CEF: Cybersecurity Digital Service Infrastructure;

|  |  |
| --- | --- |
| **Version:** | **4.0.1** |
| **Date:** | **05/11/2019** |

Core Service Platform – SMART 2015/1089

**User Manu****al**

[1 User certificate handling 4](#_Toc7182566)

[1.1 Requesting a user certificate via MELiCERTES PKI 4](#_Toc7182567)

[1.2 Applying for the certificate 4](#_Toc7182568)

[1.3 Receiving the certificate 8](#_Toc7182569)

[1.4 How to backup of user certificate 11](#_Toc7182570)

[2 How to search and visualize data with Kibana 16](#_Toc7182571)

[2.1 Searching for Data 16](#_Toc7182572)

[2.2 Visualizing Data 18](#_Toc7182573)

[3 How to manage contacts with CMM 20](#_Toc7182574)

[3.1 Introduction 20](#_Toc7182575)

[3.2 Recording data and meta data of contacts 20](#_Toc7182576)

[3.3 Receiving data of contacts 22](#_Toc7182577)

[3.4 Recording data and meta data of local team 23](#_Toc7182578)

[3.5 Exporting local team data to FIRST 24](#_Toc7182579)

[3.6 Exporting local team data to TF-CSIRT/TI 24](#_Toc7182580)

[3.7 Importing team data from TF-CSIRT/TI 24](#_Toc7182581)

[3.8 List Local Contact entries 24](#_Toc7182582)

[3.9 Read Local Contact entry 25](#_Toc7182583)

[3.10 Delete Local Contact entry 26](#_Toc7182584)

[3.11 List Local and Central Trust Circles 27](#_Toc7182585)

[3.12 Read Local Trust Circle 28](#_Toc7182586)

[3.13 Write Local Trust Circle 28](#_Toc7182587)

[3.14 Delete Local Trust Circle 29](#_Toc7182588)

[3.15 Create a new Local Trust Circle 29](#_Toc7182589)

[4 How to manage contacts with CMM 31](#_Toc7182590)

[4.1 Introduction 31](#_Toc7182591)

[4.2 Recording data and meta data of contacts 31](#_Toc7182592)

[4.3 Receiving data of contacts 33](#_Toc7182593)

[4.4 Recording data and meta data of local team 34](#_Toc7182594)

[4.5 Exporting local team data to FIRST 35](#_Toc7182595)

[4.6 Exporting local team data to TF-CSIRT/TI 35](#_Toc7182596)

[4.7 Importing team data from TF-CSIRT/TI 35](#_Toc7182597)

[4.8 List Local Contact entries 35](#_Toc7182598)

[4.9 Read Local Contact entry 36](#_Toc7182599)

[4.10 Delete Local Contact entry 37](#_Toc7182600)

[4.11 List Local and Central Trust Circles 38](#_Toc7182601)

[4.12 Read Local Trust Circle 39](#_Toc7182602)

[4.13 Write Local Trust Circle 39](#_Toc7182603)

[4.14 Delete Local Trust Circle 40](#_Toc7182604)

[4.15 Create a new Local Trust Circle 40](#_Toc7182605)

[5 How to manage incidents with RT 42](#_Toc7182606)

[5.1 Introduction 42](#_Toc7182607)

[5.2 Incident reports management 43](#_Toc7182608)

[5.3 Creating incidents 44](#_Toc7182609)

[5.3.1 Create an incident based on event driven incident report 44](#_Toc7182610)

[5.3.2 Create an incident shared by another CSP instance 46](#_Toc7182611)

[5.4 Incident sharing 49](#_Toc7182612)

[6 How to work with IntelMQ 51](#_Toc7182613)

[7 How to manage events with MISP 52](#_Toc7182614)

[7.1 Introduction 52](#_Toc7182615)

[7.2 Event management (create/edit/delete) 52](#_Toc7182616)

[7.3 Linking event with incidents 53](#_Toc7182617)

[7.4 Event sharing 55](#_Toc7182618)

[8 How to work with Viper 57](#_Toc7182619)

[9 How to manage and join video conferences with VCB 60](#_Toc7182620)

[9.1 Introduction 60](#_Toc7182621)

[9.2 Video conferences management 60](#_Toc7182622)

[9.2.1 Create a video conference 60](#_Toc7182623)

[9.2.2 Cancel a video conference 64](#_Toc7182624)

[9.2.3 Past video conferences 64](#_Toc7182625)

[9.2.4 Managing email templates 65](#_Toc7182626)

[9.3 Video conference participation 66](#_Toc7182627)

# User certificate handling

Users 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 chosen:

1. Usage of the user certificates issued by the MELiCERTES PKI – per default enabled and could be used out of the box (see chapter 1.1)
2. Usage of own user certificates – this implies CSP has to be reconfigured in order to support this case – see Administration Manual.Requesting

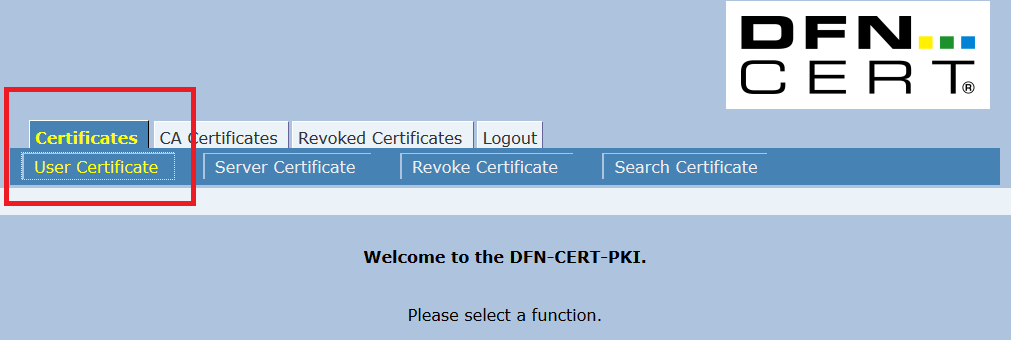
## Requesting a user certificate via MELiCERTES PKI

In order to use a certificate driven login into CSP, a user certificate with corresponding software token (private key) is required. Such certificate, inclusive token, can be obtained by performing the steps described in this section.

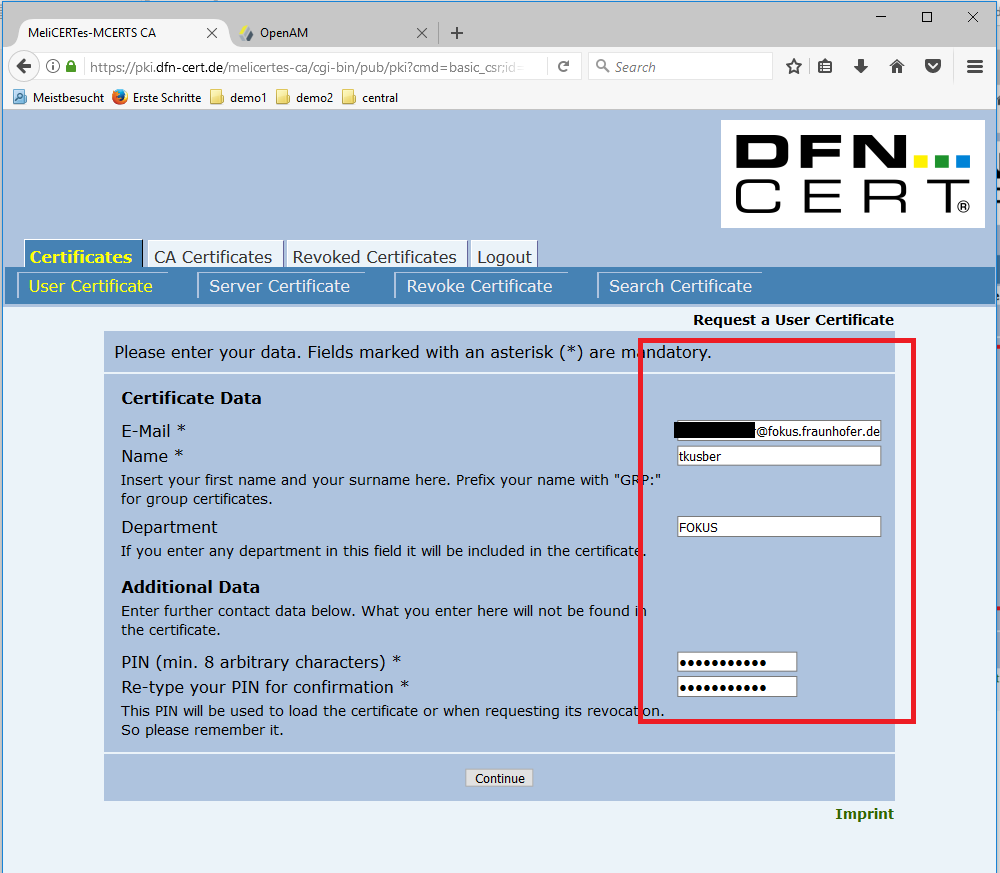
**Note! Only Firefox and Internet Explorer are currently supported.**

## Applying for the certificate

Go to <https://pki.dfn-cert.de/melicertes-ca/pub>. The Welcome Screen of the PKI-Site will be shown, please select the User Certificate tab.



The “Request a Client Certificate” page is displayed.



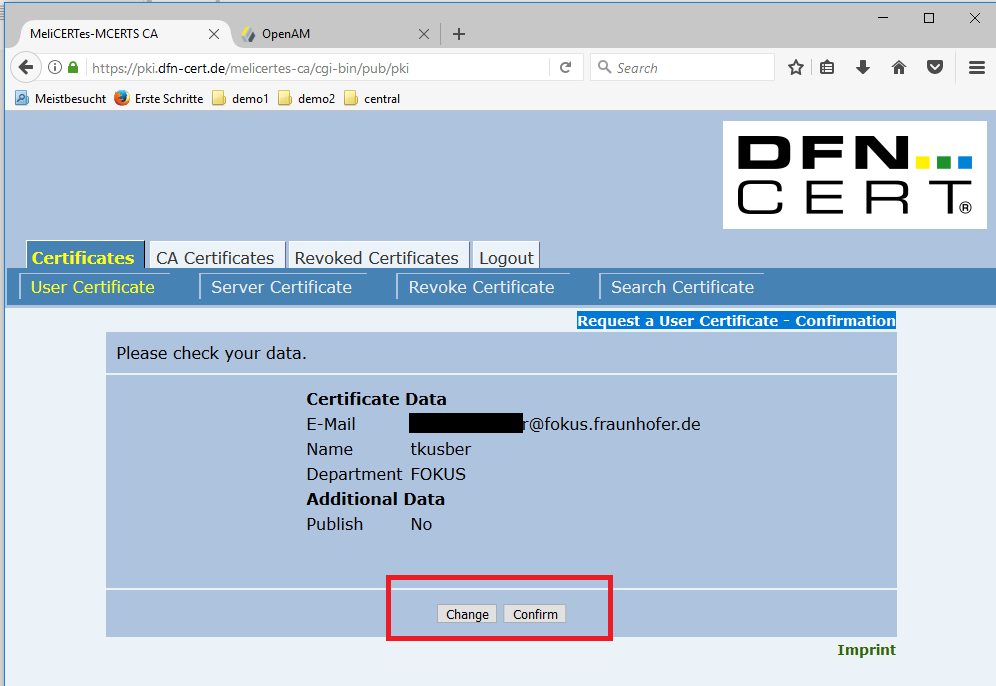
Please provide the following data:

* E-Mail: the e-mail address will be used to validate your request and to communicate the results
* Name: the provided name should cover the user name, which will be used on the CSP (uid)
* Department: (optional) the name of the department, the user is belonging to[[1]](#footnote-1)
* PIN: please type and retype a PIN (password) which will be used in case the issued certificate should be revoked

**Note! Please remember the PIN!**

**Note! Currently there is no possibility to provide any additional data, just ignore this page section.**

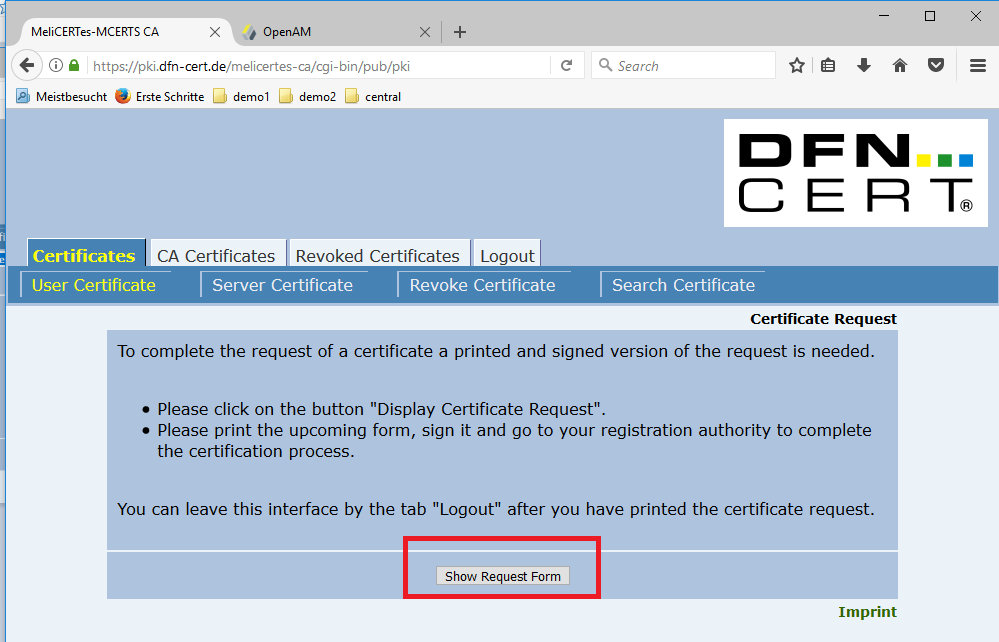
As a next step, please click on the “Continue” button. A “Request a User Certificate – Confirmation” page will be shown.



Please review the displayed information. If you noticed, some input is not correct, please click on “Change” button and adjust the information, otherwise please click on “Confirm” button to continue with application.

After the “Confirm” button has been pressed, the “Certificate Request” confirmation screen is shown. The Request has been successfully recorded, some additional paper validation by the Registration Authority (RA) has to be still done.

Please press the “Show Request Form” button



Print the resulting PDF file, fill out the necessary details (at least the application date and your signature) and submit the filled out and signed form (in scanned electronic form) to the helpdesk as a “service request”. As a subject please enter: “User certificate request - <cspId>”.

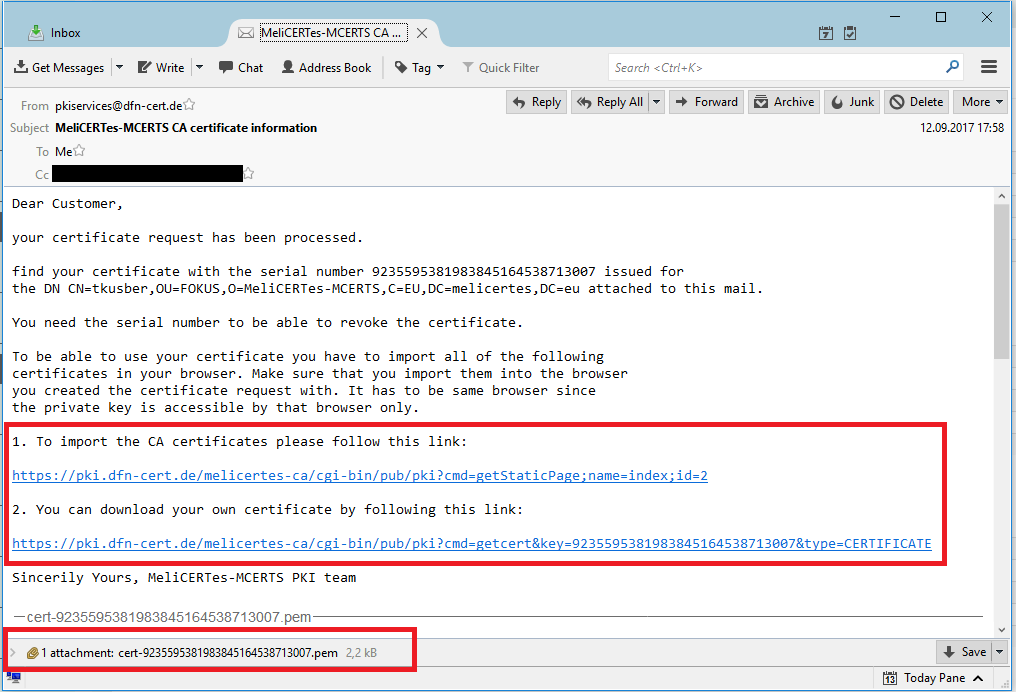


You have successfully requested a CSP user certificate.

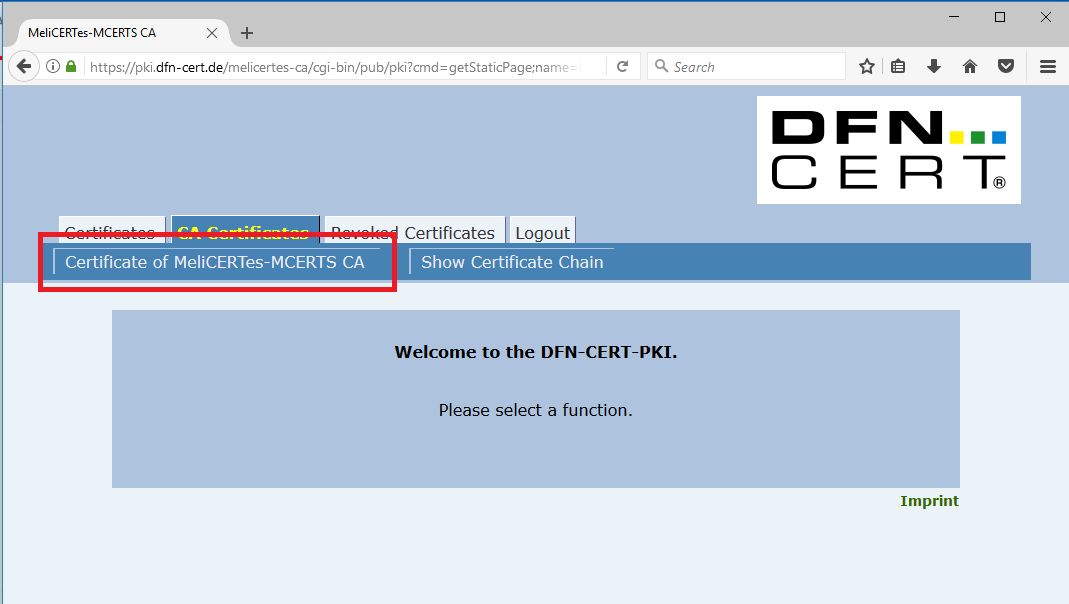
## Receiving the certificate

After the application has been approved by the RA, you will receive an email containing your certificate encoding as a pem file (see attachment). Furthermore, the email contains two links, one pointing to the corresponding certificate authority (ca) certificate and another pointing to your own certificate. By using the both links, you can install both certificates into your browser by following the instructions below.

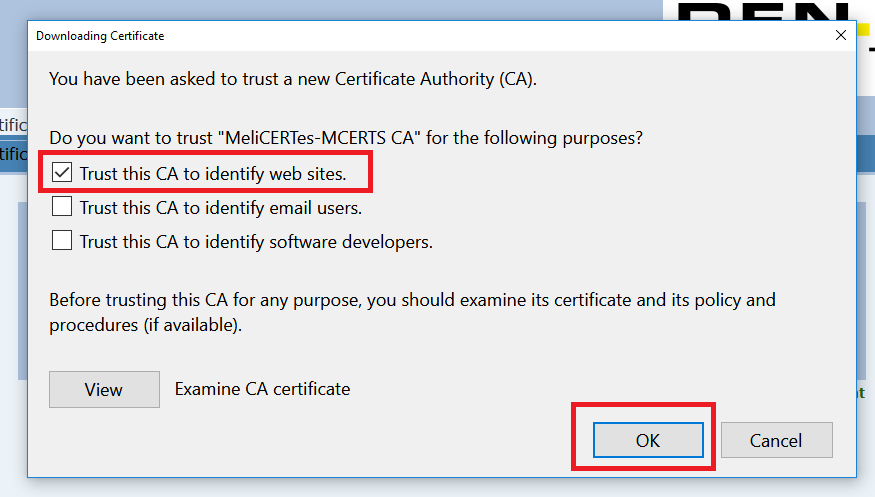
**Note! Only Firefox and Internet Explorer are currently supported. For demonstration of the following steps, a Firefox will be used.**



Please follow the first link placed in the email under “1. To import the CA certificates please follow this link”. The following screen is shown.



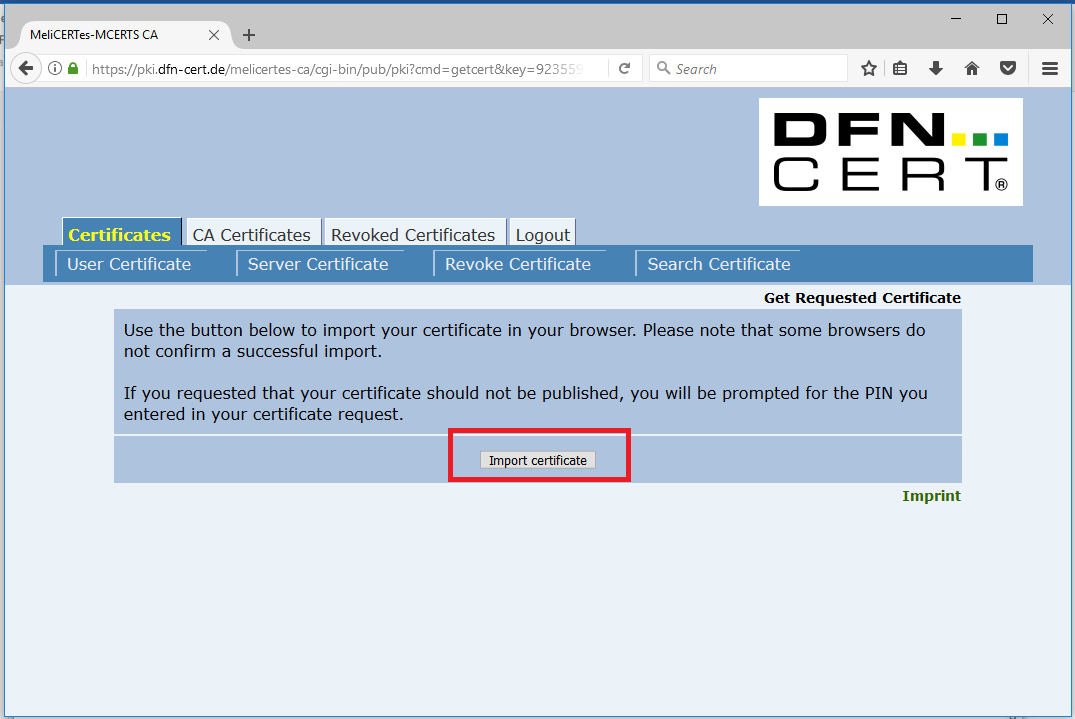
Click on the “Certificate of MeliCERTes-MCERTS CA” button in order to install ca certificate. The following screen will appear.



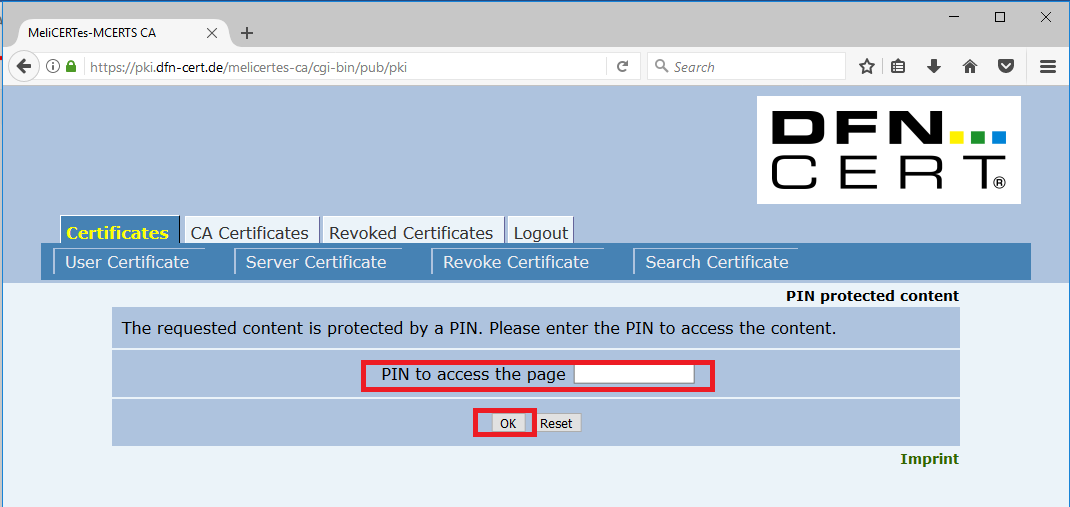
Select at least “Trust this CA to identify web sites” checkbox and confirm the import with OK button. The ca certificate has now been successfully installed in your browser.

