KNX IP Schnittstelle mit WLAN

KNX IP Interface 740.2 *wireless secure*

Bedienungs- und Montageanleitung

(Art. # 5537)

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

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

Inhalt

1 Anwendung

Das KNX IP Interface 740.2 *wireless secure* dient als drahtlose Schnittstelle zum KNX Bus auf Basis von WLAN. Das Gerät kann als Programmierschnittstelle für die ETS® verwendet werden und stellt eine drahtlose Alternative zu USB oder drahtgebundenen IP Schnittstellen dar. Durch den Buszugriff über WLAN kann sich der Installateur mit seinem Laptop weitgehend frei im Gebäude bewegen.

Das KNX IP Interface 740.2 *wireless secure* besitzt einen integrierten WLAN Access Point, mit dem sich der Laptop verbinden kann. Alternativ kann das Gerät im Client-Modus an ein bestehendes WLAN angebunden werden, die Anbindung kann über WPS (WiFi Protected Setup) erfolgen.

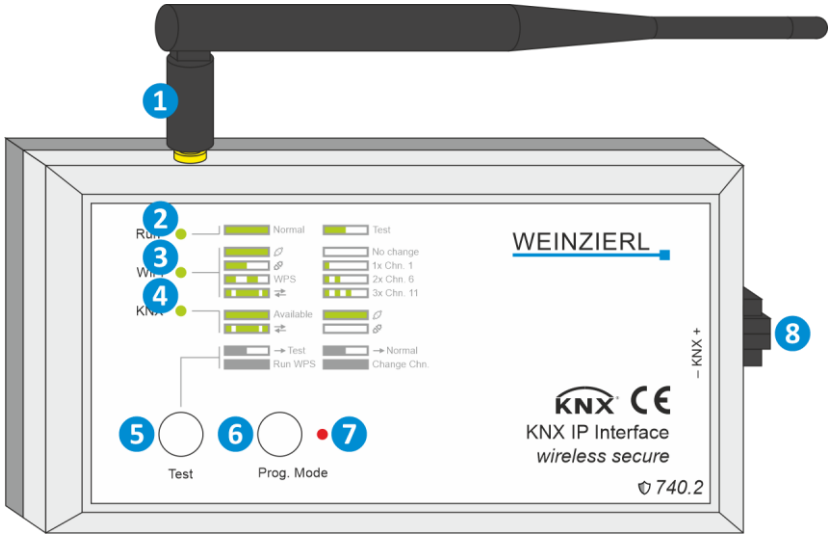
Das Gerät unterstützt den Sicherheitsstandard WPA2 sowie KNX Security.

Die Spannungsversorgung erfolgt über den KNX Bus.

Das Gerät arbeitet nach der KNXnet/IP-Spezifikation. Es ist mit der ETS® ab Version 5 verwendbar.

2 Installation und Inbetriebnahme

Das Gehäuse des KNX IP Interface 740.2 *wireless secure* hat die Abmessungen 125 x 67 x 31 mm (L x B x H). Es besitzt folgende Bedienelemente und Anzeigen:



1. Antenne
2. LED Run (grün)
3. LED WiFi (grün)
4. LED KNX (grün)
5. Taster Test
6. Taster Prog. Mode
7. Programmier-LED
8. KNX Bus Anschluss

Bei fehlender Busspannung ist das Gerät ohne Funktion.

2.1 KNX Programmiermodus

Der KNX Programmiermodus wird über den KNX-Programmiertaster 6 ein- bzw. ausgeschaltet. Bei aktivem Programmiermodus leuchtet die Programmier-LED 7 rot.

2.2 Handbedienung und Statusanzeige

Zusammenfassung der Zustände der Programmier-LED 7:

LED Verhalten	Bedeutung
LED leuchtet rot	Der Programmiermodus ist aktiv.
LED blinkt rot (schnell)	Der Programmiermodus ist nicht aktiv. Der Gerät ist nicht korrekt geladen z.B. nach Abbruch eines Downloads.

Durch kurzes Betätigen von Taster Test 5 wird zwischen normalem Betriebsmodus und Testmodus gewechselt. Der aktive Modus wird durch Leuchten, bzw. langsames Blinken der LED Run 2 in grün angezeigt.

Zusammenfassung der Zustände der LED Run 2:

LED Verhalten	Bedeutung
LED leuchtet grün	Das Gerät arbeitet im normalen Betriebsmodus.
LED blinkt grün (langsam)	Das Gerät befindet sich im Testmodus.
LED blinkt grün (schnell)	Das Gerät befindet sich gerade im ETS Download.

2.2.1 Normaler Betriebsmodus

Die LED WiFi 3 leuchtet grün bei vorhandener WLAN Verbindung. Bei Flackern dieser LED findet Telegrammverkehr über WLAN statt. Blinkt diese LED langsam in grün, ist das Gerät nicht über WLAN verbunden.

Durch langes Betätigen von Taster Test 5 wird WPS (WiFi Protected Setup) ausgeführt. Dies wird durch schnelles Blinken der LED WiFi 3 in grün angezeigt.

Zusammenfassung der Zustände der LED WiFi 3:

LED Verhalten	Bedeutung
LED leuchtet grün	Das Gerät ist über WLAN verbunden.
LED blinkt grün (langsam)	Das Gerät ist nicht über WLAN verbunden.
LED blinkt grün (schnell)	WPS wird gerade ausgeführt.
LED flackert grün	Telegrammverkehr über WLAN.

Die LED KNX 4 leuchtet grün bei vorhandener KNX Busspannung. Bei Flackern dieser LED findet Telegrammverkehr auf dem KNX Bus statt.

Zusammenfassung der Zustände der LED KNX 4:

LED Verhalten	Bedeutung
LED leuchtet grün	KNX Busspannung vorhanden.
LED flackert grün	Telegrammverkehr auf dem KNX Bus.

2.2.2 Testmodus

Im Testmodus kann der WLAN Kanal gewechselt werden sowie der Verbindungsstatus der Tunneling Verbindung angezeigt werden.

Verwenden viele Teilnehmer denselben WLAN Kanal, so kann durch einen Wechsel in einen weniger stark benutzten Kanal die Verbindungsqualität verbessert werden:

Durch langes Betätigen von Taster Test 5 wird durch die WLAN Kanäle geschaltet. Dies wird durch Aufblitzen der LED WiFi 3 in grün angezeigt. Der gewählte WLAN Kanal wird nach Verlassen des Testmodus aktiviert. Dieser wird nicht im Gerät gespeichert (Auswahl nur temporär).

Zusammenfassung der Zustände der LED WiFi 3:

LED Verhalten	Bedeutung
LED ist aus	Der über ETS konfigurierte WiFi Kanal ist gewählt.
LED blitzt 1x grün	WLAN Kanal 1 ist gewählt.
LED blitzt 2x grün	WLAN Kanal 6 ist gewählt.
LED blitzt 3x grün	WLAN Kanal 11 ist gewählt.

Die LED KNX 4 leuchtet grün bei aktiver KNXnet/IP Tunneling Verbindung.

