Step 4 - How to Configure Administrator Settings

https://campus.barracuda.com/doc/53676057/

Set and Restrict Administration Interface Access

Use the **BASIC > Administration** page to perform the following tasks related to Barracuda Message Archiver web access:

- Change the password of the administration account **admin** *(highly recommended for your security and protection).*
- Specify the **Administrator IP/Range** addresses/networks that can access the administrative web interface for the Barracuda Load Balancer ADC *(highly recommended for your security and protection).*
- Change the port used to access the Barracuda Load Balancer ADC over the web (default port is 8000).
- Change the length of time after which idle users are to be logged out of the web interface (the default value is 20 minutes).

Configure the Password Policy

On the **ADVANCED > Admin Access Control** page under **Administrator Account Settings**, click **Password Policy Settings** to configure the following:

- **Policy** - You can select either **Default** or **Custom**. Select **Custom** to modify the password policy.
- **Minimum Characters** - Specify the minimum number of characters needed for the password (the default value is 8).
- **Contains** - Specify the types of characters that must be present in each password:
    - **At Least One Upper Case Character**
    - **At Least One Lower Case Character**
    - **At Least One Special Character**
    - **At Least One Digit**
- **Expires In** - Time until password expires:
    - **3 Months**
    - **6 Months**
    - **1 Year**
    - **Never**
    - **Other** - Specify between 30 and 999 days.
- **Notify Before Expiry** - Time before notifying the user that his or her password is about to expire.

- **1 Week**
- **2 Weeks**

Configure the Account Lockout Settings

To prevent unauthorized access to the Barracuda Load Balancer ADC, go to the **ADVANCED > Admin Access Control** page and under **Administrator Account Settings** click **Account Lockout Settings**. Use these settings to specify when a user will be locked out from the Barracuda Load Balancer ADC based on the number of times they have failed to enter their login credentials correctly.

- **Maximum Failed Login Attempts** - Specify the acceptable number of failed login attempts (default is 5).
- **Failed Login Time Threshold** - Specify the time in minutes in which consecutive failed login attempts are counted (default is 15).
- **Lock User Account** - Specify the time in minutes to lock the admin account if the user fails to login more than the **Maximum Failed Login Attempts** value in less that the time specified by the **Failed Login Time Threshold** (default is 15).

If an account is locked after the maximum failed login attempt limit has been reached, an **Admin** user can clear the account lock in the **Administrator Accounts** section by clicking **Clear Lockout** next to the user.