KB11349

SYMPTOM

Unable to import into EFT because it does not use a passphrase and/or it is missing the private key.

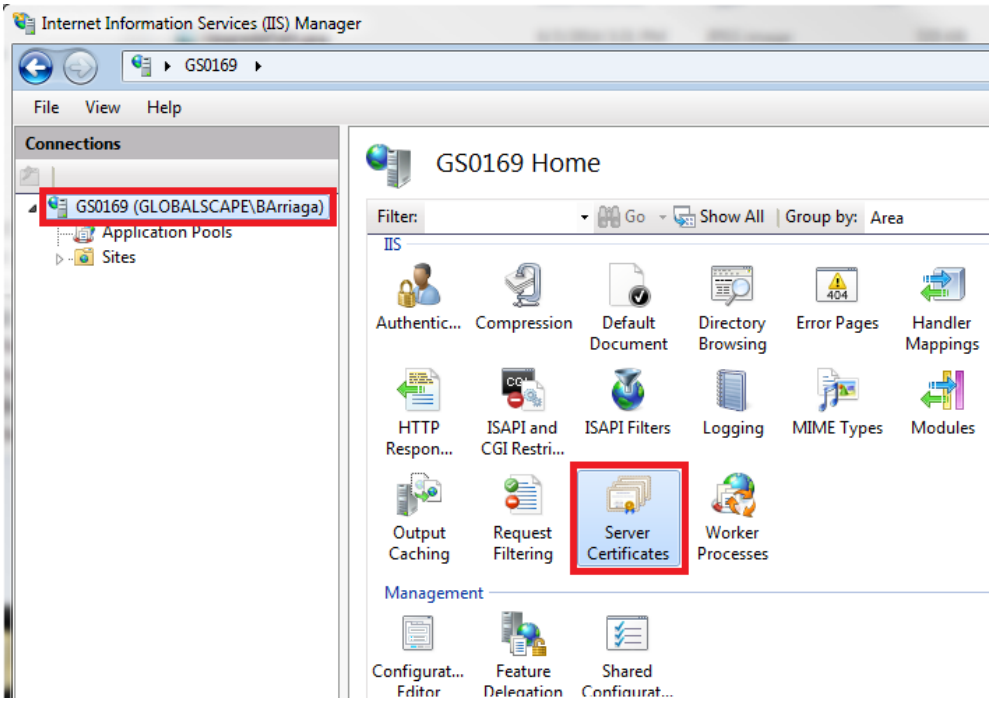
WORKAROUND

EFT requires three items to successfully implement an SSL certificate: The certificate, private key, and passphrase.

A .pfx file will usually contain both the certificate and private key.

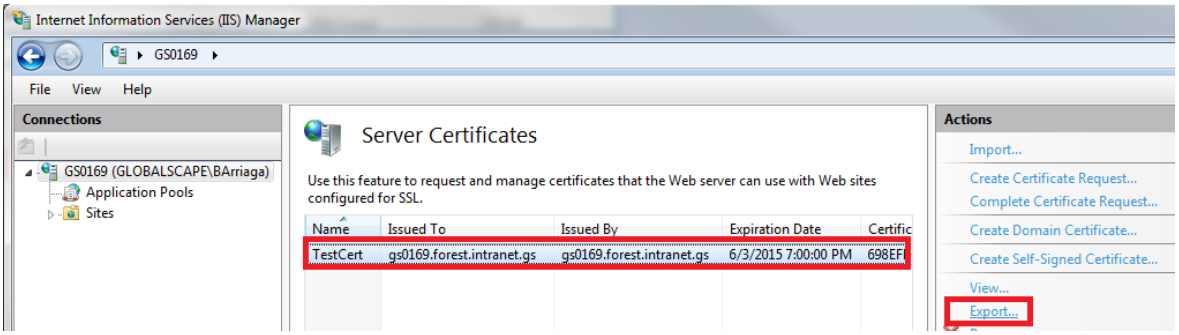
If the .pfx certificate was originally created within IIS, it most likely does not have a passphrase associated with it. You can export the corresponding private key and create a passphrase from within IIS.

