

Ajax PRO Desktop User Manual

Updated October 7, 2022

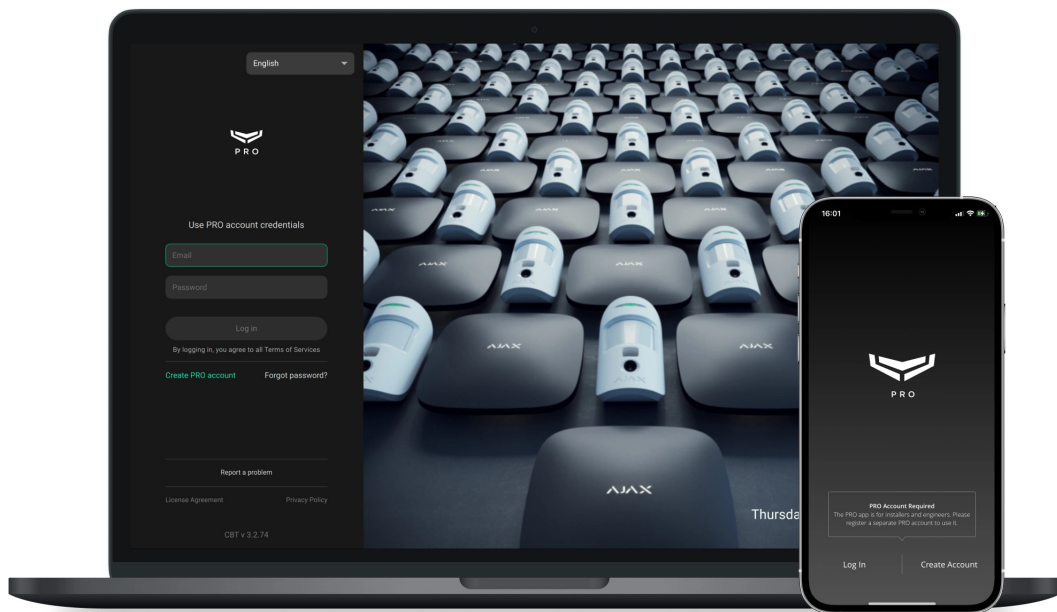


Ajax PRO Desktop is the app for monitoring and administering Ajax security systems. Allows you to configure and test devices, manage user access, and monitor and process events and alarms of an unlimited number of Ajax security systems.

PRO Desktop can be used in parallel with the PRO mobile app. Installation and service companies can use the app to set up and connect security systems, while security and monitoring companies can use it to organize a Central Monitoring Station (CMS).

[Download PRO Desktop](#)

Ajax PRO apps types and their capabilities



There are two types of Ajax PRO apps: desktop and mobile.

The PC PRO app is PRO Desktop. This app is available for Windows and macOS. In the PC app, you can create companies, manage their settings, add employees, and manage their rights. PRO Desktop is essential for monitoring and remote configuring of Ajax security systems.

The mobile PRO app is Ajax PRO: Tool for Engineers. This app is available for smartphones with iOS and Android. It allows installers to connect hubs and manage the settings of available systems.

	PRO Desktop (PC app)	Ajax PRO: Tool for Engineers (mobile app)
Connect devices and set up the system	+	+
Connect the hub to the company	+	+
Create a company	+	—
<u>More about companies</u>		
Edit company information	+	—
Add employees	+	—
<u>More about employees</u>		
Change employee rights	+	—

More about employee rights		
Events and alarms monitoring More about monitoring	+	-

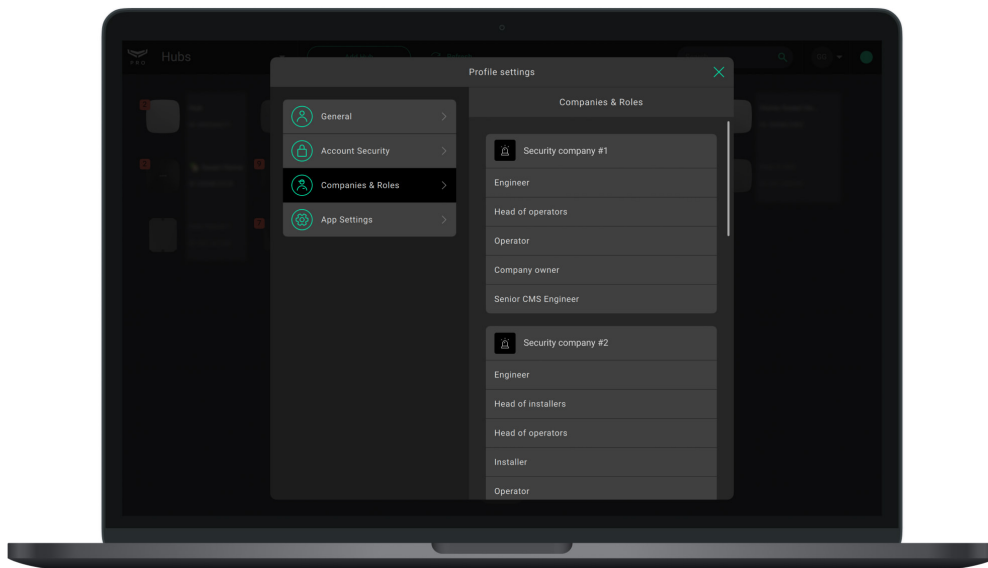
[More about Ajax apps](#)

General information

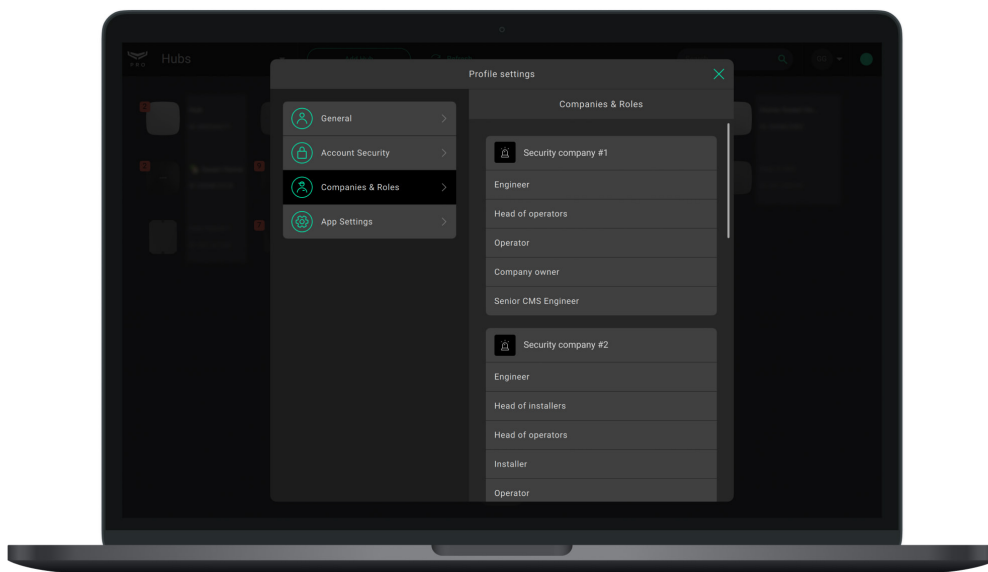
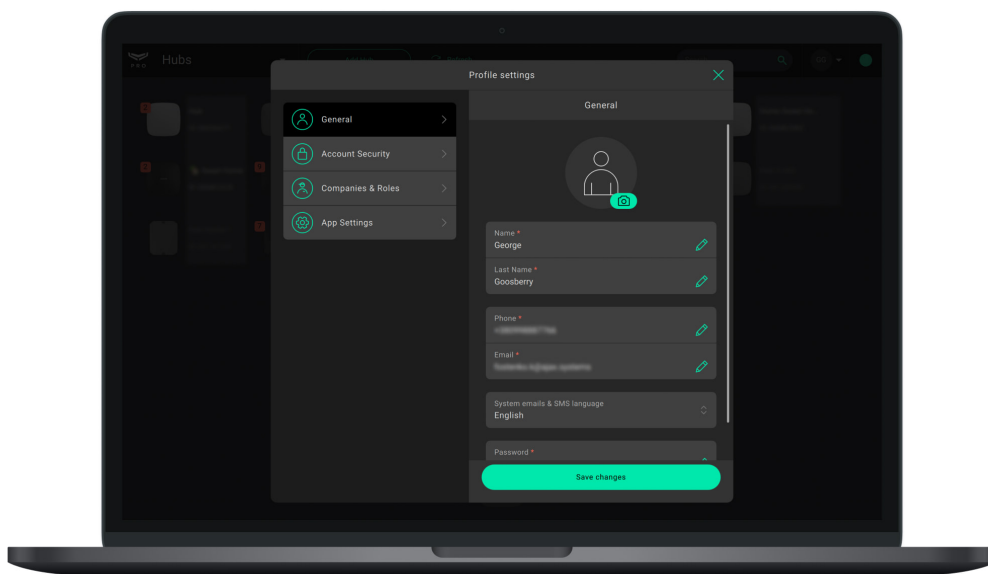
One company connected to the hub is one user. Regardless of how many employees (PRO accounts) are assigned to this company. Any number of companies can be connected to the hub within the user limit. The limit (maximum number of users) depends on the hub model.

