Hogo S3

HR-MAN-26-211-v5

Administrator's Manual

2026

This document describes the installation and administration of Hogo's S3 station range and the safety instructions related to their use.

Version	Date	Major changes
V1	02/2018	Initial version of the document
V2	05/2019	Updated following an internal review
V3	11/2025	Updated to align with the T4 2025 update
V4	01/2026	Updated following an internal review
V5	03/2026	Updated to align with the T1 2026 update

Table of contents

1 Introduction 4
1.1 Hogo 4
1.2 S3 range 4
1.3 This document 4
2 Product packaging contents 5
2.1 S3Box Tablet 5
2.2 S3Pos Station 5
2.3 Totem S3Tot 6
2.4 S3 Boot 7
3 Prerequisites 8
3.1 Environmental Requirements 8
3.2 Electrical Requirements 8
3.3 Network Requirements (if the station is connected) 9
4 Safety Instructions 10
5 Unpacking and Installation 11
5.1 S3 Stations (excluding S3Boot) 11
5.2 S3Boot Disks 11
6 Initial power-up 12
7 Home Screen 13
8 Global settings 14
8.1 Configuration Wizard 17
8.2 Update center 18
8.3 Logs 24
8.4 Certificate Manager 27
8.5 USB Manager 28
8.6 Format settings 30
8.7 Card reader parameters 32

8.8 SFS settings 34
8.9 Scan settings 36
8.10 Password Change 39
8.11 Date and hour 41
9 Initial Update 43
10 Functional Tests 44
11 S3Core Rescue mode 45
12 Additional warnings 46

1 Introduction

1.1 Hogo

Hogo Business Services SAS is a company create in 2016 in Rennes. Specializing in cybersecurity, Hogo provides fully integrated, ready-to-use security solutions to secure any information system.

Hogo also offers several associated services: support in using its products, technical support, cybersecurity expertise (risk and vulnerability analysis, integration, etc.) and development of specific software (specialized R&D).

Hogo adopts a security approach that is as pragmatic as possible. Our projects are born from concrete feedback and experience, and Hogo develops security solutions that respond quickly and effectively to its clients' needs.

Hogo is also heavily involved in reducing the environmental impact of its activities. A member of the "Institut Numérique Responsable"(INR) and a privileged partner of the public interest association "Bretagne Vivante", Hogo innovates and implements a strict and ambitious CSR policy.

1.2 S3 range

The Smart Secure Sanitizer "S3" range is a USB Clean Station solution designed to protect your sensitive Information System against infected USB devices:

- Protect your information system against infected or dangerous devices,
- Import data into your sensitive system without a direct device connection,
- Scan and filter your input data (with up to 5 antivirus programs and MIME, PGP checks...)
- Use only keys from the company's authorized network - key filtering by Serial ID -,
- Prevent any information leaks or unauthorized data entry into your system.

1.3 This document

This document is the Administrator's Manual for the S3 series of workstations. It describes their setup and the startup and reception procedures, including safety aspects. It follows a sequence based on the product's standard HMI.

To go further:

- The quick start guides for receiving a station is located here: https://hogo.eu/start/
- The support portal for all technical questions is located here: https://support.hogo.eu/
- Quick reference guides to assist you with practical use cases are available here: https://hogo.eu/zone_echange/outils_hogo/Fiches_REFLEXE_gamme_S3.pdf

2 Product packaging contents

2.1 S3Box Tablet



- 1 rugged, mobile and shock-resistant tablet
- A charging cable (230V AC to DC USB-C connector)
- A charging dock with a dedicated 12v DC output charger (optional for the tablets concerned)

2.2 S3Pos Station





- 1 all-metal unit with 13-inch touchscreen
- A power cable with a 230V AC to 19V DC transformer
- A Wi-Fi antenna (for the stations concerned)
- Front metal casing for physical protection of the USB ports (optional for applicable workstations)

2.3 Totem S3Tot



- 1 self-supporting totem post

2.4 S3 Boot



- 1 hard drive formatted with the S3Boot system (2.5" SSD or M2 NVMe as per order form))

3 Prerequisites

3.1 Environmental Requirements

- Choose a clean and clear space, suitable for the size/number of equipment to be installed.
- Choose a stable, non-electrostatic surface to avoid any electrical damage to the equipment.
- Ensure the equipment is placed in a location where it can be properly ventilated. Avoid blocking ventilation openings to prevent overheating.

3.2 Electrical Requirements

- Always use a power cable in good condition supplied by Hogo. Avoid using damaged or frayed cables.
- S3Box: Connect the charger supplied with the station to a mains power supply (230V AC, 50Hz) for DC power to the USB-C charger output.
- S3Pos: Only connect the cable to the rear of the station's mains power supply (230V AC, 50Hz) for a 19V DC output from the transformer. [1]
- S3Tot: Simply connect the cable to the rear of the totem and plug it into the mains power supply (230V AC, 50Hz).

The nominal power ranges consumed by the equipment are as follows:

- S3Box: 5 Watts (at rest) to 12 Watts (in use, typically when scanning USB media)
- S3Pos: 20 Watts (idle) to 90 Watts (active, typically when scanning USB media)
- S3Tot: 30 Watts (idle) to 110 Watts (active, typically when scanning USB media)

Finally, the internal operating temperature of these three pieces of equipment must be between 0°C and 50°C at all times (furthermore, external AC/DC power supplies must never exceed 40°C).

Attention, the equipment in the S3 range is not suitable for use in places that may accommodate children.

Attention, the power cord of the equipment constitutes its electrical disconnection device; it must be easily accessible to operators at all times.

[1] Electrical adapter type "HKA09019047-8U" with input voltage 110-240V at 50/60Hz under 1.5A and output 19.0V under 4.74A to 8A.

3.3 Network Requirements (if the station is connected)

- RJ45 network cable, category 6 minimum, for stations connected via cable.
- Or: Open Wi-Fi network, password protected or not, SSID hidden or broadcast.
- Open flows according to the following matrix:

Fonction	Source	Destination	Protocole	Port
Network Test	Station S3	S3SRV	HTTPS	443
AV Update	Station S3	S3SRV	HTTPS	443
Core Update	Station S3	S3SRV	HTTPS	443
Sending versions	Station S3	S3SRV	HTTPS	443
Sending logs (server)	Station S3	S3SRV	HTTPS	443
Sending logs (syslog)	Station S3	Syslog Server *	HTTPS	Port configured
License recovery	Station S3	S3SRV	HTTPS	443
NTP Synchronization	Station S3	NTP Server *	NTP	123
Full synchronization	Station S3	S3SRV	HTTPS	443
Connecting to the proxy	Station S3	Proxy *	HTTP or HTTPS	Port configured
Network test	S3SRV	MyHogo.eu	HTTPS	443
NTP Synchronization	S3SRV	NTP Server *	NTP	123
Sending logs (syslog)	S3SRV	Syslog Server *	HTTPS	Port configured
Connecting to the proxy	S3SRV	Proxy *	HTTP or HTTPS	Port configured
AV Update	S3SRV	MyHogo.eu	HTTPS	443
Core Update	S3SRV	MyHogo.eu	HTTPS	443
Manual AV/Core Update	Workstations	S3SRV	HTTPS	443
Web interface (portal)	Workstations	S3SRV	HTTPS	443

** : Servers marked with an asterisk are outside the scope of Hogo provision.*

4 Safety Instructions

Please ensure that you follow these safety instructions when installing and using the S3 equipment:

- Avoid static electricity:
  Static electricity can damage internal components. Touch an unpainted metal object before handling internal components or cables during connections to discharge any static electricity.
- Never force connections:
  If a cable or device doesn't seem to fit properly, don't force it. Double-check that you're using the correct port or cable.
- Keep liquids away:
  Avoid placing drinks or other liquids near your S3 equipment to prevent any risk of spillage.
- Update and maintenance:
  To ensure the safety and performance of your equipment, regularly perform software updates and check its cleanliness (e.g., dust removal).

5 Unpacking and Installation

5.1 S3 Stations (excluding S3Boot)

1. Unpacking the equipment
- Carefully remove the S3 equipment from it carrying case and place it on the docking surface.
- If additional external devices are needed (e.g., a printer, a badge reader), connect them to the appropriate ports.

2. Power supply
- Connect the charger supplied with the S3Box to its socket on the S3 device (skip this step for the S3Tot and S3Pos).
- Connect the power cord to a mains socket equipped with a grounding plug.

3. Powering on
- Press the "power" button on the S3Box, or flip the switch on the back of the S3Pos, to start it (this does not affect the S3Tot, which will start when plugged in).
- Follow any on-screen instructions for initial setup (the equipment is usually pre-configured, but questions may arise during the first startup).

5.2 S3Boot Disks

1. Unpacking the equipment
- Carefully remove the S3Boot disc from its bubble wrap envelope.

2. Retrieving your license key
- Note the beginning of the key available on the disk (s3boot-xxxxx)
- Send this part of the key to technical support on the portal https://support.hogo.eu

3. Finalizing the installation:
- You will receive your full license key from support, as well as the procedure to finalize the installation of your S3Boot.
- Once the disk is initialized and the workstation is restarted, you will have access to the Hogo white station interface.
- You will see in the top left corner that your license is invalid
- You can retrieve the reference (equipment name) in "Settings / Logs" to finalize the support procedure.
- An update will then be provided to activate your license and thus finalize the installation.

Note:

- *Once the disk is initialized, it can no longer be installed on a different machine.*
- *Attention, the computer on which you install S3Boot must have a screen natively in 16:9 format, 1920x1080 resolution.*

6 Initial power-up

Each time the station is started, a screen displays the operating conditions and system information.

After accepting the terms of use (by clicking "Yes"), you will be automatically redirected to the home screen.



