How to Use the Barracuda Networks Default Certificate for SSL Inspection

https://campus.barracuda.com/doc/39815583/

IMPORTANT

Due to recent vulnerabilities discovered with the SSL protocol, Barracuda Networks strongly recommends that you upgrade to 8.1.0.005 before using this feature. See the Barracuda Networks Security Updates blog post around this topic: Barracuda Networks Delivers Updated SSL Inspection Feature.

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.

When you enable SSL Inspection on the Barracuda Web Security Gateway, a default SSL certificate is provided which you can download from the Barracuda Web Security Gateway and install on client browsers. Note that, with the Barracuda Web Security Gateway 610 and higher, you can alternatively Create and Install a Self-Signed Certificate for SSL Inspection with your organization information from the **ADVANCED > SSL Inspection** page.

Follow these steps to use the Barracuda Networks default certificate on the Barracuda Web Security Gateway *specifically for use with the SSL Inspection feature.*

See also:

- How to Configure SSL Inspection Version 12
- How to Configure SSL Inspection Version 8.1 to 9.1
- Create and Install a Self-Signed Certificate for SSL Inspection
- Using SSL Inspection

Barracuda Web Security Gateway 410 and higher running version 7.1 and higher:

1. Download the Barracuda Networks default root certificate from the **BLOCK/ACCEPT > Configuration** page.
2. Either manually install the certificate on client browsers, or push to browsers using a Windows GPO.
3. Enable SSL Inspection on the **BLOCK/ACCEPT > Configuration** page.

Barracuda Web Security Gateway 610 and higher:

1. Go to the **ADVANCED > SSL Inspection** page.

2. You have two options for getting and distributing the default Root Certificate from the Barracuda Web Security Gateway to client browsers. In the **Available Certificates** section of the page, do one of the following:
    1. 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, either manually or with a GPO.
    2. Enable users to download and install the certificate in their browsers.
        1. Set **Enable Browser Certificate Download** to **Yes**. Click **Save Changes** at the top of the page.
        2. 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.
3. Configure other SSL Inspection settings as needed on the **ADVANCED > SSL Inspection** page.

With version 7.0.1 and higher, you cannot remove the Barracuda Networks root Certificate. You can, however, overwrite it with a self-signed certificate.

For High Availability System (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.

Example: You might have 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 enable SSL Inspection.
2. Follow instructions above to download the Barracuda Web Security Gateway root certificate.
3. Next to **Root Certificate For Web Security Gateway**, click **Download** and store the file on your system.
4. 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 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 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.

5. 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 of the **ADVANCED > SSL Inspection** page, 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 Gateways B2 and B3.

Configure other SSL Inspection settings as needed on the **ADVANCED > SSL Inspection** page of Barracuda Web Security Gateway B1 - aside from the SSL certificates, SSL Inspection settings will propagate to the other systems in the cluster.