WEINZIERL

KNX IP interface and object server

KNX IP BAOS 774.1 *secure*

Operation and installation manual
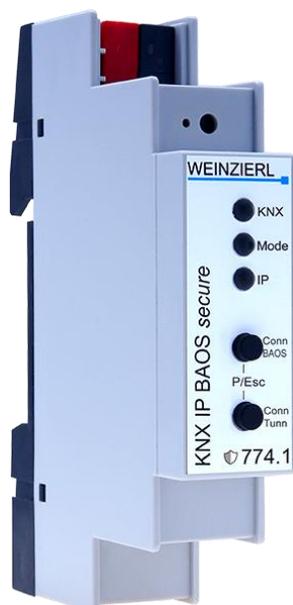
(Art. # 5475)

WEINZIERL ENGINEERING GmbH

Achatz 3-4

84508 Burgkirchen an der Alz

GERMANY

Tel.:   +49 8677 / 916 36 – 0

E-Mail: info@weinzierl.de

Web: www.weinzierl.de

Content

1 Application

The KNX IP BAOS 774.1 *secure* is a universal interface to the KNX bus. BAOS is an acronym for "Bus Access and Object Server". Communication to KNX is possible both on telegram level (KNXnet/IP Tunneling) and on data point level (KNX Application Layer). Clients can directly access KNX Group Objects via either a Binary Protocol (over TCP/IP or UDP/IP) or via JSON (Java Script Object Notation) Web Services.

The device is configured with the ETS and supports up to 1000 Group Objects. The main purpose of the KNX IP BAOS device is connecting non KNX devices and applications to the KNX bus. Implementing the BAOS protocol enables a full integration into the KNX system including ETS support.

The generic ETS entry provides a flat list of data points and parameters. It can be used for rapid integration and for development purpose. For dedicated applications individual ETS entries can be created by OEM manufacturers.

The buttons are for diagnostic purposes. The LEDs indicate the operating status and communication errors on the bus. Power is supplied via the KNX bus

1.1 Programming Interface

The KNX IP BAOS 774.1 *secure* can be used as an interface to KNX. The KNX bus can be accessed from any point in the LAN. For this purpose, an additional individual address must be assigned. This is described in the following sections.

1.2 Object Server

The KNX system is based on a specific protocol that is difficult to implement for non-KNX devices. The KNX IP BAOS 774.1 *secure* maps KNX data to an IT friendly API (Application Programming Interface). It greatly reduces the effort to connect e.g. control or visualization tools to KNX.

The KNX IP BAOS protocol is available in the following versions:

- KNX IP BAOS Binary V2:
  A binary protocol that is especially suitable for small microcontroller.
- KNX IP BAOS Web Services:
  A URL based protocol with JSON syntax

Protocol descriptions can be downloaded at the KNX IP BAOS 774.1 *secure* product site (at www.weinzierl.de).

1.3   Application specific Gateway

To connect to non KNX systems, the KNX IP BAOS 774.1 *secure* can be used as an application specific Gateway (e.g. to connect heating devices, audio applications and many more). For development purposes the generic ETS product entry (with up to 1000 data points as a flat list) is available. Of course, individual product entries can be developed.

1.4   BAOS SDK

For the development of application specific solutions the BAOS protocol must be implemented in the client. For a quick and easy integration of BAOS Binary Services a free SDK is available. More information about the BAOS SDK and the free download can be found at www.weinzierl.de.

2   Installation and connection

The KNX IP BAOS 774.1 *secure* is designed for installation on a DIN rail with a width of 1 unit (18mm). It features the following controls and displays:
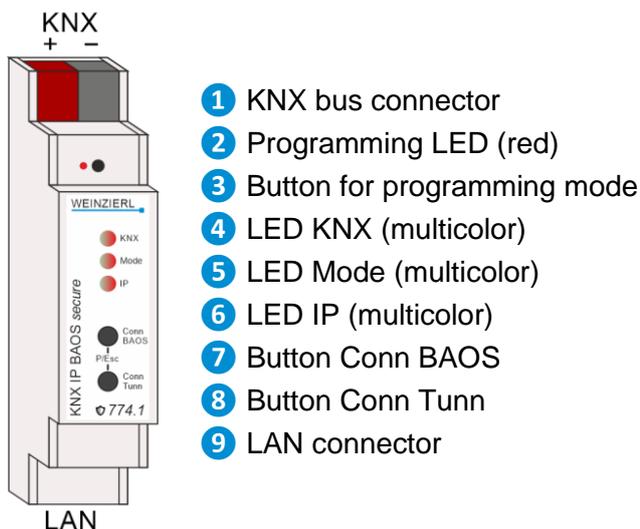
1. KNX bus connector
2. Programming LED (red)
3. Button for programming mode
4. LED KNX (multicolor)
5. LED Mode (multicolor)
6. LED IP (multicolor)
7. Button Conn BAOS
8. Button Conn Tunn
9. LAN connector

If the bus voltage is missing, the device is without function.

2.1 KNX programming mode

The KNX programming mode is activated/deactivated either by pressing the recessed KNX programming button ❸ or by simultaneously pressing the buttons (P/Esc) ❼ and ❽.

When the programming mode is active, the programming LED ❷ and the LED Mode ❺ light up red.