7 Home Screen

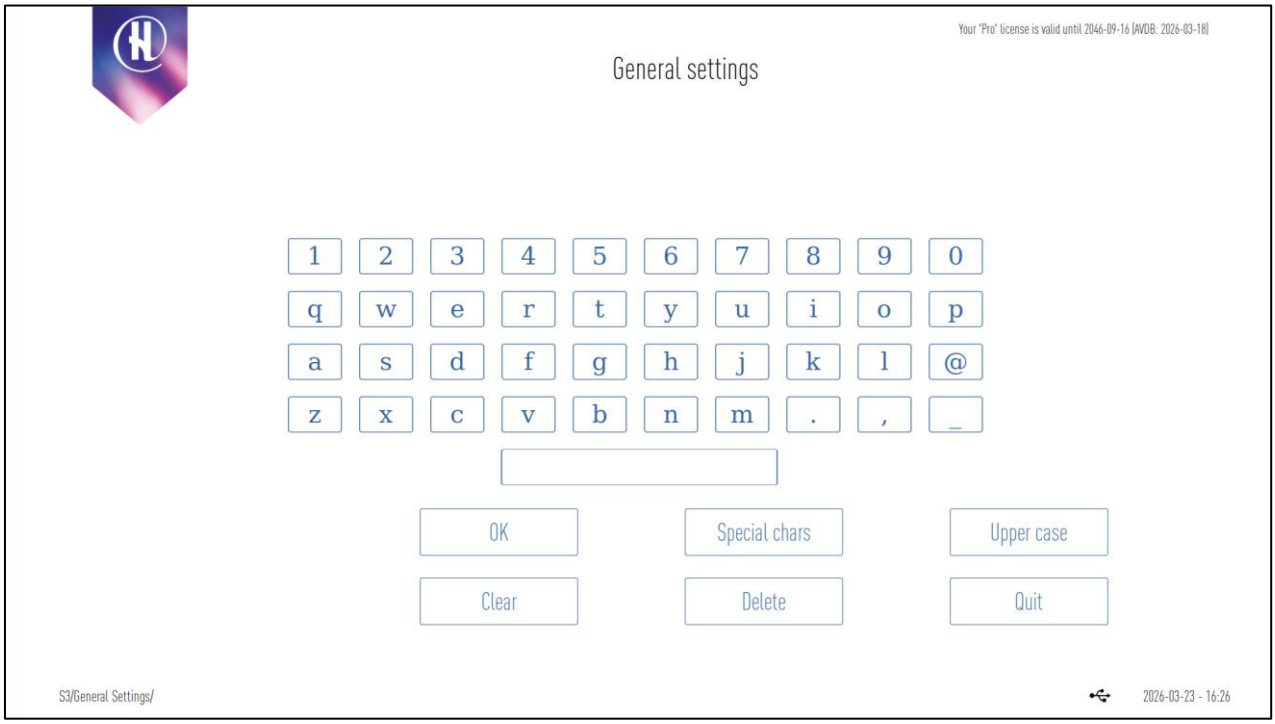


From the home screen, you can access the standard functions in the middle of the screen, in the Tools menu , the help menu , the language menu and the administration settings .

Note : For details of standard functions, please refer to the User Manual. This document focuses on Administration settings.

8 Global settings

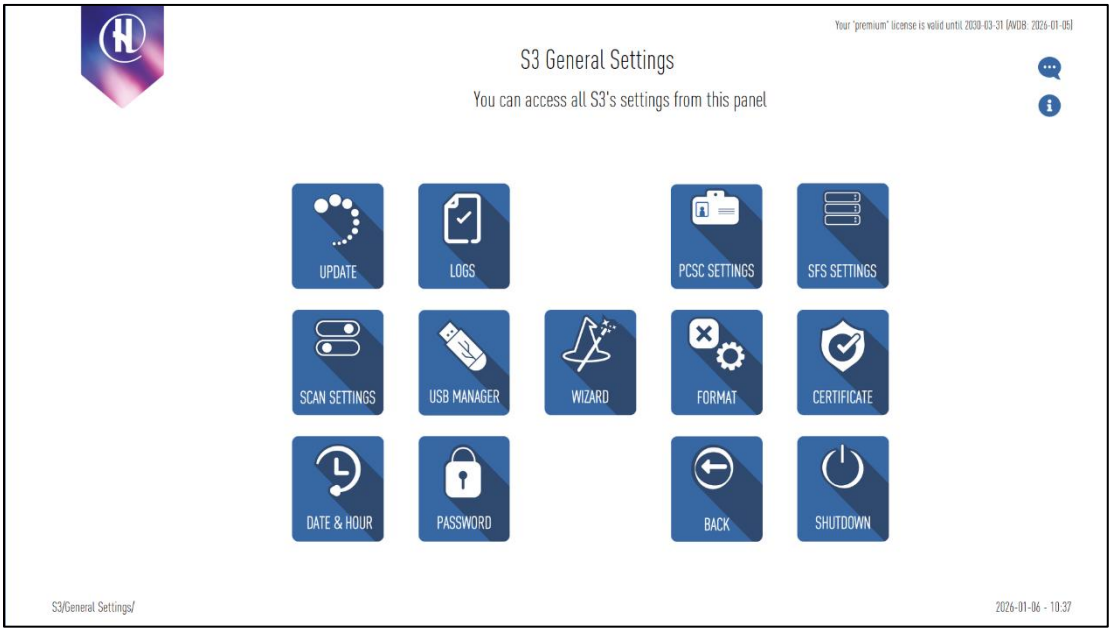
This screen can be accessed, after entering a password, from the home screen by clicking on "Settings" or the gear icon:



Note: The station's initial password is "1234567890"; it is important to change it upon first use.

Note: If you lose your password for accessing the settings, remote recovery will not be possible. Returning the station to customer service is mandatory and is not covered by the Hogo warranty.

The accessible functions are:



	Access to the update center: Opens the screen containing menus relating to Core updates, antivirus updates, online synchronization and network settings of the station, see chapter 8.2.
	Log access: Allows access to log management, including retention configuration, export of technical logs or scan logs, and sending to a remote server, see chapter 8.3.
	Badge reading management: Allows you to manage the list of authorized badges (add, delete, export) and the parameters related to PCSC control. A badge must be present in the list before the control is activated; see section 8.7.
	File sharing settings: Opens settings related to Smart-Transfer file transfer modes and network sharing options (depending on your configurations), see chapter 8.8.
	Scan settings: Allows you to configure MIME filtering, SHA256 control, antivirus scan mode, threat handling, protected ZIP management and the action applied to the output USB media, see chapter 8.9.

	USB manager for filtering allowed media: Displays the list of allowed USB media and allows you to add or remove USB media. To clear or export this list, see chapter 8.5.
	Configuration Wizard: Launches the automatic configuration wizard to help configure the network and station services in a guided manner. Never launches automatically; see section 8.1.
	USB media formatting settings, see chapter 8.6.
	Certificate Manager: Allows you to view the list of PGP certificates known to the workstation, as well as add or remove them. Certificates must comply with RGS V2 criteria, see chapter 8.4.
	Time and date settings: Allows you to configure the date, time and associated settings (NTP, possible synchronization), see chapter 8.11.
	S3 Password Manager: Allows you to change the password for accessing settings, see chapter 8.10.
	Return to the home screen: Closes the Settings menu and returns to the station's home screen.
	Turn off or restart the station: Allows you to completely stop or restart the white S3 station (choice to be made on the popup that will be displayed on the screen).

8.1 Configuration Wizard

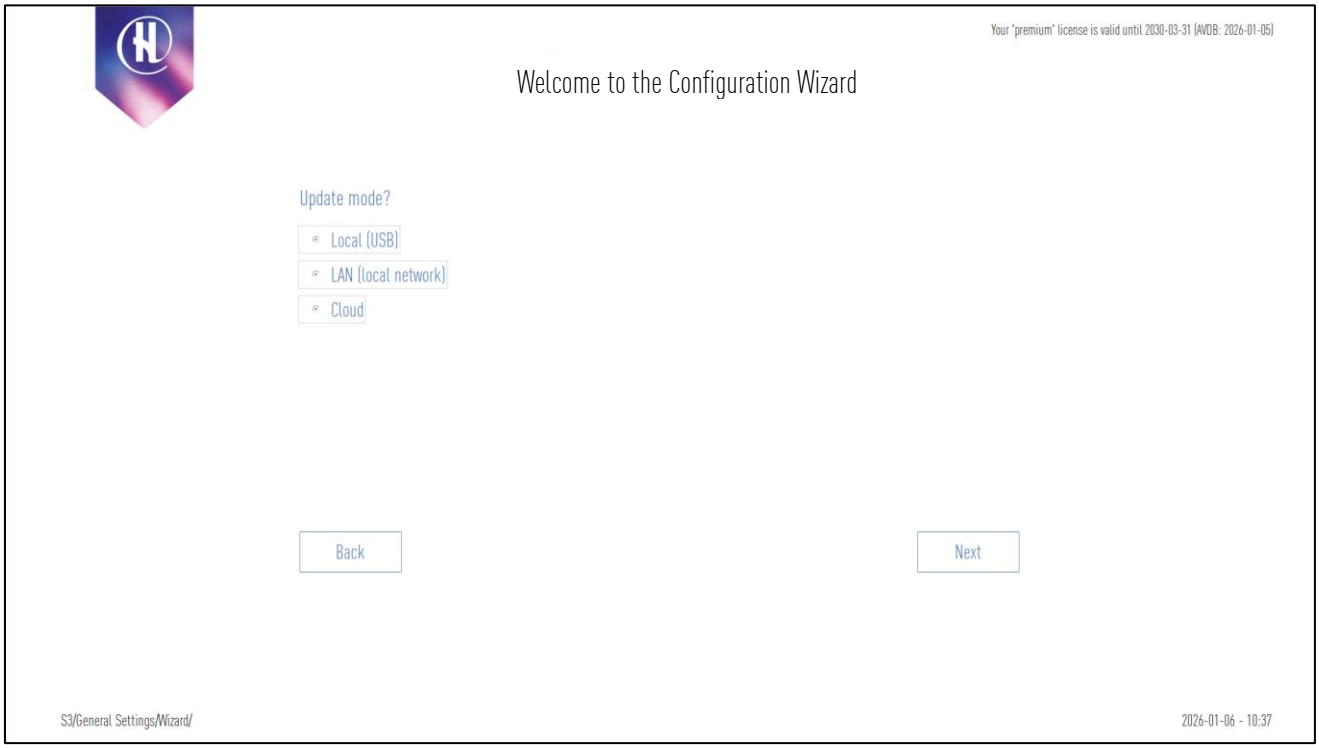


The Setup Wizard (automated setup assistant) is there to help you configure the network and services of your station:

It takes the form of a series of questions allowing you to make the initial adjustments.

