

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.

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates

Manages signer certificates in key stores.

Preferences

Add Delete Extract Retrieve from port

Select	Alias	Issued to	Fingerprint (SHA Digest)	Expiration
<input type="checkbox"/>	16.192.128.245_cert	CN=g1t4184.austin.hp.com, OU=Root Certificate, OU=g1t4184Node01Cell, OU=g1t4184_node, O=IBM, C=US	CC:B5:19:B5:6B:19:53:F5:1B:EF:2E:60:78:7A:5B:27:17:F7:FC:E3	Valid from Jun 10, 2014 to Jun 6, 2029.
<input type="checkbox"/>	16.196.64.142_cert	CN=g2t3065.austin.hp.com, OU=Root Certificate, OU=g2t3065Node01Cell, OU=g2t3065Node02, O=IBM, C=US	DC:3C:DE:73:22:19:87:A3:E4:FA:5C:11:FB:71:64:AC:7A:C8:A4:11	Valid from Jun 9, 2014 to Jun 5, 2029.
<input type="checkbox"/>	16.196.64.143_cert	CN=g2t3066.austin.hp.com, OU=Root Certificate, OU=g2t3066Node01Cell, OU=g2t3066Node02, O=IBM, C=US	39:F8:18:81:FD:24:96:3E:75:C2:54:45:20:C3:15:19:BF:3C:52:5C	Valid from Jun 9, 2014 to Jun 5, 2029.
<input type="checkbox"/>	channel_advisor	CN=*.channeladvisor.com, OU=Datacenter Operations, O=ChannelAdvisor Corporation, L=Morrisville, ST=North Carolina, C=US	0E:A4:4F:D3:01:97:F6:B3:D4:C0:2A:05:B5:11:A6:E9:28:1C:20:52	Valid from Aug 26, 2015 to Nov 23, 2018.
<input type="checkbox"/>	pqs_prod_migrate	CN=Hewlett-Packard Private Class 2 Certification Authority, O=Hewlett-Packard Company, C=US, OU=IT Infrastructure, O=hp.com	E1:A7:D7:E3:BD:6C:A0:C8:32:18:22:48:EF:7F:09:2A:72:F9:EB:67	Valid from Aug 23, 2011 to Aug 22, 2021.
<input type="checkbox"/>	pqs_root_ca	CN=HP Inc Private Root CA, OU=Infrastructure Services, O=HP Inc, C=US	DC:06:D1:AE:16:22:FB:24:CC:68:BD:18:04:74:BB:F6:5B:30:2C:5A	Valid from Jun 11, 2015 to Jun 10, 2025.
<input type="checkbox"/>	pqs_ssl_intermediate_ca	CN=HP Inc Private SSL CA, OU=Infrastructure Services, O=HP Inc, C=US	7E:B3:EA:3F:F2:23:88:B5:D1:02:ED:6F:18:32:D1:1B:3F:4E:3B:85	Valid from Jul 9, 2015 to Jun 9, 2025.

Field help
For field help select a field marker where cursor is displayed.

Page help
[More information](#)
[View admin scripting console](#)

Command .
[View admin scripting console](#)

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/

```
-rw-r--r-- 1 wcsuser wcsuser 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

View: All tasks

SSL certificate and key management

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

Specifies the security level, ciphers, and mutual authentication settings.

General Properties

Client authentication: None

Protocol: SSL_TLSv2

Provider: Predefined JSSE provider (IBMJSSE2)

Cipher suite settings

Cipher suite groups: Strong

Cipher suites: SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, SSL_RSA_WITH_AES_128_CBC_SHA, SSL_DHE_RSA_WITH_AES_128_CBC_SHA, SSL_DHE_DSS_WITH_AES_128_CBC_SHA

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@gl1t4184 properties]$ pwd
/opt/apps/IBM/WebSphere/AppServer/profiles/somcustom/properties
[wcsuser@gl1t4184 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.hpibcorp.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.hpibcorp.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=====