Events

Events

Introduction

Pandora FMS event system allows you to see a real time log containing all the events that take place in monitored systems. By default, in the event view you will see a screenshot of what is happening at that moment.

Events are the record and an essential part of monitoring systems.

Events are classified according to their severity:

- 0 Maintenance (White/Gray).
- 1 Informative (Blue).
- 2 Normal (Green).
- 3 Warning (Yellow).
- 4 Critical (Red).
- 5 Minor (Pink).
- 6 Major (Brown).

The following actions can be performed on events:

- Change its status (validated or in progress).
- Change owner.
- Delete.
- Show additional information.
- Add a comment: Any text that provides information and can be used to filter searches. If needed, URLs may be added in MarkDown format: `[]()`, even for the Event Custom ID field.
- Make customizable responses.

General information

Events are managed through the menu Operations → Events → View Events.

The event viewer shows a summary of each event and sometimes there is other associated data, such as the agent module that generated the event, the group, tags associated to the module, etc. You may also sort events by identifier, status or name, among other fields.

By clicking on the magnifying glass icon corresponding to each item you will get more details.

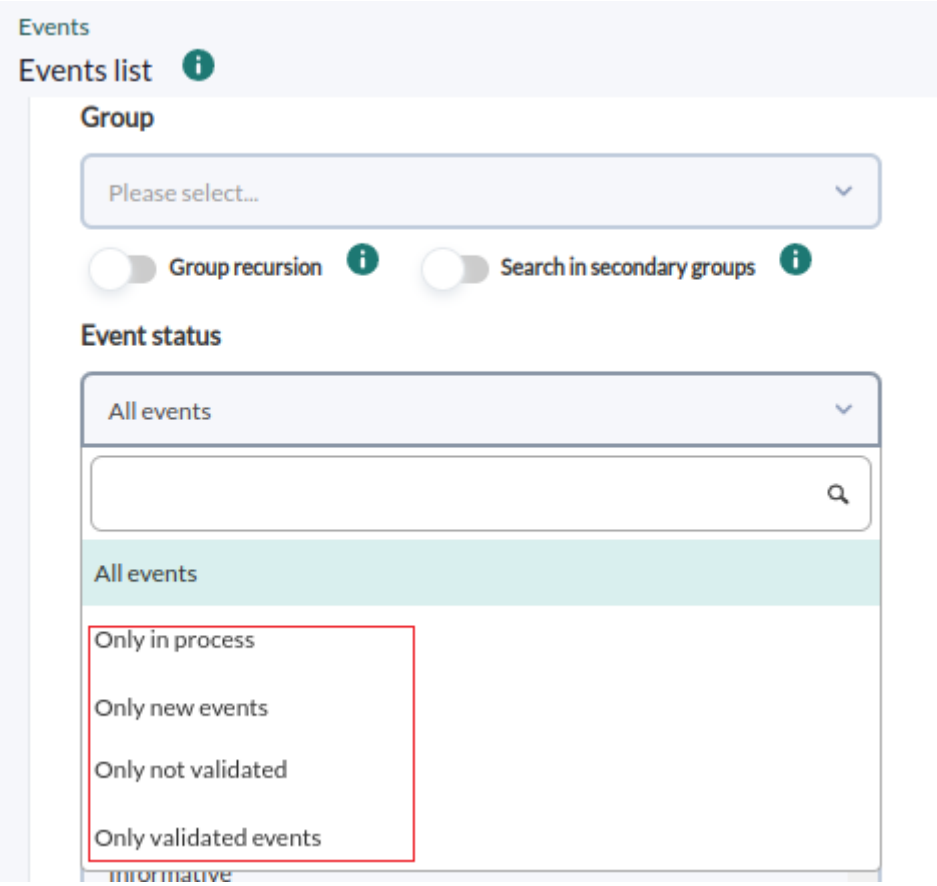
- Users will be able to see only the groups they belong to, unless the user specifically belongs to the group ALL.
- Pandora FMS may also use events to announce that the limits set by users for the monitoring system were exceeded. For example, from version NG 754 onwards, it is possible to set a limit of Agents on a given group and when that limit is reached, it will be shown by an event.