If you later need to modify the various settings, you can either restart the Wizard or access the settings in the different tabs of the "Settings" menu.

Example of questions asked by the Setup Wizard:

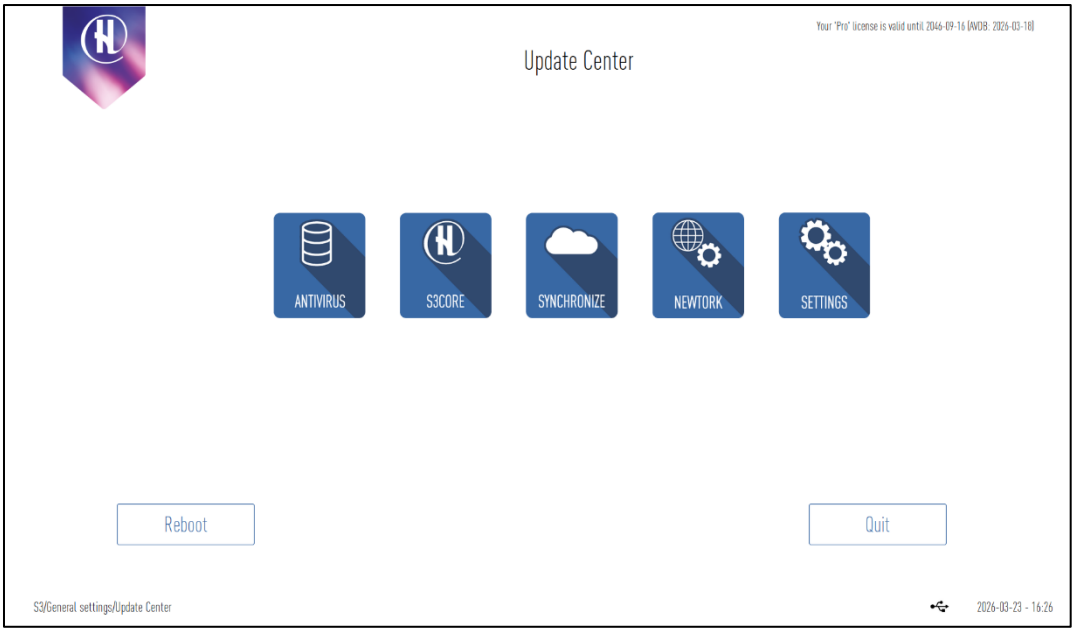


See the sequence of questions in the Setup Wizard in Appendix 1.

8.2 Update center



The update center includes various menus related to Core and Antivirus updates, as well as network settings.



	Antivirus update (detection databases)
	Core S3 update (software)
	Online synchronization (on cloud or S3Srv "on premises")

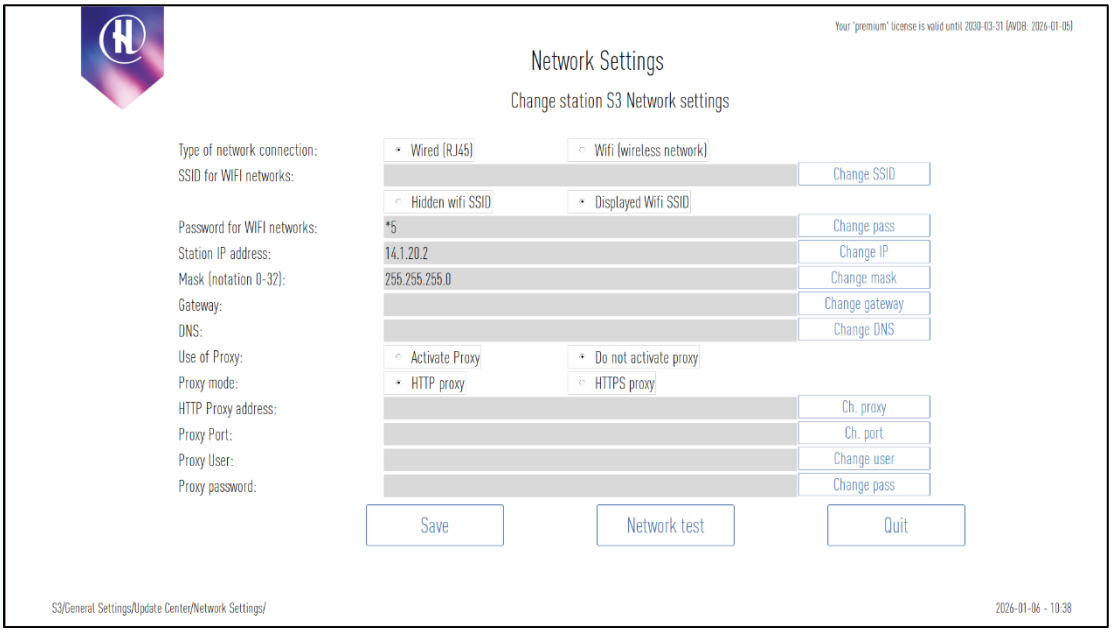
	Station network connection settings
	Station updates settings

8.2.1 Network Configuration



The network settings screen allows you to configure and manage all of the system's connectivity options. This area contains all the information needed to manage wired or wireless connections, as well as settings related to using a proxy server.

The screenshot included in this chapter illustrates the various available settings:



8.2.1.1 Connection configuration

In this section, you can view the type of connection used by the station, whether it is an Ethernet connection or a Wi-Fi network.

If the station uses a wireless connection, you have the option to view or modify:

- The Wi-Fi network SSID: the name of the access point to which the station should connect.
  It is possible to choose a hidden or broadcast SSID.
- The Wi-Fi password: the security key allowing access to the network.

These settings allow you to establish or adjust the Wi-Fi connection according to your infrastructure.

8.2.1.2 IP settings

You can also define or check the system's IP addressing settings:

- IP Address: the address assigned to the workstation (or "DHCP" for an automatically obtained IP address)
- Subnet mask: expressed in CIDR notation (from 0 to 32, or an empty field for a DHCP IP)
- Gateway: the address of the router or gateway used to access another subnet or the internet.
- DNS server: the address of the server responsible for resolving domain names.

These settings give you complete control over the system's IP configuration, whether static or automatic.

8.2.1.3 Proxy configuration

If your network environment uses a proxy server, you can enable and configure this service using the following options:

- Proxy usage: allows you to enable or disable the proxy.
- Proxy mode: choice of proxy type used (HTTP or HTTPS).
- Proxy address: proxy server address corresponding to the chosen mode.
- Proxy port: network port associated with the proxy service.
- Proxy username: Username required for authentication.
- Proxy password: password associated with the username.

These settings ensure compatibility with infrastructures requiring control or filtering of outgoing traffic.

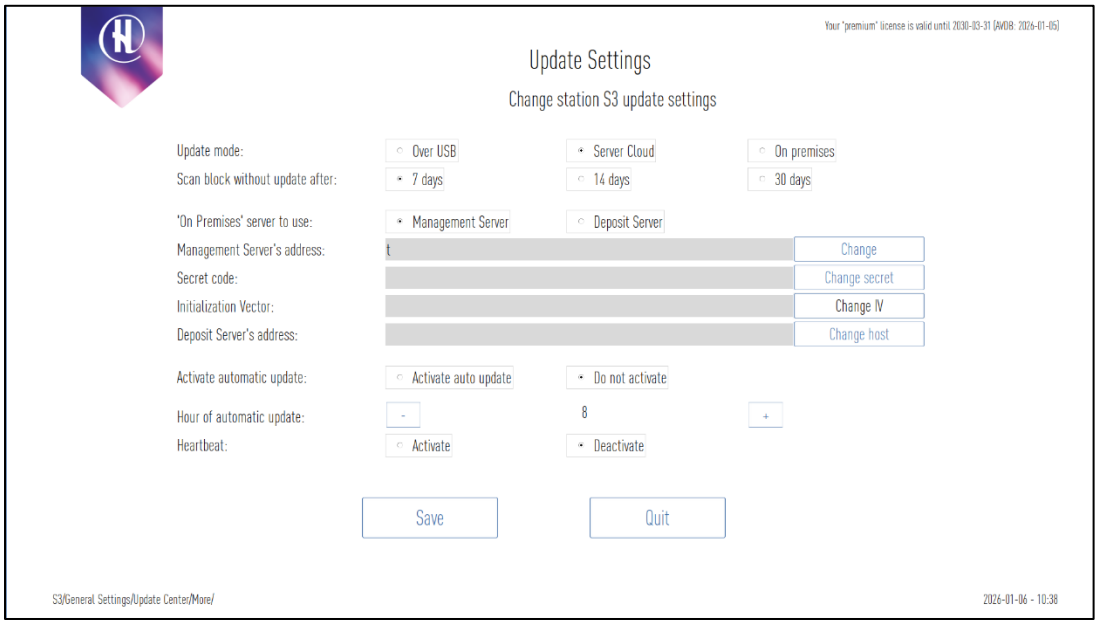
Note: To apply these proxy-related settings, a station restart is required.

8.2.2 Settings



The update settings screen allows you to define the source, behavior, and frequency of system updates. This area groups all the options necessary to ensure that the workstation remains compliant, secure, and up-to-date.

The screenshot included in this chapter illustrates the different settings available.



