

REPORT

KNX project file

Office building, sample

This report summarises what the submitted project file says about protection and documentation of the installation. All findings describe the state of the project file. The actions on page 5 are sorted by urgency.

Site	Office building, 1 Sample Street, 1234 Sampletown
Client	Sample Electrical Ltd.
File	sample_office.knxproj, exported with ETS 6
Project state	last modified on 02 Sep 2026
Scope	186 devices · 1,240 group addresses · 4 lines
Report created	14 Oct 2026

2

CHECK

4

NOTES

3

OK

6

ACTIONS

At a glance

OK

Project file is password protected.

CHECK

No BCU key stored in the project.

The KNX Association recommends one for every finished project. Details on page 3.

CHECK

KNX IP Secure switched off according to the project.

IP interface 1.0.1 is Secure-capable, the function is not enabled in the project.

NOTE

2 devices with pending download.

ACTION

Six actions, sorted by urgency, on page 5.

FINDINGS

All findings in detail

We assess what is documented in the project file. The electrical contractor checks it against the installation.

CHECK

F1 · No BCU key stored in the project.

The “BCU key” field in the project details is empty. Whether individual devices in the installation are protected cannot be determined from the file. Details on page 3.

CHECK

F2 · KNX IP Secure switched off according to the project.

According to the manufacturer data, IP interface 1.0.1 is Secure-capable; security for IP communication is set to “Off” in the project. Before enabling it, check whether visualisation, remote access and smart home servers support Secure.

NOTE

F3 · 2 devices with pending download, 2.1.12 and 2.2.5.

Parameters were changed in the project but, according to the project, not yet downloaded to the devices.

NOTE

F4 · 14 group addresses without names, e.g. 1/2/14 and 1/2/15.

Named in ETS within minutes. Makes every later fault search easier.

NOTE

F5 · 9 group addresses without datapoint type.

Without a datapoint type, visualisations and smart home servers cannot read the values correctly by themselves.

NOTE

F6 · 3 devices without room assignment: 1.1.23, 1.1.24 and 2.1.7.

OK

F7 · Project file is password protected.

Device configuration and stored keys cannot be read without the password.

OK

F8 · Building structure maintained.

38 rooms created, 183 of 186 devices assigned.

OK

F9 · Project information maintained.

Installer, project number and revision are filled in.

What the project file does not show

Whether the installation can be reached from the internet is not in the file. The free KNX Security Check (securitycheck.knx.org) shows this when run from the installation's network.

FINDING F1

BCU key: whoever sets it controls the devices.

The BCU key is a password for KNX devices. Once set, the devices can only be reprogrammed with this key. If none is set, anyone with access to the bus can set one and lock everyone else out, including the installer.

What the project file says

"BCU key" field in the project details	empty
Devices in the project	186
fully downloaded according to the project	184
Whether devices in the installation are protected	cannot be determined from the file

Why it matters

In October 2021, attackers unloaded the KNX devices in a building in Germany over the internet and set an unknown BCU key. Around three quarters of several hundred devices stopped working. According to Limes Security, a replacement would have cost over €100,000. In July 2026, the US agency CISA listed the underlying vulnerability CVE-2023-4346 as actively exploited.

Recommendation

- Set a BCU key in the project details and download it again to all devices that support it. Only then is it effective in the installation. The KNX Association recommends this for every finished project.
- Hand the key over to the owner with the project documentation and keep it safe. If it is lost, the devices can usually no longer be reprogrammed.
- In addition: no direct access to the installation from the internet, remote access only via VPN.

Sources: Limes Security, KNXlock (limessecurity.com/en/knxlock) · CISA Advisory ICSA-23-236-01 · CISA Known Exploited Vulnerabilities, entry of 15 Jul 2026 · KNX Support, article "BCU Key"

DEVICE LIST

Devices by room and manufacturer

Excerpt, 13 of 186 devices. The full list is attached to the report as CSV. Manufacturer names are anonymised in this sample.

FLOOR	ROOM	ADDRESS	DEVICE	MANUFACTURER	DOWNLOAD STATE PER PROJECT
Ground floor	GF.01 Reception	1.1.1	Switch actuator, 12-fold	Manufacturer A	downloaded
Ground floor	GF.01 Reception	1.1.2	Push-button interface, 4-fold	Manufacturer B	downloaded
Ground floor	GF.02 Meeting	1.1.5	Presence detector	Manufacturer C	downloaded
Ground floor	GF.02 Meeting	1.1.6	Blind actuator, 8-fold	Manufacturer A	downloaded
Ground floor	Plant room	1.0.1	IP interface, Secure-capable	Manufacturer D	downloaded
Ground floor	Plant room	1.1.0	Power supply 640 mA	Manufacturer A	no application
1st floor	1F.04 Office	2.1.3	Dimming actuator, 4-fold	Manufacturer B	downloaded
1st floor	1F.04 Office	2.1.12	Room temperature controller	Manufacturer C	download pending
1st floor	1F.06 Office	2.1.9	Heating actuator, 6-fold	Manufacturer A	downloaded
Roof	Plant room	2.2.5	Weather station	Manufacturer D	download pending
no room	—	1.1.23	Binary input, 4-fold	Manufacturer B	downloaded
no room	—	1.1.24	Switch actuator, 4-fold	Manufacturer A	downloaded
no room	—	2.1.7	Logic module	Manufacturer C	downloaded

4

MANUFACTURERS

38

ROOMS

2

DOWNLOAD PENDING

3

NO ROOM

ACTIONS

Six actions, sorted by urgency

Times are guide values for an experienced electrical contractor and depend on the installation.

NO.	PRIORITY	ACTION	FINDING	EFFORT
1	HIGH	Set a BCU key in the project details, download it to all supporting devices, document the key.	F1	on site or via secure remote access, ½ to 1 working day
2	HIGH	Enable KNX IP Secure for interface 1.0.1. Check beforehand that visualisation, remote access and smart home servers support Secure.	F2	approx. 1 to 2 hours
3	HIGH	Check internet exposure: run the KNX Security Check from the installation's network, remote access only via VPN.	Page 2	approx. 15 minutes
4	MEDIUM	Carry out the pending downloads for 2.1.12 and 2.2.5 or clarify the changes.	F3	approx. 15 minutes
5	MEDIUM	Hand over project file, project password and BCU key to the owner and record the handover.	F1, F7	approx. 30 minutes
6	LOW	Complete the documentation: name 14 group addresses, set 9 datapoint types, assign 3 devices to rooms.	F4 to F6	in the office, approx. 45 minutes

What this report is made for

This report is based solely on the submitted ETS project file at the time of export. It is not an inspection of the real installation, not an expert opinion and not a safety acceptance. The project file and the installation may differ.

Work on the installation is carried out by authorised contractors. The project file is deleted no later than 14 days after delivery; the project password is not stored.

Analysed with LIMITLESS Automation software

Reviewed by an electrician, LIMITLESS Automation