Hogo S3

Manuel Utilisateur v3.4

Versions s3Core V1.8 (2023-09) et supérieures

2023

Ce document décrit l'utilisation des fonctions principales de la gamme S3 de Hogo, et donne des indications aux utilisateurs. Il suit un déroulement basé sur l'IHM du produit, et se concentre sur l'expérience utilisateur.

Table des matières

1 Introduction 2
1.1 Fonctionnalités de la gamme S3 2
1.2 Installation des équipements 3
2 Interface principale – Accueil 5
2.1 Conditions d'utilisation 5
2.2 Ecran principal 6
2.3 Gestion des langues 6
3 Outils S3 7
3.1 Ecran « Outils » 7
3.2 Smart Transfer 8
3.3 Sélection des fichiers à scanner 11
3.4 Scan seul (rapide) et Décontamination 11
3.5 Scan avec partage de fichiers 11
3.6 Synchronisation de partage de fichiers 12
3.7 Scan avec Certificat de sécurité 12
3.8 Scan de téléphone 12
3.9 Formatage de clef USB 13
4 Paramètres généraux 14
4.1 Paramètres des outils 15
4.2 Mise à jour 19
4.3 Ecran de connexion – Fonctions d'administration 23
4.4 Réglage de la date 23
4.5 Ecran de veille 24
4.6 Logs 25

1 Introduction

1.1 Fonctionnalités de la gamme S3

La gamme Smart Secure Sanitizer “S3” est une solution de Stations Blanches USB, visant à protéger votre Système d’Information sensible contre les périphériques USB infectés :

- Protéger votre système d’information contre les périphériques contaminés ou dangereux,
- Importer des données vers votre système sensible sans connexion directe du périphérique,
- Scanner et filtrer vos données d’entrée (avec jusqu’à 5 antivirus et des contrôles MIME, PGP…)
- Utiliser seulement les clefs du parc autorisé de l’entreprise -filtrage des clefs par Serial-,
- Eviter toute fuite d’information ou l’entrée de données non-autorisées dans votre système.

Cette gamme est composée des stations blanches suivantes :

- S3Box : tablette durcie, mobile et résistante aux chocs
- S3Pos : poste monobloc, à disposer sur un bureau par exemple
- S3Tot : poste totem autoporteur



S3Box



S3Pos



S3Tot

Ce document décrit l’utilisation des fonctions principales de la gamme S3, et donne des indications aux utilisateurs. Il suit un déroulement basé sur l’IHM du produit, et se concentre sur l’expérience utilisateur et non sur les mécanismes sous-jacents.

A noter : les captures d’écran proposées ci-après sont extraites de l’interface d’une S3Box, mais les interfaces des trois solutions de la gamme S3 sont organisées de la même manière.

1.2 Installation des équipements

1.2.1 Caractéristiques physiques des équipements

Les équipements de la gammes S3 concernés par ce manuel nécessitent une source d'alimentation électrique pour fonctionner. Les caractéristiques de cette source d'alimentation sont les suivantes :

- **S3Box** : Branchement du chargeur fourni avec la station sur secteur (230V en courant alternatif en 50Hz) pour une alimentation en sortie de chargeur en 5V en courant continu.
- **S3Pos** : Branchement du transformateur fourni avec la station sur secteur (230V en courant alternatif en 50Hz) pour une alimentation en sortie de transformateur en 19V en courant continu.
- **S3Tot** : Uniquement branchement du câble à l'arrière du totem sur secteur (230V en courant alternatif en 50Hz).

Les plages de puissance nominalement consommées par les équipements sont ls suivantes :

- **S3Box** : 5 Watts (au repos) à 12 Watts (en activité, typiquement en scan de média USB)
- **S3Pos** : 20 Watts (au repos) à 90 Watts (en activité, typiquement en scan de média USB)
- **S3Tot** : 30 Watts (au repos) à 110 Watts (en activité, typiquement en scan de média USB)

Enfin, la température interne de fonctionnement de ces trois équipements doit être comprise entre 0°C et 50°C à tout moment.

1.2.2 Mise en place des équipements

Pour installer un équipement de la gamme S3, il convient de respecter les consignes ci-après :

1. **Préparation du lieu d'accueil**
   - Choisir un espace propre et dégagé, adapté à la taille / au nombre d'équipements à mettre en place.
   - Choisir une surface stable et non statique pour éviter tout dommage électrique aux équipements.
2. **Déballage du matériel**
   - Retirer délicatement l'équipement S3 de sa boîte de transport et la placer sur la surface d'accueil.
   - Si des périphériques externes supplémentaires sont nécessaires (par exemple, une imprimante, un lecteur de badge), les connecter aux ports appropriés.
3. **Alimentation électrique**
   - Connecter le chargeur fourni avec la S3Box, ou le transformateur fourni avec le S3Pos, à sa prise du côté de l'équipement S3 (passer l'étape pour le S3Tot).
   - Brancher le câble d'alimentation à l'arrière du S3Tot, ou l'autre extrémité du chargeur ou du transformateur, à une prise secteur munie d'une fiche de mise à la terre.
4. **Mise sous tension**
   - Appuyer sur le bouton « power » de la S3Box, ou enclencher l'interrupteur arrière du S3Pos, pour le démarrer (pas d'action sur le S3Tot, qui démarrera lors du branchement électrique).
   - Suivre les instructions éventuellement à l'écran pour la configuration initiale (les équipement sont habituellement préconfigurés, mais des questions peuvent apparaître au premier démarrage).

1.2.3 Consignes de sécurité

Veiller à suivre les consignes de sécurité suivantes lors de l'installation et de l'usage de l'équipement S3 :

- **Éviter l'électricité statique :**
  L'électricité statique peut endommager les composants internes. Touchez un objet métallique non peint avant de manipuler les composants internes ou les câbles lors des branchements, pour vous décharger de toute électricité statique.

- **Ne jamais forcer les connexions :**
  Si un câble ou un périphérique ne semble pas s'adapter naturellement, ne forcez pas. Vérifiez que vous utilisez le bon port ou le bon câble.

- **Alimentation électrique :**
  Utilisez toujours un câble d'alimentation en bon état. Évitez d'utiliser des câbles endommagés ou effilochés.

- **Garder les liquides à distance :**
  Évitez de placer des boissons ou autres liquides près de votre équipement S3 pour éviter tout risque de déversement.

- **Ventilation :**
  Assurez-vous que l'équipement est placé dans un endroit où il peut être correctement ventilé. Évitez de bloquer les ouvertures d'aération pour éviter une surchauffe.

- **Mise à jour et entretien :**
  Pour garantir la sécurité et la performance de votre équipement, effectuez régulièrement des mises à jour logicielles et vérifiez sa propreté (par exemple, enlèvement de la poussière).