8.2.2.1 Update mode

You can select the source from which the system will download its updates. Several modes are available:

- USB: The update is performed from a USB drive containing the necessary files.
- Cloud server: the station retrieves updates from your MyHogo online account (the file must be in the root of the media).
- Local Network: updates are downloaded from an S3SRV server, present in your infrastructure.

These options allow you to adapt the update strategy according to the constraints of your environment (offline, local network, or Internet).

8.2.2.2 Handling the absence of updates

To ensure system compliance, you can define a maximum time limit beyond which usage becomes restricted:

- Without update: Scanning is prohibited after 7, 14, or 30 days (Hogo recommends a 7-day waiting period).

Once the time limit has expired, the scan function is automatically blocked to prevent the use of outdated antivirus databases.

8.2.2.3 On-Premise S3SRV Server (management and repository)

If you are using an internal platform for managing or distributing updates, you can enter the following settings:

- Address of the management server (if using a Hogo S3SRV management server)
- Secret Code (only in the case of management servers, provided by Hogo)
- Code IV (only in the case of management servers, provided by Hogo)
- Address of the repository server (if using a Hogo repository S3SRV)

These settings allow the workstation to authenticate and communicate with the S3SRV servers responsible for distributing updates or performing centralized management.

8.2.2.4 Automatic Updates

The screen allows you to enable or disable background updates:

- Enable or disable automatic updates
- Choose the automatic update time

These options allow you to schedule regular updates without manual intervention, ideally outside of the station's usage periods (night, evening...).

8.2.2.5 Heartbeat

You can also enable or disable the sending of a heartbeat, which allows the system to periodically report its presence or status to a monitoring infrastructure:

- Heartbeat: Enable or disable

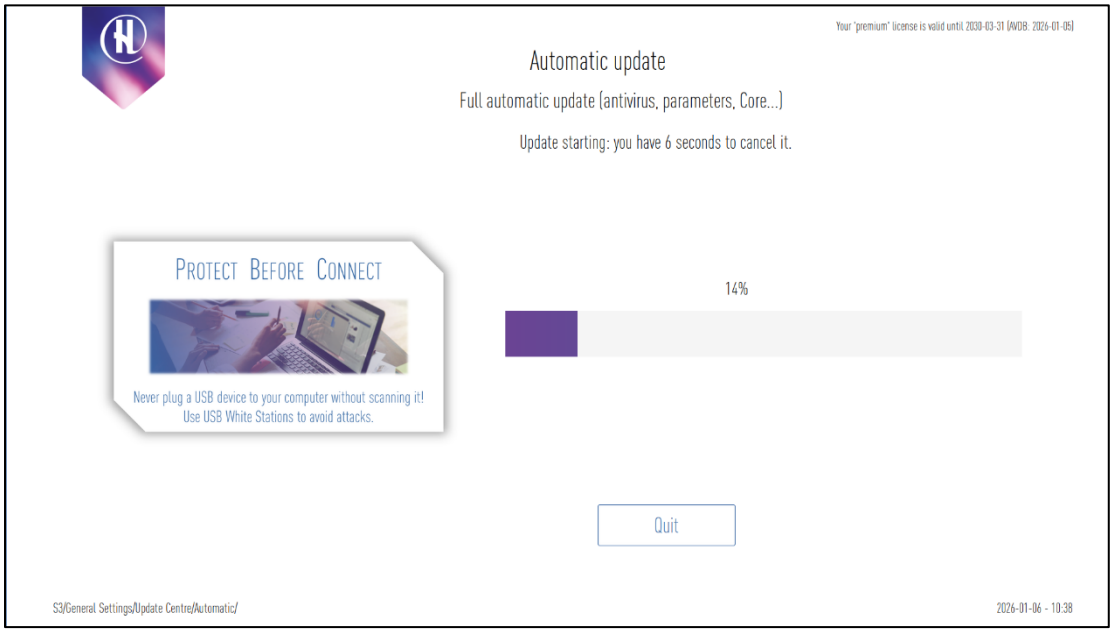
Note: The update "JIT" files must be placed in the root directory of the USB drive in case of an offline update.

8.2.3 Synchronize



Online synchronization, initiated manually or periodically, allows you to:

- Update the antivirus, update the Core
- Update the license (from an S3SRV only)
- Update the with station settings (from an S3SRV only)
- Synchronize the logs (with MyHogo, a S3SRV, and/or Syslog) and version information
- Synchronize the time via NTP (if enabled in the time settings)



The S3 white station will then need to be restarted for the new version to be operational.

When synchronization is started automatically (at the previously configured time), the restart is automatic. When synchronization is initiated manually, the restart must be triggered manually.

Note: When the automatic synchronization time is detected, the station will initiate synchronization on its own. If synchronization fails, the station may restart and retry, for example, to overcome temporary network connectivity issues. This cycle of attempts and restarts will end at the end of the configured automatic synchronization time.

8.3 Logs



The Log Access screen allows you to configure the management, storage, and export of the various logs generated by the system. This area centralizes all options related to log archiving, automatic export, and the transmission method to an external server.

The screenshot included in this chapter illustrates the available settings.



8.3.1 Log Retention Duration

You can define the period for which logs are kept in the system. Several durations are available:

- 6 months (typically suited to the strict GDPR requirements)
- 1 year (suitable for normal use cases)
- 3 years (adapted for use cases in sensitive, restricted, or II 901 related networks)
- 5 years (suitable for use cases in classified networks, or related to IG 1300)

This setting allows you to adjust the retention period according to your internal constraints, document policies, or compliance requirements.

8.3.2 Type of scan's log

You can choose the level of detail in the logs generated by the scans:

- Summary scan log
- Full scan log

This selection allows for a balance between the readability of the newspapers and the amount of information stored.

8.3.3 Scan results

When the system needs to transmit logs, you can choose the sending method:

- Send to server
- Do not send to the server

This setting allows you to enable or disable the automatic transmission of scan results to a central infrastructure.

8.3.4 Write a scan comment

You can specify whether a comment should be added before the analysis operations.:

No / Yes (Always) / Yes (ask user)

This setting allows you to adapt the documentation of operations according to your internal procedures.

8.3.5 Automatic export of scan's log

You can enable or disable automatic export of the scan log to the USB drive...

When this option is enabled, logs are automatically exported to the USB drive, without any manual action required regardless of the scan type.

8.3.6 Available stocks and options

The screen offers several buttons allowing you to access different logs or perform manual exports:

- Save: Saves the modified settings.
- Main S3 log: Opens the log associated with workstation activities.
- AV update log: Displays the antivirus update log.
- Core update log: Displays the system core update log.
- Export scan logs: Allows you to select the scan logs to export to a USB device.
- Export tech log: Exports system technical logs to a USB drive.
- Send logs: Manually sends logs to the configured server.
- Syslog parameters: Allows access to Syslog settings if a remote log server is used.
- Quit: Returns to the previous screen.

Note: Technical log exports are encrypted and readable only by the Hogo support team.

Note: If you experience any problems with your workstation, remember to export the "technical logs" and include them in your support request. [https://support.hogo.eu/].

8.4 Certificate Manager



The certificate manager allows you to view all known certificates of the S3 workstation, as well as add new ones or delete existing ones. This screen centralizes the management of certificates used for verifying the integrity and provenance of files in smart transfers.

In accordance with ANSSI recommendations (see RGS V2 – General Security Framework), certificates must meet the following requirements:

- For certificates expiring before 2030: minimum key size of 2048 bits.
- For certificates expiring after 2030: minimum key size of 3072 bits.

Hogo recommends, when possible, using 4096-bit certificates to enhance security.
You can use the following actions:

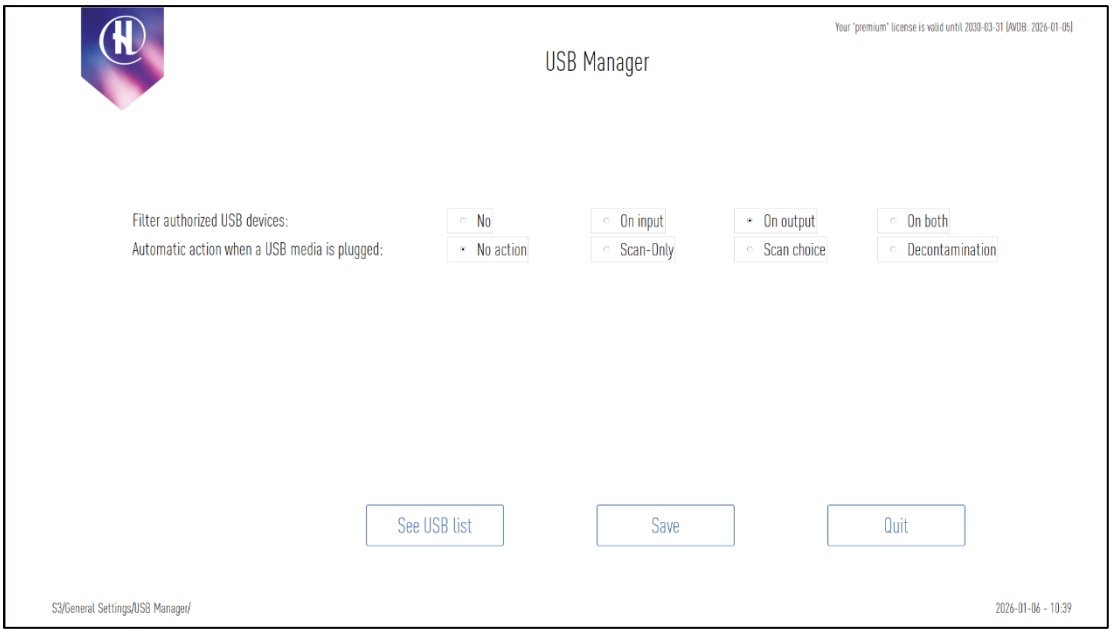
- Add: allows you to add a certificate to the S3 workstation. You must enter the certificate's internal name, its type, and the email address of the associated RECIPIENT. The certificate must be in .pgp format on a connected USB drive, and it must be the only file on that drive.
- Delete: Removes the currently selected certificate from the S3 white station.
- Quit: Returns to the previous screen.

