

Technisches Handbuch

MDT IP Router



SCN-IP100.03

Weitere Dokumente :

Datenblätter :

https://www.mdt.de/download/MDT_DB_Interface_03.pdf

Montageanleitung :

https://www.mdt.de/download/MDT_AOI_USB_IP_Interface_03.pdf

History :

https://www.mdt.de/download/MDT_CL_IP_Devices.pdf

1 Inhalt

1 Inhalt.....	2
2 Übersicht	4
2.1 Anwendungsmöglichkeiten IP-Router	4
2.2 Anwendungsmöglichkeiten E-Mail Client	4
2.3 Anwendungsmöglichkeiten Zeitserver	4
2.4 Übersicht LEDS & Bedienung.....	5
2.5 Inbetriebnahme ohne Data Secure	6
2.6 Inbetriebnahme mit Data Secure	7
2.7 Topologie.....	8
2.7.1 Linienkoppler.....	8
2.7.2 Bereichskoppler.....	9
2.7.3 gemischte Verwendung.....	10
2.7.4 Funktion als Buszugriff (KNXnet/IP Tunneling)	11
2.7.5 Beispiel-Installation	11
3 Sicherheit -> IP Secure/Data Secure.....	12
3.1 Sicherheitsmechanismen IP Secure/Data Secure.....	12
3.2 Grundbegriffe	12
3.3 Mischbetrieb	15
3.4 Inbetriebnahme.....	15
3.5 Erweiterte Sicherheitsmechanismen	17
3.6 Voraussetzungen für KNX IP Secure/Data Secure.....	17
4 Parameter -> IP-Router.....	18
4.1 Allgemein.....	18
4.2 Gerät -> Einstellungen	20
4.3 Gerät -> IP –Konfiguration.....	21
4.3.1 Beispiel zur Vergabe von IP-Adressen	22
4.4 Hauptlinie (IP).....	23
4.5 Linie (KNX TP)	25
4.6 Kommunikationseinstellungen.....	27
4.6.1 Vorgehen ETS 4.....	27
4.6.2 Vorgehen ETS 5.....	28
4.6.3 Tunneling Verbindungen setzen.....	30

5 Parameter → E-Mail Client	31
5.1 Allgemeine Einstellungen	31
5.1.1 Allgemein	31
5.1.2 Web-Interface	32
5.1.3 Uhrzeit/Datum	33
5.2 E-Mail Funktionen	34
5.2.1 Statuselemente	35
5.2.2 Bit Alarme	37
Makros	38
5.2.3 Text Alarme	39
5.2.4 Status Berichte	40
5.2.5 spezielles Verhalten und Fehlerbehandlung	41
5.3 Übersicht Kommunikationsobjekte	42
5.4 Sichere Gruppenadressenkommunikation	44
6 Web-Interface	45
6.1 Aufruf des Web-Interface	45
6.2 Übersicht Web-Interface	46
6.3 Einstellen der E-Mail Funktionalität	47
6.4 E-Mail – Error Codes & Behebung	50
6.5 E-Mails als Push-Nachricht empfangen	50
6.6 E-Mail als SMS empfangen	50
7 Index	51
7.1 Abbildungsverzeichnis	51
7.2 Tabellenverzeichnis	52
8 Anhang	53
8.1 Gesetzliche Bestimmungen	53
8.2 Entsorgungsroutine	53
8.3 Montage	53
8.4 Revisionshistorie	54

2 Übersicht

Der MDT IP Router, SCN-IP100.03, verfügt über 2 parallel laufende Applikationen.

Zum einen über die Applikation für den IP Router, welche den Zugriff auf den Bus über Ethernet ermöglicht sowie den Einsatz als Bereichs- oder Linienkoppler.

Die zweite Applikation liegt auf der TP-Seite und kann vom KNX getriggert E-Mails senden, als Zeitserver dienen und ermöglicht den Zugriff auf das Gerät via Web-Interface.

Wichtig: Da es sich um 2 verschiedene Applikationen handelt müssen beide Applikationen unabhängig voneinander programmiert werden und dem IP-Router müssen 2 physikalische Adressen zugewiesen werden!

Besonderheiten:

- Einsatz als Zeit-Server
- umfangreiche E-Mail Funktionalität mit Statusinformationen aus dem KNX-Bus
- Versorgung komplett aus dem KNX-Bus, keine zusätzliche Spannungsversorgung notwendig!
- IP Secure für Interface Applikation
- Data Secure für die E-Mail Applikation

2.1 Anwendungsmöglichkeiten IP-Router

Der MDT IP-Router verbindet den KNX-Bus mit einem Ethernet-Netzwerk. Über das Netzwerk können KNX-Telegramme an andere Geräte gesendet oder von diesen empfangen werden. Das Gerät verwendet zur Kommunikation das KNXnet/IP-Protokoll der KNX-Association. Er arbeitet somit als Programmierschnittstelle und ersetzt dadurch eine RS232 bzw. USB Schnittstelle.

Der IP-Router beinhaltet neben der Tunneling Funktion zur Punkt-zu-Punkt-Verbindung zusätzlich die Funktionen eines Linienkopplers (Routing). Dadurch kann der IP-Router Telegramme im Netzwerk zu anderen Linien und Bereichen verteilen und von dort empfangen.

Die Spannungsversorgung erfolgt über den KNX-Bus.

2.2 Anwendungsmöglichkeiten E-Mail Client

Der E-Mail Client kann Status-Berichte, Bit-Alarme und Text-Alarme aussenden. Alle E-Mail Events können via KNX-Telegramme ausgelöst werden. Darüber hinaus können Status-Berichte auch zu festen Zeitpunkten gesendet werden – der E-Mail Client verfügt hierfür über die Funktionalität als Uhren-Master. Alle E-Mails können an bis zu 3 Adressen gleichzeitig gesendet werden. Die Einstellung der E-Mail Funktionalität erfolgt bequem im Web-Interface.

2.3 Anwendungsmöglichkeiten Zeitserver

Der IP-Router empfängt Datum und Uhrzeit vom NTP Server und kann diese als „Master“ an weitere KNX-Geräte über den Bus verteilen.

2.4 Übersicht LEDS & Bedienung

Das nachfolgende Bild zeigt den Aufbau des Gerätes und die Lage der LEDS:



Abbildung 1: Aufbau Hardwaremodul

1. LED Bus Status - LAN
2. LED Bus Status - KNX
3. LED Traffic - LAN
4. LED Traffic - KNX
5. Weiterleitung von Gruppentelegrammen
6. Weiterleitung von physikalischen Adressen
7. Funktionsknopf
8. Programmier - LED
9. Programmier Knopf

Funktion Programmier-Knopf:

Kurzes Drücken: Programmier LED leuchtet dauerhaft rot -> IP Router ist im Programmiermodus

Langes Drücken: Programmier LED blinkt rot -> E-Mail Client ist im Programmiermodus

Funktion des Funktionsknopfs:

Drücken des Knopfes für 3 Sekunden: IP Router steht auf manuell mit Funktionalität gemäß der Einstellungen im Menü „Allgemein“. Durch nochmaliges betätigen des Funktionsknopfs für 3 Sekunden wird der Router wieder umgestellt.

Gerät zurücksetzen:

Drücken des Knopfes für Funktionsknopf für 15sec, die LEDs 1,2,5 und 6 leuchten rot. Nun lassen Sie den Funktionsknopf los und drücken ihn anschließend noch einmal bis alle LEDs ausgehen. Das Gerät führt einen Neustart durch.

Nun ist das Gerät auf Werkseinstellung zurückgesetzt.

Der Master Reset setzt auch die Secure Einstellungen auf den FDSK (Factory Default Setup Key) zurück. Somit ist ein Download des Geräts nur mit dem FDSK möglich.

	Grün	Rot
LED 1 Bus Status - LAN	Aus: LAN Error An: LAN OK	On: Manueller Modus aktiv
LED 2 Bus Status - KNX	Aus: KNX Bus: Error oder nicht verbunden An: KNX Bus OK	
LED 3 Traffic - LAN	Blinkend: Bus Last auf LAN-Seite Aus: Keine Bus Last auf LAN-Seite Geschwindigkeit bis zu 10 Mbit/s	Blinkend: Übertragungsfehler auf LAN Seite
LED 4 Traffic - KNX	Blinkend: Bus Last auf KNX Seite Aus: Keine Bus Last auf KNX Seite	Blinkend: Übertragungsfehler auf KNX Seite
LED 5 Weiterleitung von Gruppen-telegrammen	Weiterleitung von Gruppentelegrammen - Aus: LAN und KNX verschieden - Filtertabelle aktiv Grün und Route: alles weiterleiten	Sperren
LED 6 Weiterleitung von physikalischen Adressen	Weiterleitung von physikalisch Adressen - Aus: LAN und KNX verschieden - Filtertabelle aktiv Grün und Gelb: alles weiterleiten	Gelb: Sperren

Tabelle 1: Übersicht LEDs

2.5 Inbetriebnahme ohne Data Secure

Folgendes Vorgehen wird für die Inbetriebnahme des SCN-IP100.03 empfohlen:

1. Einfügen der Applikation „SCN-IP100.02 – KNX IP Router“
2. Konfigurieren des IP-Interface
3. Übertragen der physikalischen Adresse und der Applikation des IP-Interface. Hierzu muss die Programmier­taste **kurz** gedrückt werden. Die Programmier-LED leuchtet daraufhin dauerhaft rot.
4. Nach erfolgreicher Übertragung der physikalischen Adresse und der Applikation erlöscht die rote LED wieder.
5. Einfügen der Applikation „SCN-IP100.02 – IP Router Email- und Zeitserverfunktion“
6. Konfigurieren des E-Mail Clients
7. Übertragen der physikalischen Adresse und der Applikation des E-Mail Clients. Hierzu muss die Programmier­taste **lange** gedrückt werden. Die Programmier-LED blinkt daraufhin rot.
8. Nach erfolgreicher Übertragung der physikalischen Adresse und der Applikation erlöscht die rote LED wieder.
9. Aufrufen des Web-Clients zur Konfiguration der E-Mail Adressen durch öffnen eines Internet-Browsers und Aufruf der Adresse: http:\\IP-Adresse:Port, z.B.: http:\\192.168.1.178:8080 für die IP-Adresse 192.168.1.178 und den http-Port 8080

Wichtig: Wird die IP-Adresse des IP-Routers nachträglich geändert, so muss das Gerät einen Neustart durchführen. Dieser Neustart wird nach der Applikationsprogrammierung in der ETS nicht automatisch ausgeführt. Hier muss ein manueller Neustart ausgeführt werden, welcher wahlweise über einen Rechtsklick auf das Gerät und anschließende Auswahl „Gerät zurücksetzen“ ausgeführt wird oder durch ein kurzes Abziehen des Bussteckers.

2.6 Inbetriebnahme mit Data Secure

Folgendes Vorgehen wird für die Inbetriebnahme des SCN-IP100.03 empfohlen:

1. Einfügen der Applikation „SCN-IP100.03 – IP Router Secure“
2. Eingabe des FDSK (Aufkleber seitlich am Gerät)
3. Konfigurieren des IP-Interface
4. Übertragen der physikalischen Adresse und der Applikation des IP-Interface. Hierzu muss die Programmier Taste **kurz** gedrückt werden. Die Programmier-LED leuchtet daraufhin dauerhaft rot.
5. Nach erfolgreicher Übertragung der physikalischen Adresse und der Applikation erlischt die rote LED wieder.
6. Einfügen der Applikation „SCN-IP100.03 – IP Router Email- und Zeitserverfunktion“
7. Eingabe des FDSK (Aufkleber seitlich am Gerät)
8. Konfigurieren des E-Mail Clients
9. Übertragen der physikalischen Adresse und der Applikation des E-Mail Clients. Hierzu muss die Programmier Taste **lange** gedrückt werden. Die Programmier-LED blinkt daraufhin rot.
10. Nach erfolgreicher Übertragung der physikalischen Adresse und der Applikation erlischt die rote LED wieder.
11. Aufrufen des Web-Clients zur Konfiguration der E-Mail Adressen durch öffnen eines Internet-Browsers und Aufruf der Adresse: `http://IP-Adresse:Port`, z.B.: `http://192.168.1.178:8080` für die IP-Adresse 192.168.1.178 und den http-Port 8080

Wichtig: Durch Deaktivieren der „sicheren Inbetriebnahme“ in den Eigenschaften -> Einstellungen des Geräts wird das Gerät „unsicher“, also im „Plain Mode“, betrieben. Wenn Sie aufgefordert werden den FDSK des Geräts einzugeben, können Sie diesen Dialog mit dem Button „Später“ überspringen. Data Secure/IP Secure kann auch nachträglich aktiviert werden indem die „sichere Inbetriebnahme“ aktiviert wird und der FDSK vorhanden ist. Weitere Details zu IP Secure/Data Secure finden Sie unter 3 Sicherheit -> IP Secure/Data Secure.

2.7 Topologie

2.7.1 Linienkoppler

Das nachfolgende Bild zeigt den IP-Router als Linienkoppler:

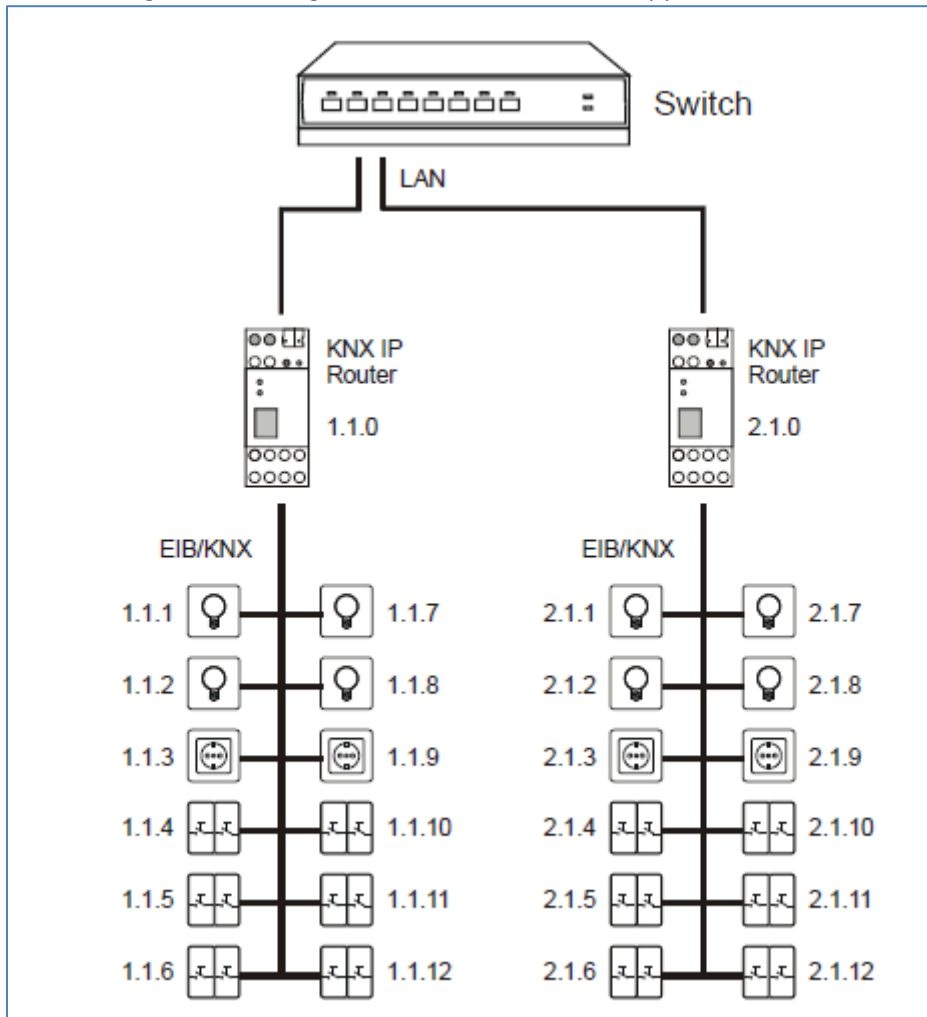


Abbildung 2: KNX IP Router als Linienkoppler

Der IP-Router kann in KNX-Anlagen die Funktion eines Linienkopplers übernehmen. Dafür muss er die physikalische Adresse eines Linienkopplers (1.1.0...15.15.0) erhalten. Es aktuell bis zu 225 Linien in der ETS angelegt werden.

