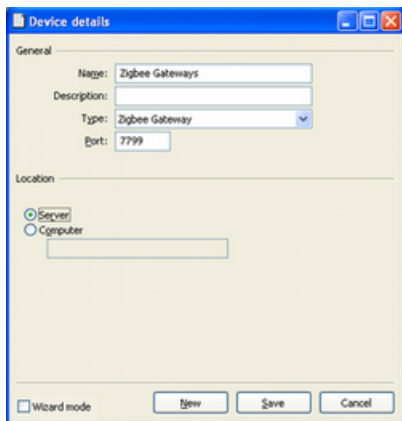


Figure 9

2. When the fields have been filled in according to Figure 9 (port 7799 is pre-filled as default when choosing 'ZigBee gateway' at **Type**), click **Save** and **Close**.  
**Note:** If desired, mark the checkbox 'Wizard mode' to get more detailed help.  
**Note:** The same device is used for all GWs.

For testing and commissioning purposes it is a good idea to have either a laptop with the server software installed which you can use to directly connect to gateways as they are installed, or a laptop with a connection to the live application server. This will allow you to test radio signal strength as you are installing the devices on each floor so issues can be addressed immediately.

**Note:** The network information is stored in the GWs and not in the laptop.

#### 3.1.1 TL Concentrator

*TL Concentrator* is a utility for simplifying the setup of a firewall when the GWs are located on a different network. TLConcentrator runs on the ZigBee server and listens for GWs on one port and forwards all traffic to the application server on another port. All traffic from the application server is sent to the correct GW. In this way, the firewall will only have to be set up to allow sockets from the ZigBee server. The alternative would be to set up the firewall to allow sockets for every GW. This would add implications, especially when adding or exchanging GWs.

#### 3.1.1.1 TL Concentrator setup

The application server is set up to listen for GWs on port 7799. This is where TLConcentrator will connect. TLConcentrator is set up to listen for GWs on port 7798 and to open sockets on the application server using port 7799.

To set up these parameters:

1. Go to **Start/Run**.
2. Browse to the installation folder, mark **TLConcentrator.exe** and click **Open**.
3. Add **/config**  
**Note:** There should be a space before /
4. Click **OK**.

A **Configuration** dialog will be shown.

1. Let the default 7798 be at **Listen Port**.
2. State the host's IP address at **Host Address**.
3. Let the default 7799 be at **Host Port**.

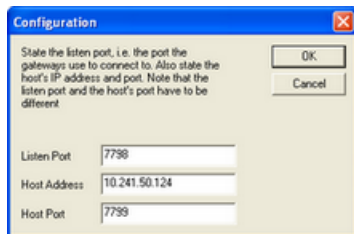


Figure 10

#### 3.1.1.2 TL Concentrator monitor

It is possible to monitor the traffic through TLConcentrator using **TLConcentrator.exe /monitor**.

1. Go to **Start/Run**.
2. Browse to the installation folder, mark **TLConcentrator.exe** and click **Open**.
3. Add **/monitor**  
**Note:** There should be a space before /
4. Click **OK**. The following dialog (with example statistics) is shown.



Figure 11

### 3.2 Installing a gateway

Power and network connections should be made in a manner that will reduce the chances of the device being unplugged.

- The GW is powered by 5VDC using a plug in wall power adapter, or via power over Ethernet.
  - For network connectivity, the GW requires an available Ethernet port and a patch cord.
1. Open the *System Monitor* (SysMon), which is used for managing the online network. To open SysMon, double click on **SysMon.exe** in the installation folder.
  2. Log on to SysMon: go to **File/Log on** and enter user ID and password. At 'Operator card', choose the applicable card encoder. Click **Enter**.
  3. If it is not open already, open SysMon's **Online Network** view at **View/Online Network**. The **Online Network** view of SysMon shows all connected GWs, RTs and ENs. Several useful commands are available by right clicking on nodes; see sections [3.8.1-3.8.3](#) for more information about the different commands.

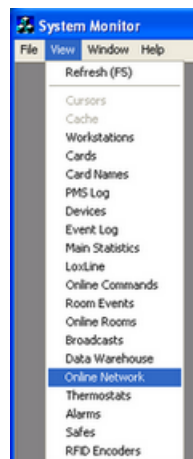


Figure 12

4. Mount the GW in a convenient, out of the way location using the VELCRO<sup>®</sup> strip.
5. Connect the network cable and power cable to the GW.
6. After approximately 30 seconds the GW will announce itself to the server and appear as a new GW in the **Online Network** tree in SysMon.



Figure 13

7. Right click on the new GW to bring up the device option menu and choose **Edit Name**.

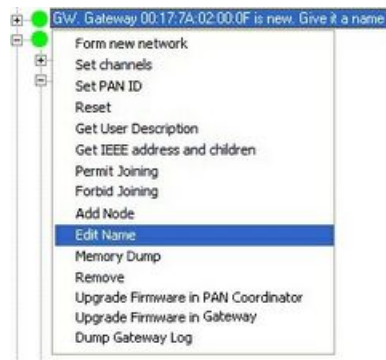


Figure 14

8. Name the GW something meaningful – it should generally indicate the GW's location or coverage area.



Figure 15

9. Right click on the GW and select **Form new network** to make sure that the GW is reset and gets a PAN ID.

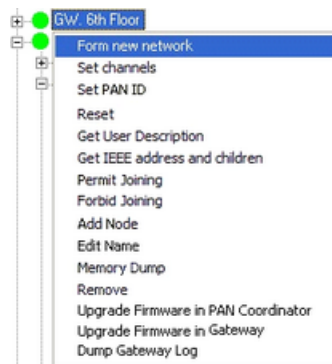


Figure 16

### 3.3 Adding routers to a gateway

The RT is powered by 5VDC using a plug in wall power adapter or a wired transformer. No wired Ethernet network connection is required as it communicates with the GW via radio.

**Note:** The recommended installation method is to use the enclosed VELCRO® strip to attach the RT to a wall or some other convenient location.

As described in [section 1.10 SysMon and the client](#), it is set up in the operator template what operations a certain operator can perform in SysMon.

1. To add an RT to the online network, right click on the GW the RT should join and choose **Permit Joining**.

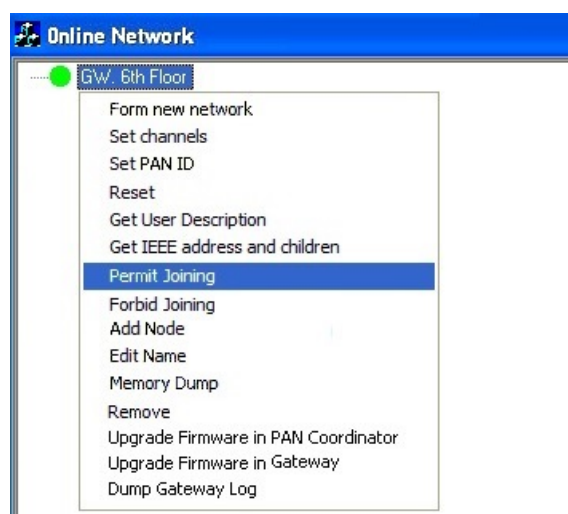


Figure 17

2. Hold your mouse over the GW name and a box will pop up containing some information about that device. At the bottom of that box you will see it says *Join permitted*, indicating that the GW now allows new connections.

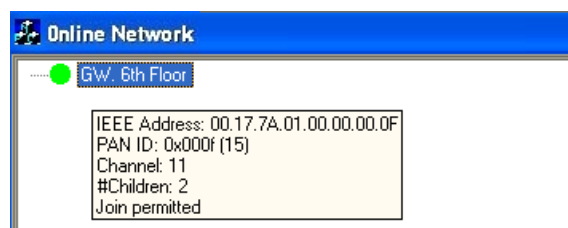


Figure 18

3. When the RT has been mounted with the VELCRO<sup>®</sup> strip, press the **F1** button on the RT while connecting power to the RT. The RT will power up and automatically begin looking for a parent device to associate with. It will discover the GW on which **Permit Joining** has been made, announce itself, and appear in the **Online Network** tree in SysMon.



Figure 19

4. Right click on the RT and choose **Edit Name** to name the RT something meaningful. In our example we have named it 'RT 620-623' to indicate the group of rooms that will be attached to that RT.

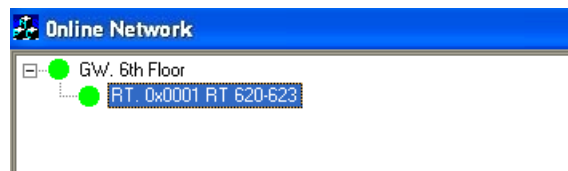


Figure 20

5. Hold your mouse over the device to view the RF link quality (LQI) between the RT and the GW. It shows the average LQI followed by the last measurement with timestamp in parentheses. **Note: The LQI should not be below 30%.**

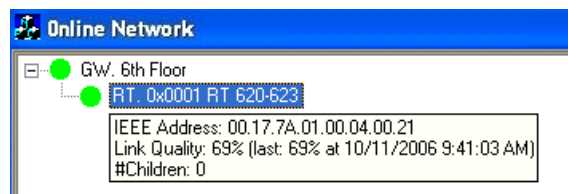


Figure 21

6. While the GW still says *Join permitted* when holding the mouse over the GW, plug in any additional RTs as needed (up to five per GW) and name them.



Figure 22

7. Hold your mouse over each RT to check the LQI making sure it is within acceptable limits.
8. When all desired RTs have been added to the GW, right click on the GW and choose **Forbid Joining**.

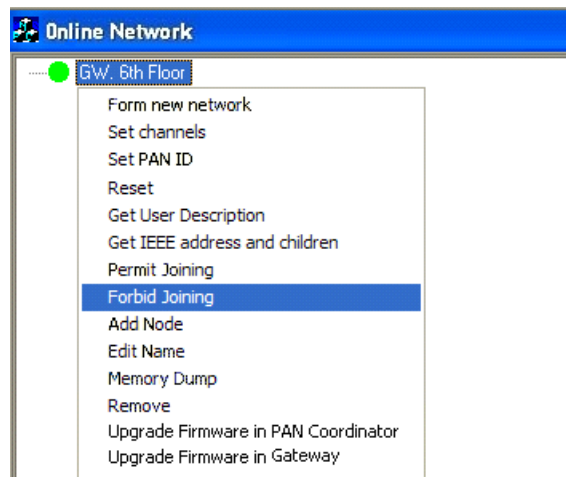


Figure 23

9. Hold your mouse over the GW to confirm it no longer says *Join permitted*.

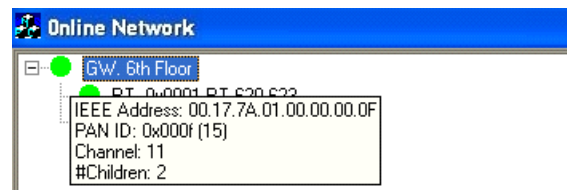


Figure 24

### 3.4 Adding endnodes to a router

The EN is the radio board inside the door lock unit. This device should not be confused with the lock electronics themselves, and when troubleshooting communication or lock issues care should be taken to diagnose the correct piece of hardware.

1. To add an EN to an RT, right click on the RT the EN should join and choose **Permit Joining** (or press the **F1** button on the RT). Hold your mouse over the RT to verify that joining is permitted.

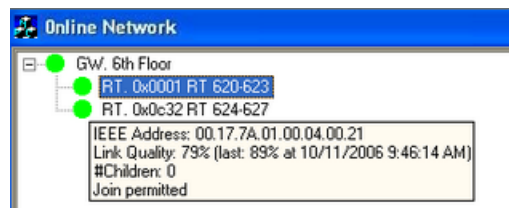


Figure 25

2. Present the Discovery card at the lock; see [chapter 5 Issuing a ZigBee configuration card](#). The lock will chirp once and/or show a green LED signal (depending on lock model) to indicate it has read the card, and will start searching for the RT on which **Permit Joining** has been made to join. When it finds the RT it will announce itself to the server and appear in the **Online Network** tree.

**Note:** The Discovery card also sets sub product ZigBee in the lock.



Figure 26

After the lock sends its first event, the room number that is programmed in the lock will automatically fill in. This can be forced by presenting a working key in the lock.



Figure 27

3. Hold your mouse over the lock to verify the LQI is within acceptable limits. Continue adding additional locks to the RT as needed. When finished, right click on the RT and choose **Forbid Joining**.

