Installation and configuration

Installation and configuration

Installation

The installations of the Instances and the Command Center (Metaconsole) must be hosted in servers that communicate in both directions.

- Check that the Command Center can contact the Instances.
- Check that the Instances can contact the Command Center.

Instances do not need to communicate with each other at any time, for more details see Command Center architecture.

- The time setting must be the same. The more synchronized the Instance and Command Center timers are, the more accurate the displayed data will be.

Instances

An Instance or node is a common Pandora FMS installation, made up by a server and a Web Console.

Command Center

A Command Center is a Pandora FMS installation with a special license for it.

Pandora FMS Console and Command Center cannot be used at the same time.

It is necessary to have a server active to be able to perform different operations related to the Command Center, such as “migration”, “self-provisioning”, service execution, etc.

License activation

After activating the license from Pandora FMS Web Console, whatever the installation method is, access Pandora FMS console:

```
http://< dir_IP_or_URL >/pandora_console/
```

A welcome screen will appear to accept the license.

In order to activate the Command Center, a Command Center license is required. *Once the node license is activated, the normal Console will appear*.

Metalicense

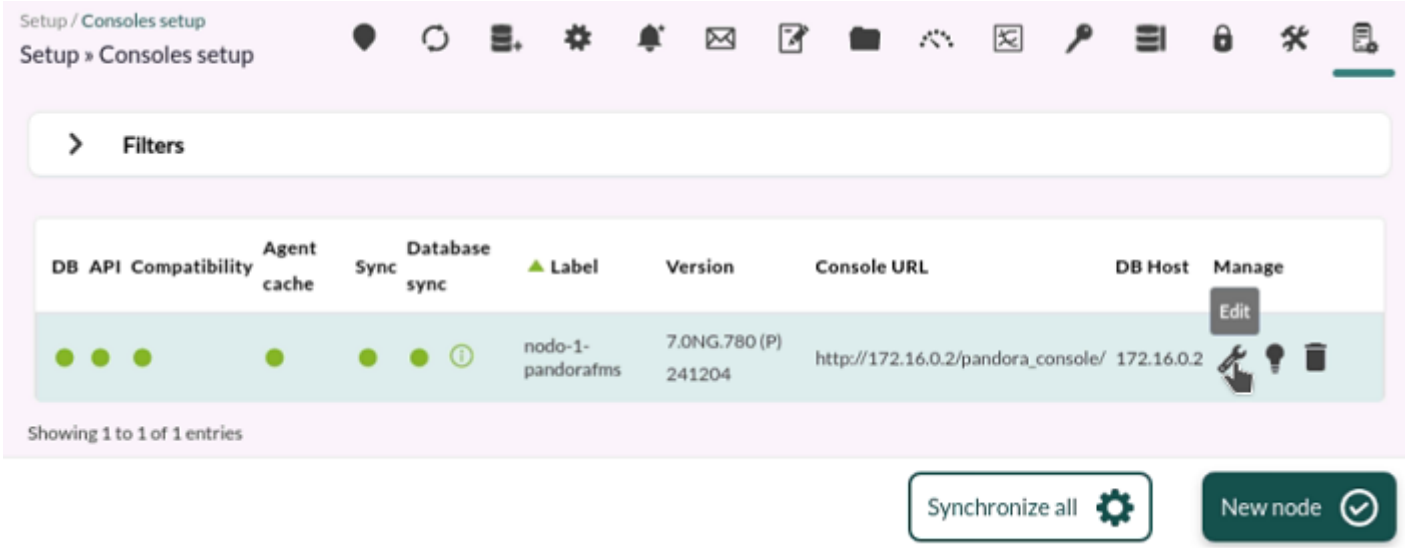
From Pandora FMS version 7.0 NG onwards, a single license is available for a Command Center environment. You may create as many Instances as you wish, as long as the total number of agents inside the Command Center is not exceeded.

This license is applied in the Command Center and may be synchronized in as many Instances as desired, thus allowing centralized management of the different agents to be deployed in those Instances.

If you need nodes that may remain disconnected from the Command Center for long time periods, contact Pandora FMS team.

Metalicense sincronization

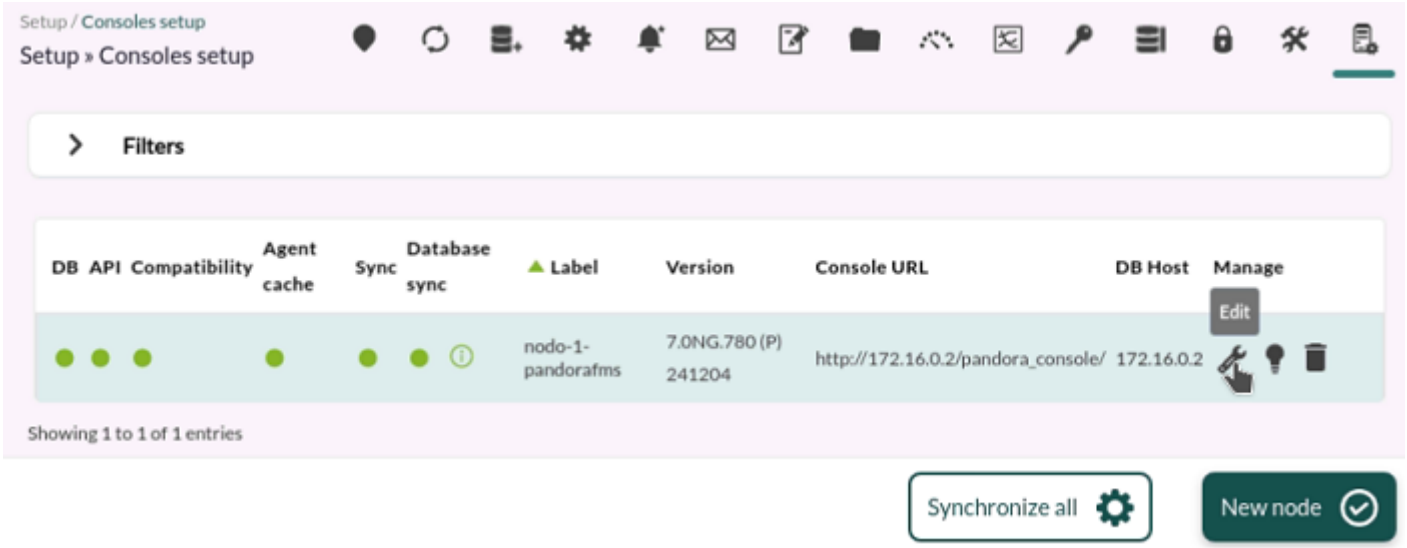
- The Instances (nodes) must have their own key generated and correctly validated.
- Once the nodes are generated and correctly validated, they are configured in the Command Center.
- All statuses should appear normal (green) and if necessary the synchronization button Synchronize all should be used:



- Once all these steps have been completed for each node, access the Command Center license and click Validate to synchronize the Metalicense with all the Instances.

Instance Registration

Setup → Metasetup → Consoles setup menu.



In the Metasetup section, you may register and configure the Instances with which the Command Center will be linked.

In order to register a new Instance, a series of parameters related to the Instance to be managed must be known. If it is the registration of an Instance that has not yet been registered with a license, the default data are:

- Server name: `localhost.localdomain`.
- API password: Empty.
- DB host: Database IP address.

