Password and Security Settings

> The Security Settings in OPSCOM provide administrators with critical tools to enforce robust password policies and manage login security for all administrative accounts. Properly configuring these settings is essential for protecting sensitive system data, preventing unauthorized access, and complying with organizational security standards.

Security settings are managed within the **System Settings** area of OPSCOM.

1. Hover over **System Configuration,** and click **System Settings**.
2. Click **Security**. The **Manage System Settings** window will open, displaying all available security configurations.

Using this Feature

The **Security** component within **System Settings** allows administrators to configure various aspects of password management and account lockout policies.

Password Security Settings

- **Salted Password Hashing**:
  - **Purpose**: This setting adds an essential layer of security to stored passwords. Hashing is a one-way, irreversible process that converts a user's password into a unique, short hash value. "Salting" introduces a random string into this process, ensuring that even if two users have the same password, their stored hash values will be

different. This prevents "lookup" (reverse engineering) of the original password, meaning forgotten passwords must be reset, not retrieved. This significantly limits an administrator's ability to view employee passwords and closes a critical security vulnerability.

> **Note**: Once **Hash and Salt** is enabled, it **should not be turned off**.

- **Require Password Update**:
  - **Purpose**: When activated, this setting forces users to change their passwords upon their next login.
  - **Use Case**: Ideal for ensuring compliance with regular password changes or after a password reset by an administrator.
- **Toggle Password Expiry**:
  - **Purpose**: By default, passwords in OPSCOM do not expire. For enhanced security, it is best practice to mandate regular password changes. This setting enables the use of password expiry.
  - **Configuration**: Toggle this setting **On**.
  - **Password Expiry in days**: Enter the number of days after which an administrator's password will expire, aligning with your organization's security policy (e.g., 90 days).
- **Enable Password History**:
  - **Purpose**: When toggled **On**, OPSCOM will remember passwords previously used by an administrator. The system will then prevent the reuse of those passwords for a specified period.
  - **Configuration**: Set **How long to remember old passwords** (in days) to define the duration for which old passwords are not allowed to be reused.

Password Strength Requirements

These settings allow you to enforce complexity rules for administrator passwords.

- **Minimum Password Length**: Sets the minimum number of characters required for a password.
- **Enable password strength requirements**: Toggles on or off the following specific complexity requirements:
  - **Numerical Characters**: Sets the minimum number of numbers required in the password.
  - **Lower Case Characters**: Sets the minimum number of lowercase characters required in the password.
  - **Upper Case Characters**: Sets the minimum number of uppercase characters required in the password.
  - **Non-Alpha Numeric**: Sets the minimum number of non-alphanumeric (special) characters required in the password (e.g., `!, &, #,` etc.).

Admin Account Lockout Settings

These settings provide an additional layer of security by locking an administrator out of their account after repeated incorrect password attempts.

- **Enable Admin Lockouts**: Toggles on or off the account lockout feature.
- **Lockout after X Attempts**: Sets the number of failed login attempts with an incorrect password before the system will lock out the administrator.

- **Login attempt timeframe**: Sets the timeframe (in minutes) during which incorrect login attempts are counted. For example, if an administrator fails 3 times within a 5-minute period, their account will be locked out.
- **Lock the admin out for X minutes**: Sets the duration (in minutes) that the administrator's account will remain locked. For example, setting it to `120 minutes` would mean the administrator is locked out for 2 hours before another login attempt is permitted.

Best Practices & Considerations

- **Robust Security Policy**: Always implement a robust security policy that combines strong password requirements (length, complexity), password expiry, and lockout mechanisms.
- **Enable Hashing**: Ensure **Salted Password Hashing** is always enabled for maximum password security.
- **Regular Password Expiry**: Enforce regular password expiry (e.g., every 90 days) to mitigate the risk of compromised credentials.
- **Meaningful Lockout Settings**: Configure lockout settings to balance security with user convenience. Too aggressive settings can lead to frequent lockouts, while too lenient settings can be a security risk.
- **Communication**: Inform administrators about the security policies in place, including password strength requirements, expiry rules, and lockout procedures. This helps them comply and understand why they might be locked out.
- **Admins can see, only OPSCOM Team can change**: Several security settings (e.g., **Hash and Salt**, **Require Password Update**, **Toggle Password Expiry**, **Enable Password History**, **Enable password**

strength requirements, **Enable Admin Lockouts**) are visible to administrators but can only be changed by the OPSCOM Team. For modifications to these specific settings, contact OPSCOM Support.

Revision #4
Created 15 May 2024 08:17:33
Updated 23 July 2025 14:33:58