### 3.5 Using routers as repeaters

In the event there are locks that are not in range of a GW and RT combination, an additional RT can be added for extended range.

1. Add the GW and first RT as normal. This first RT will act as a repeater between the GW and the 2<sup>nd</sup> RT which will be communicating with the locks. In our example we named the first RT 'RPTR 620-623' to indicate that it will act as a repeater for the RT serving 620-623.



Figure 28

2. Choose **Forbid Joining** on the GW and **Permit Joining** on the 1<sup>st</sup> RT.
3. Plug in the 2<sup>nd</sup> RT. The 2<sup>nd</sup> RT will find and attach itself to the 1<sup>st</sup> RT.
4. Choose **Forbid Joining** on the 1<sup>st</sup> RT. Name the 2<sup>nd</sup> RT and choose **Permit Joining** on it.

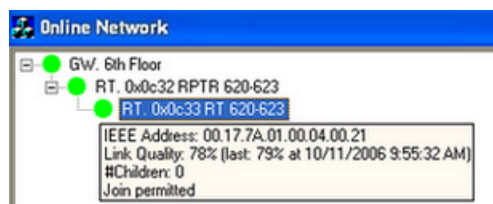


Figure 29

5. Present the Discovery card at the lock (see [chapter 5 Issuing a ZigBee configuration card](#)); the lock will chirp once and/or show a green LED signal, depending on lock model. The lock will find and attach itself to the RT on which **Permit Joining** has been made, and when the first event is received from the lock the room number will fill in.
6. Add all the necessary locks and choose **Forbid Joining** on the 2<sup>nd</sup> RT.



Figure 30

**Note:** For Z-Stack (ZigBee 2004), the RT acting as a repeater is only capable of communicating to the GW and the 2<sup>nd</sup> RT; it is in this case not possible at this time to repeat signals to a 2<sup>nd</sup> RT and communicate directly with locks at the same time.

### 3.6 Adding locks to gateways

There may be cases where the locks will communicate directly with the GW.

To do this:

1. Choose **Permit Joining** on the GW and present the Discovery card at the lock (see [chapter 5 Issuing a ZigBee configuration card](#)); the lock will chirp once and/or show a green LED signal, depending on lock model. The lock will attach itself to the GW on which **Permit Joining** has been made, and when the first event is received the room number will automatically fill in.

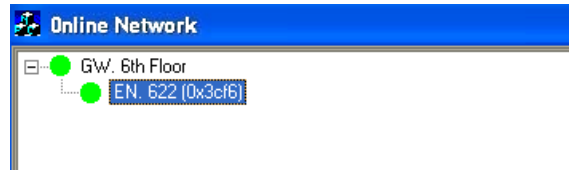


Figure 31

2. Add the necessary locks and then choose **Forbid Joining** on the GW.

**Note:** RTs should not be connected to a GW which has got ENs connected to it.

### 3.7 Forcing parents

If a device such as an EN sees two RTs when it is in discovery mode (i.e. if 'permit joining' has by mistake been made on two RTs belonging to different PANs at the same time), it is possible that the EN will not join the desired RT – i.e. the RT with which it has the strongest RF link. For this reason it is recommended that GWs, RTs and ENs be installed in a systematic way to ensure all devices are connected to the parent that makes the most sense.

If a situation arises in which a device is connected to the wrong parent, it is easy enough to force the child device to leave the network and rejoin properly. If a right click is made on the child device in SysMon, and the **Leave network** command is chosen, the child device will deregister from the parent so another node can join. The rejoining to a new parent is performed with the **Permit Joining** command.

An example when a child device is connected to the wrong parent would be that an EN is within range of both RT-A and RT-B. Signal strength between the EN and RT-A is 32%, while signal strength between the EN and RT-B is 75%. In this case it is a good idea to force the EN to connect to RT-B.

To force the EN by using the Permit Joining command:

1. Right click on the EN and choose **Leave Network**. The EN will deregister from RT-A.

**Note:** Due to a bug in BeeStack radio nodes of versions before 1.0.49, do not use the **Leave Network** command for these older versions.

2. **Important:** Wait for 40 seconds to avoid confusing RT-A from which the EN has deregistered.
3. Make sure that **Forbid Joining** has been chosen for RT-A and that **Permit Joining** has been chosen for RT-B.
4. Present a Discovery card at the EN door lock (see [chapter 5 Issuing a ZigBee configuration card](#)); the lock will chirp once and/or show a green LED signal, depending on lock model. The EN will immediately begin to look for an available parent, and since RT-A is in 'forbid joining' mode, RT-B will be its only option.
5. Once the EN has joined the correct RT, choose **Forbid Joining** on RT-B.

**Note:** The method above with **Permit Joining** can also be applied to RTs joining RTs, RTs joining GWs, and ENs joining GWs.

### **3.8 Right-click menus in SysMon**

When right clicking on GWs, RTs and ENs in SysMon, different choices appear depending on what item you right click on. The different choices are described in the following sections.

**Note:** Depending on what operator template that the logged on operator belongs to, different operations in the right-click menus are greyed or not. The operations that a certain operator template should be allowed to perform are set up in the client under the **SysMon** alternative in the **Operator Template Details** dialog; see the client setup manual for details.

### 3.8.1 Right-click menu choices for GWs

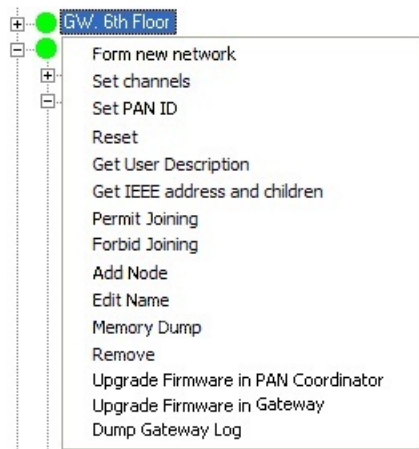


Figure 32

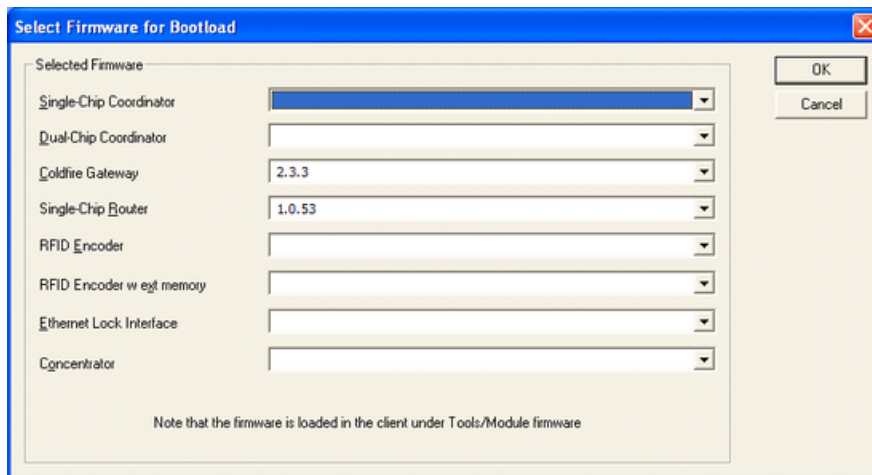


Figure 33: Bootload dialog - see 'Upgrade Firmware in PAN Coordinator' and 'Upgrade Firmware in Gateway' in [Table 1](#) and 'Upgrade Firmware in Router' in [section 3.8.2](#).

| Menu choice                                | Description                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Form new network</b>                    | makes a total reset of the GW                                                                                                                                                                                                                                                                                                               |
| <b>Set channels</b>                        | selects allowed channels; see <a href="#">section 9.1 Communication channel</a> for further information                                                                                                                                                                                                                                     |
| <b>Set PAN ID</b>                          | sets another identity<br><b>Note:</b> The Set PAN ID choice is normally not used, since the PAN ID is given automatically by the network. If the PAN ID is 0x000, choose <b>Form new network</b> in the right-click menu for the GW; see above.                                                                                             |
| <b>Reset</b>                               | makes a reset; all data is retained                                                                                                                                                                                                                                                                                                         |
| <b>Get User Description</b>                | gets parameters (e.g. version) for the node                                                                                                                                                                                                                                                                                                 |
| <b>Get IEEE address and children</b>       | gets the IEEE address as well as all children stored in the association list                                                                                                                                                                                                                                                                |
| <b>Permit Joining</b>                      | makes it possible for children to join                                                                                                                                                                                                                                                                                                      |
| <b>Forbid Joining</b>                      | forbids children to join                                                                                                                                                                                                                                                                                                                    |
| <b>Add Node</b>                            | This menu choice can be used e.g. if a gateway in a corridor is broken and needs to be replaced. The children under the gateway must then be set up as new nodes in the association table, and instead of needing to go into the guest rooms to fix this it can be done from the <b>Add Node</b> dialog; see details <a href="#">here</a> . |
| <b>Edit Name</b>                           | edits the node's name in the database                                                                                                                                                                                                                                                                                                       |
| <b>Memory Dump</b>                         | reads the memory; only used by Technical support                                                                                                                                                                                                                                                                                            |
| <b>Remove</b>                              | removes the GW from the database                                                                                                                                                                                                                                                                                                            |
| <b>Upgrade Firmware in PAN Coordinator</b> | loads a new firmware into the PAN coordinator; see bootloader dialog in <a href="#">Figure 33</a><br><b>Note:</b> The firmware shown is the one that has been loaded into the application server database at <b>Tools/Module firmware</b> ; see the client setup manual for details.                                                        |
| <b>Upgrade Firmware in Gateway</b>         | see bootloader dialog in <a href="#">Figure 33</a><br><b>Note:</b> This menu alternative is not applicable for the older type of gateway (9VDC).                                                                                                                                                                                            |
| <b>Dump Gateway Log</b>                    | creates an xls file with internal gateway events for troubleshooting purposes                                                                                                                                                                                                                                                               |
|                                            | <i>Table 1</i>                                                                                                                                                                                                                                                                                                                              |

## Details about 'Add Node':

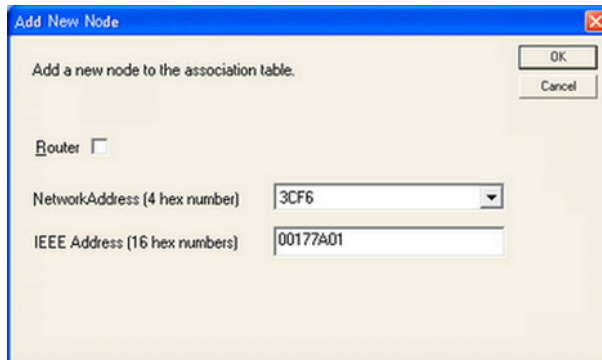


Figure 34

1. When **Add Node** is chosen in the right-click menu of a gateway or router, a dialog as in Figure 34 is shown.
2. If the node that should be added is a router, mark the checkbox **Router**.
3. Choose the applicable **Network Address** in the drop-down-menu; the network addresses are shown in the **Online Network** tree of SysMon, see example in Figure 35.
4. Complete the **IEEE Address**, which is also found in the **Online Network** tree of SysMon; see example in Figure 36 (hover with the cursor over the concerned node to show information about IEEE address etc).

