# Hogo S3

HR-MAN-26-209-v4

# User Manual

2026

Versions 1.8 (since build 2025111303) and 1.9 (since build 2024010101)

This document describes the use of the S3 product range. It follows a structure based on the product's standard HMI and focuses on the user experience.

| 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 | 03/2026 | Updated to align with the T1 2026 update |
| | | |

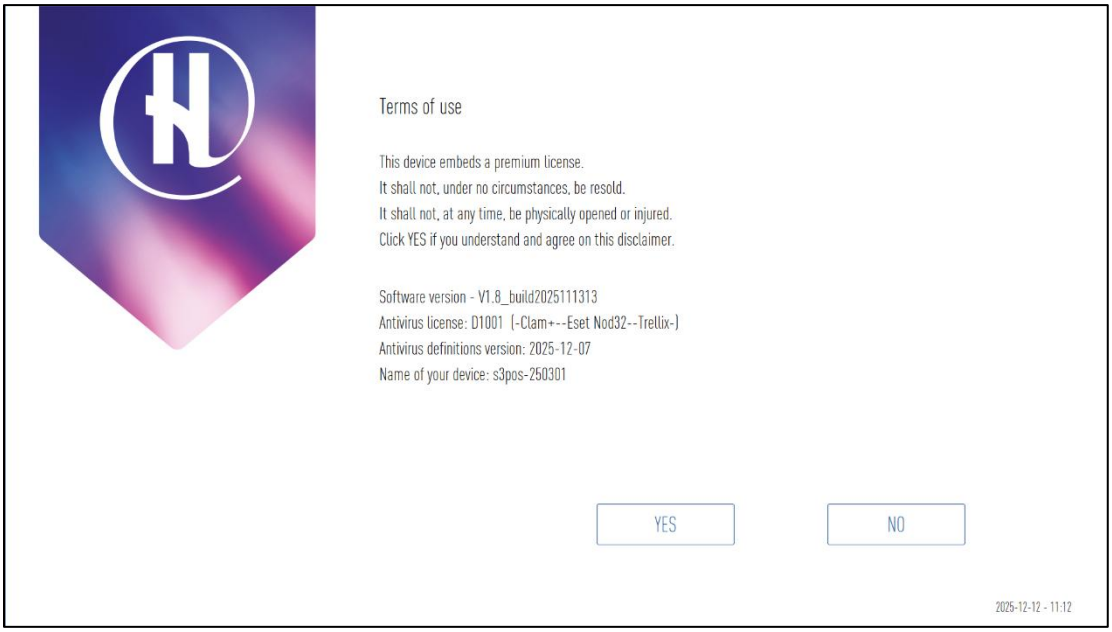
# Table of Contents


1 Main Interface – Home ..... 4
1.1 Terms of Use ..... 4
1.2 Main Screen ..... 5
1.3 User Assistance ..... 6
1.4 Language settings ..... 7
1.5 Media Support Status Display ..... 7
2 Tools S3 ..... 9
2.1 Screen « Tools » ..... 9
2.2 Secure Transfer with Protocol Break « Smart-Transfer» ..... 10
2.2.1 What is Smart-Transfer? ..... 10
2.2.2 Starting Smart-Transfer ..... 10
2.2.3 Smart Transfer with File Selection ..... 12
2.2.4 Smart Transfer « Media » ..... 13
2.2.5 Finalizing the Transfer ..... 13
2.2.6 End of Process and Logging ..... 14
2.3 Scan Only (Quick Scan) and Decontamination ..... 14
2.4 Scan with File Sharing ..... 16
2.4.1 Send ..... 16
2.4.2 Upload ..... 16
2.5 USB Key Formatting ..... 18
3 Scan Log ..... 19
3.1 Scan Log on the station ..... 19
3.2 Exported Scan Log ..... 20
3.2.1 Summary of Key Values ..... 20
3.2.2 Detailed Scan Summary ..... 20
3.2.3 Technical Metrics and Indicators ..... 21
3.2.4 Antivirus Engine Versions ..... 22
3.2.5 Detected Threats ..... 22
3.2.6 Detected Warnings ..... 23
3.2.7 Scan Settings ..... 23
4 S3Core Rescue mode ..... 24
5 Best Practices for Use ..... 24

# 1 Main Interface – Home

## 1.1 Terms of Use

The Terms of Use are displayed when the S3 stations start up:




➔ Click "Yes" if you accept these Terms of Use.
➔ Selecting "No" will prompt for the administrator password and will shut down the S3 white station.

*Note:* S3 stations feature a detection and alert mechanism for "badUSB" devices. This alert is only activated once this disclaimer is displayed. Therefore, if such a device is already connected beforehand, no warning popup will be generated. It is recommended to check the devices connected to the station at startup.

## 1.2 Main Screen

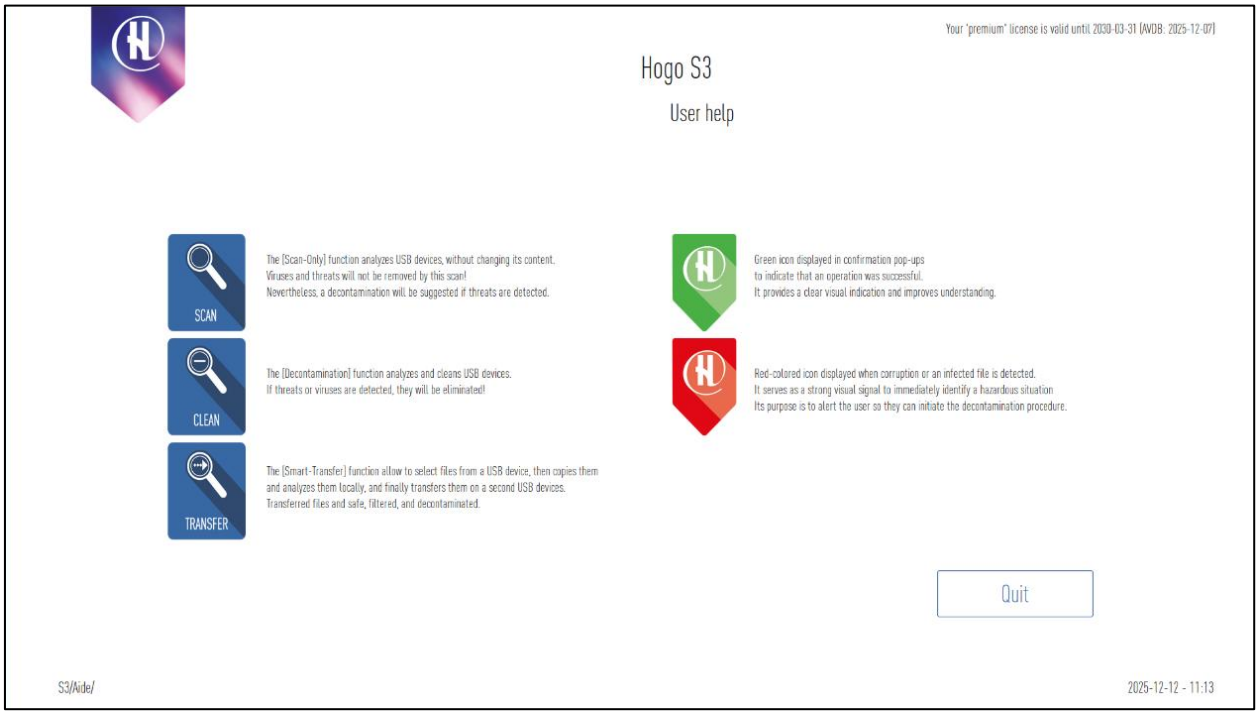
Once the Terms of Use have been accepted, the main screen is displayed:




| | |
|---|---|
|   | This button starts the Smart-Transfer function, which performs antivirus scans and advanced filtering (MIME type, USB key…) on the input files before transferring them to the output key, see chapter 2.2.<br>Note: The input USB media must be connected before starting the function. |
|   | This button starts the Scan with Decontamination function. This function performs antivirus scans without advanced filtering or file transfer, see chapter 2.3.<br>Note: The USB drive must be connected before starting the function. |
|   | This button provides access to the Tools page, see chapter 2. |
|  | This button provides access to the Settings page. See the Administrator Manual. |
|  | This button displays help related to the main functions of the station. See chapter 1.3 for more information. |
|  | This button provides access to the station's language selection. See chapter 1.4 for more information. |

## 1.3 User Assistance

The User Assistance section provides various reminders and useful information to understand how the S3 white station operates. It describes the main features available from the home screen and provides guidance on scan modes, file transfer, alert handling, and log viewing.

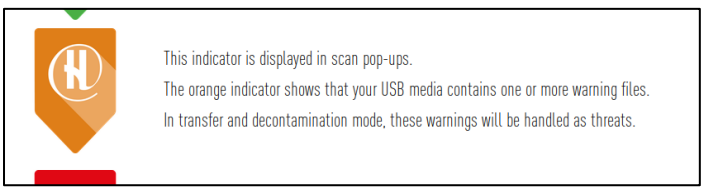



This help section guides you through common actions:

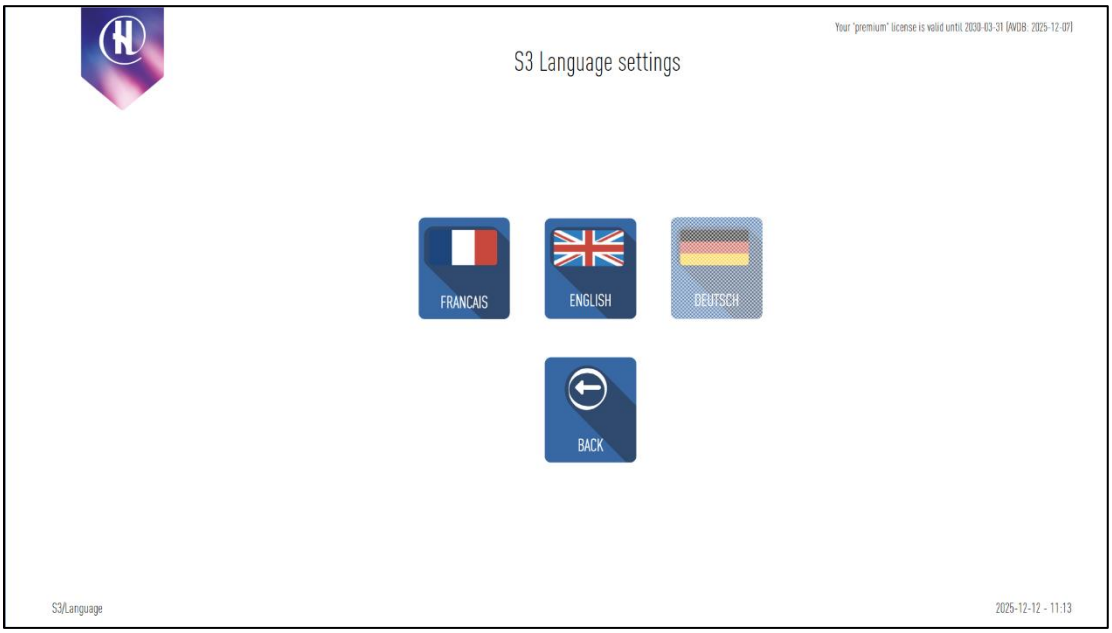
- Selecting the appropriate scan mode,
- Understanding the icons and messages displayed on the screen,
- Interpreting scan results,
- Knowing when to use Smart-Transfer or the Decontamination mode,
- Checking for the presence of a threat or a warning.

It also serves as a reference point if you are using the station for the first time or if you are unsure about the correct procedure to follow.

*Note: Depending on the configuration selected by your administrator, an orange bookmark may appear on this screen.*



## 1.4 Language settings




This window allows you to change the language used by the white station.

Each flag will restart the white station's interface in the selected language. This language will remain active during future restarts.

## 1.5 Media Support Status Display

When a USB device is connected, an icon may appear on the screen to indicate the presence of a storage medium. Two types of icons may be displayed:

- indicating that a USB flash drive is connected
- indicating the presence of a CD drive

These icons appear at the bottom of the screen, next to the station's date and time display, regardless of which screen is currently shown.




The presence of these icons confirms that your USB device has been detected by the station before any operation is performed. A change in the icon's color means that:

- The station is currently reading from or writing to the media, and disconnecting it prematurely may compromise data integrity.
- Indicates that a CD is present in the drive. If a CD drive is permanently connected to the station, this indication allows you to verify that the drive no longer contains a disc before leaving the station.

