# Security with OperationsCommander

**OperationsCommander works hard to maintain an up to date product wiki! If you have any questions or if you feel something is missing, post about it in the community.**

- Enhanced Admin Security: Multi-Factor Authentication (MFA) with OperationsCommander
- Resetting an Administrator's Forgotten Password

# Enhanced Admin Security: Multi-Factor Authentication (MFA) with OperationsCommander

> Multi-Factor Authentication (MFA) provides a critical layer of security for OPSCOM administrator accounts by requiring an email-delivered One-Time Password (OTP). Its primary purpose is to significantly strengthen account protection and prevent unauthorized access to sensitive system data. This article is intended for OPSCOM administrators.

## Setup and Configuration

The MFA feature offers three distinct configuration levels for your organization's administrative portal. Currently, modifying your site's overall MFA setting requires assistance from our team. If you wish to adjust your configuration, please contact **support@ops-com.com**.

### Available Configuration Options

- **Hidden:** MFA is strictly required for security-sensitive actions only. It will not appear during a standard login attempt.
- **Visible:** Administrators are given the choice to use MFA during standard logins. It remains mandatory for security-sensitive actions.
- **Required:** MFA is mandatory for every administrator login and all security-sensitive actions.

## Using this Feature

Depending on your organization's configuration, you will interact with the MFA prompt during the standard login process or when performing critical account updates.

### Authenticating a Login

When MFA is set to Visible or Required, the system will prompt you to authenticate your identity after entering your username and password.

1. Enter your standard administrator credentials on the login screen.
2. Check your associated email inbox for the automatically generated One-Time Password (OTP).
3. Enter the OTP into the provided MFA prompt on the screen to access the administrative portal.

### Mandatory Security Actions

Regardless of your site's overall MFA configuration level (Hidden, Visible, or Required), an OTP is always mandatory when performing the following security-sensitive actions:

- Admin Account Creation
- Password Changes

> In OperationsCommander, the MFA email is classified as a mandatory security communication. These authentication emails will always be sent to the administrator, even if they have explicitly unsubscribed from all email communication categories on their user profile.

Originally requested on this community item!

---

## Best Practices and Considerations

- **Enforce Maximum Security: Organizations should use the Required setting as their standard business rule.** Mandating MFA for every administrative login provides the highest level of protection against compromised credentials and unauthorized system access.
- **Verify Email Addresses:** If an administrator does not receive their MFA code, their email address may be missing, outdated, or misspelled on their user profile. They must contact a primary system administrator to have their profile updated before they can log in.

# Resetting an Administrator's Forgotten Password

> The Administrator Password Reset feature allows users to securely recover access to their OperationsCommander (OPSCOM) administrative accounts. Its primary purpose is to provide a self-service method for resetting forgotten credentials quickly without requiring manual intervention from a primary system administrator. This article is intended for OPSCOM administrators who need to regain access to their portal.

## Setup and Configuration

This feature is available by default on the Admin Login page and requires no specialized system setup to function. However, the system relies on the email address recorded in the user's profile to deliver the reset link.

Administrators with system configuration access can customize the automated email sent during this process by navigating to the *Email Templates* page and modifying the Lost Passwords template.

## Using this Feature

If an administrator has forgotten their login credentials, they can initiate a secure reset process directly from the login screen.

1. Navigate to the Admin Login page and click **Forgot your Username or Password**.
2. Enter the valid email address currently associated with your administrator profile.

3. Click the **Send Reminder** button to trigger the automated email. The screen will refresh to display a confirmation message.
4. Check your email inbox for the password reset message and click the provided secure link.
5. Enter your email address into the recovery interface.
6. Enter your new password, and type it a second time in the confirmation field.
7. Click the **Reset Password** button to finalize the change.
8. Log in to the OPSCOM administrative portal using your newly created password.

> If you do not receive the password reset email within a few minutes, check your spam or junk folders. The system will only send the email if the address entered exactly matches an active administrator profile.

---

## Best Practices and Considerations

- **Maintain updated contact information: Ensure that the email address on your admin profile is always accurate and current.** If an administrator loses access to the email account on file, they will be entirely unable to use this self-service reset feature and will be locked out until a primary administrator intervenes.
- **Customize the automated email: Organizations should configure the *Lost Passwords* email template to match internal IT policies.** Including specific instructions or support contact details within the template helps reduce confusion if an administrator experiences issues during the reset process.