How to Add an SSL Certificate

https://campus.barracuda.com/doc/17105127/

> This article refers to firmware 4.1 and higher.

You can create a self-signed certificate, or upload a trusted certificate.

Uploading a Signed Certificate

> You can upload a signed certificate in either PKCS12 Token Format or PEM format.

Adding a PKCS12 Token Format Certificate

Use the following steps to upload a signed certificate obtained from a trusted Certificate Authority (CA) in PKCS12 Token Format.

1. Log into the Barracuda Load Balancer web interface, and go to the **BASIC > Certificates** page.
2. In the **Upload Certificate** section, select the **Certificate Type** as *PKCS12 Token*.
3. Set **Allow Private Key Export** to *Yes* to export the private key corresponding to the certificate.
   > Certificates are downloaded in PKCS12 format including both the private key and certificate. If **Allow Private Key Export** is set to *No*, the private key is locked and the certificate can be downloaded only in *PEM format* and the system configuration backup cannot be taken.
   > **Allow Private Key Export** is valid for *generated and imported certificates only*.
4. Enter an identifying name in the **Certificate Name** field.
5. In the **Certificate Password** field, specify a password that will be used to generate the PKCS12 token for the signed certificate to be uploaded.
6. Click **Browse** next to the **Signed Certificate** field, and select the PKCS12 format signed certificate file.
   > When uploading a signed certificate as a PKCS12 token, ensure that the file uses a **.pfx** extension; otherwise the file is treated as a PEM file.
   > When uploading a certificate in **.pfx** format, verify that any intermediary certificates are bundled in the **.pfx** file.
7. Click **Upload** to upload the certificate.

Adding a PEM Format Certificate

Use the following steps to upload a signed certificate obtained from a trusted CA in PEM Format.

1. Log into the Barracuda Load Balancer web interface, and go to the **BASIC > Certificates** page.
2. In the **Upload Certificate** section, select the **Certificate Type** as *PEM Certificate*.
3. Set **Allow Private Key Export** to *Yes* to export the private key corresponding to the certificate.

   Certificates are downloaded in PKCS12 format including both the private key and certificate. If **Allow Private Key Export** is set to *No*, the private key is locked and the certificate can be download only in *PEM format* and the system configuration backup cannot be taken.
   Allow Private Key Export is valid for *generated and imported certificates only*.

4. If the certificate signing request (CSR) for this certificate was generated on the Barracuda Load Balancer, set **Assign the associated key** to *Yes,* otherwise, select *No*, and upload the private key in the **Certificate Key** field.
5. Enter an identifying name in the **Certificate Name** field.
6. If **the Assign the associated key** field is set to *No, c*lick **Browse** next to the **Certificate Key** field to select the corresponding private key for the signed certificate.

   The key must be unencrypted and in PEM format.

7. Click **Browse** next to the **Signed Certificate** field, and select the PEM format signed certificate file.
8. Click **Browse** next to the **Intermediary Certificates** field, and select the intermediary CA certificate. To add additional intermediary CA certificates, click the plus (+) button.
9. Click **Upload** to upload the certificate.

   If your certificate is signed by a trusted CA, upload the certificate in the following order:
   1 - Leaf Certificate
   2 - Intermediate Certificates
   3 - Root CA Certificate

For additional information, go to the **BASIC > Certificates** page in the Barracuda Load Balancer web interface, and click the **Help** button.

Related Articles

- [Installing SSL Certificates with Correct Chain Order](#)