

Gira KNX IP router v4 'Secure'

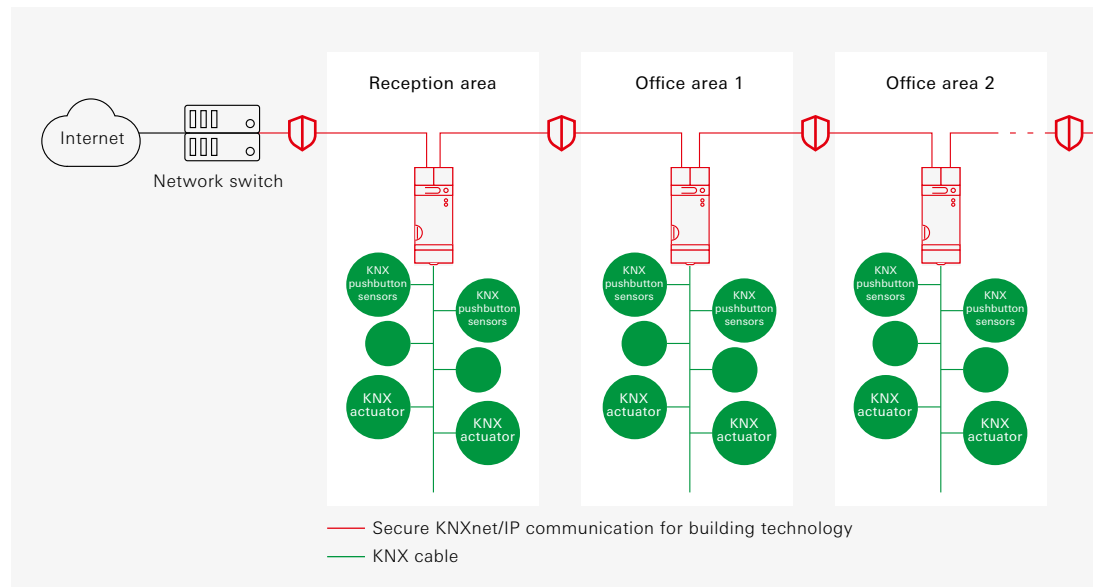
Opting for more security in building automation



Security in building automation redefined



Security is becoming increasingly important, particularly in large or public buildings, such as hotels, offices, schools and residential complexes. Attackers often exploit weaknesses in the network infrastructure. Attacks usually take place not from outside but from inside the building – e.g. via WLAN in hotel rooms. Because building automation is also part of this infrastructure in modern buildings, operators can suffer considerable damage. Functioning as an interface between the building's network infrastructure and the building automation, the Gira KNX IP router v4 'Secure' is one of the first products available on the market that systematically closes this security loophole. This is based on the new KNX Secure Standard.



Both in private homes and in larger properties such as hotels and public buildings, it is important to be certain that only the right people are getting in. This is why the building is equipped with solid entry doors, for example. However, considerably greater security can be achieved if these doors are also equipped with high-quality locks, limiting access to authorised visitors who have a key. This prevents unauthorised persons from gaining access. The new Gira KNX IP router v4 'Secure' provides a similarly great increase in building automation security thanks to key security features such as its new encryption technology.

Clever protective measures offered by the Gira KNX IP router v4 'Secure'

An up-to-date solution

The Gira KNX IP router v4 'Secure' prevents what are known as "replay attacks", i.e. it prevents unauthorised parties from transmitting data telegrams repeatedly. Commands from what are initially correct data telegrams cannot be used again in an inappropriate manner. This means, for example, that a previously-recorded command to open a door cannot be triggered again.

Data integrity

The Gira KNX IP router v4 'Secure' prevents the data content of telegrams from being changed or tampered with. This means, for example, that telegrams cannot be changed, infiltrated or sent without authorisation.

Authentication

The Gira KNX IP router v4 'Secure' ensures that the partner with whom communication is performed and data are exchanged is the correct one. Attackers do not gain access to the building automation.

Encryption

The Gira KNX IP router v4 'Secure' reliably encrypts the communication. It prevents the content of KNX telegrams from being visible. This means, for example, that configuration data cannot be read during commissioning.

