

TLsv1.2 Changes

IBM console changes:

[SSL certificate and key management](#) > [SSL configurations](#) > [CellDefaultSSLSettings](#) > **Quality of protection (QoP) settings**

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

General Properties

Client authentication

None ▼

Protocol

TLsv1.2 ▼

Provider

☒ Predefined JSSE provider

Select provider

IBMJSSE2 ▼

☐ Custom JSSE provider

Custom provider

Cipher suite settings

Cipher suite groups

Strong ▼

Update selected ciphers

Cipher suites



Add >>

<< Remove

Selected ciphers

SSL_RSA_WITH_AES_128_CBC_SHA256
SSL_DHE_RSA_WITH_AES_128_CBC_SHA256
SSL_DHE_DSS_WITH_AES_128_CBC_SHA256
SSL_RSA_WITH_AES_128_CBC_SHA
SSL_DHE_RSA_WITH_AES_128_CBC_SHA

[SSL certificate and key management](#) > [SSL configurations](#) > [NodeDefaultSSLSettings](#) > Quality of protection (QoP) settings

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

General Properties

Client authentication

None ▼

Protocol

TLSv1.2 ▼

Provider



Predefined JSSE provider

Select provider

IBMJSE2 ▼



Custom JSSE provider

Custom provider

Cipher suite settings

Cipher suite groups

Strong ▼

Update selected ciphers

Cipher suites



Add >>

<< Remove

Selected ciphers

SSL_RSA_WITH_AES_128_CBC_SHA256
SSL_DHE_RSA_WITH_AES_128_CBC_SHA256
SSL_DHE_DSS_WITH_AES_128_CBC_SHA256
SSL_RSA_WITH_AES_128_CBC_SHA
SSL_DHE_RSA_WITH_AES_128_CBC_SHA

[SSL certificate and key management](#) > [SSL configurations](#) > [XDADefaultSSLSettings](#) > Quality of protection (QoP) settings

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

General Properties

Client authentication

Required ▼

Protocol

TLSv1.2 ▼

Provider

☒ Predefined JSSE provider

Select provider

IBMJSSE2 ▼

☐ Custom JSSE provider

Custom provider

Cipher suite settings

Cipher suite groups

Strong ▼

Update selected ciphers

Cipher suites



Add >>

<< Remove

Selected ciphers

SSL_RSA_WITH_AES_128_CBC_SHA256
SSL_DHE_RSA_WITH_AES_128_CBC_SHA256
SSL_DHE_DSS_WITH_AES_128_CBC_SHA256
SSL_RSA_WITH_AES_128_CBC_SHA
SSL_DHE_RSA_WITH_AES_128_CBC_SHA

Apply → ok

Appserver settings:

/opt/apps/IBM/WebSphere/AppServer/profiles/Dmgr01/properties

```
[wcsuser@g9t3902 test]$ cd /opt/apps/IBM/WebSphere/AppServer/profiles/Dmgr01/properties/  
[wcsuser@g9t3902 properties]$
```

```
[wcsuser@g9t3902 properties]$ vi ssl.client.props
```

```
#-----  
com.ibm.ssl.alias=DefaultSSLSettings  
com.ibm.ssl.protocol=TLSv1.2  
com.ibm.ssl.securityLevel=HIGH  
com.ibm.ssl.trustManager=IbmPKIX  
com.ibm.ssl.keyManager=IbmX509  
com.ibm.ssl.contextProvider=IBMJSSE2  
com.ibm.ssl.enableSignerExchangePrompt=gui
```

/opt/apps/IBM/WebSphere/AppServer/profiles/ETRLIVE/properties

```
[wcsuser@g9t3902 properties]$ pwd
/opt/apps/IBM/WebSphere/AppServer/profiles/ETRLIVE/properties
[wcsuser@g9t3902 properties]$ vi ssl.client.props
```

```
com.ibm.ssl.alias=DefaultSSLSettings
com.ibm.ssl.protocol=TLSv1.2
com.ibm.ssl.securityLevel=HIGH
com.ibm.ssl.trustManager=IbmPKIX
com.ibm.ssl.keyManager=IbmX509
com.ibm.ssl.contextProvider=IBMJSSE2
com.ibm.ssl.enableSignerExchangePrompt=gui
```

Solr Appserver settings:

/opt/apps/IBM/WebSphere/AppServer/profiles/ETRLIVE_solr/properties

```
[wcsuser@g9t3901 apps]$ cd /opt/apps/IBM/WebSphere/AppServer/profiles/ETRLIVE_solr/properties
[wcsuser@g9t3901 properties]$
```

vi ssl.client.props

```
com.ibm.ssl.alias=DefaultSSLSettings
com.ibm.ssl.protocol=TLSv1.2
com.ibm.ssl.securityLevel=HIGH
com.ibm.ssl.trustManager=IbmPKIX
com.ibm.ssl.keyManager=IbmX509
com.ibm.ssl.contextProvider=IBMJSSE2
com.ibm.ssl.enableSignerExchangePrompt=gui
```

Webserver Changes:

```
[wcsuser@g9t3900 conf]$ pwd
/opt/apps/IBM/HTTPServer/conf
[wcsuser@g9t3900 conf]$ vi httpd.conf
```

```

SSLEnable
SSLProtocolDisable SSLv2 SSLv3 TLSv10 TLSv11
SSLClientAuth none
ServerName g9t3900.houston.hplicorp.net
</VirtualHost>

```

Agent Server settings:

- 1) Add this property in -Dhttps.protocols=TLSv1.2 in file
/opt/apps/IBM/Sterling93/bin/agentserver.sh

WESB Appserver

/opt/apps/IBM/WebSphere/AppServer/profiles/ETRLIVE/properties/ssl.client.props

```

#
com.ibm.ssl.alias=DefaultSSLSettings
com.ibm.ssl.protocol=TLSv1.2
com.ibm.ssl.securityLevel=HIGH
com.ibm.ssl.trustManager=IbmPKIX
com.ibm.ssl.keyManager=IbmX509
com.ibm.ssl.contextProvider=IBMJSSE2
com.ibm.ssl.enableSignerExchangePrompt=gui

```

Restart the dmgr using stopmanger and startmanager

Stop the node: WAS_install\profiles\AppSrv01\bin\stopNode.bat -username -password

Stop all Application Servers running on this node using stopserver command

Synchronize the node using syncnode command in each app servers & solr servers

./syncNode.sh g9t3902.houston.hplicorp.net 8879 -username configadmin -password ****

From WAS_install\profiles\AppSrv01\bin\syncNode.bat dmgrhostname dmgrsoapport -username consoleadminuser -password consoleuserpassword

Start the node: From WAS_install\profiles\AppSrv01\bin\startNode.bat

Check the Sync status of node from console.. and then start the application server from console.

Changes in Job server:

/opt/apps/IBM/WebSphere/AppServer/profiles/ETRLIVE/properties/ssl.client.props

```
#  
com.ibm.ssl.alias=DefaultSSLSettings  
com.ibm.ssl.protocol=TLSv1.2  
com.ibm.ssl.securityLevel=HIGH  
com.ibm.ssl.trustManager=IbmPKIX  
com.ibm.ssl.keyManager=IbmX509  
com.ibm.ssl.contextProvider=IBMJSSE2  
com.ibm.ssl.enableSignerExchangePrompt=gui
```