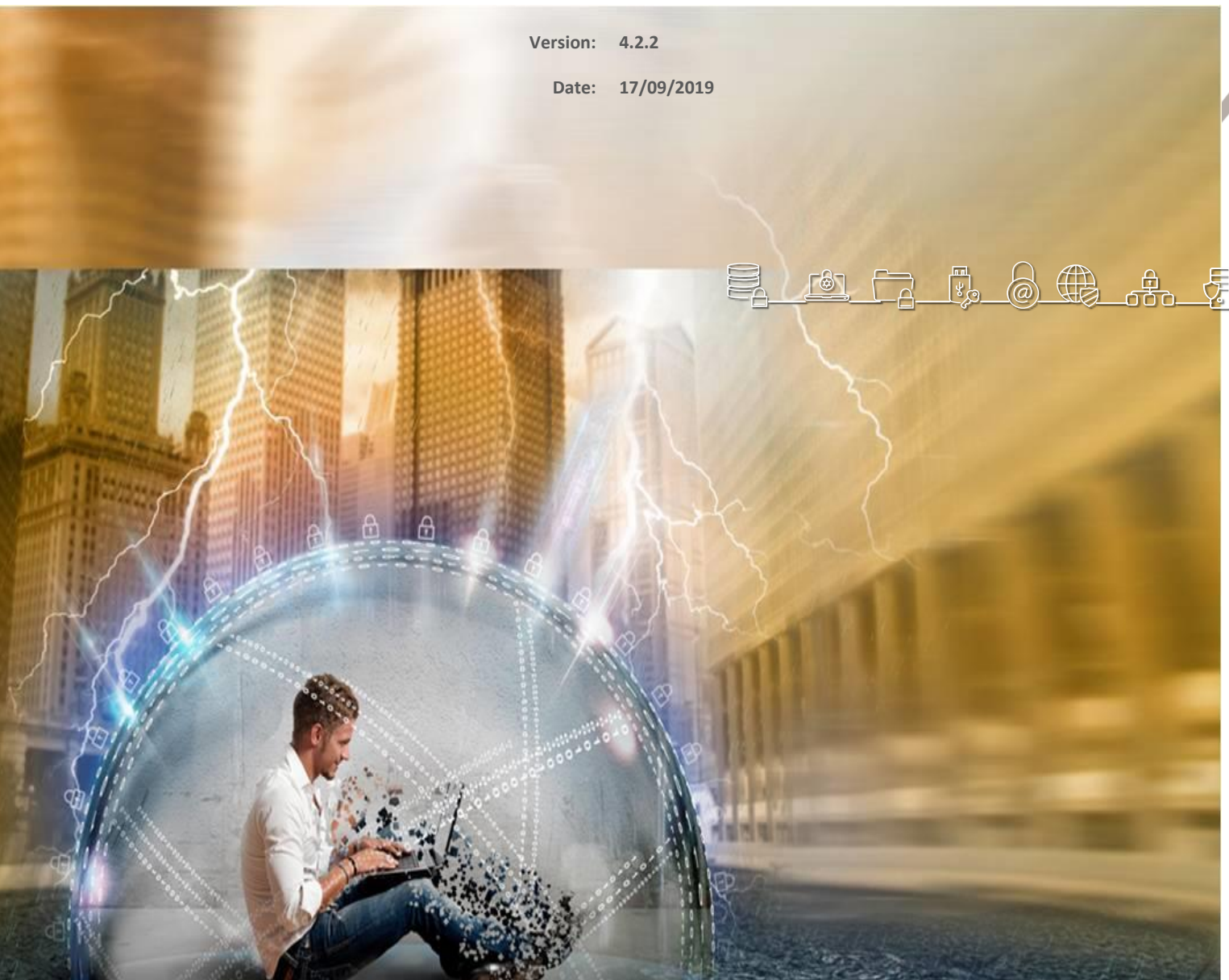


## **CEF: Cybersecurity Digital Service Infrastructure;** Core Service Platform – SMART 2015/1089

### **Installation Manual**

Version: 4.2.2

Date: 17/09/2019





## Contents

<b>1</b>	<b>PREPARATORY STEPS .....</b>	<b>4</b>
<b>2</b>	<b>EXTERNAL FACING SERVICES AND SERVICE URLS.....</b>	<b>5</b>
2.1	INTERNET FACING SERVICES .....	5
2.2	USER INTERFACES .....	5
2.3	OTHER.....	6
<b>3</b>	<b>REQUESTING A CERTIFICATE VIA THE PKI .....</b>	<b>7</b>
3.1	GET THE DOMAIN NAME.....	7
3.2	CREATE THE PRIVATE KEY AND A CSR .....	7
3.2.1	<i>Create the private key.....</i>	7
3.2.2	<i>Create the CSR .....</i>	8
3.3	SUBMIT THE CSR TO THE PKI FOR SIGNING .....	8
3.4	RECEIVE THE SIGNED CERTIFICATE.....	12
3.5	DOWNLOAD THE INTERMEDIATE ROOT CA CERTIFICATE .....	12
3.6	DOWNLOAD THE CA BUNDLE .....	14
3.7	PREPARE YOUR CERTIFICATES FOR INSTALLATION .....	15
<b>4</b>	<b>INITIAL CONFIGURATION.....</b>	<b>16</b>
4.1	IMPORTING THE VM APPLIANCE .....	16
4.2	CONNECTING TO THE VM.....	16
<b>5</b>	<b>INSTALLATION.....</b>	<b>19</b>
5.1	CSP INSTALLER HEALTH VERIFICATION.....	19
5.2	INSTALLATION OF CERTIFICATES.....	20
5.3	CSP INSTANCE REGISTRATION .....	24
5.4	DOWNLOAD OF SYSTEM UPDATES .....	27
5.5	MODULES INSTALLATION .....	32
<b>6</b>	<b>MANAGING CSP .....</b>	<b>34</b>
6.1	STARTING.....	34
6.2	STOPPING .....	37
6.3	UPDATE SMTP CONFIGURATION .....	37
<b>7</b>	<b>SMOKE-TESTING THE INSTALLATION .....</b>	<b>39</b>
7.1	CONNECTING VIA THE "SINGLE SIGN-ON" SERVICE .....	39
7.2	CONNECTING TO INDIVIDUAL SERVICES .....	41
<b>8</b>	<b>ANNEX A: CHANGING SETTINGS OF THE VM .....</b>	<b>54</b>
8.1	EXPANDING THE VM ROOT FILESYSTEM.....	54
<b>9</b>	<b>ANNEX B: JITSY VIDEOCONFERENCING BRIDGE .....</b>	<b>56</b>
9.1	EXTERNAL PORT ACCESSIBILITY .....	56
9.2	BANDWIDTH REQUIREMENTS .....	56
<b>10</b>	<b>ANNEX C: TROUBLESHOOTING CSP INSTALLER .....</b>	<b>58</b>
<b>11</b>	<b>ANNEX D: TROUBLESHOOTING THE CONNECTION TUNNEL TO THE VM .....</b>	<b>59</b>
<b>12</b>	<b>ANNEX E: MANUAL INSTALLATION AND CONFIGURATION OF THE CSP INSTALLER.....</b>	<b>60</b>

## 1 Preparatory steps

This installation manual is a step-by-step guide for the acquisition of the required certificate from the Melicertes PKI service and the installation of your local CSP.

Before proceeding to the installation, please make sure that the following preparatory steps have been taken:

1. You received the hardware requirements for the CSP installation
2. You registered for a CSP installation to the central CSP authority
  - a. You sent the required data and point of contact details
  - b. You sent the IP address that you are going to use for your installation
  - c. Your team data have been entered in the central CSP trust circles
  - d. Your domain has been assigned and registered for the given IP address
3. You received an email confirming the actions in step 2 and the following:
  - a. Your assigned CSP-ID.
  - b. Your assigned melicertes domain in the form of <cspld>.[preprod.]melicertes.eu (e.g. cert-gr.preprod.melicertes.eu)
  - c. Three manuals: Installation manual, Administration manual, User manual available in MeliCertes Github<sup>1</sup>
  - d. A link to download the base VM in OVA format, i.e. AlpineHost-v3.10-PROD.ova <sup>2</sup>

---

### ***Recommended requirements of the VM***

***(More vCPU, RAM and Hard disk could be assigned depending on your usage and needs).***

***Memory: 48 GB***

***Disk:800 GB***

***CPU:16 vCores***

***Internet connectivity***

---

<sup>1</sup> <https://github.com/melicertes/>

<sup>2</sup> Version is indicative and is subject to change

## 2 External Facing Services and Service URLs

The CSP instance during installation and operation will need access to the internet. The CSP instance needs to be able to initiate outgoing connections. After the installation and during operation, the CSP's internet facing services and ports need to be accessible from the Internet. Lastly, the CSP instance provides a set of User Interfaces for its various services that need to be accessible by the users inside the organization only.

**Note:** Domains in the pre-production environment are in the form of \*.<cspld>.preprod.melicertes.eu. Domains in the production environment are in the form of \*.<cspld>.melicertes.eu

### 2.1 Internet Facing Services

The following subdomains/ports need to be accessible from the Internet for incoming connections:

Integration Layer	https://integration.<cspld>.[preprod.]melicertes.eu	TCP 5443 (https)
OwnCloud	https://files.<cspld>.[preprod.]melicertes.eu	TCP 6443 (https)
Jitsi VideoConferencing Bridge	https://teleconf.<cspld>.[preprod.]melicertes.eu	TCP 6443 (https)
Jitsi VideoConferencing Bridge	https://vc.<cspld>.[preprod.]melicertes.eu	TCP 6443 (https)
MISP Server Sync	https://misp-ui.<cspld>.[preprod.]melicertes.eu	TCP 6443 (https)
Jitsi VideoConferencing Bridge – Media TCP	vc.<cspld>.[preprod.]melicertes.eu	TCP 4443 (SSL)
Jitsi VideoConferencing Bridge – Media UDP	vc.<cspld>.[preprod.]melicertes.eu	UDP 10000

**Important Note:** For further details on Jitsi VideoConferencing Bridge network considerations please continue to Annex B: Jitsi VideoConferencing Bridge before progressing further.

While Videoconferencing (Jitsi) and file sharing (OwnCloud) need to be generally open (ports 6443, 4443, 10000 UDP), Integration layer only needs to be accessible by the rest of the CSP instances (port 5443).

### 2.2 User Interfaces

The following subdomains/ports need to be accessible only from within your organization:

Trust Circles	https://tc.<cspld>.[preprod.]melicertes.eu	TCP 443 (https)
OpenAM Admin.	https://auth.<cspld>.[preprod.]melicertes.eu/openam	TCP 443 (https)
Search (Kibana)	https://search.<cspld>.[preprod.]melicertes.eu	TCP 443 (https)
Logs (Kibana)	https://logs.<cspld>.[preprod.]melicertes.eu	TCP 443 (https)
Sharing Policies	https://integration-ui.<cspld>.[preprod.]melicertes.eu	TCP 443 (https)
Anonymization	https://anon-ui.<cspld>.[preprod.]melicertes.eu	TCP 443 (https)
Request Tracker (RT)	https://rt.<cspld>.[preprod.]melicertes.eu/RTIR	TCP 443 (https)

MISP	<a href="https://misp-ui.&lt;cspld&gt;.[preprod.]melicertes.eu">https://misp-ui.&lt;cspld&gt;.[preprod.]melicertes.eu</a>	TCP 443 (https)
Jitsi VideoConferencing Bridge Admin.	<a href="https://teleconf-ui.&lt;cspld&gt;.[preprod.]melicertes.eu">https://teleconf-ui.&lt;cspld&gt;.[preprod.]melicertes.eu</a>	TCP 443 (https)
InteMQ Manager	<a href="https://imq.&lt;cspld&gt;.[preprod.]melicertes.eu">https://imq.&lt;cspld&gt;.[preprod.]melicertes.eu</a>	TCP 443 (https)
Viper Manager	<a href="https://viper-ui.&lt;cspld&gt;.[preprod.]melicertes.eu">https://viper-ui.&lt;cspld&gt;.[preprod.]melicertes.eu</a>	TCP 443 (https)

Note: You can bookmark the above links after replacing the correct <cspld> and adding/removing “preprod” from the URL depending on the environment.

### 2.3 Other

SSH should be accessible only from within your organization:

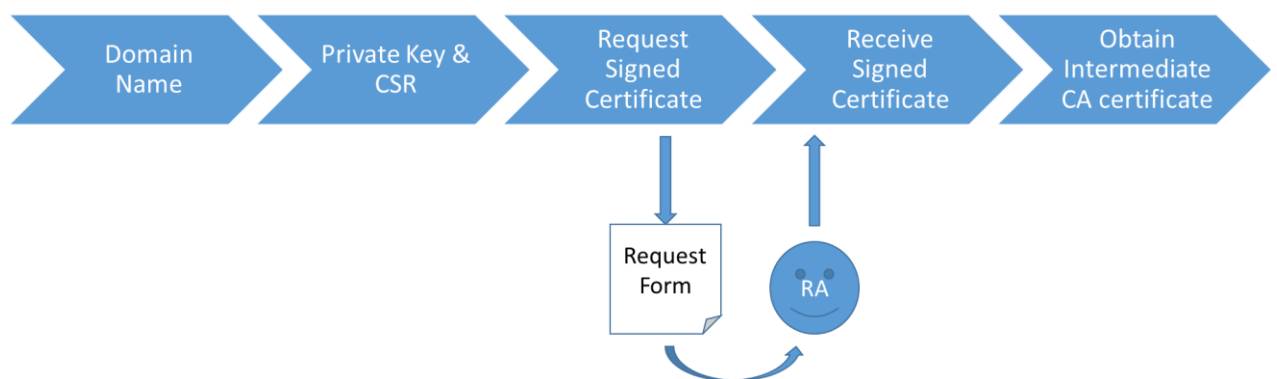
SSH	<a href="https://&lt;cspld&gt;.[preprod.]melicertes.eu">.&lt;cspld&gt;.[preprod.]melicertes.eu</a>	TCP 22
-----	--	--------

### 3 Requesting a Certificate via the PKI

The following text describes the steps to be taken for a CSIRT to obtain a signed certificate for the 'melicertes.eu' domain.

The generic steps are:

1. Get the domain name
2. Create a private key and a CSR
3. Request a signed certificate from the CSR
4. Receive the signed certificate
5. Obtain the Intermediate Root CA certificate



#### 3.1 Get the domain name

The Domain Name that you can use within the context of the MeliCERTes platform will have been determined during the application procedure.

For the remainder of this text, we'll work with the dummy domain name 'bari.test.melicertes.eu' for the examples. The certificate will be for a wildcard: \*.bari.test.melicertes.eu.

#### 3.2 Create the private key and a CSR

The commands below assume you use OpenSSL for creating the private key and CSR. As a convention, the domain name is used as a filename for reasons of clarity.

##### 3.2.1 Create the private key

By executing the following command:

```
openssl genrsa -out bari3.test.melicertes.eu.key 4096
```

We generate a self-signed private key, using the RSA algorithm and a key length of 4096 bits.

3 "bari.test" is a fictional CSIRT domain name used for example purposes

Output will be similar to:

```
Generating RSA private key, 4096 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
```

The new file designated by the option **-out**: “bari.test.melicertes.eu.key” contains the private key.

---

#### **Important Note**

You should **not** generate a private key with a passphrase. MeliCERTes currently does not support this and the reverse proxy installation will fail

---

### **3.2.2 Create the CSR**

To generate the Certificate Signing Request (CSR), we execute the following command (substitute the value of the ‘CN’ field for your assigned domain name):

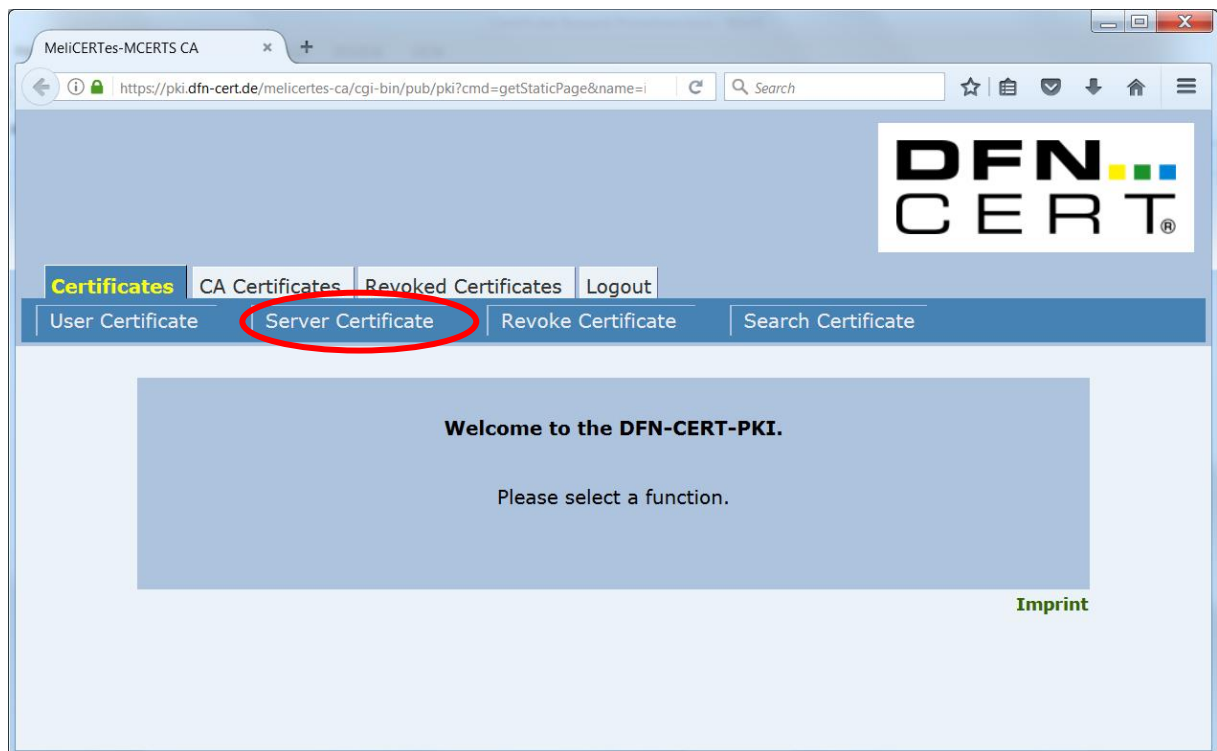
```
openssl req -new -key "bari.test.melicertes.eu.key" \
-out "bari.test.melicertes.eu.csr" -subj \
"/CN=*.bari.test.melicertes.eu/O=MeliCERTes-MCERTS/C=EU/DC=eu/DC=melicertes"
```

Although the above command does not give any output, a new file designated by the option **-out**: “bari.test.melicertes.eu.csr” contains the resulting CSR in the current directory.

