User Manual
Online Option

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

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

66 3081 004-10

FCC/IC approval

The router and the endnode comply with RSS-GEN and part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) The router and the endnode may not cause harmful interference, and (2) the router and the endnode must accept any interference received, including interference that may cause undesired operation.

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

Changes or modifications not expressively approved by Timelox 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.

Router:

FCC: WYV-RT067

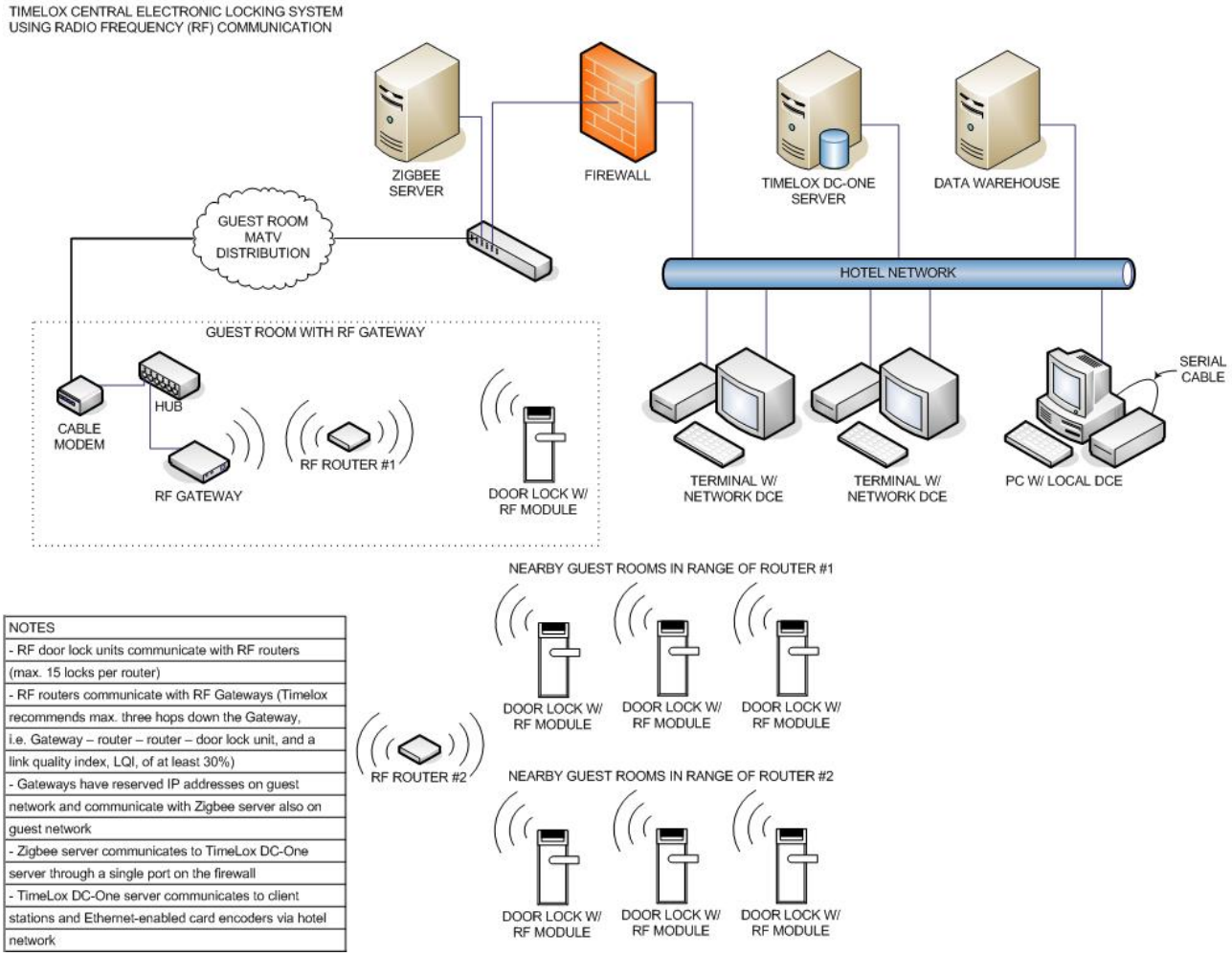
IC 8231A-RT067

Endnode:

FCC: WYV-EN055

IC 8231A-EN055

Table of contents



Example of Timelox online configuration. Several other configurations are possible (see Appendix C for some examples).

1 Introduction

With the online option, the locks can both send and retrieve information. Commands can be sent from the front desk to the lock. For example, a guest can change rooms without needing to go to the reception. Events are directly sent to the TimeLox DC-One server.

This section 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.

1.1 ZigBee standard

The online option is based on the ZigBee standard, a new 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 or RS-485. It automatically adjusts to 10 or 100 Mbit/s networks. In the TCP/IP case, the gateway starts by retrieving an IP address via DHCP (*Dynamic Host Configuration Protocol*). The gateway then automatically finds the server.

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.

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.

1.4 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.
- 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.

  Note: Timelox recommends a maximum of three hops, i.e. gateway – router – router – end node, down the gateway. 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.

- The lock and the endnode are powered by six AA cells in a special package.

See *Appendix A* for an exploded view of a lock.

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 (see section *1.10* for more information about 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* (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) is inserted into the lock. When the card is inserted, the lock will chirp once. If the endnode in the lock is busy at the moment, a tick will be heard instead. In this case, make a new try by inserting the Discovery card 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* (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) that will initiate an orphan join when inserted into a lock. When the card is inserted, the lock will chirp once. If the endnode in the lock is busy at the moment, a tick will be heard instead. In this case, make a new try by inserting the Orphan Join card again.

1.10 SysMon and TimeLox DC-One

The System Monitor (*SysMon*; found in the folder where TimeLox DC-One has been installed) is used for managing the online network. In SysMon all connected gateways, routers and endnodes are shown. There are two different operator levels for the online option in SysMon:

- *system manager* and other operators for which “Allow changing the settings in the ‘Options’ dialog” has been marked under the **Options** alternative at **Tools/Operator Template X-reference** in TimeLox DC-One.
- other operators.

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

System manager and other operators for which “Allow changing the settings in the ‘Options’ dialog” has been marked can perform all online operations in SysMon (except for those on distributor level), while other operators can basically only look in SysMon.

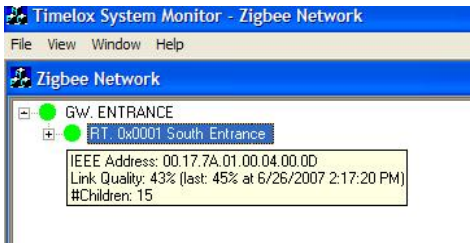
Online settings and commands are made in the TimeLox DC-One client; see sections *6 Settings in DC-One* and *7 Online Commands in DC-One*. Different operator templates can be given different authorities to give online commands; see section *6.1 Setting up operator templates*. For supervision of the system, see sections *4 Commissioning* and *5 General in DC-One*. If a dialog should be refreshed due to online changes, this is shown with a * in the dialog header (see example in the following screenshot). Click the **Refresh** button in the dialog.

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 ZigBee view; see example in the screenshot below. See section *2.3* for information about how to log on to SysMon and find the ZigBee 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 gateway, router or endnode in the SysMon ZigBee view and choose **Get User Description**.



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

If the LQI is below 25%, the dot in front of the node in SysMon is yellow; see example below.

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

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 Installation

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.

This section will describe how to install the online option in the TimeLox DC-One software, and also discuss the installation methods for each device in the system as well as options for forcing devices to connect to specific parent devices.

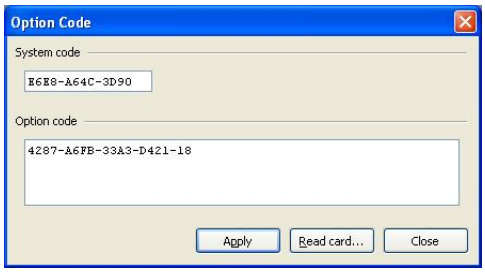
Software requirement

- TimeLox DC-One 1.7.0 or later is needed

2.1 Option installation

The online option must be installed in the Timelox DC-One software.

An operator with the authority to handle option codes must be logged on when options are set. System ID must be set before any option can be installed. Normally, options are set by the *system manager* or the distributor.

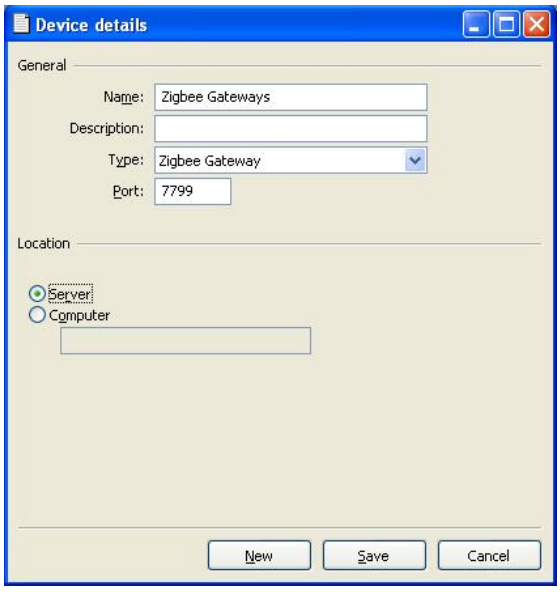


1. Go to **Tools/Option code**.
2. Click **Read card** and insert the option card in the encoder. The card will be overwritten and can only be used once.
2. **OR**
   Enter the option code (supplied by the distributor) and click **Apply**.

2.2 Server installation

- The Timelox DC-One server must be connected to the same network that the GW devices will be connected to
- The Timelox DC-One server must have the online option installed (see section *2.1*).

1. Before you install the first GW device, you must add a ZigBee gateway to the device list in DC-One (double click on **Devices** under the **Lists** tab in the navigation window and click **Add** to add a new device) using the following parameters:



2. When the fields have been filled in according to the screenshot above (port 7799 is pre-filled as default when choosing "ZigBee gateway" at **Type**), click **Save** and **Close**.

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 DC-One installed which you can use to directly connect to gateways as they are installed, or a laptop with a connection to the live TimeLox DC-One 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.

2.2.1 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 TimeLox DC-One server on another port. All traffic from the TimeLox DC-One 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.

2.2.1.1 TL Concentrator setup

The TimeLox DC-One software on the TimeLox DC-One 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 TimeLox DC-One server using port 7799.

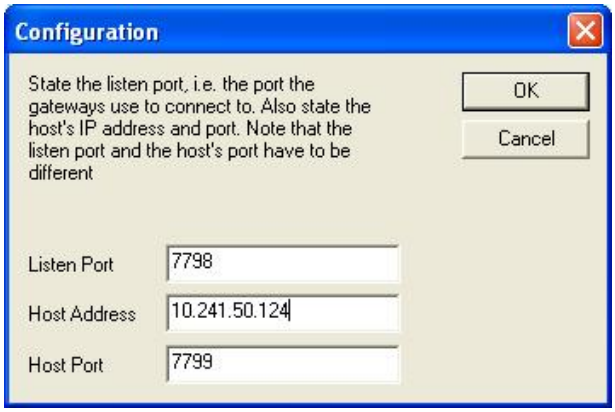
To set up these parameters:

1. Go to **Start/Run**.
2. Browse to the DC-One 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**.

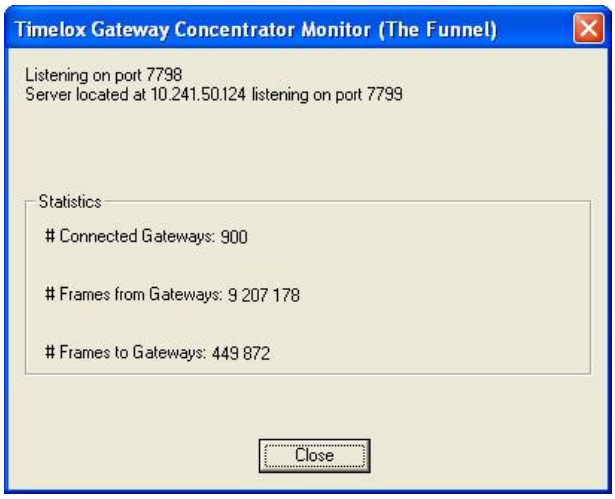


2.2.1.2 TL Concentrator monitor

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

1. Go to **Start/Run**.
2. Browse to the DC-One 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.

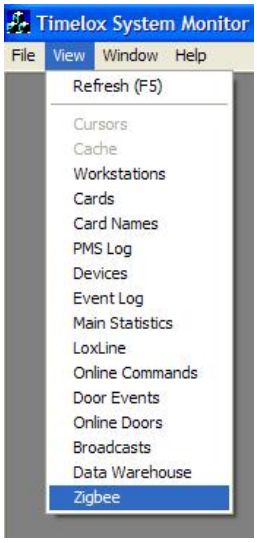


2.3 Gateway installation

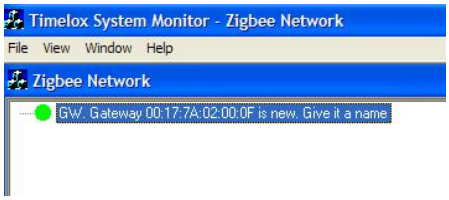
- The GW is powered by 9VDC using a plug in wall power adapter, or via power over Ethernet.
- For network connectivity the GW requires an available Ethernet port and a patch cord.

