KeyPad User Manual

Updated July 4, 2022

KeyPad is a wireless indoor touch-sensitive keyboard managing the Ajax security system. Designed for indoor use. With this device, the user can arm and disarm the system and see its security status. KeyPad is protected against attempts to guess the passcode and can raise a silent alarm when the passcode is entered under duress.

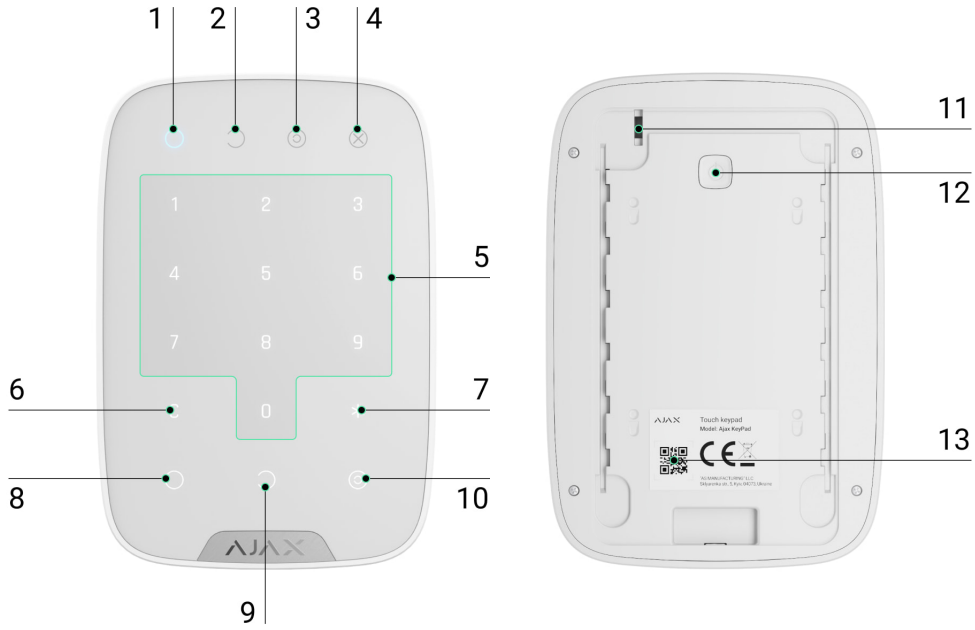
Connecting to the Ajax security system via a secured **Jeweller** radio protocol, KeyPad communicates with the **hub** at a distance of up to 1,700 m in line of sight.

KeyPad operates with Ajax hubs only and does not support connecting via ocBridge Plus or uartBridge integration modules.

The device is set up via the **Ajax apps** for iOS, Android, macOS, and Windows.

Buy keypad KeyPad

Functional elements



1. Armed mode indicator
2. Disarmed mode indicator
3. Night mode indicator
4. Malfunction indicator
5. The block of numerical buttons
6. “Clear” button
7. “Function” button
8. “Arm” button
9. “Disarm” button
10. “Night mode” button
11. Tamper button
12. On/Off button
13. QR code

To remove the SmartBracket panel, slide it down (perforated part is required for actuating the tamper in case of any attempt to tear off the device from the surface).

Operating Principle

KeyPad is a touch keypad for managing the Ajax security system. It controls the security modes of the entire object or individual groups and allows activating the **Night mode**. The keyboard supports the “silent alarm” function — the user informs the security company about being forced to disarm the security system, and is not exposed by the siren sounds or Ajax apps.

You can control the security modes with KeyPad using codes. Before entering the code, you should activate (“wake up”) the keypad by touching it. When it is activated, the button backlight is enabled, and the keypad beeps.

KeyPad supports code types as follows:

- **Keypad password** — set up for the keypad. When used, all events are delivered to Ajax apps on behalf of the keypad.
- **Personal password** — set up for users connected to the hub. When used, all events are delivered to Ajax apps on behalf of the user.
- **Keypad Access code** — set up for people who are not registered in the system. When used, events are delivered to Ajax apps with a name associated with this code.

The number of personal passwords and access codes depends on the hub model.

The brightness of the backlight and the volume of the keypad are adjusted in its **settings**. With the batteries discharged, the backlight turns on at the minimum level regardless of the settings.