### **3.3 Submit the CSR to the PKI for signing**

Go to “<https://pki.dfn-cert.de/melicertes-ca/cgi-bin/pub/pki>”. The Welcome screen is shown. Select “Server Certificate” on the “Certificates” tab.





Select "Server Certificate" on the "Certificates" tab.

The “Request a Server Certificate” screen is shown.

1. Select the CSR file with the “Browse... button”.
2. Choose “LDAP Server” as the profile (this will ensure you get a certificate which can be used both for mutual service authentication and for serverside encryption within your installation later on).
3. Fill in the Name and Email fields (these will be used to validate the signing request AND communicate the results).
4. Choose a PIN which is easy to remember (it is needed to work with the certificate later on).
5. Click “Continue”.

The “Request a Server Certificate - Confirmation” screen is shown.

**Request a Server Certificate - Confirm**

Please check your data.

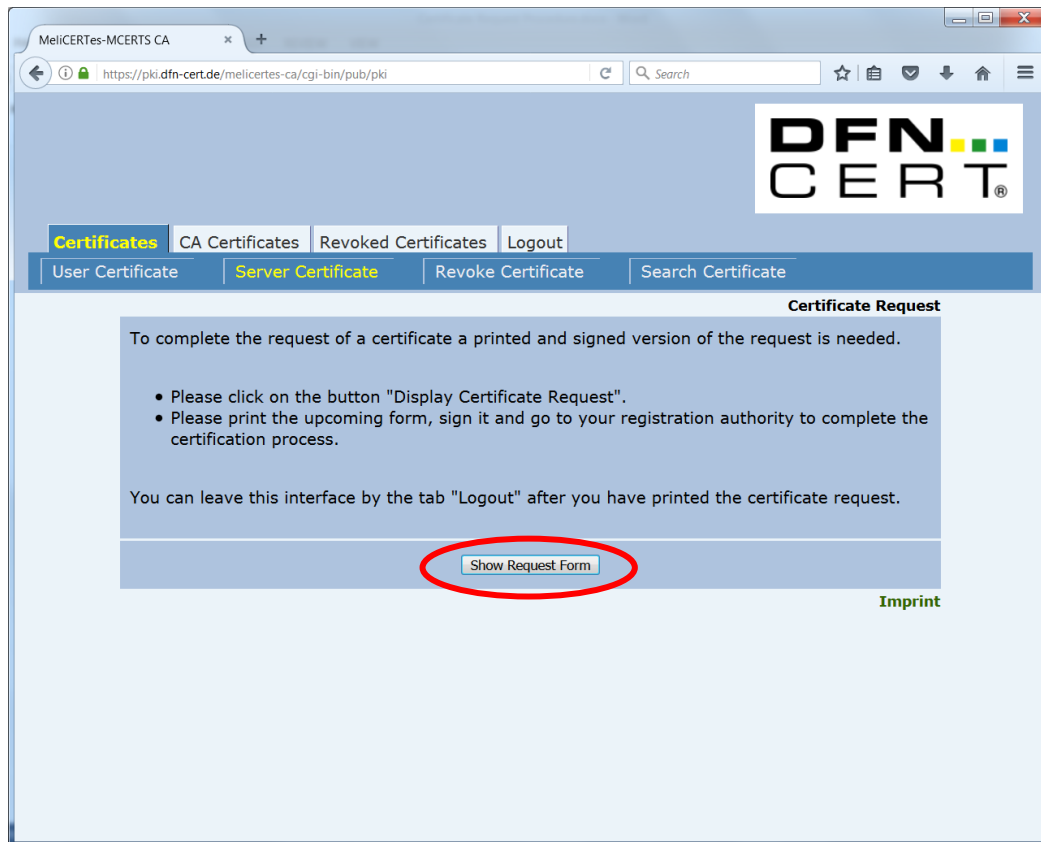
**PKCS#10 Request** -----BEGIN CERTIFICATE REQUEST-----  
MIICWjCCAAoCAQAwFTEiMCAGAlUEAwZRI5iYXJpLnRlc3QubWVsaWN1cnRlcY51  
dTEaMBGAlUECgRTWVsaUNFulRlcY1NQ0VSFVMxCzAJBgNVBAYTAkVVMRiEAYK  
CZImiZPyLGBGRYCYCZUxGjAYBgqJkiaJk/IsZAEZFgptZWxpY2VydGVzMIIBIjAN  
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGKCAQEA2R9S9ejBIUaTbSSuNPW01oo2CoWV  
qyOya8EK1ULVMRpgQy+o2wpleh3LCeNTEiIRxleF9rOi3SwgPl9Cf7qB9KNyG8S8  
gUXn6PpkeyXGUlMwG9/DC3az/EywmWB7ckiksZ781xv5k9EL8nKd3kVls4zFjeP2  
Wnq91w4AUoqrq0EnHJAZZlkoqsgk1lHjFuoA2oUU8kvyKshRuvUggHsgHMjuwna+  
oorHdH/s1WfBi95v9ZnimEGNJXpsqSNdz1vtJz/zIHWq1RctliyyotDtBHwJHoXP  
ZGhSaaopfAhNddUXpMz2b9fSURGrH1M3X8H9zdAa6bfnNq2TwB4zvW1WDWIDAQAB  
oAAWDQYJKoZIhvcNAQELBQADggEBADEAc0UV99r53cSBMtXL1Hggug8kbMHRp1bf  
B5wE27AaMwOYzq51/ZeE91bqjwvhw6tqemRUdiNUwggGQhr2Pm4rQ5ROITDyPhG9  
6KRL1K7CvBYnzN8W3xI2fzZH2Ww4875J2VHez2hMXrDBPqMjNExbmw2QV4M27IHW  
zpcJVdWHyCmPrm10AjUiJwfcnC9Q2MeqefqektzvNQhPTJfNJBIRCeW+sGhuVywS  
jWsljQghFuge7VZzC/jidF44qjF//chG96BMcrapHSMu0n13ECMHkdWZPMcswj11  
MxzLACqYby5BI2UV+V+J0iZIgnUrOPE+g6+P0GUz3/KLQb2jbLo=  
-----END CERTIFICATE REQUEST-----

Certificate Type	LDAP Server
Public key algorithm	rsaEncryption
Keysize	2048
Distinguished Name	CN=*.bari.test.melicertes.eu,O=MeliCERTes-MCERTS,C=EU,DC=melicertes,DC=eu
Subject Alternative Name	DNS:*.bari.test.melicertes.eu
Publish	No
Name (first and last name)	Bart van Riel
Email	bart.van.riel@capgemini.com
Department	

Change Confirm

Validate the information on it. If anything is out of order, click “Change” and you will be taken back to the “Request a Server Certificate” Screen. If everything is Ok, click “Confirm”.

The “Certificate Request” confirmation screen is shown. Your request has now been recorded. However, additional paper validation by the Registration Authority (RA) is needed.



Choose “Show Request Form”, print the resulting PDF file, fill out the necessary details and submit the filled out and signed form (in scanned electronic form) to the helpdesk as a “service request”. As a subject please enter: “Server Certificate Request - <cspld>”.

### 3.4 Receive the signed certificate

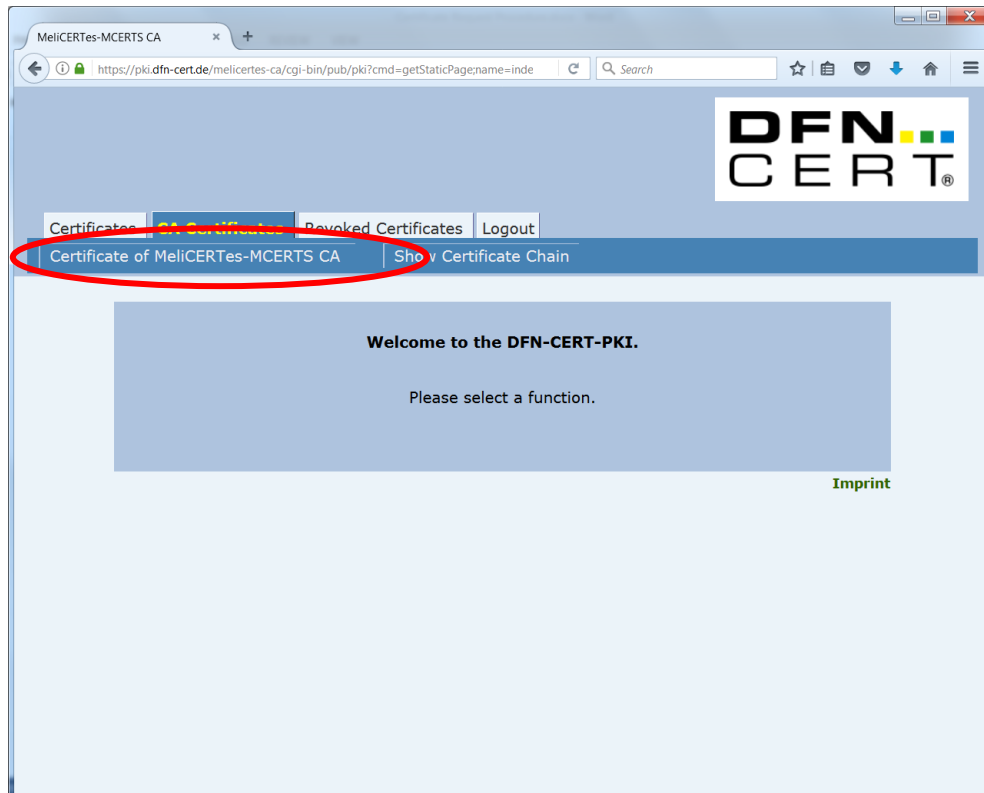
After the certificate request has been approved by the RA, you will receive an email containing the certificate as attachment (in the form of a \*.pem file). Store the certificate as desired.

You will also need a copy of this file with the extension “.crt” for the installation procedure. Copy the .pem file and rename it with the “.crt” extension (e.g. “Signed SSL Certificate.crt”).

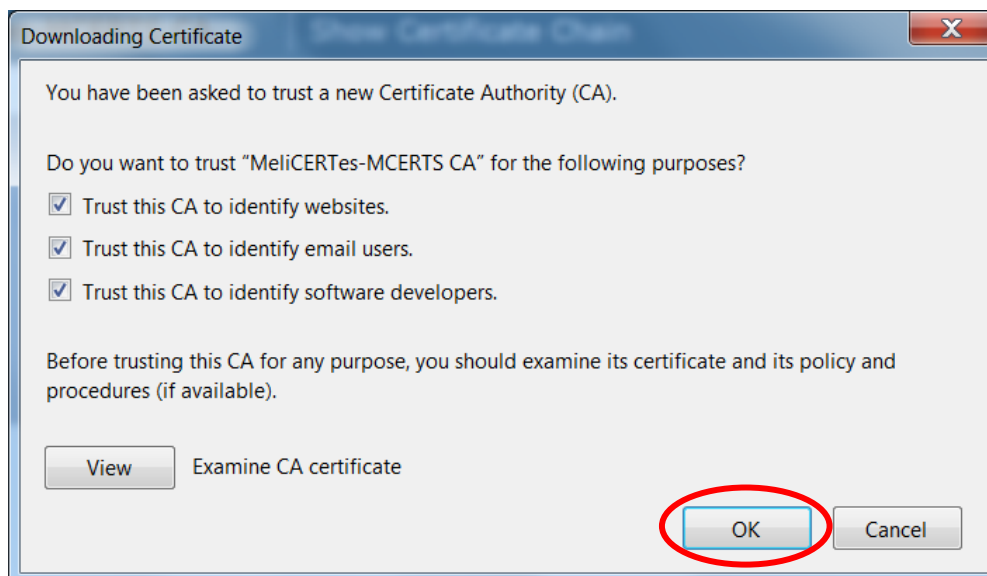
### 3.5 Download the Intermediate Root CA certificate

Click on the deeplink for “importing the CA certificate” which is in the e-mail which included the certificate. The “CA Certificates” tab of the PKI site is shown.

Click on the tab “CA Certificates” and then choose “Certificate of MeliCERTes-MCERES CA”.



In the resulting dialog box, select all checkboxes and click “OK”.



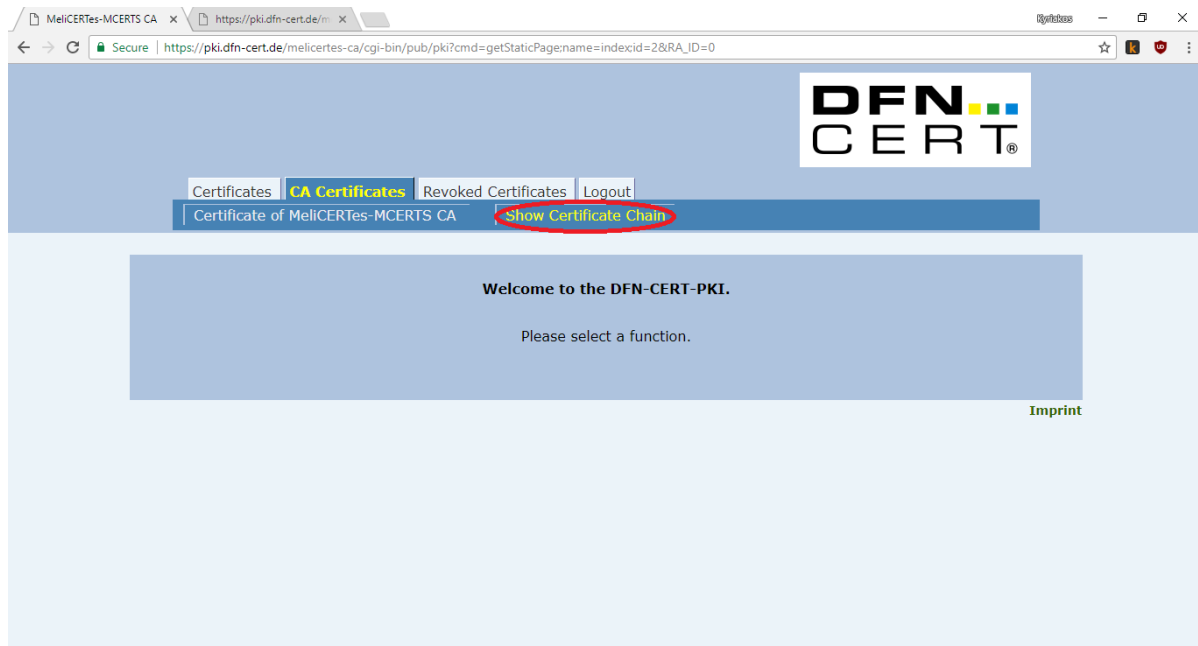
The CA certificate is now silently installed into the web browser. To retrieve it, it needs to be exported.

For Firefox, perform the following steps:

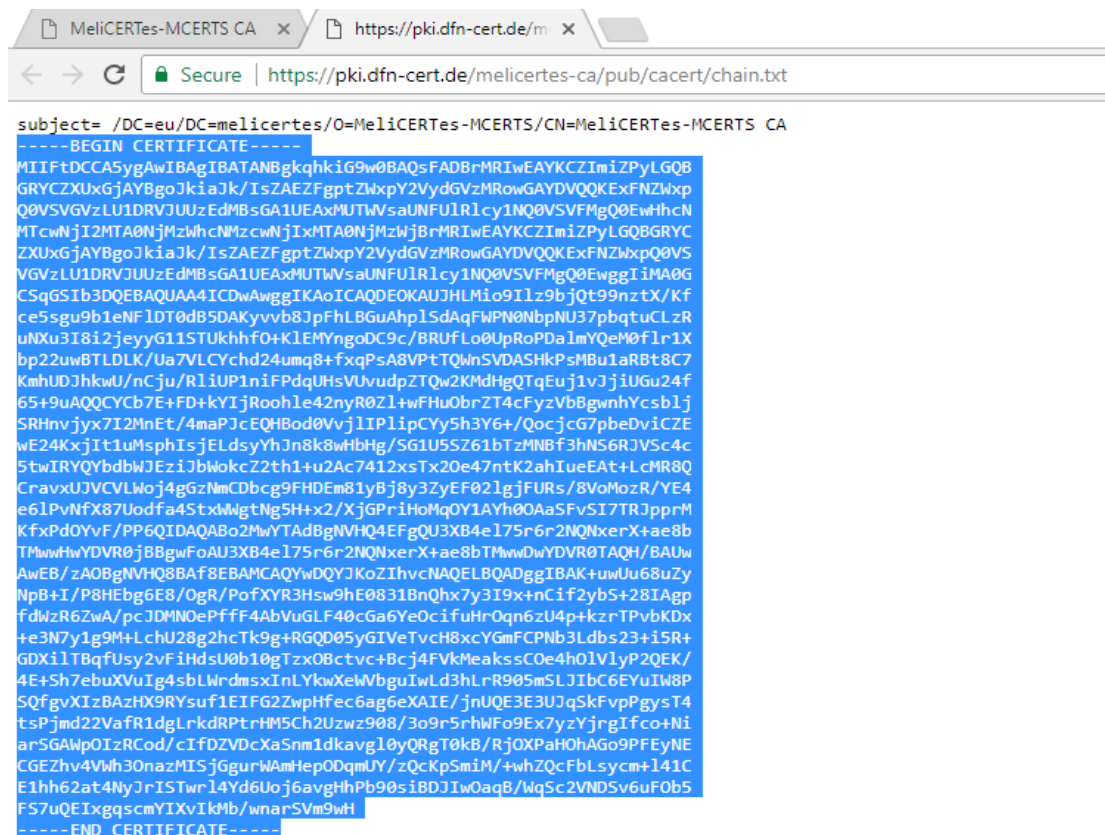
- Go to the “Options” page via the menu
- Choose “Advanced” → “View Certificates”
- Under “Authorities”, find the “MeliCERTes-MCERES” entry and select the “MeliCERTes-MCERES CA” certificate
- Choose “Export...” and save the certificate where desired.

### 3.6 Download the CA bundle

Click on the tab “CA Certificates” and this time choose “Show Certificate Chain”



A new tab will open with the certificate chain. Copy **only** the text starting with “-----BEGIN CERTIFICATE-----” and ending with “-----END CERTIFICATE-----” as shown in the picture below. Make sure you leave the first line out. Paste the text to a text file and save the file with the extension .crt (e.g. “CA Bundle.crt”). You will need this file at a later stage of the installation.