Zusammenfassung der Zustände der LED KNX 4:

LED Verhalten	Bedeutung
LED leuchtet grün	Mindestens eine KNXnet/IP Tunneling Verbindung ist aktiv.
LED ist aus	Keine KNXnet/IP Tunneling Verbindung ist aktiv.

3 Zurücksetzen auf Werkseinstellungen

Es besteht die Möglichkeit, das Gerät auf die Werkseinstellungen zurückzusetzen.

- KNX Bus Anschluss 8 vom Gerät trennen.
- Taster Prog. Mode 6 drücken und gedrückt halten.
- KNX Bus Anschluss 8 zum Gerät wiederherstellen.
- Taster Prog. Mode 6 mindestens noch 6 Sekunden gedrückt halten.
- Ein kurzes Aufblinken aller LEDs (2 3 4 7) signalisiert die erfolgreiche Rücksetzung auf Werkseinstellung.

3.1 Werkseinstellungen

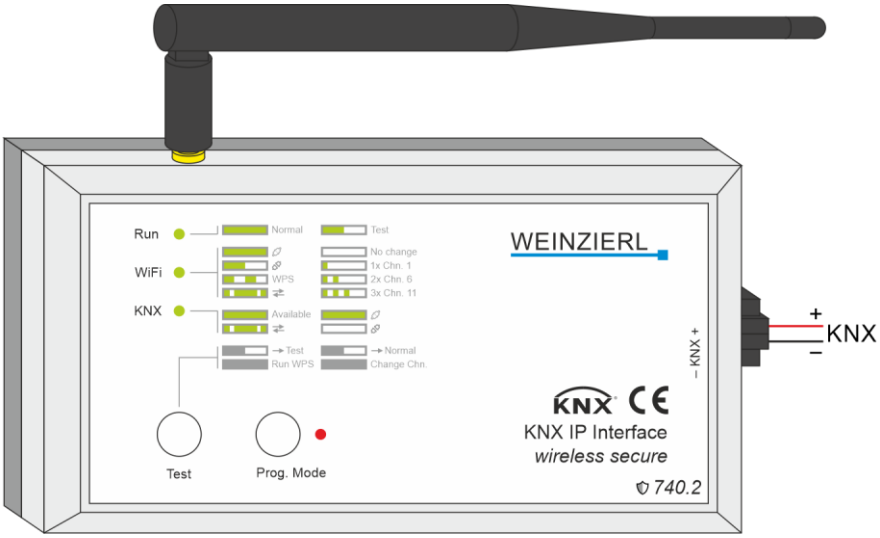
Physikalische Adressen und KNXnet/IP Tunneling Verbindungen

Physikalische Adresse: 15.15.255
Aktive KNXnet/IP Tunneling Verbindungen: 1
Physikalische Adresse der Tunneling Verbindung: 15.15.250

Konfiguration

Gerätename (SSID): KNX IP Interface 740.2 secure
Modus: Access Point
Authentifizierung: WPA2-PSK
Schlüssel: Format XXXX-XXXX-XXXX auf dem Gerätelabel
WLAN Kanal: 6

4 Anschluss-Schema



4.1 Steckbare Schraubklemme

Die Schraubklemme dient zum Anschluss des KNX Bus.

4.2 Anschlussbelegung

Anschluss	Symbol	Beschreibung
KNX	+	Positiver Anschluss für KNX Bus
KNX	-	Masse-Anschluss für KNX Bus

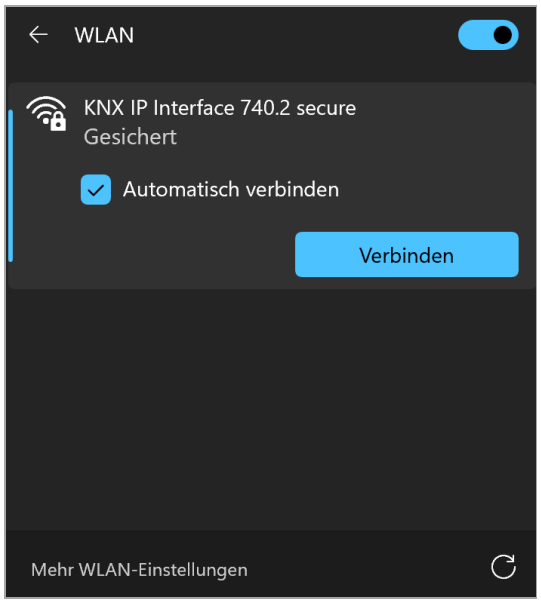
5 Aufbau einer WLAN Verbindung

5.1 KNX IP Interface 740.2 *wireless secure* ist „Access Point“

Um eine WLAN Verbindung von einem PC oder Laptop herstellen zu können, ist ein WLAN Adapter erforderlich. Bei Laptops ist dieser in der Regel im Gerät integriert.

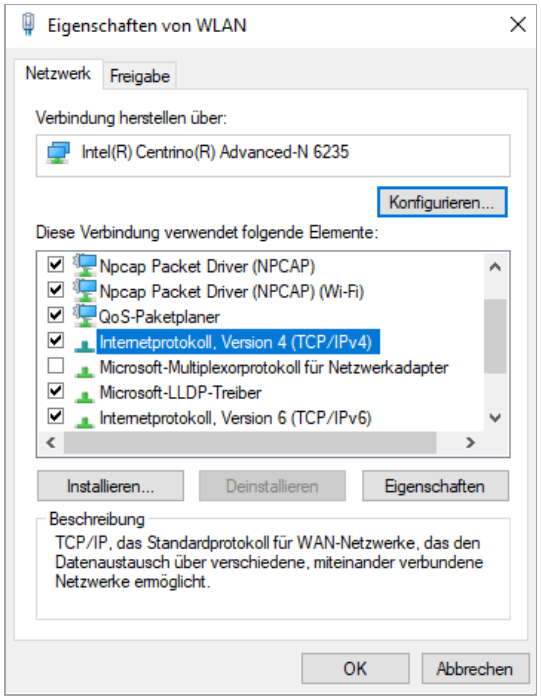
Der Aufbau der WLAN Verbindung zum KNX IP Interface 740.2 *wireless secure* läuft folgendermaßen ab:

Zunächst muss das vom KNX IP Interface 740.2 *wireless secure* zur Verfügung gestellte WLAN gefunden werden. Der Dialog „Verfügbare Netzwerke anzeigen“ von Windows® listet alle verfügbaren drahtlosen Netzwerke auf. Dieser Dialog kann über „Einstellungen / Netzwerk und Internet / WLAN Verfügbare Netzwerke anzeigen“ erreicht werden. Alternativ ist dieser Dialog über das entsprechende Icon „Netzwerk“ im Infobereich am Bildschirmrand erreichbar.

