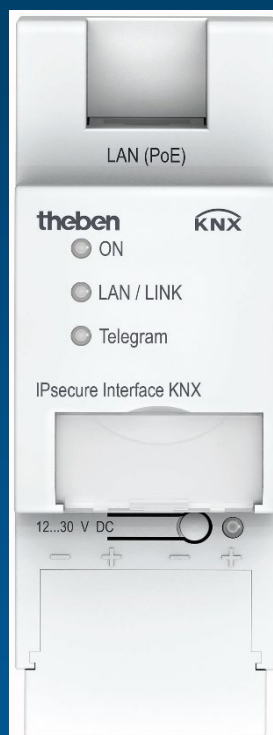


# IPsecure Interface KNX 9070771 Product Manual



# IPsecure Interface KNX

## Contents

Contents		Page
<b>1</b>	<b>General.....</b>	<b>3</b>
1.1	Using the product manual .....	3
1.1.1	Notes.....	4
1.2	Cyber security (network security).....	5
1.3	Preventing access to the different media .....	5
1.4	Twisted pair cabling.....	5
1.5	IP cabling inside the building.....	5
1.6	Connection to the Internet.....	6
1.7	KNXnet/IP Security .....	6
1.8	Product and functional overview .....	7
1.8.1	Overview of versions.....	9
<b>2</b>	<b>Device technology.....</b>	<b>11</b>
2.1	Technical data .....	11
2.2	Connection diagram .....	13
2.3	Dimension drawing .....	14
2.4	Mounting and installation.....	15
2.4.1	Unloading the device and resetting to factory settings.....	16
2.5	Description of inputs and outputs.....	18
2.6	Operating controls.....	19
2.7	Display elements .....	19
<b>3</b>	<b>Commissioning.....</b>	<b>21</b>
3.1	Overview.....	21
3.2	Parameters .....	22
3.3	Communication objects.....	24
3.4	Use of the integrated tunneling servers .....	24
3.4.1	Tunneling server settings .....	25
3.5	KNX Secure.....	26
<b>4</b>	<b>Planning and application .....</b>	<b>27</b>
4.1	The IPsecure Interface in the network.....	27
4.1.1	Assignment of IP address .....	27
4.1.2	Monitoring an IPsecure Interface KNX.....	27
4.2	The Theben IP Tool .....	28
4.2.1	Discovery.....	28
4.2.2	Firmware update .....	29
<b>5</b>	<b>Contact.....</b>	<b>30</b>
<b>6</b>	<b>Open source software components (OSS).....</b>	<b>31</b>

# IPsecure Interface KNX

## General

### 1 General

The Theben IPsecure Interface KNX connects the KNX bus to an Ethernet network. KNX telegrams can be sent to or received from other devices via the network.

The interface can be used as a programming interface (ETS), and clients, e.g. visual display systems, can access the KNX bus via the IPsecure Interface KNX. The device supports the KNX Secure protocol (KNXnet/IP Security).

#### 1.1 Using the product manual

This manual provides detailed technical information on the function, installation and programming of the Theben KNX device. The application is explained using examples.

This manual is divided into the following chapters:

Chapter 1	General
Chapter 2	Device technology
Chapter 3	Commissioning
Chapter 4	Planning and application
Chapter A	Appendix

# IP Interface KNX

## General

### 1.1.1

#### Notes


Notes and safety instructions are represented as follows in this manual:

Note
Tips for usage and operation

Examples
Application examples, installation examples, programming examples

Important
These safety instructions are used as soon as there is danger of a malfunction without risk of damage or injury.

Attention
These safety instructions are used as soon as there is danger of a malfunction without risk of damage or injury.

 Danger
These safety instructions are used if there is a danger to life and limb with inappropriate use.

  Danger
These safety instructions are used if there is an extreme danger to life with inappropriate use.

### 1.2 Cyber security (network security)

The industry is increasingly faced with cyber security risks. To increase the stability, security and robustness of its solutions, Theben has introduced official robustness tests for Internet security as part of the product development process.

In addition, the information below includes guidelines and mechanisms that you can use to improve the security of KNX systems.

### 1.3 Preventing access to the different media

The basis for any protection concept is the careful shielding of the system against unauthorized access. Only authorized persons (installers, janitors and users) should have physical access to a KNX system. The critical points of every KNX medium must be protected as well as possible during planning and installation.

In general, applications and devices should be permanently installed to prevent their easy removal and in this way prevent access to the KNX system for unauthorized persons. Subdistributions with KNX devices should be closed, or in rooms to which only authorized persons have access.

### 1.4 Twisted pair cabling

- The ends of KNX twisted pair cables should not be visible or protrude from the wall either inside or outside the building.
- If available, use the anti-theft devices on the application modules.
- Bus cables outdoors represent an elevated risk. Ensure that physical access to KNX twisted pair cables is especially difficult here.
- For extra security, devices installed in areas with limited protection (outdoor areas, underground parking lots, restrooms, etc.) can be designed as a separate line. Enabling the filter tables in the Line Couplers (KNX only) prevents attackers from gaining access to the whole system.

### 1.5 IP cabling inside the building

For building automation, use a separate LAN or WiFi network with its own hardware (routers, switches, etc.).

Regardless of the KNX system, apply the usual security mechanisms for IP networks. These are examples:

- MAC filter
- Encryption of wireless networks
- Usage of strong passwords and protection of these against access by unauthorized persons

Note
The device cannot be reached during IP, TCP or UDP flooding (access from the Internet). To prevent this reaction, set a data rate limit at network level. Please discuss the topic with your network administrator.

# IP Interface KNX

## General

### 1.6 Connection to the Internet

The device is not intended for use on the public Internet. For this reason router ports in the direction of the Internet must not be opened; this action will ensure KNX communication is not visible on the Internet.

