Hogo S3

HR-MAN-26-210-v5

Manuel Administrateur S3

2026

Ce document détaille l'installation et l'administration des stations blanches de la gamme S3 de Hogo et les consignes de sécurité liées à leur utilisation.

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	01/2026	Mise à jour suite à revue interne
V5	03/2026	Mise à jour pour s'aligner sur la mise à jour T1 2026

Table des matières

1 Introduction 4
1.1 Hogo 4
1.2 La gamme S3 4
1.3 Ce document 4
2 Contenu de l'emballage produit 5
2.1 Tablette S3Box 5
2.2 Poste S3Pos 5
2.3 Totem S3Tot 6
2.4 S3 Boot 7
3 Prérequis 8
3.1 Exigences Environnementales 8
3.2 Exigences Électriques 8
3.3 Exigences Réseau (si la station est connectée) 9
4 Consignes de sécurité 10
5 Déballage et Installation 11
5.1 Stations S3 (hors S3Boot) 11
5.2 Disques S3Boot 11
6 Première mise sous tension 12
7 Écran d'accueil 13
8 Paramètres globaux 14
8.1 Wizard de configuration 17
8.2 Centre de mise à jour 18
8.3 Journaux 24
8.4 Gestionnaire des certificats 26
8.5 Gestionnaire USB 28
8.6 Paramètres de formatage 30
8.7 Paramétrage de lecture de Badge 32

8.8 Réglages SFS 34
8.9 Réglages de scan 36
8.10 Modification du mot de passe 39
8.11 Date et heure 41
9 Mise à jour Initiale 43
10 Tests de fonctionnement 44
11 S3Core Rescue mode 45
12 Avertissements complémentaires 46

1 Introduction

1.1 Hogo

Hogo Business Services SAS est une société créée en 2016 à Rennes. Spécialisée dans la cybersécurité, Hogo fournit des solutions de sécurité prêtes à l'emploi totalement intégrées pour sécuriser tout système d'information.

Hogo propose également plusieurs services associés : accompagnement à l'utilisation de ses produits, support technique, expertise en cybersécurité (analyse des risques et vulnérabilités, intégration…) et développement de logiciels spécifiques (R&D spécialisée).

Hogo adopte une approche de la sécurité aussi pragmatique que possible. Nos projets sont nés de retours d'expériences concrets, et Hogo développe des dispositifs de sécurité répondant rapidement et efficacement aux besoins de ses clients.

Hogo est également fortement impliqué dans une démarche de réduction des impacts environnementaux de ses activités. Membre de l'Institut Numérique Durable (INR) et partenaire privilégié de l'association d'utilité publique Bretagne Vivante, Hogo innove et applique une politique RSE stricte et ambitieuse.

1.2 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 Id-,
- Éviter toute fuite d'information ou l'entrée de données non-autorisées dans votre système.

1.3 Ce document

Ce document constitue la Manuel des Administrateurs des stations de la gamme S3. Il décrit leur réglage et la procédure de démarrage et de réception, y compris les aspects liés à la sécurité. Il suit un déroulement basé sur l'IHM standard du produit.

Pour aller plus loin :

- Le guide de démarrage rapide à réception d'une station est présent ici : https://hogo.eu/start/
- Le portail de support pour toute question technique est présent ici : https://support.hogo.eu/
- Les fiches-reflexe pour vous assister sur des cas pratiques d'usage sont présentes ici : https://hogo.eu/zone_echange/outils_hogo/Fiches_REFLEXE_gamme_S3.pdf

2 Contenu de l'emballage produit

2.1 Tablette S3Box



- 1 tablette durcie, mobile et résistante aux chocs
- Un câble de chargement (230V AC vers connectique DC en USB-C)
- Un dock de chargement avec chargeur dédié sortie 12v DC (en option pour les tablettes concernées)

2.2 Poste S3Pos





- 1 poste monobloc en métal avec écran tactile 13 pouces
- Un câble d'alimentation avec transformateur de 230V AC vers 19V DC
- Une antenne Wi-Fi (pour les stations concernées)
- Coffret Métallique avant pour protection physique des ports USB (en option pour les stations concernées)

2.3 Totem S3Tot



- 1 poste totem autoporteur

2.4 S3 Boot



- 1 disque dur formaté avec le système S3Boot (2.5 SSD ou M2 NVMe selon bon de commande)

3 Prérequis

3.1 Exigences Environnementales

- Choisir un espace propre et dégagé, adapté à la taille / au nombre d'équipements à mettre en place.
- Choisir une surface stable et non électrostatique pour éviter tout dommage électrique aux équipements.
- 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.

3.2 Exigences Électriques

- Utilisez toujours un câble d'alimentation en bon état fourni par Hogo. Évitez d'utiliser des câbles endommagés ou effilochés.
- S3Box : Branchement du chargeur fourni avec la station sur secteur (230V en courant alternatif en 50Hz) pour une alimentation en sortie de chargeur USB-C en courant continu.
- S3Pos : Uniquement branchement du câble à l'arrière de la station sur secteur (230V en courant alternatif en 50Hz) pour une alimentation en sortie de transformateur en 19V en courant continu. [1]
- 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 les 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 (de plus, les alimentations AC/DC externes ne doivent jamais dépasser les 40°C).

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.

[1] Adaptateur électrique type « HKA09019047-8U » avec tension d'entrée 110-240V en 50/60Hz sous 1.5A et sortie 19.0V sous 4.74A à 8A.

3.3 Exigences Réseau (si la station est connectée)

- Câble réseau RJ45, de catégorie 6 au minimum, pour les stations branchées en câblé.
- Ou : Réseau Wifi ouvert, protégé ou non par mot de passe, SSID masqué ou diffusé.
- Flux ouverts selon la matrice suivante :

Fonction	Source	Destination	Protocole	Port
Test réseau	Station S3	S3SRV	HTTPS	443
Mise à jour AV	Station S3	S3SRV	HTTPS	443
Mise à jour Core	Station S3	S3SRV	HTTPS	443
Envoi des versions	Station S3	S3SRV	HTTPS	443
Envoi des logs (serveur)	Station S3	S3SRV	HTTPS	443
Envoi des logs (syslog)	Station S3	Serveur Syslog *	HTTPS	Port paramétré
Récupération de la licence	Station S3	S3SRV	HTTPS	443
Synchronisation NTP	Station S3	Serveur NTP *	NTP	123
Synchronisation complète	Station S3	S3SRV	HTTPS	443
Connexion au proxy	Station S3	Proxy *	HTTP ou HTTPS	Port paramétré
Test réseau	S3SRV	MyHogo.eu	HTTPS	443
Synchronisation NTP	S3SRV	Serveur NTP *	NTP	123
Envoi des logs (syslog)	S3SRV	Serveur Syslog *	HTTPS	Port paramétré
Connexion au proxy	S3SRV	Proxy *	HTTP ou HTTPS	Port paramétré
Mise à jour AV	S3SRV	MyHogo.eu	HTTPS	443
Mise à jour Core	S3SRV	MyHogo.eu	HTTPS	443
Mise à jour manuelle AV / Core	Postes de travail	S3SRV	HTTPS	443
Interface Web (portail)	Postes de travail	S3SRV	HTTPS	443

** : les serveurs marqués d'une astérisque sont hors scope de fourniture Hogo.*

4 Consignes de sécurité

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

5 Déballage et Installation

5.1 Stations S3 (hors S3Boot)

1. Déballage du matériel
- Retirer délicatement l'équipement S3 de sa boîte de transport et le 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.

2. Alimentation électrique
- Connecter le chargeur fourni avec la S3Box à sa prise du côté de l'équipement S3 (passer l'étape pour le S3Tot et le S3Pos).
- Brancher le câble d'alimentation à une prise secteur munie d'une fiche de mise à la terre.

3. 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 équipements sont habituellement préconfigurés, mais des questions peuvent apparaître au premier démarrage).

5.2 Disques S3Boot

1. Déballage du matériel
- Retirer délicatement le disque S3Boot de son enveloppe à bulle.

2. Récupération de sa clé de licence
- Noter le début de la clef disponible sur le disque (s3boot-xxxxx)
- Transmettre cette partie de clé au support technique sur le portail https://support.hogo.eu

3. Finalisation de l'installation :
- Vous recevrez du support votre clé de licence complète ainsi que la procédure pour finaliser l'installation de votre S3Boot
- Une fois le disque initialisé et le poste redémarré, vous aurez accès à l'interface de la station blanche Hogo.
- Vous observerez en haut à gauche que votre licence est invalide
- Vous pourrez récupérer la référence (nom de l'équipement) dans « Paramètres / Journaux » pour finaliser la procédure du support.
- Une mise à jour vous sera alors fournie pour activer votre licence et finaliser ainsi l'installation.