Events are presented by default search for the last eight hours and *not validated* (and can also be customized), and grouped to avoid redundancy. You may save searches as filters or apply a previously created filter.

Event-driven operation

Event validation and status. Auto validation

Events can be found in four states:



- In process.
- New.
- Not validated.
- Validated.

Auto-validation

When events take place due to state changes in modules, there will generally be two events: a first event consisting on switching from normal state to another “incorrect” state, and an event of returning to normal state, once the issue is solved. In these cases, the events that went into an undesired state (either *critical* or *warning*) are automatically validated upon return to normal. This is called event auto-validation and is an extremely useful feature.

Manual validation

If working manually, an event can also be validated: the system will memorize the date and the user who validated the event, with the possibility of recording a comment on the situation, then the screen is refreshed and the validated event is made invisible.

Note that, in addition, in the actions there are more options such as executing customized responses such as pinging the host or assigning users, among others.

In process

An event can be checked as “in process” in the Responses tab. That way the event will not be auto-validated and will remain as pending.

Individual or batch processes

Events can be validated, checked as “in process” or deleted individually by clicking on the corresponding icons or mass applied to a selection.

In the case of custom responses, the maximum number of events to which the operation can be applied is limited to ten.

Event filtering

Important aspects of this feature:

- Filters can be saved for reuse at another time.
- The maximum number of hours old (Max. hours old) of events can be customized.
- Pandora FMS, by default, groups repeated events (Duplicate → Group events), however this preference may be changed:

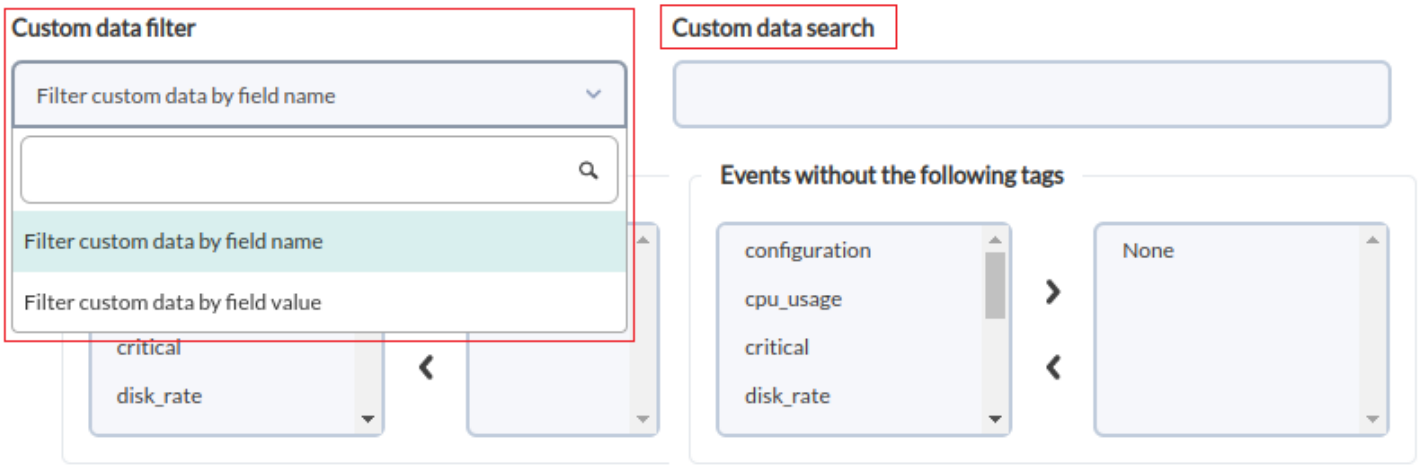
1. All events: It displays all events individually.
2. Group agents: It groups events by agent.
3. Group events: The event name, agent ID and module ID are used to identify duplicates.

