Installation and configuration

Installation and configuration

Installation

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

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

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

- Time settings must be the same. The more synchronized the Instance and Command Center clocks are, the more accurate the data displayed will be.

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

Instances

An Instance or node is a typical Pandora FMS installation, composed of a server and a Web Console.

Command Center

A Command Center is an installation of Pandora FMS with a Command Center license.

You cannot use the Pandora FMS console and the Command Center at the same time.

It is necessary to have a server active to be able to carry out different operations related to the Command Center, such as "migration", "self-provisioning", execution of services, etc.

License activation

After activate the license of the Pandora FMS console, whatever the installation method, you must

access the 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. If you activate the node license,
the normal console will appear.

Metallicence

Starting with version 7.0 NG of Pandora FMS, a single license is available for an environment with
Command Center. You can create as many Instances as you want, as long as the total number of
agents within the Command Center is not exceeded.

This license is applied in the Command Center and can be synchronized in as many Instances as
desired, thus allowing centralized management of the different agents that will be deployed in said
Instances.

If nodes are needed that can remain disconnected from the Command Center for long
periods of time, contact the Pandora FMS team.

Metalicense Synchronization

- 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 states must appear normal (in green) and if necessary the synchronization button will be used,
  Synchronize all:

- Once all these steps have been completed for each of the nodes, the Command Center license is accessed and the Validate button is pressed to synchronize the Metalicense with all the Instances.

Instance Registration

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

To register a new Instance we must know a series of parameters regarding the Instance we want to manage. If it is the registration of an Instance that has not yet been registered with a license, the default data is:

- Server name: localhost.localdomain
- API password: empty
- DB host: Database IP
- DB name: pandora
- DB user: pandora
- DB password: pandora
- DB port: 3306
- Control user: admin
- Console password: pandora
- Console URL:

```
http://<dir_IP_orURL>/pandora_console
```

Advanced fields

To guarantee connectivity between node and Command Center, we can manually configure the connection data.

- Metaconsole DB host: IP address of the database

- Metaconsole DB name: `pandora`
- Metaconsole DB user: `pandora`
- Metaconsole DB password: `pandora`
- Metaconsole DB port: `3306`

These fields indicate the configuration of the connection that the node will establish against the Command Center.

If it is a Pandora FMS installation where we have already includedor a valid license in the Instance, we will have to obtain said data from the setup of the Instance and its database.

In the view of the configured Instances we will see that the Instances can be modified, deactivated and deleted. There are some indicators that check certain information about the configuration of each Instance. These checks are performed when loading this view, but they can also be done individually by clicking on them.

The indicators are the following:

- Database: If we have configured the Instance database incorrectly or we do not have the necessary permissions, the indicator will be red and will give us information about the problem.
- API: This flag will test the Instance API. If it fails, it will give us information about the failure.
- Compatibility: This indicator checks some requirements that must exist between Instance and Command Center. The Instance server name, for example, must match the name given in its configuration in the Command Center.
- Event Replication: This indicator shows if the Instance has event replication enabled, and if events have already been received from the Instance how long ago was the last replication.
- Agent Cache: This indicator shows that the latest states of the node's agents and modules have been successfully 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 the Instances.

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

- An Instance can be well configured, but without replicating its events.
- Once you have chosen to replicate the events, all their management will be carried out from the Command Center, leaving the Instance events as merely informative.

If database encryption is enabled, all nodes and the Command Center must use the same `encryption_passphrase` configuration.

Report scheduling

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

The server packages must be installed on the system where the Command Center is installed in
order to launch the Database maintenance script (pandora_db). You must ensure that it is
correctly scheduled to run in cron every hour (as detailed in the following link.).