As next step, you will install (import) your user certificate. This user certificate corresponds to the private key that has been created and stored in the browser while applying for the certificate (see chapter 1.2), thus the same browser has to be used for the installation.

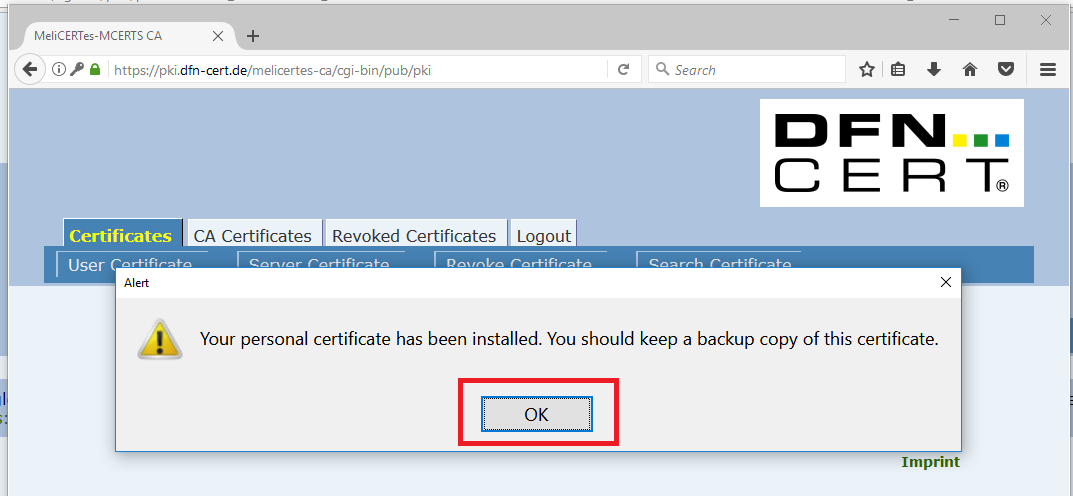
Please click the second link placed in the email under “2. You can download your own certificate by following this link”. The “Get Requested Certificate” screen is shown.



Click on the “Import certificate” button. The “PIN protected content” screen is shown.



Please, type in the PIN you set while applying for the certificate and confirm the PIN by pressing the OK button. The following confirmation dialog is shown.



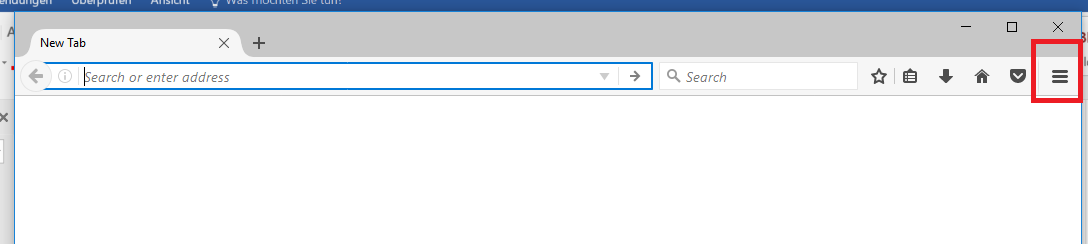
Click on the OK button, the user certificate has been successfully installed in your browser; you can use it to login into CSP.

**NOTE! Do not forget to backup your key and user certificate. Please refer to the next chapter for advice how to do that.**

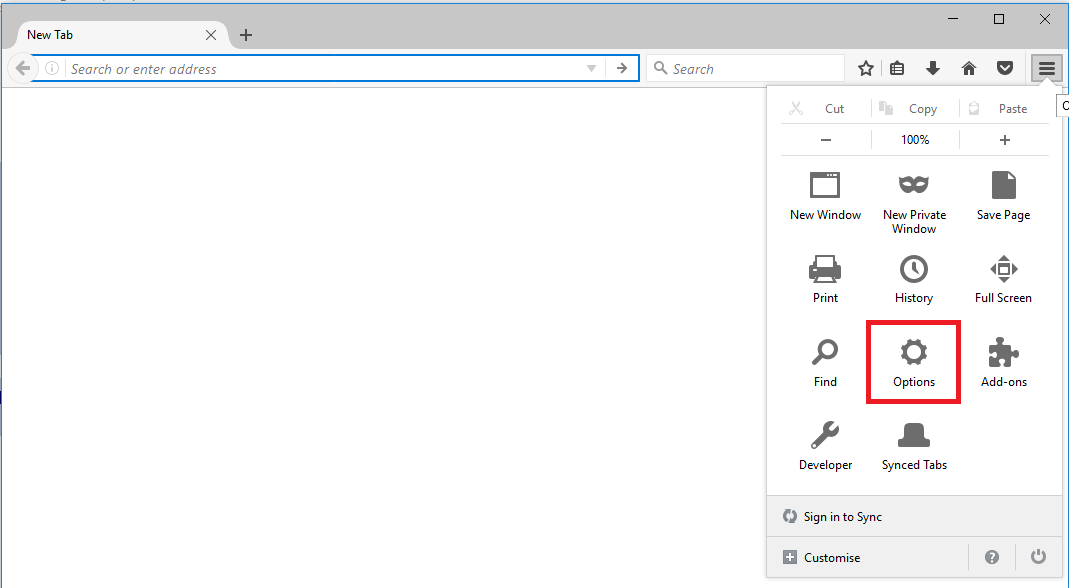
## How to backup of user certificate

In order to backup your newly issued and imported user certificate (inclusive corresponding private key) please start the browser you installed the certificate into.

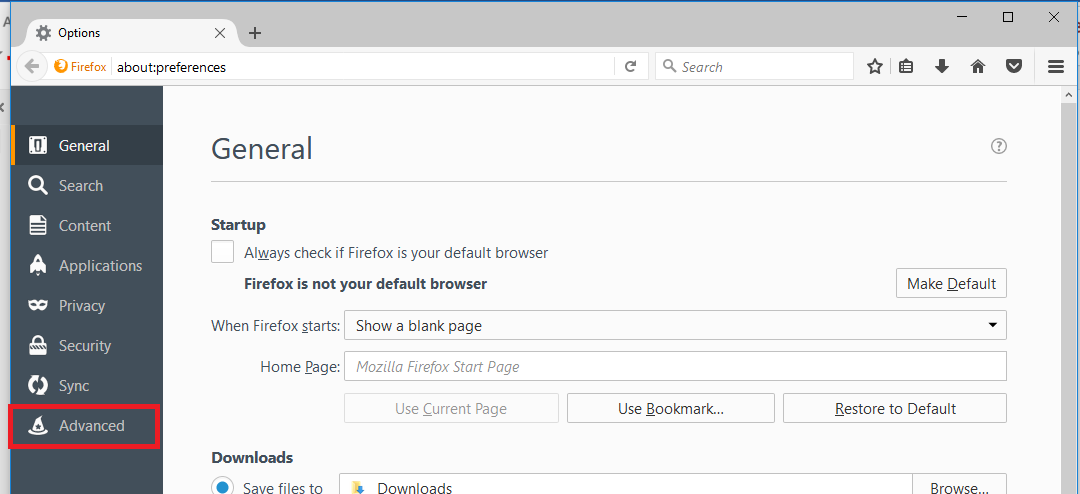
**NOTE! For the demonstration of the particular steps, a Firefox browser will be used.**



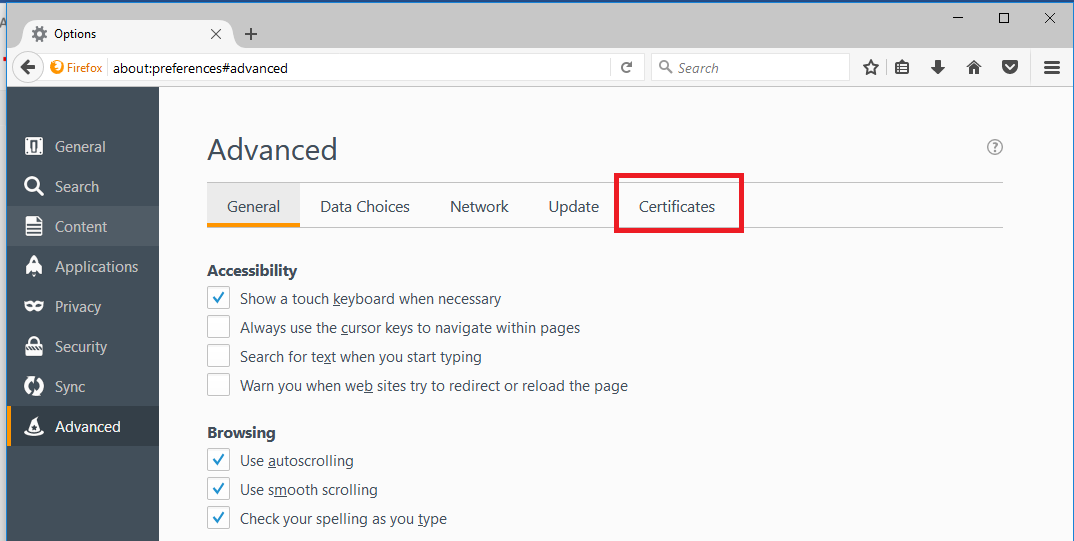
Please click on the “Open menu” button, in the upper right corner of the Firefox browser. The following screen will appear.



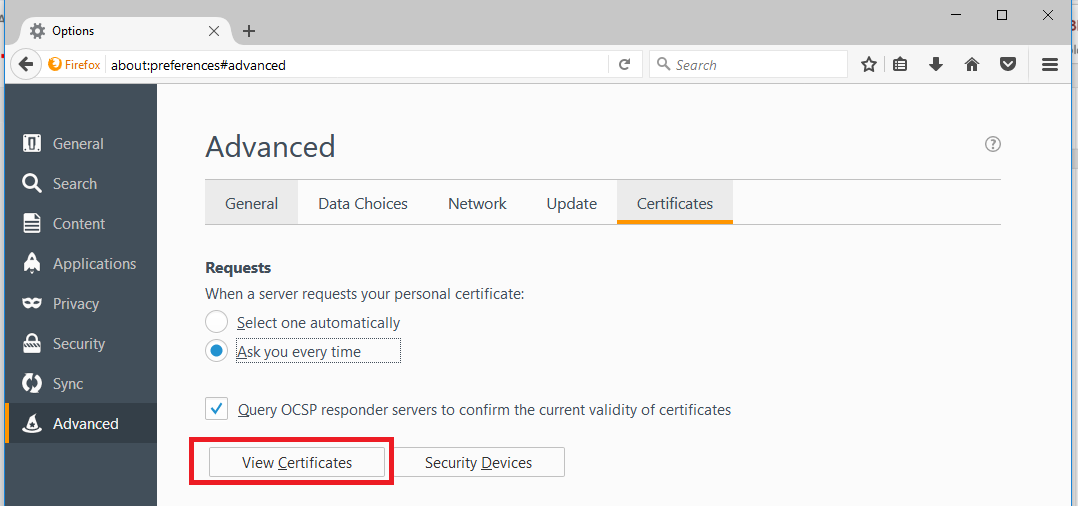
Click the Options button.



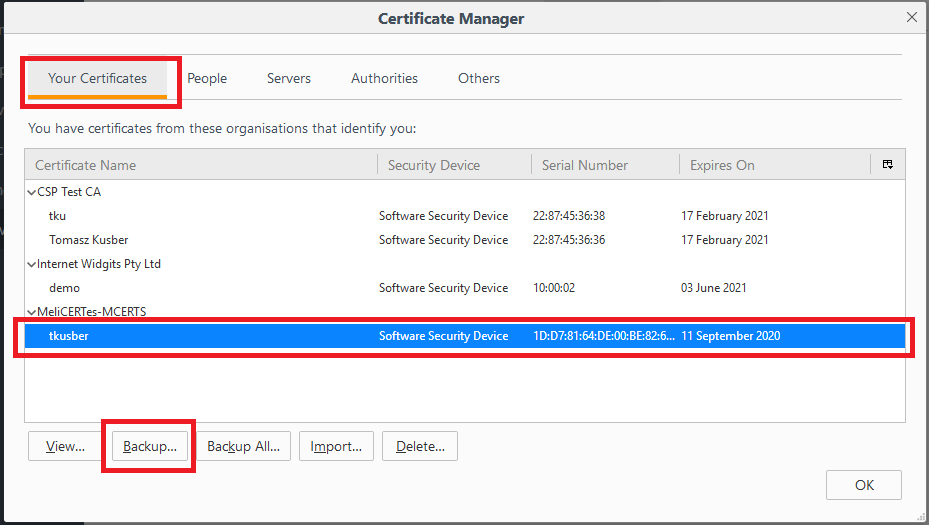
Click the Advanced tab.



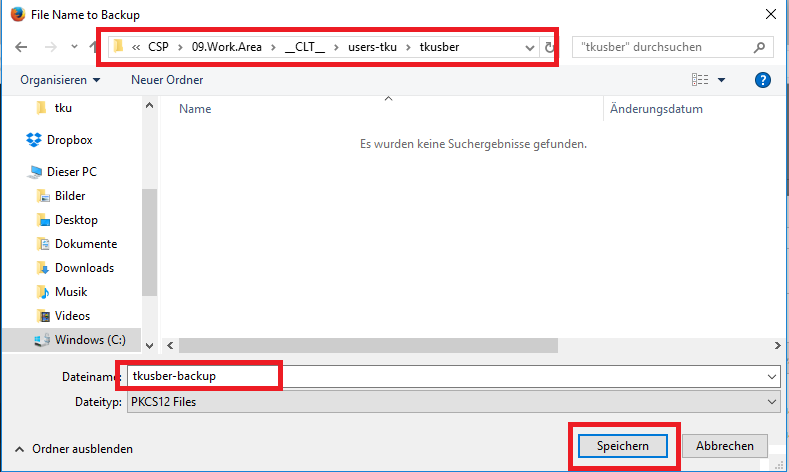
Chose the Certificates tab.



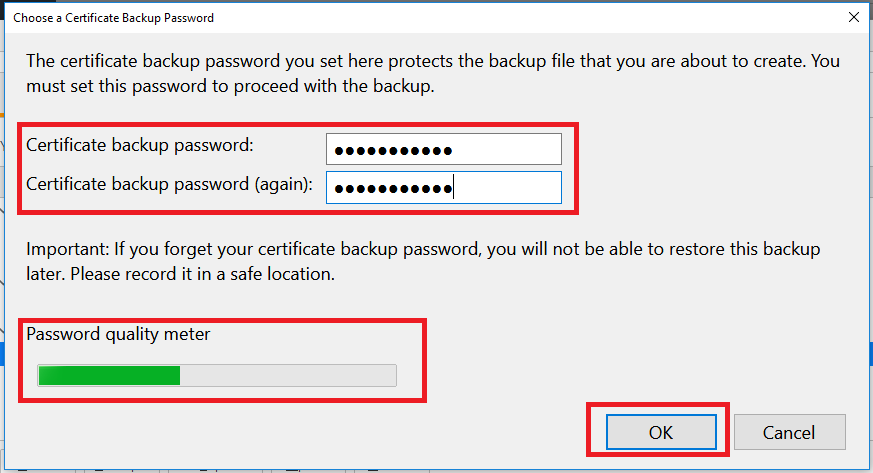
Click the View Certificates button.



Make sure the Your Certificates tab is chosen and select the newly imported certificate for backup. After selection click on the Backup... button.



Select the location the backup should be stored, provide the name of the file and confirm the operation by clicking on the Save button.



Input the password for protection the private key stored in the backup file and confirm the operation by pressing the OK button. The certificate (inclusive private key) has been successfully exported (backup).

**NOTE! It is important to choose a secure password. Therefore, in the lower left corner an indicator of how secure you password is will be displayed. The longer the green stripe, the more secure your password.**

# How to search and visualize data with Kibana

Kibana is used to search and visualize data. Kibana provides a sidebar with main options of which the first three are of interest for users, i.e. Discover, Visualize and Dashboard. Kibana is set to load the Dashboard by default when it loads.

Kibana can be accessed at

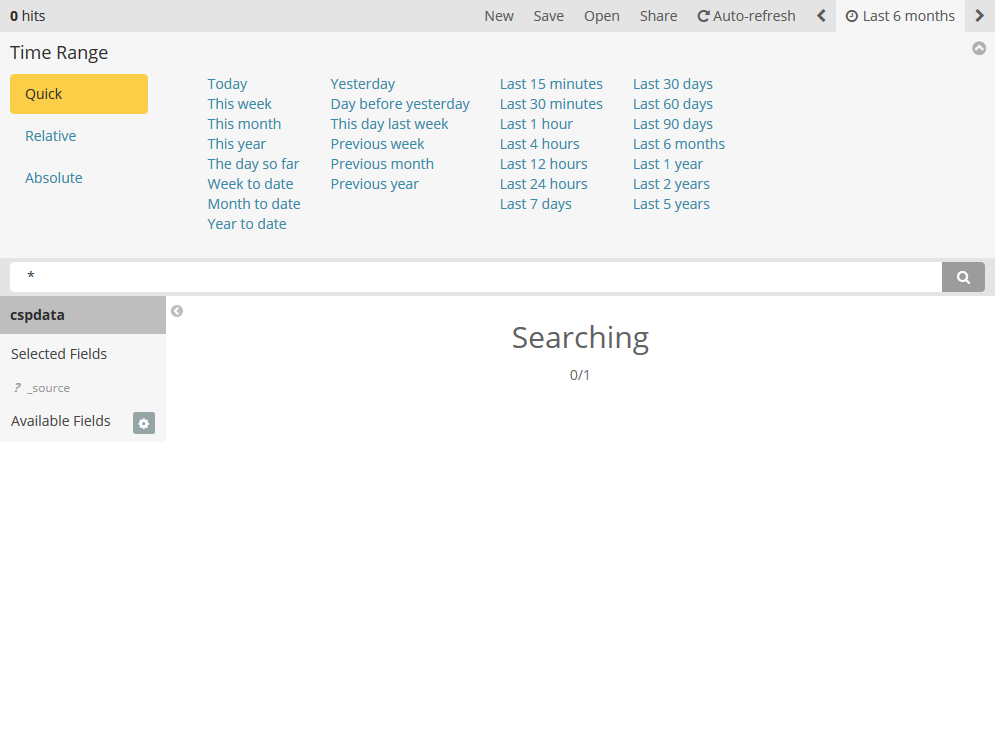
* https://search.<cspId>.[preprod.]melicertes.eu
* https://logs.<cspId>.[preprod.]melicertes.eu

The “search” instance shows all the data from all the CSP applications while the “logs” instance shows the audit and exception logs of all the CSP applications. The “logs” instance is only accessible by the CSP administrator.

## Searching for Data

To search for data, one needs to select the first link in the sidebar, i.e. “Discover”. This option allows the user to search and display raw data as well as individual attributes.

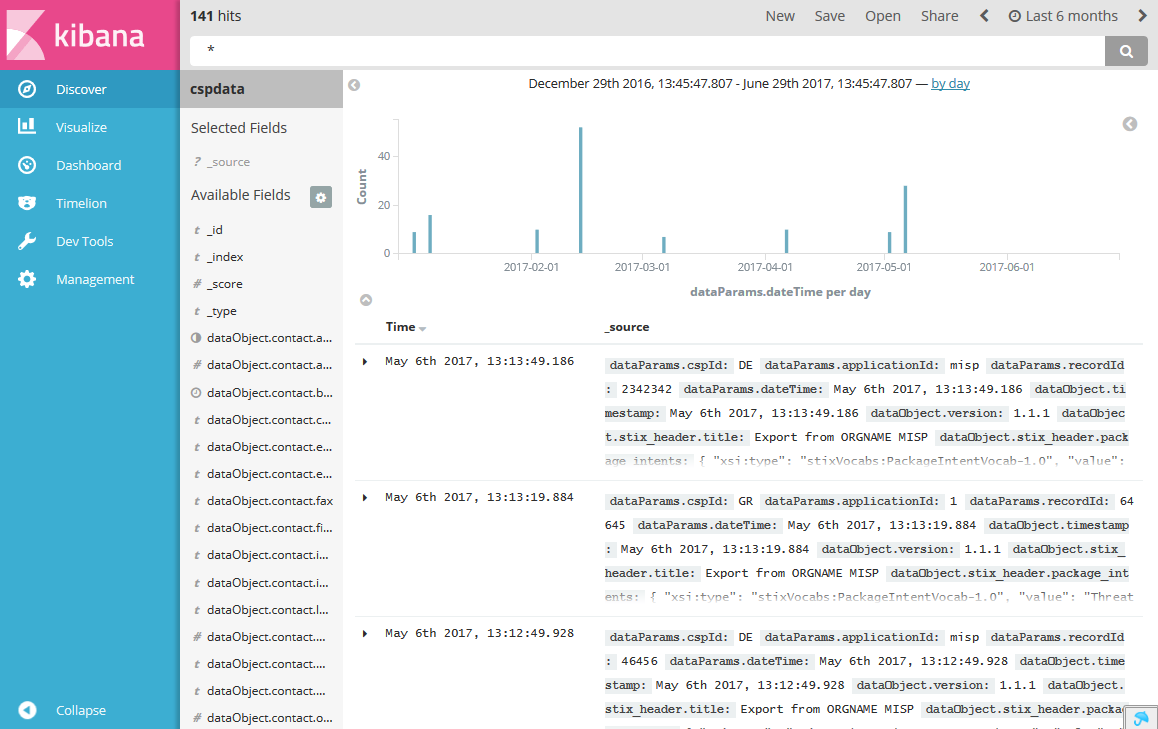
When loading the discover page, the user first needs to select from the upper right corner the timeframe for which data will be searched and displayed. The user can select one of the default options or enter a custom time. Timeframe selection applies to all data searched and displayed and should be chosen carefully to limit the number of results therefore accelerating the process. Timeframe selection appears in the following image.



As soon as the desired timeframe is selected, the user is presented with multiple visual elements:

* search bar
* time graph
* field sidebar
* raw data section

The search bar is where the search query is entered. By default, a \* is displayed showing all results. The default search appears in the following figure.



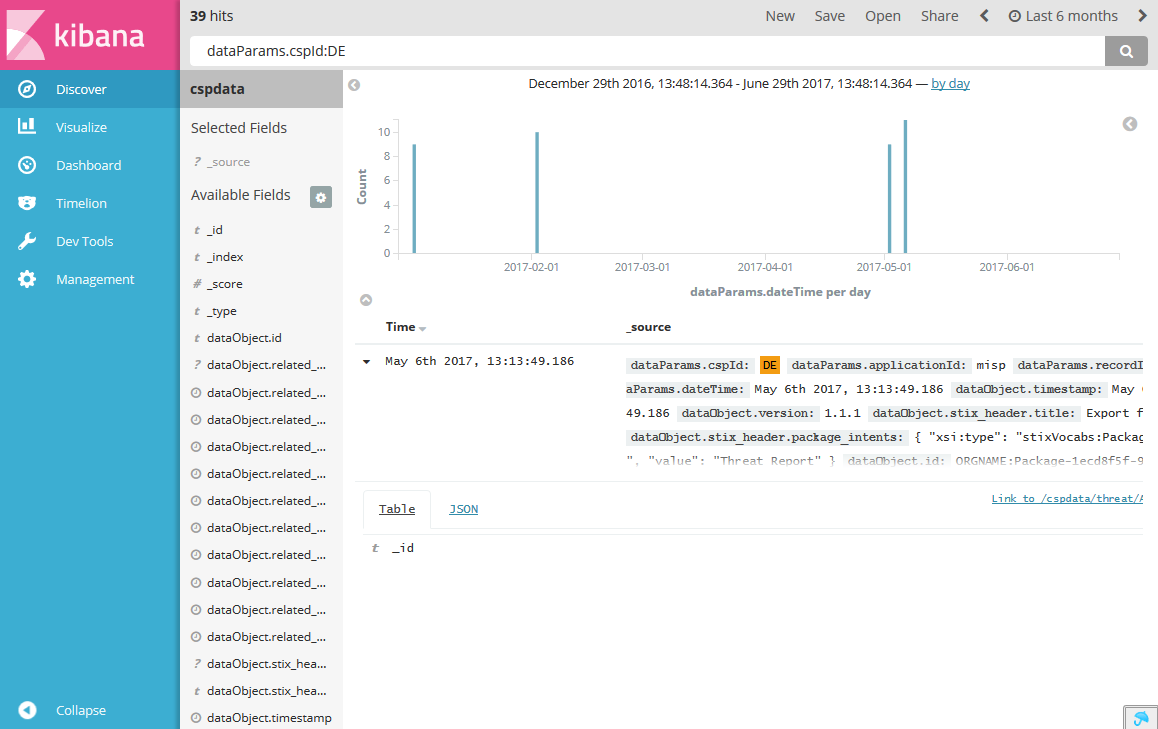
The query syntax is based on the Lucene query syntax. It allows Boolean operators, wildcards, and field filtering. Examples:

To search for all threat documents, enter: *\_type:threat*

To search for all event documents coming from the CSP called DE enter: *\_type:event AND dataParams.cspId:DE*

A list of available fields to search appears in the field sidebar. Results as graphically displayed in a bar graph at the time graph and as raw data in the raw data section.

