Configure TSL/SSL for two-way authentication

User Role: Administrator

TLS/SSL creates encrypted connections that allow private and sensitive information to be transmitted without the risk of eavesdropping, data tampering, or message forgery. HP recommends setting up a TLS/SSL connection between Service Manager and Smart Analytics, Connector Framework Server (CFS)/connectors, or Image Server. To do this, see the following steps for different scenarios.

For details about how to create two-way authentication certificates, see How to setup SingleSignOn (SSO) in a Horizontally scaled environment.

Configure TSL/SSL for two-way authentication between Service Manager and Smart Analytics

To Configure TSL/SSL for two-way authentication between Service Manager and Smart Analytics, follow these steps as an example:

1. Create a signed Service Manager server certificate and Smart Analytics certificate using the OpenSSL toolkit as a private certificate authority.

   ```
   CA Certificate keystore file: cacerts

   CA Certificate keystore password: "changeit"

   CA Certificate file: mycacert.pem

   SM Server keystore file: server.keystore

   SM Server serverkeystore password: "serverkeystore"

   Client public certificate file: clientpubkey.cert

   Client certificate private key file: exported_rsa.key

   Trusted clients keystore file: trustedclients.keystore (Import Client public
   certificate into Trustedclients keystore)

   Trusted clients keystore password: "trustedclients"
   ```

2. Configure the Service Manager server to use the server certificate and to trust the client certificate.

   a. Copy the following files to server host and put them under the RUN directory:

      - certs\cacerts
      - certs\trustedclients.keystore

- key\server.keystore

b. Set the following parameter values in the `sm.ini` file.

Parameter	Value
`ssl`	`1`
`sslConnector`	`1`
`ssl_reqClientAuth`	`2`
`trustedsignon`	`1`
`keystoreFile`	`server.keystore`
`keystorePass`	`serverkeystore`
`ssl_trustedClientsJKS`	`trustedclients.keystore`
`ssl_trustedClientsPwd`	`trustedclients`
`truststoreFile`	`cacerts`
`truststorePass`	`changeit`

c. Restart the Service Manager server.

3. Configure the Smart Analytics components to use the client certificate and to trust the server certificate.

a. Copy the following files to the <*Smart Analytics Installation*>\ssl Certificate folder on your Smart Analytics local machine:

- certs\clientpubkey.cert
- certs\ mycacert.pem
- exported_rsa.key

b. Configure all content components to use the certificates by setting the <*Smart Analytics Installation*>\Content#\Content#.cfg file.

```
[SSLOption1]

SSLMethod=SSLV23

SSLCertificate=<Smart Analytics
Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem
```

```
[IndexServer]

SSLConfig=SSLOption1

[Server]

SSLConfig=SSLOption1
```

c. Configure smart search proxy to use the certificates by setting the <*Smart Analytics Installation*>\level2proxy\autonomyIDOLServer.cfg file:

```
[Service]

SSLConfig=SSLOption1

[SSLOption1]

SSLMethod=SSLV23

SSLCertificate=<Smart Analytics Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

[IndexServer]

SSLConfig=SSLOption1

[Server]

SSLConfig=SSLOption1

SSLIDOLComponents=TRUE

[IDOLServerN]

SSLConfig=SSLOption1
```

d. Configure the Smart Analytics main server to use the certificates by setting the <*Smart Analytics Installation*>\IDOL\AutonomyIDOLServer.cfg file.

```
[SSLOption1]

SSLMethod=SSLV23

SSLCertificate=<Smart Analytics Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key
```

```
SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

[IndexServer]

SSLConfig=SSLOption1

[DataDRE]

SSLConfig=SSLOption1

[CatDRE]

SSLConfig=SSLOption1

[AgentDRE]

SSLConfig=SSLOption1

[Server]

SSLConfig=SSLOption1

SSLIDOLComponents=TRUE

[IDOLServerN]

SSLConfig=SSLOption1

[Agent]

SSLConfig=SSLOption1
```

e. Change the <*Smart Analytics Installation*>\IDOL\agentstore.cfg file.

```
[SSLOption1]

SSLMethod=SSLV23

SSLCertificate=<Smart Analytics
Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

[IndexServer]

SSLConfig=SSLOption1

[Server]

SSLConfig=SSLOption1
```

```
SSLIDOLComponents=true
```

f. Configure the Connector Framework Server (CFS) to use the certificates by setting the <*Smart Analytics Installation*>\CFS\CFS.cfg file.

```
[SSLOption1]

SSLMethod=SSLV23

SSLCertificate=<Smart Analytics Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

//Use this parameter to specify the path to a directory containing multiple CA certificates in PEM format to check against. Each file must contain one CA certificate.

//SSLCACertificatesPath=C:\Autonomy\HTTPConnector\CACERTS\

[Server]

//to make CFS ACI port ssl encrypted.

SSLConfig=SSLOption1
```

g. Restart the corresponding services for the Smart Analytics components that you modified.