1.2.4 Avertissements complémentaires

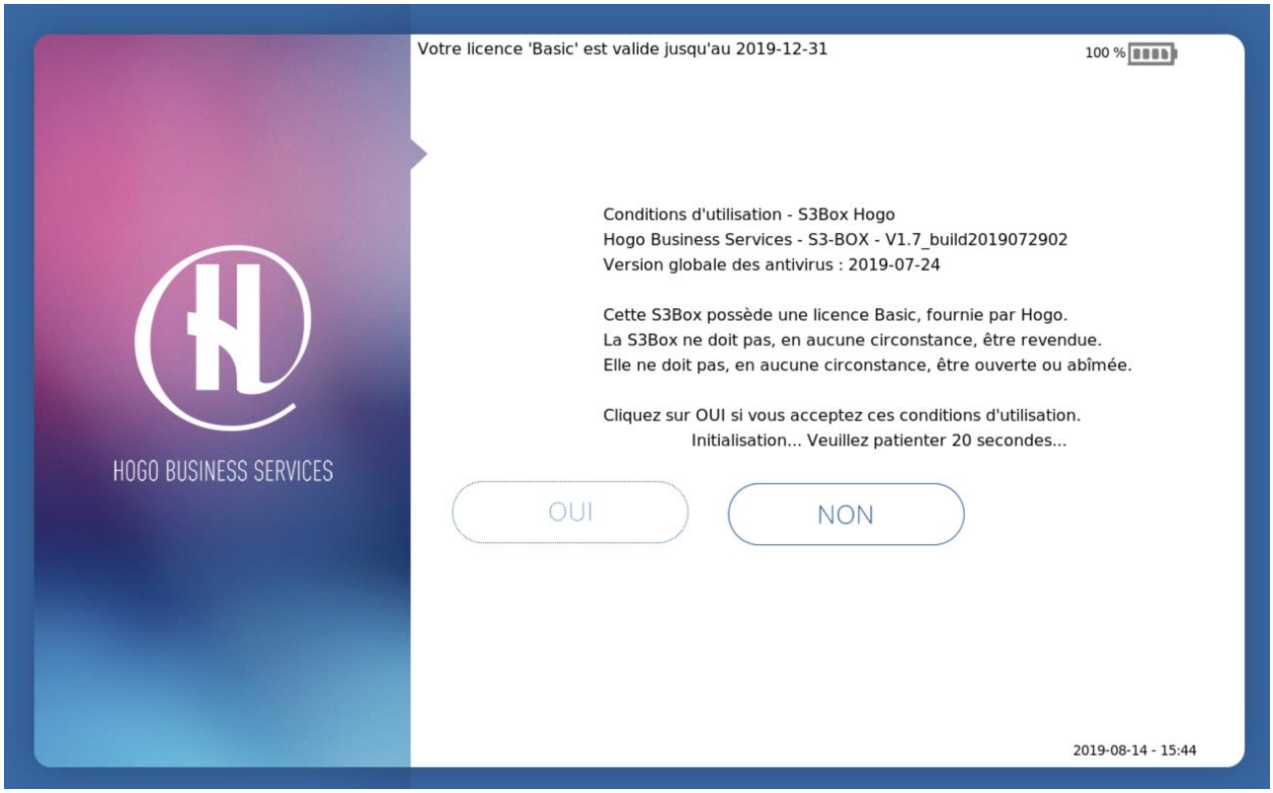
Attention, les équipements de la gamme S3 ne conviennent pas à une utilisation dans des lieux pouvant accueillir des enfants.

Attention, le cordon d'alimentation des équipements constitue leur dispositif de déconnexion électrique, ils doivent être facilement accessibles aux opérateurs à tout moment.

2 Interface principale – Accueil

2.1 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.

A 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.

2.2 Ecran principal

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

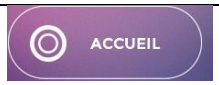
	Ce bouton lance la fonction Smart-Transfer, qui va réaliser les scans antiviraux et les filtrages avancés (MIME type, clef USB…) sur les fichiers d'entrée avant de réaliser le transfert vers la clef de sortie. Les détails concernant cette fonction sont donnés au chapitre 3.2. A noter : la clef USB doit être branchée *avant* de lancer la fonction.
	Ce bouton lance la fonction Scan-Only (scan seul, rapide). Cette fonction va réaliser les scans antiviraux sans les fonctions de filtrage avancés ni transfert de fichiers. Les détails concernant cette fonction sont donnés au chapitre 3.4. A noter : la clef USB doit être branchée *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 avancés ni transfert de fichiers. Les détails concernant cette fonction sont donnés au chapitre 3.4. A noter : la clef USB doit être branchée *avant* de lancer la fonction.
[Plus d'Outils]	Ce bouton permet d'accéder aux fonctions de SCAN/TRANSFERT et aux outils USB ; voir chapitre 3 pour plus d'information.
[Paramètres]	Ce bouton permet d'accéder aux fonctions de paramétrage et de mise à jour ; voir chapitre 4 pour plus d'information.
[Aide]	Ce bouton permet d'afficher l'aide relative aux fonctions principales de la station blanche S3.
	Ce bouton redémarre la station blanche S3.
	Ce bouton éteint la station blanche S3.

2.3 Gestion des langues

Cette fenêtre vous permet de modifier la langue utilisée par la station blanche S3.
Chaque drapeau va relancer l'interface de votre station blanche S3 dans la langue sélectionnée.
Cette langue est stockée en mémoire pour être également active lors des prochains redémarrages.

3 Outils S3

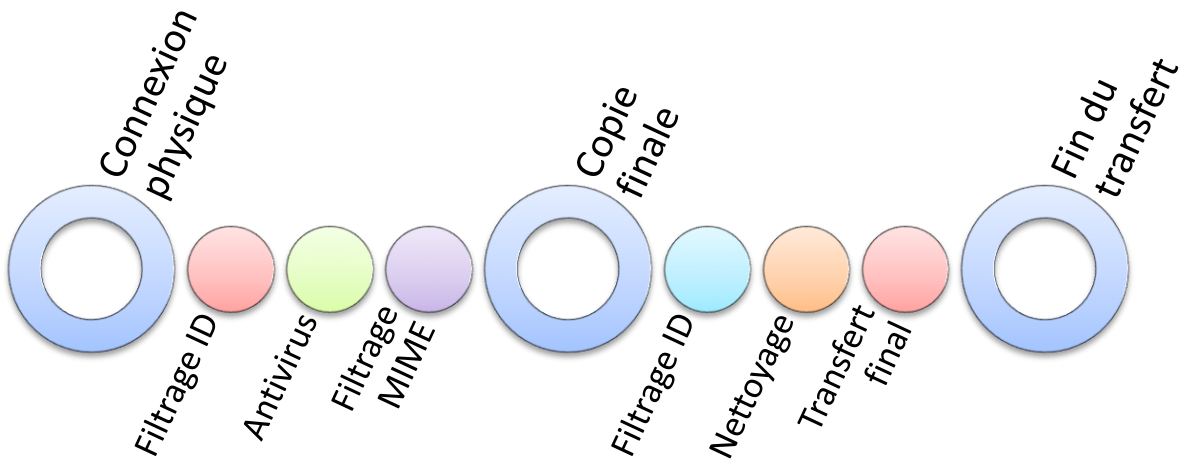
3.1 Ecran « Outils »