If you do not touch the keypad for 4 seconds, KeyPad reduces the brightness of the backlight, and 8 seconds later goes into power-saving mode and turns off the display. As the keypad goes into power saving mode, it resets the commands entered!

KeyPad supports 4 to 6 digit codes. Entering the code should be confirmed by pressing one of the buttons:  (arm),  (disarm)  (Night mode). Any characters typed by mistake are reset with button C (“Reset”).

KeyPad also supports control of security modes without entering a code, if the “Arm without code” function is enabled in the settings. This function is disabled by default.

Function button

KeyPad has a Function button that operates in 3 modes:

- **Off** — the button is disabled. Nothing happens after clicking.
- **Alarm** — after the Function button is pressed, the system sends an alarm to the monitoring station of the security company, to users, and activates the sirens connected to the system.
- **Mute Interconnected Fire Detectors Alarms** — after the Function button is pressed, the system disables the sirens of Ajax fire detectors. The option works only if Interconnected FireProtect Alarms is enabled (Hub → Settings → Service → Fire detectors settings).

Duress code

A duress code allows you to simulate alarm deactivation. Unlike the panic button, if this code is entered, the user will not be compromised by the siren sounding, and the keypad and Ajax app will inform about the successful disarming of the system. At the same time, the security company will receive an alarm.

The following types of duress codes are available:

- **Keypad code** — when used, events are delivered to Ajax apps on behalf of the keypad.
- **Personal password** — set up for each user connected to the hub. When used, events are delivered to Ajax apps on behalf of the user.
- **Keypad Access codes** — set up for people who are not registered in the system. When used, events are delivered to Ajax apps with a name associated with this code.

Learn more

Unauthorized access auto-lock

If a wrong code is entered three times within 1 minute, the keypad will be locked for the time specified in the settings. During this time, the hub will ignore all codes and inform the users of the security system and the CMS about an attempt to guess the code.

The keypad will automatically unlock after the lock time defined in the settings expires. However, user or PRO with administrator rights can unlock the keypad through the Ajax app.

Two-stage arming

KeyPad participates in arming in two stages. When this feature is enabled, the system will only arm after being re-armed with SpaceControl or after a second-stage detector is restored (for example, by closing the front door on which DoorProtect is installed).

Learn more

Jeweller data transfer protocol

The keypad uses the Jeweller radio protocol to transmit events and alarms. This is a two-way wireless data transfer protocol that provides fast and reliable communication between the hub and the connected devices.

Jeweller supports block encryption with a floating key and authentication of devices at each communication session to prevent sabotage and device spoofing. The protocol involves regular polling of devices by the hub at intervals of 12 to 300 seconds (set in the Ajax app) to monitor communication with all devices and display their statuses in the Ajax apps.

More about Jeweller

Sending events to the monitoring station

The Ajax security system can transmit alarms to the PRO Desktop monitoring app as well as the central monitoring station (CMS) via SurGard (Contact ID),

SIA (DC-09), ADEMCO 685, and **other proprietary protocols**. See the list of CMSs to which you can connect the Ajax security system **here**.

KeyPad can transmit the following events:

- Duress code is entered.
- The panic button is pressed (if the Function button works in the panic button mode).
- The keypad is locked due to an attempt to guess a code.
- Tamper alarm/recovery.
- Hub connection loss/restoration.
- The keypad is temporarily turned off/on.
- Unsuccessful attempt to arm the security system (with Integrity Check enabled).

When an alarm is received, the operator of the security company monitoring station knows what happened and where to send the fast response team. The addressability of each Ajax device allows you to send not only events but also the type of the device, the security group, the name assigned to it, and the room to the PRO Desktop or to the CMS. The list of transmitted parameters may differ depending on the type of the CMS and the selected communication protocol.

The device ID and the number of the loop (zone) can be found in its states in the Ajax app.

Indication

When touching KeyPad, it wakes up highlighting the keyboard and indicating the security mode: Armed, Disarmed, or Night Mode. The security mode is always actual, regardless of the control device that was used to change it (the key fob or app).

