Accounts

- Accounts (Info)
- Accounts (Permissions)
- Accounts (User and Access)

Accounts (Info)

Overview

The **Account Information** section provides an overview of the application account, including ownership details, account validity, resource limits, and supported platforms. This information helps administrators verify account status and available resources.

Account Details

The following details identify the application account and its subscription period.

Property	Value
App ID	XXXX
Owner	XYZ User
Email	xyz@example.com
Hash	XXXXXXXXX
Start Date	DD MMM YYYY
Expiry Date	DD MMM YYYY

> **Note:** The **Hash** is a unique identifier associated with the application account and may be used in application-specific URLs or integrations.

Account Quota

The **Account Quota** defines the maximum resources allocated to the application.

Property	Value
Product Limit	XX
Kiosk Limit	XX

Property	Value
Disk Space	XX MB / XX GB

Description

- **Product Limit** – Maximum number of products that can be created within the application.
- **Kiosk Limit** – Maximum number of kiosks that can be linked to the account.
- **Disk Space** – Total storage allocated for application data, images, and other uploaded files.

Channels

The **Channels** section displays the platforms that are enabled for the application.

Platform	Status
Enterprise	Yes / No
Android	Enabled / Disabled
iOS	Enabled / Disabled
Website	Open Dashboard

Description

- **Enterprise** – Indicates whether enterprise features are enabled.
- **Android** – Shows if Android devices are supported.
- **iOS** – Shows if iOS devices are supported.
- **Website** – Provides direct access to the application's web dashboard.

Additional Information

- Verify the **Start Date** and **Expiry Date** to ensure the subscription is active.
- Monitor the available **Product**, **Kiosk**, and **Disk Space** limits to avoid reaching account capacity.
- Use the **Dashboard** link to manage products, kiosks, users, and application settings.

Accounts (Permissions)

Overview

The **App Permissions** section allows administrators to control which features and modules are available for an application. Permissions can be enabled or disabled based on business requirements and the platforms being used.

Organize App Permissions

Permissions are categorized into different channels to simplify feature management across supported platforms.

Available Channels

Channel	Description
Website	Enables features for the web application.
Mobile	Enables features for Android and iOS applications.
Kiosk	Enables features for kiosk devices and interactive displays.

Available Permissions

The following permissions can be configured for the application.

Permission	Description
Call to Action (CTA)	Enables interactive call-to-action buttons and promotional actions.
Compare Products	Allows users to compare multiple products side by side.
Custom Forms	Enables customizable forms for collecting user information and feedback.
Kiosk	Grants access to kiosk-related functionality and configurations.

Permission	Description
Kiosk Flash Banner	Displays promotional banners or announcements on the kiosk home screen.
Kiosk Group	Allows kiosks to be organized and managed as groups.
Kiosk Order	Enables ordering functionality directly from the kiosk.
Map and Navigation	Provides interactive maps and navigation features.
Order	Enables product ordering and order management features.
Reference Products / Categories	Displays related or recommended products and categories.
Resource	Allows management of downloadable resources, documents, and media files.
Script	Enables custom scripts for additional functionality and integrations.
Video	Allows video content to be displayed within the application.
TryOn	Enables the virtual Try-On experience for supported products.

Managing Permissions

Administrators can enable or disable individual permissions depending on the application's requirements. Changes take effect after saving the configuration and may require the application to refresh or synchronize.

Best Practices

- Enable only the permissions required for your application.
- Disable unused modules to improve usability and simplify navigation.
- Review permissions regularly when adding new features or updating application requirements.
- Verify platform compatibility before enabling channel-specific features.

Accounts (User and Access)

Overview

The **Users and Access** section is used to manage all users associated with the application. Administrators can add new users, assign roles, monitor account status, and control access permissions.

User Management

This page displays a list of all registered users along with their account information and access details.

Available Information

Field	Description
Email	Email address used to sign in to the application.
Name	Full name of the user.
Role	Assigned user role (e.g., Admin, Editor, Viewer).
Expiry	Date until which the user's account remains active.
Status	Current account status (e.g., Active, Inactive, Pending Verification).
Action	Available actions such as Edit, Delete, or Manage User.

User List

The following table represents a sample user list.

Email	Name	Role	Expiry	Status
xyz.user@example.com	XYZ User	Admin	DD MMM YYYY	Active

Email	Name	Role	Expiry	Status
abc.user@example.com	ABC User	Editor	DD MMM YYYY	Active

> **Note:** The number of displayed entries can be adjusted using the **Show Entries** option, while the **Search** bar allows administrators to quickly locate users.

Available Actions

Administrators can perform the following actions from the **Users and Access** page:

- **Add User** – Invite a new user to the application.
- **Edit User** – Update user details and assigned roles.
- **Delete User** – Remove a user from the application.
- **Assign Role** – Change the user's permission level.
- **Activate** / **Deactivate** – Enable or disable user access.

User Roles

Depending on the application configuration, users may be assigned different roles.

Role	Description
Admin	Full access to all application features and settings.
Editor	Can manage content and application data but has limited administrative access.
Viewer	Read-only access to application data and reports.

Best Practices

- Assign the **Admin** role only to trusted users.
- Review user accounts regularly and remove inactive users.
- Set appropriate account expiry dates for temporary users.
- Ensure users verify their email address before granting full access.
- Periodically audit user roles to maintain application security.