Diese Topologie wird als flache Topologie bezeichnet werden, da es KNX Haupt- oder Bereichslinien gibt. Die Telegramme einer KNX-Linie werden direkt auf das Ethernet übertragen.

2.7.2 Bereichskoppler

Das nachfolgende Bild zeigt den IP-Router als Bereichskoppler:

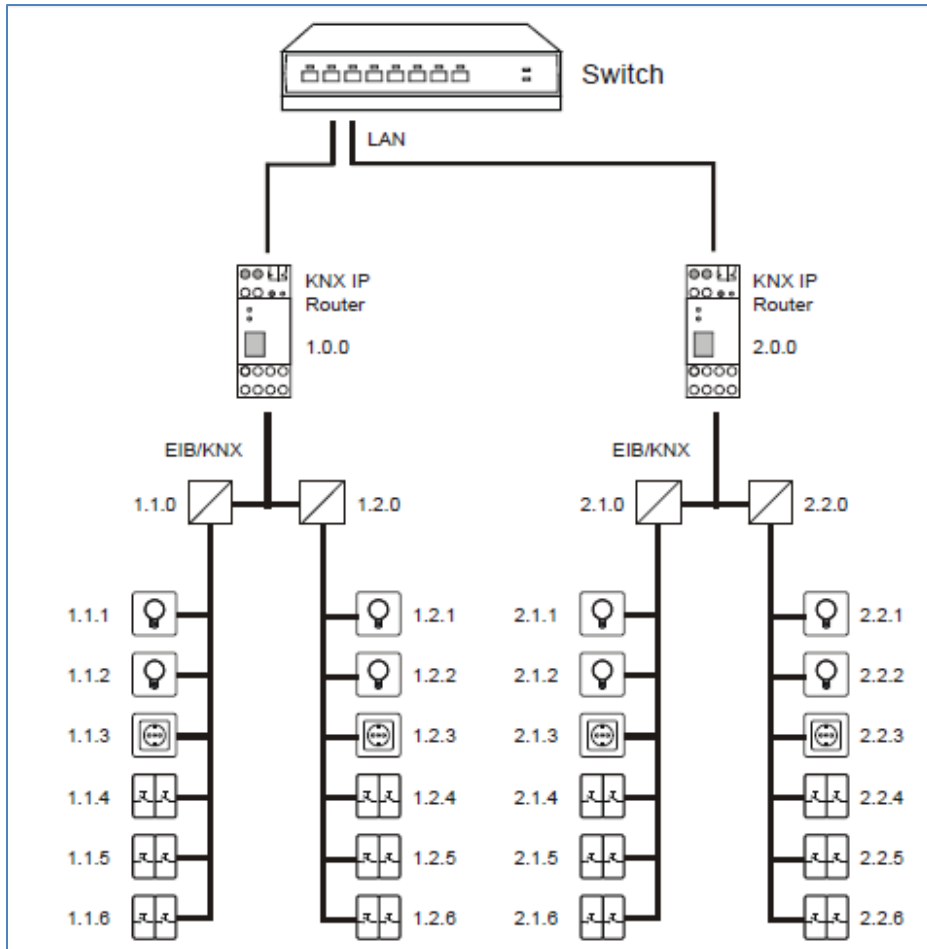


Abbildung 3: KNX IP Router als Bereichskoppler

Der IP-Router kann in größeren KNX-Anlagen die Funktion eines Bereichskopplers übernehmen. Dafür muss er die physikalische Adresse eines Bereichskopplers (1.0.0...15.0.0) erhalten. Aktuell können in einem ETS-Projekt bis zu 15 Bereiche mit Bereichskopplern angelegt werden. Jedem Bereich sind in diesem Beispiel 2 Linien untergeordnet, welche z.B. mit dem Linienkoppler SCN-LK001.02 verknüpft werden können.

2.7.3 gemischte Verwendung

Das nachfolgende Bild zeigt den IP-Router als Bereichskoppler(IP Router 1.0.0.) und Linienkoppler(IP Router 2.1.0):

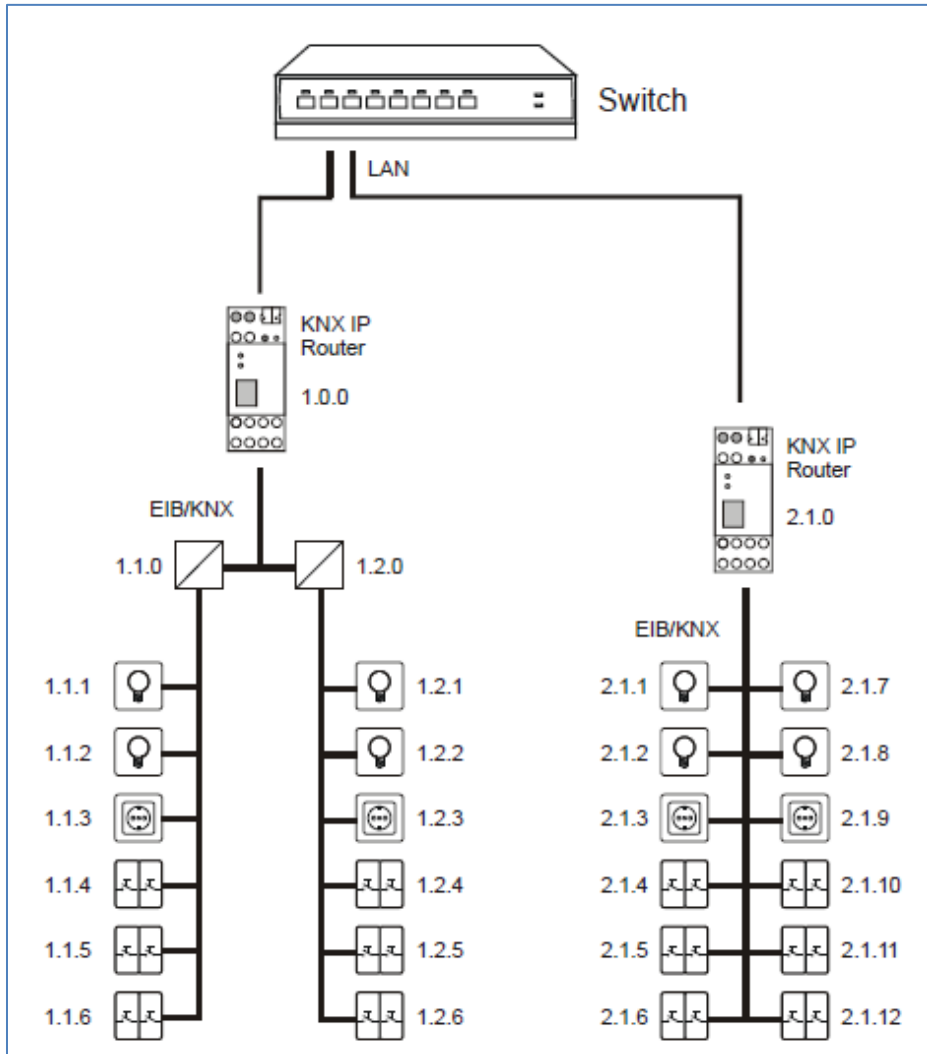


Abbildung 4: KNX IP Router als Bereichs- und Linienkoppler

Ist es innerhalb einer KNX-Anlage nötig, den IP-Router an einer Stelle z.B. Büro, als Bereichskoppler und an anderer Stelle, z.B. entfernte Tiefgarage als Linienkoppler einzusetzen, so können zwei verschiedene IP-Router diese Funktion übernehmen.

Dabei muss nur beachtet werden, dass der IP-Router als Linienkoppler die Linienkoppleradresse aus einem freien Bereich verwendet, wie z.B. oben im Bild 2.1.0.

Dem IP-Router als Bereichskoppler (1.0.0) können weitere Linien untergeordnet werden.

2.7.4 Funktion als Buszugriff (KNXnet/IP Tunneling)

Der KNX IP Router kann als Schnittstelle zum KNX/EIB genutzt werden. Es kann von jedem Punkt im LAN auf den KNX/EIB zugegriffen werden. Dazu muss eine zweite physikalische Adresse vergeben werden. Dies wird in den folgenden Kapiteln näher beschrieben.

2.7.5 Beispiel-Installation

Das nachfolgende Bild zeigt den beispielhaften Aufbau eines Netzwerks mit zwei IP-Routern jeweils als Bereichskoppler eingesetzt:

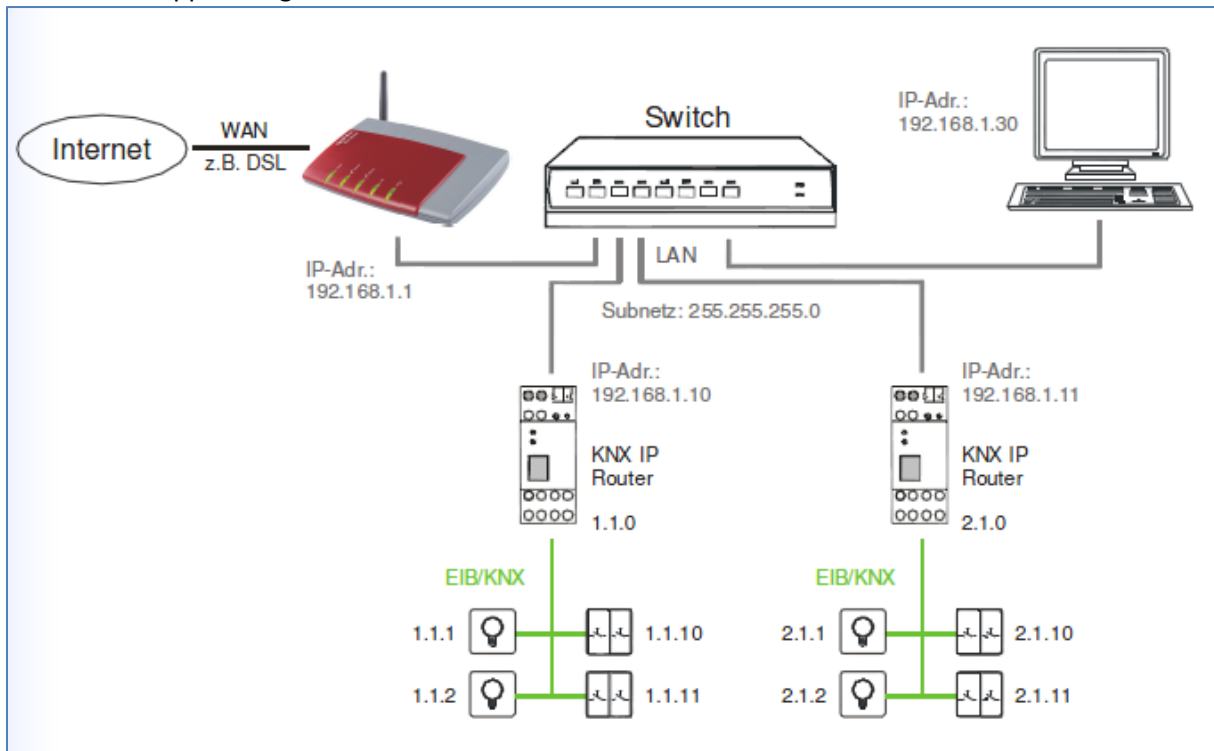


Abbildung 5: Beispiel für Installation

3 Sicherheit -> IP Secure/Data Secure

3.1 Sicherheitsmechanismen IP Secure/Data Secure

KNX Data Security unterscheidet 2 Mechanismen: IP Secure und Data Secure.

KNX IP Secure erlaubt von KNX Geräten ausgesendete Meldungen zu verschlüsseln und authentifizieren um diese sicher über die IP Ebene zu übertragen. So ist sichergestellt, dass KNX Tunneling oder Routing Meldungen auf IP nicht mitgelesen oder manipuliert werden können. KNX IP Secure bildet eine zusätzliche Sicherheitshülle, die den kompletten KNXnet IP Datenverkehr schützt.

KNX Data Secure ermöglicht die sichere Inbetriebnahme von Geräten die Data Security unterstützen sowie die verschlüsselte Übertragung von Gruppenadressen zwischen 2 Geräten die Data Secure unterstützen.

Damit 2 Geräte mit Data Secure sicher kommunizieren können müssen beide Geräte Data Secure unterstützen. Es ist jedoch auch möglich, dass ein Data Secure Gerät mit einem Gerät kommuniziert, welches kein Data Secure unterstützt. In diesem Fall jedoch nur über eine ungesicherte Verbindung.

3.2 Grundbegriffe

FDSK

Jedes Secure Gerät wird mit dem „Factory Device Set up Key“ (FDSK) ausgeliefert. Diesen Schlüssel gibt der Systemintegrator/Installateur in die ETS ein, welche daraus einen gerätespezifischen Werkzeugschlüssel erzeugt. Die ETS sendet den Werkzeugschlüssel über den KNX Bus zum Gerät welches konfiguriert werden soll. Diese Übertragung wird mit dem FDSK Schlüssel verschlüsselt und authentifiziert. Nach dieser Erstinbetriebnahme akzeptiert das Gerät nur noch den empfangenen Werkzeugschlüssel. Der FDSK wird für die weitere Übertragung nicht mehr benötigt – es sei denn das Gerät wird über den Master Reset zurückgesetzt.

Die FDSK aller Geräte eines Projektes sollten nach der Erstinbetriebnahme vom Geräteaufkleber abgetrennt werden und projektspezifisch aufbewahrt werden.

Abgesicherter Modus – Secure Mode

Ist ein Gerät so parametrierbar das es nur verschlüsselt Daten überträgt, so spricht man vom abgesicherten Modus (Secure Mode).

Nicht abgesicherter Modus – Plain Mode

Ist ein Gerät so parametrierbar das es nur unverschlüsselt überträgt, so spricht man vom nicht abgesicherten Modus (Plain Mode).