Systems can be accessed via the Internet in the following ways:

- Access to KNX installations via VPN connections. However, this requires a router with VPN server functionality.
- Use of manufacturer-specific solutions or visualizations, e.g. access via https.

### 1.7 KNXnet/IP Security

The device should always be operated in KNX Secure mode. This ensures security for the tunneling servers and for commissioning the device itself.

See also chapter 3.5, [KNX Secure](#).

# IPsecure Interface KNX

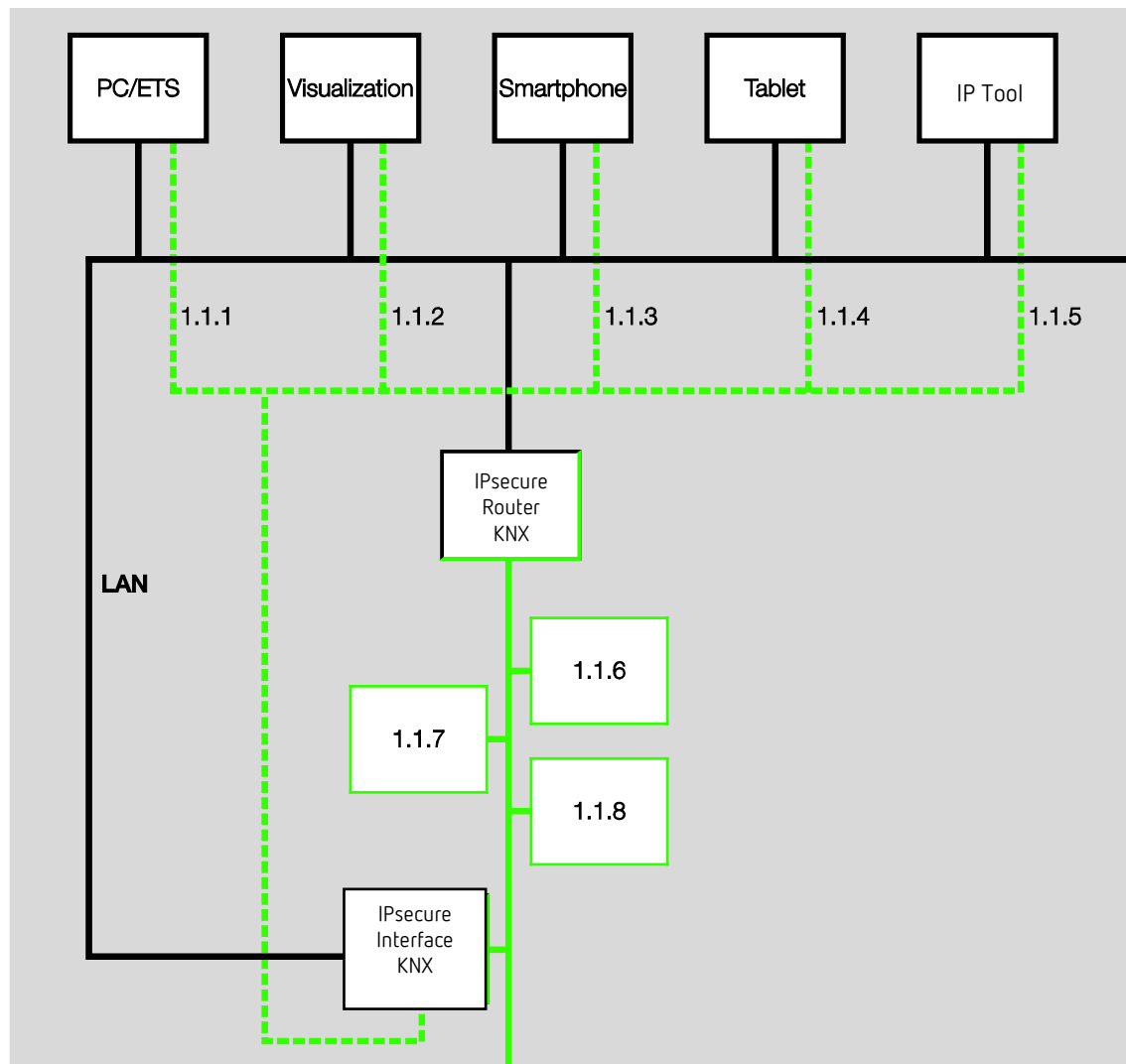
## General

### 1.8 Product and functional overview

The Theben IPsecure Interface KNX connects the KNX bus to an Ethernet network. KNX telegrams can be sent to or received from other devices via the network.

The interface can be used as a programming interface (ETS), and clients, e.g. visual display systems, can access the KNX bus via the Interface.

The device uses the KNXnet/IP protocol from the KNX Association for communication (tunneling).



The Interface features five tunneling servers, see chapter [Use of the integrated tunneling servers](#). They support both bus monitor and group monitor mode.

The tunneling servers can be operated in KNX Secure mode.

# IP Interface KNX

## General

The power supply can be implemented via PoE (Power over Ethernet) according to IEEE 802.3af class 1 or via a supply voltage. If both options are connected simultaneously, PoE will be used.

The Theben Tool, which is capable of detecting the Interface in the network (IP discovery), is available for the IPsecure Interface (see chapter [Theben Tool](#)).

An ETS app (Theben Update App) is available for the firmware update. If KNX Secure mode is not activated for the devices, a firmware update can also be performed with the Theben Tool.

During the update process, the KNX bus (TP) must be connected in addition to the IP network (LAN). Otherwise, the update process will fail.

It must be ensured that no voltage failure (KNX or IP) occurs during the update process, otherwise the device can be destroyed.



