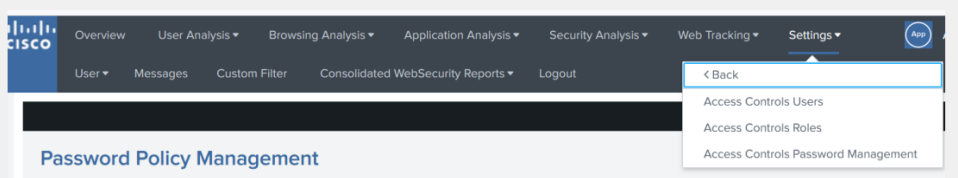
Password Policy Management

This chapter describes the password related settings that you can perform in the Cisco Advanced Web Security Reporting application web GUI. You need administrator privileges to perform these tasks. Go to the Password Policy Management page by navigating to **Settings** > **USERS AND AUTHENTICATION** > **Access Controls Password Policy Management**.



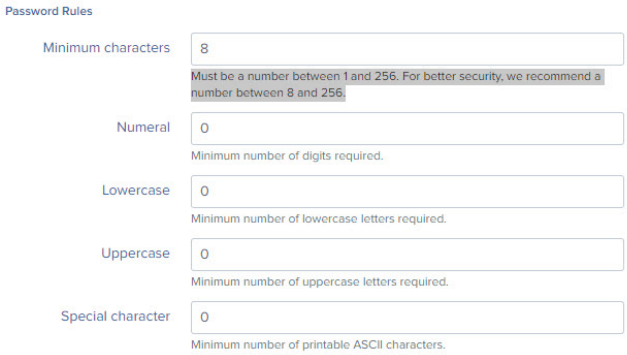
Password Rules

The password should be a combination of numbers, lowercase, uppercase, and alphanumeric characters. You can configure the following fields for setting the password:

- Minimum Characters: To set the minimum number of characters used in the password.

Note This must be a number between 1 and 256. Cisco recommends that you use a number above 8.

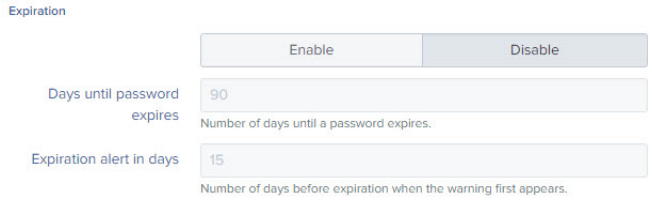
- Numerals: To set the minimum number of numeric characters in the password.
- Lowercase: To set the minimum number of lower case characters in the password.
- Uppercase: To set the minimum number of uppercase characters.
- Special character: To set the minimum number of special characters or alphanumeric characters.



Password Expiration

You can enable or disable the time period for Password expiration. The following fields can be configured:

- Date until password expires: To set the number of days until a password expires.
- Expiration alert in days: To set number of days before expiration when an alert for the user appears.



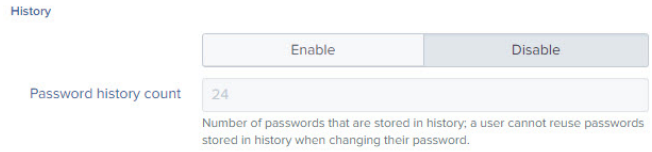
An example for an alert is shown below:

Password History

You can enable or disable the Password History option.

- Password History Count: Number of passwords that are stored in history.

Note A user cannot reuse the passwords stored in history when changing their password.

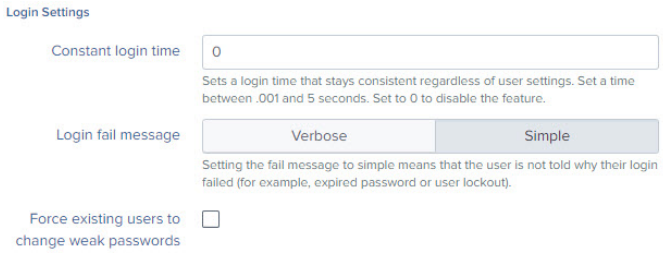


Login Settings

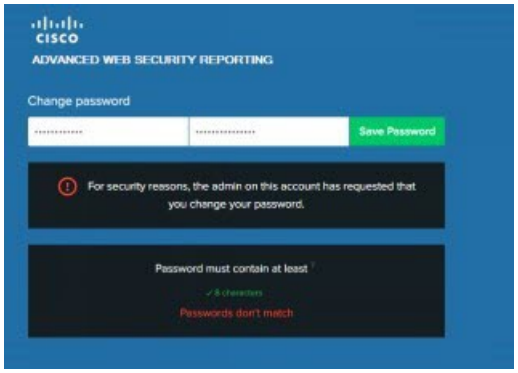
- Constant Login Time: To set a login time that stays consistent regardless of user settings.

Note Set to 0 to disable the feature.

- Login fail message: To set a fail message to the user. If you choose ‘Simple’, then the user is not informed why the login failed (for example, expired password or user lockout etc.).



If there is an error while changing the password, reasons for the error is displayed. Some examples are shown below.



Password Lockout

This feature limits the credential tries per source per unit time to prevent brute force login attacks.

You can configure the following fields:

- Failed login attempts: Number of unsuccessful login attempts that can occur before a user is locked out.
- Lockout threshold in minutes: Time required after the first unsuccessful login for the counter to reset.
- Lockout duration in minutes: Time period of the lockout duration after which a user can try to login again.

After the unsuccessful login attempts, the user account will be locked for a lockout duration specified by Administrator.