Multi-Factor Authentication - OPSCOM-Go! User Portal

> The User Portal Multi-Factor Authentication (MFA) feature adds an essential layer of security to user accounts by requiring a One-Time Password (OTP) during the login process. Its primary purpose is to protect sensitive user data and ensure that only authorized individuals can access the parking portal. This article is intended for OPSCOM administrators to help them understand the user MFA workflow and support their clients.

Setup and Configuration

This feature requires the organization to have MFA support enabled on their system. Once available, the configuration is primarily handled on the User Side, where individual users opt-in and manage their own security settings.

Admin Side: Ensure that your system's email templates are properly configured, as the OTP emails will utilize the standard system email formatting designated for your account.

Using this Feature

Administrators can use the following instructions to guide users through enabling MFA on their accounts and logging in with One-Time Passwords.

Enabling Multi Factor Authentication

1. Log in to the User Portal and click your name in the top corner of the screen.
2. Click **Security** from the drop-down menu.
3. Scroll to the Multi-Factor Authentication section and click the **Change Multifactor Authentication Settings** button.
4. Choose **Enable One-Time Passwords** from the available settings.
5. Click the **Send One-Time Password To Email** button.
6. Navigate to your registered email inbox and copy the generated OTP.
7. Return to the portal and enter the OTP alongside your current account password in the provided fields.
8. Click the **Submit** button to confirm your changes and activate MFA.

> One-Time Passwords are only valid for 15 minutes. If the user's password expires before they enter it, they must generate a new one. Generating a new OTP automatically invalidates any previously unused passwords.

Logging In with MFA Enabled

Once MFA is successfully enabled, the standard login workflow will change to include the OTP validation step.

1. Enter your username and password on the main portal login page.
2. Check your registered email address for the automatically generated OTP.
3. Enter the OTP into the prompt on the screen.
4. Click the **Submit** button to complete the login process and access the site.

> When MFA is active, the system restricts access to the portal. Users will be forcibly redirected to the OTP entry screen if they attempt to navigate to any other internal pages (such as their profile or vehicle management) before submitting a valid One-Time Password.

Understanding OTP Session Settings

When guiding users through their MFA settings, administrators should be aware of how the system handles active OTP sessions:

- **Session Storage:** Once a user enters an OTP, the validation is stored in their browser's local session data. If they clear their browser's local storage or cache, they will be forced to enter a new OTP upon their next login.
- **Different Devices:** OTP session data does not persist across different browsers or hardware. If a user logs in from a new computer, a secondary mobile device, or a different web browser, they will be prompted to enter a new OTP.

Best Practices and Considerations

- **Educate users on OTP expiration: Always remind users that One-Time Passwords strictly expire after 15 minutes.** If a user complains about invalid codes, ensure they are not attempting to use an expired OTP or one that was invalidated when they clicked the send button multiple times.
- **Assist with device switching: Inform users that they will need access to their email whenever they switch devices.** Because

OTPs are tied to local session storage, attempting to log in on a new phone or public computer will always trigger a new OTP request.

Revision #15
Created 9 October 2024 08:10:54
Updated 25 August 2026 13:51:42