

Transmitter Fibra

Module for integrating one third-party wired detector into an Ajax system

Tiny gear to boost regular into Ajax

Transmitter Fibra serves two primary purposes: first, to connect functional third-party devices to the Ajax system, enhancing their capabilities; and second, to connect specific devices not yet included in the Ajax portfolio. Transmitter Fibra can be easily installed with any third-party device. The module supports all connection types, including 3EOL, provides numerous event types for the connected device, can be remotely configured, and regularly reports its state to the hub.

Key features

Any connection type with NO, NC, EOL, 2EOL or 3EOL connection	Instant detection of wired device connection loss ¹	KeyArm feature for integrated third-party device	Numerous event types for the integrated device Intrusion Panic button Fire
Fast connection to wired devices by measurement of EOL resistors	Convenient wire connection due to accessory 5-pin cable	Remote control and configuration	Chime ³ for shops, commercial and non-commercial facilities
Compliance Grade 3 (EN 50131) PD 6662:2017	Installation inside the device enclosure	Integration of roller shutter motion detector	12 V ⁼⁼ , 50 mA power supply for the integrated device
Up to 2,000 m range of communication ² with an Ajax hub or a module that extends the Fibra line	Informative in-app notifications Production: gas detected, Transmitter Fibra in Workshop No. 1 Office: alarm detected, Transmitter Fibra in Hall No. 1	Low power consumption	Fibra wired communication Two-way communication TDMA Encryption Protection against spoofing Short circuit detection

Compatible hubs

- Hub Hybrid (2G)
- Hub Hybrid (4G)

This is the wired device of the **Fibra product line**. Only accredited Ajax Systems partners can sell, install, and administer Fibra products.

Turns outdated into innovative

After integrating a third-party device via Transmitter, this device can be managed and configured remotely. PRO's will get remote settings management and scenario setup; end-users will receive push notifications and have in-app security management. This will breathe new life into the devices already installed at the facility or enhance the functionality of new third-party devices that need integration into the Ajax system. The best Ajax user experience will be extended to third-party devices in both directions.

Ajax experience for third-party devices

Roller shutter motion detectors, IR detectors, household gas sensors, thermostats, float sensors, and other devices are ready to expand the Ajax areas of use. Connect them to a hub via Transmitter and manage the combined solution in the Ajax app.

Moreover, alarms or other events from connected devices can be used as automation triggers. Nothing stops to set up a custom automation scenario. Automation scenarios are intended to enhance security or to automate a routine. Their triggering can be alarms or service events – an ideal solution for security and automation.

Versatile security management with KeyArm

A third-party keypad or others access control devices can be connected to the Ajax system. This opens up almost unlimited integration, renovation, and system management possibilities. Thus, the user will be able to control the security of the entire facility, night mode, or even individual groups using a third-party device.

An EOL connection can be used to lock the security management when the tamper of a third-party device is triggered. Only a verified user with the appropriate rights can unlock. This will make it almost impossible to sabotage the system.

- Integration of third-party access control devices
- Management of different security modes: entire facility, night mode, separate groups
- Control locking in case of sabotage

Compatible with any third-party device

Transmitter Fibra can handle almost any third-party device. Due to its small size, the module can fit into the enclosure of most devices. Transmitter supports NC, NO, EOL, 2EOL, and 3EOL connection types. It operates with pulse and bistable devices. Also it has the function of choosing a normal contact state and supports numerous event types for the connected device. The module has two inputs (Z1 and Z2), which allows connecting one device by the AATT scheme or two devices simultaneously. Transmitter also can provide a 12 V_{DC} power supply for the connected device, which is a standard for most solutions on the market.

- Wide range of compatible devices: from NC/NO to 3EOL
- Pulse and bistable operation for any of the device sensors
- Selects the NO or NC state for any of the device sensors

Security via smartphone and PC

With Transmitter, system users get security control via app, data-rich notifications, and automation scenarios. An installer can set up the system or device in the PRO-app, both while on-site and remotely. And for monitoring companies, we provide free software for monitoring all events and alarms in Ajax systems.

For users		For PRO's	
iOS	Android	iOS	Android
		macOS	Windows

Data-rich alarms and events

With Transmitter, you can specify the device name, the type of alarm, and a room for a connected wired device. This makes notifications more informative – you know what happened and where. This information is displayed using push notifications and SMS and sent to the security company's monitoring station. Numerous types of alarms are available: intrusion, fire, auxiliary alarm, panic button, gas alarm, tamper alarm, malfunction, leakage, custom, and roller shutter alarm etc. Transmitter also notifies about its and the connected device's faults if they occur. For example, if the connection is lost.