**Note:** The **Add Node** function requires BeeStack version x.0.53 or later.

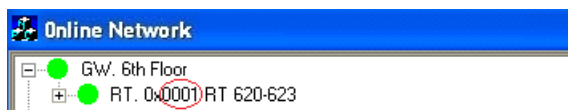


Figure 35

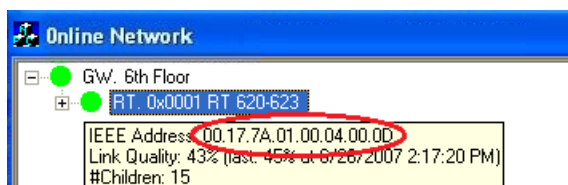


Figure 36

### 3.8.2 Right-click menu choices for RTs

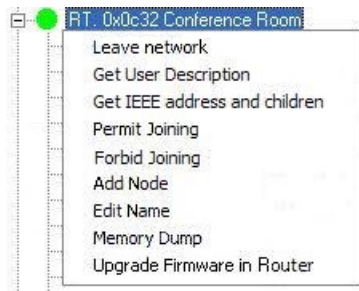


Figure 37

| Menu choice                          | Description                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Leave network</b>                 | deregisters from the parent so another node can join<br><b>Note:</b> Due to a bug in BeeStack radio nodes of versions before 1.0.49, do not use the <b>Leave Network</b> command for these older versions.                                                                                                                  |
| <b>Get User Description</b>          | gets parameters (e.g. link quality index, LQI) for the node<br><b>Note:</b> The LQI which is shown with <b>Get User Description</b> is an instantaneous value.                                                                                                                                                              |
| <b>Get IEEE address and children</b> | gets the IEEE address as well as all children stored in the association list                                                                                                                                                                                                                                                |
| <b>Permit Joining</b>                | makes it possible for children to join                                                                                                                                                                                                                                                                                      |
| <b>Forbid Joining</b>                | forbids children to join                                                                                                                                                                                                                                                                                                    |
| <b>Add Node</b>                      | This menu choice can be used e.g. if a router is broken and needs to be replaced. The children under the router must then be set up as new nodes in the association table, and instead of needing to go into the guest rooms to fix this it can be done from the <b>Add Node</b> dialog; see details <a href="#">here</a> . |
| <b>Edit Name</b>                     | edits the node's name in the database                                                                                                                                                                                                                                                                                       |
| <b>Memory Dump</b>                   | reads the memory; only used by Technical support                                                                                                                                                                                                                                                                            |
| <b>Upgrade Firmware in Router</b>    | loads a new firmware into the router; see <a href="#">Figure 33</a><br><b>Note:</b> The firmware shown is the one that has been loaded into the application server database at <b>Tools/Module firmware</b> ; see the client setup manual for details.                                                                      |
| Table 2                              |                                                                                                                                                                                                                                                                                                                             |

### 3.8.3 Right-click menu choices for ENs

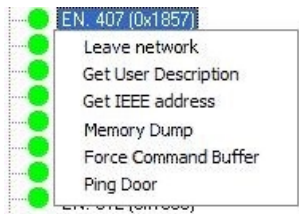


Figure 38

| Menu choice                 | Description                                                                                                                                                                                                |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Leave network</b>        | deregisters from the parent so another node can join<br><b>Note:</b> Due to a bug in BeeStack radio nodes of versions before 1.0.49, do not use the <b>Leave Network</b> command for these older versions. |
| <b>Get User Description</b> | gets parameters (e.g. link quality index, LQI) for the node<br><b>Note:</b> The LQI which is shown with <b>Get User Description</b> is an instantaneous value.                                             |
| <b>Get IEEE address</b>     | gets the IEEE address for the EN                                                                                                                                                                           |
| <b>Memory Dump</b>          | reads the memory; only used by Technical support                                                                                                                                                           |
| <b>Force Command Buffer</b> | forces the first buffered command for the lock to be sent immediately                                                                                                                                      |
| <b>Ping Door</b>            | sends a command to the door to check whether it is online or not                                                                                                                                           |
|                             | <i>Table 3</i>                                                                                                                                                                                             |

## 4. Online settings in the client

This section describes

- door parameters for online doors
- online authorities for operator templates
- the function *prevent invalid staff card usage*; this function is only applicable for hotel systems

For setup of doors (online as well as non-online doors), see the section about doors in the setup manual for the client.

### 4.1 Setting up door parameters in a hotel system

Go to **Tools/Options** in the client and click **Online** in the left column; you can make settings regarding

1. **Door ajar alarm**
2. **Status** - intruder and offline status
3. **Miscellaneous**
4. **Alarms**
5. **Safes**

#### 4.1.1 Door ajar alarm

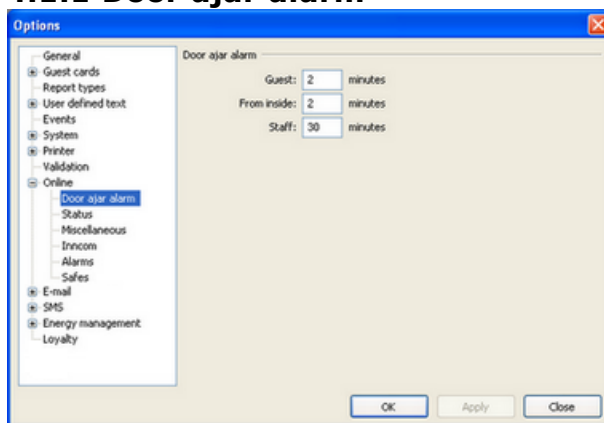


Figure 39

You can modify the time for when there will be a door ajar alarm. The door ajar alarm can be 1-60 minutes; 0 means that the alarm is not used. The default values are:

- 2 minutes when a guest card type has opened the door
- 2 minutes when a door has been opened from the inside
- 30 minutes when a staff card type has opened the door

## 4.1.2 Status

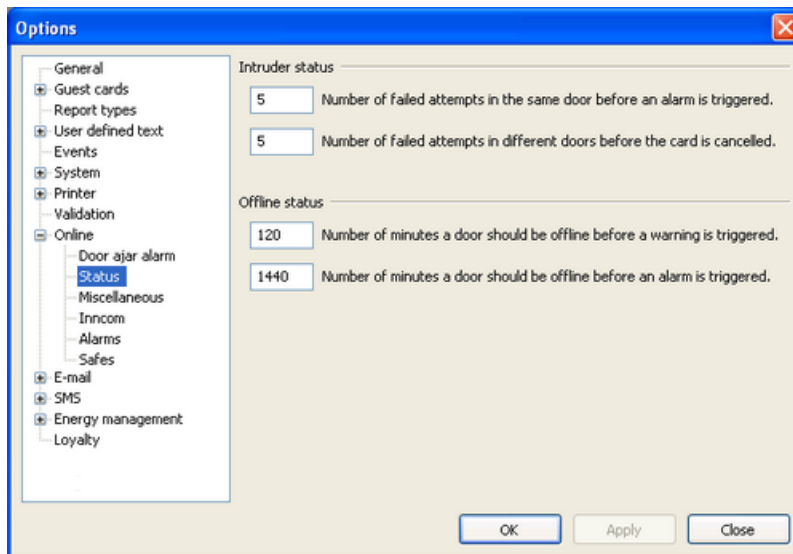


Figure 40

The values for intruder status and offline status can be modified. See the screenshot above and the sections below for default values.

### 4.1.2.1 Intruder status

- After five failed attempts in the same online door, an alarm is triggered. This is referred to as *sequential intruder*.
- After five failed attempts in different online doors, the card is cancelled and an alarm is triggered. This is referred to as *wandering intruder*.

### 4.1.2.2 Offline status

- After 120 minutes of offline status in an online door, a warning is triggered.
- After 1440 minutes of offline status in an online door, an alarm is triggered.

### 4.1.3 Miscellaneous

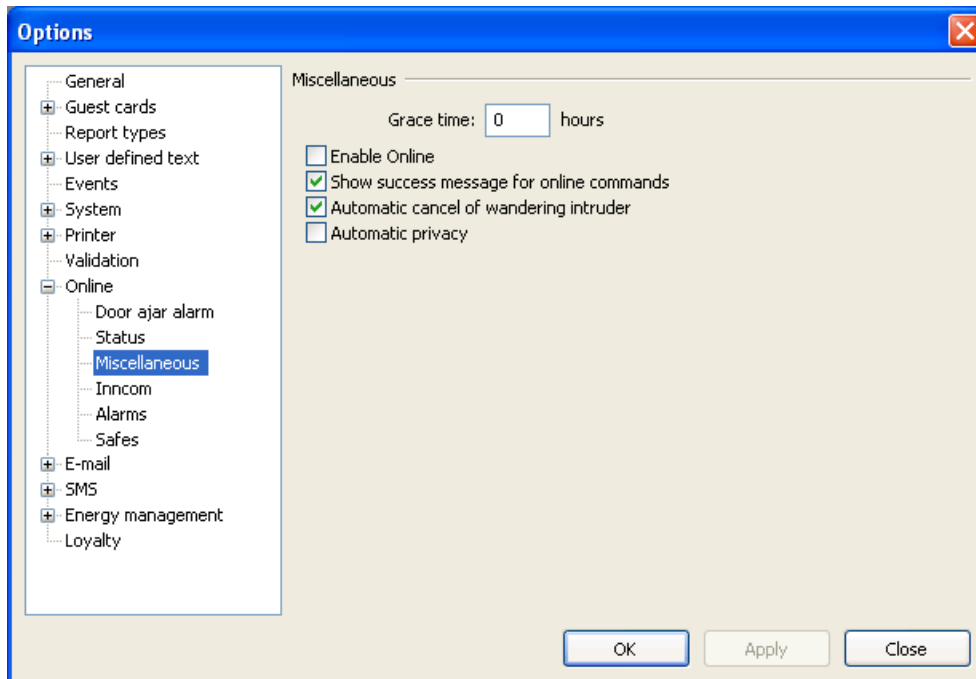


Figure 41

Under the **Miscellaneous** choice, you can

- set the grace time, i.e. for how long the guest(s) can enter a room after a check-out. The grace time can be 0-24 hours, default is 0.

**Note:** The default grace time which is set up at **Tools/Options/Online/Miscellaneous** applies unless a specific grace time is specified when the guest is checked out using the PMS interface. It also applies if the check-out is sent from the client.

- if for some reason desired, turn off the online functionality in the software by unmarking the checkbox 'Enable Online'.
- choose whether success messages should be shown or not when online commands have been successfully performed; default is that they are shown. See message below:

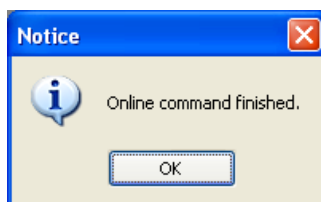


Figure 42

- choose whether *automatic cancel of wandering intruder* should be used or not. If a card is used five consecutive times in different online doors where it does not have access, the alarm 'wandering intruder' is triggered and the card is

cancelled. If the checkbox 'Automatic cancel of wandering intruder' is unmarked, the card will not be cancelled when the alarm is triggered.

- choose whether *automatic privacy* should be used or not; only applicable if the Orion EMS option is used. If 'Automatic privacy' is marked, the room will automatically be set in privacy as long as it is rented and there is a detection that someone is in the room.

**Note:** Automatic privacy is not a standard function; make sure to fully understand the function before enabling it.

Only the emergency card and – if applicable – cards belonging to user groups for which 'Ignore privacy' has been chosen in the User group details dialog will be able to enter when automatic privacy is set.

#### 4.1.4 Alarms

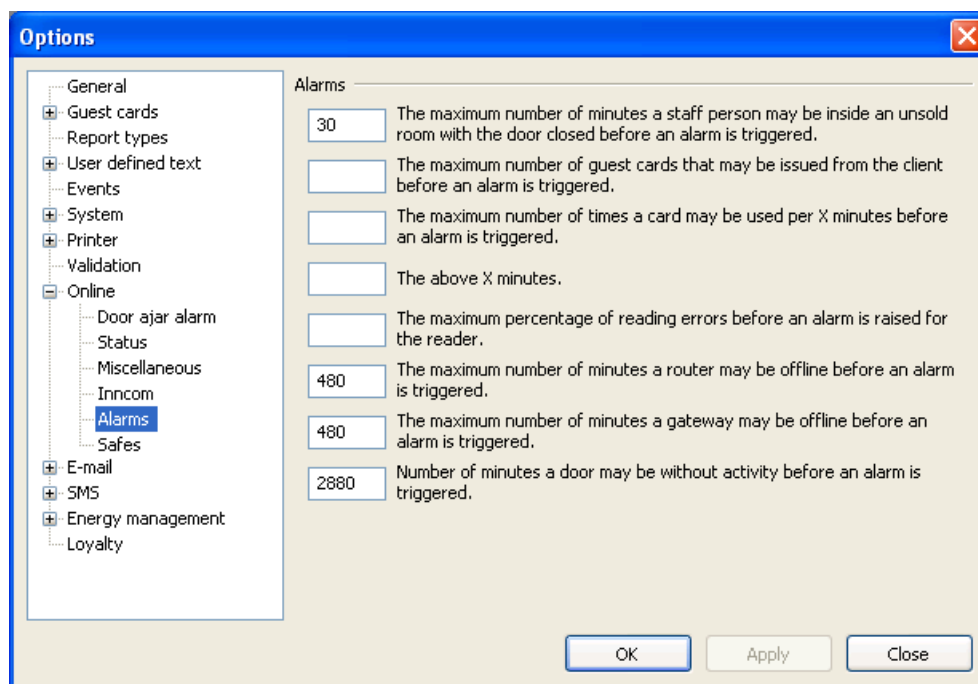


Figure 43

Under the **Alarms** choice, it is possible to set up different parameters related to the alarm list; see the user manual for the client for more information about the list.