The operation/visualization of the programming mode on the front can be activated/deactivated in the ETS® on page general settings.

2.2 Manual operation and status display

The LED KNX ❹ lights up green if the device is successfully powered by the KNX bus. This LED indicates telegram traffic on the KNX bus by flickering.

Communication failures (e.g. repetitions of telegrams or telegram fragments) are indicated by a short change of the LED color to red.

Overview of the different indications of the LED KNX ❹:

LED Status	Meaning
LED lights green	KNX bus voltage present.
LED flickers green	Telegram traffic on the KNX bus.
LED briefly red	Error in the communication on the KNX bus.

The LED IP ❻ lights up when an Ethernet link is active. This LED is green if the device has valid IP settings (IP address, Sub net and Gateway). With invalid or nonexistent IP settings the LED is red. This is also the case if e.g. the device has not yet received the IP settings by a DHCP server.

This LED indicates IP telegram traffic by flickering.

Overview of the different indications of the LED IP ❻:

LED Status	Meaning
LED lights green	The device has an active ethernet link and valid IP settings.
LED lights red	The device has an active ethernet link and invalid IP settings or has not yet received IP settings from the DHCP server.
LED flickers green	IP telegram traffic.

The LED Mode ❺ can visualize the status of each BAOS and KNXnet/IP tunneling connection.

With the button Conn BAOS ❼ you can chose each single BAOS connection. Pressing the button Conn BAOS ❼ counts the connection numbers up. The actually selected connection number is indicated by flashing (1x…10x) of the LED Mode ❺. An available BAOS connection is indicated by a green LED and a used BAOS connection is indicated by an orange LED.

With the button Conn Tunn ⑧ you can chose each single KNXnet/IP Tunneling connection. Pressing the button Conn Tunn ⑧ counts the connection numbers up. The actually selected connection number is indicated by flashing (1x…5x) of the LED Mode ⑤. An available KNXnet/IP Tunneling connection is indicated by a green LED and a used tunneling connection is indicated by an orange LED.

Via the Escape function (Esc) this indication can be ended by simultaneously pressing button Conn BAOS ⑦ and button Conn Tunn ⑧.

If neither programming mode nor manual mode are active the LED Mode ⑤ can visualize configuration errors.

Overview of the different indications of the LED Mode ⑤:

LED Status	Meaning
LED lights green	The device operates in normal operating mode.
LED lights red	The programming mode is active.
LED flashes green 1x…10x	Programming mode is not active. Manual operation is active. The selected BAOS conn. (1…10) is not used and free.
LED flashes orange 1x…10x	Programming mode is not active. Manual operation is active. The selected BAOS conn. (1…10) is used.
LED flashes green 1x...5x	Programming mode is not active. Manual operation is active. The selected tunnel (1…5) is not used and free.
LED flashes orange 1x…5x	Programming mode is not active. Manual operation is active. The selected tunnel (1…5) is used.
LED flashes red	The programming mode is not active. The device is not loaded correctly, e.g. after aborting a download.

3 Reset to factory default settings

It is possible to reset the device to its factory default settings.

- Disconnect the KNX bus connector ① from the device.
- Press the KNX programming button ③ and keep it pressed down.
- Reconnect the KNX bus connector ① to the device.
- Keep the KNX programming button ③ pressed for at least another 6 seconds.
- A short flashing of all LEDs (②④⑤⑥) visualizes the successful reset of the device to factory default settings.

In the factory default settings, the device has the physical address 15.15.255 and no group addresses are connected. Also, KNX Data Security is disabled and the initial key (FDSK) must be used for secure commissioning.

3.1 Factory default settings

Individual addresses and KNXnet/IP tunneling connections

Individual address: 15.15.255
Active KNXnet/IP tunneling connections: 1
Individual address of the tunneling connection: 15.15.240
IP address assignment: DHCP

4 Wiring scheme
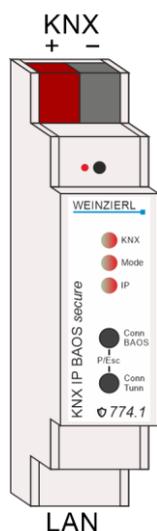
5 KNX Security

The KNX standard was extended by KNX Security to protect KNX installations from unauthorized access. KNX Security reliably prevents the monitoring of communication as well as the manipulation of the system.

The specification for KNX Security distinguishes between KNX IP Security and KNX Data Security. KNX IP Security protects the communication over IP while on KNX TP the communication remains unencrypted. Thus, KNX IP Security can also be used in existing KNX systems and with non-secure KNX TP devices.

KNX Data Security describes the encryption on telegram level. This means that the telegrams on the twisted pair bus or via RF (radio frequency) are also encrypted.

Encrypted telegrams are longer than the previously used unencrypted ones. For secure programming via the bus, it is therefore necessary that the interface used (e.g. USB) and any intermediate line couplers support the so called KNX Long Frames.

6 Interface settings in the ETS

6.1 ETS 5

In the ETS 5, interfaces can be selected and configured via the ETS menu "Bus – Interfaces". All available connections are listed under "Discovered Interfaces". After clicking on the desired connection, connection specific information and options appear on the right side of the ETS window. The selected connection can be selected as the "Current Interface" via the "Select" button.

