



How to install a certificate on Traffic Manager from IIS' certificate store

Contents:

- Export certificate from IIS
- Convert to pem format and split out the public and private certificates
- Install in to Traffic Manager
- Test the certificate

Export Certificate from IIS

To export the certificate from IIS, first create a Certificates snap-in using the Microsoft Management Console:

- Click **Start**, and then click **Run**
- Type "MMC.EXE" (without the quotation marks) and click **OK**.
- Click **Console** in the new MMC you created, and then click **Add/Remove Snap-in**.
- In the new window, click **Add**.
- Highlight the **Certificates** snap-in, and then click **Add**.
- Choose the **Computer** option and click **Next**.
- Select **Local Computer** on the next screen, and then click **OK**.
- Click **Close**, and then click **OK**.

Now that you have added the Certificates snap-in, you can export the key pair that your Web server is using (the certificate and public key). To do this, perform the following steps:

- Open the Certificates (Local Computer) snap-in you added in the last section, navigate to **Personal**, and then to **Certificates**.
- You will see your Web server certificate denoted by the CN (Common Name) found in the Subject field of the certificate (using Internet Explorer 5.0, you can easily view the certificate to see the Common Name if you are unsure).
- Right-click on the server certificate, select **All Tasks**, and then click **Export**.
- When the wizard starts, click **Next**. Choose to export the private key, and then click **Next**.
- The file format you will want to choose is the **Personal Information Exchange**. This will create a PFX file. 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). **NOTE:** If you do not select "Include all certificates in the certificate path if possible" and the issuer of the certificate

jetNEXUS, Cedar Court Grove Business Park, Waltham Road, Maidenhead, Berks, SL6 3LW

W: www.jetnexus.com **E:** info@jetnexus.com **T:** 0870 382 5050



is not trusted by your server, then you may notice that when the properties of the certificate are viewed, the "This certificate is issued to:" field may display "Windows does not have enough information about this certificate". This is by design and can be resolved by selecting "Include all certificates in the certificate path" while exporting the certificate.

- 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**.
- 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.
- 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**.
- You now have a PKCS#12 format file containing your server certificate and its corresponding private key.

Convert to pem format and split out the public and private certificates

To convert the certificate from the pfx file to the two separate files needed for Traffic Manager you can use the OpenSSL suite of tools (<http://www.openssl.org>).

- Open a command prompt and change directory to the location of the pfx file saved previously.
- Then run the following command substituting the appropriate filenames:

```
openssl pkcs12 -in file.pfx -nodes -out file.pem
```

- This will first ask for the "Import Password" this is the password that was used when exporting the certificate. Supply this and it will output the pem file.
- Next we need to split out the Private key into a separate file.
- Open the new file with a text editor like Notepad / textpad and copy the private key section from the pem file to a new file. Make sure this starts from the "Bag Attributes" down to the "End RSA ..."
- Once you are happy this is the entire section (it needs to be EXACTLY what is in the certificate) you can delete the private key from the .pem file.
- Then we need to make sure that any supporting certificates are in the right order for all browsers. Internet Explorer is unfussed as to the order of certificates. Firefox on the other hand is particular about the order. The order needs to be from the main certificate (yours) to the last supporting certificate. The default export order from IIS is to reverse the supporting certificates from the furthest to the nearest at the bottom. When moving these around, again make sure to get all the "Bag Attributes" to the "End RSA...."

jetNEXUS, Cedar Court Grove Business Park, Waltham Road, Maidenhead, Berks, SL6 3LW

W: www.jetnexus.com **E:** info@jetnexus.com **T:** 0870 382 5050



- Once you are happy with the order of the certificates save the file (probably as a new file to make sure you have all the original data). You can then move on to installing these on Traffic Manager.....

Install in to Traffic Manager

To install the certificate on to a traffic manager.

- First open the web GUI on to a traffic manager and go to “Catalogs > SSL > SSL Certificates catalog” and click “Import Certificate”. On this screen type in a name for the certificate. This is the name used to refer to the certificate when setting up an SSL virtual server.
- Then click “Browse” next to “Certificate file” and select the pem file from earlier.
- Next click “Browse” next to “Private key file” and select the file created earlier.
- Finally click “Import Certificate”. Now we need to test the certificate.

Test the Certificate

To do this we recommend testing on a test virtual server and not the live environment. This involves setting up a virtual server on an internal IP address and appointing it at a web server. Then modify your hosts file to have the website the certificate is for to be on the IP address of the new virtual server.

If your site’s certificate is for “test.site.com” and the new virtual server is listening on “192.168.100.25” you will need to add the following to your hosts file:

```
test.site.com          192.168.100.25
```

Once you have done this point your browser(s) at the new site (test.site.com) and you should get no errors regarding certificates. If you do see errors with firefox and not Internet Explorer it will be the order of the supporting certificates.