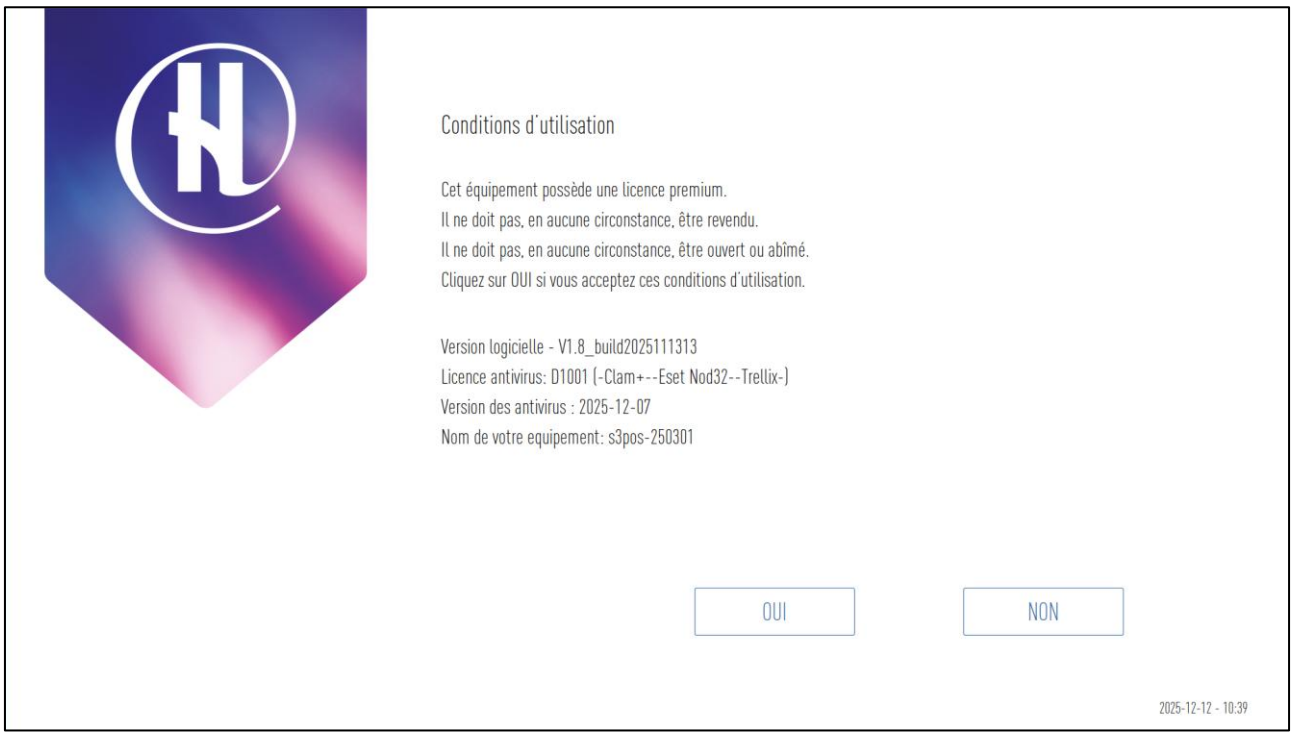
À noter :

- *Une fois le disque initialisé, il ne pourra plus être installé sur un poste différent.*
- *Attention, le poste sur lequel vous installez le S3Boot doit avoir un écran nativement au format 16:9, résolution 1920x1080.*

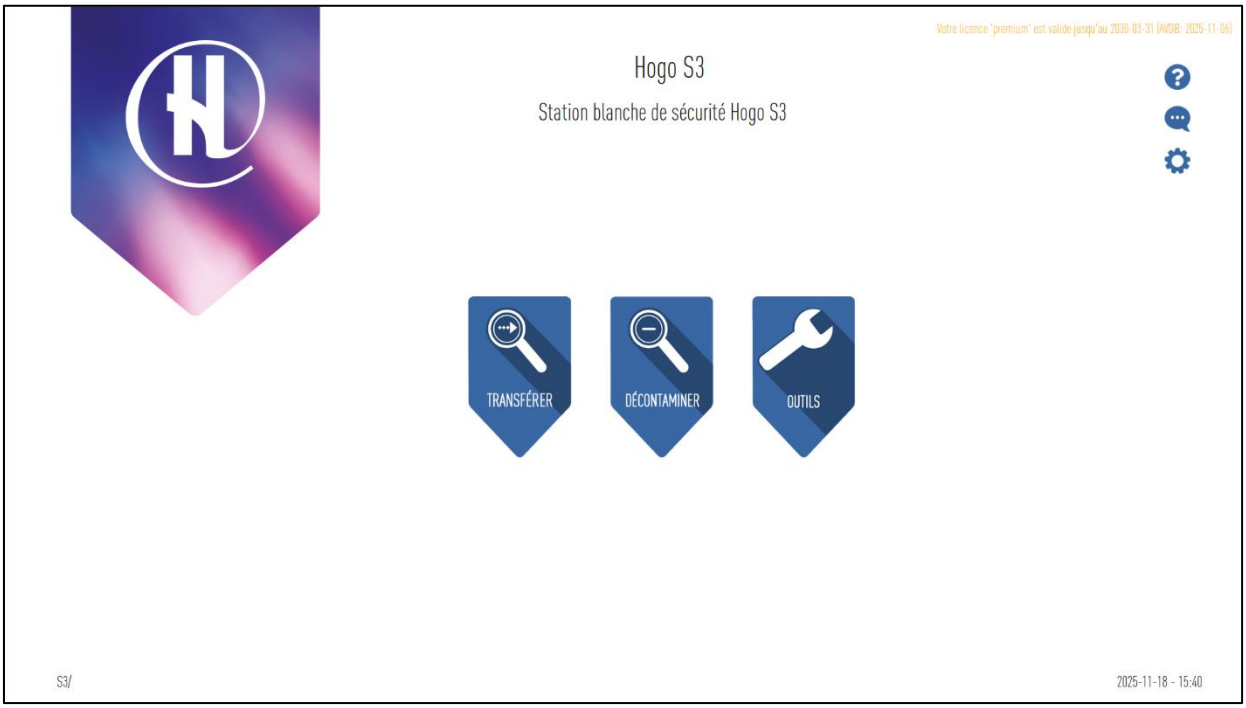
6 Première mise sous tension

À chaque démarrage de la station, un écran affiche les conditions d'utilisation ainsi que les informations système.

Après validation des conditions d'utilisation (clic sur « Oui »), vous êtes automatiquement redirigé vers l'écran d'accueil.



7 Écran d'accueil

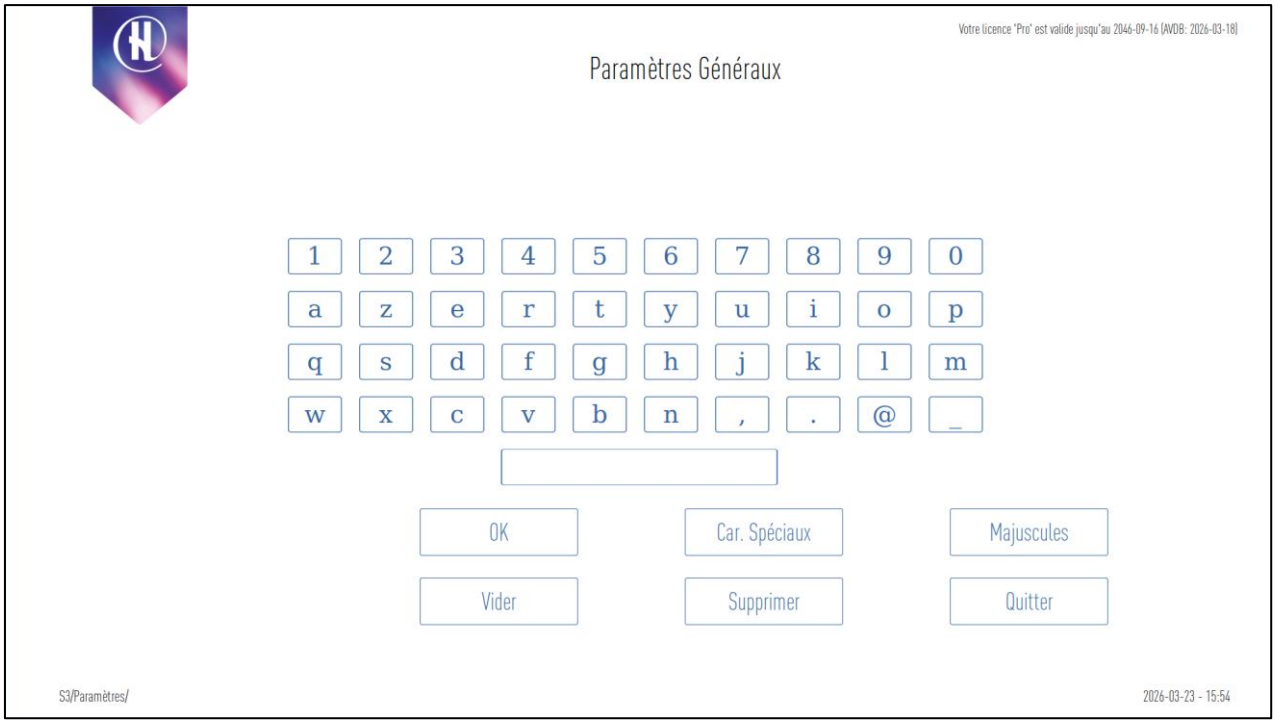


Depuis l'écran d'accueil, vous pouvez accéder aux fonctions standards en milieu d'écran, au menu Outils, et au menu Aide, au menu Langues ainsi qu'aux Paramètres d'administration.

A noter : pour le détail des fonctions standard, se reporter au manuel de l'Utilisateur. Le présent document se focalise sur les paramètres d'Administration.

8 Paramètres globaux

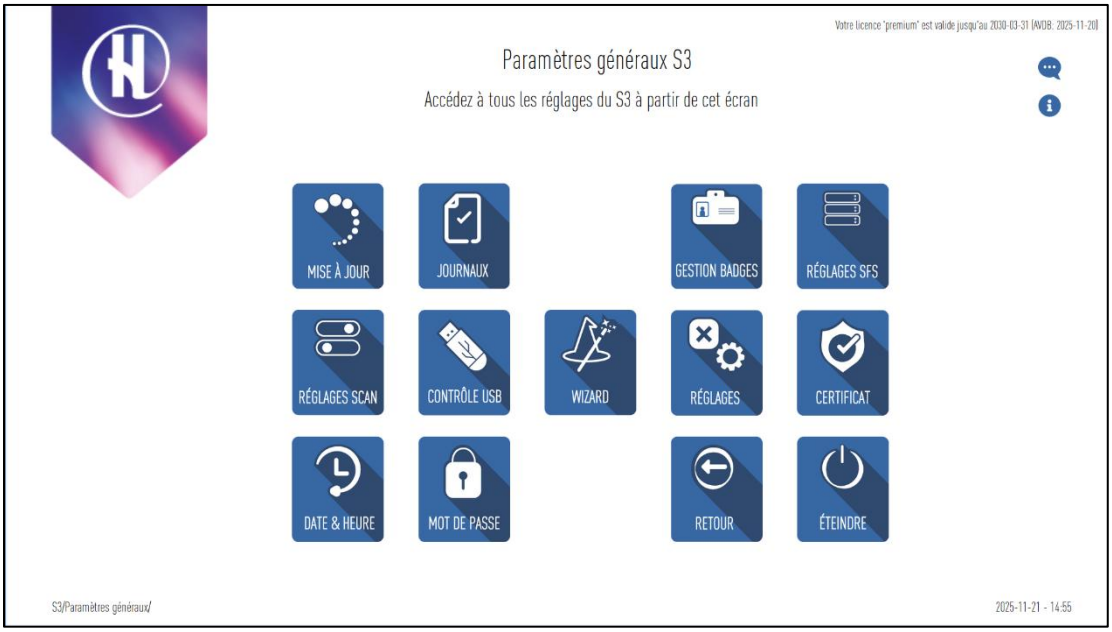
Cet écran est accessible, après saisie de mot de passe, depuis l'écran d'accueil, en cliquant sur « Paramètres » ou l'icône de roue crantée :



À noter : Le mot de passe initial de la station est « 1234567890 » il est important de le modifier à la première utilisation.

