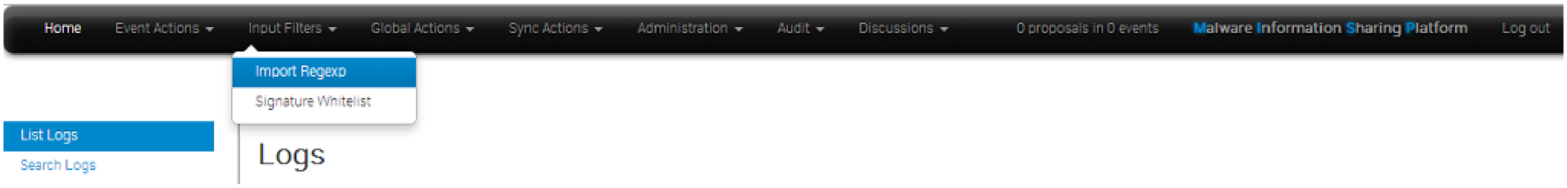
General Layout

The top bar



This menu contains all of the main functions of the site as a series of dropdown menues. These contains all (from the current 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.
- **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 organisations on this instance and a histogram of their contributions by attribute type.
- **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 synchronisation 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 synchronisation 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 organisation (or for site admins for the entire system) here or even search the logs if you are interested in something specific.
- **Discussions:** Link to the discussion threads.
- **Proposal Notifications:** This shows how many proposals your organisation has received and across how many events they are spread out. Clicking this will take you to the list of proposals.
- **Log out:** Logs you out of the system.

A list of the contents of each of the above drop-down menues

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 populating with 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.
- **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 organsiation 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 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 standardising 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 contain the values that are blocked from being used for exports and automation on this instance. Site administrators have access to editing this list.

Global Actions

- **News:** Read about the latest news regarding the MISP system
- **My Profile:** Manage your user account.
- **Members List:** View the number of users per organisation and get some statistics about the currently stored attributes.
- **Role Permissions:** You can view the role permissions here.
- **User Guide:** A link to this user guide.
- **Terms & Conditions:** View the terms & conditions again.
- **Statistics:** View a series of statistics about the users and the data on this instance.
- **Log out:** Logs the current user out.

Sync Actions

- **List Servers:** Connect your MISP instance to other instances, or view and modify the currently established connections.

Administration

- **New User:** Create an account for a new user for your organisation. Site administrators can create users for any organisation.
- **List Users:** View, modify or delete the currently registered users.
- **New 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.
- **List Roles:** List, modify or delete currently existing roles.
- **Contact Users:** You can use this view to send messages to your current or future users or send them a new temporary password.
- **Administrative Tools:** Various tools, upgrade scripts that can help a site-admin run the instance
- **Server Settings:** 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).

Audit

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

Discussions

- **List Discussions:** List all of the discussion threads.
- **Start Discussion:** Create a new discussion thread.

The left bar

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

General Concepts

Admins and Site Admins

There are two types of admins in MISP: Admins (also refered 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 refered to as "this instance" or "your instance". The instances that your instance synchronises with will be refered 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 assigned 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.

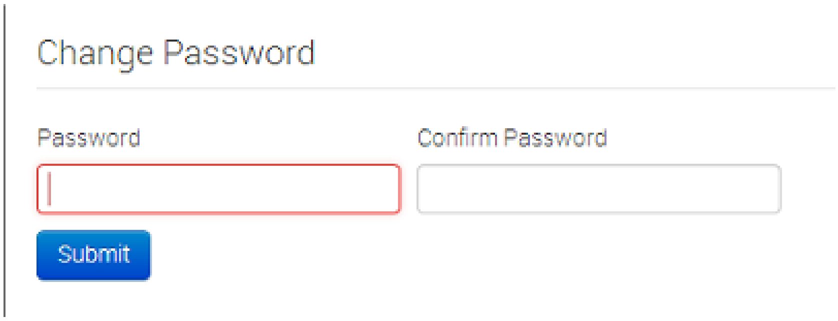
User Management and Global Actions

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.

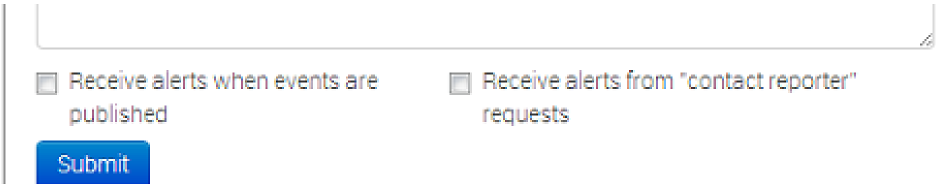
- **Acceping the Terms of use:** The terms of use are shown immediately after logging in for the first time, make sure to read through this page before clicking "Accept Terms" at the bottom of the page.

- **Changing the password:** After accepting the ToU, you'll be prompted to change your password, but keep in mind that it has to be at least 6 characters long, it has to include at least one upper-case and one lower-case character in addition to a digit or a special character. Enter the same password into the confirm password field, before clicking submit to finalise the change.



- **Setting up the GPG Key:** In order for the system to be able to encrypt the messages that you send through it, it needs to know your GPG key. Navigate to the Edit profile view (My Profile on the left -> Edit profile in the top right corner). Paste the key into the Gpgkey 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.



□ Receive alerts when events are published

□ Receive alerts from "contact reporter" requests

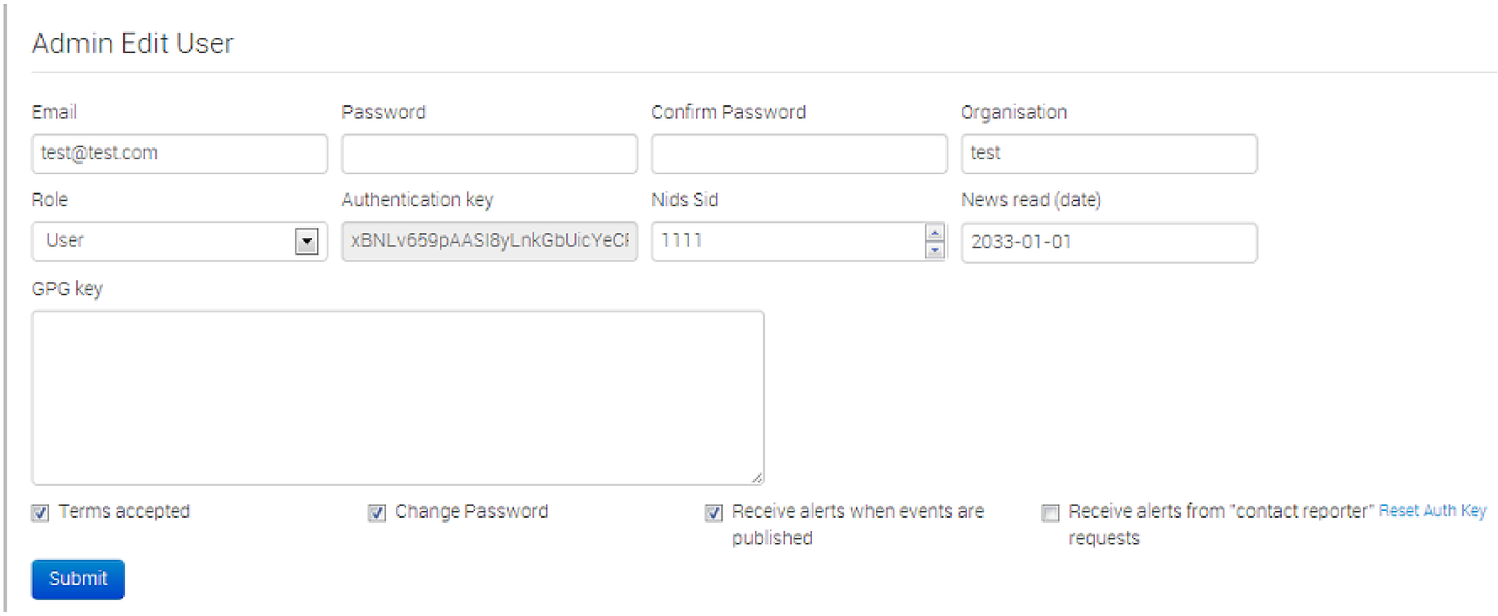
- **Subscribing to e-mails sent via the "Contact Reporter" functionality:** This feature is turned on right below the autoalerts and will allow you to receive e-mails addressed to your organisation whenever a user tries to ask about an event that was posted by a user of your organisation. Keep in mind 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.

Managing your account:

To alter any details regarding your profile, use the "My Profile" menu button to bring up the profile overview and then click on "Edit Profile" in the right upper corner.



Admin Edit User

Email: test@test.com

Password:

Confirm Password:

Organisation: test

Role: User

Authentication key: xBNLv659pAASI8yLnkGbUicYeCf

Nids Sid: 1111

News read (date): 2033-01-01

GPG key:

☑ Terms accepted ☑ Change Password ☑ Receive alerts when events are published ☐ Receive alerts from "contact reporter" requests

- **Changing your e-mail address:** Your e-mail address serves as both a login name and as a means of communication with other users of the MISP system via the contact reporter feature. To change your e-mail address, just enter the edit profile menu (My profile on the left navigation menu -> Edit profile in the top right corner) and change the field titled Email.

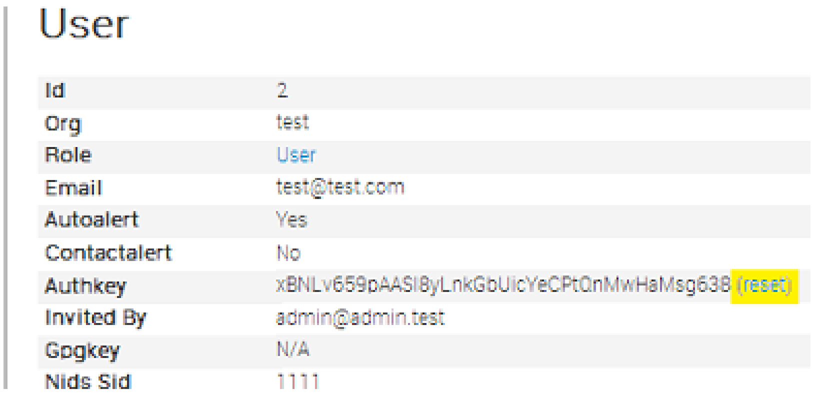
- **Changing the password:** As a next step, change the password provided by your administrator to something of your own choosing. Click on My profile on the left navigation menu, under Global Actions, which will bring up the User view. Click on Edit User on the left navigation menu or Edit Profile in the top right corner. This next screen, allows you to edit your details, including your password, by filling out the password field. Keep in mind that the password has to be at least 6 characters long, has to include at least one upper-case and one lower-case character in addition to a digit or a special character. Enter the same password into the confirm password field, before clicking submit to finalise the change.

- **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.

- **Subscribing to e-mails sent via the "Contact Reporter" functionality:** Turning this feature on 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 the person that reported an event that you yourself have created.

- **Setting up the GPG Key:** In order for the system to be able to encrypt the messages that you send through it, it needs to know your GPG key. You can acquire this by clicking on the PGP/GPG key link at the bottom left of the screen. Copy the entirety of the key and navigate to the Edit profile view (My Profile on the left -> Edit profile in the top right corner). Paste the key into the Gpgkey field and click submit.

- **Requesting a new authentication key:** It is possible to make the system generate a new authentication key for you (for example if your previous one gets compromised. This can be accessed by clicking on the My Profile button and then clicking the reset key next to the currently active authentication code. The old key will become invalid when the new one is generated.



User

Id	2
Org	test
Role	User
Email	test@test.com
Autoalert	Yes
Contactalert	No
Authkey	xBNLv659pAASI8yLnkGbUicYeCPtQnMwHaMsg638 (reset)
Invited By	admin@admin.test
Gpgkey	N/A
Nids Sid	1111

Staying up to date:

MISP also provides its users with some information about itself and its users through the links provided in the Global Actions menu.

- **News:** To read about the news regarding the system itself, click on News on the left menu. This will bring up a list of news items concerning updates and changes to MISP itself.

- **Member statistics:** By using the Members List menu button on the left, you can get a quick overview over how many users each organisation has registered on your server, and a histogram, depicting the distribution of attribute types created by each organisation.

- **User Guide:** The user guide is also accessible via the Global Actions menu. You can find out more about how to use the system by reading this.

- **Terms & Conditions:** It is possible to review the terms & conditions that were shown during the first run of the system by clicking on the terms & conditions link in the Global Actions menu.

- **Statistics:** View statistics about the users and the data contained within this instance.
  - **General Statistics:** View a set of statistics such as the number of Events and Attributes currently in existance on the platform. The number in the bracket shows the number of new items added during this week.
  - **Activity Heatmap:** This graph shows a heatmap of all activity related to creating event related data on a day by day basis. By default, the graph shows the sum of the contributions of all organisations, but using the buttons representing each organisation in existance on the platform you can switch to the activity heatmap of a single organisation. If you'd like to see the activity further back in the past, just use the arrow buttons to navigate the heatmap.

Inspecting the input filters:

All the events and attributes that get entered into MISP will be run through a series of input filters. These are defined by the site administrators or users with special privileges to edit the filters, but every user can take a look at the currently active lists.

- **Import Regexp:** All Attribute value and Event info fields will be parsed for a set of regular expressions and replaced based on the replacement values contained in this section. This has many uses, such as unifying similar data for better correlation, removing personal data from file-paths or simply for clarity. It is also possible to blacklist data by not defining a replacement for a regular expression.

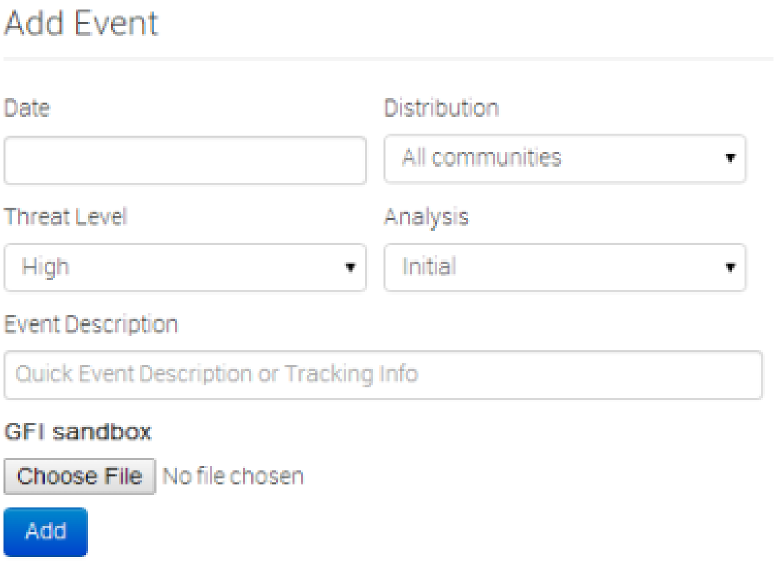
- **Signature Whitelist:** This list (can) contain a set of addresses that are allowed to be entered as attribute values but will be blocked from being exported to NIDS-es.

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 be 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: All communities

Threat Level: High

Analysis: Initial

Event Description: Quick Event Description or Tracking Info

GFI sandbox

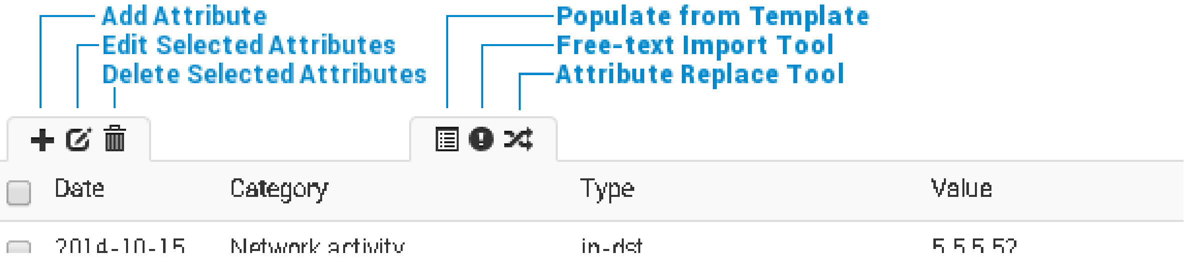
No file chosen

- **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. For more information on community-related distribution levels, click here.
      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.
- **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.

