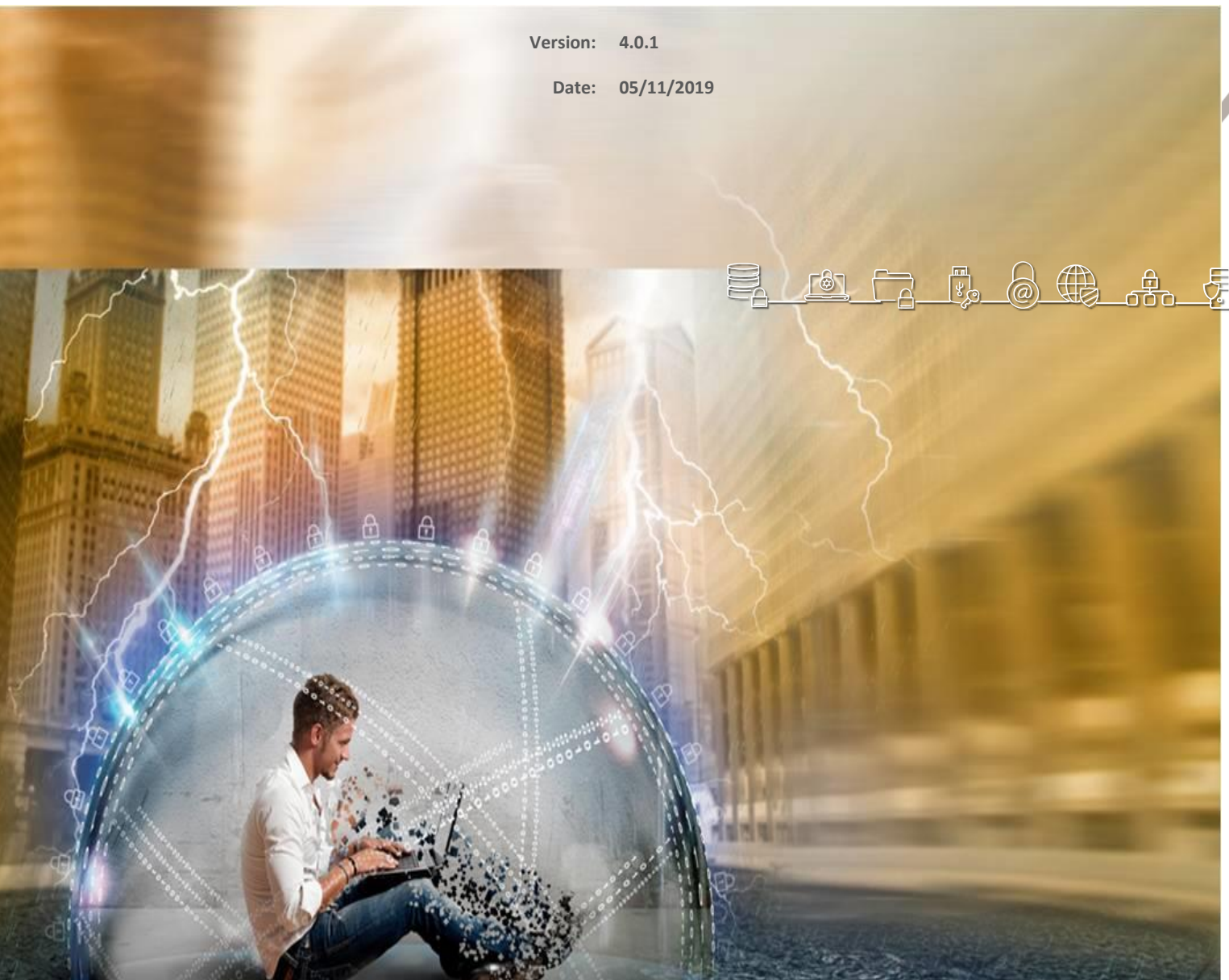


## **CEF: Cybersecurity Digital Service Infrastructure;** Core Service Platform – SMART 2015/1089

### User Manual

Version: 4.0.1

Date: 05/11/2019



<b>1</b>	<b>USER CERTIFICATE HANDLING .....</b>	<b>4</b>
1.1	Requesting a user certificate via MELiCERTES PKI .....	4
1.2	Applying for the certificate .....	4
1.3	Receiving the certificate .....	8
1.4	How to backup of user certificate .....	11
<b>2</b>	<b>HOW TO SEARCH AND VISUALIZE DATA WITH KIBANA .....</b>	<b>16</b>
2.1	Searching for Data .....	16
2.2	Visualizing Data .....	18
<b>3</b>	<b>HOW TO MANAGE CONTACTS WITH CMM .....</b>	<b>20</b>
3.1	Introduction.....	20
3.2	Recording data and meta data of contacts.....	20
3.3	Receiving data of contacts .....	22
3.4	Recording data and meta data of local team .....	23
3.5	Exporting local team data to FIRST .....	24
3.6	Exporting local team data to TF-CSIRT/TI.....	24
3.7	Importing team data from TF-CSIRT/TI .....	24
3.8	List Local Contact entries .....	24
3.9	Read Local Contact entry .....	25
3.10	Delete Local Contact entry.....	26
3.11	List Local and Central Trust Circles .....	27
3.12	Read Local Trust Circle .....	28
3.13	Write Local Trust Circle .....	28
3.14	Delete Local Trust Circle.....	29
3.15	Create a new Local Trust Circle .....	29
<b>4</b>	<b>HOW TO MANAGE CONTACTS WITH CMM .....</b>	<b>31</b>
4.1	Introduction.....	31
4.2	Recording data and meta data of contacts.....	31
4.3	Receiving data of contacts .....	33
4.4	Recording data and meta data of local team .....	34
4.5	Exporting local team data to FIRST .....	35
4.6	Exporting local team data to TF-CSIRT/TI.....	35
4.7	Importing team data from TF-CSIRT/TI .....	35
4.8	List Local Contact entries .....	35
4.9	Read Local Contact entry .....	36
4.10	Delete Local Contact entry.....	37
4.11	List Local and Central Trust Circles .....	38
4.12	Read Local Trust Circle .....	39
4.13	Write Local Trust Circle .....	39
4.14	Delete Local Trust Circle.....	40
4.15	Create a new Local Trust Circle .....	40
<b>5</b>	<b>HOW TO MANAGE INCIDENTS WITH RT .....</b>	<b>42</b>
5.1	Introduction.....	42
5.2	Incident reports management .....	43
5.3	Creating incidents .....	44
5.3.1	Create an incident based on event driven incident report.....	44
5.3.2	Create an incident shared by another CSP instance .....	46
5.4	Incident sharing .....	49

<b>6</b>	<b>HOW TO WORK WITH INTELMO</b>	<b>51</b>
<b>7</b>	<b>HOW TO MANAGE EVENTS WITH MISP</b>	<b>52</b>
7.1	Introduction	52
7.2	Event management (create/edit/delete)	52
7.3	Linking event with incidents	53
7.4	Event sharing	55
<b>8</b>	<b>HOW TO WORK WITH VIPER</b>	<b>57</b>
<b>9</b>	<b>HOW TO MANAGE AND JOIN VIDEO CONFERENCES WITH VCB</b>	<b>60</b>
9.1	Introduction	60
9.2	Video conferences management	60
9.2.1	Create a video conference	60
9.2.2	Cancel a video conference	64
9.2.3	Past video conferences	64
9.2.4	Managing email templates	65
9.3	Video conference participation	66

## 1 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

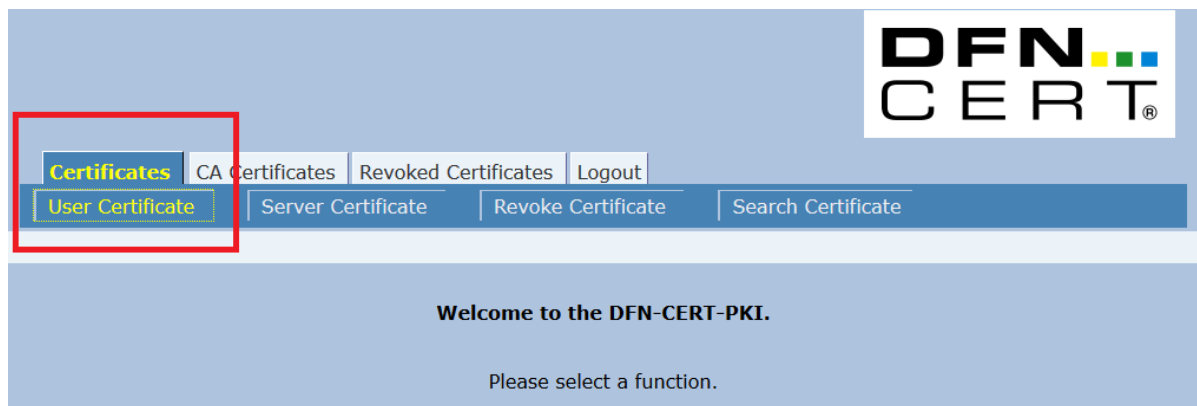
### 1.1 Requesting a user certificate via MELiCERTES PKI

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.

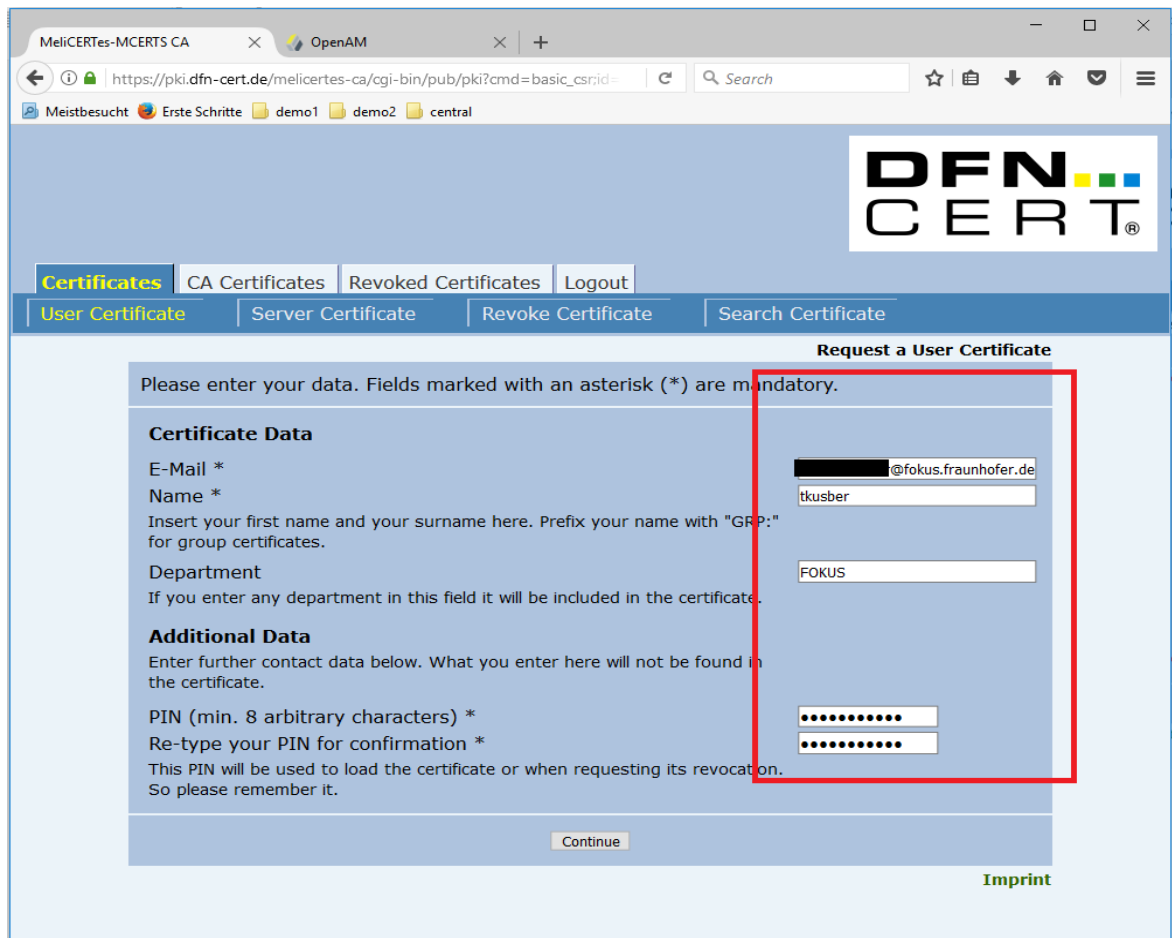
**Note! Only Firefox and Internet Explorer are currently supported.**

### 1.2 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.



MeliCERTes-MCERTS CA

OpenAM

https://pki.dfn-cert.de/melicertes-ca/cgi-bin/pub/pki?cmd=basic\_csr&id=

Meistbesucht Erste Schritte demo1 demo2 central

DFN CERT

Certificates CA Certificates Revoked Certificates Logout

User Certificate Server Certificate Revoke Certificate Search Certificate

**Request a User Certificate**

Please enter your data. Fields marked with an asterisk (\*) are mandatory.

**Certificate Data**

E-Mail \*

Name \*

Insert your first name and your surname here. Prefix your name with "GRP:" for group certificates.

Department

If you enter any department in this field it will be included in the certificate.

**Additional Data**

Enter further contact data below. What you enter here will not be found in the certificate.

PIN (min. 8 arbitrary characters) \*

Re-type your PIN for confirmation \*

This PIN will be used to load the certificate or when requesting its revocation. So please remember it.

Continue

Imprint

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
- 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.

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 contains 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.

MeliCERTes-MCERTS CA x OpenAM x +

https://pki.dfn-cert.de/melicertes-ca/cgi-bin/pub/pki

Meistbesucht Erste Schritte demo1 demo2 central

**DFN CERT**

**Certificates** CA Certificates Revoked Certificates Logout

User Certificate Server Certificate Revoke Certificate Search Certificate

**Request a User Certificate - Confirmation**

Please check your data.

**Certificate Data**

E-Mail [redacted]@fokus.fraunhofer.de

Name tkusber

Department FOKUS

**Additional Data**

Publish No

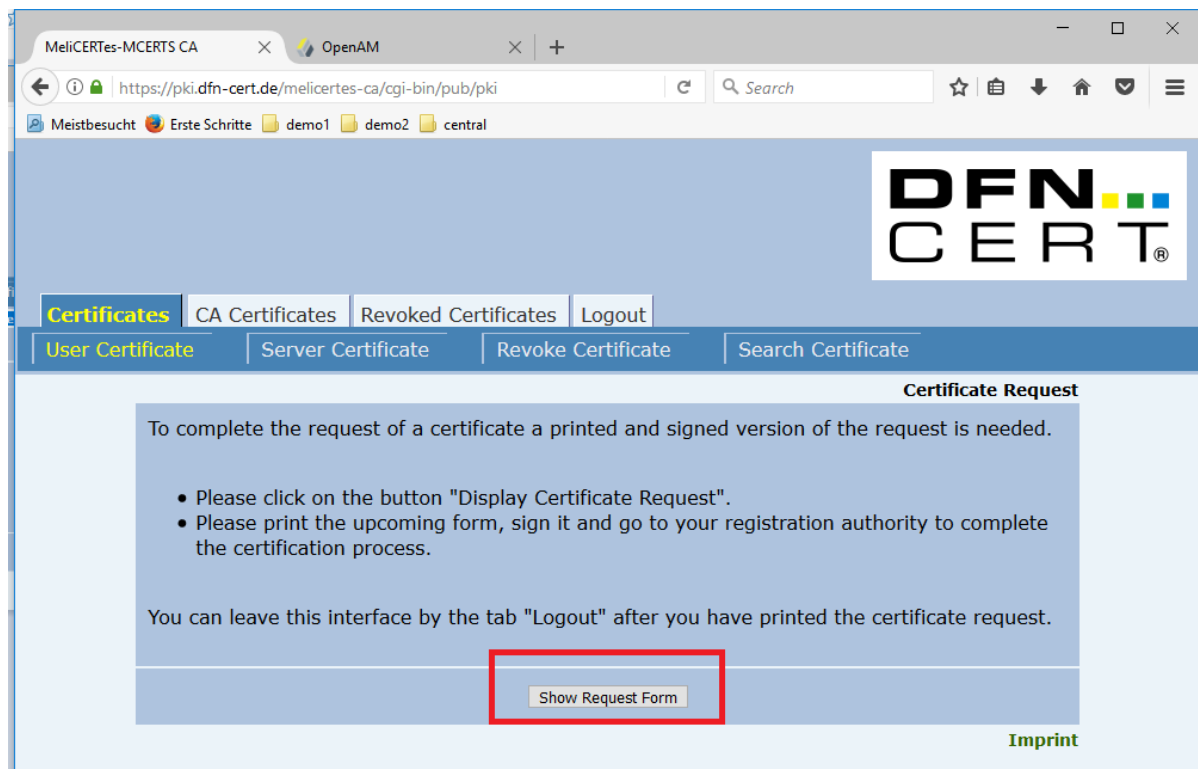
Change Confirm

Imprint

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 - <cspld>".

