KNX IP interface with WiFi

KNX IP Interface 740.2 *wireless secure*

Operation and installation manual

(Art. # 5537)

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 Interface 740.2 *wireless secure* serves as a wireless interface to the KNX bus based on WiFi. The device can be used as a programming interface for the ETS® and is a wireless alternative to USB or wired IP interfaces. The bus access via WiFi allows the installer to move freely in the building with his laptop to a large extent.

The KNX IP Interface 740.2 *wireless secure* has an integrated WiFi access point to which the laptop can connect. Alternatively, the device can be connected to an existing WiFi in client mode, the connection can be made via WPS (WiFi Protected Setup).

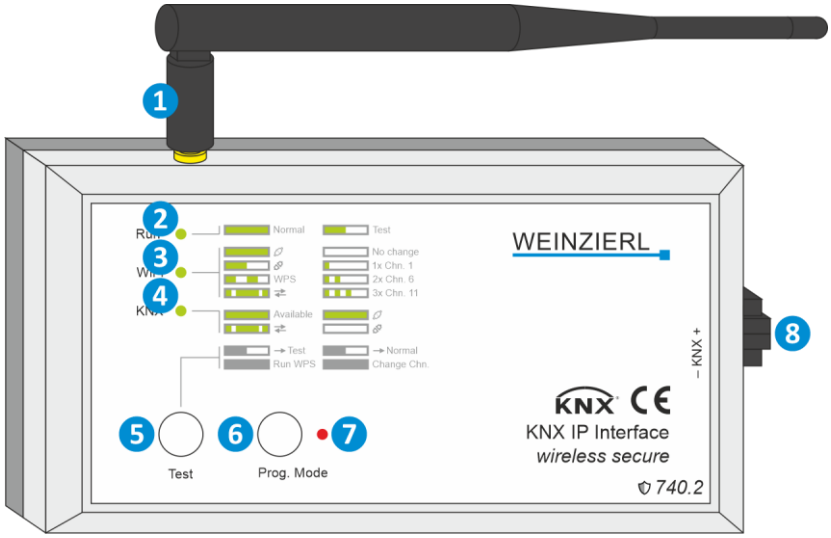
The device supports the security standard WPA2 as well as KNX Security.

Power is supplied via the KNX bus.

The device works according to the KNXnet/IP specification. It can be used with the ETS® from version 5.

2 Installation and connection

The housing of the KNX IP Interface 740.2 *wireless secure* has the dimensions 125 x 67 x 31 mm (L x W x H). It features the following controls and displays:



1 Antenna
2 LED Run (green)
3 LED WiFi (green)
4 LED KNX (green)
5 Button Test
6 Button Prog. Mode
7 Programming LED
8 KNX bus connector

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

2.1 KNX programming mode

The KNX programming mode is activated/deactivated by pressing the KNX programming button 6. When programming mode is active, the programming LED 7 lights up red.

2.2 Manual operation and status display

Summary of the states of the programming LED 7:

LED Status	Meaning
LED lights red	The programming mode is active.
LED flashes red (fast)	The programming mode is not active. The device is not loaded correctly, e.g. after aborting a download.

Pressing the button Test 5 briefly switches between normal operating mode and test mode. The active mode is indicated by the LED Run 2 lighting up or flashing slowly in green.

Summary of the states of the LED Run 2:

LED Status	Meaning
LED lights green	The device operates in normal operating mode.
LED flashes green (slowly)	The device is in test mode.
LED flashes green (fast)	The device is currently loaded by the ETS.

2.2.1 Normal operating mode

The LED WiFi 3 lights up green when a WiFi connection is available. If this LED flickers, telegram traffic is taking place via WiFi. If this LED flashes slowly in green, the device is not connected via WiFi.

Pressing and holding the button Test 5 executes WPS (WiFi Protected Setup). This is indicated by the LED WiFi 3 flashing fast in green.

Summary of the states of the LED WiFi 3:

LED Status	Meaning
LED lights green	The device is connected via WiFi.
LED flashes green (slowly)	The device is not connected via WiFi.
LED flashes green (fast)	WPS is in progress.
LED flickers green	Telegram traffic via WiFi.

The LED KNX 4 lights up green when KNX bus voltage is present. If this LED flickers, telegram traffic is taking place on the KNX bus.

Summary of the states of the LED KNX 4:

LED Status	Meaning
LED lights green	KNX bus voltage present.
LED flickers green	Telegram traffic on the KNX bus.

2.2.2 Test mode

In test mode, the WiFi channel can be changed and the connection status of the tunneling connection can be displayed.

If many participants are using the same WiFi channel, switching to a less heavily used channel can improve the connection quality:

Pressing and holding the button Test 5 switches through the WiFi channels. This is indicated by the LED WiFi 3 flashing green. The selected WiFi channel is activated after exiting the test mode. This is not stored in the device (selection only temporary).

Summary of the states of the LED WiFi 3:

LED Status	Meaning
LED is off	The WiFi channel configured via ETS is selected.
LED flashes 1x green	WiFi channel 1 is selected.
LED flashes 2x green	WiFi channel 6 is selected.
LED flashes 3x green	WiFi channel 11 is selected.

The LED KNX 4 lights up green when the KNXnet/IP tunneling connection is active.

Summary of the states of the LED KNX 4:

LED Status	Meaning
LED lights green	At least one KNXnet/IP tunneling connection is active.
LED is off	No KNXnet/IP tunneling connection is active.