Backbonekey, Backboneschlüssel

Wird ein KNX Bus über 2 IP Router mit Data Secure verbunden, so kommunizieren diese mit dem Backbone Key verschlüsselt. Dieser Schlüssel muss in allen Geräten identisch sein. Der Schlüssel wird von der ETS selbstständig vergeben und kann nicht verändert werden.

Inbetriebnahmepasswort

Das Inbetriebnahmepasswort wird in der ETS für den gesamten Vorgang/ Download bei der Inbetriebnahme/ Gerätesicherheit eines KNX IP Secure Gerät benötigt. Es dient hier auch der Authentifizierung der ETS gegenüber dem Gerät.

Es muss unterschiedlich zu Passwörtern von möglichen gesicherten, zusätzlichen Schnittstellen sein und stellt das sog. Management Level für die Gerätekonfiguration durch die ETS dar.

Nur die ETS selber kennt das Inbetriebnahmepasswort und kann Änderungen am Gerät vornehmen (Passwörter von gesicherten zusätzlichen Schnittstellen können verteilt werden, z.B an eine externe Visualisierung).

Das Inbetriebnahmepasswort kann durch den Benutzer angepasst werden und ist im Reiter Gerät -> Eigenschaften -> IP sichtbar:

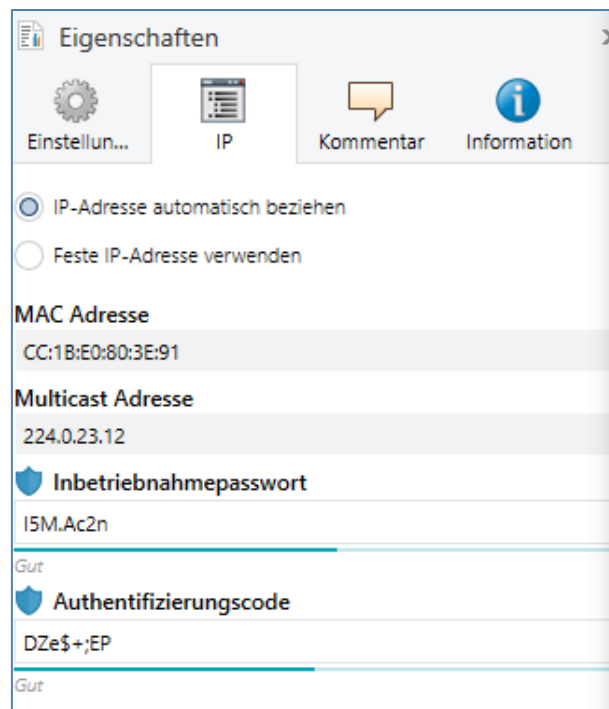


Abbildung 6: Inbetriebnahmepasswort

Es wird empfohlen jedem Gerät ein individuelles Inbetriebnahmepasswort zu geben und nicht ein universelles im gesamten Projekt oder gar projektübergreifend. Die ETS vergibt automatisch ein individuelles Passwort.

Authentifizierungscode

Der Authentifizierungscode wird für die Authentifizierung von KNX IP Secure Geräten benötigt. Da der FDSK außerhalb der ETS bekannt ist muss, zum Beispiel als QR Code oder Geräte- Aufdruck muss dieser Schlüssel im ETS Projekt geändert werden.

Der FDSK wird mit einem (für dieses ETS Projekt und dieses KNX IP Secure Gerät) individuellen Authentifizierungscode ersetzt. Nachfolgende Kommunikation des Gerätes gegenüber der ETS erfolgen dann mit diesem (neuem) Authentifizierungscode (anstatt mit dem initialen FDSK).

Jedes KNX IP Secure Gerät besitzt demzufolge nach Inbetriebnahme einen individuellen* Authentifizierungscode der verschieden vom initialen FDSK ist.

* wenn nicht vom ETS Benutzer - bei mehreren Geräten - mit einem identischen Authentifizierungscode überschrieben

Der Authentifizierungscode kann in der ETS genauso verändert werden wie das Inbetriebnahmepasswort, siehe Abbildung 6: Inbetriebnahmepasswort.

Inbetriebnahme/Sichere Inbetriebnahme

Es kann für jedes Gerät entschieden werden ob die Inbetriebnahme gesichert oder ungesichert erfolgen soll. Erfolgt die Inbetriebnahme ungesichert, so ist das Gerät fortan wie ein normales gerät ohne Data Secure zu verwenden.

Standardmäßig setzt die ETS alle Geräte beim einfügen auf sichere Inbetriebnahme aktiv. Dieser Punkt kann vom benutzer unter Gerät->Eigenschaften->Einstellungen geändert werden:

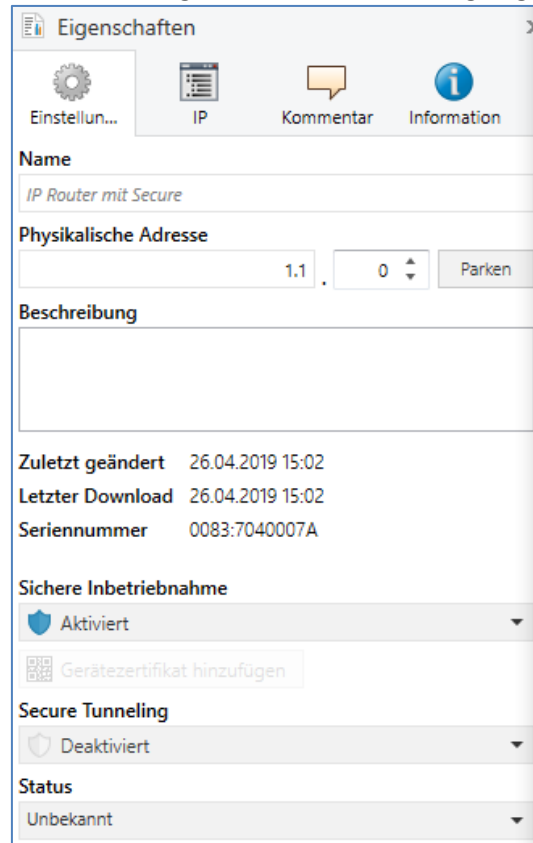


Abbildung 7: Sichere Inbetriebnahme/Secure Tunnel

Tunneling/Secure Tunneling

Tunneling bezeichnet eine KNX Punkt-zu-Punkt Verbindung auf dem TCP/IP Netzwerk. Für jedes IP Secure Gerät kann entschieden werden ob die Tunneling Verbindungen secure oder plain übertragen werden, siehe Abbildung 7: Sichere Inbetriebnahme/Secure Tunnel.

3.3 Mischbetrieb

IP Secure

Gesicherte Geräte können nur mit Geräten kommunizieren, welche auch gesichert sind. Mischungen von z.B. gesicherten KNX IP Secure Koppler mit ungesicherten KNX IP Secure Geräten oder normalen KNX IP Geräten gehen nicht.

Data Secure

Bei Data Secure können Geräte, welche Data Secure unterstützen, auch mit Geräten kommunizieren, welche kein Data Secure unterstützen. Ein Mischbetrieb in einem Projekt ist somit möglich. Sollen allerdings alle Daten einer Gruppenadresse verschlüsselt übertragen werden, so müssen alle Geräte dessen Objekte mit diese Gruppenadresse verbunden sind Data Secure unterstützen.

3.4 Inbetriebnahme

Um Secure Geräte in Betrieb zu nehmen verlangt die ETS folgende Vorgehensweise:

1. Produktdatenbank laden

Beim Laden der Produktdatenbank werde Sie in der Regel direkt aufgefordert den FDSK des Gerätes einzugeben. es öffnet sich folgender Dialog:

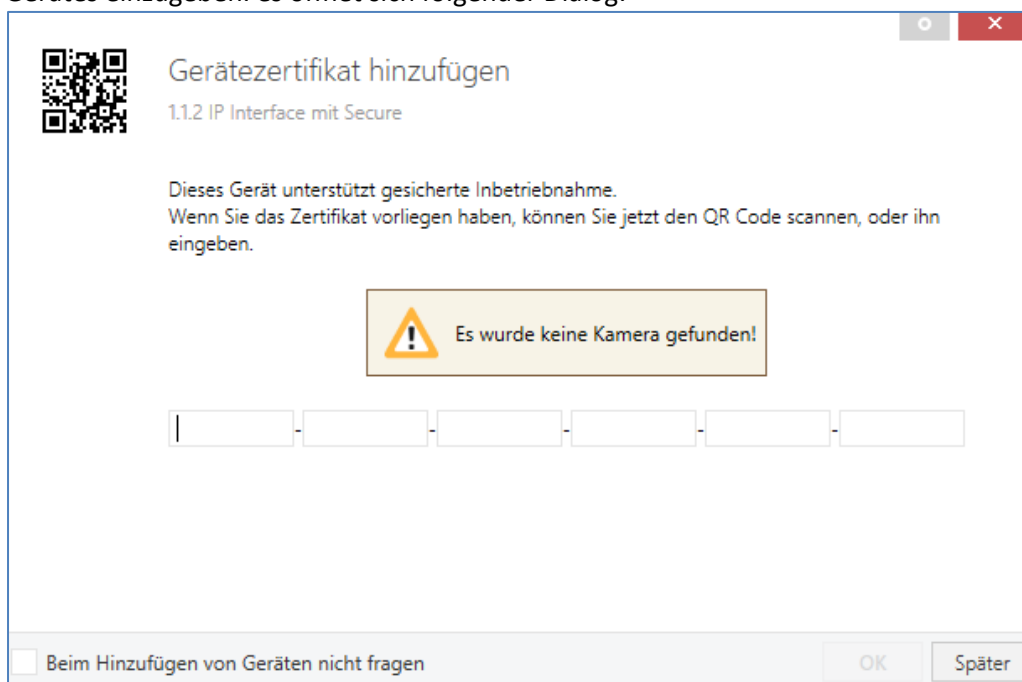


Abbildung 8: Eingabe FDSK

Sie können den FDSK manuell eingeben oder den QR Code via einer Kamera einlesen. Wollen Sie den FDSK nicht direct einlesen oder haben ihn nicht zur Hand, so können Sie dies auch nachträglich machen indem Sie diesen Dialog mit "Später" bestätigen.

Um den FDSK nachträglich einzugeben wählen Sie das jeweilige Projekt an und wählen den Reiter Sicherheit aus:

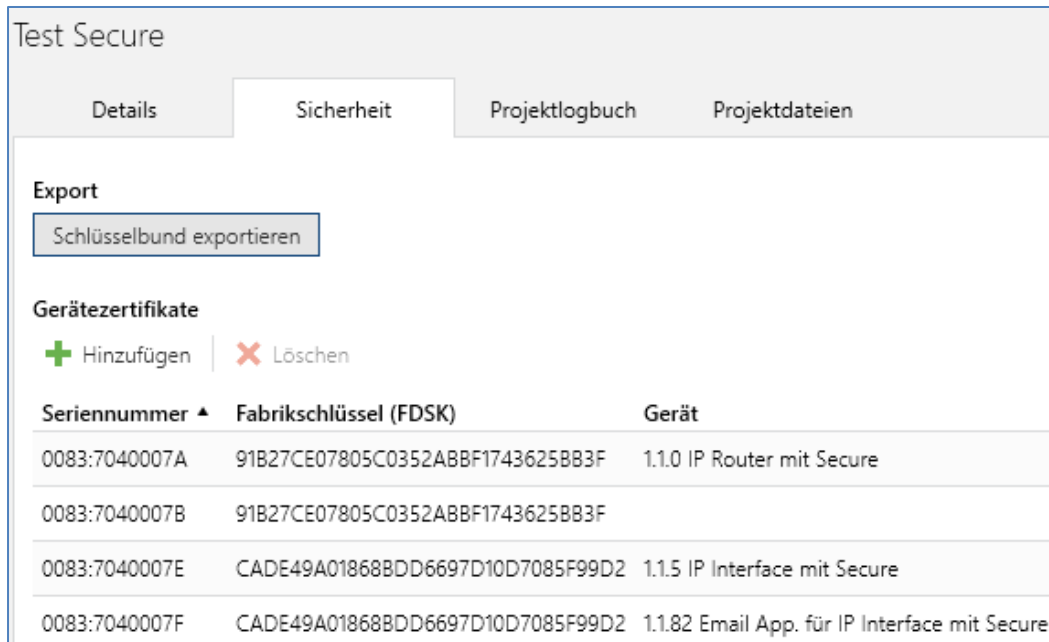


Abbildung 9: Nachträgliche Eingabe FDSK

Hier können Sie nun den Button “Hinzufügen” anwählen und den FDSK eingeben oder den QR Code scannen. Wurde der FDSK richtig erkannt, so decodiert die ETS den FDSK in Seriennummer und Fabrikschlüssel. Eine Zuordnung welcher Schlüssel zu welchem Gerät gehört, macht die ETS automatisch. Somit können Sie einfach nacheinander alle im Projekt verwendeten FDSK eingeben.

2. Aufkleber/Device Certificate abziehen

Um Sabotage zu verhindern muss das Device Certificate an einem sicheren Ort aufbewahrt werden. Daher ist es wichtig dieses vor dem Einbau des Geräts abzuziehen und projektbezogen aufzubewahren.

3. Inbetriebnahmepasswort/Authentifizierungscode anpassen (optional)

Das Inbetriebnahmepasswort pro Gerät und der Authentifizierungscode pro Gerät können nun vom Benutzer angepasst werden. Die ETS vergibt jedoch initiale Passwörter, sodass dies nicht zwangsläufig gemacht werden muss. Für jedes Gerät sollten jedoch individuelle Passwörter vergeben werden.

4. Download der Applikation

Nun kann die Applikation in das Gerät heruntergeladen werden.

5. Inbetriebnahmepasswort und Authentifizierungscode verteilen

Falls eine Visu/ein Fernzugriff erfolgen soll, so muss vor dem Verbindungsaufbau das Inbetriebnahmepasswort und (optional) der Authentifizierungscode (damit beweist der Gegenüber Kenntnisse über das Projekt) eingegeben werden.

3.5 Erweiterte Sicherheitsmechanismen

Zusätzlich zur Verwendung von KNX IP Secure sollten folgende Richtlinien bei der Planung berücksichtigt werden:

- keine Ports von Routern Richtung Internet freigeben
- LAN/WLAN Anlage über eine Firewall sichern
- Wenn kein externer Zugriff auf die KNX Anlage erforderlich ist, so kann das Standard Gateway auf den Wert 0 gesetzt werden. Somit ist die Kommunikation ins Internet unterbunden
- Der Zugang zur KNX Installation aus dem Internet sollte über eine VPN Verbindung realisiert werden

3.6 Voraussetzungen für KNX IP Secure/Data Secure

Um Geräte mit Data Secure/IP Secure in Betrieb nehmen zu können, muss mindestens die ETS 5.7 verwendet werden.

