

How to Upload a Renewed SSL Certificate

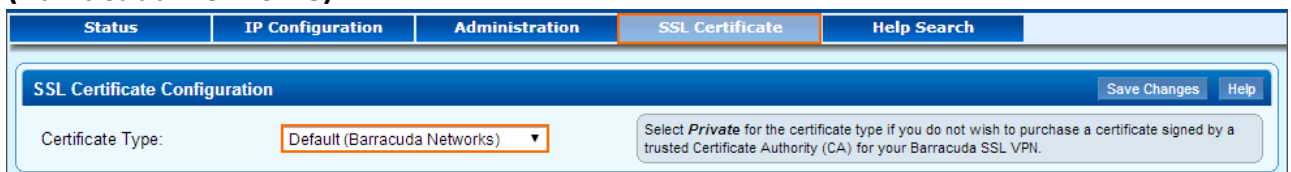
<https://campus.barracuda.com/doc/41106330/>

If the existing trusted SSL certificate needs to be replaced, and a trusted certificate is already in use, you must first change the certificate configuration to use the default certificate from Barracuda Networks before you can upload and install the new trusted SSL certificate. After the certificate has been uploaded and installed you must synchronize the trusted SSL certificate between the two interfaces, so it is used for the SSL VPN web interface as well as the Appliance web interface.

Replacing a trusted SSL certificate

Step 1. Change the certificate type to default

1. Log into the [Appliance web interface](#).
2. Open the **Basic > SSL Certificate** page.
3. In the **SSL Certificate Configuration** section, set the **Certificate Type** to **Default (Barracuda Networks)**.



Status	IP Configuration	Administration	SSL Certificate	Help Search
SSL Certificate Configuration				
Certificate Type: Default (Barracuda Networks)				
Select <i>Private</i> for the certificate type if you do not wish to purchase a certificate signed by a trusted Certificate Authority (CA) for your Barracuda SSL VPN.				

4. Click **Save Changes**.
5. If you are using a self-signed SSL certificate, add a security exception for the the new (default) SSL certificate.

The **UPDATING** window is displayed until you can log back into the Appliance web interface.



UPDATING ... Please Wait



Step 2. Upload the new trusted SSL certificate

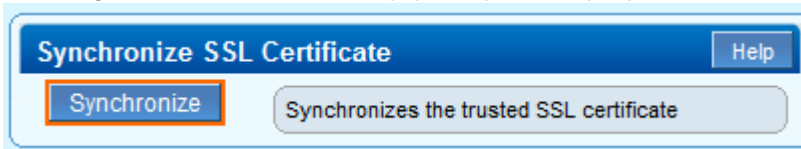
1. Log into the [Appliance web interface](#).
2. Open the **Basic > SSL Certificate** page.
3. Set the **Certificate Type** drop down box to *Trusted (Signed by a Trusted CA)*.
4. Upload the new certificate components in the **Trusted** section.

5. Next to the uploaded certificate, click **Use**.
6. If you are using a self-signed SSL certificate, add a security exception for the the new (trusted) SSL certificate for your browser.

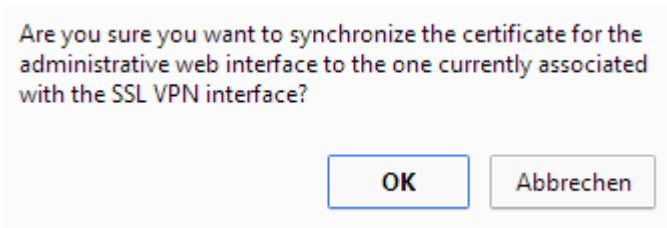
Step 3. Synchronize the new trusted SSL certificate

Certificate synchronization requires TLSv1.0 to be enabled on port 443. If your status graphs on the **Basic > Status** page on port 8000/8443 are not working, then you must enable TLSv1.0 on port 443 under **Advanced > Configuration**.

1. Log into the [Appliance web interface](#).
2. Open the **Basic > SSL Certificate** page.
3. Click **Clear All Unused Files**.
4. Click **Synchronize**. A security prompt is displayed.



5. Click **OK**.



The new SSL certificate is now used for both the Appliance and SSL VPN web interface.

Certificate Candidates	Expiry Date	Status	Use
CN=doc.org/emailAddress=support@barracuda.com	2023-12-05 00:56:00	Self-signed	In Use
CN=doc-sslvpn.doc.org	2014-12-05 01:00:00	Untrusted	Use

Figures

1. ssl_default.png
2. SSL_cert02.png
3. SSL_cert03.png
4. cert_sync.png
5. SSL_cert04.png

© Barracuda Networks Inc., 2019 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.