- DB name: `pandora`.
- DB user: `pandora`.
- DB password: `pandora`.
- DB port: `3306`.
- Control user: `admin`.
- Console password: `pandora`.
- Console URL:

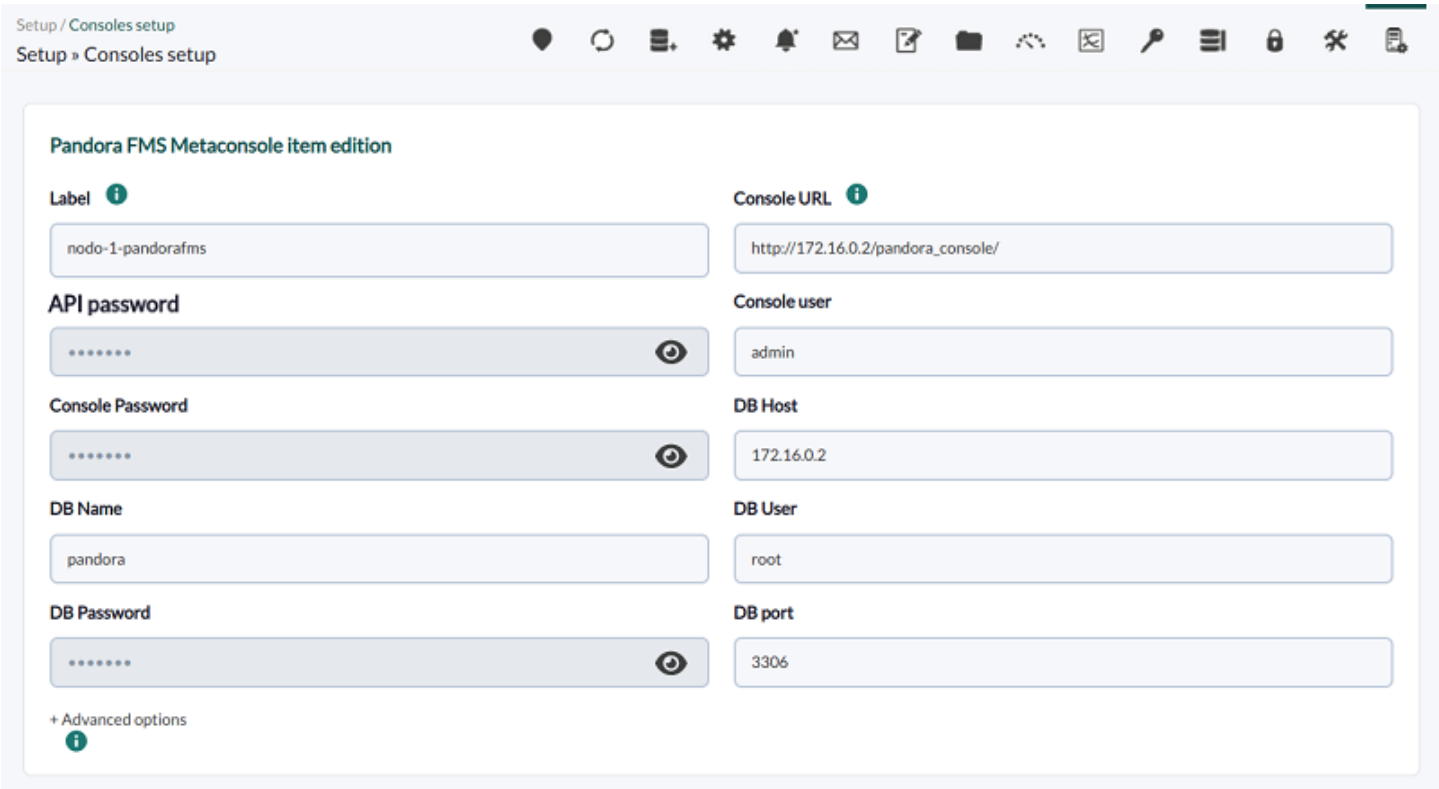
```
http://< dir_IP_or_URL >/pandora_console
```

Advanced fields

To ensure connectivity between nodes and the Command Center, connection data may be configured manually.

- Metaconsole DB host: Database IP address.
- Metaconsole DB name: `pandora`.
- Metaconsole DB user: `pandora`.
- Metaconsole DB password: `pandora`.
- Metaconsole DB port: `3306`.

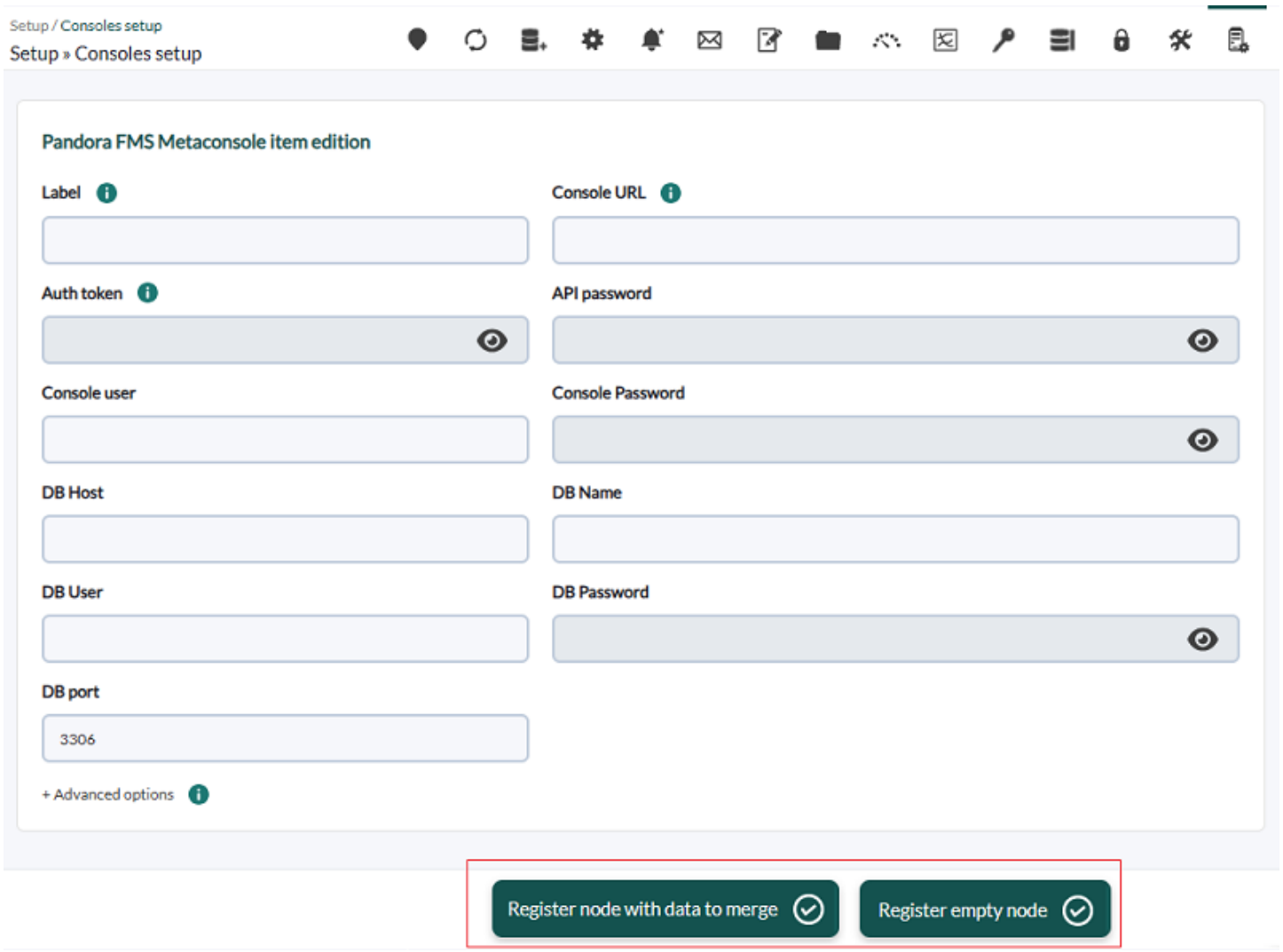
These fields indicate the configuration of the connection to be established by the *node* against the *Command Center*.



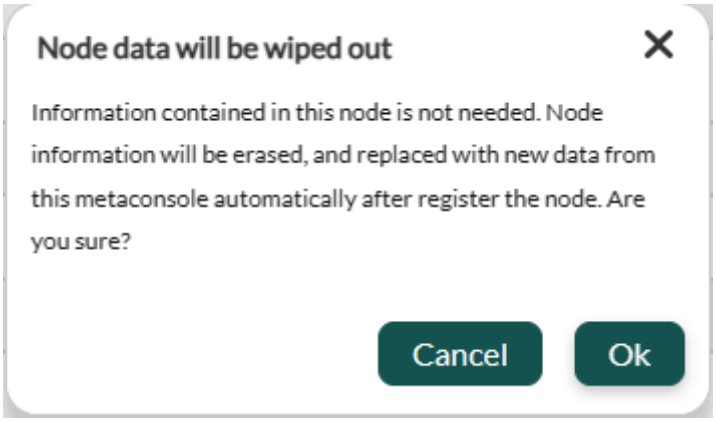
In case it is a Pandora FMS installation, where a valid license has already been included in the Instance, you have to obtain this data from the Instance configuration and the Instance database.

All the fields must be filled in to connect and when saving, if it is a completely new node, without

any data, it will be added with the Register empty node button, otherwise the Register node with data to merge button should be used.

