



# MISP – User Guide

## A Threat Sharing Platform

A collaborative effort from the MISP community

---

# Table of Contents

Introduction	1.1
Book Convention	1.2
Quick Start	1.3
Requirements	1.4
Get Your Instance	1.5
General Layout	1.6
General Concepts	1.7
User Management and Global Actions	1.8
Using the System	1.9
Delegation of Event	1.10
Extending Events	1.11
Administration	1.12
Managing Feeds	1.13
Updating Python dependencies	1.14
Automation and MISP API	1.15
PyMISP - Python Library to Access MISP	1.16
Create an Event Based on a Report	1.17
Taxonomies	1.18
Galaxies	1.19
Sightings	1.20
Warning lists	1.21
Notice lists	1.22
Categories and Types	1.23
Synchronisation/Sharing	1.24
External Connectors	1.25
Modules	1.26
ZeroMQ - MISP publish-subscribe	1.27
Translations - i18n & l10n	1.28
FAQ	1.29
Dev FAQ	1.30
Appendices	1.31

Last modified: Thu Dec 19 2019 11:30:31 GMT+0100 (CET)

# Introduction

build passing



User guide for MISP (Malware Information Sharing Platform) - An Open Source Threat Intelligence Sharing Platform. This user guide is intended for ICT professionals such as security analysts, security incident handlers, or malware reverse engineers who share threat [indicators](#) using MISP or integrate MISP into other security monitoring tools. The user guide includes day-to-day usage of the MISP's graphical user interface along with its automated interfaces ([API](#)), in order to integrate MISP within a security environment.

## Acknowledgement

The MISP user guide is a collaborative effort between all the contributors to [MISP](#) including:

- Belgian Ministry of Defence (CERT)
- [CIRCL Computer Incident Response Center Luxembourg](#)
- Iklody IT Solutions
- [NATO NCIRC](#)
- Cthulhu Solutions
- [CERT-EU](#)

and many other contributors especially the ones during the [MISP hackathons](#).

## Contributing

We welcome contributions to the MISP book. If you want to contribute, fork the [misp-book](#) repository and [pull](#) a request with your changes. You can also [open issues](#) if you find any errors or propose changes.

## Format

MISP book is available in [HTML](#), [PDF](#), [ePub](#) and [Kindle mobi format](#).

## License

The MISP user guide is dual-licensed under [GNU Affero General Public License version 3](#) and [CC-BY-SA 4.0 international](#).

- Copyright (C) 2012 Christophe Vandeplas
- Copyright (C) 2012 Belgian Defence
- Copyright (C) 2012 NATO / NCIRC
- Copyright (C) 2013-2020 Andras Iklody
- Copyright (C) 2015-2020 Alexandre Dulaunoy
- Copyright (C) 2014-2020 CIRCL - Computer Incident Response Center Luxembourg
- Copyright (C) 2018 Camille Schneider
- Copyright (C) 2018-2020 Steve Clement

Last modified: Tue Jan 21 2020 09:44:13 GMT+0100 (CET)

---

## **description: Convention Used in MISP-Book**

### **Convention Used in This Book**

code block or value

- Used for variable, function or menu names in MISP.

### **Language**

The language in this book is American English. All the screenshots and examples are in English.

### **CoC**

The same code of conduct applies to this book as for the main MISP project. As a book can sometimes be considered the inadvertent soul of a piece of software, please take good care and consideration of our [code of conduct](#). The CoC [can be read here](#).

### **Example install**

The examples and screenshots provided in this book have been created with the MISP Autogenerated VM.

To get a copy of the latest VM [click here](#)

### **MISP Instance**

In general when talking about a network of inter-connected MISP servers, each server is a [MISP instance](#). Whilst we have no strong feelings towards anyone's naming schemes, as a rule of thumb try to have a scheme that makes everyday use easy when analysts need to talk about remote MISP instances.

The hostname used for the instance in this book is `misp.local` and we will henceforth refer to it either by name or as `local MISP instance`.

### **Example Organisations**

As MISP is a platform to support information sharing, example organisations are often used within this book.

A set of users and organisations are used in the different examples.

The following two organisations are regularly used as example:

- Setec Astronomy with UUID `58d38339-7b24-4386-b4b4-4c0f950d210f`
- Acme Finance with UUID `58d38326-eda8-443a-9fa8-4e12950d210f`

Starting from MISP 2.4.71, the example organisations with the above mentioned UUID are **black-listed** to avoid large distribution of sample events while testing a [MISP instance](#). If you want to test your distribution, the sample organisation black-listing can be removed in [Administration / Manage Org Blacklists](#).

## Example IOCs

As with the example organisations, we want to make this book as useful as possible by using real life examples.

The following [IOC](#) examples have been used:

- [Sirefef](#) (aka ZeroAccess) Sample Event ID: #31337
- [WannaCry](#) Sample Event ID: #42
- [Dridex](#) Sample Event ID: #23

*Last modified: Wed Aug 19 2020 10:27:11 GMT+0200 (CEST)*

## Quick Start



MISP (Open Source Threat Intelligence and Sharing Platform) software facilitates the exchange and sharing of threat intelligence, [Indicators of Compromise \(IoCs\)](#) about targeted malware and attacks, financial fraud or any intelligence within your community of trusted members. MISP sharing is a distributed model containing technical and non-technical information which can be shared within closed, semi-private or open communities. Exchanging such information should result in faster detection of targeted attacks and improve the detection ratio, whilst also reducing the number of false positives.

With the focus on automation and standards, MISP provides you with a powerful ReST [API](#), extensibility (via misp-modules) or additional libraries such as PyMISP, jump ahead to these chapters to get started.

## Login into MISP

MISP default credentials:

Username:	admin@admin.test
Password:	admin

## I forgot my admin password :(

You can quickly reset it via the command line. You need to know the Admins E-Mail address. Replace www-data with whoever runs the webserver.

```
sudo -u www-data /var/www/MISP/app\Console/cake Password admin@admin.test Password1234
```

## Tasks to do after first Start

1. [Change site admin password](#)
2. [Activate Feeds](#)
3. [Setup your User](#) 3.1 Designate a [Site Admin](#) and an [Org Admin](#) 3.2 Add some contributing users and assign the corresponding [Roles](#)
4. [MISP Administration](#) 4.1 Edit your first organisations' name

## Password Policy

- [12]: Ensure that the password is at least 12 characters long
- [A-Z]: contains at least one upper-case
- [0-9]: includes a digit or a special character
- [a-z]: at least one lower-case character.

If you need a password generator use:

- Ubuntu / Debian: [pwgen](#)
- Website: [LastPass PW Generator](#)
- Built-in generator in KeePass\* and other password manager
- Built-in generator in various web browsers

**All Generator tools are only possibilities without any guarantee!**

**tl;dr****Create an Event**

**A. Add Event**

1. **Add Event**

2. **Populate Fields**

All IOC data entered is made up of an event object and described by its connected attributes.

3.

4.

**B. Add Attachments**

5. **Populate Fields**

The following attribute types should be added for each event:

- ip-src: source IP of attacker
- email-src: email used to send malware
- md5/sha1/sha256: checksum
- Hostname: full host/dnsname of attacker
- Domain: domain name used in malware

6.

7.

8. **Populate Fields**

9.

## Browse Past Events

The screenshot shows the 'Event Actions' dropdown menu open, with the 'List Events' option highlighted. A green callout bubble labeled '1.' points to this menu item. Below the menu, a table displays two event rows. A green callout bubble labeled '2. Filter' points to the search/filter bar above the table. Another green callout bubble labeled '3. Click any row' points to the first event row. To the right of the table, a section titled 'Related Events' lists several event IDs and dates. A final green callout bubble labeled '4. See events with one or more matching attributes' points to this section.

**Event**

ID	104					
Uuid	50fe6590-3ed4-4ab9-8351-5492ac1d4fa4					
Org	NCIRC					
Date	2013-01-22					
Risk	Undefined					
Analysis	Completed					
Distribution	All communities, this will share the event with all MISP communities, allowing the event to be freely propagated from one server to the next.					
Info	FAKEM RAT report from Trend Micro - Expanded IoCs based on ISC passive DNS					
Published	Yes					
<b>Attributes</b>						
Category	Type	Value	Related Events	IDS	Distribution	Actions
Network activity	domain	zaoto.org	81 25 7	No	All	
	domain	bluematt.me		No	All	

**Related Events**

- 2013-01-17 (103) 2012-11-27 (81)
- 2012-07-21 (45) 2012-07-16 (32)
- 2012-07-12 (26) 2012-07-12 (26)
- 2012-07-11 (31) 2012-07-02 (7)

**4. See events with one or more matching attributes**

## Export Events for logsearches



## Create an Event

**1.** 

The event created will be restricted to the organisations included in the distribution setting on the local instance only until it is published.

**Add Event**

Date	Distribution <small>i</small>
2018-05-10	This community only
Threat Level <small>i</small>	Analysis <small>i</small>
High	Initial
Event Info	
Quick Event Description or Tracking Info	
Extends event	
Event UUID or ID. Leave blank if not applicable.	
<b>GFI sandbox</b>	
<input type="button" value="Choose file"/>	No file chosen
<input type="button" value="Add"/>	

**3. Add == Save**

**2. Summarized description:**

- Distribution
- Threat Level
- Event Info
- GFI sandbox (optional)
- Does it extend? (optional)

You only have to add a few pieces of information to register your Event. Further details will be specified after the Event has been added.

## Describe Event

The event has been saved

- [View Event](#)
- [View Correlation Graph](#)
- [View Event History](#)
  
- [Edit Event](#)
- [Delete Event](#)
- [Add Attribute](#)
- [Add Object](#)
- [Add Attachment](#)
- [Populate from...](#)
- [Enrich Event](#)
- [Merge attributes from...](#)
  
- [Publish Event](#)
- [Publish \(no email\)](#)
- [Publish event to ZMQ](#)
- [Contact Reporter](#)
- [Download as...](#)
  
- [List Events](#)
- [Add Event](#)

### OSINT - Threat Spotlight: Ratsnif - New Network Vermin from OceanLotus

Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88 <a href="#">+</a>
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin.test
Tags	+  +
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial
Distribution	This community only
Info	OSINT - Threat Spotlight: Ratsnif - New Network Vermin from OceanLotus
Published	No
#Attributes	0 (0 Object)
First recorded change	1970-01-01 01:00:00
Last change	2019-07-09 06:28:19
Modification map	
Sightings	0 (0) - restricted to own organisation only

[- Pivots](#) [- Galaxy](#) [+ Event graph](#) [+ Correlation graph](#) [+ ATT&CK matrix](#) [- Attributes](#) [- Discussion](#)

1: OSINT ...

Now you can specify the information for your Event (you will need to scroll the window).

## Free-Text Import Tool

The screenshot shows a web-based application interface for managing events. At the top, there is a navigation bar with links: Pivots, Galaxy, Event graph, Correlation graph, ATT&CK matrix, Attributes, and Discussion.

A prominent red message box at the top states: "All IoC data entered is made up of an event object and described by its connected attributes".

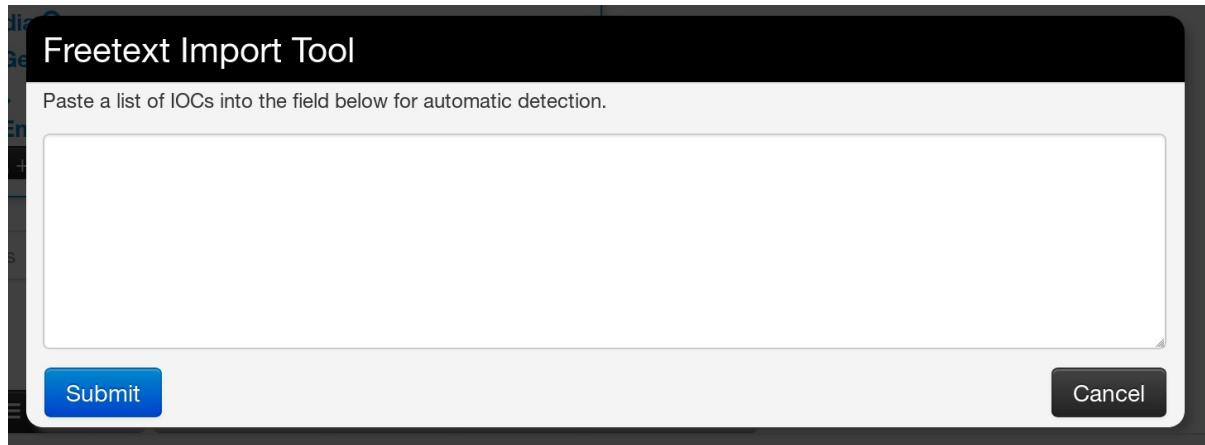
Below this, a section titled "Galaxies" contains two small icons: a globe and a person.

At the bottom of the interface, there is a toolbar with various buttons and filters. A red arrow points from the text "To get straight to the Freetext import tool click here" to one of the buttons in this toolbar.

A red banner at the very bottom of the page reads: "Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or i".

The following will pop-up.

If you have a list of [indicators](#) from which you would like to quickly generate attributes then the **Free-text import tool** is just what you need. Simply paste your list of [indicators](#) (separated by line-breaks) into this tool.



## Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS	Comment	Actions
c1e21a06a1f8	95 95	Payload delivery	sha256	<input checked="" type="checkbox"/>	Imported via the Freetext Import	

**Submit**

sha256 → authentihash **Change all**

**Update all comment fields** **Change all**

The tool will help you to find similarities between your import and other issues already registered in MISP.

A screenshot of a tooltip titled "Attribute details" containing the following information:

- Event ID: **95**
- Event Info: OSINT - LinkedIn information used to spread banking malware in the Netherlands
- Category: Payload delivery
- Type: filename|sha256
- Value: office.bin|c1e21a06a1fa1de2996392668b6910c
- Comment: downloaded malware

For example, you can see the ID of all related Events and view their information.

### Alternative to import

An alternative route to reach the Freetext import tool is shown below.

The event has been saved

To add attributes select "Populate from..."

### OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88 <a href="#">+</a>
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin.test
Tags	+  +
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial

**View Event**

[View Correlation Graph](#)

[View Event History](#)

---

[Edit Event](#)

[Delete Event](#)

[Add Attribute](#)

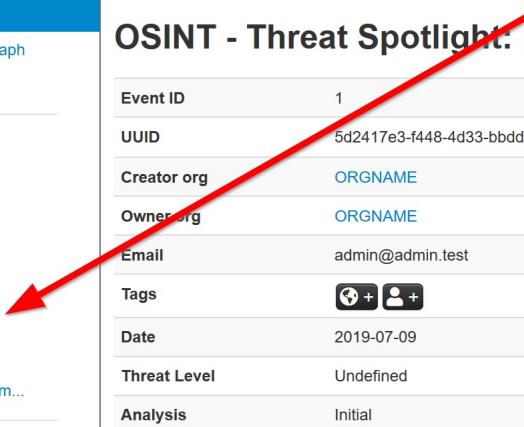
[Add Object](#)

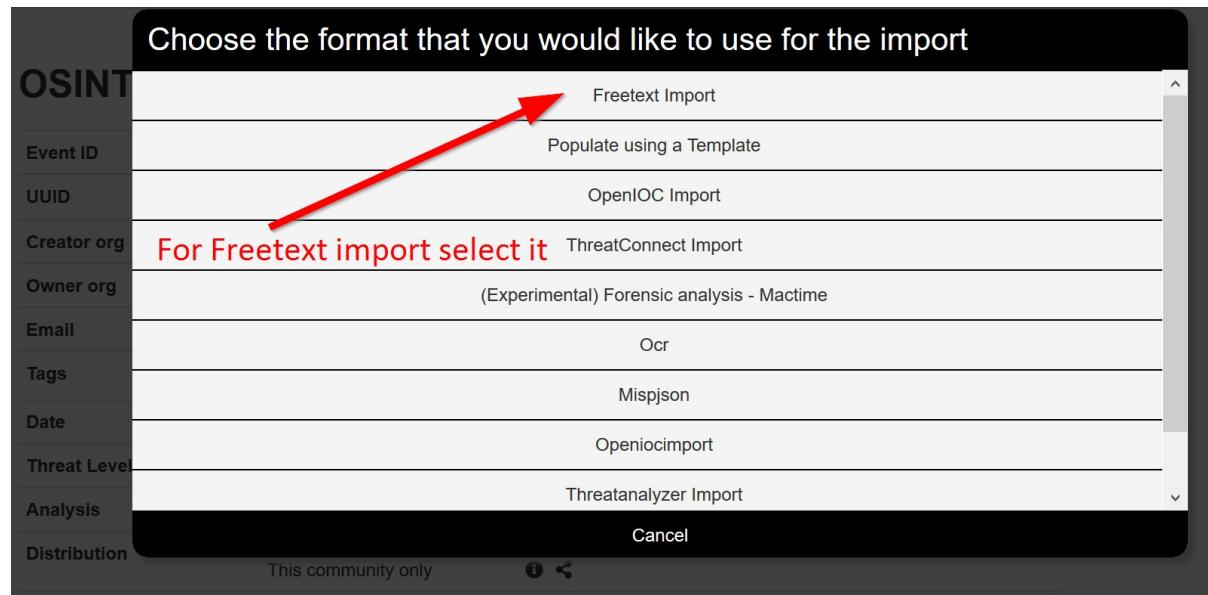
[Add Attachment](#)

[Populate from...](#)

[Enrich Event](#)

[Merge attributes from...](#)





## Tags and Taglist

### Using existing Data

Another easy way to add information is to use Tags. You can see the result of adding existing Tags (circl:incident-classification=XSS and circl:incident-classification="information-leak").

## OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88 <a href="#">+</a>
Creator org	ORGNAME <a href="#">To add tags from a Taxonomy or Custom tags, click here</a>
Owner org	ORGNAME
Email	admin@ Add a tag <a href="#">x</a>
Tags	 <a href="#">+</a> <a href="#">Add a tag</a> <a href="#">Tag Collections</a> <a href="#">Custom Tags</a> <a href="#">All Tags</a>
Date	2019-07
Threat Level	Undefined
Analysis	Initial

By clicking the button, you can add more tags from an existing Taglist.

## OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

Event ID	1	<b>/!\ If no tags show up, enable a Taxonomy or create some custom tags</b>
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88	<input style="border-radius: 50%; width: 20px; height: 20px;" type="button" value="+"/>
Creator org	ORGNAME	Select Tag collections (taxonomies) or self-created tags
Owner org	ORGNAME	
Email	admin@	Add a tag
Tags	<input style="border-radius: 50%; width: 20px; height: 20px; vertical-align: middle;" type="button" value="+"/>	
Date	2019-07	
Threat Level	Undefined	
Analysis	Initial	

Select the input box to see the tags

Select Tag collections (taxonomies) or self-created tags

Add a tag

malware

In particular the "Taxonomy Library: circl" Taglist is very complete.

Once you added the tag(s) it will show in your main event window and in the list event view.

## OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88 <span style="border: 1px solid black; padding: 2px;">+</span>
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin.test
Tags	<span style="background-color: #ff0000; color: white; padding: 2px 10px; border-radius: 5px;">malware</span> <span style="border: 1px solid black; padding: 2px;">x</span> <span style="border: 1px solid black; padding: 2px;">+ </span> <span style="border: 1px solid black; padding: 2px;">+ </span>
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial

Once you have confirmed the tag(s)  
they will appear here

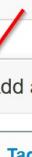
## Local tags

Local tags can be added in a similar fashion.

### OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88 <a href="#">+</a>
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin.com Add a local tag <a href="#">X</a>
Tags	<a href="#">+</a>
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial

To add local tags, click here



[Tag Collections](#) [Custom Tags](#) [All Tags](#)

They will be identified by a corresponding icon.

Tags	type:OSINT x  osint:lifetime="perpetual" x  circl:osint-feed x  tip:white x osint:source-type="blog-post" x  osint:certainty="93" x estimative-language:confidence-in-analytic-judgment="high" x workflow:todo="review-for-privacy" x  +
Date	2019-07-04
Threat Level	Low
Analysis	Ongoing
Distribution	All communities

## No tags in list

In case you get the below. You need to either enable an existing Taxonomy or add some custom tags.

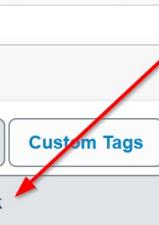
## OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88 <a href="#">+</a>
Creator org	ORGNAME <i>/!\ If no tags show up, enable a Taxonomy or create some custom tags</i>
Owner org	ORGNAME
Email	admin@
Tags	+
Date	2019-07
Threat Level	Undefined
Analysis	Initial

Add a tag

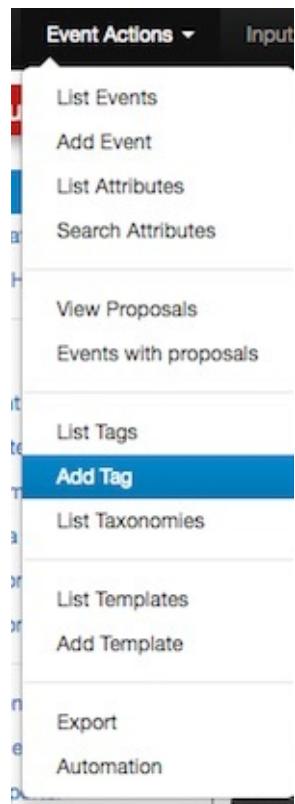
[Tag Collections](#) [Custom Tags](#) [All Tags](#)

Nothing to pick



## Make your own Taglist

If you want make your own Taglist, select Add Tag.



You will see the following window:

The screenshot shows a software application window titled "Add Tag". At the top, there is a navigation bar with links: Home, Event Actions ▾, Input Filters ▾, Global Actions ▾, Sync Actions ▾, Administration ▾, Audit ▾, and Discussions ▾. On the left side, there is a sidebar with three items: List Favourite Tags, List Tags, and Add Tag, where "Add Tag" is highlighted with a blue background. The main content area has a title "Add Tag". It contains three input fields: "Name" (Popom), "Colour" (#1bb5f7), and "Restrict tagging to" (Unrestricted). Below these fields is a checked checkbox labeled "Exportable" and a blue "Add" button.

Then, when you add the new tag it will appear in the Custom Taglist.

## Suggestions

The following attribute types should be added for each Event:

- ip-src: source IP of attacker
- email-src: email used to send malware
- md5/sha1/sha256: checksum
- Hostname: full host/dnsname of attacker
- Domain: domain name used in malware

## Browsing Events

To see your Event, select List Events from the menu Events Action. You can click any row and select a filter.

The screenshot shows the MISP web interface with the 'List Events' action selected. The left sidebar contains navigation links for Event Actions, Input Filters, Global Actions, Sync Actions, Administration, Audit, and Documentation. The main content area displays a table of events. The table has columns for Owner Org, ID, Tags, #Attr., and #Corr. Two specific rows are highlighted with green boxes and arrows pointing to them:

	Owner Org	ID	Tags	#Attr.	#Corr.
MISP	145	<b>Your Event</b>	<code>circl:incident-classification="XSS"</code> <code>circl:incident-classification="information-leak"</code> <code>hopshop</code>	1	1
MISP	95	<b>Your tag</b>	<code>Type:OSINT</code> <code>tip:white</code> <code>circl:incident-classification="malware"</code>	12	1

If you click on your Event's number, you can see all the information related to your Event.

## OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

ORGNAME

Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88 <a href="#">+</a>
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin.test
Tags	+  +
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial

This is the  
Organizations name

Related Events

OR... Unidentified Malware via SpamMailServer3  
2019-07-09 1

Number of  
matching attributes

Related events, events that share  
attributes, will be displayed here

## Export Events for Log Search

Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, the Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support NIDS signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

The screenshot shows the MISP web interface. At the top, there is a navigation bar with links for Home, Event Actions, Input Filters, Global Actions, Sync Actions, and Admin. On the left, a sidebar titled 'List Events' contains links for Add Event, Import From MISP Export, List Attributes, Search Attributes, View Proposals, Events with proposals, and Automation. The main area is titled 'Events' and displays a list of events. A red arrow points to the 'Export' link in the sidebar, with the text 'Click to go' written next to it. The event list table has columns for Published, Org, Owner Org, Id, and Tags. Two events are listed:

Published	Org	Owner Org	Id	Tags
✓	MISP	MISP	145	<code>circl:incident-classification="X"</code> <code>circl:incident-classification="In leak"</code> <code>hophop</code>
✓	TP	MISP	95	<code>Type:OSINT</code> <code>tlp:</code> <code>circl:incident-classification="m</code>

Simply click on any of the following buttons to download the appropriate data for log correlation.

<a href="#">List Events</a>
<a href="#">Add Event</a>
<a href="#">Import From MISP Export</a>
<a href="#">List Attributes</a>
<a href="#">Search Attributes</a>
<a href="#">View Proposals</a>
<a href="#">Events with proposals</a>
<b>Export</b>
<a href="#">Automation</a>

## Export

Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support NIDS signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

Simply click on any of the following buttons to download the appropriate data.

Type	Last Update	Description	Outdated	Progress	Actions
XML	N/A	Click this to download all events and attributes that you have access to (except file attachments) in a custom XML format.	Yes	N/A	<a href="#">Download</a> <a href="#">Generate</a>
CSV_Sig	N/A	Click this to download all attributes that are indicators and that you have access to (except file attachments) in CSV format.	Yes	N/A	<a href="#">Download</a> <a href="#">Generate</a>
CSV All	N/A	Click this to download all attributes that you have access to (except file attachments) in CSV	Yes	N/A	<a href="#">Download</a> <a href="#">Generate</a>

## **Enable a Taxonomy**

## **Enable and fetch a feeds**

Last modified: Thu Nov 01 2018 16:29:37 GMT+0100 (CET)

# MISP Instance requirements

- [Intro](#)
- [The biggie](#)
  - [Tool assisted sizing](#)

## Intro

There are various ways you can run a [MISP instance](#).

- Virtualized with docker/ansible/packer etc
- VMware/Virtualbox/Xen etc
- Dedicated hardware
- Road warrior setups
- Air-gapped setups

Whilst there is never an ultimate answer to what specifications a system needs, we try to give an approximate answer depending on your use case.

## The biggie

Having millions of events with millions of attributes ([Indicators](#)) will eventually result in sub-par performance. Ideally you have millions of attributes and thousands of events. But this also depends on how you ingest the data. With millions of attributes a bottleneck could be the correlation engine. Especially if you have many duplicates in your events. (Use the feed matrix to see if feeds are massively overlapping)

## Tool assisted sizing

During a hackathon [misp-sizer](#) was conceived. ([code](#)) This can give you a very rough estimate and needs some more [improvements](#).

 Last modified: Thu Sep 13 2018 15:22:36 GMT+0200 (CEST)

## Get your own MISP instance

The intention of this chapter is to support you in getting your own [MISP instance](#) up and running.

### MISP Virtual Machine

CIRCL maintains the image of a recent MISP virtual machine online. This VM is generated after every commit to the main MISP repository on Github.

This is a very easy out of the box solution, optimized for product evaluation and to support trainings held by CIRCL staff.

### MISP VM Download

The best place to get the latest version of the MISP virtual machine, as well as all the available training materials is the [MISP training materials page](#) on the CIRCL website.

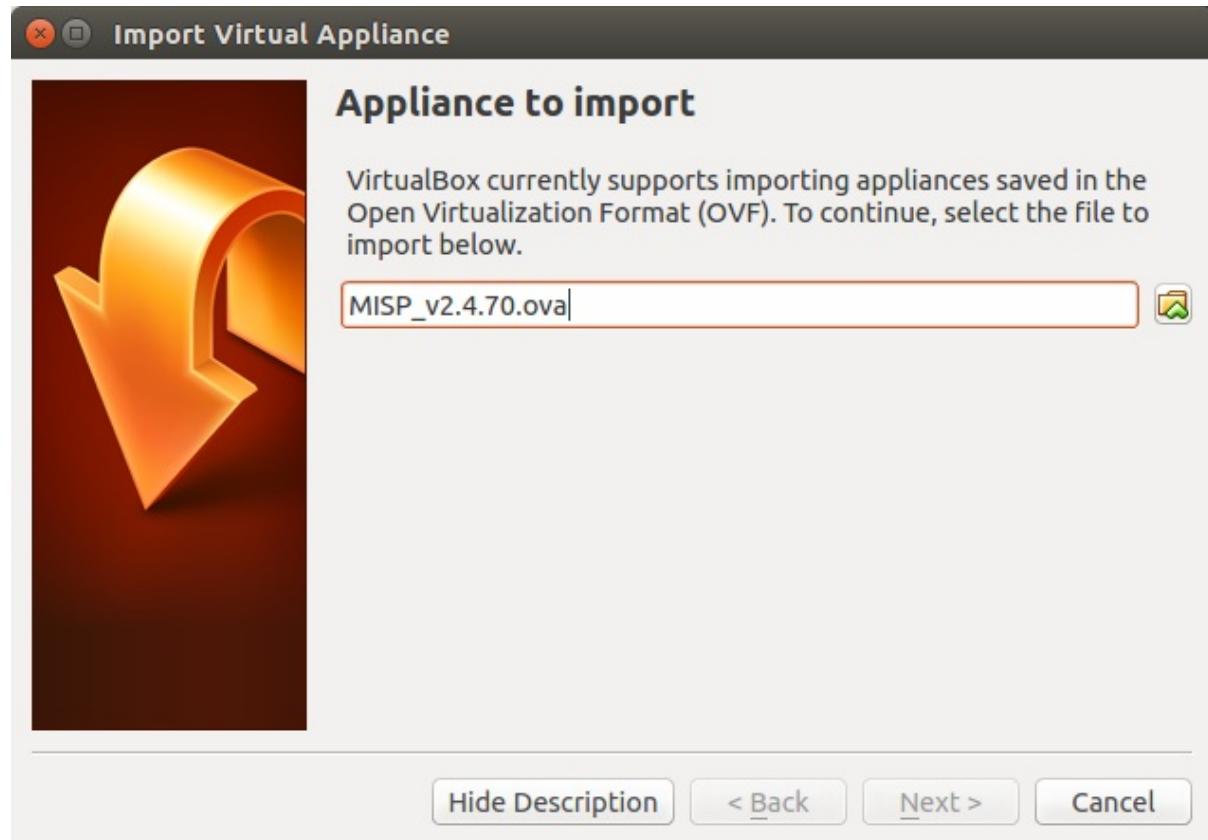
If you do not remember the direct link to the MISP training materials here are the very easy to remember steps you have to follow to reach the right place:

1. Access the [CIRCL homepage](#)
2. Navigate to the [Training area](#)
3. Click [MISP Malware Information Sharing Platform - Threat Sharing](#)
4. Follow the link to the [Training materials freely available](#)

Download the image of the virtual machine and validate the SHA512 fingerprint.

### Import Appliance

In VirtualBox use the "Import Appliance..." functionality to import the virtual machine.



The instructions in this manual covers VirtualBox only. If you prefer another virtualization solution like VMWare you can find some quick instruction on the [MISP training materials page](#).

ESXi Servers have been tested too. Should work without problem but some manual changing of the ATA-Bus is needed.

## MISP VM Credentials

The MISP image is pre-configured to be reachable on the private IP address **localhost** by SSH on port 2222. The GUI is reachable by <http://localhost:8080/>.

You should have two interfaces on your VirtualBox configuration (NAT and host-only). You can also configure access to the [MISP instance](#) by doing port forwarding on the NAT interface.

MISP credentials:

- **GUI Admin:** admin@admin.test:admin (it's the [site admin](#) account with full rights, feel free to create other users)
- **Shell/SSH:** misp : Password1234
- **MySQL:** The credentials are generated during the VM generator. The details are located in ~misp/mysql.txt

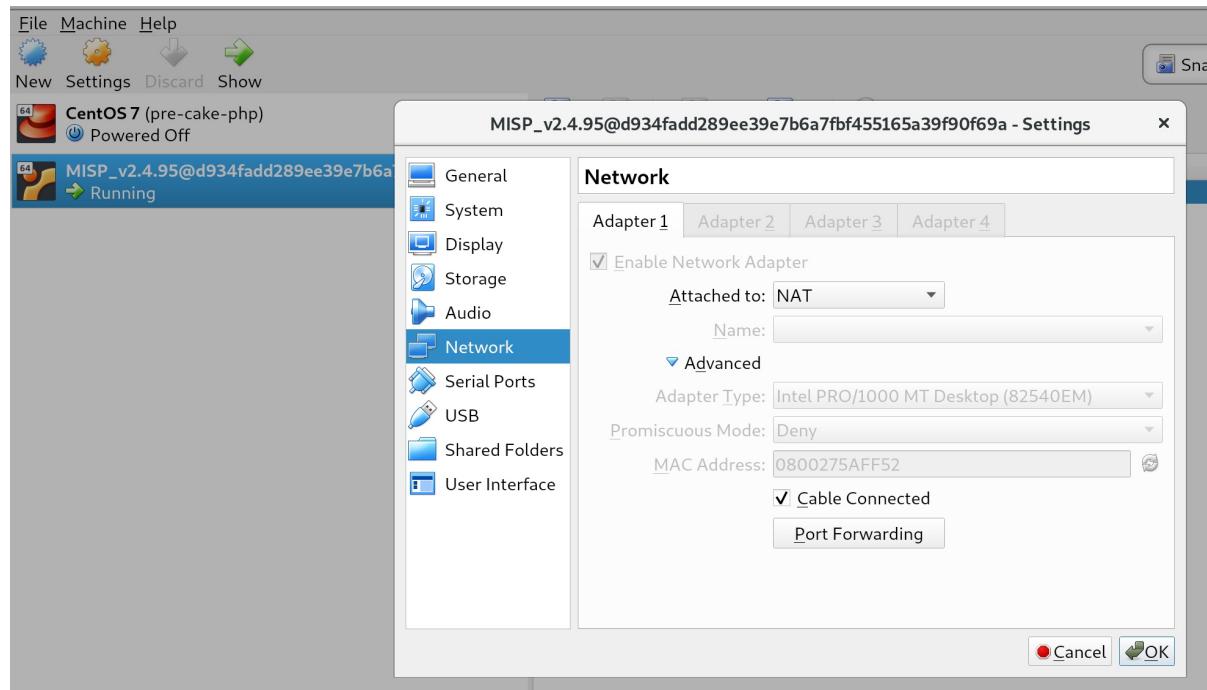
## Networking on the VM

Virtualbox has a neat feature to forward ports from your Host machine to the Guest VM. We forward the following ports:

- **ssh** Forward from 2222 on Host -> 22 on guest
- **http** Main WebUI - 8080 on Host -> 80 on guest
- **https** Not in use - 8443 on Host -> 443 on guest
- **8001** MISP Dashboard - 8001 on Host -> 8001 on guest
- **8888** Viper Web UI - 8888 on Host -> 8888 on guest
- **1666** misp-modules used to poll the misp-modules [API](#) - 1666 on Host -> 6666 on guest

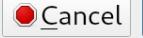
If the port is already used on your host, virtualbox will still boot and all the other ports will work.

To change the port forwarding select the running VM in the UI and click on **Settings** -> **Network** -> **Advanced** -> **Port forwarding**



## Overview of default port forwards

Name	Protocol	Host IP	Host Port	Guest IP	Guest Port	
dashboard	TCP		8001	0.0.0.0	8001	
http	TCP		8080		80	
https	TCP		8443		443	
misp-modules	TCP		1666	0.0.0.0	6666	
ssh	TCP		2222	0.0.0.0	22	
viper	TCP		8888	0.0.0.0	8888	

The reason that some entries have `0.0.0.0` and other are left blank is due to a virtualbox bug where traffic would not be sent to the Guest VM.



VMWare users will need to connect to whatever IP the VM has on your host. There is NO port forwarding done for VMWare.

## Potential issues

You might have a very old VM installed and the ports are not be forwarded. Either configure the port forwards manually or download a new VM.

Last modified: Thu Sep 13 2018 15:22:36 GMT+0200 (CEST)

## General Layout

### The top bar

#### Simple User



This menu contains all of the main functions of the site as a series of dropdown menus. These contains all (from the current simple user's perspective) accessible functions sorted into several groups.

- **Home button:** This button will return you to the start screen of the application, which is the event index page (more about this later).
- **Event Actions:** All the malware data entered into MISP is made up of an event object that is described by its connected attributes. The Event actions menu gives access to all the functionality that has to do with the creation, modification, deletion, [publishing](#), searching and listing of events and attributes.
- **Galaxies:** Shortcut to the list of [MISP Galaxies](#) on the [MISP instance](#).
- **Input Filters:** Input filters alter what and how data can be entered into this instance. Apart from the basic validation of attribute entry by type, it is possible for the site administrators to define regular expression replacements and blacklists for certain values in addition to blocking certain values from being exportable. Users can view these replacement and blacklist rules here whilst administrator can alter them.
- **Global Actions:** This menu gives you access to information about MISP and this instance. You can view and edit your own profile, view the manual, read the news or the terms of use again, see a list of the active organizations on this instance and a histogram of their contributions by attribute type.
- **MISP:** Simple link to your BASEURL
- **Steve:** Name (Auto generated from Mail address) of current logged in user
- **Envelope:** Link to User Dashboard where you can consult some of your notifications and changes since last visit. Like some of the [proposals](#) received for your organisation.
- **Log out:** The Log out button to end your session immediately.

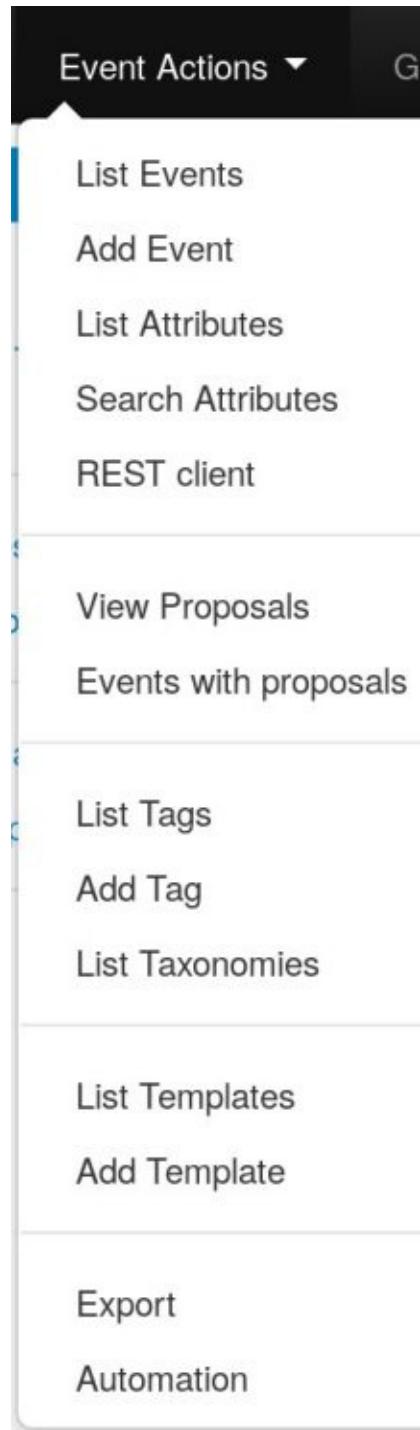
## Admin Menu Bar



- **Home button:** idem as user.
- **Event Actions:** ibidem
- **Galaxies:** You can additionally update the Galaxies.
- **Input Filters:** Ibidem
- **Global Actions:** Ibidem
- **Sync Actions:** With administrator access rights, shows a list of the connected instances and allows the initiation of a [push](#) and a [pull](#) (more about the synchronization mechanisms later).
- **Administration:** Administrators can add, edit or remove user accounts and user [roles](#). [Roles](#) define the access rights to certain features such as [publishing](#) of events, usage of the REST interface or synchronization of any user belonging to the given role. Site administrators can also access a contact form, through which it is possible to reset the passwords of users, or to just get in touch with them via encrypted e-mails.
- **Audit:** If you have audit permissions, you can view the logs for your organization (or for site admins for the entire system) here or even search the logs if you are interested in something specific.
- **MISP:** ibidem
- **Admin:** ibidem
- **Envelope:** Link to User Dashboard where you can consult some of your notifications and changes since last visit. Like some of the [proposals](#) received for your organisation.
- **Log out:** The Log out button to end your session immediately.

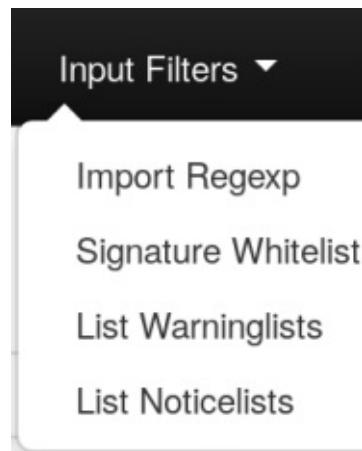
## A list of the contents of each of the above drop-down menus

### Event actions



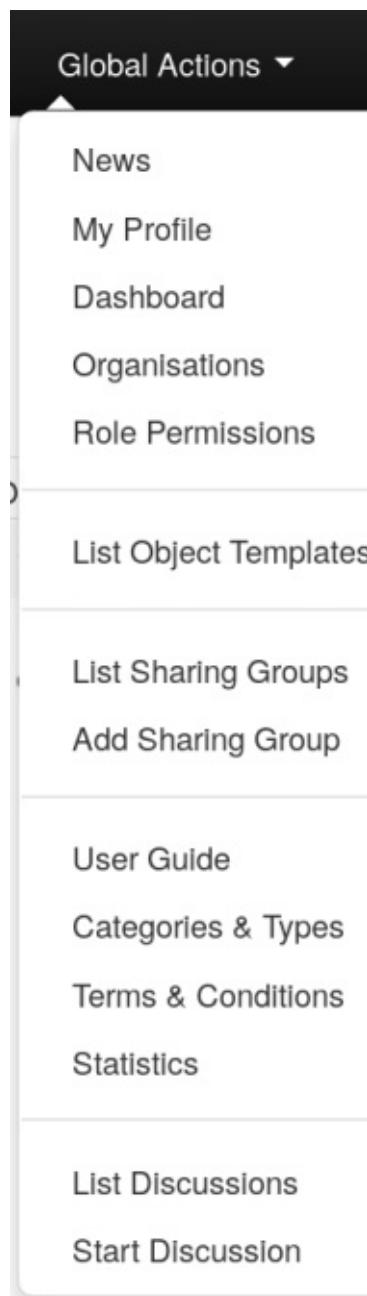
- **List Events:** Lists all the events in the system that are not private or belong to your organisation. You can add, modify, delete, publish or view individual events from this view.
- **Add Event:** Allows you to fill out an event creation form and create the event object, which you can start adding attributes.
- **List Attributes:** Lists all the attributes in the system that are not private or belong to your organisation. You can modify, delete or view each individual attribute from this view.
- **Search Attributes:** You can set search terms for a filtered attribute index view here.
- **REST client** MISP Online REST client where you can make calls directly to the [API](#) via a Web UI.
- **View Proposals:** Shows a list of all [proposals](#) that you are eligible to see.
- **Events with proposals:** Shows all of the events created by your organisation that has pending [proposals](#).
- **List Tags:** List all the tags that have been created by users with tag creation rights on this instance.
- **Add Tag:** Create a new tag.
- **List Taxonomies:** List all of the taxonomies installed on the [MISP instance](#). This is also the place to activate the taxonomies as a [Org Admin/Site Admin](#).
- **List Templates:** List all of the templates created by users with template creation rights on this instance.
- **Add Template:** Create a new template.
- **Export:** Export the data accessible to you in various formats.
- **Automation:** If you have authentication key access, you can view how to use your key to use the REST interface for automation here.

#### Input filters



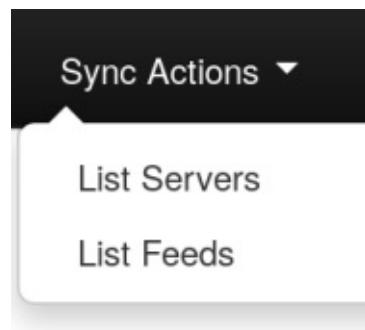
- **Import Regexp:** You can view the Regular Expression rules, which modify the data that can be entered into the system. This can and should be used to help filter out personal information from automatic imports (such as removing the username from windows file paths), having unified representation for certain common values for easier correlation or simply standardizing certain input. It is also possible to block certain values from being inserted. As a site administrator or a user with regex permission, you can also edit these rules.
- **Signature Whitelist:** You can view the whitelist rules, which contains the values that are blocked from being used for exports and automation on this instance. Site administrators have access to editing this list.
- **List Warninglists:** MISP warninglists are lists of well-known indicators that can be associated to potential false positives, errors or mistakes. The warning lists are integrated in MISP to display an info/warning box at the event and attribute level.
- **List Noticelists:** MISP noticelists are lists of #Todo: Double check description from repo!!!

#### Global Actions



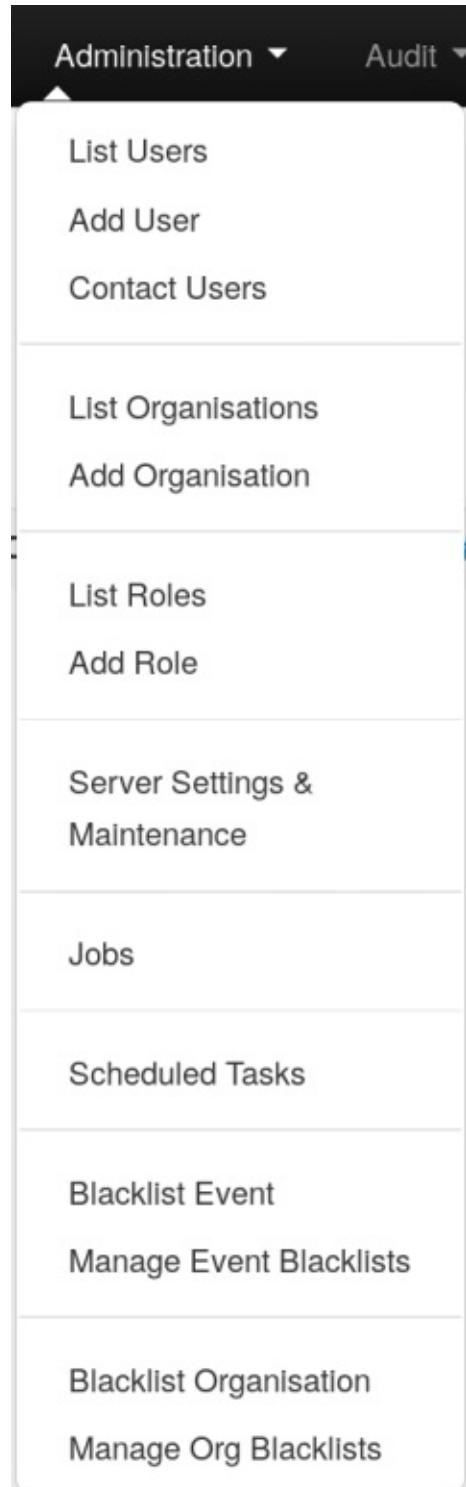
- **News:** Read about the latest news regarding the MISP system
- **My Profile:** Manage your user account.
- **Dashboard:** allow you to see your Notifications of [Proposals](#), Events with [proposals](#) and Delegation request. You can see the last changes since your last visit, as Events updates and Events publications.
- **Organizations:** View the organizations having a presence on this instance, with some useful informations as contact's name.
- **Role Permissions:** You can view the role permissions here.
- **List Sharing Groups:** You can view the list of existing [Sharing Groups](#) who you or your organization have access.
- **Add Sharing Group:** You can create a sharing group.
- **User Guide:** A link to this user guide.
- **Categories & Types:** Quick overview of Attribute Categories and Type. e.g: md5 -> Payload delivery, Artifacts dropped, Payload installation, External analysis
- **Terms & Conditions:** General terms and conditions which can be configured in Administration -> Server Settings -> MISP Settings: MISP.terms\_file . From the UI: "The filename of the terms and conditions file. Make sure that the file is located in your MISP/app/files/terms directory"
- **Statistics:** View a series of statistics about the users and the data on this instance.
- **List Discussions:** List threads of discussions created on the [MISP instance](#) by the organisations connected to this local community.
- **Start Discussion:** Create a new discussion thread.

#### Sync Actions



- **List Servers:** Connect your MISP instance to other instances, or view and modify the currently established connections.
- **List Feeds:** Follow the RSS feeds of other organization or CERTs worldwide.

#### Administration



- **List Users:** View, modify or delete the currently registered users.
- **Add User:** Create an account for a new user for your organisation. Site administrators can create users for any organisation.
- **Contact Users:** You can use this view to send messages to your current or future users or send them a temporary password.

When adding a new user to the system, or when you want to manually reset the password for a user, just use the "Send temporary password" setting.

After selecting the action, choose who the target of the e-mails should be (all users, a single user or a user not yet in the system).

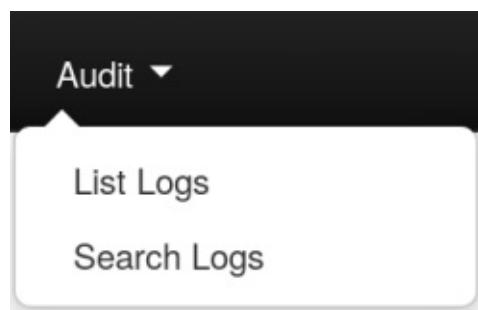
You can then specify (if eligible) what the e-mail address of the target is (for existing users you can choose from a dropdown menu).

In the case of a new user, you can specify the future user's GnuPG key, to send his/her new key in an encrypted e-mail.

The system will automatically generate a message for you, but it is also possible to write a custom message if you tick the checkbox, but don't worry about assigning a temporary password manually, the system will do that for you, right after your custom message.

- **List Organisations:** View the organizations having a presence on this instance, with some useful informations.
- **Add Organisation:**
- **List Roles:** List, modify or delete currently existing [roles](#).
- **Add Role:** Create a new role group for the users of this instance, controlling their privileges to create, modify, delete and to publish events and to access certain features such as the logs or automation.
- **Server Settings & Maintenance:** Various tools, upgrade scripts that can help a site-admin run the instance & Set up and diagnose your MISP installation.
- **Jobs:** View the background jobs and their progress
- **Scheduled Tasks:** Schedule the pre-defined tasks for your instance (this currently includes export caching, server [pull](#) and server [push](#)).
- **Blacklist Event:** Link to form where you can quickly add an event to a blacklist with its UUID.
- **Manage Event Blacklists:** List of blacklisted events on [MISP instance](#).
- **Blacklists Organisation:** Link to for where you can quickly add an organisation to a blacklist with its UUID.
- **Manage Org Blacklists:** List of blacklisted Organisations on this instance.

## Audit



- **List Logs:** View the logs of the instance.
- **Search Logs:** Search the logs by various attributes.

## The left bar

This bar changes based on each page-group. The blue selection shows you what page you are on.

Last modified: Wed Aug 19 2020 10:27:11 GMT+0200 (CEST)

- [General Concepts](#)
  - [Admins and Site Admins](#)
  - [Background Jobs](#)
  - [MISP Instance](#)
  - [Organisation administrators and Site administrators](#)
  - [Pivot path](#)
  - [Pivoting](#)
  - [Proposals](#)
  - [Publishing](#)
  - [Pull](#)
  - [Push](#)
  - [Scheduled Tasks](#)
  - [Sync User](#)
  - [Synchronisation](#)
  - [Tagging](#)
  - [Templating](#)

## General Concepts

### Admins and Site Admins

There are two types of admins in MISP: Admins (also referred to as org admins) and Site Admins. Whilst the former can only do some limited administration of users of his/her own organisation, site admins have access to all of the features and data of the system. They are in charge of making sure that the system runs correctly and the maintenance of MISP.

### Background Jobs

A lot of the heavier tasks are a burden to users, in that their actions can cause long delays (and in some cases timeouts) while the application logic is executing. To alleviate this, long processes have been (if enabled) moved to background jobs, meaning that their execution happens asynchronously in the background, allowing the user to freely interact with the platform whilst the request is being processed.

### MISP Instance

A [MISP instance](#) is an installation of the MISP software and the connected database. All the data visible to the users is stored locally in the database and data that is shareable (based on the distribution settings) can be synchronised with other instances via the Sync actions. The instance that you are reading this manual on will be referred to as "this instance" or "your instance". The instances that your instance synchronises with will be referred to as "remote instances".

### Organisation administrators and Site administrators

We have two types of administrators, site and organisation admins. The former has access to every administrator feature for all the data located on the system including global features such as the creation and modification of user [roles](#) and instance links, whilst organisation admins can administer users, events and logs of their own respective organisations.

### Pivot path

The (branching) path taken by a user from event to event while following correlation links. This is represented by the branching graph in the event view.

## Pivoting

The act of navigating from event to event through correlation links.

## Proposals

Each event can only be directly edited by users of the original creator organisation (and site admins). However, if another organisation would like to amend an event with extra information on an event, or if they'd like to correct a mistake in an attribute, they can create a Proposal. These [proposals](#) could then be accepted by the original creator organisation. These [proposals](#) can be pulled to another server, allowing users on connected instances to propose changes which then could be accepted by the original creators on another instance (and subsequently pushed back).

## Publishing

When an event is first created by a user, it is visible to everyone on the instance based on the access rights ("Your organisation only" events will not be visible to users of other organisations), but they will not be synchronised and they won't be exportable. For this, a user with [publishing](#) permission of the organisation that created the event has to publish the event. The system will then inform all the users of the instance that are subscribing to e-mail notifications and who have access to view the published event via an e-mail.

## Pull

Pulling is the process of using the configured [sync user](#) on a remote instance to REST GET all of the accessible data (based on the distribution rights) to your instance and store it.

## Push

Pushing is the process of using a configured instance link to send an event or all accessible events (limited by the distribution rights) through the REST interface to a remote instance.

## Scheduled Tasks

Certain common tasks can be scheduled for a later execution or for regular recurring executions. These tasks currently include caching all of the export formats, pulling from all eligible instances and pushing to all eligible instances.

## Sync User

A user of a role that grants sync permissions, these users (and their authentication keys) are used to serve as the points of connection between instances. Events pushed to an instance are pushed to a [sync user](#), who then creates the events on the remote instance. Events pulled are added by the [sync user](#) that is used to connect the remote instance to your instance. As an administrator, keep in mind that a [sync user](#) needs auth key and publish permissions, has to have undergone the mandatory password change and has to have accepted the Terms of Use in order for the sync to work. Please make sure that all of these steps are taken before attempting to [push](#) or [pull](#).

## Synchronisation

What we call [synchronisation](#) is an exchange of data between two (or more) MISP instances through our [pull](#) and [push](#) mechanisms.

## Tagging

Users with [tagging](#) rights can assign various dynamically created tags to events, allowing an arbitrary link between events to be created. It is possible to filter events based on these tags and they can also be used to filter events for the automation.

## **Templating**

Users with [templating](#) rights can create easy to fill forms that help with the event creation process.

Last modified: Fri May 11 2018 11:59:48 GMT+0200 (CEST)

- [User Management and Global Actions](#)
  - [First run of the system](#)

## User Management and Global Actions

### First run of the system

When first logging into MISP with the username and password provided by your administrator, there are a number of things that need to be done, before you can start using the system.

- **Accepting the Terms of use:** The terms of use are shown immediately after logging in for the first time, make sure to read through this page before clicking "Accept Terms" at the bottom of the page.
- **Changing the password:** After accepting the ToU, you'll be prompted to change your password, but keep in mind that it has to be pass to the [MISP password policy](#). Enter the same password into the confirm password field, before clicking submit to finalise the change.

The screenshot shows a 'Change Password' form. At the top, the title 'Change Password' is displayed. Below the title, there are two input fields: 'Password' and 'Confirm Password'. Both fields contain the placeholder text 'Enter password'. A blue 'Submit' button is positioned at the bottom of the form.

- **Setting up the GnuPG Key:** In order for the system to be able to encrypt the messages that you send through it, it needs to know your GnuPG key. Navigate to the Edit profile view (My Profile on the left -> Edit profile in the top right corner). Paste the key into the GnuPG Key field and click submit.
- **Subscribing to Auto-alerts:** Turning auto-alerts on will allow the system to send you e-mail notifications about any new public events entered into the system by other users and private events added by members of your organisation. To turn this on, navigate to the Edit profile view (My profile on the left navigation menu -> Edit profile in the top right corner). Tick the auto-alert checkbox and click submit to enable this feature.

The screenshot shows a portion of a web interface for editing a user profile. At the top, there's a navigation bar with icons for user management, global actions, and help. Below that, a sidebar on the left lists 'My Profile', 'Edit profile', 'Logout', and 'Help'. The main content area has a title 'Edit profile' and a sub-section titled 'Auto-alerts'. This section contains two checkboxes: one for receiving alerts when events are published and another for receiving alerts from 'contact reporter' requests. A blue 'Submit' button is located at the bottom of this form.

Receive alerts when events are published

Receive alerts from "contact reporter" requests

**Submit**

- **Subscribing to e-mails sent via the "Contact Reporter" functionality:** This feature is turned on right below the autoalerts and will allow you to receive e-mails addressed to your organisation whenever a user tries to ask about an event that was posted by a user of your organisation. Keep in mind that you can still be addressed by such a request even when this setting is turned off, if someone tries to contact you as the event creator directly or your organisation for an event that you personally have created then you will be notified.
- **Reviewing the Terms & Conditions:** To review the Terms & Conditions or to read the User Guide, use the appropriate button on the left navigation menu.
- **Making sure that compatibility mode is turned off (IE9&IE10):** Compatibility mode can cause some elements to appear differently than intended or not appear at all. Make sure you have this option turned off.

Last modified: Wed Aug 19 2020 10:27:11 GMT+0200 (CEST)

- [Using the system](#)
  - [Creating an event](#)
  - [Add attributes to the event](#)
  - [Add Attribute](#)
  - [Add Object](#)
  - [Create and manage Sharing Groups](#)
  - [Populate from Template](#)
  - [Freetext Import Tool](#)
  - [Attribute Replace Tool](#)
  - [Add attachments to the event](#)
  - [Propose a change to an event that belongs to another organisation](#)
  - [Populate from OpenIOC](#)
  - [Populate from ThreatConnect](#)
  - [Adding IOCs from a PDF report](#)
  - [Publish an event](#)
- [Browsing past events](#)
  - [To list all events](#)
  - [Filters](#)
  - [Event view](#)
  - [Event History](#)
  - [Listing all attributes](#)
  - [Searching for attributes](#)
- [Updating and modifying events and attributes](#)
- [Tagging](#)
- [Templating](#)
- [Contacting the reporter](#)
- [Automation](#)
- [Exporting data](#)
  - [Export page with background jobs disabled](#)
  - [Export page with background jobs enabled](#)
  - [Exporting search results and individual events](#)
- [Connecting to other instances](#)
  - [Setting up a connection to another server](#)
  - [Browsing the currently set up server connections and interacting with them](#)
- [Rest API](#)
  - [Requests](#)
  - [Example - Get single Event](#)
    - [Example - Add new Event](#)

## Using the system

### Creating an event

The process of entering an event can be split into 3 phases, the creation of the event itself, populating it with attributes and attachments and finally [publishing](#) it.

During this first step, you will create a basic event without any actual attributes, but storing general information such as a description, time and risk level of the incident. To start creating the event, click on the New Event button on the left and fill out the form you are presented with. The following fields need to be filled out:

## Add Event

Date	Distribution
<input type="text"/>	<input type="button" value="All communities"/>
Threat Level	Analysis
<input type="button" value="High"/>	<input type="button" value="Initial"/>
Event Description	
<input type="text" value="Quick Event Description or Tracking Info"/>	
GFI sandbox	
<input type="button" value="Choose File"/> No file chosen	
<input type="button" value="Add"/>	

- **Date:** The date when the incident has happened. Just click this field and a date-picker will pop up where you can select the desired date.
- **Distribution:** This setting controls, who will be able to see this event once it becomes published and eventually when it becomes pulled. Apart from being able to set which users on this server are allowed to see the event, this also controls whether the event will be synchronised to other servers or not. The distribution is inherited by attributes: the most restrictive setting wins. The following options are available:
  - **Your organization only:** This setting will only allow members of your organisation to see this. It can be pulled to another instance by one of your organisation members where only your organisation will be able to see it. Events with this setting will not be synchronised. Upon [push](#): do not [push](#). Upon [pull : pull](#).
  - **This Community-only:** Users that are part of your MISP community will be able to see the event. This includes your own organisation, organisations on this MISP server and organisations running MISP servers that synchronise with this server. Any other organisations connected to such linked servers will be restricted from seeing the event. Upon [push](#): do not [push](#). Upon [pull: pull](#) and downgrade to Your organization only.
  - **Connected communities:** Users that are part of your MISP community will be able to see the event. This includes all organisations on this MISP server, all organisations on MISP servers synchronising with this server and the hosting organisations of servers that connect to those afore mentioned servers (so basically any server that is 2 hops away from this one). Any other organisations connected to linked servers that are 2 hops away from this own will be restricted from seeing the event. Upon [push](#): downgrade to This Community only and [push](#). Upon [pull: pull](#) and downgrade to This Community only.
  - **All communities:** This will share the event with all MISP communities, allowing the event to be freely propagated from one server to the next. Upon [push: push](#). Upon [pull: pull](#).
  - **Sharing group:** This will share the event to the defined sharing group. This includes only the organisations defined in the sharing group. The distribution can be local and cross-instance depending of the sharing group definition. For more information on [sharing groups](#), refer to the sharing group section.
- **Threat Level:** This field indicates the risk level of the event. Incidents can be categorised into three different threat categories (low, medium, high). This field can alternatively be left as undefined. The 3 options are:
  - **Low:** General mass malware.
  - **Medium:** Advanced Persistent Threats (APT)
  - **High:** Sophisticated APTs and 0day attacks.
- **Analysis:** Indicates the current stage of the analysis for the event, with the following possible options:
  - **Initial:** The analysis is just beginning
  - **Ongoing:** The analysis is in progress
  - **Completed:** The analysis is complete
- **Event Description:** The info field, where the malware/incident can get a brief description starting with the internal reference. This field should be as brief and concise as possible, the more detailed description happens through attributes in the next stage of the event's creation. Keep in mind that the system will automatically replace detected text strings that match a regular expression entry set up by your server's administrator(s).
- **GFI Sandbox:** It is possible to upload the exported .zip file from GFI sandbox with the help of this tool. These will be dissected by the MISP and a list of attributes and attachments will automatically be generated from the .zip file. Whilst this does most of the work needed to be done in the second step of the event's creation, it is important to manually look over all the data that is being entered.

## Add attributes to the event

The second step of creating an event is to populate it with attributes and attachments. This can be done by adding them manually or importing the attributes from an external format (OpenIOC, ThreatConnect). To import from an external format or to upload an attachment use the options in the menu on the left.

The screenshot shows a user interface for managing attributes. At the top left, there are three buttons: 'Add Attribute' (with a plus sign), 'Edit Selected Attributes' (with a pencil icon), and 'Delete Selected Attributes' (with a trash bin icon). At the top right, there are three buttons: 'Populate from Template' (with a document icon), 'Free-text Import Tool' (with a magnifying glass icon), and 'Attribute Replace Tool' (with a circular arrow icon). Below these buttons is a table with four columns: 'Date', 'Category', 'Type', and 'Value'. The table contains one row with the following data: Date: 2014-10-15, Category: Network activity, Type: in-det, Value: 5 5 5 52.