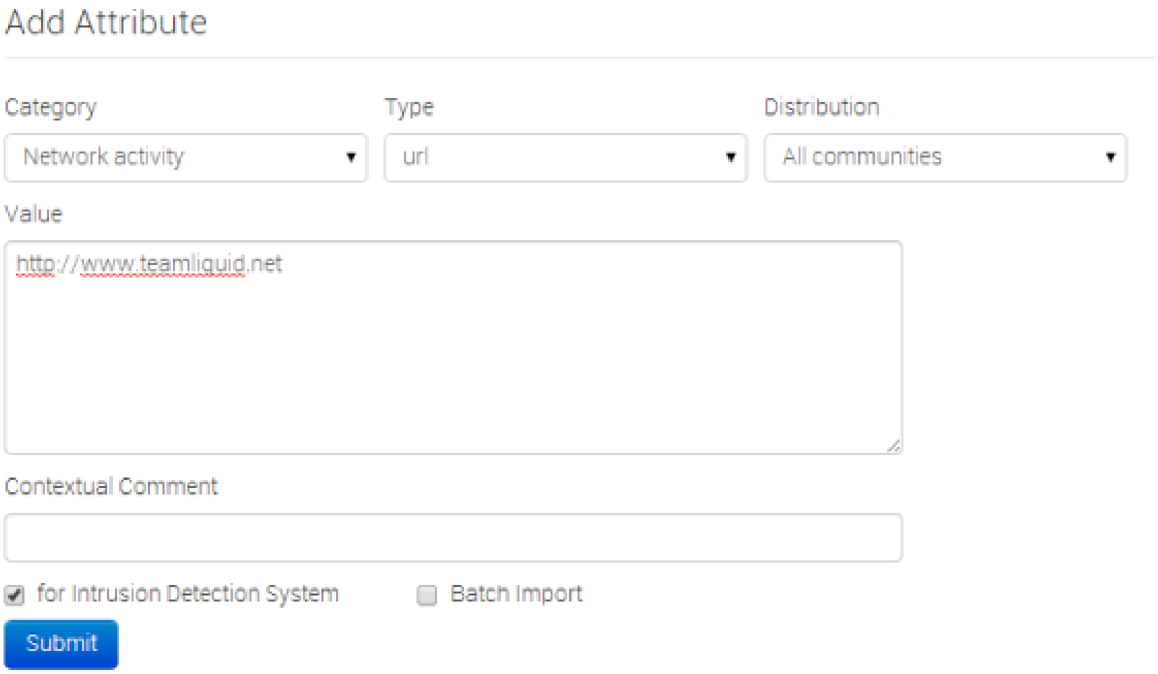


□	Date	Category	Type	Value
□	2014-10-15	Network activity	ip-dst	5.5.5.52

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: Network activity
Type: url
Distribution: All communities

Value: http://www.teamliquid.net

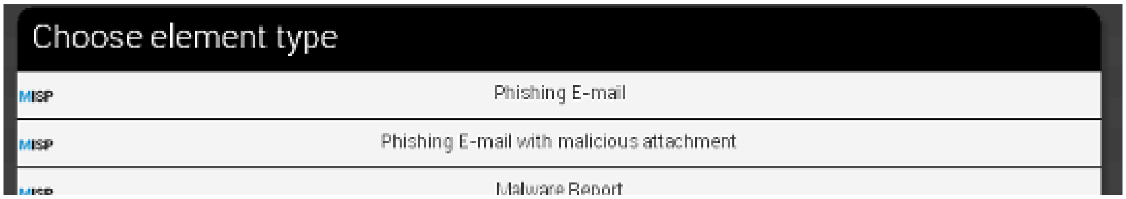
Contextual Comment:

☑ for Intrusion Detection System □ Batch Import

- **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 click here.
- **Contextual Comment:** Add a comment to the attribute. This will not be used for correlation.
- **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 whitelist, head over to the administration section.
- **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 the each attribute.

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.



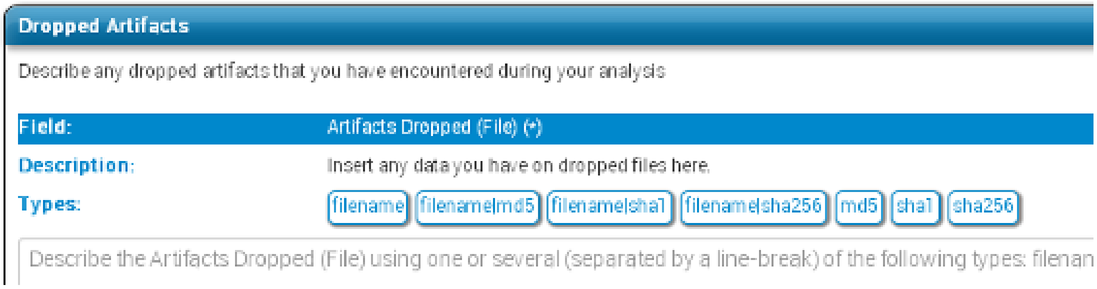
Choose element type

MISP Phishing E-mail

MISP Phishing E-mail with malicious attachment

MISP Malware Report

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 devided 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

Field: Artifacts Dropped (File) (*)

Description: Insert any data you have on dropped files here.

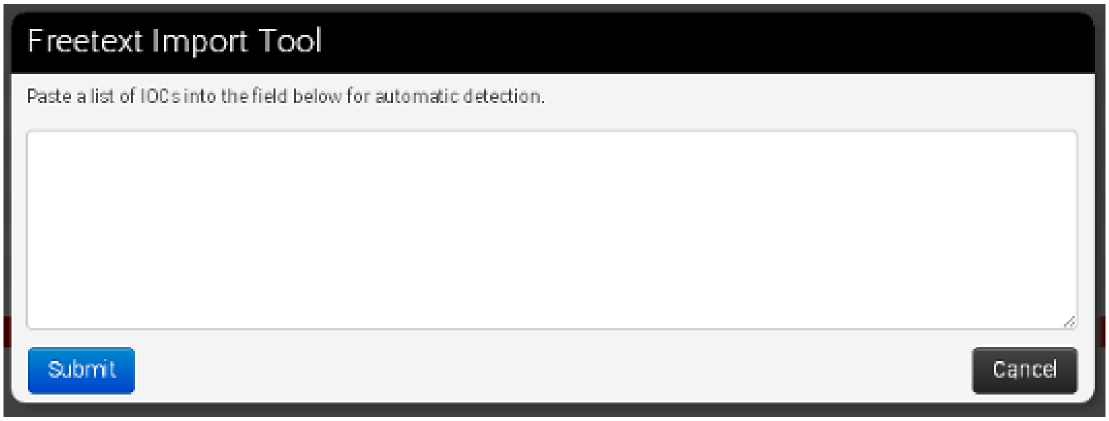
Types: filename filename|md5 filename|sha1 filename|sha256 md5 sha1 sha256

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

- **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 line textfield or a multi-line text area. For the former, enter a single value of the above indicated type, whilst for the latter you cna paste a list of values separated by line-breaks.

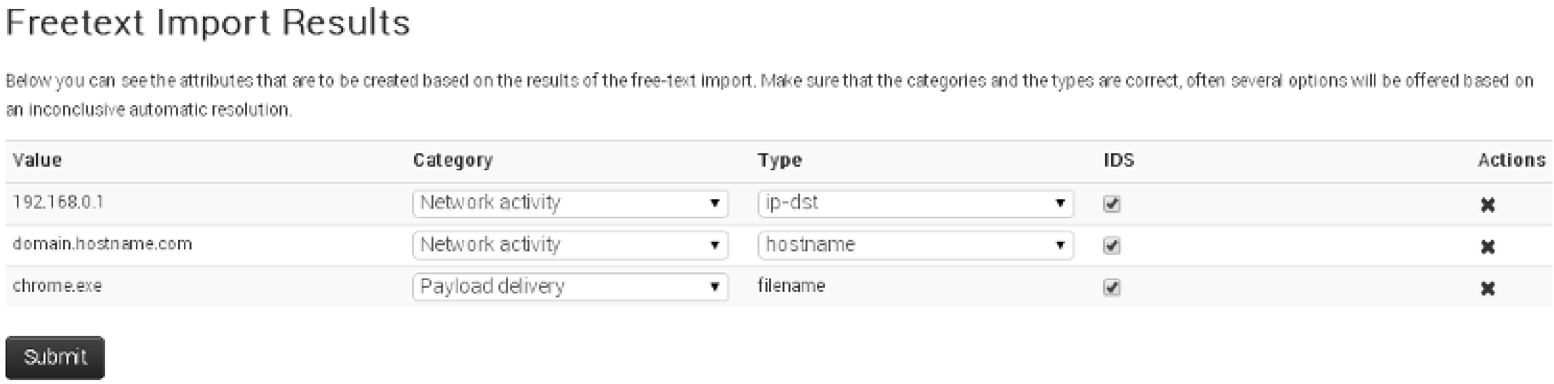
Freetext Import Tool



Freetext Import Tool

Paste a list of IOCs into the field below for automatic detection.

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

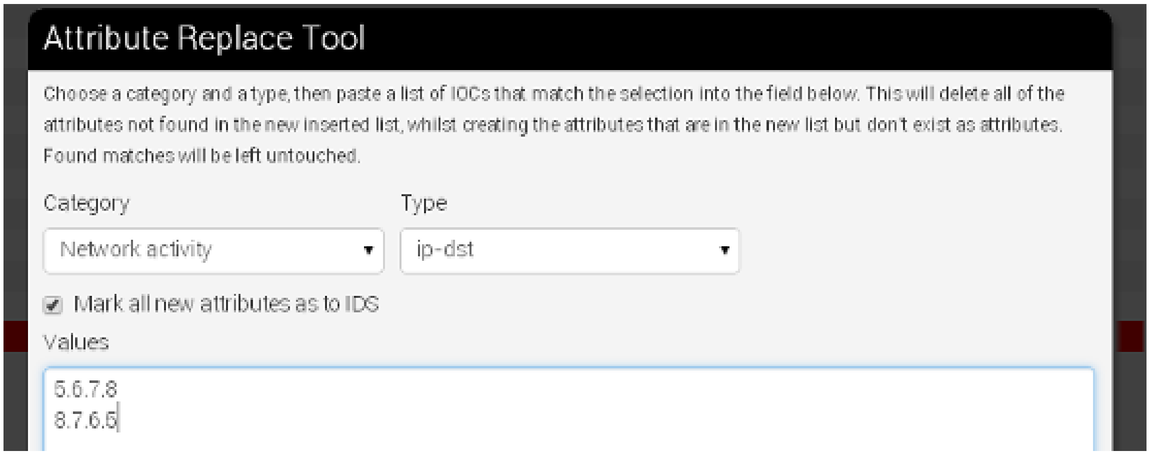
Below you can see the attributes that are to be created based on the results of the free-text import. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

Value	Category	Type	IDS	Actions
192.168.0.1	Network activity ▾	ip-dst ▾	☑	✖
domain.hostname.com	Network activity ▾	hostname ▾	☑	✖
chrome.exe	Payload delivery ▾	filename	☑	✖

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.

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.



Attribute Replace Tool

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: Network activity ▾

Type: ip-dst ▾

☑ Mark all new attributes as to IDS

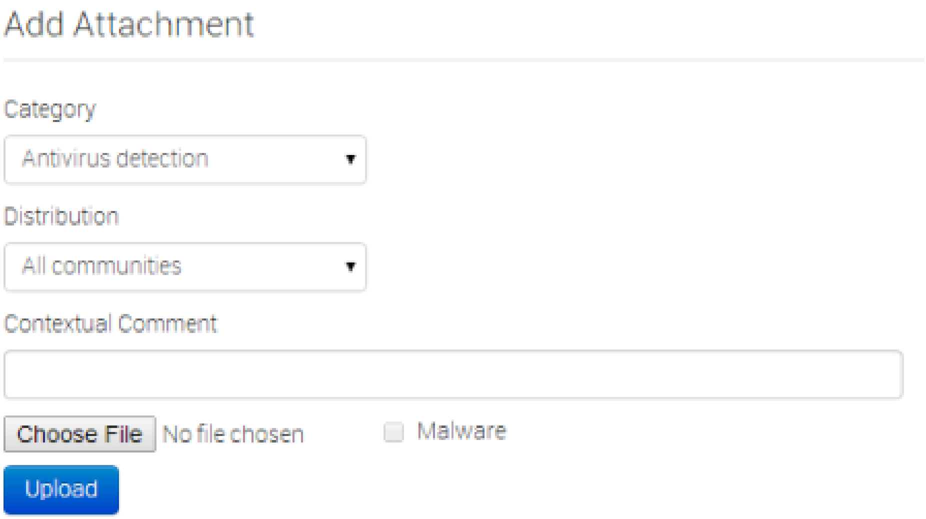
Values

```
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: Antivirus detection

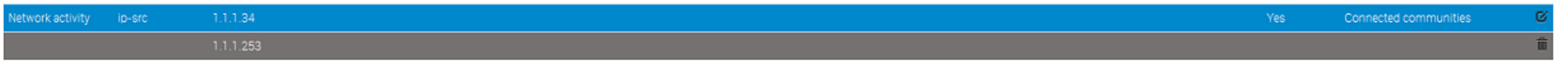
Distribution: All communities

Contextual Comment:

- **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 click here.
- **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 filed 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.

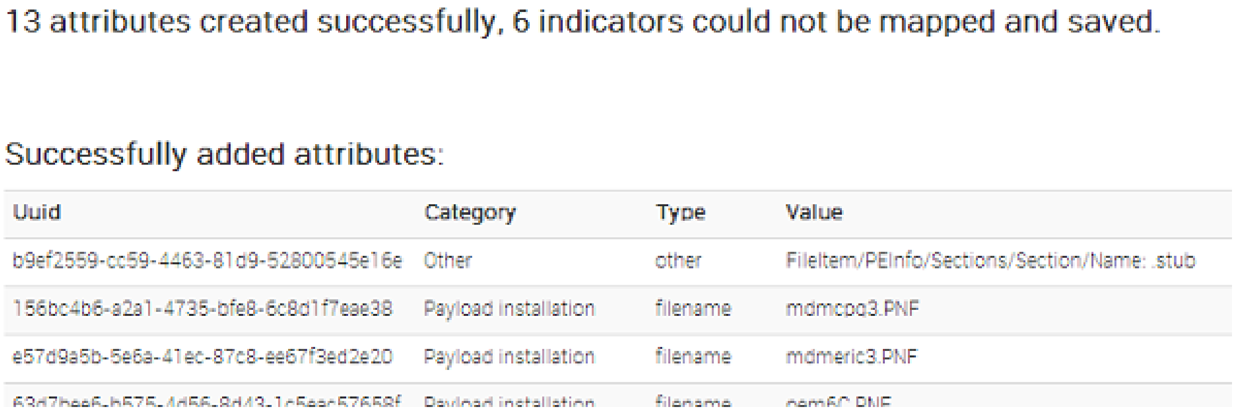


Network activity	ip-src	1.1.1.34	Yes	Connected communities	
		1.1.1.253			

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

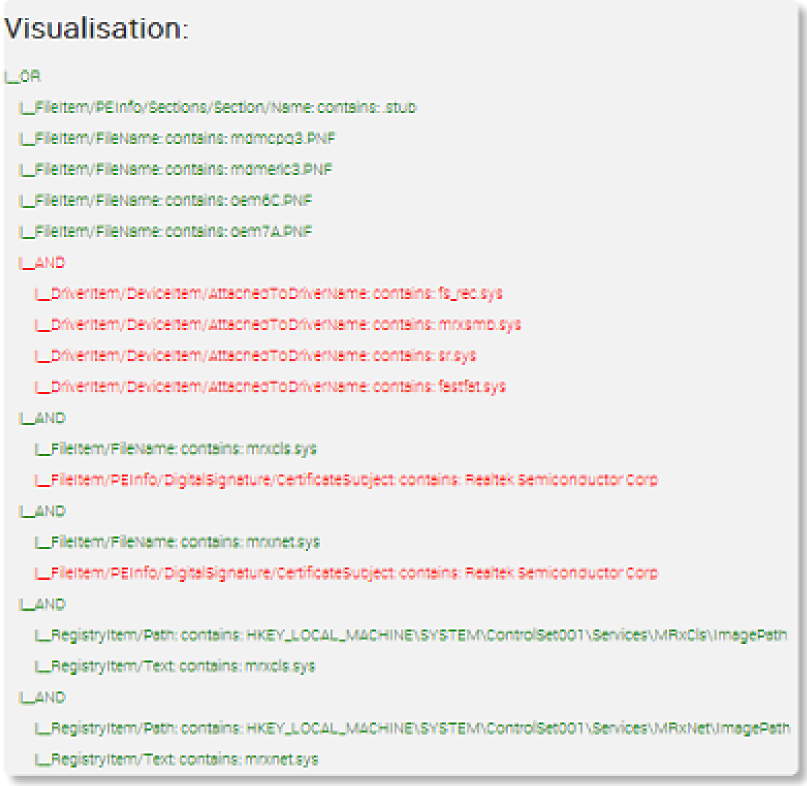
It is also possible to attempt to import the data contained in a .ioc file, The import tool will attempt to gather as many IndicatorItems within nested logical operators as possible without breaking their validity. After the procedure is done, you'll be presented with a list of successfully created attributes 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-a2a1-4735-bfe8-6c8d1f7eae38	Payload installation	filename	mdmcpq3.PNF
e57d9a5b-5e6a-41ec-87c8-ee67f3ed2e20	Payload installation	filename	mdmeric3.PNF
63d7bee6-b575-4d56-8d43-1c5eac57658f	Payload installation	filename	oem6C.PNF



Visualisation:

```
|_OR
  |_FileItem/PEInfo/Sections/Section/Name: contains: .stub
  |_FileItem/FileName: contains: mdmcpq3.PNF
  |_FileItem/FileName: contains: mdmeric3.PNF
  |_FileItem/FileName: contains: oem6C.PNF
  |_FileItem/FileName: contains: oem7A.PNF
  |_AND
    |_DriverItem/DeviceItem/AttachedToDriverName: contains: fs_rec.sys
    |_DriverItem/DeviceItem/AttachedToDriverName: contains: mrxsmb.sys
    |_DriverItem/DeviceItem/AttachedToDriverName: contains: sr.sys
    |_DriverItem/DeviceItem/AttachedToDriverName: contains: fastfat.sys
  |_AND
    |_FileItem/FileName: contains: mrxcls.sys
    |_FileItem/PEInfo/DigitalSignature/CertificateSubject: contains: Realtek Semiconductor Corp
  |_AND
    |_FileItem/FileName: contains: mrxnet.sys
    |_FileItem/PEInfo/DigitalSignature/CertificateSubject: contains: Realtek Semiconductor Corp
  |_AND
    |_RegistryItem/Path: contains: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxCls\ImagePath
    |_RegistryItem/Text: contains: mrxcls.sys
  |_AND
    |_RegistryItem/Path: contains: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxNet\ImagePath
    |_RegistryItem/Text: contains: mrxnet.sys
```

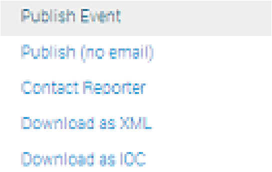
Populate from ThreatConnect

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.

Publish an event:


Publish Event
Publish (no email)
Contact Reporter
Download as XML
Download as IOC

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).

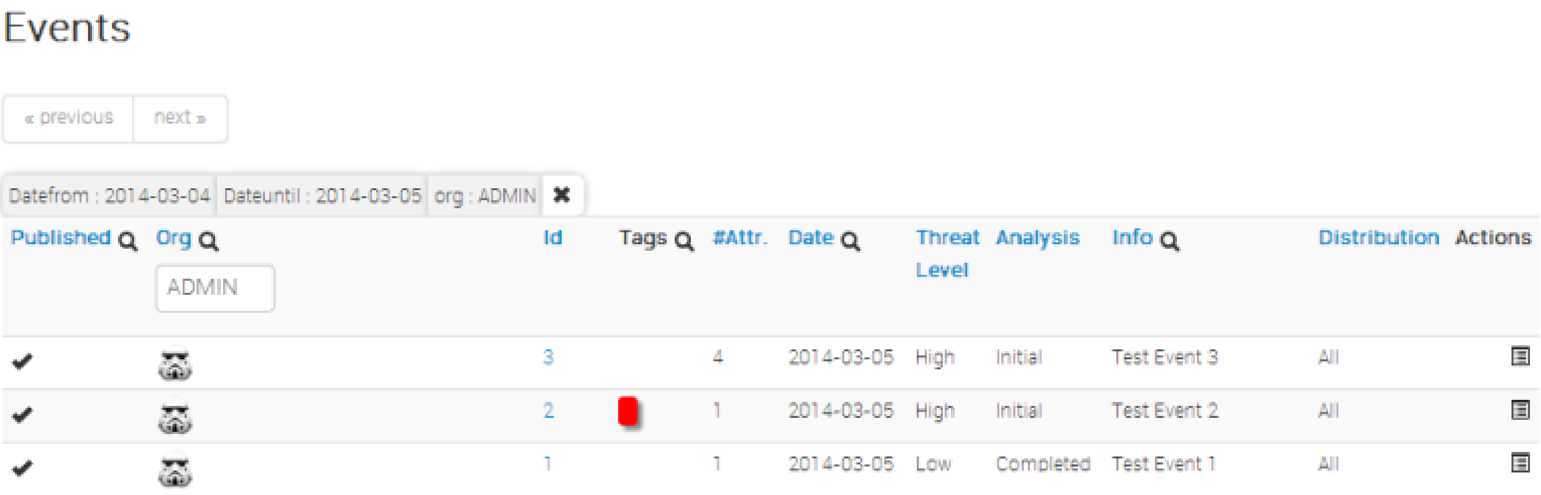
If your instance has background jobs enabled then the event might not get published immediately.

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

« previous | next »

Datefrom : 2014-03-04 | Dateuntil : 2014-03-05 | org : ADMIN | ✖

Published	Org ADMIN	Id	Tags	#Attr.	Date	Threat Level	Analysis	Info	Distribution	Actions
✓		3		4	2014-03-05	High	Initial	Test Event 3	All	
✓		2	🟥	1	2014-03-05	High	Initial	Test Event 2	All	
✓		1		1	2014-03-05	Low	Completed	Test Event 1	All	

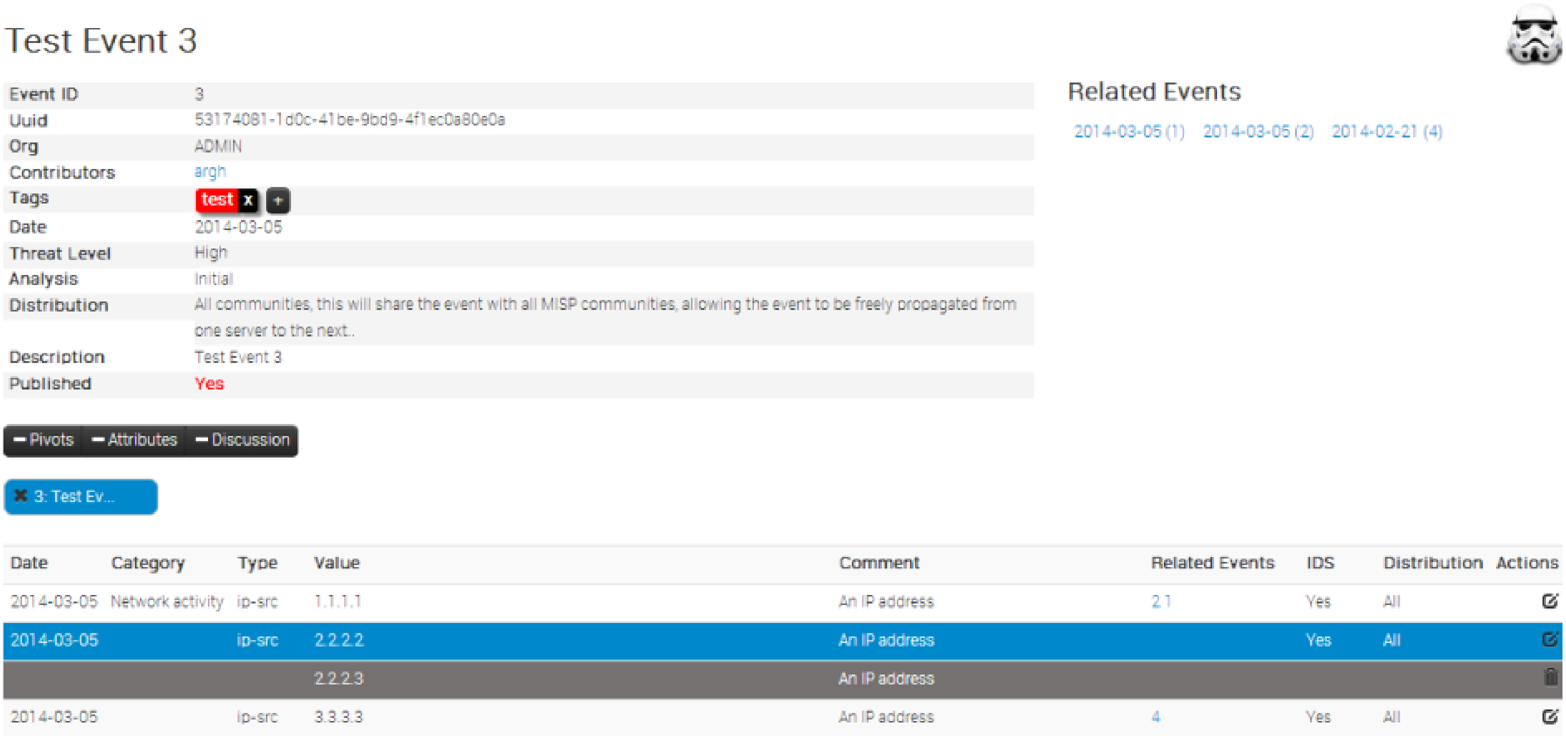
- **Published:** Already published events are marked by a checkmark. Unpublished events are marked by a cross.
- **Org:** The organisation that created the event.
- **Owner Org:** The organisation that owns the event on this instance. This field is only visible to administrators.
- **ID:** The event's 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. The options are described here.
- **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 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
Uuid	53174081-1d0c-41be-9bd9-4f1ec0a80e0a
Org	ADMIN
Contributors	argh
Tags	test x +
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

Related Events

2014-03-05 (1) 2014-03-05 (2) 2014-02-21 (4)

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	
2014-03-05		ip-src	2.2.2.2	An IP address		Yes	All	
			2.2.2.3	An IP address				
2014-03-05		ip-src	3.3.3.3	An IP address	4	Yes	All	

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 int he 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 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 test 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 sting 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.

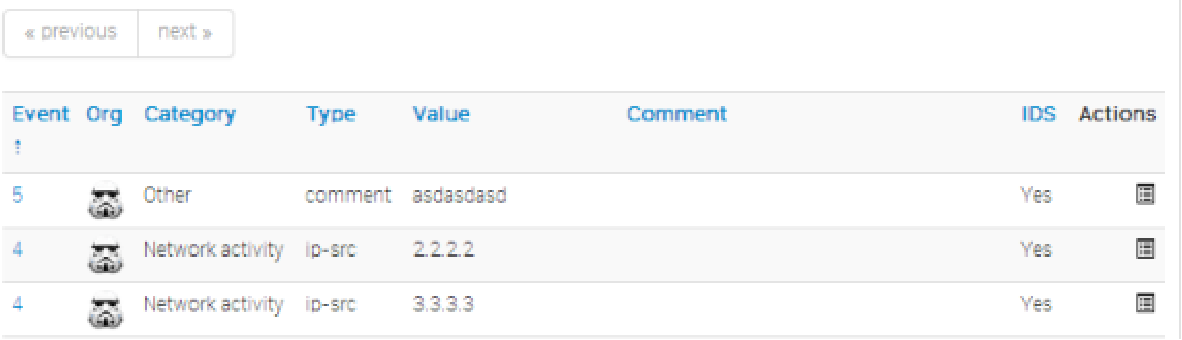
Event History:

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 contribing 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 followings fields:

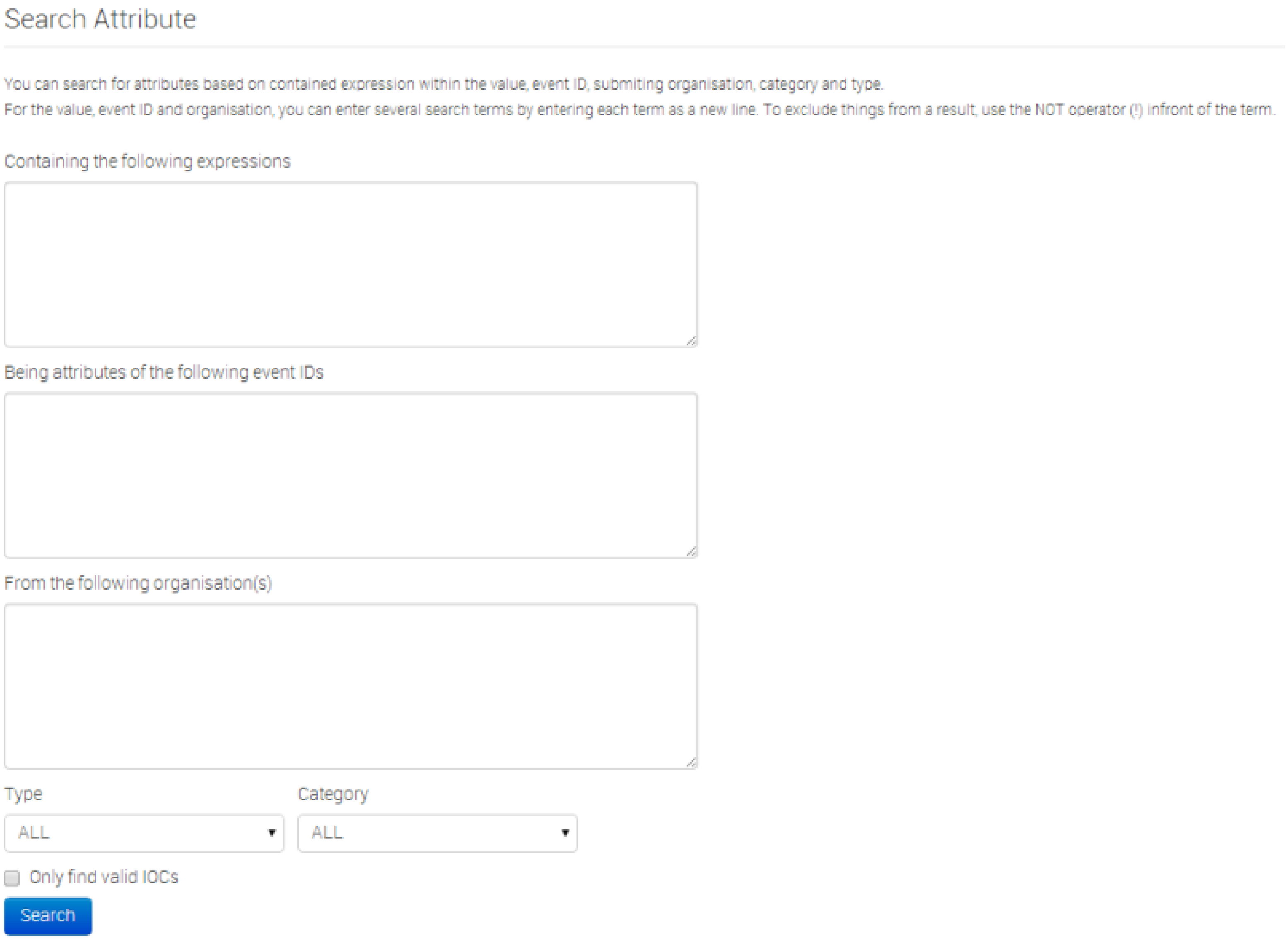


Event	Org	Category	Type	Value	Comment	IDS	Actions
5		Other	comment	asdasdasd		Yes	▤
4		Network activity	ip-src	2.2.2.2		Yes	▤
4		Network activity	ip-src	3.3.3.3		Yes	▤

- **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, submiting 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 (!) infront of the term.

Containing the following expressions

Being attributes of the following event IDs

From the following organisation(s)

Type: ALL

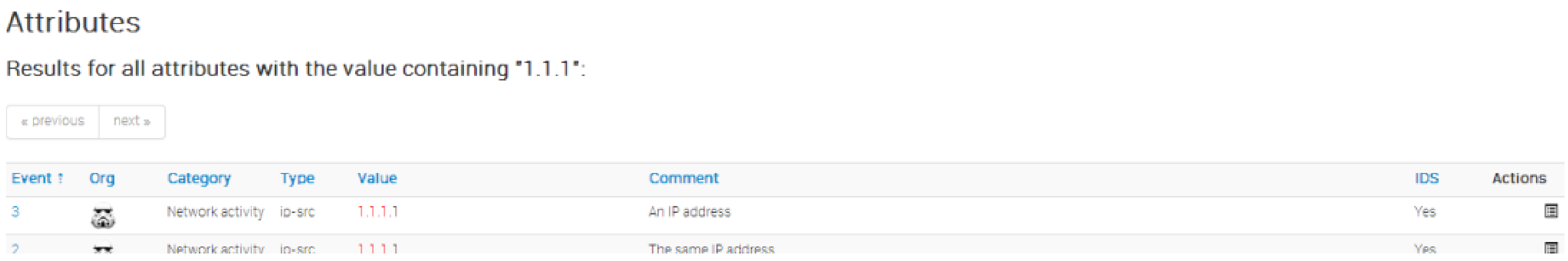
Category: ALL

□ 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:

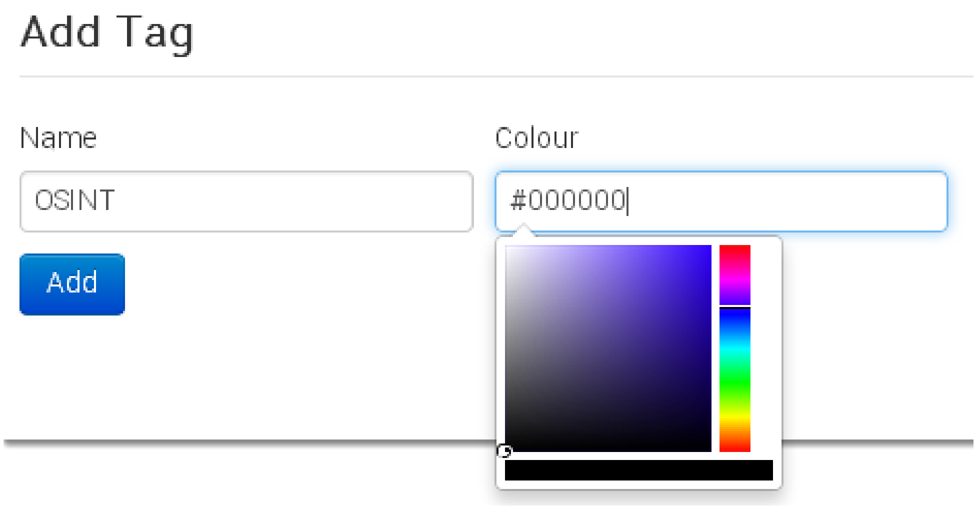
Every event and attribute can easily be edited. First of all it is important to find the event or attribute that is to be edited, using any of the methods mentioned in the section on browsing past events.

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).

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: OSINT

Colour: #000000

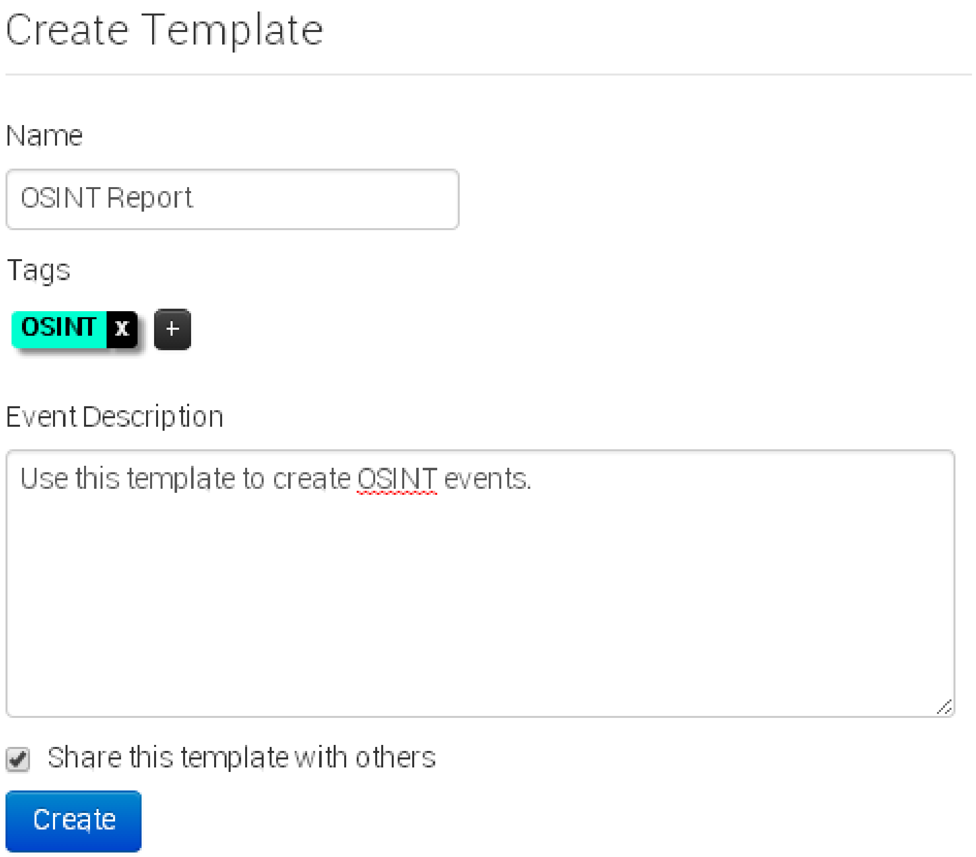
Fill out the following fields:

- **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

OSINT Report

Tags

OSINT x +

Event Description

Use this template to create OSINT events.

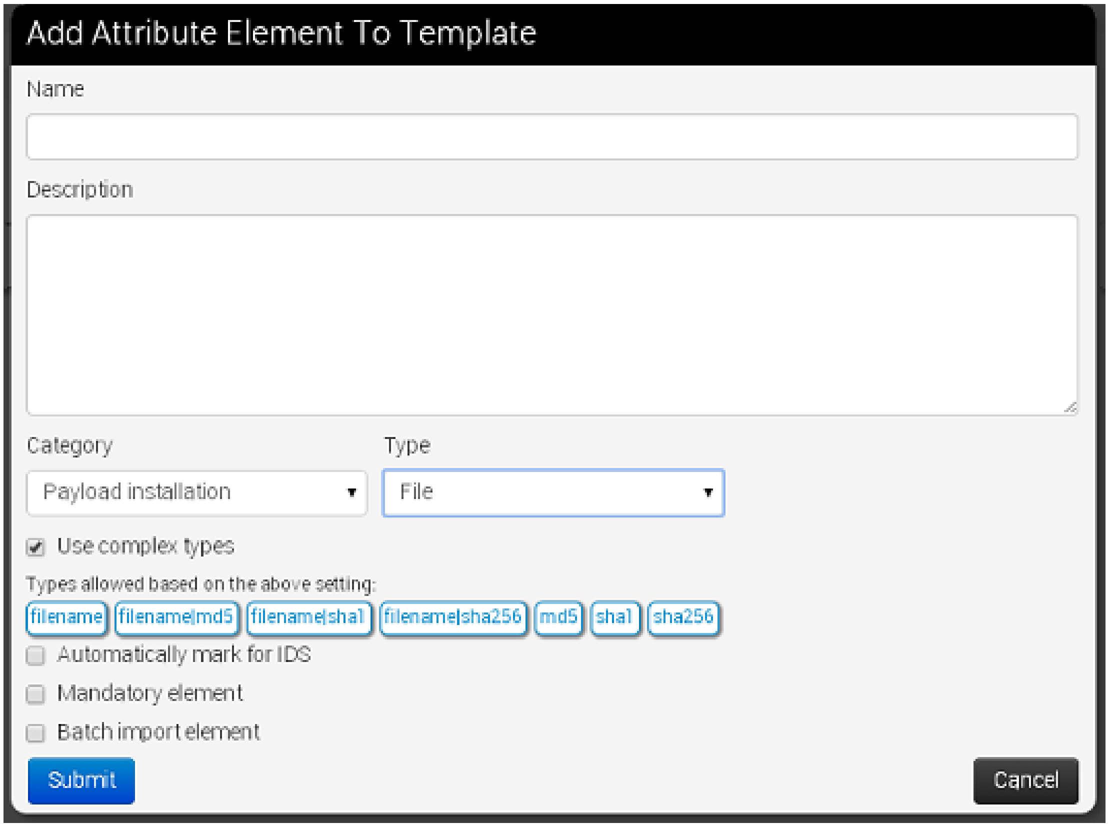
☑ Share this template with others

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 chnage 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: Payload installation

Type: File

☑ Use complex types

Types allowed based on the above setting: filename filename|md5 filename|sha1 filename|sha256 md5 sha1 sha256

□ Automatically mark for IDS

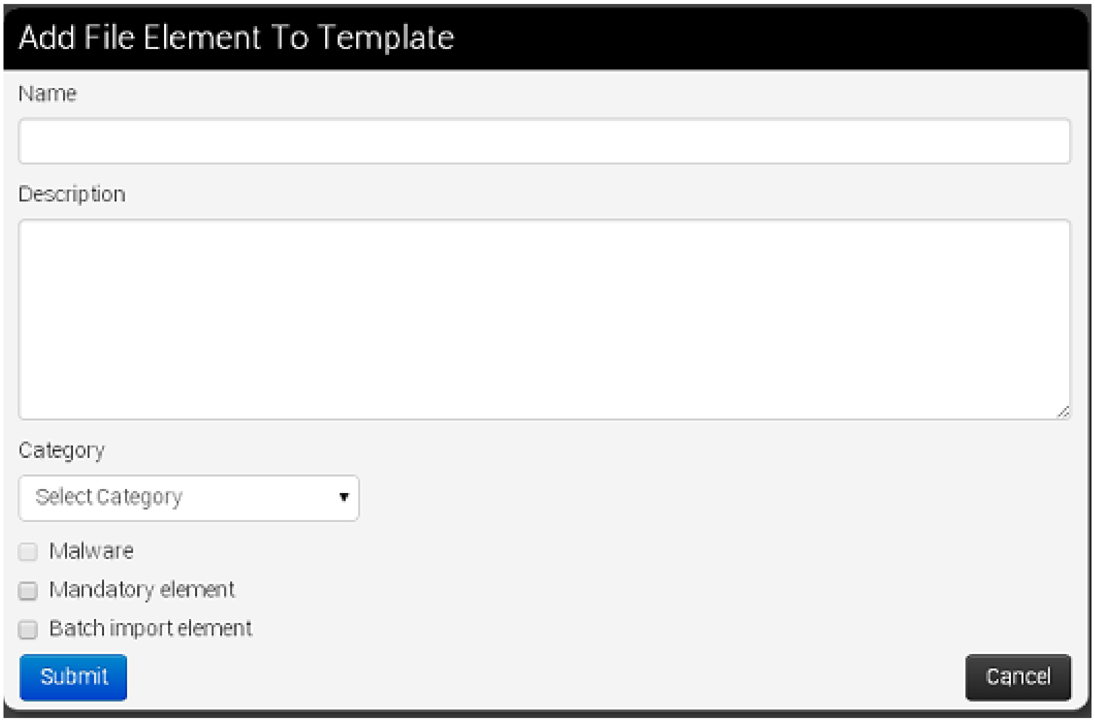
□ Mandatory element

□ Batch import element

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 elemnt 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).

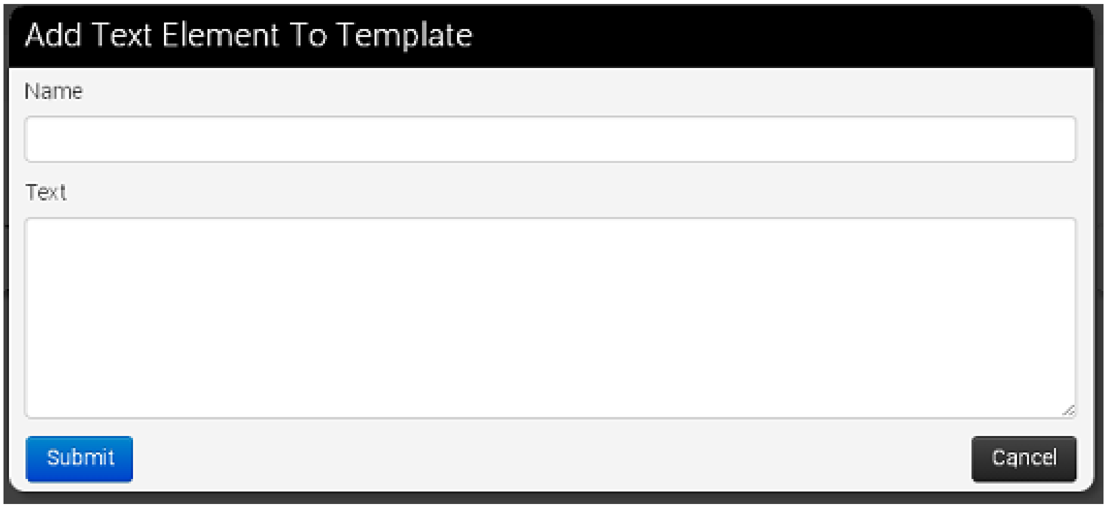
File Element



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



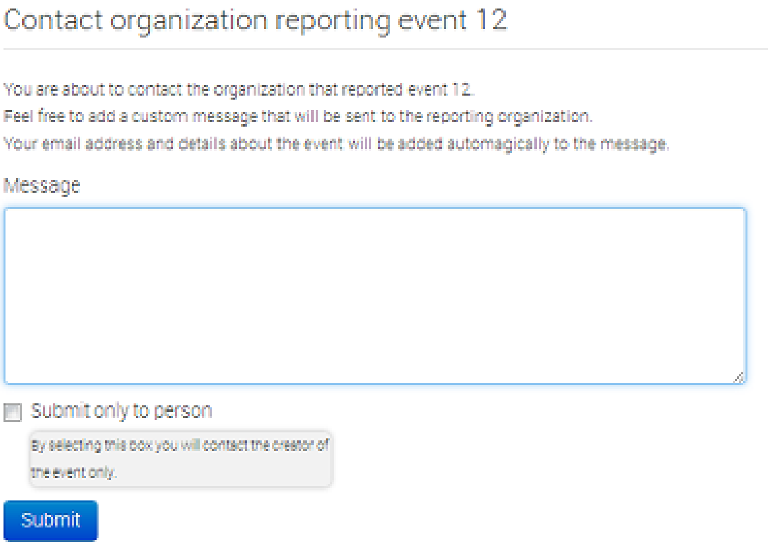
The following fields have to be filled out:

- **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 automagically to the message.

Message

□ Submit only to person

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

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 automation.

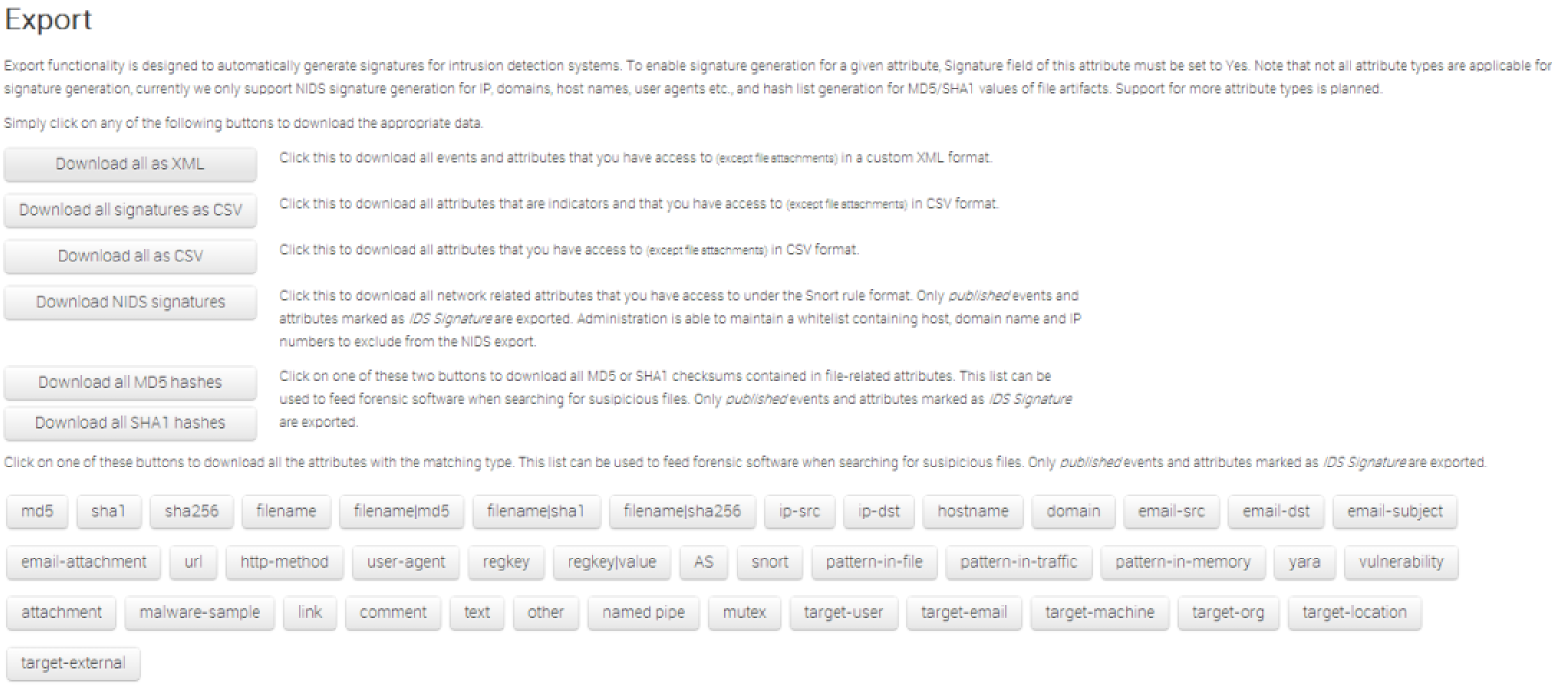
Exporting data:

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. (The setting on this instance is currently set to: `On`)

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 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.

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

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

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

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.

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 susipicious files. Only *published* events and attributes marked as *IDS Signature* are exported.

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 susipicious files. Only *published* events and attributes marked as *IDS Signature* are exported.

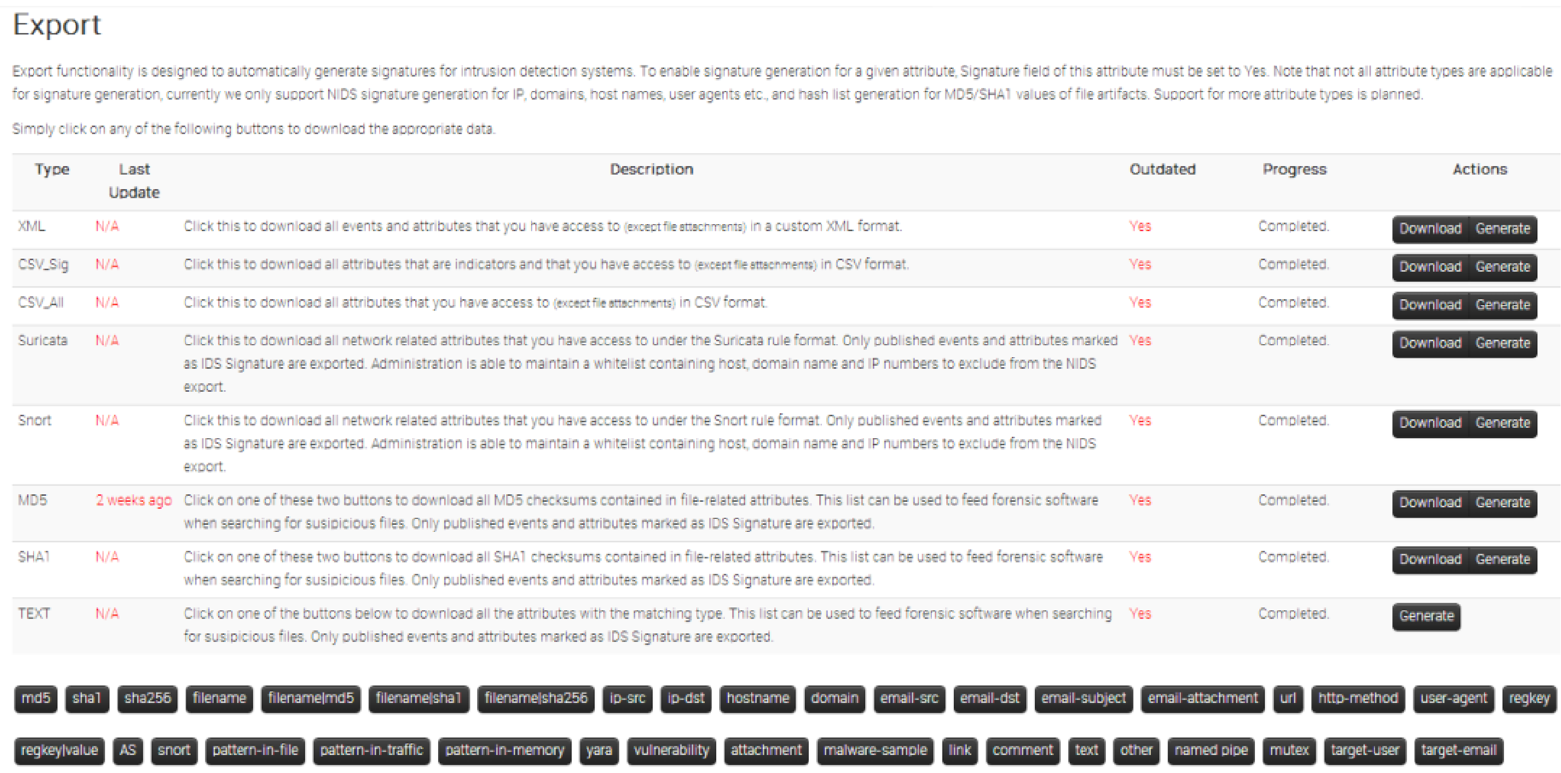
Export page with background jobs `enabled`

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

