VIMAR 01507 By me KNX Router Instruction Manual

VIMAR 01507 By me KNX Router Instruction Manual

Contents

System Requirements

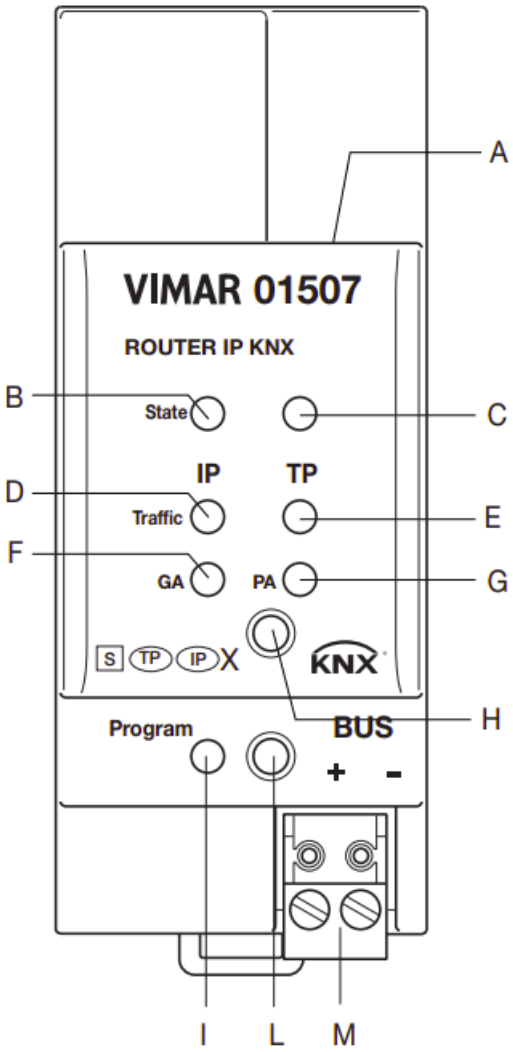
To create the network system, make sure all the devices (switch, router, firewall, etc.) are configured in such a way as to allow the passage of multicast messages the device sends on IP. We recommend you involve an IT manager to make sure the KNX/By-me system can operate in the IP solution of the connections.

Product description

The By-me/KNX router enables communication between parts of a system comprising By-me devices, grouped together within an “island”, with a system comprising KNX devices. The messages are transmitted in both directions according to criteria which define the correspondence of the communication objects belonging to the specific domains. The router allows up to 500 routing rules. Each rule is specified by the By-me group address, by the KNX address, by the direction of communication (from KNX to By-me; from By-me to KNX; both) and by the type of information exchanged (1 bit, 2 bit, …).
The device is equipped with a TP terminal for connection to the By-me BUS, an Ethernet connector and a front push button for configuration via ETS. The power supply is provided by the By-me BUS.

Router 01507 conforms to the KNX Secure requirements on the datapoints defined in the routing table. A datapoint on the KNX side can be defined for the heartbeat signa

Front view of the device



- **A:** Ethernet KNX over IP line connector
- **B:** Ethernet KNX over IP line status LED
- **C:** By-me BUS line status LED
- **D:** Traffic on Ethernet KNX over IP line LED
- **E:** Traffic on By-me BUS line LED
- **F:** GA LED
- **G:** PA LED
- **H:** Reset push button
- **I:** Configuration LED
- **L:** Configuration push button
- **M:** By-ME BUS line

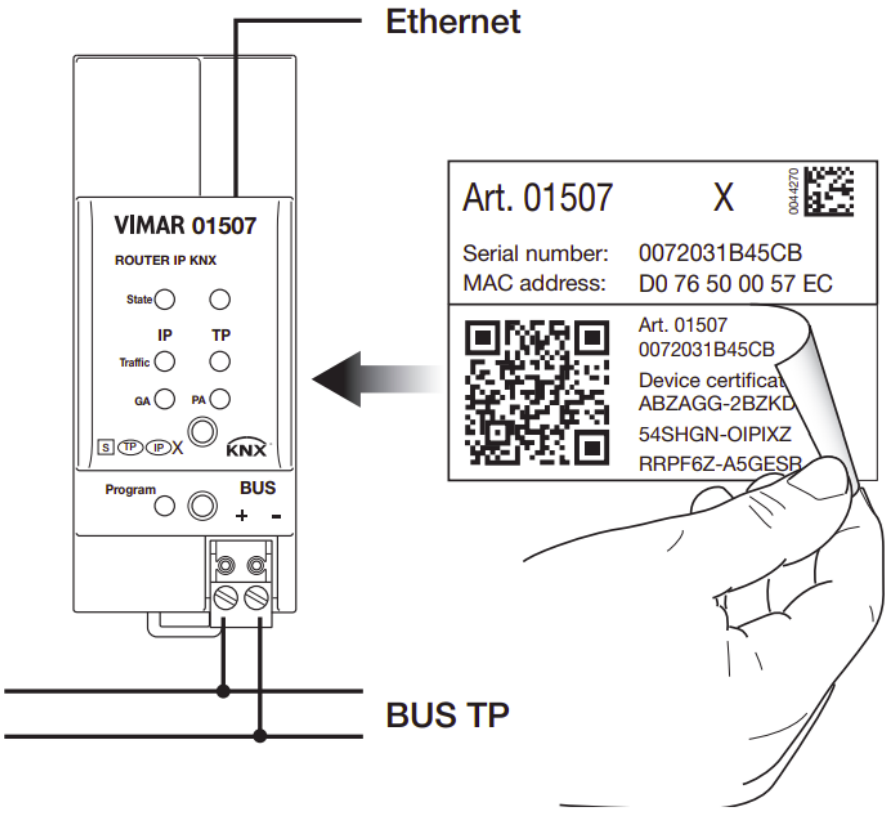
LED indications

	Green	Red
Ethernet KNX over IP line status LED (B)	ON: Correct operation	ON: Device factory reset
By-me BUS line status LED (C)		
Ethernet KNX over IP line traffic LED (D)	ON: Data traffic presence	
Traffic on By-me BUS line LED (E)		
GA LED (F)		ON: Device not configured
PA LED (G)		
Configuration LED (I)		ON: Device in the configuration phase

Commissioning

For commissioning with the default settings, keep the following in mind:

- The individual address is 15.15.255
- To activate the security function and Secure Commissioning you will need the device Certificate
- Security function activation requires a specific minimum ETS version number



✓ To launch a secure configuration download, you first need to activate the Secure Commissioning in the ETS project.

✓ Also read chapter “2.5 Important notes” before operating the device.

Secure Commissioning

To launch the secure download of the configuration settings and/or individual address, you first need to add the individual Certificate of device 01507 to the ETS project.

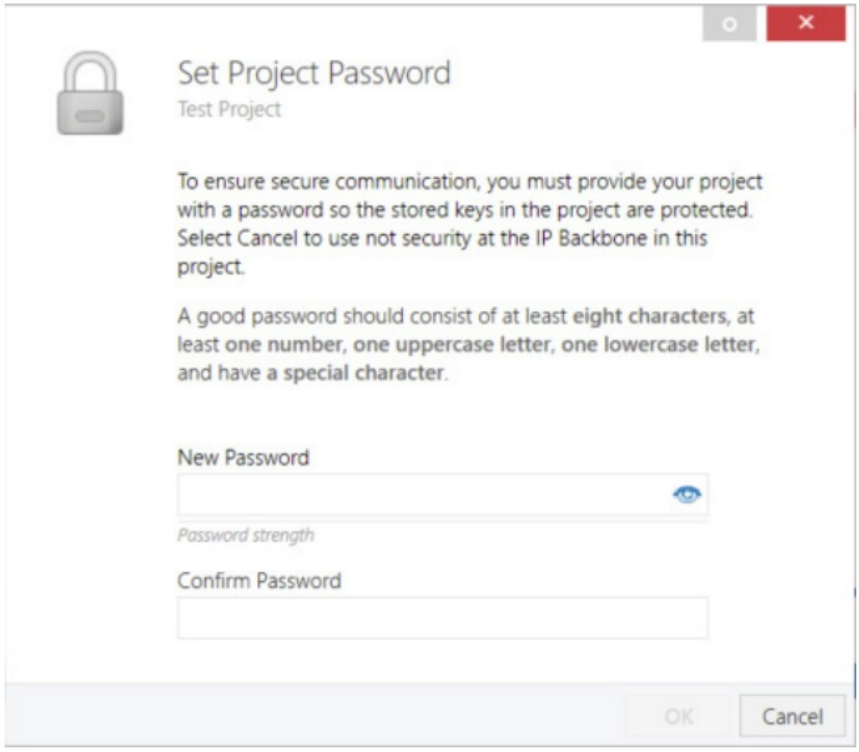
✓ To add it, the ETS project must be password-protected.

✓ Secure download is only possible after Secure Commissioning has been activated.

✓ To activate Secure Commissioning you will need the individual Certificate of the device.

✓ Device certificates can only be added to a password-protected ETS project.

If a password has not been set for the project, Secure Commissioning cannot be activated. ETS projects with Secure Commissioning and/or the Security function set to active always require a project password. If no project password proves to be set when the Security function is activated, ETS prompts you to enter one.



✓ The individual Certificate of the device is always included with the KNX Secure product. For the product to be configured by the user, make sure you do not lose the device Certificate (see chapter 2.6 Keeping the device Certificate).

Important notes

We recommend you attend standardised courses at a certified KNX training centre before installing, programming and commissioning a KNX system. The participant will gain the necessary expertise and knowledge also for troubleshooting, thanks to practical exercises.

Read this chapter thoroughly before first use and installation:

Installation and commissioning

- If the device is damaged during storage or transport, repairs must only be carried out by authorised personnel.
- Once connected to the By-me bus system, the device works with its default settings.
- Warning: do not connect to a 230 V mains power supply. The device is powered by the By-me bus and does not require any additional external power supply.
- The device must be installed and commissioned solely by a qualified electrician or an authorised person.
- For the design and creation of electrical systems, abide by the specifications, guidelines and applicable local regulations in force.
- For configuration, use ETS (or ETS Inside)

Assembly and safety

- For assembly, use appropriate equipment, in compliance with IEC60715.
- Installation on 35 mm DIN rail (TH35)

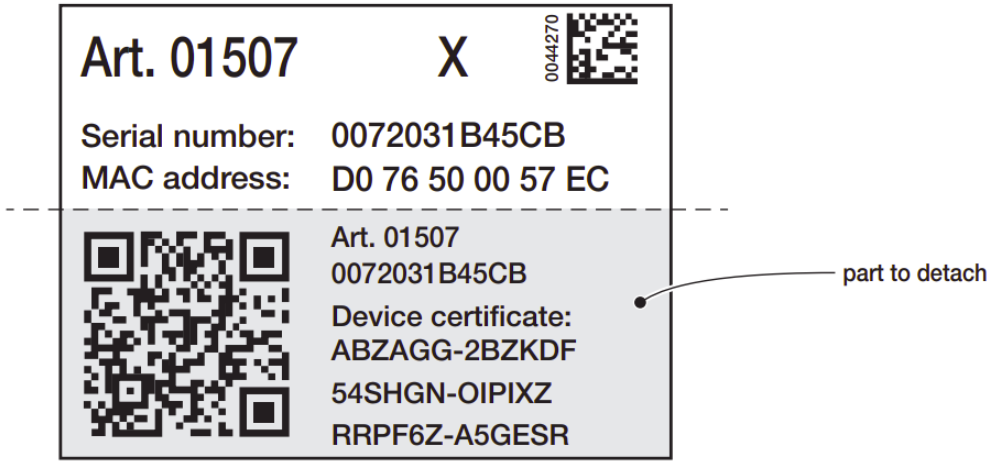
- Do not damage the electrical insulation while making the connections.
- Only install in a dry place.