**Note:** Offline alarms have a default holdback time of 24 hours, i.e. they are not shown as alarms in the client until 24 hours after they were triggered. An offline alarm is described with the name of the gateway or router that caused the alarm for any of its children.

- 'The maximum number of minutes a staff person may be inside an unsold room with the door closed before an alarm is triggered'; default is 30 minutes. This parameter is related to the alarm *Invalid staff-card usage*; see the user manual for the client for more information.
- 'The maximum number of guest cards that may be issued from the client before an alarm is triggered.' This parameter is related to the alarm *Too many guest cards issued in the client*; see 'To limit the guest card issuing' in the setup manual for the client for more information.
- 'The maximum number of times a card may be used per X minutes before an alarm is triggered.' This parameter is related to the alarm *Excessive card usage*.
- 'The above X minutes'. This parameter is related to the alarm *Excessive card usage*.
- 'The maximum percentage of reading errors before an alarm is raised for the reader.' This parameter is related to the alarm *Bad card reader*.  
**Note:** The alarm *Bad card reader* is triggered if the percentage of reading failures exceeds the percentage that is entered in this field. The alarm must be completed manually. The percentage is calculated continuously and there is no lower limit for the number of reads needed for the calculation.
- The maximum number of minutes a router may be offline before an alarm is triggered. This parameter is related to the alarm *ZigBee Router Offline*.
- The maximum number of minutes a gateway may be offline before an alarm is triggered. This parameter is related to the alarm *ZigBee Gateway Offline*.
- The maximum number of minutes a door may be without activity before an alarm is triggered. This parameter is related to the alarm *No door activity*.

#### 4.1.5 Safes

Safes can be set up at **Tools/Options/Online/Safes** and also require the *In-room safes* option; see *Installation instruction In-room safes option* for details.

## 4.2 Setting up door parameters in an access control system

Go to **Tools/Options** in the client and click **Online** in the left column; you can make settings regarding

1. **Status** - intruder and offline status; see [section 4.1.2](#) for details
2. **Miscellaneous**; see [section 4.1.3](#) for details
3. **Alarms**; see [section 4.1.4](#) for details

### 4.3 Setting up operator templates in a hotel system

In the **Operator Template Details** dialog, it is possible to set up what online commands a certain operator template should be allowed to perform. See the section about the **Online** tab in *User manual Visionline* for further information about the different online commands.

To set up/modify an operator template:

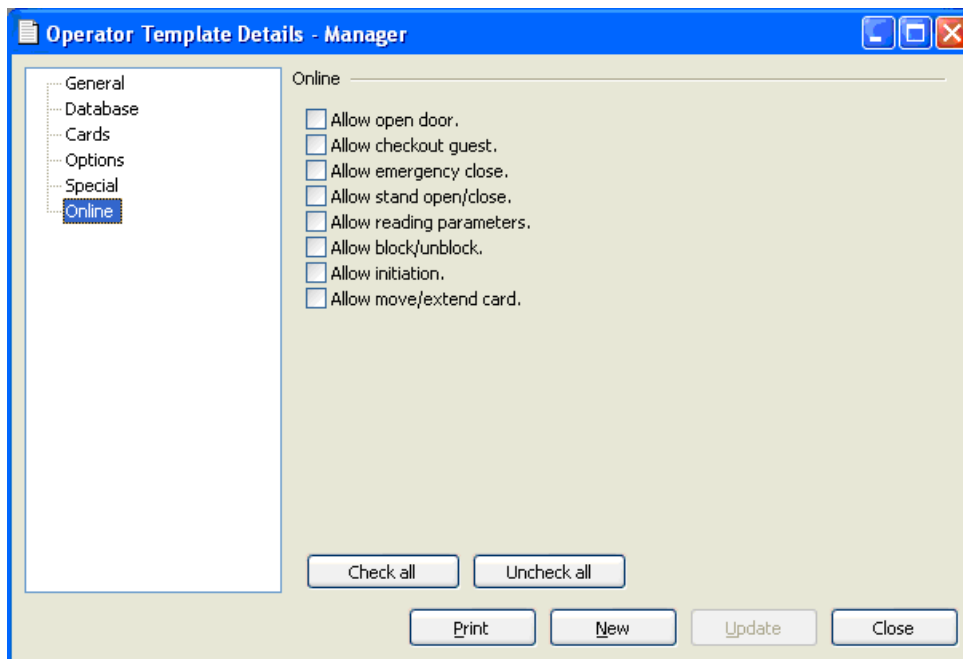


Figure 44

1. Double click on **Operator templates** under the **Lists** tab in the navigation window.
2. Mark the desired operator template and click **Properties** to open the **Operator Template Details** dialog (or click **Add** to add a new operator template; in that case, also make the appropriate choices under the other alternatives in the left part of the **Operator Template Details** dialog).
3. Mark **Online** in the left column.
4. Check the applicable online operation(s) to the right.
5. Click **Update**, if an existing operator template was updated; click **New** or **Save** if a new operator template was created.

**Note:** 'Allow emergency open' is by default only available for the distributor. Discuss with your distributor if this choice should be available for any other operator.

## 4.4 Setting up operator templates in an access control system

In the **Operator Template Details** dialog, it is possible to set up what online commands a certain operator template should be allowed to perform. See the section about the **Online** tab in the client user manual for further information about the different online commands.

To set up/modify an operator template:

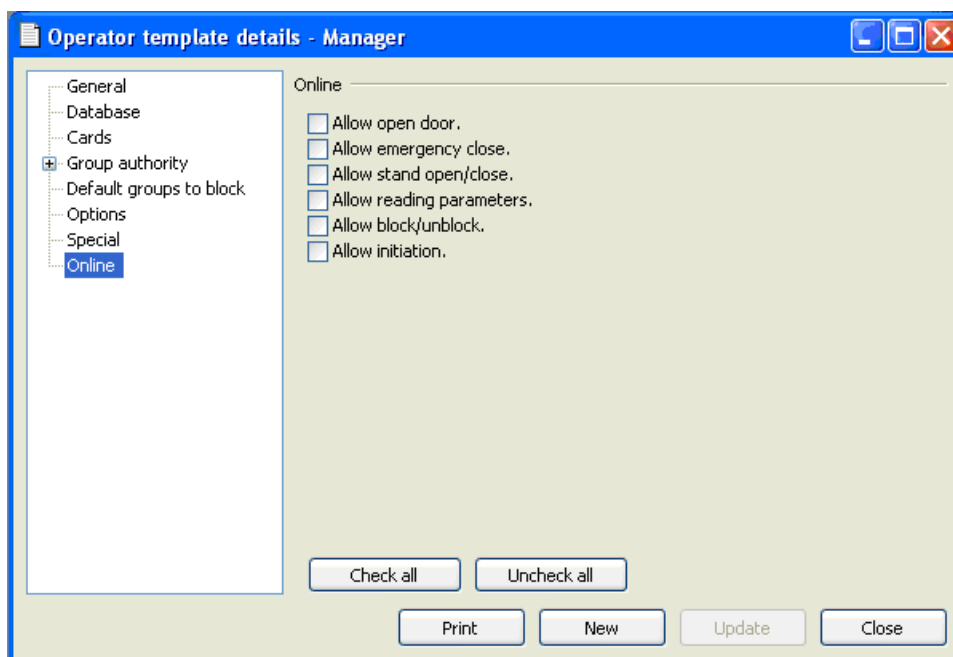


Figure 45

1. Double click on **Operator templates** under the **Lists** tab in the navigation window.
2. Mark the desired operator template and click **Properties** to open the **Operator Template Details** dialog (or click **Add** to add a new operator template; in that case, also make the appropriate choices under the other alternatives in the left part of the **Operator Template Details** dialog).
3. Mark **Online** in the left column.
4. Check the applicable online operation(s) to the right.
5. Click **Update**, if an existing operator template was updated; click **New** or **Save** if a new operator template was created.

**Note:** 'Allow emergency open' is by default only available for the distributor. Discuss with your distributor if this choice should be available for any other operator.

#### **4.5 Preventing invalid staff card usage (only applicable for hotel systems)**

To avoid unsuitable use of other cards than different types of guest cards in guest rooms, it is possible to set up that an alarm should be triggered if a person with a non-guest card dead-bolts a guest room from the inside, or stays too long inside the guest room. The function requires that the online option has been set. The invalid staff card usage function covers all card types except for cards of type guest, joiner, guest, joiner, suite, joiner suite, guest advanced, future arrival, one time and meeting room.

At **Tools/Options/Online/Alarms**, the choice 'The maximum number of minutes a staff person may be inside an unsold room with the door closed before an alarm is triggered' is available; default is 30 minutes. If the number of minutes should be changed, enter the applicable number and click **OK**; see [Figure 43](#).

To enable the alarm:

1. Go to **Tools/Enable/disable alarms**.
2. Mark 'Invalid staff-card usage'.
3. Click **Update** and **Close**.

The alarms will appear in the alarm list; see the user manual for the client for more information about the list.

See *Installation instruction Communication option* for information about

- how to set up receivers of alarm e-mails/SMSes
- how to set up e-mail receivers of reports

## 5. Issuing a ZigBee configuration card

The ZigBee configuration cards are smart/4k cards that are used for setting up online locks of ZigBee type. The following cards are available:

| Type                                                                                   | Description                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Set subproduct ZigBee                                                                  | Sets the lock in ZigBee mode                                                                                                                                                                                                                                                                                                |
| Start discovery in ZigBee                                                              | See section <a href="#">1.8 Discovery</a> . This card also sets the lock in ZigBee mode.                                                                                                                                                                                                                                    |
| Start orphan join in ZigBee                                                            | See section <a href="#">1.9 Orphan join</a> .                                                                                                                                                                                                                                                                               |
| Check ZigBee status                                                                    | See section <a href="#">7.3 Check online status with card</a>                                                                                                                                                                                                                                                               |
| Construction mode                                                                      | See section <a href="#">6.3 Set in construction mode</a>                                                                                                                                                                                                                                                                    |
| Enable EMI events <b>Note:</b> This also requires the <i>enable EMI events</i> option. | See below the EMI events that are sent to the thermostat from the lock: <ul style="list-style-type: none"> <li>- 0. Guest entrance</li> <li>- 1. Staff entrance</li> <li>- 2. Inside open</li> <li>- 3. Dead-bolt thrown</li> <li>- 4. Dead-bolt released</li> <li>- 5. Door closed</li> <li>- 6. Battery status</li> </ul> |
| Disable EMI events                                                                     |                                                                                                                                                                                                                                                                                                                             |
| Remove all sub products                                                                | Removes all sub products from the lock                                                                                                                                                                                                                                                                                      |
|                                                                                        | <i>Table 4</i>                                                                                                                                                                                                                                                                                                              |

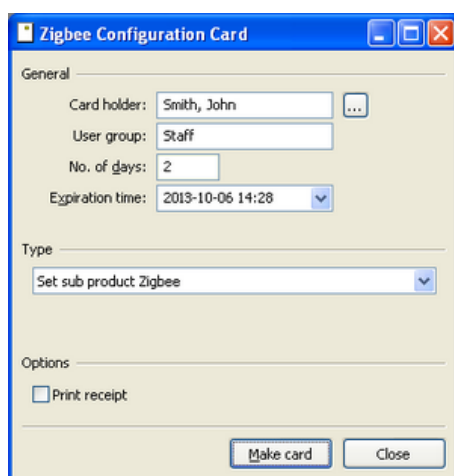


Figure 46

1. Double click on **ZigBee configuration** in the navigation window.
2. Select a cardholder from the operator list by clicking the button; double click on a name or mark the name and click **Select**.
3. Choose the expiration time of the card: enter the number of days for which the card shall be valid, or click the button next to the **Expiration time** field and mark a date in the calendar (or enter a date manually). The chosen date will appear at **Expiration time**; the number of days will change accordingly.
4. At **Type**, choose the applicable card type; see the list of available cards above for more information.
5. If you want a receipt for the cardholder to sign, check **Print receipt**. If you want an additional text of your own choice, you can add this under **Tools/Options/Printer/Receipt**, 'Note on receipt'; maximum 765 characters. This text will be added to all staff/operator receipts until it is changed or deleted.
6. Click **Make card**; present a card at the encoder.

