Installer manual

01548
KNX IP media coupler

BUILDING AUTOMATION

WELL-CONTACT PLUS

Contents

1. Product Description

The basic function of the 01548 router is to ensure KNX IP/Ethernet devices (main line) interact with KNX TP bus devices (secondary line). It is powered by the TP bus and does not require an external power supply. The router is designed to route traffic based on the type of installation in the bus system hierarchy and according to the filter tables incorporated for communication towards groups. The secondary line configuration can be deactivated. When used as an interface, the device has configuration, commissioning, display, protocol and diagnostics functions. The operating and filter statuses, the faults and the communication errors are indicated via LEDs. The device supports messages with up to 240 bytes APDU length and it features the "Function" button to deactivate the filter temporarily during commissioning or troubleshooting.

The device is for KNXnet/IP (Secure) Routing and Tunnelling and it is equipped with a dedicated QR code to be used with ETS (version 5.5 and later) during configuration. The Secure Tunnelling, Secure Commissioning and IP Backbone Protection can be activated.

The 01548 router is displayed on the network; the device settings can be set, the functions activated and the 60-minute busload history can be displayed via web. Moreover, the "bootloader" function enables the remote updating of the firmware via IP/Ethernet.

1.1 Front Panel

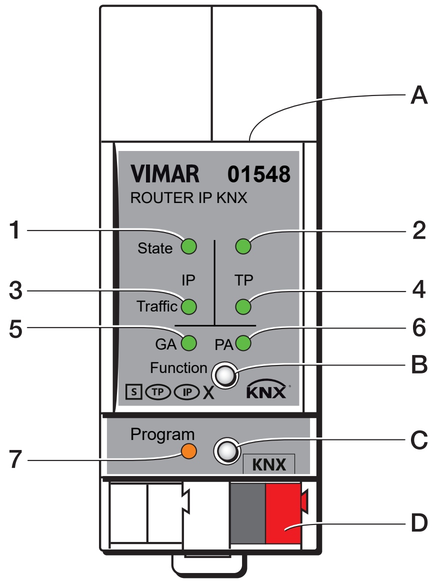


Figure 1: Front View

Table 1: Front Panel Elements

LEDs	
1	State IP (Main line)
2	Bus State KNX TP (Subline)
3	Telegram Traffic IP (Main line)
4	Telegram Traffic KNX TP (Subline)
5	Group Address Routing*
6	Individual (Physical) Address Routing
7	Programming LED

* only group telegrams with main groups 0…13

Buttons / Connectors	
A	Ethernet Connector
B	Function Button
C	Programming Button
D	KNX TP Connector

1.2 LED Indication

Following overview table gives a description of the LED display during normal operation. The display during an active special function is described in next chapter.

Table 2: Normal LED Display

Number	LED	Color	Explanation / Range
1	**State IP (Main line)**	green	IP line OK (connection established)
		orange	Manual Function active
		< off >	No IP connection
2	**Bus State KNX TP (Subline)**	green	Subline OK
		< off >	Subline not connected
3	**Telegram Traffic IP (Main line)**	blinking green	Telegram traffic extent indicated by blinking
		< off >	No telegram traffic
4	**Telegram Traffic KNX TP (Subline)**	blinking green	Telegram traffic extent indicated by blinking
		blinking red	Transmission error (BUSY, NACK, missing IACK)
		< off >	No telegram traffic
5	**Group Address Routing**	green	Filter table active
		orange	Route all
		red	Block all
		< off >	Routing of Group Telegrams is different on main line and subline
6	**Individual (Physical) Address Routing***	green	Filtering active
		orange	Route all
		red	Block all
		< off >	Routing of Physical telegrams is different on main line and subline
7	**Programming LED**	red	Programming Mode active
		blinking red	No IP connection
		< off >	Programming Mode not active

* behavior is not defined for routers having an invalid configuration i.e. Individual Address

1.3 LED Indication of Special Functions

Only LEDs described here are lighting during an active special function. Other LEDs are off.

Table 3: LED Status Display for Manual Function

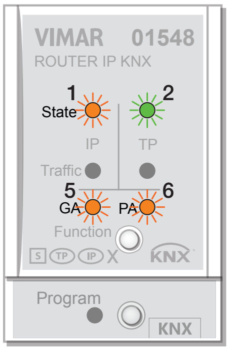
Number	LED	Color	Comment	
1	**State IP**	orange	Lights red if not connected	
2	**Bus State KNX TP**	green		
5	**Group Address Routing**	green: filter orange: route all red: block all		
6	**Individual Address Routing**			

Table 4: LED Status Display for Factory Reset after first Function Button Press

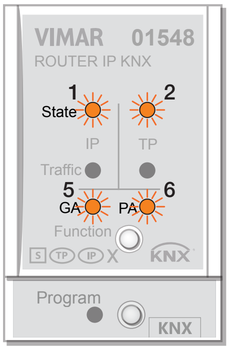
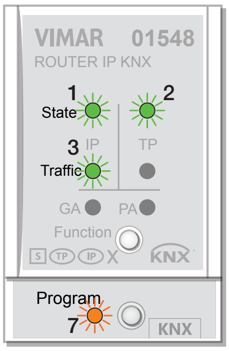
Number	LED	Color	Comment	
1	**State IP**	orange	Lights red if not connected	
2	**Bus State KNX TP**	orange		
5	**Group Address Routing**	green: filter orange: route all red: block all		
6	**Individual Address Routing**			

Table 5: LED Status Display for Firmware Update

Number	LED	Color	Comment	
1	**State IP**	green	blinking, later lighting	
2	**Bus State KNX TP**	blinking green		
3	**Telegram Traffic IP**	green		
7	**Programming LED**	red		

1.4 Commissioning

Please note for commissioning with default settings:

- All telegrams are blocked because the filter table is not defined
- The Manual Function switch-off time is 120 min
- Individual Address is 15.15.0
- Activation of Security and Secure Commissioning require the Device Certificate
- Activation of Security requires a minimum ETS version

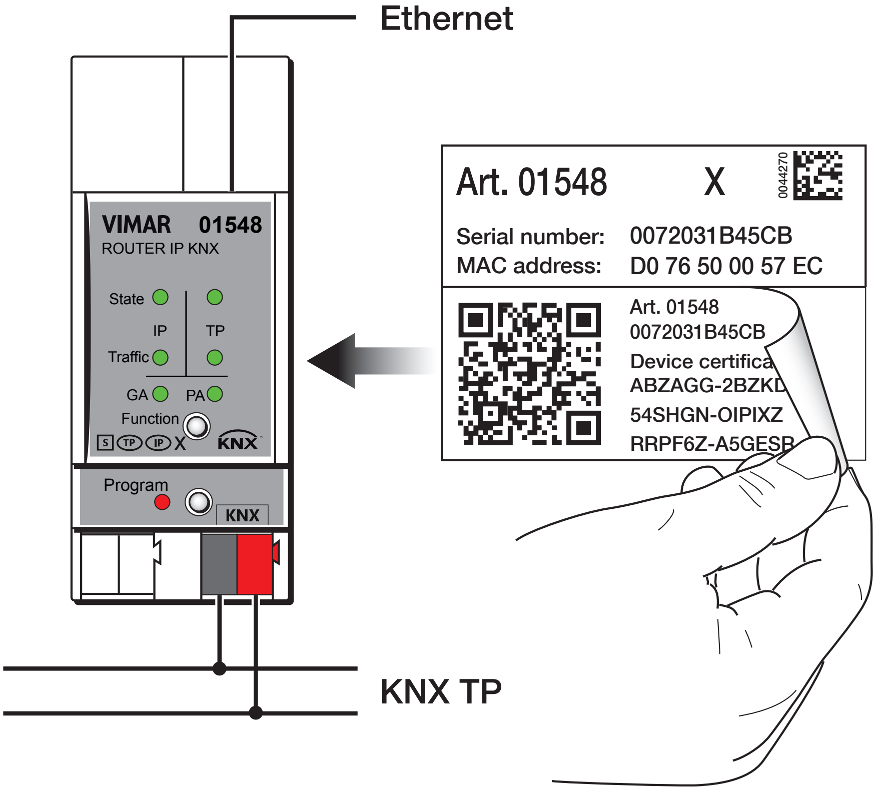


Figure 2: Connection Scheme

✓ To start a secure configuration download, Secure Commissioning must be activated in the ETS project before. Without activation, 01548 will behave like 01547.1 (without support of KNX Secure).

✓ Please also read chapter “1.6 Important Notes” before putting the device into operation.

1.5 Secure Commissioning

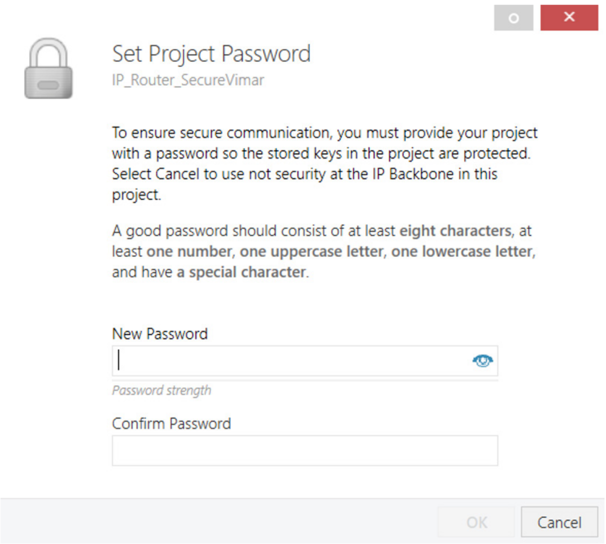
Before the secure download of configuration setting and/or Individual Address can start, the individual Device Certificate of 01548 must have been added to the ETS project. To add it, the ETS project must be password-protected.

✓ A Secure download is only possible after activation of Secure Commissioning.

✓ Activation of Secure Commissioning demands the individual Device Certificate.

✓ Device Certificates can only be added to an ETS project when it is password-protected.

When no project password is set, Secure Commissioning cannot be activated. ETS projects with having Secure Commissioning and/or Security set to active always require pre-setting a project password. Having no project password set on activation of Security, the ETS then asks to type it in.



Set Project Password

IP_Router_SecureVimar

To ensure secure communication, you must provide your project with a password so the stored keys in the project are protected. Select Cancel to use not security at the IP Backbone in this project.

A good password should consist of at least **eight characters**, at least **one number**, **one uppercase letter**, **one lowercase letter**, and have a **special character**.

New Password

Password strength

Confirm Password

Figure 3: Set Project Password

✓ The individual Device Certificate always is enclosed with the KNX Secure product. To keep the product configurable by the user, it is important to make sure the Device Certificate cannot be lost (please note chapter 1.7 Safekeeping of Device Certificate).

1.6 Important Notes

It is recommended to participate the standardized courses of a KNX-certified training center before installing, programming, and commissioning a KNX system. Here, the participant gains the necessary knowledge and skills, also required for troubleshooting, by practical exercises.

