

Installing SSL Certificates with Correct Chain Order

<https://campus.barracuda.com/doc/16680112/>

A browser running on a desktop system is capable of building the certificate chain in the correct order regardless of the order in which the certificates are presented. However, a browser running on a mobile device, such as Android, may not be capable of building the certificate chain properly if the certificates are not presented in the correct order.

This article describes how to resolve this issue by uploading the certificate chain so that the certificate is "digested" in the correct order, and thus presented to the client in the correct order.

In this article:

Step 1 - Downloading the Certificate

Use the following steps to download the certificate from the Barracuda Load Balancer:

1. Log into the Barracuda Load Balancer web interface, and go to the **BASIC > Certificates** page.
2. In the **Saved Certificates** table, locate the certificate, and click **Certificate** in the **Download** column.
3. In the **Save Token** page, enter a passphrase in the **Encryption Password** field, and click **Save**.
4. The certificate is exported as a PKCS12 token which includes the private key.

If you already have the private key, ensure that it is decrypted before uploading it to the Barracuda Load Balancer.

You can obtain the private key from the device on which the Certificate Signing Request (CSR) was generated, or you can extract it from a previously uploaded certificate.

Open the private key file in a text editor such as WordPad or Notepad++ (do not use Notepad), and look for the word ENCRYPTED. If this word is present, the private key is encrypted. Refer to [Step 2 - Extracting the Private Key](#) point **5** for the private key decryption process.

Step 2 - Extracting the Private Key

This section describes how to extract the private key from the certificate using OpenSSL.

If the private key is encrypted, use the following steps to extract the private key from the PKCS12 token and decrypt the private key on either a Linux system or a Windows system.

- Linux generally comes with OpenSSL preinstalled.
- You can download OpenSSL for Windows from <http://downloads.sourceforge.net/gnuwin32/openssl-0.9.8h-1-setup.exe>

1. If you are using a Windows system, change the working directory so that you can run OpenSSL from the command line:
C:\OpenSSL-Win32\bin\>
2. Enter the following command to simultaneously extract and encrypt the private key:
openssl pkcs12 -nocerts -in certificate.pfx -out private_key_encrypted.pem
3. When prompted, enter the password you assigned when downloading the .pfx file from the Barracuda Load Balancer in point **3** in the section [Step 1 - Downloading the Certificate](#).
4. When prompted again, enter a password to encrypt the private key. This is necessary as the private key must be secured at all times, including when it is displayed onscreen.
5. Enter the following command to decrypt the encrypted private key:
openssl rsa -in private_key_encrypted.pem -out private_key_decrypted.pem
6. When prompted, enter the password you created in point **4** of this section.

Step 3 - Getting the Intermediate and Root Certificates

You can download the intermediate and root certificates of most certificate authorities (CAs) using Microsoft® Internet Explorer®. However, you may need to follow the support link on the CA site to obtain the correct intermediate and root certificates.

1. On the system where you downloaded the certificate, double-click the downloaded certificate, for example, **mycertificate.cer**, and click the **Certificate Path** tab.
2. Double-click each CA in the issuer hierarchy, and note the details including the name of the issuer and the certificate expiry date. These details are helpful in identifying the intermediate and root certificates in the steps that follow.
3. Open Internet Explorer, and go to **Tools > Internet Options > Content > Certificates**.
4. Click the **Intermediate Certification Authorities** tab, and select the relevant certificate.
5. Click **Export**. Follow the instructions in the Wizard, exporting the certificate as **Base-64 encoded X.509 (.CER)**, and saving the export with the appropriate name.
6. In the **Certificates** page, click the **Trusted Root Certification Authorities** tab, and select