## Application for a User Certificate

- to: MeliCERTes-MCERES CA -

Application number 5408

### Applicant

Given Name(s) Last Name tkusber  
E-Mail-Addresses [redacted]@fokus.fraunhofer.de  
Organisational Unit FOKUS

### Certificate data

Distinguished Name CN=tkusber, OU=FOKUS, O=MeliCERTes-MCERES, C=EU, DC=melicertes,  
DC=eu  
Alternative Name(s) email:[redacted]@fokus.fraunhofer.de  
Public Key Fingerprint E1:4E:90:5C:94:CC:E0:6B:04:16:F8:D7:E6:E0:52:FF:7D:94:CA:46  
Publish Certificate No  
Certificate profile User

### Statement of Applicant

I hereby approve the processing and usage of my supplied data for the purpose of issuing the requested certificate.  
The supplied data may be sent to DFN-CERT Services GmbH for processing and usage for this sole purpose.

(Date) (Signature)

### To be completed by registration authority (RA)

- ☐ Entitlement of applicant checked
- ☐ E-Mail-Addresses assigned to applicant

Name of RA: \_\_\_\_\_

(Date, Signature)

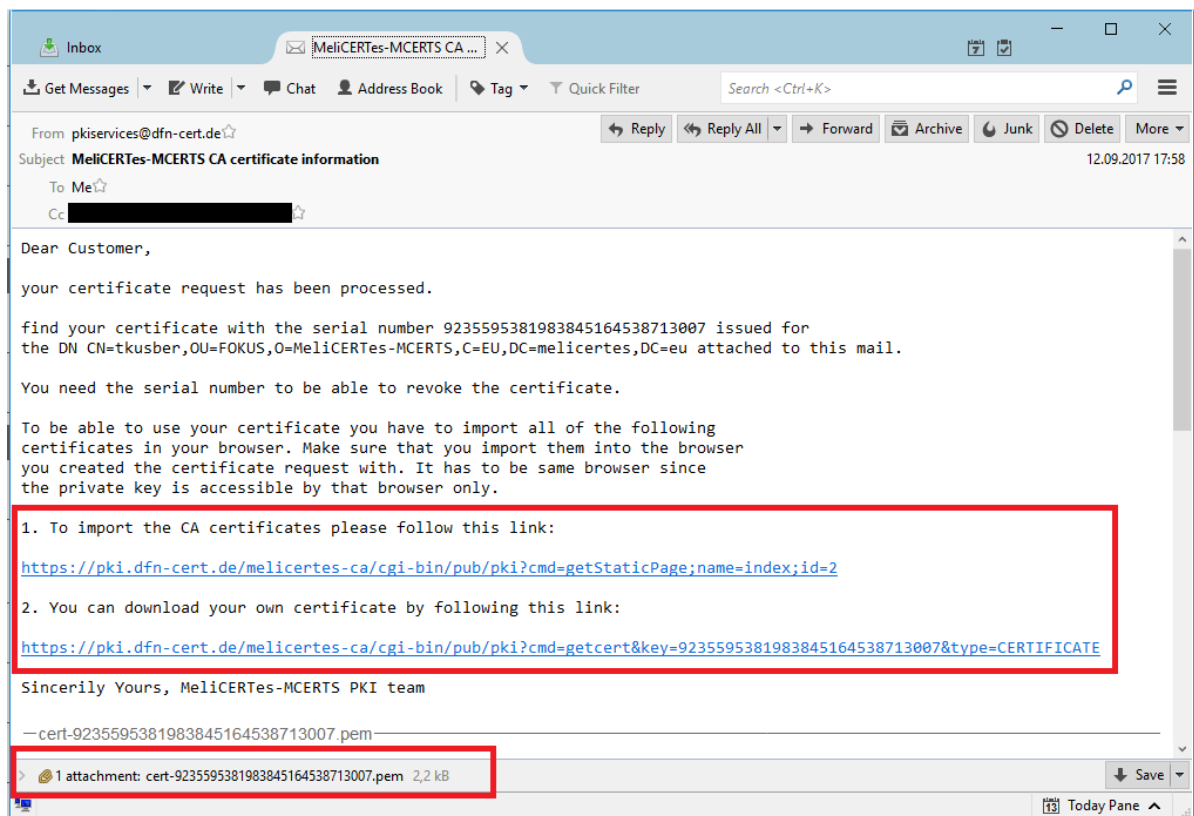
You have successfully requested a CSP user certificate.

### 1.3 Receiving the certificate

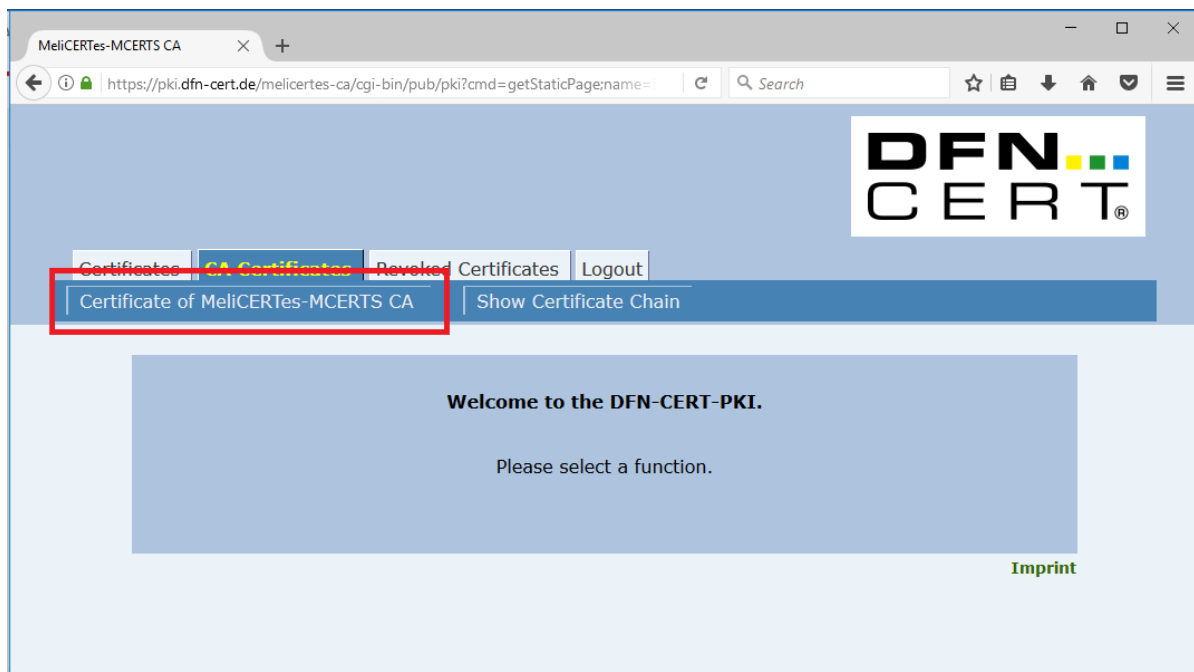
After the application has been approved by the RA, you will receive an email containing your certificate encoding as a pem file (see attachment). Furthermore, the email contains two links, one pointing to the corresponding certificate authority (ca) certificate and another pointing to your own certificate. 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.**

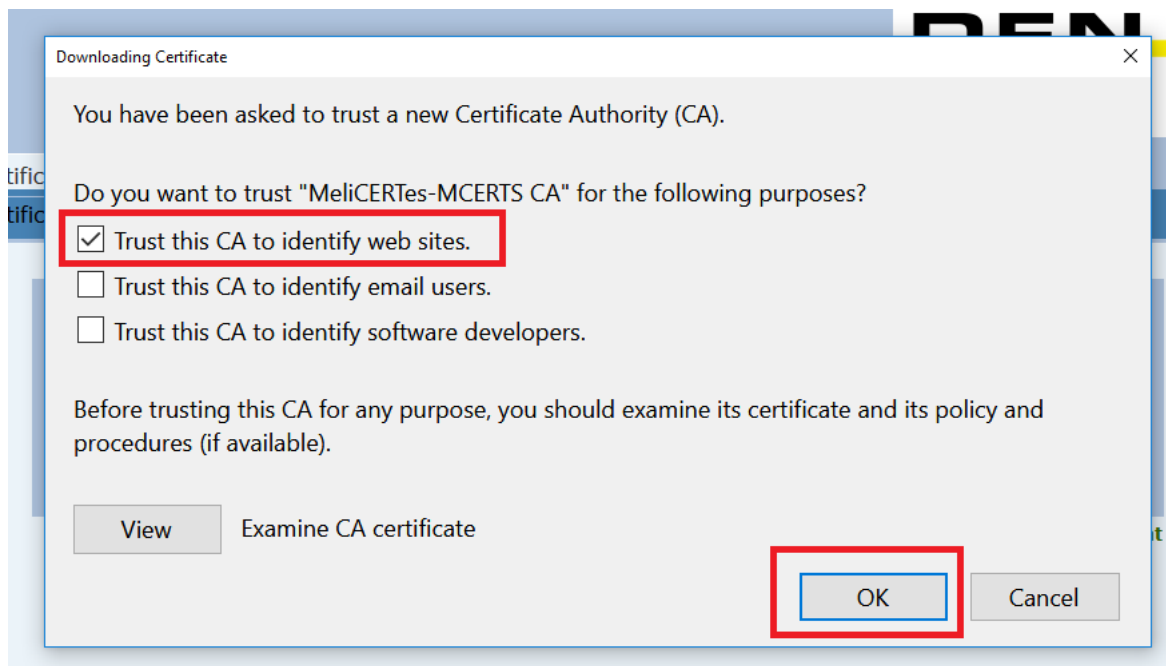




Please follow the first link placed in the email under “1. To import the CA certificates please follow this link”. The following screen is shown.



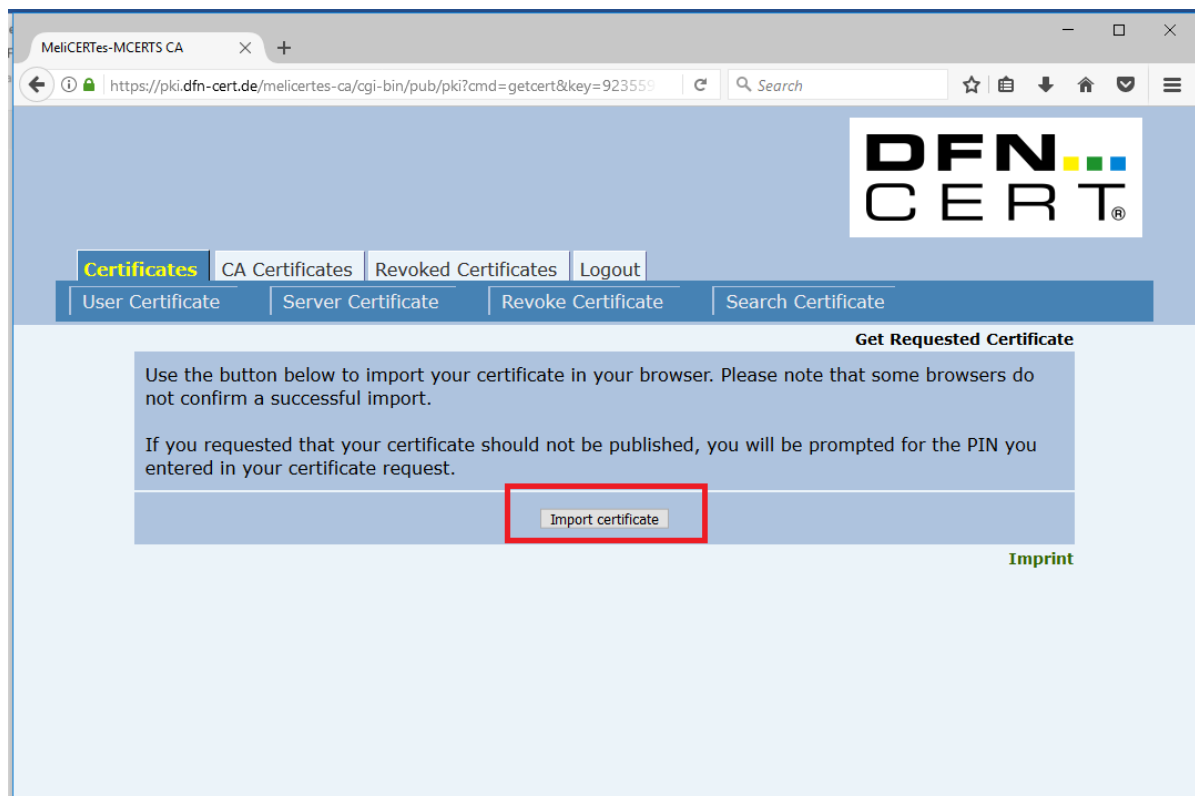
Click on the “Certificate of MeliCERTes-MCERTS CA” button in order to install ca certificate. The following screen will appear.



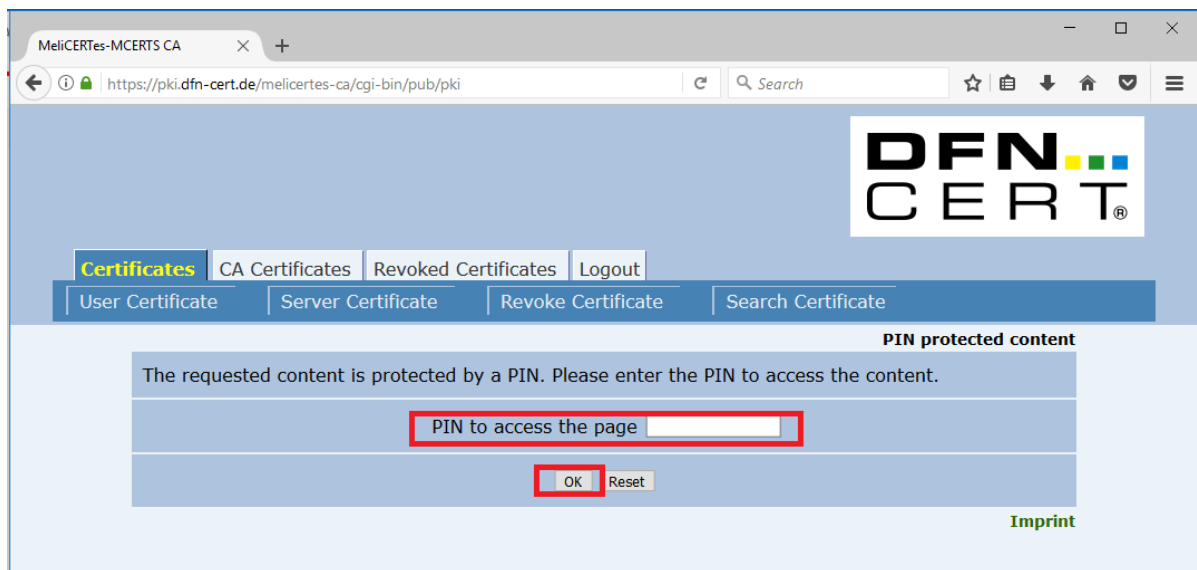
Select at least “Trust this CA to identify web sites” checkbox and confirm the import with OK button. The ca certificate has now been successfully installed in your browser.

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.

