



EUROPEAN COMMISSION

DIGIT  
Connecting Europe Facility

## **Domibus Demo**

### **FIWARE Lab**

Version [2.6]

Status [Validated]

© European Union, 2019

Reuse of this document is authorised provided the source is acknowledged. The Commission's reuse policy is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents.

Date: 08/08/2019

## Document Approver(s):

Approver Name	Role
RODRIGUES FRADE João	CEF eDelivery

## Document Reviewers:

Reviewer Name	Role
Ioana DRAGUSANU	Technical Team
Caroline AEBY	CEF Support

## Summary of Changes:

Version	Date	Created by	Short Description of Changes
0.01	21/02/2017	CEF Support	Creation of the document
0.02	22/02/2017	CEF Support	Update of the document
0.03	24/02/2017	CEF Support	Update of the document
0.04	27/02/2017	CEF Support	Apply comments
1.00	27/02/2017	CEF Support	Validation of the document
2.00	27/09/2017	Chaouki BERRAH	Update of the document
2.1	20/04/2018	Chaouki BERRAH	Update with new Fiware version
2.2	17/05/2018	Chaouki BERRAH	Document updated after review
2.3	17/05/2018	Chaouki BERRAH	Added information on Account Duration And FIWARE Nodes
2.4	26/09/2018	Caroline AEBY	End of standby service
2.5	25/07/2019	Caroline AEBY	Change in 2.3.3 – point 5
2.6	08/08/2019	Caroline AEBY	Cloud account creation and country selection

## Table of Contents

<b>1. INTRODUCTION .....</b>	<b>4</b>
1.1. Purpose.....	4
<b>2. DEPLOYMENT AND CONFIGURATION .....</b>	<b>5</b>
2.1. Registration.....	5
2.2. FIWARE Cloud Account creation .....	8
2.3. Domibus Configuration .....	11
2.3.1. Domibus Instance creation .....	11
2.3.2. Network Setup.....	14
2.3.3. Public IP Address configuration.....	15
2.3.4. The Security Options: .....	16
<b>3. LAUNCHING DOMIBUS AND TESTING .....</b>	<b>21</b>
<b>4. CONNECT TO SERVER USING SSH.....</b>	<b>25</b>
<b>5. CONTACT INFORMATION .....</b>	<b>26</b>

## 1. INTRODUCTION

This guide is intended for users who want to have a simple first-hand experience on the operations of exchanging messages between two Domibus instances.

### 1.1. Purpose

The purpose of this guide is to provide a step by step procedure for launching a Domibus instance on the FIWARE platform, preconfigured to exchange messages with the CEF **Connectivity Testing Platform**.

It provides detailed descriptions of related Security Configurations (keypair and Group Policy), network configuration and SoapUI testing.

## 2. DEPLOYMENT AND CONFIGURATION

### 2.1. Registration

1. Register on FIWARE Lab at: [https://account.lab.fiware.org/sign\\_up/](https://account.lab.fiware.org/sign_up/)

### Registration


Username  
cefsupport

E-mail  
cef-edelivery-support@ec.europa.eu

I have Gravatar and want to use it for my avatar.

Password **hard**  
.....

Password (again)  
.....

Captcha  
 I'm not a robot  reCAPTCHA Privacy

I accept FIWARE Lab [Terms and Conditions](#)

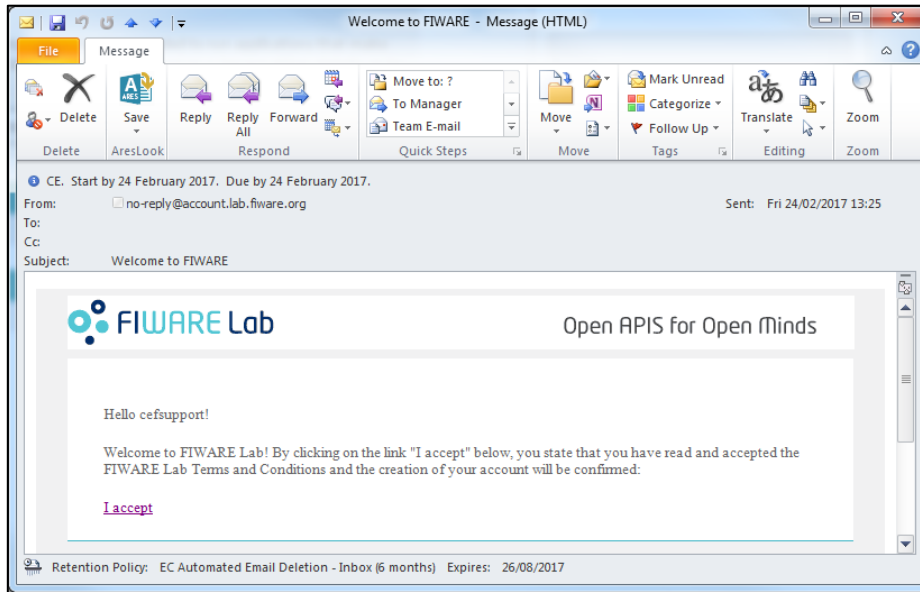
**Sign Up**

[Forgot password](#) | [Didn't receive confirmation instructions?](#)

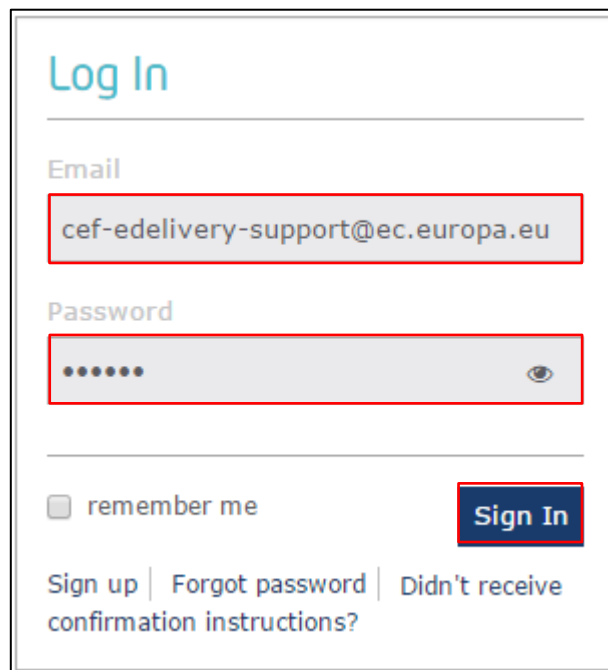
**Remark:**

- The Username, e-mail, etc. have to be adapted based on your information and requirements.
- A Trial account is opened with a minimum time of two weeks.
- The Community account duration may be extended to a minimum of 6 months, if the account is about to be deleted, by sending a request to FIWARE support.