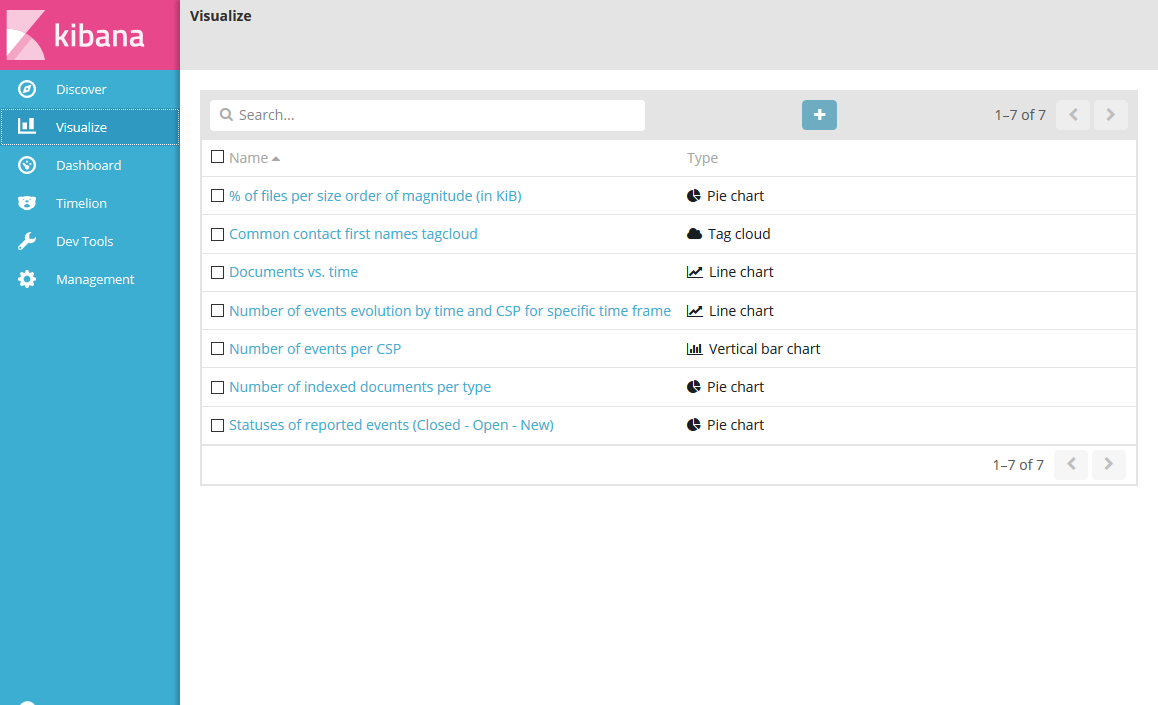
Each result is displayed in a two-column style with the first raw being the creation date and the second being the raw data. By expanding the result (clicking on the arrow) the user is presented with the full raw output in tabular format as well as JSON. A typical search result appears in the following figure.



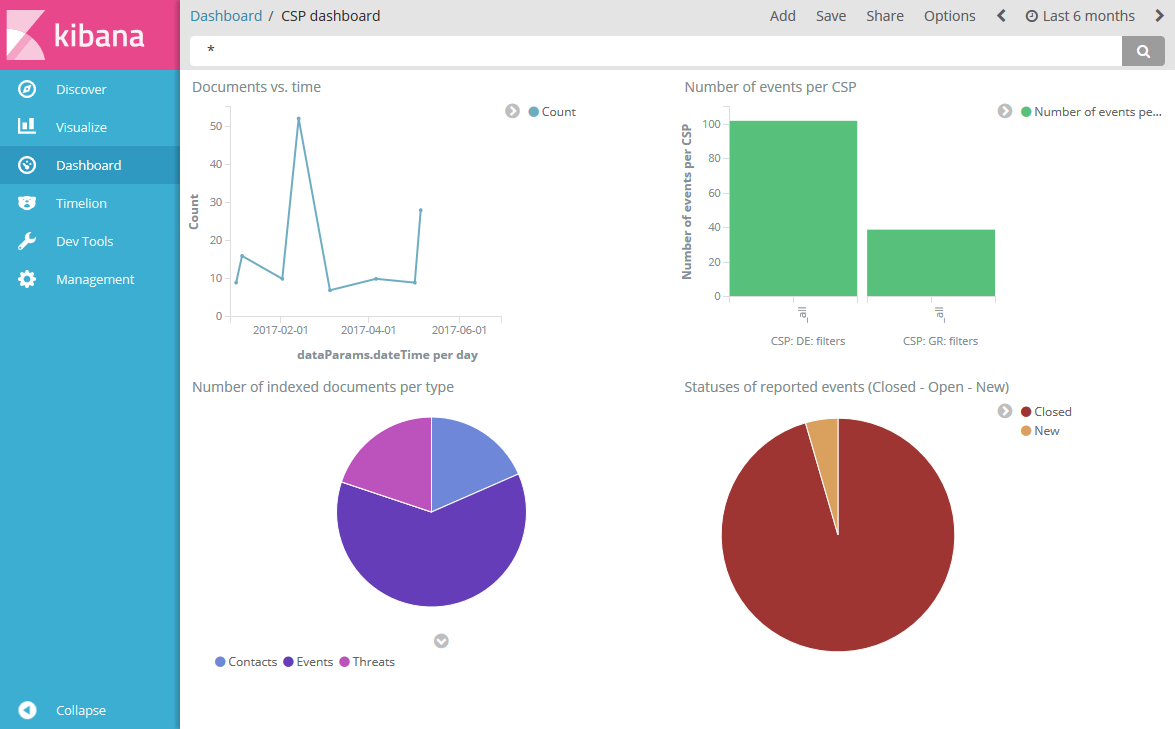
If the user tries to display too many raw results the web browser may become overloaded.

## Visualizing Data

Visualizing data in Kibana can be performed by selecting the Visualize option in the sidebar. Visualization is performed by selecting data using the same Lucene query format and timeframe selection explained in the previous section and displaying these data in several pre-existing graph types such as pie and line charts. Several visualizations have already been configured and appear as a list when selecting the visualize tab. The various visualizations appear in the following image.



In Kibana, a dashboard is a collection of visualizations that appear together in order to be able to correlate data and provide a better picture. A dashboard has been created that provides some of the most important visualizations. The dashboard is the most useful service provided to the user by Kibana and therefore appears by default when Kibana is accessed. The default Kibana dashboard appears in the following image.



The bar auto appears when the mouse is moved and auto-hides after a few seconds of inactivity.

# How to manage contacts with CMM

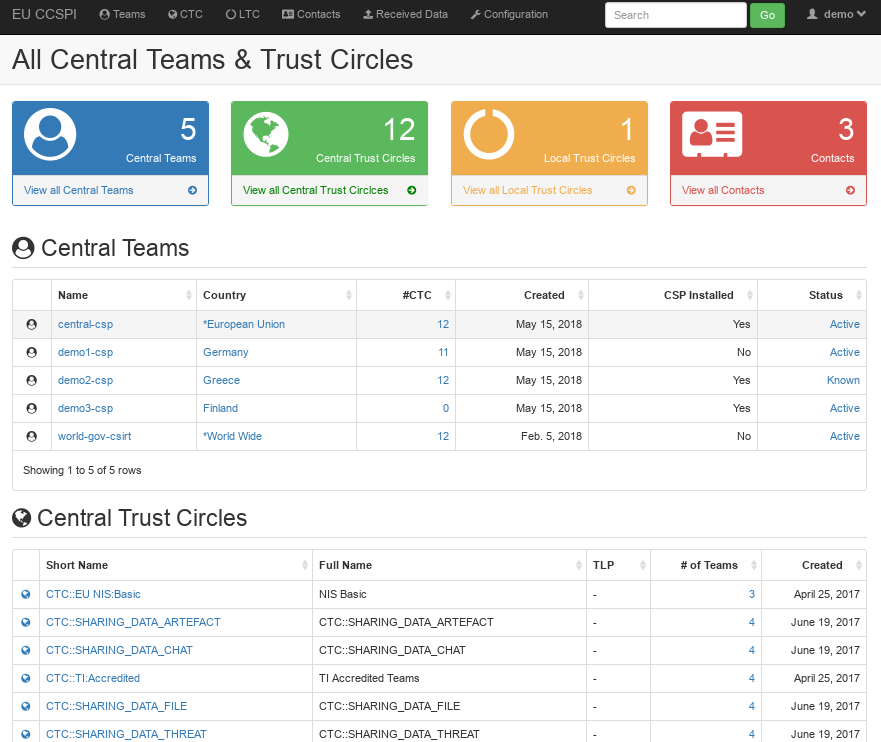
## Introduction

Contact Management Module is used to list, view, edit and share contact information of participants of the security community and facilitates the establishment of centralized or decentralized trust circles.

The module (CMM) can be accessed at

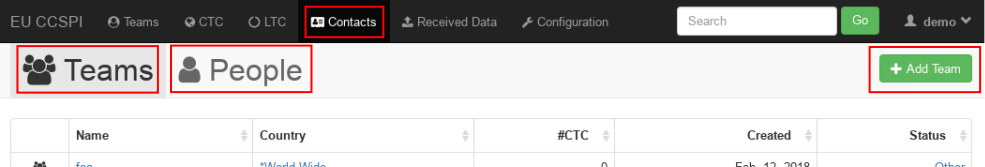
* https://tc.<cspId>.[preprod.]melicertes.eu

The on-screen presentation of the application is structured in two visual blocks: the top navigation bar and the main content area. The default start page, which is displayed upon retrieving the URL, consists of statistical dashboards with object counts and lists of Central Teams and Central Trust Circles. The screenshot below displays the UI with the default start page.

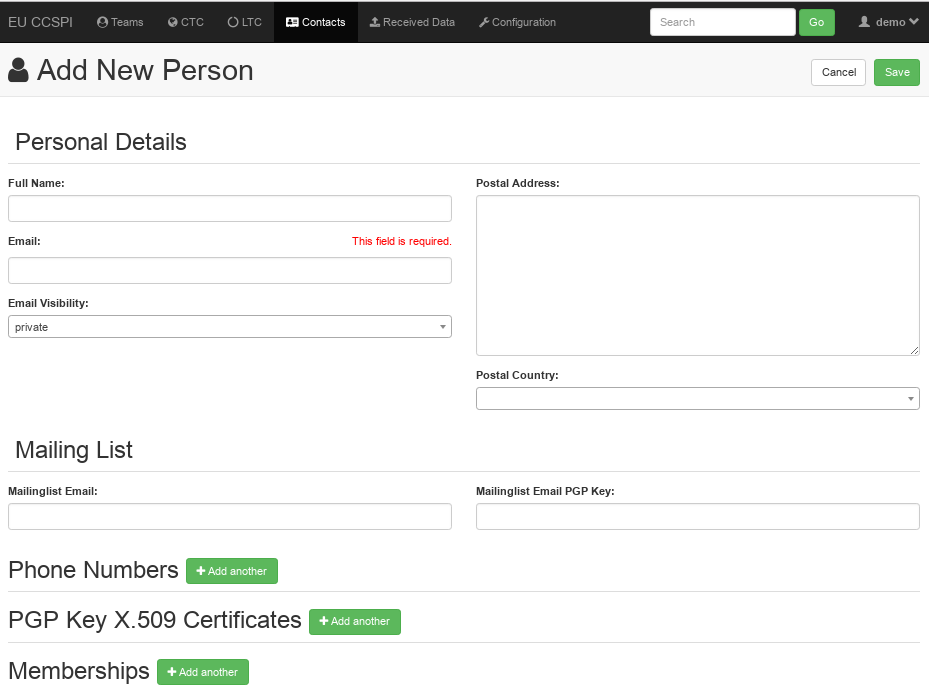


## Recording data and meta data of contacts

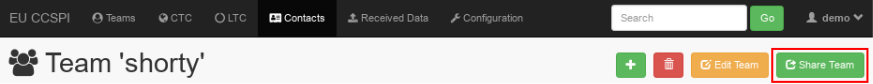
To create a new contact entry for a team or a person, please navigate to the Contacts tab in the top navigation bar. Then select whether you want to create an individual person by choosing “People” or a security team, which may or may not include individuals, by choosing “Teams”. Please refer to the screenshot below.



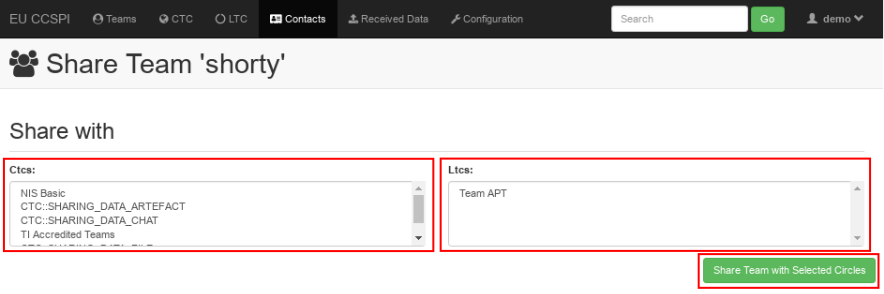
Clicking “Add Team” or “Add Person” respectively opens up the editing interface as exemplified by the screenshot below. At least the fields Status, Short Name, Country, Official Name and the Host Organization have to be provided to persist the data for a team, while only the Email is required for an individual without any team affiliation.



Once an entry has been saved, the UI switches from “edit” to a “view detail” interface. The view details interface allows to switch to the sharing interface by clicking on “Share Team”. Please refer to the screenshot below.



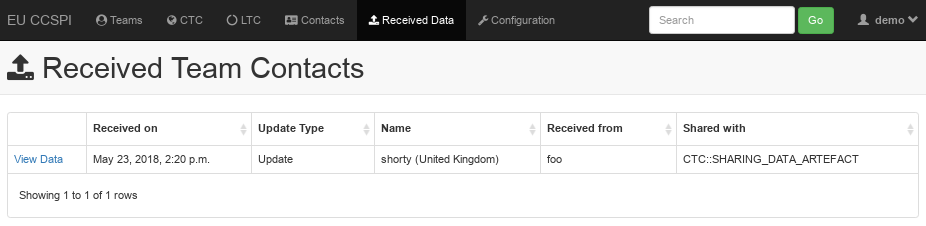
The following sharing screen then allows the selection of Trust Circles to share the entry with. This view is accessible through the details view of a team at any time. Please note, that sharing of individuals is only possible if they are part of a team.



Confirm the sharing intention by selecting the CTCs or the LTCs to share the chosen contact data with and clicking on “Share Team with Selected Circles”. No confirmation is displayed, as the data is shared in the background.

## Receiving data of contacts

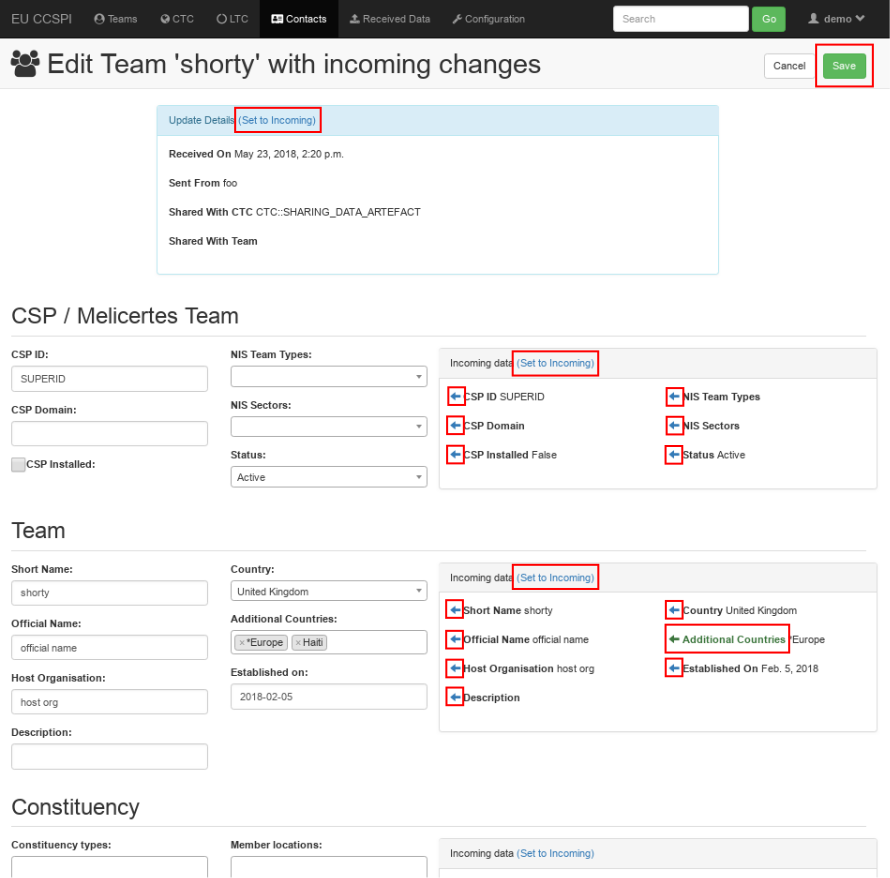
A list of an incoming data stream is available through the “Received Data” tab in the top navigation bar. Clicking on it exposes a list of incoming data units, which may be applied as a whole or in individually selected bits. As shown in the screenshot below, incoming data is differentiated by Update Type, indicating new or updated entries, by sender of the incoming data and the affected trust circles. Incoming data is expired automatically after a configurable period of time, which defaults to 31 days.



A click on “View Data” exposes a read-only view of the received data entry. In the upper area of the read-only screen the update details are summarized again. Changes can be applied by clicking on “Edit Team”, which displays the update view. The update view allows the user to collectively or selectively apply the incoming data. The screen, as shown below, is divided vertically in two halves: the data as known to the local CMM instance on the left and the incoming data as received on the right. The user now has four options of how the data may be applied.

1. As a whole – by clicking on “Set to Incoming” in the “Update Details” box.
2. Blockwise, for individual information blocks – by clicking on “Set to Incoming” in the individual “Incoming data” blocks.
3. Fieldwise, for individual data bits – by clicking on the left arrow () near the field to be applied.
4. Manually – by directly typing the data into input field.

Incoming data bits, that differ from those currently saved locally, are highlighted in a green color, as displayed in the screenshot below.



By clicking on the “Save” button, the user has the possibility to persist the data as shown on the left side. Should an entry become invalid, i.e. by manually deleting required data, an attempt to save the incoming entry will display the regular editing form with a descriptive error message.

## Recording data and meta data of local team

This use case is mostly identical to 3.2 with the distinction of the possibility to provide FIRST, TF-CSIRT/TI listing, accreditation and certification data. As of CMM version 3.6 the functionality to record FIRST and TF-CSIRT/TI data is expected in an upcoming release. In the meantime, please refer to section 3.2 for more information.

## Exporting local team data to FIRST

Reserved for future use.

## Exporting local team data to TF-CSIRT/TI

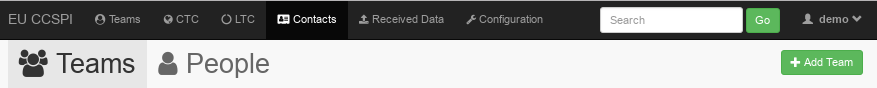
Reserved for future use.

## Importing team data from TF-CSIRT/TI

Reserved for future use.

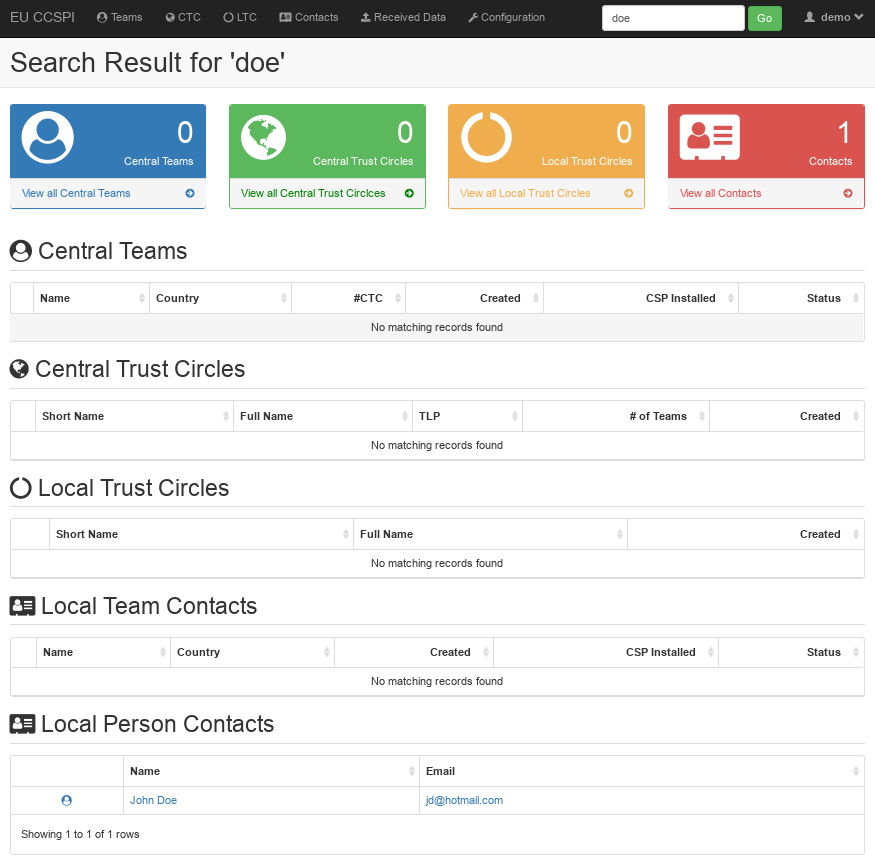
## List Local Contact entries

A list of all currently known Contacts can be accessed through the “Contacts” tab. As pictured below, a subdivision in Teams and People appears after opening the tab. Click on “People” to list all Person-like Contacts or click on Team to list all Team-like Contacts.



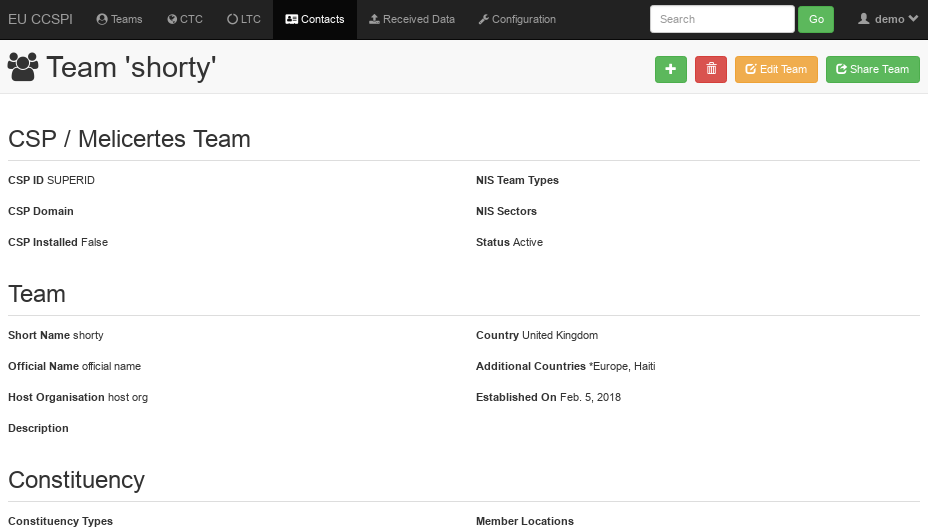
A click on the name or the icon of the entry will reveal the details of the entry. Please refer to section 3.9 for more details.

To display only a subset of Contacts filtered by any given term, please enter the search term into the search bar of the top navigation panel. For example, a search for “doe” will return all objects containing the search term “doe”. The screenshot below demonstrates the resulting hits for the search term “doe”, including a single Person Contact by the name “John Doe”. Click on the icon or the name to reveal the detailed read-only view of the Contact as described in section 3.9.



