OMS Certificate installation In WAS Console and Agents.

Please Use below steps for OMS Certificate installation.

OMS Server List

g1t4184.austin.hp.com	PRODUCTION	Sterling App 1
g1t4185.austin.hp.com	PRODUCTION	Sterling App 2
g2t3065.austin.hp.com	PRODUCTION	Sterling App 3
g2t3066.austin.hp.com	PRODUCTION	Sterling App 4
g1t4182.austin.hp.com	PRODUCTION	Sterling Agents 1
g1t4183.austin.hp.com	PRODUCTION	Sterling Agents 2
g2t3063.austin.hp.com	PRODUCTION	Sterling Agents 3
g2t3064.austin.hp.com	PRODUCTION	Sterling Agents 4
g1t1477g.austin.hp.com	PRODUCTION	Sterling HTTP 1
g1t1956g.austin.hp.com	PRODUCTION	Sterling HTTP 2
g2t2648g.austin.hp.com	PRODUCTION	Sterling HTTP 3
g2t2650g.austin.hp.com	PRODUCTION	Sterling HTTP 4

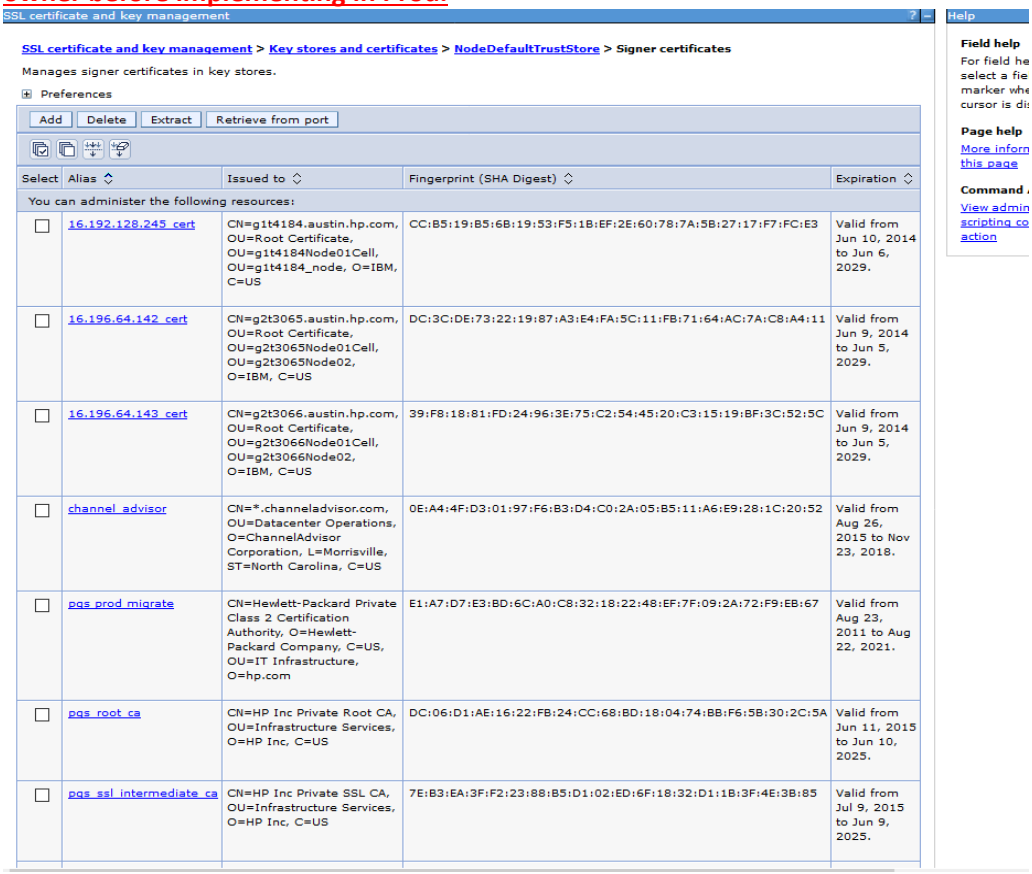
Steps to Add the certificate in WAS Below links.

Log in to WAS -> SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates
Add certificate and Sync with nodes .

https://g1t4184.austin.hp.com:9045/ibm/console
https://g1t4185.austin.hp.com:9043/ibm/console
https://g2t3065.austin.hp.com:9043/ibm/console
https://g2t3066.austin.hp.com:9043/ibm/console

PFS

Note:-- Signer certificate and personal certificate(Trust/Key) needs to be clarified with User story owner before implementing in Prod.



Restart the server in backend.

Then Implement the same in agent servers too.

Please follow below step's for all agent servers:

1. Keep the backup of certificate in /tmp/ location with all user permissions to file and that location needs to be given in keytool command.

2. Take backup of **cacerts** in oms agent server in below location.

/opt/apps/IBM/Sterling93/jdk/jre/lib/security/

```
-rwxr-xr-x 1 wcsuser wcsgroup  82K Jan  5 14:46 cacerts
[wcsuser@g1t4182 security]$ pwd
/opt/apps/IBM/Sterling93/jdk/jre/lib/security
[wcsuser@g1t4182 security]$
```

3. Go to **/opt/apps/IBM/Sterling93/jdk/jre/bin** and execute below command

keytool -import -alias hpca2016 -keystore /opt/apps/IBM/Sterling93/jdk/jre/lib/security/cacerts -trustcacerts -file /tmp/HP_Inc_Private_Root_CA.cer -storepass changeit

Give "**yes**" while asking confirmation then certificate will be added

4.Again execute below command to get message like *Certificate already exists*

keytool -import -alias hpca2017 -keystore /opt/apps/IBM/Sterling93/jdk/jre/lib/security/cacerts -trustcacerts -file /tmp/HP_Inc_Private_SSL_CA.509.pem -storepass changeit.

