Guide de Sécurité KNX

Édition du manuel: b

www.zennio.fr

MANUEL D'UTILISATION

SOMMAIRE

ACTUALISATIONS DU DOCUMENT

Version	Modifications	Page(s)
b	S'ajoutent les indications pour réaliser un démarrage d'usine.	14

1 INTRODUCTION

Jusqu'à maintenant, les données transmises sur une installation domotique KNX étaient ouvertes et pouvaient être lues et manipulées par toute personne ayant des connaissances en la matière et ayant accès au support KNX, de cette manière la sécurité est garantie en empêchant l'accès au bus KNX ou aux dispositifs. Les nouveaux protocoles de sécurité **KNX Secure** ajoutent une sécurité additionnelle aux communications sur une installation KNX pour éviter ce possible type d'attaque.

Les dispositifs qui disposent de la sécurité KNX auront la capacité de se communiquer de forme sûre avec ETS et avec n'importe quel autre dispositif KNX Secure, vue qu'ils incorporent un système d'authentification et de chiffrage de l'information.

Il se différencient deux types de sécurité KNX qui peuvent être mis en œuvre simultanément dans la même installation.

- **KNX Data Secure :** assure la communication dans une installation KNX.
- **KNX IP Secure :** pour installation KNX avec communication IP, assure la communication au travers du réseau IP.

L'utilisation de la sécurité dépend de deux paramètres significatifs dans le projet de ETS :

- Sécurité au démarrage : définit si, pendant la mise en marche, le dispositif doit se communiquer avec ETS de manière sûre et ouvre la possibilité d'activer la sécurité sur le fonctionnement.
- Sécurité sur le fonctionnement : permet de choisir si pendant l'exécution, la communication entre dispositifs doit être sûre ou non. C'est à dire, déterminer quelles adresses de groupe seront sures. Pour activer la sécurité pendant le fonctionnement, la sécurité pendant la mise en service doit être activée.

L'activation de la sécurité sur les dispositifs KNX Secure est optionnelle. S'il est activé, il est défini individuellement sur les adresses de groupe, de sorte que tout ou partie de vos objets peuvent être sécurisés, le reste fonctionnant normalement avec des dispositifs non sécurisés. C'est à dire, des dispositifs avec et sans KNX Secure peuvent coexister sur la même installation.

2 CONFIGURATION

À partir de la version 5.7 de ETS, il est permis l'utilisation de la sécurité KNX et toutes ses fonctionnalités pour travailler avec des dispositifs sûrs. Il y a deux types de sécurité, la sécurité KNX, c'est à dire, sur le bus KNX et la sécurité KNX IP qui correspond au support IP.

Dans cette section, il s'expose un guide pour la configuration de la sécurité KNX sur les projets ETS.

2.1 SÉCURITÉ SUR LE BUS KNX

Sa mise en oeuvre assure la communication entre dispositifs sur le support TP, lesquels transmettront des télégrammes chiffrés à d'autres dispositifs qui disposent aussi de la sécurité KNX.

Il sera possible de choisir pour chaque adresse de groupe, si la communication sera de forme sûre ou non.