Date	Category	Type	Value
2014-10-15	Network activity	in-det	5 5 5 52

Using the above shown buttons, you can populate an event using various tools that will be explained in the following section. Let's start with the Add Attribute button.

## Add Attribute

Keep in mind that the system searches for regular expressions in the value field of all attributes when entered, replacing detected strings within it as set up by the server's administrator (for example to enforce standardised capitalisation in paths for event correlation or to bring exact paths to a standardised format). The following fields need to be filled out:

### Add Attribute

Category	Type	Distribution
Network activity	url	All communities
Value		
<input type="text" value="http://www.teamliquid.net"/>		
Contextual Comment		
<input type="text"/>		
<input checked="" type="checkbox"/> for Intrusion Detection System <input type="checkbox"/> Batch Import		
<input type="button" value="Submit"/>		

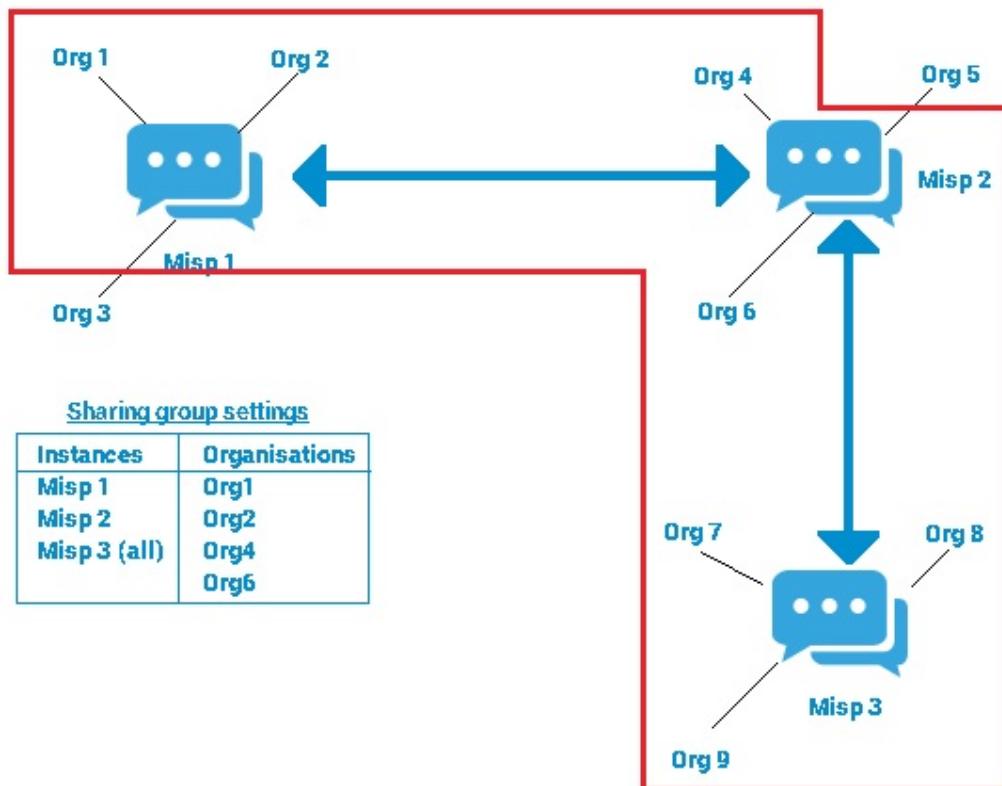
- **Category:** This drop-down menu explains the category of the attribute, meaning what aspect of the malware this attribute is describing. This could mean the persistence mechanisms of the malware or network activity, etc. For a list of valid categories, [click here](#)
- **Type:** Whilst categories determine what aspect of an event they are describing, the Type explains by what means that aspect is being described. As an example, the source IP address of an attack, a source e-mail address or a file sent through an attachment can all describe the payload delivery of a malware. These would be the types of attributes with the category of payload deliver. For an explanation of what each of the types looks like together with the valid combinations of categories and types, [click here](#)
- **Distribution:** This drop-down list allows you to control who will be able to see this attribute. The distribution is inherited by attributes: the most restrictive setting wins. For more info, read the distribution information in the creating an event section - [click here](#)
- **Value:** The actual value of the attribute, enter data about the value based on what is valid for the chosen attribute type. For example, for an attribute of type ip-src (source IP address), 11.11.11.11 would be a valid value. For more information on types and values, [click here](#)
- **Contextual Comment:** You can add some comments to the attribute that will not be used for correlation but instead serves as purely an informational field.
- **For Intrusion Detection System:** This option allows the attribute to be used as an IDS signature when exporting the [NIDS](#) data, unless it is being overruled by the white-list. For more information about the white-list, head over to the [administration](#) section. If the IDS flag is not set, the attribute is considered as contextual information and not to be used for automatic detection.
- **Batch import:** If there are several attributes of the same type to enter (such as a list of IP addresses, it is possible to enter them all into the same value-field, separated by a line break between each line. This will allow the system to create separate lines for each attribute.

## Add Object

Please have a look at the [MISP-objects chapter](#)

## Create and manage Sharing Groups

[Sharing groups](#) in MISP are a more granular way to create re-usable distribution lists for events/attributes that allow users to include organisations from their own instance (local organisations) as well as organisations from directly, or indirectly connected instances (external organisations). [Sharing groups](#) can be created by any user that has the sharing group editor permission. Additionally, [sharing groups](#) can be edited by any user that has the aforementioned permission in addition to being a member of the sharing group's creating organisation, or any organisation that is marked as an "extender" of the sharing group. The main use for the extend feature is delegating the rights to add users to trusted partners. For example, when sharing with a different industry sector, knowing all actors that should receive the information is often not possible, so delegating the rights to extend the event to a trusted representative of said sector would allow for someone with more insight to find and add the proper list of partners for the sharing group.



The most general use-cases for [sharing groups](#) are creating re-usable topical subgroups in MISP that share events or for ad-hoc sharing scenarios (such as several organisations involved in a specific incident wanting to work together). Generally [sharing groups](#) add a level of complexity for the users involved as well as a performance overhead on the data marked with it.

As a best-practice recommendation, using traditional distribution methods is preferred unless they cannot cover the given use-case. Also, whilst [sharing groups](#) can be assigned to both events and attributes, it is highly recommended to use the special "inherit" distribution setting on attributes whenever the attribute's sharing group would match the event's.

[Sharing groups](#) consist of the following elements, each of which has its own page in the sharing group creator/editor tool (accessed via the Global actions -> List [Sharing Groups](#) and Add Sharing Group functionalities):

## New Sharing Group

General    Organisations    MISP Instances    Summary and Save

Name  
Financial Sector

Releasable to  
Financial Sector organisations

Description  
A general sharing group for the financial sector including financial sector actors like banks, insurance companies or payment processing companies.

Make the sharing group selectable (active)

**Next page**

- **General:** Metadata describing the intent of the sharing group
  - **Name:** The unique name of the sharing group.
  - **Releasable to:** A human-readable description of who data marked with the sharing group is shareable with. This field is NOT used by MISP for anything besides for being an informational field aimed at extender organisations of the sharing group.
  - **Description:** A natural-text representation of the intent of the sharing group.
  - **Make the sharing group selectable (active):** A sharing group can be made passive by unchecking this setting. All events and attributes will continue to adhere to a passive sharing group's distribution setting, however, the sharing group will not be offered as a selectable option when setting the distribution of events/attributes. The idea behind this is that ad-hoc [sharing groups](#) that have outlived their purpose can be retired in order to reduce the clutter in the UI.

## New Sharing Group

Type	Name	UUID	Extend	Actions
local	Org221		<input checked="" type="checkbox"/>	
remote	CIRCL		<input type="checkbox"/>	<span>trash</span>
remote	CthulhuSPRL.be		<input type="checkbox"/>	<span>trash</span>

[Previous page](#) [Next page](#)

- **Organisations:** The second page of the tool contains the distribution list containing all organisations directly named as a member of the sharing group
  - **Add Local/remote organisations:** The organisations are split into two lists (shown as two tabs in the tool) for local and known remote/external organisations. Local organisations are expected to have at least one local user on the instance whilst remote organisations do not. Synchronising with remote instances will create remote organisations whenever a new event is received of a yet unknown organisation. Remote organisations can always be converted to local organisations - this becomes interesting if a user of an external organisation requests access to your MISP instance.
  - **Extend checkmark:** Checking the extend checkmark makes the selected organisation an extender of the sharing group, meaning they can edit the sharing group. It is expected of these trusted partners that they adhere to the "releasable to" tag set on the general page. The organisation creating the sharing group is always included as an extender.

## New Sharing Group

General    Organisations    **MISP Instances**    Summary and Save

**Enable roaming mode** for this sharing group (pass the event to any connected instance where the sync connection is tied to an organisation contained in the SG organisation list).

Add instance

Name	URL	All orgs	Actions
Local instance	http://192.168.56.101	<input checked="" type="checkbox"/>	
other	http://192.168.56.105	<input type="checkbox"/>	

[Previous page](#) [Next page](#)

- **Servers:** The third page of the tool describes the MISP instances the data marked with the given sharing group are allowed to be synchronised with. Keep in mind that any user that can view an event on a given instance will have the right to **pull** the event to their home instance, as they are part of the sharing group, however the organisation distribution list will still apply.
  - **Enable roaming mode:** This setting will disable the server list and rely purely on the organisation list to distribute the data. If a sync connection's host organisation is in the organisation distribution list the instance becomes eligible for synchronising the data marked with the sharing group. Generally this carries a slightly higher risk as it relies on administrators correctly setting up the host organisation settings, but it removes the need to know the specific instance urls where the event/attribute should flow.
  - **Add instance:** Add an instance to the distribution list from the sync instances set up under sync actions -> servers
  - **All orgs:** Checking this checkbox will automatically include all organisations on the given instance in the sharing group. This means that in order to exchange with all users of a linked community, one does not need to know every organisation residing on the instance. This also means that the distribution list will not include the organisation names, which can be interesting for certain privacy sensitive communities.

## New Sharing Group

General    Organisations    MISP Instances    **Summary and Save**

**General:** You are about to create the **Financial Sector** sharing group, which is intended to be releasable to **Financial Sector organisations**.

**Local organisations:** It will be visible to **all organisations on this instance**, from which **Org221** can extend the sharing group.

**External organisations:** It will also be visible to **CIRCL, CthulhuSPRL.be**, out of which **nobody** can extend the sharing group.

**Synchronisation:** Furthermore, events are automatically pushed to: **other**

You can edit this information by going back to one of the previous pages, or if you agree with the above mentioned information, click Submit to create the Sharing group.

**Previous page**    **Submit**

- **Summary:** Once everything is set up, MISP will summarise the sharing group in a highlighted text page, which is highly advised to be reviewed before submitting the new sharing group/editing the sharing group. Mistakes in the sharing group settings can lead to organisations that should not be involved in the sharing group getting access or organisations receiving unwanted editing rights to the sharing group. Keep in mind that even if you have submitted a sharing group, it is not propagated until an event/attribute receives the sharing group as the selected distribution.

## Populate from Template

Templates allow users to rapidly populate events of a specific type by filling out a series of pre-defined fields. Users with template creation privileges can create new templates for their organisations or for all organisations on their instance. If you are interested in template creation, please refer to the [templating](#) section. For users trying to populate an event, after clicking on the populate from template button, you'll be presented with a list of all currently accessible templates. Pick the one that best describes the event that you are creating.



Once you have chosen a template, you'll be presented with the actual form contained within. Make sure you fill out as many fields as possible with the mandatory fields - marked by a star in a bracket such as this: (\*) - are filled out. Templates are divided into sections, with each section having a title and a description in addition to a series of fields. Each field can be an attribute or a file attachment field. An attribute field has the following components:

**Dropped Artifacts**

Describe any dropped artifacts that you have encountered during your analysis

<b>Field:</b>	Artifacts Dropped (File) (*)
<b>Description:</b>	Insert any data you have on dropped files here.
<b>Types:</b>	<input type="button" value="filename"/> <input type="button" value="filenameMd5"/> <input type="button" value="filenameSha1"/> <input type="button" value="filenameSha256"/> <input type="button" value="md5"/> <input type="button" value="sha1"/> <input type="button" value="sha256"/>

Describe the Artifacts Dropped (File) using one or several (separated by a line-break) of the following types: filename

- **Field:** The name of the field along with an indication if the field is mandatory.
- **Description:** A short description of the field.
- **Types:** The value(s) that are valid for the field. In the case of several types being shown here, you can enter value(s) matching any one of the types, or in the case of a batch import field, any mixture of the given types.
- **Text field:** This field can either be a single linetextfield or a multi-line text area. For the former, enter a single value of the above indicated type, whilst for the latter you can paste a list of values separated by line-breaks.

## Freetext Import Tool

The screenshot shows a modal window titled "Freetext Import Tool". Inside the window, there is a text input field with the placeholder text "Paste a list of IOCs into the field below for automatic detection.". Below the input field are two buttons: "Submit" on the left and "Cancel" on the right.

If you have a list of [indicators](#) that you would like to quickly generate attributes out of then the Free-text import tool is just what you need. Simply paste a list of [indicators](#) (separated by line-breaks) into this tool.

## Freetext Import Results

Below you can see the attributes that are to be created based on the results of the free-text import. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

Value	Category	Type	IDS	Actions
192.168.0.1	Network activity	ip-dst	<input checked="" type="checkbox"/>	
domain.hostname.com	Network activity	hostname	<input checked="" type="checkbox"/>	
chrome.exe	Payload delivery	filename	<input checked="" type="checkbox"/>	

 Submit

Since there are several category / type combinations that can be valid for a lot of values, MISP will suggest the most common settings. You can alter the category / type / IDS fields manually if you disagree with the results. The options will be restricted to valid category/type combinations for the value that you have entered.

If any correlation is already found, these correlations will be displayed in the result page.

## Attribute Replace Tool

If you would like to create and maintain an event with a set of [indicators](#) that receives removals and additions over time, then the attribute replace tool might make this task easier for you.

The screenshot shows a web-based application window titled "Attribute Replace Tool". The interface includes a descriptive text box at the top, two dropdown menus for "Category" and "Type", a checked checkbox for marking new attributes as IDS, and a text input field for pasting values.

Choose a category and a type, then paste a list of IOCs that match the selection into the field below. This will delete all of the attributes not found in the new inserted list, whilst creating the attributes that are in the new list but don't exist as attributes. Found matches will be left untouched.

Category	Type
Network activity	ip-dst

Mark all new attributes as to IDS

Values

```
5.6.7.8  
8.7.6.5
```

Simply select the desired category / type combination, choose whether the attributes should be marked for IDS exports and paste the new list of [indicators](#) into the textarea. Attributes of the same category/type that are present in the event but not the new list will be removed, values in the pasted list that do not yet exist as attributes will be created as attributes and values that already have matching attributes will be left untouched.

## Add attachments to the event

You can also upload attachments, such as the malware itself, report files from external analysis or simply artifacts dropped by the malware. Clicking on the add attachment button brings up a form that allows you to quickly attach a file to the event. The following fields need to be filled out:

### Add Attachment

---

#### Category

#### Distribution

#### Contextual Comment

[Choose File](#)

No file chosen

Malware

[Upload](#)

- **Category:** The category is the same as with the attributes, it answers the question of what the uploaded file is meant to describe.
- **Distribution:** This drop-down list allows you to control who will be able to see this attachment. The distribution is inherited by attributes: the most restrictive setting wins. For more info, refer to the distribution information in the [event section](#).
- **Upload field:** By hitting browse, you can browse your file system and point the uploader to the file that you want to attach to the attribute. This will then be uploaded when the upload button is pushed.
- **Malware:** This check-box marks the file as malware and as such it will be zipped and passworded, to protect the users of the system from accidentally downloading and executing the file. Make sure to tick this if you suspect that the file is infected, before uploading it.
- **Contextual Comment:** You can add some comments to the attribute that will not be used for correlation but instead serves as purely an informational field.

## Propose a change to an event that belongs to another organisation

If you would like to propose a modification to an attribute, or to propose some additional attributes to the creating organisation, you can do this with the buttons that replace the add attribute field on the left and the edit icon on the right end of each listed attribute in the event view. The creating organisation of the event will be able to see any [proposals](#) and discard or accept the changes.

Network activity	id-src	1.1.1.34	Yes	Connected communities	
		1.1.1.253			

If the organisation that has created the event is on another connected server, they will be able to accept the proposal once they initiate a [pull](#) and receive your proposal. After this they can republish the event, sending the altered attribute back to your instance.

## Populate from OpenIOC

It is also possible to attempt to import the data contained in a [.ioc](#) file. The import tool will attempt to gather as many IndicatorItems within nested logical operators as possible without breaking their validity. After the procedure is done, you'll be presented with a list of successfully created attributes and a list of failed IndicatorItems as well as a graph of the [.ioc](#) file.

**13 attributes created successfully, 6 indicators could not be mapped and saved.**

**Successfully added attributes:**

Uuid	Category	Type	Value
b9ef2559-cc59-4463-81d9-52800545e16e	Other	other	FileItem/PEInfo/Sections/Section/Name:.stub
156bc4b6-a2a1-4736-bfe8-6c8d1f7eae38	Payload installation	filename	mdmcop3.PNF
e57d9a5b-5e6a-41ec-87c8-ee67f3ed2e20	Payload installation	filename	mdmeric3.PNF
A2A7BeeF-1bR7E-AHAA-L2H2Q-1cRaee576RAF	Device/Installation	filename	memRC.DMF

### Visualisation:

```
|_OR
  |_FileItem/PEInfo/Sections/Section/Name:contains:.stub
  |_FileItem/FileName:contains: mdmcp03.PNF
  |_FileItem/FileName:contains: momeric3.PNF
  |_FileItem/FileName:contains: oem6C.PNF
  |_FileItem/FileName:contains: oem7A.PNF
  |_AND
    |_DriverItem/DeviceItem/AttachedToDriverName:contains: fs_ec.sys
    |_DriverItem/DeviceItem/AttachedToDriverName:contains: mxsmb.sys
    |_DriverItem/DeviceItem/AttachedToDriverName:contains: sr.sys
    |_DriverItem/DeviceItem/AttachedToDriverName:contains: fastfets.sys
  |_AND
    |_FileItem/FileName:contains: mxcls.sys
    |_FileItem/PEInfo/DigitalSignature/CertificateSubject:contains: Realtek Semiconductor Corp
  |_AND
    |_FileItem/FileName:contains: mxnet.sys
    |_FileItem/PEInfo/DigitalSignature/CertificateSubject:contains: Realtek Semiconductor Corp
  |_AND
    |_RegistryItem/Path:contains: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxCl\ImagePath
    |_RegistryItem/Text:contains: mxcls.sys
  |_AND
    |_RegistryItem/Path:contains: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxNet\ImagePath
    |_RegistryItem/Text:contains: mxnet.sys
```

## Populate from ThreatConnect

You can also import the data from a ThreatConnect export csv file. The following columns are used by the import tool (and are thus mandatory fields to select during the export):

- Type
- Value
- Confidence
- Description
- Source

The result will be a list of attributes that get added to the currently selected event, each of which will be marked with a comment that indicates that its origin being from a ThreatConnect import.

## Adding IOCs from a PDF report

You can use a generic script called [IOC parser](#) or use a script published by Palo Alto to convert [IOC](#) parser output to a [MISP event](#): [report\_to\_misp] ([https://github.com/PaloAltoNetworks-BD/report\\_to\\_misp/](https://github.com/PaloAltoNetworks-BD/report_to_misp/)).

## Publish an event



Once all the attributes and attachments that you want to include with the event are uploaded / set, it is time to finalise its creation by [publishing](#) the event (click on publish event in the event view). This will alert the eligible users of it (based on the private-controls of the event and its attributes/attachments and whether they have auto-alert turned on), [push](#) the event to instances that your instance connects to and propagate it further based on the distribution rules. It also readies the network related attributes for [NIDS](#) signature creation (through the [NIDS](#) signature export feature, for more information, go to the export section.). There is an alternate way of [publishing](#) an event without alerting any other users, by using the "publish (no email)" button. This should only be used for minor edits (such as correcting a typo).

If your instance has background jobs enabled then the event might not get published immediately.

## Browsing past events

The MISP interface allows the user to have an overview over or to search for events and attributes of events that are already stored in the system in various ways.

### To list all events

On the left menu bar, the option "List events" will generate a list of the last 60 events. While the attributes themselves aren't shown in this view, the following pieces of information can be seen:

#### Events

		Datefrom : 2014-03-04 Dateuntil : 2014-03-05 org : ADMIN										
		Published	Org	ID	Tags	#Attr.	Date	Threat Level	Analysis	Info	Distribution	Actions
		✓	ADMIN	3		4	2014-03-05	High	Initial	Test Event 3	All	
		✓	ADMIN	2		1	2014-03-05	High	Initial	Test Event 2	All	
		✓	ADMIN	1		1	2014-03-05	Low	Completed	Test Event 1	All	

- **Published:** Already published events are marked by a checkmark. Unpublished events are marked by a cross.
- **Org:** The organisation that created the event.
- **Owner Org:** The organisation that owns the event on this instance. This field is only visible to administrators.
- **ID:** The event's ID number, assigned by the system when the event was first entered (or in the case of an event that was synchronized, when it was first copied over - more on [synchronisation](#) in chapter xy)
- **Tags:** Tags that are assigned to this event.
- **#Attr.:** The number of attributes that the event has.
- **Email:** The e-mail address of the event's reporter. This is not visible to regular users. Organisation administrators can see the e-mail addresses of their own organisation's users.
- **Date:** The date of the attack.
- **Threat Level:** The risk level of the attack, the following levels are possible:
  - **Low:** General Malware
  - **Medium:** Advanced Persistent Threats (APTs)
  - **High:** Sophisticated APTs and 0day exploits
  - **Undefined:** This field can be left undefined and edited at a later date.
- **Analysis:** Indicates the current stage of the analysis for the event, with the following possible options:
  - **Initial:** The analysis is just beginning
  - **Ongoing:** The analysis is in progress
  - **Completed:** The analysis is complete
- **Info:** A short description of the event, starting with an internal reference number.
- **Distribution:** This field indicates what the sharing privileges of the event. For details, refer to the distribution information in the [event section](#).
- **Actions:** The controls that the user has to view or modify the event. The possible actions that are available (depending on user privileges - [click here](#) to find out more about privileges):
  - **Publish:** Publishing an event will have several effects: The system will e-mail all eligible users that have auto-alert turned on (and having the needed privileges for the event, depending on its private classification) with a description of your newly published event, it will be flagged as published and it will be pushed to all eligible servers (to read more about [synchronisation](#) between servers, have a look at the [section on connecting servers](#))
  - **Edit:** Clicking on the edit button will bring up the same screen as the one used for creating new events, with the exception that all fields come filled out with the data of the event that is being edited. The distribution of an event can only be edited if you are a user of the creating organisation of the event. For more information on this view, refer to the section on [creating an event](#).
  - **Delete:** The system will prompt you before erasing the unwanted event.
  - **View:** Will bring up the event view, which besides the basic information contained in the event list, will also include the following:

## Filters

It is also possible to filter the events shown by clicking on the small magnifying glass icons next to the field names and entering a filter term.

## Event view



## Test Event 3

Event ID	3	Related Events
Uuid	53174081-1d0c-41be-9bd9-4f1ec0a80e0a	2014-03-05 (1) 2014-03-05 (2) 2014-02-21 (4)
Org	ADMIN	
Contributors	argh	
Tags	test <span style="color: red;">x</span> <span style="color: green;">+</span>	
Date	2014-03-05	
Threat Level	High	
Analysis	Initial	
Distribution	All communities, this will share the event with all MISP communities, allowing the event to be freely propagated from one server to the next.	
Description	Test Event 3	
Published	Yes	

— Pivots — Attributes — Discussion

X 3: Test Ev...

Date	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2014-03-05	Network activity	ip-src	1.1.1.1	An IP address	2.1	Yes	All	<input checked="" type="checkbox"/>
2014-03-05		ip-src	2.2.2.2	An IP address		Yes	All	<input checked="" type="checkbox"/>
			2.2.2.3	An IP address				
2014-03-05		ip-src	3.3.3.3	An IP address	4	Yes	All	<input checked="" type="checkbox"/>

## General Event Information

- **ID:** The ID of the event.
- **Uuid:** In order to avoid collisions between events and attributes (during for example a sync) a Uuid is assigned that uniquely identifies each of them.
- **Org** The organisation that has originally created the event. The logo (if it exists on the server, alternatively a string) representing the organisation is also shown in the right upper corner.
- **Contributors:** Shows a list of the organisations that have contributed to the event via [proposals](#). If you click any of the logos listed here, you'll get redirected to a filtered event history view, including only the changes made by the organisation.
- **Tags:** A list of tags associated with the event. Clicking a tag will show a list of events with the same tag attached. The little cross next to each tag allows you to remove the tag from the event, whilst the '+' button allows you to assign a tag. For the latter two options to be visible, you have to have [tagging](#) permission.
- **Date:** The date of detection, set by the user that creates the event, not to be confused with the creation date of the event.
- **Threat Level:** The assigned threat level of the event.
- **Analysis:** The status of the analysis.
- **Distribution:** This shows the distribution rules applied to this event, controlling whether only the creating organisation can see (Your organisation only) it or everyone on the instance (This community only). The two remaining settings allow the event to be propagated to organisations on remote connected instances.
- **Info:** A short description of the event itself. Make sure not to put information in here that could be used for correlation purposes and be better suited as an Attribute.
- **Published:** Whether the event has been published or not. [Publishing](#) allows the attributes of the event to be used for all eligible exports and it notifies users that have subscribed to the event alerts. Also, a publish initiates a [push](#) to all eligible instances.

**List of Related Events** The list of relations is shown on the right hand side of the general event information. Events can be related by having one or more attributes that are exact matches. For example, if two events both contain a source IP attribute of 11.11.11.11 then they are related. The list of events that are related to the currently shown one, are listed under "Related Events", as links (titled the related event's date and ID number) to the events themselves.

**Data Element Toggles** You can control some of the data that is shown on this page using three toggles. The elements that can be disabled are the pivot threads, the attributes (and [proposals](#)) and the Discussions. You can collapse these elements and then expand them again using the same button.

**Pivot Threads** While moving from event to event through the relation links (a process that we refer to as [pivoting](#)), you create a path that shows which events you have traversed. This path is reset by leaving the event view and navigating elsewhere in the application or by deleting the root pivot element. Each event visited is represented by a bubble in the pivot thread graph, connected by lines that show how the user has arrived at the next connected event. It is possible to jump back to an earlier relation and pivot to another event through that, creating branches in the graph. The currently selected event is coloured blue in the graph. If you would like to delete an element from the graph (including all of elements that branch off of it) just click on the small x within a pivot bubble. For a deletion to be possible the following conditions have to be met:

- The pivot element to be deleted cannot be on the path that leads to the currently selected event
- The pivot element residing in the graph's root can always be deleted - this will simply reset the current pivot thread

**Attributes and Proposals** A list of all attributes and [proposals](#) attached to the event. The fields for each of them only differ in the available actions and the fact that for [proposals](#) to attributes all fields are blank that would stay unchanged if the proposal was accepted (for example, proposing a change to an attribute to turn the IDS flag on will have all fields apart from the IDS flag blank in the proposal). Here is a list of what each of the fields represents:

- **Date:** The date of the last modification to the attribute. [Proposals](#) don't have a date of last edit.
- **Category:** The category of the attribute or proposal. For a list of possible categories visit the section on [categories and types](#).
- **Type:** The type of the attribute or proposal. For a list of possible categories visit the section on [categories and types](#).

- **Value:** The value or value-pair of the attribute. This is the main payload of the attribute, which is described by the category and type columns. For certain types of attributes that are made up of value-pairs the two parts will be split by a pipe (), such as for filename|md5. The value field(s) are used by the correlation engine to find relations between events. In value-pair attributes both values are correlated individually.
- **Comment:** Attributes can have a contextual comment to further describe the attribute. These comments are not used for correlation and are purely informative.
- **Related Events:** A list of the event IDs that also contain an attribute with the same value.
- **IDS:** Flags an attribute as an indicator of compromise, allowing it to be included in all of the eligible exports.
- **Distribution:** Defines the distribution of the attribute individually. An attribute can have a different distribution level than the event. In any case, the lowest distribution level of the two is used.
- **Actions:** The user can interact with the events through these buttons, which will be further described in the next portion of the guide as they differ for attributes and [proposals](#).

Depending on the colour coding of the row, you can have an attribute, a proposal to the event or a proposal to an attribute:

- **Attributes:** Each uncoloured line represents an Attribute.
- **Proposals to an Event:** Each gray line at the end of the list represents a Proposal to an event. These are [proposals](#) for a new attribute, mostly unrelated to any of the currently existing attributes. If the creator of the event accepts one of these a new attribute will be created.
- **Proposals to an Attribute:** Each attribute can have several edit [proposals](#). These will be placed right below the attribute that the proposal affects and - as with the event [proposals](#) - is coloured grey. The original attribute's row is coloured blue if a proposal exists for it.

Using the modify button will bring up the attribute creation view, with all data filled out with the attribute's currently stored data.

### Event Discussion Thread

Each event has its own assigned discussion where users (that are eligible to see the event) can participate in an open discussion. The users are anonymised in the messages, all that other users will see is their user ID number and their organisation. To post a message on the Event Discussion, either use the reply button on a previous post or use the quickresponse field at the bottom of the page. Each post is made up of the following:

- **Date:** The date when the post was created.
- **Post navigation:** This should the post's ID as well as a link to jump to the top of the discussion thread on the page itself.
- **Organisation logo:** If such an image exists for the organisation that has posted the message, then the logo is shown.
- **Message:** The body of the post itself. This can also include automatically generated links to other events and threads as well as show quoted text in embedded bubbles. Editing an event will also append a post with a message indicating that it was edited together with the timestamp of the edit.
- **User:** The e-mail address of the poster if he/she is from the organisation as the current user. Alternatively a generated string is shown that includes the user ID of the user, so that his/her e-mail address could remain hidden whilst still being identifiable.
- **Action buttons:** Edit, Delete and Reply. The first two of the three options are only available to the poster of the message or a [site admin](#). Quoting a post will automatically include the original message in [quote] tags.

Here is a list of the various tools you can use while using this feature:

- **Pagination:** There are 5 posts visible on each event page, if there have been more messages posted, use the previous and next button to navigate through the thread. This will not reload the rest of the page.
- **Discussion Tags:** Users can quote something by encapsulating it in [quote][/quote] tags, they can create a link to another event with the [event][/event] tags or to another discussion thread with [thread][/thread].
- **Quick Post:** Adding a post will take the user to a separate add Post page, something that can be a bit of an inconvenience. To avoid this, there is a quick post button, where users can add messages on the fly without having to reload the page. On top of the quick post field, 3 buttons allow users to generate quote, event and thread tags quickly.

### Event History

---

View the logs of the event that show how the event has changed over time, including the contribution from other organisations in the form of [proposals](#). There are two ways to get to this view, either by clicking on View Event History on the side menu of an event view, or by clicking on a contributing organisation's logo on the event view. The latter will show a restricted form of the logs, showing only [Proposals](#) created by the selected organisation. The fields shown in this view are as described as follows:

- **Org:** The logo (or in the lack thereof a string representation) of the organisation.
- **Action:** Each entry in the log happens during an action, such as the creation, modification or deletion of data and some special actions (such as accepting a proposal). This field shows which action caused the entry to be created.
- **Model:** As described above, a log entry is generated on certain actions. This field shows which type of data was affected that caused the log entry to be created (such as a change to the event, the creation of an attribute, the discarding of a proposal, etc).
- **Title:** This is a short description of the change itself and it is not nearly as detailed as the information administrators get in the audit logs. However, for attributes and [proposals](#) the category / type and value of the created or edited attribute is shown.
- **Created:** The date and time of the log entry's creation.

## **Listing all attributes**

Apart from having a list of all the events, it is also possible to get a list of all the stored attributes in the system by clicking on the list attributes button. The produced list of attributes will include the following fields:

Event	Org	Category	Type	Value	Comment	IDS	Actions
5		Other	comment	asdasdasd		Yes	
4		Network activity	ip-src	2.2.2.2		Yes	
4		Network activity	ip-src	3.3.3.3		Yes	

- **Event:** This is the ID number of the event that the attribute is tied to. If an event belongs to your organisation, then this field will be coloured red.
- **Org:** The organisation that has created the event.
- **Category:** The category of the attribute, showing what the attribute describes (for example the malware's payload). For more information on categories, go to section xy
- **Type:** The type of the value contained in the attribute (for example a source IP address). For more information on types, go to section xy
- **Value:** The actual value of the attribute, describing an aspect, defined by the category and type fields of the malware (for example 11.11.11.11).
- **Comment:** An optional contextual comment attached to the attribute.
- **IDS:** Shows whether the attribute has been flagged for NIDS signature generation or not.
- **Actions:** A set of buttons that allow you to view the event that the attribute is tied to, to edit the attribute (using the same view as what is used to set up attributes, but filled out with the attribute's current data) and a delete button.

## Searching for attributes

Apart from being able to list all events, it is also possible to search for data contained in the value field of an attribute, by clicking on the "Search Attributes" button.

### Search Attribute

You can search for attributes based on contained expression within the value, event ID, submitting organisation, category and type. For the value, event ID and organisation, you can enter several search terms by entering each term as a new line. To exclude things from a result, use the NOT operator (!) in front of the term.

Containing the following expressions

Being attributes of the following event IDs

From the following organisation(s)

Type

Category

Only find valid IOCs

This will bring up a form that lets you enter one or several search strings (separate search strings with line breaks) that will be compared to the values of all attributes, along with options to narrow down the search based on category and type. The entered search string has to be an exact match with (the sub-string of) a value. A second text field makes it possible to enter event IDs for events that should be excluded from the search (again, each line represents an event ID to be excluded). The third text field allows the user to restrict the results to attributes from certain organisations or to attributes not created by certain other organisations, using the above described syntax. The list generated by the search will look exactly the same as listing all attributes, except that only the attributes that matched the search criteria will be listed (to find out more about the list attributes view, [click here](#)). The search parameters will be shown above the produced list and the search terms will be highlighted. The last option is a checkbox that restricts all of the results to attributes that are marked as IDS signatures.

## Attributes

Results for all attributes with the value containing "1.1.1":

Event	Org	Category	Type	Value	Comment	IDS	Actions
3		Network activity	ip-src	1.1.1.1	An IP address	Yes	
2		Network activity	ip-src	1.1.1.1	The same IP address	Yes	

## Updating and modifying events and attributes

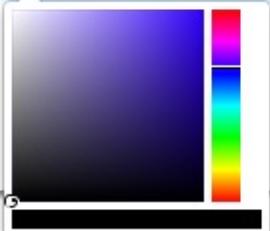
Every event and attribute can easily be edited. First of all it is important to find the event or attribute that is to be edited, using any of the methods mentioned in the section on [browsing past events](#). Once it is found, the edit button (whether it be under actions when events/attributes get listed or simply on the event view) will bring up the same screen as what is used to create the entry of the same type (for an event it would be the event screen as [seen here](#), for an attribute the attribute screen as [described here](#)). You can also simply double-click on the event you wish to edit and enter the edit mode. Keep in mind that editing any event (either directly or indirectly through an attribute) will unpublish it, meaning that you'll have to publish it (through the event view) again once you are done.

## Tagging

As described earlier, users with [tagging](#) rights can arbitrarily tag events using tags chosen from a pool of available options. If you have [tagging](#) privileges and would like to create a new tag, navigate to Event Actions - Add Tag. You'll be presented with the following form:

### Add Tag

---

Name	Colour
<input type="text" value="OSINT"/>	<input type="text" value="#000000"/> 
<input type="button" value="Add"/>	

Fill out the following fields:

- **Name:** Pick a name for the tag. Try to use consistent naming conventions across your instance, to avoid confusion.
- **Colour:** You can choose a colour for the tag by clicking on the colour field and using the colour picker tool. Try to avoid having duplicate or similar looking colours to help avoid confusion.

## Templating

Newer users can easily be overwhelmed by having to manually populate events with attributes without any guidance. What sort of information should go into the event? What should be the category and type of a C2 IP? Templates allow users to use simple forms to populate events. Even though MISP ships with a few default templates, it is possible for users (with the appropriate templating privilege) to create new templates for their users or for all users of the instance. Let's look at how you can create a template. First go to Event Actions - Add Template to go to the event creation view.

### Create Template

---

Name

Tags

OSINT X +

Event Description

Use this template to create OSINT events.

Share this template with others

**Create**

The following fields have to be filled out:

- **Name:** The name of the template should describe what type of an event it should be used to generate attributes.
- **Tags:** You can attach tags to the template - an event populated using the template would automatically receive the tag(s). Add new tags using the + button. If you change your mind about a tag you can remove it with the cross next to the tag name.
- **Event Description:** A short description about the events that this template should be used for.
- **Share this template with others:** The template can be set to be usable by any organisation on the instance or only by the one that has created it.

Once the skeleton template is created, you can start populating the template with data. There are 3 types of elements that can be used during the creation of a template: attribute, file and text elements. Text elements divide the template into sections with an information field, followed by all of the attribute/file fields until a new text field is read. Don't worry about the order of the elements during creation, they can be re-arranged using drag & drop. Let's look at the 3 element types:

#### Attribute Element

Add Attribute Element To Template

Name	
Description	
Category	Type
Payload installation	File
<input checked="" type="checkbox"/> Use complex types Types allowed based on the above setting: <a href="#">filename</a> <a href="#">filename md5</a> <a href="#">filename sha</a> <a href="#">filename sha256</a> <a href="#">md5</a> <a href="#">sha</a> <a href="#">sha256</a>	
<input type="checkbox"/> Automatically mark for IDS <input type="checkbox"/> Mandatory element <input type="checkbox"/> Batch import element	
<input type="button" value="Submit"/>	<input type="button" value="Cancel"/>

The following fields have to be filled out:

- **Name:** The field name that will be presented to the user.
- **Description:** A brief description of the element. Make sure that you provide sufficient information to the user to make it obvious what is expected.
- **Category:** The category used for any attributes created using this template element.
- **Type:** The type or complex type used for any attributes created using this template element. Complex types allow for several related types to be used on data entry. For example, a "file" complex type element allows for filenames and hashes.
- **Use Complex types:** If the category permits it, switch to a complex type using this checkbox.
- **Automatically mark for IDS:** If checked, any attributes generated using this element will be marked for IDS exporting.
- **Mandatory element:** If the element is marked as mandatory, then the template form can only be submitted by users if this field is filled out.
- **Batch import element:** Allow for multiple values to be entered (separated by line breaks).

#### File Element

Add File Element To Template

Name

Description

Category

Select Category ▾

Malware

Mandatory element

Batch import element

**Submit** **Cancel**

The following fields have to be filled out:

- **Name:** The field name that will be presented to the user.
- **Description:** A brief description of the element. Make sure that you provide sufficient information to the user to make it obvious what is expected.
- **Category:** The category to be used by all attachments uploaded through this element.
- **Malware:** If the uploaded files are malicious and should be encrypted and password protected, mark this checkbox.
- **Mandatory element:** If it should be required to upload an attachment, check this checkbox.
- **Batch import element:** Ticking this checkbox allows users to upload several files using this element.

#### Text Element

The following fields have to be filled out:

- **Name:** The name of the section that will be presented to the user.
- **Text:** The description of the section. Explain briefly to the user what the following attribute/file elements will be dealing with. There are several ways to split a template into sections, try to have ease of use in mind while creating it.

## Contacting the reporter

To get in touch with the reporter of a previously registered event, just find the event for which you would like to contact the reporter by either finding it on the list of events, by finding it through one of its attributes or by finding it through a related event. Once the event is found and the event view opened, click the button titled "Contact Reporter". This will bring up a view where you can enter your message that is to be e-mailed to all members of the reporting organisation that subscribe to receiving such reports or the reporting user himself. Along with your message, the detailed information about the event in question will be included in the e-mail.

### Contact organization reporting event 12

You are about to contact the organization that reported event 12.  
Feel free to add a custom message that will be sent to the reporting organization.  
Your email address and details about the event will be added automatically to the message.

Message

Submit only to person

By selecting this box you will contact the creator of  
the event only.

**Submit**

By default, the message will be sent to every member of the organisation that posted the event in the first place, but if you tick the check-box below the message field before sending the mail, only the person that reported the event will get e-mailed.

## Automation

It is possible to quickly and conveniently export the data contained within the system using the automation features located in the main menu on the left (available to users with authentication key access only). There are various sets of data that can be exported, by using the authentication key provided by the system (also shown on the export page). If for whatever reason you would need to invalidate your current key and get a new one instead (for example due to the old one becoming compromised) just hit the reset link next to the authentication key in the export view or in your "my profile" view. To find out about the various export formats and the usage within the automation functions, please read the page on the [API's usage](#).

## Exporting data

For users that do not have authentication key access, an alternate export feature is available that relies on your interactive login to the site. To access these, just use the export menu button to the left and you'll be presented with a list of export options.

Depending on your server's configuration, you will be presented with one of two possible pages, depending on whether you have background processing enabled or not.

### Export page with background jobs disabled

The page will list a set of export formats that you can immediately download as a file. Just click on the desired export format and MISP will start collecting all the data that you will receive in a file. Keep in mind that this can be a lengthy process. To avoid having to wait, consult with your instance's site administrator about enabling the background processing.

#### Export

Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support NIDS signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

Simply click on any of the following buttons to download the appropriate data.

[Download all as XML](#)

Click this to download all events and attributes that you have access to (except file attachments) in a custom XML format.

[Download all signatures as CSV](#)

Click this to download all attributes that are indicators and that you have access to (except file attachments) in CSV format.

[Download all as CSV](#)

Click this to download all attributes that you have access to (except file attachments) in CSV format.

[Download NIDS signatures](#)

Click this to download all network related attributes that you have access to under the Snort rule format. Only published events and attributes marked as *NIDS Signature* are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.

[Download all MD5 hashes](#)

Click on one of these two buttons to download all MD5 or SHA1 checksums contained in file-related attributes. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as *NIDS Signature* are exported.

[Download all SHA1 hashes](#)

Click on one of these buttons to download all the attributes with the matching type. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as *NIDS Signature* are exported.

[md5](#) [sha1](#) [sha256](#) [filename](#) [filename|md5](#) [filename|sha1](#) [filename|sha256](#) [ip-src](#) [ip-dst](#) [hostname](#) [domain](#) [email-src](#) [email-dst](#) [email-subject](#)

[email-attachment](#) [url](#) [http-method](#) [user-agent](#) [regkey](#) [regkey|value](#) [AS](#) [snort](#) [pattern-in-file](#) [pattern-in-traffic](#) [pattern-in-memory](#) [yara](#) [vulnerability](#)

[attachment](#) [malware-sample](#) [link](#) [comment](#) [text](#) [other](#) [named pipe](#) [mutex](#) [target-user](#) [target-email](#) [target-machine](#) [target-org](#) [target-location](#)

[target-external](#)

## Export page with background jobs enabled

If the background jobs are enabled, you'll be redirected to a different version of the export page. Here you will see a table with all of the major export formats and the current status of the cached export files. Keep in mind that these are generated on an organisation by organisation basis, so even though others have generated newer export caches your organisation may have an outdated cache. You can simply issue a generate command (by clicking the "Generate" button) on the desired export type and the background workers will start fetching and assembling your cache. A progress bar will show the progress of the export process. Once done, you can click "Download" to download the freshly generated cache file. If the cache is already up to date from before, then you don't have to regenerate the cache, just click on the "download" button. You may have noticed that the TEXT export only has a generate button - this is because TEXT exports are made up of a lot of types of exports, all of which get generated together. To download any of these files, just click on any of the attribute types at the bottom of the table. A quick description of each of the fields in the table:

- Type:** The type of the export (such as XML, Suricata, MD5, etc.).
- Last Update:** The generation date of the current cache for the given export type.
- Description:** A description of the export format.
- Outdated:** This compares the cache generation date to the last timestamp when an event was updated and lets you know whether the cache is outdated or not.
- Progress:** Shows the progress of the last initiated generation process.
- Actions:** Download or Generate the given cache with these buttons.

### Export

Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support NIDS signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

Simply click on any of the following buttons to download the appropriate data.

Type	Last Update	Description	Outdated	Progress	Actions
XML	N/A	Click this to download all events and attributes that you have access to (except file attachments) in a custom XML format.	Yes	Completed.	<a href="#">Download</a> <a href="#">Generate</a>
CSV,Sig	N/A	Click this to download all attributes that are indicators and that you have access to (except file attachments) in CSV format.	Yes	Completed.	<a href="#">Download</a> <a href="#">Generate</a>
CSV,All	N/A	Click this to download all attributes that you have access to (except file attachments) in CSV format.	Yes	Completed.	<a href="#">Download</a> <a href="#">Generate</a>
Suricata	N/A	Click this to download all network related attributes that you have access to under the Suricata rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	Completed.	<a href="#">Download</a> <a href="#">Generate</a>
Snort	N/A	Click this to download all network related attributes that you have access to under the Snort rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	Completed.	<a href="#">Download</a> <a href="#">Generate</a>
MD5	2 weeks ago	Click on one of these two buttons to download all MD5 checksums contained in file-related attributes. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as IDS Signature are exported.	Yes	Completed.	<a href="#">Download</a> <a href="#">Generate</a>
SHA1	N/A	Click on one of these two buttons to download all SHA1 checksums contained in file-related attributes. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as IDS Signature are exported.	Yes	Completed.	<a href="#">Download</a> <a href="#">Generate</a>
TEXT	N/A	Click on one of the buttons below to download all the attributes with the matching type. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as IDS Signature are exported.	Yes	Completed.	<a href="#">Generate</a>
<a href="#">md5</a> <a href="#">sha1</a> <a href="#">sha256</a> <a href="#">filename</a> <a href="#">filename md5</a> <a href="#">filename sha1</a> <a href="#">filename sha256</a> <a href="#">lo-src</a> <a href="#">lo-dst</a> <a href="#">hostname</a> <a href="#">domain</a> <a href="#">email-src</a> <a href="#">email-dist</a> <a href="#">email-subject</a> <a href="#">email-attachment</a> <a href="#">url</a> <a href="#">http-method</a> <a href="#">user-agent</a> <a href="#">regkey</a> <a href="#">regkeyvalue</a> <a href="#">AS</a> <a href="#">snort</a> <a href="#">pattern-in-file</a> <a href="#">pattern-in-traffic</a> <a href="#">pattern-in-memory</a> <a href="#">yara</a> <a href="#">vulnerability</a> <a href="#">attachment</a> <a href="#">malware-sample</a> <a href="#">link</a> <a href="#">comment</a> <a href="#">text</a> <a href="#">other</a> <a href="#">named pipe</a> <a href="#">mutex</a> <a href="#">target-user</a> <a href="#">target-email</a>					

## Exporting search results and individual events

Apart from the options offered by the export pages, it's also possible to export all events involved in a search attribute result table, by using the "Download results as XML" button on the left menu bar.

The screenshot shows a left sidebar with a blue header and a main content area. The sidebar contains links: List Events, Add Event, List Attributes, **Search Attributes** (which is highlighted in blue), Download results as XML, Export, and Automation. The main content area has a title 'Attributes' and a subtitle 'Results for all attributes with the value containing "1.1.1":'. It includes navigation buttons '« previous' and 'next »'. A table displays one record:

Event	Category	Type	Value
7	Network activity	ip-src	1.1.1.34

Below the table, a message says 'Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1'. Navigation buttons '« previous' and 'next »' are at the bottom.

Each event's view has its own export feature, both as an XML export and as a .ioc file. To reach these features, just navigate to an event and use the appropriate buttons on the right side.

List Events  
Add Event

---

List Attributes  
**Search Attributes**

---

Download results as XML

---

Export  
Automation

## Attributes

Results for all attributes with the value containing "1.1.1":

« PREVIOUS next »

Event	Category	Type	Value
7	Network activity	ip-src	1.1.1.34

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

« PREVIOUS next »

## Connecting to other instances

Apart from being a self contained repository of attacks/malware, one of the main features of MISP is its ability to connect to other instances and share (parts of) its information. The following options allow you to set up and maintain such connections.

### Setting up a connection to another server

In order to share data with a remote server via pushes and pulls, you need to request a valid authentication key from the hosting organisation of the remote instance. When clicking on List Servers and then on New Server, a form comes up that needs to be filled out in order for your instance to connect to it. The following fields need to be filled out:

Add Server

---

Base URL	Organization	Authkey
<input type="text" value="https://www.friendlymisp.com"/>	<input type="text" value="Org_name"/>	<input type="text"/>
<input checked="" type="checkbox"/> Push	<input checked="" type="checkbox"/> Pull	
<input type="checkbox"/> Self Signed		
Certificate file		
<input type="button" value="Choose File"/> No file chosen		
<input type="button" value="Add"/>		

- **Base URL:** The URL of the remote server.
- **Organization:** The organisation that runs the remote server. It is very important that this setting is filled out exactly as the organisation name set up in the bootstrap file of the remote instance.
- **Authkey:** The authentication key that you have received from the hosting organisation of the remote instance.
- **Push:** This check-box controls whether your server is allowed to **push** to the remote instance.
- **Pull:** This check-box controls whether your server can request to **pull** all data from the remote instance.
- **Self Signed:** Ticking this checkbox will allow syncing with instances using self-signed certificates.
- **Certificate File:** If the instance that you want to connect to has their entire own certificate chain, you can use this to import a .pem file with it and override CakePHP's standard root CA file.

If you are an **administrator**, trying to allow another instance to connect to your own, it is vital that two rules are followed when setting up a [synchronisation](#) account:

- The [synchronisation](#) user has to have the sync permission and full read/write/publish privileges turned on
- Both the [sync user](#) and the organisation setting in your instance's Config/bootstrap.php file have to match the organisation identifier of the hosting organisation.

## Browsing the currently set up server connections and interacting with them

If you ever need to change the data about the linked servers or remove any connections, you have the following options to view and manipulate the server connections, when clicking on List Servers: (you will be able to see a list of all servers that your server connects to, including the base address, the organisation running the server the last pushed and pulled event IDs and the control buttons.).

### Servers

			From		Cert	Self	Org	Last	Last	Actions
Push	Pull	Url			File	Signed		Pulled	Pushed	
No	Yes	http://192.168.14.11		11	5.pem	Yes	ADMIN			 

Page 1 of 1. showing 1 records out of 1 total. starting on record 1. ending on 1

- **Editing the connection to the:** By clicking edit a view, [that is identical to the new instance view](#), is loaded, with all the current information of the instance pre-entered.
- **Deleting the connection to the instance:** Clicking the delete button will delete the link to the instance.
- **Push all:** By clicking this button, all events that are eligible to be pushed on the instance you are on will start to be pushed to the remote instance. Events and attributes that exist on the far end will be updated.
- **Pull all:** By clicking this button, all events that are set to be [pull](#)-able or full access on the remote server will be copied to this instance. Existing events will not be updated.

## Rest API

The platform is also [RESTfull](#), so this means that you can use structured format (XML or JSON) to access Events data.

### Requests

Use any HTTP compliant library to perform requests. You can choose which format you would like to use as input/output for the REST calls by specifying the Accept and Content-Type headers.

The following headers are required if you wish to receive / [push](#) XML data: **Authorization:** *your authorisation key* **Accept:** *application/xml* **Content-Type:** *application/xml*

The following headers are required if you wish to receive / [push](#) JSON data: **Authorization:** *your authorisation key* **Accept:** *application/json* **Content-Type:** *application/json* The following table shows the relation of the request type and the resulting action:

HTTP format	URL	Controller action invoked
GET	/events	EventsController::index()
GET	/events/123	EventsController::view(123)
POST	/events	EventsController::add()
PUT	/events/123	EventsController::edit(123)
DELETE	/events/123	EventsController::delete(123)
POST	/events/123	EventsController::edit(123)

\*Attachments are included using base64 encoding below the `data` tag.

### Example - Get single Event

In this example we fetch the details of a single Event (and thus also his Attributes). The request should be:

```
GET https://your_misp_url/events/123
```

And with the HTTP Headers: `Accept: application/xml` `Authorization: your_api_key`

The response you're going to get is the following data:

```
<pre><?xml version="1.0" encoding="UTF-8" standalone="no"?>;
<response>
  <Event>
    <id>57</id>
    <org>NCIRC</org>
    <date>2014-03-04</date>
    <threat_level_id>1</threat_level_id>
    <info>Code monkey doing code monkey stuff</info>
    <published>1</published>
```

```

<uuid>50aa54aa-f7a0-4d74-910d-10f0ff32448e</uuid>
<attribute_count>1</attribute_count>
<analysis>1</analysis>
<timestamp>1393327600</timestamp>
<distribution>1</distribution>
<proposal_email_lock>0</proposal_email_lock>
<orgc>Iglocska</orgc>
<locked>0</locked>
<publish_timestamp>1393327600</publish_timestamp>
<Attribute>
  <id>9577</id>
  <type>other</type>
  <category>Artifacts dropped</category>
  <to_ids>1</to_ids>
  <uuid>50aa54bd-adec-4544-b494-10f0ff32448e</uuid>
  <event_id>57</event_id>
  <distribution>1</distribution>
  <timestamp>1393327600</timestamp>
  <comment>This is an Attribute</comment>
  <value>Some_attribute</value>
  <ShadowAttribute />
</Attribute>
<ShadowAttribute />
<RelatedEvent />
</Event>
<xml_version>2.2.0</xml_version>
</response>
```

## Example - Add new Event

In this example we want to add a single Event. The request should be:

```

POST https://your_misp_url/events
Accept: application/xml
Authorization: your_api_key
```

And the request body:

```

<Event>
  <date>2014-03-04</date>
  <threat_level_id>1</threat_level_id>
  <info>Something concise</info>
  <published>1</published>
  <analysis>1</analysis>
  <distribution>1</distribution>
  <Attribute>
    <type>other</type>
    <category>Artifacts dropped</category>
    <to_ids>1</to_ids>
    <distribution>1</distribution>
    <comment>This is an Attribute</comment>
    <value>Some_attribute</value>
  </Attribute>
</Event>
```

The response you're going to get is the following data:

```

HTTP/1.1 100 Continue
HTTP/1.1 200 Continue
Date: Tue, 04-Mar-2014 15:00:00
Server: Apache/2.2.22 (Ubuntu) PHP/5.4.9-4ubuntu2.3
X-Powered-By: PHP/5.4.9-4ubuntu2.3
Set-Cookie: CAKEPHP=deleted; expires=Wed, 05-Mar-2014 15:00:00 GMT; path=/
```

```
Set-Cookie: CAKEPHP=a40k3lr5p9n5drqj27025i4le3; expires Tue, 04-Mar-2014 15:00:00 GMT; path=/; HttpOnly
Content-Length: 1 kB
Content-Type: application/xml
```

```
<?xml version = "1.0" encoding = "UTF-8"?>
<response>
<Event>
<id>76</id>
<org>NCIRC</org>
<date>2014-03-04</date>
<threat_level_id>1</threat_level_id>
<info>Something concise</info>
<published>1</published>
<uuid>50aa54aa-f7a0-4d74-920d-10f0ff32448e</uuid>
<attribute_count>1</attribute_count>
<analysis>1</analysis>
<timestamp>1393328991</timestamp>
<distribution>1</distribution>
<proposal_email_lock>0</proposal_email_lock>
<orgc>Iglocska</orgc>
<locked>0</locked>
<publish_timestamp>1393947960</publish_timestamp>
<Attribute>
<id>10462</id>
<type>other</type>
<category>Artifacts dropped</category>
<to_ids>1</to_ids>
<uuid>50aa54bd-adec-4544-b412-10f0ff32448e</uuid>
<event_id>76</event_id>
<distribution>1</distribution>
<timestamp>1393328991</timestamp>
<comment/>
<value>Some_attribute</value>
<ShadowAttribute/>
</Attribute>
<ShadowAttribute/>
<RelatedEvent>
<id>75</id>
<org>NCIRC</org>
<date>2012-11-19</date>
<info>Code monkey doing code monkey stuff</info>
<uuid>50aa54aa-f7a0-4d74-910d-10f0ff32448e</uuid>
<published>1</published>
<analysis>1</analysis>
<attribute_count>1</attribute_count>
<orgc>Iglocska</orgc>
<timestamp>1393327600</timestamp>
<distribution>1</distribution>
<proposal_email_lock>0</proposal_email_lock>
<locked>0</locked>
<threat_level_id>1</threat_level_id>
<publish_timestamp>1393947655</publish_timestamp>
</RelatedEvent>
</Event>
<xml_version>2.2.0</xml_version>
</response>
```

The response from requesting an invalid page

```
<?xml version = "1.0" encoding = "UTF-8"?>
<response>
<name>Not Found</name>
<url>/The_meaning_of_life</url>
</response>
```

Last modified: Sat Jul 13 2019 10:06:38 GMT+0200 (CEST)

## Delegation

In information sharing, privacy of the reporting organisation can be important in such case as:

- an incident doesn't want to be linked to a potential victim.
- to avoid the relation of an organisation with the information shared.

MISP has a functionality to delegate the publication and completely remove the binding between the information shared and its organisation. If you want to publish an event without you or your organisation being tied to it, you can delegate the publication to an other organisation. That also means they will take the ownership of the event.

[warning] You need to have a role with "Delegation access" to delegate an event.

[warning] Also activate MISP.delegation parameter in your instance.

### Send a delegation request

To do so, you first need to put the distribution of the event as "your organisation only".

Publish Event	Distribution	Your organisation only
Publish (no email)	Info	Delegate me
Delegate Publishing	Published	No
Contact Reporter	Sightings	0 (0) ↗
Download as...	Activity	
	Correlation	Enabled ( <a href="#">disable</a> )

Otherwise the delegation option will not be available.

<a href="#">Publish Event</a>	<b>Distribution</b>	All communities
<a href="#">Publish (no email)</a>	<b>Info</b>	Delegate me
<a href="#">Contact Reporter</a>	<b>Published</b>	<b>No</b>
<a href="#">Download as...</a>	<b>Sightings</b>	0 (0) 
	<b>Activity</b>	
	<b>Correlation</b>	Enabled ( <a href="#">disable</a> )

When the "Delegate Publishing" option is clicked, a pop-up will show up:

### Delegate the publishing of the Event to another organisation

Warning: You are about to request another organisation to take ownership of this event.

Target Organisation

Select organisation

Desired Distribution

Recipient decides

Message to the recipient organisation

Yes

No

Here you can choose

- to which organisation you wish to delegate the event among all those registered on the server. For this example we are going to ask Setec Astronomy to publish the event for us.
- The distribution option you would like to put on the event. You can let the other organisation (called "recipient") choose if you don't mind it. For this example, we will request the recipient to share it to all communities, but it is only a suggestion, and the recipient will be able to modify the diffusion setting if wanted.



- Finally you can leave a free message to the recipient organisation.

## Delegate the publishing of the Event to another organisation

Warning: You are about to request another organisation to take ownership of this event.

Target Organisation

Setec Astronomy ▾

Desired Distribution

Recipient decides ▾

Message to the recipient organisation

Yes

No

•

Once the request is sent, a message will appear on the event to remind you of your request.

Publish Event	Published	No
Publish (no email)	Sightings	0 (0) 🔍
	Activity	
	Delegation request	You have requested that Setec Astronomy take over this event. (View request details)
Discard Delegation Request	Correlation	Enabled (disable)

You can also see more details by clicking on "View request details"

## Event Delegation

### Request details

Your organisation is requesting **Setec Astronomy** to take over this event.

### Message from requester

**Discard**

**Cancel**

And you can also discard the request your self, by using this pop-up or the link in the left menu.

## Answer a delegation request

As the recipient organisation, you will then receive the request of delegation. You will be notified by a red circle around the envelope on the top right of the screen.



When you click it, you will be redirected as usual on the dashboard, where we can see one delegation request on the left frame.

## Dashboard

### Notifications

Proposals: **0** ([View](#))

Events with proposals: **0** ([View](#))

Delegation requests: **1** ([View](#))

### Changes since last visit

Events updated: **571** ([View](#))

Events published: **571** ([View](#))

[Reset](#)

Clicking on the "view" link then redirect to an event list view showing all the events other organisations wish to delegate to your organisation. Here we only see one event, from Acme Factory.

## Events

[« previous](#) [next »](#)

Published	Org	ID	Clusters	Tags	#Attr.	#Corr.	#Sightings	#Posts	Date	Threat Level	Analysis	Info	Distribution	Actions
	Acme Finance	<a href="#">1096</a>			0				2017-03-23	High	Initial	Delegate	<a href="#">Organisation</a>	Not published

And here are the metadata of the so called event.

[View Event](#)

[View Correlation Graph](#)

[View Event History](#)

---

[Propose Attribute](#)

[Propose Attachment](#)

---

[Accept Delegation Request](#)

[Discard Delegation Request](#)

---

[Contact Reporter](#)

[Download as...](#)

---

[List Events](#)

[Add Event](#)

## Delegate me

Event ID	1096
Uuid	58d38964-6be8-4c5b-a338-4920950d210f
Org	Acme Finance
Contributors	
Tags	
Date	2017-03-23
Threat Level	High
Analysis	Initial
Distribution	Your organisation only
Info	Delegate me
Published	No
Sightings	0 (0) ↗
Activity	
Delegation request	Acme Finance has requested that you take over this event. (View request details)
Correlation	Enabled

You will be able to view the details by clicking the so called link.

## Event Delegation

### Request details

Acme Finance is requesting **your organisation** to take over this event.

The desired distribution level is **All communities**

### Message from requester

This is a delegation test

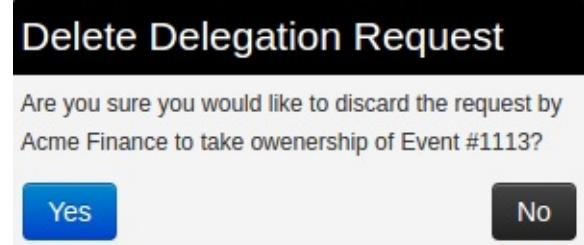
Accept

Discard

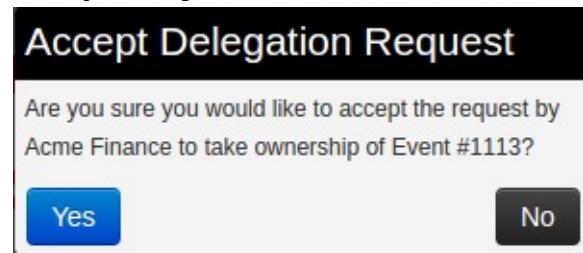
Cancel

If your role have [publishing](#) rights, you will be able to manage the delegation request by using one of the two links in the left menu.

You can either discard it:



Or accept the delegation:



Please notice that the distribution desired by the requester will not automatically be set on the event, which will stay as distributed to your own organisation only if the parameter is not modified.

