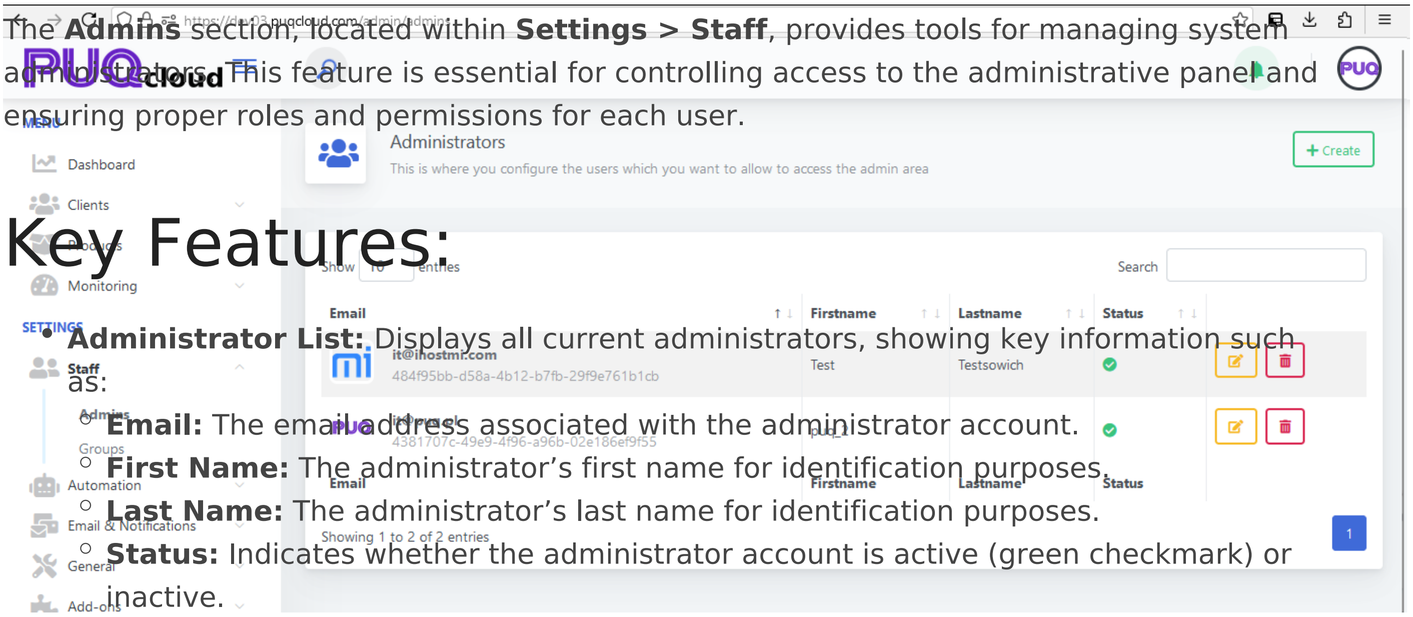
Image not found or type unknown

Staff: Admins Management Overview

PUQcloud Panel

Order Now | Download | FAQ



Administrators

This is where you configure the users which you want to allow to access the admin area

Show 10 entries

Search

Email	Firstname	Lastname	Status
it@ihostmr.com 484f95bb-d58a-4b12-b7fb-29f9e761b1cb	Test	Testsowich	✓
it@puq.pl 4381707c-49e9-4f96-a96b-02e186ef9f55	puq_1		✓
Email	Firstname	Lastname	Status

Showing 1 to 2 of 2 entries

The **Admins** section, located within **Settings > Staff**, provides tools for managing system administrators. This feature is essential for controlling access to the administrative panel and ensuring proper roles and permissions for each user.

Key Features:

- **Administrator List:** Displays all current administrators, showing key information such as:
  - **Email:** The email address associated with the administrator account.
  - **First Name:** The administrator's first name for identification purposes.
  - **Last Name:** The administrator's last name for identification purposes.
  - **Status:** Indicates whether the administrator account is active (green checkmark) or inactive.
- **Actions:**
  - **Edit:** Allows modifying administrator details, such as name, email, or permissions.
  - **Delete:** Permanently removes the administrator from the system. A confirmation prompt ensures accidental deletions are avoided.
- **Search:** The search bar enables quick filtering of administrators by name or email.
- **Pagination:** Controls the number of entries displayed per page, making it easier to navigate large lists.

