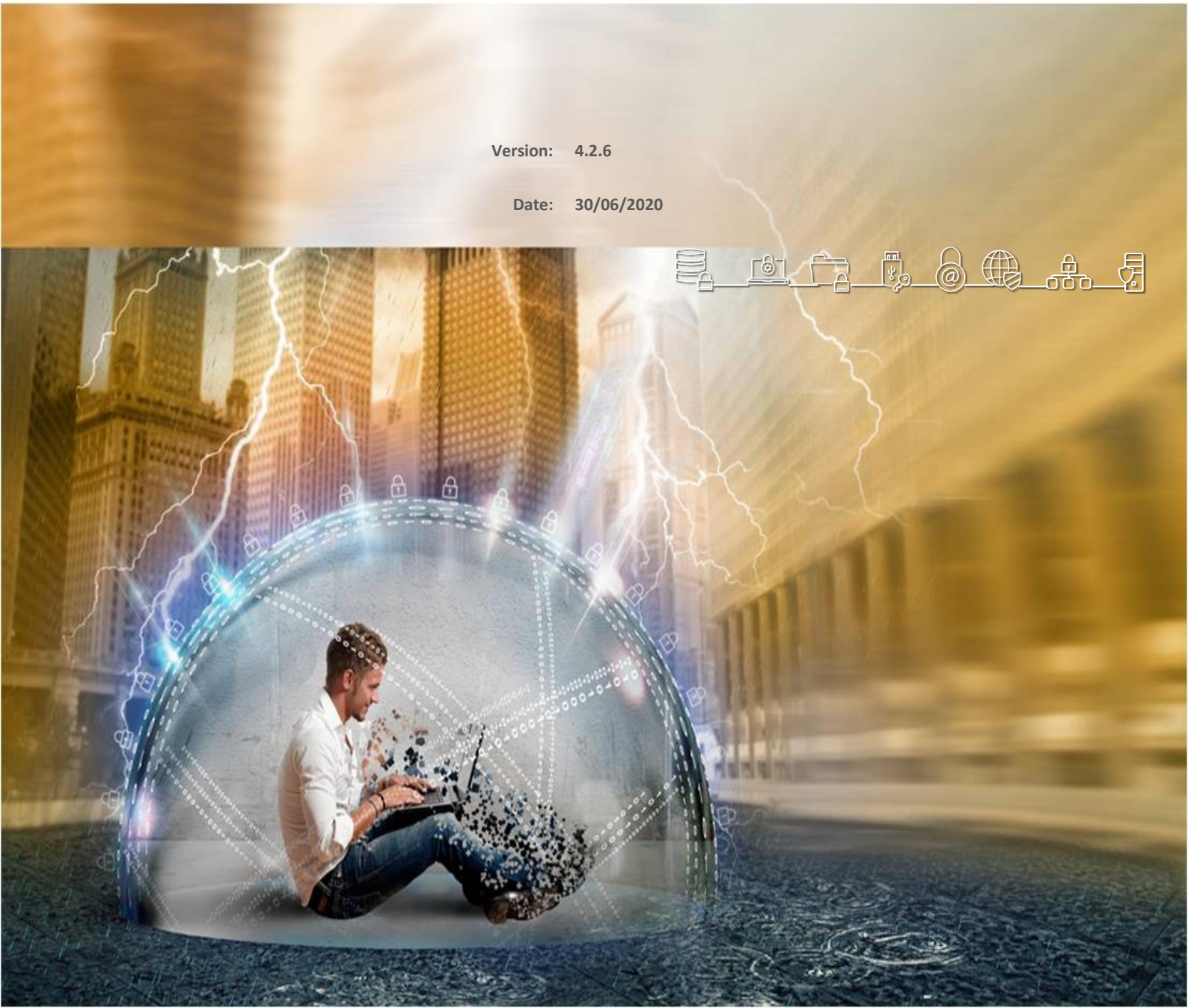
CEF: Cybersecurity Digital Service Infrastructure;

Core Service Platform – SMART 2015/1089

Installation Manual



Version: 4.2.6

Date: 30/06/2020

Contents

1 Introduction and installation Requirements for the CSP

1.1 Introduction

The CSP instance during its entire life cycle from installation to operation until end of service will need access to the Internet. The CSP instance needs to be able to initiate outgoing connections. Additionally, some of the CSP's internet facing services and ports need to be accessible from the Internet in order to provide the desired collaboration functions depending on the needs of the team running the service and its collaboration partners.

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. While it is recommended to utilize VPN technology to provide access to any such User Interface if the user connects over the Internet or non-trusted networks, this is outside the scope of this document.

Note: Domains in the production environment are in the form of *.<cspID>.prod.melicertes.eu. A specific and immutable[1] string <cspID> that represents the entity assigned to each CSP instance and DNS entries are then created for each service that is published and you will need to access, for example: **Error! Hyperlink reference not valid.**, **Error! Hyperlink reference not valid.**, etc.

The DNS entries for "***central.prod.melicertes.eu***" have specific importance, as the Central Node provides the software repository as well as the Central Team and Central Trust Circle information. Such data is authoritative for the connected instances (all instances that share the domain name "prod.melicertes.eu" and henceforth access to "central" within this domain).

On regular intervals, Central Node administrators will push to all CSP node administrators the IP addresses of all CSIRTS participating in the MeliCERTes network in order to update their firewall. This is required to facilitate cooperation and exchange of messages between CSP nodes and allows Integration layer interconnectivity.
As new instances join the network, additions and changes of the IP addresses will be communicated to all instances to allow for any configuration changes.

More details about internet facing services, firewall rules and recommendations are discussed on paragraph *2* .

[1] Administrators should not change this string after the initial assignment, because it would disrupt communications of the Central CSP to and from the CSP instance.

1.2 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 with the rest of the installation steps please make sure, you have followed these steps:

1. You are eligible to participate in the MeliCERTes network and have registered for a CSP installation with the central CSP authority.
   Your Team has submitted a digitally signed **MeliCERTes Registration Form** containing Assigned CSP-ID, General NIS team information, Point of contact details, CSP installation IP address etc.
2. You received an email confirming your registration and prompting you to continue to Request a X.509 Server Certificate from the MeliCERTes PKI Registration Authority (see paragraph 3)
   Proceed to generate a private key and CSR and request Server Certificate signed by the CA.
3. You received an email with the
   a. Signed Server Certificate,
   b. A list with all the **DNS entries** that have been registered for your IP address and melicertes domain in the form of <cspId>.prod.melicertes.eu (e.g. cert-gr.prod.melicertes.eu).
   c. Your team data have been entered in the **central CSP trust circles**
   d. A link to download the base VM in OVA format, i.e. ***AlpineHost-v3.10.5-PROD.ova*** [2] and the **hardware requirements** for the CSP installation.
   e. A link to download manuals that are relevant to the installation, configuration and operation of the CSP: **CSP Installation**, **CSP Administration** and **CSP User** manual.
   The MeliCERTes project GitHub page[3] always has most up to date manuals.
4. Once you deploy the Virtual machine from the OVF **increase the disk space!** Continue to upload the certificates, fill in the form with your CSP-ID, Domain, Team details, etc. and your dashboard should show 50% complete.


5. At this point, you have to send an email to trust-central@melicertes.eu in order for Central CSP admins to configure the software application modules to be installed on your instance.
6. Download all modules first. Then install them one at a time starting from the top and proceed to the next, only if the previous one installed without errors!
7. After all software modules are installed and you have successfully started you instance you have to login in the OpenAM and Trust Circles applications, change passwords (recommended!). After that adjust sharing policies and if all is working as expected send email to trust-central@melicertes.eu in order to inform them to initiate the initial push of trust circles data to your instance.
8. The trust central admins will distribute a list of all CSIRTs participating in the MeliCERTes network that you will have to trust and allow to connect through your firewall to reach the CSP instance IL.

[2] Version is indicative and is subject to change

[3] https://github.com/melicertes/csp/tree/develop/documentation

1	***Recommended specifications of the CSP instance VM*** ***(More vCPU, RAM and Hard disk could be assigned depending on your usage and needs).***		
2	*Memory:*	*48 GB*	*(Could work with 24GB, but depends on usage)*
3	*Disk:*	*800 GB*	*(This depends on the volume of MISP, ELK events stored)*
4	*CPU:*	*16x vCores*	*(Could work with 4x vCores for testing purposes)*
5	*Internet connectivity*		*(DNS, NTP, Email SMTP)*

2 External Facing Services and Service URLs

As mentioned earlier the CSP instance during both initial installation and operation will need access to the internet.

The CSP instance needs to be able to:

- Initiate outgoing connections to:
  - the Central CSP (ports 80/tcp and 5443/tcp),
  - other CSP instances (5443/tcp),
  - DNS (53/udp), NTP (123/tcp) and Email (587/tcp or 465/tcp or 25/tcp) and OS update (443/tcp) servers.
- Accept incoming connections from:
  - The members of the MeliCERTes distributed network (port 5443/tcp).
  - The whole internet[4] on services that are used to
    - share files using owncloud (6443/tcp)
    - share MISP events (6443/tcp) and
    - Join Jitsi conference calls (4443/tcp and 10000/udp).
  - The Administrators of the local CSP instance (port 22/tcp and 443/tcp), exposing 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 *.<cspId>.preprod. melicertes.eu. Domains in the production environment are in the form of *.<cspId>.melicertes.eu

2.1 Services that need to be reachable over the Internet

The following ports need to be accessible from the Internet to give access to several services, <cspID> needs to be replaced by the assigned identifier for your CSP instance (for example: cert-eu):

Usage	local hostname	local port	protocol
Integration Layer	integration.<cspID>.prod.melicertes.eu	5443/tcp	HTTPS
OwnCloud	files.<cspID>.prod.melicertes.eu	6443/tcp	HTTPS
MISP Server Sync	misp-ui.<cspid>.prod.melicertes.eu	6443/tcp	HTTPS
Jitsi VideoConferencing Bridge	teleconf.<cspID>.prod.melicertes.eu	6443/tcp	HTTPS

[4] Depending on the specific use cases

Jitsi VideoConferencing Bridge	vc.<cspID>.prod.melicertes.eu	6443/tcp	HTTPS
Jitsi VideoConferencing Bridge – Media TCP	vc.<cspID>.prod.melicertes.eu	4443/tcp	SSL
Jitsi VideoConferencing Bridge – Media UDP	vc.<cspID>.prod.melicertes.eu	UDP 10000	

Important Notes:

While Integration layer only needs to be accessible by the rest of the CSP instances (port 5443), video conferencing (Jitsi) and file sharing (OwnCloud) need to be accessible for all collaboration partners (ports 6443, 4443, 10000 UDP),

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

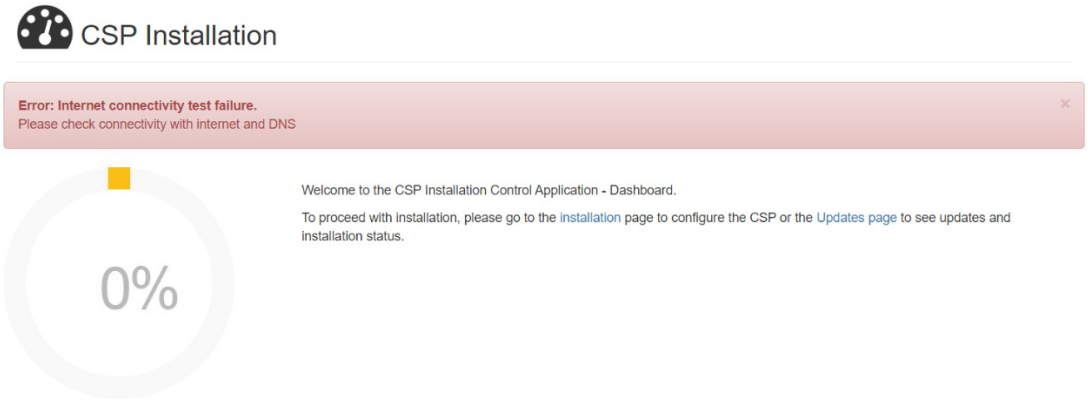
2.2 Services that need to be reached over the Internet from your Instance

The following hostnames and ports need to be accessible over the Internet for outgoing connections. <teams> needs to be replaced by each of the assigned identifier of the other CSP instance. An alternative is to allow all outgoing connections based on the remote port only, if this is allowed by local policies.

Usage	remote hostname	remote port	protocol
Integration Layer	integration.<teams>.prod.melicertes.eu	5443/tcp	HTTPS
Software Repository	central.prod.melicertes.eu	80/tcp	HTTP
Alpine Linux Updates[5]	dl-4.alpinelinux.org	80/tcp (default) **443**/tcp *(recommended)*	HTTP **HTTPS**
MeliCERTes Certificate Revocation List	https://pki.dfn-cert.de/melicertes-ca/pub/crl/cacrl.crl	443/tcp	HTTPS

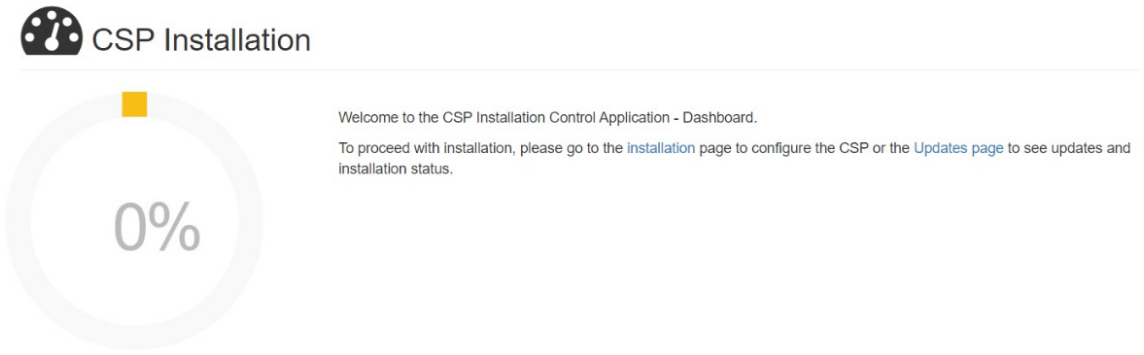
Currently the CSP installer determines Internet connectivity by checking if "central.prod.melicertes.eu" is reachable over port 80 and port 5443, by trying to make new connections every 5 minutes. Heartbeats are sent to the "central.prod.melicertes.eu" CSP every 10 minutes.

If the connectivity check fails, the CSP instance will not attempt any communication with the Central CSP: neither to send heartbeats nor to check for module updates on the MeliCERTes software repository.



So when using the installer, and connectivity checks are successful you should not see any Error:

[5] **Important Note**: The default for Alpine Linux Updates is to use ***HTTP://dl-4.alpinelinux.org*** (80/tcp). It is more secure though to switch to HTTPS (443/tcp), this is easy to accomplish by replacing each occurrence of http to https in the ***/etc/apk/repositories*** file.



The log files showing a successful network check should look like:

```
Attempting to connect to config.central.prod.melicertes.eu:5443
Connected to config.central.prod.melicertes.eu:5443
Attempting to connect to config.central.prod.melicertes.eu:80
Connected to config.central.prod.melicertes.eu:80
Internet connectivity test has completed, connection is OK
```

All lines above do have a prefix like (one string, two lines for readability) followed by one of the lines above:

```
2019-02-11 12:07:54.679  INFO 8813 --- [pool-27-thread-2]
c.i.c.c.c.s.InternetAvailabilityChecker  :
```

To check on the command line whether you can connect to the software repository of the Central node you can use "curl" (one line as one command):

```
Curl       --connect-timeout 20 -s --head \
           http://config.central.prod.melicertes.eu/repo-loads/vm/upd/
```

This will result in a response of the server if reached:

```
HTTP/1.1 200 OK
Date: ...
```

To check whether other MeliCERTes instances are reachable over port 5443/tcp (which is a requirement of the Integration Layer), you can use the console (SSH shell), by running the following command:

```
$  nc -vv csirt-xyz.prod.melicertes.eu 5443
csirt-xyz.prod.melicertes.eu (1.2.3.4:5443) open
```

This indicates that on the other IP something is listening, it is not determinable with this approach if it is really the Integration Layer accepting the TCP connection, but at least your firewall is not blocking and also that something is blocking on the remote side is unlikely given the above output. If there are issues and blocks identified by you, please inform **trust-central@melicertes.eu**.

2.3 Services that need to be reached inside your local network

The following services need to be accessible from within your organization over HTTPS (port 443/tcp):

Usage / Application	Hostname / URL	port	protocol
Trust Circles	https://tc.<cspId>.prod.melicertes.eu	443/tcp	HTTPS
OpenAM Admin.	https://auth.<cspId>.prod.melicertes.eu/openam	443/tcp	HTTPS
Search (Kibana)	https://search.<cspId>.prod.melicertes.eu	443/tcp	HTTPS
Logs (Kibana)	https://logs.<cspId>.prod.melicertes.eu	443/tcp	HTTPS
Sharing Policies	https://integration-ui.<cspId>.prod.melicertes.eu	443/tcp	HTTPS

Anonymization	https://anon-ui.<cspId>.prod.melicertes.eu	443/tcp	HTTPS
Request Tracker (RT)	https://rt.<cspId>.prod.melicertes.eu/RTIR	443/tcp	HTTPS
MISP	https://misp-ui.<cspId>.prod.melicertes.eu	443/tcp	HTTPS
Jitsi VideoConferencing Bridge Admin.	https://teleconf-ui.<cspId>.prod.melicertes.eu	443/tcp	HTTPS
InteMQ Manager	https://imq.<cspId>.prod.melicertes.eu	443/tcp	HTTPS
Viper Manager	https://viper-ui.<cspId>.prod.melicertes.eu	443/tcp	HTTPS

Note: You can bookmark the above links after replacing the correct <cspId> and changing "prod" from the URL depending on your actual environment [stage, playground, preprod, prod].

2.4 Further access for your Admins

An SSH server is configured on the CSP instance and it is required to work on the console level of your instance and therefore should be accessible only from within your organization:

Usage / Application	Hostname / URL	port	protocol
Access to console	<cspId>.prod.melicertes.eu	22/tcp	SSH

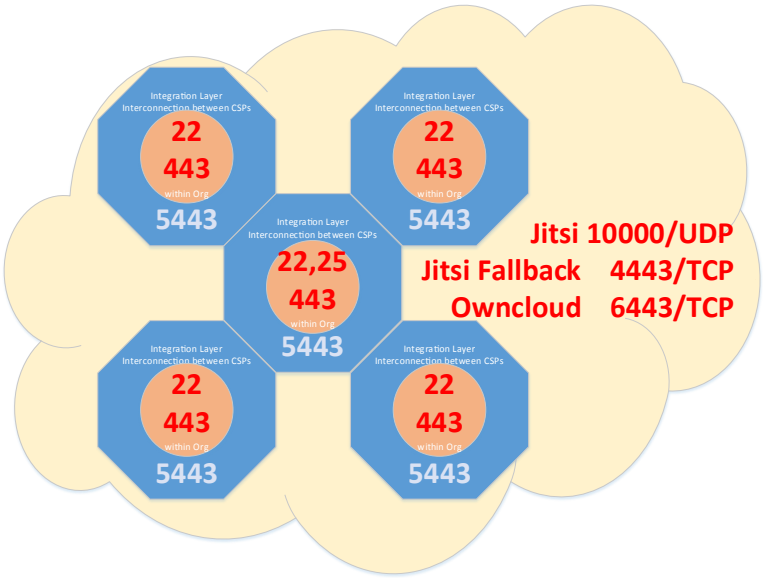
Important Note: Organisations might choose to use so called jump hosts as well as SSH public keys to provide additional security.

Via the SSH access (shown above) admins shall get access to another web server running, which ports are only accessible from that very host. This server is required to provide access to the software management interface

Usage / Application	Hostname / URL	port	protocol
access to software management	via SSH to <cspID>.prod.melicertes.eu:22 Port on client system depends on tunnel config	18080/tcp	HTTP

2.5 Simplified Firewall view

VMs should have internet connectivity to alpine repository servers to perform OS updates, DNS and NTP server. In the figure below we can see a simplified view of firewall ports used with associated services.



The Idea is that all participating CSIRT teams have to allow connections:
From and to the **whole internet** on ports:

- 10000 /UDP Jitsi VoIP and Video Conferencing
- 4443 /TCP Jitsi fallback if UDP fails (suboptimal due to TCP retransmissions, etc)
- 6443 /TCP Owncloud filesharing

All CSIRTs participating in the MeliCERTes federation (List distributed by Trust Circle Admins), on port:

- 5443 /TCP Integration Layer, to/from all participating CSIRTs and Central CSP
- 80 /TCP To Central CSP to download updates

Local administrators should have access to their own service interfaces HTTPS, on port:

- 443 /TCP accessible only from within your organization

MeliCERTes VM admins, on port:

- 22 /TCP SSH

VM outgoing connections: **SMTP** 587/TCP or 465/tcp or 25/TCP, **DNS** 53/UDP, **NTP** 123/TCP

2.6 Other Services (NTP, DNS, SMTP)

2.6.1 Time Synchronization (NTP)

The Alpine Linux is using a time synchronization package called “chrony”. This package is using time servers on the Internet by default, but own time servers can also be supported. It is in any case required to allow the appropriate connections / packets through the firewall which is protecting the CSP instance.

To further customize chrony, you could add these options in `/etc/chrony/chronyd.conf`

```
# you can comment out and add your own NTP servers.
server 0.europe.pool.ntp.org
server 1.europe.pool.ntp.org
server 2.europe.pool.ntp.org

# Required minimum number of sources that need to be considered as
# in the source selection algorithm before the local clock is updated.
minsources 2

# The initstepslew directive only works with NTP sources.
# The 10 indicates that if the system’s error is found to be < 10 seconds
# a slew will be used to correct it;
# if the error is > 10 seconds, a step will be used.
initstepslew 10 pool 0.pool.ntp.org
```

```
# This would step the system clock if the adjustment is larger than
# 0.1 seconds, but only in the first three clock updates.
# Force system clock correction at boot time.
makestep 0.1 3

driftfile /var/lib/chrony/chrony.drift
rtcsync

# Stop chrony default behaviour that listens on UDP port 323 for commands
cmdport 0

# Optionally store symmetric authentication keys.
keyfile /etc/chrony/chrony.keys
```

Important Note 4: "chrony" could also be replaced by "openntpd", however it is important to **avoid** two different packages trying to do the same "job".

Important Note 5: While it is possible to connect to time servers on the Internet, it is recommended to utilize the internal time servers (if any is available). MeliCERTes does not provide a reliable time server.