6.2   ETS 6

In the ETS 6, interfaces can be selected and configured in the ETS project via the "Interface" button. All available connections are listed here.
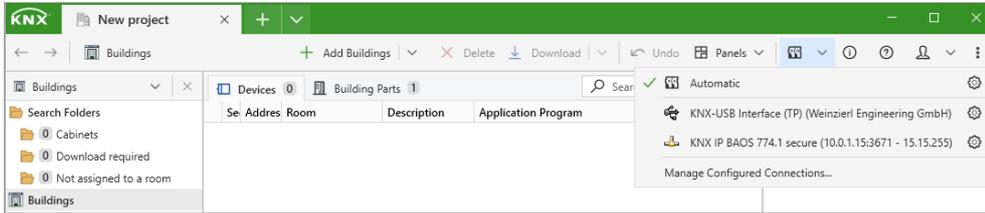
By clicking on a connection, this is selected as the desired interface.

By clicking the gear next to the desired connection, the connection specific information and options appear.
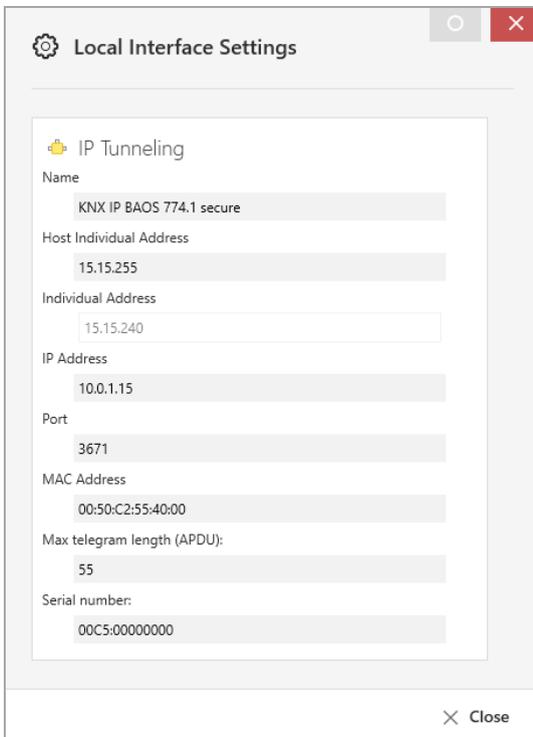
6.3 Common

The displayed device name and the "Host Individual Address" (individual address of the device) can then be changed via the database entry within your ETS project.

The KNX IP BAOS 774.1 *secure* supports up to 8 connections simultaneously. A separate individual address is used for each connection.

The ETS can access configured IP interfaces even without a database entry. If the configuration does not correspond to the conditions of the installation, it must be adapted via the database entry within your ETS project.

The individual KNX device address as well as the individual KNX addresses for the additional tunneling connections can be changed via the database entry within the ETS project after the device has been added to the project. See section "ETS database – Additional individual addresses".

Like all programmable KNX devices, the KNX IP BAOS 774.1 *secure* has a individual address with which the device can be addressed. This is used, for example, by the ETS when downloading the interface via the KNX bus.

For the interface function, the device uses additional individual addresses that can be set in the ETS (for ETS5.7 or newer). If a client (e.g. ETS) sends telegrams to the KNX bus via the KNX IP BAOS 774.1 *secure*, these contain one of the additional addresses as the sender address. Each address is assigned to a connection. In this way, response telegrams can be forwarded clearly to the respective client.

The additional individual addresses must be from the address range of the bus line in which the interface is located and must not be used by another device.

Example:

Individual address: *1.1.10 (device address in the topology)*
KNXnet/IP tunneling connection 1:   *1.1.240 (1. additional individual address)*
KNXnet/IP tunneling connection 2:   *1.1.241 (2. additional individual address)*
KNXnet/IP tunneling connection 3:   *1.1.242 (3. additional individual address)*
KNXnet/IP tunneling connection 4:   *1.1.243 (4. additional individual address)*
KNXnet/IP tunneling connection 5:   *1.1.244 (5. additional individual address)*
KNXnet/IP tunneling connection 6:   *1.1.245 (6. additional individual address)*
KNXnet/IP tunneling connection 7:   *1.1.246 (7. additional individual address)*
KNXnet/IP tunneling connection 8:   *1.1.247 (8. additional individual address)*

7 Programming

The KNX IP BAOS 774.1 *secure* can be programmed by the ETS via different ways.

7.1 Via KNX bus

For this purpose, the device must only be connected to the KNX bus. The ETS requires an additional interface (e.g. USB) to the KNX bus. Via this way, both the individual address and the entire application including IP configuration can be programmed. Programming via the KNX bus is recommended if no IP connection can be established.

7.2 Via KNXnet/IP tunneling

No additional interface is required here. Programming via KNXnet/IP tunneling is possible if the device already has a valid IP configuration (e.g. via DHCP or Auto IP). In this case, the device is displayed in the interfaces in the ETS and must be selected. The download takes place from the ETS project, as with other devices.

7.3 Via direct IP connection

While both KNXnet/IP tunneling and KNXnet/IP routing are limited to the speed of KNX TP, a direct IP connection allows the device to be loaded at high speed. The direct IP connection is possible if the device already has both a valid IP configuration and an individual address.

