User manual for S3SRV embedded web portal

2025

This document contains instructions and information to use the MyHogo customer portal.

Versions

Version	Date	Description
V1	20/05/2019	Initial version.
V2	10/02/2020	Modification of the document according to MyHogo's evolution
V3	10/05/2023	Modification of the document according to MyHogo's evolution
V4	03/05/2025	Modification of the document according to the last S3SRV's web interface
V5	20/10/2025	Adding the API JSON specification

References

#	Reference	Title/Name
#1	HR-MD-19-001	S3 product range user manual

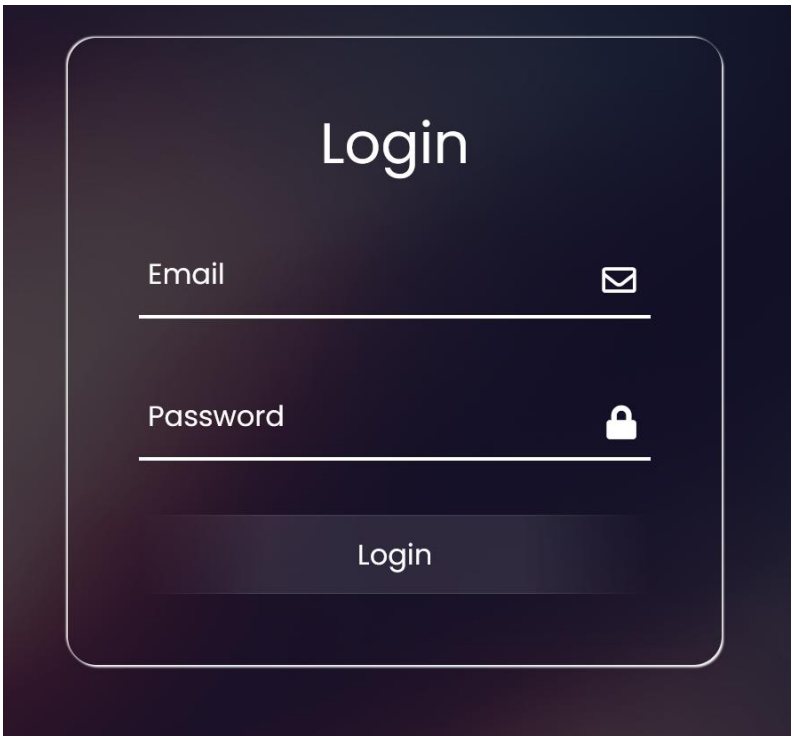
Table of content

1 Access to S3SRV's Web portal 4
2 User's welcome page and dashboard 5
3 User profile management 6
3.1 Display and modify your profile 6
3.2 Edit profile 6
3.3 Recover password 6
4 Management of devices 7
4.1 List of devices 7
5 Statistics 8
5.1 Main statistics panel 8
5.2 Scan logs 8
5.2.1 List of scan logs 8
5.2.2 Visualisation of a newspaper of scan 8
6 Security Groups and Security Policies 9
6.1 Security groups 9
6.1.1 Security Groups Manager 9
6.1.2 Create a Security Group 10
6.1.3 Edit a Security Group 11
6.2 Security Policies 12
6.2.1 Visualize security policies 12
6.2.2 Edit security policies 14
7 Manager users 15
7.1 Role and dashboard 15
7.2 Groups and user management 16
7.2.1 Group management 16
7.2.2 User management 17
7.3 Devices management 18
7.4 Licences management 19
7.5 Access to server's logs 20
7.6 S3SRV's JSON API 21
7.6.1 Access and settings 21
7.6.2 Server status API 22
7.6.3 Scan data API 24

1 Access to S3SRV's Web portal

Access to the S3SRV's web portal over https, using its hostname or IP address and your favourite web browser.

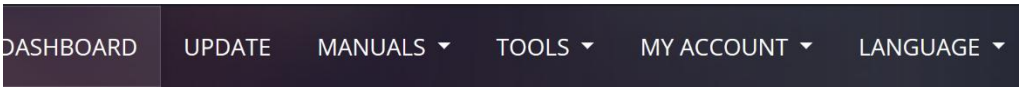
The first displayed screen allows you to connect to your account:



Type in your login and password to connect to your interface.

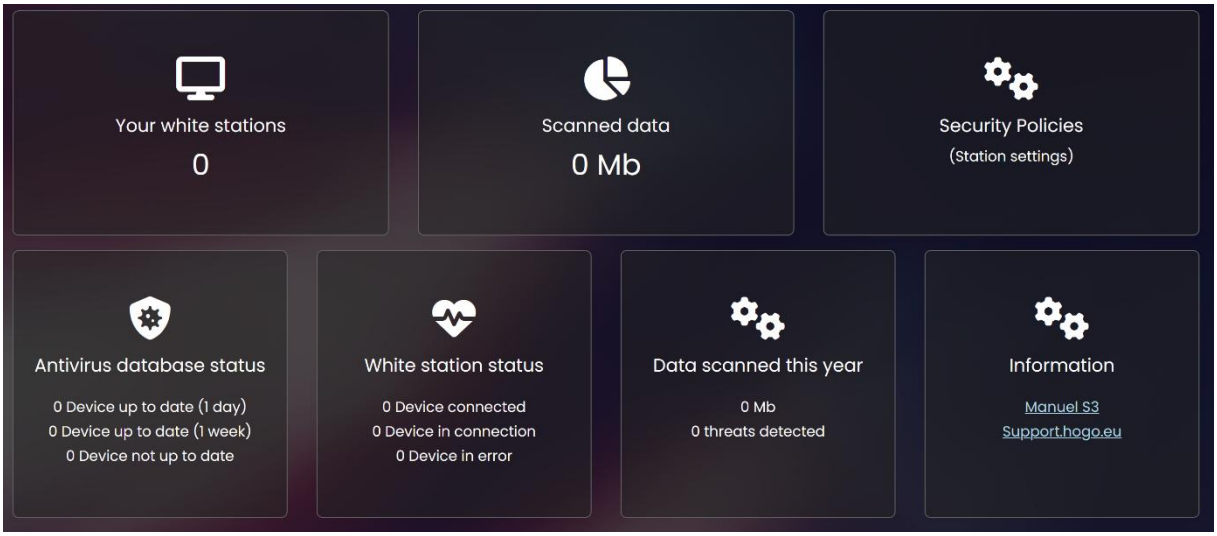
2 User's welcome page and dashboard

The welcome page of the S3SRV shortly presents the functions available on the portal, and displays the menu allowing to navigate through the site[1]:



The main page of the portal is the "dashboard", which summarize on one single page the main information and main links of the site (from left to right, top to bottom):

1. Number of Hogo devices associated to your account
2. Access to the scan statistics
3. Links to update your devices
4. Access to documentation
5. Access to the Security Manager (to manage security groups and policies)

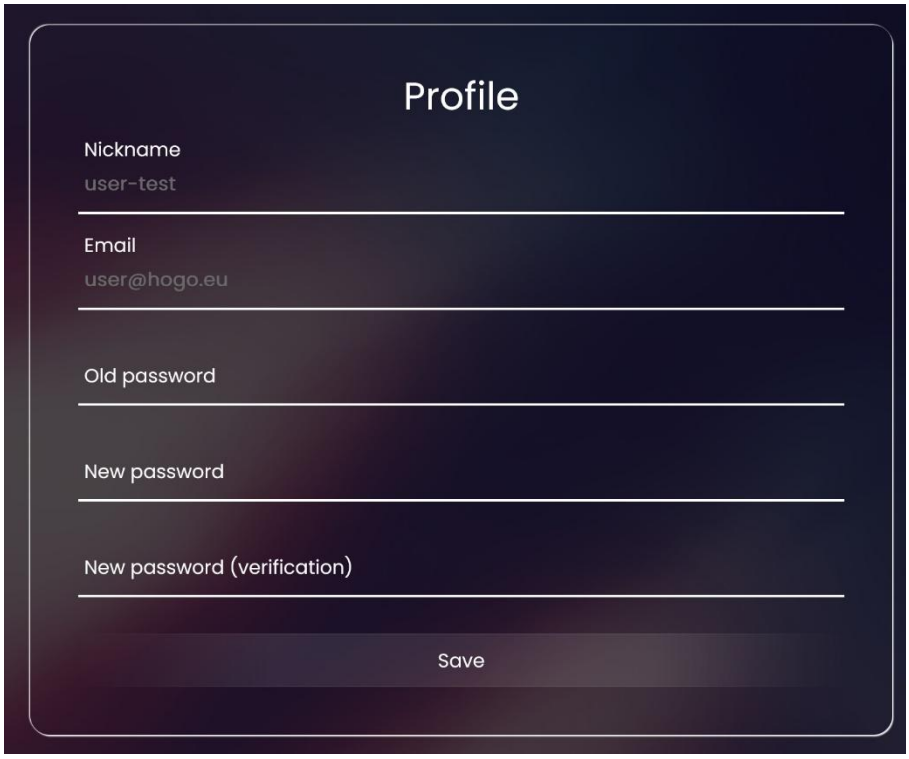


[1] This section is about regular users, not "manager" users. For these specific users, please refer to the chapter 7 of this manual.

3 User profile management

3.1 Display and modify your profile

Your user profile can be displayed with the link "My Account / Profile" in the upper menu:



3.2 Edit profile

Changing your profile can be done by changing the contents of the fields on the profile page.

Note: by default, the password is not affected (it is not displayed and not changed), you have to enter the password to be integrated, twice, to modify it.

3.3 Recover password

For security, the automatic password recovery feature has been disabled on MyHogo.