## Read Local Contact entry

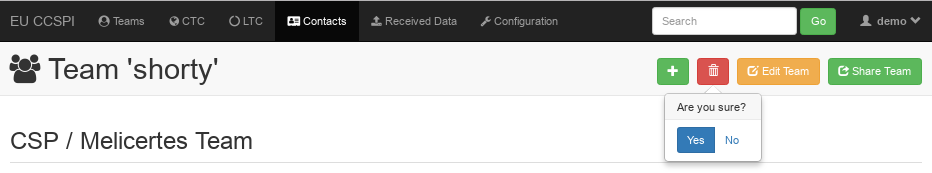
An individual Local Contact Team or People entry can be accessed through the “Contacts” tab. Upon user selection of an individual data entry of interest, a read-only view is displayed as shown below.



In this view the user also has the option to Add New, Delete, Edit or Share the team in question, including all associated team members. As exemplified in the screenshot below, the read-only view of a local Person differs from the Team view above in the lack of a “Share Team” button.

## Delete Local Contact entry

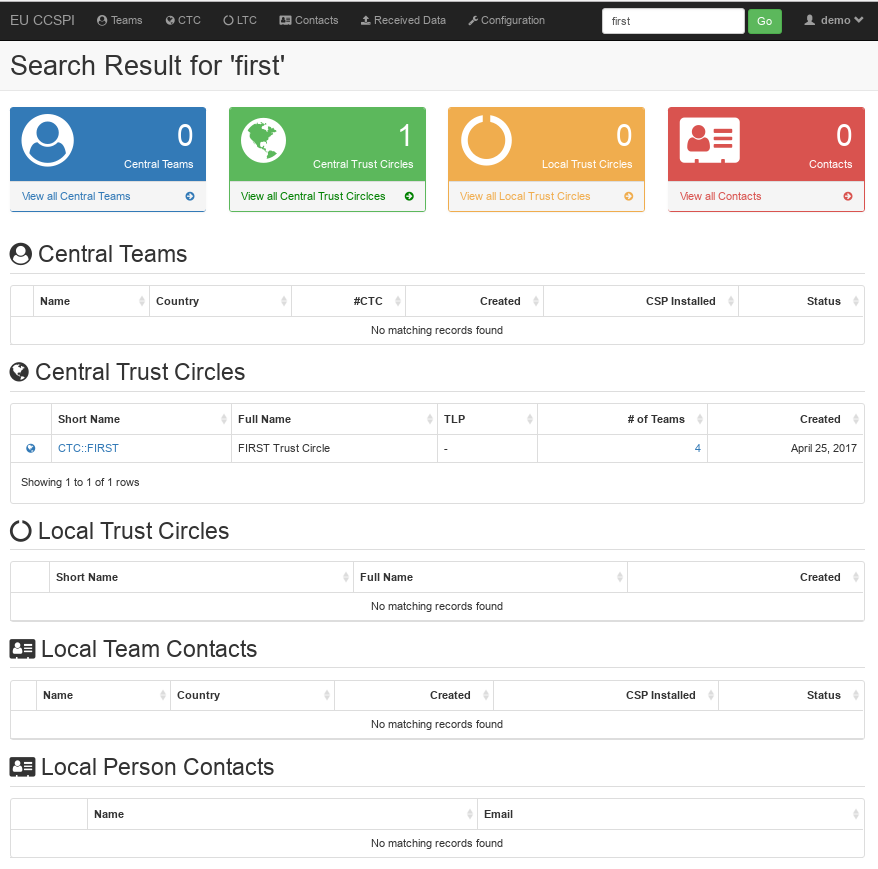
To delete a Local Contact entry locally, the user should click on the trash bin icon of the read-only view of an individual Contact. A popup for confirmation is displayed as pictured below.



## List Local and Central Trust Circles

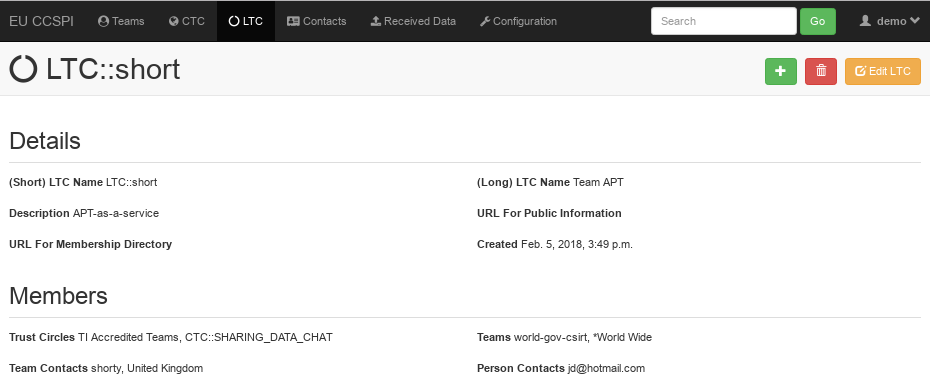
A list of all currently known Local and Central Trust Circles can be accessed through the default startpage, which is also accessible through the left-most “EU CCSPI” link of the navigation bar. To access the list of either Local or Central Trust Circles select the “LTC” or the “CTC” tab of the navigation bar, respectively. A click on the name or the icon of the entry will reveal the details of the entry. Please refer to section 3.12 and the CSP Administration Guide for more details.

To display only a subset of Local or Central Trust Circles filtered by any given term, please enter the search term into the search bar of the top navigation panel. For example, a search for “first” will return all objects containing the search term “first”. The screenshot below demonstrates the resulting hits for the search term “first”, including a single Trust Circle “CTC::FIRST”. Click on the icon or the (Short) Name to reveal the detailed read-only view of the Trust Circle as described in section 3.12 and the CSP Administration Guide.



## Read Local Trust Circle

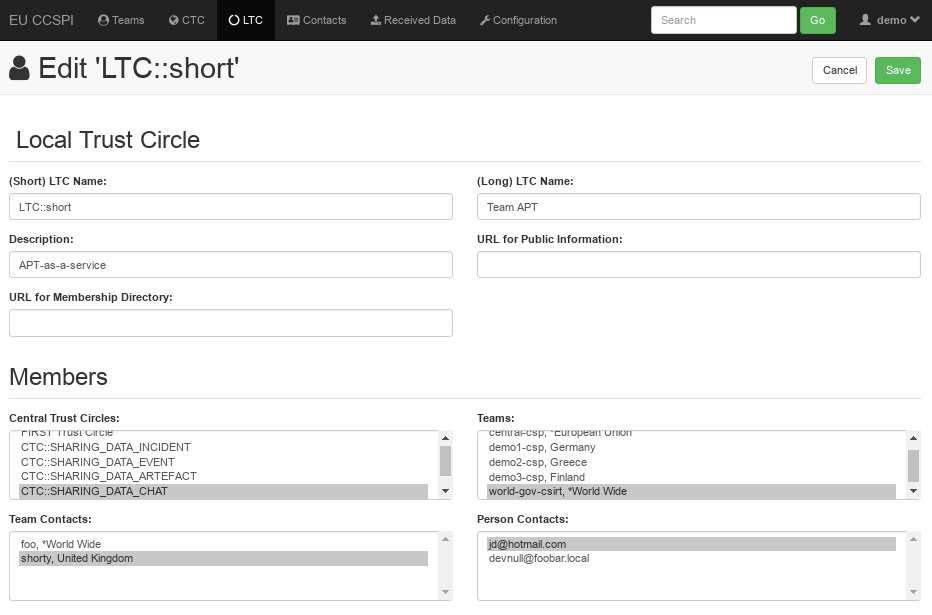
An individual Local Trust Circle entry can be accessed through the “LTC” tab. Upon user selection of an individual data entry of interest, a read-only view is displayed as shown below.



In this view the user also has the option to Add New, Delete or Edit the Local Trust Circle in question. Member of a Local Trust Circle may be any Central Trust Circle, any Central Team, any Team or Person Contact.

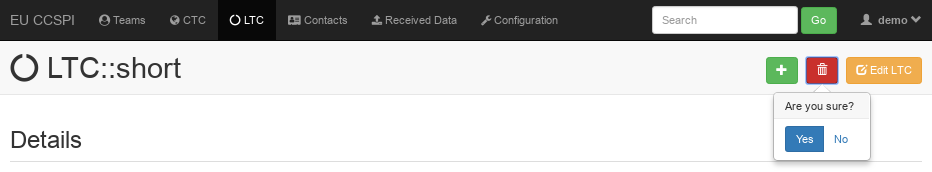
## Write Local Trust Circle

Editing of a Local Trust Circle can be triggered by clicking “Edit LTC” in the read-only view of the Local Trust Circle in question (see section 3.12 for details). The editing interface is exemplified below. To select several members of the same type, i.e. several Teams, click on additional Teams in the list while holding the “Ctrl”-Key on your keyboard.



## Delete Local Trust Circle

To delete a Local Trust Circle, the user should click on the trash bin icon of the read-only view of an individual Trust Circle (see section 3.12 for details). A popup for confirmation is displayed as pictured below.

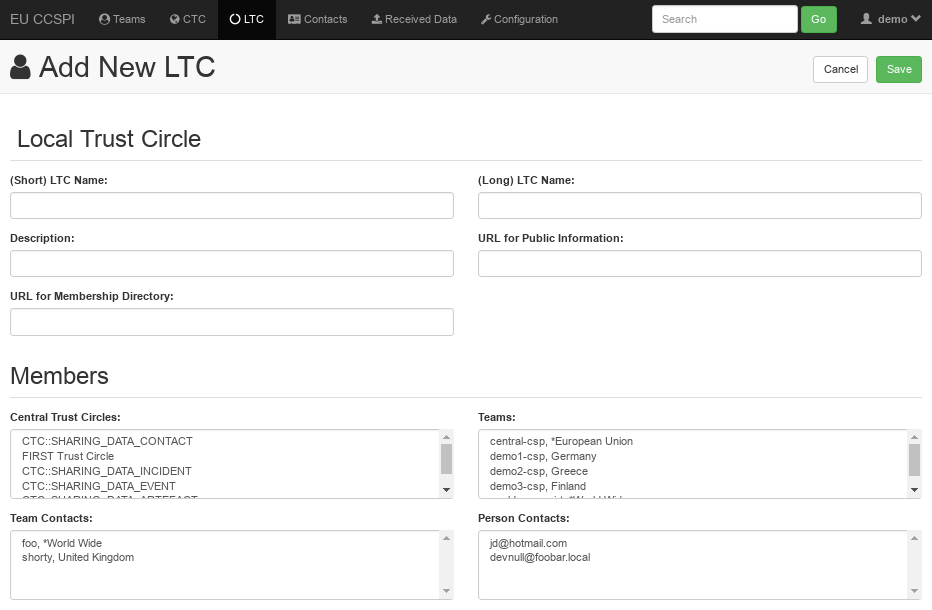


## Create a new Local Trust Circle

To create a new Local Trust Circle go to the “LTC” tab in the top navigation bar and click on “Add Local Trust Circle” and fill out the data fields. To select multiple members of the same type, please press and hold the Ctrl key on your keyboard while clicking on members. To save the Local Trust Circle, click on “Save”. To be able to successfully save a record, following fields are required:

* (Short) LTC Name has to be entered and begin with “LTC::”,
* (Long) LTC Name has to be entered,
* Description has to be entered.

A screenshot of the editing interface is displayed below.



# How to manage contacts with CMM

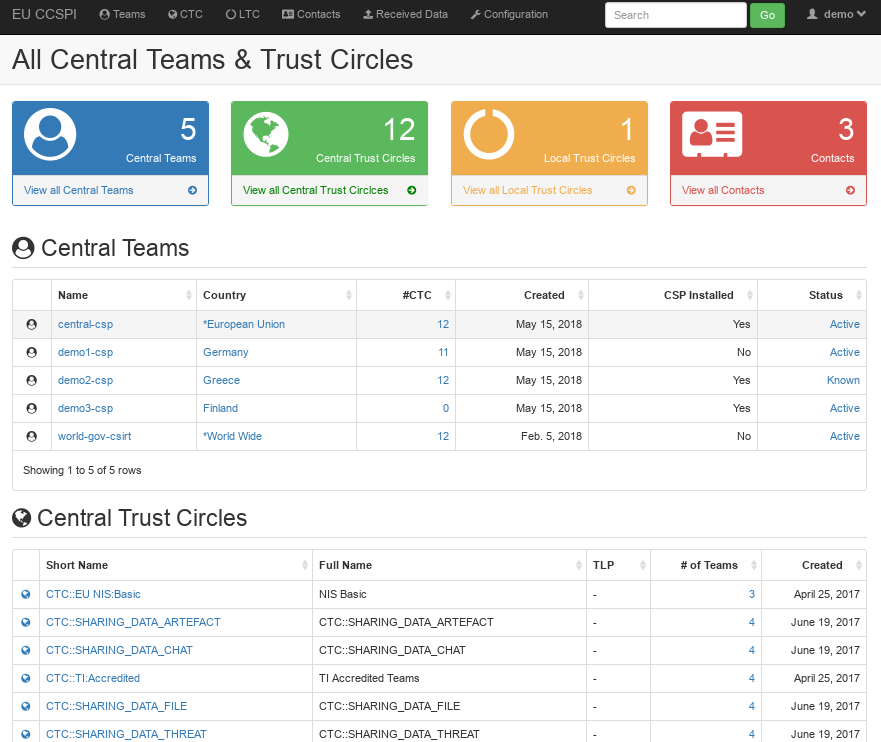
## Introduction

Contact Management Module is used to list, view, edit and share contact information of participants of the security community and facilitates the establishment of centralized or decentralized trust circles.

The module (CMM) can be accessed at

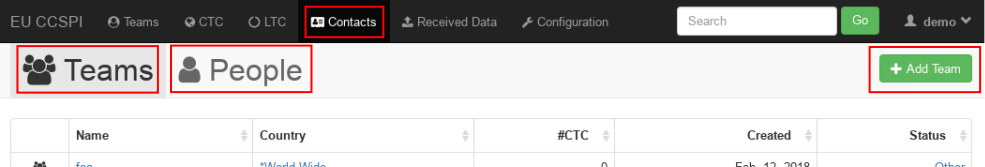
* https://tc.<cspId>.[preprod.]melicertes.eu

The on-screen presentation of the application is structured in two visual blocks: the top navigation bar and the main content area. The default start page, which is displayed upon retrieving the URL, consists of statistical dashboards with object counts and lists of Central Teams and Central Trust Circles. The screenshot below displays the UI with the default start page.

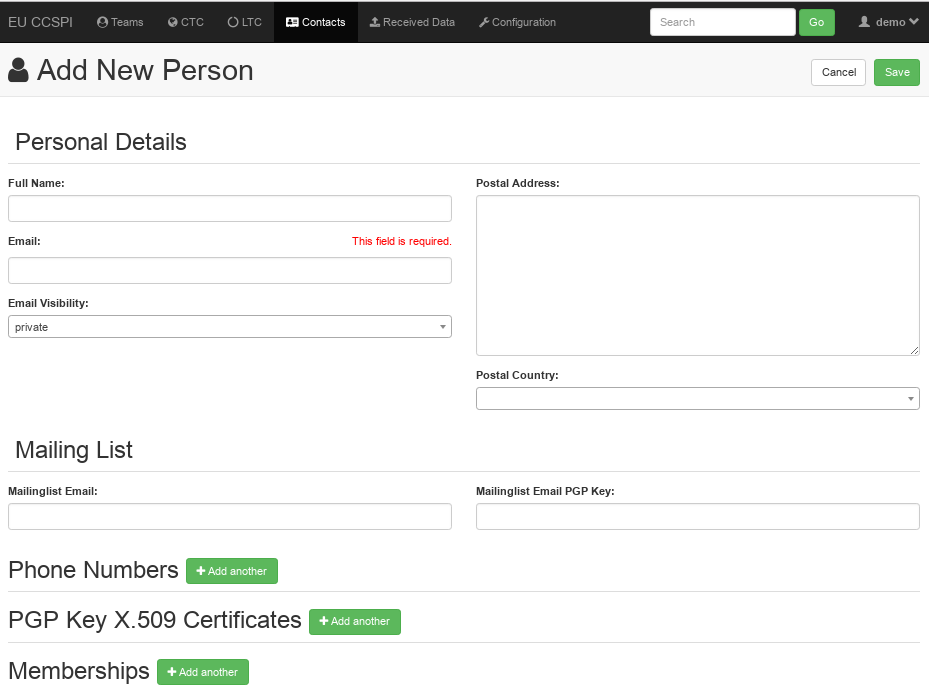


## Recording data and meta data of contacts

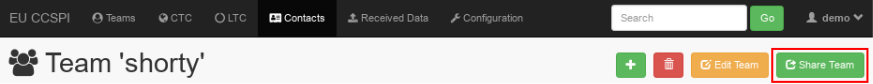
To create a new contact entry for a team or a person, please navigate to the Contacts tab in the top navigation bar. Then select whether you want to create an individual person by choosing “People” or a security team, which may or may not include individuals, by choosing “Teams”. Please refer to the screenshot below.



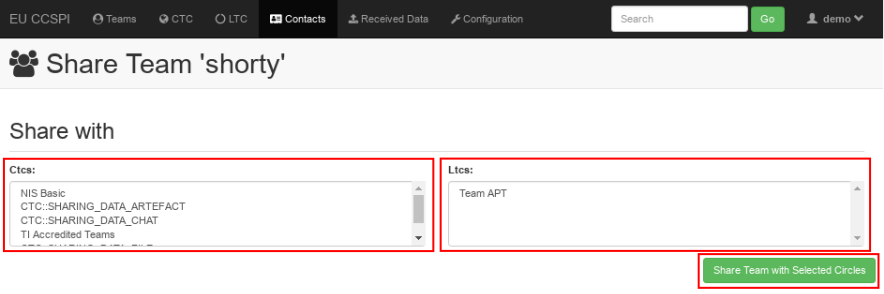
Clicking “Add Team” or “Add Person” respectively opens up the editing interface as exemplified by the screenshot below. At least the fields Status, Short Name, Country, Official Name and the Host Organization have to be provided to persist the data for a team, while only the Email is required for an individual without any team affiliation.



Once an entry has been saved, the UI switches from “edit” to a “view detail” interface. The view details interface allows to switch to the sharing interface by clicking on “Share Team”. Please refer to the screenshot below.



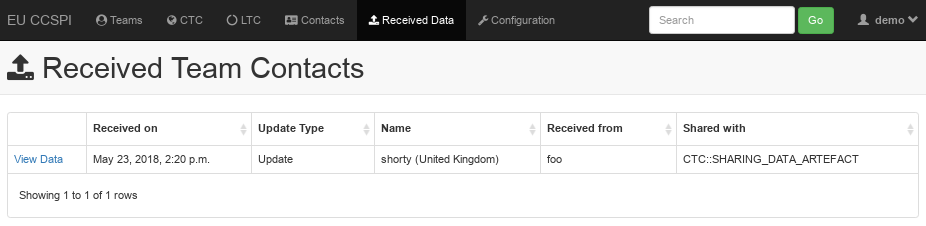
The following sharing screen then allows the selection of Trust Circles to share the entry with. This view is accessible through the details view of a team at any time. Please note, that sharing of individuals is only possible if they are part of a team.



Confirm the sharing intention by selecting the CTCs or the LTCs to share the chosen contact data with and clicking on “Share Team with Selected Circles”. No confirmation is displayed, as the data is shared in the background.

## Receiving data of contacts

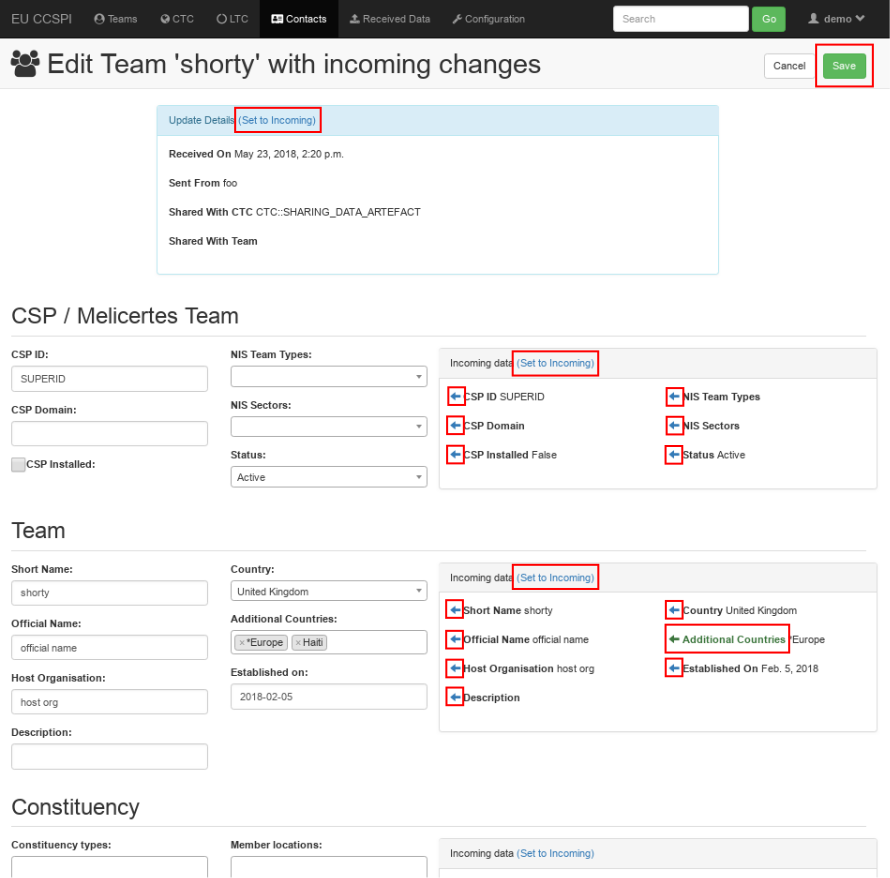
A list of an incoming data stream is available through the “Received Data” tab in the top navigation bar. Clicking on it exposes a list of incoming data units, which may be applied as a whole or in individually selected bits. As shown in the screenshot below, incoming data is differentiated by Update Type, indicating new or updated entries, by sender of the incoming data and the affected trust circles. Incoming data is expired automatically after a configurable period of time, which defaults to 31 days.



A click on “View Data” exposes a read-only view of the received data entry. In the upper area of the read-only screen the update details are summarized again. Changes can be applied by clicking on “Edit Team”, which displays the update view. The update view allows the user to collectively or selectively apply the incoming data. The screen, as shown below, is divided vertically in two halves: the data as known to the local CMM instance on the left and the incoming data as received on the right. The user now has four options of how the data may be applied.

1. As a whole – by clicking on “Set to Incoming” in the “Update Details” box.
2. Blockwise, for individual information blocks – by clicking on “Set to Incoming” in the individual “Incoming data” blocks.
3. Fieldwise, for individual data bits – by clicking on the left arrow () near the field to be applied.
4. Manually – by directly typing the data into input field.

Incoming data bits, that differ from those currently saved locally, are highlighted in a green color, as displayed in the screenshot below.



By clicking on the “Save” button, the user has the possibility to persist the data as shown on the left side. Should an entry become invalid, i.e. by manually deleting required data, an attempt to save the incoming entry will display the regular editing form with a descriptive error message.

## Recording data and meta data of local team

This use case is mostly identical to 3.2 with the distinction of the possibility to provide FIRST, TF-CSIRT/TI listing, accreditation and certification data. As of CMM version 3.6 the functionality to record FIRST and TF-CSIRT/TI data is expected in an upcoming release. In the meantime, please refer to section 3.2 for more information.

## Exporting local team data to FIRST

Reserved for future use.

## Exporting local team data to TF-CSIRT/TI

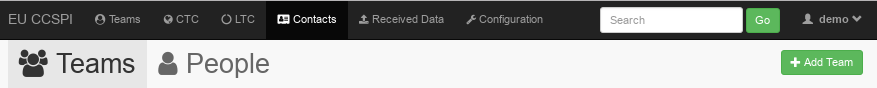
Reserved for future use.

## Importing team data from TF-CSIRT/TI

Reserved for future use.