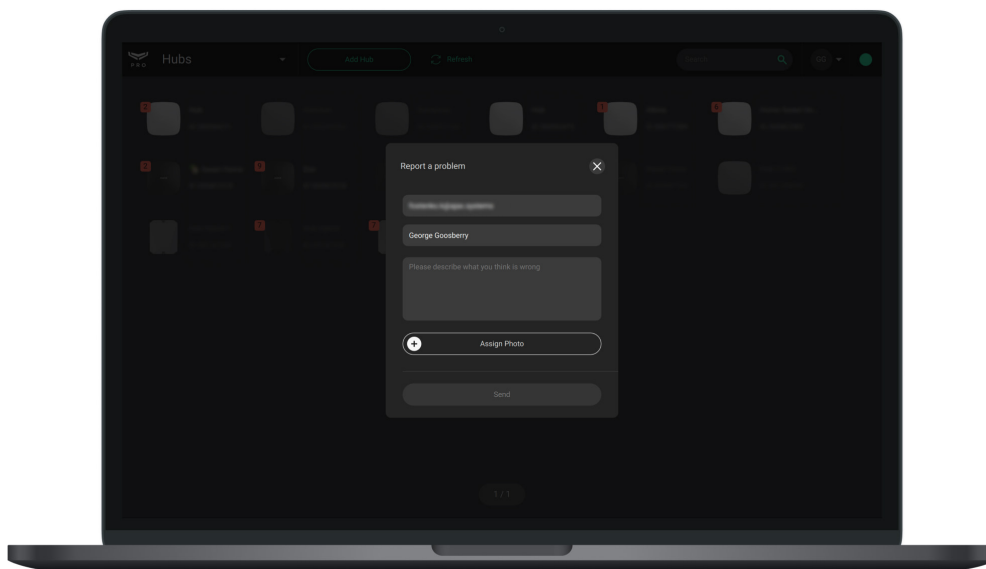
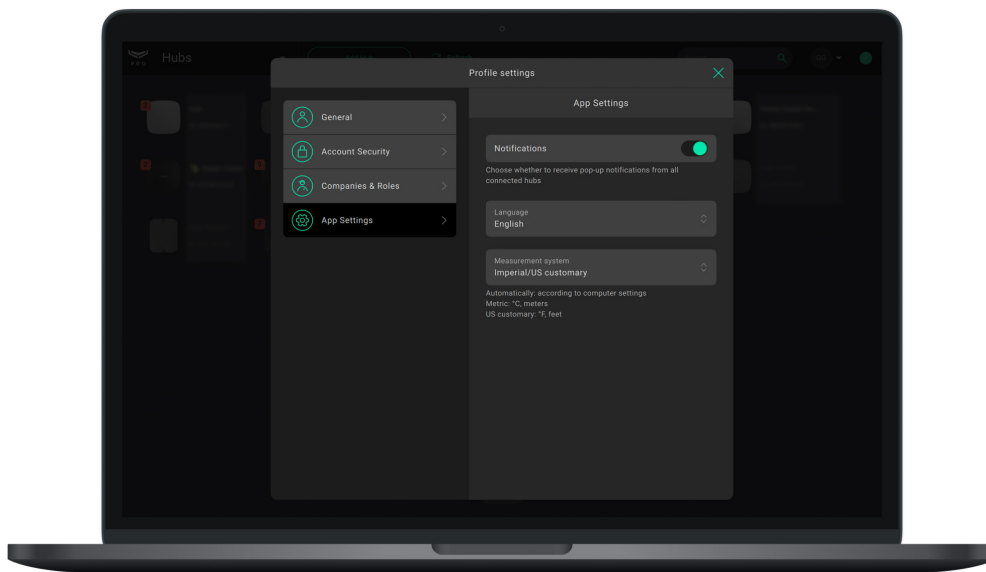
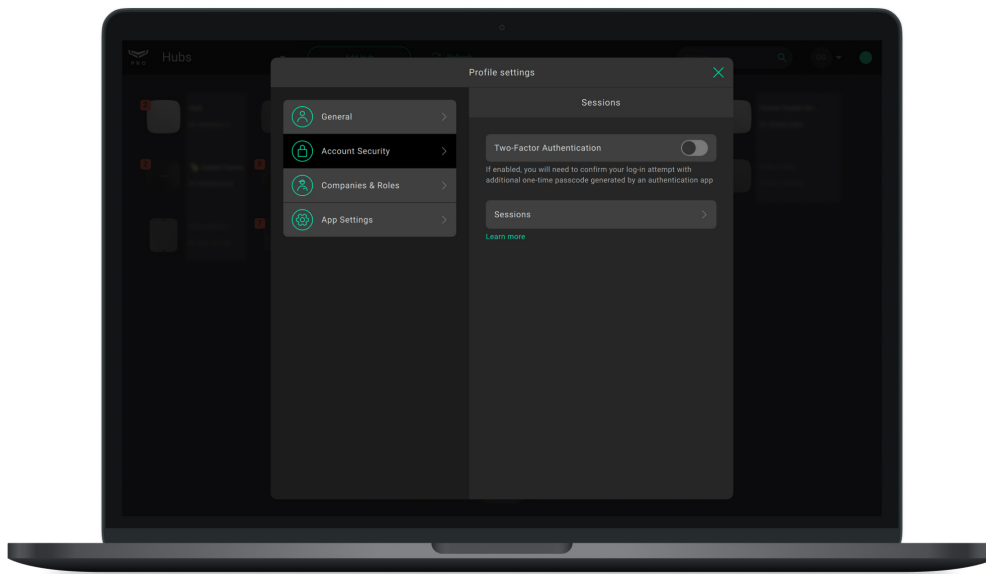
[Comparison of hubs](#)

PRO accounts can be connected to an unlimited number of companies. PRO accounts can have different roles in different companies. For example, the role of Installer in one company, and the role of Head of installers in another one.



When you log in again after closing the app, you should use the login and password from the PRO account. If two-factor authentication is enabled for a PRO account, it will need to be passed during logging in.





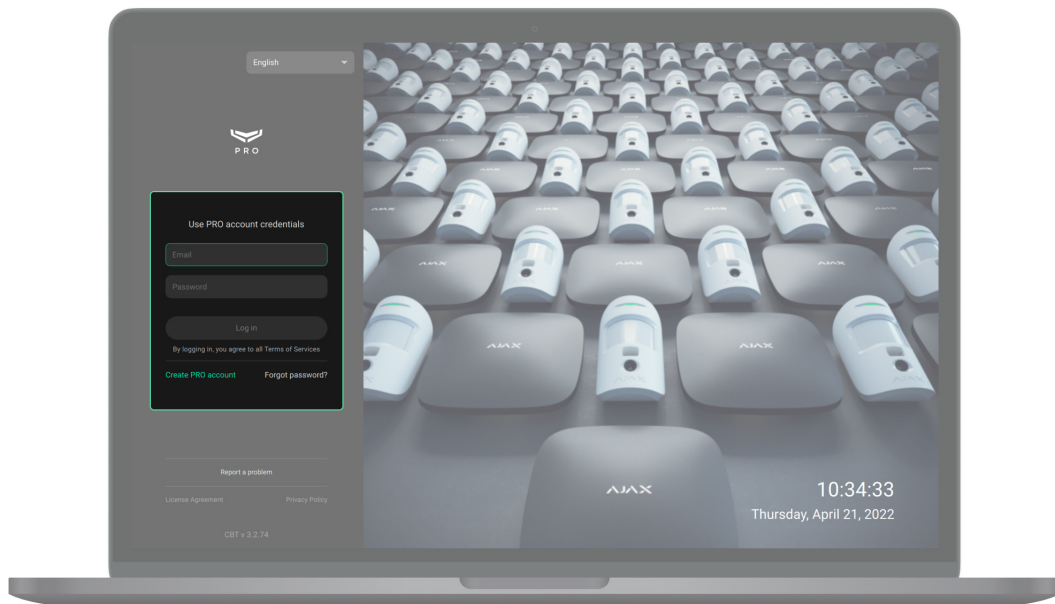
To report a bug, change PRO Desktop settings, view information about the PRO account, log out or change its settings – click on the menu with the company logo or the PRO account initials.

Installing PRO Desktop app

1. [Download the app installation file.](#)
2. Open the downloaded file.
3. Install PRO Desktop.

Creating the PRO account and logging into the app

To log in to PRO Desktop, you need the PRO account. The account should be registered in any of these two apps: PRO Desktop or Ajax PRO: Tool for Engineers. You can't log in to the PRO app with a username and password from the [Ajax Security System](#) app for end users. PRO account is different from the account created in the end-user app.



If you have a PRO account: fill in the **Email** and **Password** fields, and then click **Login**.

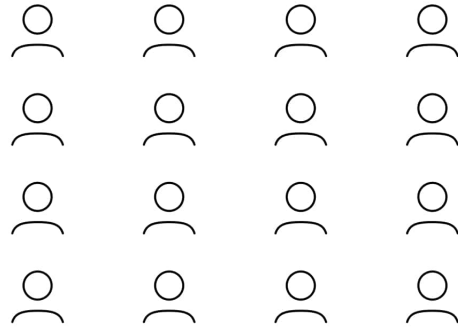
If you don't have a PRO account: click **Create PRO account** in PRO Desktop or Ajax PRO: Tool for Engineers and follow the instructions in the app. When creating a PRO account, you can use the same email and phone number as in the account of the Ajax Security System app. These will be different accounts.

[How to create a PRO account](#)

Account types



Personal PRO account



Company account

Two types of accounts are available in Ajax PRO apps: a personal PRO account and a company account.

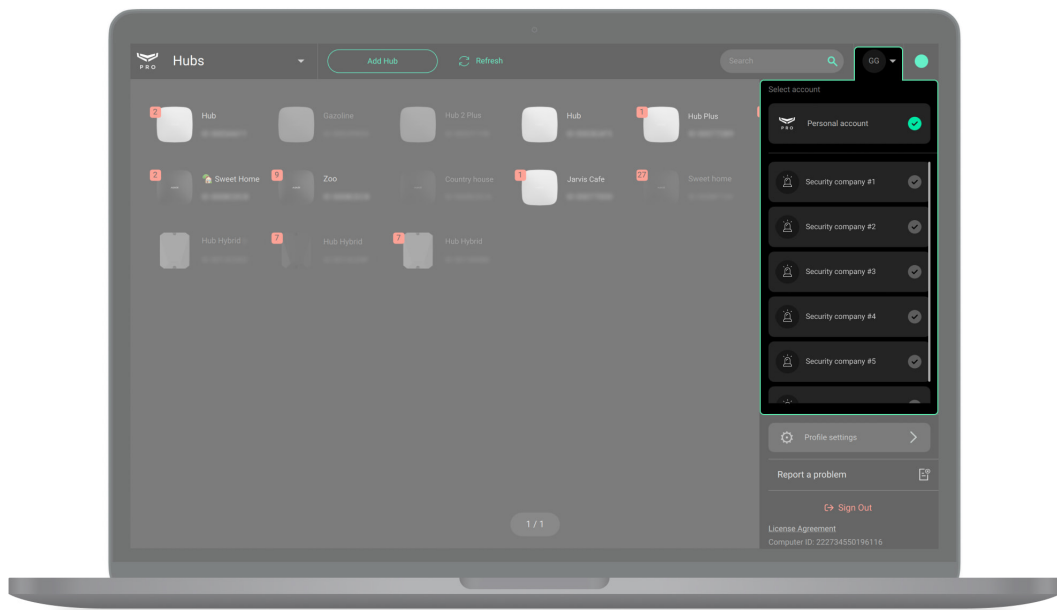
A personal PRO account is needed to connect to companies, as well as to set up and manage connected Ajax security systems.