	Ce bouton lance la fonction Smart-Transfer, et permet la sélection des fichiers à scanner. Les détails concernant cette fonction sont donnés au chapitre 0. A noter : la clef USB doit être branchée *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 avancés ni transfert de fichiers. Les détails concernant cette fonction sont donnés au chapitre 3.4. A noter : la clef USB doit être branchée *avant* de lancer la fonction.
	Ce bouton lance la fonction Smart-Transfer, et permet le partage des fichiers sur le réseau en fin de scan, au lieu de demander une clef USB de sortie. A noter : la clef USB doit être branchée *avant* de lancer la fonction.
	Ce bouton lance la fonction Smart-Transfer, mais permet de récupérer des fichiers depuis un partage réseau, avant de demander une clef USB de sortie.
	Ce bouton lance la fonction Smart-Transfer, mais permet la sélection des fichiers à scanner et la sélection des certificats à utiliser pour vérifier leurs signatures. A noter : la clef USB doit être branchée *avant* de lancer la fonction.
	Ce bouton lance la fonction Scan (scan seul, rapide) qui va réaliser les scans antiviraux sans les fonctions de filtrage avancés ni transfert de fichiers sur un téléphone Android connecté.
	La fonction de “Formatage” permet de formater une clef USB. A noter : la clef USB doit être branchée *avant* de lancer la fonction.
	Ce bouton permet de revenir à l’écran principal de la station blanche S3, cf. chapitre 0.

3.2 Smart Transfer

3.2.1 Fonctionnement global

Cette fonction de Scan réalise un contrôle antiviral sur les fichiers d'entrée, un filtrage des fichiers selon les paramètres de la station blanche S3, et une sortie de ces fichiers sur un support externe.



La première étape consiste à récupérer les fichiers depuis une clef USB, puis de les traiter :

- Premièrement, le scan vérifie si une clef USB d'entrée est connectée.
    - Si cela n'est pas le cas (ou, si l'option de contrôle des périphériques USB d'entrée est activée et que le périphérique branché n'est pas autorisé), la fonction s'arrête.
- Ensuite, la station blanche S3 est préparée (vérifications internes et des fichiers) pour le scan, puis :
    - Le(s) moteur(s) antiviral/ux installé(s) réalise(nt) la validation des fichiers,
    - Les fichiers sont filtrés (si l'option correspondante est activée) selon les règles de type MIME enregistrés,
- Enfin, les fichiers sont copiés dans un répertoire spécifique de la station blanche S3, et l'IHM informe l'utilisateur qu'il peut retirer la clef USB d'entrée et brancher la clefs USB de sortie.

La deuxième étape consiste à restituer les fichiers traités sur une clef USB de sortie :

- Une fois le bouton « End of Transfer » activé, la fonction vérifie si une clef de sortie est connectée.
    - Si cela n'est pas le cas (ou, si l'option de contrôle des périphériques USB d'entrée est activée et que le périphérique branché n'est pas autorisé), la fonction s'arrête.
- Ensuite, la clef USB de sortie est contrôlée (espace disponible…), les fichiers sont copiés sur celle-ci, et les fichiers présents sur la station blanche sont supprimés (pas de persistance de données) ;
- Enfin, l'utilisateur est averti que le transfert est terminé et qu'il peut retirer la clef USB de sortie et quitter la fonction Smart-Transfer.

3.2.2 Information de l'utilisateur

Un popup avertira l'utilisateur qu'une clef USB doit être connectée **avant** le lancement de la procédure de scan. Un popup final donnera les informations de traitement résumée à l'utilisateur

En fin de procédure, une fenêtre « Journal » permettant d'accéder aux résultats de scan est affichable par l'utilisateur. Elle contient le résumé des réglages de scan (date et heure, serial de la clef utilisée en entrée, etc.) et des actions réalisées (traitement des fichiers, verdict du/des moteur/s antivirus, etc.).

Ce journal ne peut être consulté qu'à la suite du scan, ou plus tard sur une console de gestion MyHogo (stations connectées à Internet ou à un serveur Hogo local). Comme tous les journaux, ils peuvent également être exportés en Syslog (cf. 4.6.2) ou sur clef USB dans des fichiers chiffrés/signés (cf. 4.5).

A noter : Lors de son affichage à l'écran, ce journal peut être tronqué s'il contient un trop grand nombre de lignes, pour garder un affichage lisible. Le résumé de scan est toujours affiché, et le contenu complet reste accessible sur la console de gestion ou le puit Syslog.

3.2.3 Précisions de fonctionnement

Il est obligatoire de changer de clef USB entre l'entrée de données et la sortie de données (les clefs d'entrée et de sortie ne peuvent pas être identiques).

L'utilisation du disque dur de la station blanche comme zone de rebond implique une limite sur la taille des fichiers transférables : il est impossible de transférer plus de données que l'espace disponible sur la station au moment du Smart Transfer.

La sensibilité à la casse n'est pas supportée par toutes les partitions : certains fichiers peuvent être écrasés sur la clef de sortie s'ils ont des noms identiques en milieu insensible à la casse (file.txt / FILE.txt).

Certains systèmes de fichiers ne supportent pas toutes les tailles de fichiers : e.g. limite à 4Go pour le système FAT32[1]. La station interdira les transferts vers ce type de clef si des fichiers trop volumineux sont présents. Il est également possible que certains fichiers soient perdus lors de la copie finale.

Tous les systèmes de fichiers ne gèrent pas les permissions de manière identique : pour éviter les problèmes de compatibilité post Smart Transfer, les droits des fichiers sur la clef de sortie sont donc positionnés sur l'équivalent du code Linux 777.

[1] Etant donné l'obsolescence des formats antérieur type FAT16, ceux-ci ne sont pas discriminés : il reste donc un risque de perte de données dans ce type de cas d'usage. Hogo déconseille donc fortement d'utiliser ces formats de clef, sauf éventuellement si la clef d'entrée est dans ce même format de partition.