À noter : En cas de perte du mot de passe d'accès aux paramètres, aucune récupération à distance ne sera possible. Un renvoi de la station en SAV est obligatoire et celui-ci n'est pas couvert par la garantie Hogo.

Les fonctions accessibles sont :



	Accès au centre de mise à jour : Ouvre l'écran comprenant les menus relatifs aux mises à jour Core, aux mises à jour antivirus, à la synchronisation en ligne et aux paramètres réseau de la station, cf. chapitre 8.2.
	Accès aux journaux : Permet d'accéder à la gestion des journaux, incluant la configuration de la rétention, l'export des logs techniques ou des logs de scan, et l'envoi vers un serveur distant, cf. chapitre 8.3.
	Gestion de la lecture de badge : Permet de gérer la liste des badges autorisés (ajout, suppression, export) et les paramètres liés au contrôle PCSC. Un badge doit être présent dans la liste avant activation du contrôle, cf. chapitre 0.
	Paramètres du partage de fichier : Ouvre les réglages liés aux modes de transfert de fichiers Smart-Transfer et aux options de partage réseau (selon vos configurations), cf. chapitre 8.8.
	Réglages Scan : Permet de régler le filtrage MIME, le contrôle SHA256, le mode de scan antivirus, le traitement des menaces, la gestion des ZIP protégés et l'action appliquée au média USB de sortie, cf. chapitre 8.9.

	Gestionnaire USB pour le filtrage des médias autorisés : Affiche la liste des médias USB autorisés et permet d'ajouter ou supprimer des médias USB. Vider ou exporter cette liste, cf. chapitre 8.5.
	Wizard de configuration : Lance l'assistant de configuration automatique pour aider à paramétrer le réseau et les services de la station de manière guidée. Ne se lance jamais automatiquement, cf. chapitre 8.1.
	Paramètres de formatage des médias USB, cf. chapitre 8.6.
	Gestionnaire de certificats : Permet de visualiser la liste des certificats PGP connus de la station, ainsi que d'en ajouter ou supprimer. Les certificats doivent respecter les critères RGS V2, cf. chapitre 8.4.
	Paramètres liés à l'heure et à la date : Permet de configurer la date, l'heure et les paramètres associés (NTP, synchronisation éventuelle), cf. chapitre 0.
	Gestionnaire de mot de passe S3 : Permet de modifier le mot de passe d'accès aux paramètres, cf. chapitre 8.10.
	Retour à l'écran d'accueil : Ferme le menu Paramètres et renvoie vers l'écran d'accueil de la station.
	Éteindre ou redémarrer la station : Permet d'arrêter complètement ou de redémarrer la station blanche S3 (choix à réaliser sur le popup qui sera affiché à l'écran).

8.1 Wizard de configuration



Le Wizard de configuration (assistant de configuration automatisé) est là pour vous aider dans le paramétrage du réseau et des services de votre station :

Il se présente sous la forme d'une suite de questions vous permettant d'effectuer les premiers réglages.

Si par la suite vous devez modifier les différents paramètres, vous pourrez au choix relancer le Wizard ou passer par les paramètres présents dans les différents onglets du menu « Paramètres ».

Exemple de questions posées par le Wizard de configuration :



Voir l'enchainement des questions du Wizard de configuration en Annexe 1.

8.2 Centre de mise à jour



Le centre de mise à jour comprend les différents menus relatifs aux mises à jour Core et Antivirus, ainsi qu'aux paramètres réseau.



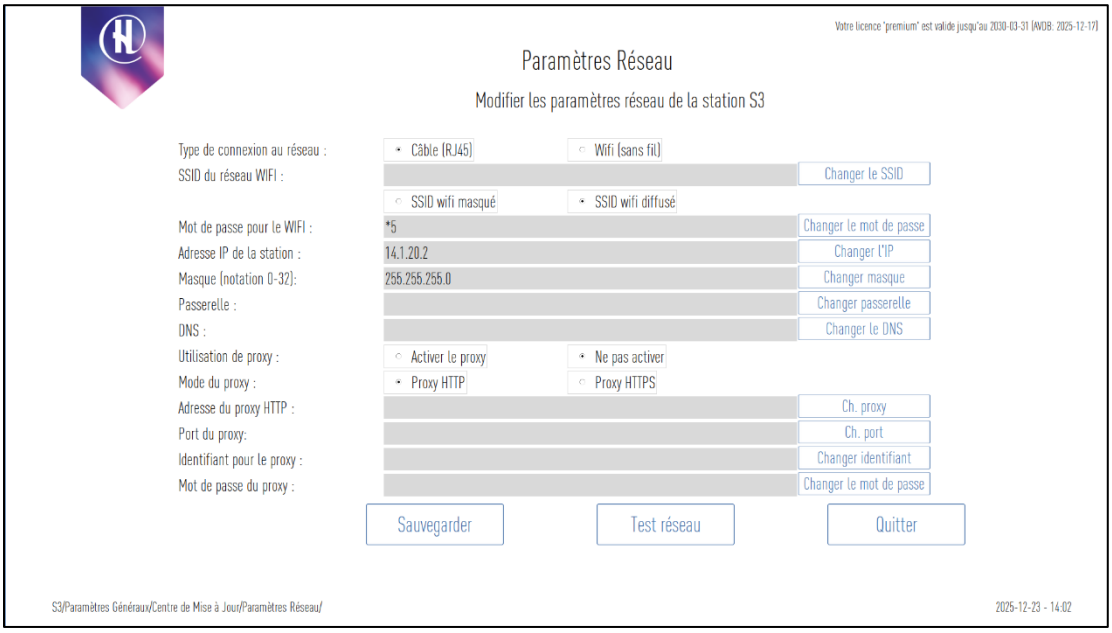
	Mise à jour des anti-virus (bases de détection)
	Mise à jour du Core S3 (logiciel)
	Synchronisation en ligne (sur cloud ou S3Srv « on premises »)

	Paramètres de connexion réseau de la station
	Paramètres de mise à jour de la station

8.2.1 Paramétrage du Réseau



L'écran des paramètres réseau vous permet de configurer et d'administrer l'ensemble des options de connectivité du système. Cet espace regroupe toutes les informations nécessaires pour gérer la connexion filaire ou sans-fil, ainsi que les réglages liés à l'utilisation d'un serveur proxy.
La capture d'écran intégrée dans ce chapitre illustre les différents paramètres disponibles :



8.2.1.1 Configuration de la connexion

Dans cette section, vous pouvez consulter le type de connexion utilisé par la station, qu'il s'agisse d'une connexion Ethernet ou d'un réseau Wi-Fi.

Si la station utilise une connexion sans-fil, vous avez la possibilité de visualiser ou de modifier :

- Le SSID du réseau Wi-Fi : le nom du point d'accès auquel la station doit se connecter.
  Il est possible de choisir un SSID masqué ou diffusé.
- Le mot de passe Wi-Fi : la clé de sécurité permettant l'accès au réseau.

Ces paramètres vous permettent d'établir ou d'ajuster la connexion Wi-Fi en fonction de votre infrastructure.

8.2.1.2 Paramètres IP

Vous pouvez également définir ou vérifier les paramètres d'adressage IP du système :

- Adresse IP : l'adresse attribuée à la station (ou « dhcp » pour une adresse IP obtenue automatiquement).
- Masque de sous-réseau : exprimé en notation CIDR (de 0 à 32, ou champ vide pour une IP en DHCP).
- Passerelle : l'adresse du routeur ou de la passerelle utilisée pour accéder aux autres sous-réseaux ou à Internet.
- Serveur DNS : l'adresse du serveur chargé de la résolution des noms de domaine.

Ces réglages vous offrent un contrôle complet sur la configuration IP du système, qu'elle soit statique ou automatique.

8.2.1.3 Configuration Proxy

Si votre environnement réseau utilise un serveur proxy, vous pouvez activer et paramétrer ce service à l'aide des options suivantes :

- Utilisation du proxy : permet d'activer ou de désactiver le proxy.
- Mode du proxy : choix du type de proxy utilisé (HTTP ou HTTPS).
- Adresse du proxy : adresse du serveur proxy correspondant au mode choisi.
- Port du proxy : port réseau associé au service proxy.
- Identifiant du proxy : nom d'utilisateur requis en cas d'authentification.
- Mot de passe du proxy : mot de passe associé à l'identifiant.

Ces paramètres vous assurent une compatibilité avec les infrastructures nécessitant un contrôle ou un filtrage du trafic sortant.