Company accounts are required for running the security business: monitoring alarms and events, maintenance, configuring, and installing Ajax security

[More about PRO account](#)

[More about company account](#)

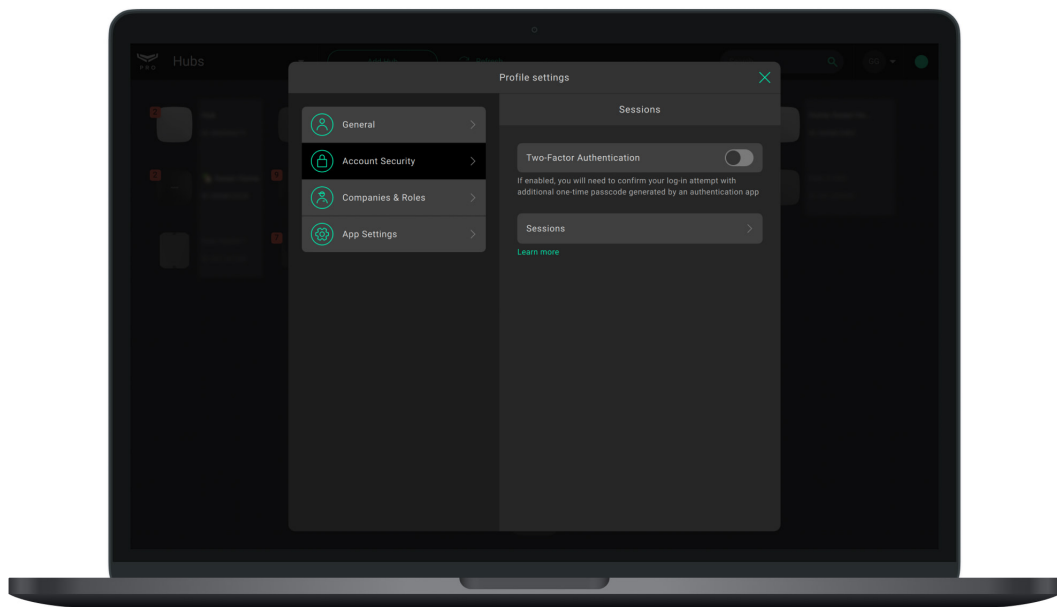
Switching between a personal PRO account and a company account



When you enter the app, the company the PRO account worked the last time with is automatically opened. To go to a personal PRO account or an account of another company:

1. Click on the menu with the security company logo or initials.
2. Select a personal PRO account or a company account.

Account security

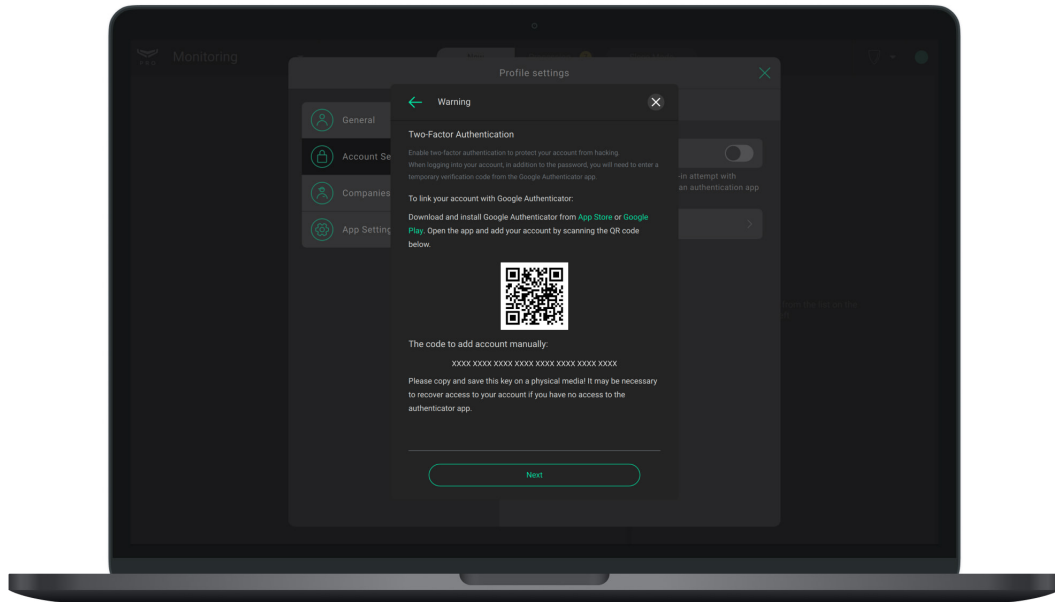


To protect the PRO account from hacking set up two-factor authentication and track sessions on other devices. Use both security tools to reduce the chances of unauthorized access to your PRO account.



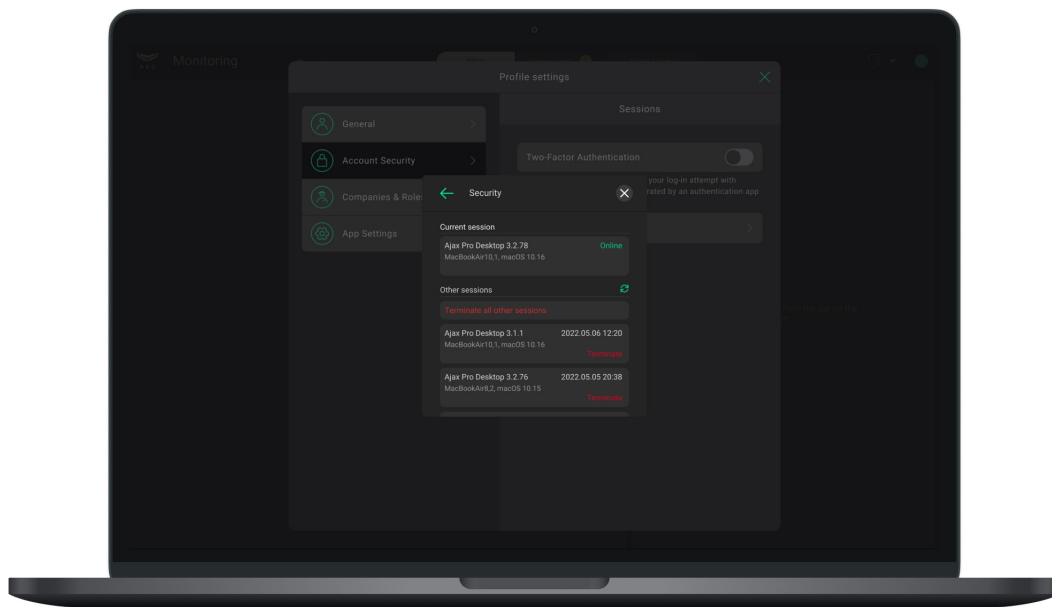
Change your password and enable two-factor authentication when rogue account sessions are detected.

How to enable the two-factor authentication



1. Click on the avatar (icon) of the PRO account.
2. Go to the **Profile Settings** menu.
3. Select the **Account Security** tab.
4. Enable the **Two-factor authentication** option.
5. Connect the authenticator following the instructions on the screen. For example, the Google Authenticator app.

How to terminate an account session

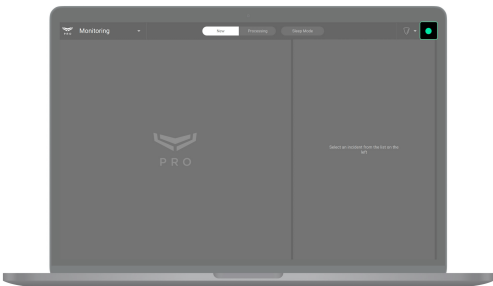
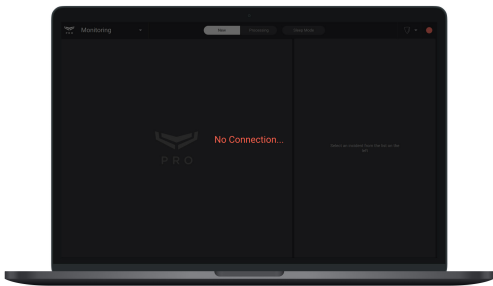


1. Click on the avatar (icon) of the account.
2. Go to the **Profile Settings** menu.
3. Select the **Account Security** tab.
4. Click on **Sessions**.

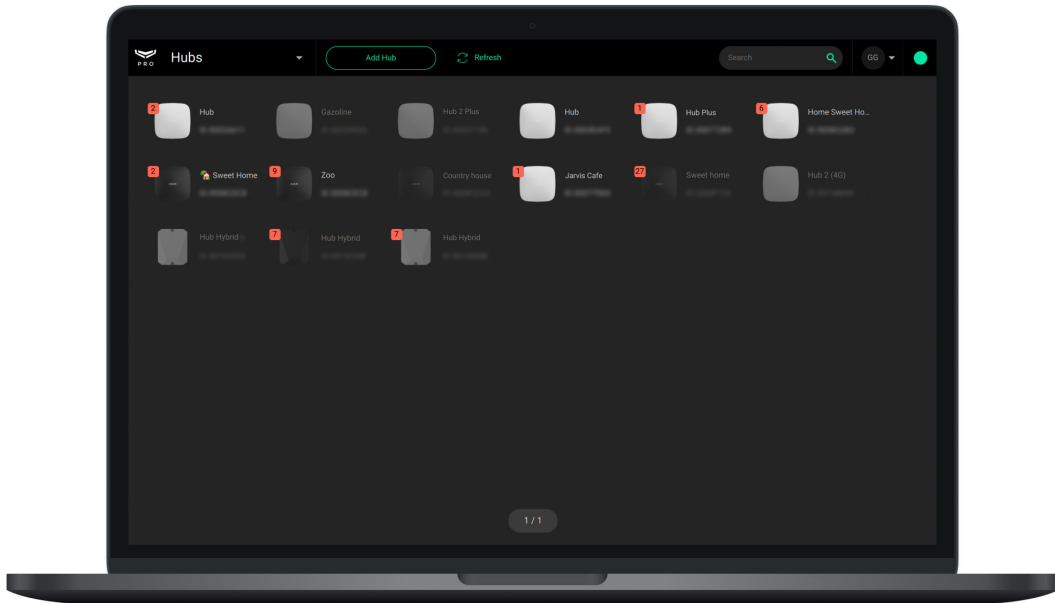
The session of the device from which you entered the app is called the **Current session**. **Other sessions** of devices from which the PRO account is logged in are available below. You can end a session by clicking **Terminate**, or **Terminate all other sessions** except the current one.

State of connection to the Ajax cloud

The indicator in the upper right corner of the PRO Desktop screen shows the connection status with the Ajax Cloud server. If the Internet connection is active, the indicator lights green. If there is no connection, it is red, and the message **No connection** is displayed on the screen.

Connection to Ajax Cloud is active	No connection to Ajax cloud
	

Working with a personal PRO account



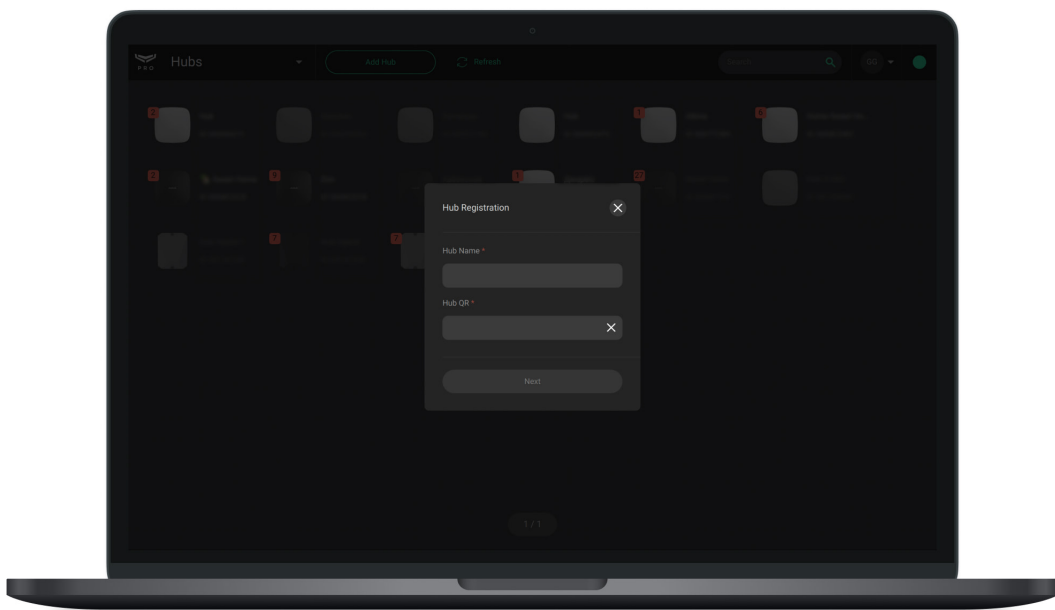
When you log in, a list of hubs linked to the PRO account opens. Hubs with which there is no connection are marked with a red caption **Offline**. The faults counter (red icon with a number) shows the total number of faults and unread events for a specific security system.