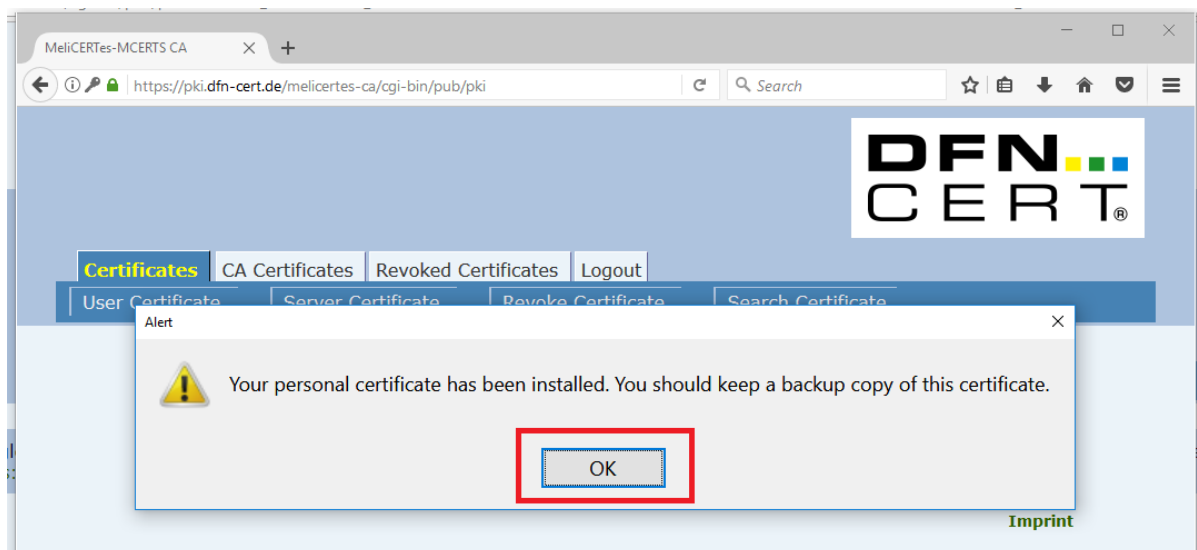


Click on the “Import certificate” button. The “PIN protected content” screen is shown.



The screenshot shows the DFN CERT website interface. The browser address bar displays 'https://pki.dfn-cert.de/melicertes-ca/cgi-bin/pub/pki'. The website has a navigation menu with 'Certificates' selected, and sub-menus for 'CA Certificates', 'Revoked Certificates', 'Logout', 'User Certificate', 'Server Certificate', 'Revoke Certificate', and 'Search Certificate'. A 'PIN protected content' dialog is displayed, stating: 'The requested content is protected by a PIN. Please enter the PIN to access the content.' Below this text is a text input field labeled 'PIN to access the page' and two buttons: 'OK' and 'Reset'. The 'OK' button is highlighted with a red rectangle. An 'Imprint' link is visible at the bottom right of the dialog area.

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.



The screenshot shows the same DFN CERT website interface, but with a confirmation dialog box overlaid. The dialog box has a yellow warning icon and the text: 'Your personal certificate has been installed. You should keep a backup copy of this certificate.' Below the text is an 'OK' button, which is highlighted with a red rectangle. The background website interface remains the same as in the previous screenshot.

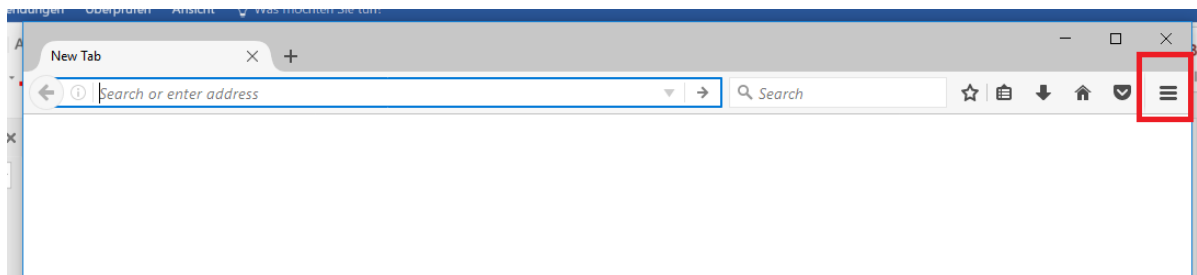
Click on the OK button, the user certificate has been successfully installed in your browser; you can use it to login into CSP.

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

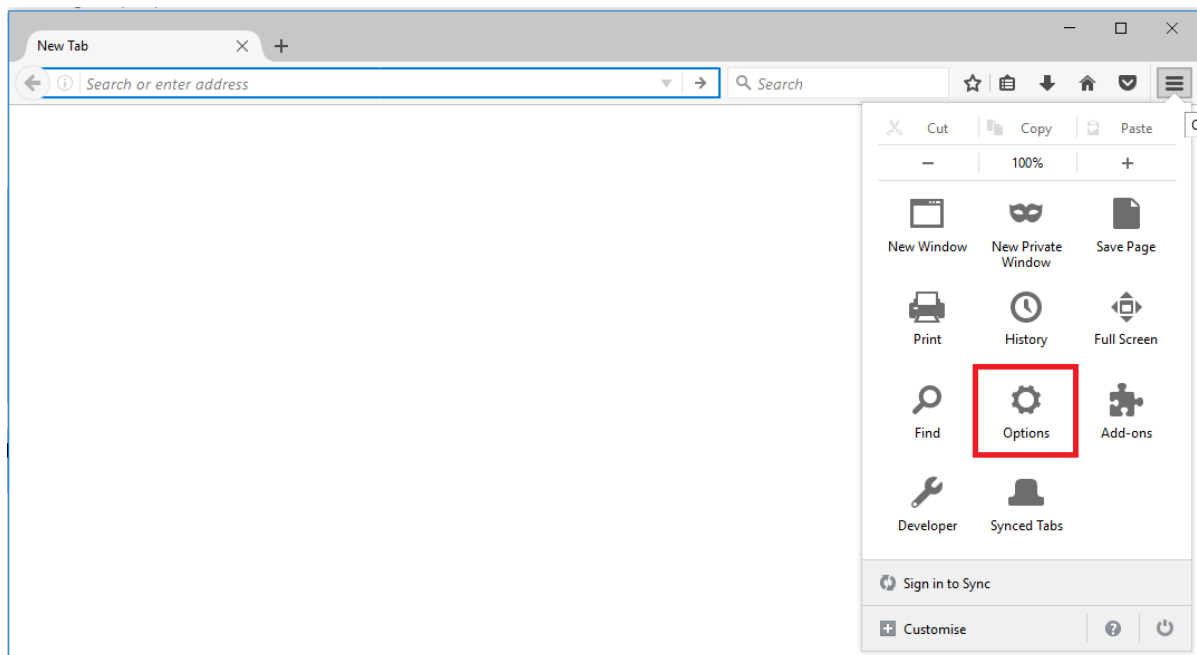
#### 1.4 How to backup of user certificate

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

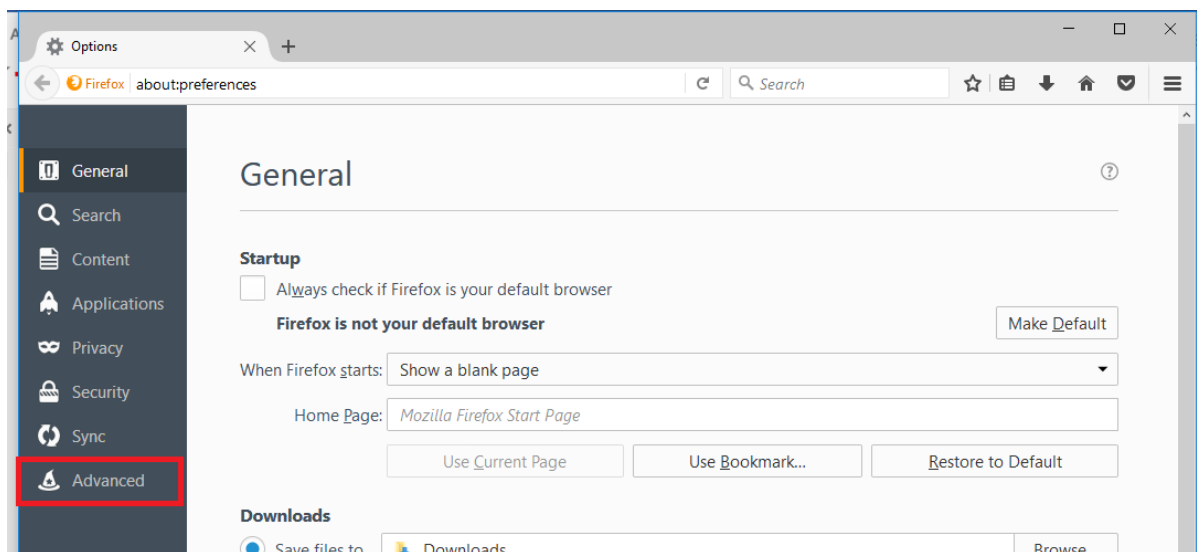
**NOTE!** For the demonstration of the particular steps, a Firefox browser will be used.



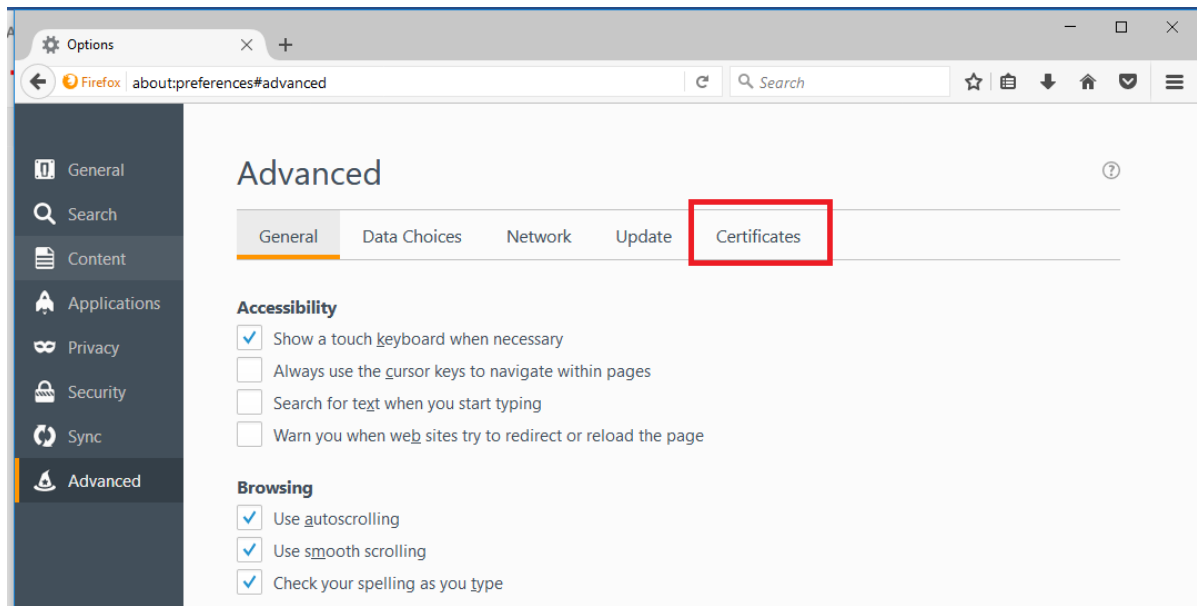
Please click on the “Open menu” button, in the upper right corner of the Firefox browser. The following screen will appear.



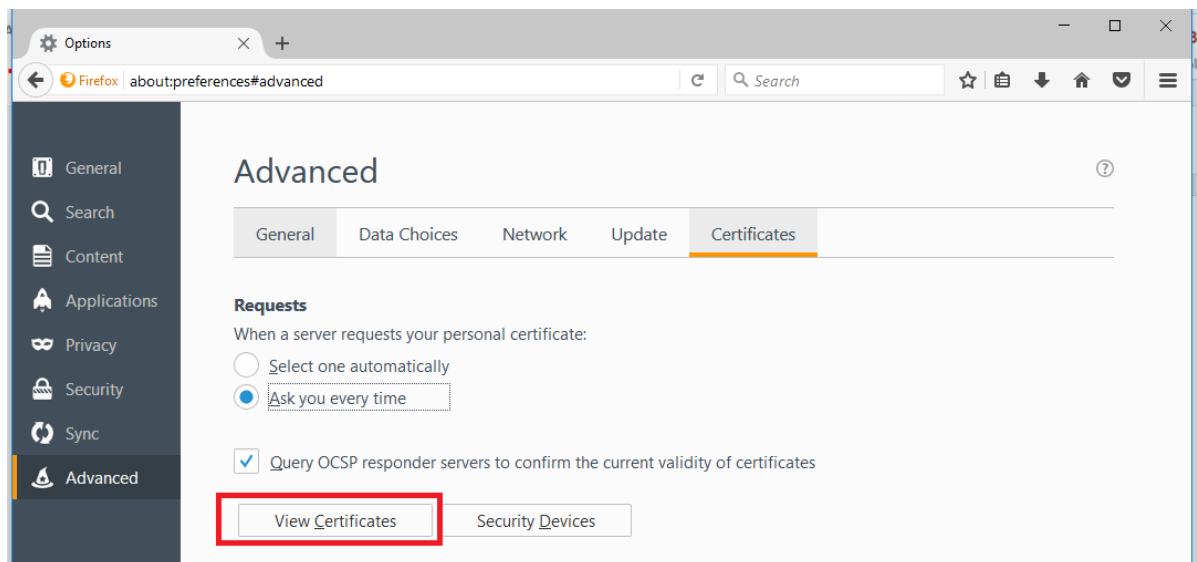
Click the Options button.



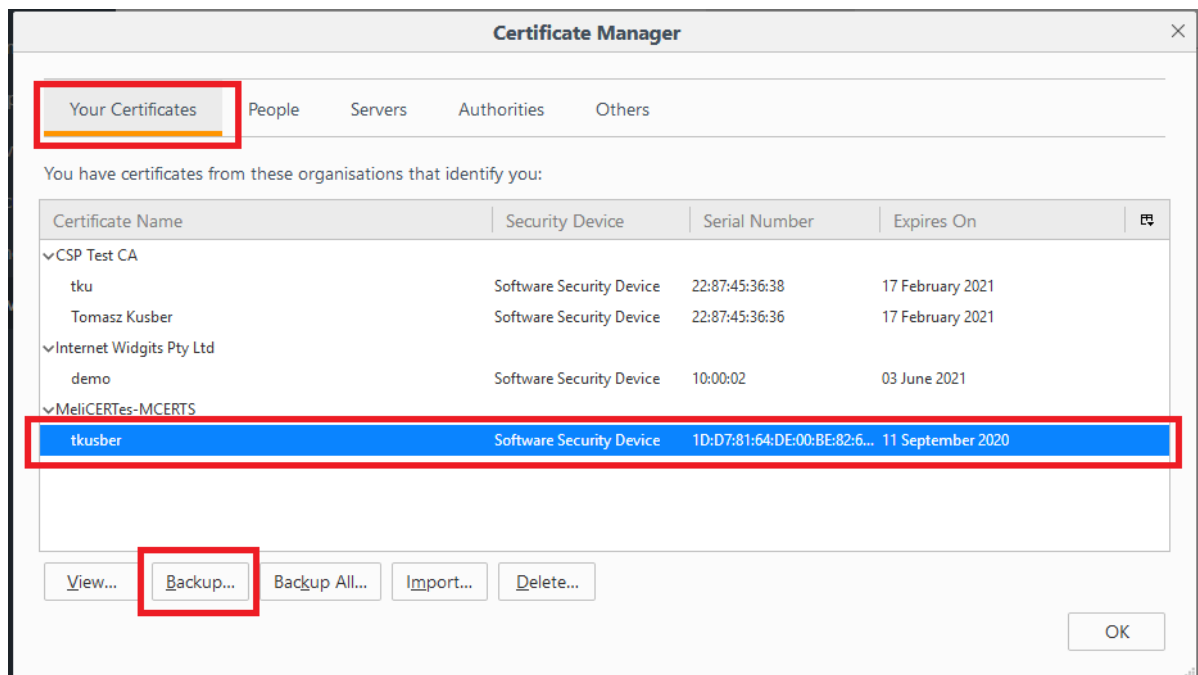
Click the Advanced tab.



