HR-PR-21-092 v8

Manuel d'Administration du S3Agent

Ce document constitue le manuel d'administration du logiciel S3Agent fourni par Hogo. Il contient les indications relatives à l'installation, la désinstallation, et le réglage avancé du S3Agent, y compris les valeurs seulement accessibles aux administrateurs des postes de travail.

Versions

#	Détail
1	Emission initiale du document.
2	Mise à jour du modèle documentaire, ajout des éléments liés à l'installation et la désinstallation.
3	Mise à jour chapitre 3.2 (Serial Extractor)
4	Ajout de la clef de registre s3srvcommunicate
5	Ajout des fichiers de configuration permettant la gestion fine du S3Filter
6	Ajout procédure S3Agent Windows XP et précision sur l'installation
7	Ajout de la clef « s3agents3eject » pour désactivation du bouton de l'IHM principale
8	Ajout de la nouvelle version du ConfigManager

Table des matières

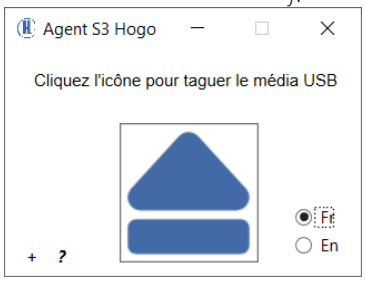
1 Introduction 3
2 Gestion du déploiement 4
2.1 Installation directe MSI 4
2.2 Désinstallation directe MSI 5
2.3 Utilitaire d'automatisation Hogo 6
2.4 Démarrage automatique 6
3 Fichiers locaux de configuration 8
3.1 Stockage des fichiers 8
3.2 Listes blanches de périphériques 8
3.3 Action de retag automatique 8
3.4 Lien avec le S3Filter 9
3.4.1 Sollicitation périodique du S3Filter 9
3.4.2 Ouverture automatique des clefs USB connectées au S3Filter 9
3.5 Filtrage des périphériques spécifiques 9
3.5.1 Valeurs possibles 9
3.5.2 Filtrage des clefs BitLocker 9
3.5.3 Filtrage des clefs TrueCrypt 9
3.5.4 Filtrage des smartphones/médias 9
4 Certificat spécifique pour le S3Agent 10
5 Clefs de registre 10
6 Gestion de la configuration S3Agent 11

1 Introduction

Le logiciel S3Agent de Hogo permet le filtrage des clefs USB sur le poste où il est installé. S'il est actif, les clefs autorisées seront seulement les clefs branchées via un S3Filter, ou les clefs préalablement taguées par une station S3.

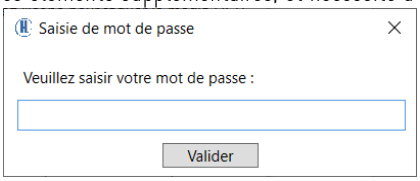
Il se présente sous la forme d'un service, nommé « Hogo S3Agent Service » (actif en tant que Local System sous Microsoft Windows) et d'une IHM liée, nommée « S3Agent » et affichant une icône dans le menu Tray.

L'interface graphique du S3Agent, accessible par clic sur l'icône du menu Tray, est la suivante :

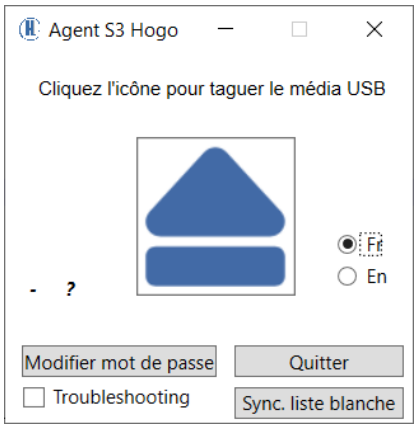


Le point d'interrogation ouvre une aide sommaire, le menu « FR / EN » permet de changer la langue de l'interface, et le bouton central permet d'éjecter un média précédemment accepté par le S3Agent, en réapposant un tag sur celui-ci.

