

Chapitre 12 :

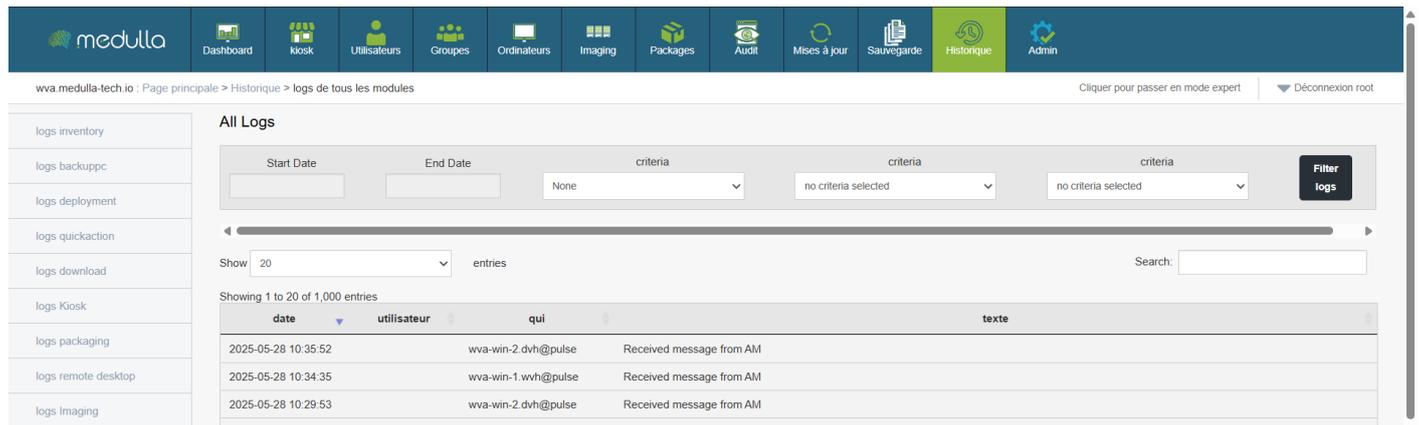
Historique

- [Accéder aux journeaux](#)
- [Rechercher et filtrer les logs](#)
- [Comprendre les logs](#)
- [Exporter les logs](#)

Accéder aux journeaux

Ce chapitre présente les différentes fonctionnalités liées à l'historique système via les journeaux (logs). Chaque section est décrite étape par étape pour faciliter la consultation, l'analyse et l'exploitation des événements enregistrés.

Objectif : Visualiser les événements enregistrés par chaque composant du système.



The screenshot shows the Medulla administration interface. At the top, there is a navigation bar with icons for various modules: Dashboard, Kiosk, Utilisateurs, Groupes, Ordinateurs, Imaging, Packages, Audit, Mises à jour, Sauvegarde, Historique (highlighted), and Admin. Below the navigation bar, the breadcrumb trail reads "wva.medulla-tech.io > Page principale > Historique > logs de tous les modules". The main content area is titled "All Logs" and features a search and filter interface. It includes fields for "Start Date", "End Date", and three "criteria" dropdown menus. A "Filter logs" button is located to the right of these fields. Below the filter interface, there is a "Show" dropdown set to "20" and a search input field. The table below shows log entries with columns for "date", "utilisateur", and "texte". The visible entries are:

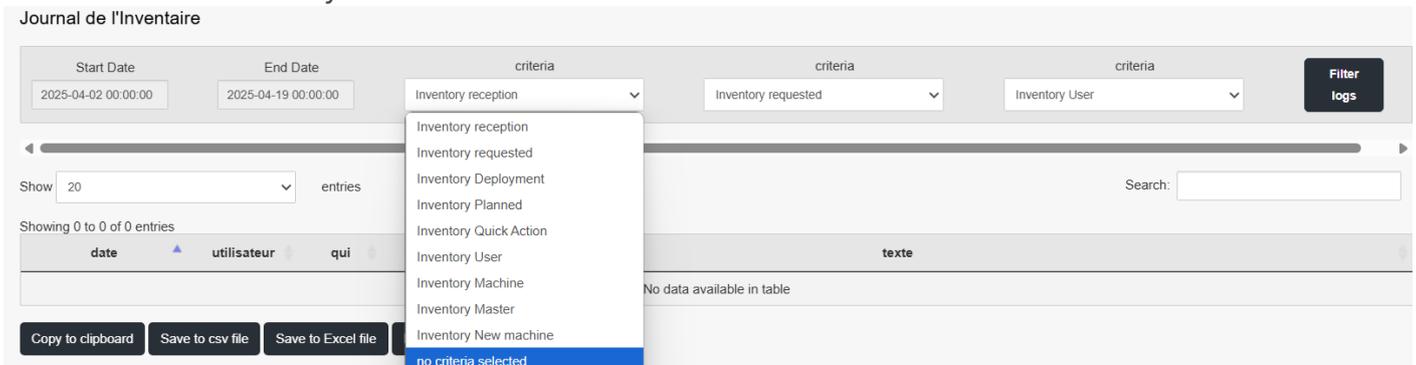
date	utilisateur	texte
2025-05-28 10:35:52	wva-win-2.dvh@pulse	Received message from AM
2025-05-28 10:34:35	wva-win-1.wvh@pulse	Received message from AM
2025-05-28 10:29:53	wva-win-2.dvh@pulse	Received message from AM