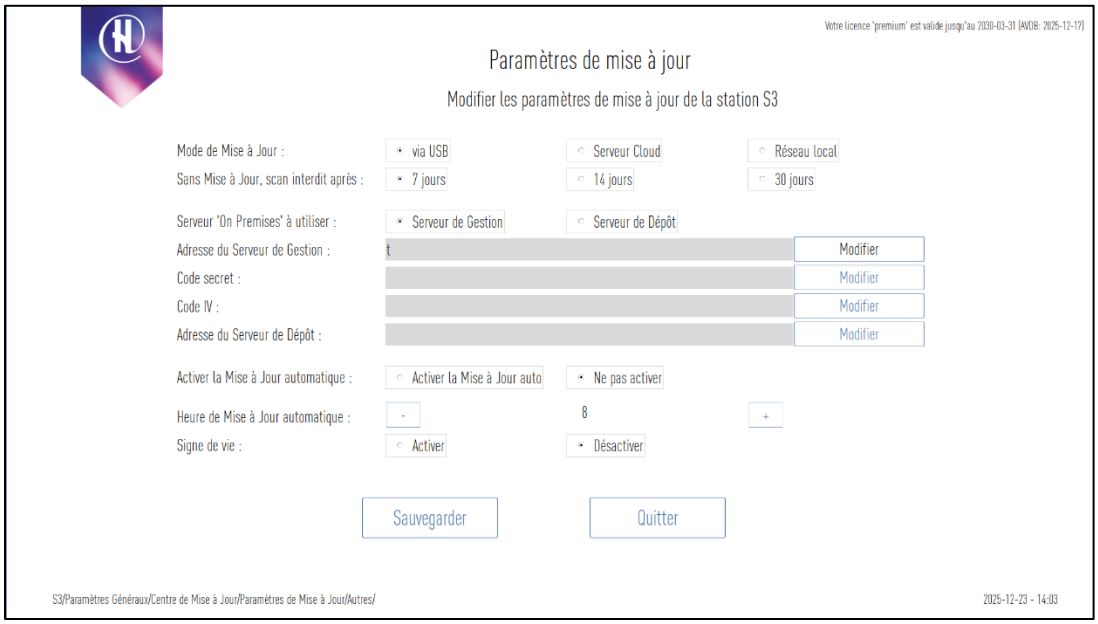
A noter : Pour l'application de ces paramètres liés au proxy, un redémarrage de la station est nécessaire.

8.2.2 Réglages



L'écran des paramètres de mise à jour vous permet de définir la source, le comportement et la fréquence des mises à jour du système. Cet espace regroupe l'ensemble des options nécessaires pour garantir que la station reste conforme, sécurisée et à jour.

La capture d'écran intégrée dans ce chapitre illustre les différents réglages disponibles.



8.2.2.1 Mode de mise à jour

Vous pouvez sélectionner la source à partir de laquelle le système téléchargera ses mises à jour. Plusieurs modes sont disponibles :

- USB : la mise à jour s'effectue depuis une clé USB contenant les fichiers nécessaires.
- Serveur cloud : la station récupère les mises à jour depuis votre compte en ligne MyHogo (le fichier doit être à la racine du média).
- Réseau local : les mises à jour sont téléchargées depuis un serveur S3SRV, présent dans votre infrastructure.

Ces options vous permettent d'adapter la stratégie de mise à jour selon les contraintes de votre environnement (déconnectée, réseau local, ou Internet).

8.2.2.2 Gestion de l'absence de mise à jour

Pour garantir la conformité du système, vous pouvez définir un délai maximal au-delà duquel l'utilisation devient restreinte :

- Sans mise à jour : scan interdit après 7 jours, 14 jours ou 30 jours (Hogo vous préconise un délai de 7 Jours)

Une fois le délai dépassé, la fonction de scan est automatiquement bloquée afin d'éviter l'utilisation de bases antivirus obsolètes.

8.2.2.3 Serveur S3SRV On-Premise (gestion et dépôt)

Si vous utilisez une plateforme interne de gestion ou de distribution des mises à jour, vous pouvez renseigner les paramètres suivants :

- Adresse du serveur de gestion (si utilisation d'un S3SRV de gestion Hogo)
- Code secret (uniquement dans le cas de serveur de gestion, fourni par Hogo)
- Code IV (uniquement dans le cas de serveur de gestion, fourni par Hogo)
- Adresse du serveur de dépôt (si utilisation d'un S3SRV de dépôt Hogo)

Ces réglages permettent à la station de s'authentifier et de communiquer avec les serveurs S3SRV chargés de distribuer les mises à jour ou de réaliser la gestion centralisée.

8.2.2.4 Mises à jour automatiques

L'écran vous permet d'activer ou non les mises à jour en arrière-plan :

- Activer la mise à jour automatique ou la désactiver
- Choix de l'heure d'exécution automatique

Ces options vous permettent de planifier une mise à jour régulière sans intervention manuelle, idéalement en dehors des périodes d'utilisation de la station (nuit, soirée...).

8.2.2.5 Signe de vie

Vous pouvez également activer ou désactiver l'envoi d'un signe de vie, qui permet au système de signaler périodiquement sa présence ou son état à une infrastructure de supervision :

- Signe de vie : activé ou désactivé

À noter : Les fichiers « JIT » de mise à jour doivent être déposés à la racine du média USB en cas de mise à jour hors ligne.

8.2.3 Synchroniser



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.

Lorsque la synchronisation est lancée de façon automatique (à l'heure configurée précédemment), le redémarrage est automatique. Lorsque la synchronisation est lancée de façon manuelle, le redémarrage doit être déclenché manuellement.

A noter : Lorsque l'heure de synchronisation automatique est détectée, la station va lancer la synchronisation seule. Si la synchronisation échoue, la station peut être amenée à redémarrer puis à retenter celle-ci, pour s'affranchir de problèmes ponctuels de connectivité réseau par exemple. A la fin de l'heure configurée pour la synchronisation automatique, ce cycle de tentatives et de redémarrages prendra fin.

8.3 Journaux



L'écran Accès aux Journaux vous permet de configurer la gestion, la conservation et l'exportation des différents journaux générés par le système. Cet espace centralise l'ensemble des options liées à l'archivage des logs, à leur exportation automatique et au mode de transmission vers un serveur externe.

La capture d'écran intégrée dans ce chapitre illustre les paramètres disponibles.



8.3.1 Durée de rétention des logs

Vous pouvez définir la période durant laquelle les journaux sont conservés dans le système. Plusieurs durées sont proposées :

- 6 mois (typiquement adapté aux fortes contraintes RGPD)
- 1 an (adapté aux cas normaux d'utilisation)
- 3 ans (adapté aux cas d'usage dans des réseaux sensibles, restreints, ou liés à l'II 901)
- 5 ans (adapté aux cas d'usage dans des réseaux classifiés, ou liés à l'IG 1300)

Ce paramètre vous permet d'adapter la durée de conservation en fonction de vos contraintes internes, de vos politiques documentaires ou de vos exigences de conformité.

8.3.2 Type de journal de scan

Vous avez la possibilité de choisir le niveau de détail des journaux générés par les analyses :

- Journal de scan résumé
- Journal de scan complet

Cette sélection permet d'équilibrer la lisibilité des journaux et la quantité d'informations stockées.

8.3.3 Résultats de scan

Lorsque le système doit transmettre les journaux, vous pouvez choisir la méthode d'envoi :

- Envoyer au serveur
- Ne pas envoyer au serveur

Ce réglage permet d'autoriser ou non la transmission automatique des résultats de scan vers une infrastructure centrale.

8.3.4 Écrire un commentaire de scan

Vous pouvez indiquer si un commentaire doit être ajouté avant les opérations d'analyse :

Non / Oui (Toujours) / Oui (sur demande)

Ce paramètre vous permet d'adapter la documentation des opérations selon vos procédures internes.

8.3.5 Export automatique du journal

Vous pouvez activer ou désactiver l'export automatique du journal de scan sur le média USB.

Lorsque cette option est active, les journaux sont automatiquement exportés vers le média USB, sans action manuelle quel que soit le type de scan.

8.3.6 Actions et options disponibles

L'écran vous propose plusieurs boutons permettant d'accéder à différents journaux ou d'effectuer des exports manuels :

- Enregistrer : sauvegarde les paramètres modifiés.
- Journal S3 : ouvre le journal associé aux activités de la station.
- Journal MàJ AV : affiche le journal des mises à jour antivirus.
- Journal MàJ Core : affiche le journal des mises à jour du cœur système.
- Export logs de scan : permet de sélectionner les journaux de scan à exporter vers un média USB.
- Export log technique : exporte les journaux techniques du système vers un média USB.
- Envoyer logs : envoie manuellement les journaux vers le serveur configuré.
- Paramètres SysLog : permet d'accéder aux réglages SysLog si un serveur de logs distant est utilisé.
- Quitter : retourne à l'écran précédent.

À noter : L'export des log techniques est chiffrés et lisible uniquement pas l'équipe support de Hogo

À noter : En cas de problème avec votre station, pensez à faire un export des « logs techniques » et à les communiquer dans votre demande au support [https://support.hogo.eu/].

8.4 Gestionnaire des certificats



Le gestionnaire de certificats vous permet de visualiser l'ensemble des certificats connus de la station blanche S3, ainsi que d'en ajouter de nouveaux ou d'en supprimer. Cet écran centralise la gestion des certificats utilisés pour le contrôle de l'intégrité et de la provenance des fichiers en smart-transfert.

Conformément aux recommandations de l'ANSSI (cf. RGS V2 – Référentiel Général de Sécurité), les certificats doivent respecter les exigences suivantes :

- Pour les certificats expirant avant 2030 : taille de clef minimale 2048 bits.
- Pour les certificats expirant après 2030 : taille de clef minimale 3072 bits.

Hogo recommande, lorsque cela est possible, l'utilisation de certificats d'une taille 4096 bits afin de renforcer le niveau de sécurité.
Vous pouvez utiliser les actions suivantes :

- Ajouter : vous permet d'ajouter un certificat à la station blanche S3. Vous devez renseigner le nom interne du certificat, son type, ainsi que l'adresse email du RECIPIENT associé. Le certificat doit être présent au format .pgp sur une clé USB connectée, et il doit être le seul fichier présent sur cette clé.