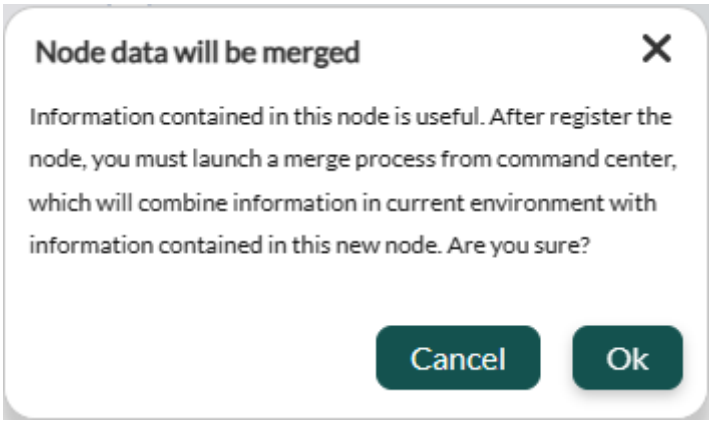


- When using the Register empty node button, a warning window will be displayed, indicating that the data in the node will be deleted:



Click OK if you are sure and the new node will be centralized.

- When using the Register node with data to merge button, a confirmation window will be displayed indicating that the data in the existing node will be centralized:



In the view of the configured Instances, it may be seen that the Instances may be modified, deactivated and deleted. There are indicators that check certain information of the configuration of each instance. These checks are performed when loading this view, but may also be done individually by clicking on them.

The indicators are as follows:

- Database: If the Instance database has been misconfigured or does not have the necessary permissions, the indicator will be red and will give information about the problem.
- API: This flag will test the Instance API. If it fails, it will give failure information.
- Compatibility: This flag checks some requirements between Instance and Command Center. The name of the Instance server, for example, must match the name given in its configuration in the Command Center.
- Event replication: This indicator shows whether the Instance has event replication enabled, and if events have already been received from the Instance, how long ago the last replication was.
- Agent cache: This indicator shows that the last statuses of the agents and modules of the node have been correctly saved in the Command Center database. When a change is generated, only that change will be modified in the database.
- Synchronization: This indicator refers to the possibility of being able to synchronize the different elements from the Command Center to those of the Instances.

The first three indicators must appear in green so that the Instance is properly linked and you start to see its data. On the other hand, the Event Replication indicator only gives information about this feature.

- An Instance may be configured, but without replicating its events.
- Once you have chosen to replicate the events, all event management will be done from the Command Center, leaving the Instance events as merely informative.

In case of enabling database encryption, all nodes and the Command Center must use the same configuration of `encryption_passphrase`.

Report scheduling

NG 755 version or earlier: you should configure the use of the Command Center, you have all the relevant information there.

It is necessary to install server packages in the system where the Command Center is installed in order to be able to launch the Database maintenance script (`pandora_db`). You should make sure that it is properly programmed for its execution in the cron every hour (as it is detailed in the following link).

If you are going to use on-demand reports (sent by e-mail) you need to schedule the execution of the cron extension just as you do in a normal Web Console. Generally, this is done by entering the following line in the cron, setting the local paths accordingly:

```
/5 * * * * <user> wget -q -O -
http://x.x.x.x/pandora_console/enterprise/extensions/cron/cron.php>>
/var/www/pandora_console/log/console.log
```

For versions prior to 747 the path will be:

```
/var/www/pandora_console/pandora_console.log
```

Finally, to configure SMTP for sending e-mails, you need to edit the corresponding parameters in the mail configuration section.

API

Access to the Instance API will be granted with the following parameters:

- Username and password: A valid username and password must be known in the Instance.
- API Password: The API access password configured in the Instance must be known.
- List of IP addresses with API access: In the Instance configuration, there is a list of IP addresses that may access the API. The asterisk may be used as a wildcard to give access to all IP addresses or to a subnet.

Self-authentication

In some parts of the Command Center there are accesses to the Instance Web Console; for example, in the event viewer, clicking on the agent associated to an event (if any) will lead to the view of that agent in the console of the Instance it belongs to.

For this type of access autoauthentication is used. This authentication is performed by activating the token Setup → General setup → Auto login in node.

Configuration

To configure the Command Center, go to Setup → Metasetup. Each instance or node has also its own configuration.

Warp Update Online

Setup → Metasetup → Warp Update Online menu. This section will only be visible if Enable Warp Update is enabled in General Settings.

If you have a valid command center license and Internet access, you will be able to update the Command Center automatically.

Warp update Offline

Setup → Metasetup → Warp Update Offline menu. This section will only be visible if Enable Warp Update is enabled in the General Settings.

Applying patches and/or updates offline may make the Web Console unusable, before that, it is recommended to perform a full backup.

- It allows you to update and/or patch the Command Center without the need to connect to the Internet.

* Only the files should be uploaded in order up to the version that needs to be updated, since they are not cumulative versions.

The Warp Update Offline also helps you install different kinds of patches: console, server and manual combined patches.

When accessing this section, a unique access code related to the applied license will be displayed and must be copied by clicking on the icon . Click on the indicated link to open in a new tab of the web browser, paste the code and log in and download the necessary files. If no code appears, sign up with an e-mail address and you will get the unique access code right away.

- When you enter the download web page, you will see the version installed according to the license and you will be able to search for updates by name and description.
- Once the search for the desired update is ready, click View details to see its contents.
- A dialog box will open with the different files for downloading one at a time.
- Once the file(s) have been downloaded, access the Warp Update Offline menu again and click Browse

it to select file by file.
- The size of each file must be smaller than specified in the `post_max_size` and `upload_max_filesize` tokens in the `/etc/php.ini` file.
- The information displayed on the screen should be checked to see whether it matches the updates and/or modifications. To process, click on the green icon in the lower right corner and wait for the Web Console to display the results of each process.

Warp Update Journal

Setup → Metasetup → Warp Update Journal menu. This section will only be visible if Enable Warp Update is enabled in the General Settings.

Click Warp Update Journal to see the updates performed, version, date and time of application, user who requested and applied it, and so on. Over time you will accumulate many records which may be filtered by expanding the Filter box and entering the keyword to search for.

Warp Update Setup

Setup → Metasetup → Warp Update Setup menu. This section will only be visible if Enable Warp Update is enabled in General Settings.

By default it is already configured to perform the update online.

Contact support before changing any of the following fields:

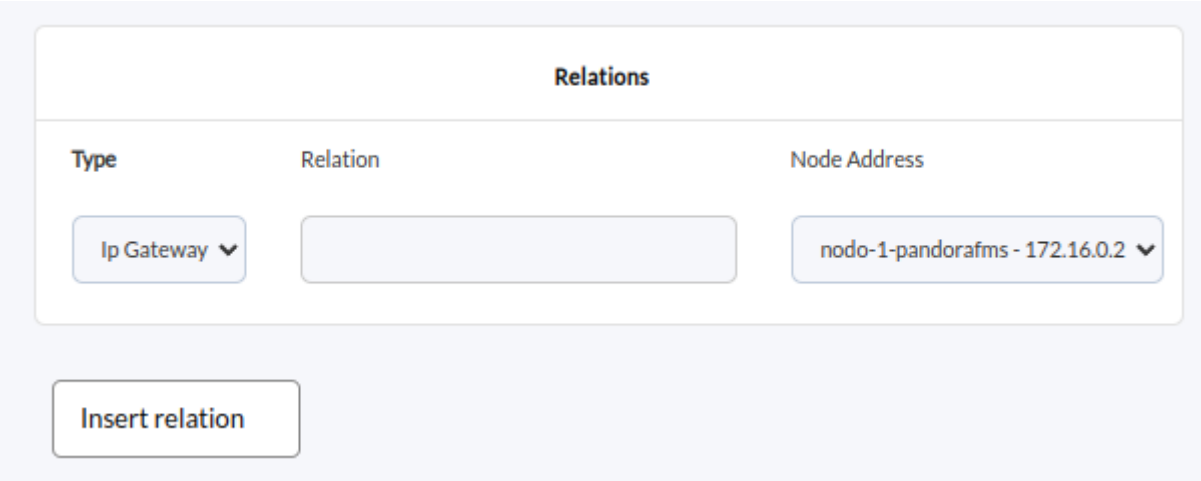
- Warp Update URL.
- Use secured Warp Update.
- Proxy server.
- Proxy port.
- Proxy user.
- Proxy password.