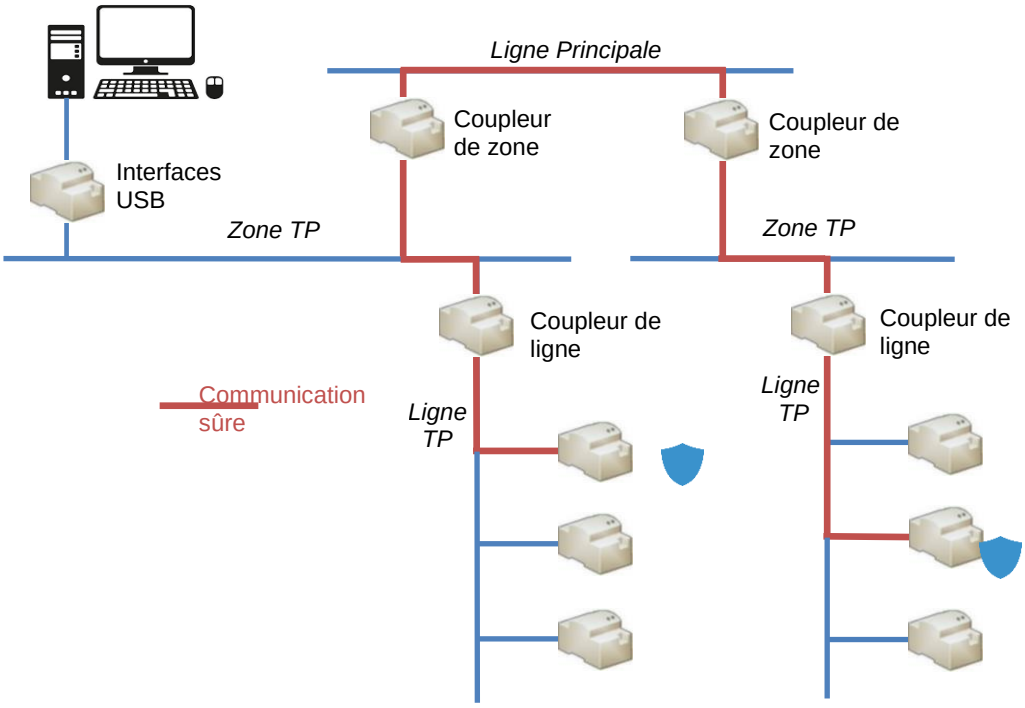


Figure 1. Schéma de sécurité sur le bus KNX

2.1.1 MISE EN MARCHE SÛRE

Lorsqu'un dispositif à un démarrage sécurisé, la communication entre le ETS et le dispositif s'effectue en mode sécurisé.

Un dispositif devra avoir un démarrage sécurisé configuré chaque fois qu'il y a sécurité pendant le fonctionnement, c'est à dire, qu'un de ses objets est associé à une adresse de groupe sécurisée (voir section 2.1.2).

Note : *Prenez en compte que la présence d'un dispositif sécurisé dans un projet ETS suppose la protection du propre projet avec un mot de passe.*

PARAMÉTRAGE ETS

La configuration de la sécurité au démarrage s'établit depuis l'onglet "Configuration", dans la fenêtre de "Propriété" du dispositif.

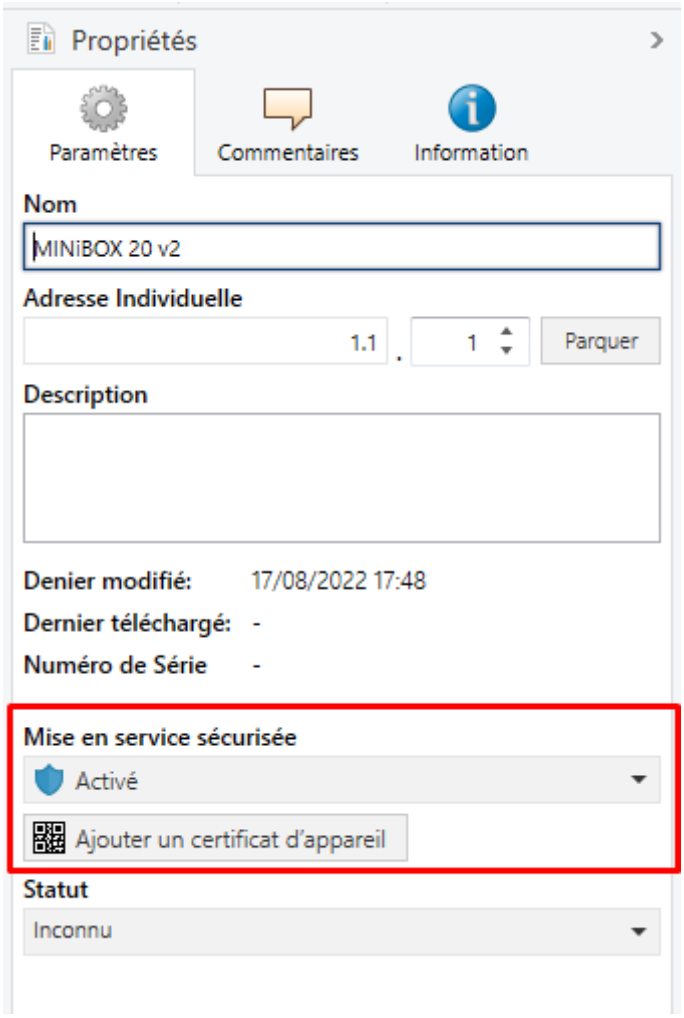


Figure 2. Sécurité sur le bus KNX - Mise en marche sûr.

- **Mise en marche sûr** [*Activé / Désactivé*] : permet de choisir si ETS doit se communiquer avec le dispositif en mode sûr ou non, c'est à dire, qu'il permet d'habiliter ou déshabiliter la sécurité KNX sur le dispositif.

Si ce choisie l'option "Activée", il sera nécessaire **d'établir un mot de passe pour le projet**, sans celle-ci il n'est pas permis de télécharger avec sécurité.