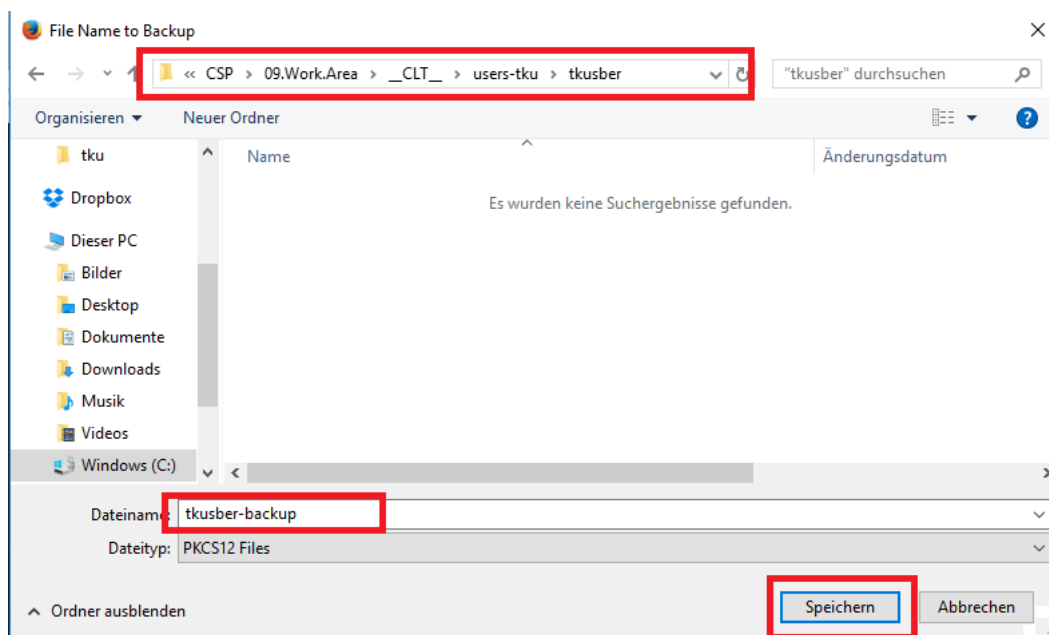
Chose the Certificates tab.



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.

Choose a Certificate Backup Password

The certificate backup password you set here protects the backup file that you are about to create. You must set this password to proceed with the backup.

Certificate backup password:

Certificate backup password (again):

Important: If you forget your certificate backup password, you will not be able to restore this backup later. Please record it in a safe location.

Password quality meter

OK Cancel

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 your password is will be displayed. The longer the green stripe, the more secure your password.

## 2 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

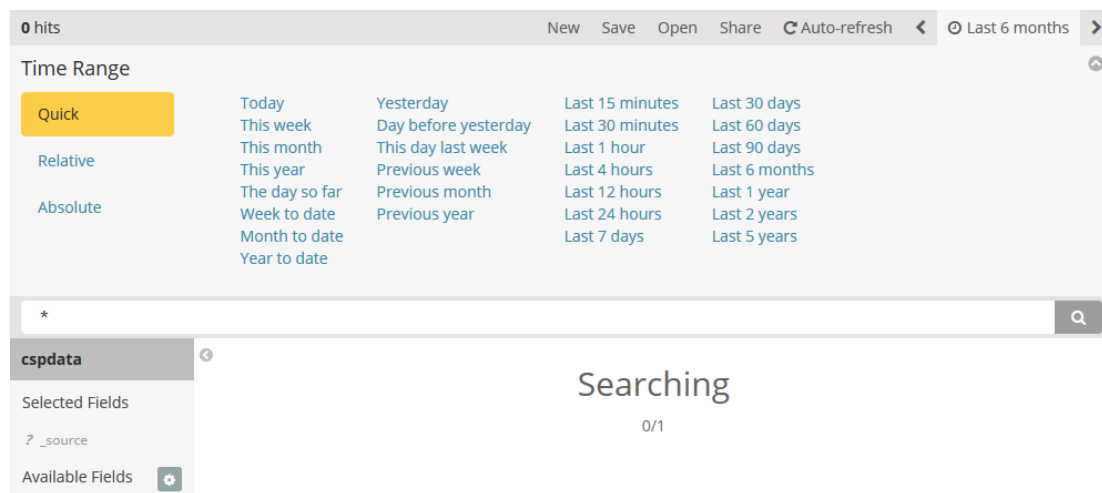
- [https://search.<cspId>.\[preprod.\]melicertes.eu](https://search.<cspId>.[preprod.]melicertes.eu)
- [https://logs.<cspId>.\[preprod.\]melicertes.eu](https://logs.<cspId>.[preprod.]melicertes.eu)

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.

### 2.1 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.

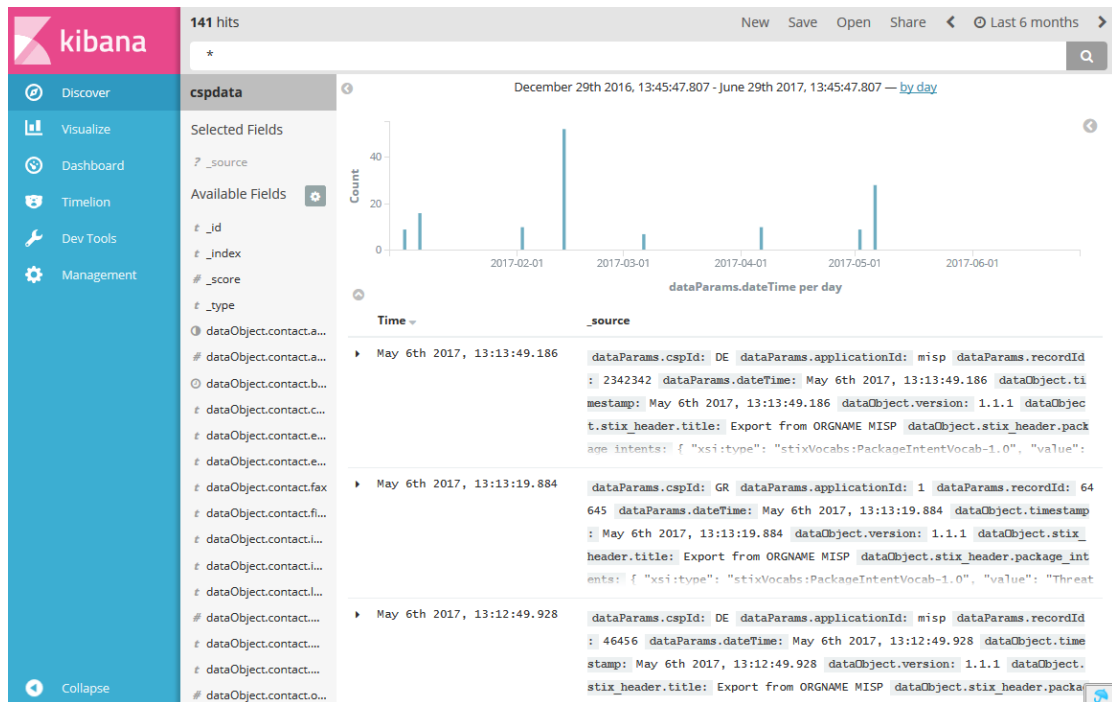


As soon as the desired timeframe is selected, the user is presented with multiple visual elements:

- 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.





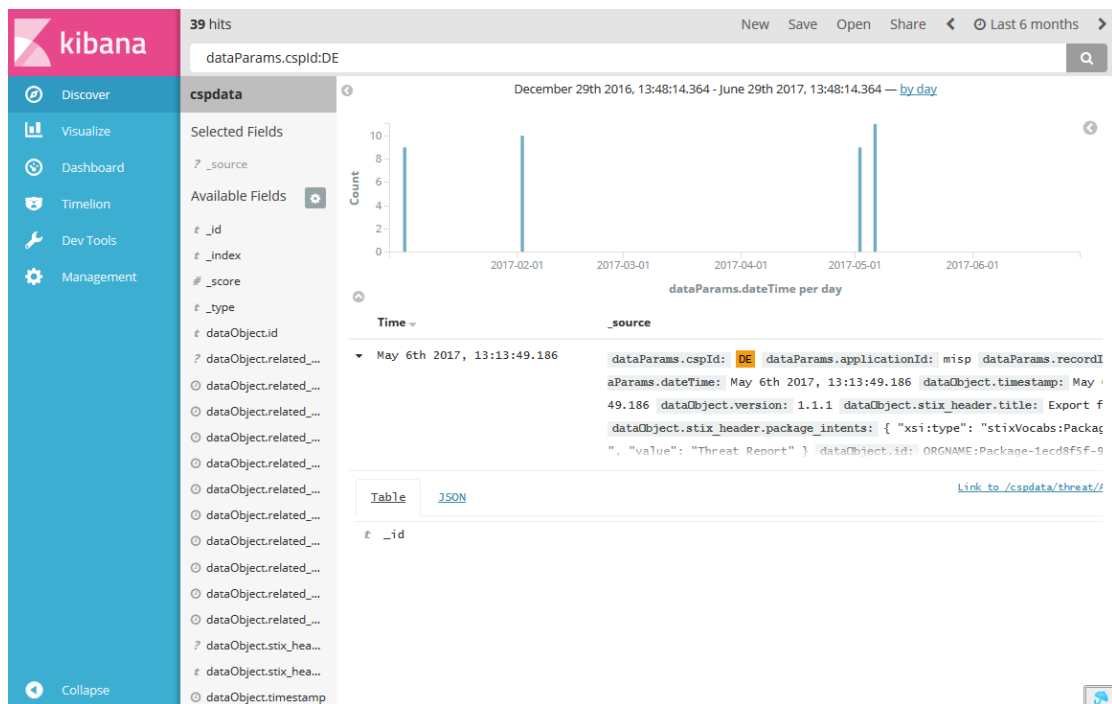
The query syntax is based on the Lucene query syntax. It allows Boolean operators, wildcards, and field filtering. Examples:

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 are graphically displayed in a bar graph at the time graph and as raw data in the raw data section.

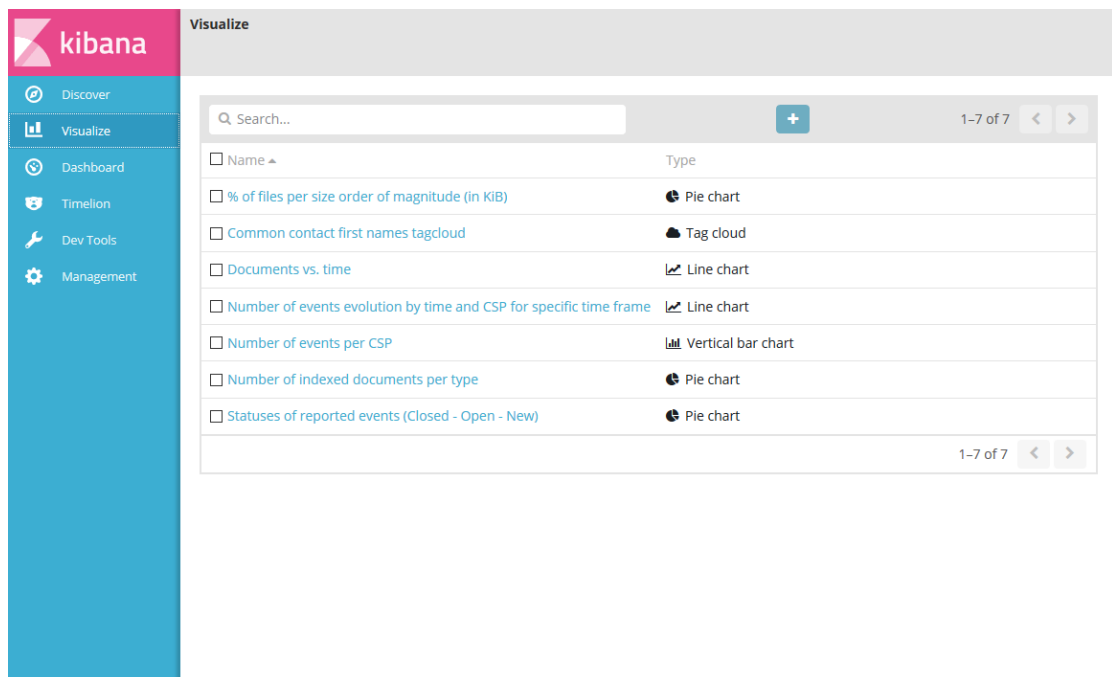
Each result is displayed in a two-column style with the first row being the creation date and the second being the raw data. By expanding the result (clicking on the arrow) the user is presented with the full raw output in tabular format as well as JSON. A typical search result appears in the following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



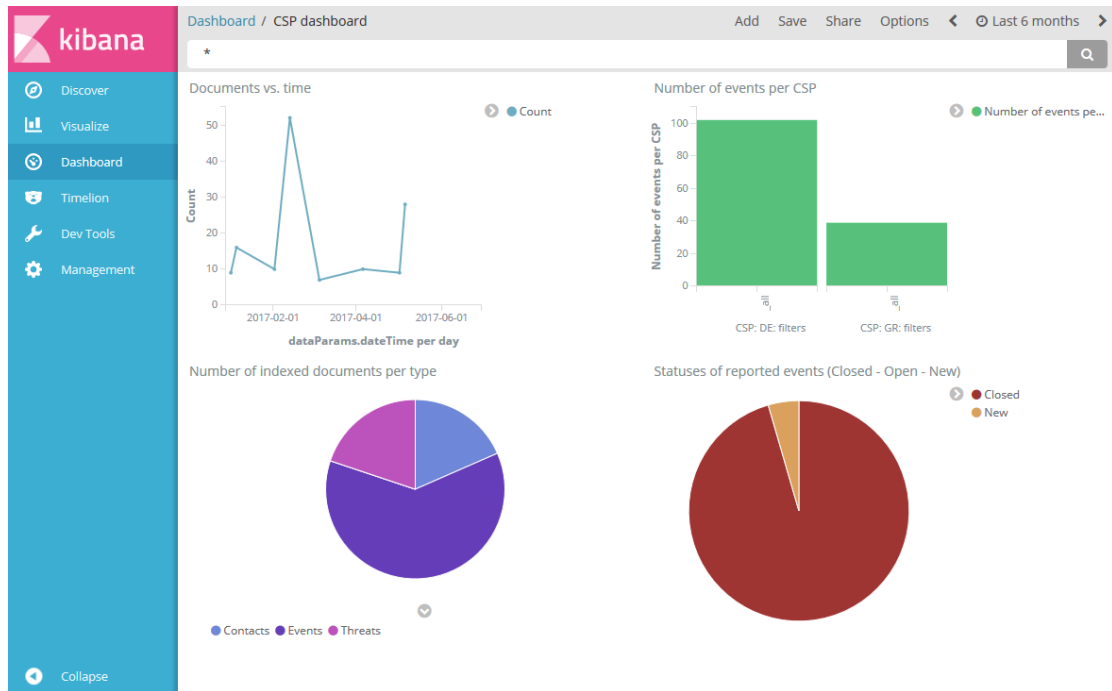
If the user tries to display too many raw results the web browser may become overloaded.

## 2.2 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.

### 3 How to manage contacts with CMM

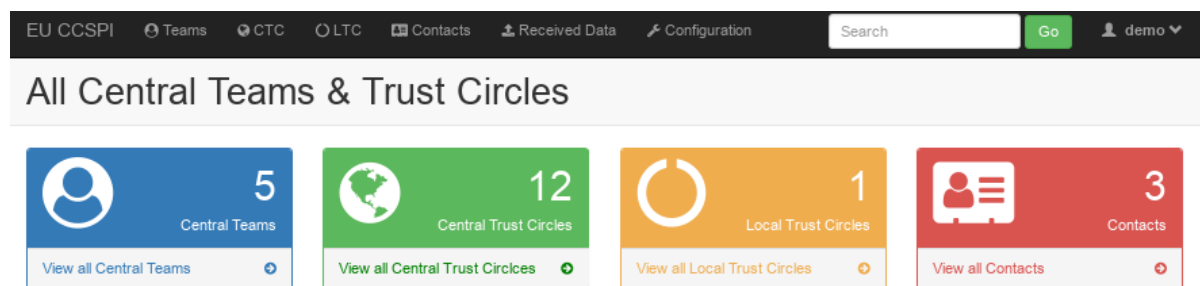
#### 3.1 Introduction

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](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.



#### Central Teams

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

Showing 1 to 5 of 5 rows

#### Central Trust Circles

	Short Name	Full Name	TLP	# of Teams	Created
	CTC::EU NIS:Basic	NIS Basic	-	3	April 25, 2017
	CTC::SHARING_DATA_ARTEFACT	CTC::SHARING_DATA_ARTEFACT	-	4	June 19, 2017
	CTC::SHARING_DATA_CHAT	CTC::SHARING_DATA_CHAT	-	4	June 19, 2017
	CTC::TI:Accredited	TI Accredited Teams	-	4	April 25, 2017
	CTC::SHARING_DATA_FILE	CTC::SHARING_DATA_FILE	-	4	June 19, 2017
	CTC::SHARING_DATA_THREAT	CTC::SHARING_DATA_THREAT	-	4	June 19, 2017

#### 3.2 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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Teams** **People** **+ Add Team**

	Name	Country	#CTC	Created	Status
	foo	USA/United States	0	Feb 12 2019	Active

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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Add New Person** Cancel Save

### Personal Details

Full Name:

Email:  This field is required.