Le bouton « + » permet d'accéder à quelques éléments supplémentaires, et nécessite d'utiliser un mot de passe (voir chapitre 5) :



Une fois le mot de passe saisi, il est possible de modifier celui-ci, de passer en mode « troubleshooting » (beaucoup plus de lignes de logs à générer, utile pour les phases de test), de quitter l'IHM, ou encore de synchroniser manuellement les listes blanches de périphériques avec le S3SRV (cf. chapitre 3.2) :



Ce logiciel supporte également plusieurs options de configuration avancées, qui sont décrites ci-après. Ces options sont stockées en fichiers (chapitre 3) ou en clefs de registre (chapitre 5).

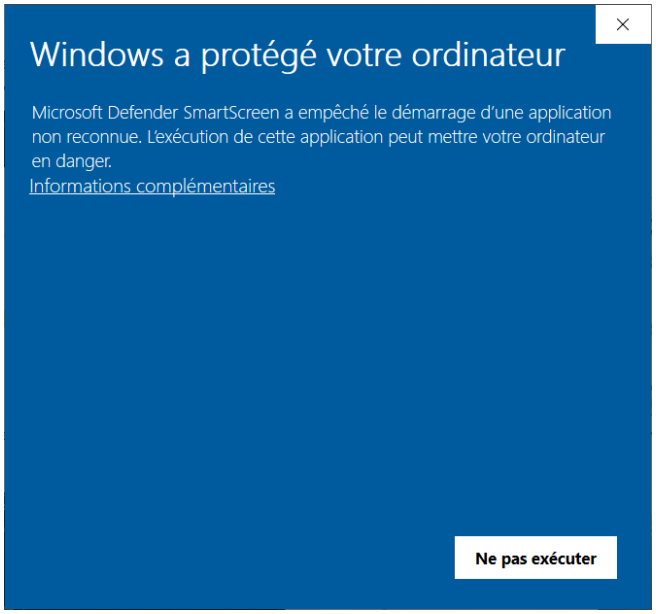
Le mode d'encodage des options, ainsi qu'un outil pour configurer rapidement celles-ci, sont fournis au chapitre 4.

2 Gestion du déploiement

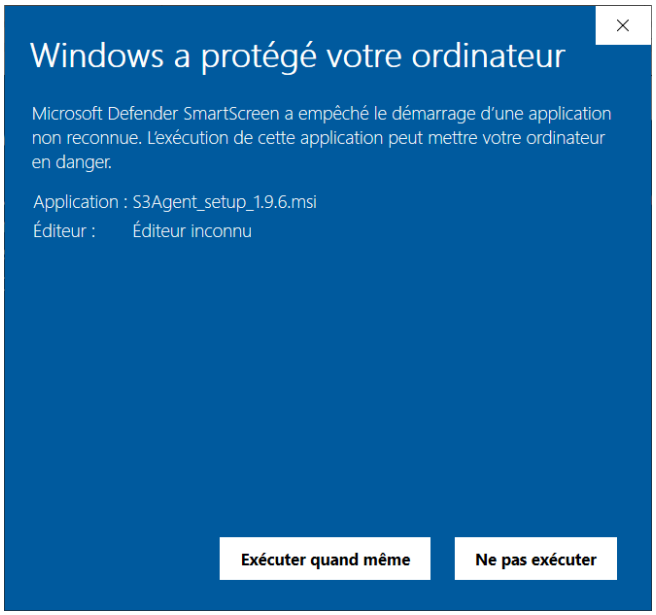
2.1 Installation directe MSI

L'installation via MSI est réalisée en ouvrant le fichier « MSI » fourni par Hogo.

