Article - CS272670

ThingWorx Java SDK - SSL Certificate Configuration Overview

Modified: 20-Oct-2017

Applies To

- ThingWorx Edge SDK 6.0

Description

- How to set-up SSL using certificates in the Java SDK
- Import certs into JRE for use by Java edge application

Resolution

1. Create a certificate on the Platform and enable SSL in Tomcat (see KCS Article CS231610 (https://www.ptc.com/en/support/article?n=CS231610))
    - This can be done in many ways, and there is no official PTC recommendation on how to do this
    - A tutorial using self-signed certificates can be found on our Developer Community (https://community.thingworx.com/community/developers/blog/2017/05/09/thingberry-secure-connections-with-tls?&art_lang=en&posno=1&q=openssl&DocumentType=Community%20Blog&ProductFamily=ThingWorx%7CNRN%7CAxeda&source=search)
        - (https://community.thingworx.com/community/developers/blog/2017/05/09/thingberry-secure-connections-with-tls?&art_lang=en&posno=1&q=openssl&DocumentType=Community%20Blog&ProductFamily=ThingWorx%7CNRN%7CAxeda&source=search)This is just a reference guide
        - This is not meant to be used exactly as it is in Production
2. Copy the server certificate for ThingWorx to the edge device
    - **Steps 2-3 are only required if the CA (certificate authority) on a trust chain is not present in this file already (such as if self-signed certs are in use)**
    - **If a common CA is in use, please skip to step 4**
    - This is the lowest level certificate in the chain of trust, often called *server.crt* or *server.key*
    - Where it goes on the edge device isn't too important
    - The password for this certificate **MUST MATCH** the password for the keystore which stores it, or Tomcat will not be able to access the cert within the keystore, even if it can access the keystore
3. Import the server certificate into the ***cacerts*** keystore of the JRE used to run the Java SDK on the Edge device
    - **If a common CA is in use, please skip to step 4**
    - The exact folder where this file is located is ***JAVA_HOME\lib\security***
    - The **default password** for the *cacerts* file is "**changeit**"
    - The command used to do this import looks like:

        ```
        keytool -importcert -keystore cacerts -file C:\location\of\cert\file.crt
        ```

    - The output should look like:

        ```
        C:\Program Files\Java\jre1.8.0_121\lib\security>keytool -importcert -keystore cacerts -file C:\OpenSSL-Win64
        Enter keystore password:
        keytool error: java.io.IOException: Keystore was tampered with, or password was incorrect

        C:\Program Files\Java\jre1.8.0_121\lib\security>keytool -importcert -keystore cacerts -file C:\OpenSSL-Win64
        Enter keystore password:
        Owner: EMAILADDRESS=vtielebein@ptc.com, CN=tori.thingworx.com, OU=TS, O=PTC, L=Exton, ST=PA, C=US
        Issuer: EMAILADDRESS=vtielebein@ptc.com, CN=Tori Intermediate CA, OU=TS, O=PTC, L=Exton, ST=PA, C=US
        Serial number: 82e62479592415bd
        Valid from: Fri Oct 20 10:27:32 EDT 2017 until: Fri Dec 06 09:27:32 EST 2019
        Certificate fingerprints:
                 MD5:  2D:1D:9A:AE:03:A7:B5:5E:F9:49:65:DE:88:74:A1:26
                 SHA1: 0A:C5:F8:DB:AA:C6:3F:64:49:6A:A7:DF:50:B9:2F:6A:8E:05:75:31
                 SHA256: 58:B0:BD:43:21:7A:77:BA:36:61:65:1F:C5:B5:6F:2E:16:E5:9A:C2:FE:A7:96:6D:9D:6B:8C:20:6C:72:0
                 Signature algorithm name: SHA256withRSA
                 Version: 1
        Trust this certificate? [no]:  yes
        Certificate was added to keystore

        C:\Program Files\Java\jre1.8.0_121\lib\security>
        ```

4. Copy the keystore file to any folder on the edge device
    - Ensure the process running the Java SDK has the **necessary permissions to read** this file
    - This file will is often named like ***keystore.jks*** or *mySpecificKeystore.jks*
    - This must be generated on the server where **Tomcat is hosted** (see step 1)
5. Within the Java SDK code, wherever the client is configured (so before the "client.start()" call), put the following code:

```
System.setProperty("javax.net.ssl.trustStore", "C:\\path\\to\\keystore\\keystore.jks");
System.setProperty("javax.net.ssl.trustStorePassword", "password_of_keystore");
```

- Ensure there is **NO** call to **ClientConfigurator.ignoreSSLErrors(true);**
  - This will prevent the SDK from checking certificates, even if SSL ports are used and SSL is configured on the Platform
  - If self-signed certs are used and are not added to the *cacerts* file, then this service must be called for the SDK to connect
  - PTC definitely does **NOT** recommend using this method in any edge device destined for a **production environment**
- For additional reading and **debugging** of certificates within the Java SDK, see the Edge Help Center (http://support.ptc.com/help/thingworx_hc/thingworx_edge_sdks_ems/#page/thingworx_edge_sdks_ems%2Fjavasdk_topics%2Fc_javasdk_security_setup_c