*Note: In some cases, with specific USB devices (for example, secure USB flash drives), both icons may appear.*

# 2 Tools S3

## 2.1 Screen « Tools »




| | |
|---|---|
|   | This button starts the Smart-Transfer function, which performs antivirus scans and advanced filtering (MIME type, USB drive, etc.) on the input files before carrying out the transfer through protocol break to the output USB media, see chapter 2.2.<br>Note: The USB media must be connected before starting the function. |
|   | This button starts the Scan Only function (without decontamination). Infected files are not removed, but the user will be notified of their presence, see chapter 2.3.<br>Note: The USB media must be connected before starting the function. |
|   | This button starts the Secure File Sharing function, enabling file sharing over the network at the end of the scan instead of requiring an output USB media, see chapter 2.4.<br>Note: The USB media must be connected before starting the function. |
|   | The "Formatting" function allows you to format a USB drive, see chapter 2.5.<br><br>Note: The USB media must be connected before starting the function. |

| | |
|---|---|
|  | This button starts the Scan with Decontamination function. This function performs antivirus scans without advanced filtering or file transfer. Infected files are deleted, see chapter 2.3.<br>Note: The USB drive must be connected before starting the function. |
|  | This button starts the Secure File Sharing function, which allows you to retrieve files from a network share before requesting an output USB drive, see chapter 2.4. |
|  | This button allows you to return to the main screen of the S3 white station, see previous chapter. |
|  | This button displays help related to the main functions of the station. See chapter 1.3 for more information. |
|  | This button provides access to the station's language selection. See chapter 1.4 for more information. |

## 2.2 Secure Transfer with Protocol Break « Smart-Transfer»

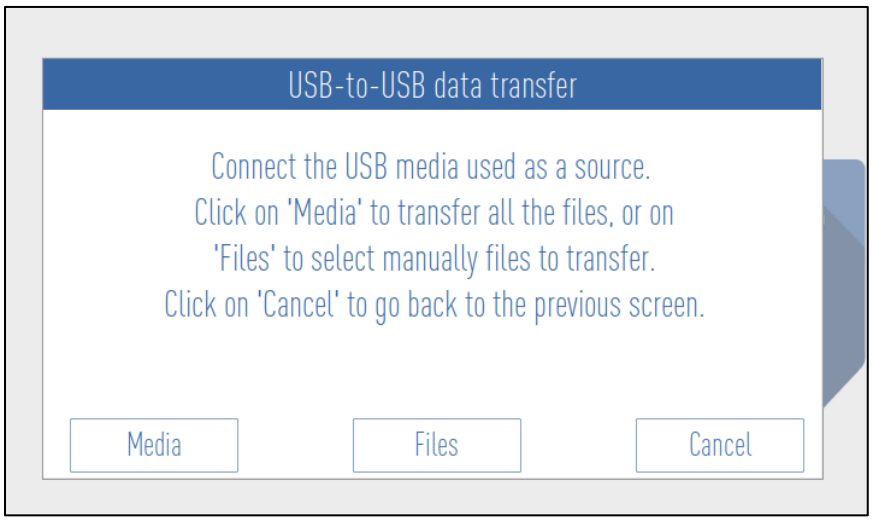
### 2.2.1 What is Smart-Transfer?

Smart-Transfer is a feature that enables data transfer from one USB media to another. The files to be transferred are selected and decontaminated beforehand.

If data is already present on the output media, it will be deleted and replaced by the transferred data.

### 2.2.2 Starting Smart-Transfer

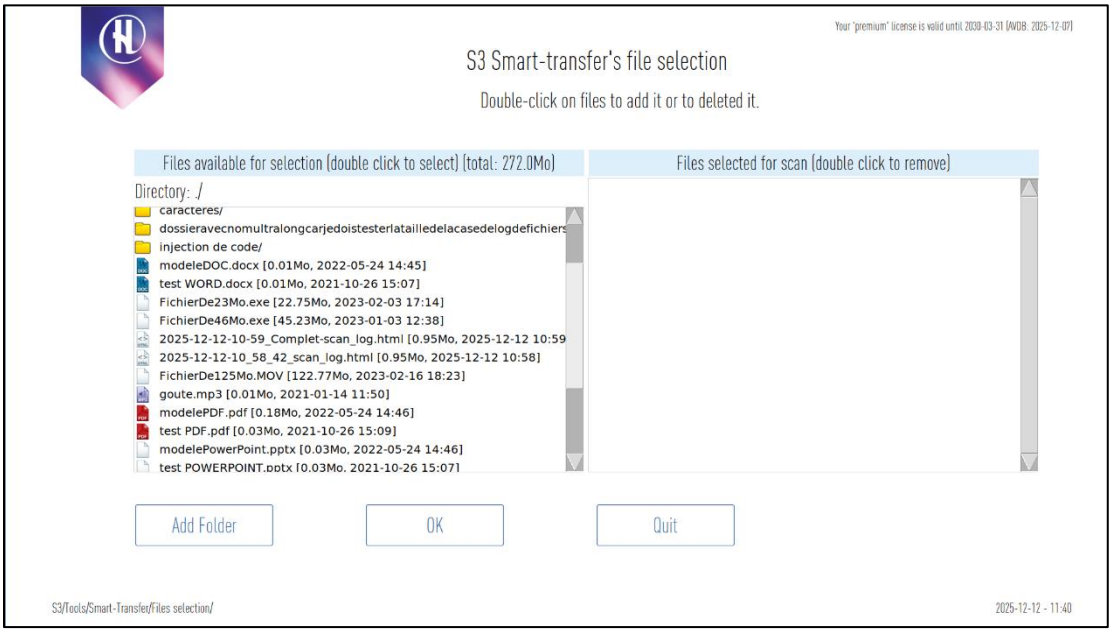
When Smart-Transfer is started, the following screen appears:




Use the ¨media¨ and ¨files¨ buttons to start the Smart-Transfer modes described below.
The ¨Cancel¨ button closes the popup.

