

# EN54 Fire Hub Jeweller user manual

Revision 1



**EN54 Fire Hub Jeweller** is a wireless control and indicating equipment (CIE) for a fire alarm system, supporting intrusion protection devices. It enables the integration of EN 54 fire detection with EN 50131 intruder alarm, automation, and video surveillance in a single system. The CIE features a 10.1" touch display that provides informative fire alarm notifications, system status updates, and convenient fire system control.

The CIE requires an internet connection to access the Ajax Cloud server. Supported communication channels include Ethernet, Wi-Fi, and two SIM cards.

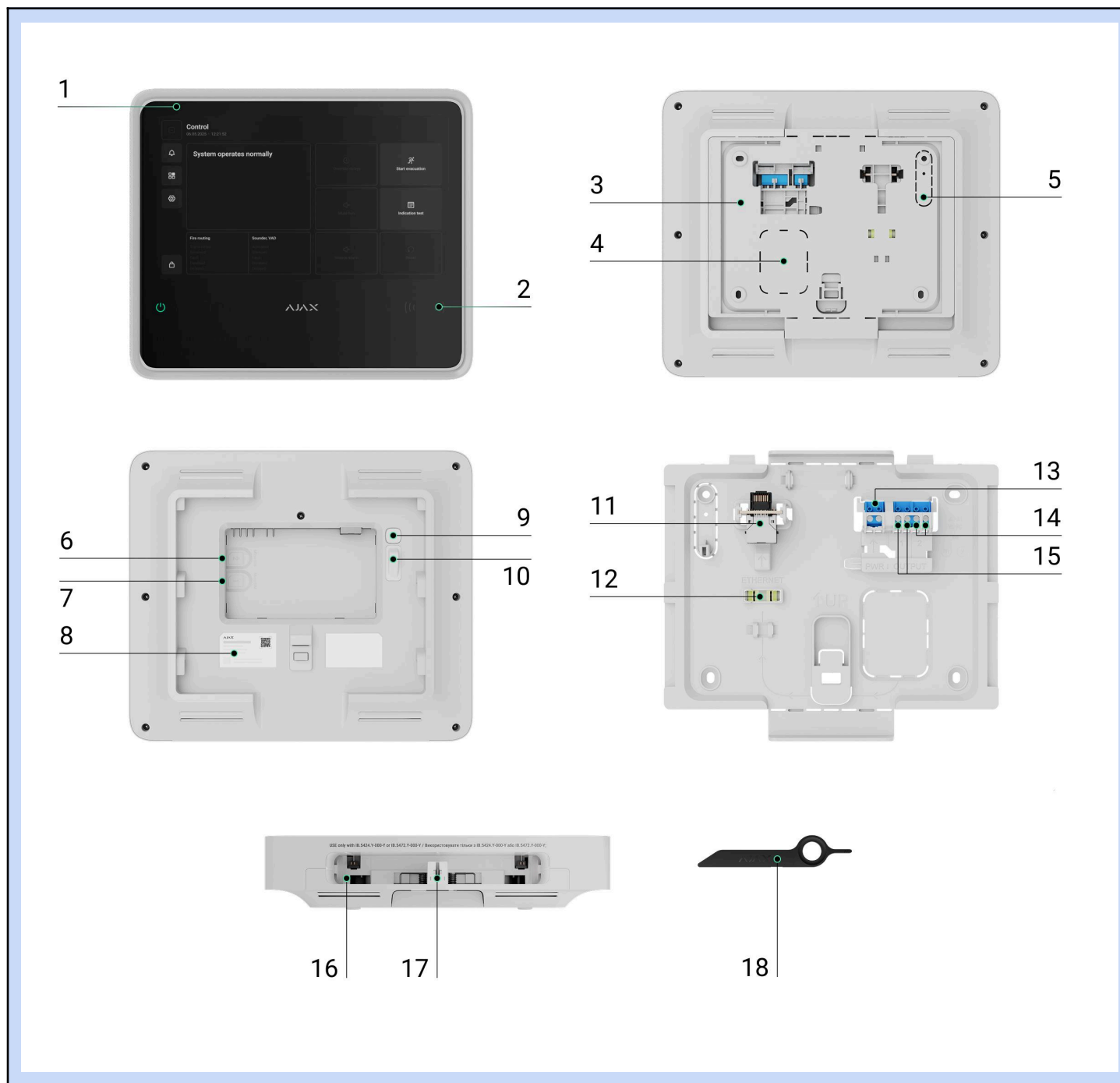
EN54 Fire Hub Jeweller can operate autonomously for 24 or 72 hours, depending on the battery. The backup battery is not included in the complete set. Only use compatible batteries: **EN54 Internal Battery (24h)** or **EN54 Internal Battery (72h)**.

👉 [Buy EN54 Fire Hub Jeweller](#)

👉 [EN54 Internal Battery \(24h\)](#)

👉 [EN54 Internal Battery \(72h\)](#)

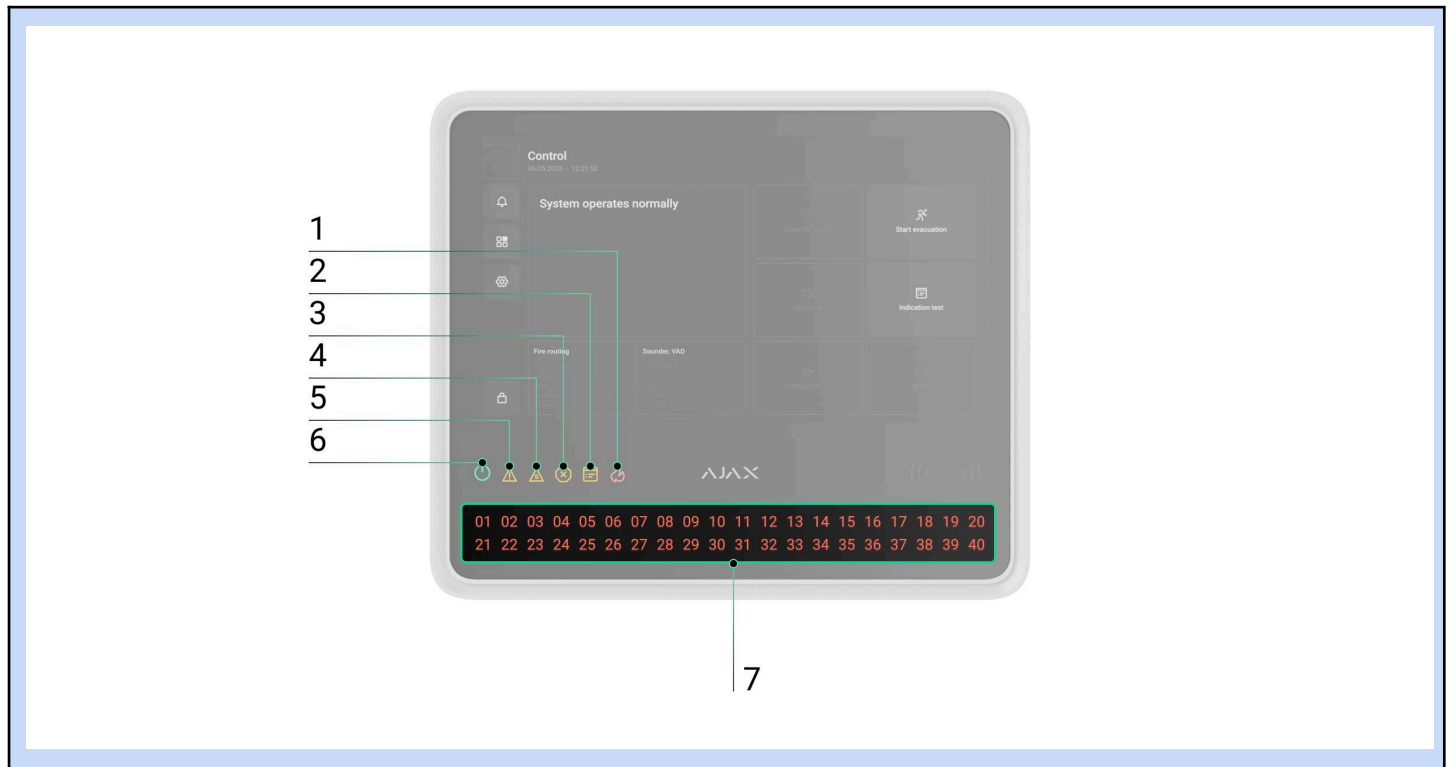
## Functional elements



1. IPS touch display with a 10.1" diagonal.
2. Card/key fob reader (*coming soon*).
3. SmartBracket mounting panel.
4. Perforated part of the mounting panel for routing cables through the wall.
5. Perforated part of the mounting panel that triggers the [tamper button](#) if the device is removed from the surface. Do not break it off.
6. Slot for micro SIM 2.
7. Slot for micro SIM 1.
8. QR code and ID (serial number) of the device.
9. Power button.
10. Tamper button.
11. Ethernet cable connector.