### 3.7 Prepare your certificates for installation

During the installation of the CSP, you will need the following three files:

1. The CA Bundle that you created in section 3.6. File extension “.crt”. File name “CA Bundle.crt”
2. The signed SSL certificate that you got from the Registration Authority, described in section 3.4. File extension “.crt”. File name “Signed SSL Certificate.crt”
3. The private key that you created in section 3.2. File extension “.key”. File name “Private SSL Key.key”

## 4 Initial configuration

### 4.1 Importing the VM appliance

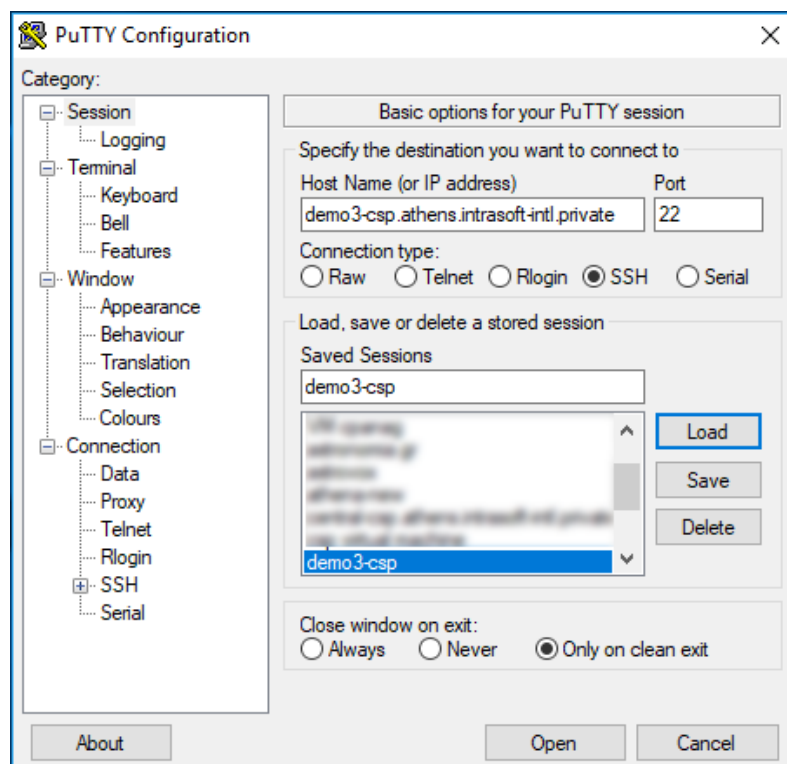
An Open Virtualization Archive (OVA file) has been distributed and contains the original VM for this project. Please note that the distributed OVA is most probably not up to date, after the initial installation you will need to manually run the command `apk --no-cache update` to incorporate security updates. This OVA has settings for memory and CPUs that need to be adjusted, according to specifications previously communicated. It is advised that the administrator revise vCPU, RAM and Hard disk assigned prior to powering up the VM and continuing with the installation steps mentioned below. In the case of the ESXi "Import from OVA..." option, the ESXi system prompts to modify settings before the machine boots. More detailed information can be found in Annex A: Changing settings of the VM.

**Important:** the OVA has *very low memory and CPU* configuration and **is not possible to complete the installation successfully** using the defaults. Please refer to Annex A: Changing settings of the VM for instructions on how to resize the VM to proper size for CSP use.

### 4.2 Connecting to the VM

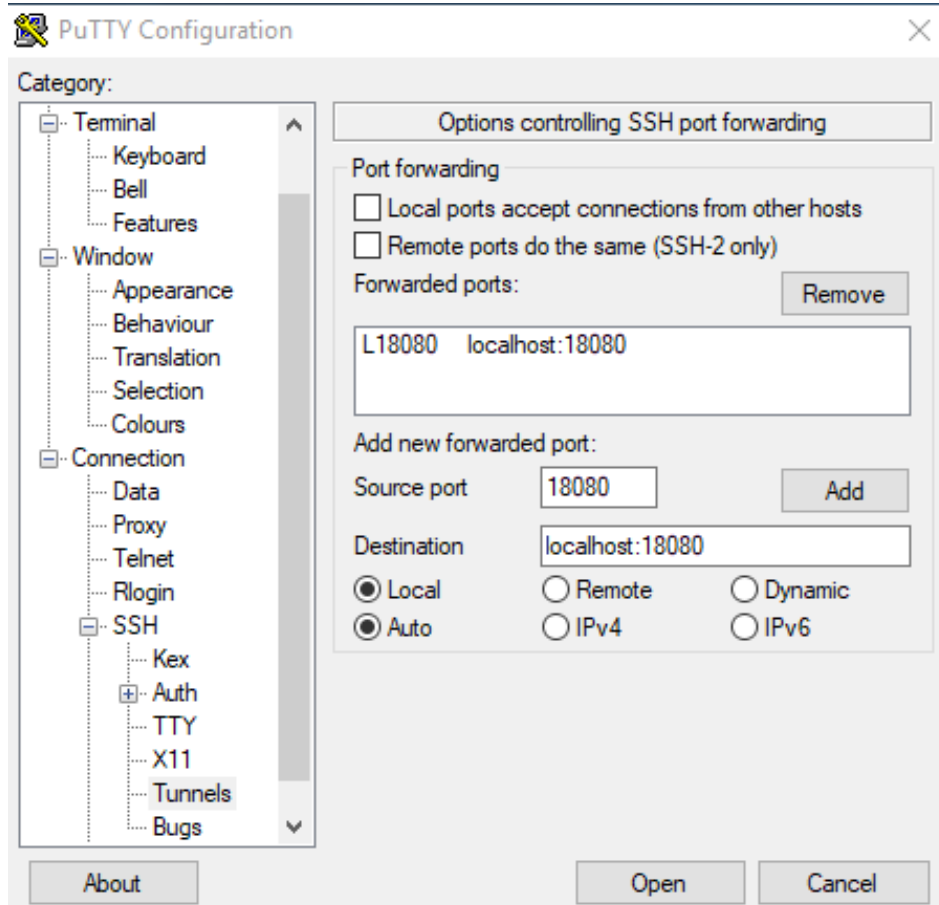
When the guest machine boots, the user should connect via SSH to the guest machine while at the same time creating an SSH tunnel between the guest machine and their computer. This is necessary so the user web browser can access the GUI installation.

This can be accomplished using either a GUI SSH client such as PuTTY or a Linux terminal. The SSH server listens to the default port (22). The default machine credential for user root is "systempass". It is advised that the administrator changes this immediately after first login. The SSH tunnel essentially allows the user to access a port on the guest machine over SSH. The port that needs to be accessed on the host machine is 18080. For simplicity, it will be mapped to local port 18080 but the user can choose otherwise.





In the case of using **PuTTY**, the user should enter guest machine hostname and port 22 in the initial screen (session) then save the SSH connection as a session. The user must then use the left-side panel and navigate to “Tunnels”. The user should enter 18080 to Source port and localhost:18080 to the Destination and then click the Add button. By clicking the “Open” button a new connection is made. The user should login using the root credentials mentioned above and PuTTY will auto-create the tunnel.



In the case of using a Linux terminal, the SSH connection with the tunnel can be created using the following command format:

```
ssh root@<guestmachinehostname> -L 18080:localhost:18080
```

where <guestmachinehostname> is the hostname or IP of the guest machine.

The system will request the root password. After entering the root password, the user is logged in to SSH and the tunnel has been created.

```
andreas@andreasubuntu:~$ ssh root@demo3-csp.athens.intrasoft-intl.private -L 18080:localhost:18080
root@demo3-csp.athens.intrasoft-intl.private's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

demo3-csp [~]#
```

Please note that in both the case of Putty and the terminal SSH client, first-time connections to the guest machine will present a prompt to confirm the authenticity of the host. The user should accept the presented key and the notification will not be presented again when using the same client on the same computer.

```
andreas@andreasubuntu:~$ ssh root@demo3-csp.athens.intrasoft-intl.private -L 18080:localhost:18080
The authenticity of host 'demo3-csp.athens.intrasoft-intl.private (10.240.125.26)' can't be established.
ECDSA key fingerprint is SHA256:ZblmN86b+uKfV0ncLDqTlSF4KGf7CdSQzkBTEwRweUA.
Are you sure you want to continue connecting (yes/no)?
```

## 5 Installation

### 5.1 CSP Installer health verification

To follow the rest of the installation steps discussed in this paragraph it is assumed you have successfully connected to the VM via SSH by also opening a tunnel to port 18080, as already mentioned in paragraph 4.2. You can do so by executing the following command in your terminal:

```
# ssh root@<guestmachinehostname> -L 18080:localhost:18080
```

After successful login you may ensure that everything is OK by checking the log file of the CSP Installer, by executing the following command:

```
# fgrep -e "connect" -e "Connected" /tmp/console.log
```

and verify that CSP Installer reports:

- connectivity to config.central.<cspId>.[preprod.]melicertes.eu:5443
- connectivity to Internet

The above may look like the following snippet, as an example:

```
# Attempting to connect to config.central.demo.melicertes.eu:5443
# Connected to config.central.demo.melicertes.eu:5443
# Internet connectivity test has completed, connection is OK
```

At this point, the administrator can now use the graphical CSP installation control application tool by entering the following URL: <http://127.0.0.1:18080> on the browser of the computer from which they initiated the SSH connection.

---

*The SSH connection should be kept alive always for the tunnel to work. If the SSH connection is closed then the web application will not be available and the user should reconnect via SSH re-establishing the ssh tunnel to port 18080*

---

After starting the graphical CSP installation tool by opening the URL <http://127.0.0.1:18080> in a web browser, the user is presented with the dashboard. Please, visit section 11 - Annex D: Troubleshooting the connection tunnel to the VM, in case you encounter issues in accessing the aforementioned URL.

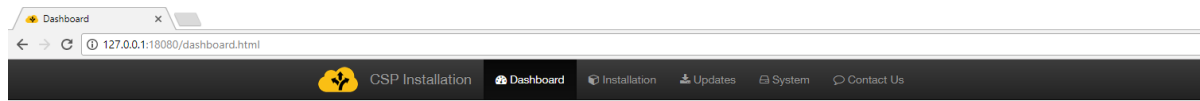
First time installation should display a progress of 0%. The menu bar at the top of the page displays the basic operations of the application which are "Dashboard", "Installation", "Updates" and "System". These options should be selected at the order instructed in this manual. A brief description of what each option does is as follows:

"Dashboard": Displays overall progress and general information. This page will be further enhanced in later releases to show system status.

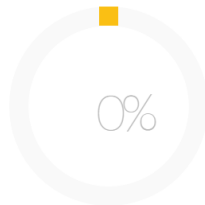
"Installation": Performs a one-time installation/configuration of the CSP.

"Updates": Downloads and updates component images and offers access to the log.

"System": Starts and stops the system and displays the status of all services.



## CSP Installation



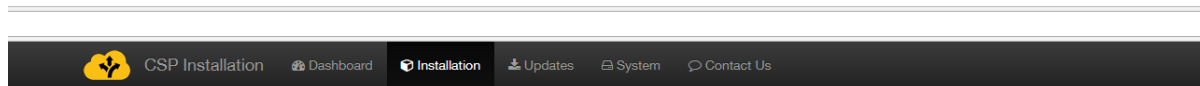
Welcome to the CSP Installation Control Application - Dashboard.

To proceed with installation, please go to the [installation](#) page to configure the CSP or the [Updates](#) page to see updates and installation status.

The first time the CSP installation control application is accessed, the user should proceed to the **Installation** page in order to perform initial configuration.

## 5.2 Installation of certificates

Completing the first installation step requires that the user has saved to his computer all certificate and key files required as mentioned in the previous sections of this manual. The necessary certificates are the CA bundle, the Private SSL Key and the Signed SSL certificate. The file names can be found in section 3.7. The user should make sure that he has them stored in a location that is easy to locate once he hits the Browse button.



## Installation

SSL Certificates

Cancel Save

(Certificates must be uploaded first!)

CA Bundle (.crt):

 Browse ...

Private SSL Key (.key):

 Browse ...

Signed SSL Certificate (.crt):

 Browse ...

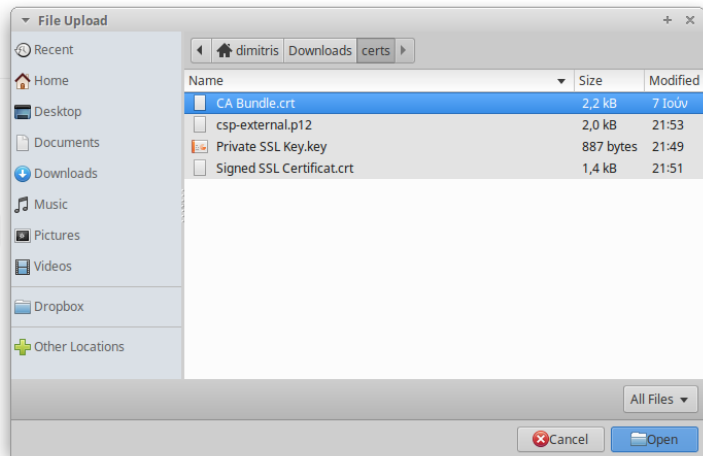
The user should browse and select the files in the order given. First, the user should click the “Browse” button for the CA Bundle certificate and select the “CA Bundle.crt” file. Once selected, the name of the file will appear in the box.



## Installation

## SSL Certificates

CA Bundle (.crt):

Then the user should click the “Browse” button of the Private SSL Key and select the “Private SSL Key.key” file. Once selected, the name of the file will also appear in the box.



## Installation

## SSL Certificates

(Certificates must be uploaded first!)

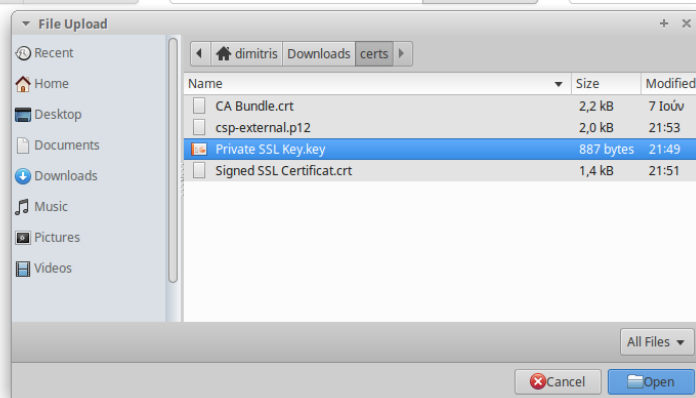
CA Bundle (.crt):

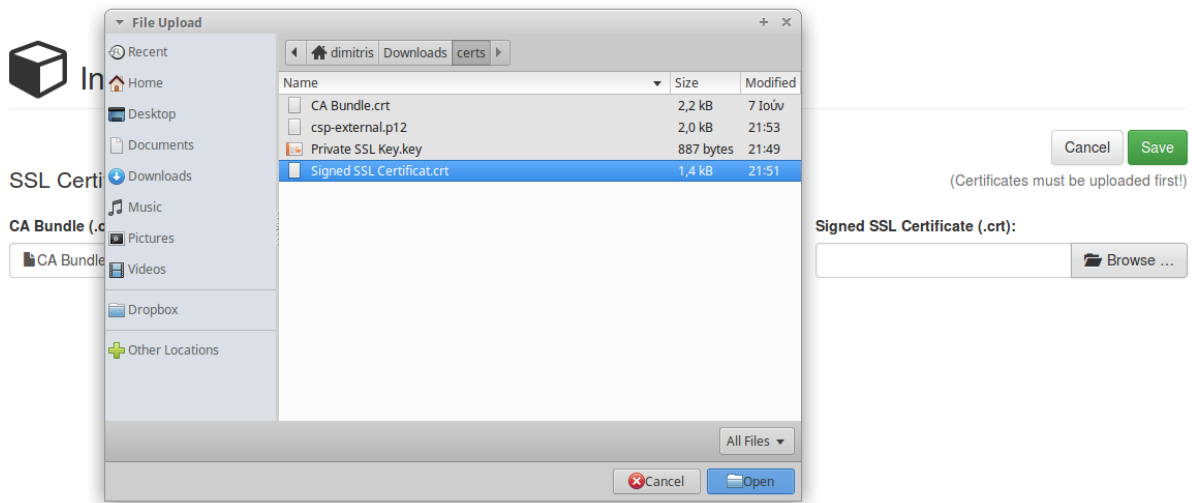
Private SSL Key (.key):

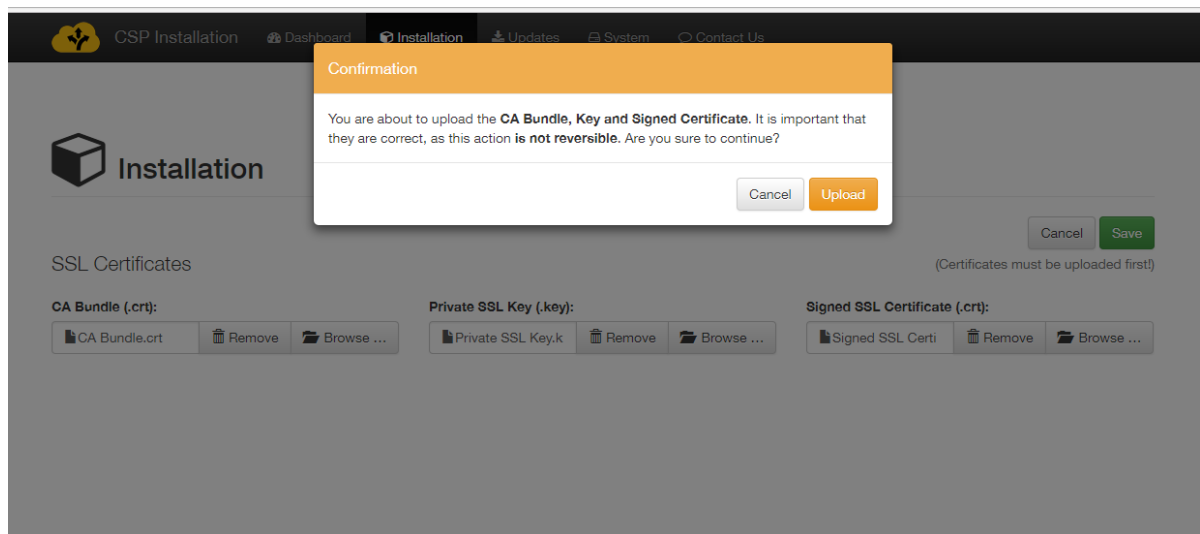
Signed SSL Certificate (.crt):

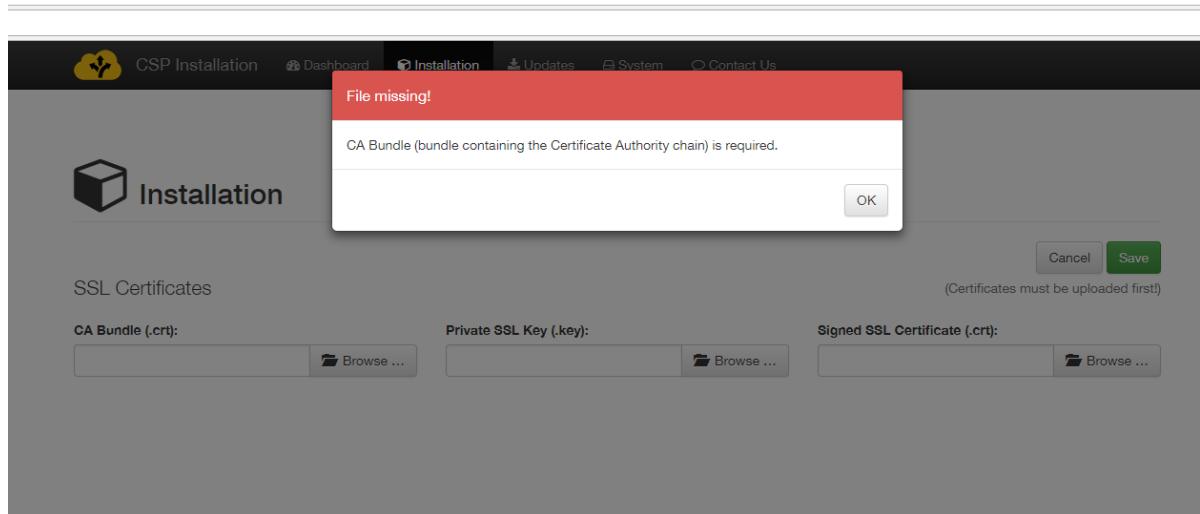
Finally, the user should click the third “Browse” button of the Signed SSL Certificate and select the “Signed SSL Certificate.crt” file. Once selected, the name of the file will also appear in the box.