2.6.2 Domain Name Services (DNS)

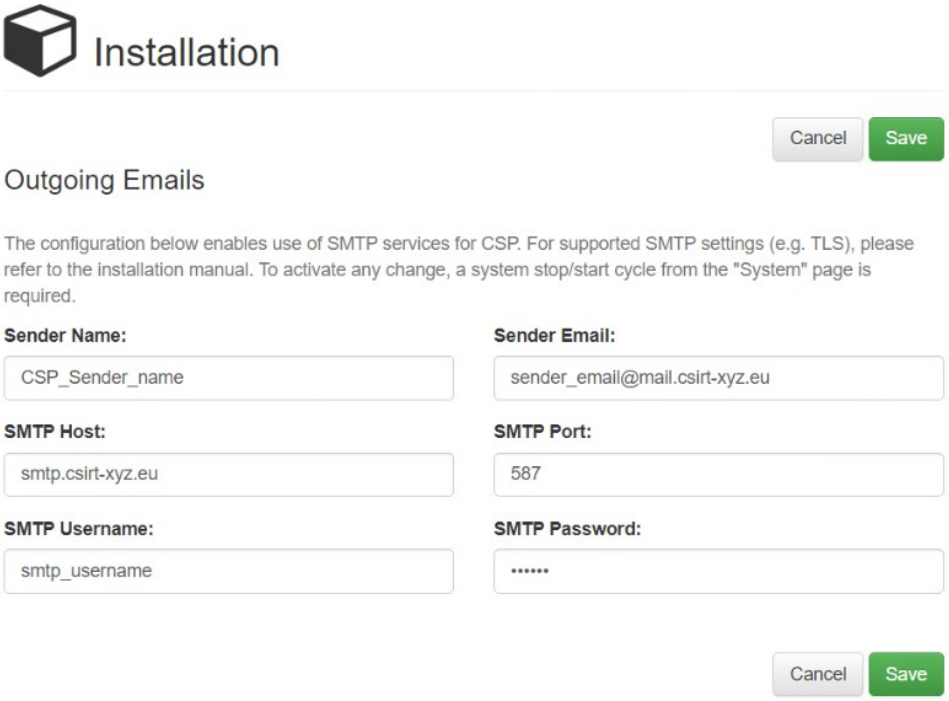
The MeliCERTes instances are depending on DNS lookups as most systems on the Internet. It is expected that the Alpine Linux is configured to use an internal DNS resolver. It is in any case required to allow the appropriate connections / packets through the firewall which is protecting the CSP instance.

2.6.3 SMTP mail relay

The CSP instance needs to be able to send e-mails, primarily for invites when scheduling video conferences. Not providing the SMTP mail relay will make the bridge lose the ability to send out invitations or cancellations to scheduled conferences and along with the email, all contained information within: assigned username, password, and bridge conference-room details.

The configuration of the SMTP mail relay is done during the initial setup, but administrators can change the details by connecting to the CSP instance by SSH, opening a tunnel and visiting the CSP installer URL http://127.0.0.1:18080/install-smtp.html. In order to be able to send email one obviously has to allow the appropriate connections/ packets through the firewall protecting the CSP instance.

The default CSP settings requires you to provide the SMTP server hostname along with a username and password that is used for SMTP authentication, to validate users who try to send emails through that server.



Note that the "Port" field should be one that supports SMTP AUTH, by default is port 587/tcp (Secure SMTP). The "Host" field needs to contain the hostname of the SMTP mail relay.

Important Note 6: While it is possible to connect to SMTP mail relays on the Internet, it is recommended to utilize your organisations' regular internal SMTP services. MeliCERTes does not provide an open SMTP mail relay for use by the CSP instances.

Some reports indicated an error like the following (splint in two lines for readability below):

```
DEBUG SMTP: could not connect to host "smtp.yourdomain.eu",
port: 587, response: -1
```

The above error, if the required outgoing connection to the SMTP server is not blocked (587/tcp) by any firewall, is probably caused by the cryptographic protocol offered or required by the SMTP server.

To change the default settings from TLS to SSL please follow this process:

1. navigate to the module directory (you should have only one directory starting with "vcb"):

   ```
   $ cd /opt/csp/modules/vcb*
   ```

2. modify and save the file 'docker-compose.yml' at the line starting with "command". (Note that this file is indented with SPACES and not TABS.) Please edit carefully the ONE line to read as below, it is just broken into multiple lines for readability:

   ```
   command: sh -c "sleep 10 && java -Xmx512m
   -Dspring.profiles.active=docker
   -Dspring.mail.properties.mail.smtp.ssl.enable=true
   -Dspring.mail.properties.mail.smtp.starttls.enable=false
   -jar server.jar"
   ```

   If you would like to receive debug output, please add two more "-D" options before "-jar" or if it already present change the log level as you see fit:

   ```
   -Dspring.mail.properties.mail.debug=true
   -Dlogging.level.com=DEBUG
   ```

3. perform a docker container re-creation:

   ```
   $ docker-compose up -d vcb-admin
   ```

After this, the next time the teleconf User Interface is used to create a new meeting request the new settings will be used. You should be able to test the new configuration with the following command as user (again one line as a command):

```
$ (echo "Subject: Topic"; echo "From: csp-info@yourdomain.eu";
echo "To: <you@yourdomain.eu>"; echo ""; echo "Message content") |
ssmtp -v you@yourdomain.eu
```

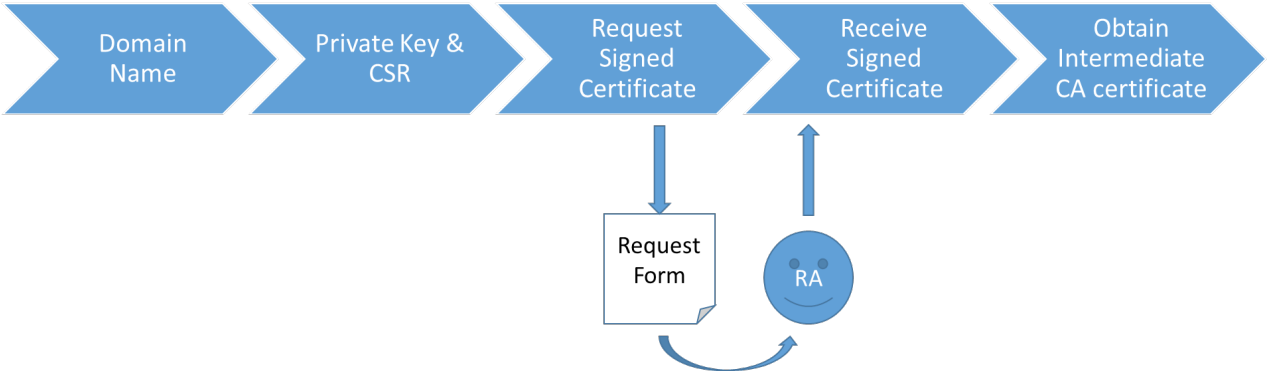
Important Note 7: If you want to send emails using another port use another protocol other than SMTP AUTH, please contact the technical helpdesk (***helpdesk.melicertes@intrasoft-intl.com***) for support and advice.

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 bari[6].test.melicertes.eu.key 4096
```

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

Output will be similar to:

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

```
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.

3.2.2 Create the CSR

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*

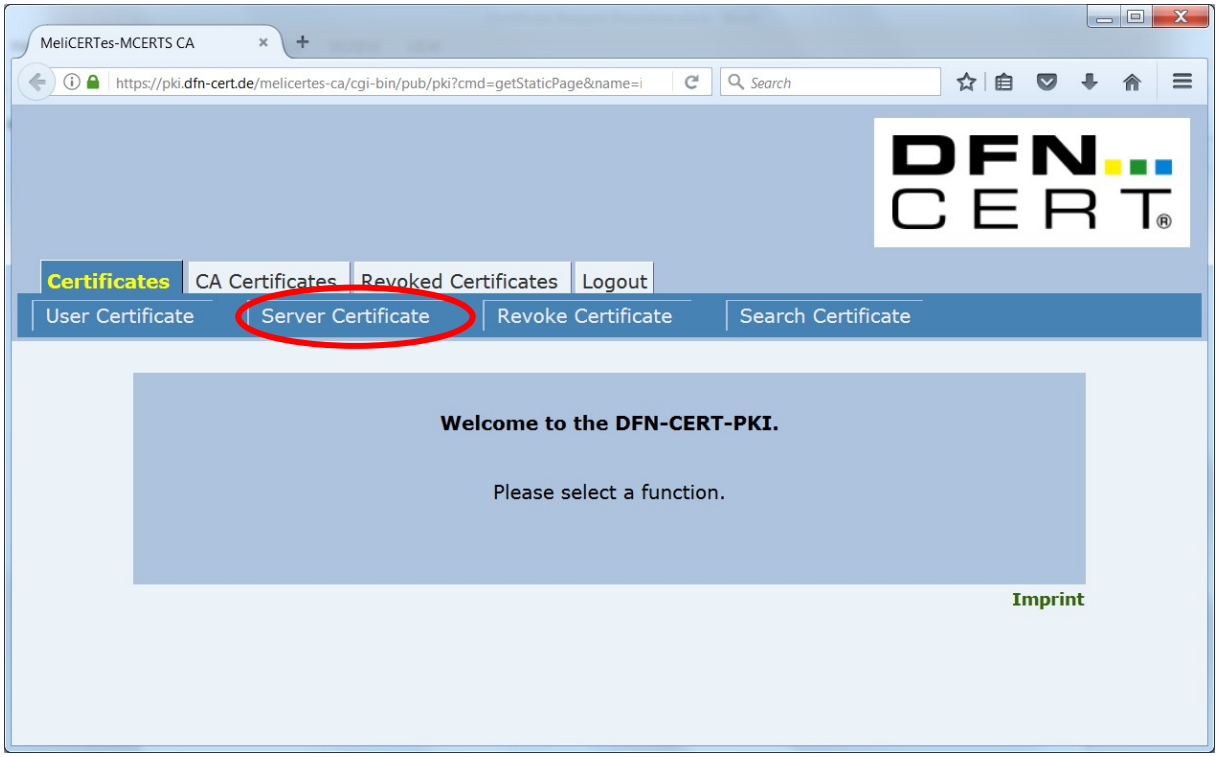
To generate the Certificate Signing Request (CSR), we execute the following command (substitute the value of the 'CN' field for your assigned domain name):

```
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.

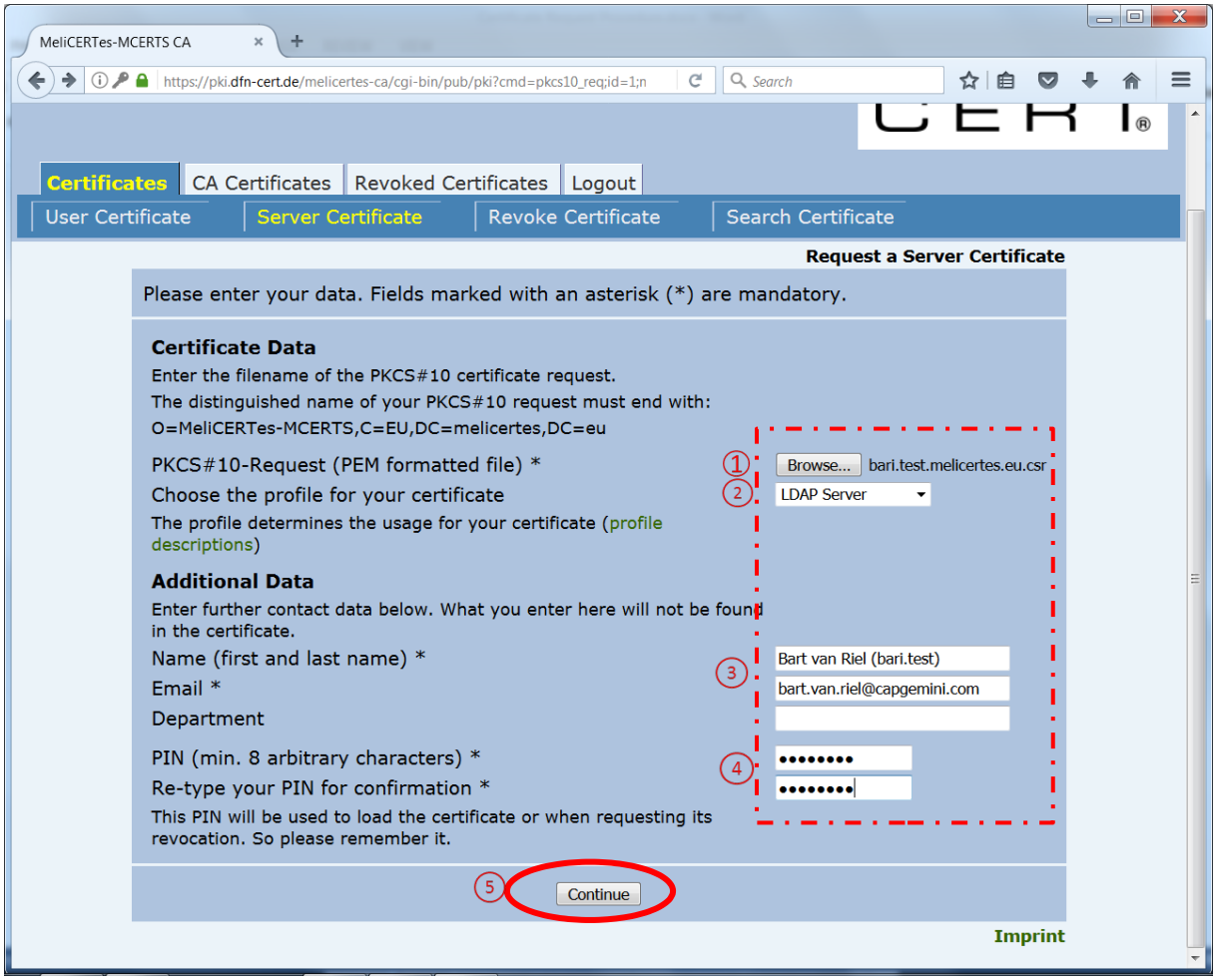
3.3 Submit the CSR to the PKI for signing

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”.

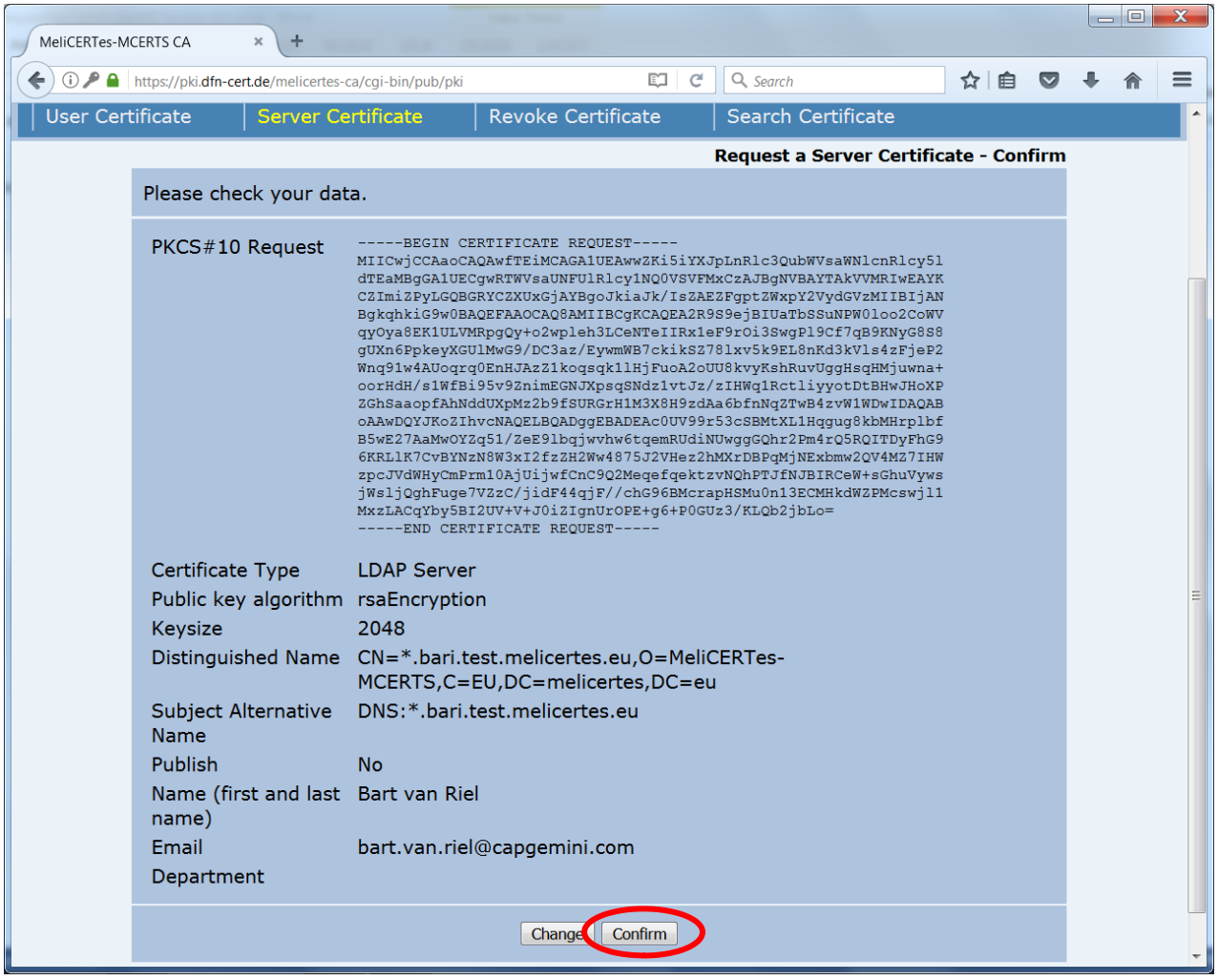
2. Choose “LDAP Server” as the profile (this will ensure you get a certificate which can be used both for mutual service authentication and for server side encryption within your installation later on).

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.

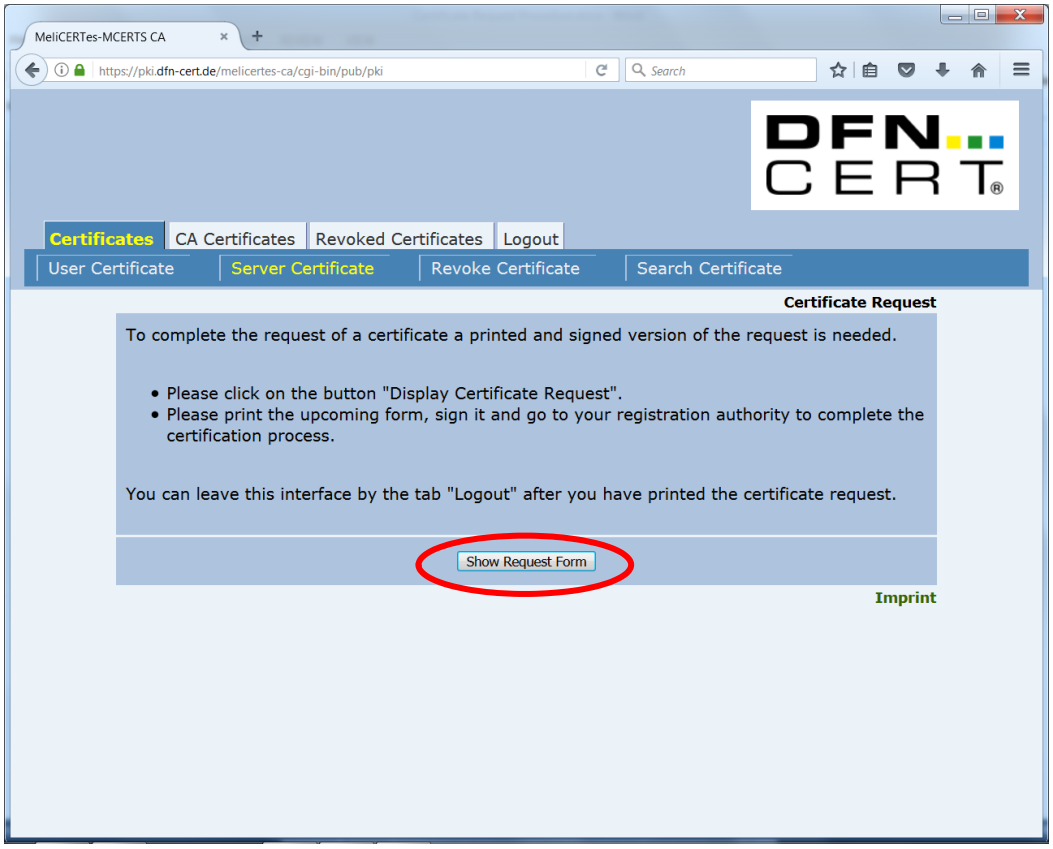


Validate the information on it.

I everything is Ok, click “Confirm”.

If anything is out of order, click “Change” and you will be taken back to the “Request a Server Certificate” Screen.

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 **trust-central@melicertes.eu** as a "Signing Request". As a subject, please enter “**Server Certificate Request - <cspId>**”.

Note: Digitally signing the email message you send with the CSR form is required!

3.4 Receive the signed certificate

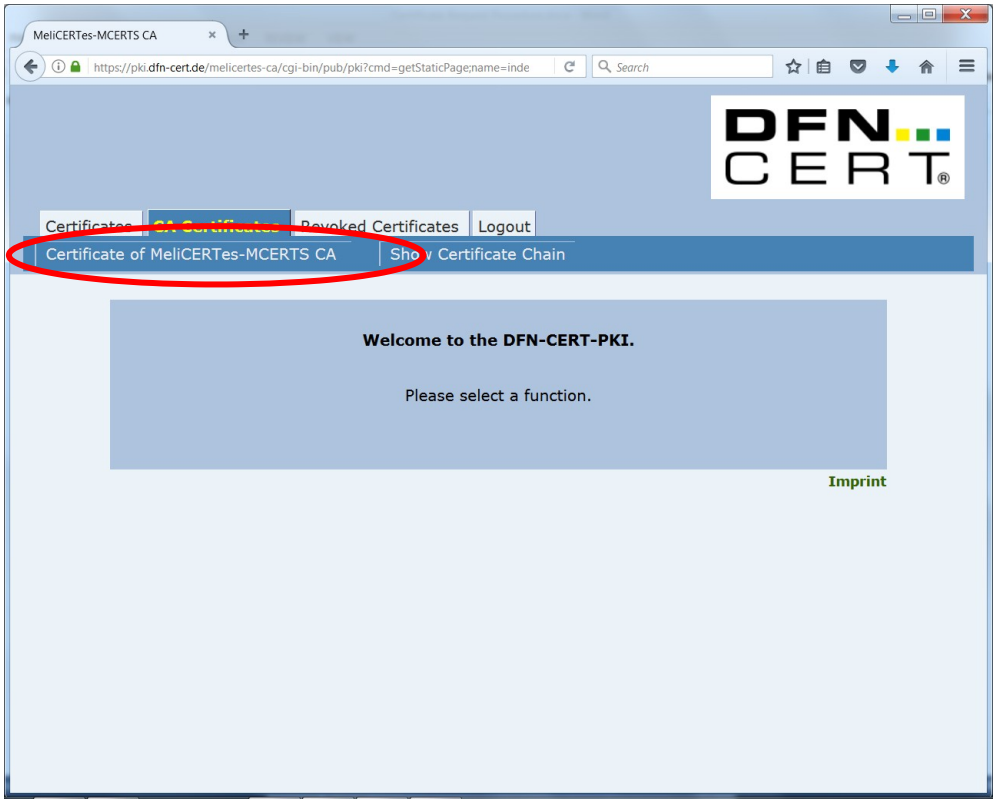
After the certificate request has been approved by the RA, you will receive an email containing the certificate as attachment (in the form of a *.pem file). Store the certificate as desired.

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**”).

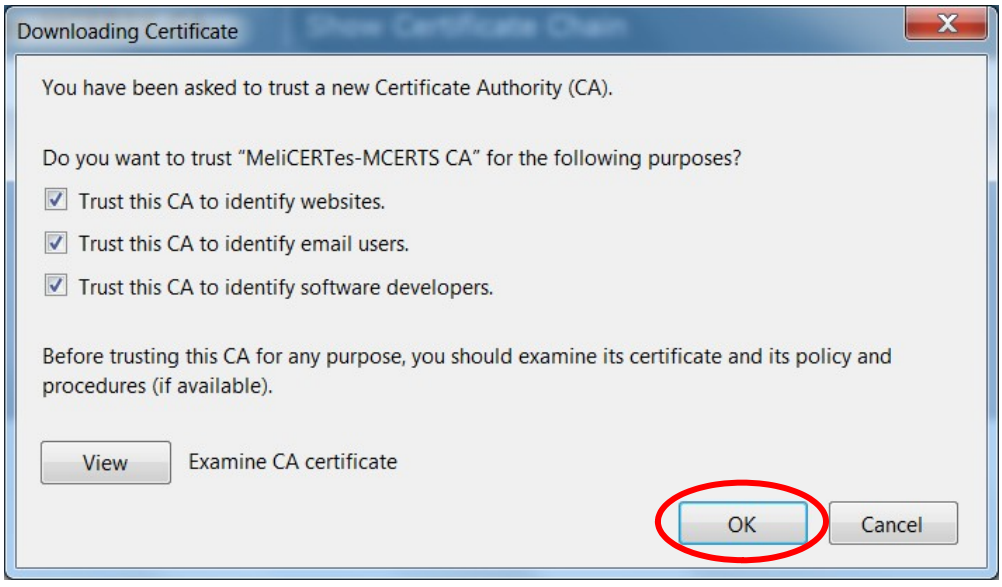
3.5 Download the Intermediate Root CA certificate

Click on the deeplink for “importing the CA certificate” which is in the e-mail which included the certificate. https://pki.dfn-cert.de/melicertes-ca/cgi-bin/pub/pki?id=2 The “CA Certificates” tab of the PKI site is shown.

Click on the tab “CA Certificates” and then choose “Certificate of MeliCERTes-MCERTS 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-MCERTS” entry and select the “MeliCERTes-MCERTS 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

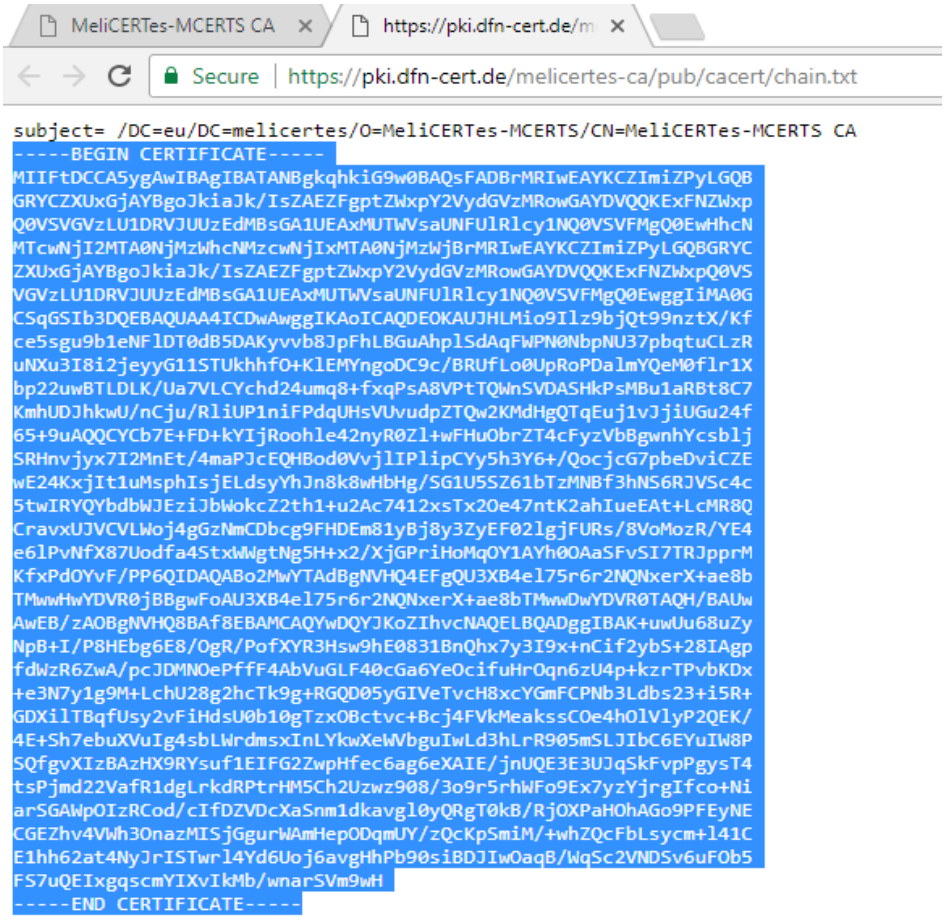
“-----BEGIN CERTIFICATE-----”

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

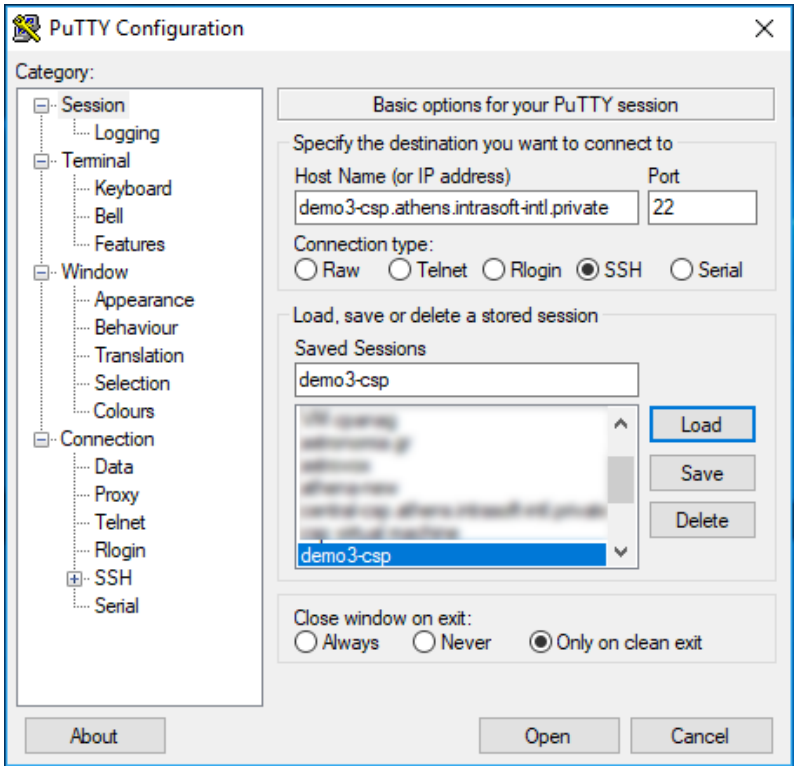
An Open Virtualization Archive (OVA file) has been distributed and contains the original VM for this project. Please note that the distributed OVA is most probably not up to date, after the initial setup and ip configuration you must apply all new Alpine Linux updates. This OVA has settings for memory 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.

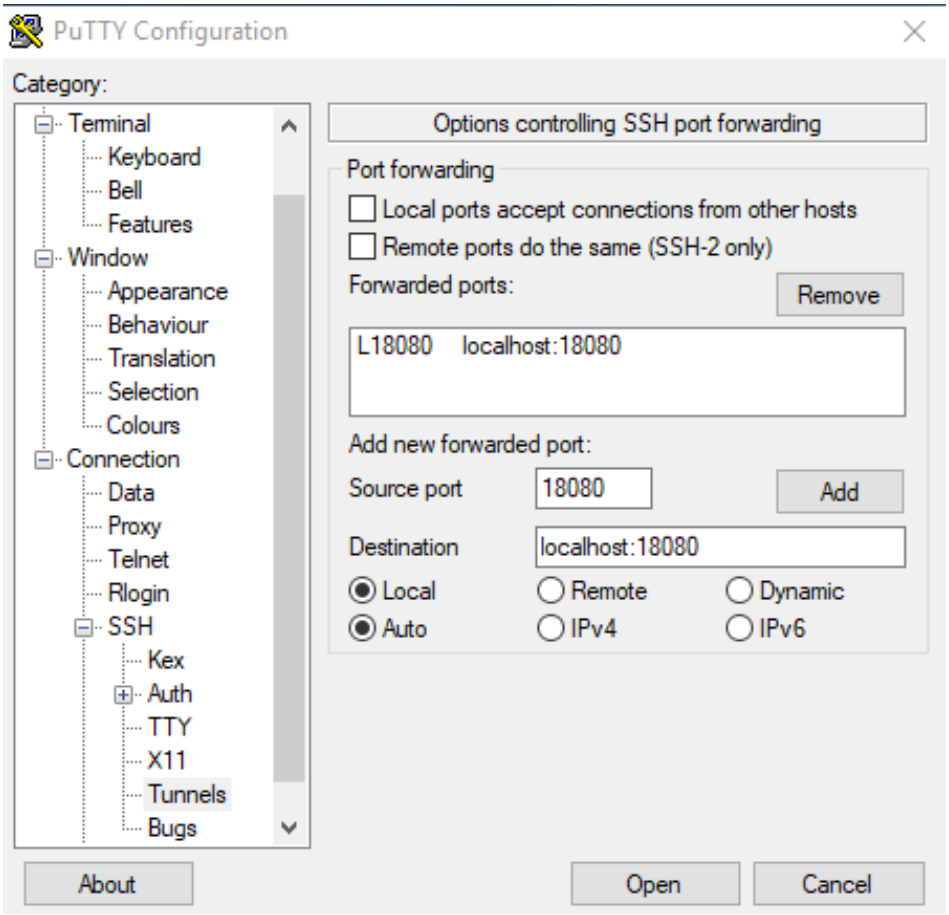
4.2 Connecting to the VM

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.

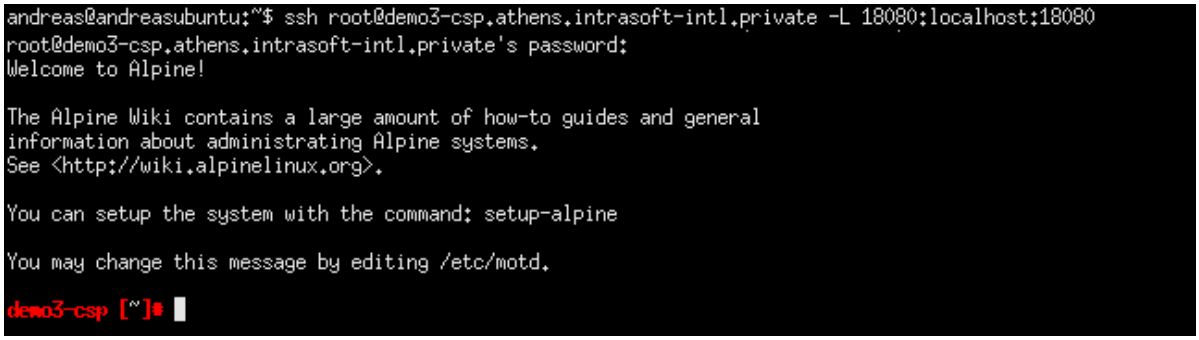


In the case of using a Linux terminal, the SSH connection with the tunnel can be created using the following command format:

```
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.



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.

5 Installation

As mentioned previously, before continuing with the configuration of the CSP installer, we need to connect to the VM using a SSH client.

First we should enable the proper repositories, one could select the repositories that are closest to its location or country. Another way would be to use the `setup-apkrepos` command to look for the fastest repository.

```
debug [~]# cat /etc/apk/repositories
https://dl-4.alpinelinux.org/alpine/latest-stable/main
https://dl-4.alpinelinux.org/alpine/latest-stable/community
https://dl-4.alpinelinux.org/alpine/edge/community
```

Verify that you have enabled the correct repositories. We suggest you use the https protocol and finally run the following commands from console as root:

```
#   apk --no-cache update && apk --no-cache upgrade
```

This will check and update the Alpine Linux repositories and upgrade all components, presuming you have internet connectivity.

```
debug [~]# apk update && apk upgrade
fetch https://dl-4.alpinelinux.org/alpine/latest-stable/main/x86_64/APKINDEX.tar.gz
fetch https://dl-4.alpinelinux.org/alpine/latest-stable/community/x86_64/APKINDEX.tar.gz
fetch https://dl-4.alpinelinux.org/alpine/edge/community/x86_64/APKINDEX.tar.gz
v3.10.2-80-g68e4e4a13a [https://dl-4.alpinelinux.org/alpine/latest-stable/main]
v3.10.2-80-g68e4e4a13a [https://dl-4.alpinelinux.org/alpine/latest-stable/community]
v20190925-101-g159b0cfb0b [https://dl-4.alpinelinux.org/alpine/edge/community]
OK: 15780 distinct packages available
(1/7) Upgrading docker-engine (19.03.2-r0 -> 19.03.2-r1)
(2/7) Upgrading docker-openrc (19.03.2-r0 -> 19.03.2-r1)
(3/7) Upgrading docker-cli (19.03.2-r0 -> 19.03.2-r1)
(4/7) Upgrading docker-bash-completion (19.03.2-r0 -> 19.03.2-r1)
(5/7) Upgrading docker (19.03.2-r0 -> 19.03.2-r1)
(6/7) Upgrading expat (2.2.7-r1 -> 2.2.8-r0)
(7/7) Upgrading docker-vim (19.03.2-r0 -> 19.03.2-r1)
Executing busybox-1.30.1-r2.trigger
Executing glibc-bin-2.28-r0.trigger
OK: 642 MiB in 189 packages
```

Now we can proceed with the rest installation steps.

It would be best to configure sshd to allow authentication using only public keys for SSH connections.

5.1 CSP Installer health verification

To follow the rest of the installation steps discusses 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 succesfull 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 config.central.<cspId>.[preprod.]melicertes.eu:80
- 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
#   Attempting to connect to config.central.demo.melicertes.eu:80
#   Connected to config.central.demo.melicertes.eu:80
#   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 12 - Annex D: Troubleshooting the connection tunnel to the VM, in case you encounter issues in accessing the aforementioned URL.

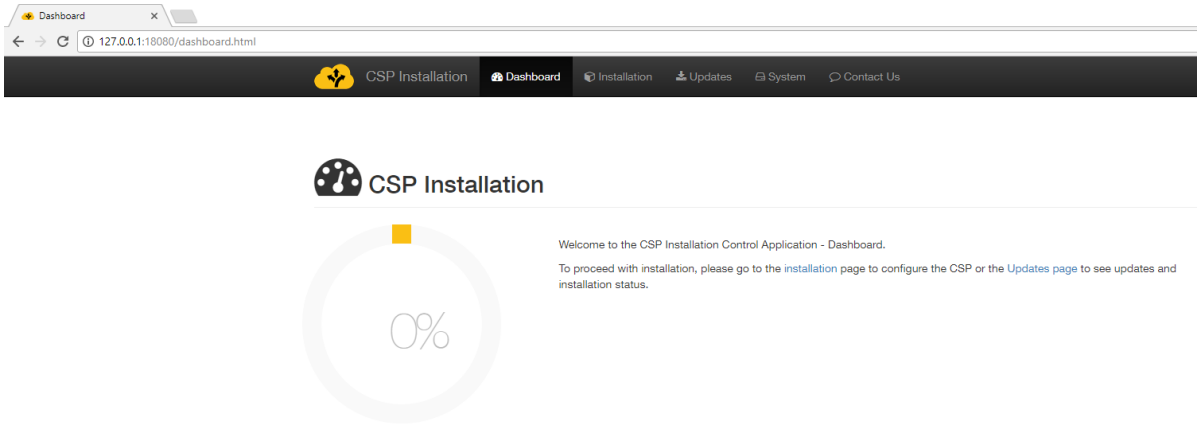
First time installation should display a progress of 0%. The menu bar at the top of the page displays the basic operations of the application which are “Dashboard”, “Installation”, “Updates” and “System”. These options should be selected at the order instructed in this manual. A brief description of 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.

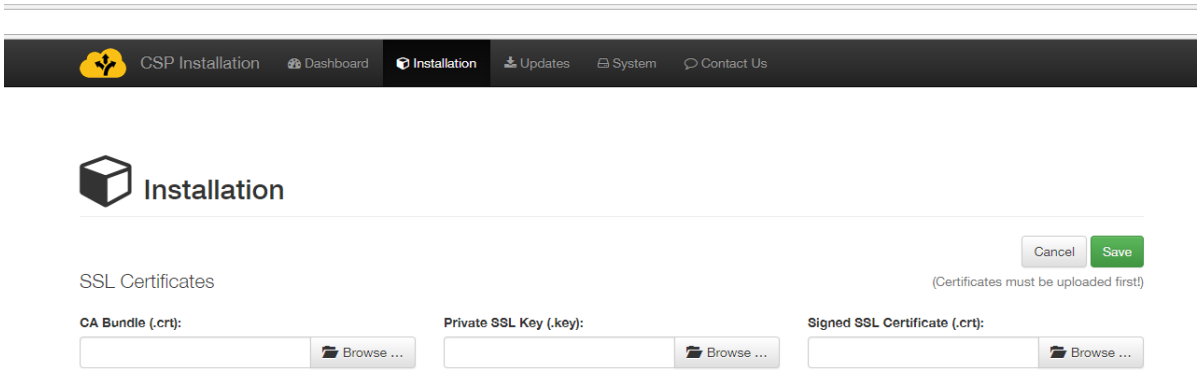
“System”: Starts and stops the system and displays the status of all services.



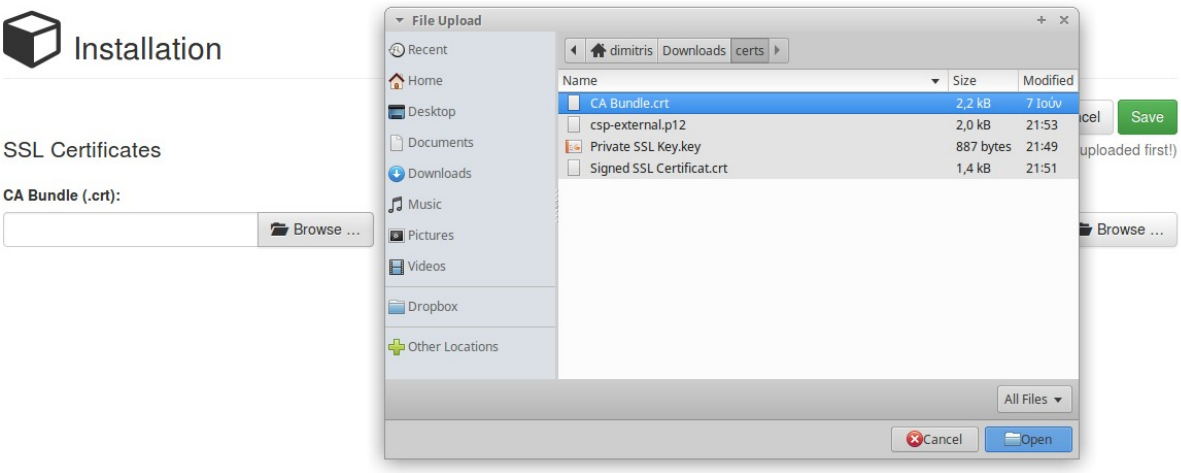
The first time the CSP installation control application is accessed, the user should proceed to the **Installation** page in order to perform initial configuration.

5.2 Installation of certificates

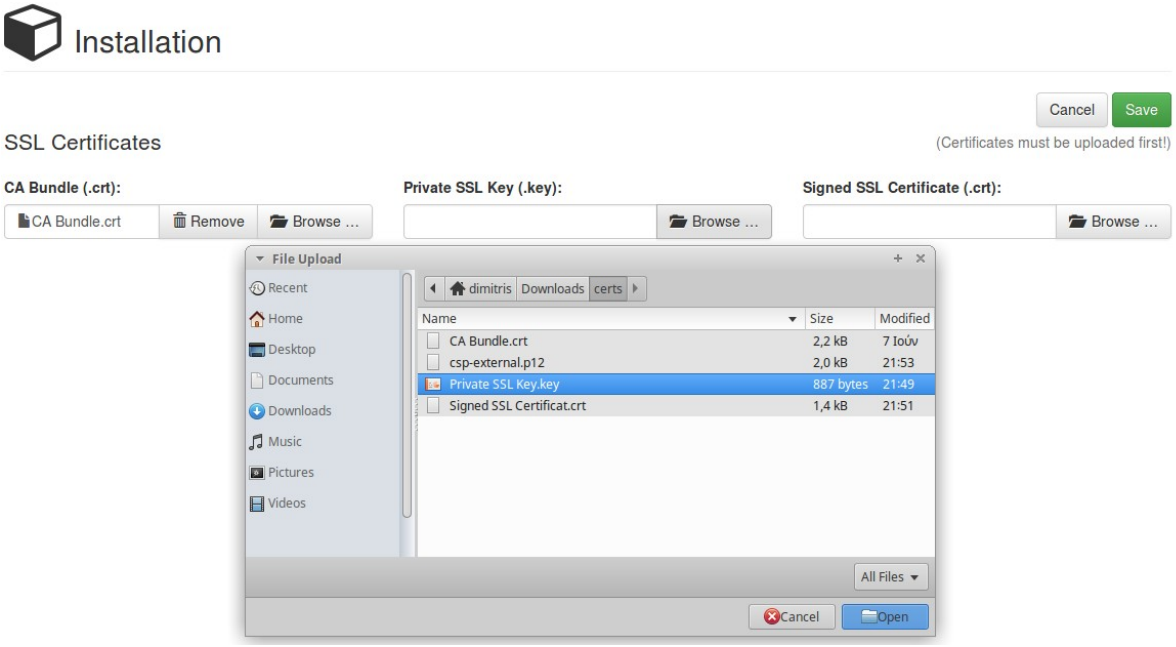
Completing the first installation step requires that the user has saved to his computer all certificate and key files required as mentioned in the previous sections of this manual. The necessary certificates are the CA bundle, the Private SSL Key and the Signed SSL certificate. The file names can be 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.