Maintenance

- Guarantee accessibility to the device for operation and visual inspection.
- Do not open the external casing.
- Protect the device against moisture, dirt and damage.
- The device does not require any maintenance.
- If necessary, you can clean it with a dry cloth.

Keeping the device Certificate

The device Certificate is on the label affixed to the side of the casing. To avoid unauthorised access, the device Certificate should be removed from the device once it has been commissioned. To this end, the label is divided into two parts, one fixed part which remains affixed to the casing (for identification), and the other removable part (to be kept).



After adding the device Certificate to the dedicated list in ETS, keep the removed part of the label in a safe place. The list of device Certificates must only include certificates of KNX Secure devices used for ETS projects. ETS will automatically use the correct certificates for device programming.

To identify the device clearly after the detachable part has been removed, the serial number is printed on both parts of the label, the one you have removed and the one that remains on the casing.

✓ If you lose the removed part with the device Certificate, it will only be available in the password-protected ETS project.

✓ **Caution!** If the device Certificate is lost and cannot be retrieved, in other words if the part of the label removed can no longer be found and the project password has also been lost, the device can no longer be used securely (the Security function will no longer be available for activation). If this is the case, even after performing a factory reset, the device may only be used in the non-protected mode, like a “normal” device.

Summary of functions

- The device Certificate guarantees that only authorised persons may access device 01507.

- When the ETS “Secure Commissioning” function is active, the configuration data are only downloaded in encrypted KNX Data Secure format.
- The device is powered by the By-me bus.
- The firmware can easily be updated from a web browser.
- Router 01507 supports KNXnet/IP, ARP, ICMP, IGMP, HTTP, UPnP discovery, UDP/IP, TCP/IP, DHCP and AutoIP

KNXnet/IP

The presence of the Internet protocol (IP) has made the definition of the KNXnet/IP protocol possible. As documented in the specifications of the KNXnet/IP protocol, the KNX data can be transmitted encapsulated in IP packages.

Updating the IP firmware

Thanks to the IP bootloader function, the firmware can be updated remotely and the contents of the flash memory can be re-written via an IP connection. This is not a simple application download. The communication stack and application software are downloaded.

The firmware update procedure via IP can be carried out from the front-end Web of router 01507, which is independent of the ETS and which uses special messages to speed up the process. In order to protect this process, it uses special encryption.

The KNX Secure protocol

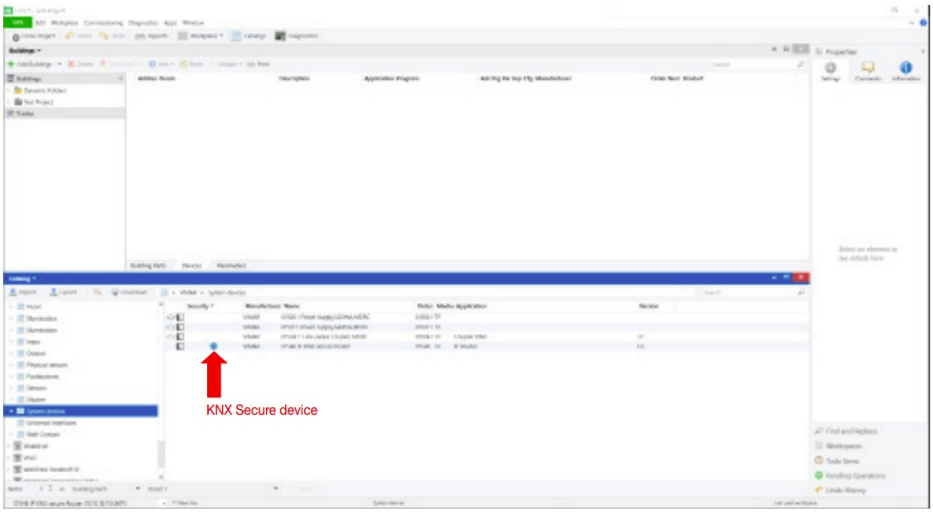
The device is used to activate the “KNX SECURE” data encryption protocol, entering the QR code or the digits in ETS and also creating a password associated to the project.
N.B.: If the QR code printed on the label is too small, take a photo of it with a smartphone and enlarge it.
The password is mandatory in the following cases:

- when enabling the Secure part of the devices in the project
- when entering the certificate of a Secure device in the project

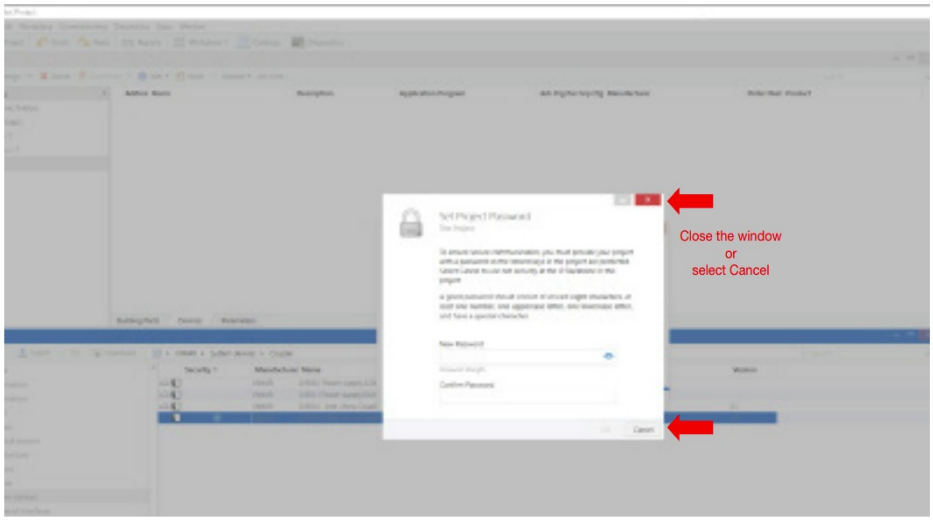
If the Secure part of a device is disabled, it acts exactly like a device that does not support this protocol.

If you do not wish to enable the Secure part, when importing the device into the project close the Secure request window as described in the following procedure.

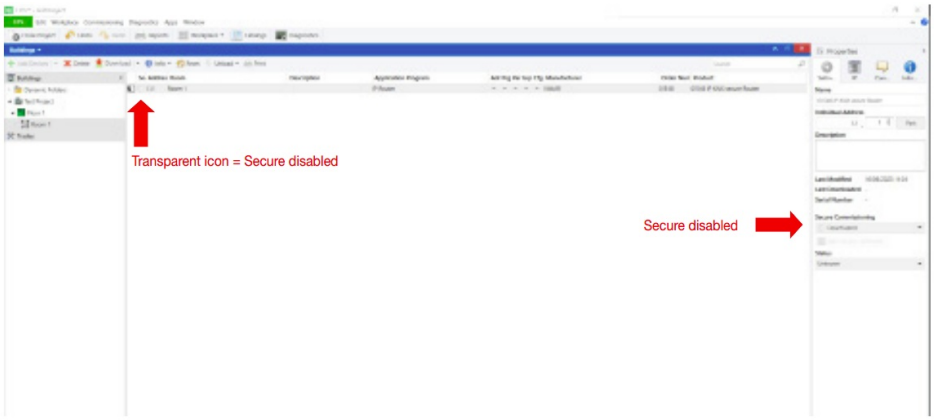
1. Add the Secure device to the ETS project.



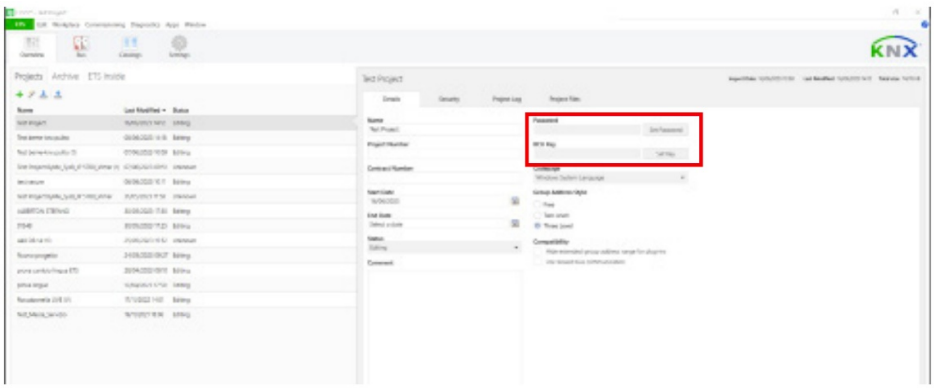
2. Ignore the set password request.



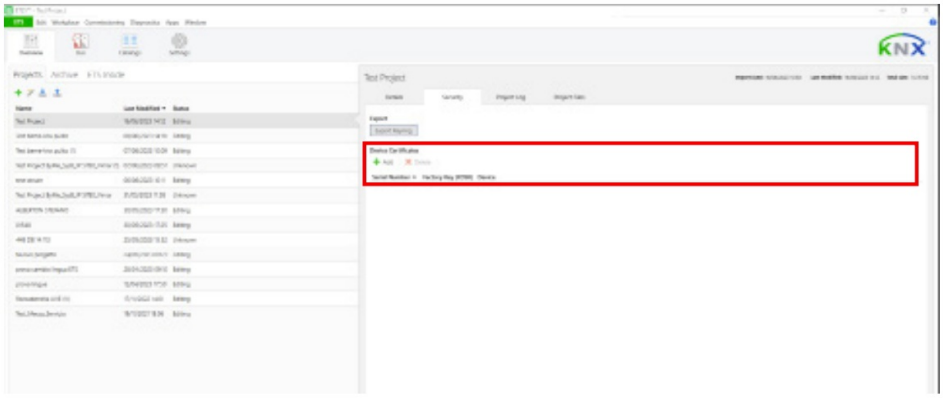
3. The device is displayed with the Secure part disabled.



