# Hogo S3
# User Manual v3.5

2024

Version V1.8 (since build 2023090101) and 1.9 (since build 2024010101)

This document describes how to use the main functions of the Hogo S3 range and provides guidance to users. It follows along with the product's GUI and focuses on the user experience.

# Table of contents

1 Introduction ..... 2
1.1 Functions of the S3 range ..... 2
1.2 Installation of the equipment ..... 3
2 Main Interface – Home ..... 5
2.1 Terms of use ..... 5
2.2 Main screen ..... 6
2.3 Language settings ..... 6
3 S3 Tools ..... 7
3.1 “Tools” screen ..... 7
3.2 Smart-Transfer ..... 8
3.3 Selecting files to scan ..... 11
3.4 Scan Only and Decontamination ..... 11
3.5 Scan with file sharing ..... 11
3.6 File sharing synchronization ..... 12
3.7 Scan with Security Certificate ..... 12
3.8 Scan my phone ..... 12
3.9 Formatting a USB key ..... 13
4 General Settings ..... 14
4.1 Tool settings ..... 15
4.2 Update ..... 19
4.3 Login screen – Administrator functions ..... 23
4.4 Set time and date ..... 23
4.5 Screensaver ..... 24
4.6 Logs ..... 24

# 1 Introduction

## 1.1 Functions of the S3 range

The "S3" Smart Secure Sanitizer range is a USB White Station solution that protects your sensitive Information System from infected USB devices:

- Protect your information system from contaminated or dangerous devices.
- Import data into your sensitive system without directly connecting the device.
- Scan and filter your input data (with up to 5 antivirus and MIME and PGP checks, etc.).
- Use only keys provided from the company's authorized stock—filter keys by serial number.
- Avoid any data leaks or unauthorized inflow of data to your system.

There are three white stations in this range:

- S3Box: rugged, portable and impact-resistant tablet.
- S3Pos: single-unit station that can be set on a desk or other surface.
- S3Tot: standalone station.



S3Box



S3Pos




S3Tot

This document describes how to use the main functions of the S3 range and provides guidance to users. It follows along with the product's GUI and focuses on the user experience and not on the underlying mechanisms.

Please note: The screenshots below are taken from an S3Box interface, but the three solutions in the S3 range share the same interface layout.

## 1.2 Installation of the equipment

### 1.2.1 Physical Characteristics of the Equipment

The S3 series equipment covered by this manual requires a power source to operate. The characteristics of this power source are as follows:

- S3Box: Connect the charger provided with the station to an electrical outlet (230V AC at 50Hz) to provide an output of 5V DC.
- S3Pos: Connect the transformer provided with the station to an electrical outlet (230V AC at 50Hz) to provide an output of 19V DC.
- S3Tot: Only connect the cable at the back of the totem to an electrical outlet (230V AC at 50Hz).

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

- S3Box: 5 Watts (at rest) to 12 Watts (in operation, typically during USB media scanning)
- S3Pos: 20 Watts (at rest) to 90 Watts (in operation, typically during USB media scanning)
- S3Tot: 30 Watts (at rest) to 110 Watts (in operation, typically during USB media scanning)

Finally, the internal operating temperature of these three devices must be between 0°C and 50°C at all times.

### 1.2.2 Setting Up the Equipment

To install S3 series equipment, follow these instructions:

1. Preparing the Location
- Choose a clean, clear space suitable for the size/number of devices to be installed.
- Select a stable and non-static surface to prevent electrical damage to the equipment.

2. Unpacking the Equipment
- Carefully remove the S3 device from its transport box and place it on the designated surface.
- If additional external peripherals are required (e.g., a printer, a badge reader), connect them to the appropriate ports.

3. Electrical Power
- Connect the charger provided with the S3Box, or the transformer provided with the S3Pos, to its port on the S3 device (skip this step for the S3Tot).
- Plug the power cable into the back of the S3Tot, or the other end of the charger or transformer, into an electrical outlet with a grounding plug.

4. Powering On
- Press the "power" button on the S3Box or flip the rear switch on the S3Pos to start it (no action is needed for the S3Tot, which will start when plugged in).
- Follow any on-screen instructions for initial setup (devices are usually pre-configured, but questions may appear on the first start-up).

### 1.2.3 Safety Instructions

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 does not seem to fit naturally, do not force it. Check that you are using the correct port or cable.

- Electrical Power:
  Always use a power cable in good condition. Avoid using damaged or frayed cables.

- Keep Liquids Away:
  Avoid placing drinks or other liquids near your S3 equipment to prevent spills.

- Ventilation:
  Ensure the equipment is placed in a well-ventilated area. Avoid blocking ventilation openings to prevent overheating.

- Updates and Maintenance:
  To ensure the safety and performance of your equipment, regularly perform software updates and check its cleanliness (e.g., dust removal).

