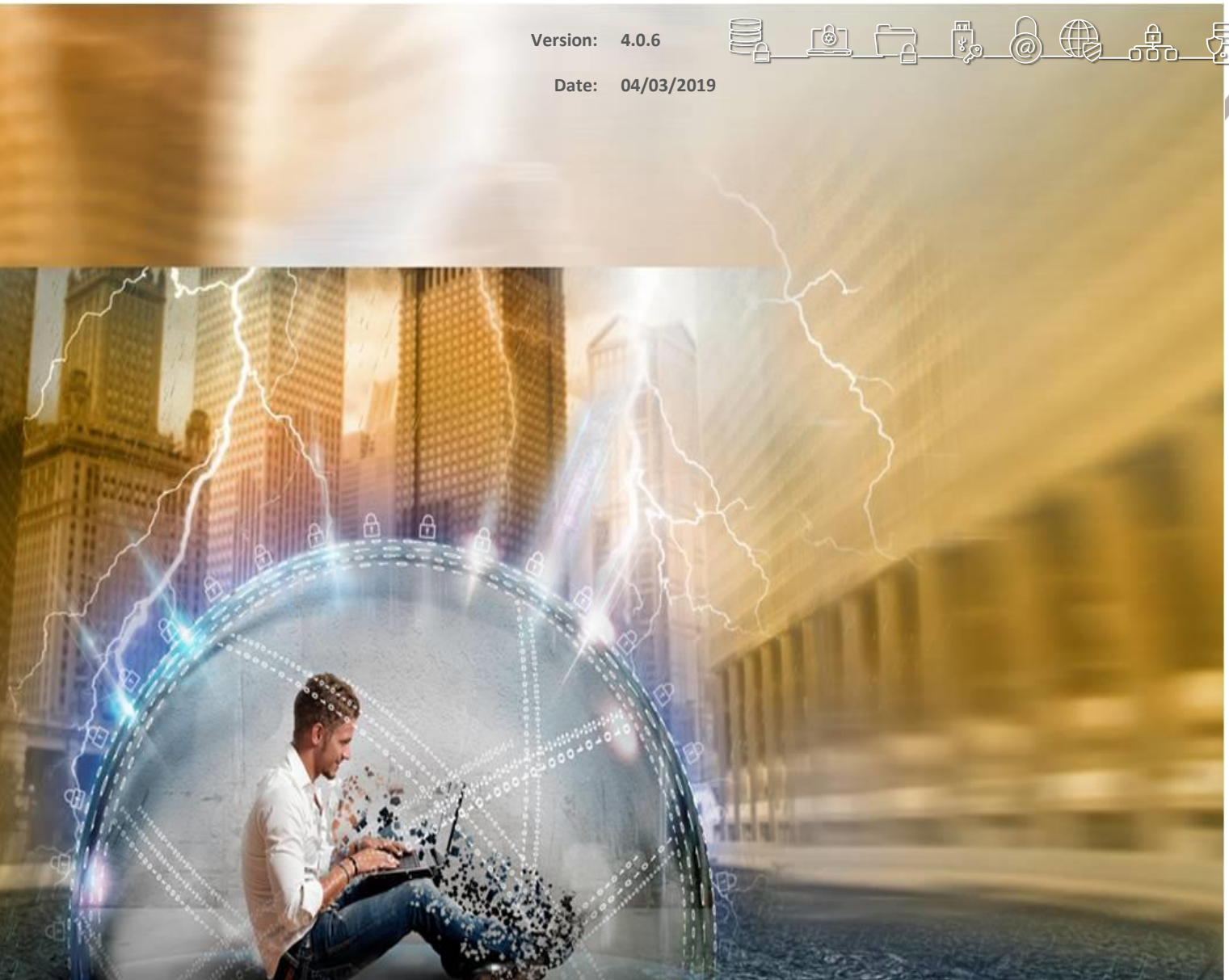
Cybersecurity Digital Service Infrastructure;

Core Service Platform – SMART 2015/1089

Installation Manual

Version: 4.0.6

Date: 04/03/2019



Contents

1 Preparatory steps

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

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

1. You received the hardware requirements for the CSP installation
2. You registered for a CSP installation to the central CSP authority
    a. You sent the required data and point of contact details
    b. You sent the IP address that you are going to use for your installation
    c. Your team data has been entered in the central CSP trust circles
    d. Your domain has been assigned and registered for the given IP address
3. You received an email confirming the actions in step 2 and the following:
    a. You are assigned a CSP Id.
    b. You are assigned a MeliCERTes domain in the form of <cspId>.prod.melicertes.eu (e.g. cert-gr.prod.melicertes.eu)
    c. Three manuals: Installation Manual, Configuration Manual, User Manual
    d. A link to download the base VM in OVA format

2 External Facing Services and Service URLs

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

Note: Domains in the production environment are in the form of *.<cspId>.prod.melicertes.eu

2.1 Internet Facing Services

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

Integration Layer	https://integration.<cspId>.prod.melicertes.eu	TCP 5443 (https)
OwnCloud	https://files.<cspid>.prod.melicertes.eu	TCP 6443 (https)
Jitsi VideoConferencing Bridge	https://teleconf.<cspid>.prod.melicertes.eu	TCP 6443 (https)
Jitsi VideoConferencing Bridge	https://vc.<cspid>.prod.melicertes.eu	TCP 6443 (https)
Jitsi VideoConferencing Bridge – Media TCP	vc.<cspid>.prod.melicertes.eu	TCP 4443 (SSL)
Jitsi VideoConferencing Bridge – Media UDP	vc.<cspid>.prod.melicertes.eu	UDP 10000

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

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

2.2 User Interfaces

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

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

Jitsi VideoConferencing Bridge Admin.	https://teleconf-ui.<cspId>.prod.melicertes.eu	TCP 443 (https)
InteMQ Manager	https://imq.<cspId>.prod.melicertes.eu	TCP 443 (https)
Viper Manager	https://viper-ui.<cspId>.prod.melicertes.eu	TCP 443 (https)

Note: You can bookmark the above links after replacing the correct <cspId>.

2.3 Other

SSH should be accessible only from within your organization:

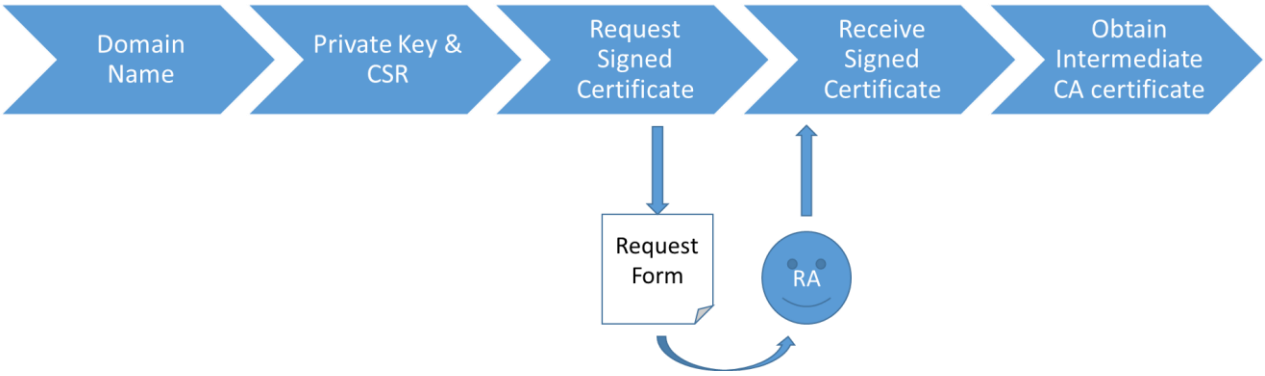
SSH	<cspId>.prod.melicertes.eu	TCP 22

3 Requesting a Certificate via the PKI

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

The generic steps are:

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



3.1 Get the domain name

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

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

3.2 Create the private key and a CSR

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

3.2.1 Create the private key

Execute the following command:

```
openssl genrsa -out bari[1].test.melicertes.eu.key 2048
```

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

Output will be similar to:

```
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.............................................+++
e is 65537 (0x10001)
```

The result will be a file named `bari.test.melicertes.eu.key`.

3.2.2 Create the CSR

Execute the following command (substitute the determined domain name for the value of the 'CN' field):

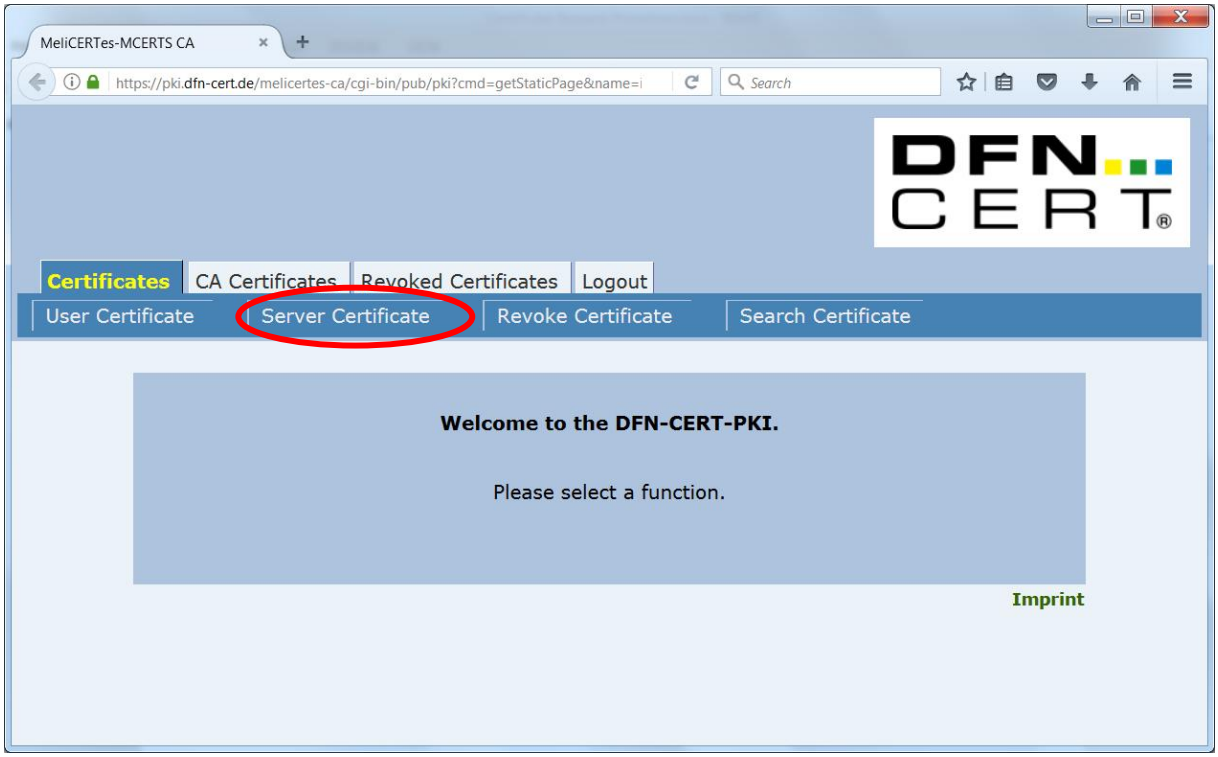
```
openssl req -new -key bari.test.melicertes.eu.key -out
bari.test.melicertes.eu.csr -subj "/CN=*.bari.test.melicertes.eu/O=MeliCERTes-
MCERTS/C=EU/DC=eu/DC=melicertes"
```

The command does not produce any console output. The result will be a file named:

`bari.test.melicertes.eu.csr`.

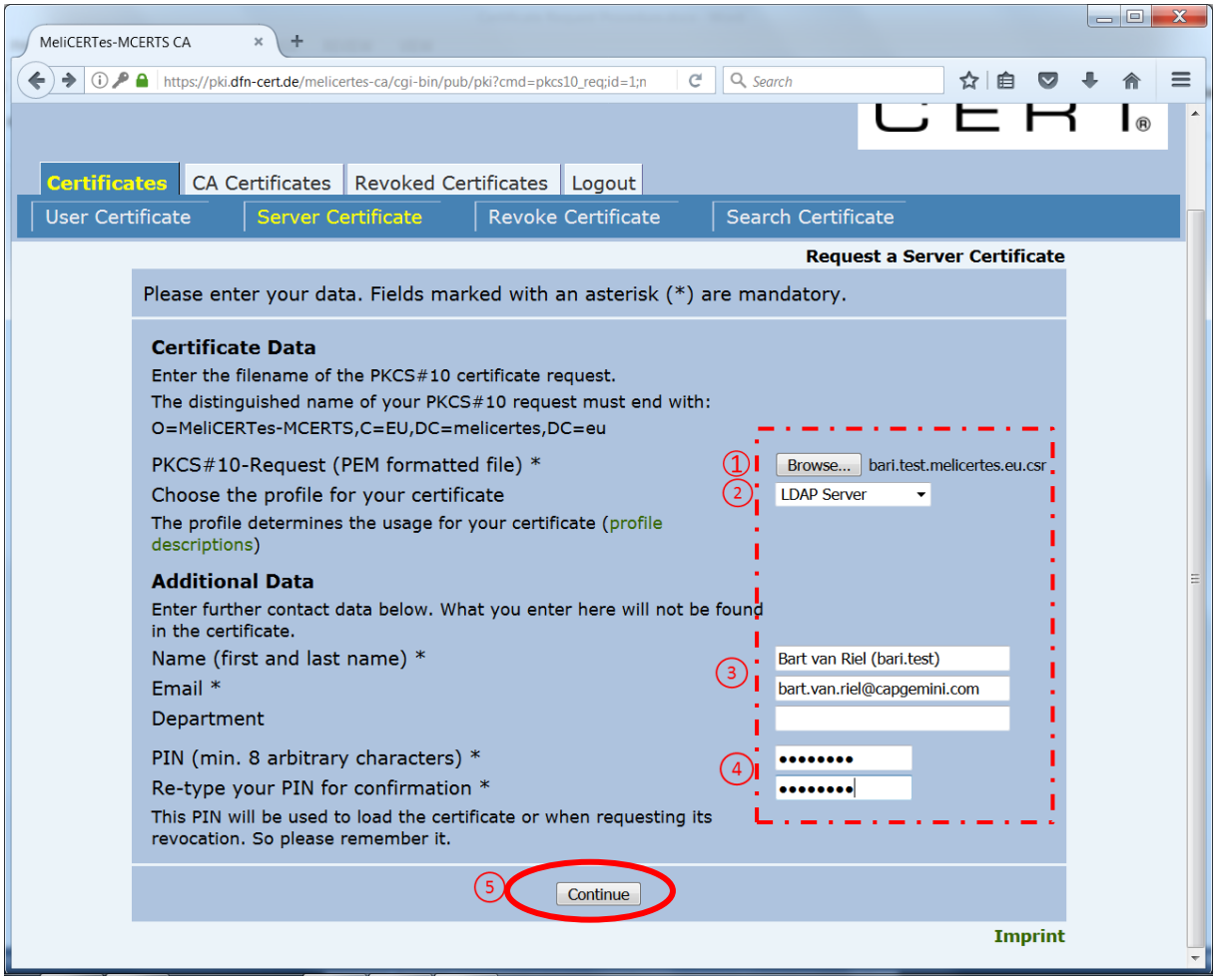
3.3 Submit the CSR to the PKI for signing

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”.

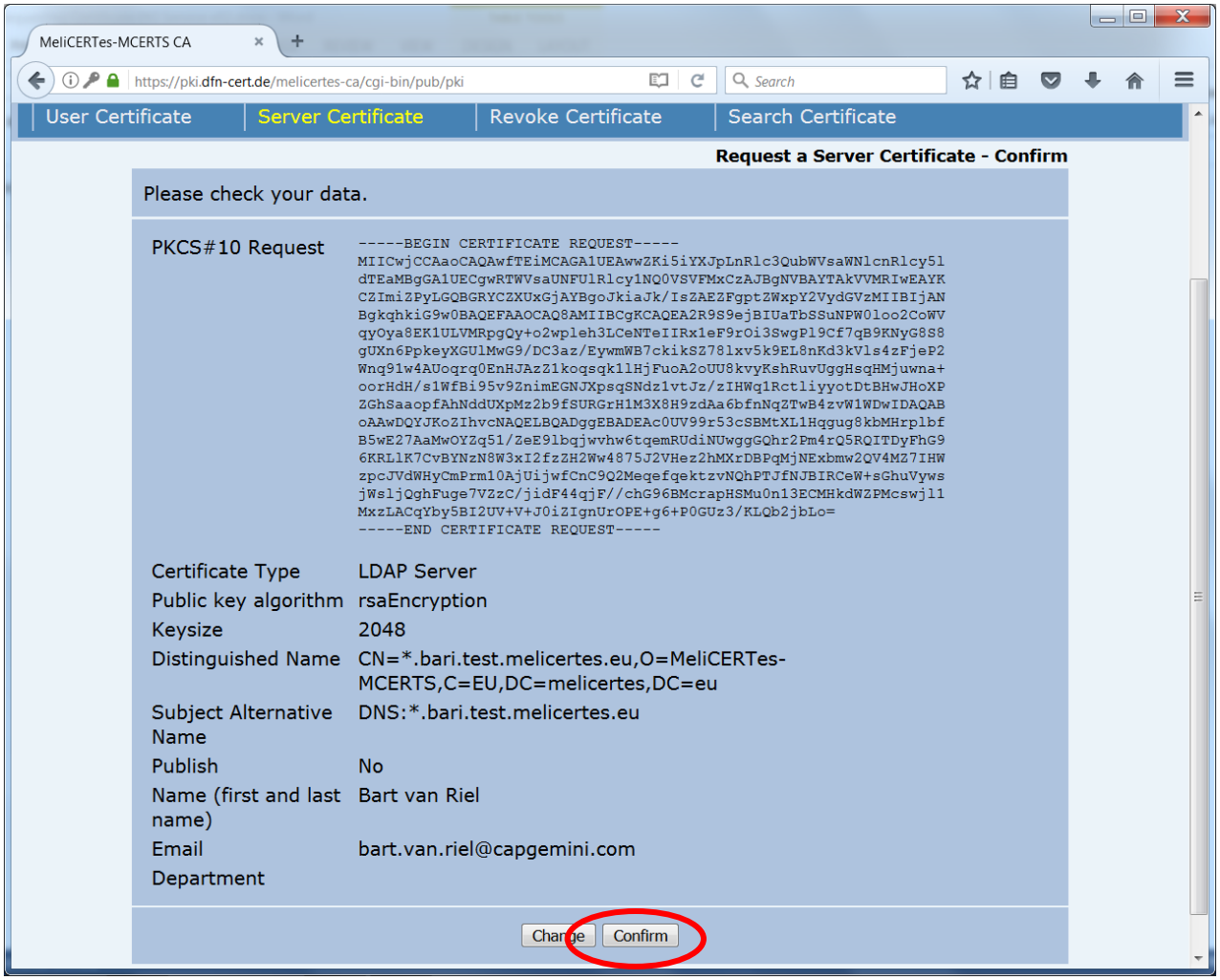
2. Choose “LDAP Server” as the profile (this will ensure you get a certificate which can be used both for mutual service authentication and for server-side encryption within your installation later on).

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 and will be needed to work with the certificate later on.