To recover your password, contact technical support directly at: https://support.hogo.eu

4 Management of devices

4.1 List of devices

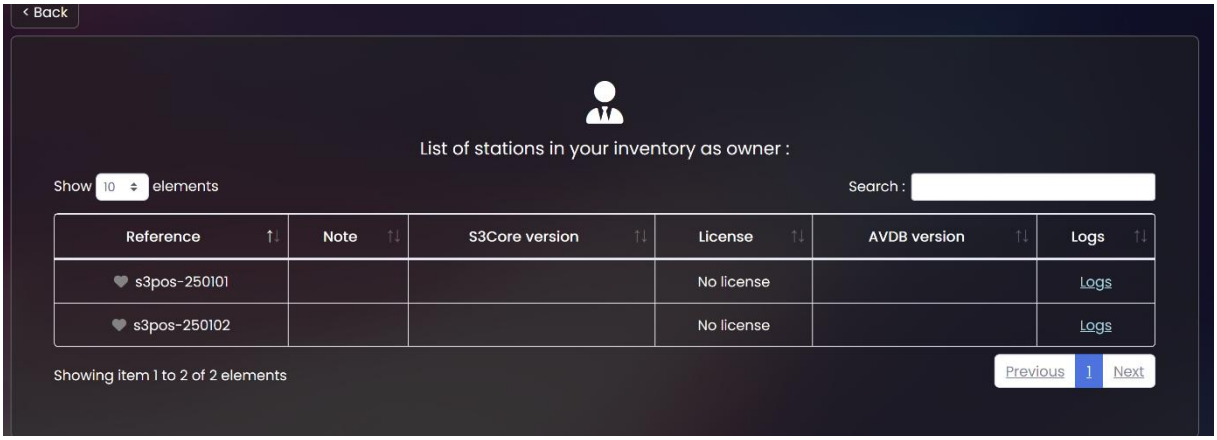
The list of devices is accessible by the first cell of the dashboard. It shows two separate lists:

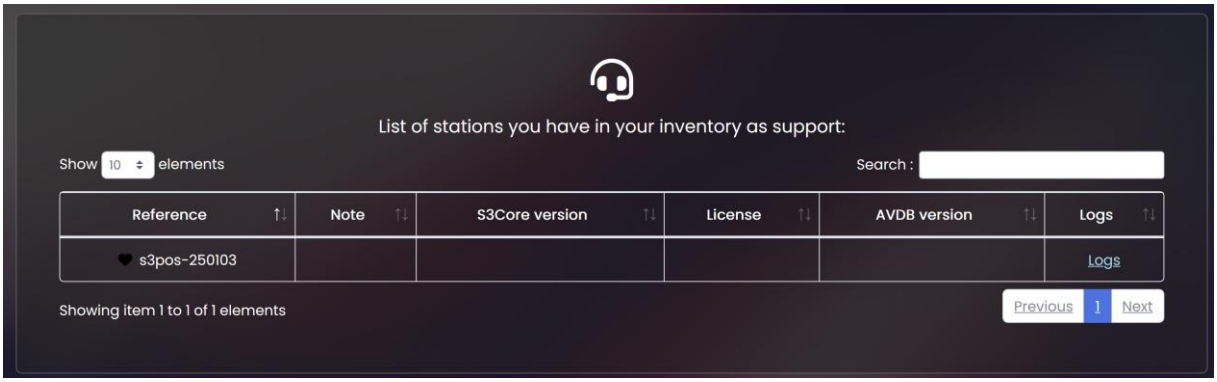
- The list of devices of which to you are the owner
- The list of devices for which you are declared as the support contact

Devices are grouped by "pages" of 10 (number can be changed). For each device, the following elements are shown:

- Reference of the device and a custom note
- Software version (if your device synchronises with MyHogo, the last installed version is displayed)
- The associated License file (licenses are supplied by Hogo)
- Version of antiviral definitions (if your equipment synchronises with MyHogo, the last installed version is available)

Furthermore, it is possible to search devices having specific names with a research bar..



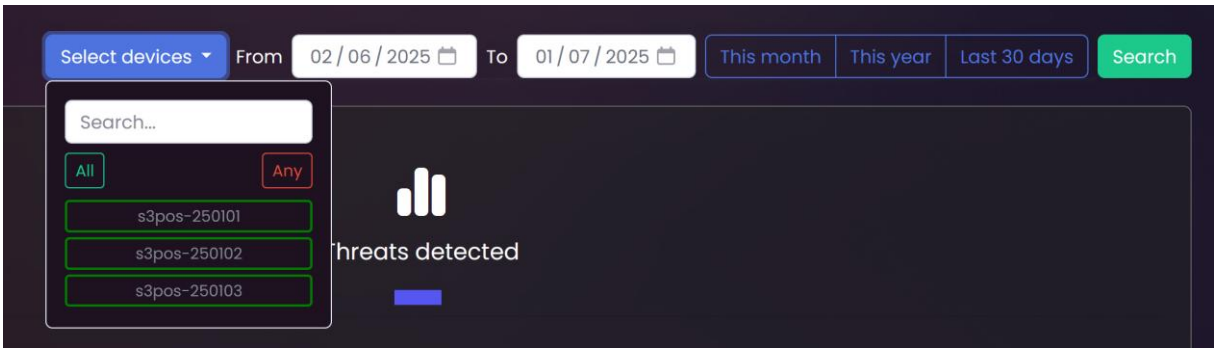


5 Statistics

5.1 Main statistics panel

The statistic panel is accessible with the 2nd cell of the dashboard. It displays statistics on data scanned by all your equipment, and includes the following elements:

- List of devices: allows to show total statistics or for selected devices only
- Data scanned: This graph represents the quantity of data scanned by your devices over given period
- Threats detected: This graph represents the number of threats (virus, malware) detected by your devices over given period
- Dates: these buttons allow to change the period to be displayed



5.2 Scan logs

5.2.1 List of scan logs

The list of scan logs for a device is accessible from the list of your devices. This list of logs is presented as a table containing dates, title and links towards the logs of the device. Each log can be consulted or deleted.

To simplify navigation, it is possible to filter the logging period to be shown with a form displayed above the table:



5.2.2 Visualisation of a newspaper of scan

By clicking on a specific scan log, its content is shown (opened directly in the web browser as a HTML file).

6 Security Groups and Security Policies

6.1 Security groups

6.1.1 Security Groups Manager

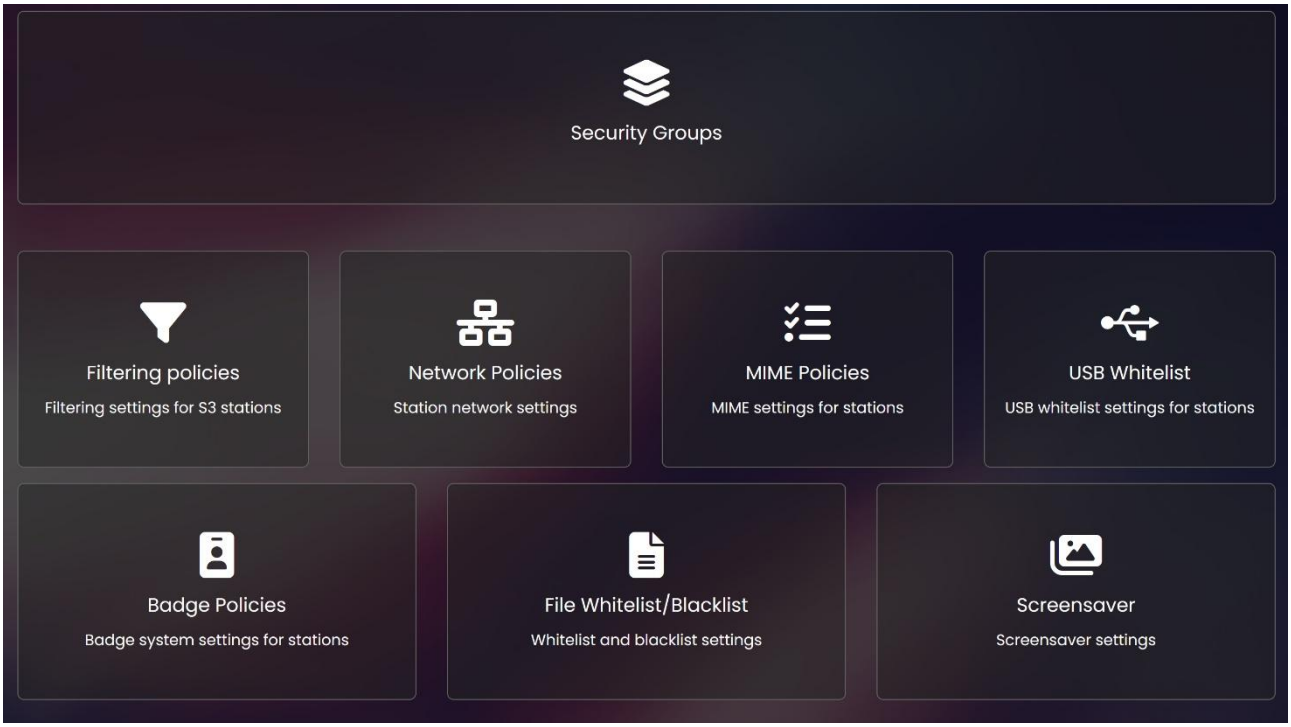
The Security Groups Manager is accessible with the 3rd cell of the dashboard. This manager allows you to create and administrate security groups for your Hogo devices.

Each security group has the following properties:

- Filtering policy: a set of parameters to tune your devices way of scanning data
- Network policy: a set of parameters to tune how your devices connects to a network and its network services
- MIME policy: a set of parameters to tune how your devices filters file with their MIME types (if license allows it)
- USB Whitelist: list of USB devices recognized by the station for the "USB media filtering" function (if license allows it)
- Badge policy: settings of the embedded PCSC car reader (if license allows it)
- File blacklist / whitelist policy: allows to save sha256 checksum to whitelist or blacklist files for Smart-Transfers
- Screensaver policy: a set of parameters for changing the screensaver's behaviour (time, image or video...)

