Settings

- Settings (Notifications)
- Settings (Services)
- Settings (Credentials)
- Settings (Codes)
- Settings (Developers)

Settings (Notifications)

Overview

The **Catalog Notification** section allows users to manage email notifications for different catalog events. Users can add notification email addresses, configure event-based notifications, and enable or disable notification status as required.

Navigation

Home → Settings → Notification

Catalog Notification

The **Catalog Notification** page allows users to:

- Add new notification email addresses.
- View all configured email accounts.
- Assign email addresses to notification events.
- Enable or disable notifications for specific events.

Add Notification Email

To add a new notification email:

1. Enter the **Name**.
2. Enter the **Email** address.
3. Click on **Save**.

The newly added email will be available for notification events.

Email List

The **Emails** section displays all configured notification email addresses.

The list contains the following details:

Field	Description
Name	Displays the user's name.
Email	Displays the notification email address.
Verified	Indicates whether the email has been verified.
Used	Shows whether the email is currently being used.
Remove	Allows users to remove the email from the notification list.

Note: The default notification email is used unless another email is configured.

Global Notification

The **Global Notification** section allows users to configure notifications for different catalog events.

Available notification events include:

- **Message** – Sends notifications for all messages.
- **Order** – Sends notifications for all orders.
- **Form** – Sends notifications for submitted forms.
- **Script** – Sends notifications related to scripts.

Each event contains the following details:

Field	Description
Event	Displays the notification event.
Event Detail	Describes the notification event.
Email	Displays the email assigned to receive notifications.
Update	Allows users to modify the assigned email.
Status	Allows users to enable or disable notifications for the selected event.

Manage Notifications

To update notification settings:

1. Open the **Catalog Notification** section.

2. Select the required notification event.
3. Update the assigned email if required.
4. Enable or disable the **Status** according to your requirement.
5. Save the changes.

Available Actions

- **Add New Email:** Adds a new notification email.
- **Save:** Saves the entered email details.
- **Update:** Updates the email assigned to a notification event.
- **Status:** Enables or disables notifications for the selected event.
- **Remove:** Removes an email from the notification list.
- **Enable/Disable:** Controls whether notifications are sent for a specific event.

Settings (Services)

Overview

The **Services** section allows administrators to configure external services required by the application, such as **SMS Gateway**, **SMTP**, and **Payment Gateway**. These settings enable communication services, email notifications, and online payment processing.

Navigate to **Settings → Services** to configure these services.

SMS Gateway

The **SMS Gateway** is used to send SMS notifications, OTPs, and other text messages from the application.

Available SMS Gateways

- **Twilio**
- **FoxGlove**

Select the required SMS provider and configure it according to your account credentials.

SMTP Configuration

The **SMTP** section is used to configure email services for sending system-generated emails such as notifications, enquiries, password resets, and other email communications.

Configure the following fields:

Field	Description
Host	Enter the SMTP server host address.
Port	Specify the SMTP server port number.
Username	Enter the SMTP account username.

Field	Description
Password	Enter the SMTP account password.
Encryption	Select the encryption type (e.g., SSL/TLS).
From	Specify the sender email address.
From Name	Enter the sender name displayed in outgoing emails.

Payment Gateway

The **Payment Gateway** section allows administrators to configure online payment services for the application.

Available Payment Gateway

- **Easebuzz UPI**

Select the preferred payment gateway to enable online payment functionality for supported kiosk orders.

Manage Services

Administrators can:

- Configure an SMS Gateway.
- Configure SMTP email settings.
- Configure the Payment Gateway.
- Update service credentials whenever required.

Best Practices

- Verify all service credentials before saving.
- Use valid SMTP credentials to ensure successful email delivery.
- Configure the correct SMS Gateway before enabling SMS features.
- Verify the Payment Gateway configuration before accepting online payments.

> **Important:**
> After configuring the required services, click the **Submit** button to save the changes. Ensure that all credentials and service settings are correct before enabling them in the application.

Settings (Credentials)

Overview

The **Credentials** section allows administrators to securely store and manage application credentials in the form of **Key–Value** pairs. These credentials can be used by different modules and integrations within the application.

Navigate to **Settings → Credentials** to manage credentials.

Add New Credential

To create a new credential:

1. Navigate to **Settings → Credentials**.
2. Click **New Credential**.
3. Enter the required **Key**.
4. Enter the corresponding **Value**.
5. Save the credential.

Each credential is stored as a **Key = Value** pair for easy management and retrieval.

Credential Details

Field	Description
Key	A unique identifier used to reference the credential.
Value	The corresponding value associated with the key.

Manage Credentials

Administrators can:

- Add new credentials.
- View existing credentials.
- Update credential values.
- Delete credentials that are no longer required.

Best Practices

- Use unique and meaningful key names.
- Store only valid configuration values.
- Update credentials whenever service configurations change.
- Remove unused credentials to keep the configuration organized.