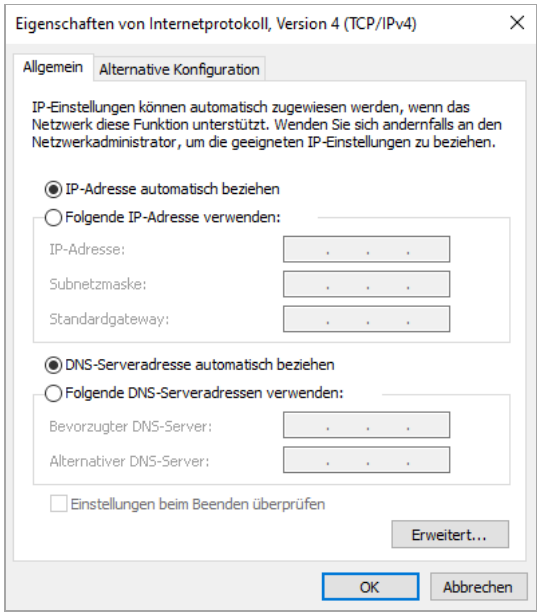


Da das KNX IP Interface 740.2 *wireless secure* einen DHCP-Server integriert hat, sollte die IP Adresse des PCs automatisch (DHCP) eingestellt werden. Bei den meisten Laptops ist dies die Standardeinstellung.

Zum Ändern der Einstellungen ist im Eigenschaften-Dialog der drahtlosen Netzwerkverbindung das Element „Internetprotokoll, Version 4 (TCP/IPv4)“ zu markieren und die Schaltfläche „Eigenschaften“ zu betätigen.



Im folgenden Dialog sollte „IP-Adresse automatisch beziehen“ aktiv sein.



Nach Aufbau der WLAN Verbindung, lässt sich das KNX IP Interface 740.2 *wireless secure* als Schnittstelle zum KNX Bus verwenden.

5.2 KNX IP Interface 740.2 *wireless secure* ist „Station / Client Mode”

Das KNX IP Interface 740.2 *wireless secure* baut die WLAN Verbindung zum konfigurierten Access Point automatisch auf, sofern die eingegebenen Daten korrekt sind. Die Eingabe der Daten erfolgt über den ETS-Parameterdialog. Siehe dazu den Abschnitt „ETS-Datenbank – Betriebsmodus „Station / Client-Mode““.

Sofern konfiguriert lässt sich die Verbindung auch über WPS herstellen. Dafür muss der Parameter **WPS (WiFi Protected Setup)** auf Temporär oder Dauerhaft gesetzt sein. Zum Verbinden muss zuerst am Access Point die WPS-Funktionen aktiviert werden und anschließend am KNX IP Interface 740.2 *wireless secure* der Taster Test 5 lange gedrückt werden (mind. 1 Sek.). Das Interface muss dabei im normalen Betriebsmodus sein (LED Run 2 leuchtet grün).

Nach Aufbau der WLAN Verbindung, lässt sich das KNX IP Interface 740.2 *wireless secure* als Schnittstelle zum KNX Bus verwenden. Dies gilt für alle PCs und Laptops in diesem Netzwerk.

6 KNX Security

Der KNX Standard wurde um KNX Security erweitert, um KNX Installationen vor unerlaubten Zugriffen zu schützen. KNX Security verhindert zuverlässig sowohl das Mithören der Kommunikation als auch die Manipulation der Anlage.

Die Spezifikation für KNX Security unterscheidet zwischen KNX IP Security und KNX Data Security. KNX IP Security schützt die Kommunikation über IP während auf KNX TP die Kommunikation unverschlüsselt bleibt. Somit kann KNX IP Security auch in bestehenden KNX Anlagen und mit nicht-secure KNX TP Geräten eingesetzt werden.

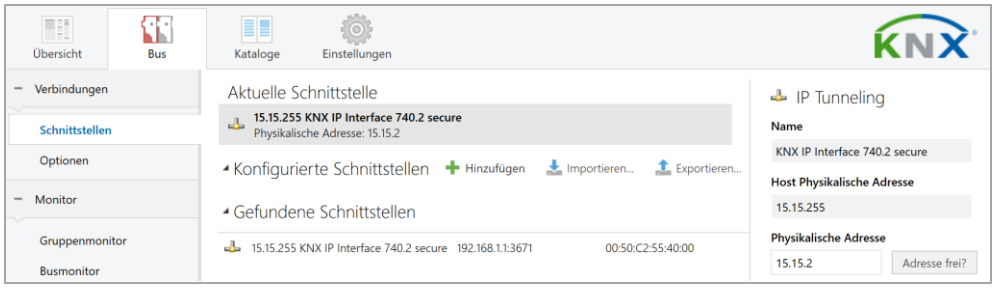
KNX Data Security beschreibt die Verschlüsselung auf Telegrammebene. Das heißt, dass auch die Telegramme auf dem Twisted Pair Bus oder über RF (Funk) verschlüsselt werden.

Verschlüsselte Telegramme sind länger als die bisher verwendeten Unverschlüsselten. Deshalb ist es für die sichere Programmierung über den Bus erforderlich, dass das verwendete Interface (z.B. USB) und ggf. dazwischenliegende Linienkoppler die sogenannten KNX Long Frames unterstützten.

7 Schnittstelleneinstellungen in der ETS

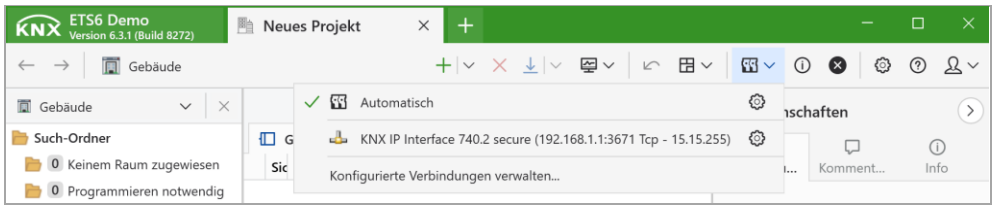
7.1 ETS 5

In der ETS 5 können Schnittstellen über das ETS Menü „Bus – Schnittstellen“ ausgewählt und konfiguriert werden. Alle verfügbaren Verbindungen werden unter „Gefundene Schnittstellen“ aufgelistet. Nach Anklicken der gewünschten Verbindung erscheinen auf der rechten Seite des ETS Fensters verbindungsspezifische Informationen und Optionen. Über die Schaltfläche „Auswählen“ kann die gewählte Verbindung als „Aktuelle Schnittstelle“ ausgewählt werden.



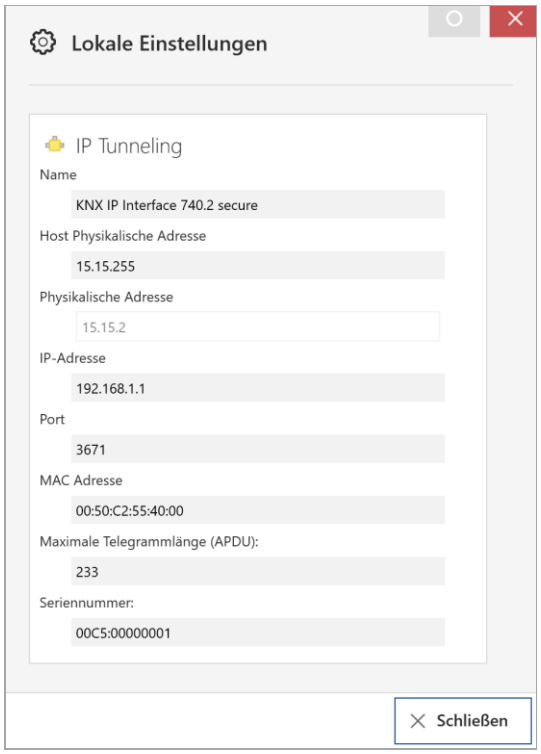
7.2 ETS 6

In der ETS 6 können Schnittstellen im ETS Projekt über die Schaltfläche „Schnittstelle“ ausgewählt und konfiguriert werden. Alle verfügbaren Verbindungen werden hier aufgelistet.