Once all three files have been selected, the user should click on the green “Save” button. Prior to uploading the files, the system will prompt the user for confirmation. By clicking the upload button, the system will upload the certificate files and redirect the user to the registration page.










Incomplete submittal of the certificates is not possible. The system will alert the user that certificate files are missing if the Save button is clicked and not all three files have been selected.



### 5.3 CSP Instance registration

In the Registration page, the user must enter basic CSP information that includes CSP-ID, Domain, Responsible contact info, internal/external IP's and SMTP configuration for outgoing e-mails.

 CSP Installation
  Dashboard
  Installation
  Updates
  System
  Contact Us

 Installation

CSP Information

CSP UUID:

f9497073-47b1-49c7-822c-6133f9e1a38a

CSP-ID:

Domain Name: (without CSP-ID)

Responsible Contacts

Name:

Email:

Type:

Name:

Email:

Type:

Internal IPs

External IPs

If host directly exposed, add external IP here also

Outgoing Emails

(Optional - videobridge support)

Sender Name:

Sender Email:

SMTP Host:

SMTP Port:

SMTP Username:

SMTP Password:

This form is protected against incomplete submission. If the Save button is clicked without all required fields completed, warning will be displayed.

The fields of this form should be completed as follows.

**CSP UUID:** This field is auto completed by the system and is the Unique Identifier of the CSP instance.

**CSP-ID:** The assigned CSP id (e.g. "csirt-gr")

**Domain Name:** The domain (without CSP-ID) as determined by the application procedure and environment (e.g. preprod.melicertes.eu). Note: the CSP-ID and Domain name should be already known. If the user doing the installation does not have them, the registration procedure will fail.

**Responsible Contacts:** At least two contacts must be provided "Technical Admin" and "Contact". For each contact line the full name and email of the person or distribution group should be filled in like the following example:

Name	Email	Type
Admin PoC	meli.admin@your-cert.org	Technical Admin



Project PoC	meli.project@your-cert.org	Contacte
-------------	----------------------------	----------

More contacts can be configured by adding lines to the form using the green + button.

**Internal/External IPs:** The internal and external IP's of the guest machine need to be inserted. Please note the following details:

- If the system is directly outside the firewalls (e.g. DMZ or direct access to the internet) then Internal IP entered should be the same as external IP, as provided by the network administrator.
- If the system is behind a NAT firewall, the Internal IP should be the IP of the system inside the corporate network. The external IP should be the one used to exit the firewall (public IP address) and it should be static (not dynamic external IP). If the administrator cannot allocate a specific IP via NAT, it is advised this machine to be put on a DMZ instead.
- Only one internal IP and only one external IP are supported.

All the above fields are **mandatory**.

The final section of the form, Outgoing Emails (Optional – videobridge support), is optional and there be no warning if it not completed. This section consists of an SMTP server configuration options, namely:

- Sender Name
- Sender Email
- SMTP Host
- SMTP Port
- SMTP Username
- SMTP Password

The videoconferencing administration requires a valid SMTP configuration so it is suggested that these details are filled in – a simple Gmail account may be used if no “real” account is available. Not entering the SMTP details will make the bridge lose the ability to send out invitations/cancellations to the scheduled conferences and together with them, the assigned username/password and bridge conference room details.

A sample filled in form appears below.

## Installation

### CSP Information

CSP UUID:  CSP-ID:  Domain Name: (without CSP-ID)

### Responsible Contacts

Name:	Email:	Type:
<input type="text" value="John Doe"/>	<input type="text" value="john@example.org"/>	<input type="text" value="TECH_ADMIN"/>
Name:	Email:	Type:
<input type="text" value="Jane Doe"/>	<input type="text" value="jane@example.org"/>	<input type="text" value="CONTACT"/>

### Internal IPs

If host directly exposed, add external IP here also

### External IPs

### Outgoing Emails

(Optional - videobridge support)

Sender Name:	Sender Email:	SMTP Host:	SMTP Port:
<input type="text" value="csirt04.demo"/>	<input type="text" value="postmaster@demo.melicertes.eu"/>	<input type="text" value="smtp.mailgun.org"/>	<input type="text" value="587"/>
SMTP Username:	SMTP Password:		
<input type="text" value="postmaster@demo.melicertes.eu"/>	<input type="password" value="....."/>		

The form is submitted by clicking the green Save button.

The screenshot shows the 'CSP Installation' web interface. A confirmation dialog box is displayed in the center, with the following text: 'The information entered will now be used to create your CSP registration in the Central Service. You need to make sure the provided information is correct, as connectivity will not be possible otherwise. Please take time to review the provided data before continuing.' The dialog has two buttons: 'Go back and review' and 'Continue and Register'. The background form is titled 'Installation' and contains the following sections:

- CSP Information:**
  - CSP UUID: f9497073-f7b1-49c7-822c-6133f9e1a38a
  - CSP-ID: csirt04
  - Domain Name: (without CSP-ID) demo.melicertes.eu
- Responsible Contacts:**
  - John Doe (Name), john@example.org (Email), TECH\_ADMIN (Type)
  - Jane Doe (Name), jane@example.org (Email), CONTACT (Type)
- Internal IPs:** 172.31.22.129
- External IPs:** 172.31.22.129
- Outgoing Emails:**
  - Sender Name: csirt04.demo
  - Sender Email: postmaster@demo.melicertes.eu
  - SMTP Host: smtp.mailgun.org
  - SMTP Port: 587
  - SMTP Username: postmaster@demo.melicertes.eu
  - SMTP Password: (masked)

Buttons for 'Cancel' and 'Save' are present at the bottom right of the form.

The system prompts for confirmation prior to final submission. It is important that all information entered is correct since connectivity will not be possible if any misspellings exist in the CSP name, domain and IP's. After pressing the "Continue and Register" button, the system will redirect to the Dashboard page.

At that point, the installation UI performs a CSP registration action and on completion, assumes the CSP as registered. **The user should contact the operators of the central CSP to inform them about the new CSP registration.**

#### 5.4 Download of system updates

In a new installation, a registered CSP is not operational yet. **Specific actions are necessary on the central CSP side to allow this new CSP to receive updates and continue the installation.** The user should proceed to the "Updates" page. The updates list should be empty until the operators of the central CSP assign updates to this CSP instance. Once the updates are assigned, the list will be populated, and the user can continue with the installation.

In an existing installation, updates may appear on the "Updates" page periodically. This page should be checked once a week during a scheduled maintenance window.

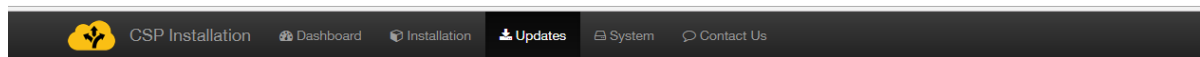
## Updates

[Click here to check again](#)

[See the system log](#)

Name	Description	Version Available	Version Installed	Release Date	Actions
No matching records found					

The user can check for updates by selecting the “Click here to check again” button. The CSP does not display *any updates on this page* until updates are assigned. The updates list will appear as below, in a configured CSP:



## Updates

[Click here to check again](#)
[See the system log](#)

Name	Description	Version Available	Version Installed	Release Date	Actions
base	base	1.0.000	Not yet installed	2017-09-15T16:41:59Z	
postgres	1909	1.0.400	Not yet installed	2017-09-19T07:06:11Z	
openam	1909	1.0.400	Not yet installed	2017-09-19T07:08:45Z	
anon	1909	1.0.400	Not yet installed	2017-09-19T07:09:17Z	
integr	1909	1.0.400	Not yet installed	2017-09-19T07:09:51Z	
mock	1909	1.0.400	Not yet installed	2017-09-19T07:10:24Z	
elastic	1909	1.0.400	Not yet installed	2017-09-19T07:10:58Z	
kibana	1909	1.0.400	Not yet installed	2017-09-19T07:11:31Z	
logstash	1909	1.0.400	Not yet installed	2017-09-19T07:12:10Z	
owncloud	1909	1.0.400	Not yet installed	2017-09-19T07:13:44Z	
jitsi	1909	1.0.400	Not yet installed	2017-09-19T07:14:21Z	
trustcircles	1909	1.0.400	Not yet installed	2017-09-19T07:12:36Z	
apache	1909	1.0.400	Not yet installed	2017-09-19T07:13:09Z	

Showing 1 to 13 of 13 rows

The user can download updates by clicking on the blue download icon in the Actions column. Each time the user clicks on a download button, the system will redirect them to the System log page.

CSP Installation
 Dashboard
 Installation
 Updates
 System
 Contact Us

## System Log

Back to Updates
 Back to System
 refresh automatically every 60s  
 Refresh now

2017-09-19T07:47:32.672 INFO Task 4 was added for background work

2017-09-19T07:47:32.672 INFO Module SystemModule(id=1, name=base, description=base, installDate=null, active=false, version=1.0.000, archivePath=null, modulePath=null, moduleState=UNKNOWN, hash=21a349e8e698f983a7ad990b796cb44e836c989c969f6d79165f9303e1023582d4e8cc59a25bbf69ed5f64b96566a3269f73c88547479830a8cb9acce17a4c0, startPriority=0) retrieved!

2017-09-19T07:47:32.672 INFO Module SystemModule(id=13, name=apache, description=1909, installDate=null, active=false, version=1.0.400, archivePath=null, modulePath=null, moduleState=UNKNOWN, hash=ef30eb7b07115707bc5a6c499708370e79daf90e2827ff5dd9071d37ff6b813be325cd7cec5d075a0098be401c8a4ed98c805c414026f402020af5f560881588, startPriority=990) saved!

2017-09-19T07:47:02.393 INFO Module SystemModule(id=12, name=trustcircles, description=1909, installDate=null, active=false, version=1.0.400, archivePath=null, modulePath=null, moduleState=UNKNOWN, hash=8000bf216243394a416fda4f43627c29eb284fab859f5af9c238867f4fdc894ea84156a01d81c758cf2ff90e789ba142abee081b2dbc98c6468f56ab3ebce47, startPriority=900) saved!

2017-09-19T07:47:02.393 INFO Module SystemModule(id=11, name=jitsi, description=1909, installDate=null, active=false, version=1.0.400, archivePath=null, modulePath=null, moduleState=UNKNOWN, hash=cc1cfdd6504151a1b4609ae17a03716440c21b1fc10ed7e3cf8eddb43b0aaid15e9b9404dc4634bc1d901d709c3dfe14d7524c466a9bdc1ef2b9bee4a8763, startPriority=831) saved!

2017-09-19T07:47:02.372 INFO Module SystemModule(id=10, name=owncloud, description=1909, installDate=null, active=false, version=1.0.400, archivePath=null, modulePath=null, moduleState=UNKNOWN, hash=54cbfb18f0c6b3cab1444039e514fbeeae5d650d009fe8544565c1f9d0216f3c518f29c1819a4d5ff18fe2cc604ce03a4c97b33186926e9e4bd525206abbf, startPriority=820) saved!

2017-09-19T07:47:02.363 INFO Module SystemModule(id=9, name=logstash, description=1909, installDate=null, active=false, version=1.0.400, archivePath=null, modulePath=null, moduleState=UNKNOWN, hash=672246677d202ce9bde487cfac54a07bb037f14b57efe0df5680d806ff8a909492272d9bc7d9c6bde6d3c2e7b31ac475826afe764c764b101ffe9221c4c90, startPriority=802) saved!

2017-09-19T07:47:02.353 INFO Module SystemModule(id=8, name=kibana, description=1909, installDate=null, active=false, version=1.0.400, archivePath=null, modulePath=null, moduleState=UNKNOWN, hash=61773bfc33694a6a55a809cc71e8cc7bedee3ceb60a78e256bf433dcd9bf3de8c38c2c0be285624a51ef73304ce0a2fa5b0ad416b4b7160ec2e254578511a38, startPriority=801) saved!

2017-09-19T07:47:02.343 INFO Module SystemModule(id=7, name=elastic, description=1909, installDate=null, active=false, version=1.0.400, archivePath=null, modulePath=null, moduleState=UNKNOWN, hash=90343f992fb80d8d9b0ebb7f6c7ec7a7fe4e26059f13897398706cc06b4ea73f94226e5f6d65249858f0e61e16f9273e5c715a9ea78368038cfb0834589fa750, startPriority=800) saved!

2017-09-19T07:47:02.333 INFO Module SystemModule(id=6, name=mark, description=1909, installDate=null, active=false, version=1.0.400, archivePath=null, modulePath=null, moduleState=UNKNOWN, hash=90343f992fb80d8d9b0ebb7f6c7ec7a7fe4e26059f13897398706cc06b4ea73f94226e5f6d65249858f0e61e16f9273e5c715a9ea78368038cfb0834589fa750, startPriority=800) saved!

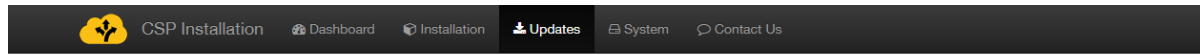
Most operations, including downloading of updates takes place in the background so the user can return to the Updates page by clicking the “Back to Update” button, and page refresh (for updated log entries) happens every 60 seconds or if the “Refresh now” button is pressed.

An indicative list of log entry extracts with explanations follows:

- “Task X was added for background work” – the system has scheduled an operation to happen in the background. Expect further information after 5-8 seconds.
- “BackgroundTaskResult(success=true, errorCode=0, moduleName=<variable>)” – indicates a successfully executed operation
- “BackgroundTaskResult(success=false, errorCode=<variable>, moduleName=<variable>)” – indicates a failed operation. The logs should be returned to the support team for further investigation<sup>4</sup>.

<sup>4</sup> Extraction of logs via the web UI is possible: Click within the log window, press “Ctrl + A” followed by “Ctrl + C” or “Cmd + A” followed by “Cmd + C” if on a Mac, then open a text editor and paste (“Ctrl + V” or “Cmd + V”). Save the file and attach it to a ticket or email to MeliCERTes support.














Note that updates that are currently downloading will present an animated gear icon in the “Actions” column.



## Updates

[Click here to check again](#)
[See the system log](#)

Refresh
Print
Grid

Name	Description	Version Available	Version Installed	Release Date	Actions
base	base	1.0.000	Not yet installed	2017-09-15T16:41:59Z	
postgres	1909	1.0.400	Not yet installed	2017-09-19T07:06:11Z	
openam	1909	1.0.400	Not yet installed	2017-09-19T07:08:45Z	
anon	1909	1.0.400	Not yet installed	2017-09-19T07:09:17Z	
integr	1909	1.0.400	Not yet installed	2017-09-19T07:09:51Z	
mock	1909	1.0.400	Not yet installed	2017-09-19T07:10:24Z	
elastic	1909	1.0.400	Not yet installed	2017-09-19T07:10:58Z	
kibana	1909	1.0.400	Not yet installed	2017-09-19T07:11:31Z	
logstash	1909	1.0.400	Not yet installed	2017-09-19T07:12:10Z	
owncloud	1909	1.0.400	Not yet installed	2017-09-19T07:13:44Z	
jitsi	1909	1.0.400	Not yet installed	2017-09-19T07:14:21Z	
trustcircles	1909	1.0.400	Not yet installed	2017-09-19T07:12:36Z	
apache	1909	1.0.400	Not yet installed	2017-09-19T07:13:08Z	
















Showing 1 to 13 of 13 rows

The user may initiate more downloads without waiting for the previous ones to finish as all download requests are added as background tasks one after the other. Completed downloads will present two new icons in the Action page, the green Install icon and the red delete icon. Note that although possible, clicking the download button multiple times should be avoided. You may monitor the download process by pressing the “Refresh” button on the button bar over the “Actions” column, without leaving this page.

## Updates

Click here to check again See the system log

Search

Name	Description	Version Available	Version Installed	Release Date	Actions
base	base	1.0.000	Not yet installed	2017-09-15T16:41:59Z	 
postgres	1909	1.0.400	Not yet installed	2017-09-19T07:06:11Z	 
openam	1909	1.0.400	Not yet installed	2017-09-19T07:08:45Z	
anon	1909	1.0.400	Not yet installed	2017-09-19T07:09:17Z	
integr	1909	1.0.400	Not yet installed	2017-09-19T07:09:51Z	
mock	1909	1.0.400	Not yet installed	2017-09-19T07:10:24Z	
elastic	1909	1.0.400	Not yet installed	2017-09-19T07:10:58Z	
kibana	1909	1.0.400	Not yet installed	2017-09-19T07:11:31Z	
logstash	1909	1.0.400	Not yet installed	2017-09-19T07:12:10Z	
owncloud	1909	1.0.400	Not yet installed	2017-09-19T07:13:44Z	
jitsi	1909	1.0.400	Not yet installed	2017-09-19T07:14:21Z	
trustcircles	1909	1.0.400	Not yet installed	2017-09-19T07:12:36Z	
apache	1909	1.0.400	Not yet installed	2017-09-19T07:13:09Z	



























Showing 1 to 13 of 13 rows

All available updates should be downloaded reaching the stage where all images are available for installation as shown in the following image.