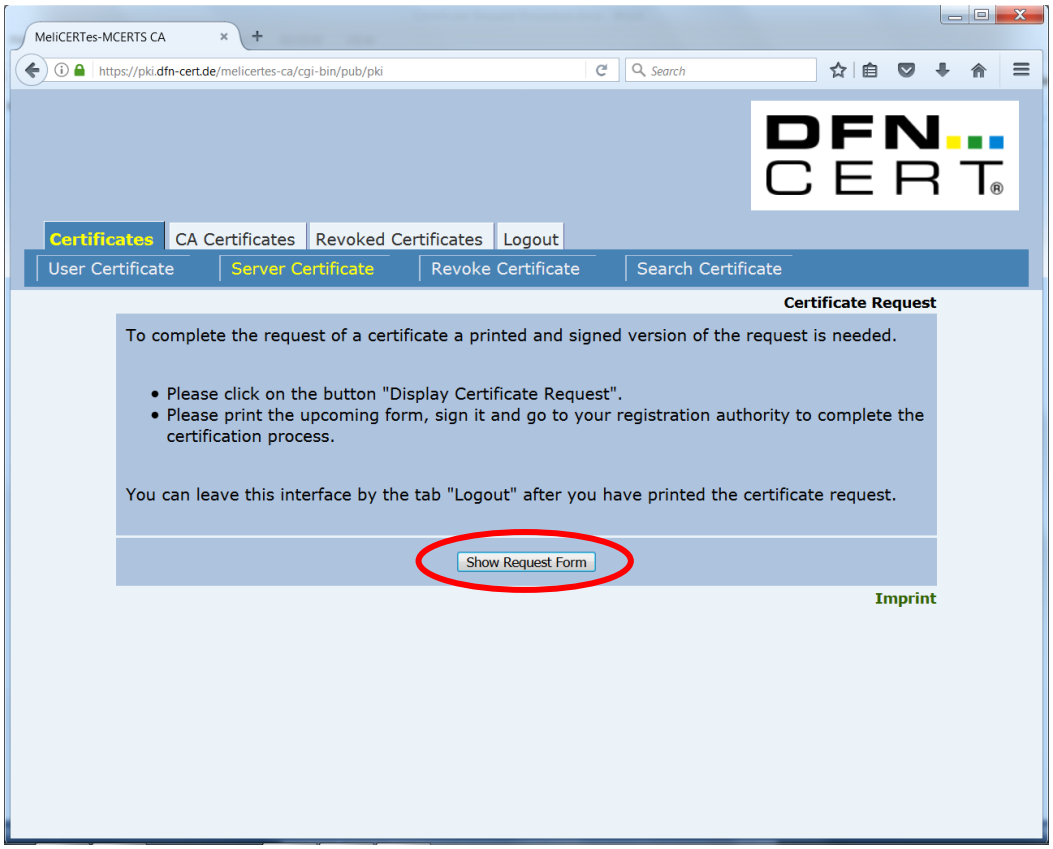
5. Click “Continue”.

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



Validate all of the information. If anything is incorrect, then click “Change” and you will be taken back to the “Request a Server Certificate” Screen. Otherwise click on “Confirm” to continue.

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 Central Trust Circle Administrator at trust-central@melicertes.eu with the subject: “Server Certificate Request - <cspId>”.

Signing by PGP is strongly encouraged. The GPG/PGP public key of the Central Trust Circle Administrator is available from: https://portal.csirt.enisa.europa.eu.

GPG/PGP fingerprint: 9291 C23F 595D 978D 2924 CE9D A367 37B3 9B85 DE44

3.4 Receive the signed certificate

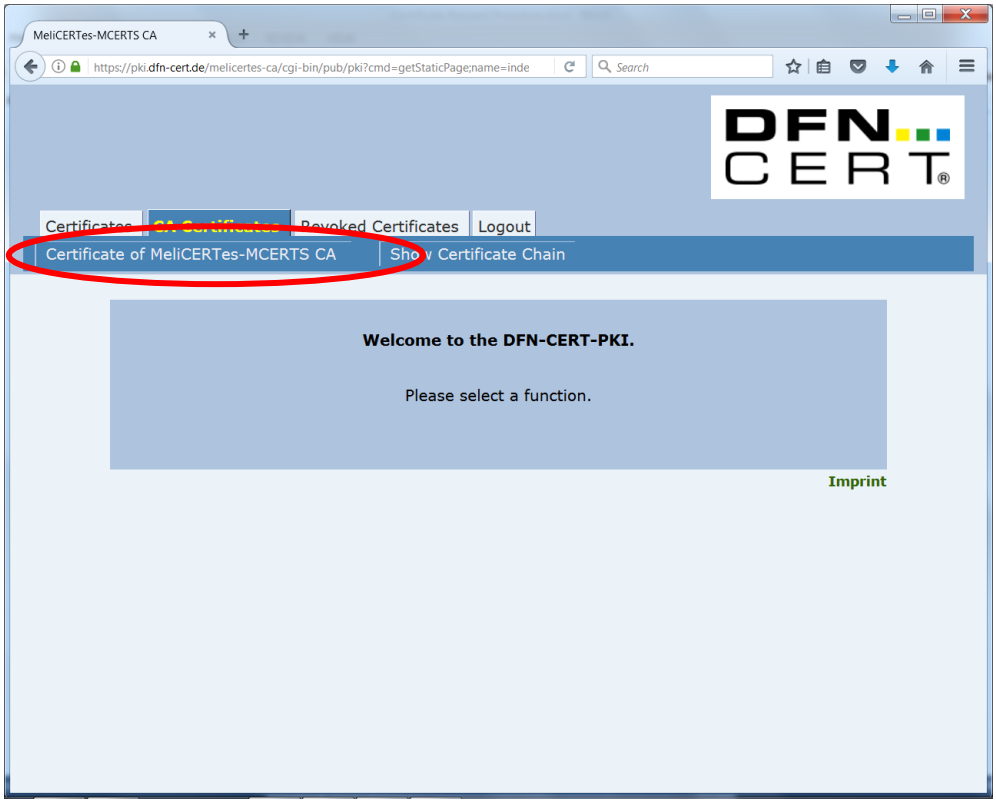
After the certificate request has been approved by the RA, you will receive an email containing the certificate as attachment (in the form of a *.pem file). Store the certificate as desired.

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

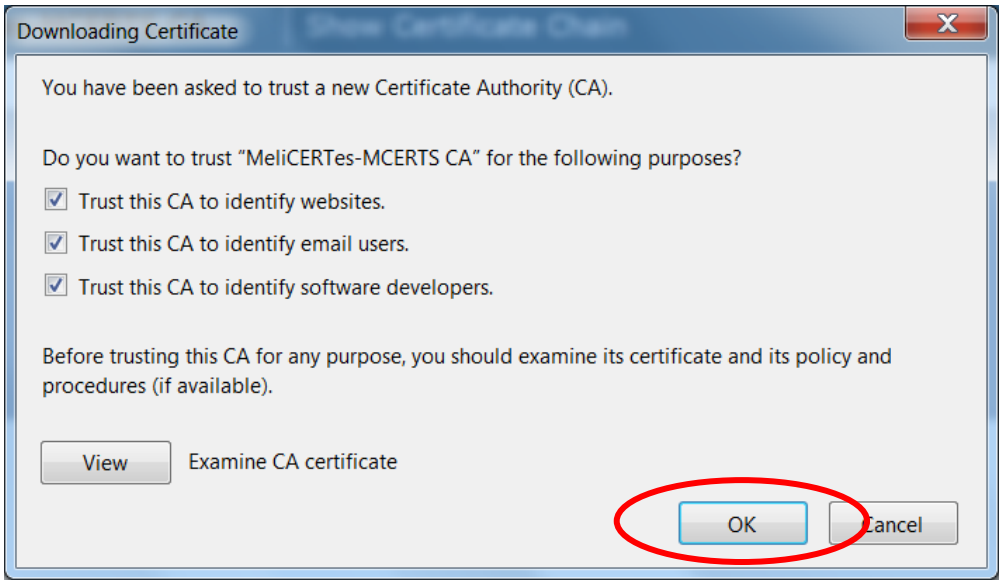
3.5 Download the Intermediate Root CA certificate

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

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



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



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

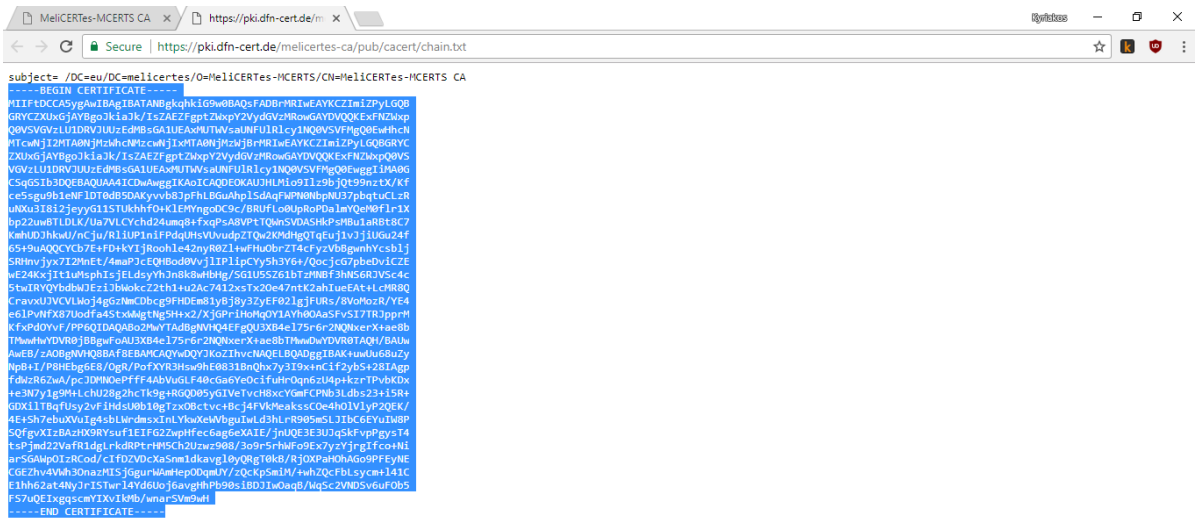
For Firefox, perform the following steps:

- 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 be needing this file for the installation.



3.7 Prepare your certificates for installation

During installation you will need the following 3 files

1. The private key that you created in section 3.2. File extension “.key”. File name “Private SSL Key.key”.

2. The signed SSL certificate that you got in section 3.4. File extension ".crt". File name "Signed SSL Certificate.crt".
3. The CA Bundle that you created in section 3.6. File extension ".crt". File name "CA Bundle.crt".

4 Initial configuration

4.1 Initial configuration screen

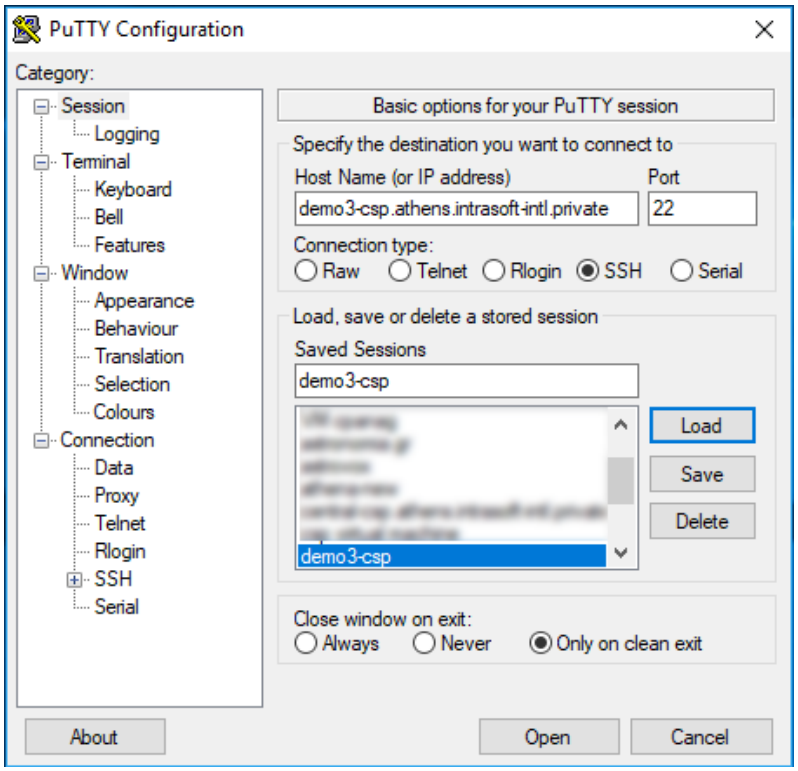
An Open Virtualization Archive (OVA file) has been distributed and contains the original VM for this project. Please do note that it is versioned and you may need to update it if instructed. This OVA has settings for memory and CPUs that need to be adjusted, according to specifications previously communicated. It is advised that the administrator importing the file proceeds with such modifications prior to 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

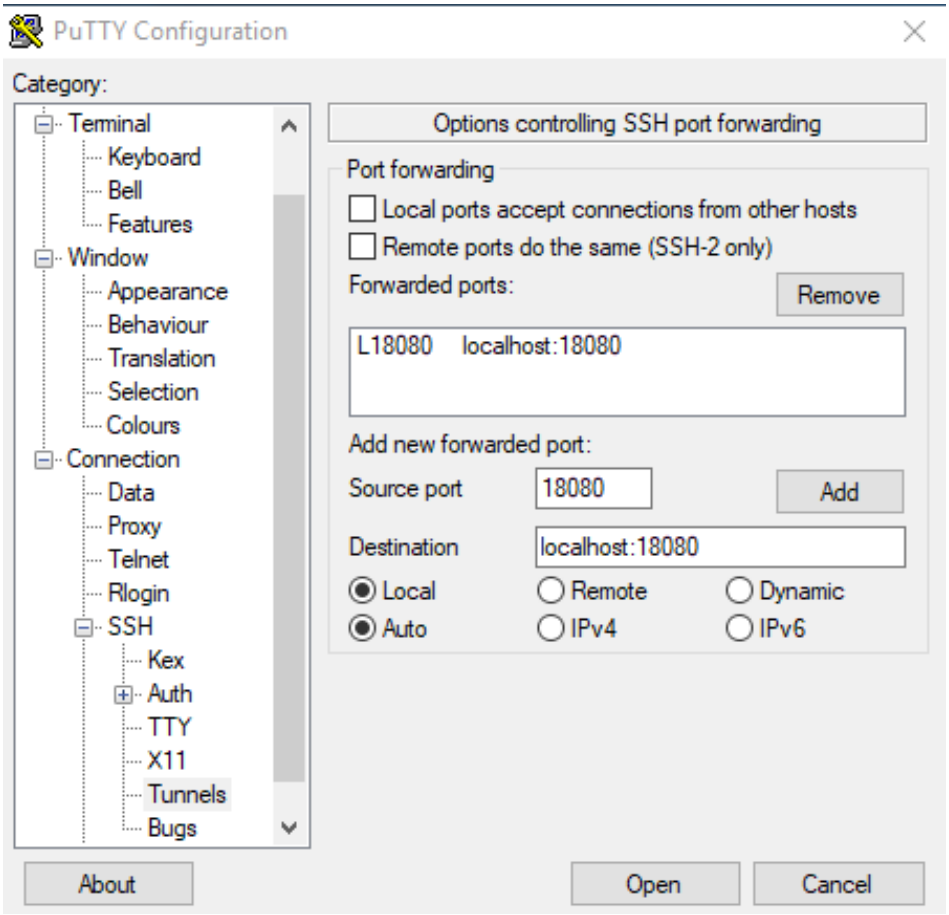
When the guest machine boots, the user should connect via SSH to the guest machine while at the same time creating an SSH tunnel between the guest machine and their computer. This is necessary so the user web browser can access the GUI installation.

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.

