Hogo S3

HR-MAN-26-208-v4

Manuel de l'Utilisateur

2026

Versions 1.8 (depuis le build 2025111321) et 1.9 (depuis le build 2024010101)

Ce document décrit l'utilisation de la gamme S3. Il suit un déroulement basé sur l'IHM standard du produit, et se concentre sur l'expérience utilisateur.

Version	Date	Modifications majeures
V1	02/2018	Version initiale du document
V2	05/2019	Mise à jour suite à revue interne
V3	11/2025	Mise à jour pour s'aligner sur la mise à jour T4 2025
V4	03/2026	Mise à jour pour s'aligner sur la mise à jour T1 2026

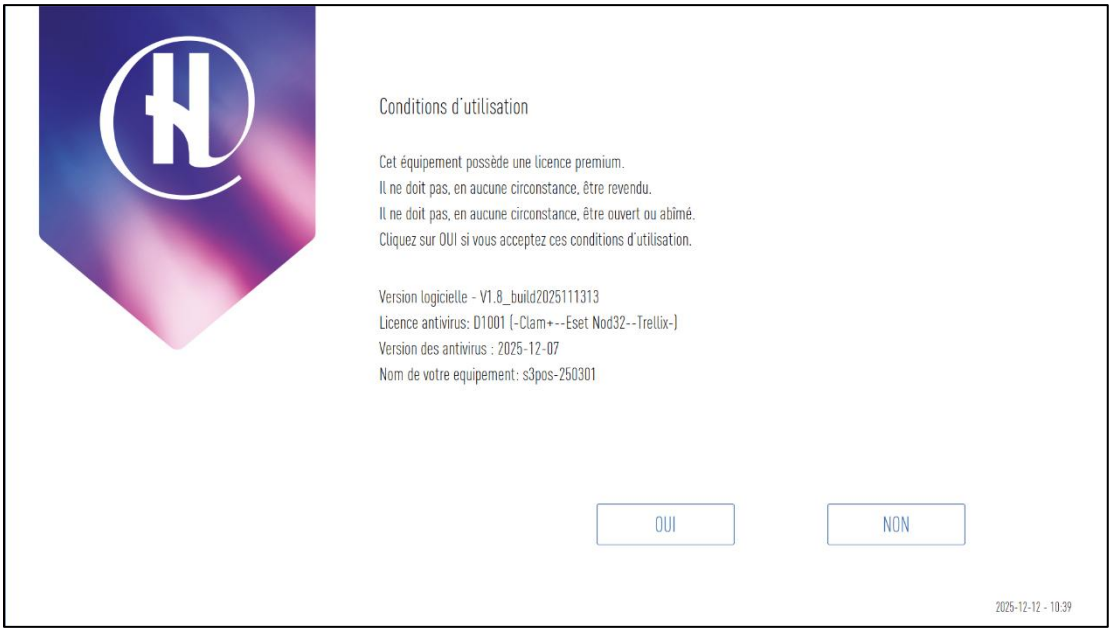
Table des matières

1 Interface principale – Accueil 3
1.1 Conditions d'utilisation 3
1.2 Écran principal 4
1.3 Aide à l'utilisation 5
1.4 Gestion des langues 6
1.5 Affichage de l'état des supports média 6
2 Outils S3 8
2.1 Écran « Outils » 8
2.2 Transfert sécurisé avec rupture protocolaire « Smart-Transfer » 10
2.2.1 Qu'est-ce que le Smart-Transfer ? 10
2.2.2 Lancement du Smart-Transfer 10
2.2.3 Smart Transfert avec Sélection de fichiers 11
2.2.4 Smart Transfert « Média » 12
2.2.5 Finalisation du transfert 12
2.2.6 Fin du processus et journalisation 13
2.3 Scan seul (rapide) et Décontamination 13
2.4 Scan avec partage de fichiers 15
2.4.1 Envoyer 15
2.4.2 Télécharger 15
2.5 Formatage de clé USB 17
3 Journal de Scan 18
3.1 Journal de Scan sur la Station 18
3.2 Journal de Scan exporté 19
3.2.1 Résumé des valeurs principales 19
3.2.2 Résumé détaillé du scan 19
3.2.3 Métriques et indicateurs techniques 20
3.2.4 Versions des moteurs antivirus 20
3.2.5 Menaces détectées 21
3.2.6 Avertissements détectés 21
3.2.7 Réglages du scan 22
4 S3Core Rescue mode 22
5 Bonnes pratiques d'utilisation 23

1 Interface principale – Accueil

1.1 Conditions d'utilisation

Les Conditions d'Utilisation sont affichées au démarrage des stations de la gamme S3 :



➔ Cliquez sur "Oui" si vous acceptez ces conditions d'utilisation.
➔ "Non" demandera le mot de passe d'administration, et éteindra la station blanche S3.

À noter : Les stations S3 ont un mécanisme de détection et de signalisation des périphériques « BadUSB ». Cette signalisation ne démarre qu'à l'affichage de ce disclaimer, si un périphérique de ce type est déjà branché avant, il ne génèrera pas de popup d'avertissement : il est conseillé de vérifier au démarrage les périphériques branchés à la station.

1.2 Écran principal

Une fois les conditions d'utilisation acceptées, l'écran principal s'affiche :



	Ce bouton lance la fonction Smart-Transfer, qui va réaliser les scans antiviraux et les filtrages avancés (MIME type, clé USB…) sur les fichiers d'entrée avant de réaliser le transfert vers la clé de sortie, cf. chapitre 2.2. À noter : le média USB d'entré doit être branché *avant* de lancer la fonction.
	Ce bouton lance la fonction Scan avec Décontamination. Cette fonction va réaliser les scans antiviraux sans les fonctions de filtrage avancé ni transfert de fichiers, cf2.3. À noter : la clé USB doit être branchée *avant* de lancer la fonction.
	Ce bouton permet d'accéder à la page outils, cf. chapitre 2.
	Ce bouton permet d'accéder à la page des paramètres. Voir le Manuel de l'administrateur
	Ce bouton permet d'afficher l'aide relative aux fonctions principales de la station. Voir chapitre 1.3 pour plus d'informations.
	Ce bouton permet d'accéder à la sélection de la langue de la station. Voir chapitre 1.4 pour plus d'informations.