Please read this chapter carefully before first use and installation:

1.6.1 Installation and Commissioning

- In the case of damage (at storage, transport) no repairs may be carried out by unauthorized persons
- After connection to the KNX bus system, the device works with its default settings
- Warning: Do not connect to 230 V. The device is supplied by the KNX bus and does not require any additional external power supply
- The device may only be installed and put into operation by a qualified electrician or authorized person
- For planning and construction of electric installations the appropriate specifications, guidelines and regulations in force of the respective country have to be complied
- For configuring, use the ETS (or ETS Inside)

1.6.2 Mounting and Safety

- For mounting use an appropriate equipment according to IEC60715
- Installation on a 35 mm DIN rail (TH35)
- Connect the KNX bus line as for common KNX bus connections with a KNX bus cable, to be stripped and plugged into a KNX TP connector
- Do not damage electrical insulations during connecting
- Installation only in dry locations

1.6.3 Maintenance

- Accessibility of the device for operation and visual inspection must be provided
- The housing must not be opened
- Protect the device from moisture, dirt and damage
- The device needs no maintenance
- If necessary, the device can be cleaned with a dry cloth

1.7 Safekeeping of Device Certificate

The Device Certificate can be found on a label that is adhered on side of the housing. To avoid unwanted access, the Device Certificate has to be removed from the device after commissioning. Therefore, the label consists of two parts, one fixed part that must remain on the housing (for identification) and one tear-off part that can be removed (for keeping at a safe place).

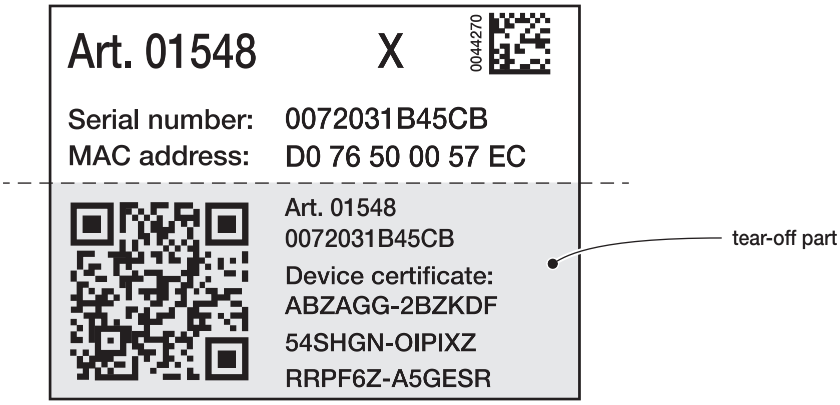


Figure 4: Device Certificate Label

After the Device Certificate was added to the Device Certificate list in ETS, the tear-off part of the Device Certificate label can be archived at a safe place. The Device Certificate list only needs to contain the certificates of the KNX Secure devices that are used within the ETS project. ETS then automatically uses the correct certificates for programming the relevant devices.

For clear identification of the device after removing the tear-off part, the serial number is printed on both label parts, on the one that was removed and the fixed one that stays on the housing.

✓ When the tear-off part that contains the Device Certificate is lost, only the password-protected ETS project contains the Device Certificate.

✓ Be aware, when the Device Certificate is completely lost, meaning the tear-off part is unavailable and the project password is lost, too, the device cannot be used in Secure mode (Security cannot be activated) anymore! From then, also after carrying out a Factory Reset, the device can only be used unsecured, as “plain” device.

1.8 Feature Summary

- Device Certificates guarantee only authorized persons can have access to 01548.
- When the ETS “Secure Commissioning” function is activated, configuration data is downloaded only in encrypted KNX Data Secure format.
- Activation of “IP Backbone Security” for protection of IP routing.
- When additional protection becomes necessary (for example, the subline is located outside the building), configuring 01548 from the subline can totally be switched off.
- 01548 supports long telegrams with up to 240 bytes APDU length. (Devices of both product series, the MEC couplers and UIM interfaces, can process long messages e.g. for energy metering applications and visualization purposes.)
- 01548 favorably replaces a common TP line/area coupler. The great advantage is using KNX IP as a fast KNX backbone medium.
- 01548 works without external power supply.
- For IP (Secure) Tunneling, four tunneling connections can be realized in parallel. On activation of Secure Tunneling, the password protection becomes available.
- Settings to increase the data throughput / decrease a high bus traffic are featured.
- IACK sending on sent out messages is configurable.
- Repetition is configurable for both Physical Telegrams and Group Telegrams.
- Telegram filtering can be temporary suspended by only pressing the Function button. Filtering then is limited to ease commissioning, troubleshooting or fast on-site diagnostics and access to other lines becomes possible without additional ETS download.
- Automatic switch back to run-time telegram filtering after expiry of the configurable suspension period (see Manual Mode). This avoids forgetting to reactivate filtering.
- UPnP Discovery enables discovering 01548 within the IP network.
- ETS recognizes 01548 as bus connection interface by KNXnet/IP Search Request.
- Updating the firmware can easily be accomplished by a web browser.
- The available web front-end provides informative settings and enables to remotely switch the device into Programming Mode without using the Programming Button.
- With the web front-end, a diagram of a 60 min busload history can be watched.
- When Security is active, the web front-end can also be used limited or fully disabled.
- 01548 supports KNXnet/IP, ARP, ICMP, IGMP, HTTP, UPnP discovery, UDP/IP, TCP/IP, DHCP and AutoIP.

2. KNXnet/IP

The presence of the Internet Protocol (IP) has led to the definition of the KNXnet/IP protocol. As documented in the KNXnet/IP protocol specifications, KNX telegrams can be transmitted encapsulated in IP packets. Ethernet networks can be used to route and tunnel KNX telegrams.

KNX IP routers are highly similar to TP line couplers. Only difference is they use the IP communication medium instead of TP and the KNXnet/IP communication protocol. According to this, IP interfaces and IP routers are an excellent alternative to USB data interfaces and TP line/area couplers. A TP backbone can be completely be replaced by a fast Ethernet based IP Backbone line. KNX end devices can be integrated directly via IP. This makes the Ethernet a real KNX medium.

2.1 IP (Secure) Tunneling

KNXnet/IP offers the possibility for point-to-point connections for the ETS (IP Tunneling connections) or, for example, between supervisory system and KNX installation. On activation of “Secure Tunneling”, these connections become IP Secure Tunneling connections. They are protected by encryption and usage of extra passwords.

2.2 IP (Secure) Routing

IP Routing is the KNXnet/IP protocol for interconnecting KNX lines and areas by IP networks. Hereby, the KNXnet/IP protocol defines the KNX IP communication. Using IP Secure Routing means runtime communication on KNX IP is entirely encrypted according to the KNX IP Secure mechanism.

2.3 IP Firmware Update

The IP bootloader function makes it possible to remotely carry out Firmware Updates and rewrite the flash memory content via an IP connection. This is not just a simple application download. Both communication stack and application software are downloaded.

The Firmware Update procedure via IP can be executed by 01548´s web front-end, which is independent from ETS, and makes use of special messages to speed up the process. To be protected, this process makes use of a special encryption.

3. KNX Secure

The KNX Secure technology adds extra security to a KNX installation, during commissioning as well as for KNX installations at runtime. Difference between normal KNX devices and KNX Secure devices is KNX Secure devices have the ability to encrypt and decrypt telegrams.

Every KNX Secure device supports a secure mode. Only when this secure mode is activated, the KNX Secure device will be able to encrypt/decrypt telegrams. For activation, device certificates are necessary (see chapter 1.5 Secure Commissioning).

KNX telegrams encrypted by KNX Secure devices are called KNX Secure telegrams. Regarding both KNX Security mechanisms, KNX IP Secure and KNX Data Secure, two types of encryption can be distinguished:

- KNX IP Secure can only be applied upon the KNX IP medium. KNX telegrams are sent as encrypted IP Secure frames, also called entirely encrypted telegrams (no matter if KNX Data Secure is used or not).
- KNX Data Secure can be applied on any KNX communication medium. End-to-end communication between end devices is encrypted. Due to an individual security key, end devices encrypt/decrypt parts of their telegrams. Then, only devices having identical Group Addresses can encrypt/decrypt the telegrams.

For programming a KNX Secure device, ETS must know both its factory key (FDSK) and its serial number. But it is not necessary entering factory key or serial number. The ETS generates this information from the Device Certificate.

A Device Certificate is a device-specific 32-character code which contains serial number and FDSK (Factory Default Setup Key). Serial number and FDSK cannot be modified. ETS retrieves the FDSK via the device certificate (see chapter 1.5 Secure Commissioning).

After a KNX Secure device has been added to an ETS project and after its Device Certificate has been added too, ETS automatically sets the Tool Key for the project. This Tool Key cannot be modified. It can only be reset to its FDSK by a Factory Reset (see chapter 4.6.2 Factory Reset).

✓ Mixing unsecure and secure communication on the same Group Address is impossible.

✓ A mix of KNX IP Secure couplers in secure mode with KNX IP Secure devices in plain mode, or simply plain KNX IP devices, does not work.

4. Operational Description

In KNX network installations, 01548 is used as KNX IP line/area coupler to couple KNX IP and KNX TP (see also chapter 2.2 IP (Secure) Routing). It can be used in the common way without activation of Security and in ETS projects where Security is set to active. After connecting to KNX TP, 01548 operates with its default settings. Setting a correct Individual Address is necessary. Only Individual Addresses x.y.0 are allowed.

4.1 IP Secure Router Application

When 01548 receives telegrams (for example during commissioning) that use Individual Addresses as destination addresses, it compares the Individual Addresses of the receiver with its own Individual Address and decides on that whether it has to route the telegrams or not.

When 01548 receives telegrams that use group addresses as destination addresses, it reacts in accordance with the parameter settings. During normal operation (with Group Telegram routing set to filter), 01548 only routes the telegrams whose group addresses are entered in the group filter table.

If a telegram is routed by 01548 without receiving the corresponding acknowledgement, i.e. due to a missing receiver or to a transmission error, the telegram will be repeated up to three times (depending on the ETS setting). With the parameters „Repetitions if errors ...“, this function can be configured separately for each line and both kinds of telegrams. It is recommended to use the default parameter setting.

IP Router is designed for use in 10/100 BaseT networks compliant to IEEE802.3. The AutoSensing function sets the baud rate (10 Mbit or 100 Mbit) automatically. IP address can be received from a DHCP server. For this, the automatic assignment setting of the IP address can be set by ETS (“obtain an IP address automatically”). If set so and no DHCP server is found, 01548 starts an AutoIP procedure and autonomously assigns the IP address. If 01548 is supposed to have a fixed IP address (as well as subnet mask and standard gateway) it can be set by ETS.

4.2 IP Network

01548 sends telegrams from/to the TP network to/from the IP network in accordance with the KNXnet/IP protocol specification. According to the default setting, IP telegrams are sent as IP Multicast to the IP address 224.0.23.12 port 3671. The Multicast IP address 224.0.23.12 is the defined address for KNXnet/IP by KNX Association in conjunction with the IANA. It is recommended to change this address only when it becomes necessary due to the existing network.

Important notes:

- All KNX IP devices that are intended to communicate with each other via IP must have the same IP multicast address.
- Multicast IP address 224.0.23.12 may need to be changed in respect of the network type and of the network components´ settings.
- IGMP (Internet Group Management Protocol) is used for IP Routing and Discovery.
- If problems occur for IP address assignment, please ask your network administrator.
- According to the topology, Individual Addresses that are used for Tunneling channels always have to be assigned in the range of subline addresses. Detailed information about additional Individual Addresses for (Secure) Tunneling can be found in chapter 5.4 IP (Secure) Tunneling Address Assignment.