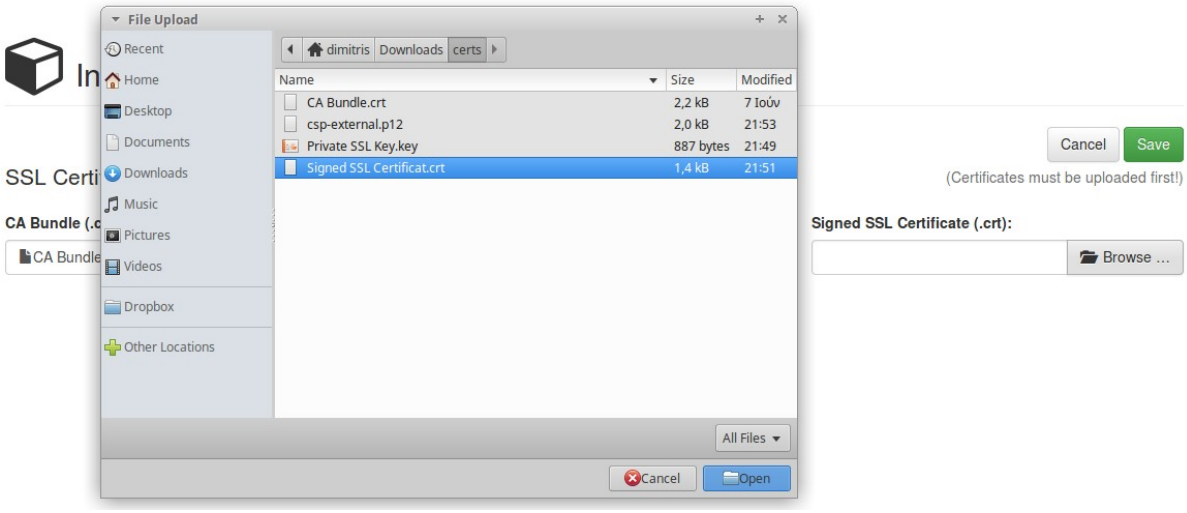
The user should browse and select the files in the order given. First, the user should click the “Browse” button for the CA Bundle certificate and select the “CA Bundle.crt” file. Once selected, the name of the file will appear in the box.



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.

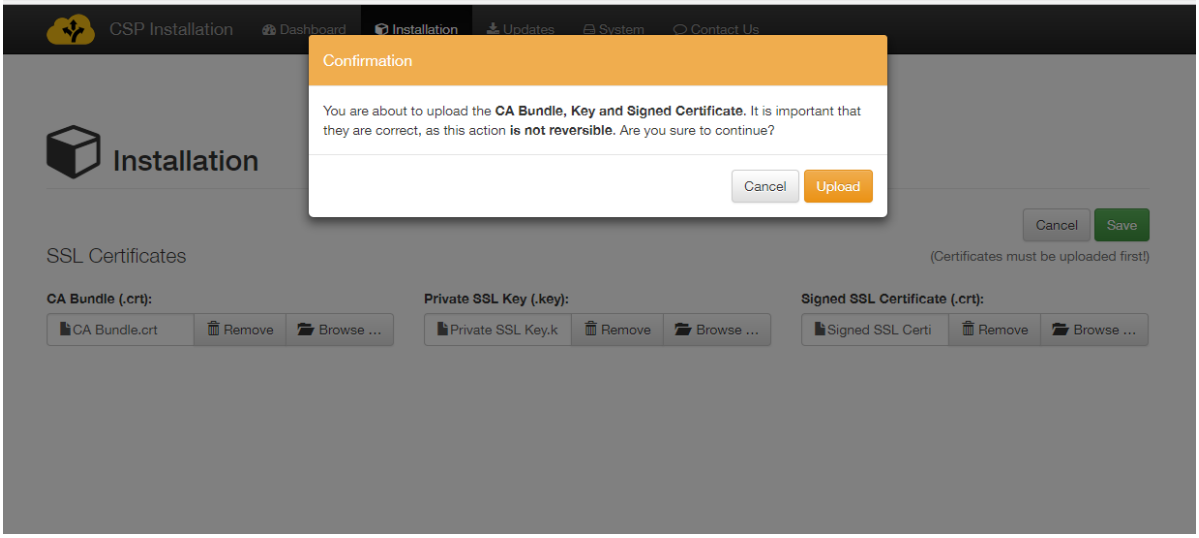


Finally, the user should click the third "Browse" button of the Signed SSL Certificate and select the "Signed SSL Certificate.crt" file. Once selected, the name of the file will also appear in the box.

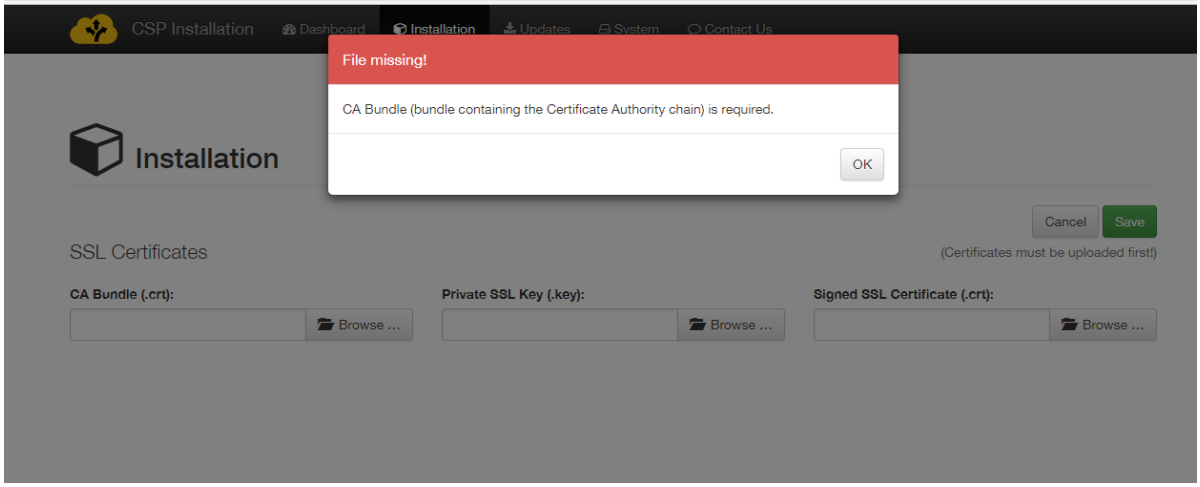


Please note that the installer expects *CA bundle* and *Signed SSL Certificate* to have extension **.crt** and not **.pem**.

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.

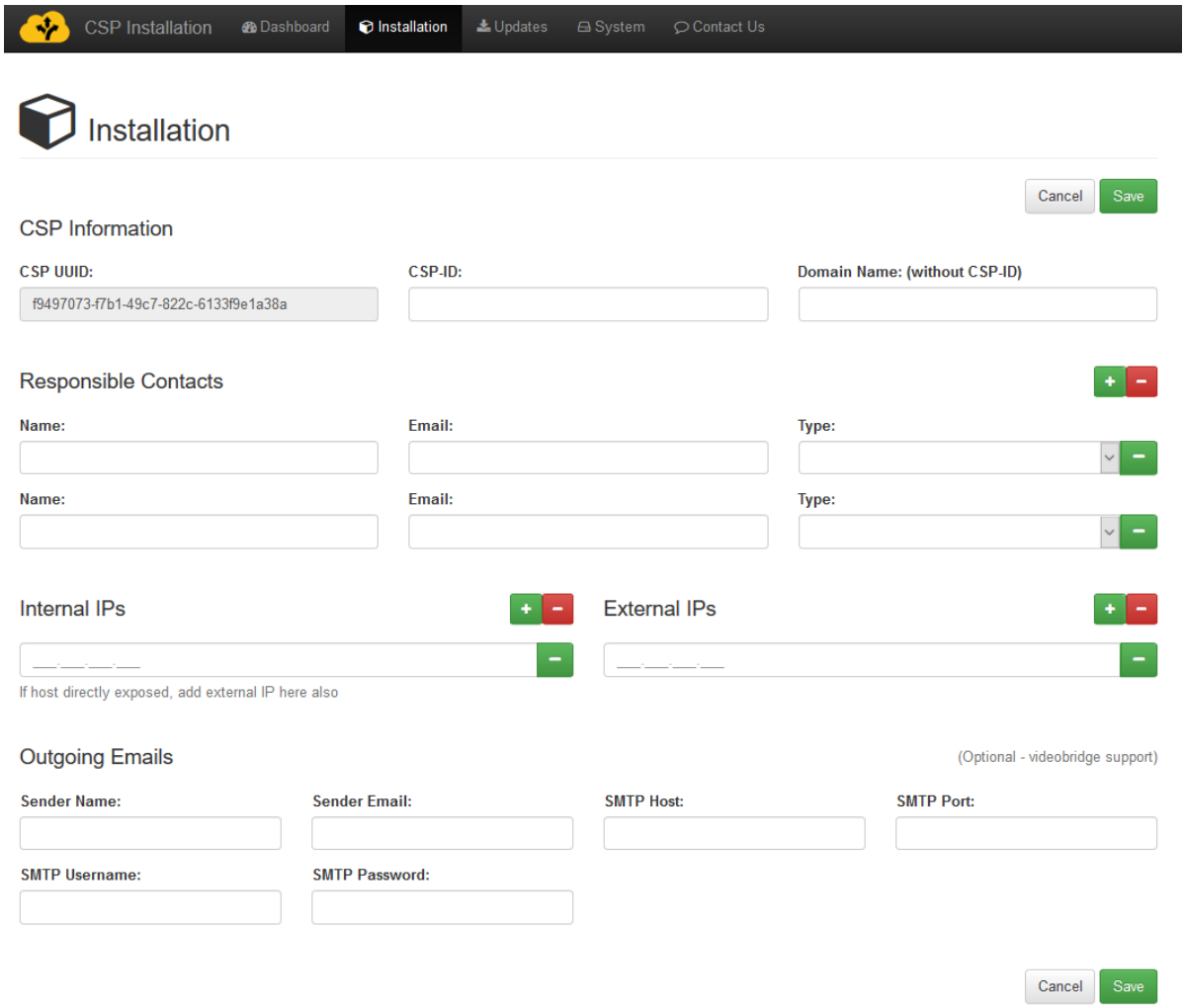


Incomplete submittal of the certificates is not possible. The system will alert the user that certificate files are missing if the Save button is clicked and not all three files have been selected.


CSP Installation
Dashboard
Installation
Updates
System
Contact Us
File missing!
CA Bundle (bundle containing the Certificate Authority chain) is required.
OK
Installation
Cancel
Save
SSL Certificates
(Certificates must be uploaded first!)
CA Bundle (.crt):
Browse ...
Private SSL Key (.key):
Browse ...
Signed SSL Certificate (.crt):
Browse ...

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.



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	Contact

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:

a. 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.
b. 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.
c. Only one internal IP and only one external IP are supported.

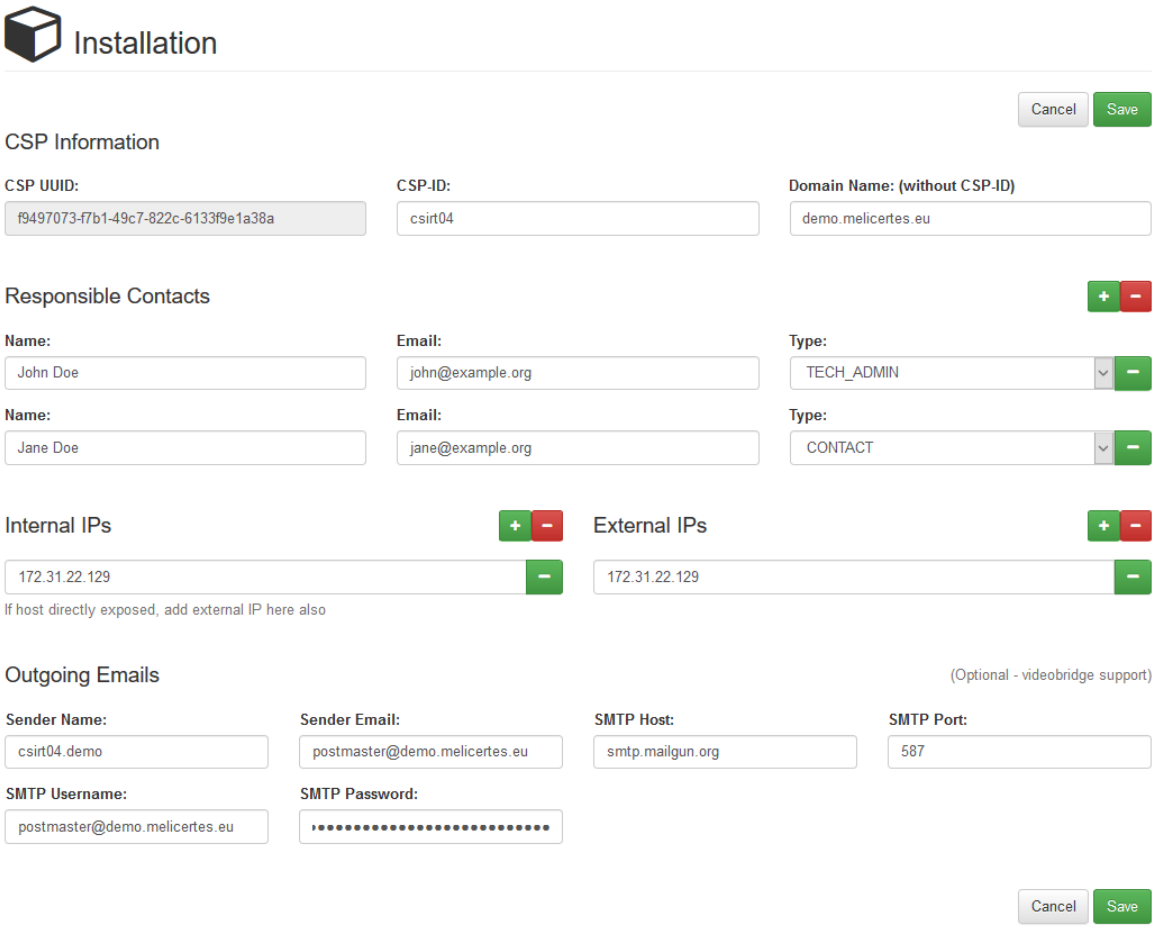
All the above fields are **mandatory**.

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:

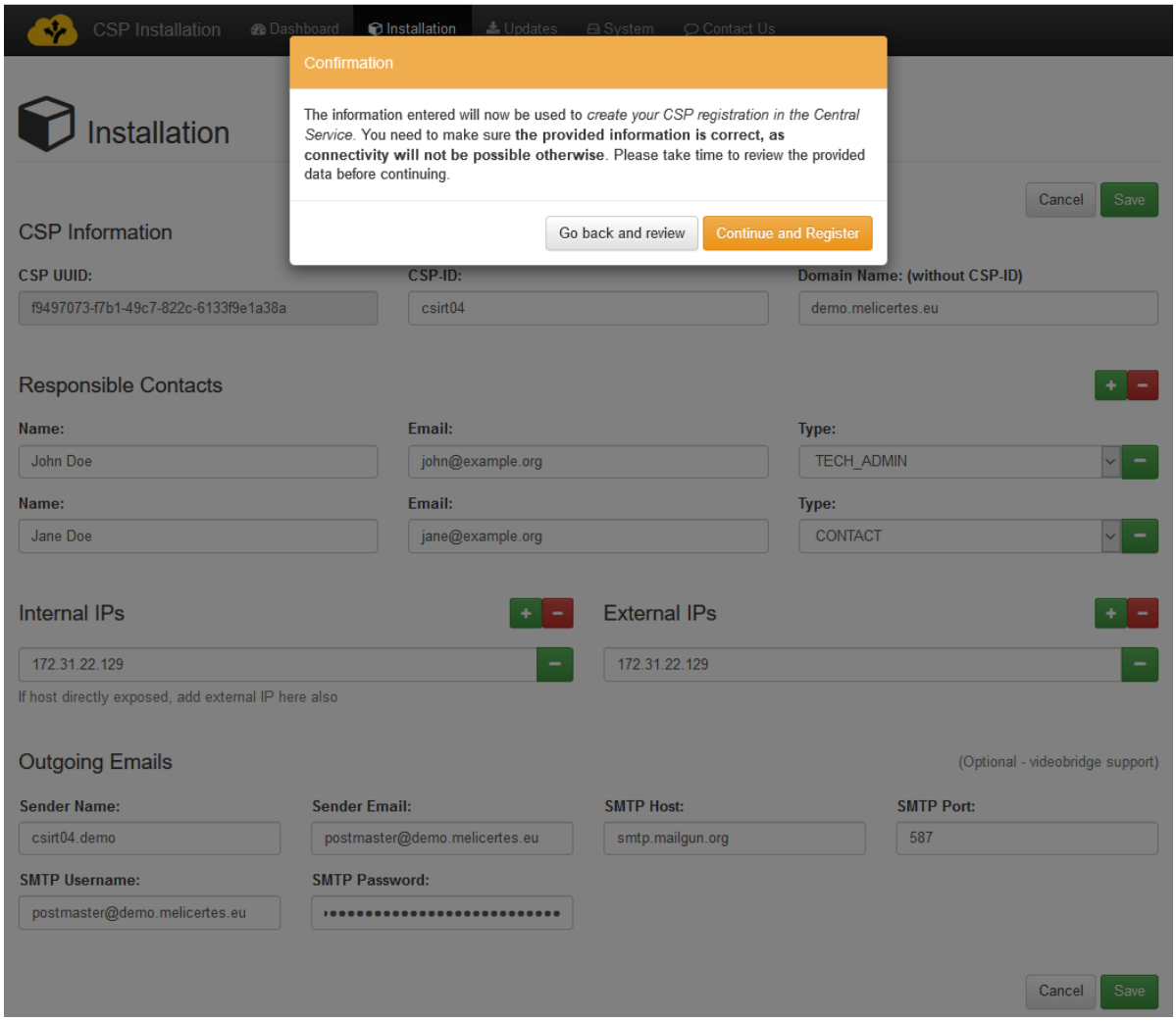
- Sender Name
- Sender Email
- SMTP Host
- SMTP Port
- SMTP Username
- SMTP Password

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.



The form is submitted by clicking the green Save button.



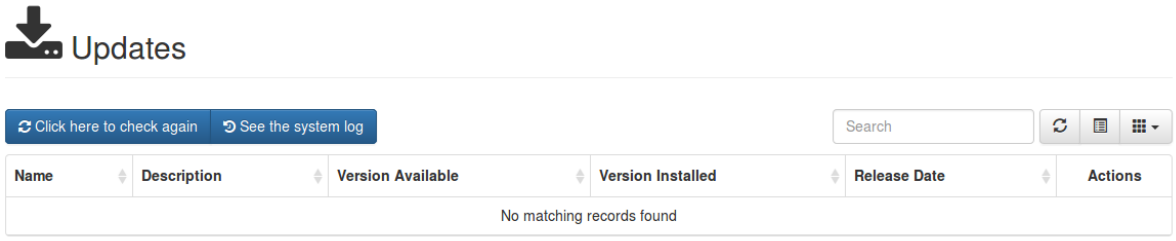
The system prompts for confirmation prior to final submission. It is important that all information entered is correct since connectivity will not be possible if any misspellings exist in the CSP name, domain and IP's. After pressing the "Continue and Register" button, the system will redirect to the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

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

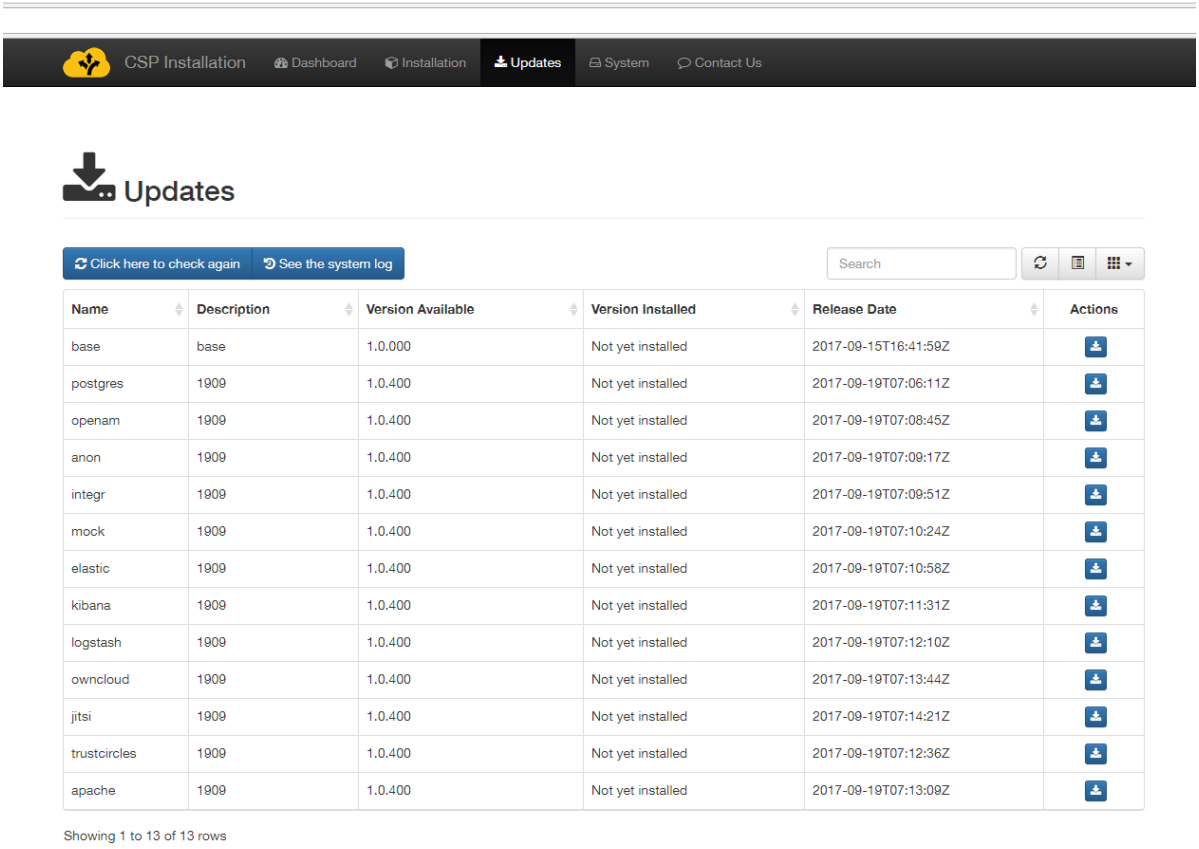
5.4 Download of system updates

In a new installation, a registered CSP is not operational yet. **Specific actions are required on the central CSP side to allow this new CSP to receive new and updated modules to 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 proceed with the installation.