12. Bubble level for checking mount inclination angle during installation.
13. Terminals for connecting a power cable.
14. Relay output 2 — for alerting the monitoring station to fire alarms.
15. Relay output 1 — for alerting the monitoring station to system faults.
16. Slot for [internal battery](#) (not included).
17. Hole for the special tool.
18. Special tool (key).

## LED indicators



1. Fire alarm indicator.
2. Test indicator.
3. Disablement indicator.
4. System fault indicator.
5. Fault indicator.
6. Power supply indicator.
7. Fire zones LED indicators.

## Operating principle

GIF

EN54 Fire Hub Jeweller is the CIE of an Ajax system, designed for comprehensive management of fire safety systems. It also supports intrusion protection, video surveillance, and automation devices, making it a unified solution for protecting commercial and municipal sites. The CIE controls the operation of connected devices and indicates the current state of the fire safety system.

The CIE is added to a [space](#) — a virtual entity that brings together various autonomous devices installed at the same facility.

## 👉 [How to create a space](#)

You can connect up to 200 wireless Ajax devices to EN54 Fire Hub Jeweller. Once connected, they provide protection against fire, intrusion, and flooding, while also enabling control of electrical appliances – either via automation scenarios or manually via mobile apps, panic button, [LightSwitch](#), or [keypad with a touch screen](#).

To monitor the operation of all connected devices, the CIE communicates with them using two [encrypted protocols](#):

1. **Jeweller** is a radio protocol for transmitting events and alarms from Ajax wireless devices. The communication range is up to 1,800 m **5,900 ft** in open space, without obstacles such as walls, doors, or inter-floor structures.

## 👉 [Learn more about Jeweller](#)

2. **Wings** is a radio protocol for transmitting large data packets. The communication range is also up to 1,800 m **5,900 ft** in open space.

## 👉 [Learn more about Wings](#)

If a fire detector is triggered, the system raises an alarm within three seconds. In this case, the CIE activates the sirens, runs scenarios, and alerts the monitoring station and all users.

## Fire protection

EN54 Fire Hub Jeweller is fully compliant with key fire detection and fire alarm system standards, specifically EN 54. It allows building wireless fire detection and alarm systems in commercial and municipal facilities.


Ajax devices from the **EN54 Line** connected to the CIE are assigned to one of 40 **Fire zones**. When a fire is detected in any zone or an [Ajax manual call point](#) is pressed, all Ajax EN54 sounders and VADs across the facility raise an alarm.


The CIE display shows complete incident information: the cause of the alarm, the time it started, and where (zone, room, location), along with the last activated zone and the total number of zones in the fire alarm state.



Thanks to its intuitive interface and detailed LED indication, users can quickly respond to alarms, locate the fire, or activate the fire alarm manually. The CIE is also equipped with a buzzer that provides audible alarm notifications with a volume of at least 60 dB at a distance of 1 m **3.3 ft** from the device.

Users with the appropriate rights and access level can silence, resound, or reset the fire alarm from the CIE

display or via Ajax apps: **Control** tab → tap the  icon. Depending on the CIE settings, a silenced fire alarm may be raised again automatically if fire is detected in a new zone, or users may be notified only via CIE indications and in-app alerts. Even if the CIE buzzer was muted earlier, it will still alert in the event of fire in a new zone or in case of new faults. Sounders and VADs can also be manually resounded from the CIE or via the

**Control**  tab in Ajax apps. If the fire alarm state is reset while detectors are still registering fire, the system will raise an alarm again after 20 seconds.

## Event center



Ajax apps keep a detailed log of alarms, security events, and user actions. The CIE display also shows an event log, limited to Ajax EN54 devices connected to the CIE. The **Event center** tab provides detailed information about fire alarms, device faults, disablements, tests, and other important events. The information is organized into separate tabs for easier navigation.

### Fire alarm tab



The **Fire alarm** tab becomes active only when a fire is detected in the system. Tapping this tab opens a list of zones currently in the fire alarm state, sorted by the time the fire started. Selecting a zone from the list displays the alarms registered in that zone.

### Fault, test, or disablement tab



The **Fault, test, or disablement** tab displays all active system events matching the types listed in its name. The tab becomes active only when the system is running a test of Ajax EN54 devices, when some devices are fully or partially disabled, or when a fault has occurred within the fire alarm system, and it has not yet been restored. Tapping this tab opens a list of the corresponding system events.

### Event log tab



The **Event log** tab is always active. Tapping it opens a chronological list of all events and alarms related to the fire alarm system. The CIE event log stores up to 10,000 events.

## Fire zones



EN54 Fire Hub Jeweller allows for managing Ajax EN54 devices in different **Fire zones**. Users can quickly access the **Fire zones** list from the CIE display to view the current state of each zone and check for any device disablements within them. An admin or a user with **access level 2** can initiate a test or disable devices directly from the CIE touch screen.

## Authorization



Unauthorized users have access to the CIE **Control** tab and can perform basic actions: start an [indication test](#), mute the CIE buzzer, or override configured delays (coming soon) to send an alarm to the monitoring

station in case of fire. Authorized users with **access level 2** or higher have access to the broader CIE functionality, such as starting evacuation, silencing alarms, running device tests, etc.

Users can authorize in the system by entering an access code on the CIE display or by presenting [Tag](#) or [Pass](#) to the reader (coming soon). Access level 2 can be configured in the CIE **Access codes** [settings](#) in Ajax apps.

👉 [Learn more](#)

👉 [User account types and rights](#)

## Settings



In the **Settings** tab on the EN54 Fire Hub Jeweller display, users can adjust the screen backlight brightness and select the interface language. These options are available to all users.

All other CIE [settings](#) can be configured via Ajax apps.

## Sabotage protection

EN54 Fire Hub Jeweller supports four communication channels for connecting to the Ajax Cloud server: Wi-Fi, Ethernet, and two SIM cards. This allows the device to work with multiple communication providers at once. If one channel becomes unavailable, the CIE automatically switches to another and notifies the monitoring station and system users.

If a jamming attempt is detected, the system switches to an idle radio frequency and sends notifications to the monitoring station and users.

👉 [What is security system jamming](#)

The CIE regularly checks the connection quality with all linked devices. If any device loses connection, and the configured timeout expires, all system users (depending on the settings) and the monitoring station will receive a notification of the incident.

👉 [Learn more](#)

To comply with the EN 54-25 standard, the time before CIE detects communication loss with connected devices must be less than 300 seconds. An admin or a PRO with system configuration rights can adjust the settings to meet this requirement.

👉 [Learn more](#)

No one can turn off the CIE unnoticed. If an intruder attempts to open the CIE enclosure, a tamper alarm is triggered immediately. An alarm notification is then sent to the monitoring company and all system users.

👉 [What is a tamper button](#)

The CIE regularly checks its connection to Ajax Cloud. The ping interval is defined in the CIE settings. When

the minimum interval is configured, the server can notify users and the monitoring company as soon as 60 seconds after the connection is lost.

👉 [Learn more](#)

A 5 Ah or 10 Ah backup battery can be installed in the CIE. **EN54 Internal Battery (24h)** provides up to 24 hours of autonomous system operation, while **EN54 Internal Battery (72h)** offers up to 72 hours.


Internal battery is not included in the CIE complete set and must be bought separately.

👉 [Learn more](#)

## OS Malevich

EN54 Fire Hub Jeweller runs on OS Malevich, a real-time operating system protected against viruses and cyberattacks.

OS Malevich brings new features and functionality to the Ajax system through over-the-air updates. A PRO or a company with firmware update rights can start an update – when available – from the EN54 Fire Hub Jeweller

field in the **Devices**  tab, or via the CIE [states](#) or [settings](#). On-screen instructions help guide the user through the process.

The update takes up to 2 minutes and requires the system to be disarmed, free of active fire alarms, and connected to an external power supply.

👉 [How OS Malevich updates](#)

## Ajax account

To set up the system, install an [Ajax app](#) and log in to your account, or create a new one if you don't have one. Don't create a new account for each space, since one account can manage multiple security systems. Where necessary, you can configure separate access rights for each space. Changing the space admin, adding or removing users does not reset the settings of devices added to the space.

👉 [How to create the user account](#)

👉 [How to create a PRO account](#)

## Adding the CIE in an Ajax app

We highly recommend creating [personal access codes](#), as well as access codes with access level 2, after adding EN54 Fire Hub Jeweller to a space. An access code is required to [log in](#) and manage the fire alarm system from the CIE touch screen.

Use the [latest versions of Ajax apps](#) to access all available features and ensure proper system operation.

After adding a CIE to your account, you become the admin of the device. Admins can invite other users to the system and determine their rights. You can connect up to 200 users to EN54 Fire Hub Jeweller. Each PRO account connected to the CIE, as well as the security company profile, is considered a user of the system.

If there are already users on the CIE, the CIE admin, PRO with the rights to configure the system, or the installation company maintaining the selected CIE can add your account. You will be notified that the CIE has already been added to another account. Contact our [Technical Support](#) to determine who has admin rights on the CIE.


