Step 1: Configure Administrative Settings

https://campus.barracuda.com/doc/5799965/

The **BASIC > Administration** page allows you to configure the following access restrictions to the web interface:

- Allow or deny administration access through the WAN interfaces. Denying access from the WAN interfaces is one way to prevent brute force log in attacks. (You cannot disable administration access via the LAN.)
- Specify the IP addresses or subnet masks of systems allowed to access the web interface. Attempts to log in from other IP addresses will be denied.
- Change the HTTP port used to access the web interface (default is port 8000).
- Change the maximum idle time allowed before an administrator is logged out of the web interface.

Change the Default Password

To prevent unauthorized use, change the default administrator password for the web interface to a secure password.

1. Log into the Barracuda Link Balancer interface.
2. Navigate to the **BASIC > Administration** page.
3. In the **Password Change** section, change the default administrator password.
4. Click **Save Password**.

For additional information, see Security for Integrating with Other Systems - Best Practices.

Set the Time Zone of the System

The current time on the system is automatically updated via Network Time Protocol (NTP). The time zone must be set correctly to coordinate traffic distribution and to record correctly in all logs and reports. If two or more Barracuda Link Balancers are clustered, the time zone must be the same for both before the cluster can be created.

1. Open the **BASIC > Administration** page.
2. In the **Time** section, set the time zone of your Barracuda Link Balancer.
3. Click **Save Changes**.

The Barracuda Link Balancer automatically reboots when you change the timezone.

Specify Email Addresses for Alerts

Alert emails are generated automatically by the Barracuda Link Balancer to notify you of system warnings, for example, when a link is down or your system is low on disk space. Generated alert emails are sent hourly. Every SNMP trap (except for the WANx saturated trap) results in an alert email. To specify email addresses for alerts:

1. Navigate to the **BASIC > Administration** page.
2. In the **Email Notifications** section, enter the email address that sends alerts from the Barracuda Link Balancer. To enter multiple addresses, separate each address with a comma. As a best practice, use a unique account for this integration point and grant it the least level of privileges required, coordinating with your email administrator. For additional information, see Security for Integrating with Other Systems - Best Practices.
3. Click **Save Changes**.
4. Open the **BASIC > IP Configuration** page.
5. Enter the **Default Host Name** and **Default Domain** of the Barracuda Link Balancer.
6. Click **Save Changes**.

The default host name and the default domain name are in all alert emails sent by the Barracuda Link Balancer.

Customize the Appearance of the Web Interface

Use the **ADVANCED > Appearance** page to customize the default images used on the web interface. This tab is only displayed on certain Barracuda Link Balancer models.

Enabling SSL for Administration

You can require that only secure SSL connections can access the web interface. SSL ensures that your passwords and transmitted and received data are encrypted.

Configure SSL on the **ADVANCED > Secure Administration** page. To allow only secure connections when accessing the web interface, you must supply a digital SSL certificate which is stored on the Barracuda Link Balancer. This certificate bcomes part of the connection process between client and server (in this case, a browser and the web interface on the Barracuda Link Balancer). The certificate contains the server name, the trusted certificate authority, and the server's public encryption key.

The supplied SSL certificate may be either private or trusted. A private, or self-signed, certificate

provides strong encryption without the cost of purchasing a certificate from a trusted certificate authority (CA). However, the client (browser), unable to verify the authenticity of a self-signed certificate, will send a warning indicating an unverified certificate. To avoid this warning, download the private root certificate and import it into each browser that accesses the Barracuda Link Balancer web interface. You may create your own private certificate using the **ADVANCED > Secure Administration** page.

Instead of a private certificate, you may use the default pre-loaded Barracuda Networks certificate. A client web browser warning will result because the certificate hostname is *"barracuda.barracudanetworks.com"* , which is not a trusted certificate. Thus, access to the web interface using the default certificate may be less secure.

A trusted certificate is a certificate signed by a trusted certificate authority (CA). The benefit of using a trusted certificate is that the browser recognizes it as trusted, so you need not manually download the private root certificate. Use the **ADVANCED > Secure Administration** page to create a **Certificate Signing Request** which you can submit to a certificate authority to purchase a trusted certificate.