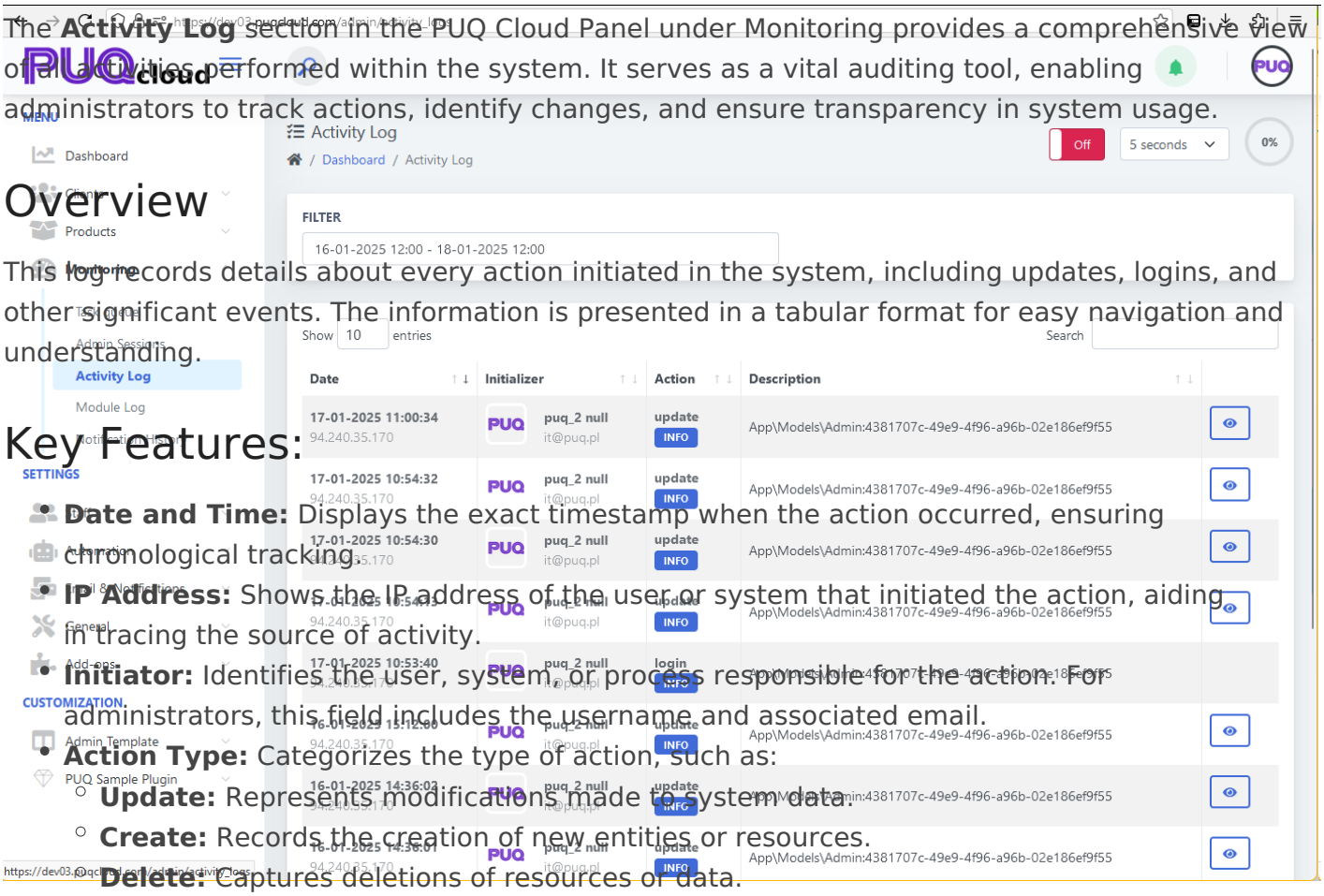
Monitoring: Activity Log Overview

PUQcloud Panel

Order Now | Download | FAQ



The **Activity Log** section in the PUQ Cloud Panel under Monitoring provides a comprehensive view of all activities performed within the system. It serves as a vital auditing tool, enabling administrators to track actions, identify changes, and ensure transparency in system usage.

Overview

This log records details about every action initiated in the system, including updates, logins, and other significant events. The information is presented in a tabular format for easy navigation and understanding.

Key Features:

- **Date and Time:** Displays the exact timestamp when the action occurred, ensuring chronological tracking.
- **IP Address:** Shows the IP address of the user or system that initiated the action, aiding in tracing the source of activity.
- **Initiator:** Identifies the user, system, or process responsible for the action. For administrators, this field includes the username and associated email.
- **Action Type:** Categorizes the type of action, such as:
  - **Update:** Represents modifications made to system data.
  - **Create:** Records the creation of new entities or resources.
  - **Delete:** Captures deletions of resources or data.
  - **Login:** Logs access attempts to the system by users or administrators.
- **Description:** Provides detailed information about the action, including references to models, entities, or resources affected by the activity.
- **Filter Options:** Administrators can narrow down results using date ranges and specific keywords to locate relevant logs efficiently.
- **Search Functionality:** A search bar allows quick filtering based on specific terms or identifiers.
- **View Details:** Each entry includes a **View** button, which provides in-depth information

about the selected action for more granular analysis.

Technical Details:

- **Data Storage:** All activity logs are stored in a secure database with redundancy to prevent data loss.
- **Log Retention:** Logs are retained based on system policies, which can be configured by the administrator to comply with regulatory or operational requirements.
- **Integration:** This section integrates with other monitoring tools, such as **Admin Sessions** and **Module Log**, for holistic system insights.

Usage Scenarios:

- **Auditing:** Track changes made by administrators to ensure compliance with internal policies.
- **Security:** Identify unauthorized access or suspicious activities by monitoring login attempts and other critical actions.
- **Troubleshooting:** Review logs to pinpoint errors or unintended changes that may impact system functionality.

Best Practices:

- Regularly review activity logs to ensure system integrity and identify potential issues early.
- Use filters and search functionality to focus on critical periods or specific actions.
- Export logs periodically for offline storage or integration with external auditing systems.

The **Activity Log** is a crucial tool for maintaining accountability and transparency within the PUQ Cloud Panel. By providing a detailed and searchable record of system activities, it empowers administrators to ensure smooth and secure operations.

Revision #4
Created 17 January 2025 04:52:11 by Dmytro Kravchenko
Updated 28 October 2025 09:17:02 by Yuliia Noha