### 2.2.3 Smart Transfer with File Selection

If the "Files" mode is selected, the following screen appears:




The "file selection" function displays the files available on the connected USB media in a navigable area on the left side of the screen:

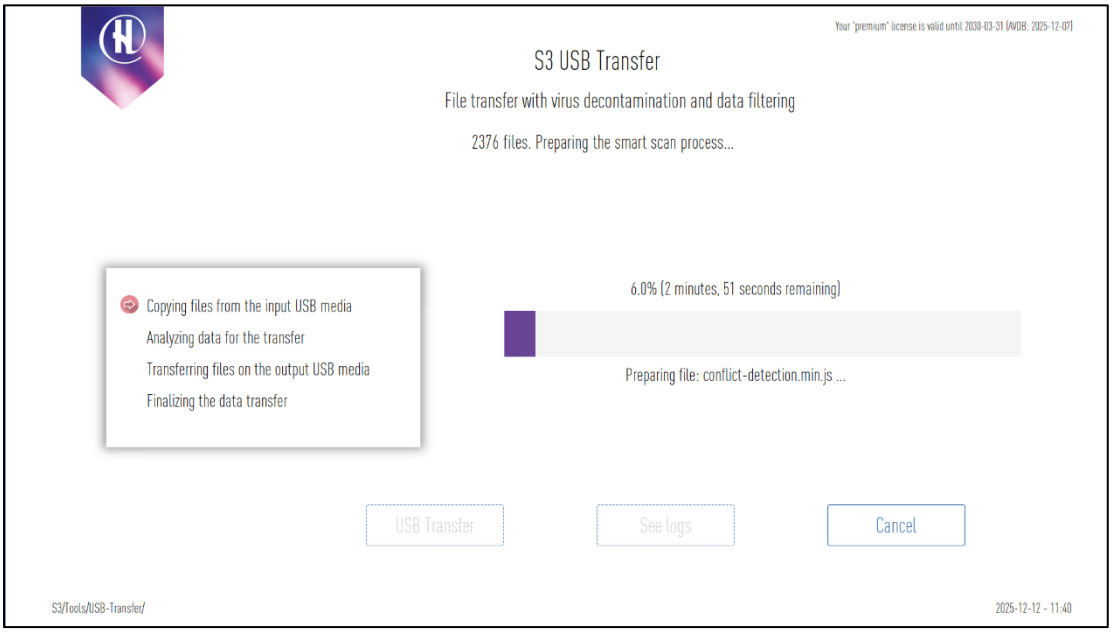
- By double-clicking on a file, you can add it to the list of files to be transferred, displayed on the right side of the screen
- The "Direct Add" button allows you to select a file or folder without double-clicking (with a single click).
- Finally, by double-clicking an item in the list on the right, you can remove it from the selection list.

Once the selection is complete, you can start the Smart-Transfer function by clicking the "OK" button. It will then proceed normally, but only considering the explicitly selected files, and not the entire USB media.

A pop-up indicates the end of the scan, see chapter 2.2.5

### 2.2.4 Smart Transfer « Media »

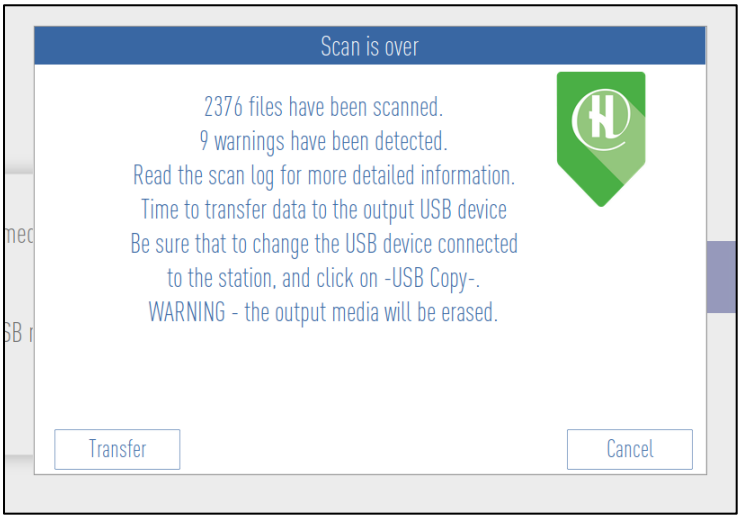
If the "Media" mode is selected, the following screen appears:




The scan of all data stored on the USB drive begins.
A pop-up indicates the end of the scan, see chapter 2.2.5.

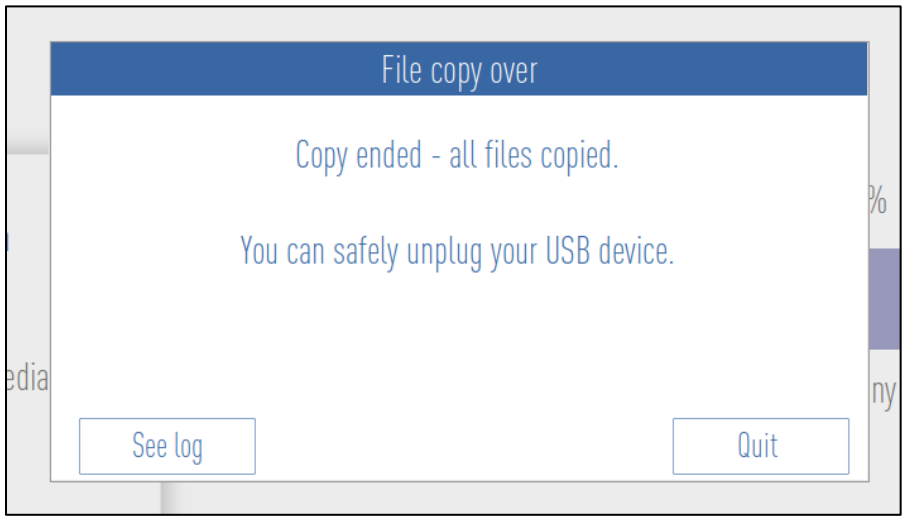
### 2.2.5 Finalizing the Transfer

At the end of the scan, a pop-up instructs you to disconnect the source media and connect the destination media.



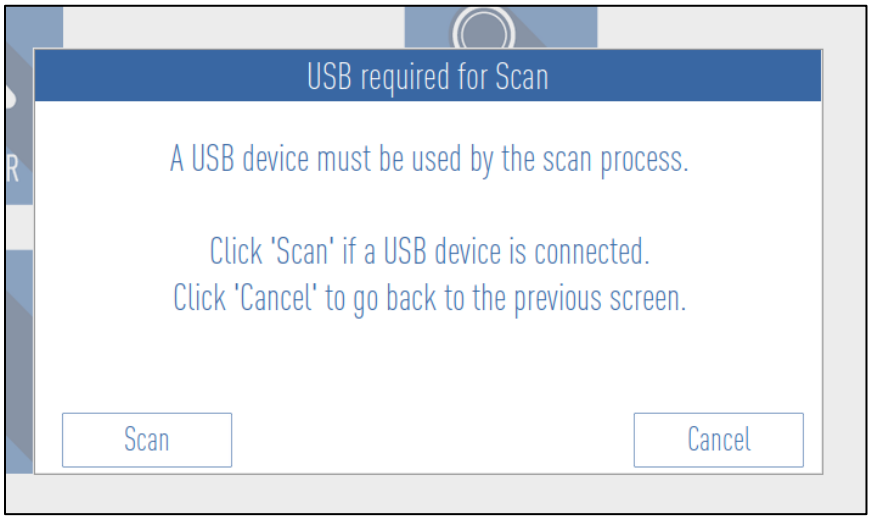
### 2.2.6 End of Process and Logging

At the end of the transfer to the destination media, a pop-up appears to inform you that the media can be disconnected.

