CEF: Cybersecurity Digital Service Infrastructure;

Core Service Platform – SMART 2015/1089

Version: 4.2.2

Date: 09/10/2019

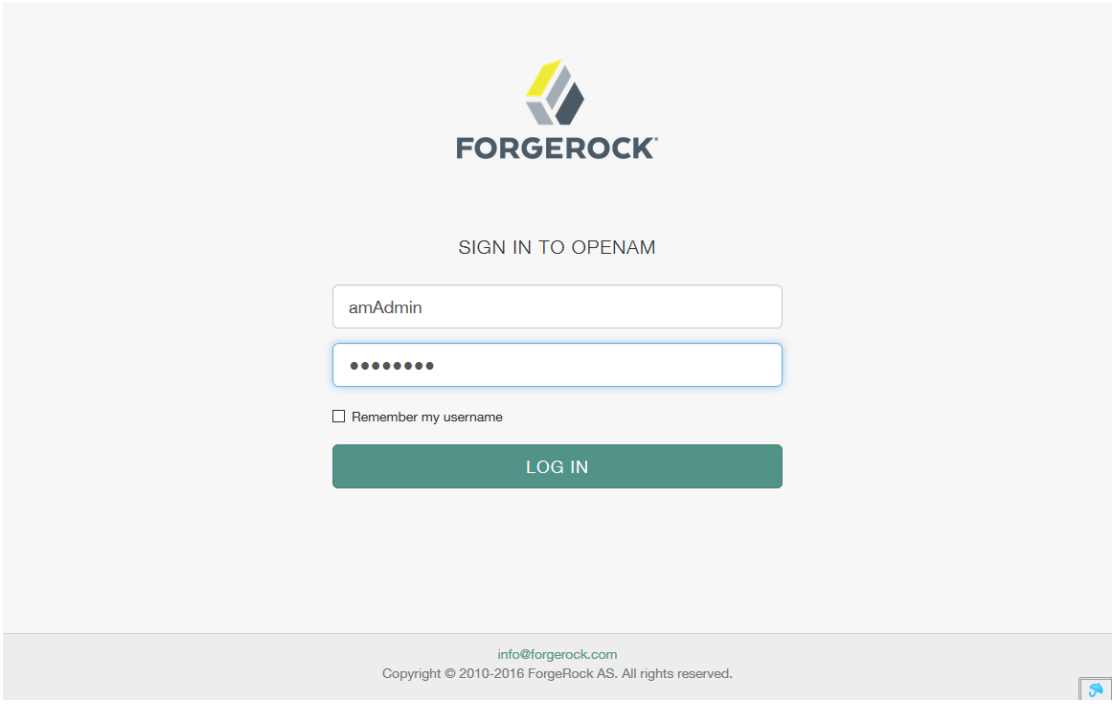
Administration Manual

Contents

1 User management with openAM

1.1 Initial setup

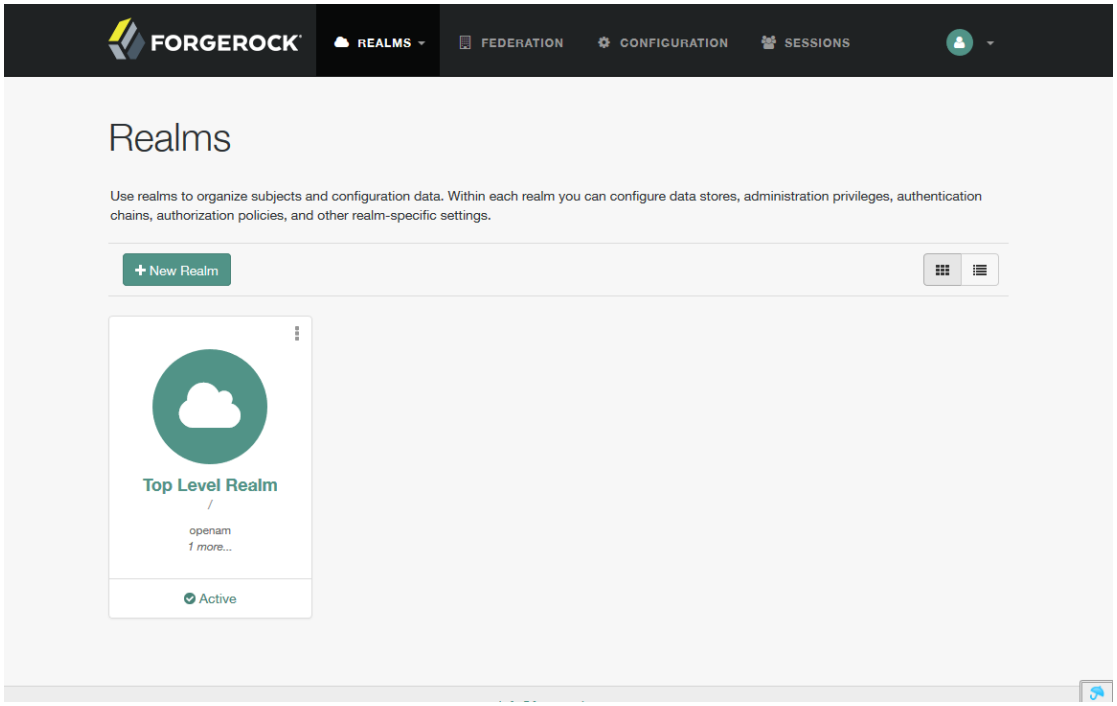
OpenAM administrative interface can be accessed at https://auth.<cspId>.[preprod.]melicertes.eu/openam URL. The user will be presented with the following screen. Default openAM administrator “amAdmin” with password “11111111”[1].



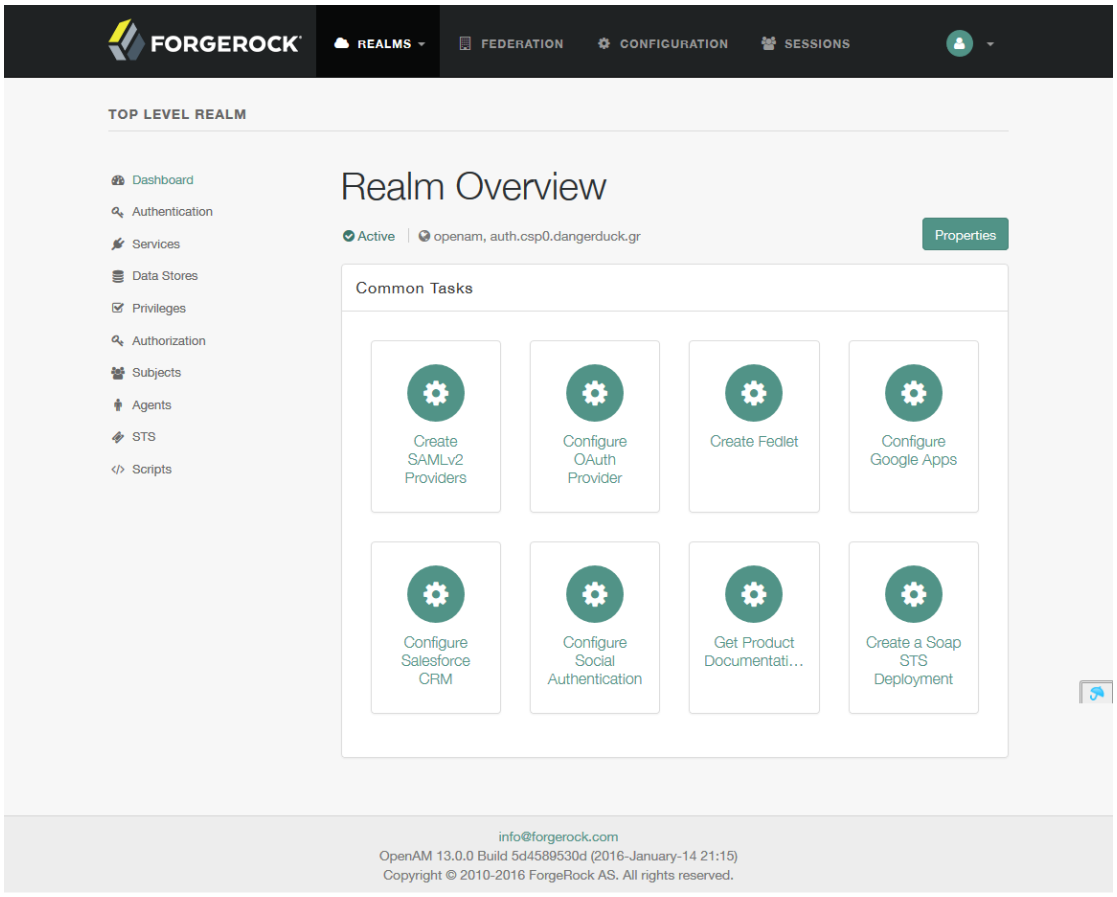
The password should be changed at first session as explained later.

After logging in, the user is presented with the Realm selection option. Only one Realm exists in this configuration, namely the Top Level Ream, and should be selected.

[1] We strongly recommend changing the pre-set password after the initial installation has been done.

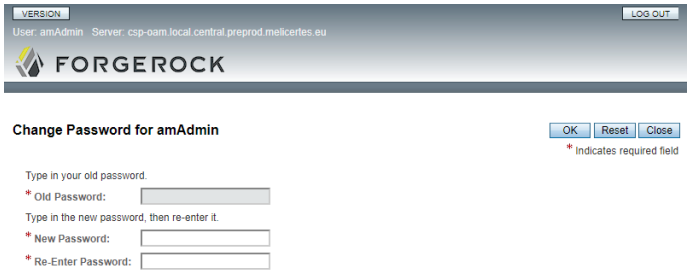


After selecting the Realm, the realm options are presented. In order to perform user management tasks, the option “Subjects” should be selected from the sidebar.



A list of users then appears. By clicking on each user, editing options are displayed while clicking on the “New…” button the add user screen is displayed.

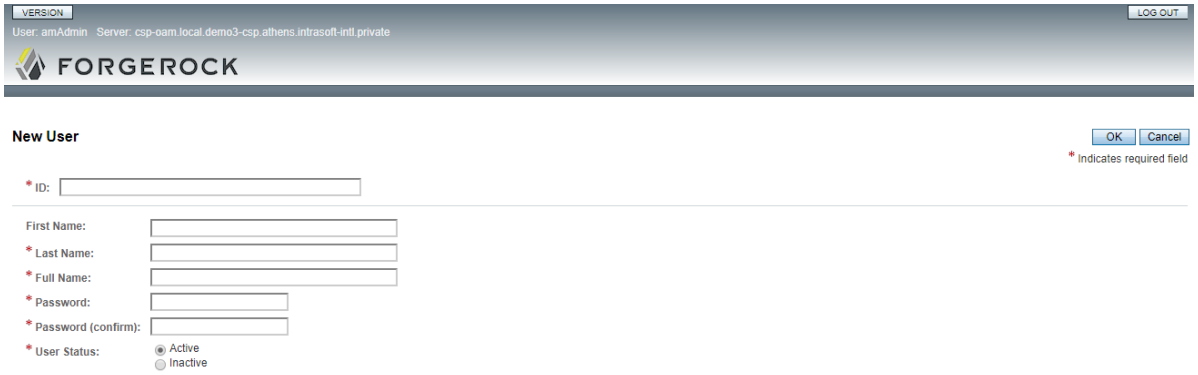
To perform the admin password change, one needs to click on the amAdmin user and then click on the “edit” link that appears next to the password option.



A default user called “demo” exists with a default password of “changeit”. This password should be changed as well. The user “demo” exists for the administrator to be able to verify that OpenAm authentication works correctly by accessing the CSP applications after installation.

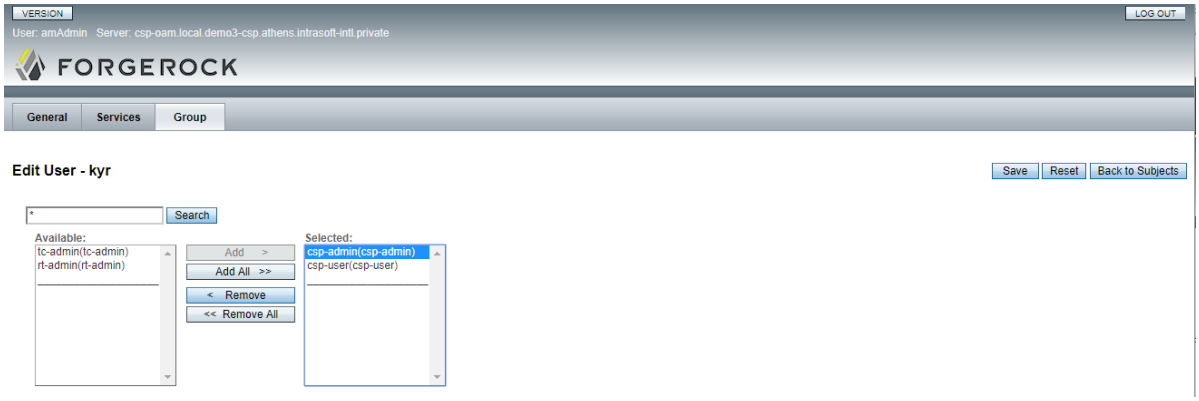
1.2 User management

User creation is done by pressing the “New…” button. The following screen appears. Enter the user details and press “OK”.



For the new user to be able to access the CSP applications, she should belong to certain groups. In order to add the user to groups, you click on the user name and select the “Group” tab from the use details screen.

A user should belong to the group “csp-user”. If the user is also an administrator, she should belong to the group “csp-admin” also. In order to have access to the RT application, the user needs to belong to rt-admin and rt-user group.



Note: No additional steps are required to allow login via user certificate for this user. As long as the user id matches the one in the user certificate and the certificate has been issued by the Melicertes PKI, the user can access the CSP applications by using either her user certificate or her login and password. Further information on how to request and install user certificates can be found in the user manual chapter 1.

Note: The user “amAdmin” cannot be used to access any applications other than the openAM administrator interface itself. The user “demo” should be deleted after the initial testing phase.

1.3 User certificate Handling

User can login into CSP either by using the user certificates or by using userid/password credentials. In case of certificate-driven authentication, one of the two following possibilities can be choose:

1. Usage of the user certificates issued by the MELiCERTES Test PKI – per default enabled and could be used out of the box (see chapter 1.1.1)
2. Usage of own user certificates – this implies CSP has to be reconfigured in order to support this case (see chapter 1.1.2)

1.3.1 Usage of MELICERTES PKI user certificates

In order to use the user certificates coming from MELICERTES PKI, ever user has to apply for such certificate in advance. The procedure of the application is detailed described in User Manual chapter 1.1.

As all the certificates issued by MELICERTES PKI are coming from the same Certificate authority (CA), the users coming from different CSIRTs but having the same userid (stored in CN of DN of subject) could authenticate successfully an all these instances. In order to have the users of one CSIRT can only be positively authenticated on this very particular CSIRT, there has to be a validation of the organisation name additional to the validation of the userid. How to specify the organisation name during the certificate application process is described in User Manual in chapter 1.1.

The configuration of the particular authentication module, in order to check the certificate is belonging to the particular organisation is described in chapter 1.1.3.

1.3.2 Usage of own user certificates

The certificate driven authentication on CSP is performed in two steps:

1. The proxy-server is terminating the TLS-session and also performing the validation of the user certificate against the specified certificate authority (CA)
2. OpenAM instance parses the incoming user certificate and maps the subject DN data on an existing user accounts in order to authenticate the user.

In order to use own certificates to authenticate the users, the both instances proxy and OpenAM have to be appropriately configured.

Proxy configuration

Proxy server checks the provided user certificates, whether they are coming from the defined issuer (CA) from. In order to use own user certificates, the corresponding CA certificate has to be known to the proxy server.

1. Stop the CSP (make sure the apache proxy server docker is properly stopped)
2. Copy your CA certificate (e.g. my-ca.crt[2]) into csp-proxy
    a. docker cp my-ca-crt csp-apache:/etc/apache2/ssl/ca/my-ca.crt
3. Make sure the copied ca certificate can read by everyone
4. Edit the file /opt/csp/apache2/csp-sites/csp-sites.oam.200.conf and change the name of the ca certificate file in the property “SSLCACertificateFile” to points to the newly copied one (e.g. /etc/apache2/ssl/ca/my-ca.crt) in the External VirtualHost configuration section
5. Start the CSP
6. Login as amadmin using the userid/password credentials and do further configuration if necessary (see chapter next chapter)

OpenAM configuration

In order to use the new certificates, at least two additional configuration steps should be performed on OpenAM:

1. Configuration of the authentication module (see also https://backstage.forgerock.com/docs/openam/13/admin-guide/#cert-module-conf-hints for further information)
    a. Login into OpenAM by using your administrator credentials (initially it is amadmin/11111111), if not already done
    b. Choose the top level realm “/”
    c. Follow the “Authentication” link on the left site of the web page

2 Please use PEM format.

d. Click on the “Modules” link
e. Click on the “CSP-Certs” link in the “MODULE NAME” column and confirm by pressing the “Yes” button, you want to edit the settings
f. Set up the userid mapping according to https://backstage.forgerock.com/docs/openam/13/admin-guide/#cert-module-conf-hints
g. Setup organisation mapping according to chapter 1.1.3
h. Scroll to the bottom of the page and press the button “Save Changes”.

2. Creation of the particular users (see chapter 1.2)[3]

1.3.3 Organisation name validation

In order to configure the validation of the organisation name, please refer to the following steps.

1. Login into OpenAM by using your administrator credentials (initially it is amadmin/11111111)
2. Choose the top level realm “/”
3. Follow the “Authentication” link on the left site of the web page
4. Click on the “Modules” link
5. Click on the “CSP-Certs” link in the “MODULE NAME” column and confirm by pressing the “Yes” button, you want to edit the settings
6. Scroll to the bottom of the page and specify in the field “Certificate field used to access organisation name”, which attribute of the DN of subject should be used for that:
   a. None – means the validation will be skipped
   b. Subject O – the attribute O of DN of subject will be used for validation
   c. Subject OU - the attribute OU of DN of subject will be used for validation[4]
7. If you chose b. or c. in step 6, than the attribute “Name of the organisation” should be appropriate adjusted.
8. Scroll to the bottom of the page and press the “Save Changes” button.

The configuration has been done and stored and is active.