When pressed, the **Refresh** button updated the states and fault counters of the connected hubs. Automatic updating of hub states is not provided.



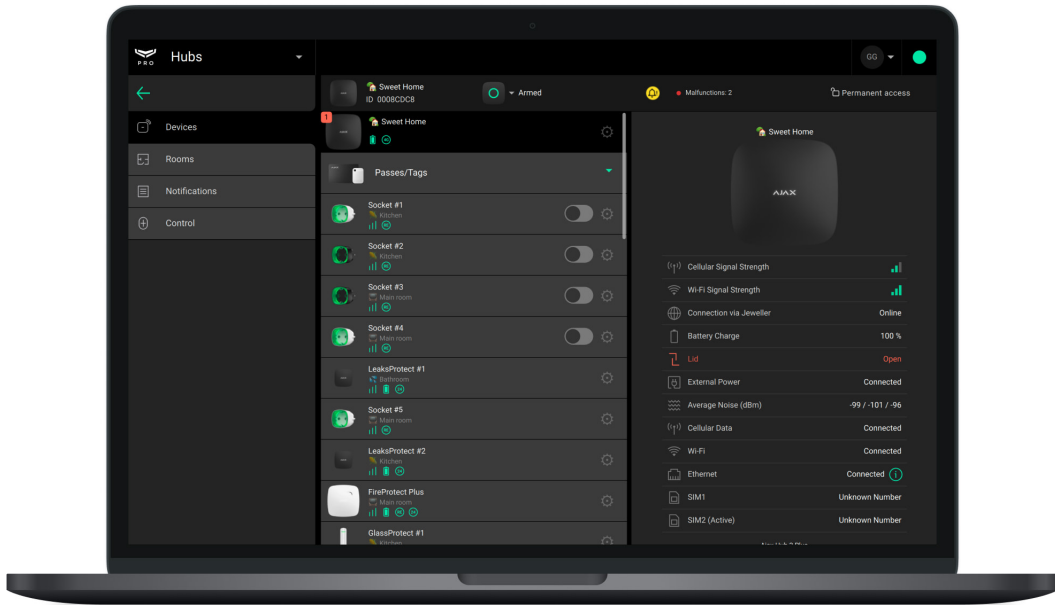
Finding the hub. The app has a search by name and by hub identifier (ID). Hubs are displayed as you type a text.



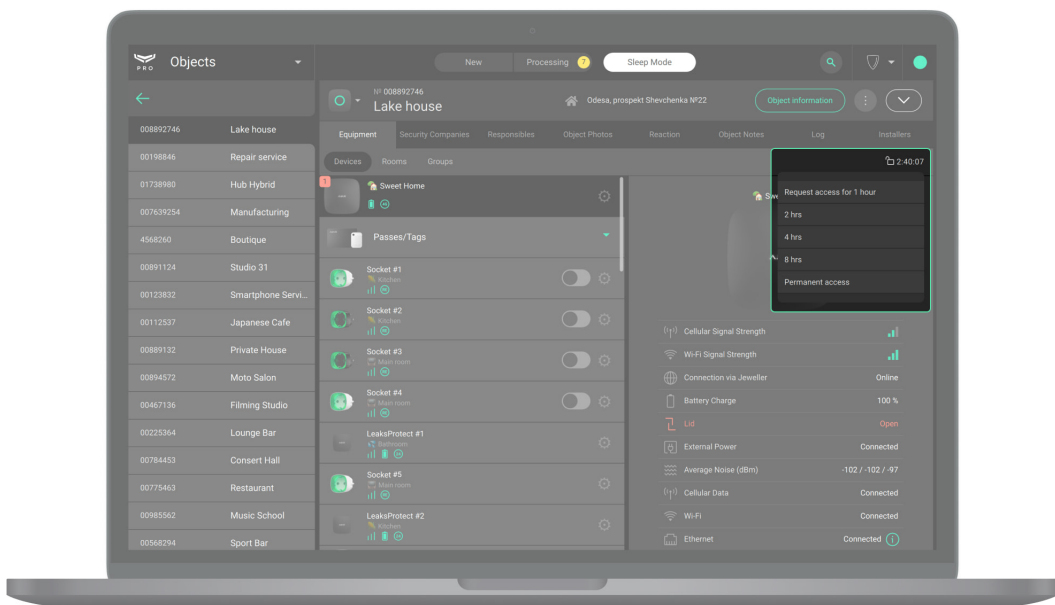
The **Add Hub** button allows you to link a new hub to a PRO account.

How to link a hub to an account

Security system menu



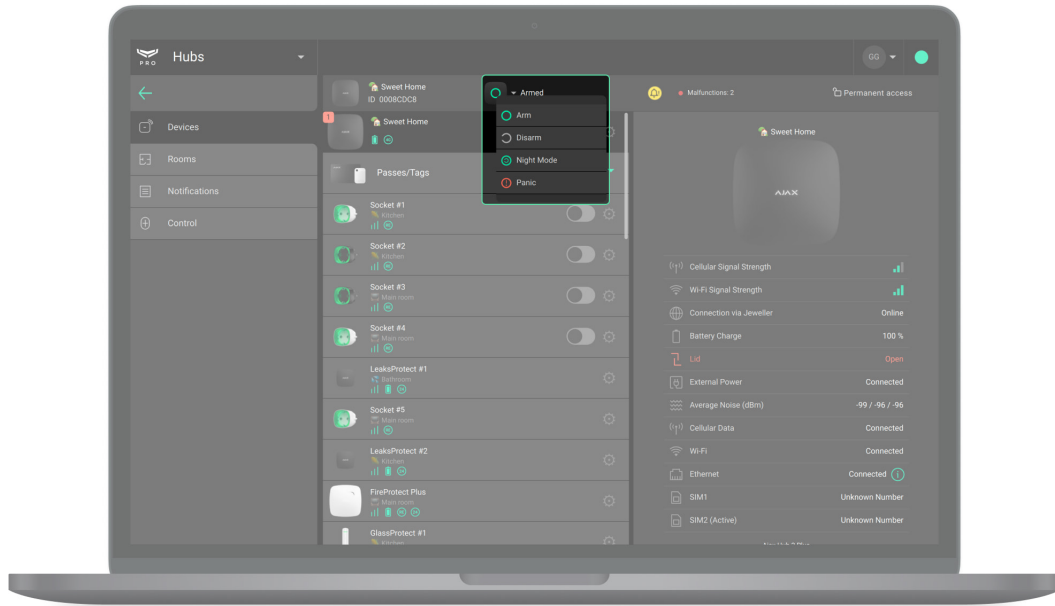
The menu contains rooms, devices, a notifications feed, and object security control buttons. The **Hubs** button returns to the list of linked hubs.



The PRO account can have temporary or permanent access to system settings. The field indicated in the screenshot shows the time during which the PRO account has access to the settings. Click on the field and select the required option to request temporary or permanent access. The request can be

confirmed by the hub administrator or another PRO account with the right to configure the system.

How to request access to hub settings





A PRO account can manage the object security modes if such a right has been granted to it by the hub admin, or another PRO account with rights to configure the system. The field indicated in the screenshot displays the security status of a specific Ajax security system. By clicking on the field, you can change the security mode or press the **Panic button**, if the PRO account is entitled to do so.

Setting up the security system

Change hub or device settings

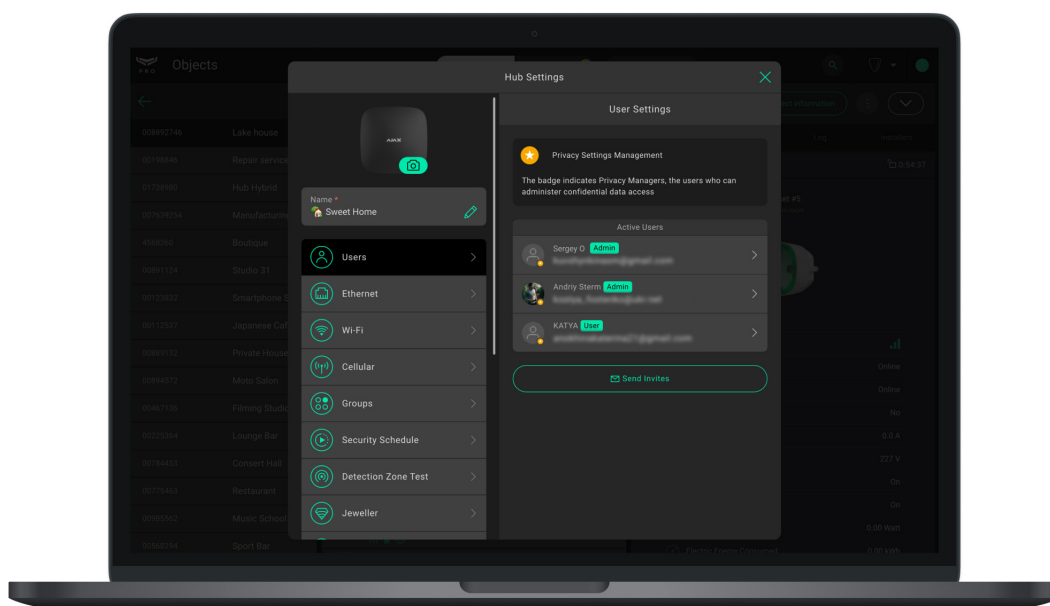


1. Go to the **Devices** menu .
2. Select the device from the list.
3. Go to its **Settings** .
4. Make changes.



All device settings are described in the user manual of this device.