1.3 Aide à l'utilisation

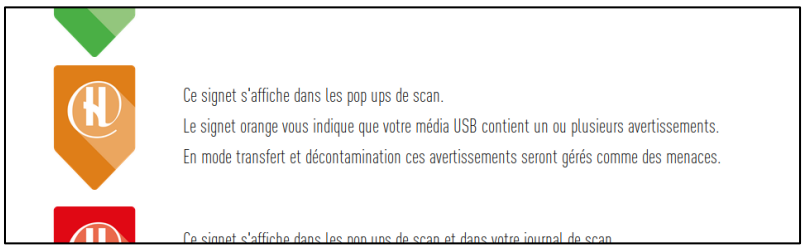
La section Aide à l'utilisation regroupe différents rappels et informations utiles pour comprendre le fonctionnement de la station blanche S3. Elle décrit les principales fonctionnalités accessibles depuis l'écran d'accueil et fournit des indications sur les modes de scan, le transfert de fichiers, la gestion des alertes et la lecture des journaux.



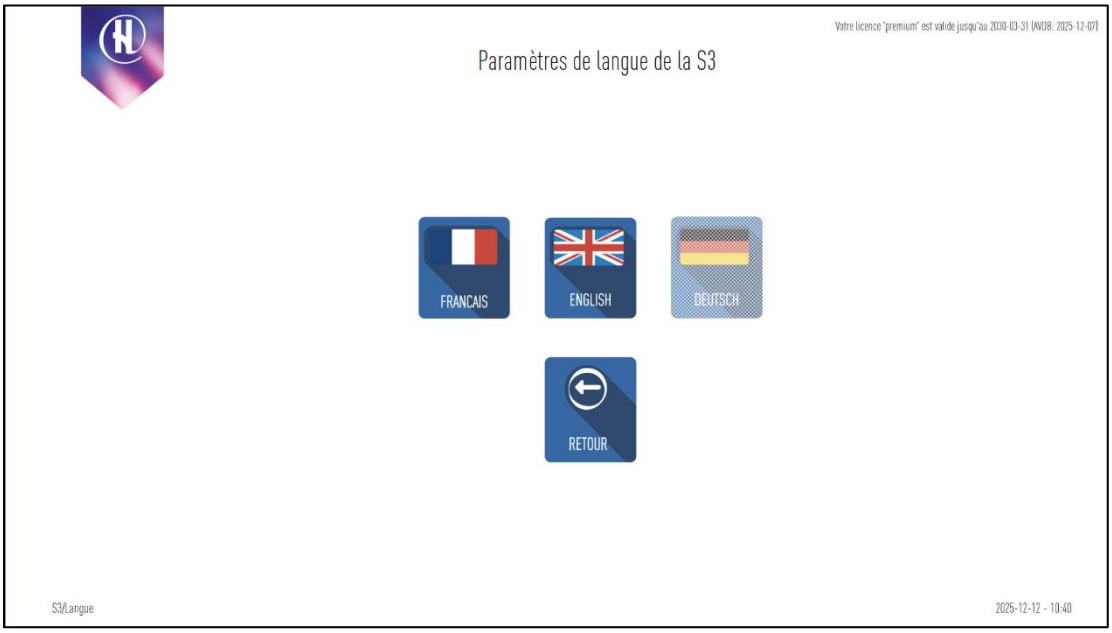
Cette aide vous accompagne dans les actions courantes :

- Choisir le bon mode d'analyse,
- Comprendre les icônes et messages affichés à l'écran,
- Interpréter les résultats d'un scan,
- Savoir quand utiliser le Smart-Transfer ou le mode Décontamination,
- Vérifier la présence d'une menace ou d'un avertissement.

Elle sert également de point de référence si vous découvrez la station pour la première fois ou si vous avez un doute sur la procédure à suivre.
Note : Selon la configuration choisie par votre administrateur, un signet orange peut apparaître sur cet écran.



1.4 Gestion des langues



Cette fenêtre vous permet de modifier la langue utilisée par la station blanche.

Chaque drapeau va relancer l'interface de votre station blanche dans la langue sélectionnée. Cette langue restera active lors des prochains redémarrages.

1.5 Affichage de l'état des supports média

Lors de la connexion d'un support USB, une icône peut apparaître à l'écran afin d'indiquer la présence d'un support de stockage. Deux types d'icônes peuvent être affichés :

- Un indiquant le branchement d'une clé USB
- Un indiquant la présence d'un lecteur de CD

Ces icônes apparaissent en bas de l'écran, au niveau de l'affichage de la date et de l'heure de la station, quel que soit l'écran affiché.



La présence de ces icônes permet de valider la détection de votre support USB avant toute opération lancée sur la station. Leur changement de couleur :

- Signifie que la station est en cours de lecture ou d'écriture sur le média et que la déconnexion prématurée de celui-ci comporte des risques pour l'intégrité des données (hors clé bitlocker).
- Signifie qu'un CD se trouve dans le lecteur. En cas de connexion permanente d'un lecteur CD à la station, cette indication permet de vérifier que le lecteur ne contient plus de disque avant de quitter la station.

Note : Dans certains cas, avec des supports USB spécifiques (par exemple : les clés USB sécurisées), il est possible que les deux icônes apparaissent.

