IPR/S 3.5.1: Secure Commissioning
Three terms about KNX IP Secure

Doc.-Type:	Step-by-Step Guide	Doc.-Nr.	9AKK107492A6838	Revision:	A
Department:	BA Engineering	Author:	Engineering Team BA/DESTO		
System:	i-bus® KNX	Product:	IPR/S 3.5.1		
Page:	1/7	Date:	23 April 2020		

Liability Disclaimer:

This document serves the sole purpose of providing additional, technical information and possible application and use cases for the contained products and solutions. It **does not** replace the necessary technical documentation required for planning, installation and commissioning of the product. Technical details are subject to change without notice.

Despite checking that the contents of this document are consistent with the current versions of the related hard and software of the products mentioned within, deviations cannot be completely excluded. We therefore assume no liability for correctness. Necessary corrections will be introduced as and when new versions of the document are generated.

Introduction

With the new ABB i-bus® IP Router Secure IPR/S 3.5.1 devices, a distinction is made between three different “Secure” terms: Secure Commissioning, Secure Tunneling and Backbone IP Secure. Every system integrator will encounter them when commissioning the Router.

Objectives of the document

- Providing a simple representation and explanation of these three terms, and particularly the handling within ETS.
- Providing practical commissioning tips and tricks for technical support.

Content

1. Secure Commissioning

The IPR/S 3.5.1 supports the KNXnet/IP Security protocol and therefore can be commissioned securely, see Fig. 1. After a device from the product catalog has been added to ETS, the IPR/S 3.5.1 will automatically be activated with Secure Commissioning by default. However, if a device with a deactivated setting is copied, for example, this property will be copied as well.

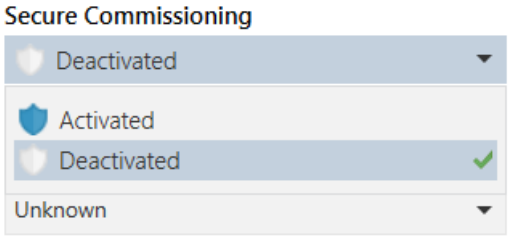

Fig. 1: Secure Commissioning setting

When “Secure Commissioning” is activated, the device will be commissioned with encrypted telegrams. It will not be possible to draw conclusions about the device parameter setting by reading the telegram traffic. For a start, this setting ensures secure communication between the IPR/S 3.5.1 and ETS during the commissioning phase (FDSK and serial number → first download).

Note: It is advisable to follow the order of commissioning when using IPR/S 3.5.1. It is best always to commission from “close” to “remote.” In other words, the interfaces close to the IPR/S 3.5.1 should be commissioned first. The reason for this is that setting the remote IP Router to “Secure” first will block access to this Router and to all devices behind it. This is due to the **local** IP Router not using a Backbone Key yet and therefore no longer being able to reach the **remote** IP Router via multicast routing.
The same thing applies if the multicast routing address is changed.

2. Secure Tunneling

When “Secure Commissioning” is activated, the “Secure Tunneling” field additionally appears in the ETS Properties window of the IP Router Secure (see Fig. 2). It is used for secure communication between a visualization system and the Router, for example.

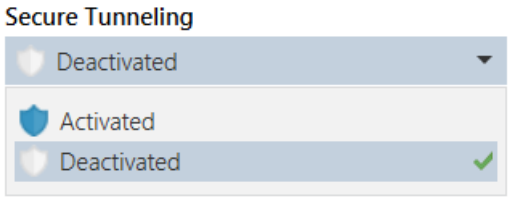

Fig. 2: Secure Tunneling setting

When “Secure Tunneling” is activated, all available tunneling servers (parked or not) will receive their own passwords created by ETS (see Fig. 3). The password can be changed in the Properties window of the respective tunneling interface.

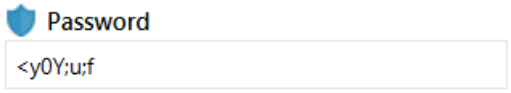

Fig. 3: Password for tunneling interface

Important: Each password can be adapted individually without restriction. Furthermore, up to five identical passwords can be assigned for five tunneling interfaces. They can be found on the “Project Security” tab in the ETS Reports function (see Figs. 4 and 5).