Étapes :

1. Ouvrez l'interface d'administration.
2. Cliquez sur l'onglet **Logs** dans le menu principal.
3. Une liste de modules s'affiche, comprenant :
 - logs inventory
 - logs backuppc
 - logs deployment
 - logs quickaction
 - logs download
 - logs kiosk
 - logs packaging
 - logs remote desktop
 - logs imaging
4. Sélectionnez le module dont vous souhaitez consulter les logs.
5. Les événements apparaissent immédiatement dans le tableau situé en dessous du titre Journal de + le log choisi.

Rechercher et filtrer les logs

Pour extraire rapidement des événements précis à partir de critères définis pour gagner en efficacité lors de l'analyse.



Étapes :

1. Définir une période de recherche

- Dans les champs **Start Date** et **End Date**, indiquez la plage temporelle souhaitée.
 - Exemple :
 - Start Date : `2025-04-14 00:00:00`
 - End Date : `2025-04-14 23:59:59`

2. Sélectionner des critères spécifiques (optionnels)

- Ouvrez le menu déroulant **Criteria** pour affiner votre recherche.
- Les options disponibles sont les suivantes :
 - `inventory reception` : événements liés à la réception de machines
 - `inventory requested` : inventaire demandé
 - `inventory deployment` : enregistrement pendant les déploiements
 - `inventory planned` : opérations planifiées
 - `inventory quick action` : actions instantanées sur les équipements
 - `inventory user` : activités des utilisateurs
 - `inventory machine` : actions associées à une machine spécifique
 - `inventory master` : interventions réalisées par un compte maître
 - `inventory new machine` : ajout de nouvelles machines
 - `no criteria selected` : permet d'afficher tous les événements sans filtrage

3. Appliquer les filtres

- Cliquez sur le bouton **Filter logs**.
- Le tableau s'actualise pour afficher uniquement les événements correspondant à vos filtres.

4. Rechercher un mot-clé libre

- Dans le champ **Show**, on peut choisir le nombre d'entrées qui seront affichées.
- Dans le champ **Search** (en haut à droite du tableau), entrez une chaîne de texte libre.
 - Exemple : `guacamole`, `error`, `registered`

5. Ajuster l'affichage

- Dans la section **Show X entries**, sélectionnez combien de lignes doivent être visibles par page.
 - Exemple : pour une lecture fluide.

Exemple de filtre combiné :

Pour afficher toutes les nouvelles machines enregistrées entre le 13 et le 14 avril 2025 :

- Start Date :
- End Date :
- Criteria :
- Cliquez sur **Filter logs**

Comprendre les logs

Afin d'interpréter les informations contenues dans chaque ligne du journal.

Chaque entrée du tableau contient les colonnes suivantes :

- **Date** : Date et heure de l'événement
- **Utilisateur** : Compte ayant généré l'action
- **Qui** : Machine ou service concerné
- **Texte** : Description de l'action effectuée

Exemple de lecture :

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

Conseil : Regroupez les logs similaires pour identifier des tendances ou séquences d'opérations (ex. : enregistrements successifs, déploiements multiples, etc.).

Exporter les logs

Pour sauvegarder les logs pour analyse externe, archivage ou partage.

Copy to clipboard

Save to csv file

Save to Excel file

Print logs

Étapes :

1. Appliquez vos filtres (par date, utilisateur, etc.) pour isoler les logs souhaités.
2. Cliquez sur le bouton **Exporter** (ou **Export logs** selon l'interface).
3. Choisissez le format de sortie :
 - **CSV** : pour un traitement dans Excel ou Google Sheets
 - **PDF** : pour un archivage ou une transmission rapide
4. Le fichier est généré et téléchargé automatiquement.
5. Sauvegardez-le ou transférez-le selon vos besoins (rapport, audit, support...).

L'historique système est un outil clé pour :

- Garantir la traçabilité des actions
- Identifier rapidement des anomalies
- Comprendre le comportement des machines ou utilisateurs
- Faciliter les diagnostics et interventions
- Assurer la conformité et la transparence du système

Une utilisation régulière et rigoureuse des logs permet de renforcer durablement la sécurité et la fiabilité de votre infrastructure.