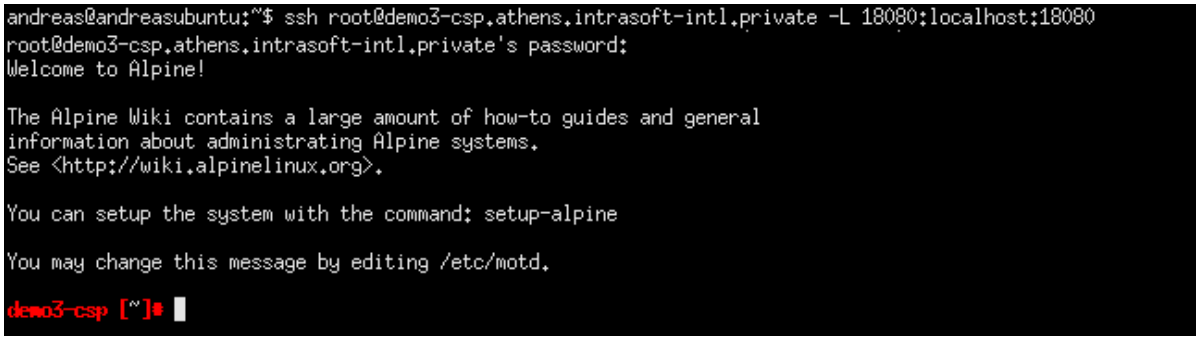


In the case of using a Linux terminal, the SSH connection with the tunnel can be created using the following command format:

```
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.

After successful login, the user can now use the graphical CSP installation control application tool through their local computer web browser by entering the following URL: http://127.0.0.1:18080 (see chapter 5).

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.

5 Installation

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 5.5 - Troubleshooting the connection tunnel to the VM, in case you encounter issues in accessing the aforementioned URL.

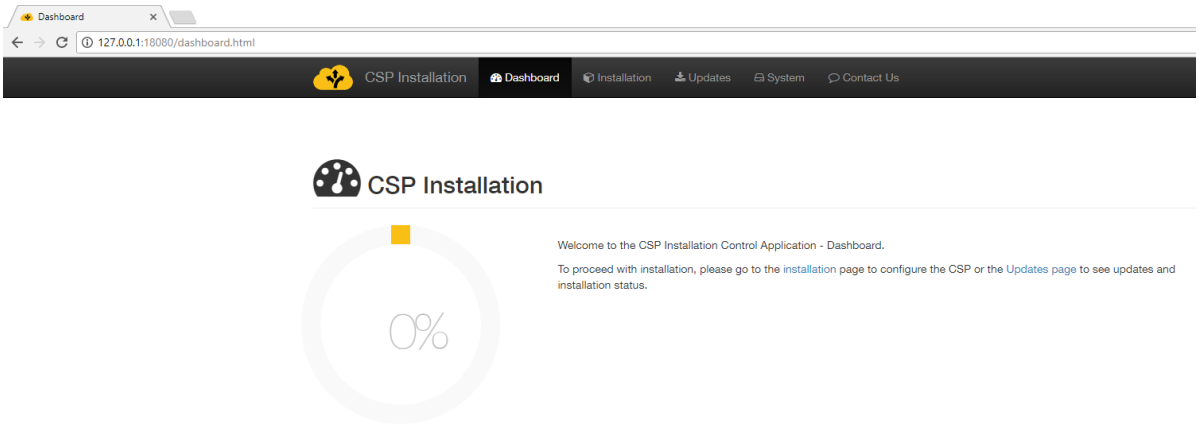
First time installation should display a progress of 0%. The menu bar at the top of the page displays the basic operations of the application which are “Dashboard”, “Installation”, “Updates” and “System”. These options should be selected at the order instructed in this manual. A brief description of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

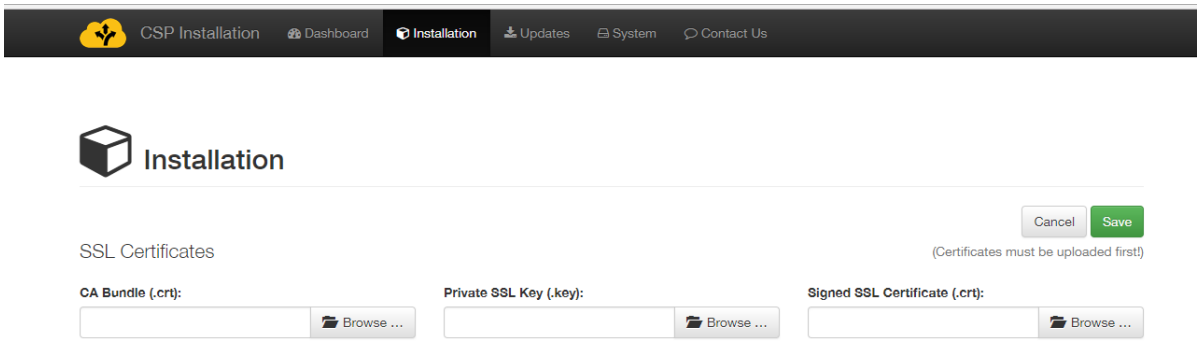
“System”: Starts and stops the system and displays the status of all services.



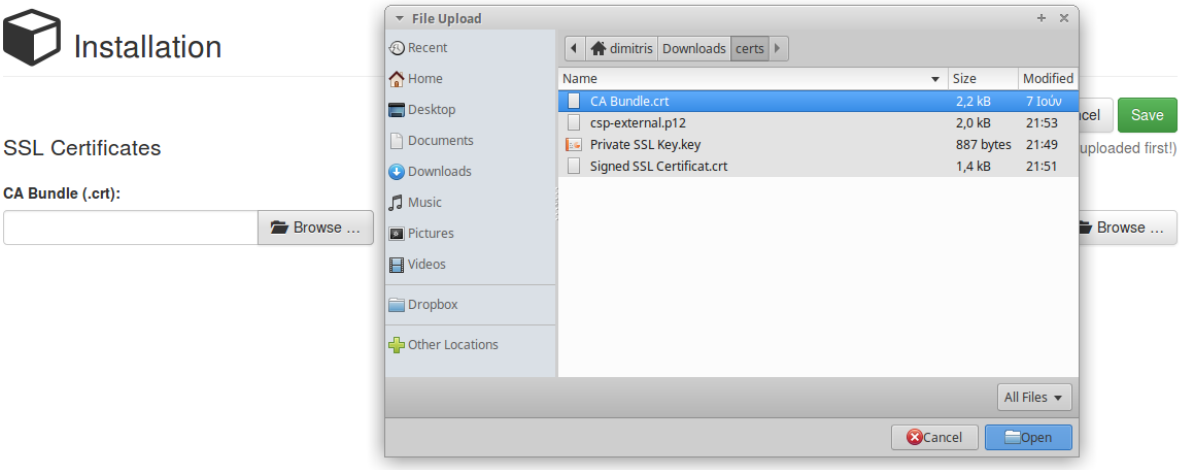
The first time the CSP installation control application is accessed, the user should proceed to the **Installation** page in order to perform the initial configuration.

5.1 Installation of certificates

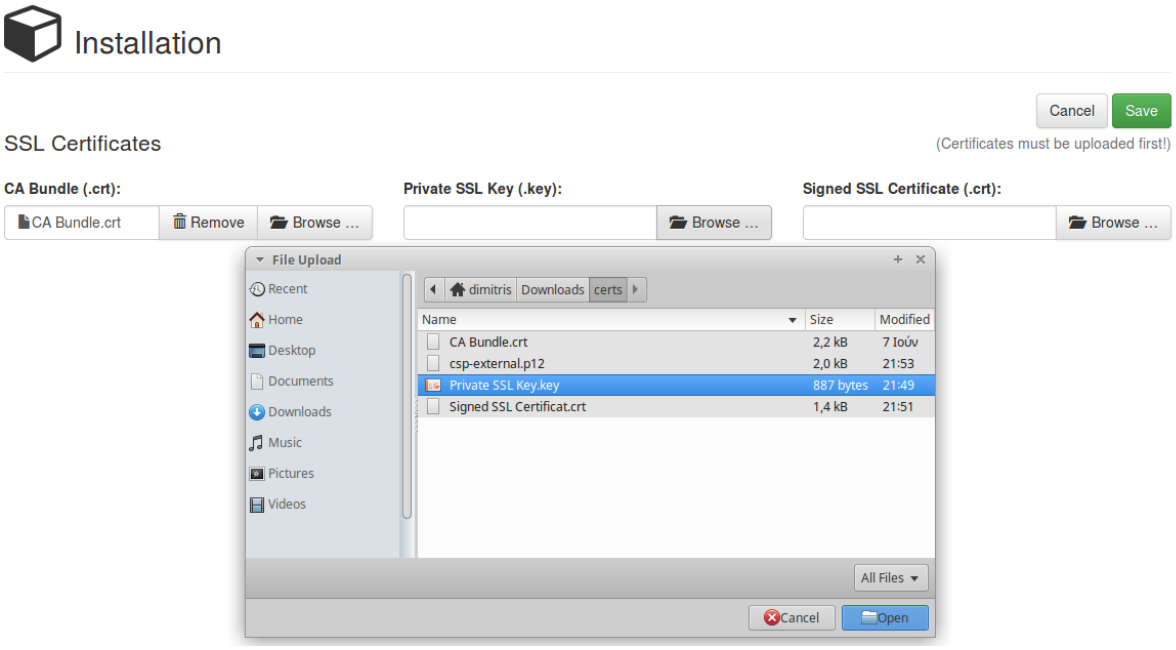
Completing the first installation step requires that the user has saved all the necessary certificates and key files to his/her computer as mentioned in the previous sections of this manual. The necessary certificates are the CA bundle, the Private SSL Key and the Signed SSL certificate. The file names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



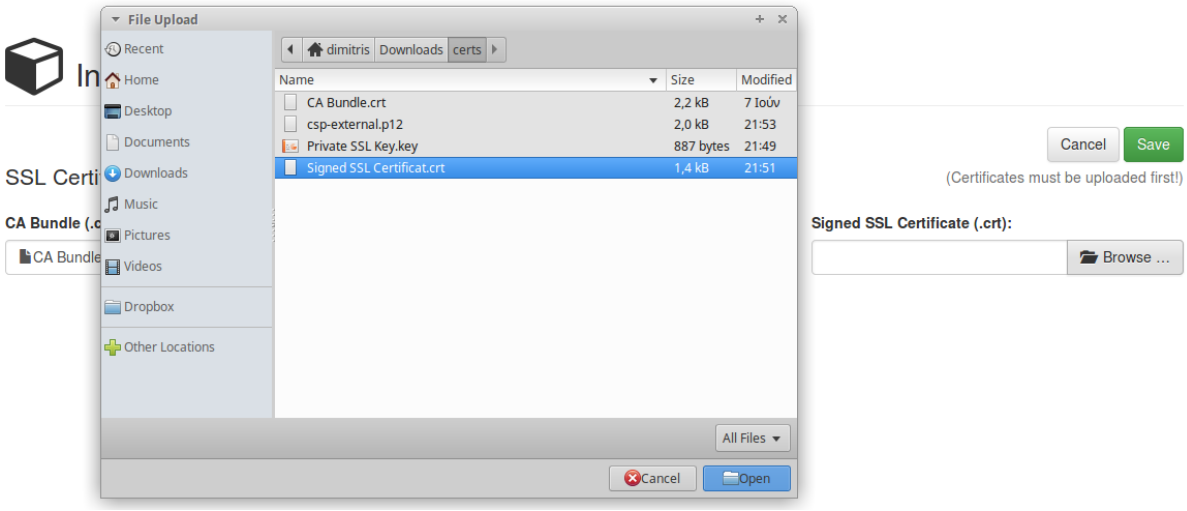
The user must browse and select the files in the following order. First, the user should click the “Browse” button for the CA Bundle certificate and select the “CA Bundle.crt” file. Once selected, the name of the file will appear in the box.



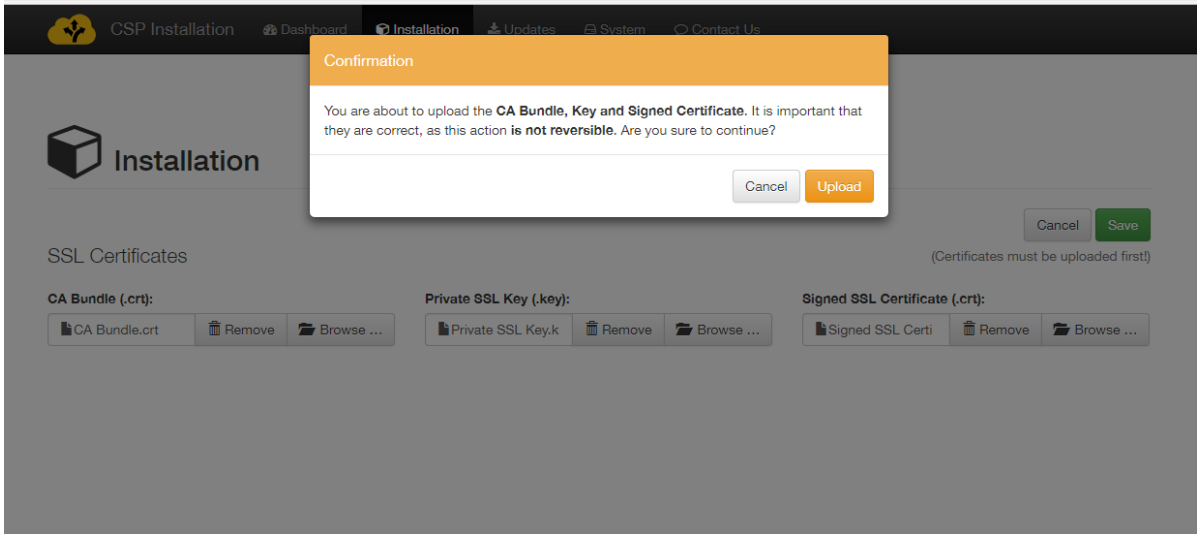
Then the user should click the “Browse” button of the Private SSL Key and select the “Private SSL Key.key” file. Once selected, the name of the file will also appear in the box.



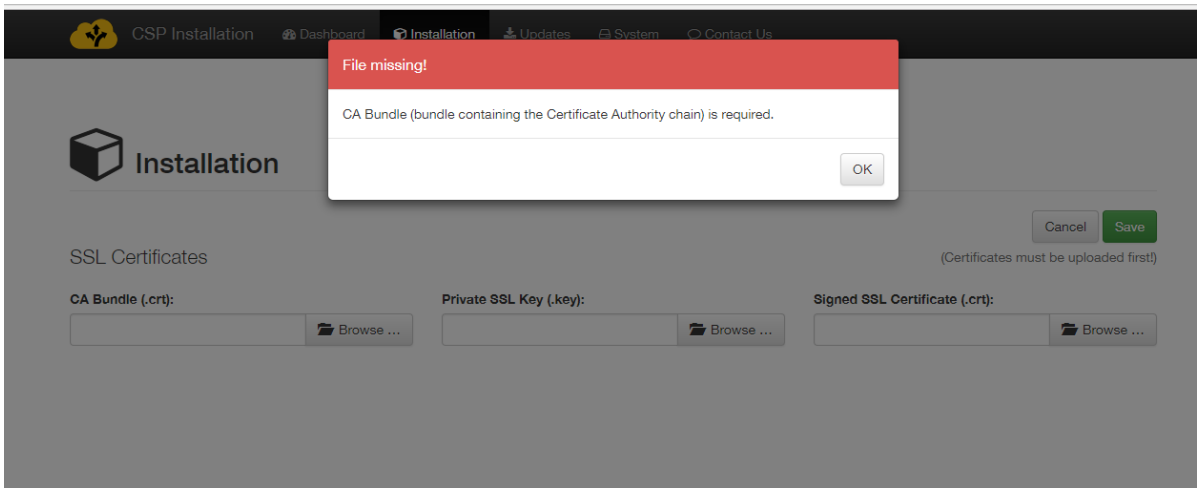
Finally, the user should click the third “Browse” button of the Signed SSL Certificate and select the “Signed SSL Certificate.crt” file. Once selected, the name of the file will also appear in the box.



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

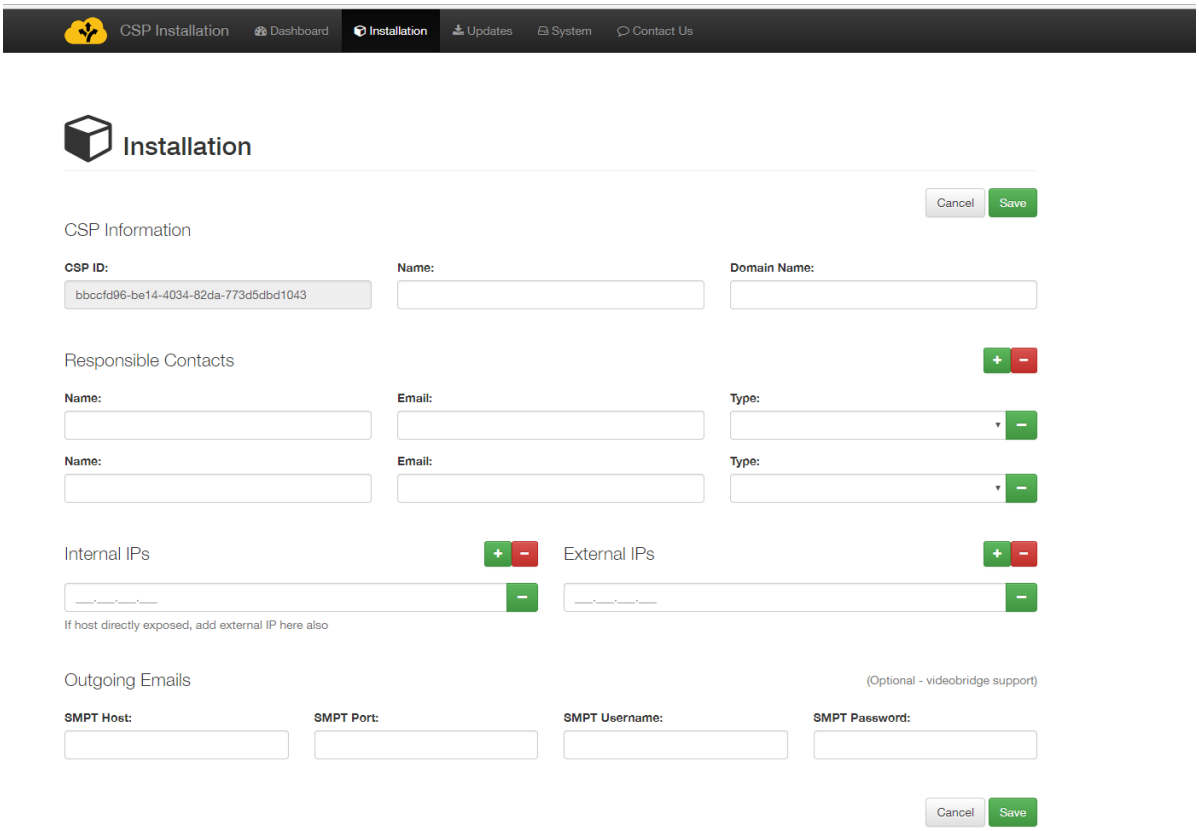


Incomplete submittal of the certificates is not possible. The system will alert the user that certificate files are missing if the Save button is clicked and not all three files have been selected.

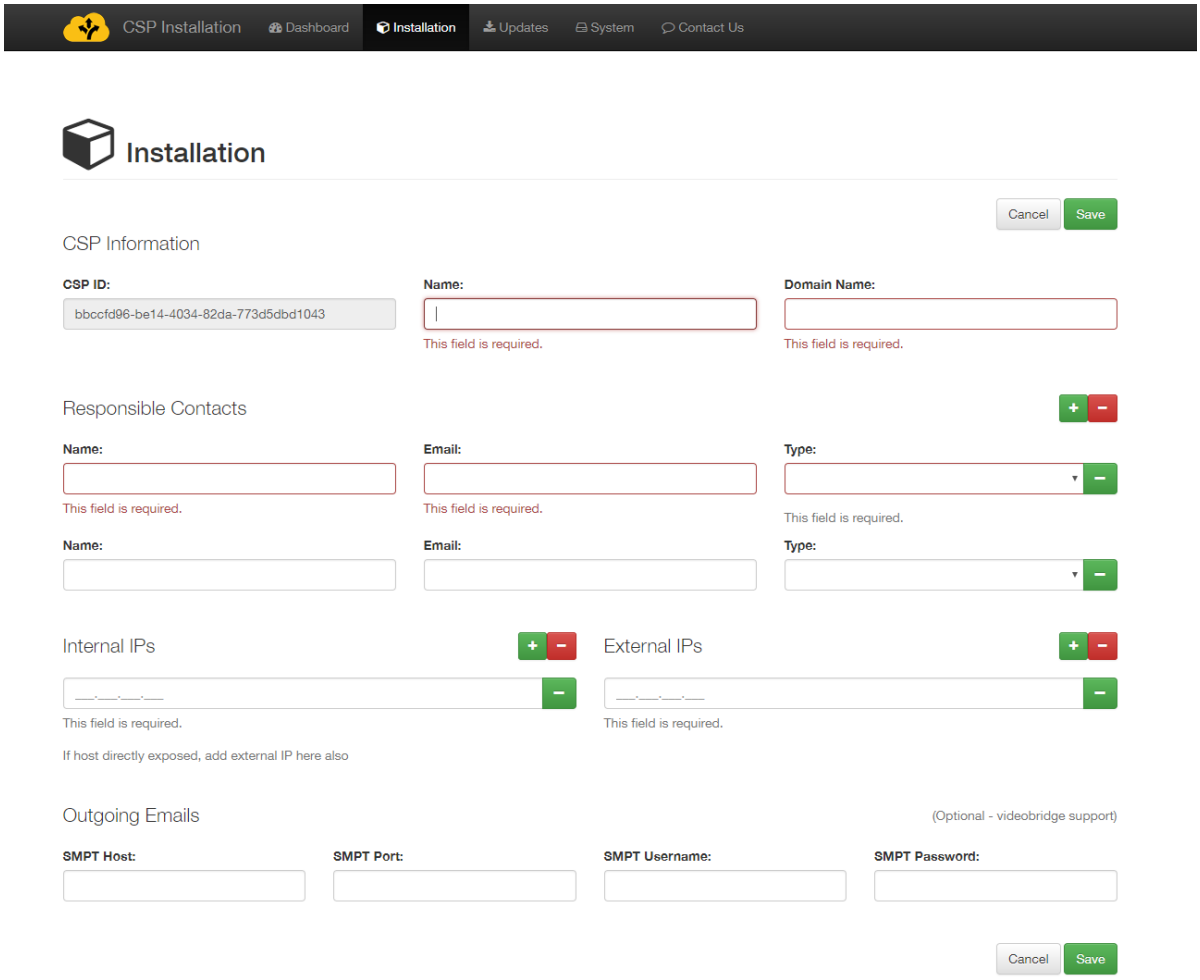


5.2 CSP Instance registration

In the Registration page, the user must enter the basic CSP information that includes CSP name, domain, responsible contacts info and internal/external IP's.



This form is protected against incomplete submission. A warning will be displayed if the Save button is clicked without completing all the required fields.



The fields of this form should be completed as follows:

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