Due to the significantly shorter transmission times, it is recommended to perform downloads via IP.

ETS 5

In ETS 5, the selection "Use direct IP connection if available" can be selected in the menu under "Bus – Connections – Options". The download then takes place directly in the device and is not visible in the ETS group monitor.
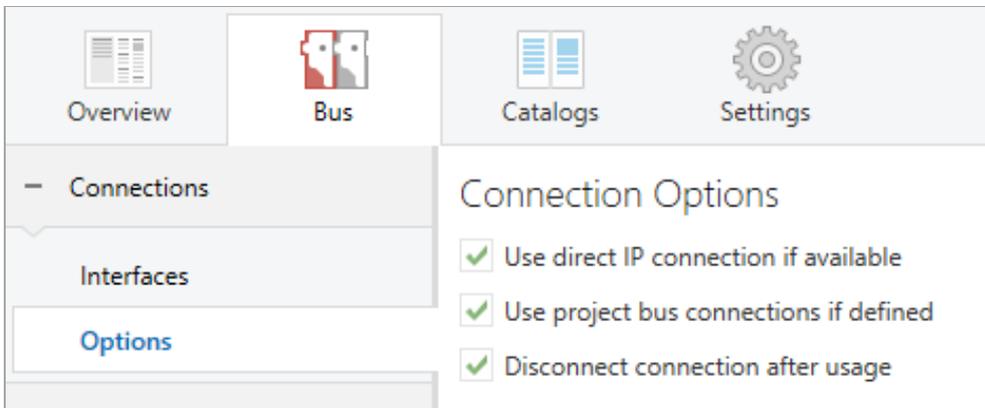
ETS 6

In ETS 6, interfaces can be selected and configured in the ETS project via the "Interface" button. All available connections are listed here.
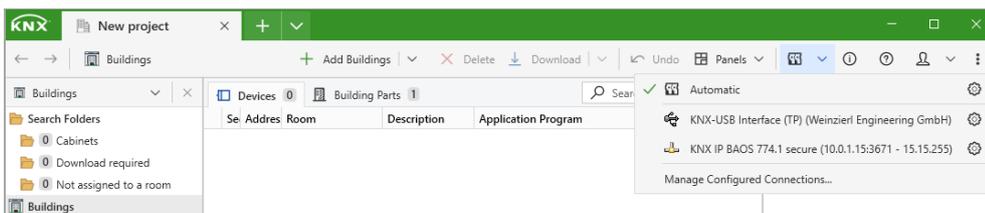
By clicking on "Automatic" selects the "Automatic Bus Connection".

By clicking the gear next to "Automatic" the specific options appear.
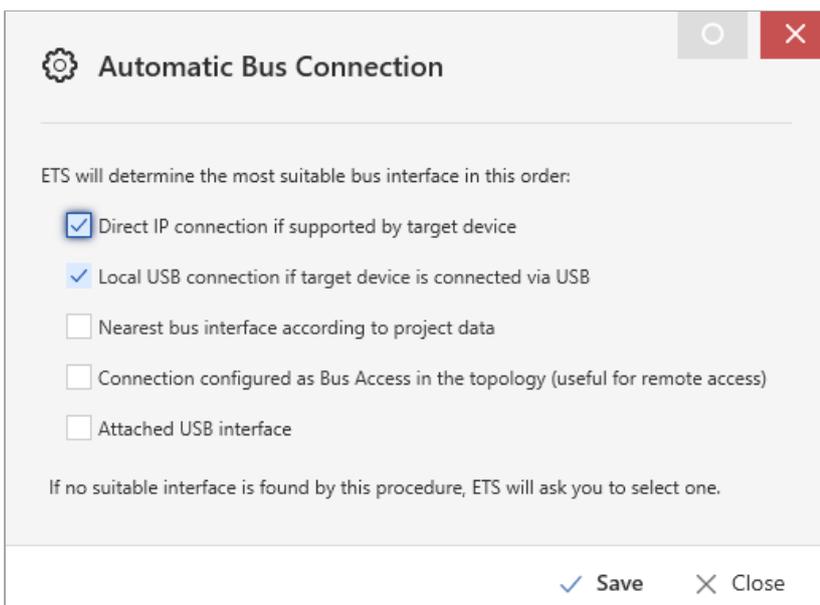
Here, the selection "Direct IP connection if supported by target device" can be selected. The download then takes place directly in the device and is not visible in the ETS group monitor.

8 ETS database

The ETS 5 database (for ETS 5.7 or newer) can be downloaded from the product website of the KNX IP BAOS 774.1 *secure* (www.weinzierl.de) or from the ETS online catalogue.

The KNX IP BAOS 774.1 *secure* supports KNX Data Security to protect the device against unauthorized access from the KNX bus. If the device is programmed via the KNX bus, this is done with encrypted telegrams.