These options allow you to maintain a set of certificates that complies with security recommendations while ensuring the proper functioning of the system's encrypted communications.

8.5 USB Manager



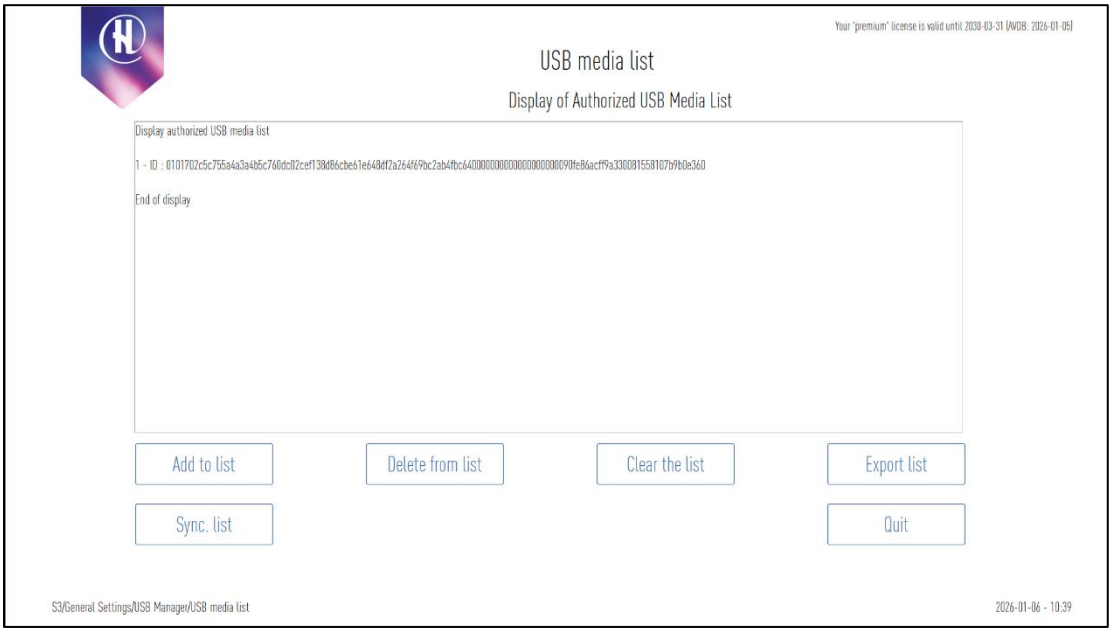
The USB manager allows you to manage the station's behavior with connected USB media, as well as manage the list of USB media authorized by the station.



Filter allowed USB media:

- No: All USB media devices are permitted to connect to the station.
- On input: Only authorized media can be connected for data transfer.
- On output: Only authorized media can be connected to the station for data retrieval via the transfer function.
- On both: Media are filtered for sending and retrieving data.

See USB list: Displaying the list of authorized media:



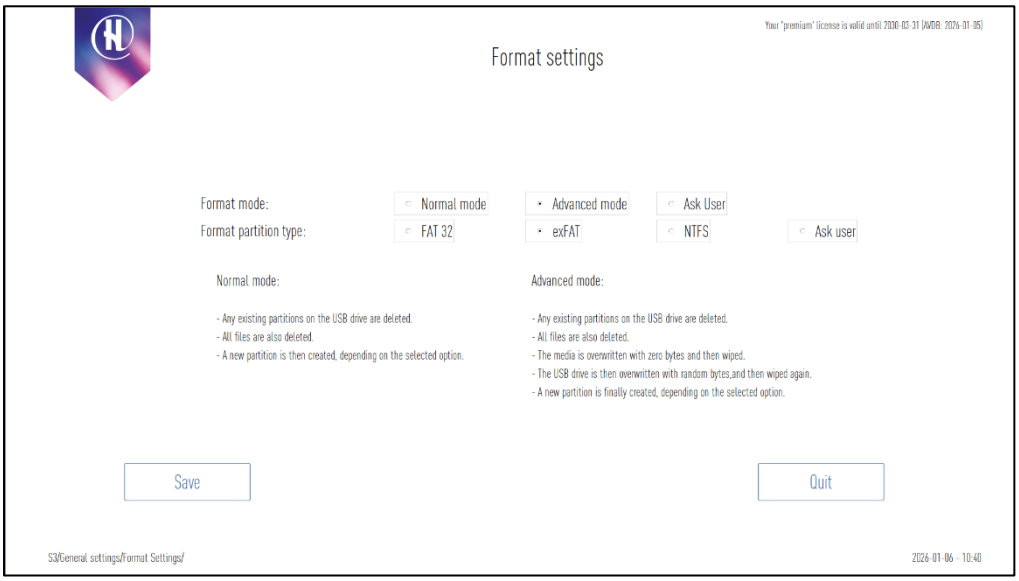
- Add to list: Adds the currently connected USB device to the list of allowed media.
- Delete from list: Removes the currently connected USB device from the list of allowed media.
- Cleat the list: Removes all media from the list of allowed USB devices at once.
- Export list: Exports the current list of allowed USB devices to a LIST file on the connected USB device.
- Sync. list: Imports a list of allowed USB devices in LIST format from a connected USB device.

8.6 Format settings



The Formatting Settings screen allows you to define how USB media will be formatted when formatted by the S3 workstation.

This section offers several operating modes and different partition types to suit the requirements of your technical environment.



8.6.1 Format mode

8.6.1.1 Normal Mode

In this mode, formatting is performed using a standard process. When you select this mode:

- Any partitions present on the media are deleted;
- All files on the media are deleted;
- A new partition is created according to the selected type.

This mode is recommended for common formatting operations.

8.6.1.2 Advanced Mode

Advanced mode applies a more thorough process to the USB media. During use:

- Existing partitions are deleted;
- All files are erased;
- The media is completely rewritten with zero-value bytes;
- The media is then rewritten with random bytes;
- A new partition is created according to the selected type.

This mode offers a more secure level of erasure, particularly suited to environments requiring enhanced destruction of residual data.

8.6.2 Partition type

You can choose the file system used during formatting from the following options:

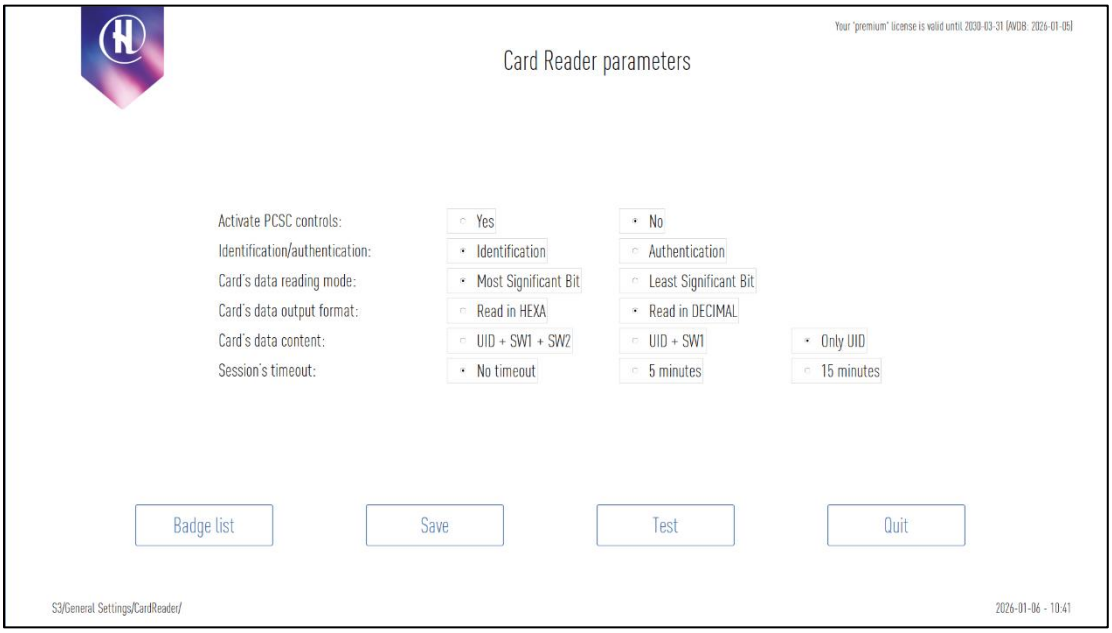
- FAT32
- exFAT
- NTFS
- Ask user (The system asks you for the desired partition type at each operation.)

The choice of partition type depends on your compatibility needs and your organization's policies.

8.7 Card reader parameters

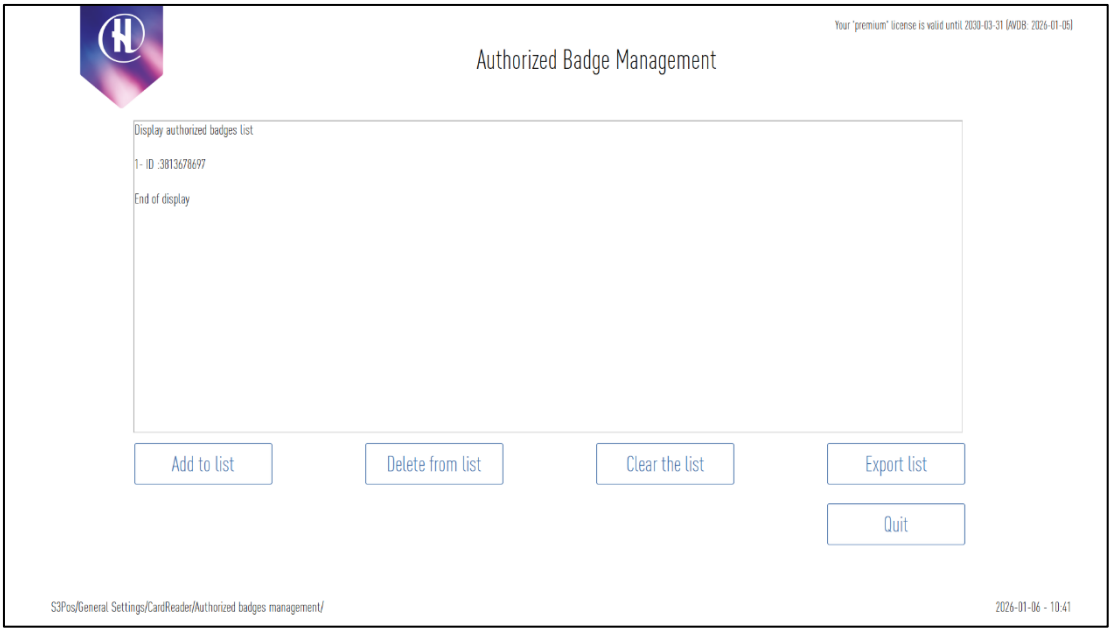


Badge reading settings allow you to adapt the badge reader to the expected level of security, compatibility, and use. Their configuration must always be consistent with the application system and operational requirements.