👉 [User account types and rights](#)

To add the CIE in an [Ajax app](#):

1. Connect external power, internal battery, Ethernet, and/or Wi-Fi and SIM cards to the CIE.
2. Open an [Ajax app](#) and allow the requested permissions. This ensures full functionality and reliable delivery of alarm and event notifications.
3. Make sure you have a space in the app. If not, create one.

👉 [What is a space](#)

👉 [How to create a space](#)

4. Scan the CIE QR code or enter its ID manually.
5. Assign a name to the CIE.
6. Add at least one [virtual room](#).
7. Turn on the CIE.
8. Install the CIE on the SmartBracket mounting panel.
9. Click **Add device**.
10. Wait until the CIE is added. Once connected, the CIE will appear in the **Devices**  tab of an Ajax app.


## Adding devices to the CIE

Check the device compatibility before adding it to the CIE. To add a device to the CIE, it should be located within the CIE radio communication range – at the same secured premises.

To add a device to the CIE:

1. Select a space with a compatible CIE.
2. Ensure the CIE is switched on and has internet access via Ethernet, Wi-Fi, and/or mobile network.
3. Check the states in an Ajax app to ensure the space is disarmed and the CIE is not starting an update.

Only a PRO or a space admin with the rights to configure the system can add a device to the CIE.

4. Go to the **Devices**  tab and tap **Add device**.
5. Scan the QR code or enter the device ID manually. A QR code with ID is placed on the device under the SmartBracket mounting panel. Also, it is duplicated on the device packaging.



- Assign a name to the device.
- Select a virtual room.
- For Ajax EN54 devices, select a fire zone. If necessary, specify the device location in the **Location** field.

Names of devices, fire zones, rooms, and locations are displayed in the text of events and alarms of the Ajax system.

- Tap **Add device**, and the countdown will begin.
- Switch on the device.



Find more information in the [user manual](#) for each device how to add it to the CIE.

## Faults

Screen

When a CIE fault is detected (e.g., the tamper alarm is triggered, the internal battery is low, the device is offline), the Ajax app displays a fault counter on the device icon. Faults are also indicated in the device’s states. Affected fields are highlighted in red.


All faults related to Ajax EN54 devices and the CIE itself are shown on its display. In the **Control** tab, users can see which zone requires attention and the reason. The built-in buzzer and LED indicators of the CIE always signal the presence of a fault.




More details about the fault can be found in the **Event center** or **Fire zones** tab on the CIE. Full information about the fire alarm system is also available in Ajax apps: **Control**  tab → Swipe or tap the  icon.









## Icons

Screen with icons

Icons display some of the EN54 Fire Hub Jeweller states. You can view them in the Ajax app, in the **Devices**  tab.

Icon	Meaning
	The CIE operates in the 2G network.
	The CIE operates in the 4G (LTE) network.
	No SIM cards. Insert at least one SIM card.

	The SIM card is faulty or has a PIN code set up. Check SIM card operation in the phone and disable the PIN code request.
	The CIE battery charge level. Displayed in 1% increments.
	The backup battery is not connected.
	EN54 Fire Hub Jeweller fault detected. Open <a href="#">CIE states</a> for details.
	The CIE is directly connected to the monitoring station of the security company. The icon is not displayed if direct connection is not available or not configured.  <a href="#">Learn more</a>
	The CIE is not directly connected to the monitoring station of the security company. The icon is not displayed if direct connection is not available or not configured.  <a href="#">Learn more</a>

## States

### In the CIE Control tab

#### Control screen

Users can check the fire alarm system states in the CIE **Control** tab. It shows whether the system operates normally, if a fire alarm is active, and other system states.

Parameter	Meaning
System state	<p>The system state field is located in the upper-left corner of the CIE and shows the following state:</p> <ul style="list-style-type: none"> <li>• <b>System operates normally.</b></li> <li>• <b>System requires attention</b> – in case of any EN54 device fault, test, or disablement.</li> <li>• <b>Fire alarm started</b> – in case of a fire alarm in the system.</li> </ul> <p>This field also contains additional details about the state, which can be checked in the <b>Event center</b>.</p>
Fire routing	<p>Signal sending status to the monitoring station:</p> <ul style="list-style-type: none"> <li>• <b>Transmitted</b> — fire alarm signal is sent to the monitoring company.</li> <li>• <b>Received</b> — CIE received a confirmation that the fire alarm signal is delivered.</li> <li>• <b>Fault</b> — CIE didn't receive a confirmation that the fire alarm signal is delivered.</li> </ul>
Sounder/VAD	<p>The state of annunciation devices in the system:</p> <ul style="list-style-type: none"> <li>• <b>Activated</b> — sounder or VAD is activated in the system.</li> </ul>



	<ul style="list-style-type: none"> <li>● <b>Silenced</b> — sounder or VAD is silenced in the system.</li> <li>● <b>Fault</b> — at least one device with a sounder or VAD in the system has a fault.</li> <li>● <b>Disablement</b> — at least one device with a sounder or VAD is partially or completely <a href="#">disabled</a>.</li> <li>● <b>Delayed</b> — at least one sounder or VAD in the system is in the delayed state.</li> </ul>
Override delays (coming soon)	The button is <b>active</b> when the investigation and/or acknowledgement delay has started, allowing users to switch the system to the fire alarm state, overriding the delay.
Start evacuation	<p>Users can start evacuation manually.</p> <p>Sounders and VADs will alert about the fire, and the fire alarm signal will be sent to the monitoring station.</p>
Mute buzzer	The button is <b>active</b> when the CIE built-in buzzer is alerting about a fire or fault, and <b>disabled</b> when the buzzer is muted.
Indication test	<p>When the button is <b>active</b>, the user can run the CIE indication test.</p> <p>When it is <b>disabled</b>, CIE indication test is already running.</p> <p><a href="#">Learn more</a></p>
Silence alarm	<p>The button is <b>active</b> when at least one sounder or VAD is active.</p> <p>When it is <b>disabled</b>, there is no fire alarm in the system, or the user has no access to silence annunciation devices.</p>
Resound alarm	The button is <b>available</b> and <b>active</b> if at least one sounder or VAD in the system is silenced after a fire alarm had started.
Reset	<p>When the button is <b>active</b>, there is a fire alarm in the system, and an admin, PRO, or a user with access level 2 can reset it.</p> <p>When it is <b>disabled</b>, there is no fire alarm in the system, or the user has no access to reset a fire alarm.</p>

## In Ajax apps

Screen with states

States can also be found in Ajax apps:

1. Go to the **Devices**  tab.
2. Select **EN54 Fire Hub Jeweller** from the list.


Parameter	Meaning
Fault	<p>Click the  button to open the list of the device faults.</p> <p>The field appears only if a fault is detected. A fault is a critical interferer for fire alarm system operation according to the EN 54 standard.</p>
Malfunction	<p>Click the  button to open the list of the device malfunctions.</p> <p>The field appears only if a malfunction is detected. A malfunction is not a critical interferer for fire alarm system operation according to the EN 54 standard.</p>
Buzzer	<p>The CIE buzzer states:</p> <ul style="list-style-type: none"><li>• <b>Not alerting</b> – not active or muted.</li><li>• <b>Alerting</b> – activated in case of a fire alarm, fault, or CIE test.</li></ul>
Cellular signal strength	<p>The signal strength of the active SIM mobile network.</p> <p>Install the CIE in places where the cellular communication level reaches 2–3 bars.</p> <p>If the CIE is installed in a place with weak or unstable signal strength, it will not be able to call or send an SMS about an event or alarm.</p>
Connection	<p>The state of connection between the CIE and Ajax Cloud:</p> <ul style="list-style-type: none"><li>• <b>Online</b> – the CIE is connected to Ajax Cloud.</li><li>• <b>Offline</b> – the CIE is not connected to Ajax Cloud. Check the CIE Internet connection.</li></ul> <p>If the device is not connected to the server, icons of the CIE and all connected devices become semi-transparent in the list of devices.</p>
Battery charge	<p>CIE backup battery charge level. Displayed in 1% increments.</p>


	<p>At a charge level of 20% and below, the CIE will report low battery charge.</p> <p><a href="#">Learn more</a></p>
Lid	<p>The state of the tamper button that responds to detachment or opening of the device enclosure:</p> <ul style="list-style-type: none"> <li>• <b>Closed</b> — the device is installed on the SmartBracket mounting panel. The integrity of the device enclosure and the mounting panel is not compromised. Normal state.</li> <li>• <b>Open</b> — the device lid is open, or its integrity is otherwise compromised. Check the device.</li> </ul> <p><a href="#">Learn more</a></p>
Main power	<p>External power supply connection state:</p> <ul style="list-style-type: none"> <li>• <b>Connected</b> — the device is connected to an external power supply.</li> <li>• <b>Disconnected</b> — no external power supply. Check the connection of the device to the external power supply.</li> </ul>
Cellular data	<p>Mobile Internet connection status of the device:</p> <ul style="list-style-type: none"> <li>• <b>Connected</b> — the device is connected to Ajax Cloud via mobile Internet.</li> <li>• <b>Not connected</b> — the device is not connected to Ajax Cloud via mobile Internet. Check the device connection to the Internet via the mobile network.</li> <li>• <b>Disabled</b> — the option is disabled in the CIE settings.</li> </ul> <p>If the cellular signal strength reaches 1–3 bars, and the CIE has enough funds and/or has bonus SMS/calls, it will be able to call and send SMS, even if this field displays the <b>Not connected</b> state.</p>
Ethernet	<p>Internet connection state of the CIE via Ethernet:</p> <ul style="list-style-type: none"> <li>• <b>Connected</b> — the device is connected to Ajax Cloud via Ethernet. Normal state.</li> <li>• <b>Not connected</b> — the device is not connected to Ajax Cloud via Ethernet. Check the device connection to the Internet via the wired Internet.</li> <li>• <b>Disabled</b> — the option is disabled in the CIE settings.</li> </ul>
SIM 1	<p>The number of the SIM card installed in the first slot.</p>