3 Reset to factory default settings

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

- Disconnect the KNX bus connection 8 from the device.
- Press the button Prog. Mode 6 and keep it pressed down.
- Reconnect the KNX bus connection 8 to the device.
- Keep the button Prog. Mode 6 pressed for at least another 6 seconds.
- A short flashing of all LEDs (2 3 4 7) visualizes the successful reset of the device to factory default settings.

3.1 Factory default settings

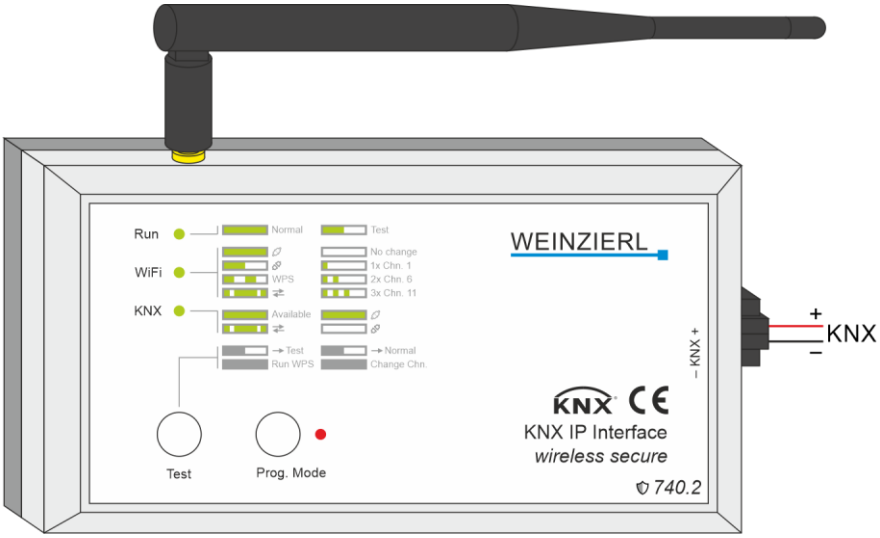
Individual addresses and KNXnet/IP tunneling connections

Individual address: 15.15.255
Active KNXnet/IP tunneling connections: 1
Individual address of the tunneling connection: 15.15.250

Configuration

Device name (SSID): KNX IP Interface 740.2 secure
Mode: Access point
Authentication: WPA2-PSK
Key: Format XXXX-XXXX-XXXX on the device label
WiFi channel: 6

4 Wiring scheme



4.1 Pluggable screw terminal

The screw terminal is used to connect the KNX bus.

4.2 Pin assignment

Connection	Symbol	Description
KNX	+	Positive connection for KNX bus
KNX	-	Ground connection for KNX bus

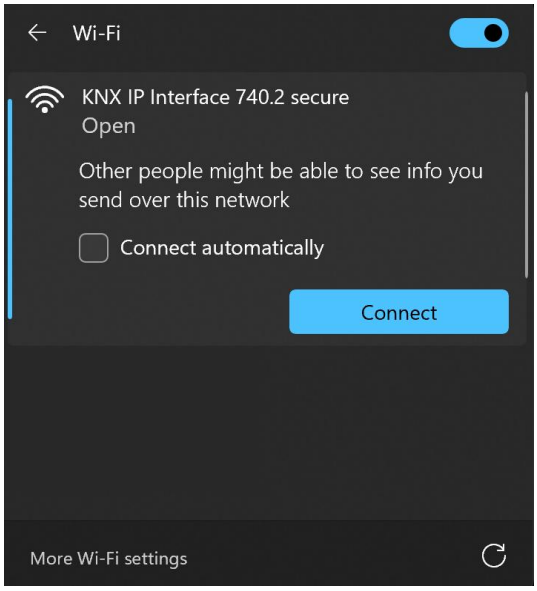
5 Setting up a WiFi connection

5.1 KNX IP Interface 740.2 *wireless secure* is “Access point”

To set up a WiFi connection from a PC or laptop, a WiFi adapter is required. For laptops, this is usually integrated in the device.

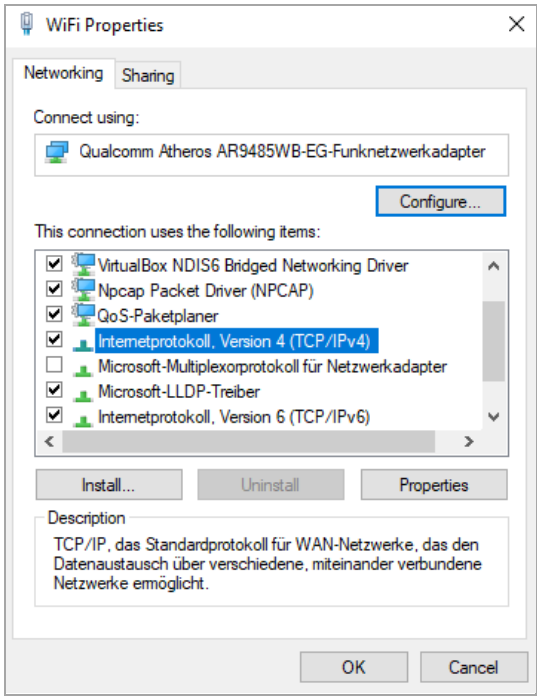
The WiFi connection to the KNX IP Interface 740.2 *wireless secure* is set up as follows:

First, the WiFi provided by the KNX IP Interface 740.2 *wireless secure* must be found. The Windows® “Show available networks” dialog lists all available wireless networks. This dialog can be accessed via “Settings / Network & Internet / Show available networks”. Alternatively, this dialog can be accessed via the corresponding “Network” icon in the notification area at the edge of the screen.

