Creating a Custom SSL Certificate

https://campus.barracuda.com/doc/97517674/

An SSL certificate is a digital identity document that enables both server and client to authenticate each other. Certificates are used with HTTPS protocol to encrypt secure information transmitted over the internet. This not only ensures that your passwords are encrypted, but also ensures that all data transmitted to, and received from, the administration interface is encrypted. There are three types of SSL certificates to choose from:

- Default (Barracuda Networks);
- Trusted certificate - a certificate signed by a trusted certificate authority (CA);
- Private (self-signed).

Create and Upload SSL Certificate

On the **System > Device Information** page in the Barracuda Backup local user interface, use the **SSL Certificate** section to create and upload a new SSL certificate. The Barracuda Backup supports the following certificate types:

- **Download latest certificate** – Default (Barracuda Networks) certificates are signed by Barracuda Networks.
- **Upload trusted certificate** or **Upload trusted key** – Upload a self-signed certificate issued by your company or a trusted certificate issued by a Certificate Authority (CA). Once the certificate is created, you must upload it to Barracuda Backup. The certificate is in effect once the upload is completed.
- **Generate custom certificate** – Generate a custom self-signed certificate. These certificates are created by providing the information requested in this section. Note that the **Common Name** is the domain secured by the certificate. Fill in the available fields and click **Generate**. The message *A new certificate has been generated and applied.* is displayed.

Generate Self-Signed Certificate Using OpenSSL

In addition to generating a self-signed certificate from your company or Barracuda Backup, you can also use OpenSSL to generate a self-signed certificate. To create a self-signed certificate using OpenSSL:

1. Ensure you have OpenSSL installed and configured in your environment.
2. Create a key and certificate using the following command:

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days
365
```

You can now accept and trust the new certificate in your browser. Note that a warning might display because this is a self-signed certificate and there is no CA. You can safely ignore the warning and proceed. To avoid this issue, Barracuda Networks recommends using a trusted certificate issued by a trusted CA.

Install the Securly SSL Certificate

Installing the Securly SSL certificate ensures that Securly is able to filter all HTTPS sites without the end user receiving an SSL Error. This certificate adds an additional safety and privacy by acting as a secure gateway between any device and the internet. The certificate does not control the level of filtering or what sites are allowed.

For instructions and more information on how to install the Securly SSL certificate on different operating systems and browsers, see https://support.securly.com/hc/en-us/articles/360033872694-Instructions-for-installing-the-Securly-SSL-certificate-manually-and-distributed.