Customer Account Access

Control customer account access by enforcing two-factor authentication, resetting passwords, disabling accounts, and unlocking accounts (which may have been locked due to the user failing to input the correct password).

2FA and OTP Authentication

You can trigger either of these authentication features on your storefront wherever you choose to in the buying journey—such as when the customer is logging into their account or immediately before checkout.

- **Two-Factor Authentication (2FA)**: This emails a 6-digit code to the customer after they attempt to log in with their username and password. This can be triggered upon every login, when a new device fingerprint is detected, or when they are accessing your site from a different region than their previous visit.
- **One-Time Password (OTP)**: This is an alternative login method that sends a temporary password to the customer as a 6-digit code.

You can enable both of these authentication strategies at the same time if you want to. When either one is triggered, the customer will have three minutes to input a valid code. If the time expires or they enter an incorrect code three times, they must request a new one.

Enable Authentication Options

Before integrating these functions into your storefront, enable them in your site settings:

1. Go to **System** > **Settings** > **General** > **Storefront**.
2. Scroll down to the the Customer Login Settings section.
3. Enable 2FA and/or OTP options depending on how you want to authenticate customers.

- **Always Require Two-Factor Authentication**: Triggers 2FA on every login attempt. If enabled, the Fingerprint Change and Region Change options will be disabled.

- **Two-Factor Authentication on Fingerprint Change**: Triggers 2FA when a login attempt is made from a new or unverified device fingerprint, including if there is no pre-existing device fingerprint to compare against. This can be enabled alongside Requires 2FA on Region Change.
- **Two-Factor Authentication on Region Change**: Triggers 2FA when a login attempt is detected from a different geographic region than the last validated region. This can be enabled alongside Requires 2FA on Fingerprint Change.
- **Allow Login using Email OTP**: Allows customers to request an email with a one-time password to log in with. This can be enabled alongside any 2FA settings.

4. Click the **Emails** tab and then toggle on **OTP for login** under Miscellaneous Emails.

5. Subscribe to the Email Requested [application event](#) (in the Email category) in order to trigger your own communications if you prefer not to use Kibo's emails.
6. Click **Save**.

Call OTP from the Storefront

To implement OTP in your storefront:

1. Provide a button or link on your storefront for the customer to request a code, which calls the Generate OTP Code endpoint (POST `.../api/commerce/customer/authtickets/otp/request`).
2. Include their User ID and email in the request body as shown below, as well as their device fingerprint and/or region. The email should generally be the address that the customer

entered in the username field, or the address associated with their account if the username is not a valid address.

```
{
  "userId": "string",
  "email": "string",
  "fingerprint": "string",
  "region": "string"
}
```

3. Once the customer enters a code on your storefront, call the Validate OTP endpoint (POST `.../api/commerce/customer/authtickets/otp/auth`) with the below IDs and entered code value.

```
{
  "userId": "string",
  "customerAccountId": 00000,
  "otpCode": "string",
  "fingerprint": "string",
  "region": "string"
}
```

4. A successful validation will return a 200 OK response with `"requires2fa" = false` and a new auth token, allowing the customer to proceed. A 401 Unauthorized error with `"requires2fa" = true` instead indicates that the code was invalid and they should try again.

Call 2FA from the Storefront

To implement 2FA on your storefront:

1. When the user attempts to log in, call the Create User Auth Ticket API and provide the region and/or device fingerprint that you obtain from the user's device.

```
{
  "username": "string",
  "password": "string",
  "accountId": 00000,
  "fingerprint": "string",
  "region": "string"
}
```

2. The system will verify the region and/or device fingerprint against their previously validated records and update the user claims to indicate whether the `requires2fa` flag is true or false. Check these user claims after making the request to determine your next step.

3. If 2FA is required, call the Generate 2FA Code endpoint (POST `.../api/commerce/customer/authtickets/2fa/request`) and provide the customer's User ID in the request body. The email with a code will be sent to the address associated with their account.

```
{
  "userId": "string"
}
```

4. Once the customer enters a code on your storefront, call the Validate 2FA and Create Auth Ticket endpoint (POST `.../api/commerce/customer/authtickets/2fa/auth`). Provide the User ID and code that they entered in the request body.

```
{
  "userId": "string",
  "otpCode": "string"
}
```

5. A successful validation will return a 200 OK response with `"requires2fa" = false` and a new auth token, allowing the customer to proceed. A 401 Unauthorized error with `"requires2fa" = true` instead indicates that the code was invalid and they should try again.

Reset Shopper Passwords

If a customer has forgotten their password or having other issues logging in, you can reset it from the Admin UI. Bear in mind that only registered shopper accounts have passwords; guest accounts cannot log in.

1. Go to **Main** > **Customers** > **Customers**.
2. Browse or search for the account you want to reset the password for.
3. Select the account.
4. Click **Reset Password** next to the **Account Status** value.
5. Confirm.

> ℹ️ All registered customers' passwords must be at least six characters in length, and include at least one number and one letter. For security purposes, the reset link will remain active for only 72 hours.

Disable Shopper Access

If needed, you can fully disable a customer's access to their account. Keep in mind that you can only disable registered shopper accounts; guest accounts cannot log in. Furthermore, disabling an account only prevents the shopper from logging in with the email address associated with the account. It does not prevent that individual from registering for another account with a different address.

1. Go to **Main** > **Customers** > **Customers**.
2. Browse or search for the shopper account you want to disable.
3. Select the account.
4. Select the **Disable Account** checkbox below the **User Name** field.
5. Click **Save**.

Unlock Locked Accounts

If a shopper tries and fails to log in too many times, the account may become locked. To unlock it:

1. Go to **Main** > **Customers** > **Customers**.
2. Browse or search for the shopper account you want to reset the password for.
3. Select the account.
4. Click **Unlock Account** next to the **Account Status** value.
5. Confirm.