CentraSite Mediator communication over HTTP(s)

**Purpose of this document:** As part of the tutorial what we are going to cover here is end - end use case of create and publish an asset for invocation in secured HTTP(s) transport.

- What is Mediator
- What is CentraSite
- Create Self Signed Certificate
- Configure HTTPS port in Mediator
  - Configure keystore and truststore
  - Create HTTP(s) port in Integration Server
- Configure the ports and certificate in Mediator
- Configure the certificate in CentraSite
- Create a target / mediator gateway in CentraSite Business UI
- Create asset in CentraSite
- Publish/ invoke asset to mediator

**What is Mediator**

webMethods Mediator is a service intermediary that enforces the run-time policies you create in CentraSite. Mediator also virtualizes shared services, making it easy to change services.

Combined with CentraSite, Mediator provides end-to-end governance of all your services and APIs from development to run-time. Combined with webMethods Enterprise Gateway, Mediator provides comprehensive API Gateway functionality.


**What is CentraSite**

CentraSite is the lifecycle management tool and enterprise catalog for APIs, SOA services, and related assets. For more information please refer the documentation.

As part of the tutorial what we are going to cover here is end - end use case of creating an asset to invocation in secured HTTP(s) transport.

In order to have communication done in a secured transport first of all what we should be having is self signed certificate or if you have valid certificates issues by CA then you don’t need to create one and ignore the below step.

**Create Self Signed Certificate**

The below mentioned steps are guide us to create one and we would use the same for HTTPS in Integration Server.

We have used the version Win64 OpenSSL v1.0.1g for demonstration, other flavors of the Open SSL can be downloaded from [here](http://www.softwareag.com/corporate/products/webmethods_integration/api/products/default.asp)

To begin with we need to have the OpenSSL installed and generate a self signed certificate and 1024 bit RSA key as shown below, if you don’t have one.
You can also use third party tools like Key Store Explorer which helps in creating the keystore and the certificates.

- Open Keystore explorer and then click on “Create a keystore” as shown below

- Select the type of keystore you want and in this case we call for a “JKS”
• Drag and drop the certificate you just created into the keystore explorer and then click on "Import" button followed by the alias name to make it as a trusted certificate.

• Generate key pair and provide the name of the alias and save the store locally with the extension.
Configure HTTPs port in Mediator

Make sure that the security configuration is done in Mediator. For further guidance on that how to configure key store and trust store refer the section below or look for "Securing Communications with the Server" in the webMethods Integration Server Administrator's Guide.
Configure keystore and truststore

If we want to deploy virtual services with the security policies apply, we have to first setup the security configuration settings in Mediator.

1. Go to the Mediator and click on Security > Key store. By default you would not find any information related to keystore added out of the box. Click on create keystore alias and and provide the certificate information as given below in the screen shots, Provide the keystore alias name, and the .jks file we just created with the store password.

2. Once the key store alias is configured, you will find that information in the key store list. Now create a trust store alias by pointing to the "cacert" in the same location and this truststore should have the public key of the certificate being used but this is not a mandatory step and can be ignore if issues by a valid CA.

   a. C:\SoftwareAG\IntegrationServer\instances\default\packages\WmMediator\config\resources\security\cacerts
   b. password would be "changeit"
Once the keystore and truststore are configured we should configure the client certificates by specifying the certificate path.

1. In Mediator, if user authenticate against X.509 certificate, user has to map with certificate. Below is the configuration step to map the user.
2. Point to the location where we have our certificate in this case its server.crt
3. Select the user as "Administrator" or any valid IS user by searching the users in the configuration section by clicking the search icon next to search field.
4. Once configured click on “Import Certificate” button and then the certificate would be added to the certificates list.
Create HTTP(s) port in Integration Server

Once the keystore and certificates are configured its now time to create a HTTPs port in Integration Server

a. To start of with open the Integration Server administration screen and then go to Security - Ports and click on add port
b. Now select the HTTP(s) port and click on OK to furnish the desired port information.
Configure the ports and certificate in Mediator

Now configure the security information in Mediator.

- Open the Mediator Administration screen
- Go to General - > Edit
- Configured Keystore and truststore information will be listed here. Choose the appropriate one.
- Add the created / desired HTTP(s) port from Available ports to Selected ports section and save the configuration.

Configure the certificate in CentraSite

Once the certificate is configured in Mediator now comes the configuring of certificate in the CentraSite instance., For which we need to add the certificates to the "cacerts" file which is located at the below location.
This file is used for the secured outbound communication from CentraSite as as client to desired destination which in our case is webMethods Mediator and password for this is “changeit”.

Open the cacerts file from key store explorer and drag the certificate in to cacerts.

Once done save the cert and restart the Software AG Runtime Tomcat.

Create a target / mediator gateway in CentraSite Business UI

In the recent versions of CentraSite there is a change in the terminology of Target and Service.

Target is now called as “Mediator” in CentraSite Business UI, Follow the below steps to create a mediator instance in CentraSite Business UI

1. Login to CentraSite Business UI using the uri http://<CentraSite _Host:port>/BusinessUI
2. Click on “Manage Governance Rules” and then click on “Add Gateway”
3. Provide the Gateway / Mediator information
   a. From the drop down select the gateway as “Mediator”
   b. Provide the name of the mediator gateway
   c. Provide the HTTPS port and host information of the mediator where it is running under the Mediator Communication
   d. Provide the credentials of the user registered in IS and then
   e. Click on Publish button so that the mediator gateway is created in CentraSite and the information is stored in the mediator as well
1. Once published you should be able to see the same information in details page and as well in the mediator centrasite communication page.
Create asset in CentraSite

As part of the tutorial we are going to create a REST based asset in CentraSite, Virtualize it and publish that asset to the Mediator gateway.

Click on Create Asset action in Business UI and select the asset type as “REST Service” and provide the asset name. If you want to create a REST based asset which takes “Swagger 2.0” or “RAML 0.8” specifications then provide the appropriate input and then click on “Next” button to take a preview of the information we provided and then click on “Save” button which would redirect you to the details page of the asset.

The second step would be to furnish the technical details the REST service for which we need to click on the “Edit” action / icon in the details page and provide the following information.

- Click on Technical details and provide the base uri or the location of the instance where your back end service is running
- Click on Resources and the add a resource which would be used internally to generate an operation of the asset which is depicted in the images given below.
Publish/ invoke asset to mediator

The next step is to create a “Virtual Alias” in CentraSite for the REST API created above and to achieve that click on the “Virtualize” action and then provide the alias name and click on “Next”

In the second page of the wizard navigation under the Message Flow in the “Receive” section click on the settings icon to select HTTPS as the required protocol and then click on publish to deploying the asset to mediator instance.

Step 1: Provide the Virtual alias name and click on Next button

Step 2: Configure the HTTPS port

Step 3: Select the desired destination of the mediator instance where the asset needs to be published
Step 4: publish in progress

Step 5: Landing in the details page of the Virtual Alias or Virtual REST Service and now go the consumer overview profile/ link to view the service access uri.

Step 6: Copy the HTTPS enabled access uri and create a new project in SOAP UI and invoke the asset.
Note: You need to configure the certificates used earlier in the SOAP UI Preferences if using it as a client to invoke the asset.