CREATING, SIGNING, CHAINING, AND ASSIGNING A CERTIFICATE IN EFT SERVER

This document provides instructions for creating an SSL certificate, signing the certificate, chaining the certificate, and then finally, adding the certificate to EFT Server.

I. Create an SSL certificate:

Refer to the online help file topic at: http://help.globalscape.com/help/eft7-3/mergedprojects/eft/creatingsslcertificates.htm

II. Sign the certificate:

The *.csr, *.crt, and *.key file are located at the EFT Server application data root: **C:\Documents and Settings\All Users\Application Data\GlobalSCAPE\EFT Server\ or \EFT Server Enterprise\.** There you can retrieve the *.csr file to send to VeriSign, Thwate, GoDaddy, etc. using the same process that you normally do. Just make certain that you request the certificate in Apache x509 certificate format.

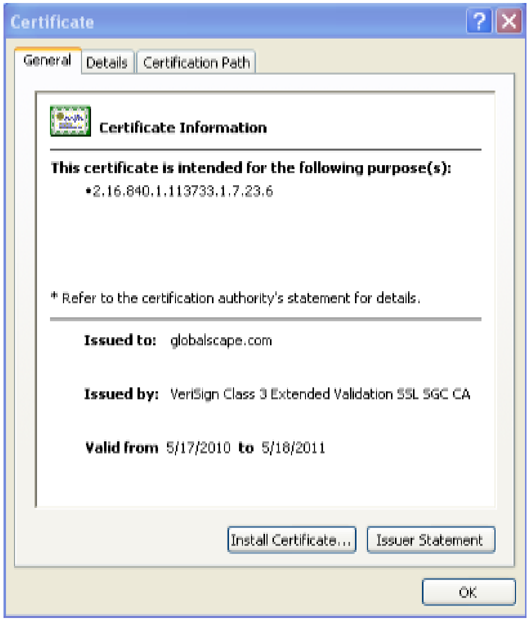
III. Chain the certificate:

Once you receive the signed *.cer from VeriSign, Thwate, GoDaddy, etc. in your normal fashion, use the procedure below to chain your signed certificate to the Certificate Authorities intermediate certificate. (Thwate certificates enrolled after June 27, 2010 require two intermediate certificates. https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=AR1373&actp=search&viewlocale=en_US&searchid=1279730423933)

In order to ensure that EFT Server and Java[2] (used for the Web Transfer Client (WTC)) present certificates in a manner that FTP clients and web browsers are going to verify successfully, use the following instructions to chain the Certificate Authorities' (CA) intermediate certificate to the signed certificate. (Unlike VeriSign, for GoDaddy and Thawte certificates, there may be two intermediate certificates. This means that both will need to be included in the chain.) (Java wants both the original certificate and the intermediate to be passed for each user.)

To chain the CA intermediate certificate to the signed certificate

1. Acquire the signed certificate in Apache x509 standard (should be a *.cer file)
2. Double click the signed certificate (*.cer) file



This certificate is intended for the following purpose(s):

- 2.16.840.1.113733.1.7.23.6

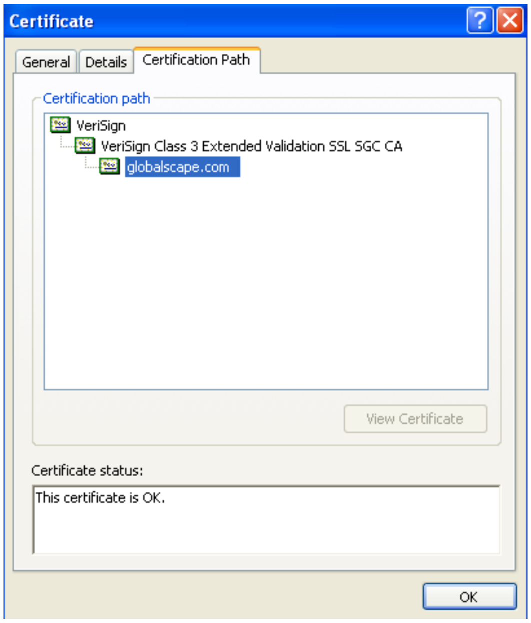
* Refer to the certification authority's statement for details.