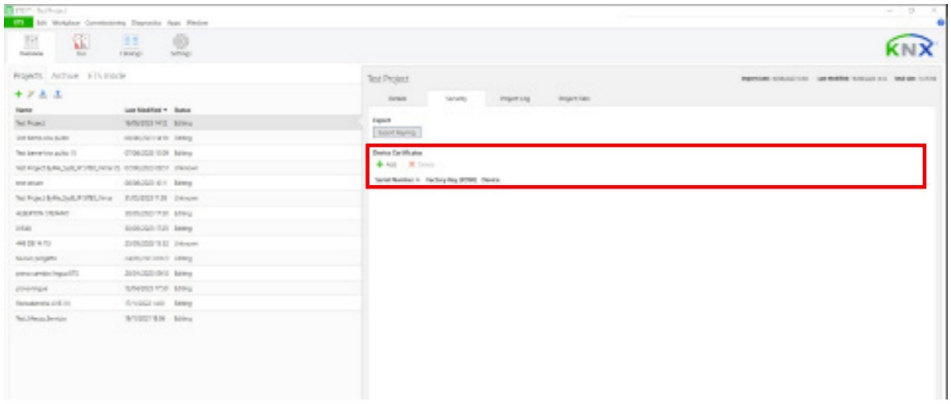
4. No password is associated with the project



5. No certificate is associated to the project



6. No certificate is associated to the project.



Description of operation

In KNX network systems, router 01507 is used to transfer messages from KNX bus to By-me bus and vice versa. The message exchange rules are totally defined by the installer using the dedicated folder (Group objects, Parameters, DCA) created in ETS for the specific device.

It can be used normally without activating the Security function and in ETS projects in which the Security function is active. After connection to KNX IP, router 01507 works with its default settings. A valid individual address must be set.

General Information

When it receives data which use group addresses, router 01507 behaves in accordance with the settings present in the DCA. During normal operation, it only forward messages whose group addresses are specified in the routing rules defined in the DCA.

If the messages forwarded by the router do not receive confirmation, for instance because the recipient is missing or due to a transmission error, the messages will be repeated up to three times.

The router is intended for use in 10/100 BaseT networks conforming to IEEE802.3. The Auto Sensing function automatically sets the baud rate (10 Mbit or 100 Mbit).

The IP address can be received by an DHCP server. For this purpose, the setting of the automatic IP address assignment can be set via ETS (“Obtain an IP address automatically”). If this setting is configured but no DHCP server is found, router 01507 starts an AutoIP procedure and autonomously assigns itself an IP address; the device must have a fixed IP address (a standard gateway and subnet address), it can be set via ETS.

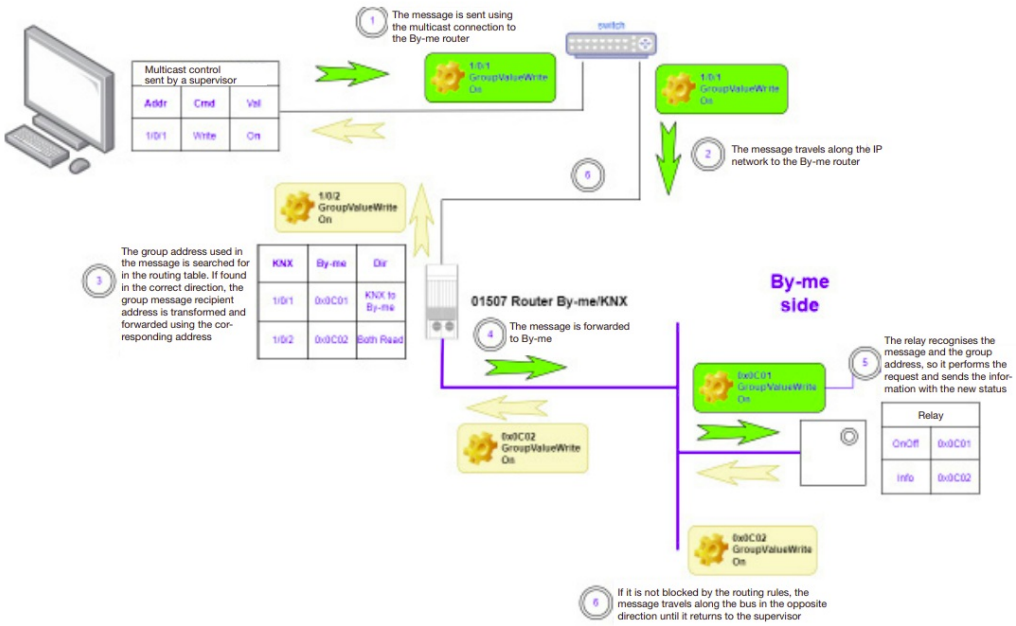
IP network

Router 01507 sends messages to/from the TP network to/from the IP network in compliance with the specifications of the KNXnet/IP protocol. Via a supervision software, in the case of a default setting, the IP data are sent as IP Multicast to the IP address 224.0.23.12 port 3671. The IP Multicast address 224.0.23.12 is the address for KNXnet/IP established by the KNX Association together with IANA. We recommend you change this address only if the need arises due to the existing network.

N.B.

- All the KNX IP devices that need to communicate with one another via IP must have the same IP multicast address.
- It may be necessary to change the IP multicast address 224.0.23.12 depending on the type of network and on the settings of the network components.
- For the IP routing and identification, the IGMP protocol (Internet Group Management Protocol) is used.
- In the event of problems assigning the IP address, please contact your network administrator.

Message flow example



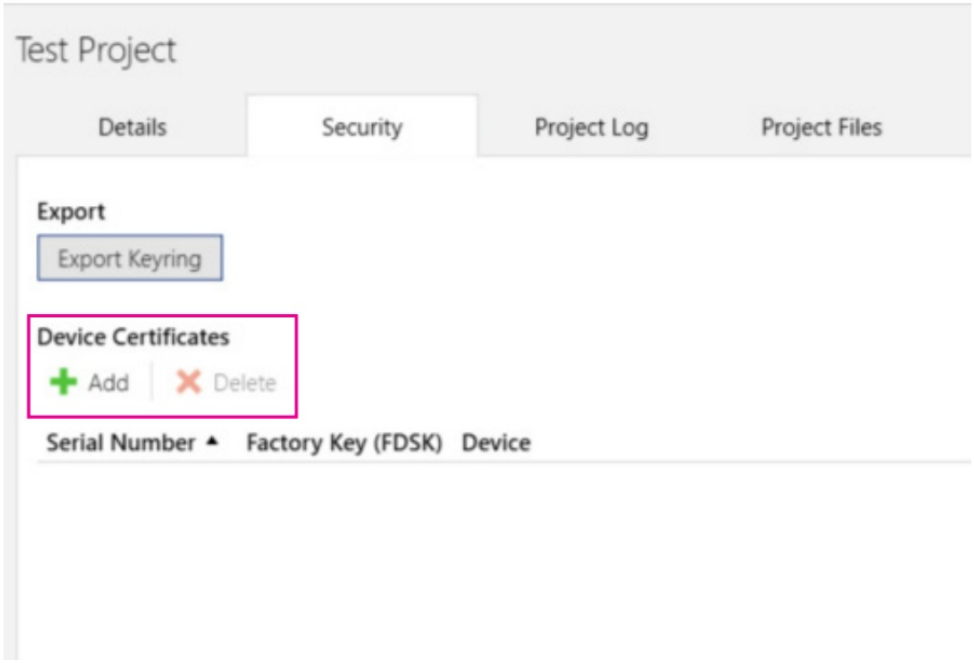
Adding the device Certificate

Each KNX Secure device uses its own Certificate. The device Certificate must be entered in ETS before activating or using the KNX security functions.

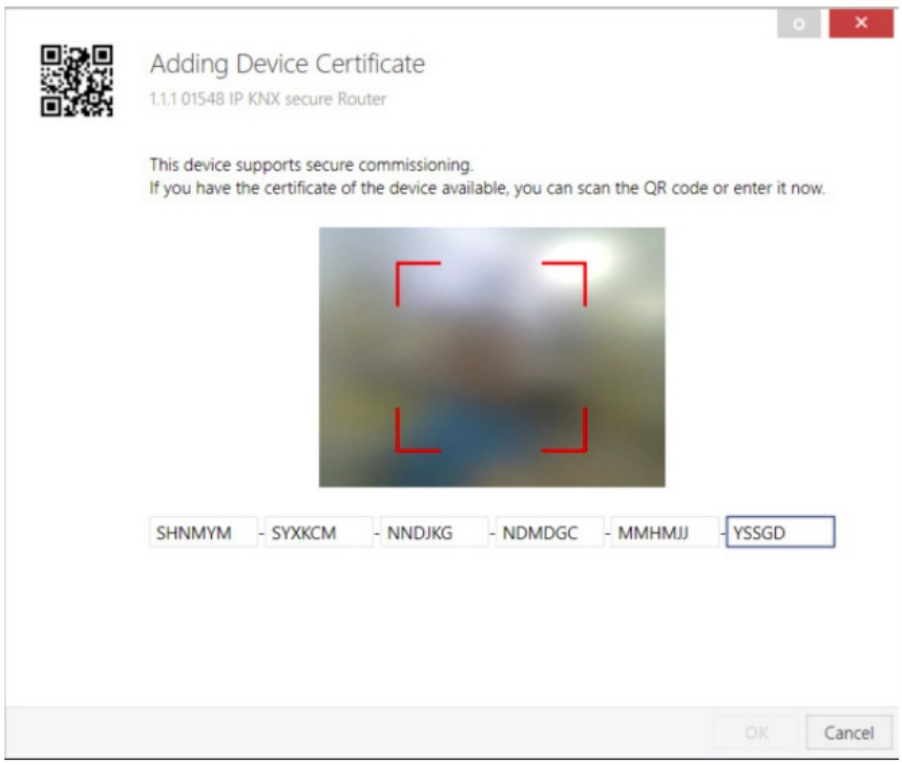
✓ The device Certificate is printed on a label affixed to the side of the casing.

✓ The device Certificates can be entered manually or by scanning the QR code with the webcam.

After the project has been opened, the list of device Certificates can be edited in the Security tab of Project Overview.



If the device Certificate has not been added to the list yet, when a protected download is launched, the following window appears.