8.1 Secure commissioning

If the first product is inserted into a project with KNX Security, the ETS prompts you to enter a project password.
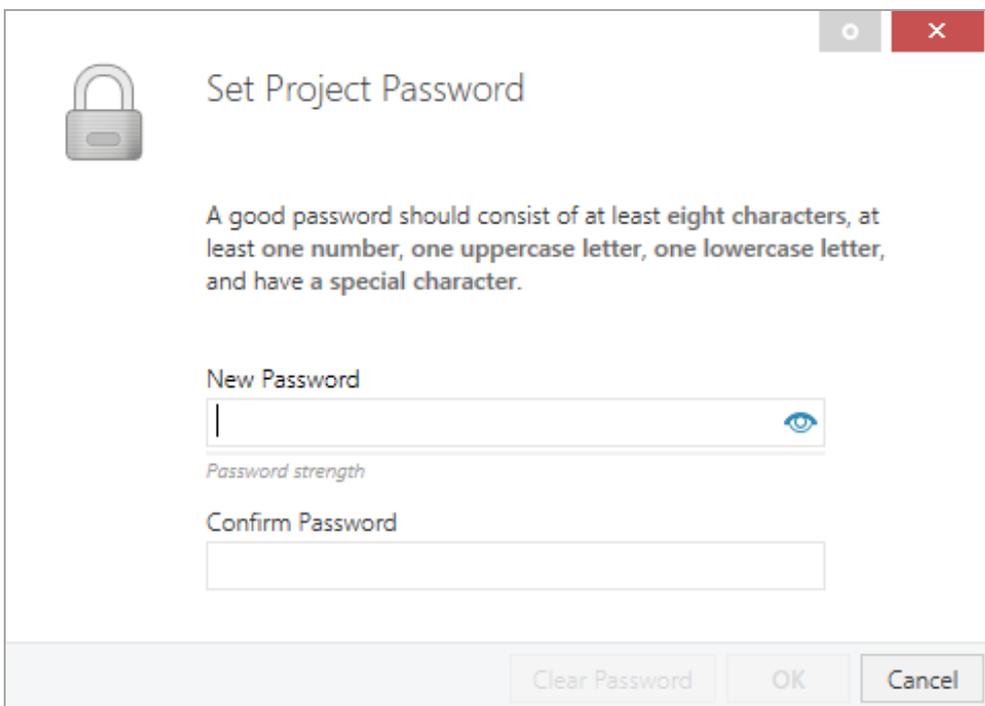
This password protects the ETS project from unauthorized access. This password is not a key that is used for KNX communication. The entry of the password can be bypassed with "Cancel", but this is not recommended for security reasons.

ETS requires a device certificate for each device with KNX Security that is created in the ETS. This certificate contains the serial number of the device as well as an initial key (FDSK = Factory Default Setup Key).
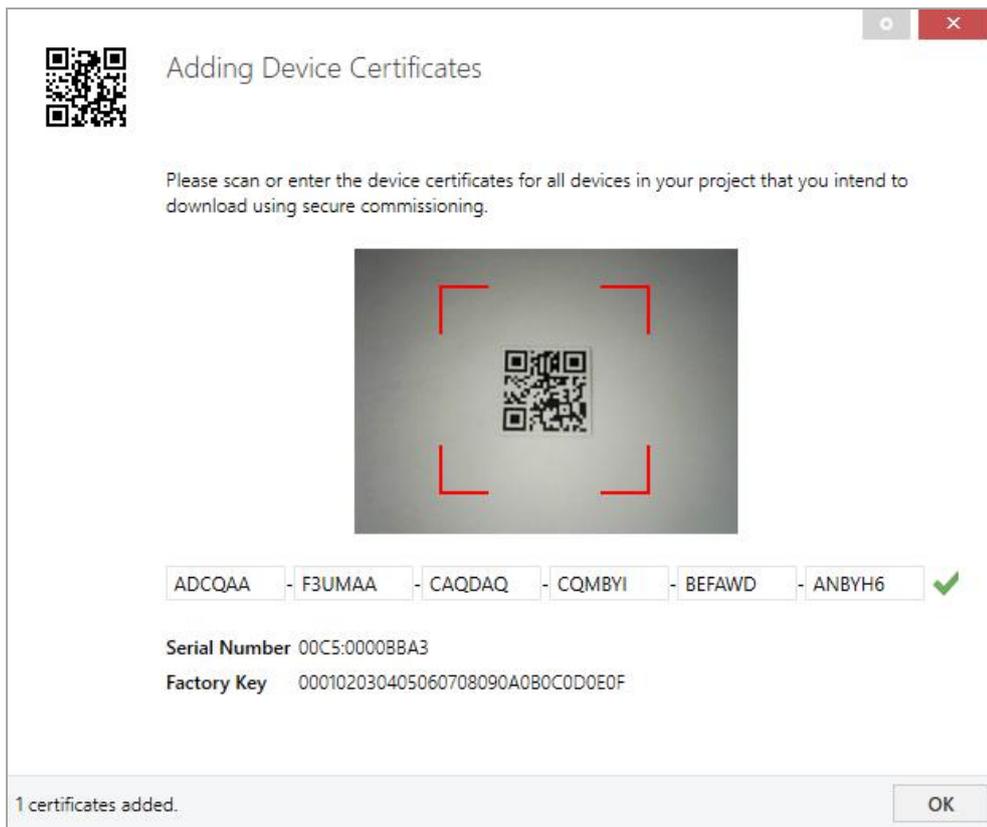
The certificate is printed as text on the device. It can also be scanned from the printed QR code via a webcam.