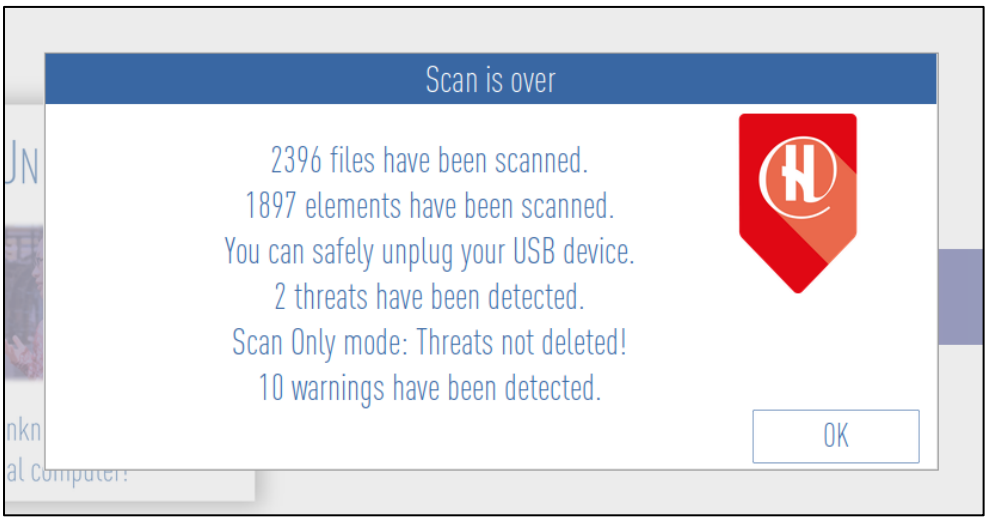



From this pop-up, you can access the scan log (see chapter 3) or exit the Smart-Transfer function to return to the main screen (see chapter 1.2).

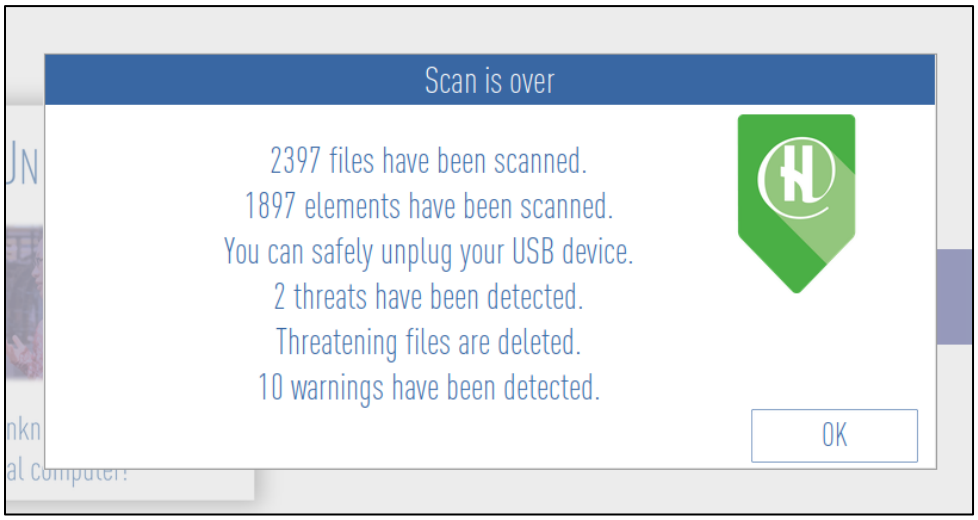
## 2.3 Scan Only (Quick Scan) and Decontamination




This scan function performs a full antivirus scan of the connected USB drive.
In "Scan Only" mode, infected files are not deleted but the user is only informed of their presence. A final pop-up summarizes all actions performed at the end of the scan.

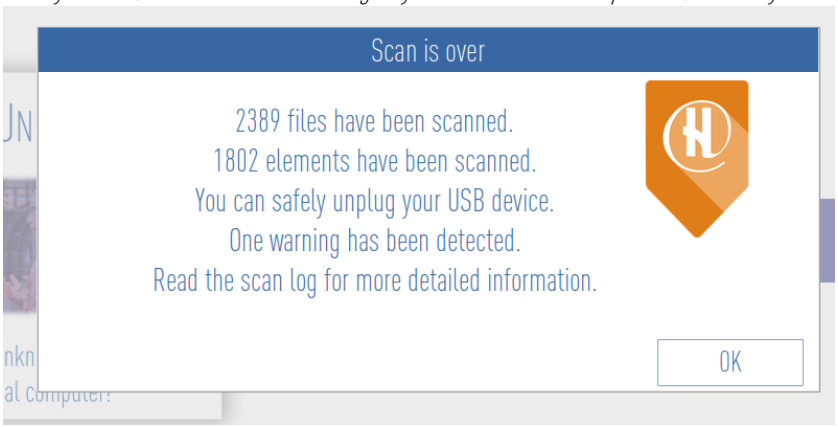



In "Decontamination" mode, infected files are permanently deleted from the USB drive. A final pop-up summarizes all actions performed at the end of the scan.




