

# Chapter 10: Updates

- [Compliance of entities](#)
- [Manage Update Lists](#)
- [Compliance monitoring](#)

# Compliance of entities

The management of updates is an essential lever to ensure the security, stability and homogeneity of your IT environment. With the tools offered by the platform, you can precisely identify the entities to be updated, monitor overall compliance, and intervene in a targeted, progressive and optimized way.

Section **Compliance of entities** offers a clear synthesis of the update status of each set of machines. It allows you to immediately identify entities at risk or requiring action.

[entityconformitychoice.png](#)

[image.png](#)

Access:

Side menu → **Compliance of entities**

Table presented:

- **Name of entity** : Ex. *Siveo Medulla, Siveo Medulla > Private*
- **Compliance rate** : percentage of machines up to date
- **Missing updates** : total number of patches not installed
- **Machinery not conforming** : Number of non-standard posts
- **Total computers** : number of machines in the entity

Example:

Available actions:

- **See details** : access the complete list of missing updates, with the posts concerned and the history of attempts to deploy
- **Search / Filter** : by entity name, compliance or volume of missing updates

This view is ideal for planning updates campaigns, preparing audits or measuring the effectiveness of your security policy.

# Manage Update Lists

The interface allows you to precisely manage the updated lists applicable to each entity or machine.

[listmajgestion.png](#)

Features available:

- **View missing updates**
- **Apply filters** (by type of patch, severity, date of publication)
- **Deploy or exclude certain updates**
- **Plan installations at a specified time**

With this level of customization, you keep your hands on the exact content of deployments, avoid inappropriate interruptions, and prioritize critical updates.

# Compliance monitoring

Compliance with updates is a health indicator of your park. The higher it is, the more protected and aligned your systems are.

## **Good practices:**

- Regularly check entities with a compliance rate below 100%
- Analyze the causes of non-compliant machines (deployment error, missing restart, software conflicts...)
- Launch a new targeted deployment from the entity concerned

Managing updates is not simply about correcting. It is a proactive, continuous and strategic approach. With the compliance tools offered by the platform, you can:

- Quickly view entities at risk
- Smartly deploy the necessary patches
- Reducing the impact on the network and users
- Maintain a high level of security across your infrastructure