Event	Indication
Malfunction indicator **X** blinks	Indicator notifies about lack of communication with hub or keypad lid opening. You can check the reason for malfunction in the **Ajax Security System app**
KeyPad button pressed	A short beep, the system's current arming state LED blinks once
The system is armed	Short sound signal, Armed mode / Night mode LED indicator lights up
The system is disarmed	Two short sound signals, LED disarmed LED indicator lights up
Incorrect passcode	Long sound signal, the keyboard backlight blinks 3 times
A malfunction is detected when arming (e.g., the detector is lost)	A long beep, the system's current arming state LED blinks 3 times
The hub does not respond to the command — no connection	Long sound signal, the malfunction indicator lights up
KeyPad is locked after 3 unsuccessful attempts to enter the passcode	Long sound signal, security mode indicators blink simultaneously
Low battery	After arming/disarming the system, the malfunction indicator blinks smoothly. The keyboard is locked while the indicator blinks. When activating KeyPad with low batteries, it will beep with a long sound signal, the malfunction indicator smoothly lights up and then switches off

Connecting

Before connecting the device:

1. Switch on the hub and check its Internet connection (the logo glows white or green).
2. Install the **Ajax app**. Create the account, add the hub to the app, and create at least one room.
3. Make sure that the hub is not armed, and it does not update by checking its status in the Ajax app.

> ⚠ Only users with administrator rights can add a device to the app

How to connect KeyPad to the hub:

1. Select the **Add Device** option in the Ajax app.
2. Name the device, scan/write manually the **QR Code** (located on the body and packaging), and select the location room.
3. Select **Add** — the countdown will begin.
4. Switch on KeyPad by holding power button for 3 seconds — it will blink once with the keyboard backlight.

For detection and pairing to occur, KeyPad should be located within the coverage of the wireless network of the hub (at the same protected object).

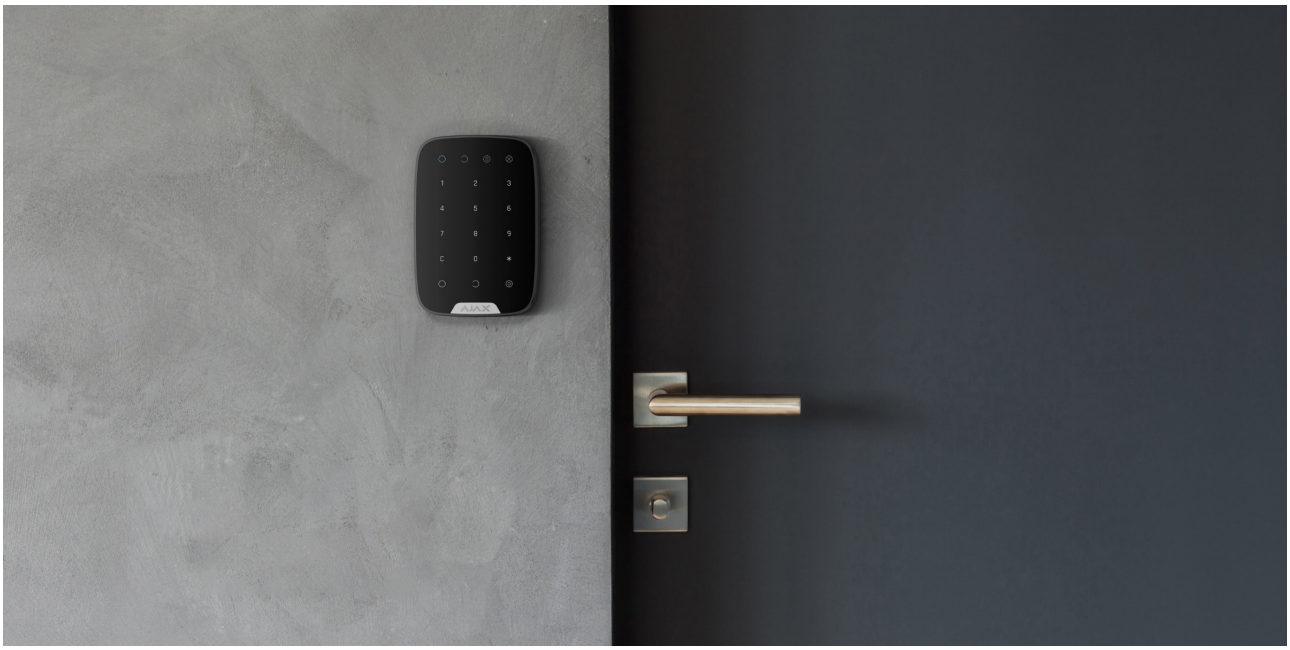
A request for connection to the hub is transmitted for a short time at the moment of switching on the device.