User management



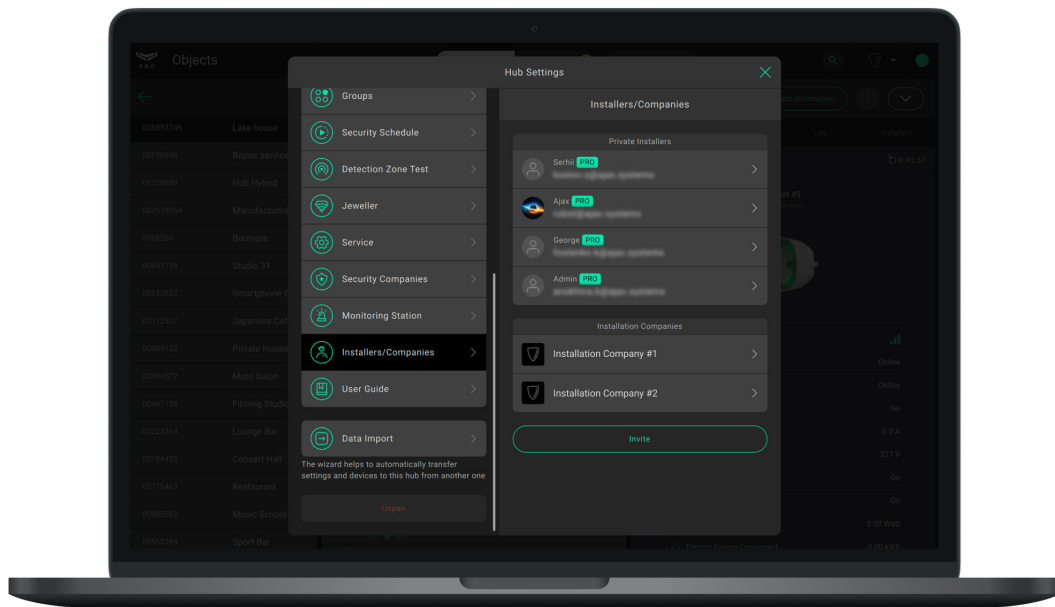
1. Go to the **Devices** menu .

2. Select the hub in the list of devices.
3. Go to its **Settings** ⚙️.
4. Select the **Users** menu.
5. Make changes: add a user, change their permissions, or delete them.

Ajax security systems user permissions

How to add a new hub user

PRO account management



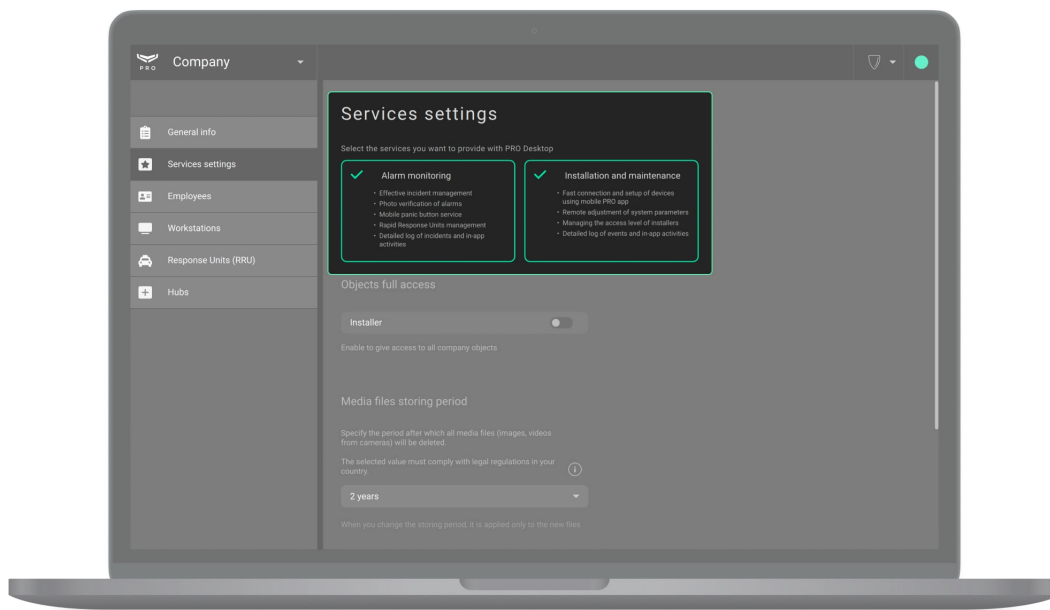
1. Go to the **Devices** menu 📱.
2. Select the hub in the list of devices.
3. Go to its **Settings** ⚙️.
4. Select the **Installers** menu.
5. Make changes: add a PRO account, change its rights or delete it.

How to add a PRO account to the hub

Working with a company account

A company account combines all security objects, employee accounts, and teams of rapid response units (RRU) in one interface.

Company service types

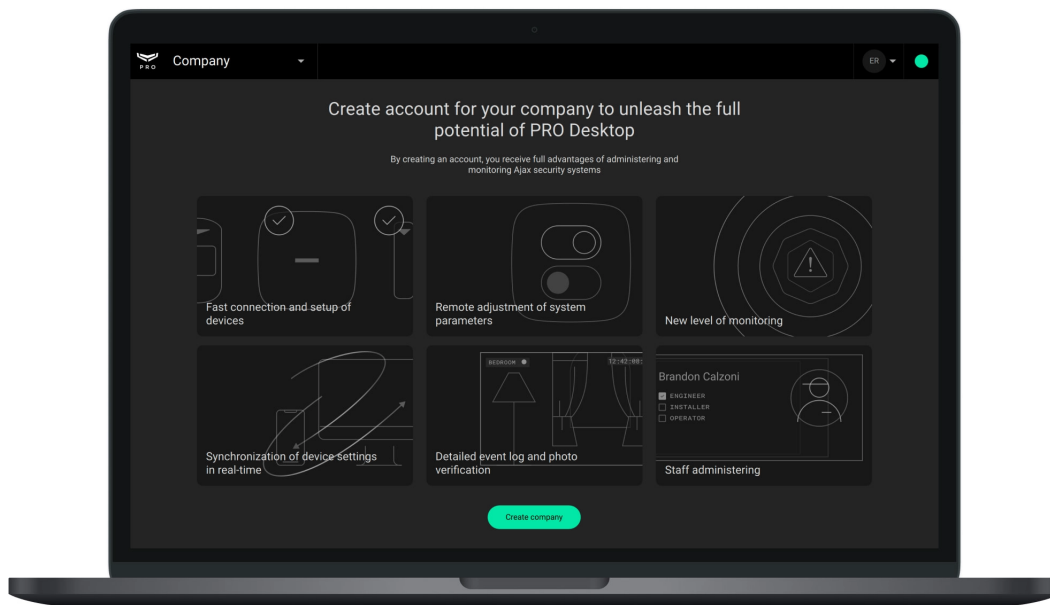


PRO Desktop is an integrated tool for security, installation and service business. The app has a set of functions for both **Alarm monitoring** and **Installation and maintenance**.

The set of functions is selected independently. The app also allows you to select both types of services at once: **Alarm monitoring** and **Installation and maintenance**. This is provided for companies that simultaneously install security systems and respond to their alarms and events.

The owner specifies the types of services when registering the company and can change them at any time. The interface and functions of the app adapt to the selected type of service.

Creating a company



The PRO account that created the company becomes the Company owner. Such a PRO account has access to all PRO Desktop modules, can add and remove employees, as well as change information about the company. One PRO account can create an unlimited number of companies.



The role of the Company owner can be assigned to one PRO account only. Only the Company owner or an authorized employee should create the company. Deleting the company or changing the Company owner is not provided.

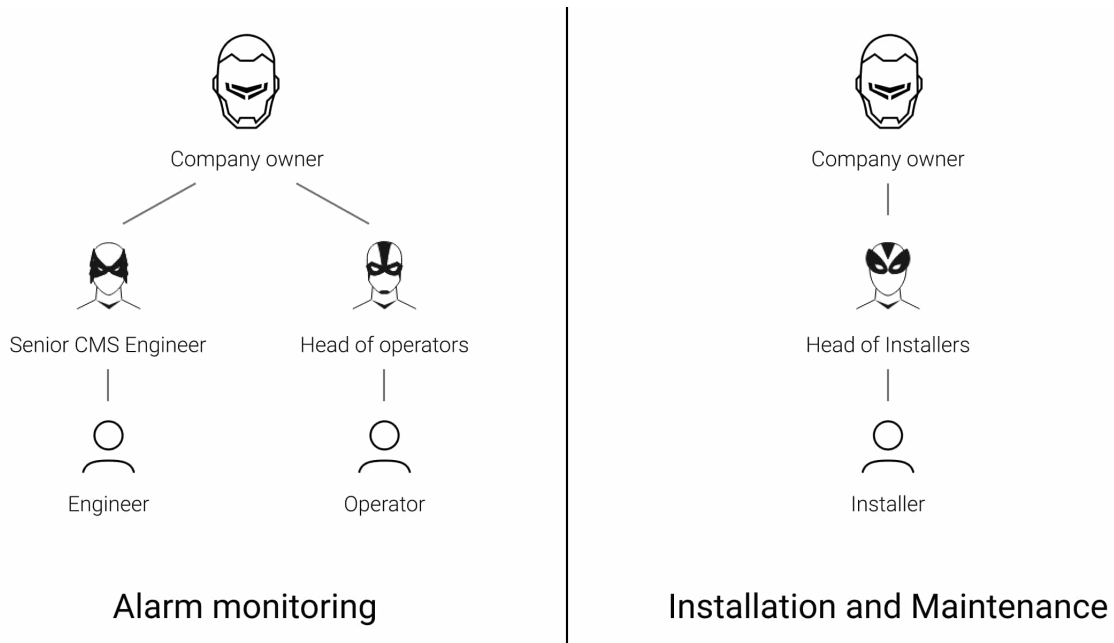
To create a company:

1. Open PRO Desktop.
2. Sign in to a PRO account.
3. Go to a personal PRO account if a company account is open.
4. Go to the **Company** module.
5. Click **Register a company**.
6. Specify the type of service the company provides: alarm monitoring, installation and maintenance, or both.
7. Fill in company information and follow the app's instructions.

In the registration form, enter an available and working email address. A validation code will be sent to the owner's email to complete the company

creation. This code should be entered at the last step of registration. After validation, the company is created automatically. You don't need to wait for additional confirmation.

Employees



You can add employees or change the roles of already connected PRO accounts in the **Employees** menu (**Company** module → **Employees** menu). You can only add an employee who already has a PRO account. An account can be registered in any of these two apps: PRO Desktop or Ajax PRO: Tool for Engineers.

Employee Roles

If the **Alarm monitoring** service type is selected:

1. Company owner
2. Senior CMS Engineer
3. Engineer
4. Head of operators
5. Operator

If the **Installation and Maintenance** service type is selected:

1. Company owner

2. Head of Installers

3. Installer

If both service types are selected: All employee roles are available.