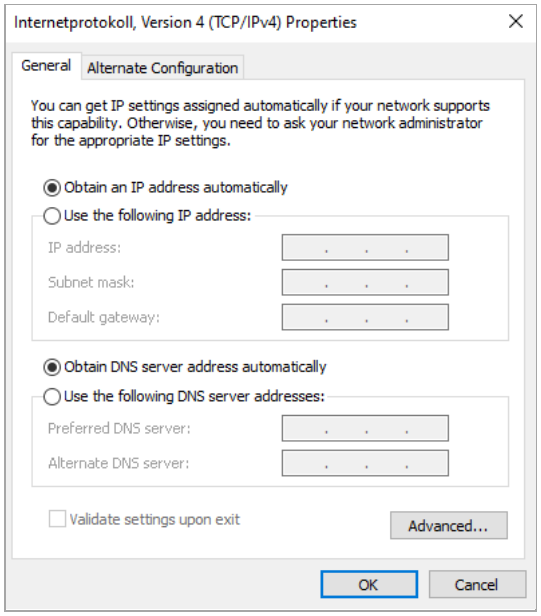


Since the KNX IP Interface 740.2 *wireless secure* has an integrated DHCP server, the IP address of the PC should be set automatically (DHCP). This is the default setting for most laptops.

To change the settings, select the item “Internet Protocol, Version 4 (TCP/IPv4)” in the properties dialog of the wireless network connection and click the “Properties” button.



In the following dialog “Obtain an IP address automatically” should be active.



After setting up the WiFi connection, the KNX IP Interface 740.2 *wireless secure* can be used as an interface to the KNX bus.

5.2 KNX IP Interface 740.2 *wireless secure* is “Station / Client Mode”

The KNX IP Interface 740.2 *wireless secure* automatically setting up the WiFi connection to the configured access point, provided the entered data is correct. The data is entered via the ETS parameter dialog. See the section “ETS database – Operating mode “Station / Client-Mode””.

If configured, the connection can also be established via WPS. For this, the parameter **WPS (WiFi protected setup)** must be set to Temporary or Permanent. To connect, the WPS functions must first be activated on the access point and then the button Test 5 on the KNX IP Interface 740.2 *wireless secure* must be pressed for a long time (at least 1 second). The interface must be in normal operating mode (LED Run 2 lights up green).

After the WiFi connection has been established, the KNX IP Interface 740.2 *wireless secure* can be used as an interface to the KNX bus. This applies to all PCs and laptops in this network.

6 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.

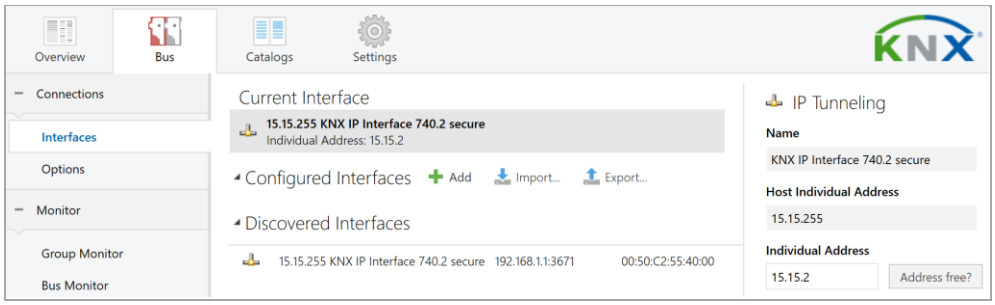
KNX Data Security describes the encryption on telegram level. This means that the telegrams on the twisted pair bus or via RF (radio frequency) are also encrypted.

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.

7 Interface settings in the ETS

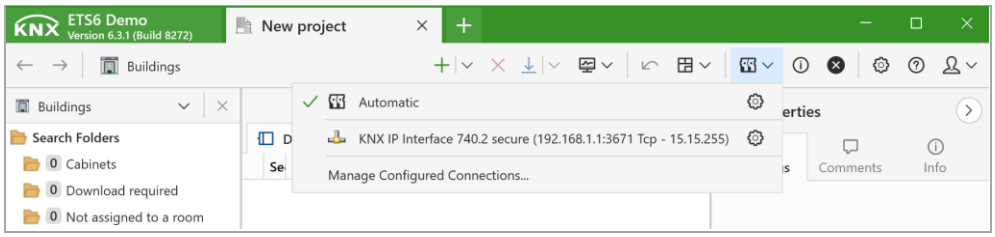
7.1 ETS 5

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.