### 1.2.4 Additional Warnings

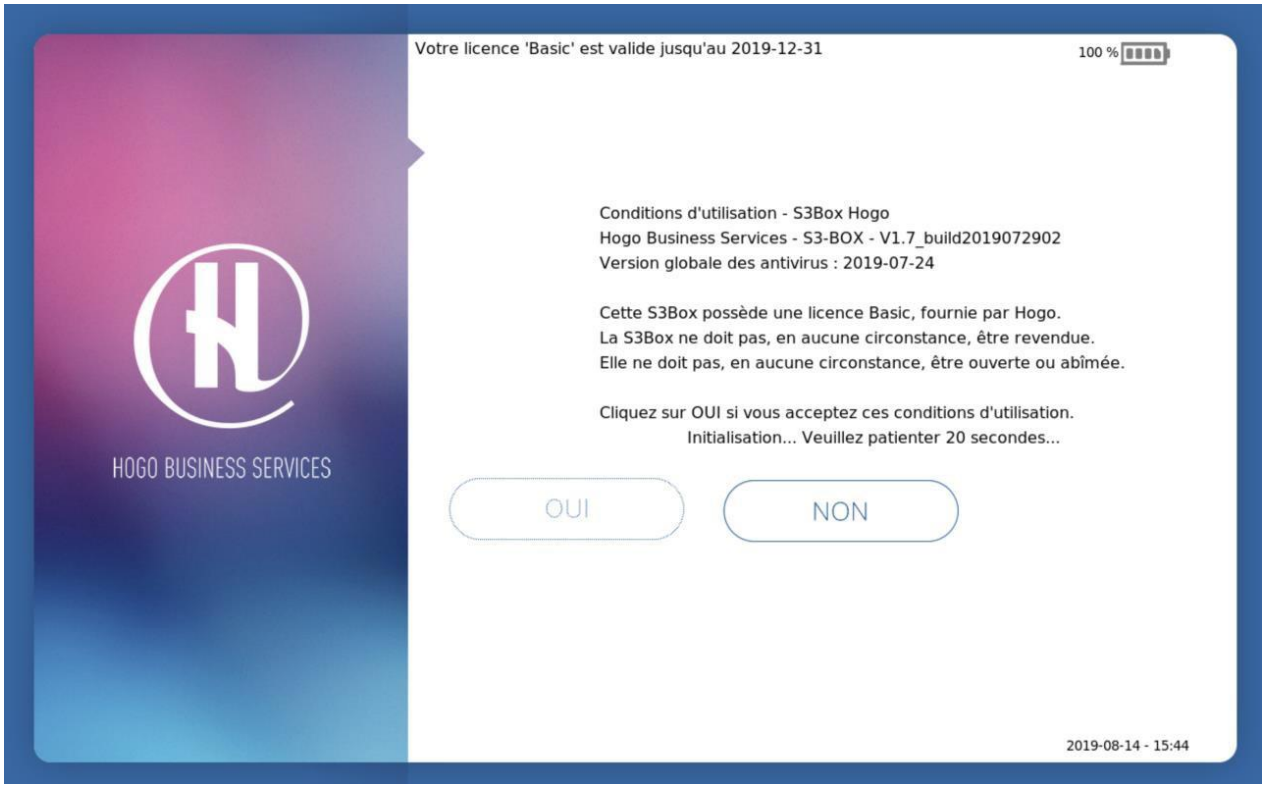
Warning: S3 series equipment is not suitable for use in places accessible to children.

Warning: the power cord of the equipment serves as its electrical disconnection device; it must be easily accessible to operators at all times.

# 2 Main Interface – Home

## 2.1 Terms of use

The "Terms of use" are displayed when the S3 range stations start up:



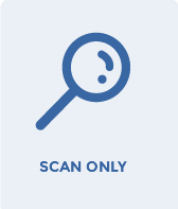

Click "Yes" to agree to these terms of use.

*Please note:* Choosing "No" will bring up a prompt for the administrator password and will turn off the S3 white station.

Note: The S3 stations have a mechanism for detecting and signaling "badUSB" peripherals. This signaling only starts upon displaying this disclaimer. If such a peripheral is already connected beforehand, it will not generate a warning popup: it is advisable to check the peripherals connected to the station at startup.

## 2.2 Main screen

Once the terms of use have been accepted, the main screen will appear, with the following buttons:

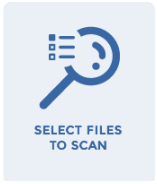
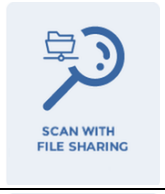
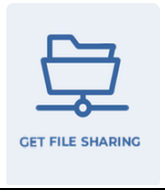
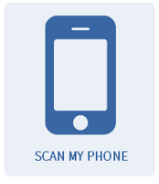
| | |
|---|---|
|  | This button starts the Smart-Transfer function, which will run antivirus scans and perform advanced filtering (MIME type, USB key, etc.) on the input files before transferring them to the output key.<br>This function is explained in detail in Chapter 3.2.<br>Please note: The USB key must be inserted *before* starting the function. |
|  | This button starts the Scan-Only function. This function will run antivirus scans without the advanced filtering functions or file transfer.<br>This function is explained in detail in Chapter 3.4.<br>Please note: The USB key must be inserted *before* starting the function. |
|  | This button starts the Scan function with Decontamination. This function will run antivirus scans without the advanced filtering functions or file transfer.<br>This function is explained in detail in Chapter 3.4.<br>Please note: The USB key must be inserted *before* starting the function. |
| [More Tools] | This button provides access to the SCAN/TRANSFER functions and USB tools; see Chapter 3 for more information. |
| [Settings] | This button provides access to the setup and update functions; see Chapter 4 for more information. |
| [Help] | This button displays help information on the main functions of the S3 white station. |
| [Reboot] | This button restarts the S3 white station. |
| [Shutdown] | This button turns off the S3 white station. |

## 2.3 Language settings

This window allows users to change the language used by the S3 white station.
Pressing on any flag will restart your S3 white station's interface in the selected language. This language selection is saved in memory so that it will also be active on future reboots.