Employee rights and access

	Company owner	Senior CMS Engineer	Engineer	Head of operators	Operator
Company module	+	+	+	+	View RRU menu
General info menu	View/Edit	View	View	View	–
Employees menu	View/Edit	View/Edit	Limited View/Edit (other engineers only)	Limited View/Edit (operators and head of operators only)	–
Workstations menu	View/Edit	View/Edit	View/Edit	View/Edit	–
Response Units menu	View/Edit	View/Edit	View/Edit. Without the ability to remove RRU	View	View
Objects module	View/Edit/arm	View/Edit/arm	View/Edit/arm	View/Arm	View/Arm

Journal module	View	View	View	View	View
New incidents menu in the Monitoring module	View	View	–	View	View
Processing menu	View/Edit	View/Edit	–	View/Edit	View/Edit incidents in the processing
Sleep Mode menu	View/Edit	View/Edit	–	View/Edit	View/Edit
Edit Company owner information	+	–	–	–	–
Add, edit or remove the Senior CMS Engineer	+	+	–	–	–
Add, edit or remove the Engineer	+	+	–	–	–
Add, edit or remove the Head of operators	+	+	+	–	–
Add, edit or remove the Operator	+	+	+	+	–
Add, edit or remove the Head of installers	+	+	–	–	–
Add, edit or remove the Installer	+	+	–	–	–
View incidents	–	–	–	+	+

					Only incidents of this operator
Process incidents	–	–	–	+	+
Control Sleep Mode	–	+	+	+	+ If incidents of this hub are not being processed
Set up events of operators (Operator offline and login from an unverified computer)	–	–	–	+	–
Arm and enable the Night mode	–	+	+	+	+
Disarm and disable Night Mode	–	–	–	–	–
Manage system settings (for example, hub settings)	–	–	–	–	–
Add and edit	+	+	+	–	–

RRU						
Delete RRU	+	+	-	-	-	
Change information about an object	-	+	+	-	-	t
Cancel the object monitoring	-	+	+	-	-	
Cancel the maintenance of an object	-	-	-	-	-	
Edit company information	+	-	-	-	-	
Enable/disable the Access to all objects option	+	+	-	-	-	
Manage media files storing period	+	-	-	-	-	
Manage installers' access to hub settings	-	-	-	-	-	
Confirm monitoring request	-	+	+	-	-	
Work with hubs availability reports	-	+	+	-	-	
Work with operators	-	+	+	+	-	

availability reports					
Send a system recovery request	-	+	+	+	+
Confirm a system recovery request	-	-	-	-	-



Adding, editing, and deactivating employees



To add an employee, they should have a PRO account registered.

[How to create a PRO account](#)



To add an employee, in PRO Desktop:

1. Go to the **Company** module.
2. Go to the **Employees** menu.
3. Click **Add employee**.
4. Enter the email address the employee's PRO account is registered with.

5. Define the role of the employee.

6. Click **Add**.

After adding, the owner of the PRO account will receive a notification email. The employee adding will be recorded in the PRO Desktop event journal.

To edit the data or delete an employee's PRO account, select it in the list. A window with details and the **Edit** and **Delete account** buttons will appear on the right.



To find an employee, use sorting or search by name, phone, and email.



PRO Desktop allows you to temporarily deactivate an employee's PRO account without deleting it from the system – in case of holiday or sick leave. To do this,

turn the toggle against the employee's name to an inactive position. A temporarily deactivated employee does not have access to company modules in PRO Desktop.

PRO Desktop modules, menus, and capabilities

The app allows you to:

- Manage employee PRO accounts – **Company** module, **Employees** menu, **RRU** menu.
- Administer an unlimited number of Ajax security systems – the **Objects** module.
- Maintain a customer database of the object – the **Objects** module and **Hubs** menu in the **Company** module.
- Receive, distribute among operators and process Ajax security system alarms – **Monitoring** module.
- Assign workstations to operators – **Company** module, **Workstations** menu.
- Generate hub availability report or CMS operators availability report – **Journal** module.
- Coordinate the work of Response Units (RRU) – **Monitoring** module.
- Maintain a journal of events and alarms of security systems – the **Journal** module.

Company

Access to the module: *Company owner, Engineer, Senior CMS Engineer, Head of operators, Operator, Installer, Head of installers.*

The **Company** module contains menus and settings for the following tasks:

- **General Info** – to view information about the company. Only the company owner can edit.

- **Services settings** – to select the type of company services, the media files storing period, the level of access to objects and hubs, and other settings.
- **Employees** – to manage employee accounts.
Workstations – for accounting of computers (PCs) operators use for work. Helps to calculate the CMS availability and track the login of operators to the PRO account from third-party devices.
- **Response Units (RRU)** – to administer Rapid Response Teams.
- **Hubs** – to manage company hubs. The menu contains objects in [Translator](#) (if connected), requests for monitoring, and requests for removal from monitoring.


General info

The menu contains information about the company. The owner can change company details by clicking the Edit button. The app allows you to change all data about the company, except for the name. To change the company name, contact [Ajax technical support service](#).

Services settings

In the menu, you can set the type of services provided by the company and manage other system settings (access to objects, media files storing period, maintenance reports). The owner of the company chooses the type of company services when registering in the app and can change the type of services at any time.

Employee access to objects



By default, an employee with the **Installer** role has access to those objects that are assigned to them by the **Head of installers**. For the installer to be able to configure all objects connected to the company, the **Access to all objects** option should be enabled.

To do this, in PRO Desktop:

1. Go to the **Company** module.
2. Open the **Services settings** menu.
3. In the **Access to all company objects** field, enable the option for **Installers**.

Now the installer and the company have the same rights to configure all objects. The rights can be following:

- Permanent access to system settings.
- Temporary access: you can configure the system for a specified time, from 1 to 8 hours.
- No access to system settings.

Media files storing period

You can set the period after which all media files (images, videos from cameras) will be deleted. The new media files storing period only applies to files created

after changes.

Available storing period for media files:

1. 7 days.
2. 30 days.
3. 90 days.
4. 180 days.
5. 1 year.
6. 2 years.



The selected media files storing period must comply with the laws of your region.

Hubs linked to a company

The Restrict access to hubs option is disabled by default. When enabled, hubs linked to the company can only be added to that company's account. Adding to accounts of other companies is not possible. Contact [Ajax technical support service](#) or your Ajax manager to learn more about this feature.

Maintenance of objects

If the **Maintenance reports** option is enabled, company employees can generate reports on the technical health of security and fire detectors used in the system. Such reports can be generated and downloaded only by those roles which received the appropriate right from the company owner. The right is assigned in the **Access rights** menu.

By default, the maintenance reports option is turned off. An employee with the **Installer** role can't generate technical health reports for those objects to which they have no access.



Employees can download up to 10 reports per request.

[Learn more](#)

Access rights

In the **Access rights** menu, the head of the company can adjust the access rights for employee roles. If the manager assigns access to a certain type of employee, then all employees with this role will have the corresponding right.

The head of the company can enable or disable the following rights:

- Creation of operation reports for systems.



If the company owner has granted the right to create maintenance reports for a specific role, all employees with this role can create reports, download them, and access the archive of these reports.

Workstations

In the **Workstations** menu, you can assign a unique identifier to each computer (computer ID) and link an employee account to it. This information is used to generate a report on CMS availability.

To assign a workstation to an operator, you need to confirm their login to the account. You can do this by clicking “+” in the line with the operator’s email in the **Unverified** tab. When you click on the line, the extended information about the account and the **Verify** button open on the right.d window, select the types of events:

When verifying the workstation, you should assign a name to it for the convenience of displaying it in the event journal. The computer ID is assigned automatically.

After confirming the workstation, the operator account displays in the **Verified** tab along with the data about the computer. A workstation can be temporarily deactivated or deleted by selecting an account in the list and clicking **Delete from verified**.

Filters are provided for convenience in navigation through the list of workstations.

In the **Workstations** menu, you can configure the types of events that generate incidents. PRO Desktop notifies about incidents in the **Monitoring** tab. To select events that generate incidents, click on the gear icon in the **Unverified** tab.

In the opened window, select the types of events:

- **The operator is offline** – the operator computer has no Internet connection.
- **Login from an unverified computer** – login to the account from a PC that has not been verified by the head of operators.

How to manage response units in the RRU menu

To add a new response unit, click the **Add RRU** button in the **Response Units (RRU)** menu.

A window will open with a form in which you need to specify the unit details. This information will be displayed in the **Monitoring** module when processing an alarm, as well as in the **Objects** module when the RRU is linked to an object. You can add 2 phone numbers to one unit. Required fields are marked with an asterisk.

It is possible to deactivate the **RRU** temporarily without removing it from the system. To do this, switch the toggle in the line with the certain unit. Left position – the unit is inactive, right position – it is active.

Hubs

The **Hubs** menu is designed to administer hubs linked to a company. Here you can receive requests for monitoring/removal from monitoring, adding/deleting objects, as well as transferring objects from Translator to PRO Desktop (if the Translator account is linked to a company account). Hubs are displayed in the menu as a list, where the hub identifier, object statuses, number, and name of the object in PRO Desktop are indicated.

The hub status is also displayed in this window. **Ajax PRO Desktop Status** is designed for monitoring services, and **Installation services** is for installing and configuring the Ajax security systems.

Ajax PRO Desktop Status	Meaning
Active	Object accepted for monitoring
Pending deletion	The object has been removed from monitoring and is in the Withdrawn from monitoring menu of the Objects module
Not connected	Monitoring request was not sent

Installation services	Meaning
Active	A request for installation services has been sent.
Not provided	Installation and maintenance services are not provided. Installers and heads of Installers do not have access to system settings.

When a hub is selected, a details window opens, where there are buttons for creating/deleting an object, going to the object card, and deleting the hub from the company account. The deletion from an account means that the object will be deleted both in PRO Desktop and in Translator (if the account in Translator is linked to an account in PRO Desktop).

Objects

Roles of employees with access to the module: *Company owner, Engineer, Senior CMS Engineer, Head of operators, Operator, Installer, Head of installers.*

The **Objects** module is designed to administer objects in PRO Desktop. To go to the module, select **Objects** in the list of modules in the upper left corner of the screen.

An object in PRO Desktop is a security system controlled by a single hub. When adding a new object, the operator enters the hub identifier and assigns a number and a name to it. All devices connected to the hub are automatically linked to the object and displayed in the **Equipment** tab.



Only one hub can be linked to one object.

The module screen consists of two parts: a list of objects and a sorting menu. The list of objects contains their numbers in PRO Desktop, names, addresses, as well as hub identifiers (IDs). The following items are available in the sorting menu:

- **Active** – the list of all objects within PRO Desktop, aside to objects in the **Withdrawn from monitoring** menu.
- **Armed** – the list of objects with the currently armed security system.
- **Disarmed** – the list of all objects with the currently disarmed security system.
- **In Sleep Mode** – the list of objects with muted alarm notifications.
- **Offline** – the list of objects where the hub is offline.
- **With malfunctions** – the list of objects where the security system reports a malfunction: low battery indicator, failed attempts to arm the detector, etc.
- **No contract** – the list of objects with empty information about the contract with the company. Contract information can be added at any time.
- **Installation services provided** – objects that are under maintenance of installers and heads of Installers.
- **Monitoring requests (from installers)** – objects from which a request was submitted to connect to the CMS via Ajax PRO apps.
- **Monitoring requests (from end-users)** – objects from which a request was submitted to connect to the CMS via the Ajax Security System app for end-

users.

- **Monitoring cancellation requests** – a list of objects from which a request was submitted to disconnect from the CMS via any Ajax app.



Only an admin or a PRO account with the right to configure the system can cancel a request for monitoring cancellation. You can do this in any Ajax app: Devices → Hub → Settings → Security companies.

- **Withdrawn from monitoring** – deleted objects. Objects are automatically deleted from the bin after 7 days.

In the **Objects** module, the following buttons are also available:

- **Add object** – allows you to link an object to a company using the QR code (ID) of the hub. You can add an object by ID (QR code) if the following conditions are met:
 - Hub is online.
 - Hub has no users.
 - Hub is not added to the account of another company.

[More about adding objects](#)

- **Maintenance reports** – opens the menu of maintenance reports.

[More about maintenance reports](#)

- **Update** – updates the list of hubs linked to the company.