 *Last modified: Thu May 24 2018 10:37:13 GMT+0200 (CEST)*

## MISP Extended Events

MISP can now extend an event (starting from version 2.4.90). This allows users to build full blown events that extend an existing event, giving way to a combined event view that includes a sum total of the event along with all extending events. [More](#)

Last modified: Tue Mar 10 2020 14:01:03 GMT+0100 (CET)

- Administration
  - Users
    - Adding a new user
    - Listing all users
    - Contacting a user
  - Organisations
    - Adding a new organisation
    - Listing all organisations
    - Merge organisations
  - Roles
    - Adding a new role
    - Listing roles
  - Tools
  - Server Settings
  - Server settings and diagnostics
    - Worker types
    - Workers dead
  - Import Blacklist
    - Adding and modifying entries
  - Import Regexp
    - The purpose of Import Regexp entries
    - Adding and modifying entries
  - Managing the Signature whitelist
    - Whitelisting an address
    - Managing the list
  - Using MISP logs
    - Browsing logs
    - Searching Logs
  - Background Processing
    - Command Line Tools for the Background Workers
    - Monitoring the Background Processes
    - Scheduling Jobs and Recurring Jobs
  - Various administration tips & tricks
    - Setting a Publish Alert Filter
    - Default sharing level
    - Adding organisation logos
    - The \_schdlr\_ worker is not starting
    - How to redirect HTTP to HTTPS
    - Increase max size of Samples / other files
    - Support & feature requests
    - More information in the notification emails about new events
    - Get top API users
    - MISP Logs
    - Logging of failed authentication attempts
    - Clearing expired sessions
    - Troubleshooting MISP not connecting to redis but redis-cli working
    - Errors about fields or tables
  - Jobs ~ TODO: Explain differences Default, Email, Cache
  - Scheduled Tasks

- [MISP Backup](#)
- [MISP Restore](#)

## Administration

- [Users](#)
- [Organisations](#)
- [Roles](#)
- [Tools](#)
- [Server Settings](#)
- [Jobs](#)
- [Scheduled Tasks](#)

[warning] This page is under modification for updating the content. Current status:

- [x] Users - Reviewed/Updated on: ?
  - [x] Organisations - Reviewed/Updated on: ?
  - [x] Roles - Reviewed/Updated on: ?
  - [x] Tools - Reviewed/Updated on: ?
  - [ ] Server Settings - Reviewed/Updated on: ?
  - [ ] Jobs aka. Background processing - Reviewed/Updated on: ?
  - [ ] Scheduled Tasks aka. Background processing - Reviewed/Updated on: ?
- 

## Users

As an admin (not to be confused with [Org Admin](#)), you can set up new accounts for users, edit user profiles, delete them, or just have a look at all the viewers' profiles. Organisation admins ([Org Admin](#)) are restricted to executing these actions exclusively within their own organisation's users only.

### Adding a new user

To add a new user, click on the Add User button in the administration menu to the left and populate the fields available the loaded view:

## Admin Add User

Email

 Set password

Password

Confirm Password

Organisation

 Choose organisation ▾

Role

 admin ▾

Authkey

 IPgSmUXk3cJrewQvkjrb76sCx8iC

Nids Sid

 ▾

Sync user for

 Not bound to a server ▾

GPG key

**Fetch GPG key** Receive alerts when events are published Receive alerts from "contact reporter" requests Disable this user account**Submit**

- **Email:** The user's e-mail address, this will be used as his/her login name and as an address to send all automated e-mails as well as e-mails sent by contacting the user as the reporter of an event.
- **Set password:** Tick the box if you want to define a temporary user-password for the user. If you don't, you should use the action button 'reset password' in the 'List Users' view to generate one and send it by email to the user.
- **Password:** This *textbox is displayed only when 'Set password' is ticked*. A Temporary password for the user that he/she should change after the first login. Ensure that password pass the [MISP password policy](#).
- **Confirm Password:** This *textbox is displayed only when 'Set password' is ticked*. This should be an exact copy of the Password field.
- **Organisation:** A drop-down list enables you to choose an organisation for the user. To learn more about organisation, [click here](#).
- **Roles:** A drop-down list allows you to select a role-group that the user should belong to. [Roles](#) define user privileges attributed to the user. To learn more about [roles](#), [click here](#).
- **Authkey:** This is assigned automatically and is the unique authentication key of said user (he/she will be able to reset this and receive a new key). It is used for exports and for connecting one server to another, but it requires the user to be assigned to a role that has auth permission enabled.
- **NIDS Sid:** ID of network intrusion detection systems.
- **Sync user for:** Use this option for granting the user the right to synchronize the event between MISP server. This option is available for admin, [Org Admin](#) and [Sync user](#) role.
- **Gpgkey:** The key used to encrypt e-mails sent through the system.
- **Fetch GnuPG key:** Fetch GnuPG public key.
- **Receive alerts when events are published:** This option will subscribe the new user to automatically generated e-mails whenever an event is published.
- **Receive alerts from "contact reporter" requests:** This option will subscribe the new user to e-mails that are generated when another user tries to get in touch with an event's reporting organisation that matches that of the new user.
- **Disable this user account:** Tick it if you want to disable this user account. (preferred to removing an account)

## Listing all users

To list all current users of the system, just click on List Users under the administration menu to the left. A view will load containing a list of all users and the following columns of information:

### Users

Filter													
	Id	Org	Role	Email	Authkey	Autoalert	Contactalert	Gpgkey	Nids Sid	Termsaccepted	Last login	Disabled	Actions
	3	CIRCL	Publisher	operator@circ.lu	1e1t1MCDoakGuLX0qT1PsBCYW56jj4IXmP19rTy	No	No	No	123456	Yes	N/A	No	 
	1	MISP	admin	admin@misp.training	JNqWBxfPilyvz7hUe58MyJf6sD5PrTVaGm7hTr6c	No	No	No	4000000	Yes	2016-08-04	No	 
	2	MISP	Publisher	user@misp.training	leK5WqbKN3l65SMPgXNWEx27xTRMcEIVTz1P0czN	No	No	No	1000001	Yes	2016-08-04	No	 

Page 1 of 1, showing 3 records out of 3 total, starting on record 1, ending on 3

[« previous](#) [next »](#)

- **Id:** The user's automatically assigned ID number.
- **Org:** The organisation that the user belongs to.
- **Email:** The e-mail address (and login name) of the user.
- **Authkey:** Unique authentication key of the user.
- **Autoalert:** Shows whether the user has subscribed to auto-alerts and is continuing to receive mass-emails regarding newly published events that he/she is eligible for.
- **Contactalert:** Shows whether the user has the subscription to contact reporter e-mails directed at his/her organisation is turned on or off.
- **Gpgkey:** Shows whether the user has entered a GnuPG key yet.
- **Nids Sid:** Displays the currently assigned NIDS ID.
- **Termsaccepted:** This flag indicates whether the user has accepted the terms of use or not.
- **Last login:** Date of last login.
- **Disabled:** Displays the user status. Enabled or disabled.
- **Action Buttons:** There are 4 options available: reset the password, edit the user, delete the user or display a user's information. These options are also available on the left menu.
  - **Reset Password:** Use this action to reset a password. If you've created a new user without A password, tick the 'First time registration' checkbox to send a welcome message. Otherwise a reset password message will be sent.



- - **Edit the user:** Same options of create user's view. Only a few options are available here:
    - **Terms accepted:** Indicates whether the user has accepted the terms of use already or not.
    - **Change Password:** Setting this flag will require the user to change password after the next login.
    - **Reset Auth Key:** Use this link for generate a new AuthKey.



#### Admin Edit User

Email

Set password

Organisation      Role

Authentication key      Nids Sid

GPG key

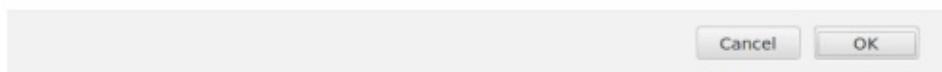
Terms accepted       Change Password       Receive alerts when events are published       Receive alerts from "contact reporter" [Reset Auth Key](#) requests

Disable this user account

- - - **Delete the user:** If you want to delete a user. (Note: disabling is the preferred method)



Are you sure you want to delete # 5? It is highly recommended to never delete users but to disable them instead.



- - **Display the user:** Display all user's information.



### User

<b>Id</b>	2
<b>Org</b>	MISP
<b>Role</b>	Publisher
<b>Email</b>	user@misp.training
<b>Autoalert</b>	No
<b>Contactalert</b>	No
<b>Authkey</b>	EwedHQwWfjGbL4GdjdmY2NikQhe2FszjZM1QX5t (reset)
<b>Invited By</b>	admin@misp.training
<b>PGP key</b>	N/A
<b>Nids Sid</b>	1000001
<b>Termsaccepted</b>	Yes
<b>Password change</b>	No
<b>Newread</b>	2016/08/04 10:18:39
<b>Disabled</b>	No

### Related Events

- -

## Contacting a user

Site admins can use the "Contact users" feature to send all or individual user an e-mail. Users that have a GnuPG key set will receive their e-mails encrypted. When clicking this button on the left, you'll be presented with a form that allows you to specify the type of the e-mail, who it should reach and what the content is using the following options:

### Contact User(s)

#### Messaging - here's a quick guide on how this feature works

You can use this view to send messages to your current or future users or send them a temporary password.

- When adding a new user to the system, or when you want to manually reset the password for a user, just use the "Send temporary password" setting.
- After selecting the action, choose who the target of the e-mails should be (all users, a single user or a user not yet in the system).
- You can then specify (if eligible) what the e-mail address of the target is (for existing users you can choose from a dropdown menu).
- In the case of a new user, you can specify the future user's gpg key, to send his/her new key in an encrypted e-mail.
- The system will automatically generate a message for you, but it is also possible to write a custom message if you tick the check-box, but don't worry about assigning a temporary password manually, the system will do that for you, right after your custom message.

Action	Subject
<input type="button" value="Custom message"/>	<input type="text"/>
Recipient	Recipient Email
<input type="button" value="A single user"/>	<input type="text" value="admin@misp.training"/>
<input type="checkbox"/> Enter a custom message	
Message	
<input type="button" value="Submit"/>	

- **Action:** This defines the e-mail type, which can be a custom message or a password reset. Password resets automatically include a new temporary password at the bottom of the message and will automatically change the user's password accordingly.
- **Subject:** In the case of a custom e-mail, you can enter a subject line here.
- **Recipient:** The recipient toggle lets you contact all your users, a single user (which creates a second drop-down list with all the e-mail addresses of the users) and potential future users (which opens up a text field for the e-mail address and a text area field for a GnuPG public key).
- **Custom message checkbox:** This is available for password resets and for welcome messages. You can either write your own message (which will be appended with a temporary key and the signature), or let the system generate one automatically.

Keep in mind that all e-mails sent through this system, in addition to your own message, will be signed in the name of the instance's host organisation's support team, the e-mail will also include the e-mail address of the instance's support (if the contact field is set in the bootstrap file), and will include the instance's GnuPG signature for users that have a GnuPG key set (and thus are eligible for an encrypted e-mail).



GnuPG instance key is the GnuPG key used by the [MISP instance](#) and which is only used to sign notification. The GnuPG key used in the [MISP instance](#) must not be used anywhere else and should not be valuable.

## Organisations

Each user belongs to an organisation. As admin, you can manage these organisations.

### Adding a new organisation

To add a new organisation, click on the "Add Organisation" button in the administration menu to the left and fill out the following fields in the view that is loaded:

**New Organisation**

If the organisation should have access to this instance, make sure that the Local organisation setting is checked.  
If you would only like to add a known external organisation for inclusion in sharing groups, uncheck the Local organisation setting.

Local organisation

**Mandatory fields.**

Organisation Identifier  
 Brief organization identifier      No image uploaded for this identifier

Uuid  
 Paste UUID or click generate     

A brief description of the organisation  
 A description of the organisation that is purely informational.

The following fields are all optional.

Nationality      Sector  
 Not specified       For example "financial".

Type of organisation  
 Freetext description of the org.

Contacts  
 You can add some contact details for the organisation here, if applicable.

- **Local organisation:** If the organisation should have access to this instance, tick the checkbox. If you would only like to add a known external organisation for inclusion in [sharing groups](#), uncheck it.
- **Organisation Identifier:** Name your organisation. If you want to add a picture, you should add a file on the webserver using the 'Server Settings menu'. Picture should have the same name. To learn more about server settings menu, [click here](#).
- **Uuid:** Unique identifier. If you want to share organisation between MISP multi-instance, use the same Uuid.
- **A brief description of the organisation:** A word for describing the organisation.
- **Nationality:** A drop-down list for selecting the country of organisation.
- **Sector:** Define the sector of organisation (financial, transport, telecom...)
- **Type of organisation:** Define the type of the organisation.
- **Contacts:** You can add some contact details for the organisation.

## Listing all organisations

To list all current organisations of the system, just click on List Organisations under the administration menu to the left. There are 3 tabs in this view to filter local organisations, remote organisations or both. The default view displays local organisations. For all views the following columns of information are available:

Local organisations having a presence on this instance											
								Filter			
Id	Logo	Name	Uuid	Description				Nationality	Sector	Type	Contacts
1		MISP	56ef3277-1ad4-42f6-b90b-04e5c0a83832	Host organisation for the training instance				International		Unknown	<input checked="" type="checkbox"/>  
2		CIRCL	55f8ea5e-2c60-40e5-9841-47a8950d210f					Not specified		admin@misp.training	<input checked="" type="checkbox"/>  

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

[« previous](#) [next »](#)

- **Id:** The organisation's automatically assigned ID number.
  - **Logo:** Picture of the organisation.
  - **Name:** Name of the organisation.
  - **Uuid:** Unique identifier of organisation. Share this Uuid when using it between MISP's multi-instance.
  - **Description:** Description of the organisation.
  - **Nationality:** Country of the organisation.
  - **Sector:** Sector defined for the organisation.
  - **Type:** Type of organisation.
  - **Contacts:** Contacts of organisation.
  - **Added by:** Login of the user who added the organisation
  - **Local:** Flag defined if the organisation is local or remote.
  - **Users:** The amount of users on this instance belonging to the organisation.
  - **Actions:** There are 3 options available: edit, delete or display an organisation's information. These options are also available on the left menu when you are on the display view.
- **Edit Organisation:** Same options of create organisation's view.

## Edit Organisation

If the organisation should have access to this instance, make sure that the Local organisation setting is checked.  
If you would only like to add a known external organisation for inclusion in sharing groups, uncheck the Local organisation setting.

Local organisation

Mandatory fields. Leave the UUID field empty if the organisation doesn't have a UUID from another instance.

Organisation Identifier

CIRCL



Uuid

55f6ea5e-2060-40e5-964f-47a8950d210f

Generate UUID

A brief description of the organisation

A description of the organisation that is purely informational.

The following fields are all optional.

Nationality

Not specified

Sector

For example 'financial'.

Type of organisation

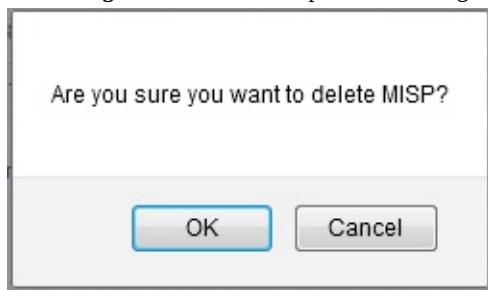
Freetext description of the org.

Contacts

You can add some contact details for the organisation here, if applicable.

Submit

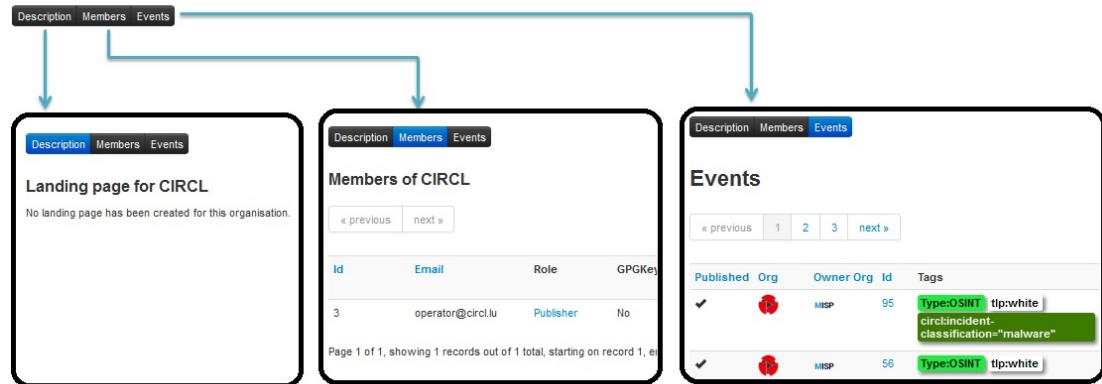
- - 
  - **Delete Organisation:** Use this option for deleting organisation.



- **View Organisation:** Use this option to display information about the selected organisation. In this view, you can display the user belongs to this organisation and events published by organisation.

### Organisation CIRCL

<b>Id</b>	2
<b>Organisation name</b>	CIRCL
<b>Local or remote</b>	<b>Local</b>
<b>Description</b>	
<b>Uuid</b>	55f6ea5e-2c60-40e5-964f-47a8950d210f
<b>Created by</b>	admin@misp.training
<b>Nationality</b>	Not specified



## Merge organisations

Merge Organisation menu is available only in the organisation view, under the left menu. Merging one organisation into another will transfer all users and data from one organisation to a different one. The organisation of which the users and data will be transferred is displayed on the left, the target organisation is displayed on the right.

**Merge Organisation**

*Warning: Merging an organisation into another will be transfer all users and data belonging to the organisation to another.*

Organisation type	Target Local Organisation
Local	MISP
<b>Organisation to be merged</b>	<b>Organisation to be merged into</b>
ID: 2 Name: CRCL UUID: 55f6ea5e-2c60-40e5-9641-47a8950d210f Type: Local	ID: 1 Name: MISP UUID: 56ef3277-1ad4-42f6-b90b-04e5c0a83832 Type: local

**Merge** **Cancel**

## Roles

Privileges are assigned to users by assigning them to rule groups. Rule groups use one of four options determining what they can do with events as well as four additional privilege elevation settings. These are the four options to edit the full options available in the [Roles](#) section: Read Only, Manage My Own Events, Manage Organisation Events, Manage & Publish Organisation Events. A short description is provided below:

- **Read Only:** Allows a user to browse events that his organisation has access to, but doesn't allow any changes to be made to the database.
- **Manage My Own Events:** Allows users to create, modify or delete their own events, but they cannot publish them.
- **Manage Organization Events:** Allows users to create events or modify and delete events created by a member of their organisation.
- **Manage & Publish Organisation Events:** Gives users the right to do all of the above and to publish the events of their organisation.

The extra permissions are defined below:

- **Perm Admin:** Gives the user limited administrator privileges, this setting is used for an organisation's admins.
- **Perm Audit:** Grants access to the logs. With the exception of site admins, only logs generated by the user's own org are visible.
- **Perm Tagger:** Allows a user to assign tags to events.
- **Perm Sharing Group:** Grant access to edit or create [sharing groups](#).
- **Perm Site Admin:** Gives the user full administrator privileges, this setting is used for site admins.
- **Perm Auth:** This setting enables the authentication key of the role's users to be used for rest requests.
- **Perm Tag Editor:** Grants access to edit or create tags.
- **Perm Delegate:** Grant access to delegate the publication of an event to a third-party organization.
- **Perm Sync:** This setting enables the users of the role to be used as a [synchronisation](#) user. The authentication key of this user can be handed out to the administrator of a remote [MISP instance](#) to allow the [synchronisation](#) features to work.
- **Perm Regexp Access:** Allows users who have this permission enabled to edit the regular expression table. Be careful when giving out this permission, incorrect regular expressions can be very harmful (infinite loops, loss of data, etc.).
- **Perm Template:** Grant access to create or modify templates.

## Adding a new role

When creating a new role, you will have to enter a name for the role to be created and set up permissions (as described above) using the drop-down menu and related check-boxes.

### Add Role

Name	Permission	
<input type="text"/>	<input type="button" value="Read Only"/> <input type="button" value=""/>	
<input type="checkbox"/> Perm Admin	<input type="checkbox"/> Perm Site Admin	<input type="checkbox"/> Perm Sync
<input type="checkbox"/> Perm Audit	<input type="checkbox"/> Perm Auth	<input type="checkbox"/> Perm Regexp Access
<input type="checkbox"/> Perm Tagger	<input type="checkbox"/> Perm Tag Editor	<input type="checkbox"/> Perm Template
<input type="checkbox"/> Perm Sharing Group	<input type="checkbox"/> Perm Delegate	
<input type="button" value="Add"/>		

## List roles

By clicking on the List Roles button, you can view a list of all currently registered roles and their enabled permissions. In addition, you can find buttons that allow you to edit and delete said roles. Keep in mind that you will need to first remove every member from a role before you can delete it.

### Roles

[« previous](#) [next »](#)

Id	Name	Permission	Actions											
			Admin	Site Admin	Sync Actions	Audit Actions	Auth key access	Regex Actions	Tagger	Tag Editor	Template Editor	Sharing Group Editor	Delegations access	Actions
6	Automation user	Manage & Publish Organization Events					✓						✓	⊕
2	Org Admin	Manage & Publish Organization Events	✓		✓	✓	✓		✓	✓	✓	✓	✓	⊕
4	Publisher	Manage & Publish Organization Events											✓	⊕
7	Read Only	Read Only												⊕
5	Sync user	Manage & Publish Organization Events			✓		✓					✓	✓	⊕
3	User	Manage Organization Events												⊕
1	admin	Manage & Publish Organization Events	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	⊕

Page 1 of 1, showing 7 records out of 7 total, starting on record 1, ending on 7

[« previous](#) [next »](#)

- **Id:** The role's automatically assigned ID number.
- **Name:** The name of role.
- **Permission:** One of the 4 permissions: Read Only, Manage My Own Events, Manage Organization Events, Manage & Publish Organisation Events.
- **Extra Permissions flag:** Flag for each extra permissions: Admin, Site Admin, Sync Actions, Audit Actions, Auth key access, Regex Actions, Tagger, Tag Editor, Template Editor, Sharing Group Editor, Delegations Access.
- **Action Buttons:** There are 2 options available: Edit Role or Delete it.
  - **Edit Role:** Same options of create role's view.

#### Edit Role

Name	Permissions
Automation user	Manage & Publish Organizational
<input type="checkbox"/> Perm Admin	<input type="checkbox"/> Perm Site Admin
<input type="checkbox"/> Perm Audit	<input checked="" type="checkbox"/> Perm Auth
<input type="checkbox"/> Perm Tagger	<input type="checkbox"/> Perm Tag Editor
<input type="checkbox"/> Perm Sharing Group	<input type="checkbox"/> Perm Delegate
<input type="button" value="Edit"/>	

- - 
  - **Delete Role:** Use this option to delete a role.

Are you sure you want to delete Read Only?





## Tools

MISP has a couple of administrative tools that help administrators keep their instance up to date and healthy. The list of these small tools can change rapidly with each new version, but they should be self-explanatory. Be sure to check this section after each upgrade to a new version, just in case there's a new upgrade script in there - though if this is the case it will be mentioned in the upgrade instructions.

### Administrative actions

- [reportValidationIssuesEvents](#)
- [reportValidationIssuesAttributes](#)
- [Reset the attribute counts](#) (Events need to have no validation issues.)
- [Recorrelate attributes](#)
- [Recorrelate proposals](#)
- [Verify GPG keys](#) (Check whether every user's GPG key is usable)
- [Verify Certificates](#) (Check whether every user's certificate is usable)
- [Extend Organization length](#) (Hotfix 2.3.57: Increase the max length of the organization field when adding a new server connection.)
- [Convert log fields to text](#) (Hotfix 2.3.78: Some of the log fields that were varchar(255) ended up truncating the data. This function will change them to "text")
- [Fix duplicate UUIDs](#) (Hotfix 2.3.107: It was previously possible to get duplicate attribute UUIDs in the database, this script will remove all duplicates and ensure that duplicates will not be entered into the database in the future.)
- [Remove duplicate events \(with the same UUID\)](#) (Hotfix 2.3.115: In some rare situations it could occur that a duplicate of an event was created on an instance, with the exact same uuid. This action will remove any such duplicates and make sure that this cannot happen again.)
- [Prune orphaned attributes](#) (In some rare occasions it can happen that you end up with some attributes in your database that do not belong to an event - for example during a race condition between an event insert and a delete. This tool will collect and delete any such orphaned attributes. If you ever run into an issue where you cannot add an attribute with a specific valid value, this is probably the reason.)
- [Clean regex table of potentially malicious entries](#) (Hotfix 2.3.160: Prior to this version it was possible for a user/admin with Regex permission to create a malicious regular expression that could be used to execute arbitrary code. Since this version it is no longer possible to input such expressions, but already existing malicious entries still have to be cleaned using this tool.)
- [Remove url type attribute sanitisation](#) (Hotfix 2.3.173: Sanitised URLs can cause issues with the NIDS exports and as of this version attributes will be modified on entry to correct this. To correct existing entries, run this script.)
- [Index tables](#) (This script will create indeces for all of the tables in MISP (other than primary keys))
- [Fix non-empty sharing group IDs](#) (This script will change the sharing\_group\_id to 0 in all non sharing group setting events and attributes))

### Upgrading a 2.3 instance to 2.4

Warning: Running these scripts below can result in the loss of data. Make sure that you back your database up before running them.

The order for the 2.4 upgrade procedure is:

1. [Upgrade to 2.4](#) - run this to migrate the 2.3 data to the 2.4 format
2. If it completes successfully, run the [2.3->2.4 cleanup script](#) to remove the fields that are specific to 2.3. Make sure that the migration of the data to the 2.4 format was successful (you can check the result in the audit logs). If you have run the 2.4 upgrade script previously but are running into SQL errors on the column 'org', run this script.

## Server Settings

Since version 2.3, MISP has a settings and diagnostics tool that allows site-admins to manage and diagnose their MISP installation. You can access this by navigating to Administration - Server settings.

### Server settings and diagnostics

Server settings		
Test	Value	Description
Overall health	Critical, your MISP instance requires immediate attention.	The overall health of your instance depends on the most severe unresolved issues.
Critical settings incorrectly or not set	1 incorrect settings.	MISP will not operate correctly or will be unsecure until these issues are resolved.
Recommended settings incorrectly or not set	0 incorrect settings.	Some of the features of MISP cannot be utilised until these issues are resolved.
Optional settings incorrectly or not set	6 incorrect settings.	There are some optional tweaks that could be done to improve the looks of your MISP instance.
Critical issues revealed by the diagnostics	0 issues detected.	Issues revealed here can be due to incorrect directory permissions or not correctly installed dependencies.

The settings and diagnostics tool is split up into several aspects, all accessible via the tabs on top of the tool. For any unset or incorrectly set setting, or failed diagnostic a number next to the tab name will indicate the number and severity of the issues. If the number is written with a red font, it means that the issue is critical. First, let's look at the various tabs:

- **Overview:** General overview of the current state of your MISP installation
- **MISP settings:** Basic MISP settings. This includes the way MISP handles the default settings for distribution settings, whether background jobs are enabled, etc
- **GnuPG settings:** GnuPG related settings.
- **Proxy settings:** HTTP proxy related settings.
- **Security settings:** Settings controlling brute-force protection and the application's salt key.
- **Misc settings:** Settings controlling debug options, please ensure that debug is always disabled on a production system.
- **Diagnostics:** The diagnostics tool checks if all directories that MISP uses to store data are writeable by the apache user. Also, the tool checks whether the STIX libraries and GnuPG are working as intended.
- **Workers:** Shows the background workers (if enabled) and shows a warning if they are not running. Admins can also restart the workers here.
- **Download report:** Download a report of all the settings visible in the tool, in JSON format.

#### Server settings

Priority	Setting	Value	Description	Error Message
Critical	MISP.baseurl	http://192.168.56.12	The base url of the application (in the format https://www.mymispinstance.com). Several features depend on this setting being correctly set to function.	The currently set baseurl does not match the URL through which you have accessed the page. Disregard this if you are accessing the page via an alternate URL (for example via IP address).
Critical	MISP.showorg	true	Setting this setting to 'False' will hide all organisation names / logos.	
Critical	MISP.email	andras.iklody@gmail.com	The e-mail address that MISP should use for all notifications	
Critical	MISP.default_event_distribution	Connected communities	The default distribution setting for events (0-3).	
Critical	MISP.default_attribute_distribution	Inherit from event	This default distribution applies for attributes, and it is 'Inherit' if you would like this attribute to default to the	

Each of the setting pages is a table with each row representing a setting. Coloured rows indicate that the setting is incorrect / not set and the colour determines the severity (red = critical, yellow = recommended, green = optional). The columns are as follows:

- **Priority:** The severity of the setting.
- **Setting:** The setting name.
- **Value:** The current value of the setting.
- **Description:** A description of what the setting does.
- **Error Message:** If the setting is incorrect / not set, this field will let the user know what is wrong.

## Server settings

Worker	Worker Id	Status	
cache	iglocska-VirtualBox:9340:cache	OK	
default	iglocska-VirtualBox:9311:default	OK	
email	iglocska-VirtualBox:9360:email	OK	
_schdler_	N/A	Worker not running!	

**Restart all workers** This will start/restart all of the workers and refresh the page. Keep in mind, this process can take a few seconds to complete, so refresh the page again in 5-10 seconds to see the correct results.

The workers tab shows a list of the workers that MISP can use. You can restart workers using the "restart all workers" button. If the button doesn't work, make sure that the workers were started using the apache user. This can however only be done using the command line, refer to the INSTALL.txt documentation on how to let the workers automatically start on each boot.

- **Worker Type:** The worker type is determined by the queue it monitors. MISP currently has 6 queues (cache, default, prio, email, update and a special *schdlr* queue).
- **Worker Id:** The ID is made up of the machine name, the PID of the worker and the queue it monitors.
- **Status:** Displays OK if the worker is running. If the *schdlr* worker is the only one not running, make sure that you copy the config file into the cakeresque directory as described in the INSTALL.txt documentation.

## Worker types

### **cache**

Role: Interdependence:

### **default**

Role: Interdependence:

### **email**

Role: Interdependence:

### **update**

Role: Interdependence:

### **prio**

Role: Interdependence:

### **scheduler**

Role: Interdependence:

## Workers dead

Even if the workers are dead, any actions related to them are on-hold. Nothing is lost. Simply restarting the worker will resume any operations.

You can either relaunch them via the UI or manually by running **sudo -u www-data bash**

**/var/www/MISP/app/Console/worker/start.sh** on the CLI. For reference, below is the script in question.

```
#!/usr/bin/env bash

# Check if run as root
if [ "$EUID" -eq 0 ]; then
    echo "Please DO NOT run the worker script as root"
    exit 1
fi

# Extract base directory where this script is and cd into it
cd "${0%/*}"
./cake CakeResque.CakeResque stop --all
./cake CakeResque.CakeResque start --interval 5 --queue default
./cake CakeResque.CakeResque start --interval 5 --queue prio
./cake CakeResque.CakeResque start --interval 5 --queue cache
./cake CakeResque.CakeResque start --interval 5 --queue email
./cake CakeResque.CakeResque startscheduler --interval 5

exit 0
```

## Import Blacklist

It is possible to ban certain values from ever being entered into the system via an event info field or an attribute value. This is done by blacklisting the value in this section.

### Adding and modifying entries

Administrators can add, edit or delete blacklisted items by using the appropriate functions in the list's action menu and the menu on the left.

## Import Regexp

The system allows administrators to set up rules for regular expressions that will automatically alter newly entered or imported events (from GFI Sandbox).

### The purpose of Import Regexp entries

They can be used for several things, such as unifying the capitalisation of file paths for more accurate event correlation or to automatically censor the usernames and use system path variable names (changing C:\Users\UserName\AppData\Roaming\file.exe to %APPDATA%\file.exe). The second use is blocking, if a regular expression is entered with a blank replacement, any event info or attribute value containing the expression will not be added. Please make sure the entered regexp expression follows the preg\_replace pattern rules as described [here](#)

### Adding and modifying entries

Administrators can add, edit or delete regular expression rules, these "expressions" are made up of a regex pattern that the system searches for and a replacement for the detected pattern.

<b>ID</b>	<b>Regexp</b>	<b>Replacement</b>	<b>Type</b>
1	/.: ProgramData./i	%ALLUSERSPROFILE%\\	ALL
2	/.: Documents and Settings.All Users./i	%ALLUSERSPROFILE%\\	ALL
3	/.: Program Files.Common Files./i	%COMMONPROGRAMFILES%\\	ALL
4	/.: Program Files (x86).Common Files./i	%COMMONPROGRAMFILES(x86)%\\	ALL
5	/.: Users.(w+).AppData.Local.Temp./i	%TEMP%\\	ALL
6	/.: ProgramData./i	%PROGRAMDATA%\\	ALL
7	/.: Program Files./i	%PROGRAMFILES%\\	ALL

## Managing the Signature whitelist

The signature whitelist view, accessible through the administration menu on the left, allows administrators to create and maintain a list of addresses that are whitelisted from ever being added to the [NIDS](#) signatures. Addresses listed here will be commented out when exporting the [NIDS](#) list.

### Whitelisting an address

While in the whitelist view, click on New Whitelist on the left to bring up the "add whitelist" view to add a new address.

### Managing the list

When viewing the list of whitelisted addresses, the following data is shown: The ID of the whitelist entry (assigned automatically when a new address is added), the address itself that is being whitelisted and a set of controls allowing you to delete the entry or edit the address.

#### Import Whitelist

		< previous	next >
Id	Name	Actions	
1	www.futuremark.com		

## Using MISP logs

Users with audit permissions are able to browse or search logs that MISP automatically appends each time certain actions are taken (actions that modify data or if a user logs in and out). Generally, the following actions are logged:

- **User:** Creation, deletion, modification, Login / Logout
- **Event:** Creation, deletion, modification, [publishing](#)
- **Attribute:** Creation, deletion, modification
- **ShadowAttribute:** Creation, deletion, Accept, Discard
- **Roles:** Creation, deletion, modification
- **Blacklist:** Creation, deletion, modification
- **Whitelist:** Creation, deletion, modification
- **Regexp:** Creation, deletion, modification

## Browsing logs

Listing all the log entries will display the following columns generated by the users of your organisation (or all organisations in the case of site admins):

### Logs

<a href="#">« previous</a>	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	<a href="#">next »</a>
<b>ID</b>	<b>Email</b>	<b>Org</b>	<b>Created</b>	<b>Action</b>	<b>Title</b>															<b>Change</b>		
1936	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (44) from Event (1): Payload installation/md5 7388d67561d0a7989202ad4d37eff24f															event_id () => (1), uuid () => (d525d2c9-		
1935	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (43) from Event (1): Payload installation/md5 6fdec862951e6b128cd7a07b2031eeef6															event_id () => (1), uuid () => (f0444f6b-<		
1934	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (42) from Event (1): Payload installation/md5 6d2320af561b2315c1241e3efd06067f															event_id () => (1), uuid () => (5023dbc8-		
1933	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (41) from Event (1): Payload installation/md5 68c67a6e26b55ebc2569d67689c69a6e															event_id () => (1), uuid () => (aeff94cef-d		
1932	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (40) from Event (1): Payload installation/md5 6670163cd34454b3d1476c134d44b9d9															event_id () => (1), uuid () => (8d300eb0-		

- **Id:** The automatically assigned ID number of the entry.
- **Email:** The e-mail address of the user whose actions triggered the entry.
- **Org:** The organisation of the above mentioned user.
- **Created:** The date and time when the entry originated.
- **Action:** The action's type. This can include: login/logout for users, add, edit, delete for events, attributes, users and servers.
- **Title:** The title of an event always includes the target type (Event, User, Attribute, Server), the target's ID and the target's name (for example: e-mail address for users, event description for events).
- **Change:** This field is only populated for entries with "add" or "edit" actions. The changes are detailed in the following format: `_variable (initial_value) => (new_value),...` When the entry is about the creation of a new item (such as adding a new event) then the change will look like this for example: `org() => (ADMIN), date() => (20012-10-19),...`

### Search Logs

Email	Organisation
<input type="text"/>	<input type="text"/>
Action	
<input type="text"/> ALL	<input type="button" value="▼"/>
Title	Change
<input type="text"/>	<input type="text"/>
<input type="button" value="Search"/>	

## Searching Logs

Another way to browse the logs is to search it by filtering the results according to the following fields (the search is a sub-string search, the sub-string has to be an exact match for the entry in the field that is being searched for):

- **Email:** By searching by Email, it is possible to view the log entries of a single user.
- **Org:** Searching for an organisation allows you to see all actions taken by any member of the organisation.
- **Action:** With the help of this drop down menu, you can search for various types of actions taken (such as logins, deletions, etc).
- **Title:** There are several ways in which to use this field, since the title fields contain several bits of information and the search searches for any substrings contained within the field, it is possible to just search for the ID number of a logged event, the username / server's name / event's name / attributes name of the event target.
- **Change:** With the help of this field, you can search for various specific changes or changes to certain variables (Ex.: using "Published" as the search term for and find all log entries where an event has been "Published", ip-src will find all attributes where a source IP address has been entered / edited, etc).

## Background Processing

If enabled, MISP can delegate a lot of the time intensive tasks to the background workers. These will then be executed in sequence, allowing the users of the instance to keep using the system without a hiccup and without having to wait for the process to finish. It also allows for certain tasks to be scheduled and automated.

## Command Line Tools for the Background Workers

The background workers are powered by [CakeResque](#), so all of the CakeResque commands work. To start all of the workers needed by MISP go to your `/var/www/MISP/app/Console/worker` (assuming a standard installation path) and execute `start.sh`. To interact with the workers, here is a list of useful commands. Go to your `/var/www/MISP/app/Console` (assuming a standard installation path) and execute one of the following commands as a parameter to `./cake CakeResque` (for example: `./cake CakeResque tail`):

- **start:** Start a new worker.
- **startscheduler:** Start a new scheduler worker.
- **stop:** Stop a worker.
- **pause:** Pause a worker.
- **resume:** Resume a paused worker.
- **cleanup:** Terminate the job that a worker is working on with immediate effect. You will be presented with a choice of workers to choose from when executing this command.
- **restart:** Stop all Resque workers, and start a new one.
- **clear:** Clear all jobs inside a queue
- **reset:** Reset CakeResque internal worker's saved status
- **stats:** Display some statistics about your workers including the count of successful and failed jobs.
- **tail:** Tail the various (workers) log files that CakeResque creates, just choose the one from the list that you are interested in.
- **track:** Track a job status.
- **load:** Load a set of predefined workers.

The other commands should not be required, instead of starting / stopping or restarting workers use the supplied `start.sh` (it stops all workers and starts them all up again). For further instructions on how to use the console commands for the workers, visit the [CakeResque list of commands](#).

## Monitoring the Background Processes

The "Jobs" menu item within the Administration menu allows site admins to get an overview of all of the current and past

The "Jobs" menu item within the Administration menu allows site admins to get an overview of all of the current and past scheduled jobs. Admins can see the status of each job, and what the queued job is trying to do. If a job fails, it will try to set an error message here too. The following columns are shown in the jobs table:

- **Id:** The job's ID (this is the ID of the job's metadata stored in the default datastore, not to be confused with the process ID stored in the redis database and used by the workers)
- **Process:** The process's ID.
- **Worker:** The name of the worker queue. There are 3+1 workers running if background jobs are enabled: default, cache, email, and a special Scheduler (this should never show up in the jobs table).
- **Job Type:** The name of the queued job.
- **Input:** Shows a basic input handled by the job - such as "Event:50" for a publish email alert job for event 50.
- **Message:** This will show what the job is currently doing or alternatively an error message describing why a job failed.
- **Org:** The string identifier of the organisation that has scheduled the job.
- **Status:** The status reported by the worker.
- **Retries:** Currently unused, it is planned to introduce automatic delayed retries for the background processing and thus add resilience.
- **Progress:** A progress bar showing how the job is coming along.

## Jobs

<a href="#">« Previous</a>											<a href="#">1</a>	<a href="#">2</a>	<a href="#">3</a>	<a href="#">4</a>	<a href="#">5</a>	<a href="#">6</a>	<a href="#">7</a>	<a href="#">8</a>	<a href="#">9</a>	<a href="#">10</a>	<a href="#">11</a>	<a href="#">12</a>	<a href="#">13</a>	<a href="#">14</a>	<a href="#">15</a>	<a href="#">16</a>	<a href="#">17</a>	<a href="#">18</a>	<a href="#">19</a>	<a href="#">20</a>	<a href="#">21</a>	<a href="#">next »</a>
<b>Id</b>	<b>Process</b>	<b>Worker</b>	<b>Job Type</b>	<b>Input</b>	<b>Message</b>			<b>Org</b>	<b>Status</b>	<b>Retries</b>	<b>Progress</b>																					
3993	efd41ac4bb4ca08a4177743b85ba20c0	default	publish_event	Event ID: 3	Event published.			ADMIN	Completed	0	<div style="width: 100%;">Completed</div>																					
3992	77f5d4d84cc3dc8e7601c3f104b225ad	default	publish_event	Event ID: 1	Event published.			ADMIN	Completed	0	<div style="width: 100%;">Completed</div>																					
3991	1aa67e0a132ed8c0e76b370557ff97f5	default	publish_event	Event ID: 2	Event published.			ADMIN	Completed	0	<div style="width: 100%;">Completed</div>																					
3990	380b4a993eb315537c3fc7fa7298b40	default	publish_event	Event ID: 1	Event published.			ADMIN	Completed	0	<div style="width: 100%;">Completed</div>																					
3989	03718c777c3d0ded2ead8564ae24f85d	default	publish_alert_email	Event: 77	Emails sent.			ADMIN	Completed	0	<div style="width: 100%;">Completed</div>																					

## Scheduling Jobs and Recurring Jobs

Apart from off-loading long-lasting jobs to the background workers, there is a second major benefit of enabling the background workers: Site-administrators can schedule recurring tasks for the jobs that generally take the longest to execute. At the moment this includes pushing / pulling other instances and generating a full export cache for every organisation and export type. MISp comes with these 3 tasks pre-defined, but further tasks are planned. The following fields make up the [scheduled tasks](#) table:

- **Id:** The ID of the task.
- **Type:** The type of the task.
- **Frequency (h):** This number sets how often the job should be executed in hours. Setting this to 168 and picking the next execution on Sunday at 01:00 would execute the task every Sunday at 1 AM. Setting this value to 0 will make the task only run once on the scheduled date / time without rescheduling it afterwards.
- **Scheduled Time:** The time (in 24h format) when the task should be executed the next time it runs (and all consecutive times if a multiple of 24 is chosen for frequency).
- **Next Run:** The date on which the task should be executed.
- **Description:** A brief description of the task.
- **Message:** This field shows when the job was queued by the scheduler for execution.

### Scheduled Tasks

Here you can schedule pre-defined tasks that will be executed every x hours. You can alter the date and time of the next scheduled execution and the frequency at which it will be repeated (expressed in hours). If you set the frequency to 0 then the task will not be repeated. To change any of the above mentioned settings just click on the appropriate field and hit update all when you are done editing the scheduled tasks.

[« previous](#)
[next »](#)

<b>Id</b>	<b>Type</b>	<b>Frequency (h)</b>	<b>Scheduled Time</b>	<b>Next Run</b>	<b>Description</b>	<b>Message</b>
3	push_all	0	12:00	2014-02-05	Initiates a full push for all eligible instances.	Not scheduled yet.
2	pull_all	0	12:00	2014-02-05	Initiates a full pull for all eligible instances.	Not scheduled yet.
1	cache_exports	36	18:00	2014-02-20	Generates export caches for every export type and for every organisation. This process is heavy, schedule so it might be a good idea to schedule this outside of working hours and before your daily automatic imports on connected services are scheduled.	32 jobs started at 20/02/2014 - 17:01:27

[Update all](#)

## Various administration tips & tricks

### Setting a Publish Alert Filter

To regulate the reception of e-mail from MISP it is possible to create filters. Each individual user account can apply such filter.

The filter can be configured by the user but also by the organization administrator.

After login goto Administration -> Set User Setting:

The screenshot shows the MISP administration interface. At the top, there is a navigation bar with links: Event Actions, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, and Audit. The 'Administration' link is highlighted. A dropdown menu is open under 'Administration', listing several options: List Users, List User Settings, Set User Setting, Add User, Contact Users, List Organisations, and Add Organisations. The 'Set User Setting' option is highlighted with a blue background. On the left, there is a sidebar with a 'List Events' section containing links for IOC Taak TODO, IOC Taak Review, Add Event, Import from..., REST client, and List Attributes. The main content area is titled 'Events' and shows search and filtering options: 'My Events' and 'Org Events'. Below these are buttons for 'Published', 'Org', 'Owner org', 'Id', and 'Clusters'.

A new screen appears. Make sure the “Setting” drop down box shows “publish\_alert\_filter”:

The screenshot shows a user interface for setting a user configuration. On the left is a sidebar with a navigation menu. The 'Set Setting' option is highlighted with a blue bar at the top. Other options include My Profile, My Settings, Dashboard, List Organisations, Role Permissions, List Sharing Groups, Add Sharing Group, User Guide, Terms & Conditions, and Statistics. The main content area is titled 'Set User Setting'. It has three input fields: 'User' (a dropdown menu), 'Setting' (a dropdown menu set to 'publish\_alert\_filter'), and 'Value' (a text area containing a JSON example). Below the Value field is a 'Submit' button.

Set User Setting

User

Setting

Value

Example:

```
{  
  "AND": {  
    "NOT": {  
      "EventTag.name": [  
        "%osint%"  
      ]  
    }  
  }  
}
```

Submit

The text field “Value” contains the filter, which needs to be provided in JSON format. Important JSON-objects which can be used here go by the name AND”, “OR” and “NOT”. These should be structured in a logical tree.

The filtering can be applied to tags or to a [publishing organization](#).

In the following example, all notifications will be filtered which carry ‘tlp.white’ and ‘tlp.green’ in the name of the tag:

```
{
  "NOT": {
    "Tag.name" : [ "tlp.white", "tlp.green" ]
  }
}
```

The publish\_alert\_filter setting allows one filter definition to be active.

After applying the configuration, the filter will show up in the “My Settings” menu:

The screenshot shows the 'User settings management' page. The left sidebar has a 'My Settings' tab selected, which is highlighted in blue. The main content area displays a table of user settings. There is one record in the table:

Id	User	Setting	Value
1		publish_alert_filter	<pre>{   "NOT": {     "Tag.name": [       "tlp.white",       "tlp.green"     ]   } }</pre>

Below the table, a message states: "Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1". Navigation buttons "« previous" and "next »" are also visible.

## Default sharing level

Choose your default sharing level to match your usage scenario for MISP. The setting is named `default_event_distribution` and the values can be:

- Your organisation only (default)
- This community only
- Connected communities
- All communities

You can also set a default distribution level for attributes contained in an event with `default_attribute_distribution`, and it has the same values as the default sharing level for events plus an additional one that allows attributes to inherit the sharing level of the event.

## Adding organisation logos

You can add a logo for your organisations in MISP by uploading them via the tab **Manage files** under the **Administration** menu & **Server Settings** sub-menu. The filename must be exactly the same as the organisation name that you will use in MISP. It is recommended to use PNG files of 48x48 pixels.

## The \_schdlr\_ worker is not starting

If you already made sure that you copied the config file under the cakeresque directory, it might be due to the FQDN of the server hosting the instance has changed. A way to fix this is to flush temporary data stored in redis. This can be done by logging in redis, for example when logging in with redis-cli, and issuing a flushall command.

## How to redirect HTTP to HTTPS

Here is a sample configuration for Apache webserver.

```
<VirtualHost *:80>
    ServerAdmin misp@misp.misp
    ServerName misp.misp.misp
    ServerAlias misp-int.misp.misp

    Redirect permanent / https://misp.misp.misp

    LogLevel warn
    ErrorLog /var/log/apache2/misp.local_error.log
    CustomLog /var/log/apache2/misp.local_access.log combined
    ServerSignature Off
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin misp@misp.misp
    ServerName misp.misp.misp
    ServerAlias misp-int.misp.misp

    DocumentRoot /var/www/MISP/app/webroot
    <Directory /var/www/MISP/app/webroot>
        Options -Indexes
        AllowOverride all
        Order allow,deny
        allow from all
    </Directory>

    SSLEngine On
    SSLCertificateFile /etc/ssl/misp.misp.misp/misp.crt
    SSLCertificateKeyFile /etc/ssl/misp.misp.misp/misp.key
```

```
SSLCertificateChainFile /etc/ssl/misp.misp.misp/mispCA.crt

LogLevel warn
ErrorLog /var/log/apache2/misp.local_error.log
CustomLog /var/log/apache2/misp.local_access.log combined
ServerSignature Off
</VirtualHost>
```

Taken from [Koen Van Impe's blog](#)

## Increase max size of Samples / other files

Trying to upload a large samples (>50M) might cause the following error: [!] 500 Server Error: Internal Server Error

Or will give you an error page in browser.

The error logs on the system will display the following:

```
PHP Warning: POST Content-Length of 57526024 bytes exceeds the limit of 8388608 bytes in Unknown on line 0, referer: https://XYZ/attributes/add_attachment/1948
```

And / Or

```
PHP Fatal error: Allowed memory size of 134217728 bytes exhausted (tried to allocate 76705009 bytes) in /var/www/MISP/app/Lib/cakephp/lib/Cake/Network/CakeRequest.php on line 996
```

To fix that you need to adjust the php settings:

```
vi /etc/php5/apache2/php.ini
```

Increase to the following values (or more if you want to)

```
; Maximum size of POST data that PHP will accept.
; Its value may be 0 to disable the limit. It is ignored if POST data reading
; is disabled through enable_post_data_reading.
; http://php.net/post-max-size
post_max_size = 256M
[...]
; Maximum amount of memory a script may consume (128MB)
; http://php.net/memory-limit
memory_limit = 1024M
```

And then restart apache2

```
service apache2 restart
```

## Support & feature requests

The preferred method for support & feature requests is to use the [GitHub ticketing system](#).

If you want to discuss something related to MISP, want some help from the community, etc... You have the [MISP Users mailing list](#) and the [MISP developers mailing list](#).

A number of companies offer custom development, consulting, and support around MISP, please check [the support page of the MISP Project website](#).

## More information in the notification emails about new events

The setting MISP.extended\_alert\_subject allows you to have an extended subject. One word of warning though. If you're using encryption : the subject will not be encrypted. Be aware that you might leak some sensitive information this way. Below is an example how the two subject types look like. First with the option disabled, then with the option enabled.

```
Event 7 - Low - TLP Amber
Event 8 - OSINT - Dissecting XXX... - Low - TLP Amber
```

Taken from [Koen Van Impe's blog](#)

## Get top API users

Enable the *log\_auth* setting in the server settings. Optionally enable *log\_client\_ip* if you want to get stats per client ip. Log into your mysql server and run the following query:

```
select ip,email,count(id) as c from logs WHERE ip IS NOT NULL group by ip,email order by c desc limit 10;
```

This will give you a top 10 table per ip and username:

ip	email	c
1.2.3.4	bob@nsa.gov	4124
5.6.7.8	vladimir@kremlin.ru	1932
9.10.11.12	fred@somewhere.eu	1317
13.14.15.16	SYSTEM	16

## MISP Logs

By default, MISP has several layers of logs that can be used to trouble-shoot and monitor the system. Let's walk through each of the available logs:

- **Apache access logs:** Rotating logs generated by apache, logging each request, by default (on Ubuntu) they are found in `/var/log/apache2/misp.local_access.log`. The location can be changed via the apache conf file
- **Apache error logs:** Rotating logs generated by apache, logging error messages, by default (on Ubuntu) they are found in `/var/log/apache2/misp.local_error.log`. This error log file will generally not be used by MISP, however, if there is a PHP level error that prevents MISP from functioning you might have relevant entries here.
- **MISP error log:** Generated by MISP, logging any exceptions that occur during usage. These can be found in `/var/www/MISP/app/tmp/logs/error.log` (assuming default installation path). If you see errors in here and are stuck with an issue [let us know via GitHub!](#)
- **MISP debug log:** Generated by MISP, any debug messages and Notice level messages will be sent to this file. Generally less interesting, but can be helpful during debugging sessions. It should not be necessary to monitor this under normal usage. The file can be found in `/var/www/MISP/app/tmp/logs/debug.log` (assuming default installation path).
- **MISP worker error log:** Generated by MISP background workers, logging any exceptions generated during a background job. It is the equivalent of the MISP error log for background jobs, so if [scheduled tasks](#), [synchronisation](#) or e-mailing with the workers enabled are causing issues, this is the place to check. It can normally be found at `/var/www/MISP/app/tmp/logs/resque-worker-error.log`
- **MISP worker logs:** Rotating logs generated by MISP background workers, logging any jobs executed by workers. This is part of the normal operation of background workers and doesn't have to be monitored, though it can help when debugging issues. Normally found at `/var/www/MISP/app/tmp/logs/resque-[current date].log`
- **MISP scheduler error log:** Generated by MISP scheduler worker, logging any exceptions generated during the scheduling

of a background job. It is the equivalent of the MISP error log for scheduled jobs. It can normally be found at `/var/www/MISP/app/tmp/logs/resque-scheduler-error.log`

- **MISP scheduler logs:** Rotating logs generated by MISP scheduler worker, logging any scheduling of jobs to be executed by workers. This is part of the normal operation of the scheduler worker and doesn't have to be monitored, though it can help when debugging issues. Normally found at `/var/www/MISP/app/tmp/logs/resque-scheduler-[current date].log`

## Logging of failed authentication attempts

By default, MISP logs all failed login and authentication attempts in the built in Audit logs. To view any such failed attempts, simply log in as a [site admin](#) and navigate to Audit - List logs.

There are two types of entries that will be interesting if you are looking for failed authentication attempts, entries of action "auth\_fail" (for failed attempts to authenticate via the [API](#) key or the external authentication system) and login\_fail (for failed login attempts via the login page).

You can also search for any such entries using the Search Logs feature, simply choose the desired action from the two listed above and hit search.

What is logged:

Auth method	Action	Failed credentials logged	IP
Webform	login_fail	None	Optional
API	auth_fail	API key	Optional
Webform	auth_fail	External auth key	Optional

In order to enable IP logging for any logged request in MISP, navigate to Administration - Server settings - MISP settings and enable the `MISP.log_client_ip` setting.

It is also possible to enable full logging of [API](#) and external authentication requests using the `MISP.log_auth` setting in the same location, but keep in mind that this is highly verbose and will log every request made. In addition to the information above, all accessed resource URLs are also logged.

## Clearing expired sessions

By default the garbage collection of sessions is disabled in PHP. It is possible to enable it, but it's not recommended and as such MISP provides a manual way of clearing the sessions.

Navigate to the diagnostics screen of MISP (Administration - Server settings - Diagnostics) and near the bottom of the page there will be a counter showing the count of currently stored expired sessions. Simply purge them by clicking the applicable button when the number grows too large.

## Troubleshooting MISP not connecting to redis but redis-cli working

If you have an IPv6 enabled OS, but an older redis version that does not support IPv6 (<v2.8), MISP might fail to connect to the redis server while redis-cli is working. The reason is that redis-cli is connecting to 127.0.0.1 directly, while the calls inside the CakeResque library used by MISP are done using "`localhost`" which resolves both to the IPv4 and IPv6 loopback addresses. For some reasons, the use of the IPv6 address is attempted first which fails.

You can confirm this by trying to connect to redis using **telnet localhost 6379**. If it fails, the error message should mention the IPv6 loopback address (":1").

Two ways to fix it:

- 1) Upgrade your redis to a server that supports IPv6 (v2.8+). This is the preferred recommendation.

2) Comment the localhost mapping to IPv6 address in /etc/hosts

## Errors about fields or tables

If you have errors with fields or tables that you can see in the error.log or in the page (if you enabled *debug* or *site\_admin\_debug* settings), an easy fix to make most of them go away is to use the **clean cache** feature on the *server settings* menu, *diagnostics* tab. An example of error message:

```
Error: [PDOException] SQLSTATE[42S22]: Column not found: 1054 Unknown column 'Task.job_id' in 'field list'
```

## Jobs

The Jobs tab gives you an overview on any currently running jobs or jobs that were previously completed and their status.



Typically this is one of the places you would turn to even some background process might not complete as expected to get an indication on any issues related to user initiated Jobs.

For ease of use, you can filter the Jobs by 'All', 'Default', 'Email', 'Cache'

#### **TODO: Explain differences Default, Email, Cache**

You can also purge the entries, either only by completed status or purge all. This is not automated and needs to be done manually.

## Scheduled Tasks

Straight from the UI:

"" Here you can schedule pre-defined tasks that will be executed every x hours. You can alter the date and time of the next scheduled execution and the frequency at which it will be repeated (expressed in hours). If you set the frequency to 0 then the task will not be repeated. To change and of the above mentioned settings just click on the appropriate field and hit update all when you are done editing the [scheduled tasks](#).

Warning: [Scheduled tasks](#) come with a lot of caveats and little in regards of customisations / granularity. You can instead simply create cron jobs out of the console commands as described here: Automating certain console tasks ""

The task scheduler is a sub-par component to enable minimal functionality in terms of automating certain MISP tasks. If you have a dedicated and concious MISP [Site Admin](#) she can keep an eye on the Scheduler to make sure everything runs smoothly.

For better performance please use a real scheduler like your systems' crontab. As a rule of thumb: If you can click on it, MISP can automate it.

## MISP Backup

Currently there exists this backup script simply called [misp-backup.sh](#)

All you need is to copy the sample config and make sure it is correct. Then launch the script.

```
cd /var/www/MISP/tools/misp-backup
sudo -u www-data cp misp-backup.conf.sample misp-backup.conf
sudo ./misp-backup.sh
```

Script output:

```
/var/www/MISP/tools/misp-backup ↵ 2.4 • $ sudo ./misp-backup.sh
File ./misp-backup.conf exists.
copy of org images and other custom images
MySQL Dump
/var/www/MISP/tools/misp-backup
MISP Backup Completed, OutputDir: /opt/backup
FileName: MISP-Backup-20181128_163215.tar.gz
FullName: /opt/backup/MISP-Backup-20181128_163214.tar.gz
```

## MISP Restore

In a similar fashion you can restore your [MISP instance](#) with the [misp-restore.sh](#) script. Read the script for details.

Last modified: Tue Nov 07 2017 15:35:13 GMT+0100 (CET)

- [Feeds](#)
  - [Managing feeds](#)
    - [Adding feeds](#)
  - [Feed correlation](#)

## Feeds

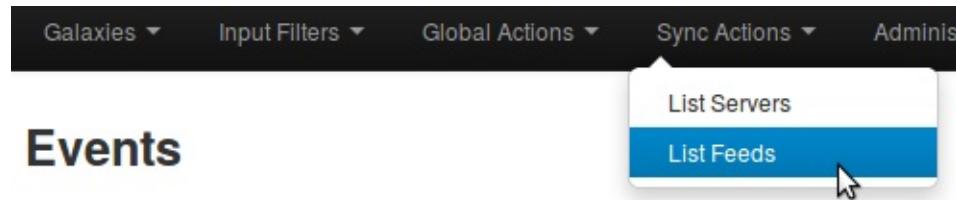
Feeds are remote or local resources containing [indicators](#) that can be automatically imported in MISP at regular intervals. Feeds can be structured in [MISP format](#), CSV format or even free-text format. You can easily import any remote or local URL to store them in your [MISP instance](#). It's a simple way to gather many external sources of information without any programming skills into MISP.

Feeds description can be also easily shared among different MISP instances as you can export a feed description as JSON and import it back in another [MISP instance](#).

## Managing feeds

[warning] A [site admin](#) role is required to perform these actions.

To do so, you first need to access the list of feeds, using the top menu.



## Adding feeds

Then select the add feed option on the side menu.

The screenshot shows a user interface for managing feeds. At the top, there is a dark header bar with four items: "Home", "Event Actions ▾", "Galaxies ▾", and "Input Filters ▾". Below this is a sidebar on the left with a blue header "List Feeds" containing three options: "Add Feed", "Import Feeds from JSON", and "Import Feeds from URL". To the right of the sidebar, the main content area has a large title "Feeds" and two small buttons at the bottom: "« previous" and "next »".

Here you will have access to a dynamic form. Let's check each field by order.

## Add MISP Feed

Add a new MISP feed source.

Enabled

Name

Feed name

Provider

Name of the content provider

Input Source

Local

Remove input after ingestion

Url

URL of the feed

Source Format

MISP Feed

Distribution

All communities

Default Tag

None

**Filter rules:**

**Modify**

**Add**

- Enabled: Is the feed active or not
- Lookup Visible: If this is not checked, the correlation will only show up to you, if checked, correlations are visible for other users as well
- Name: Just a name to identify the feed
- Provider: Name of the content provider
- Input Source: Where does the input come from

#### Input Source



- 

- Network: hosted somewhere outside the platform
- Local: Hosted on the local server. On this case, a new checkbox "Remove input after ingestion" will appear. If checked, the source is deleted after usage.

#### Input Source

Local	
-------	---

Remove input after ingestion

- -
- Url: Url of the feed, where it is located (for Local hosted files, point to the manifest.json e.g. /home/user/feed-generator/output/manifest.json)
- The Source Format can be:

#### Source Format



- MISP Feed: The source points to a list of json formated like MISP events.

Example: <https://www.circl.lu/doc/misp/feed-osint>

- Freetext Parsed Feed:

**Source Format**

Freetext Parsed Feed

**Target Event**

New Event Each Pull

**Target Event ID**

Leave blank unless you want to reuse an existing event.

**Exclusion Regex**

Regex pattern, for example: "/^https://myfeedurl/i"

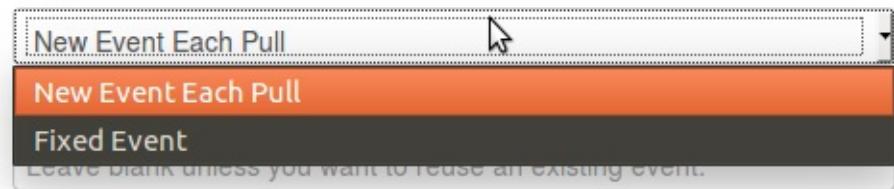
Auto Publish

Override IDS Flag

Delta Merge

- -

- Target Event: Which will be the event getting updated with the data from the feed. Can be either "New Event Each Pull" (A new event will be created each time the feed is pulled) or "Fixed Event" (A unique event will be updated with the new data. This event is determined by the next field)

**Target Event**

- - - Target Event ID: The id of the event where the data will be added (if not set, the field will be set the first time the feed is fetched)
    - Exclusion Regex: Add a regex pattern for detecting iocs that should be skipped (this can be useful to exclude any references to the actual report / feed for example)
    - Auto Publish: If checked, events created thanks to the feed will be automatically published
    - Override IDS Flag: If checked, the IDS flag will be set to false
    - Delta Merge: If checked, only data coming from the last fetch are kept, the old ones are deleted.
  - Simple CSV Parsed Feed:

**Source Format****Simple CSV Parsed Feed****Target Event****New Event Each Pull****Target Event ID**

Leave blank unless you want to reuse an existing event.