- Enable PCSC control: Before enabling PCSC control (no badge reading), ensure that at least one badge is on the list of authorized badges.
- Identification/Authentication:
    - Access to the station via Identification requires the use of a badge at startup. All badges are accepted.
    - Access to the station via Authentication requires the use of a badge registered on the list of authorized badges at station startup.
- Badge reading mode: Defines the reading order of the bits that make up the badge data.
- Read data format: Defines the display and transmission format of the read data.
- Content to read: Defines which badge information is transmitted after reading.
- Session expiration: This menu defines the validity period of a session, without any actions, after the badge is swiped on the reader.

Clicking on the Badge List displays:



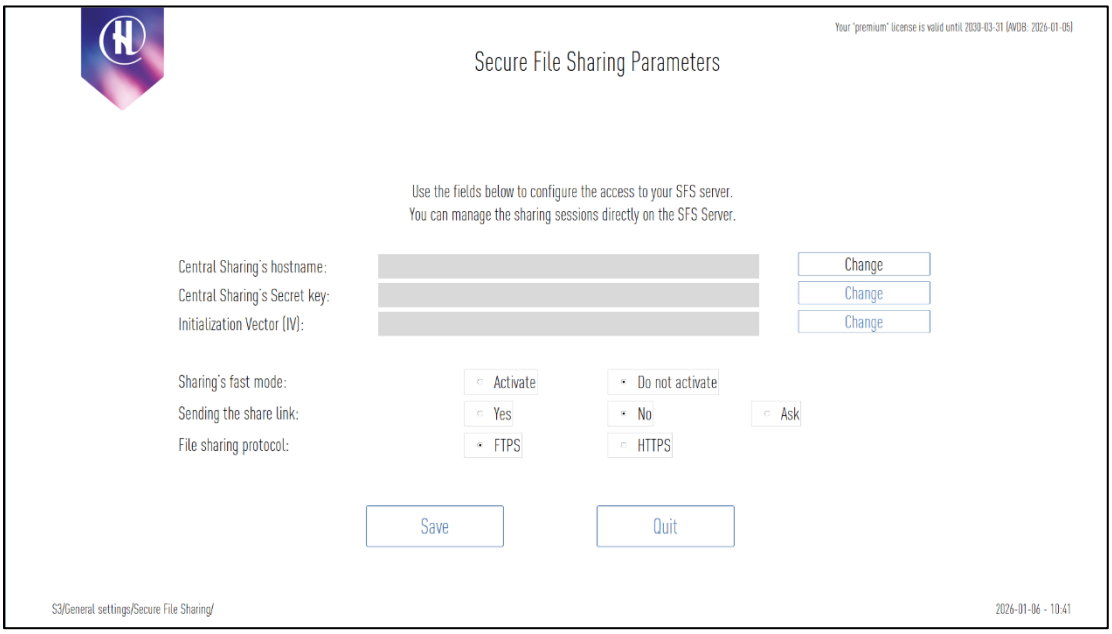
- Add to list: Adds the badge currently placed on the badge reader to the list of authorized badges.
- Delete from list: Removes the badge currently placed on the badge reader from the list of authorized badges.
- Clear the list: Delete all badges from the list of authorized badges at once.
- Export list: Allows you to export the current list of authorized badges to a LIST format file on a connected USB drive.

8.8 SFS settings



The File Sharing Settings screen allows you to configure the S3 workstation's access to your SFS server. This server is used for the secure management of sharing sessions, particularly for Smart Transfer or sending files to a shared space.

This screen displays all the authentication information and operating options necessary to establish secure communication between the workstation and the sharing server.



8.8.1 Secure file sharing parameters

To allow the station to connect to the SFS server, you must provide the following information:

- Central sharing's hostname: Address or DNS name of the SFS server to which the station must connect.
- Central sharing's secret key: Authentication key used to establish a secure session with the sharing server.
- Initialization Vector (IV): Encryption parameter required for the secure exchange protocol. This parameter must match the values configured on your S3SRV.

The fields can be modified individually using the "Edit" buttons located to the right of each line, after administrator authentication.

8.8.2 Operating Options

Several parameters allow you to adapt the sharing behavior according to your environment:

8.8.2.1 Sharing's "fast" mode

When this mode is enabled, the workstation uses a simplified and accelerated transfer method to send files to the server. This mode is useful for environments where speed is more important than advanced features; in this case, the workstation will display randomly generated identifiers.

8.8.2.2 Sending the share link

This setting determines whether the station should automatically send a link to access the shared files.

The Request mode prompts you to confirm sending each time you share.

Note: Sending the sharing link requires version 2.4 of S3SRV.

8.8.2.3 File sharing protocol

You can choose the secure protocol used for communication with the SFS server.

The choice depends on your infrastructure and current security policies:

- FTPS mode is typically used for "custom" or "non-S3SRV" file sharing servers, or when using Hogo S3SRV servers with a version lower than v2.4. This mode is considered "Legacy" by Hogo.
- HTTPS mode is the current standard mode for the "S3 Station – S3SRV Server" pair. It limits the data flows that need to be opened between the station and the server and improves the security and speed of SFS file transfers.

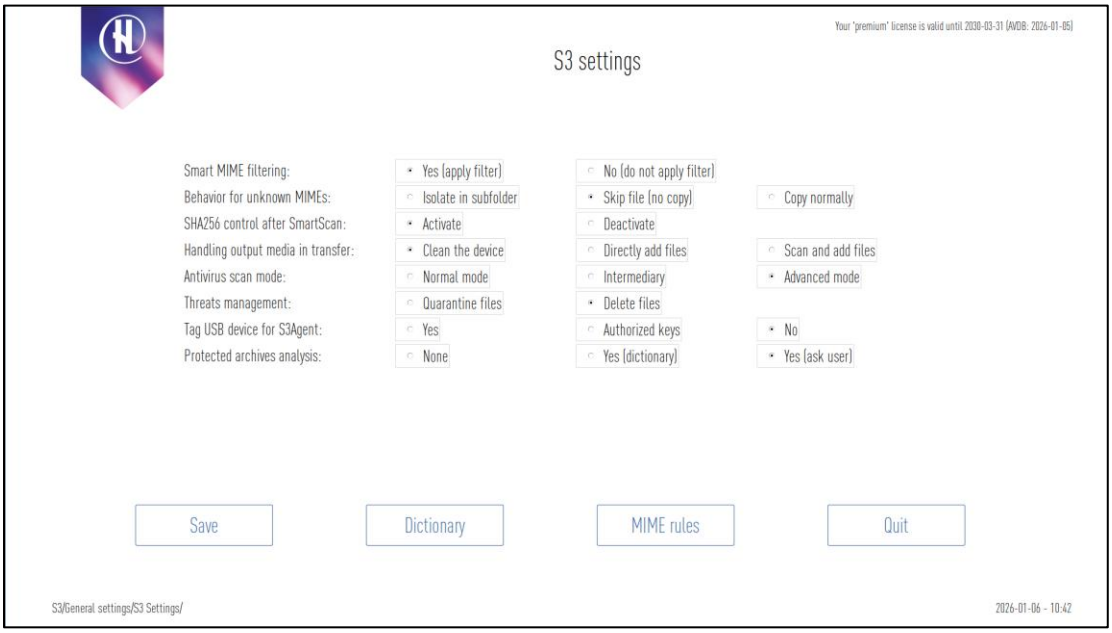
8.9 Scan settings



The S3 Settings screen allows you to define the behavior of the S3 white station when analyzing USB media.

This area groups together all the parameters that influence the detection level, the management of analyzed files, threat handling, and the production of the output media.

These settings must be adapted to your organization's security requirements and applicable internal policies.



This screen allows you to configure the following elements:

8.9.1 Scan mode

You can select the analysis mode applied when scanning the USB media. Depending on your configuration, several levels are available:

- Normal: standard analysis, suitable for most low-sensitivity environments.
- Intermediary: activates additional controls, ideal in most office and industrial cases.
- Advanced: activates all available functions for in-depth analysis, perfect in a sensitive context.

The choice of mode depends on the desired compromise between depth of analysis and processing time.

8.9.2 MIME filtering

Smart MIME filtering allows you to check the actual MIME type of files (based on extensions, but also MIME Magic Numbers to detect inconsistencies between the displayed extension and the actual content).

You can:

- Yes (filter): enable MIME filtering.
- No (do not filter): disable this control.

This mechanism makes it possible to identify potentially corrupted files.

8.9.3 Behavior for unknown MIMEs

Defines the action applied when a file has an unknown MIME type or one that does not conform to your dictionary:

- Isolate (in subfolder): moves the file to an isolated folder on the output media.
- Skip file (no copy): the file is not copied to the output media.
- Copy normally: the file is copied normally

This setting strengthens protection against unusual or suspicious files.