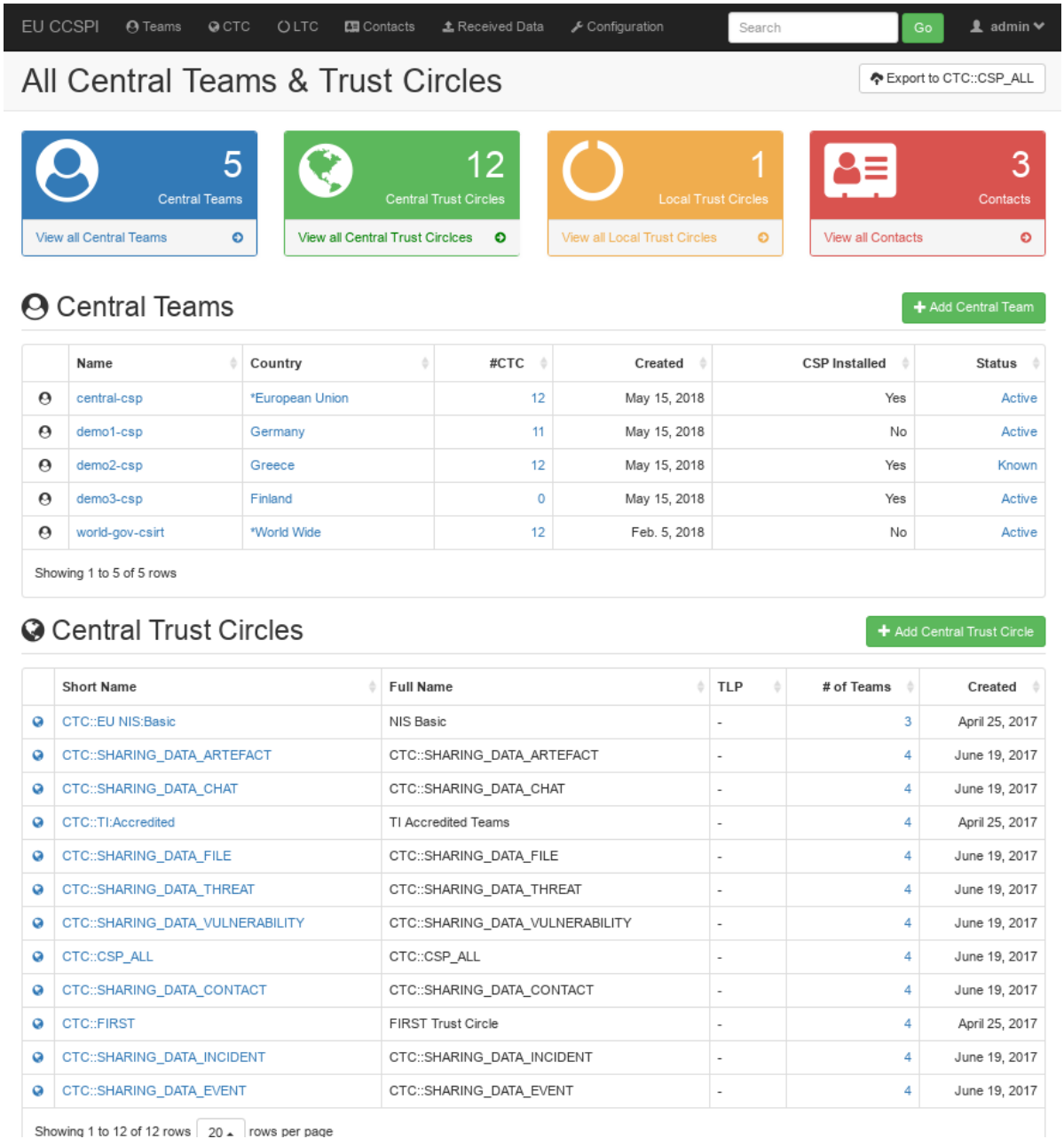
[3] Important! The userid provided to OpenAM user and the value of the corresponding attribute of the DN of subject in the certificate has to match.

[4] Note! This setting should be used together with the certificates issued by MELICERTES PKI, if the department name has been provided.

2 Trust Circle Management

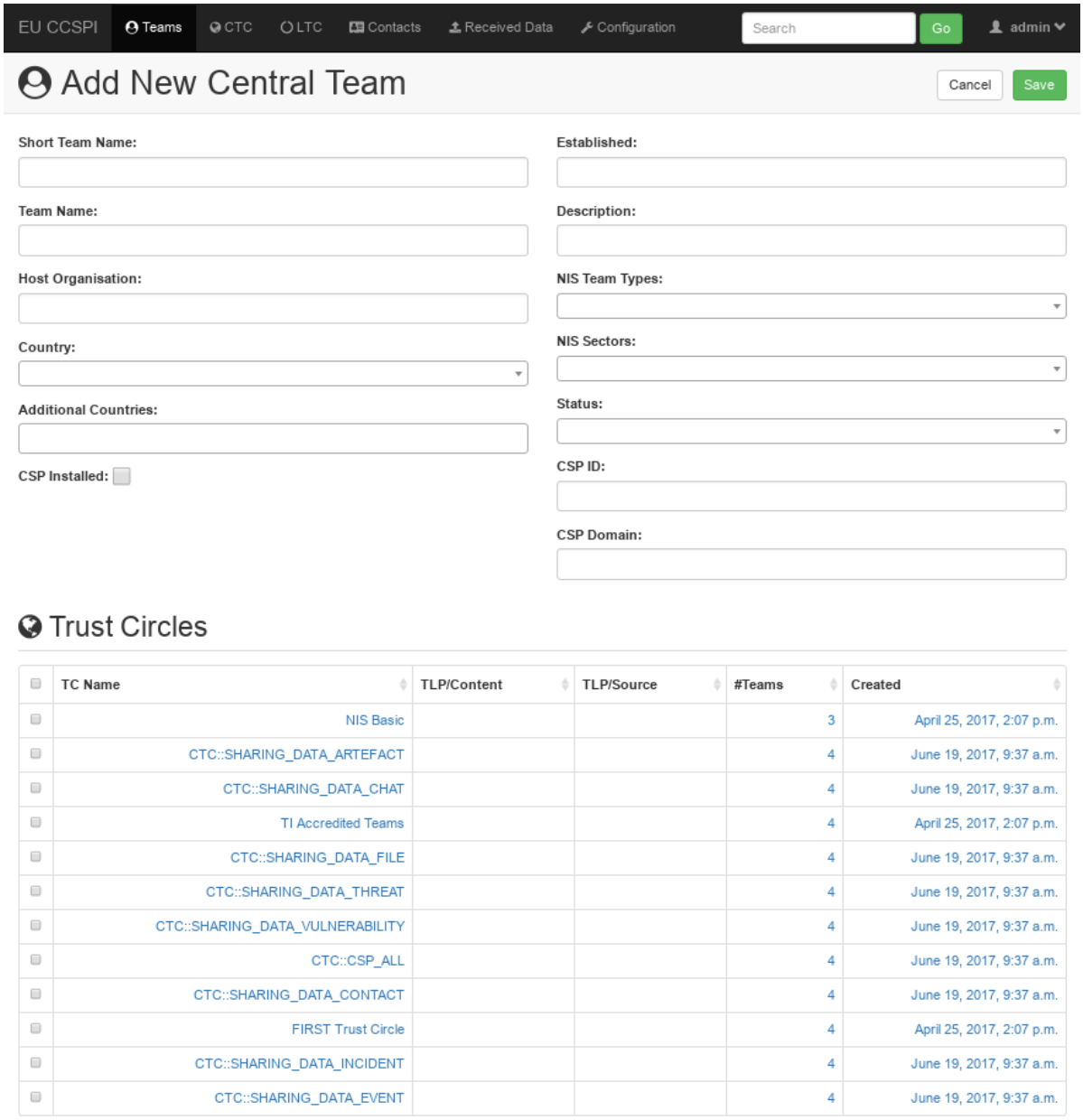
The trust circle management can be accessed at https://tc.<cspId>.[preprod.]melicertes.eu.

The default screen that appears after login is the overview screen that presents concise information on available teams and trust circles.

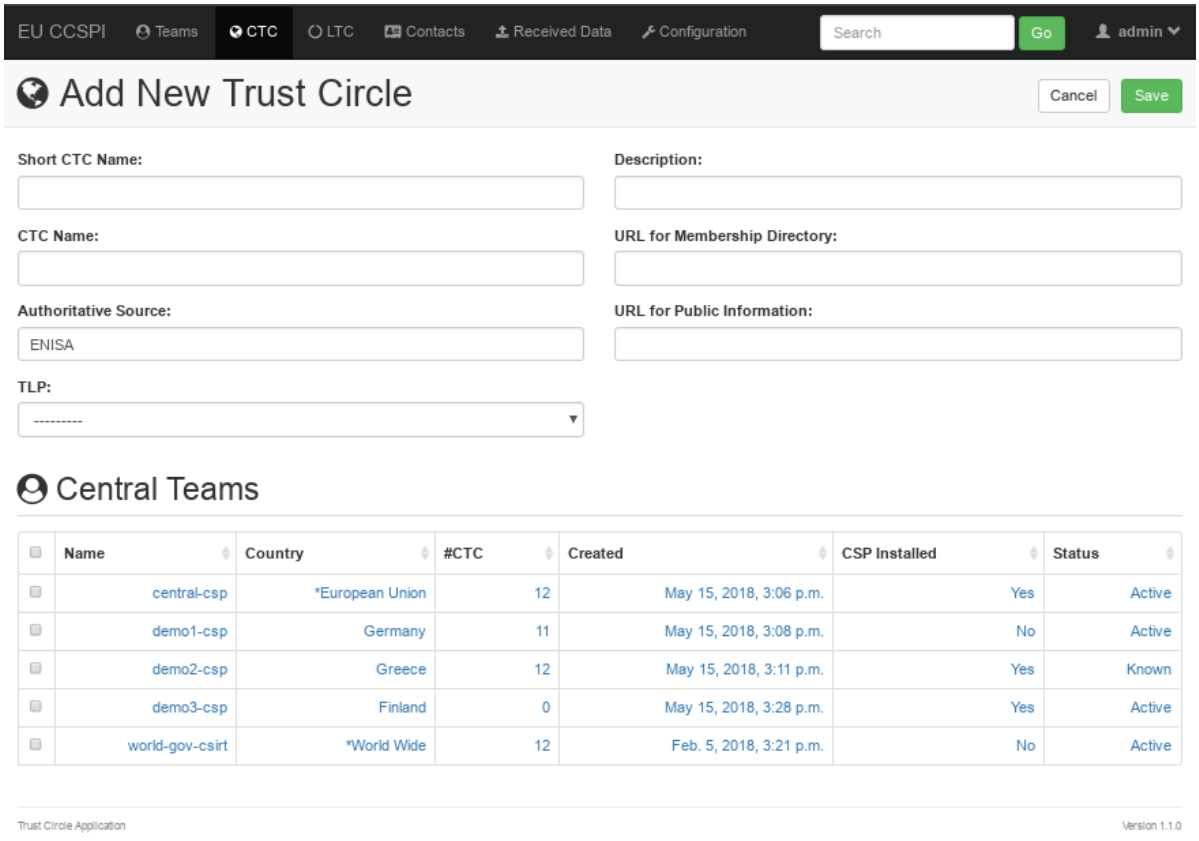


You can view the team or trust circle details by clicking on their respective names.

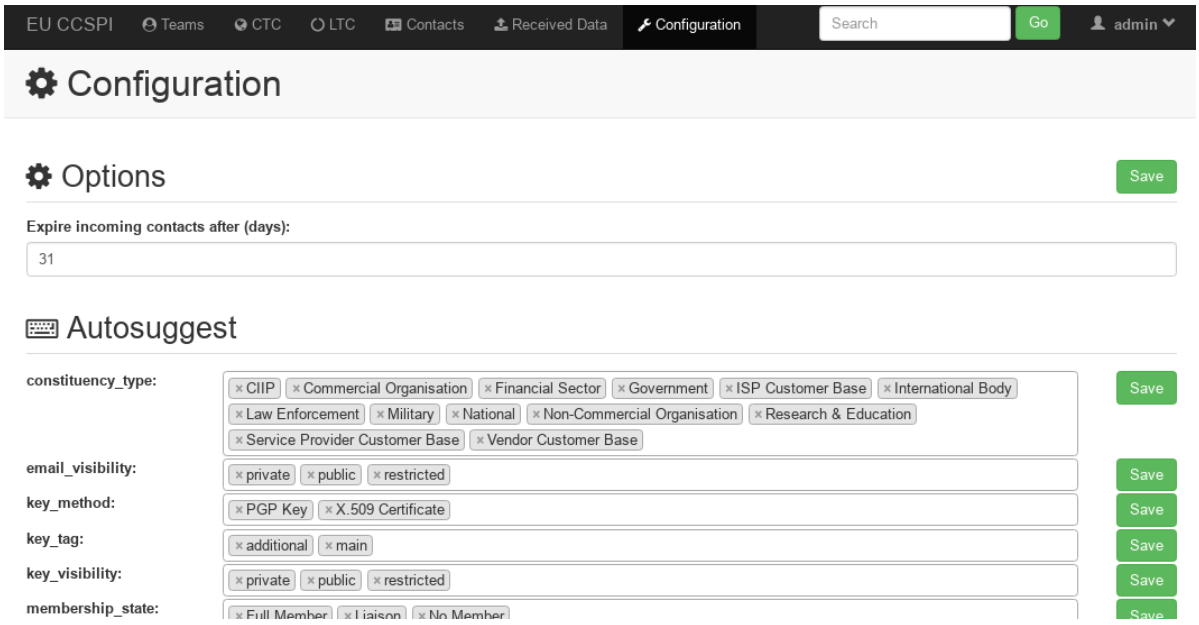
To add a new team, press the “Add Central Team” button and enter the team details as exemplified below. You can also add this team to the various existing trust circles by checking the checkboxes on the left of the trust circles names. The new team is saved by clicking “Save”.



To add a new Trust Circle, you press the “Add Central Trust Circle” button and trust circle details need to be entered in the form as seen below. You can also add existing teams to this trust circle by checking the checkboxes on the left of the team names. The new trust circle is saved by clicking “Save”.

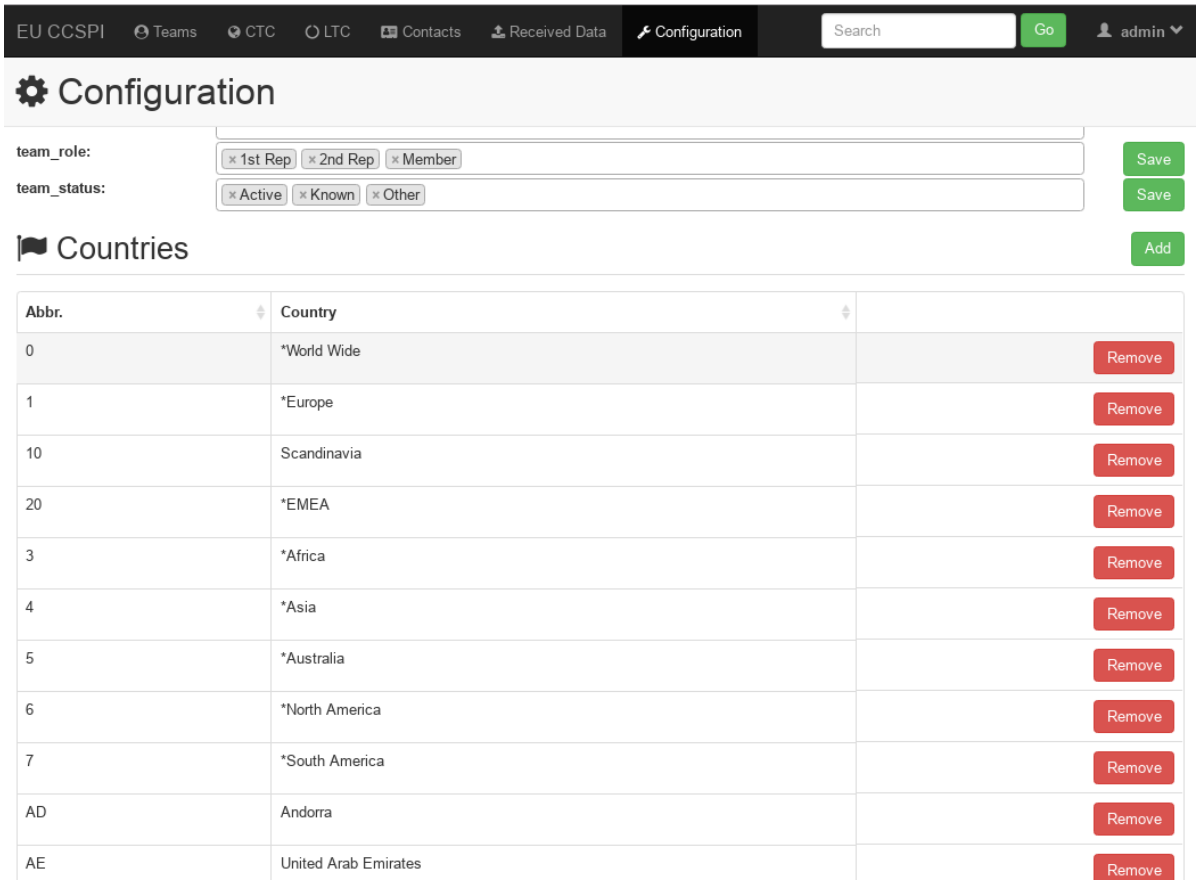


Finally, various parameters, including incoming data expiration settings, list of typeahead suggestions for all input fields and a country editor can be setup by opening the "Configuration" tab. Clicking it shows the dedicated administration interface as pictured below.

