

How to Enable SSL for Administrators and Users

<https://campus.barracuda.com/doc/73699799/>

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. The Barracuda Web Security Gateway supports SSL access without any additional configuration. However, 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 Web Security Gateway on your network, see [Securing the Barracuda Web Security Gateway](#).

The SSL configuration referred to here is related only to the web interface.

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 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. Select **Supported SSL Protocols** to be enabled for web interface.
4. Click **Save**.

If you wish to change the certificate that is used, you must first create and upload it to the Barracuda Web Security Gateway before changing the **Certificate Type** in the **SSL Certificate Configuration** section of the **ADVANCED > Secure Administration** page. Click **Help** for instructions. 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, 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.

© Barracuda Networks Inc., 2022 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.