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

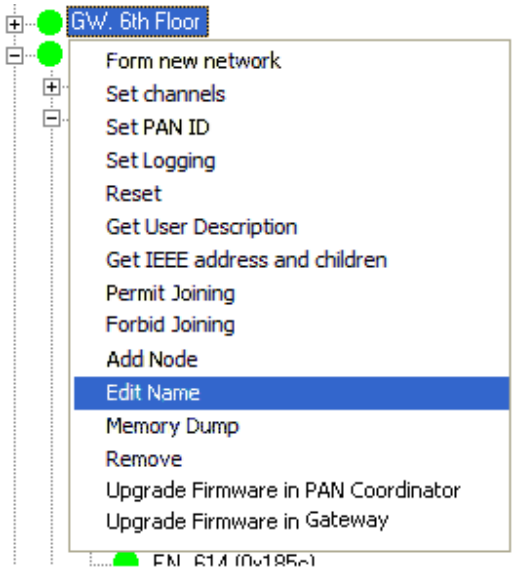
1. Open the System Monitor (SysMon), which is used for managing the online network. To open SysMon, double click on **SysMon.exe** in the DC-One installation folder.
2. Log on to SysMon: go to **File/Log on** and enter user ID and password. At "Operator card", choose the appropriate card encoder. Click **Enter**.



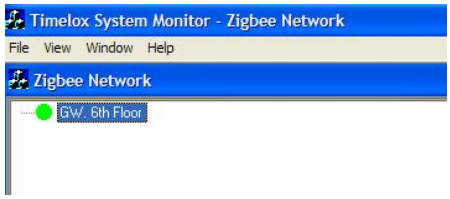
3. If it is not open already, open SysMon's ZigBee view at **View/ZigBee**. The ZigBee view of SysMon shows all connected GWs, RTs and ENs. Several useful commands are available by right clicking on nodes (see sections *2.9.1-2.9.3* for more information about the different commands).
4. Mount the GW in a convenient, out of the way location using the VELCRO® 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 ZigBee tree in SysMon.



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



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



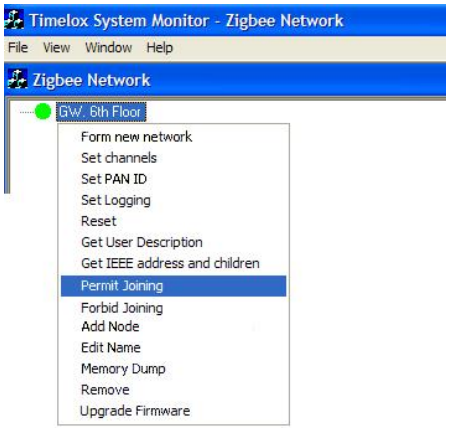
2.4 Adding routers to a gateway

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.

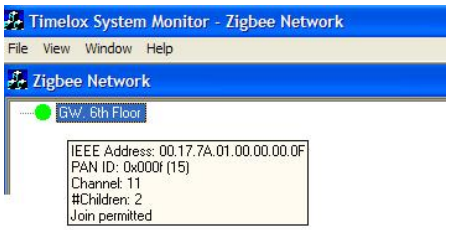
The recommended installation method is to use the enclosed VELCRO® strip to attach the RT to a wall or some other convenient location.

As described in section *1.10 SysMon and TimeLox DC-One*, system manager and other operators for which "Allow changing the settings in the 'Options' dialog" has been marked have the authority to perform all online operations in SysMon (except for those on distributor level). In sections *2.9.1-2.9.3*, it is described what operations that are available for all operators and what operations that can only be performed by system manager and other operators for which "Allow changing the settings in the 'Options' dialog" has been marked.

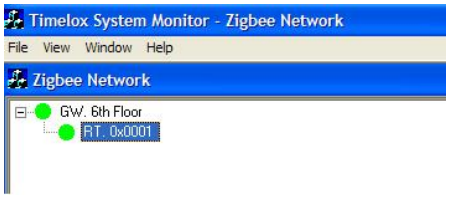
1. To add an RT to the online network, right click on the GW the RT should join and choose **Permit Joining**.



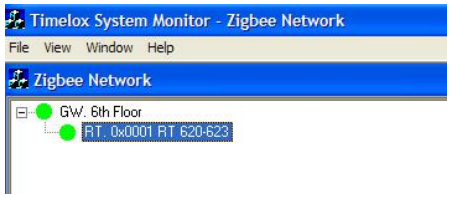
2. Hold your mouse over the GW name and a box will pop up containing some information about that device. At the bottom of that box you will see it says *Join permitted*, indicating that the GW now allows new connections.



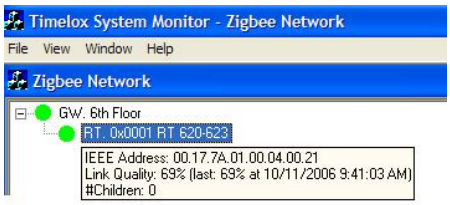
3. When the RT has been mounted with the VELCRO® strip, press the **F1** button on the RT while connecting power to the RT. The RT will power up and automatically begin looking for a parent device to associate with. It will discover the GW on which **Permit Joining** has been made, announce itself, and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



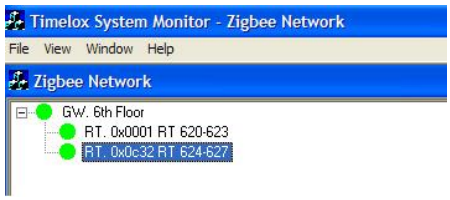
4. Right click on the RT and choose **Edit Name** to name the RT something meaningful. In our example we have named it "RT 620-623" to indicate the group of rooms that will be attached to that RT.



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%**.

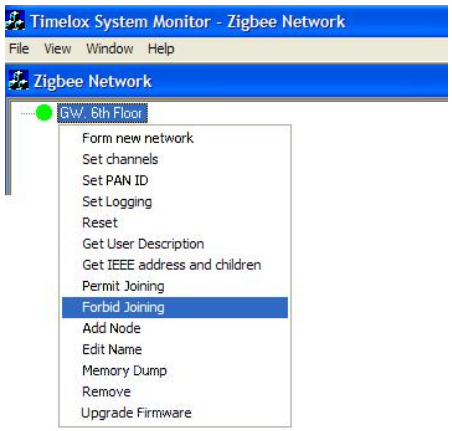


6. While the GW still says *Join permitted* when holding the mouse over the GW, plug in any additional RTs as needed (up to five per GW) and name them.

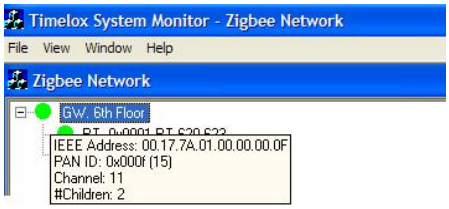


7. Hold your mouse over each RT to check the LQI making sure it is within acceptable limits.

8. When all desired RTs have been added to the GW, right click on the GW and choose **Forbid Joining**.



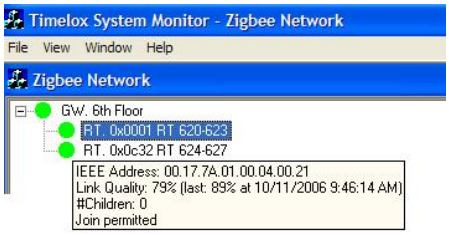
9. Hold your mouse over the GW to confirm it no longer says *Join permitted.*



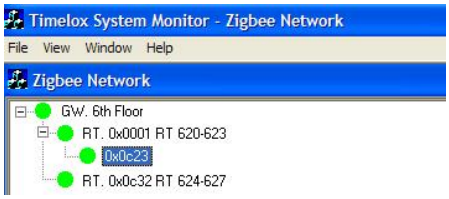
2.5 Adding endnodes to a router

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

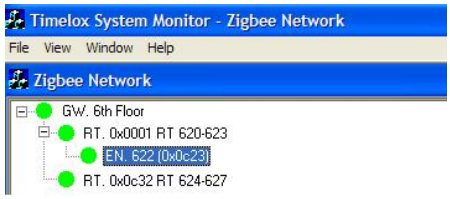
1. To add an EN to an RT, right click on the RT the EN should join and choose **Permit Joining** (or press the **F1** button on the RT). Hold your mouse over the RT to verify that joining is permitted.



2. Insert the Discovery card (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) in the lock. The lock will chirp once 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 ZigBee tree.



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 inserting a working key in the lock.

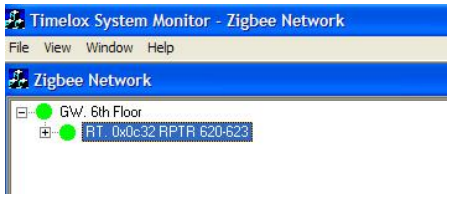


3. Hold your mouse over the lock to verify the LQI is within acceptable limits. Continue adding additional locks to the RT as needed. When finished, right click on the RT and choose **Forbid Joining**.

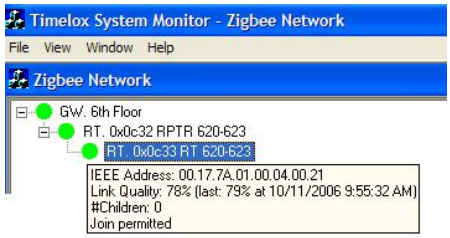
2.6 Using routers as repeaters

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 2nd 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.



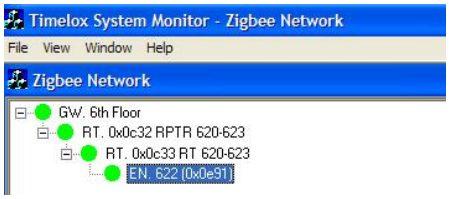
2. Choose **Forbid Joining** on the GW and **Permit Joining** on the 1st RT.
3. Plug in the 2nd RT. The 2nd RT will find and attach itself to the 1st RT.
4. Choose **Forbid Joining** on the 1st RT. Name the 2nd RT and choose **Permit Joining** on it.



5. Insert the Discovery card (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) in the lock; the lock will chirp once. 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 2nd RT.

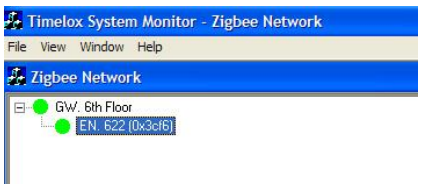


Note that the RT acting as a repeater is only capable of communicating to the GW and the 2nd RT; it is not possible at this time to repeat signals to a 2nd RT and communicate directly with locks at the same time.

2.7 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 insert the Discovery card (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) in the lock; the lock will chirp once. 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.



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

Note: RTs cannot be connected to a GW which has got ENs connected to it.