- Supprimer : supprime le certificat actuellement sélectionné de la station blanche S3.
- Quitter : retourne à l'écran précédent.

Ces options vous permettent de maintenir un ensemble de certificats conformes aux recommandations de sécurité tout en assurant le bon fonctionnement des communications chiffrées du système.

8.5 Gestionnaire USB



Le gestionnaire USB vous permet la gestion du comportement de la station avec les médias USB connectés ainsi que de gérer la liste des médias USB autorisés par la station.



Filtrer les média USB autorisés :

- Non : Tous les média USB sont autorisés à se connecter à la station
- En entrée : Seuls les médias autorisés peuvent être branchés pour l'envoi de données par fonction de transfert
- En sortie : Seuls les médias autorisés peuvent être branchés à la station pour la récupération de données par fonction de transfert.
- Les deux : Les médias sont filtrés pour l'envoi et la récupération de données.

Voir la liste USB : Affichage de la liste des médias autorisés :



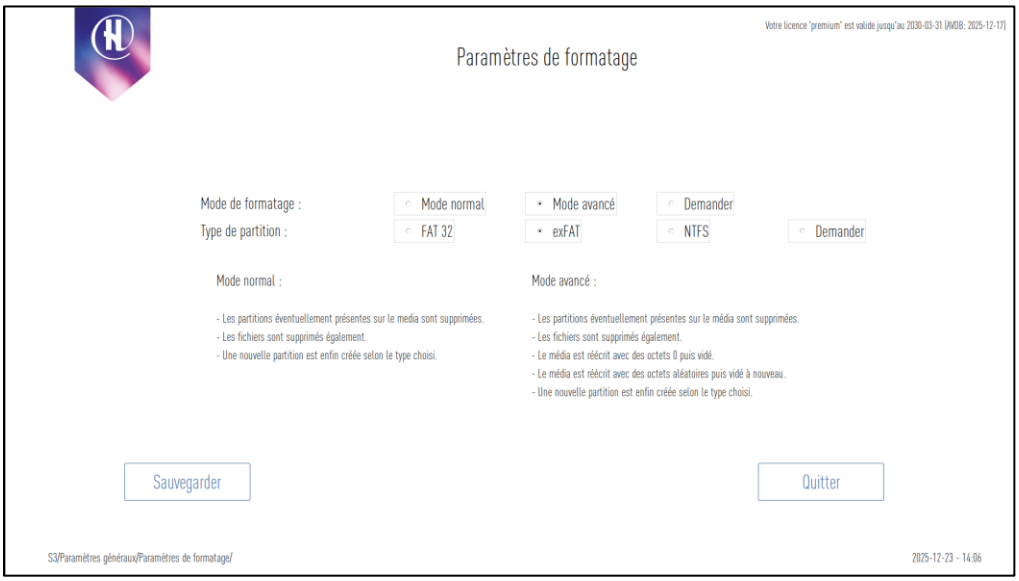
- Ajouter à la liste : Ajoute le média USB actuellement connecté à la liste des médias autorisés.
- Supprimer : Supprime le média USB actuellement connecté de la liste des médias autorisés.
- Vider la liste : Supprimer en une seule fois tous les médias de la liste des médias USB autorisés.
- Voir la liste USB : Affiche la liste complète des médias USB autorisés.
- Exporter la liste : Permet d'exporter la liste actuelle des médias USB autorisés dans un fichier au format LIST sur le média USB connecté.
- Synchro liste : Permet d'importer une liste de médias USB autorisés au format LIST depuis un média USB connecté.

8.6 Paramètres de formatage



L'écran Paramètres de formatage permet de définir la manière dont les médias USB seront formatés lors de leur formatage par la station blanche S3.

Cet espace met à disposition plusieurs modes de fonctionnement ainsi que différents types de partitions, afin de s'adapter aux exigences de votre environnement technique.



8.6.1 Mode de formatage

8.6.1.1 Mode normal

Dans ce mode, le formatage s'effectue selon un processus standard. Lorsque vous sélectionnez ce mode :

- Les partitions éventuellement présentes sur le média sont supprimées ;
- L'ensemble des fichiers présents sur le média sont supprimés ;
- Une nouvelle partition est créée selon le type choisi.

Ce mode est recommandé pour les opérations de formatage courantes.

8.6.1.2 Mode avancé

Le mode avancé applique un traitement plus approfondi du média USB. Lors de son utilisation

- Les partitions existantes sont supprimées ;
- L'ensemble des fichiers sont effacés ;
- Le média est réécrit intégralement avec des octets à valeur nulle ;
- Le média est ensuite réécrit avec des octets aléatoires ;
- Une nouvelle partition est créée selon le type choisi.

Ce mode offre un niveau d'effacement plus sécurisé, particulièrement adapté aux environnements nécessitant une destruction renforcée des données résiduelles.

8.6.2 Type de partition

Vous pouvez choisir le système de fichiers utilisé lors du formatage parmi les options suivantes :

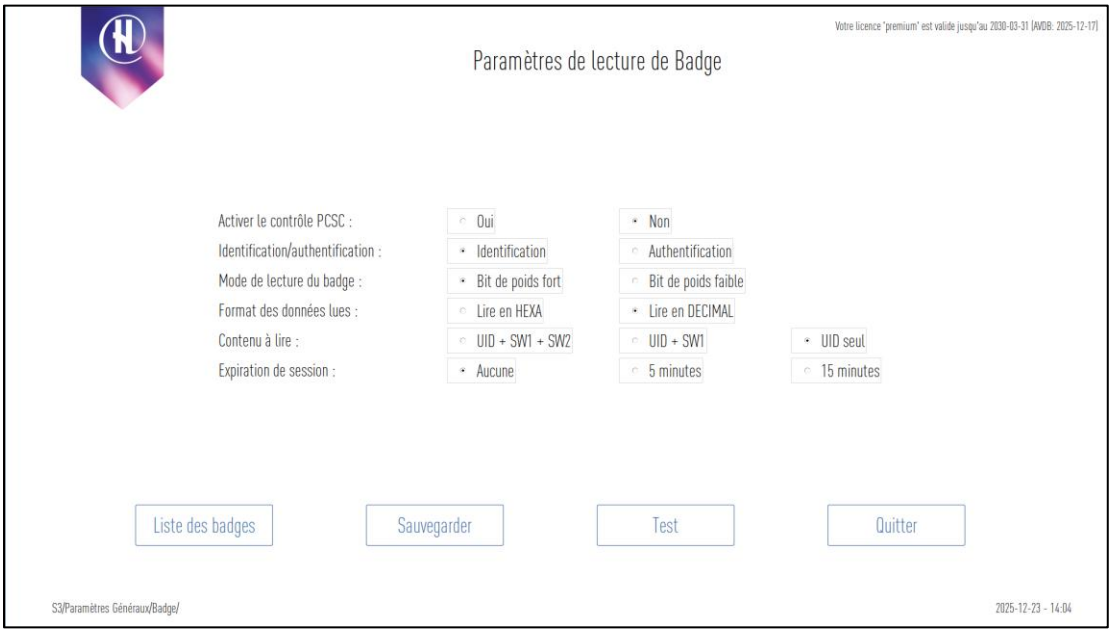
- FAT32
- exFAT
- NTFS
- Demander (le système vous demande à chaque opération le type de partition souhaité)

Le choix du type de partition dépend de vos besoins en compatibilité et des politiques de votre organisation.

8.7 Paramétrage de lecture de Badge



Le Paramétrage de lecture de Badge vous permet d'adapter le lecteur de badge au niveau de sécurité, de compatibilité et d'usage attendu. Leur paramétrage doit toujours être cohérent avec le système applicatif et les exigences opérationnelles.



- Activer le contrôle PCSC : Avant d'activer le contrôle PCSC (pas lecture de badge), assurez-vous qu'au moins un badge figure dans la liste des badges autorisés
- Identification/Authentification :
    - L'accès à la station par Identification nécessite l'utilisation d'un badge au démarrage. Tous les badges sont acceptés.
    - L'accès à la station par Authentification nécessite l'utilisation d'un badge enregistré dans la liste des badges autorisés au démarrage de la station.
- Mode de lecture du badge : Définit l'ordre de lecture des bits composant les données du badge.
- Format des données lues : Définit le format d'affichage et de transmission des données lues.
- Contenu à lire : Définit quelles informations du badge sont transmises après lecture.
- Expiration de session : Ce menu définit la durée de validité d'une session, sans action, après le passage du badge sur le lecteur.

Cliquer sur la Liste des badges affiche :



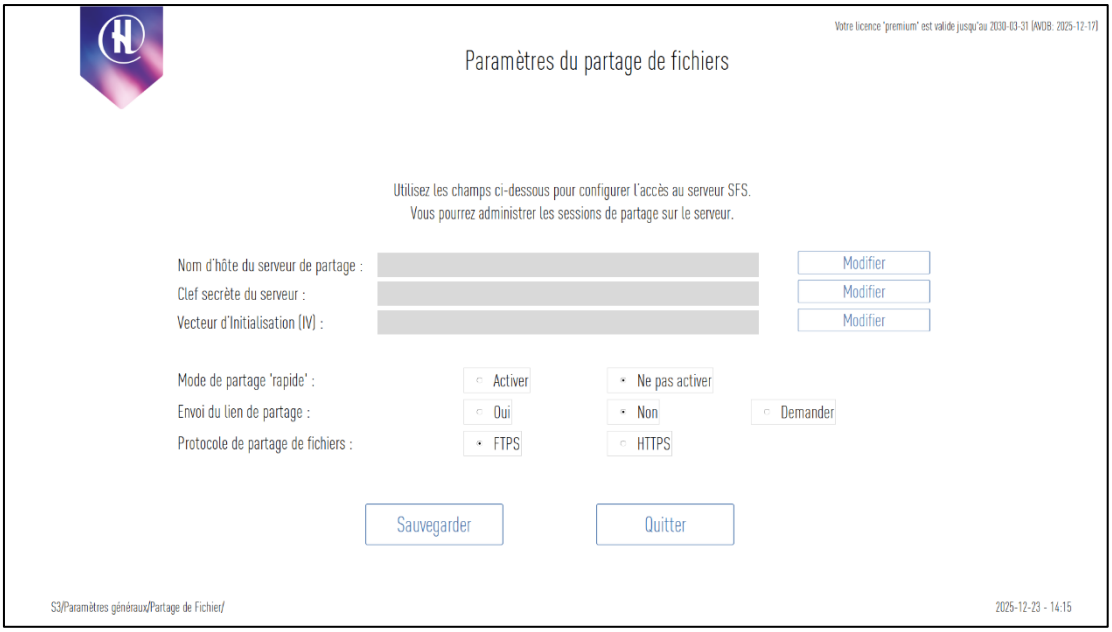
- Ajouter à la liste : Ajoute le badge actuellement posé sur le lecteur de badge à la liste des badges autorisés.
- Supprimer : Supprime le badge actuellement posé sur le lecteur de badge de la liste des badges autorisés.
- Vider la liste : Supprimer en une seule fois tous les badges de la liste des badges autorisés.
- Voir les badges : Affiche la liste complète des badges autorisés.
- Exporter la liste : Permet d'exporter la liste actuelle des badges autorisés dans un fichier au format LIST sur un média USB connecté.