2 Outils S3

2.1 Écran « Outils »



	Ce bouton lance la fonction Smart-Transfer, qui va réaliser les scans antiviraux et les filtrages avancés (MIME type, clé USB…) sur les fichiers d'entrée avant de réaliser le transfert par rupture protocolaire vers le média USB de sortie, cf. chapitre 2.2. À noter : le média USB doit être branché *avant* de lancer la fonction.
	Ce bouton lance la fonction Scan seul (Sans décontamination). Les fichiers infectés ne sont pas supprimés mais l'utilisateur sera informé de leur présence, cf. chapitre 2.3. À noter : le média USB doit être branché *avant* de lancer la fonction.
	Ce bouton lance la fonction Secure File Sharing, et permet le partage des fichiers sur le réseau en fin de scan, au lieu de demander un média USB de sortie, cf. chapitre 2.4. À noter : le média USB doit être branché *avant* de lancer la fonction.
	La fonction de "Formatage" permet de formater une clé USB, cf. chapitre 2.5. À noter : le média USB doit être branché *avant* de lancer la fonction.

	Ce bouton lance la fonction Scan avec Décontamination. Cette fonction va réaliser les scans antiviraux sans les fonctions de filtrage avancé ni transfert de fichiers. Les fichiers infectés sont supprimés, cf. chapitre 2.3. À noter : la clé USB doit être branchée *avant* de lancer la fonction.
	Ce bouton lance la fonction Secure File Sharing, elle permet de récupérer des fichiers depuis un partage réseau, avant de demander une clé USB de sortie, cf. chapitre 2.4.
	Ce bouton permet de revenir à l'écran principal de la station blanche S3, cf. chapitre précédent.
	Ce bouton permet d'afficher l'aide relative aux fonctions principales de la station. Voir chapitre 1.3 pour plus d'informations.
	Ce bouton permet d'accéder à la sélection de la langue de la station. Voir chapitre 1.4 pour plus d'informations.

2.2 Transfert sécurisé avec rupture protocolaire « Smart-Transfer »

2.2.1 Qu'est-ce que le Smart-Transfer ?

Le Smart-Transfer est une fonction permettant le transfert de données d'un média USB à un autre. Les fichiers à transférer sont sélectionnés et décontaminés au préalable.

Si des données sont déjà présentes sur le media de sortie ceux-ci seront supprimés et remplacés par les données transférées.

2.2.2 Lancement du Smart-Transfer

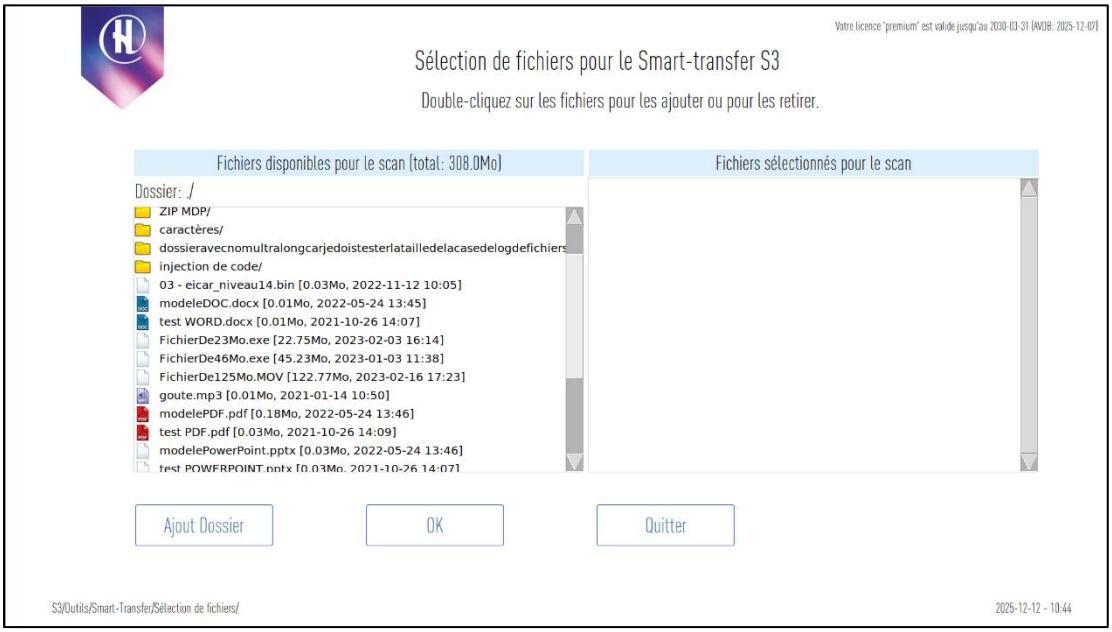
Au lancement du smart transfert l'écran suivant apparait :



Utilisez les boutons « Média » et « Fichiers » pour lancer les modes du Smart-Transfert décrits ci-après.
Le bouton « Annuler » ferme le popup.

2.2.3 Smart Transfert avec Sélection de fichiers

Si le mode « Fichiers » est choisi, l'écran suivant apparait :



La fonction de « sélection de fichiers » affiche les fichiers disponibles sur le média USB connecté dans une zone navigable, à gauche de l'écran :

