PANDORAFMS

Console Settings

Console Settings

In this section you can modify and adjust operating parameters of the Pandora FMS Console, which will affect its general operation.

In the Management → Setup → Setup section you will find all the configuration options, which are described below.

Setup

General Setup

Important fields:

- Remote configuration directory: Field that identifies the directory where the remote configuration of the default agents is saved located in:

```
/var/spool/pandora/data_in
```

- Chromium path: The path or PATH where Chromium is installed must be entered. Chromium is a special component that is used to dynamically generate graphics in PDF.
- Automatic login (hash) password: Defines a static symmetric password, used to create a hash and enable automatic validation by URL. It is used to integrate Pandora FMS into another WEB application, passing a username as a parameter, and using a hash generated by the username and this password, allowing automatic validation in Pandora FMS, without entering a password. To see an example of this integration see the file `/extras/sample_login.php` of the Pandora FMS Console.
- Time source: List where you can choose the source of the date and time to use. It can be the local system ("System") or the database ("Database"). The first is typically used when the database is on a different system with a different time zone than the Console.
- Attachment directory: Pandora FMS Console file directory. Used to host collections, issue attachments and other series of files. You must have write permissions for the web server, it is located by default at:

```
/var/www/pandora_console/attachment
```

- Enforce https: Force the redirection to https. If you enable it you will necessarily have to activate the use of Pandora FMS with https on your WEB server.

If you have enabled this field and have not configured your Apache to use HTTPS, you will not be able to access the WEB console and will have to disable this option again by accessing the database directly through MySQL and inserting the following query:

```
update tconfig set `value` = 0 WHERE `token` = 'https';
```

- Automatically check for updates: Enable/disable automatic checking for updates in the Open Update Manager. This causes the console to contact the Pandora FMS update provider every time you log in, sending anonymous information about the use of Pandora FMS (number of agents).
- API password : Authentication method to access the Pandora FMS API.
- IP list with API access: List of IP addresses that will have access to the Pandora FMS webservice API (by default `127.0.0.1`, local access only). The asterisk can be used as a wildcard, so placing * gives access to all IP addresses or, for example, `125.56.24.*` grants access to the entire subnet `125.56.24` .
- Enable GIS features: Enable/Disable the GIS features for the Pandora FMS console.
- Enable NetFlow: Enable or disable NetFlow.
- General network path (Version 770 or later): Directory where the `netflow` and `sflow` directories will be stored for the corresponding data.
- Server timezone setup: Defines the time zone in which the Console is located. Unlike the codes/abbreviations of all countries (ISO 3166), the list of time zones has complicated regulations (IANA Time Zone Database), which is why a first list with continents/countries is included and selecting an option from it will update the list. second list where you can choose exactly a country/city. The Timezone setup text box will not change until you press the Update button.
- Public URL: A public URL can be stored. It is useful to complete this field when you have a reverse proxy or, for example, with the mod_proxy mode of the Apache web server.
- Inventory changes blacklist (Version 768 or later): Inventory modules included within the blacklist will not generate events when they change.
- Server log directory: Directory where the server log files are stored.
- Event storm protection: If this option is enabled, no events or alerts will be generated, but data will still be received.
- Command line snapshot: String or string type modules that return more than one line will display their content in the form of an image.
- Change remote config encoding: Activating this parameter converts the character encoding (encoding) of the writing of the modules in the remote configuration files from UTF-8 by default to the encoding configured in the files themselves. setting.
- Referrer security: When active, it is checked for security that the user comes from a Pandora FMS URL and that the link is not external and therefore is no longer suspicious. By default it is disabled. The extreme security sites that are verified are:
    - DB manager extension.
    - User configuration.
    - Recon script configuration.
- Allows create planned downtimes in the past: Activate or deactivate the possibility of creating planned downtimes in the past. The purpose of this is to modify information for SLA reports.
- Limit for bulk operations: Limit of elements that can be modified by bulk operations at one time.
- Include manually disabled agents: Allows you to enable or disable the display of manually disabled agents in certain Console views.
- Set alias as name by default in agent creation: When this parameter is activated, the selection box in the agent creation menu collects the alias entered in the form and also saves it as the agent name and is activated by default .
- Unique IP: By activating this parameter, a token will be created when creating and editing agents by which an agent with a duplicate IP address cannot be created.
- Module custom ID readonly : Activating this parameter blocks the editing of the custom id of an agent's module from the Console but allows editing from the CLI and the API. This is useful for automatic third-party integrations without the user being able to modify this value.
- Enable console log: Due to the large amount of debug data generated by this log, it is recommended to disable it, as configured by default. If activated, the file `/var/log/php-fpm/error.log` is used to log Console events.

If you are using EL8 (Enterprise Linux 8), apart from enabling Enable console log, you must modify the file

```
/etc/php-fpm.d/www.conf
```

and comment with a semicolon the following parameter:

```
;php_admin_value[error_log] = /var/log/php-fpm/www-error.log
```

This way the data will be saved in **…**/pandora_console/log/console.log .

- Enable audit log: When activated, the file **…**/pandora_console/log/audit.log is used for auditing.
- Enable console report (NG Version 764 or later): Allows you to enable the Web Console in mode dedicated to generating reports, see the section "Dedicated console for reports" for more information.
- Check connection interval (NG Version 770 or later): Time interval (in seconds) to check the connection to the database server. Default 180, minimum value 60.
- Keep In process status for new events with extra ID: (NG version 771 or later): If there is any "In process" event with a specific extra ID and a "New" event with that extra ID is received, will be created as "In Process".
- Enable Feedback: Active by default, allows direct access to the header of the Web Console to notify of an error and include the installation data.
- Number of modules in queue: Sets the maximum number of queued modules (500 by default) and if this value is exceeded, a warning icon will be displayed for each item in the server administration.
- Keep in process status for new events with extra ID: If any In process event with a specific extra ID is triggered and a new event with that Extra ID is received, it will be created as In process instead. New events also inherit the Extra ID from the event.

NCM Configuration

- FTP server IP: IP address of the FTP server in the Network equipment templates.

Dedicated console for reports

ENG 764 version or later.

The critical mission of the dedicated Reporting Console, based on the data extracted from the PFMS databases (main and historical), is to prepare, convert into useful information, generate, save and send reports for hundreds of agents and software agents. To do this, it has preconfigured special aspects for both the software and the hardware:

- The memory (RAM, virtual or real) for PHP must be able to use, if necessary, the maximum amount that the computer has. If not, you will receive timely notice of such insufficiency. See installation for configuration details.

