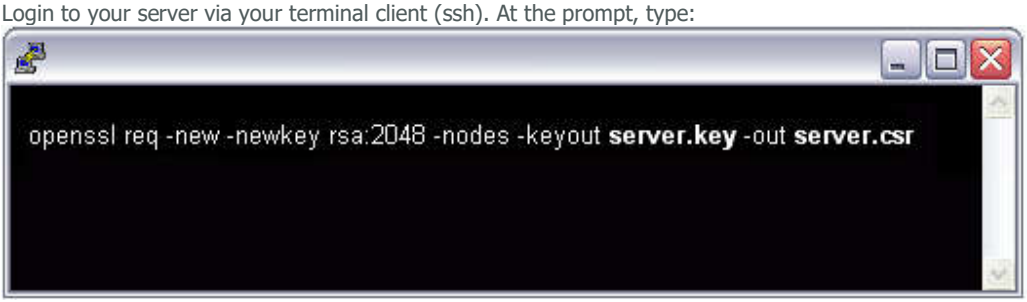
Create CSR and Install Certificates to Cerberus FTP Server

How to generate a CSR by using OpenSSL

1. Login to your server via your terminal client (ssh). At the prompt, type:
2. 

    a. **openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr**
    b. where server is the name of your server.
3. This begins the process of generating two files: the Private-Key file for the decryption of your SSL Certificate, and a certificate signing request (CSR) file (used to apply for your SSL Certificate) with apache openssl.
    a. When you are prompted for the Common Name (domain name), enter the fully qualified domain name for the site you are securing. If you are generating an Apache CSR for a Wildcard SSL Certificate your common name should start with an asterisk (such as *.example.com).
    b. You will then be prompted for your organizational information, beginning with geographic information. There may be default information set already.
    c. This will then create your openssl .csr file.
4. Open the CSR file with a text editor and save it (including the BEGIN and END tags) into text file and submit to us.
5. Save (backup) the generated .key file as it will be required later for Certificate installation.

Cerberus SSL Installation

Once you receive the .zip containing the certificate files, extract the "certs" folder somewhere on your server. We will be combining the files you received in to a .pem format.

With a text editor (such as wordpad), copy and paste the entire body of each certificate into one text file in the following order:

1. The Primary Certificate - your_domain_name.crt
2. The First Intermediate Certificate - IntermediateCA.crt
3. The Second Intermediate Certificate(if a 2nd intermediate cert is supplied) – IntermediateCA2.crt
4. The Root Certificate - TrustedRoot.crt
5. The Private Key - your_domain_name.key

Make sure to include the beginning and end tags on each certificate. The result should look like this:

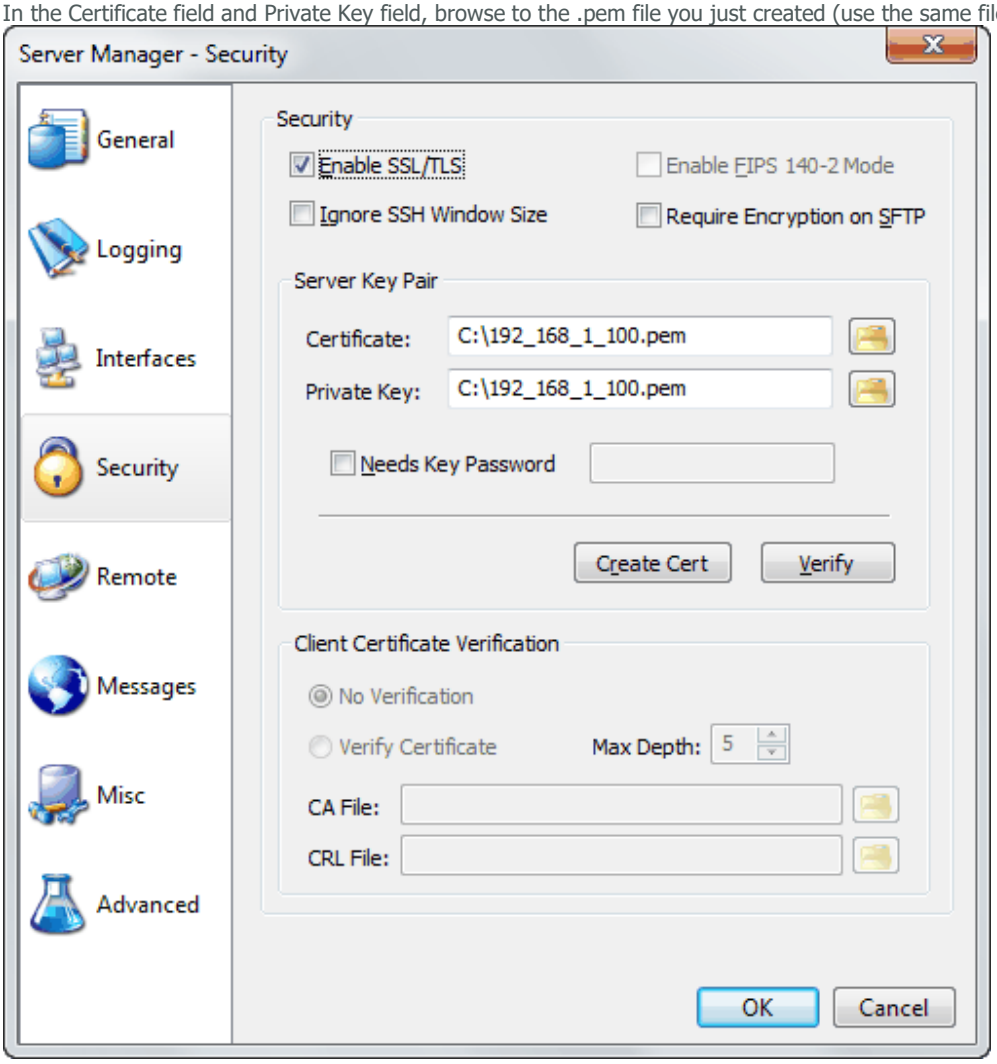
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your First Intermediate certificate: IntermediateCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Second Intermediate certificate (if applicable): IntermediateCA2.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----

Save the combined file as your_domain_name.pem. Your .pem file should be ready for use.

You will now want to open Cerberus Ftp Server and navigate to Configuration, Server Manager, then click on Security in the left column.

If Enable SSL/TLS isn't already checked, then check it now.

In the Certificate field and Private Key field, browse to the .pem file you just created (use the same file for both fields).



The SSL certificate should now be ready for use.