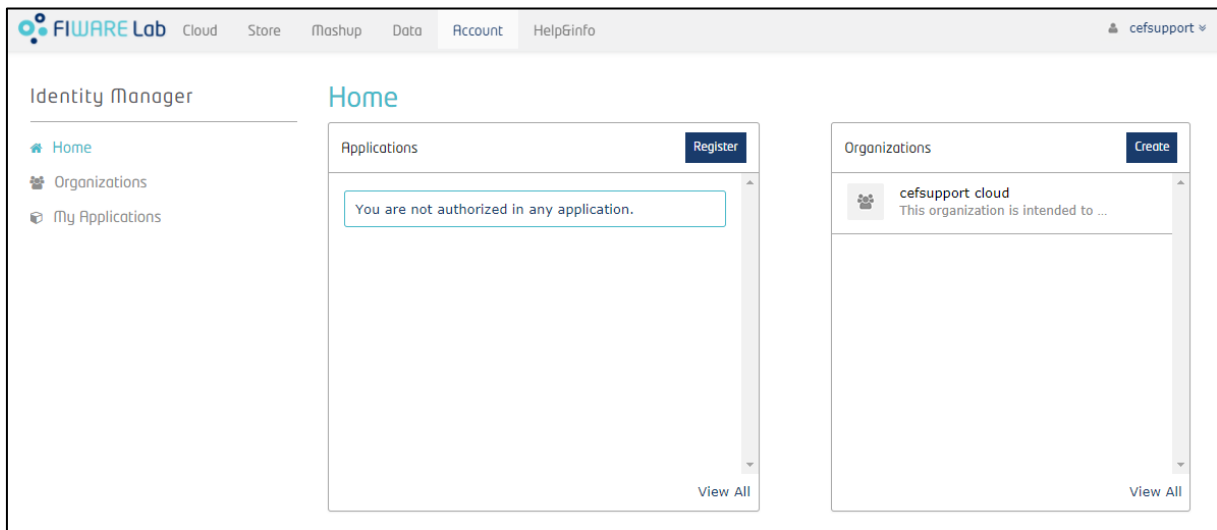
2. Once the confirmation email is received, click on **"I accept"**:



3. Log In by using the chosen email and password, click on **"Sign In"**:

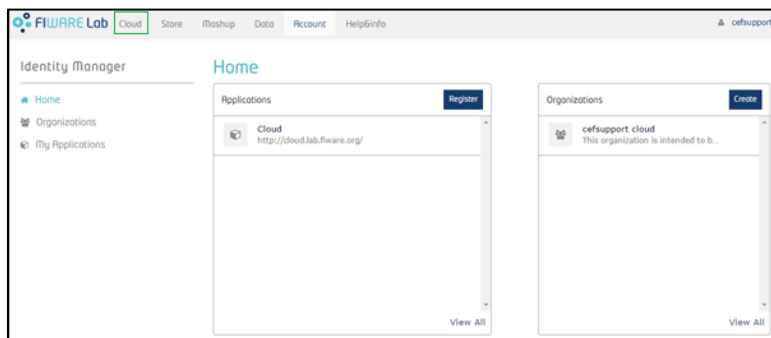


4. The following screen will be shown:



## 2.2. FIWARE Cloud Account creation

1. Click on "Cloud"



2. A Cloud portal account has to be created separately from the registration . Click on **Create Account**:



3. Enter your details including a Name and an Email address. Choose a FIWARE region closest to you from the list (e.g: **“Crete”**, **“Vicenza”**). Click on **“Envoyer”** / **“Send”** as shown in the example below:



## Create new FIWARE Lab user account

Enter your data and preferences in order to create the FIWARE Lab user account. It is important that you accept the Terms & Conditions before we create the account.

\*Obligatoire

**Name \***  
User name to be stored in the created account.

**Email \***  
Email address to be used to access to the FIWARE Lab Cloud.

**FIWARE Lab region \***  
Selected FIWARE Lab region in which you want to work.

**I accept the FIWARE Lab Terms & Conditions \***  
[http://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE\\_LAB\\_Terms\\_and\\_Conditions](http://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE_LAB_Terms_and_Conditions)

I have read and understand the Terms & Conditions

4. A message will be shown to acknowledge that the request has been sent:

## Create new FIWARE Lab user account

Your request has been submitted

5. You will receive an email asking you to confirm the account creation, as shown in the example below:

From: [fernando.lopez@fiware.org](mailto:fernando.lopez@fiware.org) <[fernando.lopez@fiware.org](mailto:fernando.lopez@fiware.org)>  
Subject: confirm: cTLHaBYO3GKaRnUm9Ag8ezcnbxcBIBG9jEGnvWxXTKDvVmGb

Thank you very much to select FIWARE Lab Cloud. We have received a request for FIWARE Lab user creation.

Here are the results.

Name cefsupport

..

6. Reply to the email as requested:

To: [fernando.lopez@fiware.org](mailto:fernando.lopez@fiware.org) <[fernando.lopez@fiware.org](mailto:fernando.lopez@fiware.org)>  
Subject: confirm: cTLHaBYO3GKaRnUm9Ag8ezcnbxcBIBG9jEGnvWxXTKDVMGb

7. Another email (waiting for approval), will be received to confirm that the request will be treated by a moderator:

From: [fiware-lab-user-creation-bounces@lists.fiware.org](mailto:fiware-lab-user-creation-bounces@lists.fiware.org) <[fiware-lab-user-creation-bounces@lists.fiware.org](mailto:fiware-lab-user-creation-bounces@lists.fiware.org)>  
Subject: Your message to Fiware-lab-user-creation awaits moderator approval  
Your mail to 'Fiware-lab-user-creation' with the subject  
confirm: cTLHaBYO3GKaRnUm9Ag8ezcnbxcBIBG9jEGnvWxXTKDVMGb  
Is being held until the list moderator can review it for approval.  
The reason it is being held:  
Post by non-member to a members-only list  
Either the message will get posted to the list, or you will receive  
notification of the moderator's decision. If you would like to cancel  
this posting, please visit the following URL:  
<https://lists.fiware.org/confirm/fiware-lab-user-creation/713cfe8ae7263741152d5468ba3409a563680f3e>

8. An email is then received after a couple of days to confirm the account has been created:

From: [noanswer@admttools.lab.fiware.org](mailto:noanswer@admttools.lab.fiware.org) <[noanswer@admttools.lab.fiware.org](mailto:noanswer@admttools.lab.fiware.org)>  
Subject: Your FIWARE Lab account has been created  
Your account in FIWARE Lab -- <https://cloud.lab.fiware.org> -- has been created  
Username: cefsupport@.....  
Password: 5094mmgzq07our1yydke  
Please, change your password in your 1st access. You can send your questions to [fiware-lab-help@lists.fiware.org](mailto:fiware-lab-help@lists.fiware.org)  
Best Regards,  
FIWARE Lab Team