4 Parameter -> IP-Router

4.1 Allgemein

Die folgenden Parameter können im Untermenü „Allgemein“ eingestellt werden:

Langsame Tunneling-Verbindungen unterstützen	<input type="radio"/> ja <input checked="" type="radio"/> nein
Manuell-Funktion	alle Telegramme weiterleiten
Abschaltung der Manuell-Funktion nach	4 Stunden
Webfrontend mit aktivierter Sicherheit	Einstellungen aktiv
DNS Server	0.0.0.0
HTTP port	<input type="radio"/> 80 <input checked="" type="radio"/> 8080

Abbildung 10: Allgemeine Einstellungen

Die nachfolgende Tabelle zeigt die Einstellmöglichkeiten für dieses Untermenü:

ETS-Text	Wertebereich [Defaultwert]	Kommentar
Langsame Tunneling Verbindungen unterstützen	<ul style="list-style-type: none"> • Ja • Nein 	Anpassen des Timeout bei Tunnelverbindungen. Standardmäßig werden langsame Verbindungen nicht unterstützt und es wird ein kurzer Timeout für die UDP Verbindung verwendet. Dieser kann durch die Unterstützung von langsamen Verbindungen hochgesetzt werden was insbesondere für Tunnelverbindungen über das Internet notwendig sein kann.
Rückfallzeit nach manueller Umstellung	<ul style="list-style-type: none"> • 10min • 1 Stunde • 4 Stunden • 8 Stunden 	Einstellung der automatischen Rückfallzeit vom manuellen Modus in den automatischen Modus
Manuelle Umstellung	<ul style="list-style-type: none"> • nicht aktiv • Alle Telegramme weiterleiten • Alle physikalischen Adressen weiterleiten • Alle Gruppenadressen weiterleiten 	Definiert das Verhalten nach manueller Umstellung

Web-Interface mit aktivierter Sicherheit	<ul style="list-style-type: none"> • Einstellungen aktiv • nur Statusanzeige • Einstellungen gesperrt 	Einstellung des Web-Interface für Firmware Update/Vergabe Tunneling Verbindung, etc.: Einstellungen aktiv: Alle Einstellungen des Web-Interface sind für den Benutzer zugänglich. Nur Statusanzeige: Sicherheitskritische Funktionen werden nur als Status im Web Interface angezeigt und es sind keine Änderungen möglich. Einstellungen gesperrt: Es kann kein Web Interface aufgerufen werden.
http Port	<ul style="list-style-type: none"> • 80 • 8080 	Einstellung des http Ports für das Web Interface
DNS Server	0.0.0.0	Eingabe DNS Server

Tabelle 2: Parameter - Allgemein

4.2 Gerät -> Einstellungen

Das nachfolgende Bild zeigt die Einstellungen des IP Interface:

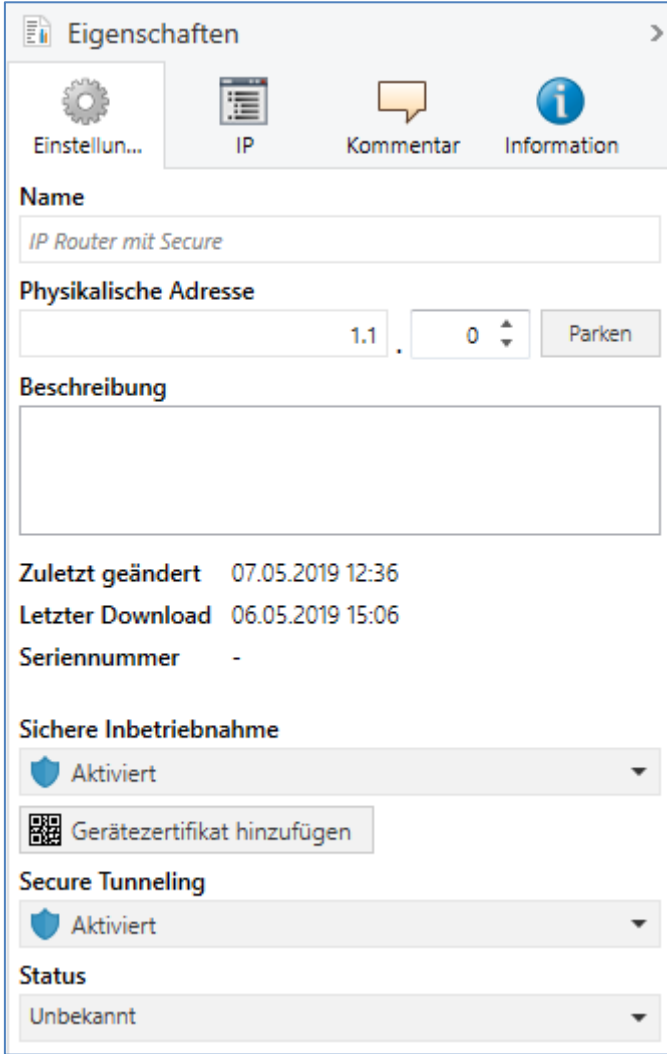


Abbildung 11: Gerät -> Einstellungen

Name

Der Name beschreibt unter anderem wie die Verbindung in der ETS angezeigt wird. Es kann ein beliebiger Name mit einer Maximallänge von 30 Zeichen angegeben werden.

Sichere Inbetriebnahme

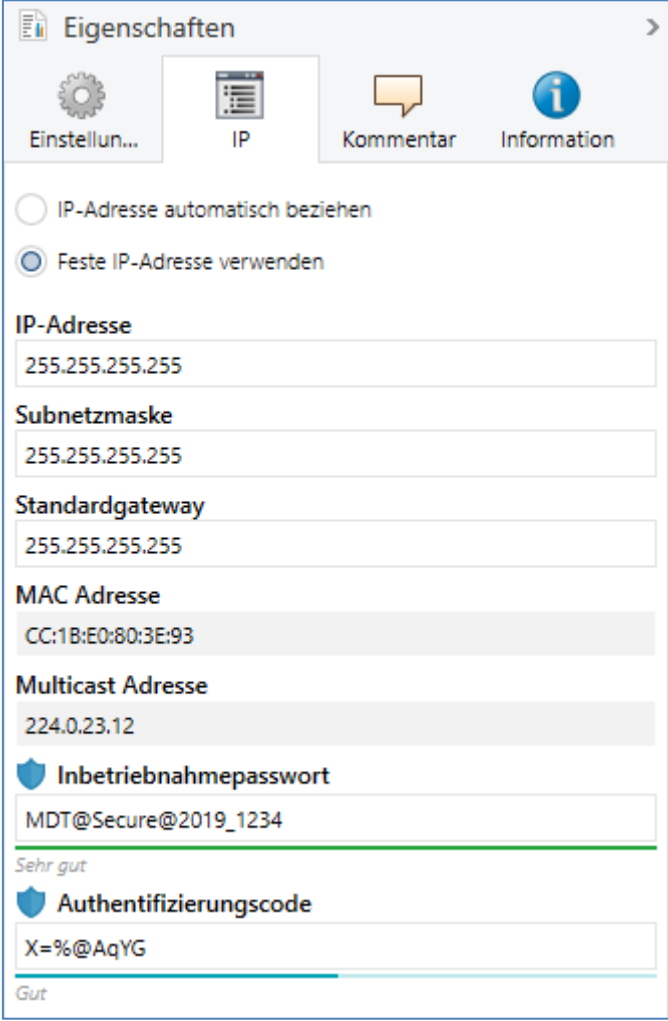
Aktivierung/Deaktivierung der sicheren Inbetriebnahme. Wird ein Gerät nicht sicher in Betrieb genommen, so sind die Secure Funktionen deaktiviert, siehe auch 3 Sicherheit -> IP Secure/Data Secure.

Secure Tunneling

Aktivierung/Deaktivierung des Secure Tunneling. Wird das Secure Tunneling aktiviert, so ist die Kommunikation über die Tunneling Verbindung verschlüsselt, siehe auch 3 Sicherheit -> IP Secure/Data Secure.

4.3 Gerät -> IP -Konfiguration

Das nachfolgende Bild zeigt die IP Einstellungen des Geräts:



The screenshot shows a configuration window titled 'Eigenschaften' with a sub-tab 'IP'. It contains the following fields and options:

- Radio buttons for 'IP-Adresse automatisch beziehen' (unselected) and 'Feste IP-Adresse verwenden' (selected).
- Text input for 'IP-Adresse' with value '255.255.255.255'.
- Text input for 'Subnetzmaske' with value '255.255.255.255'.
- Text input for 'Standardgateway' with value '255.255.255.255'.
- Text input for 'MAC Adresse' with value 'CC:1B:E0:80:3E:93'.
- Text input for 'Multicast Adresse' with value '224.0.23.12'.
- Text input for 'Inbetriebnahmepasswort' with value 'MDT@Secure@2019_1234'. Below it is a green progress bar and the text 'Sehr gut'.
- Text input for 'Authentifizierungscode' with value 'X=%@AqYG'. Below it is a blue progress bar and the text 'Gut'.

Abbildung 12: IP Einstellungen

IP-Adresse automatisch beziehen

Das Gerät bezieht die Adresse automatisch. Es muss ein DHCP Server vorhanden sein.

Feste IP-Adresse verwenden

Vorgabe einer festen IP-Adresse durch den Benutzer.

Subnetzmaske/Standardgateway

Kann nur bei der Einstellung „Feste IP-Adresse verwenden“ eingestellt werden.

Die Netzmaske dient dem Gerät 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 Gateway, das die Weiterleitung übernimmt.

Die Einstellung des Gateways ermöglicht es, dass Netzwerke, welche auf unterschiedlichen Protokollen basieren miteinander kommunizieren können.

Hinweis: Soll das KNX IP Interface nur im lokalen LAN verwendet werden, kann der Eintrag 0.0.0.0 bestehen bleiben.

Die Netzwerkeinstellungen des kommunizierenden PCs können in den Netzwerkeinstellungen des PCs abgelesen werden.

MAC Adresse

Ist vom Gerät vorgegeben.

Multicast Adresse

Die Multicast Adresse wird vom Backbone vorgegeben und kann im Projekt im Reiter „Topologie Backbone“ verändert werden.

Inbetriebnahmepasswort

Festlegen des Inbetriebnahmepassworts (optional), siehe auch 3 Sicherheit -> IP Secure/Data Secure.

Authentifizierungscode

Festlegen des Authentifizierungscode (optional), siehe auch 3 Sicherheit -> IP Secure/Data Secure.

4.3.1 Beispiel zur Vergabe von IP-Adressen

Mit einem PC soll auf das KNX IP Interface zugegriffen werden. Der PC hat folgende IP-Einstellungen:

IP-Adresse des PCs: **192.168.1.30**
Subnetz des PCs: **255.255.255.0**

Das KNX IP Interface befindet sich im selben lokalen LAN, d.h. er 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 Routers 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. Folgende Einstellungen können also im IP-Interface gemacht werden:

IP-Adresse des IP Interface: **192.168.1.31**
Subnetz des IP Interface: **255.255.255.0**

4.4 Hauptlinie (IP)

Die folgenden Parameter können im Untermenü „Routing(KNX-->IP)“ eingestellt werden:

Telegrammweiterleitung	Gruppen und Physikalische: filtern
Gruppentelegramme: Hauptgruppe 0...13	filtern
Gruppentelegramme: Hauptgruppe 14...31	filtern
Physikalische Telegramme	filtern

Abbildung 13: Einstellungen Hauptlinie

Die Tabelle zeigt die Einstellbereiche für die einzelnen Parameter:

ETS-Text	Wertebereich [Defaultwert]	Kommentar
Einstellungen	<ul style="list-style-type: none"> ▪ Gruppen filtern, Phys. blockieren ▪ Gruppen, Phys. filtern ▪ Gruppen weiterleiten, Phys. filtern ▪ Gruppen und Physikalische weiterleiten ▪ Individuell einstellen 	Einstellung der Filterung der Telegramme auf der Hauptlinie
Gruppentelegramme: Hauptgruppe 0..13	<ul style="list-style-type: none"> ▪ alles weiterleiten ▪ blockieren ▪ filtern 	Festlegung der Behandlung von Gruppentelegrammen der Hauptgruppe 0-13
Gruppentelegramme: Hauptgruppe 14..31	<ul style="list-style-type: none"> ▪ alles weiterleiten ▪ blockieren ▪ filtern 	Festlegung der Behandlung von Gruppentelegrammen der Hauptgruppe 14-31
Physikalische Adressen	<ul style="list-style-type: none"> ▪ alles weiterleiten ▪ blockieren ▪ filtern 	Festlegung wie physikalisch adressierte Telegramme behandelt werden sollen

Tabelle 3: Einstellungen Hauptlinie

Die Auswirkungen der einzelnen Einstellungen bei den jeweiligen Parametern sind nachfolgend näher beschrieben:

Gruppentelegramme:

- **blockieren**
Kein Gruppentelegramm der jeweiligen Hauptgruppen wird nach IP weitergeleitet.
- **weiterleiten**
Alle Gruppentelegramme der jeweiligen Hauptgruppen werden unabhängig von der Filtertabelle nach IP weitergeleitet.
- **filtern**
Hier wird anhand der Filtertabelle geprüft, ob das empfangene Gruppentelegramm nach IP weitergeleitet wird. Die Filtertabelle wird von der ETS automatisch erzeugt.

Physikalisch adressierte Telegramme:

- **blockieren**
Physikalisch adressierte Telegramme werden vom KNX/IP-Router gesperrt. Mit dieser Einstellung ist es nicht möglich, aus der Linie unterhalb des KNX/IP-Routers heraus in eine andere Linie hinein physikalisch adressierte Telegramme zu schicken (z.B. während der Programmierung).
- **weiterleiten**
Es werden alle physikalisch adressierten Telegramme vom KNX Bus zu IP übertragen.
- **filtern**
Es werden nur die physikalisch adressierten Telegramme vom KNX Bus zu IP übertragen, welche die Linie des KNX/IP-Routers verlassen sollen.

