

Dutch Electronic VAT Return Statement and EC Sales List

HCI Configuration Guide (version 2)

CONTENTS

| | |
|---|---|
| Introduction..... | 3 |
| HCI..... | 3 |
| Prerequisites..... | 3 |
| Preparing tenant keystore..... | 4 |
| Configuring integration flows..... | 5 |
| Configuring sender endpoint..... | 5 |
| Configuring sender channel (optional)..... | 6 |
| Configuring receiver channel..... | 6 |
| Deploying integration flows..... | 7 |
| ABAP System..... | 7 |
| Prerequisites..... | 7 |
| Importing tenant certificates to ABAP system..... | 7 |
| Creating logical ports..... | 8 |

INTRODUCTION

This document describes how to configure HCI based solution for submitting electronic VAT return statement and EC sales list to Dutch authorities.

There are four integration flows included in integration package *NL Electronic VAT Return Statement and EC Sales List*:

- | | |
|---|-------------------------|
| <ul style="list-style-type: none">Preproduction AanleverservicePreproduction Statusinformatieservice | PREPRODUCTION LANDSCAPE |
| <ul style="list-style-type: none">Production AanleverserviceProduction Statusinformatieservice | PRODUCTION LANDSCAPE |

It is advisable to first configure and test preproduction services before moving to the production phase.

The whole scenario consists of two stages:

- Submission of the statement to Aanleverservice which, if your submission is accepted, returns *submission ID*.
- Submission ID* from stage 1 is used to query status of your submission at Statusinformatieservice.

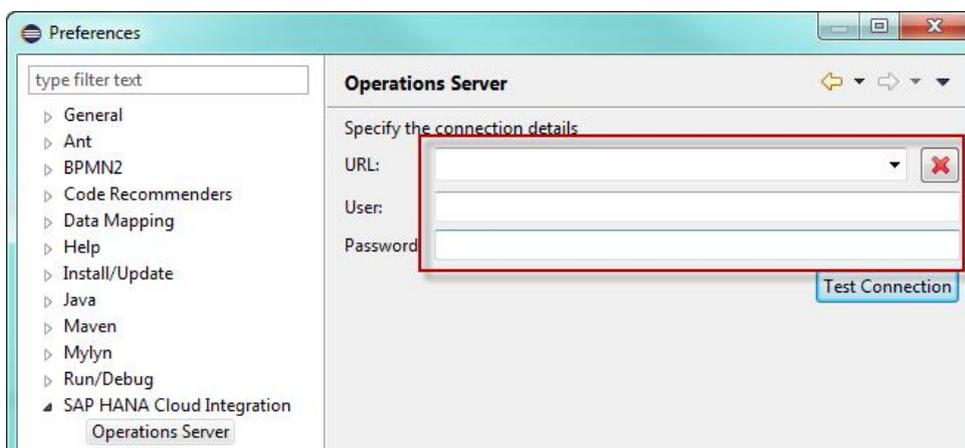
HCI

This chapter describes the configuration of integration flows which will later be invoked from the ABAP system. The ABAP system will send properly formatted XML file, our integration flow will add the required security elements to the message and forward it to Aanleverservice or Statusinformatieservice depending on which integration flow was invoked.

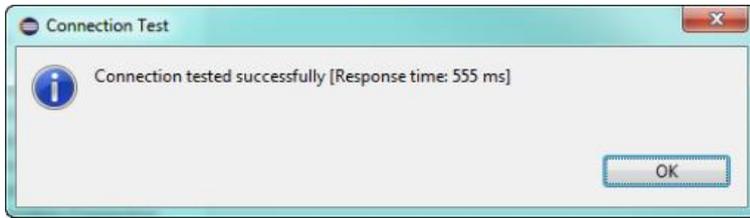
PREREQUISITES

- The certificate chain of the service you are going to communicate with and the private key pair for digital signature. This should be provided to you by the authority.
- [KeyStore Explorer](#) or a similar tool that will allow you to manipulate keystores.
- A user on your HCI tenant with enough authorization to access it through Eclipse and Web UI
- Eclipse environment with [SAP HANA Cloud Integration Tools](#).
This guide was written for Eclipse Luna Service Release 2 (4.4.2) with plugins Designer for SAP HANA Cloud Integration (2.16.2) and Operations for SAP HANA Cloud Integration (2.15.0).
- A working connection from the Eclipse environment to your Operations Server (HCI tenant).