**Remark:**

*If no email is received, please send an email the FIWARE support to request an update ([fiware-lab-user-creation-bounces@lists.fiware.org](mailto:fiware-lab-user-creation-bounces@lists.fiware.org))*

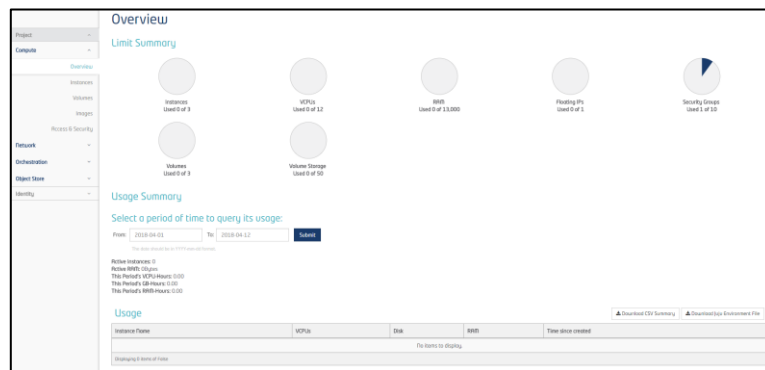
## 2.3. Domibus Configuration

### 2.3.1. Domibus Instance creation

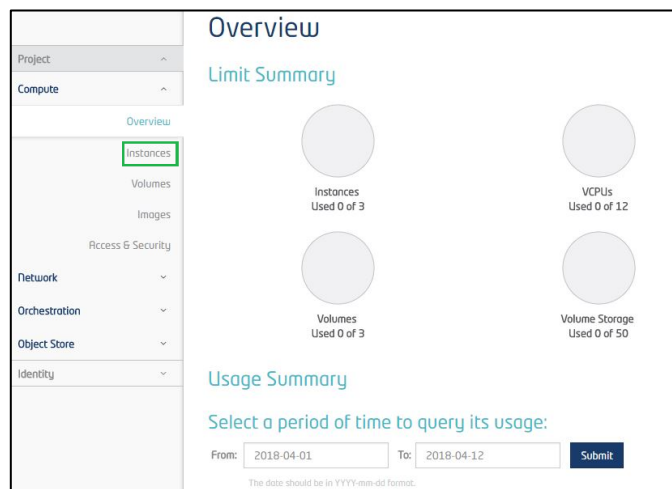
1. Logon the FIWARE Cloud (<https://cloud.lab.fiware.org>) using the credentials provided in the email:



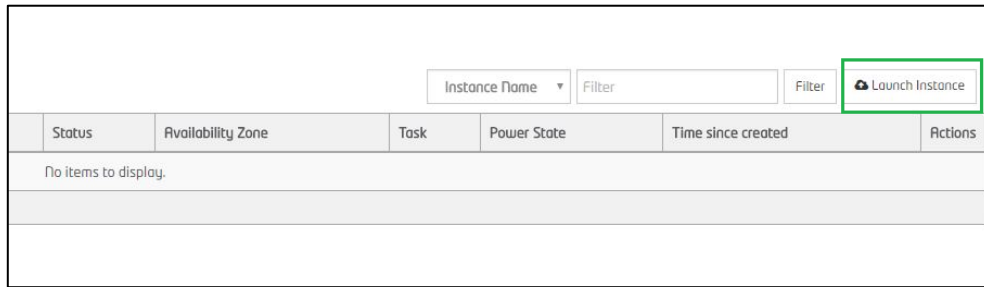
2. You will be presented with the following screen:



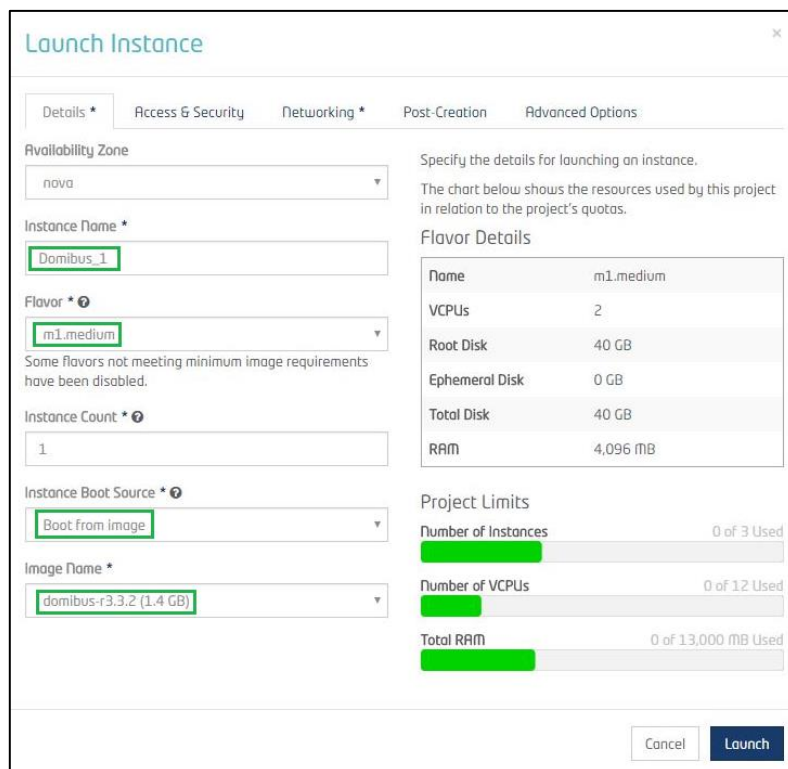
3. Click on Instances:



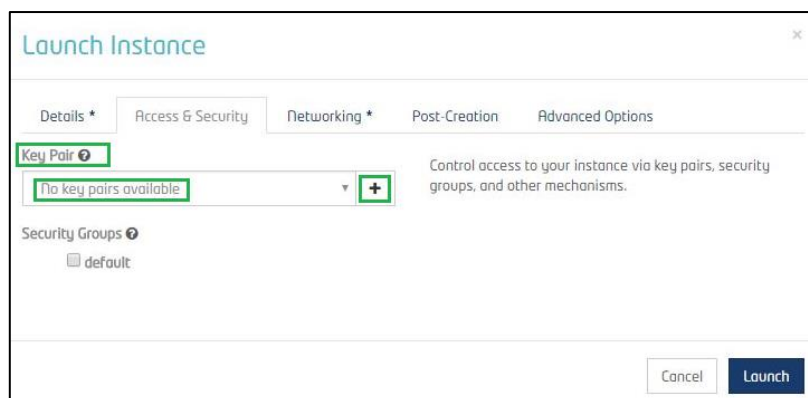
4. Click on Launch Instance



5. Choose a name for the Domibus instance, a **Flavor**, **Boot Source** and the **image** (in this case **Domibus-r.X.Y.Z**). Click on **Launch**:



6. Select the **Access and Security** tab and click on the “+” sign below Key Pair:



7. Create and Paste the Public Key as described:

**Import Key Pair**

Key Pair Name \*

keypair1

Public Key \*

BtQ3aIDXeB/PHYzuWTmu20Fnduu2ubbp0UjBBW3  
 Evrzouw/raK15+L21PmH5dd72cmjDvR+Zi2+9PCl  
 LxxHrVn2La1uaOUmATFD8nrITkROE9LrhVPFeW  
 eZvhkAaMlzV+0a1BrBRFTaOvXadKallFwOLu7ROl  
 ZMhKQBZGRaCZQr8/Yfsb42P2DP1aY13dDRbi+mE  
 anmuRxiilWjBSNhzS1kUmZzRveq7a9Xs58X/BOL3  
 1VXSCi/mfmbMuipLWkzsaBz3WDF4DM4WLXGuh  
 xh1b+I6Pw2GEDk15+5LUUqa5m/nR4Bfk0owuHnS  
 RCeT2ladisHU9artUcFgSMQl  
 berrama@b4edelliveru02

This field is required.

**Description:**  
 Key Pairs are how you login to your instance after it is launched.  
 Choose a key pair name you will recognise and paste your SSH public key into the space provided.  
 SSH key pairs can be generated with the ssh-keygen command:  

```
ssh-keygen -t rsa -f cloud.key
```

  
 This generates a pair of keys: a key you keep private (cloud.key) and a public key (cloud.key.pub). Paste the contents of the public key file here.  
 After launching an instance, you login using the private key (the username might be different depending on the image you launched):  

```
ssh -i cloud.key <username>@<instance_ip>
```

Cancel **Import Key Pair**

**Remark**

*The Private Key must be immediately kept in a safe location after it has been generated.*

8. Public Key is successfully imported:

**Launch Instance**

Details \* Access & Security Networking \* Post-Creation Advanced Options

Key Pair **keypair1** Control access to your instance via key pairs, security groups, and other mechanisms.

Security Groups  default

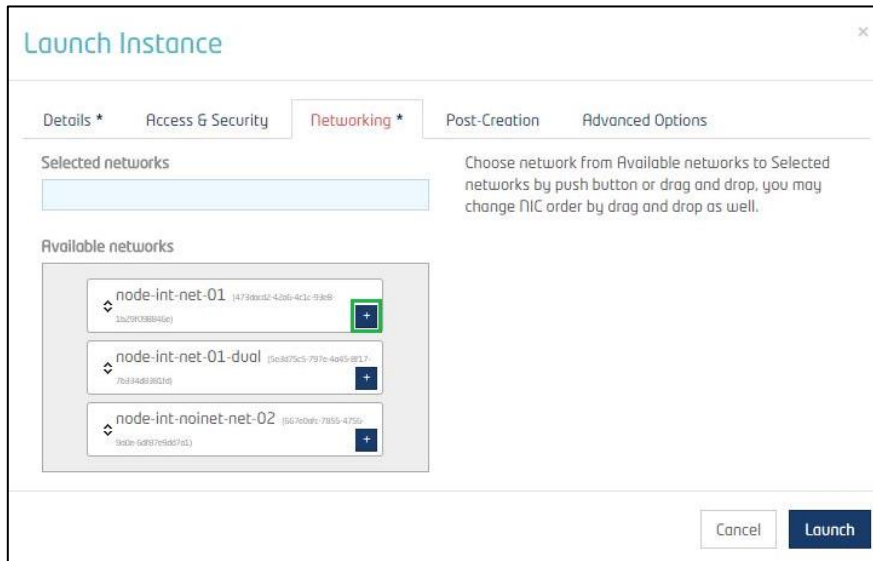
Cancel **Launch**

**Success: Successfully imported public key: keypair1**

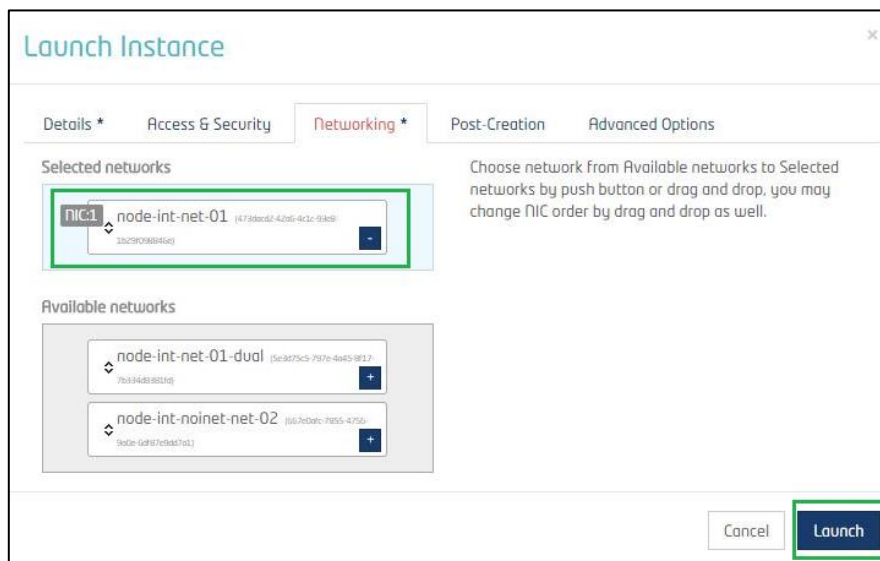
Instance Name	Filter	Filter	Launch Instance
Task	Power State	Time since created	Actions

2.3.2. Network Setup

1. Select the **Networking** Tab and click on the “+” sign next to the required network (e.g: **node-int-net-01**) to select the network:



2. Click on **Launch** once the network is selected:



3. The Domibus instance will be shown, with as task “Spawning”:

Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
Domibus_1	domibus-r3.3.2		m1.medium	cloud	Build	nova	Spawning	No State	0 minutes	Associate Floating IP

- Once spawning is done, the instance status is **Active** with a (local) IP address assigned:

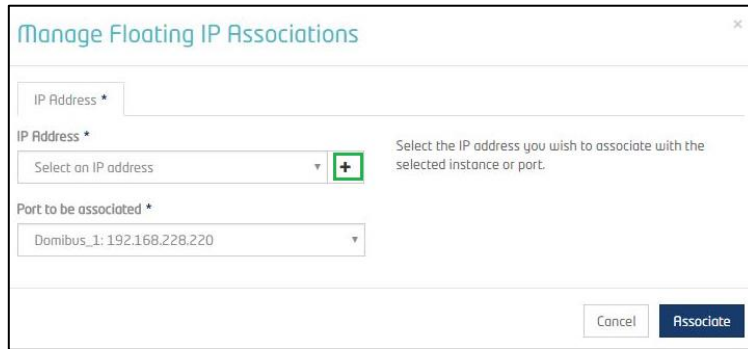
Instances										
Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
Domibus_1	domibus-r3.3.2	192.168.228.220	m1.medium	keypair1	Active	nova	None	Running	0 minutes	Create Snapshot