8.8 Réglages SFS



L'écran Paramètres du partage de fichiers vous permet de configurer l'accès de la station blanche S3 à votre serveur SFS. Ce serveur est utilisé pour la gestion sécurisée des sessions de partage, notamment dans le cadre du transfert rapide (Smart-Transfer) ou de l'envoi de fichiers vers un espace partagé.

Cet écran regroupe l'ensemble des informations d'authentification et des options de fonctionnement nécessaires pour établir une communication sécurisée entre la station et le serveur de partage.



8.8.1 Paramètres d'accès au serveur SFS

Pour permettre à la station de se connecter au serveur SFS, vous devez renseigner les éléments suivants :

- Nom d'hôte du serveur de partage : Adresse ou nom DNS du serveur SFS auquel la station doit se connecter.
- Clé secrète du serveur : Clé d'authentification utilisée pour établir une session sécurisée avec le serveur de partage.
- Vecteur d'initialisation (IV) : Paramètre de chiffrement nécessaire au protocole d'échange sécurisé. Ce paramètre doit correspondre aux valeurs configurées sur votre S3SRV.

Les champs peuvent être modifiés individuellement à l'aide des boutons « Modifier » situés à droite de chaque ligne, après authentification administrateur.

8.8.2 Options de fonctionnement

Plusieurs paramètres permettent d'adapter le comportement du partage selon votre environnement :

8.8.2.1 Mode de partage "rapide"

Lorsque ce mode est activé, la station utilise une méthode de transfert simplifiée et accélérée pour envoyer des fichiers vers le serveur. Ce mode est utile pour les environnements où la rapidité prime sur les fonctions avancées dans ce cas la station affichera des identifiants générés de manière aléatoire.

8.8.2.2 Envoi du lien de partage

Ce paramètre détermine si la station doit automatiquement envoyer, ou non, un lien permettant d'accéder aux fichiers partagés.

Le mode Demander vous invite à confirmer l'envoi à chaque partage.

À noter : L'envoie du lien de partage nécessite la version 2.4 du S3SRV.

8.8.2.3 Protocole de partage de fichiers

Vous pouvez choisir le protocole sécurisé utilisé pour la communication avec le serveur SFS.

Le choix dépend de votre infrastructure et des politiques de sécurité en vigueur :

- Le mode FTPS est typiquement utilisé pour les serveurs de partage « sur mesure » ou « non-S3SRV », ou dans le cas d'utilisation de serveurs Hogo S3SRV d'une version inférieure à v2.4. Il s'agit d'un mode considéré « Legacy » par Hogo.
- Le mode HTTPS est le mode standard actuel du couple « Station S3 – Serveur S3SRV ». Il permet de limiter les flux à ouvrir entre la station et le serveur et améliore la sécurité et la rapidité du transfert de fichiers SFS.

8.9 Réglages de scan



L'écran Réglages S3 vous permet de définir le comportement de la station blanche S3 lors de l'analyse des médias USB.

Cet espace regroupe l'ensemble des paramètres qui influencent le niveau de détection, la gestion des fichiers analysés, le traitement des menaces et la production du média de sortie.

Ces réglages doivent être adaptés aux exigences de sécurité de votre organisation et aux politiques internes en vigueur.



Cet écran vous permet de configurer les éléments suivants :

8.9.1 Mode de scan

Vous pouvez sélectionner le mode d'analyse appliqué lors du scan du média USB. Selon votre configuration, plusieurs niveaux sont disponibles :

- Normal : analyse standard, adaptée à la plupart des environnements peu sensibles.
- Intermédiaire : active des contrôles supplémentaires Ce mode est idéal dans la plupart des cas bureautiques et industriels.
- Avancé : active toutes les fonctions disponibles pour une analyse approfondie, parfaite dans un contexte sensible.

Le choix du mode dépend du compromis souhaité entre profondeur de l'analyse et temps de traitement.

8.9.2 Filtrage MIME

Le filtrage Smart MIME permet de vérifier le type MIME réel des fichiers (basé sur les extensions, mais également les Magic Numbers MIME afin de détecter les incohérences entre l'extension affichée et le contenu réel).

Vous pouvez :

- Oui (filtrer) : activer le contrôle MIME.
- Non (ne pas filtrer) : désactiver ce contrôle.

Ce mécanisme permet d'identifier les fichiers potentiellement altérés.

8.9.3 Action pour les MIME inconnus

Définit l'action appliquée lorsqu'un fichier présente un type MIME inconnu ou non conforme à votre dictionnaire :

- Isoler (sous-dossier) : déplace le fichier dans un dossier isolé sur le média de sortie.
- Ignorer (pas de copie) : le fichier n'est pas copié vers le média de sortie.
- Copie normale : le fichier est copié normalement

Ce réglage renforce la protection contre les fichiers atypiques ou suspects.

8.9.4 Contrôle SHA256

Permet d'activer ou non le calcul de l'empreinte SHA256 pour chaque fichier analysé :

- Activer : la valeur SHA256 est calculée et inscrite dans le journal de scan.
- Désactiver : la valeur SHA256 est calculée mais non inscrite dans le journal de scan.

Ce contrôle améliore la traçabilité et l'analyse post-incident.

8.9.5 Action sur les Avertissements

Lorsqu'un fichier est identifié comme un avertissement, la station peut appliquer l'une des actions suivantes :

- Ignorer : La notion d'avertissement n'apparaît pas pour l'utilisateur.
- Signaler : Les avertissements sont indiqués dans les journaux de scan et dans des pop-ups.
- Supprimer : Les avertissements sont traités comme des menaces et affichés à l'utilisateur dans un objectif pédagogique

L'action choisie doit refléter la politique de sécurité de votre organisation et le niveau de contrôle attendu. Cf. Annexe 2

8.9.6 Action sur la menace

Lorsqu'un fichier est identifié comme une menace, la station peut appliquer l'une des actions suivantes :

- Mise en Quarantaine : le fichier est isolé dans un dossier ZIP avec mot de passe.
- Suppression : le fichier est supprimé du média analysé.

L'action choisie doit refléter la politique de sécurité de votre organisation et le niveau de contrôle attendu.

À noter : Le mot de passe du fichier ZIP de mise en quarantaine est affiché dans le pop-up de fin d'analyse. Il est impératif de le conserver en lieu sûr, idéalement dans un coffre-fort numérique, car il ne pourra pas être récupéré par l'équipe support en cas de perte.

8.9.7 Action sur le média de sortie

Détermine la manière dont la station prépare le média USB de sortie :

- Vider la clef : efface le contenu du média avant d'y copier les fichiers analysés. (Cette option est l'option préconisée par HOGO)
- Ajouter les fichiers : conserve le contenu existant et ajoute les fichiers en sortie (dans ce cas, le token pour l'agent S3 n'est pas apposé sur le média USB)
- Copie normale : copie classique selon la politique définie

8.9.8 Tag de média USB pour S3Agent

Indique si la station doit apposer un marqueur spécifique sur le média USB en sortie :

- Oui : le tag S3Agent est ajouté au média.
- Clés autorisées : le tag S3Agent est ajouté seulement au média autorisé dans la liste de la station blanche.
- Non : aucun tag n'est appliqué.

8.9.9 Analyse des archives protégées

Définit la manière dont la station gère les archives protégées par mot de passe :

- Non, aucune : les archives protégées ne sont pas traitées.
- Clés autorisées : seules les archives dont le mot de passe correspond à une clé autorisée sont traitées.
- Oui (dictionnaire) : la station utilise un dictionnaire de mots de passe pour analyser les archives.

8.9.10 Actions disponibles

- Sauvegarder : enregistre les réglages configurés.
- Dictionnaire : ouvre la gestion des mots de passe utilisés pour l'analyse des archives protégées.
- Règles MIME : permet de consulter le dictionnaire MIME.
- Quitter : retourne à l'écran précédent sans sauvegarder.

