Cisco IAC 4.0 How−to configure SSL between Process Orchestrator and Service Catalog

Document ID: 117740

The scope of this document is a simple walkthrough on configuring SSL on Cisco Intelligent Automation for Cloud. This configuration will use self−signed certificates but can be used with Third−party or Trusted Root certificates. This is not a replacement for any SSL documentation in the IAC documentation portfolio.

- Configuring SSL on the Service Catalog server
- Configuring SSL on the Process Orchestrator server
- Configuring Process Orchestrator and Service Catalog to use SSL with each other
- Configuring RequestCenter and ServiceLink to use SSL to communicate (optional)

Configuring SSL on the Service Catalog server

The Service Catalog server consists of two components that will be configured for SSL: RequestCenter and ServiceLink. This configuration was done on a two−server JBoss configuration but should work on a one−server JBoss configuration as well. This configuration will work on a Windows or Linux Service Catalog server. The steps will show the configuration on a Windows Service Catalog server but can be used on a Linux Service Catalog server. In the steps below the variable <***JBOSS_RC_HOME***> refers to the JBoss home directory for RequestCenter, <***JBOSS_SL_HOME***> refers to the JBoss home directory for ServiceLink, and <***JAVA_HOME***> refers to the Java home directory.
This section contains the following topics:

Configuring SSL on RequestCenter

This section contains the following topics:

Create certificate

The first thing to do is to create a self−signed certificate.

1. Open a command prompt.
2. Change directories to <***JBOSS_RC_HOME***>***RequestCenterServer\configuration***.
3. Create a self−signed certificate by running the command <***JAVA_HOME***>***jre\bin\keytool −genkey −alias <requestcenter alias> −keyalg RSA −keypass <keypass password> −storepass <storepass password> −keystore keystore.jks***

   For the purposes of the configuration the alias used is ***RequestCenter*** and the keypass and storepass password is the default password ***changeit***.

   NOTE: You will be prompted to enter information about this certificate. The first prompt is ***What is your first and last name*** (also called the CN). This must be the host name of the machine or ***localhost***. The rest of the information can be whatever you want to put in.

Export certificate

The next thing to do is to export the certificate to a file.

1. Open a command prompt.
2. Change directories to <***JBOSS_RC_HOME***>***RequestCenterServer\configuration***.
3. Export the certificate to a file by running the command <***JAVA_HOME***>***jre\bin\keytool −export −alias <requestcenter alias> −storepass <storepass password> −file <requestcenter certificate file name> −keystore keystore.jks***

   For the purposes of the configuration the file name used is ***RequestCenter.cer***.

Import certificate to the JBoss trust store

The next thing to do is to import the certificate into the JBoss trust store.

1. Open a command prompt.
2. Change directories to ***<JBOSS_RC_HOME>\RequestCenterServer\configuration***.
3. Import the certificate into the JBoss trust store by running the command ***<JAVA_HOME>\jre\bin\keytool −import −v −trustcacerts −alias <requestcenter alias> −file <requestcenter certificate file name> −keystore cacerts.jks −keypass <keypass password> −storepass <storepass password>***.

Import certificate in the Java trust store

The next thing to do is to import the certificate into the Java Trust Store.

1. Open a command prompt.
2. Change directories to ***<JAVA_HOME>\jre\lib\security***.
3. Copy the RequestCenter certificate file from <JBOSS_RC_HOME>\RequestCenterServer\configuration into this directory.
4. Import the certificate into the Java trust store by running the command ***<JAVA_HOME>\jre\bin\keytool −import −v −trustcacerts −alias <requestcenter alias> −file <requestcenter certificate file name> −keystore cacerts −keypass <keypass password> −storepass <storepass password>***.

Edit the standalone−full.xml configuration file

The next thing to do is to edit the standalone−full.xml configuration file.

1. Open the file ***<JBOSS_RC_HOME>\RequestCenterServer\configuration\standalone−full.xml*** with an appropriate text editor.
2. Search for ***<connector name="http" protocol="HTTP/1.1" scheme="http" socket−binding="http"/>*** and add the following lines after it:

   <connector protocol="HTTP/1.1" name="https" scheme="https" socket−binding="https" secure="true">
   <ssl key−alias="<requestcenter alias>" password="changeit" certificate−key−file="<JBOSS_RC_HOME>\RequestCenterServer\configuration\keystore.jks"/>
   </connector>

   NOTE: Change ***<requestcenter alias>*** to the RequestCenter alias you are using and ***<JBOSS_RC_HOME>*** to the JBoss home directory for RequestCenter.
3. Save the file ***standalone−full.xml***.
4. Restart RequestCenter.

