



Logiciel d'application

Interface KNX/IP Secure

Caractéristiques électriques/mécaniques : voir notice du produit

- ▲ Fabricants
- ▲ Hager Electro
- ▲ Composants de base
 - Interface IP / KNX

	Référence produit	Désignation produit	Réf. logiciel d'application	Produit filaire Produit radio
	TYFS120	Interface KNX/IP Secure	STYFS120	

Table des matières

1. Application	3
2. KNX Security	3
2.1. KNX IP Security pour la fonction Interface	3
2.2. KNX Data Security pour l'appareil	3
3. Installation et connexion	4
3.1. Mode de programmation KNX	4
3.2. Affichage d'état	4
4. Paramètres d'usine par défaut	6
5. Base de données ETS	7
6. Boîte de dialogue des paramètres ETS	11
6.1. Paramètres généraux	11
6.2. Mode de programmation à l'avant de l'appareil	11
6.3. Fonctionnement manuel de l'appareil	11
7. Programmation	12
7.1. Via le bus KNX	12
7.2. Via KNXnet/IP Tunneling	12
7.3. Via une connexion IP directe	12
8. Paramètres d'interface dans ETS	13
9. Accès à distance	15
9.1. Accès à distance avec NAT	15
9.2. Accès à distance avec VPN	15
9.3. Accès à distance et sécurité KNX	16
10. Licences Open Source	17

1. Application

L'interface KNX/IP Secure sert d'interface universelle pour PC ou ordinateur portable vers le bus KNX. Le bus KNX est accessible depuis n'importe quel point du réseau local (LAN). L'interface KNX/IP Secure peut être utilisée comme interface de programmation pour ETS®. Pour l'accès via KNXnet/IP Tunneling, au maximum 8 connexions simultanées sont possibles.

L'appareil prend en charge KNX Security. L'option peut être activée dans ETS. En tant qu'interface sécurisée, l'appareil empêche tout accès non autorisé au système.

L'adresse IP peut être attribuée via DHCP ou via la configuration ETS. L'appareil fonctionne selon la spécification KNXnet/IP en utilisant core, device management et tunneling.

L'alimentation est assurée par le bus KNX.

2. KNX Security

La norme KNX a été enrichie avec KNX Security pour protéger les installations KNX contre les accès non autorisés. KNX Security empêche de manière fiable la surveillance des communications et la manipulation du système.

La spécification KNX Security établit une distinction entre KNX IP Security et KNX Data Security. KNX IP Security protège les communications sur IP, tandis que sur KNX TP, les communications restent non chiffrées. Ainsi, KNX IP Security peut également être utilisé sur les systèmes KNX existants et avec des appareils KNX TP non sécurisés.

KNX Data Security décrit le chiffrement au niveau du télégramme. Cela signifie que les télégrammes transmis sur le bus à paire torsadée sont également cryptés.

2.1. KNX IP Security pour la fonction Interface

Lors de l'utilisation d'une interface KNX IP comme interface au bus, l'accès à l'installation est possible sans sécurité pour tous les appareils qui ont accès au réseau IP. Pour KNX Security, un mot de passe est nécessaire. Une connexion sécurisée est déjà établie pour la transmission du mot de passe. Toutes les communications via IP sont cryptées et sécurisées.

Dans les deux modes, l'interface transmet les télégrammes KNX cryptés et non cryptés. Les propriétés de sécurité sont vérifiées par le récepteur ou l'outil respectif.

2.2. KNX Data Security pour l'appareil

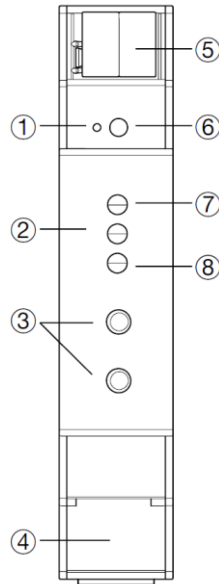
L'interface KNX/IP Secure prend également en charge KNX Data Security afin de protéger l'appareil contre les accès non autorisés du bus KNX. Si l'interface KNX IP est programmée via le bus KNX, cette opération est réalisée avec télégrammes cryptés.



Les télégrammes cryptés sont plus longs que les télégrammes non cryptés utilisés auparavant. Pour une programmation sécurisée via le bus, il est donc nécessaire que l'interface utilisée (par exemple USB) et les coupleurs de ligne intermédiaire prennent en charge les trames longues KNX.