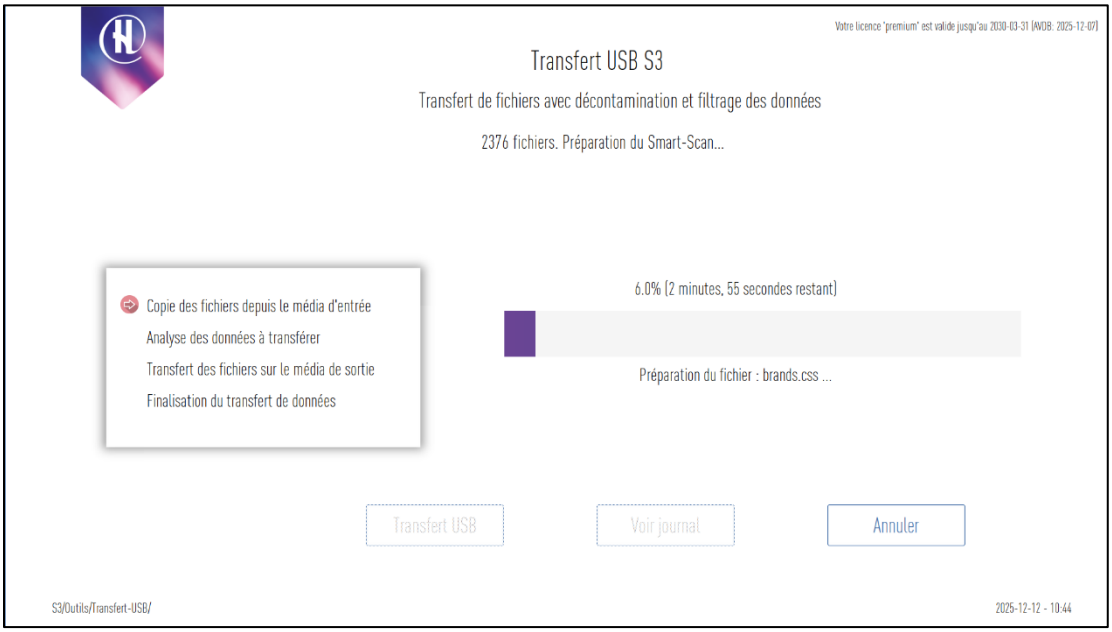
- En double-cliquant sur l'écran, vous pouvez ajouter des entrées à la liste des fichiers à transférer, à droite de l'écran.
- Le bouton « Ajout direct » permet de choisir un fichier ou un dossier sans double-clic (avec un clic simple).
- Enfin, en double cliquant sur un élément de la liste de droite, vous pouvez le supprimer de la liste de sélection.

Une fois la sélection terminée, vous pouvez lancer la fonction Smart-Transfer en cliquant sur le bouton « OK » : Celle-ci se déroule alors normalement, mais en ne considérant que les fichiers explicitement sélectionnés, et non le média USB entier.

Un pop-up indique la fin du scan cf. chapitre 2.2.5

2.2.4 Smart Transfert « Média »

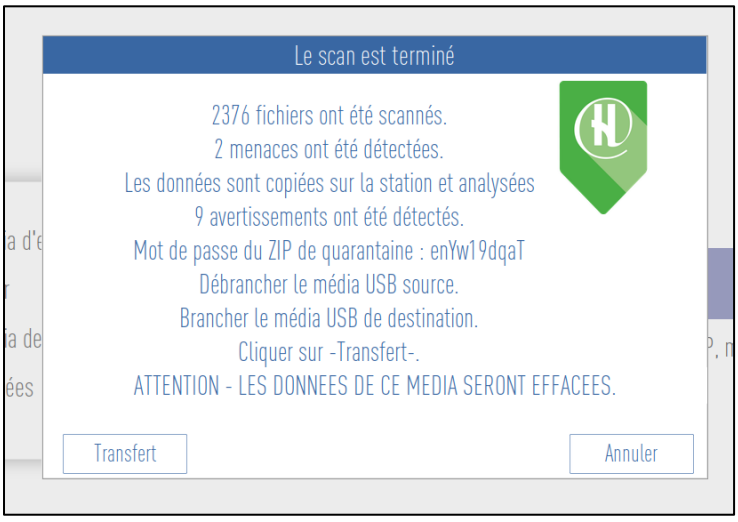
Si le mode « Média » est choisi, l'écran suivant apparait :



Le scan de l'ensemble des données stockées sur le support USB commence.
Un pop-up indique la fin du scan cf. chapitre 2.2.5

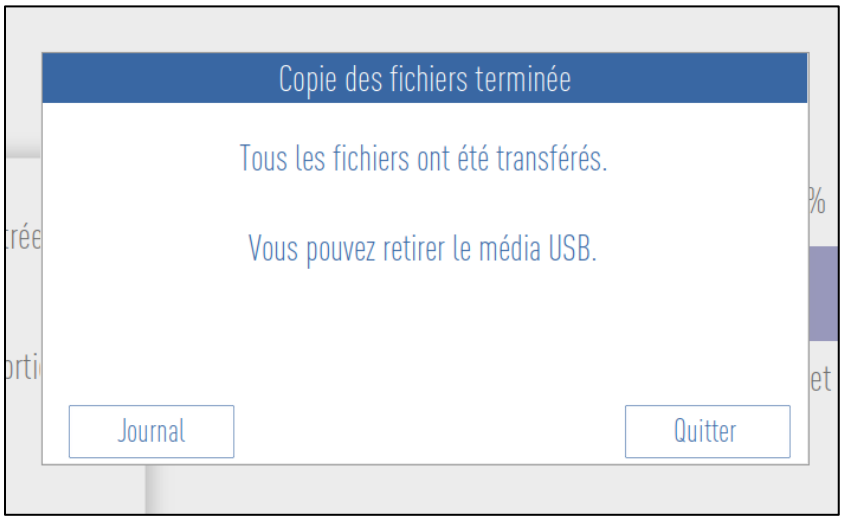
2.2.5 Finalisation du transfert

Le pop-up à la fin du scan indique de débrancher le média de départ et de brancher le média de destination.



2.2.6 Fin du processus et journalisation

A la fin du transfert sur le média de destination un popup apparait pour vous informer que le média peut être débranché.