3.2.4 Avertissements liés à l'usage

3.2.4.1 Traitement des fichiers polyglottes

Un fichier polyglotte est conçu pour être interprété comme plusieurs types de fichiers différents selon le contexte, ce qui lui permet de se masquer comme un type de fichier inoffensif tout en dissimulant potentiellement un code malveillant.

Ces fichiers peuvent donc contourner les mécanismes de filtrage basés sur le type MIME et, parfois échapper à la détection par des moteurs antiviraux.

La fonction de Smart-Transfer peut ne pas détecter les fichiers polyglottes, Hogo recommande donc une attention particulière aux fichiers susceptible d'héberger ce type de masquage : GIF (polyglotte GIFAR), JPG (polyglotte JPG+PHP), vidéo (polyglotte MP4+JS)…

3.2.4.2 Traitement des masquages par stéganographie

La stéganographie est une technique permettant de dissimuler des informations (comme du texte ou du code) à l'intérieur d'autres fichiers, tels que des images ou des fichiers audios, de manière à ce que la présence de ces informations cachées ne soit pas détectable.

Cette technique peut être utilisée pour masquer des données malveillantes ou sensibles, rendant ces fichiers potentiellement dangereux tout en apparaissant comme inoffensifs.

La fonction de Smart-Transfer peut ne pas détecter les masquages par stéganographie, Hogo recommande donc une attention particulière aux fichiers susceptible d'héberger ce type de masquage : images, fichiers audios…

3.3 Sélection des fichiers à scanner

La fonction de « sélection de fichiers » va afficher les fichiers disponibles sur la clef USB connectée dans une zone navigable, à gauche de l'écran :

- En double-cliquant sur l'écran, l'utilisateur pourra ajouter des entrées à la liste des fichiers à scanner, 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, l'utilisateur pourra supprimer un élément de la liste de sélection

Une fois la sélection terminée, l'utilisateur lance 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 la clef USB entière.

3.4 Scan seul (rapide) et Décontamination

Cette fonction de scan effectue un scan antivirus complet de la clef USB connectée. Tous les fichiers seront scannés, et les résultats de scan seront affichés à l'écran (chaque session de scan entraîne la création d'un journal, se référer au chapitre 3.2.2).

En mode « Scan seul », les fichiers infectés ne sont pas supprimés mais l'utilisateur sera uniquement informé de leur présence. En mode « Décontamination », les fichiers infectés sont supprimés de la clef USB. Un popup final résume toutes les actions effectuées en fin de scan.

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

En mode décontamination, les fichiers infectés par des virus sont supprimés. En mode « scan seul », ils sont conservés sur la clef (il s'agit d'un scan informatif dans ce dernier cas).

3.5 Scan avec partage de fichiers

Le Scan avec partage de fichiers permet de réaliser une fonction « Smart-Transfer », mais en utilisant un serveur de partage réseau à la place de la clef USB de destination.

Ce serveur de partage doit être un serveur S3SRV fourni par Hogo. La connexion à ce S3SRV (IP, codes de communication, etc.) peut être configuré sur l'interface de paramétrage de la station blanche S3.

L'utilisation est similaire à la fonction Smart-Transfer, mais en fin de traitement, un popup informe l'utilisateur du statut de son partage, et lui communique les identifiants / mot de passe à utiliser pour récupérer ses fichiers en ligne depuis le S3SRV.

3.6 Synchronisation de partage de fichiers

La Synchronisation de partage de fichiers permet de réaliser une fonction « Smart-Transfer », mais en utilisant un serveur de partage réseau à la place de la clef USB source.

Ce serveur de partage doit être un serveur S3SRV fourni par Hogo. La connexion à ce S3SRV (IP, codes de communication, etc.) peut être configuré sur l'interface de paramétrage de la station blanche S3.

L'utilisation est similaire à la fonction Smart-Transfer, mais en début de traitement, l'utilisateur doit fournir son identifiant / mot de passe à utiliser pour récupérer ses fichiers depuis le S3SRV, avant de les traiter et de les restituer sur sa clef USB de destination.

3.7 Scan avec Certificat de sécurité

La fonction de scan avec certificat de sécurité permet de vérifier, en plus des traitements habituels de la fonction Smart-Transfer, la signature PGP des fichiers d'une clef USB.

L'utilisateur doit sélectionner le (ou les) certificats PGP enregistrés dans son gestionnaire de certificat (cf. chapitre 4.1.3 – au moins un certificat doit être sélectionné, ou le scan est annulé), puis sélectionner un ou plusieurs fichier(s) et signature(s) de la clef USB d'entrée.

Cette fonction va récupérer sur la clef USB d'entrée les signatures ainsi que les fichiers à vérifier, et chercher si ces fichiers et ces signatures sont bien concordants. Elle se base pour cela sur une librairie de certificats PGP enregistrés dans la station blanche S3.

Seuls les fichiers validés (i.e. dont la signature est présente, nommée -nom_du_fichier.sig-, et est correctement vérifiée) sont alors transférés dans le cadre du Smart-Transfer. Les fichiers sans signatures sur la clef d'entrée ou avec une signature incorrecte ne sont pas transférés.

A noter : le fichier signature « .sig » ne doit contenir que le bloc de signature PGP du fichier associé, au format « armor [human-readable] » (codé en ASCII). L'ajout d'une chaine de caractère dans le fichier de signature entraînera l'échec de la vérification de signature PGP.

3.8 Scan de téléphone

Cette fonction est équivalente à la fonction « Décontamination », mais prend en charge les téléphones Android (implémentant le protocole MTP) au lieu des clefs USB.

3.9 Formatage de clef USB

Lorsque cette fonction est lancée, les actions suivantes sont réalisées :

- Les partitions éventuellement présentes sur la clef USB sont supprimées,
- Les fichiers sont supprimés également,
- Si le mode “Avancé” est activé, la clef USB est réécrite avec des octets aléatoires, puis vidée à nouveau,
- Une nouvelle partition est enfin créée (FAT32, exFAT ou NTFS selon l’option choisie dans l’écran de paramétrage des outils).

Le détail de ces étapes (i.e. messages Shell) est stocké dans le log de Formatage.

Cette IHM est relativement simple, l’utilisateur ne peut qu’attendre que le formatage soit réalisé puis cliquer sur le bouton « Quitter » pour revenir à l’écran « Outils » (cf. chapitre 3.1).

A noter :

- Un écran d’accueil avertira l’utilisateur qu’une clef USB doit être connectée **avant** le lancement de la fonction de formatage ;
- Si la clef USB est retirée pendant les actions de formatage, elle pourrait être définitivement inutilisable. De plus, la station blanche S3 pourrait être corrompue et nécessiter une maintenance lourde (i.e. retour usine à Hogo).