# IPsecure Interface KNX

## General

### 1.8.1 Overview of versions

Device	IP Interface	IPsecure Interface
Application	IP Interface	IPsecure Interface
ETS	from ETS 3	from ETS 5
<b>Properties of the IP Interface</b>		
Number of tunneling servers	1	5
IP discovery (IP Tool)	■	■
Firmware update with (IP Tool)	■	■*
Firmware update with Theben Update App	-	■
Power over Ethernet	■	■
KNX Secure	-	■

\* Only if the device is not operated in KNX Secure mode

# IPsecure Interface KNX

## Device technology

## 2 Device technology



IPsecure Interface KNX

IPsecure Interface KNX is the interface between KNX installations and IP networks. KNX telegrams can be sent to or received from other devices via the network.

The Interface can be used as a programming interface (ETS), and clients, e.g. Visualisations, can access the KNX bus via the Interface.

The device uses the KNXnet/IP protocol and the KNXnet/IP Security protocol from the KNX Association (tunneling) for communication.

The device is powered by 12 to 30 V DC or PoE (Power over Ethernet) to IEEE 802.3af class 1. If both options are connected simultaneously, PoE will be used.

### 2.1 Technical data

<b>Supply</b>	Auxiliary voltage $U_s$	12...30 V DC (+10% / -15%) or PoE (IEEE 802.3af class 1)
	Power dissipation	Maximum 1.8 W
	Auxiliary voltage current consumption	Maximum 120 mA at 12 V
	Rated voltage $U_n$	12 V DC
	Current consumption KNX	< 10 mA
<b>Connections</b>	KNX	Bus connection terminal
	Plug-in terminal for operating voltage	Plug-in terminal
	LAN	RJ45 socket for 10/100BaseT, IEEE 802.3 networks, AutoSensing
<b>Operating and display elements</b>	Red LED and button	For assignment of the physical address
	Green "On" LED	Operation readiness indicator
	Yellow "LAN/Link" LED	Network connection indicator
	Yellow "Telegram" LED	KNX telegram traffic indicator
<b>Protection degree</b>	IP 20	To DIN EN 60 529
<b>Protection class</b>	II	To DIN EN 61 140
<b>Isolation category</b>	Overvoltage category	III according to DIN EN 60 664-1
	Pollution degree	2 according to DIN EN 60 664-1
<b>KNX safety extra low voltage</b>	SELV 30 V DC	
<b>Temperature range</b>	Operation	-5...+45 °C
	Storage	-25...+55 °C
	Transport	-25...+70 °C
<b>Ambient conditions</b>	Maximum air humidity	95 %, no condensation allowed
	Atmospheric pressure	Atmosphere up to 2,000 m

# IPsecure Interface KNX

## Device technology

<b>Design</b>	Modular installation device (MDRC)	Modular installation device, ProM
	Overall dimensions	90 x 36 x 64 mm (H x W x D)
	Mounting width	2 x 18 mm modules
	Mounting depth	68 mm
<b>Installation</b>	On 35 mm mounting rail	To DIN EN 60 715
<b>Mounting position</b>	Any	
<b>Weight</b>	0.1 kg	
<b>Housing, color</b>	Plastic, halogen free, gray	
<b>Approvals</b>	KNX to EN 50 090-1, -2	
<b>CE marking</b>	In accordance with the EMC directive and low voltage directive	

Device type	Application	Maximum number of communication objects	Maximum number of group addresses	Maximum number of assignments
IPsecure Interface KNX	IPsecure Interface/...*	0	0	0

\* ... = Current version number of the application. **Please refer to the software information on our website for this purpose.**

### Note

ETS (ETS 5 version 5.7.4 or higher) and the current version of the device application are required for programming.

If the device is to be operated in KNX Secure mode, the commissioning key (FDSK; see chapter [KNX Secure](#)) on the side of the unit will be required as well.

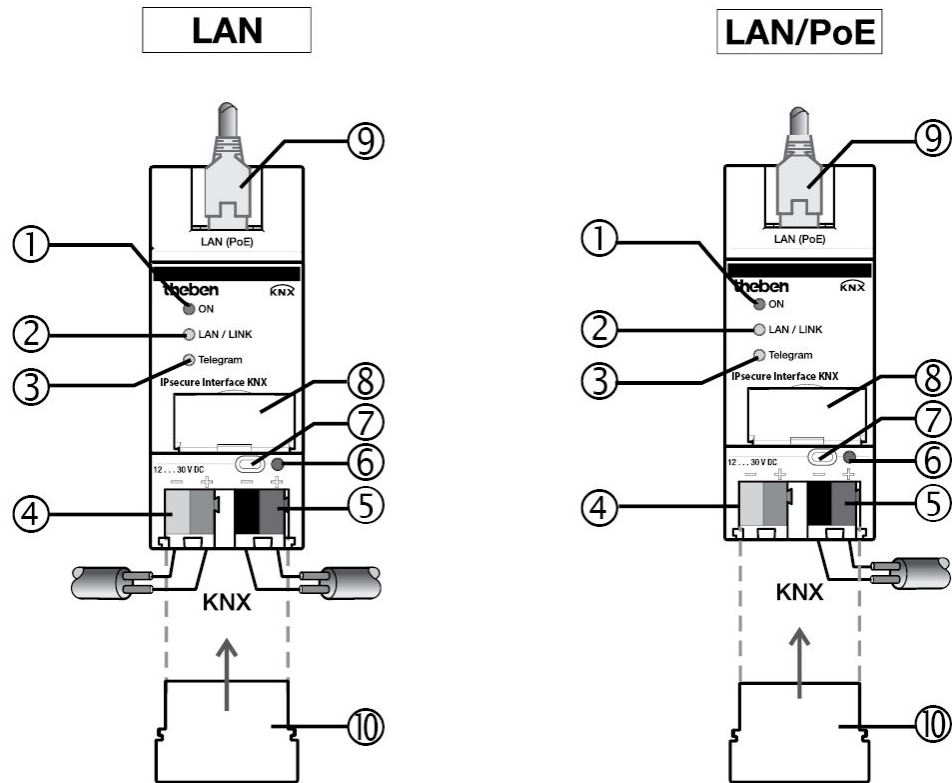
The latest version of the application and corresponding software information are available for download from [www.abb.com/knx](http://www.abb.com/knx). After import into ETS, the application is stored in the *Catalogs* window under *Manufacturers/Theben/System Infrastructure and Interfacing/IP Routers and Interfaces*.

