Administrator Account Settings

https://campus.barracuda.com/doc/78152330/

On the **ADVANCED > Admin Access Control** page in the Administrator Account Settings section, you can configure a password security policy to ensure that administrators/users create secure passwords, and a policy to lock administrator accounts after a specified number of failed login attempts.

Password Policy Settings

In the **Password Policy Settings** section, you can configure the following settings to specify the characters that users must include in their passwords and how often users must change their passwords. This policy is applicable to all user accounts.

- **Policy** - Select **Custom (Recommended)** to define the password policy for the administrators. If the value is set to **Default**, the enforced password history is put back to the default value for all of the users. However, when a new password is set, the new password is validated with the last password only.
- **Minimum Characters** - The minimum number of characters that a password must contain. You can enter a minimum of 8 to 50 characters.
- **Contains** - Password requirements.
- **Expires In** - The password duration. If you want to set a custom duration, select **Other**. After the password expires, users can still log into the Barracuda Web Application Firewall, but they will not be able to access any page until the password is reset.
- **Notify Before Expiry** - The number of weeks before the password expiry when users start receiving daily reminders to change their password. Until users change their password, they are emailed every day around 11:00 am (current local time of the appliance).
- **Enforce History** - determines the number of unique new passwords that must be remembered before an old password can be reused. The number must be between 1 and 12. The default number is 1 and can be changed by selecting the **Custom** policy option.

As a best practice, use a unique account for this integration point and grant it the least level of privileges required, coordinating with the administrator. For additional information, see Security for Integrating with Other Systems - Best Practices .

Account Lockout Settings

In the **Account Lockout Settings** section, you can configure a policy that specifies the maximum number of failed login attempts that users can make and the duration that accounts are locked after this limit is reached. This policy prevents brute-force attacks on user credentials. Users can retry

logging into the system after the specified lockout time. You can also unlock the account early by clicking **Clear Lockout** next to the user in the **Administrator Accounts** section.

- **Maximum Failed Login Attempts** - The maximum number of failed login attempts that are allowed for the user during the specified time threshold.
- **Failed Login Time Threshold (in minutes)** - The number of minutes during which consecutive failed login attempts are counted.
- **Lock User Account for (in minutes)** - The number of minutes the user account remains locked after the lockout policy is violated.