Name: The assigned CSP ID (e.g. “csirt-gr”)

Domain Name: The domain as determined by the application procedure and environment (e.g. prod.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. For each contact, the full name and email of the person listed as contact are needed as well as the type (e.g. Tech Admin). More contacts can be input by adding lines to the form using the green + button.

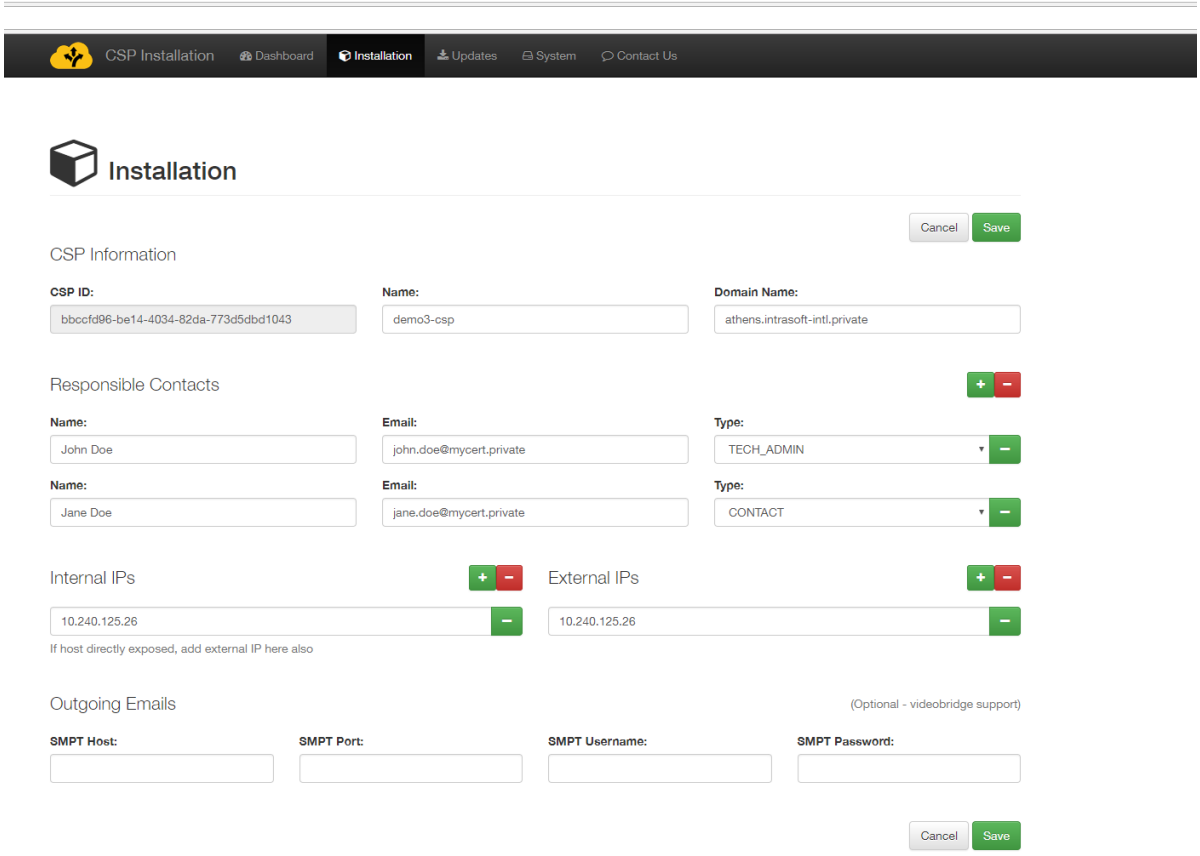
Internal/External IPs: The internal and external IP’s of the guest machine need to be inserted. Please note the following details:

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 must 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.

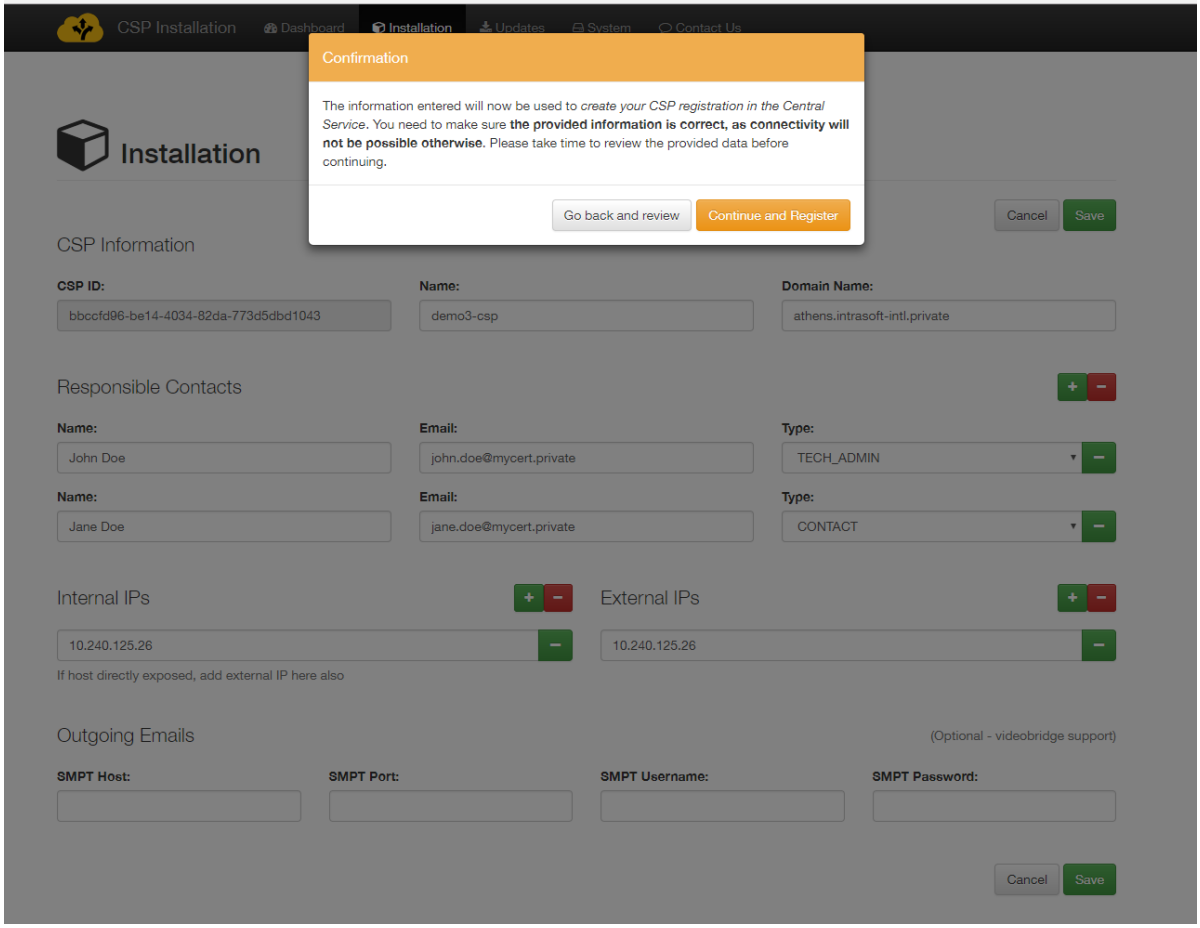
All the above fields are **mandatory**.

The final video bridge support section of the form is optional and there are no warnings if it is not completed. This section consists of an SMTP server configuration options, namely SMTP host, port, username and 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. Note that in the "Port" field, only 587 (Secure SMTP) port is applicable.

Here is a sample filled in form:



The form is submitted by clicking the green Save button.



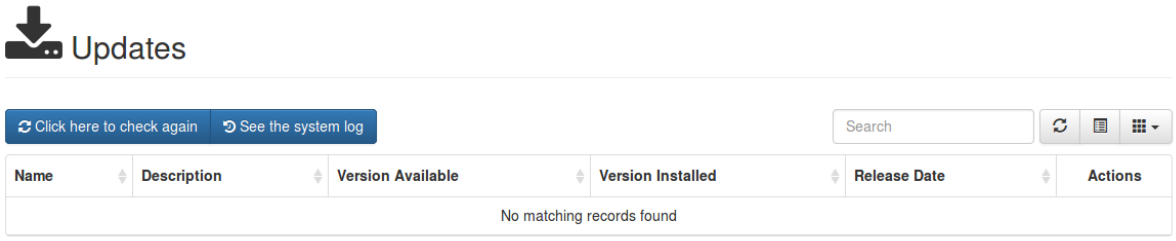
The system prompts for confirmation prior to final submission. It is important that all information entered is correct since connectivity will not be possible if any misspellings exist in the CSP name, domain and IPs. After pressing the "Continue and Register" button, the system will redirect to the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

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

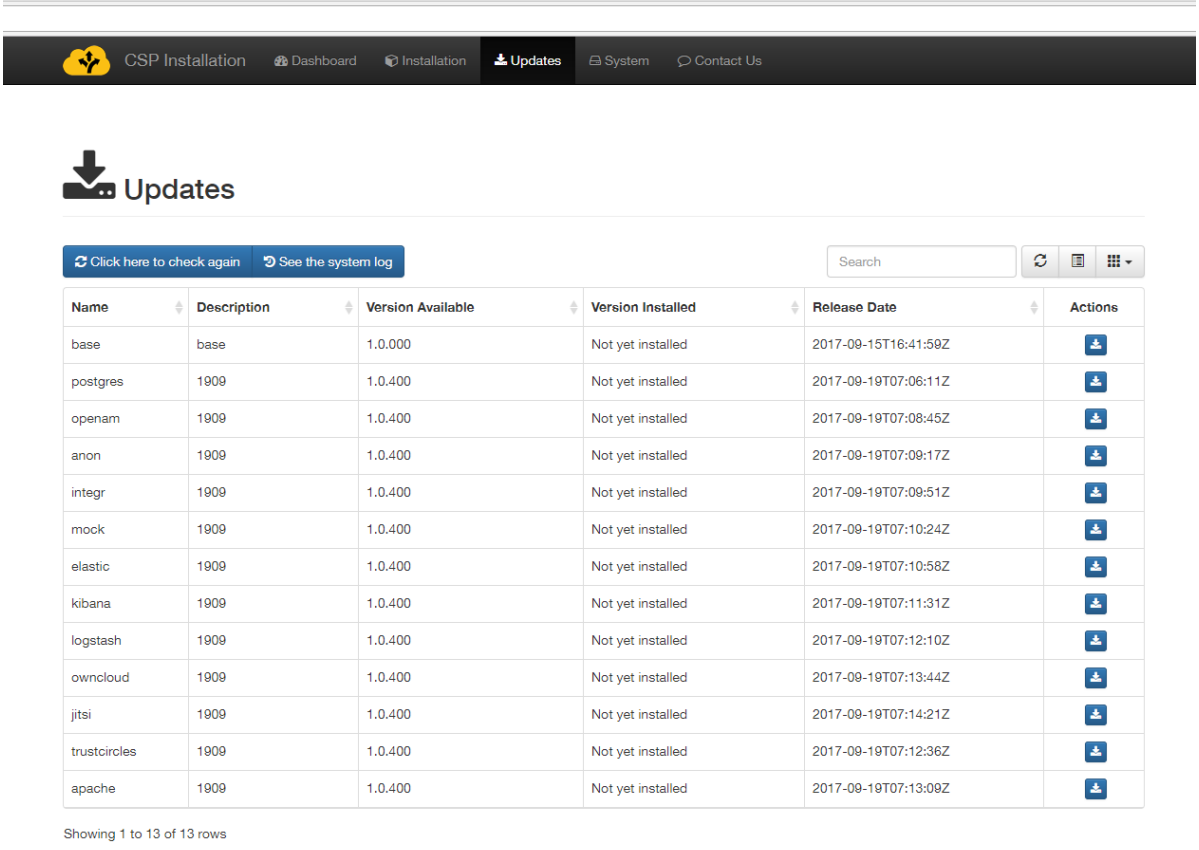
5.3 Download of system updates

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

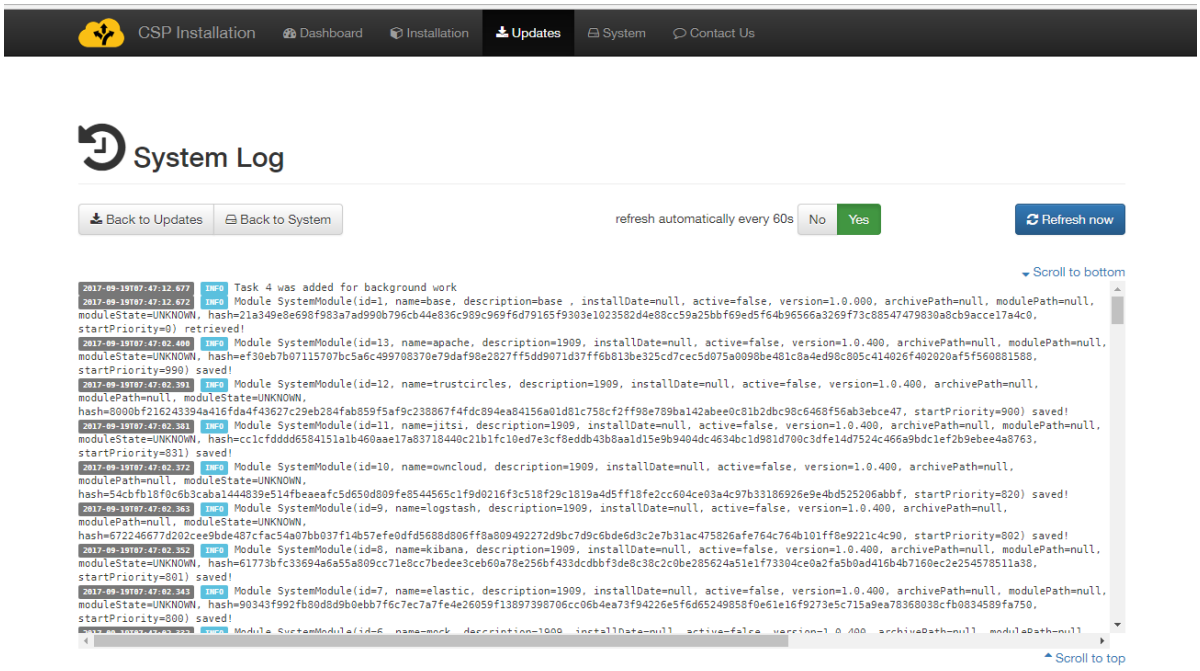
In an existing installation, updates may appear on the "Updates" page periodically. This page should be checked once a week during a scheduled maintenance window.



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 Update" button, and page refresh (for updated log entries) happens every 60 seconds or if the "Refresh now" button is pressed.

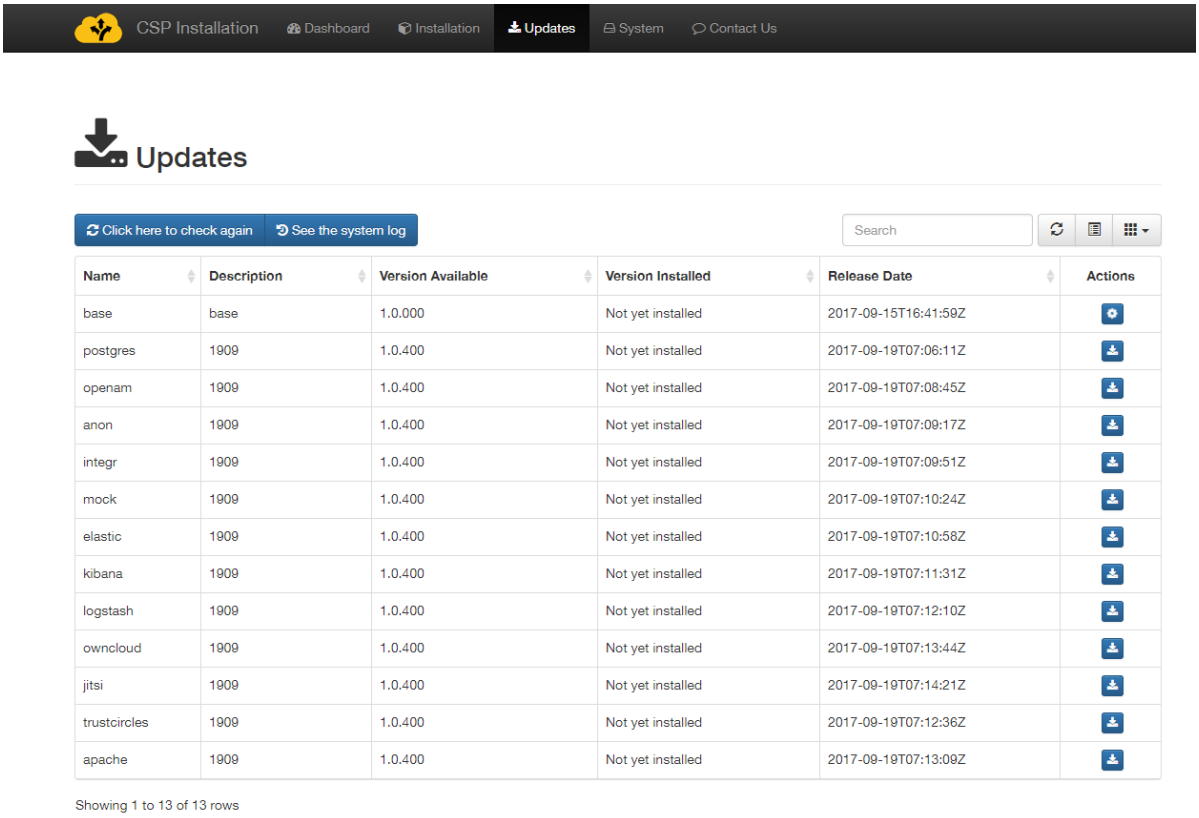
An indicative list of log entry extracts with explanations follows:

- "Task X was added for background work" – the system has scheduled an operation to happen in the background. Expect further information after 5-8 seconds.
- "BackgroundTaskResult(success=true, errorCode=0, moduleName=<variable>)" – indicates a successfully executed operation
- "BackgroundTaskResult(success=false, errorCode=<variable>, moduleName=<variable>)" – indicates a failed operation. The logs should be returned to the support team for further investigation[2].

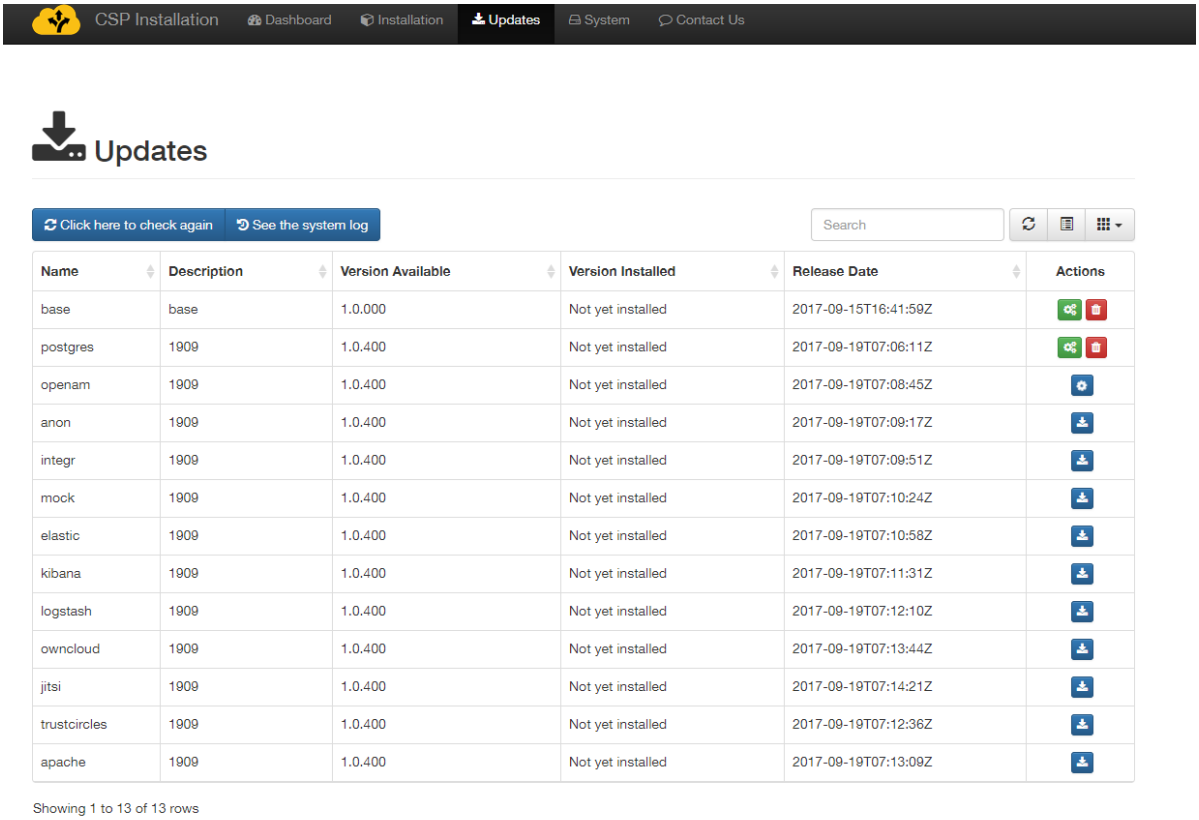
Note that updates that are currently downloading will present an animated gear icon in the "Actions" column.

2

Extraction of logs via the web UI is possible: Click within the log window, press "Ctrl + A" or "Cmd + A" 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 support.



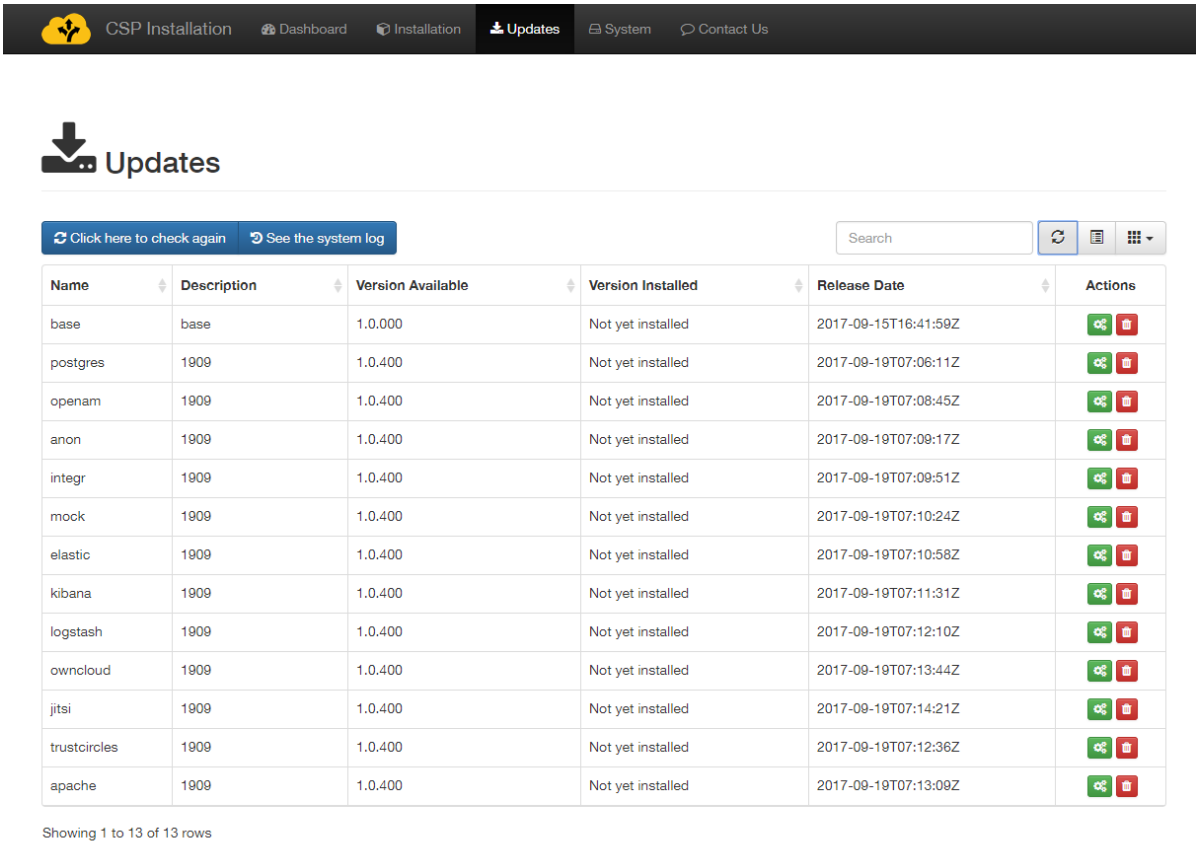
The user may request more downloads without waiting for the previous ones to finish as all download requests are added as background tasks. Completed downloads will present two new icons in the Action page, the green Install icon and the red delete icon. Note that although possible, clicking the download 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.