Durch Anklicken einer Verbindung wird diese als gewünschte Schnittstelle gewählt.

Durch Anklicken des Zahnrades neben der gewünschten Verbindung erscheinen die verbindungsspezifischen Informationen und Optionen.



7.3 Allgemein

Der angezeigte Gerätename und die „Host Physikalische Adresse“ (physikalische Adresse des Gerätes) kann über den Datenbankeintrag innerhalb Ihres ETS Projekts geändert werden.

Im Abschnitt „Physikalische Adresse” kann die physikalische KNX Adresse der aktuell verwendeten KNXnet/IP Tunneling Verbindung geändert werden. Um zu überprüfen, ob die gewünschte physikalische Adresse nicht bereits in Ihrer KNX Installation vorhanden ist, kann die Schaltfläche „Adresse frei?“ betätigt werden.

Das KNX IP Interface 740.2 *wireless secure* unterstützt bis zu 6 Verbindungen gleichzeitig. Für jede Verbindung wird eine separate physikalische Adresse verwendet.

Die ETS kann auf konfigurierte IP Schnittstellen auch ohne Datenbankeintrag zugreifen. Entspricht die Konfiguration nicht den Gegebenheiten der Installation, muss diese über den Datenbankeintrag im ETS Projekt angepasst werden.

Die physikalische KNX Geräteadresse sowie die physikalischen KNX Adressen für die zusätzlichen Tunneling Verbindungen können über den Datenbankeintrag innerhalb des ETS Projekts geändert werden, nachdem das Gerät dem Projekt hinzugefügt wurde. Siehe dazu den Abschnitt „ETS-Datenbank – Zusätzliche physikalische Adressen“.

Das KNX IP Interface 740.2 *wireless secure* verfügt, wie alle programmierbaren KNX Geräte, über eine physikalische Adresse, mit der das Gerät angesprochen werden kann. Diese wird zum Beispiel von der ETS beim Download des Interfaces über den KNX Bus verwendet.

Für die Interface-Funktion verwendet das Gerät zusätzliche physikalische Adressen, die in der ETS (für ETS5.7 oder neuer) eingestellt werden können. Sendet ein Client (z.B. ETS) über das KNX IP Interface 740.2 *wireless secure* Telegramme auf den KNX Bus, so enthalten diese als Absenderadresse eine der zusätzlichen Adressen. Jede Adresse ist einer Verbindung zugeordnet. Somit können Antworttelegramme eindeutig zum jeweiligen Client weitergeleitet werden.

Die zusätzlichen physikalischen Adressen müssen aus dem Adressbereich der Bus-Linie sein, in der sich das Interface befindet und dürfen nicht von einem anderen Gerät verwendet werden.

Beispiel:

Physikalische Adresse: *1.1.10 (Geräteadresse in der Topologie)*
KNXnet/IP Tunneling Verbindung 1: *1.1.240 (1. Zusätzliche physikalische Adresse)*
KNXnet/IP Tunneling Verbindung 2: *1.1.241 (2. Zusätzliche physikalische Adresse)*
KNXnet/IP Tunneling Verbindung 3: *1.1.242 (3. Zusätzliche physikalische Adresse)*
KNXnet/IP Tunneling Verbindung 4: *1.1.243 (4. Zusätzliche physikalische Adresse)*
KNXnet/IP Tunneling Verbindung 5: *1.1.244 (5. Zusätzliche physikalische Adresse)*
KNXnet/IP Tunneling Verbindung 6: *1.1.245 (6. Zusätzliche physikalische Adresse)*

8 Programmierung

Das KNX IP Interface 740.2 *wireless secure* kann über verschiedene Wege von der ETS programmiert werden.

8.1 Über den KNX Bus

Dazu muss das Gerät nur mit dem KNX Bus verbunden sein. Die ETS benötigt eine zusätzliche Schnittstelle (z.B. USB) zum KNX Bus. Über diesen Weg kann sowohl die physikalische Adresse, als auch die gesamte Applikation inklusive IP Konfiguration programmiert werden. Die Programmierung über den KNX Bus wird empfohlen, wenn keine IP Verbindung hergestellt werden kann.

8.2 Über KNXnet/IP Tunneling

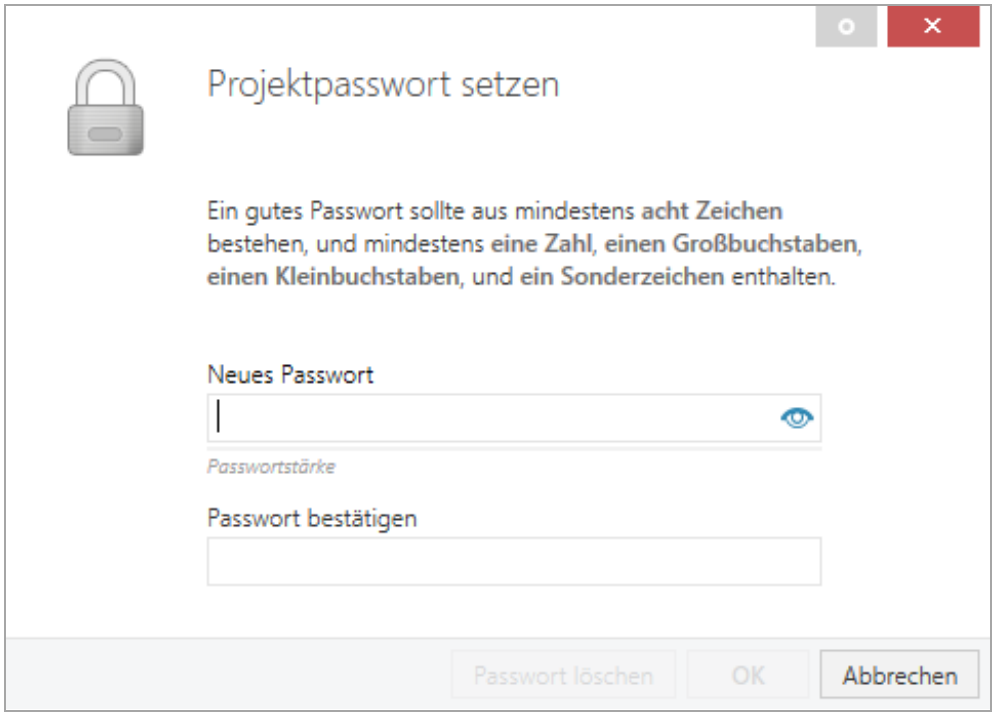
Hierbei ist keine zusätzliche Schnittstelle erforderlich. Die Programmierung über KNXnet/IP Tunneling ist möglich, wenn das Gerät bereits eine gültige IP Konfiguration besitzt (z.B. über DHCP). In diesem Fall wird das Gerät bei den Schnittstellen in der ETS angezeigt und muss ausgewählt werden. Der Download erfolgt aus dem ETS Projekt heraus, wie bei anderen Geräten auch.