	<p>To copy the number, click on it.</p> <p>If the phone number is displayed as an <b>Unknown number</b>, the operator has not written it to the memory of the SIM card.</p>
SIM 2	<p>The number of the SIM card installed in the second slot.</p> <p>To copy the number, click on it.</p> <p>If the phone number is displayed as an <b>Unknown number</b>, the operator has not written it to the memory of the SIM card.</p>
Average noise (dBm)	<p>Average noise in the radio channel. Measured in the place where the CIE is installed.</p> <p>The first two values show the level at Jeweller frequencies, and the third – at Wings frequencies.</p> <p>The acceptable value is –80 dBm or lower. For example, –95 dBm is considered acceptable and –70 dBm is invalid.</p> <p><a href="#">What is security system jamming</a></p>
Hub model	CIE model name.
Hardware	Device hardware version. Not updated.
Firmware	<p>Device firmware version. Updates remotely.</p> <p><a href="#">Learn more</a></p>
Device ID	<p>Identifier (first 8 digits of the serial number) of the device.</p> <p>The identifier is located on the device box and on the board under the QR code.</p>
IMEI	A unique 15-digit serial number for identifying the CIE modem on a GSM network. It is shown only when a SIM card is installed in the CIE.

## Settings


The CIE settings can be changed in Ajax apps. In order to change the settings:

1. Log in to the [Ajax app](#).
2. Select a facility from the list.
3. Go to the **Devices**  tab.
4. Select a CIE.

5. Go to its **Settings** by clicking on the gear icon .
6. Select a settings category and make changes. After making changes, click **Back** to save the new settings.

## Name

The CIE name is displayed in the SMS and push notification text. The name can contain up to 12 Cyrillic characters or up to 24 Latin characters.

To change it, click on the pencil icon  and enter the new CIE name.

## Room

Selection of the CIE virtual room. The room name is displayed in the SMS and push notification text.

## Control panel

Settings for the CIE display appearance and login methods:

- **Brightness** – adjust the display backlight brightness level from 0 to 100% (0 = minimum, 100 = maximum).
- **Interface language** – configure the CIE interface language. English is set by default.

### Coming soon:

- **Accidental press protection** – when enabled, tapping buttons in the **Control** tab requires additional confirmation from the user.
- **Login with pass/tag** – when enabled, users can log in via the CIE with [Pass](#) and [Tag](#) access devices.
- **Auto-logout time** – set the duration of user inactivity on the CIE before automatic logout.
- **Pass/tag reset** – allows deleting all CIE data linked to Tag or Pass from the device memory.

[Learn more](#)

## Fire system settings

Configuring system settings in case of a fire alarm:

- **Alarm signal** – configure the alarm sound for fire and non-fire alarms, and set the duration for the latter.

### Coming soon:

- **Delay settings** – set a delay for investigation and confirmation of the cause of an alarm before the system activates all EN54 sounders and visual alarm devices and notifies users and the monitoring station.
- **Evacuation button access** – configure access rights for the evacuation button. When pressed, it triggers an alarm before the delay expires. Evacuation can be started from the CIE display or an Ajax app. To start it from an app, go to:

Control  tab → tap the  icon → tap **Start evacuation** button

- **Resume silenced alarm** – when enabled, a silenced alarm restarts automatically if the fire spreads to new zones.

## Ethernet

Settings for wired Internet connection.

- **Connection via Ethernet** — enables and disables the CIE Ethernet module.
- **Connection type** — selection of a method for the CIE to obtain an IP address. If **DHCP** is selected, the CIE automatically obtains an IP address and other network settings. **Static** allows you to manually set up the IP address and other network settings for the CIE.
- **IP address** — CIE IP address.
- **Subnet mask** — mask of the subnet in which the CIE operates.
- **Gateway** — gateway used by the CIE.
- **DNS** — DNS of the CIE.

## Cellular

Settings of the mobile network and installed SIM cards. In the main menu, you can edit the settings that relate to both SIM cards, and in the sub-menu — the private parameters of SIM cards.

### Modem settings

- **Cellular data** — disables and enables the CIE cellular module.
- **Roaming** — if this option is active, the SIM cards can work in roaming.
- **Ignore network registration error** — if this option is active, the CIE ignores errors when trying to connect to the network via a SIM card. Activate this option if the SIM card cannot connect to the network.
- **Disable communication check with the operator** — if this option is active, the CIE ignores operator communication errors. Activate this option if the SIM card cannot connect to the network.

### SIM cards

- **SIM 1** — displays the number of the SIM card installed. If the phone number is displayed as an **Unknown number**, the operator has not written it to the memory of the SIM card. Clicking on the field opens the settings of this SIM card.
- **SIM 2** — displays the number of the SIM card installed. If the phone number is displayed as an **Unknown number**, the operator has not written it to the memory of the SIM card. Clicking on the field opens the settings of this SIM card.

### SIM card settings

**APN, Username, and Password** — settings for connecting to the Internet via a SIM card. To find out the settings of your cellular operator, contact your provider's support service. APN settings are applied only after successful connection with new parameters. If the connection attempt fails, the CIE continues to work with the previous APN settings.

👉 [How to set or change APN settings in the CIE](#)

**Mobile data usage.** The menu contains information about mobile traffic used by the Ajax system, allowing you to reset statistics and check the balance of the SIM card.

The data is calculated on the CIE and may differ from the operator's statistics. This is because each operator calculates incoming and outgoing traffic individually.

- **Incoming** — the amount of data received by the CIE. Displayed in KB or MB.
- **Outgoing** — the amount of data sent by the CIE. Displayed in KB or MB.



**Reset statistics** — resets statistics on incoming and outgoing traffic.

### Check balance

**USSD code.** Enter the code that is used to check the balance in this field. For example, \*111#. To send a request, after entering the code, click **Check balance**. The request result will be displayed under the balance check button.

### Access codes

Setting up keypad and CIE passcodes for users who are not registered in the system.

You can create a passcode for people who are not added to the space. This is convenient, for example, to grant service staff access to system management. Once they know the access code, they can log in using the Ajax keypad or the CIE.

To set up an access code for unregistered user:

1. Tap **Add code**.
2. Select **Access code**.
3. Set a **Title** and **Access code**.
4. Tap **Add**.
5. Tap **Back** to save the settings.

For each created access code, you can:

- Set up a duress code.
- Change the code and its ID.
- Set security management permissions (e.g., access to groups, Night mode etc.).
- Configure fire alarm system management access level.
- Temporarily disable or delete the code.

To make changes, select the code from the list.

The created access codes are valid for all keypads connected to the CIE. EN54 Fire Hub Jeweller supports up to 200 access codes.

The access code must contain 4 to 6 digits. Each digit can be any number from 0 to 9.

EN54 Fire Hub Jeweller supports over 1,000,000 passcode combinations.


 [How to manage security with access codes](#)

### Code length restrictions

This setting is only available in Ajax PRO apps.

Set the requirements for the length of passcodes that are used for users' authorization and access to the system. You can select **Flexible (4 to 6 symbols)** option or define the fixed code length: **4 symbols**, **5 symbols**, or **6 symbols**.

Note: when you set the fixed code length, the system resets all access codes configured before.

The fixed code length is required for the **Easy armed mode change** feature that allows disarming the system without pressing the  **Disarm** button on the keypad after entering a passcode or using an access device.

 [Learn more about Easy armed mode change](#)

### Detection zone test

Starts the [Detection zone test](#) for connected devices. The test allows you to check the operation of devices and their alarm detection zone.

### Jeweller

Setting the polling period between the CIE and connected devices. The settings indicate how often the CIE communicates with devices and how fast a connection loss is detected.

- **Device ping interval, sec** – the frequency of polling of connected devices by the CIE, set in the range from 12 to 300 seconds. The default value is 36 seconds.
- **Number of missed pings to determine connection failure** – counter of undelivered packets. The default value is 8 packets.

Do not decrease the default values of the ping interval and ping period unless it is necessary.

The time before sending a message regarding the loss of connection between the CIE and the device are calculated using the following formula:

$$\text{Detector ping interval} \times \text{Number of missed pings to determine connection failure}$$

The shorter the ping period, the faster the CIE will know about the events of the connected devices, and the devices will receive CIE commands. Information about alarms and sabotage is transmitted instantly, regardless of the ping interval. Decreasing the ping period will affect the battery life of wireless devices.