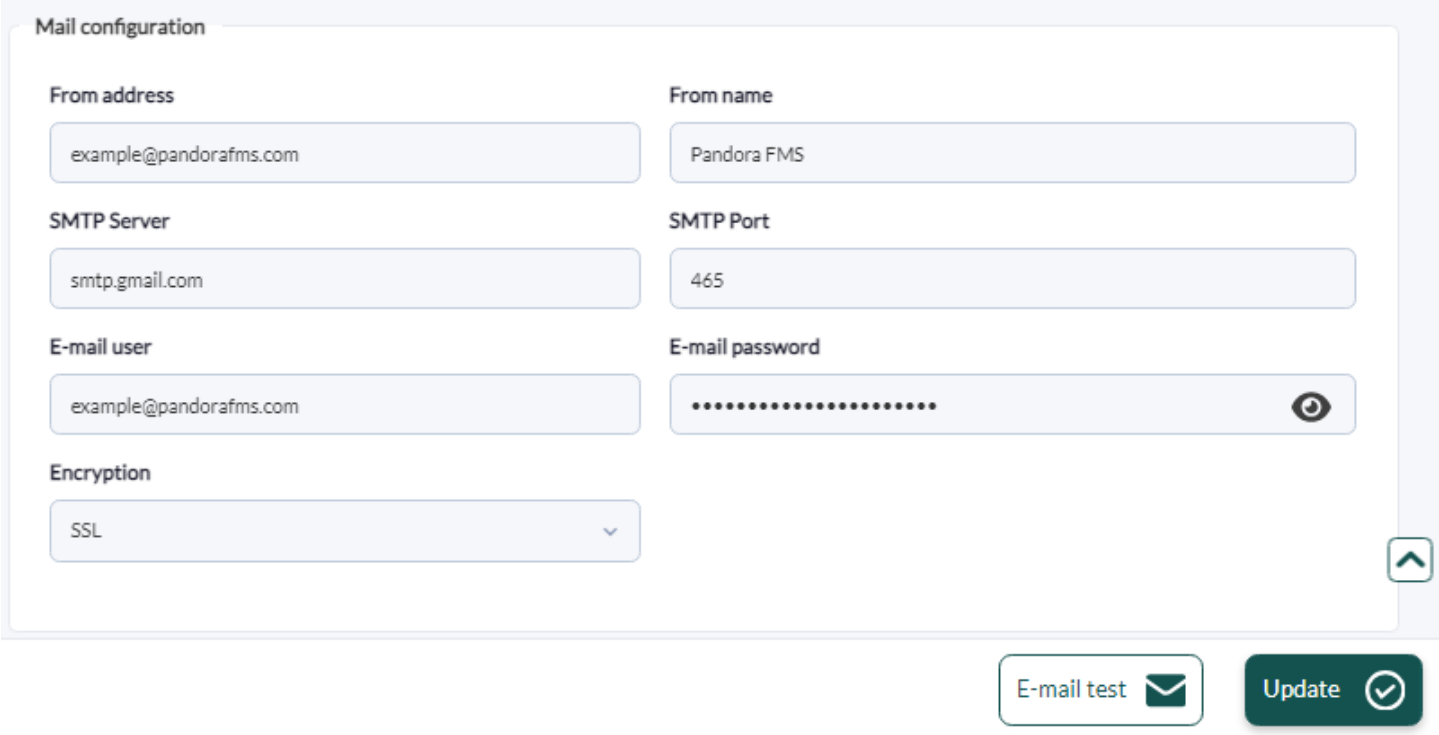
- Enable Dedicated Console mode for reports in the Enable console report option of the General configuration.
- To use the dedicated Console for reports you must add the following parameter to the respective `config.php` file:

```
$config["reporting_console_node"] = true;
```

- Only admin users will be able to log in to the Dedicated Reporting Console.
- Menu options are limited to essential operation, especially for PFMS software upgrade. You will need to configure everything else through another Web Console connected to the same databases. See the section for email sending configuration.

Email Settings

Below there is a configuration example using the Gmail® SMTP server:



If you use a Gmail® account, Google® may block authentication attempts by certain applications. For correct operation, it will therefore be necessary to enable access to unsafe applications. You may find more information about how to do this on the official Google® support pages.

For security, use a Gmail® email account created specifically and solely to send notification messages from Pandora FMS server. Never use an email account for personal use for this.

If necessary, modify the token `mta_auth` in file `/etc/pandora/pandora_server.conf`. This

token, by default, is set as a comment, so it must be activated by editing this line and setting the required authentication type, see this link for more details.

Once the email configuration has been saved, by clicking on the Email test option you may check if your configuration is correct by sending an email automatically generated by Pandora FMS to a desired email address. Only if the selected settings are correct, you will be able to see the email in your inbox.

Make sure that your Pandora FMS server is capable of resolving, through its DNS server, the mail server in charge of your email domain.

```
nslookup -type=mx my.domain
```

Also in this case, make sure that your email server accepts emails redirected from Pandora FMS server.

For more information you may check Pandora FMS server configuration.

Password policy

E To activate the password policy, you must have an administrator profile (Pandora administrator) or be superadmin .

It is configured in Management → Setup → Setup → Password policy:

Important fields:

- Enable password policy: Deactivated by default.
- Min. password size: By default four characters.
- Password expiration: By default zero 0 days (no expiration).
- Block user if login fails: Minutes that the user remains blocked if the maximum number of failed attempts is consumed, by default 5 minutes.
- Number of failed login attempts: By default 5 attempts.
- Compare previous password: Number of previous passwords that cannot be chosen for the password change, default 3.
- The password must include numbers: The password must include numbers, disabled by default.
- The password must include symbols: The password must include symbols, disabled by default.
- Force password change on first login: Force password change on first login after user creation, disabled by default.
- Apply password policy to admin users: Applies the password policy also to administrator users, activated by default.
- Enable password history: Enables/disables the activation of password history, disabled by default.
- Exclusion list for passwords: Allows you to add a list of passwords explicitly excluded from use in Pandora FMS.

Enterprise

If the Enterprise version is used, the following fields can be configured:

- Metaconsole link status: Indicates the connection status if the Metaconsole is active. See the Metaconsole Installation and Configuration section for more information.
- Forward SNMP traps to agent (if exist): Configuration that allows associating SNMP traps and agents. By activating this option, when a trap is received with the same IP address as an agent, a module is created in that same agent with the name `SNMPTrap` and type `async_string`. The value of the module will be that of the last OID received, that is, it is updated with the arrival of new traps. If Yes and change status is selected, in addition to updating the value upon receiving the trap, the module changes to `CRITICAL` state. To return to `NORMAL` state you must validate or delete all traps associated with that agent from the SNMP console. In the case of Yes without changing status only the value of the module is changed.
- Use Enterprise ACL System: This will activate the ACL system which is more flexible than the standard ACL system. See New ACL system (Enterprise)
- Collection size: This is the maximum size, in bytes, for collections. See section Collections.
- Activate log collector Activate logging.
- Enable update manager: Activate the Warp Update Manager option.
- Legacy HA database management (Version 770 or later): Disabled by default; allows you to activate the HA system controlled by `pandora_ha`.
- Critical threshold for occupied addresses: A threshold must be set for the supernet map of the extension IPAM for the critical range of occupied addresses.
- Warning threshold for occupied addresses: A threshold must be set for the supernet map of the extension IPAM for the busy address warning range.

Historical database

This functionality allows data to be saved with a configured age in a database other than the main one to speed up the exploitation of the latter.

From the menu choose Management → Setup → Setup → Historical database and press the Enable historical database button to access the connection settings (Configure connection target). After filling in the fields and connecting to the historical database, fill in the custom parameters (Customize settings):

- Advanced options: Enable advanced options.
  - String data days old to keep in active database: Age of the string data to keep in the active database. String data will be available in the active database at the time and days you specify here. The oldest information will be sent to the history database. Data will be purged from the active database after 0 days (default).
- Data days old to keep in active database: From how many days the data will be transferred to the historical database. Default value: fifteen 15 days.
- Transference block size (Step): Mechanism for transferring data (similar to a data buffer) to the historical database. The smaller the number of records, the less impact the performance of the main database will have. Default value one thousand five hundred `1500` records, recommended value one thousand. See the next point to set the time period.
- Delay between transferences (seconds): Waiting time -in seconds- between data transfers between

the main and historical databases. Default value one 1, recommended value: two 2.
- Maximum historical data age (days): Maximum number of days to retain numerical data. Default value: one hundred eighty 180.
- Maximum historical string data age (days): Maximum number of days to retain text string data. Default value: one hundred eighty 180.
- Automatic partition of big tables: To automatically create monthly partitions in IDB files of specific databases (`tagente_datos` and `tagente_datos_string`).
- Enable historical events
    - Events days old to keep in active database: Number of days to keep events in the historical database. Default value: ninety 90 days. Note that from the main database the events are deleted (purged) after seven days.
    - Maximum historical events age (days): Number of days to finally delete events from the historical database. Default value: one hundred and eighty days 180.
- Enable historical traps: Activating the Enable historical traps option allows you to store the SNMP traps in the historical database:
- Days old to keep in active database: Number of days old to keep in the active database. Default value: 6 days.
- Maximum historical traps age (days): Number of days old to maintain in the historical database. Default value: 180 days.

Log collector

Menu Management → Setup → Setup → Log collector (OpenSearch). It must be configured as explained in "Monitoring and log collection".

Authentication

The following fields are common to all options:

- Control of timeout session: By default activated, it checks if there has been no activity in the time period set in Session time (mins) to close the session.
- Session time (mins):
    - The default value is 90 minutes and when you set this value to 0 for a user, Pandora FMS will use the value saved in the General Settings, authentication section.

Local Pandora FMS

Default authentication indicates that it will be carried out using the internal Pandora FMS database. For security, superadmin type users are always authenticated in this way, the rest of the authentication types have the local option as a backup (fallback).