4 Paramètres généraux

Cet écran est accessible, après saisie de mot de passe, depuis l'écran d'accueil, en cliquant sur « Paramètres ». Les fonctions accessibles sont :

	Ce bouton permet de mettre à jour les moteurs antiviraux ou les logiciels embarqués dans la station blanche S3 (voir chapitre 4.2).
	Ce bouton permet de gérer les paramètres des outils de la station blanche S3 (voir chapitre 4.1).
	Ce bouton permet de visualiser et d'exporter les logs de la station blanche S3 (voir chapitre 4.5).
	Ce bouton permet de régler la date et l'heure de la station blanche S3 (voir chapitre 4.4).
	Ce bouton permet de changer le mot de passe d'administration de la station blanche S3 (mot de passe demandé pour accéder au paramétrage (voir chapitre 4.3).
	Ce bouton permet de configurer le serveur de partage de fichier S3SRV
	Ce bouton permet d'accéder à la gestion des langues, voir paragraphe suivant.

***A noter** : dans le menu de paramétrage, chaque écran / sous écran se ferme sans activité de l'utilisateur pendant plus de 10 minutes (sauf en cas d'action en cours par le système, comme une mise jour).*

4.1 Paramètres des outils

Cet écran est accessible depuis les « Paramètres ». Les fonctions accessibles sont :

	Ce bouton permet de lancer le manager USB (gestion des clefs USB autorisées) (voir chapitre 4.1.1).
	Ce bouton permet de lancer le paramétrage du filtrage (type MIME…) (voir chapitre 4.1.2).
	Le gestionnaire de certificats permet de gérer la fonction “Scan avec certificat de sécurité” et la liste des certificats disponibles dans la station blanche S3.
	Ce bouton permet de lancer le paramétrage du lecteur de badge, si la station en est équipée.
	Ce bouton permet de revenir à l’écran précédent.

4.1.1 Gestionnaire de clefs USB

Les boutons suivants peuvent être utilisés après saisie du code d’administration de la station blanche S3 :

[Voir la liste USB] Affiche les clefs autorisée (iSerial) sur cette station blanche S3,

[Ajouter à la liste] Si une clef USB est branchée cette fonction l’ajoute à la liste des clefs autorisées,

[Supprimer] Si une clef USB est branchée cette fonction la supprime de la liste des clefs autorisées,

[Vider la liste] La liste des clefs autorisées est remise à zéro,

[Quitter] Retourne à l’écran précédent.

A noter : les ID des clefs USB sont représentatives d’une partition. Cela signifie que la station blanche S3 peut gérer les clefs USB multi-partitionnées. Hogo recommande de garder les clefs USB sensibles de manière sécurisée, pour éviter que leurs IDs de partition soient compromis ou dupliqués.

4.1.2 Paramètres de filtrage

Les options suivantes sont disponibles :

- **Action pour les types MIME inconnus**
  - Isole les fichiers dont le type MIME est inconnu,
  - Ne copie pas les fichiers dont le type MIME est inconnu,
  - Copie les fichiers dont le type MIME est inconnu.

- **Filtrage MIME intelligent (Smart MIME)**
  - “Oui” activera le filtrage des types MIME lors de l’utilisation du Smart-Transfer ;
  - “Non” désactivera le filtrage des types MIME.

- **Filtrage des clefs USB**
  - Autorise toutes les clefs USB, sans filtrage ;
  - Utilise les clefs USB d’entrée autorisées seulement ;
  - Utilise les clefs USB de sortie autorisées seulement ;
  - Utilise les clefs USB d’entrée et de sortie autorisées seulement.

  A noter : Les clefs USB doivent être autorisée via le « USB Manager ».

- **Action automatique quand un média USB est branché**
  - Permet de choisir un mode de scan automatiquement lancé sur détection d’une clef USB
  - Il est également possible de lancer une fenêtre « Choix de scan », ou de ne rien faire

- **Nettoyer la clef USB de sortie avec la fin du transfert**
  - Si cette option est activée, la clef USB de sortie est vidée avant copie des fichiers
  - Sinon, les fichiers existants sur la clef de sortie sont conservés, *ce qui peut entraîner un risque de sécurité si ces fichiers ne sont pas maîtrisés.*

- **Empreintes SHA256**
  - Si cette option est activée, des empreintes de fichiers sont réalisées avant et après scan et transfert, pour valider l’intégrité des fichiers de bout en bout
  - Sinon, les empreintes ne sont pas réalisées

- **Durée d’autorisation du scan**
  - Cette option permet de choisir la durée pendant laquelle les scans sont possibles après une mise à jour.
  - Par défaut, la durée est de 7 jours (durée recommandée pour une sécurité maximale), mais elle peut être poussée à 14 ou 30 jours.

- **Tag de clef USB pour S3Agent :** permet de choisir si les clefs USB sont préparées (apposition d’un tag ou « token ») pour le S3Agent (protection sur poste de travail). Choix possible entre : tag de toutes les clefs (Oui), tag des clefs autorisées (cf. 4.1.1), ou aucun tag (Non).

- **Mode de scan antivirus**
  - Ces deux modes sont basés sur les recommandations des éditeurs d'antivirus.
  - Dans le mode de scan normal (*par défaut*), le niveau d'archives imbriqués scannées (ZIP dans un ZIP) est limité à 10, les fichiers de plus de 100Mo ne sont pas complètement scannés (car les virus sont usuellement propagés dans des fichiers de petite taille), et les répertoires de plus de 80 niveaux d'imbrication sont ignorés (des avertissements sont affichés).
  - Le mode de scan avancé est plus lent, mais le niveau d'imbrication maximale est de 1000, et la taille maximale des fichiers scannés est de 2500Mo.

- **Envoi des résultats de scan**
  - Si cette option est activée, les logs de scans sont conservés, de manière cryptée et sécurisée, sur la station blanche S3 pour pouvoir être envoyés à MyHogo lors des routines de synchronisation.

- **Mise en quarantaine des menaces**
  - Si cette option est activée, les fichiers contaminés sont archivés dans des ZIP protégés par mot de passe et mis sur la clef USB de sortie. Le mot de passe est affiché et loggé.

- **Mode de formatage :** permet de choisir le type de formatage réalisé par la station blanche S3 ;

- **Type de formatage :** permet de choisir le type de partition écrite par la station blanche S3 (NTFS, exFAT ou FAT32).

- **Scan de ZIP chiffré :** permet de choisir le type traitement pour les ZIP avec mot de passe (pas de traitement, ou utilisation d'un dictionnaire de mots de passe).