To comply with the EN 54-25 standard, the CIE must detect communication loss with connected devices in under 300 seconds. An admin or a PRO with system configuration rights can adjust the necessary parameters to meet this requirement.

 [Learn more](#)

The ping interval limits the maximum number of connected devices:

Interval	Connection limit
12 s	39 devices
24 s	79 devices
36 s (by default)	119 devices

48 s	159 devices
72 s	200 devices

Regardless of the ping period settings, up to 10 [intrusion sirens](#), or [keypads](#) with a built-in buzzer can be connected to EN54 Fire Hub Jeweller.

## Service

Group of CIE service settings. These are divided into two groups: general settings and advanced settings.

### General settings

#### Firmware update

This menu allows to manually check whether the new firmware version is available. If so, a PRO or a company with firmware update rights can initiate the update.

👉 [How OS Malevich updates](#)

#### Hub system logging

This setting allows you to select the transmission channel for the CIE logs or disable their recording:

- **Ethernet** – system logs are transmitted over the wired Internet.
- **Wi-Fi** – system logs are transmitted over the Wi-Fi.
- **Off** – logging is disabled.

Logs are files containing information about system operation. Do not disable the logs, as this information may be helpful in case of errors in the operation of the system.

👉 [How to send an error report](#)

#### Delaying notifications of external power loss

Settings for the delay time when sending an external power loss notification.

You can select a delay time from **1 minute** to **1 hour** with a selection interval of **1 minute**.

#### 'While hub offline' events amount

Events during communication failure with the server are recorded in the CIE buffer and will be delivered to Ajax apps after the connection is restored.

This setting allows you to choose the number of the last events, that CIE will send to Ajax apps after returning online.

You can select between **100** (default value) and **1000** events with increment of **50** events.

 [Learn more](#)

Also, all events, related to EN54 devices, are available in the CIE **Event log** that saves up to 10,000 events. To see the log on the CIE touch screen, go to the **Event center** tab → **Event log** tab.

### Advanced settings

The list of advanced CIE settings depends on the type of application: standard or PRO.

Ajax Security System	Ajax PRO
Server connection Sounds and alerts System integrity check	PD 6662 setting wizard Server connection Sounds and alerts System integrity check Alarm confirmation Restoration after alarm Arming/disarming process Devices auto deactivation LED indication

### PD 6662 setting wizard

Opens a step-by-step guide on how to set up your system to comply with the British security standard PD 6662:2017.

 [Learn more about PD 6662:2017](#)

 [System setup using PD 6662:2017](#)

### Server connection

Communication settings between the CIE and the Ajax Cloud server:

- **Delay of server connection failure alarm, sec.** The delay is necessary to reduce the risk of false notification of a lost connection with the Ajax Cloud server. Activated after 3 unsuccessful CIE–server polls. The delay is set in the range of 30 to 600 s. The recommended default value is 300 s.
- **Hub-server polling interval, sec.** Frequency of sending pings from the CIE to Ajax Cloud server. It is set in the range of 10 to 300 s. The recommended default value is 60 s.

The time before sending a notification regarding the loss of communication between the CIE and the Ajax Cloud server is calculated using the following formula:

$$(\text{Ping interval} \times 3) + \text{Time filter}.$$

With the default settings, Ajax Cloud registers the CIE loss in 8 minutes:

$$(60 \text{ s} \times 3) + 300 \text{ s} = 8 \text{ min}.$$

- **Get notified of server connection loss without alarm.** Ajax's apps can notify about the CIE-server connection loss in two ways: with a standard push notification signal or with an [intrusion siren](#) sound (enabled by default). When the option is active, the notification comes with a standard push notification signal.
- **Notify of connection loss over channels.** The Ajax security system can notify both the users and the security company about the loss of connection between the CIE and the Ajax Cloud server, even via one of the communication channels.

In the menu, you can select the communication channels via which the system will notify about the loss of connection (Ethernet, Wi-Fi, cellular), as well as the transmission delay of such notifications.

- **Loss notification delay, min** — time of the delay before sending the notification about the loss of connection via one of the communication channels. Set in the range from 3 to 30 minutes.

The time of sending a notification about the loss of connection via one of the communication channels is calculated using the following formula:

*(Ping interval × 3) + Time filter + Notification delay.*


## Sounds and alerts

The menu contains three groups of settings: intrusion siren activation parameters, siren after-alarm indication, and beep with keypad activation parameters.

### Siren activation parameters

**If lid of hub or any detector is open.** If enabled, the CIE activates the connected [intrusion sirens](#) if the body of the CIE, detector, or any other Ajax device is open.

**If in-app panic button is pressed.** If enabled, the CIE activates the connected intrusion sirens if the panic button was pressed in the Ajax app.

Disable the siren response to Ajax SpaceControl Jeweller panic button pressing in the key fob settings in the Ajax app (Devices → Ajax SpaceControl Jeweller → Settings .

**Restart alarm signal on triggering of each detector.** If enabled, each new alarm from the intrusion detector will restart the intrusion siren alarm. You can disable this setting so that the siren only reacts to alarm from the first triggered detector.

### Setting the siren after-alarm indication

This setting is only available in Ajax PRO apps.

The intrusion siren can inform about alarms in the armed system by means of LED indication. Thanks to this feature, users and passing patrols of security companies can see that the system was triggered.

👉 [Feature implementation in StreetSiren DoubleDeck Jeweller](#)

### Beep with keypad activation parameters

This setting is only available in Ajax PRO apps.

The keyboards connected to the CIE will emit an audible sound to inform of malfunctions. To activate the sound notifications enable toggles: **If any device is offline** and **If the battery of any device is low**.

### System integrity check

This parameter is responsible for checking the state of security detectors, devices and **followed groups** before arming the system. **System integrity check is disabled by default**.

👉 [Learn more](#)

### Alarm confirmation

This setting is only available in Ajax PRO apps.

This is a special event that the CIE sends to the monitoring station: and system users if several devices specified by the admin have triggered within a specified period of time.

By responding to confirmed alarms, the security company and the police reduce the number of visits on false alarms.

👉 [Learn more](#)

### Restoration after alarm

This setting is only available in Ajax PRO apps.

The feature does not allow arming the system if an alarm has been registered previously. To arm the system, an authorized user or PRO should restore it. The types of alarms that require system restoration are defined when configuring the function.

The function eliminates situations when the user arms the system with detectors that generate false alarms.

👉 [Learn more](#)

### Arming/disarming process

This setting is only available in Ajax PRO apps.

The first **Compliance with standard** option allows selecting a specific standard to set the security system according to existing requirements. Once you select the required standard, the menu will show the appropriate arming/disarming settings below. The following standards are available:

- **EN 50131** — European standard for intrusion and hold-up alarm systems, which also describes the security grades concept.

- **PD 6662** – British standard for intrusion and hold-up alarm systems, aimed to reduce the number of unconfirmed alarms and ensure police reaction only to real threats.
- **VdS** – German standard for intruder and hold-up alarm systems, which regulates arming/disarming process.
- **ANSI/SIA CP-01-2019** – American standard for security systems that regulates features and requirements to reduce false alarms caused by users or equipment.

## EN 50131


Once **EN 50131** is activated, you can set the parameters of the functions **Two-stage arming**, **Exit time restart**, and **Exit error** in the arming settings, as well as set the **Alarm transmission delay** in the disarming settings.

👉 [How to configure an Ajax system according to the EN 50131 requirements](#)

## PD 6662

Once **PD 6662** is selected, the menu shows the number of arming/disarming settings that allow configuring the system to comply with standard requirements.

👉 [Learn more about the PD 6662 standard](#)

Use the corresponding step-by-step guide in the Ajax PRO app for a quick and convenient system setup according to **PD 6662**. Go to EN54 Fire Hub Jeweller → Settings  → Service → **PD 6662 setting wizard** and follow the app prompts.

## VdS

Once **VdS** is selected, all devices in the system operate without delay when leaving, but entry delays will still work.

The system automatically checks that all doors and locks are closed. The door is locked with the third-party **Blocking element** when arming the system. Additionally, the system checks whether the door is blocked to ensure that the system is armed according to the unavoidability principle (German: Zwangsläufigkeit).

The system can't be armed if it has malfunctions. If there are any malfunctions or the door is not locked, the system notifies of the unsuccessful arming event.

👉 [Learn more](#)

## ANSI/SIA CP-01-2019

An Ajax system controlled by the hub with [OS Malevich 2.19](#) or higher can be configured following the requirements of ANSI/SIA CP-01-2019.

Only [Hub 2 \(4G\) Jeweller](#) and [Hub 2 Plus Jeweller](#) are certified according to ANSI/SIA CP-01-2019.

Once **ANSI/SIA CP-01-2019** is selected, you can configure **Exit time restart** and **Unvacated premises** for the arming settings. For the disarming settings, you can select what devices should make an annunciation on **Alarm cancellation** or **Alarm abort** and adjust the **Alarm abort window** timeout.

