USING PRIVATE SIGNED CERTIFICATES WITH IDASH

CA WORKLOAD AUTOMATION

This document describes how to use private (internally signed) certificates with iDash. Commercial Certificate Authorities (CA) like Verisign and Comodo no longer issue signed certificates for internal networks. Therefore a prerequisite to using this procedure is to have an internal CA setup. Clients (e.g. web browsers) should have the root and any intermediate certificates imported into their certificate store.

CA Workload Automation iDash installs by default without SSL enabled. To enable SSL for iDash follow these steps:

Steps to enable SSL for iDash

1. Login to the iDash host as the iDash software owner
2. Set the Java environment (default iDash directory: /opt/CA/idash)

```
export JAVA_HOME=/opt/CA/idash/jre
export PATH=$JAVA_HOME/bin:$PATH
```

3. Prepare the Certificate Keystore

```
keytool -genkey -alias tomcat -keyalg RSA -keysize 2048 \
-keystore /opt/CA/idash/tomcat8/conf/.keystore \
-storepass changeit -keypass changeit -validity <days>
```

where:

<days> expiration period of the certificate in days (e.g. 5475 = 15 years)

IMPORTANT: Enter the hostname or domain (i.e. myidashserver.mycompany.com) in the field "first and last name"

4. Change to the Tomcat configuration directory (default: /opt/CA/idash/tomcat8/conf

Backup the Tomcat configuration file

```
cp server.xml server.xml.bak
```

5. Configure the Connector in the Tomcat configuration file (server.xml). To configure the connector remove the comments (<!—and -->)

```
<!--

<Connector port=”8443”
protocol=”org.apache.coyote.http11.Http11NioProtocol” maxThreads=”150”
SSLEnabled=”true” scheme=”https” secure=”true” clientAuth=”false”
sslProtocol=”TLS” />

-->
```

6. Edit the Connector element to add the keystore

```
<!--

<Connector port=”8443”
protocol=”org.apache.coyote.http11.Http11NioProtocol” maxThreads=”150”
SSLEnabled=”true” scheme=”https” secure=”true”
keystoreFile=”/opt/CA/idash/tomcat8/conf/.keystore”
keystorePAss=”changeit” clientAuth=”false” sslProtocol=”TLS” />

-->
```

7. Change to the Tomcat bin directory (default: /opt/CA/idash/tomcat8/bin)

   Restart iDash Tomcat Application Server

```
./idash_server stop

./idash_server start
```

Steps to use private signed certificates

1. Login to the iDash host as the iDash software owner
2. Change directory to the keystore location specified in step 3 of Steps to enable SSL for iDash

   Create the certificate signing request (CSR)

   ```
   keytool -certreq -alias tomcat -keyalg RSA -keystore .keystore \
   -storepass changeit -file idash.cert.req.csr
   ```

3. Have the certificate request signed by your internal CA

   They will need to return the following:

   a. root certificate
   b. any/all intermediate certificate(s)
   c. the private (signed) certificate generated from the CSR

4. Import the root certificate. Enter 'yes' to trust the certificate

   ```
   keytool -importcert -alias RootCA -file ca.cert.pem \
   -keystore .keystore -storepass changeit
   ```

5. (Optional) Import any/all intermediate certificate(s)

   ```
   keytool -importcert -alias IntermediateCA -file intermediate.cert.pem \
   -keystore .keystore -storepass changeit
   ```

6. Import the private (signed) certificate

   ```
   keytool -importcert -trustcacerts -file idash.cert.pem -alias tomcat \
   -keystore .keystore -storepass changeit
   ```

7. Change to the Tomcat bin directory (default: /opt/CA/idash/tomcat8/bin)

   Restart iDash Tomcat Application Server

   ```
   ./idash_server stop

   ./idash_server start
   ```

IMPORTANT: Ensure that the root certificate and any intermediate certificates are imported into client (e.g. web browsers) certificate stores.