4.5 Linie (KNX TP)

Die folgenden Parameter können im Untermenü „Routing(IP-->KNX)“ eingestellt werden:

Telegrammweiterleitung	Gruppen und Physikalische: filtern
Gruppentelegramme: Hauptgruppe 0...13	filtern
Gruppentelegramme: Hauptgruppe 14...31	filtern
Physikalische Telegramme	filtern
Physikalische Telegramme: Wiederholung bei Fehlern auf Linie	bis zu 3 Wiederholungen
Gruppentelegramme: Wiederholung bei Fehlern auf Linie	bis zu 3 Wiederholungen
Telegramme auf Linie bestätigen	wenn weitergeleitet
Eigene Telegramme bestätigen	nein
Konfigurieren über Linie (KNX TP)	<input checked="" type="radio"/> zulassen <input type="radio"/> sperren

Abbildung 14: Einstellungen Nebenlinie

Die Tabelle zeigt die Einstellbereiche für die einzelnen Parameter:

ETS-Text	Wertebereich [Defaultwert]	Kommentar
Einstellungen	<ul style="list-style-type: none"> ▪ Gruppen filtern, Phys. blockieren ▪ Gruppen, Phys. filtern ▪ Gruppen weiterleiten, Phys. filtern ▪ Gruppen und Physikalische weiterleiten ▪ Individuell einstellen 	Einstellung der Filterung der Telegramme auf der Hauptlinie
Gruppentelegramme: Hauptgruppe 0..13	<ul style="list-style-type: none"> ▪ blockieren ▪ alles weiterleiten ▪ filtern 	Festlegung der Behandlung von Gruppentelegrammen der Gruppen 0-13
Gruppentelegramme: Hauptgruppe 14..31	<ul style="list-style-type: none"> ▪ blockieren ▪ alles weiterleiten ▪ filtern 	Festlegung der Behandlung von Gruppentelegrammen der Gruppen 14-31
Physikalische Adressen	<ul style="list-style-type: none"> ▪ blockieren ▪ alles weiterleiten ▪ filtern 	Festlegung wie mit individuell adressierten Telegrammen verfahren werden soll

Physikalische Adressen: Wiederholung bei Fehlern auf der Linie	<ul style="list-style-type: none"> ▪ nein ▪ bis zu 3 Wiederholungen ▪ nur eine Wiederholung 	Festlegung, ob das Telegramm im Fehlerfall wiederholt werden soll
Wiederholungssenden von Gruppentelegrammen	<ul style="list-style-type: none"> ▪ nein ▪ bis zu 3 Wiederholungen ▪ nur eine Wiederholung 	Festlegung, ob das Telegramm im Fehlerfall wiederholt werden soll
Telegramme auf Linie bestätigen	<ul style="list-style-type: none"> ▪ wenn weitergeleitet ▪ immer 	Festlegung ob der Router einen Acknowledge senden soll
Eigene Telegramme bestätigen	<ul style="list-style-type: none"> ▪ ja ▪ nein 	Festlegung ob der Router einen Acknowledge senden soll
Konfigurieren über Linie (KNX TP)	<ul style="list-style-type: none"> ▪ sperren ▪ freigeben 	Festlegung ob von TP-Seite programmiert werden kann

Tabelle 4: Einstellungen Nebenlinie

Die Auswirkungen der einzelnen Einstellungen bei den jeweiligen Parametern sind nachfolgend näher beschrieben:

Gruppentelegramme:

- **blockieren**
Kein Gruppentelegramm der jeweiligen Hauptgruppen wird nach KNX/EIB weitergeleitet.
- **weiterleiten**
Alle Gruppentelegramme der jeweiligen Hauptgruppen werden unabhängig von der Filtertabelle nach KNX/EIB weitergeleitet.
- **filtern**
Hier wird anhand der Filtertabelle geprüft, ob das empfangene Gruppentelegramm nach KNX/EIB weitergeleitet wird. Die Filtertabelle wird von der ETS automatisch erzeugt.

Wird die Weiterleitung für die Hauptgruppen 16-31 ausgewählt, so erscheint ein neues Untermenü in welchem paarweise die Weiterleitung gesperrt/freigegeben werden kann.

Konfiguration von Nebenlinie:

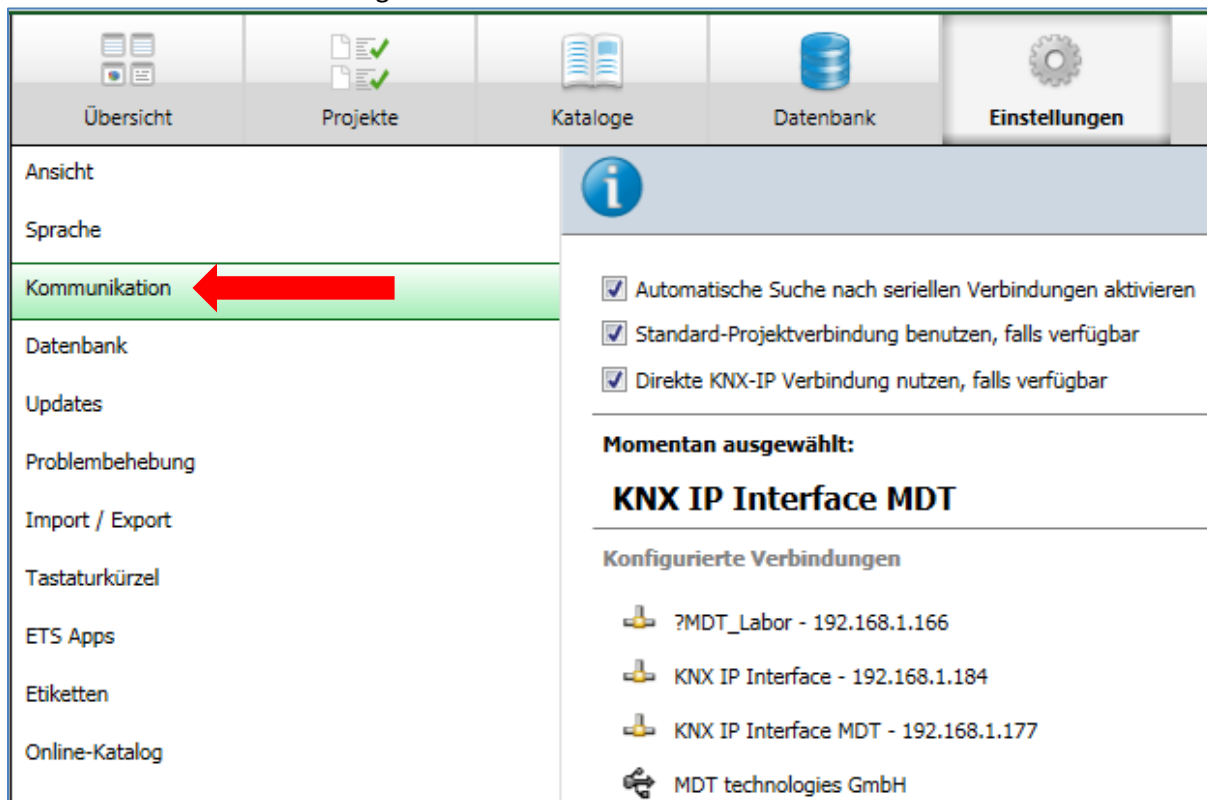
Durch diesen Parameter lässt sich das Programmieren von der TP/KNX-Seite aus unterdrücken, wodurch ein höheres Maß an Sicherheit erreicht werden kann.

4.6 Kommunikationseinstellungen

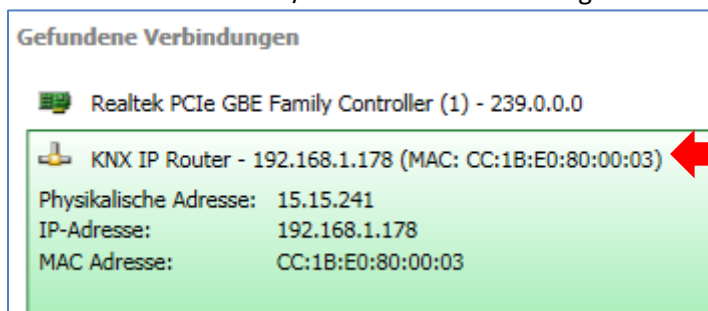
Wenn die IP-Konfiguration vom KNX Router gültig ist, kann der Router als Schnittstelle zu KNX/EIB benutzt werden. Verbinden Sie dazu den IP-Router/das IP-Interface mit dem KNX Bus und dem Netzwerk.

4.6.1 Vorgehen ETS 4

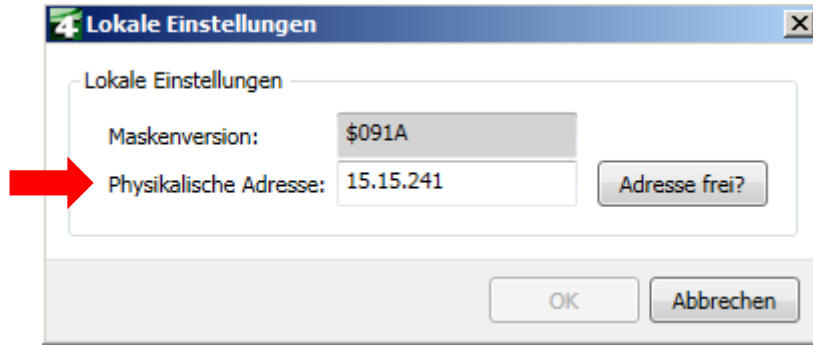
Wählen Sie im Menü Einstellungen den Reiter Kommunikation:



Hier sollte der IP-Router/das IP-Interface in den gefundenen Verbindungen aufgelistet sein:



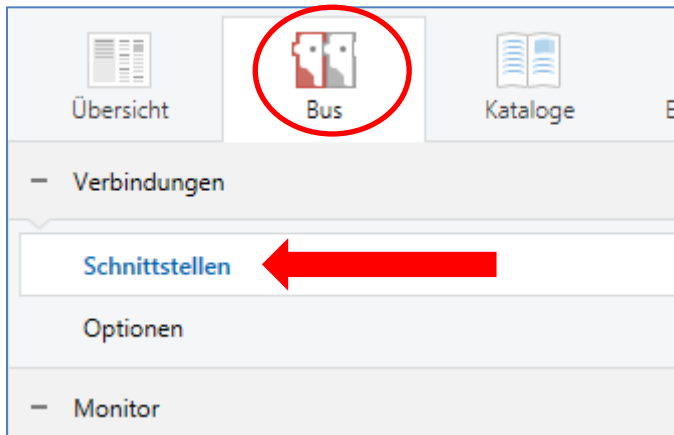
Die Verbindung kann nun durch einen Klick auf „Auswählen“ als aktiv gewählt werden. Nun können die Einstellungen für diese Schnittstelle durch selektieren und Anwahl des Buttons „Einstellungen“ aufgerufen werden:



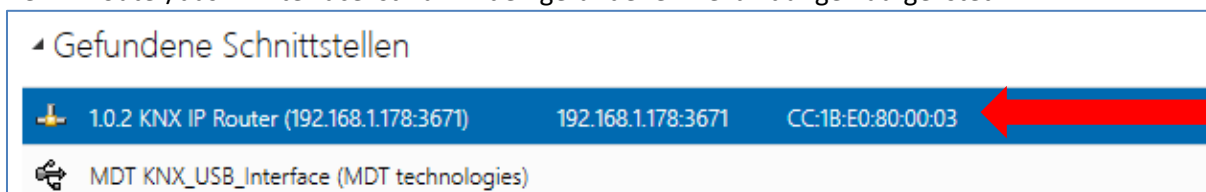
Hier kann nun die erste Tunneling Adresse vergeben werden.

4.6.2 Vorgehen ETS 5

Wählen Sie im Menü Bus den Reiter Schnittstellen:

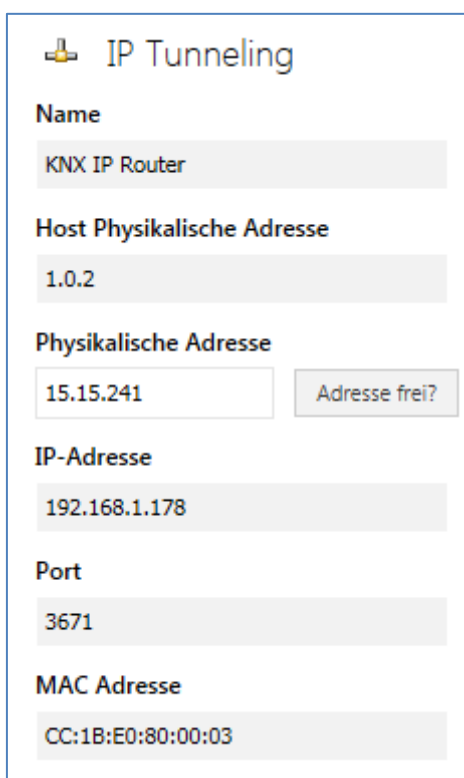


Der IP-Router/das IP-Interface ist nun in den gefundenen Verbindungen aufgelistet:



Nach dem der IP-Router/das IP-Interface selektiert wurde kann dieses durch einen Button auf der rechten Seite ausgewählt werden.

Für den ausgewählten IP-Router/IP-Interface kann anschließend die erste Tunneling Verbindung eingestellt werden:



4.6.3 Tunneling Verbindungen setzen

Der KNX IP Router/das KNX IP-Interface unterstützt bis zu 4 Verbindungen gleichzeitig. Die erste physikalische Adresse wird dabei in den ETS-Verbindungen eingestellt wie unter 4.6 beschrieben. Die weiteren physikalischen Adressen können im Web-Interface im Menü Prog.-Mode durch Drücken des Buttons „Set“ automatisch vergeben werden:


KNX IP-Router

Status Programming Mode: Off

Change Programming Mode:

Individual Address 1. 0. 2
15.15.241

Tunneling Addresses 15.15.242
15.15.243
15.15.244

Set Tunneling Addresses 

Routing Multicast Address 239.0.0.0

Serial Number 0104-262F000B

TP Device

Status Programming Mode: Off

Change Programming Mode:



Individual Address 15.15.254

Serial Number 0072-FFFF07B0

Dabei werden die 3 nachfolgenden physikalischen Adressen vergeben. Wurde zum Beispiel für den IP-Router als erste Tunneling Adresse die physikalische Adresse 15.15.241 vergeben, so stellt das Gerät die weiteren Tunneling Adressen automatisch zu 15.15.242, 15.15.243 und 15.15.244 ein. Wurde als erste Adresse die x.x.255 vergeben, so werden die weiteren Tunneling Adressen nicht automatisch zugewiesen!

Alternativ können die Adressen in der ETS 5 eingestellt werden:

5  1.1.5 IP Interface mit Secure

-  1.1.100 Tunneling Kanal 1
-  1.1.101 Tunnelling Kanal 2
-  1.1.102 Tunnelling Kanal 3
-  1.1.103 Tunnelling Kanal 4

Durch Auswahl des Tunneling Kanals kann der Name und die Adresse verändert werden.

5 Parameter -> E-Mail Client

5.1 Allgemeine Einstellungen

5.1.1 Allgemein

Das nachfolgende Bild zeigt die allgemeinen Einstellungen:

Geräteanlaufzeit	10
In Betrieb Telegramm	10 min
Sprache für Email Inhalt	<input checked="" type="radio"/> Deutsch <input type="radio"/> Englisch
Gerätename	MDT IP Interface mit IPRouting

Abbildung 15: Allgemeine Einstellungen

Geräteanlaufzeit

Die Geräteanlaufzeit bestimmt die Zeit zwischen einer Busspannungswiederkehr und einem funktionellen Anlauf des Gerätes.

In-Betrieb Telegramm

Mit Hilfe des zyklischen In-Betrieb Telegramms kann eine Ausfallerkennung für dieses Produkt realisiert werden.

Sprache für E-Mail Inhalt

Festlegen der Sprache des E-Mail Inhalts. Wird für fest vorgegebene Info Texte innerhalb der E-Mail verwendet.

Gerätename

Der Gerätename wird im Betreff der E-Mail angezeigt und kann über Makros in die E-Mail integriert werden. Es empfiehlt sich hier einen aussagekräftigen Namen des Objektes, in welchem der IP-Router eingesetzt ist, zu vergeben.

5.1.2 Web-Interface

Folgende Einstellungen sind für die Einrichtung des Web-Interfaces verfügbar:

Passwort	<input type="text" value="admin"/>
Zeitüberschreitung für gültige Login	<input type="text" value="keine zeitliche Begrenzung"/>
Zeit bis Deaktivierung des Webinterfaces nach Reset	<input type="text" value="keine zeitliche Deaktivierung"/>
Temporäre Aktivierung des Webinterfaces nach Email-Event	<input type="text" value="30 min"/>
Aktivierung / Deaktivierung des Webinterfaces über Objekt	<input checked="" type="radio"/> nicht aktiv <input type="radio"/> aktiv

Abbildung 16: Einstellungen Web-Interface

Passwort

Das Passwort wird zur Zugriffskontrolle für das Web-Interface benutzt. Es sollte immer ein Passwort angegeben werden!