Also, this standard requires enabling a number of features for the system, such as **Delay when entering/leaving**, **cross zoning\***, **Devices auto deactivation**, and **system testing**. These features are configured in the CIE and certain device settings.

👉 [How to set up the ANSI/SIA CP-01-2019 compliant system](#)

\* The **cross zoning** functionality will be available in the next OS Malevich updates.

### Devices auto deactivation

This setting is only available in Ajax PRO apps.

The function allows you to ignore alarms and/or other device events without removing them from the system. Events of disabled devices will not be sent to the monitoring station and system users.

There are three types of **Devices auto deactivation**: by timer, by number of alarms and by number of similar events. It is also possible to manually deactivate a specific device.

👉 [Learn more about deactivating devices manually](#)

👉 [Learn more about auto deactivation of devices](#)

### User guide

When pressed, opens the EN54 Fire Hub Jeweller user manual in the Ajax app.

### Transfer settings to another hub

Menu for automatically transferring devices and settings from another CIE. Note that you are in the settings of the CIE on which you want to import data.

👉 [Learn more](#)

### Scenarios and schedule

Scheduled arming/disarming settings. The security schedule can be used for individual groups and for the entire facility, as well as for the **Night mode**.



👉 [Learn more](#)

### Remove hub

Removes your account from the CIE. All settings, paired detectors, and devices, as well as invited users, are saved in the CIE memory.

👉 [How to delete the offline hub from armed space](#)



# CIE settings reset (coming soon)



Resetting the CIE to the factory settings:

- 1. Turn on the CIE if it is off.
- 2. Remove all users and installers from the CIE.
- 3. Hold the power button for 30 s.
- 4. Remove the CIE from your account.

## Space settings



Settings can be changed in the [Ajax app](#):



- 1. Select the space if you have several of them or if you are using a PRO app.
- 2. Go to the **Control**  tab.
- 3. Go to **Settings** by tapping the gear icon  in the center.
- 4. Set the required parameters.
- 5. Tap **Back** to save the new settings.










 [How to configure a space](#)

## Indication

EN54 Fire Hub Jeweller informs users of fire-related system states via its display, built-in buzzer, and LED indicators located on the front panel of the CIE enclosure. In case of a fire alarm, fault, device disablement, or test, the CIE display shows an appropriate screen. It includes details such as the cause of the alarm (e.g., smoke, heat, or manual call point activation), the location, room, and zones in alarm. The display also indicates whether the alarm signal was sent to the monitoring station and shows the current states of Ajax EN54 sounders and VADs.



Indication	Event	Note
The built-in buzzer emits a short sound	Tapping the display.	
 lights up continuously	An external power supply is connected to the CIE.	
 blinks; <b>01-40</b> Fire zones indicator lights up continuously;	A fire alarm occurred.	Fire zone indicators light up according to the zone number where fire is detected or a manual call point is pressed.

The built-in buzzer beeps continuously.		
 lights up continuously; <b>01–40</b> Fire zones indicator lights up continuously.	The CIE built-in buzzer was muted after a fire alarm had occurred.	Fire zone indicators light up according to the zone number where fire is detected or a manual call point is pressed.
 blinks;  The built-in buzzer beeps continuously.	A fault occurred.	The CIE or connected Ajax EN54 devices have a fault.  If connected, the system alerts the monitoring station.
 lights up continuously.	The CIE built-in buzzer was muted after a fault had occurred.	
 blinks;   blinks;  The built-in buzzer beeps continuously.	A system fault occurred.	The CIE has a hardware issue (e.g., the display is broken). Contact the <a href="#">Ajax Technical Support</a> for assistance.  If configured, the system alerts the monitoring station.
 lights up continuously;   lights up continuously.	The CIE built-in buzzer was muted after a system fault had occurred.	
 lights up continuously.	A test of Ajax EN54 devices in fire zones is in progress.	
 lights up continuously.	Some Ajax EN54 devices connected to the CIE are fully or partially disabled.	
All LED indicators light up, and the built-in buzzer emits sound for 7 seconds.	Indication test is in progress.	

## Indication test

To run the indication test of the CIE and ensure it functions properly:

1. Go to the **Control** tab on the CIE display.
2. Tap **Indication test**.
3. Ensure that the built-in buzzer is sounding and all CIE LED indicators are lit. During the test, the names of the LED indicators will appear on the display for 5 seconds. Then, the display will turn green for 2 seconds.

If the CIE does not perform as described during the indication test, please contact [Ajax Technical Support](#)

for assistance.

## Additional features

### Video surveillance

EN54 Fire Hub Jeweller is compatible with [Ajax cameras and NVRs](#) and with third-party cameras that support RTSP protocol or SDK integration.

👉 [How to connect cameras to the Ajax system](#)

You can calculate the number of cameras and NVRs that can be added to the space using the [video device calculator](#).

### Scenarios

EN54 Fire Hub Jeweller allows creating 64 scenarios and minimizing the human factor impact on safety. The CIE can manage the security of the entire facility or group according to a schedule; activate the smoke machine if intruders enter the room; de-energize the room and turn on emergency lighting in case of fire; shut off water in the event of a leak; control lighting devices, electric locks, roller shutters, and garage doors – when changing the security mode by pressing a button or by a detector alarm.

Scenarios can be used to reduce the number of routine actions and increase productivity. Ajax automation devices respond to changes in temperature and air quality. For example, configure the heating to turn on at low temperatures, control the supply system, humidifier, and air conditioner to maintain a comfortable climate.

👉 [How to create and customize a scenario](#)

### Photo verification

EN54 Fire Hub Jeweller supports both MotionCam and MotionCam Outdoor motion detectors. When triggered, the detectors take a series of shots you can use to evaluate the unfolding of the events at the facility over time. This relieves users of unnecessary anxiety and prevents security companies from sending unnecessary patrol dispatches.

The detector activates the camera when armed and detects movement. Only users with access to the events feed, as well as authorized employees of the security company, can see visual alarm verifications provided that the security system is connected to the monitoring station.

If **Photo on demand** function is activated, the detectors can take a photo upon the command of a system user or PRO user with the appropriate rights. The taking of a photo is always registered in the CIE events feed in the Ajax app.

The shots are protected by encryption at every stage of transmission. They are stored on the Ajax Cloud server and are not processed or analyzed.

[Learn more](#)

## Selecting the installation site

Visual with an example of the CIE installation

The CIE is designed for indoor installation only. It is recommended to install it in a visible and easily accessible location – for example, near the entrance on the first floor of the building. This helps ensure timely response to a fire alarm, quick identification of the fire location, and informed decisions about evacuation.

Install the CIE on a vertical surface. This will ensure proper tamper button response if someone attempts to remove the device. Refer to the [battery documentation](#) before installation. Note that incorrect positioning may accelerate battery degradation.

Choose a location where the CIE can access all available communication channels: Wi-Fi, Ethernet, and two SIM cards. Ensure that the cellular signal at the installation site is stable and reaches at least 2–3 bars. Correct device operation is not guaranteed if the cellular signal is weak.

When selecting the installation site, consider the distance between the CIE and wireless devices, as well as any obstacles that may interfere with radio signal transmission, such as walls, intermediate floors, or large objects in the room.

To roughly calculate the signal strength at the place of installation of wireless devices, use our [radio communication range calculator](#). Note that if the signal strength is excellent, the device can automatically adjust the power of radio transmission to reduce power consumption and radio interference.

Run the Jeweller and Wings signal strength tests before final installation. The test checks the signal strength at the device's maximum transmission power. To comply with the EN 54 requirements, the signal strength between the device and the CIE has to be three bars. With a signal strength of one or zero bars during the test, we do not guarantee stable operation of the system.

If the system has devices with signal strength of 1 or 0 bars, consider relocating the CIE or device. If this is not possible or the device still has low or unstable signal strength after being moved, use [EN54 Fire ReX Jeweller](#).

We recommend laying out power or signal cables inside the wall. Otherwise, use the [GlandBox](#) wiring accessory with 20 mm cable glands (not included) for external cable routing.

### Where EN54 Fire Hub Jeweller cannot be installed

1. Outdoors. This could result in device failure.
2. Near metal objects and mirrors. They can cause attenuation or shielding of the radio signal. This could result in the loss of connection between the CIE and wireless Ajax devices.
3. In places with high levels of radio interference. This could result in the loss of connection between the CIE and wireless Ajax devices or false notifications about [security system jamming](#).
4. Less than 1 meter away from the router and power cables. This could result in the loss of connection between the CIE and wireless devices.
5. Less than 1 meter away from Jeweller devices. This could result in the loss of connection between the

CIE and these devices.

6. In places where the CIE will have a signal strength of 1 or 0 bars with connected devices. This could result in the loss of connection between the CIE and these devices.
7. Inside premises with temperature and humidity beyond the [permissible limits](#). This could result in a failure of the CIE.
8. In places with no cellular signal or 1 bar signal strength. We do not guarantee correct operation of the device with a low cellular signal strength.