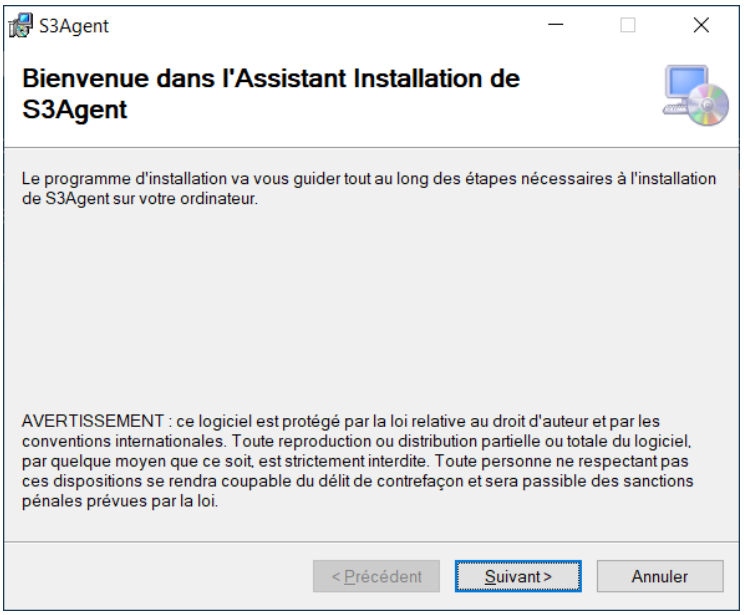
Attention : un message d'avertissement peut être affiché par le poste de travail, il convient alors de cliquer sur « Informations complémentaires » puis « Exécuter quand même » :



Cliquer sur « Informations complémentaires » puis sur « Exécuter quand même dans la seconde fenêtre :



Une fois l'installeur MSI lancé, la fenêtre suivante s'affiche :



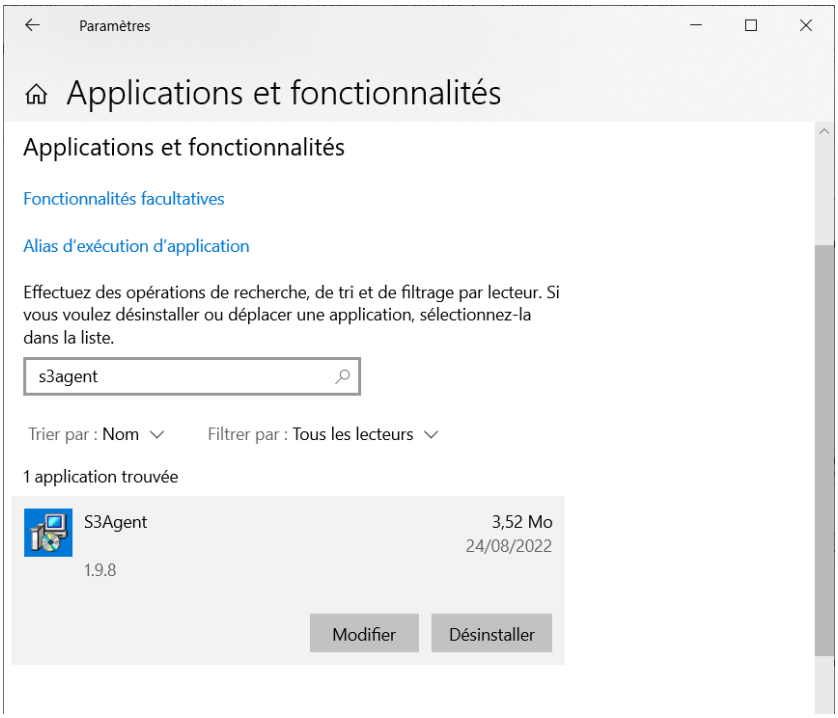
Pour finaliser l'installation, cliquer sur « Suivant » jusqu'à la fin de la procédure.

Note : il est possible de lancer le même processus sans interface graphique, en utilisant la commande MSIEXEC :

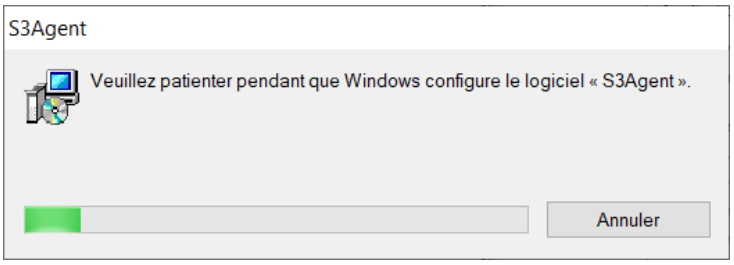
```
msiexec /package Application.msi /quiet
```

2.2 Désinstallation directe MSI

Pour désinstaller le S3Agent, lancer l'utilitaire « Application et fonctionnalités », rechercher le logiciel « S3Agent », le sélectionner, et cliquer sur « Désinstaller » :



L'utilitaire de gestion des logiciels installés va automatiquement supprimer le logiciel et le service du S3Agent :



La procédure est terminée une fois que la barre de progression est remplie.