> **Important:**
> Credentials are stored as **Key–Value** pairs and may be used by different application modules or third-party integrations. Ensure that the correct values are entered before saving.

Settings (Codes)

Overview

The **Codes** section allows administrators to configure the format used for generating unique codes across different modules of the application. These codes help identify records such as **Orders**, **Form Responses**, **Script Responses**, and **TryOn Sessions** in a consistent and organized manner.

Navigate to **Settings → Codes** to configure code generation settings.

Code Configuration

Administrators can configure the following settings:

- **Timezone**
- **Default Prefix**
- **Default Digits**
- **Order Prefix**
- **Order Digits**
- **Form Response Prefix**
- **Form Response Digits**
- **Script Response Prefix**
- **Script Response Digits**
- **TryOn User Prefix**
- **TryOn User Digits**
- **TryOn Session Prefix**
- **TryOn Session Digits**

Each module can have its own unique prefix and digit length to generate easily identifiable codes.

Timezone

Select the appropriate **Timezone** for the application.

The selected timezone is used while generating date and time-based codes.

Default Code

The **Default Code** configuration is used for general-purpose code generation.

Configure:

- **Default Prefix**
- **Pattern**
- **Default Digits**

Example Pattern:

```
[PREFIX]/[YYYY]/[MM]/[DD]/NNNN
```

Example Output:

```
DEF/2026/07/23/0001
```

Order Code

Configure the code format for customer orders.

Fields:

- **Order Prefix**
- **Pattern**
- **Order Digits**

Example Output:

```
ORD/2026/07/23/0001
```

Form Response Code

Used to generate unique identifiers for submitted forms.

Fields:

- **Form Response Prefix**
- **Pattern**
- **Form Response Digits**

Example Output:

```
FORM/2026/07/23/0001
```

Script Response Code

Used to generate unique codes whenever a script response is recorded.

Fields:

- **Script Response Prefix**
- **Pattern**
- **Script Response Digits**

Example Output:

```
RESP/2026/07/23/0001
```

TryOn User Code

Generates a unique identifier for each TryOn user.

Fields:

- **TryOn User Prefix**
- **Pattern**
- **TryOn User Digits**

Example Output:

```
TRYUSER/2026/07/23/0001
```

TryOn Session Code

Generates a unique code for every TryOn session.

Fields:

- **TryOn Session Prefix**
- **Pattern**
- **TryOn Session Digits**

Example Output:

```
TRYON/2026/07/23/0001
```

Pattern Placeholders

The following placeholders can be used while creating custom code patterns.

Placeholder	Description	Example
[PREFIX]	Uses the configured prefix for the selected module.	ORD
[YYYY]	Four-digit year.	2026
[MM]	Two-digit month.	07
[DD]	Two-digit day.	23
[H]	Two-digit hour (24-hour format).	14
[M]	Two-digit minute.	35
[S]	Two-digit second.	48

Manage Code Settings

Administrators can:

- Configure prefixes for different modules.
- Define custom code generation patterns.
- Set the number of auto-generated digits.
- Configure timezone for date-based code generation.
- Maintain unique identifiers across the application.

Best Practices

- Use meaningful prefixes for each module.
- Configure different prefixes for different record types.
- Keep digit lengths consistent for better readability.
- Avoid using duplicate prefixes across modules.
- Verify the generated pattern before saving changes.

> **Important:**
> Every module can have its own **Prefix**, **Pattern**, and **Digit Length**. The application automatically generates unique codes based on these settings, ensuring that records such as **Orders**, **Form Responses**, **Script Responses**, and **TryOn Sessions** remain unique and easy to identify.

Settings (Developers)

Overview

The **Developers** section provides API credentials required for integrating the application with external systems, custom applications, or third-party services. It allows administrators and developers to securely access the application's APIs using generated authentication credentials.

Navigate to **Settings → Developers** to manage API credentials.

API Credentials

The **API Credentials** section contains the authentication details required for API access.

The following credentials are available:

Field	Description
API Key	A unique key used to identify and authenticate API requests.
API Token	A secure authentication token used to authorize API access.

These credentials are required when connecting external applications or services with the platform.

Generate API Token

Click **Generate API Token** to create a new API token.

A newly generated token can be used for secure API authentication. If an existing token is regenerated, the previous token may no longer be valid.

Manage API Credentials

Administrators can:

- View the existing API Key.
- Generate a new API Token.
- Use API credentials for application integrations.
- Authenticate API requests securely.

Best Practices

- Keep API credentials confidential.
- Do not share API Keys or API Tokens publicly.
- Regenerate the API Token if it is compromised.
- Use API credentials only in trusted applications and integrations.

> **Important:**
> The **API Key** and **API Token** are used to authenticate API requests. After generating a new API Token, ensure that all integrated applications are updated with the latest credentials.