## 6. System operation

There is a two-way communication with the locks – online commands are sent to the locks, and the locks send events.

### 6.1 Events

This section describes the transmission of events from the locks. Events are sent from the lock as they occur. Should there be any events in the queue, the first queued event is sent instead.

#### 6.1.1 Acknowledge

If there are any queued events, the lock will send the next event when the EN sends an acknowledgement to the lock. The acknowledgement will be delayed by the EN for approximately one minute in order not to flood the network.

#### 6.1.2 Retransmission

If there has been no acknowledgement for two minutes, the lock will retransmit the first event in the queue.

#### 6.1.3 Fallback

The time between retransmissions will be doubled until it reaches three hours. As soon as an acknowledgement is received, the retransmission time is reset to two minutes. If an acknowledgement has not been received after three hours, the last event from the lock will be retransmitted.

### 6.2 Online functionality

In the software, several online commands are available. See the [section 6.2.1](#) and also see the user manual for the client for more detailed information (section about online commands for a door and section about the **Online** tab; for cancellation of card, section about card list). Certain situations give an alarm; see [section 6.2.2](#) for more information.

### 6.2.1 Commands

The commands that are sent online to the locks include:

- Room move (only applicable for hotel systems; add a card to the new room and cancel it from the old room, and/or change the card expiration time)
- Check-out of guest; only applicable for hotel systems
- Cancellation of card
- Sending of parameters; time, calendar etc
- Remote open/stand open/emergency open and clear stand open/emergency close
- Blocking and unblocking of user groups
- Read-out of missing events

#### 6.2.1.1 Buffered commands

Some commands (but not interactive commands) can be buffered. Regardless of in what order the commands have been buffered, they will be sent according to the following priority:

1. Define local card (elevator, entrance)
2. Emergency open and close
3. Cancel
4. Anti-passback block and unblock
5. Checkout
6. Auto unblock
7. Auto block
8. Other buffered commands

### 6.2.2 Alarm list

Alarms are situations that require immediate action, e.g. offline lock.

Alarms are shown in the alarm list of the server software, and also in the **Alarms** view of SysMon. These alarm lists show all types of alarms, online related as non-online related; e.g. housekeeping failed.

The alarms can be used as a work order system. From the alarm list it is possible to assign an alarm to a user. If the *Communication* option is used, the assigned user can get an e-mail and/or SMS when the alarm is triggered. The user can then acknowledge the alarm, i.e. confirm that he intends to take care of the matter. When the matter has been taken care of, the alarm should be marked as completed in the alarm list of the server software. Some alarms are however auto-completed, e.g. when the system detects that they have been attended to they are automatically marked as 'Auto-completed' in the alarm list. See the user manual for the client for more information about the alarm list.

From the user notification list of the software it is possible to define which users that should be notified by e-mail or SMS (requires the *Communication* option) when

alarms occur. From the user notification list, it is also possible to set up that reports should be sent via e-mail. The reports can either be alarm reports, or reports about items that do not trigger alarms; e.g. a summary of issued cards.

See *Installation instruction Communication option* for more information about the user notification list and other features of the *Communication* option.

### 6.2.3 Endnode list

The endnode list in the software shows ZigBee endnodes in the system with IEEE address, firmware version and door name.

**Note:** Endnodes in thermostats are not shown in the list.

To remove an endnode from the endnode list:

1. Double click on **Endnodes** under the **Lists** tab in the navigation window.

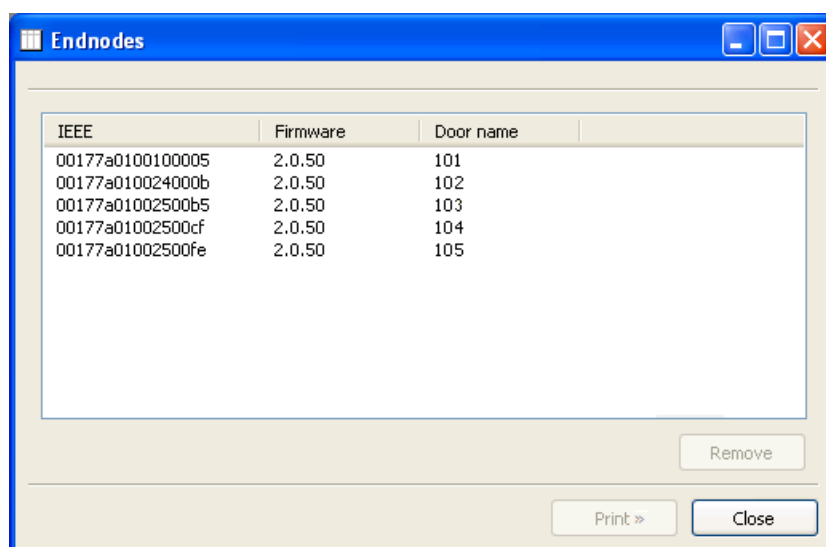


Figure 47

2. Mark the endnode in the list and click **Remove**. The endnode will automatically also be removed from the treeview in SysMon.

**Note:** If a \* is shown in the dialog caption, one or more endnodes have been added, removed or renamed. In this case, press the **Refresh** button in the endnode list.

### 6.2.4 Router list

The router list in the software contains all ZigBee routers in the system. The date column shows the last time the router announced itself. In case a router has been physically replaced there will be duplicates in the router list, but the last announcement time gives a hint of which router should be deleted.

To remove a router from the router list:

1. Double click on **Routers** under the **Lists** tab in the navigation window.

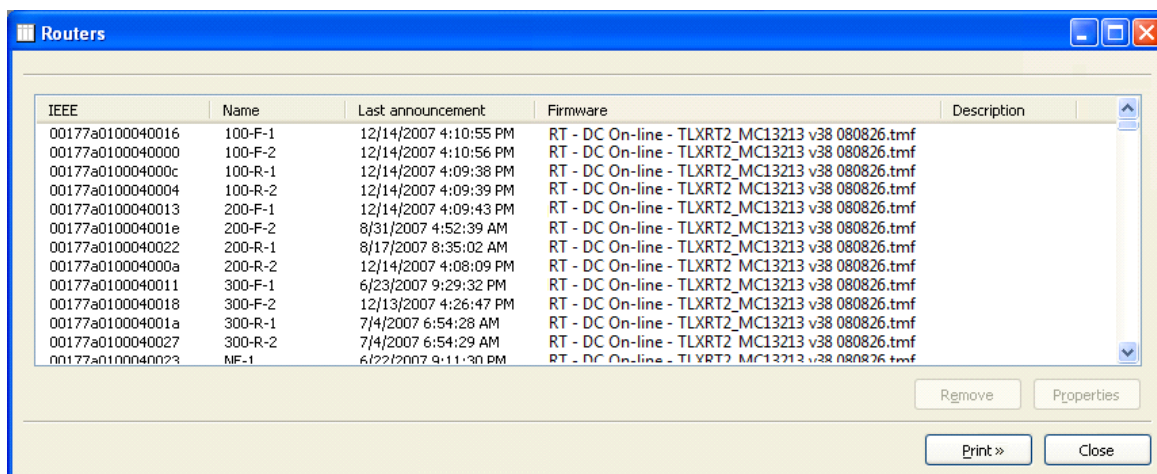


Figure 48

2. Mark the router in the list and click **Remove**. The router will automatically also be removed from the treeview in SysMon.

**Note:** If a \* is shown in the dialog caption, one or more routers have been added, removed or renamed. In this case, press the **Refresh** button in the router list.

### 6.2.5 Gateway list

The gateway list in the software contains all ZigBee gateways in the system.

To remove a gateway from the gateway list:

1. Double click on **Gateways** under the **Lists** tab in the navigation window.

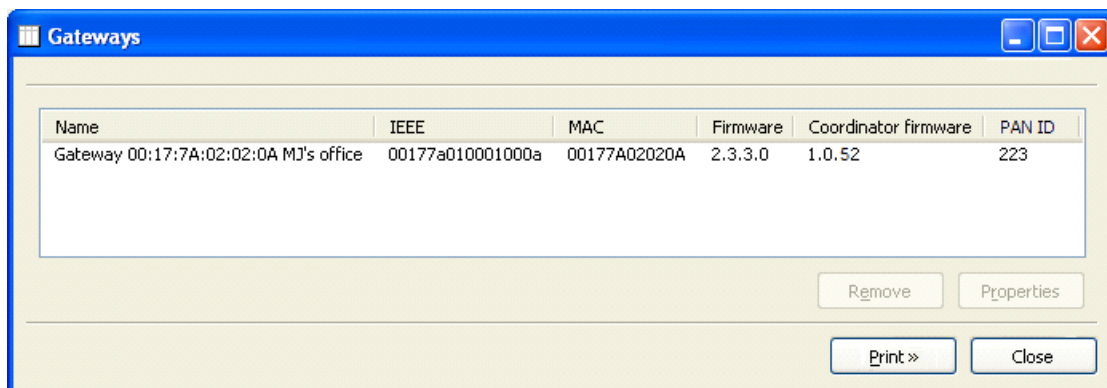


Figure 49

2. Mark the gateway in the list and click **Remove**. The gateway will automatically also be removed from the treeview in SysMon.

**Note:** If a \* is shown in the dialog caption, one or more gateways have been added, removed or renamed. In this case, press the **Refresh** button in the gateway list.

### 6.3 Setting in construction mode

If the network should be down for a period, e.g. during construction or renovation of the hotel, the locks should be set in construction mode to reduce battery consumption. Present a *Construction Mode card* at the locks (see [chapter 5 Issuing a ZigBee configuration card](#)); each lock will chirp and/or show a green LED signal, depending on lock model. When the card is presented, the EN will be turned off. If the EN in the lock is busy when the card is presented, instead a tick is heard and/or a very short green LED signal is shown. In this case, make a new try by presenting the *Construction Mode card* at the lock again.

To turn the EN on again, present a *Discovery card* at the lock; see [chapter 5 Issuing a ZigBee configuration card](#).

## 7. Commissioning

### 7.1 Printing a status report

SysMon provides a simple method for printing out the status of all the connected devices in the online network.

1. In the **Online Network** view in SysMon, click the **Print Status** button.  
**Note:** When clicking **Print Status**, it is possible to choose where to save the status report.

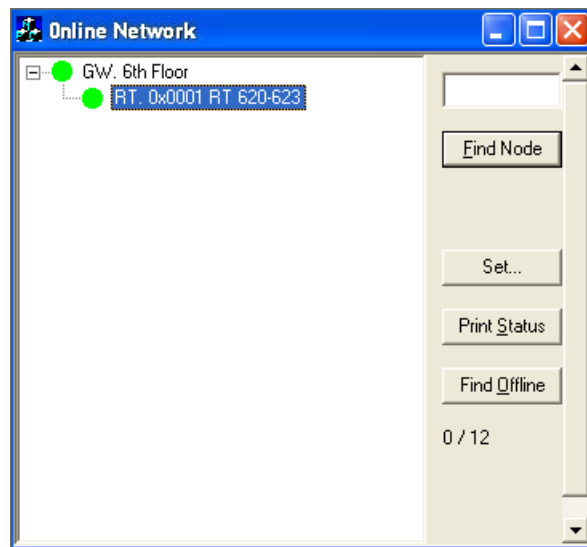


Figure 50

2. A Microsoft Excel spreadsheet will be written to the **TempData** folder in your installation folder.

The spreadsheet provides detailed information for each connected RT and EN; see example screenshot on next page. The information written to the document includes:

- name of the PAN (GW) the device is connected to
- RT name
- room; if it is an EN
- IEEE address
- version for RT, EN or GW; in the last case, GW firmware as well as version in the PAN coordinator (PC) are stated
- network address
- average link quality between the device and its parent
- time that last LQI measurement was taken
- last link quality index (LQI) recorded
- time for last successful command since the server was restarted; if this column says 'n/a', there has not yet been any answer from the lock

## 7.2 Pinging a door

While the spreadsheet described in [section 7.1](#) is convenient in showing the communication status of the online devices, it does not show that the locks themselves are communicating with the server. To do that it is necessary to 'ping' every online door from SysMon. A ping is a simple 'are you there' message sent from the server to the lock and back. The ping shows that the lock, the server, and all the devices in between are operating correctly.