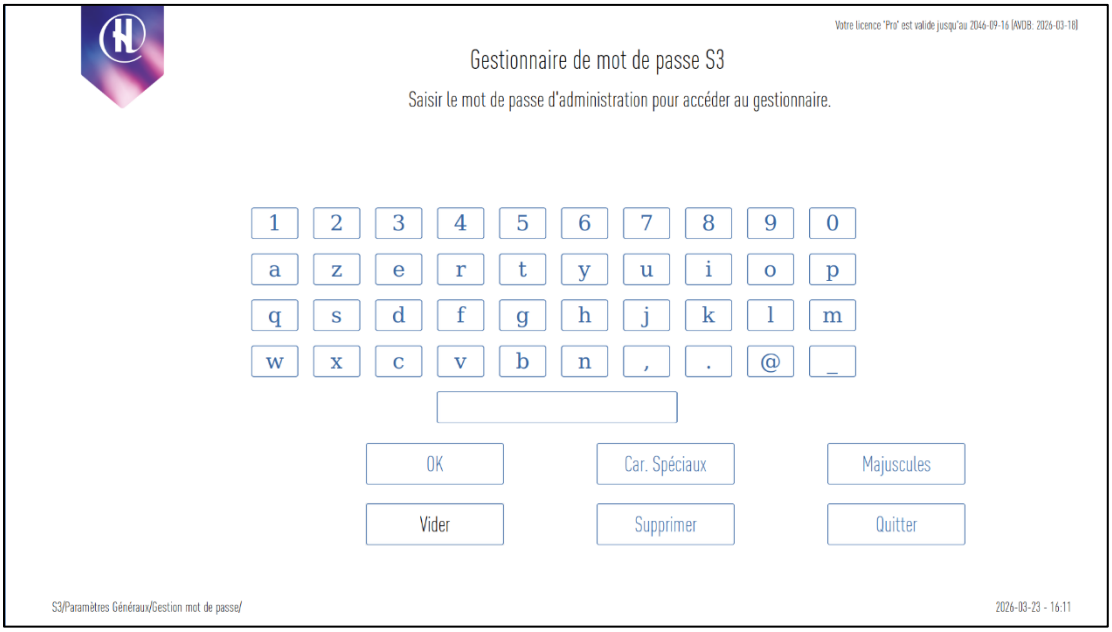
8.10 Modification du mot de passe



Le menu « Modification du mot de passe » permet à l'administrateur de changer les identifiants d'accès aux paramètres afin de garantir la confidentialité et la sécurité de la station.

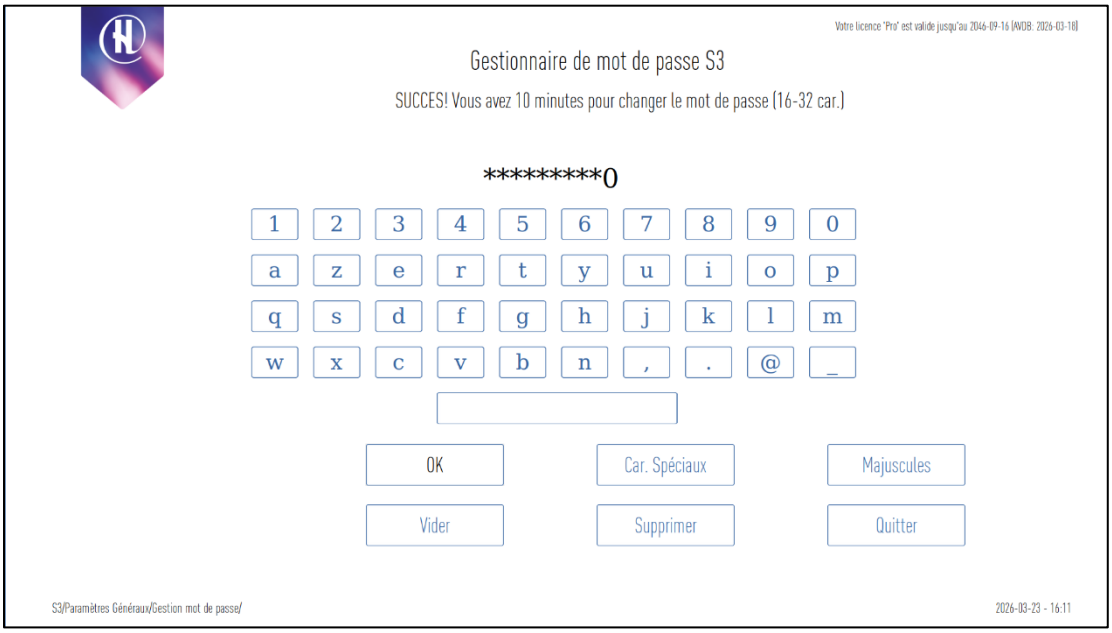
Cette fonctionnalité est essentielle pour prévenir les accès non autorisés et assurer une gestion conforme aux bonnes pratiques de sécurité.

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.



À noter : En cas de perte du mot de passe d'accès aux paramètres, aucune récupération à distance ne sera possible. Un renvoi de la station en SAV est obligatoire et non couvert par la garantie Hogo.

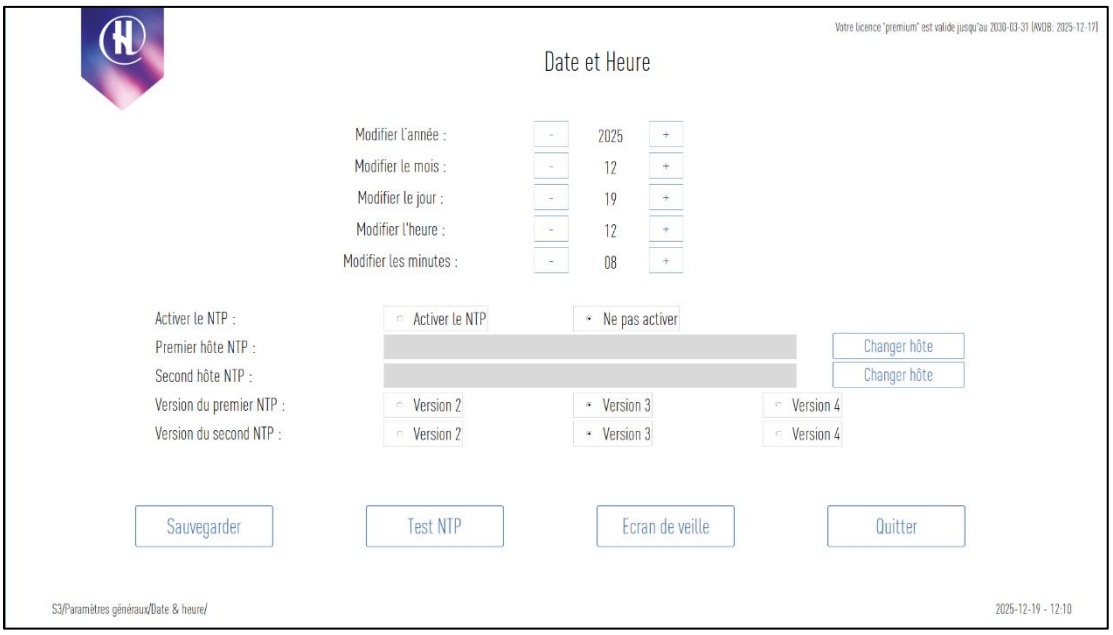
À noter : Le mot de passe initial de la station est « 1234567890 » il est important de le modifier à la première utilisation.

8.11 Date et heure



L'écran Date et Heure vous permet de configurer les informations temporelles de la station blanche S3.

Une horloge correctement réglée est essentielle au bon fonctionnement de nombreuses fonctionnalités, notamment la gestion des journaux, la synchronisation des mises à jour, la validation des certificats et la cohérence des opérations réalisées sur les médias USB.



Cet écran vous permet de définir ou de corriger les éléments suivants :

- La date du système
- L'heure du système
- Les éventuels serveurs NTP utilisés par la station (activation ou non, hôte ou IP des deux serveurs, versions du protocole NTP)

Vous pouvez modifier chacun de ces paramètres après authentification administrateur.

Une heure ou une date incorrecte peut entraîner :

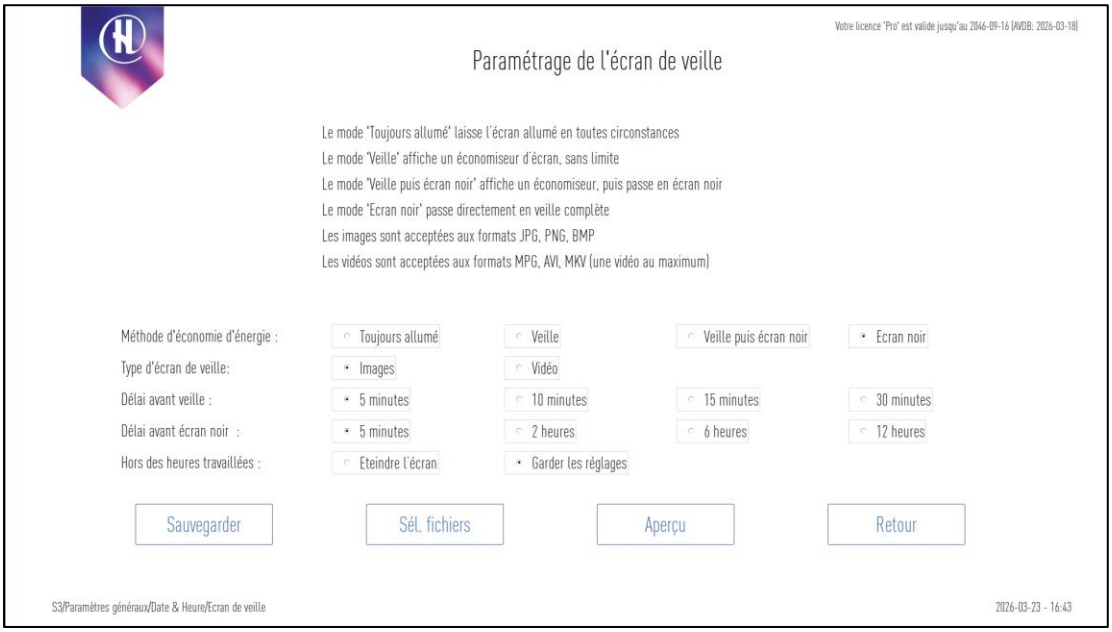
- Des incohérences dans les journaux de scan et dans les logs techniques,
- Des difficultés pour retracer des évènements de sécurité,
- Un rejet éventuel de certains certificats si leur période de validité semble incorrecte,
- Des erreurs dans les systèmes externes dépendant d'un horodatage précis.