# 3 S3 Tools

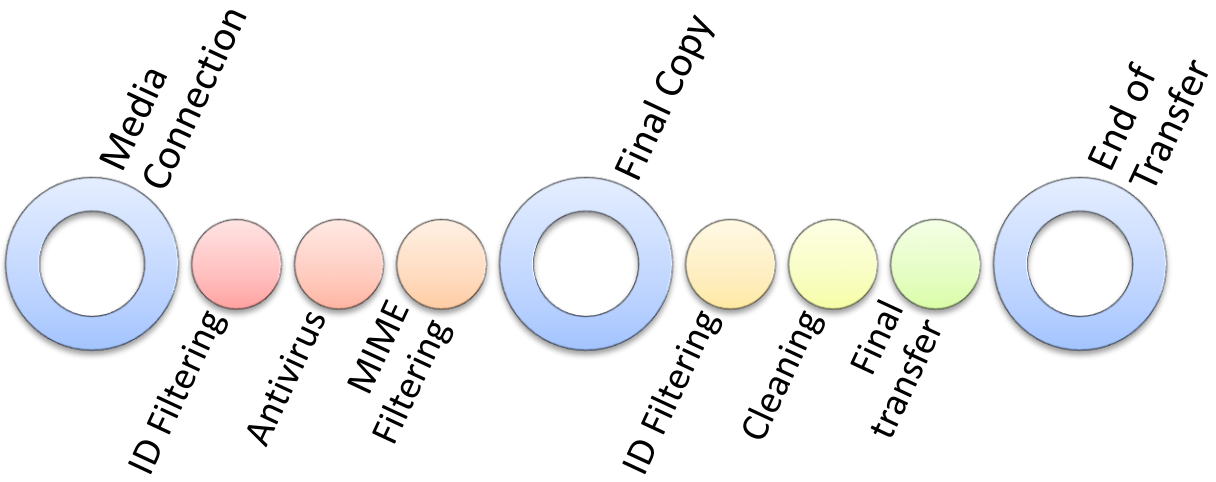
## 3.1 "Tools" screen

| | |
|---|---|
|  | This button launches the Smart-Transfer function and allows users to select which files to scan. This function is explained in detail in Chapter 3.3.<br>Please note: The USB key must be inserted *before* starting the function. |
|  | This button starts the Scan function with Decontamination. This function will run antivirus scans without the advanced filtering functions or file transfer.<br>This function is explained in detail in Chapter 3.4.<br>Please note: The USB key must be inserted *before* starting the function. |
|  | This button launches the Smart-Transfer function and allows files to be shared over the network when the scan finishes, instead of requiring an output USB key.<br><br>Please note: The USB key must be inserted *before* starting the function. |
|  | This button launches the Smart-Transfer function, but allows users to retrieve files via network sharing, before requesting an output USB key. |
|  | This button launches the Smart-Transfer function, but allows users to select files to be scanned and certificates to use to verify their signatures.<br><br>Please note: The USB key must be inserted *before* starting the function. |
|  | This button launches the Scan function (scan only, quick) which will perform antivirus scans—without the advanced filtering functions or file transfer—on a connected Android phone. |
|  | The "Format" function allows users to format a USB key.<br><br>Please note: The USB key must be inserted *before* starting the function. |
| [Home] | This button returns users to the main screen of the S3 white station, see Chapter 0. |

## 3.2 Smart-Transfer

### 3.2.1 General operation

This scan function runs an antivirus scan on the input files, filters the files according to the S3 white station's settings and outputs the files to external media.




The first step is to retrieve the files from a USB key and then process them:

- First, the scan verifies that an input USB key is connected.
    - If not or if the input USB device control option is enabled and the connected device is not authorized, the function stops.
- Next, the S3 white station is prepared (internal and file checks) for scanning, then:
    - The installed antivirus engine(s) validate(s) the files.
    - Files are filtered (if the corresponding option is activated) according to the MIME type rules saved.
- Finally, the files are copied to a specific directory in the S3 white station, and the GUI informs the user that they can remove the input USB key and insert the output USB key.

The second step is to return the processed files to an output USB key:

- After activating the "End of Transfer" button, the function checks that an output key is connected.
    - If not or if the input USB device control option is enabled and the connected device is not authorized, the function stops.
- Next, the output USB key is checked (free space, etc.), the files are copied onto it and the files present on the white station are deleted (no data persistence).
- Finally, the user is notified that the transfer is complete and that they can remove the output USB key and quit the Smart-Transfer function.

### 3.2.2 User notification

A popup will warn the user that a USB key must be connected before the scan procedure can start. A final popup will give the user the summarized processing information

At the end of the procedure, the user can open a "Log" window to view the results of the scan. It contains a summary of the scan settings (date and time, serial no. of the input key used, etc.) and the actions performed (file processing, antivirus engine verdict, etc.).