To do this, first open the IIS where the certificate originated. Then open **Server Certificates**

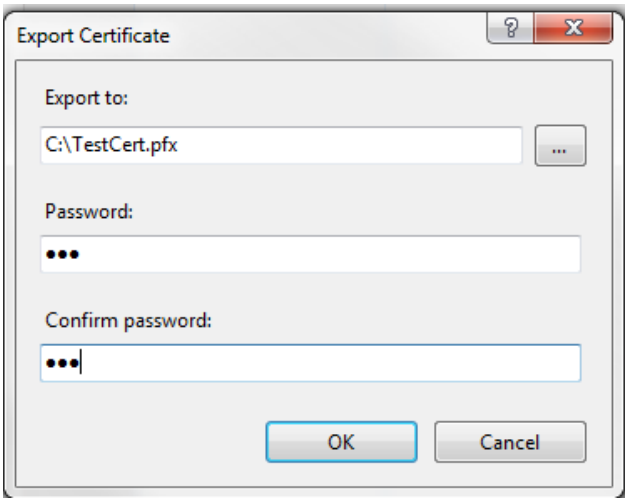


Select the certificate that the signed certificate originally came from.
Or if the signed .pfx file already has a the private key but does not have a **passphrase**, you can create one by first **importing** it,

After selecting the certificate in IIS, you have 2 different ways to export the certificate:
Method 1) Click the cert and then click **export**.



This will now pop up a prompt asking for an output path and to specify the new passphrase.

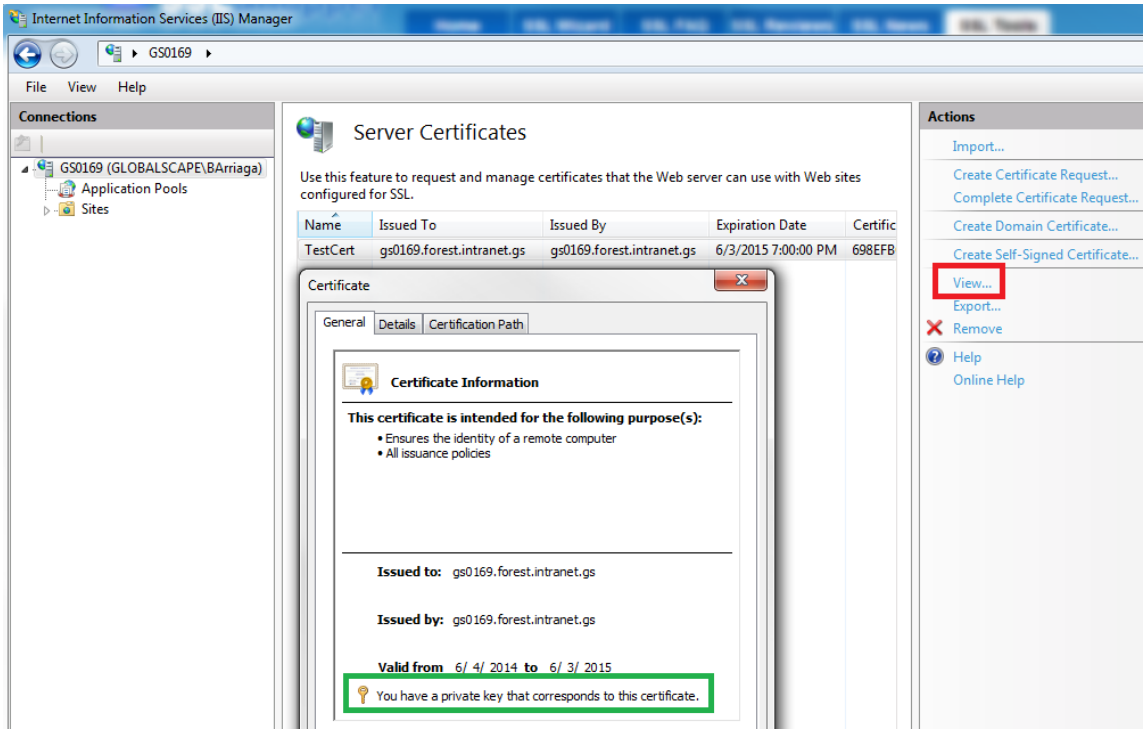


The certificate will now be outputted as **.pfx** file containing the certificate, private key, and will use the specified passphrase.
You can either use this directly in EFT as the **private key**, or you can further break this out into a .crt/.key by converting the **.pfx** file to a **.pem** using SSLshopper's SSL converter utility and extracting the components.