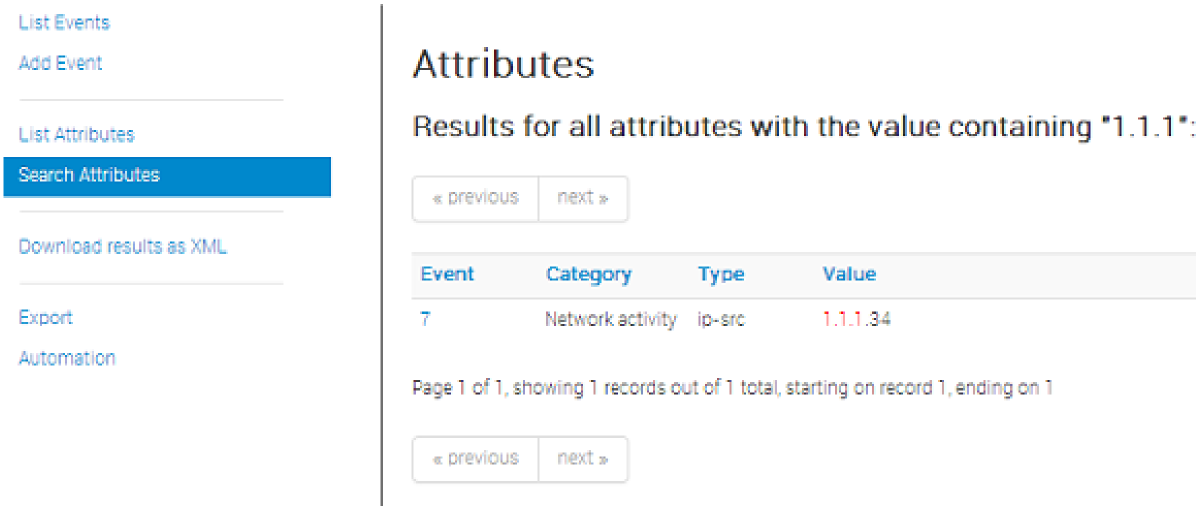
Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only 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.	Download Generate
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.	Download Generate
CSV_All	N/A	Click this to download all attributes that you have access to (except file attachments) in CSV format.	Yes	Completed.	Download Generate
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.	Download Generate
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.	Download Generate
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 susipicious files. Only published events and attributes marked as IDS Signature are exported.	Yes	Completed.	Download Generate
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 susipicious files. Only published events and attributes marked as IDS Signature are exported.	Yes	Completed.	Download Generate
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 susipicious files. Only published events and attributes marked as IDS Signature are exported.	Yes	Completed.	Generate

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.



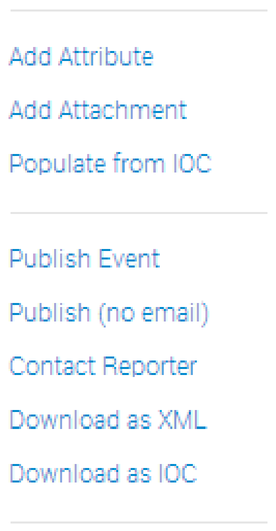
Attributes

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

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

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.



Add Attribute

Add Attachment

Populate from IOC

Publish Event

Publish (no email)

Contact Reporter

Download as XML

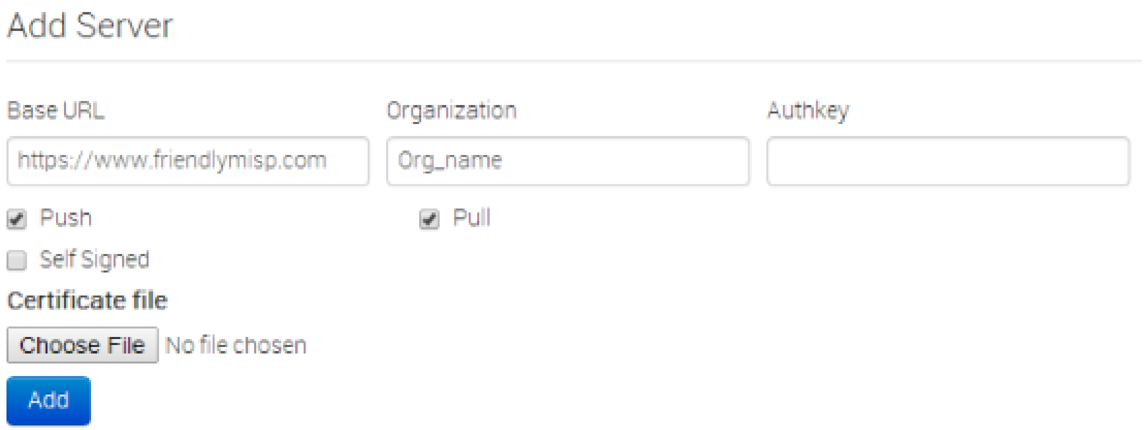
Download as IOC

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: https://www.friendlymisp.com

Organization: Org_name

Authkey:

☑ Push ☑ Pull

□ Self Signed

Certificate file

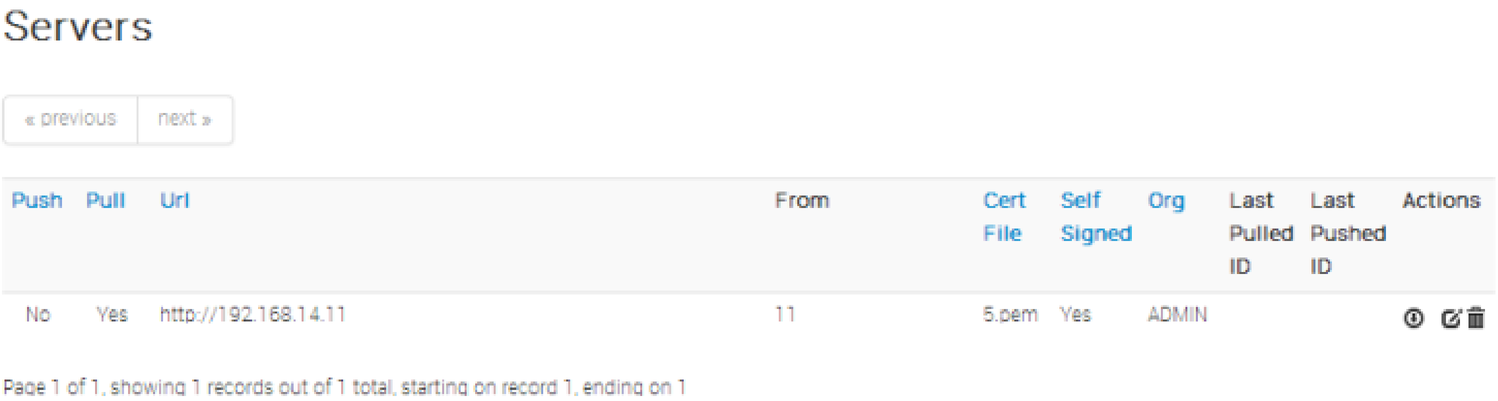
- **Base URL:** The URL of the remote server.
- **Organization:** The organisation that runs the remote server. It is very impoportant that this setting is filled out exactly as the organisation name set up in the bootstrap file of the remote instance.
- **Authkey:** The authentication key that you have 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

Push	Pull	Url	From	Cert File	Self Signed	Org	Last Pulled ID	Last Pushed ID	Actions
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) to access Events data.

Requests

Use any HTTP compliant library to perform requests. However to make clear you are doing a REST request you need to either specify the Accept type to application/xml, or append .xml to the url

The following table shows the relation of the request type and the resulting action:

HTTP format	URL	Controller action invoked
GET	/events	EventsController::index() (1)
GET	/events/123	EventsController::view(123) (2)
POST	/events	EventsController::add()
PUT	/events/123	EventsController::edit(123)

DELETE	/events/123	EventsController::delete(123)
POST	/events/123	EventsController::edit(123)

(1) Warning, there's a limit on the number of results when you call `index`.

(2) Attachments are included using base64 encoding below the `data` tag.

Authentication

REST being stateless you need to authenticate your request by using your authkey/apikey. Simply set the `Authorization` HTTP header.

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 http://192.168.56.11/events/123
```