This log can be viewed only after the scan is done or later on a MyHogo management console (stations connected to the Internet or to a local Hogo server). Like all logs, they can also be exported via Syslog (see 4.5.2) or to a USB key in encrypted/signed files (see 4.5).

Please note: When displayed on the screen, this log can be shortened if it contains too many lines, so the display is readable. The scan summary is always displayed, and the full content remains accessible on the management console or Syslog well.

### 3.2.3 Details about the operation

Switching USB keys between data input and data output is mandatory (the same key cannot be used for both input and output).

Filtering by MIME type does not take into account files hidden with Steganography (see hereafter).

The use of the white station's hard disk as a jump zone implies a limit on the size of the files that can be transferred: users cannot transfer an amount of data that exceeds the space available on the station at the time of the Smart Transfer.

Not all partitions are case sensitive: some files may be overwritten on the output key if they have identical names in case insensitive media (file.txt vs. FILE.txt).

Some file systems do not support all file sizes: e.g. 4 GB limit for the FAT32[1] system. The station will prohibit transfers to this type of key if there are files that are too large. It is also possible that some files will be lost in the final copy.

Not all file systems handle permissions in the same way: to avoid post Smart Transfer compatibility problems, the rights of the files on the output key are therefore set to the equivalent of the Linux 777 code.

[1] Due to the obsolescence of earlier formats such as FAT16, there is no differentiation: this means there is a risk of data loss when used in this case. Hogo strongly recommends against using these key formats unless the input key is in the same partition format.

### 3.2.4 Usage Warnings

#### 3.2.4.1 Handling Polyglot Files

A polyglot file is designed to be interpreted as multiple different types of files depending on the context, allowing it to masquerade as a harmless file type while potentially hiding malicious code.

These files can bypass MIME-type-based filtering mechanisms and sometimes evade detection by antivirus engines.

The Smart-Transfer function may not detect polyglot files, so Hogo recommends paying particular attention to files that might harbor this type of masking: GIF (polyglot GIFAR), JPG (polyglot JPG+PHP), video (polyglot MP4+JS), etc.

#### 3.2.4.2 Handling Steganography Masking

Steganography is a technique that allows information (such as text or code) to be hidden inside other files, such as images or audio files, in a way that makes the presence of the hidden information undetectable.

This technique can be used to conceal malicious or sensitive data, making these files potentially dangerous while appearing harmless.

The Smart-Transfer function may not detect steganography masking, so Hogo recommends paying particular attention to files that might harbor this type of masking: images, audio files, etc.

## 3.3 Selecting files to scan

The "File selection" function will display the files available on the connected USB key in a navigable area on the left-hand side of the screen:

- By double-clicking on the screen, the user will be able to add inputs to the list of files to be scanned on the right-hand side of the screen.
- The "Add directly" button allows users to select a file or folder without double-clicking (single click).
- Finally, by double-clicking on an item in the right-hand list, the user can delete an item from the selection list.

Once the selection is complete, the user launches the Smart-Transfer function by clicking on the "OK" button. The process then proceeds normally, but only considers the explicitly selected files, not everything on the USB key.

## 3.4 Scan Only and Decontamination

This scan function performs a full antivirus scan on the connected USB key. All files will be scanned, and the scan results will appear on the screen (a log is created after each scanning session, refer to Chapter 3.2.2).

In "Scan Only" mode, infected files are not deleted, the user is only informed of their presence. In "Decontamination" mode, the infected files are deleted from the USB key. A final popup summarizes all actions taken at the end of the scan.

Advanced filtering functions (MIME type, certificate, etc.) will not be applied.

In decontamination mode, virus-infected files are deleted. In "scan only" mode, they are left on the key (it is an informative scan in this latter case).

## 3.5 Scan with file sharing

The Scan with File Sharing option allows a "Smart-Transfer" function, but using a network sharing server instead of the destination USB key.

This sharing server must be an S3SRV server provided by Hogo. The connection to this S3SRV (IP, communication codes, etc.) can be configured on the S3 white station setup interface.

It is used in a similar way as the Smart-Transfer function, but at the end of the process, a popup informs the user of their sharing status and tells them what user ID/password to use to retrieve their files online from the S3SRV.

## 3.6 File sharing synchronization

File sharing synchronization completes a "Smart-Transfer" function, but using a network sharing server instead of the source USB key.

This sharing server must be an S3SRV server provided by Hogo. The connection to this S3SRV (IP, communication codes, etc.) can be configured on the S3 white station setup interface.

It is used in a similar way as the Smart-Transfer function, but when processing starts, the user must enter their user ID/password needed to retrieve their files from the S3SRV, before processing them and putting them on their destination USB key.

## 3.7 Scan with Security Certificate

In addition to the usual Smart-Transfer process, the Security Certificate Scan can verify the PGP signature of files on a USB key.

The user must select the PGP certificate(s) stored in their certificate manager (see Chapter 4.1.3—at least one certificate must be selected or the scan is aborted) and then select one or more files and signatures from the input USB key.

This function will retrieve the signatures and files to be checked from the input USB key and search for a match between these files and signatures. It is based on a PGP certificate library stored in the S3 white station.

