Managing HTTPS and SSL on server

On this page:

By default, the Authentication Server runs with HTTPS enabled, using a self-signed certificate that is created by the Teamwork Cloud installer. To change HTTPS settings please edit Authentication Server configuration file *./config/authserver.properties* and change related parameters. After the Authentication Server configuration is updated, the service must be restarted. See the HTTPS/SSL parameters description in the section HTTPS parameters.

Self-signed server certificate

By default, the Authentication Server uses a self-signed certificate that is created by the Teamwork Cloud installer. This means that web browsers will warn users about an untrusted server certificate when they first access the Authentication Server. When users choose to trust the server certificate, the warning message disappears.

CA-signed server certificate

For production environments, it is highly recommended to use a certificate signed by trusted certificate authorities (CA). The following steps should be done to generate a keystore file providing that you already have a private key and certificate signed by a trusted CA.

When executing the **OpenSSL** command you will be asked for a keystore password. Please read the instructions carefully and provide all the required information.

To generate a keystore file

1. Create a PKCS 12 file with the OpenSSL tool.

   ```
   openssl pkcs12 -export -in server.crt -inkey server.key -certfile server.crt -out keystore.p12
   ```

2. Copy the file **keystore.p12** to the *./config* directory of Teamwork Cloud.

Note for Windows users

- You can download OpenSSL binaries for Windows operating system from http://gnuwin32.sourceforge.net/packages/openssl.htm.
- All commands should be run with administrator rights in the directory where the OpenSSL executable resides.

Deployment on cluster

If the Authentication Server is deployed on a cluster, all service instances should use the same keystore. When using an automatically created keystore with a self-signed certificate, just copy the keystore file from one instance to all the other ones.

Related pages

- HTTPS parameters