A noter : une désinstallation par ce biais ne supprime ni les fichiers locaux de configuration (chapitre 3) ni les clefs de registre (chapitre 5), ni le journal des applications liés au S3Agent : « Journaux | Applications et services | S3Log ».

2.3 Utilitaire d'automatisation Hogo

Hogo fourni un logiciel permettant d'automatiser les fonctions suivantes :

- Désinstallation de toute version précédente du S3Agent sur un poste (y compris arrêt des logiciels et services)
- Installation d'une nouvelle version
- Option : initialisation automatique de la liste des périphériques internes, (chapitre 3.2)

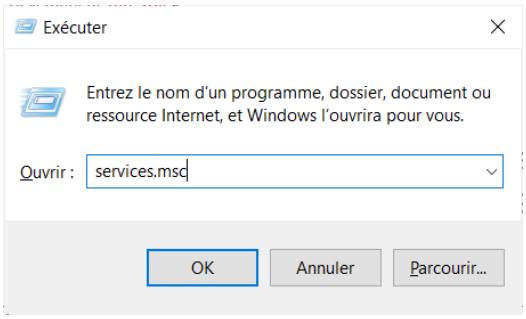
Ce logiciel se lance en invite de commande, en mode administrateur : `"Hogo.InstallManager.exe"`

- La version précédente est désinstallée
- Si un fichier MSI nommé `"S3Agent.msi"` est présent dans le même dossier, il est installé
- Si la commande saisie contient l'option `"initList"`, la liste interne est initialisée.

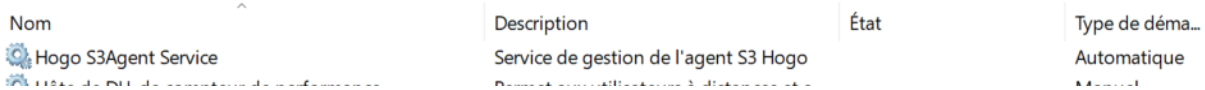
A noter : une désinstallation par ce biais ne supprime ni les fichiers locaux de configuration (chapitre 3) ni les clefs de registre (chapitre 5), ni le journal des applications liés au S3Agent : « Journaux | Applications et services | S3Log ».

2.4 Démarrage automatique

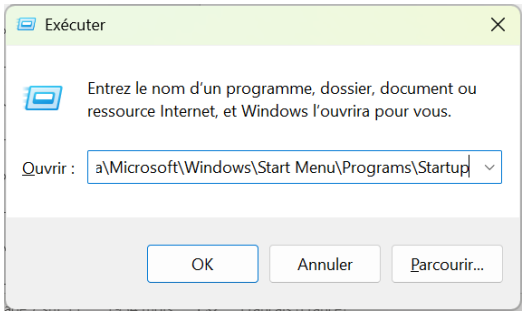
Pour vérifier le démarrage automatique du service, lancer « Windows + R » (fenêtre d'exécution) et saisir la commande « services.msc » :



