CyDefSIG: Cyber Defence Signature Sharing Platform, version: 1.1.1

Table of contents

1. General Layout
2. User Management and Global Actions
3. Using the system
4. Administration
   - a. Import Regexp
   - b. Signature Whitelist
   - c. User Management
   - d. Role Management
   - e. Logging
5. Categories and Types

Import Regexp

The system allows administrators to set up rules for regular expressions that will automatically altered 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 standardise the file paths (changing C:\Users\UserName\Appdata\Roaming\file.exe to %APPDATA%\Roaming\file.exe). The second use is blocking, if just the regexp is given and no replacement, any event or attribute containing info or value conform the regexp will not be added.

Adding and modifying entries

Administrators can add, edit or delete Import Regexp rules, which are made up of a regexp pattern that the system searches for and a replacement for the detected pattern.

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.

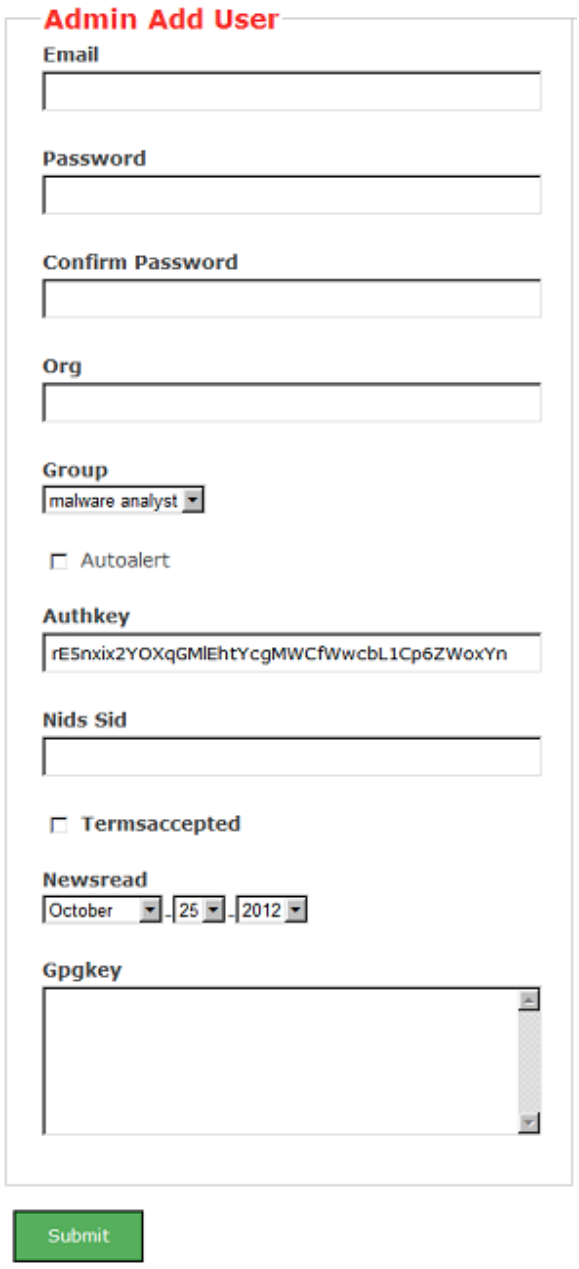
Managing the list:

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.

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.

Adding a new user:

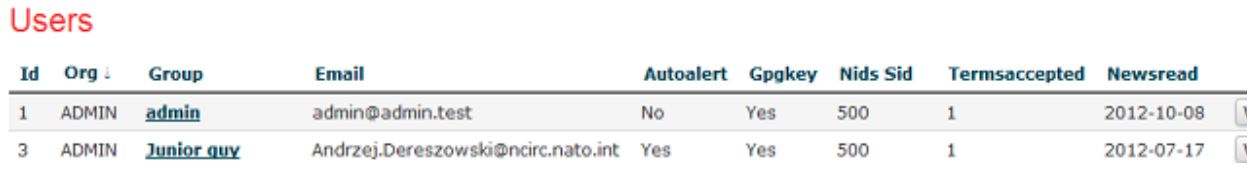


To add a new user, click on the New User button in the administration menu to the left and fill out the following fields in the view that is loaded:

- ***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.
- ***Roles:*** A drop-down list allows you to choose a role-roup that the user should belong to. Roles define the privileges of the user. To learn more about roles, **click here**.
- ***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 (as described in section xxyyzz).
- ***NIDS Sid:*** Nids ID, not yet implemented.
- ***Termsaccepted:*** Indicates whether the user has accepted the terms of use already or not.
- ***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	Group	Email	Autoalert	Gpgkey	Nids Sid	Termsaccepted	Newsread
1	ADMIN	admin	admin@admin.test	No	Yes	500	1	2012-10-08
3	ADMIN	Junior guy	Andrzej.Dereszowski@ncirc.nato.int	Yes	Yes	500	1	2012-07-17

- ***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 auto-alerts enabled and is always receiving the mass-emails that he is eligible for.
- ***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.

Managing the roles

Privileges are assigned to users by assigning them to role-roles, which use one of four options to determine what the users belonging to them are able to do on the site. The four options are: Read Only, Manage My Own Events, Manage Organisation Events, Manage & Publish Organisation Events.

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.

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 four check-boxes, one for each permission flag.

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	Actions	
2	admin	Manage & Publish Organization Events	Edit	Delete
4	guest	Read Only	Edit	Delete
3	IDS analyst	Manage & Publish Organization Events	Edit	Delete

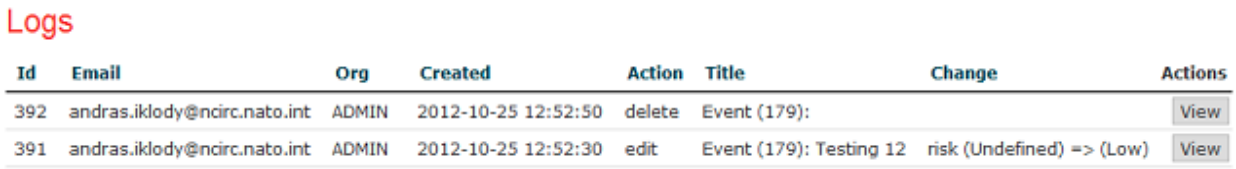
---

Using the logs of MISP

Admins are able to browse or search the logs that MISP automatically appends each time any action is taken that alters the data contained within the system (or if a user logs in and out).

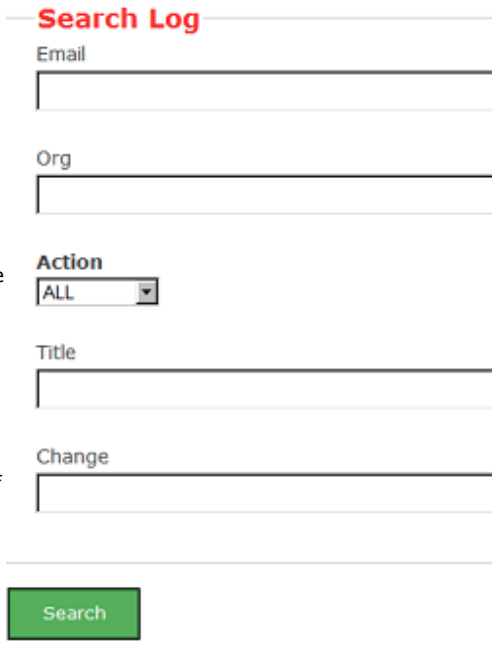
Browsing the logs:

Listing all the log entries will show the following columns:



- ***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):

- ***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).