Only validated files (i.e. with signature present—named "filename.sig"—and properly verified) are then transferred as part of the Smart-Transfer. Files without signatures on the input key or with an incorrect signature are not transferred.

Please note: The ".sig" signature file must contain only the PGP signature block for the associated file, in "armor [human-readable]" (ASCII encoded) format. Adding a string of characters to the signature file will cause PGP signature verification to fail.

## 3.8 Scan my phone

This function is equivalent to "Decontamination," but supports Android phones (implementing the MTP protocol) instead of USB keys.

## 3.9 Formatting a USB key

Starting this function performs the following actions:

- Any partitions on the USB key are deleted.
- The files are also deleted.
- If "Advanced" mode is enabled, the USB key is rewritten twice with random bytes and then erased again.
- Lastly, a new partition is created (FAT32, exFAT or NTFS depending on the option chosen in the tools setup screen).

The details of these steps (i.e. Shell messages) are stored in the Formatting log.

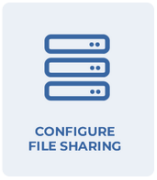
This GUI is relatively simple, the user must simply wait for the formatting to be completed and then click on "Quit" to return to the "Tools" screen (see Chapter 3.1).

Please note:

- A start screen will warn the user that a USB key must be connected before formatting can begin.
- Removing the USB key during the formatting actions may irreparably damage it. In addition, the S3 white station could become corrupted and require heavy maintenance (i.e. factory return to Hogo).

# 4 General Settings

After entering the password, users can enter this screen from the welcome screen by clicking on "Settings." The following functions are available:

| | |
|---|---|
|  | This button is used to update the antivirus engines or the embedded software in the S3 white station (see Chapter 4.2). |
|  | This button is used to manage the S3 white station's tool settings (see Chapter 4.1). |
|  | This button is used to view and export the S3 white station's logs (see Chapter 4.5). |
|  | This button is used to set the date and time on the S3 white station (see Chapter 4.4). |
|  | This button is used to change the administrator password on the S3 white station (password required to access setup) (see Chapter 4.3). |
|  | This button is used to configure the S3SRV file sharing server. |
|  | This button allows access to language management (see next section). |

Note: In the settings menu, each screen/sub-screen will close if there is no user activity for more than 10 minutes (except when an action is being performed by the system, such as an update).

## 4.1 Tool settings

Users can access this screen from the "Settings." The following functions are available:

| | |
|---|---|
|  | This button opens the USB manager (management of authorized USB keys) (see Chapter 4.1.1). |
|  | This button is used to open the filtering settings (MIME type, etc.) (see Chapter 4.1.2). |
|  | The certificate manager allows users to manage the "Scan with security certificate" function and the list of certificates available in the S3 white station. |
|  | If the station is equipped with a reader, this button opens the ID card reader settings. |
|  | This button takes users back to the previous screen. |

### 4.1.1 USB Manager

The following buttons can be used after entering the S3 white station's administrator code:

[See USB list] Displays the authorized (iSerial) keys on this S3 white station.

[Add to list] If a USB key is connected, this function adds it to the list of authorized keys.

[Delete from list] If a USB flash drive is connected, this function removes it from the list of authorized keys.

[Clear the list] The list of authorized keys is reset.

[Quit] Returns the user to the previous screen.

*Please note:* The USB key IDs are representative of a partition. This means that the S3 white station can manage USB keys with multiple partitions. Hogo recommends storing sensitive USB keys securely, to prevent their partition IDs from being compromised or duplicated.

### 4.1.2 Filtering settings

The following options are available:

- Behavior for unknown MIME types
  - Isolate files with unknown MIME type.
  - Skip files with unknown MIME type.
  - Copy files with unknown MIME type.

- Smart MIME filtering
  - "Yes" will enable MIME type filtering when using Smart-Transfer.
  - "No" will disable MIME type filtering.

- Filtering USB keys
  - Allows all USB keys, without filtering.
  - Uses authorized input USB keys only.
  - Uses authorized output USB keys only.
  - Uses authorized input and output USB keys only.

  Please note: USB keys must be authorized via the "USB Manager."

- Action when USB media are plugged in
  - Allows users to choose a scanning mode that starts automatically when a USB key is detected.
  - Users can also open a "Scan choice" window or take no action.

- Clean the output USB key with the end of the transfer
  - When this option is enabled, the output USB key is emptied before copying the files.
  - Otherwise, the existing files on the output key are kept, which *can lead to a security risk if these files are not dealt with*.

- SHA256 fingerprints
  - If this option is enabled, files are fingerprinted before and after scanning and transfer for end-to-end integrity validation.
  - Otherwise, the fingerprints are not made.

- Duration of scan authorization
  - This option allows users to choose the length of time for which scans are possible after an update.
  - By default, the duration is 7 days (recommended for maximum security), but it can be extended to 14 or 30 days.

- USB Key Tagging for S3Agent:
  - Allows the selection of whether USB keys are prepared (by attaching a tag or "token") for S3Agent (protection on the workstation). The options are: tag all keys (Yes), tag only authorized keys (see 4.1.1), or no tag (No).

