Convert from PFX Format to PEM Format for SSL certifcates imported from IIS

- Parallels Remote Application Server 18.2
- Parallels Remote Application Server 18.3
- Parallels Remote Application Server 19.1
- Parallels Remote Application Server 18.0
- Parallels Remote Application Server 19.0
- Parallels Remote Application Server 18.1

To use this certificate with a Parallels Client Gateway, one must convert the PFX file to the un-encrypted PEM format.

Use the open-source utility OpenSSL to perform the conversion from PFX to PEM. A downloadable Win32 distribution of OpenSSL is available here:

http://gnuwin32.sourceforge.net/packages/openssl.htm

To convert a PFX file to a PEM file, follow these steps on a Windows machine:

1. Download and install the Win32 OpenSSL package, using the link above.
2. Create a folder **c:\certs** and copy the file **cert.pfx** (the created PFX file) into the **c:\certs** folder.
3. Open a command prompt, and move to the GnuWin32\bin directory, using:

   ```
   cd %ProgramFiles%\GnuWin32\bin
   ```
4. Type the following command to convert the PFX file to an unencrypted PEM file:

   ```
   openssl pkcs12 -in c:\certs\cert.pfx -out c:\certs\cert.pem -nodes
   ```
5. When prompted for the import password, enter the password you used when exporting the certificate to a PFX file.

You should then receive a message that says"

MAC verified OK

- To enable SSL with **cert.pem**

  1. On the Parallels Client Gateway page, enable Secure Sockets Layering (SSL) and click "**...**" to browse for the PEM file.
  2. Click **Apply** to apply the new settings.

Note that your browser may not support the display of this image.

- If the Issuer is not a trusted authority, an additional step is necessary, as Parallels clients do not trust and are unaware of the Issuer Certificate authority. It's therefore necessary to extract the certificate from the certificate authority and assign it to Parallels Remote Application Server clients. The Issuer refers to the authority that issued the certificate.

  1. Using the certificate snap-in, find Issuer's certificate from the certificates console.

     Note that your browser may not support the display of this image.
  2. Right-click on the Issuer certificate, select **All Tasks > Export**.

3. Choose **No** and do not export the private key, as only the certificate is necessary.
4. Then choose a Base-64 encoded X.509 (.CER) format.

   Note that your browser may not support the display of this image.
5. Specify the filename you'd like to export, and save the certificate.
6. Click **Finish**.
7. Open the exported certificate with a word processor and copy the contents to the clipboard.

- On the client side, under C:\Program Files\Parallels\Client\, the file **trusted.pem** should be visible. This file contains certificates of common trusted authorities. Paste the content of the exported certificate, which is attached to the certificates list.

This will add the Issuer certificate and list of trusted authorities on the client side, and one would be able to connect over SSL with a certificate from an organization certification authority.