Active Directory

- Automatically create remote users: Enables or disables automatic creation of remote users. This option makes it possible for Pandora FMS to create users automatically once they log in. If you enable this feature, the following fields will be available:

- Save Password: If activated, it allows you to save AD passwords in the local Pandora FMS database.
- Advanced Configuration AD: If this option is enabled, the Advanced Permissions AD configuration will be used.
    - Advanced Permissions AD: Lists the advanced permissions that have been added in Add new permissions.
- Automatically create profile: When the automatic creation of remote users is active, this field makes it possible to assign a type of profile to these users that are created automatically. The default profiles are: `Chief Operator`, `Group Coordinator`, `Operator (Read)`, `Operator (Write)` and `Pandora Administrator`. The different profiles available can be consulted in the Profiles → Profile management section.
- Automatically create profile group: When activating the automatic creation of remote users, this field makes it possible to assign a group to these automatically created users. The different groups available can be consulted in the Profiles → Manage agent groups section.
- Automatically create profile tags: When the automatic creation of remote users is active, this field makes it possible to assign a profile to a group with the desired tags. The different available groups can be consulted in the Profiles section → Module tags.
- Autocreate blacklist: Allows you to write a list of users, separated by commas, that will not be created automatically.
- Active Directory server: Define here the path where our Active Directory server is located.
- Active Directory port: To define the port number of the Active Directory server (389 by default).
- Start TLS: Defines whether or not the Transport Layer Security (TLS) protocol will be used in communications between the client and the server.
- Enable secondary active directory: Allows you to activate the connection to a secondary Active Directory server. It has the same fields as the primary server but also supports configuring a search expiration time (AD search timeout) with a default value of 5 seconds.
- Double authentication: Users can choose whether to enable two-step authentication on their accounts. To learn more about how to enable two-step authentication on an account, you can read this section. This functionality requires that the server and mobile devices have a synchronized and as accurate date and time as possible.
- In the event that there is a user password change, MS Windows® allows you to use an old password by default for 60 minutes in Active Directory. Being a Windows configuration, this behavior is totally foreign to Pandora FMS. If you wish to modify, you can consult the documentation at Microsoft .
- Domain: Define the domain that the Active Directory will use.
    - At this time a user's primary groups are not supported with advanced group settings in AD Authentication.
    - If you are using Advanced Configuration AD, be sure to set the full path in the domain field (Domain).
    - If the Active Directory installation is with LDAP, you must define here the LDAP path in which the server is located, generally:

```
ldap:addc.mydomain
```

LDAP

- In order to use this mode, it is necessary to have the openLDAP dependencies installed.
- Depending on the operating system used, the commands are used: `yum install openldap*` or `apt install ldap-utils`

Important fields:

- Fallback to local authentication: If this option is enabled, a local authentication will be done if LDAP fails. Administrator users will always have fallback enabled, so as not to lose access to Pandora FMS in case of failure of the remote authentication system.
- Automatically create remote users: Enables or disables automatic creation of remote users. This option makes it possible for Pandora FMS to create users automatically once they have logged in using LDAP.
- LDAP function: When searching in LDAP, you can choose whether to use the native PHP function or use the local ldapsearch command. It is recommended to use the local command for those environments that have an LDAP with many elements.

Advanced LDAP Config

- If the option is activated, a list appears with all saved advanced permissions. You can add new permissions by selecting the profile, groups and tags, next to the attributes filter. If the user meets any of those attributes (for example, a specific organizational unit or group) then the user will be created.
- If this option is not activated, the simple system for creating user profiles is used (Automatically create profile, Automatically create profile group, Automatically create profile tags, Automatically assigned no hierarchy).

Attributes must have the following format Attribute_Name
= Attribute_Value

- Enable secondary LDAP: If you enable a secondary LDAP server as a backup, respective fields of the primary LDAP server will appear.
- Double authentication: Users will be able to choose whether to enable two-step authentication on their accounts. This functionality requires that the server and mobile devices have a synchronized and as accurate date and time as possible.

Double authentication

Users will be able to choose whether to enable two-step authentication on their accounts.

To use this functionality, the administrator must activate double authentication in the authentication section of the global configuration of the Pandora FMS console. It will also be necessary to have the code generating application on a mobile device you own. To know where and how to download it:

https://support.google.com/accounts/answer/1066447

This functionality requires that the server and mobile devices have a synchronized and as accurate date and time as possible.

Force 2FA for all users is enabled

Enabling this option will force all users to use two-step authentication.

To disable this functionality without using the graphical interface, an administrator can use the PFMS CLI.

SAML

For SAML configuration, you can consult this section.

Performance

The performance of Pandora FMS is affected by various factors that must be refined in the following sections. Go to menu Management → Setup → Setup → Performance.

Database maintenance status

- Pandora_db running in active database: If `pandora_db` exceeds 12 hours without running, it will mark a critical state.
- Pandora_db running in historical database Only appears if there is a historical database configured; Likewise, if `pandora_db` exceeds 12 hours without running on the historical database, it will mark a critical state.

Database maintenance options

Menu Management → Setup → Setup → Performance.

- Max. days before events are deleted: Maximum number of days before events are deleted.
- Max. days before traps are deleted: Maximum number of days before deleting the SNMP traps.
- Max. days before audited events are deleted: Maximum number of days before auditing events are deleted.
- Max. days before string data is deleted: Maximum number of days before data strings are deleted.
- Max. days before GIS data is deleted: Maximum number of days before GIS data is deleted.
- Max. days before purge: Maximum number of days before purging data. This also specifies the maximum number of days to maintain historical inventory data.
- Max. days before data is compacted: Maximum number of days before compactardata.
- Max. days before unknown modules are deleted: Maximum number of days before unknown modules are deleted except if they are in a policy.
- Max. days before delete not initialized modules: Maximum number of days before deleting uninitialized modules.
- Max. days before autodisabled agents are deleted: Number of days (default 30) from which auto disabled agents will be deleted.
- Retention period of past special days: Number of days from which special days that have already passed will be deleted.
- Max. macro data fields : Number of macros that can be used for alertas.
- Max. days before delete old messages: Number of days from which received messages will be

deleted.
- Max. days before inventory data is deleted: Number of days from which the data from inventario will be deleted.
- Max. days before disabled agents are deleted: Number of days from which disabled agents will be deleted (default `0`, never).

Historical database maintenance options

These parameters will only appear if there is a history database configured in Pandora FMS.

- Max. days before purge: Maximum number of days before purging data.
- Max. days before compact data: Maximum number of days before compacting data.
- Compact interpolation in hours (1 Fine-20 bad): It is the length of the compaction interval in hours, a value close to one is recommended. For example, a module with a 5-minute interval generates 288 values per day. If this interval is set to 2, the data will be grouped into 2 hour intervals and averaged, resulting in 12 values per day instead of 288. The higher this value, the lower the resolution.
- Max. days before delete events: Maximum number of days before deleting events.
- Max. days before delete string dat: Maximum number of days before deleting string data.