4. Group Extra IDs: Events will be grouped only by Extra ID, sorted by Timestamp.

- You may filter by specific group. If you use the Group recursion option, it will also search in the subgroups of that group. Likewise, if you select Search in secondary groups, the events of agents with assigned secondary groups will be included. *These last two options may affect PFMS server performance*.

Advanced options

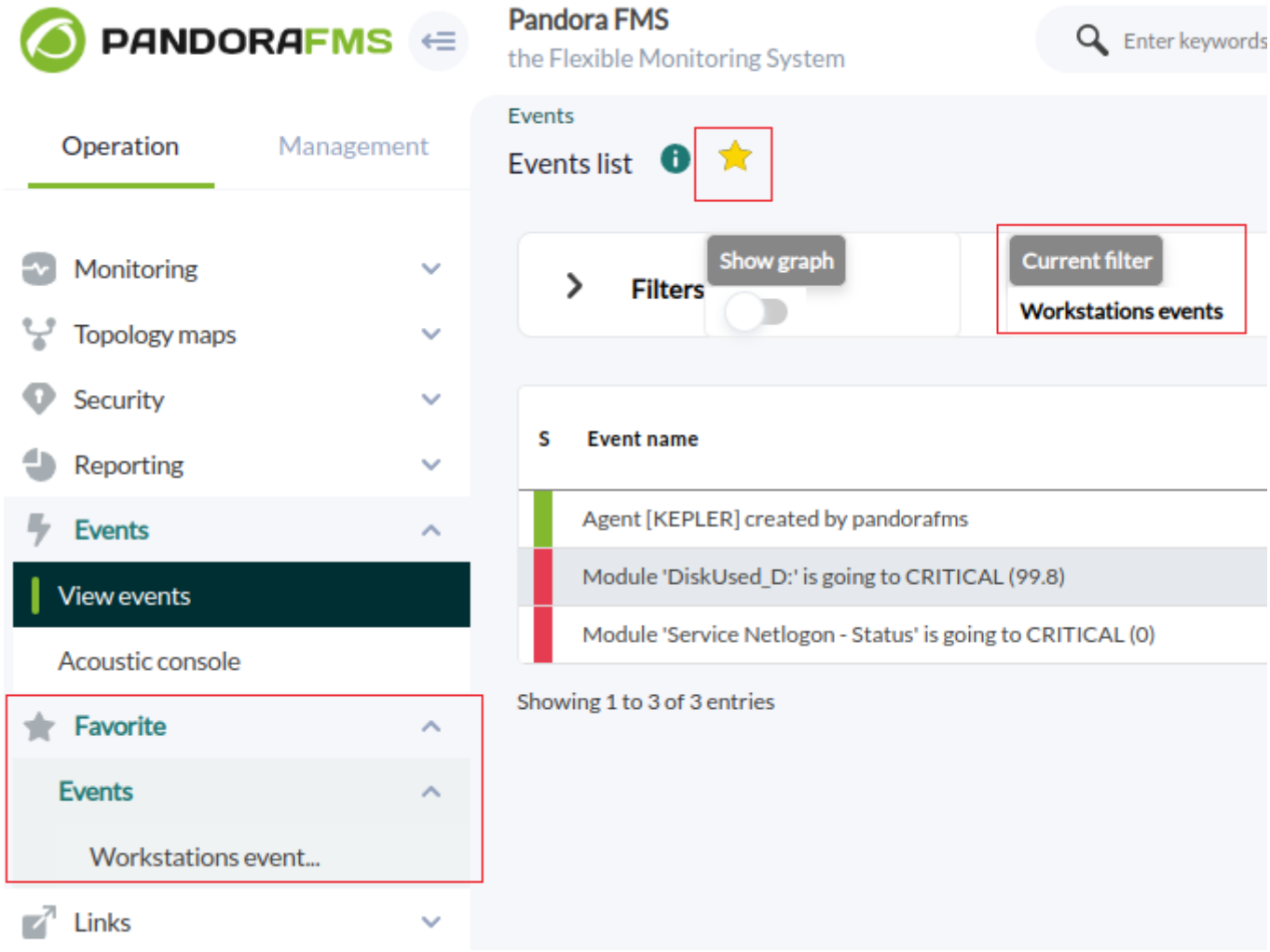
- You may request events that took place within a given time span using From (date) and To (date) date fields.
- In the Free search field you may use a *regular expression* (for example, to search for `Connections` and `Network` enter `(Connections|Network)`). The search is performed by agent name, event name, extra ID, source, custom data and comments.
- You may filter by custom fields using Custom data filter fields, either through Filter custom data by field name or Filter custom data by field value. Such fields will be displayed as columns in the event view.