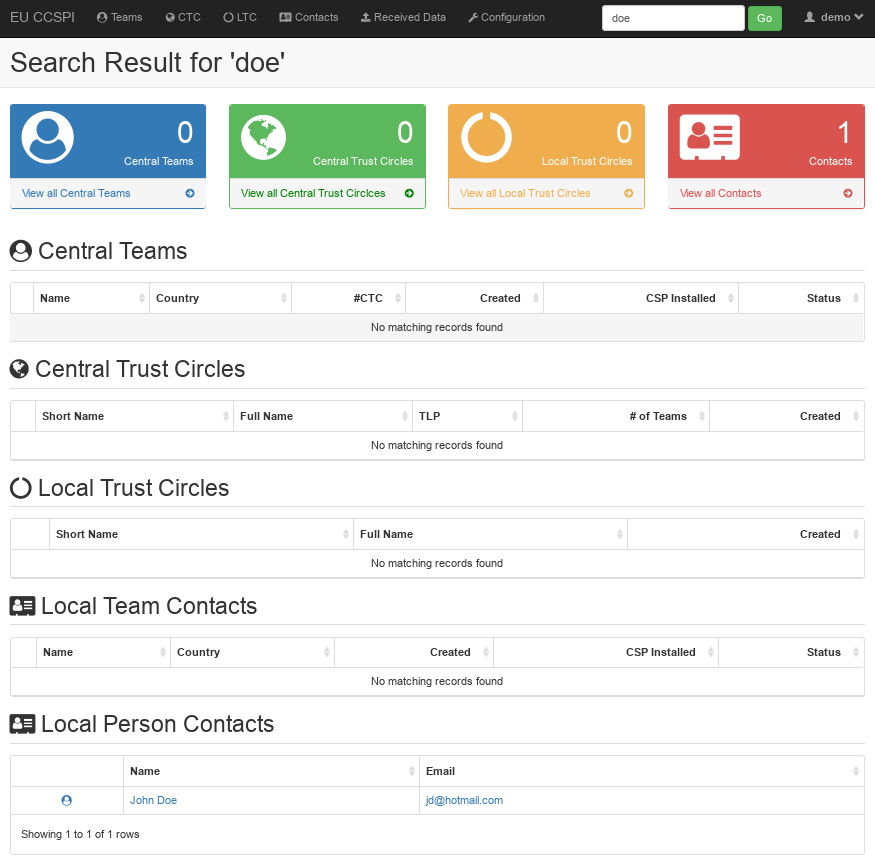
## List Local Contact entries

A list of all currently known Contacts can be accessed through the “Contacts” tab. As pictured below, a subdivision in Teams and People appears after opening the tab. Click on “People” to list all Person-like Contacts or click on Team to list all Team-like Contacts.



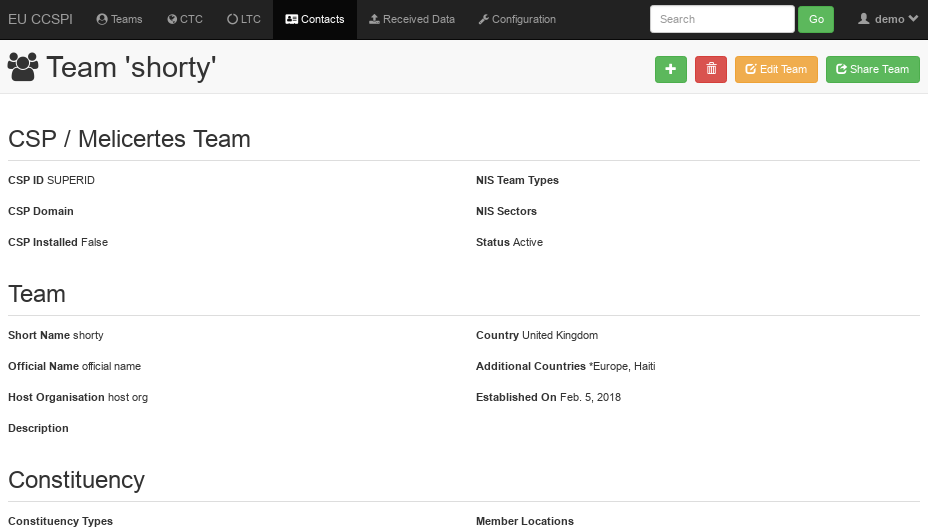
A click on the name or the icon of the entry will reveal the details of the entry. Please refer to section 3.9 for more details.

To display only a subset of Contacts filtered by any given term, please enter the search term into the search bar of the top navigation panel. For example, a search for “doe” will return all objects containing the search term “doe”. The screenshot below demonstrates the resulting hits for the search term “doe”, including a single Person Contact by the name “John Doe”. Click on the icon or the name to reveal the detailed read-only view of the Contact as described in section 3.9.



## Read Local Contact entry

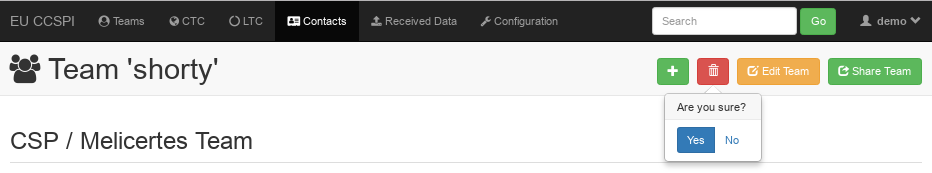
An individual Local Contact Team or People entry can be accessed through the “Contacts” tab. Upon user selection of an individual data entry of interest, a read-only view is displayed as shown below.



In this view the user also has the option to Add New, Delete, Edit or Share the team in question, including all associated team members. As exemplified in the screenshot below, the read-only view of a local Person differs from the Team view above in the lack of a “Share Team” button.

## Delete Local Contact entry

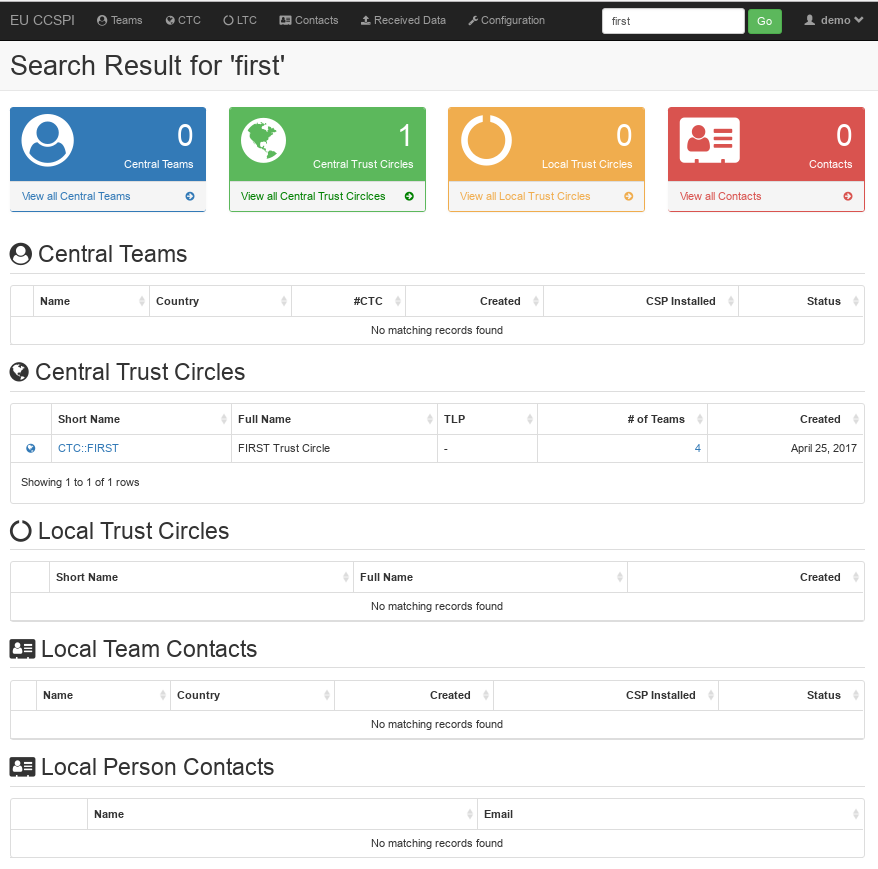
To delete a Local Contact entry locally, the user should click on the trash bin icon of the read-only view of an individual Contact. A popup for confirmation is displayed as pictured below.



## List Local and Central Trust Circles

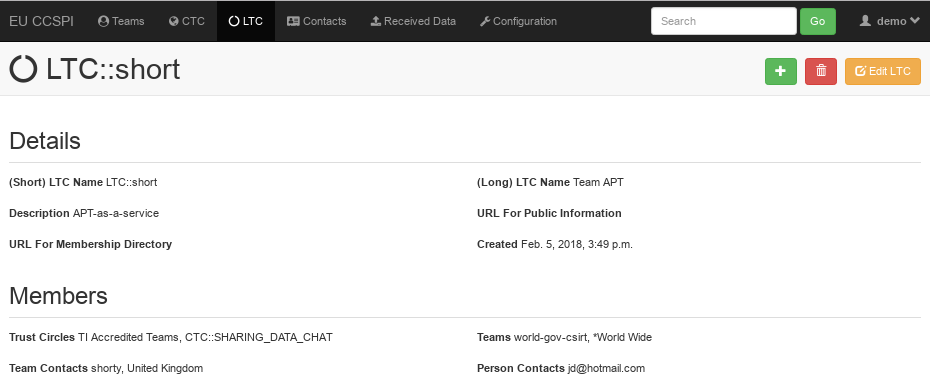
A list of all currently known Local and Central Trust Circles can be accessed through the default startpage, which is also accessible through the left-most “EU CCSPI” link of the navigation bar. To access the list of either Local or Central Trust Circles select the “LTC” or the “CTC” tab of the navigation bar, respectively. A click on the name or the icon of the entry will reveal the details of the entry. Please refer to section 3.12 and the CSP Administration Guide for more details.

To display only a subset of Local or Central Trust Circles filtered by any given term, please enter the search term into the search bar of the top navigation panel. For example, a search for “first” will return all objects containing the search term “first”. The screenshot below demonstrates the resulting hits for the search term “first”, including a single Trust Circle “CTC::FIRST”. Click on the icon or the (Short) Name to reveal the detailed read-only view of the Trust Circle as described in section 3.12 and the CSP Administration Guide.



## Read Local Trust Circle

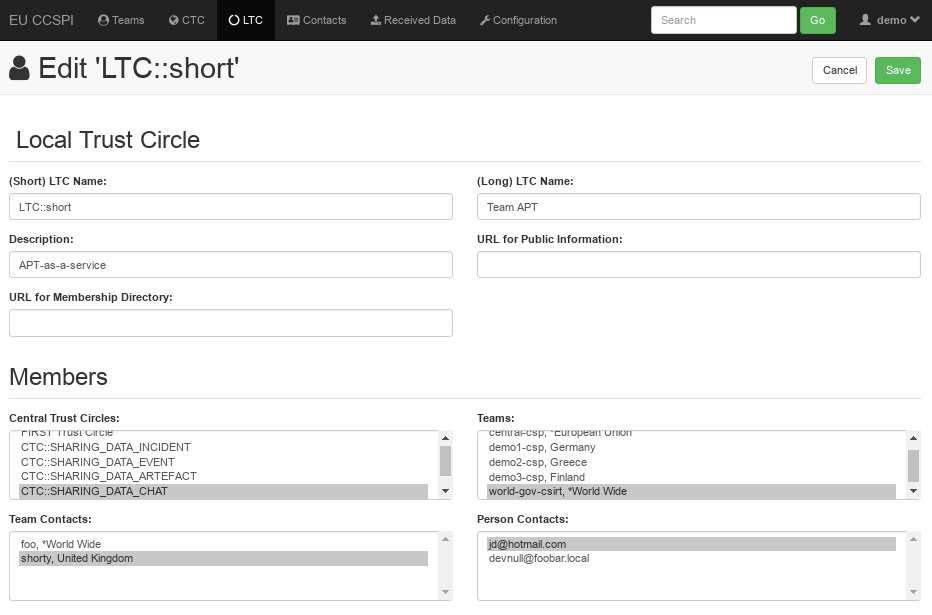
An individual Local Trust Circle entry can be accessed through the “LTC” tab. Upon user selection of an individual data entry of interest, a read-only view is displayed as shown below.



In this view the user also has the option to Add New, Delete or Edit the Local Trust Circle in question. Member of a Local Trust Circle may be any Central Trust Circle, any Central Team, any Team or Person Contact.

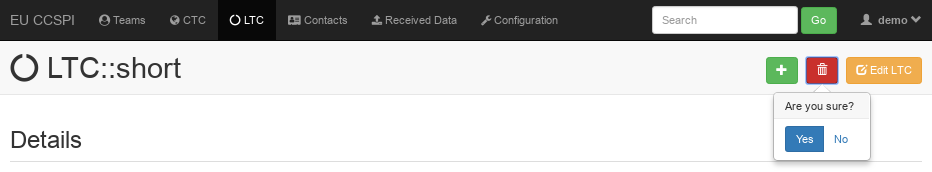
## Write Local Trust Circle

Editing of a Local Trust Circle can be triggered by clicking “Edit LTC” in the read-only view of the Local Trust Circle in question (see section 3.12 for details). The editing interface is exemplified below. To select several members of the same type, i.e. several Teams, click on additional Teams in the list while holding the “Ctrl”-Key on your keyboard.



## Delete Local Trust Circle

To delete a Local Trust Circle, the user should click on the trash bin icon of the read-only view of an individual Trust Circle (see section 3.12 for details). A popup for confirmation is displayed as pictured below.

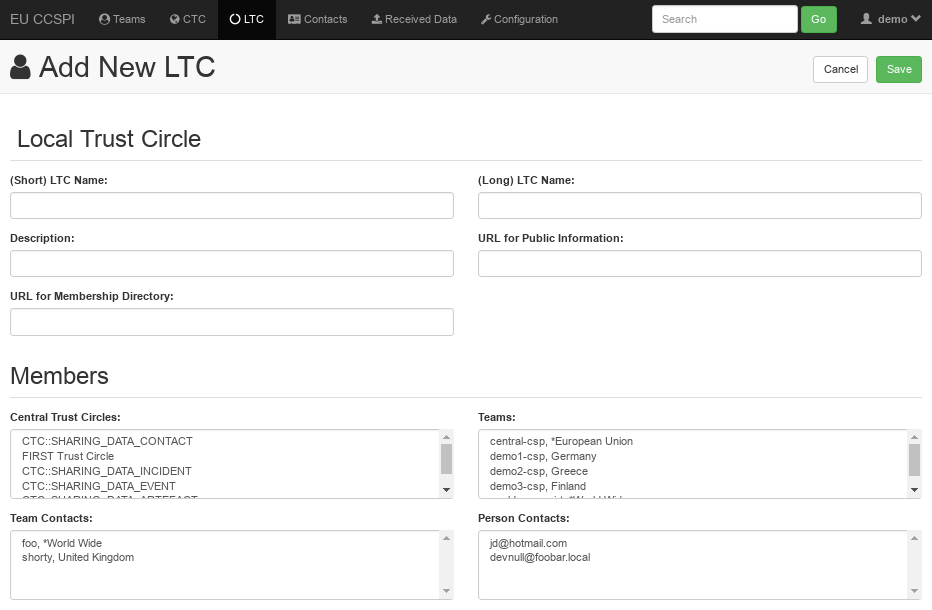


## Create a new Local Trust Circle

To create a new Local Trust Circle go to the “LTC” tab in the top navigation bar and click on “Add Local Trust Circle” and fill out the data fields. To select multiple members of the same type, please press and hold the Ctrl key on your keyboard while clicking on members. To save the Local Trust Circle, click on “Save”. To be able to successfully save a record, following fields are required:

* (Short) LTC Name has to be entered and begin with “LTC::”,
* (Long) LTC Name has to be entered,
* Description has to be entered.

A screenshot of the editing interface is displayed below.



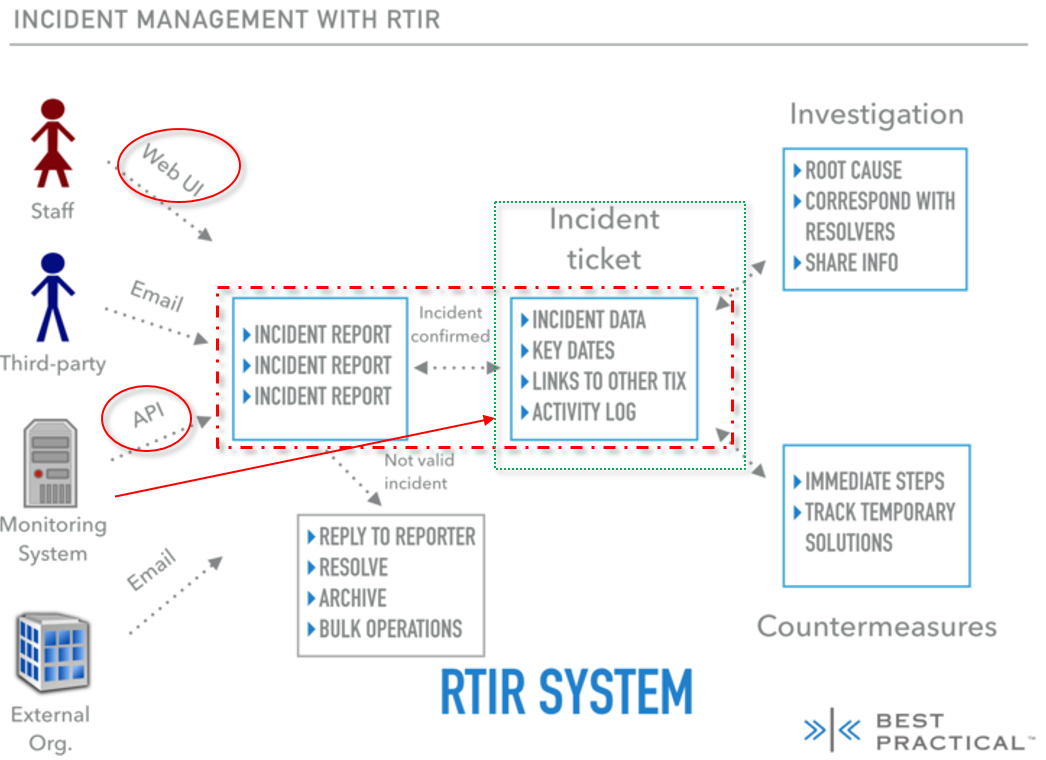
# How to manage incidents with RT

## Introduction

CSP provides the Request Tracker ticketing system as a tool to be used to manage the incidents. The used version is the latest one – 4.4.2. Furthermore, a dedicated extension RT for Incident Response - RT::IR – is used (in the version 4.0.0), in order to handle the tasks of incident management properly[[2]](#footnote-2).

Figure below (source: Best Practical) depicts the default workflow of incident management, which is implemented using RT. The common functionality of the RT remains the same and has not been changed by implementing the CSP-extension. Some CSP-specific adjustments are marked using the red colour and they are the following:

* Staff can perform some additional tasks using the web user interface:
  + Manually linking of corresponding threats, vulnerabilities and events (managed by dedicated application) into particular incident or incident report (only link will be stored on RT application, the data will remain in the leading application for the particular type of the linked artefact: e.g. event -> MISP application etc.),
  + Manually providing any additional data to the given incident, which will be stored directly in RT application,
  + Set up the sharing policy, which should be used in order to share the incident information across the CSP instances.
* Furthermore there are some automatically done tasks, either directly by RT (using the CSP-specific extensions) or by the CSP-adapter (using the RT remote REST interface):
  + Every ticket has a CSP-wide unique ID (RT\_UUID), which is automatically assigned while creating the ticket. This ID exists parallel to the ticket numbers, which are used by the RT per default, but which are only unique in a single instance of RT,
  + The originator CSP of a ticket and the CSP, which changed (updated) the ticket as a last are stored in the ticket data,
  + CSP-RT-adapter create automatically event-, threat- or vulnerability-driven incident reports, in case the underlying policy has been fulfilled.



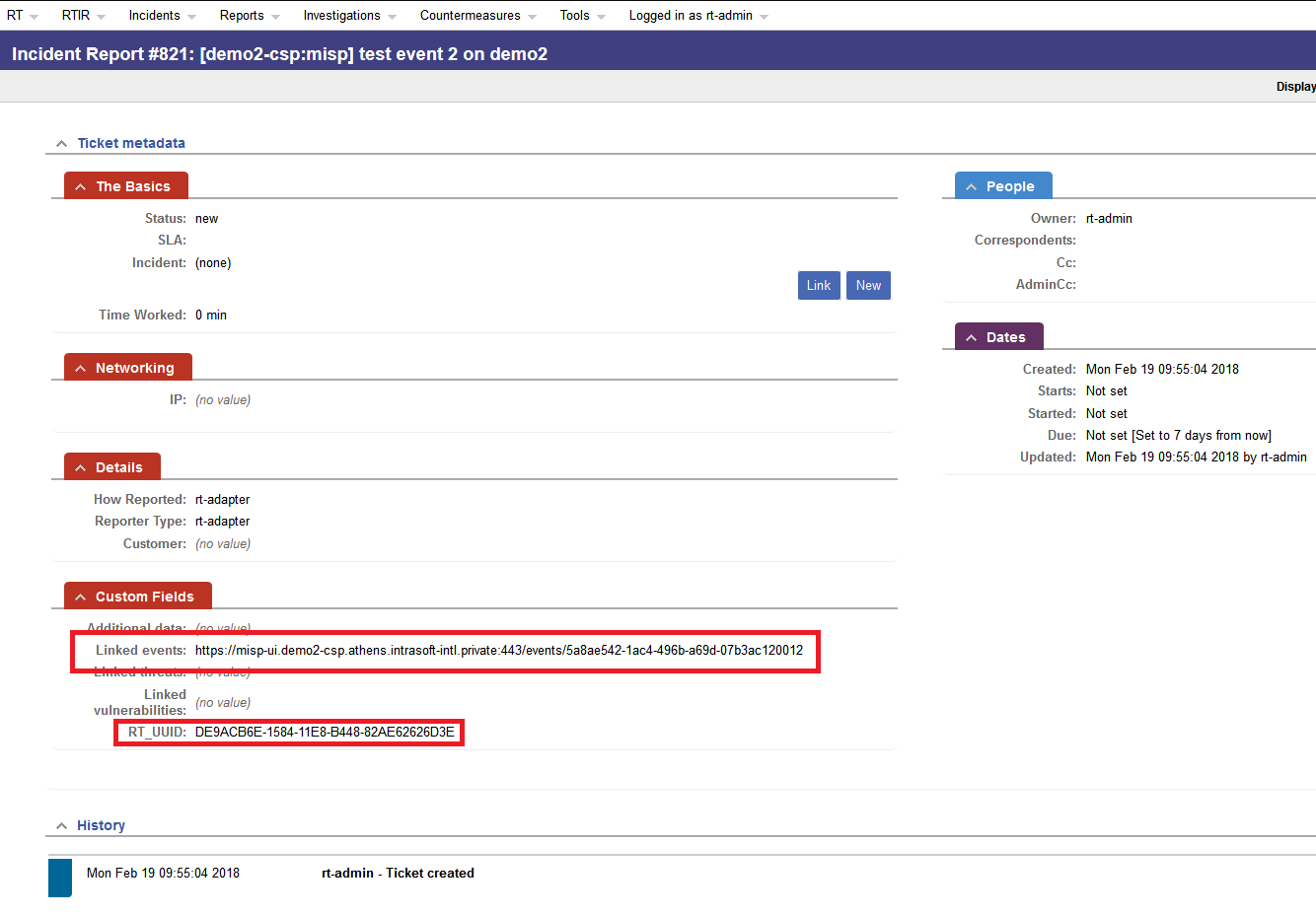
Following chapters will describe especially the CSP-specific functionality. In order to get information about the default functionality of RT and RT::IR please visit the corresponding product web sites: <https://bestpractical.com/resources/> or respective <https://docs.bestpractical.com/rtir/4.0.1/index.html>.

The RT-application is accessible by using the following links:

* https://rt.<cspId>.[preprod.]melicertes.eu – access to the pure RT-application (not the RT::IR extension), e.g. https://rt.demo2-csp.athens.intrasoft-intl.private
* https://rt.<cspId>.[preprod.]melicertes.eu/RTIR – access to the RT::IR extension, e.g. https://rt.demo2-csp.athens.intrasoft-intl.private/RTIR

## Incident reports management

CSP integration layer (IL) is continually taking care of the managed artefacts to be announced to the connected application. Thus also in case of the events, threats and vulnerabilities, if one of them is created or changed (or published), the data will be transferred to all remaining applications (apart of the leading application) for further processing. If for example a new event has been created and published on the event leading application, which is MISP, than the information will be routed by the IL to the CSP-RT-adapter. The CSP-RT-adapter evaluates the information according to the given event-handling policy and can automatically create an incident report on RT, if the policy requirement for doing that has been fulfilled. Following figure shows an automatically created incident report, which is based on an event.



