Password and Security Settings

> The Password and Security Settings feature provides administrators with critical tools to enforce robust password policies and manage login security for all backend administrative accounts. Its primary purpose is to protect sensitive system data, prevent unauthorized access, and ensure organizational compliance with modern security standards. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing backend system configuration and access security.

Setup and Configuration

This feature requires high-level administrative access to view and manage global security protocols.

Admin Side: Administrators must have the appropriate system role permissions enabled to access the centralized system settings menu.

1. Hover over **System Configuration** and click **System Settings**.
2. Click **Security** to open the management window and view all available security configurations.

User Side: This feature dictates backend administrative security and does not directly configure the end-user parking portal login policies.

Using this Feature

Administrators can use the configuration window to define various aspects of password management, strength requirements, and automated account lockout policies.

Password Security Settings

- **Salted Password Hashing:** Adds an essential layer of security by irreversibly converting passwords into unique, short hash values with a randomized "salt" string. This ensures that even if two users share the same password, their stored hash values remain completely different. It prevents reverse engineering, meaning forgotten passwords must be reset rather than retrieved.
- **Require Password Update:** Forces administrators to change their passwords upon their next successful login. This is ideal for ensuring compliance after a manual password reset.
- **Toggle Password Expiry:** Mandates regular password changes. When enabled, enter a numerical value into the **Password Expiry in days** field to define the exact lifecycle of an active password (e.g., 90 days).
- **Enable Password History:** Remembers passwords previously used by an administrator to prevent immediate reuse. When enabled, set the **How long to remember old passwords** field (in days) to define the restriction duration.

Password Strength Requirements

These settings allow you to enforce complexity rules for all new administrator passwords:

- **Minimum Password Length:** Sets the absolute minimum number of characters required for a valid password.

- **Enable password strength requirements:** Toggles specific complexity rules on or off. When enabled, you can set a minimum required character count for **Numerical Characters**, **Lower Case Characters**, **Upper Case Characters**, and **Non-Alpha Numeric** characters (e.g., !, &, #).

Admin Account Lockout Settings

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

- **Enable Admin Lockouts:** Toggles the automated account lockout feature on or off.
- **Lockout after X Attempts:** Sets the threshold for failed login attempts with an incorrect password before the system actively locks 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 means the administrator is completely locked out for 2 hours before another login attempt is permitted.

> Several major security settings (such as Salted Password Hashing, password expiry, and lockouts) are visible to administrators but can only be changed by the OPSCOM Team. For modifications to these restricted,

> read-only settings, please contact support@ops-com.com.

Best Practices and Considerations

- **Enable salted password hashing: Ensure Salted Password Hashing is permanently enabled for maximum password security.** Once enabled, this setting should never be turned off, as doing so reopens a critical security vulnerability and allows administrators to view raw employee passwords.
- **Maintain a robust security policy: Always implement a comprehensive security policy that combines strong password requirements, mandatory expiry limits, and lockout mechanisms.**
- **Enforce regular password expiry: Enforce regular password expiry intervals (e.g., every 90 days) to mitigate the risk of compromised credentials.** Stale passwords are a primary vector for unauthorized access.
- **Configure meaningful lockout settings: Configure lockout settings to balance strict security with user convenience.** Overly aggressive settings can lead to constant lockouts and administrative overhead, while lenient settings fail to prevent active brute-force attacks.
- **Communicate policies to staff: Inform administrators about the security policies in place, including password strength requirements and lockout procedures.** Clear communication helps staff comply and understand exactly why they might be temporarily locked out of the system.

Revision #6
Created 15 May 2024 08:17:33
Updated 17 August 2026 14:47:57