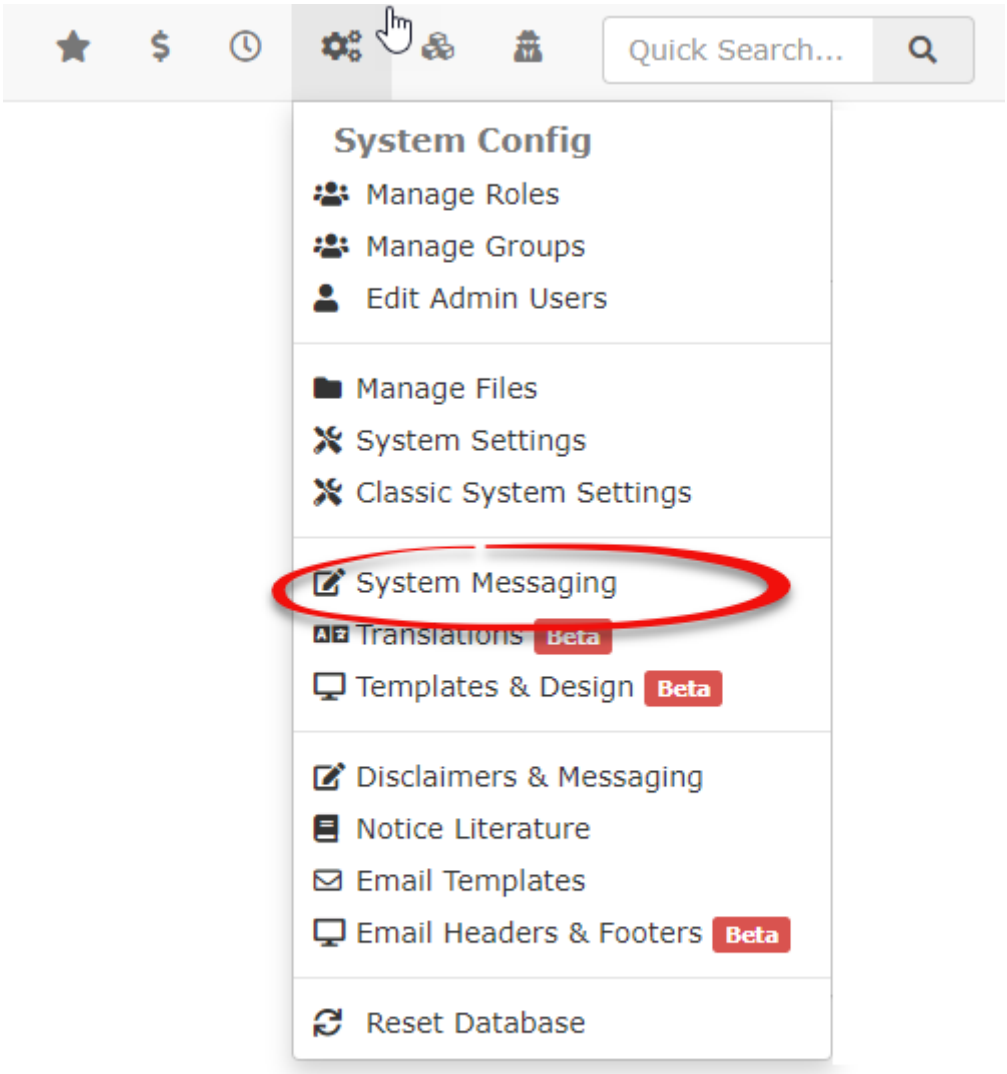