3. Installation et connexion

L'interface KNX/IP Secure a été conçue pour être installée sur un rail DIN d'une largeur de 1 unité (18 mm). Elle comporte les contrôles et affichages suivants :



- ① Voyant LED de programmation
- ② Voyant LED de Mode
- ③ Bouton de mode de programmation
- ④ Connexion réseau RJ45
- ⑤ Connexion au bus KNX
- ⑥ Bouton de programmation
- ⑦ Voyant LED d'état KNX
- ⑧ Voyant LED d'état Ethernet/IP

L'interface KNX/IP Secure est alimentée par le bus KNX. Une alimentation externe n'est pas nécessaire.

i L'appareil ne fonctionne pas sans l'alimentation du bus KNX.

3.1. Mode de programmation KNX

Le mode de programmation KNX s'active/se désactive soit en appuyant sur le bouton de programmation KNX ⑥, soit en appuyant simultanément sur les boutons ③.

3.2. Affichage d'état

Le voyant KNX ⑦ s'allume en vert si l'appareil est alimenté avec succès par le bus KNX. Ce voyant indique la présence de télégrammes sur le bus KNX par un clignotement.

Les défaillances de communication (par exemple, les répétitions de télégrammes ou les fragments de télégrammes) sont indiquées par un bref changement de la couleur du voyant LED, en rouge.

État des voyants LED ⑦	Signification
Voyant LED vert	L'appareil est correctement alimenté par le bus KNX.
Voyant LED clignote en vert	Trafic de télégrammes sur le bus KNX
Voyant LED brièvement rouge	Défaillances de communication sur le bus KNX

Tableau 1 - Aperçu des différentes indications des voyants LED KNX

Le voyant IP ⑧ s'allume lorsqu'une liaison Ethernet est active. Ce voyant est vert si l'appareil a des paramètres IP valides (adresse IP, sous-réseau et passerelle). Avec des paramètres IP non valides ou inexistantes, le voyant est rouge. C'est également le cas si, par exemple, l'appareil n'a pas encore reçu les paramètres IP de la part d'un serveur DHCP. Le voyant LED indique la présence de télégrammes IP par un clignotement.

Installation et connexion

État des voyants LED ⑧	Signification
Voyant LED vert	L'appareil dispose d'une liaison Ethernet active et de paramètres IP valides.
Voyant LED rouge	L'appareil dispose d'une liaison Ethernet active et des paramètres IP non valides (ou n'a pas encore reçu les paramètres IP de la part d'un serveur DHCP).
Voyant LED clignote en vert	Trafic de télégrammes IP

Tableau 2 - Présentation des différentes indications du voyant LED IP

Le voyant de mode ② permet de visualiser l'état de chaque connexion de KNXnet/IP Tunneling.

Avec les boutons Conn Up/Dn ③, vous pouvez choisir chaque connexion. Conn Up ③ change le numéro de connexion vers le haut et Conn Dn ③ vers le bas. Le numéro de connexion réellement sélectionné est indiqué par un clignotement (1x...8x) du voyant LED de mode ②. Une connexion KNXnet/IP Tunneling disponible est indiquée par un voyant LED vert et une connexion Tunneling utilisée est indiquée par un voyant LED orange.

Via la fonction Escape (Esc), cette indication peut se terminer lorsque vous appuyez simultanément sur les boutons Conn Up/Dn ③.

Si ni le mode de programmation ni le fonctionnement manuel ne sont actifs, le voyant LED de Mode ② peut visualiser les erreurs de configuration.

État des voyants LED ②	Signification
Voyant LED vert	Le dispositif fonctionne en mode standard.
Voyant LED rouge	Le mode de programmation est actif
Voyant LED clignote en vert 1x.8x	Le mode de programmation n'est pas actif. Le fonctionnement manuel est actif. Le tunnel sélectionné (1-8) n'est pas utilisé et est libre
Le voyant LED clignote en orange 1x...8x	Le mode de programmation n'est pas actif. Le fonctionnement manuel est actif. Le tunnel sélectionné (1-8) est utilisé
Le voyant LED clignote en rouge	Le mode de programmation n'est pas actif. Le fonctionnement manuel n'est pas actif. L'appareil n'est pas chargé correctement, par exemple après un téléchargement interrompu.

Tableau 3 - Présentation des différentes indications du voyant LED de Mode

4. Paramètres d'usine par défaut

Configuration d'usine par défaut :

Adresse individuelle du dispositif :	15.15.255
Nombre de configurations KNXnet/IP Tunneling configurées :	1
Adresse individuelle de la configuration de tunnelisation :	15.15.240
Attribution d'adresses IP :	DHCP
Clé initiale (FDSK) :	active
Mode de sécurité :	inactif

Rétablir les paramètres d'usine de l'appareil (Master Reset)

Il est possible de rétablir les paramètres d'usine de l'appareil :

- Déconnectez le connecteur KNX Bus ⑤ de l'appareil.
- Appuyez sur le bouton de programmation KNX ⑥ et maintenez-le enfoncé
- Reconnectez le connecteur KNX Bus ⑤ de l'appareil.
- Maintenez le bouton de programmation KNX ⑥ enfoncé pendant au moins 6 secondes
- Un bref clignotement de tous les voyants LED (①②⑦⑧) permet de visualiser la réinitialisation des paramètres d'usine par défaut de l'appareil.