Email Visibility:

Postal Address:

Postal Country:

### Mailing List

Mailinglist Email:

Mailinglist Email PGP Key:

Phone Numbers **+ Add another**

PGP Key X.509 Certificates **+ Add another**

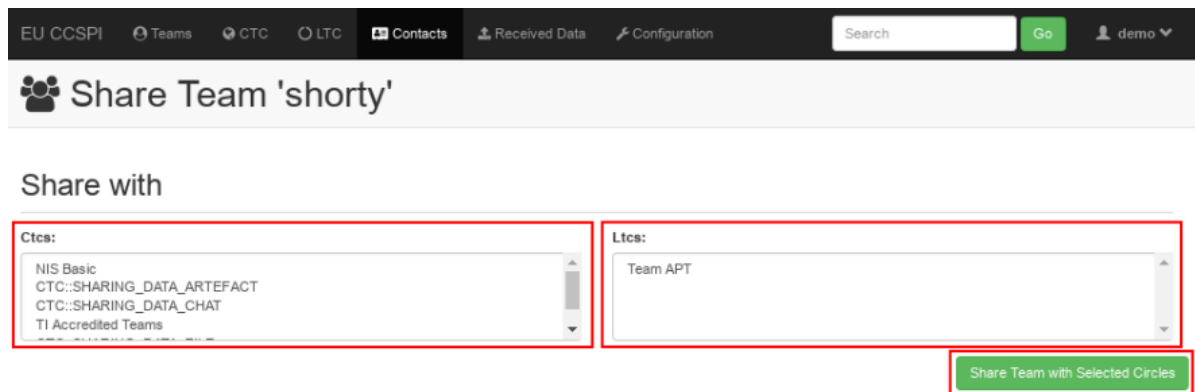
Memberships **+ Add another**

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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Team 'shorty'** **+ Add** **Remove** **Edit Team** **Share Team**

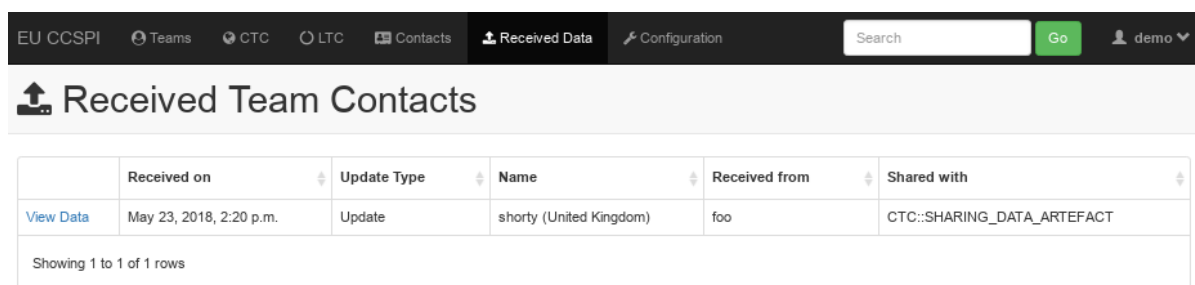
The following sharing screen then allows the selection of Trust Circles to share the entry with. This view is accessible through the details view of a team at any time. Please note, that sharing of individuals is only possible if they are part of a team.



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.

### 3.3 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.



	Received on	Update Type	Name	Received from	Shared with
<a href="#">View Data</a>	May 23, 2018, 2:20 p.m.	Update	shorty (United Kingdom)	foo	CTC::SHARING_DATA_ARTEFACT

Showing 1 to 1 of 1 rows

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.

EU CCSPi Teams CTC LTC Contacts Received Data Configuration Search Go demo

## Edit Team 'shorty' with incoming changes

Cancel Save

Update Details (Set to Incoming)

Received On May 23, 2018, 2:20 p.m.

Sent From foo

Shared With CTC CTC::SHARING\_DATA\_ARTEFACT

Shared With Team

### CSP / Melicertes Team

CSP ID: SUPERID

CSP Domain:

☐ CSP Installed:

NIS Team Types:

NIS Sectors:

Status: Active

Incoming data (Set to Incoming)

- ☒ CSP ID SUPERID
- ☒ CSP Domain
- ☒ CSP Installed False
- ☒ NIS Team Types
- ☒ NIS Sectors
- ☒ Status Active

### Team

Short Name: shorty

Official Name: official name

Host Organisation: host org

Description:

Country: United Kingdom

Additional Countries: ☒ Europe ☒ Haiti

Established on: 2018-02-05

Incoming data (Set to Incoming)

- ☒ Short Name shorty
- ☒ Official Name official name
- ☒ Host Organisation host org
- ☒ Description
- ☒ Country United Kingdom
- ☒ Additional Countries Europe
- ☒ Established On Feb. 5, 2018

### Constituency

Constituency types:

Member locations:

Incoming data (Set to Incoming)

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.

### 3.4 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.

### 3.5 Exporting local team data to FIRST

Reserved for future use.

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

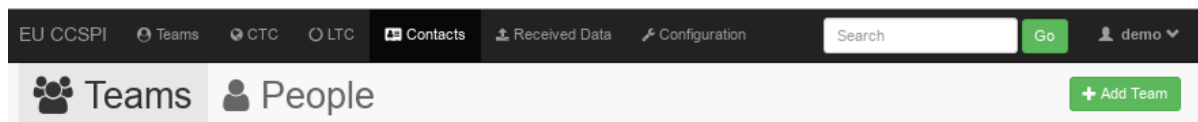
Reserved for future use.

### 3.7 Importing team data from TF-CSIRT/TI

Reserved for future use.

### 3.8 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.



EU CCSPI Teams CTC LTC Contacts Received Data Configuration   demo

### Search Result for 'doe'

0

Central Teams

View all Central Teams

0

Central Trust Circles

View all Central Trust Circles

0

Local Trust Circles

View all Local Trust Circles

1

Contacts

View all Contacts

#### Central Teams

Name	Country	#CTC	Created	CSP Installed	Status
No matching records found					

#### Central Trust Circles

Short Name	Full Name	TLP	# of Teams	Created
No matching records found				

#### Local Trust Circles

Short Name	Full Name	Created
No matching records found		

#### Local Team Contacts

Name	Country	Created	CSP Installed	Status
No matching records found				

#### Local Person Contacts

	Name	Email
	John Doe	jd@hotmail.com

Showing 1 to 1 of 1 rows

### 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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Team 'shorty'** + - Edit Team Share Team

## CSP / Melicertes Team

CSP ID SUPERID	NIS Team Types
CSP Domain	NIS Sectors
CSP Installed False	Status Active

## Team

Short Name shorty	Country United Kingdom
Official Name official name	Additional Countries *Europe, Haiti
Host Organisation host org	Established On Feb. 5, 2018
Description	

## Constituency

Constituency Types	Member Locations
--------------------	------------------

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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Person 'John Doe'** + - Edit Person

## Personal Details

Full Name John Doe	Postal Address
Email jd@hotmail.com	Postal Country
Email Visibility private	

## Mailing List

Mailinglist Email	Mailinglist Email PGP Key
-------------------	---------------------------

### 3.10 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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Team 'shorty'** + - Edit Team Share Team

**CSP / Melicertes Team**

Are you sure?  
Yes No

### 3.11 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.

EU CCSPI
Teams
CTC
LTC
Contacts
Received Data
Configuration
first
Go
demo

### Search Result for 'first'

0
Central Teams
View all Central Teams

1
Central Trust Circles
View all Central Trust Circles

0
Local Trust Circles
View all Local Trust Circles

0
Contacts
View all Contacts

#### Central Teams

Name	Country	#CTC	Created	CSP Installed	Status
No matching records found					

#### Central Trust Circles

Short Name	Full Name	TLP	# of Teams	Created
CTC::FIRST	FIRST Trust Circle	-	4	April 25, 2017

Showing 1 to 1 of 1 rows

#### Local Trust Circles

Short Name	Full Name	Created
No matching records found		

#### Local Team Contacts

Name	Country	Created	CSP Installed	Status
No matching records found				

#### Local Person Contacts

Name	Email
No matching records found	

### 3.12 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.

EU CCSPi Teams CTC **LTC** Contacts Received Data Configuration Search Go demo

**LTC::short** + Delete Edit LTC

#### Details

(Short) LTC Name LTC::short	(Long) LTC Name Team APT
Description APT-as-a-service	URL For Public Information
URL For Membership Directory	Created Feb. 5, 2018, 3:49 p.m.

#### Members

Trust Circles TI Accredited Teams, CTC::SHARING_DATA_CHAT	Teams world-gov-csirt, *World Wide
Team Contacts shorty, United Kingdom	Person Contacts jd@hotmail.com

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.

### 3.13 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.

EU CCSPi
Teams
CTC
LTC
Contacts
Received Data
Configuration
Search
Go
demo

Edit 'LTC::short'
Cancel
Save

### Local Trust Circle

(Short) LTC Name:

(Long) LTC Name:

Description:

URL for Public Information:

URL for Membership Directory:

### Members

Central Trust Circles:  
  
CTC::SHARING\_DATA\_INCIDENT  
CTC::SHARING\_DATA\_EVENT  
CTC::SHARING\_DATA\_ARTEFACT  
CTC::SHARING\_DATA\_CHAT

Teams:  
central-csp, \*European Union  
demo1-csp, Germany  
demo2-csp, Greece  
demo3-csp, Finland  
world-gov-csirt, \*World Wide

Team Contacts:  
foo, \*World Wide  
shorty, United Kingdom

Person Contacts:  
jd@hotmail.com  
devnull@foobar.local

### 3.14 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.

EU CCSPi
Teams
CTC
LTC
Contacts
Received Data
Configuration
Search
Go
demo

LTC::short
+
trash bin
Edit LTC

Details

Are you sure?  
Yes No

### 3.15 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.

## Add New LTC

Cancel

Save

### Local Trust Circle

(Short) LTC Name:

(Long) LTC Name:

Description:

URL for Public Information:

URL for Membership Directory:

### Members

Central Trust Circles:

CTC::SHARING\_DATA\_CONTACT  
FIRST Trust Circle  
CTC::SHARING\_DATA\_INCIDENT  
CTC::SHARING\_DATA\_EVENT  
CTC::SHARING\_DATA\_MESSAGE

Teams:

central-csp, "European Union  
demo1-csp, Germany  
demo2-csp, Greece  
demo3-csp, Finland

Team Contacts:

foo, "World Wide  
shorty, United Kingdom

Person Contacts:

jd@hotmail.com  
devnull@foobar.local

## 4 How to manage contacts with CMM

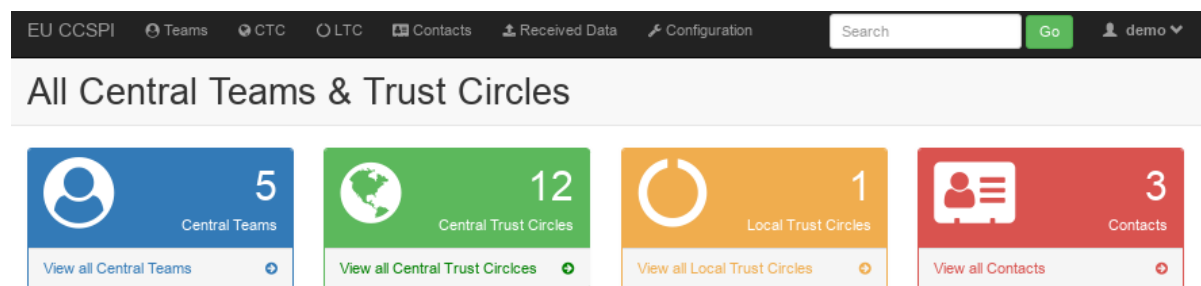
### 4.1 Introduction

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](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.



#### Central Teams

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

Showing 1 to 5 of 5 rows

#### Central Trust Circles

	Short Name	Full Name	TLP	# of Teams	Created
	CTC::EU NIS:Basic	NIS Basic	-	3	April 25, 2017
	CTC::SHARING_DATA_ARTEFACT	CTC::SHARING_DATA_ARTEFACT	-	4	June 19, 2017
	CTC::SHARING_DATA_CHAT	CTC::SHARING_DATA_CHAT	-	4	June 19, 2017
	CTC::TI:Accredited	TI Accredited Teams	-	4	April 25, 2017
	CTC::SHARING_DATA_FILE	CTC::SHARING_DATA_FILE	-	4	June 19, 2017
	CTC::SHARING_DATA_THREAT	CTC::SHARING_DATA_THREAT	-	4	June 19, 2017

### 4.2 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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Teams** **People** **+ Add Team**

	Name	Country	#CTC	Created	Status
	foo	Malaysia	0	Feb 12 2019	Active

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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Add New Person** Cancel Save

### Personal Details

Full Name:

Email:  This field is required.

Email Visibility:

Postal Address:

Postal Country:

### Mailing List

Mailinglist Email:

Mailinglist Email PGP Key:

Phone Numbers **+ Add another**

PGP Key X.509 Certificates **+ Add another**

Memberships **+ Add another**

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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Team 'shorty'** **+ Add** **Remove** **Edit Team** **Share Team**



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.

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

### Share Team 'shorty'

Share with

**CTCs:**

- NIS Basic
- CTC::SHARING\_DATA\_ARTEFACT
- CTC::SHARING\_DATA\_CHAT
- TI Accredited Teams

**LTcs:**

- Team APT

Share Team with Selected Circles

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.

### 4.3 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.

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

### Received Team Contacts

	Received on	Update Type	Name	Received from	Shared with
<a href="#">View Data</a>	May 23, 2018, 2:20 p.m.	Update	shorty (United Kingdom)	foo	CTC::SHARING_DATA_ARTEFACT

Showing 1 to 1 of 1 rows

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.

- As a whole – by clicking on “Set to Incoming” in the “Update Details” box.
- Blockwise, for individual information blocks – by clicking on “Set to Incoming” in the individual “Incoming data” blocks.
- Fieldwise, for individual data bits – by clicking on the left arrow (←) near the field to be applied.

8. 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.

The screenshot shows the S-CURE interface for editing a team. The top navigation bar includes links for EU CCSPi, Teams, CTC, LTC, Contacts, Received Data, and Configuration. The main header reads 'Edit Team 'shorty' with incoming changes' with 'Cancel' and 'Save' buttons. A 'Update Details (Set to Incoming)' box shows metadata: Received On May 23, 2018, 2:20 p.m., Sent From foo, Shared With CTC CTC::SHARING\_DATA\_ARTEFACT, and Shared With Team.

The 'CSP / Melicertes Team' section contains input fields for CSP ID (SUPERID), CSP Domain, CSP Installed (checkbox), NIS Team Types, NIS Sectors, and Status (Active). An 'Incoming data (Set to Incoming)' box lists fields with blue arrows indicating incoming changes: CSP ID SUPERID, CSP Domain, CSP Installed False, NIS Team Types, NIS Sectors, and Status Active.

The 'Team' section contains input fields for Short Name (shorty), Official Name (official name), Host Organisation (host org), Description, Country (United Kingdom), Additional Countries (Europe, Haiti), and Established on (2018-02-05). An 'Incoming data (Set to Incoming)' box lists fields with blue arrows: Short Name shorty, Official Name official name, Host Organisation host org, Description, Country United Kingdom, Additional Countries Europe, and Established On Feb. 5, 2018.

The 'Constituency' section contains input fields for Constituency types and Member locations, with an 'Incoming data (Set to Incoming)' box.

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.

#### 4.4 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.

#### 4.5 Exporting local team data to FIRST

Reserved for future use.

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

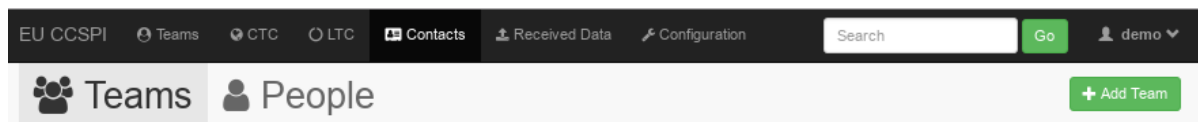
Reserved for future use.

#### 4.7 Importing team data from TF-CSIRT/TI

Reserved for future use.

