November 10, 2020

Certificate Implementation on ICAI

Jharana Patra, GCS

Informatica™

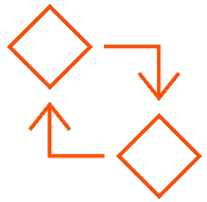
Housekeeping Tips

- Today's Webinar is scheduled for 1 hour
- The session will include a webcast and then your questions will be answered live at the end of the presentation
- All dial-in participants will be muted to enable the speakers to present without interruption
- Questions can be submitted to "All Panelists" via the Q&A option and we will respond at the end of the presentation
- The webinar is being recorded and will be available to view on our INFASupport YouTube channel and Success Portal. The link will be emailed as well.
- Please take time to complete the post-webinar survey and provide your feedback and suggestions for upcoming topics.

Feature Rich Success Portal

Bootstrap trial and POC Customers

Enriched Customer Onboarding experience



Product Learning Paths and Weekly Expert Sessions

Informatica Concierge with Chatbot integrations

Tailored training and content recommendations

Informatica

More Information

Success Portal

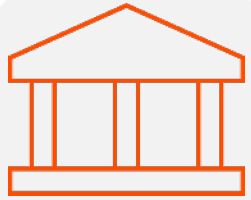
https://success.informatica.com

Communities & Support

https://network.informatica.com

Documentation

https://docs.informatica.com



University

https://www.informatica.com/in/services-and-training/informatica-university.html

Informatica

Safe Harbor

The information being provided today is for informational purposes only. The development, release, and timing of any Informatica product or functionality described today remain at the sole discretion of Informatica and should not be relied upon in making a purchasing decision.

Statements made today are based on currently available information, which is subject to change. Such statements should not be relied upon as a representation, warranty or commitment to deliver specific products or functionality in the future.

How to implement certificate in CAI?

Agenda

- Use cases
- Truststore
- Keystore
- Service properties of Process-Server
- Brief on SSL handshake
- Demo on setting up the service properties
- Common Issues
- Related articles and commands

Different ways to invoke process deployed on Agent?

- When you deploy Informatica Process Designer (IPD) processes, the endpoint URL construction for anonymous access is different from the endpoint URL construction for non anonymous access.

Type of Access	REST Endpoint	SOAP 1.2 Endpoint
Non anonymous access of an IPD process using HTTP	http://[host][:port]/process-engine/rt/[serviceName] Swagger: http://[host][:port]/process-engine/rt/[serviceName]?swagger	http://[host][:port]/process-engine/soap/[serviceName] WSDL: http://[host][:port]/process-engine/soap/[serviceName]?wsdl
Anonymous access of an IPD process using HTTP	http://[host][:port]/process-engine/public/rt/[serviceName] Swagger: http://[host][:port]/process-engine/public/rt/[serviceName]?swagger	http://[host][:port]/process-engine/public/soap/[serviceName] WSDL: http://[host][:port]/process-engine/public/soap/[serviceName]?wsdl
Non anonymous access of an IPD process using HTTPS.	https://[host][:port]/process-engine/rt/[serviceName] Swagger: https://[host][:port]/process-engine/rt/[serviceName]?swagger	https://[host][:port]/process-engine/soap/[serviceName] WSDL: https://[host][:port]/process-engine/soap/[serviceName]?wsdl
Anonymous access of an IPD process using HTTPS.	https://[host][:port]/process-engine/public/rt/[serviceName] Swagger: https://[host][:port]/process-engine/public/rt/[serviceName]?swagger	https://[host][:port]/process-engine/public/soap/[serviceName] WSDL: https://[host][:port]/process-engine/public/soap/[serviceName]?wsdl

Prerequisites to expose HTTPS IPD process on secure agent

- You may need to configure the Process Server service of an Informatica Cloud Secure Agent when invoking services that require X.509 client certificate-based mutual authentication or exposing an HTTPS/TLS endpoint on the agent.
- To enable this, the Process Server service needs to be configured with a KeyStore and a TrustStore.

Keystore:

- When establishing a HTTPS/TLS handshake the TrustStore is used to verify credentials.

Truststore:

The KeyStore on the other hand is used to provide credentials.

1. The KeyStore in Java stores private keys and certificates corresponding to their public keys.
2. It is required to expose a trusted endpoint as part of the HTTPS/TLS handshake, or required to perform client authentication when an endpoint requires it.

Prerequisites to invoke HTTPS services that requires certificate authentication

- You may need to configure the Process Server service of an Informatica Cloud Secure Agent when invoking services that require X.509 client certificate-based mutual authentication.
- To enable this, the Process Server service needs to be configured with a custom KeyStore and add required certificate in {agent}/apps/process-engine/conf/certs.