Favorite filters

Version 770 or later.

Frequently used event filters may be added to the Events section in the Favorite menu (Operation menu). For that purpose, click on the star icon that will appear when loading a saved filter (Current filter). Clicking again will allow you to uncheck the icon and remove it from the favorite system.



Event deletion

Events may be deleted individually (manually) and/or automatically: in the menu Management → Setup → Setup → Setup → Max. days before events are deleted specify the time they will be saved for in days.

By activating Enable event history in Management → Setup → Setup → Historical database, there is the option to keep them for the purpose of creating special reports.

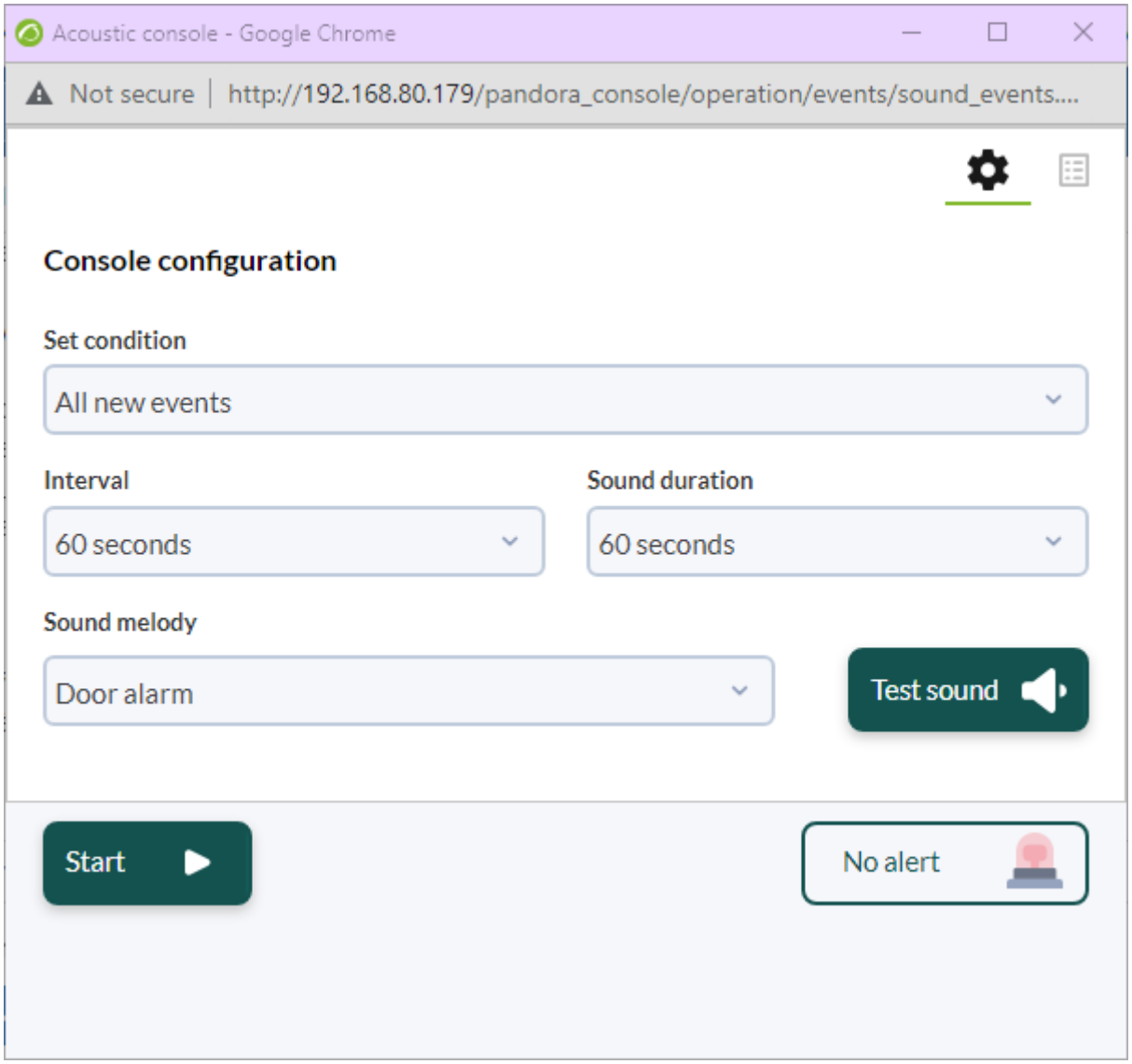
Events in RSS

- In order to access the event *RSS* feed, configure the IP addresses that are allowed access in the IP list with API access field inside Setup.
- You will also need an RSS reader such as Inoreader, Selfoss or any RSS reader of your choosing.

To see the events in a news feed you may access Operation → Events → RSS and with that link you may subscribe to the news reader of your choice.

Event sound console

It allows you to broadcast multiple sound alerts when an event takes place. The melody will play continuously until you pause the sound event or click OK.



List of events that generate sounds by default (and can be customized):

- The triggering of any alert.
- A module going into `warning` status.
- A module going into `critical` status.
- A module going into `unknown` status.

Menu Operation → Events → Acoustic console: this option opens a pop-up window to control all sound events. The web browser must be configured to allow pop-up windows to be opened.

Minimizing the Acoustic Console window will cause it to not work as expected.