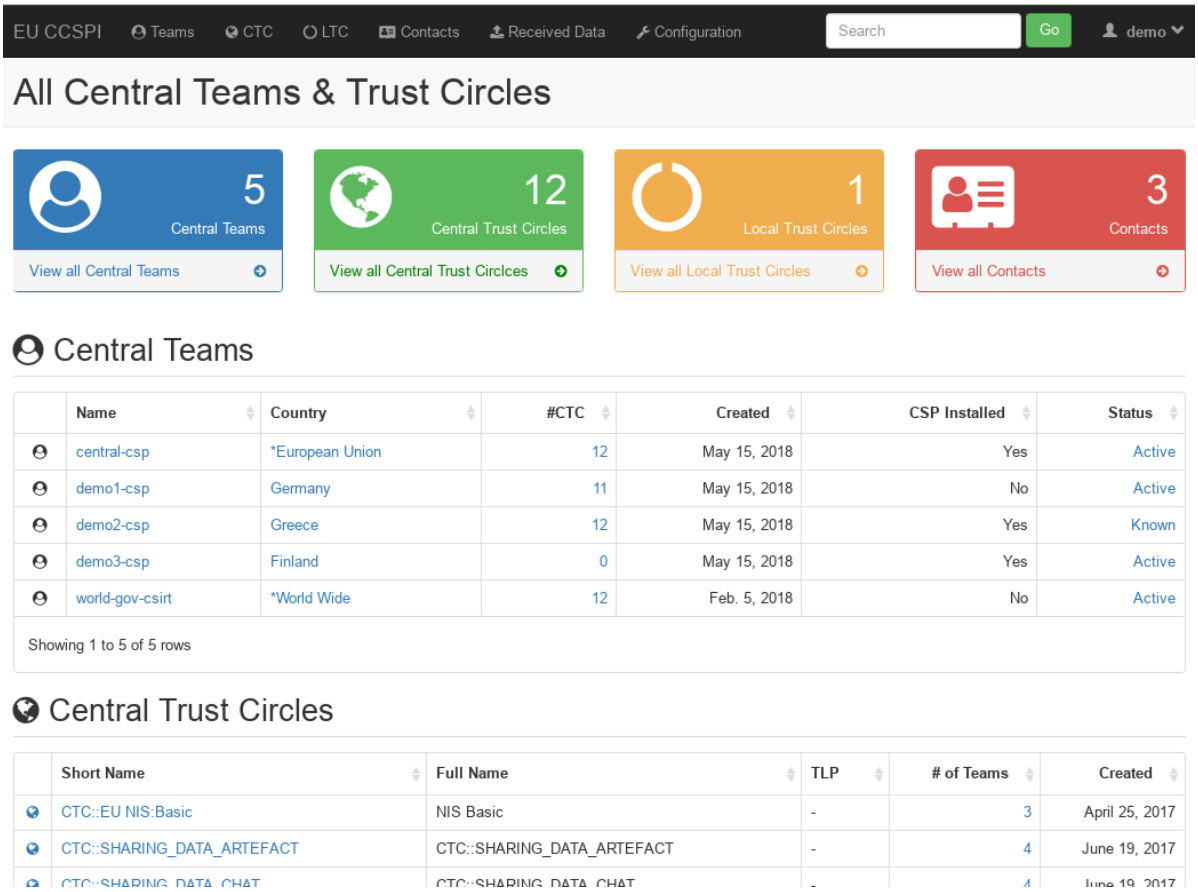


A default configuration is deployed after installation of the TC module. By default, incoming contacts are expired after 31 days. This configuration option is accessible by any role with access to the web interface of the TC application and only applies to the local installation.

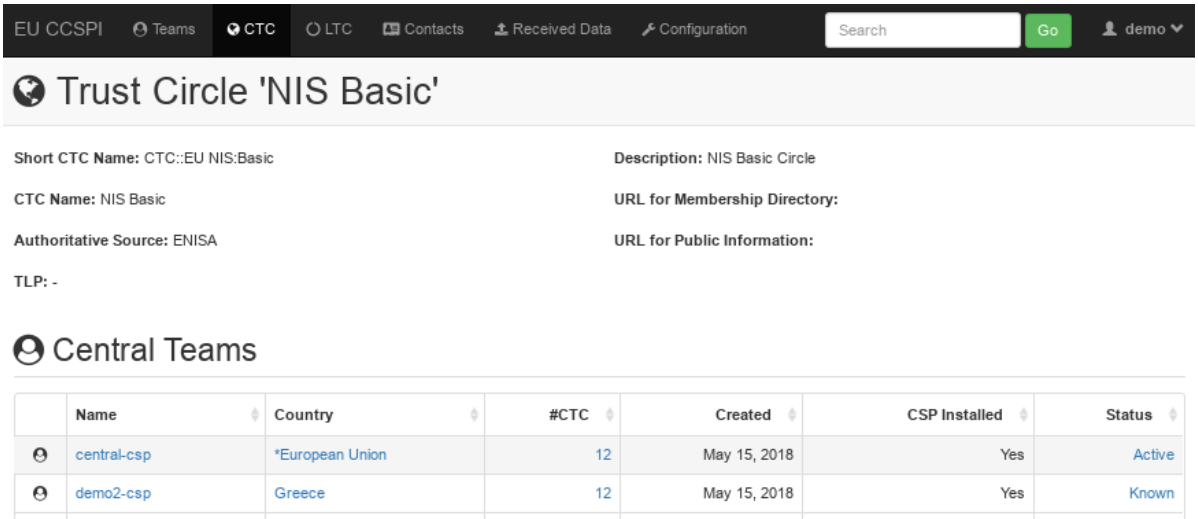
In addition to expiry options, the tc-admin role also has access to an autosuggest and the countries editor, as pictured below. These entries assist the user by suggesting sane values (autosuggest) in all the user forms. Furthermore, the list of countries can be helpful to homogeneously name regions for contact management purposes. Note, that the user may still decide to enter a free-text country name instead of suggested values. Currently, the countries and autosuggest options are not shared across instances in a way a central trust circle may be shared.



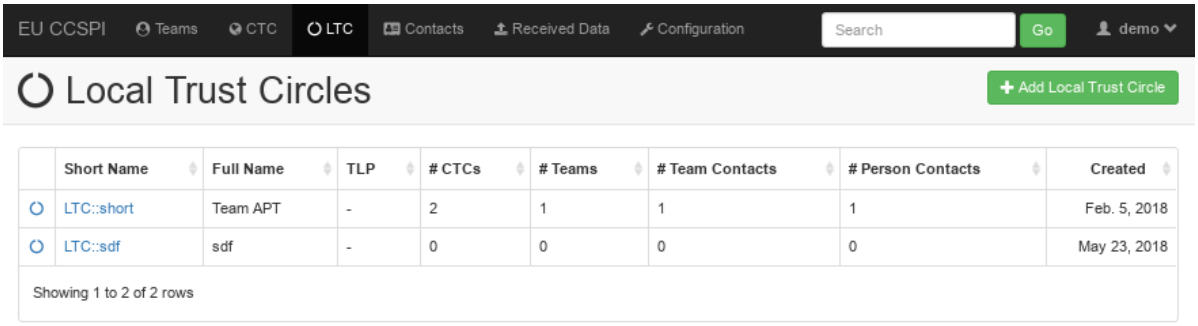
Main dashboard for a the CSP administrator with read only access can be seen below.



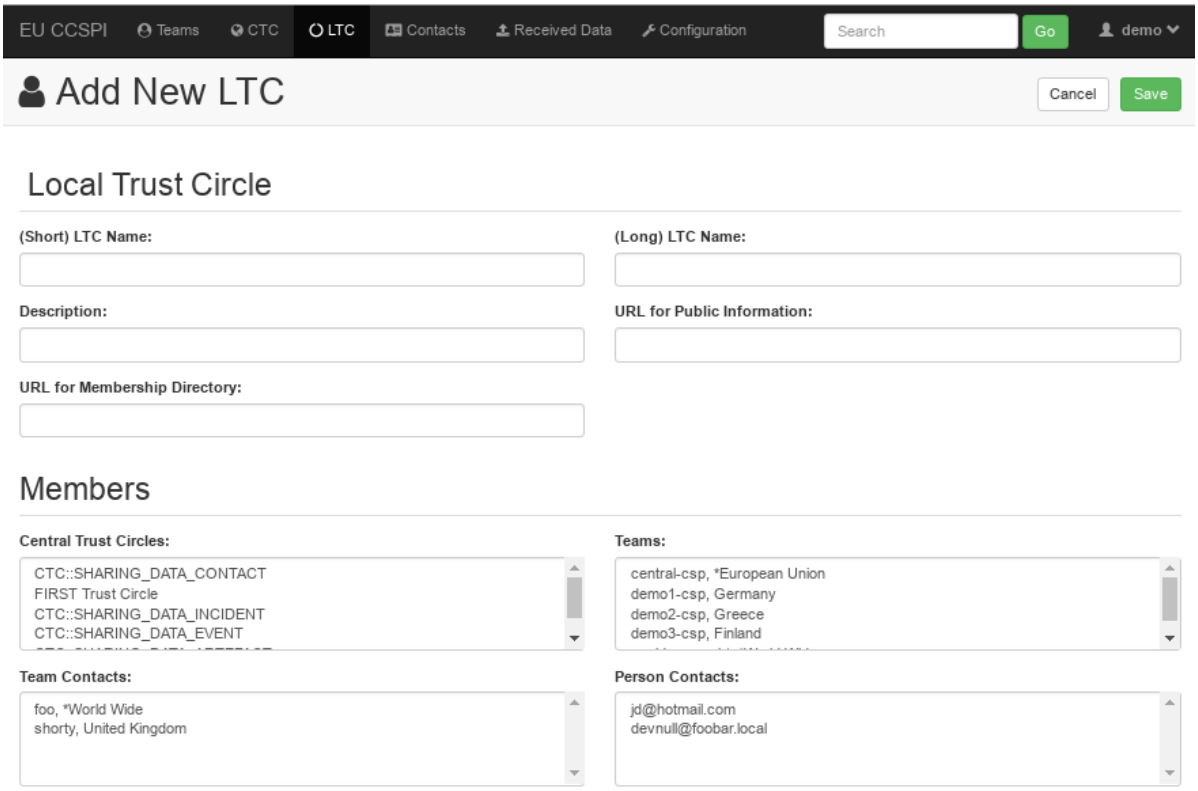
When clicking on a team name, the CSP administrator can view the team details without been able to edit them as seen below. When clicking on a trust circle name, the CSP administrator can view the trust circle details without been able to edit them as seen below.



To create a new Local Trust Circle please visit the “LTC” tab in the top navigation bar and click on “Add Local Trust Circle” button on the resulting webpage. A screenshot of the page is attached below.



The editing interface allow to fill in details like names, descriptions and URLs. As shown below, the "Add New LTC" page allows the user to pick the recipient list consisting of any number of (Central) Trust Circles, Teams, Team Contacts and Person Contacts.

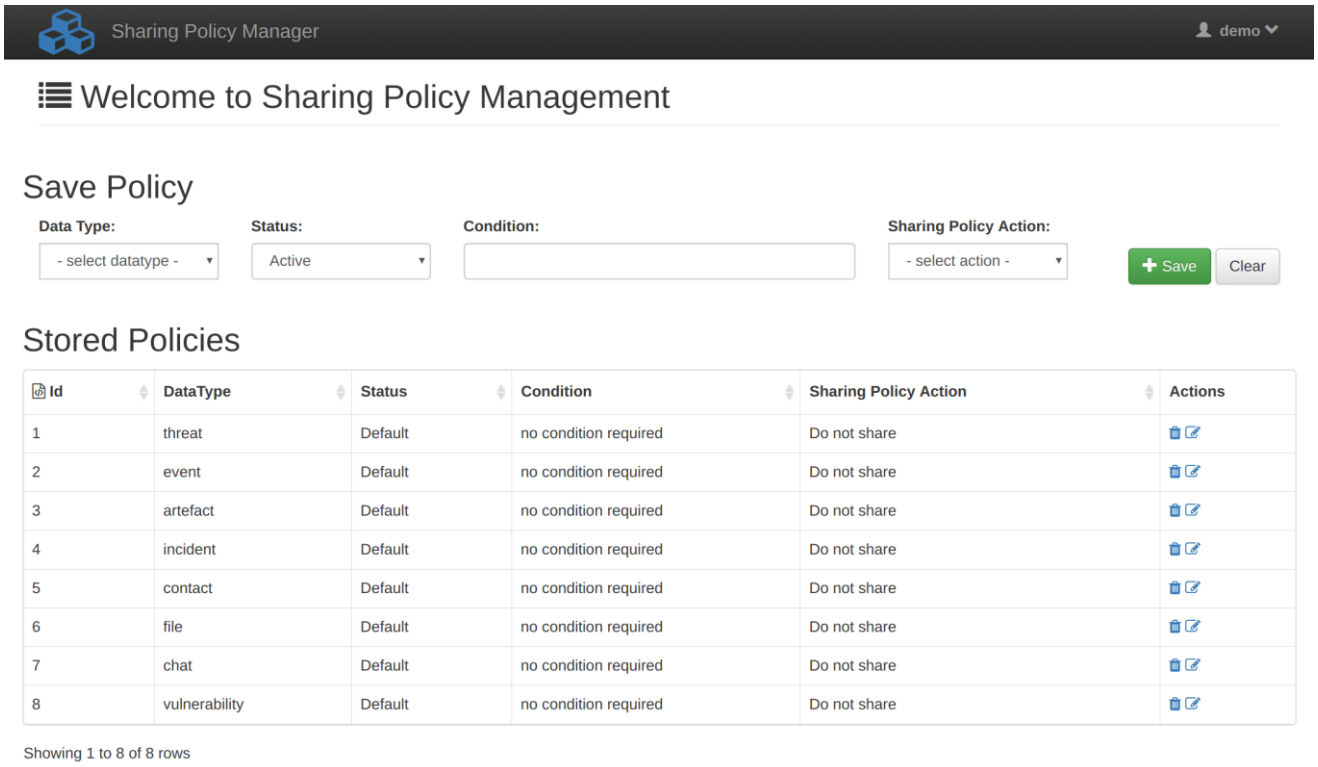


To save the current LTC press the "Save" button.

3 Policy Management

Policy Management can be accessed at the https://integration-ui.<cspId>.[preprod.]melicertes.eu URL.

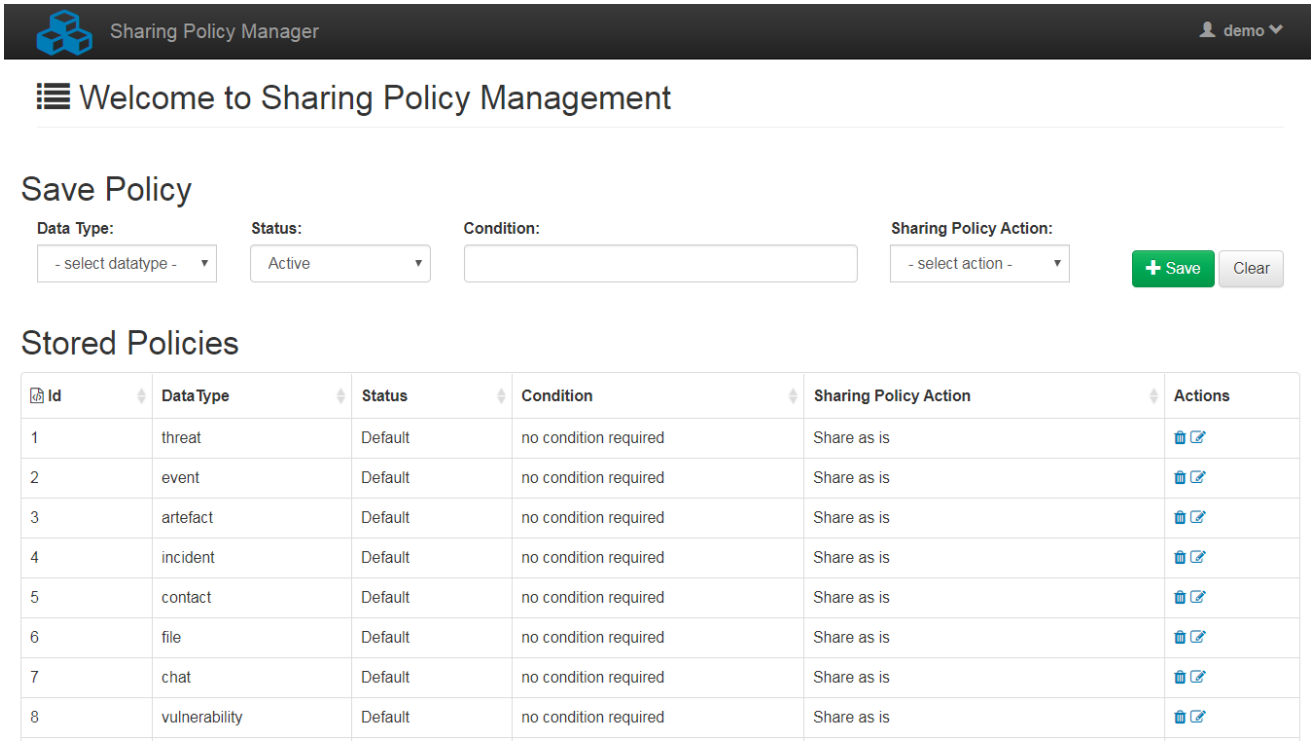
At the time of initial installation, the Sharing Policies are set to disallow any sharing by default. In that case, the policy manager shows the configured policies as shown in the next screen



3.1 Recommended Sharing Policy settings before first use

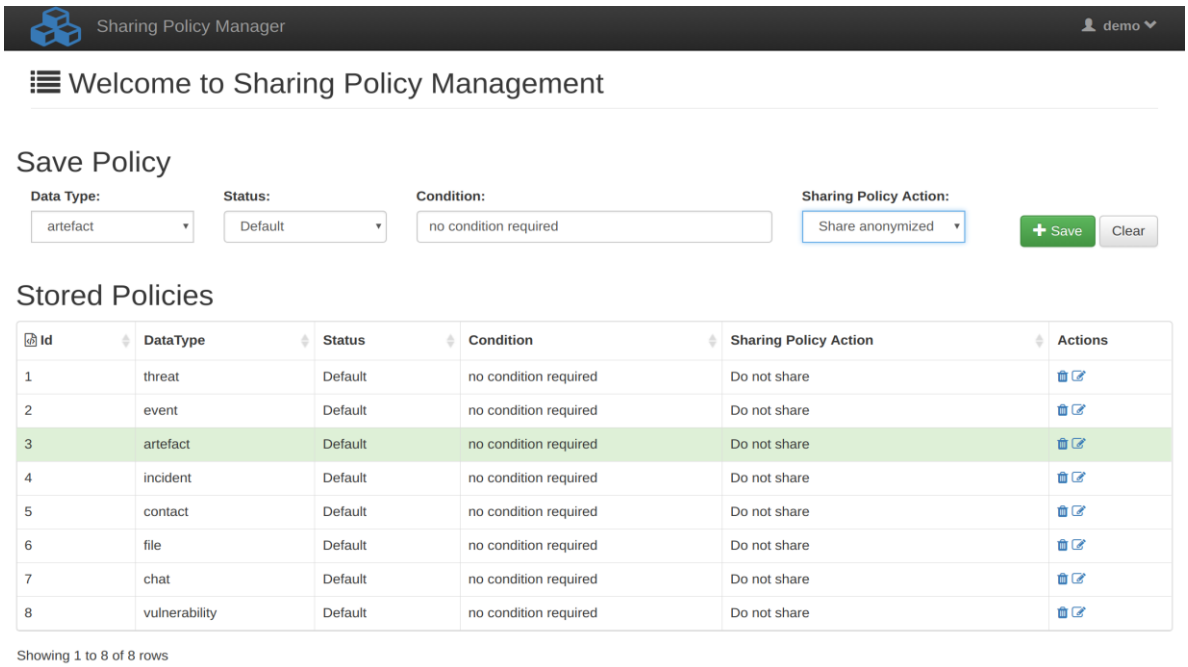
Sharing Policies are a rather powerful mechanism with advanced configuration options to allow for finegrained alignment with the sharing preferences of your organization. However, to ensure that sharing can take place initially, it is recommended to start with a rather relaxed set of Sharing Policies and configure restrictions at a later phase.