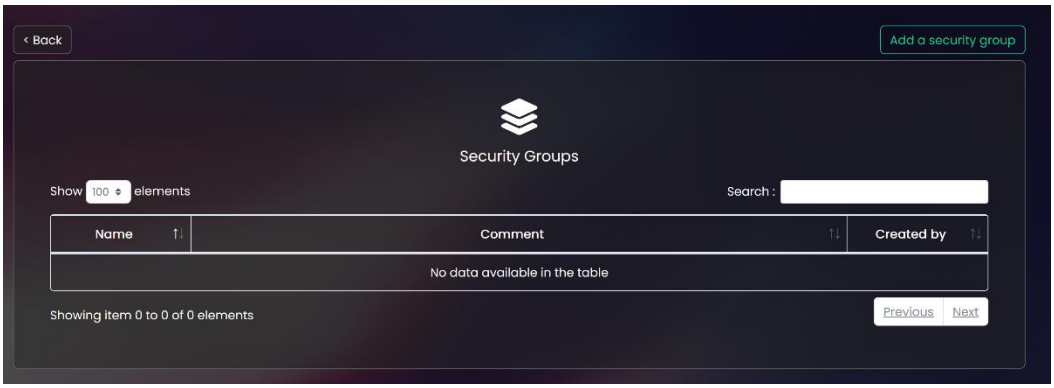
With this manager, you can declare security groups, and then set the associated policies : You can also declare which device is attributed to each security group.

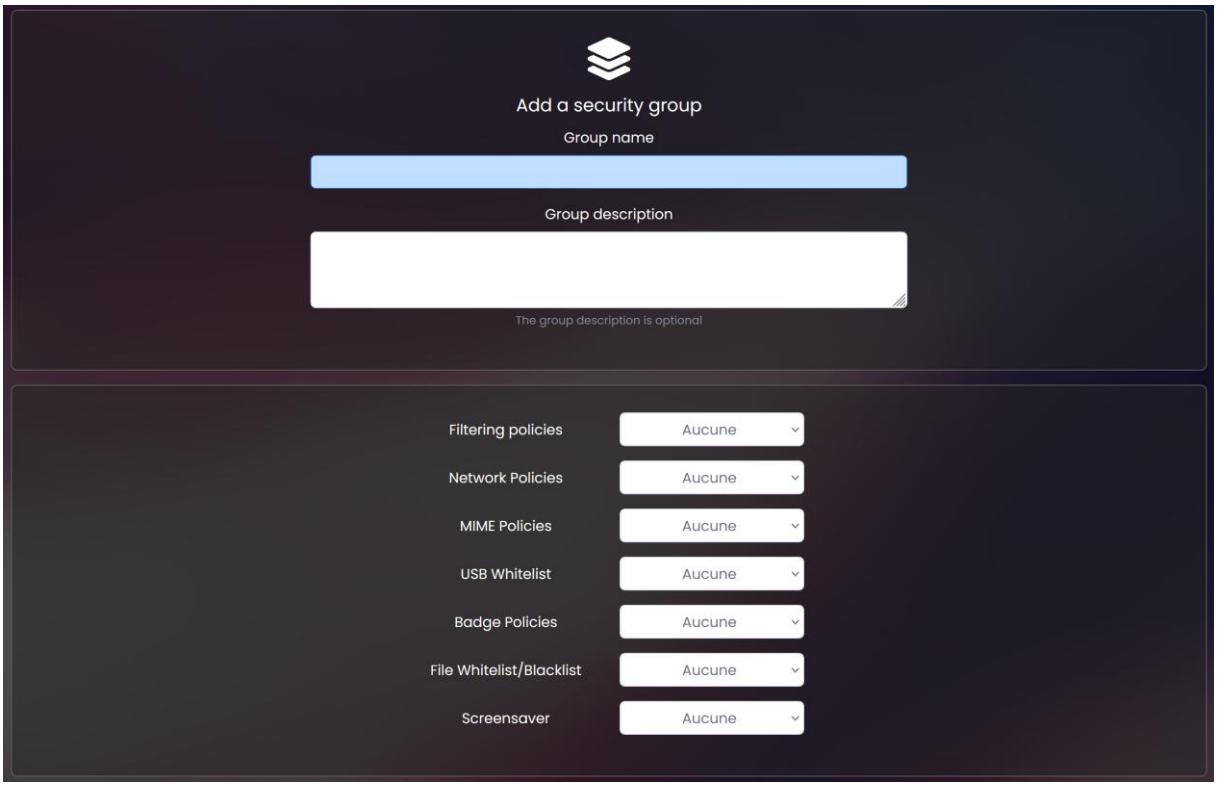
This attribution is then used by the device, when synchronizing with the S3SRV, to retrieve its filtering and network policies. To be noted: a device can only be associated to one security group.



6.1.2 Create a Security Group

You can create a Security Group with the link "Security Groups / Add a security group" in the Security Group Manager. A form will be displayed to enter the name of the group:





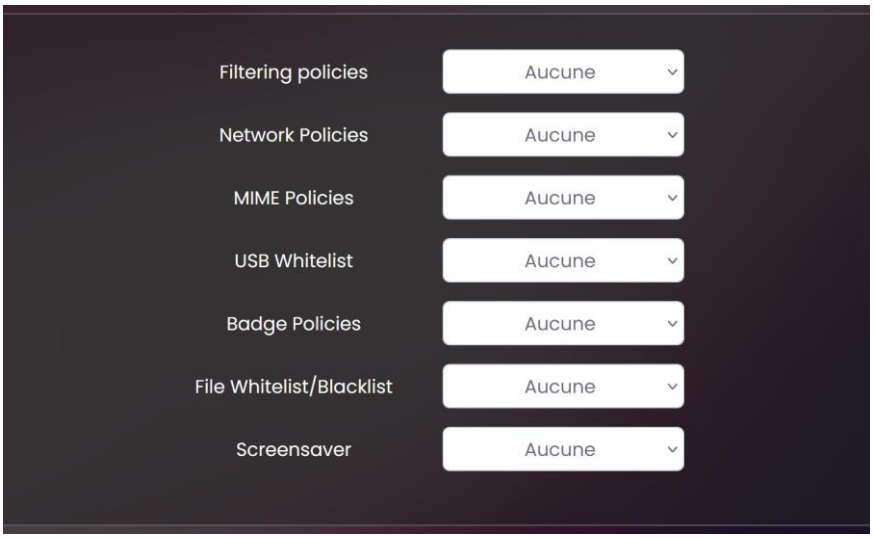
6.1.3 Edit a Security Group

To edit a group, click on its name in group list from the Security Group Manager. A page specific for this group will appear.

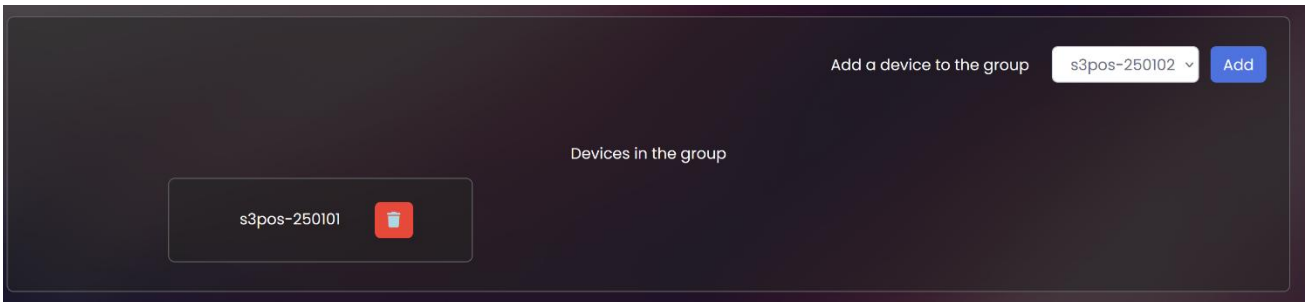
This page displays the policies associated with the group and allows to modify it. It also displays the list of devices in and out of this group and allows to add or remove devices.

Finally, it allows you to delete the security group.

To modify a security policy, use the list of options displayed and click on "Ok":



To add a device to the group, click on the "add" button in the devices list. To remove on, click on the "remove" button:



6.2 Security Policies

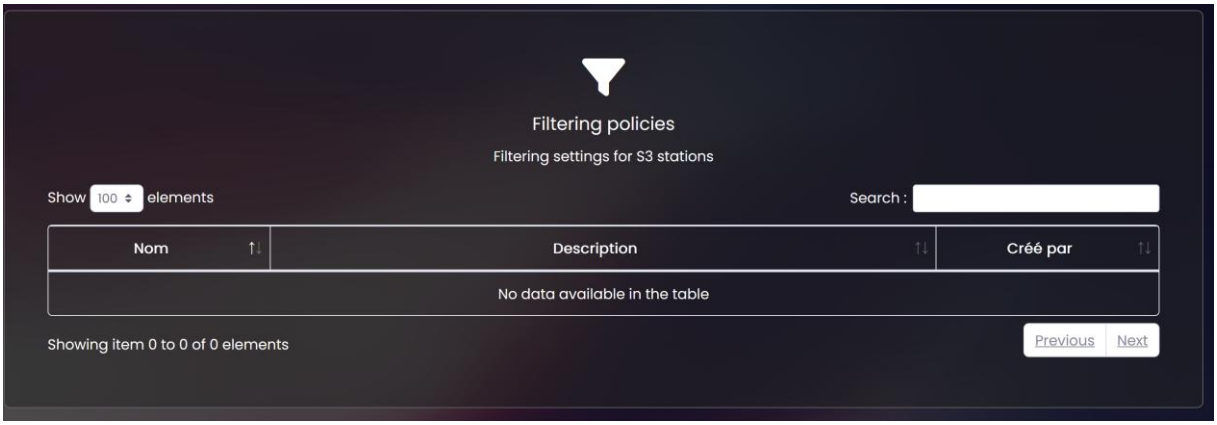
There are 7 types of security policies that can be created/modified/deleted and associated to Security Groups.

