

Chapitre 10 : Mises à Jour

- [Conformité des entités](#)
- [Gérer les listes de mises à jour](#)
- [Suivi de la conformité](#)

Conformité des entités

La gestion des mises à jour est un levier essentiel pour garantir la sécurité, la stabilité et l'homogénéité de votre environnement informatique. Grâce aux outils proposés par la plateforme, vous pouvez identifier précisément les entités à mettre à jour, suivre la conformité globale, et intervenir de manière ciblée, progressive et optimisée.

La section **Conformité des entités** offre une synthèse claire de l'état de mise à jour de chaque ensemble de machines. Elle vous permet d'identifier immédiatement les entités à risque ou nécessitant une action.

Conformité des entités

☒ Medulla ☐ Glpi

medulla

Dashboard

kiosk

Utilisateurs

Groupes

Ordinateurs

Imaging

Packages

Audit

Mises à jour

Sauvegarde

Historique

Admin

wva.medulla-tech.io : Page principale > Mises à jour > Conformité des entités

Cliquer pour passer en mode expert

▼ Déconnexion root

Conformité des entités

OS Upgrades




Gérer les listes de mises à jour

Conformité des entités

☒ Medulla ☐ Glpi

Rechercher

Elements 1 à 1 - Total 1

Nom de l'entité	Taux de conformité	Mises à jour manquantes	Machines non conformes	Total ordinateurs	Actions
Siveo Medulla	100%	0	0	2	  

Accès :

Menu latéral → **Conformité des entités**

Tableau présenté :

- **Nom de l'entité** : Ex. *Siveo Medulla*, *Siveo Medulla > Private*
- **Taux de conformité** : pourcentage de machines à jour
- **Mises à jour manquantes** : nombre total de correctifs non installés
- **Machines non conformes** : nombre de postes hors standard
- **Total ordinateurs** : nombre de machines dans l'entité

Exemple :

Actions disponibles :

- **Voir détails** : accéder à la liste complète des mises à jour manquantes, avec les postes concernés et l'historique des tentatives de déploiement
- **Rechercher / filtrer** : par nom d'entité, conformité ou volume de mises à jour manquantes

Cette vue est idéale pour planifier des campagnes de mises à jour, préparer des audits ou mesurer l'efficacité de votre politique de sécurité.

Gérer les listes de mises à jour

L'interface vous permet de gérer précisément les listes de mises à jour applicables à chaque entité ou machine.

Gérer les listes de mises à jour

Liste grise (mises à jour manuelles)
Elements 0 à 0 - Total 0

Nom de la mise à jour	Id de la mise à jour	Sévérité	Actions
-----------------------	----------------------	----------	---------

Liste blanche (mises à jour automatiques)
Elements 0 à 0 - Total 0

Nom de la mise à jour	Id de la mise à jour	Sévérité	Actions
-----------------------	----------------------	----------	---------

Liste noire (mises à jour bannies)
Elements 0 à 0 - Total 0

Nom de la mise à jour	Id de la mise à jour	Sévérité	Actions
-----------------------	----------------------	----------	---------

Fonctionnalités disponibles :

- **Consulter les mises à jour manquantes**
- **Appliquer des filtres** (par type de correctif, gravité, date de publication)
- **Déployer ou exclure certaines mises à jour**
- **Planifier les installations à un horaire défini**

Grâce à ce niveau de personnalisation, vous gardez la main sur le contenu exact des déploiements, évitez les interruptions inopportunes, et priorisez les mises à jour critiques.

Suivi de la conformité

La conformité des mises à jour est un indicateur de santé de votre parc. Plus elle est élevée, plus vos systèmes sont protégés et alignés.

Bonnes pratiques :

- Vérifiez régulièrement les entités avec un taux de conformité inférieur à 100%
- Analysez les causes des machines non conformes (erreur de déploiement, redémarrage manquant, conflits logiciels...)
- Lancez un nouveau déploiement ciblé à partir de l'entité concernée

Gérer les mises à jour ne consiste pas simplement à corriger. C'est une démarche proactive, continue et stratégique. Avec les outils de conformité proposés par la plateforme, vous pouvez :

- Visualiser rapidement les entités à risque
- Déployer intelligemment les correctifs nécessaires
- Réduire l'impact sur le réseau et les utilisateurs
- Maintenir un haut niveau de sécurité à l'échelle de votre infrastructure