TrustStore:

- When establishing a HTTPS/TLS handshake the TrustStore is used to verify credentials.

Keystore:

The KeyStore on the other hand is used to provide credentials.

1. The KeyStore in Java stores private keys and certificates corresponding to their public keys.
2. It is required to expose a trusted endpoint as part of the HTTPS/TLS handshake, or required to perform client authentication when an endpoint requires it.

Properties that need be configured in process server

Property Name	Description
key-store	The path to the key store file that the Process Server service uses for HTTPS/TLS communication. When you install a Secure Agent, you will find the default key store at the default location: {Agent.Home}/apps/process-engine/conf/ae.keystore.
key-store-password	The KeyStore password. The default password is password. You can change the password if you want to generate a new KeyStore file.
trust-store	The path to the trust store file that the Process Server service uses for HTTPS communication. When you install a Secure Agent, you find the trust-store at the default location: {Agent.Home}/apps/process-engine/conf/ae.cacerts.
trust-store-password	The TrustStore password. The default password is changeit. You can change the password if you want to generate a new trust store file **Command:** keytool -storepasswd -new NewPwd -truststore Security\truststore.jks

How to configure TrustStore

Default TrustStore Configuration :

- The Process Server service creates a default TrustStore file with it is deployed to a Secure Agent. This TrustStore file is located at {Agent.Home}/apps/process-engine/conf/ae.cacerts.
- To add a new certificate to your configuration, you need to copy the certificates to the {Agent.Home}/apps/process-engine/conf/certs directory.

Custom TrustStore Configuration :

- You can create a custom TrustStore file and provide the path to this file (using the Agent Runtime Environment Process Server setting) using the “trust-store” property and the corresponding “trust-storepassword” property with the password for the TrustStore file
- If you use a custom TrustStore file, this file will not be overwritten on agent restart. You need to import all public certificates you need to that TrustStore file and keys distributed within {Agent.Home}/jre/lib/security/cacerts.

Note: If you import a public certificate directly to the default TrustStore at /apps/process-engine/conf/ae.cacerts, you should also copy the certificate file into the /apps/process-engine/conf/certs folder.

How to configure Keystore

Default Keystore Configuration :

- The Process Server service creates a default KeyStore file when it is deployed to a Secure Agent. This KeyStore file is located at {Agent.Home}/apps/process-engine/conf/ae.keystore. This KeyStore file is intended to be used to store private keys.
- You need to import additional private keys you intend to use (in addition to the default provided to you) into the KeyStore file. By default, a certificate with a localhost alias is installed into the default KeyStore.

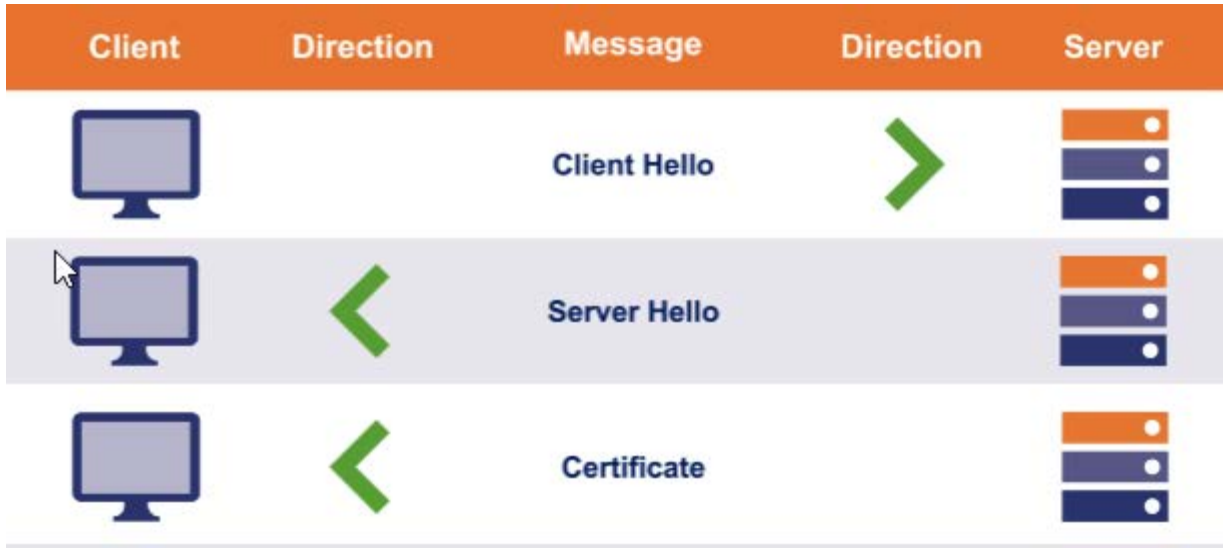
Custom Keystore Configuration :

- If you intend to expose an agent-based endpoint and intend to connect to this endpoint using HTTPS/TLS, you will need to generate a custom KeyStore or import your private key to the KeyStore Informatica provides. .