Update the Sharing Policy Action for each default policy from “Do not share” to “Share as is”. The instructions for updating a policy action are described in the next paragraphs, but the relaxed set of Sharing Policies should look like this:

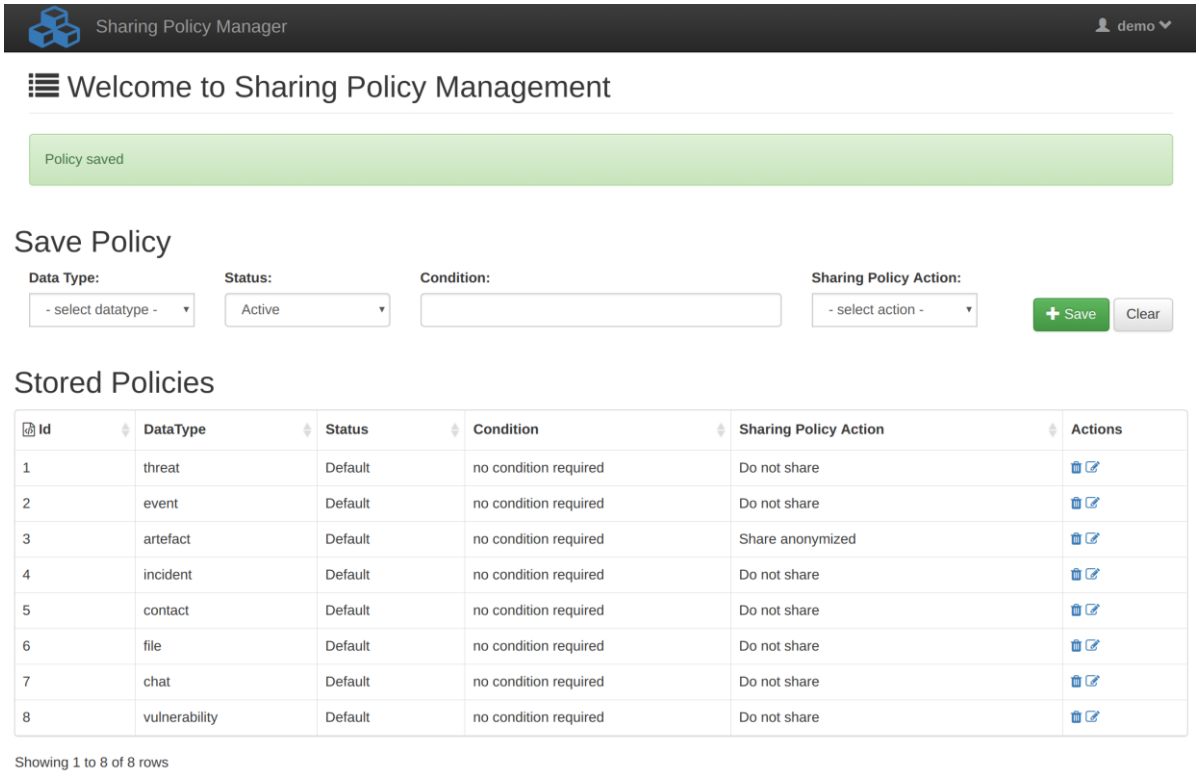


3.2 Modifying a policy

The user can select from any existing policy and update the action. In the example below, the action is to perform anonymization on data for the type 'artefact':



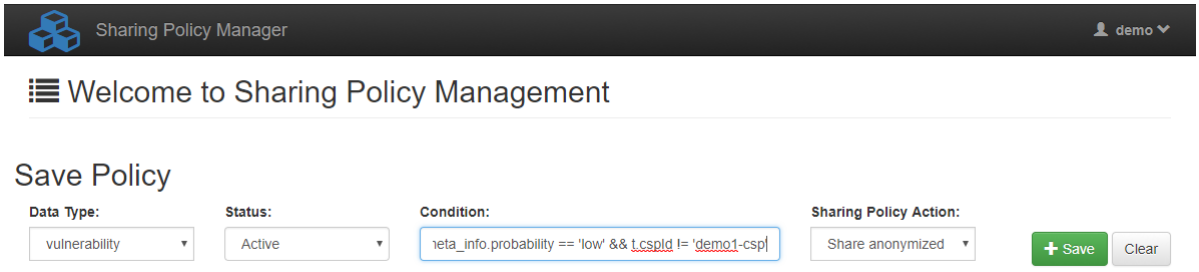
By changing the action from the "Sharing Policy Action" dropdown list and pressing the "Save" button. Per example, the action of the policy with id=3, will be updated:



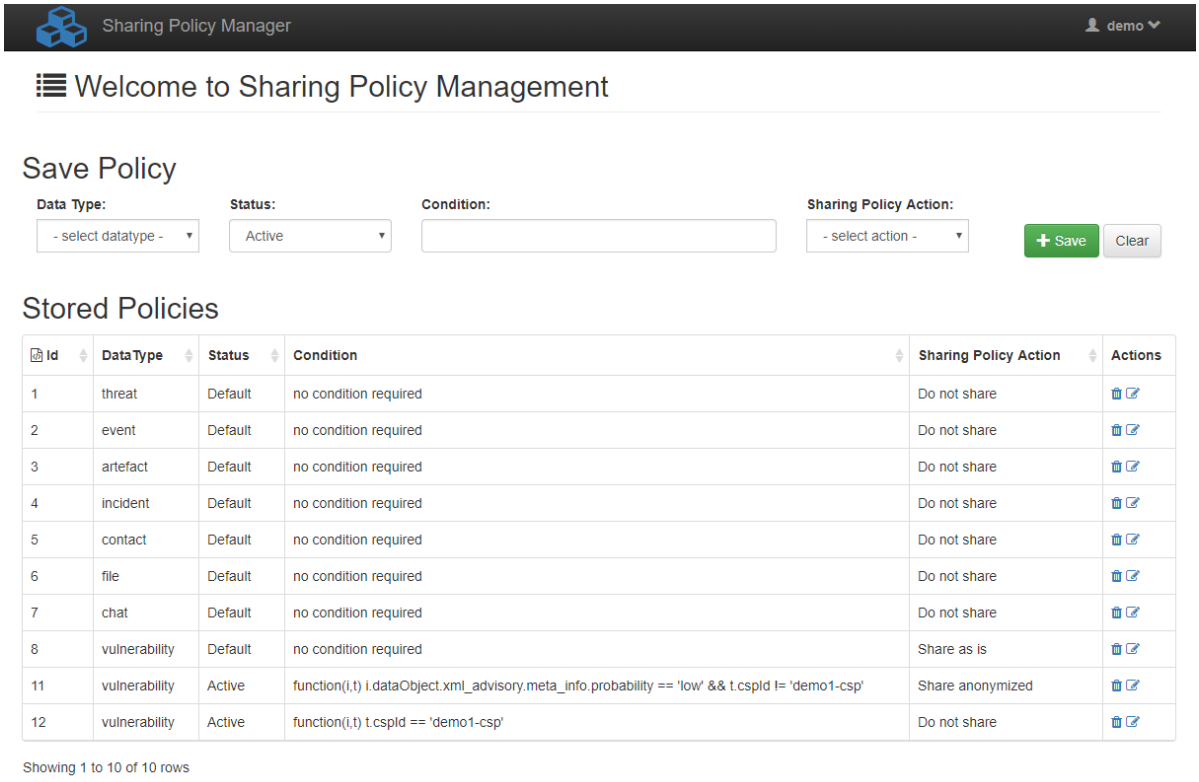
To update a sharing policy to share data without any anonymization, simply select 'Share as is' and Save the change.

3.3 Creating a new policy

In order to insert a new policy, choose a datatype, set the policy status, write the condition, choose the action and press the "Save" button.

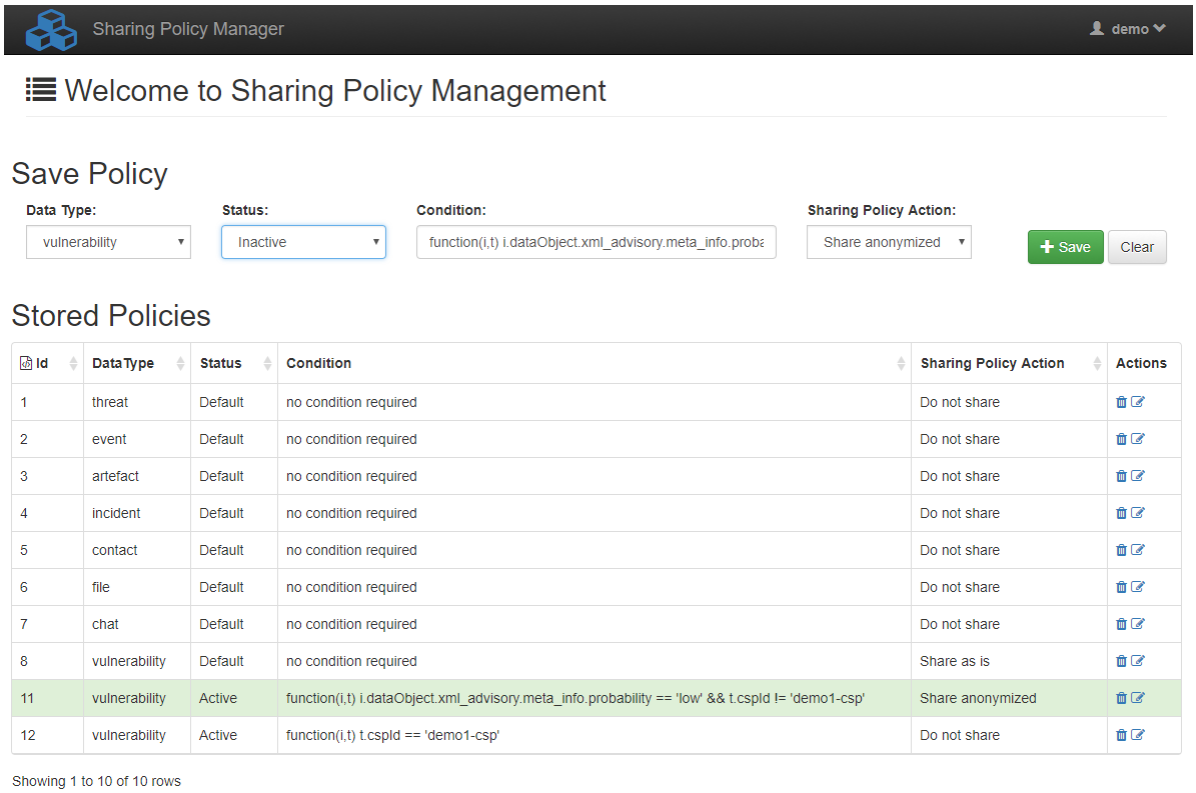


Per example, on successful save the policy with id=11 will be created:

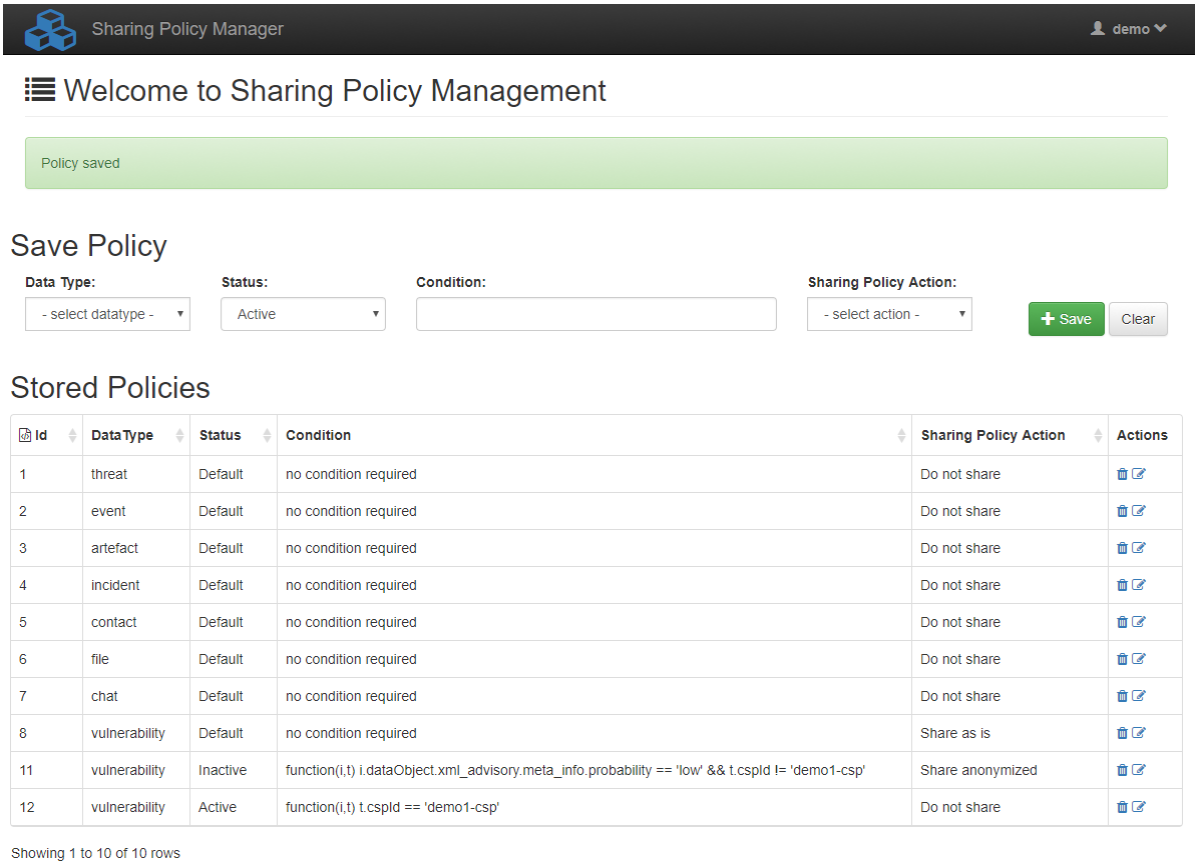


3.4 Deactivating a policy

In order to deactivate a policy, press the button to edit the policy and select “Inactive” from the “Status” dropdown list:



And save it:



4 Policy Management business logic

The CSP Integration Layer policy management engine performs data sharing policy logic. The CSP Integration Layer policy management engine supports one or more conditions to be evaluated per datatype each time an application sends a message (an IntegrationData object) through the integration layer. The engine runs for each outgoing message and each recipient. This means that if an application sends a message to the integration layer and the trust circles dictate that this message should be send to “n” external CSPs, the engine will run the whole evaluation process “n” times, once for each recipient.

A condition compares fields from the “IntegrationData” and “Team” objects and if the evaluation returns “true” it results in one of the following actions:

1. share as is (highest)
2. share anonymized (medium)
3. Do not share (lowest)

The priorities in the parentheses mean that after evaluating all the active conditions for a given datatype, the engine chooses the action with the highest priority. If no conditions are evaluated as true, it chooses the action in the “default” condition. If for some reason no active policies are evaluated as true and the default policy is missing it will fall back to “Do not share”.

Note: The Integration Layer on first installation will bundle for each datatype a default policy which the administrator can access through its UI. The default policy is “Do not share” for all datatypes. This means that a newly installed CSP will not share anything with anyone without explicit configuration.

4.1 Conditions

The condition is a JS expression evaluated in Java by using the Nashorn ScriptEngine resulting in a Lambda expression. This way the administrator can write arbitrary conditions by utilizing any of the fields from the passing objects. The objects that can be used are the “IntegrationData” and “Team” objects. The “IntegrationData” object contains all the data of the outgoing message while the “Team” object contains all the data of the current recipient.

Note: Detailed structure of the IntegratioData object for each datatype will be distributed in separate documents once the applications are integrated within the CSP platform

Examples:

```
function(i,t) t.cspId == 'demo1-csp'

function(i,t) i.dataObject.xml_advisory.meta_info.probability == 'low' && t.cspId != 'demo1-csp'
```

A condition always starts with:

```
function(i,t)
```

“I” is the “IntegrationData” object and “t” is the “Team” object

In case of an error due to a badly written condition an exception is thrown, the condition will evaluate as false and the system will log the error. The engine will continue evaluating the rest of the active conditions.