Sound events are scanned every 10 seconds asynchronously, when an event takes place, the window will start flashing red and vibrating and also, depending on the configuration of your browser and/or operating system, the window will come to the front compared to the rest of the open windows.

Only those events that take place from and while the previous window remains open, match with the selected ones and have a sound alert configured will be alerted with sound.

Advanced settings

To add new melodies, copy these files in WAV format, to the directory:

```
/var/www/pandora_console/include/sounds/
```

Export events in CSV

To export the events to CSV format, click Operation → Events → View events → Export to CSV file.

Event alerts. Event correlation

For version 741 or later, there is the management of event-related alerts, which is covered in a separate chapter.

Command line events

Event creation and validation

Pandora FMS external API is used by making remote calls (through HTTPS) on the `/include/api.php` file. This is the method defined in Pandora FMS to integrate third-party applications with Pandora FMS. It basically consists of a call with the formatted parameters to receive a value or a list of values that will later be used by this application to perform operations.

The three main points to activate PFMS API:

1. Enable access to the IP from which the command is to be executed.
2. Set a general API password.
3. Define a specific user and password that can only connect through API.

The dedicated tool to create or validate events by Pandora FMS API can be copied from:

```
/usr/share/pandora_server/util/pandora_revent.pl
```

When executed on the client device, without parameters, you will be able to see the full syntax.

The options to validate events are:

```
./pandora_revent.pl -p <path_to_consoleAPI> -u <credentials> -validate_event
<options> -id <id_event>
```

For the `unknown`, `critical` or `warning` instruction fields to appear in the details of the generated event, the event must be `going_unknown`, `going_down_critical`, or `going_down_warning`, accordingly.