5.Check datestamp for update happened in cacerts file in all agent servers.

**********On Request Only **********

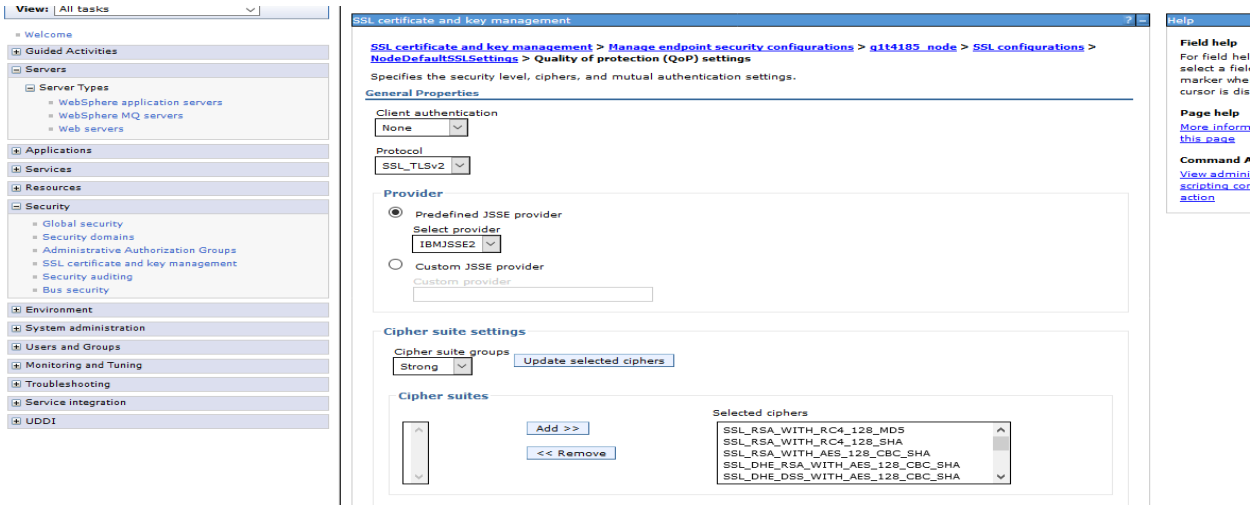
If SSL handshake is experienced between agent server and application server , we will do this below request.

For SSL Change On Request only by client HP .
Email Attached

SSL protocol change in OMS.msg

Step -1 – Change Protocol in Application servers, Follow below steps.

SSL certificate and key management > Manage endpoint security configurations > g1t4185_node > SSL configurations > NodeDefaultSSLSettings > Quality of protection (QoP) settings



Step 2 . Change Protocol in Application server, before take backup of **ssl.client.props**

ssl.client.props : change com.ibm.ssl.protocol from SSL_TLS to SSL_TLSv2

```
-rw-rw-r-- 1 wcsuser wcsgroup 5.0K Jan  5 16:26 ssl.client.props
[wcsuser@g1t4184 properties]$ pwd
/opt/apps/IBM/WebSphere/AppServer/profiles/somcustom/properties
[wcsuser@g1t4184 properties]$
```

Step 3 : Change in Agent Server too and backup before doing it.

Add this property in **-Dhttps.protocols=SSL_TLSv2** in file **/opt/apps/IBM/Sterling93/bin/agentserver.sh**

PFS

AGENT_JAVA_OPTS="-Dvendor=shell -Xverbosegclog:/opt/apps/IBM/Sterling93/logs/agents/$1_$$_gc.log -verbose:gc -DvendorFile=/opt/apps/IBM/Sterling93/properties/servers.properties -DCACHE_PS=true -DDISABLE_DS_EXTENSIONS=Y -Duser.timezone=UTC -Dhttps.proxyHost=web-proxy.austin.hpicorp.net -Dhttps.proxyPort=8080 -Dhttps.protocols=SSL_TLSv2"

```
      AGENT_JAVA_OPTS="-Dvendor=shell -Xverbosegclog:/opt/apps/IBM/Sterling93/logs/agents/$1_$$_gc.log -verbose:gc -DvendorFile=/opt/apps/IBM/Sterling93/pr
operties/servers.properties -DCACHE_PS=true -DDISABLE_DS_EXTENSIONS=Y -Duser.timezone=UTC -Dhttps.proxyHost=web-proxy.austin.hpicorp.net  -Dhttps.proxyPort=8
080 -Dhttps.protocols=SSL_TLSv2"
export AGENT_JAVA_OPTS

# The first parameter is the server name
set -x
   ${AGENT_JAVA_SERVER} -classpath /opt/apps/IBM/Sterling93/jar/bootstrapper.jar ${AGENT_JAVA_OPTS} com.sterlingcommerce.woodstock.noapp.NoAppLoader -class c
om.yantra.integration.adapter.IntegrationAdapter -f /opt/apps/IBM/Sterling93/properties/AGENTDynamicclasspath.cfg -invokeargs "$@"
set +x
~
```

==========END==========