4.2 Policy examples

Let’s assume we have the following table with policies:

datatype	status	condition	action

threat	active	function(i,t) i.dataObject.ip_range == t.ip_range	Share as is
threat	active	function(i,t) i.dataObject.country == t.country	Share anonymized
threat	default	No condition	Do not share
event	inactive	function(i,t) i.dataObject.country == t.country	Share anonymized
event	default	No condition	Do not share
vulnerability	active	function(i,t) i.dataObject.xml_advisory.meta_info.probability == 'low' && t.cspId != 'demo1-csp'	Share anonymized
vulnerability	active	function(i,t) t.cspId == 'demo1-csp'	Do not share
vulnerability	default	No condition	Share as is

If a message of datatype “threat” is encountered and the recipient is team “demo2-csp”:

- If demo2-csp’s ip range is equal to the threat’s ip range, the message will be shared as is. This will happen regardless of the countries in the two objects since the action is of higher priority.
- If demo2-csp’s country is the same as the threat’s country, the message will be shared anonymized only if the ip ranges are different due to the action’s priority being lower that the one in the ip range policy.
- If both ip range and country are the same, the message will be shared as is since the ip range policy has the highest priority
- If neither the ip range nor the country are the same, the message will not be shared at all since it will fall to the default policy

If a message of datatype “event” is encountered:

- The message will not be shared at all since the only policy for events is inactive thus it will always fall to the default policy

If a message of datatype “vulnerability” is encountered and the recipient is team “demo1-csp”:

- The message will not be shared at all. This happens because the policy that would result in anonymization will always result in false while the policy that compares the cspId with the word “demo1-csp” will always result in true. Hence the action will always be not to share the message

If a message of datatype “vulnerability” is encountered and the recipient is team “demo2-csp”:

- If the vulnerability’s probability is “low”, the message will be shared anonymized. The policy that evaluates the vulnerability’s probability will result in true.
- Otherwise the message will be shared as is. None of the active policies can be true, thus is falls to the default policy

5 Anonymization Management

5.1 Introduction

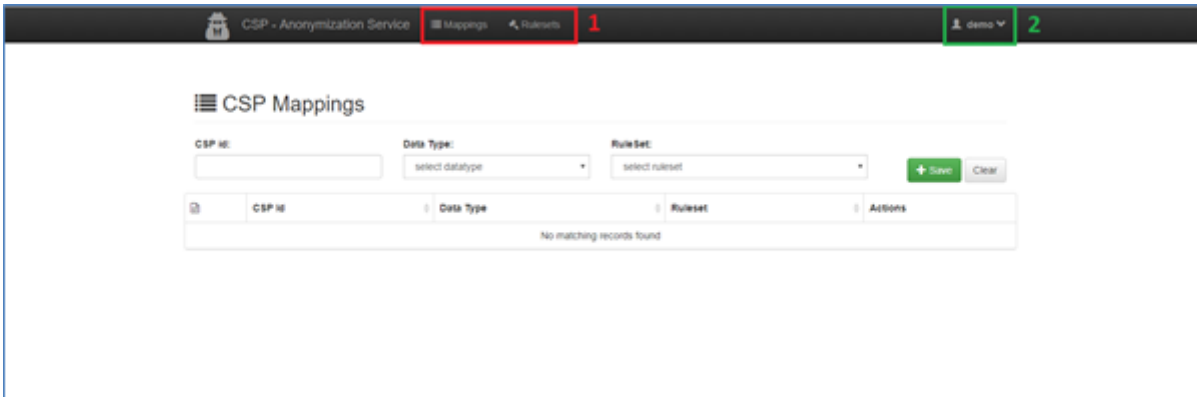
The anonymization module aims to ensure privacy through the processing of specific information in the data objects that are shared among the CSPs. Data privacy is delivered through 2 techniques, anonymization and pseudonymization.

Anonymization in an irreversible method to make unidentifiable the information that a field carries in the json structure of the data object. The anonymization application can anonymize fields that hold alphanumeric, numeric, ip and email values which overwrites with an empty string value (“”).

Pseudonymization replaces the value of the pseudonymized field with a pseudonym. This pseudonym is a value that does not allow the data to be directly identified. The pseudonym is a keyed-hash message authentication code (HMAC) and derives from a SHA256 hash function and a unique cryptographic key which changes every month. In contrast to anonymization, pseudonymization delivers a level of data privacy but not in a destructive, irreversible manner. Initial data can be reconstructed if the cryptographic key is available. The Anonymization module records the cryptographic keys that are used for the data pseudonymization each month to the local database. Hence, the authorized personnel of each CSP can obtain the key and give it to the recipient to use it to reconstruct data that were pseudonymized with that particular key.

The anonymization module can be configured through the web interface of the application, where the user can insert anonymization rules that apply to the sharing data objects. The user can insert various rulesets and differentiate the anonymization policies that will map to each datatype, applicationkey and recipient CSP respectively. The home page (mappings/) presents the existing rulesets that are mapped to specific datatypes and CSP’s as shown below. The red outline(1) denotes the navigation menu while the green outline(2) denotes the authorized user. The functionality of the application is given through the “mappings” and “rulesets” pages and described in the following chapters of the manual.

Pseudonymization on IP values is performed by the CryptoPAN tool based on the MD5 checksum of the same secret key that is used by the pseudonymization process as described previously.



5.2 Rulesets

5.2.1 Ruleset file

The anonymization policies are implemented through respective configuration files. The configuration file for each ruleset is a json that lists the actions that should be performed on each field of the sharing data object as separate rules. This json document is stored in the application database as described in the next section. Each rule is a json object that consists of 4 fields:

condition: In this field the user should fill expression that describes the json node that contains the field to anonymize/ pseudonymized. This expression follows the JSONPath syntax in the same way as XPath expressions are used in combination with an XML document. [https://github.com/json-path/JsonPath]

field: The field of the dataObject that should be anonymized/pseudonymized.

action: Defines whether the dataObject field should be:

- anonymized, by setting value “anon”
- pseudonymized by setting value “pseudo”

fieldtype: The type of the field to anonymize. It is valid only for anonymization (pseudonymization ignores the fieldtype values) and the available options are:

- “string” - For keys that hold alphanumeric values (**********).
- “numeric” - For keys that hold numeric values (00000000).
- “ip”- For keys that hold ip values (***.***.***.***).
- “email”- For keys that hold email values (****@******.**).

The presence of an array, and the application of the given rule to all elements of the array are denoted as 'node’[*]. An indicative ruleset for anonymizing an incident data object shared with a particular CSP (a part of such a json structure is shown in Table 1) is given in Table 2. This ruleset defines 5 rules for 5 respective fields of the data object.

Table 1. Part of an incident data object sample.


```
{
	"dataParams": {
		"cspId": "demo1-csp",
		"applicationId": "rt",
		"recordId": "v117",
		"originCspId": "CERT-GR",
		"originApplicationId": "rt",
		"originRecordId": "v227",
		"dateTime": "2014-11-13T07:30:17+0000",
		"url": "https://www.something.com"
	},
	"sharingParams": {
		"toShare": true,
		"isExternal": false,
		"trustCircleId": "",
		"teamId": ""
	},
	"dataType": "incident",
	"dataObject": {
		"incident": {
			"details": {
				"classification.identifier": "heartbleed",
				"classification.taxonomy": "attack on the critical infrastructure",
				"classification.type": "command and control servers for example",
				"comment": "Very serious issue",
				"destination.abuse_contact": "Mr Bill Gates",
				"destination.account": "abuse@microsoft.com",
				"destination.allocated": "1487827718",
```

```
                        "destination.as_name": "System Name",
                        "destination.asn": 123654789,
                        "destination.fqdn": "www.microsoft.com",
                        "destination.geolocation.cc": "US",
                        "destination.geolocation.city": "Seattle",
                        "destination.geolocation.country": "United States",
                        "destination.geolocation.latitude": 32.543234,
                        "destination.geolocation.longitude": 24.654321,
                        "destination.geolocation.region": "Americas",
                        "destination.geolocation.state": "Washington",
                        "destination.ip": "127.0.0.1",
                        "destination.local_hostname": "hostname",
                        "destination.local_ip": "192.168.1.1",
                        "source.reverse_dns": "www.microsoft.com",
                        "source.tor_node": true,
                        "source.url": "https://somesite.org",
                        "status": "offline",
                        "time.observation": "1487827718",
                        "time.source": "1487827715"
                    }
                }
            }
}
```


Table 2. Ruleset sample for an incident data object.


```
        {
          "rules": [
            {
              "condition": "$.incident.details",
              "field": "classification.identifier",
              "action": "pseudo",
              "fieldtype": "string"
            },
            {
              "condition": "$.incident.details",
              "field": "classification.taxonomy",
              "action": "pseudo",
              "fieldtype": "string"
            },
            {
```

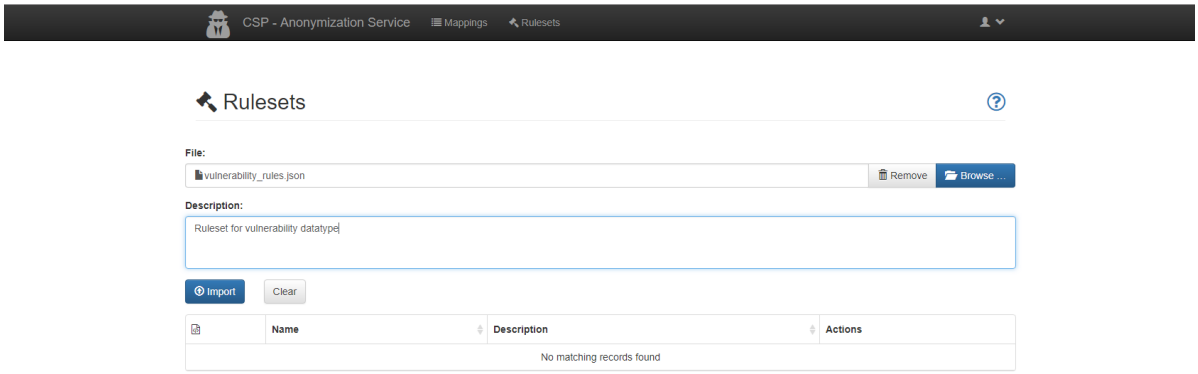
```
            "condition": "$.incident.details",
            "field": "destination.account",
            "action": "anon",
            "fieldtype": "email"
          },
          {
            "condition": "$.incident.details",
            "field": "destination.local_ip",
            "action": "anon",
            "fieldtype": "ip"
          },
          {
            "condition": "$.incident.details",
            "field": "destination.asn",
            "action": "anon",
            "fieldtype": "numeric"
          }
        ]
      }
```

5.2.2 The Rulesets page

In order to populate the anonymization module with rules mapped to the existing datatypes and CSPs, rulesets should be initially imported to the database. The ruleset file is constructed as described in the previous section and is imported through the “rulesets” page of the anonymization module as seen below. This page consists of a form with two fields:

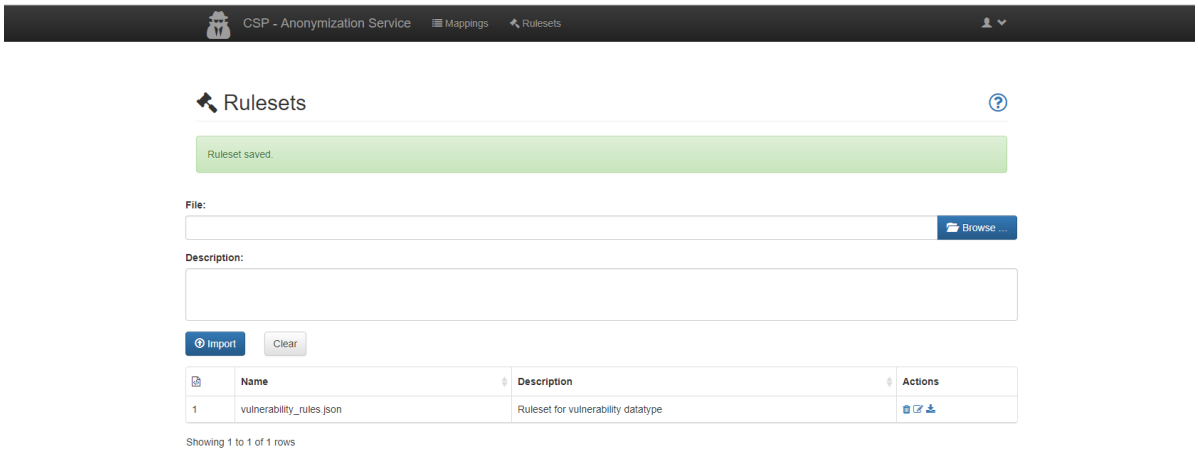
- File input field: browse your local file system and select the ruleset file to import. The field is required in order to submit the form successfully.

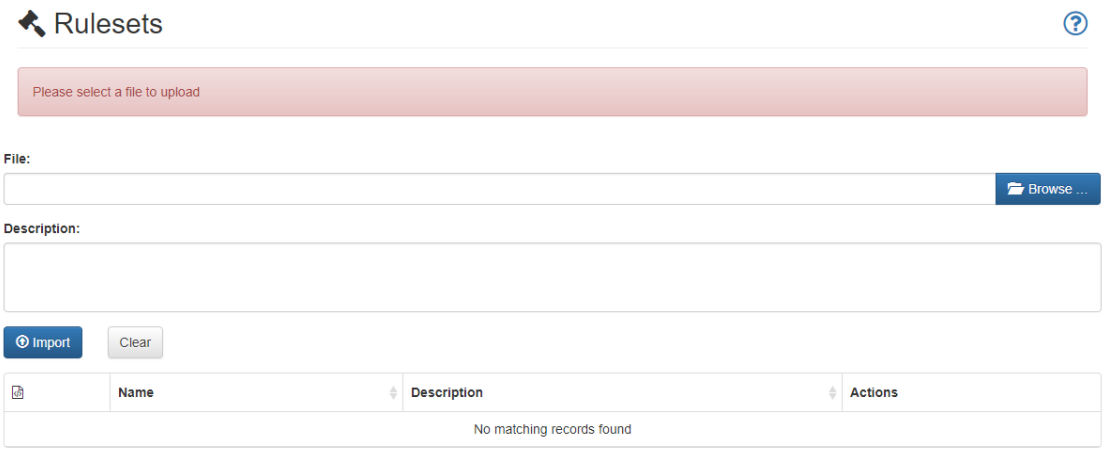
- Description text area: write a short text that describes the contents of the ruleset to import. The field is optional.

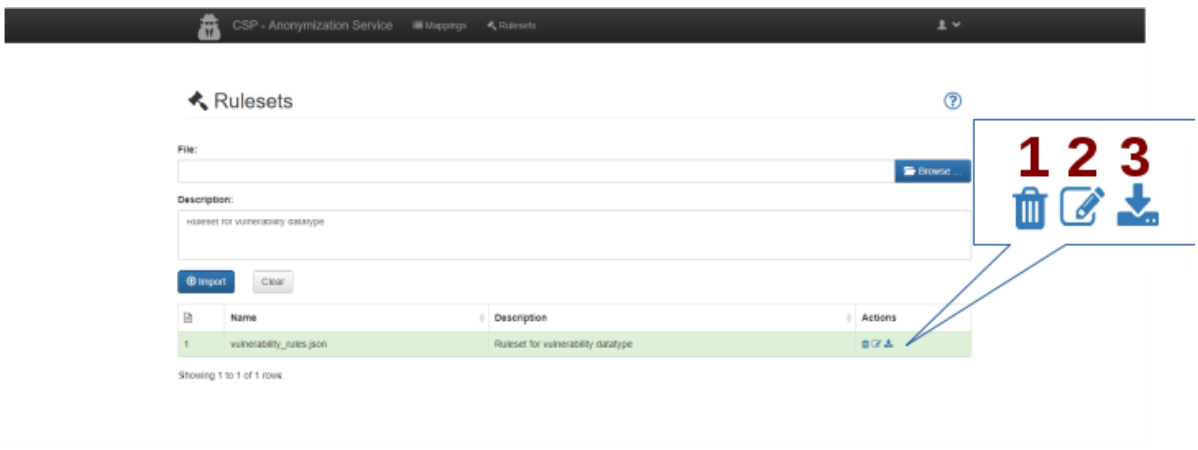


The “Import” button submits the form and saves the new ruleset. The successful status of the form submission is shown through the feedback message as seen below. If a form submission is attempted without filling the required fields of the form (the file input field) an error message warns the user and the form submission stops as seen below. After the successful submission of the ruleset, the new record is shown as a table row with 4 columns:

- **id**: order id of each row
- **Name**: the filename of the imported ruleset filename
- **Description**: the description of the ruleset (if set by the user)
- **Actions**: The user has 3 available options for handling each ruleset, namely: delete ruleset, edit and download ruleset file as seen below