Sometimes, maybe for security reasons, it is necessary to have only the event creation option, for that purpose `pandora_revent_create.pl` can be copied to the client device. It is located at:

```
/usr/share/pandora_server/util/pandora_revent_create.pl
```

This tool shares similar features with `pandora_revent.pl`.

Use of custom fields in events

Events with custom fields can be generated through Pandora FMS CLI:

```
pandora_manage /etc/pandora/pandora_server.conf \
  --create_event 'Custom event' system Firewalls \
  'localhost' 'module' 0 4 '' 'admin' '' '' '' '' \
  '{"Location": "Office", "Priority": 42}'
```

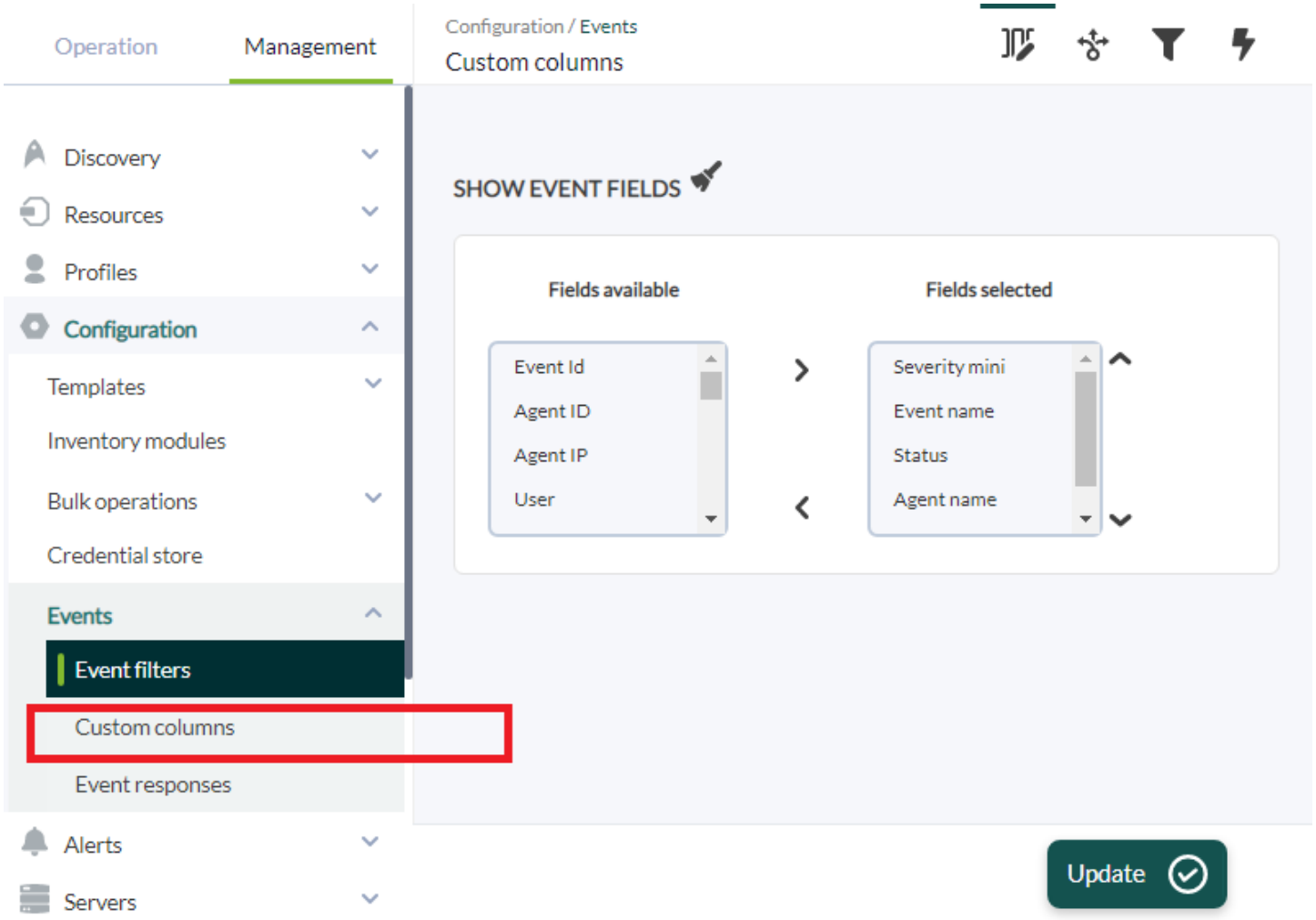
Event configuration

By means of Management → Configuration → Events it is possible to configure:

- Custom columns.
- Responses.
- Filter configuration.

Event view customization

It is possible to customize the fields displayed by default by the event viewer. To do so, choose the fields to be displayed from Events → View events → Manage events → Custom columns.



The default fields are five, however there are more fields to add:

- Event ID.
- Agent name.
- User.
- Group.

- Event type.
- Module name.
- Alert.
- Severity.
- Comment.
- Tags.

- Source.
- Extra ID.
- Owner.
- ACK Timestamp.
- Instructions.
- Server name.
- Data.
- Module status.
- Module custom ID.

Event Filter Creation

Menu Management → Configuration → Events → Events filters.

It allows you to create, delete and edit the filters applied to the event view. After saving, you may go to View events and load the appropriate filter.

Event Responses

Introduction

An event response is a custom action that may be executed on an event, such as creating a ticket in Pandora ITSM with the relevant event information. More information about Pandora ITSM can be found in Pandora FMS documentation.

Enter a representative name, description, the parameters to be used separated by commas, the command to be used (the latter allows the use of macros), the type and the server that will run the command. In Parameters you may set as many as you need, separated by commas. When the response is made, a dialog box will appear to fill in each one of them and thus add it to the event.