9 ETS-Datenbank

Die ETS5 Datenbank (für ETS 5.7 oder neuer) kann auf der Produkt-Website des KNX IP Interface 740.2 *wireless secure* (www.weinzierl.de) oder über den ETS Online Katalog heruntergeladen werden.

9.1 Gesicherte Inbetriebnahme

Wird das erste Produkt mit KNX Security in ein Projekt eingefügt, fordert die ETS dazu auf, ein Projektpasswort einzugeben.



Dieses Passwort schützt das ETS Projekt vor unberechtigtem Zugriff. Dieses Passwort ist kein Schlüssel, der für die KNX Kommunikation verwendet wird. Die Eingabe des Passwortes kann mit „Abbrechen“ umgangen werden, dies wird aus Sicherheitsgründen aber nicht empfohlen.

Für jedes Gerät mit KNX Security, das in der ETS angelegt wird, benötigt die ETS ein Gerätezertifikat. Dieses Zertifikat beinhaltet die Seriennummer des Geräts, sowie einen initialen Schlüssel (FDSK = Factory Default Setup Key).

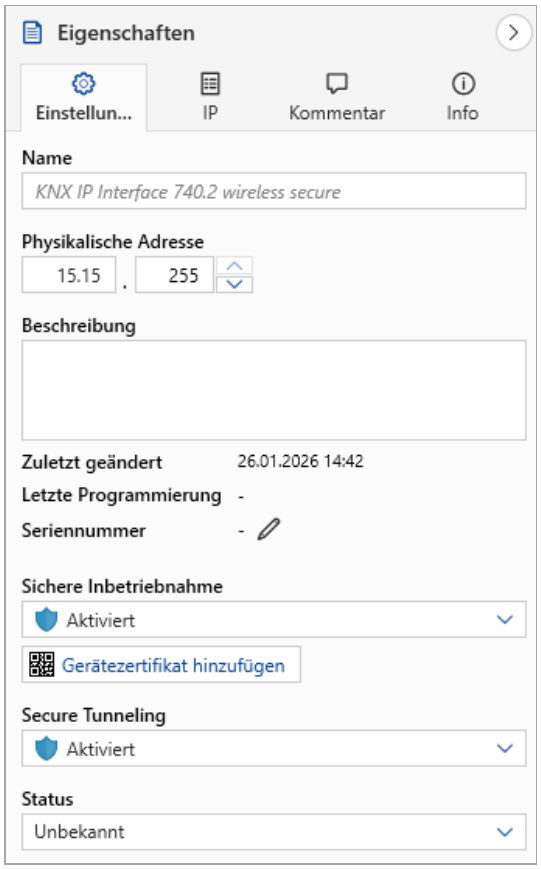
Das Zertifikat ist als Text auf dem Gerät aufgedruckt. Es kann auch über eine Webcam vom aufgedruckten QR-Code abgescannt werden.

Die Liste aller Gerätezertifikate kann im ETS-Fenster Reports – Projekt-Sicherheit verwaltet werden.

Der initiale Schlüssel wird benötigt, um ein Gerät von Anfang an sicher in Betrieb zu nehmen. Selbst wenn der ETS-Download von einem Dritten mitgeschnitten wird, hat dieser anschließend keinen Zugriff auf die gesicherten Geräte. Während dem ersten sicheren Download wird der initiale Schlüssel von der ETS durch einen neuen Schlüssel ersetzt, der für jedes Gerät einzeln erzeugt wird. Somit wird verhindert, dass Personen oder Geräte Zugriff auf das Gerät haben, die den initialen Schlüssel eventuell kennen. Der initiale Schlüssel wird beim Zurücksetzen auf Werkseinstellungen wieder aktiviert.

Durch die Seriennummer im Zertifikat kann die ETS während eines Downloads den richtigen Schlüssel zu einem Gerät zuordnen.

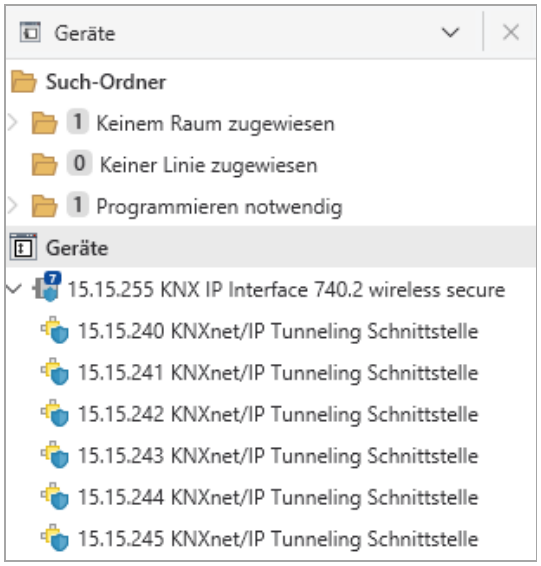
Im ETS-Projekt in den Eigenschaften des Geräts kann die sichere Inbetriebnahme aktiviert und das Gerätezertifikat hinzugefügt werden:



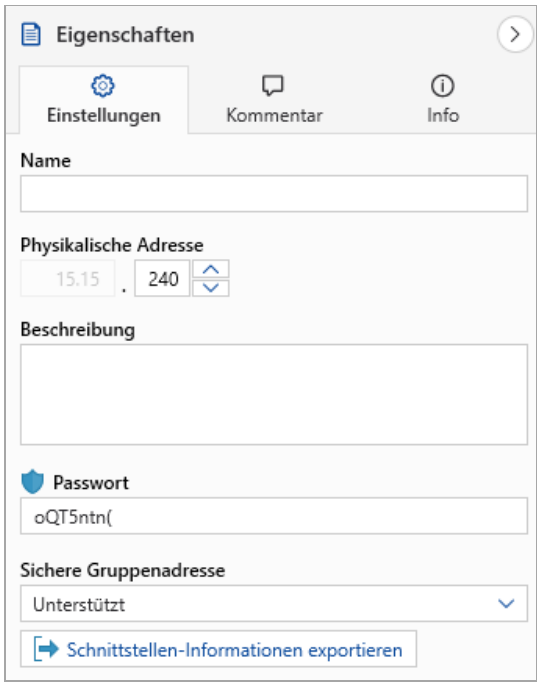
Wenn Secure Tunneling aktiviert ist, wird automatisch ein Passwort für jeden Tunnel vergeben. Dieses Passwort wird unter Menüpunkt „Einstellungen“ angezeigt, wenn ein Tunnel ausgewählt ist.