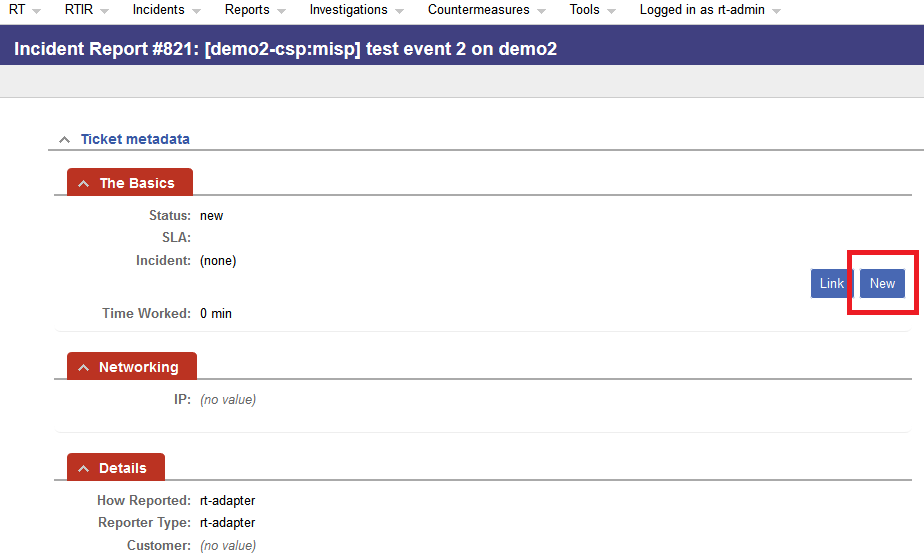
The red rectangles point especially to the automatically linked event this incident report bases on and automatically created UUID of the incident report.

## Creating incidents

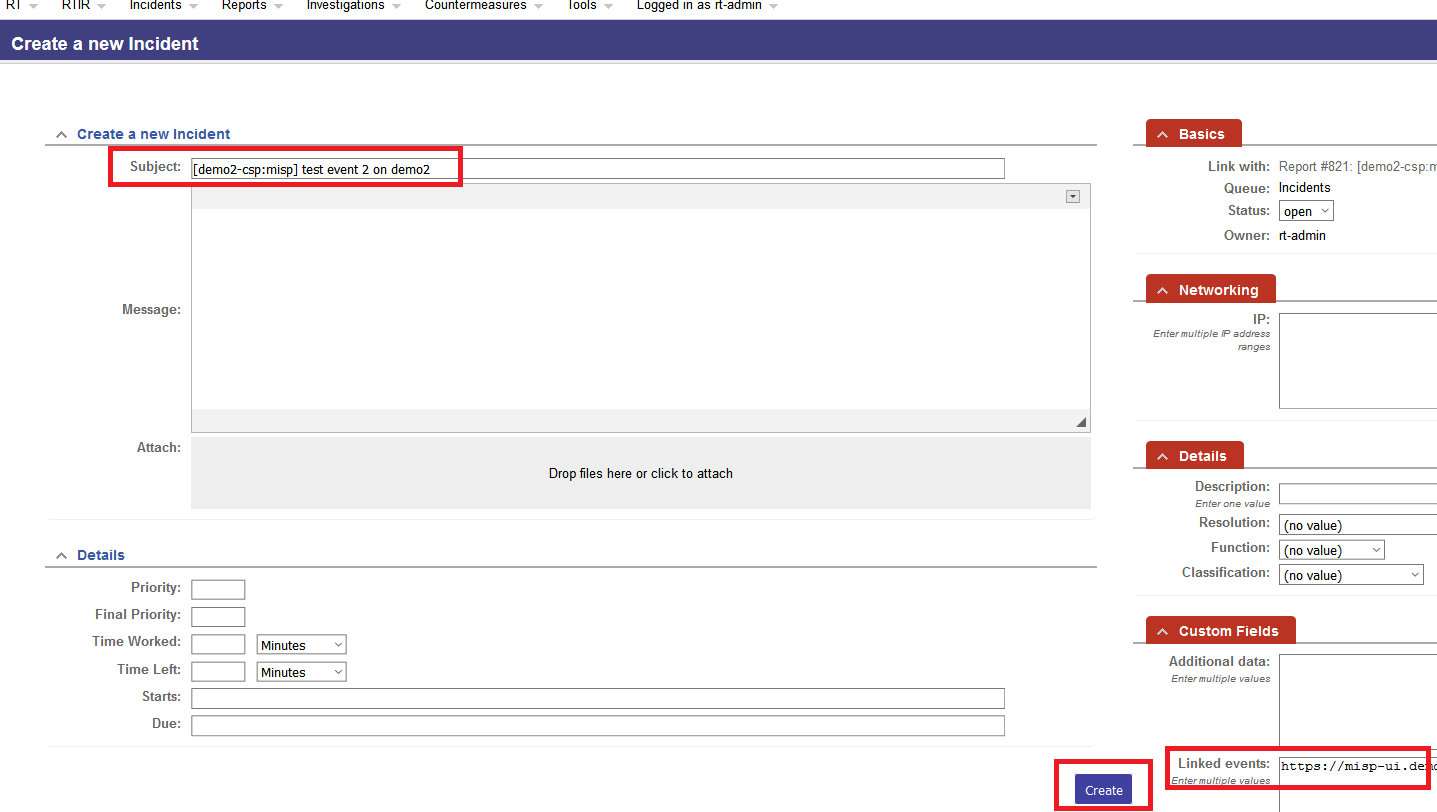
Apart of the default functionality provided by the RT to create new incidents, there is another case, where an incident will be automatically created after it has been shared by another CSP instance.

### Create an incident based on event driven incident report

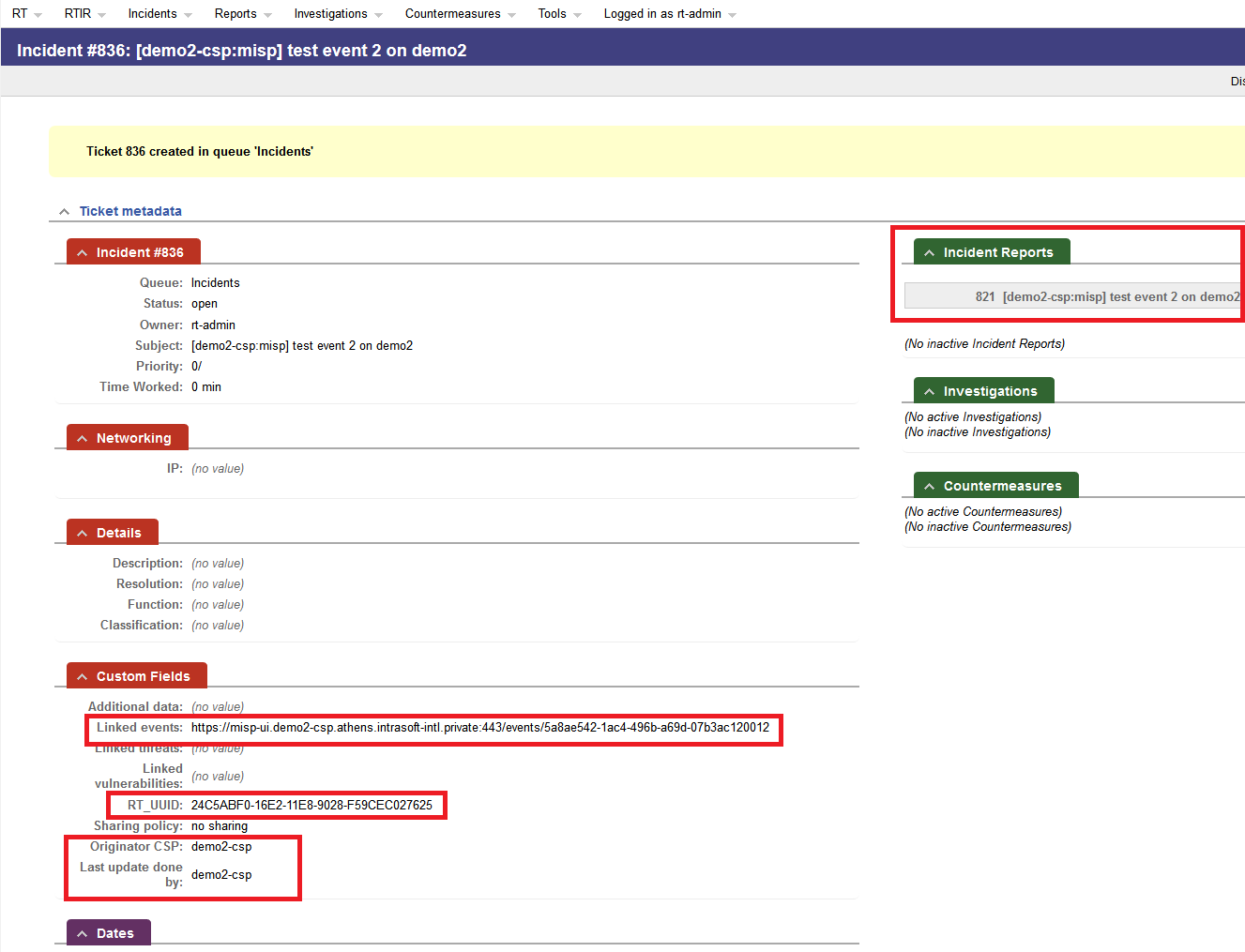
An automatically created even-driven incident report (see chapter 5.2) can be converted into an incident. The additional CSP-driven information already attached to the report will be adopted to the newly created incident. It can be done by clicking on the “New” button in the particular report view, as depicted in the figure below.



The result will be a new incident, which can be edited in the following mask as the next step.



The subject and the link to the basis event are automatically adopted. After the “Create” button has been pressed, the incident ticket has been created and following view is displayed.



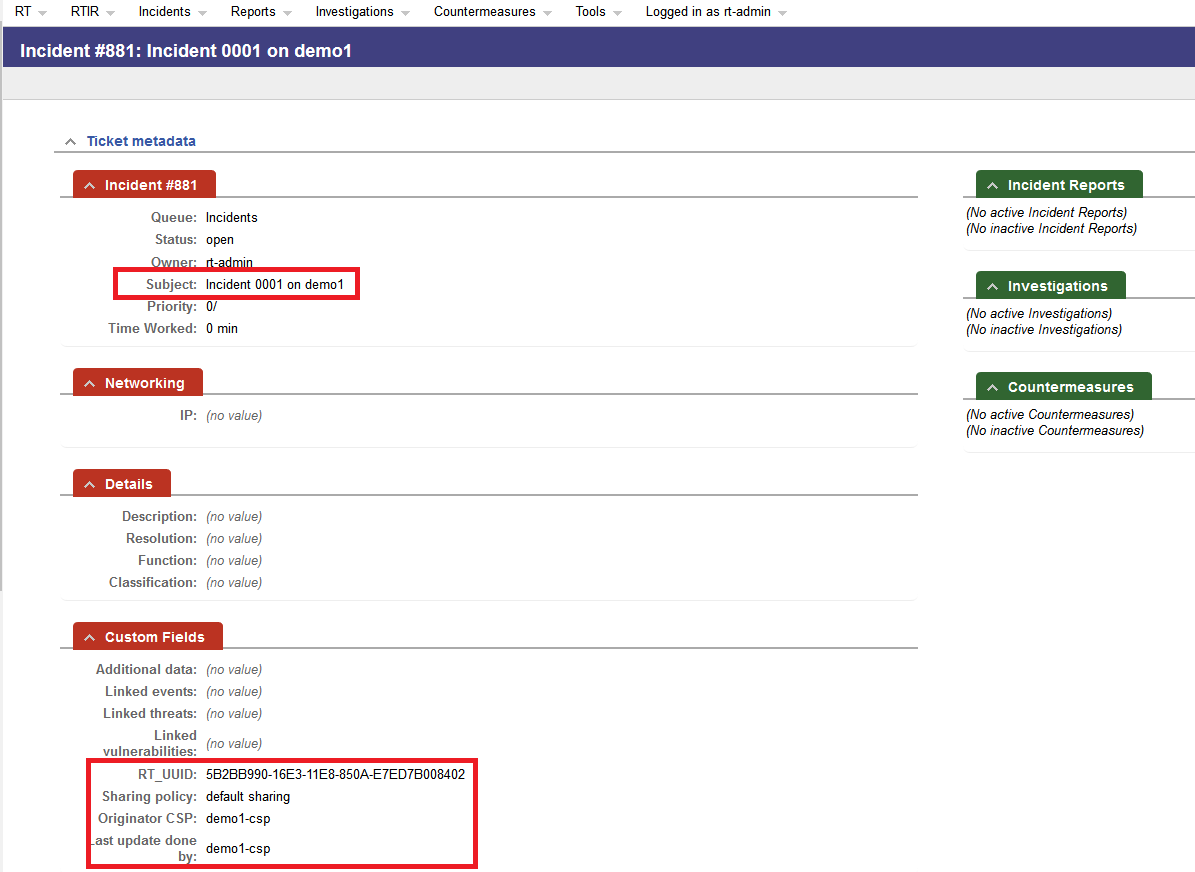
The incident report is based on the current incident, is automatically linked to this incident (see right upper corner), similar as the event which caused the creation of the basis report. The incident has a new UUID and bot values for originator CSP and the CSP, which did the last update, are assigned to the current CSP (demo2-csp in this example).

### Create an incident shared by another CSP instance

In case an incident has been shared by other CSP and the sharing policy foreseen, that this information will be transferred also to the current CSP a new incident will be automatically created in the current CSP.

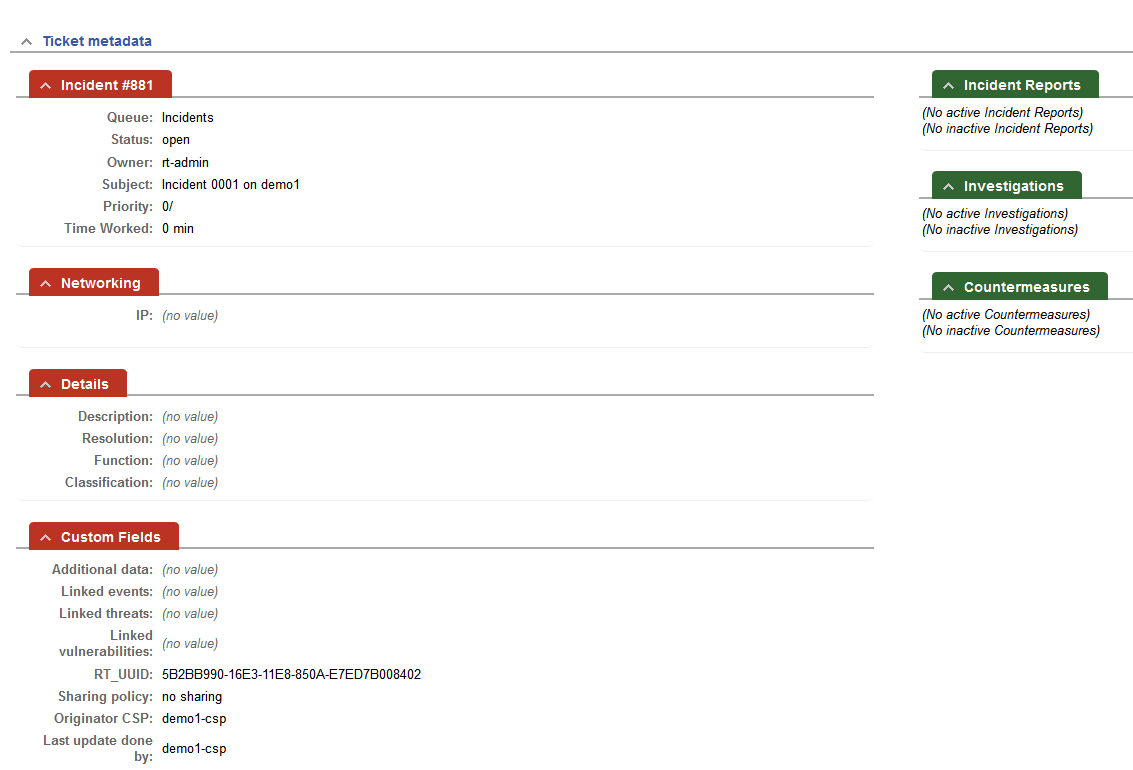
The remote CSP (CSP demo1 in the example) created an incident and set the sharing policy to “default sharing”, which caused the transfer of the incident data to the current CSP (CSP demo2 in the example). Following figure shows the incident in the remote CSP (demo1).

For more information, how to set up the appropriate sharing policy please refer to the chapter 5.3.2.



The Subject of the newly created and shared incident is “Incident 0001 on demo1”, the UUID is “5B2BB990-16E3-11E8-850A-E7ED7B008402”, “default sharing” is the policy currently applying, originator CSP is “demo1” as well as the last update has been done by CSP “demo1”.

After receiving the transferred incident data and creating an incident, locally following data can be viewed on the current (local) CSP (demo2).



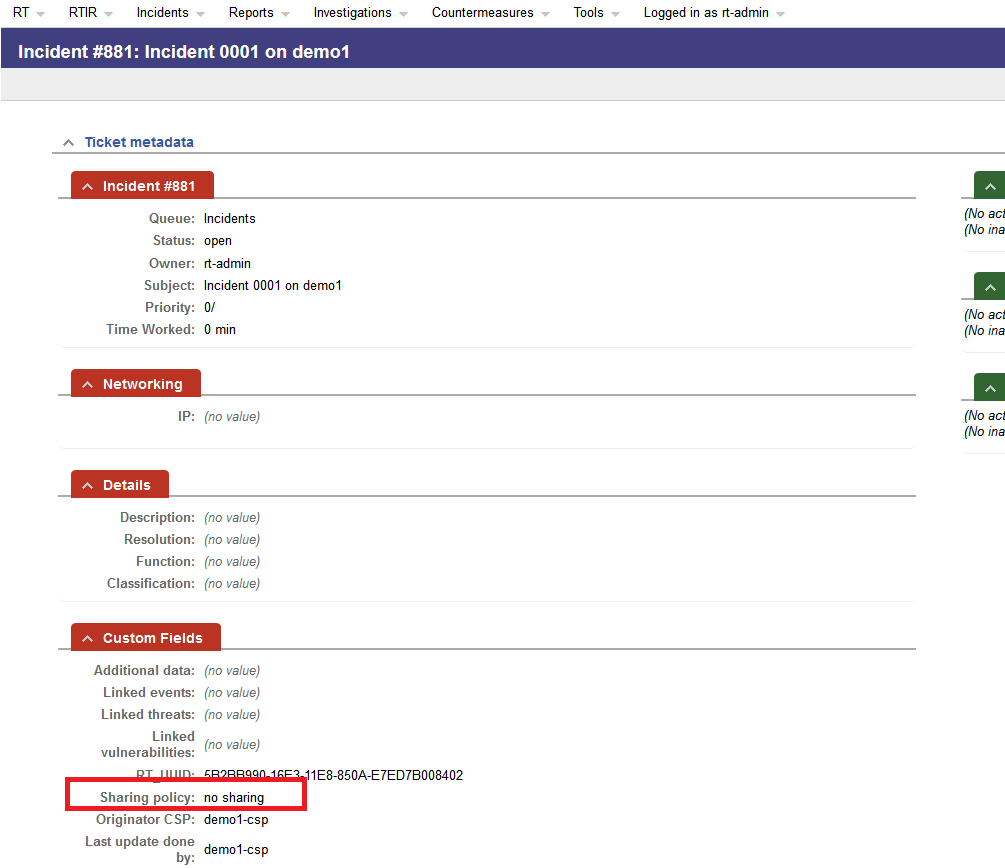
The incident data has been successfully adopted. The value of the filed “Originator CSP” gives the indication where the creator of the given incident is. Following table gives a short overview of the mostl important sent and received data:

|  |  |  |  |
| --- | --- | --- | --- |
| **Remote CSP (demo1)** | | **Current (local) CSP (demo2)** | |
| **Name** | **Value** | **Name** | **Value** |
| *Subject* | Incident 0001 on demo1 | *Subject* | Incident 0001 on demo1 |
| *Ticket number* | 881 | *Ticket number* | xxx[[3]](#footnote-3) |
| *RT\_UUID* | 5B2BB990-16E3-11E8-850A-E7ED7B008402 | *RT\_UUID* | 5B2BB990-16E3-11E8-850A-E7ED7B008402 |
| *Sharing policy* | default sharing | *Sharing policy* | no sharing[[4]](#footnote-4) |
| *Originator CSP* | demo1-csp | *Originator CSP* | demo1-csp |
| *Last update done by* | demo1-csp | *Last update done by* | demo1-csp |

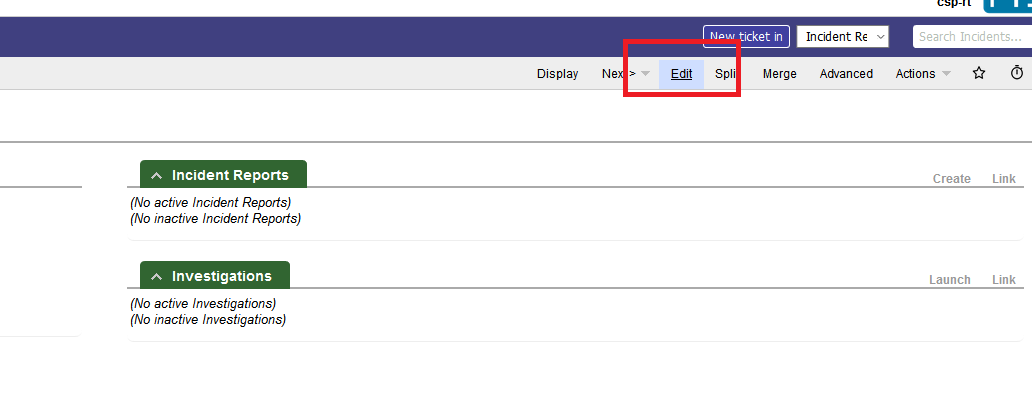
## Incident sharing

In order to share the incident with other CSP instances a particular sharing policy has to be assigned to a given incident.

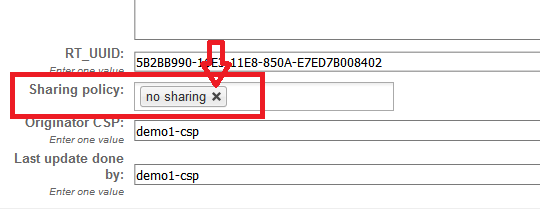
Select an incident to be shared (per default a newly created incident is not shared and the sharing policy is pre-set to “no sharing”).



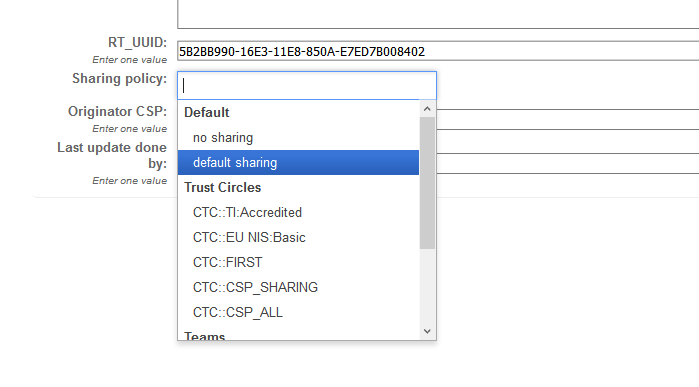
Click on the link “Edit”.



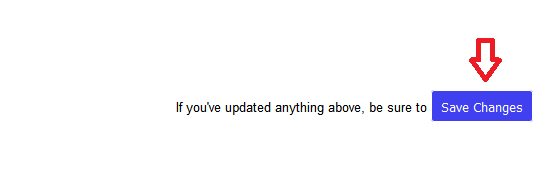
The editing view of the incident will display. Delete the “no sharing” policy, by clicking on the cross



Provide a new policy chosen from the drop-down-list, displayed after clicking on the empty field of “sharing policy”. In the example, a “default sharing” policy has been chosen.



After sharing policy has been set up, click on the “Save changes” button.



The new value of “sharing policy” has been stored by RT and the data of a given incident has been transferred to the IL in order to forward it to the recipients defined by the chosen policy.

# How to work with IntelMQ

Due to the special operation mode of IntelMQ (automatic intelligence harvester) a common CSP-user is not directly connected to this tool. Only IntelMQ Managers should be able to access the management GUI of IntelMQ and change its behaviour. If you are an IntelMQ manager/administrator please refer to the “Administration Guide” for further information on that.

# How to manage events with MISP

## Introduction

CSP provides the MISP (Malware Information Sharing Platform - http://www.misp-project.org) as a tool to be used to manage events. The used version of MISP is the latest one – 2.4.88. Furthermore, two dedicated MISP objects csp-rtir and csp-vulnerability are delivered together with MISP application, to properly handle the task of linking events with incidents and vulnerabilities.

For basic usage of MISP you may refer to the official guide: https://www.circl.lu/doc/misp/. This chapter aims to present the parts that are relevant to CSP functionality.

