TAPKO
TECHNOLOGIES GMBH

MEC IP
SECURE
IP TP MEDIA COUPLER
State
IP
Traffic
TP
GA
PA
Function
S
TP
IP
TAPKO
KNX
Program
KNX

MECip-Sec

KNX IP Secure Router

Technical & Application Description

This document is property of the company named at the last page.
Without written approval, it may not be reproduced or commercialized, distributed or presented to other individuals for commercial purpose.
Details and information contained within may be subject to change without notice. For the accuracy of the document no warranty is given.
All rights reserved.

Content

1 Product Description 5
1.1 Front Panel 6
1.2 LED Indication 7
1.3 LED Indication of Special Functions 8
1.4 Commissioning 9
1.5 Secure Commissioning 10
1.6 Important Notes 11
1.6.1 Installation and Commissioning 11
1.6.2 Mounting and Safety 11
1.6.3 Maintenance 11
1.7 Safekeeping of Device Certificate 12
1.8 Feature Summary 13

2 KNXnet/IP 14
2.1 IP Secure Tunneling 14
2.2 IP Secure Routing 14
2.3 IP Firmware Update 14

3 KNX Secure 15

4 Operational Description 16
4.1 IP Secure Router Application 16
4.2 IP Network 17
4.3 KNX Network Installation 18
4.4 Adding Device Certificate 19
4.5 Programming 21
4.5.1 Programming of Individual Address (and Application) 21
4.5.2 IP Configuration 22
4.6 Special Functions 24
4.6.1 Manual Function 24
4.6.2 Factory Reset 24
4.6.3 IP Firmware Update Request 25

5 ETS Database 26
5.1 General 26
5.2 Main Line (IP) 27
5.3 Subline (KNX TP) 28
5.4 IP (Secure) Tunneling Address Assignment 30

6 Web Front-end 31
6.1 Protection of the MECip-Sec Web Front-end 31
6.2 Accessing the MECip-Sec Web Front-end 32
6.2.1 via Windows Explorer 32
6.2.2 via IP Address 33
6.2.3 via MAC Address 34
6.3 Device Info 35
6.4 KNX 36
6.5 IP Firmware Update 38

7 Glossary 40

8 Technical 43
8.1 State of Delivery 43
8.2 Datasheet 44
8.3 Drawings 45

9 Legal Notice 46

10 FAQ 47

1 Product Description

MECip-Sec, the secured version of MECip, is a KNX IP Secure Router supporting both KNX Secure mechanisms, KNX IP Secure and KNX Data Secure. It provides a bi-directional data connection between KNXnet/IP main line and KNX TP subline, to interconnect TP lines or areas via an IP (Secure) Backbone. The Device Certificate utilization enables the usage of Security functions “Secure Commissioning”, “Secure Tunneling” and “IP Backbone Security”.

MECip-Sec can also work as a KNX IP Secure Interface for connecting KNX IP devices, a PC, or an Ethernet network to KNX TP. It establishes access to bus devices for commissioning, address assignment, setting parameters, visualization, protocolling, and diagnostics. With the ETS (or compatible commissioning tool) MECip-Sec works as the KNX programming interface. Connecting a personal computer to KNX TP can be done directly and via Ethernet. Four tunneling channels are available for IP (Secure) Tunneling. For every channel, an Individual Address (plus Security password) can be set.

MECip-Sec also features a comfortable web front-end for watching the busload history, to remotely control functions of MECip-Sec and to update its firmware via IP. With using this web front-end, it´s easy to identify MECip-Sec in an installation by remotely switching on the Programming LED. For reasons of protection, the web-frontend can be deactivated completely or be set to only allow showing actual settings and operational data.

MECip-Sec is suitable for the Extended Frame format and has no KNX communication objects for itself. Long telegrams are supported with up to 240 bytes APDU length. Filtering of telegrams can be configured for both Physical Telegrams and Group Telegrams. Operational modes, line states, telegram traffic, and filter states are shown at the duo-LED display. Telegram repetition (on TP side) is also configurable. For bus traffic reduction, special repetition/confirmation settings are provided.

It is possible to set programming of MECip-Sec and main line devices via the subline to inactive. To be more exact, the sub-to-main transmission of telegrams for configuring purpose can be switched off. This function can avoid unwanted access to devices (and their configurations) from a subline (that may be located outside of a building).

The configurable Manual Function for short-time filter switch-off can ease commissioning and troubleshooting. For example, “transmit all group telegrams” can be activated by a single on-device button press. After the pre-set time period, MECip-Sec then switches automatically back to normal operation.

1.1 Front Panel

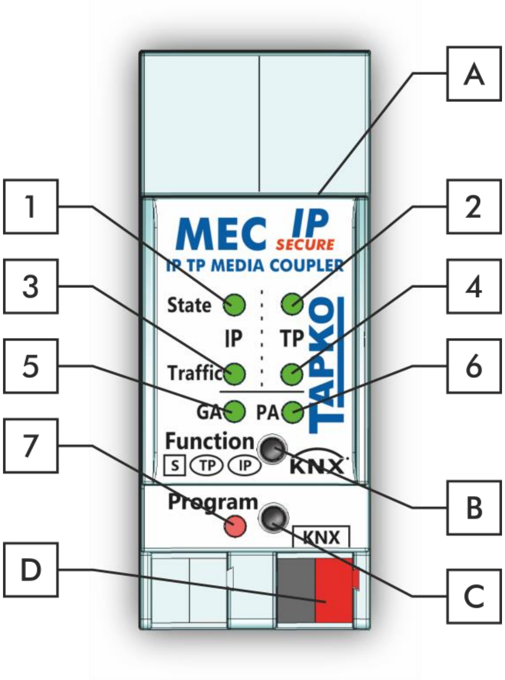

A
1
2
3
4
5
6
7
B
D
C
MEC IP SECURE
IP TP MEDIA COUPLER
State
IP
TP
Traffic
GA
PA
Function
S
TP
IP
KNX
TAPKO
Program
KNX

Figure 1: Front View

Table 1: Front Panel Elements

LEDs		Buttons / Connectors	
1	State IP (Main line)	A	Ethernet Connector
2	Bus State KNX TP (Subline)	B	Function Button
3	Telegram Traffic IP (Main line)	C	Programming Button
4	Telegram Traffic KNX TP (Subline)	D	KNX TP Connector
5	Group Address Routing*		
6	Individual (Physical) Address Routing		
7	Programming LED		

* only group telegrams with main groups 0...13

1.2 LED Indication

Following table gives a general description of the LED display indication intended for normal operation. Constellations of LED lighting during active special functions are further 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

1.3 LED Indication of Special Functions

During an active special function, only LEDs described here are lighting. Other LEDs are off.

Table 3: LED Status Display for Manual Function

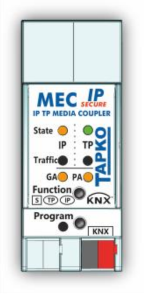
Number	LED	Color	Comment	
1	**State IP**	orange	lights red if not connected	
2	**Bus State KNX TP**	green		
5	**Group Address Routing**	green: filter orange: route all red: block all		
6	**Individual Address Routing**			

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

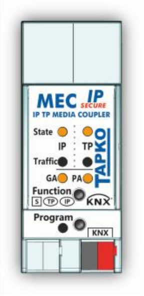
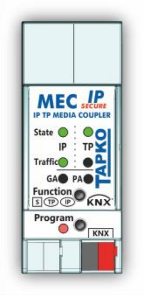
Number	LED	Color	Comment	
1	**State IP**	orange	lights red if not connected	
2	**Bus State KNX TP**	orange		
5	**Group Address Routing**	green: filter orange: route all red: block all		
6	**Individual Address Routing**			

Table 5: LED Status Display for Firmware Update

Number	LED	Color	Comment	
1	**State IP**	green	blinking, then 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 Secure Commissioning requires the Device Certificate
- Activation of Secure Commissioning requires a minimum ETS version (see also Security functions)

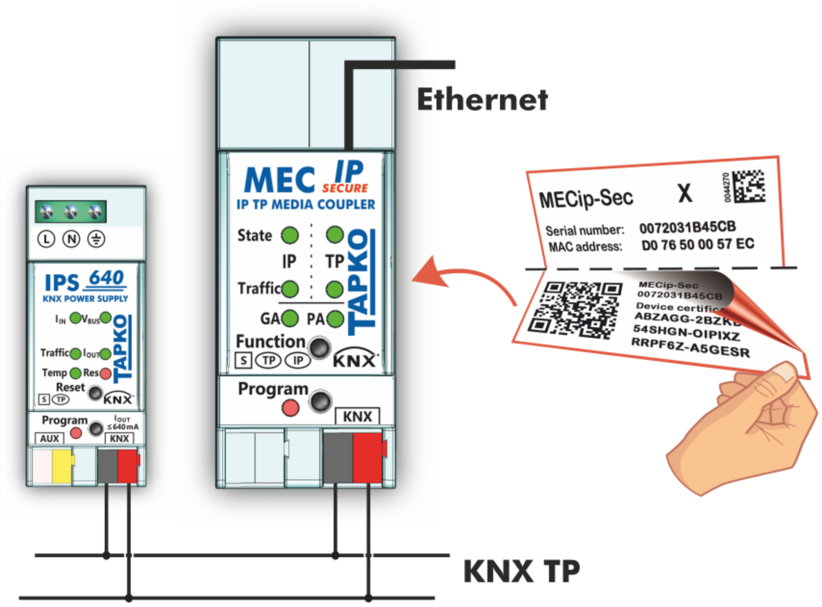

Ethernet
MEC IP SECURE
IP TP MEDIA COUPLER
State
IP
TP
Traffic
GA
PA
Function
S
TP
IP
KNX
TAPKO
Program
KNX
IPS 640
KNX POWER SUPPLY
L N
I_IN
V_BUS
Traffic
I_OUT
Temp
Res
Reset
Program
I_OUT ≤640mA
AUX
KNX
MECip-Sec
X
0044270
Serial number: 0072031B45CB
MAC address: D0 76 50 00 57 EC
MECip-Sec
0072031B45CB
Device certific
ABZAGG-2BZKD
54SHGN-OIPIXZ
RRPF6Z-A5GESR
KNX TP

Figure 2: Connection Scheme

To start a secured configuration download, Secure Commissioning must be activated in the ETS project before. Without activation, MECip-Sec is working as plain device and will behave like MECip (without supporting KNX Secure).