The device does not support the locking function of a KNX device in ETS. If you use a *BCU code* to disable access to all the project devices, it has no effect on this device. Data can still be read and programmed.

**Exception:** When KNX Secure mode is activated, the device can be programmed only using the existing project.

# IPsecure Interface KNX Device technology

## 2.2 Connection diagram



### IPsecure Interface KNX

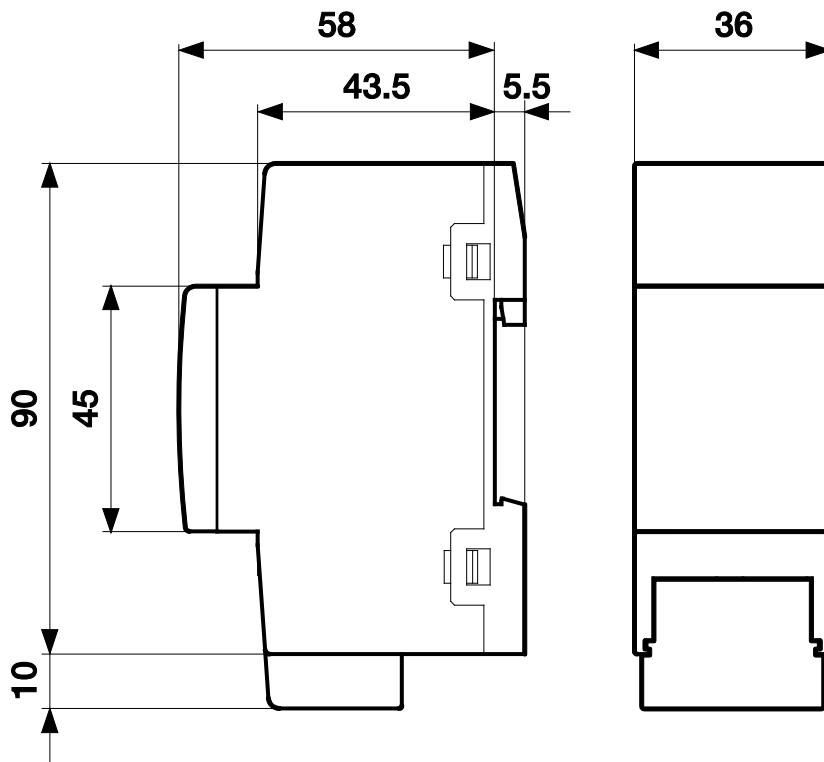
- |   |                         |    |                           |
|---|-------------------------|----|---------------------------|
| 1 | ON LED                  | 6  | Programming LED           |
| 2 | LAN / LINK LED          | 7  | Programming button        |
| 3 | Telegram LED            | 8  | Label carrier             |
| 4 | Power supply connection | 9  | LAN or LAN/PoE connection |
| 5 | KNX connection          | 10 | Cover cap                 |

### Note

It is also possible to power the Interface via the voltage output without choke of an Theben KNX power supply.  
This reduces the number of KNX devices that can be connected to the Theben KNX power supply accordingly.

# IPsecure Interface KNX Device technology

## 2.3 Dimension drawing



IPsecure Interface KNX

### 2.4 Mounting and installation

The device is a modular installation device for quick installation in distribution boards on 35 mm mounting rails to DIN EN 60 715.

The installation position can be selected as required.

The connection to the bus is implemented using the supplied bus connection terminal. The terminal assignment is located on the housing.

The device is ready for operation after connecting the bus voltage and the auxiliary voltage.

Accessibility to the device for the purpose of operation, testing, visual inspection, maintenance and repair must be provided compliant to DIN VDE 0100-520.

#### Prerequisites for commissioning

In order to commission the device, a PC with ETS (ETS 5 version 5.7.4 or higher) and a supply voltage of 12 to 30 V DC are required. Alternatively, the device can be powered via PoE (Power over Ethernet) to IEEE 802.3af class 1.

The device is ready for operation after connection to the bus voltage and auxiliary voltage.

Mounting and commissioning may only be carried out by electrical specialists. The appropriate standards, directives, regulations and specifications for the appropriate country should be observed when planning and setting up electrical installations and security systems for intrusion and fire detection.

- Protect the device from damp, dirt and damage during transport, storage and operation.
- Only operate the device within the specified technical data!
- The device should only be operated in an enclosed housing (distribution board)!
- The voltage supply to the device must be switched off before mounting work is performed.



#### Danger

To avoid dangerous touch voltages which originate through feedback from differing phase conductors, all poles must be disconnected when extending or modifying the electrical connections.

#### Supplied state

All physical tunneling connection addresses are set to 15.15.100 in the supplied state. In other words, only one tunnel is visible to the outside. The tunneling connection addresses set in ETS will be adopted only after the first download.

The IP address is set to automatic IP assignment (DHCP/AutoIP).

#### Assignment of the physical address

The physical addresses and parameters are assigned and programmed in ETS.

The device features a *Programming* button for assignment of the physical address. The red *Programming* LED lights up after the button has been pressed. It goes off as soon as ETS has assigned the physical address or the *Programming* button is pressed again.