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

Showing 1 to 13 of 13 rows

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



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

5.4 Modules installation

After downloading all the updates, the components can be installed. By clicking the green Install icon for each image, the user must 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 he/she can monitor the 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 can be monitored on the system log page. The user should expect a log entry with “BackgroundTaskResult” indicating “success=true”.

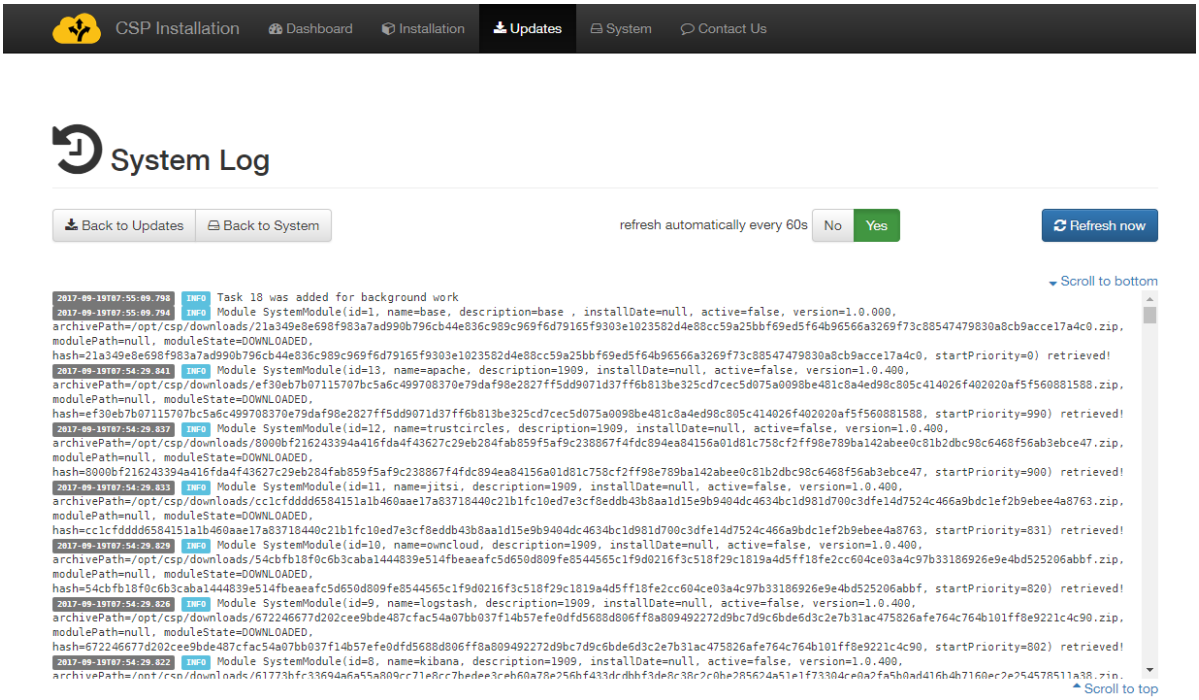
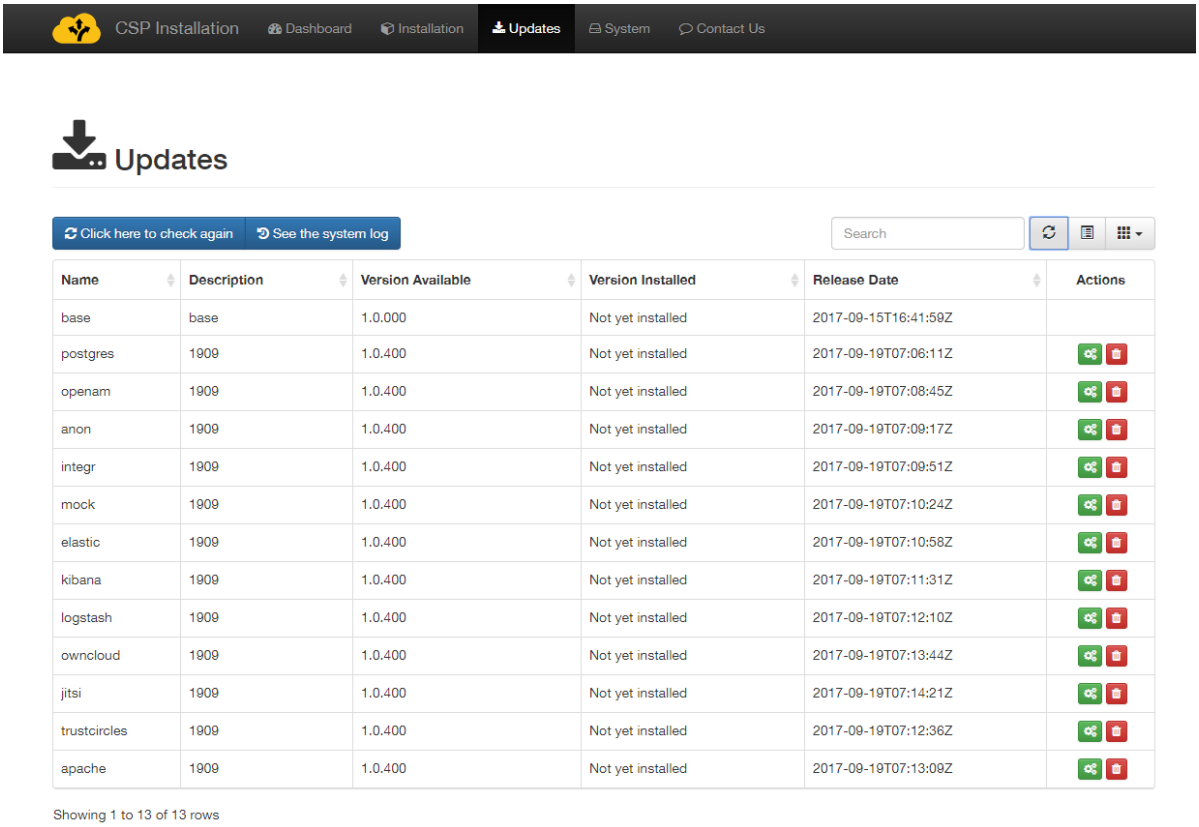


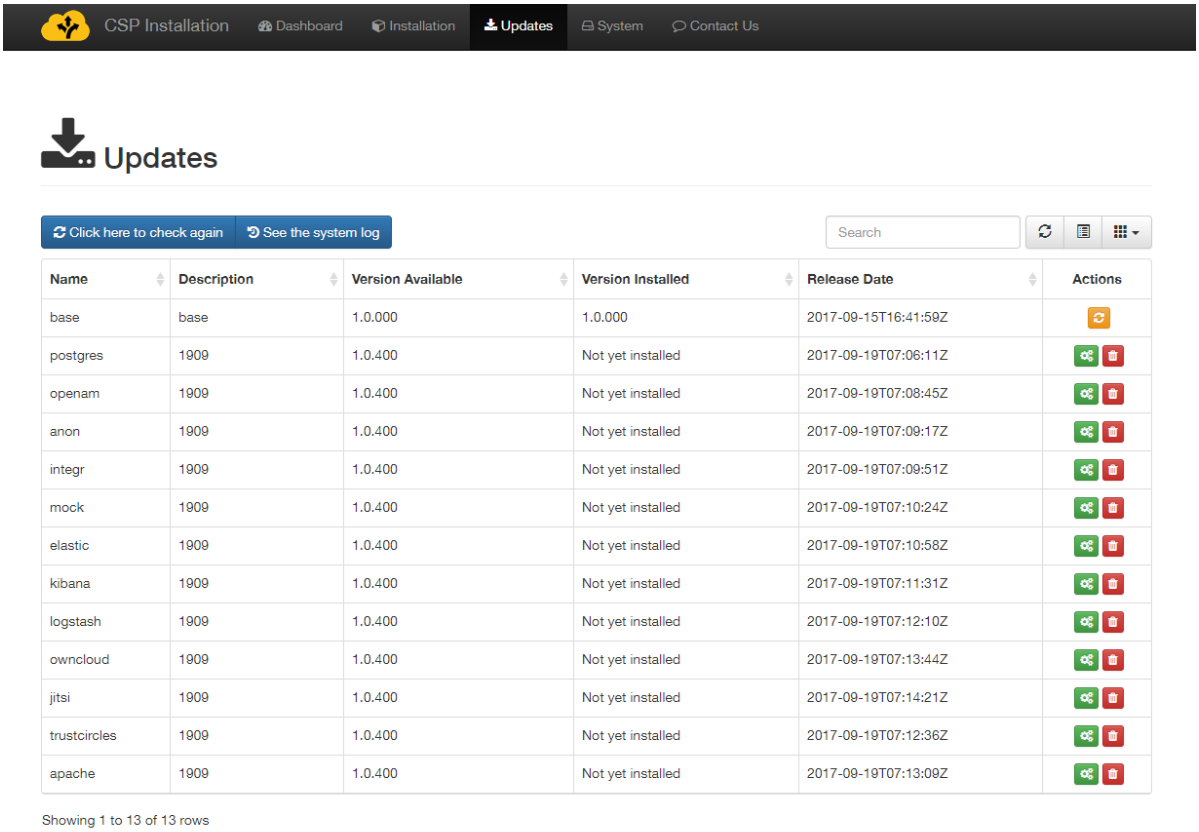
Image installations must **NOT** be performed concurrently. The user must wait until the installation of each image completes successfully before proceeding to the next image installation. Please note that while an image installation is taking place, nothing appears in the Action column for the module being installed, as shown in the figure below.



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

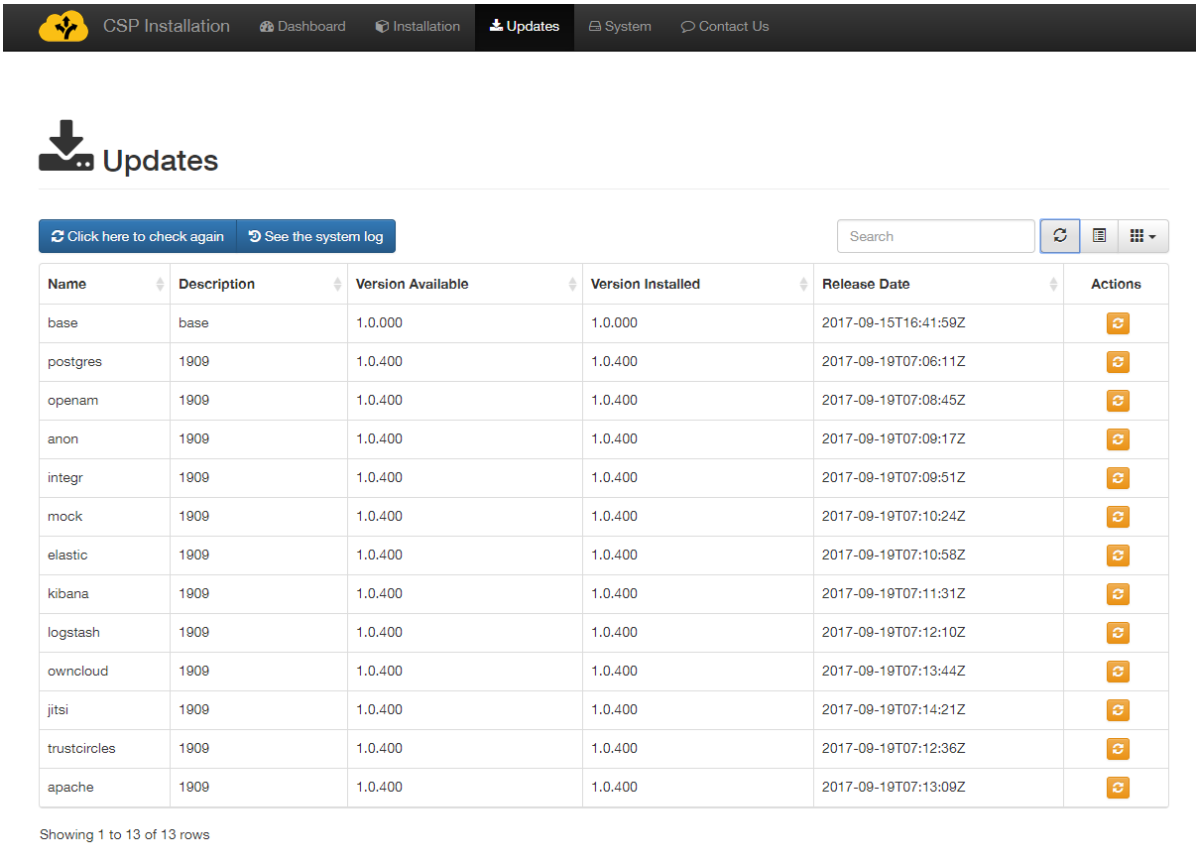
When an image installation is finished, an orange Re-install icon appears in the Actions column. This should only be selected if specific circumstances mandate re-installation of an image, or if explicitly requested by the support team.



Name	Description	Version Available	Version Installed	Release Date	Actions
base	base	1.0.000	1.0.000	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

It is highly recommended that the user proceeds with the installation of the images in the order presented in the table. After successful installation of all the images, the Updates page should appear as follows (all modules have been installed and only orange icons are visible).



Name	Description	Version Available	Version Installed	Release Date	Actions
base	base	1.0.000	1.0.000	2017-09-15T16:41:59Z	
postgres	1909	1.0.400	1.0.400	2017-09-19T07:06:11Z	
openam	1909	1.0.400	1.0.400	2017-09-19T07:08:45Z	
anon	1909	1.0.400	1.0.400	2017-09-19T07:09:17Z	
integr	1909	1.0.400	1.0.400	2017-09-19T07:09:51Z	
mock	1909	1.0.400	1.0.400	2017-09-19T07:10:24Z	
elastic	1909	1.0.400	1.0.400	2017-09-19T07:10:58Z	
kibana	1909	1.0.400	1.0.400	2017-09-19T07:11:31Z	
logstash	1909	1.0.400	1.0.400	2017-09-19T07:12:10Z	
owncloud	1909	1.0.400	1.0.400	2017-09-19T07:13:44Z	
jitsi	1909	1.0.400	1.0.400	2017-09-19T07:14:21Z	
trustcircles	1909	1.0.400	1.0.400	2017-09-19T07:12:36Z	
apache	1909	1.0.400	1.0.400	2017-09-19T07:13:09Z	

Showing 1 to 13 of 13 rows

All available images must be installed and only after the user reaches the above stage, with only orange re-install icons appearing in the Actions column, should the user proceed to the next step which is available in the System page.

5.5 Troubleshooting the connection tunnel to the VM

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

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

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

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

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

Additionally, you can 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
```