In Eclipse, navigate to *Window → Preferences → SAP HANA Cloud Integration → Operations Server* and specify the URL of your operations server, user name and password.



Once you do this, you will be able to trigger a connection test which should end successfully.



- Correct perspective opened in Eclipse

Navigate to *Window* → *Open Perspective* → *Other* and select *Integration Designer* perspective.

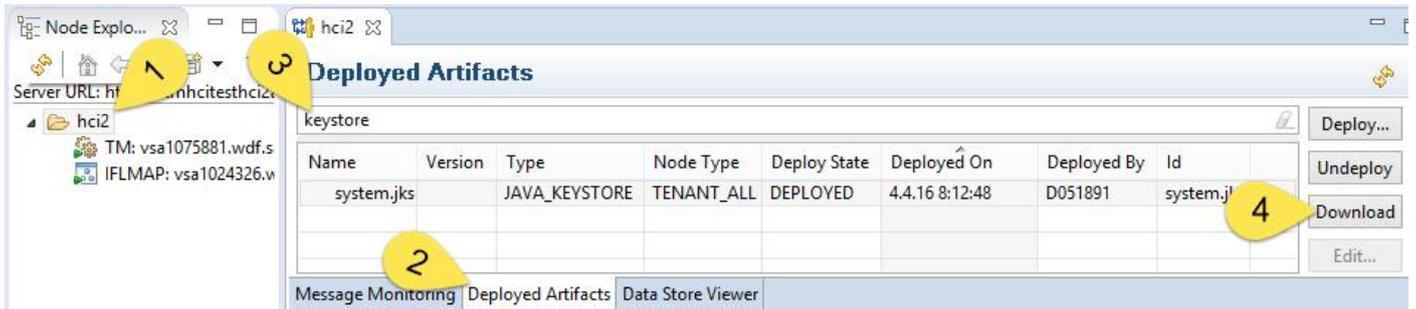
PREPARING TENANT KEYSTORE

Keystore preparation is the only step that must be done in Eclipse.

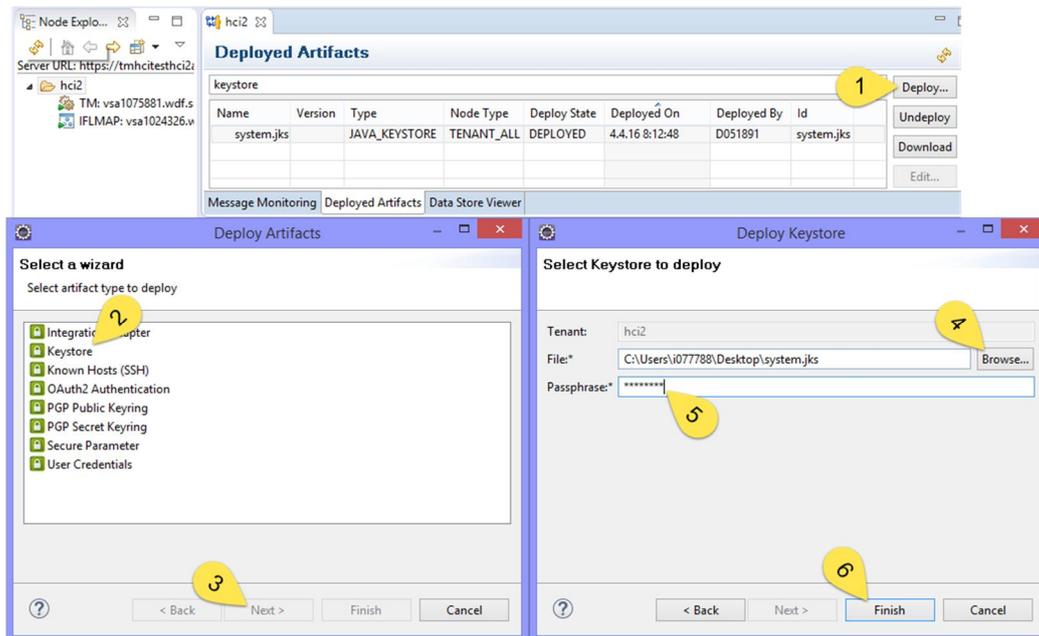
Following security artifacts must be acquired from authorities:

- Private key pair for preproduction landscape (including password)
- Certificate chain for preproduction landscape
- Private key pair for production landscape (including password)
- Certificate chain for production landscape

Download the keystore from your tenant (steps 1, 2, 3, 4 pictured below) and open it with the KeyStore explorer. Import all acquired security artifacts to the keystore. Once you import the private key pair, you will be asked to enter a password and then you will be requested to set a new one. Please note that the new password must be identical to the password of the keystore itself! Set the preproduction private key pair alias to "digipoort_preprod" and the production private key pair alias to "digipoort_prod". It will be used later when configuring the receiver channel.