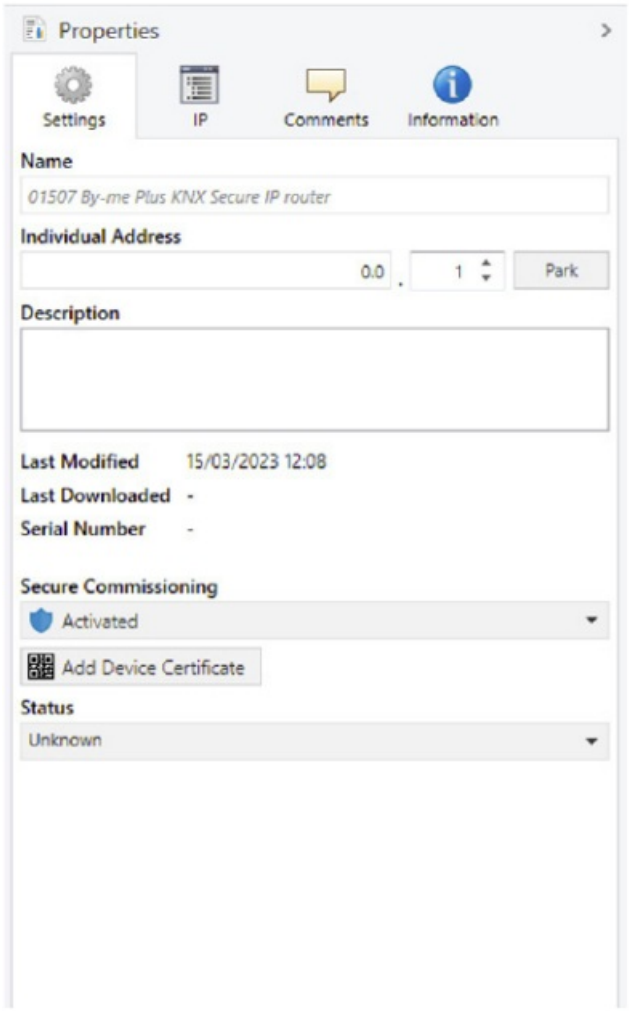
Programming

Programming the individual address (and application)

To download the individual address in a device, the Programming mode must be active. Press the programming button to activate or deactivate the programming mode. A red lit configuration LED (I) indicates the programming mode is active. When the download from ETS is activated and you press the programming button, the device stores the new individual address in the memory. The security settings are updated by downloading the individual address and application (L).

The KNX address can be assigned to the device by setting the desired address in the ETS properties window. At

the end of download from ETS, the device will restart.



✓ The device is supplied with the individual address 15.15.255 (default factory setting). We advise against using this address for normal operation of a system and recommend assigning a different address when commissioning.

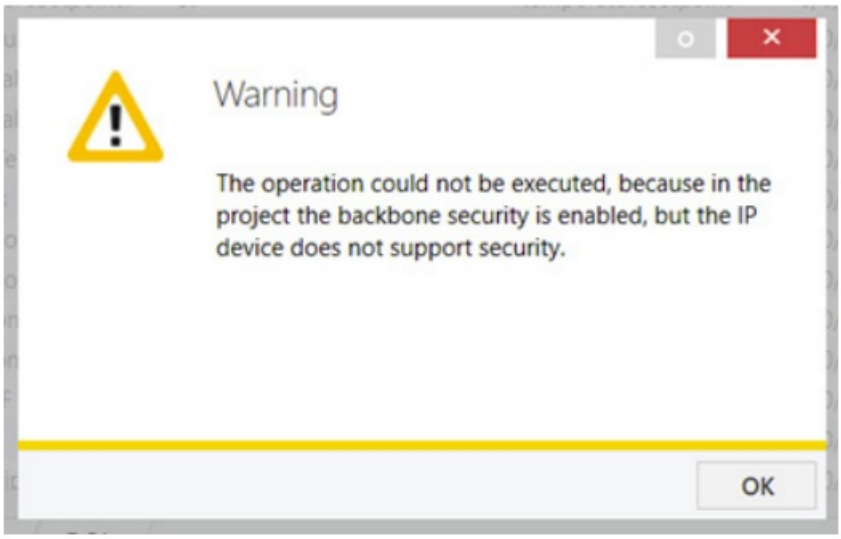
✓ If the configuration LED (I) flashes red, this means the Ethernet cable is not connected correctly or that a connection with an IP network is not available.

✓ The ETS database is available on the company website and in the ETS on-line catalogue.

Network backbone configuration with KNX Secure active.
If you want to use KNX Secure we recommend you set the Backbone IP to Secure (by default ETS sets it to “Automatic”). To set the backbone to secure, display the Topology and edit the “Security” property

This means that all the IP/KNX devices connected to the system support and are configured with KNX Secure.

In the presence of IP/KNX devices that are not configured in KNX Secure, ETS will display the following warning:

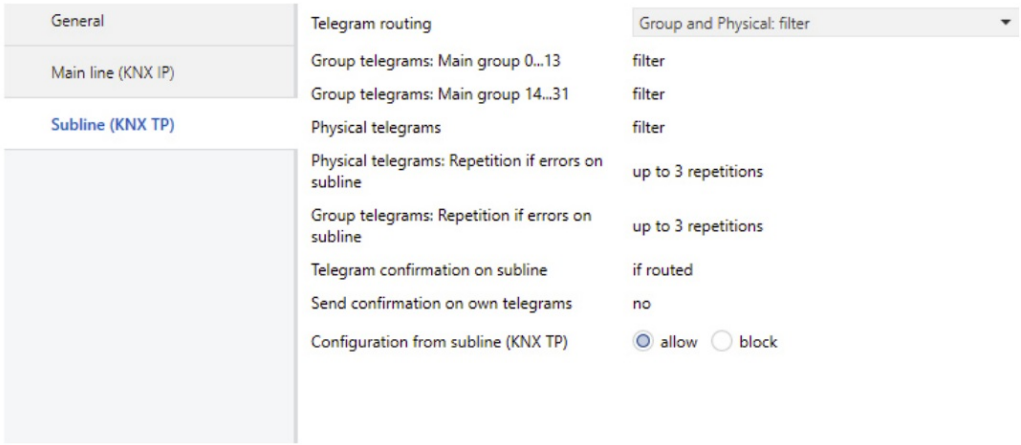


N.B. If reset devices are present, the default physical address 15.15.255 is not read by the ETS diagnostics because it is transmitted unencrypted when the

Backbone is Secure. Once the Backbone secure is activated, the configuration status of the various Secure devices will show as not up to date and so the application programmes will have to be downloaded again.

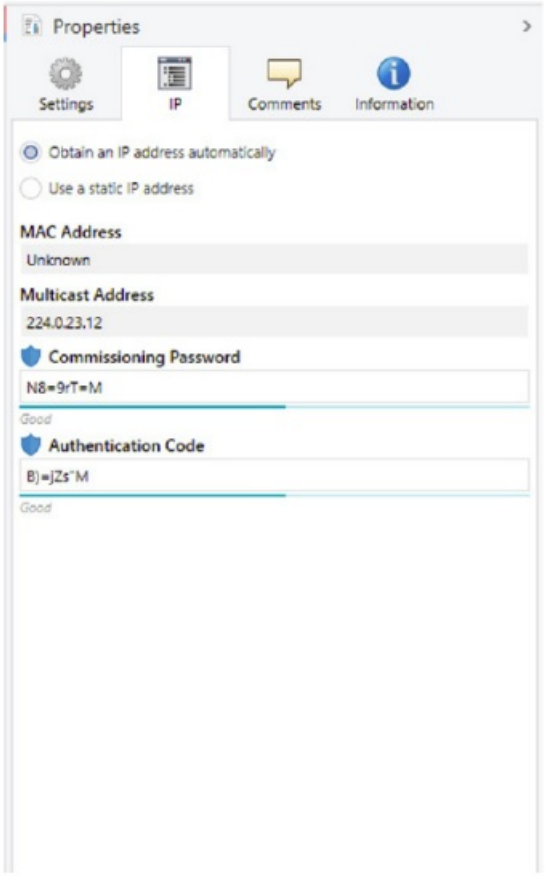
01548 interface configuration

For the correct operation of the router 01507 configuration procedure, the physical addresses on the secondary line (TP) must be filtered

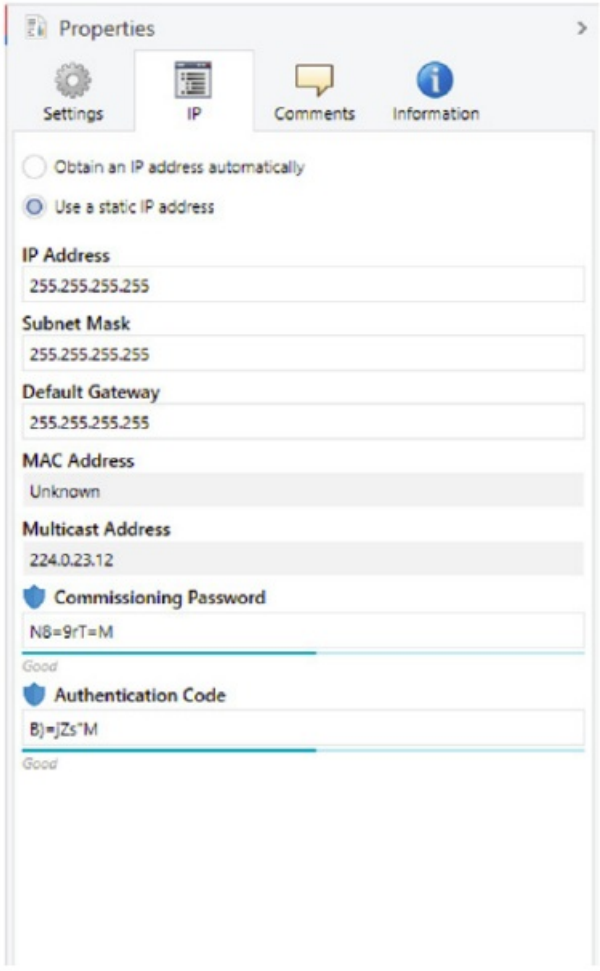


IP configuration

The IP configuration of 01507 can be specified in the ETS properties window. To activate DHCP/AutoIP, set the option: “Obtain an IP address automatically”. For further details and information about IP network configuration, please contact your local network administrator.

