

[KB11349](#)

SYMPTOM

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

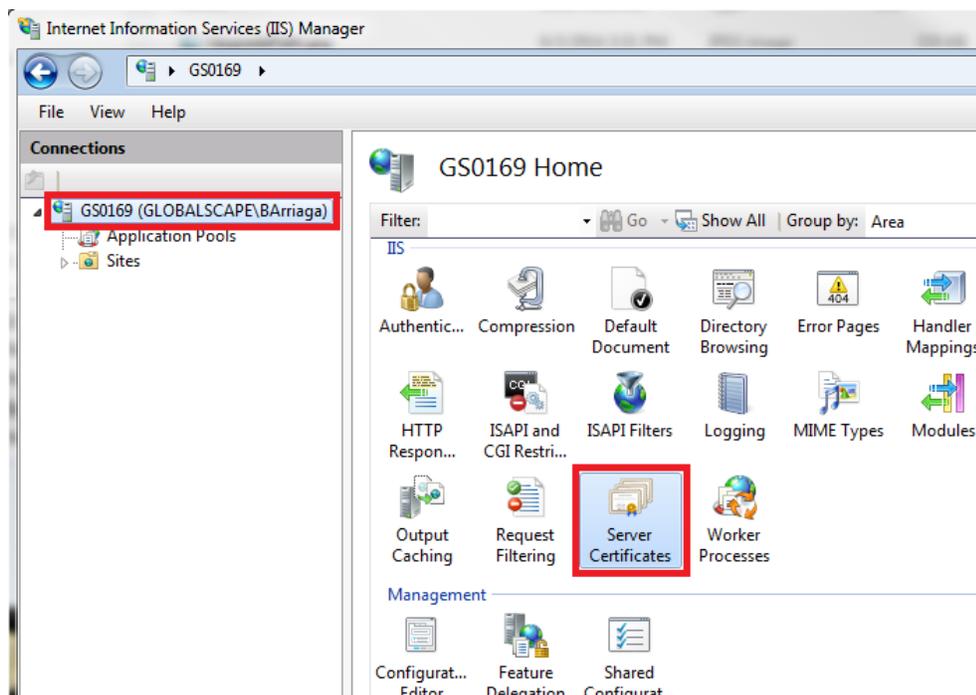
WORKAROUND

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**

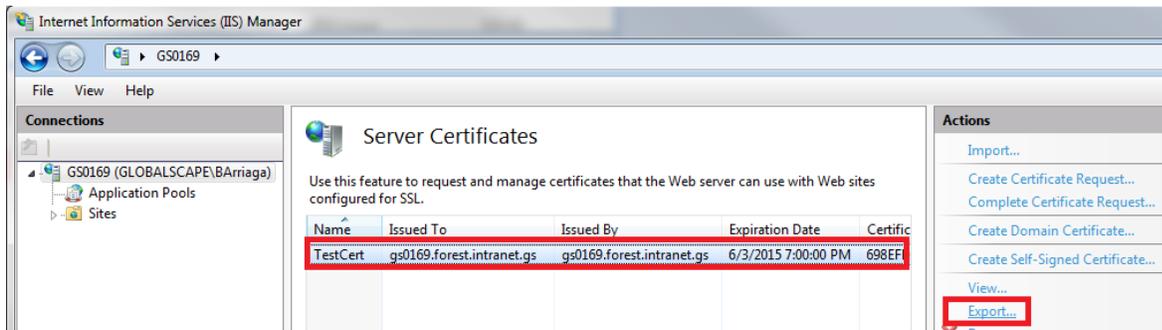


Select the certificate that the signed certificate originally came from.