To ping a door in SysMon:

1. Open the **Online Rooms** window at **View/Online Rooms**.
2. Mark the door you want to ping and click the **Ping Door** button on the right. You will see the status for the door change to offline.

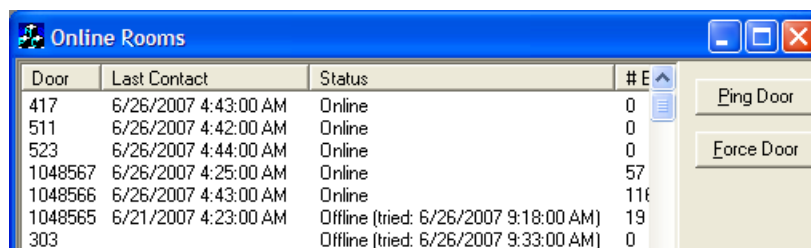


Figure 51

3. At the same time, you should watch the **Online Command Log** (found at **View/Online Commands**) so you can see the **Ping** command go out.

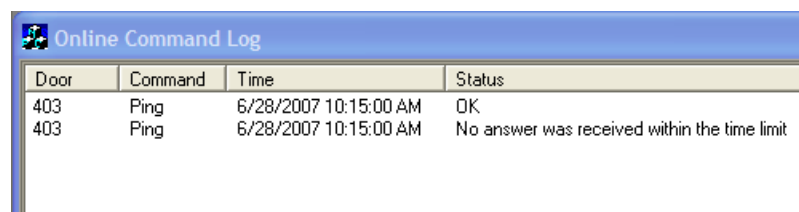


Figure 52

The status in the **Online Command Log** will always say 'No answer was received within the time limit' when the ping first goes out. If the ping is successful a response of **OK** will be sent back. If the ping fails you will not receive any other notification. You should allow up to 25 seconds for a ping to respond before labeling it a failure.

|   | A                                          | B                                                             | C                    | D                | E                | F               | G             | H        | I                | J                          |
|---|--------------------------------------------|---------------------------------------------------------------|----------------------|------------------|------------------|-----------------|---------------|----------|------------------|----------------------------|
| 1 | PAN name                                   | RT name                                                       | Room                 | IEEE address     | Version          | network address | LQI (average) | Last LQI | Last LQI at      | Last successful command at |
| 2 | Gateway 00:17:7A:02:00:02 Timelox Corridor |                                                               | 117 00177A0100240000 |                  |                  | 40 0x0c23       | 69%           | 88%      | 2009-03-25 04:06 | n/a                        |
| 3 | Gateway 00:17:7A:02:00:02 Timelox Corridor |                                                               | 103 00177A0100244C27 |                  |                  | 34 0x0c25       | 72%           | 80%      | 2009-03-25 04:07 | 2009-03-24 12:02           |
| 4 | Gateway 00:17:7A:02:00:02 Timelox Corridor |                                                               | 102 00177A0100245B2B |                  |                  | 34 0x0c26       | 80%           | 82%      | 2009-03-25 04:07 | 2009-03-24 12:00           |
| 5 | Gateway 00:17:7A:02:00:02 Timelox Corridor |                                                               | Hybrid               | 00177A0100245224 |                  | 40 0x0c24       | 97%           | 92%      | 2009-03-25 04:07 | 2009-03-24 10:32           |
| 6 | Gateway 00:17:7A:02:00:02 Timelox Corridor |                                                               |                      | 00177A0100050005 |                  | 38 0x0011       | 98%           | 99%      | 2009-03-25 04:06 | n/a                        |
| 7 | Gateway 00:17:7A:02:00:02 Timelox Corridor | Gateway 00:17:7A:02:00:02 Timelox Corridor. Mac: 00177A020002 |                      | 00177A010001001F | GW: 2.0.0.9. PC: | 40 0x0000       | 100%          |          |                  | n/a                        |

Figure 53: The screenshot shows an example of a status report; see [section 7.1](#) for more information.

As part of the commissioning process it is necessary to show that the server is able to communicate to every lock. This is shown in the last column of the status report in [section 7.1](#). If the server has been restarted, the last column of the status report will show 'n/a' for all locks – in this case the **Broadcast Answers** dialog can be used to determine whether the locks have answered or not, for all broadcast commands except for 'Ping'. See the user manual for the client for further information about **Broadcast Answers**.

As each floor or wing is completed, sign off on the status report to indicate that all of the online devices are communicating and the server is able to communicate with the locks.

### **7.3 Checking online status with card**

To check the online status directly at the lock, a *Check ZigBee Status card* can be used; see [chapter 5 ZigBee configuration card](#). When the card is presented at the lock, a check is made whether the EN in the lock has still got contact with its parent or not. If a chirp is heard when the card is presented at the lock, the lock is online; if an error beep is heard and/or three red LED signals are shown (depending on lock model) when the card is presented, the lock is offline. If the EN in the lock either is busy at the moment or is connected to the LCA (*lock case adapter*; for lock types where this is applicable), a tick is heard and/or a very short green LED signal is shown instead. In this case, make a new try by presenting the *Check ZigBee Status card* at the lock again.

## 8. Power loss and hardware failure

This section describes the mechanisms in place to recover from power loss as well as instructions to replace devices in case of hardware failure.

### 8.1 Lock electronics

If the lock electronics (not the online EN radio) have gone bad, they can be replaced with no interruption to the online network. Replace the lock electronics and put the lock back together. If power was temporarily disconnected from the EN, it will rejoin its parent on power up.

### 8.2 Endnode

If an EN loses power - typically due to a dead battery or battery replacement - it will rejoin its parent on power up using an *orphan join*. The radio ID is already in the appropriate RT and so it is allowed to join again without requiring a technician to re-open the RT.

If an EN needs to be replaced:

1. Make a leave on the old EN: right click on the EN in SysMon's **Online Network** view and choose **Leave Network**. In this way the old EN will deregister from the parent.  
**Note:** Due to a bug in BeeStack radio nodes of versions before 1.0.49, do not use the **Leave Network** command for these older versions.
2. **Important:** Wait for 40 seconds to avoid confusing the parent from which the EN has deregistered.
3. Make **Permit Joining** on the RT to which the EN should be connected. This can be done either by right clicking on the RT in SysMon's **Online Network** view and choosing **Permit Joining**, or by pressing the **F1** button on the RT.
4. Once **Permit Joining** has been made on the RT, install the new EN device in the lock. When it is powered up, present a Discovery card at the lock (see [chapter 5 Issuing a ZigBee configuration card](#)); the lock will chirp once and/or show a green LED signal, depending on lock model. The EN will announce itself to the server.
5. After the EN has joined the network, make **Forbid Joining** on the RT by right clicking on the RT in SysMon's **Online Network** view, or by pressing the **F1** button on the RT.

### 8.3 Router

If an RT loses power none of its children will be able to communicate to the server. When an RT loses power it will send a special SOS message to the server at least once to indicate that power may have been disconnected.

A power cut is illustrated with a red dot in front of the RT in SysMon:

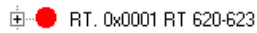


Figure 54

It can take up to three hours for the ENs to get online after recovery from a power cut. Upon power up the RT will perform an orphan join and will rejoin its parent GW or RT. Any children (EN or RT) will rejoin the RT automatically by performing orphan joins after they realize they have lost their parent.

To expedite this process in ENs:

1. Present an *Orphan Join card* at the door lock of each EN (see [chapter 5 Issuing a ZigBee configuration card](#)); each lock will chirp once and/or show a green LED signal, depending on lock model.

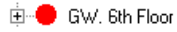
This may be a necessary step if the RT has been without power for an extended period of time as the ENs will only attempt an orphan join every so often (i.e. every three hours) in an attempt to conserve power.

If an RT needs to be replaced, the 'Permit Joining' command is used:

1. Make a leave on the old RT: right click on the RT in SysMon's **Online Network** view and choose **Leave Network**.  
In this way the old RT will deregister from the parent.  
**Note:** Due to a bug in BeeStack radio nodes of versions before 1.0.49, do not use the **Leave Network** command for these older versions.
2. **Important:** Wait for 40 seconds to avoid confusing the parent from which the old RT has deregistered.
3. Choose **Permit Joining** on the GW that the new RT should associate itself with.
4. Press the **F1** button when powering up the new RT. The RT will make a discovery, i.e. it will search for and join the GW on which **Permit Joining** has been made. After this, choose **Forbid Joining** on the GW.
5. Make **Permit Joining** on the new RT. This can be done either by right clicking on the new RT and choosing **Permit Joining**, or by pressing the **F1** button on the new RT. Present a Discovery card at the door lock of each EN that should associate with the new RT; each lock will chirp once and/or show a green LED signal, depending on lock model. For more information about the ZigBee configuration card, see [chapter 5 Issuing a ZigBee configuration card](#).
6. Each EN will search for and join the new RT on which **Permit Joining** has been chosen. After this, make **Forbid Joining** on the new RT. This is done either by right clicking on the new RT and choosing **Forbid Joining**, or by pressing the **F1** button on the new RT.

## 8.4 Gateway

If a GW loses power, none of its children (RT or EN) will be able to communicate to the server. A power cut is illustrated with a red dot in front of the GW in SysMon:



*Figure 55*

**Note:** If a GW is replaced, the entire commissioning process must be performed again; see sections [3.2-3.7](#).

## 8.5 Server

If the server loses power, no commands can be sent to the locks. When the server is recovered it will need to query the locks to retrieve any events it may have missed while it was down.

## 9. Redundancy and recovery

### 9.1 Communication channel

The ZigBee communication protocol has the built in capability to communicate on any one of 16 different channels (or frequencies). In the event that one or more channels are blocked or do not allow for adequate signal strength and stability, other channels may be used. **Important:** The ZigBee communication can be disturbed by e.g. Wi-Fi networks; always make sure to have as long distances as is physically possible between ZigBee devices and other radio equipment. It is also possible to use the **Set all coordinators** checkbox in the **Select channels** dialog; see details [below](#). If Wi-Fi disturbance still causes problems at a site, automatic channel change can be enabled. See more information about automatic channel change in [section 9.1.1](#).

If there are circumstances that dictate the devices should communicate on a specific channel (i.e. if there are other online devices or known interference on other channels), it is possible to force the devices to stay on a specific channel.

1. Right click on the concerned GW in SysMon's **Online Network** view and choose **Set channels**; a dialog as in Figure 56 will be shown.



Figure 56

2. By default, all 16 channels are checked since the GW will normally choose which of the 16 channels in the 2.4GHz band the nodes in the PAN should use. If a specific channel should be used, click **Clear** to uncheck all channels.
3. Check the desired channel(s); if more than one channel is checked, the best one will be chosen.
4. If the chosen channel(s) should be used for all GWs in the system, mark the checkbox **Set all coordinators**.
5. Click **OK**.

### 9.1.1 Automatic channel change

**Note:** Automatic channel change requires Visionline 1.12.2 or higher.

**Note:** Contact Technical support for details about how to enable automatic channel change.

The channel is automatically changed if:

- more than 25% of the end nodes are offline or have an LQI less than 30%
- (requires the *Orion EMS* option) more than five offline alarms have been received from the same thermostat during the last 24 hours; these alarms are triggered when the thermostat detects that a motion detector, lock or door switch is offline

The new channel is accepted if all routers report back within 15 minutes. If not, a new channel is selected. When the new channel has been accepted it will be retained during at least 24 hours even if the conditions above are met. At automatic channel change, all 16 channels are used regardless of the channels selected by the user.

## 9.2 Recovery

### 9.2.1 Polling

In order to preserve the battery, the ENs use a scheme called *polling*. Each EN wakes up periodically to check (poll) its parent for messages. Any message for the node is sent as an answer to the poll. The polling is the reason of variable answering times.

### 9.2.2 Fallback

If the poll does not give any answer five successive times, the EN has a fallback procedure. The missing answer can have two causes:

- the parent is offline due to a power cut
- the channel is jammed

In the latter case, follow steps 1-3 in section [Communication channel](#) to choose another channel. The EN will start orphan joining as a fallback, but continue to send polls even after this. This will find the parent in case there has been a channel switch. It will also find the parent in case there has been a power cut and the power returns. Due to the high power consumption of orphan joining, it will be performed at very long intervals:

- Initially, the interval will be one minute.
- For every time the orphan join fails, the interval is doubled until it reaches three hours.

**Note:** RTs have the same functionality, but as they are powered externally they will make an orphan join every 30 seconds.

