Installing SSL Certificates with Correct Chain Order

https://campus.barracuda.com/doc/19334080/

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.

Step 1 - Downloading the Certificate

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

1. Log into the Barracuda Load Balancer ADC 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 PKCS #12 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 ADC.

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

If the private key is encrypted, use the following steps to extract the private key from the PKCS #12

token and decrypt the private key on either a Linux system or a Windows system using OpenSSL.

- Linux generally comes with OpenSSL preinstalled.
- You can download OpenSSL version 1.0.2d for Windows from https://slproweb.com/download/Win32OpenSSL-1_0_2d.exe (download a later version if one is available from https://slproweb.com/products/Win32OpenSSL.html).

1. If you are using a Windows system, open a command prompt and change the working directory to the one where you installed OpenSSL so 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. This command looks for the certificate file in the C:\\OpenSSL-Win32\bin\ folder. If the file is located in a different drive or folder, prefix the path to the file name accordingly.
   `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 ADC in point **3** in the section Step 1 - Downloading the Certificate.
4. (Optional) You can export the signed certificate using the following command:
   `openssl pkcs12 -nokeys –nodes -in certificate.pfx -out signed_cert.cer`
5. (Optional) You can decrypt the encrypted private key using the following command:
   `openssl rsa -in private_key_encrypted.pem -out private_key_decrypted.pem`

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 ADC web interface, go to the **BASIC > Certificates** page.
2. In the **Upload Certificate** section, enter a name for the certificate in the **Certificate Name** field.
3. Select the **Certificate Type** as *PEM Certificate*.
4. Select *Yes* for **Allow Private Key Export**, and set **Assign Associated Key** to *No.*
5. In the **Signed Certificate** field, click **Browse**, and navigate to and select the Server Certificate.
6. In the **Certificate Key** field, click **Browse**, and navigate to and select the Private Key.
7. In the **intermediary Certificates** field, click **Browse**, and navigate to and select the Intermediate Certificate.
8. Click the plus (+) symbol following the **Intermediary Certificates** field.
9. In the new **intermediary Certificates** field, click **Browse**, and navigate to and select the Root Certificate.
10. Click **Upload Now** to upload the certificate.
11. 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 ADC is unable to verify the issuer from the Barracuda Load Balancer ADC's issuer information internal bundle. This Barracuda Load Balancer ADC internal bundle contains issuer information updated with each firmware release, and therefore may be incomplete. Conversely, client browsers update issuer information dynamically and are able to verify the issuer from the information presented and so this warning can be ignored.