## Updates

Click here to check again See the system log

Search

Name	Description	Version Available	Version Installed	Release Date	Actions
base	base	1.0.000	Not yet installed	2017-09-15T16:41:59Z	 
postgres	1909	1.0.400	Not yet installed	2017-09-19T07:06:11Z	 
openam	1909	1.0.400	Not yet installed	2017-09-19T07:08:45Z	 
anon	1909	1.0.400	Not yet installed	2017-09-19T07:09:17Z	 
integr	1909	1.0.400	Not yet installed	2017-09-19T07:09:51Z	 
mock	1909	1.0.400	Not yet installed	2017-09-19T07:10:24Z	 
elastic	1909	1.0.400	Not yet installed	2017-09-19T07:10:58Z	 
kibana	1909	1.0.400	Not yet installed	2017-09-19T07:11:31Z	 
logstash	1909	1.0.400	Not yet installed	2017-09-19T07:12:10Z	 
owncloud	1909	1.0.400	Not yet installed	2017-09-19T07:13:44Z	 
jitsi	1909	1.0.400	Not yet installed	2017-09-19T07:14:21Z	 
trustcircles	1909	1.0.400	Not yet installed	2017-09-19T07:12:36Z	 
apache	1909	1.0.400	Not yet installed	2017-09-19T07:13:09Z	 

Showing 1 to 13 of 13 rows

## 5.5 Modules installation

Now, component installation should begin. By clicking the green Install icon for each image, the user should install ALL available images, by consecutively clicking the install buttons, for the system to properly function.

By clicking the install button for an image, the user is redirected to the System log where they can monitor installation progress. The installation process for some modules may take more than 5 minutes, as there is an implicit setup phase that happens. The process may be monitored at the system log page. The user should expect a log entry with "BackgroundTaskResult" indicating "success=true".






Image installations must begin from top to bottom in the same order as they are displayed, but they should not be performed concurrently. Users should wait until the installation of each module completes successfully before proceeding to the installation of the next one. Please note that *while an image installation is taking place, nothing appears in the Action column* for the module being installed, as shown in the figure below.

misp	fix docker-compose	4.0.002	Not yet installed	2019-04-25T09:37:17Z	
rt	FIX the https://git-csp.athens.intrasoft-intl.private/csp/xscsp/issues/4. There are NO log files from RT adapter under /opt/csp/logs/ - /opt/csp/logs/ - /opt/csplogs to dicker-compose volumes:	3.6.003	Not yet installed	2019-04-25T09:37:58Z	 
intelmq	20180919 build	4.0.005	Not yet installed	2019-04-25T09:38:46Z	 

When an image installation is finished:

- a yellow Re-install icon appears in the Actions column. This should only be selected if specific circumstances mandate re-installation of an image, or if explicitly requested by the support team.
- a red Delete icon appears in the Actions column. This should be selected if the corresponding module no longer is required. Please note that this will result in the removal of any persistent data saved by that module.



owncloud	Port moved to 6443 for public access	3.6.001	3.6.001	2019-04-25T09:35:57Z	 
trustcircles	Fixed TeamContact sharing of field "description" Remove csp_id uniqueness requirement in TeamContacts	3.8.001	3.8.001	2019-04-25T09:36:33Z	 
misp	fix docker-compose	4.0.002	Not yet installed	2019-04-25T09:37:17Z	
rt	FIX the https://git-csp.athens.intrasoft-intl.private/csp/sxcsp/issues/4. There are NO log files from RT adapter under /opt/csp/logs added - /opt/csp/logs/: /opt/csplogs to dicker-compose volumes:	3.6.003	Not yet installed	2019-04-25T09:37:58Z	  
intelmq	20180919 build	4.0.005	Not yet installed	2019-04-25T09:38:46Z	  

As noted, it is suggested that users proceed with installation of images in the order presented in the table. After successful installation of all images, the Updates page should appear as follows (all modules have been installed, only re-install or deletion is possible).

## Updates

Click here to check again

See the system log

Search

Name	Description	Version Available	Version Installed	Release Date	Actions
base	Updated base modules for 4.0.4 (20180903 build)	4.0.004	4.0.004	2019-04-25T09:30:15Z	<div></div> <div></div>
postgres	pg 19/2	2.0.000	2.0.000	2019-04-25T09:30:44Z	<div></div> <div></div>
redis	2018-05-29: added empty "external_host"	3.6.001	3.6.001	2019-04-25T09:31:06Z	<div></div> <div></div>
oam	2018-06-05: fix for update-datastore line	3.6.005	3.6.005	2019-04-25T09:31:42Z	<div></div> <div></div>
ActiveMQ	ActiveMQ Module	2.8.001	2.8.001	2019-04-25T09:32:41Z	<div></div> <div></div>
anon	anonymization in arrays element fix	4.0.001	4.0.001	2019-04-25T09:33:18Z	<div></div> <div></div>
il	vulnerability routing fixes	4.0.001	4.0.001	2019-04-25T09:33:40Z	<div></div> <div></div>
mocknode	Migrating mockservices to node	2.0.001	2.0.001	2019-04-25T09:34:05Z	<div></div> <div></div>
es	Elasticsearch with new misp-vulnerability support latest fix	4.0.002	4.0.002	2019-04-25T09:34:43Z	<div></div> <div></div>
kibana	kibana 19/2	2.0.000	2.0.000	2019-04-25T09:35:08Z	<div></div> <div></div>
logs	3.6.007	3.6.007	3.6.007	2019-04-25T09:35:30Z	<div></div> <div></div>
owncloud	Port moved to 6443 for public access	3.6.001	3.6.001	2019-04-25T09:35:57Z	<div></div> <div></div>
trustcircles	Fixed TeamContact sharing of field "description" Remove csp_id uniqueness requirement in TeamContacts	3.8.001	3.8.001	2019-04-25T09:36:33Z	<div></div> <div></div>
misp	fix docker-compose	4.0.002	4.0.002	2019-04-25T09:37:17Z	<div></div> <div></div>
rt	FIX the https://git-csp.athens.intrasoft-intl.private/csp/sxcsp/issues/4. There are NO log files from RT adapter under /opt/csp/logs added - /opt/csp/logs/: /opt/csplogs to dicker-compose volumes:	3.6.003	3.6.003	2019-04-25T09:37:58Z	<div></div> <div></div>
intelmq	20180919 build	4.0.005	4.0.005	2019-04-25T09:38:46Z	<div></div> <div></div>
regrep	Regular Reports with the latest fixes	4.0.001	4.0.001	2019-04-25T09:39:21Z	<div></div> <div></div>
vcb	vcb:3.8.002	3.8.002	3.8.002	2019-04-25T09:39:49Z	<div></div> <div></div>
viper	image fix	4.0.003	4.0.003	2019-04-25T09:40:11Z	<div></div> <div></div>
apache cri	20180917 build	4.0.004	4.0.004	2019-04-25T09:40:28Z	<div></div> <div></div>
apache	20180920 build	4.0.006	4.0.006	2019-04-25T09:40:46Z	<div></div> <div></div>

Showing 1 to 21 of 21 rows

50

▲

records per page

Showing 1 to 21 of 21 rows 50 records per page

Only after all available images are installed and all modules appear with the yellow “re-install” icon, should the user continue to start all services from the System page. This is important because the first time each service is started, module configuration are taking place that might require the presence of other modules.

## 6 Managing CSP


### 6.1 Starting

The “system” page shows a current view of the system services registered, together with their current status. The following states are possible:



- Stopped – the service is not currently running
- Running – the service is enabled and running




The column “Can start?” indicates if this is a supporting service or an actual component of the system. Services that indicate the value “No” mean that they do not have a controlling element to start and stop. This is normal for the “base” service in this release.

Current state should be stopped for all modules the first time this page is accessed.

By clicking the Start  button, all registered modules are queued to start one by one. The system will start modules in the order displayed in the table, from the one having the lowest priority value (100) up to the one with the highest priority value (990).


#### System






Name	Current State	Can start?	Priority	Version
base	Stopped	No	0	4.0.004
postgres	Running	Yes	100	2.0.000
redis	Running	Yes	110	3.6.001
oam	Stopped	Yes	200	3.6.005
ActiveMQ	Stopped	Yes	400	2.8.001
anon	Stopped	Yes	500	4.0.001
il	Stopped	Yes	501	4.0.001
mocknode	Stopped	Yes	502	2.0.001
es	Stopped	Yes	800	4.0.002
kibana	Stopped	Yes	801	2.0.000
logs	Stopped	Yes	802	3.6.007
owncloud	Stopped	Yes	820	3.6.001
trustcircles	Stopped	Yes	900	3.8.001
misp	Stopped	Yes	901	4.0.002
rt	Stopped	Yes	902	3.6.003
intelmq	Stopped	Yes	903	4.0.005
regrep	Stopped	Yes	904	4.0.001
vcb	Stopped	Yes	905	3.8.002
viper	Stopped	Yes	906	4.0.003
apache cri	Stopped	Yes	980	4.0.004
apache	Stopped	Yes	990	4.0.006

Showing 1 to 21 of 21 rows
 

50
 

 records per page

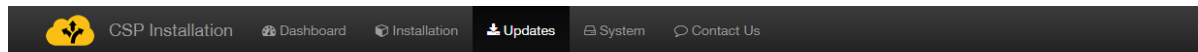
While the system is starting, the Start button is dimmed and the only available option is to stop the system. To initiate a System stop, click on the Stop  button.

Note that due to complexity of services, system Start and Stop are operations that take several minutes to complete. The stop sequence **is queued and will take effect after the system has fully started** (all modules – apart base – indicating Running state) **or all previous queued tasks have finished/exited**.

Especially system Start is normal to take several minutes to complete. The user should be patient until all modules report their state as “Running”. Depending on VM settings: configured RAM, type of disk drives (Solid state or Hard disk) it may take up to 30 minutes for all modules to start.

During this wait period, users can use the **System** menu and click on the “refresh” button to refresh the table so as to be informed about the system Start/Stop progress, taking notice to the “Current State” column as it changed to reflect the module state.

Anytime the user can navigate to the System Log (available through the **Updates** menu and then click on the “See the system log” button to see a snapshot of the log files as they are appended.



## System Log

[Back to Updates](#)
[Back to System](#)

refresh automatically every 60s

2017-09-19T08:05:39.134

INFO

Waiting 60 sec for openam to be ready.....

2017-09-19T08:05:39.137

INFO

Monitor returned 0

2017-09-19T08:05:39.099

INFO

Monitoring attempt 1...

2017-09-19T08:05:27.432

INFO

Module SystemModule(id=13, name=apache, description=1909, installDate=2017-09-19T08:03:54.720, active=true, version=1.0.400, archivePath=/opt/csp/downloads/ef30eb7b07115707bc5a6c499708370e79daf98e2827ff5dd9071d37ff6b813be325cd7cec5d075a0098be481c8a4ed98c805c414026f402020af5f560881588.zip, modulePath=/opt/csp/modules/apacheef30eb7b0711, moduleState=INSTALLED, hash=ef30eb7b07115707bc5a6c499708370e79daf98e2827ff5dd9071d37ff6b813be325cd7cec5d075a0098be481c8a4ed98c805c414026f402020af5f560881588, startPriority=990) retrieved!

2017-09-19T08:05:27.430

INFO

Module SystemModule(id=12, name=trustcircles, description=1909, installDate=2017-09-19T08:03:54.610, active=true, version=1.0.400, archivePath=/opt/csp/downloads/8000bf216243394a416fda4f43627c29eb284fab859f5af9c238867f4f4dc894ea84156a01d81c758cf2ff98e789ba142abee0c81b2dbc98c6468f56ab3ebce47.zip, modulePath=/opt/csp/modules/trustcircles8000bf216243, moduleState=INSTALLED, hash=8000bf216243394a416fda4f43627c29eb284fab859f5af9c238867f4f4dc894ea84156a01d81c758cf2ff98e789ba142abee0c81b2dbc98c6468f56ab3ebce47, startPriority=900) retrieved!

2017-09-19T08:05:27.429

INFO

Module SystemModule(id=11, name=jitsi, description=1909, installDate=2017-09-19T08:03:51.443, active=true, version=1.0.400, archivePath=/opt/csp/downloads/cc1cfddddd584151a1b460aae17a83718440c21b1fc10ed7e3cf8eddb43b8aad15e9b9404dc4634bc1d981d700c3dfe14d7524c466a9bdc1ef2b9bee4a8763.zip, modulePath=/opt/csp/modules/jitsic1cfddddd584151a1b460aae17a83718440c21b1fc10ed7e3cf8eddb43b8aad15e9b9404dc4634bc1d981d700c3dfe14d7524c466a9bdc1ef2b9bee4a8763, startPriority=831) retrieved!

2017-09-19T08:05:27.425

INFO

Module SystemModule(id=10, name=owncloud, description=1909, installDate=2017-09-19T08:02:49.458, active=true, version=1.0.400, archivePath=/opt/csp/downloads/54cbfb18f0c6b3caba1444839e514fbaeaf5c5d650d809fe8544565c1f9d0216f3c518f29c1819a4d5ff18fe2cc604ce03a4c97b33186926e9e4bd525206abbf.zip, modulePath=/opt/csp/modules/owncloud54cbfb18f0c6, moduleState=INSTALLED, hash=54cbfb18f0c6b3caba1444839e514fbaeaf5c5d650d809fe8544565c1f9d0216f3c518f29c1819a4d5ff18fe2cc604ce03a4c97b33186926e9e4bd525206abbf, startPriority=820) retrieved!

2017-09-19T08:05:27.423

INFO

Module SystemModule(id=9, name=logstash, description=1909, installDate=2017-09-19T08:02:32.884, active=true, version=1.0.400, archivePath=/opt/csp/downloads/672246677d202cee9bde407cfac54a07bb037f14b57efe0df5688d806ff8a809492272d9bc7d9c6bde6d3c2e7b31ac475826afe764c764b101ff8e9221c4c90.zip, modulePath=/opt/csp/modules/logstash672246677d20, moduleState=INSTALLED, hash=672246677d202cee9bde407cfac54a07bb037f14b57efe0df5688d806ff8a809492272d9bc7d9c6bde6d3c2e7b31ac475826afe764c764b101ff8e9221c4c90, startPriority=802) retrieved!

2017-09-19T08:05:27.421

INFO

Module SystemModule(id=8, name=kibana, description=1909, installDate=2017-09-19T08:01:26.857, active=true, version=1.0.400, archivePath=/opt/csp/modules/kibana61773bfc33694a6a55a809cc71e8cc7bedee3ceb60a78e256bf433dcd8bbf3de8c38c2c0be285624a51e1f73304ce0a2fa5b0ad416b4b7160ec2e254578511a38.zip, modulePath=/opt/csp/modules/kibana61773bfc3369, moduleState=INSTALLED, hash=61773bfc33694a6a55a809cc71e8cc7bedee3ceb60a78e256bf433dcd8bbf3de8c38c2c0be285624a51e1f73304ce0a2fa5b0ad416b4b7160ec2e254578511a38, startPriority=801) retrieved!

The user should wait until all modules (except Base) report “Running” state. Depending on the performance of the system, the initial start of modules may take more than 30 minutes, due to initialization of security components. Subsequent restarts (if needed) will be much faster. When the system has successfully started, the following should appear.

## System

▶ Start

■ Stop

↺

📄

⌵

Name	Current State	Can start?	Priority	Version
base	Stopped	No	0	4.0.004
postgres	Running	Yes	100	2.0.000
redis	Running	Yes	110	3.6.001
oam	Running	Yes	200	3.6.005
ActiveMQ	Running	Yes	400	2.8.001
anon	Running	Yes	500	4.0.001
il	Running	Yes	501	4.0.001
mocknode	Running	Yes	502	2.0.001
es	Running	Yes	800	4.0.002
kibana	Running	Yes	801	2.0.000
logs	Running	Yes	802	3.6.007
owncloud	Running	Yes	820	3.6.001
trustcircles	Running	Yes	900	3.8.001
misp	Running	Yes	901	4.0.002
rt	Running	Yes	902	3.6.003
intelmq	Running	Yes	903	4.0.005
regrep	Running	Yes	904	4.0.001
vcb	Running	Yes	905	3.8.002
viper	Running	Yes	906	4.0.003
apache crl	Running	Yes	980	4.0.004
apache	Running	Yes	990	4.0.006

Showing 1 to 21 of 21 rows

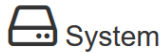
50 ▲

records per page

Please note once again that the base module simply contains other module images and is not expected to start so a state of Stopped is expected.

## 6.2 Stopping

Stopping the system is possible using the “Stop” button. The system shall produce similar output to the “Start” button, and all information provided above is relevant. Note that stopping happens in the reverse order, so the Apache proxy will stop first hence losing access to all applications.



▶ Start

■ Stop

Search

↺

📄

⌵

Name	Current State	Can start?	Priority	Version
base	Stopped	No	0	4.0.004
postgres	Stopped	Yes	100	2.0.000
redis	Stopped	Yes	110	3.6.001
oam	Stopped	Yes	200	3.6.005
ActiveMQ	Stopped	Yes	400	2.8.001
anon	Stopped	Yes	500	4.0.001
il	Stopped	Yes	501	4.0.001
mocknode	Stopped	Yes	502	2.0.001
es	Stopped	Yes	800	4.0.002
kibana	Stopped	Yes	801	2.0.000
logs	Stopped	Yes	802	3.6.007
owncloud	Stopped	Yes	820	3.6.001
trustcircles	Stopped	Yes	900	3.8.001
misp	Stopped	Yes	901	4.0.002
rt	Stopped	Yes	902	3.6.003
intelmq	Stopped	Yes	903	4.0.005
regrep	Stopped	Yes	904	4.0.001
vcb	Stopped	Yes	905	3.8.002
viper	Stopped	Yes	906	4.0.003
apache cri	Stopped	Yes	980	4.0.004
apache	Stopped	Yes	990	4.0.006

Showing 1 to 21 of 21 rows 50 records per page

The “Stop” button will *only be available* if at least one service is in “Running” state. Otherwise, (as in the figure above) it will appear disabled.

If a service is started using the console, the installer will not reflect its actual status showing it as “Stopped”. When we press the “Stop” button all services will begin to stop one after the other, but it is a good practice to verify that all services have indeed stopped afterwards by issuing the command “`docker ps`” in the console, as presented in chapter 7.