**Value field(s) in the CSV**

2,3,4 (column position separated by commas)

**Delimiter**

,

**Exclusion Regex**

Regex pattern, for example: "/^https://myfeedurl/i"

- Auto Publish
- Override IDS Flag
- Delta Merge

- - - Target Event: Which will be the event getting updated with the data from the feed. Can be either "New Event Each Pull" (A new event will be created each time the feed is pulled) or "Fixed Event" (A unique event will be updated with the new data. This event is determined by the next field)
    - Target Event ID: The id of the event where the data will be added (if not set, the field will be set the first time the feed is fetched)
    - Exclusion Regex: Add a regex pattern for detecting iocs that should be skipped (this can be useful to exclude any references to the actual report / feed for example)
    - Value field(s) in the CSV: Select one or several fields that should be parsed by the CSV parser and converted into MISP attributes
    - Delimiter: Set the default CSV delimiter (default = ",")
    - Auto Publish: If checked, events created thanks to the feed will be automatically published
    - Override IDS Flag: If checked, the IDS flag will be set to false
    - Delta Merge: If checked, only data coming from the last fetch are kept, the old ones are deleted.
- Distribution: Define the distribution option that will be set on the event created by the feed
- Default Tag: A default tag can be added to the created event(s)
- Filter rules: Here you can define which tags or organisations are allowed or blocked.

### Set pull rules

**Allowed Tags**

<< >>

<< >>

**Blocked Tags**

**Allowed Organisations**

<< >>

<< >>

**Blocked Organisations**

- 

To add a tag (resp. organisation), first type it into the top middle (resp. bottom middle) text field . Then use the arrows that point to the outside to add it to the allowed or blocked tags (resp. organisations) list.

### Set pull rules

**Allowed Tags**

<< >> tlp:green << >>

**Blocked Tags**

<< >>

**Allowed Organisations**

<< >>

**Blocked Organisations**

<< >>

**Update** **Cancel**

## Set pull rules

**Allowed Tags**

tlp:white

<< >> |

**Blocked Tags**

tlp:green

**Allowed Organisations**

<< >> |

**Blocked Organisations**

**Update** **Cancel**

This screenshot shows a configuration interface for 'pull rules'. It features four main sections: 'Allowed Tags' (containing 'tlp:white'), 'Blocked Tags' (containing 'tlp:green'), 'Allowed Organisations' (empty), and 'Blocked Organisations' (empty). Each section includes a central input field with navigation arrows ('<<', '>>') on either side. At the bottom left is a blue 'Update' button, and at the bottom right is a dark grey 'Cancel' button.

To remove a tag (resp. organisation), select it in the list and click on the arrow pointing to the inside.

## Set pull rules

**Allowed Tags**

tlp:white

<<>>

tlp:green

**Blocked Tags**

**Allowed Organisations**

<<>>

**Blocked Organisations**

Update Cancel

## Set pull rules

**Allowed Tags**

Empty list area.

Buttons: << >>

Text input field: (empty)

Buttons: << >>

**Blocked Tags**

Blocked tag: tlp:green

Empty list area.

**Allowed Organisations**

Empty list area.

Buttons: << >>

Text input field: (empty)

Buttons: << >>

**Blocked Organisations**

Empty list area.

**Buttons:**

Update      Cancel

## Feed correlation

If an indicator from a feed matches an indicator within a [MISP event](#), it will show up as "Feed hits" in the event overview. The correlation will not show up in the correlation graph of the event.

*Last modified: Thu Nov 07 2019 09:38:30 GMT+0100 (CET)*

# Updating Python Dependencies

MISP requires a couple of python libraries to be installed for the entire set of functionalities to work properly.

These functionalities include for instance the different import and export tools, the binaries extraction from attachments or PyMISP.

---

## Installation

We started using virtual environments in MISP to make the installation and maintenance of the python versions easier.

Either using the [installation script](#) to setup a running MISP on your machine, or starting using the automatically generated [virtual machine](#) will give you access to the latest version of the required python libraries installed within a virtual environment called `virtualenv`.

But if you are using an older MISP version, you may want to install the virtual environment

### Set the virtual environment up

```
# Create a python3 virtualenv
sudo -H -u www-data virtualenv -p python3 /var/www/MISP/venv

# Make pip happy
sudo mkdir /var/www/.cache
sudo chown www-data:www-data /var/www/.cache
```

If you already have a `venv` directory, you can skip this step

---

## Updating MISP and its dependencies

Keeping MISP up-to-date as much as possible is the safest way to avoid most of the potential issues.

It can be done either by using the Update button in the diagnostic tool available with the MISP UI, or by using the command line.

### Updating MISP core

In order to update MISP dependencies, we first want to [pull](#) the latest MISP version, so we have the latest submodule references as well.

## MISP version

Every version of MISP includes a json file with the current version. This is checked against the latest tag on github, if there is a version mismatch the tool will warn you about it. Make sure that you update MISP regularly.

Currently installed version... v2.4.117 (b825e44a3988db8430089b0ebf787af272e06f88)

Latest available version... v2.4.117 (b825e44a3988db8430089b0ebf787af272e06f88)

Status... OK

Current branch 2.4

[Update MISP](#)

[Update Progress](#)

OR

```
sudo -H -u www-data git pull origin 2.4
```

Once we have the latest MISP update, we can start updating the python libraries.

## Updating the python dependencies

MISP is provided with a lot of submodules used to ensure all the additional functionalities work as expected. Thus it is important to keep those dependencies up-to-date.

```
sudo -H -u www-data git submodule update --init --recursive
```

## Updating python dependencies

It is possible to check the status of all the python libraries required by MISP, using again the diagnostic tool.

### Advanced attachment handler

The advanced attachment tools are used by the add attachment functionality to extract additional data about the uploaded sample.

```
pydeep:... OK  
lief:... OK  
magic:... OK  
pymisp:... OK
```

### STIX and Cybox libraries

Mitre's STIX and Cybox python libraries have to be installed in order for MISP's STIX export to work. Make sure that you install them (as described in the MISP installation instructions) if you receive an error below.

If you run into any issues here, make sure that both STIX and CyBox are installed as described in the INSTALL.txt file. The required versions are:

```
STIX: >1.2.0.6  
CyBox: >2.1.0.18.dev0  
mixbox: 1.0.3  
maec: >4.1.0.14  
STIX2: >1.2.0  
PyMISP: >2.4.93
```

Other versions might work but are not tested / recommended.

```
Current libraries status...OK  
STIX library version...OK  
CYBOX library version...OK  
MIXBOX library version...OK  
MAEC library version...OK  
STIX2 library version...OK  
PYMISP library version...OK
```

### Yara

This tool tests whether plyara, the library used by the yara export tool is installed or not.

```
plyara library installed...OK
```

If something is going wrong, updating the corresponding library will make the diagnostic happy.

```
# Update PyMISP
cd /var/www/MISP/PyMISP
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .

# Update the advanced attachment handler libraries (PICK THE ONE.S YOU NEED TO UPDATE)
# pydeep
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U git+https://github.com/kbandla/pydeep.git
# lief
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U https://github.com/lief-project/packages/raw/lief-mas
ter-latest/pylief-0.9.0.dev.zip
# python-magic
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U python-magic

# Update the STIX dependencies (PICK THE ONE.S YOU NEED TO UPDATE)
# STIX
cd /var/www/MISP/app/files/scripts/python-stix
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .
# mixbox
cd /var/www/MISP/app/files/scripts/mixbox
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .
# Cybox
cd /var/www/MISP/app/files/scripts/python-cybox
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .
# MAEC
cd /var/www/MISP/app/files/scripts/python-maec
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .
# STIX 2
cd /var/www/MISP/cti-python-stix2
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .

# Update Yara python library
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U plyara
```

Note that if any of the STIX, Cybox, mixbox or MAEC update fails because of a `No such file or directory` error, you just have to `git clone` them and start again the `pip` command above.

```
cd /var/www/MISP/app/files/scripts
sudo -H -u www-data git clone https://github.com/Cyb0XProject/python-cybox.git
sudo -H -u www-data git clone https://github.com/STIXProject/python-stix.git
sudo -H -u www-data git clone https://github.com/MAECProject/python-maec.git
sudo -H -u www-data git clone https://github.com/Cyb0XProject/mixbox.git
```

If you want to use / update the ZeroMQ functionality, you can also install / update the zmq python library.

```
# Install zmq library
sudo -H -u www-data /var/www/MISP/venv/bin/pip install zmq
# Update zmq library
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U zmq
```

## Updating MISP modules

Another set of dependencies you may want to update are [MISP modules](#).

[MISP modules](#) have their own dependencies that need to be up-to-date as well as the modules scripts themselves.

**Note that the following instructions consider your [MISP modules](#) are installed in the default path where we install them on our virtual machine or following the install script. Please change the path accordingly if needed.**

```
# Change here the path if needed
```

```
cd /usr/local/src/misp-modules
# Update misp-modules requirements
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U -r REQUIREMENTS
# Update misp-modules scripts
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .
```

You will then need to restart the modules, please refer to the [documentation](#).

Last modified: Tue May 26 2020 22:34:05 GMT+0200 (CEST)

- Automation API
  - General
    - Automation URL
    - Automation key
    - Accept and Content-Type headers
  - Automation using PyMISP
  - Status Codes
  - Error Handling
    - Wrong endpoint chosen ~ [Example](#)
  - Search
  - Events management
    - /events ~ Accepted Methods ~ Description
    - GET /events ~ Description ~ URL Arguments ~ Output ~ [Example](#)
    - POST /events ~ [Example](#)
    - DELETE /events ~ Description ~ URL Arguments ~ Output ~ [Example](#)
    - GET /events/index ~ Description ~ Output ~ [Example](#)
    - POST /events/addTag Add or remove tags from events
    - GET /events/pushEventToZMQ/ ~ Description ~ URL Arguments ~ [Example](#)
    - GET /events/nids NIDS rules export
    - GET /events/hids Hash - HIDS database export
    - GET /events/stix STIX export ~ Various ways to narrow down the search results of the STIX export
  - Tag management
    - POST /tags/add ~ Description
    - POST /tags/attachTagToObject ~ Description ~ URL Arguments ~ Response ~ [Example](#)
    - POST /tags/removeTagFromObject ~ Description ~ URL Arguments ~ Response ~ [Example](#)
    - GET /tags/tagStatistics/ ~ Description ~ Output ~ [Example](#)
  - Attribute management
    - POST /attributes/add/ ~ URL Arguments ~ Output ~ [Example](#)
    - GET /attributes ~ URL Arguments ~ URL Attributes ~ Output ~ [Example](#)
    - POST /attributes/delete/ ~ Description ~ URL Arguments ~ Output ~ [Example](#)
    - GET /attributes/attributeStatistics ~ Description ~ Output ~ [Example](#)
    - GET /attributes/describeTypes Describe types API ~ [Example](#)
  - Server management
    - GET /servers/getPyMISPVersion ~ Result ~ [Example](#)
    - GET /servers/getVersion ~ Result ~ [Example](#)
  - Sightings
    - POST /sightings/add/
  - User management
    - POST /admin/users/add
    - POST admin/users/edit/
    - POST admin/users/delete/ ~ Parameters ~ [Example](#)
    - GET admin/users ~ Description ~ Output ~ [Example](#)
    - GET admin/users/view/ ~ Description ~ Parameters ~ Output ~ [Example](#)
    - POST admin/users/add/
  - Discussion API
  - Organisation management
  - Special Cases
    - XML Export ~ JSON query format ~ XML query format ~ XML download and URL parameters
    - CSV export ~ [Update 2.4.82](#)

- [RPZ export](#)
- [Text export](#)
- [RESTful searches with JSON result](#)
  - [POST /attributes/restSearch ~ Example](#)
- [RESTful searches with XML result export](#)
- [Export attributes of event with specified type as XML](#)
- [Filtering event metadata](#)
- [Download attachment or malware sample](#)
- [Download malware sample by hash](#)
- [Upload malware samples using the "Upload Sample" API](#)
- [Proposals API](#)
- [Sharing groups](#)
- [Enable, disable and fetching feeds via the API](#)
- [Sightings API](#)
- [Warninglists API](#)
  - [GET warninglists/index ~ Description ~ Parameters ~ Output ~ Example](#)
  - [GET warninglists/view/1 ~ Description ~ Parameters ~ Output ~ Example](#)
- [Attribute statistics API](#)
- [Additional statistics](#)
- [MISP modules](#)
  - [Description](#)
    - [GET /modules/ ~ Example ~ Output](#)
    - [POST /modules/queryEnrichment ~ Example](#)

## Automation API

Automation functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support [NIDS](#) signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artefacts. Support for more attribute types is planned. To make this functionality available for automated tools an authentication key is used. This makes it easier for your tools to access the data without further form-based-authentication.

## General

### Automation URL

The documentation will include a default MISP URL in the examples. Don't forget to replace it with your MISP URL.

Default MISP URL in the documentation:

```
https://<misp url>/
```

### Automation key

The authentication of the automation is performed via a secure key available in the MISP UI interface. Make sure you keep that key secret as it gives access to the entire database! The [API](#) key is available in the event actions menu under automation.

Since version 2.2 the usage of the authentication key in the URL is deprecated. Instead, pass the auth key in an Authorization header in the request. The legacy option of having the auth key in the URL is temporarily still supported but not recommended.

The authorization is performed by using the following header:

```
Authorization: YOUR API KEY
```

## Accept and Content-Type headers

When performing your request, depending on the type of request, you might need to explicitly specify in what content type you want to get your results. This is done by setting one of the below Accept headers:

```
Accept: application/json  
Accept: application/xml
```

When submitting data in a POST, PUT or DELETE operation you also need to specify in what content-type you encoded the payload. This is done by setting one of the below Content-Type headers:

```
Content-Type: application/json  
Content-Type: application/xml
```

Example:

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" https://<misp url>/
```

By appending .json or .xml the content type can also be set without the need for a header.

## Automation using PyMISP

PyMISP is a Python library to access MISP platforms via their REST [API](#).

PyMISP allows you to fetch events, add or update events/attributes, add or update samples or search for attributes.

[PyMISP is available](#) including a documentation with various examples.

## Status Codes

To be done

- 50x
- 400 - 499

## Error Handling

### Wrong endpoint chosen

#### Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" http://10.50.13.60/servers/gaaa
```

```
{"name": "Not Found", "message": "Not Found", "url": "\servers\gaaa"}
```

## Search

It is possible to search in the database for a list of attributes or events based on a list of criterias.

To return attributes or events in a desired format, use the following URL and header settings:

URL:

```
YOUR_MISP_URL/attributes/restSearch
YOUR_MISP_URL/events/restSearch
```

Headers:

```
Accept: application/json
Content-type: application/json
Authorization: YOUR_API_KEY
```

The next feature to take care of then is the body of the query. This is where you are going to put your filters.

As an example, if we want to export all the IP addresses that have a TLP marking and not marked as TLP:red, you can find below the corresponding filters to use:

```
{
    "returnFormat": "json",
    "type": {
        "OR": [
            "ip-src",
            "ip-dst"
        ]
    },
    "tags": {
        "NOT": [
            "tlp:red"
        ],
        "OR": [
            "tlp:%"
        ]
    }
}
```

Find below a non exhaustive list of parameters that can be used to filter data in your search (some parameters specific to given export formats are not mentioned):

- **returnFormat:** Set the return format of the search (Currently supported: json, xml, openioc, suricata, snort - more formats are being moved to restSearch with the goal being that all searches happen through this [API](#)). Can be passed as the first parameter after restSearch or via the JSON payload.
- **limit:** Limit the number of results returned, depending on the scope (for example 10 attributes or 10 full events).
- **page:** If a limit is set, sets the page to be returned. page 3, limit 100 will return records 201->300).
- **value:** Search for the given value in the attributes' value field.
- **type:** The attribute type, any valid [MISP attribute](#) type is accepted.
- **category:** The attribute category, any valid [MISP attribute](#) category is accepted.
- **org:** Search by the creator organisation by supplying the organisation identifier.
- **tags:** To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'.
- **quickfilter:** Enabling this (by passing "1" as the argument) will make the search ignore all of the other arguments, except for

the auth key and value. MISP will return an xml / json (depending on the header sent) of all events that have a sub-string match on value in the event info, event orgc, or any of the attribute value1 / value2 fields, or in the attribute comment.

- **from:** Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.
- **to:** Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.
- **eventid:** The events that should be included / excluded from the search
- **withAttachments:** If set, encodes the attachments / zipped malware samples as base64 in the data field within each attribute
- **metadata:** Only the metadata (event, tags, relations) is returned, attributes and [proposals](#) are omitted.
- **uuid:** Restrict the results by uuid.
- **publish\_timestamp:** Restrict the results by the timestamp of the last [publishing](#) of the event. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **last:** (Deprecated synonym for publish\_timestamp) Restrict the results by the timestamp of the last [publishing](#) of the event. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **timestamp:** Restrict the results by the timestamp (last edit). Any event with a timestamp newer than the given timestamp will be returned. In case you are dealing with /attributes as scope, the attribute's timestamp will be used for the lookup. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **published:** Set whether published or unpublished events should be returned. Do not set the parameter if you want both.
- **enforceWarninglist:** Remove any attributes from the result that would cause a hit on a warninglist entry.
- **to\_ids:** By default (0) all attributes are returned that match the other filter parameters, irregardless of their to\_ids setting. To restrict the returned data set to to\_ids only attributes set this parameter to 1. You can only use the special "exclude" setting to only return attributes that have the to\_ids flag disabled.
- **deleted:** If this parameter is set to 1, it will return soft-deleted attributes along with active ones. By using "only" as a parameter it will limit the returned data set to soft-deleted data only.
- **includeEventUuid:** Instead of just including the event ID, also include the event UUID in each of the attributes.
- **event\_timestamp:** Only return attributes from events that have received a modification after the given timestamp. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **sgReferenceOnly:** If this flag is set, sharing group objects will not be included, instead only the sharing group ID is set.
- **eventinfo:** Filter on the event's info field.
- **searchall:** Search for a full or a substring (delimited by % for substrings) in the event info, event tags, attribute tags, attribute values or attribute comment fields.
- **attackGalaxy:** Select the ATT&CK matrix like galaxy to use when using returnFormat = attack. Defaults to the Mitre ATT&CK library via mitre-attack-pattern.

## Events management

### /events

#### Accepted Methods

- GET
- POST
- PUT
- DELETE

#### Description

Receive, update or delete Events. There is also a good amount of special output formats that can be triggered.

## GET /events

### Description

Receive events based on criteria

### URL Arguments

- event\_id: Event id to receive
- event\_uuid : Event uuid to receive

### Output

```
[{"id": "1", "org_id": "1", "date": "2014-12-10", "info": "OSINT - F-Secure W32\\Regin, Stage #1", "uuid": "54884656-2da8-4625-bf07-43ef950d210b", "published": true, "analysis": "2", "attribute_count": "39", "orgc_id": "2", "timestamp": "1418217625", "distribution": "3", "sharing_group_id": "0", "proposal_email_lock": false, "locked": false, "threat_level_id": "1", "publish_timestamp": "1515749192", "disable_correlation": false, "Org": {"id": "1", "name": "ORGNAME"}, "Orgc": {"id": "2", "name": "CIRCL"}, "EventTag": [{"id": "1", "event_id": "1", "tag_id": "1", "Tag": {"id": "1", "name": "Type:OSINT", "colour": "#1eedd40", "exportable": true}}], "SharingGroup": {"id": null, "name": null}}]
```

### Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" https://<misp url>/
```

## POST /events

### Example

```
curl -i -H "Accept: application/json" -H "content-type: application/json" -H "Authorization: YOUR API KEY" --data "@event.json" -X POST http://10.50.13.60/events
```

That is how an event JSON object should look like

```
{"Event": {"date": "2015-01-01", "threat_level_id": "1", "info": "testevent", "published": false, "analysis": "0", "distribution": "0", "Attribute": [{"type": "domain", "category": "Network activity", "to_ids": false, "distribution": "0", "comment": "", "value": "test.com"}]}}
```

## DELETE /events

### Description

Delete events based on criteria

### URL Arguments

- event\_id: Event id to receive
- event\_uuid : Event uuid to receive

## Output

```
{
  "name": "Event deleted.",
  "message": "Event deleted.",
  "url": "\/events\/delete\/1"
}
```

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json"
https://<misp url>/events/1
```

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" -X "DELETE" http://10.50.13.60/events/1
```

## GET /events/index

### Description

Return the event index. - Warning, there's a limit on the number of results

## Output

```
[{"id": "1", "org_id": "1", "date": "2014-12-10", "info": "OSINT - F-Secure W32\\Regin, Stage #1", "uuid": "54884656-2da8-4625-bf07-43ef950d210b", "published": true, "analysis": "2", "attribute_count": "39", "orgc_id": "2", "timestamp": "1418217625", "distribution": "3", "sharing_group_id": "0", "proposal_email_lock": false, "locked": false, "threat_level_id": "1", "publish_timestamp": "1515749192", "disable_correlation": false, "Org": {"id": "1", "name": "ORGNAME"}, "Orgc": {"id": "2", "name": "CIRCL"}, "EventTag": [{"id": "1", "event_id": "1", "tag_id": "1", "Tag": {"id": "1", "name": "Type:OSINT", "colour": "#1eed40", "exportable": true}}], "SharingGroup": {"id": null, "name": null}}
```

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" http://10.50.13.60/events/index
```

## POST /events/addTag Add or remove tags from events

You can add or remove an existing tag from an event in the following way:

```
https://<misp url>/events/addTag
https://<misp url>/events/removeTag
```

Just POST a JSON object in the following format (to the appropriate [API](#) depending on whether you want to add or delete a tag from an event):

```
{"request": {"Event": {"id": "228", "tag": "8"}}}
```

Where "tag" is the ID of the tag. You can also use the name of the tag the following way (has to be an exact match):

```
{"request": {"Event": {"id": "228", "tag": "OSINT"}}}
```

## GET /events/pushEventToZMQ/

### Description

Will [push](#) an Event to ZMQ

### URL Arguments

- event\_id

### Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" https://<misp url>events/pushEventToZMQ/223
```

## GET /events/nids NIDS rules export

Automatic export of all network related attributes is available under the Snort or Suricata rule format. Only published events and attributes marked as IDS Signature are exported.

You can configure your tools to automatically download the following file:

```
https://<misp url>/events/nids/suricata/download  
https://<misp url>/events/nids/snort/download
```

The full [API](#) syntax is as follows:

```
https://<misp url>/events/nids/[format]/download/[eventid]/[frame]/[tags]/[from]/[to]/[last]
```

#### *format*

The export format, can be "suricata" or "snort"

#### *eventid*

Restrict the download to a single event

#### *frame*

Some commented out explanation framing the data. The reason to disable this would be if you would like to concatenate a list of exports from various select events in order to avoid unnecessary duplication of the comments.

#### *tags*

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/events/nids/snort/download/false/false/tag1&&tag2&&!tag3
```

#### *from*

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

#### *to*

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of

the event.

#### **last**

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 6d or 12h or 30m). This filter will use the published timestamp of the event.

The keywords false or null should be used for optional empty parameters in the URL.

An example for a Suricata export for all events excluding those tagged tag1, without all of the commented information at the start of the file would look like this:

```
https://<misp url>/events/nids/suricata/download/null/true/!tag1
```

Administration is able to maintain a white-list containing host, domain name and IP numbers to exclude from the [NIDS](#) export.

## **GET /events/hids Hash - HIDS database export**

Automatic export of MD5/SHA1 checksums contained in file-related attributes. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as IDS Signature are exported.

You can configure your tools to automatically download all the MD5 hashes from MISP:

```
https://<misp url>/events/hids/md5/download
```

Or the SHA1 hashes:

```
https://<misp url>/events/hids/sha1/download
```

The [API](#)'s full format is as follow:

```
https://<misp url>/events/hids/[format]/download/[tags]/[from]/[to]/[last]
```

#### **format**

The export format, can be "md5" or "sha1"

#### **tags**

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/events/hids/md5/download/tag1&&tag2&&!tag3
```

#### **from**

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

#### **to**

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

#### **last**

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

The keywords false or null should be used for optional empty parameters in the URL.

For example, to only show sha1 values from events tagged tag1, use:

```
https://<misp url>/events/hids/sha1/download/tag1
```

## GET /events/stix STIX export

You can export MISP events in MITRE's STIX format (to read more about [STIX](#)). The STIX XML export is currently very slow and can lead to timeouts with larger events or collections of events. The STIX JSON return format does not suffer from this issue.

Usage of the [API](#):

```
https://<misp url>/events/stix/download
```

Search parameters can be passed to the function via URL parameters or by POSTing an xml or json object (depending on the return type). The following parameters can be passed to the STIX export tool: id, withAttachments, tags. Both id and tags can use the && (and) and ! (not) operators to build queries. Using the URL parameters, the syntax is as follows:

```
https://<misp url>/events/stix/download/[id]/[withAttachments]/[tags]/[from]/[to]/[last]
```

### ***id***

The event's ID

### ***withAttachments***

Encode attachments where applicable

### ***tags***

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead).

For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/events/stix/download/false/true/tag1&&tag2&&!tag3
```

### ***from***

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

### ***to***

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

### ***last***

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

You can post an XML or JSON object containing additional parameters in the following formats.

If you use JSON query objects:

```
https://<misp url>/events/stix/download.json
```

```
{"request": {"id": ["!51", "!62"], "withAttachment": false, "tags": ["APT1", "!OSINT"], "from": false, "to": "2015-02-15"}}
```

If you use XML query objects:

```
https://<misp url>/events/stix/download
```

```
<request><id>!51</id><id>!62</id><withAttachment>false</withAttachment><tags>APT1</tags><tags>!OSINT</tags><from>false</from><to>2015-02-15</to></request>
```

## Various ways to narrow down the search results of the STIX export

For example, to retrieve all events tagged "APT1" but excluding events tagged "OSINT" and excluding events #51 and #62 without any attachments:

```
https://<misp url>/events/stix/download/?51&&!62/false/APT1&&!OSINT/2015-02-15
```

To export the same events using a POST request use:

```
https://<misp url>/events/stix/download.json
```

Together with this JSON object in the POST message:

```
{"request": {"id": ["!51", "!62"], "tags": ["APT1", "!OSINT"], "from": "2015-02-15"}}
```

XML is automatically assumed when using the STIX export:

```
https://<misp url>/events/stix/download
```

The same search could be accomplished using the following POSTed XML object (note that ampersands need to be escaped, or alternatively separate id and tag elements can be used):

```
<request><id>!51</id><id>!62</id><tags>APT1</tags><tags>!OSINT</tags><from>2015-02-15</from></request>
```

## Tag management

### POST /tags/add

#### Description

### POST /tags/attachTagToObject

#### Description

Attaches an Tag to an Object by a given UUID

### URL Arguments

- tag
- UUID

## Response

```
{  
    "name": "Tag tlp3Awhite(7) successfully attached to Attribute(153).",  
    "message": "Tag tlp3Awhite(7) successfully attached to Attribute(153).",  
    "url": "\/tags\/attachTagToObject"  
}
```

## Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json" --header "Content-Type: application/json" -X POST http://10.50.13.60/tags/attachTagToObject/5a0d68b3-6da0-4ced-8233-77bb950d210f/tlp3Awhite
```

```
curl --header "Authorization: YOUR API KEY " -d "{\"uuid\":\"5a0d68b3-6da0-4ced-8233-77bb950d210f\" \"tag\"=\"tlp:white\"}" --header "Accept: application/json" --header "Content-Type: application/json" -X POST http://10.50.13.60/tags/attachTagToObject/
```

## POST /tags/removeTagFromObject

### Description

Removes an Tag to an Object by a given UUID

### URL Arguments

- tag
- UUID

## Response

```
{  
    "name": "Tag tlp3Awhite(7) successfully removed from Attribute(153).",  
    "message": "Tag tlp3Awhite(7) successfully removed from Attribute(153).",  
    "url": "\/tags\/removeTagFromObject"  
}
```

## Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json" --header "Content-Type: application/json" -X POST http://10.50.13.60/tags/removeTagFromObject/5a0d68b3-6da0-4ced-8233-77bb950d210f/tlp3Awhite
```

## GET /tags/tagStatistics/

### Description

Will give an overview of the used attribute tags

### Output

```
{
  "tags": {
    "Type:OSINT": "1",
    "tlp:white": "1",
    "osint:source-type=\"technical-report\"": "1",
    "misp-galaxy:threat-actor=\"Lazarus Group\"": "1",
    "misp-galaxy:rat=\"FALLCHILL\"": "1"
  },
  "taxonomies": []
}
```

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" -X GET http://10.50.13.60/tags/tagStatistics/
```

# Attribute management

## POST /attributes/add/

Adds an Attribute to an event

### URL Arguments

- event id

### Output

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" -d "{\"event_id\":\"3542\", \"value\":\"1.2.3.4\", \"category\":\"Network activity\", \"type\":\"ip-dst\"}" http://10.50.13.60/attributes/add/3542
```

## GET /attributes

Get an attribute

### URL Arguments

- attribute uuid

### URL Attributes

### Output

```
{"Attribute": {"id": "39", "event_id": "1", "object_id": "0", "object_relation": null, "category": "Payload installation", "type": "md5", "to_ids": true, "uuid": "548847db-060c-4275-a0c7-15bb950d210b", "timestamp": "1418217435", "distribution": "3", "sharing_group_id": "0", "comment": "Regin samples collected.", "deleted": false, "disable_correlation": false, "value": "049436bb90f71cf38549817d9b90e2da", "event_uuid": "54884656-2da8-4625-bf07-43ef950d210b"}}
```

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" http://10.50.13.60/attributes/548847db-060c-4275-a0c7-15bb950d210b
```

## POST /attributes/delete/

### Description

Delete attributes.

### URL Arguments

- attribute uuid
- attribute id
- attribute id/1 <-- hard delete

### Output

```
{"message": "Attribute deleted."}
```

## Example

```
curl -X POST --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" https://<misp url>/attributes/delete/12345
```

```
curl -X POST --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" http://10.50.13.60/attributes/delete/548847db-060c-4275-a0c7-15bb950d210b
```

Hard delete:

```
curl -X POST --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" https://<misp url>/attributes/delete/12345/1
```

## GET /attributes/attributeStatistics

### Description

Will give an overview of the used attribute types

### Output

```
{  
    "attachment": "1",  
    "comment": "1",  
    "filename": "2",  
    "float": "2",  
    "ip-dst": "90",  
    "ip-dst|port": "3",  
    "link": "3",  
    "text": "2",  
    "url": "2",  
    "whois": "2",  
    "x509": "2",  
    "yara": "2",  
    "md5": "1",  
    "sha1": "1",  
    "sha256": "1",  
    "sha512": "1",  
    "ssdeep": "1",  
    "entropy": "1",  
    "size": "1",  
    "confidence": "1",  
    "reputation": "1",  
    "category": "1",  
    "type": "1",  
    "value": "1",  
    "count": 1  
}
```

```
    "md5": "16",
    "port": "3",
    "sha1": "2",
    "sha256": "2",
    "size-in-bytes": "1",
    "ssdeep": "2"
}
```

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" -X GET http://10.50.13.60/attributes/attributeStatistics/
```

## GET /attributes/describeTypes Describe types API

MISP can procedurally describe all attribute types and attribute categories it currently supports including the category - type mappings. To access this information simply send a GET request to:

## Example

```
https://<misp url>/attributes/describeTypes
```

Depending on the headers passed the returned data will be a JSON object or an XML, with 3 main sections: types, categories, category\_type\_mappings.

## Server management

### GET /servers/getPyMISPVersion

#### Result

```
{"version": "2.4.85"}
```

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" http://10.50.13.60/servers/getPyMISPVersion.json
```

### GET /servers/getVersion

#### Result

```
{"version": "2.4.85", "perm_sync": true}
```

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" http://10.50.13.60/servers/getPyMISPVersion.json
```

## Sightings

### POST /sightings/add/

- attribute\_id
- attribute\_uuid

The different sightings types are:

```
0 => 'sighting',
1 => 'false-positive',
2 => 'expiration'
```

## User management

MISP allows administrators to create and manage users via its REST [API](#)

```
https://<misp url>/admin/users/view/[user id]
```

### POST /admin/users/add

To create a new user, send a POST request to:

#### Sample input

```
{
    "email": "andras.iklody@circl.lu",
    "org_id": 1,
    "role_id": 1
}
```

To view the mandatory and optional fields, use a GET request on the above URL.

#### Sample output

```
{
    "name": "\/admin\/users\/add API description",
    "description": "POST a User object in JSON format to this API to create a new user.",
    "mandatory_fields": [
        "email",
        "org_id",
        "role_id"
    ],
    "optional_fields": [
        "password",
        "external_auth_required",
        "external_auth_key",
        "enable_password",
        "nids_sid",
        "server_id",
        "gpgkey",
        "certif_public",
        "autoalert",
        "contactalert",
        "disabled",
        "change_pw",
        "last_login",
        "last_logout",
        "last_ip",
        "last_browser",
        "last_os",
        "last_location",
        "last_geolocation",
        "last_email",
        "last_file",
        "last_domain",
        "last_url",
        "last_ip_hex",
        "last_browser_hex",
        "last_os_hex",
        "last_location_hex",
        "last_geolocation_hex",
        "last_email_hex",
        "last_file_hex",
        "last_domain_hex",
        "last_url_hex"
    ]
}
```

```
        "termsaccepted",
        "newsread"
    ],
    "url": "\/admin\/users\/add"
}
```

## POST admin/users/edit/

To edit an existing user send a POST request to:

```
https://<misp url>/admin/users/edit/[user id]
```

Only the fields POSTed will be updated, the rest is left intact. To view all possible parameters, simply send a GET request to the above URL.

## POST admin/users/delete/

You can also delete users by POSTing to the below URL, but keep in mind that disabling users (by setting the disabled flag via an edit) is always preferred to keep user associations to events intact.

### Parameters

- [user id]

### Example

```
https://<misp url>/admin/users/delete/[user id]
```

## GET admin/users

### Description

Will output all users

### Output

```
[
  {
    "User": {
      "id": "1",
      "password": "F00000000000",
      "org_id": "1",
      "server_id": "0",
      "email": "admin@admin.test",
      "autoalert": false,
      "authkey": "YOUR API KEY",
      "invited_by": "0",
      "gpgkey": null,
      "certif_public": "",
      "nids_sid": "4000000",
      "termsaccepted": true,
      "newsread": "0",
      "role_id": "1",
      "change_pw": "0",
      "contactalert": false,
      "disabled": false,
      "last_login": null
    }
  }
]
```

```

        "expiration": null,
        "current_login": "1515752313",
        "last_login": "1515748671",
        "force_logout": false,
        "date_created": null,
        "date_modified": null,
        "org_ci": "ORGNAME"
    },
    "Role": {
        "id": "1",
        "name": "admin",
        "perm_auth": true
    },
    "organisation": {
        "id": "1",
        "name": "ORGNAME"
    }
}
]

```

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" -X GET http://10.50.13.60/admin/users
```

## GET admin/users/view/

### Description

Will return a single user. To view a user simply send a GET request.

### Parameters

- id

### Output

```
{
    "User": {
        "id": "1",
        "password": "*****",
        "org_id": "1",
        "server_id": "0",
        "email": "admin@admin.test",
        "autoalert": false,
        "authkey": "YOUR API KEY",
        "invited_by": "0",
        "gpgkey": null,
        "certif_public": "",
        "nids_sid": "4000000",
        "termsaccepted": true,
        "newsread": "0",
        "role_id": "1",
        "change_pw": "0",
        "contactalert": false,
        "disabled": false,
        "expiration": null,
        "current_login": "1515752313",
        "last_login": "1515748671",
        "force_logout": false,
        "orgAdmins": []
    }
}
```

```
    }  
}
```

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: application/json" -X GET http://10.50.13.60/admin/users/view/1
```

## POST admin/users/add/

## Discussion API

If you would like to fetch a discussion thread including all of its posts, simply send a GET request to:

```
https://<misp url>/threads/view/<thread id>
```

Using the following headers:

```
Authorization: [Your auth key]  
Content-type: application/json  
Accept: application/json
```

To get all posts related to an event simply send a GET request to:

```
https://<misp url>/threads/viewEvent/<event id>
```

## Organisation management

MISP allows administrators to create and manage organisations via its REST [API](#)

The [API](#) is available in JSON format so make sure you use the following headers:

```
Authorization: [Your auth key]  
Content-type: application/json  
Accept: application/json
```

To fetch all organisations send a GET request to:

```
https://<misp url>/organisations
```

To view an individual organisation, send a get request to:

```
https://<misp url>/organisations/view/id
```

The management of users happens via three apis:

```
https://<misp url>/admin/organisations/add  
https://<misp url>/admin/organisations/edit/[org id]  
https://<misp url>/admin/organisations/delete/[org id]
```

To delete an organisation simply send a POST or DELETE request to the above URL.

For creating or modifying an organisation, simply POST a JSON containing the relevant fields to the appropriate [API](#). The only mandatory field is the organisation name, with a host of optional parameters

An example for a simple organisation object:

```
{  
    "name": "Blizzard",  
    "nationality": "US"  
}
```

Not setting a field will assume the default settings for the given field in the case of a new organisation whilst it would retain the existing setting for existing organisations. The above example would create the following object in MISP:

```
{  
    "Organisation": {  
        "id": "1108",  
        "name": "Blizzard",  
        "alias": "",  
        "anonymise": false,  
        "date_created": "2017-01-22 17:32:29",  
        "date_modified": "2017-01-22 17:32:29",  
        "description": "",  
        "type": "",  
        "nationality": "US",  
        "sector": "",  
        "created_by": "1",  
        "uuid": "5884de9d-04f0-4d7d-bf15-0b88c0a83865",  
        "contacts": "",  
        "local": true,  
        "landingpage": ""  
    }  
}
```

To query the add or edit APIs for the valid parameters, simply send a GET requests to either [API](#). The result currently looks like this (which might change when new fields are added):

```
{  
    "name": "\/admin\/organisations\/add API description",  
    "description": "POST an Organisation object in JSON format to this API to create a new organisation.",  
    "mandatory_fields": [  
        "name"  
    ],  
    "optional_fields": [  
        "anonymise",  
        "description",  
        "type",  
        "nationality",  
        "sector",  
        "uuid",  
        "contacts",  
        "local"  
    ],  
    "url": "\/admin\/organisations\/add"  
}
```

## Special Cases

### XML Export

An automatic export of all events and attributes (except file attachments) is available under a custom XML format.

You can configure your tools to automatically download the following file:

```
https://<misp url>/events/xml/download
```

If you only want to fetch a specific event append the eventid number:

```
https://<misp url>/events/xml/download/1
```

You can post an XML or JSON object containing additional parameters in the JSON query format or XML query format. Query parameters provide a way to filter the output to specific parameters.

## JSON query format

The URL is appended with json:

```
https://<misp url>/events/xml/download.json
```

The query parameters can be the following:

```
{"request": {"eventid": ["!51", "!62"], "withAttachment": false, "tags": ["APT1", "!OSINT"], "from": false, "to": "2015-02-15"}}
```

## XML query format

The URL is path is:

```
https://<misp url>/events/xml/download
```

The query parameters can be the following:

```
<request><eventid>!51</eventid><eventid>!62</eventid><withAttachment>false</withAttachment><tags>APT1</tags><tags>!OSINT</tags><from>false</from><to>2015-02-15</to></request>
```

## XML download and URL parameters

The XML download also accepts two additional the following optional parameters in the url:

```
https://<misp url>/events/xml/download/[eventid]/[withattachments]/[tags]/[from]/[to]/[last]
```

### **eventid**

Restrict the download to a single event

### **withattachments**

A boolean field that determines whether attachments should be encoded and a second parameter that controls the eligible tags.

### **tags**

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/events/xml/download/false/true/tag1&&tag2&&!tag3
```

**from**

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

**to**

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

**last**

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

The keywords false or null should be used for optional empty parameters in the URL. Also check out the User Guide to read about the [REST API](#).

## CSV export

An automatic export of attributes is available as CSV. Only attributes that are flagged "to\_ids" will get exported.

You can configure your tools to automatically download the following file:

```
https://<misp url>/events/csv/download
```

This will download all the valid attributes in your [MISP instance](#) (might take some time).

You can also configure your tools to download the attributes from a specific event. Here is the old legacy CSV export that will work like exporting all attributes:

```
https://<misp url>/events/csv/download/<event-id>
```

You can specify additional flags for CSV exports as follows:

POST to:

```
https://<misp url>/events/csv/download
```

Headers:

```
Authorization: <your auth key>
Content-type: application/json
```

Body:

```
{"parameter1":"value1", "parameter2":1, "parameter3":["value3", "value4", "!value5"]}
```

**eventid**

Restrict the download to a single event

**ignore**

Setting this flag to true will include attributes that are not marked "to\_ids".

**tags**

Simply add a list of tags that should be included or negated (by prepending the tag name with a "!"'). Any event with a negated tag will be ignored, even if an included tag is matching. An example is included further down.

**category**

The attribute category, any valid [MISP attribute](#) category is accepted.

**type**

The attribute type, any valid [MISP attribute](#) type is accepted.

**includeContext**

Include the event data with each attribute.

**from**

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

**to**

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

**last**

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

For example, to only download a csv generated of the "domain" type and the "Network activity" category attributes all events except for the one and further restricting it to events that are tagged "tag1" or "tag2" but not "tag3", only allowing attributes that are IDS flagged use the following syntax:

POST to:

```
https://<misp url>/events/csv/download
```

Headers:

```
Authorization: <your auth key>
Content-type: application/json
```

Body:

```
{"tags": ["tag1", "tag2", "!tag3"], "category": "Network activity", "type": "domain"}
```

Alternatively you can fall back to the deprecated syntax of passing parameters in a GET request via the URL, however this is discouraged:

```
https://<misp url>/events/csv/download/[eventid]/[ignore]/[tags]/[category]/[type]/[includeContext]/[from]/[to]
/[last]
```

If you use the deprecated URL parameter method, keep in mind that the keywords false or null should be used for optional empty parameters. To export the attributes of all events that are of the type "domain", use the following syntax:

```
https://<misp url>/events/csv/download/false/false/false/false/domain
```

## Update 2.4.82

Since version 2.4.82, the new export format allows to select more columns using the following query format:

```
https://<misp-instance>/events/csv/download/<event-id>?attributes=timestamp,type,uuid,value
```

The order of columns will be honoured including those related to object level information.

To select object level columns, simply prepend the given object column's name by object\_, such as:

```
https://<misp-instance>/events/csv/download/<event-id>?attributes=timestamp,type,uuid,value&object_attributes=object_uuid,object_name
```

The following columns will be returned (all columns related to objects will be prefixed with object\_):

```
timestamp,type,uuid,value,object_uuid,object_name
```

includeContext option includes the tags for the event for each line.

## RPZ export

You can export RPZ zone files for DNS level firewall by using the RPZ export functionality of MISP. The file generated will include all of the IDS flagged domain, hostname and IP-src/IP-dst attribute values that you have access to.

It is possible to further restrict the exported values using the following filters:

### **tags**

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search when passed through the URL. Use semicolons instead (the search will automatically search for colons instead).

### **id**

The event's ID

### **from**

Events with the date set to a date after the one specified in the from field (format: 2015-02-03)

### **to**

Events with the date set to a date before the one specified in the to field (format: 2015-02-03)

MISP will inject header values into the zone file as well as define the action taken for each of the values that can all be overwritten. By default these values are either the default values shipped with the application, or ones that are overwritten by your site administrator. The values are as follows:

Value name	Default value
RPZ_policy	DROP
RPZ_walled_garden	127.0.0.1
RPZ_serial	\$date00
RPZ_refresh	2h
RPZ_retry	30m
RPZ_expiry	30d
RPZ_minimum_ttl	1h
RPZ_ttl	1w
RPZ_ns	localhost.

RPZ_ns_alt	
RPZ_email	root.localhost

To override the above values, either use the URL parameters as described below:

```
https://<misp url>/attributes/rpz/download/[tags]/[eventId]/[from]/[to]/[policy]/[walled_garden]/[ns]/[ns_alt]/[email]/[serial]/[refresh]/[retry]/[expiry]/[minim um_ttl]/[ttl]
```

Or POST an XML or JSON object with the above listed options:

```
<request><tags>OSINT&&!OUTDATED</tags><policy>walled-garden</policy><walled_garden>teamliquid.net</walled_garde n><refresh>5h</refresh></request>
```

```
{"request": {"tags": ["OSINT", "!OUTDATED"], "policy": "walled-garden", "walled_garden": "teamliquid.net", "refresh": "5h"}}
```

## Text export

An export of all attributes of a specific type to a plain text file. By default only published and IDS flagged attributes are exported.

You can configure your tools to automatically download the following files:

```
https://<misp url>/attributes/text/download/md5
https://<misp url>/attributes/text/download/sha1
https://<misp url>/attributes/text/download/sha256
https://<misp url>/attributes/text/download/filename
https://<misp url>/attributes/text/download/filename|md5
https://<misp url>/attributes/text/download/filename|sha1
https://<misp url>/attributes/text/download/filename|sha256
https://<misp url>/attributes/text/download/ip-src
https://<misp url>/attributes/text/download/ip-dst
https://<misp url>/attributes/text/download/hostname
https://<misp url>/attributes/text/download/domain
https://<misp url>/attributes/text/download/email-src
https://<misp url>/attributes/text/download/email-dst
https://<misp url>/attributes/text/download/email-subject
https://<misp url>/attributes/text/download/email-attachment
https://<misp url>/attributes/text/download/url
https://<misp url>/attributes/text/download/http-method
https://<misp url>/attributes/text/download/user-agent
https://<misp url>/attributes/text/download/regkey
https://<misp url>/attributes/text/download/regkey|value
https://<misp url>/attributes/text/download/AS
https://<misp url>/attributes/text/download/snort
https://<misp url>/attributes/text/download/pattern-in-file
https://<misp url>/attributes/text/download/pattern-in-traffic
https://<misp url>/attributes/text/download/pattern-in-memory
https://<misp url>/attributes/text/download/yara
https://<misp url>/attributes/text/download/vulnerability
https://<misp url>/attributes/text/download/attachment
https://<misp url>/attributes/text/download/malware-sample
https://<misp url>/attributes/text/download/link
https://<misp url>/attributes/text/download/comment
https://<misp url>/attributes/text/download/text
https://<misp url>/attributes/text/download/other
https://<misp url>/attributes/text/download/named pipe
https://<misp url>/attributes/text/download/mutex
https://<misp url>/attributes/text/download/target-user
https://<misp url>/attributes/text/download/target-email
```

```
https://<misp url>/attributes/text/download/target-machine  
https://<misp url>/attributes/text/download/target-org  
https://<misp url>/attributes/text/download/target-location  
https://<misp url>/attributes/text/download/target-external
```

To restrict the results by tags, use the usual syntax. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). To get ip-src values from events tagged tag1 but not tag2 use:

```
https://<misp url>/attributes/text/download/ip-src/tag1&&
```

It is possible to restrict the text exports on additional flags. The first allows the user to restrict based on event ID, whilst the second is a boolean switch allowing non IDS flagged attributes to be exported. Additionally, choosing "all" in the type field will return all eligible attributes.

```
https://<misp url>/attributes/text/download/[type]/[tags]/[event_id]/[allowNonIDS]/[from]/[to]/[last]
```

#### **type**

The attribute type, any valid [MISP attribute](#) type is accepted.

#### **tags**

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead).

#### **allowNonIDS**

Include attributes that would normally be excluded due to the IDS flag not being set or due to being whitelisted

#### **from**

Set the lowest "date" field value that should be included in the export (format YYYY-MM-DD)

#### **to**

Set the highest "date" field value that should be included in the export (format YYYY-MM-DD)

#### **last**

Set the timeframe of the export based on the "timestamp" value. The parameter uses a time + metric notation (valid examples: "2w", "60m", "24h")

For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/attributes/text/download/all/tag1&&tag2&&!tag3
```

#### **event\_id**

Restrict the results to the given event IDs.

#### **allowNonIDS**

Allow attributes to be exported that are not marked as "to\_ids".

#### **from**

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

#### **to**

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

#### **last**

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

The keywords false or null should be used for optional empty parameters in the URL.

For example, to retrieve all attributes for event #5, including non IDS marked attributes too, use the following line:

```
https://<misp url>/attributes/text/download/all/null/5/true
```

## RESTful searches with JSON result

It is possible to search the database for attributes based on a list of criteria

To return an event with all of its attributes, relations, shadowAttributes, use the following syntax:

```
https://<misp url>/attributes/restSearch/json/[value]/[type]/[category]/[org]/[tag]/[quickfilter]/[from]/[to]/[last]/[eventid]/[withAttachments]/[metadata]/[uuid]
```

If you include "includeEventUuid":1" in the json request, it will give you the event\_uuid as a result as well.

Be careful if you GET the /attributes/restSearch/json/ without an value, it will return all attributes.

### POST /attributes/restSearch

Do not use that function with GET!

#### Example

```
curl -X POST -k -H 'Accept: application/json' -H 'Authorization: API Key' -H 'Content-Type: application/json' -i 'https://URL/attributes/restSearch' --data '{"value":"foobar"}'
```

```
{
    "response": []
}
```

## RESTful searches with XML result export

It is possible to search the database for attributes based on a list of criteria.

To return an event with all of its attributes, relations, shadowAttributes, use the following syntax:

```
https://<misp url>/events/restSearch/download/[value]/[type]/[category]/[org]/[tag]/[quickfilter]/[from]/[to]/[last]/[eventid]/[withAttachments]/[metadata]/[uuid]
```

#### *value*

Search for the given value in the attributes' value field.

#### *type*

The attribute type, any valid [MISP attribute](#) type is accepted.

#### *category*

The attribute category, any valid [MISP attribute](#) category is accepted.

**org**

Search by the creator organisation by supplying the organisation identifier.

**tags**

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead).

For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/events/restSearch/download/null/null/null/null/tag1&&tag2&&!tag3
```

**quickfilter**

Enabling this (by passing "1" as the argument) will make the search ignore all of the other arguments, except for the auth key and value. MISP will return an xml / json (depending on the header sent) of all events that have a sub-string match on value in the event info, event orgc, or any of the attribute value1 / value2 fields, or in the attribute comment.

**from**

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

**to**

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

**last**

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

**eventid**

The events that should be included / excluded from the search

**withAttachments**

Include the attachments/encrypted samples in the export

**metadata**

Only fetch the event metadata (event data, tags, relations) and skip the attributes

**limit**

Limit the number of results returned; use together with page.

**page**

If a limit is set, sets the page to be returned, starting at 1; page 3, limit 100 will return records 201->300). When requesting a page beyond the number of available pages, the returned results list will be empty.

The keywords false or null should be used for optional empty parameters in the URL.

For example, to find any event with the term "red october" mentioned, use the following syntax (the example is shown as a POST request instead of a GET, which is highly recommended):

POST to:

```
https://<misp url>/events/restSearch/download
```

POST message payload (XML):

```
<request><value>red october</value><searchall>1</searchall><eventid>!15</eventid></request>
```

POST message payload (JSON):

```
{"request": {"value": "red october", "searchall": 1, "eventid": "!15"}}
```

To just return a list of attributes, use the following syntax:

**value**

Search for the given value in the attributes' value field.

**type**

The attribute type, any valid [MISP attribute](#) type is accepted.

**category**

The attribute category, any valid [MISP attribute](#) category is accepted.

**org**

Search by the creator organisation by supplying the organisation identifier.

**tags**

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead).

**from**

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

**to**

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

**last**

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

**eventid**

The events that should be included / excluded from the search.

**uuid**

The returned events must include an attribute with the given UUID, or alternatively the event's UUID must match the value(s) passed.

The keywords false or null should be used for optional empty parameters in the URL.

```
https://<misp url>/attributes/restSearch/download/[value]/[type]/[category]/[org]/[tag]/[from]/[to]/[last]/[eve  
ntid]/[withattachments]/[uuid]
```

Value, type, category and org are optional. It is possible to search for several terms in each category by joining them with the '&&' operator. It is also possible to negate a term with the '!' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). For example, in order to search for all attributes created by your organisation that contain 192.168 or 127.0 but not 0.1 and are of the type ip-src, excluding the events that were tagged tag1 use the following syntax:

```
https://<misp url>/attributes/restSearch/download/192.168&&127.0&&!0.1/ip-src/false/CIRCL/!tag1
```

You can also use search for IP addresses using CIDR. Make sure that you use '|' (pipe) instead of '/' (slashes). Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). See below for an example:

```
https://<misp url>/attributes/restSearch/download/192.168.1.1|16/ip-src/null/CIRCL
```

## Export attributes of event with specified type as XML

If you want to export all attributes of a pre-defined type that belong to an event, use the following syntax:

```
https://<misp url>/attributes/returnAttributes/download/[id]/[type]/[sigOnly]
```

`sigOnly` is an optional flag that will block all attributes from being exported that don't have the IDS flag turned on. It is possible to search for several types with the '`&&`' operator and to exclude values with the '`!`' operator. For example, to get all IDS signature attributes of type md5 and sha256, but not filename|md5 and filename|sha256 from event 25, use the following:

```
https://<misp url>/attributes/returnAttributes/download/25/md5&&sha256&&!filename=true
```

## Filtering event metadata

As described in the REST section, it is possible to retrieve a list of events along with their metadata by sending a GET request to the /events [API](#). However, this [API](#) in particular is a bit more versatile. You can pass search parameters along to search among the events on various fields and retrieve a list of matching events (along with their metadata). Use the following URL:

```
https://<misp url>/events/index
```

POST a JSON object with the desired lookup fields and values to receive a JSON back. An example for a valid lookup:

```
Authorization: <your API key>
Accept: application/json
Content-type: application/json
```

Body:

```
{"searchinfo": "Locky", "searchpublished": 1, "searchdistribution": 0}
```

The list of valid parameters:

***searchpublished:***

Filters on published or unpublished events [0,1] - negatable

***searchinfo:***

Filters on strings found in the event info - negatable

***searchtag:***

Filters on attached tag names - negatable

***searcheventid:***

Filters on specific event IDs - negatable

***searchthreatlevel:***

Filters on a given event threat level [1,2,3,4] - negatable

***searchdistribution:***

Filters on the distribution level [0,1,2,3] - negatable

***searchanalysis:***

Filters on the given analysis phase of the event [0,1,2,3] - negatable

***searchattribute:***

Filters on a contained attribute value - negatable

***searchorg:***

Filters on the creator organisation - negatable

***searchemail:***

Filters on the creator user's email address (admin only) - negatable

***searchDatefrom:***

Filters on the date, anything newer than the given date in YYYY-MM-DD format is taken - non-negatable

***searchDateuntil:***

Filters on the date, anything older than the given date in YYYY-MM-DD format is taken - non-negatable

## Download attachment or malware sample

If you know the attribute ID of a malware-sample or an attachment, you can download it with the following syntax:

```
https://<misp url>/attributes/downloadAttachment/download/[Attribute_id]
```

## Download malware sample by hash

You can also download samples by knowing its MD5 hash. Simply pass the hash along as a JSON/XML object or in the URL (with the URL having overruling the passed objects) to receive a JSON/XML object back with the zipped sample base64 encoded along with some contextual information.

You can also use this [API](#) to get all samples from events that contain the passed hash. For this functionality, just pass the "allSamples" flag along. Note that if you are getting all samples from matching events, you can use all supported hash types (md5, sha1, sha256) for the lookup.

You can also get all the samples from an event with a given event ID, by passing along the eventID parameter. Make sure that either an event ID or a hash is passed along, otherwise an error message will be returned. Also, if no hash is set, the allSamples flag will get set automatically.

[https://attributes/downloadSample/\[hash\]/\[allSamples\]/\[eventID\]](https://attributes/downloadSample/[hash]/[allSamples]/[eventID])

POST message payload (XML):

```
<request><hash>7c12772809c1c0c3deda6103b10fdfa0</hash><allSamples>1</allSamples><eventID>13</eventID></request>
```

POST message payload (json):

```
{"request": {"hash": "7c12772809c1c0c3deda6103b10fdfa0", "allSamples": 1, "eventID": 13}}
```

A description of all the parameters in the passed object:

**hash**

A hash in MD5 format. If allSamples is set, this can be any one of the following: md5, sha1, sha256.

**allSamples**

If set, it will return all samples from events that have a match for the hash provided above.

**eventID**

If set, it will only fetch data from the given event ID.

## Upload malware samples using the "Upload Sample" API

```
https://<misp url>/events/upload_sample/[Event_id]
```

This [API](#) will allow you to populate an event that you have modify rights to with malware samples (and all related hashes).

Alternatively, if you do not supply an event ID, it will create a new event for you.

The files have to be base64 encoded and POSTed as explained below. All samples will be zipped and password protected (with the password being "infected"). The hashes of the original file will be captured as additional attributes.

For sample upload (for objects in general) there is no check for duplicates.

The event ID is optional. MISP will accept either a JSON or an XML object posted to the above URL.

The general structure of the expected objects is as follows:

```
{"request": {"files": [{"filename": filename1, "data": base64encodedfile1}, {"filename": filename2, "data": base64encodedfile2}], "optional_parameter1", "optional_parameter2", "optional_parameter3"}}
```

JSON:

```
{"request": {"files": [{"filename": "test1.txt", "data": "dGVzdA=="}, {"filename": "test2.txt", "data": "dGVzddI=="}], "distribution": 1, "info": "test", "event_id": 15}}
```

XML:

```
<request><files><filename>test3.txt</filename><data>dGVzdA==</data></files><files><filename>test4.txt</filename><data>dGVzddI=</data></files><info>test</info><distribution>1</distribution><event_id>15</event_id></request>
```

The following optional parameters are expected:

**event\_id**

The Event's ID is optional. It can be either supplied via the URL or the POSTed object, but the URL has priority if both are provided. Not supplying an event ID will cause MISP to create a single new event for all of the POSTed malware samples. You can define the default settings for the event, otherwise a set of default settings will be used.

**distribution**

The distribution setting used for the attributes and for the newly created event, if relevant. [0-3]

**to\_ids**

You can flag all attributes created during the transaction to be marked as "to\_ids" or not.

**category**

The category that will be assigned to the uploaded samples. Valid options are: Payload delivery, Artifacts dropped, Payload Installation, External Analysis.

**info**

Used to populate the event info field if no event ID supplied. Alternatively, if not set, MISP will simply generate a message showing that it's a malware sample collection generated on the given day.

**analysis**

The analysis level of the newly created event, if applicable. [0-2] threat\_level\_id: The threat level ID of the newly created event, if applicable. [0-3]

**comment**

This will populate the comment field of any attribute created using this [API](#).

The **threat\_level\_id** is mapped as such:

```
0 = high
1 = medium
2 = low
3 = undefined
```

## Proposals API

You can interact with the [proposals](#) via the [API](#) directly since version 2.3.148.

HTTP	URL	Explanation	Expected Payload	Response
GET	/shadow_attributes/view/[proposal_id]	View a proposal	N/A	ShadowAttribute object
POST	/shadow_attributes/add/[event_id]	Propose a new attribute to an event	ShadowAttribute object	ShadowAttribute object
POST	/shadow_attributes/edit/[attribute_id]	Propose an edit to an attribute	ShadowAttribute object	ShadowAttribute object
POST	/shadow_attributes/accept/[proposal_id]	Accept a proposal	N/A	Message
POST	/shadow_attributes/discard/[proposal_id]	Discard a proposal	N/A	Message

When posting a shadow attribute object, use the following format

JSON:

```
{"request": {"ShadowAttribute": {"value": "5.5.5.5", "to_ids": false, "type": "ip-dst", "category": "Network activity"}}}
```

XML:

```
<request><ShadowAttribute><value>5.5.5.5</value><to_ids>0</to_ids><type>ip-src</type><category>Network activity</category></ShadowAttribute></request>
```

None of the above fields are mandatory, but at least one of them has to be provided.

## Sharing groups

MISP allows [sharing groups](#) to be retrieved via the [API](#).

```
https://<misp url>/sharing_groups/index.json
```

Based on the [API](#) key used, the list of visible [sharing groups](#) will be returned in a JSON file. The JSON includes the organization parts of a given sharing group along with the associated server.

## Enable, disable and fetching feeds via the API

The [MISP feeds](#) can be enabled via the [API](#).

A feed can be enabled by POSTing on the following URL (feed\_id is the id of the feed):

```
/feeds/enable/feed_id
```

A feed can be disabled by POSTing on the following URL (feed\_id is the id of the feed):

```
/feeds/disable/feed_id
```

All feeds can be cached via the [API](#):

```
/feeds/cacheFeeds/all
```

or you can replace `all` by the feed format to fetch like `misp` or `freetext`. `all` can be replaced with the `id` value of the feed to fetch a specific feed.

To fetch a feed or all feeds:

```
/feeds/fetchFromFeed/feed_id  
/feeds/fetchFromAllFeeds
```

This [API](#) can be also used to download feeds at regular interval via cronjobs or alike.

## Sightings API

MISP allows Sightings data to be conveyed in several ways.

The most basic way is to POST a blank message to the Sightings [API](#) with the attribute ID or attribute UUID. This will create a sightings entry with the creation of the entry as the timestamp for the organisation of the authenticated user.