Configure TSL/SSL for two-way authentication between Service Manager and CFS/connectors

To Configure TSL/SSL for two-way authentication between Service Manager and CFS/connectors, follow these steps as an example:

1. Create a signed Service Manager server certificate and Connector Framework Server (CFS) or connectors certificate using the OpenSSL toolkit as a private certificate authority.

```
CA Certificate keystore file: cacerts

CA Certificate keystore password: "changeit"

CA Certificate file: mycacert.pem

SM Server keystore file: server.keystore

SM Server serverkeystore password: "serverkeystore"

Client public certificate file: clientpubkey.cert

Client certificate private key file: exported_rsa.key
```

```
Trusted clients keystore file: trustedclients.keystore (Import Client public
certificate into Trustedclients keystore)

Trusted clients keystore password: "trustedclients"
```

2. Configure the Service Manager server to use the server certificate and to trust the client certificate.

   a. Copy the following files to server host and put them under the RUN directory:

      - certs\cacerts
      - certs\trustedclients.keystore
      - key\server.keystore

   b. Set the following parameter values in the `sm.ini` file.

Parameter	Value
`ssl`	`1`
`sslConnector`	`1`
`ssl_reqClientAuth`	`2`
`trustedsignon`	`1`
`keystoreFile`	`server.keystore`
`keystorePass`	`serverkeystore`
`ssl_trustedClientsJKS`	`trustedclients.keystore`
`ssl_trustedClientsPwd`	`trustedclients`
`truststoreFile`	`cacerts`
`truststorePass`	`changeit`

   c. Restart the Service Manager server.

3. Configure the Smart Analytics Connector Framework Server (CFS) or connectors to use the client certificate and to trust the server certificate.

   a. Copy the following files to the <*Smart Analytics Installation*>\ssl Certificate folder on your Smart Analytics local machine:

      - certs\clientpubkey.cert
      - certs\ mycacert.pem
      - exported_rsa.key

b. Configure the Connector Framework Server (CFS) to use the certificates by setting the <*Smart Analytics Installation*>\CFS\CFS.cfg file.

```
[SSLOption1]

SSLMethod=SSLV23

SSLCertificate=<Smart Analytics
Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

//Use this parameter to specify the path to a directory containing multiple
CA certificates in PEM format to check against. Each file must contain one
CA certificate.

//SSLCACertificatesPath=C:\Autonomy\HTTPConnector\CACERTS\

[Server]

//to make CFS ACI port ssl encrypted.

SSLConfig=SSLOption1
```

c. Configure the connectors to use the certificates by setting the <*connector*>.cfg file.

```
[Ingestion]

//If CFS ACI port is ssl encrypted

IngestSSLConfig=SSLOption1
```

d. Restart the corresponding CFS and connector services.

Configure TSL/SSL for two-way authentication between Service Manager and Image Server

To Configure TSL/SSL for two-way authentication between Service Manager and Image Server, follow these steps as an example:

1. Create a signed Service Manager server certificate and Image Server certificate using the OpenSSL toolkit as a private certificate authority.

```
CA Certificate keystore file: cacerts

CA Certificate keystore password: "changeit"

CA Certificate file: mycacert.pem

SM Server keystore file: server.keystore
SM Server serverkeystore password: "serverkeystore"

Client public certificate file: clientpubkey.cert

Client certificate private key file: exported_rsa.key

Trusted clients keystore file: trustedclients.keystore (Import Client public
certificate into Trustedclients keystore)

Trusted clients keystore password: "trustedclients"
```

2. Configure the Service Manager server to use the server certificate and to trust the client certificate.

   a. Copy the following files to server host and put them under the RUN directory:

      - certs\cacerts
      - certs\trustedclients.keystore
      - key\server.keystore

   b. Set the following parameter values in the `sm.ini` file.

Parameter	**Value**
`ssl`	`1`
`sslConnector`	`1`
`ssl_reqClientAuth`	`2`
`trustedsignon`	`1`
`keystoreFile`	`server.keystore`
`keystorePass`	`serverkeystore`
`ssl_trustedClientsJKS`	`trustedclients.keystore`
`ssl_trustedClientsPwd`	`trustedclients`
`truststoreFile`	`cacerts`
`truststorePass`	`changeit`

   c. Restart the Service Manager server.

3. Configure the Smart Analytics Image Server to use the client certificate and to trust the server certificate.

   a. Copy the following files to the <*Smart Analytics Installation*>\ssl Certificate folder on your Smart Analytics local machine:

- certs\clientpubkey.cert
- certs\ mycacert.pem
- exported_rsa.key

b. Configure the Image Server to use the certificates by setting the <*Smart Analytics Installation*>\ImageServer1\ImageServer1.cfg file.

```
[SSLOption1]

SSLMethod=SSLV23

SSLCertificate=<Smart Analytics Installation>\sslCertificate\clientpubkey.cert

SSLPrivateKey=<Smart Analytics Installation>\sslCertificate\exported_rsa.key

SSLCACertificate=<Smart Analytics Installation>\sslCertificate\mycacert.pem

[Server]

SSLConfig=SSLOption1
```

c. Restart the Image Server service.