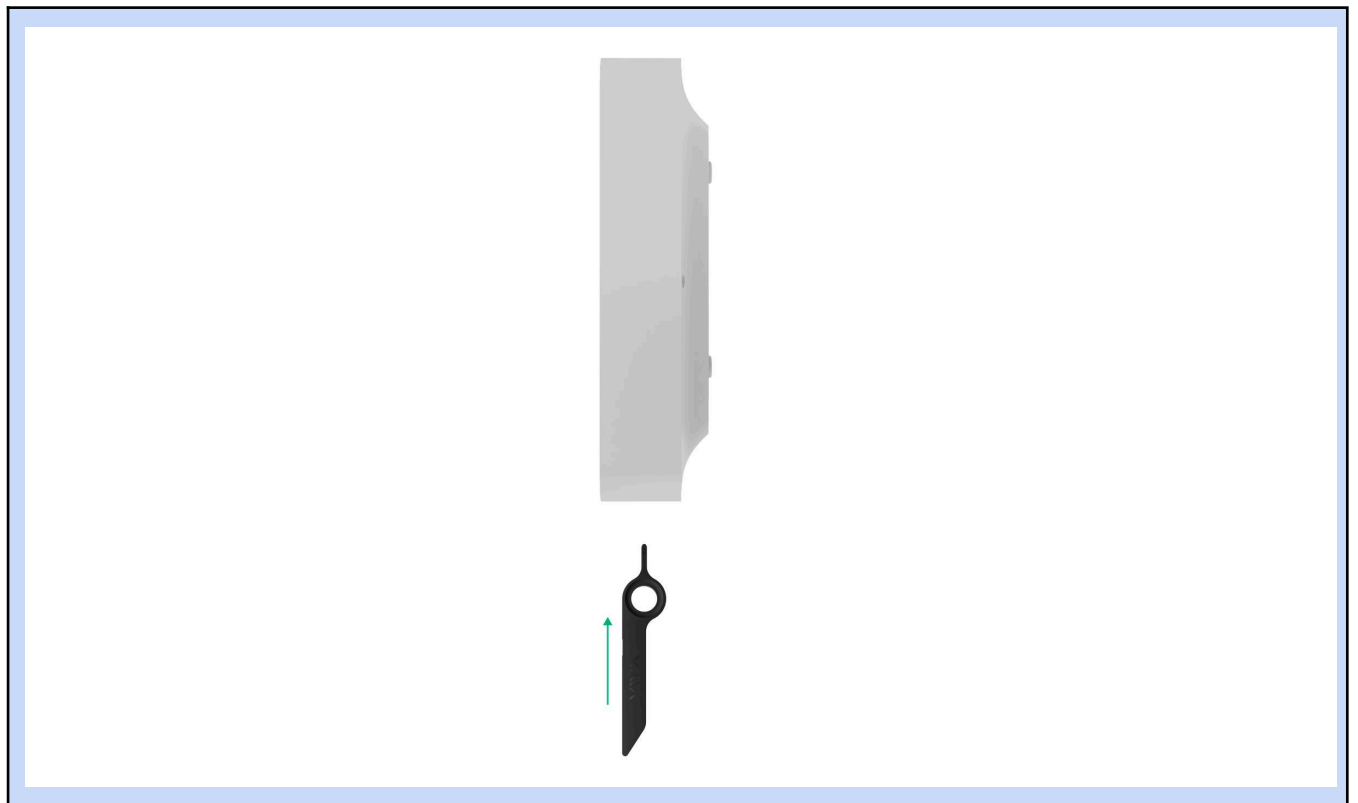
## Installation

During installation and operation of the Ajax system, adhere to the rules and requirements of regulatory legal acts on electrical safety. Do not disassemble the device while it is energized or use it with a damaged power cable. **Observe the safety procedures and the rules for electrical installation work when connecting the CIE and wired devices.**

Before installing EN54 Fire Hub Jeweller make sure that you have selected the optimal location and that it meets the requirements of this manual.

### To install EN54 Fire Hub Jeweller:

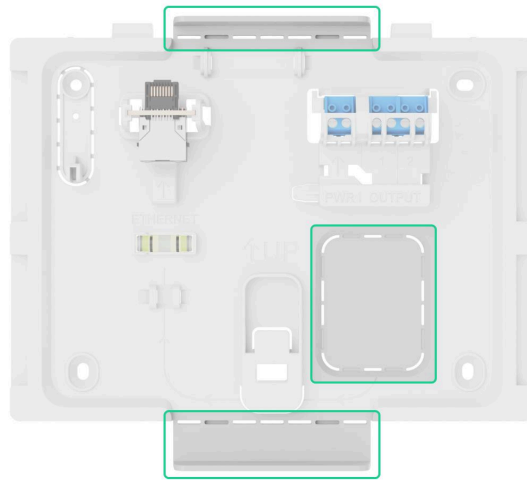
1. Remove the SmartBracket mounting panel from the device. To do this, insert the special tool into the hole, and slide the mounting plate down.



2. Carefully break out the necessary perforated part to output the cable from the rear side (top, bottom, or through the wall).

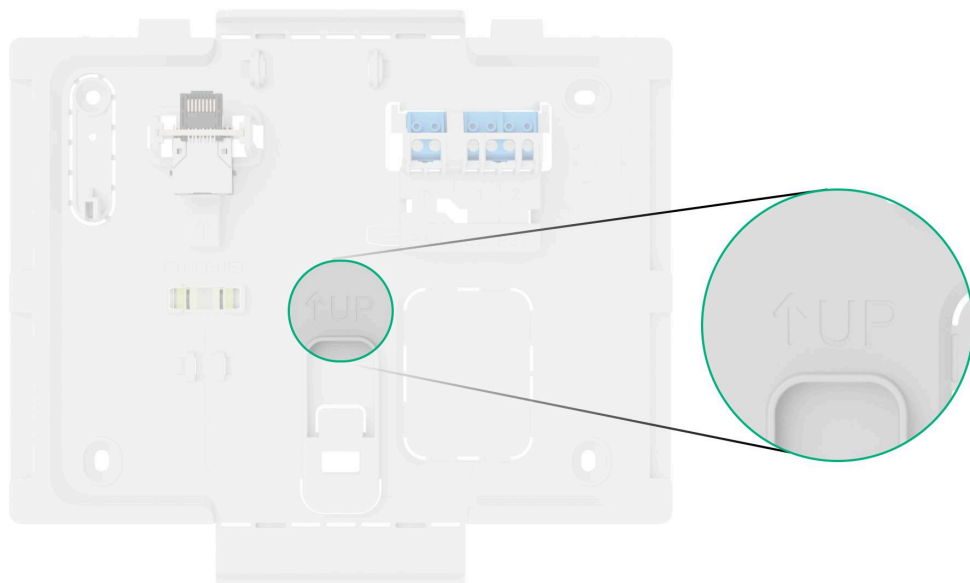
If you are not routing cables inside the wall, use the [GlandBox](#) wiring accessory with red cable glands (not included).

## 👉 How to install GlandBox



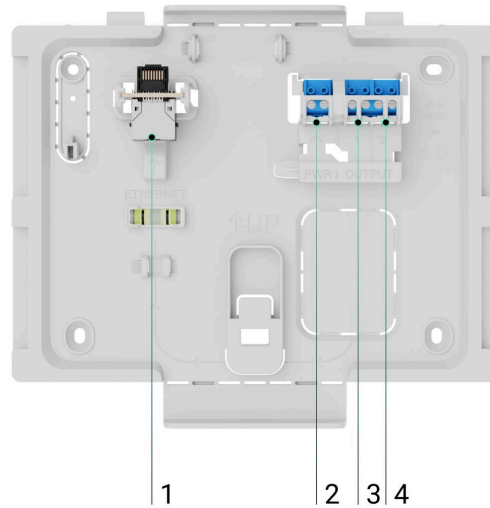
3. Run the power, Ethernet, and optionally signal cables into the CIE enclosure.
4. Secure the SmartBracket mounting panel to a vertical surface at the selected installation site using the bundled screws at all fixation points. One of them is in the perforated part above the tamper button – it is required for tamper alarm triggering in case of any attempt to detach the device.

The **UP** key on SmartBracket marks the top of the device. Orient these markings when installing the CIE. Also use the bubble level to check the inclination angle of the mount during installation.



5. Connect the Ethernet, external power cable, and optionally signal cables to the appropriate connector and terminals.

Selecting the cables for connecting to power supply and relay outputs, adhere to the rules and requirements of regulatory legal acts on electrical safety.