```
https://<misp url>/sightings/add/[attribute_id]  
https://<misp url>/sightings/add/[attribute_uuid]
```

Alternatively, it is possible to POST a JSON object and gain additional granularity. The following fields are recognised by the [API](#):

### ***id***

The attribute's ID

### ***uuid***

The attribute's UUID

### ***value***

Will create a sighting for any attribute with the given value or for composite attributes, for the value matching any element of the attribute value

**values**

Expects a list, MISP will create sightings for any attribute matching any of the given values or for composite attributes, for any of the values matching any element of the attribute value

**timestamp**

Unix timestamp of the sighting, overrides the current time

Some examples:

To create a sighting for attribute #9001:

```
{"id": "9001"}
```

To create a sighting for any attribute with the value being teamliquid.net or 173.231.136.216 with the time of sighting being :

```
{"values": ["teamliquid.net", "173.231.136.216"], "timestamp": 1460558710}
```

It is also possible to POST a STIX indicator with sighting data to the following URL (keep in mind that the content type has to be XML):

```
https://<misp url>/sightings/add/stix
```

MISP will use the sightings related observables to gather all values and create sightings for each attribute that matches any of the values. If no related observables are provided in the Sighting object, then MISP will fall back to the Indicator itself and use its observables' values to create the sightings. The time of the sighting is the current time, unless the timestamp attribute is set on the Sightings object, in which case that is taken.

An example STIX sightings document:

```
<stix:STIX_Package
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
  xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:example="http://example.com/"
  xsi:schemaLocation="
    http://stix.mitre.org/stix-1 ..../stix_core.xsd
    http://stix.mitre.org/Indicator-2 ..../indicator.xsd
    http://cybox.mitre.org/objects#DomainNameObject-1 http://cybox.mitre.org/XMLSchema/objects/Domain_Name/1.0/
    Domain_Name_Object.xsd
    http://stix.mitre.org/common-1 http://stix.mitre.org/XMLSchema/common/1.1.1/stix_common.xsd
    http://cybox.mitre.org/default_vocabularies-2 ..../cybox/cybox_default_vocabularies.xsd
    http://stix.mitre.org/default_vocabularies-1 ..../stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 ..../cybox/objects/Address_Object.xsd"
  id="example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d"
  timestamp="2014-05-08T09:00:00.000000Z"
  version="1.1.1"
  >
<stix:STIX_Header>
  <stix:Title>Example watchlist that contains IP information.</stix:Title>
  <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_Intent>
</stix:STIX_Header>
<stix:Indicators>
  <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-2e20c5b2-56fa-46cd-9662-8f199c69d2c9" timestamp="2014-05-08T09:00:00.000000Z">
```

```

<indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain Watchlist</indicator:Type>
<indicator:Observable id="example:Observable-87c9a5bb-d005-4b3e-8081-99f720fad62b">
    <cybox:Object id="example:Object-12c760ba-cd2c-4f5d-a37d-18212eac7928">
        <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType" type="FQDN">
            <DomainNameObj:Value condition="Equals" apply_condition="ANY">malicious1.example.com##com
ma##malicious2.example.com##comma##malicious3.example.com</DomainNameObj:Value>
        </cybox:Properties>
    </cybox:Object>
</indicator:Observable>
<indicator:Sightings>
    <indicator:Sighting timestamp="2014-05-08T09:00:00.000000Z">
        <indicator:Source>
            <stixCommon:Identity>
                <stixCommon:Name>FooBar Inc.</stixCommon:Name>
            </stixCommon:Identity>
        </indicator:Source>
        <indicator:Related_Observables>
            <indicator:Related_Observable>
                <stixCommon:Observable id="example:Observable-45b3acdf-1888-4bcc-89a9-6d9f8116fede">
                    <cybox:Object id="example:Object-a3d36250-42fa-4653-9172-87b87598390c">
                        <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType" type="FQDN">
                            <DomainNameObj:Value>malicious2.example.com</DomainNameObj:Value>
                        </cybox:Properties>
                    </cybox:Object>
                </stixCommon:Observable>
            </indicator:Related_Observable>
        </indicator:Related_Observables>
    </indicator:Sighting>
    <indicator:Sightings>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>

```

POSTing this as the message's body to MISP will sight any attributes visible to the user with the value "malicious2.example.com". For composite types, a match on a component will also trigger a sighting (so for example for attributes of type domain|ip a domain match would be sufficient).

If no Related observables are set in the Sighting itself, MISP will fall back to the `observable` directly contained in the indicator. So in the following example:

```

<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
        http://stix.mitre.org/stix-1 ..../stix_core.xsd
        http://stix.mitre.org/Indicator-2 ..../indicator.xsd
        http://cybox.mitre.org/objects#DomainNameObject-1 http://cybox.mitre.org/XMLSchema/objects/Domain_Name/1.0/
        Domain_Name_Object.xsd
        http://stix.mitre.org/common-1 http://stix.mitre.org/XMLSchema/common/1.1.1/stix_common.xsd
        http://cybox.mitre.org/default_vocabularies-2 ..../cybox/cybox_default_vocabularies.xsd
        http://stix.mitre.org/default_vocabularies-1 ..../stix_default_vocabularies.xsd
        http://cybox.mitre.org/objects#AddressObject-2 ..../cybox/objects/Address_Object.xsd"
    id="example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d"
    timestamp="2014-05-08T09:00:00.000000Z"
    version="1.1.1"
    >
    <stix:STIX_Header>
        <stix:Title>Example watchlist that contains IP information.</stix:Title>

```

```

<stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_Intent>
</stix:STIX_Header>
<stix:Indicators>
  <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-2e20c5b2-56fa-46cd-9662-8f199c69d2c9" timestamp="2014-05-08T09:00:00.000000Z">
    <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain Watchlist</indicator:Type>
    <indicator:Observable id="example:Observable-87c9a5bb-d005-4b3e-8081-99f720fad62b">
      <cybox:Object id="example:Object-12c760ba-cd2c-4f5d-a37d-18212eac7928">
        <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType" type="FQDN">
          <DomainNameObj:Value condition="Equals" apply_condition="ANY">malicious1.example.com##comma##malicious2.example.com##comma##malicious3.example.com</DomainNameObj:Value>
        </cybox:Properties>
      </cybox:Object>
    </indicator:Observable>
    <indicator:Sightings>
      <indicator:Sighting timestamp="2014-05-08T09:00:00.000000Z">
        <indicator:Source>
          <stixCommon:Identity>
            <stixCommon:Name>FooBar Inc.</stixCommon:Name>
          </stixCommon:Identity>
        </indicator:Source>
      </indicator:Sighting>
    </indicator:Sightings>
  </stix:Indicator>
</stix:Indicators>
</stix:STIX_Package>

```

MISP would create sightings for attributes matching any of the following: malicious1.example.com, malicious2.example.com, malicious3.example.com

## Warninglists API

### GET warninglists/index

#### Description

Return the index of warninglists enabled on the [MISP instance](#)

#### Parameters

- id

#### Output

```

...
[{"Warninglists":[{"Warninglist":{"id":"17","name":"List of known Office 365 URLs and IP address ranges","type":"string","description":"Office 365 URLs and IP address ranges","version":"20170212","enabled":true,"warninglist_entry_count":1516,"valid_attributes":"ip-src, ip-dst, domain|ip, hostname"}},{"Warninglist":{"id":"16","name":"List of known google domains","type":"string","description":"Event contains one or more entries of known google domains","version":"3","enabled":true,"warninglist_entry_count":665,"valid_attributes":"domain, hostname, domain|ip"}], {"Warninglist":{"id":"15","name":"List of hashes for EICAR test virus","type":"string","description":"Event contains one or more entries based on hashes for EICAR test virus","version":1,"enabled":true,"warninglist_entry_count":15,"valid_attributes":"md5, sha1, sha256, sha512, filename|md5, filename|sha1, filename|sha256, filename|sha512"}, {"Warninglist":{"id":"14","name":"Top 1000 website from Alexa","type":"string","description":"Event contains one or more entries from the top 1000 of the most used website (Alexa).","version":20170212,"enabled":true,"warninglist_entry_count":1000,"valid_attributes":"hostname, domain"}, {"Warninglist":{"id":"13","name":"TLDs as known by IANA","type":"string","description":"Event contains one or more TLDs as attribute with an IDS flag set","version":2,"enabled":true,"warninglist_entry_count":1290,"valid_attributes":"hostname, domain, domain|ip"}, {"Warninglist":{"id":"12","name":"Second level TLDs as known by Mozilla Foundation","type":"string","description":"Event contains one or more second level TLDs as attribute with an IDS flag set"}]}

```

```

set","version":"2","enabled":true,"warninglist_entry_count":6462,"valid_attributes":hostname, domain, domain
|ip"}},{"Warninglist":{"id":11,"name":"List of RFC 5735 CIDR blocks","type":"cidr","description":"Event conta
ins one or more entries part of the RFC 5735 CIDR blocks - Special Use IPv4 Addresses","version":2,"enabled":
true,"warninglist_entry_count":15,"valid_attributes":ip-src, ip-dst, domain|ip"}},{"Warninglist":{"id":10,
"name":"List of RFC 3849 CIDR blocks","type":"cidr","description":"Event contains one or more entries part of t
he IPv6 documentation prefix (RFC 3849)","version":2,"enabled":true,"warninglist_entry_count":1,"valid_attr
ibutes":ip-src, ip-dst, domain|ip"}},{"Warninglist":{"id":9,"name":"List of RFC 1918 CIDR blocks","type":"ci
dr","description":"Event contains one or more entries part of the RFC 1918 CIDR blocks","version":2,"enabled":
true,"warninglist_entry_count":3,"valid_attributes":ip-src, ip-dst, domain|ip"}},{"Warninglist":{"id":8,"
name":"List of known IPv6 public DNS resolvers","type":"string","description":"Event contains one or more publi
c IPv6 DNS resolvers as attribute with an IDS flag set","version":20160803,"enabled":true,"warninglist_entry_
count":172,"valid_attributes":ALL"}},{"Warninglist":{"id":7,"name":"List of known IPv4 public DNS resolver
s","type":"string","description":"Event contains one or more public IPv4 DNS resolvers as attribute with an IDS
flag set","version":20160803,"enabled":true,"warninglist_entry_count":77857,"valid_attributes":ALL"}},
{"Warninglist":{"id":6,"name":"List of RFC 5771 multicast CIDR blocks","type":"cidr","description":"Event contai
ns one or more entries part of the RFC 5771 multicast CIDR blocks","version":2,"enabled":true,"warninglist_en
try_count":16,"valid_attributes":ip-src, ip-dst, domain|ip"}},{"Warninglist":{"id":5,"name":"List of known
microsoft domains","type":"string","description":"Event contains one or more entries of known microsoft domain
s","version":1,"enabled":true,"warninglist_entry_count":152,"valid_attributes":domain, hostname, domain|ip
"}},{"Warninglist":{"id":4,"name":"List of IPv6 link local blocks","type":"cidr","description":"Event contain
s one or more entries part of the IPv6 link local prefix (RFC 4291)","version":1,"enabled":true,"warninglist_
entry_count":1,"valid_attributes":ip-src, ip-dst, domain|ip"}}

...

```

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: appli
cation/json" -X "GET" https://10.50.13.60/warninglists/index
```

## GET warninglists/view/1

### Description

Return the a warninglist by id

### Parameters

- id

### Output

```
to long
```

## Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json" --header "Content-Type: appli
cation/json" -X "GET" https://10.50.13.60/warninglists/view/17
```

## Attribute statistics API

If you are interested in the attribute type or attribute category data distribution on your instance, MISP offers an [API](#) that will create an aggregates list. To access the [API](#), simple sent a GET request to:

```
https://<misp url>/attributes/attributeStatistics/[context]/[percentage]
```

Where the following parameters can be set:

#### **Context**

Set whether you are interested in the type or category statistics of your instance. This parameter can be either set to "type" or "category", with type being the default setting if the parameter is not set.

#### **Percentage**

An optional field, if set, it will return the results in percentages instead of the count.

The results are always returned as JSON.

Sample output of the types in percentages from CIRCL's [MISP instance](#):

```
{  
    "AS": "0.015%",  
    "attachment": "0.177%",  
    "btc": "0.005%",  
    "campaign-name": "0.005%",  
    "comment": "1.47%",  
    "domain": "15.992%",  
    "domain|ip": "0.005%",  
    "email-attachment": "0.207%",  
    "email-dst": "0.121%",  
    "email-src": "0.192%",  
    "email-subject": "0.146%",  
    "filename": "3.698%",  
    "filename|md5": "0.349%",  
    "filename|sha1": "0.894%",  
    "filename|sha256": "0.652%",  
    "hostname": "17.558%",  
    "http-method": "0.045%",  
    "ip-dst": "7.087%",  
    "ip-src": "2.707%",  
    "link": "5.748%",  
    "malware-sample": "0.702%",  
    "malware-type": "0.005%",  
    "md5": "21.064%",  
    "mutex": "0.278%",  
    "named pipe": "0.03%",  
    "other": "1.495%",  
    "pattern-in-file": "0.192%",  
    "pattern-in-memory": "0.303%",  
    "pattern-in-traffic": "0.051%",  
    "regkey": "0.126%",  
    "regkey|value": "0.187%",  
    "sha1": "8.921%",  
    "sha256": "5.597%",  
    "snort": "0.045%",  
    "target-machine": "0.248%",  
    "target-org": "0.01%",  
    "target-user": "0.106%",  
    "text": "0.934%",  
    "threat-actor": "0.005%",  
    "url": "2.258%",  
    "user-agent": "0.081%",  
    "vulnerability": "0.182%",  
    "whois-registrant-email": "0.01%",  
    "x509-fingerprint-sha1": "0.01%",  
    "yara": "0.086%"  
}
```

## **Additional statistics**

Additional statistics are available as JSON which are the statistics also usable via the user interface. A ".json" can be appended to the following URLs:

```
- https://<misp url>/users/statistics/tags.json
- https://<misp url>/users/statistics.json
- https://<misp url>/users/statistics/attributehistogram.json
- https://<misp url>/users/statistics/orgs.json
```

An example output of https://users/statistics.json:

```
{
  "stats": {
    "event_count": 5233,
    "event_count_month": 21,
    "attribute_count": 645498,
    "attribute_count_month": 723,
    "correlation_count": 207152,
    "proposal_count": 48944,
    "user_count": 1073,
    "org_count": 587,
    "thread_count": 191,
    "thread_count_month": 0,
    "post_count": 337,
    "post_count_month": 0
  }
}
```

## MISP modules

### Description

It is possible call misp-modules directly from [API](#). If the module needs credentials, [API](#) will get the information directly from MISP configuration.

#### GET /modules/

Retrieve a list of all modules enabled.

#### Example

```
curl --header "Authorization: <APIKEY>" --header "Accept: application/json" --header "Content-Type: application/json" -X GET http://<MISP>/modules/
```

#### Output

```
[
  {
    "name": "passivetotal",
    "type": "expansion",
    "mispattributes": {
      "input": [
        "hostname",
        "domain",
        "ip-src",
        "ip-dst"
      ],
      "output": [
        "ip-src"
      ]
    }
  }
]
```

```
        "output": [
            "ip-src",
            "ip-dst",
            "hostname",
            "domain"
        ],
    },
    "meta": {
        "description": "PassiveTotal expansion service to expand values with multiple Passive DNS sources",
        "config": [
            "username",
            "password"
        ],
        "author": "Alexandre Dulaunoy",
        "version": "0.1"
    }
},
{
    "name": "sourcecache",
    "type": "expansion",
    "mispattributes": {
        "input": [
            "link"
        ],
        "output": [
            "link"
        ]
    },
    "meta": {
        "description": "Module to cache web pages of analysis reports, OSINT sources. The module returns a link of the cached page.",
        "author": "Alexandre Dulaunoy",
        "version": "0.1"
    }
},
{
    "name": "dns",
    "type": "expansion",
    "mispattributes": {
        "input": [
            "hostname",
            "domain"
        ],
        "output": [
            "ip-src",
            "ip-dst"
        ]
    },
    "meta": {
        "description": "Simple DNS expansion service to resolve IP address from MISP attributes",
        "author": "Alexandre Dulaunoy",
        "version": "0.1"
    }
}
```

## POST /modules/queryEnrichment

Call any enabled module.

### Example

Content of dns.json

```
{
```

```
        "hostname": "www.foo.be",
        "module": "dns"
    }
```

Query using MISP [API](#)

```
curl --header "Authorization: <APIKEY>" --header "Accept: application/json" --header "Content-Type: application/json" --data @dns.json -X POST http://<MISP>/modules/queryEnrichment
```

The output will be following JSON:

```
{
    "results": [
        {
            "types": [
                "ip-src",
                "ip-dst"
            ],
            "values": [
                "188.65.217.78"
            ]
        }
    ]
}
```

Last modified: Fri Apr 12 2019 12:03:26 GMT+0200 (CEST)

## PyMISP - Python Library to access MISP

PyMISP is a Python library to access MISP platforms via their REST [API](#).

PyMISP allows you to fetch events, add or update events/attributes, add or update samples or search for attributes.

Note that you need to have Auth Key access in your [MISP instance](#) to use PyMISP

### Capabilities

- Add, get, update, publish, delete events
- Add or remove tags
- Add file attributes: hashes, registry key, patterns, pipe, mutex
- Add network attributes: IP dest/src, hostname, domain, url, UA, ...
- Add Email attributes: source, destination, subject, attachment, ...
- Upload/download samples
- Update sightings
- [Proposals](#): add, edit, accept, discard
- Full text search and search by attributes
- Get STIX event
- Export statistics And even more, just look at the [api.py](#) file

### Installation

You can install PyMISP by either using pip or by getting the last version from the [GitHub repository](#)

#### Install from pip

```
pip install pymisp
```

#### Install the latest version from the repository

```
git clone https://github.com/MISP/PyMISP.git && cd PyMISP
python setup.py install
```

Note that you will also need to install [requests](#) if you don't have it already.

### Getting started

You now need to get your automation key. You can find it on the automation page:

```
https://<misp url>/events/automation
```

or on your profile

```
https://<misp url>/users/view/me
```

If you did not install using the repository, you can still fetch it to get examples to work on:

```
git clone https://github.com/MISP/PyMISP.git
```

In order to use these, you need to create a file named `keys.py` in the examples folder and edit it to put the url of your [MISP instance](#) and your automation key.

```
cd examples
cp keys.py.sample keys.py
vim keys.py
```

Once you are done with it, you are ready to start.

This is how `keys.py` looks:

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

misp_url = 'https://'
misp_key = 'Your MISP auth key' # The MISP auth key can be found on the MISP web interface under the automation section
misp_verifycert = True
```

## Using PyMISP

To have a better understanding of how to use PyMISP, we will have a look at one of the existing examples:

`add_named_attribute.py` This script allow us to add an attribute to an existing event while knowing only its type (the category is determined by default).

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

from pymisp import PyMISP
from keys import misp_url, misp_key
import argparse
```

First of all, it is obvious that we need to import PyMISP. Then we also need to know both the instance with which we will work and the [API](#) key to use: Both should be stored in the `keys.py` file. Finally we import argparse library so the script can handle arguments.

```
# For python2 & 3 compat, a bit dirty, but it seems to be the least bad one
try:
    input = raw_input
except NameError:
    pass
```

Just a few lines to be sure that python 2 and 3 are supported

```
def init(url, key):
    return PyMISP(url, key, True, 'json', debug=True)
```

This function will create a PyMISP object that will be used later to interact with the [MISP instance](#). As seen in the `api.py`, a PyMISP object need both the URL of the [MISP instance](#) and the [API](#) key to use. It can also take additional and not mandatory data, such as the use or not of SSL or the name of the export format.

```
if __name__ == '__main__':
    parser = argparse.ArgumentParser(description='Create an event on MISP.')
    parser.add_argument("-e", "--event", type=int, help="The id of the event to update.")
```

```
parser.add_argument("-t", "--type", help="The type of the added attribute")
parser.add_argument("-v", "--value", help="The value of the attribute")
args = parser.parse_args()
```

Then the function starts by preparing the awaited arguments:

- **event**: The event that will get a new attribute
- **type**: The type of the attribute that will be added. See [here](#) for more information
- **value**: The value of the new attribute

```
misp = init(misp_url, misp_key)
```

Thanks to the previously created function, we create a PyMISP object.

```
event = misp.get_event(args.event)
event = misp.add_named_attribute(event, args.type, args.value)
```

In order to add the new argument, we first need to fetch the event in the MISP database using the `get_event` function which only need the `event_id`. Then only once we have it, we can call the function `add_named_attribute` that will add the argument.

```
print(event)
```

Finally the new event is printed, so we can check that the attribute was correctly added, and that a category was attached to it automatically.

## Existing examples

As the name implies you will find several example scripts in the examples folder. For each you can get help if you do  
`scriptname.py -h`

Let us have a look at some of these examples:

### **add\_named\_attribute.py**

Allow to add an argument to an existing event by giving only the type of the attribute. The category will be set with a default value.

Arguments:

- **event**: The id of the event to update.
- **type**: The type of the added attribute.
- **value**: The value of the attribute.

### **add\_user.py**

Allow to add a user by giving the mandatory fields as entries.

Arguments:

- **email**: Email linked to the account.
- **org\_id**: Organisation linked to the user.
- **role\_id**: Role linked to the user.

### **add\_user\_json.py**

Add the user described in the given json. If no file is provided, returns a json listing all the fields used to describe a user.

Arguments:

- **json\_file**: The name of the json file describing the user you want to create.

## create\_events.py

Allow a user to create a new event on the [MISP instance](#).

Arguments:

- **distrib**: The distribution setting used for the attributes and for the newly created event, if relevant. [0-3].
- **info**: Used to populate the event info field if no event ID supplied.
- **analysis**: The analysis level of the newly created event, if applicable. [0-2]
- **threat**: The threat level ID of the newly created event, if applicable. [1-4]

## del.py

Delete an event or an attribute from a [MISP instance](#). The event has the priority: if both are set, only the event will be deleted.

Arguments:

- **event**: Event ID to delete.
- **attribute**: Attribute ID to delete.

## delete\_user.py

Delete the user with the given id. Keep in mind that disabling users (by setting the disabled flag via an edit) is always preferred to keep user associations to events intact.

Arguments:

- **user\_id**: The id of the user you want to delete.

## edit\_user.py

Edit the email of the user designed by the user\_id.

Arguments:

- **user\_id**: The name of the json file describing the user you want to modify.
- **email**: Email linked to the account.

## edit\_user\_json.py

Edit the user designed by the user\_id. If no file is provided, returns a json listing all the fields used to describe a user.

Arguments:

- **user\_id**: The name of the json file describing the user you want to modify.
- **json\_file**: The name of the json file describing your modifications.

## get.py

Get an event from a [MISP instance](#) in json format.

Arguments:

- **event**: Event ID to get.

- **output:** Output file

## last.py

Download latest events from a [MISP instance](#). A output file can be created to store these events.

Arguments:

- **last:** can be defined in days, hours, minutes (for example 5d or 12h or 30m).
- **output:** Output file

## searchall.py

Get all the events matching a value.

Arguments:

- **search:** String to search.
- **quiet:** Only display URLs to MISP
- **output:** Output file

## sharing\_groups.py

Get a list of the [sharing groups](#) from the [MISP instance](#). No argument.

## sighting.py

Add sighting.

Arguments:

- **json\_file:** The name of the json file describing the attribute you want to add sighting to.

## stats.py

Output attributes statistics from a [MISP instance](#). No argument.

## suricata.py

Download Suricata events.

Arguments:

- **all:** Download all suricata rules available.
- **event:** Download suricata rules from one event.

## tags.py

Get tags from [MISP instance](#). No argument.

## tagstatistics.py

Get statistics from tags.

Arguments:

- **percentage:** An optional field, if set, it will return the results in percentages, otherwise it returns exact count.

- **namesort**: An optional field, if set, values are sort by the namespace, otherwise the sorting will happen on the value.

## up.py

Update an existing event regarding the data inside a given json file.

Arguments:

- **event**: Event ID to modify.
- **input**: Input file

## upload.py

Send malware sample to MISP.

Arguments:

- **upload**: File or directory of files to upload.
- **event**: Not supplying an event ID will cause MISP to create a single new event for all of the POSTed malware samples.
- **distrib**: The distribution setting used for the attributes and for the newly created event, if relevant. [0-3].
- **ids**: You can flag all attributes created during the transaction to be marked as \"to\_ids\" or not.
- **categ**: The category that will be assigned to the uploaded samples. Valid options are: Payload delivery, Artefacts dropped, Payload Installation, External Analysis.
- **info**: Used to populate the event info field if no event ID supplied.
- **analysis**: The analysis level of the newly created event, if applicable. [0-2]
- **threat**: The threat level ID of the newly created event, if applicable. [1-4]
- **comment**: Comment for the uploaded file(s).

## users\_list.py

Get a list of the [sharing groups](#) from the [MISP instance](#). No argument.

## Going further

### feed-generator

It is used to generate the CIRCL [OSINT](#) feed. This script export the events as json, based on tags, organisation, events, ... It automatically update the dumps and the metadata file.

Here is an example of a config file:

```
url = ''  
key = ''  
ssl = True  
outputdir = 'output'  
# filters = {'tag' : 'tlp : white|feed-export|!privint', 'org':'CIRCL'}  
filters = {}  
  
valid_attribute_distribution_levels = ['0', '1', '2', '3', '4', '5']
```

## Consuming feed

As the feed is a simple set of MISP json files, the files can be easily imported directly into any [MISP instance](#). The script below processes the manifest file of an [OSINT](#) feed and reimport them in a MISP directly.

```

#!/usr/bin/env python
# -*- coding: utf-8 -*-

from pymisp import PyMISP
import requests

url = 'https://www.circl.lu/doc/misp/feed-osint/'
osintcircl = requests.get('{}.manifest.json'.format(url))

misp = PyMISP('http://misp.test/', 'key', False, 'json')
for uri in osintcircl.json():
    req = requests.get('{}.{}.json'.format(url,uri))
    misp.add_event(req.json())

```

## ioc-2-misp

Allow to import OpenIOC files into MISP easily. It is also possible to set specific tags on these events.

## Situational Awareness

- attribute\_treemap.py generate a tree-map showing the distribution of the attributes on the [MISP instance](#).
- tags\_\* : these functions help having statistics and graphs about the tag repartition.

## Simple example on fetching the last events

```

#!/usr/bin/env python
# -*- coding: utf-8 -*-

from pymisp import PyMISP
from keys import misp_url, misp_key, misp_verifycert
import argparse
import os
import json

# Usage for pipe masters: ./last.py -l 5h | jq .

def init(url, key):
    return PyMISP(url, key, misp_verifycert, 'json')

def download_last(m, last, out=None):
    result = m.download_last(last)
    if out is None:
        if 'response' in result:
            print(json.dumps(result['response']))
        else:
            print('No results for that time period')
            exit(0)
    else:
        with open(out, 'w') as f:
            f.write(json.dumps(result['response']))

if __name__ == '__main__':
    parser = argparse.ArgumentParser(description='Download latest events from a MISP instance.')
    parser.add_argument("-l", "--last", required=True, help="can be defined in days, hours, minutes (for example 5d or 12h or 30m).")
    parser.add_argument("-o", "--output", help="Output file")

    args = parser.parse_args()

    if args.output is not None and os.path.exists(args.output):

```

```
print('Output file already exists, abord.')
exit(0)

misp = init(misp_url, misp_key)

download_last(misp, args.last, args.output)
```

Last modified: Tue Aug 28 2018 21:13:11 GMT+0200 (CEST)

## Create an event based on a report

[warning] A specific permission is required to create an event.

For this example, we will use a report found on [Bleeping Computer](#), so considered as [OSINT](#).

### Researcher finds the Karma Ransomware being distributed via Pay-per-Install Network

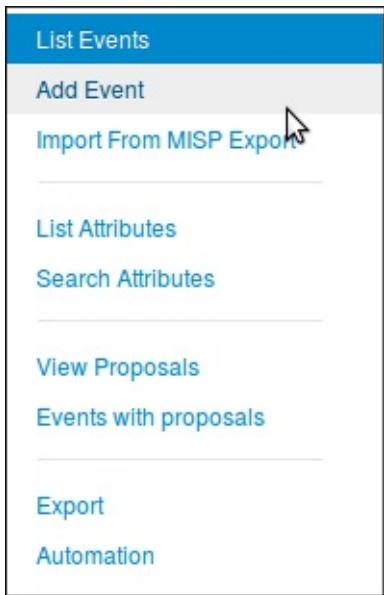
By [Lawrence Abrams](#)

 November 14, 2016  07:01 PM  2

A security researcher named [slipstream/RoL](#) has discovered the Karma Ransomware, which pretends to be a Windows optimization program called Windows-TuneUp. What is worse is that this sample was discovered as software that would potentially be distributed by a pay-per-install software monetization company when people install free software downloaded from the Internet.

## Adding an event

First of all, we need to create a new event. To do so, we click the "Add Event" option when on the Events list view.



Then we get the add event form.

## Add Event

Date	Distribution <small>i</small>
2016-11-16	All communities
Threat Level <small>i</small>	Analysis <small>i</small>
High	Initial
Event Info	
Quick Event Description or Tracking Info	
<b>GFI sandbox</b>	
Browse...	No file selected.
<b>Add</b>	

Let's fill it with the data we already have:

- Date: Here we will put the date of the report, so 2016-11-14
- Distribution: Depending on the event, we might want it to be more or less spread across the MISP instances. For this one, since it is a public report, there is no reason to limit the diffusion so "All communities".
- Threat Level: Self explanatory. Since the ransomware in the report is not using a huge exploit, we can use low, or undefined as we don't really know. we'll go for the latter since it can be edited.
- Analysis: Give the current stage of the analysis. Since the report is published, we can assume that the analysis is completed.
- Event Info: The event's info is in fact the name or title of the event, so it seems legit to put the title of the report here as well. Since it is public information, we also prefix it with "OSINT".
- GFI sandbox: Since we don't have any sample or anything here, we leave this alone.

### Add Event

Date	Distribution <small>i</small>
2016-11-14	All communities
Threat Level <small>i</small>	Analysis <small>i</small>
Undefined	Completed
Event Info	
OSINT - Researcher finds the Karma Ransomware being distributed via	
GFI sandbox	
Browse...	No file selected.
<b>Add</b>	

Then just press the blue "Add" button and here we have a brand new event. Empty.

The event has been saved

## OSINT - Researcher finds the Karma Ransomware being dis...

Event ID	801
Uuid	582d6967-3054-4108-a7ac-40c6950d210f
Org	CIRCL
Owner org	CIRCL
Contributors	[REDACTED]
Email	[REDACTED]
Tags	[REDACTED]
Date	2016-11-14
Threat Level	Undefined
Analysis	Completed
Distribution	All communities
Info	OSINT - Researcher finds the Karma Ransomware being distributed via Pay-per-Install Network
Published	No
Sightings	0 (0)

Pivots   Attributes   Discussion

801: OSINT ...

« previous   next »   view all

**Attribute warning:** This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (Indicators, observables, etc.)

Date   Org   Category   Type   Value

Filters: All File Network Financial Proposal Correlation Warning

« previous   next »   view all

(Displayed information can change depending on your role on the [MISP instance](#))

## Adding Attributes

Now it is time to populate this event. But before even adding [IoC](#), we are going to add global information about the report itself: the link of the report and a short explanation or introduction. To do so, we need to click on the "Add Attribute" option in the side menu. This will show us this view:

**Add Attribute**

**Category i** **Type i**

(choose one) (first choose category)

**Distribution i**

Inherit event

**Value**

Contextual Comment

for Intrusion Detection System  Batch Import

**Submit**

- First we are going to add the link of the report. Since it has been written by an other researcher, it will be considered as an "External analysis", we choose this category.
- Concerning the type, regarding the kind of data we are adding it is obvious that we will choose the "link" type.
- The distribution field can be a little tricky. We can either choose one of the option that was already available at event level or "Inherit event". If we choose the latter, the attribute will be shared the same way as the event it is included in (here to "All communities"). On the other hand, if we choose manually a distribution for the attribute, the most restrictive between event distribution and attribute distribution will be applied. That is to say: if both event and attribute distributions are the same, there will be no change (similar to "Inherit event"). However, if for instance the event distribution is "all communities" while the attribute is limited to "This community only", the event will indeed be distributed to all communities but without this particular attribute which will be limited to this community only. The same works the other way around, if the attribute can be distributed to "all communities" while the related event is limited to this community, the attribute being dependant of the event, it will be shared to this community only, basing its distribution on the event (most restrictive) one.
- The value is simply the data we want to add, here it is the link of the report.
- The contextual comment is a field that will not be used for correlation and is mainly there to add some complementary information on the attribute. Can be a port for an IP, or an indication of any type. Here there is no particular information to add, except maybe tell that it is the source of the report, so let us put this information.
- "for Intrusion Detection System" is used to set the IDS flag or not. If set, the attribute will be used as an IDS signature when exporting the NIDS data. In this case, we have no reason to check it.
- The Batch Import is a useful option when we need to add several IoC of the same category/type which allow you to add them at once by separated by a line break between each line in the value field. However it is of no use here.

## Add Attribute

**Category i**      **Type i**

**Distribution i**

**Value**

<http://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/>

**Contextual Comment**

Source Report

Submit

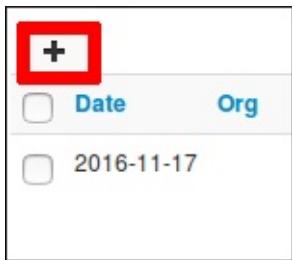
All fields are properly filled ? Then let's press the "submit" button, and Ta-dah !

The attribute has been saved

### OSINT - Researcher finds the Karma Ransomware being dis...

Event ID	801												
Uuld	582d6967-3054-4108-a7ac-40c6950d210f												
Org	CIRCL												
Owner org	CIRCL												
Contributors													
Email	[REDACTED]												
Tags	[REDACTED]												
Date	2016-11-14												
Threat Level	Undefined												
Analysis	Completed												
Distribution	All communities												
Info	OSINT - Researcher finds the Karma Ransomware being distributed via Pay-per-Install Network												
<b>Published</b>	<b>No</b>												
Sightings	0 (0)												
<a href="#">- Pivots</a> <a href="#">- Attributes</a> <a href="#">- Discussion</a>													
<a href="#">801: OSINT ...</a>													
<a href="#">« previous</a> <a href="#">next »</a> <a href="#">view all</a>													
<input style="float: left; margin-right: 10px;" type="button" value="+"/> <span style="float: left; margin-right: 10px;"> </span> <span style="float: left; margin-right: 10px;">Filters:</span> <input checked="" type="radio"/> All <input type="radio"/> File <input type="radio"/> Network <input type="radio"/> Financial <input type="radio"/> Proposal <input type="radio"/> Correlation <input type="radio"/> Warnings <input type="radio"/> Include deleted attributes <input type="radio"/> Show context fields													
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Date</th> <th style="text-align: left; padding: 2px;">Org</th> <th style="text-align: left; padding: 2px;">Category</th> <th style="text-align: left; padding: 2px;">Type</th> <th style="text-align: left; padding: 2px;">Value</th> <th style="text-align: right; padding: 2px;">Comment</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;">2016-11-17</td> <td style="padding: 2px;"></td> <td style="padding: 2px;">External analysis</td> <td style="padding: 2px;">link</td> <td style="padding: 2px;">http://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/</td> <td style="text-align: right; padding: 2px;">Source Report</td> </tr> </tbody> </table>		Date	Org	Category	Type	Value	Comment	2016-11-17		External analysis	link	http://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/	Source Report
Date	Org	Category	Type	Value	Comment								
2016-11-17		External analysis	link	http://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/	Source Report								

Now we can do a similar procedure to add an introduction to the report (that is to say the first paragraph of the report). We will simply change the type for text. But this time, we will access the add attribute form by clicking on the small + symbol next to the attribute table.



The same form as before will appear in a popup.

**Add Attribute**

<b>Category <small>i</small></b>	<b>Type <small>i</small></b>
(choose one)	(first choose category)
<b>Distribution <small>i</small></b>	
Inherit event	
<b>Value</b>	
<b>Contextual Comment</b>	
<input type="checkbox"/> for Intrusion Detection System	<input type="checkbox"/> Batch Import
<b>Submit</b>	<b>Cancel</b>

Again, we fill it with the required data.

**Add Attribute**

<b>Category</b> ⓘ	<b>Type</b> ⓘ
External analysis	text
<b>Distribution</b> ⓘ	
Inherit event	
<b>Value</b>	
A security researcher named slipstream/RoL has discovered the Karma Ransomware, which pretends to be a Windows optimization program called Windows-TuneUp. What is worse is that this sample was discovered as software that would potentially be distributed by a pay-per-install software monetization company when people install free software downloaded from the Internet.	
<b>Contextual Comment</b>	
Source Report	
<input type="checkbox"/> for Intrusion Detection System	<input type="checkbox"/> Batch Import
<b>Submit</b>	<b>Cancel</b>

Then we submit it by clicking on the blue button *Et voilà!*

  					
				Filters: All File Network Financial Proposal Correlation Warnings In	
<input type="checkbox"/>	Date	Org	Category	Type	Value
Show context fields					
	2016-11-17	External analysis	link	Source	No
	2016-11-17	External analysis	text	Report	No

Okay, now it is time to add some [Indicators](#) of Compromise. In this report, they are mainly listed at the end.

### Files associated with the Karma Ransomware

Windows-TuneUp.exe

### Registry entries associated with the Karma Ransomware

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer "auth"  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ "Saffron"= "%Desktop%\# DECRYPT MY FILES #.html"  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ "Safron"= "%Desktop%\# DECRYPT MY FILES #.txt"
```

### IOCs:

```
SHA256: 6545ae2b8811884ad257a7fb25b1eb0cb63cfc66a742fa76fd44bdd05b74fe8  
SHA256: cf5fda29f8e1f135aa68620ce7298e930be2cb93888e3f04c9cd0b13f5bc4092
```

### Network Communication:

```
karma2xgg6ccmupd.onion  
windows-tuneup.com/web293/xUser.php
```

Let's try to define which category/type those IoC belong to.

First, Windows-TuneUp.exe is without a doubt a *filename*, and the associated category may be *Payload delivery*.

Second the registry entries (type *regkey*) seems to be from *Artifacts dropped* category

Then the hashes that are already said to be *SHA 256*, and a quick test on VirusTotal also reveals that they correspond to the filename seen earlier. so we can add both as an association *filename|SHA256*. Once again, the category will be *Payload delivery*.

And finally the network communication. No doubt here for the category: *Network activity*, and the type might be *url* but for the example, we will let MISP decide for us.

So we begin with the filename. No real change from before for this one, except that we will set the IDS flag to true.

**Add Attribute**

Category <small>i</small>	Type <small>i</small>
Payload delivery	filename
Distribution <small>i</small>	
Inherit event	
Value	<input type="text" value="Windows-TuneUp.exe"/>
Contextual Comment	<input type="text"/>
<input checked="" type="checkbox"/> for Intrusion Detection System <input type="checkbox"/> Batch Import	
<b>Submit</b>	<b>Cancel</b>

## Freetext Import Tool

Then we can add the hashes in a similar way. We will have them both alone and combined with the filename. In order to do it quickly, we are going to use the freetext import tool, hidden there



It will open a popup with a text area field where we will paste our [IoC](#), one per line. As said previously, we add both the hashes alone and with the filename.

**Freetext Import Tool**

Paste a list of IOCs into the field below for automatic detection.

```
6545ae2b8811884ad257a7fb25b1eb0cb63fcf66a742fa76fd44bdd05b74fe8  
cf5fda29f8e1f135aa68620ce7298e930be2cb93888e3f04c9cd0b13f5bc4092  
Windows-TuneUp.exe|6545ae2b8811884ad257a7fb25b1eb0cb63fcf66a742fa76fd44bdd05b74fe8  
Windows-TuneUp.exe|cf5fda29f8e1f135aa68620ce7298e930be2cb93888e3f04c9cd0b13f5bc4092
```

**Submit** **Cancel**

Then when we press the submit button, we are redirected on this page to control the sent data.

### Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS	Comment	Actions
6545ae2b8811884ad257a		Payload delivery	sha256	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	X
cf5fda29f8e1f135aa68620		Payload delivery	sha256	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	X
Windows-TuneUp.exe 654		Payload delivery	filename\sha256	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	X
Windows-TuneUp.exe cf5f		Payload delivery	filename\sha256	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	X

**Submit**

sha256 → authentihash **Change all**

**Update all comment fields** **Change all**

Here, MISP detected by itself what should be the category and type associated to our [IoC](#) and surprise! It matches our suppositions. Plus, it also put the IDS flag, so it is perfect. But before submitting, please double check to be sure all the values are correct and no information was lost (That can happen when the data are not formatted as expected by MISP).

If the results of MISP were not what we expected, we can still modify it, however MISP will only suggest suitable category/type regarding the format of your data. We can change for each attribute individually or all at the same time using the option on the bottom right of the form. The same principle also applies for the comments, individually or for all.

Category	Type	IDS
Payload delivery	sha256	<input checked="" type="checkbox"/>
Payload delivery	sha256	<input checked="" type="checkbox"/>
Artifacts dropped	authentihash	<input checked="" type="checkbox"/>
Payload installation	sha512/256	<input checked="" type="checkbox"/>
External analysis		<input checked="" type="checkbox"/>
Payload delivery	filename sha256	<input checked="" type="checkbox"/>

(Yes I have two cursors, MISP is magic!)

We only have the network [indicators](#) left, and as said before, we will let MISP determine for us which type is the best for the data we have.

**Freetext Import Tool**

Paste a list of IOCs into the field below for automatic detection.

karma2xgg6ccmupd.onion  
windows-tuneup.com/web293/xUser.php

**Submit** **Cancel**

## Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered.

Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS
karma2xgg6ccmupd.onion		Payload delivery	filename	<input checked="" type="checkbox"/>
windows-tuneup.com/web293/xUser.php		Network activity	url	<input checked="" type="checkbox"/>

**Submit**

[Update all comment fields](#)

Oh well, that was unexpected. In fact, it is not that surprising regarding the format of the tor address that look more like a filename than like a url but it is still a problem, since we can't change the type nor the category to a more consistant one. This is indeed one of the limitation of freetext import. To solve this issue, we will use a simple trick: we will add a slash at the end of the tor address so it won't be confused for a filename.

**Freetext Import Tool**

Paste a list of IOCs into the field below for automatic detection.

karma2xgg6ccmupd.onion/  
windows-tuneup.com/web293/xUser.php

**Submit** **Cancel**

## Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be available.

Proposals instead of attributes

Value	Similar Attributes	Category	Type
karma2xgg6ccmupd.onion/		Network activity	url
windows-tuneup.com/web293/xUser.php		Network activity	url

Thanks to the added character, the first string is recognised as an url which is more consistent with the reality. The second also seems okay, so we can now submit both.

## Batch Import

The Freetext Import works properly only with a string of data without any spaces in one line. But if you have lines of text with spaces between values, like e.g.

### Associated Files:

```
%Appdata%\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta  
%Appdata%\Microsoft\Windows\Start Menu\Programs\Startup\cmb_ransomware.exe  
%Appdata%\Info.hta  
%UserProfile%\Desktop\FILES ENCRYPTED.txt  
C:\Users\Public\Desktop\FILES ENCRYPTED.txt
```

you can still import them at once using the "Add Attribute" option. Click on *Add Attribute*, copy the data and paste it into the *Value* box. Choose the right category and type. Now check both checkboxes for *Intrusion Detection System* and *Batch Import*. The option *Batch Import* will import your data line for line just like the *Freetext Import* option without losing any information. Like this:

The screenshot shows a user interface for managing events. At the top, there's a navigation bar with links: Home, Event Actions ▾, Galaxies ▾, Input Filters ▾, and Global Actions ▾. On the left, a sidebar lists various actions: View Event, View Correlation Graph, View Event History, Edit Event, Delete Event, **Add Attribute** (which is selected), Add Object, Add Attachment, Populate from..., Enrich Event, Merge attributes from..., Publish Event, Publish (no email), Publish event to ZMQ, Contact Reporter, Download as..., List Events, and Add Event.

The main content area is titled "Add Attribute". A red banner at the top asks, "Did you consider adding an object instead of a composite attribute?". Below this, there are fields for "Category" (set to "Artifacts dropped") and "Type" (set to "regkey|value"). Under "Distribution", the dropdown is set to "Inherit event". The "Value" field contains the following text, which is also highlighted in red:

```
%Appdata%\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta
%Appdata%\Microsoft\Windows\Start Menu\Programs\Startup
\cmb_ransomware.exe
%Appdata%\Info.hta
%UserProfile%\Desktop\FILES ENCRYPTED.txt
C:\Users\Public\Desktop\FILES ENCRYPTED.txt
```

Below the value field is a "Contextual Comment" input box, which is currently empty. At the bottom of the form, there are two checkboxes: "for Intrusion Detection System" and "Batch Import", both of which are checked. A "Notices:" section contains a note about GDPR compliance: "[gdpr]: This attribute is likely to contain personal data and the data subject could be potentially directly identifiable. Please verify. Where applicable, please ensure that you have taken the necessary steps to ensure transparency towards the data subjects in". Finally, a blue "Submit" button is located at the bottom left.

And that is all we can get for the main informations and [IoC](#) in this report. If we search more carefully, there might still be some information left in it, like the filename of the ransomnote for instance, but we will stop here for this example.

## Modify the event

If you want to modify your event from the home page, you can either double click on the event or click the edit symbol located in the column **Actions** on the right side. You will be redirected to the editing mode of the selected event.

Last modified: Sat Jul 13 2019 10:06:38 GMT+0200 (CEST)

- [Taxonomies](#)
- [Contributing to Taxonomy](#)
- [Reserved Taxonomy](#)
- [Adding Taxonomy in MISP](#)
- [Adding a private taxonomy](#)
- [How to use Taxonomy in MISP](#)
  - [Filtering the distribution of events among MISP instances](#)
  - [MISP Taxonomies - tools](#)
  - [Other use cases using MISP taxonomies](#)
- [Future functionalities related to MISP taxonomies](#)

## Taxonomies

In MISP 2.4.X, a flexible mechanism has been introduced to support various [taxonomy of classification](#).

You can access the taxonomy by going into 'Event Actions' and select 'List Taxonomies'. For fresh install, make sure to click 'Update Taxonomies' to view available taxonomies.

A [complete list of the available taxonomies PDF](#) are available on the MISP project website.

List Taxonomies					
Taxonomies					
<a href="#">Id</a>	<a href="#">Namespace</a>	<a href="#">Description</a>		<a href="#">Version</a>	<a href="#">Enabled</a>
8	nato	NATO classification markings.		1	<span>Yes</span>
7	eucl	EU classified information' (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.		1	<span>Yes</span>
6	dni-ism	A subset of Information Security Marking Metadata ISM as required by Executive Order (EO) 13526. As described by DNI.gov as Data Encoding Specifications for Information Security Marking Metadata in Controlled Vocabulary Enumeration Values for ISM		3	<span>No</span>
5	ecisrt	Incident Classification by the ecisrt.net project WP4 clearinghouse policy and updated by IntelMQ.		1	<span>Yes</span>
4	veris	Vocabulary for Event Recording and Incident Sharing (VERIS)		2	<span>No</span>
3	tip	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.		1	<span>Yes</span>
2	circl	CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection		1	<span>Yes</span>
1	admiralty-scale	The Admiralty Scale (also called the NATO System) is used to rank the reliability of a source and the credibility of an information.		1	<span>Yes</span>

Page 1 of 1, showing 8 records out of 8 total, starting on record 1, ending on 8

The following taxonomies can be used in MISP (as local or distributed tags) or in other tools willing to share common taxonomies among security information sharing tools.

## MISP taxonomies – Flexible Classification for Information Sharing

MISP taxonomies is a solution to use existing taxonomies (or create your own) to classify your cybersecurity events, indicators and threats. This technique is integrated as a default mechanism for tagging in MISP (Malware Information Sharing Platform & Threat Sharing) and to support a distributed classification where organizations can share common taxonomies in a local or distributed fashion.

Classifications are distributed as simple JSON files to use with MISP but can be easily integrated into any other information sharing software. You can also propose new taxonomies to the community.

Examples of machine tags and human readable tags :

**admiralty-scale:source-reliability="c"**  
admiralty-scale:Source Reliability="Fairly reliable"

**admiralty-scale:information-credibility="3"**  
admiralty-scale:Information Credibility="Possibly true"

**nato:classification="NU"**  
nato:Classification="NATO UNCLASSIFIED"

**tlp:amber**

Traffic Light Protocol (TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.

namespace  
predicate  
value



<https://github.com/MISP/misp-taxonomies/>

1. [Admiralty Scale](#): The Admiralty Scale (also called the NATO System) is used to rank the reliability of a source and the credibility of an information.
2. [adversary](#) An overview and description of the adversary infrastructure.
3. [CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection](#) CIRCL Taxonomy is a simple scheme for incident classification and area topic where the incident took place.
4. [Cyber Kill Chain](#) from Lockheed Martin as described in [Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains](#).
5. DE German (DE) [Government classification markings \(VS\)](#) Taxonomy for the handling of protectively marked information in MISP with German (DE) Government classification markings (VS).
6. [DHS CIIP Sectors](#) DHS critical sectors as described in <https://www.dhs.gov/critical-infrastructure-sectors>.
7. [Diamond Model for Intrusion Analysis](#), a phase-based model developed by Lockheed Martin, aims to help categorise and identify the stage of an attack.
8. [Domain Name Abuse](#) - taxonomy to tag domain names used for cybercrime. Use europol-incident to tag abuse-activity
9. [eCSIRT](#) eCSIRT incident classification Appendix C of the eCSIRT EU project including IntelMQ updates.
10. [ENISA](#) ENISA Threat Taxonomy - A tool for structuring threat information [as published](#)
11. [Estimative Language](#) Estimative language - including likelihood or probability of event based on the Intelligence Community Directive 203 (ICD 203) (6.2.(a)).
12. [EU Marketop and Publicadmin][EU critical sectors](#) Market operators and public administrations that must comply to some notifications requirements under EU NIS directive.
13. [EUCI](#) EU classified information (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States [as described](#).
14. [Europol Incident](#) EUROPOL class of incident taxonomy
15. [Europol Events](#) - EUROPOL type of events taxonomy
16. [FIRST CSIRT Case](#) FIRST CSIRT Case Classification.
17. [FIRST Information Exchange Policy \(IEP\)](#) framework
18. [French gov information classification system](#)
19. [Information Security Indicators](#) Information security [indicators](#) have been standardized by the [ETSI Industrial Specification Group \(ISG\) ISI](#). These [indicators](#) provide the basis to switch from a qualitative to a quantitative culture in IT Security Scope of measurements: External and internal threats (attempt and success), user's deviant behaviours, nonconformities and/or vulnerabilities (software, configuration, behavioural, general security framework).
20. [Information Security Marking Metadata \(ISM\) V13](#) as described by DNI.gov.
21. [Malware](#) classification based on different categories. Based on a [SANS whitepaper about malware](#).
22. Malware Type and Platform classification based on Microsoft's implementation of the [Computer Antivirus Research Organization \(CARO\)](#) Naming Scheme and Malware Terminology. Based on [Microsoft Malware naming conventions](#), [Microsoft Glossary](#), [Microsoft Objective Criteria](#), and [CARO's definitions](#). Malware families are extracted from Microsoft SIRs since 2008 based on [Microsoft Malware, virus, and threat encyclopedia](#). Note that SIRs do NOT include all Microsoft malware families.
23. [MISP taxonomy](#) to infer with MISP behavior or operation.

24. [ms-caro-malware](#) Malware Type and Platform classification based on Microsoft's implementation of the Computer Antivirus Research Organization (CARO) Naming Scheme and Malware Terminology.
25. [NATO Classification Marking](#) Marking of Classified and Unclassified materials as described by the North Atlantic Treaty Organization, NATO.
26. [Open Threat Taxonomy v1.1 \(SANS\)](#) based on James Tarala of SANS ([http://www.auditscripts.com/resources/open\\_threat\\_taxonomy\\_v1.1a.pdf](http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf)).
27. [OSINT Open Source Intelligence - Classification](#)
28. [The Permissible Actions Protocol - or short: PAP](#) PAP was designed to indicate how the received information can be used. It's a protocol/taxonomy similar to TLP informing the recipients of information what they can do with the received information.
29. Status of events used in [Request Tracker](#).
30. Classification based on [malware stealth](#) techniques. Described in [Introducing Stealth Malware Taxonomy](#)
31. [TLP - Traffic Light Protocol](#) The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.
32. Vocabulary for Event Recording and Incident Sharing [VERIS](#)

A taxonomy contains a series of tags that can be used as normal tags in your [MISP instance](#).

[Tagging](#) is a simple way to attach a classification to an event. In the early version of MISP, [tagging](#) was local to an instance. Classification must be globally used to be efficient. After evaluating different solutions of classification, we build a new scheme using the concept of machine tags.

Taxonomy is a classification of informations. Taxonomies are implemented in a simple JSON format. Anyone can create their own taxonomy or reuse an existing one.

Taxonomies are in an [independent git repository](#).

These can be **freely reused** and **integrated** in other threat intel tools.

The advantage is that you can set a specific tag as being exportable. This means that you can **export** your classification with other [MISP instance](#) and **share** the same taxonomies. [Tagging](#) is a simple way to attach a classification to an event.

#### Classification must be globally used to be efficient.

If you want to enable a specific taxonomy, you can click on the cross to enable it.

The screenshot shows the 'List Taxonomies' page with a single taxonomy entry for 'tip'. A modal dialog box is open, asking '192.168.56.50 indique : Are you sure you want to enable this taxonomy library?'. The 'OK' button is highlighted with a red circle and arrow. On the main table, the 'Enabled' column for the 'tip' taxonomy is set to 'Yes' (indicated by a red arrow), and the 'Actions' column contains a red circle with a minus sign, indicating a delete action.

List Taxonomies		Taxonomies										
		192.168.56.50 indique : Are you sure you want to enable this taxonomy library?										
		<input type="button" value="Annuler"/> <input type="button" value="OK"/>										
		<input type="button" value="« previous"/> <input type="button" value="next »"/>										
		<th>Id ↑</th> <th>Namespace</th> <th>Description</th> <th>Version</th> <th>Enabled</th> <th>Active Tags</th> <th>Actions</th>				Id ↑	Namespace	Description	Version	Enabled	Active Tags	Actions
		<table border="1"> <tr> <td>22</td> <td>tip</td> <td>The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.</td> <td>3</td> <td>Yes</td> <td>2 / 5 (enable all)</td> <td><input type="button" value="–"/></td> </tr> </table>				22	tip	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.	3	Yes	2 / 5 (enable all)	<input type="button" value="–"/>
22	tip	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.	3	Yes	2 / 5 (enable all)	<input type="button" value="–"/>						

Then you can even cherry-pick the tags you want to use on the system. If you want to use the whole taxonomy, select all and then click on the cross in the top left.

## Contributing to Taxonomy

It is quite easy. Create a JSON file describing your taxonomy as triple tags.

```
1 {
2   "namespace": "admiralty-scale",
3   "description": "The Admiralty Scale (also called the NATO
4                 System) is used to rank the reliability of a source and
5                 the credibility of an information.",
6   "version": 1,
7   "predicates": [
8     {
9       "value": "source-reliability",
10      "expanded": "Source Reliability"
11    },
12    {
13      "value": "information-credibility",
14      "expanded": "Information Credibility"
15    }
16  ],
17  ....
```

```
1 {
2   "values": [
3     {
4       "predicate": "source-reliability",
5       "entry": [
6         {
7           "value": "a",
8           "expanded": "Completely reliable"
9         },
10        ...
11      ]
12    }
13  ]
14}
```

(e.g. check an existing one like [Admiralty Scale](#)), create a directory matching your name space, put your machinetag file in the directory and [pull](#) your request. [Publishing](#) your taxonomy is as easy as a simple git [pull](#) request on misp-taxonomies (<https://github.com/MISP/misp-taxonomies>). That's it. Everyone can benefit from your taxonomy and can be automatically enabled in information sharing tools like [MISP](#).

## Reserved Taxonomy

The following taxonomy namespaces are reserved and used internally to MISP.

- [galaxy](#) mapping taxonomy with cluster:element:"value".

## Adding Taxonomy in MISP

How are taxonomies integrated in MISP?

MISP administrators have only to import (or even cherry pick) the namespace or predicates they want to use as tags.

Tags can be exported to other instances.

Tags are also accessible via the MISP REST [API](#).

For more information, "[Information Sharing and Taxonomies Practical Classification of Threat Indicators using MISP](#)" presentation given to the last MISP training in Luxembourg.

## Adding a private taxonomy

```
$ cd /var/www/MISP/app/files/taxonomies/
$ mkdir privatetaxonomy
$ cd privatetaxonomy
$ vi machinetag.json
```

Create a JSON file describing your taxonomy as triple tags.

```
For example :
mkdir sample
cd sample
vim machinetag.json
```

Sample JSON with triple tags. You can use the JSON validator to be sure that there is no syntax error.

```
{
  "namespace": "sample",
  "description": "Some descriptive words",
  "version": 1,
  "predicates": [
    {
      "value": "my-predicate",
      "expanded": "my-predicate"
    }
  ],
  "values": [
    {
      "predicate": "my-predicate",
      "entry": [
        {
          "value": "a-value",
          "expanded": "a-value"
        }
      ]
    }
  ]
}
```

```

        "expanded": "A value"
    }
}
]
}
}
```

Go to MISP Web GUI taxonomies/index and update the taxonomies once you are happy with your file. The newly created taxonomy should be visible. Now you need to activate the tags within your taxonomy.

## How to use Taxonomy in MISP

### Filtering the distribution of events among MISP instances

Applying rules for distribution based on tags:

### MISP Taxonomies - tools

- [machinetag.py](#) is a parsing tool to dump taxonomies expressed in Machine Tags (Triple Tags) and list all valid tags from a specific taxonomy.

```
% cd tools
% python machinetag.py
    admiralty-scale:source-reliability="a"
    admiralty-scale:source-reliability="b"
    admiralty-scale:source-reliability="c"
    admiralty-scale:source-reliability="d"
    admiralty-scale:source-reliability="e"
    admiralty-scale:source-reliability="f"
    admiralty-scale:information-credibility="1"
    admiralty-scale:information-credibility="2"
    admiralty-scale:information-credibility="3"
    admiralty-scale:information-credibility="4"
    admiralty-scale:information-credibility="5"
    admiralty-scale:information-credibility="6"
    ...
    ...
```

- [PyTaxonomies](#) - Python module to use the [MISP Taxonomies](#)

### Other use cases using MISP taxonomies

Tags can be used to:

- Set events for further processing by external tools (e.g. VirusTotal auto-expansion using Viper).
- Ensure a classification manager classes the events before release (e.g. release of information from air-gapped/classified networks).
- Enrich IDS export with tags to fit your [NIDS](#) deployment.

## Future functionalities related to MISP taxonomies

- Sighting support (thanks to NCSC-NL) is integrated in MISP allowing to auto expire [IOC](#) based on user detection.
- Adjusting taxonomies (adding/removing tags) based on their score or visibility via sighting.
- Simple taxonomy editors to help non-technical users to create their taxonomies.

- Filtering mechanisms in MISP to rename or replace taxonomies/tags at [pull](#) and [push synchronisation](#).
- More public taxonomies to be included

*Last modified: Tue Mar 10 2020 14:01:03 GMT+0100 (CET)*

- Galaxies
  - Managing Galaxies in MISP
  - Adding a custom Galaxy repository in MISP (WiP - notFunctional))
  - Adding a new Galaxy
    - Context
    - Directory structure
    - The galaxy management GUI
    - The galaxy file
    - The cluster file
    - Implementation
    - Troubleshooting
    - Example ~ Simple galaxy ~ Matrix-shaped galaxy
    - Dependencies
    - Create a fork
    - Understanding directory structure
    - Removing a Galaxy to better understand the add
  - Using Galaxies in MISP Events - Example
  - Available Galaxies
    - Clusters
    - Vocabularies ~ Common ~ threat-actor

## Galaxies

Galaxies in MISP are a method used to express a large object called cluster that can be attached to MISP events or attributes. A cluster can be composed of one or more elements. Elements are expressed as key-values.

There are default vocabularies available in MISP Galaxy but those can be overwritten, replaced or updated as you wish.

Vocabularies are from existing standards (like STIX, Veris, ATT&CK, MISP and so on) or custom ones you only use for your organization.

Existing clusters and vocabularies can be used as-is or as a template. MISP distribution can be applied to each cluster to permit a limited or broader distribution scheme.

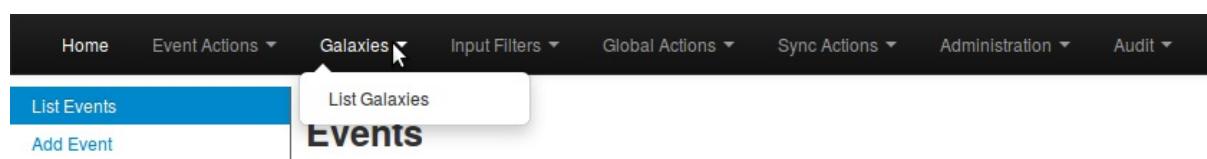
The objective is to have a common set of clusters for organizations starting analysis but that can be expanded to localized information (which is not shared) or additional information (that can be shared).

[MISP Galaxy](#) is available on Github.

## Managing Galaxies in MISP

[warning] You need to have a specific role to manage Galaxies on a [MISP instance](#).

Galaxies management is accessed using the Galaxies link on the top menu.



A list with all the galaxies existing on the server will appear.

## Galaxies

[« previous](#) [next »](#)

Id	Name	Version	Description	
23	Preventive Measure	1	Preventive measures based on the ransomware document overview as published in <a href="https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdljWdCEsGIM0Y0Hvmc5g/pubhtml#">https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdljWdCEsGIM0Y0Hvmc5g/pubhtml#</a> . The preventive measures are quite generic and can fit any standard Windows infrastructure and their security measures.	
22	Ransomware	1	<a href="https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdljWdCEsGIM0Y0Hvmc5g/pubhtml">Ransomware galaxy based on https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdljWdCEsGIM0Y0Hvmc5g/pubhtml</a>	
21	TDS	2	TDS is a list of Traffic Direction System used by adversaries	
20	Exploit-Kit	2	Exploit-Kit is an enumeration of some exploitation kits used by adversaries. The list includes document, browser and router exploit kits. It's not meant to be totally exhaustive but aim at covering the most seen in the past 5 years	
19	Tool	1	Threat actors tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries.	
18	Threat Actor	1	Threat actors are characteristics of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.	
17	Microsoft Activity Group actor	1	Activity groups as described by Microsoft	

Page 1 of 1, showing 7 records out of 7 total, starting on record 1, ending on 7

Each galaxy can be explored using the **View** icon at the end of the line.

## Tool galaxy

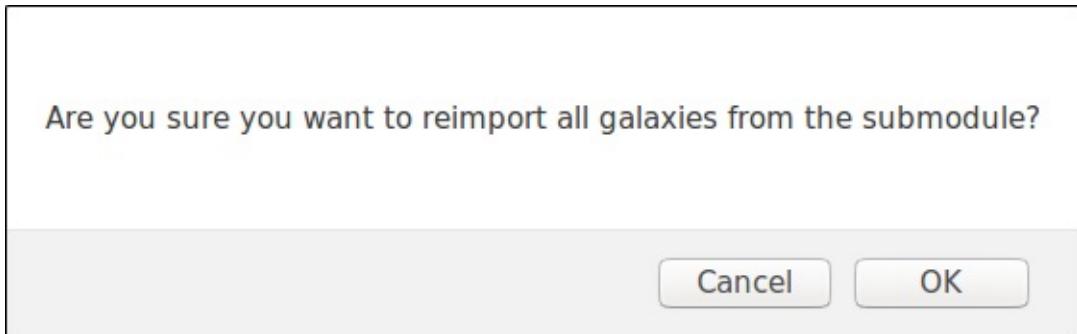
Galaxy ID	19
Name	Tool
Uuid	9b8037f7-bc8f-4de1-a797-37266619bc00
Description	Threat actors tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries.
Version	1

« previous 1 2 3 4 next »

Value ↓	Synonyms	Activity	#Events	Description	Actions
<b>EyePyramid Malware</b>		0	0	Two Italians referred to as the "Occhionero brothers" have been arrested and accused of using malware and a carefully-prepared spear-phishing scheme to spy on high-profile politicians and businessmen. This case has been called "EyePyramid", which we first discussed last week. (Conspiracy theories aside, the name came from a domain name and directory path that was found during the research.)	
<b>Adwind</b>	<b>AlienSpy</b> <b>Frutas</b> <b>Unrecom</b> <b>Sockrat</b> <b>JSocket</b> <b>JRat</b> <b>Backdoor:Java/Adwind</b>	1	1	Adwind is a backdoor written purely in Java that targets system supporting the Java runtime environment. Commands that can be used, among other things, to display messages on the system, open URLs, update the malware, download/execute files, and download/load plugins. A significant amount of additional functionality can be provided through downloadable plugins, including such things as remote control options and shell command execution.	

Here the metadata of the selected galaxy is shown. You also see a table with each available value as well as some complementary data such as a description of the value or the activity ([MISP Sightings](#)), that is to say the evolution of the use of each value.

Galaxies can be reimported from the submodules by clicking the "Update Galaxies" link on either the galaxies list or while browsing a specific galaxy. A popup will appear to confirm the reimportation.



All galaxies will always be updated, even while browsing a specific galaxy.

## Adding a custom Galaxy repository in MISP (WiP - notFunctional)

Fork the [misp-galaxy](#) repository to your github account.