Adding an object

There are three ways to add a new object to PRO Desktop:

1. Using the hub ID (its QR code).
2. Accepting a monitoring request from the Ajax app.

3. Transferring the object from Translator to PRO Desktop.



After connecting the hub, specify the necessary information in the object card. In Ajax apps, this will make easier navigation and object searching.

How PRO account can access the hub

Adding via ID

When adding an object, a card is created with all the information necessary for alarms processing: address, contacts, room layouts, road maps, responsible people, comments, etc. You can add an object by ID (QR code) if the following conditions are met:

- Hub is online.
- Hub has no users.
- The hub is not added to another company account.

The installer or head of installers can connect the hub. You can add a hub from a company account only, but not from a personal PRO account. After adding a hub, the company has permanent access to the object's settings.

To add a hub, in PRO Desktop:

1. Open the **Objects** module.
2. Click the **Add object** button.
3. Specify the name of the object, as well as the 20-digit hub ID (located under the QR code on the hub or packaging, the format is xxxxx-xxxxx-xxxxx-xxxxx).
4. Click **Add**.

Adding an object via a monitoring request

The request to add is sent via Ajax apps by the hub admin or a PRO account with access to the object's settings. The list of requests for monitoring and monitoring cancellation is displayed in the corresponding tabs of the **Objects** module, as well as in the **Hubs** menu of the **Company** module.

The adding method depends on the type of services provided:

- **To access alarm monitoring**, you should send a request for monitoring.
- **To access installation and maintenance**, you should send a request for access to the system settings.
- **For both types of access**, you should send both requests.

To send a request for alarm monitoring, in the Ajax app:

1. Select an object if you have more than one or if you use the Ajax PRO app.
2. Select the hub in the list of devices.
3. Go to its settings.
4. Open the **Security companies** menu.
5. Select a company and click **Send request**.



A monitoring request can also be sent if you know the company's email address. To do this, click on the envelope icon in the **Security companies** menu, enter the company's email address, and click **Continue**. Select a company from the list and confirm sending the request.

To accept a monitoring request, in PRO Desktop:

1. In the **Objects** module, go to the **Monitoring requests** (from end-users) and/or **Monitoring requests** (from installers).
2. Select a hub.
3. Click **Accept request**. An object card will be automatically created for the hub to fill in the information.

4. Enter the number, name of the object and click **Save**. A new object will appear in PRO Desktop.

To send a request for access to installation and maintenance, in the Ajax app:

1. Select an object if you have more than one or if you use the Ajax PRO app.
2. Select the hub in the list of devices.
3. Go to its settings.
4. Open the **Installers** menu.
5. Click the **Assign** button.
6. Enter the email address of the company specified when registering.
7. Select a company and confirm the sending of a request.

You do not need to accept a request for the installation company services in PRO Desktop. After adding, the company has 8 hours to change the hub settings, add devices and invite users. On the expiry of this access time, the company can no longer change the object's settings.

If necessary, the installer, or head of installers can request temporary or permanent access, which should be confirmed by the hub admin or a PRO account with rights to configure the system.

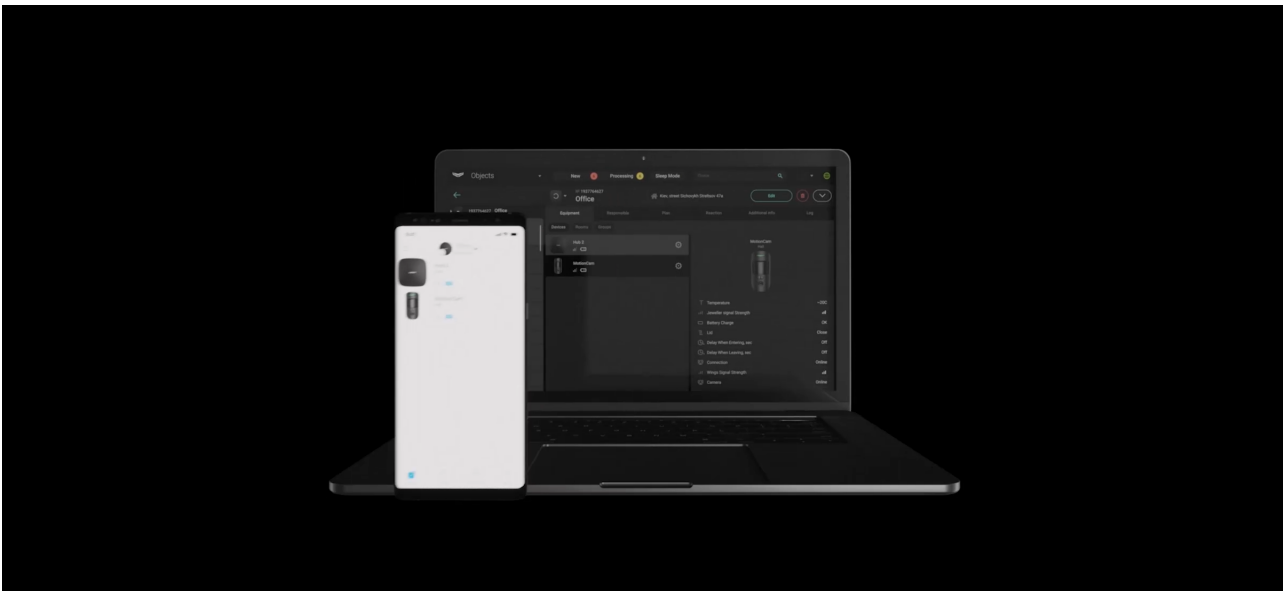


PRO receives permanent rights to configure the system if there is no single hub admin.

Transferring objects from Translator

To transfer objects from Translator, contact [Ajax technical support service](#).

Configuring an object



By default, the installer has the same rights for setting as his company. The installer does not have access to the hub settings (if access to all objects is disabled) until the head of Installers grants him such a right. Once access is granted, installers can begin setting up the object.

There are two ways to grant access to the installer:

The first way	The second way
<ol style="list-style-type: none"> 1. Open the object list in PRO Desktop. 2. Select the object. 3. Go to the Installers menu. 4. Click Assign. 5. Enter the email address of the installer's PRO account, or select it from the list. 6. Define its access rights. The access rights of the installer cannot exceed the rights of the company. 7. Click Add. 	<ol style="list-style-type: none"> 1. Open the object list in PRO Desktop. 2. Go to the Company module and select the Employees menu. 3. Select the employee. 4. Go to the Assigned objects menu and click Assign. 5. Enter the name/ID of the object or select it from the list. 6. Define the access rights of the installer. Their access rights cannot exceed the rights of the company. 7. Click Add.

Prolongation of access time to the hub settings

The field indicated in the screenshot shows the time during which the installer has access to the system settings. By clicking on the field, you can request permanent or temporary access (for 1, 2, 4 or 8 hours).

If there is not enough time to set up, the installer can send a request to extend the time to access the settings. All head of installers of this company will receive such a request.

If the company has sufficient rights, any head of installers can grant this right to the installer. Such a request can only be confirmed in the PRO Desktop app.

If the rights are not enough, for example, the company has rights to configure within 4 hours, and the installer needs 8 hours, the head of installers can request access rights from the hub admin. When approved, access will be granted to the company and this particular installer.

Set up company rights

The hub admin or PRO account with the right to configure the system can assign company access rights. These settings apply to all employees of the company. To assign access rights to a company, in the Ajax app:

1. Select an object if you have several of them, or use the Ajax PRO app.
2. Select the hub in the list of devices.
3. Go to its settings.
4. Open the **Installers** menu.
5. Select a company. Go to its settings. These settings allow you to grant or disable the right to:
 1. Change security modes.
 2. Activate panic button in Ajax apps.
 3. View cameras.
 4. Control relays and smart plugs.
 5. Enable **Chimes**.

The hub admin or PRO account with the right to configure the system can also remove the company from the hub or cancel its access.

Object Card

Data about the object can be supplemented and edited. The data is divided into tabs:

- **Equipment** – a list of devices, virtual rooms, and security groups of an object. When a device is selected, the status screen opens, showing battery charge, connection status, tamper status, and other data about the operation.
- **Responsibles** – names and phone numbers of people with whom the operator can contact in case of an alarm at the object.
- **Object Photos** – a photo of the object, a map of approaches to the object, room layouts of the object, and road maps for directions to the object.
- **Reaction** – information about the main and reserve RRU's assigned to the object. To manage units in this menu, you should first create them in the **Company** module, the **Response Units (RRU)** menu.
- **Object Notes** – technical information about the object: dates and detailed information on the installation work, connecting to the monitoring station, data of the installer assigned to the object.
- **Log** – event journal of an object.

In addition to the access time to the object settings, the object card displays the **Maintenance reports** button. The button is available only for those employee roles for which the company owner has assigned such a right.

Keep in mind that employees with **Installer** role can create reports if they have access to the settings of this hub.

By clicking on the button, you can generate a new report or download a previously created report from the archive. When trying to create a new report, the **Maintenance reports** tab opens.

Editing a card and deleting an object

The menu to control security modes, the object number, its name and address, buttons to edit and delete, and a button that opens contacts and details of the object operation are located above the informational tabs.

To delete an object, click on the icon with three dots. There will be a menu with two options: **Stop monitoring** or **Stop maintenance services**. Their functions are different. For example, if the object remains under monitoring and the service is stopped, the operators will receive alarms and events of this system, but the installer will not be able to change the equipment settings at the facility.

When monitoring is stopped, the object is moved to the **Withdrawn from monitoring** menu and automatically deleted after 7 days. During this time, the object can be returned to the list of active ones by going to the **Withdrawn from monitoring** menu in the **Objects** module and clicking **Restore**. You can stop the monitoring only for those objects that do not have open incidents.

To delete an object, click the bin icon. The object will be moved to the **Withdrawn from monitoring** menu and automatically deleted after 7 days. During this time, the object can be returned to the list of active ones by going to the **Withdrawn from monitoring** menu in the **Objects** module and clicking **Restore**. You can delete only those objects that do not have open incidents.

To delete objects without waiting 7 days, select the object from the **Withdrawn from monitoring** menu and click the red bin icon. Confirm the action by clicking **Stop monitoring**.

When the maintenance services are stopped, the object is permanently removed. This means that installers and head of installers will no longer be able to maintain this object. To restore the object, the company needs to be reconnected through the hub settings.

Maintenance reports



Employees can download up to 10 reports per request.

Maintenance reports allow you to generate PDF files that contain information about security and fire detectors connected to the hub, and their states. Reports allow you to regularly monitor the status of all monitored objects.

One report is generated for one object. The language of the report downloaded matches the language selected in the PRO Desktop app as a language for SMS messages.



The company owner can enable or disable the maintenance reports option at any time.

The maintenance reports menu contains three tabs:

1. **Objects** – contains a list of objects for which you can generate maintenance reports. In this menu, you can also generate these reports.

[Learn more](#)

2. **Upload CSV** – menu for uploading the list of hubs for generating a maintenance report.

[Learn more](#)

3. **Archive** – contains previously created maintenance reports.

