About Fraud Protection
Data Hub
Bots
Graph
Export
Rules
Drive
Settings
User roles and permissions

User roles and permissions

To manage access to the Fraud Protection admin panel, users are assigned roles that define a specific set of permissions. A user's access level depends on the roles and the projects those roles are associated with.

Each user can hold multiple roles across different projects to accurately reflect their responsibilities and comply with internal regulations for incident monitoring, response, and security policies.

Access levels can be adjusted by adding or removing roles and projects for them as needed.

User roles

A user role is a predefined set of permissions that determines what a user can view and do in the Fraud Protection platform. Roles help control access to sensitive operations and data within companies and projects.

Fraud Protection provides two categories of roles:

- **Main roles**: Core roles for day-to-day system use and administration.
- **Special roles**: Additional roles for extra modules and restricted access.

Main roles

Owner
Grants full access to all system features and settings.

Integrator
Designed for Group-IB partners and technical specialists responsible for deploying and integrating the Fraud Protection solution for clients.

Admin
Applies to company-level administrators managing projects and operations within one or more companies.

Security Officer
Focuses on user security and access management within the system.

Expert
Intended for second-line incident response specialists.

Manager
Provides read-only access across the Fraud Protection admin panel.

Senior Analyst
Designed for first-line response specialists with extended privileges for rule operations.

Analyst
Intended for first-line response specialists focused on incident analysis.

Special roles

Preventive Proxy Admin, Cloud Admin
Provides full administrative control over the Preventive Proxy module and related cloud integrations.

Contributor
Grants access to the Fraud Intelligence (FI) module.

Guest
Provides restricted access to the Help Center only.

Permissions

Below you can find detailed permissions for each role, organized by modules and sections of the Fraud Protection platform. These tables show which actions are available to different roles across system settings, data access, detection rules, and additional features.

ⓘ The Owner role has unrestricted access to all features and settings, even if not explicitly listed in the permissions tables.

Settings

The **Settings** section is used to configure system parameters and manage companies, projects, and users within the Fraud Protection platform. This section contains multiple tabs, each dedicated to a specific area of configuration. Access to actions in this section depends on the user role.

Section	Permissions	OWNER	INTEGRATOR	ADMIN	SECURITY OFFICER	EXPERT	MANAGER	SENIOR ANALYST	ANALYST
Users	User management: • View user list • Export user list • Block/unblock users User account actions: • Create user • Update user details • Send invitation • Edit user roles and access to projects • Manage subscriptions to specific events (User details → Subscriptions)	•	•	•	•				
Users	• Delete user • Assign extended permissions for rules (see Extended permissions)	•	•	•					
Company	Create company	•	•						
Company	Edit company info	•	•	•					
Projects	Create projects	•	•						
Projects	Update projects	•	•	•					
Projects	View project details	•	•	•	•	•	•	•	•
Rules	View configured rules and export them	•	•	•	•	•		•	
Rules	Set up rules	•	•	•		•		•	
Rules	Migarate project rules	•	•	•		•			
Data stream	View available datastreams	•	•	•	•	•		•	
Data stream	Add, configure, and delete datastream	•							
API settings	Generate and edit an API key	•	•	•					
API settings	View configured APIs	•	•	•	•				
IP rules	Add parsing rules	•	•	•					
IP rules	View configured IP rules	•	•	•	•				
Trusted IPs	View and configure trusted IPs	•	•						
Domains	View and configure domains	•	•	•	•				
GSSC key	View GSSC key tab	•	•	•	•				
GSSC key	Enable or generate a new key	•	•	•					
Attributes	Configure attributes	•							
Subscription stats	Access subscription data	•	•	•		•			
Statuses	• View statuses • Configure statuses	•	•	•	•			•	•
List	• Access lists and their values • Export lists	•	•	•	•	•	•	•	•
List	• **Custom lists**: Import, create, edit, and delete lists and their items; add tags • **System lists**: Import, add, edit, and delete items in lists	•	•	•		•		•	•
Decrypt	Decrypt cookies and packages	•	•	•	•	•	•	•	•
Logs	View logs	•	•	•	•				

Data Hub

The **Data Hub** section is used for managing and exploring event and session data within the Fraud Protection system. Access to actions in this section depends on the user role.