5. Base de données ETS

La base de données ETS (ETS 5.7 ou version ultérieure) peut être téléchargée sur le site Web de l'interface KNX/IP Secure ou via le catalogue en ligne KNX.

Si la fonctionnalité KNX IP Secure ne vous intéresse pas, vous avez toujours la possibilité d'utiliser une version non sécurisée de l'application pour configurer votre appareil.

Si vous utilisez la version sécurisée de l'application, les étapes suivantes doivent être effectuées.

Si le premier produit est inséré dans un projet avec KNX Security, ETS vous invite à entrer un mot de passe de projet.

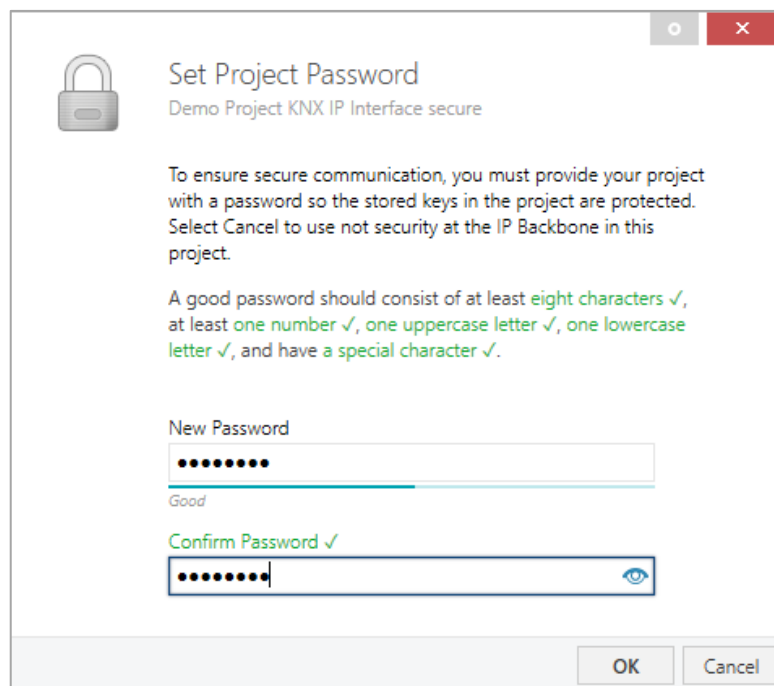


Figure 1 : Définition du mot de passe du projet

Ce mot de passe protège le projet ETS contre les accès non autorisés. Ce mot de passe n'est pas une clé utilisée pour la communication KNX. L'entrée du mot de passe peut être ignorée en cliquant sur le bouton « Annuler », mais cela n'est pas recommandé, pour des raisons de sécurité.

ETS nécessite un certificat pour chaque appareil créé dans ETS qui utilise KNX Security. Ce certificat contient le numéro de série de l'appareil, ainsi qu'une clé intangible (FDSK = Factory Default Setup Key).

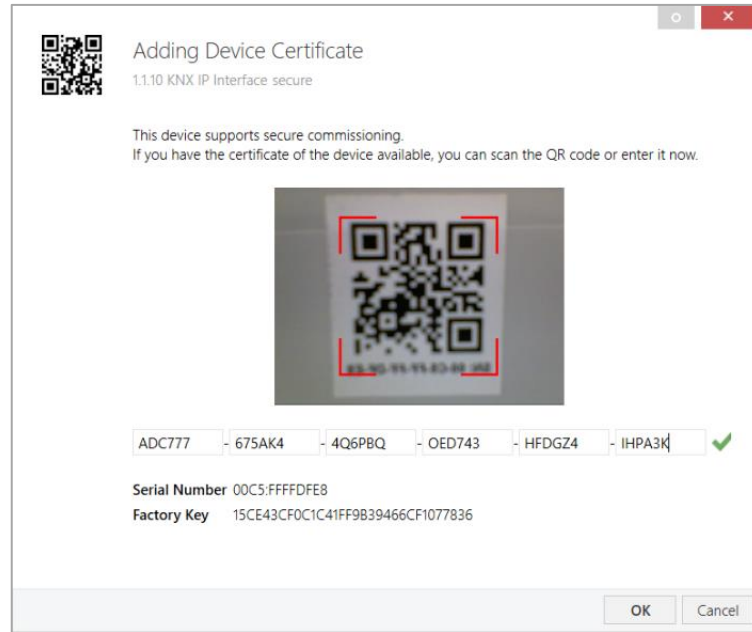


Figure 2 - Ajout d'un certificat d'appareil

Le certificat est imprimé sous forme de texte sur l'appareil. Il peut également être facilement scanné à partir du QR code imprimé via une webcam.