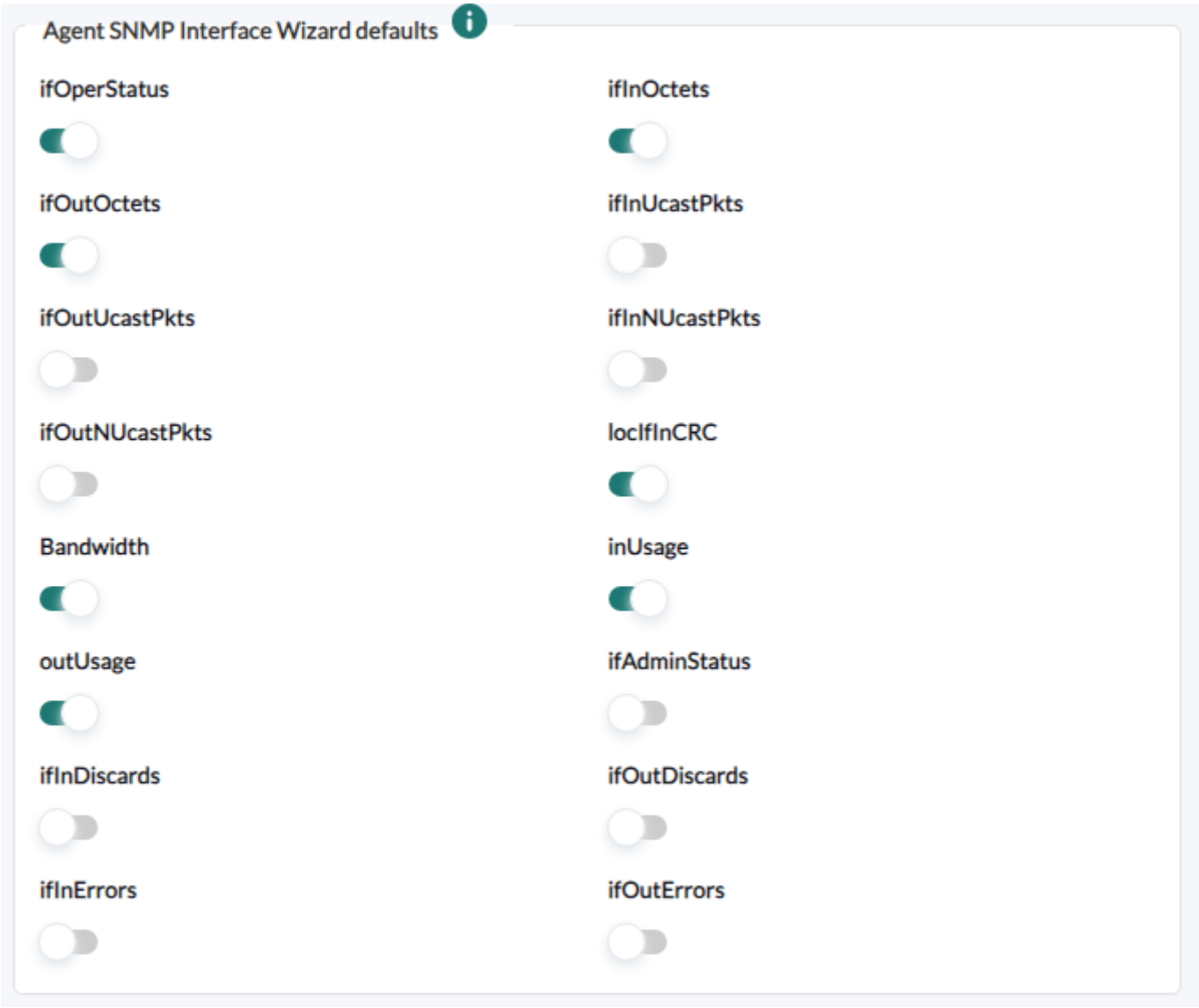
Others

- Item limit for real-time reports : Field where the maximum number of data that the graph will represent in real time is defined.
- Limit of events per query: To set a maximum limit on the number of events returned in a query.
- Compact interpolation in hours (1 = fine / 20 = bad): It is the length of the compaction interval in hours.
- Default hours for event view: Field where the hours field of the default filter in the event view is defined. This field also affects the display, counting and graphing of events in the tactical view.
- Use real-time statistics: Enable or disable the use of real-time statistics.
    - Batch statistics period (secs): If real-time statistics are disabled, the refresh time for the statistics will be defined here.
- Use agent access graph: The agent access graph, renders the number of contacts per hour on a graph with a daily scale (24 hours). This is used to know the contact frequency of each agent. It may take a long time to process, so if you have low resources it is recommended to disable it.
- Max. recommended number of files in attachment directory: Maximum number of files that are stored in the `attachment` directory.
- Delete not initialized modules: Enables or disables deletion of uninitialized modules.
- Big Operation Step to purge old data: Number of blocks into which the `pandora_manage.pl` script divides a time interval. A higher value implies larger blocks of time, which means performing more but lighter operations. In overloaded systems and very large databases it may be advisable to increase this value even if purging the data takes more time.
    - Small Operation Step to purge old data: Number of rows that `pandora_manage.pl` processes in a single SQL query. This means that for each block of time defined by the Big Operation Step to purge old data parameter, at most 1000 records will be purged with each query (using the default value). A larger value means larger queries, which means performing fewer automatic operations that heavier. In overloaded systems it may be advisable to reduce this value, although purging the data will take longer. The default and recommended value is 1000.
- Graph container - Max. Items: Field where the number of maximum items in the graph container view is defined.
- Events response max. execution: Field where the maximum number of events that can perform the

massive Event Responses operation is defined.
- Row limit in csv log: Row limit for the log in CSV format.
- SNMP walk binary and SNMP walk binary (fallback): When SNMP bulk walk is not able to request V1 SNMP, this option will be used instead (default `snmpwalk`, slower).
- WMI binary: Executable file to use in WMI queries, by default `pandorawmic`.

Default values for SNMP interface

To complete the SNMP configuration from the previous section, you can either set the default values to be used for the different modules in the SNMP interface wizard.



Visual styles

In this section you can configure all visual elements of Pandora FMS.

Go to menu Management → Setup → Setup → Visual styles.

Behavior configuration

- Block size for pagination: Field where the size of the pagination of elements (events, alerts, etc.) is chosen.
    - Paginated module view: Activate pagination in the module list.
- Display data of proc modules in other format: proc type data represents binary states of a module. In the database they are collected as a number, but they could also be represented descriptively with an identifier for each of the two states. Activating this option uses this second form of representation.
    - Display text when proc modules are in OK status: When the Display data of proc modules in other format option is activated, this text appears instead of the number when the module has an OK status.
    - Display text when proc modules are in critical status: When the Display data of proc modules in other format option is enabled, this text appears instead of the number when the module is in a failed status.
- Click to display lateral menus: This parameter will configure whether the lateral menu is displayed when you click (main mouse button) on it or when you place the mouse over it.
- Service label font size: Default font size for services.
- Space between items in Service maps: Distance (in pixels) between two elements of the service maps. To avoid overlapping this value must be greater than 80 pixels.

GIS configuration

- GIS Labels: Activate the labels with the agent name in the GIS maps. It is advisable to disable this option when you have many agents on a map, this way it is more readable.
- Default icon in GIS: Default icon for agents on GIS maps.

Style configuration

Style settings for graphic elements:

Style configuration

Style template

Default theme

Status icon set

Colours View

Custom favicon

Default

Custom background logo

flowers.jpg View

Custom logo (menu)

logo-default-pandorafms.png View

Custom logo collapsed (menu)

logo-default-pandorafms-collapsed.p... View

Custom logo (header white background)

pandora_logo_head_white_bg.png View

Custom logo (login)

Pandora-FMS-1.png View

Custom Splash (login)

none.png View

Custom documentation logo

default_docs.png View

Custom support logo

default_support.png View

Custom networkmap center logo

Default View

Custom mobile console icon

Default View

Title (header)

Pandora FMS

Subtitle (header)

the Flexible Monitoring System

Title 1 (login)

ONE TOOL TO RULE THEM ALL

Title 2 (login)

Docs URL (login)

https://pandorafms.com/manual

Support URL (login)

https://support.pandorafms.com

Product name

Pandora FMS

Copyright notice

PandoraFMS.com

Background opacity % (login)

20

Disable logo in graphs

Disable helps

Fixed header

Automatically hide submenu

Visual effects and animation

Random background (login)

Important notes:

- Style template: To add new themes you must add a CSS file in the `include/styles` directory.
- Status icon set: In the case of users with color blindness, these can be replaced by other conceptual icons that allow the statuses to be differentiated in another way.
- Custom favicon: It must be in `.ico` format and its dimensions in 16 by 16 pixels for it to work correctly. You can add icons to choose from in the `images/custom_favicon` folder.
- Custom documentation logo and Custom support logo: Icon for the link to the documentation and support on the login screen. If left blank no icon will be seen. The path to upload more icons is `enterprise/images/custom_general_logos/`.
- Product name and Copyright notice: By default, the product name is Pandora FMS. However, in the Enterprise version, the user is given the option to rebrand and change it to another text string and thus have a personalized version.
- Background opacity % (login): Allows you to specify an opacity percentage (default 30%) on the login screen.
- Disable helps: Hide all Pandora FMS helps. This configuration option affects both the modal windows and the wizard and other links to the Pandora FMS documentation.
- Fixed header: The header is always shown, that is, it is not hidden when scrolling (vertical scrolling of the window).
- Automatically hide sub-menu: Activating this option minimizes the side menu.
- Random background (login): If you do not have a wallpaper configured for the login screen (see Custom background logo), activating this option will randomly have one of several graphic files stored in:

