
How to secure RESTful API (using Tomcat) with https

- **Product:** Aleph
 - **Product Version:** 22, 23
 - **Relevant for Installation Type:** Multi-Tenant Direct, Dedicated-Direct, Local, TotalCare
-

Question

What are the steps to secure RESTful API (using Tomcat) and switch it to https:// ?

Answer

The general description and instructions how to secure Tomcat are available at <https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html>

Basic steps to be executed on Aleph server are following:

1. create a keystore file to store the server's private key and self-signed certificate

```
$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA
```

The keystore password will be used in the next step in the Tomcat configuration, see "your_password" below.

2. uncomment the "SSL HTTP/1.1 Connector" entry in the template file \$aleph_dev/ng/aleph/home/profile/overwrites/thirdparty/tomcat/conf/server.xml.tmpl and modify accordingly:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"  
maxThreads="150" scheme="https" secure="true"  
clientAuth="false" sslProtocol="TLS" keystorePass="your_password" />
```

3. execute the script \$aleph_dev/ng/aleph/home/system/bin/set_globals.sh:

```
jbin  
./set_globals.sh
```

4. when received BUILD SUCCESSFUL, restart Tomcat by executing util W-3-7-9 (it will take some seconds to be accomplished)

5. check that Tomcat is running using:

```
curl -k "https://localhost:8443/rest-dlf/record"
```

When RESTful API should be available ONLY through https, you can block http port on your firewall or you can add a following parameter to \$alephe_root/jboss_conf/main.properties:

```
api.rest.https=Y
```

Standard http requests will then be answered with HTTP 401 error - "This request requires HTTP authentication."

- **Article last edited:** 07-Jun-2017