# IPsecure Interface KNX

## Device technology

### Download reaction

The device can be programmed in various ways: via one of the integrated tunneling servers ("local download") or via another programming interface (USB or IP).

Note
Any USB interface used for programming a KNX Secure device must support "long frames." Suitable is an USB interface from Theben.

There must be a connection to the KNX TP (twisted pair) in order to program the device.

Approx. 10 seconds after the download is complete, the device reboots and closes all open tunneling connections. If the device's IP address was changed during the download, the tunneling connections must be reconfigured manually in the tunneling clients. Tunneling clients establish the connection to the server via the IP address.

The data programmed with ETS is adopted approx. 30-60 seconds after the download.

### 2.4.1

#### Unloading the device and resetting to factory settings

The device can be reset to the factory settings. This is a Secure device, so the following information must be observed:

When the device is operated in KNX Secure mode, it can be reset via ETS only if ETS uses the project with which the device was parametrized or if the commissioning key is available in the project.

The device can be unloaded by right-clicking it in ETS.

#### Option: unloading the application

- The IP address and IP configuration will be retained
- The passwords and IP addresses of the tunneling servers will be deleted
- The tool key assigned by ETS will be retained. In other words, the FDSK will not be needed for reprogramming
- The physical address will be retained

#### Option: unloading the physical address and the application

- The device will be reset to the factory state
- The FDSK will be needed for re-commissioning unless it is still available in the ETS project from the original commissioning process

# IPsecure Interface KNX

## Device technology

Resetting to factory settings can also be performed directly on the device. This is not a security risk, because the device will no longer be part of the system afterward.

- Press the Programming button when the KNX bus is not connected
- Hold the Programming button down and plug on the bus terminal. The Programming LED flashes (2 Hz)
- Press the button, hold it for at least 5 s and then release it. The Programming LED goes out, and the device reboots with the factory settings

The Interface can be reprogrammed if ETS connects with the device after reset and if the device's FDSK is still known to ETS. ETS will report that the device was reset in this case.

See chapter [KNX Secure](#), for more information about the FDSK (Factory Default Setup Key).

### **Cleaning**

Disconnect the device from the electrical power supply before cleaning. If devices become dirty, they can be cleaned using a dry cloth or a cloth dampened with a soapy solution. Never use corrosive agents or solutions.

### **Maintenance**

In the event of damage, e.g. during transport and/or storage, repairs are not allowed to be made. Please keep the device's firmware up to date; see chapter [Firmware update](#).



### 2.5 Description of inputs and outputs

#### Supply voltage input 12 to 30 V DC

Only a DC voltage in a range of 12 to 30 V may be connected to the power supply input. We recommend using an power supply 640 mA S KNX from our range. It is also possible to power the Interface via the voltage output without choke of an Theben KNX power supply.

#### Caution

The supply voltage must be 12 to 30 V DC, or the device is powered via PoE (Power over Ethernet) according to IEEE 802.3af class 1.

Connecting the device to a voltage outside the permissible range can destroy it!

#### KNX connection

The supplied bus connection terminal is used to connect to the KNX bus.

#### Note

Programming requires ETS (ETS 5 version 5.7.4 or higher).

#### LAN connection

The network connection is carried out via an Ethernet RJ45 interface for LAN networks. The network interface can be operated with a transmission speed of 10/100 Mbit/s. Network activity is indicated by the LAN/LINK LED on the front of the device.

# IPsecure Interface KNX

## Device technology

### 2.6 Operating controls

There are no operating controls located on the IPsecure Interface.

### 2.7 Display elements

Three indicator LEDs are located on the front of the device:



ON



LAN/LINK



Telegram

#### ON

- The LED lights up a few seconds after the auxiliary voltage is connected.
- After the supply voltage is connected, the LED initially lights up continuously. After approx. 40 seconds, the LED starts flashing until the startup process is complete and the LED lights up continuously again.

#### LAN/LINK

- The LED lights up when the auxiliary voltage is present and the interface is connected to an Ethernet network.
- The LED flashes when the device detects activity on the network, e.g. when data is exchanged.

#### Telegram

- The LED lights up when the interface is connected to a TP network and the startup process is complete (see "On" LED).
- The LED flashes when the device detects activity on the KNX subline TP1 (twisted pair 1), e.g. when data is exchanged.

# IPsecure Interface KNX Commissioning

## 3 Commissioning

The IPsecure Interface KNX is parameterized using the application and the Engineering Tool Software ETS.

The application can be found under *Theben AG/System components/Interfaces*.

For parameterization purposes, a PC or laptop with ETS and a connection to KNX are required.

### 3.1 Overview

The IPsecure Interface is parameterized using the Engineering Tool Software (ETS 5 version 5.7.4 or higher).

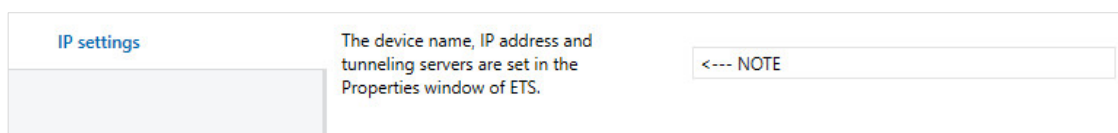
# IPsecure Interface KNX Commissioning

## 3.2 Parameters

This chapter describes the parameters of the IPsecure Interface using the parameter windows.