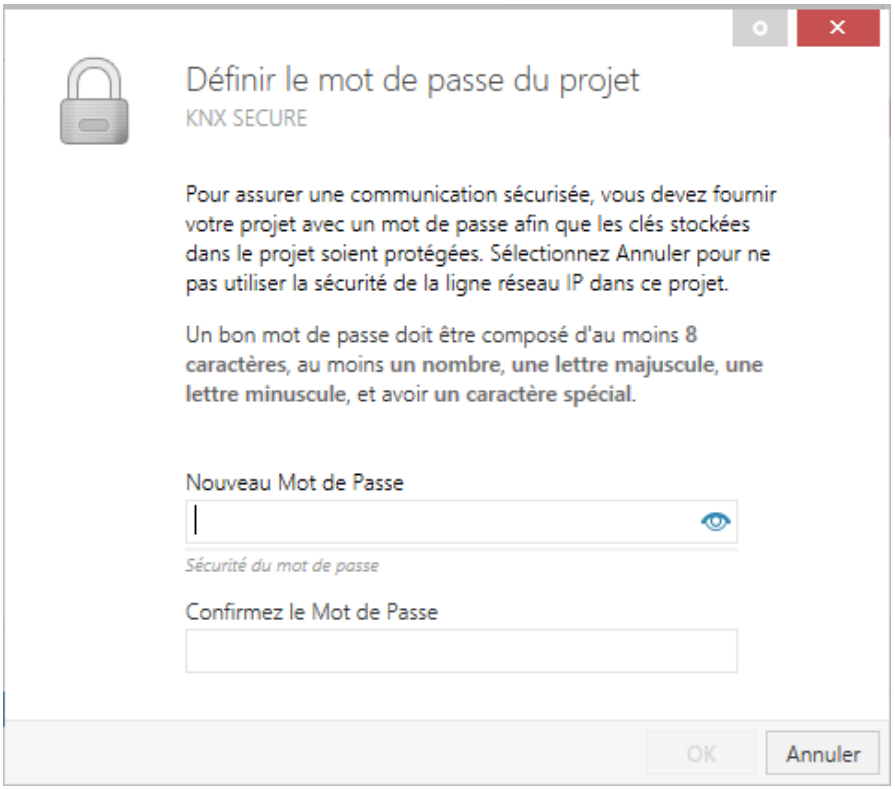


Figure 3. Projet - Établir mot de passe.

Un mode additionnel d'établir un mot de passe sur un projet est à travers de la fenêtre principale ("Vision générale") de ETS À sélectionner le projet, il se montrera une section sur la partie de droite ou, dans "détails", il sera possible d'introduire le mot de passe désiré.

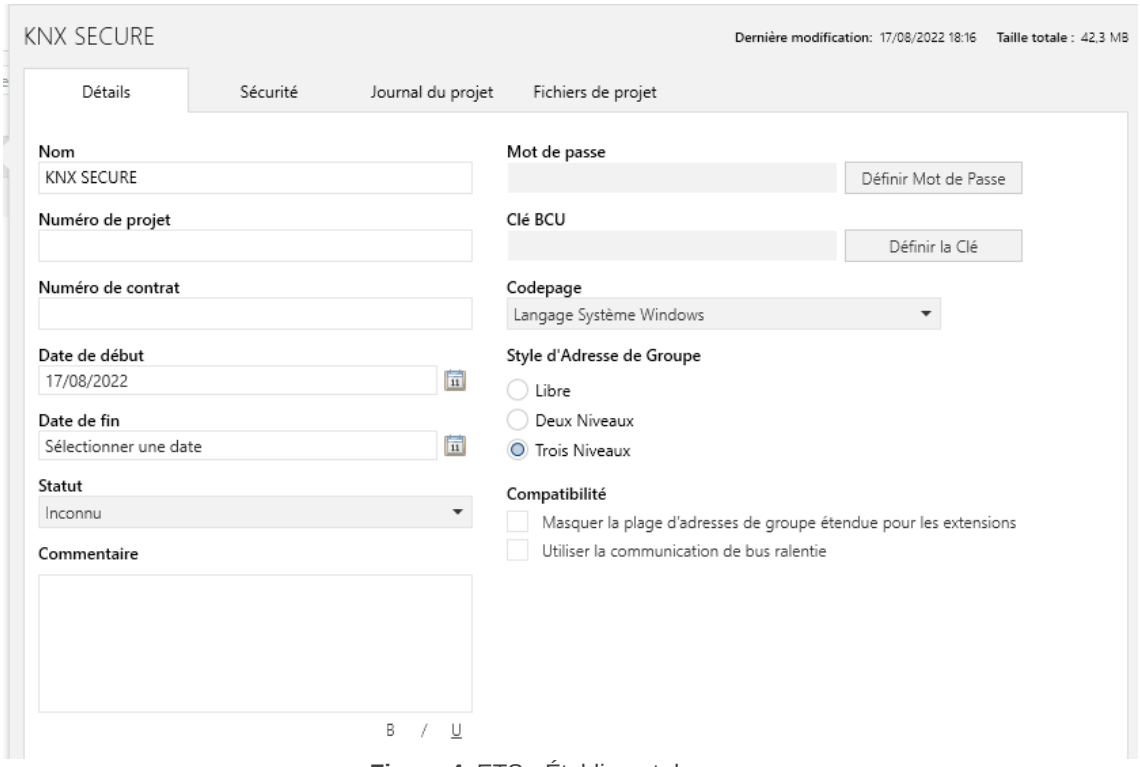


Figure 4. ETS - Établir mot de passe.