Once you have forked the repo you can do the following, assuming you have followed the [Standard MISP Install](#).

```
cd /var/www/MISP/app/files/
sudo rm -rf misp-galaxy
# Replace the following line with your fork
sudo -u www-data git clone https://github.com/SteveClement/misp-galaxy.git
```

Once this is done double check if you can still see the Galaxies in the Web UI.

[warning] This will impact the UI "Update MISP" functionality in administration. Your git head might get [detached](#) in your misp-galaxy repo.

## Adding a new Galaxy

### Context

A Galaxy is designed to provide more info than a tag. It comes in two formats: regular or matrix-shape. In a tag, you can only display one label and one color. In a galaxy, you can display:

- name
- synonymous
- description
- categories (for matrix-galaxies)

### Directory structure

Galaxies are represented by two json files stored in:

```
/var/www/MISP/app/files/misp-galaxy/galaxies/mygalaxy.json
/var/www/MISP/app/files/misp-galaxy/clusters/mygalaxy.json
```

The `/galaxies` file contains metatdata and galaxy structure. The `/clusters` file contains actual data.

### The galaxy managment GUI

## Galaxies

[« previous](#) [next »](#)

4

<a href="#">Id</a>	<a href="#">Icon</a>	<a href="#">Name</a>	<a href="#">Version</a>	<a href="#">Namespace</a>	<a href="#">Description</a>	<a href="#">1</a>
406		Dark Patterns	1	misp	Social Engineering - Dark Patterns	
405		Surveillance Vendor	1	misp	List of vendors selling surveillance technologies including malware, interception devices or computer exploitation services	
404		Misinformation Pattern	4	misinfosec	AMITT Tactic	
403		Regions UN M49	2	misp	Regions based on UN M49.	
402		Target Information	1	misp	Description of targets of threat actors.	
401		o365-exchange-techniques	1	misp	o365-exchange-techniques - Office365/Exchange related techniques by @johnLaTwC	
400		attck4fraud	1	misp	attck4fraud - Principles of MITRE ATT&CK in the fraud domain	
399		Election guidelines	1	misp	Universal Development and Security Guidelines as Applicable to Election Technology.	
398		Malpedia	1	misp	Malware galaxy based on Malpedia archive.	
397		Backdoor	1	misp	Malware Backdoor galaxy.	
396		Stealer	1	misp	Malware stealer galaxy.	
395		Mobile Attack - Relationship	4	mitre-attack	Mitre Relationship	
394		Mobile Attack - Malware	5	deprecated	Name of ATT&CK software	

In this windows, you will be able to check all your galaxies and if your newly created ones are OK.

## The galaxy file

The galaxy file provides the framework for the data stored in the cluster file. For example:

```
{
  "description": "attck4fraud - Principles of MITRE ATT&CK in the fraud domain",
  "icon": "map",
  "kill_chain_order": [
    "fraud-tactics": [
      "Initiation",
      "Target Compromise",
      "Perform Fraud",
      "Obtain Fraudulent Assets",
      "Assets Transfer",
      "Monetisation"
    ]
  ],
  "name": "attck4fraud",
  "namespace": "misp",
  "type": "financial-fraud",
  "uuid": "cc0c8ae9-aec2-42c6-9939-f4f82b051836",
  "version": 1
}
```

19 lines (19 sloc) | 452 Bytes

```

1   {
2  1   "description": "attck4fraud - Principles of MITRE ATT&CK in the fraud domain",
3  2   "icon": "map",
4  8   "kill_chain_order": [
5     "fraud-tactics": [
6       "Initiation",
7       "Target Compromise",
8       "Perform Fraud",
9       "Obtain Fraudulent Assets",
10      "Assets Transfer",
11      "Monetisation"
12    ]
13  },
14 3   "name": "attck4fraud",
15 4   "namespace": "misp",
16 5   "type": "financial-fraud",
17 6   "uuid": "cc0c8ae9-aec2-42c6-9939-f4f82b051836",
18 7   "version": 1
19 }
```

- **description:** generalities about the galaxy (1)
- **icon:** the icon used in the MISP interface (2)
- **name:** the name of the galaxy (3)
- **namespace:** the namespace where is stored the galaxy. Namespace are used to regroup similar galaxies (4)
- **type:** **IMPORTANT field**, it MUST match the galaxy and cluster files name to actually chain both files together (5)
- **uuid:** as any MISP object, it has a uuid. **IMPORTANT**, it MUST be repeated in the uuid property of the cluster file (6)
- **version:** as usual in MISP, versioning, especially to force update (7)
- **kill\_chain\_order:** a special and optionnal field: it will be used if you want to create a matrix-galaxy. In this field, you insert a named table (*fraud-tactics* in the example above) containing the categories labels of your data. They will be used then in the cluster file (8)

More detail on galaxy fields here: <https://tools.ietf.org/html/draft-dulaunoy-misp-galaxy-format-06#page-9>

## The cluster file

The cluster file provides the actual data of the galaxy. For example (Attck4fraud):

```
{
  "authors": [
    "Francesco Bigarella"
  ],
  "category": "guidelines",
  "description": "attck4fraud - Principles of MITRE ATT&CK in the fraud domain",
  "name": "attck4fraud",
  "source": "Open Sources",
  "__type": "financial-fraud",
  "__uuid": "cc0c8ae9-aec2-42c6-9939-f4f82b051836",
  "values": [
    {
      "description": "In the context of ATT&CK for Fraud, phishing is described as the sending of fraudulent emails to a large audience in order to obtain sensitive information (PII, credentials, payment information). Phishing is never targeted to a specific individual or organisation. Phishing tries to create a sense of urgency or curiosity in order to capture the victim.",
      "meta": {
        "detection": "Email sender is spoofed; Email sender belongs to a domain recently created; Presence of typos or poor grammar in the email text; The request in the mail is unsolicited and creates urgency; No recollection of the subject or the sender of the phishing email; Request for credentials; Presence of a suspicious URL or attachment."
      },
      "examples": [
        "Phishing messages were sent to Amazon users posing as the Amazon customer support",
        "Fake Apple invoices were sent to Apple App Store customers in order to obtain their Apple ID credentials"
      ],
      "external_id": "FT1001",
      "kill_chain": [
        "fraud-tactics:Initiation"
      ],
      "mitigation": "Implementation of DKIM and SPF authentication to detect spoofed email senders; anti-phishing solutions.",
      "refs": [
        "https://blog.malwarebytes.com/cybercrime/2015/02/amazon-notice-ticket-number-phish-seeks-card-details/",
        "https://www.bleepingcomputer.com/news/security/widespread-apple-id-phishing-attack-pretends-to-be-app-store-receipts/"
      ],
      ...
    },
    {
      "version": 3
    }
}
```

384 lines (384 sloc) | 13.8 KB

Raw Blame History

```
1  {
2  1 "authors": [
3      "Francesco Bigarella"
4  ],
5  2 "category": "guidelines",
6  3 "description": "attck4fraud - Principles of MITRE ATT&CK in the fraud domain",
7  4 "name": "attck4fraud",
8  5 "source": "Open Sources",
9  6 "type": "financial-fraud",
10 7 "uuid": "cc0c8ae9-aec2-42c6-9939-f4f82b051836",
11 8 "values": [
12      {
13          "description": "In the context of ATT&CK for Fraud, phishing is described as the sending of fraudulent emails to a large audience",
14          "meta": {
15              9 "detection": "Email sender is spoofed; Email sender belongs to a domain recently created; Presence of typos or poor grammar is detected",
16              "examples": [
17                  "Phishing messages were sent to Amazon users posing as the Amazon customer support",
18                  "Fake Apple invoices were sent to Apple App Store customers in order to obtain their Apple ID credentials"
19              ],
20              "external_id": "FT1001",
21              10 "kill_chain": [
22                  "fraud-tactics:Initiation"
23              ],
24              "mitigation": "Implementation of DKIM and SPF authentication to detect spoofed email senders; anti-phishing solutions.",
25              "refs": [
26                  "https://blog.malwarebytes.com/cybercrime/2015/02/amazon-notice-ticket-number-phish-seeks-card-details/",
27                  "https://www.bleepingcomputer.com/news/security/widespread-apple-id-phishing-attack-pretends-to-be-app-store-receipts/"
28              ],
29          }
30      }
31  ]
```

- **authors:** descriptive field (1)
- **category:** descriptive field (2)
- **description:** descriptive field (3)
- **name:** same as in /galaxy file, used in the Matrix display (4)
- **source:** descriptive field (5)
- **type:** IMPORTANT, this field MUST match the /galaxy and /cluster files names AND the type field in the /galaxy file name -5 in above paragraph- (6)
- **uuid:** IMPORTANT, this field MUST match the /galaxy uuid field -6 in above paragraph- (7)
- **values:** a table containing the actual values (8)
- **data fields:** fields used to describe single data are detailed here: <https://tools.ietf.org/html/draft-dulaunoy-misp-galaxy-format-06#page-9> (9)
- **kill\_chain:** IMPORTANT, provide the column of the Matrix where the data will be displayed: (10)
  - **arg1:** MUST match /galaxy file's killchain arg (*\_fraud-tactics* in the example)
  - **arg2:** name of the column of the data (*Initiation* in the example)
- **version:** same as for galaxies

More details on /cluster fields can be found here: <https://tools.ietf.org/html/draft-dulaunoy-misp-galaxy-format-06#page-9>

## Implementation

- Once your files are ready, ALWAYS submit them in a json validator such as: <https://jsonformatter.curiousconcept.com/>. Do it before putting them into your instance, your sanity is at stake.
- Copy/paste your files in both folders (/galaxies and /clusters)
- Go to Galaxies/List galaxies and clic on Update galaxies
- Your new galaxy should be displayed on the screen with the others

The screenshot shows the MISP web interface. At the top, there is a navigation bar with links: Home, Event Actions, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Audit, MISP, Admin, and a mail icon. On the left, a sidebar menu includes 'Create Galaxies', 'Update Galaxies', 'Delete Galaxies', and 'New Galaxy'. The 'New Galaxy' option is highlighted with a blue background. The main content area displays a 'shadowrun galaxy' entry. The details are as follows:

Galaxy ID	41
Name	shadowrun
Namespace	RPG
Uuid	7a956b4d-613c-4c08-b5d6-19974682aea8
Description	My Shadowrun test galaxy
Version	1

Below the details, there are navigation buttons: '<< previous' and 'next >>'. Further down, a table lists galaxies with columns: Value, Synonyms, Activity, #Events, Description, and Actions. A 'Filter' input field is located above the table. The table shows one record:

Value	Synonyms	Activity	#Events	Description	Actions
shadowrun			0	My Shadowrun test galaxy	

At the bottom of the page, a message indicates 'Page 1 of 1, showing 0 records out of 0 total, starting on record 0, ending on 0' and navigation buttons: '<< previous' and 'next >>'.

- Your galaxy is available in the events for selecting in the right namespace

The screenshot shows a user interface for managing security events. At the top, there's a header titled "Galaxies". Below it, a search bar contains the text "shadowrun". A dropdown menu is open, showing several namespaces: "All namespaces", "deprecated", "misp", "mitre-attack", and "RPG". Underneath these, another dropdown shows "All clusters" and "shadowrun". A list of event details is displayed, including:  
A nation-scale corporation.  
only extraterritorial compagnies.

At the bottom of the interface, there are buttons for "Submit", "Comment", and "Correlate". A red warning message at the bottom states: "Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes / indic".

## Troubleshooting

- **The galaxy does not update, galaxy is empty**
  - Check json validation
  - Remove commas on last items of any {} or []
  - Update version of files
  - Check files names
  - Delete the galaxy in the GUI and update
- **Matrix is not displayed**
  - Check the kill\_chain\_order array in the /galaxies json
  - Check the chaining

## Example

We will create a galaxy from scratch. To demonstrate MISP can handle any type of use-case, we will not work on malware but on Shadowrun pen and paper RPG. In this RPG, 2060's large megacorporations launch paramilitary actions against each other. They can belong to 3 main categories (ranked by international standards):

- AAA: extraterritorial corporation and seating at the top-10 council;
- AA: only extraterritorial companies;
- A: nation-scale corporation.

A corporation can act in several fields:

- energy
- IT
- biotechnology
- cybertechnology (body enhancement)

It can work on several continents:

- Europe;
- Asia;
- Africa;
- Oceania;
- America.

All these context elements are enough to build a galaxy.

### Simple galaxy

- the galaxy file: galaxies/shadowrun.json

```
{
  "description": "My Shadowrun test galaxy",
  "icon": "user-secret",
  "name": "shadowrun",
  "namespace": "RPG",
  "type": "shadowrun",
  "uuid": "7a956b4d-613c-4c08-b5d6-19974682aea8",
  "version": 1
}
```

Keep the uuid and type, it will be necessary later.

- Check your json
- Click on update and see your work:

The screenshot shows the MISP web interface for managing Galaxies. At the top, there's a navigation bar with links for Home, Event Actions, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, and Audit. On the far right, there are links for MISp and Admin.

The main content area displays a Galaxy named "shadowrun galaxy". The details shown are:

Galaxy ID	41
Name	shadowrun
Namespace	RPG
Uuid	7a956b4d-613c-4c08-b5d6-19974682aea8
Description	My Shadowrun test galaxy
Version	1

Below the Galaxy details, there are navigation buttons: « previous and next ».

Further down, there's a table header with columns: Value, Synonyms, Activity, #Events, Description, and Actions. A "Filter" button is located above the table.

The table body contains one row of data:

Value	Synonyms	Activity	#Events	Description	Actions

Text below the table indicates: "Page 1 of 1, showing 0 records out of 0 total, starting on record 0, ending on 0".

At the bottom of the table, there are navigation buttons: « previous and next ».

- the cluster file: clusters/shadowrun.json

```
{
  "authors": [
    "myself"
  ],
  "category": "RPG",
  "description": "Shadowrun galaxy",
  "name": "shadowrun corporations",
  "source": "Internal",
  "type": "shadowrun",
  "uuid": "7a956b4d-613c-4c08-b5d6-19974682aea8",
  "values": [
    {
      "description": "extraterritorial corporation and seating at the top-10 council.",
      "meta": {
        "Corporate council seat": "Yes",
        "examples": [
          "Renraku",
          "Shiawase",
          "Aztechnology",
          "Ares Macrotechnologies",
          "Saeder Krupps"
        ]
      },
      "uuid": "43e1b900-5a03-11ea-9ad1-080027cbfd66",
      "value": "AAA"
    },
    {
      "description": "only extraterritorial compagnies.",
      "meta": {
        "Corporate council seat": "No",
        "examples": [
          "Shibata",
          "Monobe",
          "Zeta Impchem",
          "ESUS"
        ]
      },
      "uuid": "7aad2dd4-5a03-11ea-ad69-080027cbfd66",
      "value": "AA"
    },
    {
      "description": "nation-scale corporation.",
      "meta": {
        "Corporate council seat": "No",
        "examples": [
          "Genom",
          "KSAF",
          "SereTech",
          "Infocore",
          "MicroDek (ex-Microsoft)",
          "Tan Tien"
        ]
      },
      "uuid": "50c0d622-5c67-11ea-bd4b-080027bbff6",
      "value": "A"
    },
    {
      "description": "energy sector: exploitation, , refining, selling",
      "meta": {
        "examples": [
          "Saeder Krupps"
        ],
        "subsectors": [
          "petroleum",
          "gas"
        ]
      }
    }
  ]
}
```

```

        "electricity",
        "gas",
        "bio"
    ],
},
"uuid": "293e7e5c-51a8-411f-9b47-d52ed62d4b78",
"value": "energy"
},
{
"description": "cybertechnology sector: manufacturing, selling and implanting modifications.",
"meta": {
    "Delta clinic (for implanting)": [
        "Yes",
        "No"
    ],
    "examples": [
        "headware",
        "bodyware",
        "eyeware",
        "earware",
        "cyberlimbs"
    ]
},
"uuid": "7e962290-cba7-49ad-95c2-115575c8a9d2",
"value": "cybertechnology"
},
{
"description": "Biotechnology: bioware, genetics, etc",
"meta": {
    "examples": [
        "bioware",
        "genetics",
        "biodrones",
        "biocosmetics"
    ]
},
"uuid": "c899564c-bfe4-460f-a2ed-aae98e1355a3",
"value": "biotechnology"
},
{
"description": "IT: softwares, hardware, cybersec",
"meta": {
    "examples": [
        "software dev",
        "hardware manufacturing",
        "intrusion countermeasures"
    ]
},
"uuid": "16c49ba4-8a79-4f67-a98a-07cdc08f8a2d",
"value": "IT"
},
{
"description": "Europe",
"meta": {
    "examples": [
        "France",
        "Belgium",
        "Luxembourg",
        "Germany",
        "Italy"
    ]
},
"uuid": "8e745c22-9b14-4334-887a-0000eda58f75",
"value": "Europe"
},
{
"description": "Asia",
"meta": {
    "examples": [

```

```

        "China",
        "Japan",
        "Thailand"
    ],
},
"uuid": "95d4ff78-42f8-4fe8-bb63-af2c7e500ec8",
"value": "Asia"
},
{
"description": "Russia and former USSR",
"meta": {
    "examples": [
        "Russia",
        "kazakhstan"
    ],
    "uuid": "87a3ac08-6ffc-45eb-826e-e8e0af392563",
    "value": "Russia"
},
{
"description": "Africa",
"meta": {
    "examples": [
        "Nigeria",
        "Malia",
        "Algeria"
    ],
    "uuid": "aba705b7-fcb4-4bf4-81d4-b896314f53ed",
    "value": "Africa"
},
{
"description": "Oceania",
"meta": {
    "examples": [
        "Asutralia",
        "Polynesia"
    ],
    "uuid": "ae28830b-b90f-48d9-8b89-acda0864ff4e",
    "value": "Oceania"
},
{
"description": "America",
"meta": {
    "examples": [
        "UCAS",
        "CAS",
        "Pueblo Corporate Council",
        "AZtlan"
    ],
    "uuid": "d41c6222-4d10-43e9-9a8e-47d586eaf0e7",
    "value": "America"
}
],
"version": 3
}

```

**IMPORTANT:**

- the ""uuid": "7a956b4d-613c-4c08-b5d6-19974682aea8," is the same in both files
- the cluster filename is the same as the "type" field in the galaxy file
- CHECK YOUR JSON (<https://jsonformatter.curiousconcept.com/>) AND SAVE YOUR SANITY!

We check the thing by clicking on the update button in the galaxy GUI:

Home Event Actions Galaxies Input Filters Global Actions Sync Actions Administration Audit MISP Admin Log out

List Galaxies Update Galaxies Force Update Galaxies View Galaxy

## shadowrun galaxy

Galaxy ID	39
Name	shadowrun
Namespace	RPG
Uuid	7a956b4d-613c-4c08-b5d6-19974682aea8
Description	My Shadowrun test galaxy
Version	1

« previous next »

Value	Synonyms	Activity	#Events	Description	Actions
A			0	nation-scale corporation.	
AA			0	only extraterritorial compagnies.	
AAA			0	extraterritorial corporation and sealing at the top-10 council.	

Page 1 of 1, showing 3 records out of 3 total, starting on record 1, ending on 3

« previous next »

We can test our work on the MISP GUI:

The screenshot shows the MISP GUI with the 'Galaxies' tab selected. A modal dialog box is open, titled 'Galaxies'. Inside the dialog, there is a search bar with the placeholder 'All clusters' and a dropdown menu showing the result 'shadowrun'. Below the search bar, there is a list of items: 'A', 'AA', and 'AAA'. To the right of the list, there is descriptive text: 'nation-scale corporation.' and 'only extraterritorial compagnies.'. At the bottom right of the dialog is a blue 'Submit' button. The background of the main interface shows various namespaces like 'All namespaces', 'deprecated', 'misp', 'mitre-attack', and 'RPG'.

Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes / indic

- Pivots - Galaxy + Event graph + Correlation graph + ATT&CK matrix - Attributes - Discussion

✖ 3: corp

## Galaxies

shadowrun 

+ AA  

Add



Galaxies    Input Filters    Global Actions    Sync Actions    Administration    Audit    MISP

## shadowrun galaxy

<b>Galaxy ID</b>	62
<b>Name</b>	shadowrun
<b>Namespace</b>	RPG
<b>Uuid</b>	7a956b4d-613c-4c08-b5d6-19974682aea8
<b>Description</b>	My Shadowrun test galaxy
<b>Version</b>	2

« previous    next »

Value ↓	Synonyms	Activity	#Events	Description	Actions
A			0	nation-scale corporation.	
AA			0	only extraterritorial compagnies.	
AAA			0	extraterritorial corporation and seating at the top-10 council.	
Africa			0	Africa	
America			0	America	
Asia			0	Asia	
Europe			0	Europe	
IT			0	IT: softwares, hardware, cybersec	
Oceania			0	Oceania	
Russia			0	Russia and former USSR	
biotechnology			0	Biotechnology: bioware, genetics, etc	
cybertechnology			0	cybertechnology sector: manufacturing, selling and implanting modifications.	
energy			0	energy sector: exploitation, , refining, selling	

Page 1 of 1, showing 13 records out of 13 total, starting on record 1, ending on 13

« previous    next »

This is an initial install Powered by [MISP 2.4.120](#) Please configure and harden accordingly - 2020-03-02 10:55:00

Add a tag

All namespaces   deprecated   misp   mitre-attack   police   policetaxo   RPG

All clusters   shadowrun*!*

A nation-scale corporation.  
AA only extraterritorial compagnies.  
AAA  
Africa Africa  
America America  
Asia Asia  
Europe Europe  
IT IT: softwares, hardware, cybersec  
Oceania Oceania  
Russia Russia and former USSR

Submit

Context   Relate

alaxies   Comment

Event Thread Link Code

Remark: we created a simple galaxy. We will later see how to create a Matrix-shaped one.

### Matrix-shaped galaxy

To create a matrix-shaped galaxy, a new field is added:

- **kill\_chain** for the /galaxy json
- **kill\_chain\_order** for the /cluster json

In the galaxy json, categories are listed:

```
"kill_chain": [
    "killchain_name": [
        "category_1",
        "category_2",
        "category_3"
    ]
}
```

The final galaxy file:

```
{
    "description": "My Shadowrun test matrix galaxy",
    "icon": "user-secret",
    "kill_chain_order": {
        "shadowrun": [
            "ranking",
            "sector",
            "area"
        ]
    },
    "name": "shadowrun_matrix",
    "namespace": "RPG",
    "type": "shadowrun",
    "uuid": "1b013b10-5c6e-11ea-8881-0800275bbff6",
    "version": 1
}
```

In the cluster json, reference to the categories are done:

```
"values": [
    {
        "description": "",
        "meta": {
            "kill_chain": [
                "killchain_name:category_1"
            ],
        }
    }
]
```

The final cluster file:

```
{
    "authors": [
        "myself"
    ],
    "category": "RPG",
    "description": "Shadowrun matrix galaxy",
    "name": "shadowrun corporations",
    "source": "Internal",
    "type": "shadowrun",
    "uuid": "1b013b10-5c6e-11ea-8881-0800275bbff6",
    "values": [
        {
            "killchain_name": "category_1"
        }
    ]
}
```

```

"description": "extraterritorial corporation and seating at the top-10 council.",
"meta": {
"kill_chain": [
    "shadowrun:ranking"
],
"Corporate council seat": "Yes",
"examples": [
    "Renraku",
    "Shiawase",
    "Aztechnology",
    "Ares Macrotechnologies",
    "Saeder Krupps"
]
},
"uuid": "43e1b900-5a03-11ea-9ad1-080027cbfd66",
"value": "AAA"
},
{
"description": "only extraterritorial compagnies.",
"meta": {
"kill_chain": [
    "shadowrun:ranking"
],
"Corporate council seat": "No",
"examples": [
    "Shibata",
    "Monobe",
    "Zeta Impchem",
    "ESUS"
]
},
"uuid": "7aad2dd4-5a03-11ea-ad69-080027cbfd66",
"value": "AA"
},
{
"description": "nation-scale corporation.",
"meta": {
"kill_chain": [
    "shadowrun:ranking"
],
"Corporate council seat": "No",
"examples": [
    "Genom",
    "KSAF",
    "Seretech",
    "Infocore",
    "MicroDek (ex-Microsoft)",
    "Tan Tien"
]
},
"uuid": "50c0d622-5c67-11ea-bd4b-0800275bbff6",
"value": "A"
},
{
"description": "energy sector: exploitation, , refining, selling",
"meta": {
"kill_chain": [
    "shadowrun:sector"
],
"examples": [
    "Saeder Krupps"
],
"subsectors": [
    "petroleum",
    "electricity",
    "gas",
    "bio"
]
}
}

```

```

    "uuid": "293e7e5c-51a8-411f-9b47-d52ed62d4b78",
    "value": "energy"
},
{
  "description": "cybertechnology sector: manufacturing, selling and implanting modifications.",
  "meta": {
  },
  "kill_chain": [
    "shadowrun:sector"
  ],
  "Delta clinic (for implanting)": [
    "Yes",
    "No"
  ],
  "examples": [
    "headware",
    "bodyware",
    "eyeware",
    "earware",
    "cyberlimbs"
  ]
},
"uuid": "7e962290-cba7-49ad-95c2-115575c8a9d2",
"value": "cybertechnology"
},
{
  "description": "Biotechnology: bioware, genetics, etc",
  "meta": {
  },
  "kill_chain": [
    "shadowrun:sector"
  ],
  "examples": [
    "bioware",
    "genetics",
    "biodrones",
    "biocosmetics"
  ]
},
"uuid": "c899564c-bfe4-460f-a2ed-aae98e1355a3",
"value": "biotechnology"
},
{
  "description": "IT: softwares, hardware, cybersec",
  "meta": {
  },
  "kill_chain": [
    "shadowrun:sector"
  ],
  "examples": [
    "software dev",
    "hardware manufacturing",
    "intrusion countermeasures"
  ]
},
"uuid": "16c49ba4-8a79-4f67-a98a-07cdc08f8a2d",
"value": "IT"
},
{
  "description": "Europe",
  "meta": {
  },
  "kill_chain": [
    "shadowrun:area"
  ],
  "examples": [
    "France",
    "Belgium",
    "Luxembourg",
    "Germany",
    "Italy"
  ]
}
,
```

```

    "uuid": "8e745c22-9b14-4334-887a-0000eda58f75",
    "value": "Europe"
},
{
    "description": "Asia",
    "meta": {
        "kill_chain": [
            "shadowrun:area"
        ],
        "examples": [
            "China",
            "Japan",
            "Thailand"
        ]
    },
    "uuid": "95d4ff78-42f8-4fe8-bb63-af2c7e500ec8",
    "value": "Asia"
},
{
    "description": "Russia and former USSR",
    "meta": {
        "kill_chain": [
            "shadowrun:area"
        ],
        "examples": [
            "Russia",
            "Kazakhstan"
        ]
    },
    "uuid": "87a3ac08-6ffc-45eb-826e-e8e0af392563",
    "value": "Russia"
},
{
    "description": "Africa",
    "meta": {
        "kill_chain": [
            "shadowrun:area"
        ],
        "examples": [
            "Nigeria",
            "Malia",
            "Algeria"
        ]
    },
    "uuid": "aba705b7-fcb4-4bf4-81d4-b896314f53ed",
    "value": "Africa"
},
{
    "description": "Oceania",
    "meta": {
        "kill_chain": [
            "shadowrun:area"
        ],
        "examples": [
            "Australia",
            "Polynesia"
        ]
    },
    "uuid": "ae28830b-b90f-48d9-8b89-acda0864ff4e",
    "value": "Oceania"
},
{
    "description": "America",
    "meta": {
        "kill_chain": [
            "shadowrun:area"
        ],
        "examples": [
            "UCAS",
            "USA"
        ]
    }
}

```

```

    "CAS",
    "Pueblo Corporate Council",
    "Aztlan"
  ],
  "uuid": "d41c6222-4d10-43e9-9a8e-47d586eaf0e7",
  "value": "America"
}
],
"version": 4
}

```

The final result:

Ranking (3 items)	Sector (4 items)	Area (6 items)
A	IT	Africa
AA	biotechnology	America
AAA	cybertechnology	Asia
	energy	Europe
		Oceania
		Russia

Select Some Options

Cancel

Done! Eventually!

## Dependencies

To create your own Galaxies the following tools are needed to run the validation scripts.

- jsonschema (>v2.4)
- jq
- moreutils (sponge)

On a Debian flavoured distribution you can potentially do this:

```
sudo apt install jq moreutils python3-jsonschema
sudo wget -O /usr/local/bin/jsonschema https://gist.githubusercontent.com/SteveClement/e6ac60e153e9657913000216
fc77c6ef/raw/c273ace06ad338d609dd2c84a0a6e215a268ea11/jsonschema
sudo chmod +x /usr/local/bin/jsonschema # This will only work with jsonschema >2.4 (before no CLI interface was
available)
```

## Create a fork

To add your custom Galaxy it is preferable to [fork](#) the [misp-galaxy](#) repository. See above for details.

## Understanding directory structure

### Removing a Galaxy to better understand the add

Let's start with removing a single Galaxy.

```
cd /var/www/MISP/app/files/misp-galaxy
sudo -u www-data rm galaxies/android.json
sudo -u www-data rm clusters/android.json
sudo -u www-data /var/www/MISP/app/Console/cake Admin updateGalaxies force
```

After this you will have removed the android Galaxy Cluster.

## Using Galaxies in MISP Events - Example

For this example, we will try to add a cluster to an existing event. This cluster contains information about threat actor known as Sneaky Panda.

## Test Event

Event ID	790
Uuid	580b20cf-2d28-4b1c-bbc4-404a950d210f
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	[REDACTED]
Tags	<b>admiralty-scale:information-credibility="1"</b> <span>x</span> <span>+</span>
Date	2016-10-22
Threat Level	High
Analysis	Initial
Distribution	<b>Your organisation only</b>
Info	Test Event
Published	No
Sightings	1 (1)

[- Pivots](#) [- Galaxy](#) [- Attributes](#) [- Discussion](#)

[✖ 790: Test E...](#)

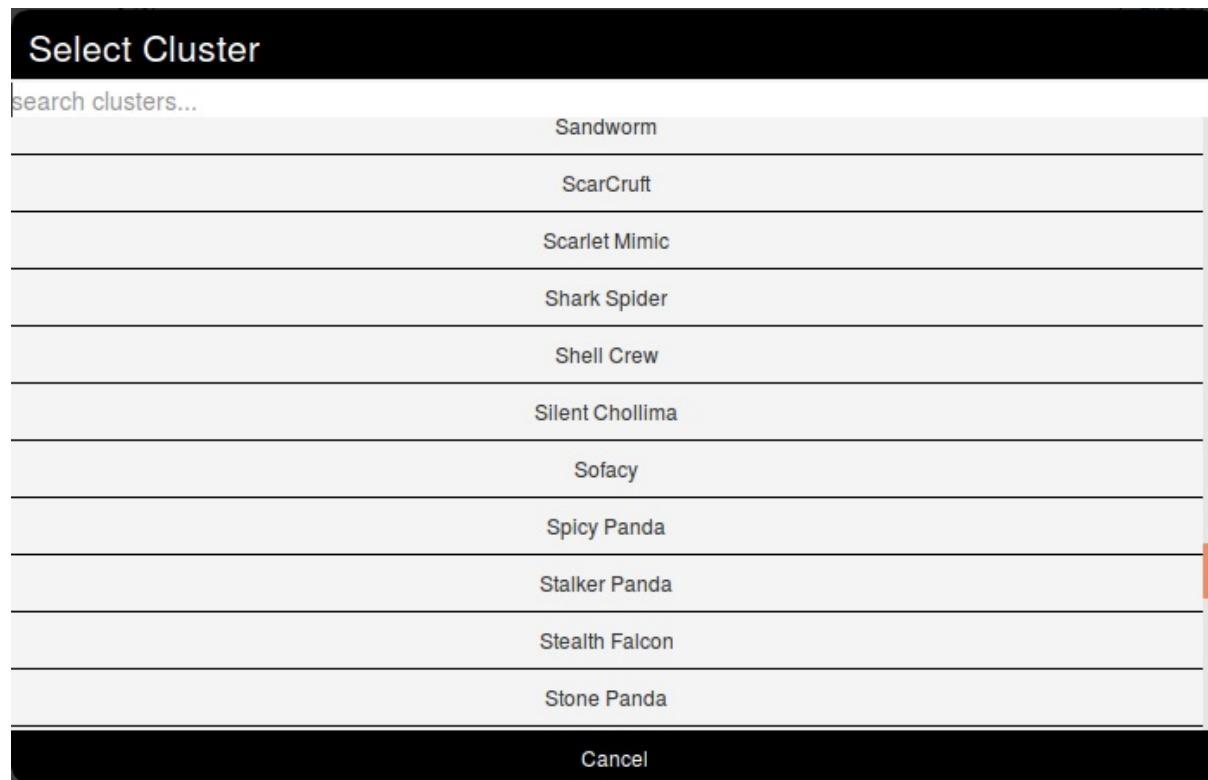
### Galaxies

[Add new cluster](#)

Here on the event view, we notice a blue frame under the metadatas with the title "Galaxies" and a button "Add new cluster". Let's click on the latter to begin.



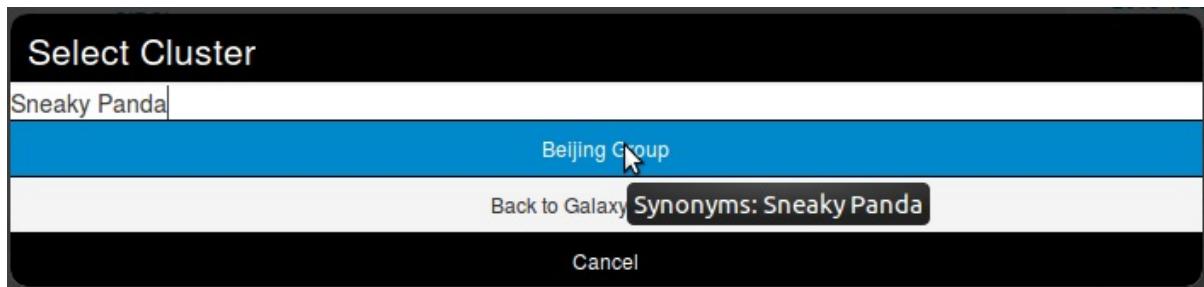
A popup will appear proposing to explore a particular galaxy or all at the same time. Here, as we know we want to as a threat actor, we will choose the second option and scroll to find Sneaky Panda (We are courageous, aren't we?).



Wait. No Sneaky Panda? Hm that's strange. Or maybe it is only registered as a alias. Let's have a look! To do so we will use the search field which stay on top of the list. So what do we get? Beijing Group, is it an alias of our threat actor.



Pointing the cursor on it will give us the answer.



We have a match. So we select it and here we go.

The screenshot shows a user interface titled "Galaxies". At the top left, there is a search bar with the placeholder text "Search Threat Actors". Below the search bar, there are two search results displayed in a grid format:

- Threat Actor** (with a magnifying glass icon)
- + Beijing Group** (with a magnifying glass icon) (with a list icon) (with a trash bin icon)

At the bottom left of the interface, there is a button labeled "Add new cluster".

Clicking on the magnifying glass next to Threat actor redirects to the list of all threat actors Clicking on the magnifying glass next to Beijing Group redirects us to a page about this group Clicking on the addition symbol on the left of Beijing Group extends the module.

## Available Galaxies

### Clusters

[Android](#) - Android malware galaxy based on multiple open sources.

[Backdoor](#) - A list of backdoor malware.

[Banker](#) - A list of banker malware.

[Botnet](#) - botnet galaxy

[Branded vulnerability](#) - List of known vulnerabilities and attacks with a branding

[Cert eu govsector](#) - Cert EU GovSector

[Exploit kit](#) - Exploit-Kit is an enumeration of some exploitation kits used by adversaries. The list includes document, browser and router exploit kits. It's not meant to be totally exhaustive but aim at covering the most seen in the past 5 years

[Malpedia](#) - Malware galaxy cluster based on Malpedia.

[Microsoft activity group](#) - Activity groups as described by Microsoft

[Mitre attack pattern](#) - ATT&CK tactic

[Mitre course of action](#) - ATT&CK Mitigation

[Mitre enterprise attack attack pattern](#) - ATT&CK tactic

[Mitre enterprise attack course of action](#) - ATT&CK Mitigation

[Mitre enterprise attack intrusion set](#) - Name of ATT&CK Group

[Mitre enterprise attack malware](#) - Name of ATT&CK software

[Mitre enterprise attack tool](#) - Name of ATT&CK software

[Mitre intrusion set](#) - Name of ATT&CK Group

[Mitre malware](#) - Name of ATT&CK software

[Mitre mobile attack attack pattern](#) - ATT&CK tactic

[Mitre mobile attack course of action](#) - ATT&CK Mitigation

[Mitre mobile attack intrusion set](#) - Name of ATT&CK Group

[Mitre mobile attack malware](#) - Name of ATT&CK software

[Mitre mobile attack tool](#) - Name of ATT&CK software

[Mitre pre attack attack pattern](#) - ATT&CK tactic

[Mitre pre attack intrusion set](#) - Name of ATT&CK Group

[Mitre tool](#) - Name of ATT&CK software

**Preventive measure** - Preventive measures based on the ransomware document overview as published in <https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdiJWdCEsGIM0Y0Hvmc5g/pubhtml#>. The preventive measures are quite generic and can fit any standard Windows infrastructure and their security measures.

**Ransomware** - Ransomware galaxy based on <https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdiJWdCEsGIM0Y0Hvmc5g/pubhtml> and <http://pastebin.com/raw/GHgpWjar>

**Rat** - remote administration tool or remote access tool (RAT), also called sometimes remote access trojan, is a piece of software or programming that allows a remote "operator" to control a system as if they have physical access to that system.

**Sector** - Activity sectors

**Stealer** - A list of malware stealer.

**Tds** - TDS is a list of Traffic Direction System used by adversaries

**Threat actor** - Known or estimated adversary groups targeting organizations and employees. Adversary groups are regularly confused with their initial operation or campaign.

**Tool** - threat-actor-tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries.

## Vocabularies

### Common

**Certainty level** - Certainty level of an associated element or cluster.

**Sector** - List of activity sectors

**Threat actor type** - threat actor type vocab as defined by Cert EU.

**Ttp category** - ttp category vocab as defined by Cert EU.

**Ttp type** - ttp type vocab as defined by Cert EU.

### threat-actor

**Cert eu motive** - Motive vocab as defined by Cert EU.

**Intended effect** - The IntendedEffectVocab is the default STIX vocabulary for expressing the intended effect of a threat actor

**Motivation** - The MotivationVocab is the default STIX vocabulary for expressing the motivation of a threat actor.

**Planning and operational support** - The PlanningAndOperationalSupportVocab is the default STIX vocabulary for expressing the planning and operational support functions available to a threat actor.

**Sophistication** - The ThreatActorSophisticationVocab enumeration is used to define the default STIX vocabulary for expressing the subjective level of sophistication of a threat actor.

**Type** - The ThreatActorTypeVocab enumeration is used to define the default STIX vocabulary for expressing the subjective type of a threat actor.

Last modified: Tue Jul 31 2018 10:23:22 GMT+0200 (CEST)

- [Sightings](#)
  - [Explanation](#)
  - [Using sightings on an event \(GUI\)](#)
    - [Advanced sightings](#)
    - [At Event level](#)
  - [Using sightings on an event \(API\)](#)

## Sightings

Basically, sighting is a system allowing people to react on attributes on an event. It was originally designed to provide an easy method for user to tell when they see a given attribute, giving it more credibility.

Now sightings have been improved to also provide a method to signal false positives, but also to give an expiration date for some attributes.

### Explanation

As said before, Sighting is a way for a user to say that they have seen or notice an attribute and confirm its validity. An attribute can be spotted several times by the same user, that is why a single user can use sighting several times on a single attribute.

Sometimes, some attributes can be considered as false positives, even if the false positive list do not detect them (for instance, if the IDS flag is set to false) so they can also be notified. As well as concerning sighting, the same user can signal a single attribute as a false positive several times.

It also happens that some attributes are only valid a certain time (for instance, in case of a phishing campaign that is assumed to be up for only one week). In this case, people can also assign an expiration date to an attribute, but this time, there can be only one valid expiration date per *organisation*.

### Using sightings on an event (GUI)

Sighting is applied to every attribute, under the column "Sightings", easily identifiable with its colored number. This column shows three icons and three values.

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events	IDS	Distribution	Sightings	Activity	Actions
2017-04-03	Network activity	ip-src	123.56.76.7		+		<input checked="" type="checkbox"/>		No	Inherit	   (0 0 0)		*     *  

These three values show respectively:

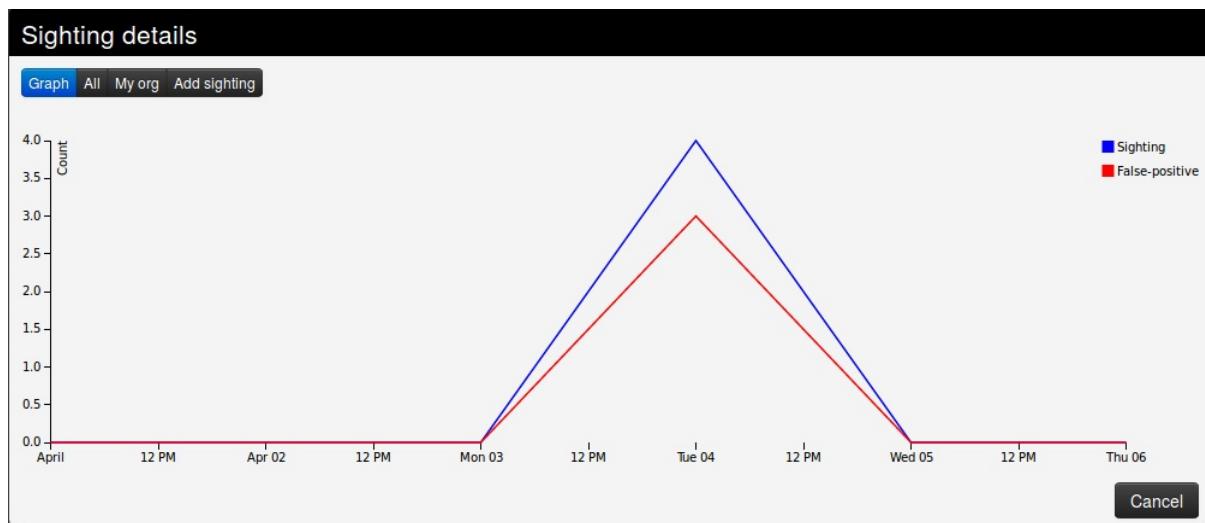
- The number of true positives detected with the attribute, in green. Malicious activity as described in the event.
- The number of times the attribute has been marked as false positive, in red. Non-malicious activity or incorrect detection.
- The number of different expiration dates that have been affected on this attribute, in orange

Concerning the three icons:

- The first one (Thumb up) allows to add a sighting (true positive) on an attribute.
- The second one (Thumb down) allows to mark the attribute as a false positive.
- The third one (Tool) opens a popup for advanced sightings, showing sightings details and allowing different actions.

## Advanced sightings

- The first tab, "Graph", represents a line graph showing the evolution of sightings and false positives over time.



- The second tab gives a quick view of all the sightings applied to the attribute.

Sighting details						
Date	Organisation	Type	Source	Event ID	Attribute ID	Actions
2017-04-22 08:14:03	Setec Astronomy	Expiration		1120	303398	
2017-04-07 08:09:28		Expiration		1120	303398	
2017-04-04 08:43:25		Sighting		1120	303398	
2017-04-04 08:10:47	Setec Astronomy	False-positive		1120	303398	
2017-04-04 08:10:46	Setec Astronomy	False-positive		1120	303398	
2017-04-04 08:10:45	Setec Astronomy	Sighting		1120	303398	
2017-04-04 08:10:31	Setec Astronomy	Sighting		1120	303398	
2017-04-04 07:50:00		False-positive		1120	303398	
2017-04-04 07:49:58		Sighting		1120	303398	

Cancel

- The third tab gives a quick view of the sightings applied to the attribute by your own organisation only.

Sighting details						
Date	Organisation	Type	Source	Event ID	Attribute ID	Actions
2017-04-07 08:09:28		Expiration		1120	303398	
2017-04-04 08:43:25		Sighting		1120	303398	
2017-04-04 07:50:00		False-positive		1120	303398	
2017-04-04 07:49:58		Sighting		1120	303398	

[Cancel](#)

- The last tab can be used to add either a sighting, mark the attribute as a false positive, or define an expiration date. You can precise both the date and time of day, as well as note a particular source where the sighting comes from.

Sighting details

Graph All My org Add sighting

Add Sighting

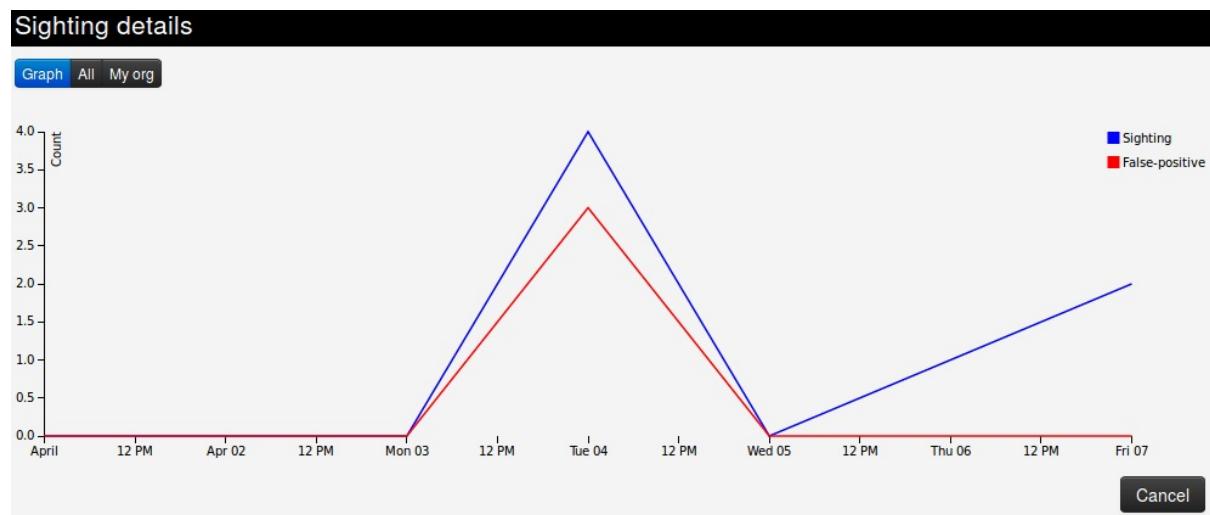
Type	Source	Sighting Date	
Sighting	honeypot, IDS sensor id, SIEM,...	2017-04-06 10:09:07	Add
Sighting			Cancel
False-positive			
Expiration			

## At Event level

The total number of sightings is also visible as part of the metadata in front of the Sightings label, as well as a sparkline graph that summarize the evolution of sightings.



Clicking on the tool will show sighting details for the whole event.



## Using sightings on an event (API)

Please have a look at the [automation API](#)

Last modified: Thu Sep 13 2018 15:22:36 GMT+0200 (CEST)

## MISP warninglists

MISP warninglists are lists of well-known [indicators](#) that can be associated to potential false positives, errors or mistakes. There is a Python module available to work with warninglists in a Pythonic way called [PyMISPWarningLists](#). [MISP warninglists GitHub Repo](#)

### MISP warning lists: The dilemma of false-positive

- False-positive is a common issue in threat intelligence sharing.
- It's often a contextual issue:
  - false-positive might be different per community of users sharing information.
  - organization might have their own view on false-positive.
- Based on the success of the MISP taxonomy model, we build misp-warninglists. They are lists of well-known [indicators](#) that can be associated to potential false positives, errors or mistakes. They are Simple JSON files.



The warning lists are integrated in MISP to display an info/warning box at the event and attribute level. This can be enabled at [MISP instance](#) level. Default warning lists can be enabled or disabled like known public resolver, multicast IP addresses, hashes for empty values, rfc1918, TLDs or known google domains. The warning lists can be expanded or added in JSON locally or via pull requests (<https://github.com/MISP/misp-warninglists>). Warning lists can be also used for critical or core infrastructure warning, personally identifiable information...

 *Last modified: Thu May 24 2018 10:37:13 GMT+0200 (CEST)*

## MISP noticelist

Notice lists to inform MISP users of the legal, privacy, policy or even technical implications of using specific attributes, categories or objects. [MISP noticelist GitHub Repo](#)

Last modified: Fri Sep 04 2020 15:59:49 GMT+0200 (CEST)

- Attribute Categories vs. Types
- Categories
- Types

## Attribute Categories vs. Types

Category	Antivirus detection	Artifacts dropped	Attribution	External analysis	Financial fraud	Internal reference
AS				X		
aba rtn					X	
anonymised	X	X	X	X	X	X
attachment	X	X		X		
authentihash		X				
bank-account-nr					X	
bic					X	
bin					X	
boolean						
bro				X		
btc					X	
campaign-id				X		
campaign-name				X		
cc-number					X	
cdhash		X				
chrome-extension-id						
comment	X	X	X	X	X	X
community-id					X	
cookie		X				
cortex					X	
counter						
country-of-residence						
cpe						
dash					X	
date-of-birth						
datetime						
dns-soa-email				X		
domain					X	
domain ip					X	

email			X			
email-attachment						
email-body						
email-dst						
email-dst-display-name						
email-header						
email-message-id						
email-mime-boundary						
email-reply-to						
email-src						
email-src-display-name						
email-subject						
email-thread-index						
email-x-mailer						
eppn						
filename		X		X		
filename authentihash		X				
filename impfuzzy		X				
filename imphash		X				
filename md5		X		X		
filename pehash		X				
filename sha1		X		X		
filename sha224		X				
filename sha256		X		X		
filename sha3-224		X		X		
filename sha3-256		X		X		
filename sha3-384		X		X		
filename sha3-512		X		X		
filename sha384		X				
filename sha512		X				
filename sha512/224		X				
filename sha512/256		X				
filename ssdeep		X				
filename tlsh		X				
filename vhash		X				
first-name						

float						
frequent-flyer-number						
gender						
gene		X				
git-commit-id						X
github-organisation						
github-repository				X		
github-username						
hassh-md5				X		
hasshserver-md5				X		
hex	X	X			X	X
hostname				X		
hostname port						
http-method						
iban					X	
identity-card-number						
impfuzzy		X				
imphash		X				
ip-dst				X		
ip-dst port				X		
ip-src				X		
ip-src port				X		
issue-date-of-the-visa						
ja3-fingerprint-md5				X		
jabber-id						
kusto-query		X				
last-name						
link	X			X		X
mac-address				X		
mac-eui-64				X		
malware-sample		X		X		
malware-type						
md5		X		X		
middle-name						
mime-type		X				
mobile-application-id						

mutex		X				
named pipe		X				
nationality						
other	X	X	X	X	X	X
passenger-name-record-locator-number						
passport-country						
passport-expiration						
passport-number						
pattern-in-file		X		X		
pattern-in-memory		X		X		
pattern-in-traffic				X		
payment-details						
pdb		X				
pehash						
pgp-private-key		X				
pgp-public-key		X				
phone-number						X
place-of-birth						
place-port-of-clearance						
place-port-of-onward-foreign-destination						
place-port-of-original-embarkation						
port						
primary-residence						
prtn					X	
redress-number						
regkey		X		X		
regkey value		X		X		
sha1		X		X		
sha224		X				
sha256		X		X		
sha3-224		X		X		
sha3-256		X		X		
sha3-384		X		X		
sha3-512		X		X		

sha384		X				
sha512		X				
sha512/224		X				
sha512/256		X				
sigma		X				
size-in-bytes						
snort				X		
special-service-request						
ssdeep		X				
stix2-pattern		X				
target-email						
target-external						
target-location						
target-machine						
target-org						
target-user						
text	X	X	X	X	X	X
threat-actor			X			
tlsh						
travel-details						
twitter-id						
uri						
url				X		
user-agent					X	
vhash		X				
visa-number						
vulnerability				X		
weakness					X	
whois-creation-date			X			
whois-registrant-email			X			
whois-registrant-name			X			
whois-registrant-org			X			
whois-registrant-phone			X			
whois-registrar			X			
windows-scheduled-task		X				
windows-service-		--				

windows-service-displayname		X					
windows-service-name		X					
x509-fingerprint-md5		X	X	X			
x509-fingerprint-sha1		X	X	X			
x509-fingerprint-sha256		X	X	X			
xmr						X	
yara		X					
zeek					X		

Category	Network activity	Other	Payload delivery	Payload installation	Payload type	Persistence mechanism
AS	X		X			
aba rtn						
anonymised	X	X	X	X	X	X
attachment	X		X	X		
authentihash			X	X		
bank-account-nr						
bic						
bin						
boolean		X				
bro	X					
btc						
campaign-id						
campaign-name						
cc-number						
cdhash			X	X		
chrome-extension-id			X	X		
comment	X	X	X	X	X	X
community-id	X					
cookie	X					
cortex						
counter		X				
country-of-residence						
cpe		X				
dash						
date-of-birth						
datatype		v				

category		A			
dns-soa-email					
domain	X		X		
domain ip	X				
email	X		X		
email-attachment			X		
email-body			X		
email-dst	X		X		
email-dst-display-name			X		
email-header			X		
email-message-id			X		
email-mime-boundary			X		
email-reply-to			X		
email-src	X		X		
email-src-display-name			X		
email-subject	X		X		
email-thread-index			X		
email-x-mailer			X		
eppn	X				
filename			X	X	X
filename authentihash			X	X	
filename impfuzzy			X	X	
filename imphash			X	X	
filename md5			X	X	
filename pehash			X	X	
filename sha1			X	X	
filename sha224			X	X	
filename sha256			X	X	
filename sha3-224			X	X	
filename sha3-256			X	X	
filename sha3-384			X	X	
filename sha3-512			X	X	
filename sha384			X	X	
filename sha512			X	X	
filename sha512/224			X	X	
filename sha512/256			X	X	

filename ssdeep		X	X			
filename tlsh		X	X			
filename vhash		X	X			
first-name						
float	X					
frequent-flyer-number						
gender						
gene						
git-commit-id						
github-organisation						
github-repository						
github-username						
hassh-md5	X		X			
hasshserver-md5	X		X			
hex	X	X	X	X		X
hostname	X		X			
hostname port	X		X			
http-method	X					
iban						
identity-card-number						
impfuzzy			X	X		
imphash			X	X		
ip-dst	X		X			
ip-dst port	X		X			
ip-src	X		X			
ip-src port	X		X			
issue-date-of-the-visa						
ja3-fingerprint-md5	X		X			
jabber-id						
kusto-query						
last-name						
link			X			
mac-address	X		X			
mac-eui-64	X		X			
malware-sample			X	X		
malware-type			X	X		
--	--	--	--	--	--	--

md5			X	X		
middle-name						
mime-type			X	X		
mobile-application-id			X	X		
mutex						
named pipe						
nationality						
other	X	X	X	X	X	X
passenger-name-record-locator-number						
passport-country						
passport-expiration						
passport-number						
pattern-in-file	X		X	X		
pattern-in-memory				X		
pattern-in-traffic	X		X	X		
payment-details						
pdb						
pehash			X	X		
pgp-private-key		X				
pgp-public-key		X				
phone-number		X				
place-of-birth						
place-port-of-clearance						
place-port-of-onward-foreign-destination						
place-port-of-original-embarkation						
port	X	X				
primary-residence						
prtn						
redress-number						
regkey						X
regkey value						X
sha1			X	X		
sha224			X	X		
sha256			X	X		
sha3-224			X	X		

sha3-256			X	X			
sha3-384			X	X			
sha3-512			X	X			
sha384			X	X			
sha512			X	X			
sha512/224			X	X			
sha512/256			X	X			
sigma			X	X			
size-in-bytes		X					
snort	X						
special-service-request							
ssdeep			X	X			
stix2-pattern	X		X	X			
target-email							
target-external							
target-location							
target-machine							
target-org							
target-user							
text	X	X	X	X	X	X	X
threat-actor							
tlsh			X	X			
travel-details							
twitter-id							
uri	X						
url	X		X				
user-agent	X		X				
vhash			X	X			
visa-number							
vulnerability			X	X			
weakness			X	X			
whois-creation-date							
whois-registrant-email			X				
whois-registrant-name							
whois-registrant-org							
whois-registrant-phone							

whois-registrar					
windows-scheduled-task					
windows-service-displayname					
windows-service-name					
x509-fingerprint-md5	X		X	X	
x509-fingerprint-sha1	X		X	X	
x509-fingerprint-sha256	X		X	X	
xmr					
yara			X	X	
zeek	X				

Category	Person	Social network	Support Tool	Targeting data
AS				
aba rtn				
anonymised	X	X	X	X
attachment			X	
authentihash				
bank-account-nr				
bic				
bin				
boolean				
bro				
btc				
campaign-id				
campaign-name				
cc-number				
cdhash				
chrome-extension-id				
comment	X	X	X	X
community-id				
cookie				
cortex				
counter				
country-of-residence	X			
cpe				
dash				

date-of-birth		X		
datetime				
dns-soa-email				
domain				
domain ip				
email	X	X		
email-attachment				
email-body				
email-dst		X		
email-dst-display-name				
email-header				
email-message-id				
email-mime-boundary				
email-reply-to				
email-src		X		
email-src-display-name				
email-subject				
email-thread-index				
email-x-mailer				
epn		X		
filename				
filename authentihash				
filename impfuzzy				
filename imphash				
filename md5				
filename pehash				
filename sha1				
filename sha224				
filename sha256				
filename sha3-224				
filename sha3-256				
filename sha3-384				
filename sha3-512				
filename sha384				
filename sha512				

filename sha512/224				
filename sha512/256				
filename ssdeep				
filename tlsh				
filename vhash				
first-name	X			
float				
frequent-flyer-number	X			
gender	X			
gene				
git-commit-id				
github-organisation		X		
github-repository		X		
github-username		X		
hassh-md5				
hasshserver-md5				
hex			X	
hostname				
hostname port				
http-method				
iban				
identity-card-number	X			
impfuzzy				
imphash				
ip-dst				
ip-dst port				
ip-src				
ip-src port				
issue-date-of-the-visa	X			
ja3-fingerprint-md5				
jabber-id		X		
kusto-query				
last-name	X			
link			X	
mac-address				
mac-eui-64				

malware-sample				
malware-type				
md5				
middle-name	X			
mime-type				
mobile-application-id				
mutex				
named pipe				
nationality	X			
other	X	X	X	
passenger-name-record-locator-number	X			
passport-country	X			
passport-expiration	X			
passport-number	X			
pattern-in-file				
pattern-in-memory				
pattern-in-traffic				
payment-details	X			
pdb				
pehash				
pgp-private-key	X	X		
pgp-public-key	X	X		
phone-number	X			
place-of-birth	X			
place-port-of-clearance	X			
place-port-of-onward-foreign-destination	X			
place-port-of-original-embarkation	X			
port				
primary-residence	X			
prtn				
redress-number	X			
regkey				
regkey value				
sha1				
sha224				

sha256				
sha3-224				
sha3-256				
sha3-384				
sha3-512				
sha384				
sha512				
sha512/224				
sha512/256				
sigma				
size-in-bytes				
snort				
special-service-request	X			
ssdeep				
stix2-pattern				
target-email				X
target-external				X
target-location				X
target-machine				X
target-org				X
target-user				X
text	X	X	X	
threat-actor				
tlsh				
travel-details	X			
twitter-id		X		
uri				
url				
user-agent				
vhash				
visa-number	X			
vulnerability				
weakness				
whois-creation-date				
whois-registrant-email		X		

whois-registrant-name				
whois-registrant-org				
whois-registrant-phone				
whois-registrar				
windows-scheduled-task				
windows-service-displayname				
windows-service-name				
x509-fingerprint-md5				
x509-fingerprint-sha1				
x509-fingerprint-sha256				
xmr				
yara				
zeek				

## Categories

- **Antivirus detection:** All the info about how the malware is detected by the antivirus products
- **Artifacts dropped:** Any artifact (files, registry keys etc.) dropped by the malware or other modifications to the system
- **Attribution:** Identification of the group, organisation, or country behind the attack
- **External analysis:** Any other result from additional analysis of the malware like tools output
- **Financial fraud:** Financial Fraud [indicators](#)
- **Internal reference:** Reference used by the [publishing](#) party (e.g. ticket number)
- **Network activity:** Information about network traffic generated by the malware
- **Other:** Attributes that are not part of any other category or are meant to be used as a component in [MISP objects](#) in the future
- **Payload delivery:** Information about how the malware is delivered
- **Payload installation:** Info on where the malware gets installed in the system
- **Payload type:** Information about the final payload(s)
- **Persistence mechanism:** Mechanisms used by the malware to start at boot
- **Person:** A human being - natural person
- **Social network:** Social networks and platforms
- **Support Tool:** Tools supporting analysis or detection of the event
- **Targeting data:** Internal Attack Targeting and Compromise Information

## Types

- **AS:** Autonomous system
- **aba-rtn:** ABA routing transit number
- **anonymised:** Anonymised value - described with the anonymisation object via a relationship
- **attachment:** Attachment with external information
- **authentihash:** Authenticode executable signature hash
- **bank-account-nr:** Bank account number without any routing number
- **bic:** Bank Identifier Code Number also known as SWIFT-BIC, SWIFT code or ISO 9362 code
- **bin:** Bank Identification Number
- **boolean:** Boolean value - to be used in objects
- **bro:** An [NIDS](#) rule in the Bro rule-format

- **btc:** Bitcoin Address
- **campaign-id:** Associated campaign ID
- **campaign-name:** Associated campaign name
- **cc-number:** Credit-Card Number
- **cdhash:** An Apple Code Directory Hash, identifying a code-signed Mach-O executable file
- **chrome-extension-id:** Chrome extension id
- **comment:** Comment or description in a human language
- **community-id:** a community ID flow hashing algorithm to map multiple traffic monitors into common flow id
- **cookie:** HTTP cookie as often stored on the user web client. This can include authentication cookie or session cookie.
- **cortex:** Cortex analysis result
- **counter:** An integer counter, generally to be used in objects
- **country-of-residence:** The country of residence of a natural person
- **cpe:** Common platform enumeration
- **dash:** Dash Address
- **date-of-birth:** Date of birth of a natural person (in YYYY-MM-DD format)
- **datetime:** Datetime in the ISO 8601 format
- **dns-soa-email:** RFC1035 mandates that DNS zones should have a SOA (Statement Of Authority) record that contains an email address where a PoC for the domain could be contacted. This can sometimes be used for attribution/linkage between different domains even if protected by whois privacy
- **domain:** A domain name used in the malware
- **domain|ip:** A domain name and its IP address (as found in DNS lookup) separated by a |
- **email:** An e-mail address
- **email-attachment:** File name of the email attachment.
- **email-body:** Email body
- **email-dst:** The destination email address. Used to describe the recipient when describing an e-mail.
- **email-dst-display-name:** Email destination display name
- **email-header:** Email header
- **email-message-id:** The email message ID
- **email-mime-boundary:** The email mime boundary separating parts in a multipart email
- **email-reply-to:** Email reply to header
- **email-src:** The source email address. Used to describe the sender when describing an e-mail.
- **email-src-display-name:** Email source display name
- **email-subject:** The subject of the email
- **email-thread-index:** The email thread index header
- **email-x-mailer:** Email x-mailer header
- **eppn:** eduPersonPrincipalName - eppn - the NetId of the person for the purposes of inter-institutional authentication. Should be stored in the form of user@univ.edu, where univ.edu is the name of the local security domain.
- **filename:** Filename
- **filename|authentihash:** A checksum in md5 format
- **filename|impfuzzy:** Import fuzzy hash - a fuzzy hash created based on the imports in the sample.
- **filename|imphash:** Import hash - a hash created based on the imports in the sample.
- **filename|md5:** A filename and an md5 hash separated by a |
- **filename|pehash:** A filename and a PEhash separated by a |
- **filename|sha1:** A filename and an sha1 hash separated by a |
- **filename|sha224:** A filename and a sha-224 hash separated by a |
- **filename|sha256:** A filename and an sha256 hash separated by a |
- **filename|sha3-224:** A filename and an sha3-224 hash separated by a |
- **filename|sha3-256:** A filename and an sha3-256 hash separated by a |
- **filename|sha3-384:** A filename and an sha3-384 hash separated by a |
- **filename|sha3-512:** A filename and an sha3-512 hash separated by a |
- **filename|sha384:** A filename and an sha-384 hash separated by a |