Adding a New Administrator:

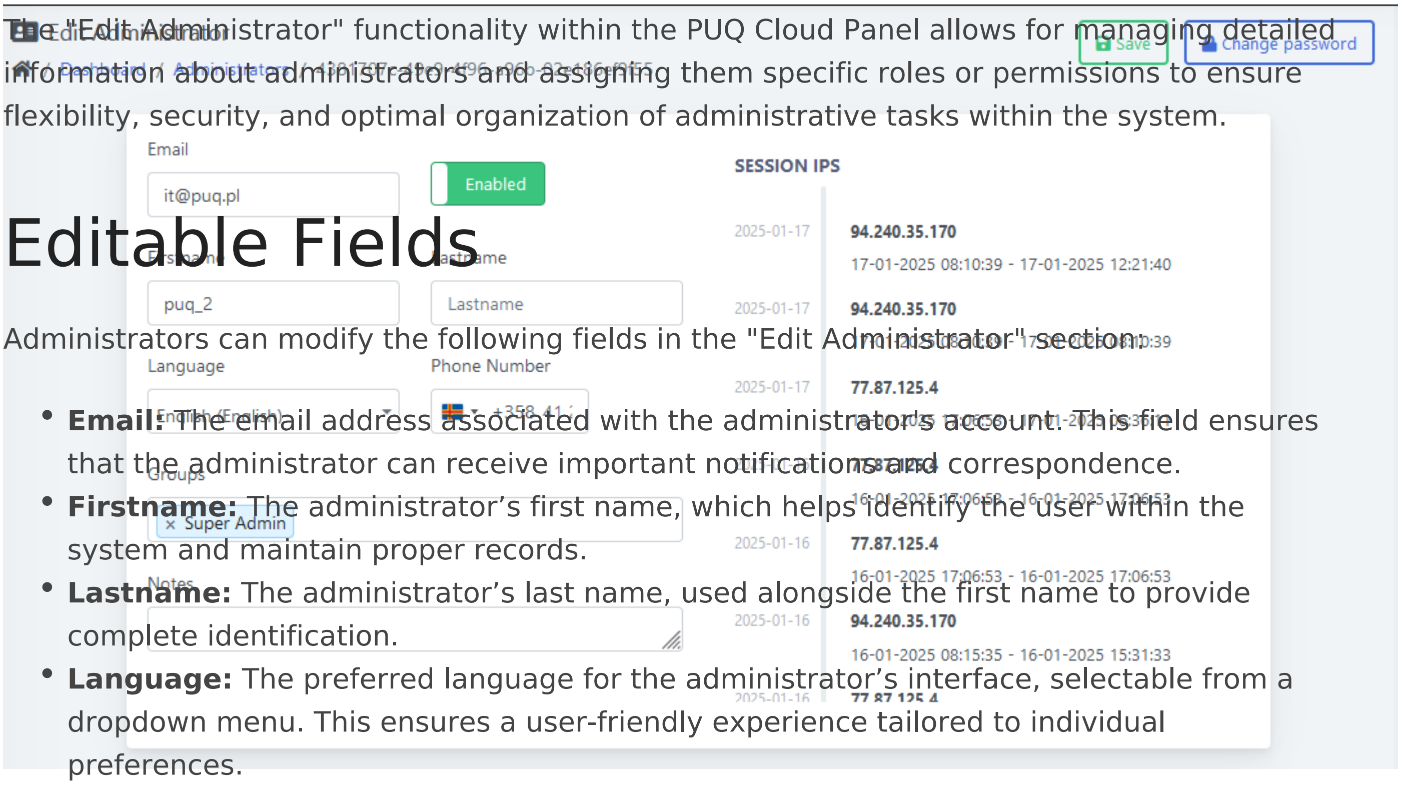
Clicking the **Create** button opens a form where administrators can input the following details:

- **Email:** The email address for the new administrator account.
- **First Name:** The administrator's first name.

- **Last Name:** The administrator’s last name.
- **Password:** A secure password for account access.
- **Confirm Password:** Ensures the password is entered correctly.
- **Status:** Specifies whether the account should be active upon creation.

Editing Administrator Details

The "Edit Administrator" functionality within the PUQ Cloud Panel allows for managing detailed information about administrators and assigning them specific roles or permissions to ensure flexibility, security, and optimal organization of administrative tasks within the system.



