Step 4 - How to Configure Administrative Settings

https://campus.barracuda.com/doc/2490427/

This article refers to the Barracuda Message Archiver release 5.0 or higher.

Before configuring administrative settings, complete Step 3 - How to Configure the Web Interface.

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 Message Archiver *(highly recommended for your security and protection)*
- Change the port used to access the Barracuda Message Archiver 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)
- Specify the IP addresses or netmask of the systems that can communicate with the Barracuda Message Archiver via SNMP (available on Barracuda Message Archiver model 450 and higher)

Set the System Time Zone

Set the time zone of your Barracuda Message Archiver from the **Basic > Administration** page. The current time on the system is automatically updated via Network Time Protocol (NTP). When the Barracuda Message Archiver resides behind a firewall, NTP requires port 123 to be opened for outbound UDP traffic.

- It is important that the time zone is set correctly as this information is used in all logs and reports
- The Barracuda Message Archiver automatically reboots when you change the time zone

Customize the Web Interface Appearance

The **Advanced > Appearance** page allows you to customize the default images used on the web interface. This tab is available only on the Barracuda Message Archiver 650 and above.

Enable SSL for Administrators and Users

Use the **Advanced > Secure Administration** page to modify various settings related to SSL (https) access to the Barracuda Message Archiver web interface.

SSL not only ensures that your passwords are encrypted, but also ensures that all data transmitted to, and received from, the administration interface is encrypted. The Barracuda Message Archiver supports SSL access without any additional configuration. However, some sites may enforce the use of a secured connection to access the web interface, or prefer to use their own trusted certificates.

The SSL configuration referred to here is related only to the web-based administrative interface; it is unnecessary to explicitly configure SSL for traffic between the Barracuda Message Archiver and your email servers.

To enforce SSL-only access:

1. Go to the **Advanced > Secure Administration** page, and set the following options:
   - **HTTPS/SSL Access Only** – Specify whether users are required to use HTTPS to access the web interface
   - **Use HTTPS links in Emails** – Specify whether notices and emails from the Barracuda Message Archiver use HTTP or HTTPS links
   - **Web Interface HTTPS/SSL** – Enter the appropriate port number; the default value is 443
2. Click **Save** to save and activate your settings.

To change the certificate that is used, you must first create and upload the new certificate before changing the **Certificate Type** in the **SSL Certificate Configuration** section. The Barracuda Message Archiver supports the following certificate types:

- **Default (Barracuda Networks)** certificates are signed by Barracuda Networks. On some browsers, these may generate some benign warnings which can be safely ignored. No additional configuration is required to use these certificates which are provided free of charge as the default certificate type.

  During a configuration backup, the certificate type is reset to **Default** if the original certificate cannot be located. Go to the **Advanced > Secure Administration** page, and in the **SSL Certificate Configuration** section, reselect the certificate from the **Certificate Type** drop-down menu to reactivate your certificate once the restore is complete.

- **Private (Self-signed)** certificates provide strong encryption without the cost of purchasing a certificate from a trusted Certificate Authority (CA). These certificates are created by providing the information requested in the **Certificate Generation** section of the **Advanced > Secure Administration** page. Additionally, you can download the Private Root Certificate and import it into your browser to allow verification of certificate authenticity and to prevent warnings from displaying when accessing the web interface.
- **Trusted (Signed by a trusted CA)** certificates are issued by trusted CAs, and must be purchased separately with a Certificate Signing Request (CSR). This can be downloaded after providing the information requested in the **Certificate Generation** section of the **Advanced > Secure Administration** page. Once you receive the third-party certificate from the CA, you must upload it to the Barracuda Message Archiver from the **Trusted Certificate** section of that same page. The certificate is in effect once the upload is completed.

Archived Data Backup

Once you are storing data, you need to back up the Barracuda Message Archiver data. You can back up your raw email data as well as data directories that house statistics, index, and other metadata snapshots the Barracuda Message Archiver generates about your content. For details, refer to How to Back Up Archives.

Continue with Step 5 - Understanding Message Archiving Concepts.