Section	Permissions	OWNER	INTEGRATOR	ADMIN	SECURITY OFFICER	EXPERT	MANAGER	SENIOR ANALYST	ANALYST
Events	Can view data, apply filters, and export event information	•	•	•	•	•	•	•	•
Sessions	Can view session data, apply filters, and export session information	•	•	•	•	•	•	•	•
Sessions	Can import session labeling, edit session status	•	•	•		•		•	•
Operations	Can view data, apply filters	•	•	•		•		•	•

Rules

For detailed information on working with rules, refer to Roles and permissions for rules.

Permissions	OWNER	INTEGRATOR	ADMIN	SECURITY OFFICER	EXPERT	MANAGER	SENIOR ANALYST	ANALYST
View rules	•	•	•	•	•	•	•	•
Create a new rule draft	•		•		•		•	
Review the rule (approve or reject)	•		•		•		•	
Enable rules	•	•	•		•		•	

Graph

The Graph section is used for building and analyzing visual relationships between entities within the Fraud Protection system. Access to actions in this section depends on the user role.

Role	Permissions
Owner, Integrator, Admin, Security Officer, Expert, Senior Analyst, Manager, Analyst	Build graphs
Owner, Integrator, Admin, Expert, Senior Analyst, Analyst	Add nodes to lists, remove nodes from lists via context menu

Drive

The Drive section is used for managing reports and monitoring storage within the Fraud Protection system. Access to actions depends on the user role.

Role	Permissions
Owner, Integrator, Admin, Security Officer, Expert, Senior Analyst, Manager, Analyst	Can create and delete reports, monitor remaining storage space, download reports, track report status, and regenerate reports

Bots

The Bots section manages bot detection and traffic filtering through the Preventive Proxy module. Access to this section depends on the user role:

- Some roles can only view analytics and information related to Preventive Proxy.
- Other roles have full permissions to configure the Preventive Proxy, including critical security and traffic control settings.

See the table below for details:

Role	Permissions
Integrator, Admin, Security Officer, Expert, Senior Analyst, Manager, Analyst, Cloud Admin, Preventive Proxy Admin	Can view Preventive Proxy-related analytics and information
Integrator, Admin, Cloud Admin, Preventive Proxy Admin	Can fully configure the Preventive Proxy, including: • Integration for the Preventive Proxy module • TLS settings • Rules for traffic processing

Scripts

Users with the following roles can view and work with the Scripts tab: **Owner, Integrator, Admin, Security Officer, Expert, Senior Analyst, Manager, Analyst**.

Fraud Intelligence

Users require a **Contributor** role to access FI. This role allows them to view and contribute to the content. By default, users with the **Owner** role have full administrative control over the FI section. Other roles do not have access to this section.

See the table below for role capabilities:

Role	Permissions
Contributor	• Create reports for FI • Edit and delete their own reports • View public FI reports
Owner	Grants full control over FI, including: • Make reports public • Create, update, and delete mitigations and detections

The **Contributor** role can be assigned by users who have the necessary permissions. For detailed instructions on assigning the role, see Access to Fraud Intelligence.

Help Center

By default, all roles have access to the Help Center. It provides users with documentation, guides, and resources to effectively use the platform.

There is a dedicated **Guest** role, which can be assigned to limit access exclusively to the Help Center. When a user has the **Guest** role, they can access only the Help Center within the admin panel. No other sections are available.

User roles
Main roles
Special roles
Permissions
Settings
Data Hub
Rules
Graph
Drive
Bots
Scripts
Fraud Intelligence
Help Center

Still need help?
Get support