8.9.4 SHA256 control

Enables or disables the calculation of the SHA256 hash for each analyzed file:

- Enable: The SHA256 value is calculated and recorded in the scan log.
- Disable: The SHA256 value is calculated but not written to the scan log.

This control improves traceability and post-incident analysis.

8.9.5 Warnings management

When a file is identified as a warning, the station can apply one of the following actions:

- Ignore: The warning is not displayed to the user.
- Report: Warnings are recorded in the scan logs and displayed through pop-up notifications.
- Delete: Warnings are treated as threats and displayed to the user for educational purposes.

The chosen action should reflect your organization's security policy and the expected level of control. See Appendix 2

8.9.6 Threats management

When a file is identified as a threat, the workstation can apply one of the following actions:

- Quarantine files: The file is isolated in a password-protected ZIP folder.
- Delete files: the file is deleted from the analyzed media.

The chosen action should reflect your organization's security policy and the expected level of control.

Note: The password for the quarantined ZIP file is displayed in the post-analysis pop-up. It is imperative to keep it in a safe place, ideally in a digital vault, as it cannot be recovered by the support team if lost.

8.9.7 Handling output media in transfer

Determines how the station prepares the output USB media:

- Clean the device: It erases the media's contents before copying the analyzed files. (This is the option recommended by HOGO)
- Directly add files: preserves the existing content and adds the output files (in this case, the token for the S3 agent is not affixed to the USB media)
- Scan and add files: classic copy according to the defined policy

8.9.8 Tag USB device for S3Agent

Indicates whether the station should affix a specific marker to the output USB media:

- Yes: The S3Agent tag is added to the media.
- Authorized keys: The S3Agent tag is added only to authorized media in the white station list.
- No: No tag is applied.

8.9.9 Protected archives analysis

Defines how the station manages password-protected archives:

- None: protected archives are not processed.
- Yes (Ask): The station requests the password corresponding to the user.
- Yes (dictionary): The station uses a password dictionary to analyze the archives.

8.9.10 Available Actions

- Save: saves the configured settings.
- Dictionary: opens the management of passwords used for analyzing protected archives.
- MIME rules: allows you to consult the MIME dictionary.
- Quit: returns to the previous screen without saving.

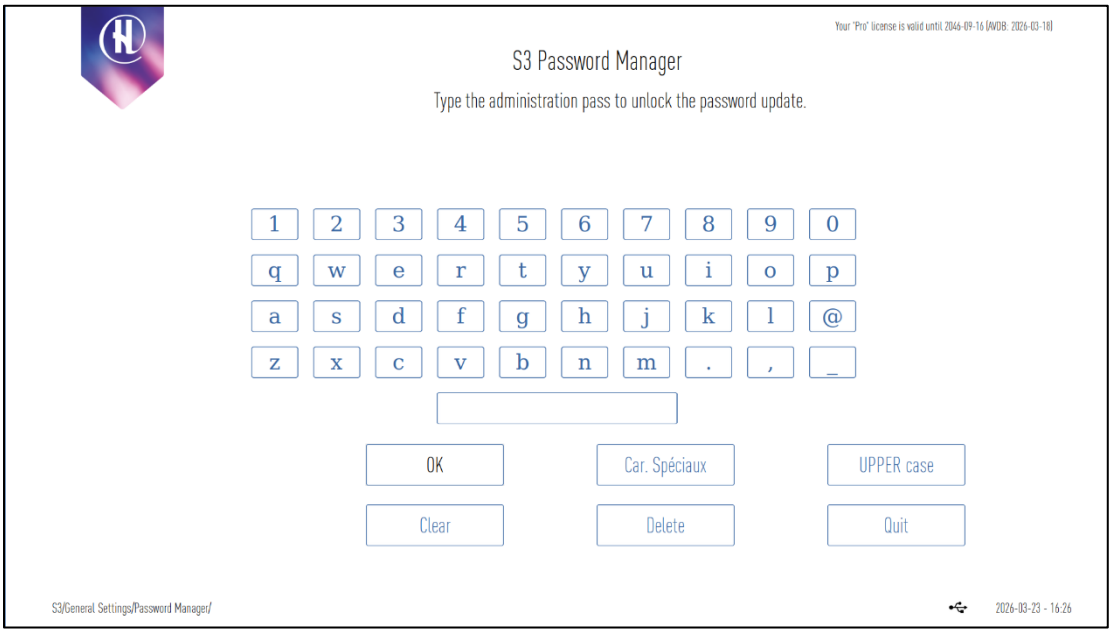
8.10 Password Change



The "Change Password" menu allows the administrator to change the access credentials for the setting in order to ensure the confidentiality and security of the station.

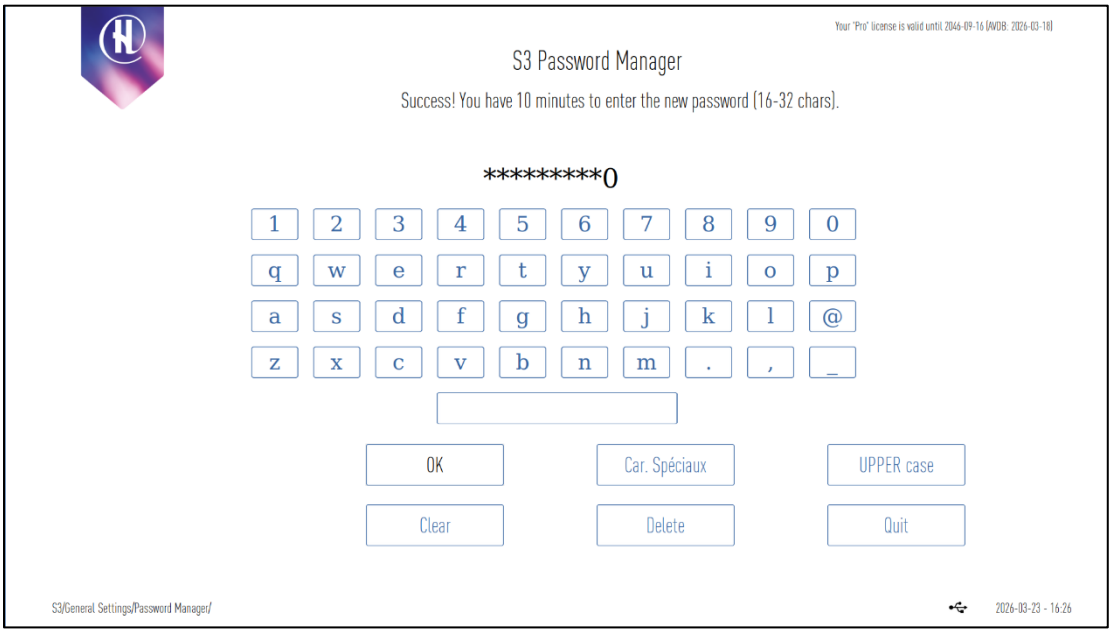
This feature is essential to prevent unauthorized access and ensure management complies with best security practices.

The administrator password must be between 16 and 32 characters long, chosen from the Hogo keyboard characters (10 numeric digits, the 26 letters of the alphabet in lowercase or uppercase, and 25 specials, accented, or punctuation characters). It must contain at least one lowercase letter, one uppercase letter, and one number...



Regarding this renewal, Hogo's recommendations are as follows:

- Hogo recommends changing the password every 6 months to a maximum of 2 years, depending on the sensitivity of the information system using the clean workstation;
- Hogo recommends not reusing passwords that have already been used.



Note: If you lose your password for accessing the settings, remote recovery will not be possible. Returning the station to customer service is mandatory and is not covered by the Hogo warranty.

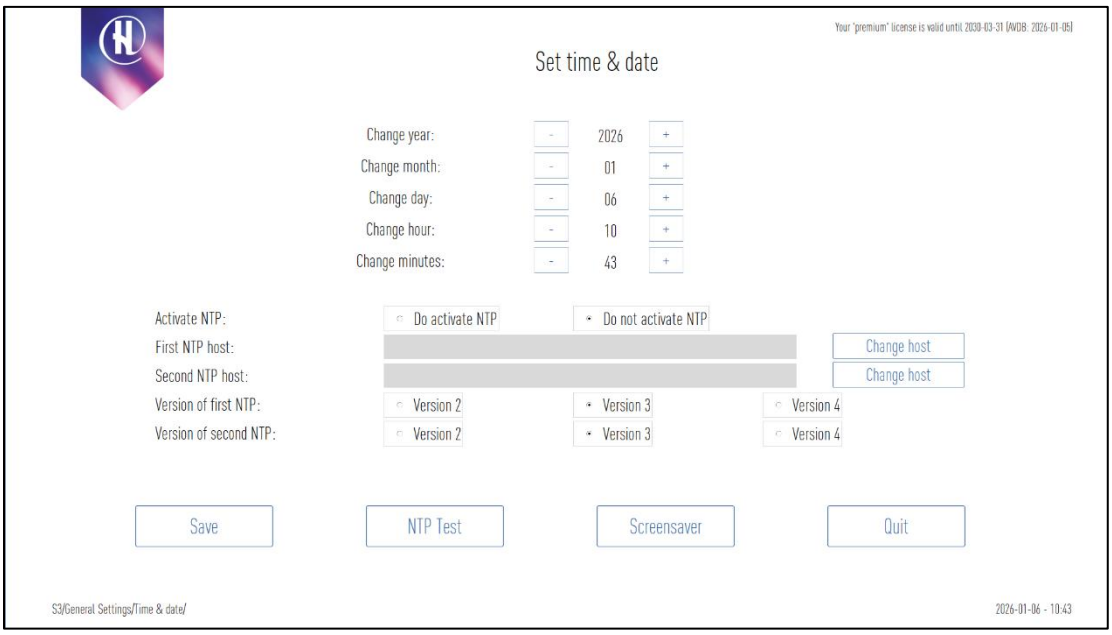
Note: The station's initial password is "1234567890"; it is important to change it upon first use.