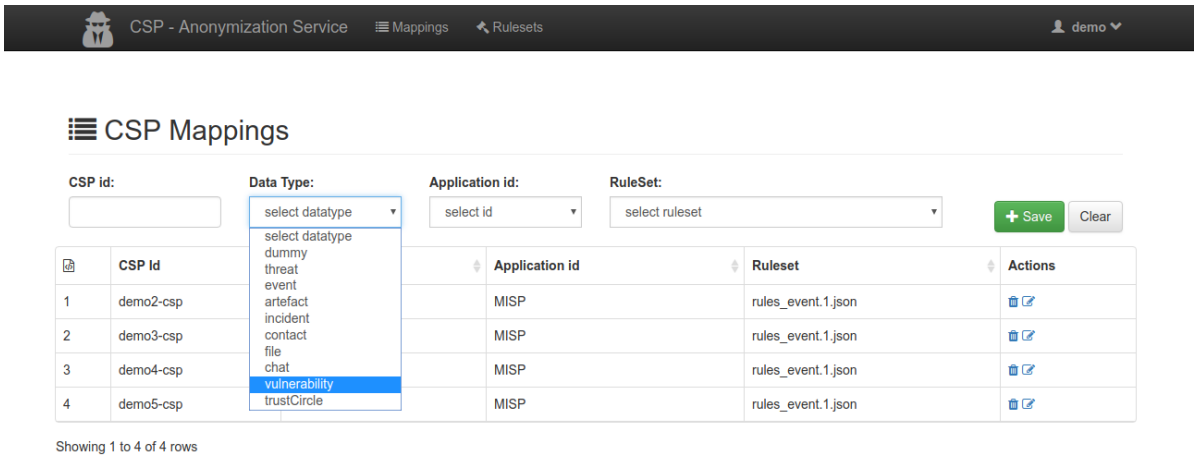


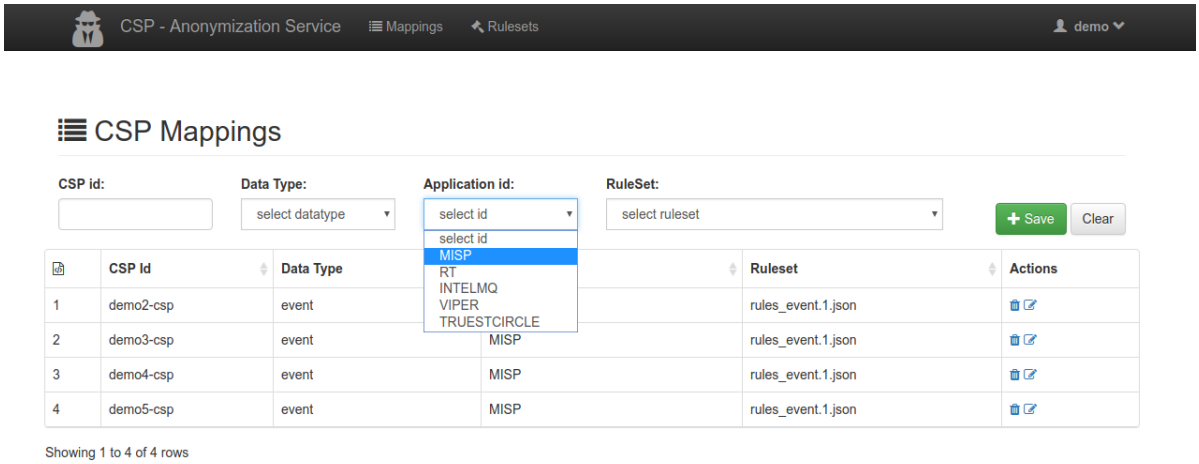


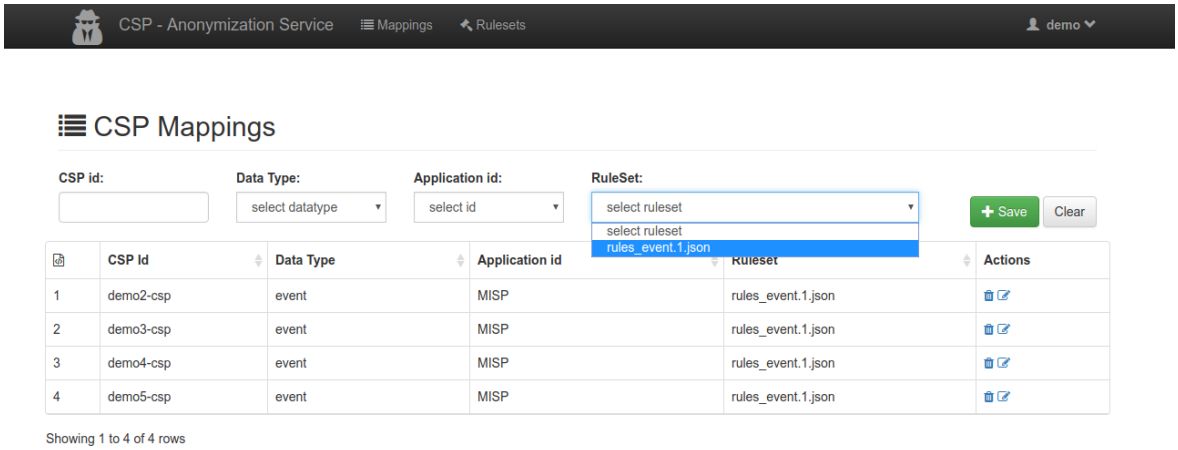
5.2.3 Mappings

When new rulesets are imported to the application's database they should be mapped to specific datatypes and CSPs in order to be applied when the anonymization service is called. This is performed through the "mappings" page of the application. To create a new mapping, 3 pieces of information need to be provided via the "mappings" page . These fields are:

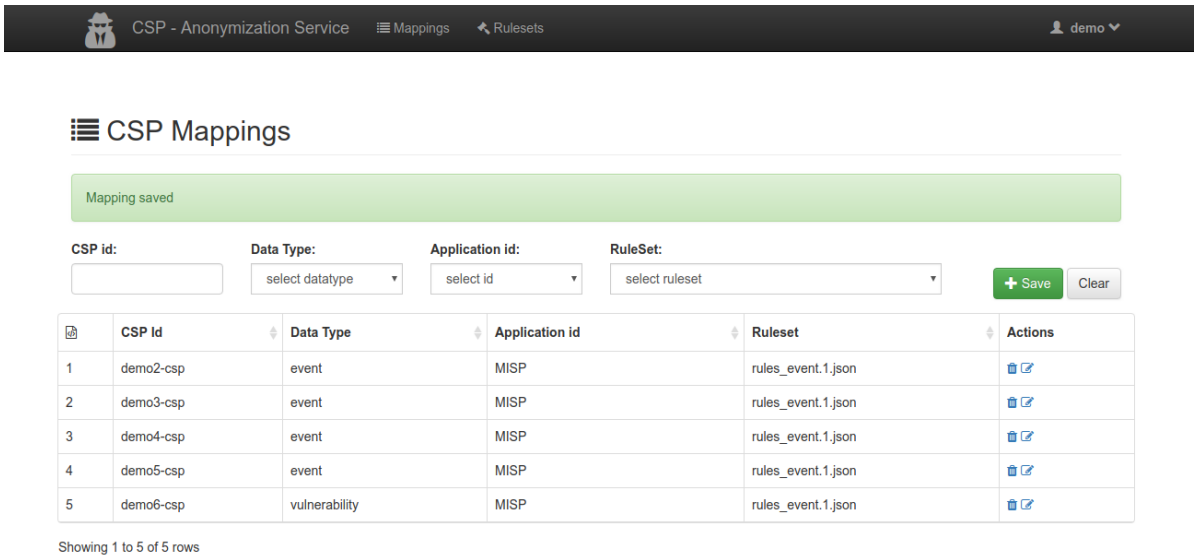
- CSP Id: A text field asking for the unique id that identifies each CSP
- Datatype: A dropdown menu populated with all the available datatypes
- Ruleset: A dropdown menu populated with the available rulesets

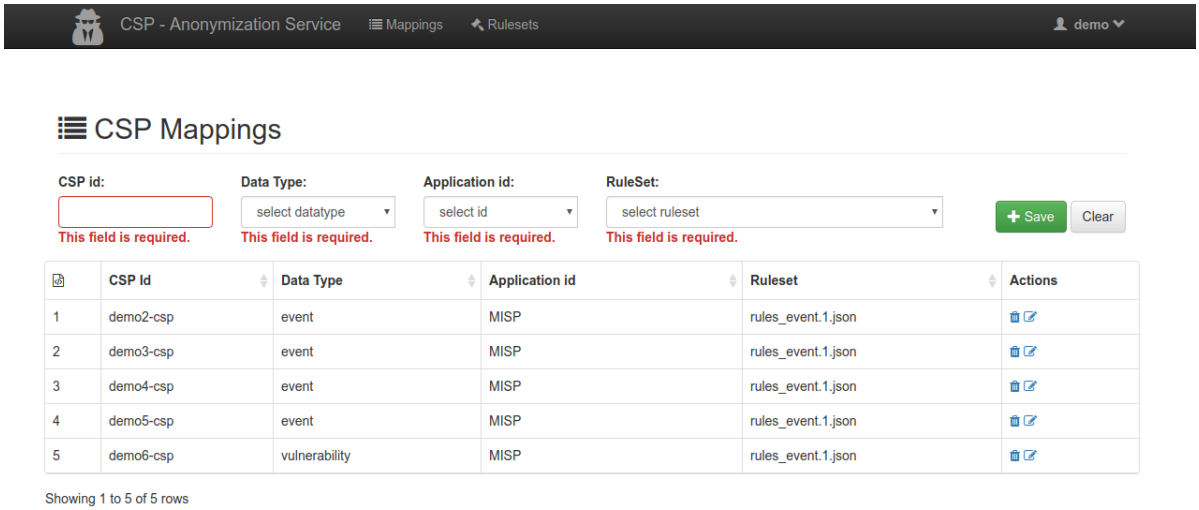






The mapping is finally created by clicking the "Save" button and a feedback message is given to the user.





Submitting the form without filling out all the three input fields is not permitted.

Edit and delete functionalities of each mapping are given in the Actions column of the table populated by the existing mapping records.

Each time the sharing policies (see previous section) dictate that a message to a specific recipient CSP should be anonymized, the anonymization module chooses the respective ruleset based on the existing mappings.

6 RT Administration

The administration of the Request Tracker instance (RT) being implemented in CSP occur according to the common rules defined. There are no special administration issues, which are CSP-specific. The common RT documentation can be accessed directly on the product web page under https://docs.bestpractical.com/rt/4.4.2/index.html. If the RT extension is used for Incident Response (RT::IR), the same condition applies. The documentation of the RT::IR is accessible on the product web page under https://docs.bestpractical.com/rtir/4.0.1/index.html.

6.1 User Management

In order to login to RT, the user has to authenticate (by using the user certificate or userid/password credentials) on OpenAM. The user has to be a member of either rt-admin or rt-user group. At the moment, OpenAM doesn't differ between those two roles, the assignment of the role is done by RT. If an authenticated user doesn't exist yet in RT, it will create an acount automatically on-the-fly and set the role as user.

There is one predefined administrator account on the RT, which can be accessed by using following credentials:

- Certificate: no certificate provided for this purpose
- Userid: rt-admin
- Password: changeit[5]

[5] We strongly recommend changing the pre-set password after the initial installation has been done (see chapter 1).

7 IntelMQ Administration

The administration functionality of IntelMQ has not been changed for the purposes of CSP. The IntelMQ documentation can be found on the product web page at https://github.com/certtools/intelmq/tree/develop/docs, the documentation on the IntelMQ Manager is provided at following web address https://github.com/certtools/intelmq-manager/tree/master/docs.

7.1 User management

As IntelMQ itself does not provide any user interaction there is no directl access to them defined in CSP. The IntelMQ Manager provides some management functionality, which is offered via web interface and should be only accessible by IntelMQ Administrator. The access is controlled by OpenAM and gained only to users, which are members of the imq-admin group. Neither IntelMQ nor IntelMQ Manager implement own user management.

There is a predefined user which is member of imq-admin group on OpenAM with following credentials:

- Certificate: no user certificate provided for this purpose
- Userid: imq-admin[6]
- Password: changeit[7]

7.2 User management

IntelMQ Manager is a graphical interface to manage configurations for the IntelMQ framework. CSP IntelMQ configuration is like every IntelMQ configuration a set of config files which describe which bots and processing steps should be run in which order. It is similar to describing the dataflow in dataflow oriented languages. IntelMQ Manager is therefore an intuitive tool to allow non-programmers to specify the data flow in IntelMQ.

7.3 Screenshots

Here some Screenshots to improve understanding the CSP pipe line and Bots configuration.

7.3.1 Pipelines

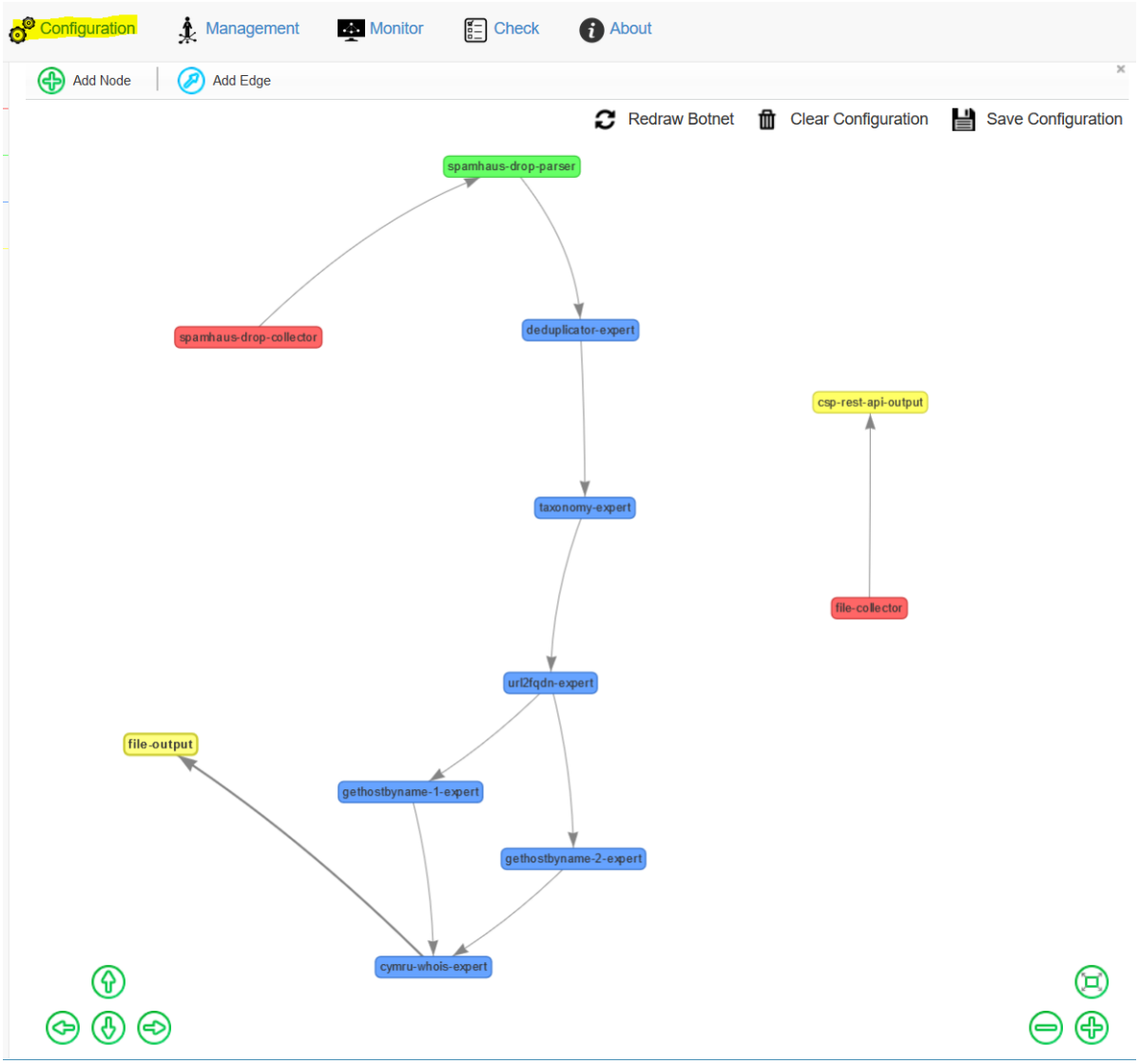
This interface lets you visually configure the whole IntelMQ pipeline(s) and the parameters of every single bot. You will be able to see the pipeline in a graph-like visualisation similar to the following screenshot (click to magnify and expand):

Initially we have two pipelines in Botnet, in order to demonstrate the functionality of the IntelMQ:

- **Spamhaus pipiline**, collect and analyse information from given Spamhuas (spamhaus.org) public feed. Parse and analyse and forward these to the file-output directory as defined in the Botnet.
- **CSP Rest api pipeline**, gathers and classifies information coming from file collector. That information can be recognized as an event and will be forwarded by using CSP to the corresponding Event Management Module (MISP) for further processing.

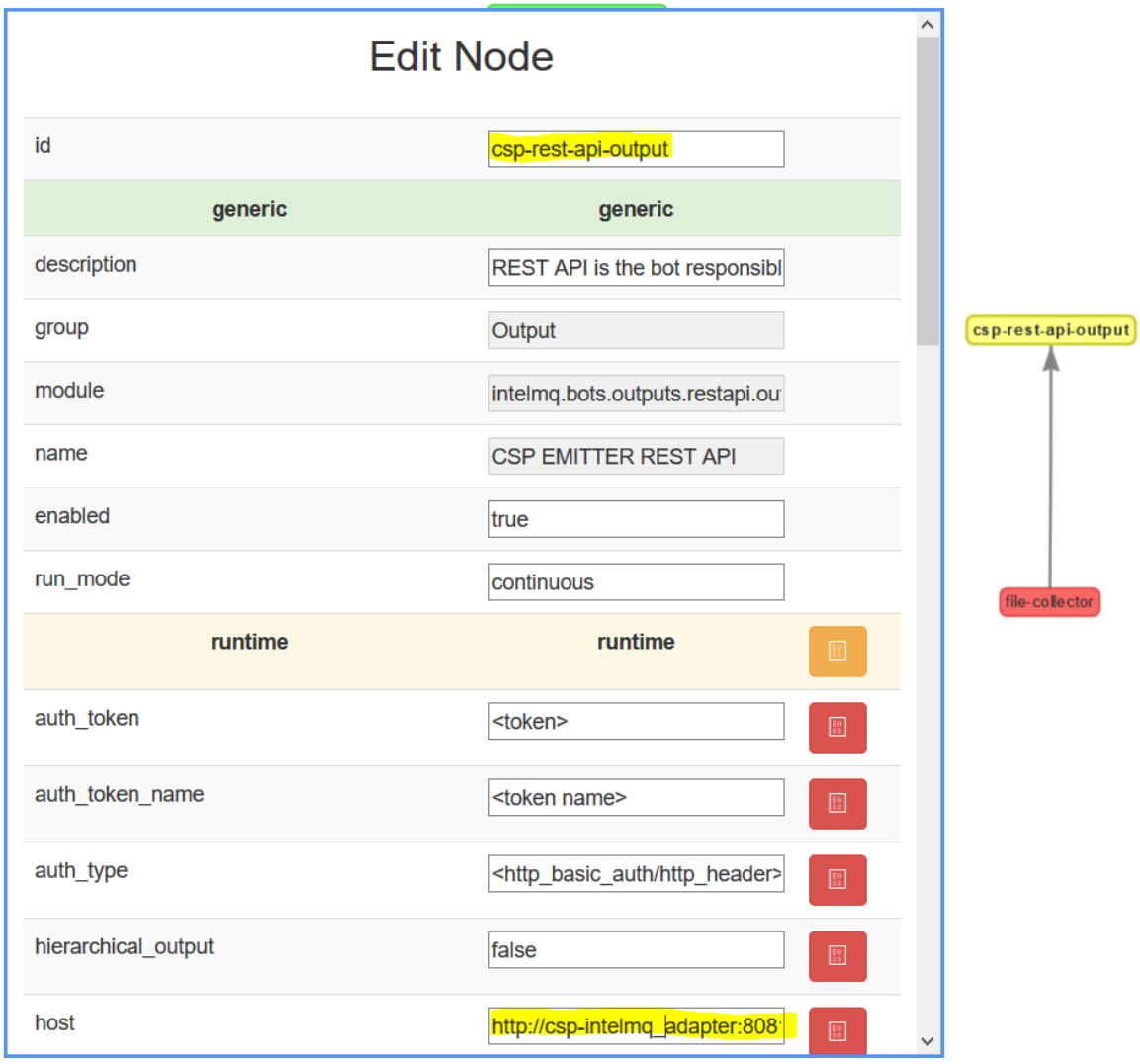
6 In general, users, which belongs to the OpenAM-group “imq-admin” have access to the IntelMQ Management Interface.