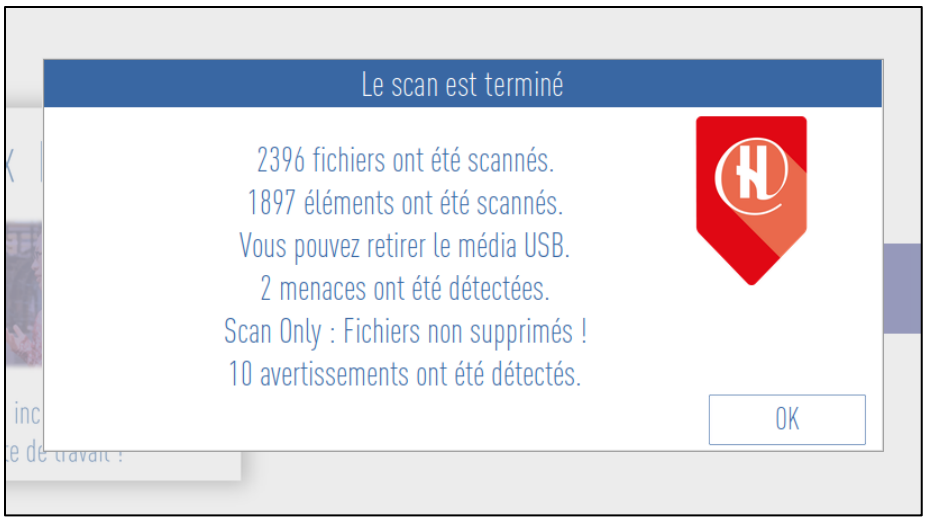


Depuis ce pop-up vous pouvez vous rendre sur le journal de scan (cf. 3) ou quitter la fonction smart-transfert pour retourner sur l'écran principal (cf. 1.2).

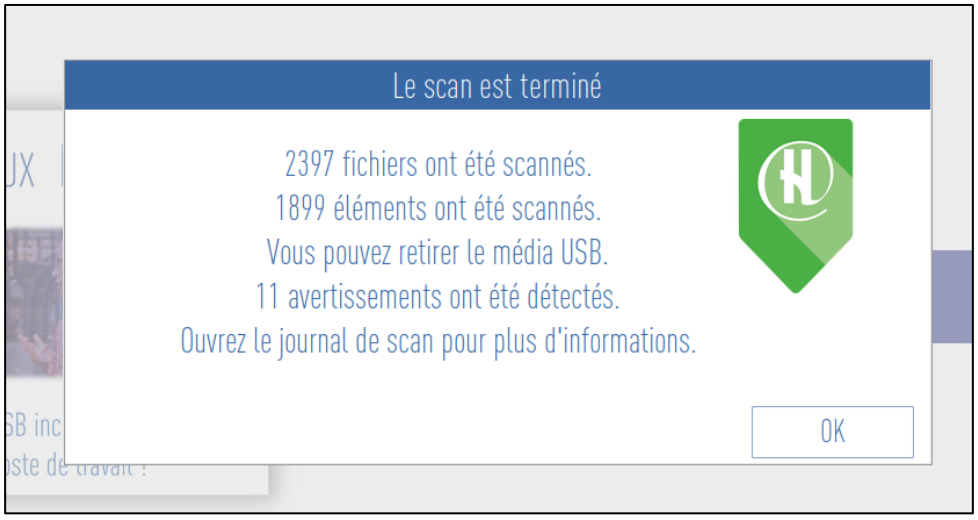
2.3 Scan seul (rapide) et Décontamination



Cette fonction de scan effectue un scan antivirus complet de la clé USB connectée.
En mode « Scan seul », les fichiers infectés ne sont pas supprimés mais l'utilisateur sera uniquement informé de leur présence. Un popup final résume toutes les actions effectuées en fin de scan.

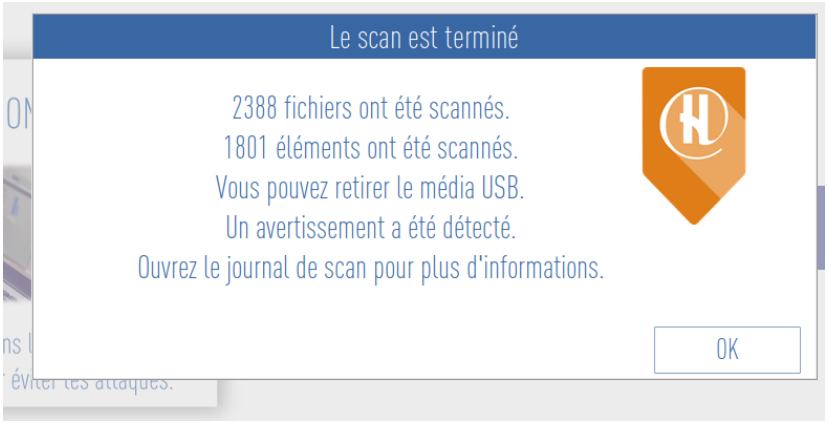


En mode « Décontamination », les fichiers infectés sont supprimés de la clé USB définitivement. Un popup final résume toutes les actions effectuées en fin de scan.



Les fonctions de filtrage avancé (type MIME, certificat…) ne seront pas appliquées.

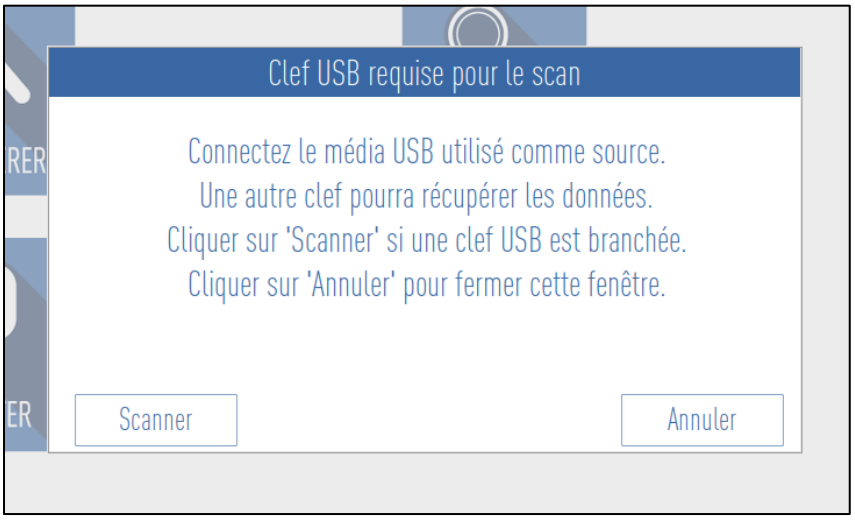
Note : Selon la configuration choisie par votre administrateur, un signet orange peut apparaitre sur le popup, cela signifie que votre clé ne contient pas de menace mais au moins un avertissement. En cas de doute sur la marche à suivre, contactez votre administrateur.