- **Ajouter le Certificat du dispositif :** Si la **mise en marche sûr** est "*activée*", ETS en plus du mot de passe, demandera un certificat unique pour le dispositif

  Le **certificat** à ajouter [*xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx*] compte de 36 caractères alphanumériques généré à partir du numéro de série et la clé de fabrique ou *FDSK* (*Factory Default Setup Key*) du dispositif. Il est inclu avec le dispositif et contient le code QR correspond pour pouvoir le scanner facilement.

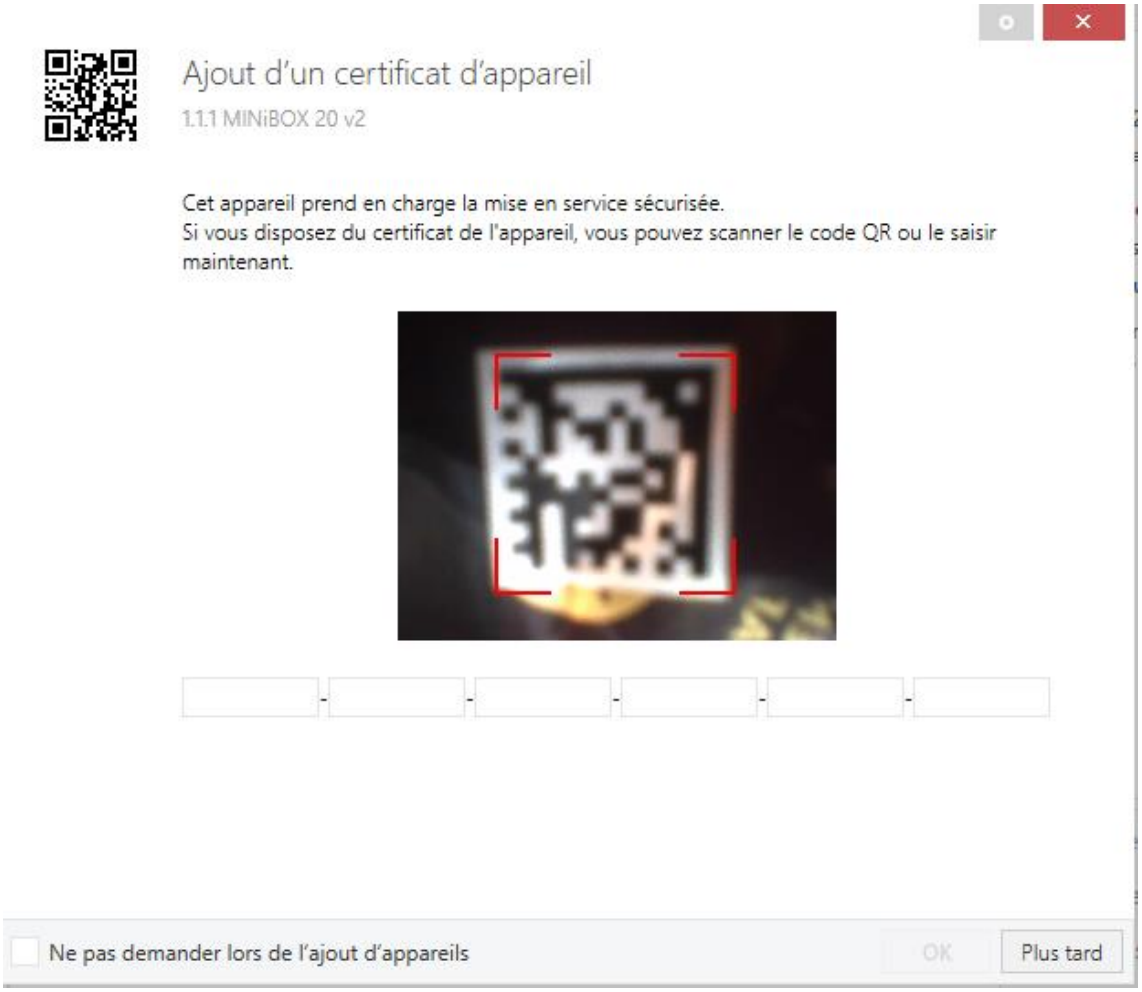


Figure 5. Projet - insérer le certificat du dispositif.