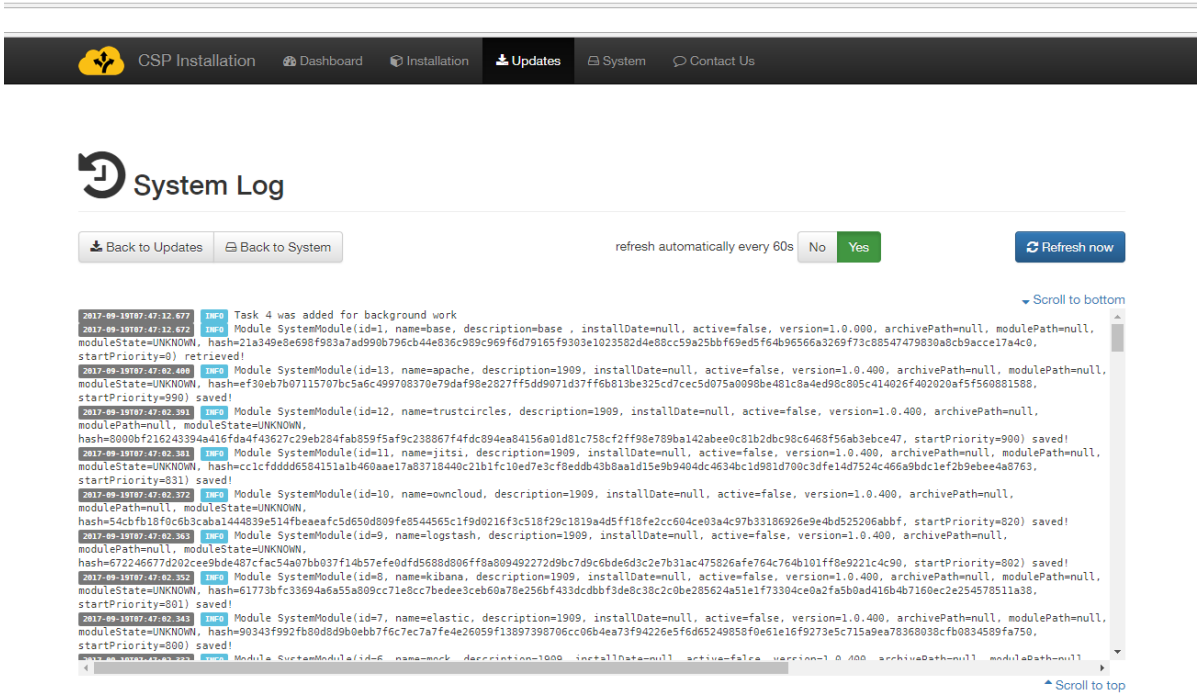
In an existing installation, updates may appear on the "Updates" page as they become available. This page should be checked once a week during a scheduled maintenance window.



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:



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.

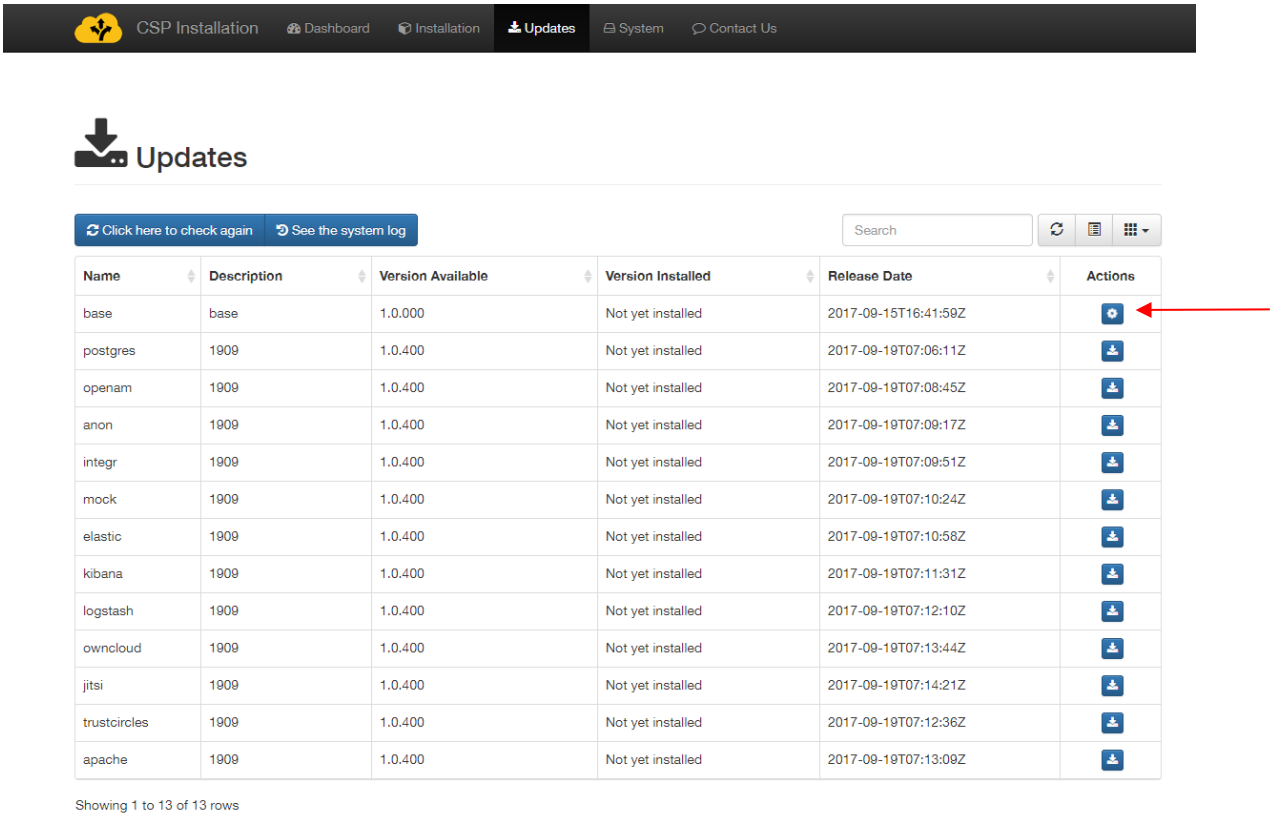


Most operations, including downloading of updates takes place in the background so the user can return to the Updates page by clicking the "Back to Updates" button, and page refresh (for updated log entries) happens every 60 seconds or if the "Refresh now" button Refresh now is pressed.

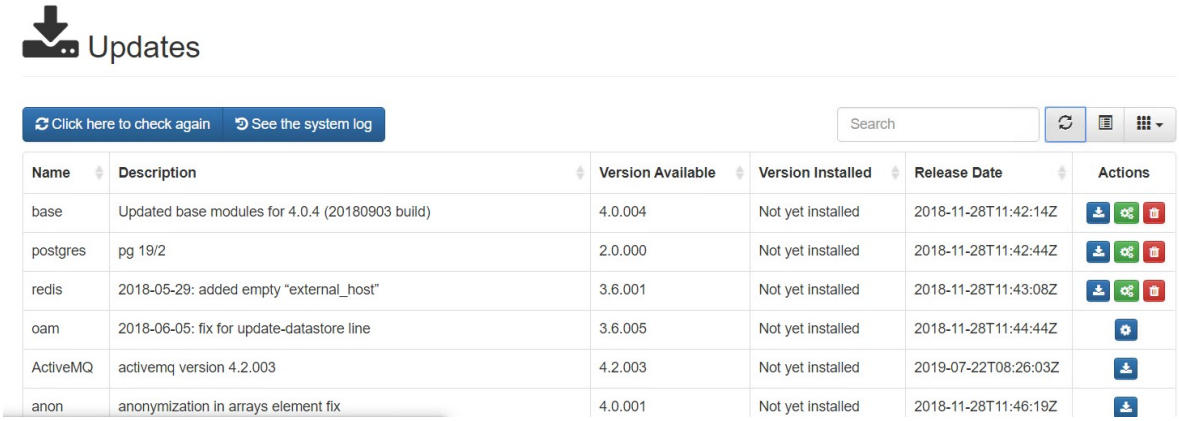
An indicative list of log entry extracts with explanations follows:

- "Task X was added for background work"
  – the system has scheduled an operation to happen in the background.
- Result in BackgroundTaskResult(success=SystemModule(id=12, name=owncloud, description=owncloud version 4.2.001, installDate=null, active=fal;se, version=4.2.001, archivePath=/opt/csp/downloads/649…b507.zip, modulePath=null, moduleState=DOWNLOADED, hash 649…b507, startPriority=820, manifestJsonAsText=null, externalName=null), errorCode=true, moduleName=null)
  – indicates the module owncloud was Downloaded successfully

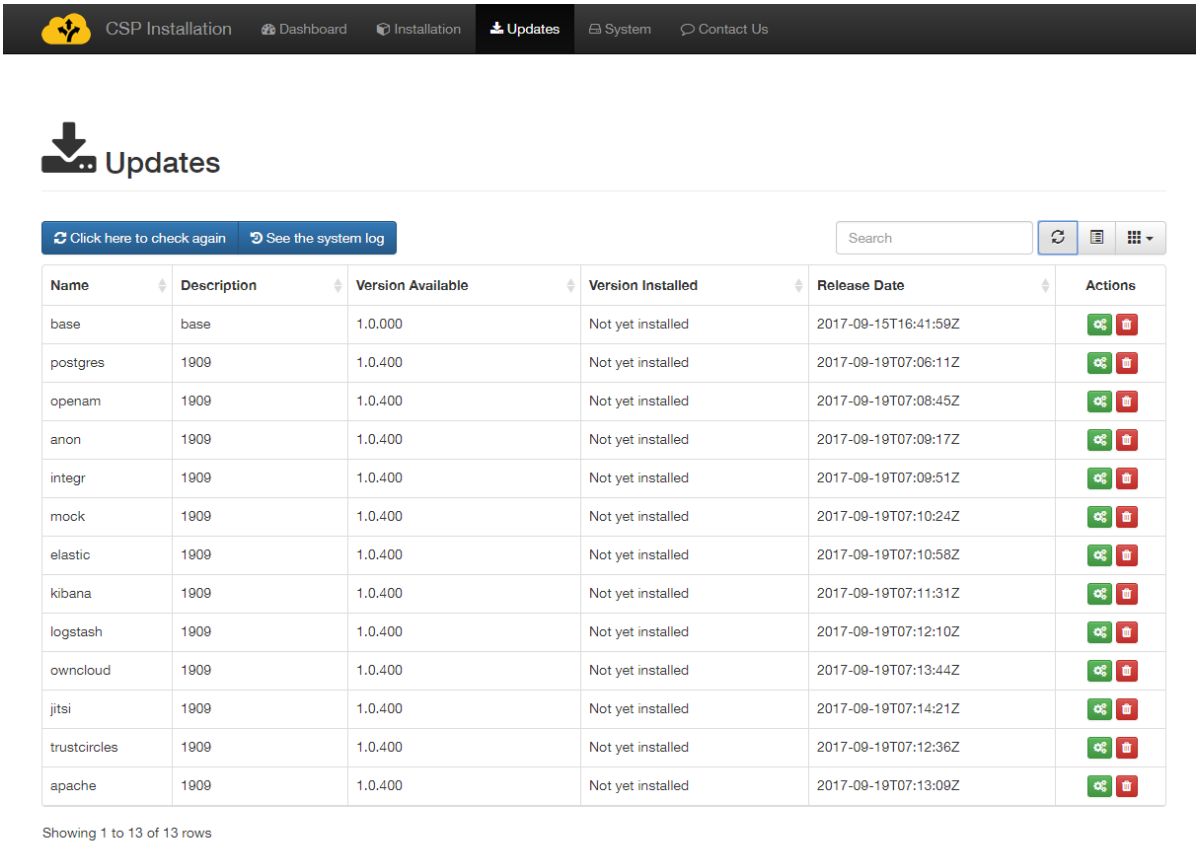
Note that updates that are currently downloading will present an animated gear icon in the “Actions” column.



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.



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



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	

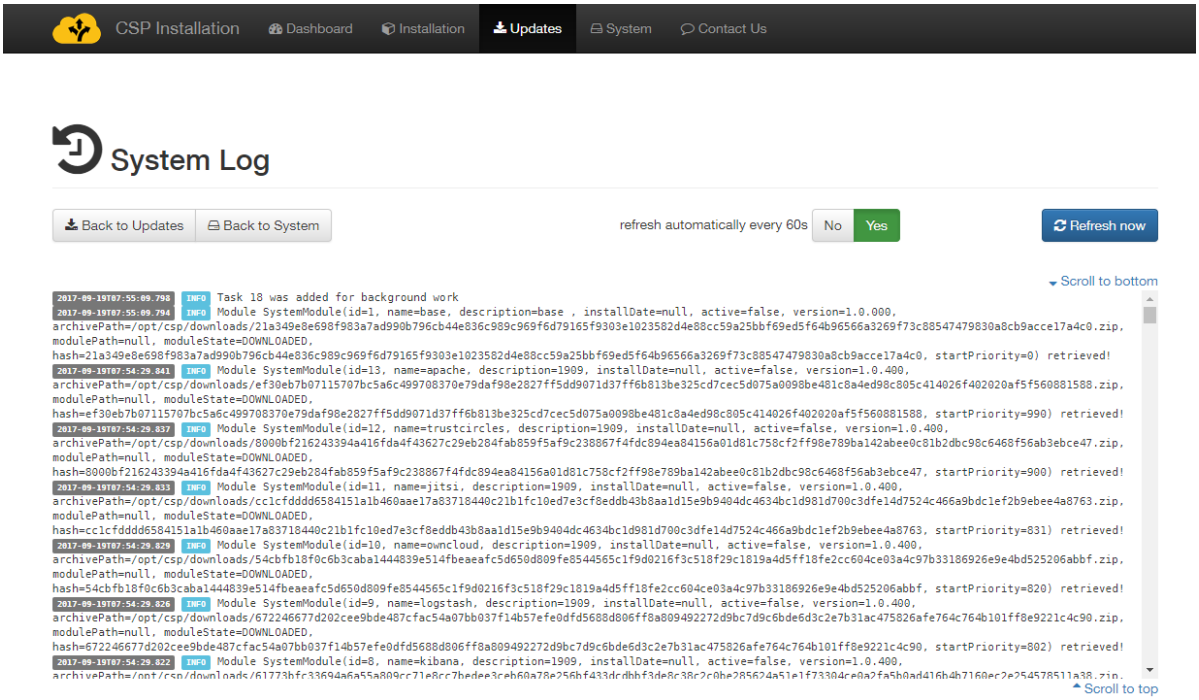
Showing 1 to 13 of 13 rows

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”.



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.
- Completed Task Installation of module xyz/com.intrasoft.csp.conf.clientcspapp.service.BackgroundTaskService$$Lambda$64/1234567@1234aea result is "BackgroundTaskResult(success=true, errorCode=0, moduleName=null)"
  – indicates a successfully executed operation
- "BackgroundTaskResult(success=false, errorCode=<variable>, moduleName=<variable>)"
  – indicates a failed operation. You should collect all logs and submit them to the support team for further investigation[7].

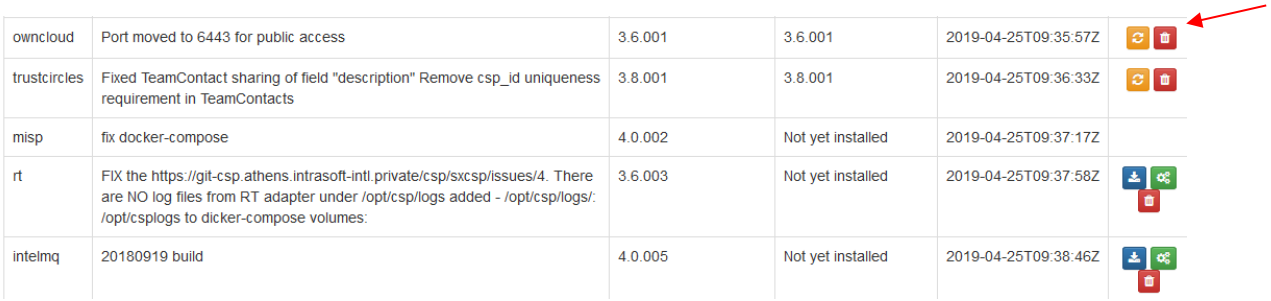
Image installations must begin from top to bottom in the same order as they are displayed, but they should not be performed concurrently. Users should wait until the installation of each module completes successfully before proceeding to the installation of the next one. Please note that *while an image 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/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	

[7] 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.

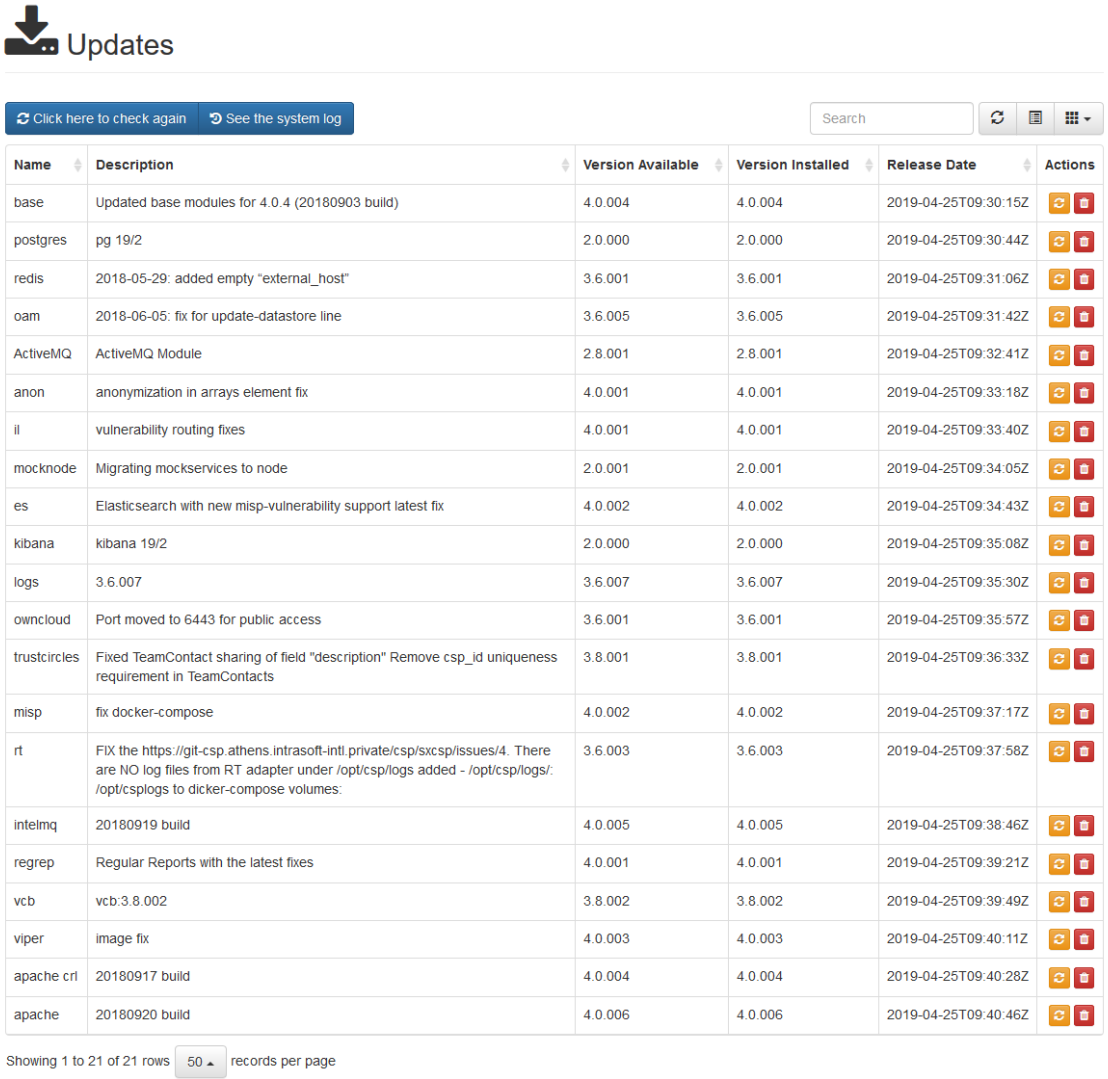
When an image installation is finished:

- 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).