## 6.3 Update SMTP configuration

SMTP configuration provided during registration of the CSP Node can be updated by visiting Installation menu, if system is stopped, as described in previous paragraph. In such case, and when entering Installation menu the installer prompts for SMTP configuration, as shown below:

## Installation

👉 Data entry is complete! Click [here](#) to navigate to the dashboard, or [check and modify the SMTP settings](#).  
You may also go to the [Updates page](#) to see updates and installation status. To see the logs go to [the system logs](#).

By clicking on the link: “check or modify the SMTP settings” the user is prompted to enter or update the SMTP configuration, as shown below:

## Installation

### Outgoing Emails

The configuration below enables use of SMTP services for CSP. For supported SMTP settings (e.g. TLS), please refer to the installation manual. To activate any change, a system stop/start cycle from the “System” page is required.

<b>Sender Name:</b>	<b>Sender Email:</b>	<b>SMTP Host:</b>	<b>SMTP Port:</b>
<input type="text" value="csirt04.demo"/>	<input type="text" value="postmaster@demo.melicertes.eu"/>	<input type="text" value="smtp.mailgun.org"/>	<input type="text" value="587"/>
<b>SMTP Username:</b>	<b>SMTP Password:</b>		
<input type="text" value="postmaster@demo.melicertes.eu"/>	<input type="password" value="....."/>		

## 7 Smoke-testing the Installation

At this point, the system is ready, and the user should verify connectivity and successful operation of each application.

First check the status of the services via the console. Run the following command

```
docker stats --all --format "table {{.Name}}\t{{.CPUPerc}}\t{{.MemUsage}}"
--no-stream | sort
```

The output should be similar to the screenshot below

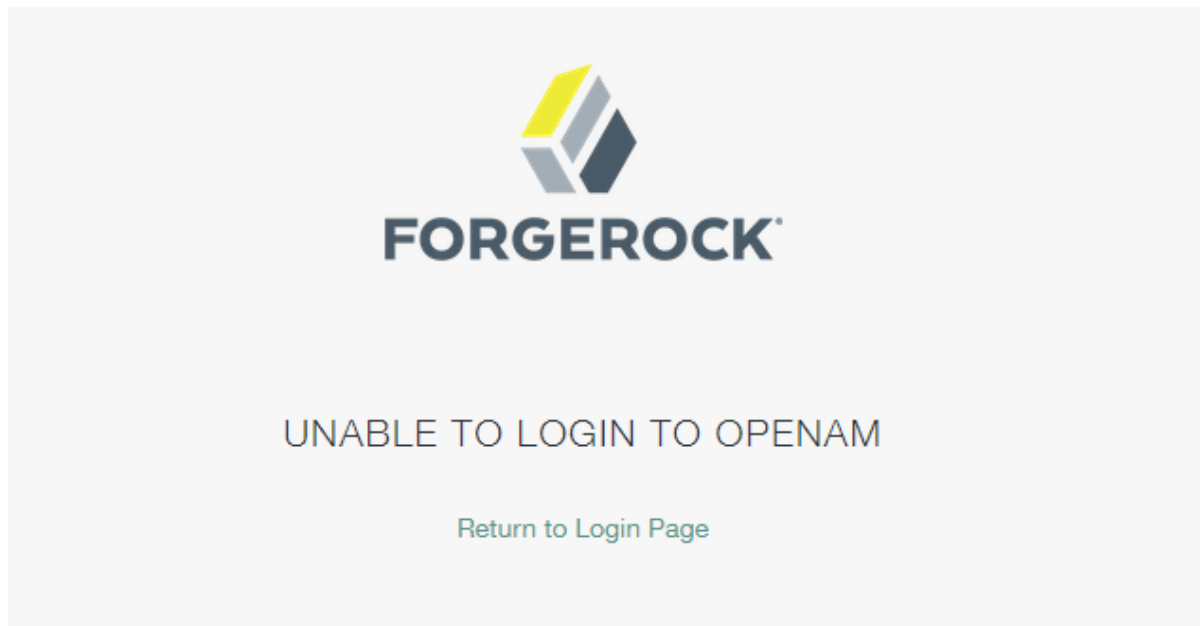
NAME	CPU %	MEM USAGE / LIMIT
csp-activemq	0.00%	0B / 0B
csp-anon	0.00%	0B / 0B
csp-apache	0.00%	0B / 0B
csp-apache-crl	0.00%	0B / 0B
csp-es	0.00%	0B / 0B
csp-filebeat	0.00%	0B / 0B
csp-il	0.00%	0B / 0B
csp-imq	0.00%	0B / 0B
csp-intelmq_adapter	0.00%	0B / 0B
csp-jitsi	0.00%	0B / 0B
csp-kibana	0.00%	0B / 0B
csp-kibana_logs	0.00%	0B / 0B
csp-logstash	0.00%	0B / 0B
csp-misp	0.00%	0B / 0B
csp-misp-filebeat	0.00%	0B / 0B
csp-misp-logstash	0.00%	0B / 0B
csp-misp_adapter	0.00%	0B / 0B
csp-mock	0.00%	0B / 0B
csp-mysql	0.00%	0B / 0B
csp-oam	0.00%	0B / 0B
csp-oam-filebeat	0.00%	0B / 0B
csp-oam-logstash	0.00%	0B / 0B
csp-oc	0.00%	0B / 0B
csp-ocdb	0.00%	0B / 0B
csp-ocredis	0.00%	0B / 0B
csp-postgres	0.00%	0B / 0B
csp-redis	0.00%	0B / 0B
csp-regrep	0.00%	0B / 0B
csp-rt	0.00%	0B / 0B
csp-rt_adapter	0.00%	0B / 0B
csp-tc	0.00%	0B / 0B
csp-tc-dsl	0.00%	0B / 0B
csp-vcb_admin	0.00%	0B / 0B
csp-vcb_teleconf	0.00%	0B / 0B
csp-viper	0.00%	0B / 0B

After making sure that **ALL** the docker containers are up and running, you should proceed to check if the application user interfaces are responding. Please see the URLs of web interfaces at the beginning of this manual.

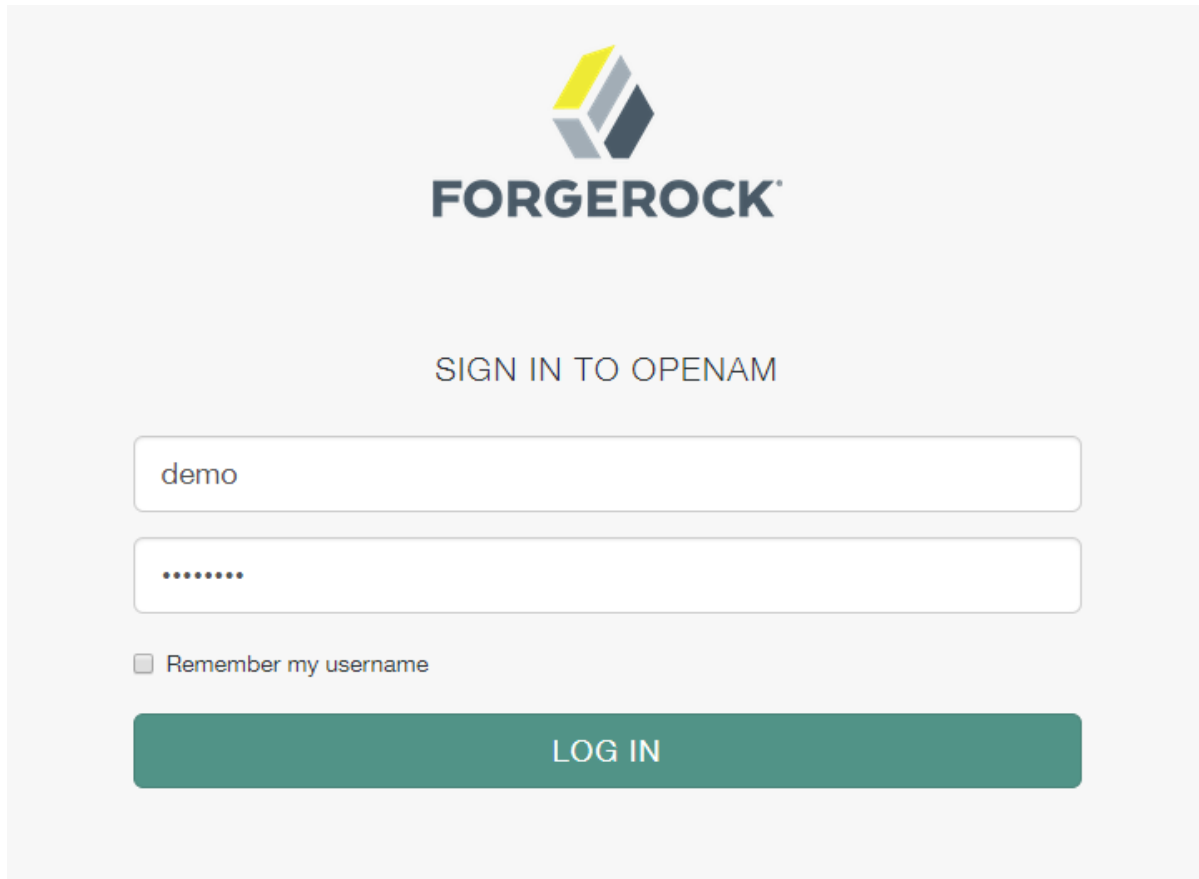
### 7.1 Connecting via the “Single Sign-on” service

When the user tries to access any application through its web interface, the system will initially try to perform a certificate authentication. If no valid certificate is found or the user is not prompted for a client Certificate (or if the user cancels the certificate driven authentication), the system will prompt the user to visit the user authentication page via OpenAM. (depending on the browser, the user may need to press “continue” in a system dialog presented).

The following image is shown when the browser is unable to authenticate using a client certificate making OpenAM fall back to traditional “username/password” authentication. using the “Return to the login page” link.



By visiting the login page, the user should enter default credentials for authentication (currently demo/changeit). The administrator should change them and/or introduce further users of the platform.





Please note that since the authentication system functions as Single Sign On system, the user will not be prompted again for authentication in each application unless logging out of an application or terminating the session due to time expiration or cookie deletion (e.g. by closing the web browser). Not all web interfaces currently offer a log-out option but in any case, this can be performed by visiting the OpenAM web interface.

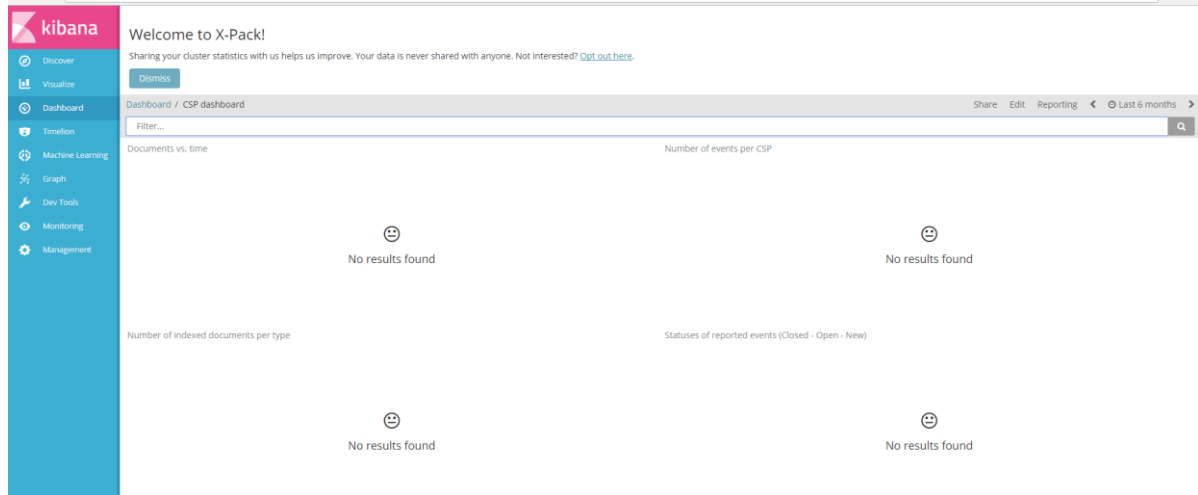
Also note than when accessing the various web interfaces, an SSL Insecure connection notice may appear due to the existence of self-signed certificates. The user should bypass the warning and proceed.

## **7.2 Connecting to individual services**

The proper operation of all the following services should be confirmed.

Search: [https://search.<cspld>.\[preprod.\]melicertes.eu](https://search.<cspld>.[preprod.]melicertes.eu)

Navigate to Kibana by entering the above URL to your browser.



The web interface will display an empty Kibana dashboard. This is normal behaviour for the first time the system is used. Data will appear in the Kibana dashboard as soon as information of the CSP is synchronized.

Trust Circles: [https://tc.<cspld>.\[preprod.\]melicertes.eu](https://tc.<cspld>.[preprod.]melicertes.eu)

Navigate to Trust Circles by entering the above URL to a browser. A page similar to the following should appear and a user as assigned with OpenAM should appear as logged in in the top right corner.

EU CCSPI
Teams
CTC
LTC
Contacts
Received Data
Configuration
Search
Go
admin

## All Central Teams & Trust Circles

5
Central Teams
View all Central Teams

12
Central Trust Circles
View all Central Trust Circles

2
Local Trust Circles
View all Local Trust Circles

4
Contacts
View all Contacts

### Central Teams

+ Add Central Team

	Name	Country	#CTC	Created	CSP Installed	Status
	central-csp	*European Union	12	May 15, 2018	Yes	Active
	demo1-csp	Germany	11	May 15, 2018	No	Active
	demo2-csp	Greece	12	May 15, 2018	Yes	Known
	demo3-csp	Finland	0	May 15, 2018	Yes	Active
	world-gov-csirt	*World Wide	12	Feb. 5, 2018	No	Active

Showing 1 to 5 of 5 rows

### Central Trust Circles

+ Add Central Trust Circle

	Short Name	Full Name	TLP	# of Teams	Created
	CTC::SHARING_DATA_CONTACT	CTC::SHARING_DATA_CONTACT	-	4	June 19, 2017
	CTC::FIRST	FIRST Trust Circle	-	4	April 25, 2017
	CTC::SHARING_DATA_INCIDENT	CTC::SHARING_DATA_INCIDENT	-	4	June 19, 2017
	CTC::SHARING_DATA_EVENT	CTC::SHARING_DATA_EVENT	-	4	June 19, 2017
	CTC::SHARING_DATA_ARTEFACT	CTC::SHARING_DATA_ARTEFACT	-	4	June 19, 2017
	CTC::SHARING_DATA_CHAT	CTC::SHARING_DATA_CHAT	-	4	June 19, 2017
	CTC::TI:Accredited	TI Accredited Teams	-	4	April 25, 2017
	CTC::SHARING_DATA_FILE	CTC::SHARING_DATA_FILE	-	4	June 19, 2017
	CTC::SHARING_DATA_THREAT	CTC::SHARING_DATA_THREAT	-	4	June 19, 2017
	CTC::SHARING_DATA_VULNERABILITY	CTC::SHARING_DATA_VULNERABILITY	-	4	June 19, 2017

**Contact Management:** [https://tc.<cspld>.\[preprod.\]melicertes.eu/local/contacts/teams/](https://tc.<cspld>.[preprod.]melicertes.eu/local/contacts/teams/)

Navigate to Contact Management by entering the above URL to a browser. A page similar to the following should appear and a user as assigned with OpenAM should appear as logged in in the top right corner.

EU CCSPi					
Teams					
CTC					
LTC					
Contacts					
Received Data					
Configuration					
Search					
Go					
admin					
Teams					
People					
+ Add Team					
	Name	Country	#CTC	Created	Status
	foo	*World Wide	0	Feb. 12, 2018	Other
	official name	United Kingdom	0	March 6, 2018	Active
Showing 1 to 2 of 2 rows					

RT: [https://rt.<cspld>.\[preprod.\]melicertes.eu/RTIR](https://rt.<cspld>.[preprod.]melicertes.eu/RTIR)

Navigate to RT by entering the above URL to your browser.

A page similar to those depicted on the following figure will be displayed and the logged in user will be displayed at the top of the page.

RTIR at a glance

Logged in as rt-admin

New unlinked Incident Reports...