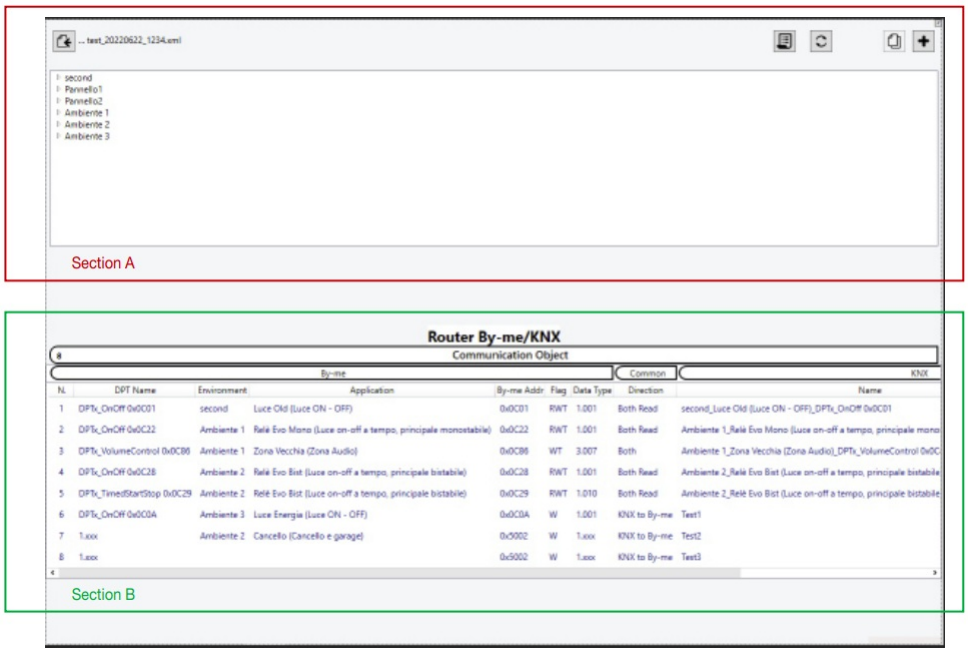


If you select the “Use a static IP address” option, you can manually set the IP address, the subnet and default gateway address.



Organising the DCA for customising associations

To simplify the definition of the association between By-me group and KNX group, there is a tab called DCA available (as in the figure below).



Controls

- Importing By-me plant
- Refresh
- Copy communication object
- Add communication object (not By-me)

Section A

Displays the By-me Plus system organised in a navigation tree:

- the “Environments” nodes are present at level I;
- the “Applications” nodes are present at level II;
- the “Group” nodes are present at level III;
- the “Group address” nodes are present at level IV.

The “Group” nodes are only displayed in the presence of applications which need several groups (see temperature control operation). If this is not the case, Level III is not displayed whereas information of Level IV Group addresses is presented.

Section B

Displays the list of all the By-me Plus/KNX associations which the installer has defined (max 500).

In the above figure, the area reserved for By-me information (on the left) is clearly distinguished from the area for the KNX data (on the right). The “Common” column contains the direction of group messages which cross the Router.

Each communication object defined can be deleted by tapping the icon  , which activates the deletion function

Tab

This is the section of ETS which contains all the default “Tab Group Object” and “Parameters”. A specific “DCA” tab is dedicate to “01507 Router By-me KNX” for the definition of the routing rules.

Preliminary procedures on the By-me Plus system
After configuring the By-me Plus system using the View Pro App, import the information in an xml file (see the By-me Plus manual).

Configured By-me Plus system
Allows you to import the By-me Plus system into the DCA.

1. Activate the function by clicking on icon  .
2. Using the file explorer, select the xml file containing the By-me Plus system data.

Section A contains the By-me Plus system data.

Adding a communication object from By-me Plus data

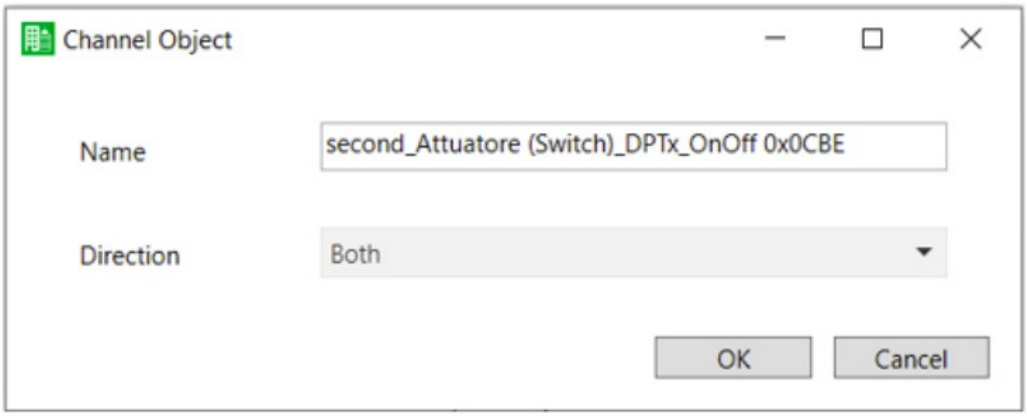
There are two ways to do this:

- Drag&Drop the “Group” node from Section A to the area reserved for Communication objects;
- Double-click on the “Group” node in Section A

Before adding the new Communication Object to the “By-me Plus KNX SECURE Router” a check is carried out for any error conditions:

- addition of a Communication Object when the By-me Plus KNX SECURE Router table has already reached 500 rows;
- duplicate Communication object name.

The installer can always customize the “Direction” and “Name” by double-clicking on the routing table row.

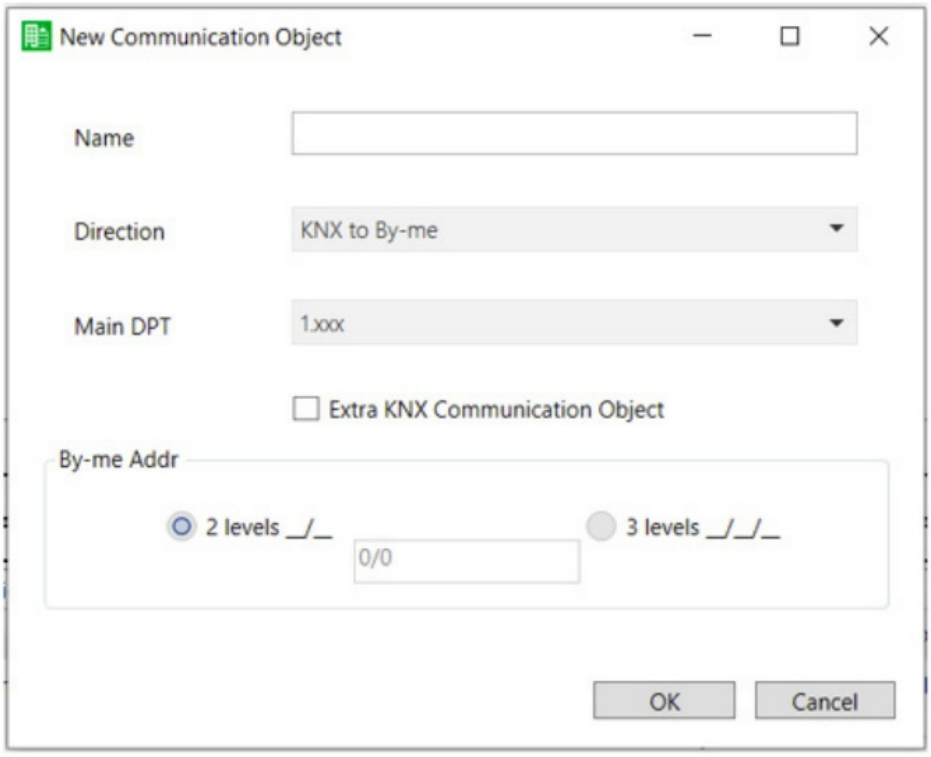


Non-configured By-me Plus system

Before importing the By-me Plus xml file, manually add all the Communication Objects on the KNX side using icon

.

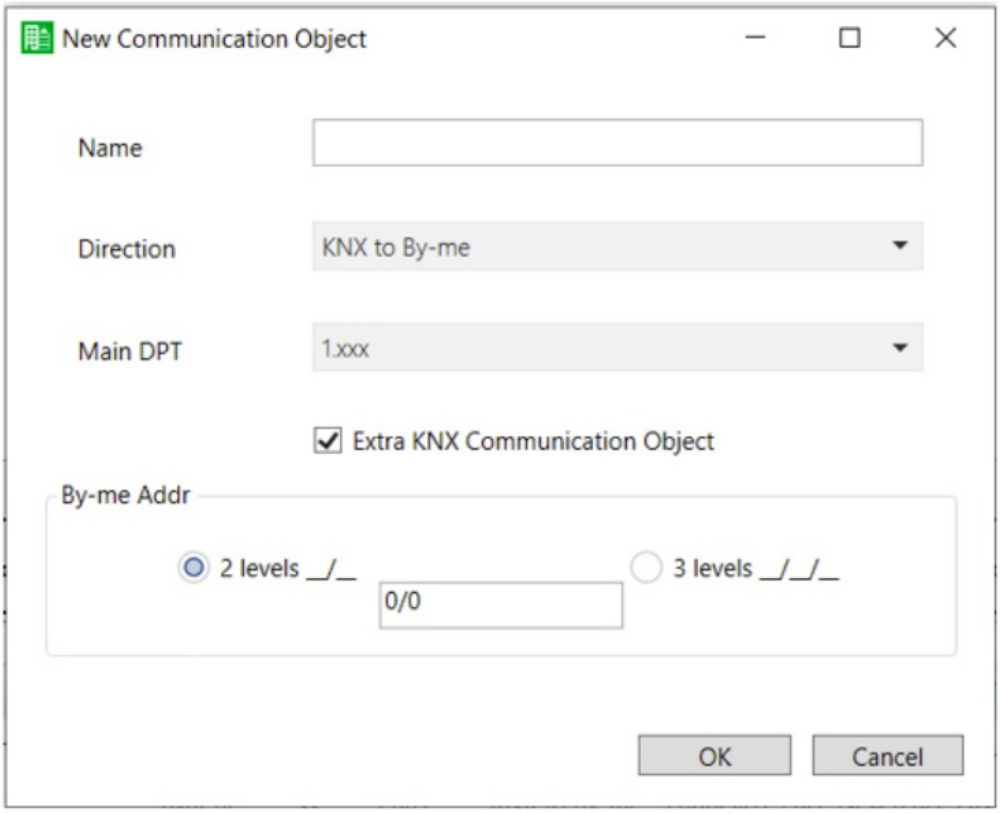
Once you have done this, you can import the By-me Plus system and complete the definition of associations.



In this case the name of the communication object is not automatically prompted by the procedure but is left up to the installer, who can also set the direction of the messages and the type of data transported (1.xxx will be valid for 1.001, 1.002, 1.003, etc.).

KNX Communication objects present in the By-me Plus island

With the “Extra KNX Communication Object” option, you can manage the KNX devices (not By-me Plus) connected inside the By-me Plus island. In this case, the device is not present in the By-me Plus xml file exported from the View Pro App.



To complete configuration, you need to specify the KNX format that the By-me Plus KNX SECURE Router should adopt; the options are:

- 2 levels
- 3 levels.

Next, the installer can set the KNX group address of the communication object they have just defined.

The group address is inserted in the “By-me Addr” column in the chosen KNX format.