Relations rules

Setup → Metasetup → Relations rules menu.

To enable this feature, the Enable API agent token must be enabled in the general settings.

It allows to quickly retrieve information about certain special devices by means of an API (different from the main API).



In the Relationships box choose a Type, drop-down list: Ip Gateway or IMEI) and assign a relationship value which will be used in the API query. This query will return the Node address that you selected, either one of the Command Center (Metaconsole) nodes or a custom node through Custom. Once the three fields described above have been set, click Insert relation to save the new relation.

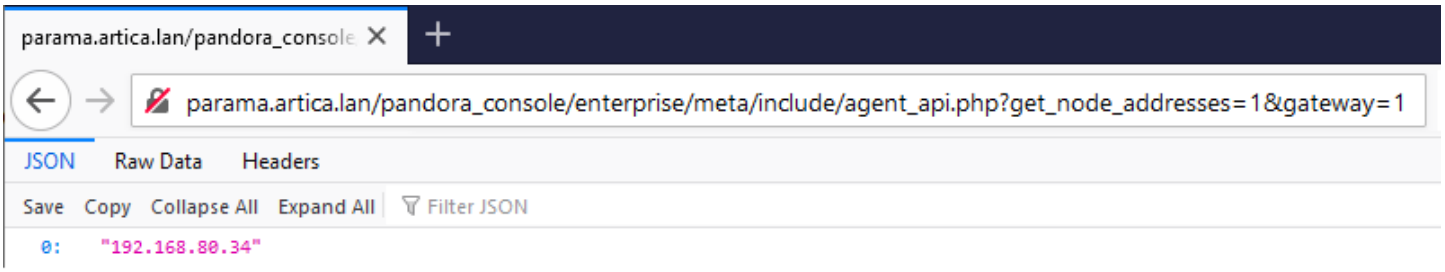
To load a list of relations prepare a file in CSV format with the following order:

`imei,<rule>,<node>` o `gateway,<rule>,<node>` .

Illustrative values: `gateway,4,192.168.80.37` .

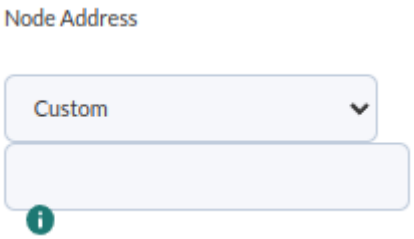
The saved relationships will be displayed at the bottom and may be filtered by type, value or node address. You may also delete relationships one by one or select several or all of them with the corresponding checkbox and then clicking Delete to mass delete.

Relationship queries will be returned in JSON format. In Mozilla Firefox web browser for `gateway=1`:



In Mozilla Firefox web browser for `imei=2`:

By means of the Node Address Default button you may configure to return a preset response when there is no relationship rule established or when no relationship rule is found that matches the request made. This response may be either the IP address of one of the Metaconsole nodes *or a custom message by selecting the option* Custom:



Notifications

Setup → Metasetup → Notifications menu.

In Pandora FMS there is a system for monitoring Console and system status in general.

- By clicking on the notifications icon you may add or subscribe to each category of notifications those users or groups who will receive the notification.
- For System status you may additionally specify each technical aspect for each of the registered users or groups.

The different types of notification are as follows:

1. System status.
2. Message.
3. Pending task.
4. Advertisement.
5. Official communication.
6. Suggestion.

The Enable user configuration token enables users, in the Operation → Workspace → Configure user notifications section, to enable or disable such notifications in Console and/or by e-mail.

For notifications to arrive by e-mail, users must have their user profile e-mail configured, and Pandora FMS server must also be configured to send e-mails.

If a user belongs to a group and that group is added to one of the notification categories, said user will have active Console notifications for that corresponding notification category, however they cannot modify them even if the Enable user configuration token is already enabled (for that category).

By default, the `admin` user comes with the active notifications of System status and Official communication *even if these categories are inactive*. All superuser that is added later will be in all notification categories.

Mail

Setup → Metasetup → Mail ✉ menu.

In this configuration a series of values must be established such as:

- Exit address (From dir -From address-).
- Name of outgoing address (From name).
- The IP address or FQND of the SMTP server (Server SMTP).
- SMTP port number (Port SMTP).
- Type of encryption for privacy (Encryption): SSL, SSLv2, SSLv3, STARTTLS.
- If necessary, the user and password of the email user (E-mail user and E-mail password).

When using a Gmail® account, Google® may block authentication attempts by certain applications. For proper operation, it will therefore be necessary to enable access by insecure applications. More information on how to do this can be found on the official Google® support pages.

For security reasons use a Gmail® email account created specifically and only to send Pandora FMS server warning messages. Never use a personal email account for this purpose.

If necessary, modify the `mta_auth` token in the `/etc/pandora/pandora_server.conf` file. This token, by default, is established as a comment, so it should be activated by editing this line and placing the required authentication type, see this link for more details.

Once the email configuration is saved, by clicking on the E-mail test option you will be able to check whether your configuration is correct by sending an email automatically generated by Pandora FMS to a desired email address. Only if the selected configuration is correct, you will be able to see the email in your inbox.

Make sure that Pandora FMS server is able to *resolve*, through its DNS server, the mail server in charge of your mail domain.

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

It is necessary to check, also in this case, that the mail server accepts the mails redirected from Pandora FMS server.

For more information you may check Pandora FMS server configuration.

Strings translation

Setup → Metasetup → Strings translation menu.

It allows to translate text strings from Pandora FMS interface in a customized way.

- Language: It allows you to filter the string by language.
- Free text for search (*): Content of the string to be customized (this field may be left blank to display all strings).

Three columns will appear: the first one will show the original string, the second one the current translation and the third one the custom translation to be added. The last column must be completed and the Update button clicked to save.

Care should be taken to copy exactly the same HTML code and JavaScript language that may appear in the text to be translated.

File manager

Setup → Metasetup → File manager menu.

File manager where you may upload and delete files in the folder images of the Command Center installation.

The Command Center code reuses some images from the normal console code. These images will not be accessible from this manager and it will be necessary to access the installation manually to manage them.

Performance setup

Setup → Metasetup → Performance setup menu.

The Database maintenance status section informs about the maintenance and compaction of PFMS database. The following parameters are used for these processes.

Performance.

- Max. days before events are deleted: Field where the maximum number of days before deleting events is defined.
- Front page for custom reports: The custom report cover page will be applied by default to all reports and templates.
- Max. days before audited events are deleted: Number of days of event auditing to be maintained.
- Default hours for event view: Field where the hours field of the default filter in the event view is defined. If it is 8 by default, the event view will show only the events that took place in the last 8 hours. This field also affects event display, counting and graphing in the tactical view.
- Migration block size: Migration block size. It is used to migrate (move) agents between nodes in Command Center environments, especially to transfer history data between one node and another.
- Events response max. execution: Number of events that will perform the desired action at the same time.
- Max. number of events per node: Maximum number of events to be displayed for each node.
- Row limit in CSV log: Limit of rows for the record in CSV format.
- Max. macro data fields: Field where the number of macros that may be used for alerts is defined.
- Limit of events per query: Limit set for the maximum number of events in a query, by default five thousand items.
- Max. days before purge: Field where the maximum number of days before deleting data is defined. This also specifies the maximum number of days to keep history inventory data.
- Rows limit for SQL report item PDF (per node): Before increasing this value, it should be noted that a high value may affect the performance of PDF generation. You may use `0` to disable this limit.

Visual setup

Setup → Metasetup → Visual setup menu.

Note that group synchronization may change the node's group configuration.

Visual styles:

- Date format string: It allows specific formatting of the date and time. By default it uses `F j, Y, g:i a` (full name of month and day, year and hour and minute). It is denoted according to PHP language; to add the timezone add `T` and/or `e`.
- Graph color: It allows you to choose a color for each of the three graphics.
- Data precision for reports and visual consoles: Number of decimal places to display in reports and visual consoles. It must be between `0` and `5`.