2.4 Scan avec partage de fichiers

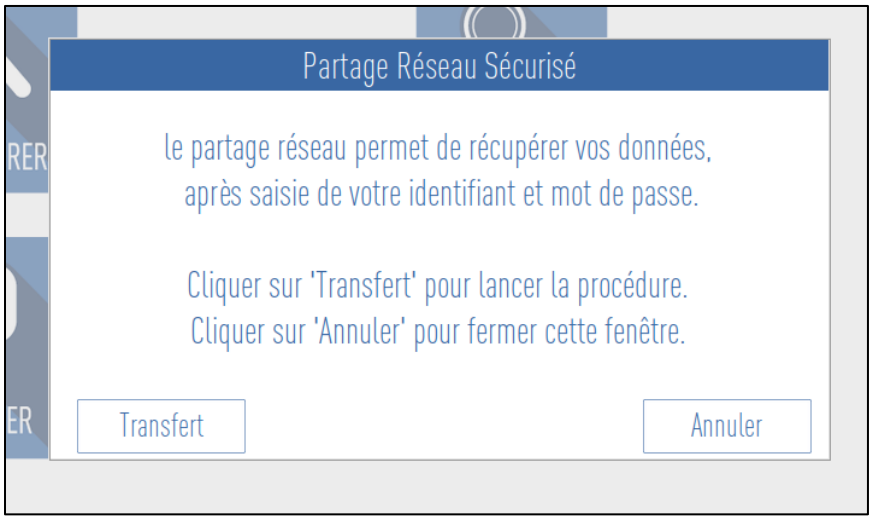
2.4.1 Envoyer

La fonction Envoyer du Scan avec partage de fichiers permet de réaliser une fonction « Smart-Transfer », mais en utilisant le S3SRV à la place du média USB de destination.



2.4.2 Télécharger

La fonction Télécharger du Scan avec partage de fichiers permet de réaliser une fonction « Smart-Transfer », mais en récupérant des fichiers depuis le S3SRV, avant de solliciter une clé USB de sortie.

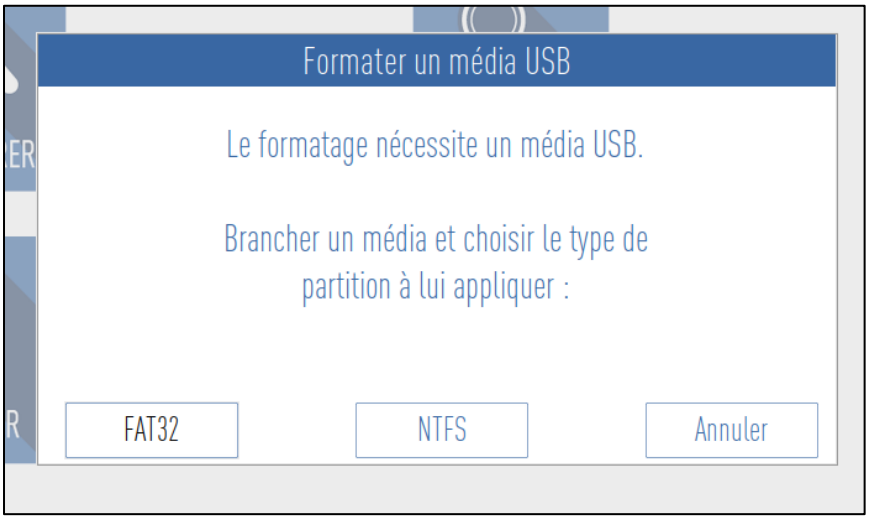

Partage Réseau Sécurisé
le partage réseau permet de récupérer vos données,
après saisie de votre identifiant et mot de passe.
Cliquer sur 'Transfert' pour lancer la procédure.
Cliquer sur 'Annuler' pour fermer cette fenêtre.
Transfert
Annuler

2.5 Formatage de clé USB

La fonction « Formater » vous permet d'effacer complètement le contenu d'un média USB. Cette opération peut être nécessaire avant un transfert ou pour remettre un support dans un état maitrisé.

Au lancement de la fonction plusieurs type pop-up peuvent être affichés en fonction des paramètres choisis par votre administrateur. Suivez les instructions affichées sur votre écran.





Selon la configuration définie par l'administrateur, plusieurs comportements peuvent exister :

- Formatage normal : effacement du contenu et création d'une nouvelle partition.
- Formatage avancé : effacement approfondi avec réécriture sécurisée (plus long).
- Choix du Type formatage.
- Type de partition : FAT32, exFAT ou NTFS selon le paramétrage de la station.

- Choix du Type de partition.

3 Journal de Scan

3.1 Journal de Scan sur la Station



Depuis l'écran de journal de scan, il est possible de consulter le journal, de l'exporter au format HTML (complet ou résumé) ou encore au format JIT (Format chiffré HOGO).