And with the HTTP Headers:

```
Accept: application/xml
Authorization: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

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

```
<?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 http://192.168.56.11/events
Accept: application/xml
Authorization: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

And the request body:

```
<Event>
        <id>72</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>1393329599</publish_timestamp>
        <Attribute>
                <id>9577</id>
                <type>other</type>
                <category>Artifacts dropped</category>
                <to_ids>1</to_ids>
                <uuid>50aa54bd-adec-4544-b412-10f0ff32448e</uuid>
                <event_id>57</event_id>
                <distribution>1</distribution>
                <timestamp>1393328991</timestamp>
                <comment>This is an Attribute</comment>
                <value>Some_attribute</value>
                <ShadowAttribute />
        </Attribute>
        <ShadowAttribute />
        <RelatedEvent />
</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=a4ok3lr5p9n5drqj27025i4le3; 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>
```

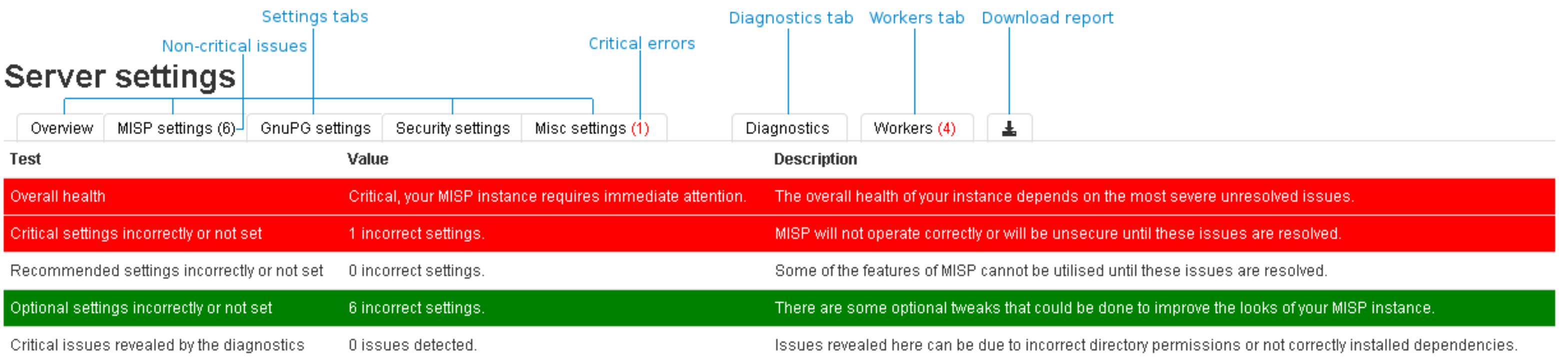
```
                <id>76</id>
                <org>NCIRC</org>
                <date>2014-03-04</date>
                <threat_level_id>1</threat_level_id>
                <info>Something concise</info>
                <published>1</published>
                <uuid>50aa54aa-f7a0-4d74-920d-10f0ff32448e</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 respone from requesting an invalid page

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

Server settings and diagnostics

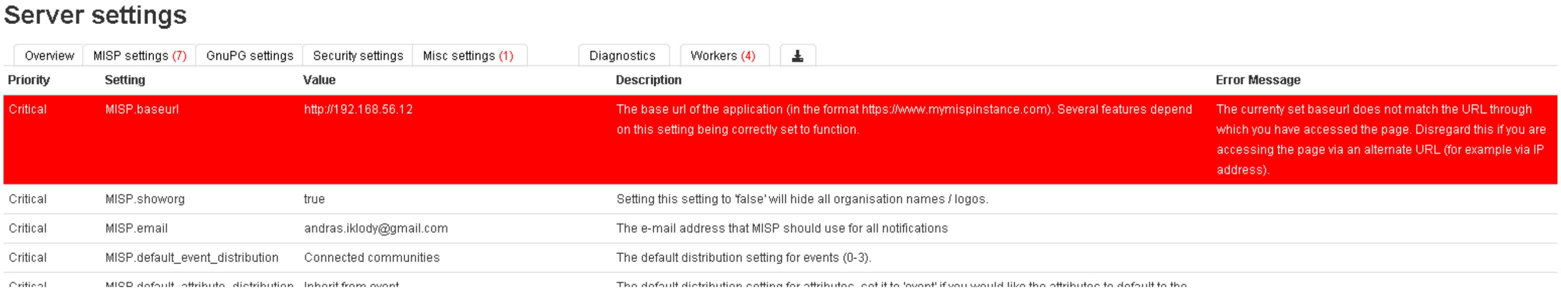
Since version 2.3, MISP has a settings and diagnostics tool that allows site-admins to manage and diagnose their MISP installation. You can access this by navigating to Administration - Server settings



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 ontop 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:

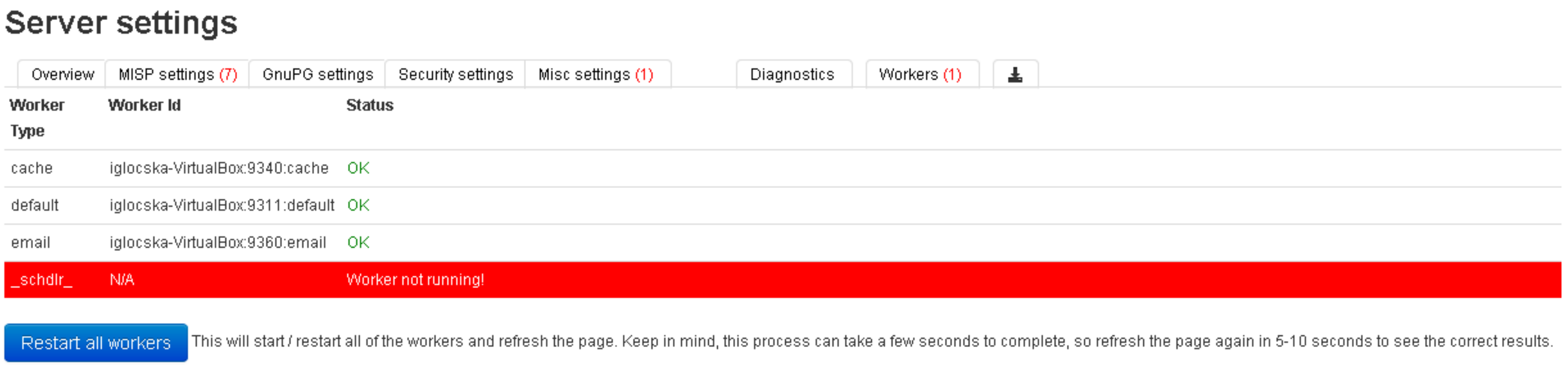
- **Overview**: General overview of the current state of your MISP installation
- **MISP settings**: Basic MISP settings. This includes the way MISP handles the default settings for distribution settings, whether background jobs are enabled, etc
- **GnuPG settings**: GPG related settings.
- **Security settings**: Settings controlling the brute-force protection and the application's salt key.
- **Misc settings**: You change the debug options here, but make sure 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 GPG 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 in JSON format, compiled of all of the settings visible in the tool.



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 currenty 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	The default distribution setting for attributes, set it to 'event' if you would like the attributes 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, then this field will let the user know what is wrong.



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

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 the workers using the restart all workers, 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 4 queues (cache, default, email 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.

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

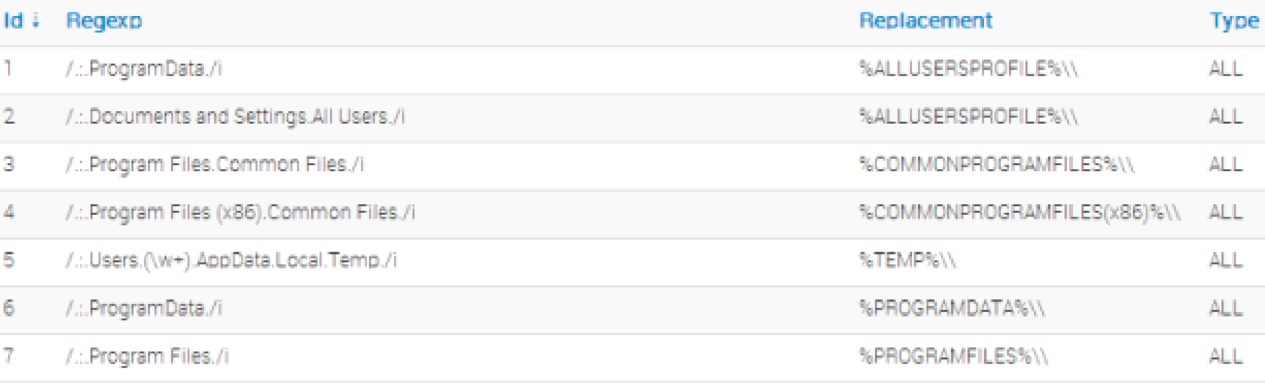
The system allows administrators to set up rules for regular expressions that will automatically alter newly entered or imported events (from GFI Sandbox).

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, which are made up of a regex pattern that the system searches for and a replacement for the detected pattern.



Id ⇣	Regexp	Replacement	Type
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

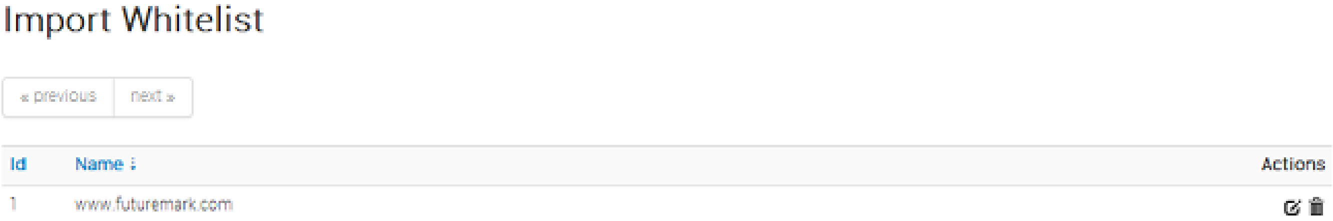
The signature whitelist view, accessible through the administration menu on the left, allows administrators to create and maintain a list of addresses that are whitelisted from ever being added to the NIDS signatures. Addresses listed here will be commented out when exporting the NIDS list.

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 pieces of information are 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

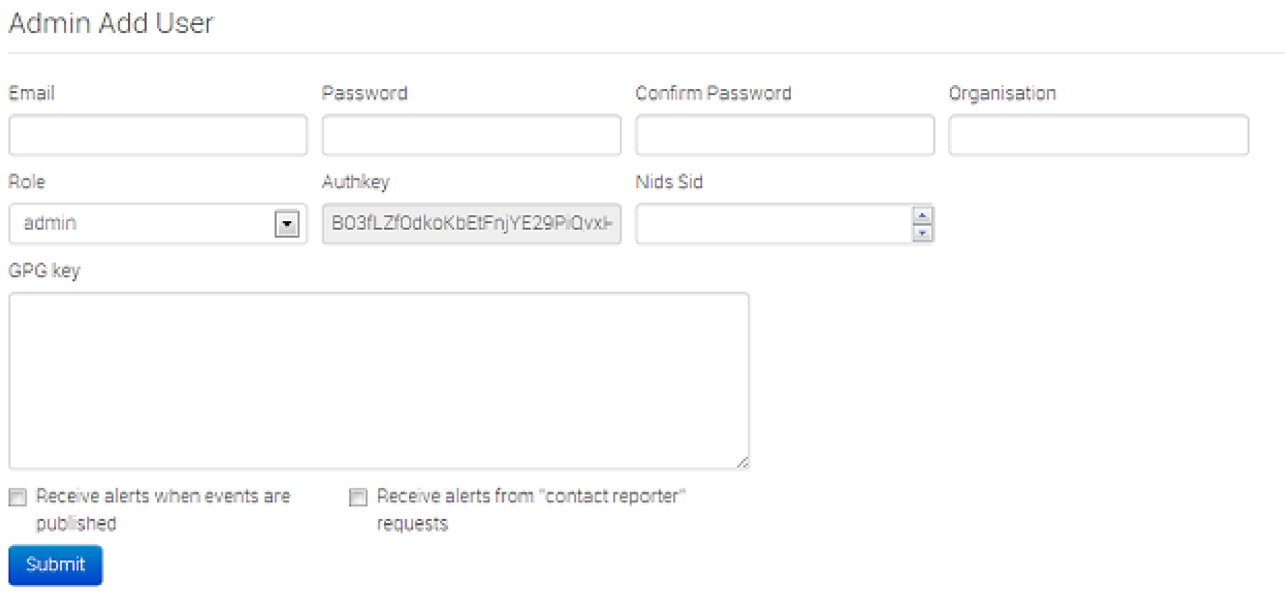
Id	Name ⇣	Actions
1	www.futuremark.com	✎ 🗑

Managing the users:

As an admin, you can set up new accounts for users, edit the profiles of users, delete them, or just have a look at all the viewers' profiles. Organisation admins are restricted to executing the same actions on their organisation's users only.

Adding a new user:

To add a new user, click on the New User button in the administration menu to the left and fill out the following fields in the view that is loaded:



Admin Add User

Email	Password	Confirm Password	Organisation
Role: admin	Authkey: B03fLZf0dkoKbEtFnjYE29PiQvxH	Nids Sid	

GPG key

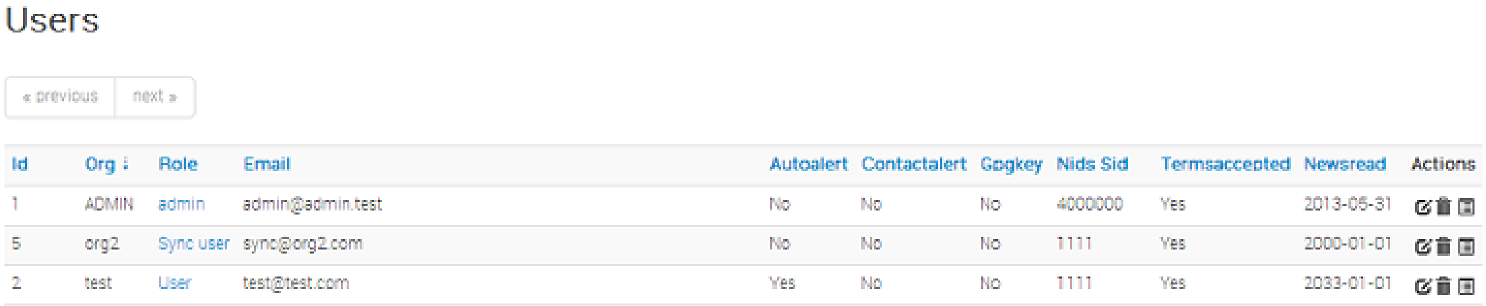
☐ Receive alerts when events are published

☐ Receive alerts from "contact reporter" requests

- **Email:** The user's e-mail address, this will be used as his/her login name and as an address to send all the automatic e-mails and e-mails sent by contacting the user as the reporter of an event.
- **Password:** A temporary password for the user that he/she should change after the first login. Make sure that it is at least 6 characters long, includes a digit or a special character and contains at least one upper-case and at least one lower-case character.
- **Confirm Password:** This should be an exact copy of the Password field.
- **Org:**The organisation of the user. Entering ADMIN into this field will give administrator privileges to the user. If you are an organisation admin, then this field will be unchangeable and be set to your own organisation.
- **Roles:** A drop-down list allows you to choose a role-group that the user should belong to. Roles define the privileges of the user. To learn more about roles, click here.
- **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.
- **Authkey:** This is assigned automatically and is the unique authentication key of the 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:** Nids ID, not yet implemented.
- **Gpgkey:** The key used for encrypting e-mails sent through the system.

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 be loaded with a list of all users and the following columns of information:



Users

Id	Org	Role	Email	Autoalert	Contactalert	Gpgkey	Nids Sid	Termsaccepted	Newsread	Actions
1	ADMIN	admin	admin@admin.test	No	No	No	4000000	Yes	2013-05-31	
5	org2	Sync user	sync@org2.com	No	No	No	1111	Yes	2000-01-01	
2	test	User	test@test.com	Yes	No	No	1111	Yes	2033-01-01	

- **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.
- **Autoalert:** Shows whether the user has subscribed to auto-alerts and is always receiving the mass-emails regarding newly published

events that he/she is eligible for.

- **ontactalert:** Shows whether the user has the subscription to contact reporter e-mails directed at his/her organisation turned on or off.
- **Gpgkey:** Shows whether the user has entered a Gpgkey yet.
- **Nids Sid:** Shows the currently assigned NIDS ID.
- **Termsaccepted:** This flag indicates whether the user has accepted the terms of use or not.
- **Newsread:** The last point in time when the user has looked at the news section of the system.
- **Action Buttons:** Here you can view a detailed view of a user, edit the basic details of a user (same view as the one used for creating a new user, but all the fields come filled out by default) or remove a user completely.

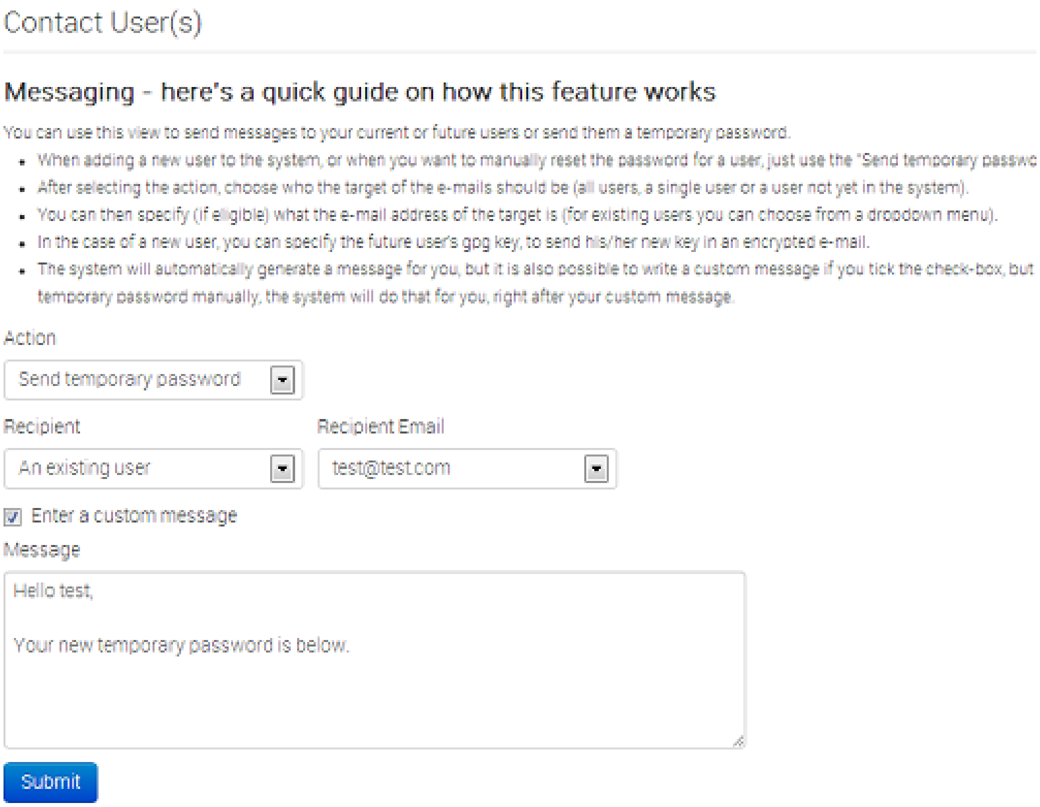
Editing a user:

To add a new user, click on the New User button in the administration menu to the left and fill out the following fields in the view that is loaded:

- **Email:** The user's e-mail address, this will be used as his/her login name and as an address to send all the automatic e-mails and e-mails sent by contacting the user as the reporter of an event.
- **Password:** It is possible to assign a new password manually for a user. For example, in case that he/she forgot the old one a new temporary one can be assigned. Make sure to check the "Change password" field if you do give out a temporary password, so that the user will be forced to change it after login.
- **Confirm Password:** This should be an exact copy of the Password field.
- **Org:**The organisation of the user. Entering ADMIN into this field will give administrator privileges to the user. If you are an organisation admin, then this field will be unchangeable and be set to your own organisation.
- **Roles:** A drop-down list allows you to choose a role-group that the user should belong to. Roles define the privileges of the user. To learn more about roles, click here.
- **Receive alerts when events are published:** This option will subscribe the user to automatically generated e-mails whenever an event is published.
- **Receive alerts from "contact reporter" requests:** This option will subscribe the 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 user.
- **Authkey:** It is possible to request a new authentication key for the user.
- **NIDS Sid:** Nids ID, not yet implemented.
- **Termsaccepted:** 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.
- **Gpgkey:** The key used for encrypting e-mails sent through the system.

Contacting a user:

Site admins can use the "Contact users" feature to send all or an individual user an e-mail. Users that have a PGP 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 passwo
- 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 temporary password manually, the system will do that for you, right after your custom message.

Action: Send temporary password

Recipient: An existing user

Recipient Email: test@test.com

☑ Enter a custom message

Message:

Hello test,

Your new temporary password is below.

- **Action:** This defines the type of the e-mail, 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.
- **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 PGP public key).
- **Subject:** In the case of a custom e-mail, you can enter a subject line here.
- **Subject:** In the case of a custom e-mail, you can enter a subject line here.
- **Custom message checkbox:** This is available for password resets, 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 will, in addition to your own message, will be signed in the name of the instance's host organisation's support team, will 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 PGP signature for users that have a PGP key set (and thus are eligible for an encrypted e-mail).

Managing the roles

Privileges are assigned to users by assigning them to rule groups, which use one of four options determining what they can do with events and four additional privilege elevating settings. The four options for event manipulation are: Read Only, Manage My Own Events, Manage Organisation Events, Manage & Publish Organisation Events. The extra privileges are admin, sync, authentication key usage and audit permission

- **Read Only:** This allows the 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:** The second option, gives its users rights 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:** This last setting, gives users the right to do all of the above and also to publish the events of their organisation.
- **Perm sync:** This setting allows 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.

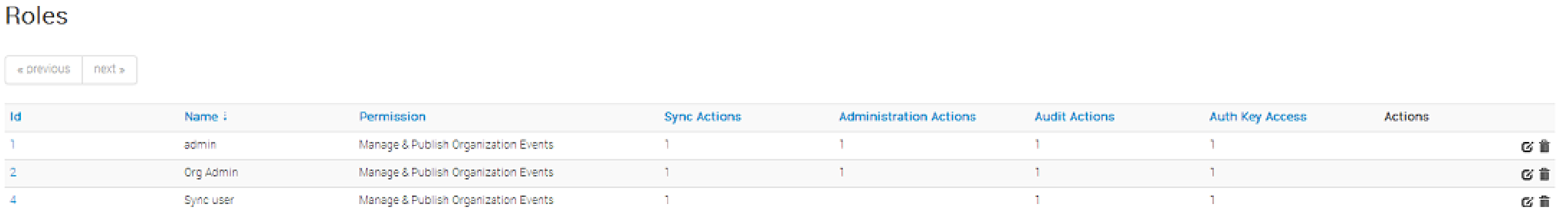
- **Perm auth:** This setting enables the authentication key of the role's users to be used for rest requests.
- **Perm admin:** Gives the user limited administrator privileges, this setting is used for the organisation admins.