## Appendix A: Online devices

### Gateway

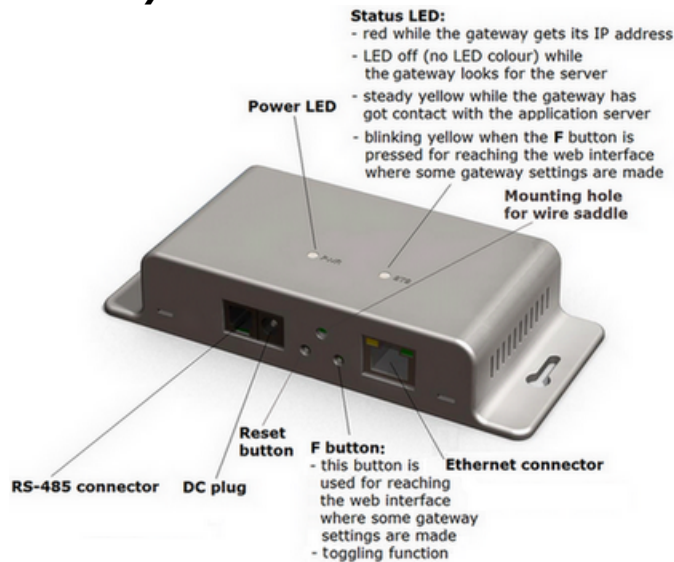


Figure A1

- Automatic adjustment to 10 or 100 Mbit/s networks
- Powered via Ethernet or by a power adapter (5VDC)  
**Note:** The gateway is of PoE class 1; power range 0.44-3.84W.
- Low power consumption
- The total number of gateways is virtually unlimited
- Can have either five routers or 15 endnodes connected as direct descendants
- Case with the dimensions 63 mm x 144 mm x 27,5 mm (2,48" x 5,67" x 1,08")
- Easy mounting (can be mounted either with adhesive VELCRO<sup>®</sup> strips or fastening screws; a package with two VELCRO<sup>®</sup> strips and two fastenings screws are enclosed)
- Weight: 116 g
- Flame retardant ABS
- UL94 V-0 approved
- Colour: RAL 7047
- Suitable for operation in the range 5-50° C and 10-90% non-condensed relative humidity

## Router

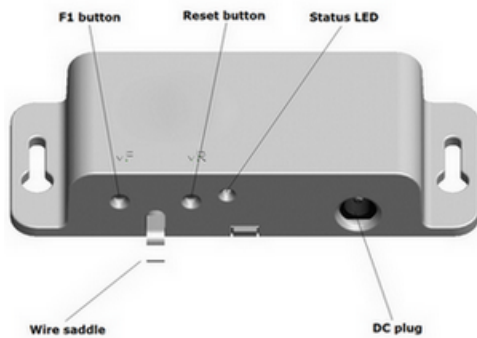


Figure A2

- Powered by a power adapter (5VDC)
- Low power consumption
- Can have either five routers or 15 endnodes connected as direct descendants
- There can be a maximum of five hops down the gateway (i.e. gateway - router - router - router - router - endnode). This limits the physical coverage of a PAN.  
***Important: Even though it is possible to have five hops, it is recommended to have maximum three hops, i.e. gateway - router - router - endnode. The link quality index (LQI) should be at least 30%.***
- Case with the dimensions 40 mm x 105 mm x 19,5 mm (1,57" x 4,13" x 0,77")
- Easy mounting (can be mounted either with adhesive VELCRO<sup>®</sup> strips or fastening screws; a package with two VELCRO<sup>®</sup> strips and two fastenings screws are enclosed)
- Weight: 36 g
- Flame retardant ABS
- UL94 V-0 approved
- Colour: RAL 7047
- Suitable for operation in the range 5-50° C and 10-90% non-condensed relative humidity

## Appendix B: Mounting of gateway and router

Preferred way of mounting the gateway is horizontally on the wall:

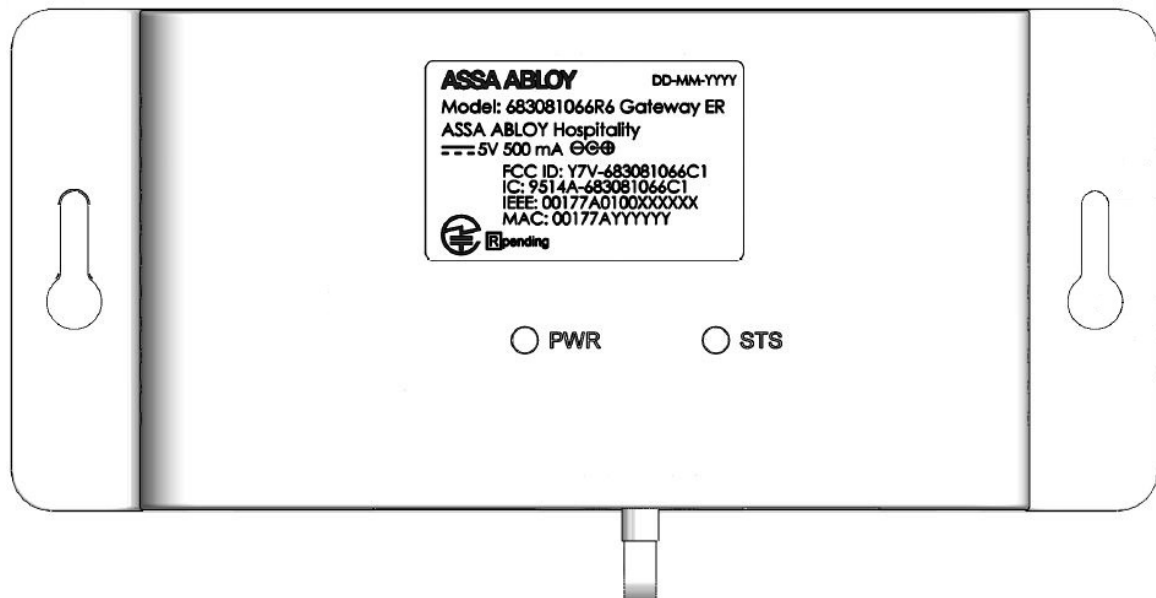


Figure B1

**Note:** The older type of gateway (9VDC) should be mounted vertically.

Preferred way of mounting the router is horizontally:



Figure B2

## Appendix C: Example configurations

Several online configurations are possible. Here are some examples:

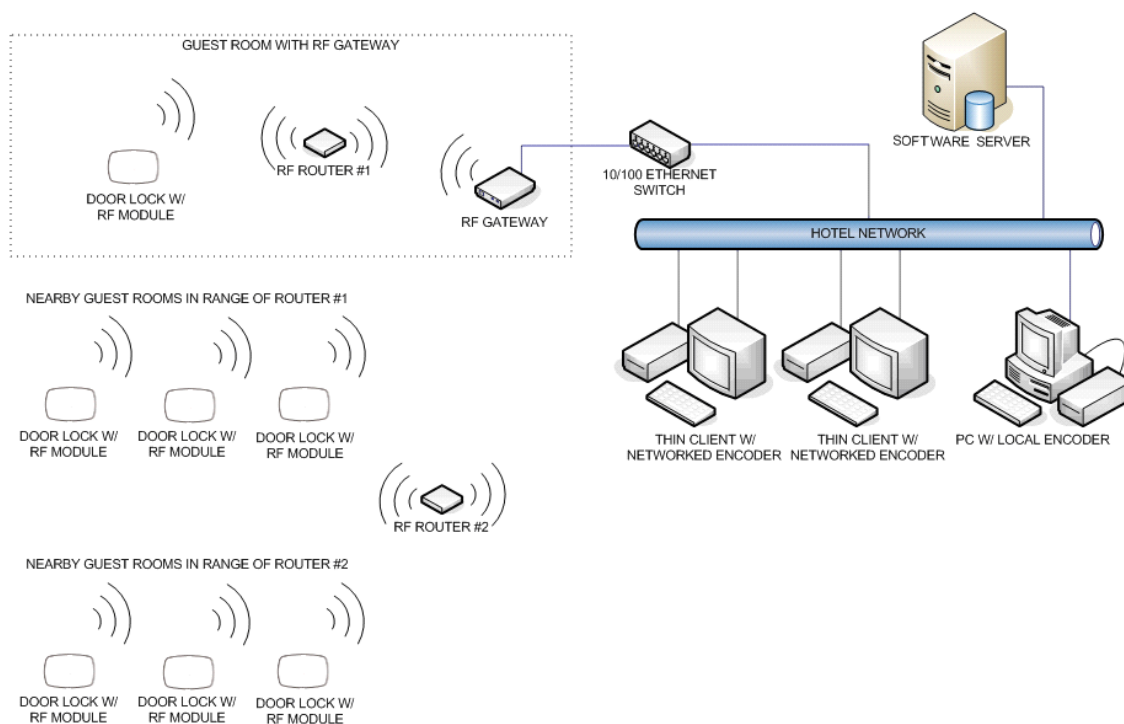


Figure C1: Basic setup with GWs, RTs and no firewall

### **Notes for the configuration in Figure C1:**

- RF door locks communicate with RF routers; maximum 15 locks per router.
- RF routers 1 and 2 communicate with the Rf gateway (it is recommended to have maximum three hops down the gateway, i.e. gateway - router - router - door lock, and an LQI, *link quality index*, of at least 30%). Routers are powered by a 5VDC plug-in transformer.
- RF gateways communicate with the application server over the Ethernet network of the property. Gateways are powered by a 5VDC plug-in transformer.
- The application server communicates to client stations and networked card encoders via the network of the property.

## Appendix C: Example configurations

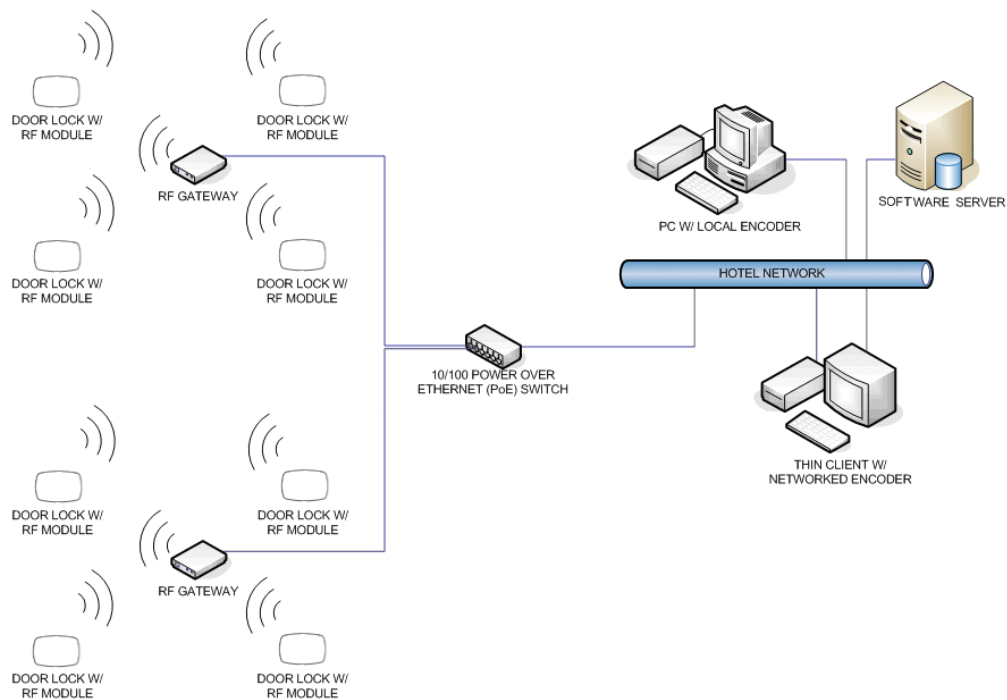


Figure C2: GWs using Power over Ethernet (PoE) communicating directly with doors.

### **Notes for the configuration in Figure C2:**

- RF door locks communicate with RF gateways; maximum 15 locks per gateway.
- RF gateways communicate with the application server over the Ethernet network of the property. Gateways are powered centrally by a PoE (*Power over Ethernet*) network switch.
- The application server communicates to client stations and networked card encoders via the network of the property.

## Appendix D: Web interface for gateway

The gateway parameters can be modified to suit the network where the gateway is located. This is done via the web interface as described below.