9.2 Zusätzliche physikalische Adressen

Die zusätzlichen physikalischen Adressen erscheinen in der Topologie-Ansicht.



Um die einzelnen Adressen zu ändern, ist der entsprechende Eintrag in der Liste zu markieren und unter „Eigenschaften – Einstellungen“ im Textfeld die gewünschte Adresse einzugeben. Sollte der Rahmen des Textfeldes, nach Eingabe, seine Farbe auf Rot wechseln, weist dies darauf hin, dass die eingegebene Adresse bereits verwendet wird. Die Änderungen werden erst nach Download im Gerät übernommen.



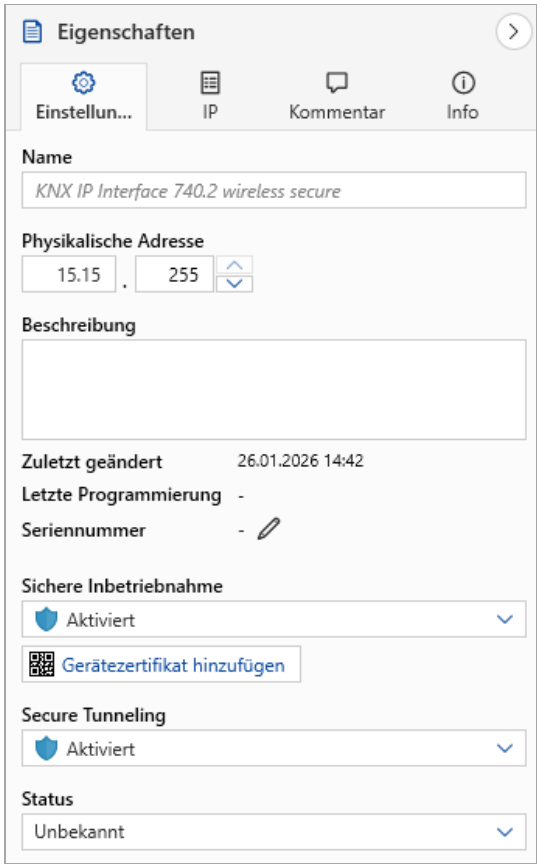
Stellen Sie sicher, dass keine der angegebenen Adressen bereits in Ihrer KNX Installation verwendet wird.

9.3 IP Einstellungen

Durch Markieren des KNX IP Interface 740.2 *wireless secure* in der Baumstruktur der Topologie Ansicht des ETS Projekts, erscheint auf der rechten Seite des ETS Fensters die Übersicht „Eigenschaften“.

9.3.1 Gerätename (SSID)

Unter Eigenschaften Menüpunkt „Einstellungen“ kann der Gerätename (SSID) des KNX IP Interface 740.2 *wireless secure* geändert werden. Es werden die ersten 30 Zeichen verwendet.

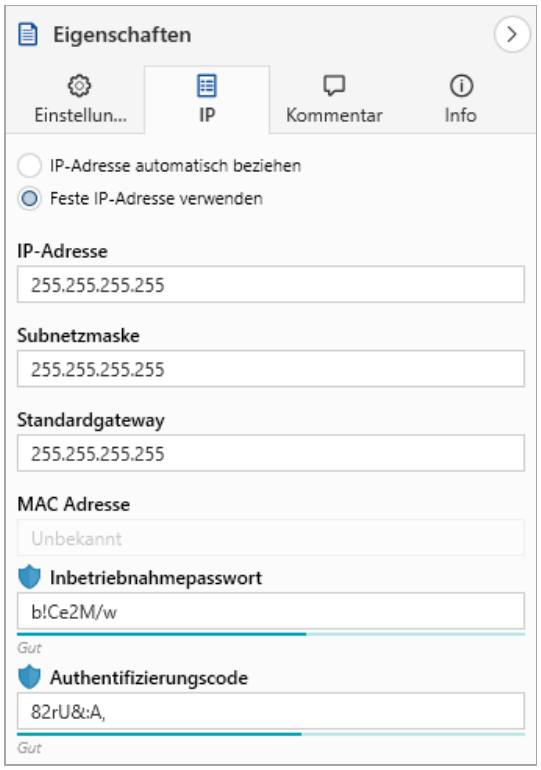


Die vorgenommene Änderung wird erst nach einem ETS-Download wirksam.

9.3.2 IP Konfiguration

Die IP Konfiguration wird nur im Betriebsmodus „Station / Client mode“ verwendet. Im Betriebsmodus „Access Point“ wird die IP Konfiguration nicht verwendet.

Unter Eigenschaften Menüpunkt „IP“ können die IP spezifischen Optionen des KNX IP Interface 740.2 *wireless secure* geändert werden.



Die vorgenommene Änderung wird erst nach einem ETS-Download wirksam.

Durch Umschalten von „IP-Adresse automatisch beziehen“ (über DHCP) auf „Feste IP-Adresse verwenden“ (statische IP Adresse) können die IP-Adresse, Subnetzmaske und das Standardgateway frei gewählt werden.

IP-Adresse

Hier ist die IP-Adresse des KNX IP Interface 740.2 *wireless secure* einzutragen. Diese dient der Adressierung des Gerätes über das IP-Netzwerk (WLAN). Die IP-Adressierung sollte mit dem Administrator des Netzwerks abgestimmt werden.

Subnetzmaske

Hier ist die Subnetzmaske anzugeben. Diese Maske dient dem Gerät um festzustellen, ob ein Kommunikationspartner sich im lokalen Netz befindet. Sollte sich ein Partner nicht im lokalen Netz befinden, sendet das Gerät die Telegramme nicht direkt an den Partner, sondern an das Standardgateway, das die Weiterleitung übernimmt.

Standardgateway

Hier ist die IP-Adresse des Gateways anzugeben, z.B. der Access Point der Installation.

Beispiel zur Vergabe von IP-Adressen

Mit einem PC soll auf das KNX IP Interface 740.2 *wireless secure* zugegriffen werden.

IP-Adresse von PC: 192.168.1.30
Subnetzmaske von PC: 255.255.255.0

Das KNX IP Interface 740.2 *wireless secure* befindet sich im selben lokalen Netz, d.h. es verwendet das gleiche Subnetz. Durch das Subnetz ist die Vergabe der IP-Adresse eingeschränkt, d.h. in diesem Beispiel muss die IP-Adresse des IP Interfaces 192.168.1.xx betragen, xx kann eine Zahl von 1 bis 254 sein (mit Ausnahme von 30, die schon verwendet wurde). Es ist darauf zu achten, keine Adressen doppelt zu vergeben.

IP-Adresse von KNX IP Interface 740.2 wireless secure: 192.168.1.31
Subnetzmaske von KNX IP Interface 740.2 wireless secure: 255.255.255.0

Inbetriebnahmepasswort

Das Inbetriebnahmepasswort wird in der ETS für den gesamten Inbetriebnahmeprozess eines KNX IP Secure Geräts benötigt. Es dient auch zur Authentifizierung der ETS gegenüber dem Gerät.