La liste de tous les certificats d'appareils peut être gérée dans la fenêtre Vue d'ensemble - Projets - Sécurité.

Cette clé initiale est nécessaire pour mettre un appareil en service en toute sécurité dès le début. Même si le téléchargement ETS est enregistré par un tiers, ce dernier n'a aucun accès par la suite aux appareils sécurisés. Au cours du premier téléchargement sécurisé, la clé initiale est remplacée par ETS par une nouvelle clé générée individuellement pour chaque appareil. Cela empêche les personnes ou les dispositifs qui connaissent la clé initiale d'accéder à l'appareil. La clé initiale n'est réactivée qu'après une réinitialisation de type Master Reset.

Le numéro de série du certificat permet à ETS d'affecter la clé appropriée à un appareil lors d'un téléchargement.

Dans ETS, certains paramètres s'affichent dans la fenêtre Propriétés (sur le côté droit) en plus de la fenêtre Paramètres. Les paramètres IP peuvent être définis ici. Les adresses supplémentaires des connexions d'interface sont affichées dans la vue topologique.

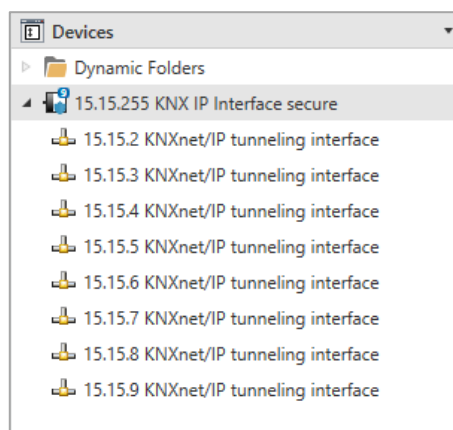


Figure 3 : Appareils

Chaque adresse individuelle KNX peut être modifiée en cliquant sur l'entrée de liste et en tapant l'adresse souhaitée dans la zone de texte « Adresse Individuelle ». Si le cadre de la zone de texte devient rouge une fois que vous avez entré l'adresse, cela signifie que l'adresse est déjà utilisée dans votre projet ETS.

Assurez-vous qu'aucune des adresses ci-dessus n'est déjà utilisée dans votre installation KNX.

Lorsque vous cliquez sur l'entrée du dispositif « Interface KNX IP Secure » dans la vue topologique de vos projets ETS, une colonne d'informations « Propriétés » apparaît à droite de la fenêtre ETS. Dans la vue d'ensemble « Paramètres », vous pouvez modifier le nom de l'appareil.

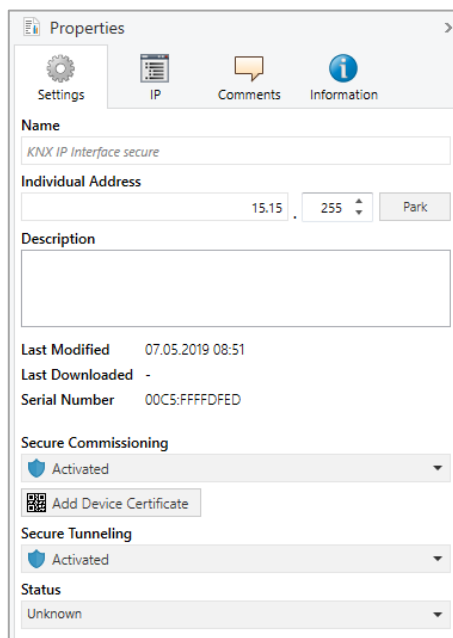


Figure 4 - Propriétés

Si le Tunneling sécurisé est activé, un mot de passe unique sera créé automatiquement pour chaque tunnel. Ces mots de passe peuvent être affichés dans la vue d'ensemble « Paramètres », lorsqu'un tunnel est sélectionné.