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

1.5 Secure Commissioning

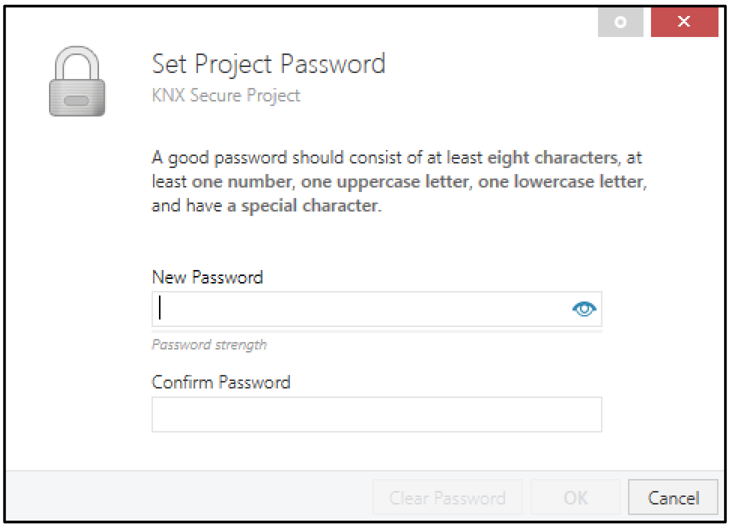
Before the secured download of a configuration setting and/or the Individual Address can start, the individual Device Certificate of MECip-Sec must have been added to the ETS project. To be able to add it, the ETS project must be password-protected.

A secured 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 a password-protected ETS project.

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



Set Project Password
KNX Secure 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 a KNX Secure product. To keep the product fully 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

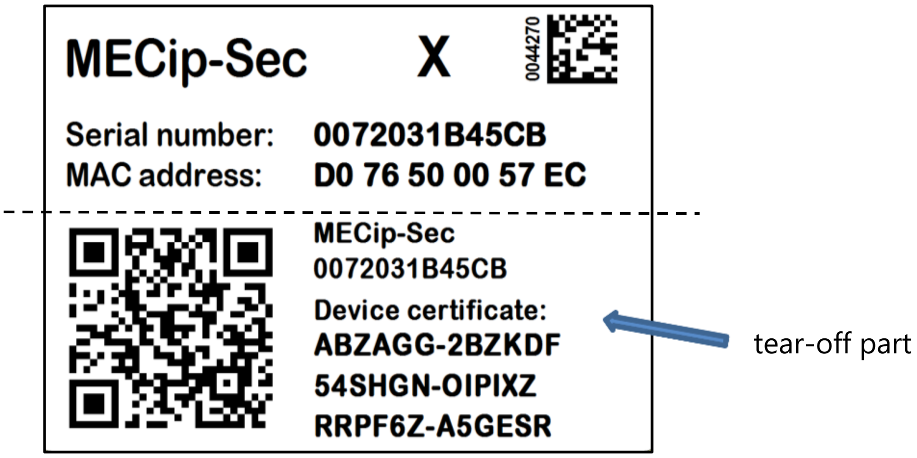
- For mounting use an appropriate equipment according to IEC60715
- Installation on a 35 mm DIN rail (TH35)
- Connect the KNX bus line as for common KNX bus connections with a KNX bus cable, to be stripped and plugged into a KNX TP connector
- Do not damage electrical insulations during connecting
- 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 label consists of two parts. The upper part must remain on the housing, for identifying the device. The lower one is the tear-off part. This part contains the Device Certificate and should be removed from the device for keeping the information at a safe place after commissioning.



MECip-Sec **X** 0044270

Serial number: **0072031B45CB**
MAC address: **D0 76 50 00 57 EC**

MECip-Sec
0072031B45CB
Device certificate:
ABZAGG-2BZKDF
54SHGN-OIPIXZ
RRPF6Z-A5GESR

tear-off part

Figure 4: Device Certificate Label

After adding the Device Certificate 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 on 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 (that contained the certificate) is lost, too, a Secure device cannot be set to active secure mode anymore! Consequently, Security cannot be activated within a new ETS project. In this case, to reprogram a Secure device with active secure mode, a Reset has to be carried out and the Secure device can only be used unsecured, as “plain” device, from then.

1.8 Feature Summary

- Device Certificates guarantee only authorized persons can have access to MECip-Sec.
- When the ETS “Secure Commissioning” function is active, configuration data is downloaded only in encrypted KNX Data Secure format.
- Activation of “IP Backbone Security” for protection of IP routing.
- Configuring MECip-Sec plus devices on the main line from the subline can be switched off. (This is very useful, when there are sublines that bear a high risk of being misused.)
- MECip-Sec supports long telegrams with up to 240 bytes APDU length. (Both product series, the MEC couplers and UIM interfaces, can process long messages e.g. for energy metering applications and visualization purposes, and support Extended Frames.)
- The great advantage, when MECip-Sec replaces a common TP line/area coupler is using a KNX IP line as a fast KNX backbone instead of a TP backbone.
- MECip-Sec 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 data throughput and decrease high bus traffic are featured.
- IACK sending on sent out messages is configurable.
- Repetition is configurable for both Physical Telegrams and Group Telegrams.
- To ease commissioning, troubleshooting and fast on-site diagnostics, normal run-time filtering can temporarily be suspended by a single Function button press. Other lines can be fully accessed without having to carry out additional ETS downloads. Switching back to normal run-time filter settings after suspension period expiry is automatic (see Manual Function). This avoids forgetting to reactivate the settings for normal filtering.
- UPnP Discovery enables discovering MECip-Sec within the IP network.
- ETS recognizes MECip-Sec 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 60 min busload history diagram can be watched.
- For Security, the web front-end can fully be disabled or be set to display only status info.
- MECip-Sec 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 specifications, KNX telegrams are transmitted encapsulated in IP packets, and Ethernet networks can be used to route and tunnel KNX telegrams.

IP routers and IP interfaces are an excellent alternative to TP line/area couplers and USB data interfaces. KNX IP routers are similar to TP line couplers, but make use of the KNXnet/IP communication protocol. They connect the IP communication medium to TP, instead of connecting two TP lines. According to this, a TP backbone can completely be replaced by an Ethernet based IP backbone. It is even possible to integrate end devices directly via IP.

2.1 IP Secure Tunneling

KNXnet/IP provides KNX connection via IP Tunneling. Such point-to-point IP Tunneling connections usually are used to connect clients like the ETS or supervisory systems to the KNX installation. On activation of “Secure Tunneling”, these then called IP Secure Tunneling connections become secured. This means the data communication of every channel is encrypted and the possibility is offered to protect the single channels by passwords.

2.2 IP Secure Routing

Regarding KNX topology, KNX TP lines and areas can be connected by an Ethernet/IP network, what then is called a KNX IP (backbone) line. KNX IP media couplers hereby transfer the KNX data from TP to IP and vice versa, and are often called KNX IP routers for this reason. For the data communication on KNX IP, or to be more exact, for the communication between KNX IP devices, KNXnet/IP is the fundamental protocol for IP Routing. When IP Security is active, the IP Routing specification is replaced by the IP Secure Routing specification and KNX IP communication becomes entirely encrypted according to the security concept KNX Secure. The KNX Secure part, that is relevant for IP, is called KNX IP Secure.

2.3 IP Firmware Update

To provide updating the firmware remotely via IP, MECip-Sec has a bootloader functionality integrated. This function is called IP Firmware Update and can be executed in the web front-end. The download process for rewriting the program memory content is independent from ETS and replaces both communication stack and application software.

3 KNX Secure

KNX devices that support KNX Secure are able to use a special protection basing on telegram encryption. Also, access to the device for configuring is protected and limited to the user that knows its Device Certificate. The Device Certificate is a device-specific protection code that is enclosed with the device on delivery.