Issued to: globalscape.com

Issued by: VeriSign Class 3 Extended Validation SSL SGC CA

Valid from 5/17/2010 to 5/18/2011

3. Click the **Certification Path** tab.



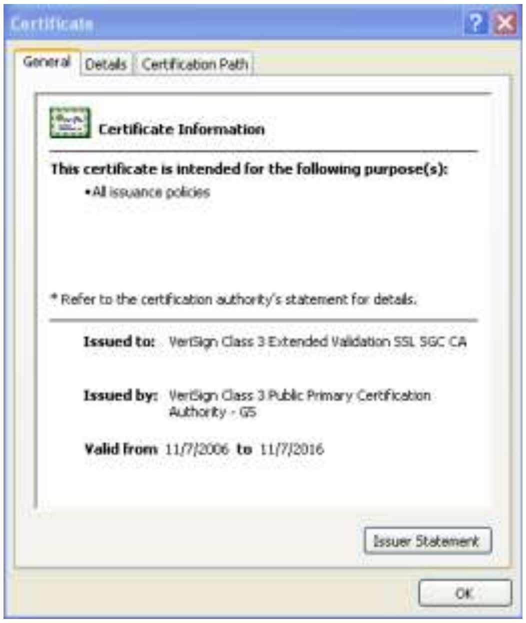
VeriSign
VeriSign Class 3 Extended Validation SSL SGC CA
globalscape.com

Certificate status:

This certificate is OK.

(For GoDaddy and Thawte, there could be four certificates instead of three.)

4. The top most certificate is the CA's root certificate and the bottom most is the signed certificate from the CA. Please ignore both and focus solely on the middle certificate(s).
5. Click on a middle certificate
6. Click **View Certificate**. The certificate information appears.



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies

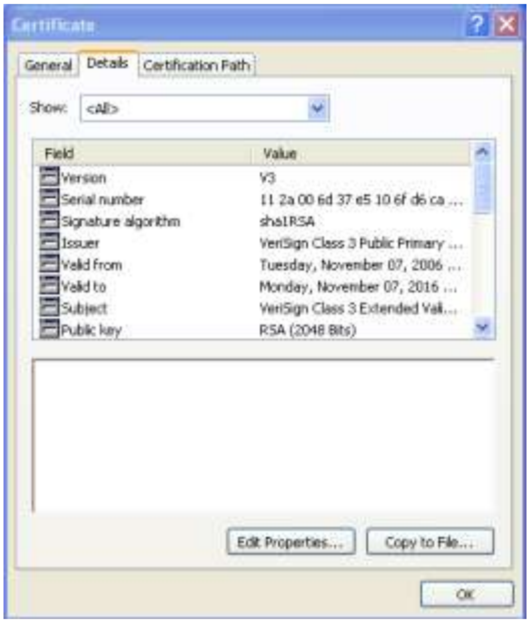
* Refer to the certification authority's statement for details.

Issued to: VeriSign Class 3 Extended Validation SSL SGC CA

Issued by: VeriSign Class 3 Public Primary Certification Authority - G5

Valid from 11/7/2006 **to** 11/7/2016

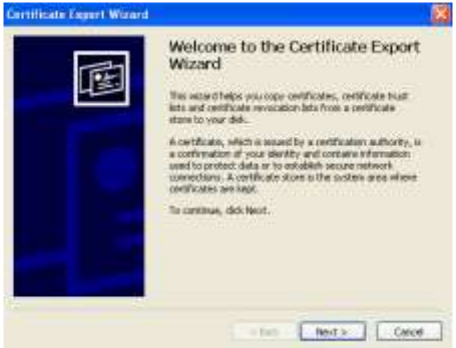
7. Click the **Details** tab.



Show: <All>

Field	Value
Version	V3
Serial number	11 2a 00 6d 37 e5 10 6f d6 ca ...
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Public Primary ...
Valid from	Tuesday, November 07, 2006 ...
Valid to	Monday, November 07, 2016 ...
Subject	VeriSign Class 3 Extended Vali...
Public key	RSA (2048 Bits)

8. Click **Copy to File**. The **Certificate Export Wizard** appears.
9. On the first page of the **Certificate Export Wizard**, click **Next**.