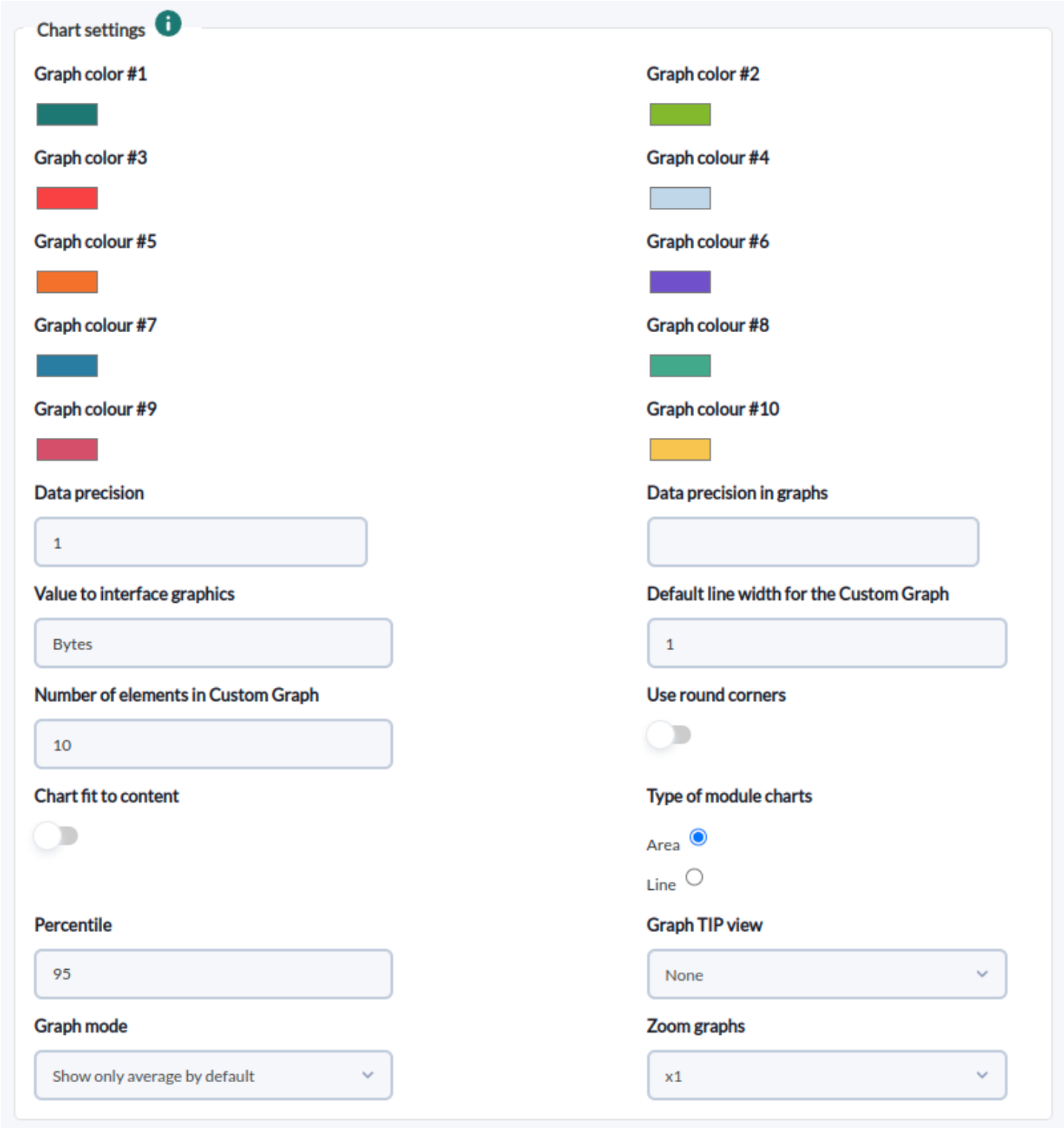
```
…/pandora_console/images/backgrounds/random_backgrounds
```

The following alternative rebranding configuration tokens are stored as a comment (commented) in config.php to preserve the configuration in case of database failure.

```
----------Rebranding--------------------
Uncomment these lines and add your customs text and paths.
$config["custom_logo_login_alt"] ="login_logo.png";
$config["custom_splash_login_alt"] = "splash_image_default.png";
$config["custom_title1_login_alt"] = "WELCOME TO Pandora FMS";
$config["custom_title2_login_alt"] = "NEXT GENERATION";
$config["rb_product_name_alt"] = "Pandora FMS";
$config["custom_docs_url_alt"] = "http://pandorafms.com/manual/";
$config["custom_support_url_alt"] = "https://support.pandorafms.com";
```

Chart settings

Graphics settings:



Important notes:

- Value to interface graphics: Name of the units for interface graphics.
- Data precision: Number of decimal places to display in reports and visual consoles. It must be between 0 and 5.
- Data precision in graphs: Number of decimal places to display in the graphs. It must be between 0 and 5.
- Number of elements in custom graph: To limit the number of legends in combined graphs. Also consider decreasing the width of the legends, making them condensed and as short as possible. The combined graphs that respond to this token are of type:
    - Line.
    - Area.

    - Vertical bars.
    - Horizontal bars.
    - Stacked or stacked.
- Chart fit to content: There are graphs whose values are percentages and the top of the graph exceeds the maximum value one hundred, you can configure the graphs so that they stop adding a proportional upper margin by activating this option.
- Percentile: Shows a line with the percentile indicated in the graphs. The default value is 95.
- Graph TIP view: This parameter indicates whether TIP graphs will be displayed.
    - None (None): The TIP option of the graphics setup will be disabled (default option).
    - All (All): The TIP option in the graph menu will be activated.
    - On Boolean graphs: The TIP option will only be activated in the true and false type graphs menu.

Font and text settings

Letter and text font settings:

- Graphs font size: Field where you choose the font size used by Pandora FMS for the graphics.
- Agent size text: When the agent name is too long, in some sections of Pandora FMS the text is truncated showing only the first characters (default values: 18 characters when the font is small and 50 characters when it is normal size).
- Module size text: When the name of the modules is too long, in some sections of Pandora FMS the text is truncated, showing only the first characters (default values: 25 characters when the font is small and 50 characters when It is normal size).
- Description size text: When the description is too long, in some sections of Pandora FMS the text is truncated showing only the first characters (default value: 60 characters).
- Item title size text: When the title is too long, in some sections of Pandora FMS the text is truncated, showing only the first characters (default value: 45 characters).
- Show unit along with value in reports: Show units in addition to the module value in reports.
- Truncate agent text at end and Truncate module text at end: When activated, they cut the name of the agents and modules at the end and place three ellipses (the default behavior is to cut in half) for the Operation → Monitoring → Views section.

Visual console configuration

Visual console configuration:

- Legacy Visual Console View: If this token is activated, the visual consoles view will be kept in the original form. When disabled, it allows you to configure the token below.
- Default cache expiration: This section indicates how often the cache of the state of the elements is cleared and, therefore, how often each element's state is calculated individually.
- Default interval for Visual Console to refresh: This interval will only affect the visual console pages, establishing how often they will be automatically refreshed.
- Type of view of visual consoles: Drop-down to indicate whether you want the favorite visual consoles to be displayed in the menu.
- Number of favorite visual consoles to show in the menu: To avoid overlapping and help the performance of the Web Console, this token limits the number of favorite consoles to show in the side menu.
- Default line width for the Visual Console: Width of the line in the visual consoles. This option can be

changed within the visual console itself individually for each line, but the default value is detailed here.
- Mobile view not allow visual console orientation: In the mobile console it prevents the screen from being rotated according to the motion sensor.
- Display item frame on alert triggered: Allows you to hide an orange box when you have an alert triggered in the Static image, Simple value, Icon and Group elements of the Visual consoles. Enabled by default.

Reports configuration

Configuration of reports:

- Show report info with description: Description of custom report information. Applies to all reports and templates by default.
- Front page for custom reports: Front page for custom reports. Applies to all reports and templates by default.
- PDF font size (px): Text font size, in pixels, for PDF files.
- HTML font size for SLA (em): Font size for SLA reports (HTML only). It is in a relative measurement called em which is equivalent to the number of times the size of the chosen font in pixels.
- Graph image height for HTML reports: Height in pixels of module graphs or custom graphs in reports (HTML only).
- Interval description: Shows the description of the time interval in abbreviated form or not. A long description (Long) is, for example, “10 hours, 20 minutes, 33 seconds”; a short one (Short) is “10h 20m 33s”.

