

Configuring Multi-Factor Authentication on the User Portal

Multi-Factor Authentication (MFA) adds a crucial second layer of security to user accounts in OPS-COM, significantly enhancing protection against unauthorized access. Currently, the primary method implemented is the use of **one-time passwords (OTPs)** sent via email. This article outlines how administrators can configure MFA at the system level and how users interact with this enhanced security feature on their portal.

Setup & Configuration

Implementing MFA involves administrator-side configuration within 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 **System Settings**.

1. Hover over **System Configuration** and click **System Settings**.
2. On the **User Profile** tab, click **Enable Multi-Factor Authentication**.

If this setting is not available for you to change, please have your primary Admin contact support@ops-com.com to have it turned on.

This is a **ternary setting**, meaning it has three different states, allowing for flexible control over MFA implementation:

- **Hidden:** The use of one-time passwords is **disabled** site-wide. Users will not see or be able to enable MFA.
- **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 website.

- If MFA is set to **Required**, users who do not have it enabled on their account will be automatically redirected to the setup page upon their next login and will be required to set it up before they can access their account.

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, Content & Designs** and click **Email Templates**.
2. Locate and edit the **One-Time Password Email Template**.

Here, administrators can define the message and branding of the email. In addition to general user-specific shortcodes, this template includes specific shortcodes for OTP details:

- `[one_time_password]`: Inserts the randomly generated one-time password.
- `[one_time_password value="issued_at"]`: Inserts the time the one-time password was generated.
- `[one_time_password value="expires_at"]`: Inserts the time the one-time password expires.

One-time passwords always expire after **15 minutes**. This cannot be changed.

The screenshot displays the configuration interface for the 'One-Time Password Email Template'. On the left, under 'HTML Content', a list of tokens is provided: `[one_time_password]` (The one-time password), `[one_time_password value="issued_at"]` (The time the one-time password was generated), `[one_time_password value="expires_at"]` (The time the one-time password expires), `[user show="firstname"]` (The first name of the user), `[user show="lastname"]` (The last name of the user), `[user show="email"]` (The email of the user), `[user show="username"]` (The username of the user), and `[user show="salutation"]` (The salutation of the user). The main editor on the right shows a preview of the email content, which includes a title 'Your One-Time Password', a greeting 'Hi, [user show="username"]!', a password display 'Here is your one-time password: [one_time_password]', a validity notice 'This password is only valid for the next 15 minutes and will expire at [one_time_password value="expires_at"]', and a security warning 'If the password has expired, a new one will need to be generated. For security purposes, you should not share this password with anyone else.' The interface also features a standard rich text editor toolbar and a footer indicating 'Powered by TinyMCE' and 'Words: 59'.

Using this Feature

User-Side MFA Management

Users can enable and manage their one-time password settings from their security page (formerly the passwords page). [Refer to this wiki article](#) to see the steps involved.

The state of the user's one-time password verification is stored in the local storage of their session data. If the local storage is cleared (e.g., clearing browser cache), they will have to enter another one-time password. The MFA verification does not persist across different web browsers or devices, meaning the user will have to enter a new one-time password if they try to log in using another browser or device.

Best Practices & Considerations

- **Security Enhancement:** MFA significantly reduces the risk of unauthorized access, even if primary login credentials are compromised. It is highly recommended for all users.
- **Gradual Rollout (Visible vs. Required):** When introducing MFA, consider starting with the **Visible** setting to allow users to opt-in voluntarily. Once accustomed, transition to **Required** for all users if your security policy mandates it.
- **Clear Communication:** Inform users about the MFA requirement, how to set it up, and how to log in using OTPs. Provide clear instructions and troubleshooting tips.
- **Email Deliverability:** Ensure that your system's email settings are correctly configured and that OTP emails are not being blocked by spam filters. Users need to receive these emails promptly to log in.
- **Template Customization:** Customize the OTP email template to include your organization's branding and any specific instructions for your users.
- **User Training:** Consider providing brief training or a guide for users on how to manage their MFA settings and log in with OTPs.
- **OTP Expiry:** Remind users that OTPs are time-sensitive (15 minutes) and that generating a new one invalidates previous ones.

Revision #5

Created 9 October 2024 08:02:29 by Co-op Student

Updated 19 June 2025 09:56:30 by Cedar Boulianne