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	
postgres	pg 19/2	2.0.000	2.0.000	2019-04-25T09:30:44Z	
redis	2018-05-29: added empty "external_host"	3.6.001	3.6.001	2019-04-25T09:31:06Z	
oam	2018-06-05: fix for update-datastore line	3.6.005	3.6.005	2019-04-25T09:31:42Z	
ActiveMQ	ActiveMQ Module	2.8.001	2.8.001	2019-04-25T09:32:41Z	
anon	anonymization in arrays element fix	4.0.001	4.0.001	2019-04-25T09:33:18Z	
il	vulnerability routing fixes	4.0.001	4.0.001	2019-04-25T09:33:40Z	
mocknode	Migrating mockservices to node	2.0.001	2.0.001	2019-04-25T09:34:05Z	
es	Elasticsearch with new misp-vulnerability support latest fix	4.0.002	4.0.002	2019-04-25T09:34:43Z	
kibana	kibana 19/2	2.0.000	2.0.000	2019-04-25T09:35:08Z	
logs	3.6.007	3.6.007	3.6.007	2019-04-25T09:35:30Z	
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	4.0.002	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	3.6.003	2019-04-25T09:37:58Z	
intelmq	20180919 build	4.0.005	4.0.005	2019-04-25T09:38:46Z	
regrep	Regular Reports with the latest fixes	4.0.001	4.0.001	2019-04-25T09:39:21Z	
vcb	vcb:3.8.002	3.8.002	3.8.002	2019-04-25T09:39:49Z	
viper	image fix	4.0.003	4.0.003	2019-04-25T09:40:11Z	
apache crl	20180917 build	4.0.004	4.0.004	2019-04-25T09:40:28Z	
apache	20180920 build	4.0.006	4.0.006	2019-04-25T09:40:46Z	

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

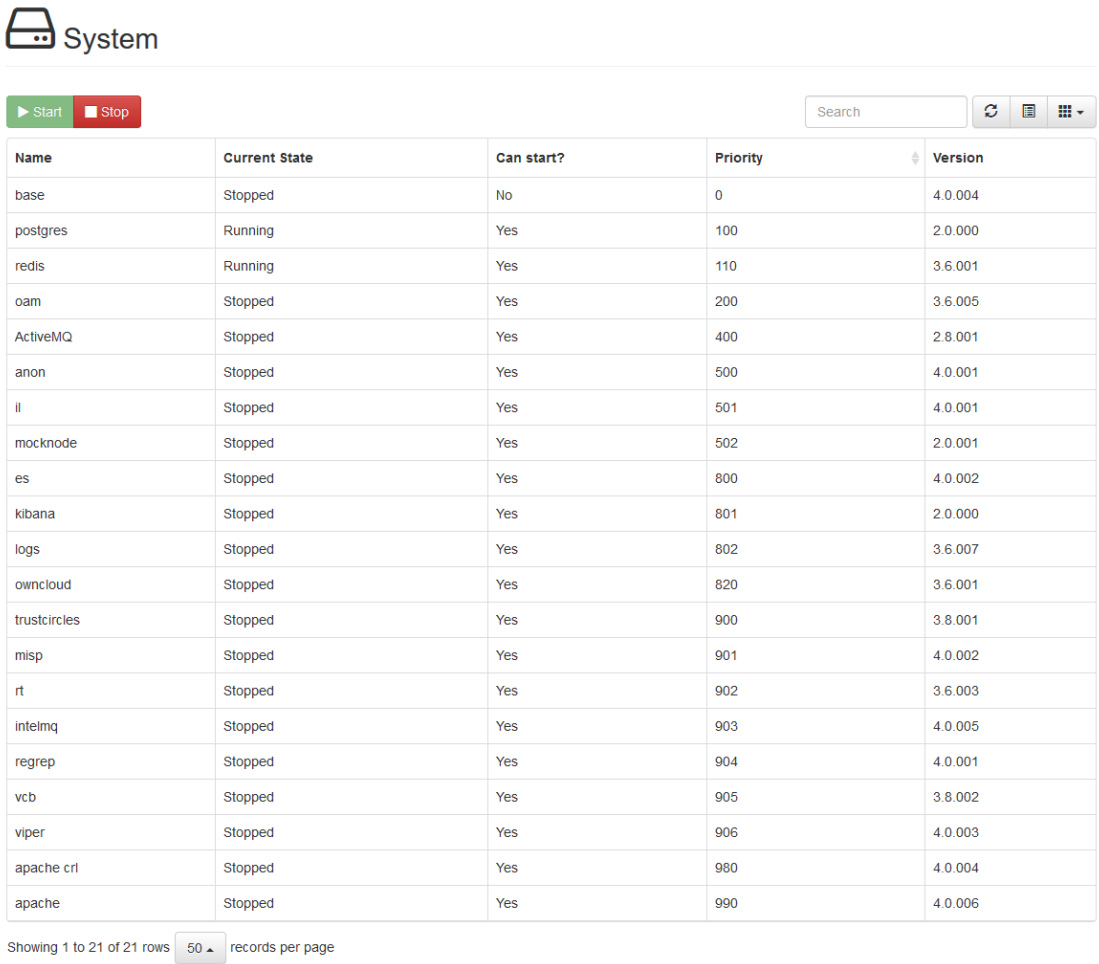
The “system” page shows a current view of the system services registered, together with their current status. The following states are possible:

- 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 ▶ 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).



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 crl	Stopped	Yes	980	4.0.004
apache	Stopped	Yes	990	4.0.006

Showing 1 to 21 of 21 rows 50 records per page

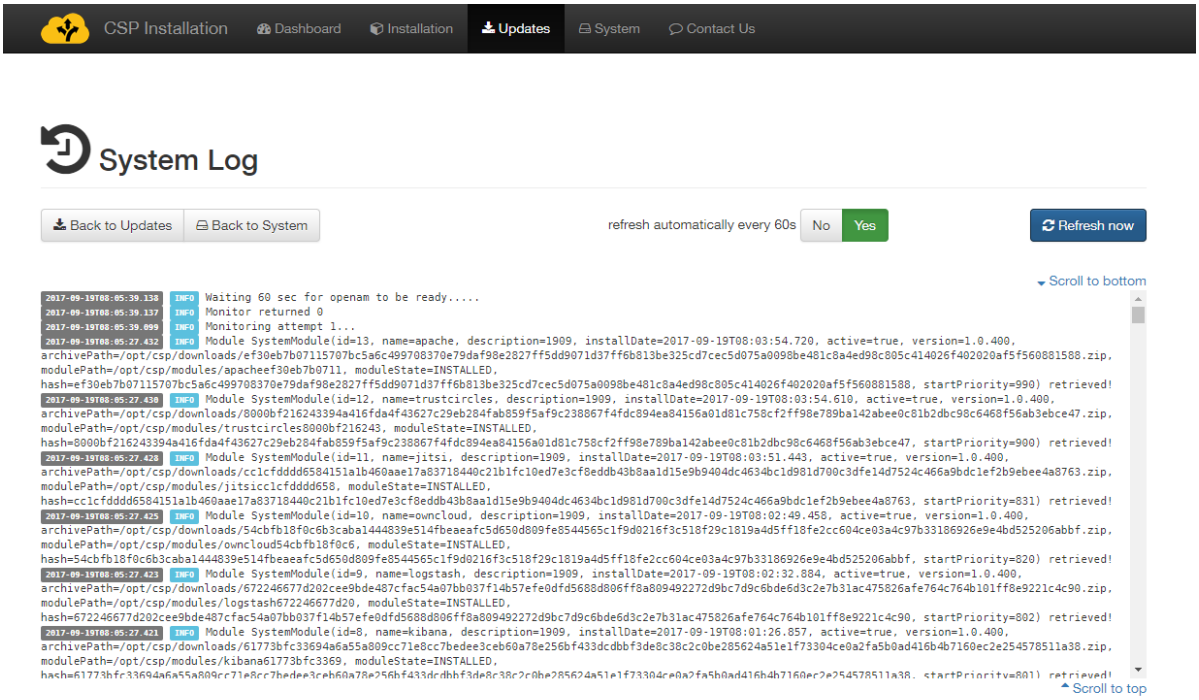
While the system is starting, the Start button is greyed out and the only available action is to stop the system. To initiate a System stop, click on the Stop ■ Stop button.

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**.

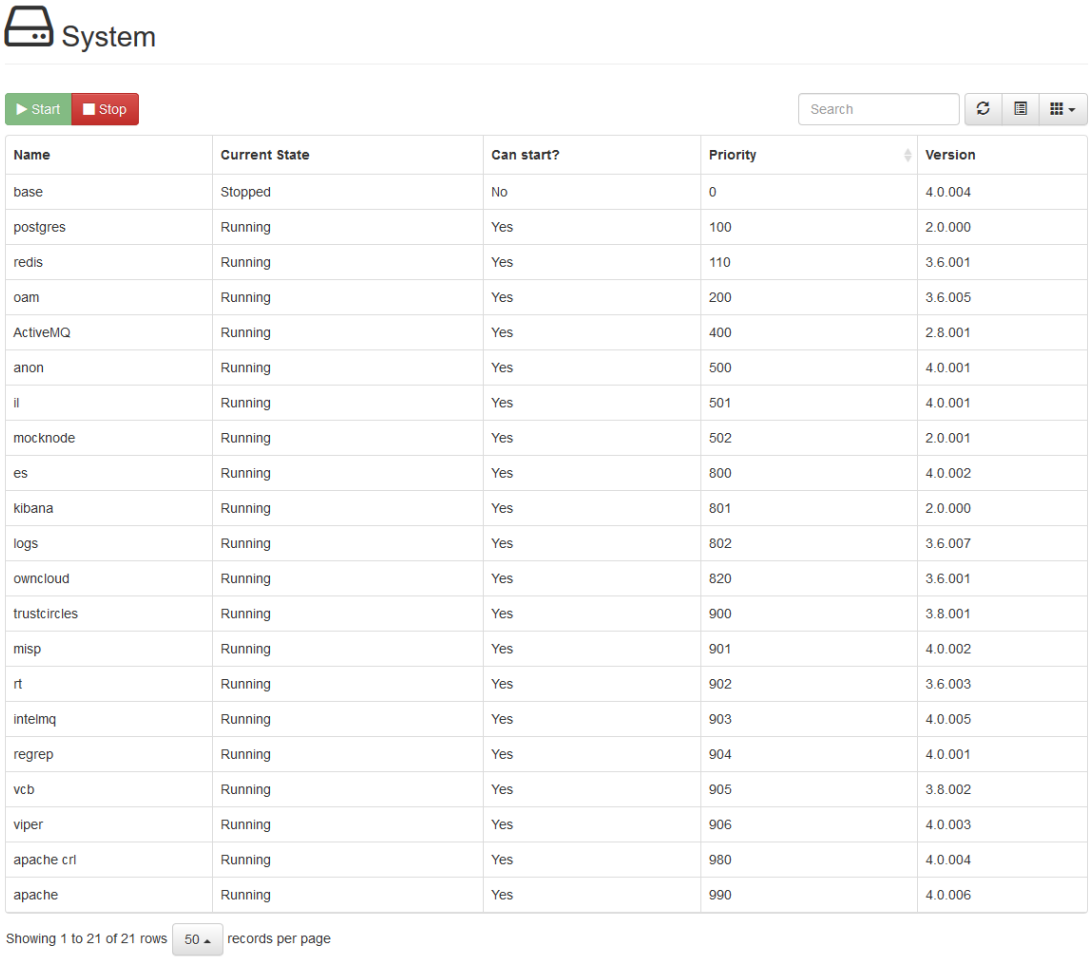
Especially system Start is normal to take several minutes to complete. The user should be patient until all modules report their state as “Running”. Depending on VM settings: configured RAM, type of disk drives (Solid state or Hard disk) it may take up to 30 minutes for all modules to start.

During this wait period, users can use the System 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.

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



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.



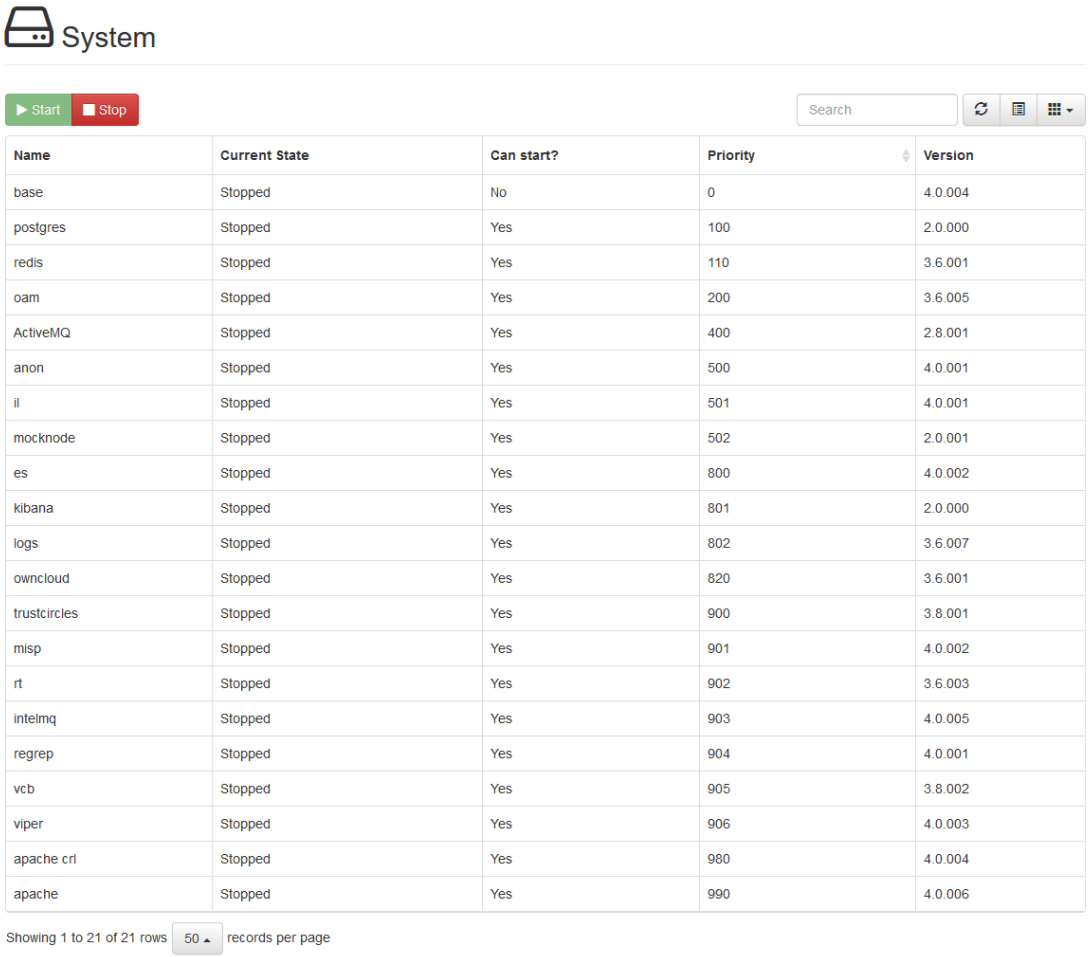
Name	Current State	Can start?	Priority	Version
base	Stopped	No	0	4.0.004
postgres	Running	Yes	100	2.0.000
redis	Running	Yes	110	3.6.001
oam	Running	Yes	200	3.6.005
ActiveMQ	Running	Yes	400	2.8.001
anon	Running	Yes	500	4.0.001
il	Running	Yes	501	4.0.001
mocknode	Running	Yes	502	2.0.001
es	Running	Yes	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.



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 crl	Stopped	Yes	980	4.0.004
apache	Stopped	Yes	990	4.0.006

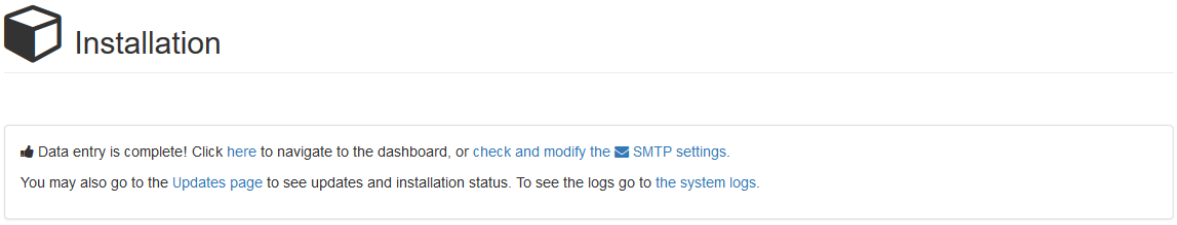
Showing 1 to 21 of 21 rows 50 records per page

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.

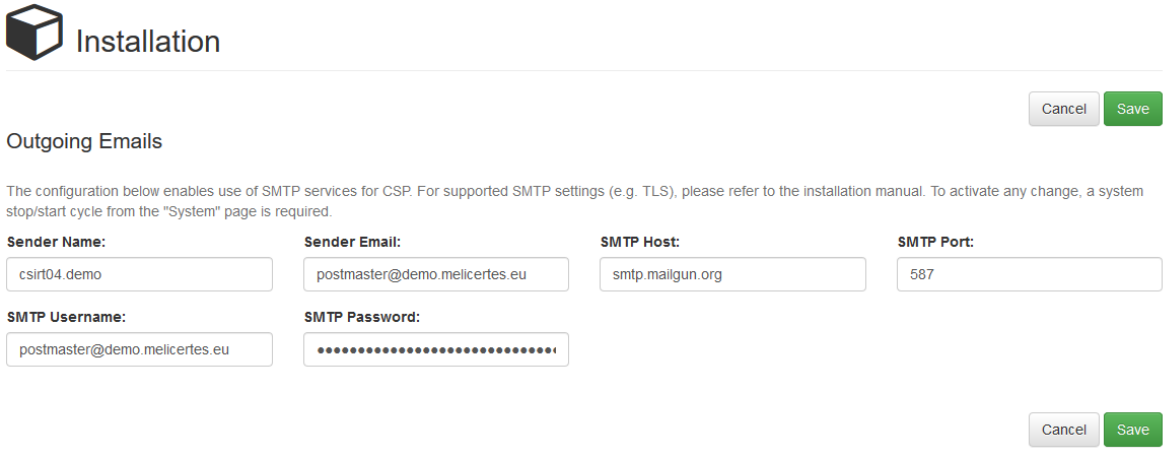
If a service is started using the console, the installer will not reflect its actual status showing it as “Stopped”. When we press the “Stop” button all services will begin to stop one after the other, but it is a good practice to verify that all services have indeed stopped afterwards by issuing the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



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:



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

```
cspvm [~]# docker stats --all --format "table {{.Name}}\t{{.CPUPerc}}\t{{.MemUsage}}" --no-stream | sort
NAME                CPU %               MEM USAGE / LIMIT
clever_banach       0.00%               0B / 0B
csp-activemq        0.07%               221.3MiB / 62.83GiB
csp-anon            0.14%               399MiB / 62.83GiB
csp-apache          0.05%               14.77MiB / 62.83GiB
csp-apache-crl      0.00%               1.52MiB / 62.83GiB
csp-es              1.77%               4.373GiB / 16GiB
csp-filebeat        0.08%               6.973MiB / 62.83GiB
csp-il              0.11%               434.1MiB / 62.83GiB
csp-imq             2.16%               369.8MiB / 62.83GiB
csp-intelmq_adapter 0.04%               301.7MiB / 62.83GiB
csp-jitsi           3.89%               351.9MiB / 62.83GiB
csp-kibana          0.56%               590.5MiB / 62.83GiB
csp-kibana_logs     0.20%               600.4MiB / 62.83GiB
csp-logstash        1.64%               484.8MiB / 62.83GiB
csp-misp            0.00%               0B / 0B
csp-misp-filebeat   0.02%               2.492MiB / 62.83GiB
csp-misp-logstash   1.29%               447.6MiB / 62.83GiB
csp-misp_adapter    0.09%               1.383MiB / 62.83GiB
csp-misp_proxy      0.06%               1.133MiB / 62.83GiB
csp-mock            0.00%               15.39MiB / 62.83GiB
csp-mysql           0.02%               104.3MiB / 62.83GiB
csp-oam             0.24%               1007MiB / 62.83GiB
csp-oam-filebeat    0.02%               7.59MiB / 62.83GiB
csp-oam-logstash    1.71%               479.8MiB / 62.83GiB
csp-oc              0.00%               52.43MiB / 62.83GiB
csp-ocdb            0.03%               43.93MiB / 62.83GiB
csp-ocredis         0.06%               3.215MiB / 62.83GiB
csp-postgres        0.12%               9.023MiB / 62.83GiB
csp-redis           0.00%               0B / 0B
csp-regrep          0.04%               335MiB / 62.83GiB
csp-rt              0.00%               623.7MiB / 62.83GiB
csp-rt_adapter      0.08%               362.5MiB / 62.83GiB
csp-tc              0.01%               113.7MiB / 62.83GiB
csp-tc-dsl          0.01%               1.547MiB / 62.83GiB
csp-vcb_admin       0.03%               419MiB / 62.83GiB
csp-vcb_teleconf    0.09%               383.1MiB / 62.83GiB
csp-viper           0.08%               1.656MiB / 62.83GiB
practical_feistel   0.00%               0B / 0B
cspvm [~]#
```

On the figure above we can see that two modules: csp-redis and csp-misp do not consume any CPU and do not use any memory, which is an indication that these two Docker containers are not operating.

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.

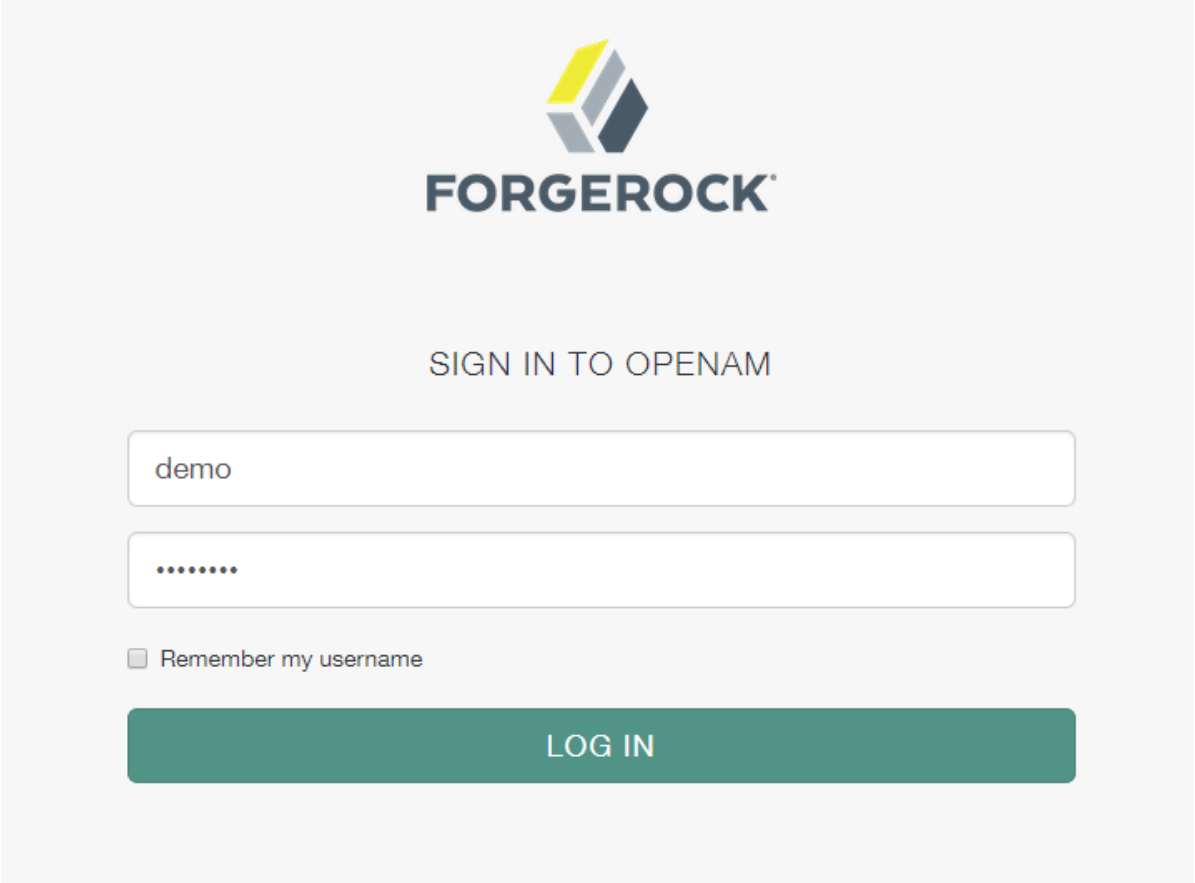
7.1 Connecting via the “Single Sign-on” service

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.