- Percentile: It displays a percentile in graphs, by default 95.
- Value to interface graphics: Name of the units for the network interface graphics, by default `Bytes`.
- Block size for pagination: It allows paginating multiple results (alerts, events, etc.); by default in blocks of 20 elements. If a lower value is defined, notifications will be obtained according to this.
- Number of elements in Custom Graph: To limit the number of legends in combined plots, *it is recommended to reduce the width of the legends, make them summarized and as short as possible*. The combined charts that respond to this token are: Line, Area, Vertical Bars, Horizontal Bars, Stacked.
- Use round corners: Use rounded corners in graphics.
- Chart fit to content: There are graphs whose values are percentages and the top of the graph exceeds the maximum value of one hundred, by enabling this option you may configure the graphs to stop adding a proportional upper margin.
- Graph TIP view: (*This option may cause performance problems*) It indicates whether to display TIP charts:

1. None: The TIP option in the graphics setup will be disabled (default option).
2. All: The TIP option in the graphs menu will be activated in all graphs.
3. On Boolean graphs: The TIP option will only be activated in the menu for true and false graphs.

- Graph mode: It allows to show only the average or the average with the minimum and maximum values.
- Zoom graphs: Graphics zoom, by default 100%.
- Type of module charts: By default the modules will be presented as area charts, the other option is line charts.
- Metaconsole elements: The number of elements that each instance or node will return in certain views. By default `100`.
- Add new custom value to intervals: It allows to add custom time intervals (except for the event comment view). The numerical value must be entered and the time unit selected, then click Update. The added interval will then appear in the Delete interval list where it may be deleted. The deletion process consists of selecting the interval to be deleted from the list, clicking Delete and then Update.
- Show only the name of the group: To display the group name instead of its icon.
- Display data of proc modules in other format: proc data represent 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. By enabling this option, this second form of representation is used.

1. Display text when proc modules are in OK status: If the Display data of proc modules in other format option is enabled, this text appears instead of the number when the module has a correct status.
2. Display text when proc modules are in critical status: If the Display data of proc modules in other format option is enabled, this text appears instead of the number when the module has a critical status.

- Custom favicon: It must be in `.ico` format and its dimensions in 16 by 16 pixels to work properly. You may add icons to choose from in the `images/custom_favicon` folder.
- Custom background login: It allows you to choose a background for the login. Custom images may be placed in the `images/backgrounds/` folder. If the token Random background (login) is enabled, this option will be ignored.

- Product name and Copyright notice: These first two tokens to appear correspond to the instance (nodes) and allow the product to be renamed.
- Product name and Copyright notice: The second two tokens to appear correspond to the Command Center and allow the product to be renamed.

The following tokens allow you to change the Web Console icons for the expanded and collapsed

main menu:

- Custom logo (menu).
- Custom logo collapsed (menu).
- Custom logo (header white background).

The following tokens allow you to change text and images at user login, their names are self-descriptive:

- Title (header).
- Subtitle (header) (also used in the Web Console).
- Custom logo (login).
- Custom Splash (login).
- Background opacity % (login).
- Title 1 (login).
- Title 2 (login).
- Docs URL (login).
- Support URL (login).
- Random background (login).

- Graphs font family: Default font Lato selected, value immutable.
- Visual effects and animation: It allows you to disable animations at the start of each user session.
- Default cache expiration: This section indicates how often it clears the status cache of the elements and, therefore, how often it calculates the status of each element individually.
- Default interval for Visual Console to refresh: This interval will affect only the visual console pages, setting how often they will be refreshed automatically.
- Data multiplier to use in graphs/data: Value by which you will multiply the displayed data to represent it in the graphs. This is useful in case the unit of value is bytes; for all other conversions use Custom value post processing.
- Mobile view not allow visual console orientation: On the mobile console it prevents the screen from being rotated according to the motion sensor.
- Display item frame on alert triggered: It allows you to hide an orange box when you have a triggered alert in the Static image, Simple value, Icon, Group elements of the Visual Consoles. Enabled by default.
- Graphs font size: Field to choose the font size used by Pandora FMS for graphs. Immutable value, by default.
- Show unit along with value in reports: It displays the units in addition to the module value in the reports.
- Truncate agent text at end and Truncate module text at end: For the Operation → Monitoring → Views section, if enabled cut the name of the agents and modules at the end and place three ellipses (the default behavior is to cut in the middle).
- Agent text size and Module text: To choose the text size in the representation of agents and modules, accordingly.

Reports configuration:

- Show report info with description: Custom report description information. It applies to all reports and templates by default.
- Front page for custom reports: Custom report cover. It will be applied to all reports and templates by default.
- PDF font size (px): Font size for PDF report, default `10` dots per inch.
- HTML font size for SLA (em): Font size for SLA reports, default `2 em` (means 2 times the current font

size).
- Graph image height for HTML reports: It is the height in pixels of the module's graphic or of the custom graphic in HTML reports, default value `250`.
- CSV divider: Character or character set 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.
- Interval description: It displays the description of the time interval in abbreviated or unabbreviated form. A Long description would be “10 hours, 20 minutes, 33 seconds”; a Short interval is “10h 20m 33s”.
- Custom logo: The path to the custom logos is located at `images/custom_logo`, in the Web Console installation. More files in JPG and PNG format may be uploaded with the upload tool.

Authentication

The following fields are common to all options:

- Control of timeout session: By default enabled, it checks if there has been no activity in the time period set in Session time (mins) to log off.
- Session time (mins): The default value is `90` minutes and when this value is set to `0` for users, Pandora FMS will use the value saved in the General Settings, section authentication.
- Double authentication: Users may choose whether to enable two-step authentication on their accounts.

In remote authentication processes, it must be verified that port numbers are configured correctly.

Local Pandora FMS

Default authentication, it indicates that it will be done using Pandora FMS internal database. Users type superadmin for security reasons, always authenticate this way, the rest of the authentication types have the local option as fallback.

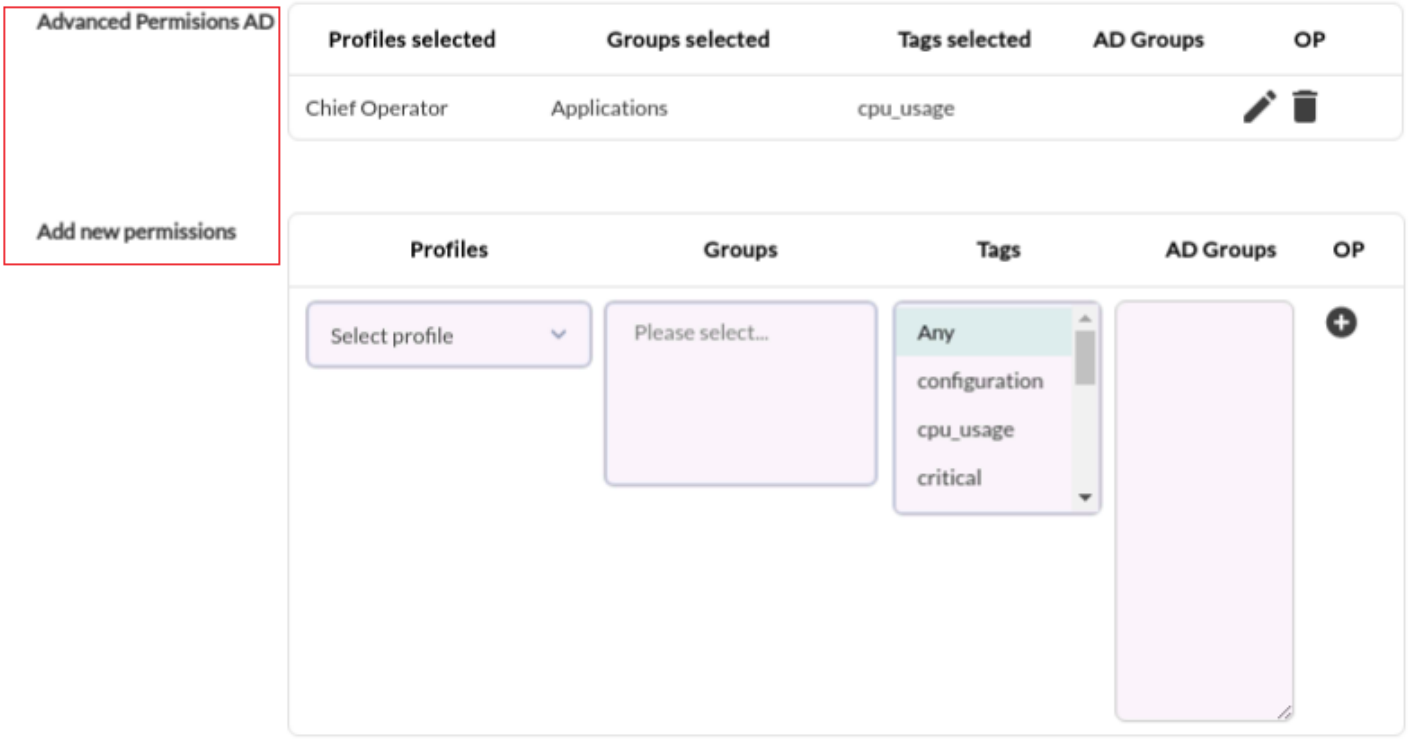
When choosing an authentication method such as Active Directory®, LDAP or SAML the Local Pandora FMS option will no longer be available as the exclusive authentication method. *However, users will always have the option of local authentication as a fallback*.