- Antivirus scan mode
    - Both of these modes are based on the recommendations of the antivirus software publishers.
    - In normal scan mode *(default)*, the level of nested archives scanned (ZIPs within a ZIP) is limited to 10, files larger than 100 MB are not fully scanned (as viruses are usually propagated in small files) and directories with more than 80 nesting levels are ignored (warnings are displayed).
    - The advanced scan mode is slower, but the maximum nesting level is 1000, and the max size of scanned files is 2500 MB.

- Sending Scan results
    - When this option is enabled, the scan logs are encrypted and stored securely on the S3 white station to be sent to MyHogo during synchronization routines.

- Quarantine files
    - When this option is enabled, the contaminated files are archived in password-protected ZIP files and put on the output USB key. The password is displayed and logged.

- Format mode: Select the type of formatting performed by the S3 white station.

- Format partition type: Select the type of partition written by the S3 white station (NTFS, exFAT or FAT32).

- Encrypted ZIP scan: Allows users to choose the type of processing for password-protected ZIPs (no processing or use of a password dictionary).

The Encrypted ZIP button displays the ZIP password dictionary stored in the S3 white station. Each password is used (if checking is enabled) to try to scan inside the ZIPs.

The MIME Rules button brings up the MIME filtering rules saved in the S3 white station. Each known MIME type (and the corresponding action) is described.

Please note (1): For reasons of processing time and security, we do not recommend authorizing MIME types for "archive" files. This includes the following MIME extensions and types:

7z: application/octet-stream
a: application/octet-stream
arc: application/octet-stream
arj: application/arj, octet-stream
bin: application/x-binary, octet-stream
bz: application/x-bzip
bz2: application/x-bzip2
dump application/octet-stream
gtar: application/x-gtar
gz: application/x-compressed, x-gzip
lha: application/x-lha, octet-stream
lzx: application/x-lzx, octet-stream
rar: application/x-rar-compressed
tar: application/x-tar
tgz: application/gnutar, x-compressed
wim: application/octet-stream
wim: application/x-ms-wim
xz: application/x-xz
z: application/x-compressed
zip: application/x-compressed, zip, x-zip

Please note (2): By default, executable files are allowed so as not to impose too many constraints on the use of USB media (as these MIME types can be used for perfectly legitimate reasons). However, Hogo cautions that these EXE files may be self-extracting archives and encourages users to contact their local IT administrator or Hogo directly if a stricter configuration not allowing these files is desired.

### 4.1.3 Certificate Manager

The certificate manager allows users to view the list of certificates known to the S3 white station and to add new certificates or remove existing ones.

In accordance with ANSSI recommendations (see the French General Security Reference System RGS V2 – *Référentiel Général de Sécurité*), certificates must have a minimum key size of 2048 bits, for those expiring in 2030. Certificates expiring after 2030 must have a minimum key size of 3072 bits.

Hogo recommends using 4096-bit certificates when possible.

The following buttons can be used after entering the S3 white station's administrator code:

| | |
|---|---|
| [Add to list] | Adds a certificate to the S3 white station (enter the internal name, type, email address of the associated RECIPIENT). The certificate must be present in [.pgp] on a connected USB key (it must be the only file present). |
| [Delete from list] | Deletes the selected certificate from the S3 white station. |
| [Quit] | Returns the user to the previous screen. |

## 4.2 Update

### 4.2.1 Main screen

From the update screen, users can manually start an update or set how updates are performed on the S3 white station:

| | |
|---|---|
|  | This button is used to update the antivirus definitions.<br>Please note: The USB key must be inserted *before* starting the function. |
|  | This button is used to update the S3 white station Core (see Chapter 4.2.4).<br>Please note: The USB key must be inserted *before* starting the function. |
|  | This button is used to manually start the S3 white station's daily synchronization routine.<br>This routine will download and install updates to the white station, synchronize logs and the NTP with MyHogo (cloud or on premises) and synchronize applicable licenses and security policies for the station. |
|  | This button is used to change the white station's update settings. |
|  | This button shows the software and antivirus versions installed on the S3 white station (see Chapter 4.2.6). |
|  | This button takes users back to the previous screen. |

### 4.2.2 Update settings

From this screen, users can set how the S3 white station updates itself:

| | |
|---|---|
|  | This button is used to change the S3 white station's update mode (see Chapter 4.2.2.1). |
|  | This button is used to change the S3 white station's connection settings (see Chapter 4.2.2.2). |
|  | The "Local Relay Settings" button is used to configure the connection to your S3SRV(s) for an update in "On premises" mode (see Chapter 4.2.2.3). |
|  | Use this button to take into account the details of your connection (mode, LAN connection, S3SRV, etc.) and to perform a quick test to validate the configuration of the S3 white station. |
|  | This button takes users back to the previous screen. |

#### 1.1.1.1 Update mode

This window is used to choose how the S3 white station updates itself:

[Over USB] Update using a USB key containing the update file.

[MyHogo Cloud] Update via S3SRV server, after connecting to the local network.

[On premises] Update by logging into the MyHogo website to download files.

On this screen, users can also enable/disable automatic updates (automatic start of the "Synchronization" routine) and choose the time when it is triggered, if applicable.