6.2.1 Visualize security policies

Each type of security policy can be accessed with the menu of the Security Group Manager.

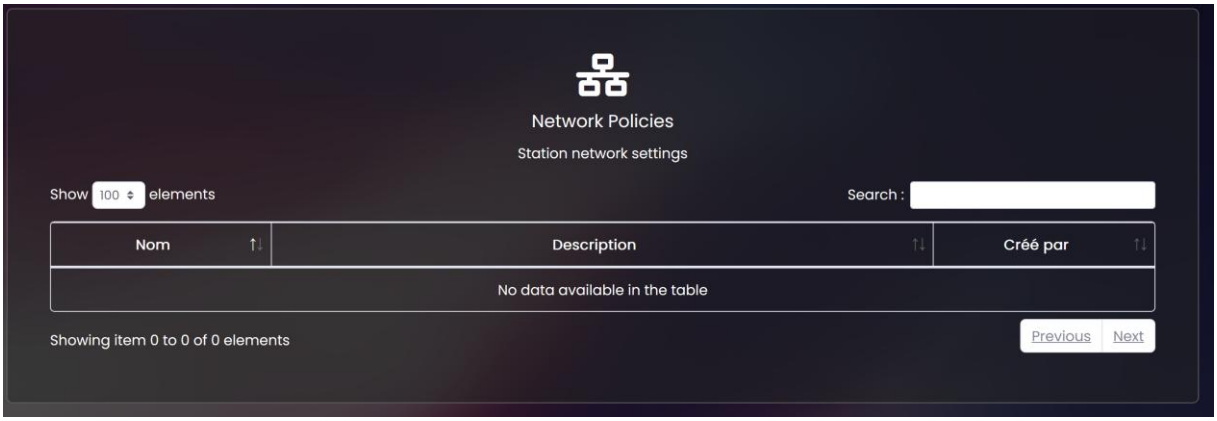
6.2.1.1 Scan filtering policies

The list of scan filtering policies can be accessed with the link labelled "Filtering policies":



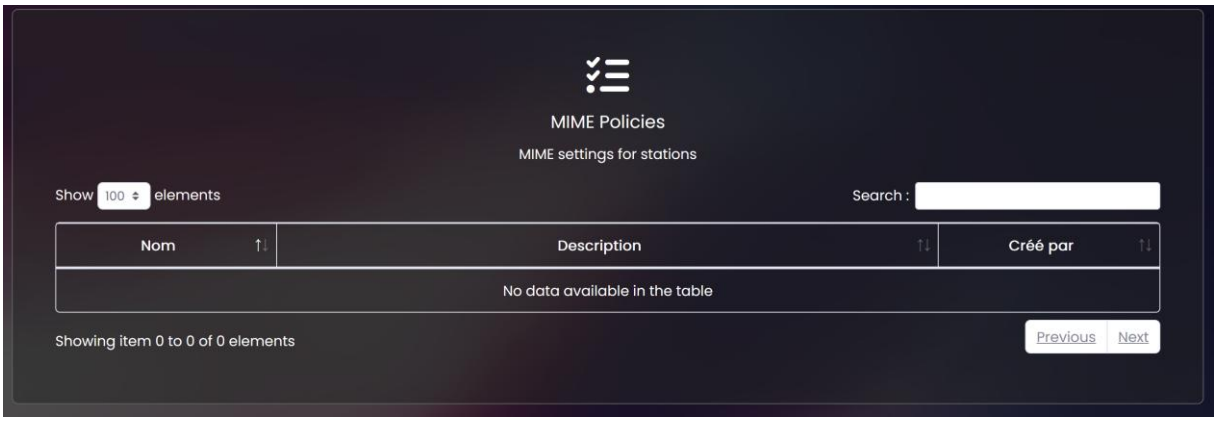
6.2.1.2 Network and services policies

The list of network policies can be accessed with the link labelled "Manage network policies":



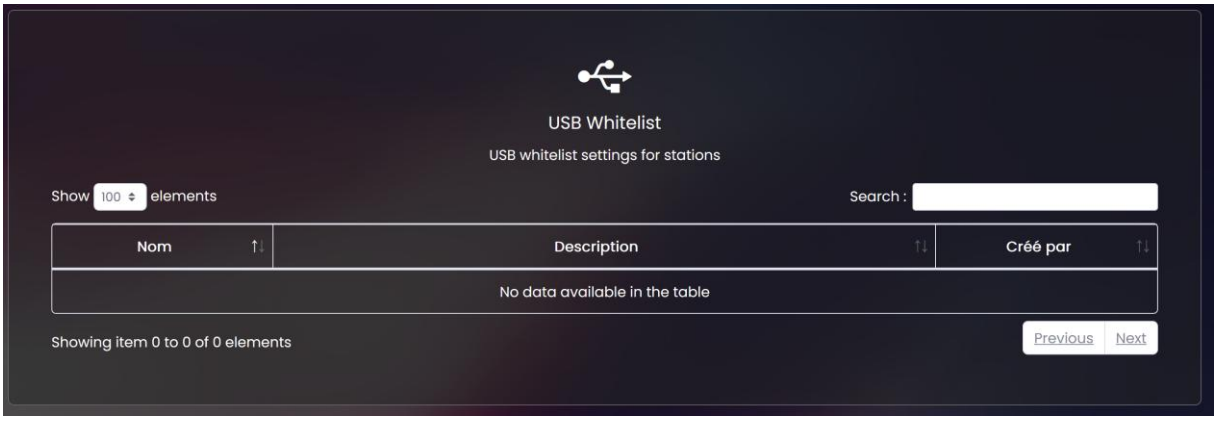
6.2.1.3 MIME filtering policies

The list of MIME filtering policies can be accessed with the link labelled "Manage MIME policies":



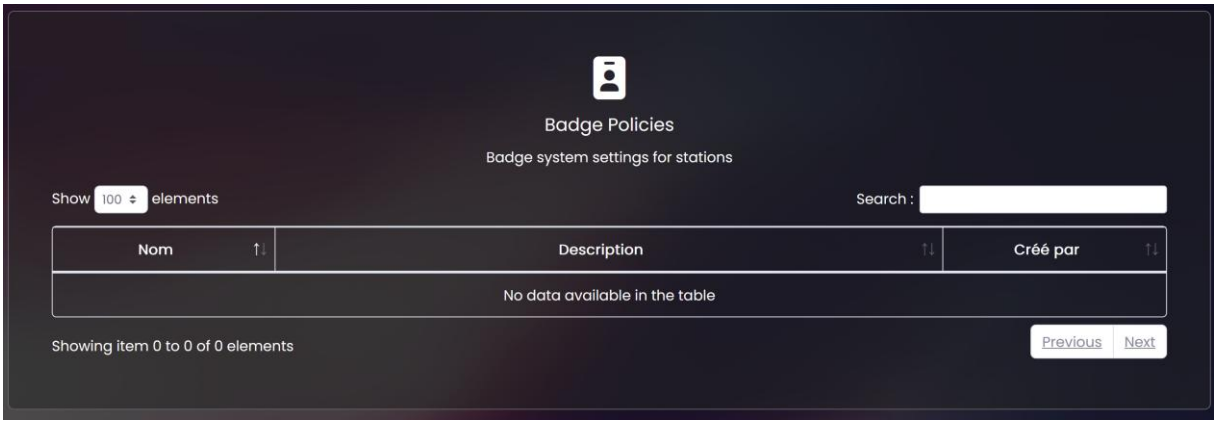
6.2.1.4 USB whitelist policies

The list of USB whitelist policies can be accessed with the link labelled "Manage MIME policies":



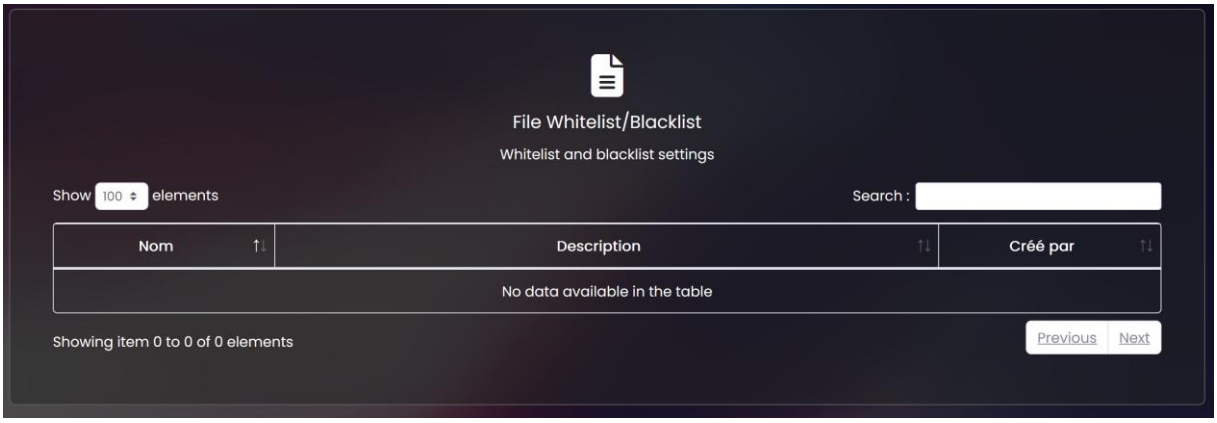
6.2.1.5 Badge policies

The list of badging policies can be accessed with the link labelled "Manage MIME policies":