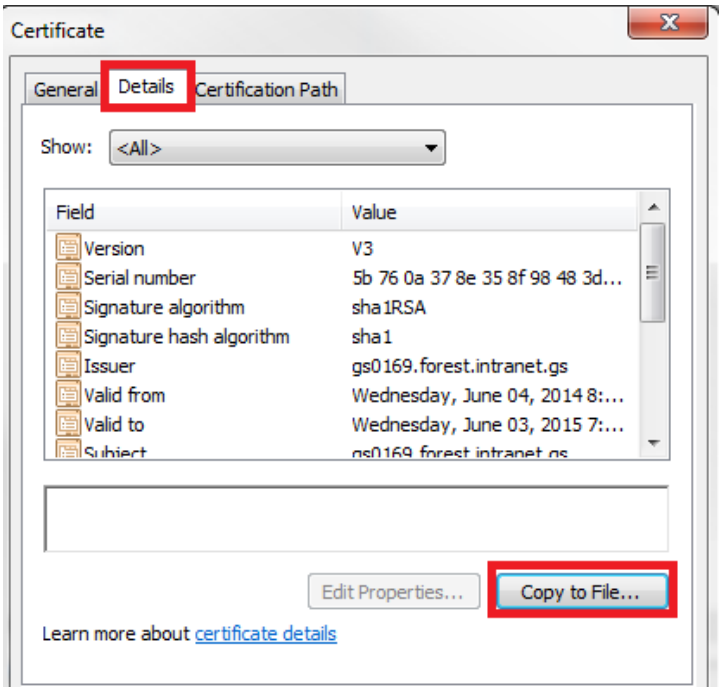
NOTE You will still want to use the signed certificate that was received by the CA as the **certificate**, but you will use the exported private key/passphrase portion within EFT.

Method 2) Double-click the certificate or select it and press **View**.

From here, you can confirm that the certificate has the private key.

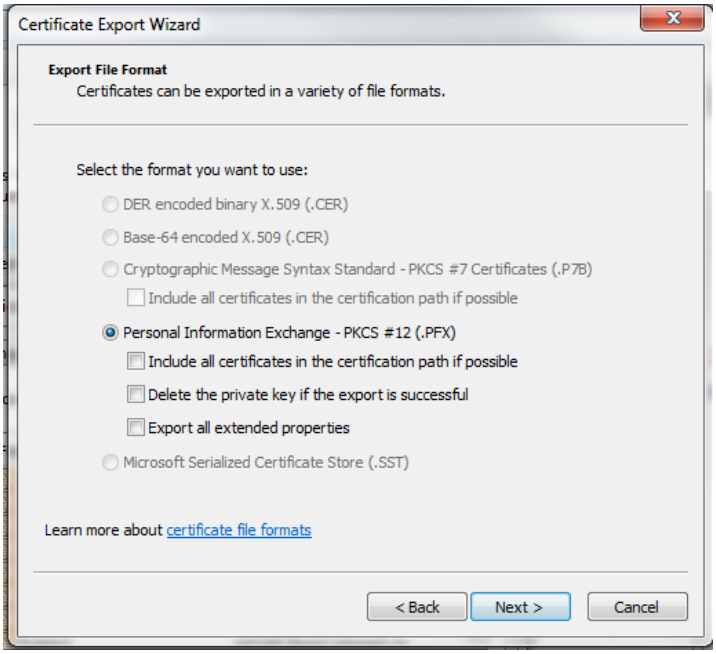


Click on the **Details** tab, then click **Copy to File.**



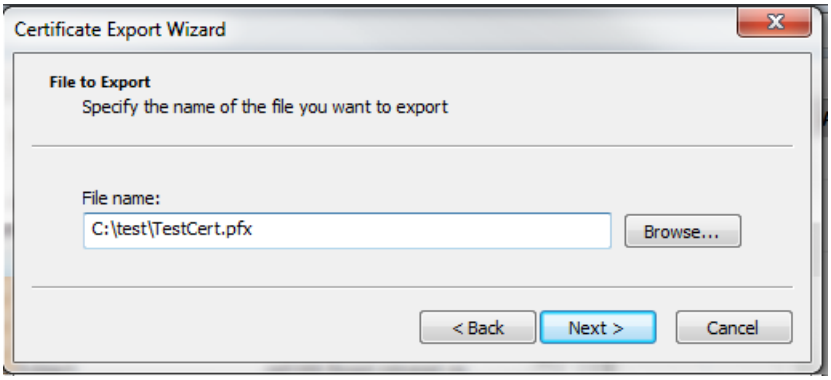
The Certificate Export Wizard appears.

Click the option to export the private key:



You will then be prompted to specify/create the passphrase:

Specify the output location of the certificate:



The certificate will now be output as .**pfx** file containing the certificate, private key, and will use the specified passphrase.
You can either use this directly in EFT as the **private key**, or you can further break this out into a .crt/.key by converting the **.pfx** file to a **.pem** using SSLshopper's SSL converter utility and extracting the components.

NOTE You will still want to use the signed certificate that was received by the CA as the **certificate**, but you will use the exported private key/passphrase portion within EFT.

To convert a **.pfx** cert into a **.pem** and then break apart into a **.crt** / **.key** please see the certificate chaining guide.