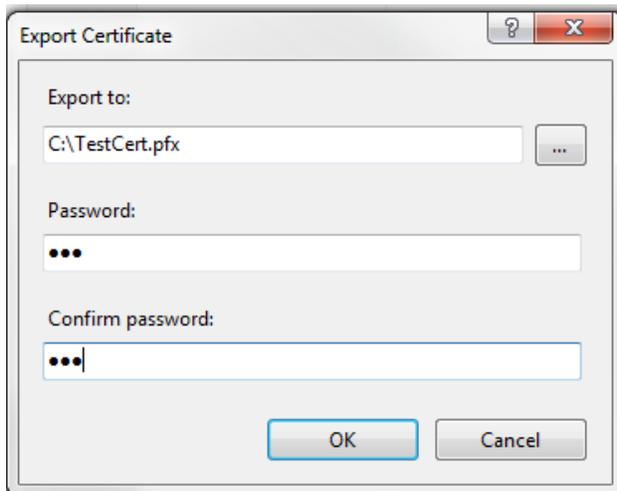
Or if the signed .pfx file already has a the private key but does not have a **passphrase**, you can create one by first **importing** it,

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.



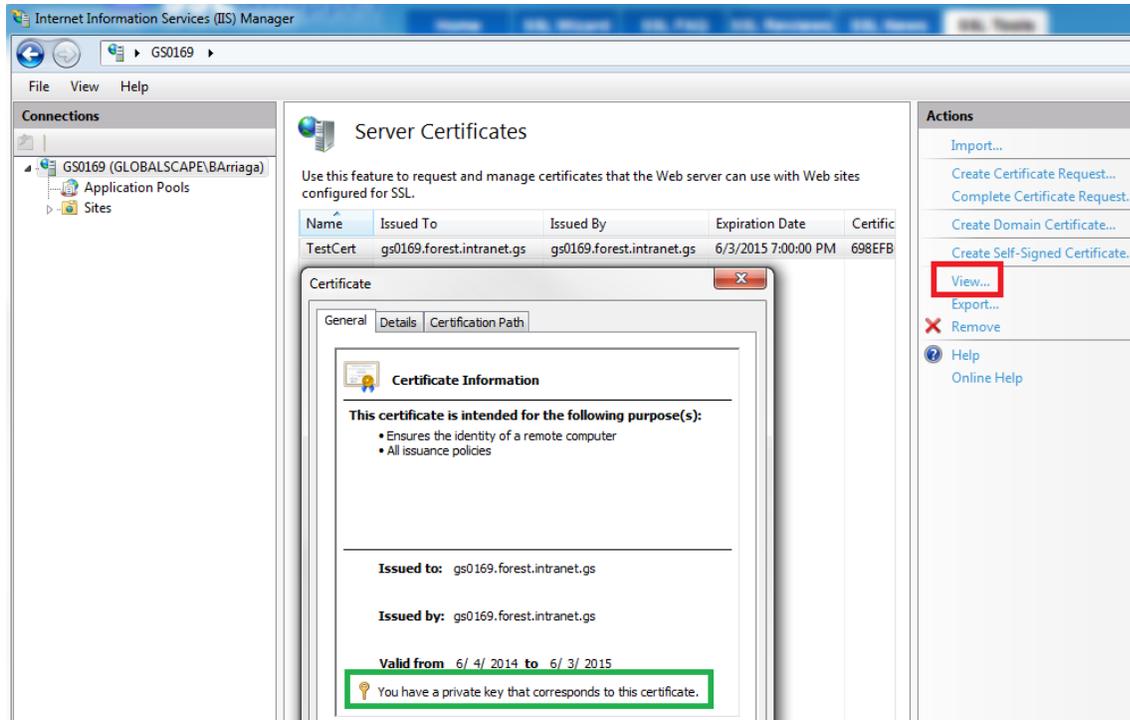
The certificate will now be outputted as **.pfx** file containing the certificate, private key, and will use the specified passphrase.

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.