## Event management (create/edit/delete)

Event creation can be accomplished by selecting from the main menu: Event Actions -> Add Event. At this stage, as shown in the figures below, the user can determine the distribution level of the new event.

|  |  |
| --- | --- |
|  |  |

Please notice the following rules:

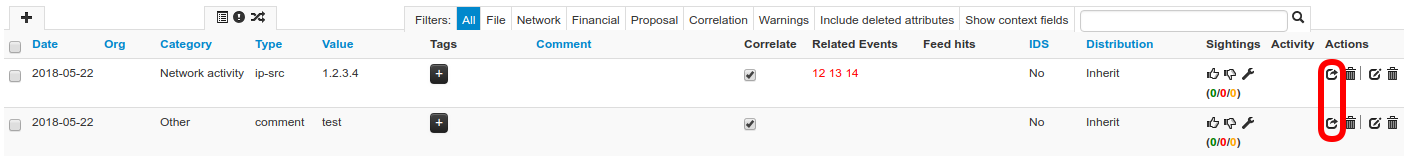
* If user does not select Sharing Group option for Distribution level, the Event will be automatically shared based on Integration Layer (IL) policies.
* If user desires the event to be shared with a specific Trust Circle, then he has to select Sharing group as Distribution level of the event and the corresponding Sharing Group has to be be selected from the extra drop down menu. Sharing groups names are formatted like CSP::CTC::{name} or CSP::LTC::{name}, for Central Trust Circles and Local Trust Circles, respectively, where {name} represents the name of the Trust Circle. For better understanding the link between Trust Circles and Sharing Groups, please have in mind the following remarks:
  + Local and Central Trust Circles are synchronized as MISP Sharing Groups, with name in format: CSP::LTC::{name} or CSP::CTC::{name}, where:
  + LTC part stands for Local Trust Circle
  + CTC part stands for Central Trust Circle
  + {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
  + MISP’s local administrator(s) 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.

After the user presses the Add button he is automatically transferred to the view of the newly added event. The left-most menu of this page provides a list of useful operations such as:

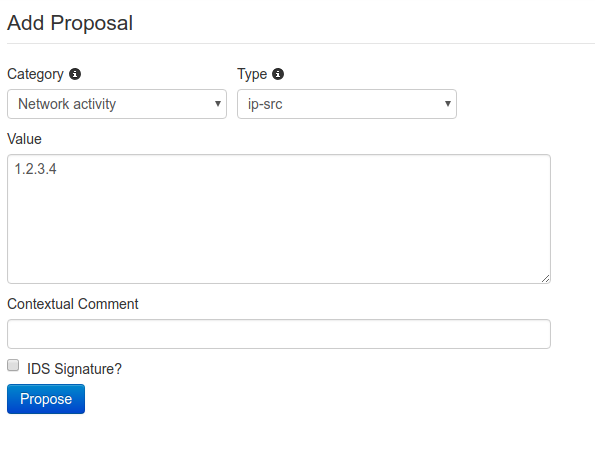
* Edit the event
* Delete the event
* Add Attributes/Objects/Attachments
* Publish the event.

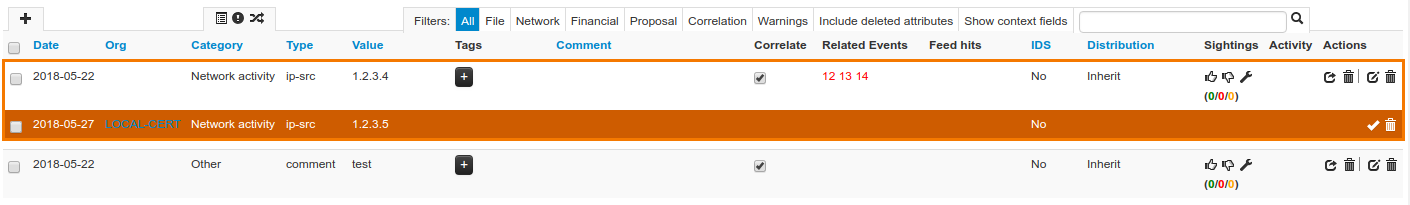
The user has full control of editing and sharing Events that are owned by the organization the user belongs to. In that case the user can edit an Event’s info field or attributes/objects and share them with the IL through the standard mechanism.

However, users that want to edit events that were created and shared from an external organization should not edit the event fields and share it to the IL. In that case, user should use the proposal mechanism that MISP provides. The user can propose edits on attributes and objects via the “Propose Edit” command.



By pressing the “Propose Edit”, MISP opens “Add Proposal” page where the user proposes a new value for the respective field.

By issuing the “Propose” command through the respective button the proposal is added under the attribute.

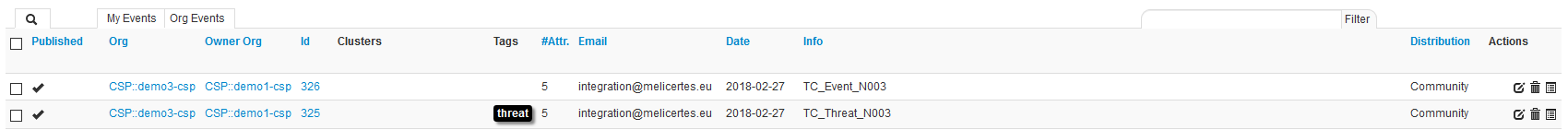


## Linking event with incidents

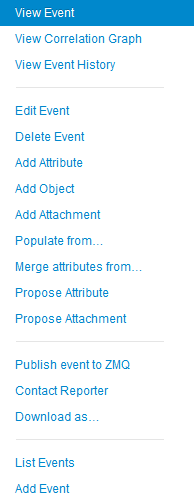
As already mentioned, A dedicated MISP object “csp-rtir” is delivered together with MISP application, to properly handle the task of linking events with incidents.

This can be accomplished by adding objects to an already existing MISP event as following:

From the main menu, we select: Event Actions -> List Events and search the event we would like to link with incidents. After locating the record of interest, we press the edit or the view button in right-most column of the table named Actions, as shown below:



Afterwards we are transferred to the Edit/View screen of the selected event. In both cases, the option “Add Object” is visible to the right-most menu, as shown below:



By pressing “Add Object” we can link the selected event with Incidents, by selecting “Misc” category in the popup menu and then “Csp-rtir” object

These are illustrated below:

|  |  |
| --- | --- |
|  |  |
|  |  |

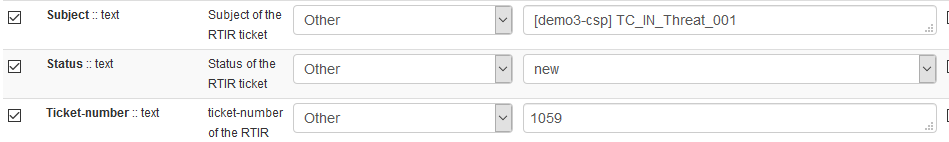
Csp-rtir objects require 3-additional parameters to be specified, named:

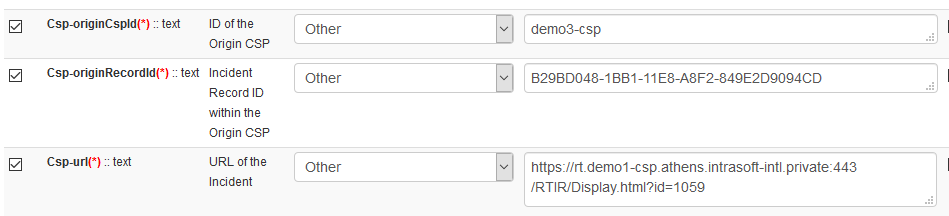
* Csp-originCspId: the {cspId} value of the origin CSP of the incident/threat
* Csp-originRecordId: the incident ID of the origin record (within the origin CSP)
* Csp-url: the url of the incident

***Note:***

*The values from the above mentioned fields, regarding specific incidents can be acquired via the Search (Kibana) app.*

An example of how to complete the required fields on Csp-rtir object is provided below together with a screenshot of related Kibana results:



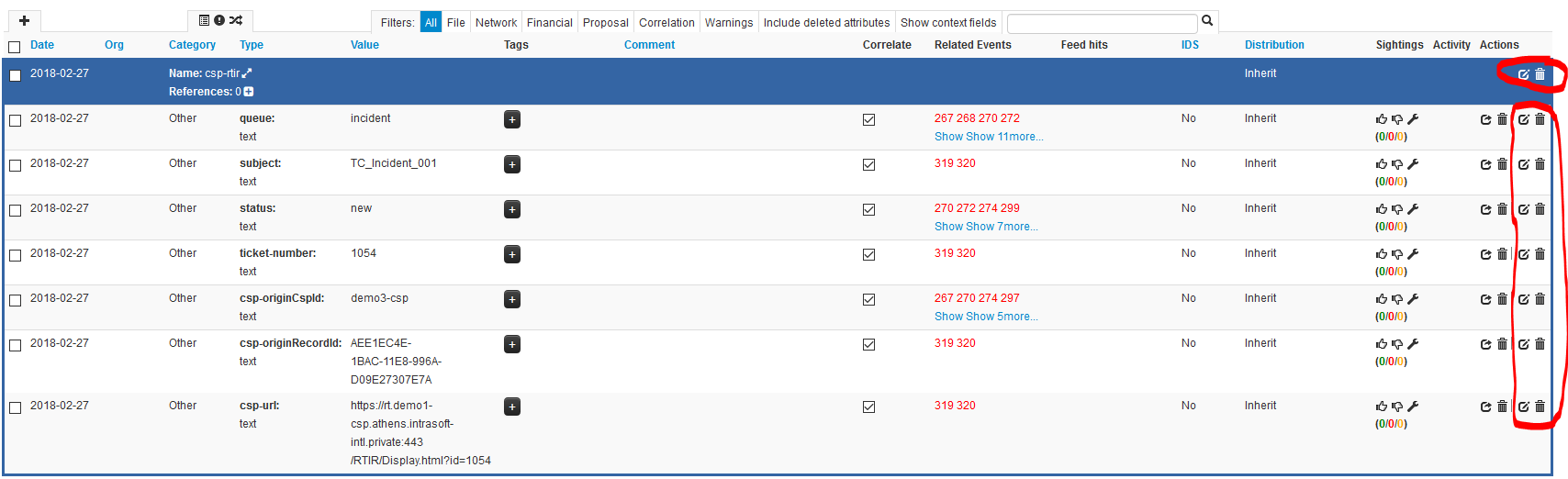








Managing the Csp-rtir objects themselves can be accomplished either on the Edit or the View screen of an event. In the example below, the edit/delete buttons for the entire object and per specific field of the object are highlighted.



## Event sharing

In general, publishing an event via Integration Layer (IL) can be accomplished via command “Publish Event” or “Publish (no email)”. The event that the user creates is not shared via IL unless the user publishes it (“Publish (no email)”).

Also, when the event is being edited (either itself or its linked objects/attributes) the user has to publish it again (“Publish Event” or “Publish (no email)”) in order to share the updates with the IL.

In case the event is already published (the commands “Publish Event” and “Publish (no email)” are not available at left most menu) and the user needs to share the Event (e.g. he wants to share some proposals on a published event) with the IL, then he can accomplish that via the command “Publish event to ZMQ” located at the left most menu.

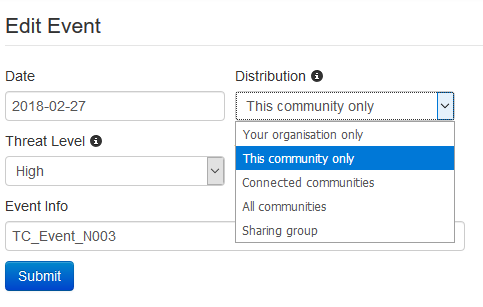
For better understanding CSP integration with MISP application, please have in mind the following remarks, regarding Event Sharing.

A. Distribution

When adding a new Event or editing an existing one, Distribution field should have one of the following values in order for the Event to able to be shared, as illustrated in following figure:

* This community only
* Connected communities
* All communities
* Sharing group. In this case the appropriate Sharing Group should also be selected from the extra provided drop down field.

Distribution value “Your organisation only” will not allow the Event to be shared.



B. Sharing

Provided that Distribution field of a specific Event has not the value “Your organisation only”, the Event should be published in order to be shared with other CSP instances. Please refer to 7.2 for more information.

**Important notice:**

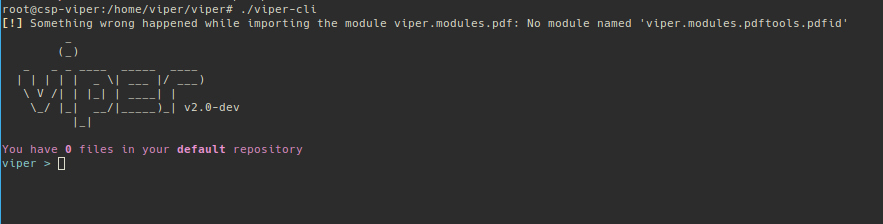
CSP sharing mechanism can share events based on the Sharing Group or Distribution field selected by the user for this event. Although MISP supports more fine-grained sharing policies for individual attributes and objects, this is not taken into account by the CSP. In case special handling of sharing policies is required, this can be done either in Sharing Policies or in Anonymization applications of CSP.

# How to work with Viper

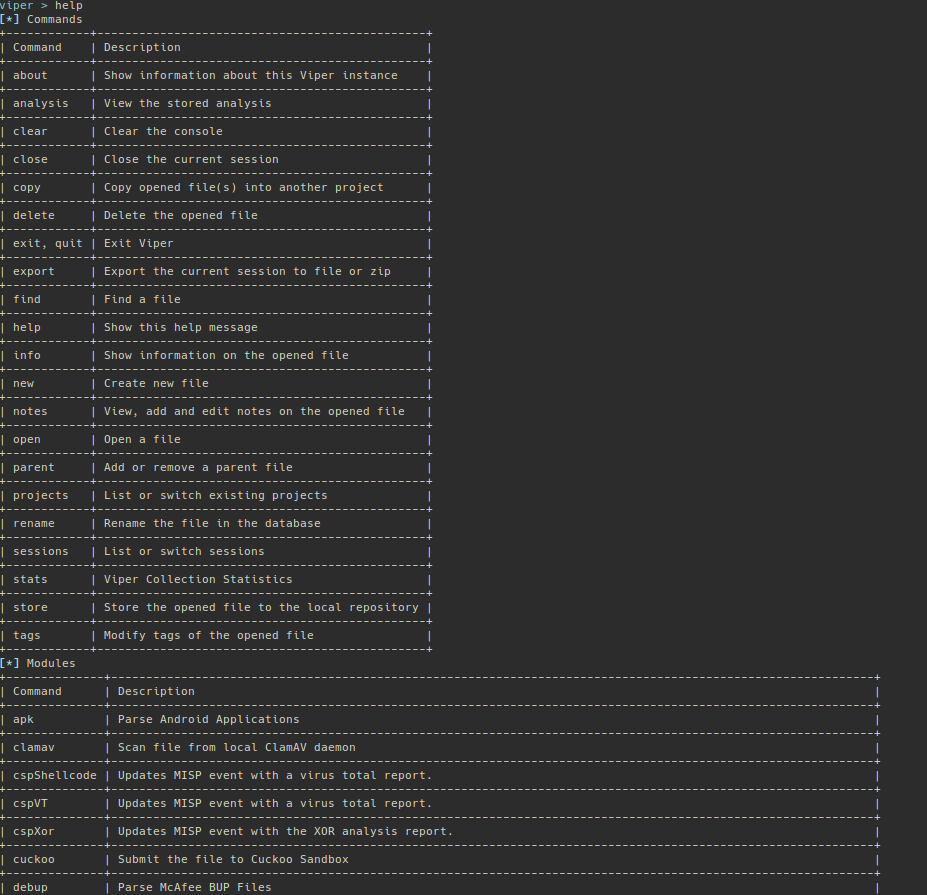
CSP provides Viper, a binary analysis and management framework. Its fundamental objective is to provide a solution to easily organize your collection of malware and exploit samples as well as your collection of scripts you created or found over the time to facilitate your daily research. Think of it as a Metasploit for malware researchers: it provides a terminal interface that you can use to store, search and analyze arbitraty files with and a framework to easily create plugins of any sort.

CSP integrates Viper with MISP to share malware analysis results through MISP events. For that purpose, three additional modules that manifest that integration are implemented for Viper, namely: cspVT, cspXor and cspShellcode.

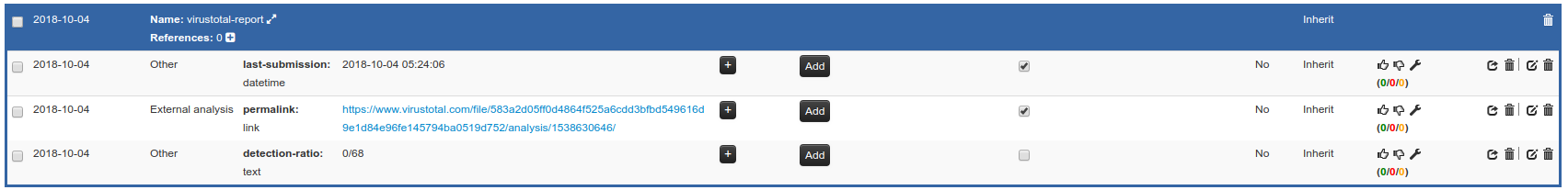
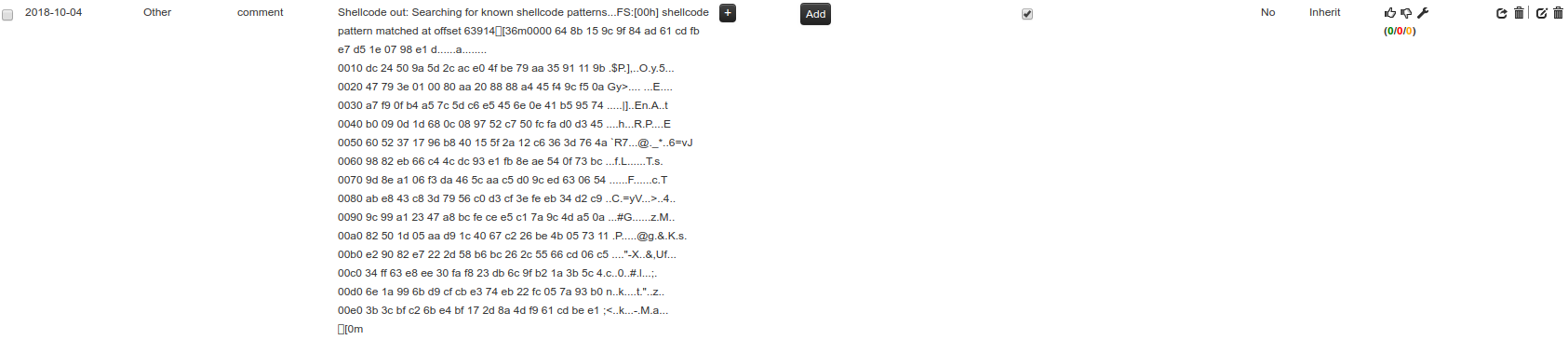
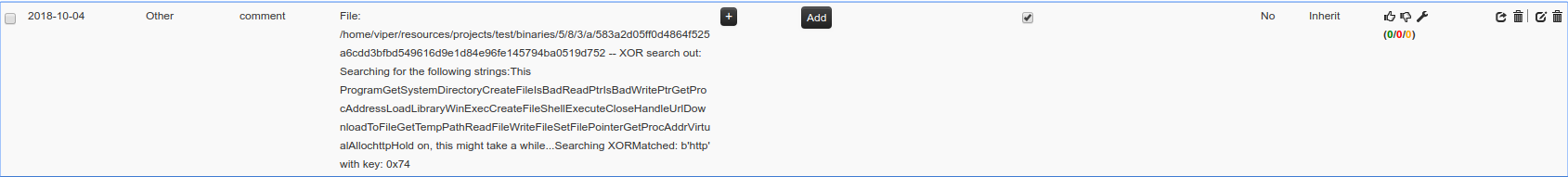
The Viper module provides two interfaces for user interaction. First, a web UI is provided where the user authenticates its identity through the CSP SSO mechanism. Web UI supports basic functionality for Viper while the Viper functionalities in full scale are exposed through the command line interface (CLI). User can access the Viper cli through the csp-viper container. Particularly, the steps that need to be performed to access viper-cli are the following:

* 1. SSH to the CSP server
  2. Enter the csp-viper container: 
  3. Enter the viper-cli as shown in screenshot: 

After entering the viper-cli, user has full access to all the functionality that Viper provides. The help command will print a list of all the available commands along with a brief description. As shown below, among the rest of Viper modules, exist the cspVT, cspXor, and cspShellcode modules. These modules integrate the vt, shellcode and xor modules that already exist in Viper with the CSP-MISP instance.



In order to observe how these modules, integrate Viper with MISP you should perform the following steps:

1. Create a new MISP event from the MISP web ui
2. Enter Viper web UI (SSO should work and log you in as the demo user that OpenAM authenticates) & create a new Viper project through the Viper web ui
3. Upload an artifact to Viper project through the Viper UI
4. Log in to your CSP server through ssh
5. Enter the csp-viper container:   
   **#docker exec -ti csp-viper /bin/bash**
6. List existing viper projects:  
   **>projects -l**
7. Open the project you created through the web ui:  
   **>projects -s <project name>**
8. Find files contained in the viper projects:  
   **>find all**
9. Open the respective file:  
   **>open <the file hash as reported at previous step>**
10. Pull the MISP event you created at step 1:  
    **>misp pull <event id>**
11. Store the hashes that viper generates to the MISP event:  
    **>misp upload**  
    The event at the MISP UI should be populated with a new file object as shown below:  
    likecspVT module:  
    **>cspVT**Since the execution of cspVT is completed the event should be populated with a new object (virustotal-report) that should look like the following:  
      
    The permalink link attribute of the virustotal-report object, gets the report that the virus total service created for that particular object.
12. Run the cspShellcode module:  
    **>cspShellcode**  
    The results of the cspShellcode populate a new MISP event attribute like the following:  
    
13. Run the cspXor module:  
    **>cspXor**  
    The results of the cspXor populate a new MISP event attribute like the following:  
    

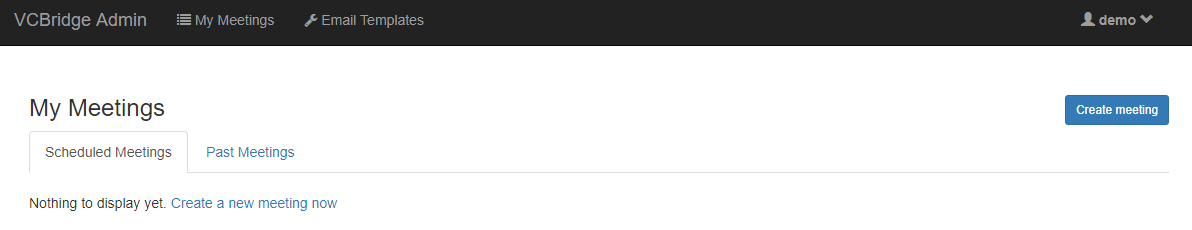
# How to manage and join video conferences with VCB

## Introduction

CSP provides the VCB (Video Conference Bridge) module as a tool to be used to organize and join video conferences with organization’s internal or external users. The VCB module is based on Jitsi open-source project (<https://jitsi.org/>). VCB module and offered features is delivered with two user interfaces; one for creating/managing the video conferences (namely: teleconf-ui) and one for allowing (internal or external) users to participate in scheduled video conferences (namely: teleconf). This chapter covers features and functionalities of the user interfaces while for basic usage of Jitsi you may refer to the official guide: https://jitsi.org/. This chapter aims to present the parts that are relevant to CSP functionality.

## Video conferences management

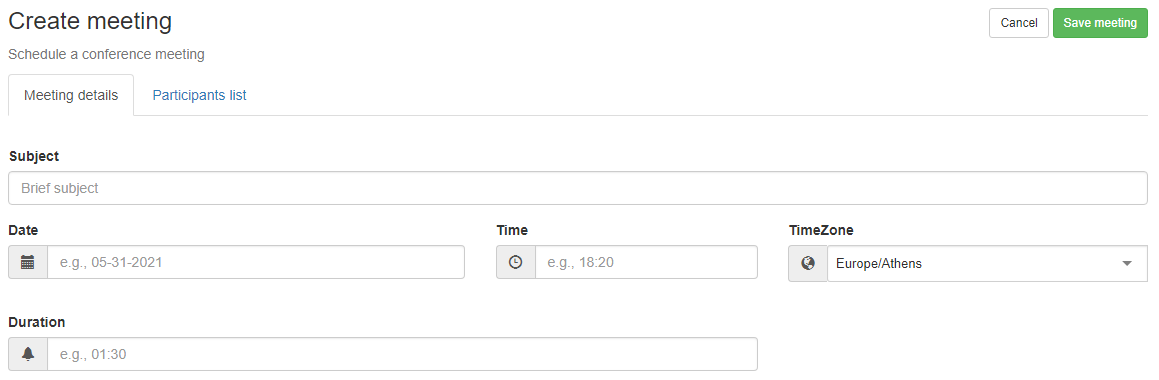
Video conferences management interface (teleconf-ui) can be reached via: **Error! Hyperlink reference not valid.**, after authenticating via OpenAM. Two functionalities are offered in a simple interface, as shown in the image below; management of meeting, i.e. schedule new meetings or list previous ones and managing email templates for meetings notifications.