Le bouton **ZIP chiffré** affiche le dictionnaire de mot de passe ZIP enregistrés dans la station blanche S3. Chaque mot de passe est utilisé (si le contrôle est activé) pour essayer de scanner l'intérieur des ZIP.

Le bouton **Règles MIME** affiche les règles de filtrage MIME enregistrées dans la station blanche S3. Chaque type MIME connu (et l'action correspondante) est décrit.

A noter (1) : Pour des raisons de temps de traitement et de sécurité, il est déconseillé d'autoriser les types MIME des fichiers « archives ». Cela comprend les extensions et types MIME suivants :

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

A noter (2) : Par défaut, les fichiers exécutables sont autorisés pour ne pas imposer de contraintes trop fortes sur l'utilisation de médias USB (ces types MIME étant utilisés pour des raisons parfaitement légitimes). Toutefois, Hogo attire l'attention sur le fait que ces fichiers EXE peuvent être des archives auto-extractibles, et invite les utilisateurs à se référer à leur administrateur informatique local ou directement à Hogo si une configuration plus dure, ne permettant pas ces fichiers, est souhaitée.

4.1.3 Gestionnaire de certificats

Le gestionnaire de certificat permet de visualiser la liste des certificats connus de la station blanche S3, et d'en ajouter de nouveau / d'en supprimer.

Conformément aux recommandations de l'ANSSI (cf. RGS V2 – Référentiel Général de Sécurité), les certificats doivent correspondre une taille de clef minimale de 2048 bits, pour ceux expirant avec 2030. Les certificats expirant après 2030 doivent avoir une taille de clef minimale de 3072 bits.

Hogo recommande l'utilisation de certificats de 4096 bits lorsque cela est possible.

Les boutons suivants peuvent être utilisés après saisie du code d'administration de la station blanche S3 :

[Ajouter]	Ajoute un certificat à la station blanche S3 (saisie du nom interne, du type, de l'adresse email du RECIPIENT associé). Le certificat doit être présent en [.pgp] sur une clef USB connectée (il doit être le seul fichier présent).
[Supprimer]	Supprime le certificat sélectionné de la station blanche S3 ;
[Quitter]	Retourne à l'écran précédent.

4.2 Mise à jour

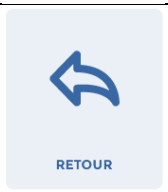
4.2.1 Ecran principal

L'écran des mises à jour permet de déclencher manuellement une mise à jour, ou de régler la façon dont celles-ci se déroulent sur la station blanche S3 :

	Ce bouton permet de mettre à jour les définitions antivirales. A noter : la clef USB doit être branchée *avant* de lancer la fonction.
	Ce bouton permet de mettre à jour le Core de la station blanche S3 (voir chapitre 4.2.4). A noter : la clef USB doit être branchée *avant* de lancer la fonction.
	Ce bouton permet de lancer la routine de synchronisation quotidienne de la station blanche S3 manuellement. Cette routine va télécharger et installer les mises à jour de la station blanche, synchroniser les logs et le NTP avec MyHogo (cloud ou « on premises »), et synchroniser les licences et les politiques de sécurité applicables à la station.
	Ce bouton permet de modifier les paramètres de mise à jour de la station blanche.
	Ce bouton permet de visualiser les versions logicielles et antivirales installées sur la station blanche S3 (voir chapitre 4.2.6).
	Ce bouton permet de revenir à l'écran précédent.

4.2.2 Paramètres de mise à jour

Cet écran permet de régler la façon dont la station blanche S3 se met à jour :

	Ce bouton permet de modifier le mode de mise à jour de la station blanche S3 (voir chapitre 4.2.2.1).
	Ce bouton permet de modifier les paramètres de connexion de la station blanche S3 (voir chapitre 4.2.2.2).
	Le bouton « Paramètres Relai local » permet de configurer la connexion à votre/vos S3SRV dans le cas d'une mise en jour en mode « On Premises » (voir chapitre 4.2.2.3).
	Ce bouton permet de prendre en compte vos éléments de connexion (mode, connexion LAN, connexion S3SRV…) et de réaliser un test rapide pour valider la configuration de la station blanche S3.
	Ce bouton permet de revenir à l'écran précédent.

4.2.2.1 Mode de mise à jour

Cette fenêtre permet de choisir comment la station blanche S3 se met à jour :

[MàJ USB] mise à jour avec une clef USB contenant le fichier de mise à jour ;
[MyHogo] mise à jour via un serveur S3SRV, après connexion au réseau local ;
[On Premises] mise à jour en se connectant au site MyHogo pour télécharger les fichiers ;

Cet écran permet également d'activer/de désactiver la mise à jour automatique (lancement automatique de la routine « Synchronisation », et de choisir l'heure de déclenchement de celle-ci, le cas échéant.

4.2.2.2 Paramètres Réseau

Cet écran permet de configurer le mode et les options de connexion pour les mises à jour en ligne :

- Type de connexion : Choix entre Wifi ,4G/LTE (modèles compatibles) et RJ45
- Paramétrage du Wifi :
    - SSID du Wifi à utiliser
    - Mot de passe du Wifi à utiliser
- Paramétrage de l'IP :
    - Adresse IP à utiliser (IP fixe ou « dhcp »)
    - Masque de sous-réseau (format 0-32)
    - Passerelle (IP ou « dhcp »)
    - DNS (IP ou « dhcp »)
    - APN 4G (code « Access Point Name », modèles compatibles)
- Activer ou désactiver le « Signe de vie » (envoi périodique d'un signal de vie à MyHogo ou S3SRV)

Chaque paramètre peut être renseigné grâce au clavier embarqué Hogo (saisie limitée à 50 caractères par paramètre). Il est également possible de configurer un proxy en cliquant sur le bouton « Proxy » :

- Activer / Désactiver le proxy
- Changer le mode de proxy (http ou HTTPS)
- Paramétrer l'hôte du proxy, le nom d'utilisateur, et le mot de passe d'accès si nécessaire

4.2.2.3 Paramètres Relai Local

Cette fenêtre permet de configurer la façon dont la station blanche S3 se connecte au S3SRV local :

- Type de relai local (S3SRV de « Dépôt » ou de « Gestion »)
- Adresse de l'hôte (ou nom d'hôte),
- Code de communication : Clef secrète et code IV.

Chaque paramètre peut être renseigné grâce au clavier embarqué Hogo (saisie limitée à 50 caractères par paramètre). Les éléments de configuration d'un S3SRV sont fournis par Hogo avec le serveur.

