Configuring Multi-Factor Authentication on the User Portal

> Multi-Factor Authentication (MFA) adds a crucial second layer of security to user accounts by requiring one-time passwords (OTPs) sent via email. Its primary purpose is to significantly enhance protection against unauthorized access to the system. This article is intended for OperationsCommander (OPSCOM) administrators responsible for configuring global security settings and managing the user login experience.

Setup and Configuration

Implementing MFA involves administrator-side configuration within the system settings and customizing the associated email template.

Admin Side Configuration

One-time passwords will not be available on the user portal until enabled within the global settings.

1. Hover over **System Configuration** and click **System Settings**.
2. Navigate to the **User Profile** tab.
3. Configure the **Enable Multi-Factor Authentication** setting to your desired state.

> If the MFA setting is not available for you to change, please have your primary administrator contact support@ops-com.com to have the feature enabled for your environment.

Email Template Configuration

The content of the one-time password email sent to users is defined within a dedicated email template.

1. Hover over **System Configuration**, click **Content & Designs**, then **Email Templates**.
2. Locate and click the **One-Time Password Email Template** to edit its contents.
3. Define the message and insert any relevant organizational branding.
4. Utilize the available shortcodes to insert the OTP details:
   - `[one_time_password]`: Inserts the randomly generated one-time password.
   - `[one_time_password value="issued_at"]`: Inserts the time the password was generated.
   - `[one_time_password value="expires_at"]`: Inserts the time the password expires.

Using this Feature

Administrators can use the ternary setting to flexibly control how MFA is implemented across the user portal, while users manage their individual settings from their profile.

Available Configuration States

The **Enable Multi-Factor Authentication** setting has three distinct states:

- **Hidden:** The use of one-time passwords is disabled site-wide. Users will not see or be able to enable MFA on their accounts.
- **Visible:** The use of one-time passwords is enabled, but it is left optional for individual users to decide if they want to enable it on their account.
- **Required:** The use of one-time passwords is mandatory for all users of the portal. Users who do not have it enabled will be automatically redirected to the setup page upon their next login and must configure it before accessing their account.

User Management

Users can enable and manage their one-time password settings directly from their security page. For detailed instructions on the user experience, please refer to the *Multi-Factor Authentication - OPSCOM-Go! User Portal* wiki article.

> The state of a user's one-time password verification is stored in the local storage of their session data. If a user clears their browser cache, or attempts to log in using a different web browser or device, the MFA verification will not persist and they will be forced to enter a new one-time password.

Best Practices and Considerations

- **Execute a gradual rollout: When introducing MFA, consider starting with the Visible setting to allow users to opt-in voluntarily.** Once your user base is accustomed to the feature,

transition the setting to the **Required** state for all users if your organizational security policy mandates it.

- **Verify email deliverability: Ensure that your system's email settings are correctly configured and that OTP emails are not being blocked by institutional spam filters.** Users must receive these emails promptly to successfully log in.
- **Communicate OTP expiry limits: Remind users that one-time passwords are time-sensitive and permanently expire after 15 minutes.** Generating a new password will automatically invalidate any previous ones, and this system default cannot be changed.
- **Provide clear communication and training: Inform users about the MFA requirement, how to set it up, and how to log in using OTPs.** Providing clear instructions and troubleshooting tips on your portal homepage reduces support tickets during the initial rollout.

Revision #11
Created 9 October 2024 08:02:29
Updated 2 September 2026 12:37:42