4.3 KNX Network Installation

Up to 15 areas and 225 different addresses for line couplers can be defined. For line coupler functionality in a KNX network, 01548 has to use the correct Individual Address of a line coupler (x.y.0). For backbone coupler functionality in a KNX network, 01548 has to use the correct Individual Address of an area coupler (x.0.0).

✓ It is recommended to make sure the factory default Individual Address 15.15.0 is not used in the installation network.

✓ Defining a correct topology is absolutely mandatory to guarantee proper functioning of an installation.

In a KNX system with 01548 backbone couplers and 01504.2 line couplers, it is necessary to ensure that 01548 has an address assigned from a free addressing area. Following figure illustrates a possible topology scenario.

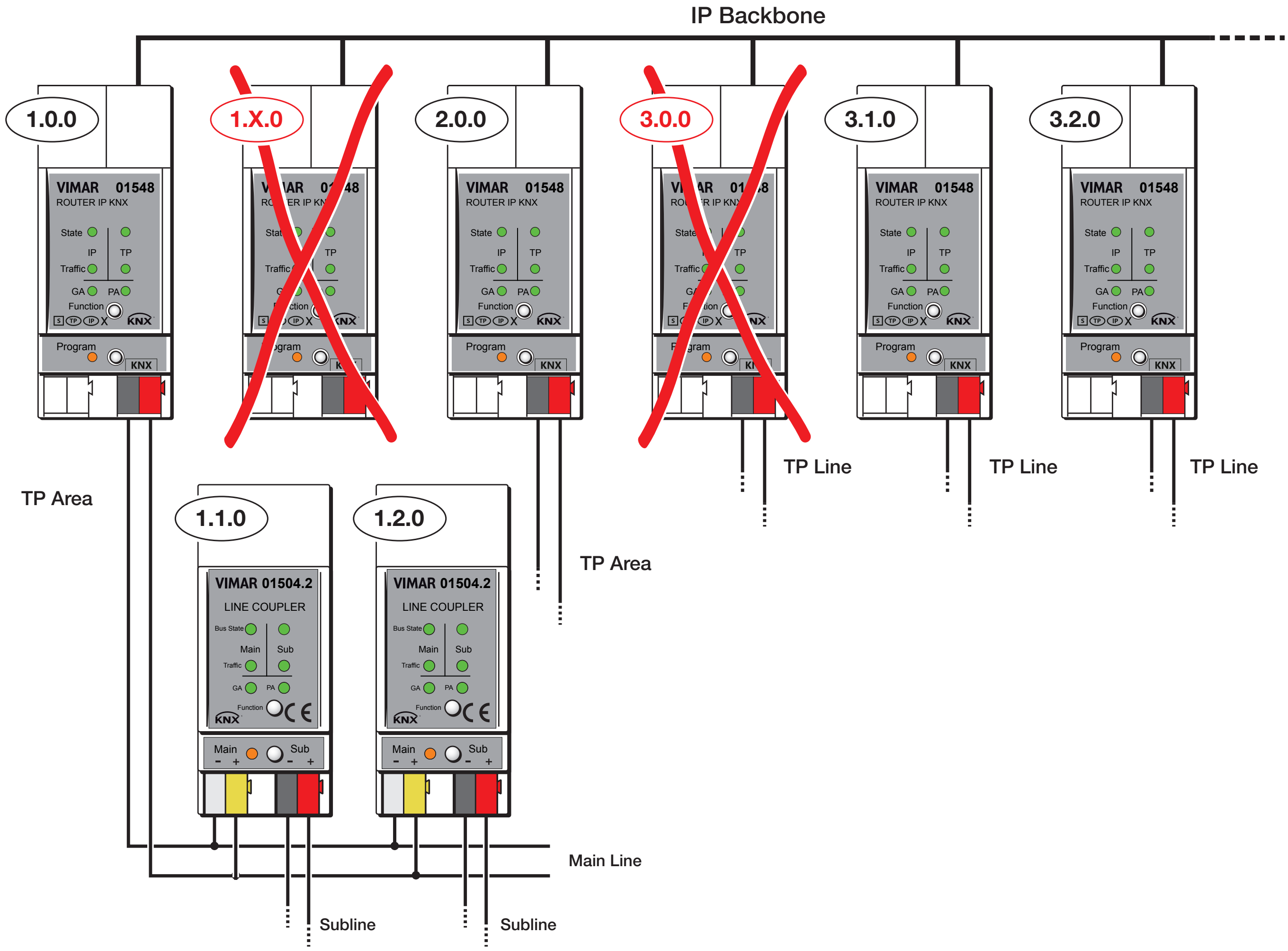


Figure 5: 01548 Network Topology

Example:
If a KNX IP router with address 1.0.0 already exists on the backbone no KNX IP router with address 1.x.0 can be added here. Even if no line coupler with address 1.1.0 exists on the subline of the 1.0.0 router. Vice versa, when line couplers with addresses 3.x.0 already exist in an installation, an IP router with address 3.0.0 cannot be added.

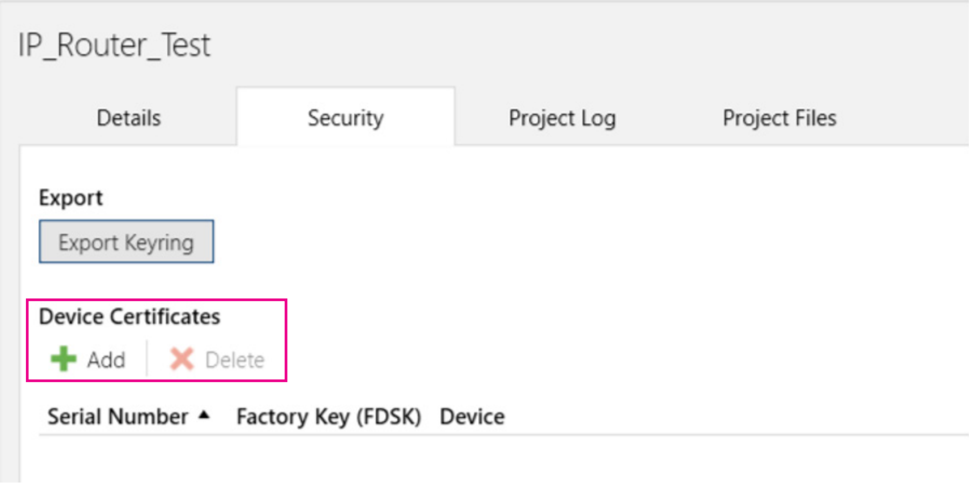
4.4 Adding Device Certificate

Every KNX Secure device uses its own Device Certificate. Entering this Device Certificate in ETS is mandatory before activating or using KNX Security functions.

✓ The Device Certificate can be found printed on a side label on the housing.

✓ Device Certificates can be entered manually and by taking a QR code webcam picture.

After opening the project, the Device Certificate list can be edited In the Security tab under Project Overview.



IP_Router_Test

Details | Security | Project Log | Project Files

Export

Export Keyring

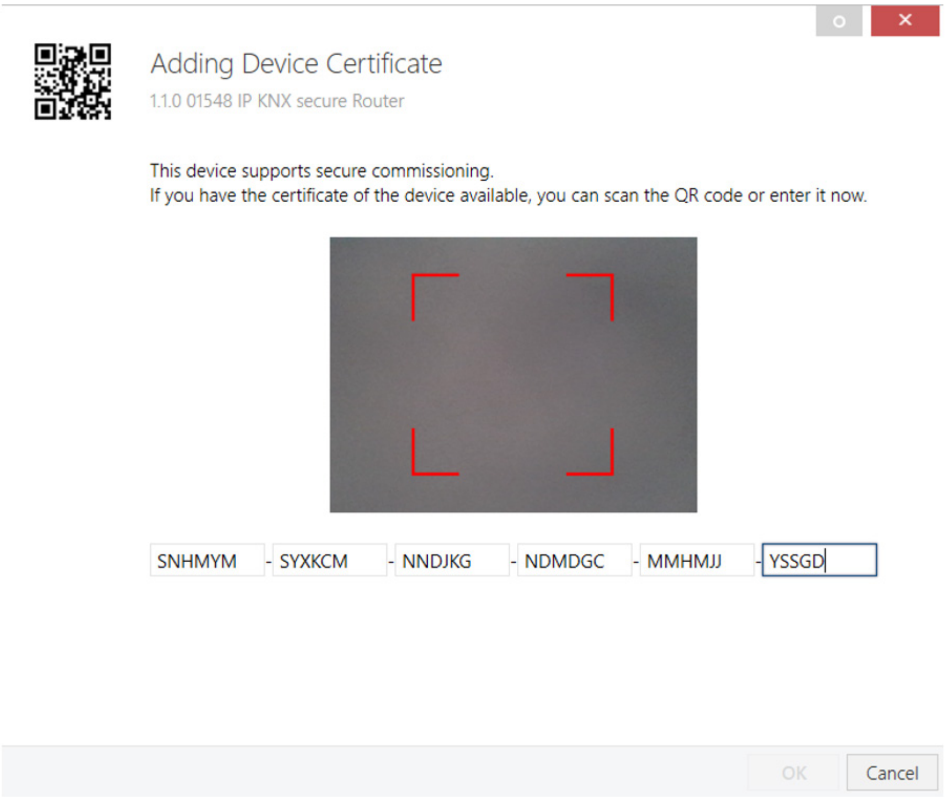
Device Certificates

Add | Delete

Serial Number | Factory Key (FDSK) | Device

Figure 6: Device Certificate List

If not already having the Device Certificate added to the list, on starting a Secure download following window appears.



Adding Device Certificate

1.1.0 01548 IP KNX secure Router

This device supports secure commissioning.
If you have the certificate of the device available, you can scan the QR code or enter it now.

SNHMYM - SYXKCM - NNDJKG - NDMDGC - MMHMJJ - YSSGD

OK | Cancel

Figure 7: Adding Device Certificate

4.5 Programming

4.5.1 Programming of Individual Address (and Application)

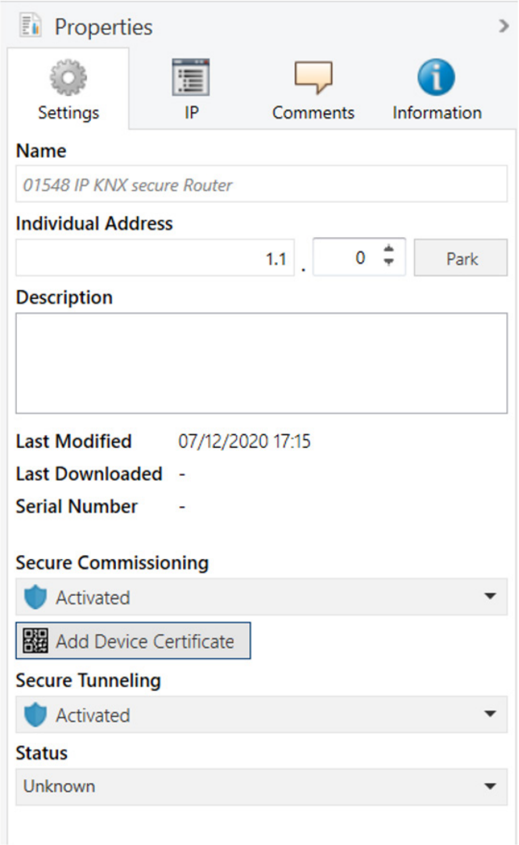
To download the Individual Address (IA) into the device, Programming Mode must be active. Successive pressing the Programming Button switches Programming Mode on and off. LED 7 lighting red indicates Programming Mode is set active. On activation of the ETS download and pressing the Programming Button, the device stores the new Individual Address in its memory. Security settings are actualized via both IA download and application download.

