How to Enable SSL for Administrators and Users

https://campus.barracuda.com/doc/3866671/

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 Email Security Gateways support SSL access without any additional configuration, and Barracuda Networks strongly recommends securing external access to the web interface as described below. Additionally, some sites may wish to enforce using a secured connection to access the web interface, or prefer to use their own trusted certificates. For more information about and best practices for securing your Barracuda Email Security Gateway on your network, see Securing the Barracuda Email Security Gateway.

The SSL configuration referred to here is related only to the web interface. There is no need to explicitly configure SSL for traffic between the Barracuda Email Security Gateway and your mail servers.

How to Enforce SSL-only Access (recommended)

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 Email Security Gateway to accept non-SSL connections.
2. Select *Yes* to **Use HTTPS Links in Emails** for per-user quarantine messages sent from the Barracuda Email Security Gateway.
3. Enter your desired **Web Interface HTTPS/SSL Port** for the web interface. The default is 443.
4. Select **Supported SSL Protocols** you want the Barracuda Email Security Gateway to support: *TLSv1, TLSv1.1, TLSv1.2, TLSv1.3*
5. Click **Save**.

If you wish to change the certificate that is used, you must first create and upload it to the Barracuda Email Security Gateway before changing the **Certificate Type** in the **SSL Certificate Configuration** section of the **ADVANCED > Secure Administration** page. See the online help for instructions. The Barracuda Email 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, and 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)** - A certificate signed by and purchased from a trusted CA. Web browsers are able to recognize and verify these certificates as coming from a trusted source, so in most circumstances there is no need for a Private Root Certificate to be downloaded for every Web browser. The following types of Trusted Certificates are supported:
  - Obtained from a Third-Party CA
  - Microsoft Certificate Services
  - Wildcard Certificates

To upload a trusted certificate (Barracuda Email Security Gateway version 8 and above):

1. Go to the **ADVANCED > Secure Administration** page.
2. In the **SSL Certificate Configuration** section. select *Trusted* for the **Certificate Type**.
3. In the **Trusted (Signed by a trusted CA)** section, lick **Edit Data**.
4. Fill in and save the **CSR Generation** data.
5. Click **Download CSR**.
6. Click **Download Key** (this is the private key).
7. Send the CSR to the Certificate Authority you want to use.
8. From the CA (Certificate Authority), get the Apache version of the certificate. This is the certificate and the chain, or intermediate certificates.
9. On the **ADVANCED > Secure Administration** page, click **Upload** to upload the KEY (private key) you downloaded above.
10. Upload the Certificates received from the CA.