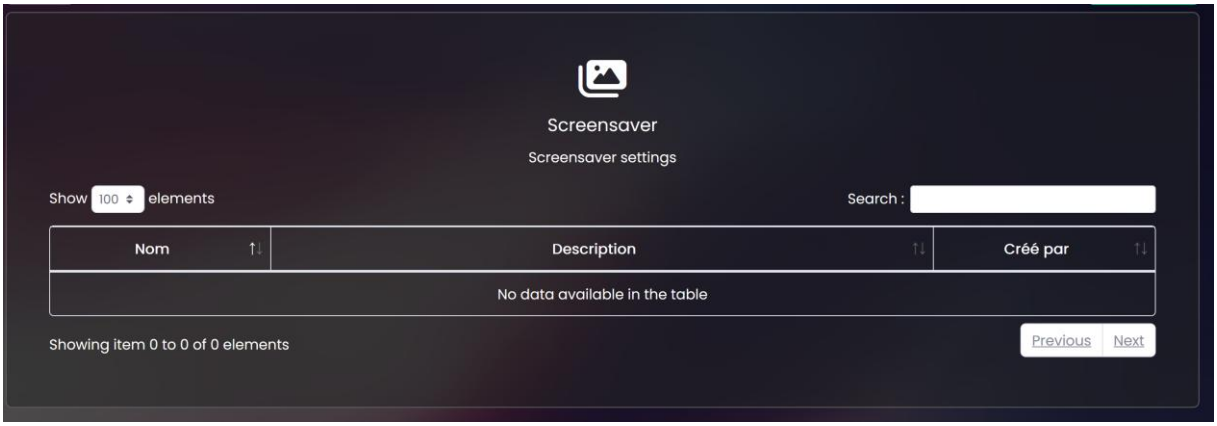
6.2.1.6 File whitelist/blacklist policies

The list of file filtering (whitelist/blacklist) policies can be accessed with the link labelled "Manage MIME policies":



6.2.1.7 Screensaver policies

The list of screensaver policies can be accessed with the link labelled "Manage MIME policies":



6.2.2 Edit security policies

It is possible to display/edit the details of a given policy from the list of security policies by clicking on its title. This edition is done through the use specific forms, that allow you to change all parameters according to the "S3 user manual" (ref. #1).

Each modified policy is taken into account by Hogo's infrastructure within 15 minutes. This means that after 15 minutes, the policy will be able to be synchronized with the devices during their update.

7 Manager users

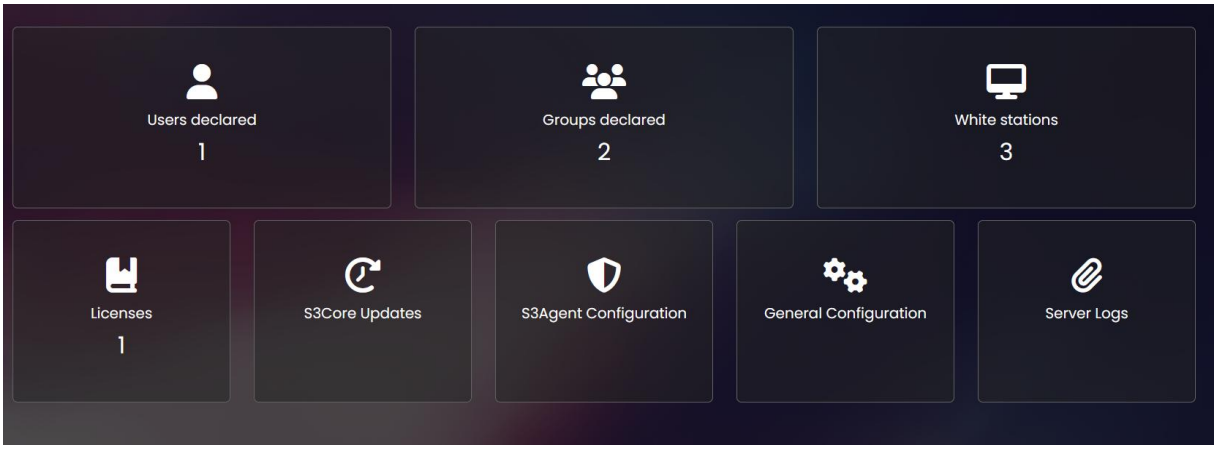
7.1 Role and dashboard

The "MANAGER" users are a specific category of users, that cannot see the devices security policies or statistics, but can create other users, manage the devices (create or delete devices from the database) and the licence files :

Function	Manager user	Owner user	Support user
Can create other users, groups, reset passwords...	Yes	No	No
Can add licence files, declare new devices...	Yes	No	No
Can associate users and devices with groups	Yes	No	No
Can see the S3SRV's internal logs	Yes	No	No
Can see the devices logs and statistics	No	Yes	Yes
Can see the devices info and status	No	Yes	Yes
Can edit the device's security policies	No	Yes	No

These users can also associate users accounts with devices (with the support or owner roles) and access the S3SRV's technical logs for maintenance or reporting purposes.

Their dashboard is a bit different from the regular user's dashboard, showing these tiles[2]:

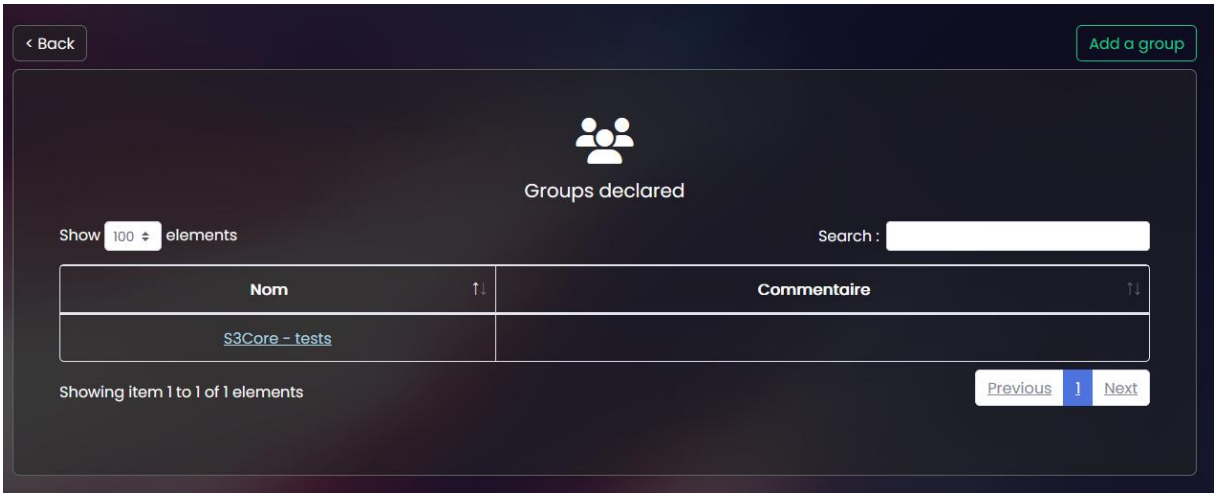


[2] The access to the tiles can be limited by your current S3SRV's version and/or license. Some module may not be activated by default.

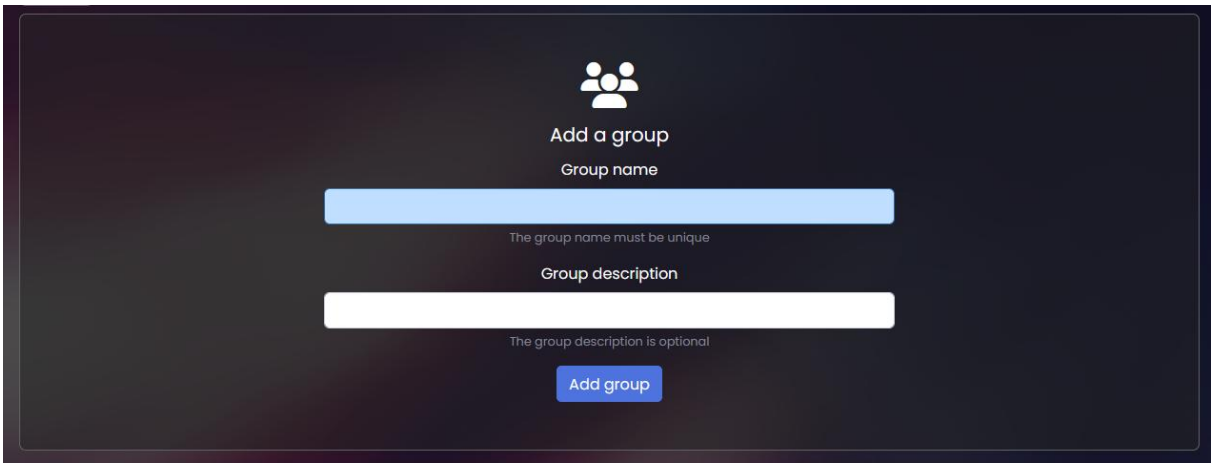
7.2 Groups and user management

7.2.1 Group management

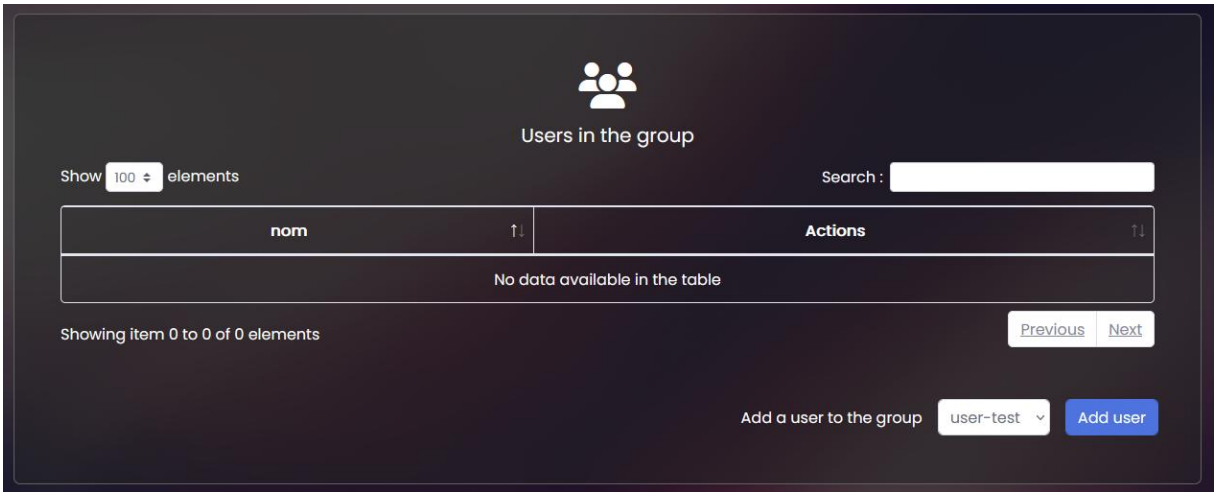
The group management module can be accessed by the second tile of the manager's dashboard. The list of groups currently on the Server can be shown:



Clicking on "add a group", the manager can create a new user group:

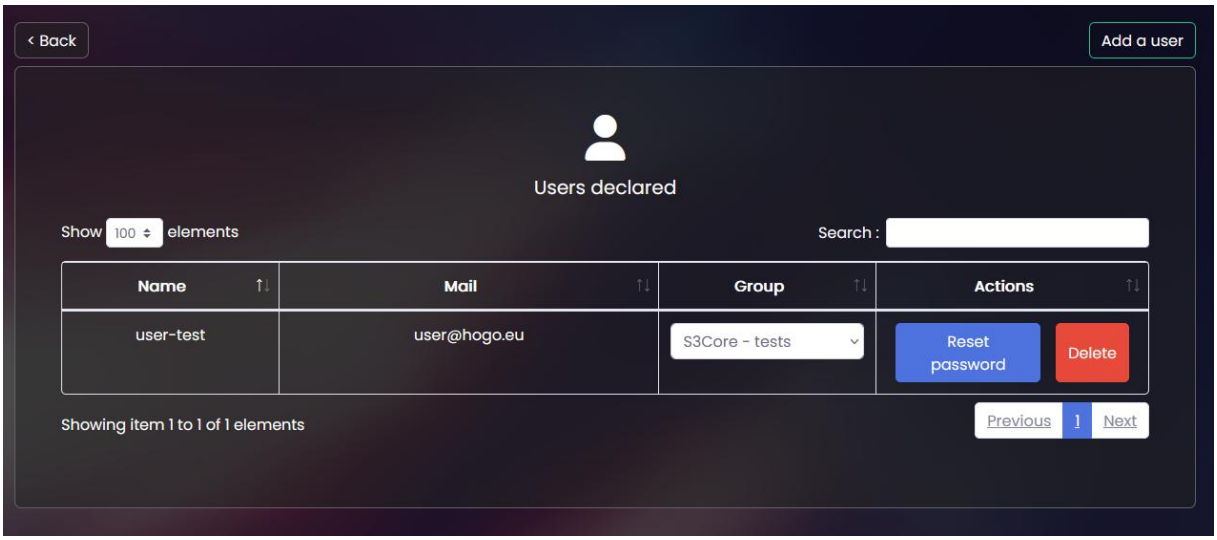


Then he can see which users are in the group and add/remove users from it:



7.2.2 User management

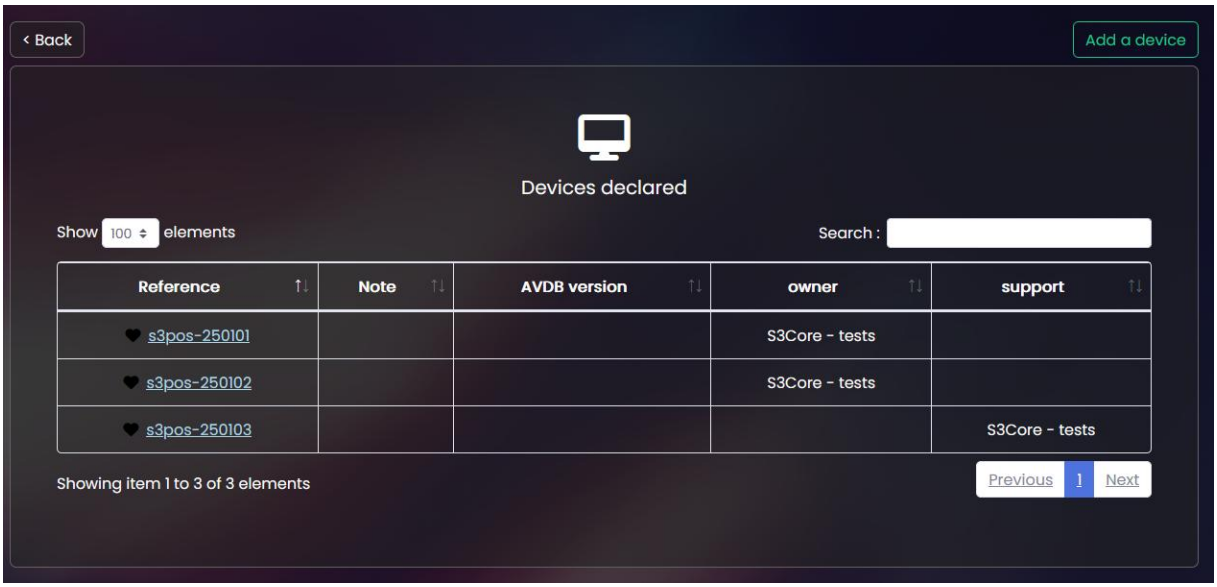
The manager can also create users (first tile of its dashboard) and see the currently declared users:



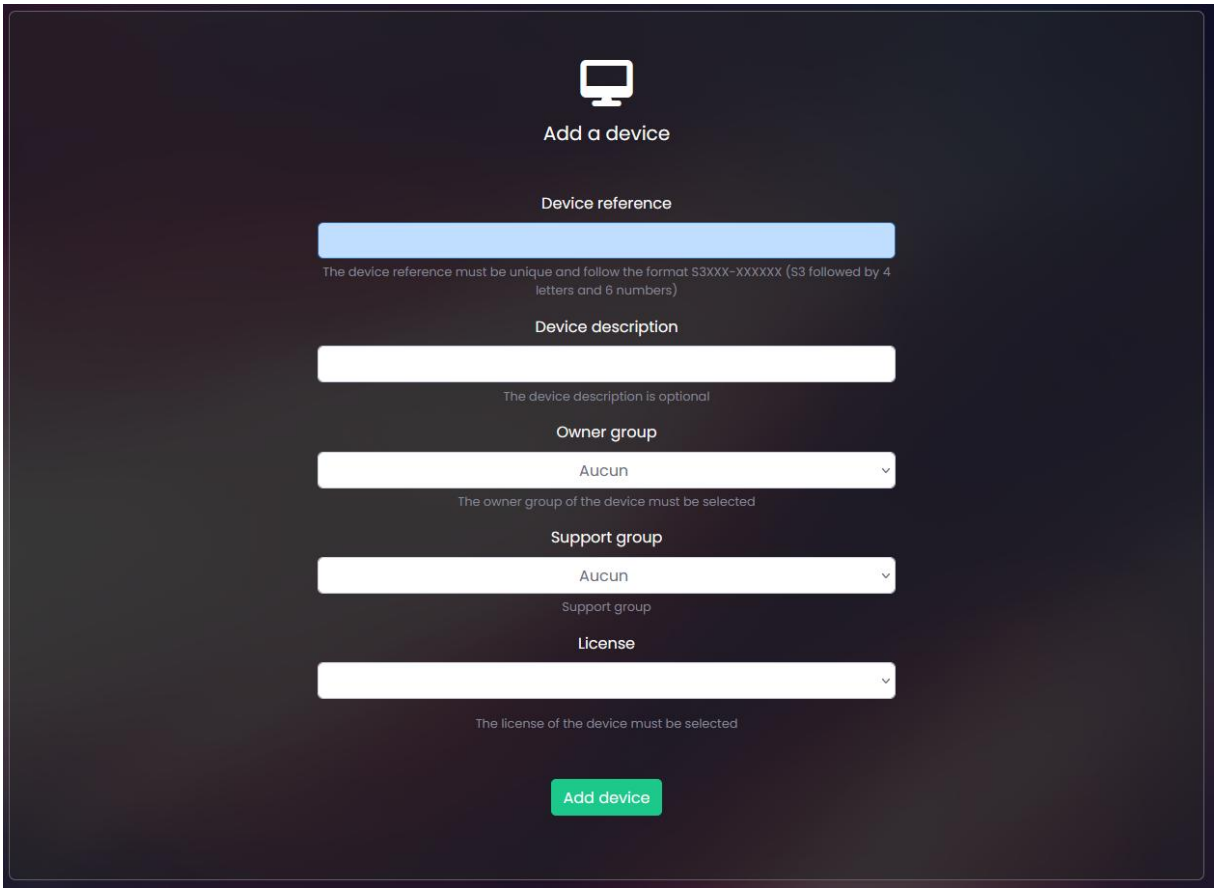
For each user, he can declare a group, reset the password (if the user loses it) or completely deleted the user's account.