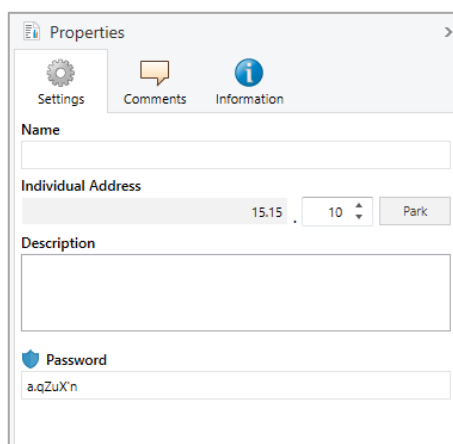


Figure 5 - Propriétés

Dans la vue d'ensemble « IP », les options spécifiques au réseau IP de l'interface KNX/IP Secure peuvent être modifiées.

En remplaçant « Obtenir une adresse IP automatiquement » par « Utiliser une adresse IP statique », l'adresse IP, le masque de sous-réseau et la passerelle par défaut peuvent être définis librement.

Toutes les modifications apportées au menu des propriétés prennent effet uniquement après un téléchargement réussi de l'application.

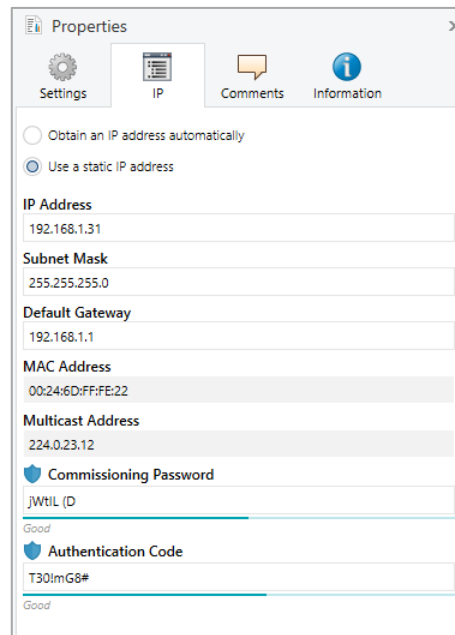


Figure 6 - Propriétés

■ Adresse IP

Ici, l'adresse IP de l'interface KNX/IP Secure peut être saisie. Cela permet d'adresser l'appareil via le réseau IP (LAN). L'adressage IP doit être coordonné avec l'administrateur du réseau.

■ Masque de sous-réseau

Entrez le masque de sous-réseau ici. L'appareil utilise les valeurs entrées dans ce masque pour déterminer s'il existe un partenaire de communication sur le réseau local. S'il n'y a pas de partenaire sur le réseau local, l'appareil n'enverra pas les télégrammes directement au partenaire, mais à la passerelle qui achemine le télégramme.

■ Passerelle par défaut

Entrez ici l'adresse IP de la passerelle, par exemple le routeur DSL de l'installation.

■ Exemple d'attribution d'adresses IP :

Un PC est utilisé pour l'accès à l'interface sécurisée IP de KNX :

Adresse IP du PC :192.168.1.30

Sous-réseau du PC :255.255.255.0

L'interface KNX/IP Secure est située sur le même réseau local, c'est-à-dire qu'elle utilise le même sous-réseau. Le sous-réseau restreint les adresses IP qui peuvent être affectées. Dans cet exemple, l'adresse IP de l'interface IP doit être 192.168.1.xx, où xx peut être un nombre compris entre 1 et 254 (à l'exception de 30, qui est déjà utilisé). Il faudra s'assurer qu'aucune adresse IP n'est attribuée deux fois.

Adresse IP de l'interface IP :192.168.1.31

Sous-réseau de l'interface IP :255.255.255.0

6. Boîte de dialogue des paramètres ETS

Les paramètres suivants peuvent être définis à l'aide d'ETS.

6.1. Paramètres généraux

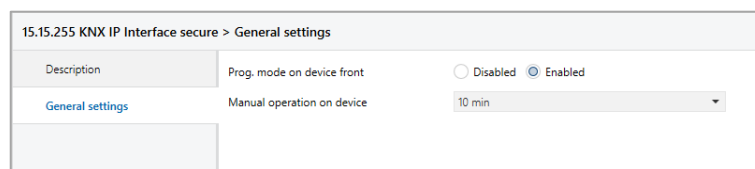


Figure 7 - Paramètres généraux

6.2. Mode de programmation à l'avant de l'appareil

En plus du bouton de programmation normal ⑥, vous pouvez activer le mode de programmation sur le devant de l'appareil sans ouvrir le capot du tableau de distribution. Le mode de programmation peut être activé et désactivé en appuyant simultanément sur les boutons ③.

Cette fonctionnalité peut être activée et désactivée via le paramètre « Mode Prog. en face avant ». Le bouton de programmation encastré ⑥ (à côté du voyant de programmation ①) est toujours activé et n'est pas influencé par ce paramètre.