- Sends all important information to users and to the hub
- 10 Numerous event types for the connected device
- Notifications about events of the Transmitter and connected device

Less hassle with automated security

With Transmitter, even an old third-party device becomes part of a safe and smart home. An integrated device's alarms or events can trigger automation scenarios. Use automation scenarios so that the security system instantly responds to threats without waiting for response group or police. Ajax will turn on the light upon the motion detector alarm, switch off potential ignition sources at the first sign of fire, or close the roller shutter and gate in case of an attempt to break the front door.

Unique wired technology

An Ajax system uses secure two-way communication based on **Fibra proprietary protocol**. It features **encryption** and **device authentication** to prevent sabotage, spoofing, and data theft. Fibra lines are **versatile** and support connecting different types of devices to one line: sirens, keypads, and detectors with photo verification.

- Up to 2,000 m of wired communication with a hub
- One line for different types of devices
- Photo delivery via Fibra line without interference
- Protection against sabotage and spoofing

Sabotage resistance

Instant detection of short circuits or breakage of connected device Due to EOL connections support, the Transmitter can instantly detect a breakage or short circuit on the cables between alarm zones of the Transmitter and the connected device. Additionally, the Transmitter detects short circuits of the power supply line of a third-party device. Therefore, every sabotage effort will be noticed.	Anti-sabotage detection of connected device The Transmitter supports all connection types from NC/NO to 3EOL and identifies all events of the connected device. Therefore, users and the CMS are immediately notified in case of tamper alarm, masking, or any other malfunction or sabotage attempts.
Protection against short circuits Fibra protocol and a special digital algorithm provide reliable protection against unnoticed short-circuiting of the module or Fibra line. If someone tries to short-circuit it, it notifies of a malfunction. Hub informs both the Central Monitoring Station (CMS) and users about the incident.	Communication failure detection The Transmitter regularly exchanges data with the hub. With minimal polling settings (3 data packages in 12 seconds), it takes 36 seconds to identify communication loss and notify the security company and users about the incident.
Encryption of transmitted between Transmitter and hub data All data the system stores and transmits is protected by block encryption with a dynamic key. Encryption makes it extremely difficult to connect to the module with the intention of sabotage.	Event notifications The monitoring station instantly receives notifications on events. The information includes time, device type and name, event type, and location room ⁴ .

Enhanced security for wired devices with LineProtect Fibra

LineProtect is a module to protect the Fibra line and devices from electrical sabotage. If an intruder tries to damage the security system and, for example, hits the StreetSiren Fibra with a stun gun, LineProtect will take the hit. All devices between LineProtect and the hub will continue to operate.

PRO is king

The myth that wired systems are difficult to install has been busted. Ajax has transformed what used to be an expensive, lengthy, and dusty experience for PROs by developing an ultimate set of tools to make the process easy and flexible, from project design to client support and system maintenance. Intuitive Ajax apps ensure the device can be integrated into the system quickly, and each device can be reconfigured remotely without the need for site visits.

Fibra power supply calculator

Use our online calculator to ensure the Fibra system covers your facility. It helps verify the project of a wired security system and provides additional information for installers.

Installation

The Transmitter Fibra is installed in the enclosure of a third-party device. The device has the smallest possible size and a accessory 5-pin cable for convenient connection of third-party device. There is no need to measure the EOL resistances of the resistors - the Transmitter can read them and memorize them to the settings.

- Smallest module dimensions for installation in any device enclosure
- Accessory 5-pin cable for connecting an third-party device - for easier installation
- Tool for automatic scanning of EOL resistors

Setup

Installers can add a Transmitter in two ways: by automatically scanning lines or scanning a QR code. When scanning lines, they can identify the desired device either by clicking in the app or by triggering the connected device. Once a device is added by an installer, it immediately has a default name and settings suitable for most cases.

- Pairing with a hub via line scanning or QR code
- Device identification via triggering
- Optimal default settings

Configuration

Forget about configuring via the keyboard.

All testing and configuration can be done in mobile and desktop Ajax apps. An installer can work both on behalf of the company and as a sole installer.

- Configuration and testing remotely and on-site
- Desktop and mobile apps
- Accounts for companies and installers

Monitoring

Using proprietary protocols, any Ajax system can transmit alarms to the PRO Desktop monitoring app and third-party CMS. When an alarm is received, the monitoring station operator knows what happened and where to send the rapid response unit. All Ajax devices are addressable, allowing the transmission of events, device type, assigned name, and room to PRO Desktop or third-party monitoring software.

- Fully addressability of the device
- Instant notifications in Ajax apps
- Alarm and event monitoring in PRO Desktop for monitoring companies

1 – Valid for EOL, 2EOL or 3EOL connections.

2 – With U/UTP cat.5 4×2×0.51 cable. Other cable types may have different values. Please use **Fibra power supply calculator** to check the wired system project before installation.

3 – The Chime feature requires the siren to operate. It functions like a shopkeeper's bell: when the system is disarmed, the sirens alert users of a door opening.

4 – The list of transmitted parameters may differ depending on the type of the CMS and the selected communication protocol.