

Chapter 12:

Background

- [Access to newspapers](#)
- [Search and filter logs](#)
- [Understanding logs](#)
- [Export logs](#)

Access to newspapers

This chapter presents the various features related to historical system via logs (logs). Each section is described step by step to facilitate consultation, analysis and operation of recorded events.

Objective : View events recorded by each component of the system.

The screenshot displays the Medulla administration interface. At the top, a dark blue navigation bar contains the Medulla logo and several menu items: Dashboard, kiosk, Utilisateurs, Groupes, Ordinateurs, Imaging, Packages, Audit, Mises à jour, Sauvegarde, Historique (highlighted in green), and Admin. Below the navigation bar, a breadcrumb trail reads 'wva.medulla-tech.io : Page principale > Historique > logs de tous les modules'. On the right, there are links for 'Cliquer pour passer en mode expert' and 'Déconnexion root'. A left sidebar lists various log modules: logs inventory, logs backuppc, logs deployment, logs quickaction, logs download, logs Kiosk, logs packaging, logs remote desktop, and logs imaging. The main content area is titled 'All Logs' and features a search and filter interface with fields for Start Date, End Date, and three criteria dropdowns (all set to 'None' or 'no criteria selected'). A 'Filter logs' button is present. Below this is a pagination bar showing 'Showing 1 to 20 of 1,000 entries' and a search input. A table displays the log entries with columns for date, utilisateur, qui, and texte. The first three entries show messages received from AM at specific times on 2025-05-28.

date	utilisateur	qui	texte
2025-05-28 10:35:52	wva-win-2.dvh@pulse		Received message from AM
2025-05-28 10:34:35	wva-win-1.wwh@pulse		Received message from AM
2025-05-28 10:29:53	wva-win-2.dvh@pulse		Received message from AM

Steps :

1. Open the administration interface.
2. Click on the tab **Logs** in the main menu.
3. A list of modules is displayed, including:
 - logs inventory
 - logs backuppc
 - logs deployment
 - logs quickaction
 - logs download
 - logs kiosk
 - logs packaging
 - logs remote desktop
 - logs imaging
4. Select the module you want to view from the logs.
5. The events appear immediately in the table below the title Journal of + the log chosen.

Search and filter logs

To quickly extract specific events from defined criteria to increase efficiency during analysis.

The screenshot shows the 'Journal de l'Inventaire' interface. At the top, there are fields for 'Start Date' (2025-04-02 00:00:00) and 'End Date' (2025-04-19 00:00:00). Below these are three 'criteria' dropdown menus. The first dropdown is open, showing a list of options: 'Inventory reception', 'Inventory requested', 'Inventory Deployment', 'Inventory Planned', 'Inventory Quick Action', 'Inventory User', 'Inventory Machine', 'Inventory Master', 'Inventory New machine', and 'no criteria selected'. To the right of the criteria dropdowns is a 'Filter logs' button. Below the criteria dropdowns, there is a 'Show' field with a value of '20' and a unit of 'entries'. To the right of the 'Show' field is a 'Search:' input field. Below the 'Show' field, there is a table with columns 'date', 'utilisateur', and 'qui'. The table is currently empty, with the text 'Showing 0 to 0 of 0 entries' above it. At the bottom of the interface, there are three buttons: 'Copy to clipboard', 'Save to csv file', and 'Save to Excel file'.

Steps:

1. Define a search period

- In the fields **Start Date** and **End Date**, indicate the desired time range.
 - Example:
 - Start Date: 2025-04-14 00:00:00
 - End Date: 2025-04-14 23:59:59

2. Select specific criteria (optional)

- Open the drop-down menu **Criteria** to refine your search.
- The options available are:
 - **inventory reception** : events related to the reception of machines
 - **inventory requested** Inventory requested
 - **inventory deployment** : recording during deployments
 - **inventory planned** Planned operations
 - **inventory quick action** : Instant actions on equipment
 - **inventory user** : user activities
 - **inventory machine** : actions associated with a specific machine
 - **inventory master** : interventions carried out by a master account
 - **inventory new machine** : addition of new machines
 - **no criteria selected** : allows to display all events without filtering

3. Apply filters

- Click on the button **Filter logs**.
- The table updates to display only events corresponding to your filters.

4. Search for a free keyword

- In the Show field, you can choose the number of entries that will be displayed.
- In the field **Search** (at the top right of the table), enter a free text string.
 - Example: guacamole, error, registered

5. Adjust Display

- In the section **Show X entries**, select how many lines should be visible per page.
 - Example: 20 for smooth reading.

Example of a combined filter:

To display all new machines recorded between April 13 and 14, 2025:

- Start Date:
- End Date:
- Criteria:
- Click **Filter logs**

Understanding logs

In order to interpret the information contained in each line of the newspaper.

Each table entry contains the following columns: :

- **Date** : Date and time of event
- **User** : Equity-generated account
- **Who** : Machine or service concerned
- **Text** Description of the action

Example of reading :

```
Date : 2025-04-15 08:38:29
Utilisateur : master@pulse
Qui : rspulse@pulse/mainrelay
Texte : Machine registered
```

Council Consolidate similar logs to identify trends or sequence of operations (e.g. successive recordings, multiple deployments, etc.).

Export logs

To save logs for external analysis, archiving or sharing.



Steps :

1. Apply your filters (by date, user, etc.) to isolate the desired logs.
2. Click on the button **Export** (or **Export logs** depending on the interface).
3. Choose the output format:
 - **CSV** : for processing in Excel or Google Sheets
 - **PDF** : for quick archiving or transmission
4. The file is generated and downloaded automatically.
5. Save it or transfer it according to your needs (report, audit, support...).

The historical system is a key tool for:

- Ensuring traceability of actions
- Quickly identify anomalies
- Understanding the behaviour of machines or users
- Facilitate diagnosis and intervention
- Ensuring system compliance and transparency

Regular and rigorous use of logs will ensure the long-term security and reliability of your infrastructure.