Le certificat du dispositif pourra être aussi ajouté depuis l'onglet principal de ETS ("vision générale"), en accédant à la section "Sécurité" du nouvel onglet qui se visualise sur la partie de droite à sélectionner le projet.

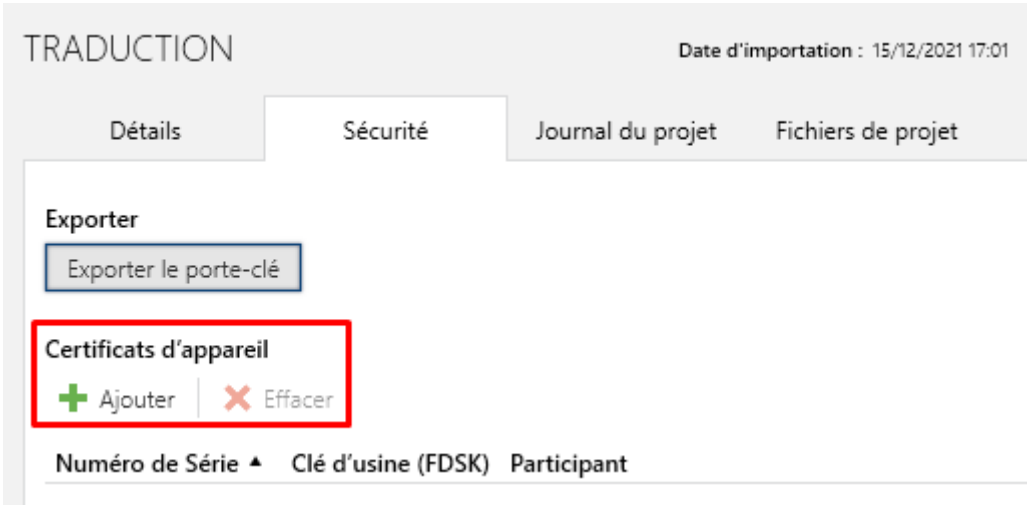


Figure 6. ETS - Ajouter le Certificat du dispositif:

Pendant le premier démarrage sécurisé, ETS change le FDSK du dispositif par une nouvelle clé, la clé de l'outil (*Tool Key*) qui se génère individuellement pour chaque dispositif que démarre de manière sécurisée.

Si le projet se perd, toutes les clés de l'outil se perdront avec lui. Ce qui fera que les dispositifs ne pourront pas se reprogrammer. Pour pouvoir les récupérer, il faut rétablir la clé de fabrique (FDSK).

La FDSK peut être restituée de deux façons différentes : avec une déprogrammation, à condition qu'elle soit effectuée à partir du projet dans lequel la mise en service a été effectuée, ou après une réinitialisation manuelle des valeurs d'usine (voir section 3).

2.1.2 COMMUNICATION DU GROUPE SÉCURISÉ

Chaque objet d'un dispositif pourra transmettre son information de façon cryptée, en établissant ainsi une sécurité dans la communication ou fonctionnement.

Pour qu'un objet dispose de la sécurité KNX, celle-ci devra être configurée depuis la propre adresse de groupe, c'est à dire, l'adresse à laquelle l'objet sera associé.

PARAMÉTRAGE ETS

La configuration de la sécurité dans la communication s'établit depuis le sous onglet "Configuration", dans la fenêtre de "Propriété" de l'adresse de groupe.

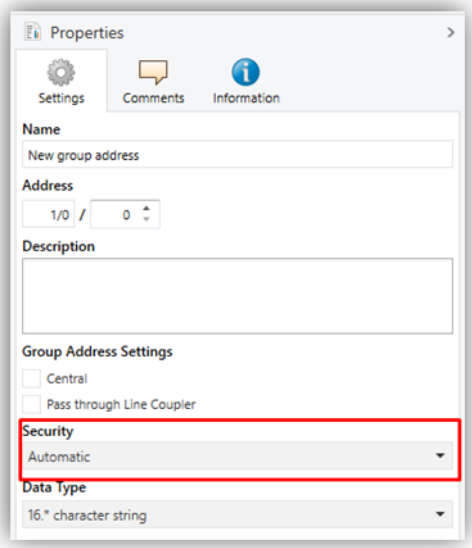


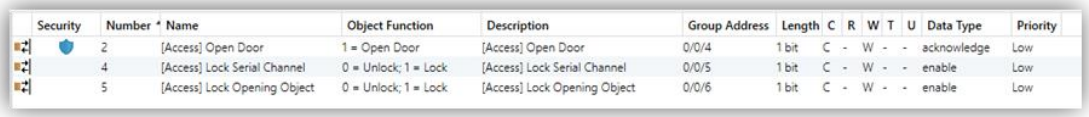
Figure 7. Sécurité sur le bus KNX - Sécurité sur les adresses de groupe.

