

<u>KB11349</u>

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**.

globalscape[®]

📬 Internet Information Services (IIS) Manag	er				
GS0169 ►					
File View Help					
Connections	Server Certificates Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.			Actions	
GS0169 (GLOBALSCAPE\BArriaga) GS0169 (GLOBALSCAPE\BArriaga) G Application Pools Sites				Import	
				Create Certificate Request Complete Certificate Request	
	Name Issued To	Issued By	Expiration Date	Certific	Create Domain Certificate
	TestCert gs0169.forest.intranet.gs	gs0169.forest.intranet.gs	6/3/2015 7:00:00 PM	698EFI	Create Self-Signed Certificate
					View
					Export

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

Export Certificate			? <mark>X</mark>
Export to:			
C:\TestCert.pfx			
Password:			
•••			
Confirm password:			
•••			
	ОК	Ca	ancel

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.

😋 Internet Information Services (IIS) Manage	r		8. Marcel 1 10. 744		-	COLUMN TOWN
GS0169 ►						
File View Help						
Connections	An Comer Cartificates				Actions	
之一	Server Certificates				Import	
GS0169 (GLOBALSCAPE\BArriaga)	Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.				Create Certificate Request Complete Certificate Request	
p · · · · · · · · · · · · · · · · · · ·	Name	Issued To	Issued By	Expiration Date	Certific	Create Domain Certificate
	TestCert	gs0169.forest.intranet.gs	gs0169.forest.intranet.gs	6/3/2015 7:00:00 PM	698EFB	Create Self-Signed Certificate
	Certificate				View	
	Genera	Details Certification Path				Export
					Help	
		Certificate Information	1			Online Help
	This cartificate is intended for the following purpose(s):					
	Ensures the identity of a remote computer					
	All issuance policies					
	Travel to: a0150 fixed interest or					
	Issued to: gso to3, torest, ind aret. gs					
	Issued by: gs0169.forest.intranet.gs					
		Valid from 6/4/2014 to	6/3/2015			
		You have a private key that (corresponds to this certificate.	1		

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

Certificate General Details Certification Pail Show: <all></all>	th
Field	Value 🔺
Version Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Subject Valid from Valid to	V3 5b 76 0a 37 8e 35 8f 98 48 3d sha 1RSA sha 1 gs0 169. forest.intranet.gs Wednesday, June 04, 2014 8: Wednesday, June 03, 2015 7: os0169. forest.intranet.gs
Learn more about <u>certificate detai</u>	Edit Properties 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 <u>exporting private keys</u>
< 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:
OER 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 <u>certificate file formats</u>
< Back Next > Cancel



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

Certificate Export Wizard	x				
Password To maintain security, you must protect the private key by using a password.					
Type and confirm a password. Password:					
Type and confirm password (mandatory):					
< Back Next > Can	el				

Specify the output location of the certificate:

Certific	ate Export Wizard	J
File	to Export Specify the name of the file you want to export	
	File name: C:\test\TestCert.ofx	
	< Back Next > 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 .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 <u>certificate</u> <u>chaining guide</u>.