✓ When 01548 is the Current Interface, an application download is necessary for actualizing IP settings of 01548.

✓ For downloading, an interface connection to the KNX bus system is required.

✓ To program devices of a line different to which the device used as ETS Current Interface is connected, a correct topology is mandatory.

The Individual Address can be assigned to the device by setting the desired address in the properties window of the ETS. When the ETS download is complete, the device restarts itself.



Name
01548 IP KNX secure Router

Individual Address
1.1 . 0

Description

Last Modified 07/12/2020 17:15
Last Downloaded -
Serial Number -

Secure Commissioning
Activated

Secure Tunneling
Activated

Status
Unknown

Figure 8: ETS Properties Windowt

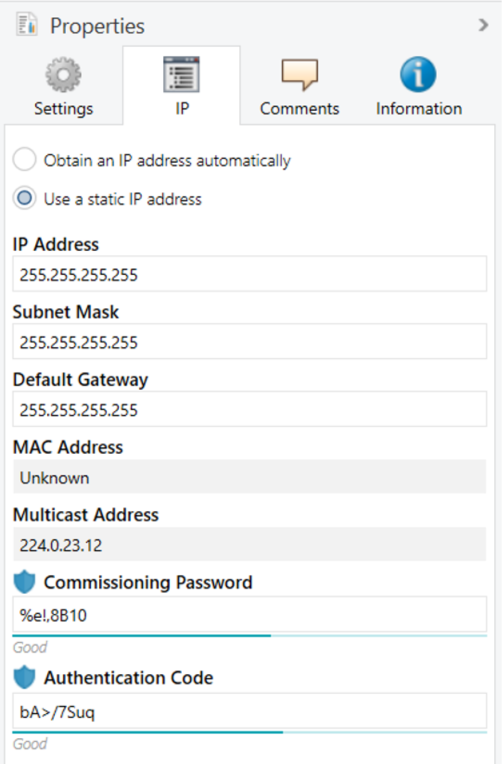
✓ The device is supplied with the Individual Address 15.15.0 (Factory Default Setting). It is recommended not to use this address for normal operation of an installation and to assign a different address when commissioning.

✓ A blinking red Programming LED indicates the Ethernet cable is not properly connected or no IP network connection is available.

✓ ETS database is available at the company website and in the ETS Online Catalog.

4.5.2 IP Configuration

The IP configuration of 01548 can be set in the Properties window of the ETS. To activate DHCP/AutoIP, the "Obtain an IP address automatically" option must be set. For more details and information about configuration of IP networks, please ask your local network administrator.



○ Obtain an IP address automatically

● Use a static IP address

IP Address
255.255.255.255

Subnet Mask
255.255.255.255

Default Gateway
255.255.255.255

MAC Address
Unknown

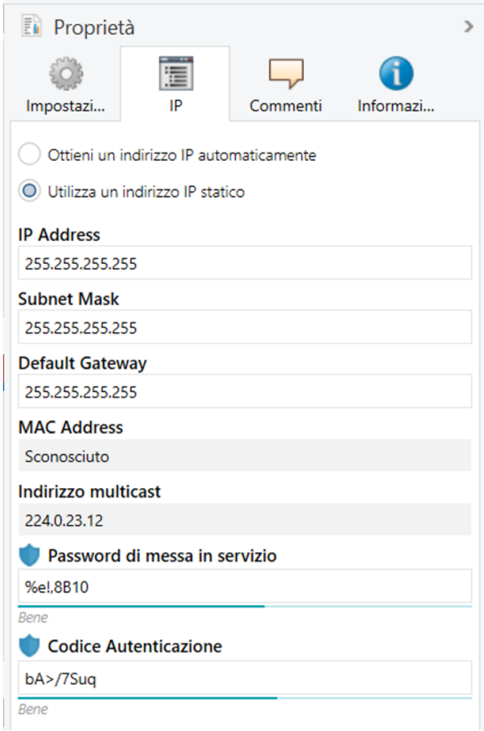
Multicast Address
224.0.23.12

Commissioning Password
%e!,8B10
Good

Authentication Code
bA>/7Suq
Good

Figure 9: Automatic IP Address Assignment

When the „Use a static IP address" option is chosen, IP address, Subnet Mask and Default Gateway can be set manually.



○ Ottieni un indirizzo IP automaticamente

● Utilizza un indirizzo IP statico

IP Address
255.255.255.255

Subnet Mask
255.255.255.255

Default Gateway
255.255.255.255

MAC Address
Sconosciuto

Indirizzo multicast
224.0.23.12

Password di messa in servizio
%e!,8B10
Bene

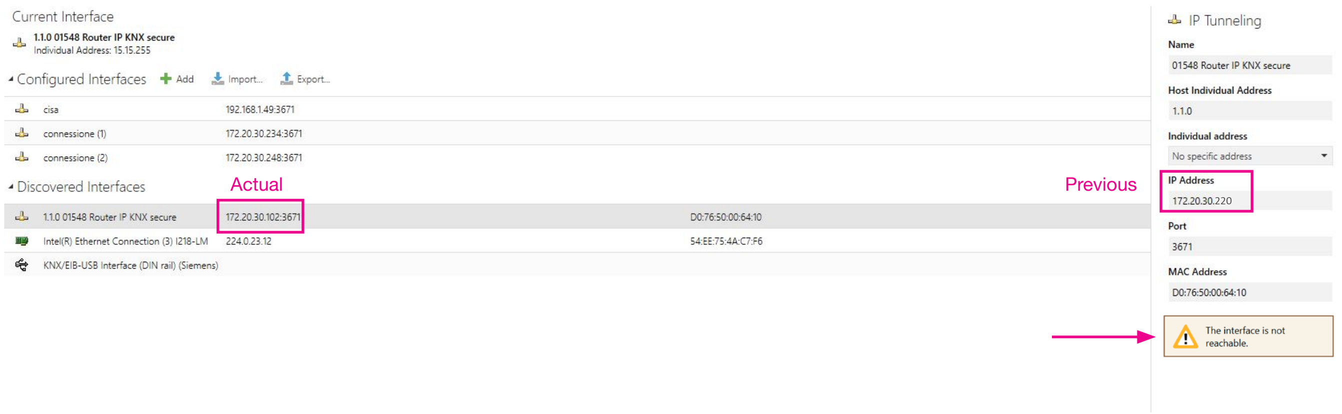
Codice Autenticazione
bA>/7Suq
Bene

Figure 10: Manual IP Address Assignment

✓ KNX IP devices intended to communicate with each other via the IP (Secure) Routing protocol must use the same Multicast Address.

✓ Changing the Multicast Address can only be done under the IP (configuration) tab in the Backbone´s Properties window. It appears after a click on the blue Topology bar.

✓ When 01548 is used as ETS Current Interface and its IP address is changed by a configuration download, ETS tries to maintain the connection to the Current Interface having the previous IP address. 01548 (now containing the actualized IP address) must be selected as Current Interface again from the list of Discovered Interfaces. Until then, the previous IP Address is still visible in the IP Tunneling window and ETS shows the Current Interface is not reachable.



Current Interface
1.1.0 01548 Router IP KNX secure
Individual Address: 15.15.255

Configured Interfaces

cisa	192.168.1.49:3671	
connessione (1)	172.20.30.234:3671	
connessione (2)	172.20.30.248:3671	

Discovered Interfaces

1.1.0 01548 Router IP KNX secure	172.20.30.102:3671	D0:76:50:00:64:10
Intel(R) Ethernet Connection (3) I218-LM	224.0.23.12	54:EE:75:4A:C7:F6
KNX/EIB-USB Interface (DIN rail) (Siemens)		

IP Tunneling

Name: 01548 Router IP KNX secure
Host Individual Address: 1.1.0
Individual address: No specific address
IP Address: 172.20.30.220
Port: 3671
MAC Address: D0:76:50:00:64:10

The interface is not reachable.

Figure 11: IP Address of the Current Interface before and after Actualization

4.6 Special Functions

The Function Button activates 01548´s special functions. Manual Function and Factory Reset can be activated. Device settings of 01548 can be reset to manufacturer default values with the Factory Reset function. During the Firmware Update procedure, the Function Button has to be pressed. The status of an active special function is indicated by the LED display (see chapter “1.3 LED Indication of Special Functions”).

4.6.1 Manual Function

During normal operation, a rather short press (≈ 3 sec) activates and deactivates the Manual Function. LED 5 and LED 6 show the current filtering states.

When the Manual Function is active, either all Physical Telegrams or all Group Telegrams or both can pass the 01548 without filtering. When the Switch-off time has elapsed, 01548 automatically switches back to normal operation. To configure the Manual Function and set the Switch-off time, use the parameter tab General like shown in chapter 5.1 General. After switching back from Manual Function to normal operation, the latest downloaded parameter setting / filter table entries are active again.

Table 6: Activation of Manual Functions

Step	Manual Function
1	Hold Function button for 3 seconds
2	LED 1 now is orange indicating Manual Function is on
3	After switch-off, normal operation is indicated by LED 1 lighting green

4.6.2 Factory Reset

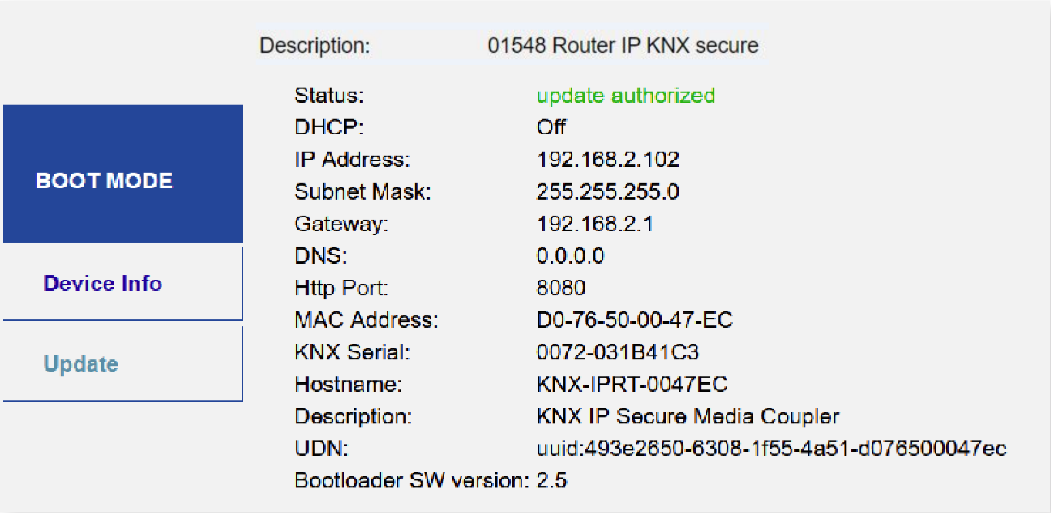
A long press (≈ 15 sec) of the Function Button soon followed by a short press (≈ 3 sec) executes the Factory Reset. After the first press, the LED display lights like described in Table 4: LED Status Display for Factory Reset after first Function Button Press. After the second press, all parameters (incl. Individual Address) will be set to factory default. When Security is activated, also the Tool Key is set back to its FDSK. Subsequently, LEDs show the normal operation display again.