Configuring SSL on ServiceLink

To configure SSL on ServiceLink, repeat the steps in the Configuring SSL on RequestCenter section of the document, making sure you use the ***<JBOSS_SL_HOME>*** directory and the <servicelink alias>.

Configuring SSL on the Process Orchestrator server

The Process Orchestrator server is a Windows server that uses IIS. This section contains the following topics:

- Create certificate
- Export certificate
- Bind certificate to Process Orchestrator SSL port

Create certificate

The first thing to do is to create a self−signed certificate.

1. Open IIS Manager.
2. On the left side of the window, select the Process Orchestrator server.
3. On the right side of the window, double−click on Server Certificates.
4. On the far right side of the Server Certificates windows, click on Create Self−Signed Certificate.
5. Enter a friendly name for the certificate and click OK.

Export certificate

1. After the certificate is created, right−click on it and select View.
2. Click on the Details tab and click on Copy to File
3. On the Certificate Export Wizard click ***Next***.
4. Select ***"No, do not export private key"*** and click ***Next***.
5. Select ***Base−64 encoded x.509 (.CER)*** and click ***Next***.
6. Enter a file name and click ***Next***.
7. Click ***Finish*** to save the certificate file.

Bind certificate to Process Orchestrator SSL port

1. Open the certificate file, click on the Details tab, and scroll down to Thumbprint in the Field section of the Details tab. Copy the Hex value for Thumbprint − this is the certificate hash value.
2. Open a command prompt.
3. Run the command "netsh http add sslcert ipport=0.0.0.0:61526 certhash=<thumbprint> appid={1776a671−8e9c−45b0−8304−dec6f472131f}"

   The ipport=0.0.0.0:61526 is the IP Address and SSL Port for the Process Orchestrator. It should be 0.0.0.0:61526.

   The certhash is the Thumbprint value you copied in Step 1.

   *NOTE: You must remove the spaces in the Thumbprint value. The appid is always {1776a671−8e9c−45b0−8304−dec6f472131f}.

Configuring Process Orchestrator and Service Catalog to use SSL with each other

Now that SSL is configured on Service Catalog and Process Orchestrator, these servers need to be configured to communicate with each other using SSL. To do that the servers need to trust each other. That is done by adding the server certificate files into the Trust Store. This section contains the following topics:

- Adding the Service Catalog certificates to the Process Orchestrator trust store
- Adding the Process Orchestrator certificates to the Service Catalog trust store
- Configuring the Process Orchestrator server to use SSL
- Configure the RequestCenter Agents to use SSL

Adding the Service Catalog certificates to the Process Orchestrator trust store

The Process Orchestrator server needs to have the certificates of the Service Catalog server (both the RequestCenter and ServiceLink certificates) installed in its Trust Store.

1. Copy the RequestCenter and ServiceLink certificate files onto the Process Orchestrator server.
2. Right−click on the RequestCenter certificate file and select "Install Certificate".
3. On the Certificate Import Wizard window click Next.
4. Select "Place all certificates in the following store" and click Browse.
5. Select "Trusted Root Certification Authorities" and click OK.
6. Click Next
7. Click Finish to complete the certificate installation.
8. An error message may pop up in regards to the certificate claiming it is from "localhost". This error is okay. Click Yes to install the certificate.
9. On the last window, click OK to complete the installation process.
10. Repeat Steps 2−9 to install the ServiceLink certificate.

Adding the Process Orchestrator certificates to the Service Catalog trust store

The Service Catalog server needs to have the certificate of the Process Orchestrator server installed in its Trust Store.

1. Open a command prompt.
2. Change directories to <JAVA_HOME>\jre\lib\security.
3. Copy the Process Orchestrator certificate file to the Service Catalog server in the <JAVA_HOME>\jre\lib\security directory.
4. Import the certificate into the Java trust store by running the command ***<JAVA_HOME>\jre\bin\keytool −import −v −trustcacerts −alias <Process Orchestrator alias> −file <Process Orchestrator certificate file name> −keystore cacerts −keypass <keypass password> −storepass <storepass password>***.
5. Restart RequestCenter and ServiceLink.

Configuring the Process Orchestrator server to use SSL

The Process Orchestrator server needs to be configured to use SSL. The server properties and various Targets need to be configured to use SSL. This section contains the following topics:

- Change the server properties (environment properties)
- Configure the targets

Change the server properties (environment properties)

1. Open and log into the Process Orchestrator Console.
2. From the File Menu, select server Properties (Environment Properties in IAC 4.0).
3. Select the Web Service tab
4. Deselect "Enable non−secure Web Service (HTTP)" and select "Enable secure Web Service (HTTPS)". You may see the following message:

   Enabling Cisco Process Orchestrator Web Services on a secure port (HTTPS) requires additional manual configuration. Please refer to the documentation for instructions.