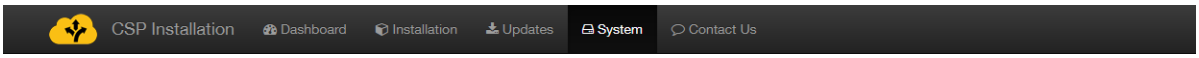
6 Managing CSP

6.1 Starting

The “System” page shows a current view of the registered system services 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.



System

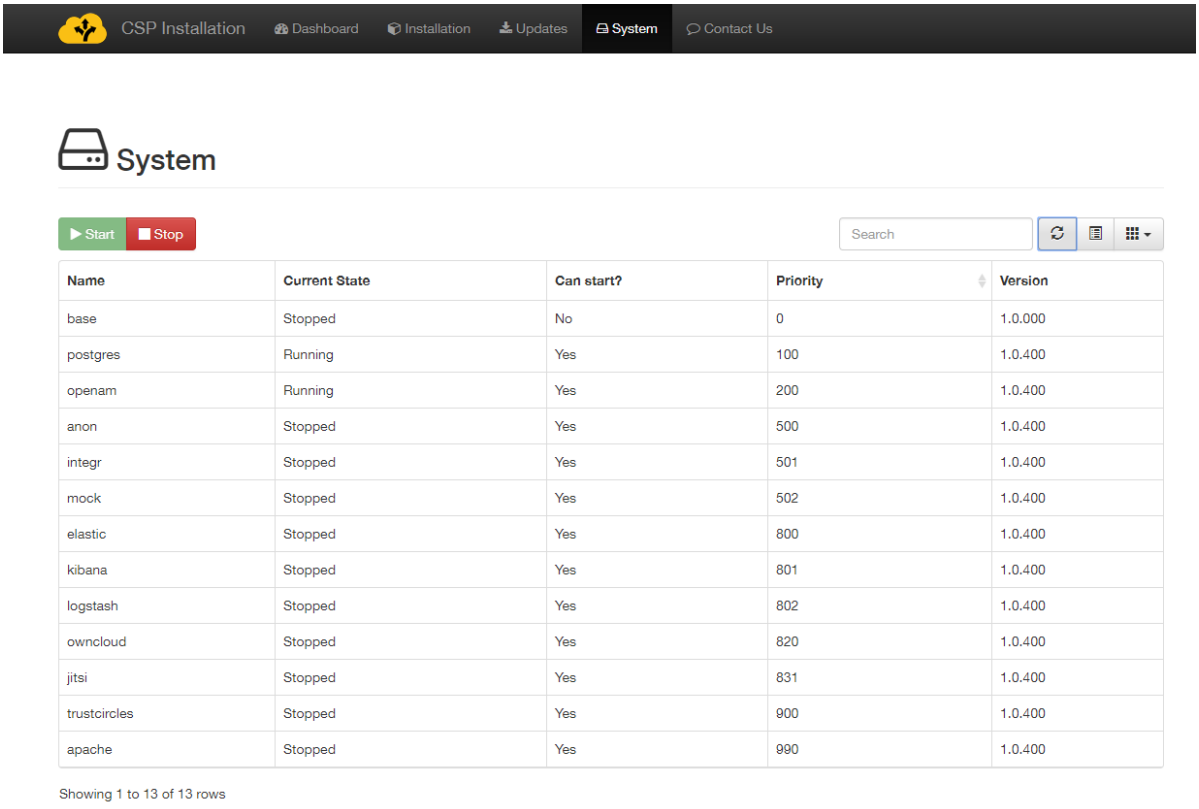
Start Stop Search

Name	Current State	Can start?	Priority	Version
base	Stopped	No	0	1.0.000
postgres	Stopped	Yes	100	1.0.400
openam	Stopped	Yes	200	1.0.400
anon	Stopped	Yes	500	1.0.400
integr	Stopped	Yes	501	1.0.400
mock	Stopped	Yes	502	1.0.400
elastic	Stopped	Yes	800	1.0.400
kibana	Stopped	Yes	801	1.0.400
logstash	Stopped	Yes	802	1.0.400
owncloud	Stopped	Yes	820	1.0.400
jitsi	Stopped	Yes	831	1.0.400
trustcircles	Stopped	Yes	900	1.0.400
apache	Stopped	Yes	990	1.0.400

Showing 1 to 13 of 13 rows

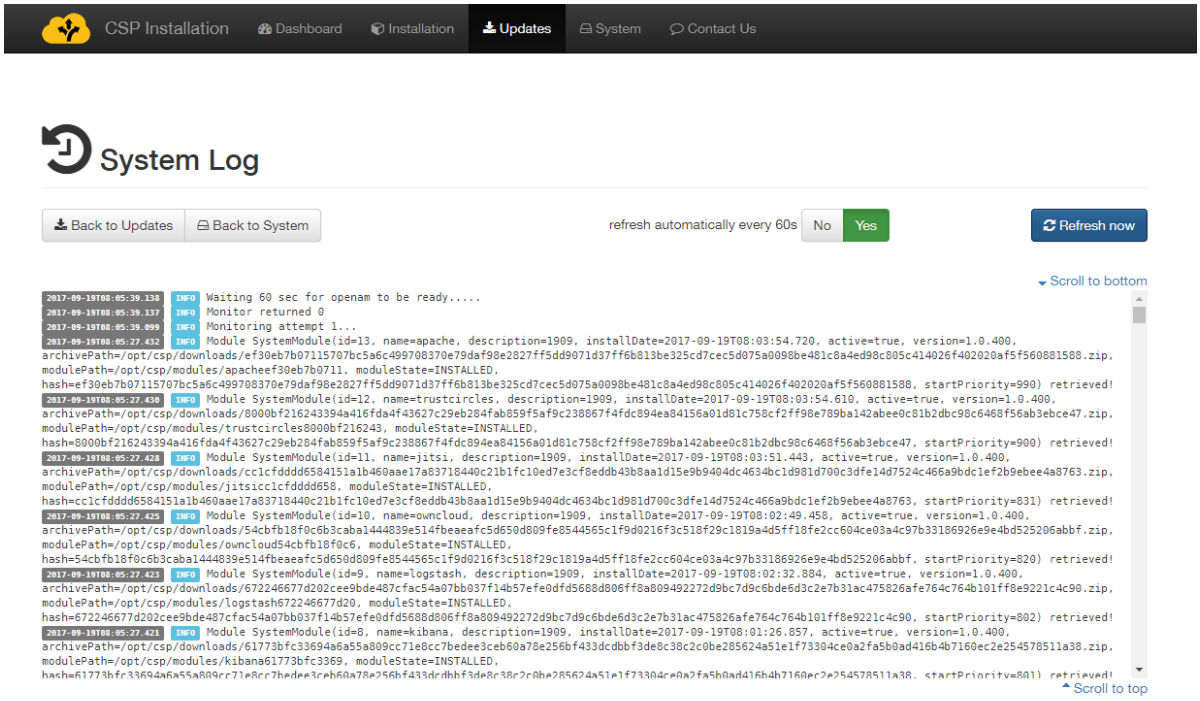
Current state should be Stopped for all modules the first time this page is accessed.

By clicking the Start button, System start begins. Use the “refresh” button to track progress.

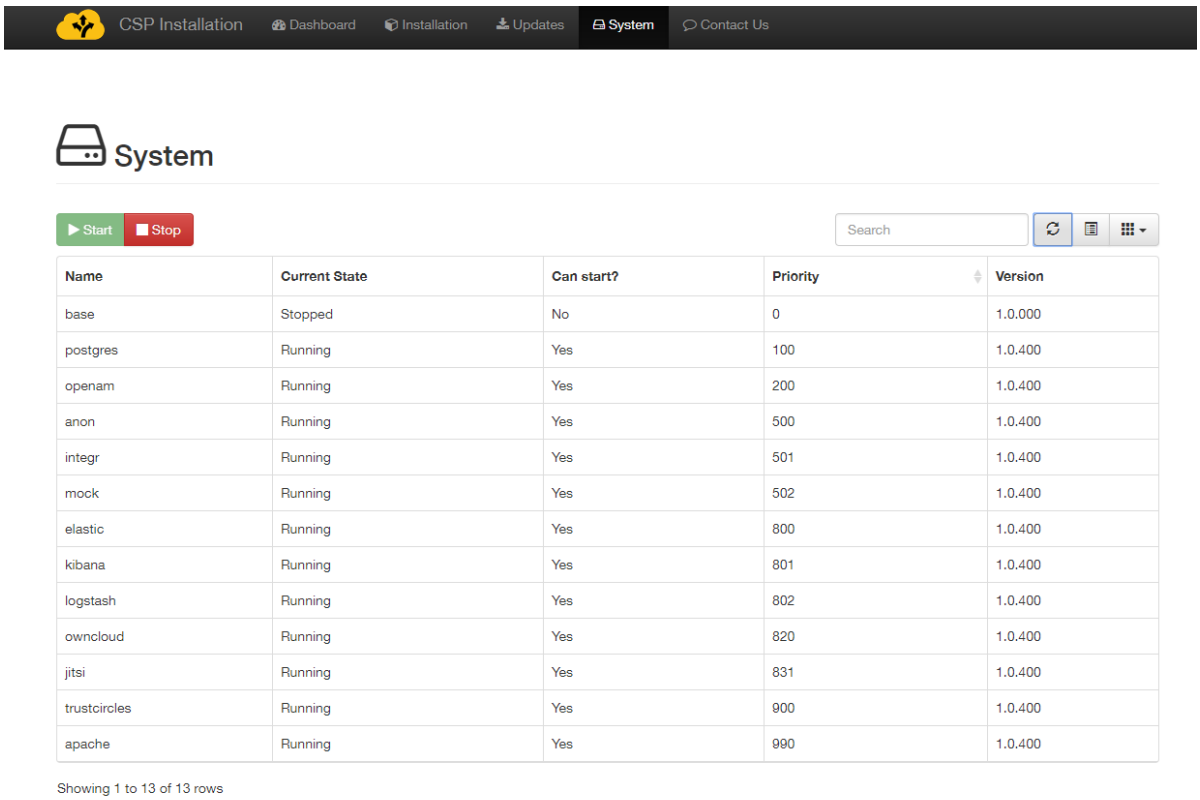


While the system is starting, the Start button is dimmed and only the Stop button is available. The Stop button can be pressed to initiate a System stop, **but not until the system has fully started** (all the modules, except for the base module, will be in the Running state). Note that due to the complexity of the services, the system Start and Stop are operations that may take a few minutes to complete. Especially system Start is normally expected to last more than 30 minutes to complete, so the user should be patient until all the modules report their Running state. During this wait period the user can only refresh the table to be informed about the system Start/Stop progress (note that system the Stop should not be executed until system has fully started). Modules that have been started will present a “Running” status in the Current State column. The system will start modules in the order displayed in the table.

An anytime the user can navigate to the System Log (available through the Updates page) to watch the system start log entries.



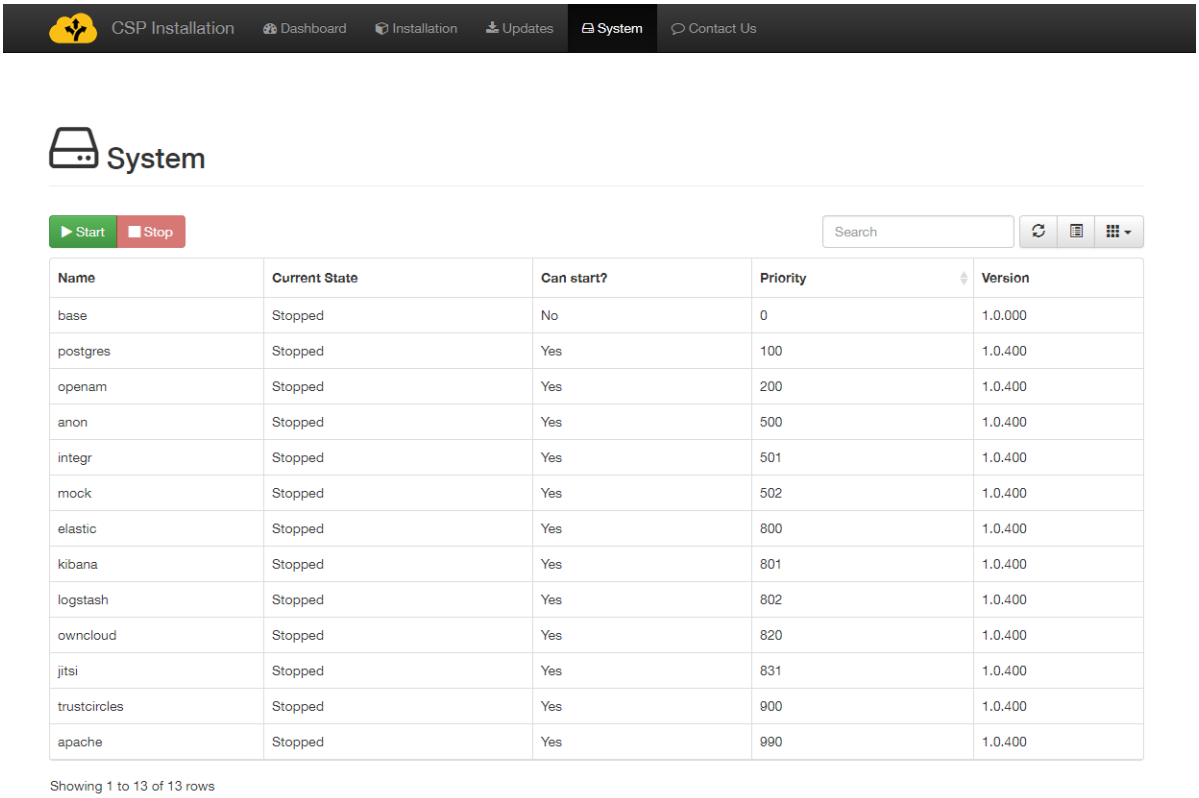
Once again, the user should wait until all the modules (except the base module) report a “Running” state. Depending on the performance of the system, the initial start of modules may take more than 30 minutes, due to initialization of security components. When the system has successfully started, the following should appear.



Please note 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 the applications.



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 was started via the console, the installer will not be updated on its status. Therefore that service will not be stopped when pressing the “Stop” button. If any services have been started manually, it is a good practice to check that all the services have been stopped correctly when you press the “Stop” button. This check can be done by running “docker ps” in the console.

7 Smoke-testing the Installation

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

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

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

The output should be similar to the screenshot below

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

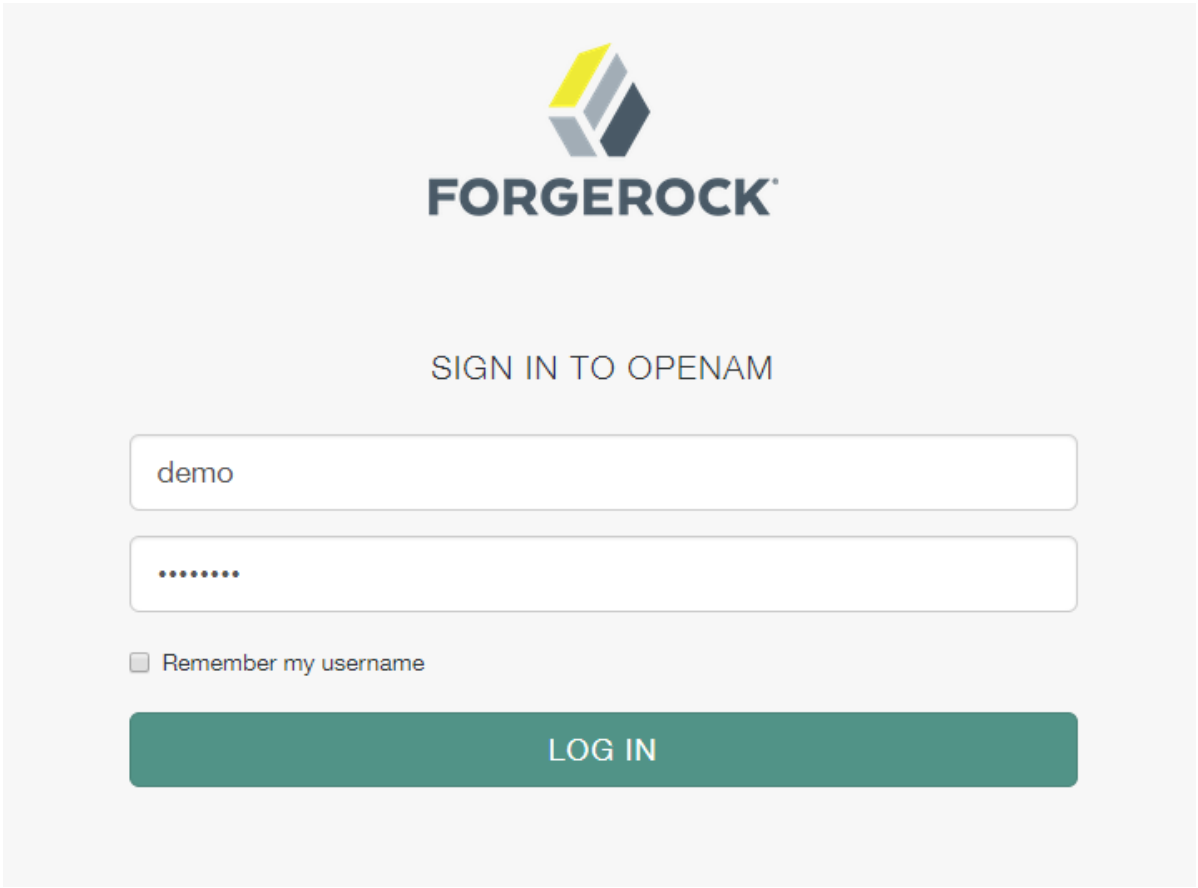
After making sure that **ALL** the docker containers are up and running, you should proceed to check if the application user interfaces are responding. Please see the URLs of web interfaces at the beginning of this manual.