#### 1.1.1.2 Network settings

This screen is used to configure the connection mode and options for online updates:

- Type of connection: Choice of WIFI, 4G/LTE (compatible models) and RJ45
- WIFI setup[1]:
    - SSID for the WIFI network to be used
    - Password for the WIFI network to be used
- IP address:
    - IP address to be used (static IP or "DHCP")
    - Subnet mask (format 0-32)
    - Gateway (IP or "DHCP")
    - DNS (IP or "DHCP")
    - 4G APN (Access Point Name code, compatible models)
- Enable or disable "Heartbeat" (periodically send a heartbeat message to MyHogo or S3SRV)

Each parameter can be entered using the integrated Hogo keyboard (entry limited to 50 characters per parameter). To configure a proxy, click on the "Proxy" button:

- Activate/Deactivate proxy
- Change the proxy mode (HTTP or HTTPS)
- Set the proxy host, username and access password, if required

#### 1.1.1.3 Local Relay Settings

This window is used to configure how the S3 white station connects to the local S3SRV:

- Type of local relay (S3SRV of "Deposit Server" or "Management Server")
- Host address (or host name)
- Communication code: Secret code and IV code

Each parameter can be entered using the integrated Hogo keyboard (entry limited to 50 characters per parameter). The configuration elements for an S3SRV are provided by Hogo simultaneously with the server.

Please note the settings on the server side:

- The protocol used is HTTPS with TLS version 1.3 and an encryption key of at least 2048 bits (before 2030).
- The only CipherSuites allowed are TLS_DHE_RSA_WITH_AES_256_CCM, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CCM and TLS_DHE_RSA_WITH_AES_128_CCM (*please note: The EMPTY_RENEGOTIATION renegotiation option is also presented for compatibility reasons*).
- It is necessary to use a signed SSL certificate, either by a known authority (CA) or by an authority added to the station (contact Hogo to add a CA certificate to the S3 station).

For more information, please refer to the ANSSI guide "Security Recommendations for TLS."

[1] *Use of Wifi in the 2400MHz to 2483.5MHz band, with a maximum measured power of 1.09mW.*

### 4.2.3 Antivirus update

The antivirus engine update function opens if the preconditions are met (accessible USB key or network and new update available). The update file will be analyzed, validated and then applied to the system.

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

In the case of a USB update[2], if the station detects input/output errors on the USB key, the GUI will ask the user to reselect an update file (otherwise, the user can directly exit the interface afterwards).

Please note: It is possible to manually update the station with definitions from one or two days previous (even if newer bases are already installed) to temporarily revert to an earlier version, for example, in case of unwanted false positives due to an antivirus update.

Hogo only recommends this downgrade action if the new antivirus bases have a strong impact on the usability of the stations and after an ad hoc security study.

### 4.2.4 Updating the Core

The Core software update function opens if the preconditions are met (accessible USB key or network and new update available). The update file will be analyzed, validated and then applied to the system.

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

In the case of a USB update[2], if the station detects input/output errors on the USB key, the GUI will ask the user to reselect an update file (otherwise, the user can directly exit the interface afterwards).

### 4.2.5 Online synchronization

Online synchronization, launched manually or periodically, makes it possible to:

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

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

### 4.2.6 Viewing versions

This screen shows the versions of the Core and antivirus engines, as well as the device name and MAC address.

The only option available is ¨Quit¨ to return to the previous screen.

[2] *"JIT" update files must be placed at the root of the USB media in case of offline updates.*

## 4.3 Login screen – Administrator functions

This GUI is a keyboard specifically designed by Hogo containing three sets of characters:

- Lower case characters (as well as numbers and some punctuation marks, broadly corresponding to the "AZERTY lower case" keyboard)
- Upper case characters (as well as numbers and some punctuation marks, broadly corresponding to the "AZERTY upper case" keyboard)
- Special characters (with accents)

It allows users to enter the administrator password for the S3 white station so they can access the protected functions (Core updates, USB Manager, etc.).

Once the password has been entered correctly, the functions can be accessed.

The same keypad is displayed when renewing the white station's password.

The administrator password must be between 16 and 32 characters long, chosen from the Hogo keyboard (10 numbers, all 26 letters of the alphabet in upper and lower case and 25 special, accented and punctuation characters). It must contain at least one lower case letter, one upper case letter and one number.

For this password renewal, Hogo's recommendations are as follows:

- Hogo recommends renewing the password every 6 months to every 2 years, depending on the sensibility of the information system, using the S3 station;
- Hogo recommends not reusing passwords that have already been used.

## 4.4 Set time and date

This interface is used to set the S3 white station's time and date.

- "Year," "Month," "Day," "Hour" and "Minutes" are used to set the time and date.
- "Save" saves the settings in the S3 white station.
- Use the NTP settings to set the parameters used for NTP synchronization:
    - Activate/Deactivate NTP synchronization
    - Select the IP/hostname of the first NTP server to contact, as well as its protocol version
    - Select the IP/hostname of the second NTP server to contact, as well as its protocol version
- "Quit" closes this interface.

## 4.5 Screensaver

This interface allows you to modify the sleep and screensaver settings of the white S3 station.

- Sleep Mode: Choose between "no sleep", "screensaver", "sleep then energy saving", or "energy saving" (black screen).
- Screensaver Type, if enabled: Rotating images, Video.
- Delay before screensaver and/or sleep (black screen): Defines the delay between stopping use and switching to the screensaver, and switching to a black screen (if enabled).
- "Select Files": Access files on a USB key connected to the station to choose images or a video for the screensaver.
- "Save": Saves the changes, "Preview" shows the screensaver as it will appear when the timeout is triggered.
- "Exit": Closes this interface.

