Superior KeyPad Outdoor Fibra

Wired keypad supporting authentication via Pass, Tag, smartphones, and codes. For outdoor and indoor use.

Control your space, rain or shine

Meet the all-weather key to security and automation. Control security modes, activate Night Mode, manage specific groups, and run scenarios with one keypad. Use classic passcodes or go contactless. The ultra-narrow enclosure fits anywhere and still has big, glove-friendly mechanical buttons with sleek feedback. The durable enclosure is built to withstand any operating conditions and maintain full functionality even after being hit or physically damaged. Uncompromisingly secure keypad that gives intruders a hard time to hack it open.

Key features

Support for contactless access devices Pass cards and Tag key fobs featuring DESFire® technology	**Duress codes** when a user is forced to disarm a system	**Four types of access codes** • main keypad code • personal codes • codes for unregistered users • RRU code	**Big mechanical buttons** sleek feedback even if a user wearing gloves or mittens
Contactless control via smartphone using Bluetooth Low Energy (BLE)	**Two operating modes:** **Security** **Automation** easy mode switching with a long press of the OK button	**Passcode guessing protection**	**Bypass mode** the keypad starts an entry delay to confirm a security mode change
Built-in panic button	**IP66** protection against dust, water, and harsh temperatures	**IK08** protection against physical impacts	**Up to 2,000 m (6,550 ft) of wired communication[1]** with an Ajax hub or a module that extends a Fibra line
Fibra wired connection	**Remote control and configuration** **Ultra-low power consumption** **up to 0.6 W**	**Tamper alarm** enclosure has two tamper buttons	**60 dB buzzer for sound notifications** informs about alarms, security mode being changed, delay when entering/leaving, Chime, and other events
Connection with other Fibra devices on the line	**Informative push notifications** **Ajax** Home: Backyard armed by John **Ajax** Office: Night Mode activated by Ann	**Three colors of stainless steel enclosure**	**Compliance** Grade 3 (EN 50131) PD 6662:2017 ANSI/SIA CP-01-2019 INCERT SSF

In an Ajax system, you can combine devices of all product categories: **Intrusion protection** (both

Superior and Baseline), **Video surveillance**, **Fire and life safety**, or **Comfort and automation**. Create the system to suit your needs and manage it in a single interface.

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

Ready to withstand in any setting

Store	Warehouse	Office	Manufacturing	Private residence

Three missions, one device

Security management	**Automation device control**	**Sound and LED indication**
Easily manage the security of an entire site, separate groups, or activate Night Mode using just one device. It additionally features a Function button, which can be configured as a panic button or to mute fire alarms. Superior KeyPad Outdoor Fibra can also operate in bypass mode: it starts an entry delay for users to confirm the security mode change via the main keypad, for example, with another Ajax keypad installed inside the facility.	The keypad can control one or multiple automation devices, such as switches, relays, sockets, outlets, and shut-off valves. For example, a user can open garage doors and turn on outdoor lights when arriving home (or close the garage and turn the lights off when leaving). Just one press of an OK button will set a scenario in motion. The buttons' backlight indicates the automation device state[2]: red for off and green for on.	The glove-friendly keypad has backlit digits that do not fade. The built-in buzzer notifies you of alarms, doors being opened (**Chime**), arming/disarming, and entry/exit delays. The LED brightness and buzzer volume can be adjusted via Ajax apps.
• Security management of an entire site or separate groups • Night Mode activation • Bypass mode to start an entry delay to confirm a security mode change	• Control over one or multiple automation devices with OK button • Indication of an automation device state with backlight	• Sound notifications of alarms and events • Mechanical buttons with backlit digits that are not fading off • Adjustable sound volume and LED brightness

Fast and secure authentication

There are three easy ways to control the keypad, giving users the flexibility to choose what suits them best. Ajax apps display all events, including user activity and authentication details.

Pass card and Tag key fob

With Ajax Pass or Tag, the system can be armed or disarmed with one move of a hand: just present the access device to the keypad reader. Each use of a contactless access device is recorded in the Ajax app event feed. The admin can revoke, restrict, or temporarily suspend the access devices at any time. Administrators can also modify users rights by granting or limiting access to specific groups.

The keypad features DESFire® technology, a contactless solution for identifying a user by card or key fob. DESFire® is based on the ISO 14443 international standard and combines comprehensive 128-bit encryption and copy protection. This technology is also used in transportation systems of European capitals and access systems at NASA.

Smartphone

Get granted access rights by the system admin and pre-authorize your smartphone via Ajax apps for contactless control of the keypad using Bluetooth Low Energy (BLE).

