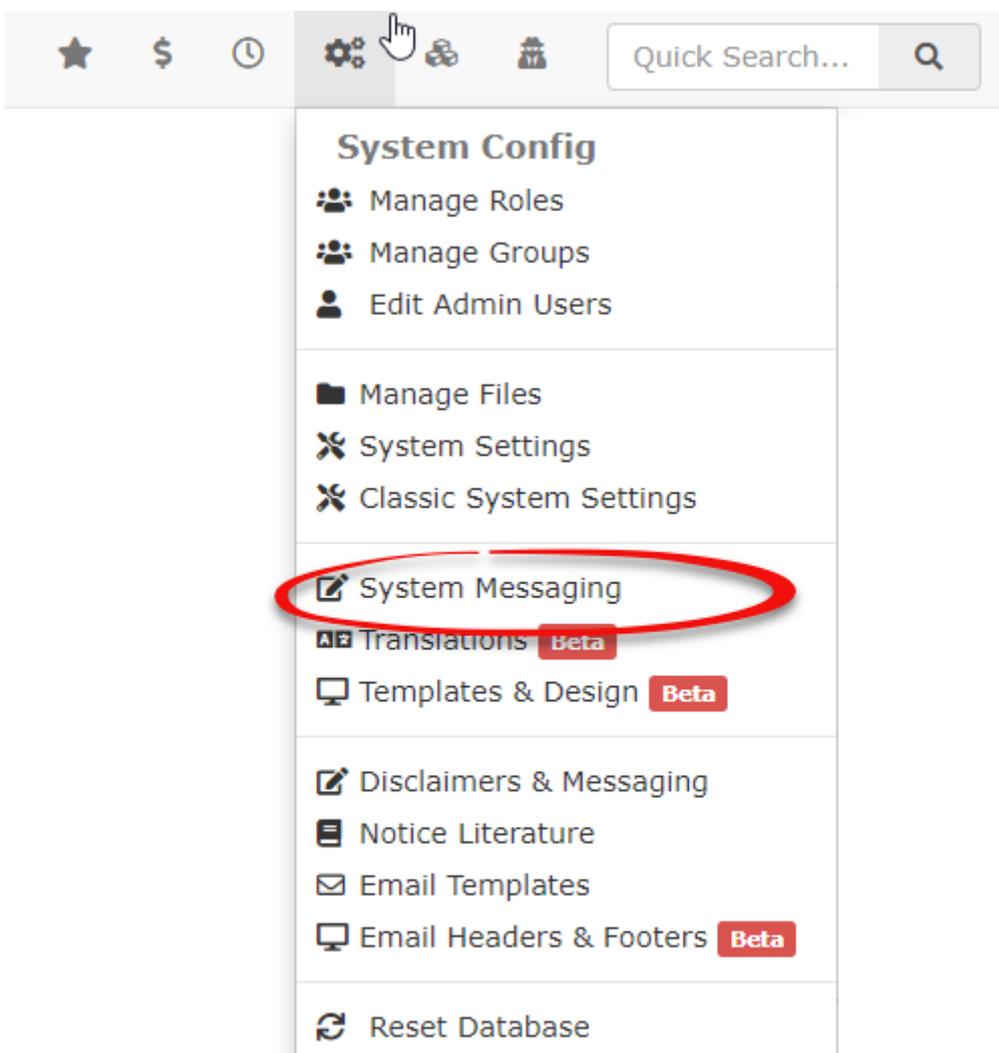


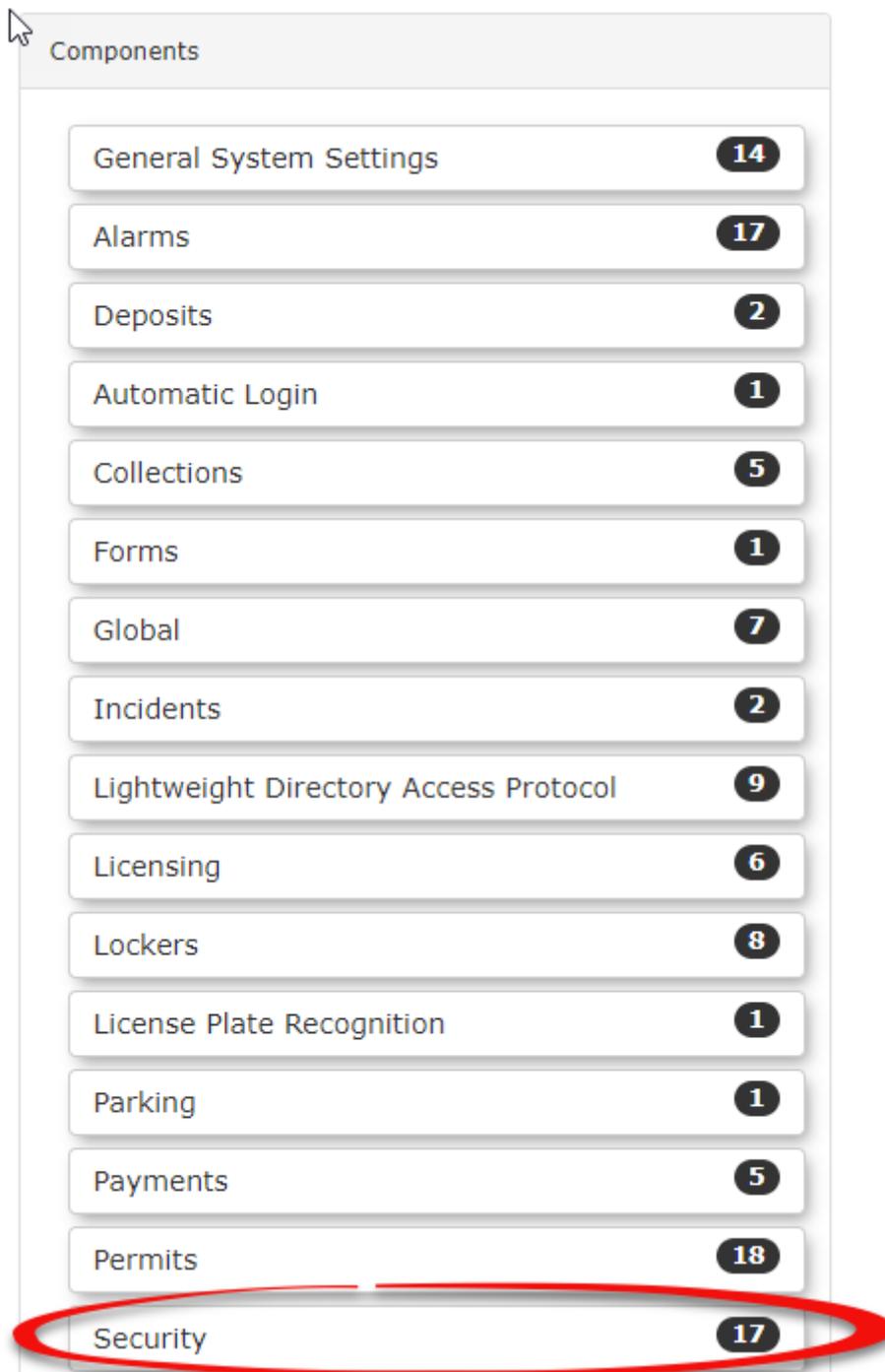
# Password and Security Features

## Manage Security Settings

To edit security settings, hover over **System Config** and click **System Settings**.



In System Settings, click **Security** in the list of settings.



The image shows a software interface with a 'Components' menu. The menu items are listed in a vertical stack, each with a corresponding count in a black circle. The 'Security' item at the bottom is circled in red.

Component	Count
General System Settings	14
Alarms	17
Deposits	2
Automatic Login	1
Collections	5
Forms	1
Global	7
Incidents	2
Lightweight Directory Access Protocol	9
Licensing	6
Lockers	8
License Plate Recognition	1
Parking	1
Payments	5
Permits	18
Security	17

The Manage System Settings window will open and all the security settings will be available.

## Manage System Settings

Editing Settings: Security **17**

These settings are used to control the Security Module.

Hash and Salt Passwords

**Password storage method** salthash

Require Password Update

Toggle Password Expiry

**Password Expiry in Days** 90

Enable Password History

**How long to remember old passwords** 365

# Salted Password Hashing, Password Update, Toggle Password Expiry and Enable Password History

Using salted password hashing adds an extra layer of security to stored passwords. Hashing is a one-way, irreversible process that takes the password a user enters and converts it into a short hash value. Salting randomizes the string of digits for the hash value so that two users have the same password, they will have different hash strings. It is not possible to reverse engineer a hash, so you cannot “look up” what the original password was. Instead, a user who forgets their password, for example, would have to reset it completely. This limits an administrator’s ability to view the passwords of employees and closes up a security vulnerability.

**Require Password Update** - When activated, this setting will force users to change their passwords on next login.

**Toggle Password Expiry** - By default passwords do not expire. For added security, it is good practice to have passwords expire every 90 days. You can enter the number of days before a password expiry to conform with your organization's security policy and toggle it on.