Table 7: Activation of Factory Reset

Step	Factory Reset
1	Hold Function button for 15 seconds
2	LEDs 1/2 now are orange
3	Hold Function button for 3 seconds
4	Device restarts

4.6.3 IP Firmware Update Request

During normal operation, a rather short press (≈ 3 sec) activates and deactivates the Manual Function. LED 5 and LED 6 show the current filtering states.



Description: 01548 Router IP KNX secure

Status: update authorized
DHCP: Off
IP Address: 192.168.2.102
Subnet Mask: 255.255.255.0
Gateway: 192.168.2.1
DNS: 0.0.0.0
Http Port: 8080
MAC Address: D0-76-50-00-47-EC
KNX Serial: 0072-031B41C3
Hostname: KNX-IPRT-0047EC
Description: KNX IP Secure Media Coupler
UDN: uuid:493e2650-6308-1f55-4a51-d076500047ec
Bootloader SW version: 2.5

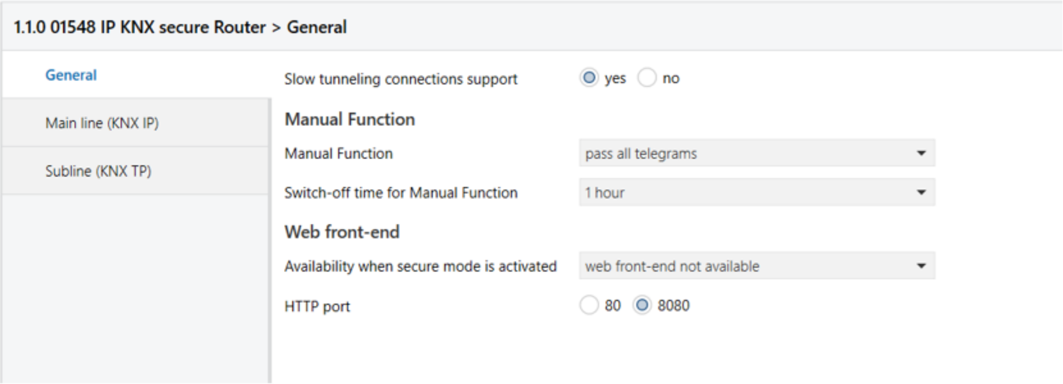
Figure 12: Authorized Update Request

Table 8: Activation of Firmware Update

Step	Firmware Update
1	Short press on Program button
2	Short press on Function button
3	Click on “request update” in the web front-end
4	LED2 is blinking green
5	Firmware file can be selected
6	Device restarts

5. ETS Database

5.1 General



1.1.0 01548 IP KNX secure Router > General

Slow tunneling connections support ● yes ○ no

Manual Function

Manual Function: pass all telegrams

Switch-off time for Manual Function: 1 hour

Web front-end

Availability when secure mode is activated: web front-end not available

HTTP port ○ 80 ● 8080

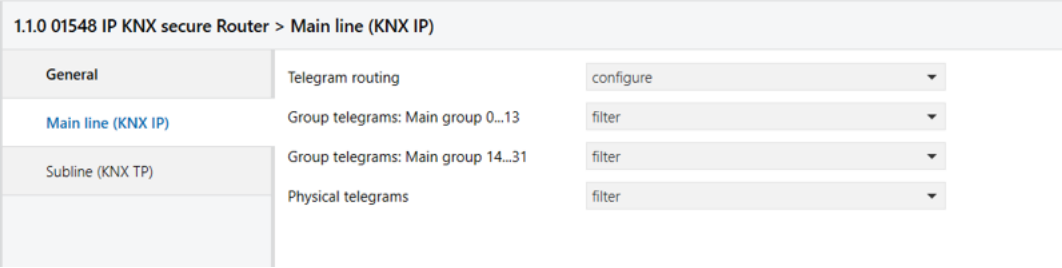
Figure 13: General Tab Parameters

Table 9: General Tab Parameter Settings

ETS Parameter	Settings [Default Parameter]	Comment
Slow tunneling connections support	yes no **[no]**	Enable or disable support of slow tunneling connections.
Manual Function		
Manual Function	disabled pass all telegrams pass all Physical telegrams pass all Group telegrams **[pass all telegrams]**	Configuration setting for telegram routing when the Manual Function is active.
Switch-off time for Manual Function	10 min, 1 hour, 4 hours, 8 hours **[1 hour]**	After expiry of this time period the Manual Function is switched off automatically.
Web front-end		
Availability when secure mode is activated	available having full functionality only status info display web front-end not available **[web front-end not available]**	When Security is switched on, the web front-end can be fully available (read/write), be available for limited usage (only read) or be deactivated.
HTTP port	80 8080 **[8080]**	Select the HTTP port.

5.2 Main Line (IP)

✓ Setting “transmit all” is intended only for testing use. Please do not use for normal operation.



1.1.0 01548 IP KNX secure Router > Main line (KNX IP)

Telegram routing: configure

Group telegrams: Main group 0...13: filter

Group telegrams: Main group 14...31: filter

Physical telegrams: filter

Figure 14: Main Line (IP) Tab Parameters

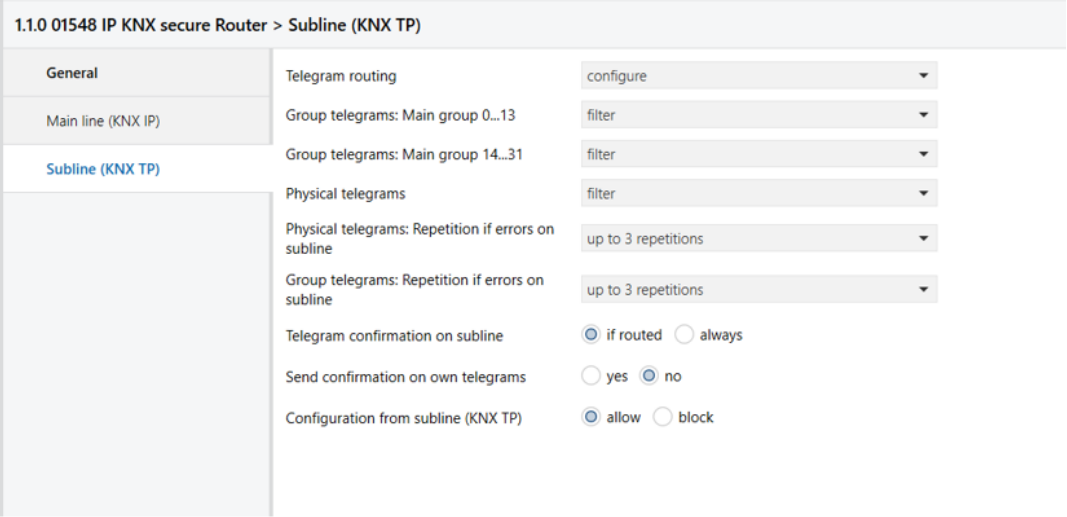
Table 10: Main Line (IP) Tab Parameter Settings

ETS Parameter	Settings [Default Parameter]	Comment
Telegram routing (Main line -> Subline)	Group: filter, Physical: block Group and Physical: filter Group: route, Physical: filter Group and Physical: route configure **[Group and Physical: filter]**	Routing of Physical Telegrams and Group Telegrams can be set to ‘block’ (no routing), ‘filter’ (telegrams are routed according to filtering) and ‘route’ (all telegrams are transmitted). To set parameters different as available here, use ‘configure’.
Group telegrams: Main group 0…13	transmit all (not recommended) block filter **[filter]**	Filtering of Group telegrams (with main groups 0…13) can be configured to route all telegrams, no telegrams, or only telegrams entered in the filter table.
Group telegrams: Main group 14…31	transmit all (not recommended) block filter **[filter]**	Filtering of Group telegrams (with main groups 14…31) can be configured to route all telegrams, no telegrams, or only telegrams entered in the filter table.
Physical telegrams	transmit all (not recommended) block filter **[filter]**	Filtering of Physical telegrams can be configured to route all telegrams, no telegrams, or only telegrams depending on their Individual Address.

5.3 Subline (KNX TP)

Setting “transmit all” is intended only for testing use. Please do not use for normal operation.

✓ If the parameter “Send confirmation on own telegrams” is set to “yes”, 01548 systematically sends an ACK on any own routed telegram. For example, since repeaters do not use filter tables, it is useful to have an ACK sent along with routed telegrams.



1.1.0 01548 IP KNX secure Router > Subline (KNX TP)

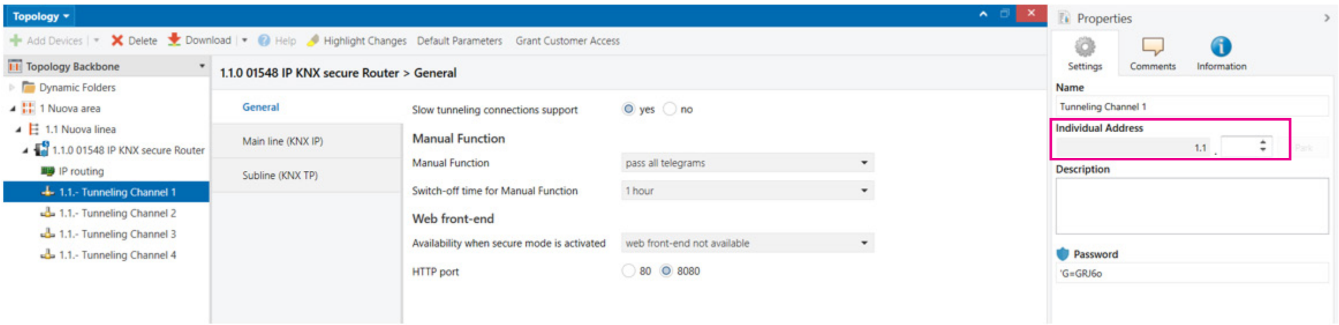
Telegram routing	configure
Group telegrams: Main group 0...13	filter
Group telegrams: Main group 14...31	filter
Physical telegrams	filter
Physical telegrams: Repetition if errors on subline	up to 3 repetitions
Group telegrams: Repetition if errors on subline	up to 3 repetitions
Telegram confirmation on subline	● if routed ○ always
Send confirmation on own telegrams	○ yes ● no
Configuration from subline (KNX TP)	● allow ○ block