To make use of the KNX Secure protection, every KNX Secure device supports a secure mode. When its secure mode is on, commissioning, configuring and runtime communication run in an encrypted manner so that the device is shielded against intruder attack and unwanted manipulation. For activation, the Device Certificate is necessary (see chapter 1.5 Secure Commissioning). Only when secure mode is active, the KNX Secure device is able to read and send encrypted telegrams. When secure mode is off, the Secure device behaves like a common KNX device without KNX Secure support (also called plain KNX device). KNX Secure devices in secure mode and plain devices can´t be combined by the same group object, but it is possible to have a mixed installation consisting of secured devices and plain devices.

Mixing unsecure and secure communication on the same group address is impossible. Also, a mix of KNX IP Secure couplers in secure mode and plain KNX IP Secure couplers cannot be configured when IP Backbone Security is on.

Encrypted KNX telegrams that are processed by secured devices can be distinguished between telegrams for KNX IP Secure and telegrams for KNX Data Secure:

- KNX IP Secure can only be applied upon the KNX IP medium. KNX Secure telegrams are sent as encrypted IP Secure frames (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, better say group communication for one or more certain group objects is encrypted. Due to an individual security key, only end devices having identical Group Addresses can encrypt/decrypt the telegrams of their secured group.

For programming a KNX Secure device, ETS must know its FDSK (Factory Default Setup Key) and its serial number. But it is not necessary entering FDSK or serial number. ETS retrieves this information from the Device Certificate, a device-specific 36-character code containing both serial number and FDSK. Serial number and FDSK cannot be modified. After adding a KNX Secure device plus Device Certificate to the ETS project, ETS automatically sets the project-specific Tool Key that is used for programming from then. This Tool Key cannot be modified and only be deleted by a device reset (see chapter 4.6.2 Factory Reset). After the reset, ETS uses the registered FDSK to get access to the device to program a new Tool Key.

4 Operational Description

In KNX network installations, MECip-Sec is used as KNX IP line/area coupler to connect KNX IP and KNX TP (see also chapter 2.2 IP Secure Routing). It can be used in plain mode, without activation of Security, and in ETS projects where Security is set to active. After connecting to KNX TP, MECip-Sec operates with its default settings. For KNX IP routers, only Individual Addresses x.y.0 can be set. Setting the correct Individual Address is necessary for proper telegram transmission and functioning within the installation.

4.1 IP Secure Router Application

During normal operation, MECip-Sec reacts in accordance with its filter settings. When MECip-Sec receives telegrams that use Individual Addresses as destination (for example during commissioning), it compares the Individual Address of the receiver with its own Individual Address and decides on that whether it has to route the telegrams or not. When MECip-Sec receives telegrams that use group addresses as destination, only the telegrams whose group addresses are entered in the filter table are routed.

If a telegram is routed by MECip-Sec to TP 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 parameter „Repetitions if errors …“, this function can be configured for the KNX TP line and both kinds of telegrams. It is recommended to use the default parameter setting.

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

4.2 IP Network

In the IP network, MECip-Sec sends and receives telegrams 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. Multicast IP address 224.0.23.12 and port 3671 are the defined values for KNXnet/IP by KNX Association in conjunction with IANA.

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. It is recommended to change this address only when it becomes necessary due to the environment.
- 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 these additional Individual Addresses can be found in chapter 5.4 IP (Secure) Tunneling Address Assignment.

4.3 KNX Network Installation

For MECip-Sec´s usage in a KNX installation, one of the available Individual Addresses must be chosen. Having set an Individual Address (x.y.0), a TP Line is connected to KNX IP. To connect a TP Area to the IP Backbone, an area coupler address (x.0.0) must be set.

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.

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

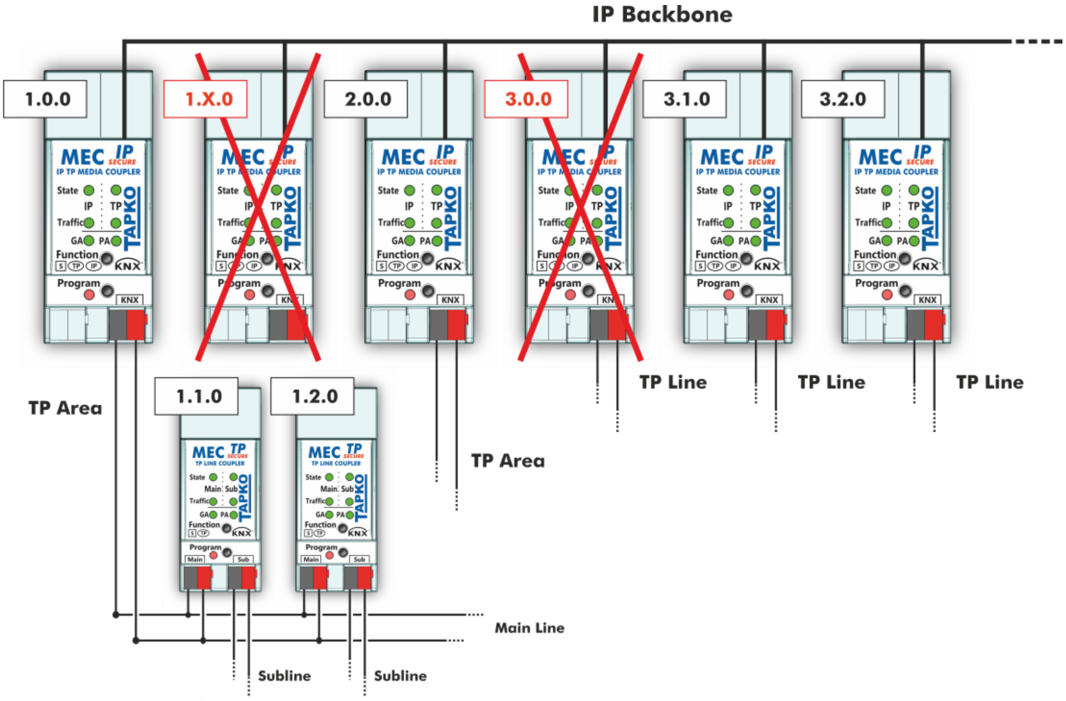


Figure 5: MECip-Sec Network Topology

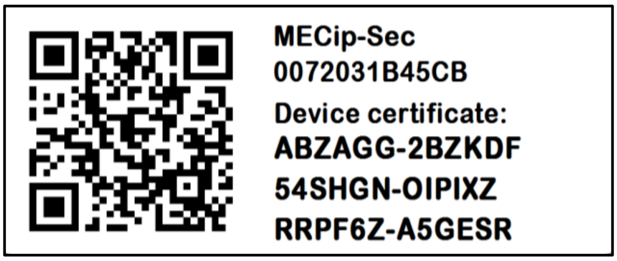
Example: If a KNX IP router with address 1.0.0 already exists on the backbone no KNX IP router with address 1.x.0 can be added here. Even if no line coupler with address 1.1.0 exists on the subline of the 1.0.0 router. Vice versa, when line couplers with addresses 3.x.0 already exist in an installation,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

4.4 Adding Device Certificate

The Device Certificate can be found printed on a side label on the housing. Every KNX Secure device uses its own Device Certificate. Entering this Device Certificate in ETS is mandatory before activating or using KNX Security functions.

Please also follow the advice on handling the tear-off part of the side label in chapter 1.7 Safekeeping of Device Certificate.

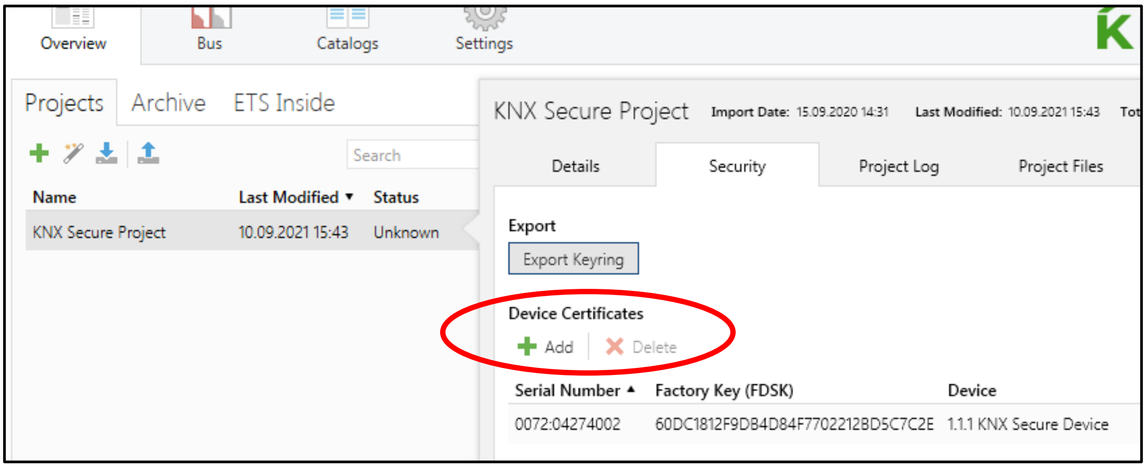
The Device Certificate can be entered manually and by taking a webcam picture of the QR code that is additionally contained on the tear-off part of the Device Certificate side label.