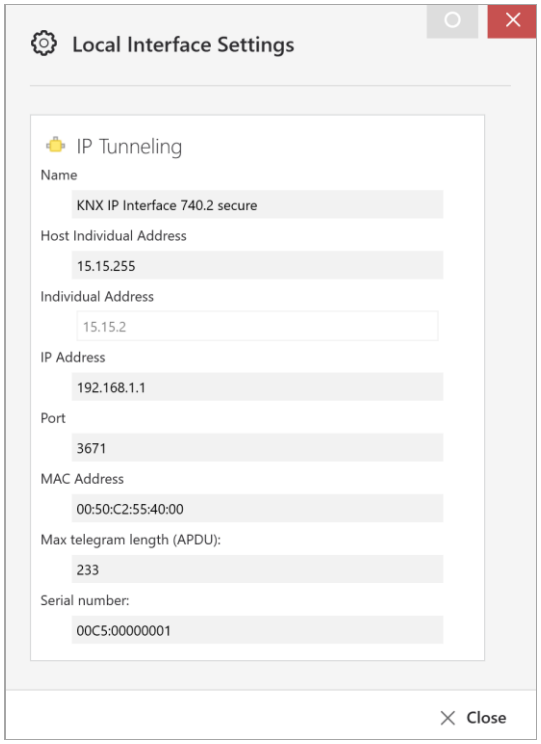
7.2 ETS 6

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.



7.3 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.

In the “Individual address” section, the individual KNX address of the currently used KNXnet/IP tunneling connection can be changed. In order to check whether the desired individual address is not already available in your KNX installation, the button “Address free?” can be pressed.

The KNX IP Interface 740.2 *wireless 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 Interface 740.2 *wireless 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 Interface 740.2 *wireless 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)*

8 Programming

The KNX IP Interface 740.2 *wireless secure* can be programmed by the ETS in various ways.

8.1 Via the KNX bus

For this, the device must only be connected to the KNX bus. The ETS requires an additional interface (e.g. USB) to the KNX bus. 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.

8.2 Via KNXnet/IP tunneling

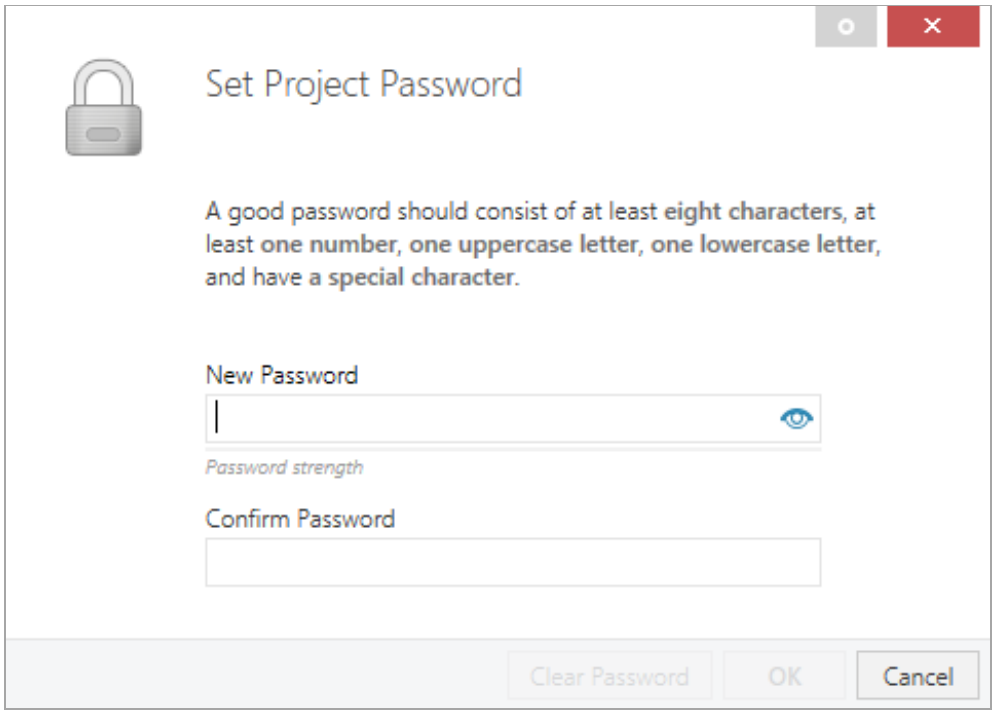
No additional interface is required here. Programming via KNXnet/IP tunneling is possible if the device already has a valid IP configuration (e.g. via DHCP). In this case, the device is displayed in the interfaces in the ETS and must be selected. The download takes place from the ETS project, as with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

9 ETS database

The ETS5 database (for ETS 5.7 or newer) can be downloaded from the product website of the KNX IP Interface 740.2 *wireless secure* (www.weinzierl.de) or from the ETS online catalogue.