2.8 Forcing parents

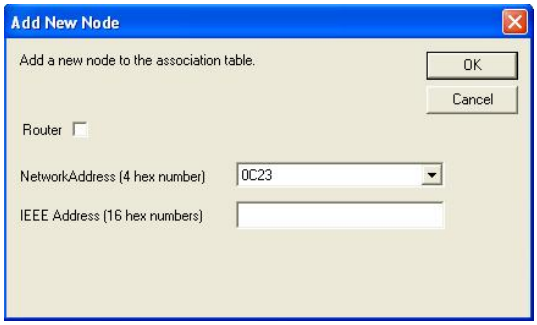
If a device such as an EN sees two RTs when it is in discovery mode (i.e. if "permit joining" has by mistake been made on two RTs belonging to different PANs at the same time), it is possible that the EN will not join the desired RT – i.e. the RT with which it has the strongest RF link. For this reason 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 can then be performed in two different ways; either by using the **Add Node** command or by using the **Permit Joining** command. With the **Add Node** command, you do not have to make discovery on the new device when it is added to its parent.

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.

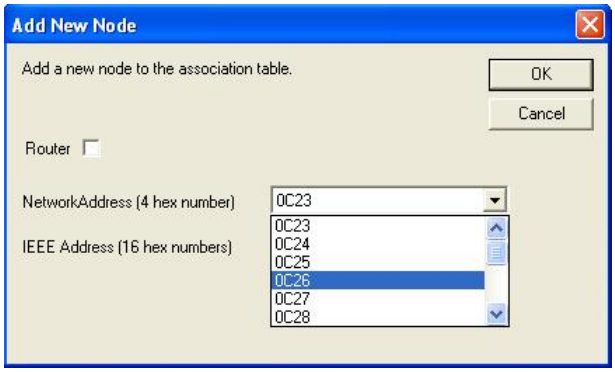
To force the EN by using the **Add Node** command:

1. Hover with the mouse over the EN in SysMon's ZigBee view and make a note of the IEEE address of the EN.
2. Right click on the EN and choose **Leave network**. The EN will deregister from RT-A.
3. **Important:** Wait for 40 seconds to avoid confusing RT-A from which the EN has deregistered.
4. Right click on RT-B and choose **Add Node**. The following dialog is shown.

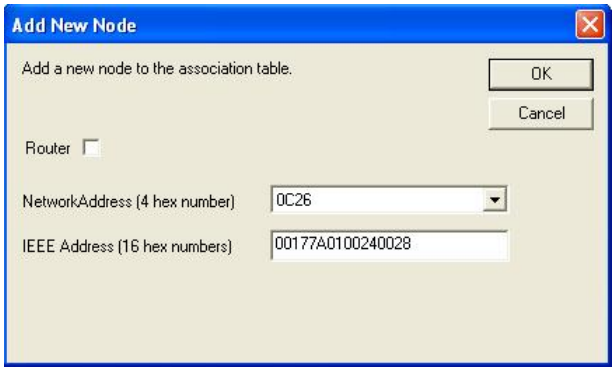


5. Choose the appropriate **Network Address** in the drop-down list (see example in the following screenshot).

Note: The **Add node** command only works on Z-stack devices.



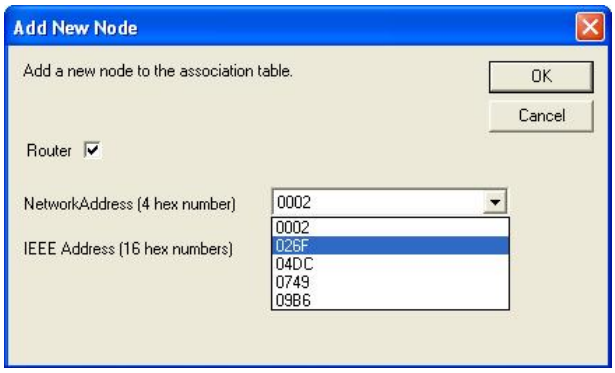
6. Enter the **IEEE Address** of the EN and click **OK**.



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.
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. Insert a Discovery card (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) in the EN door lock; the lock will chirp once. 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.

The two methods above with **Add Node** and **Permit Joining** respectively can also be applied to RTs joining RTs, RTs joining GWs, and ENs joining GWs. If the node that should be forced is an RT, the **Add New Node** dialog should be filled in according to the following steps:



1. Mark the "Router" check box.
2. Choose the appropriate **Network Address** in the drop-down list (see example in the screenshot above).
3. Enter the **IEEE Address** of the RT and click **OK**.

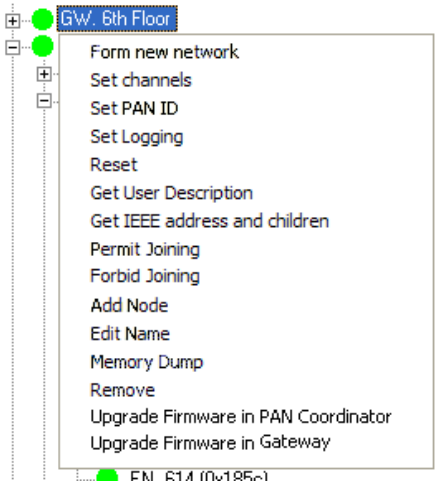
2.9 Right-click menus in SysMon

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: If another operator than system manager or an operator for which "Allow changing the settings in the 'Options' dialog" has been marked is logged on to SysMon, several choices in the right-click menus will be grayed. In the following description of the different menu choices, it is also stated which choices that are only available for sym etc. Other operators than sym can basically look in SysMon but not perform any operations.

Note: In sections *2.9.1-2.9.3*, "sym only" means system manager or another operator for which "Allow changing the settings in the 'Options' dialog" has been marked.

2.9.1 Right-click menu choices for GWs



Form new network (*sym only*) – makes a total reset of the GW

Set channels (*sym only*) – selects allowed channels (see section *9.1 Communication channel* for further information)

Set PAN ID (*sym only*) – sets another identity

Set Logging – defines logging for the node

Reset – makes a reset; all data is retained

Get User Description – gets parameters (for example link quality index, LQI) for the node. The LQI which is shown with **Get User Description** is an instantaneous value.

Get IEEE address and children – gets the IEEE address as well as all children stored in the association list

Permit Joining (*sym only*) – makes it possible for children to join

Forbid Joining – forbids children to join

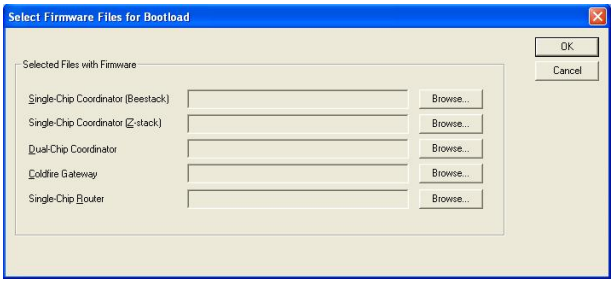
Add Node (*sym only*) – manually adds a node to the association list. When adding a new node, the network address is selected from a list. The network addresses shown are the ones that are possible for the parent that the node is added to. The network address uniquely defines the node's position in the PAN hierarchy and whether it is an RT or an EN. The GW has network address zero.

Edit Name (*sym only*) – edits the node's name in the database

Memory Dump (*sym only*) – reads the memory; only used by Technical support

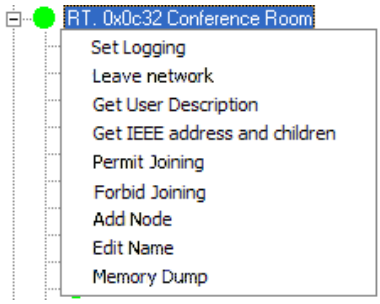
Remove (*sym only*) – removes the GW from the database

Upgrade Firmware in PAN Coordinator (*sym only*) – loads a new firmware into the PAN coordinator. In order to select which firmware file to load, click the **Set** button in the ZigBee view and select **Set Firmware Files for Bootloading**.



Upgrade Firmware in Gateway (*sym only*) – applicable for gateways with "GATEWAY ER" on the label.

2.9.2 Right-click menu choices for RTs



Set Logging – defines logging for the node

Leave network (*sym only*) – deregisters from the parent so another node can join

Get User Description – gets parameters (for example link quality index, LQI) for the node. The LQI which is shown with **Get User Description** is an instantaneous value.

Get IEEE address and children – gets the IEEE address as well as all children stored in the association list

Permit Joining (*sym only*) – makes it possible for children to join

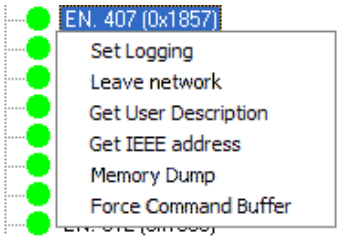
Forbid Joining – forbids children to join

Add Node (*sym only*) – manually adds a node to the association list. When adding a new node, the network address is selected from a list. The network addresses shown are the ones that are possible for the parent that the node is added to. The network address uniquely defines the node's position in the PAN hierarchy and whether it is an RT or an EN. The GW has network address zero.

Edit Name (*sym only*) – edits the node's name in the database

Memory Dump (*sym only*) – reads the memory; only used by Technical support

2.9.3 Right-click menu choices for ENs



Set Logging – defines logging for the node

Leave network (*sym only*) – deregisters from the parent so another node can join

Get User Description – gets parameters (for example link quality index, LQI) for the node. The LQI which is shown with **Get User Description** is an instantaneous value.

Get IEEE address – gets the IEEE address for the EN

Memory Dump (*sym only*) – reads the memory; only used by Technical support

Force Command Buffer – forces the first buffered command for the lock to be sent immediately

3 System operation

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

3.1 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.

3.1.1 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.

3.1.2 Retransmission

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

3.1.3 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.

3.2 Online functionality

In TimeLox DC-One, several online commands are available. See section *3.2.1* below and also see section *7 Online Commands in DC-One* for more information.

Certain situations (see sections *3.2.2-3.2.4*) give an alert, warning or alarm.

3.2.1 Commands

The commands that are sent online to the locks include:

- Room move (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
- 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

3.2.2 Alerts

By filtering events it is possible to alert users about situations that may need attention. These are *battery-low alarm* and *sequential intruder*.

3.2.3 Warnings

When a door has been offline for the time set up at **Tools/Options/Online/Status** in DC-One (default is 2 hours), a warning is given.

3.2.4 Alarms

Alarms are situations that require immediate action. The following alarm types are available:

- Sequential intruder*
- Report event (128 different reporting cards)
- Too many guest cards
- HotSOS error*
- Door ajar*
- Lock emergency open*
- Lock stand open*
- Inncom offline*
- Wandering intruder
- Time in the lock is off*
- Watchlist card used
- First usage of guest card
- Invalid staff card usage
- Emergency card is encoded
- Battery alarm*
- Housekeeping failed*

Alarms are shown in the alarm list of DC-One. Items marked with an asterisk are automatically revoked from the alarm list if they are revoked in reality, e.g. *door ajar* is revoked when the door is closed.

From the user notification list of DC-One it is possible to define which users that should be notified by e-mail (requires the mail notification option) or SMS (requires the SMS 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 *User manual TimeLox DC-One* (Art. No 865 100) for more information about the alarm list, the user notification list, the mail notification option and the SMS option.

3.3 Setting in construction mode

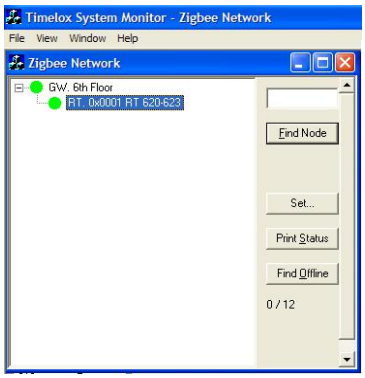
If the network should be down for a period, e.g. during construction or renovation of the hotel, the locks should be set in construction mode to reduce battery consumption. Insert a *Construction Mode card* (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) in the locks; a chirp is heard in each lock. If the EN in the lock is busy at the moment, a tick is heard instead. In this case, make a new try by inserting the Construction Mode card again.

4 Commissioning

4.1 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 ZigBee view in SysMon, click the **Print Status** button.