MECip-Sec
0072031B45CB
Device certificate:
ABZAGG-2BZKDF
54SHGN-OIPIXZ
RRPF6Z-A5GESR

Figure 6: Tear-off Part of the Device Certificate Side Label

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



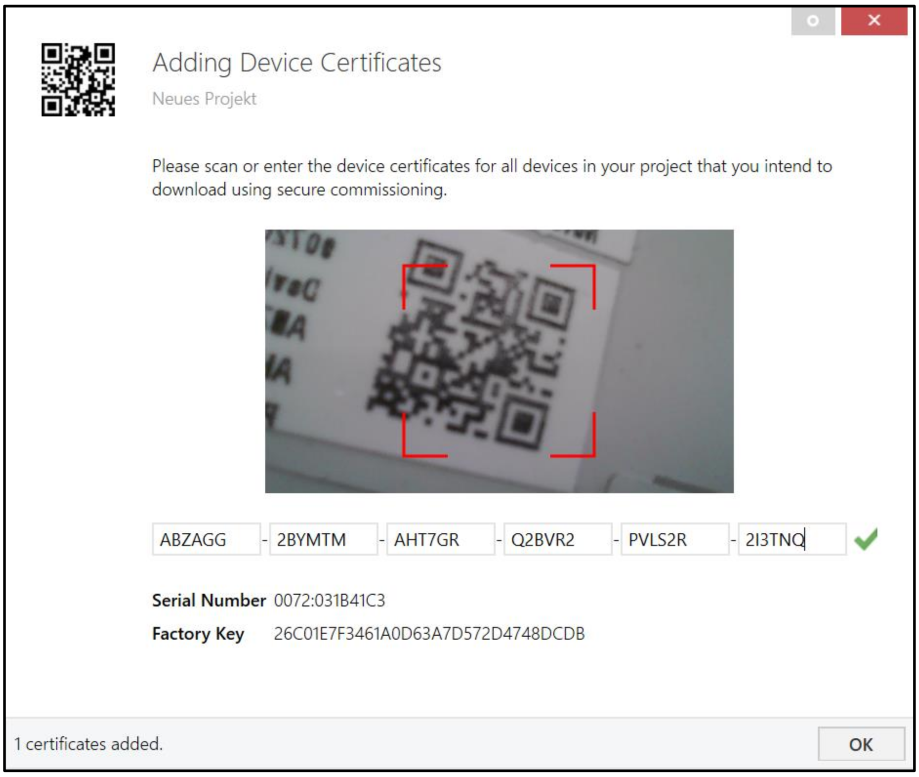
Name	Last Modified ▾	Status
KNX Secure Project	10.09.2021 15:43	Unknown

KNX Secure Project **Import Date:** 15.09.2020 14:31 **Last Modified:** 10.09.2021 15:43 **Tot**

Serial Number ▴	Factory Key (FDSK)	Device
0072:04274002	60DC1812F9DB4D84F7702212BD5C7C2E	1.1.1 KNX Secure Device

Figure 7: Device Certificate List

When the Device Certificate list doesn´t contain the Device Certificate of a certain Secure device, on starting the Secure download into this device following window appears. Then, the QR code must be scanned, or alternatively, the 36-character code of the Device Certificate must be entered manually to continue.



Adding Device Certificates

Neues Projekt

Please scan or enter the device certificates for all devices in your project that you intend to download using secure commissioning.

ABZAGG - 2BYMTM - AHT7GR - Q2BVR2 - PVLS2R - 2I3TNQ ✓

Serial Number 0072:031B41C3

Factory Key 26C01E7F3461A0D63A7D572D4748DCDB

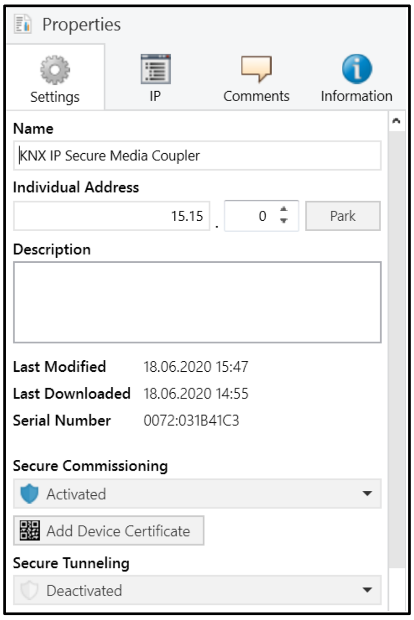
1 certificates added.

Figure 8: Adding Device Certificate

4.5 Programming

4.5.1 Programming of Individual Address (and Application)

The Individual Address (IA) can be assigned to MECip-Sec by setting the desired address in the properties window of ETS. After downloading it into the device, MECip-Sec can be addressed and identified by its new Individual Address.



Name
KNX IP Secure Media Coupler

Individual Address
15.15 . 0

Description

Last Modified 18.06.2020 15:47
Last Downloaded 18.06.2020 14:55
Serial Number 0072:031B41C3

Secure Commissioning
Activated

Secure Tunneling
Deactivated

Figure 9: ETS Properties Window

To download the Individual Address 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 on. Once the download is started in ETS, the Programming Button has to be pressed. After that, the new Individual Address becomes stored in the memory of the device.

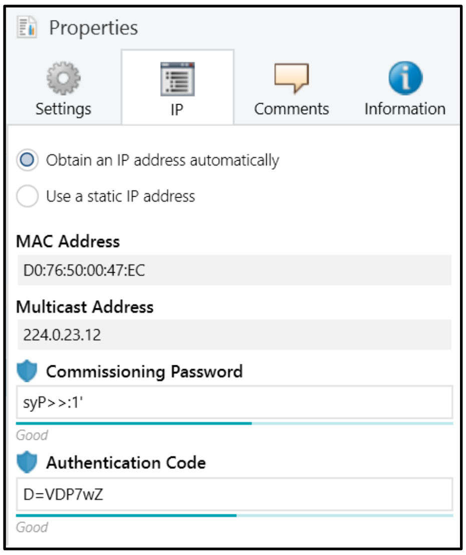
To program devices of a line different to which the device used as ETS Current Interface is connected, a correct topology is mandatory.

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 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.

4.5.2 IP Configuration

The IP configuration of MECip-Sec 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 configuring IP networks, please ask your local network administrator.



● Obtain an IP address automatically
○ Use a static IP address

MAC Address
D0:76:50:00:47:EC

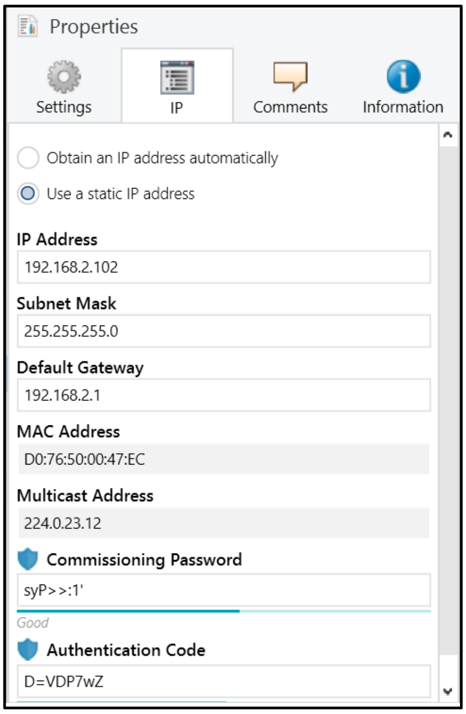
Multicast Address
224.0.23.12

Commissioning Password
syP>>:1'
Good

Authentication Code
D=VDP7wZ
Good

Figure 10: 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.



○ Obtain an IP address automatically
● Use a static IP address

IP Address
192.168.2.102

Subnet Mask
255.255.255.0

Default Gateway
192.168.2.1

MAC Address
D0:76:50:00:47:EC

Multicast Address
224.0.23.12

Commissioning Password
syP>>:1'
Good

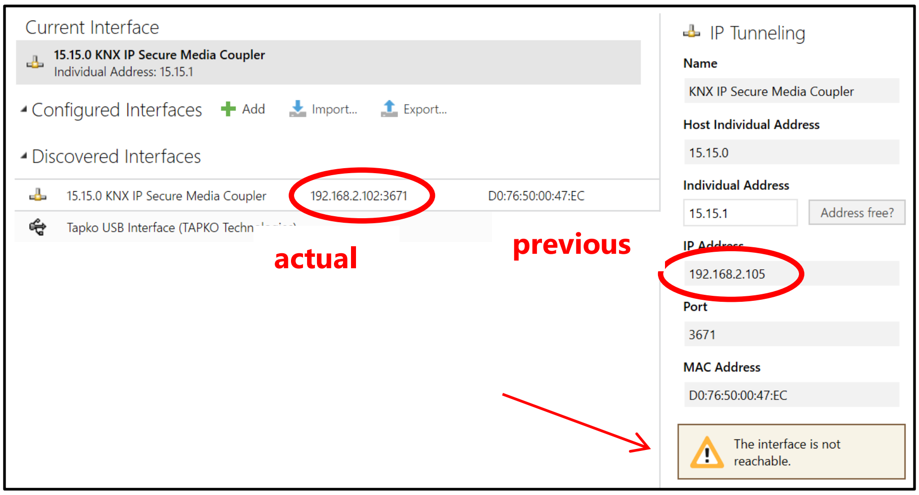
Authentication Code
D=VDP7wZ

Figure 11: 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 MECip-Sec 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). To be more exact, the previous IP Address is still visible in the IP Tunneling window and ETS shows the Current Interface is not reachable. MECip-Sec (containing the actualized IP address) now is listed under Discovered Interfaces and must be selected as new Current Interface.