**Note:** See [Table E1](#) in *Appendix E* for a description of the gateway parameters.

To modify the gateway parameters:

Figure D1

1. Press the **F** button on the gateway for a short while; the status LED on top of the gateway will blink yellow. See in [Appendix A](#) where the **F** button is located.
2. In the web browser, enter <http://ipaddress>; the IP address to enter is shown when hovering over the gateway in SysMon. See example below for IP address entered in the web browser:

Figure D2

- Note:** If no DHCP server is available, use the *zero config* IP address which is shown in Wireshark; see [section 1.3.1](#) for more information about *zero config*.
3. Make the desired changes in the **ZigBee Gateway Setup** page; see example in Figure D1.
  4. If the server IP should be changed and there is no DNS (*Domain Name System*):
    - Enter the applicable **Server IP**
    - OR**
    - Mark the radio button 'Enable' for **Announcement Broadcast**; this makes the gateway find the server.
  5. When all desired changes have been done in the **ZigBee Gateway Setup** page:
    - Click **Save**.
    - Click **Reboot**.
    - Press the **F** button on the gateway again.

## Appendix E: Reset of gateway

If the gateway parameters need to be reset to default values, e.g. if a gateway should be used at a demo installation, press and hold the **F** button while powering up the gateway.

| Parameter                                                              | Default value |
|------------------------------------------------------------------------|---------------|
| Dynamic IP address (DHCP; <i>Dynamic Host Configuration Protocol</i> ) | Enabled       |
| Host IP address                                                        | 192.168.0.100 |
| Default gateway                                                        | 192.168.0.1   |
| Subnet mask                                                            | 255.255.255.0 |
| Announcement broadcast                                                 | Enabled       |
| Server port                                                            | 7799          |

*Table E1: Default values and descriptions of gateway parameters*

## Appendix F: Gateway boot-up

1. When a ZigBee gateway comes out of reset, it reads its IP configuration from a non-volatile memory.
2. If 'Dynamic IP Address' is set to **Disable** (see [Appendix D](#)): the gateway sets its IP address to the address stored in the config memory. Continue at [step 13](#) below.
3. If 'Dynamic IP Address' is set to **Enable** (see [Appendix D](#)): the gateway sends a *DHCP Request packet* with IP destination address 255.255.255.255, i.e. IP broadcast, requesting its most recently used IP address.
4. If the network/subnet configuration has not changed, the DHCP server will most likely send a *DHCP ACK packet*, allowing the gateway to continue to use the same IP. The DHCP server may use either *IP broadcast* or *unicast* for this packet; *broadcast* is however most commonly used. Continue at [step 10](#) below.
5. If the DHCP server is unwilling to let the gateway use the same address as before, or if the requested IP is out of scope, it sends a DHCP NAK.
6. Then the gateway resets its IP address to 0.0.0.0 and sends a *DHCP Discover packet* with IP destination address 255.255.255.255; IP broadcast.
7. If a DHCP server is available, it sends a *DHCP Offer packet*. Since the gateway has no valid IP address, the DHCP server must send to IP destination 255.255.255.255; IP broadcast.
8. The gateway receives the offer and sends a *DHCP Request packet*, as in [step 3](#) above, but this time requests the IP address offered by the DHCP server.
9. The DHCP server sends a *DHCP ACK packet*, confirming that the gateway may start using the new IP address. Unlike the ACK in [step 4](#) above, this ACK packet must be sent to IP destination address 255.255.255.255 (IP broadcast), since the gateway has not got any confirmed IP address yet.
10. The gateway performs gratuitous ARP (*Address Resolution Protocol*) to ensure that no other host has got the same IP.
11. If IP collision is detected, the gateway sends a *DHCP Decline packet* which refuses the assigned IP address and restarts the gateway's IP acquisition procedure.
12. *New functionality, Zigbee gateway version 2.3.0 and later*: If there is no DHCP server available on the subnet, the gateway self-assigns an IP address from the IPv4 Local Link address space (169.254.0.0/16), and sends gratuitous ARP to ensure that no other host has got the same IP.
13. The gateway reads the most recently used Visionline server IP address and tries to open a TCP connection to the server.
14. If the TCP connection attempt fails, the gateway will continue to try connections to the same IP over and over again – unless it detects that the network/subnet setup has changed, e.g. the gateway may have been moved to a new location. Then it will send an application specific service discovery request (*announcement broadcast*) with IP destination address 255.255.255.255; IP broadcast.
- 14 b. *New functionality, Zigbee gateway version 2.3.0 and later*: Even if the network/subnet setup is unchanged, but long time (one hour) has elapsed without any successful TCP connection with the Visionline server, the gateway will start sending service discovery requests.

## Appendix F: Gateway boot-up

15. If a Visionline server is on the same subnet, or if another gateway with a valid TCP connection to the server is on the subnet, they will send a reply to the querying unit, letting it know the IP address and TCP port of the Visionline server. The gateway then tries TCP connection to that IP.
- 15 b. *New functionality, Zigbee gateway version 2.3.0 and later:* From the payload supplied in the reply (the reply is sent with IP destination address 255.255.255.255, IP broadcast), the querying unit can determine if its own IP address properties are correct with respect to network class, default gateway IP and subnet mask. If required, it will self-assign a new IP-address within the subnet specified in the reply, and then send gratuitous ARP to ensure that no other host has got the same IP. Then it goes on and tries TCP connection to the received server IP address.
16. *New functionality, Zigbee gateway version 2.3.0 and later:* Prior to sending the service discovery request, the gateway tries to contact a DNS server (*Domain Name System*), with a request for resolving the most recently used Server Host Name. If that name is unknown to the DNS, the gateway tries to resolve the factory default Server Host Name. If any of the two names renders a successful DNS reply, the gateway uses the IP address received from the DNS server, and tries TCP connections to that address. If the factory default name is unknown too, or if a DNS server is not available at all, the gateway sends a service discovery request.

**Note:** 14, 14 b, (15/15b) and 16 will go on in a round robin way until the gateway has reached the server.

# Appendix G: More about how the gateway finds the server

## ***Introduction***

This appendix describes the process of how the gateway finds the server. The solution is based on DNS (*domain name system*) as well as on *announcement broadcast*, which is a proprietary implementation of *zero config*.

**Note:** A general description of setup of DNS entries cannot be made in this document, since this varies with the type of DNS server that is used.

There are three challenges when the gateway is connected to the network:

1. A new gateway must be able to find the server even if it is located on a separate subnet.
2. The gateway must be able to locate a backup server in case the primary server fails. The backup server is assumed to have the latest database from the primary server.
3. The above must be fulfilled even if there are multiple Visionline servers on the same network.

Commissioning of gateways:

[Single server - commissioning of gateways with DNS](#)

[Multiple servers - commissioning of gateways with DNS](#)

[Commissioning of gateways without DNS](#)

Switching to backup server:

[Single server - switching to backup server with DNS](#)

[Multiple servers - switching to backup server with DNS](#)

[Switching to backup server without DNS](#)

## Appendix G: More about how the gateway finds the server

### ***Commissioning of gateways***

If the gateway is located on the same subnet as the server, the gateway will locate the server using *announcement broadcast* without any need for manual configuration. However, the normal case is that the server and the gateway are located on different subnets. The first gateway for each subnet requires help from the DNS to locate the server.

### **Single server - commissioning of gateways with DNS**

1. Add a DNS entry called *timeloxserver* and let its IP address be the address of the application server to which the new gateway shall connect. The gateway will then make a DNS query using the name *timeloxserver* and in this way get the IP address of the server.
2. Connect the gateway to Ethernet and wait for it to appear in the SysMon **Online Network** tree.

### **Multiple servers - commissioning of gateways with DNS**

In the steps below, it is necessary to know the *system code*. To find it, double click on **System settings** under **Reports** in the software navigation window.

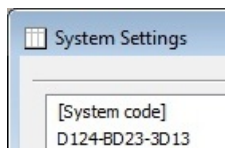


Figure G1

1. For each application server, add a new DNS entry with the system name for the concerned server. The system name is *timelox\_12-character system code without dashes*, e.g. *timelox\_D124BD233D13*.
2. In order to find the correct server at first installation, the gateways must be installed for one server at a time.
3. Let *timeloxserver* refer to the IP address of the first application server.
4. When all gateways have been installed for one server, the DNS entry for *timeloxserver* must be changed to the IP address of the next server.
5. When all gateways for the last server have been installed, the *timeloxserver* entry must be removed.

### **Commissioning of gateways without DNS**

1. Connect one gateway to each subnet. Use the web interface for the gateway to configure the IP address of the Visionline server. **Note:** This is only needed for the first gateway for each subnet, since the other gateways on the same subnet will retrieve the server IP address from the first one by *announcement broadcast*.
2. Continue adding gateways. They will automatically obtain the IP address of the application server from the gateways on the same subnet that are already online with the server.

### **Switching to backup server**

#### **Single server - switching to backup server with DNS**

1. Change the IP address of the *timeloxserver* entry in the DNS so it points to the backup server. The gateways will then connect to the backup server if the connection to the primary server is lost and cannot be re-established.

#### **Multiple servers - switching to backup server with DNS**

1. For the concerned application server, change the IP address of the system name entry in the DNS so it points to the backup server. The gateways will then connect to the backup server if the connection to the primary server is lost and cannot be re-established.

#### **Switching to backup server without DNS**

1. Remove the primary server from the network.
2. Assign the IP address of the primary server to the backup server  
**OR**  
enter the IP address of the backup server in the web interface for one gateway per subnet.

— **Note:** It will take one hour after the primary server closes its sockets until the rest of the gateways enable their *announcement broadcast*.

## Appendix H: Firmware upgrade

If one or a few online devices should be upgraded, this is done from SysMon; the applicable firmware must however first be saved to the database from the **Tools/Module firmware** dialog in the client. For details about **Tools/Module firmware**, see the appendix about firmware upgrade in the client setup manual.

When the firmware that is applicable for an upgrade has been loaded into the database, follow the steps below:

1. Click the **Set** button in the **Online Network** dialog and choose **Set Firmware Files for Bootloading**.

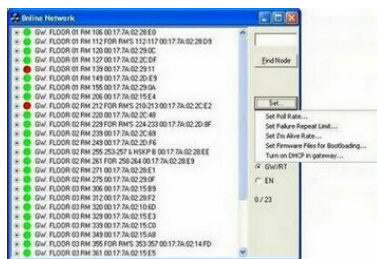


Figure H1

2. The **Select Firmware Files for Bootload** will show the firmwares that have been saved to the database. If several versions of the same firmware have been saved to the database, click the applicable  button if another version should be chosen.

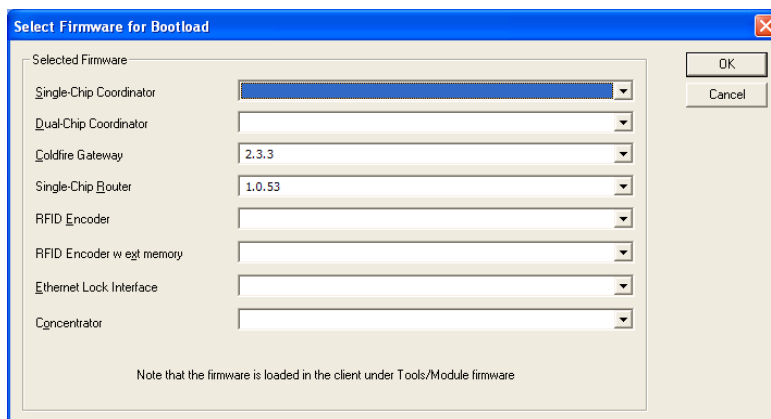


Figure H2

Page 10/10

**ASSA ABLOY Hospitality APAC**

E-mail: [apac.hospitality@assaabloy.com](mailto:apac.hospitality@assaabloy.com)

Phone: +65 6305 7670

**ASSA ABLOY Hospitality EMEA**

E-mail: [emea.hospitality@assaabloy.com](mailto:emea.hospitality@assaabloy.com)

Phone: +47 69 24 50 00

**ASSA ABLOY Hospitality North America**

E-mail: [northam.hospitality@assaabloy.com](mailto:northam.hospitality@assaabloy.com)

Phone: +1 972 907 2273

**ASSA ABLOY Hospitality Latin America**

E-mail: [lam.hospitality@assaabloy.com](mailto:lam.hospitality@assaabloy.com)

Phone: +52 55 36 40 12 00

**[www.assaabloyhospitality.com](http://www.assaabloyhospitality.com)**