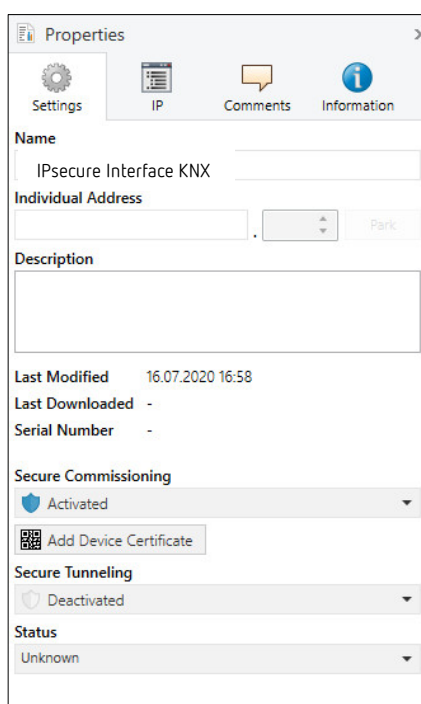
Parameter window *IP settings*

All parameters for the device are set in the Properties window of ETS.



**Note**  
The device name, IP address and tunneling servers are set in the Properties window of ETS.

The IP parameters (device name, assignment of the IP address by DHCP or static) are configured in the Properties window of ETS.



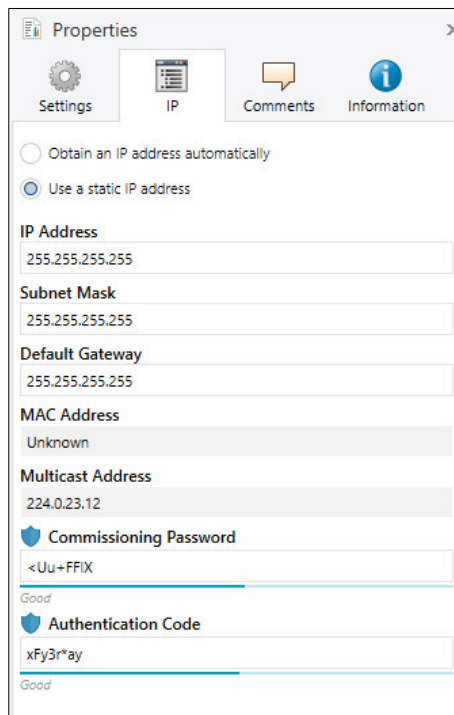
The device name can be entered in the *Settings* Properties window. The device name loaded into the device can be changed in the *Name* field. The device name is used for identification of the device on LAN. After a search query, e.g. by ETS, every KNXnet/IP device reports its name and can be allocated accordingly. For example, the installation location can be identified by the names assigned to the devices, e.g. IP Interface, HALL, SUB7, etc.

**Note**  
The default device name on delivery is "IPsecure Interface". After the first download, the device name entered in the Properties window of ETS is loaded into the device.

**Caution**  
Only the first 30 characters of the device name are loaded into the device; the rest is truncated.

# IPsecure Interface KNX Commissioning

The IP address can be defined in the *IP* Properties window.



The screenshot shows the 'Properties' window for the IP interface. It has four tabs: 'Settings', 'IP', 'Comments', and 'Information'. The 'IP' tab is selected. Under 'Settings', there are two radio buttons: 'Obtain an IP address automatically' (unselected) and 'Use a static IP address' (selected). Below this, there are input fields for 'IP Address' (255.255.255.255), 'Subnet Mask' (255.255.255.255), and 'Default Gateway' (255.255.255.255). The 'MAC Address' is 'Unknown'. The 'Multicast Address' is '224.0.23.12'. There is a 'Commissioning Password' field with the value '<Uu+FFiX' and a 'Good' status indicator. Below that is an 'Authentication Code' field with the value 'xFy3r\*ay' and a 'Good' status indicator.

The following options are available for setting the IP address:

Options: Obtain an IP address automatically  
Use the following IP address

- *Obtain an IP address automatically:* In the default setting, the IP Interface Secure expects the assignment of an IP address by a DHCP (dynamic host configuration protocol) server. This server responds to a request by assigning a free IP address to the device. If a DHCP server is not available in the network, the device starts an auto IP procedure. It assigns itself an address from the reserved range for auto IP addresses (169.254.1.0 to 196.254.254.255).

For information about DHCP: see chapter [Assignment of IP address](#)

- *Use a static IP address:* If no DHCP server is installed in the network or if the IP address should remain the same, it can be assigned as static.  
When assigning static IP addresses, ensure that each device receives a different IP address.

## Note

The MAC address is read from the device after a download.

The MAC address is additionally labeled on the device, or it can be determined via the IP Tool.