Figure 15: Subline (KNX TP) Tab Parameters

Table 11: Subline (KNX TP) Tab Parameter Settings

ETS Parameter	Settings [Default Parameter]	Comment
Telegram routing (Subline -> Main line)	Group: filter, Physical: block Group and Physical: filter Group: route, Physical: filter Group and Physical: route configure **[Group and Physical: filter]**	Routing of Physical Telegrams and Group Telegrams can be set to ‘block’ (no routing), ‘filter’ (telegrams are routed according to filtering) and ‘route’ (all telegrams are transmitted). To set parameters different as available here, use ‘configure’.
Group telegrams: Main group 0…13	transmit all (not recommended) block filter **[filter]**	Filtering of Group telegrams (with main groups 0…13) can be configured to route all telegrams, no telegrams, or only telegrams entered in the filter table.
Group telegrams: Main group 14…31	transmit all (not recommended) block filter **[filter]**	Filtering of Group telegrams (with main groups 14…31) can be configured to route all telegrams, no telegrams, or only telegrams entered in the filter table.
Physical telegrams	transmit all (not recommended) block filter **[filter]**	Filtering of Physical telegrams can be configured to route all telegrams, no telegrams, or only telegrams depending on their Individual Address.
Physical telegrams: Repetition if errors on subline	no up to 3 repetitions one repetition **[up to 3 repetitions]**	After subline transmission error (e.g. due to missing receiver) Physical telegrams can be not repeated, be repeated only once, or be repeated for max. 3 times.
Group telegrams: Repetition if errors on subline	no up to 3 repetitions one repetition **[up to 3 repetitions]**	After subline transmission error (e.g. due to missing receiver) Group telegrams can be not repeated, be repeated only once, or be repeated for max. 3 times.
Telegram confirmation on subline	if routed always **[if routed]**	Either only routed telegrams to IP main line are confirmed by an ACK on the subline or each telegram on the subline is confirmed by an ACK.
Send confirmation on own telegrams	yes no **[no]**	Telegrams sent out to the subline can be confirmed by an added ACK.
Configuration from subline (KNX TP)	allow block [allow]	If blocked 01548 can only be configured via the main line.

5.4 IP (Secure) Tunneling Address Assignment



1.1.0 01548 IP KNX secure Router > General

Slow tunneling connections support ● yes ○ no

Manual Function

Manual Function: pass all telegrams

Switch-off time for Manual Function: 1 hour

Web front-end

Availability when secure mode is activated: web front-end not available

HTTP port ○ 80 ● 8080

Name: Tunneling Channel 1

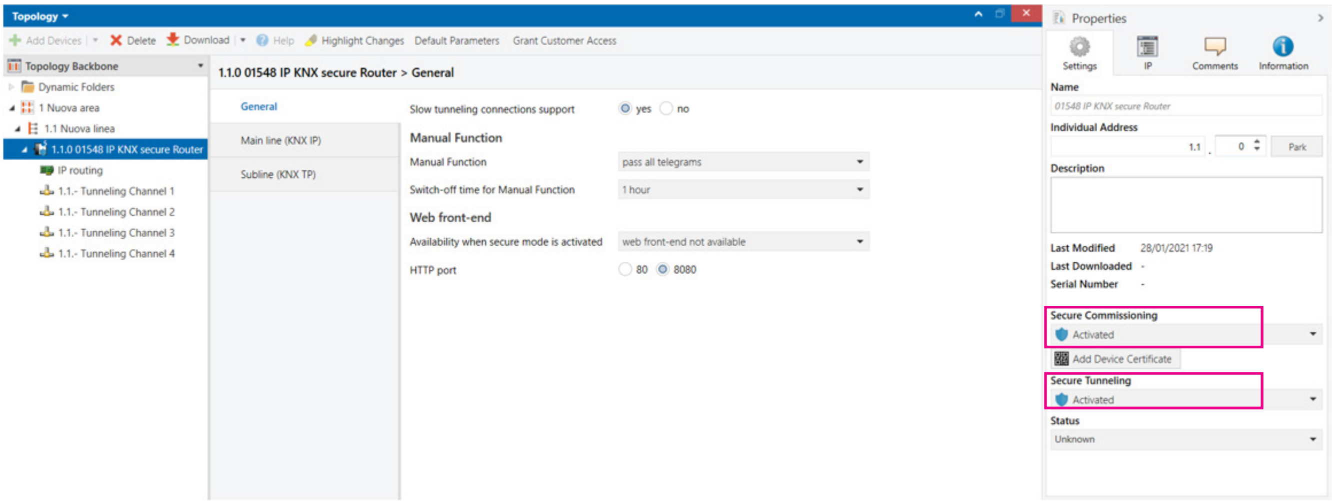
Individual Address: 1.1 .

Description

Password: 'G=GRJ6o

Figure 16: Configuring of IP (Secure) Tunneling Cannels

To use IP Secure Tunneling both Secure Commissioning and Secure Tunneling must be activated in the Properties window of 01548. Then, also the password protection option for each Tunneling Channel is available.



1.1.0 01548 IP KNX secure Router > General

Slow tunneling connections support ● yes ○ no

Manual Function

Manual Function: pass all telegrams

Switch-off time for Manual Function: 1 hour

Web front-end

Availability when secure mode is activated: web front-end not available

HTTP port ○ 80 ● 8080

Name: 01548 IP KNX secure Router

Individual Address: 1.1 . 0

Description

Last Modified: 28/01/2021 17:19

Last Downloaded: -

Serial Number: -

Secure Commissioning: Activated

Secure Tunneling: Activated

Status: Unknown

Figure 17: Activation of Secure Tunneling

6. Web Front-end

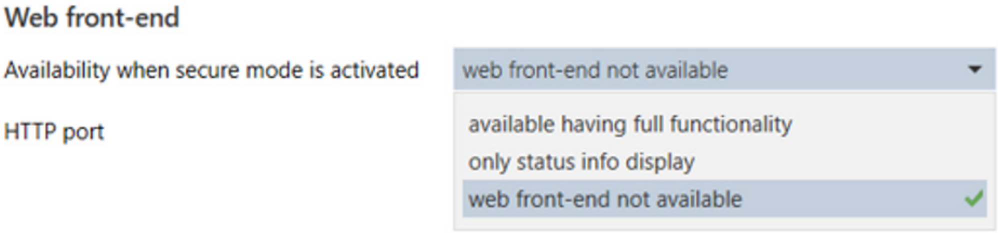
The web front-end can be used to read out 01548´s actual device parameters (HTTP port, IP address, MAC address, …), to update its firmware and set (additional) Individual Addresses for Tunneling. For identifying a certain 01548 in a KNX network, the Programming LED/Programming Mode can be remotely switched on and off without pressing the on-device Programming Button.

✓ To switch back from boot mode to normal operation it is necessary to run the firmware update procedure, then press abort, or wait for the 10 min timeout.

6.1 Protection of the 01548 Web Front-end

The web front-end can be used for remotely carrying out firmware updates, control functions and readout device settings. To guarantee full protection of an installation the web front-end must be set to “not available” during normal runtime operation.

To use the remote functions of the web front-end when Security is activated, it must be set to “available having full functionality”.



Web front-end

Availability when secure mode is activated: web front-end not available

HTTP port

available having full functionality
only status info display
web front-end not available ✓

Figure 18: ETS Parameter for Web Front-End Availability

When the web front-end is set to “only status info display”, remote control functions (Program Mode activation, Set Tunneling) and the update function are off. Only the informational readout is available.

✓ To ensure full protection of a secured installation the web front-end availability must be set to “web front-end not available” (default value).

✓ For reasons of efficient protection, it is strictly recommended not to use the “available having full functionality” option on a permanent basis.

6.2 Accessing the 01548 Web Front-end

There are three ways to access the 01548 web front-end. It can be accessed via Windows explorer directly, or by a web browser. For access via web browser either the IP address or the MAC address, together with the HTTP port, have to be known. How to use IP address and MAC address with the browser´s URL bar is described in the following.

✓ For access via web browser the correct HTTP port must be used.

✓ Factory default HTTP port is 8080.

6.2.1 via Windows Explorer

Due to UPnP discovery, 01548 appears in the local network window. A double click on the 01548 device opens the web front-end in the standard web browser.

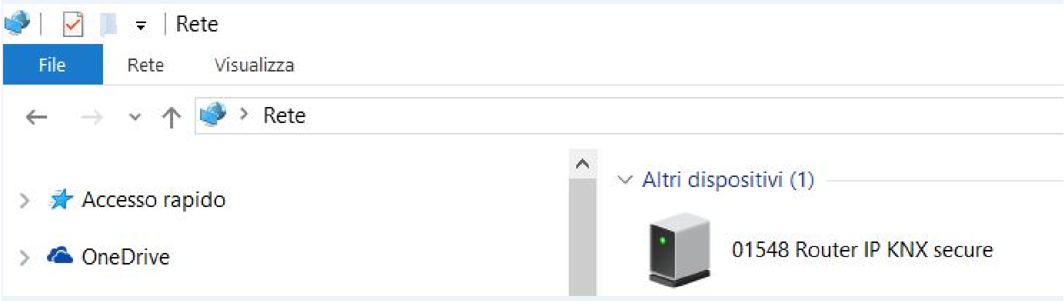
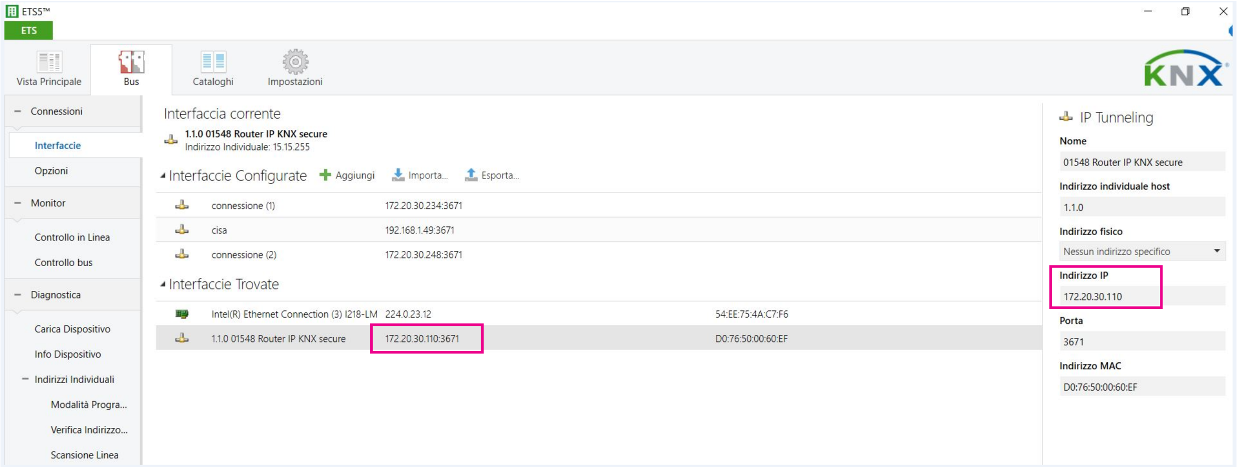


Figure 19: Windows Explorer showing 01548 (“KNX IP Secure Meda Coupler”)

6.2.2 via IP Address

When IP address and HTTP port are known, this information is sufficient to access the 01548 web front-end by a web browser. As 01548 can work also as ETS Current Interface, its IP address is shown under Discovered Interfaces in ETS. For 01548, the HTTP port can be set to 80 or 8080..