2. A Microsoft Excel spreadsheet will be written to the **TempData** folder in your DC-One 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)

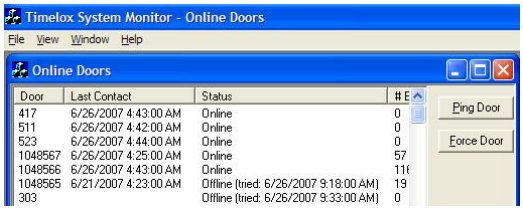
4.2 Pinging a door

While the spreadsheet described in section *4.1* 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.

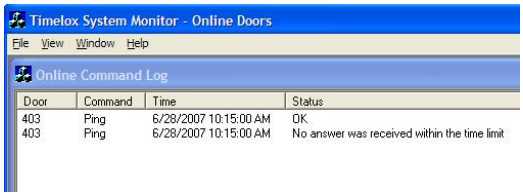
A ping is a simple "are you there" message sent from the server to the lock and back. The ping shows that the lock, the server, and all the devices in between are operating correctly.

To ping a door in SysMon:

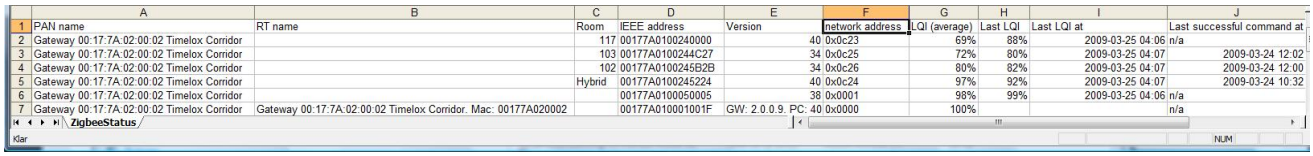
1. Open the **Online Doors** window at **View/Online Doors**.
2. Mark the door you want to ping and click the **Ping Door** button on the right. You will see the status for the door change to offline.



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.



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	0x0001	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

ZigbeeStatus

Klar

NUM

The screenshot shows an example of a status report; see section 4.1 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 *4.1*. 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 (see section *7.5 Broadcast commands* for further information) can be used to determine whether the locks have answered or not (for all broadcast commands except for “Ping”).

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.

4.3 Checking online status with card

To check the online status directly at the lock, a *Check ZigBee Status card* (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) can be used. When the card is inserted in 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 inserted, the lock is online; if an error beep is heard when the card is inserted, the lock is offline. If the EN in the lock is busy at the moment, a tick is heard instead. In this case, make a new try by inserting the Check ZigBee Status card again.

5 General in DC-One

5.1 Automatic operations

The following operations are performed automatically:

- The time is at regular intervals set in all online doors to avoid unsynchronized clocks.
- If the calendar is used, it is sent to all online doors initially (for 12 months ahead) and if changes are made to it. The calendar is also sent to all online doors every six months.
- Lock parameters are transferred to the locks at initiation with initiation card, service device or HCU. If any of the "ordinary" parameters event filters, open function or open mode – or any of the online parameters door ajar time or automatic privacy – is after the first initiation changed under **Tools/Options** in the DC-One software, the changes are sent to the concerned online locks by broadcast.
  Note: Automatic privacy is not applicable.

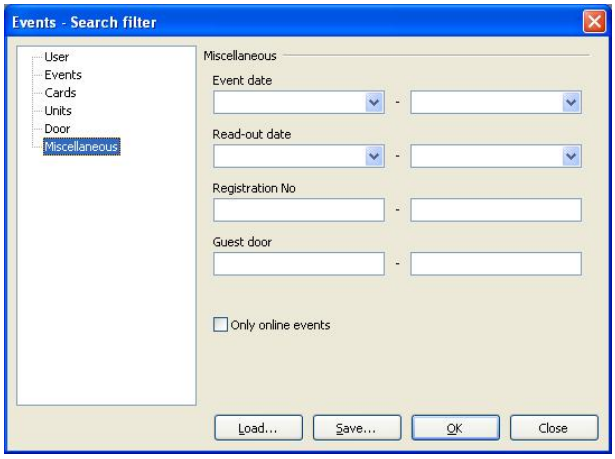
5.2 Online events

It is possible to show only online events in DC-One.

1. Double click on **Events** under the **Reports** tab in the navigation window.
2. Choose the applicable event search filter(s) in the left column of the **Events – Search filter** dialog.
   Note: At least one of the following requirements must be met when entering search filters:

- A door is selected
- Maximum two selected event sub groups have been chosen

3. Click **Miscellaneous** in the left column of the **Events – Search filter** dialog.

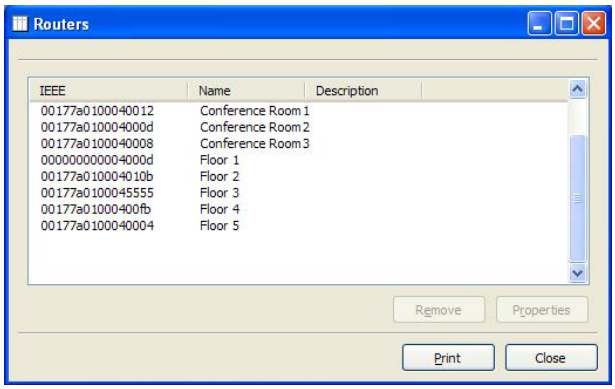


4. Check "Only online events" and click **OK**.
5. The events are shown in an event report.

5.3 Router list

When a router is connected, it will automatically appear in the router list of DC-One.

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

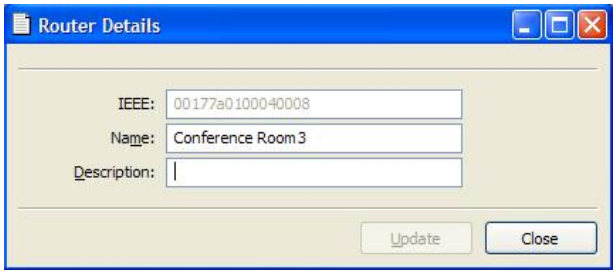


Each router's IEEE address is shown in the router list.

1. If a router is removed from the network, click **Remove** in the router list.

To modify the properties of a router:

1. Mark the router in the router list and click **Properties**.



2. The **Name** for the router is the same as the corresponding router name in SysMon. When the network is set up, the name can if desired be modified either in the DC-One dialog above or in SysMon.

   Note: If the name is changed in SysMon, the dialog **Router Details** in the DC-One client needs to be re-opened to show the new name. If the name is changed in the DC-One client, the ZigBee view in SysMon needs to be closed and open again for the change to be shown directly in SysMon.

3. If desired, enter a **Description** for the router.
4. Click **Update** and **Close**.

Note: The IEEE address is automatically included in the router list and cannot be modified in the DC-One client.

6 Settings in DC-One

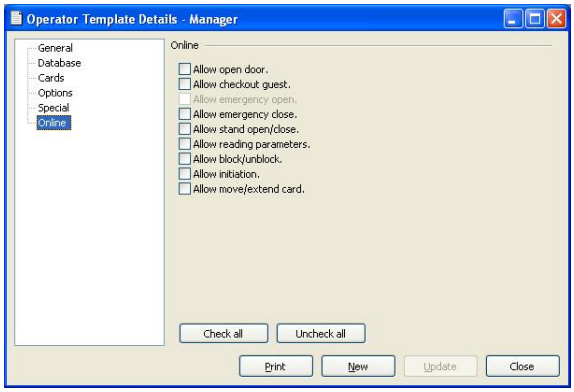
In the TimeLox DC-One software, settings for operator templates and online doors are made. For door setup in DC-One, see section *Doors* in *User manual TimeLox DC-One* (Art. No 865 100).

6.1 Setting up operator templates

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 section *7 Online commands in DC-One* for further information about the different commands.

To set up/modify an operator template:



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 appropriate online operations to the right.
5. Click **Update**, if an existing operator template was updated; click **New** or **Save** if a new operator template was created.

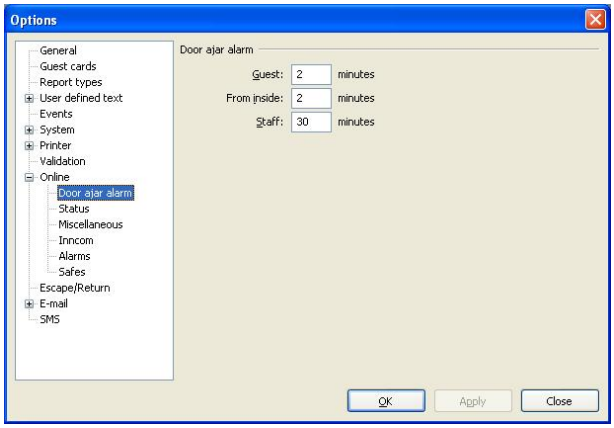
Note: "Allow emergency open" is by default only available for the distributor. Discuss with your distributor if this choice should be available for any other operator.

6.2 Setting up door parameters

Go to **Tools/Options** in the DC-One software and click **Online** in the left column; you can make settings regarding

1. **Door ajar alarm**
2. **Status** - intruder and offline status
3. **Miscellaneous** - grace time

6.2.1 Door ajar alarm

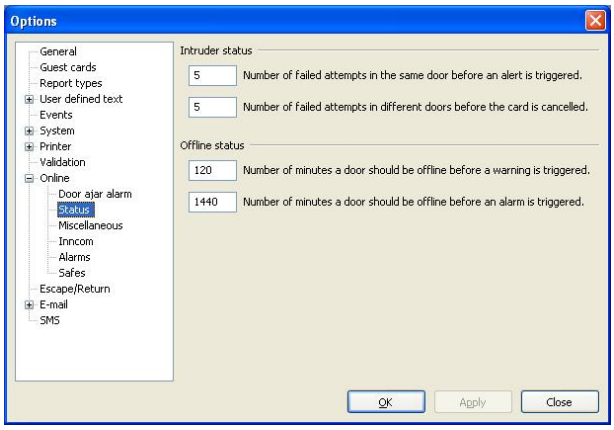


You can modify the time for when there will be a door ajar alarm. The door ajar alarm can be 1-60 minutes; 0 means that the alarm is not used.

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

6.2.2 Status



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

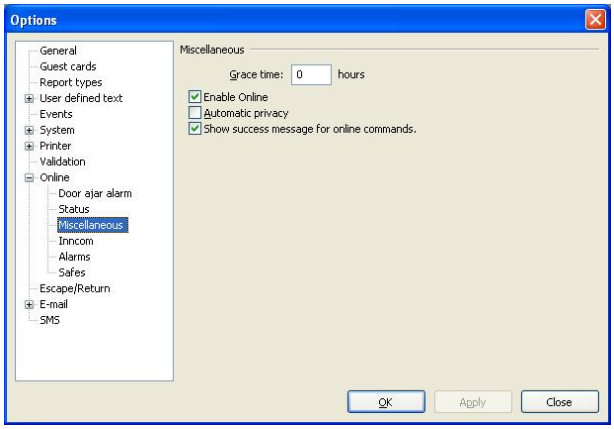
6.2.2.1 Intruder status

- After five failed attempts in the same online door, an alert 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*.

6.2.2.2 Offline status

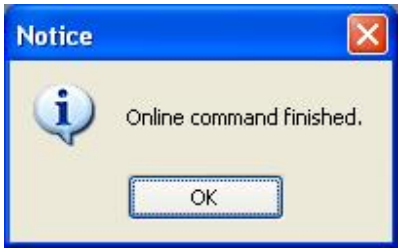
- After 120 minutes of offline status in an online door, a warning is triggered.
- After 1440 minutes of offline status in an online door, an alarm is triggered.