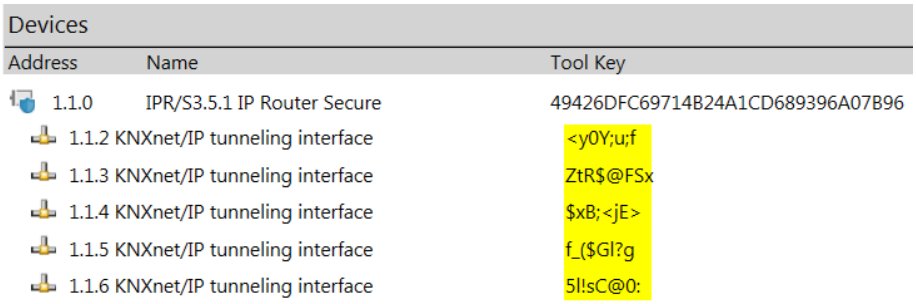

Fig. 4: Tunneling passwords, ETS variation

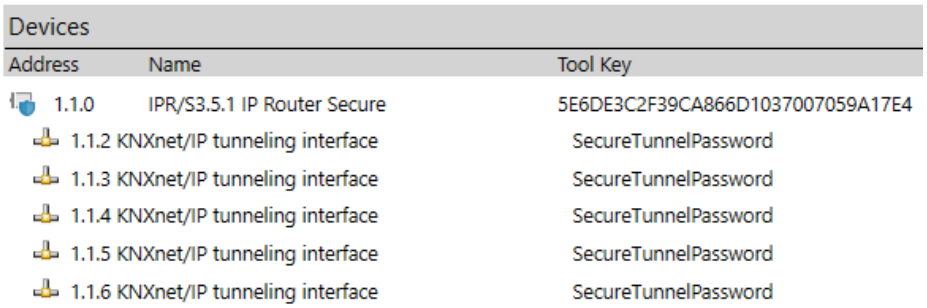

Fig. 5: Adapted tunneling passwords

3. IP Secure backbone

In a topology with traditional IP Routers, the IP backbone is always unsecured and appears as follows in ETS (see Fig. 6). It can be found under the “Topology Backbone” button in the Topology window in ETS. Simply left-click it.

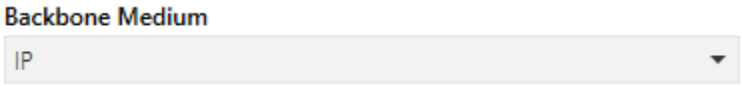

Fig. 6: Backbone Medium without Secure

Once all IPR/S 3.5.1 devices are set to KNX Secure mode, the IP backbone is also Secure (see Fig. 7).

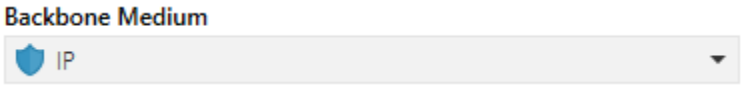

Fig. 7: Backbone Medium with Secure

A shared security key (Backbone Key) is assigned for all IP Router Secure devices in the background. However, this key is not immediately visible in the ETS interface. It can be found under “Project Security” in the ETS Reports function; see Fig. 8.

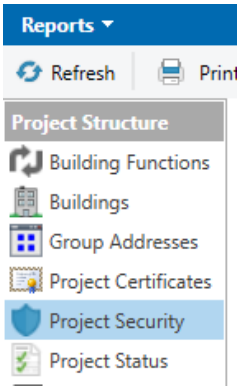

Fig. 8: Project Security report

This key is used for secure multicast communication. The key will then be loaded into the device when the Router is commissioned. Therefore, all devices can communicate with each other via an encrypted backbone only after all devices involved in the backbone have been fully commissioned.

4. Exceptions with IPR/S 3.1.1 and IPR/S 3.5.1

First of all, it is worth knowing that the default security setting in an ETS project is “Automatic” (see Fig. 9). This mode has far-reaching effects on the device security of the IP Router Secure. In other words, when an IP Router Secure is added, there initially will be no apparent difference compared to a normal IP Router (IPR/S 3.1.1). This is because the Router in question is also added to the ETS project with the non-secure setting by default.

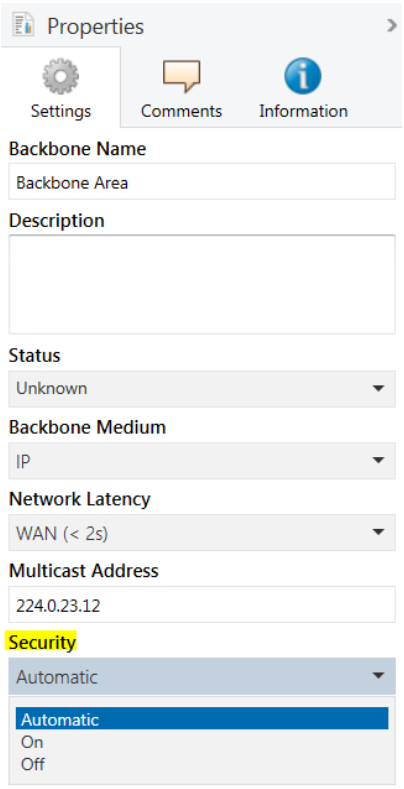

Fig. 9: Backbone area security setting

In the “On” setting, a project password must be assigned when an IPR/S 3.5.1 or KNX IP Secure device is added to an empty project. Additionally, for example, it will then no longer be possible to add an IPR/S 3.1.1 to the ETS project because it is not an IP Secure device (see Fig. 10).