Active Directory®

- Automatically create remote users: It enables or disables remote user automatic creation. This option allows Pandora FMS to create users automatically once they log in. If this feature is enabled, the following numbered fields will be available:

1. Save Password: If enabled, it allows to save the AD passwords in Pandora FMS local database.
2. Advanced Configuration AD: If this option is enabled, the configuration of Advanced Permissions AD.
3. Advanced Permissions AD: It lists the advanced permissions that have been added in Add new permissions. This option will be enabled if you first save the preliminary authentication settings with Active Directory®.
4. Automatically create profile: If Automatically create remote users is enabled and Advanced Configuration AD is disabled, this field makes it possible to assign a profile type to these automatically created users. The profiles by default are: `Chief Operator`, `Group Coordinator`, `Operator (Read)`, `Operator (Write)` and `Pandora Administrator`. The different available profiles may be checked in section Centralised management → User management → Profile management.
5. Automatically create profile group: IfAutomatically create remote users is enabled and Advanced Configuration AD is disabled, this field makes it possible to assign a group to these automatically created users. The different groups available may be checked in section Centralised management → Agent management → Group management.
6. Automatically create profile tags: If Automatically create remote users is activated and Advanced Configuration AD is deactivated, this field makes it possible to assign a profile to a group with the desired tags. The different groups available may be found in the Centralised management → Component management → Tags management section.

Advanced Permissions AD and Add new permissions details:



- Auto enable node access: New users will be able to connect to the nodes.
- Recursive group search: It allows an iterative search by groups.
- Automatically create blacklist: It allows you to type a comma-separated list of users *that will not be created* automatically.
- Active Directory server: Here you may define the path where the Active Directory® server is located.
- Active Directory port: To define the port number of the Active Directory® server (389 by default).
- Start TLS: It defines whether or not to use the Transport Layer Security (TLS) protocol in communications between the client and the server.
- Domain: Define the domain to be used by Active Directory®. Please note the following numbered

indications:

1. At the moment the primary groups of a user are not supported by the advanced group configuration in AD Authentication.
2. If Advanced Configuration AD is used, set the full path in the Domain field (Domain).
3. If the Active Directory® installation is with LDAP, the LDAP path where the server is usually located must be defined here:

```
ldap://addc.mydomain
```

- Enable secondary active directory: It allows you to activate the connection to a secondary Active Directory server. It has the same fields as the primary server and also allows you to configure a search AD search timeout), with a default value of 5 seconds.
- In case there is a password change in users, MS Windows® allows to use by default an old password during 60 minutes in Active Directory®. As it is a MS Windows® configuration, this behaviour is totally external to Pandora FMS®. If you wish to modify it, you may check the documentation by Microsoft.
- Double authentication: Users may choose whether to enable two-step authentication on their accounts.

LDAP

In order to use this mode, it is necessary to have the openLDAP dependencies installed. Depending on the operating system used, following commands are used:

`dnf install openldap*` or `apt install ldap-utils`

- Fallback to local authentication: If this option is enabled, local authentication will be done if LDAP fails. Admin users will always have fallback enabled, to always maintain access to Pandora FMS in case of remote authentication system failure.
- Automatically create remote users: It enables or disables remote user automatic creation. This option allows Pandora FMS to create users automatically once they have logged in using LDAP. If this option is enabled, the following numbered options will be enabled:

1. Save password: If enabled, it allows to save LDAP passwords in local Pandora FMS database.
2. Force automatically create profile user: This option makes it possible to assign a profile type to these automatically created users.

- Login user attribute: It allows you to choose whether users will be identified by their name or by their e-mail address.
- LDAP function: When searching LDAP, you may choose whether to use the native PHP function or use the local ldapsearch command. It is recommended to use the local command for environments that have a large LDAP with many items.

Advanced Config LDAP: If the option is enabled, a list of all saved advanced permissions is displayed. You may add new permissions by selecting the profile, groups and tags, next to the attribute filter. If the user meets any of these attributes (e.g. a particular organisational 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, the corresponding 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.

Double authentication

This feature requires PFMS server and mobile devices to have an accurately synchronised date and time.

It will also be necessary to have the code generator application on a mobile device owned by each user. To find out where and how to download it:

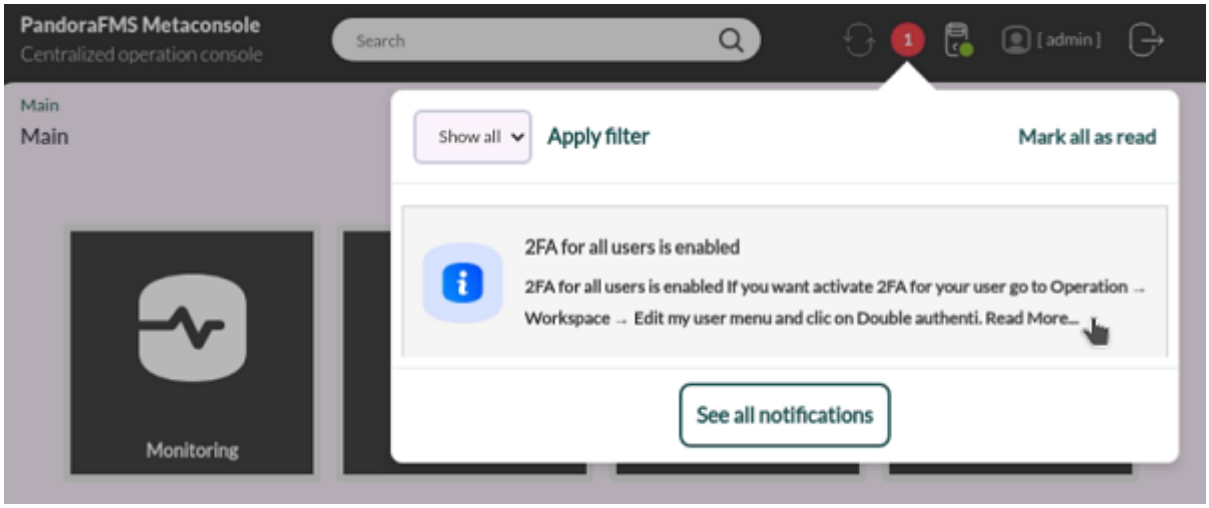
https://support.google.com/accounts/answer/1066447

To use this feature in PFMS an administrator or superadmin user should activate double authentication in the authentication section of Pandora FMS Web Console global configuration.

To do this in the Setup → Metasetup → Authentication menu, click on the Double authentication button to activate it and then click on the Update button to save the change.

Users may choose whether to enable two-step authentication on their accounts by accessing the Edit my user option.

You may use the Command Center notification system to inform all users that 2FA is available and how to activate this personal option. To do this in the Reports → Messages menu, click the Create new message button and type in a message to the `All` group similar to this one:



Force 2FA for all users is enabled

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

To disable this feature for a specific user without using the graphical interface, an administrator may use PFMS CLI.

SAML

For SAML configuration, see this section.

History database

Setup → Metasetup → Historical database menu.

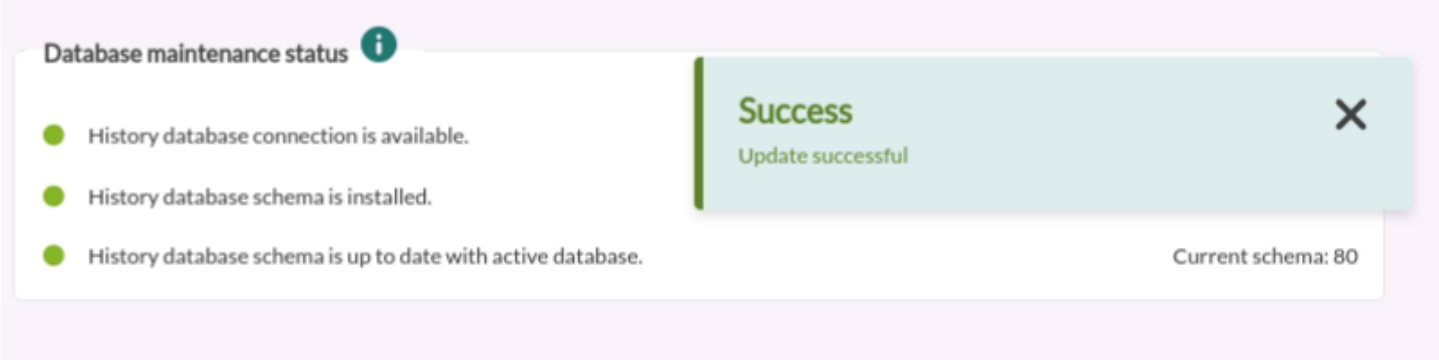
It enables the use of the history database in the Command Center. This feature allows to save data with a configured age in a database different from the main one, in order to speed up the exploitation of the latter.