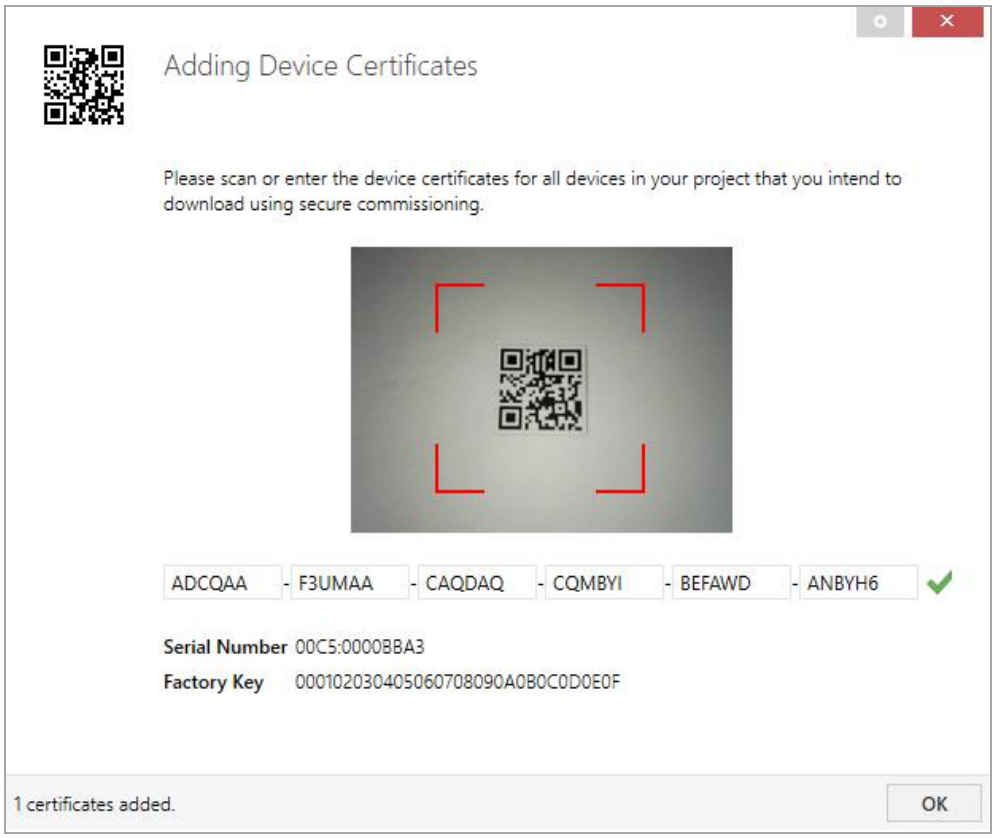
9.1 Secure commissioning

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).



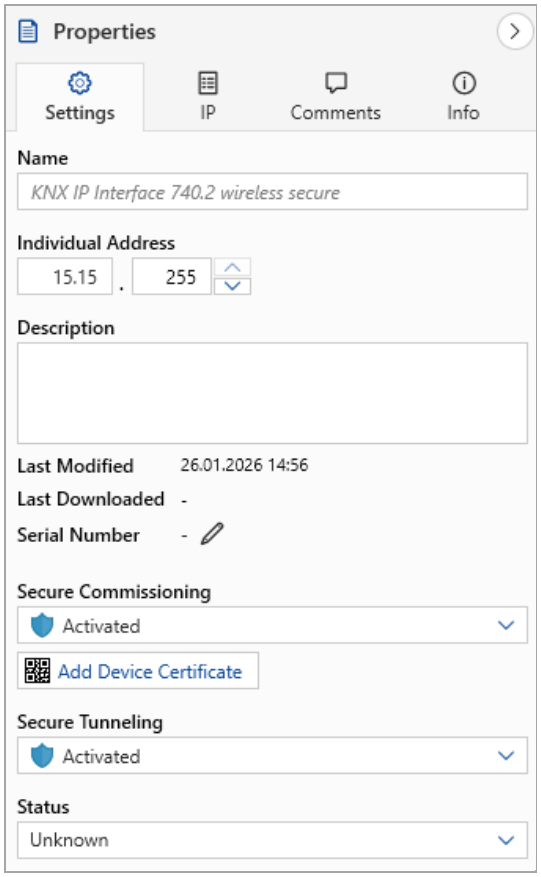
The certificate is printed as text on the device. It can also be scanned from the printed QR code via a webcam.

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.

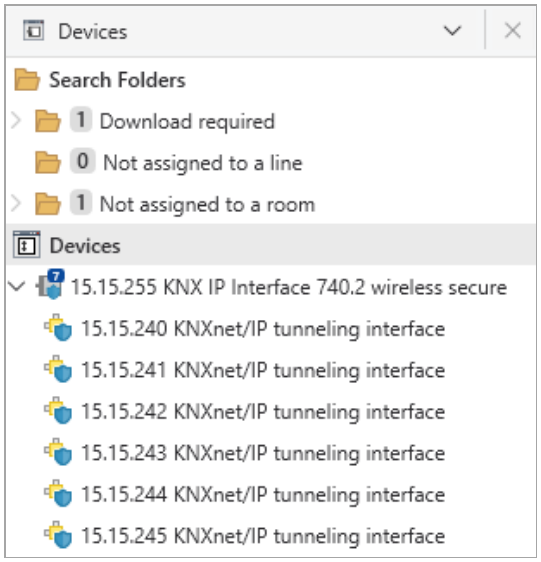
In the ETS project in the properties of the device, secure commissioning can be activated and the device certificate can be added:



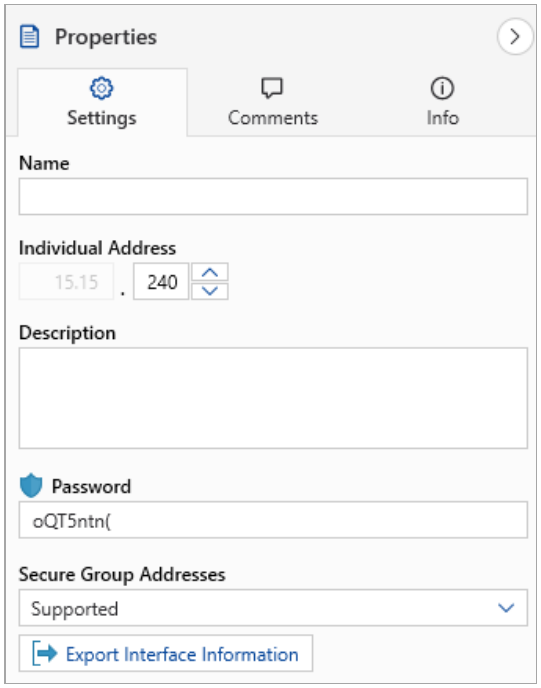
If secure tunneling is activated, a unique password will be created automatically for each tunnel. These passwords can be displayed under the ‘Settings’ overview, when a tunnel is selected.