Assigning By-me data to Communication Objects
After adding the KNX communication objects to the By-me Plus KNX SECURE Router device, proceed as follows:

1. Configure the By-me system with the home automation system gateway;
2. Export the system in xml format;
3. Access the “DCA” of the By-me/KNX gateway;
4. Import the xml file;
5. Drag&Drop the By-me Plus node to the row associated with the By-me Plus KNX SECURE Router of the routing table.

In this case the DCA should check the consistency of the “Data Type of the By-me DPTx” selected with what is already set in the destination row (Main DPT). Only if the respective Main DPTs match will the Drop be permitted (permitting the same format of the Main DPT on the By-me side with respect to the one on the KNX side: e.g. By-me Data Type 1.001 KNX Main Data Type 1.xxx).

Copying Communication Objects
The Copy function allows you to make a copy of a Communication Object for those which only have KNX data.

Once you have selected a row in the Communication Objects table, you can duplicate the related

Communication Object, whose window appears with the “Direction” and “Data Type” fields already set. You will need to edit the “Name” (which must be different).

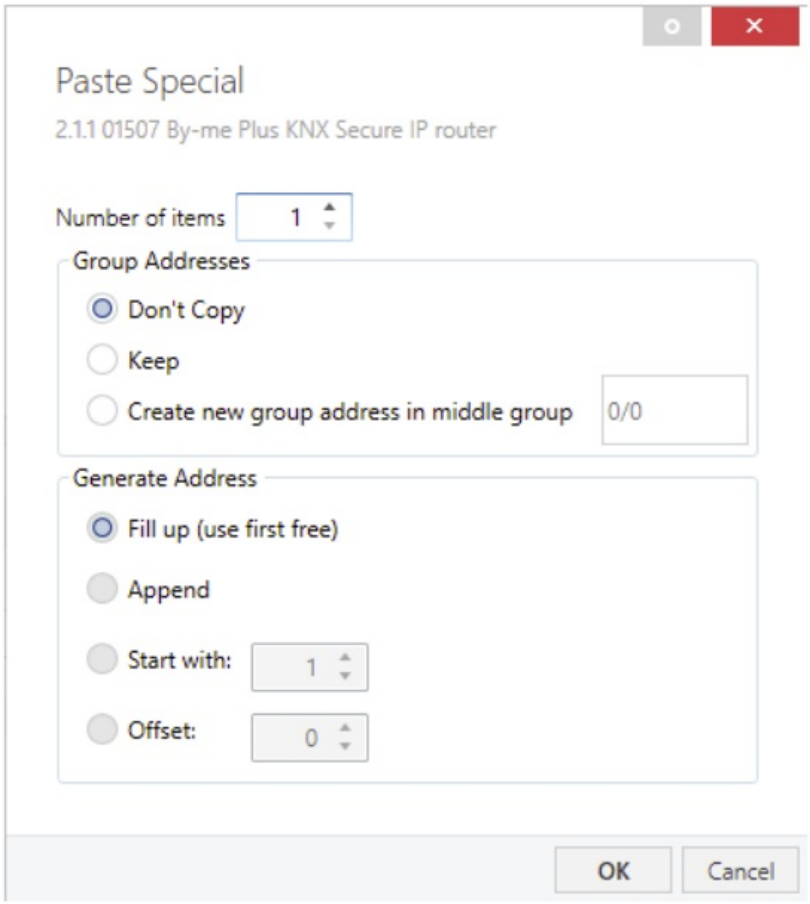
Errors

The following errors are envisaged:

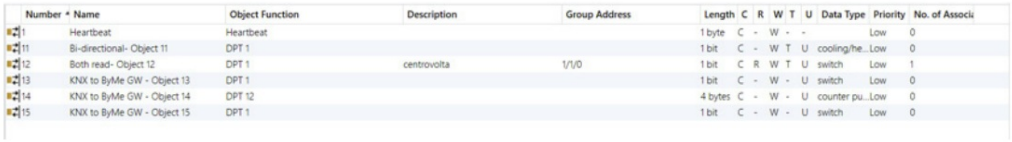
- “Copy Communication Object is disabled when there is no row in the By-me/KNX Gateway or it hasn’t been selected
- “Addition” of a Communication Object when the By-me/KNX Gateway table has already reached 500 rows.
- Communication Object selected has all the By-me parameters defined: in this case only the KNX part is duplicated (the name changes everywhere) whereas the By-me part stays empty and has to be associated starting with a node of the By-me tree.

N.B.: In the event that the By-me parameters are defined, the copy function is disabled.

Copying the By-me/KNX gateway from ETS
After defining the By-me/KNX Gateway, ETS can be used to duplicate the device inside the same KNX system and set its characteristics (see figure below).



Completing the ETS configuration
On completion of the By-me Plus KNX SECURE Router definition, tap the “Group Objects” tab to associate the group address with each communication object defined. This way, the information is managed similarly to the system KNX device information.

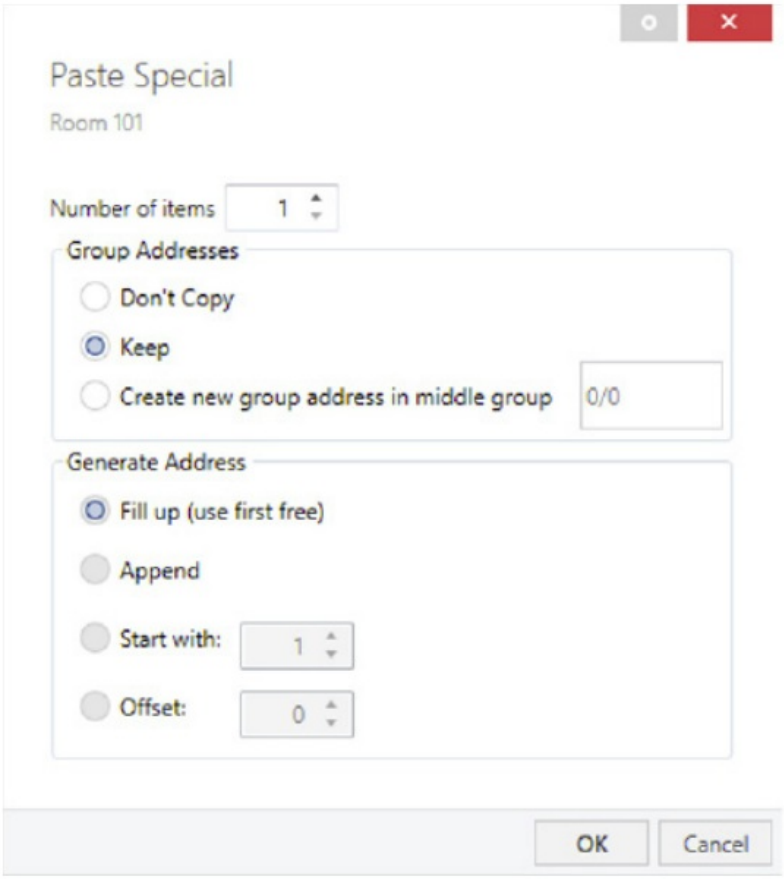


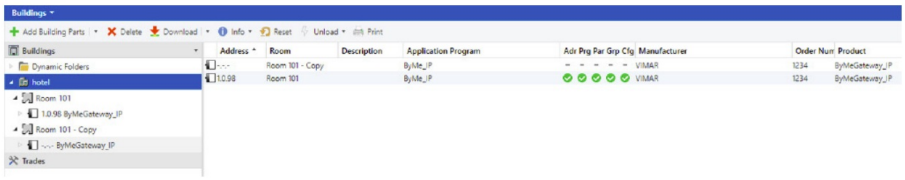
Number	Name	Object Function	Description	Group Address	Length	C	R	W	T	U	Data Type	Priority	No. of Associ
1	Heartbeat	Heartbeat			1 byte	C	-	W	-	-		Low	0
11	Bi-directional- Object 11	DPT 1			1 bit	C	-	W	T	U	cooling/he...	Low	0
12	Both read- Object 12	DPT 1	centrovolta	1/1/0	1 bit	C	R	W	T	U	switch	Low	1
13	KNX to ByMe GW - Object 13	DPT 1			1 bit	C	-	W	-	U	switch	Low	0
14	KNX to ByMe GW - Object 14	DPT 12			4 bytes	C	-	W	-	U	counter pu...	Low	0
15	KNX to ByMe GW - Object 15	DPT 1			1 bit	C	-	W	-	U	switch	Low	0

Cloning a room/area

This option allows you to clone a room (or area) already configured in another.

In the following example, room 101 is copied to room 102.





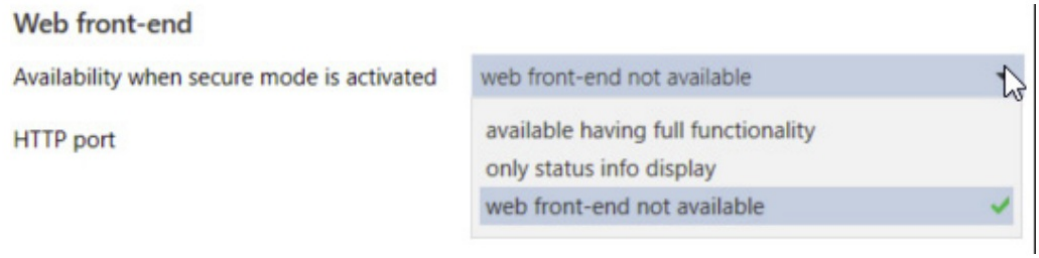
You can now rename Room 101 – Copy in Room 102 and attribute the physical address of the Gateway.

Front-end Web
The front-end Web can be used to read the actual parameters of device 01507 (HTTP port, IP address, MAC address, etc.) to update its firmware. To identify a specific device 01507 in a KNX network, the programming LED/remote programming mode can be turned on and off without pressing the programming button on the device.

✓ To return to the normal operation start mode, perform the firmware update procedure, then cancel it or wait 10 minutes until the automatic time-out.

Protecting the front-end Web of 01507
The front-end Web can be used to perform firmware updates remotely, for the control functions and to read the

device settings. To guarantee total protection of an installation, the front-end Web must be set to “not available” during runtime operation.
To use the remote functions of the front-end Web when the security function is active, it must be set to “available with all functions”.



If the front-end Web is set to “status display only”, the remote control functions (programming mode activation, tunnelling setting) and the updating function are disabled.
Information read only is available

✓ To guarantee the complete protection of a protected installation, the availability of the front-end Web must be set to “web front-end not available” which is the default value.

✓ For effective protection, we strongly advise the use of the “available with all functions” option as your permanent setting

Accessing the front-end Web of router 01507
You can access the front-end Web of 01507 in two ways. You can access it directly from Windows Explorer or from a web browser. To access via web browser, you need to know the IP address or the MAC address and the HTTP port. Below is a description of how to use the IP address or the MAC address in the browser address bar.