7.3 Devices management

The manager can also create users (first tile of its dashboard) and see the currently declared users:



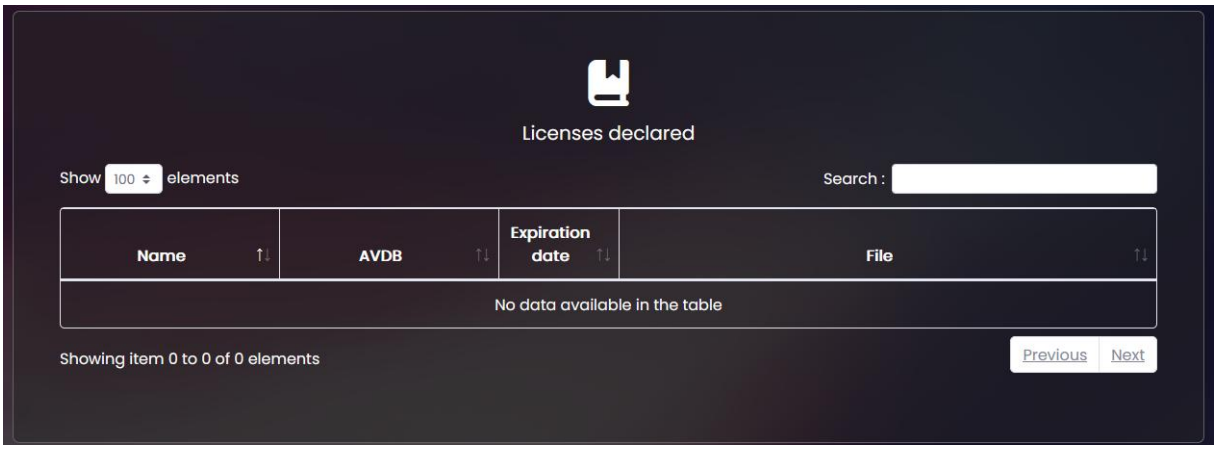
Clicking on "add a device", the manager can create a new user device, and associate it with a owner group and/or a support group:



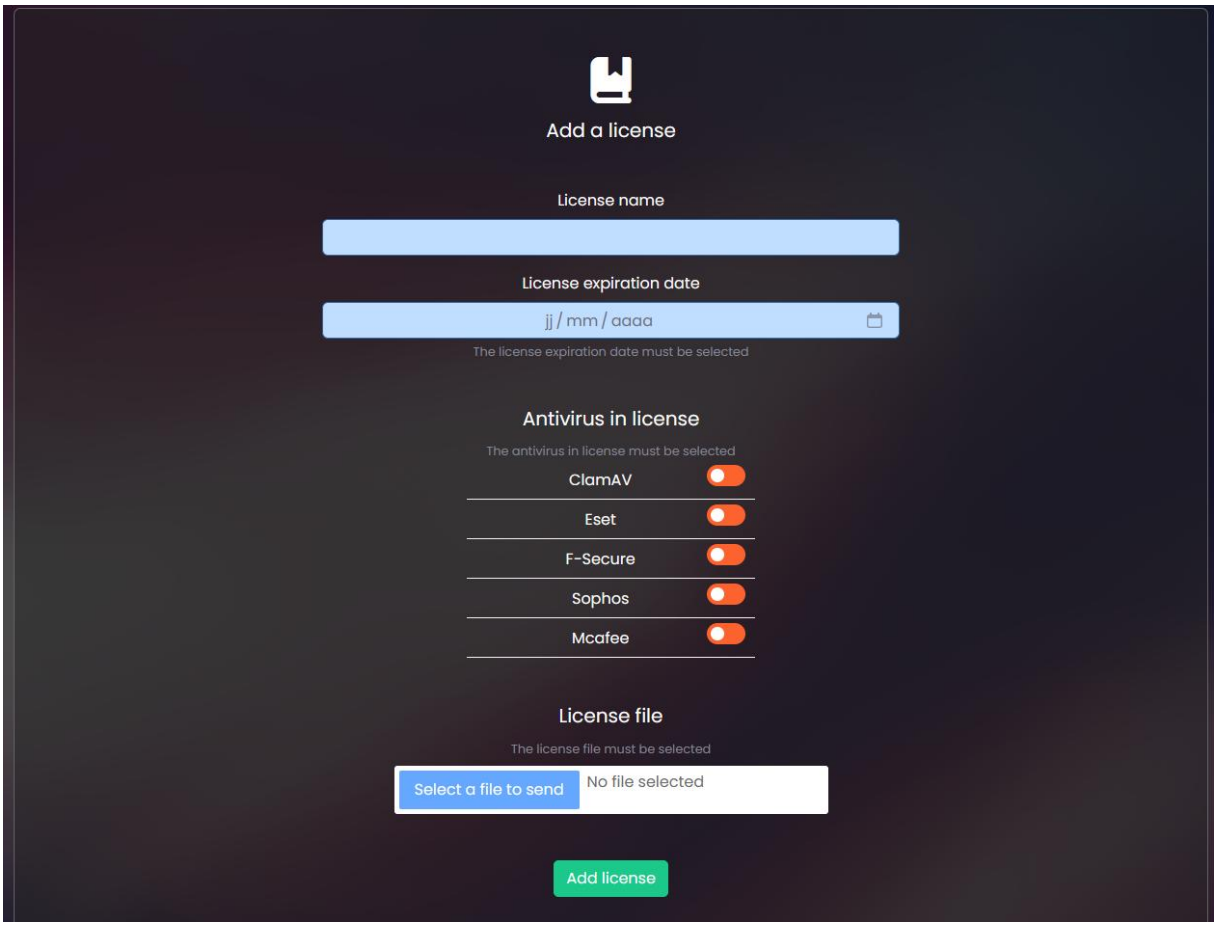
Each user will see the devices associated with his own group, with the level that is associated with each device.

7.4 Licences management

The manager can import license files and see the currently imported license for the devices:



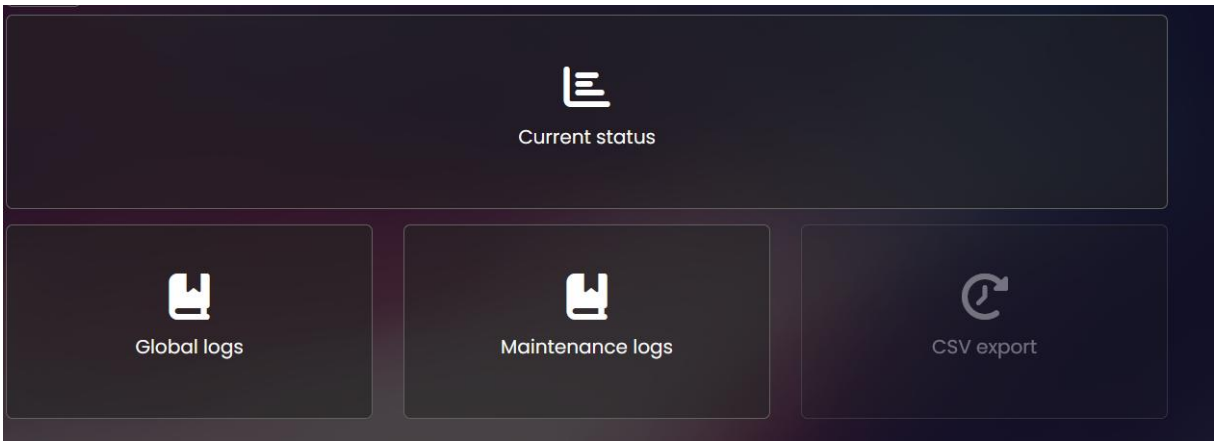
On each import, the license's information can be entered: name, expiration date, antivirus included, etc.



To be noted: this information is entered only for information, e.g. it does not modify the "real" expiration date of the license.

7.5 Access to server's logs

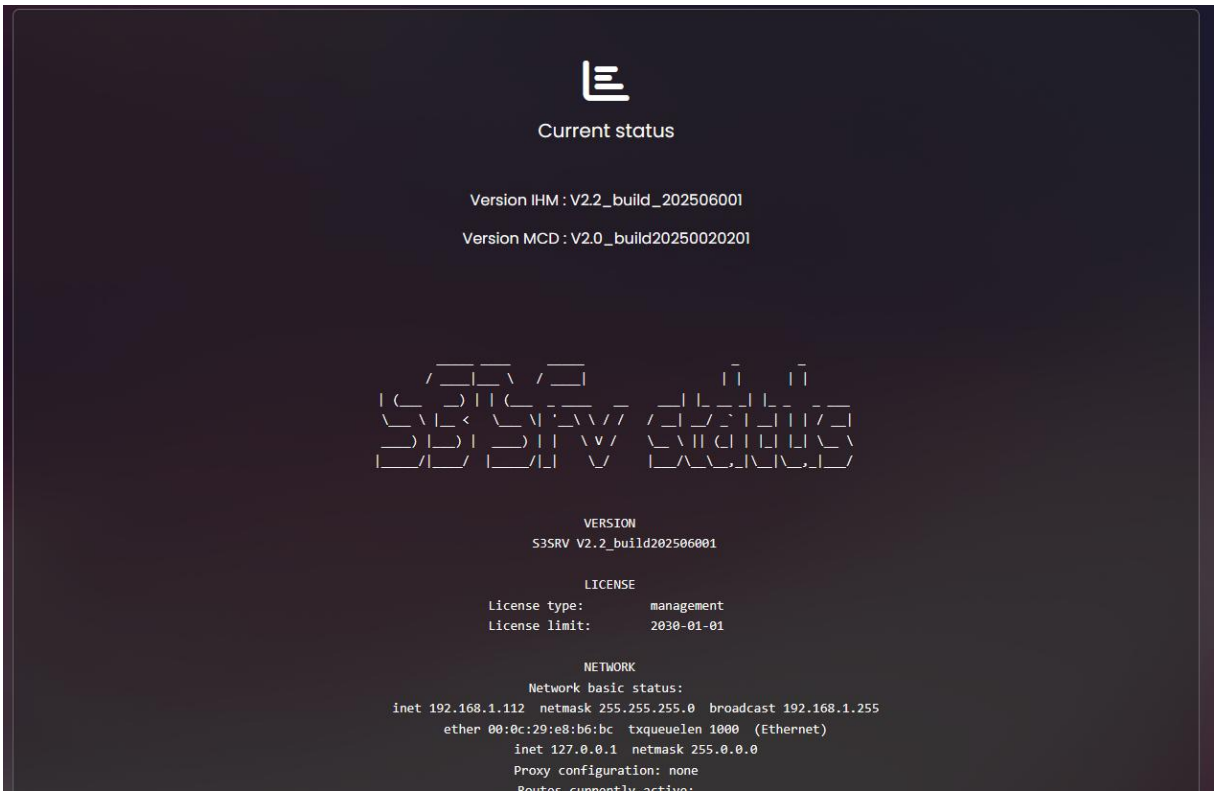
The manager can access the logs of the server:



The "current status" is a quick overview of the server (uptime, services ids, available av database...).