6.2.3 Miscellaneous

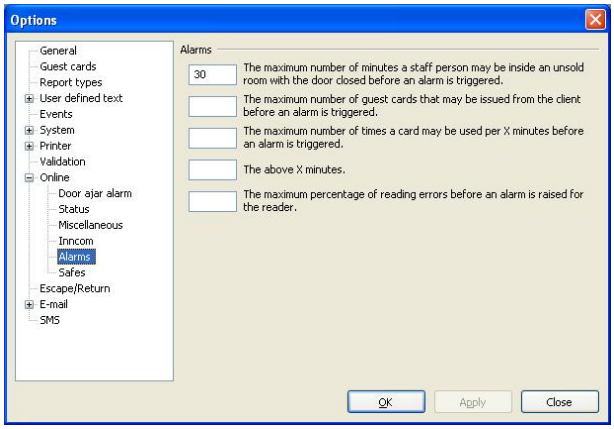


Under the "Miscellaneous" choice, you can

- 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 DC-One client.
- handle automatic privacy (not applicable).
- 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:



6.2.4 Alarms



Under the "Alarms" choice, it is possible to set up different parameters related to the alarm list (see *User manual TimeLox DC-One*, Art. No 865 100, for more information about the list).

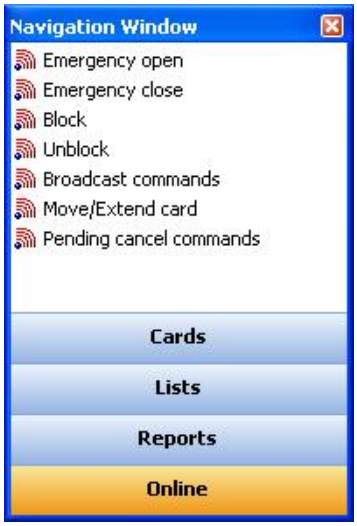
- "The maximum number of minutes a staff person may be inside an unsold room with the door closed before an alarm is triggered" (default is 30 minutes). This parameter is related to the alarm *Invalid staff card usage* (see *User manual TimeLox DC-One* for more information).
- "The maximum number of 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* (see "Limitation of guest card issuing" in *User manual TimeLox DC-One* 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*.

6.2.5 Safes

Safes can be set up at **Tools/Options/Online/Safes** but are not supported.

7. Online commands in DC-One

When the online option has been enabled in the Timelox software, there will be an **Online** tab in the navigation window. There will also be an **Online** menu with the same choices as in the navigation window. All online commands given from the Timelox software require that the operator enters his password.

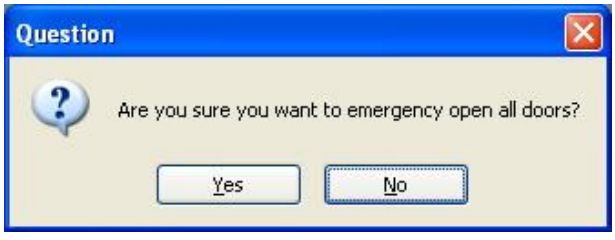


7.1 Emergency open

By one single command, it is possible to emergency open all online doors. This command can only be performed by the distributor.

Note: This is not recommended, unless a real emergency situation occurs!

1. Double click on **Emergency open** in the navigation window and enter your password. You will get a question:



2. Click **Yes**. A progress bar will appear, showing how far the emergency opening has proceeded.

7.2 Emergency close

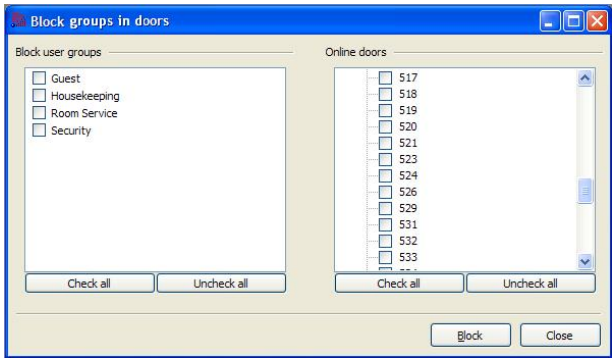
By one single command, it is possible to emergency close all online doors.

1. Double click on **Emergency close** in the navigation window and enter your password. As for the emergency opening, you will get a question whether you really want to emergency close all doors.
2. Click **Yes**. A progress bar will show how far the emergency closing has proceeded.

7.3 Block

One or more user groups can be blocked from some or all online doors.

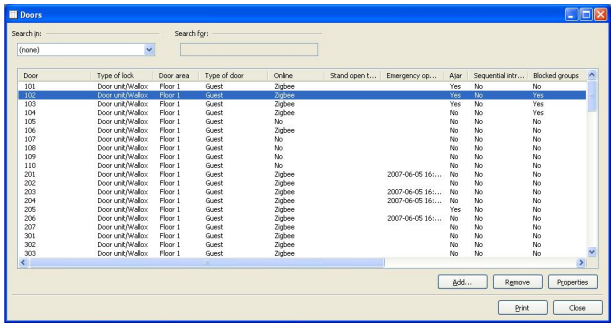
1. Double click on **Block** in the navigation window. You will get the dialog **Block groups in doors**, where all user groups and online doors of the system will appear (see picture).



2. Under “Block user groups”, check the user group(s) you want to block.
   Note: All groups except for the ones that are unchecked will be blocked - also user groups that are added to the system after the blocking mode has been set in the lock(s).
3. Under “Online doors”, check one or more doors from which you want to block the marked user group(s). All door areas which contain one or more online doors are shown. By clicking the plus sign of a door area, you will see the different online doors of that area. Check the appropriate one(s).
   Note: The blocking command is sent for one door at a time.

4. Click **Block** and enter your password.
5. Click **Close**.

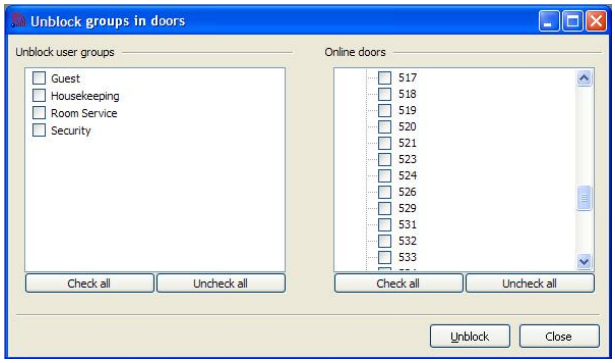
When one or more user groups have been blocked from a door, this will be shown with a “Yes” under the column “Blocked groups” in the door list (see example in the following picture).



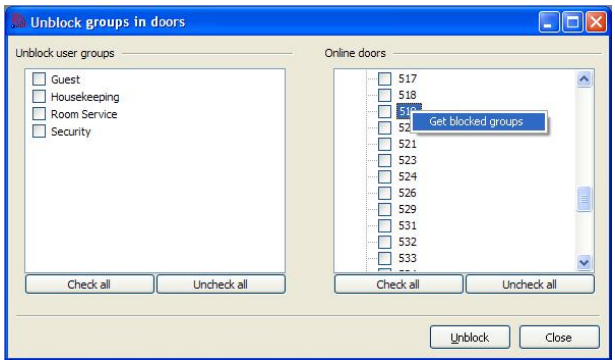
7.4 Unblock

One or more user groups can be unblocked from some or all online doors.

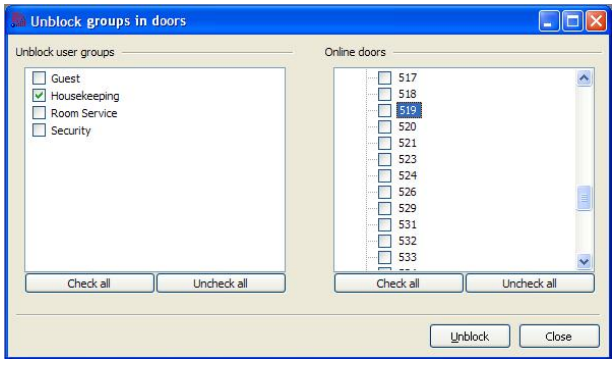
1. Double click on **Unblock** in the navigation window. You will get the dialog **Unblock groups in doors**, where all user groups and online doors of the system will appear (see picture).



2. If you are not sure in which door(s) there are blocked user groups, look in the column “Blocked groups” in the door list (double click on Doors under the Lists tab in the navigation window; click on the column “Blocked groups” twice to get the doors with blocked groups on top of the door list). If you are not sure which user group(s) that has previously been blocked from a certain door: right click in the dialog **Unblock groups in doors** on the appropriate door under “Online doors” and choose **Get blocked groups**.



The group(s) that has previously been blocked will be checked – see example in the following picture.

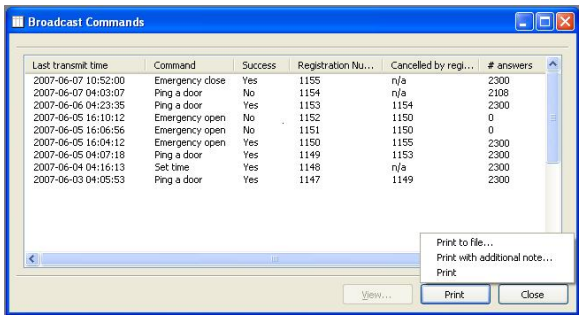


3. Under “Online doors”, check one or more doors from which you want to unblock the user group(s). All door areas which contain one or more online doors are shown. By clicking the plus sign of a door area, you will see the different online doors of that area. Check the appropriate one(s). If the user group(s) which should be unblocked has not been marked by using **Get blocked groups** as described in step 2, also check the user group(s) under “Unblock user groups”.
   Note: The unblocking command is sent for one door at a time.
4. Click **Unblock** and enter your password.
5. Click **Close**.

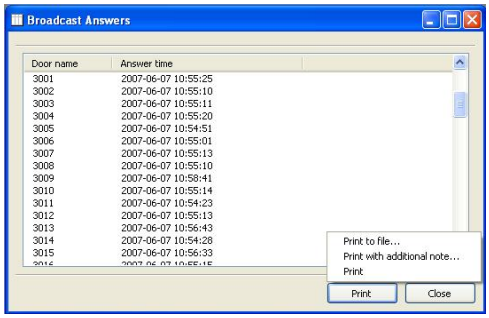
7.5 Broadcast commands

To see what broadcast commands that have been sent out, follow the steps below:

1. Double click on **Broadcast Commands**.



2. If desired, the list can be printed. If **Print** is pressed, the alternatives **Print to file**, **Print with additional note** and **Print** are shown. Choose the applicable one.
3. By marking a broadcast command in the list and clicking **View**, you will get the dialog **Broadcast Answers** which shows all online doors. For doors which have answered to the command, the column "Answer time" states at what time the answer was given. For doors which have not answered, "n/a" is shown at "Answer time".
   Note: It takes a few minutes before "n/a" is shown, since it is shown after the broadcast has made timeout.



4. If desired, the **Broadcast Answers** list can be printed. If **Print** is pressed, the alternatives **Print to file**, **Print with additional note** and **Print** are shown. Choose the applicable one.

7.6 Move/extend card

If a guest or guest party wants to change rooms and/or extend the validity of the guest card(s), this can be done without the guests needing to update their cards at the reception. If the guests just inform the reception about the situation, the reception personnel can send a command

- to a new guest room door which will then accept the guest card(s) from the first room, and if applicable also for an extended time.

OR

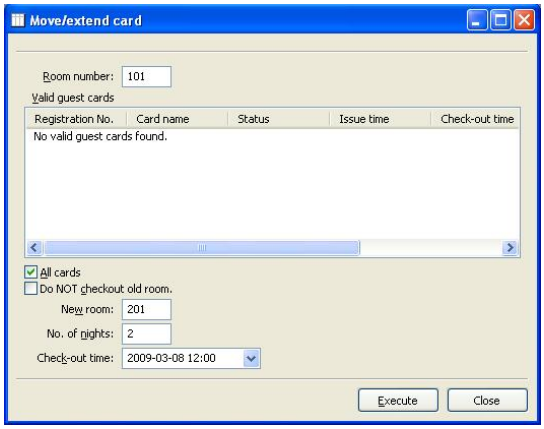
- to the current guest room door which will then accept the guest card(s) for an extended time.

Note: This can also be done via PMS.

Note: A guest card that is moved online to a new guest room will also automatically be added to any foyer door and/or guest entrance associated with the new guest room.

Note: No more than ten cards can be moved from one room at a time. Both rooms – the one you are moving from and the one you are moving to – must be set up as online doors. The limitation of ten cards is also applicable if the cards are still valid for the same room but are given an extended validity.