#	Subject	Requestor	Owner	Due	Queue	Take
16	[demo2-csp:misp] testing timestamps 01		rt-admin		Incident Reports	
34	[demo1-csp:misp] test timestamp 05		rt-admin		Incident Reports	
7	[demo3-csp:misp] monday morning 1		rt-admin		Incident Reports	
17	[demo2-csp:misp] testing timestamps 01		rt-admin		Incident Reports	
4	[demo3-csp:misp] christos4 demo3.1		rt-admin		Incident Reports	
35	[demo1-csp:misp] test event 01		rt-admin		Incident Reports	
18	[demo2-csp:misp] testing timestamps 01		rt-admin		Incident Reports	
3	[demo3-csp:misp] christos4 demo3.1		user1		Incident Reports	
5	[demo3-csp:misp] christos4 demo3.1		rt-admin		Incident Reports	
19	[demo2-csp:misp] testing timestamps 01		rt-admin		Incident Reports	

Most due incidents owned by rt-admin

#	Subject	Due	Owner	Updates
800	p-005		rt-admin	No
806	test 0.4.0 05 incident		rt-admin	No
677	1623 msg origin demo3		rt-admin	New
807	p-006		rt-admin	No
873	TC_Incident_001		rt-admin	No
808	msg demo2 update last by demo3		rt-admin	No
611	[demo1-csp:misp] example event 0101		rt-admin	No
809	demo3 update on demo2		rt-admin	No
810	demo3 nummer 2sdfgdfg		rt-admin	No
804	demo3 updated on demo3		rt-admin	No

Work with constituency

All constituencies

Countermeasures

	pending activation	active
Countermeasures	-	-

Incident Reports

Incidents

Investigations

Refresh

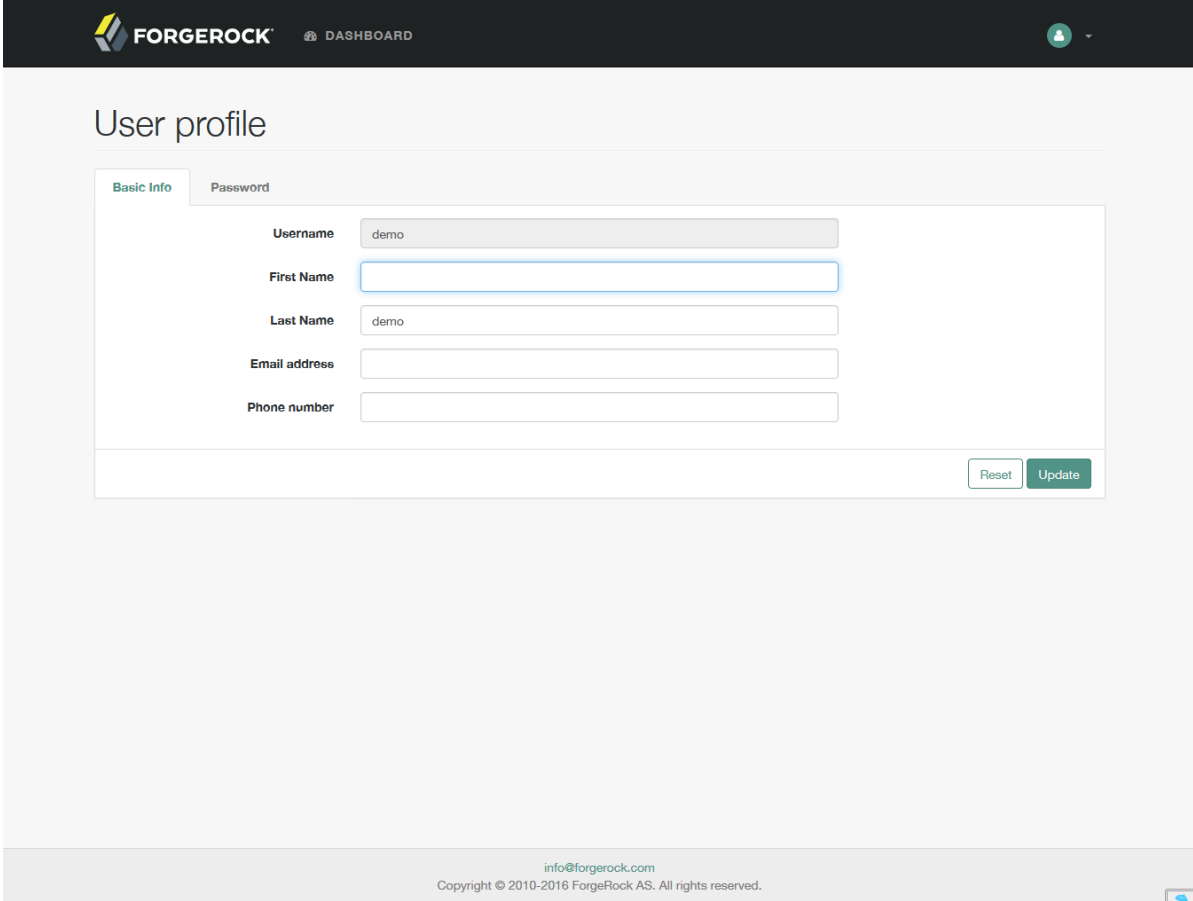
Don't refresh this page.

Go!

**OpenAM:** [https://auth.<cspld>.\[preprod.\]melicertes.eu/openam](https://auth.<cspld>.[preprod.]melicertes.eu/openam)

Navigate to OpenAM by entering the above URL to your browser.

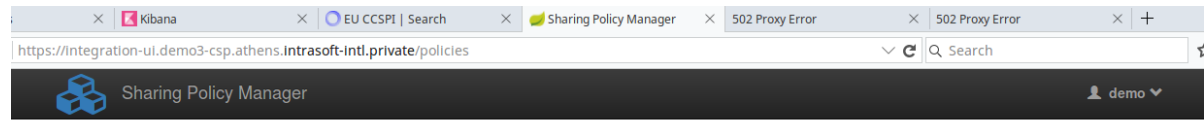
A basic user editing information should be displayed.



The screenshot shows the ForgeRock user profile management interface. At the top, there is a dark header with the ForgeRock logo, a 'DASHBOARD' link, and a user profile icon. Below the header, the main content area is titled 'User profile'. There are two tabs: 'Basic Info' (selected) and 'Password'. The 'Basic Info' tab contains a form with the following fields: 'Username' (pre-filled with 'demo'), 'First Name' (empty), 'Last Name' (pre-filled with 'demo'), 'Email address' (empty), and 'Phone number' (empty). At the bottom right of the form are 'Reset' and 'Update' buttons. The footer of the page contains the email 'info@forgerock.com' and the copyright notice 'Copyright © 2010-2016 ForgeRock AS. All rights reserved.'

Sharing Policies: [https://integration-ui.<cspld>.\[preprod.\]melicertes.eu](https://integration-ui.<cspld>.[preprod.]melicertes.eu)

Navigate to Sharing Policies application by entering the above URL to a browser.



## Welcome to Sharing Policy Management

### Save Policy

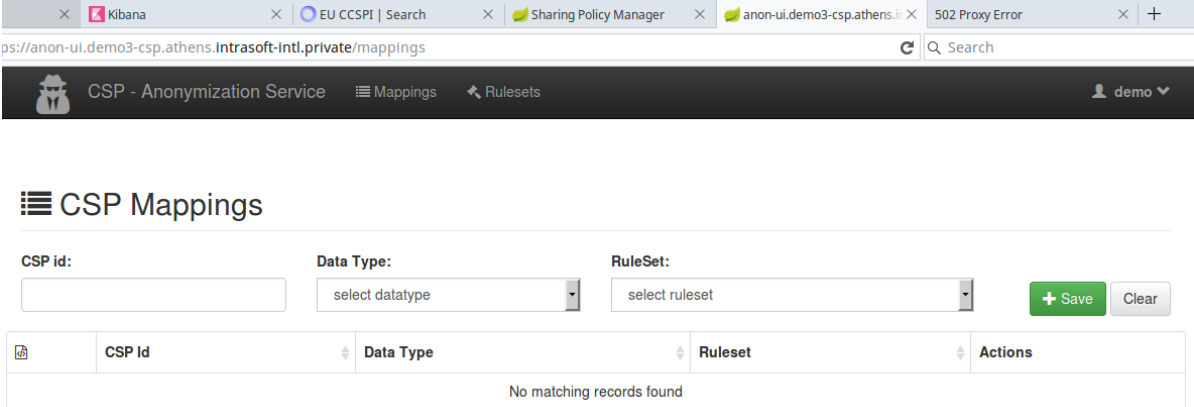
**Data Type:** 
**Status:** 
**Condition:** 
**Sharing Policy Action:**

### Stored Policies

Id	DataType	Status	Condition	Sharing Policy Action	Actions
1	threat	Default	no condition required	Do not share	
2	event	Default	no condition required	Do not share	
3	artefact	Default	no condition required	Do not share	
4	incident	Default	no condition required	Do not share	
5	contact	Default	no condition required	Do not share	
6	file	Default	no condition required	Do not share	
7	chat	Default	no condition required	Do not share	
8	vulnerability	Default	no condition required	Do not share	

**Anonymization:** [https://anon-ui.<cspld>.\[preprod.\]melicertes.eu](https://anon-ui.<cspld>.[preprod.]melicertes.eu)

Navigate to Anonymization application by entering the above URL to a browser.



ps://anon-ui.demo3-csp.athens.intrasoft-intl.private/mappings

CSP - Anonymization Service | Mappings | Rulesets | demo

### CSP Mappings

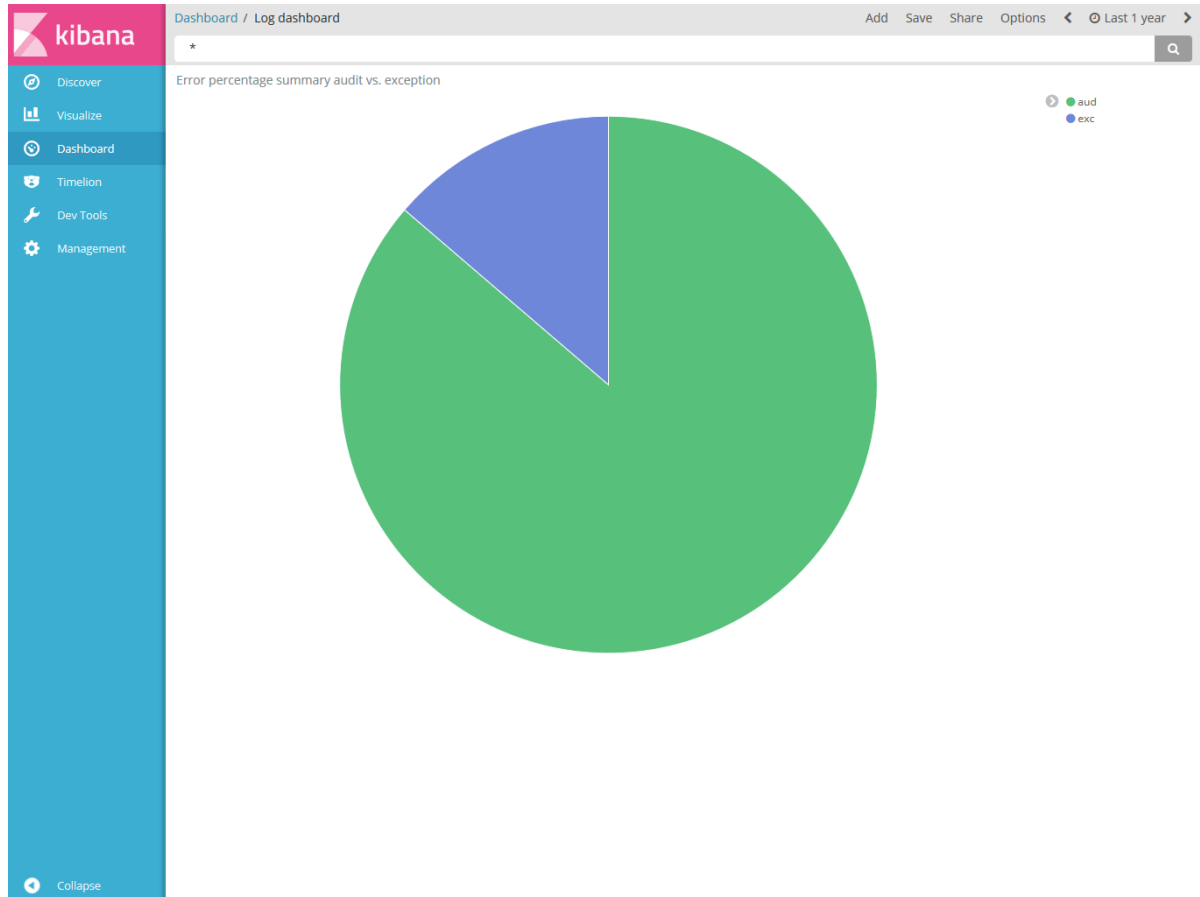
**CSP id:**   
**Data Type:**   
**RuleSet:**

	CSP Id	Data Type	Ruleset	Actions
No matching records found				



Logs: [https://logs.<cspld>.\[preprod.\]melicertes.eu](https://logs.<cspld>.[preprod.]melicertes.eu)

Navigate to the log display application by entering the above URL to a browser



A log dashboard regarding audit and exception logs should be displayed.

MISP: [https://misp-ui.<cspld>.\[preprod.\]melicertes.eu](https://misp-ui.<cspld>.[preprod.]melicertes.eu)

Navigate to the MISP web interface by entering the above URL to a browser

[Home](#)
[Event Actions](#)
[Galaxies](#)
[Input Filters](#)
[Global Actions](#)
[Sync Actions](#)
[Administration](#)
[Audit](#)

MISP Demo Log out

[List Events](#)
[Add Event](#)
[Import From MISP Export](#)

[List Attributes](#)
[Search Attributes](#)

[View Proposals](#)
[Events with proposals](#)

[Export](#)
[Automation](#)

## Events

« previous
1
2
3
next »

My Events Org Events


Filter


<input type="checkbox"/>	Published	Org	Owner Org	Id	Clusters	Tags	#Attr.	Email	Date	Info	Distribution	Actions
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	327			0	demo@intrasoft-intl.private	2018-03-01	3	Community	
<input type="checkbox"/>		CSP::demo3-csp	CSP::demo1-csp	326			5	integration@melicertes.eu	2018-02-27	TC_Event_N003	Community	
<input type="checkbox"/>		CSP::demo3-csp	CSP::demo1-csp	325		threat	5	integration@melicertes.eu	2018-02-27	TC_Threat_N003	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	324			0	demo@intrasoft-intl.private	2018-02-27	TC_Event_N002	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	323		threat	0	demo@intrasoft-intl.private	2018-02-27	TC_Threat_N002	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	322			0	demo@intrasoft-intl.private	2018-02-27	test	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	321		threat	0	demo@intrasoft-intl.private	2018-02-27	TC_Threat_091	Community	
<input type="checkbox"/>		CSP::demo3-csp	CSP::demo1-csp	320			7	integration@melicertes.eu	2018-02-27	TC_EVENT_090	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	318			0	demo@intrasoft-intl.private	2018-02-27	TC_Threat_006.1	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	319		threat	6	demo@intrasoft-intl.private	2018-02-27	TC_Threat_006.2	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	317			7	demo@intrasoft-intl.private	2018-02-27	TC_Threat_006	Community	
<input type="checkbox"/>		CSP::demo3-csp	CSP::demo1-csp	316			7	integration@melicertes.eu	2018-02-27	TC_Event_005	Community	
<input type="checkbox"/>		CSP::demo3-csp	CSP::demo1-csp	315		threat	7	integration@melicertes.eu	2018-02-27	TC_Threat_005	Community	
<input type="checkbox"/>		CSP::demo3-csp	CSP::demo1-csp	311			0	integration@melicertes.eu	2018-02-27	TC_Event_003	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	313		threat	0	demo@intrasoft-intl.private	2018-02-27	TC_Threat_004.1	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	314			1	demo@intrasoft-intl.private	2018-02-27	TC_Event_004	Community	
<input type="checkbox"/>		CSP::demo3-csp	CSP::demo1-csp	310		threat	1	integration@melicertes.eu	2018-02-27	TC_Threat_003	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	312			1	demo@intrasoft-intl.private	2018-02-27	TC_Threat_004	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	309			0	demo@intrasoft-intl.private	2018-02-27	TC_Event_002	Community	
<input type="checkbox"/>		CSP::demo1-csp	CSP::demo1-csp	308		threat	0	demo@intrasoft-intl.private	2018-02-27	TC_Threat_002	Community	
<input type="checkbox"/>		CSP::demo3-csp	CSP::demo1-csp	307			0	integration@melicertes.eu	2018-02-27	TC_Event_001	Community	

Could not locate the PGP/GPG public key.


Powered by MISP 2.4.87

IntelMQ: [https://imq.<cspld>.\[preprod.\]melicertes.eu](https://imq.<cspld>.[preprod.]melicertes.eu)


[Configuration](#)
[Management](#)
[Monitor](#)
[Check](#)
[About](#)




# INTELMQ




### Configuration

To either change the currently deployed configuration or to create a new one in a graphical fashion.




### Management

This is where you go to start/stop your bots or check on their status.




### Monitor

This feature is meant to allow you to check on the overall status of your botnet. You can read the bot logs, see how the queues are behaving and other features that allow you to have a better overview of the overall health of the system.



### Check

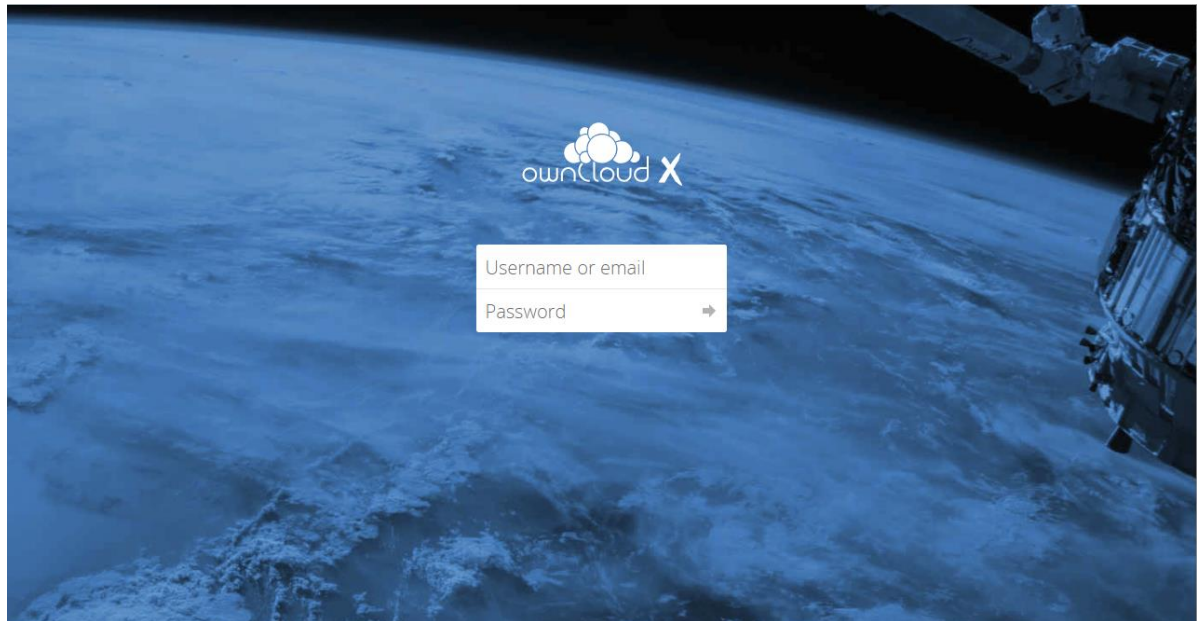
Check IntelMQ is running properly.



### About

To learn more about the project's goals and contributors.