#### 4.8 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.

EU CCSPI Teams CTC LTC Contacts Received Data Configuration   demo

### Search Result for 'doe'

0

Central Teams

View all Central Teams

0

Central Trust Circles

View all Central Trust Circles

0

Local Trust Circles

View all Local Trust Circles

1

Contacts

View all Contacts

#### Central Teams

Name	Country	#CTC	Created	CSP Installed	Status
No matching records found					

#### Central Trust Circles

Short Name	Full Name	TLP	# of Teams	Created
No matching records found				

#### Local Trust Circles

Short Name	Full Name	Created
No matching records found		

#### Local Team Contacts

Name	Country	Created	CSP Installed	Status
No matching records found				

#### Local Person Contacts

	Name	Email
	John Doe	jd@hotmail.com

Showing 1 to 1 of 1 rows

#### 4.9 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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Team 'shorty'** + - Edit Team Share Team

## CSP / Melicertes Team

CSP ID SUPERID	NIS Team Types
CSP Domain	NIS Sectors
CSP Installed False	Status Active

## Team

Short Name shorty	Country United Kingdom
Official Name official name	Additional Countries *Europe, Haiti
Host Organisation host org	Established On Feb. 5, 2018
Description	

## Constituency

Constituency Types	Member Locations
--------------------	------------------

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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Person 'John Doe'** + - Edit Person

## Personal Details

Full Name John Doe	Postal Address
Email jd@hotmail.com	Postal Country
Email Visibility private	

## Mailing List

Mailinglist Email	Mailinglist Email PGP Key
-------------------	---------------------------

### 4.10 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.

EU CCSPi Teams CTC LTC **Contacts** Received Data Configuration Search Go demo

**Team 'shorty'** + - Edit Team Share Team

**CSP / Melicertes Team**

Are you sure?  
Yes No

#### 4.11 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.

EU CCSPI
Teams
CTC
LTC
Contacts
Received Data
Configuration
first
Go
demo

### Search Result for 'first'

0
Central Teams
View all Central Teams

1
Central Trust Circles
View all Central Trust Circles

0
Local Trust Circles
View all Local Trust Circles

0
Contacts
View all Contacts

#### Central Teams

Name	Country	#CTC	Created	CSP Installed	Status
No matching records found					

#### Central Trust Circles

Short Name	Full Name	TLP	# of Teams	Created
CTC::FIRST	FIRST Trust Circle	-	4	April 25, 2017

Showing 1 to 1 of 1 rows

#### Local Trust Circles

Short Name	Full Name	Created
No matching records found		

#### Local Team Contacts

Name	Country	Created	CSP Installed	Status
No matching records found				

#### Local Person Contacts

Name	Email
No matching records found	

#### 4.12 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.

EU CCSPi Teams CTC **LTC** Contacts Received Data Configuration Search Go demo

**LTC::short** + Edit LTC Go

### Details

(Short) LTC Name LTC::short	(Long) LTC Name Team APT
Description APT-as-a-service	URL For Public Information
URL For Membership Directory	Created Feb. 5, 2018, 3:49 p.m.

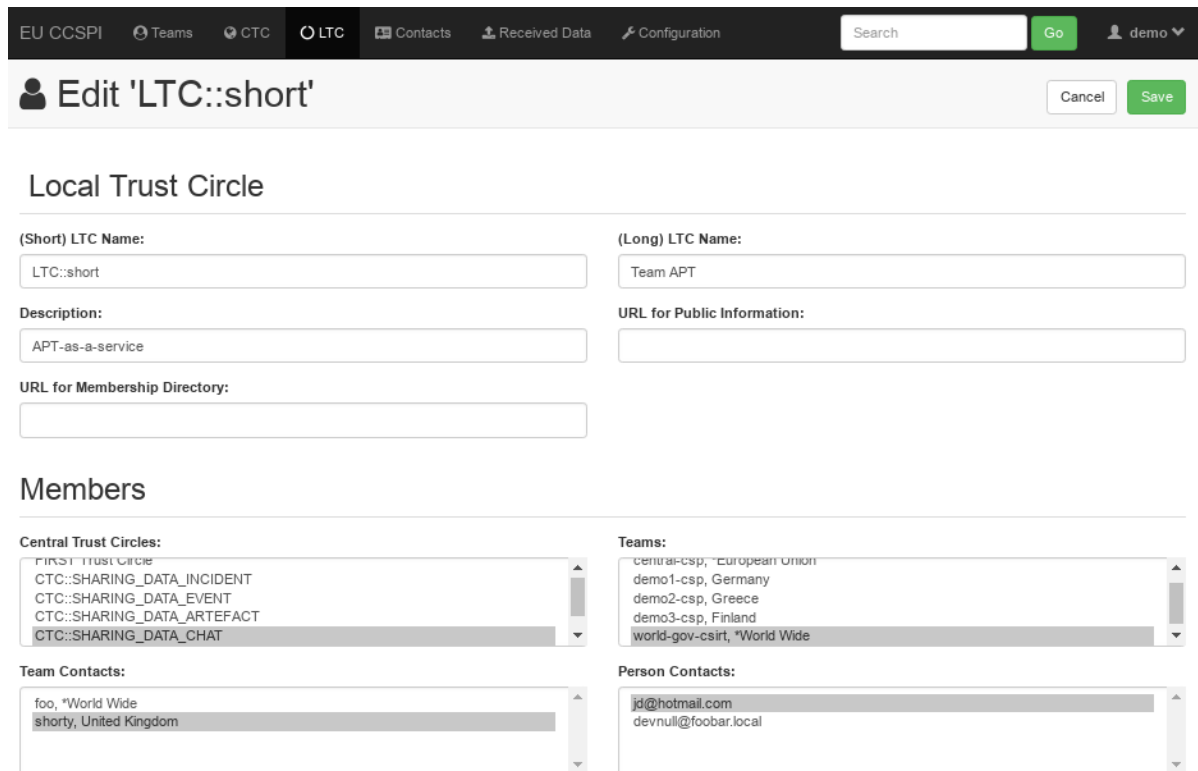
### Members

Trust Circles TI Accredited Teams, CTC::SHARING_DATA_CHAT	Teams world-gov-csirt, *World Wide
Team Contacts shorty, United Kingdom	Person Contacts jd@hotmail.com

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.

#### 4.13 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.



EU CCSPI Teams CTC **LTC** Contacts Received Data Configuration Search Go demo

## Edit 'LTC::short'

Cancel Save

### Local Trust Circle

(Short) LTC Name: LTC::short

(Long) LTC Name: Team APT

Description: APT-as-a-service

URL for Public Information:

URL for Membership Directory:

### Members

Central Trust Circles:

- CTC::SHARING\_DATA\_INCIDENT
- CTC::SHARING\_DATA\_EVENT
- CTC::SHARING\_DATA\_ARTEFACT
- CTC::SHARING\_DATA\_CHAT

Teams:

- central-csp, \*European Union
- demo1-csp, Germany
- demo2-csp, Greece
- demo3-csp, Finland
- world-gov-csirt, \*World Wide

Team Contacts:

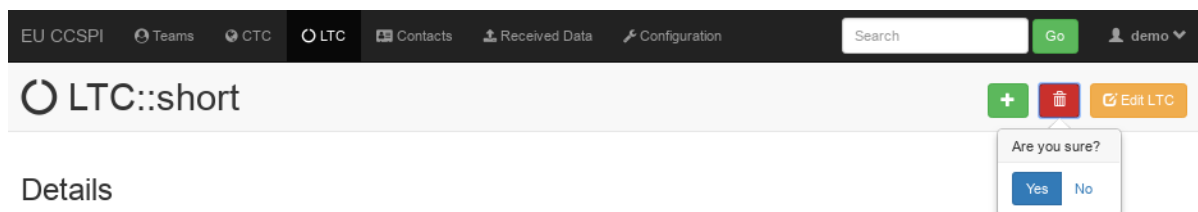
- foo, \*World Wide
- shorty, United Kingdom

Person Contacts:

- jd@hotmail.com
- devnull@foobar.local

#### 4.14 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.



EU CCSPI Teams CTC **LTC** Contacts Received Data Configuration Search Go demo

## LTC::short

+ trash Edit LTC

Are you sure?

Yes No

### Details

#### 4.15 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.



## Add New LTC

Cancel

Save

### Local Trust Circle

(Short) LTC Name:

(Long) LTC Name:

Description:

URL for Public Information:

URL for Membership Directory:

### Members

Central Trust Circles:

CTC::SHARING\_DATA\_CONTACT  
FIRST Trust Circle  
CTC::SHARING\_DATA\_INCIDENT  
CTC::SHARING\_DATA\_EVENT  
CTC::SHARING\_DATA\_MESSAGE

Teams:

central-csp, "European Union  
demo1-csp, Germany  
demo2-csp, Greece  
demo3-csp, Finland

Team Contacts:

foo, "World Wide  
shorty, United Kingdom

Person Contacts:

jd@hotmail.com  
devnull@foobar.local

## 5 How to manage incidents with RT

### 5.1 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<sup>2</sup>.

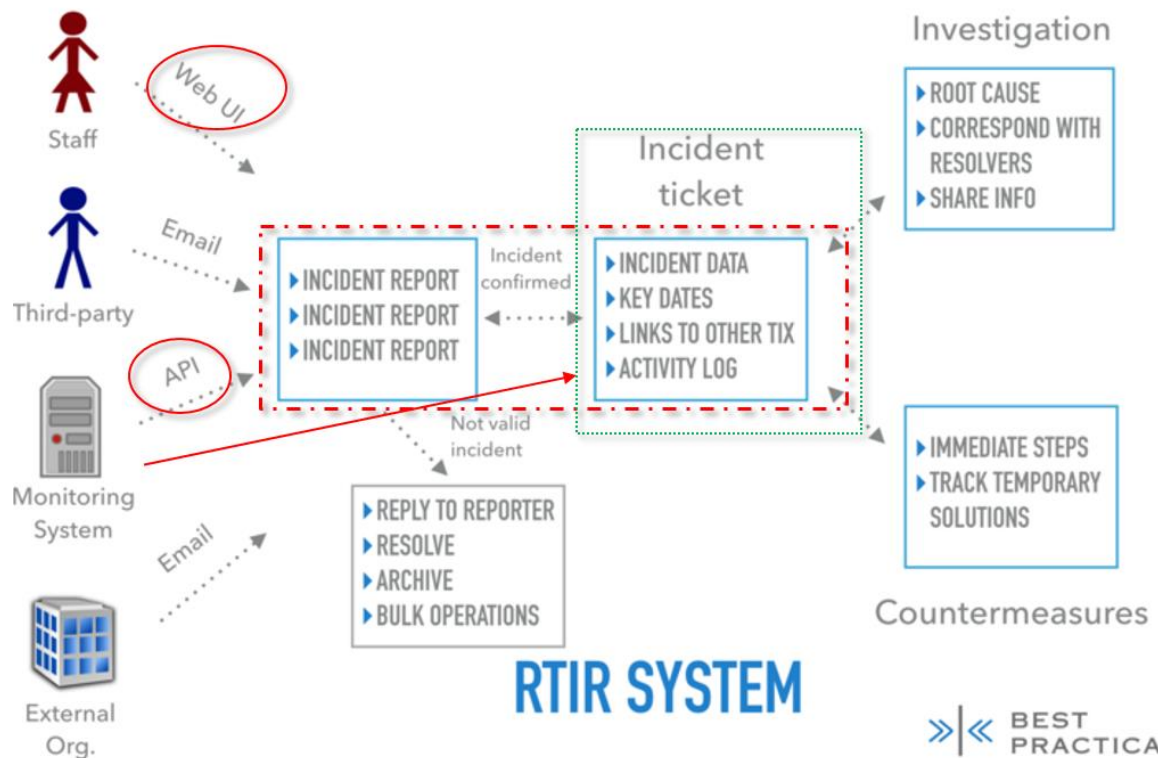
Figure below (source: Best Practical) depicts the default workflow of incident management, which is implemented using RT. The common functionality of the RT remains the same and has not been changed by implementing the CSP-extension. Some CSP-specific adjustments are marked using the red colour and they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

---

<sup>2</sup> For the future use in this chapter: if the terminus RT is used, than it means always RT plus RT::IR.

## INCIDENT MANAGEMENT WITH RTIR



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](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](https://rt.<cspId>.[preprod.]melicertes.eu/RTIR) – access to the RT::IR extension, e.g. <https://rt.demo2-csp.athens.intrasoft-intl.private/RTIR>

## 5.2 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.

RT
RTIR
Incidents
Reports
Investigations
Countermeasures
Tools
Logged in as rt-admin

Incident Report #821: [demo2-csp:misp] test event 2 on demo2

Display

Ticket metadata

The Basics

Status: new  
SLA:  
Incident: (none)  
  
Time Worked: 0 min  
  
Link New

Networking

IP: (no value)

Details

How Reported: rt-adapter  
Reporter Type: rt-adapter  
Customer: (no value)

Custom Fields

Additional data: (no value)  
Linked events: https://misp-ui.demo2-csp.athens.intrasoft-intl.private:443/events/5a8ae542-1ac4-496b-a69d-07b3ac120012  
Linked threads: (no value)  
Linked vulnerabilities: (no value)  
RT UUID: DE9ACB6E-1584-11E8-B448-82AE62626D3E

People

Owner: rt-admin  
Correspondents:  
Cc:  
AdminCc:

Dates

Created: Mon Feb 19 09:55:04 2018  
Starts: Not set  
Started: Not set  
Due: Not set [Set to 7 days from now]  
Updated: Mon Feb 19 09:55:04 2018 by rt-admin

History

Mon Feb 19 09:55:04 2018 rt-admin - Ticket created

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

## 5.3 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.

### 5.3.1 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.

RT ▾ RTIR ▾ Incidents ▾ Reports ▾ Investigations ▾ Countermeasures ▾ Tools ▾ Logged in as rt-admin ▾

## Incident Report #821: [demo2-csp:misp] test event 2 on demo2

### ^ Ticket metadata

#### ^ The Basics

Status: new  
SLA:  
Incident: (none)

Time Worked: 0 min

Link

New

#### ^ Networking

IP: (no value)

#### ^ Details

How Reported: rt-adapter  
Reporter Type: rt-adapter  
Customer: (no value)

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

RI ▾ RTIR ▾ Incidents ▾ Reports ▾ Investigations ▾ Countermeasures ▾ Tools ▾ Logged in as rt-admin ▾

## Create a new Incident

### ^ Create a new Incident

Subject: [demo2-csp:misp] test event 2 on demo2

Message:

Attach:

Drop files here or click to attach

#### ^ Details

Priority:   
Final Priority:   
Time Worked:  Minutes ▾  
Time Left:  Minutes ▾  
Starts:   
Due:

#### ^ Basics

Link with: Report #821: [demo2-csp:misp] test event 2 on demo2  
Queue: Incidents  
Status: open ▾  
Owner: rt-admin

#### ^ Networking

IP:  
Enter multiple IP address ranges

#### ^ Details

Description:   
Enter one value  
Resolution: (no value)  
Function: (no value) ▾  
Classification: (no value) ▾

#### ^ Custom Fields

Additional data:  
Enter multiple values

Linked events: https://misp-ui.demo2-csp.misp-project.org/

Create

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.

RT RTIR Incidents Reports Investigations Countermeasures Tools Logged in as rt-admin

**Incident #836: [demo2-csp:misp] test event 2 on demo2**

Ticket 836 created in queue 'Incidents'

**Ticket metadata**

**Incident #836**

Queue: Incidents  
Status: open  
Owner: rt-admin  
Subject: [demo2-csp:misp] test event 2 on demo2  
Priority: 0/  
Time Worked: 0 min

**Networking**

IP: (no value)

**Details**

Description: (no value)  
Resolution: (no value)  
Function: (no value)  
Classification: (no value)

**Custom Fields**

Additional data: (no value)  
Linked events: <https://misp-ui.demo2-csp.athens.intrasoft-intl.private:443/events/5a8ae542-1ac4-496b-a69d-07b3ac120012>  
Linked threats: (no value)  
Linked vulnerabilities: [RT\\_UUID: 24C5ABF0-16E2-11E8-9028-F59CEC027625](#)  
Sharing policy: no sharing  
Originator CSP: demo2-csp  
Last update done by: demo2-csp

**Dates**

**Incident Reports**

821 [demo2-csp:misp] test event 2 on demo2

(No inactive Incident Reports)

**Investigations**

(No active Investigations)  
(No inactive Investigations)

**Countermeasures**

(No active Countermeasures)  
(No inactive Countermeasures)

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).