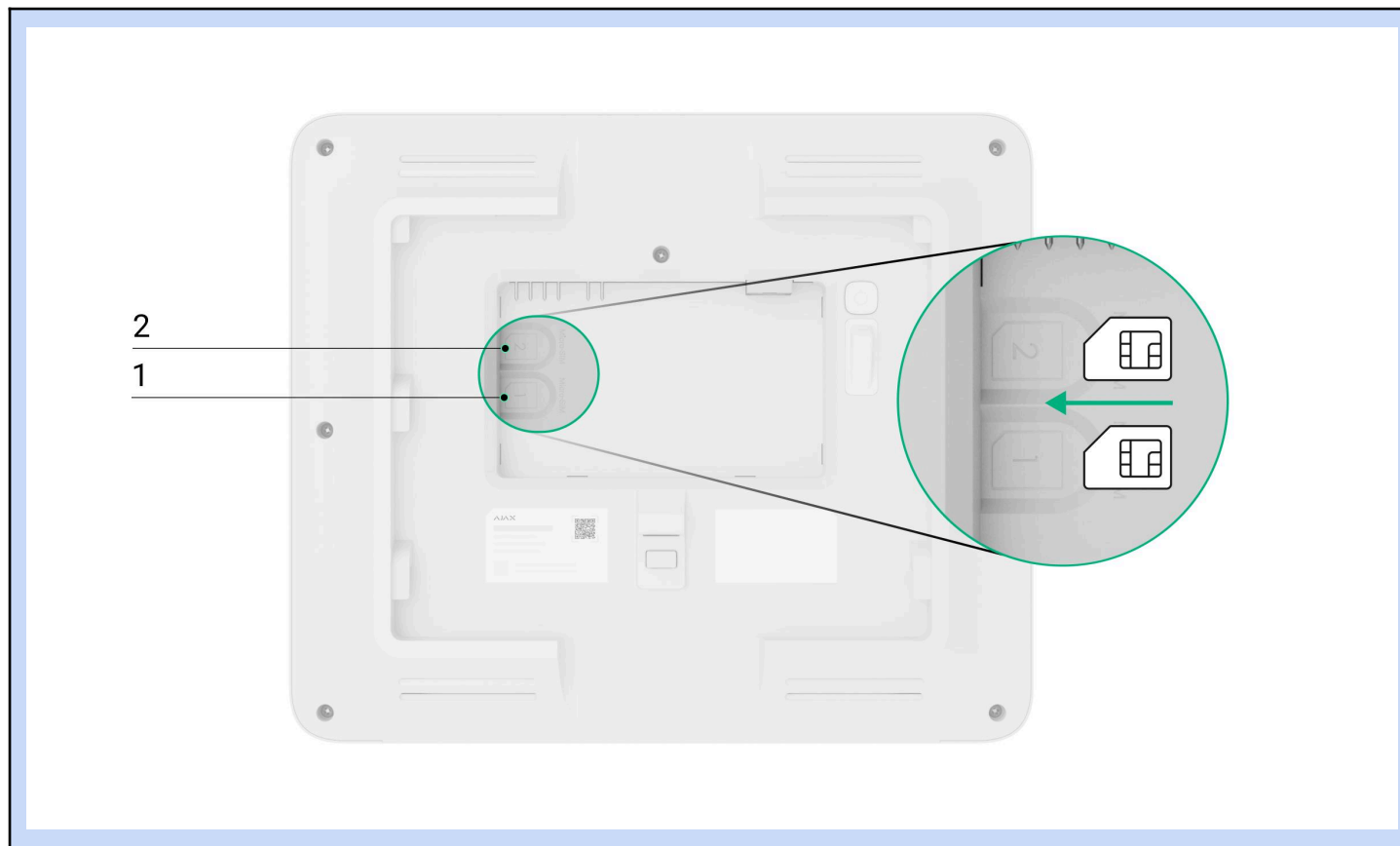


- 1 – Ethernet cable connector.
- 2 – terminals for connecting external power supply 110–240 V, 50/60 Hz.
- 3 – relay output for connecting the signal cable for sending events to the monitoring station in case of any fault in the system.
- 4 – relay output for connecting the signal cable for sending events to the monitoring station in case of in case of fire alarm.

6. Install the internal battery.

Use only EN54 Internal Battery (24h) or EN54 Internal Battery (72h). We do not guarantee correct device operation with third-party batteries, and they can cause the CIE to fail.

## 7. Install SIM cards:



1 – the first micro SIM slot.

2 – the second micro SIM slot.

### 8. **Add the CIE to a space.**

9. Place the turned on device on the SmartBracket mounting panel.

10. Switch on the external power supply, if the power cable was de-energized previously.

11. Check the status of the CIE in an [Ajax app](#). If a tamper alarm is indicated, ensure that the mounting panel is closed tightly.

12. Run the CIE [indication test](#).

## If Ethernet connection fails

If the Ethernet connection is not established, disable proxy and MAC address filtration and activate DHCP in the router settings. The CIE will automatically receive an IP address. After that, you can assign a static IP address to the CIE in the Ajax app.

## If SIM connection fails

To connect to the cellular network, you need to install a micro SIM card with a PIN code request disabled and a sufficient amount of funds on the account to pay for services as per the operator's tariff. To disable the PIN code request, insert the SIM card into the phone.

If the CIE fails to connect to the cellular network, use Ethernet to configure the network parameters: roaming, APN access point, user name, and password. To find out these parameters, contact the support service of your mobile operator.

👉 [How to set or change APN settings in the CIE](#)



# Zone management

## How to disable or enable EN54 devices

A user with Access level 2 can disable EN54 devices in fire zones. Information that some devices are disabled is shown on the CIE **Control** tab, and in the **Event center** tab → **Fault, test or disablement** tab.

To provide the device disablement or activation:

### With the CIE

1. Log in using an access code, or present Tag/Pass to the reader (coming soon) on the CIE front panel.
2. Go to the **Fire zones** tab.
3. Tap zone, where you want to disable/enable devices.
4. If you want to disable a particular device, tap **Open device list**, and select the device. Tap **Disable device** or **Enable device**, choose its sensors or annunciation devices you want to enable/disable (e.g., heat sensor, VAD, or sounder).
5. If you want to enable/disable all sensors or annunciation devices in a particular zone, tap **Disable zone devices** or **Enable zone devices**. Select sensors, sounders, and VADs you need to enable or disable.
6. Tap **Save**.



A zone in which devices are partially or completely disabled will be marked correspondingly in the **Fire zones** tab.


### In Ajax apps

1. Open an [Ajax app](#).
2. Log in to your account.

👉 [How to create the Ajax personal account](#)

👉 [How to create the Ajax PRO account](#)

3. Go to the **Devices**  tab.
4. Find EN54 Fire Hub Jeweller in the list, and select the **Fire zones** menu.
5. Select the fire zone.
6. Select the device.
7. Go to its **Settings** .
8. Tap **Device disablement**.
9. Choose what device function to disable or enable (e.g., sound alarm signal, high temperature detection etc.).
10. Tap **Save**.
11. Go back to the device list of zone, or to the list of zones.
12. Repeat steps from 5 to 10 for other devices you need to enable/disable.

All devices added to the CIE are also available from the **Devices**  tab.

## How to run an alarm annunciation test

An admin, PRO, or user with **access level 2** can run an alarm annunciation test of EN54 devices. The test allows checking the sound and visual alarm signals, and to ensure that fire alarm signals are clearly audible and visible within the premises. It runs for up to 10 minutes and can be stopped earlier if needed. Information

that some devices are in test mode is shown on the CIE **Control** tab, and in the **Event center** → **Fault, test, or disablement** tab.

To run the test:

#### With CIE



1. Log in with your personal or access code, or apply Tag/Pass to the reader on the CIE front panel.
2. Go to the **Fire zones** tab.
3. Select zone, where you want to run the test.
4. Tap **Open device list**, and select the device.
5. Tap **Run alarm annunciation test**.
6. Choose annunciation devices you want to test.
7. Tap **Start test**.
8. To stop the test, repeat steps from 2 to 4, and tap **Stop active test**.


#### In Ajax apps

1. Open an [Ajax app](#).
2. Log in to your account.

👉 [How to create the Ajax personal account](#)

👉 [How to create the Ajax PRO account](#)

3. Go to the **Devices**  tab.
4. Find EN54 Fire Hub Jeweller in the list, and select the **Fire zones** menu.
5. Select the fire zone.
6. Select the device.
7. Go to its **Settings** .
8. Tap **Alarm annunciation test**.
9. Select what you want to test.
10. Tap **Start**.
11. Go back to the device list of zone, or to the list of zones.
12. Repeat steps from 5 to 10 for other devices you need to test.
13. To stop the test, tap **Stop** in each device **Alarm annunciation test** setting.

All devices added to the CIE are also available from the **Devices**  tab.

## Maintenance

Check the functioning of EN54 Fire Hub Jeweller and connected devices on a regular basis. The optimal frequency of checks is once every three months. Clean the device enclosure from dust, cobwebs, and other contaminants as they emerge. Use a soft, dry cloth that is suitable for equipment care.

Do not use substances that contain alcohol, acetone, petrol, and other active solvents to clean the device.

## Technical specifications

👉 [All technical specifications](#)

👉 [Compliance with standards](#)

# Warranty

Warranty for the Limited Liability Company "Ajax Systems Manufacturing" products is valid for 2 years after the purchase.

If the device does not operate properly, we recommend contacting Ajax Technical Support first. In most cases, technical issues can be resolved remotely.

👉 [Warranty obligations](#)

👉 [User Agreement](#)

## Contact Technical Support:

- [email](#)
- [Telegram](#)
- phone number: **0 (800) 331 911**

Manufactured by "AS Manufacturing" LLC