   Click OK on this message.
5. You can select an HTTPS port but the default of 61526 should be okay.
6. Click "Refresh Web Service" and then click on OK.

Configure the targets

The targets "Cisco Cloud Portal Integration API", "Cisco Cloud Portal Request Center API", "Cisco Process Orchestrator Web Service", and "Cisco Service Portal Server" all need to be configured to use HTTPS and the SSL port.

1. On the Process Orchestrator console, on the bottom left part of the window select Definitions, on the top left part of the window select Targets, and on the right side of the window double−click on the "Cisco Cloud Portal Integration API" target.
2. Click on the Connection tab change the Base URL to:

   https://<cp hostname>:<ServiceLink SSL port>/IntegrationServer/services

   where <cp hostname> is the hostname or IP Address of the Service Catalog server and <ServiceLink SSL port> is the SSL port of ServiceLink. The default port is 6443.
3. Click OK to save changes.
4. Repeat Steps 2−3 for the other targets using the following Base URL information:

   Target: Cisco Cloud Portal Request Center API
   Base URL: https://<cp hostname>:<RequestCenter SSL port>/RequestCenter
   The default RequestCenter SSL port is 8443

   Target: Cisco Process Orchestrator Web Service
   Base URL: https://<Process Orchestrator hostname>:<Process Orchestrator SSL port>/WS/
   The default Process Orchestrator SSL port is 61526
5. The Cisco Service Portal server is a different type of target. To configure this target double−click on it.
6. Click on the Connection tab change the Service Link port to the ServiceLink SSL port (default is 6443), change the Request Center port to the RequestCenter SSL port (default is 8443). Also select "Access Service Portal via Secure Socket Layer (SSL)" and also "Ignore Secure Socket Layer (SSL) certificate error".
7. Click OK to save changes. Note that this target will verify the SSL connection with the Service Catalog server. The Service Catalog server needs to be running and have SSL configured.

Configure the RequestCenter Agents to use SSL

Now that Process Orchestrator is configured the RequestCenter Agents need to be configured to use SSL.

1. Log into the Service Catalog Web Console as the Admin user.
2. From the pulldown select "My workspace" and go to the "Configuration Wizard". If it is not on "My Workspace" then click on the "+" and add it.
3. Click Next Step to go to Step 1 and select "Set HTTP Agent Configuration"
4. For the "Process Orchestrator Web Service URL" enter

   https://<Process Orchestrator hostname>:<Process Orchestrator SSL port>

   where <Process Orchestrator hostname> is the hostname or IP Address of the Process Orchestrator server and <Process Orchestrator SSL port> is the SSL port of Process Orchestrator. The default port is 61526.
5. For the Process Orchestrator Username, Password, and Domain enter in a username, password, and domain for the user that will connect with the Process Orchestrator server.
6. For the "Service Catalog Service Link URL" enter

   https://<cp hostname>:<ServiceLink SSL port>/IntegrationServer

   where <cp hostname> is the hostname or IP Address of the Service Catalog server and <ServiceLink SSL port> is the SSL port of ServiceLink. The default port is 6443.
7. Click Submit Order.
8. Close The Submit Order response window.
9. After the Order has completed, Click on "Start all other agents". If the agents are already started then they need to be stopped and started again for the new configuration to take effect.
10. Select all the agents on Page 1 and click "Stop Selected"
11. Select Yes on the confirmation window.
12. Repeat Steps 10−11 for all of the other pages.
13. Go back to Page 1, select all the agents and click "Start Selected"
14. Select Yes on the confirmation window.
15. Repeat Steps 13−14 for all of the other pages.

Configuring RequestCenter and ServiceLink to use SSL to communicate (optional)

The final step is optional configuring RequestCenter and ServiceLink to use SSL to communicate.

1. On the Service Catalog server, open your favorite file editor.
2. Open the file <JBOSS_RC_HOME>\RequestCenterServer\deployments\RequestCenter.war\WEB−INF−classes\config\news
3. Search for isee.base.url=http://<cp hostname>:6080 where <cp hostname> is the hostname of the Service Catalog server.
4. Change the line to be isee.base.url=https://<cp hostname>:6443. The port 6443 is the default port for ServiceLink SSL. If you are using a different port then enter it instead of 6443.
5. Save the newscale.properties file.
6. Restart RequestCenter.

Updated: Jun 11, 2014 Document ID: 117740