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

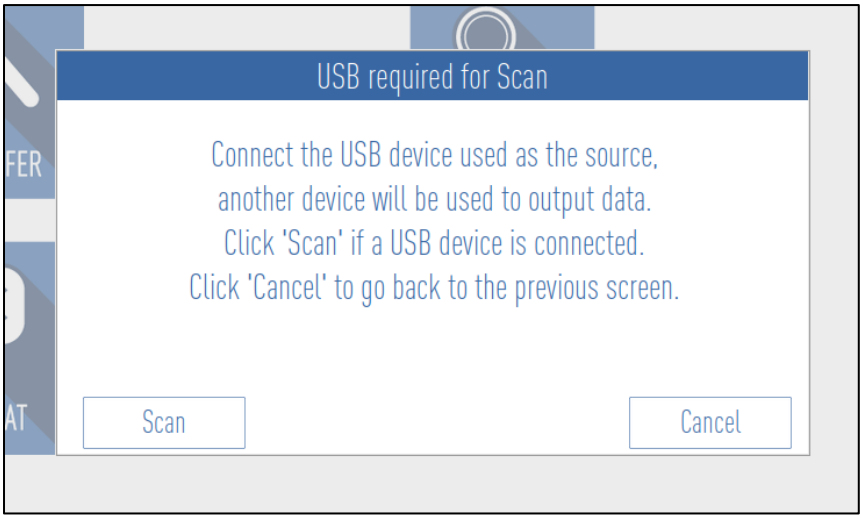
*Note: Depending on the configuration selected by your administrator, an orange bookmark may appear in the popup. This means that your key does not contain any threats, but at least one warning. If you are unsure how to proceed, contact your administrator.*




## 2.4 Scan with File Sharing

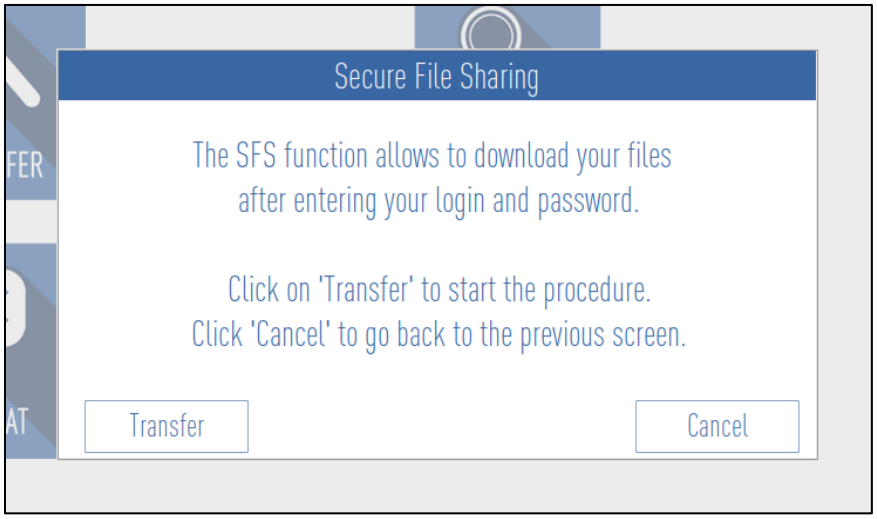
### 2.4.1 Send

The Send function of Scan with File Sharing performs a "Smart-Transfer", but uses the S3SRV instead of the destination USB media.




### 2.4.2 Upload

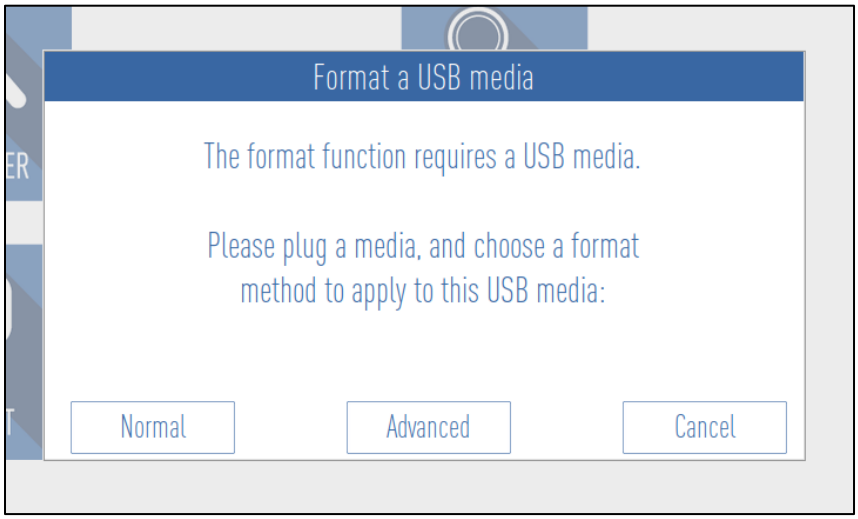
The Download function of Scan with File Sharing performs a "Smart-Transfer", but retrieves files from the S3SRV before requesting an output USB drive.

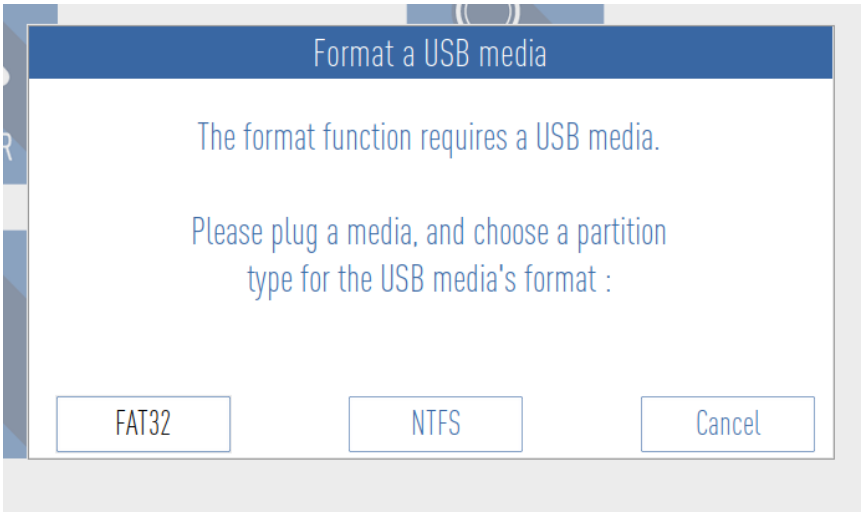

Secure File Sharing
The SFS function allows to download your files
after entering your login and password.
Click on 'Transfer' to start the procedure.
Click 'Cancel' to go back to the previous screen.
Transfer
Cancel

## 2.5 USB Key Formatting

The "Format" function allows you to completely erase the contents of a USB storage device. This operation may be required prior to a transfer or to restore the media to a controlled state.

When the function is launched, several types of pop-up messages may be displayed depending on the settings defined by your administrator. Follow the instructions shown on your screen.