Services configuration

Number of favorite services to show in the menu: Maximum number of favorite visual consoles that can be shown in the visual console submenu.

Other configuration

Other settings:

- Network map max width: Maximum width, in pixels, of the network map (adjust for each screen size).
- Show only the name of the group: The name of the group will be shown instead of its icon.
- Show empty groups in group view: Allows you to display empty groups in the group view.
- Date format string: Field where the date and time format is defined as denoted by the PHP language.
- Decimal separator: Decimal separator to use in reports.
- Timestamp, time comparison, or compact mode: Defines what date and time is used, the system timestamp (Timestamp in rollover), a comparison with the database (Rollover comparison) or in a compact way (Compact mode). This is useful when the database is on a different system than where the Web console is located.
- Custom value post processing: Custom conversion values for post processing. Update a table in the database to have custom conversions from one unit to another. If you accidentally add an incorrect numeric value, select it from the Delete custom values list and delete it using the Delete button below and add the custom conversion value again.

- Interval values: Here you can customize the time values (seconds, minutes, etc.) that the Interval field will take in Pandora FMS forms.
- Module units: This option allows you to define the unit of the data that the modules will collect.
- CSV divider: Character or set of characters with which the data will be separated when exporting to CSV.
- CSV decimal separator: Symbol to use in the decimal separator when exporting to CSV.
- Data multiplier to use in graphs/data: Value by which the displayed data will be multiplied to represent them in the graphs. This is useful in the case where the unit of value is bytes; for other conversions use Custom value post processing.

NetFlow

For more information, see the topic "Network monitoring with NetFlow". Notable fields:

- Data storage path: Directory where NetFlow data is stored.
- Daemon binary path: Directory where the nfcapd program is stored.
- Nfdump binary path: Directory where the nfdump program is stored.
- Nfexpire binary path: Directory where the nfexpire program is stored.
- Name resolution for the IP address: Activate this parameter to resolve the address IP to obtain their hostnames. This process can take a long time to complete.

eHorus

By enabling the integration with eHorus you will have access to the configuration:

- eHorus configuration at user level: Allows you to configure the connection with eHorus at the user level. Disabled by default, if enabled the following fields User and Password will no longer be available in the configuration.
- Test: Press to perform a connectivity test

You can find more information about the integration with eHorus in this section

Pandora ITSM

Allows you to enable the connection and communication between Pandora FMS and Pandora ITSM. The activate button can be configured to be used for all users (default option enabled) or for each user to configure their own connection.

It is made up of three sections:

- Pandora ITSM API settings: The main section to configure allows the connection and transfer of data and information through the PITSM API.
- Alert default values: Configure default values for alerts.
- Event custom response default values: Configures the default response values for events.

Pandora ITSM API settings

Both the incoming connection for Pandora ITSM and the incoming connection for Pandora FMS must be configured to guarantee bidirectional communication.

- URL to Pandora ITSM setup: Web address or IP address to connect to the Pandora ITSM API, for example:

```
http://172.16.0.2/integria/api/v1
```

- URL connect to API Pandora FMS: URL to connect to the Pandora FMS API, by default it takes the one established in the Public URL token and if not the one in `config.php` is established.
- Test buttons: Each one will test the connection from Pandora FMS to Pandora ITSM and vice versa.
- If the connection tests are successful, Pandora ITSM will take the PFMS agents and convert them into inventory objects and PITSM incident management will be available from PFMS.

Alert default values

In this section called Default values for alerts, the default parameters will be established to register incidents in Pandora ITSM from the alerts generated in Pandora FMS. All fields refer to Pandora ITSM and the connection must have been configured first according to the Pandora ITSM API settings section.

Event custom response default values

In this section called Default values for events, the default parameters will be established to register incidents in Pandora ITSM from the events generated in Pandora FMS. All fields refer to Pandora ITSM and the connection must have been configured first according to the Pandora ITSM API settings section.

Module Library

E This option allows you to save the credentials to access the Pandora FMS Enterprise Library directly from the Console.

Notifications

In Pandora FMS there is a notification and monitoring system for the status of the console and the system in general. You can enable notifications by following the instructions in the Console Management section.

QuickShell

From version 774 onwards, Pandora FMS QuickShell feature was upgraded and for its proper functioning, it will be necessary to have the pandora_gotty binary installed in `/usr/bin/`. This feature is installed by default in version 774 of Pandora FMS and the only additional configuration will be to allow the connection to the installed firewall and add port number `8080`.

If you are upgrading to PFMS version 774, see the migration process to `pandora_gotty`: "Upgrade to version 774".

QuickShell Settings

In menu Management → Setup → QuickShell → GoTTY general parameters, in the Address field, enter the IP address or URL of PFMS Web Console and the port number to use (remember to allow connection in the corresponding firewall). Save the values by clicking on Update (saving forces QuickShell to be run).

Connection can be enabled through SSH (Enable SSH method) and/or Telnet (Enable telnet method), when configuring the desired values, save with the Update button (when saving, it forces QuickShell to be run). The connection can then be tested and verified with the corresponding Test buttons.

Optional QuickShell configuration with safe methods

If you have SSL certificates, it is advisable to encrypt conection transmission to strengthen computer security.

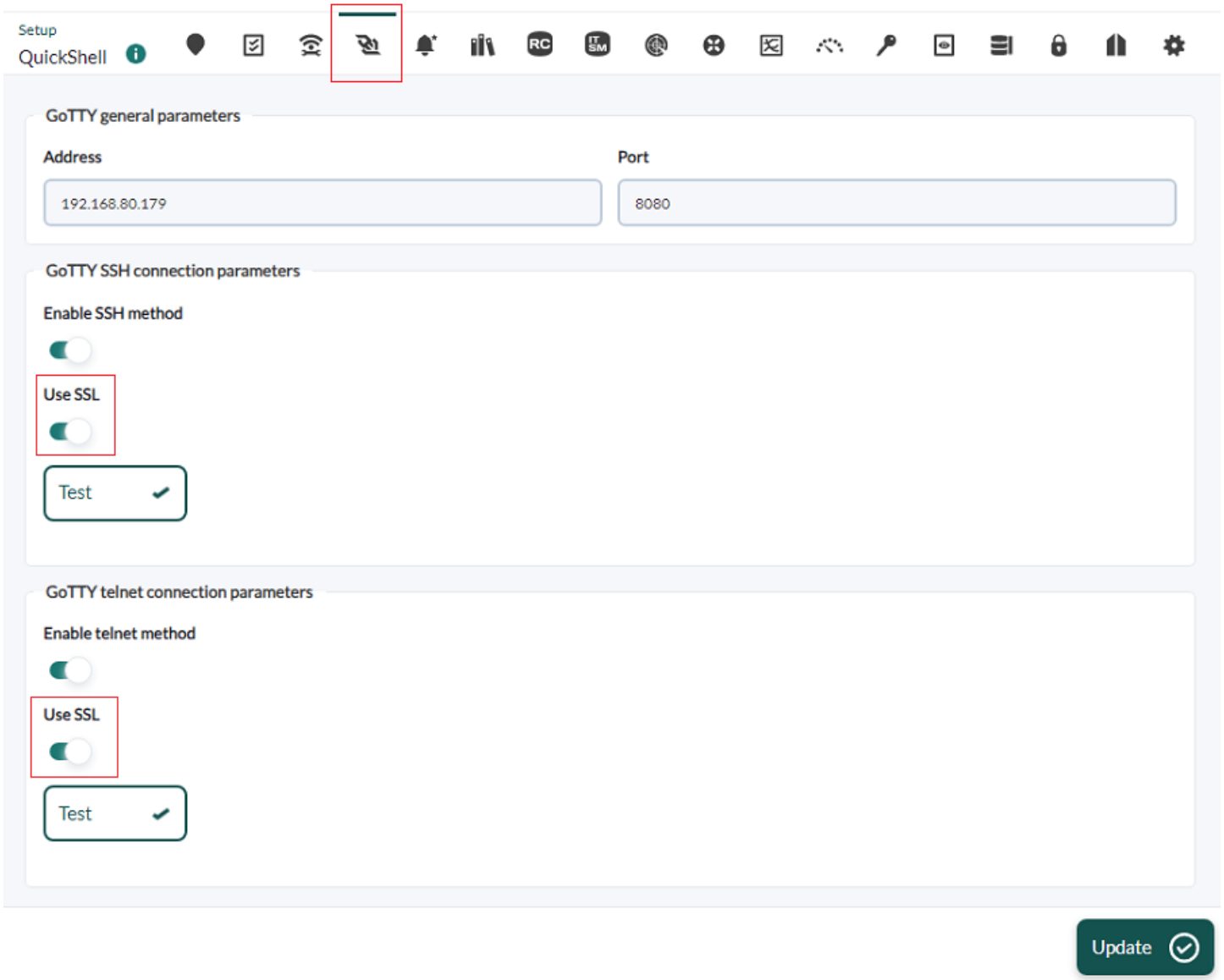
Before proceeding to encrypt communications (Use SSL corresponding to SSH and/or Telnet) the following configurations must first be made:

- You must have SSL certificates in Pandora FMS Web Console
- These certificates must have reading permissions for the Apache web server.
- Add the following TLS/SSL options to the file `/etc/pandora_gotty/pandora_gotty.conf` (replace the path and file name for each parameter with the values to use):

```
Pandora Gotty config file

(…)

  [bool] Enable TLS/SSL
enable_tls = true

  [string] Default TLS certificate file path
```

```
tls_crt_file = "/path/.cert.crt"

  [string] Default TLS key file path
tls_key_file = "/path/key.key"

  [bool] Enable client certificate authentication
enable_tls_client_auth = false

  [string] Certificate file of CA for client certificates
tls_ca_crt_file = "/path/ca_cert.ca.crt"

(…)
```

Again in the menu Management → Setup → QuickShell → GoTTY general parameters in the Address field, enter the IP address or URL that matches the added values, check Use SSL for SSH and/or or Telnet and save by clicking Update (saving forces QuickShell to run). The connection can then be tested and verified with the corresponding Test buttons.



Update to version 774

- The WebSocket service on the PFMS server to be updated must be stopped and then disabled.
- Stop the old gotty process. The following command identifies it and stops it:

```
kill $(ps aux | grep gotty | awk '{print $2}')
```

- To verify that it stopped running:

```
ps aux | grep -v grep | grep gotty
```

- Download and install the pandora_gotty package:

- For Ubuntu server:

https://firefly.pandorafms.com/ubuntu/pandora_gotty_1.1.0.deb

- For EL 7 / EL 8:

https://firefly.pandorafms.com/centos8/pandora_gotty-1.1-1.el8.x86_64.rpm

- Configure Quickshell in PFMS web console. When performing the update, the connection must be enabled through SSH (option Enable SSH method) and/or Telnet (option Enable telnet method), when configuring the desired values, save with the Update button (saving forces QuickShell to run). The connection can then be tested and verified with the corresponding Test buttons.

External tools

In the external tools section you can configure the alarm sounds for them, in addition to the default paths of their executable files. You can also define your own custom commands using macros to interact with Pandora FMS agents.

Welcome tips

Menu Management → Setup → Setup → Welcome tips.

Tips are short messages, whether or not accompanied by a web link to further details of the tip displayed when you log in to the PFMS Web Console. You can set the language for each of them and to edit them, it has a filter that allows you to search by keyword in the title of each tip. Each user will be able to establish their own user configuration with the Show usage tips at startup token.

Through the classification of Profiles established read in PFMS you can configure the welcome tips in the drop-down list in Profile, depending on the profile allowed to each user, they may or may not view them.

- Add one or more related images as long as their size is 464 by 260 pixels.
- Each tip may or may not be enabled to be viewed.

GIS map connection

All documentation on GIS maps can be found in the section Pandora FMS GIS.

License

Once you have installed Pandora FMS you can perform the application of a license. Then in this section you can find out its status, request a validation (Validate button) in the case of reinstalling a Pandora FMS instance or request a new license (Request new license button). . In the Show agent usage detail button you can see the total number of agents (with the option to filter by enabled agents) as well as the subtotals classified into three large categories.

If the Satellite server option is active, a license encryption key can be configured (License encryption key) that will guarantee the secure transmission of said token to the Satellite server. This same key will need to be configured on the Satellite server.

The server is installed with a trial license valid for a maximum of 100 agents and one month of use. If you wish to expand this license, contact your trusted sales representative or fill out the following contact form.

The Community version (Open) does not require any license to use.

Skins

This functionality allows you to customize the appearance of the interface (skin) of the Pandora FMS console. This is achieved by changing the CSS style files and icons associated with the interface.

To create a new skin, you must replicate the directory structure that the console has by default:

- `images`: the directory that will contain the skin images.
- `include/styles`: the directory that will contain the skin's CSS files.

This will hang from the `<pandora_root>/images/skin/` directory. This entire file structure and its content must be compressed in a zip file.

A skin can be applied at two levels:

- User: It will be applied to the user directly.
- Group: Will apply to all users who belong only to that group.

If a user has a skin applied per user and group, priority will be given to the user assignment and then to the group assignment.

Translate string

Go to the side menu and click Setup → Translate string. You can make your custom translations (Customize translation column) even with macro variables; This extension is fully described in the section Translate string.

Admin tools

System audit log

Menu Management → Admin tools → System Audit Log

Pandora FMS keeps a record or log of all important changes and actions produced in the Pandora FMS Console. You can get more information in the section Audit log.

Links

From Management → Admin tools → Links you can access the web links management page of the Pandora FMS console.

Both to create a new web link and to update an existing one, the process is practically the same. Once you have edited and/or added all the necessary web links you will always have them at hand in the left side menu.

Diagnostic info

Access through Management → Admin tools → Diagnostic info the visual tool that shows the current status of the Pandora FMS server and console. If you want to obtain this information via the command line, see Pandora FMS Optimization and Troubleshooting.

E There is the option to export all the information in PDF.

Omnishell

E

Omnishell is an Enterprise functionality of Pandora FMS that is used for the orchestration and automation of information technologies. You can get more information in the section IT Omnishell Automation.

IPAM

With the IPAM extension you can manage the IP addresses of the networks. You can get more information in the section IPAM: IP Address Management.

Site news

From Management → Admin tools → Site news it is possible to add the news that appears on the home page when a user enters the console.

To create a news item press Add, write the subject or title in Subject, select the group that will receive the announcement and the deadline to be shown. If you select Modal window the news will be displayed in a pop-up that the user must read and close.

File Manager

Useful tool to upload content to Pandora FMS, menu Manage → Admin tools → File Manager . The entire contents of the `images` folder within the Pandora FMS installation will be displayed.

- Download the files you want by clicking on the name of each one of them.
- Navigate through the directories, these are identified with the icon  . You can also create subdirectories in them.
- Upload files by clicking on the icon  , these image files will be identified with the icon  (only formats are allowed GIF, PNG and JPG).
- You can also delete some files that have the icon  , since the rest are system files used by the PFMS Console.
- A directory can only be deleted if it is empty.
- If you want to customize the images in the Visual Consoles, four different images are needed, one for each state, using a special nomenclature for these images: < image_name>_<state>.png where the state can be:
  - < image_name >_bad.png
  - < image_name >_ok.png
  - < image_name >_warning.png
  - < image_name >.png (no state)

Keep in mind that if the compressed file you upload contains a structure of directories and subdirectories with the files in each of them, said structure will also be created in `/var/www/html/pandora_console/images/` .

DB Schema Check

This check can only be performed on MySQL Databases.

This is an extension that allows you to check the structural differences between the established Pandora FMS database, and a pattern scheme to compare possible errors. See the section "Console management and administration".

DB Interface

This is an extension that allows you to run commands on the database and see the result. It is an advanced tool that should only be used by people who know SQL and the Pandora FMS database schema in sufficient detail.

DB Backup Manager

Allows you to manage scheduled database backups using a Console task ("Console Task").

- In the Filter section you can choose from the drop-down list in Path backups the location of the available backups. Press the Filter button to update the backup list.
- You can download the backups to your local machine using the corresponding button.
- You can delete backups using the corresponding button.
- To restore a backup press the corresponding button.

Elasticsearch Interface

To activate the Elasticsearch interface, the Activate Log Collector token must be enabled in Management → Setup → Setup → Enterprise.

In the default configuration Pandora FMS generates an index per day, which ElasticSearch is responsible for fragmenting and distributing for future searches. For these searches to be optimal, by default ElasticSearch generates an index for each of them, so as many searches must be configured in the environment as there are ElasticSearch nodes installed.