**2.3.3. Public IP Address configuration**

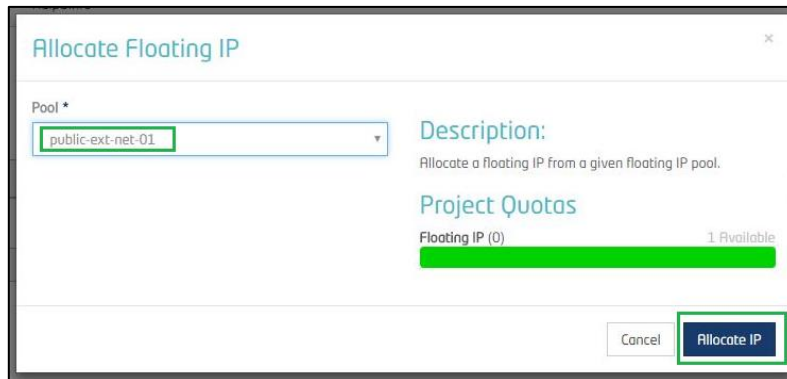
- A public IP address has to be associated to the instance just created. Click on **Associate Floating IP** from the **Actions** menu:

The screenshot shows a close-up of the 'Actions' column from the table above. The 'Create Snapshot' dropdown menu is open, and the 'Associate Floating IP' option is highlighted with a green box. Other options in the menu include Attach Interface, Detach Interface, Edit Instance, Edit Security Groups, Console, View Log, Pause Instance, Suspend Instance, Shelve Instance, Resize Instance, Lock Instance, Unlock Instance, Soft Reboot Instance, Hard Reboot Instance, Shut Off Instance, Rebuild Instance, and Terminate Instance.

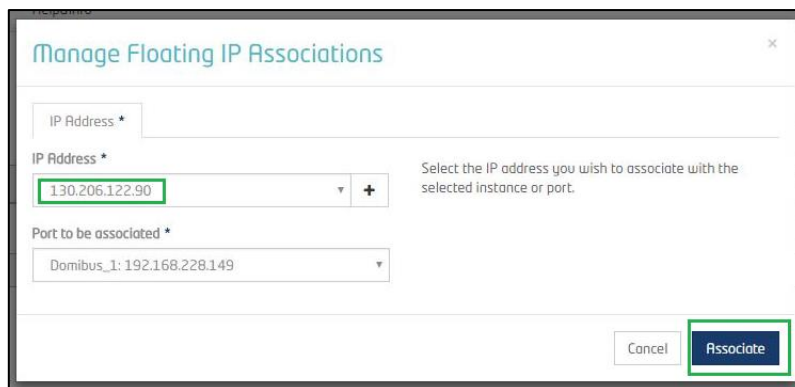
- Click on the “+” sign to get a Public IP address:



- Choose the **public-ext-net-01** option, from the pull down menu and click on **Allocate IP**:



- A public IP address is proposed (e.g: **130.206.122.90**): click on **Associate** to select it:



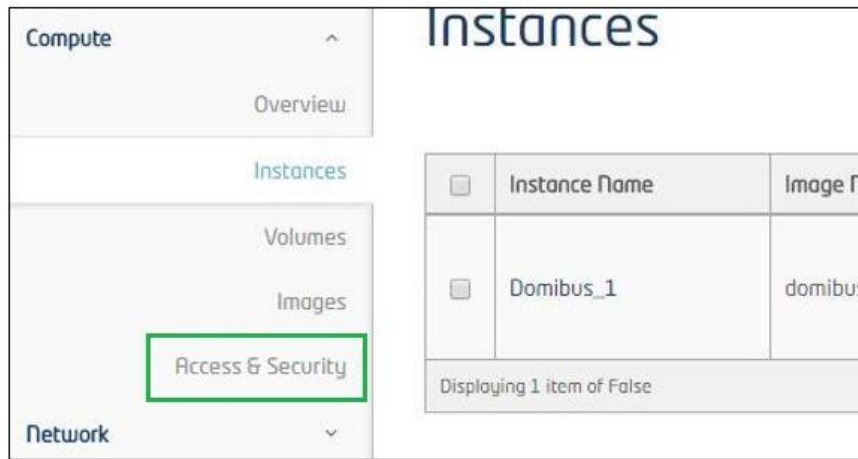
- The Instance is now shown with the new selected details (if not, click on the “Refresh” button):

Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
Domibus_1	domibus-v3.3.2	192.168.228.220 Floating IPs: 130.206.122.90	m1.medium	keypair1	Active	nova	None	Running	7 minutes	Create Snapshot

**2.3.4. The Security Options:**

- Use the **Access & Security** menu to create a **Security Group**:

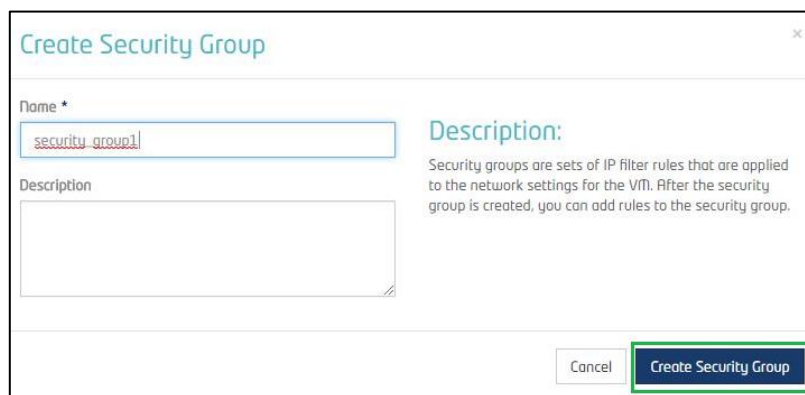




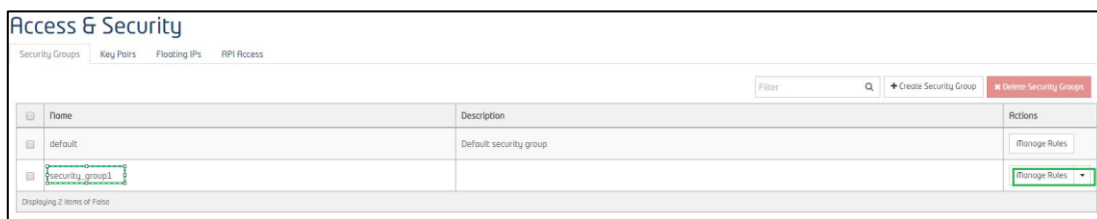
2. In the **Security Groups** tab, click on **Create Security Group**:



3. Enter a **Name** for the new Security Group and click on **Create Security Group**:



4. The new security group is now listed together with the **Default** security Group. Click on **Manage Rules** for the newly created Security Group (e.g: security\_group1):



5. Click on **Add Rule**:

Manage Security Group Rules: security\_group1 (ea02713e-0687-4dae-8126-88dc2ba81bb4)

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
<input type="checkbox"/>	Egress	IPv4	Rng	Rng	0.0.0.0/0	-	Delete Rule
<input type="checkbox"/>	Egress	IPv6	Rng	Rng	::0	-	Delete Rule

Displaying 2 items of False

6. Set the rules for port **22** as shown below and click on **Add**:

### Add Rule

**Rule \***

**Direction**

**Open Port \***

**Port**

**Remote \***

**CIDR**

**Description:**

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

**Rule:** You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

**Open Port/Port Range:** For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

**Remote:** You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

7. Add the same rule for port **8080** as shown below:

### Add Rule

**Rule \***

**Direction**

**Open Port \***

**Port**

**Remote \***

**CIDR**

**Description:**

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

**Rule:** You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

**Open Port/Port Range:** For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

**Remote:** You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

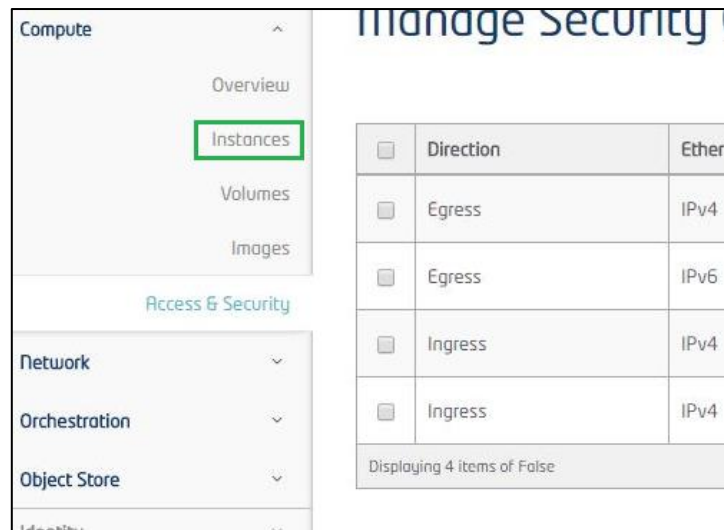
8. The resulting rules are shown:

Manage Security Group Rules: security\_group1 (ea02713e-0687-4dae-8126-88dc2ba81bb4)

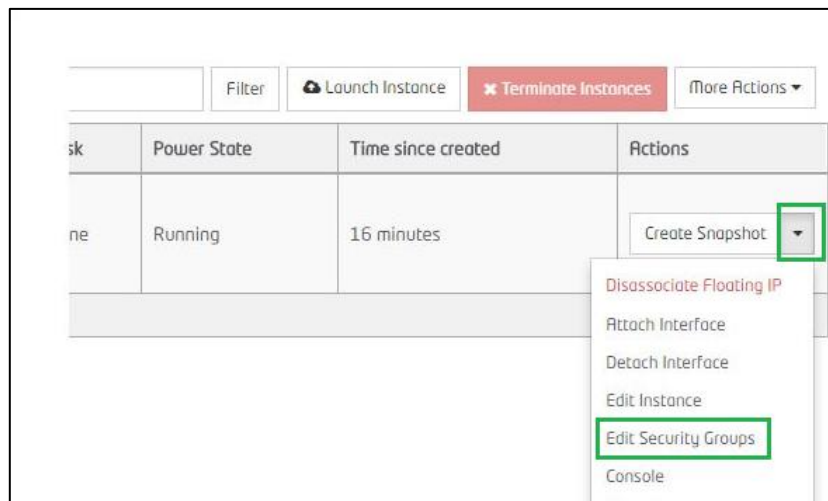
Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
Egress	IPv4	Any	Any	0.0.0.0/0	-	Delete Rule
Egress	IPv6	Any	Any	:::0	-	Delete Rule
Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-	Delete Rule
Ingress	IPv4	TCP	8080	0.0.0.0/0	-	Delete Rule

Displaying 4 items of False

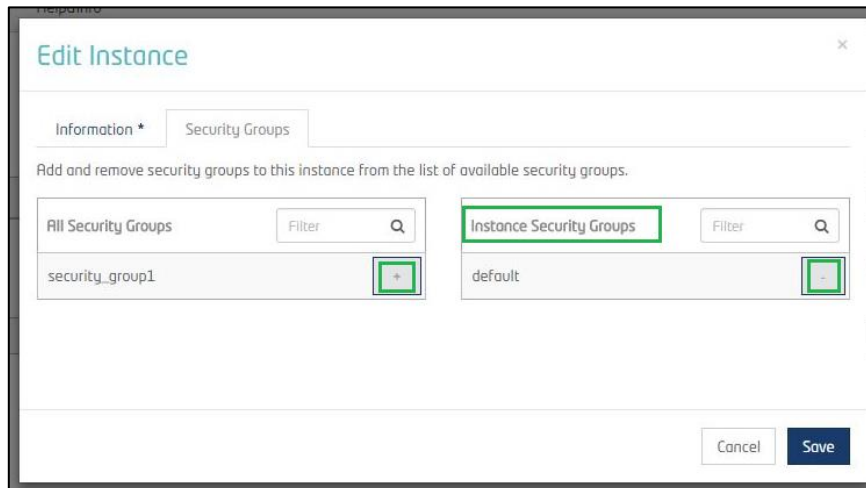
9. To attach the new security group to the Domibus Instance, click on the **Instances** option:



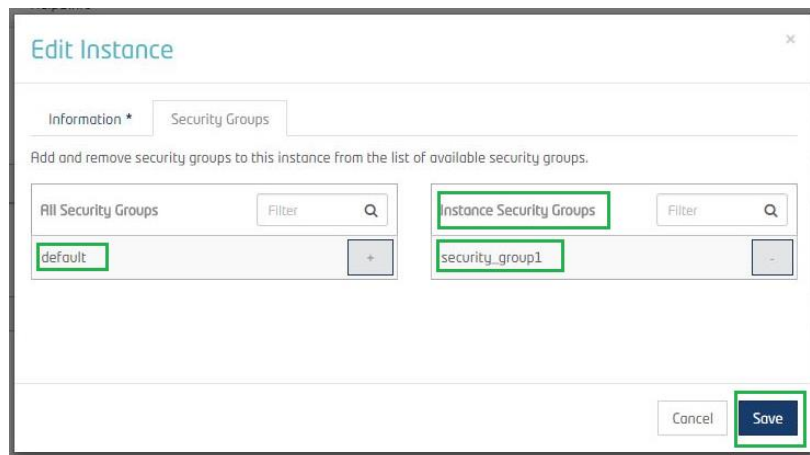
10. Click on the **Create Snapshot** Pull Down Menu to get to the **Edit Security Groups** Sub-Menu:



11. Use the “+” and “-” signs to set the **Instance Security Groups**:



12. The created Security Group (e.g. security\_group1) must be attached to the **Instance Security Groups** as shown here:



13. Click on **Save**.

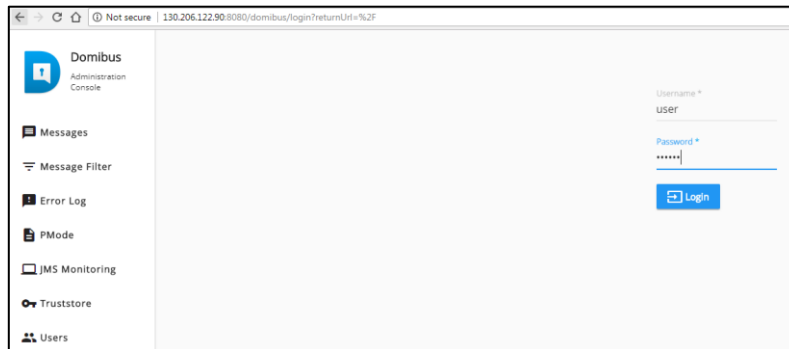
### 3. LAUNCHING DOMIBUS AND TESTING

1. Launch your Domibus in an internet browser, using the public address associated previously:  
Example for IP=130.206.122.90 used in our latest test:

<http://130.206.122.90:8080/domibus>

Username: **user**

Password: **123456**



- Download the **SoapUI** project and the **PMode** configuration from the following address:  
<https://catalogue-server.fiware.org/enablers/electronic-data-exchange-domibus/instances>

Secure | <https://catalogue-server.fiware.org/enablers/electronic-data-exchange-domibus/instances>

**FIWARE Catalogue**

2018-05-16  
 Contact Person:  
 CEF Support Team  
 Email: CEF-EDELIVERY-SUPPORT@ec.europa.eu  
 Phone: +32 2 299 09 09

Send feedback

**Service Endpoint (URL):**  
<http://domibus.lab.fiware.org:8080/domibus>

**Specific Features:**  
 user: user  
 password: 123456

**Testing:**  
 This testing instance is configured via a **Processing Mode (pMode)** file to send messages to the AP in eDelivery's Connectivity Test Platform

**SoapUI**  
 A SoapUI project is available to help you test the sending of messages using this instance. The steps are:

- save the SoapUI project ZIP to your disk and unzip it
- open SoapUI and import the project (File->Import->browse to AS4ConnectivitySoapTest-soapui-project\_gw9.xml)
- open AS4ConnectivitySoapTest->BackendService\_1\_1SoapBinding->SendMessage->Request 1
- click on the green button to send a message; the result will be a unique messageID
- in the browser, go to <http://domibus.lab.fiware.org:8080/domibus> to check your message was ACKNOWLEDGED

**CURL**  
 Test messages may be sent also using CURL.

**Send message**  
 Save the `sendMessage.txt` and run the command:  

```
$ curl --header "Content-Type: text/xml;charset=UTF-8" --header "SOAPAction: sendMessage" --data @sendMessage.txt http://domibus.lab.fiware.org:8080/domibus/services/backend -v
```

**Download message**  
 Save the `downloadMessage.txt` and run the command:  

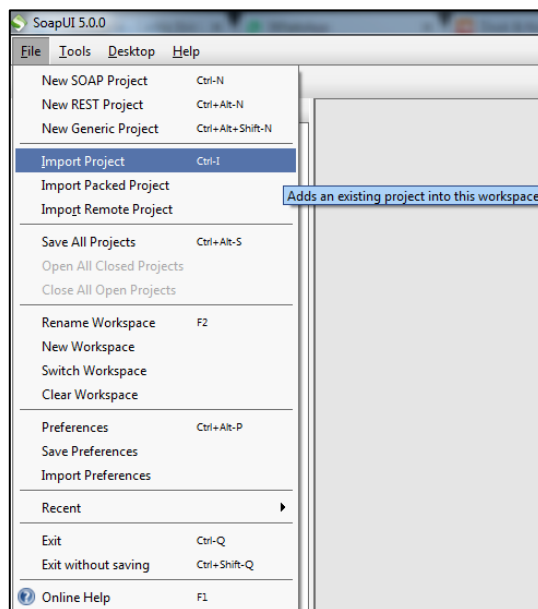
```
$ curl --header "Content-Type: text/xml;charset=UTF-8" --header "SOAPAction: downloadMessage" --data @downloadMessage_0.txt http://40.115.23.114:8080/domibus/services/backend -v
```

Take into account that this is an instance shared among all its users **That means that your actions on the instance could impact to other users or viceversa.** In this sense, this instance is to be used only to do prospective testing and to analyze the feasibility of the GEI to your purposes.  
 In order not collapse the instance due to uncontrolled usage please make sure your payload size is not greater than 100 MB (base64 encoded) and that you do not send more than 10 messages per minute.

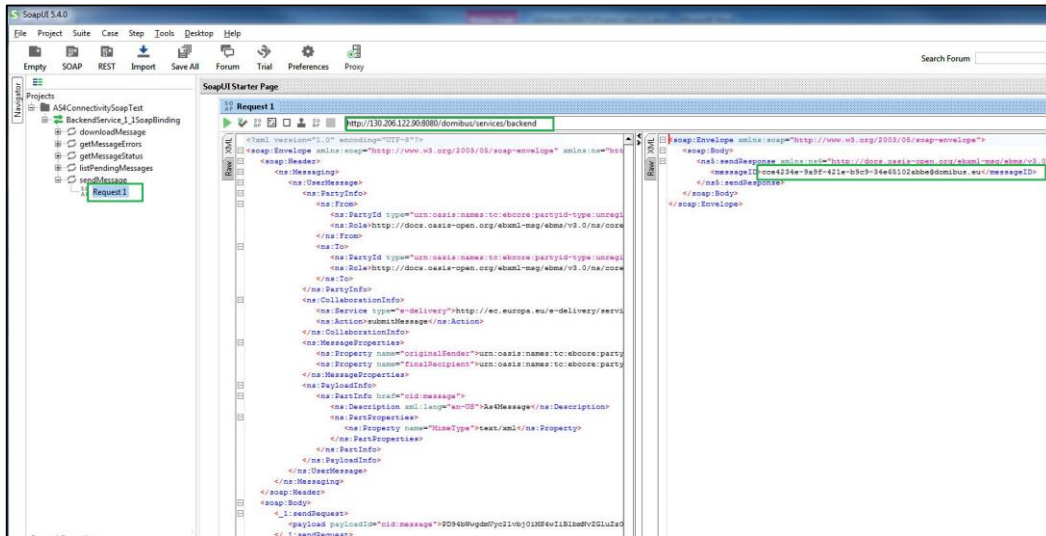
**Downloads:**

- curlSOAPrequest.txt
- downloadMessage.txt
- sendMessage.txt
- AS4ConnectivitySoapTest-soapui-project\_gw9.xml\_zip