Email: it@puq.pl
Enabled
Firstname: puq_2
Lastname: Lastname
Language: English (English)
Phone Number: +358 41
Groups: × Super Admin
Notes:

2025-01-17 94.240.35.170 17-01-2025 08:10:39 - 17-01-2025 12:21:40
2025-01-17 94.240.35.170 17-01-2025 08:10:39 - 17-01-2025 08:10:39
2025-01-17 77.87.125.4 16-01-2025 17:06:53 - 17-01-2025 08:35:31
77.87.125.4 16-01-2025 17:06:53 - 16-01-2025 17:06:53
2025-01-16 77.87.125.4 16-01-2025 17:06:53 - 16-01-2025 17:06:53
2025-01-16 94.240.35.170 16-01-2025 08:15:35 - 16-01-2025 15:31:33
2025-01-16 77.87.125.4

Editable Fields

Administrators can modify the following fields in the "Edit Administrator" section:

- **Email:** The email address associated with the administrator’s account. This field ensures that the administrator can receive important notifications and correspondence.
- **Firstname:** The administrator’s first name, which helps identify the user within the system and maintain proper records.
- **Lastname:** The administrator’s last name, used alongside the first name to provide complete identification.
- **Language:** The preferred language for the administrator’s interface, selectable from a dropdown menu. This ensures a user-friendly experience tailored to individual preferences.
- **Phone Number:** The administrator’s phone number, including country code. This field is particularly useful for contact purposes or integrating with two-factor authentication systems.
- **Status:** Enable or disable an administrator account ("Enabled" or "Disabled"). This feature is critical for managing active personnel and suspending access for inactive or terminated staff.
- **Groups:** Assign the administrator to one or multiple groups with predefined permissions. Groups dictate the administrator’s level of access and operational capabilities within the system.
- **Notes:** Add internal notes related to the administrator’s account or role. This can include special instructions, reminders, or historical context about the account.

Groups and Permissions

Groups are a vital feature in the PUQ Cloud Panel that allow granular control over administrator access. By assigning administrators to specific groups, you can define the scope of their permissions. Groups are highly flexible and customizable to suit various organizational needs.

Below are some examples of group configurations:

- **View-Only Accountant:**
    - Permissions: Can only view invoices and financial data. They cannot modify, delete, or add data, ensuring secure access to sensitive information.
    - Use Case: Ideal for accounting staff who need access to billing information but should not edit or access other areas. This ensures separation of duties and enhances internal controls.
- **Product Manager:**
    - Permissions: Can edit product details, manage pricing, and update inventory. They can also access relevant reports to monitor product performance.
    - Use Case: Suitable for administrators responsible for managing products and their associated data. This group empowers them to maintain an up-to-date catalog and respond to market changes.
- **Super Admin:**
    - Permissions: Full access to all sections and functionalities of the system, including user management, system logs, and settings adjustments.
    - Use Case: Reserved for high-level administrators who oversee all operations. They ensure that the system runs smoothly and can intervene in critical situations.

Advanced Flexibility

Groups can be customized to allow or restrict access to specific features based on the organization’s structure. For instance:

- An administrator can be allowed to **view logs** but not modify system settings, maintaining accountability without compromising security.
- Permissions can be assigned for specific modules, such as allowing access only to the **Task Queue** or **Notification History**. This ensures that administrators focus on their designated responsibilities.
- Temporary permissions can be granted to an administrator for specific tasks and revoked afterward. This feature is particularly useful during audits, special projects, or temporary staffing situations.

Changing Passwords

The "Edit Administrator" section includes an option to **Change Password**. This is useful for resetting an administrator’s password if it is forgotten or needs to be updated for security reasons. Password changes can be enforced periodically to comply with organizational security policies.

Session IPs

Administrators can view the **Session IPs** associated with their account to track login activity and ensure security. This feature provides a detailed record of IP addresses used to access the account, helping identify unauthorized access attempts. Any suspicious activity can be flagged and addressed promptly, ensuring the integrity of the system.

Usage

This feature ensures that administrator accounts can be managed efficiently and securely. By leveraging the group and permission functionality, organizations can enforce strict access control while maintaining operational flexibility. The ability to customize groups and track activity adds a layer of accountability and transparency, fostering a secure and well-regulated administrative environment.

Revision #3
Created 17 January 2025 12:04:49 by Dmytro Kravchenko
Updated 17 January 2025 14:09:42 by Dmytro Kravchenko