These search and replicas are configured when an index is created, which Pandora FMS generates automatically, so to modify this configuration we must do use the templates.

Acoustic console setup

Allows you to configure the default sounds for the different event alarms.

API checker

The API checker allows you to call and check the Pandora FMS external API. See the External API section.

Extension manager

Extension manager view

Extensions are a way to develop new functionality for the Pandora FMS console, as well as plugins. See the topic Developing console extensions for more information.

From the menu Admin tools → Extension manager → Extension manager view you can disable by clicking on the icon  corresponding to each extension.

You can also delete an extension with the corresponding  button. Managing extensions of visible type adds or removes elements in the left side menu.

Extension uploader

From the menu Management → Admin tools → Extension manager → Extension uploader view you can upload an extension. The file must be compressed in `.zip` format. If the extension uses the `gpolicies` component, check the Upload Enterprise extension option. Once you have chosen the file, click the Upload button.

System logfiles

In the menu Management → Admin tools → Extension manager → System logfiles it can be viewed, limited to the size of the token Log size limit in system logs viewer extension (General setup), the content of the following files:

```
/var/www/html/pandora_console/log/console.log
/var/log/pandora/pandora_server.log
/var/log/pandora/pandora_server.error
```

CSV import group

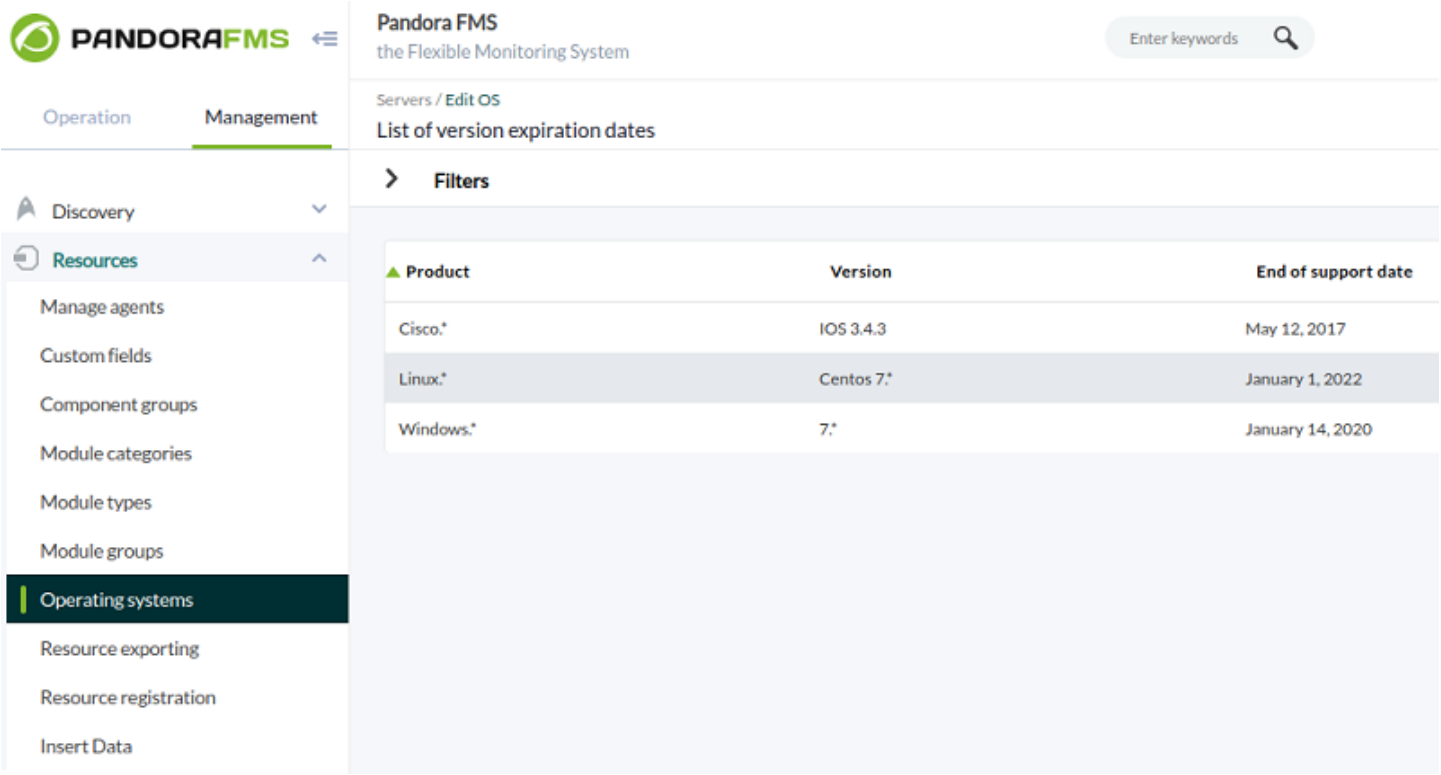
 See the section Import groups from CSV in “Console management and administration” .

Resources

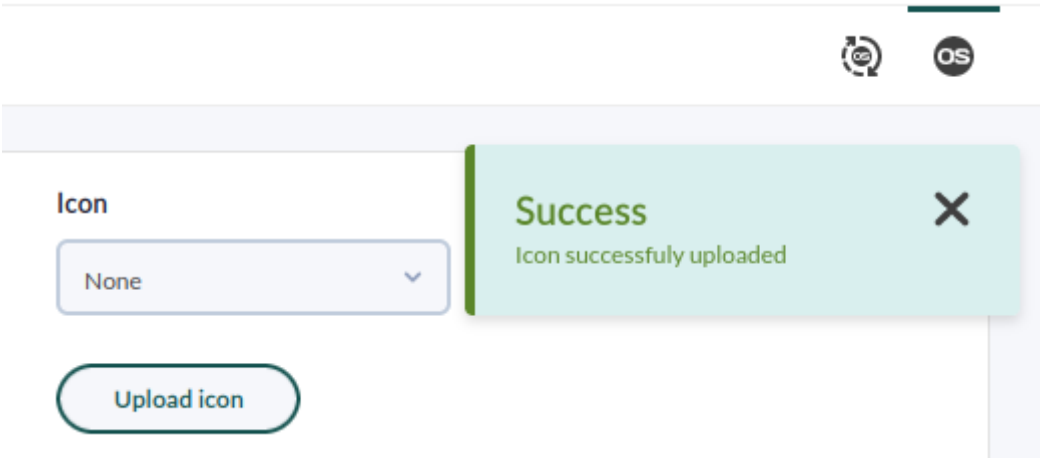
Operating systems

In this section you may edit or create new types of Operating System (OS), Management → Resources → Operating systems. These groups are important for automatic agent provisioning.

Starting with version 774, PFMS has the scheduled obsolescence feature enabled, which works with inventory to obtain reports with filters for monitored devices.



If you have a new operating system, you can add it to the default list when installing PFMS. To do this, click on the Create OS button, enter the corresponding name and choose an icon from the list. If you have a new icon in JPG, JPEG, PNG or SVG format, use the Upload icon button, store it in PFMS and then search and select it by name. The process is finished with the Create button.



Tools

Export data

The menu Management → Tools → Export data allows you to choose an agent (which can be filtered by group) by its name and then select one more modules from it. By default, the time period is the last 24 hours and the available export formats are:

- Data Table: A special PHP language format that displays the agent name, module name, data value and date and time of data collection.
- Average per hour/day: If the data is numeric and can be averaged, it will be displayed on the screen in a similar way to the Data table option.
- CSV: File in comma delimited fields format.
- MS Excel: Spreadsheet file, format for Microsoft Excel.

File repository manager

The file repository manager allows you to add the resources you need to be downloaded by the devices to be monitored when appropriate. It can be accessed from Management → Admin tools → Extension manager → File repository or from Management → Tools → Tools → File repository and then click on the Management view icon.

Select the group(s) that will download this resource and browse your local disk to *upload* this file. If you need to make this resource public, check the Public link box. Click the Add button and wait for the *upload* process to complete.

- To share the public link of each file click on the icon , copy and paste the web link.
- If another operator of the same PFMS Console is on another computer, you will be able to download it by clicking on the button .
- If the file is no longer needed, delete it with the button .

Return to Pandora FMS documentation index