Note: The sleep and screensaver settings cannot be modified on the S3Box tablet to save battery life; the system controls these settings:

- The tablet screen turns off after 5 to 15 minutes ("black screen").
- The system enters deeper sleep after one to three hours ("suspend").
- Occasionally, the system goes into deep sleep ("freeze state") to save battery (after one to seven days of being on without use): in this case, a restart may be necessary.

## 4.6 Logs

### 4.6.1 Main screen

| | |
|---|---|
| Main S3 log | This button shows the main log of the S3 interface (listing the user and administrator actions performed).[3] |
| AV update log | This button opens the antivirus definition update log (see Chapter 4.2.3).[3] |
| Core update log | This button opens the Core update log (see Chapter 4.2.4).[3] |
| Export logs | This button moves all logs to an output USB key. The logs will be moved to a specially created encrypted file on this USB key. The USB key must be inserted *before* launching the function. |
| Send logs | This button is used to send all logs to MyHogo (Cloud or on premises). |
| Syslog parameters | This button provides access to the Syslog settings (see Chapter 4.5.2). |
| Quit | This button closes the log interface. |

[3] *If you have any questions, please contact Hogo with the reference code(s) of the message(s) you would like explained.*

### 4.6.2 Syslog connection parameters

On this screen, users can set up the Syslog server(s) used for sending logs and synchronizing (automatically or manually) the S3 white station:

- Enable/Disable Syslog
- Choose the sending mode (UDP if available, TCP, TCP over SSL)
- Choose the IP/hostname of the first Syslog server to contact and its port
- Choose the IP/hostname of the second Syslog server to contact and its port

### 4.6.3 Displaying Logs

The contents of the logs are shown on the screen. The screen can be closed by clicking on "Quit." It is not possible to edit logs. For security reasons, logs are read-only.

To make it easier to read logs, the messages shown on this screen were selected using ANSSI recommendations. Many more messages are tracked by the S3 system and can be reported to a SYSLOG server or exported to a USB key in encrypted files.

The messages that come up are either notifications (black messages) or errors (red messages). The given code has the prefix "LogEvent" for notifications and "LogError" for errors.

This message code is unique and consists of YYxZZ, where YY is the decimal code of the module in question and ZZ the code of the message in that module.

Please note: When displayed on the screen, logs can be shortened if they contain too many lines, so the display is readable. The shortening follows a FIFO (First In, First Out) logic and the full content can be accessed via the management console or the Syslog sink.

For more information on the posted events, see the ANSSI document: DAT-NT- 012/ANSSI/SDE/NP "Security recommendations for the implementation of a logging system."

### 4.6.4 Details of log messages

The table below provides the details, for S3 terminals, of the events that are logged and viewable in the administrator interface. The subject and examples are taken from the ANSSI document "Security recommendations for the implementation of a logging system."

| Subject | ANSSI example | S3Core logging |
|---|---|---|
| Authentication | Authentication successes and failures | All authentication attempts are tracked, both those that are successful and those that failed. |
| | Uses of different authentication mechanisms | Opening the S3 Administrator password input interfaces. |
| | Elevations of privileges | All authentication attempts are tracked, both those that are successful and those that failed. |
| Account and rights management | Adding/deleting accounts/groups/roles | *Not applicable to the S3Core.* |
| | Assigning/deleting rights to/from accounts/groups/roles | *Not applicable to the S3Core.* |
| | Changes to authentication data | Changing the administrator password, successes and failures. |
| Access to resources | R/W/X access or attempted access to resources | SCAN Access to data in transit and scanned data is tracked, both in writing (data storage, deletion) and reading (various controls).<br>*Please note: In accordance with ANSSI recommendations, there is no execute access for this data.* |
| | | UPDATE Access to update data is tracked during writing (retrieval, storage, deletion), reading (various checks) and execution (application of update scripts). |
| | | LOGGING Read access (opening logs) to log data is tracked.<br>*Please note: In accordance with ANSSI recommendations, there is no execute access for this data.* |
| Changing security policies | Editing, applications, configuration resets | PARAMETERS Each recorded parameter change is logged ("before" and "after" values). Each unsuccessful attempt to make a change is also tracked. |
| | | UPDATE Each update attempt, whether successful or failed, is tracked, with details of the steps taken, in the update logs. |
| Process activity | Starts/Stops | Each start or stop of an S3Core internal process (i.e. panel displayed or process used) is logged. |
| | Malfunctions | Any process errors are logged. |
| | Loading/unloading of modules | *Not applicable to the S3Core: considered in the "Start/Stop" case.* |
| System activity | Starts/Stops | Each start, stop or restart of the device is logged. |
| | System malfunctions/overloads | Every system event of "error" level or higher is logged. |
| | Loading/unloading of modules | *Not applicable to the S3Core: considered in the "Start/Stop" case.* |
| | Hardware activity (failures, physical connections/disconnections, etc.) | FAILURE Each system event of "error" level or higher is logged. |
| | | (DIS)CONNECTION Each connection or disconnection event of a removable storage or HID device is logged. |