Once you have imported all necessary artifacts, deploy modified keystore back to your tenant (steps 1, 2, 3, 4, 5, 6 pictured below).



Please note that for each tenant there is always only one keystore shared by everyone. Therefore you should not deploy a brand new keystore with only your security artifacts to the tenant. Such an action would overwrite the existing tenant keystore with your own, and all other security artifacts would be lost. Always download the existing keystore, modify it, and then deploy it back.

CONFIGURING INTEGRATION FLOWS

Execute the following steps for each integration flow in the package.

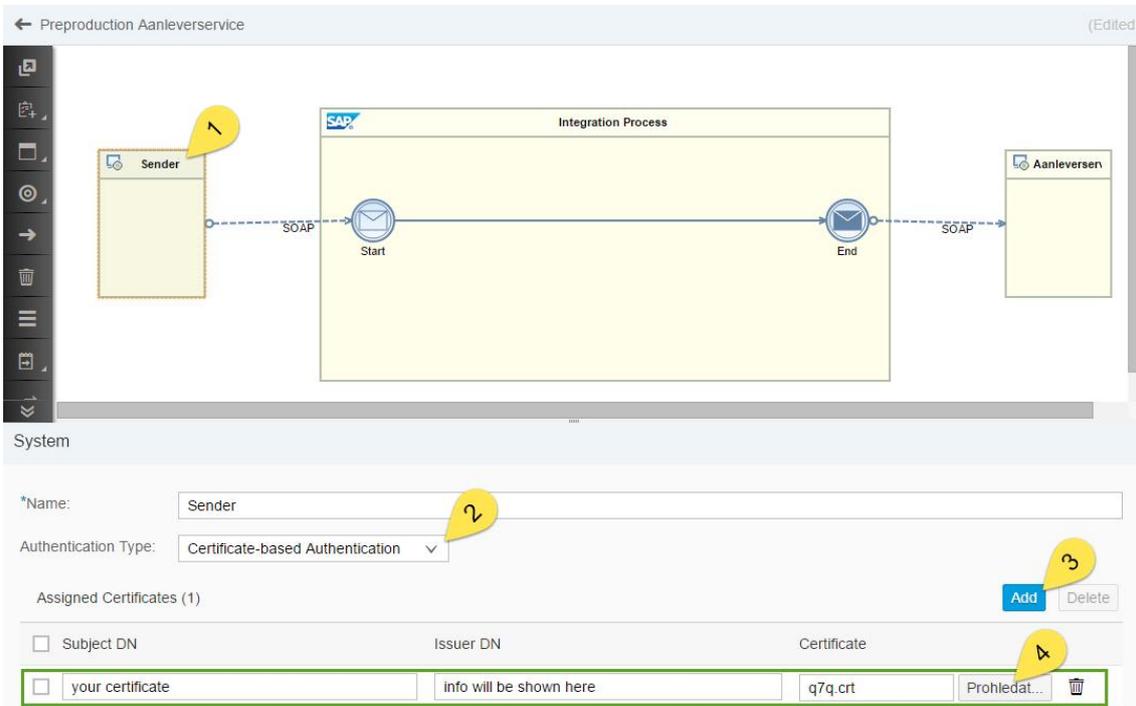
CONFIGURING SENDER ENDPOINT

Sender authentication mode has to be decided. There are two modes available:

- *Role-based Authentication* means that username/password will be used when accessing deployed service.
- *Certificate-based Authentication* means that SSL certificates will be used to authenticate anyone who tries to access this service.

By default, sender endpoint is set to use *Role-based Authentication*. In practice it may be more convenient to use *Certificate-based Authentication*. To get it working you need to export the SSL certificate from your ABAP system (transaction STRUST → SSL client SSL client (Standard)) and import it to the integration flow.