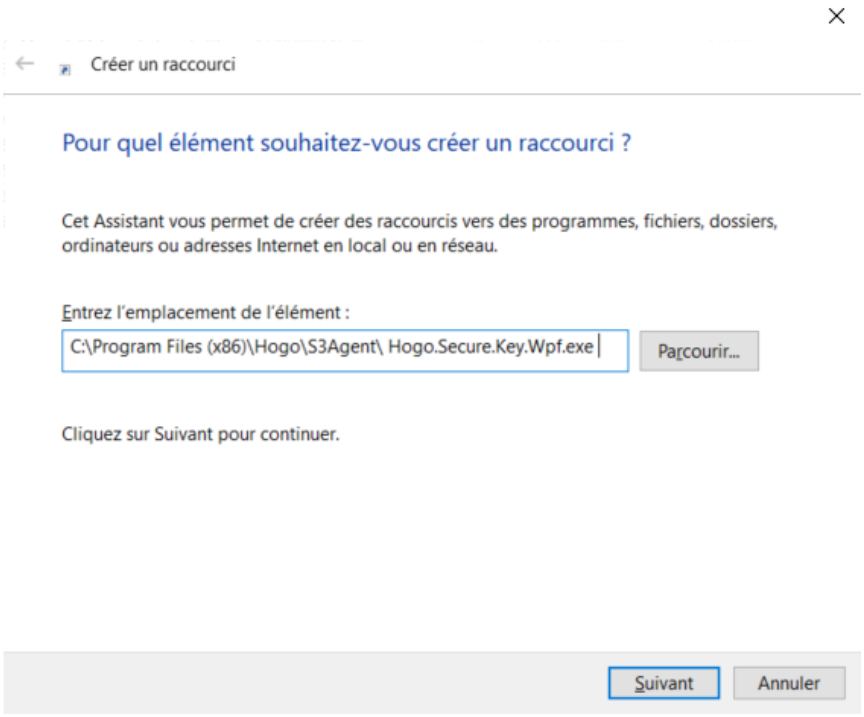
Dans la liste des services, vérifier que la ligne « Hogo S3Agent Service » existe et est bien en lancement automatique :



Pour vérifier le démarrage automatique de l'interface homme-machine, lancer « Windows + R » (fenêtre d'exécution) et saisir la commande « `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup` » :



Créer un nouveau raccourci dans le dossier qui s'ouvre, en pointant vers :
« C:\Program Files (x86)\Hogo\S3Agent\ Hogo.Secure.Key.Wpf.exe »



3 Fichiers locaux de configuration

3.1 Stockage des fichiers

Tous les fichiers de configuration doivent être stockés dans le dossier suivant : `C:\ProgramData\Hogo\S3Agent`

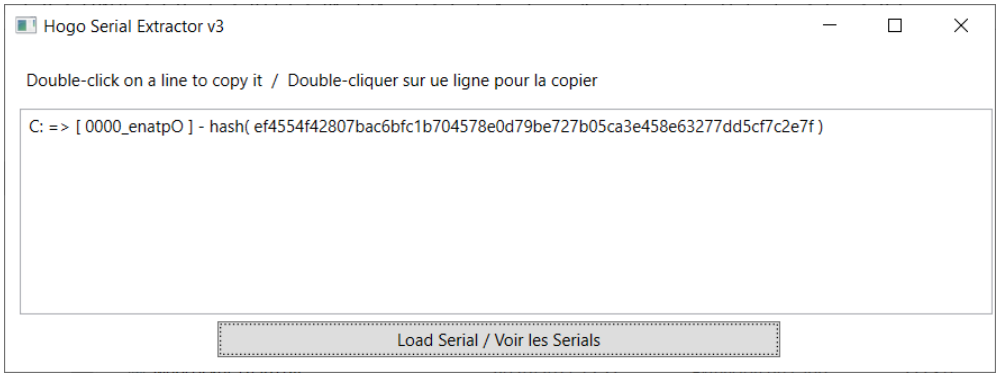
3.2 Listes blanches de périphériques

Le S3Agent peut considérer certains médias comme spécifiquement autorisés (sans nécessité de tag), ce sont les périphériques « en liste blanche ». Les numéro de série de ces périphériques doivent être enregistrés, hashés, dans : `"whiteUSB.list"`

Dans le cas de l'usage de disques durs externes « à demeure » sur un poste de travail, il est également possible pour le S3Agent de ne pas les filtrer (autorisés par défaut) en les considérants comme « périphériques internes ». Dans ce cas ; les numéros de série doivent être enregistrés dans : `"hogo.init.conf"`

Le S3SRV peut être utilisé par le S3Agent pour récupérer la liste des médias USB autorisés en liste blanche (premier cas décrit ci-dessus). Dans ce cas, les clefs de registre doivent demander cette synchronisation (cf. plus bas) et l'adresse ou l'IP du S3SRV local doit dans ce cas être renseigné dans le fichier : `"s3srv.addr"`

Pour récupérer les numéros de série des disques durs, il convient d'utiliser l'outil Hogo « Serial Extractor », qui liste les numéros de série (pour `"hogo.init.conf"`) et leur version hashée (pour `"whiteUSB.list"`) des disques et médias connectés :



3.3 Action de retag automatique

Il est possible pour le S3Agent de retaguer périodiquement, automatiquement, les périphériques USB qui sont connectés au poste de travail et qui ont été acceptés.

