# SSL configuration

**What is SSL?**

SSL (Secure Socket Layer) is a protocol of secure communication between a server and client through a network.

**What is TLS?**

TLS (Transport Layer Security) is a newer version of SSL. In practice, the terms "SSL" and "TLS" may be used interchangeably.

**What do I gain from enabling SSL?**

Enabling SSL ensures that data sent from application (e.g., reports about license usage) to application (e.g., login credentials) is encrypted. Enabling SSL also allows the web browser to verify that the connection is secure.

See Enabling LDAP SSL or Enabling Tomcat SSL for configuration details.

**What is keystore?**

Keystore is a file secured with a password that can contain one or many certificates with or without their private keys.

**Which SSL protocols should I enable?**

Generally, enabling the newest SSL protocols is recommended (currently, the newest is TLS v1.3); however, be aware that some older browsers may not support newer protocol versions.

**Which ciphers should I enable/disable?**

The ciphers that are known to be broken should be disabled. The list of valid ciphers changes with time–new ciphers are created, and some old ones become broken. The default ciphers should normally be up to date.

**I have a certificate file and key, how do I create a keystore?**

See Creating a keystore.

**How do I migrate SSL settings from License Statistics v5.x to v6.x?**

In License Statistics v5.x, two files were needed for migrating SSL settings: certificate (defined as SSL_CERTIFICATE_FILE) and certificate private key (defined as SSL_CERTIFICATE_KEY_FILE).

In License Statistics v6.x, both of these files must be placed into a keystore. After generating the keystore, see Enabling Tomcat SSL for configuration details.