- **Sécurité** [*Automatique / Allumé / Désactivé*] : Si se sélectionne l'option "*Automatique*", ETS sera celui qui décide si s'active ou non la sécurité selon si les deux objets liés peuvent se communiquer de façon sécurisée.

Notes :

- Tous les objets associés à une **adresse de groupe sécurisée** seront des **objets sécurisés**
- *Un même dispositif peut avoir des adresses de groupe sécurisées et non sécurisées.*

Les objets sécurisés peuvent s'identifier avec un "bouclier bleu".



Security	Number	Name	Object Function	Description	Group Address	Length	C	R	W	T	U	Data Type	Priority
🛡	2	[Access] Open Door	1 = Open Door	[Access] Open Door	0/0/4	1 bit	C	-	W	-	-	acknowledge	Low
	4	[Access] Lock Serial Channel	0 = Unlock; 1 = Lock	[Access] Lock Serial Channel	0/0/5	1 bit	C	-	W	-	-	enable	Low
	5	[Access] Lock Opening Object	0 = Unlock; 1 = Lock	[Access] Lock Opening Object	0/0/6	1 bit	C	-	W	-	-	enable	Low

Figure 8. Objet sûr.

2.2 SÉCURITÉ KNX-IP

La sécurité KNX IP a été conçu pour les installations KNX avec communication IP. Sa mise en oeuvre garantit l'échange sécurisé des données KNX entre les installations via des dispositifs KNX sécurisés avec connexion IP

Ce type de sécurité s'applique sur des interfaces de bus et uniquement sur le support IP, c'est à dire, les télégrammes sécurisés se transmettent entre coupleurs, dispositifs et interfaces KNX-IP sécurisés.

Pour que la transmission des télégrammes sur une ligne principale ou sous-ligne soit aussi sécurisée, il faudra activer la sécurité sur le bus KNX (voir section 2.1).

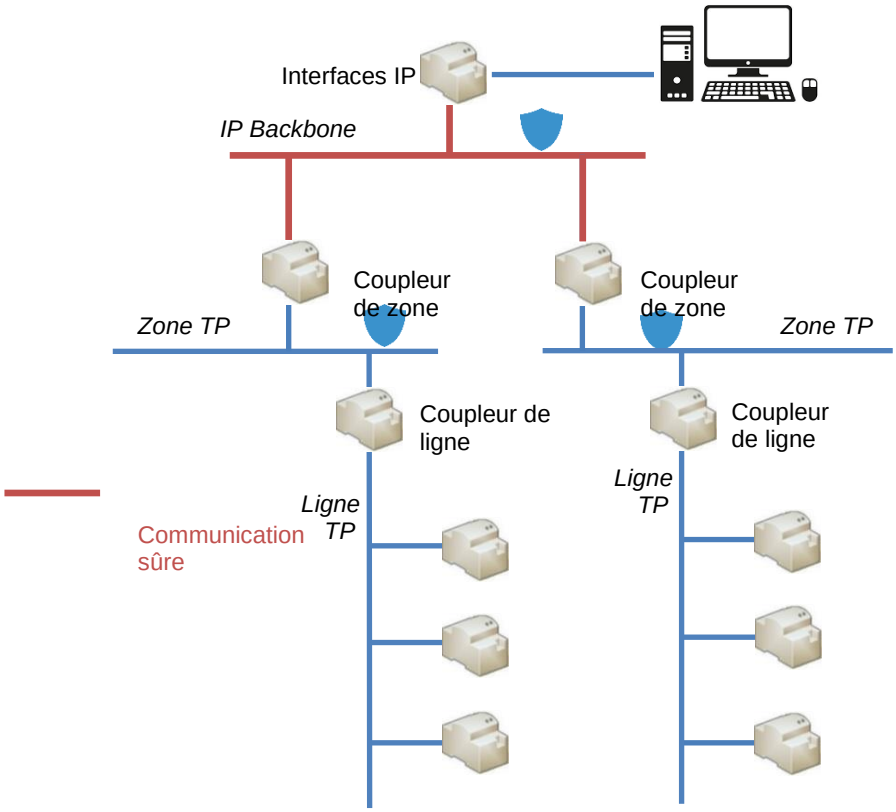


Figure 9. Schéma de Sécurité KNX IP

2.2.1 MISE EN MARCHE SÛRE

Dans ce type de sécurité, à part la mise en marche sécurisée de la section 2.1.1, il peut s'activer aussi le "Tunneling sécurisé". Ce paramètre se trouve dans l'onglet de "Configuration" de la fenêtre de propriétés des dispositifs sécurisés avec connexion IP sur la partie droite de l'écran de ETS.