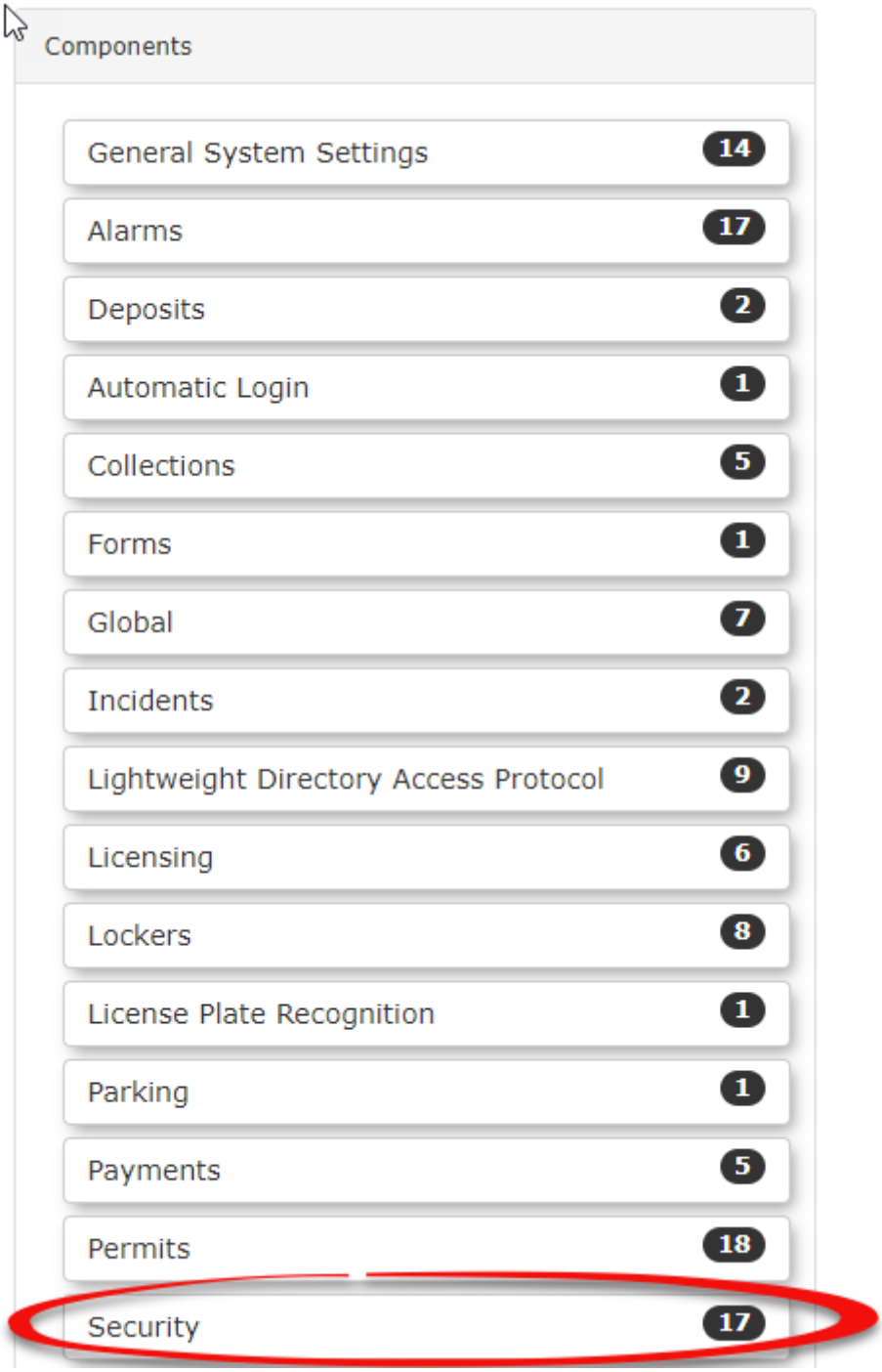
Password and Security Features