### 5.3.2 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.

RT ▾ RTIR ▾ Incidents ▾ Reports ▾ Investigations ▾ Countermeasures ▾ Tools ▾ Logged in as rt-admin ▾

### Incident #881: Incident 0001 on demo1

---

^ Ticket metadata

^ Incident #881

Queue: Incidents  
Status: open  
Owner: rt-admin  
**Subject: Incident 0001 on demo1**  
Priority: 0/  
Time Worked: 0 min

^ Incident Reports

(No active Incident Reports)  
(No inactive Incident Reports)

---

^ Networking

IP: (no value)

^ Investigations

(No active Investigations)  
(No inactive Investigations)

---

^ Details

Description: (no value)  
Resolution: (no value)  
Function: (no value)  
Classification: (no value)

^ Countermeasures

(No active Countermeasures)  
(No inactive Countermeasures)

---

^ Custom Fields

Additional data: (no value)  
Linked events: (no value)  
Linked threats: (no value)  
Linked vulnerabilities:  
**RT\_UUID: 5B2BB990-16E3-11E8-850A-E7ED7B008402**  
Sharing policy: default sharing  
Originator CSP: demo1-csp  
Last update done by: demo1-csp

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).

^ Ticket metadata

^ Incident #881

Queue: Incidents  
Status: open  
Owner: rt-admin  
Subject: Incident 0001 on demo1  
Priority: 0/  
Time Worked: 0 min

^ Incident Reports

(No active Incident Reports)  
(No inactive Incident Reports)

^ Investigations

(No active Investigations)  
(No inactive Investigations)

^ Countermeasures

(No active Countermeasures)  
(No inactive Countermeasures)

^ Networking

IP: (no value)

^ Details

Description: (no value)  
Resolution: (no value)  
Function: (no value)  
Classification: (no value)

^ Custom Fields

Additional data: (no value)  
Linked events: (no value)  
Linked threats: (no value)  
Linked vulnerabilities: (no value)  
RT\_UUID: 5B2BB990-16E3-11E8-850A-E7ED7B008402  
Sharing policy: no sharing  
Originator CSP: demo1-csp  
Last update done by: demo1-csp

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	xxx3
RT_UUID	5B2BB990-16E3-11E8-850A-E7ED7B008402	RT_UUID	5B2BB990-16E3-11E8-850A-E7ED7B008402
Sharing policy	default sharing	Sharing policy	no sharing <sup>4</sup>
Originator CSP	demo1-csp	Originator CSP	demo1-csp
Last update done by	demo1-csp	Last update done by	demo1-csp

<sup>3</sup> Every RT instance manages the ticket numbers locally, which are unique only inside of this instance of RT.

<sup>4</sup> While creating a new incident, „no sharing“ has been set as a sharing policy. The operator can change the policy any time.



## 5.4 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”).

RT ▾ RTIR ▾ Incidents ▾ Reports ▾ Investigations ▾ Countermeasures ▾ Tools ▾ Logged in as rt-admin ▾

**Incident #881: Incident 0001 on demo1**

---

^ Ticket metadata

^ Incident #881

Queue: Incidents  
Status: open  
Owner: rt-admin  
Subject: Incident 0001 on demo1  
Priority: 0/  
Time Worked: 0 min

(No act)  
(No ina)

---

^ Networking

IP: (no value)

(No act)  
(No ina)

---

^ Details

Description: (no value)  
Resolution: (no value)  
Function: (no value)  
Classification: (no value)

---

^ Custom Fields

Additional data: (no value)  
Linked events: (no value)  
Linked threats: (no value)  
Linked vulnerabilities: (no value)  
RT\_UUID: 5B2BB990-16E3-11E8-850A-E7ED7B008402  
**Sharing policy: no sharing**  
Originator CSP: demo1-csp  
Last update done by: demo1-csp

Click on the link “Edit”.

csp-rt

New ticket in Incident Re ▾ Search Incidents...

Display Next > ▾ **Edit** Split Merge Advanced Actions ▾ ☆ ⌚

---

^ Incident Reports

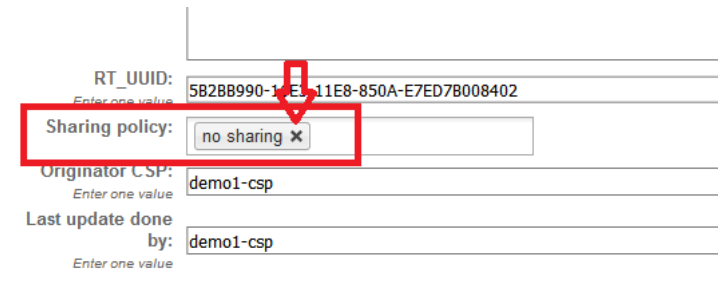
Create Link  
(No active Incident Reports)  
(No inactive Incident Reports)

---

^ Investigations

Launch Link  
(No active Investigations)  
(No inactive Investigations)

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



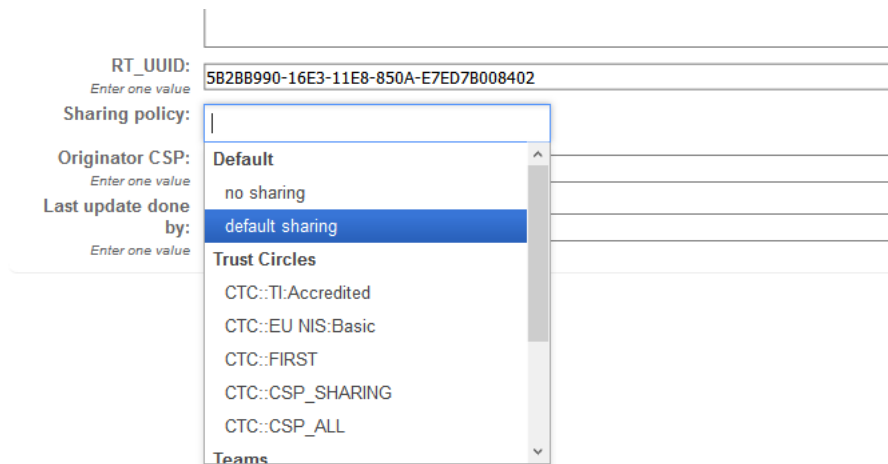
RT\_UUID: 5B2B8990-16E3-11E8-850A-E7ED7B008402

Sharing policy: no sharing X

Originator CSP: demo1-csp

Last update done by: demo1-csp

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.



RT\_UUID: 5B2B8990-16E3-11E8-850A-E7ED7B008402

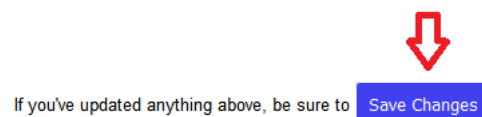
Sharing policy: [dropdown menu open]

Originator CSP: demo1-csp

Last update done by: demo1-csp

Dropdown menu options: Default, no sharing, default sharing, Trust Circles (CTC::TI:Accredited, CTC::EU NIS:Basic, CTC::FIRST, CTC::CSP\_SHARING, CTC::CSP\_ALL), Teams

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



If you've updated anything above, be sure to [Save Changes](#)

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.

## 6 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.

## 7 How to manage events with MISP

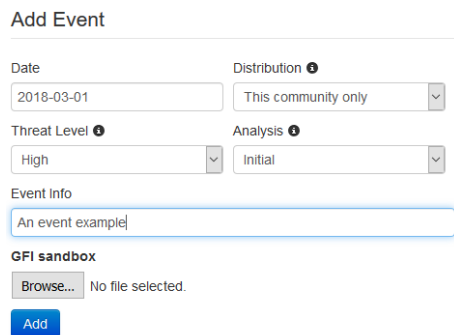
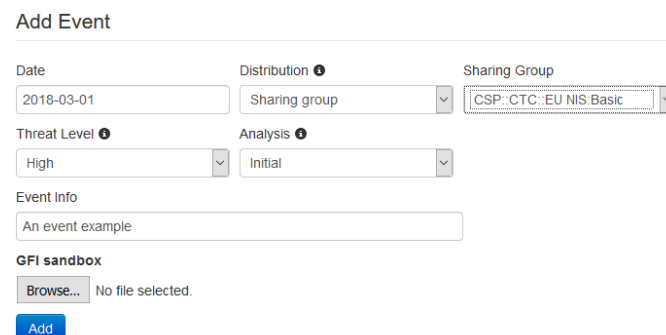
### 7.1 Introduction

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.

### 7.2 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:

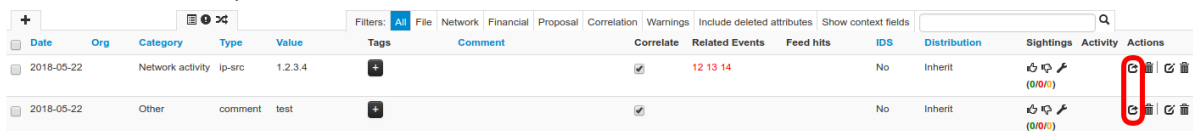
- If user does not select Sharing Group option for Distribution level, the Event will be automatically shared based on Integration Layer (IL) policies.
- If user desires the event to be shared with a specific Trust Circle, then he has to select Sharing group as Distribution level of the event and the corresponding Sharing Group has to be 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.





Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2018-05-22		Network activity	ip-src	1.2.3.4	+		<input checked="" type="checkbox"/>	12 13 14		No	Inherit	(0/0/0)		  
2018-05-22		Other	comment	test	+		<input checked="" type="checkbox"/>			No	Inherit	(0/0/0)		  

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

#### Add Proposal

Category  Type 

Network activity  ip-src 

Value

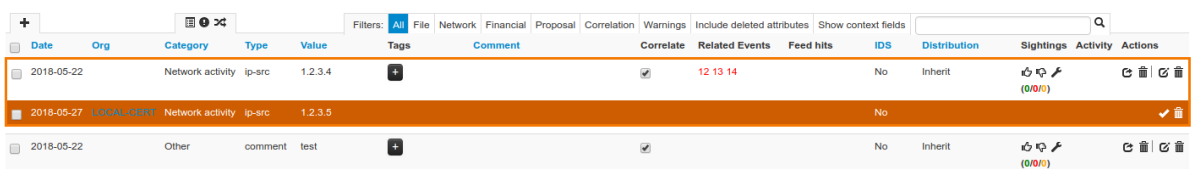
1.2.3.4










Contextual Comment

☐ IDS Signature?

[Propose](#)

By issuing the "Propose" command through the respective button the proposal is added under



Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2018-05-22		Network activity	ip-src	1.2.3.4	+		<input checked="" type="checkbox"/>	12 13 14		No	Inherit	(0/0/0)		  
2018-05-27	LOCAL-CDRT	Network activity	ip-src	1.2.3.5						No				  
2018-05-22		Other	comment	test	+		<input checked="" type="checkbox"/>			No	Inherit	(0/0/0)		  

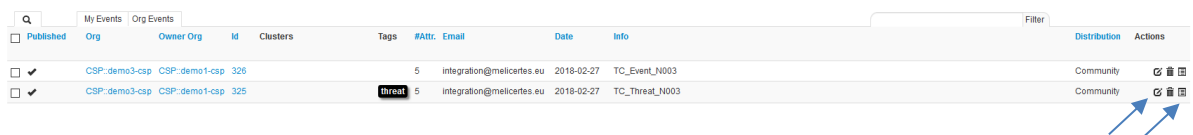
the attribute.







### 7.3 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.

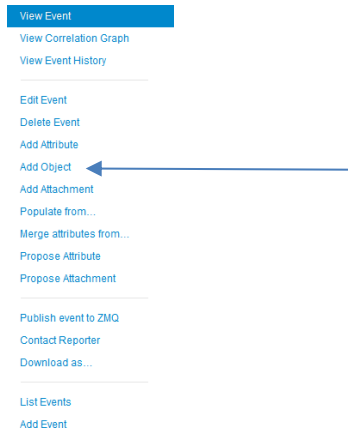
This can be accomplished by adding objects to an already existing MISP event as following:

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:



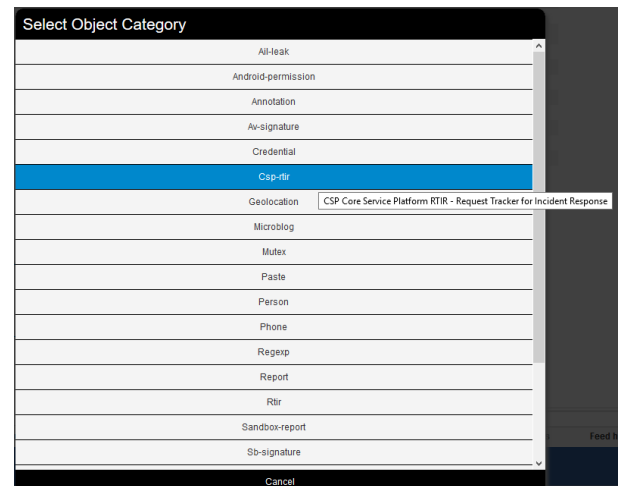
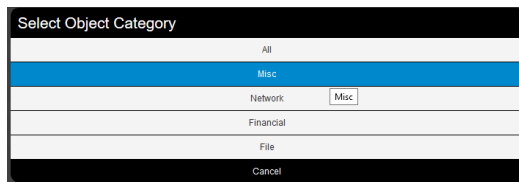
Published	Org	Owner Org	Id	Clusters	Tags	#Attr.	Email	Date	Info	Distribution	Actions
<input checked="" type="checkbox"/>	CSP-demo3-csp	CSP-demo1-csp	326			5	integration@melicentes.eu	2018-02-27	TC_Event_N003	Community	  
<input checked="" type="checkbox"/>	CSP-demo3-csp	CSP-demo1-csp	325		threat	5	integration@melicentes.eu	2018-02-27	TC_Threat_N003	Community	  

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:

<input checked="" type="checkbox"/>	<b>Subject</b> :: text	Subject of the RTIR ticket	Other	[demo3-csp] TC_IN_Threat_001
<input checked="" type="checkbox"/>	<b>Status</b> :: text	Status of the RTIR ticket	Other	new
<input checked="" type="checkbox"/>	<b>Ticket-number</b> :: text	ticket-number of the RTIR	Other	1059

<input checked="" type="checkbox"/>	Csp-originCspId(*) :: text	ID of the Origin CSP	Other	demo3-csp
<input checked="" type="checkbox"/>	Csp-originRecordId(*) :: text	Incident Record ID within the Origin CSP	Other	B29BD048-1BB1-11E8-A8F2-849E2D9094CD
<input checked="" type="checkbox"/>	Csp-uri(*) :: text	URL of the Incident	Other	https://rt.demo1-csp.athens.intrasoft-intl.private:443/RTIR/Display.html?id=1059

dataObject.id	1059
dataObject.subject	[demo3-csp] TC_IN_Threat_001
dataParams.originApplicationId	rt
dataParams.originCspId	demo3-csp
dataParams.originRecordId	B29BD048-1BB1-11E8-A8F2-849E2D9094CD
dataParams.recordId	B29BD048-1BB1-11E8-A8F2-849E2D9094CD
dataParams.uri	https://rt.demo1-csp.athens.intrasoft-intl.private:443/RTIR/Display.html?id=1059

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.

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2018-02-27		Name: csp-rtir*												 
2018-02-27	Other	queue:	incident				<input checked="" type="checkbox"/>	267 268 270 272 <a href="#">Show Show 11more...</a>		No	Inherit	 		 
2018-02-27	Other	subject:	TC_Incident_001				<input checked="" type="checkbox"/>	319 320		No	Inherit	 		 
2018-02-27	Other	status:	new				<input checked="" type="checkbox"/>	270 272 274 299 <a href="#">Show Show 7more...</a>		No	Inherit	 		 
2018-02-27	Other	ticket-number:	1054				<input checked="" type="checkbox"/>	319 320		No	Inherit	 		 
2018-02-27	Other	csp-originCspId:	demo3-csp				<input checked="" type="checkbox"/>	267 270 274 297 <a href="#">Show Show 5more...</a>		No	Inherit	 		 
2018-02-27	Other	csp-originRecordId:	AEE1EC4E-1BAC-11E8-996A-D09E27307E7A				<input checked="" type="checkbox"/>	319 320		No	Inherit	 		 
2018-02-27	Other	csp-uri:	https://rt.demo1-csp.athens.intrasoft-intl.private:443/RTIR/Display.html?id=1054				<input checked="" type="checkbox"/>	319 320		No	Inherit	 		 

## 7.4 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.

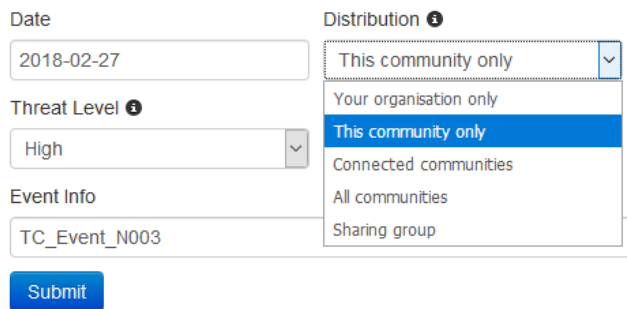
For better understanding CSP integration with MISP application, please have in mind the following remarks, regarding Event Sharing.

