

SSL Certificate Key Issues

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- Mail Express, all versions

SYMPTOM

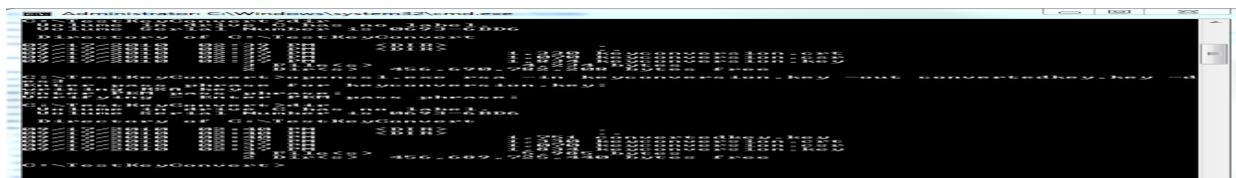
Client uses EFT to generate the CSR and KEY file to obtain a signed SSL Certificate. When attempting to apply the received signed SSL Certificate and the KEY file, the process fails.

RESOLUTION

EFT does not generate the private key in a format recognized by Mail Express. Follow the steps below to use OpenSSL to convert the private key into a format recognized by Mail Express:

1. Acquire OpenSSL by going to <http://www.slproweb.com/products/Win32OpenSSL.html> and downloading the following:
 - a. Win32 - Win32 OpenSSL v1.0.0(x) Light "x" should be the most recent version.
 - b. Win32 - Visual C++ 2008 Redistributables
- OR**
- a. Win64 - Win64 OpenSSL v1.0.0(x) Light "x" should be the most recent version.
 - b. Win64 - Visual C++ 2008 Redistributables (x64)
2. Install the appropriate package from 1.b above.
3. Install the appropriate package from 1.a above.
4. Navigate to the bin subdirectory of the OpenSSL directory (or add it to the Windows Path so it is recognized).
5. Run the following command:

```
openssl.exe rsa -in <path:\PKCS8 Format Encrypted Key Filename> -out <path:\Traditional  
Format Encrypted Key Filename> -des3
```



SSL Certificate Key Issues

/>

NOTE: The command will prompt for the original key's password and a password for the new key. The same password can be used for both.

GlobalSCAPE Knowledge Base

<https://kb.globalscape.com/Knowledgebase/11067/SSL-Certificate-Key-Issues>