The list of all device certificates can be managed in the ETS panel Reports – Project Security.

This initial key is required to safely put a device into operation from the start. Even if the ETS download is recorded by a third party, the third party has no access to the secured devices afterwards. During the first secure download, the initial key is replaced by the ETS with a new key that is generated individually for each device. This prevents persons or devices who may know the initial key from accessing the device. The initial key is reactivated after a reset to factory default settings.

The serial number in the certificate enables the ETS to assign the correct key to a device during a download.

In the ETS project in the properties of the device, secure commissioning can be activated and the device certificate can be added:
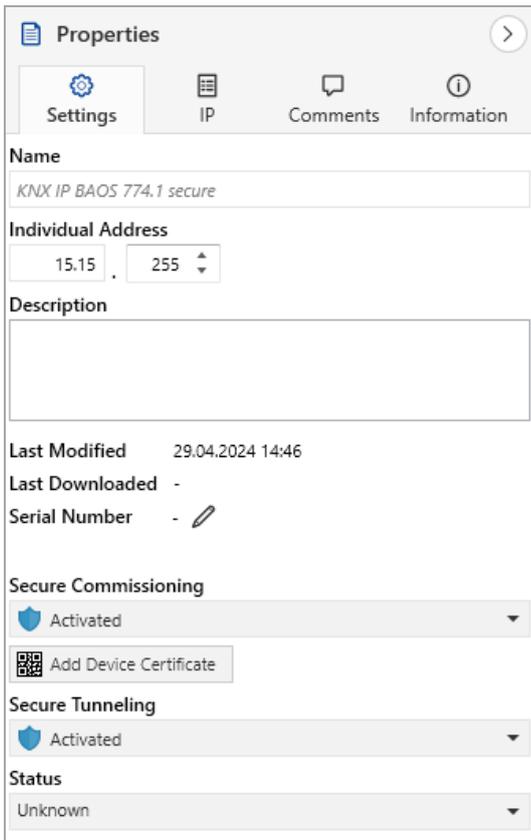
8.2 Secure group communication

Each object of the device can communicate either encrypted or unencrypted. The encryption is set under "Security" in the properties of the used group address:

The setting "Automatic" activates encryption if both objects to be connected can communicate encrypted. Otherwise encrypted communication between the objects is not possible.

In the overview of communication objects in the ETS project, secured objects can be recognized by a shield symbol:

	Security	Number ▲	Name	Object Function	Description	Group Address
⬛↯	🛡	11	Button A0: Object a	Switch	Switch a	1/1/1
⬛↯		12	Button A0: Object b	Switch	Switch b	1/1/2
⬛↯	🛡	21	Button A1: Object a	Switch	Switch a	1/1/1
⬛↯		22	Button A1: Object b	Switch	Switch b	1/1/2

A separate key is automatically generated by the ETS for each secured group address. These keys can also be checked in the ETS panel Reports – Project Security. To enable all devices to communicate with a secure group address, the keys must be known to all. Therefore a download must be made into all devices that use this group address when a key is created or changed. A key is changed by the ETS e.g. when the encryption of a group address is switched off and on again.

8.3   Additional individual addresses

The additional individual addresses appear in the topology view.
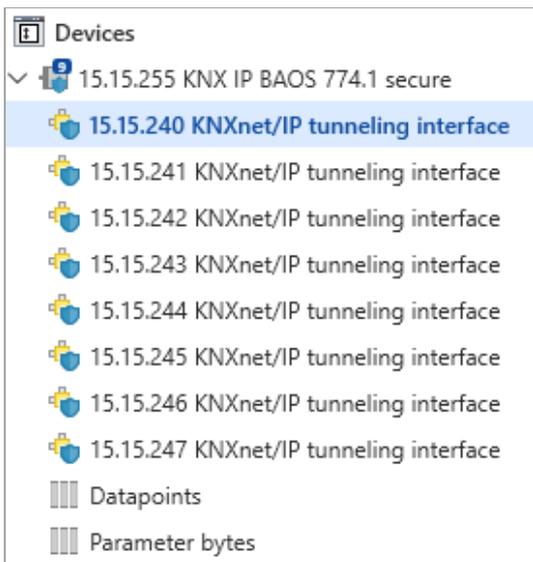
To change the individual addresses, select the corresponding entry in the list and enter the desired address in the text field under "Properties – Settings". If the frame of the text field changes its colour to red after entry, this indicates that the address entered is already being used. The changes are only applied in the device after download.

Properties

Settings | Comments | Information

Name

Individual Address

15.15 . 240

Description

Password

>ugX9Zgw

Secure Group Addresses

Supported

Export Interface Information

Make sure that none of the specified addresses are already used in your KNX installation.

8.4 IP settings

By marking the KNX IP BAOS 774.1 *secure* in the tree structure of the topology view of the ETS project, the overview "Properties" appears on the right side of the ETS window.