If KeyPad failed to connect to the hub, switch it off for 5 seconds and retry.

The connected device will appear in the app device list. Update of the device statuses in the list depends on the detector ping interval in the hub settings (the default value is 36 seconds).

> ⚠ There are no pre-set passwords for KeyPad. Before using a KeyPad, set all necessary passwords: common, personal, and duress code if you are forced to disarm the system.

Selecting the Location



The location of the device depends on its remoteness from the hub, and obstacles hindering the radio signal transmission: walls, floors, large objects inside the room.

The device developed only for indoor use.

Do not install KeyPad:

1. Near the radio transmission equipment, including that operates in 2G/3G/4G mobile networks, Wi-Fi routers, transceivers, radio stations, as well as an Ajax hub (it uses a GSM network).
2. Close to electrical wiring.
3. Close to metal objects and mirrors that can cause radio signal attenuation or shading.
4. Outside the premises (outdoors).
5. Inside premises with the temperature and humidity beyond the range of permissible limits.
6. Closer than 1 m to the hub.

Check the Jeweller signal strength at the installation location

During testing, the signal level is displayed in the app and on the keyboard with security mode indicators ◯ (Armed mode), ◯ (Disarmed mode), ◯ (Night mode) and malfunction indicator **X**.

If the signal level is low (one bar), we cannot guarantee the stable operation of the device. Take all possible measures to improve the quality of the signal. At least, move the device: even a 20 cm shift can significantly improve the quality of signal reception.

If after moving the device still has a low or unstable signal strength, use a **radio signal range extender**.

KeyPad is designed for operation when fixed to the vertical surface. When using KeyPad in hands, we cannot guarantee successful operation of the sensor keyboard.

States

1. Devices –
2. KeyPad

Parameter	Value
Temperature	Temperature of the device. Measured on the processor and changes gradually
Jeweller Signal Strength	Signal strength between the hub and KeyPad
Battery Charge	Battery level of the device. Two states available: • OK • Battery discharged **How battery charge is displayed in Ajax apps**
Lid	The tamper mode of the device, which reacts to

	the detachment of or damage to the body
Connection	Connection status between the hub and the KeyPad
ReX	Displays the status of using a **radio signal range extender**
Temporary Deactivation	Shows the status of the device: active, completely disabled by the user, or only notifications about triggering of the device tamper button are disabled
Firmware	Detector firmware version
Device ID	Device identifier

Settings

1. Devices
2. KeyPad
3. Settings

Setting	Value
First field	Device name, can be edited
Room	Selecting the virtual room to which the device is assigned
Arming/Disarming Permissions	Selecting the security group to which KeyPad is assigned
Group management	Selecting the way of verification for arming/disarming • Keypad code only • User passcode only • Keypad and user passcode To activate the **Access Codes** set up for people who are not registered in the system, select the options on the keypad:

	Keypad code only or **Keypad and user code**
Keypad code	Setting a passcode for arming/disarming
Duress Code	Setting a duress code for silent alarm
Function Button	Selection of the button function * • **Off** — the Function button is disabled and does not execute any commands when pressed • **Alarm** — by pressing the Function button, the system sends an alarm to the monitoring station of the security company and to all users • **Mute Interconnected Fire Detectors Alarm** — when pressed, mutes the fire alarm of FireProtect/FireProtect Plus detectors. The feature works only if Interconnected Fire Detectors Alarms is enabled Learn more
Arming without Passcode	If active, the system can be armed by pressing Arm button without passcode
Unathorised Access Auto-lock	If active, the keyboard is locked for the pre-set time after entering incorrect passcode three times in a row (during 30 min). During this time, the system cannot be disarmed via KeyPad
Auto-lock Time (min)	Lock period after wrong passcode attempts
Brightness	Brightness of the keyboard backlight
Buttons Volume	Volume of the beeper
Alert with a siren if panic button is pressed	The setting appears if the **Alarm** mode is selected for **Function** button. If active, the Function button pressing triggers the sirens installed at the object
Jeweller Signal Strength Test	Switches the device to the signal strength test mode
Signal Attenuation Test	Switches the KeyPad to the signal fade test

	mode (available in devices with **firmware version 3.50 and later**)
Temporary Deactivation	Allows the user to disconnect the device without removing it from the system. Two options are available: • **Entirely** — the device will not execute system commands or participate in automation scenarios, and the system will ignore device alarms and other notifications • **Lid only** — the system will ignore only notifications about the triggering of the device tamper button **Learn more about temporary deactivation of devices**
User Guide	Opens the KeyPad User Manual
Unpair Device	Disconnects the device from the hub and deletes its settings

Setting up codes and passwords

Ajax security system allows you to set up a keypad password, as well as personal passwords for users added to the hub.