Note: The default KeyStore is not overwritten on upgrades.To use a custom KeyStore you need to configure the key-store property using the Agent Runtime Environment properties of the Process Server.

Command : keytool -list -keystore cacerts

Part One: The Normal Handshake



Informatica

Part Two: Certificate-Based Authentication

Informatica

How to configure process server service properties to expose HTTPS IPD process on secure agent ?

In the ICS Console > Configure > Runtime Environment. Select the agent, select Edit, and update these Process Server service properties:

	Type	Name	Value
1	server	Host-name	'localhost'/CN as per certificate/wildcard entries
2	server	key-alias	'localhost'/as per the keystore
3	server	key-store	'../conf/ae.keystore'
4	server	key-store-password	*'password' The key and keystore password should be the same.
5	server	trust-store	'../conf/ae.cacerts'
6	server	trust-store-password	'changeit'

How to configure process server service properties for invoking services that requires certificate authentication?

In the ICS Console > Configure > Runtime Environment. Select the agent, select Edit, and update these Process Server service properties:

	Type	name	Value
1	jvm	additional properties	Djavax.net.ssl.keyStore=<Cert required for mutual auth> -Djavax.net.ssl.keyStorePassword=<password>

1.Import the certificate or place it in conf/cert

2.Set the following JVM Keystore parameters under addition properties
Djavax.net.ssl.keyStore=<Cert required for mutual auth> -Djavax.net.ssl.keyStorePassword=<password>

Example: Djavax.net.ssl.keyStore=C:\ICSLabFiles\debug.keystore -Djavax.net.ssl.keyStorePassword=sample?

3.Restart the Secure Agent.

The Client

Config Problems

- Missing certs from cacerts or keys from keystore.
- Invalid key-store format
- Expired/Revoked/Self-Signed Certificates

The Server

Config Problems

- Hostname Mismatch/Incorrect Cert Chain.
- Expired/Revoked/Self-Signed Certificates.
- Invalid key-store format
- Invalid key-alias

Informatica

Identifying the certificate issue

Incorrect custom keystore:

```
... 13 more
Caused by: java.io.FileNotFoundException: C:\Program Files\Informatica Cloud Secure Agent\apps\process-engine\conf\debug.jks (The system cannot find the file specified)
    at java.io.FileInputStream.open0(Native Method) ~[?:1.8.0_252]
    at java.io.FileInputStream.open(FileInputStream.java:195) ~[?:1.8.0_252]
    at java.io.FileInputStream.<init>(FileInputStream.java:138) ~[?:1.8.0_252]
    at java.io.FileInputStream.<init>(FileInputStream.java:93) ~[?:1.8.0_252]
    at sun.net.www.protocol.file.FileURLConnection.connect(FileURLConnection.java:90) ~[?:1.8.0_252]
    at sun.net.www.protocol.file.FileURLConnection.getInputStream(FileURLConnection.java:188) ~[?:1.8.0_252]
    at org.apache.tomcat.util.file.ConfigFileLoader.getInputStream(ConfigFileLoader.java:89) ~[tomcat-util.jar:8.5.57]
    at org.apache.tomcat.util.net.SSLUtilBase.getStore(SSLUtilBase.java:196) ~[tomcat-coyote.jar:8.5.57]
    at org.apache.tomcat.util.net.SSLHostConfigCertificate.getCertificateKeystore(SSLHostConfigCertificate.java:207) ~[tomcat-coyote.jar:8.5.57]
    at org.apache.tomcat.util.net.SSLUtilBase.getKeyManagers(SSLUtilBase.java:281) ~[tomcat-coyote.jar:8.5.57]
    at org.apache.tomcat.util.net.SSLUtilBase.createSSLContext(SSLUtilBase.java:245) ~[tomcat-coyote.jar:8.5.57]
```