- Open **SoapUI** and import the unzipped SoapUI project (**AS4ConnectivitySoapTest-soapui-project\_gw9.xml**):



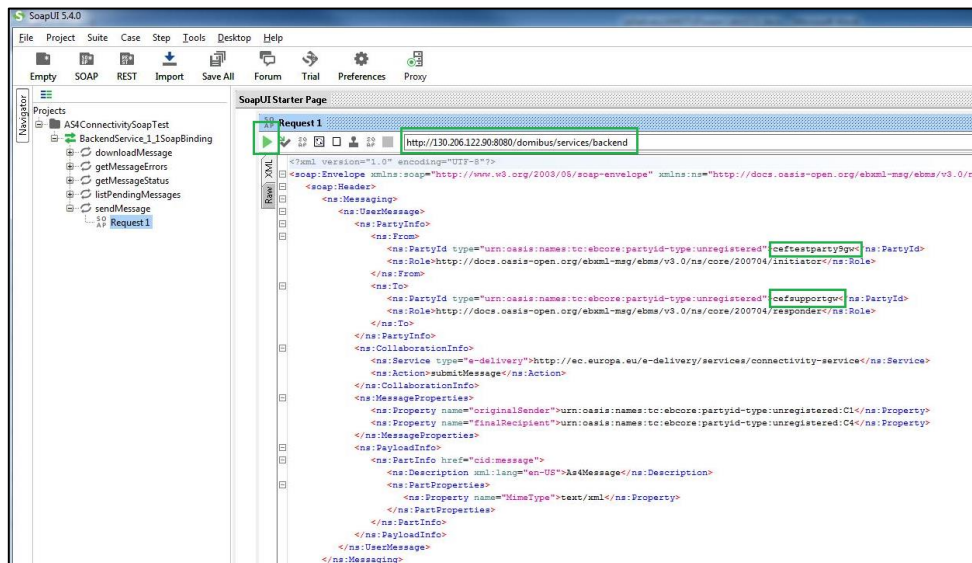
4. Open **AS4ConnectivitySoapTest** → **BackendService\_1\_1SoapBinding** → **SendMessage** → **Request 1**:



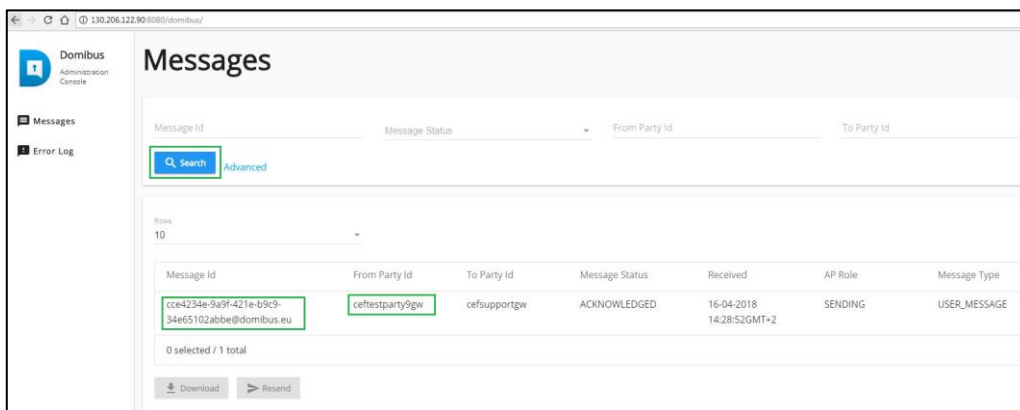
**Remark:**

- You need to use the Public IP Address of your Domibus instance.
- Setup the proxy if needed in SoapUI.

- Click on the green button to send a message. The result will be a unique **messageID** as shown below:



- In your Internet browser, go to your Domibus Admin Console and click on "**Messages**" to check if your message status is "**ACKNOWLEDGED**"



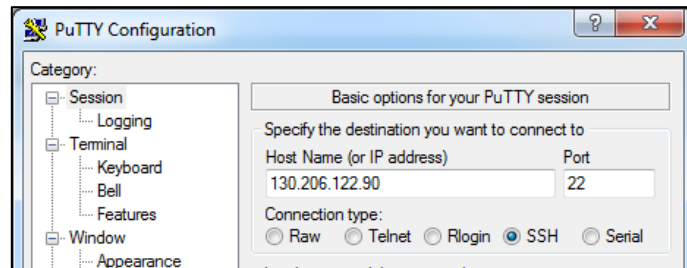


## 4. CONNECT TO SERVER USING SSH

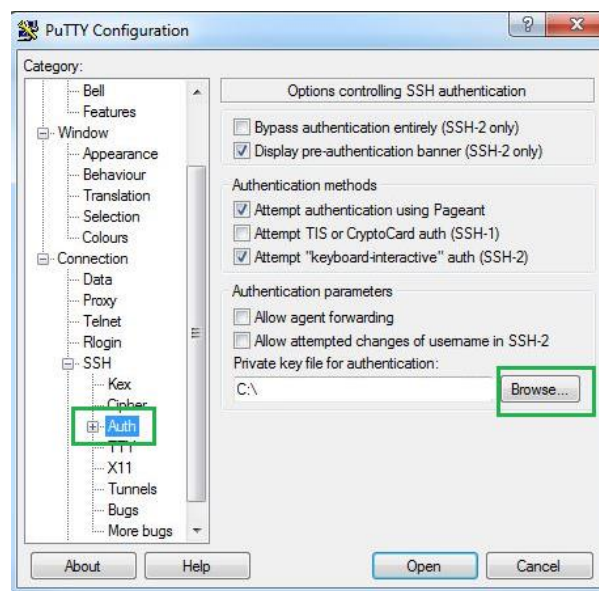
This section explains how to logon to the instance hosting Domibus.

Logon to the server, using putty as an example:

1. Create a putty session using the public IP address of the Domibus Instance:



2. Then use the SSH authentication option and browse to fetch the Private key created in section §6:



3. Save the Putty Session and open it.
4. Login as Ubuntu (no password needed)

**Remark:**

*Use puttygen to import the private key and convert it to a .ppk format.*

## 5. CONTACT INFORMATION

CEF Support Team

By email: CEF-EDELIVERY-SUPPORT@ec.europa.eu

Support Service: 8am to 6pm (Normal EC working Days)