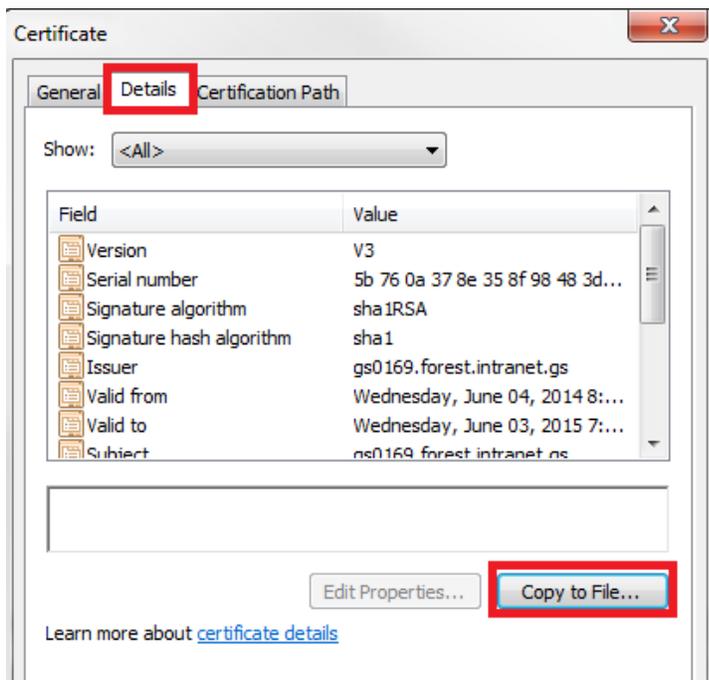
NOTE You will still want to use the signed certificate that was received by the CA as the **certificate**, but you will use the exported private key/passphrase portion within EFT.

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:

Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

Yes, export the private key
 No, do not export the private key

Learn more about [exporting private keys](#)

< Back Next > Cancel

Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

DER encoded binary X.509 (.CER)
 Base-64 encoded X.509 (.CER)
 Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 Include all certificates in the certification path if possible

Personal Information Exchange - PKCS #12 (.PFX)
 Include all certificates in the certification path if possible
 Delete the private key if the export is successful
 Export all extended properties

Microsoft Serialized Certificate Store (.SST)

Learn more about [certificate file formats](#)

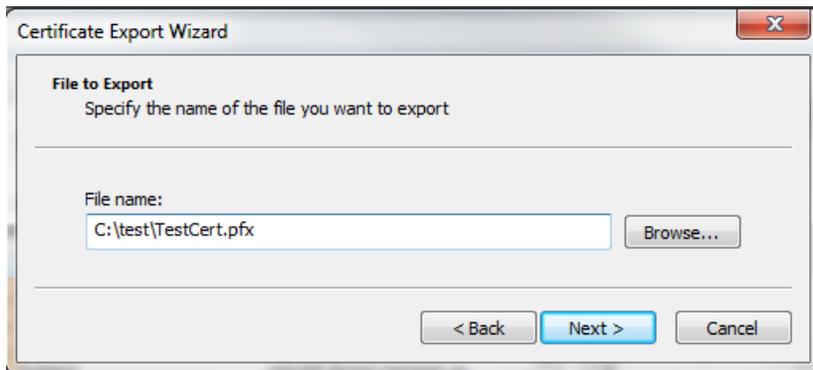
< Back Next > Cancel

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



The screenshot shows the 'Certificate Export Wizard' dialog box. The title bar reads 'Certificate Export Wizard'. The main content area is titled 'Password' and contains the text: 'To maintain security, you must protect the private key by using a password.' Below this, it says 'Type and confirm a password.' There are two text input fields: the first is labeled 'Password:' and the second is labeled 'Type and confirm password (mandatory):'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Specify the output location of the certificate:



The screenshot shows the 'Certificate Export Wizard' dialog box. The title bar reads 'Certificate Export Wizard'. The main content area is titled 'File to Export' and contains the text: 'Specify the name of the file you want to export'. Below this, there is a text input field labeled 'File name:' containing the text 'C:\test\TestCert.pfx'. To the right of the input field is a 'Browse...' button. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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 **.cert/.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 **.cert / .key** please see the [certificate chaining guide](#).