Owncloud: [https://files.<cspld>.\[preprod.\]melicertes.eu](https://files.<cspld>.[preprod.]melicertes.eu)



Videobridge (Jitsi): [https://teleconf-ui.<cspld>.\[preprod.\]melicertes.eu](https://teleconf-ui.<cspld>.[preprod.]melicertes.eu)

VCBridge Admin    My Meetings    Email Templates    demo

### My Meetings

Scheduled Meetings    Past Meetings

Nothing to display yet. [Create a new meeting now](#)

Create meeting

Viper: [https://viper-ui.<cspld>.\[preprod.\]melicertes.eu](https://viper-ui.<cspld>.[preprod.]melicertes.eu)

VIPERS    Projects    Yara Rules    CLI    Search in all Projects    Name    Search    More    Logout (demo)

Home / default

Upload new Sample File    Upload Sample(s) Archive    Download Sample from URL    Download Sample from Virustotal (disabled)

Choose file    Tags for Sample (comma separated)    Upload

Samples in Project: default

Show 10 entries    Search:

#	SHA256	Name	Mime Type	Size	Tags
No data available in table					

Showing 0 to 0 of 0 entries    First    Previous    Next    Last

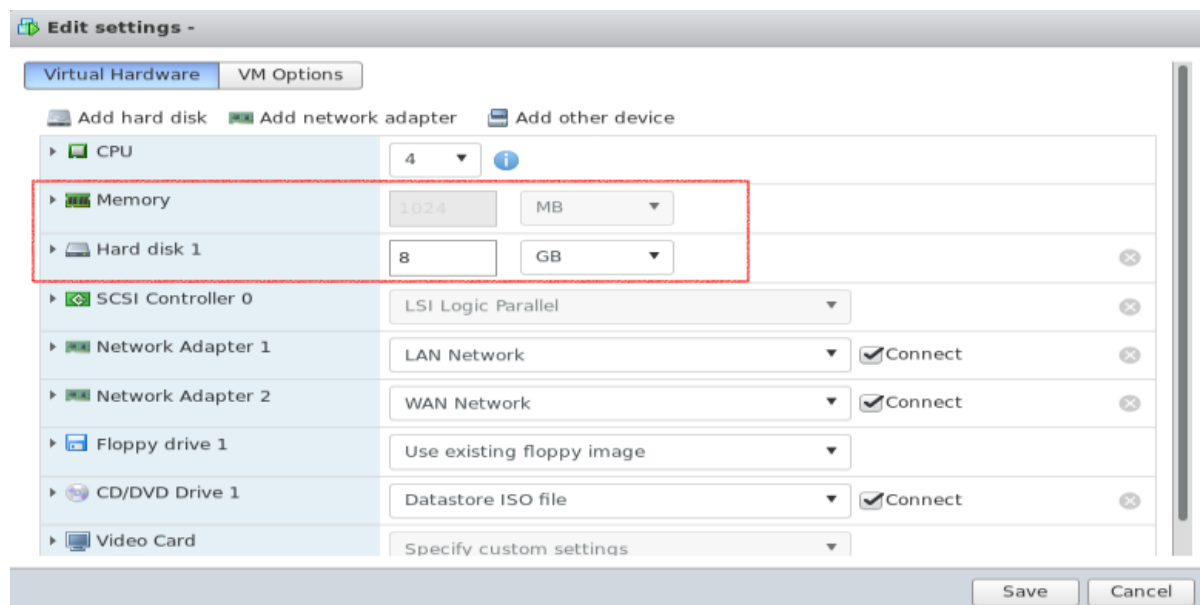
## 8 Annex A: Changing settings of the VM

The virtual machine settings in ESXi allow two operations, prior to booting the machine up:

- Changing of allocated memory: The administrator should allocate at least 24GB (half of recommended) to complete installation and initial CSP sanity tests, using the settings page of the virtual machine.
- Changing of allocated disk: the allocated disk for this VM is too small (16GB) and out of disk is possible. The administrator should allocate 400 GB of fast disk (as per the recommended setup) for the initial period, in a "thin" type of disk (so no pre-allocation). However, this only expands the disk itself, not the underlying filesystem and a reboot will be necessary if the machine is powered on for the change to be made visible. Please check below for instructions to achieve this.

Note: if the machine has already booted, you should shut it down normally (use either the root account or ESXi option) to configure settings.

See the figure below for a typical ESXi 6.0 settings screen (web UI):



The highlighted part of the settings is the one that needs to be adjusted. Please make sure the adjustments are made when the machine is stopped, otherwise the settings will not be available to be modified.

To complete the adjustment process, follow the next section to expand the file system *within the VM*.

### 8.1 Expanding the VM root filesystem

The expansion of the filesystem is a two phase process: first phase is to adjust settings (previous section). The next phase is to expand filesystem (this section).

To expand the root filesystem (ext4fs) the following steps are necessary (all items are root commands):

- Check partition size:

```
$ df -h /
Filesystem      Size      Used Available Use% Mounted on
/dev/sda3       40G       913.8M    39,1G     1% /
```

- Verify that partition is indeed larger:

```
$ dmesg | grep sda #check the output to see new disk size
```

- Stop docker services running:

```
$ rc-service docker stop
```

- Add packages required for this operation:

```
$ apk update add parted e2fsprogs-extra
```

- Resize partition, using fdisk (note that all commands below after fdisk, are to be entered one after the other:

```
$ fdisk /dev/sda
```

```

▪      d
▪      3
▪      n
▪      p
▪      3
▪      enter
▪      enter
▪      N
▪      w

```

*With the last one the system should exit fdisk writing changes.*

- Refresh partition table:

```
$ partprobe
```

- Resize partition:

```
$ resize2fs /dev/sda3
```

- Verify partition is resized:

```
$ df -h /
```

Filesystem	Size	Used	Available	Use%	Mounted on
/dev/sda3	400G	913.8M	399,1G	1%	/

- Reboot the machine:

```
$ sync;sync;reboot
```

On reboot of the machine, the system should be ready for installation.

## 9 Annex B: Jitsi VideoConferencing Bridge

The Jitsi VideoConferencing bridge provides a number of features to assist the user in scheduling and conducting a video conference meeting. The following sections discuss the requirements and configuration necessary for successful meetings.

### 9.1 External port accessibility

The following ports should be available from the internet via either full exposure (e.g. installation in DMZ) or a “Full-Cone NAT” or Symmetric NAT:

- Port 10000, UDP – used for encrypted media (audio/video). This port should be enabled in order to allow low-latency communication;
- Port 4443, TCP – used for encrypted media (audio/video) in case of problems accessing the UDP port.
- Port 6443, TCP – used for the main web interface

**Important note:** If the UDP port is not available, conferences may experience bandwidth and/or latency issues due to the nature of TCP fallback (retransmissions, ack window, etc.).

### 9.2 Bandwidth requirements

The Jitsi Videoconferencing Bridge implements a “Selective Forwarding Units – SFU” in Videoconferencing terms. This means that it is scalable and geared towards “asymmetric” links, having more “downstream” bandwidth in the case of a client / participant, and “near” symmetric bandwidth in the case of the bridge itself. Technically the bridge requires as much bandwidth as necessary to be able to receive all streams from all participants and then N times as much to be able to distribute all the received streams to all participants.

A full example for a HD conference (720p) is shown below:

- The audio stream consumes about 50 Kbps (average) for each participant;
- The video stream consumes about 500 Kbps (average) for a combined audio/video total of 550 Kbps per participant.
- For a conference with 5 endpoints ( $N = 5$ ), the theoretical bandwidth required would be:
  - o Clients:
    - Send: 550 Kbps (one video and one audio channel)
    - Receive:  $550 \times (N - 1) = 550 \times 4 = 2200$  Kbps (video/audio from 4 participants)
  - o Server (bridge):
    - Receive:  $550 \times N = 550 \times 4 = 2200$  Kbps (Bridge receives N participant audio/video streams)
    - Send:  $550 \times (N) \times (N - 1) = 550 \times 5 \times 4 = 11000$  Kbps (Bridge transmits 4 audio/video streams to each of 5 participants, each participant does not receive back his/her own stream)

However, there are optimization techniques used that make the bandwidth requirements much less:

- *Available Bandwidth detection* – Jitsi actively monitors latency of the links and bandwidth availability; in cases of reduced bandwidth, video quality may be lowered, or video stopped completely.
- *Use of “Simulcast”* – a browser feature that allows various levels of quality for a video stream to be concurrently streamed from a client, allowing the bridge to decide based on bandwidth calculations whether to forward an HD / SD / LD stream to other participants.
- *Use of “Last-N” active speakers* – using activity detection, the bridge only forwards video/audio of the “Last-N” active speakers instead of everyone to everyone.

<sup>5</sup> See <https://jitsi.org/jitsi-videobridge-performance-evaluation/> and <https://webrtcglossary.com/sfu/> for SFU explanation



To conclude, the numbers for the above calculation can be considered as the absolute maximum, for 5 participants and HD video.

## 10 Annex C: Troubleshooting CSP Installer

In case you experience errors in accessing CSP applications after the completion of the CSP installation, in this chapter you may find specific steps to follow, especially for HTTP Error Code 403 (Forbidden) when requesting a CSP application UI.

To resolve the situation you have to connect to the CSP VM via SSH as described earlier in this manual.

At this point you have to make sure that the installation of the CSP Installer application has successfully created all the required OpenAM and Apache web agents for accessing any available CSP application.

### Checking the creation of OpenAM web agents:

In your terminal execute the command:

```
# fgrep "ACTIONS COMPLETED" /tmp/spring.log
```

If all OpenAM web agents have successfully created the output should contain the following lines (indicating true in all services):

```
ACTIONS COMPLETED: OAM : true - APC : true for service ActiveMQ
ACTIONS COMPLETED: OAM : true - APC : true for service anon
ACTIONS COMPLETED: OAM : true - APC : true for service il
ACTIONS COMPLETED: OAM : true - APC : true for service kibana
ACTIONS COMPLETED: OAM : true - APC : true for service logs
ACTIONS COMPLETED: OAM : true - APC : true for service trustcircles
ACTIONS COMPLETED: OAM : true - APC : true for service misp
ACTIONS COMPLETED: OAM : true - APC : true for service rt
ACTIONS COMPLETED: OAM : true - APC : true for service intelmq
ACTIONS COMPLETED: OAM : true - APC : true for service vcb
ACTIONS COMPLETED: OAM : true - APC : true for service viper
```

In other words, the complete output of the above command should look like:

```
2018-10-12 11:35:26.265 INFO 2363 --- [pool-3-thread-1] c.i.c.c.service.BackgroundTaskService : ACTIONS COMPLETED: OAM : true - APC : true for service ActiveMQ
2018-10-12 11:35:43.026 INFO 2363 --- [pool-3-thread-1] c.i.c.c.service.BackgroundTaskService : ACTIONS COMPLETED: OAM : true - APC : true for service anon
2018-10-12 11:36:01.162 INFO 2363 --- [pool-3-thread-1] c.i.c.c.service.BackgroundTaskService : ACTIONS COMPLETED: OAM : true - APC : true for service il
2018-10-12 11:41:20.341 INFO 2363 --- [pool-3-thread-1] c.i.c.c.service.BackgroundTaskService : ACTIONS COMPLETED: OAM : true - APC : true for service kibana
2018-10-12 11:41:37.401 INFO 2363 --- [pool-3-thread-1] c.i.c.c.service.BackgroundTaskService : ACTIONS COMPLETED: OAM : true - APC : true for service logs
2018-10-12 11:42:06.261 INFO 2363 --- [pool-3-thread-1] c.i.c.c.service.BackgroundTaskService : ACTIONS COMPLETED: OAM : true - APC : true for service trustcircles
2018-10-12 11:42:26.198 INFO 2363 --- [pool-3-thread-1] c.i.c.c.service.BackgroundTaskService : ACTIONS COMPLETED: OAM : true - APC : true for service misp
2018-10-12 11:42:45.213 INFO 2363 --- [pool-3-thread-1] c.i.c.c.service.BackgroundTaskService : ACTIONS COMPLETED: OAM : true - APC : true for service rt
2018-10-12 11:43:09.721 INFO 2363 --- [pool-3-thread-1] c.i.c.c.service.BackgroundTaskService : ACTIONS COMPLETED: OAM : true - APC : true for service intelmq
2018-10-12 11:47:44.368 INFO 2363 --- [pool-3-thread-1] c.i.c.c.service.BackgroundTaskService : ACTIONS COMPLETED: OAM : true - APC : true for service vcb
2018-10-12 11:54:26.152 INFO 2363 --- [pool-3-thread-1] c.i.c.c.service.BackgroundTaskService : ACTIONS COMPLETED: OAM : true - APC : true for service viper
```

In case one or more from the above listed lines is missing from your terminal you have to execute the following command (one time per missing line):

```
# docker exec -it csp-oam script /dev/null -c "create-agent.sh {ITEM}"
```

where {ITEM} represents the missing item and can be one of the following:

- activemq
- anon-ui
- integration-ui
- search
- logs
- tc
- misp-ui
- rt
- imq
- teleconf-ui
- viper-ui

## 11 Annex D: Troubleshooting the connection tunnel to the VM

The initial start of a VM does several checks, including an auto-update check that may take a significant amount of time. However, the installer process is setup to automatically restart, and it will eventually do so.

You are always able to check that the CSP Installer process is running by issuing the following command on the VM terminal:

```
# ps -ef | grep cspinst
```

Normally, and provided that the CSP Installer is running and its start-up has been completed, the output of the previous command should look like:

```
# cspvm [~]# ps -ef | grep cspinst
# 2170 root      0:00 grep cspinst
# 32135 root      0:00 /bin/bash -c /opt/cspinst/cspinstaller.sh
>/tmp/console.log 2>&1
# 32136 root      0:00 bash /opt/cspinst/cspinstaller.sh
# 32149 root      0:00 {cspinstaller.jar} /bin/bash ./cspinstaller.jar
# 32166 root     109:35 /opt/cspinst/java/bin/java -
Dsun.misc.URLClassPath.disableJarChecking=true -jar
/opt/cspinst/cspinstaller.jar
```

Additionally, you are able to check that the tunnel to port TCP/18080 has been opened, thus you will be able to access CSP Installer's web interface, by issuing the command:

```
# netstat -tnl | grep 18080
```

In case tunnel to port TCP/18080 has been opened, you should see a single line, with "LISTEN" at the end, as follows:

```
# cspvm [~]# netstat -tnl | grep 18080
# tcp          0          0 :::ffff:127.0.0.1:18080 :::*      LISTEN
```

## 12 Annex E: Manual Installation and configuration of the CSP Installer

---

*This Annex describes the process of configuring CSP Installer in a clean Alpine Host and is **obsolete**.*

*OVA files that are delivered from CSP Central in production (prod.melicertes.eu) and staging (stage.melicertes.eu) environments already include the configuration described here.*

*What is described here is applicable if CSP Helpdesk requires that you install manually a new installer.*

---

Before installing a CSP Node a set of certain steps have to be taken so as to properly configure the CSP Installer daemon which will in turn communicate with the Central CSP Server and acquire applications, updates, etc.

Prerequisites for the pre-installation steps mentioned in this paragraph are:

- You have configured your network according to guidelines reported in chapter 2 of this manual
- You have ensured SSH access to the CSP Node, as described in previous chapter
- You have obtained an image of the CSP Installer application, i.e. a file named: CSP-VM-installer-v1.tgz

### STEP 1

From your terminal run the following command to upload the CSP Installer's tarball to the /tmp directory of the CSP VM:

```
# scp CSP-VM-installer-v1.tgz root@<guestmachinehostname>:/tmp
```

Alternatively, you may use an SFTP client application of your choice, i.e. FileZilla.

After uploading the compressed tarball file, execute the following command to extract its contents and ensuring that /opt directory is present on the VM:

```
# cd /tmp
# tar -zxvf CSP-VM-installer-v1.tgz
# mkdir -p /opt
```

### STEP 2

At this point you are ready to start the installation of the CSP Installer as follows:

```
# sh install.sh
```

Let the script finish and notice/copy the last line of its response, that should like:

```
# tty5::respawn:/bin/bash -c /opt/cspinst/cspinstaller.sh
```

### STEP 3

At this step CSP Installer application will be configured to run automatically. To do this we are going to replace the tty5 related line in file /etc/inittab with the one copied from previous step. In details, open /etc/inittab for editing via:

```
# vi /etc/inittab
```

Navigate to line starting with tty5 and when the cursor is blinking at the start of the line press keys: **i** and **#**.

Add a line right after this line and paste the copied line from previous step. After the modification the file should look as shown below:

```
# /etc/inittab

::sysinit:/sbin/openrc sysinit
::sysinit:/sbin/openrc boot
::wait:/sbin/openrc default

# Set up a couple of getty's
tty1::respawn:/sbin/getty 38400 tty1
tty2::respawn:/sbin/getty 38400 tty2
tty3::respawn:/sbin/getty 38400 tty3
tty4::respawn:/sbin/getty 38400 tty4
#tty5::respawn:/sbin/getty 38400 tty5
tty5::respawn:/bin/bash -c /opt/cspinst/cspinstaller.sh
tty6::respawn:/sbin/getty 38400 tty6

# Put a getty on the serial port
#ttys0::respawn:/sbin/getty -L ttys0 115200 vt100

# Stuff to do for the 3-finger salute
::ctrlaltdel:/sbin/reboot

# Stuff to do before rebooting
::shutdown:/sbin/openrc shutdown
```

Press keys: **Esc** and the sequence: **wq** to save and exit editor.

#### Important Notice:

It is strongly recommended for administrative reasons the above line could also include a log file to monitor CSP Installer's activity. If such functionality is desired, then the line should be entered as follows:

```
# tty5::respawn:/bin/bash -c "/opt/cspinst/cspinstaller.sh >/tmp/console.log 2>&1"
```

assuming that /tmp/console.log is the desired log file.

### STEP 4

Configure CSP Installer daemon with the proper DNS entries, regarding your Central CSP Node. To do this you have to edit file /opt/cspinst/cspinstaller.sh as follows:

```
# vi /opt/cspinst/cspinstaller.sh
```

Edit lines 10 and 11 to configure the correct CSPHOST and CSPCONFUI parameters. An example is shown below:

```
CSPHOST="central.{YOUR-CSP-environment.}melicertes.eu"
```

```
CSPCONFUI="config.central.{YOUR-CSP-environment.}melicertes.eu"
```

Where,{YOUR-CSP-environment.} is the DNS prefix of your CSP installation in the melicertes.eu ecosystem.

## STEP 5

At this point you have to upload and insert the Root Certificate obtained via the process described in chapter 3 of this manual (and specifically in paragraph 3.5). Uploading can be done by executing in your terminal:

```
# scp CA_Bundle.crt
root@<guestmachinehostname>:/opt/cspinst/jdk1.8.0_144/jre/lib/security/
```

assuming that the certificate obtained from paragraph 3.5 is named: CA\_Bundle.crt. Also, this step can be alternatively performed by using an SFTP client application of your choice, i.e. FileZilla.

After uploading the certificate, execute the following commands:

```
# cd /opt/cspinst/jdk1.8.0_144/jre/lib/security/
# /opt/cspinst/jdk1.8.0_144/bin/keytool -importcert -file CA_Bundle.crt -
keystore cacerts -trustcacerts
```

When prompted for password you have to enter: **changeit** and when prompted for trusting the certificate you have to type: **yes** and hit **Enter**.

## STEP 6

At this point you have to reboot the VM in order to let the CSP Installer application autostart. Also notice that each time the CSP Installer starts it also checks for updates and execute a self-update procedure.

For information on CSP Installer application troubleshooting you may see Chapter 10 (Annex C: Troubleshooting CSP Installer) of this manual.

- End of document-