Changing the SSL certificate

On this page:

By default, Teamwork Cloud and WebApp use a self-signed certificate generated during installation. However, for production environments, it is strongly recommended that you use a certificate signed by a trusted Certificate Authority (CA). Follow the steps outlined on this page to replace the self-signed certificate with a CA certificate and Java keystore, provided that you either have a private key and certificate signed by a trusted CA, or a PFX file containing the private key and signed certificate.

Changing the self-signed certificate to a CA certificate

If you have a .pfx file containing both the private key and signed certificate, use the following steps to extract the key and certificate into separate files first. PFX is a PKCS#12 certificate archive file. This procedure uses the OpenSSL command line tool.

To process PFX certificate files

---

1. Extract the private key to key.pem file.

   ```
   openssl pkcs12 -in <certname.pfx> -nocerts -out key.pem -nodes
   ```

2. If there is a passphrase associated with the private key, remove the passphrase and generate a new private key file *server.key*

   ```
   openssl rsa -in key.pem -out server.key
   ```

3. Extract the certificate to *teamworkcloud.crt*

   ```
   openssl pkcs12 -in <certname.pfx> -nokeys -out teamworkcloud.crt
   ```

   The .pfx file has now been converted to a private key file and a public certificate file. You can now proceed to use these two files to generate the keystore file required by Teamwork Cloud components.

The new certificate will have to be converted to a Java keystore for Teamwork Cloud components. Use the following procedure to update the keystore file with your new certificate and private key files.

To change the self-signed certificate using the keystore file

---

1. Locate the default keystore file at <*install_root*>*configuration**keystore.p12*.
2. Update the keystore file with the new private/public key:

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

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

   ⚠ In the example above, *teamworkcloud* is a sample alias. If you use a different alias, remember to update it in the <*install_root*>*WebAppPlatform**shared**conf**authserver.properties* file.

   b. Copy the **keystore.p12** file to the <*install_root*>*configuration* directory, replacing the default file with the new one.
3. Add the public certificate file to the <*install_root*>*configuration* directory.

> ⚠ The public certificate file, or .crt, is the public key from the private/public (.key/.crt) key pair.

4. (Recommended) Secure .key and .p12 files with a password. Make sure to keep the .key file in a safe place.
5. If you need to switch from IP to FQDN, see how to change server or service address.

If the default configuration (file names, locations, passwords, aliases, etc.) is not changed, no additional steps are necessary. However, if you are changing the default configuration, then you also need to update the relevant properties in the corresponding files, as described below.

> ⚠ **Note for Windows users**
>
> - You can download OpenSSL binaries for Windows operating systems from http://gnuwin32.sourceforge.net/packages/openssl.htm.
> - All commands should be run with administrator rights in the directory containing the OpenSSL executable file.

Updating Teamwork Cloud configuration

Update the default values for the properties indicated below in the *<install_root>\configuration\application.conf* file if any of the applicable values were changed.

application.conf

```
https {
        # the file name of the certificate or the key store (should be a full path)
        file = "configuration/teamworkcloud.crt"
}
```

> ⚠ You can customize both the name and the path of the teamworkcloud.crt file. However, we recommend using the default file name and path. If necessary, change them after confirming that the initial installation is successful.

application.conf

```
ssl {
                keystorePath = "configuration/keystore.p12"
                keystoreType = "pkcs12"
                keystorePassword = "nomagic"
                keyPassword = "nomagic"
}
```

application.conf

```
cassandra {
                enabled = false
                keystorePath = "configuration/keystore.p12"
                keystoreType = "pkcs12"
                keystorePassword = "nomagic"
                truststorePath = "configuration/keystore.p12"
                truststoreType = "pkcs12"
                truststorePassword = "nomagic"
}
```

Updating AuthServer configuration

Update the default values for the properties indicated below in the *<install_root>\WebAppPlatform\shared\conf\authserver.properties* file if any of the applicable values were changed.

authserver.properties

```
authentication.server.key-store=../configuration/keystore.p12
authentication.server.key-store-type=PKCS12
authentication.server.key-store-password=nomagic
authentication.server.key-password=nomagic
authentication.server.key-alias=teamworkcloud
```

Updating Web Application platform configuration

Update the default values for the properties indicated below in the *<install_root>\WebAppPlatform\conf\server.xml* file if any of the applicable values were changed.

server.xml

```
<Certificate    certificateKeystoreFile="../configuration/keystore.p12"
                                certificateKeystorePassword="nomagic"
                                type="RSA"
/>
```

Both services (Teamwork Cloud and Webapp) must be restarted once all of the configuration changes are completed.

Useful OpenSSL Commands

To check a private key:

```
openssl rsa -in <private_key_file> -check
```

To check a signed certificate:

```
openssl x509 -in <certificate.crt> -text -noout
```

To check a PKCS#12 file (.pfx or .p12):

```
openssl pkcs12 -info -in keystore.p12
```

Related pages

- Managing HTTPS and SSL on server
- Enabling secure connection between client and server