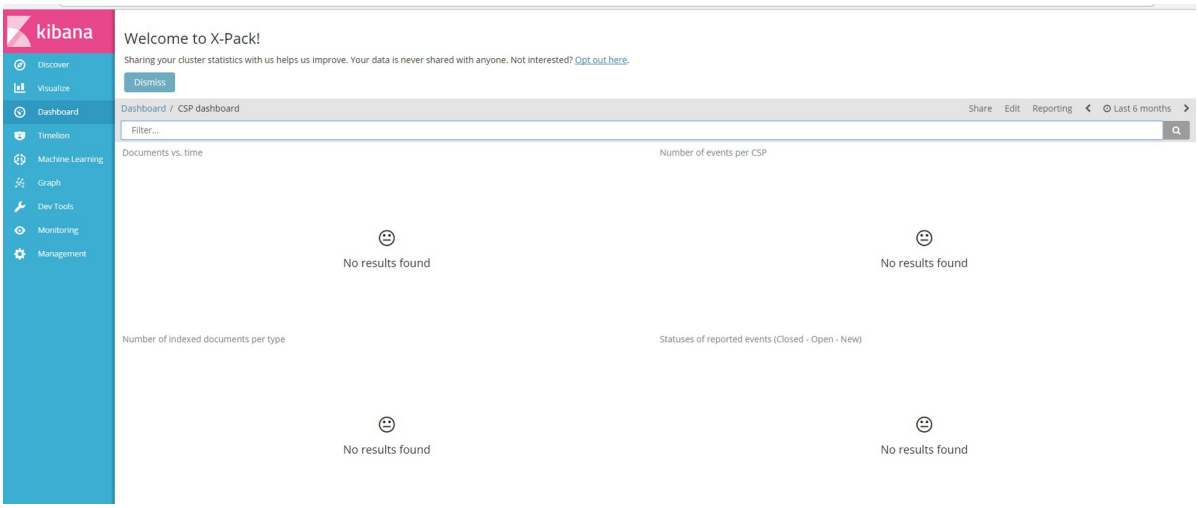
Also note than when accessing the various web interfaces, an SSL Insecure connection notice may appear due to the existence of self-signed certificates. The user should bypass the warning and proceed.

7.2 Connecting to individual services

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

Search: https://search.<cspId>.[preprod.]melicertes.eu

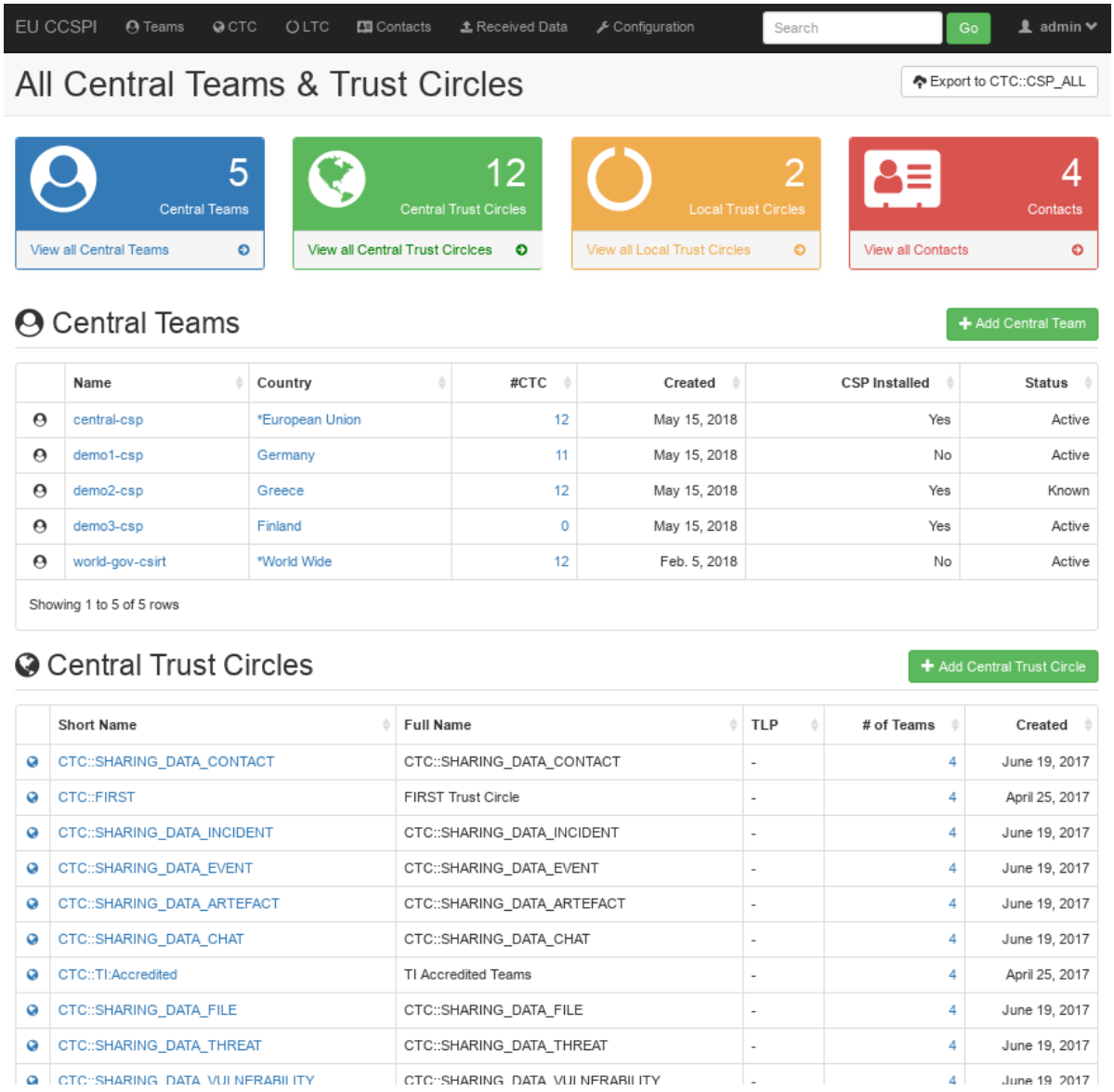
Navigate to Kibana by entering the above URL to your browser.



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.

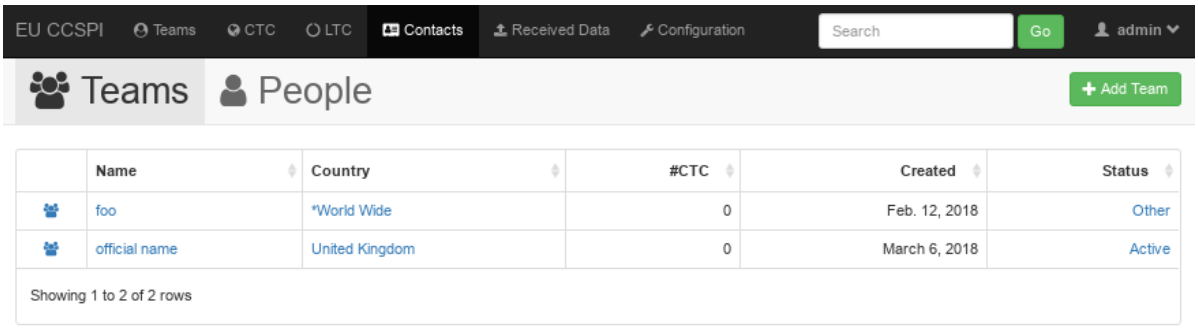
Trust Circles: https://tc.<cspId>.[preprod.]melicertes.eu

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.



Contact Management: https://tc.<cspId>.[preprod.]melicertes.eu/local/contacts/teams/

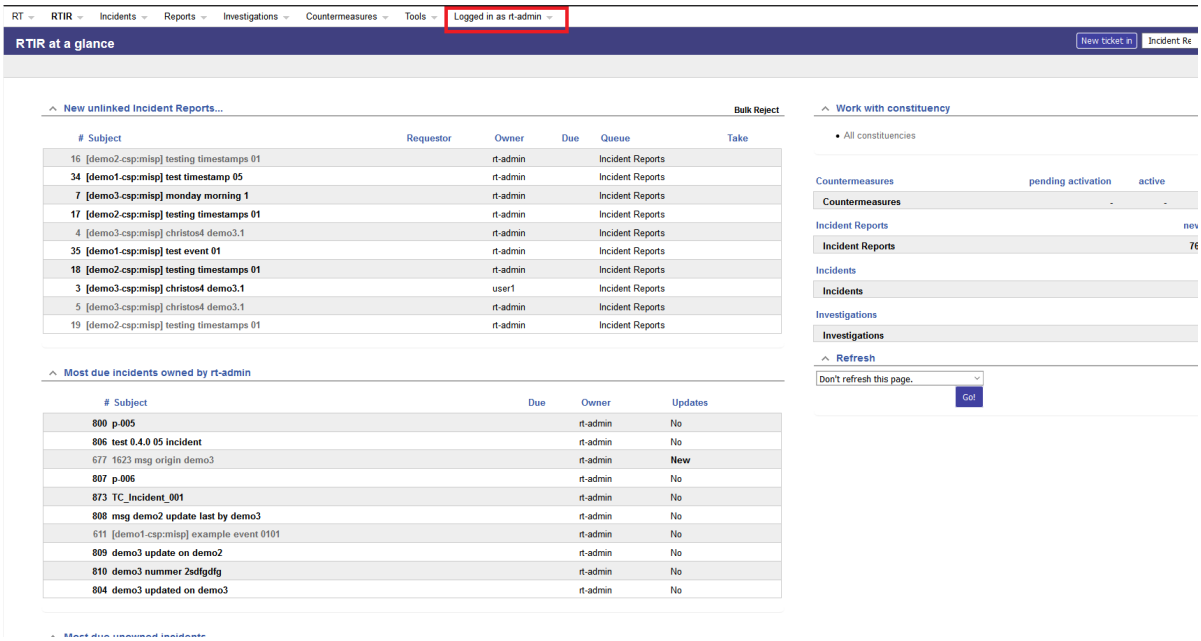
Navigate to Contact Management by entering the above URL to a browser. A page similar to the following should appear and a user as assigned with OpenAM should appear as logged in in the top right corner.



RT: https://rt.<cspId>.[preprod.]melicertes.eu/RTIR

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

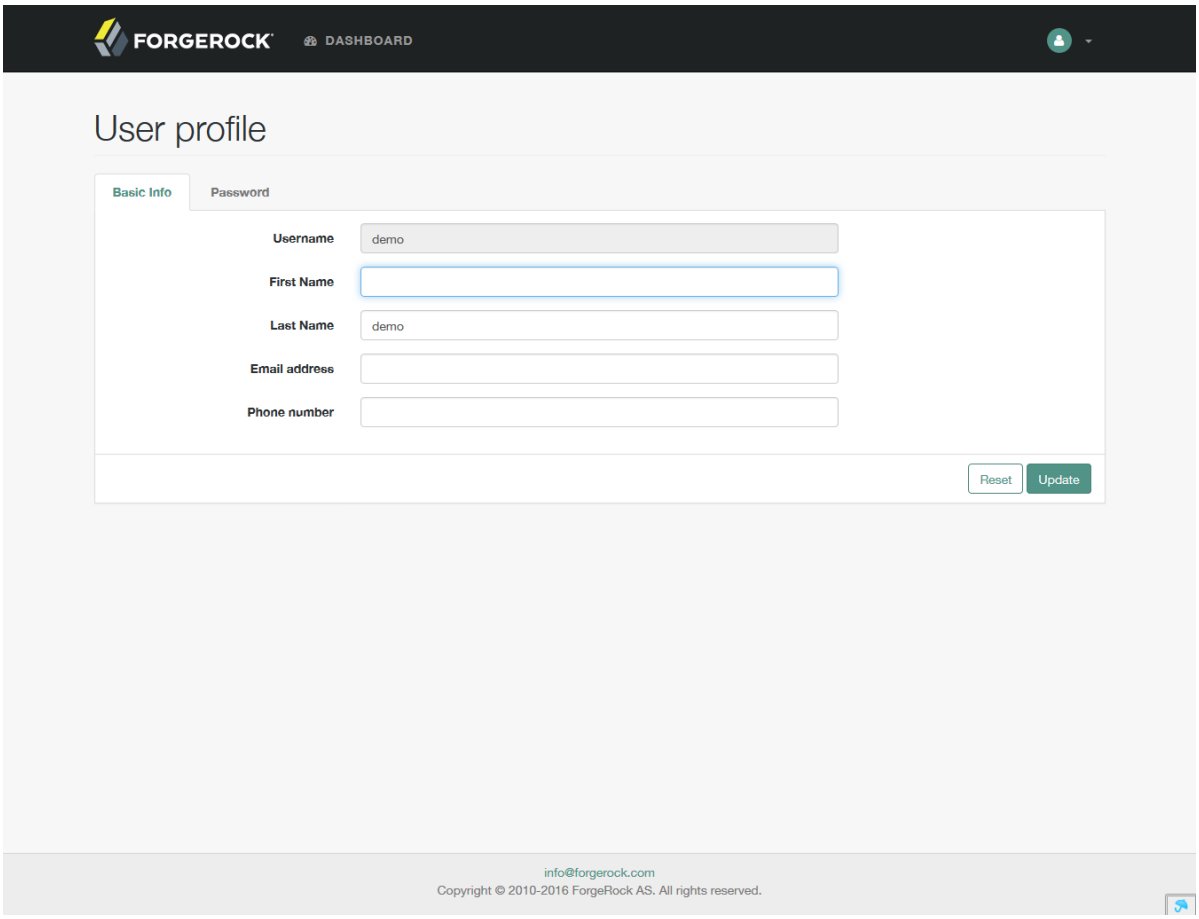
A page similar to those depicted on the following figure will be displayed and the logged in user will be displayed at the top of the page.



OpenAM: https://auth.<cspId>.[preprod.]melicertes.eu/openam

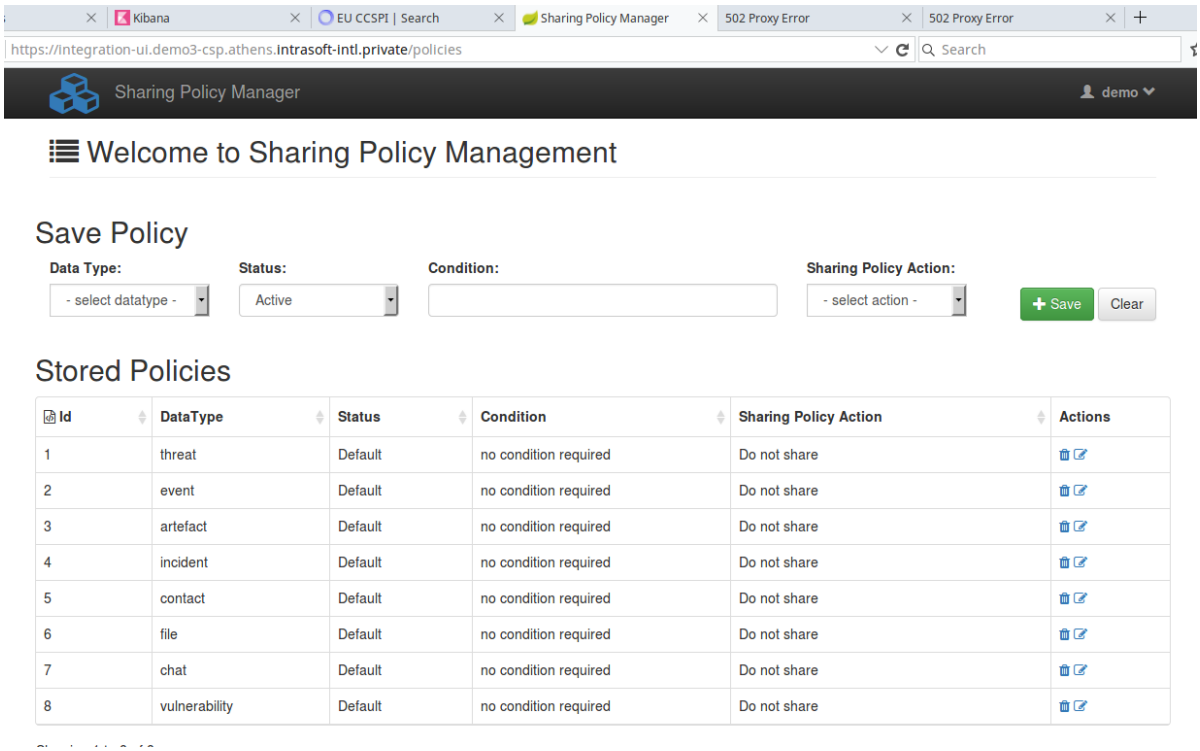
Navigate to OpenAM by entering the above URL to your browser.

A basic user editing information should be displayed.



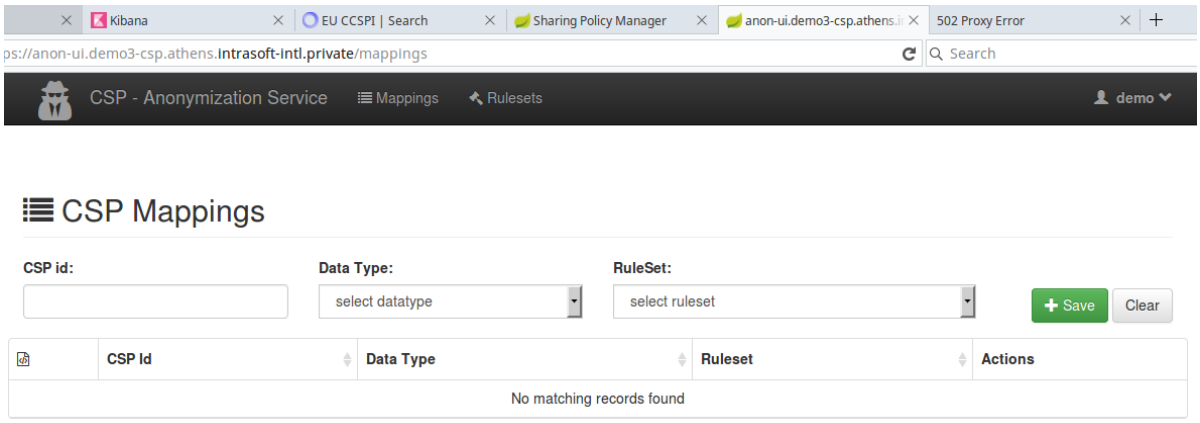
Sharing Policies: https://integration-ui.<cspId>.[preprod.]melicertes.eu

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



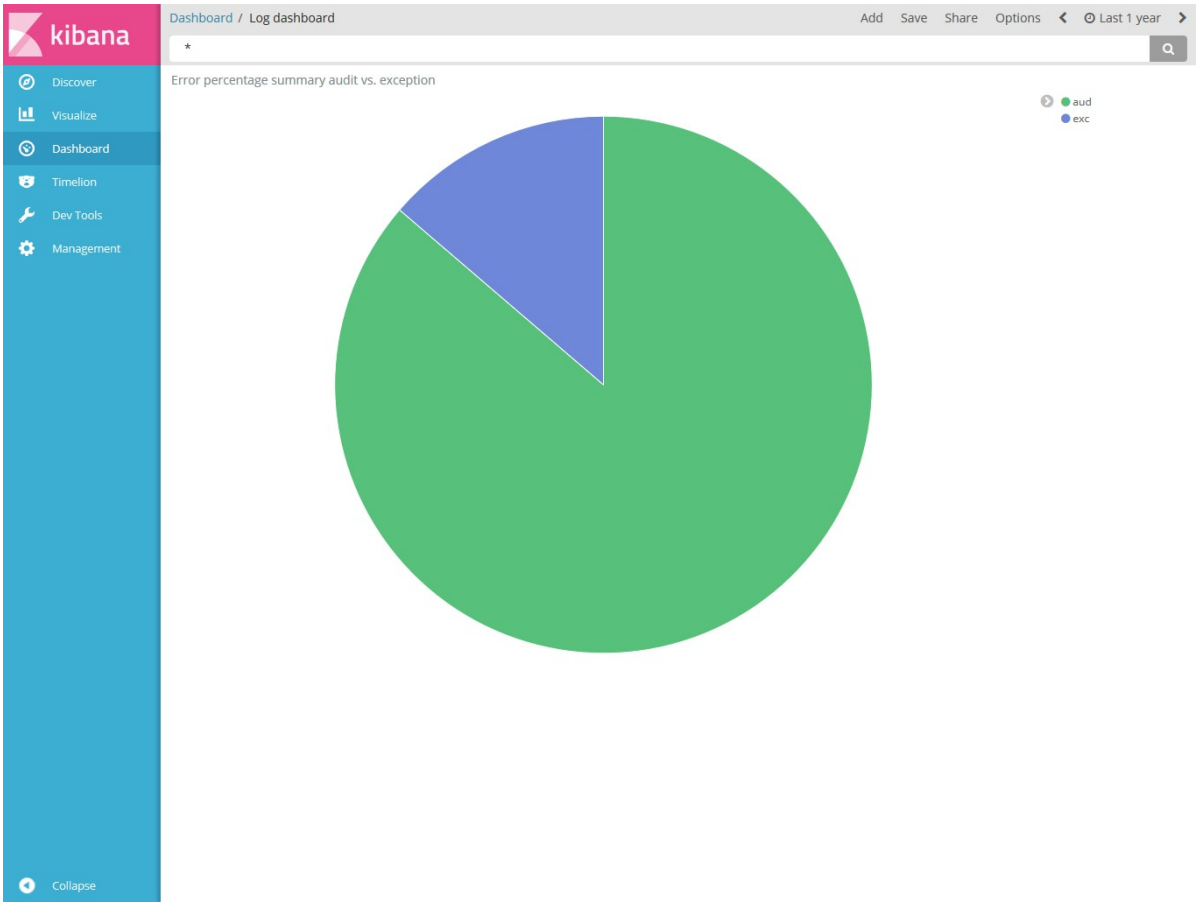
Anonymization: https://anon-ui.<cspId>.[preprod.]melicertes.eu