Es muss sich von den Passwörtern möglicher gesicherter Zusatzschnittstellen unterscheiden und stellt die sogenannte Managementebene für die Gerätekonfiguration durch die ETS dar.

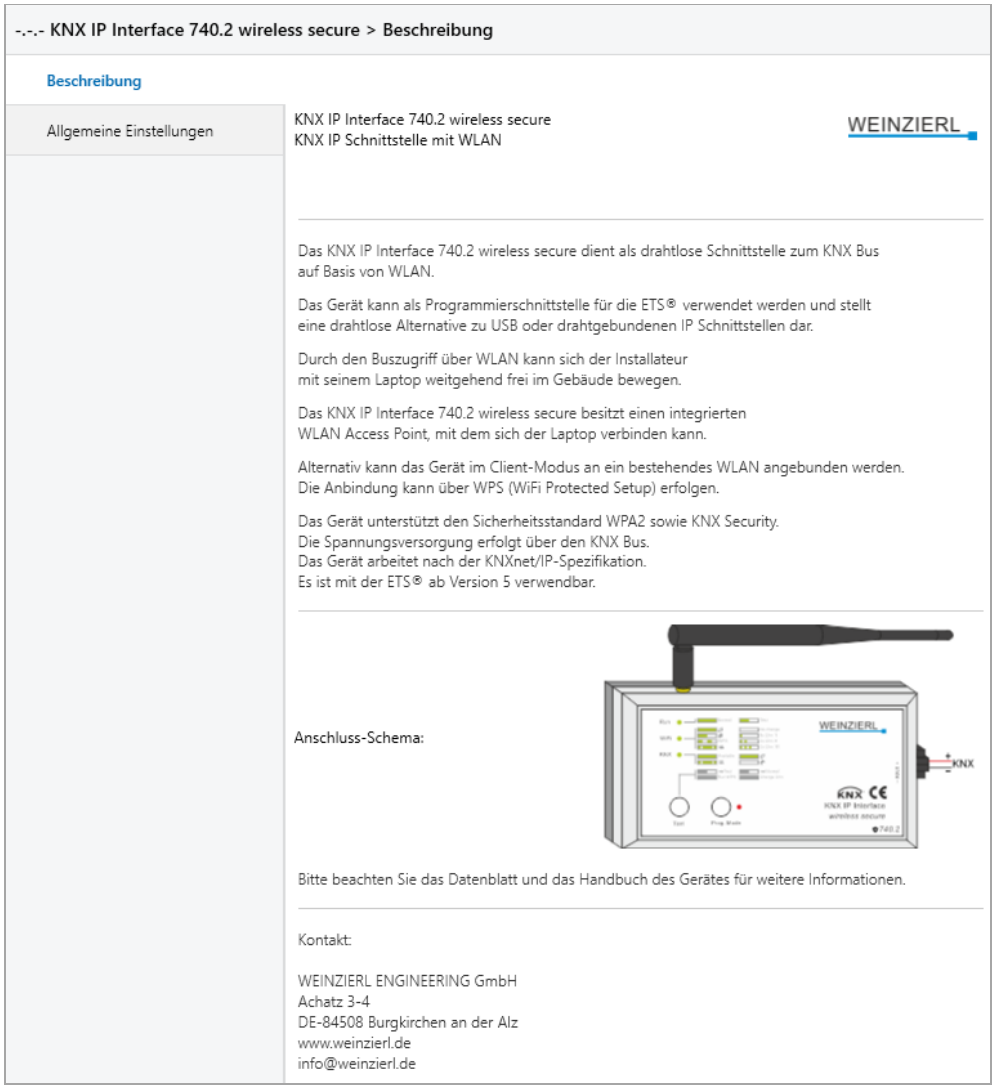
Das Inbetriebnahmepasswort ist nur der ETS bekannt und kann daher Änderungen am Gerät vornehmen (Passwörter von gesicherten Zusatzschnittstellen können verteilt werden, z.B. an eine externe Visualisierung).

Authentifizierungscode

Der Authentifizierungscode wird für die (weitere) Authentifizierung von KNX IP Secure Geräten (Gerät gegenüber ETS) benötigt.

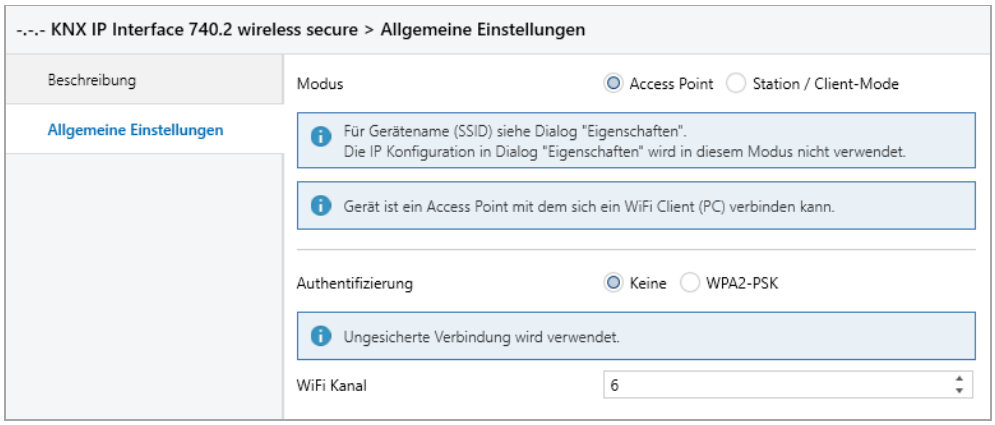
- Da der FDSK außerhalb der ETS bekannt ist, z.B. als QR-Code oder Geräteetikett, muss dieser Schlüssel im ETS Projekt geändert werden. Bleibt der FDSK bekannt, könnte ein autorisiertes Gerät mit „Man in the Middle“ simuliert werden.
- Der FDSK wird durch einen separaten (für diese ETS und dieses KNX IP Secure Gerät) Authentifizierungscode ersetzt. Die nachfolgende Kommunikation des Geräts gegenüber der ETS erfolgt dann mit diesem (neuen) Authentifizierungscode (anstelle des ursprünglichen FDSK). Folglich verfügt jedes KNX IP Secure Gerät nach der Inbetriebnahme über einen separaten Authentifizierungscode, der sich vom ursprünglichen FDSK unterscheidet, sofern er nicht vom ETS Benutzer – für mehrere Geräte – durch einen identischen Authentifizierungscode überschrieben wurde.
- Der Authentifizierungscode kann vom ETS Benutzer geändert werden.
- Der Authentifizierungscode kann hier in der ETS Oberfläche eingesehen werden.

9.4 Beschreibungsseite



Diese Seite zeigt die Gerätebeschreibung, sowie den zugehörigen Anschlussplan.