Selon les politiques de votre organisation, vous pouvez réaliser ces réglages manuellement ou vous appuyer sur une synchronisation externe. Dans un environnement totalement déconnecté, il est particulièrement important de s'assurer régulièrement que l'horloge du système reste synchronisée.

Une fois les réglages effectués, sélectionnez le bouton Sauvegarder pour appliquer vos modifications, ou Quitter pour revenir à l'écran précédent sans enregistrer les changements.

8.11.1 Écran de veille

Ce bouton permet d'accéder aux paramètres de l'écran de veille de la station.



- Mode du système de veille : Permet de choisir le comportement de la station après un temps donné d'inactivité.
- Type d'économiseur d'écran : Permet de choisir le type d'écran de veille utilisé par la station après un temps d'inactivité. L'affichage d'une vidéo (codec MPEG et durée < 2 minutes recommandés) ou un défilement d'images (12 maximum).
- Délai avant économiseur : Permet de choisir le temps d'inactivité nécessaire avant le lancement de l'économiseur.
- Délai avant mise en veille : Permet de choisir le temps nécessaire d'économiseur avant la mise en veille de la station (écran noir).
- Hors de heures travaillées : Comportement de la station hors des heures travaillés (entre 19h et 7h)

9 Mise à jour Initiale

La mise à jour initiale constitue une étape obligatoire avant la première utilisation opérationnelle de votre station blanche S3. Elle permet d'installer l'ensemble des composants nécessaires au bon fonctionnement de la station : moteurs d'analyse activés dans votre configuration, bases de signatures, modules du Core S3 et paramètres de sécurité essentiels.

Avant de procéder à cette mise à jour, vous devez au préalable configurer la station.

Deux options vous sont proposées :

- Configuration manuelle : vous renseignez vous-même les différents paramètres réseau et les sources de mise à jour.
- Configuration via le Wizard : un assistant de configuration guidée qui vous pose une série de questions simples pour réaliser les réglages indispensables (réseau, source des mises à jour, paramètres de base).

Le choix entre configuration manuelle ou assistée dépend de vos préférences ou de la politique de votre organisation. Dans les deux cas, vous devez définir les paramètres réseaux et les paramètres de mise à jour avant de lancer la mise à jour initiale.

Une fois la configuration réseau établie ou le média de mise à jour préparé, il est recommandé de lancer une mise à jour initiale pour :

- Vérifier que les moteurs d'analyse activés dans votre configuration sont bien installés et fonctionnels ;
- Actualiser les bases de signatures et les composants du Core ;
- Synchroniser les paramètres nécessaires avec votre serveur interne S3SRV, si vous utilisez un déploiement On-Premise ;
- Garantir une cohérence complète entre la configuration usine et votre environnement de production.

Même si un scan peut être techniquement réalisé sans mise à jour initiale, il est déconseillé de procéder à l'analyse d'un média USB tant que la station n'a pas été vérifiée et harmonisée avec votre infrastructure. Une mise à jour initiale constitue donc une bonne pratique indispensable, renforçant la fiabilité des détections et la conformité de l'équipement.

Une fois la mise à jour initiale effectuée, il est recommandé d'effectuer un test de fonctionnement afin de confirmer que la station est pleinement opérationnelle avant une utilisation régulière (voir chapitre suivant).

10 Tests de fonctionnement

Après l'installation et la mise à jour initiale de votre station blanche S3, il est recommandé d'effectuer un test de fonctionnement afin de vérifier que l'équipement est correctement configuré et pleinement opérationnel.

Ce test permet de valider les principaux éléments du système : interface utilisateur, détection antivirus, fonctionnement du Core et gestion des médias USB.

Pour réaliser ce test, vous pouvez utiliser un média USB de contrôle (contenant par exemple un fichier de test sécurisé tel qu'un fichier EICAR, voir ci-dessous). La station blanche S3 disposant de plusieurs ports USB, il est conseillé de tester chaque port afin de confirmer le bon fonctionnement matériel de l'ensemble des connectiques.

Pour chaque port USB testé, vérifiez que :

- Le média est correctement détecté par la station ;
- Le scan démarre et se déroule normalement ;
- Les fichiers sont analysés selon les réglages définis (moteurs d'analyse, filtrage MIME, contrôle SHA256…) ;
- Les éventuelles menaces de test sont correctement identifiées et traitées selon la politique définie (suppression, quarantaine, isolement…) ;

À l'issue de l'analyse, vous pouvez consulter les journaux de scan afin de confirmer que l'ensemble des modules a fonctionné comme prévu et qu'aucune anomalie n'a été détectée.

Ce test simple garantit que la station blanche S3 est prête et qu'elle répond aux exigences de sécurité requises.

À noter : Pour réaliser des tests de détection antivirus, vous pouvez utiliser le fichier de test EICAR, spécialement conçu pour vérifier le bon fonctionnement des moteurs d'analyse sans présenter aucun risque pour votre système.

Ce fichier est reconnu comme une menace par la majorité des antivirus, ce qui permet de valider que la station blanche S3 réagit correctement. Vous pouvez le télécharger depuis le site officiel : https://www.eicar.org/download-anti-malware-testfile

Ce fichier est disponible sous plusieurs formats (texte, exécutable simulé, fichiers ZIP) afin de tester différents scénarios de détection.

11 S3Core Rescue mode

L'écran de Rescue est un écran s'affichant en cas de problème au démarrage.



A l'apparition de cet écran :

- Branchez un média USB à votre station
- Sélectionnez « Export data for Tech Support »
- Créez un ticket auprès du support en joignant votre export https://support.hogo.eu
- Suivez les instructions du support

À noter : L'utilisation de « Restore factory Core configuration » supprimera la totalité de vos données stockées dans la station et nécessitera de contacter le support pour une remise en fonctionnement. Vos données ne pourront pas être récupérées. L'utilisation de ce mode ne doit pas être effectuée sans une demande explicite du support.

12 Avertissements complémentaires

Afin de garantir un fonctionnement sécurisé et conforme de la station blanche S3, veuillez respecter les points suivants :

- ➔ Utilisez uniquement des clés USB en bon état et sans défaut physique.
- ➔ N'insérez jamais un média endommagé, humide ou déformé dans la station.
- ➔ Ne retirez pas un média USB pendant un scan, une copie ou un formatage.
- ➔ Vérifiez régulièrement que la station dispose de versions récentes des moteurs d'analyse.
- ➔ Réalisez une mise à jour initiale avant la première utilisation opérationnelle.
- ➔ Activez les mises à jour automatiques lorsque les politiques internes le permettent.
- ➔ Pour les environnements déconnectés, mettez à jour régulièrement via clé USB, exportez les logs, vérifiez la date et l'heure de la station (1 fois par semaine).
- ➔ Conservez le mot de passe administrateur dans un lieu sûr (comme un coffre-fort numérique) ; sa perte nécessite un retour SAV non couvert par la garantie.
- ➔ Changez périodiquement le mot de passe administrateur conformément à vos règles internes.
- ➔ Ne communiquez jamais les identifiants d'administration à du personnel non autorisé.
- ➔ Si vous utilisez le contrôle PCSC, ajoutez les badges autorisés avant l'activation.
- ➔ N'éteignez jamais la station pendant un formatage, un scan ou une mise à jour.
- ➔ Utilisez le mode avancé de formatage uniquement si un effacement renforcé est requis.
- ➔ Assurez-vous que les paramètres réseau (IP, DNS, passerelle...) sont exacts avant d'activer une mise à jour réseau.
- ➔ Utilisez uniquement les paramètres proxy fournis par votre service informatique.
- ➔ Veillez à ne pas obstruer les aérations de la station.
- ➔ Réalisez régulièrement un test de fonctionnement (EICAR, ports USB, mise à jour).
- ➔ Consultez les journaux en cas de comportement inhabituel.
- ➔ Exportez périodiquement les logs techniques pour archivage ou diagnostic.

En cas de doute ou d'incident, pensez à faire un export des « logs techniques » et à les communiquer dans votre demande au support :

https://support.hogo.eu

Annexe 1 – Déroulé du Wizard de configuration

1. Mode de mise à jour :

- Local (USB) ⟶ Accès direct au résumé de la configuration.
- LAN (réseau local) ⟶ Poursuite vers la sélection du type de serveur.
- Cloud ⟶ Poursuite vers la configuration des mises à jour automatiques.

2. Sélection du type de serveur (LAN uniquement)

- Serveur de Gestion
  - Saisir l'adresse ou le nom du serveur de Gestion.
  - Saisir le code secret (management).
  - Saisir le Code IV.
- Serveur de Dépôt
  - Saisir l'adresse ou le nom du serveur de Dépôt.

➔ Poursuite vers la configuration des mises à jour automatiques

3. Mises à jour automatiques

- Oui
  - Saisir l'heure d'exécution de la mise à jour automatique (valeur comprise entre 0 et 23).
- Non

➔ Poursuite vers le type de connexion au réseau.

4. Type de connexion au réseau

- Câble (RJ45)
- Wi-Fi
  - Saisir le SSID du réseau Wi-Fi.
  - Indiquer si le réseau Wi-Fi est masqué (Oui / Non).
  - Configuration de la sécurité Wi-Fi :
    - Saisir le mot de passe

- Pas de mot de passe (réseau ouvert)

➔ Poursuite vers le mode d'adressage IP.

5. Mode d'adressage IP

- DHCP (automatique)
- Statique (IP fixe)
  - Saisir l'adresse IP statique.
  - Saisir le masque au format CIDR (valeur comprise entre 0 et 32).
  - Saisir l'adresse de la passerelle.

➔ Poursuite vers la configuration DNS.

6. Configuration DNS

- Automatique (DHCP / passerelle)
- Manuel
  - Saisir l'adresse du serveur DNS (IPv4).

➔ Poursuite vers le résumé de la configuration.

7. Résumé de la configuration

- Le système affiche un résumé complet de la configuration.
- L'administrateur valide la configuration en sélectionnant OK, ce qui termine la procédure.

Annexe 2 – Définition des couleurs de signets