9.2 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.



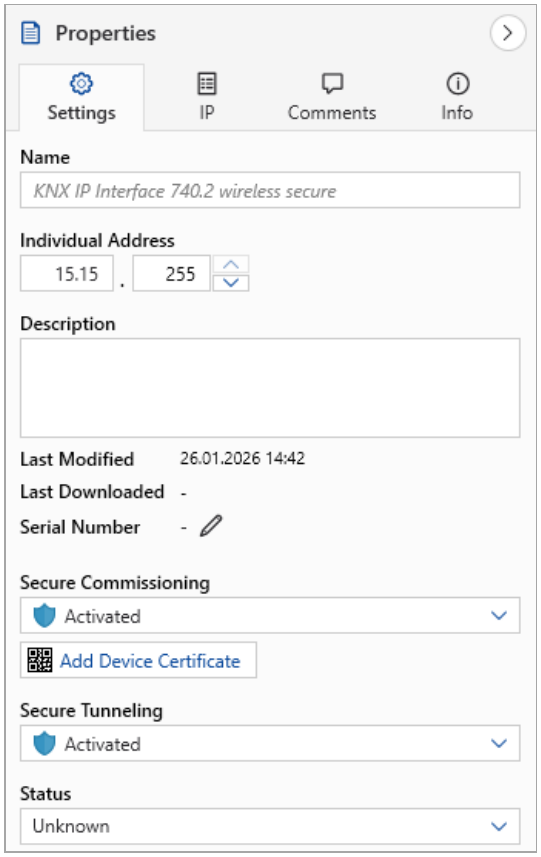
Make sure that none of the specified addresses are already used in your KNX installation.

9.3 IP settings

By marking the KNX IP Interface 740.2 *wireless 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.

9.3.1 Device name (SSID)

Under Properties menu item “Settings”, the device name (SSID) of the KNX IP Interface 740.2 *wireless secure* can be changed. The first 30 characters are used.

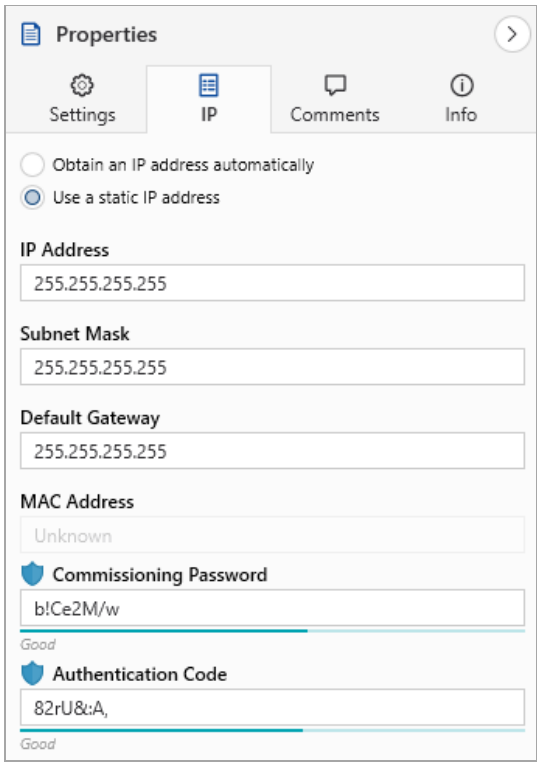


The change made will only take effect after an ETS download.

9.3.2 IP configuration

The IP configuration is only used in “Station / Client mode”.
In operating mode “Access point” the IP configuration is not used.

Under Properties menu item “IP”, the IP specific options of the KNX IP Interface 740.2 *wireless 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 Interface 740.2 *wireless secure* must be entered here. This is used to address the device via the IP network (WiFi). 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 Interface 740.2 *wireless 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 Interface 740.2 *wireless 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 Interface 740.2 wireless secure: 192.168.1.31
Subnet mask of KNX IP Interface 740.2 wireless secure: 255.255.255.0

Commissioning Password

The commissioning password is required in ETS for the entire commissioning process for a KNX IP Secure device. It serves also for the authentication of the ETS vis-à-vis the device.

It shall be different from passwords of possible secured additional interfaces and represents the so-called management level for device configuration by ETS.