[Learn more](#)

Objects tab

All objects for which you can generate maintenance reports are shown in this menu. Objects can be sorted:

1. By object number.
2. By name or address of the object.
3. By hub ID (identifier).

4. By date of generation of the last report.

To generate a report, in the **Objects** menu:

1. Select the required objects. For ease of navigation, we have provided search by name of the object, its number and address, as well as by the hub ID. If you want to hide extra objects, enable the option **Hide unselected**.
2. Press **Create report**.
3. Confirm report generation by selecting **Create**.
4. Wait until the report is generated.
5. Go to the **Archive** tab. Select the required reports.
6. Press **Download selected**.
7. Select a folder and save the files.



To automatically download selected reports to your PC after creation, enable the option **Automatically download when created**.

Upload CSV tab

Drag the CSV file or upload it from your computer to generate a report for the required list of objects. CSV file should contain hub IDs (identifiers) or object numbers. If you upload a file in the wrong format, the app will return an error.

After uploading the file, reports on the necessary objects will be generated and available in the **Archive** tab.



You can download an example of CSV in the required file format in the **Upload CSV** tab.

Archive tab

The maintenance reports generated are located in this tab. The tab shows only the last 5 reports for each object. Older reports are deleted.

Objects can be sorted:

1. By report number (the higher the number, the newer the report).
2. By object number.
3. By name or address of the object (one of the two options can be selected by clicking on the column name).
4. By name or e-mail address of the company employee who generated the report (one of the two options can be selected by clicking on the column name).
5. By hub ID (identifier).



For ease of navigation, we have provided search by name of the object, its number and address, as well as by the hub ID.

To download a report:

1. Go to the **Archive** tab.
2. Select the required reports.
3. Press **Download selected**.
4. Select a folder and save the files.



After selecting an object in the **Archive** tab, you can also generate a new report for this object if necessary.

PDF file of the report

PDF file of the report contains all the necessary information about the object and the states of all devices of the security system. At the beginning of each file, in addition to general data, a short summary of the check is also available: if the engineer should visit the object or not. A recommendation to visit the object appears if at least one device in the system has a malfunction.

The file name has the following format: AA_XXXXXXXX_YYYYYYY_MM

- AA – the result of the check.
 - p – the test passed, and the report does not contain a malfunction.
 - pw – the test passed, but the report contains some malfunctions. It is recommended that an engineer visit the object to check. For example, if one of the detectors has a low hub signal strength or this detector is temporarily disabled.
 - f – the test failed. It is recommended that an engineer visit the object to check. For example, one of the detectors has lost connection with the hub.
- XXXXXXXX – the date when the report was created in the DDMMYYYY. For example, 27032022.
- YYYYYYYY – the assigned object number. If there is no number, the hub ID is used.
- MM – report number.

Monitoring

Module access: *Company owner, Senior CMS Engineer, Head of operators, Operator.*

The **Monitoring** module allows you to process events and alarms of Ajax security systems, as well as notifications about the operators work. **New**, **Processing**, and **Sleep Mode** tabs are located at the top of the PRO Desktop screen.

New alarm notifications are displayed in the **New** tab and are accompanied by the sound of a siren until the incident will be considered. An incident is not considered closed until it is closed by the operator. One notification can include multiple alarms or events of the security system. The latter three are displayed as icons in the notification line, in the **Source** column.

An incident is created after the following Ajax security events:

- Detector alarms.
- Tamper triggering of any device in the system.
- StreetSiren or StreetSiren Double Deck accelerometer triggering.
- Jamming detection.
- Loss of connection with any device in the system.
- Loss of connection between the hub and the Ajax Cloud server via one or all communication channels.
- Loss of the central unit, range extender, vbfBridge or integration modules external power supply.
- Any other malfunction of the system devices.

Meaning of system alarms and events icons		
Event icon	Description	Recovery icon
Malfunctions		
	Testing	
	The device is temporarily disconnected	
	Disconnecting of Ethernet communication channel	
	Disconnecting of SIM communication channel	
	Loss of detector connection	
	Loss of hub connection	
	Loss of siren connection	

	Loss of hub main power	
	Hub battery discharge	
Alarms		
	Leakage detector alarm	
	Hub body opened	
	Device body opened	
	Security alarm of the motion detector	
	Security alarm of the glass break detector	
	Security alarm of the opening detector	
	Security alarm of the shock/tilt detector	
	Panic button: silent alarm	
	Panic button: regular alarm	
	Fire alarm	

	Alarm due to excess carbon monoxide concentration	
	Fire alarm: smoke	
	Fire alarm: threshold temperature rise	
	Gas alarm	
	Medical assistance	

The notification line displays the name, address, object number, as well as the status and time elapsed since the alarm was received, during which the operator is viewing the incident. Which operator and when started viewing the incident is recorded in the **Journal** module. The journal also records all other actions of operators to process the incident: from consideration to closing the incident.

Icons for operator incident viewing status	
	Not viewed
	Viewed
	Processing

Operator incidents

Separately, the list shows incidents of loss of connection with the operator and operator logins to the PRO account from an unverified computer. These types of incidents are generated according to the operators' workstations, which are confirmed in the **Company** module, processed as security alarms, indicating the cause of the incident, and recorded in the journal.

Notification **Operator is offline** – an incident type that contains information about the loss of connection with the computer that is confirmed as the operator's workstation in the **Company** module.

Notification **Login from an unverified computer** – an incident type that contains information about the user and the computer from which the login was made.

[More about operator workstations](#)

Incident processing

Incident processing algorithm

1. Sending an Ajax security alarm by the hub.
2. Automatic creation of an **Incident** in the **Monitoring** module.
3. Review of the **Incident** by the CMS operator or the head of operators.
4. Processing the **Incident** by the CMS operator or the head of operators.
5. Checking the cause of the alarm: communication with contact persons, checking pictures from detectors with photo verification.
 1. **If the alarm is real or it is impossible to determine the cause of the alarm:** Sending the RRU. After finding out the causes of the alarm, end the incident processing, indicating the cause of the alarm.
 2. **If the alarm is false:** Set the cause of the alarm as "False alarm" or "No incident" and end the incident processing.

Information on incident processing screens

Clicking on the notification opens:

- Incident details – alarm time, triggered device, room, photo verification (if detectors with photo verification triggered).
- Object info – address, contacts, schemes of premises, etc.

By clicking the **Start processing**, the operator starts processing the alarm, and the incident goes to the **Processing** tab. The operator has limited access to the tab: they see only those incidents that are being processed. The head of operators has full access to see all incidents that are being processed by the operators.

In the centre of the **Processing tab**, information about the object, a list of alarms, a menu for controlling security modes, as well as notes, a list of devices, road maps, and room layouts are displayed.

If **motion detectors with photo verification** are installed at the object, the operator can view a series of photos taken by the detector to check the cause of the alarm. Photos are displayed in the **MotionCam** tab in chronological order, starting with the latest.

The operator can contact one of the responsible people indicated in the object card – when processing an alarm, their names, and phone numbers are displayed on the app screen. PRO Desktop does not support calls from the app. But the operator can copy the phone number of the responsible person and call them using third-party software. For example, using an app for IP telephony.

Responsible people are assigned when creating an object in PRO Desktop. This may be, for example, the owner of the flat or the head of the security service at the production site.

Based on the results of the connection, the operator puts a mark **Accepted** – if it was possible to contact and the responsible person accepted the information. If there is no connection with the responsible person, the operator puts the mark **Not responding**. You can switch between responsible people using the arrows. They appear if all responsible people cannot be displayed at the current size of the app window.

The rapid response teams assigned to the object are displayed under the responsible people. When communicating with the RRU, the operator checks if the unit has been **Dispatched, Arrived**, or is **Unavailable**. You can switch

between assigned groups using the arrows. They appear if all RRUs cannot be displayed at the current app window size.



RRUs are assigned when an object is created in PRO Desktop.

The incident processing log is displayed in the lower right corner of the screen. For each record in the log, the operator can leave a comment by clicking on the record. At the top of the processing journal, you can select the cause of the alarm from the drop-down list and complete the processing. If necessary, you can comment on the cause of the alarm. For example, to describe in more detail the cause of a false alarm at an object.

When processing an incident related to the operator's workstation, you can specify the reason from the drop-down list, and, if necessary, accompany it with a comment. When processing an incident about an operator logging in from an unverified computer, the workstation can be verified in the same window. To do this, click the "+" button next to the operator details.



After the incident is processed, it closes and goes to the **Journal**, where the log of its processing is saved. **You cannot return to incident processing.**

Sleep Mode

An employee who has access to the monitoring module can switch an object into **Sleep Mode** if installation work is being carried out at the object or false alarms are coming from it. Objects with alarms and events that are temporarily ignored are on the **Sleep Mode** tab. You can switch the object to **Sleep Mode** using the menu for managing security modes.

When transferring an object to **Sleep Mode**, the operator specifies the time after which the object will return to normal operation. You can select 1, 5, 15, or 30 minutes, or manually enter the time from 1 to 300 minutes.

While the object is put into **Sleep Mode**, PRO Desktop ignores its alarms and events – they are not displayed in the **New** tab but are recorded in the **Journal** module. At the end of the set time, the object returns to normal operation.

To remove an object from Sleep Mode before the end of the set period:

1. Open the security mode controlling menu.
2. Disable **Sleep Mode**.

Journal

Access to the module: *Company owner, Engineer, Senior CMS Engineer, Head of operators, Operator, Head of installers.*

PRO Desktop maintains a journal of alarms and events of all company objects, and also allows you to generate reports on the availability of hubs and CMS operators. To go to it, select the **Journal** in the list of app modules.

Object notifications are displayed in chronological order. To set the time interval for notifications, their type, or object number, use the filters. Above the filters, a counter of filtered records is displayed, as well as buttons for resetting filters and refreshing the journal.

To filter notifications by device, room, or user, click on them in the list of notifications. By clicking on the number of the object in the column, you can filter the notifications of this object. Notifications can also be filtered by clicking on the event icon – you will get a list of all events of the same type.

To open the incident processing log, click on the clock icon on the incident ending record.

Availability reports

PRO Desktop can generate reports showing the connection time with security systems (**Hubs availability**). You can also generate a report on the **Operators availability**. To generate reports on hub availability, select the **Hubs availability** filter. By default, the report has information of the last 7 days. If necessary, the period can be changed in the **Time frame** filter, and you can also set the object number.

The availability report will be generated for the selected objects if the filter by object number is active. If the filter by object number is inactive, the report will be generated for all hubs of the company. After setting parameters, click the report generation button next to the filter name – the report will open in a new window.

To generate the operators availability report, only the workstations of operators verified in the **Company** module are considered. To generate a report, click the **Operators availability** filter. A list of events will be displayed on the right:

- **Operator signed in** – login to the operator account is registered.
- **Operator signed out** – logout of the operator account is registered.
- **Loss of connection with the operator** – loss of Internet connection with the operator's computer.
- **Connection with the operator restored** – restoring the Internet connection with the operator's computer.
- **Monitoring is paused** – there is no available operator.
- **Monitoring is resumed** – at least one operator is available.

Set and apply the range to filter events by time. To generate a report based on the specified parameters, click the report generation button next to the filter name.

System requirements

For Windows app



For macOS app



Subscribe to the newsletter about safe life. No spam

Email

Subscribe