To access all the options, first activate the Enable history database button. The configuration box (Configure connection target) will appear, which allows you to connect to the future history database.

All options may be configured despite being disconnected from the history database.
Only when a successful connection has been configured, data transfer will start.

Saving the connection configuration and your user credentials in the future history database will

check these values, resulting in a view similar to the following:



Once connection is established, and if necessary, it is possible to configure the customized parameters (Customize settings), which are divided into history general values, general data, events data and SNMP traps data.

Active to historical settings

- Advanced options: It enables the String data days old to keep in active database option, which sets the maximum age of string data to keep in the active database. The string data will be available in the active database at the time and days specified here. Older information will be sent to the history database. The data will be purged from the active database after 7 days (default value).
- Data days old to keep in active database: Value indicating after how many days the data will be transferred to the history database. Default value: 15 days. Note that the data will be deleted from the active database after 45 days.
- Transference block size (Step): Mechanism for transferring data (similar to a data buffer) to the history database. The smaller the number of records, the lower the impact on the performance of the main database. Default value 1500 records. See the next item to configure the time period.
- Delay between transferences (seconds): Waiting time -in seconds- between data transfers between the main database and the history database. Default value: 1.

History data settings

- Maximum history data age (days): Maximum number of days to retain numeric data. Default value: 180.
- Maximum history string data age (days): Maximum number of days to retain string data. Default value: 180.
- Automatic partition of big tables: To automatically create monthly partitions in IDB files of specific databases (`tagente_datos` and `tagente_datos_string`).

History events settings

When Enable history events is activated, the following tokens will be displayed:

- Events days old to keep in active database: Number of days to keep the events in the history database. Default value: 90 days. Note that from the main database, the events are deleted (*purged*) after 7 days.
- Maximum history events age (days): Number of days to finally delete the events from the history database. Default value: 180.

History trap settings

Enabling the Enable history traps option will allow storing SNMP traps in the history database:

- Days old to keep in active database: Number of days of seniority to be kept in the active database. Default value: 6 days. Note that in the main database, traps are deleted after 7 days.
- Maximum history traps age (days): Number of days old to be kept in the history database. Default value: 180 days.

Log Viewer

Setup → Metasetup → Log Viewer menu.

To activate the Log Viewer interface, first enable the Enable log viewer token in Setup → Metasetup → General setup and saving the changes will activate the corresponding tab.

Then the Activate Log Collector button should be enabled in order to have access the connection configuration to OpenSearch. In OpenSearch options and Basic authentication sections, the necessary values should be placed: IP address and port number of the OpenSearch server, if safe connection with HTTPS will be used, the default number of logs to be displayed and the user credentials.

By activating Index configuration, you will have access to the following options:

It is only recommended to change this setting if you have advanced knowledge of OpenSearch. A wrong configuration could destabilize the system.

- Indexing size: The value of this parameter will be used as the `ignore_above` setting in OpenSearch.
- Number of shards: The number of primary shards an index should have. The default value is `1`. This value may only be set at the time of index creation. It cannot be changed in a closed index.
- Auto expand replicas: Automatically expand the number of replicas according to the number of data nodes in the cluster. You may set a lower and upper limit by delimiting with dashes (default `0-1`) or use all for the upper limit (`0-all`). Note that the auto-expanded number of replicas only takes into account the allocation filtering rules and ignores other allocation rules such as total shards per node. This may lead to the cluster's *health* changing to YELLOW (warning notification) if the applicable rules prevent all replicas from being allocated.
- Number of replicas: The number of replicas that each primary fragment has. By default it is `1`.

Setting Number of replicas to `0` may result in a temporary loss of availability during node restarts or a permanent data loss in case of data corruption.

Passwords setup

Setup → Metasetup → Passwords setup menu.

To activate the password policy you should have administrator profile (Pandora administrator) or be superadmin. First the Enable password policy button should be activated to be able to configure the other tokens:

- Min. password size: The password must have a minimum length, by default 4 characters.
- Password expiration: Password expiration, in days. By default `0` days (no expiration).
- Number of failed login attempts: Number of failed attempts before blocking the login. Default value 5 attempts.
- Block user if login fails: If the maximum number of failed attempts is exceeded, the user is blocked for a few minutes (default 5).
- Enable password history and Compare previous password: They work together to prevent users from using repeated passwords. The first token must be enabled and the second token must be greater than zero (default 3), so that a user's new password will be compared to the 3 previously used by the same user (or the number of times indicated).
- The password must include numbers: The password must have numbers, disabled by default.
- The password must include symbols: The password must have 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: It applies the password policy also to administrator users, *enabled by default*.
- Exclusion list for passwords: It allows to add a list of passwords explicitly excluded from use in Pandora FMS.

General setup

Setup → Metasetup → General setup menu.

Basic

Language settings

Language settings: It allows to set up the default language of the Web Console, except for users that choose a specific language individually.

Auto login in node

Auto login in node: Available from version 777, it allows you to go from Command Center (Metaconsole) to each of the centralized nodes' Web Consoles and log in automatically.

Time source

Time source: List where you may choose the source of the date and time to be used. It may be the local system (`System`), which is usually used when the database is in a different system with a different time zone than that of the Web Console, or the database (`Database`).

Enforce https

Enforce https: It allows to force redirection to HTTPS. If it is enabled, you will have to activate the use of Pandora FMS with https in the WEB server.

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

```
UPDATE tconfig  SET `value` = 0 WHERE `token` = 'https';
```

Attachment directory

Attachment directory: Pandora FMS Console directory, used to host collections, incident attachments and other files. You must have writing permissions for the web server and it is located by default at:

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

Remote configuration directory

Remote configuration directory: Path to the directory that stores agent remote configuration, by default located at:

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

Chromium path

Chromium path: Chromium is a special component used to dynamically generate PDF graphics. Enter the PATH where this component is installed. Default value:

```
/usr/bin/chromium-browser
```

Server timezone setup

Server timezone setup: It defines the time zone in which the Web Console is located. Unlike the codes and abbreviations of all countries (ISO 3166 standard), the list of time zones has complicated rules (IANA Time Zone Database) and therefore a first list with continents with their countries is included and selecting an option from it will update the second list where you may choose a specific country or city and then save the changes by clicking on Update. Note: the edit icon  (change timezone) is of no use.

Public URL

Public URL: A public URL may 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.

Force use Public URL

Force use Public URL: It forces the use of public URLs. If this field is active, no matter which system is implemented, links and references will always be built based on `public_url`.

Public URL host exclusions

Public URL host exclusions: Hosts added in this field will ignore the Force use Public URL field.

Customize sections

Customize sections: It allows you to enable and disable sections in the Command Center.

Disable custom live view filters

Disable custom live view filters: If in Customize sections the NetFlow® monitoring view has been enabled, it disables the definition of custom filters (filters that are already created may still be used).

Command line snapshot

Command line snapshot: String modules with multiple lines are shown as command output.

API password

API password: Authentication method to access the Pandora FMS API. It is recommended to use HTTPS to be able to encrypt communication and keep this token secret.

IP list with API access

IP list with API access: List of IP addresses that will have access to Pandora FMS API (by default `127.0.0.1`, only for local access). You may use the asterisk as a wildcard, in such a way that placing * will give access to all IP addresses.

Enable Warp Update

Enable Warp Update: This option allows you to activate the Warp Update for updating the Command Center.

Collection size

Collection size: This is the maximum size, in bytes (default value one million), for Collections.

Max. agents to add in policy concurrently

Max. agents to add in policy concurrently: Maximum number of agents allowed to be added

concurrently to the policy (adding a high number of agents at the same time may cause performance problems). By default `200`.