**Enable Password History** - When toggled on, OPS-COM will remember the passwords you have used in the past, and will not allow repeat use of the password for the time set in days.

The image shows a configuration interface with two main sections: Password Strength Settings and Admin Lockout Settings. The Password Strength Settings section includes a 'Minimum Password Length' field set to 2, a toggle for 'Enable Password Strength Requirements' which is currently off, and four character requirement fields: Numerical Characters (0), Lower Case Characters (3), Upper Case Characters (2), and Non-Alpha Numeric (1). The Admin Lockout Settings section includes a toggle for 'Enable Admin lockouts' which is currently off, and three fields: 'Lockout after X attempts' (3), 'Login attempt timeframe' (5), and 'Lock the admin out for X minutes' (120). A 'Save Settings' button is located at the bottom of the Admin Lockout Settings section.

Password Strength Settings	
Minimum Password Length	2
<input type="checkbox"/> Enable Password Strength Requirements	
Numerical Characters	0
Lower Case Characters	3
Upper Case Characters	2
Non-Alpha Numeric	1

Admin Lockout Settings	
<input type="checkbox"/> Enable Admin lockouts	
Lockout after X attempts	3
Login attempt timeframe	5
Lock the admin out for X minutes	120

Save Settings

## Password Strength and Admin Lockout

Using **Password Strength Settings** the admin can set rules for how complex a password needs to be to meet security rules.

These settings include:

**Minimum Password Length** - minimum number of characters in the password

**Enable Password Strength Requirements** - Toggles on or off the following requirements:

- Minimum number of Numerical Characters required in the password
- Minimum number of Lower Case Characters required in the password
- Minimum number of Upper Case Characters required in the password
- Minimum number of Non-Alpha numeric Characters required in the password (Special characters such as !,&,#, etc.)

Admins can opt to set up additional security settings that can lock the user out of the system if an incorrect password is entered repeatedly within a specific time frame. In the setting example, 120 minutes would lock the Admin out of their account for 2 hours, if three failed attempts to log in occur during a five minute period.

---

Revision #2

Created 15 May 2024 08:17:33

Updated 11 September 2024 13:40:49