7 We strongly recommend changing the pre-set password after the initial installation has been done (see chapter 1)



7.3.2 Bots Configuration

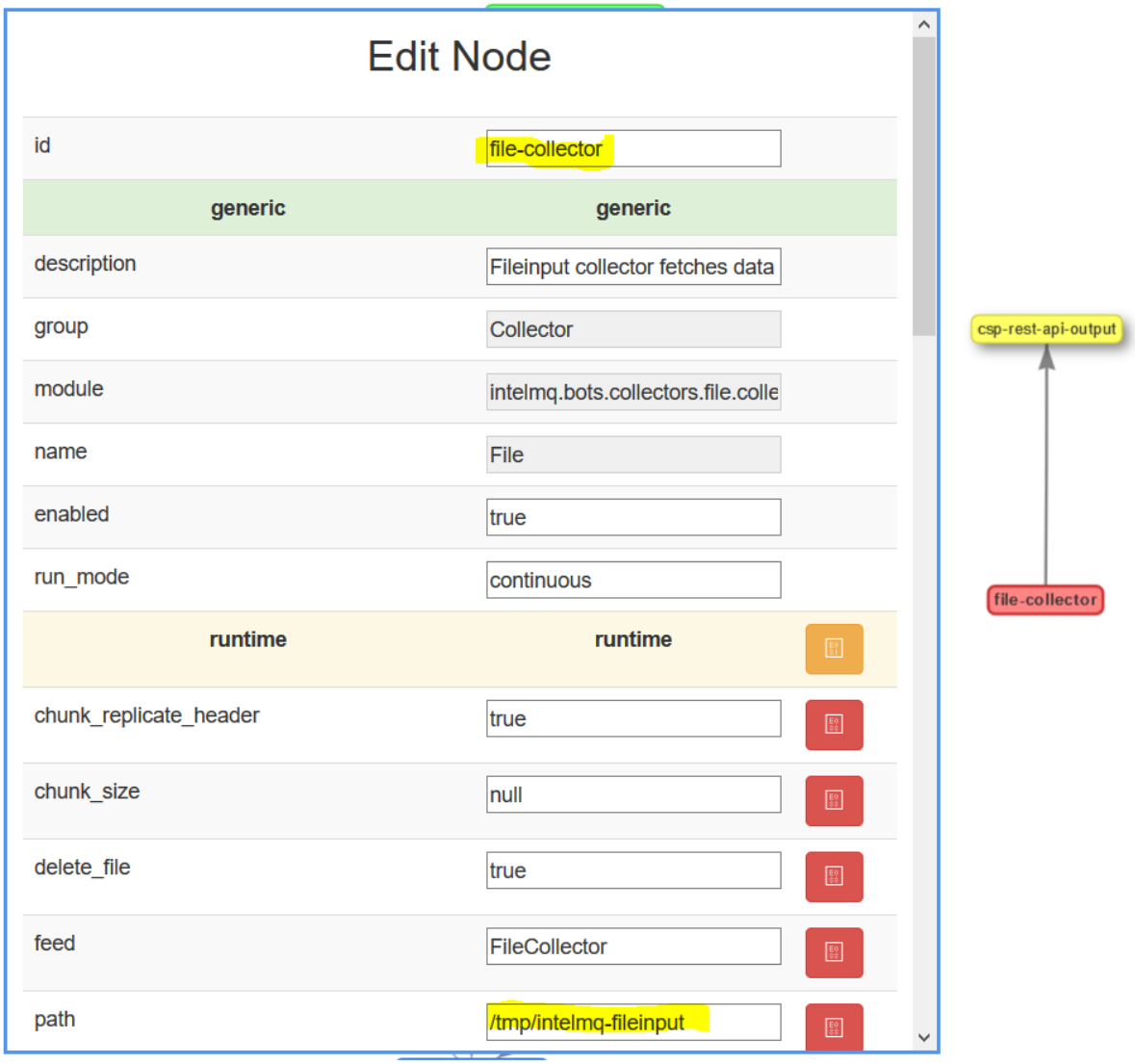
When you add a node or edit one you'll be presented with a form with the available parameters for a bot. There you can easily change the parameters of the csp-rest-api-output as show in the screenshots:



Or change the parameters of File input collector that fetches data from a file.

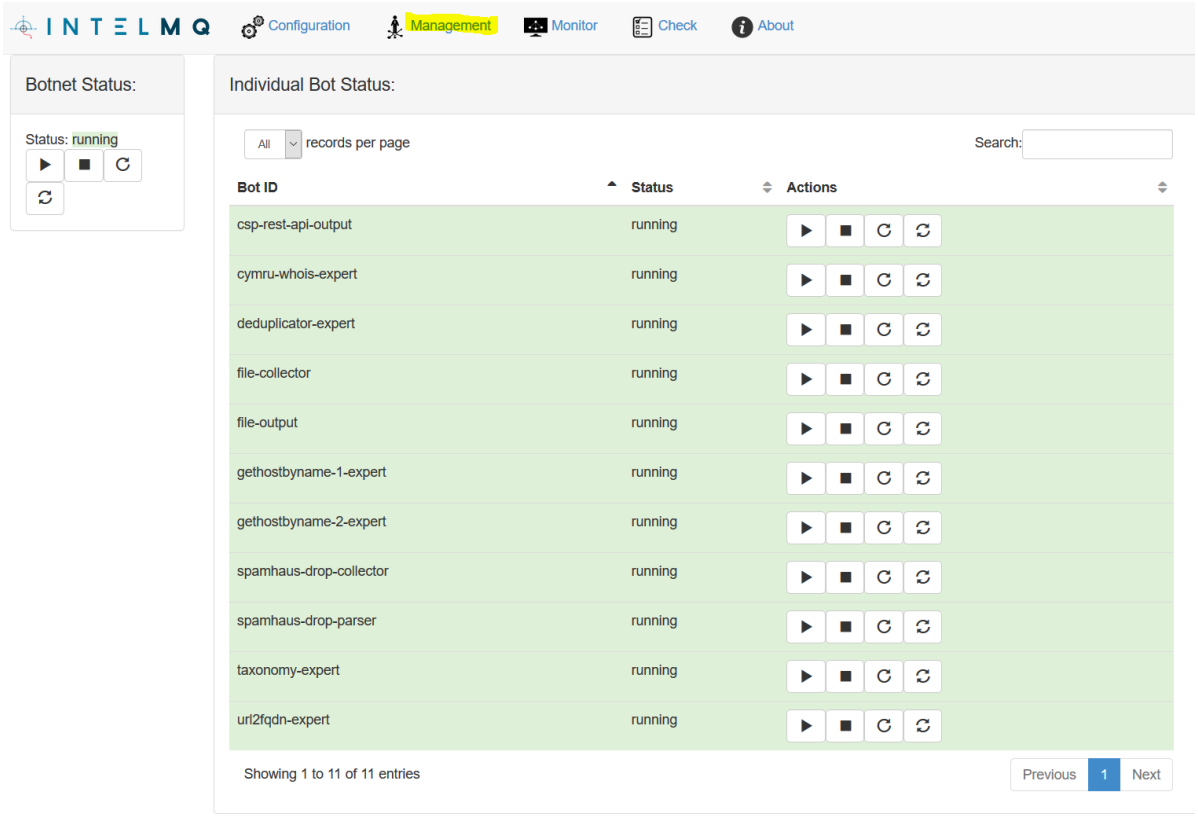
After editing the bots' configuration and pipeline, if you have changed something the "**Save Configuration**" button is highlighted yellow and blinking. Simply click "Save Configuration" to automatically write the changes to the correct files. The configurations are now ready to be deployed.

Note: if you do not press "**Save Configuration**" your changes will be lost whenever you reload the web page or move between different tabs within the intelmq manager page.



7.3.3 Botnet Management

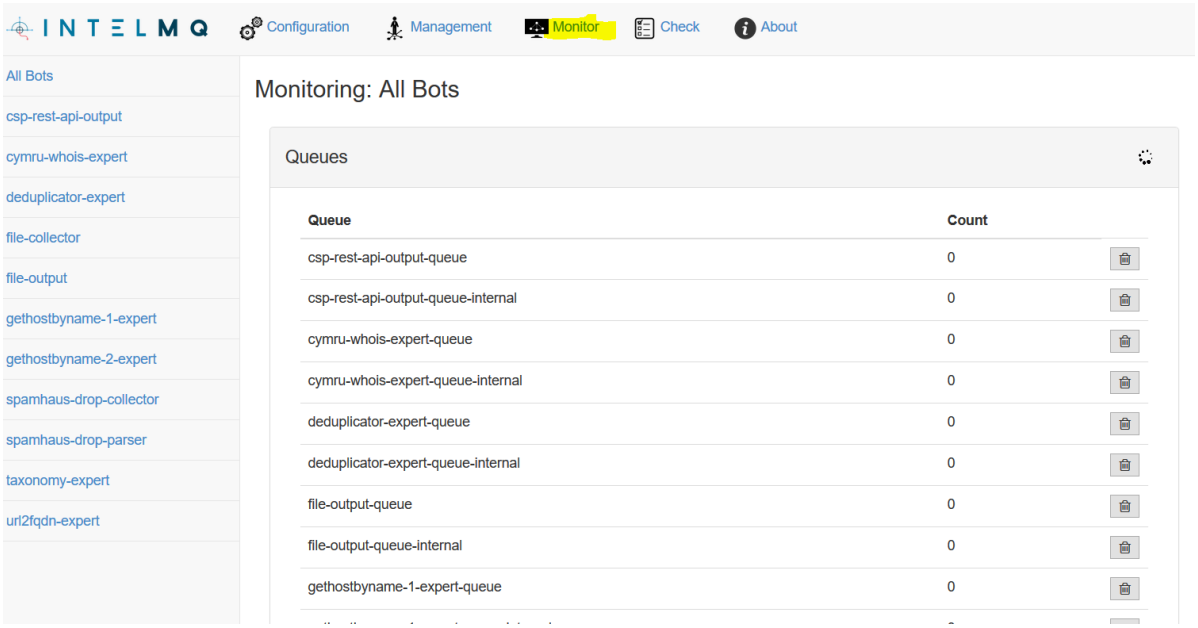
When you save a configuration you can go to the 'Management' section to see what bots are running and start/stop the entire botnet, or a single bot.



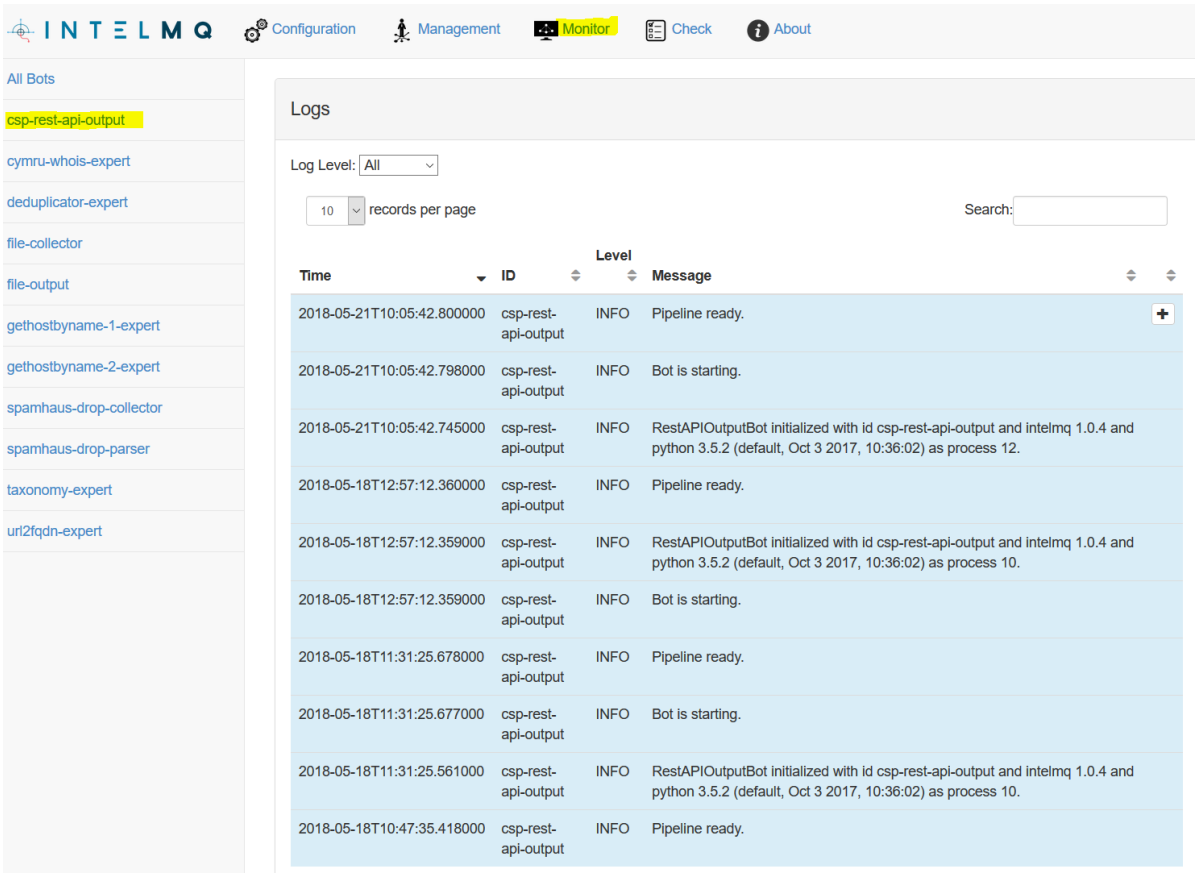
7.3.4 Botnet Monitoring

You can also monitor the logs of individual bots or see the status of the queues for the entire system or for single bots.

In this next screenshot we can see the number of queued messages for all the queues in the system.



The following example we can see the status information of a single bot **csp-rest-api-output**. Namely, the number of queued messages in the queues that are related to that bot and the last 10 log lines of this bot.



8 MISP Administration

This chapter aims to describe step-by-step the procedures required to successfully administer the MISP (Malware Information Sharing Platform - http://www.misp-project.org) instance within a CSP. The guide is divided into two sections, regarding a) steps required immediately after installation so as to have a healthy-running MISP module within the CSP and b) the continuous management/administration for day-to-day operations.

8.1 After installation

This section describes the required steps that are to be executed right after the successful installation of MISP module within a CSP in order to take advantage of CSP features together with MISP functionality. Each of the required steps are presented in a separate paragraph.

8.1.1 First login on MISP

First, the 'misp-admin' user role needs to be linked to the default internal administrator user in MISP. To do so, the administrator must first login to MISP via OpenAM and directly after that enter the default internal MISP administrator credentials. MISP will then create the needed mapping.

After installing MISP module on a CSP the administrator (as any other user) is able to login in MISP UI via its URL: https://misp-ui.{cspId}.{domain}, where:

- {cspId} represents the CSP-ID, for example: demo1-csp
- {domain} represents the domain of the CSP, for example: preprod.melicertes.eu

When the administrator first accesses MISP on the above URL, the OpenAM login screen is presented. The administrator should login with the 'misp-admin' OpenAM credentials as follows:

MISP default username (in OpenAM)	misp-admin
MISP default password (in OpenAM)	changeit

However, for the first time, login on MISP UI via OpenAM will fail (OpenAM user won't be recognised by MISP), so the administrator will have to enter the default credentials for MISP installation in the MISP built-in login screen. The default credentials for MISP installation are:

MISP default username	admin@admin.test
MISP default password	NewP@ssword1234

The administrator will now have logged into OpenAM and MISP and the needed mapping is automatically created.

8.1.2 Update MISP Objects

After logging in for the first time, the administrator will have to check for the presence of two additional MISP Objects required for CSP functionality, within MISP installation. This can be accomplished by choosing from the main menu: Global Actions > List Object Templates. The table that will appear lists all available MISP objects. The administrator should search for two objects named: "csp-rtir" and "csp-vulnerability" and check that they are both active.

In case any of the two aforementioned objects are not listed the administrator has to press the second choice (Update Objects) on the left-most menu and verify that the two objects are finally listed.

MISP UI will respond with a flash message that 2-object templates have been added. In case MISP UI's flash message responds with message: "All object templates are up to date already." this means that no further action is required.

8.1.3 Update MISP settings

Please note that the complete guide on MISP settings can be found on MISP official website: https://www.circl.lu/doc/misp/administration/#server-settings

This section intends to present the required settings that have to be set in order to enable CSP functionality within MISP. For any other information, the administrator should refer to official MISP administration guide.

Important notice:

For changing a MISP setting the user has to double click its value and then type or select its new value, depending on the type of the setting. After setting a new value it is necessary to refresh the page and re-visit the appropriate tab on "Server Settings & Maintenance" page so as to ensure that the right setting has been entered and also saved/acknowledged by the MISP UI.

Also note that even if the following fields appear to have the correct default value, the user needs to click on the field again and enter the correct value by hand, as mentioned above.