8.4.1 Device name (user friendly name)

Under Properties menu item "Settings", the device name (user friendly name) of the KNX IP BAOS 774.1 *secure* can be changed. The first 30 characters are used.
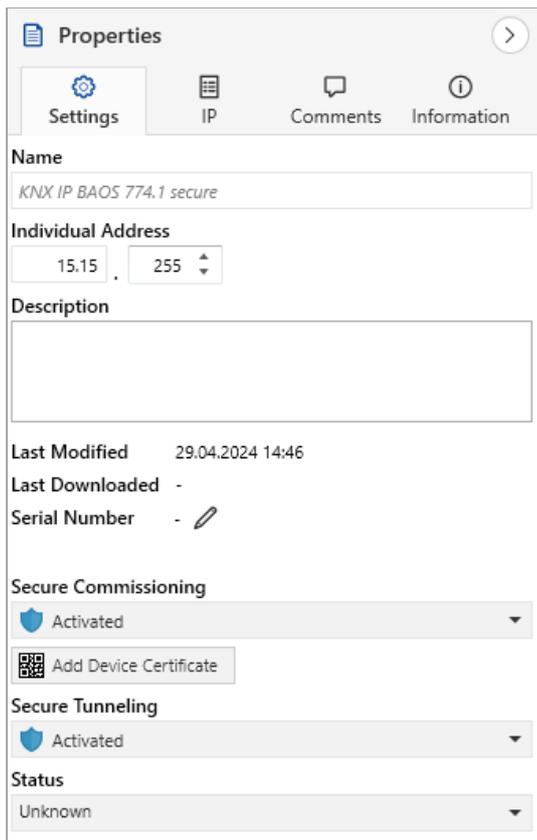
ℹ️ *The change made will only take effect after an ETS download.*

8.4.2 IP configuration

Under Properties menu item "IP", the IP specific options of the KNX IP BAOS 774.1 *secure* can be changed.
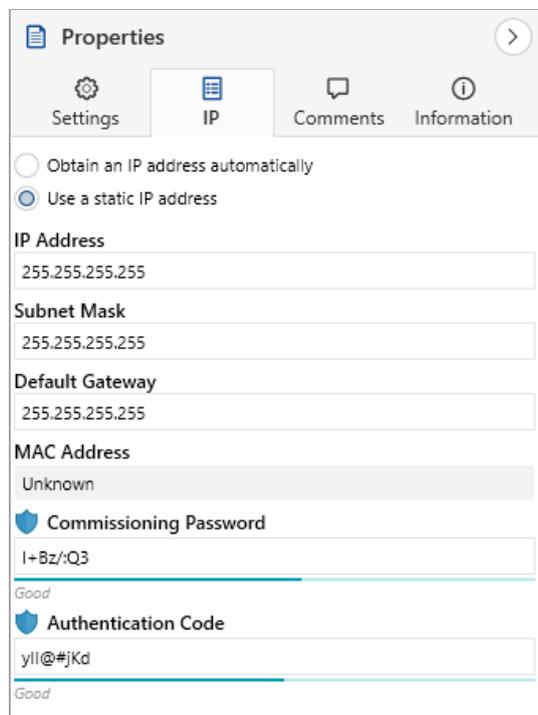
 The change made will only take effect after an ETS download.

By switching from "Obtain an IP address automatically" (via DHCP) to "Use a static IP address" (static IP address), the IP address, subnet mask and standard gateway can be freely selected.

IP Address

The IP address of the KNX IP BAOS 774.1 *secure* must be entered here. This is used to address the device via the IP network (Wi-Fi). The IP addressing should be coordinated with the administrator of the network.

Subnet Mask

The subnet mask must be entered here. This mask is used by the device to determine whether a communication partner is located in the local network. If a partner is not in the local network, the device does not send the telegrams directly to the partner, but to the standard gateway, which takes over the forwarding.

Default Gateway

Enter the IP address of the gateway here, e.g. the access point of the installation.

Example for the assignment of IP addresses

The KNX IP BAOS 774.1 *secure* is to be accessed with a PC.

IP address of PC: 192.168.1.30
Subnet mask of PC: 255.255.255.0

The KNX IP BAOS 774.1 *secure* is located in the same local network, i.e. it uses the same subnet. The assignment of the IP address is restricted by the subnet, i.e. in this example the IP address of the IP interface must be 192.168.1.xx, xx can be a number from 1 to 254 (with the exception of 30, which has already been used). Care must be taken not to assign addresses twice.

IP address of KNX IP BAOS 774.1 secure*: 192.168.1.31*
Subnet mask of KNX IP BAOS 774.1 secure*: 255.255.255.0*

Remote access

Remote access via Internet is possible with the KNX IP BAOS 774.1 *secure*. More details can be found in the document "Remote access with the ETS" at www.weinzierl.de.

8.5 Description

Description

General settings

+ Datapoints

+ Parameter bytes

KNX IP BAOS 774.1 secure
KNX IP interface and object server

WEINZIERL

The KNX IP BAOS 774.1 secure is used as Interface for connecting to KNX
both on telegram level (KNXnet/IP Tunneling) and on datapoint level
(KNX Application Layer).

Clients can directly access group objects over TCP/IP
via a binary protocol.

The device is configured with the ETS and supports up to 1000 group objects.
10 simultaneous client connections are supported via the BAOS protocol.

BAOS is an acronym for "Bus Access and Object Server". It is possible to
connect to the KNX bus everywhere over LAN. Bus connection over the internet
with KNX IP BAOS 774.1 secure is also possible.