3.2 Journal de Scan exporté

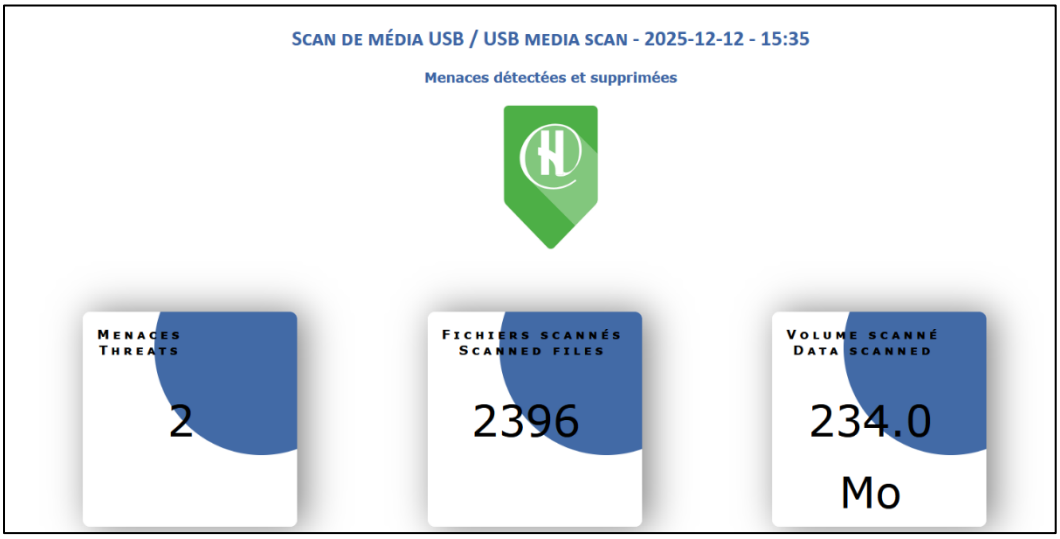
Le journal de scan est divisé en plusieurs sections vous permettant de comprendre rapidement l'état du scan, les informations essentielles et les détails techniques associés.

3.2.1 Résumé des valeurs principales

La première section du journal met en évidence trois indicateurs essentiels :

- Nombre de menaces détectées : indique la quantité de menaces identifiées durant l'analyse.
- Nombre de fichiers scannés : correspond au total des fichiers examinés pendant le scan.
- Volume de données scannées : précise la taille cumulée des fichiers analysés.

Ces informations offrent une vue d'ensemble immédiate sur l'efficacité et l'étendue du scan.

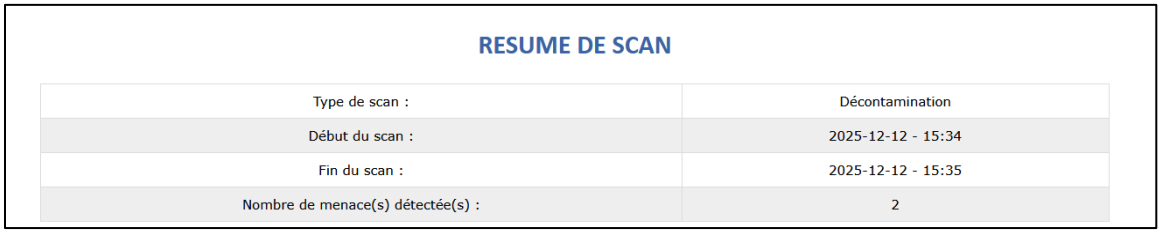


3.2.2 Résumé détaillé du scan

Cette deuxième section fournit un aperçu plus complet du déroulement du scan :

- Type de scan effectué
- Date et heure de début
- Date et heure de fin
- Nombre total de menaces détectées
-

Elle vous permet de situer le scan dans le temps et de connaître les résultats généraux avant de consulter les informations techniques.



RESUME DE SCAN

Type de scan :	Décontamination
Début du scan :	2025-12-12 - 15:34
Fin du scan :	2025-12-12 - 15:35
Nombre de menace(s) détectée(s) :	2

3.2.3 Métriques et indicateurs techniques

Cette section regroupe les données techniques associées au contexte du scan, telles que :

- Version du moteur antivirus (Core)
- Détails et versions des différents moteurs antivirus utilisés
- Informations liées au support USB scanné :
    - Numéro de série (iSerial)
    - Nom du volume
    - Taille de la partition
    - Type de partition
- Statistiques avancées :
    - Taille totale des fichiers analysés
    - Quantité totale de données traitées
    - Nombre d'éléments examinés
    -

Ces informations sont utiles pour la traçabilité et pour des analyses plus approfondies.

METRIQUES ET INDICATEURS

Version du S3Core :	V1.8_build2025111313
Antivirus utilisé(s) :	ClamAV, Eset, McAfee-Trellix
Version globale du(des) Antivirus :	2025-12-07
	1
iSerial du media USB :	6610-721E
Label du media USB :	CLETEST1
Taille de la partition :	29G
Type de partition USB :	vfa
Taille des fichiers analysée:	245433039
Quantité de données scannées :	234.0 Mo
Nombre de fichiers scannés :	2396
Nombre d'éléments scannés :	1895

3.2.4 Versions des moteurs antivirus

Le journal liste ensuite les versions complètes de l'ensemble des moteurs antivirus utilisés.

- Les moteurs et leur version logicielle
- La version de la base de signatures
- Les dates de dernière mise à jour
- Les différents modules internes, leur version et leur numéro de build

Cette section permet de garantir que le scan a été effectué avec des moteurs à jour.

VERSIONS COMPLETE DES MOTEURS

ClamAV 1.0.5/27846/Wed Dec 10 10:28:17 2025
Eset Nod32 Antivirus Engine
ECLS Command-line scanner, version 1.4.0.0, Copyright © 1992-2024 ESET, spol. s r. o. All rights reserved.
Module loader, version 1088 (20250708), build 1162
Module perseus, version 1631.1 (20251105), build 2486
Module scanner, version 32316 (20251207), build 67686
Module archiver, version 1360 (20251117), build 1485
Module advheur, version 1233.1 (20251103), build 1257
Trellix McAfee Antivirus Engine
Command Line Scanner for Linux64 Version: 7.0.2.694

3.2.5 Menaces détectées

Lorsque des menaces sont identifiées, elles apparaissent sous forme de liste contenant généralement :

- Le nom ou la signature de la menace
- L'empreinte hash (ex. : SHA256)
- Le ou les emplacement(s) concerné(s) sur le support USB
-

Chaque menace est présentée de manière suffisamment détaillée pour permettre une analyse ou une action corrective.