Erlaubte Zeichen: Alle Zeichen aus Codepage ISO 8859-1 exklusive Leerzeichen und " & ' € Š Ž ě Ć œ Ÿ

Zeitüberschreitung für gültige Login

Der Parameter gibt die Zeit an die das Web-Interface nach einem Login erreichbar ist. Nach Ablauf der eingestellten Zeit wird das Web-Interface automatisch gesperrt.

Zeit bis Deaktivierung des Webinterfaces nach Reset

Der Parameter gibt die Zeit an die das Web-Interface nach einem Neustart (Zuschalten der Busspannung oder Reset über ETS) erreichbar ist. Nach Ablauf der eingestellten Zeit ist das Web-Interface nicht mehr erreichbar und kann auch erst wieder nach einem Neustart oder nach einer Aktivierung des Webinterfaces über Objekt erreicht werden.

Temporäre Aktivierung des Webinterfaces nach Email-Event

Der Parameter ermöglicht die zeitliche Aktivierung des Webinterfaces nach dem Aussenden einer E-Mail.

Aktivierung/Deaktivierung des Webinterfaces über Objekt

Um das via Bus, unabhängig von sonstigen Einstellungen, aktivieren zu können, kann ein Kommunikationsobjekt eingeblendet werden um das Web-Interface via Objekt aktivieren zu können. Folgendes Kommunikationsobjekt wird hierzu eingeblendet:

Nummer	Name	Größe	Verwendung
55	Webinterface	1 Bit	Sperren und freigeben des Web-Interfaces

Tabelle 5: Kommunikationsobjekt- Sperren/freigeben Web-Interface

Achtung: Es wird empfohlen das Web-Interface aus Sicherheitsgründen nach einer gewissen Zeit über den Parameter „Zeit bis Deaktivierung des Webinterfaces nach Reset“ zu deaktivieren oder das Web-Interface nur über Objekt zu aktivieren und bei Nichtbenutzung zu deaktivieren!

5.1.3 Uhrzeit/Datum

Folgende Einstellungen sind für die Uhrzeit und das Datum verfügbar:

Systemzeit zyklisch senden jede	10 min
Sommer/Winterzeit Zeitemstellung	<input type="radio"/> nicht aktiv <input checked="" type="radio"/> aktiv
Zeitdifferenz zur Weltzeit (UTC + ...)	(UTC +01:00) Amsterdam, Berlin, Bern, Rom, Wien

Abbildung 17: Einstellungen Zeit/Datum

Systemzeit zyklisch senden jede...

Einstellung ob die Systemzeit zyklisch gesendet werden soll.

Sommer/Winterzeit Zeitemstellung

Einstellung ob die Zeit automatisch zwischen Sommer- und Winterzeit umgestellt wird.

Zeitdifferenz zur Weltzeit (UTC+...)

Einstellung der Zeitzone.

Folgende Kommunikationsobjekte werden eingeblendet:

Nummer	Name	Größe	Verwendung
2	Uhrzeit	3 Byte	Senden der Uhrzeit
3	Datum	3 Byte	Senden des Datums
4	Datum / Uhrzeit	8 Byte	Senden von Datum und Uhrzeit

Tabelle 6: Kommunikationsobjekte- Uhrzeit/Datum

5.2 E-Mail Funktionen

Das IP-Interface unterstützt umfangreiche E-Mail Funktionalität. So stehen bis zu 30 Status-elemente zur Verfügung, wessen Namen und Werte in den E-Mails angezeigt werden können. Die E-Mails können über Bit-Telegramme (Bit-Alarme) ausgelöst werden oder über das Senden von Text-Strings (Text Alarme).

Des Weiteren können bis zu 3 Status Berichte gesendet werden, in welchen die 30 Status-elemente angezeigt werden können. Diese Status-Berichte können sowohl über Objekte als auch zu festen Zeitpunkten ausgesendet werden.

Die Konfiguration der E-Mail Funktionalität, wie sendende E-Mail Adresse, E-Mail Empfänger, etc., wird im Web-Interface vorgenommen, siehe 5.4 Sichere Gruppenadressenkommunikation

Soll eine Gruppenadresse verschlüsselt übertragen werden, so müssen alle Geräte dessen Kommunikationsobjekte mit dieser Gruppenadresse kommunizieren Data Secure unterstützen. Das IP Interface/IP Router unterstützt bis zu 255 sichere Gruppenadressen mit maximal 64 verschiedenen Secure Geräten.

Wenn 2 Kommunikationsobjekte, welche beide Data Secure unterstützen, mit einer Gruppenadresse verbunden werden, so setzt die ETS diese Gruppenadresse automatisch auf „Sicherheit aktiv“. Dies wird durch ein blaues Schutzschild im Reiter Sicherheit angezeigt:





	Sicherheit	Objekt	Gerät ▾
		1: In Betrieb - Status senden	1.1.82 Email App. für IP Interface mit Secure
		1: In Betrieb - Status senden	1.1.15 Email App. für IP Router mit Secure

Abbildung 22: Gesicherte Gruppenadresse

Über den Reiter Sicherheit in den Einstellungen der Gruppenadressen kann die Sicherheit für diese Gruppenadresse explizit ausgeschaltet oder eingeschaltet werden. Die Einstellung „automatisch“ ist die Standardeinstellung. Auf diese Weise entscheidet die ETS selbstständig ob die Gruppenadresse sicher übertragen werden kann und aktiviert dies wenn möglich:

Sicherheit

Automatisch ▾

Abbildung 23: Ändern der Sicherheitseinstellungen für die Gruppenadresse

6 Web-Interface.

5.2.1 Status Elemente

Für das Status Element 1 stehen folgende Einstellungen zur Verfügung:

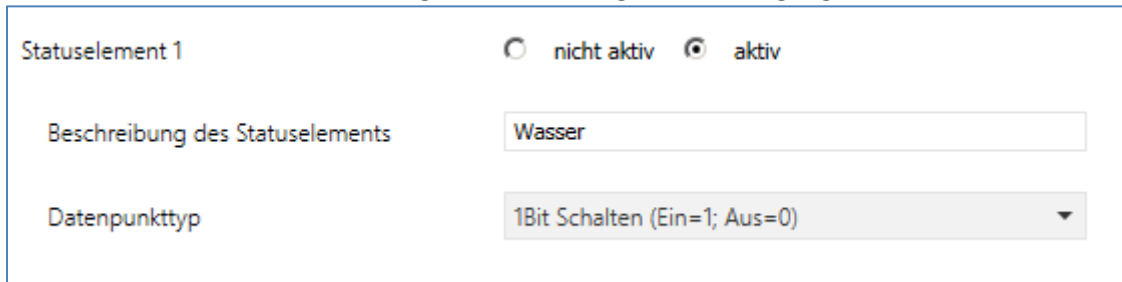


Abbildung 18: Einstellungen Status Element 1

Jedem Status Element kann ein Anzeige-Name und ein Datenpunkttyp zugewiesen werden. Der Anzeige-Name kann anschließend in den E-Mails dargestellt werden.

Folgende Datenpunkttypen mit den dazugehörigen Werten können eingestellt werden:

Größe: 1 Bit

Datenpunkttyp	Wert für 1	Wert für 0
1 Bit Schalten	Ein	Aus
1 Bit Sperren	gesperrt	nicht gesperrt
1 Bit Oben/Unten	Unten	Oben
1 Bit Offen/Geschlossen	Geschlossen	Offen
1 Bit Heizen/Kühlen	Heizen	Kühlen
1 Bit Ja/Nein	Ja	Nein
1 Bit Anwesend/Abwesend	Anwesend	Abwesend
1 Bit Tag	Tag	Nacht
1 Bit Nacht	Nacht	Tag

Tabelle 7: Status Elemente - 1 Bit

Größe 1 Byte

Datenpunkttyp	Wertebereich
1 Byte Wert	0-255
1 Byte Prozentwert	0-100%
1 Byte HVAC Status	0x01 -> Komfort 0x02 -> Standby 0x03 -> Nacht 0x04 -> Frost-/Hitzeschutz
1 Byte HVAC Modus	Der HVAC-Mode wird bitweise ausgewertet und angezeigt: Bit 0 -> 1= Komfort Bit 1 -> 1 = Standby Bit 2 -> 1 = Nacht Bit 3 -> 1 = Frost-/Hitzeschutz Bit 5 -> 0 = Kühlen/ 1= Heizen Bit 7 -> 1 = Frostalarm

Tabelle 8: Status Elemente - 1 Byte

Größe 2 Byte

Datenpunkttyp	Wertebereich
2 Byte Wert vorzeichenlos	0 – 65535
2 Byte Wert vorzeichenbehaftet	-32768 – 32767
2 Byte Gleitkommawert	-670760 - 670760

Tabelle 9: Status Elemente - 2 Byte

Größe 4 Byte

Datenpunkttyp	Wertebereich
4 Byte Wert vorzeichenlos	0 – 4 294 967 295
4 Byte Wert vorzeichenbehaftet	-2 147 483 648 – 2 147 483 647
4 Byte Gleitkommawert	Gleitkomma gemäß IEEE 754

Tabelle 10: Status Elemente - 2 Byte

Größe 14 Byte Zeichen

Datenpunkttyp	Wertebereich
14 Byte Zeichen (ISO 8859-1)	beliebiger String mit max. 14 Zeichen

Tabelle 11: Status Elemente - 14 Byte

Die nachfolgende Tabelle zeigt die verfügbaren Kommunikationsobjekte:

Nummer	Name	Größe	Verwendung
21	Status Element 1	1 Bit 1 Byte 2 Byte 4 Byte 14 Byte	Setzen des Wertes für das Status Element
+1	nächstes Status Element		

Tabelle 12: Kommunikationsobjekte- Status Elemente

5.2.2 Bit Alarme

Das nachfolgende Bild zeigt die verfügbaren Einstellungen für den ersten Bit-Alarm:

Bit Alarm 1 nicht aktiv aktiv

Text für Email

Sendeverhalten senden bei Ein ▼

Email an Empfänger Adresse 1 senden nein ja

Email an Empfänger Adresse 2 senden nein ja

Email an Empfänger Adresse 3 senden nein ja

Abbildung 19: Einstellungen Bit-Alarm 1

Die nachfolgende Tabelle zeigt die verfügbaren Einstellungen für einen aktivierten Bit-Alarm:

ETS-Text	Wertebereich [Defaultwert]	Kommentar
Text für E-Mail	beliebiger Text, alternativ Verwendung von Makros (siehe Makros)	Einstellung des Textes der in der E-Mail angezeigt werden soll
Sendeverhalten	<ul style="list-style-type: none"> ▪ senden bei Ein ▪ senden bei Aus ▪ senden bei Änderung auf Aus oder Ein ▪ senden bei Änderung auf Ein ▪ senden bei Änderung auf Aus 	Einstellung wann die E-Mail ausgesendet werden soll
E-Mail an Empfänger Adresse 1 senden	<ul style="list-style-type: none"> ▪ ja ▪ nein 	Einstellung ob an Empfänger 1 gesendet werden soll
E-Mail an Empfänger Adresse 2 senden	<ul style="list-style-type: none"> ▪ ja ▪ nein 	Einstellung ob an Empfänger 2 gesendet werden soll
E-Mail an Empfänger Adresse 3 senden	<ul style="list-style-type: none"> ▪ ja ▪ nein 	Einstellung ob an Empfänger 3 gesendet werden soll

Tabelle 13: Einstellmöglichkeiten - Bit Alarme

Die nachfolgende Tabelle zeigt die verfügbaren Kommunikationsobjekte:

Nummer	Name	Größe	Verwendung
11	Bit Alarm 1	1 Bit	Auslösen des ersten Bit Alarms
+1	nächster Bit Alarm		

Tabelle 14: Kommunikationsobjekte- Bit Alarm

Makros

Um in E-Mails auch Werte anzeigen zu können, können Makros verwendet werden. Folgende Makros sind verfügbar:

- `D` -> Wird dieses Makro in den Text eingesetzt, so ersetzt das IP-Interface dieses durch den Gerätenamen.
- `T` -> Wird dieses Makro in den Text eingesetzt, so ersetzt das IP-Interface dieses durch das Datum und die Uhrzeit zu dem das E-Mail Event ausgelöst wurde.
- `Nxx` -> Wird dieses Makro in den Text eingesetzt, so ersetzt das IP-Interface dieses durch den Namen des Statuslements „xx“. Soll z.B. der Name des Statuslements 11 angezeigt werden, so muss `$N11$` eingegeben werden. Für das Statuslement 1 reicht `$N1$`.
- `Vxx` -> Wird dieses Makro in den Text eingesetzt, so ersetzt das IP-Interface dieses durch den Wert des Statuslements „xx“. Soll z.B. der Wert des Statuslements 11 angezeigt werden, so muss `$V11$` eingegeben werden. Für das Statuslement 1 reicht `$V1$`.
- Ein Semikolon erzeugt einen Zeilenumbruch, bzw. schreibt den ersten Teil vor dem Semikolon in den Betreff der E-Mail.

Beispiele:

Für nachfolgende Beispiele wurde der Gerätename MDT vergeben. Das Statuslement 1 hat den Namen „Licht Küche“ und den Datenpunkttyp 1 Bit Schalten.

- 1) Text für E-Mail: `D T $N1$ $V1$`

Es wird eine E-Mail mit dem Betreff Bit Alarm: MDT gesendet. Im Text der E-Mail steht:
MDT Datum-Uhrzeit Licht Küche Aus

Da nichts mit Semikolon abgetrennt wird, wird der gesamte Text in das Textfeld der E-Mail gesetzt und für den Betreff der Standard-Betreff verwendet. Die Makros im Textfeld werden durch das IP-Interface ersetzt und aneinander gereiht.

- 2) Text für E-Mail: `D; T; $N1$: $V1$`

Es wird eine E-Mail mit dem Betreff MDT gesendet. Im Text der E-Mail steht:
Datum –Uhrzeit

Licht Küche: Aus (je nach aktuellem Wert)

Die Semikolons trennen den Name des Gerätes als Betreff und den Text der E-Mail ab. Nach dem Datum wird ein weiterer Zeilenumbruch erzeugt.