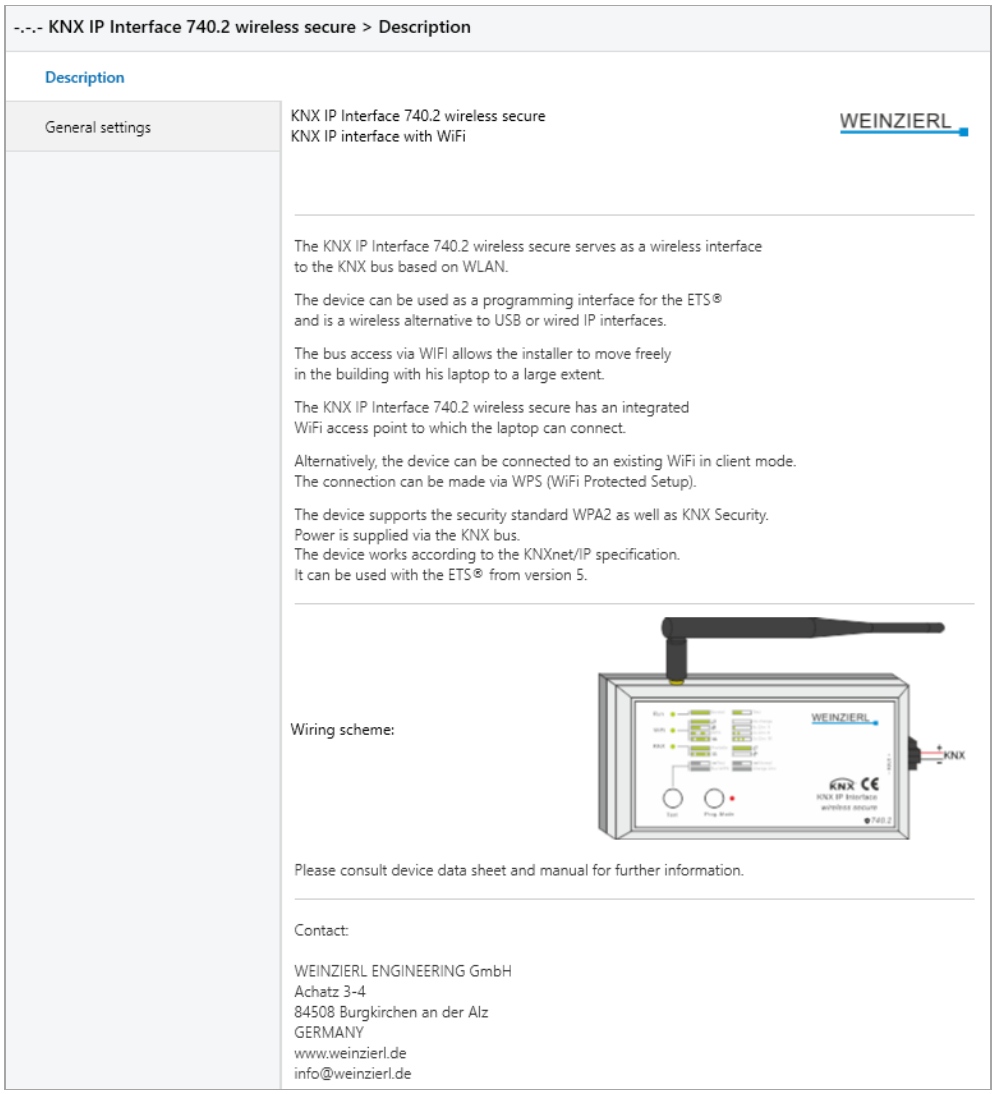
The commissioning password is only known to ETS and therefore can make changes on the device (passwords from secured additional interfaces can be distributed, e.g. to an external visualization).

Authentication Code

The authentication code is required for the (further) authentication of KNX IP Secure devices (device vis-à-vis ETS).

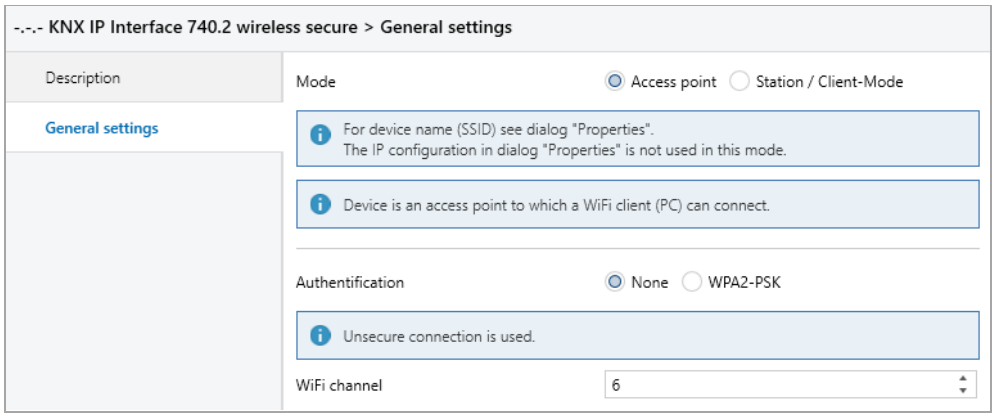
- Because the FDSK is known outside of ETS, e.g. as a QR code or device label, this key shall be changed in the ETS project. If the FDSK remains known, an authorized device could be simulated using „Man in the Middle“.
- The FDSK is replaced by a separate (for this ETS and this KNX IP Secure device) authentication code. The subsequent communication of the device vis-à-vis ETS is then performed with this (new) authentication code (instead of the initial FDSK). Consequently, every KNX IP Secure device has a separate authentication code which is different from the initial FDSK after commissioning, if it has not been overwritten by the ETS user - for several devices - by an identical authentication code.
- The authentication code can be modified by the ETS user.
- The authentication code can be seen here in the ETS interface.