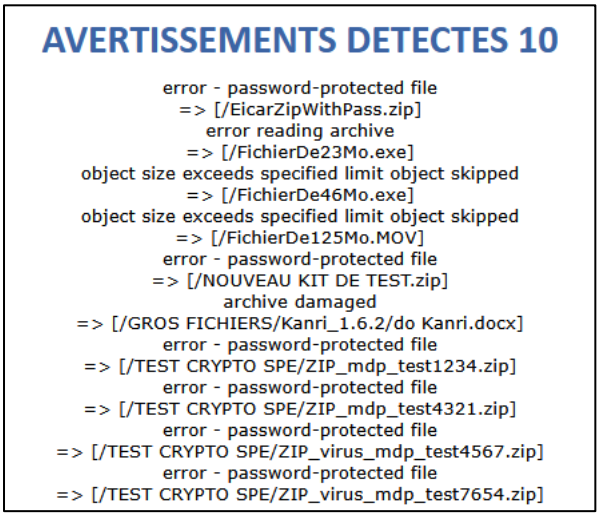


3.2.6 Avertissements détectés

Les avertissements indiquent les éléments que les moteurs n'ont pas pu analyser.
Ils peuvent concerner, par exemple :

- Des fichiers protégés par mot de passe
- Des archives endommagées
- Des fichiers dépassant la limite de taille autorisée
- Des objets non reconnus ou non pris en charge

Chaque avertissement est accompagné de l'élément concerné.

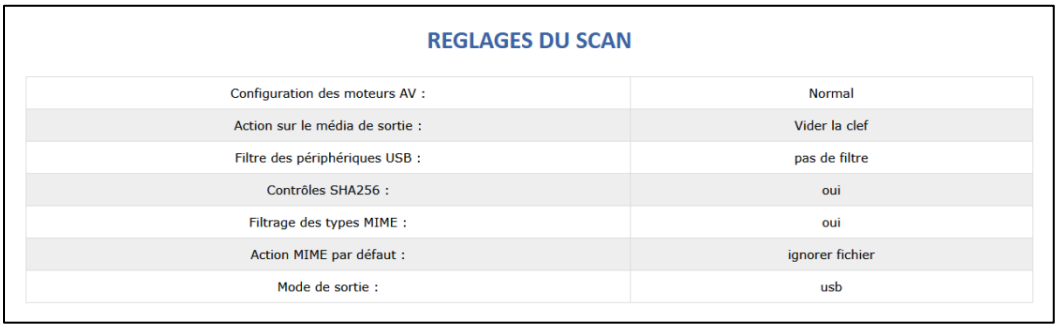


3.2.7 Réglages du scan

Cette section indique la configuration active au moment du scan, tels que :

- Mode de configuration des moteurs antivirus
- Action à appliquer au média de sortie
- Présence ou non d'un filtre USB
- Activation des contrôles SHA256
- Activation du filtrage MIME
- Action par défaut appliquée aux types MIME inconnus
- Mode de sortie sélectionné

Elle vous permet de vérifier le contexte opérationnel du scan effectué.

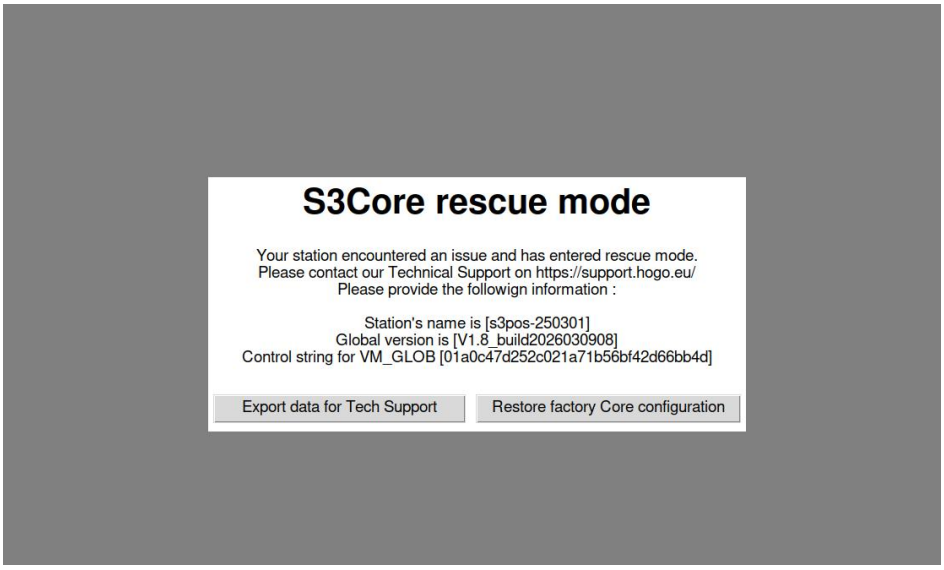


REGLAGES DU SCAN

Configuration des moteurs AV :	Normal
Action sur le média de sortie :	Vider la clef
Filtre des périphériques USB :	pas de filtre
Contrôles SHA256 :	oui
Filtrage des types MIME :	oui
Action MIME par défaut :	ignorer fichier
Mode de sortie :	usb

4 S3Core Rescue mode

Si cet écran apparaît au démarrage de la station, contactez immédiatement votre administrateur.



5 Bonnes pratiques d'utilisation

Pour garantir une utilisation correcte de la station blanche S3, respectez les bonnes pratiques suivantes :

- ➔ Insérez toujours la clé USB complètement avant de commencer un scan.
- ➔ Ne retirez jamais un média pendant l'analyse ou la copie.
- ➔ Attendez systématiquement le message de fin de scan avant de débrancher votre clé.
- ➔ Utilisez uniquement des supports USB en bon état.
- ➔ Vérifiez régulièrement les messages affichés par la station.
- ➔ Lisez attentivement les alertes ou avertissements avant de poursuivre.
- ➔ En cas de doute, répétez le scan ou contactez votre administrateur.
- ➔ Après une décontamination, vérifiez que les fichiers attendus sont bien présents sur la clé de sortie.
- ➔ Ne tentez jamais de contourner les réglages administrateur : ils garantissent votre sécurité.