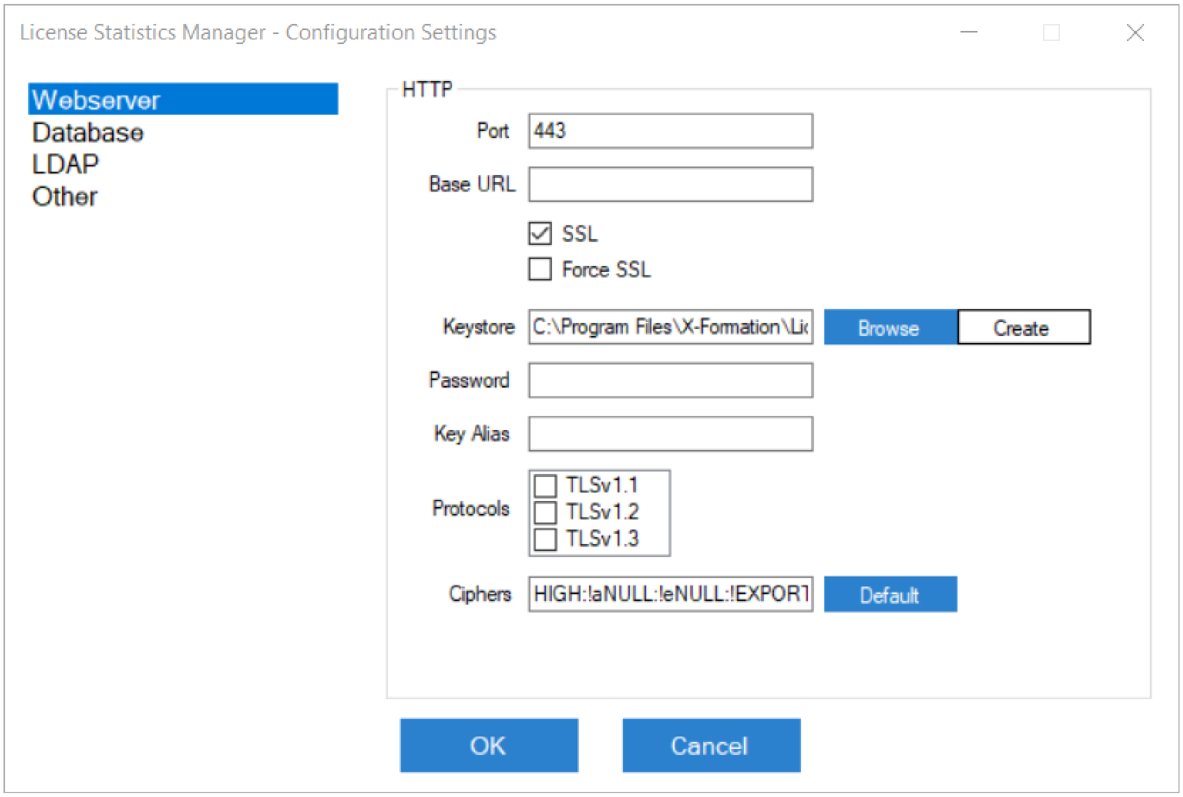
Enabling Tomcat SSL

The information on this page refers to License Statistics v6.6 or newer, which introduced the License Statistics Manager to replace direct editing of the xflicstat.cfg configuration file (Windows only). If you are using an earlier version of License Statistics, please refer to the documentation for releases prior to v6.6.

Windows configuration

In Windows, SSL can be enabled using the webserver settings in the License Statistics Manager. See Using the License Statistics Manager for more information.



License Statistics Manager - Configuration Settings

HTTP

Port: 443

Base URL:

☑ SSL

□ Force SSL

Keystore: C:\Program Files\X-Formation\Lic

Password:

Key Alias:

Protocols: □ TLSv1.1 □ TLSv1.2 □ TLSv1.3

Ciphers: HIGH:!aNULL:!eNULL:!EXPORT

Linux configuration

In Linux, SSL can be enabled using the xflicstat.cfg file. Available settings in the xflicstat.cfg file include the following.

Setting	Default	Description
HTTP_SSL	FALSE	May be set to TRUE or FALSE. To enable SSL, set it to TRUE.
HTTP_SSL_REDIRECT	FALSE	May be set to TRUE or FALSE. Set the value to TRUE to enable automatic redirection from http to https.
SSL_KEYSTORE	*empty*	Path to keystore with loaded certificate and its private key.
SSL_KEYSTORE_PASSWORD	*empty*	Password to keystore.
SSL_KEYSTORE_KEY_ALIAS	xflicstat	Key under which certificate is stored inside keystore.
SSL_PROTOCOLS	TLSv1.1,TLSv1.2,TLSv1.3	Defines which SSL/TLS protocols are enabled.
SSL_CIPHERS	HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!kRSA	List of enabled/disabled ciphers.

Every key should either be commented out or non-empty. Commented-out settings contain the default value.

Example xflicstat.cfg configuration

The configuration example below shows:

- Enabled SSL with automatic redirection from http to https.
- The certificate is stored inside keystore located at *C:\Keystores\keystore.p12* under alias x*flicstat.*
- The only allowed protocol is *TLSv1.2*.
- Only algorithms with long keys (HIGH) with support for authentication (!aNULL) and encryption (!eNULL) are allowed, and some weaker algorithms are blocked (!EXPORT:!DES:!RC4:!MD5:!kRSA).

```
HTTP_SSL = TRUE
HTTP_SSL_REDIRECT = TRUE
SSL_KEYSTORE = C:\Keystores\keystore.p12
SSL_KEYSTORE_PASSWORD = Password123
SSL_KEYSTORE_KEY_ALIAS = xflicstat
SSL_PROTOCOLS = TLSv1.2
SSL_CIPHERS = HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!kRSA
```