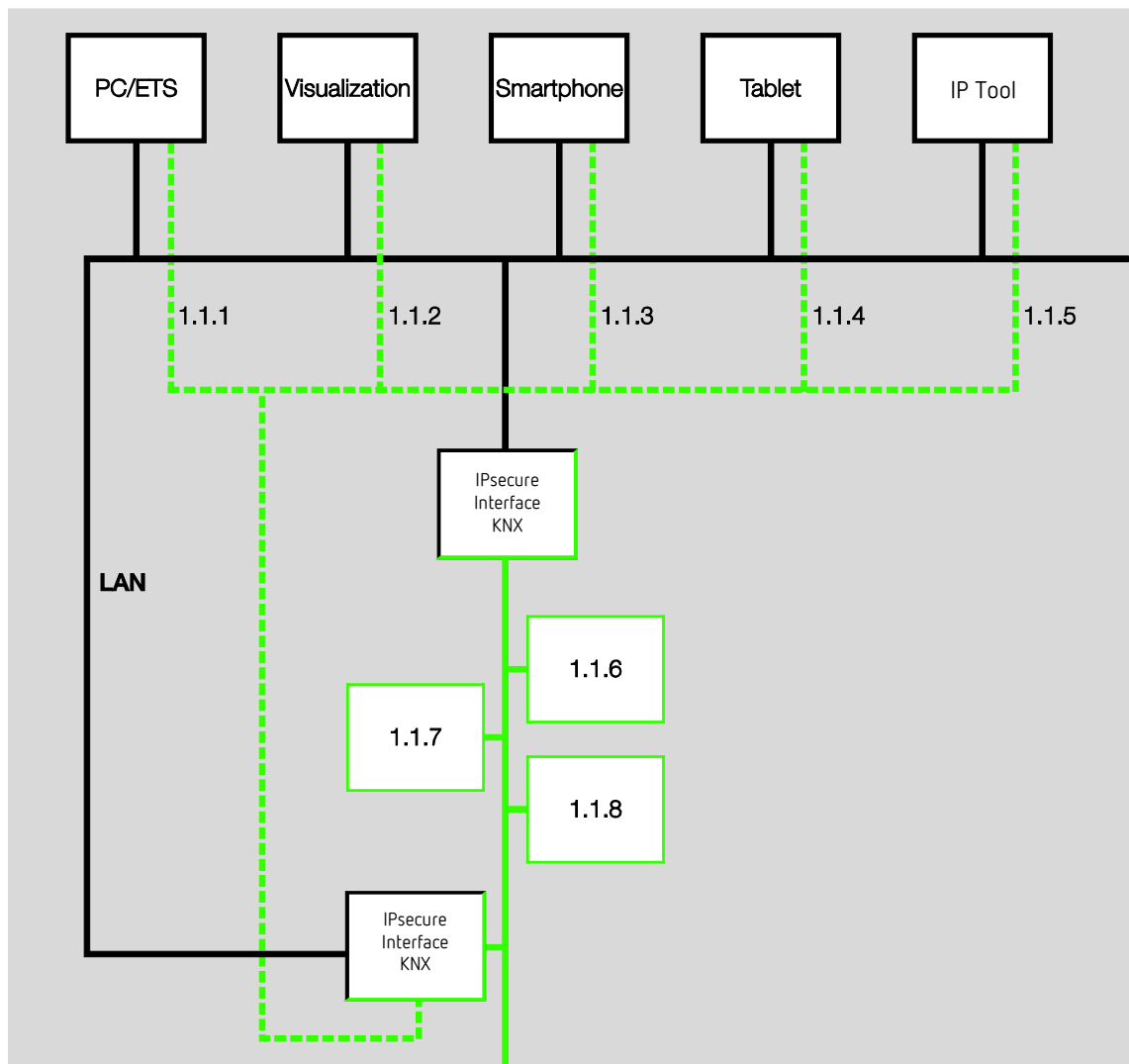
# IPsecure Interface KNX Commissioning

## 3.3 Communication objects

The IPsecure Interface has no group objects.

## 3.4 Use of the integrated tunneling servers

The IPsecure Interface offers five additional physical addresses, which can be used for a tunneling connection. These so-called tunneling servers can be used with the ETS as a programming interface or with another client, e.g. a Visualisation.



Tunneling involves a client connecting to a bus line. The tunneling process uses UDP, but includes a data link layer so that telegrams are repeated in the event of an error. Tunneling V2 is supported from ETS 5. TCP is used instead of UDP here, and the TCP's data link layer is used for transmission.

The tunneling servers can also be encrypted with KNX Secure. When KNX Secure mode is activated, a client will need the password assigned in ETS.

For details, see chapter [KNX Secure](#).

# IPsecure Interface KNX Commissioning

## Note

The physical address for the tunneling connection must fit the topology. Therefore, the addresses must be selected from the address range of the subordinate line. On delivery, all tunneling servers have the address 15.15.100.

In ETS 5, the first five free addresses in the line are assigned automatically after the Interface has been inserted into a line.

The tunneling servers can also be encrypted with KNX Secure. When KNX Secure mode is activated, a client will need the password assigned in ETS.

For details, see chapter 3.5, [KNX Secure](#).

### 3.4.1

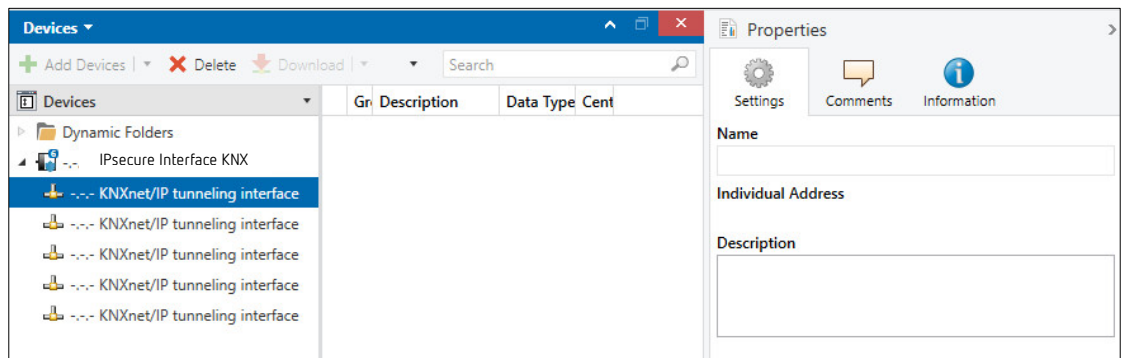
#### Tunneling server settings

An additional Properties window is available in ETS for setting the additional physical addresses.

After insertion of the Interface into the line, ETS automatically reserves the first five free addresses of this line for the tunneling servers of the Interface. This is a property of ETS and cannot be changed.

The addresses will be available in the device after the first download.

If this is not desired, the setting can be changed manually in the Properties window.



To change the address, mark the current device address or additional address and then select the desired numerals using the up or down arrow key. The changed address is saved when another address is marked.

The changed addresses are adopted by the device only after a download.

#### Park

If the option *Park* is activated for a tunnel, this tunnel will receive the address 15.15.255.