The new functions of the Gira KNX IP router v4 'Secure'

- **Additional password protection**

Thanks to additional password protection, access to the diagnostic page of the Gira KNX IP router v4 'Secure' is now restricted to authorised users only.

- **Data logger with remote access**

Since the first generation, the Gira KNX IP router has offered the option of recording telegram traffic on an SD card and using it for error analysis. Unattended recording means, a PC with an ETS does not need to remain in the system. The Gira KNX IP router v4 'Secure' now makes it possible to load the data stored on the SD card via the device diagnostic page. This means that it is no longer necessary for the SD card to be removed on site; network access and the password are enough. Remote access to these data is even possible in combination with the Gira S1.

- **Expanded filter options**

The Gira KNX IP router v4 'Secure' has an expanded filter function. This means that the functions "filter", "forward unfiltered" and "block" are now also available for extended group telegrams in main group 14–31. This minimises the telegram load and facilitates efficient management of the KNX installation.

- **Clear overview in the ETS product database**
The new Gira KNX IP router v4 'Secure' ensures rapid and trouble-free start-up with enhanced clarity in the ETS product database. Functions that are not needed can simply be hidden.

- **4 KNXnet/IP tunnelling interfaces**

The Gira KNX IP router v4 'Secure' supports up to 4 KNXnet/IP tunnelling connections and thus enables parallel bus access, e.g. via the ETS and other PC software. When combined with KNX Secure, each of these tunnelling connections can be protected with an individual password.

- **Update capability**

Thanks to the fact that the Gira KNX IP router can be updated, even devices that are already installed can benefit from the new functions in the ETS product database, in the data logger and on the device diagnostic page. This means that the functions described here can be used on many existing Gira KNX IP routers 2167 00. The existing additional functions of "KNX clock" via NTP and "data logger" will, of course, continue to be available. KNX Secure can be downloaded onto Gira KNX IP routers from index status I14.



A special function of the Gira KNX IP router v4 'Secure' is its reliable communication over WLAN. Even in systems in which the KNX communication is to be transmitted via WLAN, this additional mechanism ensures that all commands are executed reliably and minimises data loss through potentially unreliable connections.



Easy installation and expansion

The Gira KNX IP router v4 'Secure' has an especially compact DRA design with just two modular widths. The integrated network switch is particularly beneficial, facilitating easy "looping" of the network line ("daisy chain"). Only one data line for the network needs to be installed in the distributor for several network devices, reducing installation costs and saving time. Both network sockets are located under the distributor cover plate, and are therefore protected against unauthorised or accidental unplugging.

Gira
Giersiepen GmbH & Co. KG
Electrical installation systems

Industriegebiet Mermbach
Dahlienstrasse
42477 Radevormwald

PO Box 12 20
42461 Radevormwald

Germany

Phone +49 2195 602-0
Fax +49 2195 602-191

www.gira.de
info@gira.com

Follow the Gira community on
Facebook, Twitter, YouTube or
Instagram.
For more information, please
visit:
www.gira.com/socialmedia



Lithography:
vimago GmbH,
Oberhausen

Picture credits:
Haus&Gross

Technical data

Gira KNX IP router v4 'Secure'

- KNX medium: KNXnet/IP and TP1-256
- Rated voltage: DC 24 to 30 V
- IP communication: Ethernet 10/100 BaseT (10/100 Mbit/s)
- Supported protocols: ARP, ICMP, IGMP, DHCP, AutoIP, UDP/IP (Core, Routing, Tunnelling, Device Management)
- microSD card: up to 32 GB

Connections

- IP: Pin jack RJ45
- KNX: Connection and junction terminal
- Ambient temperature: 0°C to +45°C

Notes

- Supply via external DC 24 V.
- The Gira Project Assistant (GPA) is required for firmware updates. The GPA is available free of charge in the Gira download area.

Included contents

- microSD card not included in delivery.

Prerequisites for KNX Secure systems

Hardware:

- KNX IP router from Index Standard I15
- KNX IP router from Index Standard I14 with firmware update

Software:

- ETS from Version 5.6.6
- ETS product database for router: 4.0
- ETS product database for router (additional function): 4.0