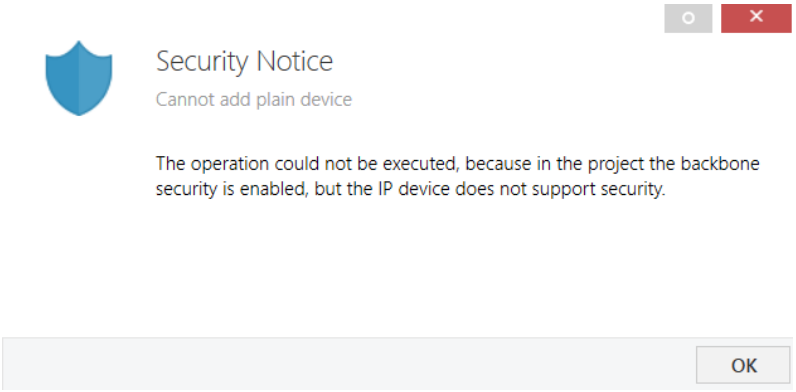

Fig. 10: Security setting “On”

The situation is exactly the opposite in the “Off” setting. Devices will not be operated securely despite available IP Secure technology. A special case would be an existing project with a mixed device configuration (IPR/S 3.5.1 and IPR/S 3.1.1). The following message would appear in ETS during switchover to “On” in this case (see Fig. 11).

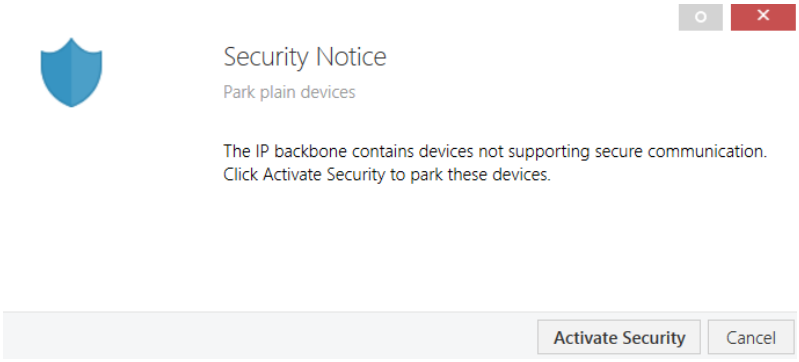

Fig. 11: Security setting change

Another example would be an existing project with one or more IPR/S 3.5.1 devices (Secure mode). If the setting is now changed from “Automatic” to “Off,” the following message will appear and the IP backbone will lose the “Secure” setting. In other words, the blue shield will no longer be visible in ETS (Fig. 6).

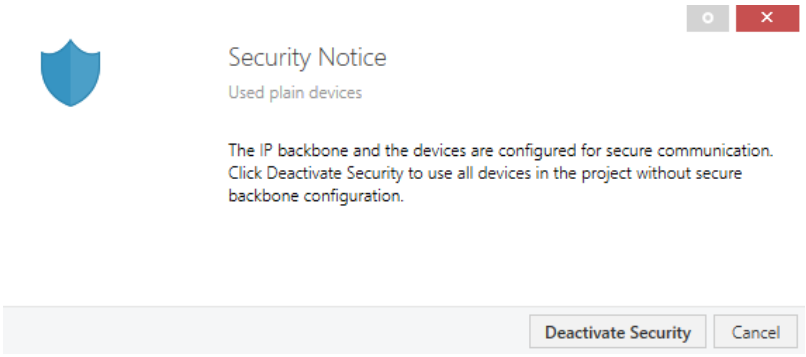

Fig. 12: Change from “Automatic” to “Off”

The following combination is the final exception: IPR/S 3.5.1 (Secure mode) and secure backbone. When an IPR/S 3.1.1 is added to the project, the following message will appear with the “Automatic” security setting. Here too, the backbone will then no longer be secure.

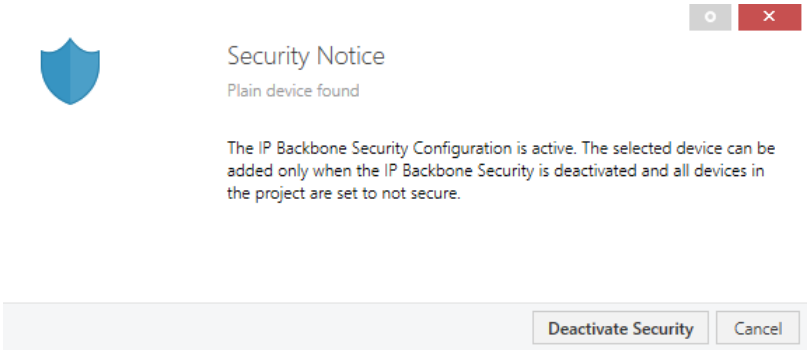

Fig. 13: IPR/S 3.1.1 import

References to other documents

- FAQ Home and Building Automation
- Engineering Guide Database