Creating a keystore

The information on this page refers to License Statistics v6.14 or newer, which introduced the ability to use the License Statistics Manager to create a keystore. If you are running an older version of License Statistics, see documentation for previous versions.

License Statistics accepts PKCS12 and JKS keystores. If you already have PKCS12 or JKS keystore with a loaded certificate and its key, then you don't need to do anything more.

In this article we describe how to put your certificates into PKCS12 keystore manually. If you are running License Statistics on Windows, you can more easily create a keystore using the License Statistics Manager to guide the process.

To generate a keystore, you will need one of the toolkits for SSL/TLS protocol. You can use any of them; in our examples, we are using openssl [1].

Depending on the format of your certificate, you will need to take different steps. Your certificate format can be identified by its file extension, the most common of which are described below. In every case, you will need two files: one containing certificate, and one containing certificate private key.

- **CER, PEM (.cer, .pem)**

```
openssl pkcs12 -export -out {path_to_created_keystore_file} -in {certificate_file_path} -inkey
{key_file_path} -name {certificate_alias} -noiter -nomaciter
```

Windows example

```
openssl pkcs12 -export -out C:\MyDirectory\keystore.p12 -in C:\MyDirectory\certificate.cer -inkey C:
\MyDirectory\certificate.key -name xflicstat -noiter -nomaciter
```

Linux example

```
openssl pkcs12 -export -out /home/mydirectory/keystore.p12 -in /home/mydirectory/certificate.cer -inkey
/home/mydirectory/certificate.key -name xflicstat -noiter -nomaciter
```

- **DER (.der)**

```
1. Create intermediate .pem file from .der file:
openssl x509 -inform der -in {certificate_file_path} -out {created_pem_file}
2. Create keystore from intermediate .pem file - described in first "CER, PEM (.cer, .pem)" bullet point.
```

Windows example

```
openssl x509 -inform der -in C:\MyDirectory\certificate.der -out C:\MyDirectory\intermediate.pem
```

Linux example

```
openssl x509 -inform der -in /home/mydirectory/certificate.der -out /home/mydirectory/intermediate.pem
```

- **P7B (.p7b)**

```
1. Create intermediate .cer file from .p7b file
openssl pkcs7 -print_certs -in {certificate_file_path} -out {intermediate_cer_file}
2. Create keystore from intermediate .cer file - described in first "CER, PEM (.cer, .pem)" bullet point.
```

Windows example

```
openssl pkcs7 -print_certs -in C:\MyDirectory\certificate.p7b -out C:\MyDirectory\intermediate.cer
```

Linux example

```
openssl pkcs7 -print_certs -in /home/mydirectory/certificate.p7b -out /home/mydirectory/intermediate.cer
```

Remarks:

- In every case, you will be prompted for a password. This password should be put under SSL_KEYSTORE_PASSWORD in the xflicstat.cfg file, or for Windows, under the LDAP configuration section of the License Statistics Manager.
- The {path_to_created_keystore_file} value should be the path that you put under SSL_KEYSTORE key in the xflicstat.cfg file, or for Windows, under the LDAP configuration section of the License Statistics Manager.
- The {certificate_alias} value should be the name that you put under SSL_KEYSTORE_KEY_ALIAS key in the xflicstat.cfg file, or for Windows, under the LDAP configuration section of the License Statistics Manager.
- If you are migrating from v5.x settings, the {certificate_file_path} value is the path to the previously used certificate, defined as SSL_CERTIFICATE_FILE in your old xflicstat.cfg file.
- If you are migrating from v5.x settings, the {key_file_path} value is the path to the previously used certificate key, defined as SSL_CERTIFICATE_KEY_FILE in your old xflicstat.cfg file.
- On Windows, you may get an *"openssl unable to write 'random state'"* error. This error occurs when openssl cannot access the "C:\.rnd" file. You can either gain access to the file or change the value of RANDFILE (the environmental variable that stores the path to the .rnd file). RANDFILE should contain the path to the file that you have access to. If you are using Powershell, the setting can be changed by entering the following:

  ```
  $env:RANDFILE="C:\directory_i_own\.rnd"
  ```

Annotations:

[1] On many Linux distributions, openssl is available by default. On Windows, you will probably need to install openssl. The installer can be compiled from source (git://git.openssl.org/openssl.git) or downloaded from one of the providers (https://wiki.openssl.org/index.php/Binaries).