A noter concernant le paramétrage du côté serveur :

- Le protocole utilisé est HTTPS avec TLS version 1.3 et une clef de chiffrement de 2048bits au minimum (avant 2030),
- Les seules suites de chiffrement (CipherSuites) autorisées sont 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, et TLS_DHE_RSA_WITH_AES_128_CCM (*à noter : l'option de renégociation EMPTY_RENEGOTIATION est aussi présentée pour des raisons de compatibilité*),
- Il est nécessaire d'utiliser un certificat SSL signé, soit par une autorité (CA) connue, soit par une autorité ajoutée à la station (contacter Hogo pour ajouter un certificat CA à la station S3).

Pour plus d'informations, se reporter au guide ANSSI « Recommandations de sécurité relatives à TLS » et au RGS v2 (Référentiel Général de Sécurité).

4.2.3 Mise à jour antivirale

La fonction de mise à jour des moteurs antivirus est lancée si les préconditions sont remplies (clef USB accessible, ou réseau accessible, et nouvelle mise à jour disponible). Le fichier de mise à jour sera analysé et validé, et sera ensuite appliqué au système.

La station blanche S3 devra ensuite être redémarrée pour que la nouvelle version soit opérationnelle.

Dans le cas d'une mise à jour USB[2], si la station détecte des erreurs d'entrée/sortie sur la clef USB, l'utilisateur est invité à resélectionner un fichier de mise à jour (sinon, l'interface pourra être quittée).

A noter : Il est possible de mettre manuellement à jour la station avec des définitions datant d'un ou deux jours (y compris si des bases plus récentes sont déjà installées) pour revenir temporairement à une version antérieure, par exemple en cas de faux positifs indésirables dû à une mise à jour antivirale.

Hogo ne recommande cette action de rétrogradation qu'en cas d'impact fort des nouvelles bases antivirales sur l'utilisabilité des stations, et après une étude de sécurité ad hoc.

4.2.4 Mise à jour du Core

La fonction de mise à jour du logiciel Core est lancée si les préconditions sont remplies (clef USB accessible, ou réseau accessible, et nouvelle mise à jour disponible). Le fichier de mise à jour sera analysé et validé, et sera ensuite appliqué au système.

La station blanche S3 devra ensuite être redémarrée pour que la nouvelle version soit opérationnelle.

Dans le cas d'une mise à jour USB[2], si la station détecte des erreurs d'entrée/sortie sur la clef USB, l'utilisateur est invité à resélectionner un fichier de mise à jour (sinon, l'interface pourra être quittée).

4.2.5 Synchronisation en ligne

La synchronisation en ligne, lancée manuellement ou périodiquement, permet de :

- Mettre à jour l'antivirus
- Mettre à jour le Core
- Mettre à jour la licence (depuis un S3SRV uniquement)
- Mettre à jour le paramétrage de la station blanche (depuis un S3SRV uniquement)
- Synchroniser les logs (avec MyHogo, un S3SRV, et/ou un Syslog) et les informations de version
- Synchroniser le temps en NTP (si activé dans les réglages de l'heure)

La station blanche S3 devra ensuite être redémarrée pour que la nouvelle version soit opérationnelle.

[2] Les fichiers « JIT » de mise à jour doivent être déposés à la racine du média USB en cas de mise à jour hors ligne.

4.2.6 Affichage des versions

Cet écran affiche les versions du Core et des moteurs antiviraux, ainsi que le nom de l'équipement et son adresse MAC. La seule option disponible est « Quitter » pour revenir à l'écran précédent.

4.3 Ecran de connexion – Fonctions d'administration

Cette IHM est un clavier spécifiquement conçu par Hogo, contenant trois jeux de caractères :

- Caractères minuscules (ainsi que digits et certains signes de ponctuation, correspondant globalement au clavier « AZERTY minuscule »)
- Caractères majuscules (ainsi que digits et certains signes de ponctuation, correspondant globalement au clavier « AZERTY majuscule »)
- Caractères spéciaux (accentués).

Elle permet de saisir le mot de passe d'administration de la station blanche S3, pour accéder aux fonctions protégées (mises à jour de Core, USB Manager…).

Une fois le mot de passe saisi correctement, les fonctions sont accessibles. Le même clavier est affiché lors de la procédure de renouvellement du mot de passe de la station blanche.

Le mot de passe d'administration fait obligatoirement entre 16 et 32 caractères, choisis parmi les caractères du clavier Hogo (10 digits numériques, les 26 lettres de l'alphabet en minuscule ou en majuscule, ainsi que 25 caractères spéciaux, accentués ou de ponctuation). Il doit contenir à minima une lettre minuscule, une lettre majuscule, et un chiffre.

Concernant ce renouvellement, les recommandations Hogo sont les suivantes :

- Hogo recommande le renouvellement du mot de passe tous les 6 mois à 2 ans au maximum selon la sensibilité du système d'information utilisant la station blanche ;
- Hogo recommande de ne pas réutiliser les mots de passe déjà utilisés.

4.4 Réglage de la date

Cette interface permet le réglage de la date et de l'heure de la station blanche S3.

- "Année", "Mois", "Jour", "Heure" et "Minute" permettent de régler la date et l'heure.
- « Sauvegarder » enregistre les paramètres dans la station blanche S3.
- « Paramètres NTP » permet de régler les paramètres utilisés pour la synchronisation NTP :
    - Activer / Désactiver la synchronisation NTP
    - Choisir l'IP/le nom d'hôte du premier serveur NTP à contacter, et la version de son protocole
    - Choisir l'IP/le nom d'hôte du second serveur NTP à contacter, et la version de son protocole
- « Ecran de veille » permet de modifier les paramètres de mise en veille et économiseur d'écran
- « Quitter » ferme cette interface.

4.5 Ecran de veille

Cette interface permet modifier les paramètres de mise en veille et économiseur d'écran de la station blanche S3.

- Mode de mise en veille : choix entre « pas de veille », « écran de veille » (économiseur), « veille puis éco » ou « économie d'énergie » (écran noir).
- Type d'économiseur, si activé : Images en rotation, Vidéo.
- Délais avant économiseur et/ou mise en veille (écran noir) : défini le délai entre l'arrêt d'utilisation et le passage en économiseur, et le passage en écran noir (si activés).
- « Sél. Fichiers » permet d'acéder aux fichiers présents sur une clef USB branchée à la station pour choisir des images ou une vidéo à appliquer en économiseur d'écran.
- « Sauvegarder » enregistre les modifications, « Aperçu » montre l'économiseur d'écran tel qu'il apparaîtra sur déclenchement du timeout
- « Quitter » ferme cette interface.

A noter : La mise en veille et l'économiseur d'écran n'est pas modifiable sur la tablette S3Box pour économiser la batterie, c'est le système qui reste maître des paramètres :

- L'écran de la tablette d'éteint au bout de 5 à 15 minutes (« écran noir »)
- Le système passe en veille plus profonde au bout d'une à trois heures (« suspend »)
- Parfois, le système passe en veille profonde (« freeze state ») pour économiser la batterie (au bout d'un à sept jours allumés, sans utilisation) : dans ce cas un redémarrage peut être nécessaire.