### 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 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.



The screenshot shows a form with the following fields:

- Date:** 2018-02-27
- Threat Level:** High
- Event Info:** TC\_Event\_N003
- Distribution:** A dropdown menu is open, showing the following options:
  - This community only (selected)
  - Your organisation only
  - Connected communities
  - All communities
  - Sharing group

A blue **Submit** button is located at the bottom left of the form.

## 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.





```
viper > help
[*] Commands
```

Command	Description
about	Show information about this Viper instance
analysis	View the stored analysis
clear	Clear the console
close	Close the current session
copy	Copy opened file(s) into another project
delete	Delete the opened file
exit, quit	Exit Viper
export	Export the current session to file or zip
find	Find a file
help	Show this help message
info	Show information on the opened file
new	Create new file
notes	View, add and edit notes on the opened file
open	Open a file
parent	Add or remove a parent file
projects	List or switch existing projects
rename	Rename the file in the database
sessions	List or switch sessions
stats	Viper Collection Statistics
store	Store the opened file to the local repository
tags	Modify tags of the opened file

```

[*] Modules

```

Command	Description
apk	Parse Android Applications
clamav	Scan file from local ClamAV daemon
cspShellcode	Updates MISP event with a virus total report.
cspVT	Updates MISP event with a virus total report.
cspXor	Updates MISP event with the XOR analysis report.
cuckoo	Submit the file to Cuckoo Sandbox
debug	Parse McAfee BUP Files

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:

2018-10-04	Name: virustotal-report	References: 0	Inherit
2018-10-04	Other	last-submission: 2018-10-04 05:24:08 date-time	No Inherit
2018-10-04	External analysis	permalink: https://www.virustotal.com/file/563a2d09f04484f525a6cdd3bfb2549616d5e1d84e98e145794ba0519d752/analysis/15386306446/	No Inherit
2018-10-04	Other	detection-ratio: 0/68 text	No Inherit

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:

2018-10-04	Other	comment	Shellcode out: Searching for known shellcode patterns... FS[00h] shellcode pattern matched at offset 63914C[36m0000 64 8b 15 9c 9f 84 ad 61 cd fb e7 d5 1e 07 98 e1 d.....a..... 0010 dc 24 50 9a 5d 2c ac e0 4f be 79 aa 35 91 11 9b SP]...O.y.5... 0020 47 79 3e 01 00 80 aa 20 88 88 a4 45 f4 9c f5 da Gy*.....E... 0030 a7 f9 0f b4 a5 7c 5d c6 e5 45 6e 0e 41 b5 95 74 ....].EnA.L 0040 b0 09 0d 1d 68 0c 08 97 52 c7 50 fc fa d0 d3 45 ....h..R.P...E 0050 60 52 37 17 96 b8 40 15 9f 2a 12 c6 36 3d 76 4a RT...@...6~vJ 0060 98 82 e5 66 c4 4c 0c 93 e1 fb 8e ae 54 0f 73 bc ...L.....T.A. 0070 9d 8e a1 06 f3 da 46 5c aa c5 d0 9c ed 63 06 54 ....F.....T 0080 ab e8 43 c8 3d 78 56 c0 d3 c7 3e fe eb 34 d2 c9 ...C.mV...>.A. 0090 9c 99 a1 23 47 a8 bc fe ce e5 c1 7a 9c 4d a5 0a ...@G...z.M. 00a0 82 50 1d 05 aa d9 1c 40 67 c2 26 be 4b 05 73 11 P....@p&K.s. 00b0 e2 90 82 e7 22 2d 58 b6 bc 26 2c 55 66 cd 06 c5 ....X.&Uf... 00c0 34 ff 63 e8 ee 30 fa f8 23 db 6c 9f b2 1a 3b 5c 4.c.0..#L... 00d0 6e 1a 99 6b d9 cf cb e3 74 eb 22 fc 05 7a 93 b0 n.k...t..z... 00e0 3b 3c bf c2 6b e4 bf 17 2d 8a 4d f9 61 cd be e1 <.k...M.a... []0m	No Inherit
------------	-------	---------	---	------------

13. Run the cspXor module:

```
>cspXor
```

The results of the cspXor populate a new MISP event attribute like the following:

2018-10-04	Other	comment	File: /home/viper/resources/projects/test/binaries/58/3/a/563a2d09f04484f525a6cdd3bfb2549616d5e1d84e98e145794ba0519d752 --XOR search out: afcd3bfb2549616d5e1d84e98e145794ba0519d752 --XOR search out: Searching for the following strings:This ProgramGetSystemDirectoryCreateFileBadReadPtrIsBadWritePtrGetPro cAddressLoadLibraryWinExecCreateFileShellExecuteCloseHandleUnDow nloadToFileGetTempPathReadFileWriteFileSelfFilePointerGetProcAddrVirtu alGetProcAddress on, this might take a while...Searching XORMatched: bhttp with key: 0x74	No Inherit
------------	-------	---------	---	------------

## 9 How to manage and join video conferences with VCB

### 9.1 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.

### 9.2 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.

#### 9.2.1 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.

## Create meeting

Schedule a conference meeting

Cancel Save meeting

Meeting details Participants list

Search for Team Contact

Add External Participant

Remove Participant

Select	Firstname	Lastname	Email address
--------	-----------	----------	---------------

### 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.

## Create meeting

Schedule a conference meeting

Cancel Save meeting

Meeting details Participants list

Search for Team Contact

Dropdown list showing suggestions for internal participants.

Add External Participant

Remove Participant

Email address

## Create meeting

Schedule a conference meeting

Cancel Save meeting

Meeting details Participants list

Search for Team Contact

Add External Participant

Remove Participant

Select	Firstname	Lastname	Email address
--------	-----------	----------	---------------

**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.

Add External Participant

Enter email Add

Add in Bulk

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

Add participants in Bulk

Enter participants' email addresses (any format).

Add Cancel

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:

```
1 email1@example.com;email2@example.com,email3@example.com
2 email4@example.com
3
4 fname1 lname1 <fname1@example.org>
5 fname2 fname2@example.org
6 fname3 lname3 fname3@example.org
7 fname4@example.org fname4
8
9 fname5 lname5 <fname5@example.org>;fname6 lname6 <fname6@example.org>,fname7
10 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.


 Παρ 18/05/2018 11:34  
 csp.testbed.demo3-csp <csp.testbed.demo3-csp@intrasoft-intl.com>  
 Invitation: test-1

To \_\_\_\_\_

 Mail Attachment.ics  
 1 KB

Dear \_\_\_\_\_

You have been invited to a meeting to be held at 18/05/2018 and 08:35 +0000 (planned meeting duration: 1 hour(s) and 00 minutes).

To connect use the following details:

Meeting URL: <https://teleconf.demo3-csp.athens.intrasoft-intl.private:6443?uid=d5b6e241-27cf-4c1e-b6c4-afc0fa9b254c> - this meeting uses WebRTC technology: please use Chrome (latest).

Username: 2CC9F8

Password: DE1024A0ED

Thank you,

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

## My Meetings

Create meeting

Scheduled Meetings [Past Meetings](#)

Cancel meeting

Showing 1-1 of 1

<input type="checkbox"/>	Subject	Start Date/Time ⓘ	Duration	Participants	UID	Status
<input type="checkbox"/>	test	2018-05-30 12:38	1h 0m	1 ⓘ	9d8208ba-37ad-4515-a87e-9d769e86e016	Pending

← First « 1 » Last →


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.

Participants			
Email	Fullname	Username	Password
_____	_____	6005E8	E47929985B

12:38 1h 0m 1 ⓘ 9d8208ba-37ad-4515-a

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

### 9.2.2 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.



Dear 

The meeting at 18/05/2018 and 08:35 +0000 has been cancelled.

Best regards,

#### 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.

### 9.2.3 Past video conferences

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

My Meetings Create meeting

[Scheduled Meetings](#) [Past Meetings](#)

Showing 1-7 of 7

Subject	Start Date/Time ⓘ	Duration	Participants	UID	Status
test meeting	2018-05-23 05:05	1h 0m	0 ⓘ	ec9c4ad3-99b7-4d5b-8465-5200b07f7895	<span>Cancel</span>
test meeting	2018-05-23 05:05	1h 0m	1 ⓘ	4a75c763-64e7-4f4c-9566-a2e11e3f9e4b	<span>Completed</span>
test meeting	2018-05-23 05:00	1h 0m	0 ⓘ	c39d08c5-178d-452b-b2f5-c9b09d64d32a	<span>Cancel</span>
test-2	2018-05-18 11:49	1h 0m	2 ⓘ	cab80036-284e-4a38-8aef-2a19368ae05f	<span>Completed</span>
test-1	2018-05-18 11:35	1h 0m	2 ⓘ	d5b6e241-27cf-4c1e-b6c4-afc0fa9b254c	<span>Cancel</span>
test-2	2018-05-18 01:00	1h 0m	2 ⓘ	587fc041-e85f-4acc-b8c8-3123cfee5d55	<span>Completed</span>
test-1	2018-05-18 00:40	1h 0m	2 ⓘ	06f84cf4-75cc-4e1b-aa65-91109e6a3537	<span>Completed</span>

← First « 1 » Last →



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.

#### 9.2.4 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.

VCBridge Admin | My Meetings | Email Templates | demo

My Email Templates

Create template

Delete template

Showing 1-2 of 2

<input type="checkbox"/>	Name	Type	Last modified ⓘ	Enabled
<input type="checkbox"/>	Auto-generated Invitation	Invitation	2018-05-18 00:29	Active
<input type="checkbox"/>	Auto-generated Cancellation	Cancellation	2018-05-18 00:29	Active

← First
 « 1 »
 Last →

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:

## Update email template

Customize the email template using WYSIWYG editor & shortcodes.

Name

Auto-generated invitation

Type Invitation

Set default

☒ Active

Subject

Invitation: [[\$(meeting\_subject)]]

Message

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta name="viewport"
  content="width=device-width, initial-scale=1, shrink-to-fit=no" />
<meta name="description" content="Login" />
<meta name="author" content="Intrasoft" />
<meta name="keyword" content="Intrasoft" />
<!-- <link rel="shortcut icon" href="assets/ico/favicon.png" -->
<title>Meeting notification</title>
</head>
<body th:inline="text" class="app flex-row align-items-center">
<h3>Dear [[$(email)]]</h3>
<p>You have been invited to a meeting to be held at [[$(meeting_date)]] and [[$(meeting_time)]] (planned
meeting duration: [[$(meeting_duration_str)]]).</p>
<p>To connect use the following details:</p>
<p>Meeting URL: [[$(meeting_url)]] - this meeting uses WebRTC technology: please use Chrome (latest).</p>
<p>Username: [[$(meeting_username)]]</p>
<p>Password: [[$(meeting_password)]]</p>
```

### Shortcodes

[[\$(email)]]	user email
[[\$(meeting_date)]]	date in dd/MM/yyyy format
[[\$(meeting_time)]]	time in HH:mm ZZZ (timezone) format
[[\$(meeting_duration_str)]]	Meeting duration e.g., 2 hour(s) and 10 minutes
[[\$(meeting_duration_str)]]	Meeting duration e.g., 2 hour(s) and 10 minutes
[[\$(meeting_username)]]	the generated/unique username for the participant
[[\$(meeting_password)]]	the generated/unique password for the participant
[[\$(user_first)]]	user first name
[[\$(user_lastname)]]	user last name

- 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.

## 9.3 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.


 Παρ 18/05/2018 11:34  
 csp.testbed.demo3-csp <csp.testbed.demo3-csp@intrasoft-intl.com>  
 Invitation: test-1

To

 Mail Attachment.ics  
 1 KB

Dear

You have been invited to a meeting to be held at 18/05/2018 and 08:35 +0000 (planned meeting duration: 1 hour(s) and 00 minutes).

To connect use the following details:

Meeting URL: <https://teleconf.demo3-csp.athens.intrasoft-intl.private:6443?uid=d5b6e241-27cf-4c1e-b6c4-afc0fa9b254c> - this meeting uses WebRTC technology: please use Chrome (latest).

Username: 2CC9F8

Password: DE1024A0ED

Thank you,

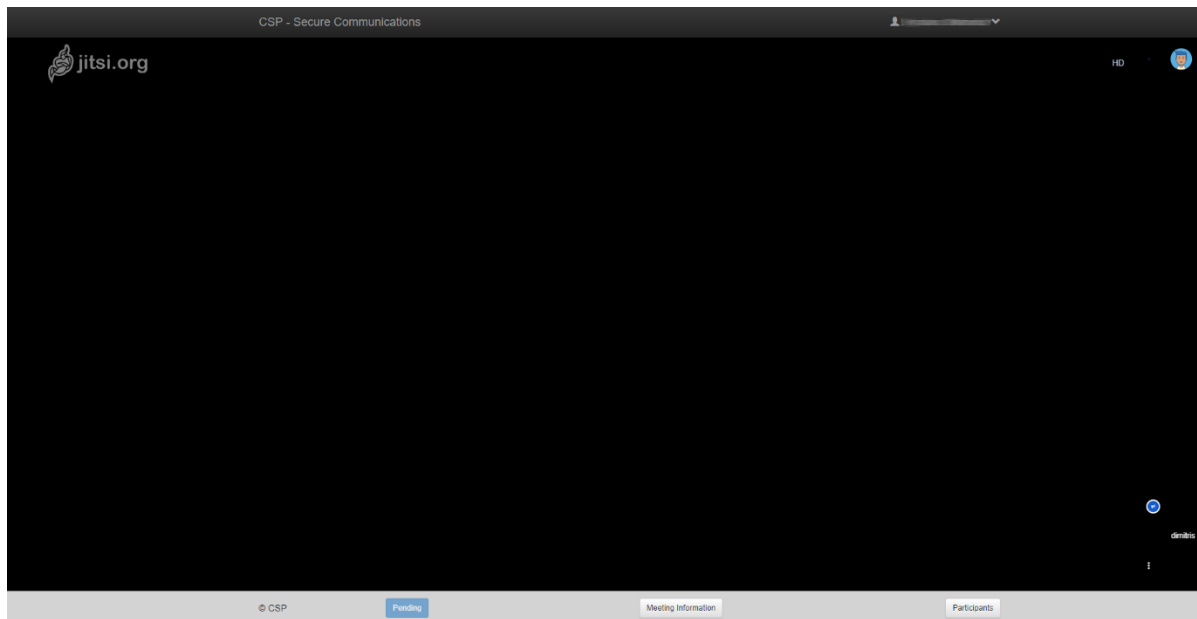
The participant has to follow the URL and provide the credentials that are also mentioned in the invitation's email body. Notice that the conference application (namely: teleconf) does not require an OpenAM session, but only valid user credentials so as to allow external participants from outside the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

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

Please sign in

Sign in

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

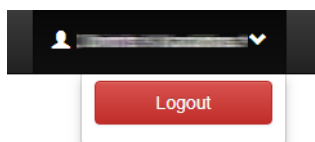


#### Note:

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.

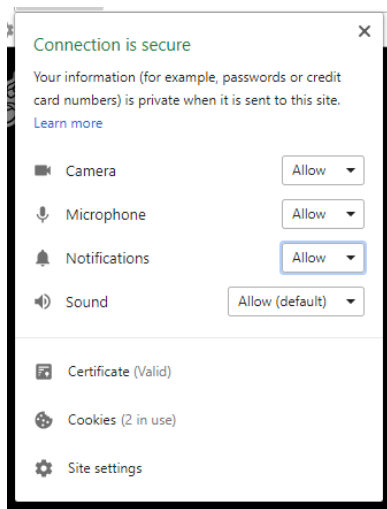


The participant is able to logout from the video conference application by selecting "Logout" from the dropdown menu located at the right of the top most menu.



#### 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.

CSP - Secure Communications	CSP - Secure Communications
<p><b>Completed</b></p> <p>Requested meeting has been completed since: 23/05/2018 03:05 +0000</p>	<p><b>Cancel</b></p> <p>Requested meeting has been cancelled by the organizer!</p>

- End of document-