If the option *Park* is selected for all tunneling servers, all tunneling servers will be assigned the address 15.15.255. Only one tunneling server is available as a result.

# IPsecure Interface KNX

## Commissioning

### 3.5 KNX Secure

The Theben IPsecure Interface is a KNX device according to the KNX Secure standard. In other words, the device can be put into operation in a secure manner and the tunneling connections are encrypted.

The following information must therefore be taken into account during device commissioning:

- It is essential to assign a project password as soon as a KNX Secure device is imported into a project. This will protect the project against unauthorized access.  
**The password must be kept in a safe place – access to the project is not possible without it (not even the KNX Association or Theben will be able to access it)!**
- A commissioning key is required when commissioning a KNX Secure device (first download). This key (FDSK = Factory Default Setup Key) is included on a sticker on the side of the device, and it must be imported into ETS prior to the first download.
  - On the first download of the device, a window opens in ETS to prompt the user to enter the key. The certificate can also be read using a QR code scanner (recommended).
  - Alternatively, the certificates of all Secure devices can be entered in ETS beforehand. This is done on the “Security” tab on the project overview page.
  - Two FDSK stickers are applied on the device. One of them can be used for the project documentation, and the other one can remain on the device.  
**Without the FDSK, it will no longer be possible to operate the device in KNX Secure mode after a reset.**

The FDSK is required only for initial commissioning. ETS then assigns new keys.

The FDSK will be required again only if the device was reset to its factory settings (e.g. if the device is to be used in a different system with a different ETS project).

ETS generates separate passwords for each tunneling server. The passwords can be changed as required.

ETS generates and administers the keys. Keys and passwords can be exported as needed (e.g. if a client would like to access one of the tunnels).

The interface can be reset to its factory settings if necessary; see chapter [Unloading the device and resetting to factory settings](#).



# IPsecure Interface KNX

## Planning and application

### 4 Planning and application

#### 4.1 The IPsecure Interface in the network

The IPsecure Interface is designed for use in 10/100 BaseT networks compliant to IEEE 802.3. The device features an AutoSensing function and sets the baud rate (10 or 100 Mbit) automatically.

##### 4.1.1 Assignment of IP address

###### DHCP/AutoIP

The IP address of the device can be received from a DHCP server. This requires setting automatic IP address assignment in ETS, see parameter window [IP settings](#). If no DHCP server is found with this setting, the device starts an AutoIP procedure and autonomously assigns itself an IP address from the range 169.254.xxx.yyy.

The IP address that the device receives (via DHCP or AutoIP) during startup will be retained until

- the next reboot (switching off/on or reprogramming).
- a DHCP server is available
- the DHCP lease expires

###### No DHCP server is available during startup

If no DHCP server is available during startup of the IP Interface Secure, the device will assign itself an AutoIP address. The Interface then cyclically (three telegrams at intervals of 3 seconds, followed by a pause of 20 seconds) searches for a DHCP server. As soon as a server is available again, the address assigned by the DHCP server is used.

###### DHCP server fails (device has already received IP address from DHCP)

Each IP address assigned by a DHCP has a validity time for use (lease time). This validity time is extended prior to expiry by means of a request from the device to the DHCP server. If the device's validity time for use is not extended, the device searches for an AutoIP address after expiry of the validity time.

###### Static IP address

If the IP address of the IPsecure Interface KNX is to have a fixed assignment, a static IP address (as well as a subnet mask and a default gateway) can be set in ETS, see parameter window [IP settings](#).

If no default gateway is available, the value must be set to 0.0.0.0.

##### 4.1.2 Monitoring an IPsecure Interface KNX

If the device is to be monitored by a Visualisation that maintains a tunneling connection to the device, the active tunneling connection should be used for monitoring.

If the device is to be monitored by a Monitoring Unit, monitoring should take place for the device address and not for one of the tunneling connections.

# IPsecure Interface KNX

## Planning and application

### 4.2 The Theben IP Tool

#### 4.2.1 Discovery

The IP Interfaces can be found in the network using the IP Tool.

Select *Discovery* mode in the ribbon area. This function serves to find and display Theben IP devices in the network.

<b>Note</b>
The functions are described in the IP Tool online help.

# IPsecure Interface KNX

## Planning and application

### 4.2.2

#### Firmware update

The device's firmware should always be kept up to date. Theben provides tools with which the device's firmware status can be checked.

Theben IP Tool can be used for a firmware update in non-secure mode.  
It can be downloaded free of charge from our website.

The device cannot be updated with the IP Tool in KNX Secure mode.  
In this case, the firmware update will be possible only with the ETS app "Theben Update App".

#### **Important**

During the update process, the KNX bus (TP) must be connected in addition to the IP network (LAN) so that the KNX parameters can be restored correctly.

Otherwise, the update process will fail.

It must be ensured that no voltage failure (KNX or IP) occurs during the update process, otherwise the device can be destroyed.

### 5 Contact

**Theben AG**

Hohenbergstraße 32  
72401 Haigerloch  
GERMANY

Tel.: +49 7474 692-0  
Fax: +49 7474 692-150  
e-mail: [info@theben.de](mailto:info@theben.de)

**Further information and local contacts:**

[www.theben.de](http://www.theben.de)

**Note:**

We reserve the right to make technical changes or modify the contents of this document without prior notice.

The agreed properties are definitive for any orders placed. Theben AG does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein.

Reproduction, transfer to third parties or processing of the content – including sections thereof – is not permitted without prior expressed written permission from Theben AG.

Copyright© 2020 Theben AG  
All rights reserved

# IPsecure Interface KNX

## Appendix

### **6 Open source software components (OSS)**

A list of the open source components used is available on the Internet at:

<https://www.theben.de/OSS>