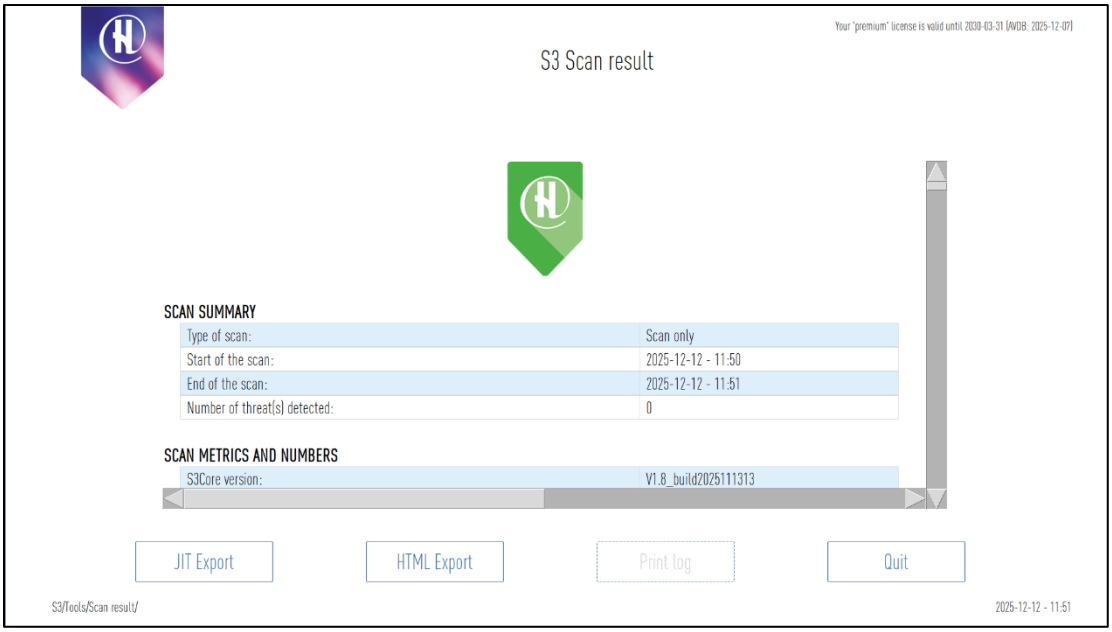




Depending on the configuration defined by the administrator, several behaviors may occur:

- Standard formatting: erases the contents and creates a new partition.
- Advanced formatting: performs a deep erase with secure overwriting (takes longer).
- Formatting type selection.
- Partition type: FAT32, exFAT, or NTFS, depending on the workstation configuration
- Partition type selection.

# 3 Scan Log

## 3.1 Scan Log on the station




From the scan log screen, you can view the log, export it in HTML format (full or summary), or export it in JIT format (HOGO encrypted format).

## 3.2 Exported Scan Log

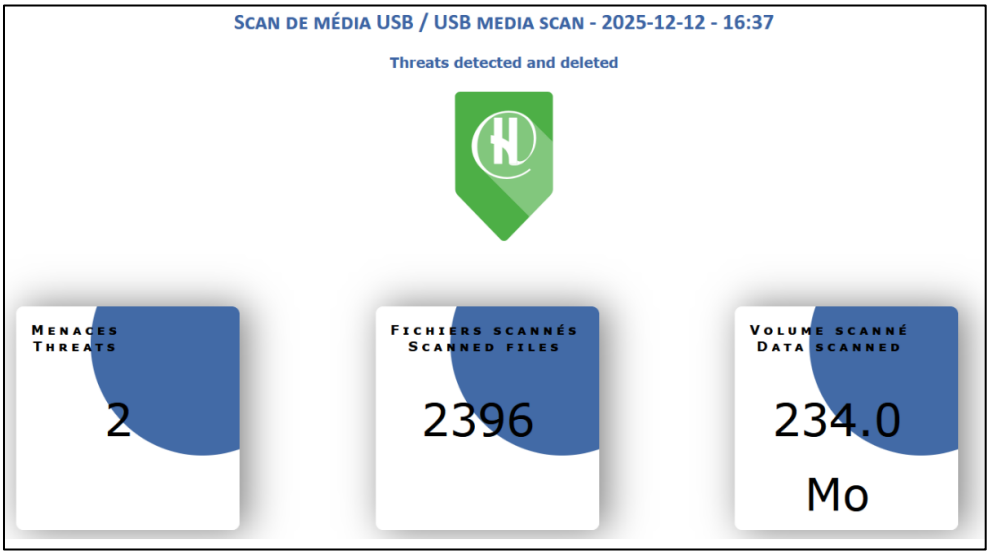
The scan log is divided into several sections, allowing you to quickly understand the scan status, the essential information, and the associated technical details.

### 3.2.1 Summary of Key Values

The first section of the log highlights three essential indicators:

- Number of detected threats: indicates the number of threats identified during the scan.
- Number of scanned files: corresponds to the total number of files examined during the scan.
- Scanned data volume: specifies the cumulative size of the files analyzed.

This information provides an immediate overview of the effectiveness and scope of the scan.




### 3.2.2 Detailed Scan Summary

This second section provides a more comprehensive overview of the scan execution:

- Type of scan performed
- Start date and time
- End date and time
- Total number of detected threats

It allows you to place the scan in its time context and review the overall results before consulting the technical details.

| SCAN SUMMARY | |
|---|---|
| Type of scan: | Decontamination |
| Start of the scan: | 2025-12-12 - 16:36 |
| End of the scan: | 2025-12-12 - 16:37 |
| Number of threat(s) detected: | 2 |

### 3.2.3 Technical Metrics and Indicators

This section groups together the technical data associated with the scan context, such as:

- Antivirus engine version (Core)
- Details and versions of the various antivirus engines used
- Information related to the scanned USB device:
    - Serial number (iSerial)
    - Volume name
    - Partition size
    - Partition type
- Advances statistics :
    - Total size of analyzed files
    - Total amount of data processed
    - Nunber of items examined

This information is useful for traceability and for more in-depth analysis.