9.5 Allgemeine Einstellungen

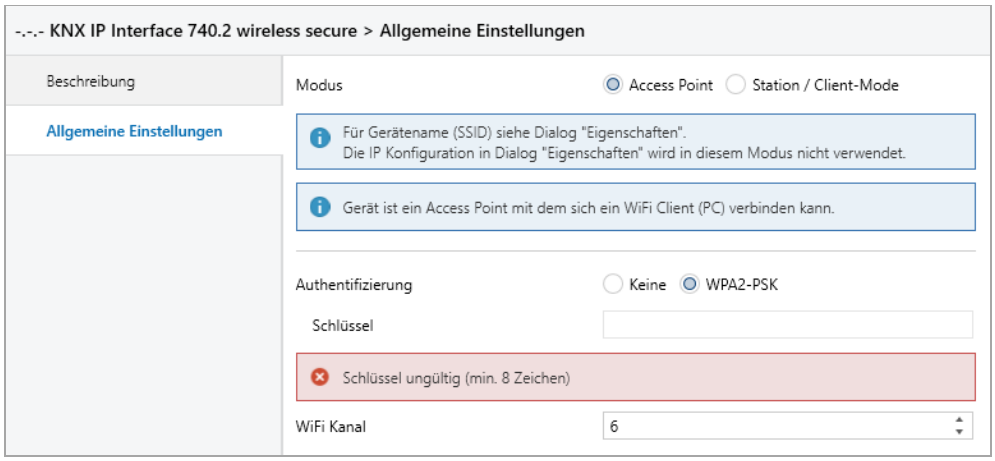


Modus

Hier wird der Betriebsmodus des Geräts konfiguriert. Es stehen folgende Möglichkeiten zur Verfügung:

- Access Point
  Gerät ist ein Access Point mit dem sich ein WiFi Client (PC) verbinden kann.
- Station / Client-Mode
  Gerät ist ein Client, welcher sich mit einem Access Point verbindet.

9.6 Betriebsmodus „Access Point“



Authentifizierung

Über den Parameter Authentifizierung kann die WLAN-Verschlüsselung aktiviert/deaktiviert werden.

Zur Auswahl steht:

- Keine
  Der Installateur kann sich ohne Passworteingabe zum WLAN verbinden.
  Das WLAN ist nicht verschlüsselt.

- WPA2-PSK
  Als Verschlüsselungsstandard wird WPA2-PSK (WiFi Protected Access 2, pre-shared-key) verwendet.

Schlüssel *(nur bei WPA2-PSK, 63 Zeichen)*

Hier ist der verwendete Schlüssel anzugeben (8 … 63 Zeichen). Dieser ist beim Aufbau der WLAN-Verbindung auch im WiFi Client (PC) anzugeben.

WiFi Kanal

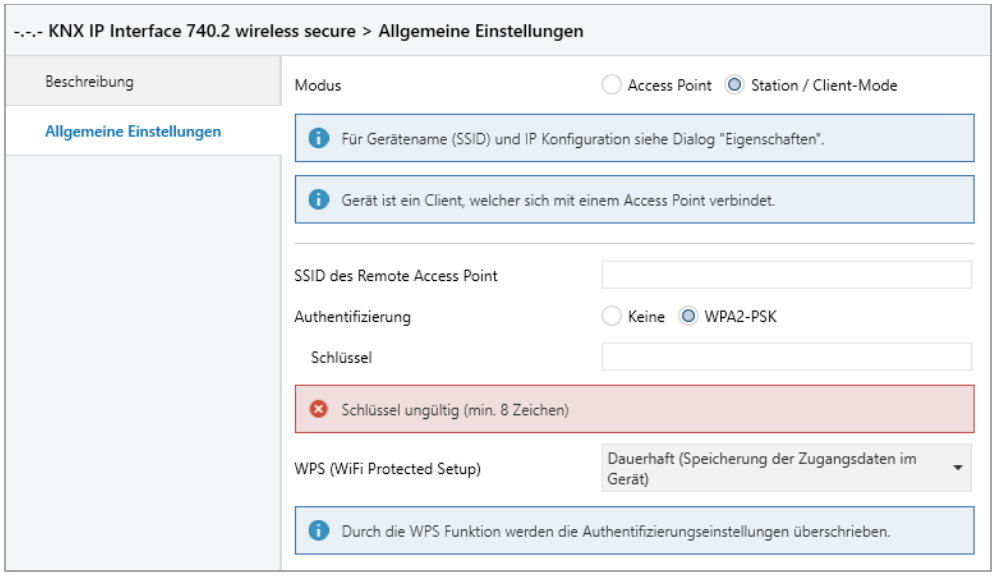
Hier wird der verwendete WiFi Kanal konfiguriert.

Beispiel: Authentifizierung

Um eine hohe Sicherheit zu gewährleisten, sollte der Schlüssel mindestens 10 Zeichen lang sein, Groß- und Kleinbuchstaben sowie Sonderzeichen und Zahlen beinhalten.

Gerätename (SSID): KNX IP Interface 740.2 secure
Authentifizierung: WPA2-PSK
*Schlüssel: iEn49*s/kP*

9.7 Betriebsmodus „Station / Client-Mode“



SSID des Remote Access Point *(32 Zeichen)*

Hier ist die Kennung des WLAN-Netzes (SSID, Service Set Identifier) einzugeben, mit welchem sich das Gerät verbinden soll.

Authentifizierung

Über den Parameter Authentifizierung kann konfiguriert werden, ob der Remote Access Point eine WLAN-Verschlüsselung verwendet.

Zur Auswahl steht:

- Keine
  Das WLAN ist nicht verschlüsselt.

- WPA2-PSK
  Als Verschlüsselungsstandard wird WPA2-PSK (WiFi Protected Access 2, pre-shared-key) verwendet.

Schlüssel *(nur bei WPA2-PSK, 63 Zeichen)*

Hier ist der verwendete Schlüssel anzugeben (8 … 63 Zeichen). Dieser wird zum Aufbau der WLAN-Verbindung zum Remote Access Point benötigt.

WPS (WiFi Protected Setup)

Hier wird konfiguriert, ob sich das Gerät über WPS (WiFi Protected Setup) mit dem Remote Access Point verbinden kann.

Zur Auswahl steht:

- Deaktiviert
- Temporär
- Dauerhaft (Speicherung der Zugangsdaten im Gerät)
  Durch die WPS Funktion werden die Authentifizierungseinstellungen überschrieben.

WARNUNG

- Das Gerät darf nur von einer zugelassenen Elektrofachkraft installiert und in Betrieb genommen werden.
- Die geltenden Sicherheits- und Unfallverhütungsvorschriften sind zu beachten.
- Das Gerät darf nicht geöffnet werden.
- Bei der Planung und Errichtung von elektrischen Anlagen sind die einschlägigen Richtlinien, Vorschriften und Bestimmungen des jeweiligen Landes zu beachten.

Produktdatenbank für ETS 5/6
www.weinzierl.de/de/products/740.2/ets6

Datenblatt
www.weinzierl.de/de/products/740.2/datasheet

CE-Erklärung
www.weinzierl.de/de/products/740.2/ce-declaration

Ausschreibungstext
www.weinzierl.de/de/products/740.2/tender-text

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

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

2026-01-26