Step 4 - Configure and Secure the Web Interface

https://campus.barracuda.com/doc/6160428/

Controlling Access to the Web Interface

Use the **BASIC > Administration** page to perform the following tasks for initial setup:

1. For maximum security, Barracuda strongly recommends assigning a new administration password to the Barracuda Web Security Gateway.
2. Make sure the local time zone is set correctly. Time on the Barracuda Web Security Gateway is automatically updated via NTP (Network Time Protocol). It requires that port 123 is opened for inbound and outbound UDP (User Datagram Protocol) traffic on your firewall (if the Barracuda Web Security Gateway is located behind one).
   It is important that the time zone is set correctly because this information is used to determine the delivery times for messages and is displayed in certain mail reading programs. The current time is also used to deliver accurate cache updates if caching is enabled (see the **ADVANCED > Caching** page).
3. If desired, change the port number used to access the Barracuda Web Security Gateway Web interface. The default port is 8000.
4. Enter the amount of time for the **Session Expiration Length** (in minutes) of your Web interface session. If the session expires, you are required to log back into the web interface.
5. Specify your local SMTP server information. Enter the email address for your Administrator to receive system and threat email alerts and notifications.
6. Click **Save Changes**.

Customizing the Appearance of the Web interface

The **ADVANCED > Appearance** page allows you to customize the default images used on the web interface. You can also give the Barracuda Web Security Gateway a name (e.g. “Science Library Web Security Gateway”) that will appear in the login page above the login panel that contains the Language selector and the Username and Password prompts. The **ADVANCED > Appearance** page is only displayed on the Barracuda Web Security Gateway 410 and above.

Changing the Language of the Web Interface

You can change the language of the web interface by selecting a language from the drop-down menu in the upper right corner of the page near the **Log Off** link and the breadcrumbs. Supported languages include Chinese, Japanese, Spanish, French, and others. The language you select is only applied to your individual web interface. No other user’s web interface is affected.

Enabling SSL for Administrators and Users

SSL (Secure Socket Layer) ensures that your passwords are encrypted and that all data transmitted to and received from the web interface is encrypted as well. All Barracuda Web Security Gateways support SSL access without any additional configuration, and Barracuda strongly recommends enabling HTTPS/SSL access only, as instructed below.

To enforce SSL-only access:

1. On the **ADVANCED > Secure Administration** page, select *Yes* to enable **HTTPS/SSL Access Only** to the web interface. Setting this to *No* will still allow the Barracuda Web Security Gateway to accept non-SSL connections.
2. Enter your desired **Web Interface HTTPS/SSL port** for the web interface. The default is 443.
3. Click **Save**.

If you wish to change the certificate that is used, you can either create a self-signed certificate or upload a certificate you purchase from a trusted Certificate Authority (CA) to the Barracuda Web Security Gateway. Changing the **Certificate Type** in the **SSL Certificate Configuration** section of the **ADVANCED > Secure Administration** page allows you to either create a self-signed certificate with your organization information, or create a Certificate Signing Request (CSR) to purchase a trusted certificate. Click the **Help** button on the **ADVANCED > Secure Administration** page for instructions to create and/or upload a certificate. The Barracuda Web Security Gateway supports the following types of certificates:

- **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 type of certificate.
- **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 **Private (self-signed)** section of the page. You may also want to download the Private Root Certificate and import it into your browser, to allow it to verify the authenticity of the certificate and prevent any warnings that may come up when accessing the web interface.
- **Trusted (signed by a trusted CA)** certificates are issued by trusted Certificate Authorities (CA), and must be purchased from them separately with a Certificate Signing Request (CSR). The CSR can be downloaded from the Barracuda Web Security Gateway after providing the information requested in the **Trusted (Signed by a trusted CA)** section of the page. Once you have received the certificate and key from the CA, you must upload both items to the Barracuda Web Security Gateway from this section of the page. The certificate will be in effect as soon as the upload is complete.

Continue with Step 5 - Connect the Barracuda Web Security Gateway to Your Network.