A. Basic settings

From the main menu, select: Administration > Server Settings & Maintenance and then the tab named: "MISP settings". The following values have to be entered:

Setting	Value
MISP.live	true
Important notice: **In order to find the value of the CSP::{csp-short-name} needed for the next option you can visit Administration > List Organizations and check the existance of records in format: CSP::{csp-short-name}. It takes about 1 minute for the organizations to synchronize AFTER you change the "MISP.live" setting to "true". You will find your organization as a local organization in that list.** **The correct setting of "MISP.Org" is a requirement for the sharing via the CSP to work. So please make sure that this setting has the correct name of your organization as shown in the list of organizations.** **You can continue with the rest of the configuration and change the "MISP.Org" last**	
MISP.Org	CSP::{csp-short-name}

B. Enable Single Sign On (SSO)

From the main menu, select: Administration -> Server & Maintenance and then the tab named: "Plugin settings". From there select the pill named: "CustomAuth". The following values must be entered:

Setting	Value
Plugin.CustomAuth_enable	true
Plugin.CustomAuth_header	CUSTOM_USER_ID

Plugin.CustomAuth_use_header_namespace	true
Plugin.CustomAuth_header_namespace	HTTP_
Plugin.CustomAuth_required	false
Plugin.CustomAuth_only_allow_source	
Plugin.CustomAuth_name	External authentication
Plugin.CustomAuth_disable_logout	true
Plugin.CustomAuth_custom_password_reset	
Plugin.CustomAuth_custom_logout	/logout/

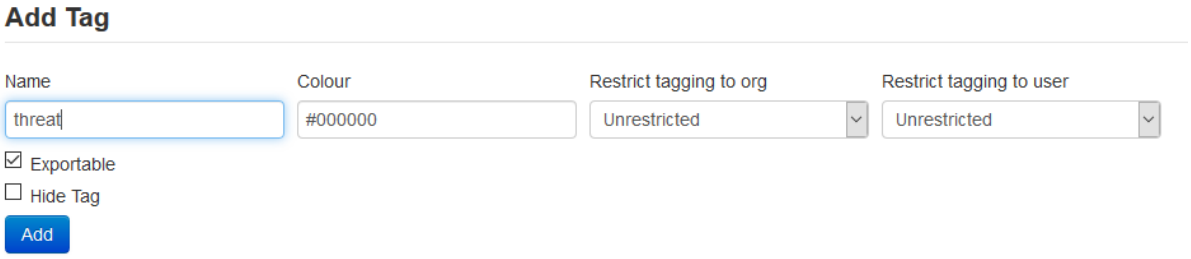
C. Enable events sharing via CSP

From the main menu, select: Administration -> Server & Maintenance and then the tab named: "Plugin settings". From there select the pill named: "ZeroMQ". The following values have to be entered:

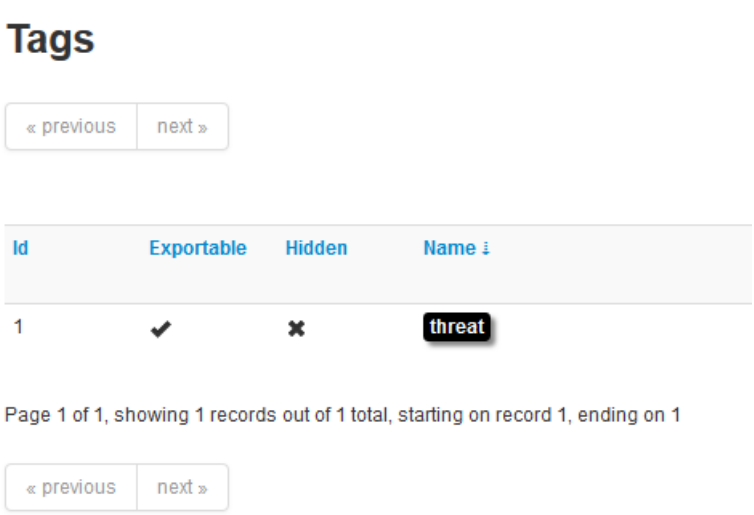
Setting	Value
Plugin.ZeroMQ_enable	true
Plugin.ZeroMQ_user_notifications_enable	true
Plugin.ZeroMQ_audit_notifications_enable	True
Plugin.ZeroMQ_event_notifications_enable	True

8.1.4 Create "threat" tag

For CSP functionality reasons the administrator has to create a tag with MISP with name "threat", colored black. This can be accomplished by selecting from the main menu: Event Actions -> Add Tag and enter the corresponding information as shown below:

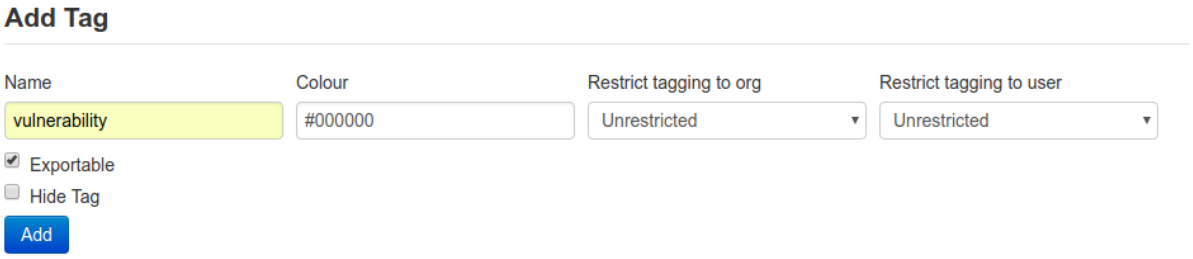


Finally, selecting the option "List Tags" from the left-most menu the following information should appear:

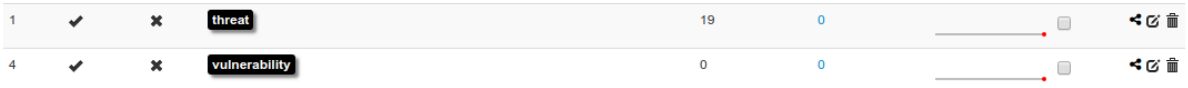


8.1.5 Create "vulnerability" tag

Similarly to the "threat" tag, the administrator has to create a tag with MISP with name "vulnerability", colored black. This can be accomplished by selecting from the main menu: Event Actions -> Add Tag and enter the corresponding information as shown below:



Finally, selecting the option "List Tags" from the left-most menu the following information should appear:



8.1.6 User management of Adminstration user

Important notice:

New users should be added after Trust Circles (TC) MISP ORG synchronization finishes, which usually lasts about 1-minute to complete. To verify that synchronization has been completed visit: Administration > List Organizations and check the existance of records in format: CSP::{csp-short-name}.

After synchronization with TCs the following steps should be executed:

1. Rename default (local) MISP user's username (the one used in first time login – see 8.1.1) from admin@admin.test to integration@melicertes.eu. This action can be executed by:
   1.1. navigating from MISP's main menu: Administration > List Users
   1.2. press edit action in the provided table for the user having email: admin@admin.test
   1.3. type the new email (integration@melicertes.eu) in the Email field
   1.4. press Submit button (and return to users table)

2. Rename MISP's default organisation from ORGNAME to {cspId}-admin, where {cspId} represents the local CSP. This action can be executed by:
   2.1. navigating from MISP's main menu: Administration > List Organizations
   2.2. press edit action in the provided table for the organisation having name: ORGNAME
   2.3. type the new Organization Identifier {cspId}-admin in the provided text field
   2.4. press Submit button (and return to organisations table)
3. Set "MISP.Org" to your organization name. This action can be executed by:
   3.1. Navigate from MISP's main menu: Administration > Server Settings & Maintenance
   3.2. Choose the "MISP Settings" tab
   3.3. Navigate to "MISP.Org" setting
   3.4. Change it from "ORGNAME" to "CSP::{csp-short-name}"

Important notice:

Finally, administrator should ensure that nobody and for no reason should ever reset the automation key of user integration@melicertes.eu, which is available from the main menu: Event Actions -> Automation

8.1.7 Creation of at least 1 Additional User Account

The standard MISP Administrator account configured above, is NOT suitable for data sharing via MISP. Additional user accounts must be created to for those users who will do data sharing via MISP. To create such user accounts, follow the following steps:

1. Create a user account in OpenAM according to the instructions in "1.2 User management"
   1.1. You may create a new user or reuse the predefined 'demo' user for initial setup hereafter
2. Create the new user (or the 'demo' user) as described in "8.2.1 User management" below.
   2.1. The text in "8.2.1 User management" gives the example for the 'demo' user.

You can now use the userid created in MISP, for MISP data sharing.

8.2 Continuous management

This section describes day-to-day operations that are required to be performed by the MISP administrator.

8.2.1 User management

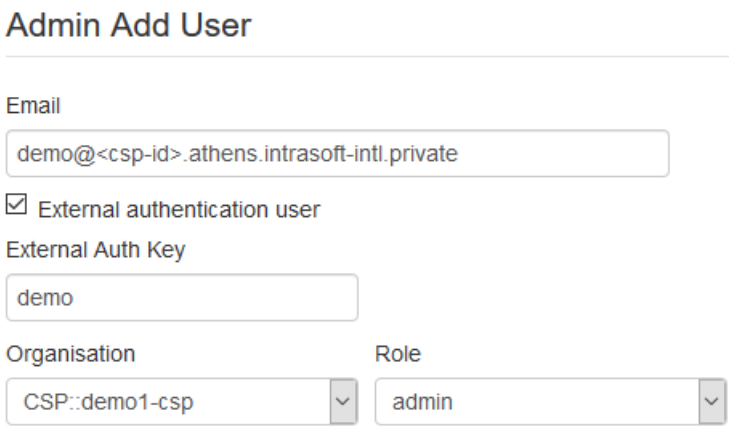
Any new user that should be able to access MISP UI should also be created in OpenAM first using the same email. When adding a new user in MISP that is also added in OpenAM the following should be considered:

- Email field in MISP should be identical with email field in OpenAM
- The "External authentication user" option should be checked in MISP
- The "External Auth Key" in MISP should be identical with UserID in OpenAM
- The Organisation option in MISP should match the CSP::{csp-short-name}

To add a new user, for the main menu select: Administration → Add User and complete the corresponding information, as presented in the following example:

Setting	Value
Email	userid@{cspid}.preprod.melicertes.eu
External Authentication user	true
External Auth Key	userid

Organisation	CSP::{csp-short-name}



8.2.2 Teams and Organizations

MISP's administrator should also take into consideration the following remarks, when managing MISP application within a CSP, regarding TC Teams and MISP's Organisations.

1. All CSP Teams from Trust Circles (TC) are synchronized as MISP Organisations every 1-minute with name in format: CSP::{csp-short-name}
2. According to MISP's policy, Organisations are never removed from MISP. This means that even if a Team gets removed from TCs, the corresponding organisations will still exist in MISP applications.
3. From TC Teams that are synchronized as MISP Organisations, one is local, representing its own organisation, and all the others are remote
4. Each MISP user that should use MISP application should exist into local MISP Organisation, as explained in previous paragraph

Important notice:

TC Teams synchronisation as MISP Organisations is an automated procedure, fully managed by the Integration Layer of the CSP and should not be intervented by the administrator. The above remarks are listed for clarification and better understanding of CSP's funtionality and integration with MISP.

8.2.3 Trust Circles and Sharing Groups

MISP's administrator should also take into consideration the following remarks, when managing MISP application within a CSP, regarding Trust Circles and MISP's Sharing Groups.

1. Local and Central Trust Circles are synchronized as MISP Sharing Groups, with name in format: CSP::LTC::{name} or CSP::CTC::{name}, where:
   1.1. LTC part stands for Local Trust Circle
   1.2. CTC part stands for Central Trust Circle
   1.3. {name} represents the name of the Trust Circle

   Listing and verification of the above can be executed by navigating from MISP's main menu to: Global Actions > Sharing Groups.
2. MISP's administrator could also add more Sharing Groups, according to MISP's own functionality, but it is noticed that only Sharing Groups that have been synchronized from Trust Circles are taken into account in CSP sharing mechanism.

Important notice:

TCs synchronisation as MISP Sharing Groups is an automated procedure, fully managed by the Integration Layer of the CSP and should not be intervented by the administrator. The above remarks are listed for clarification and better understanding of CSP's funtionality and integration with MISP.

8.3 MISP's Server Sync feature

As of version 4.2.1 CSP also supports Server Sync with MISP instances outside Melicertes ecosystem. This paragraph describes the steps CSP administrator has to take to properly configure two MISP instances towards MISP Server Sync. More on MISP Server Sync feature can be found on official MISP's website (https://www.circl.lu/doc/misp/sharing/#synchronisation).

For the conception of this manual we assume two MISP instances as follows:

- EXT MISP: a MISP instance external to Melicertes ecosystem, available at: https://misp.host.org. For the following examples and figures a random domain has been used (https://misp.dangerduck.gr)
- CSP MISP: a MISP instance within Melicertes ecosystem, available at: https://misp-ui{.cspId}{.environment}.melicertes.eu. For the following examples and figures debug CSP ID in the preprod environment has been chosen (https://misp-ui.debug.preprod.melicertes.eu)

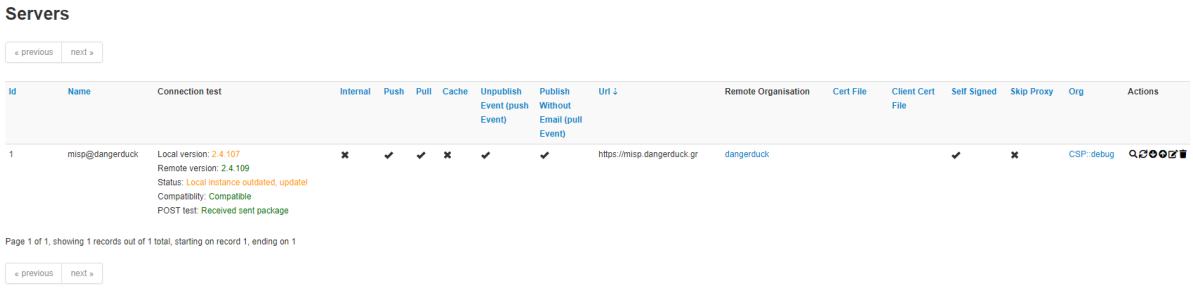
Important notice:

The MISP Server Sync feature is supported in CSP only after 4.2.1 version.

8.3.1 Connect CSP MISP with EXT MISP

Connecting a MISP instance, which is external to Melicertes, with a CSP MISP instance (within Melicertes) can be achieved by following the official MISP website (https://www.circl.lu/doc/misp/sharing/#synchronisation).

As explained in the official documentation, when everything has been properly configured, the connectivity test should look like the following screenshot:



8.3.2 Connect EXT MISP with CSP MISP

Connecting a CSP MISP instance (within Melicertes) with a MISP instance, which is external to Melicertes, can be achieved based on the fundamental actions, as described in the official MISP website (https://www.circl.lu/doc/misp/sharing/#synchronisation).

However, the following points must be taken into consideration.

Url

The Base URL of the CSP MISP instance has to be in the following formation:

https://misp-ui{.cspId}{.environment}.melicertes.eu:6443, where:

- cspId: is the CSP Identification
- environment: corresponds the Melicertes environment, i.e. preprod, prod, demo, etc.

As an example, for the debug CSP in preprod environment, the MISP Base URL to be entered in the Sync Server Configuation should be: https://misp-ui.debug.preprod.melicertes.eu:6443

Remote Organization's Uuid

The CSP MISP instance has to registered as "New external organisation" in the Organisation Type field and the proper Remote Organisation Uuid must be set, which can be retrieved by the MISP settings Administration submenu of the CSP MISP instance (Administration → Server Settings and Maintenance → MISP settings → MISP.uuid)

Authkey

The CSP MISP API Key must be set and can be retrieved by the following pages in the CSP MISP instance:

Event Actions → Automation, or Global Actions → My Profile → Authkey.

Certificates

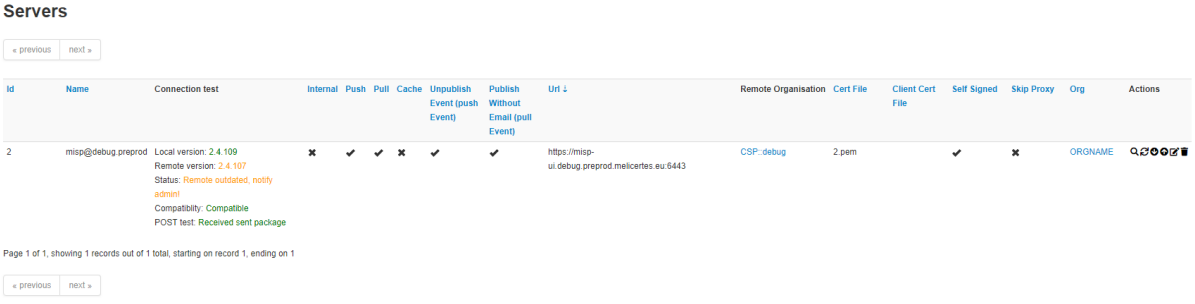
A server certificate has to be provided in *.pem format which must correspond to "CA Bundle.crt" as explained in chapter 3 of CSP Installation Manual.

In case *.pem formatted certificate, as originally emailed to you by the DFN-CERT PKI is not available to you, you may create it with the "CA Bundle.crt", as follows:

```
# openssl x509 -in common-external-ca.crt -out common-external-ca.pem -outform PEM
```

where common-external-ca.crt stands for the "CA Bundle.crt", and can be also found in "/opt/csp/apache2/ssl/ca" directory of your CSP instance.

Provided that the described configurations have been properly set, the connectivity test should look like the following screenshot:



9 Viper Administration

After the successful installation of the Viper module the only action that needs to be taken is the configuration of the Viper-VirusTotal integration. Particularly, the administrator should enter the csp-viper container:

```
$docker exec -ti csp-viper /bin/bash
```

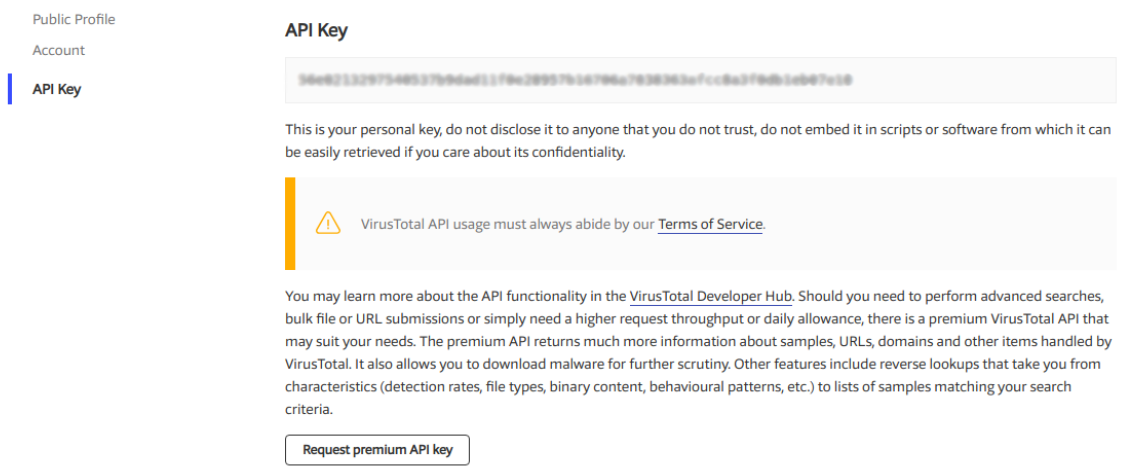
```
demo1-csp [/]# docker exec -ti csp-viper /bin/bash
root@csp-viper:/home/viper/viper# 
```

Then, the administrator should open the file */home/viper/viper/viper.conf*, find the section that refers to VirusTotal and update the virustotal_key property.

```
##
# Modules
##

[virustotal]
virustotal_has_private_key = False
virustotal_has_intel_key = False
virustotal_key =
```

The virustotal_key can be obtained from the Virus Total website (user should be logged in), and particularly from the page settings>API Key (https://www.virustotal.com/#/settings/apikey) as shown below.



Since this configuration step is completed, the csp-viper module is ready for use.

- End of document-