15.15.0 KNX IP Secure Media Coupler
Individual Address: 15.15.1

15.15.0 KNX IP Secure Media Coupler 192.168.2.102:3671 D0:76:50:00:47:EC
Tapko USB Interface (TAPKO Techn

Name: KNX IP Secure Media Coupler
Host Individual Address: 15.15.0
Individual Address: 15.15.1
IP Address: 192.168.2.105
Port: 3671
MAC Address: D0:76:50:00:47:EC

The interface is not reachable.

Figure 12: IP Address of the Current Interface before and after Actualization

4.6 Special Functions

The Function Button activates MECip-Sec´s special functions Manual Function and Factory Reset. With the Manual Function, the device switches to a special filter setting and with the Factory Reset, MECip-Sec can be reset to its manufacturer default state. Pressing the Function Button is also necessary during the Firmware Update process. The active special function status 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 1 indicates the status. 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 MECip-Sec without filtering. When the Switch-off time has elapsed, MECip-Sec 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 filter parameter settings plus filter table entries become 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

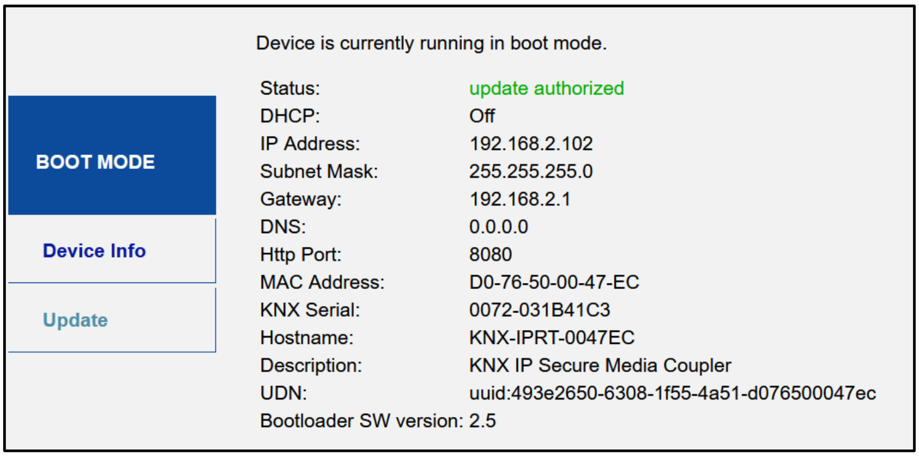
A long press (≈ 15 sec) of the Function Button soon followed by a short press (≈ 3 sec) executes the Factory Reset. After the first press, the LED display lights like described in Table 4: LED Status Display for Factory Reset after first Function Button Press. After the second press, all parameters (incl. Individual Address) will be set to factory default. The Tool Key, if set, becomes deleted and the FDSK becomes the relevant key for configuring again. 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

To start the Firmware Update download process, a short press on the Function Button is necessary during Programming Mode is active. After a click on the “request update” button in the web front-end, MECip-Sec switches to its boot mode (see chapter 6.5 Firmware Update) and ‘Status: update authorized’ is indicated.



Device is currently running in boot mode.

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 13: Authorized Update Request

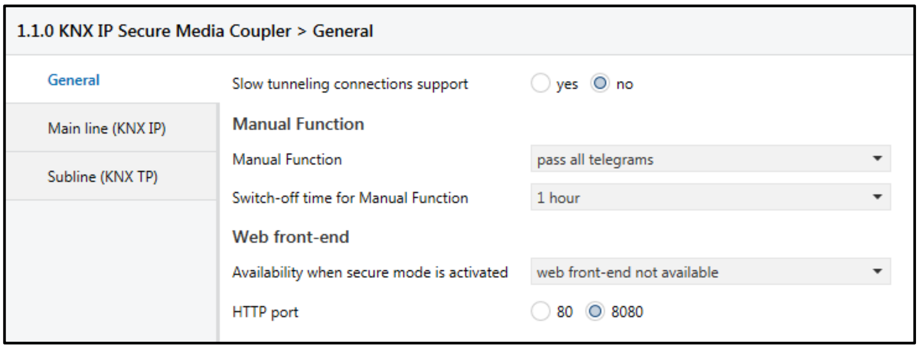
Table 8: Activation of Firmware Update

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

For UDP, support of slow tunneling connections can be activated.



1.1.0 KNX IP Secure Media Coupler > 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

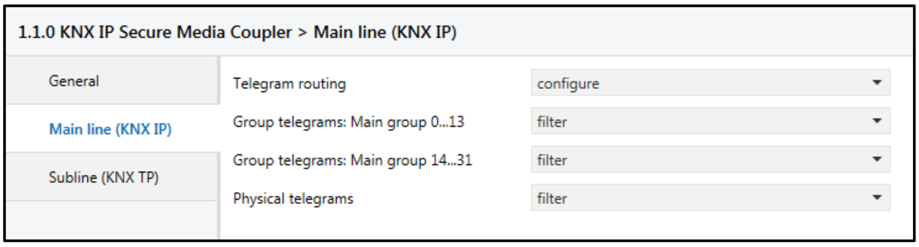
Figure 14: General Tab Parameters

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 set to fully available (read/write), to available with limited usage (only readout) 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 this setting for normal operation.



1.1.0 KNX IP Secure Media Coupler > 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 15: Main Line (IP) Tab Parameters

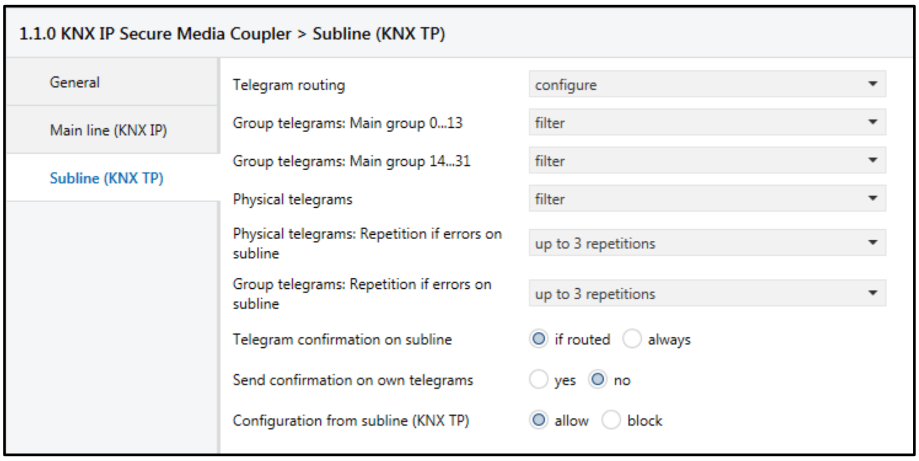
Table 10: Main Line (IP) Tab Parameter Settings

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 telegram routing 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 according to their Individual Address.

5.3 Subline (KNX TP)

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

If the parameter “Send confirmation on own telegrams” is set to “yes”, MECip-Sec 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 KNX IP Secure Media Coupler > 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 16: Subline (KNX TP) Tab Parameters

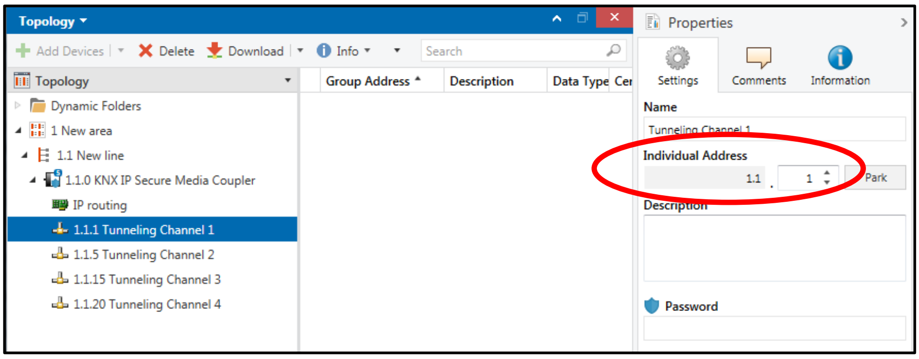
Table 11: Subline (KNX TP) Tab Parameter Settings

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 telegram routing 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 according to their Individual Address.

ETS Parameter	Settings [Default Parameter]	Comment
Physical telegrams: Repetition if errors on subline	no up to 3 repetitions only 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 only 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]**	'Block' means MECip-Sec can only be configured from its main line side and configuring devices on main line (and behind) from the subline side is blocked.

5.4 IP (Secure) Tunneling Address Assignment

MECip-Sec provides four channels for connections via IP (Secure) Tunneling. To establish such IP Tunneling connection, a free Individual Address must be assigned to the Tunneling Channel. To do this, the Topology window must be used. A click on the Tunneling Channel opens the channel´s Properties window for configuring. Then, up to four Individual Addresses of the subline can be set.