8.11 Date and hour



The Date and Time screen allows you to configure the time information for the S3 white station.

A properly set clock is essential for the correct operation of many features, including log management, update synchronization, certificate validation, and consistency of operations performed on USB media.



This screen allows you to define or correct the following elements:

- The system date
- The system hour
- Any NTP servers used by the station (whether activated or not, host or IP address of the two servers, NTP protocol versions))

You can modify each of these settings after administrator authentication.

An incorrect time or date can lead to:

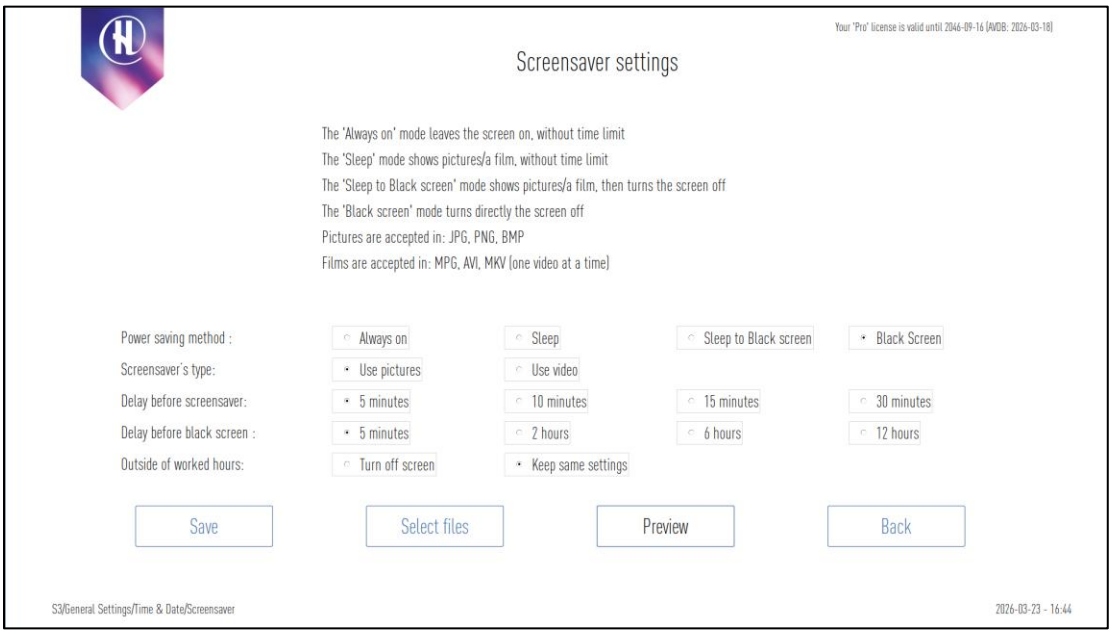
- Inconsistencies in scan logs and technical logs,
- Difficulties in tracing security events,
- Possible rejection of certain certificates if their validity period appears incorrect,
- Errors in external systems that depend on a precise timestamp.

Depending on your organization's policies, you can make these adjustments manually or rely on external synchronization. In a completely disconnected environment, it is particularly important to regularly ensure that the system clock remains synchronized.

Once you have made your adjustments, select the Save button to apply your changes, or Exit to return to the previous screen without saving the changes.

8.11.1 Screensaver

This button provides access to the station's screensaver settings.



- Suspend system's mode: Allows you to choose the station's behavior after a given period of inactivity.
- Screensaver's type: Allows you to choose the type of screensaver used by the station after a period of inactivity. Displaying a video (MPEG codec and duration < 2 minutes recommended) or a slideshow of images (12 maximum).
- Delay before screensaver: Allows you to choose the required period of inactivity before the power saver starts.
- Delay before hibernation: Allows you to choose the required time-saving mode before the station goes into standby (black screen).
- Outside of worked hours: Station behavior outside of working hours (between 7pm and 7am)

9 Initial Update

The initial update is a mandatory step before the first operational use of your S3 clean workstation. It installs all the components necessary for the workstation to function correctly: analysis engines activated in your configuration, signature databases, S3 Core modules, and essential security settings.

Before proceeding with this update, you must first configure the station.

Two options are available to you:

- Manual configuration: You enter the various network settings and update sources yourself.
- Configuration via the Wizard: a guided setup assistant that asks you a series of simple questions to make the necessary adjustments (network, source of updates, basic settings).

The choice between manual or guided configuration depends on your preferences or your organization's policy. In both cases, you must configure the network settings and update parameters before starting the initial update.

Once the network configuration is established or the update media is prepared, it is recommended to launch an initial update to:

- Verify that the analysis engines enabled in your configuration are properly installed and functional;
- Update the signature databases and Core components;
- Synchronize the necessary settings with your internal S3SRV server, if you are using an On-Premise deployment;
- Ensure complete consistency between the factory configuration and your production environment.

While a scan can technically be performed without an initial update, it is not recommended to analyze a USB drive until the workstation has been verified and harmonized with your infrastructure. An initial update is therefore an essential best practice, enhancing the reliability of detections and equipment compliance.

Once the initial update has been completed, it is recommended to perform a functional test to confirm that the station is fully operational before regular use (see next chapter).

10 Functional Tests

After the initial installation and update of your S3 clean station, it is recommended to perform a functional test to verify that the equipment is correctly configured and fully operational.

This test validates the main system components: user interface, antivirus detection, Core operation, and USB media management.

To perform this test, you can use a USB control medium (containing, for example, a secure test file such as an EICAR file, see below). Since the S3 white station has several USB ports, it is advisable to test each port to confirm the proper hardware functionality of all connections.

For each USB port tested, check that:

- The media is correctly detected by the station;
- The scan starts and proceeds normally;
- The files are analyzed according to the defined settings (analysis engines, MIME filtering, SHA256 checking, etc.);
- Potential testing threats are correctly identified and dealt with according to the defined policy (deletion, quarantine, isolation, etc.);

Following the analysis, you can consult the scan logs to confirm that all modules functioned as expected and that no anomalies were detected.

This simple test ensures that the S3 white station is ready and meets the required safety standards..

Note: To perform antivirus detection tests, you can use the EICAR test file, which is specifically designed to verify the proper functioning of scanning engines without posing any risk to your system.

This file is recognized as a threat by most antivirus programs, which confirms that the S3 white station is responding correctly. You can download it from the official website: https://www.eicar.org/download-anti-malware-testfile

This file is available in several formats (text, simulated executable, ZIP files) in order to test different detection scenarios.

11 S3Core Rescue mode

The Rescue screen is a screen that appears when a startup issue occurs.



When this screen appears:

- Plug a USB media into your station
- Select "Export data for Tech Support"
- Create a support ticket and attach your export https://support.hogo.eu
- Follow the support team's instructions

Note: Using "Restore factory Core configuration" will permanently delete all data stored on your station and will require you to contact support to restore it to working order. Your data cannot be recovered. This mode should not be used without an explicit request from the support team.

12 Additional warnings

To ensure safe and compliant operation of the S3 clean station, please observe the following points:

- ➔ Only use USB drives that are in good condition and without physical defects.
- ➔ Never insert damaged, wet, or deformed media into the station.
- ➔ Do not remove a USB drive during scanning, copying, or formatting.
- ➔ Regularly check that the station has recent versions of the analysis engines.
- ➔ Perform an initial update before the first operational use.
- ➔ Enable automatic updates when internal policies allow it.
- ➔ For offline environments, update regularly via USB drive, export logs, and check the station's date and time (once a week).
- ➔ Keep the administrator password in a safe place (such as a digital safe); losing it will require a return for repair not covered by the warranty.
- ➔ Change the administrator password periodically in accordance with your internal rules.
- ➔ Never share administrative credentials with unauthorized personnel.
- ➔ If you are using PCSC control, add the authorized badges before activation.
- ➔ Never turn off the station during formatting, scanning, or updating.
- ➔ Use advanced formatting mode only if a thorough erasure is required.
- ➔ Ensure that the network settings (IP, DNS, gateway...) are correct before enabling a network update.
- ➔ Only use the proxy settings provided by your IT department.
- ➔ Be careful not to obstruct the station's ventilation openings.
- ➔ Regularly perform a functional test (EICAR, USB ports, update).
- ➔ Check the logs in case of unusual behavior.
- ➔ Periodically export the technical logs for archiving or diagnostic purposes.

In case of doubt or incident, remember to export the "technical logs" and include them in your support request:

https://support.hogo.eu

Appendix 1 – Setup Wizard Workflow

1. Update method:

- Local (USB) ⟶ Direct access to the configuration summary.
- LAN (local network) ⟶ Proceed to server type selection.
- Cloud ⟶ Continue to the automatic update configuration.

2. Server type selection (LAN only)

- Management Server
  - Enter the address or name of the Management Server.
  - Enter the secret code (management).
  - Enter Code IV.
- Repository Server
  - Enter the address or name of the repository server.

➔ Continue to the automatic update configuration

3. Automatic updates

- Yes
  - Enter the time for the automatic update (value between 0 and 23).
- No

➔ Continue to the network connection type.

4. Network connection type

- Cable (RJ45)
- Wi-Fi
  - Enter the Wi-Fi network SSID.
  - Indicate whether the Wi-Fi network is hidden (Yes / No).
  - Configuring Wi-Fi security:
    - Enter the password
    - No password (open network)

➔ Continuation to IP addressing mode.

5. IP Addressing Mode

- DHCP (automatic)
- Static (fixed IP)
    - Enter the static IP address.
    - Enter the mask in CIDR format (value between 0 and 32).
    - Enter the gateway address.

➔ Continue to DNS configuration.

6. DNS Configuration

- Automatic (DHCP / gateway)
- Manual
    - Enter the DNS server address (IPv4).

➔ Continue to the configuration summary.

7. Configuration summary

- The system displays a complete summary of the configuration.
- The administrator validates the configuration by selecting OK, which completes the procedure.

Appendix 2 – Bookmarks colors definition