Manage Security Settings

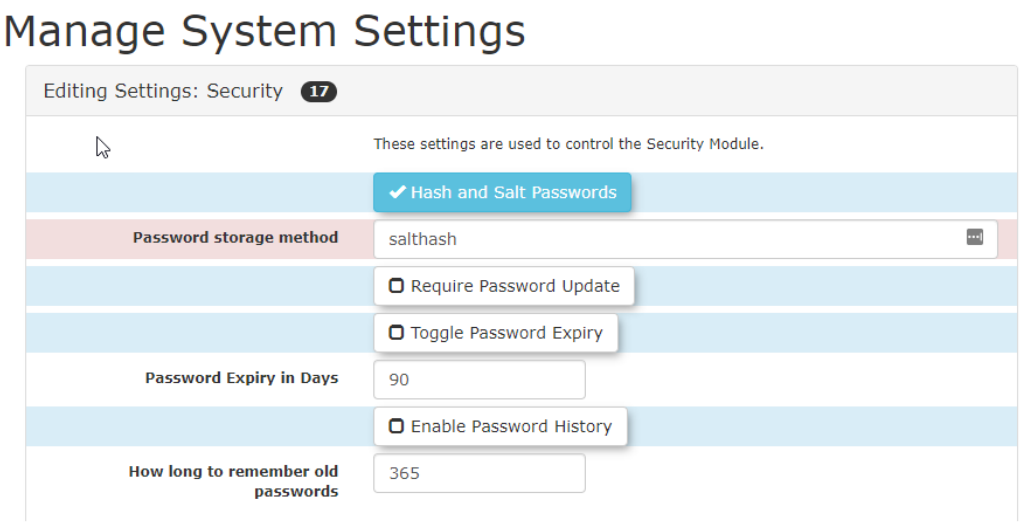
To edit security settings, hover over **System Config** and click **System Settings**.



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



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



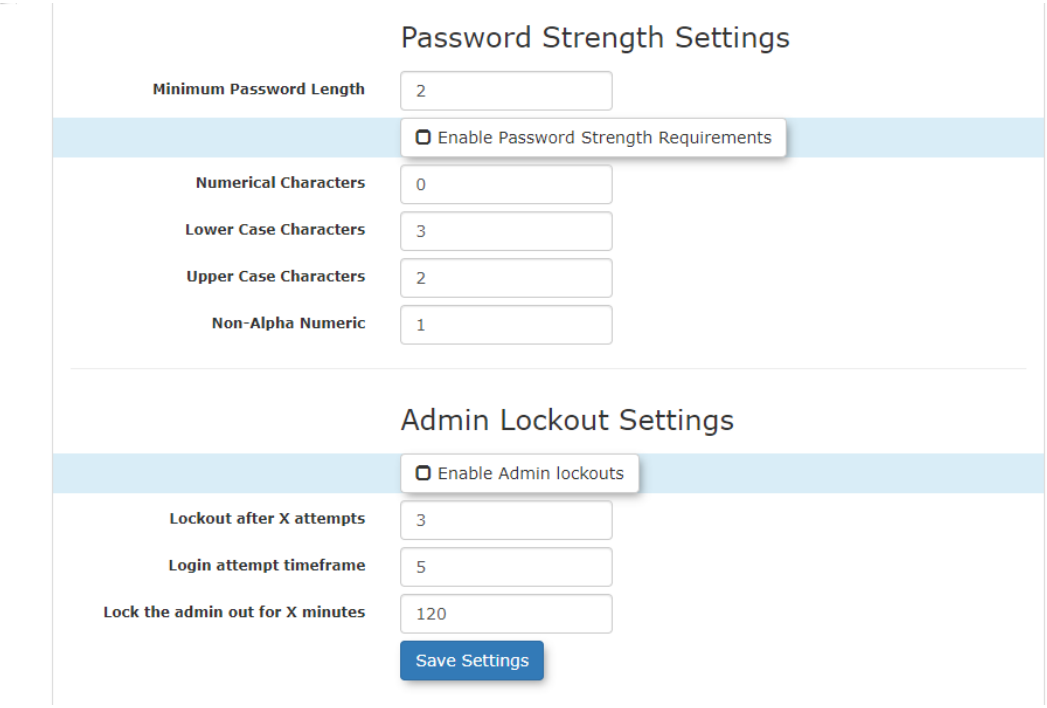
Salted Password Hashing, Password Update, Toggle Password Expiry and Enable Password History

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.



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