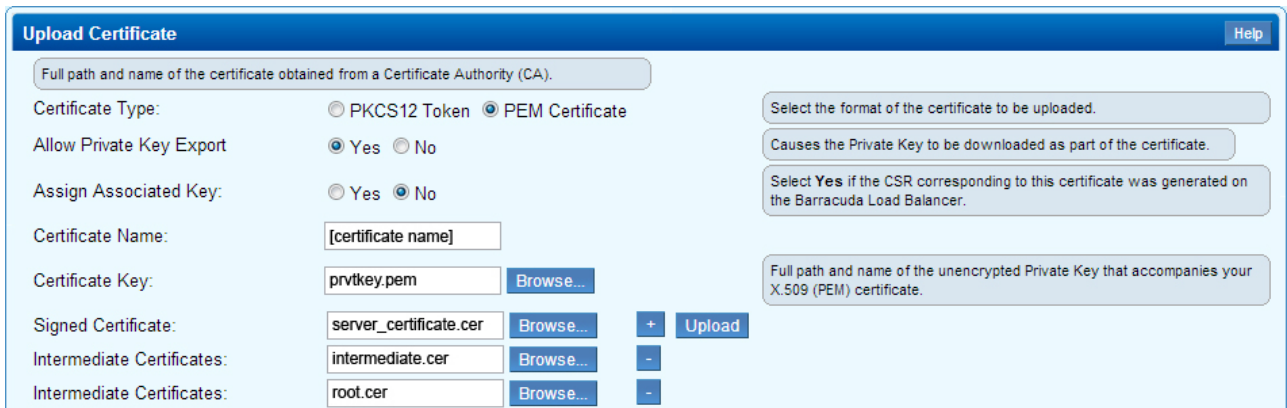
the root certificate.

7. Click **Export**. Follow the instructions in the Wizard, exporting the certificate as a **Base-64 encoded X.509 (.CER)**, and saving the export with an appropriate name.
8. Because Internet Explorer adds trailing line breaks to files, open each exported file in a basic editing program such as WordPad or Notepad++ (do not use Notepad), and remove any trailing line breaks.

Step 4 - Uploading the Certificate

Use the following steps to upload the certificate chain in the correct order, using the screenshot for reference:

1. In the Barracuda Load Balancer web interface, go to the **BASIC > Certificates** page.
2. In the **Upload Certificate** section, select the **Certificate Type** as *PEM Certificate*.
3. Select **Yes** for **Allow Private Key Export**, and set **Assign Associated Key** to *No*.
4. In the **Certificate Name** field, enter a recognizable name for the certificate.
5. In the **Certificate Key** field, click **Browse**, and navigate to and select the Private Key.
6. In the **Signed Certificate** field, click **Browse**, and navigate to and select the Server Certificate.
7. In the **Intermediate Certificates** field, click **Browse**, and navigate to and select the Intermediate Certificate.
8. Click the plus (+) symbol following the **Intermediate Certificates** field.
9. In the new **Intermediate Certificates** field, click **Browse**, and navigate to and select the Root Certificate.



Upload Certificate Help

Full path and name of the certificate obtained from a Certificate Authority (CA).

Certificate Type: ☐ PKCS12 Token ☒ PEM Certificate Select the format of the certificate to be uploaded.

Allow Private Key Export: ☒ Yes ☐ No Causes the Private Key to be downloaded as part of the certificate.

Assign Associated Key: ☐ Yes ☒ No Select Yes if the CSR corresponding to this certificate was generated on the Barracuda Load Balancer.

Certificate Name:

Certificate Key: Browse...

Signed Certificate: Browse... + Upload

Intermediate Certificates: Browse... -

Intermediate Certificates: Browse... -

Full path and name of the unencrypted Private Key that accompanies your X.509 (PEM) certificate.

10. The uploaded certificate displays in the **Upload Certificates** section of the **Saved Certificates** table.

If a warning message such as *Unable to verify issuer certificate* displays when uploading the certificates, this means that the Barracuda Load Balancer is unable to verify the issuer from the Barracuda Load Balancer's issuer information internal bundle. This Barracuda Load Balancer internal bundle contains issuer information updated with each firmware release, and therefore may be incomplete. Conversely, client browsers update issue information dynamically and are able to verify the issuer from the information presented and so this warning can be ignored.

Figures

1. upload_certificates.jpg

© Barracuda Networks Inc., 2024 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.