5.2.3 Text Alarme

Das nachfolgende Bild zeigt die verfügbaren Einstellungen für den ersten Text-Alarm:

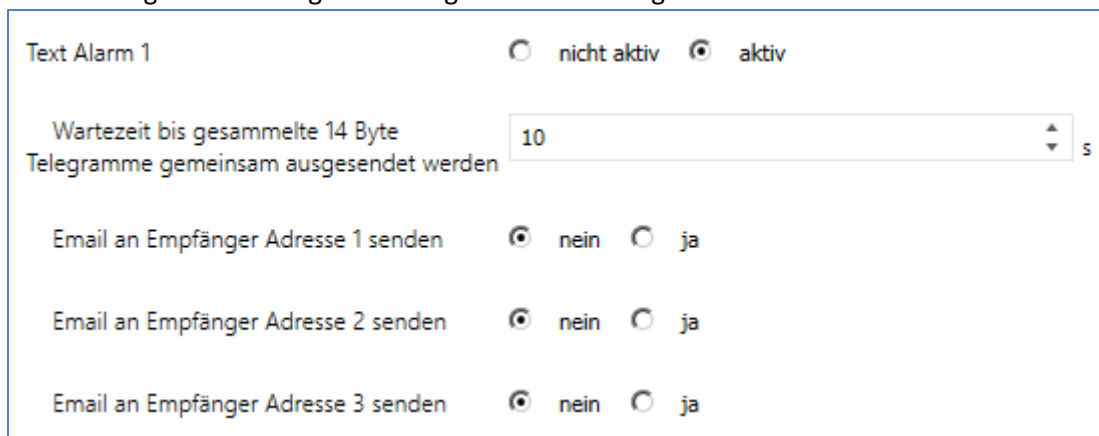


Abbildung 20: Einstellungen Text-Alarm 1

Die nachfolgende Tabelle zeigt die verfügbaren Einstellungen für einen aktivierten Text-Alarm:

ETS-Text	Wertebereich [Defaultwert]	Kommentar
Wartezeit bis gesammelte 14 Byte Telegramme gemeinsam ausgesendet werden	1-120s [10s]	Einstellung des Zeitfensters in denen Textnachrichten zu einer E-Mail zusammengefasst werden.
E-Mail an Empfänger Adresse 1 senden	<ul style="list-style-type: none"> ▪ ja ▪ nein 	Einstellung ob an Empfänger 1 gesendet werden soll
E-Mail an Empfänger Adresse 2 senden	<ul style="list-style-type: none"> ▪ ja ▪ nein 	Einstellung ob an Empfänger 2 gesendet werden soll
E-Mail an Empfänger Adresse 3 senden	<ul style="list-style-type: none"> ▪ ja ▪ nein 	Einstellung ob an Empfänger 3 gesendet werden soll

Tabelle 15: Einstellmöglichkeiten - Text Alarme

Ein Text-Alarm wird ausgelöst sobald ein Wert auf das dazugehörige Kommunikationsobjekt geschrieben wird. Um jedoch auch längere Texte als 14 Zeichen senden zu können wartet das IP-Interface nach dem Senden eines Wertes auf das dazugehörige Kommunikationsobjekt die eingestellte Wartezeit ab. Wird nun innerhalb der eingestellten Wartezeit ein weiterer String an das Kommunikationsobjekt gesendet, so werden in der E-Mail die aneinandergereihten Strings gesendet.

Die nachfolgende Tabelle zeigt die verfügbaren Kommunikationsobjekte:

Nummer	Name	Größe	Verwendung
8	Text Alarm 1	1 Bit	Setzen des Wertes für den Text Alarm
+1	nächster Text Alarm		

Tabelle 16: Kommunikationsobjekte- Text Alarme

5.2.4 Status Berichte

Das nachfolgende Bild zeigt die verfügbaren Einstellungen für den ersten Statusbericht:

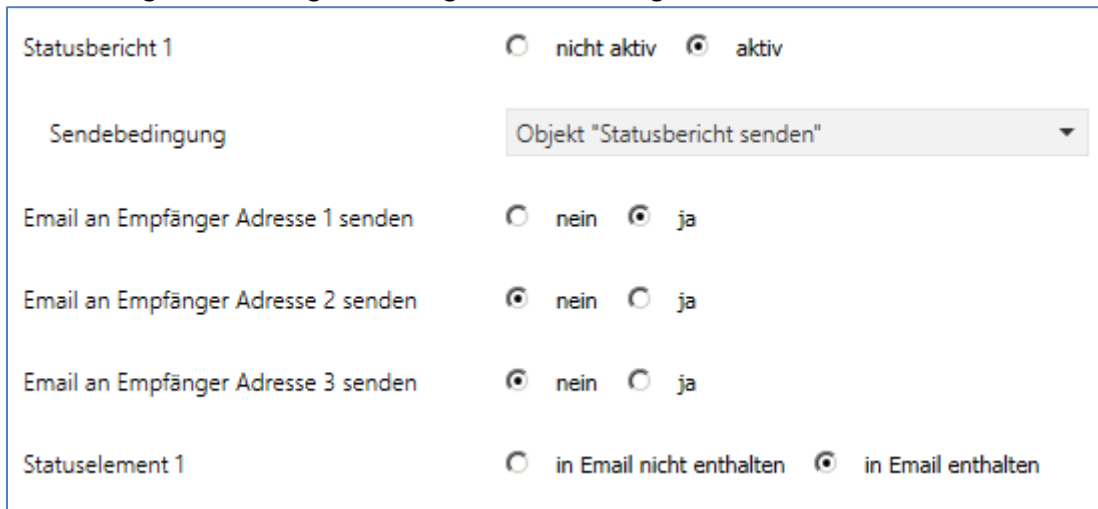


Abbildung 21: Einstellungen Statusbericht 1

Die nachfolgende Tabelle zeigt die verfügbaren Einstellungen für einen aktivierten Statusbericht:

ETS-Text	Wertebereich [Defaultwert]	Kommentar
Sendebedingung	<ul style="list-style-type: none"> ▪ fester Tag in der Woche ▪ festes Datum im Monat ▪ Objekt „Statusbericht senden“ 	Einstellung wann der Statusbericht gesendet werden soll.
E-Mail an Empfänger Adresse 1 senden	<ul style="list-style-type: none"> ▪ ja ▪ nein 	Einstellung ob an Empfänger 1 gesendet werden soll
E-Mail an Empfänger Adresse 2 senden	<ul style="list-style-type: none"> ▪ ja ▪ nein 	Einstellung ob an Empfänger 2 gesendet werden soll
E-Mail an Empfänger Adresse 3 senden	<ul style="list-style-type: none"> ▪ ja ▪ nein 	Einstellung ob an Empfänger 3 gesendet werden soll
Statusselement 1-30	<ul style="list-style-type: none"> ▪ in E-Mail nicht enthalten ▪ in E-Mail enthalten 	Einstellung ob das Statusselement in der E-Mail angezeigt werden soll

Tabelle 17: Einstellmöglichkeiten - Statusberichte

Der Statusbericht kann sowohl zyklisch, einmal wöchentlich oder einmal im Monat, als auch über Objekt ausgesendet werden.

Jedes aktivierte Statusselement kann in den Statusbericht integriert werden. Die aktivierten Statusselement werden in dem Statusbericht wie folgt angezeigt:

Name des Statuselements: Wert des Statuselements

Die nachfolgende Tabelle zeigt die verfügbaren Kommunikationsobjekte:

Nummer	Name	Größe	Verwendung
8	Statusbericht 1	1 Bit	Aussenden des Statusberichts; wird nur angezeigt wenn die Sendebedingung auf Objekt steht
+1	nächster Statusbericht		

Tabelle 18: Kommunikationsobjekte- Statusbericht

5.2.5 spezielles Verhalten und Fehlerbehandlung

Bei der E-Mail Funktionalität sind folgende Punkte zu beachten:

- Zwischen zwei Emails wird bei einer fehlerfreien Abarbeitung aus technischen Gründen eine Pause von 5 Sekunden vorgesehen.
- E-Mails werden nur mit aktueller Uhrzeit ausgesendet. Daher wird geprüft ob jemals eine Uhrzeit über NTP empfangen wurde. Wenn nicht werden die Emails nach 5 Minuten mit dem Startdatum 00:00 01.01.1970 ausgesendet.

Fehlercode-Objekt:

Das Fehlercode-Objekt wird gesetzt und ausgesendet, wenn...

- die E-Mail 4mal versucht wurde zu übertragen und dies jedes Mal fehlschlug und der vorherige Email-Versand ohne Fehler war oder es die erste Email nach einem Neustart ist. Zwischen den Versuchen werden die nachfolgenden Verzögerungen eingehalten:
 - Verzögerung vor der ersten Wiederholung: 10 Sekunden
 - Verzögerung vor der zweiten Wiederholung: 1 Minute
 - Verzögerung vor der dritten Wiederholung: 10 Minuten
- die E-Mail 1mal versucht wurde zu übertragen und dies fehl schlug und der vorherige E-Mail Versand ebenfalls fehlerhaft war.

Die nachfolgende Tabelle zeigt das dazugehörige Kommunikationsobjekt:

Nummer	Name	Größe	Verwendung
52	E-Mail – Fehlercode	1 Bit	Aussenden eines Fehlers

Tabelle 19: Kommunikationsobjekt E-Mail Fehlercode

E-Mail Puffer:

Es können 10Emails gepuffert werden.

- Ab der 8. Email im Puffer wird ein Alarm auf den Bus gesendet.
- Ist der Puffer voll, werden weitere Email-Requests verworfen
- Alle Werte die in Bit-Alarm-Emails bzw. Status-Emails abgebildet werden, können nur den Wert ausgeben der zum Zeitpunkt des Versands herrscht.

Beispiel:

- T=0: Statuselement 3 = Aus
- T=10: Statuselement 3 = An
- Wenn zum Zeitpunkt t=0 der Emailversand ausgelöst wird (z.B. über Objekt), die E-Mail jedoch erst zum Zeitpunkt t = 10s ausgesendet wird, wird der Wert „An“ in der Email eingefügt.

Die nachfolgende Tabelle zeigt das dazugehörige Kommunikationsobjekt:

Nummer	Name	Größe	Verwendung
52	E-Mail Pufferspeicher – Überlauf	1 Bit	Zeigt einen Überlauf des E-Mail Puffers an

Tabelle 20: Kommunikationsobjekt E-Mail Pufferspeicher

5.3 Übersicht Kommunikationsobjekte

Nr.	Name	Objektfunktion	Datentyp	Richtung	Info	Verwendung	Hinweis
allgemeine Objekte:							
1	In-Betrieb	Status senden	DPT 1.011	senden	Gerät sendet zyklisches In-Betrieb Telegramm	Diagnose	Kommunikationsobjekt wird eingeblendet sobald das „zyklische In-Betrieb Telegramm“ aktiviert wurde.
2	Uhrzeit	Aktuelle Zeit senden	DPT 10.001	senden	Gerät sendet Uhrzeit	Uhrzeit Synchronisierung	Kommunikationsobjekt ist dauerhaft eingeblendet.
3	Datum	Aktuelles Datum senden	DPT 11.001	senden	Gerät sendet Datum	Uhrzeit Synchronisierung	Kommunikationsobjekt ist dauerhaft eingeblendet.
4	Datum/Uhrzeit	Aktuelles Datum und Zeit senden	DPT 19.001	senden	Gerät sendet Datum und Uhrzeit	Uhrzeit Synchronisierung	Kommunikationsobjekt ist dauerhaft eingeblendet.
51	E-Mail Pufferspeicher	Überlauf	DPT 1.005	senden	Gerät meldet Fehler	Diagnose	Kommunikationsobjekt ist dauerhaft eingeblendet und zeigt einen E-Mail Überlauf an.
52	E-Mail	Fehlercode	DPT 1.005	senden	Gerät meldet Fehler	Diagnose	Kommunikationsobjekt ist dauerhaft eingeblendet und zeigt einen E-Mail Sendefehler an.
53	NTP Zeitserver	Fehler	DPT 1.005	senden	Gerät meldet Fehler	Diagnose	Kommunikationsobjekt ist dauerhaft eingeblendet und zeigt einen an, dass keine Uhrzeit vom NTP-Server empfangen werden konnte.
54	Webinterface	Sperrstatus	DPT 1.003	senden	Gerät sendet Status	Diagnose, Visualisierung	Kommunikationsobjekt ist dauerhaft eingeblendet und zeigt an ob das Web-Interface zugänglich ist.

55	Webinterface	Sperren	DPT 1.003	empfangen	Gerät empfängt Eingangs-Telegramm	Diagnose, Inbetriebnahme	Kommunikationsobjekt muss in den Parametern aktiviert werden; gibt das Web-Interface frei.
E-Mail Funktionen:							
5	Statusbericht 1	E-Mail senden	DPT 1.010	empfangen	Gerät empfängt Eingangs-Telegramm	Auslösen des Statusberichts	Kommunikationsobjekt wird eingeblendet sobald der Statusbericht aktiv ist und die Sendebedingung auf Objekt steht
+1	nächster Statusbericht						
8	Text Alarm 1	E-Mail senden	DPT 16.001	empfangen	Gerät empfängt Eingangs-Telegramm	Auslösen des Text-Alarms	Kommunikationsobjekt wird eingeblendet sobald der Text-Alarm aktiv ist
+1	nächster Text Alarm						
11	Bit Alarm 1	E-Mail senden	DPT 1.005	empfangen	Gerät empfängt Eingangs-Telegramm	Auslösen des Bit-Alarms	Kommunikationsobjekt wird eingeblendet sobald der Bit-Alarm aktiv ist
+1	nächster Bit Alarm						
21	Statuselement 1	gemäß Parameter	DPT xxx	empfangen	Gerät empfängt Status	Status anderer Geräte im KNX-Bus	Kommunikationsobjekt wird eingeblendet sobald das Statuselement aktiv ist; DPT wird gemäß der Parametereinstellung eingestellt
+1	nächstes Statuselement						

Tabelle 21: Übersicht Kommunikationsobjekte

5.4 Sichere Gruppenadressenkommunikation

Soll eine Gruppenadresse verschlüsselt übertragen werden, so müssen alle Geräte dessen Kommunikationsobjekte mit dieser Gruppenadresse kommunizieren Data Secure unterstützen. Das IP Interface/IP Router unterstützt bis zu 255 sichere Gruppenadressen mit maximal 64 verschiedenen Secure Geräten.

Wenn 2 Kommunikationsobjekte, welche beide Data Secure unterstützen, mit einer Gruppenadresse verbunden werden, so setzt die ETS diese Gruppenadresse automatisch auf „Sicherheit aktiv“. Dies wird durch ein blaues Schutzschild im Reiter Sicherheit angezeigt:





	Sicherheit	Objekt	Gerät ▾
		1: In Betrieb - Status senden	1.1.82 Email App. für IP Interface mit Secure
		1: In Betrieb - Status senden	1.1.15 Email App. für IP Router mit Secure

Abbildung 22: Gesicherte Gruppenadresse

Über den Reiter Sicherheit in den Einstellungen der Gruppenadressen kann die Sicherheit für diese Gruppenadresse explizit ausgeschaltet oder eingeschaltet werden. Die Einstellung „automatisch“ ist die Standardeinstellung. Auf diese Weise entscheidet die ETS selbstständig ob die Gruppenadresse sicher übertragen werden kann und aktiviert dies wenn möglich:

Sicherheit

Automatisch ▾

Abbildung 23: Ändern der Sicherheitseinstellungen für die Gruppenadresse

6 Web-Interface

6.1 Aufruf des Web-Interface

Das Web-Interface kann auf 2 arten aufgerufen werden:

1.) Über den Browse:

Dazu öffnen Sie Ihren Standard-Browser und geben in die Adresszeile folgendes ein:

http:\\ip-adresse:Port

Beispiel: Folgende Einstellungen wurden für den IP-Router vorgenommen:

DHCP	<input checked="" type="radio"/> nicht benutzen <input type="radio"/> benutzen
IP Adresse	<input type="text" value="192.168.1.178"/>
Netzmaske	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.3"/>
dns	<input type="text" value="192.168.1.3"/>
HTTP Port	<input type="radio"/> 80 <input checked="" type="radio"/> 8080

Abbildung 24: Beispiel IP-Konfiguration

Dann geben Sie in die Adresszeile <http://192.168.1.178:8080> ein.