- **filename|sha512**: A filename and a sha-512 hash separated by a |
- **filename|sha512/224**: A filename and a sha-512/224 hash separated by a |
- **filename|sha512/256**: A filename and a sha-512/256 hash separated by a |
- **filename|ssdeep**: A checksum in ssdeep format
- **filename|tlsh**: A filename and a Trend Micro Locality Sensitive Hash separated by a |
- **filename|vhash**: A filename and a VirusTotal hash separated by a |
- **first-name**: First name of a natural person
- **float**: A floating point value.
- **frequent-flyer-number**: The frequent flyer number of a passenger
- **gender**: The gender of a natural person (Male, Female, Other, Prefer not to say)
- **gene**: GENE - Go Evtx sigNature Engine
- **git-commit-id**: A git commit ID.
- **github-organisation**: A github organisation
- **github-repository**: A github repository
- **github-username**: A github user name
- **hashh-md5**: hashh is a network fingerprinting standard which can be used to identify specific Client SSH implementations. The fingerprints can be easily stored, searched and shared in the form of an MD5 fingerprint.
- **hashhserver-md5**: hashhServer is a network fingerprinting standard which can be used to identify specific Server SSH implementations. The fingerprints can be easily stored, searched and shared in the form of an MD5 fingerprint.
- **hex**: A value in hexadecimal format
- **hostname**: A full host/dnsname of an attacker
- **hostname|port**: Hostname and port number separated by a |
- **http-method**: HTTP method used by the malware (e.g. POST, GET, ...).
- **iban**: International Bank Account Number
- **identity-card-number**: Identity card number
- **impfuzzy**: A fuzzy hash of import table of Portable Executable format
- **imphash**: Import hash - a hash created based on the imports in the sample.
- **ip-dst**: A destination IP address of the attacker or C&C server
- **ip-dst|port**: IP destination and port number separated by a |
- **ip-src**: A source IP address of the attacker
- **ip-src|port**: IP source and port number separated by a |
- **issue-date-of-the-visa**: The date on which the visa was issued
- **ja3-fingerprint-md5**: JA3 is a method for creating SSL/TLS client fingerprints that should be easy to produce on any platform and can be easily shared for threat intelligence.
- **jabber-id**: Jabber ID
- **kusto-query**: Kusto query - Kusto from Microsoft Azure is a service for storing and running interactive analytics over Big Data.
- **last-name**: Last name of a natural person
- **link**: Link to an external information
- **mac-address**: Mac address
- **mac-eui-64**: Mac EUI-64 address
- **malware-sample**: Attachment containing encrypted malware sample
- **malware-type**:
- **md5**: A checksum in md5 format
- **middle-name**: Middle name of a natural person
- **mime-type**: A media type (also MIME type and content type) is a two-part identifier for file formats and format contents transmitted on the Internet
- **mobile-application-id**: The application id of a mobile application
- **mutex**: Mutex, use the format \BaseNamedObjects\
- **named pipe**: Named pipe, use the format .\pipe\
- **nationality**: The nationality of a natural person

- **other:** Other attribute
- **passenger-name-record-locator-number:** The Passenger Name Record Locator is a key under which the reservation for a trip is stored in the system. The PNR contains, among other data, the name, flight segments and address of the passenger. It is defined by a combination of five or six letters and numbers.
- **passport-country:** The country in which the passport was issued
- **passport-expiration:** The expiration date of a passport
- **passport-number:** The passport number of a natural person
- **pattern-in-file:** Pattern in file that identifies the malware
- **pattern-in-memory:** Pattern in memory dump that identifies the malware
- **pattern-in-traffic:** Pattern in network traffic that identifies the malware
- **payment-details:** Payment details
- **pdb:** Microsoft Program database (PDB) path information
- **pehash:** PEhash - a hash calculated based of certain pieces of a PE executable file
- **pgp-private-key:** A PGP private key
- **pgp-public-key:** A PGP public key
- **phone-number:** Telephone Number
- **place-of-birth:** Place of birth of a natural person
- **place-port-of-clearance:** The port of clearance
- **place-port-of-onward-foreign-destination:** A Port where the passenger is transiting to
- **place-port-of-original-embarkation:** The original port of embarkation
- **port:** Port number
- **primary-residence:** The primary residence of a natural person
- **prtn:** Premium-Rate Telephone Number
- **redress-number:** The Redress Control Number is the record identifier for people who apply for redress through the DHS Travel Redress Inquiry Program (DHS TRIP). DHS TRIP is for travelers who have been repeatedly identified for additional screening and who want to file an inquiry to have erroneous information corrected in DHS systems
- **regkey:** Registry key or value
- **regkey|value:** Registry value + data separated by |
- **sha1:** A checksum in sha1 format
- **sha224:** A checksum in sha-224 format
- **sha256:** A checksum in sha256 format
- **sha3-224:** A checksum in sha3-224 format
- **sha3-256:** A checksum in sha3-256 format
- **sha3-384:** A checksum in sha3-384 format
- **sha3-512:** A checksum in sha3-512 format
- **sha384:** A checksum in sha-384 format
- **sha512:** A checksum in sha-512 format
- **sha512/224:** A checksum in the sha-512/224 format
- **sha512/256:** A checksum in the sha-512/256 format
- **sigma:** Sigma - Generic Signature Format for SIEM Systems
- **size-in-bytes:** Size expressed in bytes
- **snort:** An IDS rule in Snort rule-format
- **special-service-request:** A Special Service Request is a function to an airline to provide a particular facility for A Passenger or passengers.
- **ssdeep:** A checksum in ssdeep format
- **stix2-pattern:** STIX 2 pattern
- **target-email:** Attack Targets Email(s)
- **target-external:** External Target Organizations Affected by this Attack
- **target-location:** Attack Targets Physical Location(s)
- **target-machine:** Attack Targets Machine Name(s)
- **target-org:** Attack Targets Department or Organization(s)

- **target-user**: Attack Targets Username(s)
- **text**: Name, ID or a reference
- **threat-actor**: A string identifying the threat actor
- **tlsh**: A checksum in the Trend Micro Locality Sensitive Hash format
- **travel-details**: Travel details
- **twitter-id**: Twitter ID
- **uri**: Uniform Resource Identifier
- **url**: url
- **user-agent**: The user-agent used by the malware in the HTTP request.
- **vhash**: A VirusTotal checksum
- **visa-number**: Visa number
- **vulnerability**: A reference to the vulnerability used in the exploit
- **weakness**: A reference to the weakness used in the exploit
- **whois-creation-date**: The date of domain's creation, obtained from the WHOIS information.
- **whois-registrant-email**: The e-mail of a domain's registrant, obtained from the WHOIS information.
- **whois-registrant-name**: The name of a domain's registrant, obtained from the WHOIS information.
- **whois-registrant-org**: The org of a domain's registrant, obtained from the WHOIS information.
- **whois-registrant-phone**: The phone number of a domain's registrant, obtained from the WHOIS information.
- **whois-registrar**: The registrar of the domain, obtained from the WHOIS information.
- **windows-scheduled-task**: A scheduled task in windows
- **windows-service-displayname**: A windows service's displayname, not to be confused with the windows-service-name. This is the name that applications will generally display as the service's name in applications.
- **windows-service-name**: A windows service name. This is the name used internally by windows. Not to be confused with the windows-service-displayname.
- **x509-fingerprint-md5**: X509 fingerprint in MD5 format
- **x509-fingerprint-sha1**: X509 fingerprint in SHA-1 format
- **x509-fingerprint-sha256**: X509 fingerprint in SHA-256 format
- **xmr**: Monero Address
- **yara**: Yara signature
- **zeek**: An [NIDS](#) rule in the Zeek rule-format

Last modified: Thu May 23 2019 10:38:13 GMT+0200 (CEST)

- [Sharing / Synchronisation](#)
- [Synchronisation](#)
  - [Concept](#)
  - [Adding a server](#)
  - [Test connection](#)
  - [Rules](#)
  - [Troubleshooting](#)
- [Sharing and distribution](#)
  - [Distribution settings](#)
  - [Community](#)
  - [Distribution mechanisms](#)
  - [Sharing-groups](#)
- [Collaboration](#)
  - [Proposals](#)
  - [Forums / Threats](#)
    - [Create a new Topic](#)
    - [Comment a topic](#)
  - [Comments to events](#)
  - [Contact a reporter](#)
  - [Receive alerts](#)
- [Recommendation](#)
  - [MISP Staging System](#)
  - [MISP SECOps System](#)

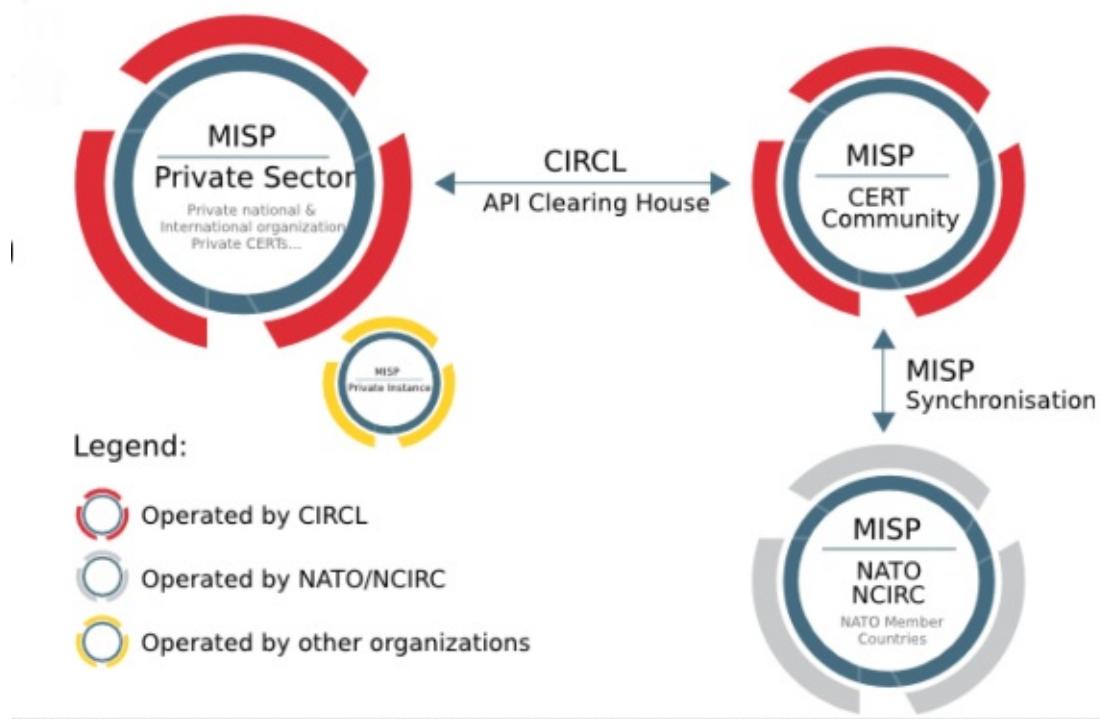
## Sharing / Synchronisation

- MISP's core functionality is sharing where everyone can be a consumer and/or a contributor/producer.
- Quick benefit without the obligation to contribute
- Low barrier access to get acquainted to the system

## Synchronisation

### Concept

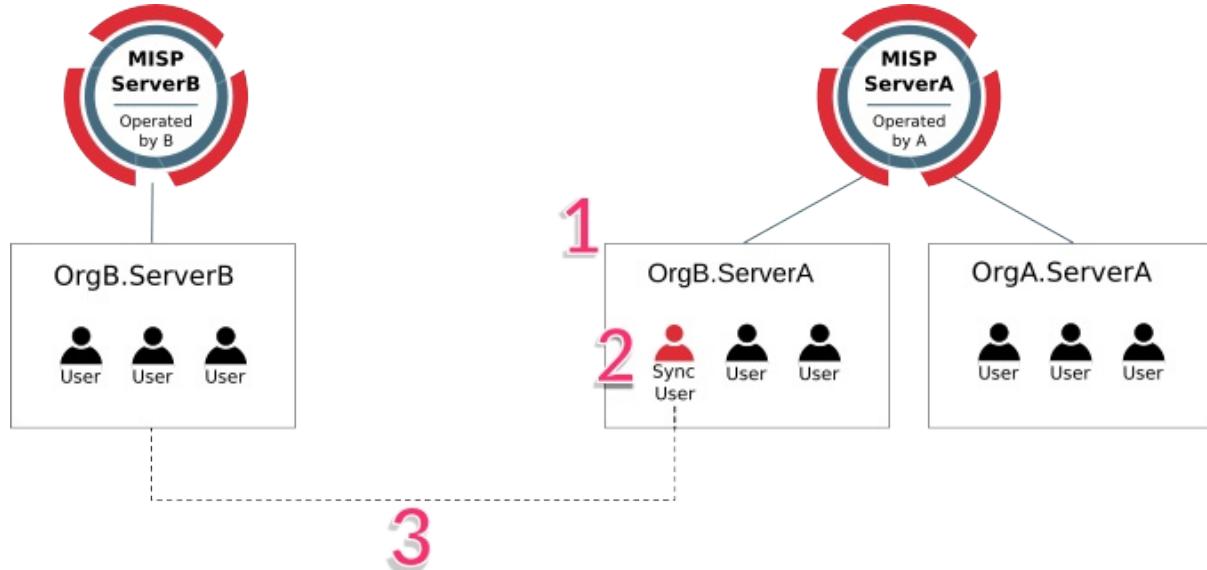
The following figure shows the concept how different MISP instances could tie together.



In MISP, two ways exist to get events from remote sources:

- **Use case 1:** From another MISP server (also called [MISP instance](#)), by synchronising two MISP servers.
- **Use case 2:** From a link, by using [Feeds](#).

The example below illustrate the [synchronisation](#) between two MISP servers (use case 1). An organisation B (OrgB) wants to synchronise its MISP server, called ServerB, with the MISP server of an organisation A (Org A), called ServerA. The following steps can be taken to syncronise ServerB with ServerA:



Legend:

- Synchronisation between two MISP servers
- Organisation in the MISP database of a MISP server
- [Box] Organisation
- [User icon] User of an organisation in the MISP database of a MISP server
- [MISP server icon] MISP server (also called MISP instance)

FIGURE: Illustration of the [synchronisation](#) between two MISP servers

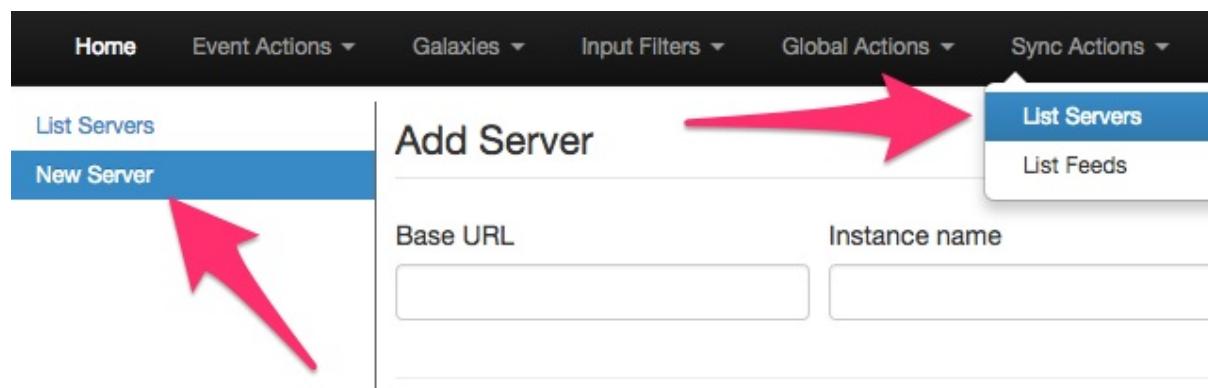
- **Step 1:** Add OrgB as a local organisation on ServerA (OrgB.ServerA) using OrgB's existing UUID from their local organisation on ServerB.
- **Step 2:** Add a [Sync User](#) (syncuser@OrgB.ServerA) in the organisation OrgB.ServerA on the MISP ServerA.
- **Step 3:** Set up a sync server on MISP ServerB using the key (called Authkey) from the [sync user](#) (syncuser@OrgB.ServerA) created on MISP ServerA.

For additional information on the [synchronisation](#) process, refer to the [MISP GitHub issues](#), for example, [issue 2595](#).

## Adding a server

Servers can be added by users via

`https://<misp url>/servers/add`



The Add Server Form has several input fields:

## Add Server

Base URL

Instance name

Information about the organisation that will receive the events, typically the remote instance's host organisation.

Remote Sync Organisation Type      Local Organisation

Local organisation

CIRCL

Authkey

Push

Pull

Self Signed

**Server certificate file**

**Client certificate file**

Push rules:

**Modify**

Pull rules:

**Modify**

**Submit**

## 1. Base URL

The base-url to the external server you want to sync with. Example: <https://foo.sig.mil.be>

## 2. Instance Name

A name that will make it clear to your users what this instance is. For example: Organisation A's instance

## 3. Remote Sync Organisation Type

MISP has several organisation "pools", one for local and one for known external organisations. When adding a [synchronisation](#) connection, you need to define the host organisation of the remote instance. Select which pool you wish to pick the organisation from using this drop-down. You also have the option of adding a new organisation directly from this interface.

## 4. Local/Known remote Organisation

Choose the organisation from the selected pool that defines the host organisation on the remote side. Make sure that the remote instance is actually run by the organisation you select as this is used in an integral part of the sharing mechanism. Do not select your own organisation for this setting.

## 5. Authkey

You can find the authentication key on your profile on the external server.

## 6. Push

Allow the upload of events and their attributes. That means only Events that match the given filter will be pushed to the server.

E.g. it can limit [push](#) of events to events not being TLP:RED

### 1. Pull

Allow the download of events and their attributes from the server. That means only Events matching the given criteria will be pulled.

E.g. it can limit to NOT download Type:[OSINT](#) events.

### 2. Self Signed

Click this, if you would like to allow a connection despite the other instance using a self-signed certificate (not recommended). (server certificate file still needed)

### 3. Server certificate file

You can also upload a certificate file if the instance you are trying to connect to has its own signing authority. (\*.pem)

### 4. Client certificate file

You can also upload a certificate file if the instance you are trying to connect to has its own signing authority. (\*.pem)

## Test connection

Test connection can be used to test the connection to the remote server and will give a feedback about local and remote version of MISP.

## Rules

Rules are used to limit sharing when synchronising events and attributes, to e.g. events with a given tag, or disabling sharing for events containing a certain Tag.

## Troubleshooting

If you have issues connecting to a remote servers try to do the following things:

- try to connect with your user account to the remote server, to ensure the password is still valid and that your [API](#) key is valid
- try to connect with your user account to the remote server and check your [roles](#) on the remote server
- with connection issues do a package capture to find out more
- if you have a SSL connection issue to a remote server with a signed by a CA that is not included in OS, make sure the whole certificate path is included in the path.

## Sharing and distribution

The following section describes how distribution mechanisms of events and attributes work.

### Distribution settings

The below five distribution settings are available for events and attributes. Descriptions of those settings can be found [here](#).

- Your organisation only
- This community only
- Connected communities
- All communities
- Sharing group

Events that are not published are only distributed/shared to the local organisations on the same MISP server/instance (within the limit of the distribution model). Only events that are **published** will be shared with remote organisations on other MISP servers via [push/pull](#) mechanisms. More details on [publishing](#) events [here](#).

### Community

A community is composed of the local organisations on a MISP server and the remote organisations connected by the sync users. For more information on the concept of community, refer to an article on [MISP information sharing following ISO/IEC 27010](#), explaining the concept of community.

Specifically, communities are not reversible. Taking the example of [the above figure](#), illustrating the [synchronisation](#) between two MISP servers, OrgB.ServerB is part of the MISP ServerA community but OrgB.ServerA is not part of MISP ServerB community.

### Distribution mechanisms

The distribution level of an event is automatically decreased as it is synchronised with other MISP instances, when it was originally set to:

- Community only (to organisation only)
- Connected community (to community only)

It is not decreased when it was originally set to:

- Organisation only
- All communities
- Sharing group

[!] This rule does not apply if “Internal instance” has been checked when creating the server.

As an example, the figure below illustrates two events **e** and **e'** created by OrgA and respectively shared as "This community only" and "Connected communities" and how they propagate in an illustrative MISP set of instances synchronised with each others.



*FIGURE: Illustration of MISP organisations and community interactions*

## Sharing-groups

There is an article about [sharing groups](#) in [here](#)

# Collaboration

## Proposals

[Proposals](#) can be used to propose new attribute values that can be reviewed by the event owner.

## Forums / Threats

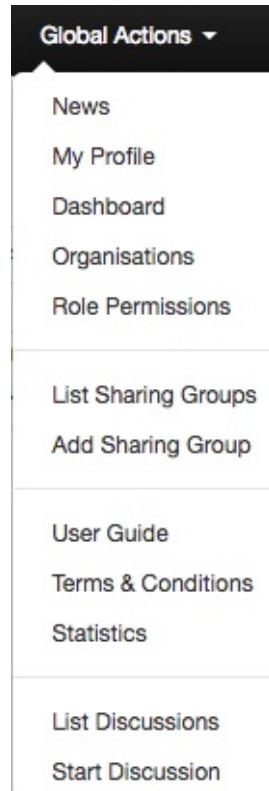
Forums can be used to discuss non event related topics.

Discussions can be accessed on the top "Global Actions - List Discussions"

**Discussions will and can not be shared with other servers**

and via URL:

```
https://<misp url>/threads/index
```



## Create a new Topic

To create a new topic

<https://<misp url>/posts/add>

[List Threads](#)

[New Thread](#)

### Add Post

Thread Subject

This is a test subject

[Quote](#) [Event](#) [Thread](#) [Link](#) [Code](#)

I would like to talk about foo bar because...

[Submit](#)

## Comment a topic

A topic can be commented by any user

```
https://<misp url>/threads/view/<topic id>
```

## Comments to events

In MISP ongoing events can be commented by every user to ask free text question to events. **Comments to events will not be shared with other servers**

The screenshot shows a MISP web interface for commenting on an event. At the top, there is a header bar with the date "Date: 2017-01-21 16:09:25" and a "Top | #2" link. Below the header, a message from the user "MISP" reads "this is a test". The message is timestamped at "2017-01-21 16:09:25". The message area has a "Delete" and "Edit" button. Below the message, the email "admin@misp.training" is listed. At the bottom of the page, there is a navigation bar with links "Quote", "Event", "Thread", "Link", and "Code". A large blue "Send" button is located at the bottom left. A red arrow points from the "Send" button towards the message input area.

## Contact a reporter

This feature can be used to contact the person or the organisation that the person belongs to that has created the event.

All E-Mails can be enforced to be encrypted

## Contact organization reporting event 4

---

You are about to contact the organization that reported event 4.

Feel free to add a custom message that will be sent to the reporting organization.

Your email address and details about the event will be added automatically to the message.

### Message

Hello,

we have seen several of the indicators mentioned in this event in our network, do you have any more information on it?

- Submit only to the person that  
created the event

**Submit**

## Receive alerts

It is possible to get alerts via encrypted mail in the following cases:

- published events by other user of the [MISP instance](#)
- events pushed to the [MISP instance](#)
- events pulled by the [MISP instance](#)

These E-Mail alerts are an opt-in feature

## Edit My Profile

Email	Password	Confirm Password
admin@misp.training		
Organisation	Role	Nids Sid
	admin	4000000
GPG key		
<input type="button" value="Fetch GPG key"/>		
<input type="checkbox"/> Receive alerts when events are published <input type="checkbox"/> Receive alerts from "contact reporter" requests		
<input type="button" value="Submit"/>		



## Recommendation

The following section will describe what is the best practice how many MISP instances that showed to be good for orgs. Of course depending on your specific requirements an architecture could be more spread or simplified.

The architecture is divided into several systems / stages beginning with:

### MISP Staging System

This systems purpose is to be linked to all available external MISP systems that you have access to. It will download all events and do enrichment between these events.

### MISP SECOps System

This system is the main system used by human analysts. It will it is not linked to any external [MISP instance](#) other then the Staging System.

To publish events to the community assign the right tags to match your [push Rules](#) and [publish the event](#)

Last modified: Tue Dec 31 2019 09:27:21 GMT+0100 (CET)

## External Connectors

The **MISP to Microsoft Graph Security Script** enables you to connect your custom threat [indicators](#) or [Indicators of Compromise \(IoCs\)](#) and make these available in the following Microsoft products.

### Azure Sentinel

[Azure Sentinel](#)

### Microsoft Defender ATP

[Microsoft Defender ATP](#)

## MISP to Microsoft Graph Security Script

The script provides clients with MISP instances to migrate threat [indicators](#) to the [Microsoft Graph Security API](#).

For more information on Microsoft Graph Security API visit [Microsoft Graph Security API](#).

For more information on Microsoft Graph visit [Microsoft Graph](#).

### Prerequisites

Before installing the sample:

- Install Python 3.x version from <https://www.python.org/>.
- To register your application for access to Microsoft Graph, you'll need either a [Microsoft account](#) or an [Office 365 for business account](#). If you don't have one of these, you can create a Microsoft account for free at [outlook.com](https://outlook.com).

### Getting Started

After the prerequisites are installed or met, perform the following steps to use these scripts:

1. Download or clone this repository.
2. Go to directory `security-api-solutions/Samples/MISP`
3. Install dependencies. In the command line, run `pip3 install requests requests-futures pymisp`
4. To run script, go to the root directory of `misp-graph-script` and enter `PYTHONHASHSEED=0 python3 script.py` in the command line.

### App Registration

To configure the sample, you'll need to register a new application in the Microsoft [Application Registration Portal](#). Follow these steps to register a new application:

1. Sign in to the [Application Registration Portal](#) using either your personal or work or school account.
2. Choose **New registration**.

3. Enter an application name, and choose **Register**.
  4. Next you'll see the overview page for your app. Copy and save the **Application Id** field. You will need it later to complete the configuration process.
  5. Under **Certificates & secrets**, choose **New client secret** and add a quick description. A new secret will be displayed in the **Value** column. Copy this password. You will need it later to complete the configuration process and it will not be shown again.
  6. Under **API permissions**, choose **Add a permission > Microsoft Graph**.
  7. Under **Application Permissions**, add the permissions/scopes required for the sample. This sample requires **ThreatIndicators.ReadWrite.OwnedBy**.
- Note:** See the [Microsoft Graph permissions reference](#) for more information about Graph's permission model.
8. Modify the RequestManager.py file to comment out line 121-124. (This allows the script to run without failing due to line 123 being divided by `avg_speed` incase it starts as `0` .
  9. Modify the script.py to add in `config.misp_verifycert` at line 13. Ensure it looks like below.

```
misp = PyMISP(config.misp_domain, config.misp_key, config.misp_verifycert)
```

10. Modify config.py file to add in `misp_verifycert = False` anywhere in the file.

As the final step in configuring the script, modify the config.py file in the root folder of your cloned repo.

Update tenant, client\_id, and client\_secret in config.py

```
graph_auth = {
    'tenant': '<tenant id>',
    'client_id': '<client id>',
    'client_secret': '<client secret>',
}
```

Once changes are complete, save the config file.

## Configurations

### Target Product

```
targetProduct = "Azure Sentinel" or targetProduct = "Microsoft Defender ATP"
```

### Misp Event Filter

Filters can be set in the config.py file under the "misp\_event\_filters" property

Below is a list of parameters that can be passed to the filter (source: <https://pymisp.readthedocs.io/modules.html>):

- values – values to search for
- not\_values – values not to search for
- type\_attribute – Type of attribute
- category – Category to search
- org – Org reporting the event
- tags – Tags to search for
- not\_tags – Tags not to search for
- date\_from – First date (Format: '2019-01-01')

- date\_to – Last date (Format: '2019-01-01')
- last – Last published events (for example 5d or 12h or 30m)
- eventid – Event ID
- withAttachments – return events with or without the attachments
- uuid – search by uuid
- publish\_timestamp – the publish timestamp (Note: Uses UNIX timestamp. Format: '1551811160')
- published – return only published events (Format: True or False)

A list or a specific value can be passed to the above parameters. If a list is passed to the parameter, the filtered events are the result of the union of provided list.

This field needs to be a list that contains multiple filters. The filtered events are the result of the intersection of provided filters.

## First Example of How This Field can be Configured

```
misp_event_filters = [
    {
        "type_attribute": "mutex"
    },
    {
        "type_attribute": "filename|md5"
    },
]
```

An event meets this filtering criteria if the event has an attribute with attribute type of 'mutex' AND the event has an attribute with attribute type of 'filename|md5'.

## Second Example of How This Field can be Configured

```
misp_event_filters = [
    {
        "type_attribute": ['mutex', 'filename|md5']
    }
]
```

An event meets this filtering criteria if the event has an attribute with attribute type of 'mutex' OR the event has an attribute with attribute type of 'filename|md5'.

## Third Example of How This Field can be Configured

```
misp_event_filters = [
    {
        "values": 'http://www.test.com'
    }
]
```

An event meets this filtering criteria if the event has an attribute with attribute value of '<http://www.test.com>'.

## Fourth Example of How This Field can be Configured

```
misp_event_filters = []
```

This gets all events.

## Action

Possible **action** values are: `alert` , `allow` , `block` .

```
action = "alert" (This is default).
```

## Passive Only

```
passiveOnly = False (This is default).
```

## Days to Expire

This property is used to specify the amount of days the records will expire in Microsoft Graph Security API. The default value for days to expire is 30.

```
days_to_expire = 5
```

## Misp Key

The Misp Auth Key is required to fetch data from your [Misp instance](#). Configure a [sync user](#).

```
misp_key = '<misp key>'
```

## Verify Cert

This gives you the option to choose if python should validate the certificate of the [misp instance](#). (This allows ease within testing environments)

```
misp_verifycert = False IT IS RECOMENDED TO USE A VALID SSL CERT IN PRODUCTION AND CHANGE THIS TO TRUE
```

## Instructions on Reading TiIndicators That Have Been Pushed

In the command line, run `python3 script.py -r`

## Instructions on Seeing All Requests That Resulted in Errors

1. In the command line, run `cd logs` to go to the logs folder.
2.
  - o To print all the requests that resulted in errors to the console, simply run `cat *_error_*` in the command line.
  - o To aggregate all the requests that resulted in errors to a file, run `cat *_error_* > <filename>.txt` in the command line.

## Script Output

As the script runs, it prints out the request body sent to the Microsoft Graph Security API and the response from the Microsoft Graph Security API.

Every request is logged as a json file under the directory "logs". The name of the json file is the datetime of when the request is completed.

## Schedule with CRONTAB

Below is a CRONTAB entry example of running the script every Sunday at 2am

```
0 2 Sun /home/mark/misp-graph-script/python3 script.sh
```

This README.md has been adapted from the README.md found in the [Microsoft Graph Security API MISP sample](#). For most recent changes, visit [Microsoft Graph Security API MISP sample](#). Provide your feedback on this sample by [filing a GitHub request](#).

Last modified: Fri May 17 2019 12:07:48 GMT+0200 (CEST)

## MISP modules

[MISP modules](#) are autonomous modules that can be used for expansion and other services in MISP. The modules are written in Python 3 following a simple [API](#) interface. The objective is to ease the extensions of MISP functionalities without modifying core components. The [API](#) is available via a simple REST [API](#) which is independent from MISP installation or configuration.

MISP modules support is included in MISP starting from version 2.4.28.

[More](#)

[MISP modules GitHub Repo](#)

## Installation

[Install guide on Ubuntu](#)

[Install guide RHEL/CentOS](#)

Last modified: Fri Dec 14 2018 09:14:09 GMT+0100 (CET)

- [MISP ZeroMQ](#)
  - [MISP ZeroMQ configuration](#)
  - [MISP ZeroMQ debugging and testing](#)
  - [Testing with sub.py tool](#)
  - [Notification Schemas](#)
    - `misp_json` - events published
    - `misp_json_attribute` - attribute updated or created
    - `misp_json_sighting` - sighting added to an attribute or an event
    - `misp_json_user` - user updates or creation
    - `misp_json_organisation` - organisation updates or creation
    - `misp_json_self` - keep-alive messages sent every minute
  - [Tips for Building a Subscriber](#)

## MISP ZeroMQ

MISP includes a flexible publish-subscribe model to allow real-time integration of the MISP activities (event publication, attribute creation or removal, sighting). The MISP ZeroMQ plugin operates at global level in MISP which means standard distribution rules don't apply and every activities will be published within the ZeroMQ pub-sub channels.

MISP ZeroMQ functionality can be used for various model of integration or to extend MISP functionalities:

- real-time search of [indicators](#) into a SIEM
- automatic expansion
- dashboard activities
- logging mechanisms
- continuous indexing
- custom software or scripting

The following notification topic channels exist and can be included in the MISP ZeroMQ pub-sub:

- `misp_json` - events published
- `misp_json_attribute` - attribute updated or created
- `misp_json_sighting` - sighting added to an attribute or an event
- `misp_json_user` - user updates or creation
- `misp_json_organisation` - organisation updates or creation
- `misp_json_self` - keep-alive messages sent every minute

## MISP ZeroMQ configuration

To enable MISP ZeroMQ, the feature must be enabled in the Plugin setting tab.

Prior to enabling it, make sure that you have the pyzmq installed by running

```
sudo pip install pyzmq  
sudo pip install redis
```

If you have problems and the plugin does not start, the logfile may be helpful.

```
sudo cat /var/www/MISP/app/tmp/logs/mispzmq.error.log
```

**Server settings**

<a href="#">Overview</a>   <a href="#">MISP settings (27)</a>   <a href="#">Encryption settings (6)</a>   <a href="#">Proxy settings (5)</a>   <a href="#">Security settings (2)</a>   <a href="#">Plugin settings (50)</a>   <span style="border: 1px solid #ccc; padding: 2px;"> </span>   <a href="#">Diagnostics</a>   <span style="border: 1px solid #ccc; padding: 2px;"> </span>   <a href="#">Workers</a>   <span style="border: 1px solid #ccc; padding: 2px;"> </span>   <a href="#">Manage files</a>   <span style="border: 1px solid #ccc; padding: 2px;"> </span>   <span style="border: 1px solid #ccc; padding: 2px;"> </span>				
<a href="#">Enrichment</a>   <span style="border: 1px solid #ccc; padding: 2px;">Import</span>   <span style="border: 1px solid #ccc; padding: 2px;">Export</span>   <span style="border: 1px solid #ccc; padding: 2px;">Cortex</span>   <span style="border: 1px solid #ccc; padding: 2px;">Sightings</span>   <span style="border: 1px solid #ccc; padding: 2px;">RPZ</span>   <span style="border: 1px solid #ccc; padding: 2px;">ZeroMQ</span>				
Priority	Setting	Value	Description	Error Message
Optional	Plugin.ZeroMQ_enable	true	Enables or disables the pub/sub feature of MISP. Make sure that you install the requirements for the plugin to work. Refer to the installation instructions for more information.	
Optional	Plugin.ZeroMQ_port	50000	The port that the pub/sub feature will use.	Value not set.
Optional	Plugin.ZeroMQ_redis_host	localhost	Location of the Redis db used by MISP and the Python PUB script to queue data to be published.	Value not set.
Optional	Plugin.ZeroMQ_redis_port	7777	The port that Redis is listening on.	
Optional	Plugin.ZeroMQ_redis_password		The password, if set for Redis.	Value not set.
Optional	Plugin.ZeroMQ_redis_database	1	The database to be used for queuing messages for the pub/sub functionality.	Value not set.
Optional	Plugin.ZeroMQ_redis_namespace	mispq	The namespace to be used for queuing messages for the pub/sub functionality.	Value not set.
Optional	Plugin.ZeroMQ_event_notifications_enable	true	Enables or disables the publishing of any event creations/edits/deletions.	
Optional	Plugin.ZeroMQ_object_notifications_enable	true	Enables or disables the publishing of any object creations/edits/deletions.	
Optional	Plugin.ZeroMQ_object_reference_notifications_enable	true	Enables or disables the publishing of any object reference creations/deletions.	
Optional	Plugin.ZeroMQ_attribute_notifications_enable	true	Enables or disables the publishing of any attribute creations/edits/soft deletions.	
Optional	Plugin.ZeroMQ_sighting_notifications_enable	true	Enables or disables the publishing of new sightings to the ZMQ pubsub feed.	
Optional	Plugin.ZeroMQ_user_notifications_enable	true	Enables or disables the publishing of new/modified users to the ZMQ pubsub feed.	
Optional	Plugin.ZeroMQ_organisation_notifications_enable	true	Enables or disables the publishing of new/modified organisations to the ZMQ pubsub feed.	

Each notification channels can be enabled (from event publication to sightings), the MISP [site admin](#) can decide which type of message to publish.

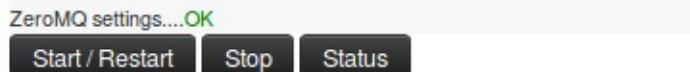
By default, the ZMQ pub-sub channel is available to localhost only on TCP port 50000. The binding of the pub-sub channel can be updated in the configuration interface as shown above

## MISP ZeroMQ debugging and testing

In the diagnostic section, ZeroMQ service can be started and stopped. There is a small status option to give information about the numbers of events processed by the service.

### ZeroMQ

This tool tests whether the ZeroMQ extension is installed and functional.



## Testing with sub.py tool

A simple command line tool is included with MISP to connect to the MISP ZeroMQ channel and get the notifications:

```
python3 sub.py --help
usage: sub.py [-h] [-s] [-p PORT] [-r HOST] [-o ONLY] [-t SLEEP]

Generic ZMQ client to gather events, attributes and sighting updates from a
MISP instance

optional arguments:
  -h, --help            show this help message and exit
  -s, --stats           print regular statistics on stderr
  -p PORT, --port PORT set TCP port of the MISP ZMQ (default: 50000)
  -r HOST, --host HOST  set host of the MISP ZMQ (default: 127.0.0.1)
  -o ONLY, --only ONLY   set filter (misp_json, misp_json_attribute or
                        misp_json_sighting) to limit the output a specific
                        type (default: no filter)
  -t SLEEP, --sleep SLEEP
                        sleep time (default: 2)
```

The `sub.py` will output the JSON objects for the subscribed topic, by default, all the topic channels are dumped:

```
misp@cpeb:/var/www/MISP/tools/misp-zmq$ python3 -u sub.py | jq .
...
{
  "uptime": 50,
  "status": "And when you're dead I will be still alive."
}
{
  "uptime": 60,
  "status": "And believe me I am still alive."
}
{
  "uptime": 70,
  "status": "I'm doing science and I'm still alive."
}
{
  "uptime": 80,
  "status": "I feel FANTASTIC and I'm still alive."
}
{
  "uptime": 90,
  "status": "While you're dying I'll be still alive."
}
{
  "Sighting": {
    "uuid": "592d9588-fda0-490f-bf6e-4e56950d210f",
    "source": "",
    "type": "0",
    "date_sighting": 1496159624,
    "org_id": "2",
    "event_id": "8102",
    "attribute_id": "1044812"
  }
}
{
  "Attribute": {
    "id": "1044802",
    "value2": "",
    "value1": "1.2.3.4",
    "uuid": "592d8494-7120-4760-b5e2-4858950d210f",
    "batch_import": "0",
    "comment": "",
    "value": "1.2.3.4",
    "type": "0"
  }
}
```

```

    "type": "ip-dst",
    "to_ids": 0,
    "timestamp": 1496155284,
    "distribution": "5",
    "sharing_group_id": 0,
    "deleted": "0",
    "disable_correlation": "0",
    "event_id": "8100",
    "category": "Network activity"
}
}
....

```

## Notification Schemas

Each notification channel uses a slightly different JSON schema. Consult this section to identify which MISP components exist in a channel:

### **misp\_json - events published**

When an event is published to ZMQ (which is different from being published in MISP) the ZMQ notification will just contain the [MISP event](#) data along with all its component children. These components include:

- A list of attributes
- A list of objects, which contain their own lists of attributes
- A list of related events - added when attributes in separate events correlate
- Any galaxies that this event belongs to
- A list of tags that apply to the event

Example:

```
{
  "Event": {
    "id": "625",
    "orgc_id": "2",
    "org_id": "1",
    "date": "2017-05-24",
    "threat_level_id": "3",
    "info": "M2M - Fwd: IMG_3428.pdf",
    "published": false,
    "uuid": "59259036-fcd0-4749-8a6c-4d88950d210f",
    "attribute_count": "7",
    "analysis": "1",
    "timestamp": "1505755565",
    "distribution": "3",
    "proposal_email_lock": false,
    "locked": false,
    "publish_timestamp": "1505416766",
    "sharing_group_id": "0",
    "disable_correlation": false,
    "Org": {"id": "1", "name": "MISP", "uuid": "56ef3277-1ad4-42f6-b90b-04e5c0a83832"},
    "Orgc": {"id": "2", "name": "CIRCL", "uuid": "55f6ea5e-2c60-40e5-964f-47a8950d210f"},
    "Attribute": [
      {
        "id": "157835",
        "type": "attachment",
        "category": "Artifacts dropped",
        "to_ids": false,
        "uuid": "59259037-1014-4669-96b1-46af950d210f",
        "event_id": "625",
        "distribution": "5",
        "timestamp": "1495633975",
        "comment": "IMG_3428.pdf",
        "File": {
          "id": "157835",
          "name": "IMG_3428.pdf",
          "size": 123456789,
          "type": "application/pdf"
        }
      }
    ]
  }
}
```

```

        "sharing_group_id": "0",
        "deleted": false,
        "disable_correlation": false,
        "object_id": "0",
        "object_relation": null,
        "value": "tmpzuni0skf",
        "ShadowAttribute": []
    }
],
"ShadowAttribute": [],
"RelatedEvent": [],
"Galaxy": [],
"Object": [
{
    "id": "1",
    "name": "http-request",
    "meta-category": "network",
    "description": "A single HTTP request header",
    "template_uuid": "b4a8d163-8110-4239-bfcf-e08f3a9fdf7b",
    "template_version": "1",
    "event_id": "625",
    "uuid": "59c0016c-0984-4779-9688-05b8c0a83832",
    "timestamp": "1505755500",
    "distribution": "5",
    "sharing_group_id": "0",
    "comment": "",
    "deleted": false,
    "ObjectReference": [],
    "Attribute": [
{
        "id": "164371",
        "type": "http-method",
        "category": "Network activity",
        "to_ids": false,
        "uuid": "59c0016c-a744-440d-ad92-05b8c0a83832",
        "event_id": "625",
        "distribution": "5",
        "timestamp": "1505760143",
        "comment": "",
        "sharing_group_id": "0",
        "deleted": false,
        "disable_correlation": false,
        "object_id": "1",
        "object_relation": "method",
        "value": "POST",
        "ShadowAttribute": []
},
{
        "id": "164372",
        "type": "uri",
        "category": "Network activity",
        "to_ids": true,
        "uuid": "59c0016c-fac0-4055-9f3d-05b8c0a83832",
        "event_id": "625",
        "distribution": "5",
        "timestamp": "1505755500",
        "comment": "",
        "sharing_group_id": "0",
        "deleted": false,
        "disable_correlation": false,
        "object_id": "1",
        "object_relation": "uri",
        "value": "\/test.php",
        "ShadowAttribute": []
}
]
}
],
"Tag": [{"id": "2", "name": "tlp:white", "colour": "#ffffff", "exportable": true, "hide_tag": false}]

```

```

    }
}
```

## misp\_json\_attribute - attribute updated or created

The attributes appear to have the most diversity depending on the action applied to them.

When an attribute gets created, just the attribute gets sent out via ZMQ. Its parent event id is sent inside the attribute JSON, but there is no extra event metadata like there is when an attribute is deleted or modified.

Create Example:

```
{
  "Attribute": {
    "to_ids": "1",
    "timestamp": 1505235275,
    "distribution": "5",
    "deleted": "0",
    "disable_correlation": "0",
    "event_id": "625",
    "category": "Network activity",
    "type": "domain",
    "value": "microsoft.net",
    "comment": "",
    "batch_import": "0",
    "uuid": "59b8114b-1c80-4149-be3a-03e9c0a83832",
    "sharing_group_id": 0,
    "value1": "microsoft.net",
    "value2": "",
    "id": "164363"
  }
}
```

Edited attribute notifications send metadata about their parent events and information about the attribute's sharing group, attribute-level tags, and sightings data. It's important to note that only the new value of the edited attribute is sent along the ZMQ channel. In order to diff the new and old values, you'd have to have a copy of the old attribute value stored somewhere and can use the attribute's `uuid` key (which never changes) to correlate the new and old values.

Edit Example:

```
// microsoft.net --> microsoft.com
{
  "Attribute": {
    "id": "164363",
    "event_id": "625",
    "category": "Network activity",
    "type": "domain",
    "value1": "microsoft.com",
    "value2": "",
    "to_ids": "1",
    "uuid": "59b8114b-1c80-4149-be3a-03e9c0a83832",
    "timestamp": 1505235283,
    "distribution": "5",
    "sharing_group_id": 0,
    "comment": "",
    "deleted": false,
    "disable_correlation": false,
    "value": "microsoft.com",
    "batch_import": "0"
  },
  "Event": {
    "id": "625",
    "org_id": "1",
  }
}
```

```

    "date": "2017-05-24",
    "info": "M2M - Fwd: IMG_3428.pdf",
    "user_id": "1",
    "uuid": "59259036-fcd0-4749-8a6c-4d88950d210f",
    "published": false,
    "analysis": "1",
    "attribute_count": "5",
    "orgc_id": "2",
    "timestamp": "1505235275",
    "distribution": "3",
    "sharing_group_id": "0",
    "proposal_email_lock": false,
    "locked": false,
    "threat_level_id": "3",
    "publish_timestamp": "1505233367",
    "disable_correlation": false
},
"SharingGroup": {
    "id": null,
    "name": null,
    "releasability": null,
    "description": null,
    "uuid": null,
    "organisation_uuid": null,
    "org_id": null,
    "sync_user_id": null,
    "active": null,
    "created": null,
    "modified": null,
    "local": null,
    "roaming": null
},
"AttributeTag": [],
"Sighting": []
},

```

When an attribute gets deleted, the `deleted` key gets set to `1`, and the attribute's event metadata gets sent alongside it.

Delete Example:

```

{
    "Attribute": {
        "id": "164362",
        "event_id": "625",
        "category": "Network activity",
        "type": "domain",
        "value1": "microsoft.com",
        "value2": "",
        "to_ids": true,
        "uuid": "59b81121-f4b4-4ed3-aa43-03eac0a83832",
        "timestamp": 1505235262,
        "distribution": "5",
        "sharing_group_id": 0,
        "comment": "",
        "deleted": 1,
        "disable_correlation": false,
        "value": "microsoft.net"
    },
    "Event": {
        "id": "625",
        "org_id": "1",
        "date": "2017-05-24",
        "info": "M2M - Fwd: IMG_3428.pdf",
        "user_id": "1",
        "uuid": "59259036-fcd0-4749-8a6c-4d88950d210f",
        "published": false,
        "analysis": "1",
        "attribute_count": "5",
        "orgc_id": "2",
        "timestamp": "1505235275",
        "distribution": "3",
        "sharing_group_id": "0",
        "proposal_email_lock": false,
        "locked": false,
        "threat_level_id": "3",
        "publish_timestamp": "1505233367",
        "disable_correlation": false
    }
}

```

```

        "attribute_count": "5",
        "orgc_id": "2",
        "timestamp": "1505235233",
        "distribution": "3",
        "sharing_group_id": "0",
        "proposal_email_lock": false,
        "locked": false,
        "threat_level_id": "3",
        "publish_timestamp": "1505233367",
        "disable_correlation": false
    }
}

```

## **misp\_json\_sighting - sighting added to an attribute or an event**

The message sent for sightings is fairly simple, with the type of sighting (0 = Addition, 1 = False Positive), the date (in seconds-since-epoch format), the id of the attribute it applies to, and the id of the attribute's parent event.

Addition Example:

```

{
    "Sighting": {
        "type": "0",
        "attribute_id": "164373",
        "event_id": "625",
        "org_id": "1",
        "date_sighting": 1505767537,
        "source": "",
        "uuid": "59c03071-f480-4311-a710-03edc0a83832",
        "id": "1"
    }
}

```

False Positive Example:

```

{
    "Sighting": {
        "type": "1",
        "attribute_id": "164373",
        "event_id": "625",
        "org_id": "1",
        "date_sighting": 1505767543,
        "source": "",
        "uuid": "59c03077-d560-4a8b-b841-05b8c0a83832",
        "id": "2"
    }
}

```

## **misp\_json\_user - user updates or creation**

An update is sent through ZMQ when users log in. There are actually two messages in this - both being fairly sparse. The `current_login` message just contains who logged in and what time (in seconds-since-epoch format) it happened. The `last_login` message contains who just logged in, what time the login occurred (technically the date the record was modified, but it's modified when the user logs in, so it appears to be interchangeable in this case), and what time the user last logged in.

Login Example:

```

{
    "User": {
        "id": "1",
        "last_login": "1000046766",

```

```

        "date_modified": 1000060160
    }
}
{
    "User": {
        "id": "1",
        "current_login": 1000060160,
        "date_modified": 1000060160
    }
}

```

When a user gets created, all of the information about the user (id, email, base64 encoded GnuPG key, role, etc.) gets sent along ZMQ. If this information is modified, the same JSON will be sent along the ZMQ channel, with updated values. For example, if the below user is disabled, the same JSON will be sent, but the `disabled` key will be set to `"1"`

User Creation and User Edit Example:

```

{
    "User": {
        "server_id": 0,
        "autoalert": "1",
        "invited_by": "1",
        "nids_sid": 5976699,
        "termsaccepted": 0,
        "role_id": "3",
        "change_pw": 1,
        "contactalert": "1",
        "disabled": "0",
        "current_login": "0",
        "last_login": "0",
        "force_logout": "0",
        "email": "user@testemail.com",
        "enable_password": "0",
        "org_id": "1",
        "authkey": "__<redacted>__",
        "gpgkey": "__<redacted>__",
        "notify": "1",
        "date_created": 1000000000,
        "date_modified": 1000000000,
        "newsread": 0,
        "certif_public": "",
        "id": "4"
    }
}

```

## **misp\_json\_organisation - organisation updates or creation**

Org notifications are sent when Orgs are updated and created, but not deleted. They are generally the same, except the fields `created_by` and `date_created` are present when an Org is created.

Creation Example:

```

{
    "Organisation": {
        "created_by": "1",
        "local": "1",
        "name": "test",
        "uuid": "59c0367d-fe8c-42a4-9db2-03ecc0a83832",
        "description": "Test",
        "nationality": "Not specified",
        "sector": "",
        "type": "",
        "contacts": "",
        "logo": {

```

```

        "name": "",
        "type": "",
        "tmp_name": "",
        "error": 4,
        "size": 0
    },
    "date_created": "2017-09-18 23:11:28",
    "date_modified": "2017-09-18 23:11:28",
    "id": "10"
}
}

```

Edit Example:

```

{
    "Organisation": {
        "local": "1",
        "name": "test",
        "uuid": "59c0367d-fe8c-42a4-9db2-03ecc0a83832",
        "description": "Alternate Test",
        "nationality": "Not specified",
        "sector": "",
        "type": "",
        "contacts": "",
        "logo": {
            "name": "",
            "type": "",
            "tmp_name": "",
            "error": 4,
            "size": 0
        },
        "id": "10",
        "date_modified": "2017-09-18 23:11:37"
    }
}

```

## **misp\_json\_self - keep-alive messages sent every minute**

Only really useful to ensure the ZMQ server is running. And for a bit of humor

```

{
    "status": "I'm doing science and I'm still alive.",
    "uptime": 9170
}

```

## **Tips for Building a Subscriber**

1. `misp_json_attribute` notifications are sent when attributes are created, deleted, and edited
  - o Check the `deleted` key to identify if an attribute has been created or deleted
  - o If an attribute has been edited, the new value will be sent out via ZMQ, but the `uuid` key will remain the same. Use this to determine if an attribute has existed before or not
2. Some compound attribute types have component types that don't exist outside of them
  - o For example, MISP doesn't have a single `ip` attribute type except in the `domain|ip` type
  - o If you're going to split up and resubmit these attributes, you may have to modify these component types so MISP will recognize them (e.g. `domain|ip` -> `domain`, `ip-dst`)

Last modified: Sun Nov 18 2018 06:24:52 GMT+0100 (CET)

# MISP and Internationalization (i18n)

## Requirements

Please read the following [CakePHP documentation about i18n & l10n](#).

## Add one .md per translation effort

Please add a file à la: ja\_JP.md (Japanese\_Japan) or it\_CH.md (Italian\_Switzerland), in which you briefly describe what the current status of your translation effort is and what has been translated and which parts might be gotchas. This would also be a good place to quickly explain what your language is about, like whether most technical terms are a translation from the original, an adaptation from the English word or perhaps you just mostly use English terms.

## Style

Please follow whatever is the purest and most intelligible form of written language in the native tongue being translated.

## Formatting

It is important to use correct formatting. This is wrong:

```
<p><?php echo __('Are you sure you want to delete Proposal #') . $id . '?'; ?></p>
```

You want to have ultimate flexibility and that line should look more like this:

```
<p><?php echo __('Are you sure you want to delete Proposal #{$id}?'); ?></p>
```

In the above example we use an alternative notation of the format string in PHP. Using the above, the generated po-template file ([default.pot](#)) will have the name of the to-be-translated variable in the "msgid" part of the file. Which is easier to read than a non descriptive %s and allows the translator to have context on how the phrase is used in MISP.

In case you have HTML-Tags, move them out of the sentence, out of the php code if possible:

```
<p><?php echo __('<h1>Are you sure you want to:<br />Delete Proposal #%%s?', $id); ?></h1></p>
```

```
<p><h1><?php echo __('Are you sure you want to:%%sDelete Proposal #{$id}?', '<br />'); ?></h1></p>
```

## Issues

Some times it might be impossible to translate some phrases. Or you notice a certain bad formatting, or segmentation of sentences. In that case, please either open an [Issue on Github](#)

## Quirks

Lines like this:

```
echo $this->Form->button('Submit', array('class' => 'btn btn-primary'));$
```

Should be prepared as such:

```
echo $this->Form->button(__('Submit'), array('class' => 'btn btn-primary'));
```

Or another case:

```
echo $this->Form->input('sharing_group_id', array(
    'options' => array($sharingGroups),
    'label' => 'Sharing Group',
));
```

To:

```
echo $this->Form->input('sharing_group_id', array(
    'options' => array($sharingGroups),
    'label' => __('Sharing Group'),
));
```

## Let us know!

Are you planning to do a translation or localization? Please open a ticket on the [issue system](#). This will allow us and others to track what is being worked on. You can keep it very light, as all the details should be in your markdown in misp-book.

## Reach out to the community

Want to chat with other MISP contributors? Make sure to join our [MISP Gitter channel](#).

Last modified: Wed Aug 19 2020 10:27:11 GMT+0200 (CEST)

- Frequently Asked Questions
  - General questions
    - Where can I get support?
    - What are the hardware requirements?
    - How to monitor MISP?
  - Specific questions
    - Can I configure MISP encrypted notification emails to contain more information in the subject?
    - How can I restart the workers?
    - How can I redirect HTTP to HTTPS?
    - When I try to access my new installation, I am redirected to localhost:8443 and get an error.
    - How can I define the default sharing level?
    - How can I add an organisation logo and/or footer logo?
    - All workers are starting correctly except `schdlr`. How can I fix this?
    - How can I import data directly from PDF reports?
    - I am having trouble updating beyond version 2.4.50 (stuck loading any page beyond the login), what can I do?,-  
[what-can-i-do?](#)
    - I have many failed jobs when doing email notification. What should I do?
    - Upgrading from MISP 2.4.65 to MISP 2.4.66 - Unable to merge due to the Composer file.
    - I have issues with pushing events
    - I have many users or API accesses, what's the best PHP session handler?
    - Is there TAXII support?
    - Wipe MISP data - Remove all data
    - Constantly acknowledging my self-signed certificate drives me nuts
    - How can I change the theme?
    - How can I deal with a MISP instance that has pulled in feeds over and over into new events, generating hundreds of GBs of junk correlations, rendering the instance unusable?
    - I have a long list of events that I want to delete via the API, do I really have to loop through each and issue a delete to /events/delete?
    - I can no longer log in. How do I reset the admin password?
  - Usage questions
    - How can I see all the deleted events in a MISP instance?
  - Permission issues
    - RHEL/CentOS
    - Redis Connection problems
  - RHEL/CentOS SELinux debug
    - Clearing the audit logs
  - When to update MISP?
    - How to switch from tagged releases and back?
  - Update MISP fails
    - What can go wrong if I update MISP?
    - error: pathspec 'app/composer.json' did not match any file(s) known to git-known-to-git)
    - MISP modules "Connection refused"
  - Uninstalling MISP
  - Updating PyMISP to incorporate newer versions of the MISP object templates
  - How to disable freetext/custom/user-created tags and only allow certain tags
  - How to enable the csv import module?
  - Why do I see 'The request has been black-holed' when I submit forms?
  - Importing large feeds creates PHP Fatal error
  - I deleted the admin user by mistake

- [config.php is not writeable](#)
- [How to debug misp-dashboard](#)
- [How to update object templates?](#)
- [What to do if my REST client is throwing SSL errors when trying to query my MISP instance?](#)
- [What to do if my REST client cannot reach the host, despite me being able to issue requests using Curl / Postman / etc.?](#)
- [How would one set up a sharing group with a remote org, where we only share a mutual community instance \(i.e. we both have sync users on that instance\). On our local instance, they exist as a remote org \(from events that have synced from their instance via our shared community instance\)..-on-our-local-instance,-they-exist-as-a-remote-org-\(from-events-that-have-synced-from-their-instance-via-our-shared-community-instance\).\)](#)
- [Is it possible to propose objects to an event?](#)
- [How to use the enforceWarninglist parameter in REST search?](#)
- [Column not found issue ~ Symptoms](#)
- [WatchList Customization](#)
  - [How to create a customized WatchList.](#)
- [How to upgrade PHP on RHEL/CentOS?](#)
  - [Example: Upgrade from PHP 7.2 to 7.3 on CentOS 7 ~ Enable repository ~ Install packages ~ Install required PEAR-modules ~ PHP configuration ~ Switch to PHP 7.3 ~ Disable/enable services](#)
- [How to add a galaxy to an event via PyMISP](#)
- [Updating PHP from 7.2 to 7.4.5 on Ubuntu 18.04](#)
  - [Installation](#)
  - [Verification of php 7.2 to 7.4](#)
  - [What are the required steps after a MISP installation to have a properly running instance?](#)

## Frequently Asked Questions

The following page hosts some frequently asked questions as noticed in our [issues](#) and [gitter](#) channels.

---

### General questions

#### Where can I get support?

If you have feature requests or you found a bug you can open a ticket on [MISP's GitHub repository issue](#) tracker.

If you want to discuss something related to MISP or want help from the MISP community, join the appropriate MISP Gitter channel:

- [MISP Developer Room](#) Dev discussions
- [MISP Support Room](#) OMGoo! My MISP doesn't work discussions
- [MISP Sharing Room](#) Threat Intelligence Sharing discussions
- [misp-cloud Room](#) Using MISP in the clouds discussions

#### What are the hardware requirements?

From a hardware perspective, MISP's requirements are quite humble, a web server with 2+ cores and 8-16 GB of memory should be plenty, though more is always better of course. A lot of it depends on the data set and the number of users you are dealing with.

We recommend a standard LAMP stack on top of Ubuntu >18.04 LTS. For details on the exact dependencies please refer to the [installation guide](#) as well as the [requirements for the MISP modules](#).

During a [Hackathon](#) a small tool called **MISP-Sizer** was conceived. It will give you a **very rough** idea on what requirements are if you have a bigger installation. [source-code is here](#)

## How to monitor MISP?

Currently there are 2 documented ways to monitor MISP.

Either with [MUNIN](#) -> [misp-monitor](#) for instructions. Or [OpenNMS](#) -> [Instructions here](#)

## Specific questions

### Can I configure MISP encrypted notification emails to contain more information in the subject?

The setting 'MISP.extended\_alert\_subject' allows you to have an extended subject. ! Beware if you're using encryption: the subject will not be encrypted. Be aware that you might leak some sensitive information this way. Below is an example how the two subject types look like. First with the option disabled, then with the option enabled.

```
Event 7 - Low - TLP Amber
Event 8 - OSINT - Dissecting XXX... - Low - TLP Amber
```

(Source: [Getting started with MISP](#))

### How can I restart the workers?

The workers can be restarted from the web interface:

```
administration -> server settings -> workers -> restart all
```

You can also follow the manual process below.

If you are on Ubuntu / Debian based systems:

```
sudo su -l www-data -s /bin/bash -c "bash /var/www/MISP/app/Console/worker/start.sh"
```

If you are on RHEL / Fedora based systems:

```
su -s /bin/bash apache -c 'bash /var/www/MISP/app/Console/worker/start.sh'
```

### How can I redirect HTTP to HTTPS?

```
<VirtualHost *:80>
    ServerAdmin misp@misp.misp
    ServerName misp.misp.misp
    ServerAlias misp-int.misp.misp

    Redirect permanent / https://misp.misp.misp

    LogLevel warn
    ErrorLog /var/log/apache2/misp.local_error.log
    CustomLog /var/log/apache2/misp.local_access.log combined
    ServerSignature Off
</VirtualHost>
```

```

<VirtualHost *:443>
    ServerAdmin misp@misp.misp
    ServerName misp.misp.misp
    ServerAlias misp-int.misp.misp

    DocumentRoot /var/www/MISP/app/webroot
    <Directory /var/www/MISP/app/webroot>
        Options -Indexes
        AllowOverride all
        Order allow,deny
        allow from all
    </Directory>

    SSLEngine On
    SSLCertificateFile /etc/ssl/misp.misp.misp/misp.crt
    SSLCertificateKeyFile /etc/ssl/misp.misp.misp/misp.key
    SSLCertificateChainFile /etc/ssl/misp.misp.misp/mispCA.crt

    LogLevel warn
    ErrorLog /var/log/apache2/misp.local_error.log
    CustomLog /var/log/apache2/misp.local_access.log combined
    ServerSignature Off
</VirtualHost>

```

Source: [Getting started with MISP](#)

## When I try to access my new installation, I am redirected to localhost:8443 and get an error.

By default, MISP runs on a local instance and is setup for local access upon installation. This allows you to setup security and customizations before making it available elsewhere. If you would like to access the [MISP instance](#) from a remote host (including another VM host/client), assign an IP to the MISP host and point your browser accordingly. Upon login, you may get the “localhost:8443” redirection. Change that piece of the URL back to the IP assigned to the MISP host (or associated DNS name) and refresh the browser. Once in, go to Administration - Server Settings and Maintenance - MISP settings. You can change the top two items to your MISP IP or DNS name and the redirect will start using that address instead of ‘localhost’.