With the **OS Malevich 2.13.1** update, we have also added the ability to create passwords for people who are not connected to the hub. This is convenient, for example, to provide a cleaning company with access to security management. See how to set up and use each type of a password below.

To install a personal passcode:

1. Go to profile settings (**Hub** → **Settings** → **Users** → **Your profile settings**)
2. Click **Access Code Settings** (in this menu you can also see the user identifier)
3. Set the **User Code** and **Duress Code**

Each user sets a personal passcode individually!

To set up an access code for an unregistered person in the system

1. Go to the hub settings (**Hub** → **Settings**).
2. Select **Keypad Access Codes**.
3. Set up **Username** and **Access Code**.

If you want to set up a duress code, change settings for access to groups, Night mode, code ID, temporarily disable or delete this code, select it in the list and make changes.

PRO or a user with administrator rights can set up an access code or change its settings. This function is supported by hubs with OS Malevich 2.13.1 and higher. Access codes are not supported by the Hub control panel.

Security management by passwords

You can control the security of the entire facility or separate groups using common or personal passwords as well as using access codes (configured by PRO or a user with administrator rights).

If a personal password is used, the name of the user who armed/disarmed the system is displayed in notifications and in the hub event feed. If a common password is used, the name of the user who changed the security mode is not displayed.

Keypad access codes support hubs with OS Malevich 2.13.1 and higher. Hub control panel does not support this function.

Security management of the entire facility using a common password

Enter the **common password** and press the **arming** / **disarming** / **Night mode activation**.

For example: 1234 →

Group security management with a common password

Enter the **common password**, press the *, enter the **group ID** and press the **arming** / **disarming** / **Night mode activation**.

For example: 1234 → * → 2 →

What is Group ID?

If a group is assigned to the KeyPad (**Arming / Disarming permission** field in the keypad settings), you do not need to enter the group ID. To manage the arming mode of this group, entering a common or personal password is sufficient.

Please note that if a group is assigned to the KeyPad, you will not be able to manage **Night mode** using a common password.

In this case, **Night mode** can only be managed using a personal password (if the user has the appropriate rights).

Rights in the Ajax security system

Security management of the entire facility using a personal password

Enter **user ID**, press *, enter **personal password**, and press the **arming** / **disarming** / **Night mode activation**.

For example: 2 → * → 1234 →

What is User ID?

Group security management using a personal password

Enter **user ID**, press *, enter **personal password**, press *, enter **group ID**, and press the **arming** / **disarming** / **Night mode activation**.

For example: 2 → * → 1234 → * → 5 →

What is Group ID?

What is User ID?

If a group is assigned to the KeyPad (**Arming / Disarming permission** field in the keypad settings), you do not need to enter the group ID. To manage the arming mode of this group, entering a personal password is sufficient.

Security control of the entire object using an access code

Enter the **access code** and press the **arming** / **disarming** / **Night mode activation** key.

For example: 1234 →

Security management of the group using a common code

Enter the **access code**, press the *, enter the **group ID** and press the **arming** / **disarming** / **Night mode activation** key.

For example: 1234 → * → 2 →

What is Group ID?

Using a duress password

A **duress password** allows you to raise a silent alarm and imitate alarm deactivation. A silent alarm means that the Ajax app and sirens will not shout and expose you. But a security company and other users will be alerted instantly. You can use both **personal** and **common** duress password. You can also set up a duress access code for people not registered in the system.

What is a duress password and how do you use it?

Scenarios and sirens react to disarming under duress in the same way as to normal disarming.

To use a common duress password:

Enter the **common duress password** and press the **disarming** key .

For example: 4321 →

To use a personal duress password:

Enter **user ID**, press *, then enter **personal duress password** and press the **disarming** key .