- 2.) Gehen Sie in den Windows Explorer und öffnen Sie den Reiter Netzwerk. Hier sollte Ihr IP-Router mit den angegebenen Host-Name auftauchen. Durch einen Doppelklick auf den Router wird Ihr Standard-Browser mit der richtigen Adresse aufgerufen.

6.2 Übersicht Web-Interface

Nach Aufruf des Web-Interface erscheint das Login-Fenster:

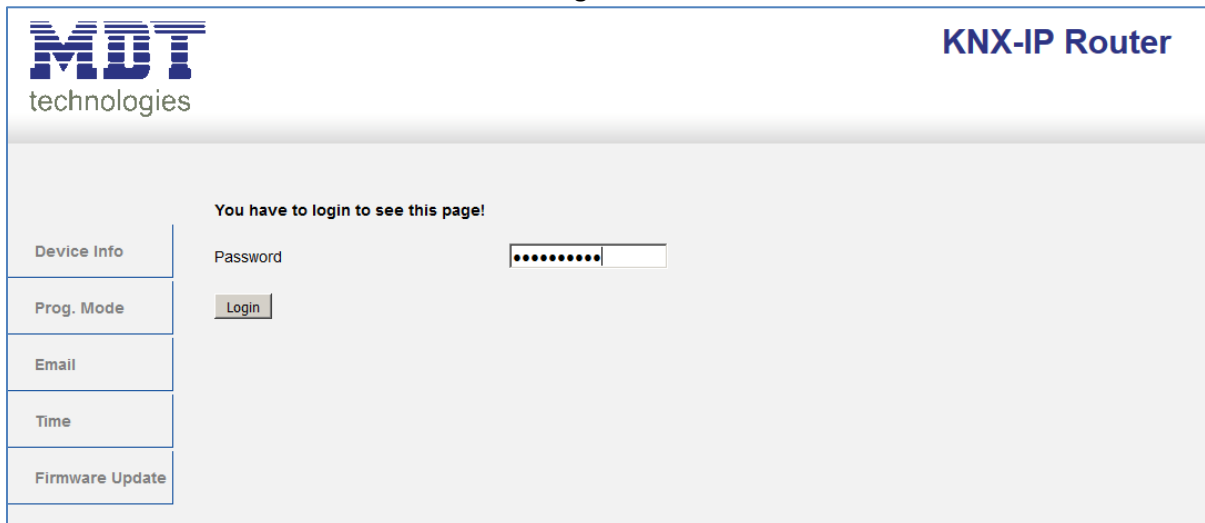


Abbildung 25: Login-Fenster

Nach erfolgreichem Login können die Menüs auf der linken Seite angewählt werden. Die Menüs haben die folgende Funktionalität:

- **Device Info**
Im Menü Device Info stehen Infos und Einstellungen des IP-Interfaces, wie MAC-Adresse, IP-Adresse, Netzwerkeinstellungen, Software-Stand, etc.
- **Prog. Mode**
Im Menü Prog. Mode können die Programmier-LEDs für die TP- und die IP-Seite an- und ausgeschaltet werden. Des Weiteren können die vergebenen physikalischen Adressen, die Tunneling Adressen und die Seriennummer eingesehen werden.
- **Email**
Hier wird die E-Mail Funktionalität eingestellt, siehe hierzu 6.3 Einstellen der E-Mail Funktionalität.
- **Time**
Hier können Infos bzgl. des Zeitserver eingesehen werden.
- **Firmware Update**
Es ist möglich ein Update für den IP-Router zu fahren. Wenden Sie sich diesbezüglich an den MDT Support ob ein Update für Ihr Gerät sinnvoll ist. Der MDT Support teilt Ihnen die erforderlichen Schritte mit.

6.3 Einstellen der E-Mail Funktionalität

Um die E-Mail Funktionalität einzurichten, öffnen Sie das Menü E-Mail und klicken Sie auf „Settings“:

Destination E-Mail Test:


E-Mail Address 1: knx@mdt.de

E-Mail Address 2:

E-Mail Address 3:

Status: no error

Server Response:

[Settings](#) 

Anschließend öffnet sich das folgende Menü:

Email settings

Outgoing (SMTP) settings:

SMTP server address

SMTP server port

E-Mail Address

Username

Password

Destination E-Mail Address:

E-Mail Address 1

E-Mail Address 2

E-Mail Address 3

Hier können nun die E-Mail Adresse von der gesendet wird und die Zieladressen (bis zu 3) eingestellt werden.

Für die sendende E-Mail Adresse sind folgende Einstellungen vorzunehmen:

- **SMTP server address**
Hier muss der Postausgangsserver angegeben werden.
- **SMTP server port**
Hier wird der Port für den Postausgang angegeben.
- **E-Mail Address**
Angabe der sendenden E-Mail Adresse.
- **Username**
Hier wird der Name eingegeben mit dem Sie sich an Ihrer E-Mail Adresse anmelden. Dies kann je nach Anbieter variieren und z.B. die komplette E-Mail Adresse, ein User-Name oder eine ID sein.
- **Password**
Angabe des Passwort mit dem Sie sich an Ihrer E-Mail Adresse anmelden.


Sucht man bei z.B. bei web.de nach Serverdaten, so sind folgende Daten angegeben:

Serverdaten

POP3 steht für die englische Abkürzung "Post Office Protocol Version 3". Per POP3 werden E-Mails von einem Server in ein E-Mail-Programm übertragen und gleichzeitig vom jeweiligen Server gelöscht.

Posteingang:
 Server: **pop3.web.de**
 Port: **995**
 Verschlüsselung: **SSL-Verschlüsselung**
 (Steht in einem Programm "SSL" nicht zur Verfügung, genügt es, die Option "Verschlüsselung" zu aktivieren.)

Postausgang:
 Server: **smtp.web.de**
 Port: **587**
 Verschlüsselung: **STARTTLS**
 (Steht in einem Programm "STARTTLS" nicht zur Verfügung, nutzen Sie bitte das Protokoll "TLS". Existiert auch hierfür keine Option, genügt es, die Option "Verschlüsselung" zu aktivieren.)

 Welche Ordner werden per POP3 abgerufen?

Damit kann im Feld smtp server address der Wert smtp.web.de eingetragen werden und im Feld smtp server port der Wert 587.


Bei dem Anbieter web.de ist es des Weiteren erforderlich, dass der Versand von E-Mails über externe Programme in den Einstellungen freigeschaltet wird:

WEB.DE Mail über POP3 & IMAP

Wenn Sie Ihre E-Mails mit Outlook oder einem anderen E-Mail-Programm abrufen möchten, müssen Sie dazu POP3 und IMAP aktivieren. Bitte verwenden Sie die angezeigten Zugangsdaten.

E-Mails per externem Programm (Outlook, Thunderbird) versenden und empfangen

Für die wichtigsten E-Mail-Programme bieten wir Ihnen Schritt-für-Schritt-Anleitungen an.

 POP3

Serverdaten für den POP3 Abruf:

POP3-Server	pop3.web.de
SMTP-Server	smtp.web.de

Neben dem oben beschriebenen Anbieter, **web.de**, sind folgende Anbieter getestet und die Einstellungen nachfolgend aufgelistet:

gmx.de

SMTP server adress: mail.gmx.net
SMTP server port: 587

1&1

SMTP server adress: smtp.1und1.de
SMTP server port: 587

Telekom

SMTP server adress: smtpmail.t-online.de
SMTP server port: 465

HotMail, jetzt outlook.com/de

SMTP server adress: smtpmail.live.com
SMTP server port: 587

Strato

SMTP server adress: smtp.strato.de
SMTP server port: 587

Alle Daten der E-Mail Provider sind auf dem Stand des Handbuches, siehe Titelseite, und sind ohne Gewähr.

Als Destination Address tragen Sie dann alle E-Mail Adressen (max. 3) ein an die Sie eine E-Mail verschicken wollen.

Anschließend schließen Sie das Menü durch den Button OK.

Nun kann in folgendem Menü die E-Mail Konfiguration getestet werden:

Destination E-Mail Test:

E-Mail Address 1: dahl@mdt.de Test E-Mail Adresse 1

E-Mail Address 2:

E-Mail Address 3:

Status: no error Status

Server Response: 250 Requested mail action okay, completed: id=0LIWGZ-1aOQqt0hWR-00bJ7A

[Settings](#)

Nach erfolgreicher Konfiguration kann eine Test E-Mail an die eingestellten Ziel-Adressen ausgelöst werden.

Der Status wird anschließend angezeigt und ggf. ein Error angezeigt. Die Bedeutung der Error-Codes ist in 6.4 E-Mail – Error Codes & Behebung dargestellt.

6.4 E-Mail – Error Codes & Behebung

Der Status im Web-Interface gibt immer den Status der letzten E-Mail Versendung wieder. Falls ein Error auftritt, haben die Error-Codes die folgende Bedeutung:

- Error 0: No error (250 Requested mail action okay, completed: id=0LgK3g-1alfqB1ZsS-00nhnX)
 - letzte Email wurde ohne Probleme ausgesendet.
- Error 4: unable to connect to server
 - Falscher Port angegeben
 - Port überprüfen
- Error 6: invalid sending Email address
 - Sende-Emailadresse ist ungültig
 - Sende-Emailadresse wird vom Server nicht akzeptiert
 - Einstellungen für die E-Mail Adresse überprüfen
- Error 8: invalid receiving Email address
 - Ziel-Emailadresse ist ungültig
 - Ziel E-Mail Adresse überprüfen
- Error 9: Socket unexpectedly closed
 - Gerät neustarten und ggf. neu programmieren
- Error 12: Unknown/unsupported server authentication request (535 Authentication credentials invalid)
 - Ungültiger Benutzername oder Passwort
 - Benutzername und Passwort überprüfen

6.5 E-Mails als Push-Nachricht empfangen

E-Mails können als Push-Nachricht auf dem Handy empfangen werden. Dazu müssen bestimmte Dienste verwendet werden. So kann z.B. für Apple-Geräte der Dienst Prowl verwendet werden: <http://www.prowlapp.com/>.

Durch das Verwenden von Push-Nachrichten werden E-Mails sofort als „Notification“ auf dem Gerät angezeigt.

6.6 E-Mail als SMS empfangen

Um E-Mails in SMS umzuwandeln und diese zu versenden, bieten diverse Anbieter diesen Service in gewissen Paketen an, z.B. Telekom. Unterstützt Ihr E-Mail Provider keinen SMS-Service für E-Mails, so können Drittanbieter wie sms77 - <https://www.sms77.de/> - verwendet werden.

7 Index

7.1 Abbildungsverzeichnis

Abbildung 1: Aufbau Hardwaremodul	5
Abbildung 2: KNX IP Router als Linienkoppler.....	8
Abbildung 3: KNX IP Router als Bereichskoppler.....	9
Abbildung 4: KNX IP Router als Bereichs- und Linienkoppler.....	10
Abbildung 5: Beispiel für Installation	11
Abbildung 2: Inbetriebnahmepasswort.....	13
Abbildung 3: Sichere Inbetriebnahme/Secure Tunnel	14
Abbildung 4: Eingabe FDSK.....	15
Abbildung 5: Nachträgliche Eingabe FDSK	16
Abbildung 6: Allgemeine Einstellungen.....	18
Abbildung 7: Gerät -> Einstellungen.....	20
Abbildung 8: IP Einstellungen.....	21
Abbildung 8: Einstellungen Hauptlinie	23
Abbildung 9: Einstellungen Nebenlinie	25
Abbildung 9: Allgemeine Einstellungen.....	31
Abbildung 11: Einstellungen Web-Interface	32
Abbildung 12: Einstellungen Zeit/Datum	33
Abbildung 13: Einstellungen Statuselement 1	35
Abbildung 14: Einstellungen Bit-Alarm 1.....	37
Abbildung 15: Einstellungen Text-Alarm 1.....	39
Abbildung 16: Einstellungen Statusbericht 1	40
Abbildung 16: Gesicherte Gruppenadresse	44
Abbildung 17: Ändern der Sicherheitseinstellungen für die Gruppenadresse	44
Abbildung 17: Beispiel IP-Konfiguration	45
Abbildung 18: Login-Fenster	46

7.2 Tabellenverzeichnis

Tabelle 1: Übersicht LEDs	6
Tabelle 2: Parameter - Allgemein	19
Tabelle 5: Einstellungen Hauptlinie	23
Tabelle 6: Einstellungen Nebenlinie	26
Tabelle 7: Kommunikationsobjekt- Sperren/freigeben Web-Interface	32
Tabelle 8: Kommunikationsobjekte- Uhrzeit/Datum	33
Tabelle 9: Status Elemente - 1 Bit	35
Tabelle 10: Status Elemente - 1 Byte	36
Tabelle 11: Status Elemente - 2 Byte	36
Tabelle 12: Status Elemente - 2 Byte	36
Tabelle 13: Status Elemente - 14 Byte	36
Tabelle 14: Kommunikationsobjekte- Status Elemente	36
Tabelle 15: Einstellmöglichkeiten - Bit Alarme	37
Tabelle 16: Kommunikationsobjekte- Bit Alarm	37
Tabelle 17: Einstellmöglichkeiten - Text Alarme	39
Tabelle 18: Kommunikationsobjekte- Text Alarme	39
Tabelle 19: Einstellmöglichkeiten - Statusberichte	40
Tabelle 20: Kommunikationsobjekte- Statusbericht	40
Tabelle 21: Kommunikationsobjekt E-Mail Fehlercode	41
Tabelle 22: Kommunikationsobjekt E-Mail Pufferspeicher	41
Tabelle 23: Übersicht Kommunikationsobjekte	43

8 Anhang

8.1 Gesetzliche Bestimmungen

Die oben beschriebenen Geräte dürfen nicht in Verbindung mit Geräten benutzt werden, welche direkt oder indirekt menschlichen-, gesundheits- oder lebenssichernden Zwecken dienen. Ferner dürfen die beschriebenen Geräte nicht benutzt werden, wenn durch ihre Verwendung Gefahren für Menschen, Tiere oder Sachwerte entstehen können.

Lassen Sie das Verpackungsmaterial nicht achtlos liegen, Plastikfolien/-tüten etc. können für Kinder zu einem gefährlichen Spielzeug werden.

8.2 Entsorgungsroutine

Werfen Sie die Altgeräte nicht in den Hausmüll. Das Gerät enthält elektrische Bauteile, welche als Elektronikschrott entsorgt werden müssen. Das Gehäuse besteht aus wiederverwertbarem Kunststoff.

8.3 Montage



Lebensgefahr durch elektrischen Strom:

Alle Tätigkeiten am Gerät dürfen nur durch Elektrofachkräfte erfolgen. Die länderspezifischen Vorschriften, sowie die gültigen EIB-Richtlinien sind zu beachten.

8.4 Revisionshistorie

V 1.0 - Handbuch für die 3. Generation IP Router – SCN-IP100.03

05/2019