Note: When a card has been moved to another room, or when the validity for the card has been extended, the registration number of the card will be logged in the event report.



To move card(s) to another room:

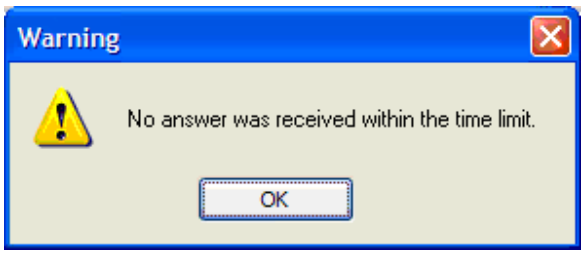
1. Double click on **Move/Extend card** in the navigation window.

2. At **Room number**, enter the number of the room where the guests are currently staying. All guest cards that are valid in the room will be shown.
3. By default, all guest cards that are valid in the room will be moved (**All cards** is checked). If this is not applicable, uncheck **All cards** and mark the cards that should be moved.
4. Check **Do NOT checkout old room** if the cards shall have access both to the old and the new room.
5. At **New room**, enter the number of the new room to which the card(s) shall have access.
6. If the number of nights is to be changed, enter at **No of nights** the appropriate number of nights for which the card(s) shall be valid. The **Check-out time** will change accordingly. The check-out time can also be chosen by using the calendar control: mark the

    button

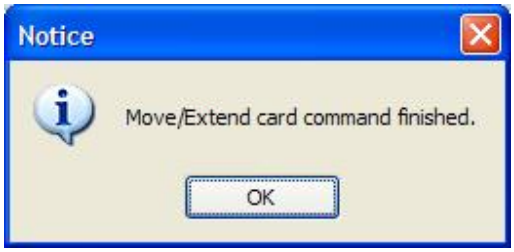
   next to the **Check-out time** field and mark a date in the calendar. The chosen date will appear at **Check-out time**; the number of nights will change accordingly.
7. Click **Execute** and enter your password.
8. If any of the rooms has not been set up as an online room, you will get the following message:

9. If any of the rooms is offline, you will get the following message:



10. If the new room is not vacant, you will get a message as in the following example. Choose the appropriate alternative.

11. When a card has been successfully moved, you will get the following message:



To extend the validity of one or more cards:

1. Double click on **Move/Extend card** in the navigation window.
2. At **Room number**, enter the number of the room where the guests are currently staying. All guest cards that are valid in the room will be shown.
3. By default, all guest cards that are valid in the room will have changed expiration time (**All cards** is checked). If this is not applicable, uncheck **All cards** and mark the cards that should have changed expiration time.
4. Check **Do NOT checkout old room**.
5. Leave the **New room** field empty.
6. Enter at **No of nights** the appropriate number of nights for which the card(s) shall be valid. The **Check-out time** will change accordingly. The check-out time can also be chosen by using the calendar control: mark the

    button

   next to the **Check-out time** field and mark a date in the calendar. The chosen date will appear at **Check-out time**; the number of nights will change accordingly.
7. Click **Execute** and enter your password.

8. If the current room has not been set up as an online room, you will get a message about this (see picture at step 8 under *To move card(s) to another room*).
9. If the current room is offline, you will get a message about this (see picture at step 9 under *To move card(s) to another room*).
10. When a card has been successfully extended, you will get a message about this (see picture at step 11 under *To move card(s) to another room*).

7.6.1 Add card to room

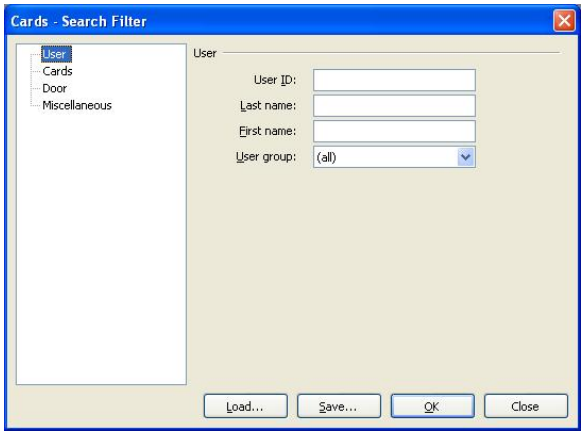
There is also another way of moving cards from one online room to another online room without the guest needing to go to the reception; with the command **Add card to room**, which is shown in the right-click menu for a card. It can be used for VIP guests arriving with a card. By choosing **Add card to room** for the concerned card, the card can be added to any online guest room in the hotel. It is possible to choose whether the current guest should be checked out from the old room or not.

7.6.2 Show history

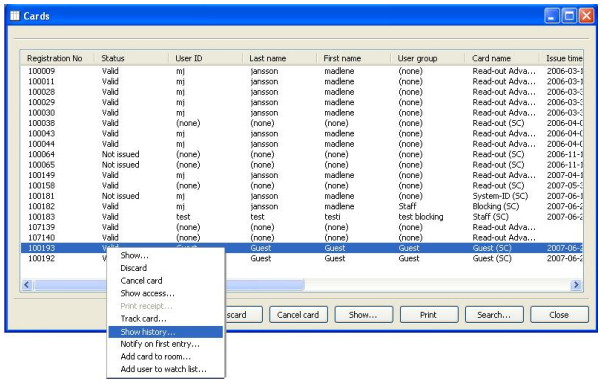
It is possible to show the history of a card which has been moved or extended. This can be done from the card list or the event report.

To show card history from the card list:

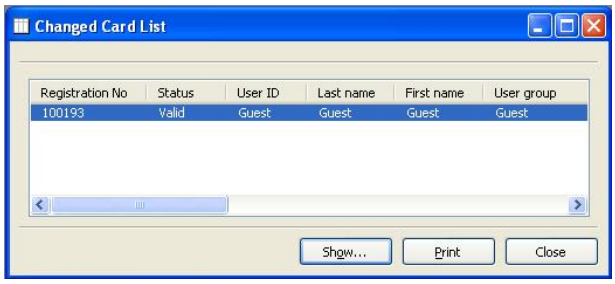
1. Double click on **Cards** under the **Lists** tab in the navigation window of DC-One.



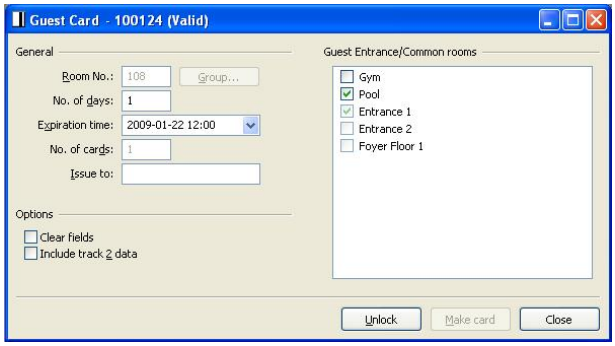
2. If applicable, enter a card list search filter under any of the alternatives in the left part of the **Cards – Search filter** dialog before clicking **OK**.



3. Right click on the card in the card list and choose **Show history**. The **Changed Card List** dialog will appear.

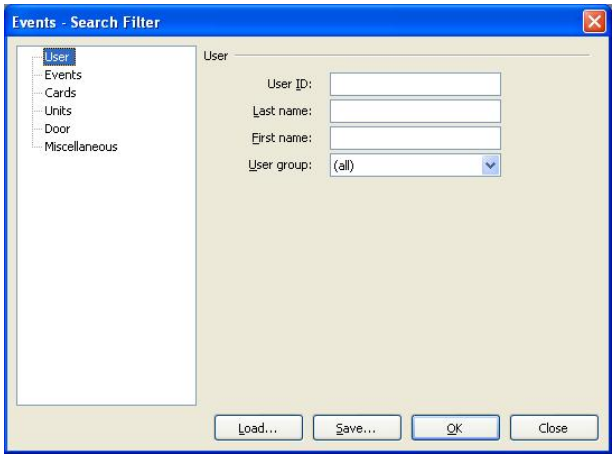


4. Click **Show** to show the original card dialog (see the following picture).

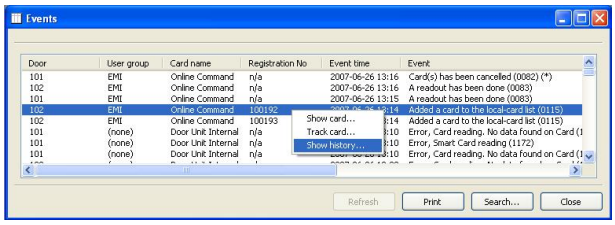


To show card history from the event report:

1. Double click on **Events** under the **Reports** tab in the navigation window of DC-One.



2. Enter a search filter in the left part of the **Events - Search Filter** dialog and click **OK**.



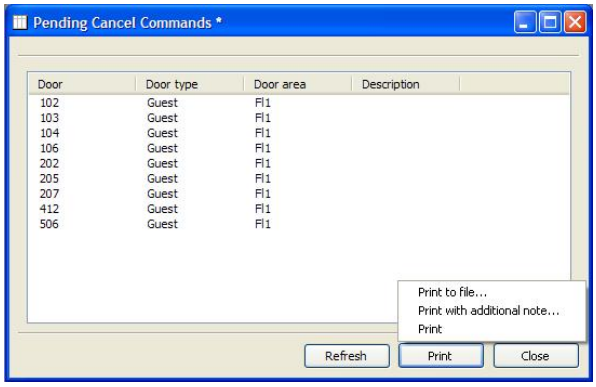
3. The **Events** dialog is shown. Right click on the event and choose **Show history**. **Note:** This is only possible for events that are related to a card.
4. The **Changed Card List** dialog is shown – see step 3 under *To show card history from the card list* above.

7.7 Pending cancel commands

If a card has been cancelled but this command has not yet reached one or more doors, the door(s) will appear in the dialog **Pending Cancel Commands**.

1. Double click on **Pending Cancel Commands**.

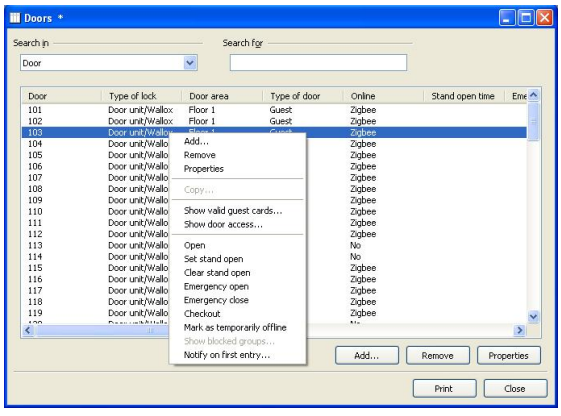
Note: Use a cancel card in the locks which appear in the dialog **Pending Cancel Commands**.



2. If a * is shown in the dialog header, new cancel commands have – since the dialog was opened – been sent but not yet been received by the locks. In this case, press **Refresh** to show all pending cancel commands.
3. If **Print** is pressed, the alternatives **Print to file**, **Print with additional note** and **Print** are shown. Choose the applicable one.

7.8 Online commands for a specific door

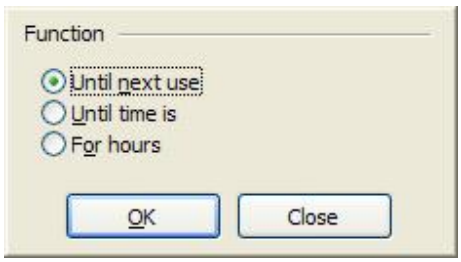
1. Open the door list by double clicking on **Doors** under the **Lists** tab in the navigation window.
2. Mark the concerned online door in the door list and right click on the door; a menu will be shown (see the following picture).
3. Choose the appropriate command in the menu. See the rest of this section *7.8* for descriptions of the different commands.



Open – the door will open.

Set stand open – the door will be set in stand open (unlocked) mode, i.e. no card or code will be needed to open it.

1. You will get the dialog below, where you mark the appropriate radio button for the stand open function you want to use. If “Until time is” or “For hours” is chosen, enter the corresponding field.