The "global" log shows the standard activity of the server (devices connections...) and the "maintenance" log show all events linked to update processes, reboots, etc.

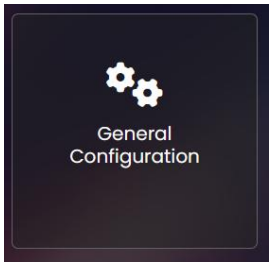
Each log with be displayed directly into the web browser, here is for example the "status" part:



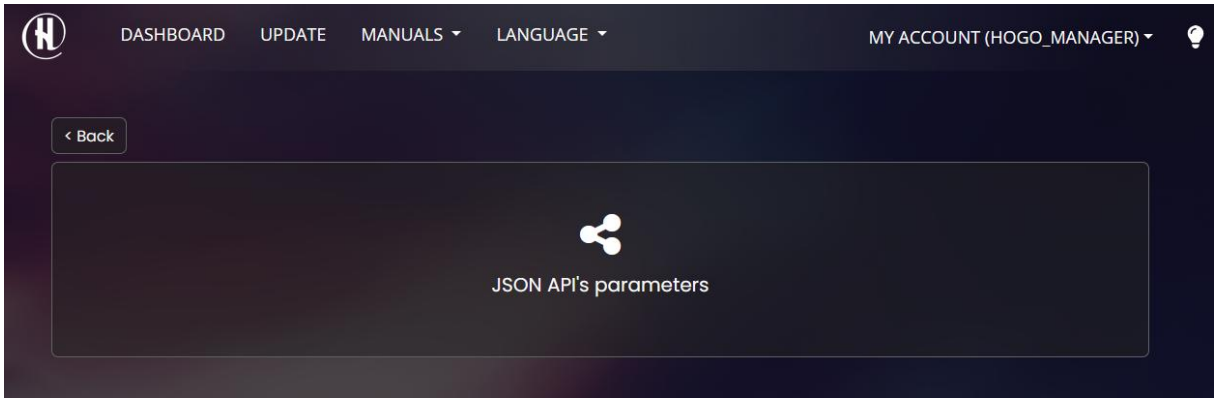
7.6 S3SRV's JSON API

7.6.1 Access and settings

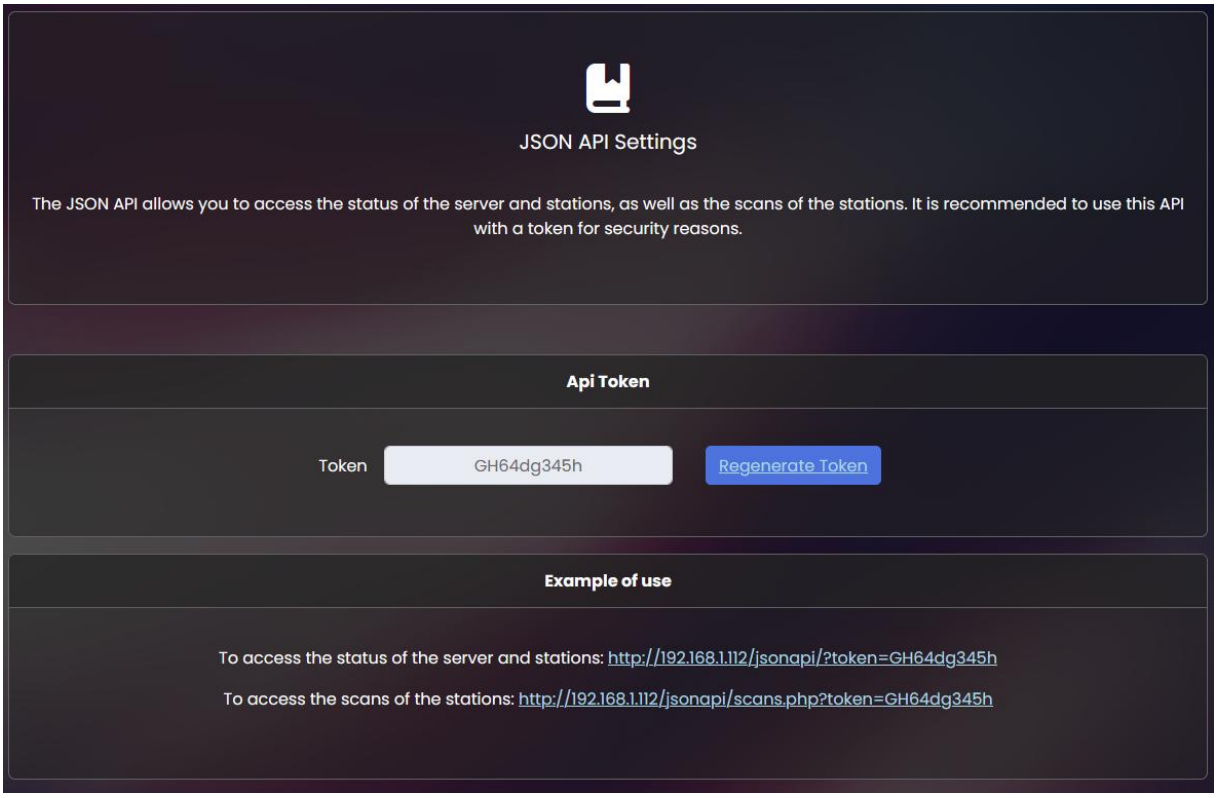
The S3SRV provides two JSON APIs, accessible if activated by the "Manager" users, using the "General Settings" button:



On the General Settings page, managers must click on " JSON API's parameters":



They will be able to change the settings of the JSON APIs and be provided with the endpoints URLs:



The APIs structure are described hereafter.

7.6.2 Server status API

The server status API provides information about the state of the server and all connected stations.
Its structure is as follows:

```
{
    "s3srv": {
        "name": STRING,
        "uptime": STRING,
        "avdb": {
            "a0000": STRING,
            "a0001": STRING,
             "..." : STRING,
            "d1111": STRING
        },
        "s3core": {
            "s3box": STRING,
            "s3pos": STRING,
            "s3tot": STRING
        }
    },
    "stations": [
        {
            "id": INT,
            "name": STRING,
            "heartbeat": ENUM,
            "avdb": DATE_SHORT,
            "s3core": STRING
        },
        { ... }
    ]
}
```

The root object contains two main keys:

- s3srv: information related to the central server.
- stations: list of stations connected to the server.

The server-related information is as follows:

Key	Type	Description
name	STRING	Server name (hostname).
uptime	STRING	Server uptime since the last reboot (Unix-formatted string, e.g. `"32 D - 18 H - 21 M - 26 S"`).
avdb	OBJECT	Dictionary of available antivirus database versions on the server, using the format `"reference": "file"`. The reference is written in the range A0001 to D1111, and the file corresponds to the available database, for example `"12-08-2025_defs.jit"`.
s3core	OBJECT	Information about the main software components of the server, using the format `"type": "file"`. The type can be s3box, s3pos, or s3tot, and the file represents the available package, for example: "S3Box_V1.8_build2024072006_Core.jit".

The station-related information is presented as an array of objects, each element representing a station:

Key	Type	Description
id	INT	Unique station identifier (numeric).
name	STRING	Station hostname.
heartbeat	ENUM	Communication status with the server. Possible values: `"perfect"`, `"good"`, `"low"`, `"none"`.
avdb	DATE_SHORT	Date of the last antivirus database update on the station (short format, e.g. `"2025-08-20"`).
s3core	STRING	Version of the software core installed on the station, e.g. `"V1.8 build2025030112"`.

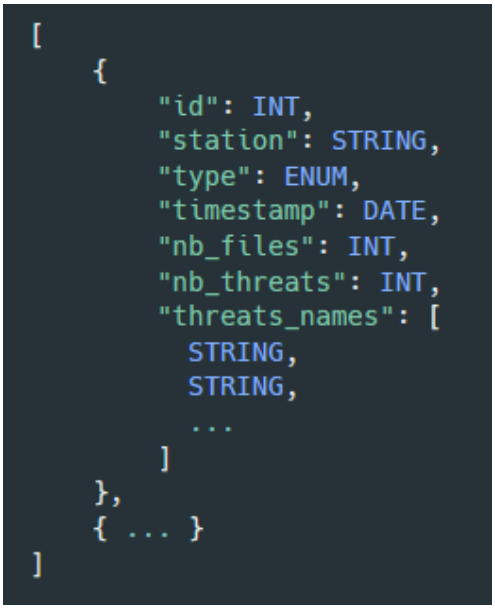
This API can be accessed with the following URL pattern:

https://IP_OR_HOSTNAME/jsonapi/?token=TOKEN

With IP_OR_HOSTNAME the IP addres or hostname of your server, and TOKEN the security token set by the Manager users.

7.6.3 Scan data API

The scan data API provides access to the summaries of all scans sent to the server over the last 30 days.
Its structure is as follows:



Each object represents a scan report originating from a station:

Key	Type	Description
id	INT	Unique scan identifier (incremental numeric value).
station	STRING	Name of the station from which the scan originated.
type	ENUM	Type of event or report. Possible values depending on context: `"scan"`, `"smart-scan"`, `"decontamination"`.
timestamp	DATE	Date and time of the event, in ISO 8601 format (e.g. `"2025-10-20 14:32:11"`).
nb_files	INT	Total number of files scanned or affected by the operation.
nb_threats	INT	Total number of detected threats.
threats_names	ARRAY[STRING]	List of detected threat names. May be empty if no threats were found.

This API can be accessed with the following URL pattern:

https://IP_OR_HOSTNAME/jsonapi/scans.php?token=TOKEN

With IP_OR_HOSTNAME the IP addres or hostname of your server, and TOKEN the security token set by the Manager users.