✓ You need to use the correct HTTP port to access from a web browser.

✓ The value of the HTTP port is 8080 (non-editable

With the MAC address
When NetBIOS is installed (by default setting in Windows systems), the MAC address can be used. It is printed on the label affixed to the side of the 01507 device casing (which is also listed in the interfaces identified by ETS). Due to the name resolution, the communication must be established according to the Host name.

The activation of NetBIOS is required to do this.

Use the MAC address in format AA-BB-CC-XX-YY-ZZ and the HTTP port set by default to be entered in the browser address bar as specified below, without the brackets:

http://knx-iprt-[XXYYZZ]:[HTTPport]/

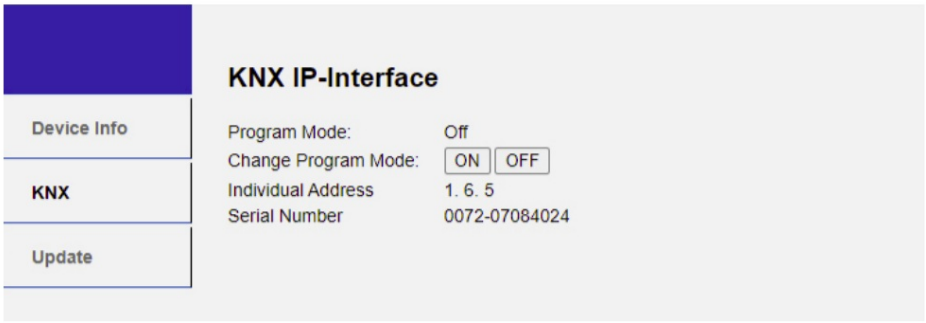
Example:
the label on the side of the 01507 device casing shows the MAC address D0-76-50-11-22-33 and the HTTP port is 8080. Enter in the browser address bar.

Information about the device
After accessing the front-end Web, the Device Info chart is displayed, which contains general information about the current device parameters (addresses, name, software versions).

KNX

The specific KNX addresses are shown on this screen. Checking the settings is simple. Click on “ON” to activate the programming mode (which is the equivalent to pressing the programming button). Together with the device information screen, this function is useful to distinguish the device concerned (since it has a specific IP address, MAC address and serial number) from other similar devices in the network.

The individual address and the multicast routing address are displayed.



Special functions

IP firmware update request

Press the H button followed by button L on router 01507 (steps 1 and 2 in Table 8); then activate “request update” to enter boot mode. This displays ”Status: update authorised”.

Table 8: Activating the firmware update

Step Firmware update

1. Brief press of the programming button
2. Brief press of the function button and page refresh
3. Click on “request update” in the front-end Web
4. The By-me BUS line status LED (C) is flashing green
5. The firmware file can be selected
6. The device restarts

Updating the IP firmware

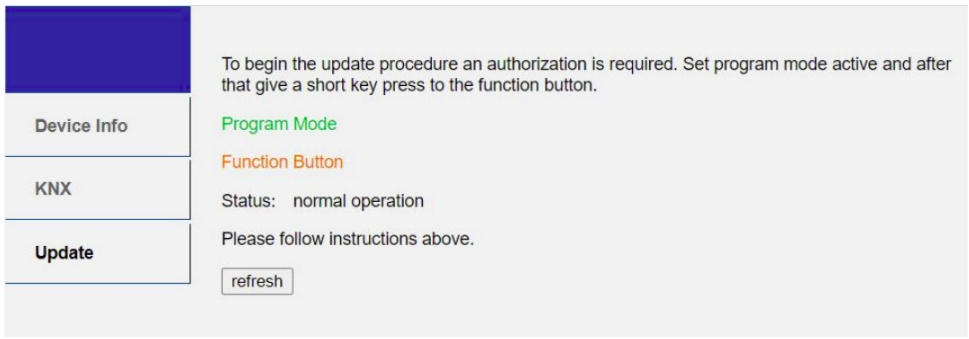
In the Update screen of device 01507 you can update the firmware via IP, or the Ethernet network. The following steps describe the complete remote updating
procedure. During the process, device 01507 enters boot mode. So LEDs D, E, F and G light up as described in Table 5: LED status for firmware updating

If boot mode is already active, only follow the instructions of the front-end Web from step 3 to 5 (update, request update).

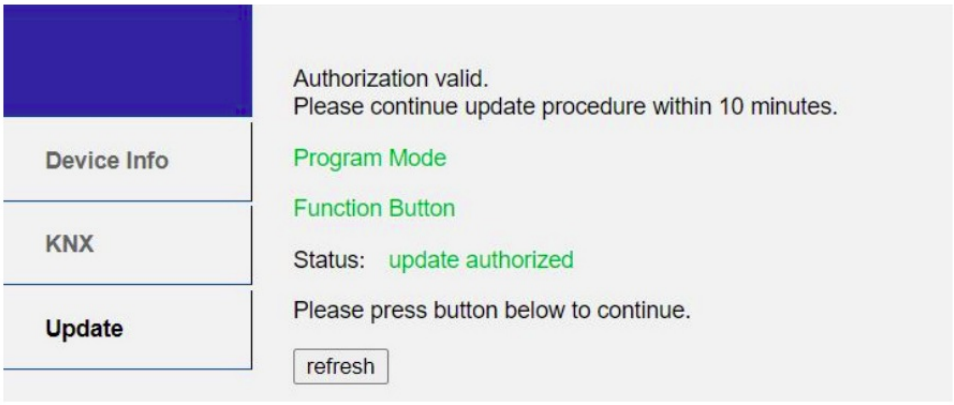
To quit boot mode, access the Update screen on the front-end Web. You can then complete the firmware updating, as described in steps 1 to 5, or suspend the firmware updating by clicking on the “Abort” button (see step 5). Next, device 01507 is restarted and resumes normal operation.

Step 1: Open the Update screen on the front-end Web.

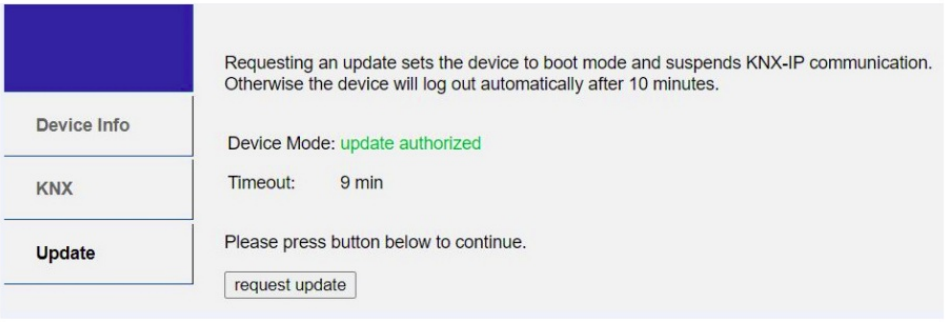
Step 2: Activate programming mode (KNX tab or programming button).



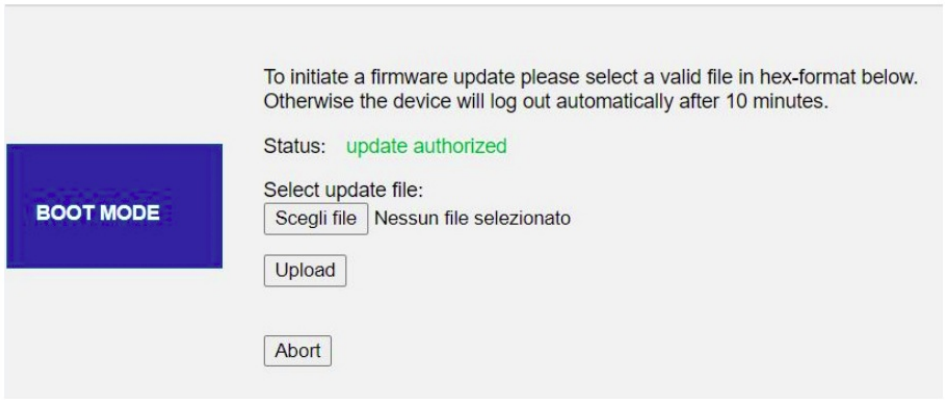
Step 3: After activating programming mode, briefly press the function button. Then press the “refresh” button.



Step 4: When the “request update” button is displayed, press it to select the update file and access boot mode.



Step 5: You can select the update file (which has the extension .hex) and upload it. At the end, the device exits boot mode and is restarted. If you click on the “Abort” button the firmware updating procedure is cancelled and the device exits boot mode.

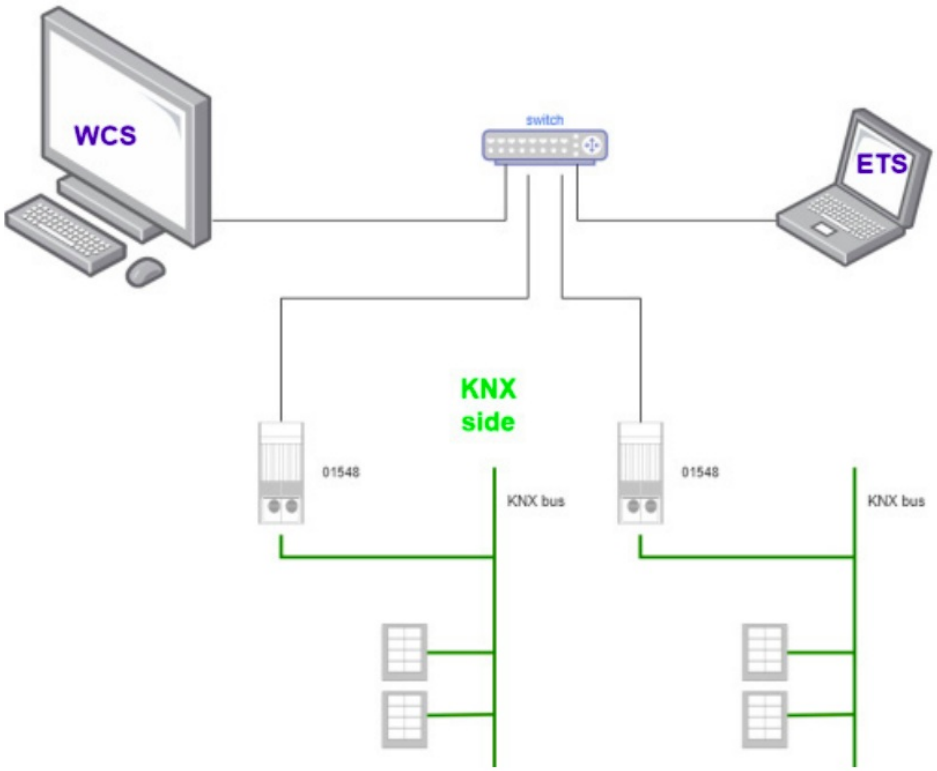


Resetting the device
The reset button (H) activates the factory reset. The settings of device 01507 can be restored to the default manufacturer settings with the factory reset function

