

Customer Portal: Multi-Factor Authentication (MFA)

Last updated by | David Mishler Gomocha | Oct 1, 2025 at 11:45 AM GMT+2



Customer Portal: Multi-Factor Authentication (MFA)

 41099 As an organization I would like to have MFA authentication on the FSP Customer Portal | Done

Description

Efficiency

- Secure Customer Access with Always-On Protection

What it is

- Multi-Factor Authentication (MFA) for Customer Portal

What it does

- Requires customers to verify their identity using both their password and a secondary authentication method (email or SMS) every time they log into the Customer Portal, with MFA permanently enabled for all users.

Why it Matters

- Password breaches happen daily, and compromised customer accounts can expose sensitive asset data and service information. When customers access your portal with just a password, you're one data leak away from a security disaster that damages trust and potentially violates compliance requirements.

Value

- Prevents unauthorized access even with compromised passwords
- Protects sensitive customer asset and service data
- Maintains compliance with security standards
- Builds customer trust through visible security measures
- Reduces risk of data breaches and associated costs

Where it Fits in Gomocha FSP

- Digital Transformation
-

Configuration Steps

- **MFA Enforcement**

- Multi-Factor Authentication (MFA) is always enabled and cannot be turned on or off by the user.

- **User Contact Information**

- Customer Portal users cannot edit their phone number or email address.
- When a contact person is promoted to a Customer Portal user, both their email and phone number are applied to the account (including updates).
- Phone numbers are validated to ensure they are real and parseable; if validation fails, the phone number field will remain blank in the Customer Portal account.

- **Portal Settings for SMS (Twilio)**

- New system-wide settings are added under the **System Settings** tab (not organization-specific).
- Required parameters: **Twilio Client ID, Client Secret, From Phone Number**.

- **Login Process with MFA**

- When logging in, MFA is required.
- Users are presented with two verification options:
 - **Send to Email** – always available if the email address is confirmed.
 - **Send to SMS** – available only if the user has a valid phone number and SMS settings are correctly configured in the Portal.

Contact [@Christopher Dashiell Gomocha](#) when needing to configure SMS settings

Output/Usage

Steps to Log In to the Customer Portal with Multi-Factor Authentication (MFA):

1. Go to the **Customer Portal login screen** and log in.
2. User will be directed to the “**Choose Verification Method**” screen. Select preferred verification method:
 - **Email** – always available
 - **SMS** – available only if configured
3. A **verification code** will be sent using the selected method.
4. Enter the **verification code**.
5. User is now logged into the Customer Portal using **Multi-Factor Authentication**.



Login

Reset password

Login

Email address

dmishler@gomocha.com

Password

Login



Choose a Verification Method

☒ Email – Send code to your registered email address

Submit

Verification Code

QA test | Gomocha
To: David Mishler | Gomocha

Reply Reply All Forward More
Wed 9/25/2023 10:21 PM

Hello David Mishler,
For security purposes, please use the code below to complete your sign-in.

Your verification code: 104993

If you did not request this code, you can safely ignore this email.

This email was sent by Gomocha BV.
© 2024 Gomocha BV. All rights reserved.



Enter Verification Code

Verification Code

104993

Submit

Announcement				
Asset	Contract	Open orders	Planned orders	Open quotes
2	2	22	3	1