BLE (Bluetooth Low Energy) is a radio protocol that allows a smartphone to control a keypad instead of access cards or key fobs. Data transmission between a smartphone and the keypad is encrypted. The system incorporates measures to prevent spoofing attacks, making it impossible for burglars to gain unauthorized access. Superior KeyPad Outdoor Fibra supports iOS and Android smartphones with BLE 4.2 or later.

Passcode

The keypad supports several types of access passcodes:

- **Keypad code (one per keypad)**: a general code set up for the keypad.
- **Personal codes**: individual access codes configured personally by each system user in their Ajax app.
- **Codes for unregistered users**: codes created by an admin for cleaning personnel or real estate agents who don't have Ajax accounts. They use the keypad but have no access to the system info.
- **RRU code**: the access code configured by an admin for the rapid response units (RRU) to access the premises after receiving an alarm when the owner is not home. The code is activated only after an alarm and is valid for a specified period.

Contactless access devices

Pass and Tag are equipped with original DESFire® chips and share the same functionality but in a different shape of enclosures. One Tag or Pass can control up to 13 security systems. Access devices are sold separately in batches of 3, 10, or 100 pieces.

Pass Contactless card to control security modes	Tag Contactless key fob to control security modes

Remote access control

Change access rights and codes in real time via the Ajax apps. Lost access devices and compromised codes can be remotely altered within minutes. An installer doesn't need to visit the facility.

- Remote code management
- Remote user access rights management
- Remote blocking of cards, key fobs, and smartphones

Access for unregistered users

With a simple assignment in the hub settings, a PRO can create a temporary access code for office employees, cleaning company staff, or other verified visitors.

- Notifications that the codes being added, removed, or deactivated
- The unique name and ID binding to identify the user
- Up to 99 codes for unregistered users

Ready to assist in emergencies

User notifies about emergency	System transmits an alarm	ARC calls a rapid response unit

The keypad has a panic button that triggers an alarm when pressed. The panic button can be configured to alert users about the alarm, activate sirens, or even run an automation scenario. If the user is forced to let in intruders, they can use a duress code to fake disarm: the keypad simulates regular disarming and immediately sends an alarm to the security company, notifying them about the emergency. Meanwhile, Ajax apps and sirens installed at the facility remain silent to prevent revealing a user.

- Panic button to trigger an alarm
- Duress code for fake disarming

Discover future-proof hardware

Weatherproof IP66 enclosure with IK08 impact protection
to withstand in any environment, even in rain, snow, or scorching sun
Big mechanical buttons
for easy and fast access, even in gloves or mittens
LED backlight
to indicate security modes, scenario execution, mode switching, and other keypad commands
DESFire® and BLE reader
for contactless access with Tag, Pass, or smartphones
60 dB buzzer
to inform about the alarms, security mode being changed, delay when entering/leaving, Chime, and other events
SmartBracket mounting panel
to install the keypad with no need to disassemble the enclosure
Removable terminal board
to simplify the wiring process
Two tamper buttons
to notify about attempts to detach the keypad from the surface or remove it from the mounting panel
Holding screw
to secure the keypad on a mounting panel

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 (6,550 ft) of wired communication[1] with a hub or a module that extends the Fibra line
- One line for different types of devices
- Photo delivery via Fibra line without interference
- Protection against sabotage and spoofing

Energy efficiency as a priority

Fibra communication requires minimum power consumption: the keypad consumes only up to 0.6 W at its peak. Fibra also follows the TDMA principle. Each device has a short time frame to exchange data with a hub, and its communication module is inactive the rest of the time. This significantly reduces power consumption and helps avoid interferences even when multiple devices communicate simultaneously.

- Power consumption of up to 0.6 W
- TDMA and power-saving modes

Advanced system supervision

The keypad is a part of the Ajax ecosystem, which makes it a genuine IoT device. Each element of the ecosystem is constantly supervised. The keypad exchanges data with a hub via Fibra protocol. The hub has two-way communication with Ajax Cloud which provides real-time information to Ajax apps. The Ajax system supervises device state every minute. If a keypad has an issue, you will receive a notification.