## How can I define the default sharing level?

MISP allows you to define the group of people with whom you want to share your threat data. If you do not set it to your preferred default then it’s likely that at one given moment you’ll make an error and share your intel with the wrong group. Defining the sharing level is done with the setting `default_event_distribution` in the configuration file. There are three levels:

```

0 : Your organisation only (default)
1 : This community only
2 : Connected communities
3 : All communities

```

You can set a similar configuration setting for the attributes. The setting `default_attribute_distribution` has the same values as `default_event_distribution`. Additionally it has the value `event` which allows the attribute to get the setting from the event to which it belongs.

Source: [Getting started with MISP](#)

## How can I add an organisation logo and/or footer logo?

MISP can be made more appealing to the eye by adding some graphics.

As Org.- or Site-admin navigate to *Administration -> List organisations* and edit the corresponding organization. Within this editor you will be able to update the logo.

Other ways to achieve this, would be:

Set your organisation logo by adding an image (.png) that has the same name as your organisation in the directory `/var/www/MISP/app/webroot/img/orgs/`.

Yet another way of doing this is by logging into your [MISP instance](#) with Admin rights, navigate to *Administration -> Server Settings*, tab -> *Manage files*.

You can add a footer logo. Add an image to the directory `/var/www/MISP/app/webroot/img/custom/` and define the footer logo in the config file (config.php) or in *Administration -> Server Settings... -> MISP settings* (search for: "footer\_logo") point to the location on-disk of the image.

Partial source: [Getting started with MISP](#)

## All workers are starting correctly except schdlr . How can I fix this?

This can happen if the [FQDN](#) of the server hosting the instance has changed. A way to fix this is to flush temporary data stored in redis. This can be done by logging in redis, for example when logging in with redis-cli, and issuing a `flushall` command.

## How can I import data directly from PDF reports?

!\\ This section needs review, verification and eventual amendments to make sure it works.

You can use a generic script called [IOC parser](#) ([https://github.com/armbues/ioc\\_parser](https://github.com/armbues/ioc_parser)) or use a script published by Palo Alto to convert [IOC](#) parser output to a [MISP event](#) ([https://github.com/PaloAltoNetworks-BD/report\\_to\\_misp](https://github.com/PaloAltoNetworks-BD/report_to_misp)). You have also the option to select all the text and paste it in the free-text import form.

Another option is the new [OCR import module](#) that can be used via the import modules. You will need to install the OCR software tesseract.

## I am having trouble updating beyond version 2.4.50 (stuck loading any page beyond the login), what can I do?

!\\ This applies to an earlier version of MISP, do not randomly try this fix on valuable data. By all means try it on a test-machine and report back if your problem was solved by this.

This is most likely due to the fact that MISP did not clean up expired sessions prior to version 2.4.51 automatically and relied on a site-admin occasionally cleaning it up using the button found on the diagnostics page. Once you upgrade to 2.4.51, MISP will try to cull the table with each page load by a site-admin, which in some cases if the table has grown to extreme sizes it will get stuck on. To resolve the issue, log into mysql:

```
mysql -u [misp-db-user-name] -p [misp-db-name];
```

and execute the following commands:

```
DROP cake_sessions; CREATE TABLE IF NOT EXISTS cake_sessions ( id varchar(255) COLLATE utf8_bin NOT NULL DEFAULT "", data text COLLATE utf8_bin NOT NULL, expires int(11) NOT NULL, PRIMARY KEY ( id ), INDEX expires ( expires ) ) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
```

After this everything should work and the session table will be trimmed each time a site-admin loads a page.

## I have many failed jobs when doing email notification. What should I do?

This is most probably due to some encryption failing for some users. We strongly advise to review the current PGP keys and to ensure that they keys are not expired or perhaps not supported anymore (weak keys). The keys can be reviewed at the following location in MISP:

```
https://<YOUR MISP URL>/users/verifyGPG
```

## Upgrading from MISP 2.4.65 to MISP 2.4.66 - Unable to merge due to the Composer file.

In MISP 2.4.66, Composer is included by default to avoid the risk of downloading a rogue PHP Composer version (if the composer repository is compromised or MiTM are performed) via the download and php execution. But when upgrading (via a git pull), the git merge process might complain about the composer phar file still being there. You can safely remove that file and `git pull origin 2.4` again.

## I have issues with pushing events

- What does the 'Connection test' for the specific server report? (*Sync Actions -> List Servers*)
- Is the event you assume to `push/pull` ready to be published?
- Is the distribution level set not too restrictive?
- Have you enabled `push` in the servers config you want to `push` to?
- Do you have any limitations to the `push` rules e.g. limited to a certain TLP Level tag or other?
- What is written in your job log?

```
https://jobs/index
```

Have a look at: /var/www/MISP/app/tmp/logs and /var/log/apache2/misp (or the relevant apache log folder of the instance in cause)

## I have many users or API accesses, what's the best PHP session handler?

We strongly recommend production-level MISP installations to rely on PHP session in Redis. As Redis is already part of a standard MISP setup, we recommend to enable the redis session handling.

To configure the redis session handling in PHP, edit :

```
session.save_handler = redis
session.save_path = "tcp://127.0.0.1:6379"
```

## Is there TAXII support?

A TAXII 1 implementation can be found at <https://github.com/MISP/MISP-Taxii-Server>. This is mostly a TAXII server hooked up to MISP, meant to receive STIX files to its inbox and uploading them to MISP. There is also an experimental feature to `push` MISP events to the TAXII server when they're published - that's in `scripts/push_published_to_taxii.py`. It seems to work, but may occasionally re-upload duplicate events to MISP.

TAXII 2 is provided in the future once the specification, which is at time of writing in draft, reaches a stable form.

## Wipe MISP data - Remove all data

If you need to start from scratch with your MISP database and remove all data you can use the `misp-wipe` script provided in the `tools/` folder.

## Constantly acknowledging my self-signed certificate drives me nuts

You want to add it in 2 places: Your browser(s) and your OS.

The following steps can be performed on the CLI to install the Certificate:

```
sudo mkdir -m 0755 /usr/local/share/ca-certificates/MISP
sudo cp /etc/ssl/private/misp.local.crt /usr/local/share/ca-certificates/MISP
sudo chmod 0644 /usr/local/share/ca-certificates/MISP/misp.local.crt
sudo update-ca-certificates
```

For the Chrome Browser:

1. Visit: "Advanced Settings" -> chrome://settings/?search=Manage+certificates
2. Scroll down to: Manage Certificates (click)
3. Select: "Authorities"
4. Click: "Import"
5. Browse to your .crt file and import it.
6. On the next screen tick: "Trust this certificate for identifying websites"
7. Done, enjoy the new gained quality of life

Note: Chrome might expect a **Subject Alternative Name** make sure you created your certificate with '-extension san'.

To allow insecure localhost connections enable this option: chrome://flags/#allow-insecure-localhost

Sources: [CLI](#) and [Chrome/Chrome insecure localhost](#)

For the Firefox Browser

## How can I change the theme?

MISP uses `bootstrap.css` the specific CSS file can be found on a typical MISP install at

```
/var/www/MISP/app/webroot/css/bootstrap.css .
```

You can customize this for your own needs. There are also pre-made bootstrap themes which you can use as-is or build upon.

Before making any changes, confirm the version of bootstrap currently used by running `head -5 /var/www/MISP/app/webroot/css/bootstrap.css .` You can find themes on sites like [Bootswatch](#).

To replace the current theme with a theme you found on bootsplash, run: `wget`

```
https://bootswatch.com/2/readable/bootstrap.css -O /var/www/MISP/app/webroot/css/bootstrap.css , replacing the URL as needed.
```

Some bootswatch themes applied on MISP:

- <https://i.imgur.com/usONTLk.png>
- <https://i.imgur.com/5XMjB7o.png>
- <https://i.imgur.com/5gc57VU.png>
- <https://i.imgur.com/4AJCPgf.png>
- <https://i.imgur.com/JuMGm8U.png>
- <https://i.imgur.com/v1Wu6xW.png>

## How can I deal with a MISP instance that has pulled in feeds over and over into new events, generating hundreds of GBs of junk correlations, rendering the instance unusable?

*Step 1:* ensure that all your CSV/freetext source\_format feeds are using the fixed event setting. If you want to make sure this is the case, you can run this SQL query instead of doing it manually:

```
UPDATE feeds SET fixed_event = 1 WHERE source_format="csv" OR source_format="freetext";
```

*Step 2:* purge all of your correlations (this will make the next steps much faster), for which you have two methods at your disposal:

- either go to your administration -> server settings -> MISP tab and set `MISP.completely_disable_correlation` to true
- via MySQL run `TRUNCATE correlations;`

*Step 3:* purge all of your feed data that have been pulled into multiple events. The easiest way of doing this: check which feeds are enabled (ignore misp source format feeds, they are not causing issues) and note down the IDs. Afterwards, use the CLI cleanup tool to remove all the feed events:

```
/var/www/MISP/app/Console/cake Admin purgeFeedEvents [user_id] [feed_id]
```

Execute this for each feed that you had enabled, replacing `user_id` with your admin user's ID and `feed_id` with the individual feed IDs on your list.

*Step 4:* recorrelate your data, depending on which method you've used in *Step 2* you have two options:

- either go to your *Administration -> Server Settings... -> MISP...* tab and set `MISP.completely_disable_correlation` to *false*
- recorrelate your current data-set via the recorrelate attributes tool on `/pages/display/administration`

## I have a long list of events that I want to delete via the API, do I really have to loop through each and issue a delete to /events/delete?

No, the delete action also accepts a list of IDs when it comes to bulk event deletions.

Simply POST your ID list to `/events/delete` in the following format:

```
{
  "id": [1,3,5,7,9]
}
```

## I can no longer log in. How do I reset the admin password?

You can reset the password via the console. See [Issue #1160](#)

```
/var/www/MISP/app/Console/cake Password [email] [password]
```

## Usage questions

### How can I see all the deleted events in a MISP instance?

You can use the logging system for this, to see all deleted events, simply go to *Audit -> Search Logs* and use the following parameters:

```
model: Event
```

```
action: delete
```

This will list all event deletions. To find out more about what a particular deleted event was, simply grab the ID from the above search results and search for:

```
model: Event
action: add
model_id: <Event ID retrieved from the listing of all event deletions>
```

To do the same via the [API](#), first search for the deletions:

```
POST request:
url: https://url.of.your.misp/logs/index
headers:
  Authorization: <your_api_key>
  Accept: application/json
  Content-type: application/json
Body:
{
  "model": "Event",
  "action": "delete"
}
```

Then find the individual event's metadata that was deleted

```
POST request:
url: https://url.of.your.misp/logs/index
headers:
  Authorization: <your_api_key>
  Accept: application/json
  Content-type: application/json
Body:
{
  "model": "Event",
  "action": "add",
  "model_id": "<Event ID retrieved from the query before>"
}
```

## Permission issues

If you have any permission issues, please [set the permissions](#) to something sane first.

### RHEL/CentOS

There are a plethora of issues that might arise when using SELinux when it comes to permissions. First, please familiarize yourself with [the basics](#) of SELinux. RedHat has a comprehensive [SELINUX USER'S AND ADMINISTRATOR'S GUIDE](#).

For file system permissions, refer to the [install guide](#) first.

Another way to see what SELinux might not be happy about is to use **ausearch**. This assumes Audit is enabled.

```
# Just php-fpm
sudo ausearch -c 'php-fpm' --message AVC
# All messages
sudo ausearch --message AVC
```

## Redis Connection problems

If you have the following in **error.log**

```
2019-05-08 10:16:05 Error: [RedisException] Permission denied
Request URL: /events/view/1
Stack Trace:
#0 /var/www/MISP/app/Model/AppModel.php(1776): Redis->connect('127.0.0.1', 6379)
#1 /var/www/MISP/app/Model/Feed.php(329): AppModel->setupRedis()
#2 /var/www/MISP/app/Model/Event.php(2073): Feed->attachFeedCorrelations(Array, Array, Array, false)
#3 /var/www/MISP/app/Controller/EventsController.php(1547): Event->fetchEvent(Array, Array)
#4 [internal function]: EventsController->view('1')
#5 /var/www/MISP/app/Lib/cakephp/lib/Cake/Controller/Controller.php(499): ReflectionMethod->invokeArgs(Object(EventController), Array)
#6 /var/www/MISP/app/Lib/cakephp/lib/Cake/Routing/Dispatcher.php(193): Controller->invokeAction(Object(CakeRequest))
#7 /var/www/MISP/app/Lib/cakephp/lib/Cake/Routing/Dispatcher.php(167): Dispatcher->_invoke(Object(EventController), Object(CakeRequest))
#8 /var/www/MISP/app/webroot/index.php(92): Dispatcher->dispatch(Object(CakeRequest), Object(CakeResponse))
#9 {main}
```

This means that apache/php-fpm cannot connect over the network (localhost included).

Fix:

```
sudo setsebool -P httpd_can_network_connect on
# Perhaps a reload is not needed, but good practice wants us to test it anyways.
sudo systemctl restart rh-php72-php-fpm.service
sudo systemctl restart httpd.service
```

## RHEL/CentOS SELinux debug

More often than not there might be issues with SELinux when not configured correctly. The below will give you pointers where to look and how to figure out what is wrong.

You can investigate SELinux issues without any tools by opening the audit log it generates. This log is found at `/var/log/audit/audit.log`. However, unless you know exactly what to look for and have a lot of free time, you're going to find it difficult making sense of the log.

Install some handy tools:

```
# Note: This will pull in some X tools, you have been warned
sudo yum install setroubleshoot setools
```

We now have a tool called sealert that analyzes the audit log used by SELinux. Sealert will scan the log file and will then generate a report containing all discovered SELinux issues. In this overview of what went wrong you will see suggestions on how to fix them after the issue detected.

To run sealert from the command-line, we need to point it to the SELinux audit log.

```
sudo sealert -a /var/log/audit/audit.log
```

## Clearing the audit logs

It is not recommended to clear the audit logs as they might contain information needed in the future for troubleshooting or security investigations. However, if that is not the case, just empty the audit log:

```
# > /var/log/audit/audit.log
```

[Partial source](#)

[StackExchange](#)

[Gentoo Wiki](#)

## When to update MISP?

One question might be how often to update MISP. You can update MISP as often as you like. If you see the following:

### MISP version

Every version of MISP includes a json file with the current version. This is checked against the latest tag on github, if there is a version mismatch the tool will warn you about it. Make sure that you update MISP regularly.

Currently installed version... [v2.4.97 \(4462a72206a9cce39559c1facee90efdec2a308d\)](#)

Latest available version... [v2.4.97 \(6e9b6fb80382346f338aa94f37b52d326b7cc551\)](#)

Status... [OK](#)

Current branch... [2.4](#)

[Update MISP](#)

This means that the main repository has an update available.

If you want to play it safer or want to integrate it in your Weekly/Bi-Monthly update routine you can track our [Changelog](#) a more up to date version is available [here](#)

Further on we do regular tagged releases. (Approximately once per month.) The releases happen either if a milestone has been hit for a certain feature/improvement/fix or for any security related matters.

Thus you have the choice of either tracking 2.4 which is on a rolling release schedule, or track the tagged releases.

## How to switch from tagged releases and back?

This can be achieved with the following git commands:

```
$ cd /var/www/MISP # aka. $PATH_TO_MISP
$ sudo -H -u www-data git checkout tags/$(git describe --tags `git rev-list --tags --max-count=1`)

## OS Upgrades

In theory all should "just work"(tm), but in practice the following dependencies might make your install unstable and need a little though before just doing the updates.

* php/pear
* python
* apache
* init scheme/scripts
* mariadb/mysql
* redis
* git

### PHP

This is probably the most likely one that might get you into trouble.
The following happened on a Debian Testing lately. During the upgrade php got upgraded to php-7.3 and seemingly some php-7.2 dependencies were deinstalled and the system now had 2 concurrent versions of php installed.
The fix was to remove any *libapache2-mod-php7.2* packages and make sure that *apt remove libapache2-mod-php7.3* was installed. Most certainly you need to add symbolic links to */etc/apache2/mods-enabled* to make php7.3 work.
Then double check if all the php dependencies are install, refer to the install documents.

The same for pear, where we mostly use 2 (bundled) packages: Console Command Line, Crypt GPG.
If you upgrade from a very old and out of date version of MISP this might raise issues.

php.ini might also become problematic if you just erase the recommended defaults.

### Python3

If you use python2 for MISP, please read the install docs about MISP being Python 3 only.
Currently Python3.6 is minimum. It is known working on 3.7 with some minor difficulties (see PyMISP issues).
The biggest issue is certainly with PyMISP doing unexpected things when python might be updated.
Using a virtualenv, whilst not always ideal for all setups, will at least make sure that problems are contained a little more.

### Apache

Mostly config issues might be a show stopper. And major version updates where some underlying config might need to be changed.

### init/systemd

MISP launches a couple of things on boot. Changing what handles boot behavious might have an impact.

### MariaDB/MySQL/redis

Similar to apache, most importantly always take good care that the DB engine is not all of a sudden changed wit
```

```

hout you noticing it.
From minor to major updates, rarely things might need to be adapted.

### git

Currently (as of v2.4.108) the git-cli command is used in MISP core. In very rare cases where the expected output changes, this might be an issue.
Included here more as an FYI then anything else.

## Hardening

### How do I harden my MISP instance?

You can check the [hardening section](https://misp.github.io/MISP/generic/hardening/) in the install guide.

## Maintenance mode

### Is there a MISP maintenance mode?

Yes, you want to flip your instances "Live-mode".
This wants to be done on the CLI if you experience issues:

```bash
$PATH_TO_MISP/app/Console/cake "MISP.live" 0
```

```

#### Other related MISP Settings

Optional MISP.maintenance\_message Great things are happening! MISP is undergoing maintenance, but will return shortly. You can contact the administration at \$email or call CIRCL. The message that users will see if the instance is not live.

Critical MISP.live true Unless set to true, the instance will only be accessible by site-admins.

## Update MISP fails

If your MISP instance is outdated, meaning ONLY the core, not the modules or dashboard or python modules, you well see the following.

### MISP version

Every version of MISP includes a json file with the current version. This is checked against the latest tag on github, if there is a version mismatch the tool will warn you about it. Make sure that you update MISP regularly.

Currently installed version... v2.4.96 (f3850747da103ca616a7dbaab955df373db272f7)

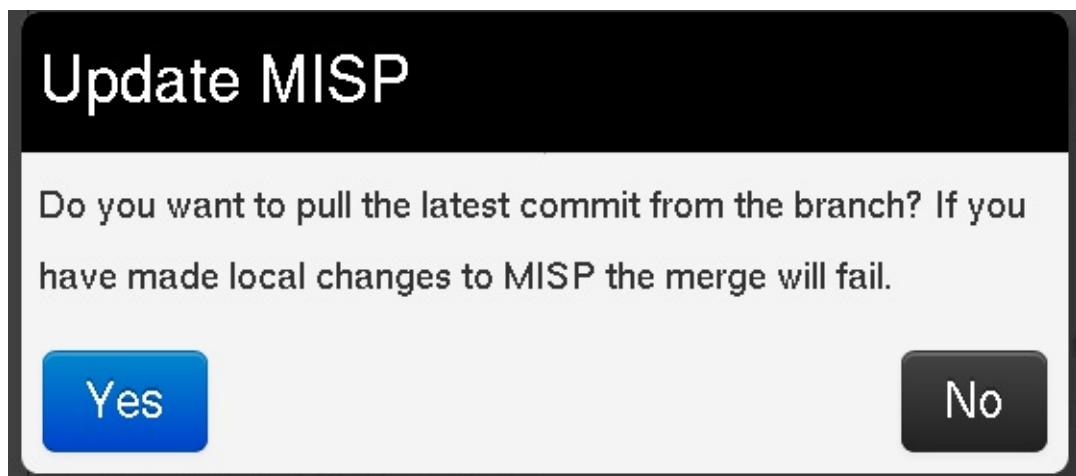
Latest available version... v2.4.97 (ce3c78cd7db60812d0147ced992a7650509d31da)

Status... Outdated version

Current branch... 2.4

**Update MISP**

Once you click on update MISP you will be asked confirmation.



If you are not on a branch, the UI will tell you this, the update will fail.

Currently installed version... v2.4.96 (bbc8a8bf4dce4d64fb676a3a76bb4c6be091e890)

Latest available version... v2.4.97 (ce3c78cd7db60812d0147ced992a7650509d31da)

Status... **Outdated version**

Current branch... **You are not on a branch, Update MISP will fail**

```
git checkout app/composer.json 2>&1
```

```
error: pathspec 'app/composer.json' did not match any file(s) known to git
```

```
git pull origin 2>&1
```

```
error: pathspec 'app/composer.json' did not match any file(s) known to git
```

```
You are not currently on a branch.
```

```
Please specify which branch you want to merge with.
```

```
See git-pull(1) for details.
```

```
git pull <remote> <branch>
```

```
=====
```

```
git submodule update --init --recursive 2>&1
```

**Update MISP**

If you cannot write the `.git` files and directory as the user running the web server (and thus PHP), the update will fail. The following diagnostic check will let you know if you can update or not.

## Writable Files

```
/var/www/MISP-priv/app/Config/config.php...OK  
/var/www/MISP-priv/.git/ORIG_HEAD...File is not writeable
```

In case you get a file not found on **.git/ORIG\_HEAD**, this means that you have never updated your MISP OR you have installed git from an archive file (like .zip/.tar.gz or similar) Try to click update MISP and see what happens.

## Writable Files

/var/www/MISP/app/Config/config.php...OK

/var/www/MISP/.git/ORIG\_HEAD...File not found

## What can go wrong if I update MISP?

In theory nothing. We put great effort into protecting the integrity of the data stored in your [MISP instance](#). DB upgrades happen upon login or on reload once you have update the repository. You cannot "break" anything by clicking **Update MISP** worse case it will complain about something and you will certainly find the answer on this page.

If not, please open an [issue](#) on GitHub or come to our [gitter](#) chat to see if the community can help.

### **error: pathspec 'app/composer.json' did not match any file(s) known to git**

This is **not** an error and can be ignore. Nothing will be impacted by this.

```
Currently installed version... v2.4.96 (f3850747da103ca616a7dbaab955df373db272f7)
Latest available version... v2.4.97 (ce3c78cd7db60812d0147ced992a7650509d31da)
Status... Outdated version
Current branch... 2.4

git checkout app/composer.json 2>&1

error: pathspec 'app/composer.json' did not match any file(s) known to git

git pull origin 2.4 2>&1

error: pathspec 'app/composer.json' did not match any file(s) known to git
From https://github.com/MISP/MISP
 * branch            2.4      -> FETCH_HEAD
   f3850747d..ce3c78cd7  2.4      -> origin/2.4
Updating f3850747d..ce3c78cd7
Fast-forward
 VERSION.json                  |  2 ++
 app/Controller/AppController.php |  2 ++
 app/Controller/Component/ACLComponent.php |  1 +
 app/Controller/Component/RestResponseComponent.php | 16 ++
 app/Controller/EventsController.php |  2 ++
 app/Controller/SightingsController.php | 36 ++++++
 app/Lib/Export/CsvExport.php | 28 +++++
 app/Lib/Export/JsonExport.php |  9 +-
```

## MISP modules "Connection refused"

### Module System

This tool tests the various module systems and whether they are reachable based on the module settings.

Enrichment module system... **Connection refused**

Import module system... **Connection refused**

Export module system... **Connection refused**

Cortex module system... **System not enabled**

If you get have a **Connection refused state** on your modules one of the following might be true.

- You have no `misp-modules` not installed
- They are instaled but not running
- Something completly different

If they are not installed, check out this section of the [INSTALL guide of misp-modules](#).

In case they are not running, try this on the console:

```
sudo -u www-data /var/www/MISP/venv/bin/misp-modules -l 127.0.0.1 -s &
```

OR if you were foolish enough to not install in a Python virtualenv:

```
sudo -u www-data misp-modules -l 127.0.0.1 -s &
```

[warning] Running misp-modules like this will certainly kill it once you quit the session. Make sure it is in your `/etc/rc.local` or some ther init script that gets run on boot.

## Uninstalling MISP

There is no official procedure to uninstalling a [MISP instance](#).

If you want to re-use a machine where MISP was installed, wipe the machine and do a fresh install. Consider the data in your [MISP instance](#) as potentially confidential and if you synchronized with other instances, be respectful and wipe it clean.

## Updating PyMISP to incorporate newer versions of the MISP object templates

In some cases, for instance if a newer version of a MISP object is present on the server but not yet on PyMISP, you want to reflect the current state in your PyMISP installation.

In order to do so, perform the following steps. It fetches the latest object templates and installs PyMISP again:

```
git clone https://github.com/MISP/PyMISP.git
cd PyMISP/pymisp/data
git submodule update --init
cd misp-objects
git pull origin master
cd ../../..
sudo pip3 install -I .
```

## How to disable freetext/custom/user-created tags and only allow certain tags

Remove the "tag editor" from the permissions that you grant to users. Set all tags that you do not want to "hidden". There is a server setting to treat all incoming tags as hidden by default: `MISP.incoming_tags_disabled_by_default`

**Important** Make sure that you don't remove "tag editor" from sync users, or you'll be stripping tags from synchronized data.

## How to enable the csv import module?

First you have to enable the import services: double-click on "false" in the very first line and change it to "true".

In Server Settings & Maintenance -> Plugin Settings -> Import -> set "Plugin.Import\_csvimport\_enabled" to true. Afterwards you'll find the csvimport from within the newly created event: "Populate from..."

Don't use from the main site ("Import from...").

## Why do I see 'The request has been black-holed' when I submit forms?

That's a security measure for form tampering protection.

All forms have a timeout (~15min) and all of them can only be submitted once. If you use your browser's "back" button and resubmit the form MISP will consider it as a potential attempt at form tampering.

## Importing large feeds creates PHP Fatal error

When importing a large feed like the CIRCL feed, the job reaches 99% and then fails. The log file records:

```
PHP Fatal error: Allowed memory size of 536870912 bytes exhausted (tried to allocate 1941504 bytes) in /var/www/MISP/app/Model/Feed.php on line 691
```

In this case you will need to increase the memory\_limit option in `php.ini` file

## I deleted the admin user by mistake

Now, I only have [Org Admin](#).

You have several options:

1. Delete the [org admin](#). MISP automatically creates a new default site-admin user if no users are found in the db (mysql: truncate users;)
2. Upgrade a user to a site-admin, such as an [org admin](#) user:

```
SELECT id, email from users;
```

Note down the ID you want to upgrade. Let's say this is 2 for the example's sake.

```
SELECT id, name from roles;
```

Note down the role ID you want to upgrade. Let's say this is 1 for the example's sake.

```
UPDATE users set role_id = 1 where id = 2;
```

## config.php is not writeable

```
Warning: app/Config/config.php is not writeable. This means that any setting changes made here will NOT be saved.
```

According to the install guide, make sure to:

```
chown -R apache:apache /var/www/MISP
find /var/www/MISP -type d -exec chmod g=rx {} \;
chmod -R g+r,o= /var/www/MISP
```

If it still doesn't work, make sure SELinux is not enabled or modify the rule set:

```
chcon -t httpd_sys_rw_content_t /var/www/MISP/app/files
chcon -t httpd_sys_rw_content_t /var/www/MISP/app/files/terms
chcon -t httpd_sys_rw_content_t /var/www/MISP/app/files/scripts/tmp
chcon -t httpd_sys_rw_content_t /var/www/MISP/app/Plugin/CakeResque/tmp
chcon -R -t httpd_sys_rw_content_t /var/www/MISP/app/tmp
chcon -R -t httpd_sys_rw_content_t /var/www/MISP/app/webroot/img/orgs
chcon -R -t httpd_sys_rw_content_t /var/www/MISP/app/webroot/img/custom
```

## How to debug misp-dashboard

This is the full chain from MISP to the live dashboard and some tips to find out which link is faulty.

1. MISP Ensure that ZMQ is installed and enabled with the correct settings
2. MISP ZMQ You can use MISP/tools/misp-zmq/sub.py which will subscribe to the ZMQ and print the data
3. ZMQ\_subscriber You can change the logging level from logging.INFO to logging.DEBUG and look in the logs for the string Pushed: \* Or add a print statement in the put\_in\_redis\_list function
4. ZMQ\_dispatcher Look in the logs for the string Handling \*
5. Server (Flask) and Browser (live Dashboard) Open the Web developer Network tab in your browser and look for the url /\_logs with Content-Type: text/event-stream;

## How to update object templates?

```
git submodule update
```

in your MISP directory (or via the diagnostic page) and just click "Update Objects" in List Object Templates.

## What to do if my REST client is throwing SSL errors when trying to query my MISP instance?

The REST client will use the framework's certificate store to validate the contacted host. If your root CA / self-signed certificate is not known by the certificate store, the request will fail. You can skip the SSL validation altogether using the "Skip SSL validation" checkbox.

## What to do if my REST client cannot reach the host, despite me being able to issue requests using Curl / Postman / etc.?

The REST client issues instructions to your MISP server to contact a remote host (most commonly itself). Always consider how your MISP server can address itself when using the REST client, by default it will prepend the requested relative path in the URL field with the instance's baseurl.

If your MISP cannot reach itself via the baseurl the request will fail. You can use the "Use full path - disclose my API key" checkbox along with the full URL in the URL field to instruct MISP to use another path than what it would construct using the baseurl.

## **How would one set up a sharing group with a remote org, where we only share a mutual community instance (i.e. we both have sync users on that instance). On our local instance, they exist as a remote org (from events that have synced from their instance via our shared community instance).**

It is not possible to do that. Keep in mind that if you are both on a mutual community instance, someone is in charge of that instance that will have database and admin level access. They would be able to inspect the data you exchange on their community instance with one another, so MISP will block any attempt to share with them.

If you really want to go through the community instance to exchange with them, you explicitly have to include the host organisation of the community instance (they would get access if they wanted to anyway, this way we can ensure that you are clear about that):

- You are org a on instance A.
- Your partner that you want to share with is org b on instance B.
- You have no way of directly reaching org b, but you both have access to instance C, which is run by org c (the sharing instance)
- In order to reach org b, you have two options for [sharing groups](#), depending on whether you want to be able to [push](#) to them or want to rely on them pulling data from the community instance:

```
SG Option 1 (push all the way to B)
orgs: a, b, c
instances: A, B, C
```

```
SG Option 2 (b has to pull from C):
orgs: a, b, c
instances: A, C
```

## **Is it possible to propose objects to an event?**

This is not possible yet. What you can do at the moment: Create a new event and extend it with the other (foreign) event.

## **How to use the enforceWarninglist parameter in REST search?**

If you would like to export IoCs, for example into a suricata rule and exclude all values matching your warning lists, you can use the following:

```
{
  "returnFormat": "suricata",
  "published": 0,
  "enforceWarninglist": 1
}
```

Keep in mind that unpublished events need the `"published": 0` parameter in order to be exported.

## Column not found issue

When a user attempts to add an object to an event and the following error is received (Level 1 debug enabled):

```
SQLSTATE[42S22]: Column not found: 1054 Unknown column 'Event.org_id' in 'where clause'
```

One potential resolution is to upgrade MISP to 2.4.107.

### Symptoms

Users with the site-admin role are able to add objects to events without any error. This error was encountered when a user belonged to every role **except** site-admin.

## WatchList Customization

### How to create a customized WatchList.

WatchLists are stored within folder under /var/www/MISP/app/files/warninglists/lists Every folder contains a list.json file. Create a new folder and copy and modify an existing list (or create a new one from scratch). Ensure the "name" value within the file is unique. Increment the version number when the file is changed.

Within the MISP GUI, go to WarningLists and "Update WarningLists".

The new WarningList will now show up. In case of errors, check the permissions on the list.json and it's folder.

To modify the list or to add entries to it, go back to the file via the CLI, modify the file and reload it via the GUI ("Update WarningLists").

## How to upgrade PHP on RHEL/CentOS?

To our knowledge, there is no way to "upgrade" PHP. You'll need to install the new PHP version like you're doing a fresh install. You may try copying your old `php.ini` to your new PHP config directory which may work. We would recommend redoing the config though.

### Example: Upgrade from PHP 7.2 to 7.3 on CentOS 7

#### Enable repository

```
$ sudo yum install -y http://rpms.remirepo.net/enterprise/remi-release-7.rpm
$ sudo yum-config-manager --enable remi-php73
```

#### Install packages

```
$ sudo yum install -y php73-php php73-php-cli php73-php-fpm php73-php-devel php73-php-mysqlnd php73-php-mbstring
g php73-php-xml php73-php-bcmath php73-php-opcache php73-php-gd php73-php-pecl-redis4 php73-php-pecl-gnupg php7
3-php-pear
```

Confirm GPG key if required:

```
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-remi
Importing GPG key 0x00F97F56:
Userid      : "Remi Collet <RPMS@FamilleCollet.com>"
Fingerprint: 1ee0 4cce 88a4 ae4a a29a 5df5 004e 6f47 00f9 7f56
```

```
Package      : remi-release-7.6-2.el7.remi.noarch (installed)
From        : /etc/pki/rpm-gpg/RPM-GPG-KEY-remi
Is this ok [y/N]: y
```

## Install required PEAR-modules

```
$ sudo php73-pear channel-update pear.php.net
Updating channel "pear.php.net"
Update of Channel "pear.php.net" succeeded
$ sudo php73-pear install /var/www/MISP/INSTALL/dependencies/Console_CommandLine/package.xml
install ok: channel://pear.php.net/Console_CommandLine-1.2.2
$ sudo php73-pear install /var/www/MISP/INSTALL/dependencies/Crypt_GPG/package.xml
install ok: channel://pear.php.net/Crypt_GPG-1.6.3
```

## PHP configuration

Edit `/etc/opt/remi/php73/php.ini`:

```
date.timezone = "Europe/Berlin"
max_execution_time = 300
memory_limit = 512M
upload_max_filesize = 50M
post_max_size = 50M
```

## Switch to PHP 7.3

```
$ sudo systemctl stop rh-php70-php-fpm
$ sudo systemctl start php73-php-fpm
# check if everything's fine
$ sudo systemctl status php73-php-fpm
```

Now check if the MISP web UI is accessible and if the diagnostics page shows any errors.

The diagnostics page will show "PHP CLI Version (>7.2 recommended): Unknown (Issues determining version)". That's a [known issue](#).

## Disable/enable services

```
$ sudo systemctl disable rh-php70-php-fpm
Removed symlink /etc/systemd/system/multi-user.target.wants/rh-php70-php-fpm.service.
$ sudo systemctl enable php73-php-fpm
Created symlink from /etc/systemd/system/multi-user.target.wants/php73-php-fpm.service to /usr/lib/systemd/system/php73-php-fpm.service.
```

## How to add a galaxy to an event via PyMISP

A galaxy can be assigned like a tag. You can use the add tag function and copy the full connector-tag. Example `misp-galaxy:ransomware="Locky"` , which can be found in `/galaxy_clusters/view/`

## Updating PHP from 7.2 to 7.4.5 on Ubuntu 18.04

### Installation

## 1. Disable and Uninstall Currently Installed SSDEEP

```
sudo phpdismod ssdeep
sudo pecl uninstall ssdeep
sudo apt purge ssdeep
sudo rm -rf /etc/php/7.2/mods-available/ssdeep.ini
```

## 2. Install PHP 7.4.5

```
sudo apt install software-properties-common -qy
sudo add-apt-repository ppa:ondrej/php -y
sudo apt update
sudo apt install -qy \
    libapache2-mod-php7.4 \
    php7.4 \
    php7.4-cli \
    php7.4-dev \
    php7.4-json \
    php7.4-xml \
    php7.4-mysql \
    php7.4-opcache \
    php7.4-readline \
    php7.4-mbstring \
    php-redis \
    php-gnupg \
    php-gd
sudo apt update
sudo apt upgrade -y
```

## 3. Install SSDEEP

```
cd /usr/local/src
sudo rm -rf ssdeep-2.14.1.tar.gz ssdeep-2.14.1
sudo wget https://github.com/ssdeep-project/ssdeep/releases/download/release-2.14.1/ssdeep-2.14.1.tar.gz
sudo tar zxvf ssdeep-2.14.1.tar.gz
cd ssdeep-2.14.1
sudo ./configure --datadir=/usr --prefix=/usr --localstatedir=/var --sysconfdir=/etc
sudo make
sudo make install
```

## 4. Test SSDEEP

```
ssdeep -h
```

## 5. Install ssdeep\_php

```
sudo pecl channel-update pecl.php.net
sudo pecl install ssdeep
```

## 6. Enable SSDEEP in both 7.2 and 7.4 ( as root sudo su )

```
echo 'extension=ssdeep.so' > /etc/php/7.2/mods-available/ssdeep.ini
echo 'extension=ssdeep.so' > /etc/php/7.4/mods-available/ssdeep.ini
```

## 7. Enable SSDEEP PHP Mod

```
sudo phpenmod ssdeep
```

8. Set PHP 7.4.5 to default PHP

```
sudo a2dismod php7.2
sudo a2enmod php7.4
sudo update-alternatives --set php /usr/bin/php7.4
```

9. [Optional] Set better values for defaults

```
sudo sed -i "s/max_execution_time = 30/max_execution_time = 300/" /etc/php/7.4/apache2/php.ini ; \
sudo sed -i "s/memory_limit = 128M/memory_limit = 2048M/" /etc/php/7.4/apache2/php.ini ; \
sudo sed -i "s/upload_max_filesize = 2M/upload_max_filesize = 500M/" /etc/php/7.4/apache2/php.ini ; \
sudo sed -i "s/post_max_size = 8M/post_max_size = 500M/" /etc/php/7.4/apache2/php.ini ; \
sudo sed -i "s/max_execution_time = 30/max_execution_time = 300/" /etc/php/7.4/cli/php.ini ; \
sudo sed -i "s/upload_max_filesize = 2M/upload_max_filesize = 500M/" /etc/php/7.4/cli/php.ini ; \
sudo sed -i "s/post_max_size = 8M/post_max_size = 5000M/" /etc/php/7.4/cli/php.ini ;
```

10. Restart Apache to implement changes

```
sudo sudo systemctl restart apache2
```

## Verification of php 7.2 to 7.4

1. Administration > Server Settings & Maintenance

2. Diagnostics

3. Scroll down to the **PHP Settings** section and verify

## What are the required steps after a MISP installation to have a properly running instance?

- First login with the installation credentials and change the password immediatly (especially if your instance is publicly accessible)
- Set the base\_url to the hostname of your machine (apache virtualhost name)
- Create a new organisation which will be the host organisation running the [MISP instance](#)
- Set the new organisation in `MISP.host_org_id` to replace the default one
- Set messages like `MISP.footermiddleleft` and alike to a proper message to help your users
- Create a new user as `admin` role with the new organisation
- Log with the new user, if successful, remove the default user used during the installation such as `admin@admin.test`
- Select and enable required taxonomies for your sharing community
- Select and enable the external feeds (as caching only if you don't want full events but you can get the full feeds too)
- Select and enable the warning-list (if you don't know what to enable, select all)
- Add the remote MISP instances where you have access to (either caching only or full [pull](#) if you want the complete events)

 Last modified: Sun Nov 18 2018 06:24:52 GMT+0100 (CET)

## Developer FAQ

### Main Developer Resources

The main developer resources can be found on GitHub in the [MISP Wiki](#).

The following pages are worth inspecting closer in case you want to actively develop for MISP:

- [The real FAQ](#)
- [Contributor Overview](#)
- [Some objectives of MISP](#)
- [Various deployment tools](#)
- [MISP Code of Conduct](#)
- [UI coloring scheme](#)
- [Notes on MISP and STIX 2](#)
- [Commit Messages Best Practices](#)
- [Internationalization \(i18n\)](#)

Our [gitter channel](#) is a welcome place to ask other community developers in case you are stuck.

Last modified: Wed Aug 19 2020 10:27:11 GMT+0200 (CEST)

## Summary

- [Appendix A: External Authentication](#)

- ~ [The external authentication mechanism described](#the-external-authentication-mechanism-described)
- ~ [Setting up the external authentication mechanism](#setting-up-the-external-authentication-mechanism)
- ~ [User management](#user-management)
- ~ [Logging](#logging)

- [Appendix B: ACL descriptors](#)

- ~ [Querying the ACL system](#querying-the-acl-system)
- ~ [Getting a list of URLs accessible to a role](#getting-a-list-of-urls-accessible-to-a-role)
- ~ [Getting a list of all accessible controllers and actions in MISP](#getting-a-list-of-all-accessible-controllers-and-actions-in-misp)
- ~ [Viewing a list of yet unmapped functions](#viewing-a-list-of-yet-unmapped-functions)

- [Appendix C: Official MISP developments](#)

- [Appendix D: Third-party development](#)

- [Appendix E: Other Threat Intel Ressources](#)

- [Appendix F: LDAP Authentication](#)

- ~ [Installation and configuration](#installation-and-configuration)
- ~ [Debugging](#debugging)
- ~ [Migrating existing user to LDAP](#migrating-existing-user-to-ldap)
- ~ [Caveats](#caveats)

## Appendix A: External Authentication

### The external authentication mechanism described

The external authentication allows a user or an external tool to authenticate with MISP using an arbitrary value passed along in a custom header. This authentication method overrides the regular authentication mechanisms and is customisable by a site-admin.

It is possible to create a mixed mode MISP setup where certain users can go through the normal authentication mechanism and other users are required to use the external authentication method.

### Setting up the external authentication mechanism

To change the authentication settings, navigate to Administration - Server settings - Plugin settings

The settings associated with the external authentication can be found by pressing the CustomAuth button as depicted below:

| ZeroMQ     |   |                            |  |
|------------|---|----------------------------|--|
| CustomAuth |   |                            |  |
| Priority   | Setting                                 | Value                      | Description  |
| Optional   | Plugin.CustomAuth_enable                | true                       | Enable this function to authenticate without a password.                 |
| Optional   | Plugin.CustomAuth_header                | radac_auth_header          | Set the header name for the authentication header.                       |
| Optional   | Plugin.CustomAuth_required              | false                      | If this setting is true, users will be required to provide a password.   |
| Optional   | Plugin.CustomAuth_only_allow_source     |                            | If you are using a proxy, set the source url as a valid proxy URL.       |
| Optional   | Plugin.CustomAuth_name                  | Radac                      | The name of the user creation page as defined in the configuration file. |
| Optional   | Plugin.CustomAuth_disable_logout        | true                       | Disable the logout link.   |
| Optional   | Plugin.CustomAuth_custom_password_reset | https://my/custom/pw/reset | Provide your custom URL for password reset.                              |
| Optional   | Plugin.CustomAuth_custom_logout         | https://my/custom/logout   | Provide a custom URL for the logout system you use.                      |

To change a setting simply double click on the value to edit the field. Use the guidance provided by the setting tool to configure the external authentication. The accessible settings are as follows:

- **enable**: Enable or disable external authentication (off by default)
- **header**: The header which MISP will use to identify users
- **required**: Enabling this setting will force all users to use the external authentication. Leave this disabled allows administrators to assign external authentication or regular authentication users.
- **only\_allow\_source**: Setting a url / IP address here will only allow requests that originated from the given address
- **name**: The name to be used for the authentication mechanism. This is reflected in the user creation / edit views, the logs and the error messages on failed logins.
- **disable\_logout**: Disable the default logout button. Using an external authentication mechanism that authenticates via the header with each request makes the logout button obsolete.
- **custom\_password\_reset**: If your authentication system has a url that a user can access to reset his/her password, please specify the full url for it here. This will then be reused in the UI.
- **custom\_password\_logout**: If your authentication system has a url that a user can access to logout, please specify the full url for it here. This will then be reused in the UI.

## User management

Using a new setting, user self management can be disabled for all users that are not administrators via the MISP.disableUserSelfManagement setting, found in the MISP settings tab. Enabling this setting removes the ability of users to change their user settings and reset their authentication keys. All other functionality remains unchanged.

## Email

 External authentication user Set password

## Organisation

 Choose organisation ▾

## Role

 Site Admin ▾

## Authkey

 DdeSGRSNBvSS9pbGEupf0d9ic

## Nids Sid

## Sync user for

 Not bound to a server ▾

## GPG key

**Fetch GPG key** Receive alerts when events are published Receive alerts from "contact reporter" requests Disable this user account**Submit**

To create an external authenticated user, simply tick the External authentication user checkbox, after which an external auth key field will appear. This will be used to identify the users via the passed along header.

## Logging

For a description of the logging facilities provided by this plugin, please refer to the "Logging of failed authentication attempts" section of the Administration section.

# Appendix B: ACL descriptors

## Querying the ACL system

MISP allows site admins to query the ACL system for various types of data. This can be interesting when tuning for example WAF access to MISP. All applicable queries can be requested via /servers/queryACL

### Getting a list of URLs accessible to a role

```
https://<misp url>/servers/queryACL/printRoleAccess/<role id>
```

The above URL will return a JSON with all accessible URLs for the given role ID. If no Role ID is provided, a JSON containing all [roles](#) and their access lists will be returned.

Example:

```
{  
  "2": {  
    "name": "User",  
    "urls": [  
      "/attributes/add/*",  
      "/attributes/add_attachment/*",  
      "/attributes/add_threatconnect/*",  
      "/attributes/attributeReplace/*",  
      "/attributes/delete/*",  
      "/attributes/deleteSelected/*",  
      "/attributes/download/*",  
      "/attributes/downloadAttachment/*",  
      "/attributes/downloadSample/*",  
      "/attributes/edit/*",  
      "/attributes/editField/*",  
      "/attributes/editSelected/*",  
      "/attributes/fetchEditForm/*",  
      "/attributes/fetchViewValue/*",  
      "/attributes/hoverEnrichment/*",  
      "/attributes/index/*",  
      "/attributes/restSearch/*",  
      "/attributes/returnAttributes/*",  
      "/attributes/rpz/*",  
      "/attributes/search/*",  
      "/attributes/searchAlternate/*",  
      "/attributes/text/*",  
      "/attributes/updateAttributeValues/*",  
      "/attributes/view/*",  
      "/eventDelegations/acceptDelegation/*",  
      "/eventDelegations/delegateEvent/*",  
      "/eventDelegations/deleteDelegation/*",  
      "/eventDelegations/view/*",  
      "/events/add/*",  
      "/events/addIOC/*",  
      "/events/addTag/*",  
      ...  
    ]  
  }  
}
```

```
"/events/add_misp_export/*",
"/events/contact/*",
"/events/csv/*",
"/events/delegation_index/*",
"/events/delete/*",
"/events/downloadExport/*",
"/events/downloadOpenIOCEvent/*",
"/events/downloadSearchResult/*",
"/events/edit/*",
"/events/export/*",
"/events/exportChoice/*",
"/events/filterEventIndex/*",
"/events/freeTextImport/*",
"/events/hids/*",
"/events/index/*",
"/events/nids/*",
"/events/proposalEventIndex/*",
"/events/queryEnrichment/*",
"/events/removePivot/*",
"/events/removeTag/*",
"/events/restSearch/*",
"/events/saveFreeText/*",
"/events/stix/*",
"/events/updateGraph/*",
"/events/view/*",
"/events/viewEventAttributes/*",
"/events/viewGraph/*",
"/events/xml/*",
"/jobs/cache/*",
"/jobs/getGenerateCorrelationProgress/*",
"/jobs/getProgress/*",
"/logs/event_index/*",
"/logs/maxDateActivity/*",
"/logs/returnDates/*",
"/organisations/fetchOrgsForSG/*",
"/organisations/fetchSGOrgRow/*",
"/organisations/index/*",
"/organisations/landingpage/*",
"/organisations/view/*",
"/pages/display/*",
"/posts/add/*",
"/posts/delete/*",
"/posts/edit/*",
"/regexp/index/*",
"/roles/index/*",
"/roles/view/*",
"/servers/fetchServersForSG/*",
"/shadowAttributes/accept/*",
"/shadowAttributes/acceptSelected/*",
"/shadowAttributes/add/*",
"/shadowAttributes/add_attachment/*",
"/shadowAttributes/delete/*",
"/shadowAttributes/discard/*",
"/shadowAttributes/discardSelected/*",
"/shadowAttributes/download/*",
"/shadowAttributes/edit/*",
"/shadowAttributes/editField/*",
"/shadowAttributes/fetchEditForm/*",
"/shadowAttributes/index/*",
"/shadowAttributes/view/*",
"/sharingGroups/index/*",
"/sharingGroups/view/*",
"/sightings/add/*",
"/sightings/delete/*",
"/tags/add/*",
"/tags/delete/*",
"/tags/edit/*",
"/tags/index/*",
"/tags/quickAdd/*",
```

```

"/tags/selectTag/*",
"/tags/selectTaxonomy/*",
"/tags/showEventTag/*",
"/tags/view/*",
"/tags/viewTag/*",
"/taxonomies/index/*",
"/taxonomies/taxonomyMassConfirmation/*",
"/taxonomies/view/*",
"/templateElements/index/*",
"/templates/deleteTemporaryFile/*",
"/templates/index/*",
"/templates/populateEventFromTemplate/*",
"/templates/submitEventPopulation/*",
"/templates/templateChoices/*",
"/templates/uploadFile/*",
"/templates/view/*",
"/threads/index/*",
"/threads/view/*",
"/threads/viewEvent/*",
"/users/dashBoard/*",
"/users/downloadTerms/*",
"/users/edit/*",
"/users/histogram/*",
"/users/index/*",
"/users/login/*",
"/users/logout/*",
"/users/memberslist/*",
"/users/resetauthkey/*",
"/users/routeafterlogin/*",
"/users/statistics/*",
"/users/terms/*",
"/users/updateLoginTime/*",
"/users/view/*",
"/whitelists/index/*"
]
}
}
}

```

## Getting a list of all accessible controllers and actions in MISP

```
https://<misp url>/servers/queryACL/printAllFunctionNames
```

This URL will return a JSON with all controller and all mapped functions within them.

## Viewing a list of yet unmapped functions

```
https://<misp url>/servers/queryACL/findMissingFunctionNames
```

Functions that have not been tied into the new ACL yet show up here. These functions will (until added to the ACL) only be accessible to site admins.

## Appendix C: Official MISP developments

This section lists the projects that can be found on the main [MISP GitHub](#) page we know of but not officially support and rely on their respective maintainers to keep up to date to the MISP 2.4 developments.

| Project      | Description  | Status                                      |
|--------------|--|---|
| misp-objects | Definition, description and relationship types of <a href="#">MISP objects</a> | Core to MISP, frequently updated and tested |

| Relationship types of threat objects |                                       |  |
|--------------------------------------|---------------------------------------|--|
| Best Practices in ThreatIntel        | Best practices in threat intelligence | Book available here: <a href="https://www.misp-project.org/best-practices-in-threat-intelligence.html">https://www.misp-project.org/best-practices-in-threat-intelligence.html</a> |

## Appendix D: Third-party development

This section lists some projects we know of but not officially support and rely on their respective maintainers to keep up to date to the MISP 2.4 developments.

| Project                 | Description   | Status                                  |
|-------------------------|---|---|
| MISP-STIX-ESM           | Exports MISP events to STIX and ingest into McAfee ESM  | Not tested by MISP core team            |
| Docker MISP             | Automated Docker MISP container   | Not tested by MISP core team            |
| misp42splunk            | A Splunk app to use MISP in background and combine with TheHive   | Not tested by MISP core team            |
| getmispioc              | getiocmisp is a Splunk custom search command that helps to extract IOCs from a <a href="#">MISP instance</a> .  | Not tested by MISP core team            |
| OTX MISP                | Imports AlienVault OTX pulses to a <a href="#">MISP instance</a>  | Not tested by MISP core team            |
| BTG                     | BTG's purpose is to make fast and efficient search on <a href="#">IOC</a>   | Not tested by MISP core team            |
| MISP OSINT Collection   | Collection of best practices to add <a href="#">OSINT</a> into MISP and/or MISP communities   | Not tested by MISP core team            |
| IBM XFE module          | Various IBM X-Force Exchange modules  | Not tested by MISP core team            |
| MISP dockerized         | MISP dockerized is a project designed to provide an easy-to-use and easy-to-install 'out of the box' <a href="#">MISP instance</a> that includes everything you need to run MISP with minimal host-side requirements. | Not tested by MISP core team            |
| MISP dockerized modules | MISP-modules for MISP dockerized  | Not tested by MISP core team            |
| FireMISP                | FireEye Alert json files to MISP Malware information sharing platform (Alpha)   | Not tested by MISP core team            |
| MISP Chrome Plugin      | MISP Chrome plugin for adding and looking up <a href="#">indicators</a>   | Not tested by MISP core team            |
| PySight2MISP            | PySight2MISP is a project that can be run to be used as glue between iSight intel <a href="#">API</a> and MISP <a href="#">API</a>  | Not tested by MISP core team            |
| tie2misp                | Import DCSO TIE IOCs as MISP events   | Not tested by MISP core team            |
| security onion MISP     | Grab <a href="#">NIDS</a> rules and Bro Intel generated from a <a href="#">MISP instance</a> and use them in Security Onion   | Not tested by MISP core team            |
| virustream              | A script to track malware IOCs with <a href="#">OSINT</a> on Twitter.   | Not tested by MISP core team            |
| LAC CSV Import          | Register MISP events based on information described in files such as CSV and TSV.   | Not tested by MISP core team            |
|                         |   | Strong links between core team members, |

|   |  |                              |
|---|--|------------------------------|
| <a href="#">The Hive</a>                          | <a href="#">TheHive: a Scalable, Open Source and Free Security Incident Response Platform</a>  | tested and known working     |
| <a href="#">puppet-misp</a>                       | This module installs and configures MISP - <a href="#">puppet forge site</a>   | Not tested by MISP core team |
| <a href="#">Ansible MISP</a>                      | Ansible playbook to install Malware Information Sharing Platform (MISP)  | <b>unmaintained</b>          |
| <a href="#">ansible MISP</a>                      | ansible role to setup MISP   | Not tested by MISP core team |
| <a href="#">OpenDXL ATD MISP</a>                  | Automated threat intelligence collection with McAfee ATD, OpenDXL and MISP   | Not tested by MISP core team |
| <a href="#">IMAP Proxy</a>                        | Modular IMAP proxy (including PyCIRCLEanMail and MISP forward modules)   | Not tested by MISP core team |
| <a href="#">AutoMISP</a>                          | automate your MISP installs - This shell script is designed to automatically install <a href="#">MISP</a> and the <a href="#">misp-modules</a> extension on either Ubuntu 16.04, or 18.04. | Not tested by MISP core team |
| <a href="#">Palo Alto Networks report_to_misp</a> | Parse a report and import the events into MISP   | Not tested by MISP core team |
| <a href="#">Palo Alto Networks minemeld-misp</a>  | MineMeld nodes for MISP  | Not tested by MISP core team |
| <a href="#">golang-misp</a>                       | Golang Library to interact with your <a href="#">MISP instance</a>   | Not tested by MISP core team |
| <a href="#">go-misp</a>                           | Golang MISP API Client   | Not tested by MISP core team |
| <a href="#">MISP MAR</a>                          | Integration between MISP platform and McAfee Active Response   | Not tested by MISP core team |
| <a href="#">MISP IoC Validator</a>                | Validate <a href="#">IOC</a> from MISP ; Export results and iocs to SIEM and sensors using syslog and CEF format   | Not tested by MISP core team |
| <a href="#">vt2misp</a>                           | Script to fetch data from virustotal and add it to a specific event as an object   | Not tested by MISP core team |
| <a href="#">Threat Pinch Lookup</a>               | Documentation and Sharing Repository for ThreatPinch Lookup Chrome & Firefox <a href="#">Extension</a>   | Not tested by MISP core team |
| <a href="#">dovehawk</a>                          | Dovehawk is a Bro module that automatically imports MISP <a href="#">indicators</a> and reports Sightings  | Not tested by MISP core team |
| <a href="#">yara-exporter</a>                     | Exporting <a href="#">MISP event</a> attributes to yara rules usable with Thor apt scanner   | Not tested by MISP core team |
| <a href="#">volatility-misp</a>                   | Volatility plugin to interface with MISP   | Not tested by MISP core team |
| <a href="#">misp2bro</a>                          | Python script that gets <a href="#">IOC</a> from MISP and converts it into BRO intel files.  | Not tested by MISP core team |
| <a href="#">TA-misp</a>                           | Splunk integration with MISP   | Not tested by MISP core team |
| <a href="#">MISP QRadar</a>                       | The Project can used to integrate QRadar with MISP Threat Sharing Platform   | Not tested by MISP core team |
| <a href="#">pymisp-suricata_search</a>            | Multi-threaded suricata search module for MISP   | Not tested by MISP core team |
| <a href="#">MISP-</a>                             | <a href="#">Script to interface MISP with Facebook ThreatExchange</a>  | Not tested by MISP           |

|                                       |   |                              |
|---------------------------------------|---|------------------------------|
| ThreatExchange                        | Script to interface MISP with Facebook ThreatExchange                       | core team                    |
| aptc                                  | Automated Payload Test Controller   | Not tested by MISP core team |
| aptmap                                | A map displaying threat actors from the <a href="#">misp-galaxy</a>         | Not tested by MISP core team |
| mispy                                 | Another MISP module for Python  | Not tested by MISP core team |
| MispSharp                             | C# Library for MISP   | Not tested by MISP core team |
| misp_btc                              | get BTC addresses from MISP and fetch BTC transactions                      | Tested by MISP core team     |
| Privacy Aware Sharing of IoCs in MISP | Master Thesis including MISP data.  | Master thesis                |
| sam-bot                               | Bot to create MISP events from data in Slack                                | Not tested by MISP core team |
| Polarity.io Connector                 | "Polarity is the memory augmentation platform that makes your team smarter" | Not tested by MISP core team |

## Appendix E: Other Threat Intel Ressources

A brief list of online ressources that around #ThreatIntel

- A curated list of awesome malware analysis tools and resources. Inspired by [awesome-python](#) and [awesome-php](#).
- An authoritative list of awesome devsecops tools with the help from community experiments and contributions.[DEV.SEC.OPS](#)
- Advance Python IoC extractor

## Appendix F: LDAP Authentication

MISP supports LDAP authentication from version 2.4.xxx. This manual will show how to configure LDAP authentication.

### Installation and configuration

1. Install `mod_ldap` PHP module

```
# for Centos or RHEL
yum install rh-php72-php-ldap
# for Ubuntu or debian
apt install php-ldap
```

2. Prepare variables for configuration

3. ` - a full LDAP URI of server. For example: `ldap://example.com``.
4. ` - DN for path that contains users. For example: `cn=users,cn=accounts,dc=example,dc=com``.
5. ` - user that can read. For example: `uid=misp,cn=sysaccounts,cn=etc,dc=example,dc=com``.
6. `` - password for that user.
7. ` - group with access to MISP. For example: `cn=misp-users,cn=groups,cn=accounts,dc=example,dc=com``.

## 8. Configure MISP ApacheSecureAuth in `app/Config/config.php`

```
'LdapAuth' => array(
    'enabled' => true,
    'name' => 'My Identity provider',
    'ldapServer' => '',
    'ldapDN' => '',
    'ldapSearchFilter' => '(objectclass=inetuser)',
    'ldapReaderUser' => '',
    'ldapReaderPassword' => '',
    'ldapUserGroup' => '',
    'updateUser' => true,
);
```

Required variables:

- `enabled` – if it is true, all users must log in through LDAP account.
- `ldapServer` – a full LDAP URI of the form `ldap://hostname:port` or `ldaps://hostname:port` for TLS encryption.
- `ldapDN` – DN for a path that contains users.

Optional variables:

- `name` – identity provider name. Will be shown in the login screen and user editing for. Can contain HTML.
- `ldapReaderUser` – DN or RDN LDAP user with permission to read LDAP information about users.
- `ldapReaderPassword` – password for that user.
- `ldapSearchFilter` – LDAP search filter.
- `ldapSearchAttribute` – LDAP attribute that contains username. Default: `uid`.
- `ldapEmailField` – LDAP attribute (string) or attributes (array) that will be checked if contains user e-mail address. If you want to change or add field, you should also add that field/fields to `ldapAttributes`. Default: `mail`.
- `ldapAttributes` – fields that will be fetched from LDAP server. Default: `mail` and `memberof`.
- `ldapUserGroup` – LDAP group that must be assigned to user to access MISP. Default: not set.
- `createUser` – if `true`, MISP will create new user from LDAP. Default `true`.
- `updateUser` – if `true`, MISP will update existing users information (e-mail address and role) from LDAP after login. Default: `false`.
- `ldapDefaultOrg` – default organization ID for user from LDAP. By default it is the first organization in the database.
- `ldapDefaultRoleId` – default role for newly created user. It can be integer or array when key contains LDAP group and value assigned role ID. Must be defined if `updateUser` is set to `true` (without that variable, user will be disabled).
- `ldapProtocol` – protocol version used. Default: 3.
- `ldapNetworkTimeout` – timeout for communication with LDAP server in seconds. Default: 5 seconds.
- `ldapAllowReferrals` – follow referrals returned by the LDAP server. Default: `false`.
- `ldapStartTls` – enable STARTTLS. Default: `true`.

## Debugging

Setting LDAP authentication can be sometimes tricky. For debugging, you can check MISP error log (by default in `/var/www/MISP/app/tmp/logs/error.log`) or debug log (by default in `/var/www/MISP/app/tmp/logs/debug.log`) that can contain useful information with problem description.

## Migrating existing user to LDAP

Because LDAP and MISP users are paired by e-mail address, it is possible to migrate existing user account to LDAP managed. When you enable LDAP support and LDAP user will try to log in, an existing user in MISP with the same e-mail address will be found and then assigned to LDAP user.

## Caveats

- When a user is disabled in LDAP or is removed from the required group, it will be not automatically disabled in MISP. That means that user will be disabled when he tries to login (with form or with Auth key), but for example, notification e-mails will still work until he tries to log in.
- When a user is disabled in LDAP and also in MISP and then enabled in LDAP, it will be enabled in MISP for next login just when `updateUser` is set to `true`.
- Currently it is not possible to log in with both LDAP and local (MISP) accounts.
- Admins can change users email address. But when `updateUser` is set to true, when the user will log in again, the e-mail address will be updated from LDAP.
- `Security.require_password_confirmation` setting currently doesn't work with LDAP authentication. But on the other hand, since user cannot change e-mail address and password, this setting is not important.