2. Click **OK**. The time when stand open was set will be shown in the door list.

Clear stand open – the stand open (unlocked) mode in the door will be revoked and the door will go back to normal mode again, i.e. card and/or code will be required to open it.

Emergency open (can only be performed by the distributor) – the door will be set in emergency stand open mode, i.e. be unlocked until it is emergency closed. The time when emergency open was set will be shown in the door list.

Emergency close – the door will be emergency closed, i.e. the emergency open will be revoked and the door will go back to normal mode again, i.e. card and/or code will be required to open it.

Checkout – the override number in the door will increase, so that none of the guest cards (guest, joiner, suite, joiner suite, guest advanced and future arrival) that have been valid in the room will be able to enter anymore. However, if a grace time has been set (see section *6.2.3 Miscellaneous* for details), the cards will be able to enter during the grace time.

Mark as temporarily offline – the door will be offline until an event comes from the door.

Show blocked groups – this alternative will show

- user groups (or blocking groups) that have been blocked with the blocking command; see section *7.3 Block*
- blocking groups that have been automatically blocked when the guest checked in (this requires that the option auto-blocking in rented rooms is set)

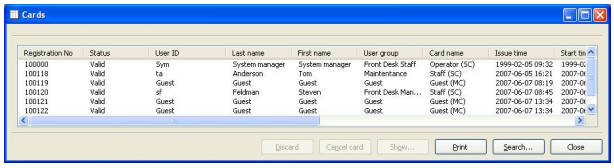
Notify on first entry – if the mail notification option and/or SMS option is used, it is possible to notify one or more users the first time the valid guest card is used in the door after the function **Notify on first entry** was set. When the alternative **Notify on first entry** is chosen, a list of all users with e-mail address and/or cell phone will be shown. Mark the desired user in the **Users <Doors>** dialog and click **Select**. If the user has got both e-mail address and cell phone number, you will be asked to choose one of the media e-mail or SMS, or both. The user will then get an e-mail and/or SMS the first time the concerned guest card is used. If the room is rented, you will be asked whether the e-mail/SMS notification should be triggered by the current guest or the next arriving guest. See *User manual TimeLox DC-One*, Art. No 865 100, for more information about the mail notification option and the SMS option.
Note: The notification on first entry requires that the guest’s name was entered at **Issue to** when the guest card was issued.

7.9 Cancelling a card

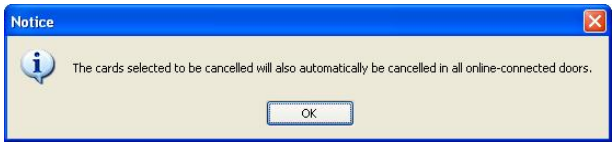
When cancelling a card in the card list, it will automatically be cancelled in all online doors.

Note: If a card cannot be used anymore at all, e.g. if it has been broken, it should be discarded. A discarded card will by default not appear in the card list. Please note the difference between discarding and cancelling a card. If a card has been lost, improperly used etc, it should be cancelled and not discarded. A cancelled card can (if found) be re-encoded and used again, while a discarded card should not be used anymore at all.

To cancel a card:

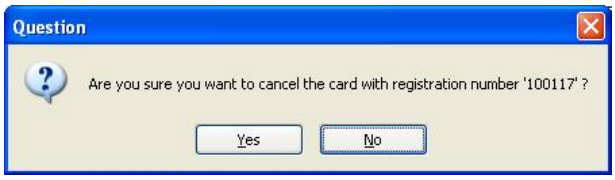


1. Mark a card in the card list and click **Cancel card**. You will get the following message:



2. Click **OK**.

3. The dialog above follows. If the card should really be cancelled, click **OK**.



4. The dialog above is shown. Click **Yes**.

8 Power loss & 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 ZigBee view and choose **Leave Network**). In this way the old EN will deregister from the parent.
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 ZigBee 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, insert a Discovery card (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) in the lock; the lock will chirp once. 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 ZigBee 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:

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. Insert an Orphan Join card (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) in the door lock of each EN; each lock will chirp once.

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:

There are in SysMon two methods to replace an RT; either by using the **Add Node** command or the **Permit Joining** command.

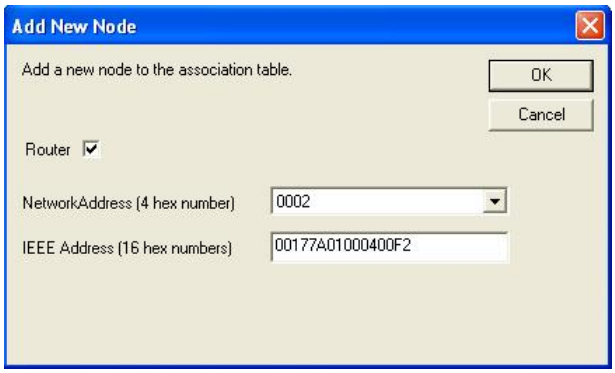
With the **Add Node** command, you do not have to make discovery on the new RT when it is added to

its parent, or on the children of the old RT when they should be added to the new RT instead.

To use the **Add Node** command when replacing an RT:

Each RT contains a table of its connected children including RTs and ENs. A copy of this table is automatically stored on the server. In the event a defective RT should be replaced, it is possible to build up the table for the new RT by following the steps below.

1. In the SysMon ZigBee view, hover over the old RT and make a note of its network address.
2. Hover over the RTs and/or ENs which are directly under the old RT and make a note of the IEEE address and network address for each one of these RTs/ENs.
3. Right click on the old RT in the SysMon ZigBee view and choose **Leave network** so the new RT can instead join the parent of the old RT.
4. **Important:** Wait for 40 seconds to avoid confusing the parent from which the old RT has deregistered.
5. Disconnect the old RT and remove it.
6. Mount and connect the new RT.
7. Make the new RT join its parent by right clicking on the parent and choosing **Add Node**. In the **Add New Node** dialog that appears, make the following steps (see example in the following screenshot):



   - Mark the checkbox “Router”.
   - At **Network Address**, choose in the drop-down list the 4 hex number that you have taken a note of according to step 1 above.
   - At **IEEE Address**, enter the IEEE address that is found on the label of the new RT.
   - Click **OK**.
8. Give the new RT a name by right clicking on it in the SysMon ZigBee view and choosing **Edit Name**.
9. The children of the old RT should now be added to the new RT in the SysMon ZigBee view. Right click on the new RT and choose **Add Node**.
10. In the **Add New Node** dialog, make the following steps:
    - Mark the checkbox “Router” if applicable.
    - At **Network Address**, choose in the drop-down list the 4 hex number that you have taken a note of according to step 2 above.
    - At **IEEE Address**, enter the IEEE address that you have taken a note of according to step 2 above.
    - Click **OK**.
11. Repeat steps 9-10 for each node that should be connected to the new RT.

After this, the new RT will begin communicating with its children without the need for making **Permit Joining** and associating RTs and ENs.

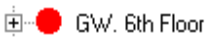
To use the **Permit Joining** command when replacing an RT:

1. Make a leave on the old RT (right click on the RT in SysMon’s ZigBee view and choose **Leave Network**). In this way the old RT will deregister from the parent.
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. Insert a Discovery card (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) in the door lock of each EN (each lock will chirp once) that should associate with the new RT.
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:



On power up the GW will reconnect to the server and any children will rejoin the GW by performing orphan joins.

To expedite this process in ENs:

1. Insert an Orphan Join card (see section about ZigBee configuration card in *User manual TimeLox DC-One*, Art. No 865 100) in the door lock of each EN; each lock will chirp once.

The GW regularly sends messages to the server so any interruption in power will be immediately apparent at the server.

Each GW contains a table of its connected children including RTs and ENs. A copy of this table is automatically stored on the server. In the event a defective GW should be replaced, it is possible to build up the table for the new GW by following these steps:

1. In the SysMon ZigBee view, hover over the different RTs and/or ENs which are directly under the old GW and make a note of the IEEE address and network address for each one of these RTs/ENs.
2. Disconnect the old GW and remove it.
3. Mount, connect and – when the new GW appears in the SysMon ZigBee view – name the new GW. See section *2.3 Gateway installation* for screenshots and more details.
4. Right click on the new GW in the ZigBee view and choose **Add Node**.
5. In the **Add New Node** dialog (see step 7 in section *8.3 Router* for example screenshot), make the following steps:
    - Mark the checkbox “Router” if applicable.
    - At **Network Address**, choose in the drop-down list the 4 hex number that you have taken a note of according to step 1 above.
    - At **IEEE Address**, enter the IEEE address that you have taken a note of according to step 1 above.
    - Click **OK**.
6. Repeat steps 4-5 for each node that should be connected to the new GW.
7. Right click on the old GW in the SysMon ZigBee view and choose **Remove**.

After this, the new GW will begin communicating with its children without the need for making **Permit Joining** and associating RTs and ENs.

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.

If there are circumstances that dictate the devices should communicate on a specific channel (i.e. if there are other online devices or known inter-ference 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 ZigBee view and choose **Set channels**; the dialog below will be shown.

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) and click OK. If more than one channel is checked, the best one will be chosen.

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 the GW will automatically switch to another channel.

The EN will start orphan joining as a fallback. 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.

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

Appendix A: Online devices

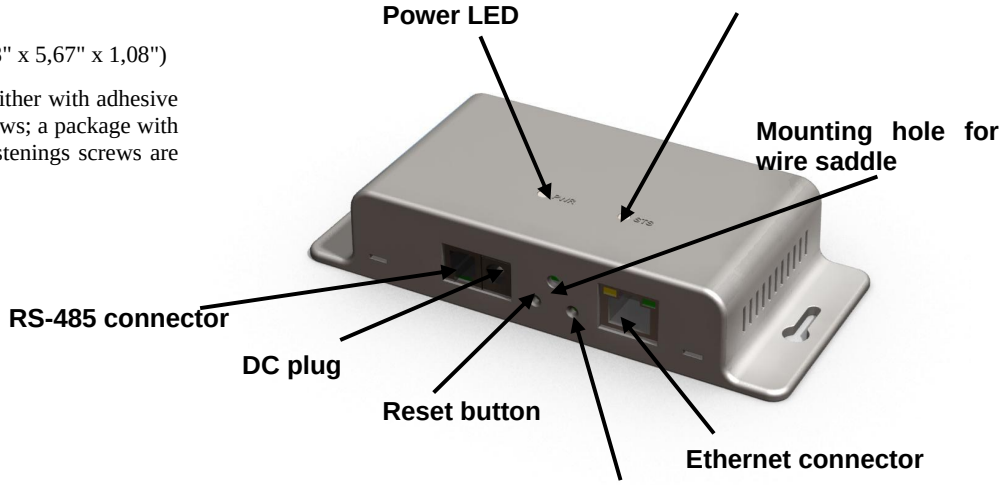
Gateway

- Automatic adjustment to 10 or 100 Mbit/s networks
- Powered via Ethernet or by a power adapter (9VDC)
- Low power consumption
- The total number of gateways is virtually unlimited
- Can have either five routers or 15 endnodes connected
- 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® strips or fastening screws; a package with two VELCRO® strips and two fastenings screws are enclosed)
- Weight: 116 g
- Flame retardant ABS
- UL94 V-0 approved
- Colour: RAL 7047

Status LED

- red while the gateway gets its IP address
- LED off (no LED colour) while the gateway looks for the Timelox server
- steady yellow while the gateway has got contact with the Timelox server
- blinking yellow when the F button is pressed for reaching the web interface where some gateway settings are made



F button (this button is used for reaching the web interface where some gateway settings are made. Toggling function).

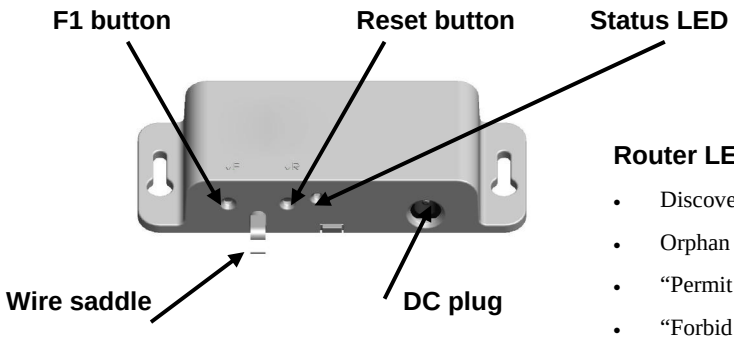
Router

- Powered by a power adapter (5VDC)
- Low power consumption
- Can have either five routers or 15 endnodes connected
- 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.