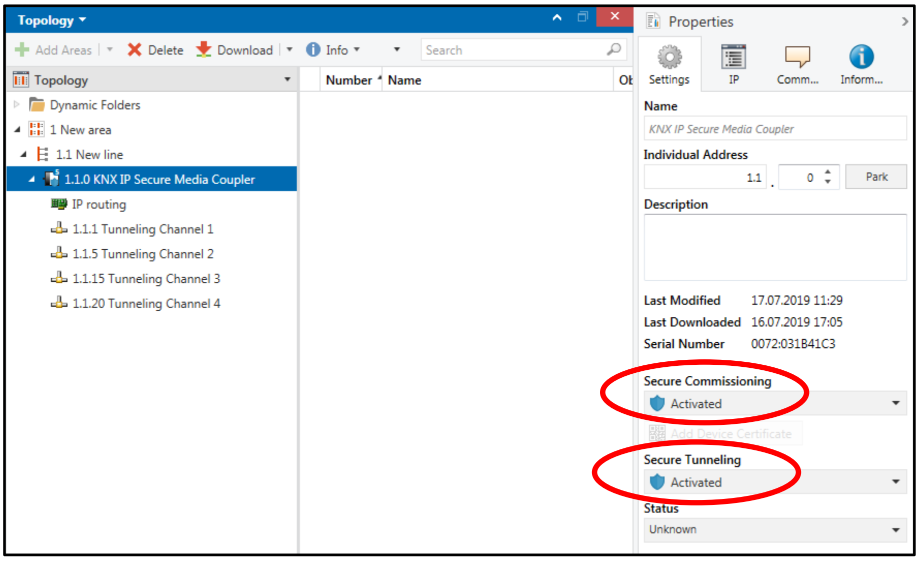

Topology
Add Devices
Delete
Download
Info
Search
Topology
Group Address
Description
Data Type
Properties
Settings
Comments
Information
Dynamic Folders
1 New area
1.1 New line
1.1.0 KNX IP Secure Media Coupler
IP routing
1.1.1 Tunneling Channel 1
1.1.5 Tunneling Channel 2
1.1.15 Tunneling Channel 3
1.1.20 Tunneling Channel 4
Park
Description
Password

Name: Tunneling Channel 1

Individual Address: 1.1 . 1

Figure 17: 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 MECip-Sec. After that, the passwords for protection of each Tunneling Channel can be entered (or changed).


Topology
Add Areas
Delete
Download
Info
Search
Topology
Number
Name
Properties
Settings
IP
Comm...
Inform...
Dynamic Folders
1 New area
1.1 New line
1.1.0 KNX IP Secure Media Coupler
IP routing
1.1.1 Tunneling Channel 1
1.1.5 Tunneling Channel 2
1.1.15 Tunneling Channel 3
1.1.20 Tunneling Channel 4
Park
Description
Add Device Certificate

Name: KNX IP Secure Media Coupler

Individual Address: 1.1 . 0

Last Modified 17.07.2019 11:29
Last Downloaded 16.07.2019 17:05
Serial Number 0072:031B41C3

Secure Commissioning: Activated

Secure Tunneling: Activated

Status: Unknown

Figure 18: Activation of Secure Tunneling

6 Web Front-end

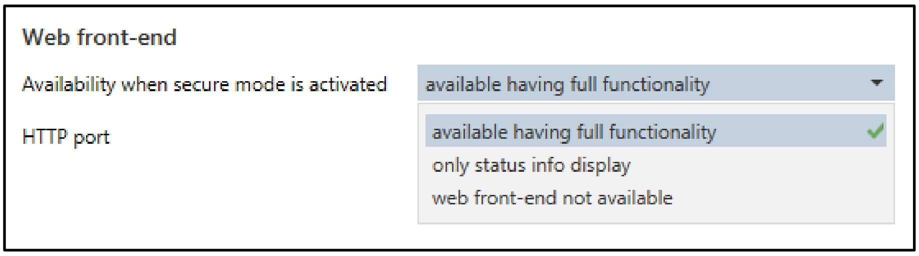
The web front-end can be used to read out MECip-Sec´s actual device settings (HTTP port, IP address, MAC address, …), to update the firmware and to set (additional) Individual Addresses for Tunneling. For identifying a certain MECip-Sec in a KNX network, Programming Mode can be remotely switched on and off without having to press 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 MECip-Sec Web Front-end

The web front-end can be used for remotely carrying out firmware updates, control functions and readout device settings. To raise protection for an installation, the web front-end availability is configurable. The highest degree is reached, when "not available" is set for normal runtime operation.

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



Web front-end

Availability when secure mode is activated: available having full functionality

HTTP port

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

Figure 19: ETS Parameter for Web Front-End Availability

When the web front-end is set to "only status info display", remote control functions (Programming Mode activation, Set Tunneling) and the update function are off. Changing settings or parameters via IP is not possible, and 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 MECip-Sec Web Front-end

There are three ways to access the MECip-Sec 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

When the web front-end is set to be available, MECip-Sec appears in the local network window (due to UPnP discovery). A double click on MECip-Sec, indicated by its set Product Name, opens the web front-end in the standard web browser.

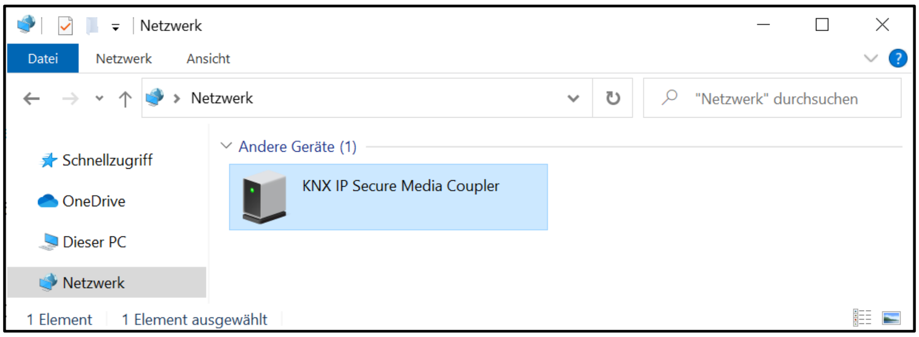
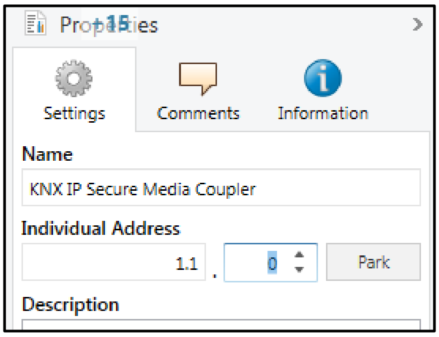

Netzwerk
Datei
Netzwerk
Ansicht
Netzwerk
"Netzwerk" durchsuchen
Schnellzugriff
OneDrive
Dieser PC
Netzwerk
Andere Geräte (1)
KNX IP Secure Media Coupler
1 Element
1 Element ausgewählt

Figure 20: Windows Explorer showing MECip-Sec

Changing MECip-Sec´s name that is shown in the network can be done by setting a new Product Name in the Properties window of ETS. After downloading the changed data to the device, the name of the network device is actualized.


Properties
Settings
Comments
Information
Park

Name
KNX IP Secure Media Coupler

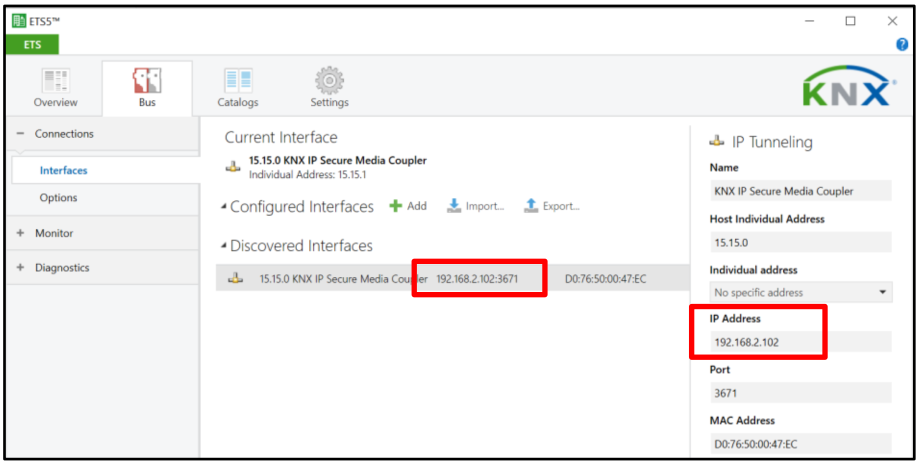
Individual Address
1.1 . 0

Description

Figure 21: Product Name Setting

6.2.2 via IP Address

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


ETS5™
ETS
Overview
Bus
Catalogs
Settings
KNX
Connections
Interfaces
Options
Monitor
Diagnostics
Configured Interfaces
Add
Import...
Export...
IP Tunneling

Current Interface
15.15.0 KNX IP Secure Media Coupler
Individual Address: 15.15.1

Discovered Interfaces
15.15.0 KNX IP Secure Media Coupler 192.168.2.102:3671 D0:76:50:00:47:EC

Name: KNX IP Secure Media Coupler
Host Individual Address: 15.15.0
Individual address: No specific address
IP Address: 192.168.2.102
Port: 3671
MAC Address: D0:76:50:00:47:EC

Figure 22: Identifying MECip-Sec´s IP address with ETS

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

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

Example1: 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/”.