The buttons are for diagnostic purposes. The LEDs indicate the operating
status and communication errors on the bus.

Power is supplied via the KNX bus.
The device supports KNX Security and BAOS Security.

Wiring scheme:

Please consult device data sheet and manual for further information.

Contact:

WEINZIERL ENGINEERING GmbH
Achatz 3-4
84508 Burgkirchen an der Alz
GERMANY
www.weinzierl.de
info@weinzierl.de

This page shows the device description and the corresponding connection diagram.

8.6 General settings

Prog. mode on device front

In addition to the normal programming button ❸ the device allows activating the programming mode on the device front without opening the switchboard cover. The programming mode can be activated and deactivated via pressing simultaneously both buttons ❼ and ❽.

This feature can be enabled and disabled via the parameter Prog. mode on device front. The recessed programming button ❸ (next to the programming LED ❷) is always enabled and is not affected by this parameter.

Manual operation on device

This parameter is used to configure manual operation on the device. Manual operation can be activated or deactivated. After the configured time limit, the normal operating status is automatically restored.

BAOS services

The BAOS services can be enabled or disabled here. The following are available:

- Disabled
- Enabled
- Enabled (auto connect)
  This mode is used for the downward compatibility of existing installations that used the earlier model KNX IP BAOS 774, for example. The communication is "connectionless".

Communication

This parameter can be used to set whether BAOS communication is secure or unsecure.

Password *(only for secure communication)*

The password for secure BAOS communication can be set here.

Object server port

The TCP port which is used for the BAOS communication can be set here.

8.7 Datapoint N – M

A maximum of 1000 data points can be parameterized. Each data point can be assigned a group address to send to the bus. Several group addresses can be assigned per object for reception.

Description for this page

A description for this page can be assigned here. This text is displayed dynamically in the lefthand column as the name of the parameter page. This provides a better overview in the project.

Datapoint type

The datapoint type (DPT) can be set for each datapoint.
The following datapoint types are available:

- DPT 1.001 – Switch – 1 bit
- DPT 2.001 – Switch with control – 2 bits
- DPT 3.007 – Dimming up/down – 4 bits
- DPT 4.001 – Character ASCII – 1 byte
- DPT 5.001 – Percent value – 1 byte
- DPT 6.010 – Signed value – 1 byte
- DPT 7.001 – Unsigned value – 2 bytes
- DPT 8.001 – Signed value – 2 bytes
- DPT 9.001 – Temperature – 2 bytes
- DPT 10.001 – Time – 3 bytes
- DPT 11.001 – Date – 3 bytes
- DPT 12.001 – Unsigned value – 4 bytes
- DPT 13.001 – Signed value – 4 bytes
- DPT 14.000 – Acceleration – 4 bytes
- DPT 15.000 – Access data – 4 bytes

- DPT 16.000 – String ASCII – 14 bytes
- DPT 17.001 – Scene – 1 byte
- DPT 18.001 – Scene with control – 1 byte
- DPT 19.001 – Date and time – 8 bytes
- DPT 20.102 – HVAC mode – 1 byte
- DPT 232.600 – Color RGB – 3 bytes
- DPT 251.600 – Color RGBW – 6 bytes

If a required DPT cannot be selected, e.g. "DPT 9.007 – Relative humidity – 2 bytes", a similar DPT with a suitable length must be selected "DPT 9.001 – Temperature – 2 bytes". This must be adapted in the ETS.

Description

A description for the object can be assigned here. This text is displayed dynamically for the corresponding group object. This provides a better overview in the project.
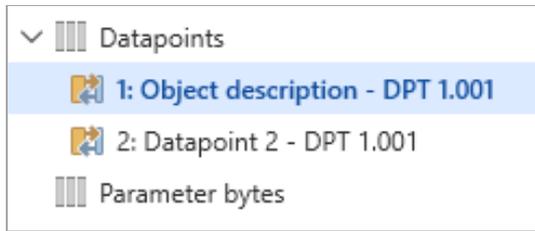
- Datapoint 1 with description text
- Datapoint 2 without description text

8.8 Parameter byte N – M

Description for this page

A description for this page can be assigned here. This text is displayed dynamically in the lefthand column as the name of the parameter page. This provides a better overview in the project.

Parameter byte

A value between 0 … 255 can be set for each parameter byte.

Description

A description for the parameter byte can be assigned here.
This provides a better overview in the project.

WEINZIERL

> ⚠ **WARNING**
>
> - The device must be mounted and commissioned by an authorized electrician.
> - The prevailing safety rules must be heeded.
> - The device must not be opened.
> - For planning and construction of electric installations, the relevant guidelines, regulations and standards of the respective country are to be considered.

KNX

Product database for ETS 5/6
www.weinzierl.de/en/products/774.1/ets6

Data sheet
www.weinzierl.de/en/products/774.1/datasheet

CE Declaration
www.weinzierl.de/en/products/774.1/ce-declaration

WEINZIERL ENGINEERING GmbH
Achatz 3-4
84508 Burgkirchen an der Alz
GERMANY

Tel.: +49 8677 / 916 36 – 0
E-Mail: info@weinzierl.de
Web: www.weinzierl.de

2024-05-07