- **Perm site admin:** Gives the user full administrator privileges, this setting is used for the site 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 regexp access:** Allows the users with 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 tagger:** Allows the user with this permission to create custom tags and assign them to events.

Creating roles:

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

Listing roles:

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



Id	Name ⁝	Permission	Sync Actions	Administration Actions	Audit Actions	Auth Key Access	Actions
1	admin	Manage & Publish Organization Events	1	1	1	1	
2	Org Admin	Manage & Publish Organization Events	1	1	1	1	
4	Sync user	Manage & Publish Organization Events	1		1	1	

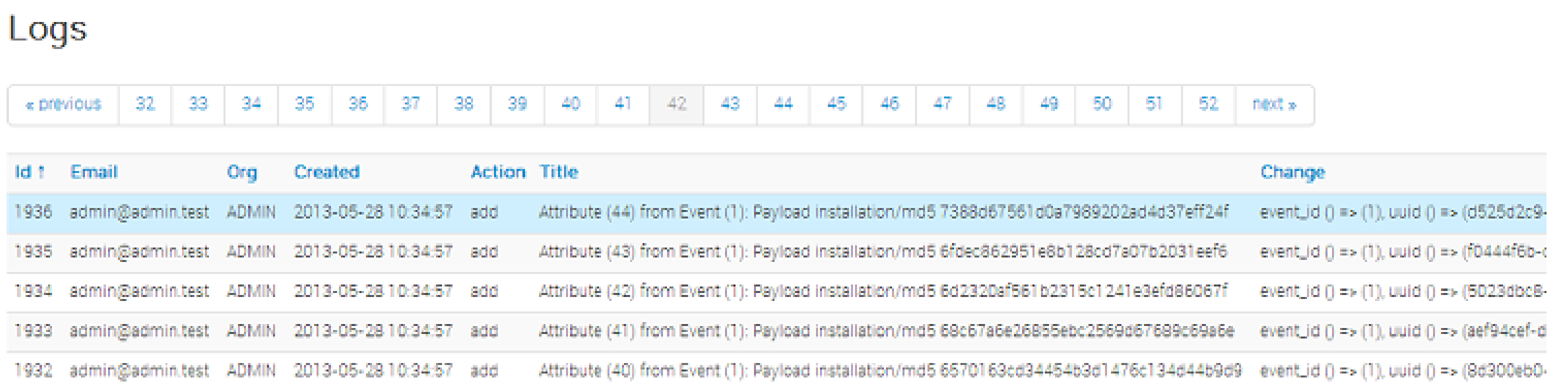
Using the logs of MISP

Users with audit permissions are able to browse or search the 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 the logs:

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



Logs

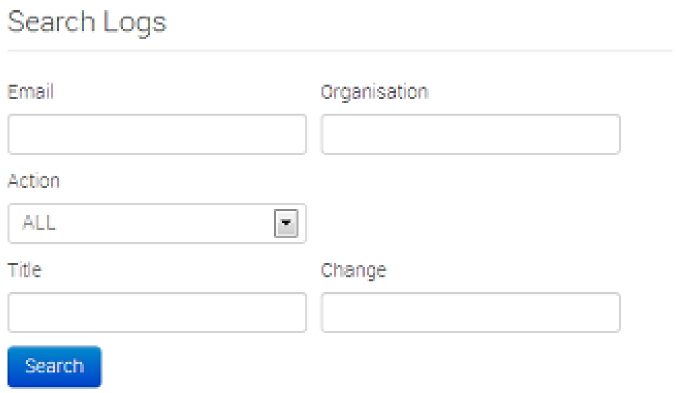
« previous | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | next »

Id ↑	Email	Org	Created	Action	Title	Change
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 6fdec862951e8b128cd7a07b2031eef6	event_id () => (1), uuid () => (f0444f6b-c
1934	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (42) from Event (1): Payload installation/md5 6d2320af561b2315c1241e3efd86067f	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 68c67a6e26855ebc2569d67689c69a6e	event_id () => (1), uuid () => (aef94cef-d
1932	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (40) from Event (1): Payload installation/md5 6570163cd34454b3d1476c134d44b9d9	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 filled out for entries with the action being add or edit. 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),...

Searching the 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):



Search Logs

Email

Organisation

Action

ALL

Title

Change

- **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 / attribute's name of the event target.
- **Change:** With the help of this field, you can search for various specific changes or changes to certain variables (such as published will find all the log entries where an event has gotten published, ip-src will find all attributes where a source IP address has been entered / edited, etc).

Administrative 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. Make sure to check this section after upgrading to a new version, just in case there is a new upgrade script in there - though if this is the case it will be mentioned in the upgrade instructions.

Background Processing

If enabled, MISP can delegate a lot of the time intensive tasks to the background workers. These will then be executed in order, 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.CakeResque` (for example: `./cake CakeResque.CakeResque tail`):

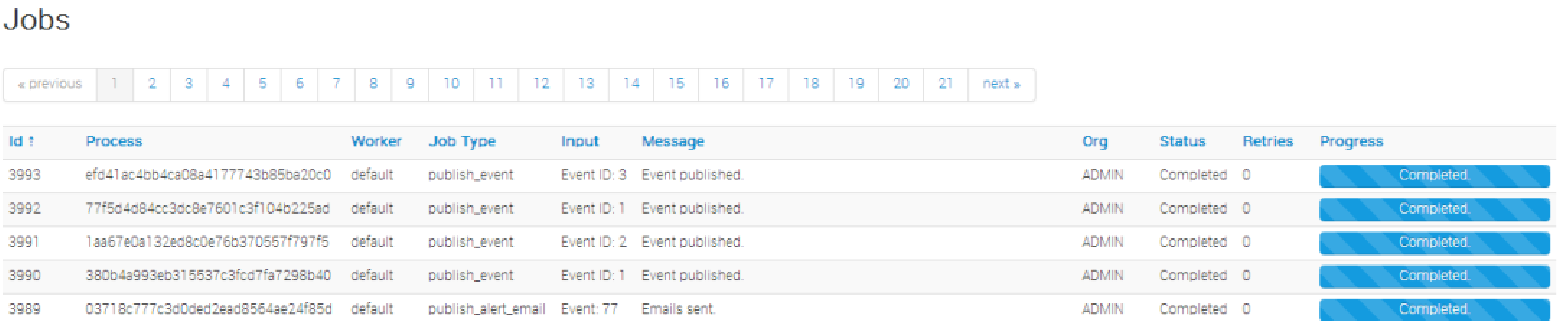
- **tail**: tail the various log files that CakeResque creates, just choose the one from the list that you are interested in.
- **cleanup**: terminate the job that a worker is working on immediately. You will be presented with a choice of workers to choose from when executing this command.
- **clear**: Clear the queue of a worker immediately.
- **stats**: shows some statistics about your workers including the count of successful and failed jobs.

The other commands should not be needed, 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 currently and in the 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 introduced automatic delayed retries for the background processing to add resilience.
- **Progress**: A progress bar showing how the job is coming along.

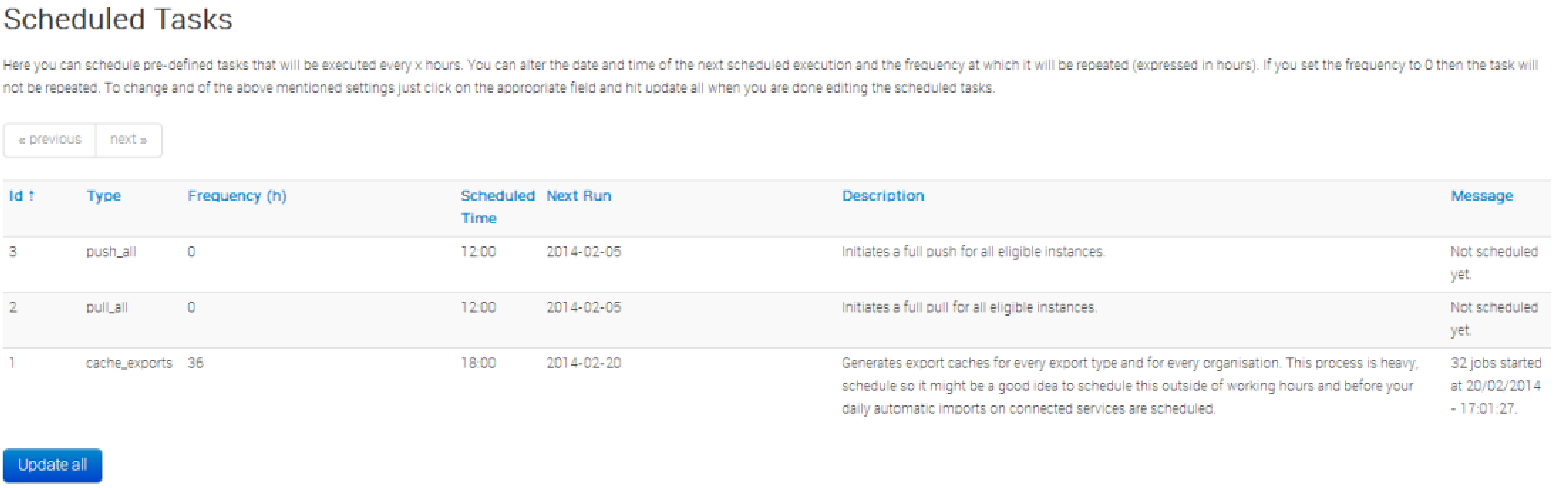


Id ↕	Process	Worker	Job Type	Input	Message	Org	Status	Retries	Progress
3993	efd41ac4bb4ca08a4177743b85ba20c0	default	publish_event	Event ID: 3	Event published.	ADMIN	Completed	0	Completed.
3992	77f5d4d84cc3dc8e7601c3f104b225ad	default	publish_event	Event ID: 1	Event published.	ADMIN	Completed	0	Completed.
3991	1aa67e0a132ed8c0e76b370557f797f5	default	publish_event	Event ID: 2	Event published.	ADMIN	Completed	0	Completed.
3990	380b4a993eb315537c3fcd7fa7298b40	default	publish_event	Event ID: 1	Event published.	ADMIN	Completed	0	Completed.
3989	03718c777c3d0ded2ead8564ae24f85d	default	publish_alert_email	Event: 77	Emails sent.	ADMIN	Completed	0	Completed.

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 and of the above mentioned settings just click on the appropriate field and hit update all when you are done editing the scheduled tasks.

Id ↕	Type	Frequency (h)	Scheduled Time	Next Run	Description	Message
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.

Attribute Categories and Types

Attribute Categories vs Types

Category	Internal reference	Targeting data	Antivirus detection	Payload delivery	Artifacts dropped	Payload installation	Persistence mechanism	Network activity	Payload type	Attribution	External analysis	Other	Category
md5				X	X	X					X		**md5**
sha1				X	X	X					X		**sha1**
sha256				X	X	X					X		**sha256**
filename				X	X	X	X				X		**filename**
filename|md5				X	X	X					X		**filename|md5**
filename|sha1				X	X	X					X		**filename|sha1**
filename|sha256				X	X	X					X		**filename|sha256**
ip-src				X				X			X		**ip-src**
ip-dst				X				X			X		**ip-dst**
hostname				X				X			X		**hostname**
domain				X				X			X		**domain**
email-src				X									**email-src**
email-dst				X				X					**email-dst**
email-subject				X									**email-subject**
email-attachment				X									**email-attachment**
url				X				X			X		**url**
http-method								X					**http-method**
user-agent				X				X			X		**user-agent**
regkey					X		X				X		**regkey**
regkey|value					X		X				X		**regkey|value**
AS				X				X			X		**AS**
snort								X			X		**snort**
pattern-in-file				X	X	X		X			X		**pattern-in-file**
pattern-in-traffic				X		X		X			X		**pattern-in-traffic**
pattern-in-memory					X	X					X		**pattern-in-memory**
yara				X	X	X							**yara**
vulnerability				X		X					X		**vulnerability**
attachment			X	X	X	X		X			X		**attachment**
malware-sample				X	X	X					X		**malware-sample**
link	X		X	X							X		**link**
comment	X	X	X	X	X	X	X	X	X	X	X	X	**comment**
text	X		X	X	X	X	X	X	X	X	X	X	**text**
other	X		X	X	X	X	X	X	X	X	X	X	**other**
named pipe					X								**named pipe**
mutex					X								**mutex**

target-user		X											**target-user**
target-email		X											**target-email**
target-machine		X											**target-machine**
target-org		X											**target-org**
target-location		X											**target-location**
target-external		X											**target-external**
Category	**Internal reference**	**Targeting data**	**Antivirus detection**	**Payload delivery**	**Artifacts dropped**	**Payload installation**	**Persistence mechanism**	**Network activity**	**Payload type**	**Attribution**	**External analysis**	**Other**	**Category**

Categories

Category	Description
Internal reference	Reference used by the publishing party (e.g. ticket number)
Targeting data	Targeting information to include recipient email, infected machines, department, and or locations.
Antivirus detection	List of anti-virus vendors detecting the malware or information on detection performance (e.g. 13/43 or 67%). Attachment with list of detection or link to VirusTotal could be placed here as well.
Payload delivery	Information about the way the malware payload is initially delivered, for example information about the email or web-site, vulnerability used, originating IP etc. Malware sample itself should be attached here.
Artifacts dropped	Any artifact (files, registry keys etc.) dropped by the malware or other modifications to the system
Payload installation	Location where the payload was placed in the system and the way it was installed. For example, a filename|md5 type attribute can be added here like this: c:\windows\system32\malicious.exe|41d8cd98f00b204e9800998ecf8427e.
Persistence mechanism	Mechanisms used by the malware to start at boot. This could be a registry key, legitimate driver modification, LNK file in startup
Network activity	Information about network traffic generated by the malware
Payload type	Information about the final payload(s). Can contain a function of the payload, e.g. keylogger, RAT, or a name if identified, such as Poison Ivy.
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 Examples: pdf-parser output, automated sandbox analysis, reverse engineering report.
Other	Attributes that are not part of any other category

Types

Type	Description
md5	You are encouraged to use filename|md5 instead. A checksum in md5 format, only use this if you don't know the correct filename
sha1	You are encouraged to use filename|sha1 instead. A checksum in sha1 format, only use this if you don't know the correct filename
sha256	You are encouraged to use filename|sha256 instead. A checksum in sha256 format, only use this if you don't know the correct filename
filename	Filename
filename|md5	A filename and an md5 hash separated by a | (no spaces)
filename|sha1	A filename and an sha1 hash separated by a | (no spaces)
filename|sha256	A filename and an sha256 hash separated by a | (no spaces)
ip-src	A source IP address of the attacker
ip-dst	A destination IP address of the attacker or C&C server. Also set the IDS flag on when this IP is hardcoded in malware
hostname	A full host/dnsname of an attacker. Also set the IDS flag on when this hostname is hardcoded in malware
domain	A domain name used in the malware. Use this instead of hostname when the upper domain is important or can be used to create links between events.
email-src	The email address (or domainname) used to send the malware.
email-dst	A recipient email address that is not related to your constituency.

email-subject	The subject of the email
email-attachment	File name of the email attachment.
url	url
http-method	HTTP method used by the malware (e.g. POST, GET, ...).
user-agent	The user-agent used by the malware in the HTTP request.
regkey	Registry key or value
regkey|value	Registry value + data separated by |
AS	Autonomous system
snort	An IDS rule in Snort rule-format. This rule will be automatically rewritten in the NIDS exports.
pattern-in-file	Pattern in file that identifies the malware
pattern-in-traffic	Pattern in network traffic that identifies the malware
pattern-in-memory	Pattern in memory dump that identifies the malware
yara	Yara signature
vulnerability	A reference to the vulnerability used in the exploit
attachment	Please upload files using the *Upload Attachment* button.
malware-sample	Please upload files using the *Upload Attachment* button.
link	Link to an external information
comment	Comment or description in a human language. This will not be correlated with other attributes (NOT IMPLEMENTED YET)
text	Name, ID or a reference
other	Other attribute
named pipe	Named pipe, use the format \\.\pipe\
mutex	Mutex, use the format \BaseNamedObjects\
target-user	Attack Targets Username(s)
target-email	Attack Targets Email(s)
target-machine	Attack Targets Machine Name(s)
target-org	Attack Targets Department or Orginization(s)
target-location	Attack Targets Physical Location(s)
target-external	External Target Orginizations Affected by this Attack

Automation

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 artifacts. Support for more attribute types is planned. To 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-authentiation.
Make sure you keep that key secret as it gives access to the entire database !

Your current key is: `mabfFjft0auFM3bj2FhJQGmclxT3ASvW2HcH0rb1` . You can reset this key.

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.

Please use the use the following header:
`Authorization: mabfFjft0auFM3bj2FhJQGmclxT3ASvW2HcH0rb1`

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:

```
http://192.168.56.11/events/xml/download
```

If you only want to fetch a specific event append the eventid number:

```
http://192.168.56.11/events/xml/download/1
```

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

JSON:

```
http://192.168.56.11/events/xml/download.json
```

`{"request": {"eventid":["!51","!62"],"withAttachment":false,"tags":["APT1","!OSINT"],"from":false,"to":"2015-01-01"}}`

XML:

```
http://192.168.56.11/events/xml/download
```

`<request><eventid>!51</eventid><eventid>!62</eventid><withAttachment>false</withAttachment><tags>APT1</tags><tags>!OSINT</tags><from>false</from><to>2015-01-01</to></`

The xml download also accepts two additional the following optional parameters in the url:

```
http://192.168.56.11/events/xml/download/[eventid]/[withattachments]/[tags]/[from]/[to]
```

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:
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)

```
http://192.168.56.11/events/xml/download/false/true/tag1&&tag2&&!tag3
```

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:

```
http://192.168.56.11/events/csv/download/
```

You can specify additional flags for CSV exports as follows::

```
http://192.168.56.11/events/csv/download/[eventid]/[ignore]/[tags]/[category]/[type]/[includeInfo]/[from]/[to]
```

eventid: Restrict the download to a single event
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:
ignore: Setting this flag to true will include attributes that are not marked "to_ids".
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)

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:

```
http://192.168.56.11/events/csv/download/false/false/tag1&&tag2&&!tag3/Network%20Activity/domain
```

To export the attributes of all events that are of the type "domain", use the following syntax:

```
http://192.168.56.11/events/csv/download/false/false/false/false/domain
```

NIDS rules export

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

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

```
http://192.168.56.11/events/nids/suricata/download
http://192.168.56.11/events/nids/snort/download
```

The full API syntax is as follows:

```
http://192.168.56.11/events/nids/[format]/download/[eventid]/[frame]/[tags]/[from]/[to]
```

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 unnecasary 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:
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)

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:

```
http://192.168.56.11/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.

Hash 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 the following files:

md5

```
http://192.168.56.11/events/hids/md5/download
```

sha1

```
http://192.168.56.11/events/hids/sha1/download
```

The API's full format is as follows:

```
http://192.168.56.11/events/hids/[format]/download/[tags]/[from]/[to]
```

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:
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)

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

```
http://192.168.56.11/events/hids/sha1/download/tag1
```

STIX export

You can export MISP events in Mitre's STIX format (to read more about STIX, click here). The STIX XML export is currently very slow and can lead to timeouts with larger events or collections of events. The JSON return format does not suffer from this issue. Usage:

```
http://192.168.56.11/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:

```
http://192.168.56.11/events/stix/download/[id]/[withAttachments]/[tags]/[from]/[to]
```

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:
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)

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

JSON:

```
http://192.168.56.11/events/stix/download.json
```

```
{"request": {"id":["!51","!62"],"withAttachment":false,"tags":["APT1","!OSINT"],"from":false,"to":"2015-01-01"}}
```

XML:

```
http://192.168.56.11/events/stix/download
```

```
<request><id>!51</id><id>!62</id><withAttachment>false</withAttachment><tags>APT1</tags><tags>!OSINT</tags><from>false</from><to>2015-01-01</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:

```
http://192.168.56.11/events/stix/download/!51&&!62/false/APT1&&!OSINT/2015-01-01
```

To export the same events using a POST request use:

```
http://192.168.56.11/events/stix/download.json
```

Together with this JSON object in the POST message:

```
{"request": {"id":["!51","!62"],"tags":["APT1","!OSINT"],"from":"2015-01-01"}}
```

XML is automatically assumed when using the stix export:

```
http://192.168.56.11/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>2015-01-01</from></request>
```

Text export

An automatic export of all attributes of a specific type to a plain text file.

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

```
http://192.168.56.11/attributes/text/download/md5
http://192.168.56.11/attributes/text/download/sha1
http://192.168.56.11/attributes/text/download/sha256
http://192.168.56.11/attributes/text/download/filename
http://192.168.56.11/attributes/text/download/filename|md5
http://192.168.56.11/attributes/text/download/filename|sha1
http://192.168.56.11/attributes/text/download/filename|sha256
http://192.168.56.11/attributes/text/download/ip-src
http://192.168.56.11/attributes/text/download/ip-dst
http://192.168.56.11/attributes/text/download/hostname
http://192.168.56.11/attributes/text/download/domain
http://192.168.56.11/attributes/text/download/email-src
http://192.168.56.11/attributes/text/download/email-dst
http://192.168.56.11/attributes/text/download/email-subject
http://192.168.56.11/attributes/text/download/email-attachment
http://192.168.56.11/attributes/text/download/url
http://192.168.56.11/attributes/text/download/http-method
http://192.168.56.11/attributes/text/download/user-agent
http://192.168.56.11/attributes/text/download/regkey
http://192.168.56.11/attributes/text/download/regkey|value
http://192.168.56.11/attributes/text/download/AS
http://192.168.56.11/attributes/text/download/snort
http://192.168.56.11/attributes/text/download/pattern-in-file
http://192.168.56.11/attributes/text/download/pattern-in-traffic
http://192.168.56.11/attributes/text/download/pattern-in-memory
http://192.168.56.11/attributes/text/download/yara
http://192.168.56.11/attributes/text/download/vulnerability
http://192.168.56.11/attributes/text/download/attachment
http://192.168.56.11/attributes/text/download/malware-sample
http://192.168.56.11/attributes/text/download/link
http://192.168.56.11/attributes/text/download/comment
http://192.168.56.11/attributes/text/download/text
http://192.168.56.11/attributes/text/download/other
http://192.168.56.11/attributes/text/download/named pipe
http://192.168.56.11/attributes/text/download/mutex
http://192.168.56.11/attributes/text/download/target-user
http://192.168.56.11/attributes/text/download/target-email
http://192.168.56.11/attributes/text/download/target-machine
http://192.168.56.11/attributes/text/download/target-org
http://192.168.56.11/attributes/text/download/target-location
http://192.168.56.11/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:

```
http://192.168.56.11/attributes/text/download/ip-src/tag1&&!tag2
```

As of version 2.3.38, it is possible to restrict the text exports on two 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.

```
http://192.168.56.11/attributes/text/download/[type]/[tags]/[event_id]/[allowNonIDS]/[from]/[to]
```

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). For example, to include tag1 and tag2 but exclude tag3 you would use:
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: 2015-02-03)
to: Events with the date set to a date before the one specified in the to field (format: 2015-02-03)
For example, to retrieve all attributes for event #5, including non IDS marked attributes too, use the following line:

```
http://192.168.56.11/attributes/text/download/all/null/5/true
```

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:

```
http://192.168.56.11/events/restSearch/download/[value]/[type]/[category]/[org]/[tag]/[quickfilter]/[from]/[to]
```

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 idenfitier.
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:
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: 2015-02-03)
to: Events with the date set to a date before the one specified in the to field (format: 2015-02-03)

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:

```
http://192.168.56.11/events/restSearch/download
```

POST message payload (XML):

```
<request><value>red october</value><searchall>1</searchall></request>
```

POST message payload (json):

```
{"request": {"value":"red october","searchall":1}}
```

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 idenfitier.
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:
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)

```
http://192.168.56.11/attributes/restSearch/download/[value]/[type]/[category]/[org]/[tag]/[from]/[to]
```

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:

```
http://192.168.56.11/attributes/restSearch/download/192.168&&127.0&&!0.1/ip-src/false/ADMIN/!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:

```
http://192.168.56.11/attributes/restSearch/download/192.168.1.1|16/ip-src/null/ADMIN
```

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:

```
http://192.168.56.11/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:

```
http://192.168.56.11/attributes/returnAttributes/download/25/md5&&sha256&&!filename/true
```

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:

```
http://192.168.56.11/attributes/downloadAttachment/download/[Attribute_id]
```