- IoT device
- Setting the ping interval in the hub settings
- Instant maintenance notifications

Tamper alarm The device enclosure has two tamper buttons to alert when the keypad is detached from the surface or removed from the mounting panel. Additionally, the keypad is secured with a holding screw at the bottom of the enclosure to enhance its resistance to any dismantling attempts.	**Protection against code guessing** The system blocks the keypad after three unsuccessful attempts for a specified period and immediately notifies about the incident, effectively preventing unauthorized individuals from guessing the access code.	**Protection against copying access devices** The keypad responds only to access devices authorized via Ajax apps. The DESFire® chips in cards and key fobs comply with the ISO 14443 international standard and combine comprehensive 128-bit encryption and copy protection. The BLE reader simply does not react on a smartphone if it's not authorized via Ajax apps.
Durable enclosure The keypad has IP66 protection and withstands temperatures from –25 °C to +60 °C (from −13 °F to 140 °F) . It works fine in rain and snow. Mechanical buttons are not fading, so it's impossible to figure out the most used digits and determine the code. The enclosure meets the requirements of the IK08 impact protection class and stays solid even if it was hit or physically damaged.	**Device authentication against spoofing** The hub checks the device's unique parameters for authentication during each communication session. If any parameter fails the check, the hub ignores commands from the device.	**Communication failure detection** The device regularly exchanges data with the hub. With maximum ping interval settings available (3 data packages once in 12 seconds), it takes only 36 seconds to identify communication loss and notify the security company and users about the incident.
Protection against short circuit The system instantly detects a short circuit on the line and notifies the security company and the users. And when the problem is fixed, there is no need to replace the fuses: the system will restore operation automatically.	**Data encryption** All data the system stores and transmits is protected by a block cipher with a dynamic key. Encryption makes it extremely difficult to reprogram the device, replace or steal the data.	**Informative push notifications** The Ajax system instantly notifies about alarms and events: a security company and users know exactly which device triggered, when and where it happened.
Regular polling The device regularly exchanges data with the hub. The system controls each device state and reports if there is a malfunction or connection loss.		

Next-level protection of Fibra line

Introducing Superior LineProtect Fibra, the module designed to protect an Ajax hub and connected wired devices from sabotage when intruders cause overvoltage, short circuits, apply 110/230 V~, or use stun guns.

PRO is king

The myth about wired systems being difficult to install is busted. Ajax minimized an expensive, long, 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. There is no need to disassemble the device for installation. Intuitive Ajax apps help quickly make the device a part of the system, and each device can be reconfigured remotely at any moment. No programming required — everything is available out of the box.

Fibra power supply calculator

The online tool provides security engineers with detailed data on device power consumption, enabling easy pre-installation assessment of the wired system project. It helps design the project in real time, highlights problem spots, and offers solutions. Upon completion, results can be downloaded as a PDF file.

Installation

With the SmartBracket mounting panel, an installer can effortlessly mount the device on the wall. The installation kit includes all the necessary fasteners. There is no need to disassemble the device: the board with terminals is placed outside the enclosure under SmartBracket to eliminate hardware damage during installation. The board is removable, which makes the whole process nice and easy. A built-in spirit level assists the professional in a perfectly accurate mounting position. For cable management, there are bracings inside SmartBracket to secure the wires with ties.

- No need to disassemble the device's enclosure
- Removable terminal board
- All the necessary fasteners included in the installation kit
- Holding screw to secure the device on a mounting panel

Setup

The device is paired with the hub automatically via Fibra line scanning. This tool is available in the desktop or mobile PRO apps. An installer only needs to name the device and assign it to the room and security group. The device can also be added by scanning the QR code or entering its ID manually.

- Pairing with a hub via automatic line scanning or QR code
- Device identification via triggering or LED indication
- Optimal default settings to cover major requests

Configuration

Intuitive Ajax apps provide remote set-up and testing with all device information from anywhere the Internet is available, on a smartphone or PC. An installer can remotely change the settings and provide services promptly without visiting the object.

- Configuration and testing remotely or on site
- iOS, Android, macOS, and Windows apps
- Accounts for companies and installers

Monitoring

An Ajax system transmits alarms to the **PRO Desktop** monitoring app or any third-party CMS. The security company receives an alarm notification in less than a second. Notifications include all the necessary information: name of the device, time of the event, and the exact room where the device is located. The security company also receives photo or video verification, capturing the reason for the alarm.

- Full addressability of connected devices
- Instant in-app notifications
- Alarm and event monitoring through the PRO Desktop app or third-party CMS

[1] Wired Ajax devices have a communication range of up to 2,000 m (6,550 ft) without line extenders when using the U/UTP cat.5 twisted pair cable. Other cable types may have different values. Please use the Fibra power supply calculator to check the wired system project before installation.

[2] When the keypad controls a scenario involving multiple automation devices, the OK button cannot display the state of the device or scenario with an LED indicator. Instead, the keypad will notify whether the set action is completed with a short buzzer beep.