6.3. Fonctionnement manuel de l'appareil

Le fonctionnement manuel de l'interface KNX/IP Secure ne contient que l'affichage de l'état. Ce paramètre définit la durée du mode manuel. Une fois l'opération terminée, le mode d'affichage normal est rétabli.

7. Programmation

L'interface KNX/IP Secure peut être programmée de différentes manières via ETS :

7.1. Via le bus KNX

L'appareil ne doit être connecté qu'au bus KNX. ETS nécessite une interface supplémentaire (par exemple, USB) pour avoir accès au bus. De cette façon, l'adresse individuelle et l'application complète (y compris la configuration IP) peuvent être programmées. La programmation via le bus est recommandée si aucune connexion IP ne peut être établie.

7.2. Via KNXnet/IP Tunneling

Aucune interface supplémentaire n'est requise. La programmation via KNXnet/IP Tunneling est possible si l'appareil possède déjà une configuration IP valide (par exemple via DHCP). Dans ce cas, l'appareil s'affiche dans la configuration de l'interface d'ETS et doit être sélectionné. Le téléchargement est exécuté via le projet ETS, comme pour beaucoup d'autres appareils.

7.3. Via une connexion IP directe

Alors que KNXnet/IP Tunneling est limité à la vitesse de KNX TP, l'appareil peut être chargé via une connexion IP directe haut débit. La connexion IP directe est possible si l'appareil possède déjà une configuration IP valide, ainsi qu'une adresse physique. Pour cela, sélectionnez « Utiliser une connexion IP directe si disponible » dans le menu « Bus - Options de Connexions ». Le téléchargement est alors effectué directement sur l'appareil et n'est pas visible dans le moniteur de groupe ETS.

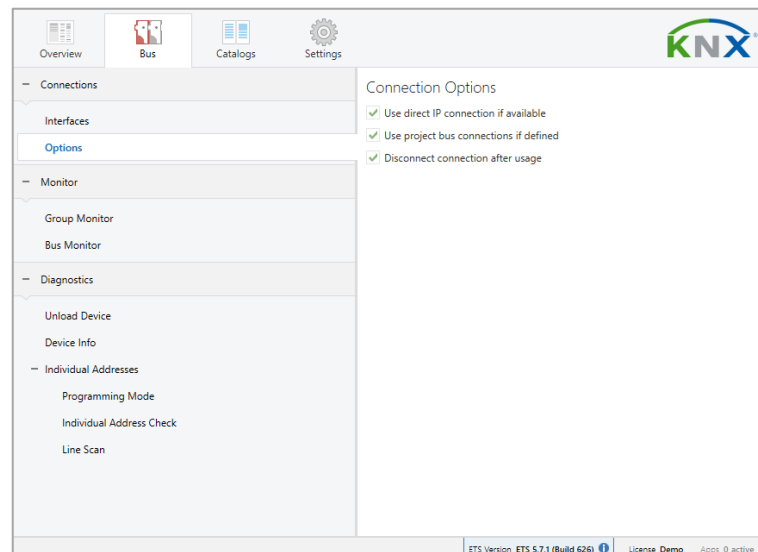


Figure 8 - Options de connexion



En raison des temps de transmission beaucoup plus courts, il est recommandé d'effectuer les téléchargements via IP.

8. Paramètres d'interface dans ETS

L'interface KNX/IP Secure peut être utilisée comme interface de programmation. ETS peut utiliser cette fonction pour établir une connexion via IP à la ligne TP correspondante.

Dans ETS, les interfaces KNX peuvent être sélectionnées et configurées via le menu « Interfaces Bus » d'ETS.

ETS peut accéder aux interfaces KNX IP configurées, même sans entrée dans la base de données. Si la configuration de l'interface KNX IP ne respecte pas les conditions de l'installation KNX, elle doit être configurée via un projet ETS. Pour plus d'informations, consultez la section ETS consacrée aux bases de données.

Si le mode de sécurité est activé dans l'interface KNX IP, un mot de passe est requis pour établir une connexion.

En tant que valeur par défaut, l'attribution de l'adresse IP est définie sur « obtenir une adresse IP automatiquement » et aucun autre paramètre n'est donc nécessaire. Pour pouvoir utiliser cette fonctionnalité, un serveur DHCP doit être présent sur le LAN (par exemple, de nombreux routeurs DSL possèdent un serveur DHCP intégré).

Si l'interface KNX IP a été connectée au réseau local et possède une adresse IP valide, elle doit apparaître automatiquement dans le menu « Bus », sous « Interfaces Trouvées ».

En cliquant sur l'interface découverte, cette dernière est sélectionnée comme interface actuelle. Sur le côté droit de la fenêtre ETS, toutes les informations et options spécifiques de la connexion apparaissent.

