Installing SSL Certificates with Correct Chain Order

https://campus.barracuda.com/doc/20644033/

A browser running on a desktop system can build a certificate chain correctly regardless of the order in which certificates are presented. However, a browser running on a mobile device, such as Android, may require the certificates to be presented in the correct order.

This article explains how to upload the certificate chain in the order that ensures it is properly presented to the client.

Step 1 - Download the Certificate

Use the following steps to download the certificate from the Barracuda Web Application Firewall:

1. Log into the Barracuda Web Application Firewall 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 pass phrase in the **Encryption Password** field, and click **Save**.
4. The certificate is exported as a PKCS #12 token, which includes the private key.

Private Key

If you already have the private key, ensure it is decrypted before you upload it to the Barracuda Web Application Firewall.

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 if the word ENCRYPTED 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 - Extract the Private Key

This section describes how to extract the private key from a PKCS #12 file using OpenSSL.

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.

OpenSSL

- 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, open a command prompt and change the working directory to the one where you installed OpenSSL 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. 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 Web Application Firewall 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 - Get 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.

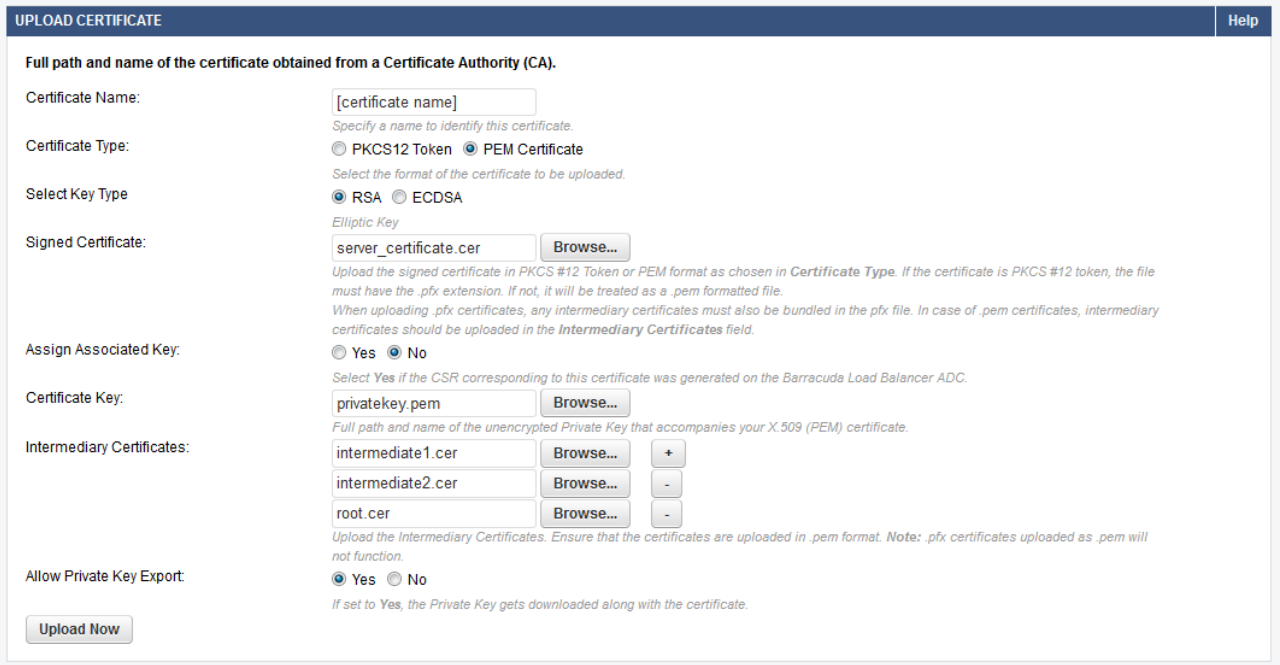
1. On the system where you downloaded the certificate, double-click the downloaded certificate, for example, **mycertificate.cer**, and click the **Certificate Path** tab.
2. Double-click each CA in the issuer hierarchy, and note the details, including the name of the issuer and the certificate expiry 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 - Upload the Certificate

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

1. In the Barracuda Web Application Firewall 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 the key/algorithm used in the certificate.
   - **RSA** - RSA is a public-key cryptography algorithm.
   - **ECDSA** - Elliptic Curve Digital Security Algorithm (ECDSA) is a digital signature algorithm which uses Elliptic Curve Cryptography (ECC).
5. In the **Signed Certificate** field, click **Browse**, and navigate to and select the Server Certificate.
6. Set **Assign Associated Key** to *No*.
7. In the **Certificate Key** field, click **Browse**, and navigate to and select the Private Key.
8. In the **intermediary Certificates** field, click **Browse**, and navigate to and select the Intermediate Certificate.
9. Click the plus (+) symbol following the **Intermediary Certificates** field.
10. In the new **intermediary Certificates** field, click **Browse**, and add the second Intermediate Certificate.
11. Click the plus (+) symbol following the **Intermediary Certificates** field, navigate to and select the Root Certificate.
12. Select *Yes* for **Allow Private Key Export**.
13. Click **Upload Now** to upload the certificate.



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

Warning Message

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

Figures