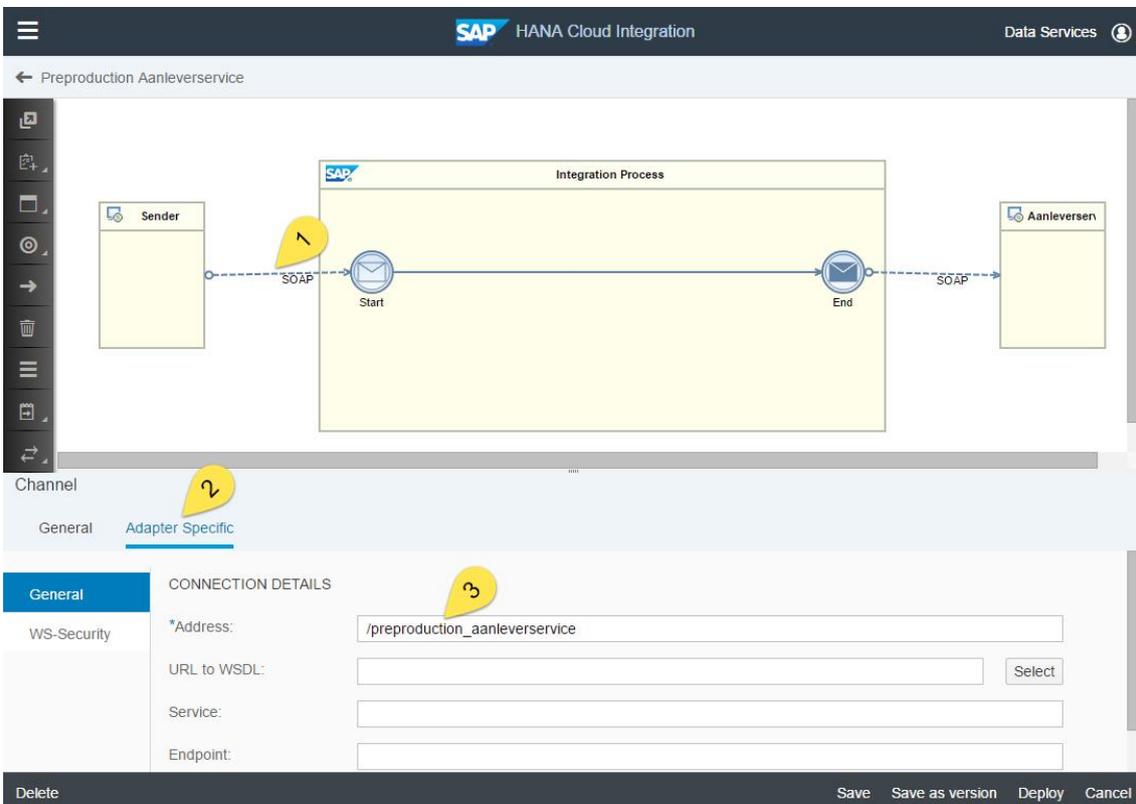
Once you get hold of ABAP system certificate, add it to your integration flow:



CONFIGURING SENDER CHANNEL (OPTIONAL)

The sender channel is already configured. You only need to execute this step if you want to change the address of the deployed service.