Le nom d'appareil indiqué et la « Host Individual Address » (adresse individuelle de l'appareil) peuvent uniquement être modifiés dans votre projet ETS.

Comme tous les appareils KNX programmables, l'interface KNX/IP Secure a une adresse individuelle qui peut être utilisée pour l'accès à l'appareil. Elle est utilisée, par exemple, par ETS lors du transfert vers l'interface KNX IP via le bus.

Pour la fonction d'interface, l'appareil contient des adresses individuelles supplémentaires qui peuvent être définies dans ETS. Lorsqu'un client (par exemple ETS) envoie via l'interface KNX IP des télégrammes au bus, ceux-ci contiennent une adresse d'expéditeur figurant parmi les adresses supplémentaires. Chaque adresse est associée à une connexion. Les télégrammes de réponse peuvent ainsi être clairement transmis au client respectif.

Les adresses individuelles supplémentaires doivent être sélectionnées dans la plage d'adresses de la ligne de bus dans laquelle l'interface est installée ; elles ne peuvent pas être utilisées par un autre appareil.

Exemple :

Adresse du dispositif	1.1.10	(adresse dans la topologie ETS)
Connexion 1	11.1.240	(1. adresse supplémentaire)
Connexion 2	11.1.241	(2. adresse supplémentaire)
Connexion 3	11.1.242	(3. adresse supplémentaire)
Connexion 4	11.1.243	(4. adresse supplémentaire)
Connexion 5	11.1.244	(5. adresse supplémentaire)
Connexion 6	11.1.245	(6. adresse supplémentaire)
Connexion 7	11.1.246	(7. adresse supplémentaire)
Connexion 8	11.1.247	(8. adresse supplémentaire)

La section « Adresse Individuelle » vous permet de sélectionner l'adresse KNX individuelle de la connexion KNXnet/IP Tunneling actuellement utilisée.

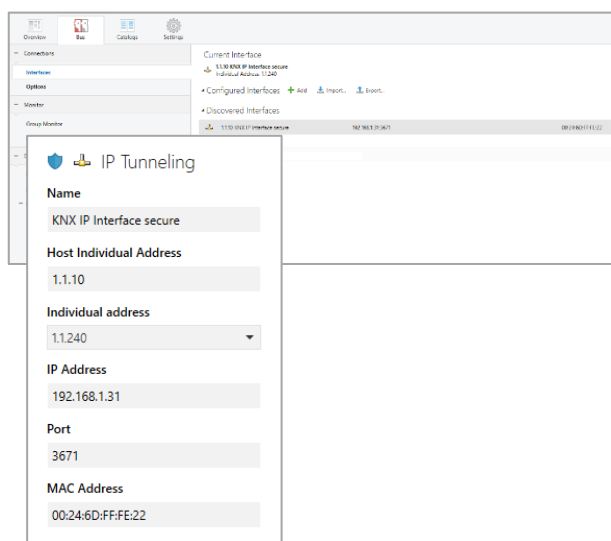


Figure 9 - IP Tunneling

L'adresse individuelle de l'appareil KNX et les adresses individuelles des connexions Tunneling supplémentaires peuvent être modifiées dans le projet ETS après l'ajout de l'appareil au projet.

9. Accès à distance

9.1. Accès à distance avec NAT

NAT (Network Address Translation) est une méthode utilisée pour traduire les adresses IP. Elle est principalement utilisée par les routeurs (par exemple, par les routeurs DSL/Fibre).

AVERTISSEMENT

Veillez noter que l'accès à distance via NAT, sans autres mesures de sécurité, présente des dangers importants. La redirection de port fournit un accès universel à votre réseau IP local et à votre système KNX.

Tout utilisateur d'Internet peut découvrir le port ouvert de votre adresse IP publique statique et peut, par exemple, accéder à votre réseau KNX via le logiciel ETS.

Nous vous conseillons fortement d'utiliser NAT uniquement temporairement à des fins de test ou de diagnostic. Après cela, fermez à nouveau le port pour éviter tout usage abusif.



Si l'accès à distance est assuré par NAT, nous vous conseillons fortement de ne pas spécifier le port par défaut (3671) vers Internet. Le port 3671 est le port officiel efc - eFieldControl(EIBnet), déposé par l'Association KNX. Ce port peut être facilement déterminé par des personnes non autorisées. Utilisez un port figurant dans la plage non réservée comprise entre le port 50000 et le port 60000.

L'accès permanent à distance ne devrait être établi que lorsqu'il est protégé ! Nous recommandons l'accès à distance via VPN (Virtual Private Network). La fonctionnalité VPN est déjà intégrée à la plupart des routeurs DSL.