PARAMÉTRAGE ETS

La configuration de la sécurité au démarrage et dans le *tunneling* s'établit depuis l'onglet "Configuration", dans la fenêtre de "Propriété" du dispositif.

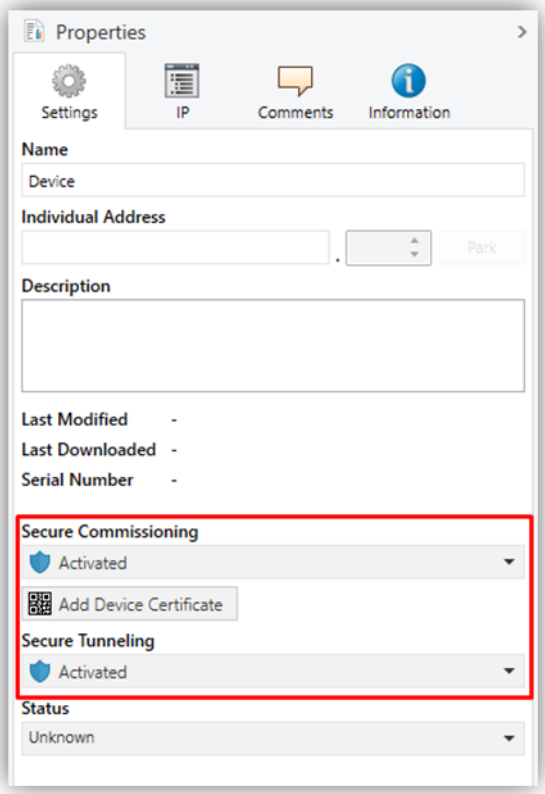


Figure 10. Sécurité KNX IP - Mise en marche et *Tunneling* sécurisé.

En plus de la **mise en marche sécurisé** et le bouton **Ajouter Certificat du Dispositif**, expliqués dans la section 2.1.1, il apparaîtra aussi :

- ***Tunneling* sécurisé** [*Activé / Désactivé*] : paramètre seulement disponible si le **démarrage sécurisé est activé.** Si cette propriété est "*Activé*", les données transmises à travers des connexions de tunnel, seront sécurisées, c'est à dire, l'information sera chiffrée par le moyen IP. Chaque adresse de tunnel aura son propre mot de passe.

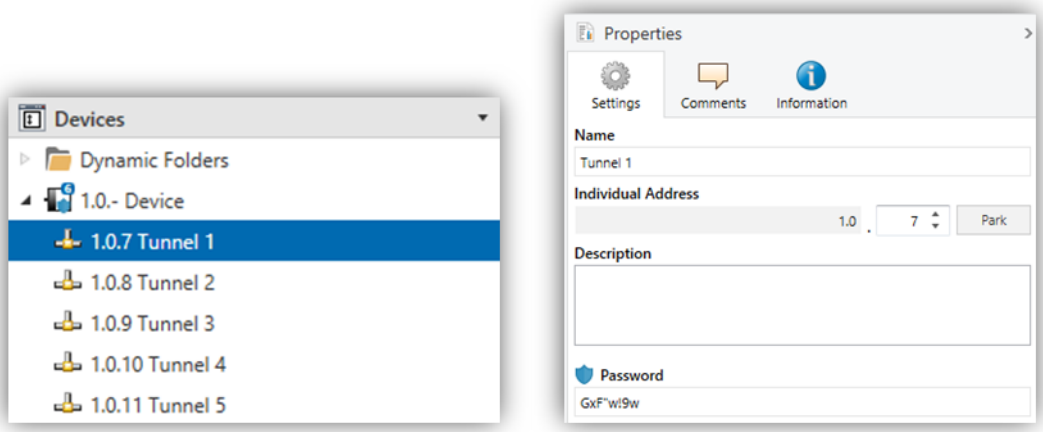


Figure 11. Mot de passe de l'adresse de tunnel.

L'onglet "IP" contient le **Mot de passe de démarrage** et **Code d'authentification**, nécessaires pour réaliser n'importe quelle connexion sécurisée avec le dispositif.