4.6 Logs

4.6.1 Ecran principal

Journal S3	Ce bouton permet d'afficher le log principal de l'interface S3 (listant les actions utilisateur et administrateur réalisées).[3]
Journal MàJ AV	Ce bouton permet d'afficher le log de mise à jour des définitions antivirales (voir chapitre 4.2.3).[2]
Journal MàJ Core	Ce bouton permet d'afficher le log de mise à jour du Core (voir chapitre 4.2.4).[2]
Exporter journaux	Ce bouton permet de **déplacer** tous les logs vers une clef USB de sortie. Les logs seront déplacés dans un fichier crypté créé spécialement sur cette clef USB. La clef USB doit être branchée *avant* de lancer la fonction.
Envoyer journaux	Ce bouton permet d'envoyer tous les logs vers MyHogo (Cloud ou « on premises »).
Paramètres Syslog	Ce bouton permet d'accéder aux paramètres Syslog (voir chapitre 4.6.2).
Quitter	Ce bouton permet de quitter l'interface des logs.

[3] Les journaux sont rédigés en Anglais par le système. En cas de question, contacter Hogo avec le(s) référence(s) de(s) message(s) nécessitant une explication.

4.6.2 Paramétrage du Syslog

Cet écran permet de paramétrer le(s) serveur(s) Syslog utilisés lors de l'envoi des logs et de la synchronisation (automatique ou manuelle) de la station blanche S3 :

- Activer / Désactiver le Syslog
- Choisir le mode d'envoi (UDP si disponible, TCP, TCP sur SSL)
- Choisir l'IP / le nom d'hôte du premier serveur Syslog à contacter, et son port
- Choisir l'IP / le nom d'hôte du second serveur Syslog à contacter, et son port

4.6.3 Affichage des Logs

Le contenu des logs est affiché à l'écran. L'écran peut être fermé en cliquant sur « Quitter ». L'édition des logs n'est pas disponible : pour des raisons de sécurité, seule la consultation des logs est possible.

Pour faciliter la lecture des journaux, les messages affichés dans cet écran ont été sélectionnés conformément aux recommandations de l'ANSSI. De plus nombreux messages supplémentaires sont tracés par le système S3 et peuvent par exemple être remontés à un serveur SYSLOG ou exportés sur une clef USB, dans des fichiers chiffrés.

Les messages affichés sont soit des notifications (messages en noir) ou des erreurs (messages en rouge). Le code donné est préfixé « LogEvent » pour les notifications, et LogError pour les erreurs.

Ce code de message est unique, il est composé comme suit : YYxZZ, où YY est le code décimal du module concerné, et ZZ le code du message dans ce module.

A noter : Lors de leur affichage à l'écran, les journaux peuvent être tronqués s'ils contiennent un trop grand nombre de lignes, pour garder un affichage lisible. Le troncage suit alors une logique FIFO (First In, First Out : premier entré, premier sorti) et le contenu complet reste accessible sur la console de gestion ou le puit Syslog.

Pour plus d'information sur les évènements affichés, consulter le document de l'ANSSI : DAT-NT-012/ANSSI/SDE/NP « Recommandations de sécurité pour la mise en œuvre d'un système de journalisation ».

Le tableau ci-dessous détaille, pour les bornes S3, les évènement journalisés et visualisables dans l'interface d'administration. Le thème et les exemples sont extraits du document de l'ANSSI « Recommandations de sécurité pour la mise en œuvre d'un système de journalisation ».

Thème	Exemple de l'ANSSI	Journalisation du S3Core
Authentification	Réussites et échecs d'authentification	Toutes les tentatives d'authentification sont tracées, en réussite ou en erreur
	Utilisations des différents mécanismes d'authentification	Lancement des interfaces de saisie de mot de passe Administrateur S3
	Elévations de privilèges	Toutes les tentatives d'authentification sont tracées, en réussite ou en erreur
Gestion des comptes et des droits	Ajouts/suppressions de comptes/groupes/rôles	*Sans objet pour le S3Core.*
	Affectations/suppressions de droits aux comptes/groupes/rôles	*Sans objet pour le S3Core.*
	Modifications des données d'authentification	Modification du mot de passe d'administration, en réussite ou en erreur
Accès aux ressources	Accès ou tentatives d'accès en R/W/X aux ressources	**SCAN** Les accès aux données en transit et scannées sont tracés, en écriture (entreposage de données, suppression), et lecture (contrôles divers). *A noter : conformément aux recommandations de l'ANSSI, il n'y a pas d'accès en exécution sur ces données.*
		MISE A JOUR Les accès aux données de mise à jour sont tracés pendant leur écriture (récupération, entreposage, suppression), lecture (contrôles divers) et exécution (application des scripts de mise à jour éventuels).
		JOURNALISATION Les accès en lecture (ouverture de log) aux données des journaux sont tracés. *A noter : conformément aux recommandations de l'ANSSI, il n'y a pas d'accès en exécution sur ces données.*
Modification des stratégies de sécurité	Editions, applications, réinitialisations de configurations	**PARAMETRES** Chaque modification enregistrée de paramètre est tracée dans les journaux (valeurs « avant » et « après » modification). Chaque tentative de modification n'ayant pas abouti est également tracée.
		MISE A JOUR Chaque tentative de mise à jour, en réussite ou en erreur, est tracée, avec le détail des étapes réalisées, dans les journaux de mise à jour.
Activité des processus	Démarrages/arrêts	Chaque démarrage ou arrêt d'un processus interne au S3Core (i.e. panel affiché ou processus utilisé) est tracé dans les logs.
	Dysfonctionnements	Les cas d'erreur de fonctionnement des processus sont tracés dans les logs.
	Chargements/déchargements de modules	*Sans objet pour le S3Core : considéré dans le cas « Démarrages/arrêts ».*
Activité des systèmes	Démarrages/arrêts	Chaque démarrage, arrêt ou redémarrage du matériel est tracé dans les logs.
	Dysfonctionnements/surcharges du système	Chaque évènement système de niveau "erreur" ou plus, est tracé dans les logs.
	Chargements/déchargements de modules	*Sans objet pour le S3Core : considéré dans le cas « Démarrages/arrêts ».*
	Activité matérielle (défaillances, connexions/déconnexions physiques…)	**DEFAILLANCE** Chaque évènement système de niveau "erreur" ou plus est tracé.
		CO/DECONNEXION Chaque évènement de branchement ou débranchement de périphérique amovible de catégorie stockage ou HID est tracé dans les logs.