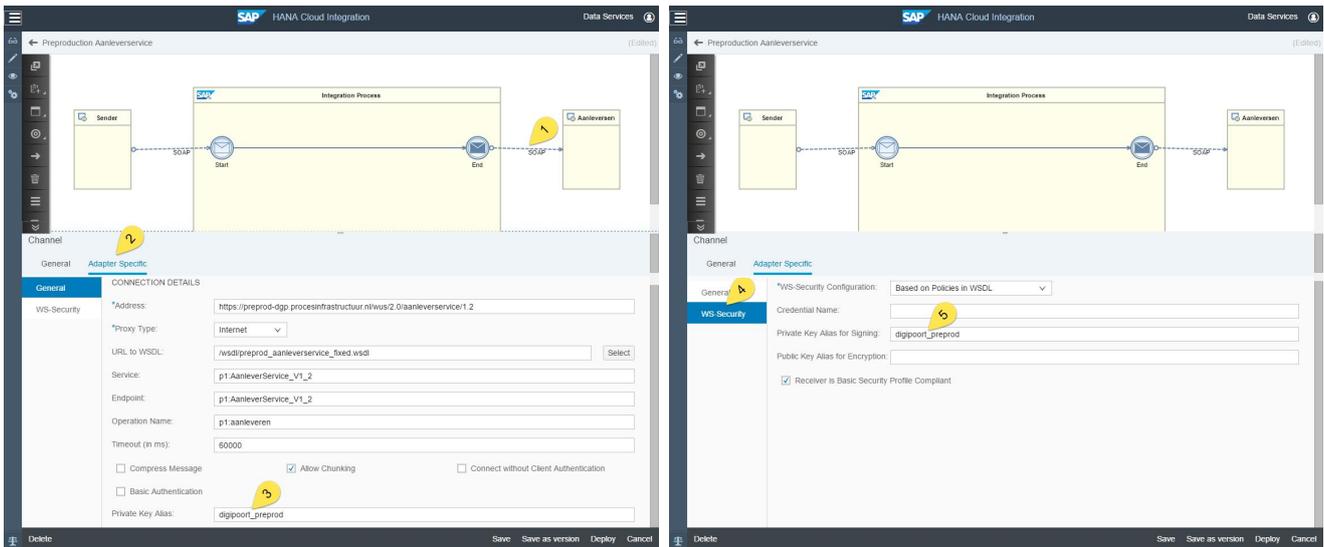
Click on the Sender Channel (1), switch to *Adapter Specific* tab (2) and enter *Address* e.g. `/preproduction_aanleverservice` (3). Once you deploy your integration flow it will be accessible via `<worker node url>/cxf/ preproduction_aanleverservice` (or whatever you have entered).



CONFIGURING RECEIVER CHANNEL

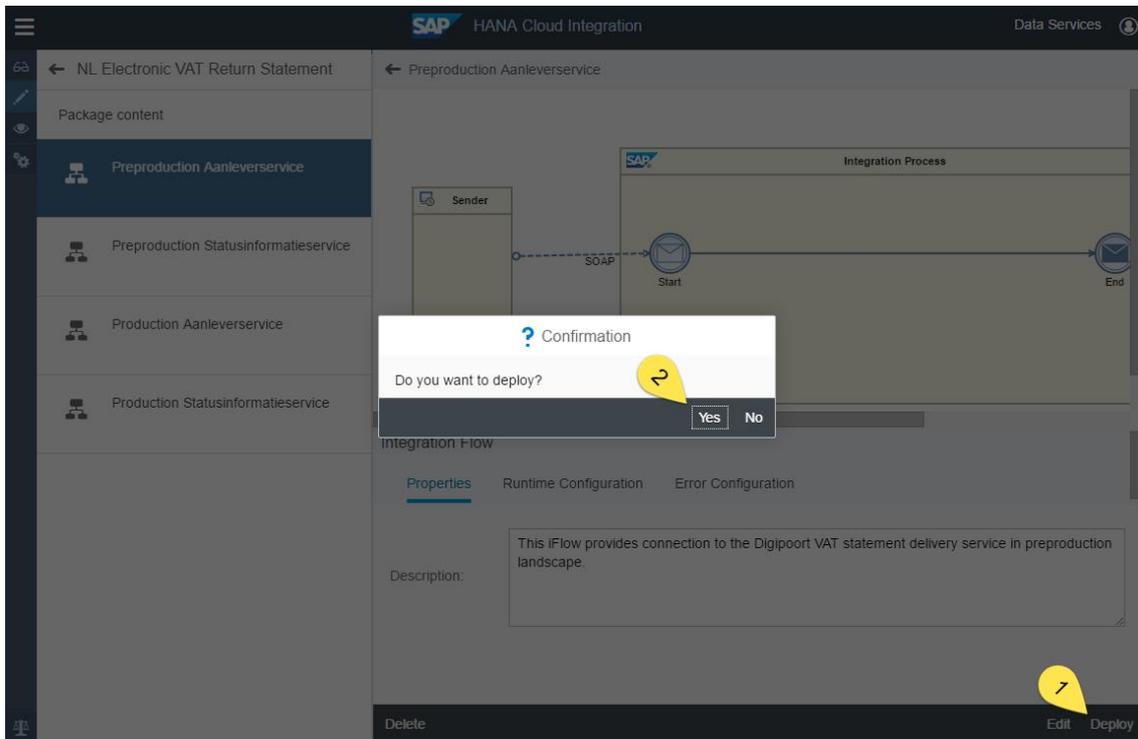
The receiver channel is already configured. The only thing that might need adjustment is the private key alias.