7.1 Connecting via the “Single Sign-on” service

When the user tries to access any application through its web interface, the system will initially try to perform a certificate authentication. If no valid certificate is installed at the user client (or the user has cancelled 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 page will indicate that the certificate authentication for the user has failed; OpenAM will indicate that the traditional “username/password” option for login is still available, 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.

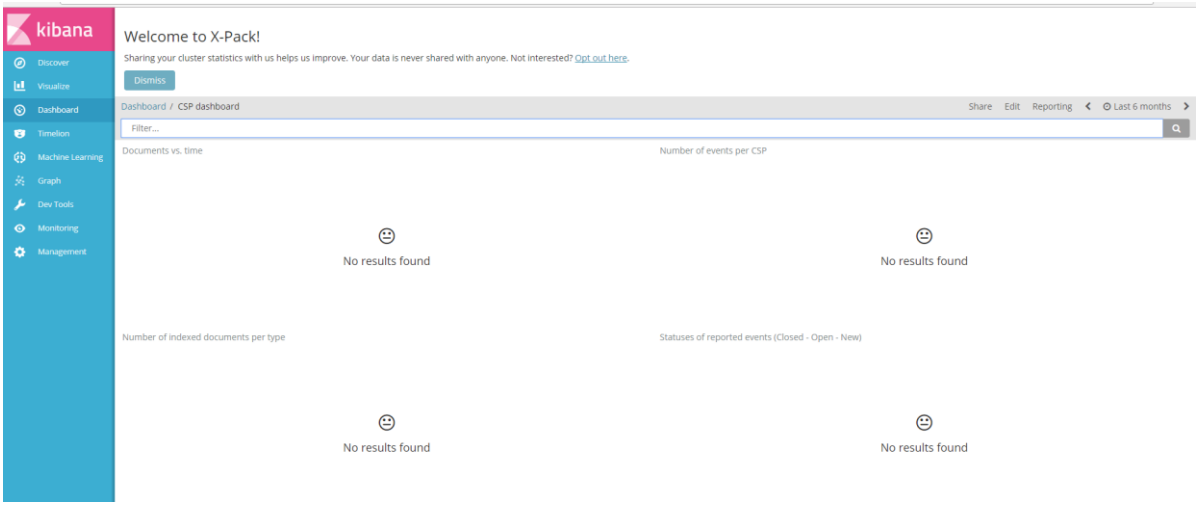
Also note than when accessing the various web interfaces, an SSL Insecure connection notice may appear due to the existence of self-signed certificates. The user should bypass the warning and proceed.

7.2 Connecting to individual services

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

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

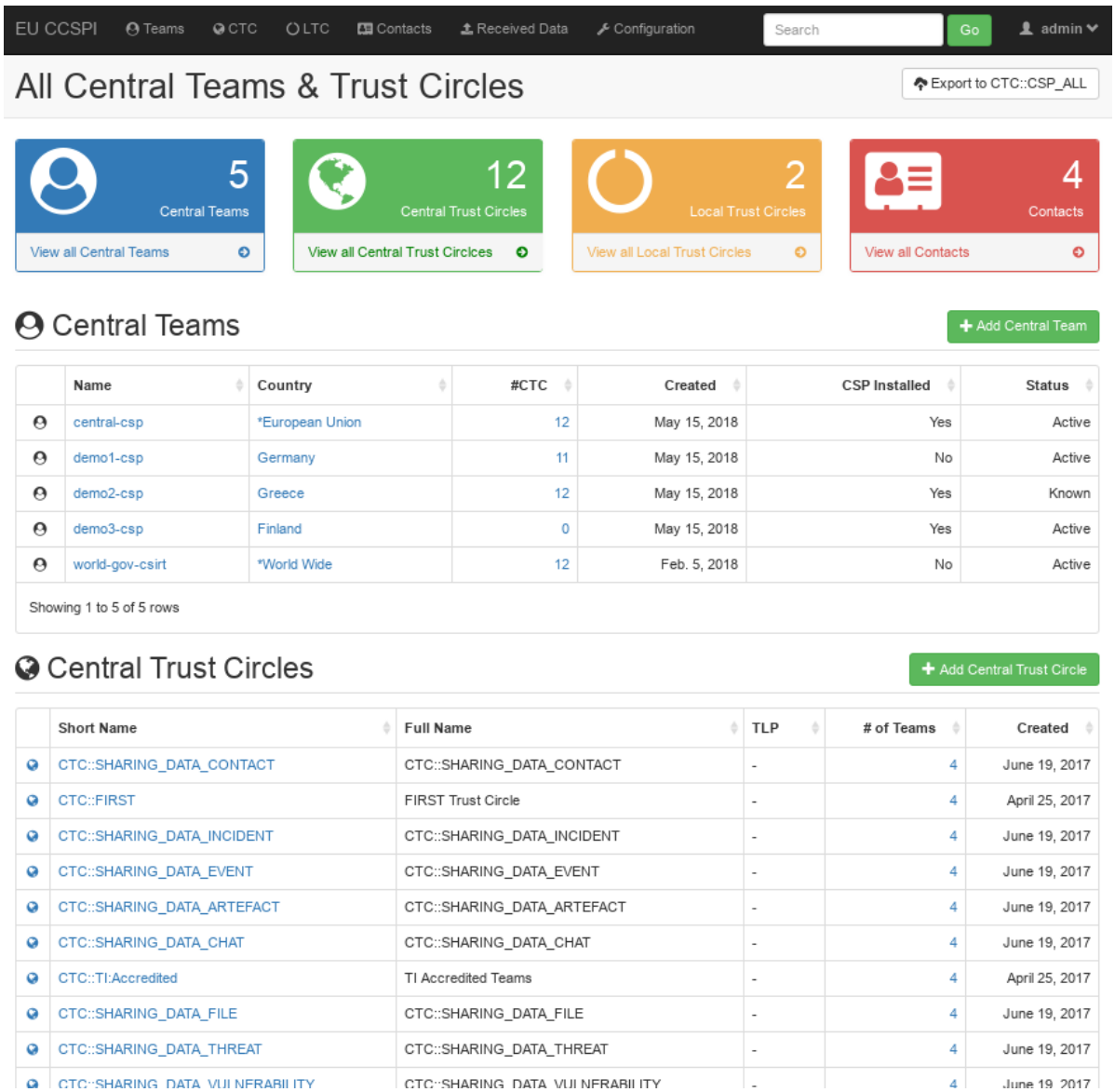
Navigate to Kibana by entering the above URL to your browser.



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.

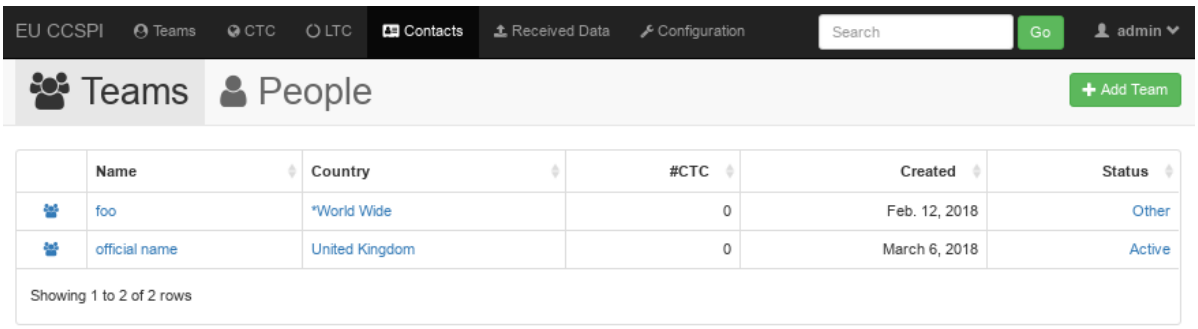
Trust Circles: https://tc.<cspId>.prod.melicertes.eu

Navigate to Trust Circles by entering the above URL in the browser. The "All Central Teams & Trust Circles" page will be displayed with the logged-in user details in the top right corner.



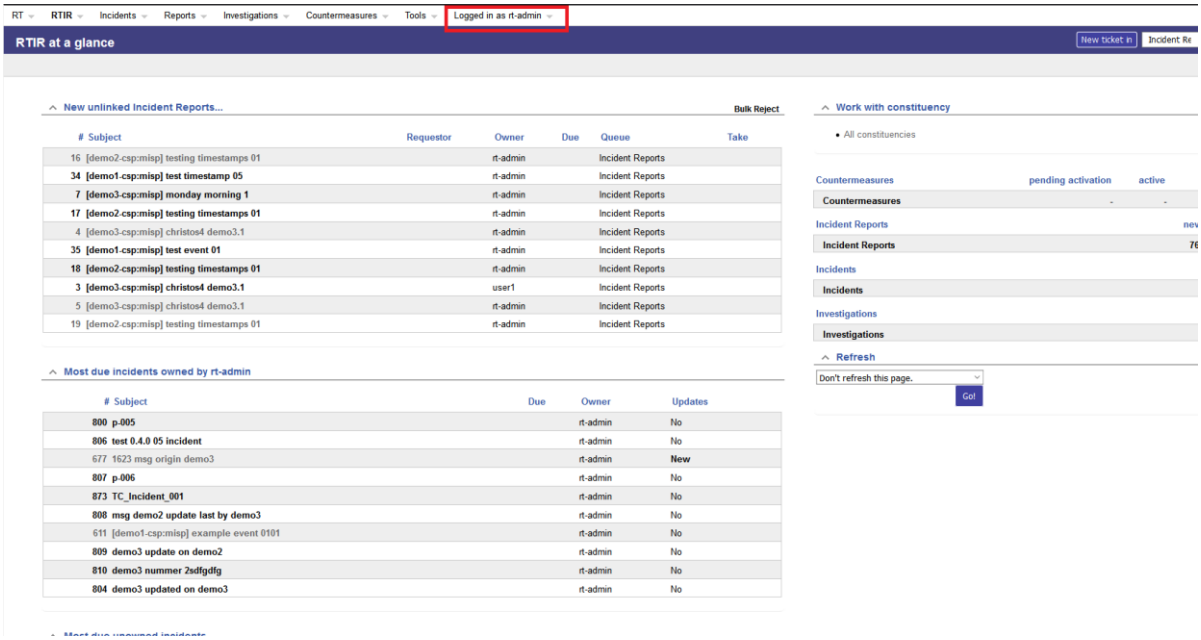
Contact Management: https://tc.<cspId>.prod.melicertes.eu/local/contacts/teams/

Navigate to Contact Management by entering the above URL to a browser. The "Teams" page will be displayed with the logged-in user details in the top right corner.



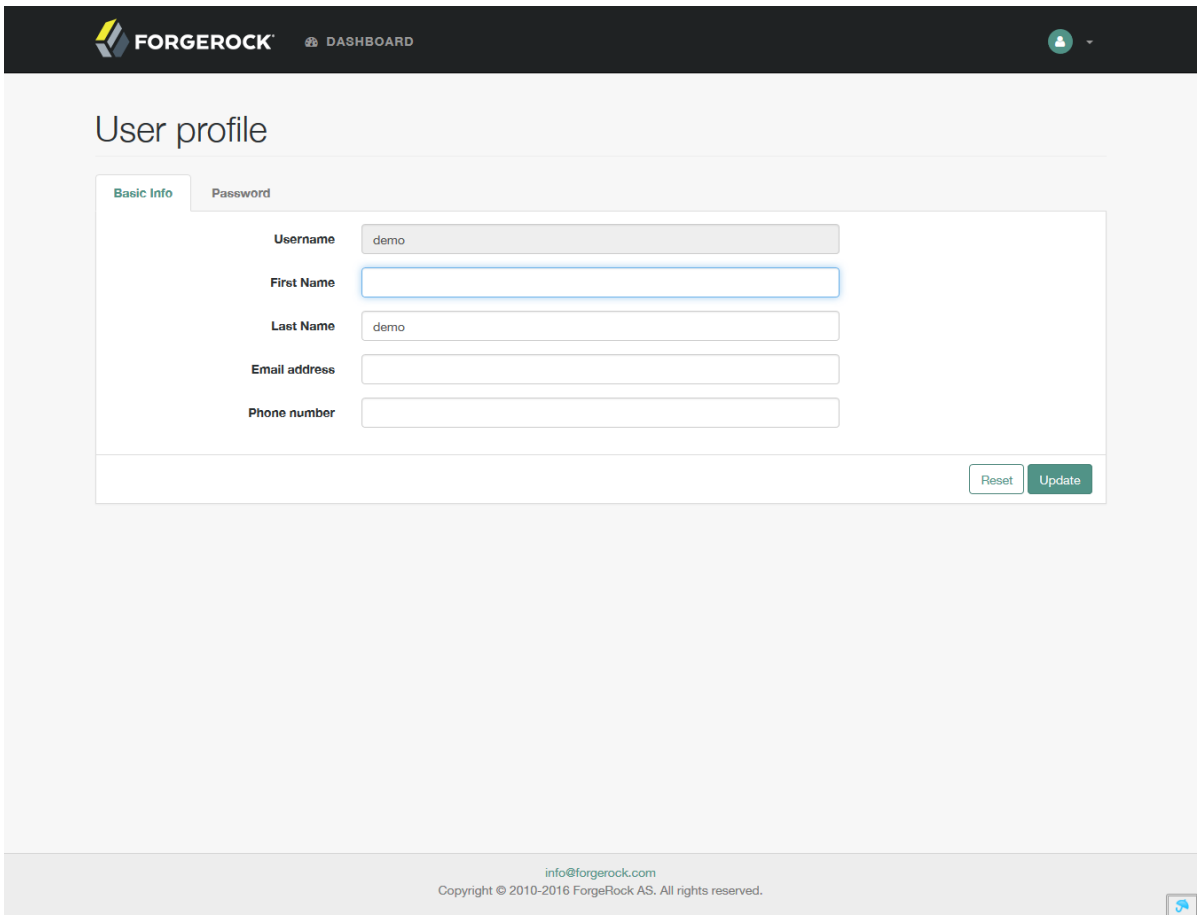
RT: https://rt.<cspId>.prod.melicertes.eu/RTIR

Navigate to RT by entering the above URL to your browser. The "RTIR at a glance" page will be displayed with the logged-in user details in the top right corner.



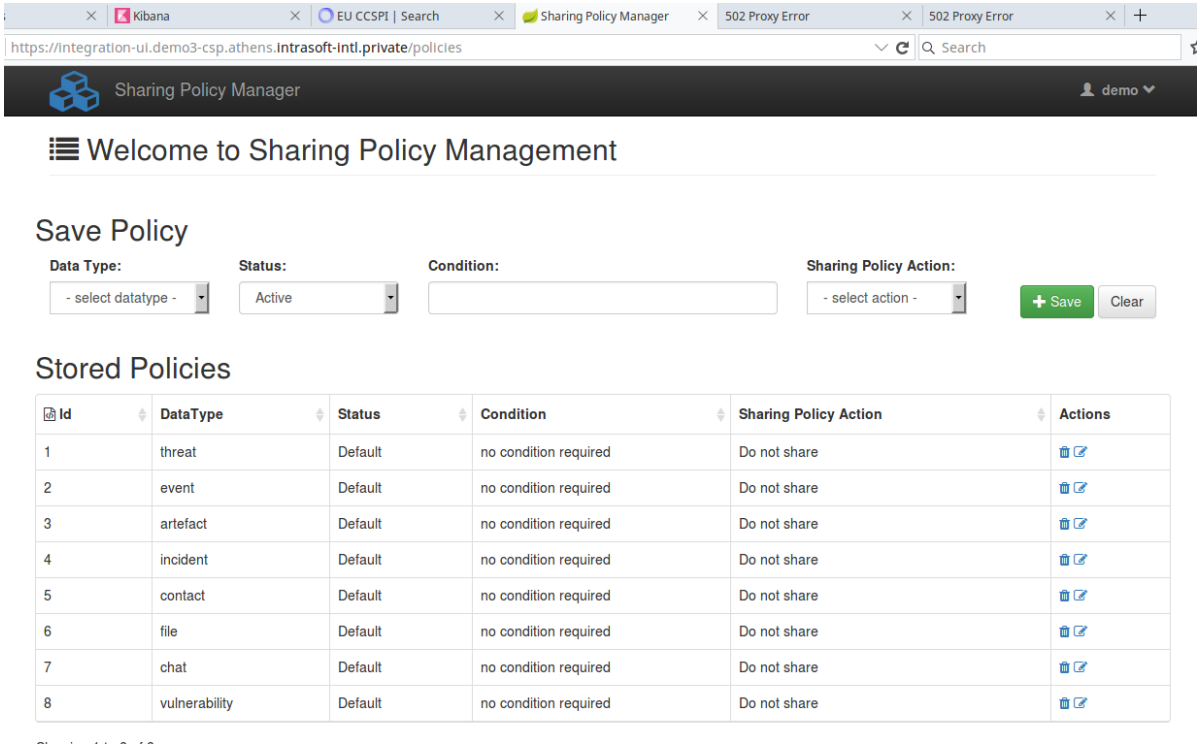
OpenAM: https://auth.<cspId>.prod.melicertes.eu/openam

Navigate to OpenAM by entering the above URL to your browser. The basic user editing information will be displayed.



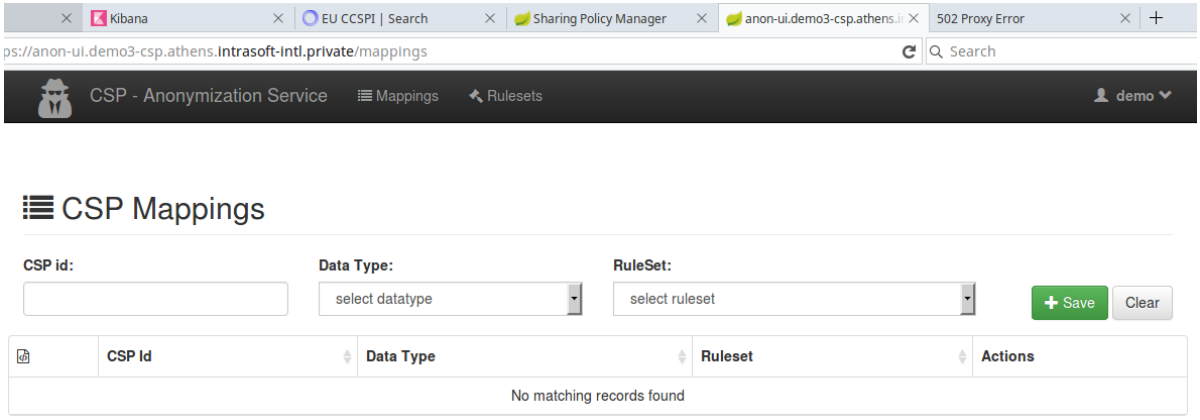
Sharing Policies: https://integration-ui.<cspId>.prod.melicertes.eu

Navigate to Sharing Policies application by entering the above URL in the browser. The "Welcome to Sharing Policy Management" page will be displayed with the logged-in user details in the top right corner.