If you are going to use on-demand reports (sent by email), you need to schedule the cron
extension to run just like you do in a console. Generally, this is done by putting the following line in
the cron, adjusting the corresponding local paths:

```
/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 route will be:

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

Finally, to configure the SMTP for sending emails, you must edit the corresponding parameters in
the email configuration section.

API

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

- User and password: A valid user and password must be known in the Instance.
- API Password: You must know the API access password configured in the Instance.
- List of IPs with access to the API: In the Instance configuration there is a list of IP addresses that can
  access the API. The asterisk can be used as a wildcard to give access to all IP addresses or 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 with an event (if any) will take you
to the view of that agent in the console of the Instance it belongs to.

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

Settings

To configure the Command Center go to Setup → Metasetup.

Warp Update Online

Version NG 763 or later.

By possessing a valid Command Center license and having access to the internet, you will be able to update the Command Center automatically. This section will only be visible if Enable Warp Update is activated in General Settings.

Warp Update Offline

Version NG 763 or later.

- Allows you to update and/or patch the Command Center without having to connect to the internet.
- This section will only be visible if Enable Warp Update is activated in General Configuration.
- Only "upload" the files in order up to the version you need to update, since they are not cumulative versions. See the complete procedure in the main article, Warp Update Offline

Offline patching may render your console unusable, it is recommended that you make a full backup of all files before applying any patches.

Warp Update Journal

Click on the Warp Update Journal icon to see the updates made, version, date and time of application, user who requested and applied it, etc. This section will only be visible if Enable Warp Update is activated in General Settings.

Over time, you will accumulate many records which you can filter by expanding the Filter box and entering the keyword to search for.

Warp Update Options

Version NG 763 or later.

By default it is already configured to be able to update online. This section will only be visible if Enable Warp Update is activated in General Settings.

Please contact support before changing any of the following fields:

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

Notifications

In Pandora FMS there is a system for monitoring the status of the console and the system in general.

- By clicking on the notifications icon (Notifications) you can add or subscribe to each category of notifications those users or groups that will receive the notification.
- For the system status (System status) you can also specify each technical aspect for each of the registered users or groups.

Email

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

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

String Translation

You can make your custom translations (String translation icon) even with macro variables; This extension is fully described in the Translate string section.

File manager

File manager where images of the Command Center installation can be uploaded and deleted from the files in the folder.

The Command Center code reuses some images from the regular 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 Settings

- Max. days before events are deleted: Field where the maximum number of days before events are deleted are defined.
- Use real-time statistics: Enable or disable the use of real-time statistics.
- Max. days before audited events are deleted: Number of days to keep audited events.
- Default hours for event view: Field where the hours field of the default filter in the event view is defined. If the default is 8, the events view will only show events that have occurred in the last 8 hours. This field also affects the display, counting and graphs of the events in the tactical view.
- Migration block size: Size of the migration block. It is used to migrate (move) agents between nodes in Command Center environments, especially to transfer historical data between one node and another.
- Events response max. execution: Number of events that will carry out the desired action at the same time.
- Max. number of events per node: Maximum number of events to be displayed by each node.
- Row limit in CSV log: Row limit for the log in CSV format.
- Max. macro data fields: Field where the number of macros that can be used for alerts is defined.
- Limits of events per query: Limit established 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 purging data is defined. This also specifies the maximum number of days to maintain historical inventory data.

Visual Settings

All configuration related to data representation. Colors and resolution of the graphics, number of elements in the views pagination, etc. There is more information about visual settings in this link.

Authentication

To learn more about authentication, visit the section Authentification.

Historical database

Allows you to activate the use of the historical database in the Command Center (Enable historical database). To learn more about historical database setup visit Console Setup.

Log Viewer

From version 774 of Pandora FMS the access configuration is incorporated to the OpenSearch.

Password Policy

A password policy can be established with limitations on the number of characters in passwords, expiration, temporary blocking of a user. To learn more about the password policy, visit the section Password policy.

General Settings

In this section you will find general Command Center data such as the language, date/time settings or the customization of certain sections, among others.

They can be customized if we want the NetFlow sections, the tree view classified by tags, the visual console or the possibility of creating web checks from the Wizard to be activated or deactivated.

Notable fields:

- Force use Public URL: Force the use of public URLs. If this field is active, regardless of the system that is implemented, links and references will always be built based on `public_url`.
- Public URL host exclusions: Hosts added in this field will ignore the previous field.
- Enable update manager: This option allows you to activate Warp Update to update the Command Center.
- Enable log viewer: This option allows you to activate the log viewer tab to edit the Elasticsearch server configuration.
- Auto login in node: Available since version 777, it allows you to go from Command Center (Metaconsole) to each of the centralized nodes' web consoles and log in automatically.

Return to Pandora FMS Documentation Index