Make sure *Private Key Alias* (3) and *Private Key Alias for Signing* (5) correspond to the alias that you have used in your keystore.



DEPLOYING INTEGRATION FLOWS

Once everything is configured, the integration flow is ready to be deployed.



ABAP SYSTEM

PREREQUISITES

Implement SAP note 1943145 - XBRL Solutions for VAT and ICP in Netherlands. PI related note 1941806 does not have to be implemented.

IMPORTING TENANT CERTIFICATES TO ABAP SYSTEM

This step is required to establish trust between your ABAP system and your tenant. In transaction STRUST import certificate (actually the whole certificate chain) of your tenant to SSL Client Anonymous folder.

- Tenant certificates can be obtained via browser from *<URL of your worker node>/cxf*.

- You may not be authorized to manipulate trust store so it may be necessary to ask someone who is to import required certificates.

CREATING LOGICAL PORTS

Call transaction SOAMANAGER and navigate to Web Service Configuration. Search by Object Name for *CO_NL**. You should get at least two results – consumer proxies CO_NLAANLEVERSERVICE and CO_NLSTATUSINFORMATIESERVICE – that were created during the implementation of SAP note 1943145.

Open CO_NLAANLEVERSERVICE and create a new logical port with manual configuration (described below) for the preproduction landscape and a separate logical port directed to the production landscape. Once finished, repeat the same steps for consumer proxy CO_NLSTATUSINFORMATIESERVICE.

Depending on integration flow authentication mode configured earlier select authentication settings.

Configuration: Consumer Proxy 'CO_NLAANLEVERSERVICE', Logical Port 'PREPROD'

Save Edit Ping Web Service

Consumer Security Messaging Transport Settings Identifiable Business Context Operation Settings Administrative Information

Configuration of Consumer Settings without WSDL Document. LP=PREPROD

Authentication Level: Basic

Authentication Settings

User ID / Password
 SAP Authentication Assertion Ticket
 X.509 SSL Client Certificate

X.509 SSL Client PSE

SSL Client PSE of transaction STRUST: 

Make sure you select Suppress ID Transfer as Message ID Protocol in Messaging tab.

Web Service Configuration (Q7Q;002)

Configuration: Consumer Proxy 'CO_NLAANLEVERSERVICE', Logical Port 'HCI2'

Save Edit Ping Web Service

Consumer Security **Messaging** Transport Settings Identifiable Business Context Operation Settings Administrative Information

Message ID (Synchronous)

Message ID Protocol:

Metering of Service Calls

Data transfer scope:

Transfer protocol:

Switch to Transport Settings tab and enter

- Enter relative path to your service. By default it is
 - /cxf/preproduction_aanleverservice for preproduction aanleverservice
 - /cxf/preproduction_statusinformatieservice for preproduction statusinformatieservice
 - /cxf/production_aanleverservice for production aanleverservice

- /cxf/production_statusinformatieservice for production statusinformatieservice
2. Enter worker node address
 3. Enter port 443
 4. And switch to HTTPS
 5. (Optional) If you are behind a proxy server you can define it here in order to be able to get outside
 6. (Optional) Proxy port

Configuration: Consumer Proxy 'CO_NLAANLEVERSERVICE', Logical Port 'PREPROD'

Save Edit Ping Web Service

Consumer Security Messaging **Transport Settings** Identifiable Business Context Operation Settings Administrative Information

Transport Binding

* URL Access Path: /cxf/preproduction_aanleverservice 7

Computer Name of Access URL: ifilmaphcitesthci2avtdmo-hci2.bsn.neo.ondemand.com 2

Port Number of Access URL: 443

URL Protocol Information: HTTPS 3 4

Logon Language: Language of User Context 5

Name of Proxy Host: proxy 6

Port Number of Proxy Host: 8080

User Name for Proxy Access:

Password of Proxy User:

Make Local Call: No Call in Local System

* Transport Binding Type: SOAP 1.1

Maximum Wait for WS Consumer: 0

Optimized XML Transfer: None

Compress HTTP Message: Inactive

Compress Response: True

Save and go back to the list of logical ports. Make sure your newly created preproduction port is set as default. Once you fine tune the preproduction scenario, you will switch the default port to the one leading to the production landscape.