Move Certificate from Microsoft IIS 6.0 to Apache

(index?page=content&id=SO5997&pmy=print&actp=PRINT&viewlocale=en_US) Printer Friendly (index?page=content&id=SO5997&pmy=print&actp=PRINT&viewlocale=en_US)

Solution ID: SO5997
Version: 2.0
Published: 12/13/2007
Updated: 09/05/2008

Average Rating
★★★★★
2 rating(s)

Select the number of stars and add (optional) article comments here. To submit click 'Rate'.

Rate

Resolution

To Move a Certificate from IIS 6.0 to Apache do the following:

Create an MMC Snap-in for Managing Certificates:

1. Start > run > MMC

2. Go into the Console Tab > 'File' > 'Add/Remove Snap-in'

3. Click on 'Add' > Click on 'Certificates' and click on 'Add'

4. Choose 'Computer Account'

5. Choose 'Local Computer'

6. Close the 'Add Standalone Snap-in' window

7. Click on 'OK' at the 'Add/Remove Snap-in' window

Export your certificate and private key .pfx file from IIS6:

1. Open the Certificates (Local Computer) snap-in you added in the last section, navigate to Personal, and then to Certificates

2. You will see your Web server certificate denoted by the CN (Common Name) found in the Subject field of the certificate (using Microsoft Internet Explorer, you can easily view the certificate to see the Common Name if you are unsure)

3. Right-click on the server certificate, select All Tasks, and then click Export

4. When the wizard starts, click Next. Choose to export the private key, and then click Next

> NOTE: If you export the certificate for use on an IIS Web server, do not select Require Strong Encryption.This option causes a password prompt every time an application attempts to access the private key, and causes IIS to fail.

5. The file format you will want to choose is the Personal Information Exchange (though you can select from several options). This will create a PFX file.

> Notice that you can export any certificates in the certification path by selecting the option on this screen. This is very handy if your certificate was issued by a non-trusted certificate authority (for example, Microsoft Certificate Server)
>
> Only choose delete the private key if the export is successful to be sure it is not left on the computer (for example if your migrating from one server to another)

6. Click Next, and then choose a password to protect the PFX file. You will need to enter the same password twice to ensure that the password is typed correctly. When you have completed this step, click Next

7. Choose the file name you want to save this as. Do not include an extension in your file name; the wizard will automatically add the PFX extension for you

8. Click Next, and then read the summary

> Pay special attention to where the file is being saved to
>
> If you are sure the information is correct, choose Finish

9. You now have a PFX file containing you server certificate and its corresponding private key.

Be sure to protect this file. You may want to move it to a floppy disk and store it somewhere safe from outside disturbance. Keep in mind, if you run a backup on the server, this file may be saved in that backup if it is still on the server.

To convert the .pfx file to a file that your Apache server will understand

Run the following command using OPENSSL:

1. To export the Private key file from the .pfx file

> openssl pkcs12 -in filename.pfx -nocerts -out key.pem

2. To export the Certificate file from the .pfx file

> openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cert.pem

3. You now need to copy the files to the locations as described in the httpd.conf

4. To find out where the files should be copied to run this on the httpd.conf

cat httpd.conf | grep SSLCertificateFile (this will give you the location of where to copy the certficate file)

cat httpd.conf | grep SSLCertificateKeyFile (this will give you the location of where to copy the key file)

5. You will now need to restart the http daemon

6. If you do not want to include a passphrase you can use the following command: openssl rsa -in key.pem -out server.key