Interfaccia corrente

1.1.0 01548 Router IP KNX secure
Indirizzo Individuale: 15.15.255

Interfaccie Configurate

connessione (1)	172.20.30.234:3671
cisa	192.168.1.49:3671
connessione (2)	172.20.30.248:3671

Interfaccie Trovate

Intel(R) Ethernet Connection (3) I218-LM	224.0.23.12	54:EE:75:4A:C7:F6
1.1.0 01548 Router IP KNX secure	172.20.30.110:3671	D0:76:50:00:60:EF

IP Tunneling

Nome: 01548 Router IP KNX secure

Indirizzo individuale host: 1.1.0

Indirizzo fisico: Nessun indirizzo specifico

Indirizzo IP: 172.20.30.110

Porta: 3671

Indirizzo MAC: D0:76:50:00:60:EF

Figure 20: Identifying 01548´s IP address with ETS

According to 01548´s pre-set IP configuration (HTTP port, IP address and DHCP, respectively) in the URL bar has to be entered (without brackets):

http://[IP address]:[HTTP port]/

Example 1:

DHCP is not used. With the latest ETS download the IP address was set to 192.168.1.32 and HTTP port was set to 80. In the browser´s URL bar has to be entered “http://192.168.1.32:80/”.

Example 2:

01548 is used with its factory default setting. This means HTTP port is 8080 and DHCP is active. The DHCP server assigned the IP address 192.168.1.201. Then, in the browser´s URL bar has to be entered “http://192.168.1.201:8080/”.

6.2.3 via MAC Address

When NetBIOS is installed (by default on Windows systems), the MAC address that is printed on a label on the side of the 01548 housing (also shown in ETS list under Discovered Interfaces) can be used. Due to name resolution, it is mandatory to establish communication by Host name. Hereby, activation of NetBIOS is necessary.

Use the MAC address in the form of AA-BB-CC-XX-YY-ZZ and the pre-set HTTP port to be entered in the browser´s URL bar as described here (without brackets):

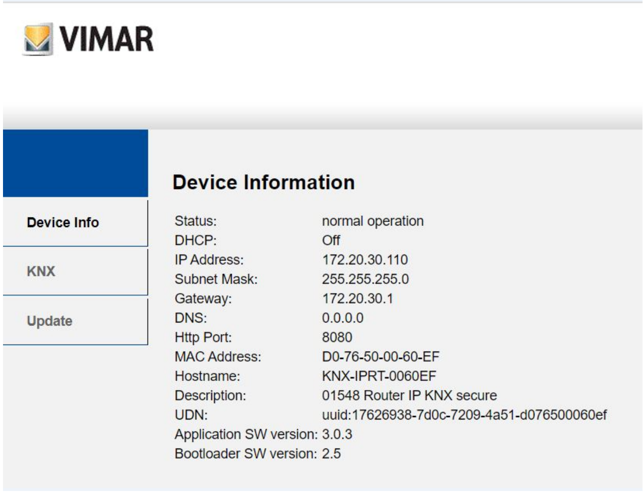
http://knx-iprt-[XXYYZZ]:[HTTP port]/

Example:

On the side of its housing, 01548 is labelled with MAC address D0-76-50-11-22-33 and the pre-set HTTP port is 8080. Then, in the web browser´s URL bar has to be entered “http://knx-iprt-112233:8080/”.

6.3 Device Info

After accessing the web front-end the Device Info tab appears. General information about current device parameters (addresses, names, software versions) is shown here.



Device Information

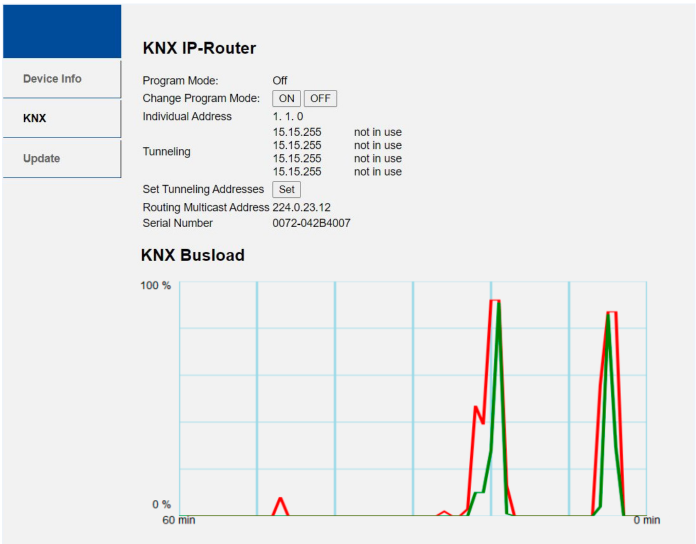
Status:	normal operation
DHCP:	Off
IP Address:	172.20.30.110
Subnet Mask:	255.255.255.0
Gateway:	172.20.30.1
DNS:	0.0.0.0
Http Port:	8080
MAC Address:	D0-76-50-00-60-EF
Hostname:	KNX-IPRT-0060EF
Description:	01548 Router IP KNX secure
UDN:	uuid:17626938-7d0c-7209-4a51-d076500060ef
Application SW version:	3.0.3
Bootloader SW version:	2.5

Figure 21: Device Info Tab

6.4 KNX

KNX-specific addresses are shown here. Settings can easily be checked. With a click on “On”, Programming Mode can be activated (same as a Programming Button press). Together with the Device Info tab, this function is useful to distinguish the regarded device (having a certain IP address, MAC address and serial number) from other similar network devices.

The Individual Address, the four Individual Addresses for Tunneling (additional tunneling addresses), routing multicast address, serial number of 01548 and a last-60-minutes KNX busload diagram (web browser must support SVG graphics) are visible. The red curve shows the maximum busload on TP and the green one shows the average busload on TP.



KNX IP-Router

Program Mode:	Off	
Change Program Mode:	ON OFF	
Individual Address	1. 1. 0	
Tunneling	15.15.255 15.15.255 15.15.255 15.15.255	not in use not in use not in use not in use
Set Tunneling Addresses	Set	
Routing Multicast Address	224.0.23.12	
Serial Number	0072-042B4007	

KNX Busload

Figure 22: KNX Tab

✓ For showing the busload diagram, the web browser must support SVG graphics.

For IP Tunneling, four Individual Addresses can be set. Setting a different Individual Address for every tunneling channel via the web front-end is relevant for ETS versions lower than 5.7. In this case, the first tunneling address must be set in the “Individual Address” field of the ETS Bus Connections window. With a click on “Set” the other ones consecutively follow the first one. Reason is tunneling channels using the same Individual Address can cause a reduction of usable connections. With the Set button they can be reassigned to have differing Individual Addresses.

✓ Before reassigning with using the Set button, it must be made sure these addresses do not exist in the project or the installation and clients do not loose connectivity due to reassignment.

✓ When Security is active, it is highly recommended to assign the additional Individual Addresses only by ETS projects and configuration downloads (see chapter “5.4 IP (Secure) Tunneling Address Assignment”).

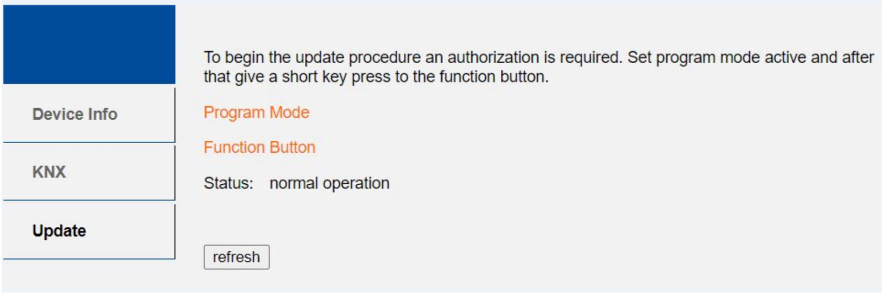
6.5 IP Firmware Update

Under the Update tab the 01548 firmware can be updated via IP i.e. the Ethernet network. The complete remote update process is described in following steps. During this process, 01548 enters its boot mode. Then LEDs 1, 2, 3 and 7 light as described in Table 5: LED Status Display for Firmware Update.

✓ If boot mode is already active only the web front-end instructions from step 3 to step 5 must be followed (refresh, request update).

To exit the boot mode, it is necessary to enter the Update tab of the web front-end. Then, either the firmware update has to be completed (like shown by steps 1 to 5) or the firmware update process has to be stopped by a click on the “Abort” button (see step 5, Figure 27). After that, 01548 restarts and continues with normal operation.

Step 1: Open the Update tab of the web front-end.



To begin the update procedure an authorization is required. Set program mode active and after that give a short key press to the function button.

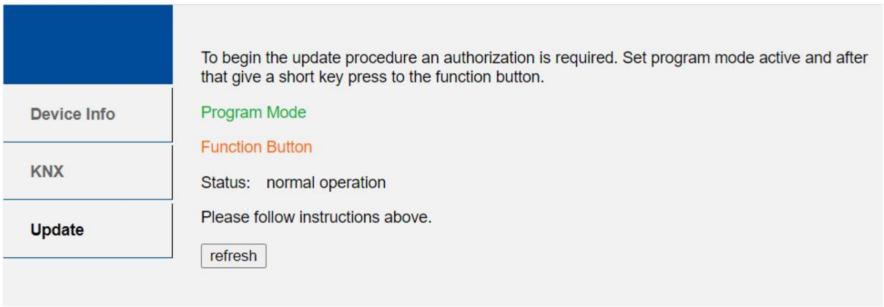
Program Mode

Function Button

Status: normal operation

Figure 23: Update Tab

Step 2: Activate Programming Mode (KNX tab or Programming Button).



To begin the update procedure an authorization is required. Set program mode active and after that give a short key press to the function button.

Program Mode

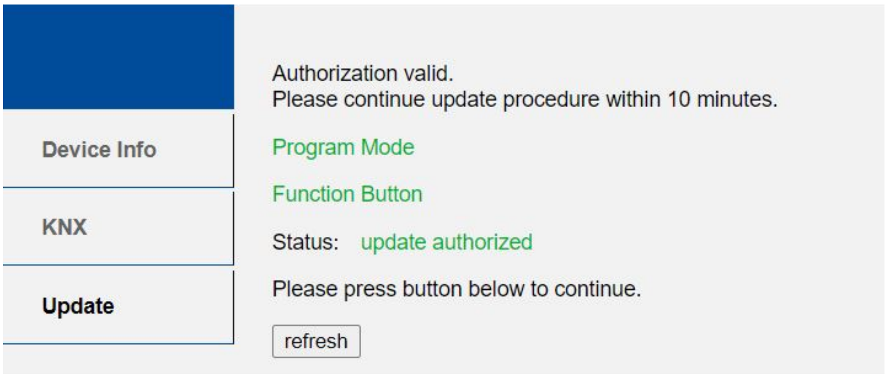
Function Button

Status: normal operation

Please follow instructions above.

Figure 24: Update Tab and activated Programming Mode

Step 3: After Programming Mode activation, give a short press to the Function Button. Then click on the “refresh” button.



Authorization valid.
Please continue update procedure within 10 minutes.

