How to Create and Install a Self-Signed Certificate for SSL Inspection

https://campus.barracuda.com/doc/38240386/

Note that the Firefox browser does not store certificates, nor does it use the default store in Windows the way Chrome and Internet Explorer do. Additionally, Firefox uses its own separate proxy configuration settings. Barracuda Networks recommends enforcing a supported browser policy, in addition to enforcing browser control at the firewall using Barracuda NG firewalls.

- **Barracuda Web Security Gateway 310 running 14.x or below** – Download the Barracuda Networks default root certificate from the **BLOCK/ACCEPT > Configuration** page. See How to Configure SSL Inspection for details.
- **Barracuda Web Security Gateway 410 and above running version 15.x and higher** – Either download the Barracuda Networks default root certificate or create and download your own self-signed certificate from the Barracuda Web Security Gateway and install it in client browsers, as described in this article. Barracuda Networks recommends creating a self-signed certificate.

To install a self-signed certificate on the Barracuda Web Security Gateway 310, *specifically for use with the SSL Inspection feature:*

1. Go to the **BLOCK/ACCEPT > Configuration** page and, in the **SSL Inspection** section, click **Generate Certificate**
   and follow the instructions.
2. Install the certificate file in all client browsers. If you want to enable users to install the certificate in their browsers, you can email the certificate, post it on an internal network share or post it on a public or private web server. SSL Inspection will then be applied when accessing **YouTube for Schools** and when using any Safe Search selections you make on the **BLOCK/ACCEPT > Content Filters** page.

To create and install a self-signed certificate on the Barracuda Web Security Gateway 410 and higher, *specifically for use with the SSL Inspection feature:*

1. Go to the **ADVANCED > SSL Inspection** page and, in the **Certificate Creation** section, click **Create Certificate.**
2. In the **Certificate Generation** section of the page, fill in the **Organization Info** fields, and then click **Create Certificate**. Your certificate appears in the **Available Certificates** section of the page.
3. Now you have two options:
    - Either push or manually install the certificate on client browsers. Next to **Root Certificate For Browsers**, click **Download** to obtain the certificate file, and then install the certificate on each client browser.
    - Enable users to download and install the certificate in their browsers. Do this by setting

Enable Browser Certificate Download to **Yes**. Click the **Save Changes** at the top of the page. Next, send users an email message, paste in the URL displayed next to **Enable Browser Certificate Download** on the page, and include instructions to upload the certificate from this URL to their browsers. Or you can embed the URL in the block page by customizing the content on the **BLOCK/ACCEPT > Block Messages** page. Typically the client browser provides a wizard to guide the install of the certificate. If you choose this option, you can also require users to authenticate via LDAP before downloading the certificate.

Configure other SSL Inspection settings as needed on the **ADVANCED > SSL Inspection** page.

For High Availability Systems (Linked Management/Clustering)

If you have a high availability (Linked Management) deployment, you must install a certificate on each Barracuda Web Security Gateway in the cluster. You must also install a browser certificate in all client browsers. In this example, there are three Barracuda Web Security Gateways in the cluster: B1, B2, and B3.

1. Go to the **ADVANCED > SSL Inspection** page of the Barracuda Web Security Gateway B1 and follow the instructions above to create a self-signed certificate.
2. Next to **Root Certificate For Web Security Gateway**, click **Download** and store the file on your system.
3. Now you have two options:
    1. Either push or install the certificate on client browsers. Next to **Root Certificate For Browsers**, click **Download** to obtain the certificate file, and then install the certificate on each client browser.
    2. Enable users to download and install the certificate in their browsers. Do this by setting **Enable Browser Certificate Download** to **Yes**. Click **Save Changes** at the top of the page. Next, send users an email message, paste in the URL displayed next to **Enable Browser Certificate Download** on the page, and include instructions on how to upload the certificate from this URL to their browsers. Typically the browser provides a wizard to guide the install of the certificate. If you choose this option, you can also require users to authenticate via LDAP before downloading the certificate.
4. On Barracuda Web Security Gateways B2 and B3:
    1. In the **Certificate Creation** section of the page, select **Upload Certificate** for the **Certificate Creation Method**.
    2. In the **Certificate Generation** section, click **Browse** next to **Certificate Authority.** Find the root certificate file for the Barracuda Web Security Gateway that you downloaded from B1 in step 2.
    3. Click **Upload Certificate** to install the root certificate on the Barracuda Web Security Gateway B2 and B3.

Configure other SSL Inspection settings as needed on the **ADVANCED > SSL Inspection** page of each Barracuda Web Security Gateway in the cluster.