  Note: Timelox recommends a maximum of three hops, i.e. gateway – router – router – endnode, down the gateway. The link quality index (LQI) should be at least 30%.
- Case with the dimensions 40 mm x 105 mm x 19,5 mm (1,97" x 4,13" x 0,77")
- Easy mounting (can be mounted either with adhesive VELCRO® strips or fastening screws; a package with two VELCRO® strips and two fastenings screws are enclosed)
- Weight: 36 g
- Flame retardant ABS
- UL94 V-0 approved
- Colour: RAL 7047

Toggling "permit joining"/ "forbid joining":

Press the **F1** button.

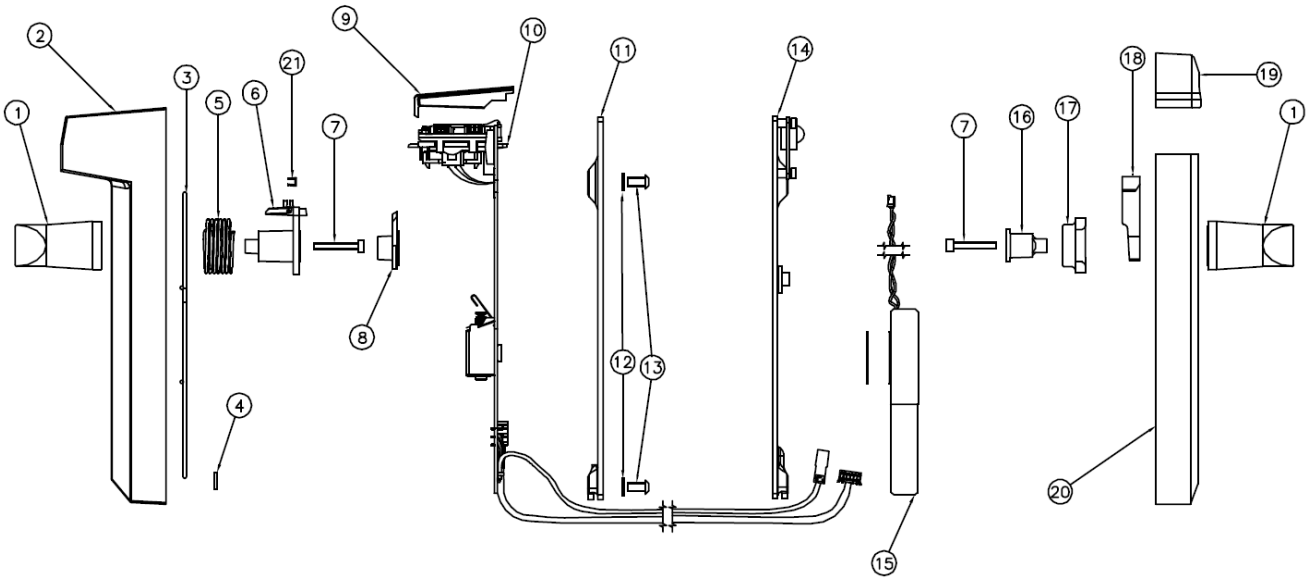


Router LED Signals

- Discovery: long blink every 5 seconds
- Orphan join: long blink every 2 seconds
- "Permit joining": Short blink every 0.5 seconds
- "Forbid joining": Short blink every 2 seconds

66 3081 004-10

Lock



1 Handle
2 Outside escutcheon
3 Clamp
4 Starlock washer
5 Torsion spring
6 Driver
7 Allen screw
8 Follower
9 Cap
10 Electronics
11 Outside mounting plate
12 Washer
13 Backplate screw
14 Inside mounting plate with endnode
15 Battery pack
16 Handle holder
17 Curve
18 Spring
19 Communication window
20 Inside escutcheon
21 Edge strip

Appendix B: Mounting of gateway and router

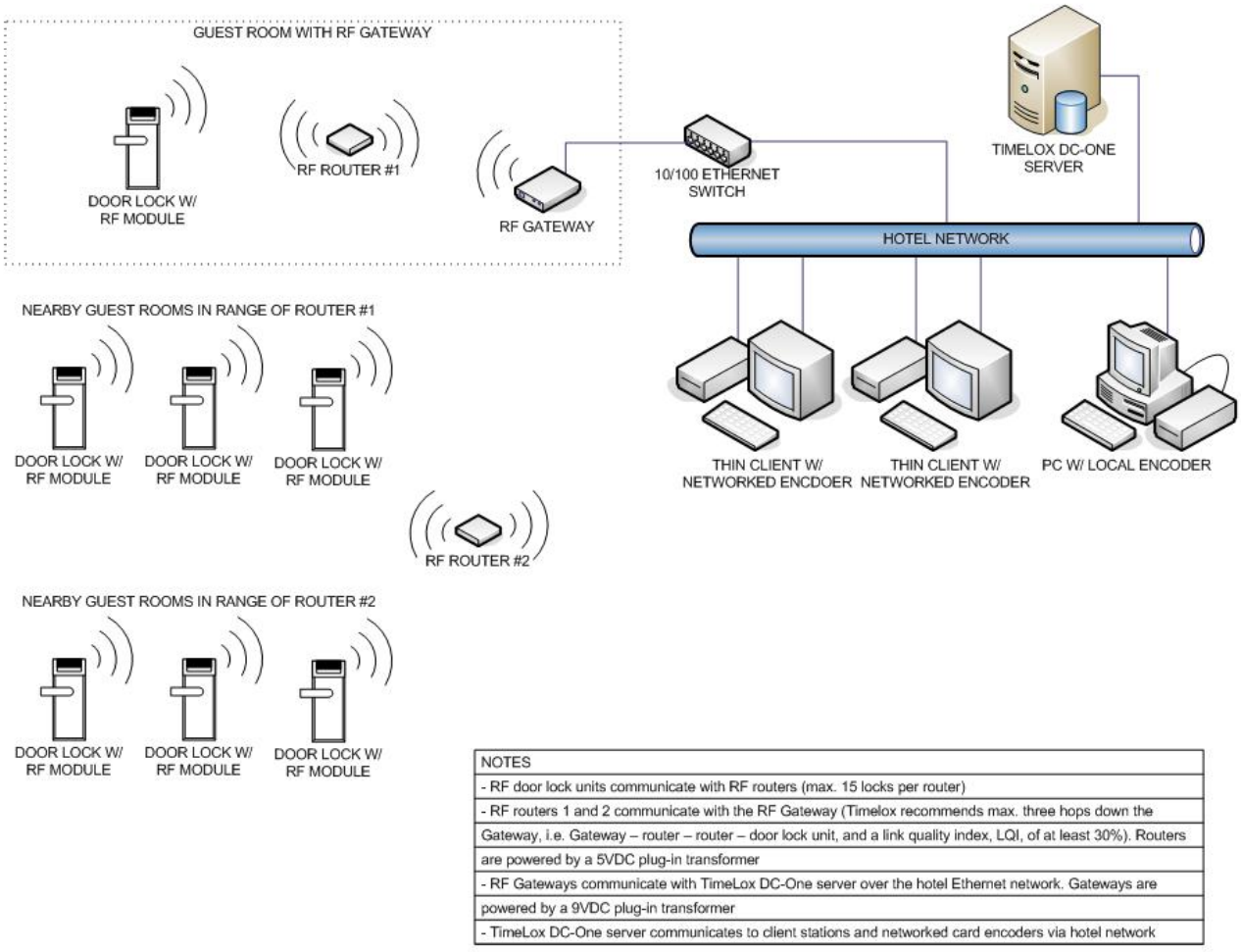
Preferred way of mounting the gateway is horisontally:

Note: If the label does not say “GATEWAY ER”, the gateway is of another type and should be mounted vertically.

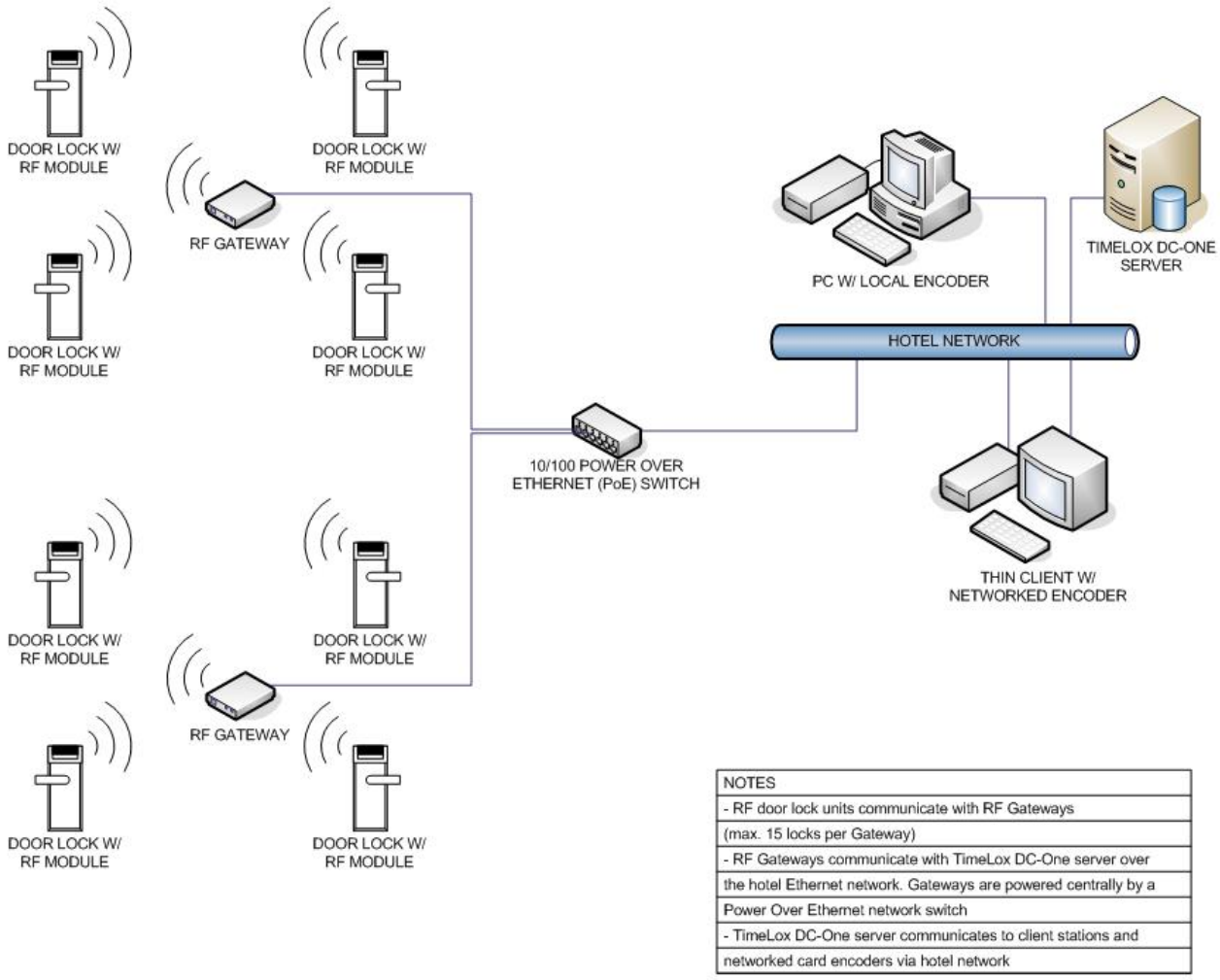
Preferred way of mounting the router is horizontally:

Appendix C: Example configurations

Several online configurations are possible. Here are some examples:



Example configuration 1: Basic setup with GWs and RTs and no firewall.



Example configuration 2: GWs using Power over Ethernet (PoE) communicating directly with doors.