Program Mode

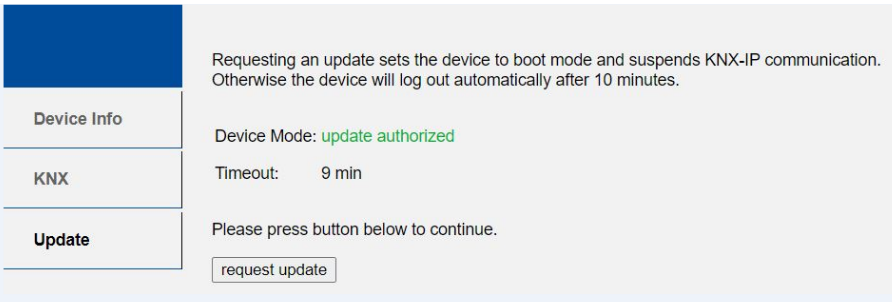
Function Button

Status: update authorized

Please press button below to continue.

Figure 25: Update Authorized

Step 4: When the „request update“ button appears it has to be pressed to select the update file and enter boot mode”.



Requesting an update sets the device to boot mode and suspends KNX-IP communication. Otherwise the device will log out automatically after 10 minutes.

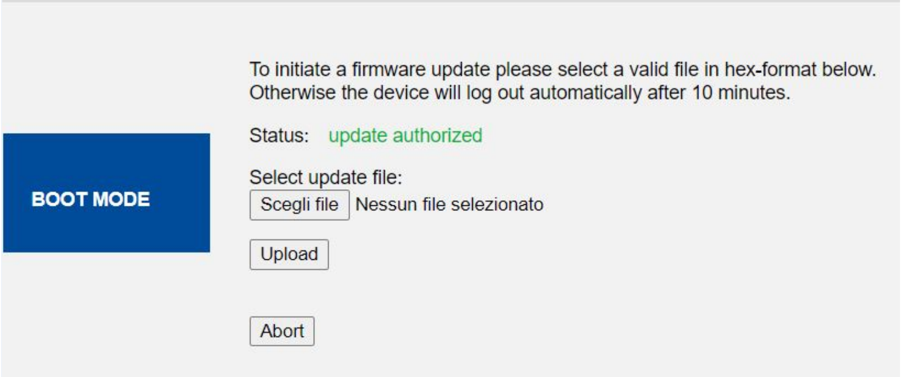
Device Mode: update authorized

Timeout: 9 min

Please press button below to continue.

Figure 26: Request Update

Step 5: The update file can be selected and uploaded. After that, the device exits boot mode and restarts. Clicking on the „Abort“ button cancels the firmware update procedure and the device exits boot mode.



To initiate a firmware update please select a valid file in hex-format below. Otherwise the device will log out automatically after 10 minutes.

Status: update authorized

Select update file:

Figure 27: Select Update File

7. Glossary

Step	Manual Function
ACK	An ACK is a positive IACK frame. If the sender detects an ACK, then the sender´s data has been received correctly, i.e. been successfully transmitted to the receiver.
Acknowledgement frames	Acknowledgment on the KNX Link Layer is also called Immediate ACK (IACK) in KNX jargon, presumably to differentiate it from other ack methods on the upper layers. In practice, IACK frames are used to confirm to a sender the transmitted data was correctly received by the receiver (ACK) or not (BUSY/NACK). Furthermore, a receiver cannot respond by sending back an IACK when a frame is damaged or incorrectly addressed (missing IACK).
BUSY	A BUSY is a negative IACK frame. If the sender detects a BUSY, then the receiver was not able to process the received frame. Consequently, the sender waits for a short period and re-sends the frame (up to three times).
Communication Object	same as Group Object
Extended Frames format	An extended frame has a maximum APDU length of 254 octets and a maximum length of 263 octets (incl. checksum).
Filtering	Filtering of telegrams can be accomplished according to the topology via Individual Addresses (Physical Telegrams) and according to filter tables for group communication (Group Telegrams) via Group Addresses.
Group Object	A data point in KNX is called a 'Group Object' or short an 'Object'.
Group Telegram	Group-oriented telegrams are named Group Telegrams. Filtering of Group Telegrams is accomplished according to the built-in filter tables for group communication.
IACK	see Acknowledgement frames
Individual Address	The Individual Address of a device defines the location of the device within the topology.
Long Telegrams	Long telegrams or long frames are telegrams having an APDU length that exceeds 15 octets. Long telegrams use the extended frame format.
NACK	A NACK is a negative IACK frame. If the sender detects a NACK, then the sender´s data has not been received correctly, i.e. successfully transmitted to the receiver. Consequently, the sender re-sends the frame (up to three times).
Physical Address	same as Individual Address
Physical Telegram	Individually addressed telegrams are named Physical Telegrams.
Repetition of telegrams	When there is no positive IACK on the TP line (e.g. NACK, BUSY, missing IACK), couplers usually repeat messages up to three times. For all MEC couplers, the number of repetition is configurable.
Security functions	For using ETS Security functions, a minimum ETS version is necessary. Security functions have been available since ETS version 5.7.2 (ETS Inside 1.4.0).
Short Telegrams	Short telegrams or short frames are telegrams having an APDU length that is not exceeding 15 octets. Short telegrams use the standard frame format.
Standard Frame format	A standard frame has a maximum APDU length of 15 octets and a maximum length of 23 octets (incl. checksum).

8. Technical

8.1 State of Delivery

Table 12: State of Delivery

General	
Individual Address	15.15.0
Individual Addresses for (Secure) Tunneling	• 15.15.241 • 15.15.242 • 15.15.243 • 15.15.244

IP configuration	
IP address assignment	DHCP/AutoIP
IP routing multicast address	224.0.23.12

IP (IP Main line to KNX TP Subline)	
Group telegrams (main group 0…13)	DHCP/AutoIP
Group telegrams (main group 14…31)	224.0.23.12
Physical telegrams	filter

KNX TP (KNX TP Subline to IP Main line)	
Group telegrams (main group 0…13)	filter (filter table is empty)
Group telegrams (main group 14…31)	route all
Physical telegrams	filter
Physical: Repetition if errors on subline (KNX TP)	up to 3 repetitions
Group: Repetition if errors on subline (KNX TP)	up to 3 repetitions
Telegram confirmations on subline (KNX TP)	if routed
Send confirmation on own telegrams	no
Configuration from subline (KNX TP)	allow

8.2 Datasheet

Table 13

Marking/Design	01548
Current consumption	< 20 mA
Connections	IP (line): RJ45 socket for 100 Mbit and 10 Mbit BaseT, IEEE 802.3 networks
	KNX TP line: KNX TP connector (red/black), screwless, for single-core cable Ø 0.6…0.8 mm
LED Display elements	State (IP and TP) Traffic (IP and TP) Routing (GA and PA) Programming LED
Control elements	Function Button Programming Button
Mounting	35 mm top-hat rail (TH35) according to IEC60715
Protection type	IP20 according to IEC60529
Pollution degree	2 according to IEC60664-1
Protection class	III according to IEC61140
Overvoltage category	II according to IEC60664-1
Approbation	KNX-certified according to ISO/IEC14543-3 and EN ISO 22510
CE Marking	In compliance with directives 2014/35/EU (LVD), 2014/30/EU (EMC), 2011/65/EU (RoHS)
Standards	EN50491-5-1, EN50491-5-2, EN50491-5-3, EN50581, EN60950-1, EN61000-6-2, EN61000-6-3, IEC60950-1
Voltage supply	KNX: 21…30V DC (SELV)
Housing color	Plastic PA66 housing, grey
Housing dimensions	H = 90 mm, W = 36 mm (2 modules), D = 71 mm
Mounting depth	64 mm
Weight	68 g
Operating temperature	-5…45 °C
Storage temperature	-20…60 °C
Ambient humidity	5…93 %, non-condensing

9. FAQ

- **I lost the Device Certificate. What can I do?**

  Take an ETS project where it is contained and open the Project Certificates Report.

- **I opened a new project in ETS and added the Device Certificate. But the download to the secure 01548 doesn´t work.**

  Either use Commissioning Password and Authentication Code from your former project or make a factory reset to set 01548´s tool key back to its FDSK.

- **I lost the Device Certificate and the password for the project where it was contained. What can I do?**

  Make a factory reset and use the device from then on only unsecured.

- **The firmware update finished successfully but the device doesn´t work.**

  To restart turn the power off and on again (dis-/reconnection of KNX TP line).

- **Is it Ok to connect and disconnect the Ethernet cable quickly?**

  No! Don't do this. Before reconnection, wait for a few seconds.

- **What shows the Programming LED if the Ethernet cable is not connected?**

  Similar to having no IP network available, the Programming LED is blinking red.

- **What can be a transmission error when LED 2 Bus State KNX TP is lighting red?**

  For every telegram sent out on KNX TP, 01548 waits for an acknowledgement on the TP line. When the receiver was busy (BUSY) or received an incorrect telegram (NACK) or 01548 didn´t receive a response (missing IACK), LED 2 is lighting red to show a transmission error exists on the line.

- **LED 2 Bus State KNX TP is continuously blinking green. Why?**

  This indicates 01548 is waiting for his firmware file download. For more information and how to switch back to normal operation please see chapter 6.5.

- **I disabled DHCP and assigned a correct IP configuration, but I cannot access the web front-end.**

  Reset the 01548 and try again. More information about changing the IP network configuration can be found in chapter 4.5.2.

- **I try to access the web front-end but I'm not successful. What can I do?**

  Make sure the web front-end is not deactivated and the URL bar entry matches the correct IP address together with the right HTTP port or use the MAC address in exactly the way as explained (chapter 6.2.3). Then refresh the browser and try again. Or check IP configuration via TP by ETS.

- **Is it possible to reach the web front-end when the device is in boot mode?**

  Yes, it is. The web front-end is accessible (chapter 6.5). When boot mode is active, the web front-end looks like illustrated in Figure 12. To exit boot mode the web front-end Update tab must be used or, after 10 min, it will be switched off automatically.

- **Is it possible to do a Factory Reset during the device is in boot mode?**

  No. LED 2 Bus State KNX TP will light up red when holding the Function button.

- **How can I find out the actual IP address of my 01548?**

  In the web front-end, the Device Info tab shows the actual IP address.

  When ETS can connect to 01548 via IP, the IP address is contained in the list of Discovered Interfaces.

  In Windows, with a right click on the network device the properties window can be opened. MAC address, IP address, HTTP port, serial number and version of firmware (application software version) can be found here.

- **How can I reach the web front-end in case I don´t know IP address and MAC address?**

  When 01548 cannot be accessed via the device list in the Windows network explorer (after refreshing the window), the actual IP address must be found at first. Then use Windows or the ETS like described in last question.

- **When can it be necessary to send IACKs on sent out messages?**

  For example, when a visualization is part of the installation and this visualization is not configurable by ETS.

- **I linked my IP router with an DSL router. Can I open a port on WAN side to connect to my installation from the Internet?**

  It should not be done to open a port at the WAN side. KNXnet/IP, even KNX IP Secure, is not designed for that. It is highly recommend using a VPN connection or making use of an available web or KNX IoT solution.

CE

VIMAR
Viale Vicenza, 14
36063 Marostica VI - Italy
www.vimar.com