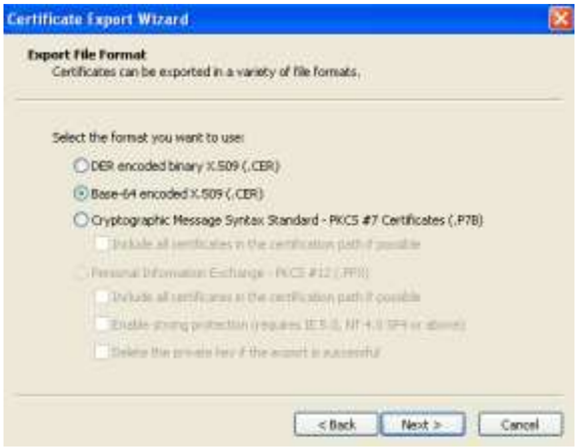
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

10. Click **Base-64 encoded X.509 (.CER)**, then click **Next**.



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

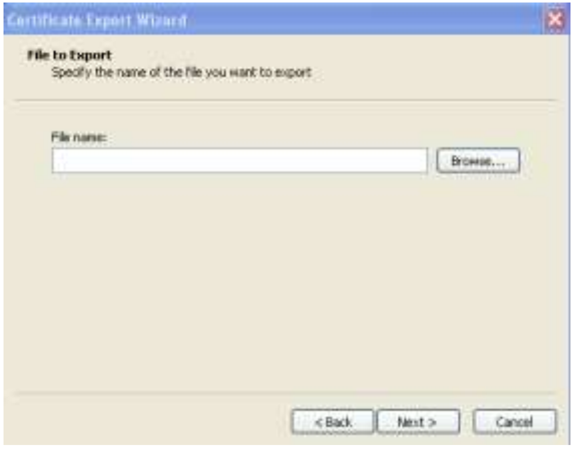
○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

11. Specify the location in which to save the intermediate certificate, then click **Next**.



File to Export

Specify the name of the file you want to export

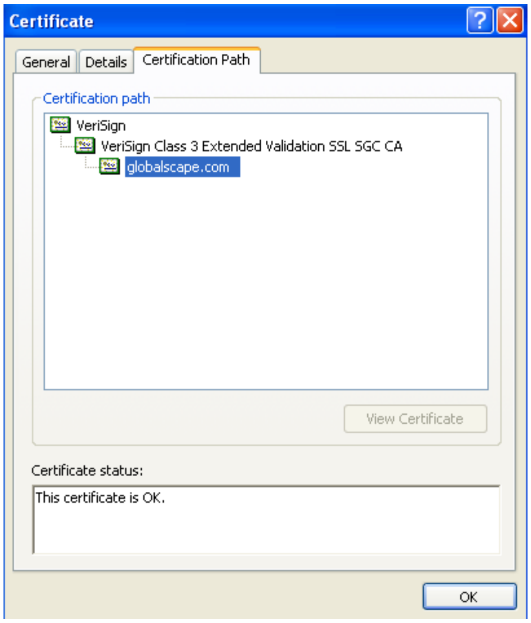
File name:

12. Click **Finish** to complete the export. (Repeat steps 5 thru 12, if there were two intermediate certificates.)
13. Using Notepad, open the signed certificate from the CA.
14. After the -----END CERTIFICATE----- line, press ENTER twice (2).
15. Using Notepad, open the intermediate certificate(s) (the exported certificate(s)).
16. Copy the entire contents, ensuring that -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- and everything in-between are included.
17. Paste this information into the open signed certificate with the signed certificate on top and the intermediate second. Should there be a second intermediate, place it after the first intermediate.

```
-----BEGIN CERTIFICATE-----
MIIDgzCCAuygAwIBAgIQRvzrurTQLw+SYJgjP5MHjzANBgkqhkiG9w0BAQUFA
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
HSUELTArBggrBgEFBQcDAQYIKwYBBQUHAwIGCWCGSAGG+EIEAQYKYIZ
-----END CERTIFICATE-----
```

18. Save this new file as **combined_certificatename.crt** or **certificatename_combined.crt**.
19. Double click the saved file (it should open as a certificate).
20. Verify that the Certificate Path is complete.



This certificate is OK.

IV. Add the chained certificate to EFT Server:

Add the certificate to EFT Server using the procedure in the EFT Server online help article Assigning an SSL certificate.

EFT Server will now have a properly signed SSL certificate working for your EFT Server site.