Example2: MECip-Sec 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/”.

To access MECip-Sec via its IP address, the correct HTTP port must be entered in the URL bar.

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 MECip-Sec housing can be used. The MAC address is also shown in the ETS listing of Discovered Interfaces and in the properties window (of the network device) in the Windows explorer. Due to name resolution, it is mandatory to establish communication by Host name. Hereby, activation of NetBIOS is necessary.

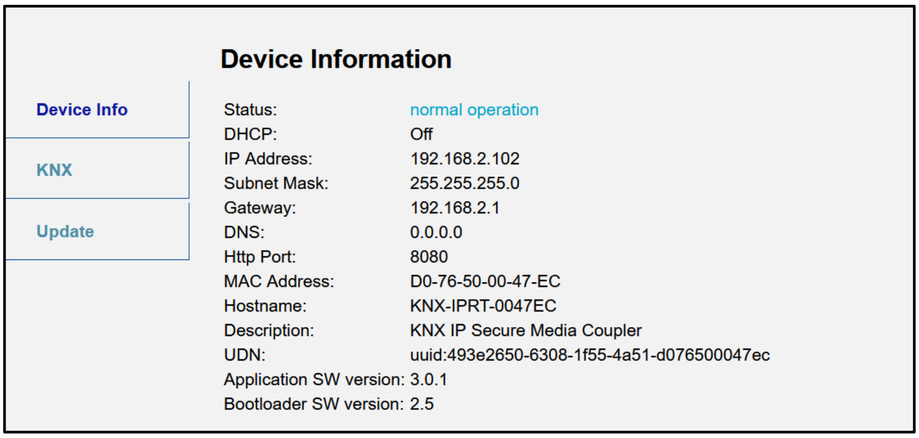
Use the MAC address AA-BB-CC-XX-YY-ZZ and the pre-set HTTP port and enter both in the browser´s URL bar, as described here (without brackets):

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

Example: On the side of its housing, MECip-Sec 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 actual device state, current settings, device parameters (like addresses, names, etc.), and software versions are shown.



Device Information

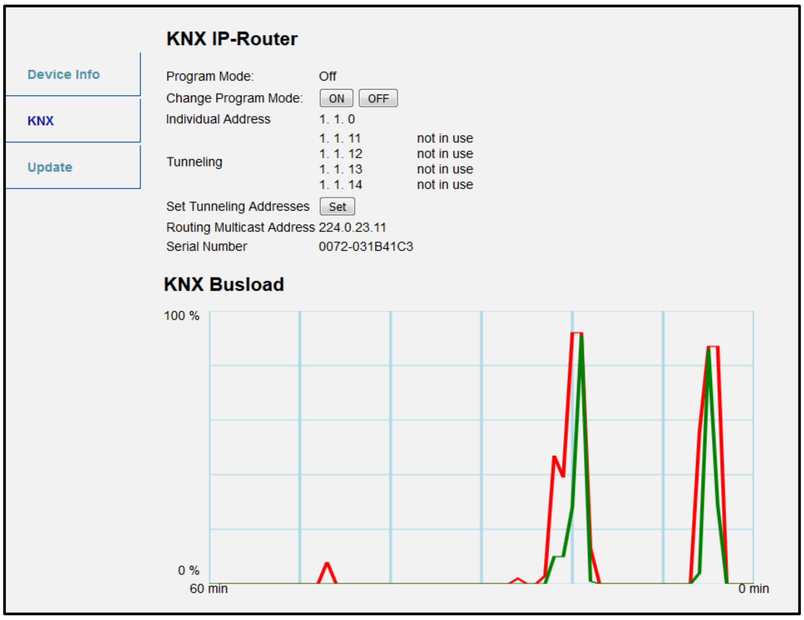
Status: normal operation
DHCP: Off
IP Address: 192.168.2.102
Subnet Mask: 255.255.255.0
Gateway: 192.168.2.1
DNS: 0.0.0.0
Http Port: 8080
MAC Address: D0-76-50-00-47-EC
Hostname: KNX-IPRT-0047EC
Description: KNX IP Secure Media Coupler
UDN: uuid:493e2650-6308-1f55-4a51-d076500047ec
Application SW version: 3.0.1
Bootloader SW version: 2.5

Figure 23: 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 MECip-Sec device (having a certain IP address, MAC address and serial number) from other MECip-Sec devices used in the installation network.

The Individual Address, the four Individual Addresses for Tunneling (additional tunneling addresses), routing multicast address, and the serial number of MECip-Sec are shown here. If the web browser supports SVG graphics, a last-60-minutes KNX busload diagram is additionally 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:
Individual Address 1. 1. 0
Tunneling
1. 1. 11 not in use
1. 1. 12 not in use
1. 1. 13 not in use
1. 1. 14 not in use
Set Tunneling Addresses
Routing Multicast Address 224.0.23.11
Serial Number 0072-031B41C3

KNX Busload

Figure 24: 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 when ETS versions lower than 5.7 are used for configuring. 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. In other words, with the Set button the addresses are reassigned to make sure the assigned Individual Addresses differ from each other. Reason is tunneling channels using the same Individual Address can cause a reduction of available connections for tunneling.

Care must be taken with using the Set button for reassignment. Clients maybe loose connectivity due to reassignment. It must be made sure the new assigned addresses have not been existing in the project before, or in the installation.

When Security is active, it is highly recommended not to press the Set button and to assign the additional Individual Addresses only by ETS projects and configuration downloads (see also chapter 5.4 IP (Secure) Tunneling Address Assignment).

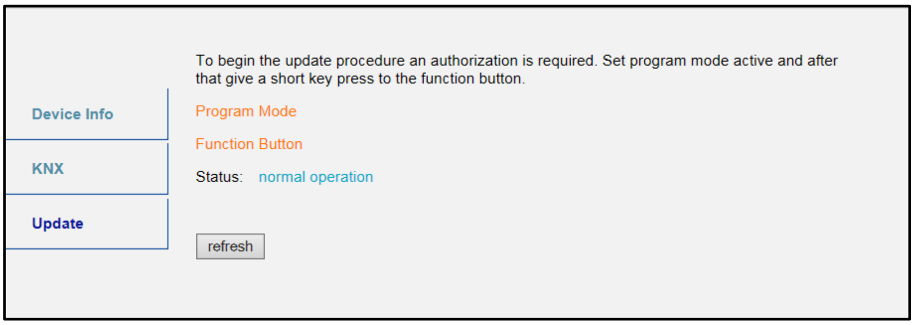
6.5 IP Firmware Update

Under the Update tab the MECip-Sec firmware can be updated via IP i.e. the Ethernet network. The complete remote update process is described in following steps. During this process, MECip-Sec 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 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 29). After that, MECip-Sec restarts and continues with normal operation.

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

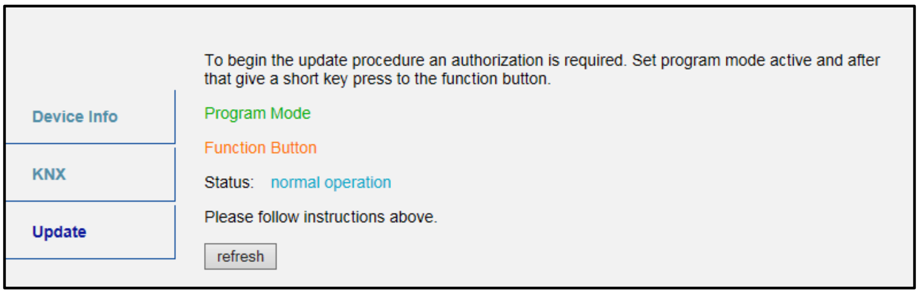


To begin the update procedure an authorization is required. Set program mode active and after that give a short key press to the function button.

Status: normal operation

Figure 25: Update Tab

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



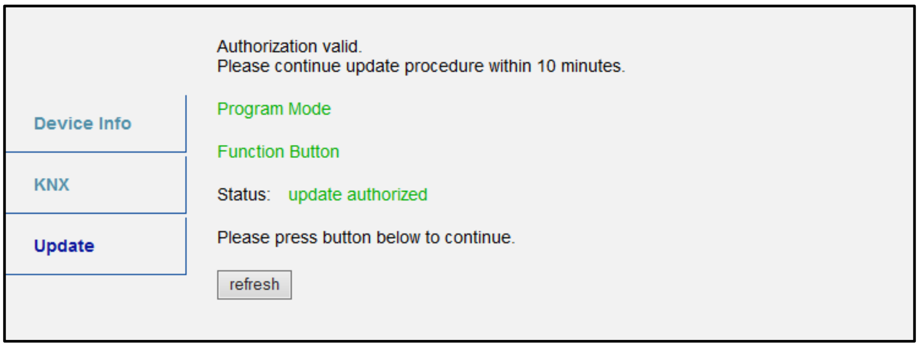
To begin the update procedure an authorization is required. Set program mode active and after that give a short key press to the function button.

Status: normal operation

Please follow instructions above.

