

Creating a keystore with a signed certificate


In several locations within Servoy a keystore with a signed SSL Certificate is used:

- For enabling HTTPS access to all web pages hosted by the Servoy Application Server, including the Servoy Web Clients
- For enabling SSL encryption of the traffic between the Servoy Application Server and the Servoy Smart Clients
- For (re)signing all libraries of Servoy and additional plugins & beans that get downloaded to the Smart Client

In all three scenario's a keystore is required containing a signed certificate. While a keystore with a [self signed certificate](#) can be easily created, in order to achieve proper security, a certificate signed by a trusted third part [Certificate Authority](#) (CA) is required. Self signed certificates will not be recognized as secure by browsers or Java WebStart and thus will raise warnings to the end user.

The process of creating a keystore with a signed certificate by a trusted third part Certificate authority consists of 2 steps:

1. [Creating a keystore with a self signed certificate](#)
2. Getting the self signed certificate authenticated/signed by a Certificate Authority and importing the updated certificate back into the keystore (see [Authorize a self signed certificate by a trusted 3rd party Certificate Authority](#))

 It is important to note that for signing libraries a Code Signing certificate is required from the CA, while for HTTPS/SSL support a SSL certificate is needed

Once the keystore is ready, it can be used to configure HTTPS, SSL or (re)sign all libraries.

Enabling HTTPS

With HTTPS enabled, all web pages served by the Servoy Application Server will be send over the network encrypted, so what gets send over the network cannot be read by third parties. It's advised to run Web Clients over HTTPS in production environment, as most likely there will be private data being send back and forth between the Servoy Application Server and the Web clients, for example login credentials.

For more information on how to enable HTTPS see [Network related settings](#) .

Enabling SSL

Smart Clients communicate with the Servoy Application Server over the network and depending on where the client is located, this could also means the internet. By enabled SSL on teh Servoy Application Server, all traffic between the Smart clients and the Servoy Application Server is encrypted.

For more information on how to enable SSL see [Network related settings](#) .

Signing libraries

Java WebStart requires all libraries that are downloaded to be signed using a Code signing Certificate. This does not mean that all libraries need to be signed using the same certificate, however, the first time Java WebStart downloads a library that is signed with a certificate that it doesn't already know, it will present the user with a dialog and asks the user if he/she trusts the vendor to which the certificate is issued.

Out of the box all libraries, plugins, beans and Look and Feels that come with Servoy are properly signed by Servoy. Any additional plugins and beans that are added to the environment also need to be signed. Most 3rd party plugin & bean vendors already take care of this.

However, this means that the user will be presented at first launch with a dialog for each certificate/vendor. This can be prevented by resigning all libraries using the same certificate.

For more information on resigning, see the [SignTester tool](#) or the new [code-signer](#) on [ServoyForge](#).