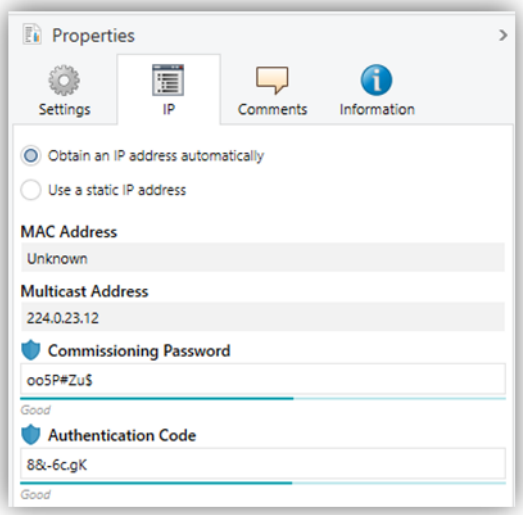


Figure 12. Mot de passe de la mise en marche et Code d'authentification.

Important : *Il est recommandé que le code d'authentification de chaque dispositif soit individuel (et de préférence celui établie par défaut sur ETS).*

Le mot de passe de démarrage sera demandé à sélectionner l'interface IP sur ETS pour se connecter (le code d'authentification est optionnel) :

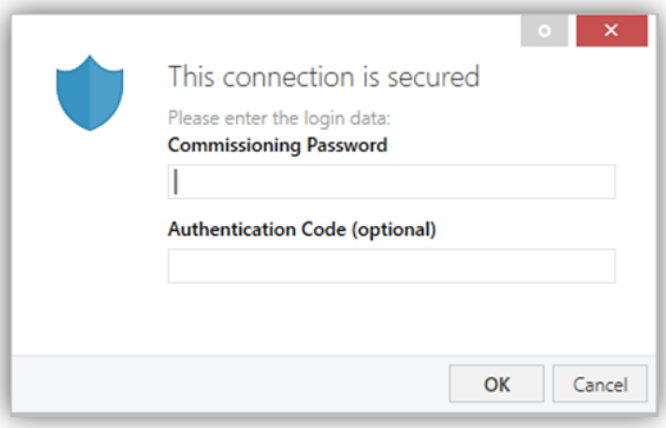


Figure 13. Pétition de mot de passe démarrage à sélectionner une interface IP sécurisée.

3 REDÉMARRAGE D'USINE

Comme mesure pour ne pas laisser un dispositif hors d'usage, dans le cas de perte du projet et/ou de la clé (*Tool Key)* avec laquelle il a été programmé, il est possible de revenir à l'état d'usine en réinitialisant la clé FDSK au moyen des pas suivants.

1. Mettre le dispositif en mode sûr. Ceci se réalise en l'alimentant avec le bouton de programmation enfoncé jusqu'à ce que l'on voie la LED de programmation clignoter.
2. On relâche le bouton de programmation. Voir qu'il continue à clignoter
3. On réalise un appui de 10 secondes sur le bouton de programmation. Pendant l'appui le bouton restera allumé en rouge. Il s'observera le redémarrage lorsque la led s'éteint momentanément.

Ce processus, à part du ***Tool Key***, efface aussi le ***mot de passe BCU*** et restaure l'adresse individuelle à la valeur 15.15.255.

Une déprogrammation du programme d'application efface aussi le *Tool Key* et le mot de passe BCU, bien que dans ce cas il est nécessaire d'avoir le projet ETS avec lequel il a été programmé pour pouvoir le réaliser.

4 OBSERVATIONS

Quelques considérations pour l'utilisation de sécurité KNX :

- **Changement d'adresse individuelle** : sur un projet avec plusieurs dispositifs sécurisés déjà programmés qui partagent des adresses de groupe entres elles, la modification de l'adresse individuelle de l'un d'eux obligent à reprogrammer le reste des dispositifs qui partagent avec lui des adresses de groupe.

- **Programmation d'un dispositif réinitialisé** : a essayer de programmer un dispositif en le réinitialisant aux valeurs de fabrique, ETS détecte qu'il s'utilise le *FDSK* et demande la confirmation pour générer une nouvelle *Clé d'outil* pour pouvoir reprogrammer le dispositif.

- **Dispositif programmé sur un autre projet :** Si on essaye de télécharger un dispositif (de manière sécurisée ou non) qui a déjà été programmé en toute sécurité dans un autre projet, le téléchargement échouera. Il faudra récupérer le projet original ou réaliser une réinitialisation d'usine.

- **Mot de passe de la BCU** : ce mot de passe est perdu à la fois avec une réinitialisation manuelle des paramètres de fabrique et avec une déprogrammation.

Venez poser vos questions
sur les dispositifs Zennio :
https://support.zennio.com

Zennio Avance y Tecnología S.L.
C/ Río Jarama, 132. Nave P-8.11
45007 Toledo. Espagne

Tél.: +33 (0)1 76 54 09 27 et +34 925 232 002.

www.zennio.fr
info@zennio.fr