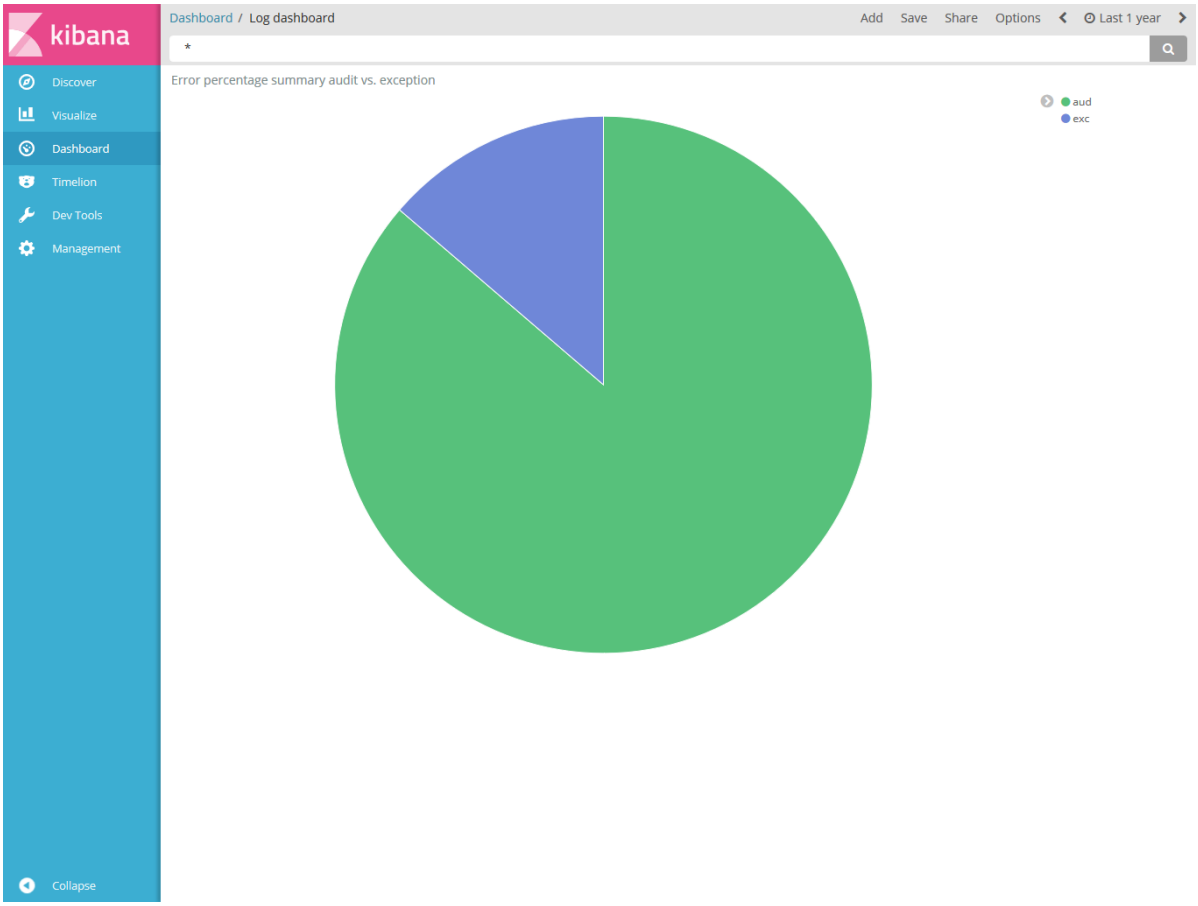
Anonymization: https://anon-ui.<cspId>.prod.melicertes.eu

Navigate to Anonymization application by entering the above URL in the browser. The "CSP Mappings" page will be displayed with the logged-in user details in the top right corner.



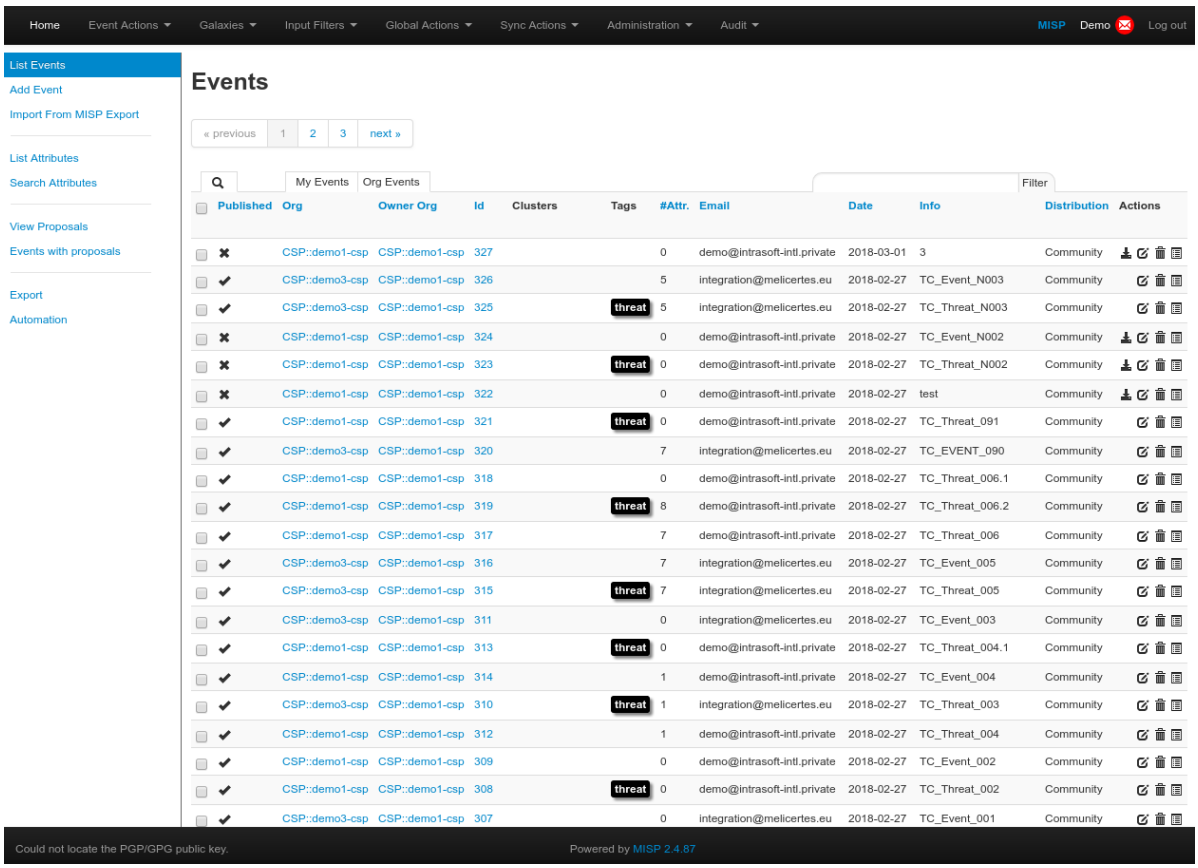
Logs: https://logs.<cspId>.prod.melicertes.eu

Navigate to the log display application by entering the above URL in the browser. This will launch the Kibana dashboard with the audit and exception logs.



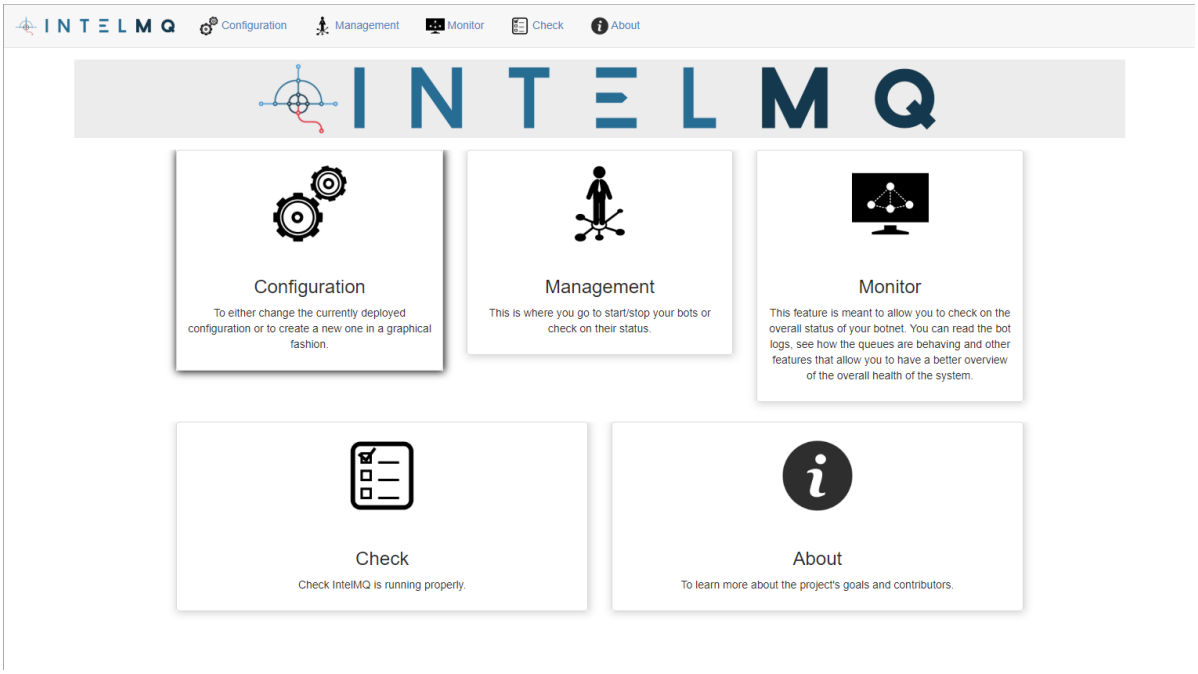
MISP: https://misp-ui.<cspId>.prod.melicertes.eu

Navigate to the MISP web interface by entering the above URL in the browser. The "Last Events" page will be displayed with the logged-in user details in the top right corner.



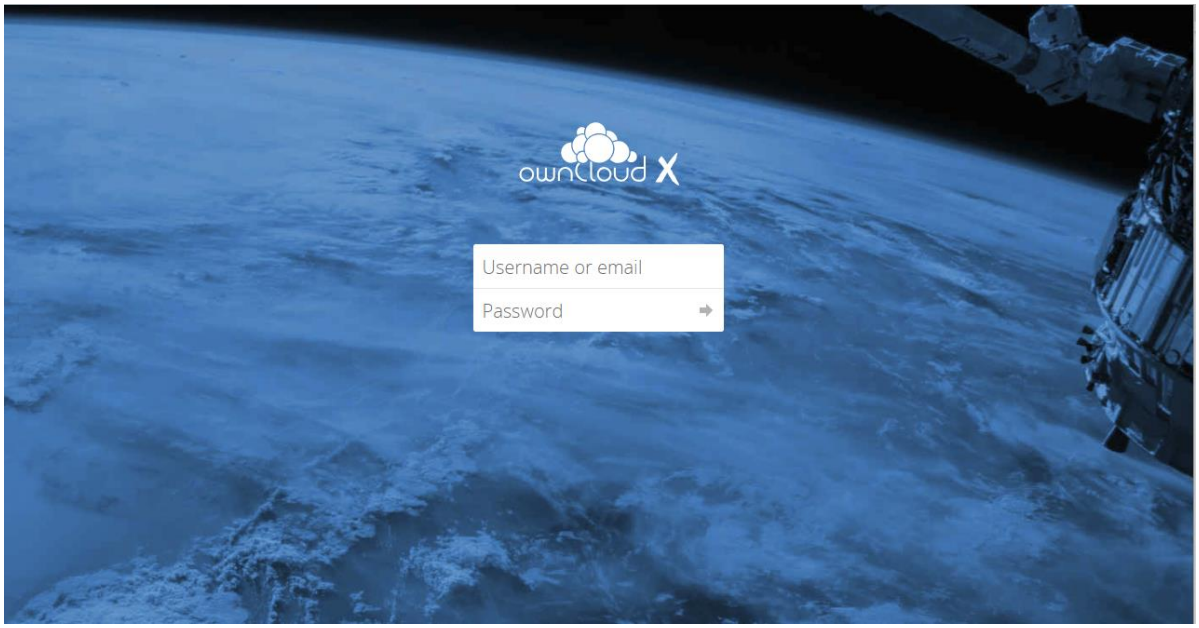
IntelMQ: https://imq.<cspId>.prod.melicertes.eu

Navigate to the INTELMQ web interface by entering the above URL in the browser. This will launch the INTELMQ dashboard.



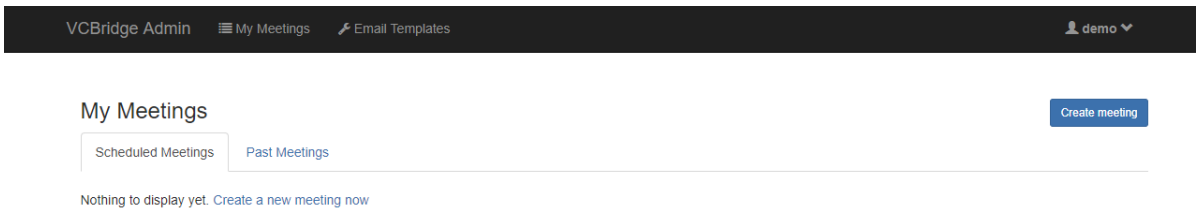
OwnCloud: https://files.<cspId>.prod.melicertes.eu

Navigate to the OwnCloud web interface by entering the above URL in the browser. The OwnCloud login screen will be displayed.



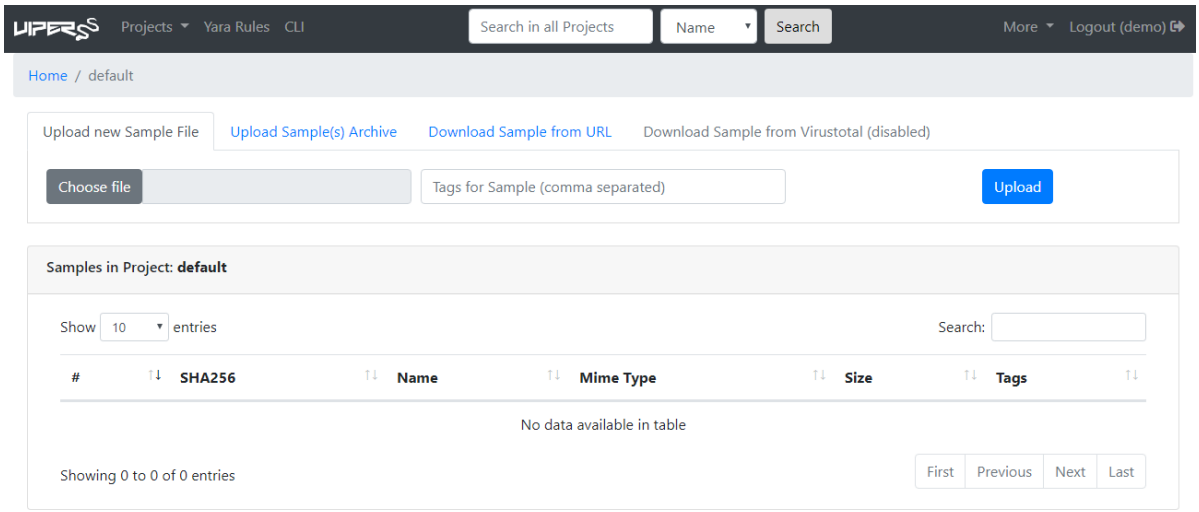
VCBridge (Jitsi): https://teleconf-ui. <cspId>.prod.melicertes.eu

Navigate to the VCBridge web interface by entering the above URL in the browser. The "My Meetings" page will be displayed with the logged-in user details in the top right corner.



Viper: https://viper-ui. <cspId>.prod.melicertes.eu

Navigate to the Viper web interface by entering the above URL in the browser. The Viper home page will be displayed with the logged-in user details in the top right corner.



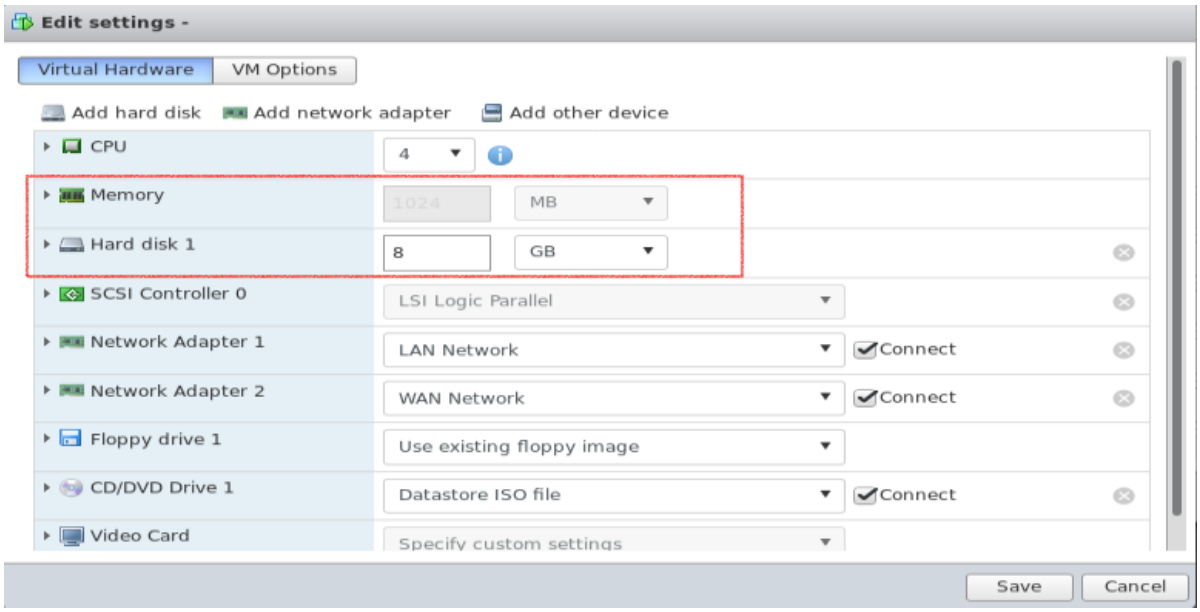
8 Annex A: Changing settings of the VM

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

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

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

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



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

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

1.1 Expanding the VM root filesystem

The expansion of the filesystem is a two-step process:

- The first step is to adjust the settings (previous section).
- The second step is to expand the 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 the partition is indeed larger:

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

- Stop the running docker services:

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

- Add the packages required for this operation:

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

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

```
$ partprobe
```

- Resize the partition:

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

- Verify that the 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 rebooting the machine, the system is ready for the installation.

9 Annex B: Jitsi VideoConferencing Bridge

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

9.1 External port accessibility

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

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

9.2 Bandwidth requirements

The Jitsi Videoconferencing Bridge implements a "Selective Forwarding Unit[3] – SFU" in Videoconferencing terms. This means that it is scalable and geared towards "asymmetric" links, having more "downstream" bandwidth in the case of a client / participant, and "near" symmetric bandwidth in the case of the bridge itself. Technically the bridge requires as much bandwidth as necessary to be able to receive all streams from all participants and then N times as much to be able to distribute all the received streams to all participants.

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

- The audio stream consumes about 50 Kbps (average) for each participant;
- The video stream consumes about 500 Kbps (average) for a combined audio/video total of 550 Kbps per participant.
- For a conference with 5 endpoints (N = 5), the theoretical bandwidth required would be:
    - 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.

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

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

10 Annex C: Troubleshooting CSP Installer

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

```
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

- End of document-