Event Response Macros

_agent_address_

Agent address.

_agent_alias_

Agent alias.

_agent_id_

Agent identifier.

_agent_name_

Agent name.

_alert_id_

Identifier of the alert associated with the event.

_command_timeout_

Command response time (seconds).

_current_user_

Identifier of the user running the response.

_current_username_

Full name of the user executing the response.

_customdata_json_

It retrieves information from custom data in JSON format.

_customdata_text_

Output all custom data in text mode (with line breaks).

_customdata_X_

It retrieves a particular field from custom data, replacing the X with the field name.

_event_date_

Date on which the event took place.

_event_extra_id_

Extra identifier.

_event_id_

Event identifier.

_event_instruction_

Event Instructions.

_event_severity_id_

Event severity identifier.

_event_severity_text_

Event severity (translated by Pandora FMS console).

_event_source_

Event source.

_event_status_

Event status (new, validated or event in process).

_event_tags_

Event tags separated by commas.

_event_text_

Full event text.

_event_type_

Type of event:

- Monitor in critical status.
- Monitor in warning status.
- Monitor in normal status.
- Unknown.
- Unknown Monitor.
- Alert triggered.
- Alert recovered.
- Alert stopped.
- Manual alert validation.
- Agent created.
- Recon host detected.
- System.
- Error.
- Configuration change.

- Network configuration manager.

_event_utimestamp_

Date on which the event took place in utimestamp format.

_group_id_

Group identifier.

_group_name_

Name of the group in the database.

_group_contact_

Contact information of a group of agents.

_module_address_

Address of the module associated with the event.

_module_id_

Identifier of the module associated to the event.

_module_name_

Name of the module associated with the event.

_node_id_

For Command Center (Metaconsole) and Node: it returns the node identifier.

_node_name_

For Command Center (Metaconsole) and Node: it returns the node name.

_owner_user_

User who owns the event.

_owner_username_

Full name of the user who owns the event.

_user_id_

User identifier.

Back to Pandora FMS Documentation Index