Incorrect password

```
    ... 44 more
06-Nov-2020 12:18:27.056 IST WARN [SystemWorkManager-WorkerThread-1] [com.amazonaws.http.SystemPropertyTlsKeyManagersProvider] [{}] - Unable to load KeyManager from system properties
java.io.IOException: Keystore was tampered with, or password was incorrect
    at sun.security.provider.JavaKeyStore.engineLoad(JavaKeyStore.java:792) ~[?:1.8.0_252]
    at sun.security.provider.JavaKeyStore$JKS.engineLoad(JavaKeyStore.java:57) ~[?:1.8.0_252]
    at sun.security.provider.KeyStoreDelegator.engineLoad(KeyStoreDelegator.java:224) ~[?:1.8.0_252]
    at sun.security.provider.JavaKeyStore$DualFormatJKS.engineLoad(JavaKeyStore.java:71) ~[?:1.8.0_252]
    at java.security.KeyStore.load(KeyStore.java:1445) ~[?:1.8.0_252]
    at com.amazonaws.http.AbstractFileTlsKeyManagersProvider.createKeyStore(AbstractFileTlsKeyManagersProvider.java:53) ~[aws-java-sdk-core-1.11.714.jar:?]
    at com.amazonaws.http.AbstractFileTlsKeyManagersProvider.createKeyManagers(AbstractFileTlsKeyManagersProvider.java:42) ~[aws-java-sdk-core-1.11.714.jar:?]
    at com.amazonaws.http.SystemPropertyTlsKeyManagersProvider.getKeyManagers(SystemPropertyTlsKeyManagersProvider.java:55) [aws-java-sdk-core-1.11.714.jar:?]
    at com.amazonaws.http.apache.client.impl.ApacheConnectionManagerFactory.getKeyManagers(ApacheConnectionManagerFactory.java:121) [aws-java-sdk-core-1.11.714.jar:?]
```

Incorrect key-alias

```
    ... 13 more
Caused by: java.io.IOException: Alias name [localhost] does not identify a key entry
    at org.apache.tomcat.util.net.SSLUtilBase.getKeyManagers(SSLUtilBase.java:326) ~[tomcat-coyote.jar:8.5.57]
    at org.apache.tomcat.util.net.SSLUtilBase.createSSLContext(SSLUtilBase.java:245) ~[tomcat-coyote.jar:8.5.57]
    at org.apache.tomcat.util.net.AbstractJsseEndpoint.createSSLContext(AbstractJsseEndpoint.java:98) ~[tomcat-coyote.jar:8.5.5
    at org.apache.tomcat.util.net.AbstractJsseEndpoint.initialiseSsl(AbstractJsseEndpoint.java:72) ~[tomcat-coyote.jar:8.5.57]
    at org.apache.tomcat.util.net.NioEndpoint.bind(NioEndpoint.java:246) ~[tomcat-coyote.jar:8.5.57]
    at org.apache.tomcat.util.net.AbstractEndpoint.init(AbstractEndpoint.java:1118) ~[tomcat-coyote.jar:8.5.57]
    at org.apache.tomcat.util.net.AbstractJsseEndpoint.init(AbstractJsseEndpoint.java:222) ~[tomcat-coyote.jar:8.5.57]
    at org.apache.coyote.AbstractProtocol.init(AbstractProtocol.java:587) ~[tomcat-coyote.jar:8.5.57]
    at org.apache.coyote.http11.AbstractHttp11Protocol.init(AbstractHttp11Protocol.java:74) ~[tomcat-coyote.jar:8.5.57]
    at org.apache.catalina.connector.Connector.initInternal(Connector.java:1075) ~[catalina.jar:8.5.57]
```


Informatica

keytool -genkey -alias mydomain -keyalg RSA -keystore keystore.jks -keysize 2048

Related articles

- Missing certs from cacerts or keys from keystore.
  - Follow -> CERT IMPORTER TOOL -- http://kb.informatica.com/howto/6/Pages/21/527498.aspx
  - Get Keys from vendor and import.
  - Test JMS Connectivity outside of Informatica Cloud Application Integration : https://knowledge.informatica.com/s/article/617363
  - How to import public certificates Integration

  https://knowledge.informatica.com/s/article/619056
  - -Custom certificate on secureagent

  https://knowledge.informatica.com/s/article/627046

  SSL-hand-shake:

  https://medium.com/@kasunpdh/ssl-handshake-explained-4dabb87cdce

Related articles

Frequently used Keytool Commands :

keytool -genkey -alias mydomain -keyalg RSA -keystore keystore.jks -keysize 2048

keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore keystore.jks

keytool -export -alias mydomain -file mydomain.crt -keystore keystore.jks

Common Keytool commands

https://www.sslshopper.com/article-most-common-java-keytool-keystore-commands.html

https://docs.oracle.com/en/java/javase/13/docs/specs/man/keytool.html

Keytool explorer:

https://keystore-explorer.org/

The Exception - ICAI

1. There is no possible way to set SSL Debug.

Ex: The JVM Option "-Djavax.net.debug=ssl:handshake “ or -Djavax.net.debug=debug doesn’t collect the debug log

1. Cert Based Auth can only be configured to one API

Ex: More than one certificate based API can’t be called using service connector

Questions?


Thank You