**SCAN METRICS AND NUMBERS**

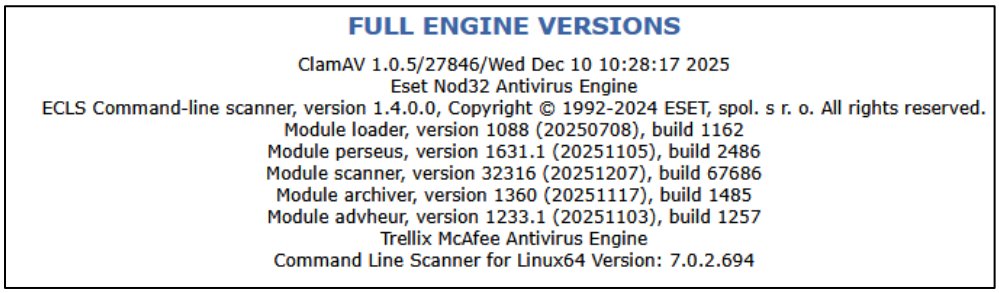
| | |
|---|---|
| S3Core version: | V1.8_build2025111313 |
| Antivirus engines used: | ClamAV, Eset, McAfee-Trellix |
| Antivirus engines global version: | 2025-12-07 |
| Partition nb : | 1 |
| iSerial of the USB device: | 6610-721E |
| Label of the USB device: | CLETEST1 |
| USB device partition size: | 29G |
| USB device partition type: | vfa |
| Scanned files size: | 245433039 |
| Quantity of data scanned: | 234.0 Mo |
| Number of file(s) scanned: | 2396 |
| Nomber of element(s) scanned : | 1895 |

### 3.2.4 Antivirus Engine Versions

The log then lists the full versions of all antivirus engines used:

- The engines and their software versions
- The signature database version
- The dates of the last updates
- The various internal modules, their versions, and their build numbers

This section ensures that the scan was performed using up-to-date engines.

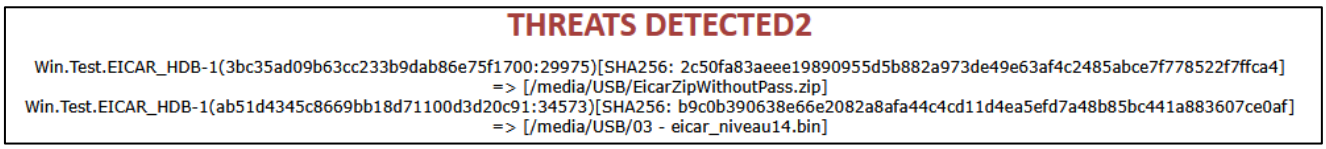



### 3.2.5 Detected Threats

When threats are identified, they are displayed as a list generally containing:

- The threat name or signature
- The hash fingerprint (e.g., SHA-256)
- The affected location(s) on the USB device

Each threat is presented with sufficient detail to allow further analysis or corrective action.



### 3.2.6 Detected Warnings

Warnings indicate items that the engines were unable to analyze.
They may concern, for example:

- Password-protected files
- Corrupted archives
- Files exceeding the allowed size limit
- Unrecognized or unsupported objects

Each warning is accompanied by the corresponding affected item.

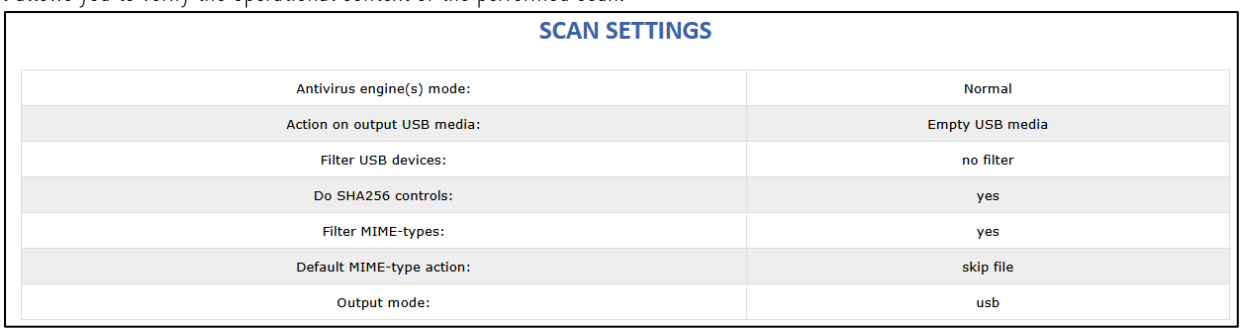



### 3.2.7 Scan Settings

This section indicates the configuration active at the time of the scan, such as:

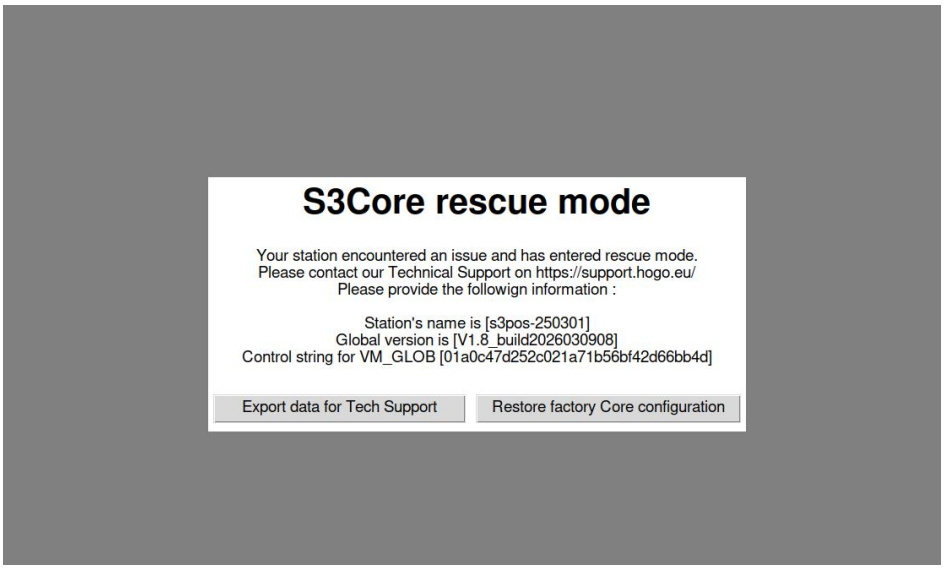
- Antivirus engine configuration mode
- Action applied to the output media
- Presence or absence of a USB filter
- SHA-256 checks enabled or disabled
- MIME filtering enabled or disabled
- Default action applied to unknown MIME types
- Selected output mode

It allows you to verify the operational context of the performed scan.



# 4 S3Core Rescue mode

If this screen appears when the station starts up, immediately contact your administrator.




# 5 Best Practices for Use

To ensure proper use of the S3 white station, follow these best practices:

- ➔ Always insert the USB drive fully before starting a scan.
- ➔ Never remove a device during analysis or copying.
- ➔ Always wait for the scan completion message before unplugging your USB drive.
- ➔ Use only USB media that is in good condition.
- ➔ Regularly check the messages displayed by the station.
- ➔ Carefully read alerts or warnings before proceeding.
- ➔ In case of doubt, repeat the scan or contact your administrator.
- ➔ After decontamination, verify that the expected files are present on the output USB drive.
- ➔ Never attempt to bypass administrator settings, as they ensure your security.