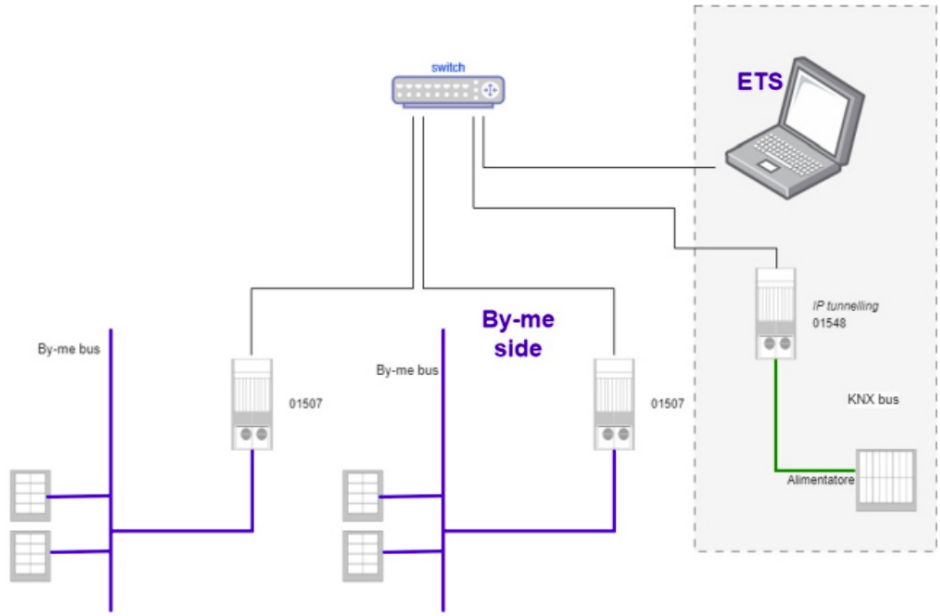
Usage examples

Caution: Devices 01507 and 01548 cannot be configured on the same area/line since the former is TP and the other IP.

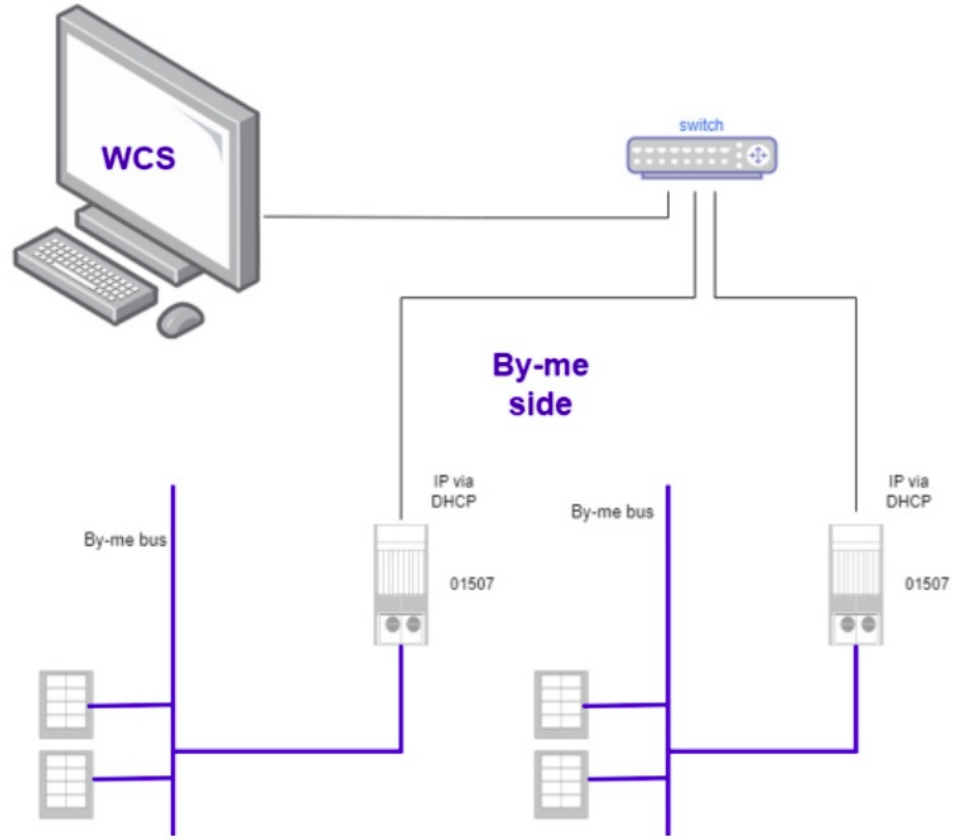
KNX system with supervision from Well-contact Suite and configuration with ETS



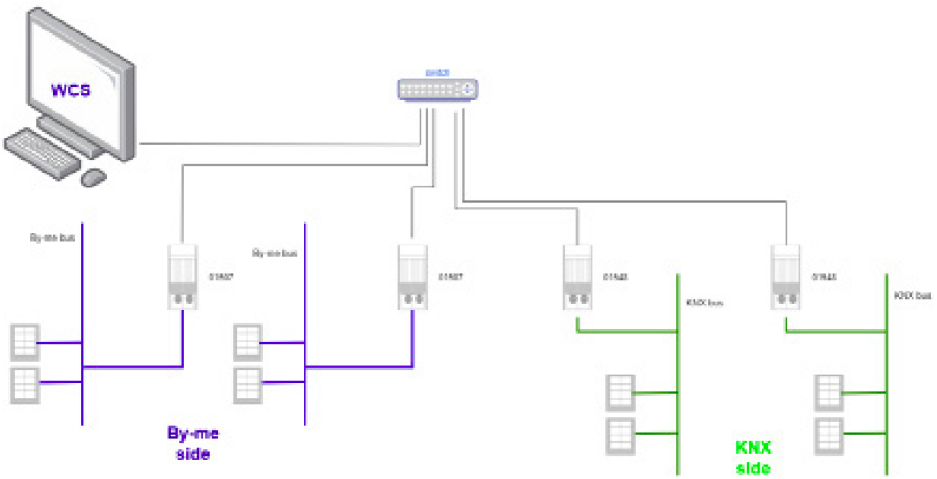
By-me system with 01507 TP/IP, configuration with interface 01548



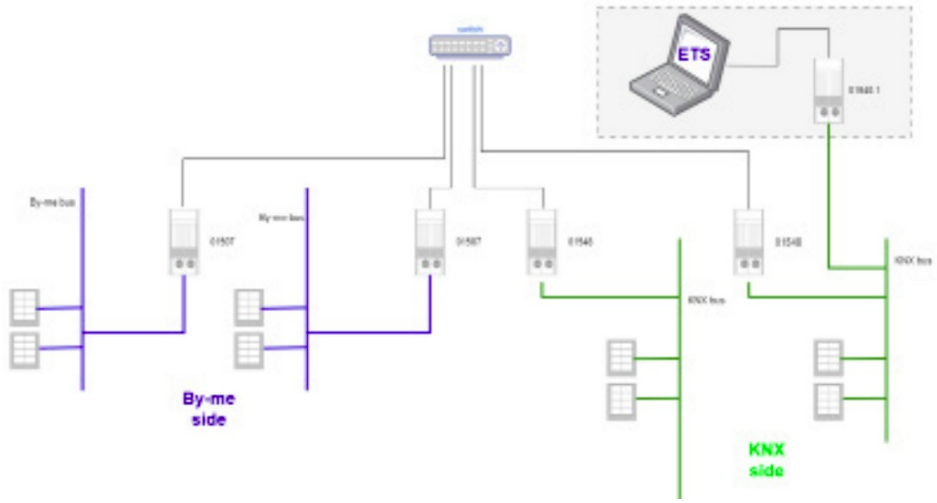
By-me system with 01507 TP/IP, WCS supervision



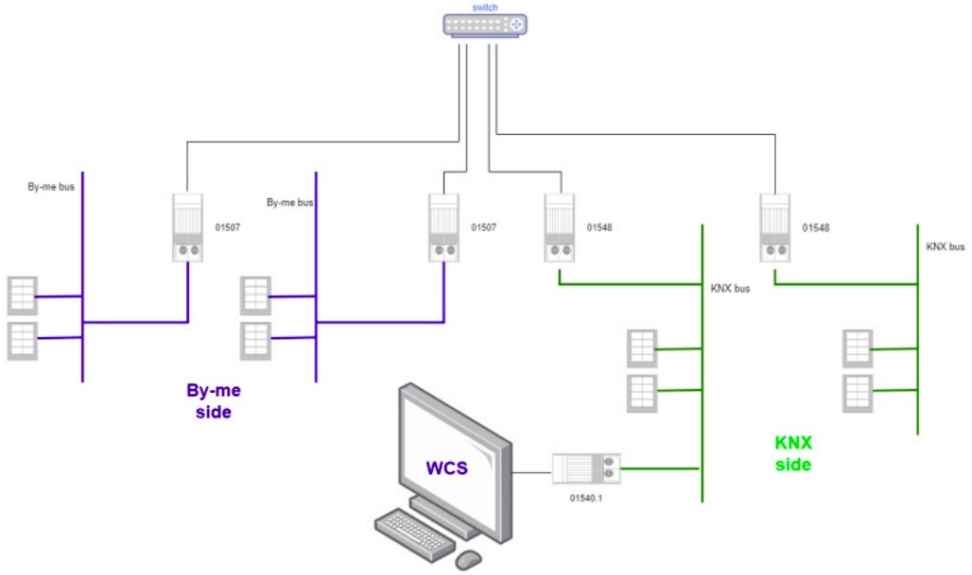
Mixed system with 01507 TP/IP, WCS supervision



Mixed system with 01507 TP/IP, configuration with 01540.1



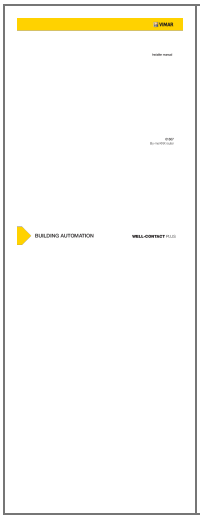
Mixed system with 01507 TP/IP, supervision with 01540.1



01507IT 01 230

Viale Vicenza 14
36063 Marostica VI – Italy
01507IT 01 2309 www.vimar.com

Documents / Resources

	VIMAR 01507 By me KNX Router [pdf] Instruction Manual 01507 By me KNX Router, 01507, By me KNX Router, KNX Router, Router

References

- Home automation, electrical equipment, smart home - Vimar energia positiva