9.4 Description page



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

9.5 General settings

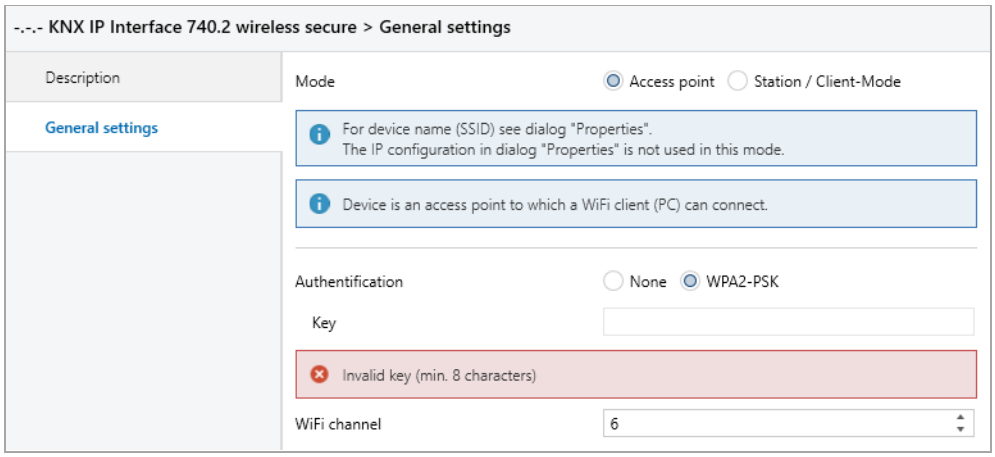


Mode

The operating mode of the device is configured here. The following options are available:

- Access point
  Device is an access point to which a WiFi client (PC) can connect.
- Station / Client-Mode
  Device is a client that connects to an access point.

9.6 Operating mode “Access point”



Authentification

The WiFi encryption can be activated/deactivated via the authentification parameter.

The choices are:

- None
  The installer can connect to the WiFi without entering a password.
  The WiFi is not encrypted.

- WPA2-PSK
  As encryption standard WPA2-PSK (WiFi Protected Access 2, pre-shared-key) is used.

Key *(only for WPA2-PSK, 63 characters)*

The key used must be entered here (8 ... 63 characters). This must also be entered in the WiFi client (PC) when establishing the WiFi connection.

WiFi channel

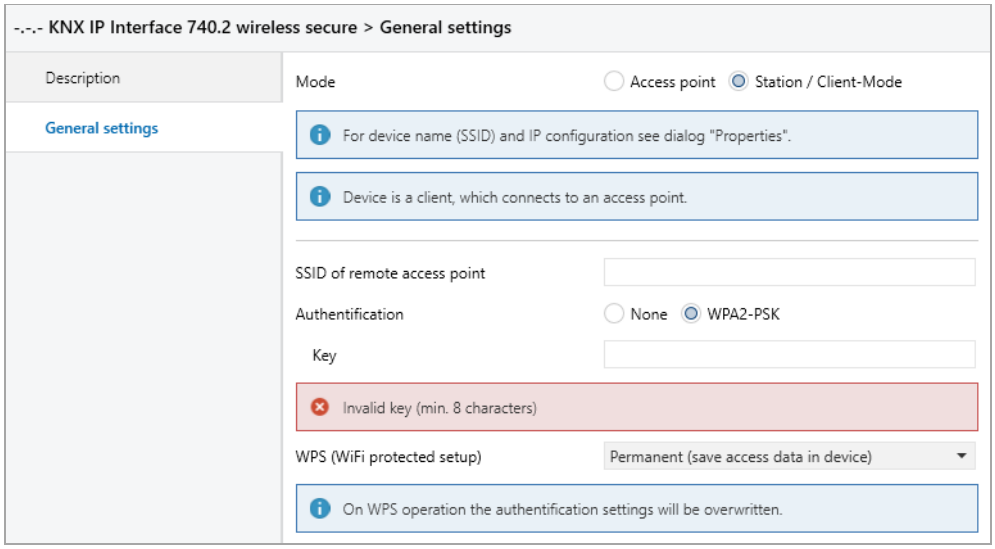
The used WiFi channel is configured here.

Example: Authentification

To ensure a high level of security, the key should be at least 10 characters long. Also it should contain upper and lower case letters as well as special characters and numbers.

Device name (SSID): KNX IP Interface 740.2 secure
Authentification: WPA2-PSK
*Key: iEn49*s/kP*

9.7 Operating mode “Station / Client-Mode”



SSID of remote access point *(32 characters)*

Here the identifier of the WiFi network (SSID, Service Set Identifier) to which the device is to connect has to be entered.

Authentification

The Authentification parameter can be used to configure whether the remote access point uses WiFi encryption.

The choices are:

- None
  The WiFi is not encrypted.

- WPA2-PSK
  As encryption standard WPA2-PSK (WiFi Protected Access 2, pre-shared-key) is used.

Key *(only for WPA2-PSK, 63 characters)*

The key used must be entered here (8 ... 63 characters). This is required to establish the WiFi connection to the remote access point.

WPS (WiFi protected setup)

This configures whether the device can connect to the remote access point using WPS (WiFi protected setup).

The choices are:

- Disabled
- Temporary
- Permanent (save access data in device)
  The WPS function overwrites the authentification settings.

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.

Product database for ETS 5/6
www.weinzierl.de/en/products/740.2/ets6

Data sheet
www.weinzierl.de/en/products/740.2/datasheet

CE Declaration
www.weinzierl.de/en/products/740.2/ce-declaration

Tender text
www.weinzierl.de/en/products/740.2/tender-text

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

2026-01-26