9.2. Accès à distance avec VPN

Un VPN est une extension de réseaux privés. Il peut être utilisé pour activer l'accès à distance et pour relier des réseaux privés (site à site) via Internet.

Site-to-end (du site à la destination)

Un VPN du site à la destination peut être utilisé pour établir l'accès à un réseau interne. Par exemple, les employés sur le terrain peuvent l'utiliser pour se connecter à leur réseau d'entreprise.

Site-to-site (de site à site)

Un VPN de site à site peut être utilisé pour le lien de réseaux privés. Par exemple, un VPN de site à site peut effectuer le lien de deux réseaux d'entreprise distants.

Il n'est pas possible pour ETS d'identifier automatiquement l'interface via la connexion VPN. Dans la zone de texte « Serveur », vous devez renseigner l'adresse IP de l'interface KNX IP.



La case à cocher « Se connecter en mode de conversion (NAT) » doit être activée. Bien que la connexion ne soit pas établie en mode NAT, cette option permet de réaliser certaines initialisations nécessaires à une connexion KNXnet/IP.

9.3. Accès à distance et sécurité KNX

En raison des différentes possibilités d'accès à distance et de la possibilité de choisir entre KNX sécurisé et KNX non sécurisé, les options suivantes sont possibles.

	NAT	VPN
KNX non sécurisé	Avertissement non protégé	OK
KNX sécurisé	OK	Protection optimale

L'accès à distance via NAT et KNX non sécurisé est entièrement non protégé et ne doit jamais être utilisé. L'utilisation simultanée de KNX Security et de VPN permet d'obtenir des résultats optimaux en matière de protection.

10. Licences Open Source

Ce produit contient une licence logicielle open source :

curve25519-donna : Courbe elliptique Curve25519, fonction de clé publique

Source : <http://code.google.com/p/curve25519-donna/>

Copyright 2008, Google Inc. Tous droits réservés.

La redistribution et l'utilisation sous forme source et binaire, avec ou sans modification, sont autorisées à condition que les conditions suivantes soient remplies :

Les redistributions de code source doivent conserver l'avis de copyright ci-dessus, cette liste de conditions et la clause de non-responsabilité suivante.

Les redistributions sous forme binaire doivent reproduire l'avis de copyright ci-dessus, cette liste de conditions et la clause de non-responsabilité suivante dans la documentation et/ou les autres documents fournis dans le cadre de la distribution.

Ni le nom de Google Inc. ni le nom de ses contributeurs ne peuvent être utilisés pour approuver ou promouvoir des produits dérivés de ce logiciel sans autorisation écrite préalable spécifique.

CE LOGICIEL EST FOURNI PAR LES TITULAIRES DE DROITS D'AUTEUR ET LES CONTRIBUTEURS « EN L'ÉTAT » ET TOUTE GARANTIE EXPRESSE OU IMPLICITE, Y COMPRIS, SANS S'Y LIMITER, LES GARANTIES IMPLICITES DE COMMERCIALISATION ET D'ADÉQUATION À UN USAGE PARTICULIER, EST EXCLUE. EN AUCUN CAS, LE PROPRIÉTAIRE DES DROITS D'AUTEUR OU LES CONTRIBUTEURS NE PEUVENT ÊTRE TENUS RESPONSABLES DE TOUT DOMMAGE DIRECT, INDIRECT, ACCIDENTEL, SPÉCIAL, EXEMPLAIRE OU CONSÉQUENT (Y COMPRIS, SANS S'Y LIMITER, L'ACHAT DE BIENS OU DE SERVICES DE SUBSTITUTION, PERTE D'UTILISATION, DE DONNÉES OU DE PROFITS, D'INTERRUPTION D'ACTIVITÉ) QUELLE QU'EN SOIT LA CAUSE ET QUELLE QUE SOIT LA THÉORIE DE RESPONSABILITÉ, QU'IL S'AGISSE D'UN CONTRAT, D'UNE RESPONSABILITÉ STRICTE OU D'UN DÉLIT (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE QUELQUE MANIÈRE QUE CE SOIT DE L'UTILISATION DE CE LOGICIEL, EN CAS DE NOTIFICATION DE LA POSSIBILITÉ DE TELS DOMMAGES.



AVERTISSEMENT

- L'appareil doit être monté et mis en service par un électricien agréé.
- Les règles de sécurité en vigueur doivent être respectées.
- L'appareil ne doit pas être ouvert.
- Concernant la planification et la construction d'installations électriques, les directives, réglementations et normes pertinentes de chaque pays doivent être prises en considération



Hager Electro SAS
132 boulevard d'Europe
BP3
67210 OBERNAL cedex
hager.com

6LE008078A