Warning for synchronization queue

Warning for synchronization queue: If the number of pending items (per node) is greater than this number, a notification will be displayed. Default value: `200`.

Enable Agent API

Enable Agent API: It enables access to the Relations rules.

Enable log viewer

Enable log viewer: This option enables the log viewer tab.

Enable console log

Enable console log: Due to the large amount of debugging data generated by this log, it is recommended to disable it, as it is configured by default.

If enabled, the file `/var/log/php-fpm/error.log` is used for logging Web Console events.

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

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

and *comment* with a semicolon the next parameter:

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

That way the data will be saved in:

```
…/pandora_console/log/console.log
```

Enable audit log

Enable audit log: When activated it also uses the file `…/pandora_console/log/audit.log` to record the audit.

Enable console report

Enable console report: It allows to enable the Web Console in dedicated mode for report generation.

Check connection interval

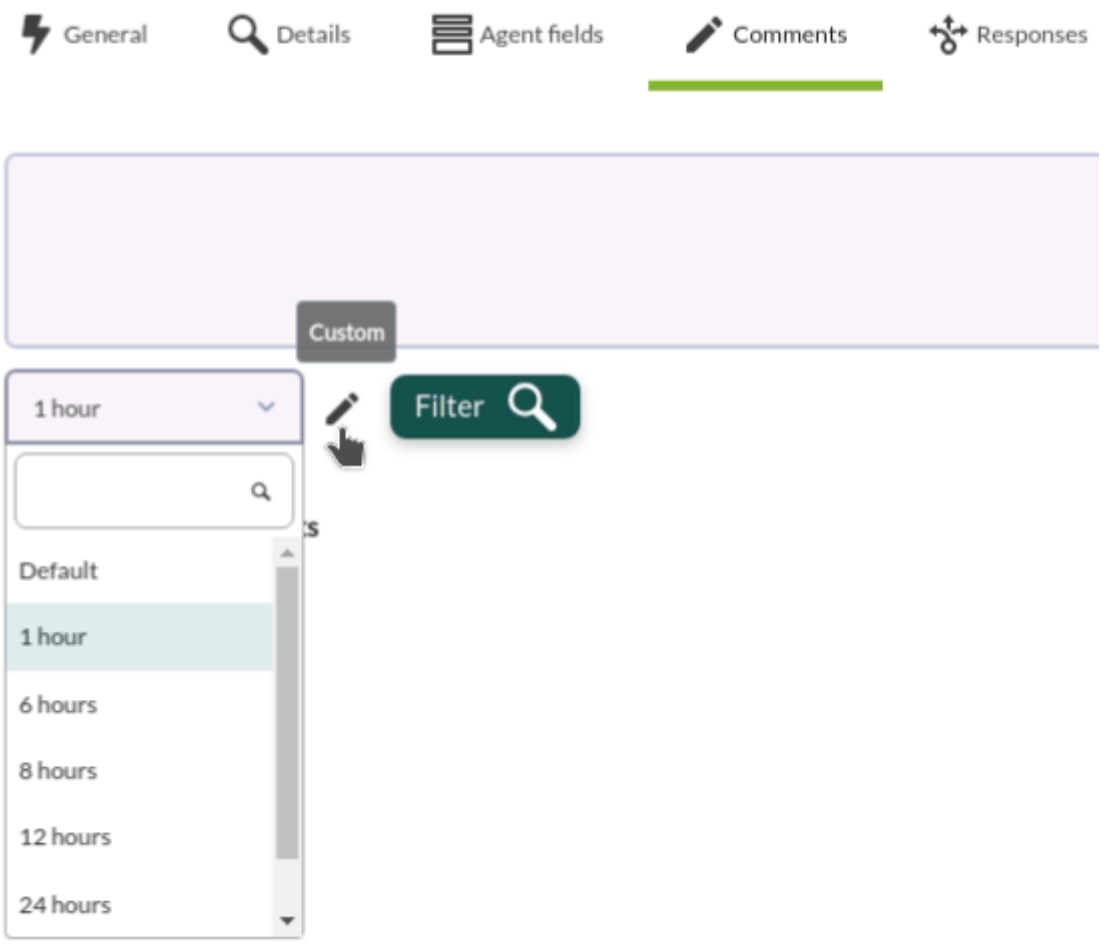
Check connection interval: Time interval (in seconds) to check the connection with the database server. Minimum value `60`, by default `180`.

Keep in process status for new events with extra ID

Keep in process status for new events with extra ID: If any In process with a specific ID Extra is triggered and a new event with the same ID Extra is received, it will be created as In process instead. *New events also inherit the* ID Extra *of the event*.

Max. hours old events comments

Max. hours old events comments: Filter comments in events by elapsed hours. The default value is 8 (integer values). There are other values available for users and only the superadmin will be able to set a custom value, which is independent of the value of this token.



Limit for bulk operations

Limit for bulk operations: Limit of elements that may be modified by massive one-time operations, 500 by default.

Show experimental features

Show experimental features: Advanced features offered for testing prior to final release. Disabled by default.

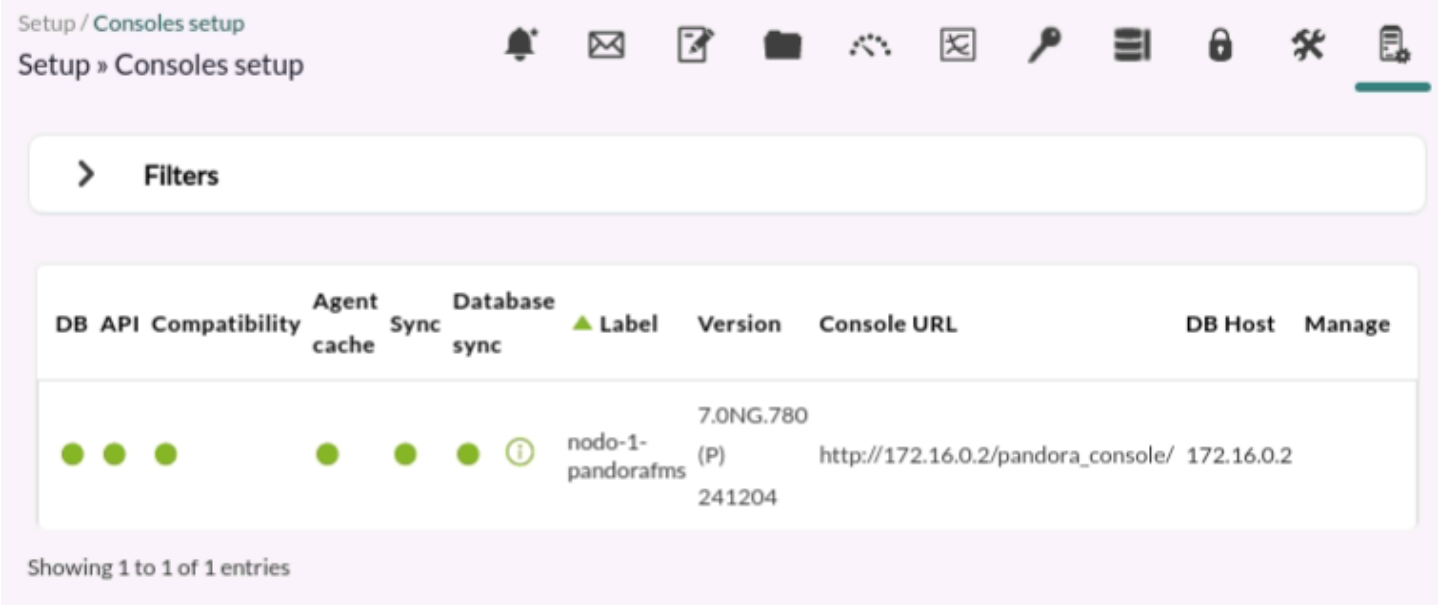
Number of modules in queue

Number of modules in queue: It sets the maximum number of queued modules (by default 500) and if this value is exceeded, a warning icon will be displayed for each item in server administration.

Consoles setup

Setup → Metasetup → Consoles setup menu.

This section includes registering new instances.



The first six columns include buttons that allow you to check each of the instances and their corresponding statuses:

1. BD.
2. API.
3. Compatibility.
4. Agent cache.
5. Sync.
6. Database sync.

The last three columns in Manage allow to:

1. Edit.
2. Deactivate.
3. Delete.

Return to Pandora FMS Documentation Index