**Configure Tomcat to support SSL or https**

# Introduction

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are technologies which allow web browsers and web servers to communicate over a secured connection. This means that the data being sent is encrypted by one side, transmitted, then decrypted by the other side before processing. This is a two-way process, meaning that both the server AND the browser encrypt all traffic before sending out data.

Another important aspect of the SSL/TLS protocol is Authentication. This means that during your initial attempt to communicate with a web server over a secure connection, that server will present your web browser with a set of credentials, in the form of a "Certificate", as proof the site is who and what it claims to be. In certain cases, the server may also request a Certificate from your web browser, asking for proof that you are who you claim to be. This is known as "Client Authentication," although in practice this is used more for business-to-business (B2B) transactions than with individual users. Most SSL-enabled web servers do not request Client Authentication.

# Certificates

In order to implement SSL, a web server must have an associated Certificate for each external interface (IP address) that accepts secure connections. The theory behind this design is that a server should provide some kind of reasonable assurance that its owner is who you think it is, particularly before receiving any sensitive information. While a broader explanation of Certificates is beyond the scope of this document, think of a Certificate as a "digital passport" for an Internet address. It states which organization the site is associated with, along with some basic contact information about the site owner or administrator.

This certificate is cryptographically signed by its owner, and is therefore extremely difficult for anyone else to forge. For the certificate to work in the visitors browsers without warnings, it needs to be signed by a trusted third party. These are called Certificate Authorities (CAs). To obtain a signed certificate, you need to choose a CA (Ex: VerySign) and follow the instructions your chosen CA provides to obtain your certificate. A range of CAs is available including some that offer certificates at no cost.

# Enable https on GTAS

1).Obtain a signed certificate from Certificate Authorities. Store it in a folder on your server.

2).Go to Tomcat server Installation directory and add/modify the server.xml file with the below.

========================================================================

**<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"**

**maxThreads="150" SSLEnabled="true" scheme="https" secure="true"**

**clientAuth="false" sslProtocol="TLS" keystoreFile="FILE PATH TO OUR SAVED KEY" keystorePass="password for your key"/>**

KeystoreFile is the file path of your stored certificate key.

keystorePass is the password for your key.

Once you modified the server.xml with the above you can restart your server and your server is ready to accept and deliver content using https.