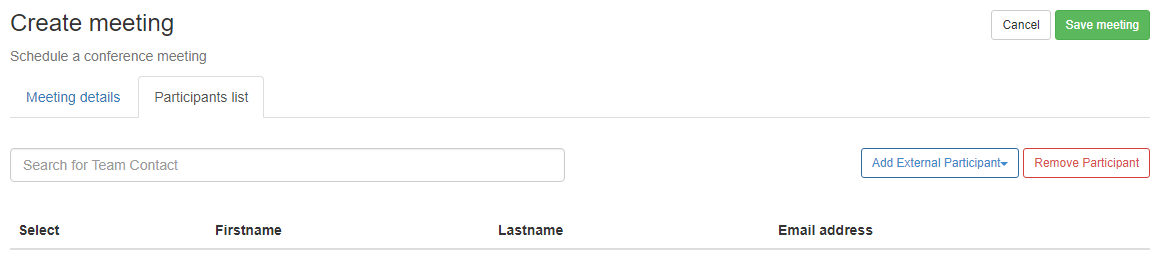
### Create a video conference

In order to create/schedule a video conference, the user has to press the button “Create meeting”, as shown in the previous screenshot and fill the two tabs with required information.

The first tab requires meeting’s basic details, such as: Subject, Date, Time, TimeZone and Duration, as depicted below.



The second tab requires participants information, as depicted below.

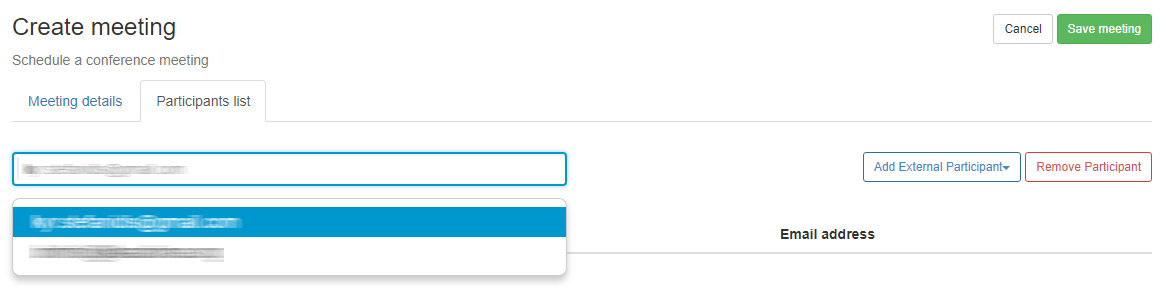


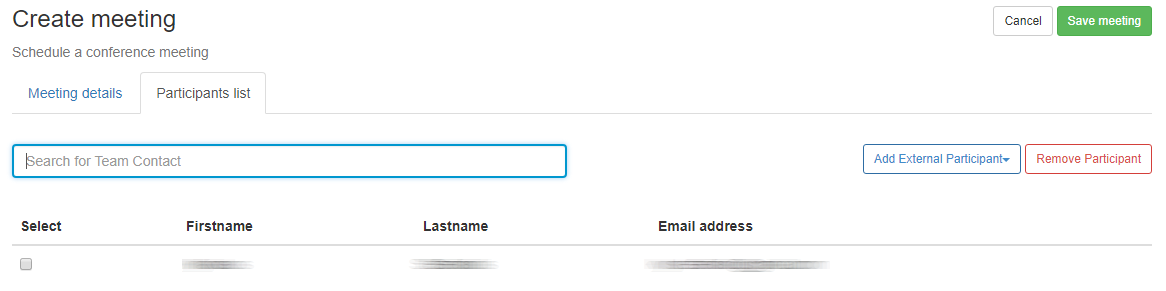
**Note:**

All fields in both tabs are required when creating a meeting.

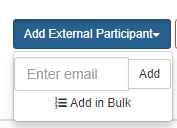
Meeting’s participants can be added in two ways, based on their originality; if they are organization’s internal contacts (already known to Trust Circles) or external to organization.

**To add an internal participant**, user should begin typing in the text-field named “Search for Team Contact” some characters based on participant’s email, first or last name. Then a dropdown list appears suggesting matching contacts from organizations Trust Circles Person Contacts (refer to chapter 3 for more information) and selecting one of the proposed entries concludes in the addition of the selected contact as a participant to the current meeting, as shown in the next screenshots.

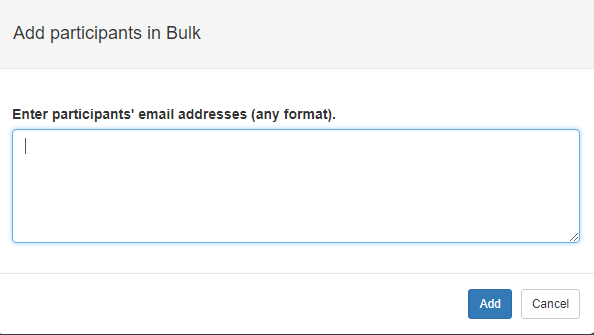




**To add an external participant**, the button “Add External Participant” has to be selected, which offers the options either to add a single external participant by adding his/her email to the textbox and press “Add” button or to add multiple external participants in bulk mode.



In case bulk mode is selected a dialog opens prompting for massively entering email address, while various formats are supported, as explained below.



Participants emails must be entered in format:

{First Name} {Last Name} <{email}>

and multiple entries can be separated by comma (,), semicolon (;) and carriage returns/line feeds.

Participants emails could be also entered without name information, using only the email field and separated as previously mentioned.

Below is an extended example for better understanding:

email1@example.com;email2@example.com,email3@example.com

email4@example.com

fname1 lname1 <fname1@example.org>

fname2 fname2@example.org

fname3 lname3 fname3@example.org

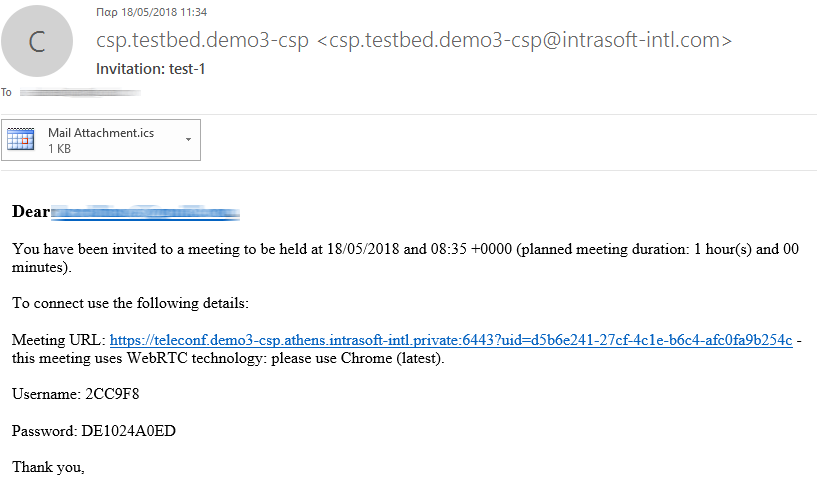
fname4@example.org fname4

fname5 lname5 <fname5@example.org>;fname6 lname6 <fname6@example.org>,fname7 lname7 fname7@example.org

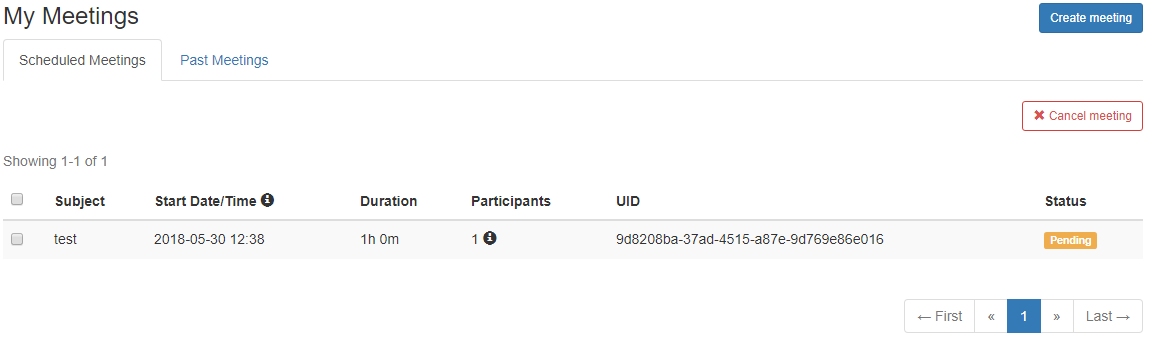
All above notations are valid. Lines 5 and 7 will conclude to participant with only email, since they do not follow: first last email, notation, but they will not trigger an error and the corresponding email will be added.

When all previously mentioned information regarding the meeting is entered, the user has to save the meeting by pressing the “Save” button.

Saving a meeting will trigger the process of sending email invitations to all added participants. The invitation email will be formed as in the following example.



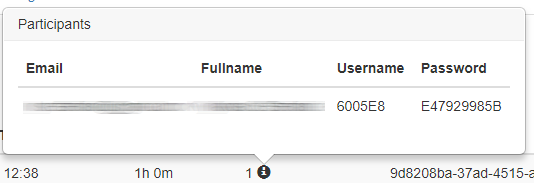
After a meeting has been saved, the list of scheduled meetings is presented, as shown below.



Here the meeting organizer is able to quickly review meeting’s information, participants and status. Status label will have one of the following:

* Pending, a meeting is scheduled and has not started yet (based on its Start Date/Time and Time zone)
* In progress, a meeting has started (based on its Start Date/Time and Time zone)
* Error, a meeting failed to start due to a systemic error.

Finally the list of participants can be quickly reached together with their login information for participating in the video conference, by pressing the  icon in the middle of each entry, as shown below.

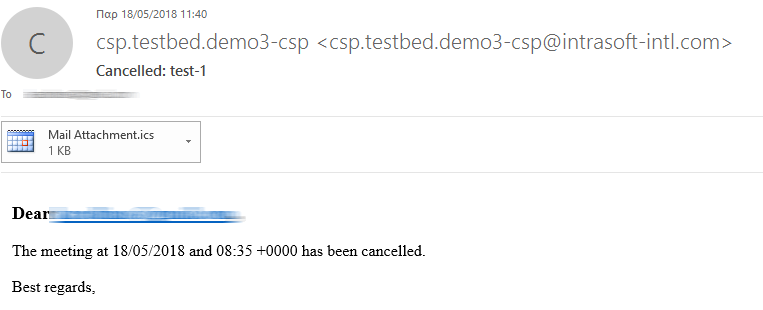


The appeared window can be closed by pressing the  icon again.

### Cancel a video conference

A scheduled or in progress meeting can be canceled by the meeting organizer by selecting its preceding select box  (first item in entry row) and then pressing the “Cancel meeting” button.

Saving a meeting will trigger the process of sending email cancelations to all added participants. The cancellation email will be formed as in the following example.

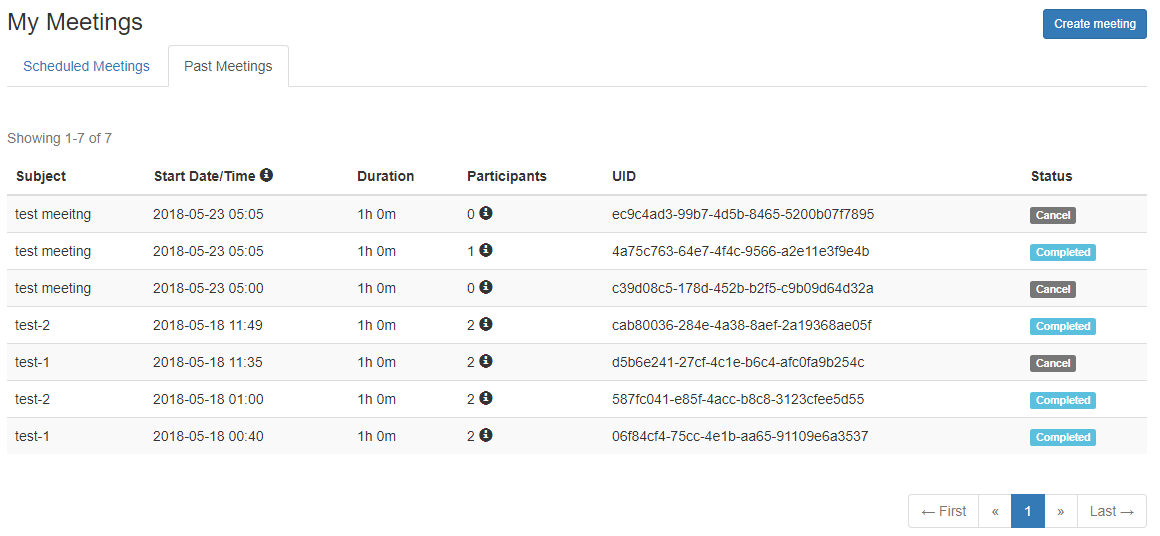


**Important notice:**

If the meeting organizer selects to cancel a meeting that is already in progress and participants have already logged in it, meeting cancellation won’t be able to dynamically stop the already ongoing conference. Participants to a cancelled meeting will be prohibited from entering in it only if they try to log in after the meeting cancellation.

### Past video conferences

Past video conferences list is presented after selecting the “Past Meeting” tab, as shown below.

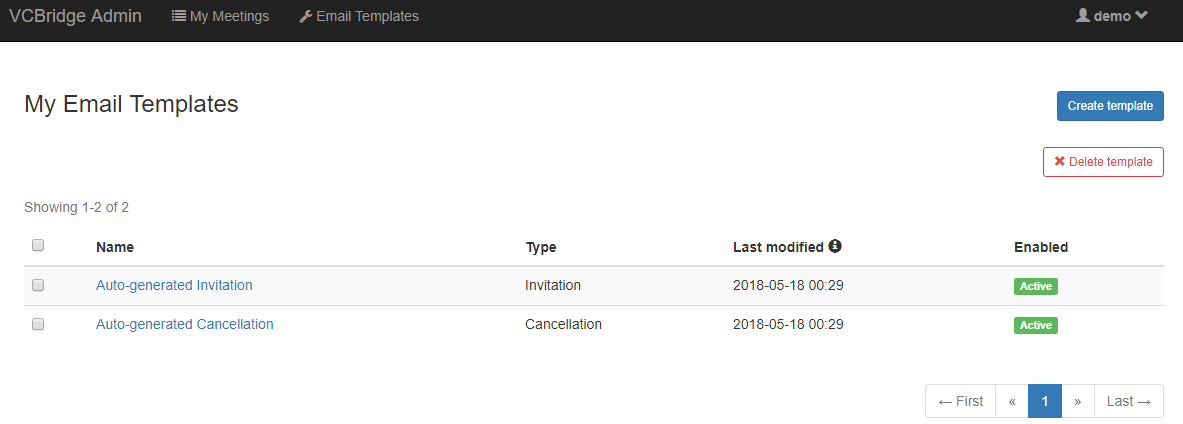


Similarly as previously mentioned, the organizer can quickly review meetings’ information, participants, etc. as well as its status, whereas the status label can be:

* Completed, for a meeting that has normally expired (based on its Start Date/Time and Time zone)
* Cancel, for a meeting that has been cancelled by the organizer
* Error, a meeting failed to start due to a systemic error.

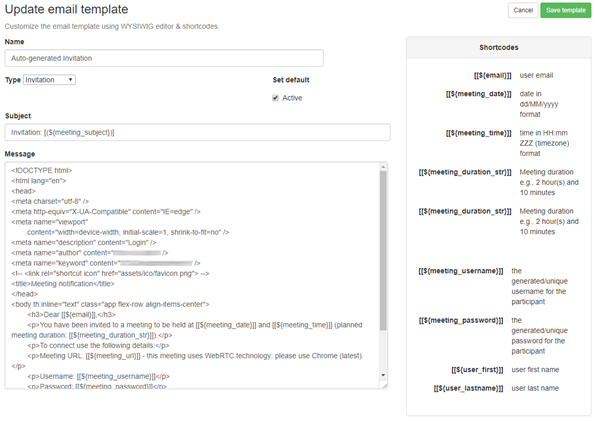
### Managing email templates

As already mentioned, two types of emails are sent by the system to the participants of a meeting; one as an invitation to a scheduled meeting and one as a cancellation to a cancelled meeting. The email templates and their content can be managed by selecting the menu “Email Templates” from the top-most menu, as shown below.



By default, system auto-generates the two email templates, and the user is able either to edit them or create new templates.

When editing an email template, the user has to fill the following fields:



* Name: a name for the template
* Type: has to be either Invitation or Cancellation
* Active: Exactly one template has to be active per template type, i.e. one active invitation template and one active cancellation template
* Subject: the subject of the email to be delivered
* Message: the message of the email to be delivered

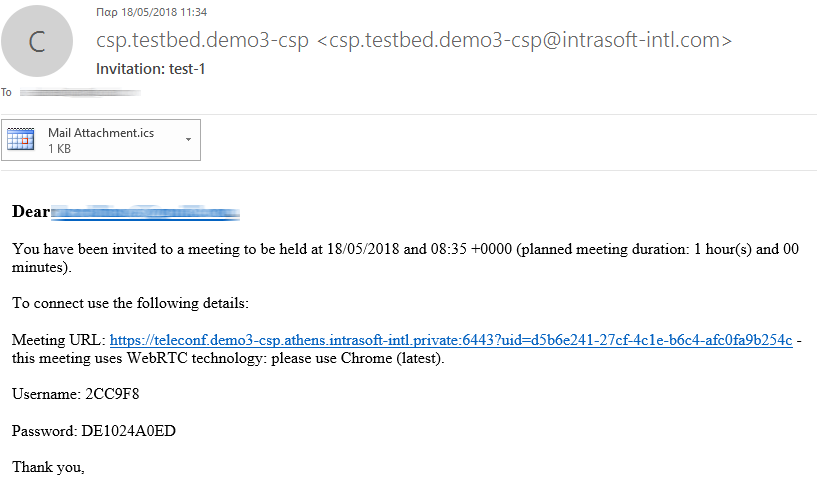
In Subject and Message fields user can enter some shortcodes, as shown in the right part of previous screenshot.

**Important notice**:

Message field has to be filled with proper HTML syntax.

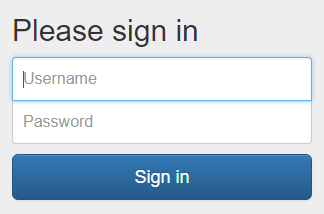
## Video conference participation

As previously explained, each of a meeting’s participants will be sent an email invitation to his email, with all required data for entering the video conference. The email received by a participant will be like the following screenshot.

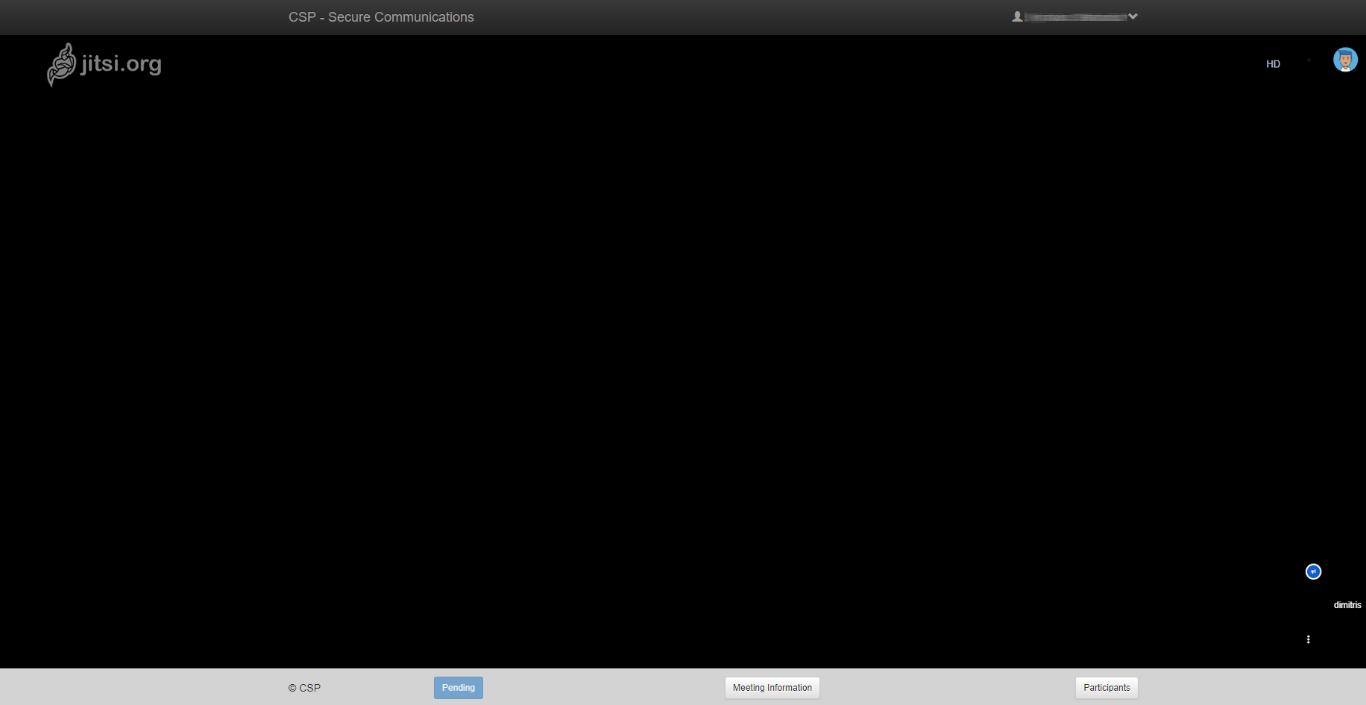


The participant has to follow the URL and provide the credentials that are also mentioned in the invitation’s email body. Notice that the conference application (namely: teleconf) does not require an OpenAM session, but only valid user credentials so as to allow external participants from outside the organization.

The login prompt to the conference application will be as follows:



After successful login, the user will be redirected to the video conference application, as shown below:

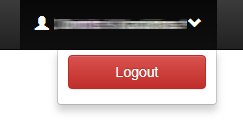


**Note**:

At the bottom of the window the user is able to find useful information regarding the meeting, such as meeting start/end date/time and participants.

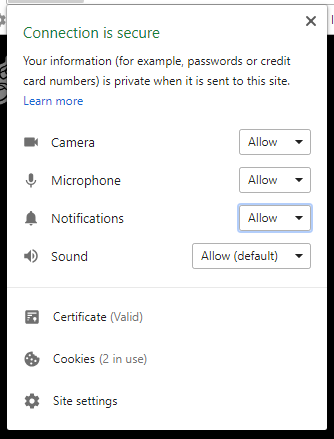


The participant is able to logout from the video conference application by selecting “Logout” from the dropdown menu located at the right of the top most menu.

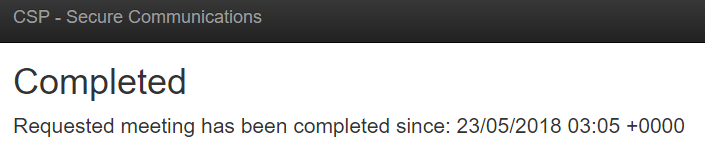
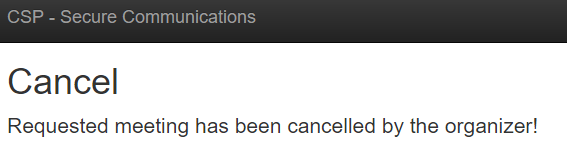


**Important Notice**:

For best experience and smooth operation of the video conference the user should use Chrome browser (latest version), since the application is based on Jitsi which uses WebRTC technology. Moreover, browser should be advised to allow access on specific devices, such as camera, microphone and sound, as shown below.



In case a participant tries to login after a meeting has expired (based on its Start Date/Time and Time zone) or has been cancelled by the organizer, then he won’t be able to actively join a video conference and will be subsequently inform for the meeting state, as shown below.

- End of document-

1. In case you would like to use MELICERTES certificates, it is strongly recommended to provide the department name in order to be able to revoke certificates of other CSIRTs, which containes a user name also valid for your CSP instance. Background: the certificate driven authentication procedure checks the issuer of the certificate (in both cases the same) and maps the CN of DN into an existing userid in OpenAM. If there is a department name specified while applying the certificate, it is stored as OU. This could be checked as well during authentication, thus the certificate with the same userid (CN) but different department names (OU) wouldn’t work on the same CSP instance. [↑](#footnote-ref-1)
2. For the future use in this chapter: if the terminus RT is used, than it means always RT plus RT::IR. [↑](#footnote-ref-2)
3. Every RT instance manages the ticket numbers locally, which are unique only inside of this instance of RT. [↑](#footnote-ref-3)
4. While creating a new incident, „no sharing“ has been set as a sharing policy. The operator can change the policy any time. [↑](#footnote-ref-4)