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



Logs: https://logs.<cspId>.[preprod.]melicertes.eu

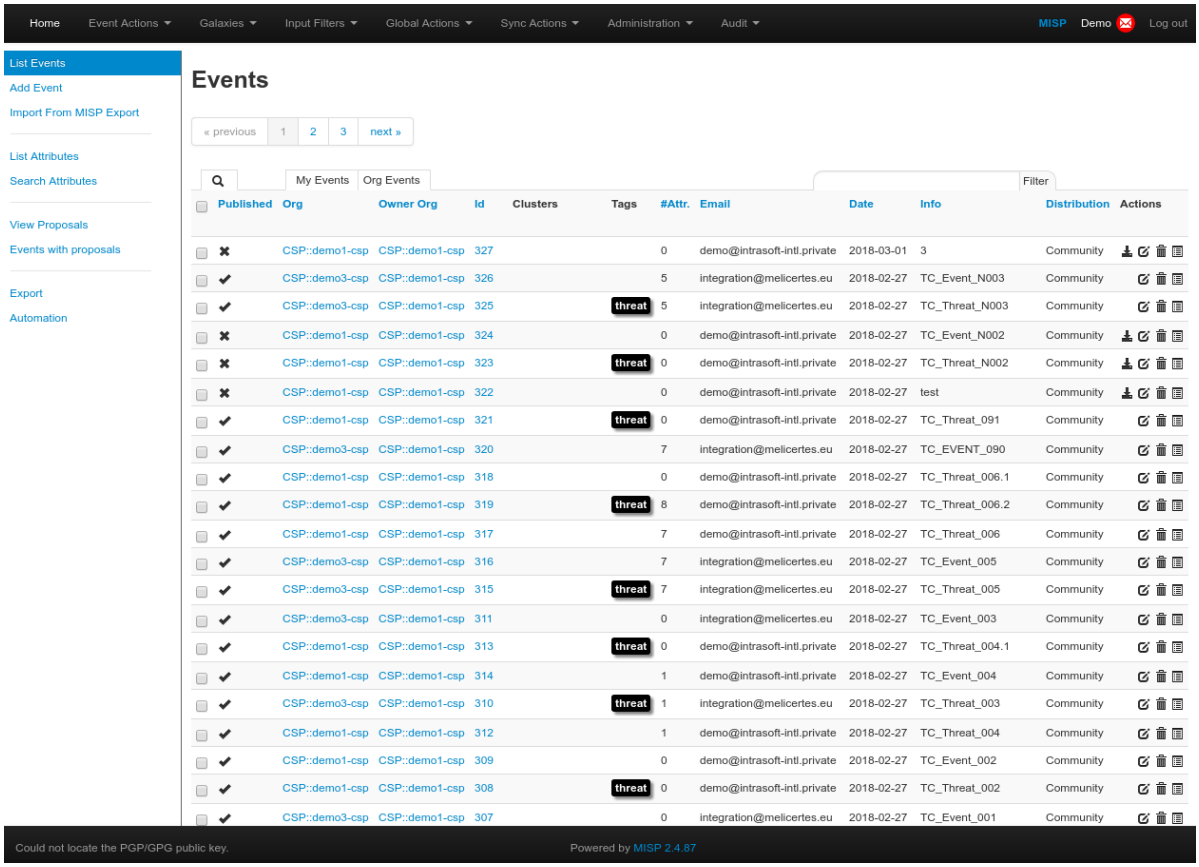
Navigate to the log display application by entering the above URL to a browser



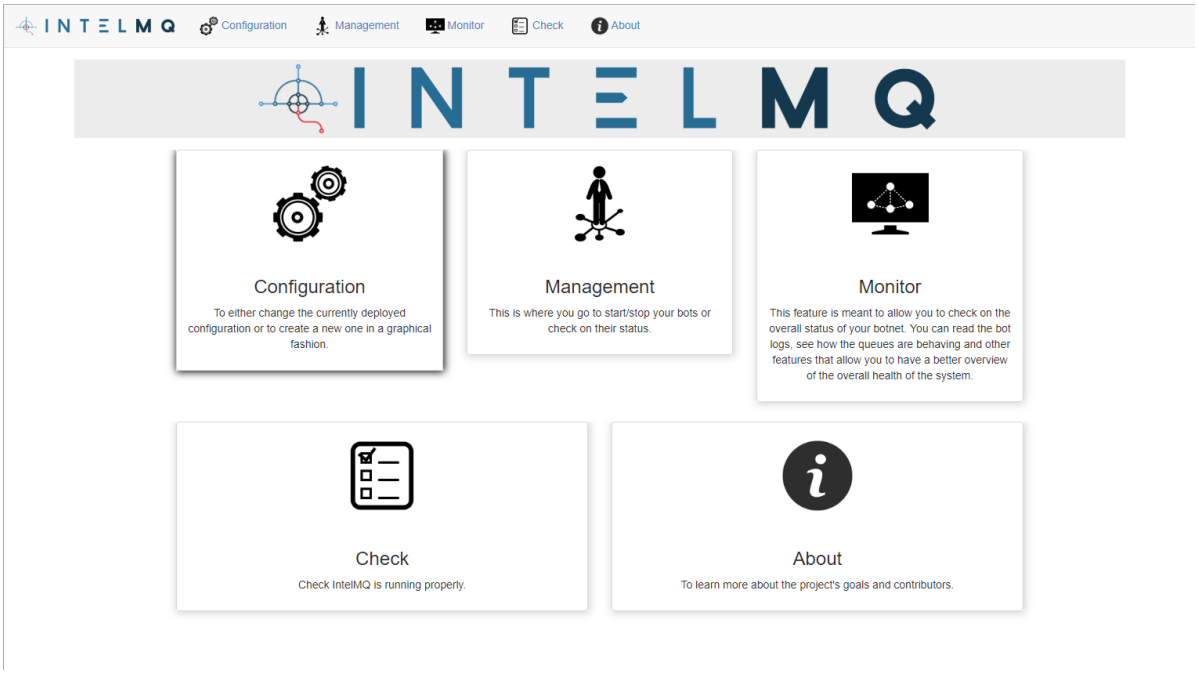
A log dashboard regarding audit and exception logs should be displayed.

MISP: https://misp-ui.<cspId>.[preprod.]melicertes.eu

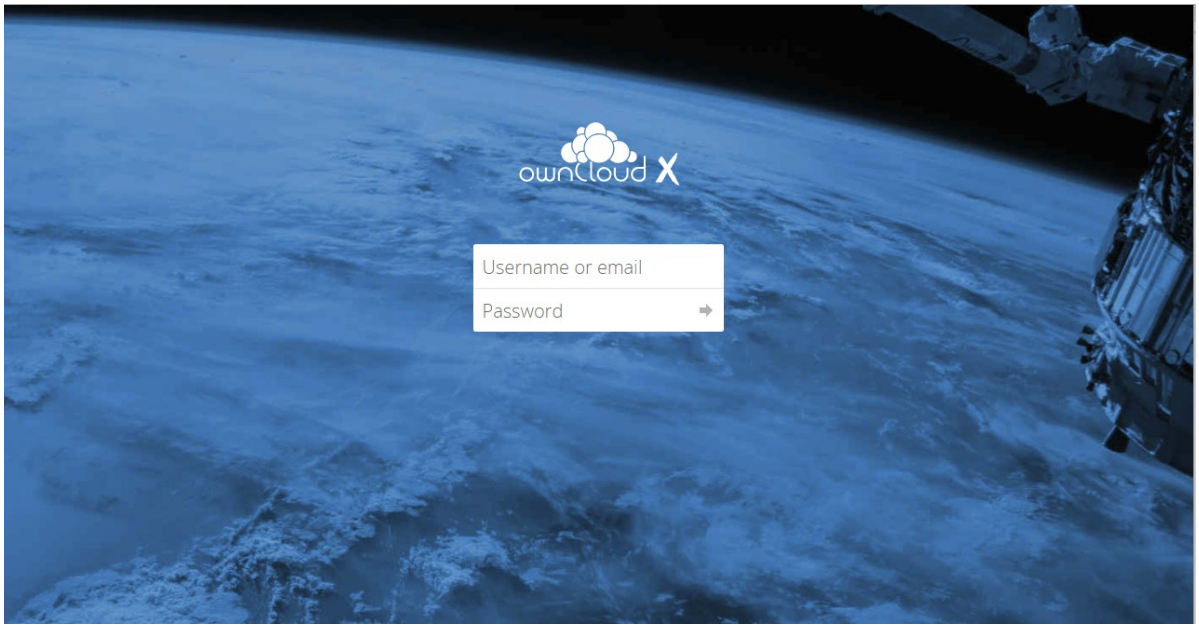
Navigate to the MISP web interface by entering the above URL to a browser



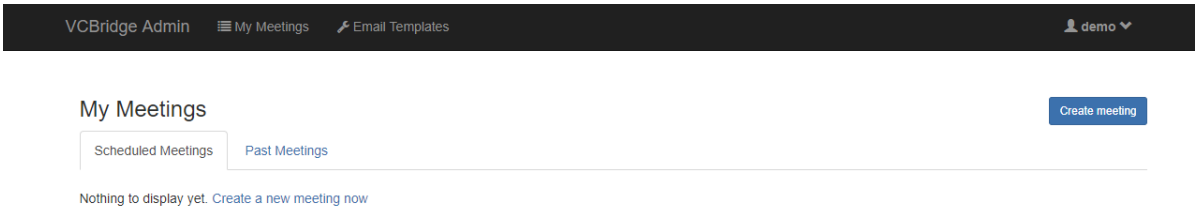
IntelMQ: https://imq.<cspId>.[preprod.]melicertes.eu



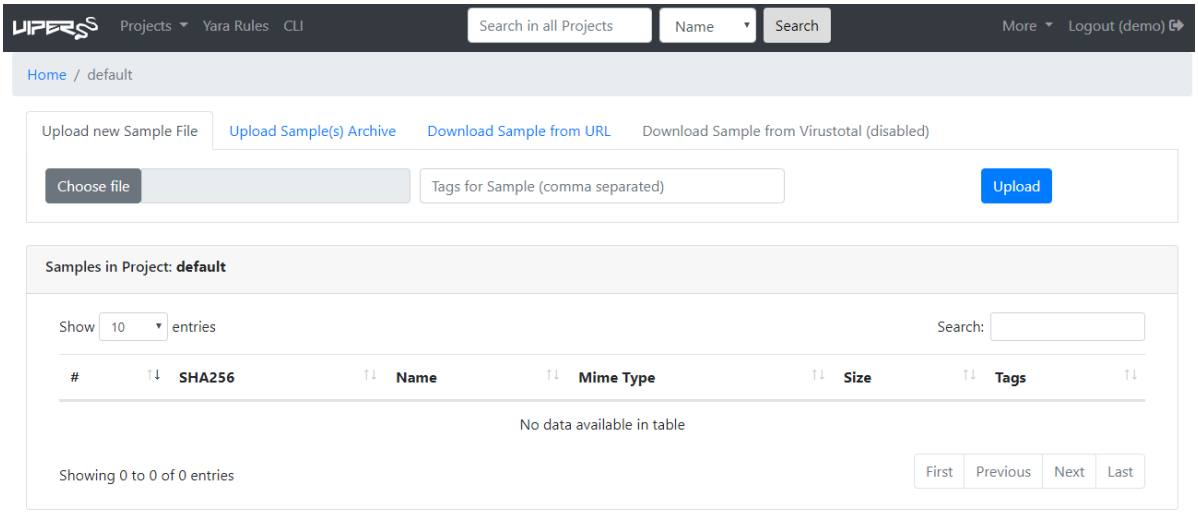
Owncloud: https://files.<cspId>.[preprod.]melicertes.eu



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



Viper: https://viper-ui. <cspId>.[preprod.]melicertes.eu



8 Hardening CSP

8.1 Configure a host firewall on VM

For sites with default configuration, this can be achieved by executing the following steps on the MeliCERTes VM. If you have modified the host firewall configuration, adjust it to ensure that ports which are not required by the MeliCERTes configuration are blocked accordingly.

1. Stop all CSP modules in CSP Installer/System

2. Paste lines below into /etc/iptables/rules-save:

```
# Content of /etc/iptables/rules-save

*filter

:INPUT DROP [0:0]

:FORWARD DROP [0:0]

:OUTPUT ACCEPT [0:0]

:DOCKER - [0:0]

:DOCKER-ISOLATION-STAGE-1 - [0:0]

:DOCKER-ISOLATION-STAGE-2 - [0:0]

:DOCKER-USER - [0:0]

[0:0] -A INPUT -i lo -j ACCEPT

[0:0] -A INPUT -i br+ -j ACCEPT

[0:0] -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

[0:0] -A INPUT -m state --state INVALID -j DROP

[0:0] -A INPUT -i eth0 -m state --state NEW -p tcp -m tcp --dport 22 -j ACCEPT

[0:0] -A DOCKER-USER -m state --state RELATED,ESTABLISHED -j ACCEPT

[0:0] -A DOCKER-USER -m state --state INVALID -j DROP

[0:0] -A DOCKER-USER -i eth0 -p udp -m udp ! --dport 10000 -j DROP

[0:0] -A DOCKER-USER -i eth0 -p tcp -m multiport ! --dports 5443,6443,4443,443 -j DROP

[0:0] -A DOCKER-USER -j RETURN

COMMIT
```

3. Disable auto-saving iptables:

```
sed -i 's/SAVE_ON_STOP="yes"/SAVE_ON_STOP="no"/' /etc/conf.d/iptables
```

4. Enable iptables on startup:

```
rc-update add iptables
```

5. Ensure Docker is started after the iptables rules are loaded:

```
sed -i 's/need sysfs cgroups$/need sysfs cgroups firewall/' /etc/init.d/docker
```

8.2 Change the default password for ActiveMQ

1. Generate a new admin password for ActiveMQ management interface and save it by applying the following commands:

```
PASS=`dd if=/dev/random bs=1 count=13 2>/dev/null | base64`

sed -i "s~admin: admin, admin~admin: $PASS, admin~g" \
/var/lib/docker/volumes/AMQConfigVolume/_data/jetty-realm.properties

echo $PASS
```

Make sure to backup the password in case access to the management interface is needed in the future.

8.3 Finalize the MeliCERTes VM changes

The simplest way to apply all the changes is to restart the entire appliance.

1. Restart the VM

```
reboot
```

8.4 Networking best practices

1. Use the “deny by default” policy when configuring access to the MeliCERTes instance. Only allow the ports that are required by chapter 2.2

2. Place the MeliCERTes instance in a separate network segment with no access to/from your internal infrastructure, with the exception of “known good” connections. Refer to chapter 2.3 and your organization’s best practices.

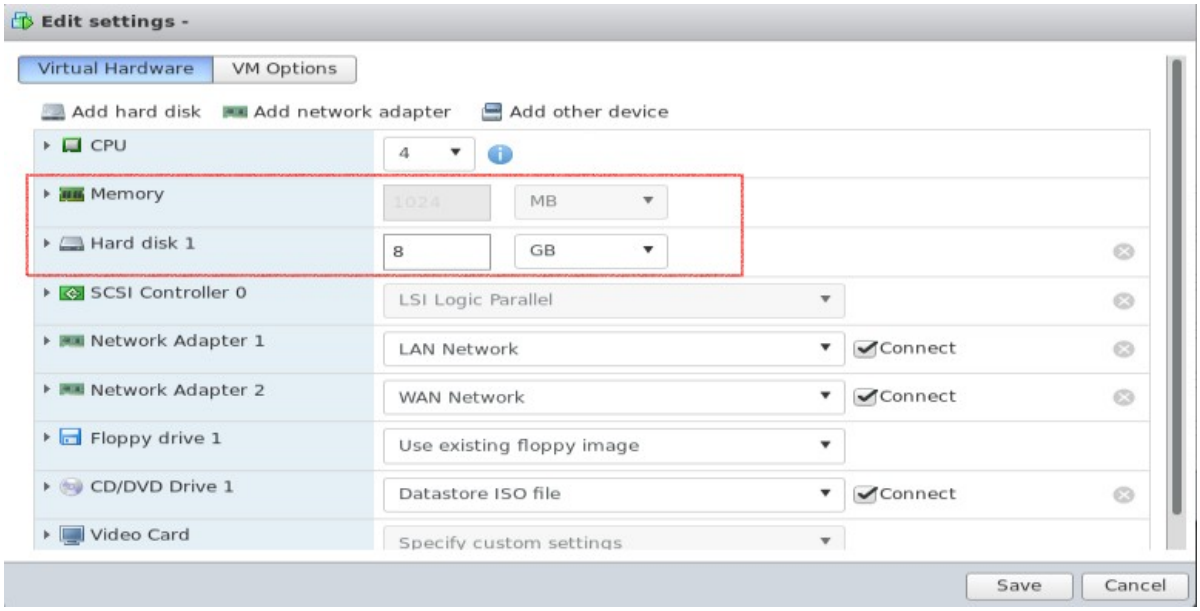
9 Annex A: Changing settings of the VM

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.*

9.1 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 (**very important step!**):

```
$ 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.

10 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.

10.1 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 with HTTPS

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.).

10.2 Bandwidth requirements

The Jitsi Videoconferencing Bridge implements a "Selective Forwarding Unit[8] – 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.

In the following example is the absolute maximum requirements for a 5 participant HD conference (720p):

- 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:
  - Clients:
    - Send: 550 Kbps (one video and one audio channel)
    - Receive: 550 x (N - 1) = 550 x 4 = 2200 Kbps (video/audio from 4 participants)
  - Server (bridge):
    - Receive: 550 x N = 550 x 4 = 2200 Kbps (Bridge receives N participant audio/video streams)
    - Send: 550 x (N) x (N - 1) = 550 x 5 x 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.

[8] See https://jitsi.org/jitsi-videobridge-performance-evaluation/ and https://webrtcglossary.com/sfu/ for SFU explanation

11 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 applicarion 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 abobe command should look like:

```
2018-10-12 11:35:26.265  INFO 2363 --- [pool-3-thread-1] c.i.c.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.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.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.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.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.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.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.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.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.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.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

12 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:

```
ps -ef | grep cspinst
 UUID   PID PPID C STIME TTY       TIME CMD
 root  2170    0 0 Sep23   ?   00:00:00 grep cspinst
 root 32135    0 0 Sep23   ?   00:00:00 /bin/bash -c /opt/cspinst/cspinstaller.sh>/tmp/console.log 2>&1
 root 32136    0 0 Sep23   ?   00:00:00 bash opt/cspinst/cspinstaller.sh
 root 32149    0 0 Sep23   ?   00:00:00 {cspinstaller.ja} /bin/bash ./cspinstaller.jar
 root 32166    0 0 Sep23   ?   00:00:00 /opt/cspinst/java/bin/java -
Dsun.misc.URLClassPath.disableJarChecking=true -jar /opt/cspinst/cspinstaller.jar
```

The command ***cspinstaller.sh*** starts automatically on boot, you should not attempt to manually start it! It would be preferable you opened a ticket to help you troubleshooting it.

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
```

13 Annex E: Manual Installation and configuration of the CSP Installer

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

7 *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.*

8 *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.

Prerequisities 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 reponse, 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 /tc/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 reccomended 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 preffix 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 11 (Services that need to be reached inside your local network) of this manual.

14 Annex F: Module Overview

Short Name	Module Name	Relates to	used on	required	type
base	Base Images	Default	Basic / Central	Yes	Configuration
postgres	PostgreSQL Database	Default	Basic / Central	Yes	Service (Startable)
redis	REDIS Database	Default	Basic / Central	Yes	Service (Startable)
oam	OpenAM	Default	Basic / Central	Yes	Service (Startable)
cfg	Configuration	Central	Central	Yes (*2)	Service not handled by 18080/tcp
activemq	ActiveMQ for IL	Default	Basic / Central	Yes	Service (Startable)
anon	Anonymisation	Shared Services	Basic / Central	Yes	Service (Startable)
il	Integration Layer	Shared Services	Basic / Central	Yes	Service (Startable)
mock	Mock component used by IL	Shared Services	Basic / Central	No	Service (Startable)
es	Elastic Search main	Shared Services (ELK)	Basic / Central	Yes (*1)	Service (Startable)
kibana	Elastic Search Kibana	Shared Services (ELK)	Basic / Central	Yes (*1)	Service (Startable)
logs	Elastic Search Logstash	Shared Services (ELK)	Basic / Central	Yes (*1)	Service (Startable)
owncloud	Owncloud	Secure Comms	Basic	No	Service (Startable)
trustcircles	Trust Circles / CMM	Shared Services	Basic / Central	Yes	Service (Startable)
misp	MiSP	Apps	Advanced	No	Service (Startable)
rt	RT(IR)	Apps	Advanced	No	Service (Startable)
intelmq	IntelMQ	Apps	Advanced	No	Service (Startable)
regrep	Report Generation	Shared Services (ELK)	Advanced	No	Service (Startable)
vcb	VideoConfBridge	Secure Comms	Basic	No	Service (Startable)
viper	VIPER	Apps	Advanced	No	Service (Startable)
apache-crl	Apache CRL	Shared Services	Basic / Central	Yes	Service (Startable)
apache	Apache Web Server	Shared Services	Basic / Central	Yes	Service (Startable)

(*1) change request is pending to make these modules optional!

(*2) This is the only module which only runs on the Central Node and therefore is different from all other instances. It's a repository for all instances (including the Central Node itself) to offer the available the software modules as configured per instance.

- End of document-