Figure 26: 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

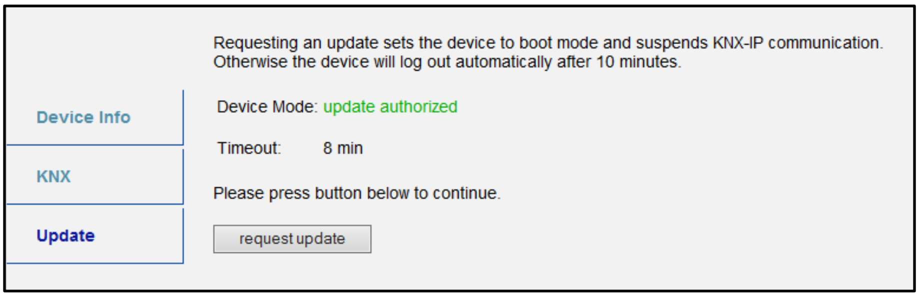
Function Button

Status: update authorized

Please press button below to continue.

Figure 27: 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.

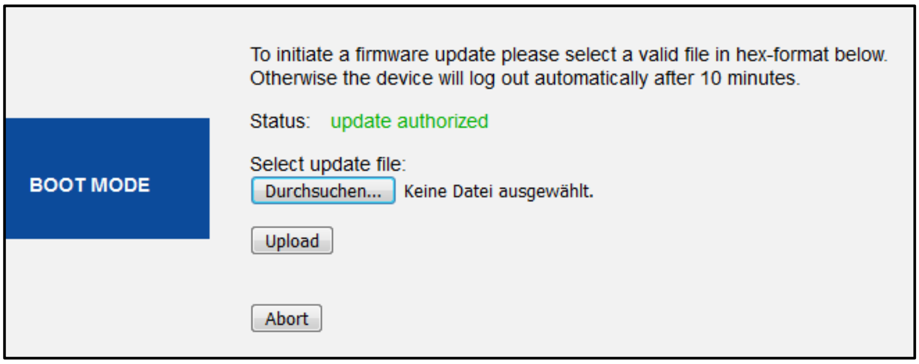
Device Mode: update authorized

Timeout: 8 min

Please press button below to continue.

Figure 28: Request Update

Step 5: **The update file can be selected and be uploaded by a click on „Upload". 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:
Keine Datei ausgewählt.

Figure 29: Select Update File

7 Glossary

ACK	An ACK is a positive IACK frame. If the sender detects an ACK, then the sender´s data has been received correctly, meaning the data has 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. Regarding sender and receiver, IACK frames are used to confirm to the sender the transmitted data was received correctly by the receiver (ACK) or not (BUSY/NACK). Also, a receiver cannot respond by sending back an IACK when a frame is damaged or incorrectly addressed (missing IACK). The IACK confirmation is a mechanism within a KNX TP line or segment. For communication across different lines or segments, the couplers connecting the lines generate the relevant IACKs.
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. Thereafter, the sender waits for a short time period and retries to send the frame.
Communication Object	same as Group Object
Data Point Type (DPT)	Standardized data format for transmitting values via KNX. The complete list of DPTs is available at KNX Association.
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 by couplers can be accomplished according to the topology via Individual Addresses (Physical Telegrams) and according to filter tables for group communication via Group Addresses (Group Telegrams).
Group Address	Group addresses are used to link group communication objects.

Group Communication Object	Group communication objects contain the datapoints which are transmitted via runtime communication. One or more group addresses are assigned to one group communication object. One of these assigned group addresses is the sending group address (to send the group communication object value to the bus). The remaining assigned group addresses, if available, then receive the value.
Group Object	same as Group Communication Object. A data point in KNX can be called shortly a 'Group Object' or just 'Object'.
Group Telegram	Group-oriented telegrams are named Group Telegrams. Filtering of Group Telegrams by couplers is accomplished according to their 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. When the sender detects a NACK, then the sender´s data has not been received correctly by at least one device meaning it has not been successfully transmitted to one or more receivers. Thereafter, the sender waits for a short time period and retries to send the frame.
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 regarded TP line (e.g. NACK, BUSY, missing IACK), couplers usually repeat messages up to three times. For all MEC couplers, the number of repetitions on TP 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: Factory Default Setting

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)	filter (filter table is empty)
Group telegrams (main group 14…31)	route all
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

Marking/Design	MECip-Sec
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	EN IEC 62368-1, EN IEC 63044-5-1, EN IEC 63044-5-2, EN IEC 63044-5-3, EN50581, EN61000-6-2, EN61000-6-3
Voltage supply	KNX: 21...30V DC (SELV)
Housing color	Plastic PA66 housing, light grey (similar to RAL9018 Papyrus white)
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

8.3 Drawings

Dimensions shown here are specified in mm.

The total device width is 2 modules at 18 mm.

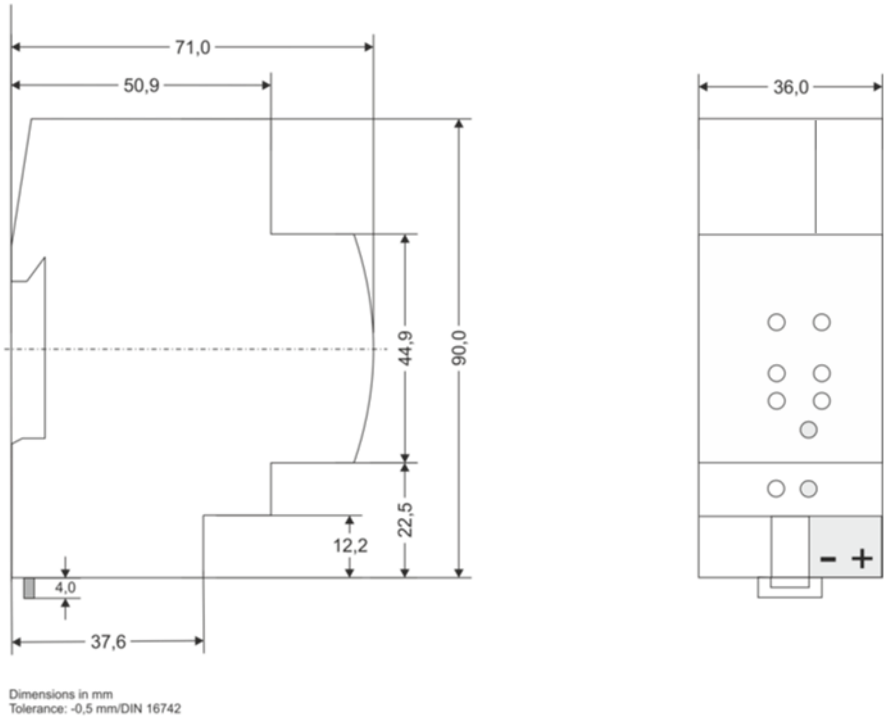

71,0
50,9
36,0
44,9
90,0
22,5
12,2
4,0
37,6
− +
Dimensions in mm
Tolerance: -0,5 mm/DIN 16742

Figure 30: Dimension drawings

9 Legal Notice

lwIP is used in developing the MECip-Sec.

lwIP is licenced under the BSD licence.

Copyright (c) 2001-2004 Swedish Institute of Computer Science. All rights reserved.

Providing that the following conditions are met redistribution and use in source and binary forms, with or without modification, are permitted:

- Redistributions of the source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR `` AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

10 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 MECip-Sec doesn´t work.**

  Either use Commissioning Password and Authentication Code from your former project or make a factory reset to set MECip-Sec´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 only unsecured from then.

- **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, MECip-Sec waits for an acknowledgement on the TP line. When the receiver was busy (BUSY) or received an incorrect telegram (NACK) or MECip-Sec didn´t receive an acknowledgement (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 MECip-Sec 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 MECip-Sec 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 13. 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 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 MECip-Sec?**

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

  When ETS can connect to MECip-Sec 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 MECip-Sec 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. Use the properties window of the network device in Windows or the list of Discovered Interfaces in ETS to do that.

- **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 ETS-configurable.

- **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.

- **I use MECip-Sec as the Current Interface in ETS. Can I change its IP address?**

  Yes. Set the new IP address in the IP window of the device properties, download the application and select the MECip-Sec that is now indicated by the new IP address.

- **I want to set filter settings, but LED 5 works not as described in the manual. What is the problem?**

  As long as the coupler doesn´t support the segment coupler extension, the coupler must have a certain configuration regarding its Individual address. This means the correct Individual address for KNX couplers must be assigned, according to x.y.0.

- **It happens that my ETS loses connection to MECip-Sec. What is the problem?**

  In case the data throughput on the IP line is too low, tunneling connections can disconnect due to timeout. When this problem appears for clients like ETS or visualizations, setting the slow tunneling connection support to “yes” can solve the problem.

TAPKO
TECHNOLOGIES GMBH

MECip
SECURE

MECip-Sec

Application:	KNX IP Secure Router
Doctype:	Technical & Application Description
Release Number / Release Date:	R1-0 / March 2022
TAD is intended for: (x = 0,1,2, … and y = a,b,c, …)	Firmware 3.0.x Databases R1-0y ETS version ETS5.7.3 and higher
Weblink to actual ETS Database:	https://www.tapko.de/mecip-sec
Contact:	sales@tapko.de
Telephone:	+49 941 30747-0

© 1999-2022

TAPKO Technologies GmbH
Im Gewerbepark A15
93059 Regensburg
Germany