For example: 2 → * → 4422 →

To use a duress access code:

Enter the **duress access code** and press the **disarm** key .

For example: 4567 →

How the fire alarm muting function works

Using the KeyPad, you can mute the interconnected fire detectors alarm by pressing the Function button (if the corresponding setting is enabled). The reaction of the system to pressing a button depends on the state of the system:

- **Interconnected Fire Detectors Alarms have already propagated** — by the first press of the Function button, all sirens of the fire detectors are muted, except for those that registered the alarm. Pressing the button again mutes the remaining detectors.
- **The interconnected alarms delay time lasts** — by pressing the Function button, the siren of the triggered FireProtect/FireProtect Plus detector is muted.

Learn more about Interconnected Fire Detectors Alarms

With the OS Malevich 2.12 update, users can mute fire alarms in their groups without affecting detectors in the groups to which they do not have access.

Learn more

Functionality Testing

The Ajax security system allows conducting tests for checking the functionality of connected devices.

The tests do not start straight away but within a period of 36 seconds when using the standard settings. The test time start depends on the settings of the detector scanning period (the paragraph on “**Jeweller**” settings in hub settings).

Jeweller Signal Strength Test

Attenuation Test

Installation

Before installing the detector, make sure that you have selected the optimal location and it is in compliance with the guidelines contained in this manual!

KeyPad should be attached to the vertical surface.

1. Attach the SmartBracket panel to the surface using bundled screws, using at least two fixing points (one of them — above the tamper). After selecting other attachment hardware, make sure that they do not damage or deform the panel.

The double-sided adhesive tape may be only used for temporary attachment of KeyPad. The tape will run dry in course of time, which may result in the falling of the KeyPad and damage of the device.

2. Put KeyPad on the attachment panel and tighten the mounting screw on the body underside.

As soon as the KeyPad is fixed in SmartBracket, it will blink with the LED **X** (Fault) — this will be a signal that the tamper has been actuated.

If the malfunction indicator **X** did not blink after installation in SmartBracket, check the status of the tamper in the **Ajax app** and then check the fixing tightness of the panel.

If the KeyPad is torn off from the surface or removed from the attachment panel, you will receive the notification.

KeyPad Maintenance and Battery Replacement

Check the KeyPad operating capability on a regular basis.

The battery installed in the KeyPad ensures up to 2 years of autonomous operation (with the inquiry frequency by the hub of 3 minutes). If the KeyPad battery is low, the security system will send the relevant notices, and the malfunction indicator will smoothly lights up and goes out after each successful passcode entry.

How long Ajax devices operate on batteries, and what affects this

Battery Replacement

Complete Set

1. KeyPad
2. SmartBracket mounting panel
3. Batteries AAA (pre-installed) — 4 pcs
4. Installation kit
5. Quick Start Guide

Technical Specifications

Sensor type	Capacitive
Anti-tamper switch	Yes
Protection against passcode guessing	Yes
Radio communication protocol	Jeweller **Learn more**
Radio frequency band	866.0 – 866.5 MHz 868.0 – 868.6 MHz 868.7 – 869.2 MHz 905.0 – 926.5 MHz 915.85 – 926.5 MHz 921.0 – 922.0 MHz Depends on the region of sale.
Compatibility	Operates only with all Ajax **hubs**, and **radio signal range extenders**
Maximum RF output power	Up to 20 mW
Modulation of the radio signal	GFSK
Radio signal range	Up to 1,700 m (if there are no obstacles) **Learn more**
Power supply	4 × AAA batteries
Power supply voltage	3 V (batteries are installed in pairs)
Battery life	Up to 2 years
Installation method	Indoors
Operating temperature range	From -10°C to +40°C
Operating humidity	Up to 75%
Overall dimensions	150 × 103 × 14 mm
Weight	197 g
Service life	10 years
Certification	Security Grade 2, Environmental Class II in conformity with the requirements of EN 50131-1, EN 50131-3, EN 50131-5-3

Compliance with standards

Warranty

Warranty for the “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY products is valid for 2 years after the purchase and does not apply to the pre-installed battery.

If the device does not work correctly, you should first contact the support service — in half of the cases, technical issues can be solved remotely!

The full text of the warranty

User Agreement

Technical support: **support@ajax.systems**