Pour cela, il convient d'écrire la valeur « True » compilée avec l'utilitaire Hogo (chapitre 4) dans `"hogo.retag.conf"`, et de définir l'intervalle de retag, en secondes, dans la base de registre (cf. chapitre 5).

3.4 Lien avec le S3Filter

3.4.1 Sollicitation périodique du S3Filter

Il est possible pour le S3Agent de solliciter régulièrement l'IP 10.34.58.37 pour afficher des infobulles « S3Filter connecté », « S3Filter démarré », « Clef USB connectée au S3Filter »...

Pour cela, il convient d'écrire la valeur « true » compilée avec l'utilitaire Hogo (chapitre 4) dans `"hogo.s3filter.conf"`.

3.4.2 Ouverture automatique des clefs USB connectées au S3Filter

Il est possible pour le S3Agent d'ouvrir automatiquement l'explorateur Windows dans le dossier correspondant à la dernière clef USB branchée au S3Filter lors de la détection de l'évènement « Clef USB connectée au S3Filter »...

Pour cela, il convient d'écrire la valeur « true » compilée avec l'utilitaire Hogo (chapitre 4) dans `"hogo.openS3Fusb.conf"`.

3.5 Filtrage des périphériques spécifiques

Les périphériques dits « spécifiques » sont les périphériques chiffrés, en BitLocker ou en Veracrypt / Truecrypt, et les périphériques média (smartphones par exemple). Pour chacun de ces types de périphérique, il est possible de définir une politique à appliquer par l'agent, en écrivant une valeur particulière dans un fichier de configuration.

Ces valeurs sont données ci-après, ainsi que les fichiers paramétrant le comportement du S3Agent pour chaque type de périphérique.

3.5.1 Valeurs possibles

Trois valeurs sont possible pour le filtrage des périphériques spécifiques :

- « ignore » : ignorer les périphériques, c'est-à-dire laisser l'OS se charger de leur montage et ne pas les filtrer
- « filter » : vérifier la présence de tag sur le périphérique, ne bloquer que si celui-ci est absent ou invalide et autoriser le périphérique sinon
- « block » : ignorer la présence du tag et systématiquement bloquer le périphérique.

3.5.2 Filtrage des clefs BitLocker

Le paramétrage du S3Agent relatif au filtrage des clefs BitLocker est réalisé via l'écriture de l'option souhaitée dans le fichier :

`“hogo.bitlocker.conf”`

3.5.3 Filtrage des clefs TrueCrypt

Le paramétrage du S3Agent relatif au filtrage des clefs TrueCrypt[1] est réalisé via l'écriture de l'option souhaitée dans le fichier :

`"hogo.veracrypt.conf"`

3.5.4 Filtrage des smartphones/médias

Le paramétrage du S3Agent relatif au filtrage des périphériques de type « média » (smartphone...) est réalisé via l'écriture de l'option souhaitée dans le fichier :

`"hogo.phone.conf"`

[1] Les clefs doivent être formattées en deux partitions, la première étant une partition lisible, contenant par exemple le logiciel TrueCrypt portable, et la seconde étant une partition invisible, chiffrée.

4 Certificat spécifique pour le S3Agent

Le S3Agent peut utiliser un certificat de salage spécifique à votre organisation, pour caractériser les tag réalisés par vos stations S3 et les discriminer des tags des autres stations blanches vendues par Hogo.

Ce certificat est composé de chiffres, de lettres minuscules et de lettres majuscule, et est scindé par un tiret « - ».

Pour stocker un certificat propre à votre organisation, stocker le texte de celui-ci dans le fichier `"hogo.certif.conf"`

5 Clefs de registre

Les clefs de registre utilisées par le S3Agent sont situées dans[2] : `\LOCAL_MACHINE\SOFTWARE\Hogo`

Ces clefs sont les suivantes :

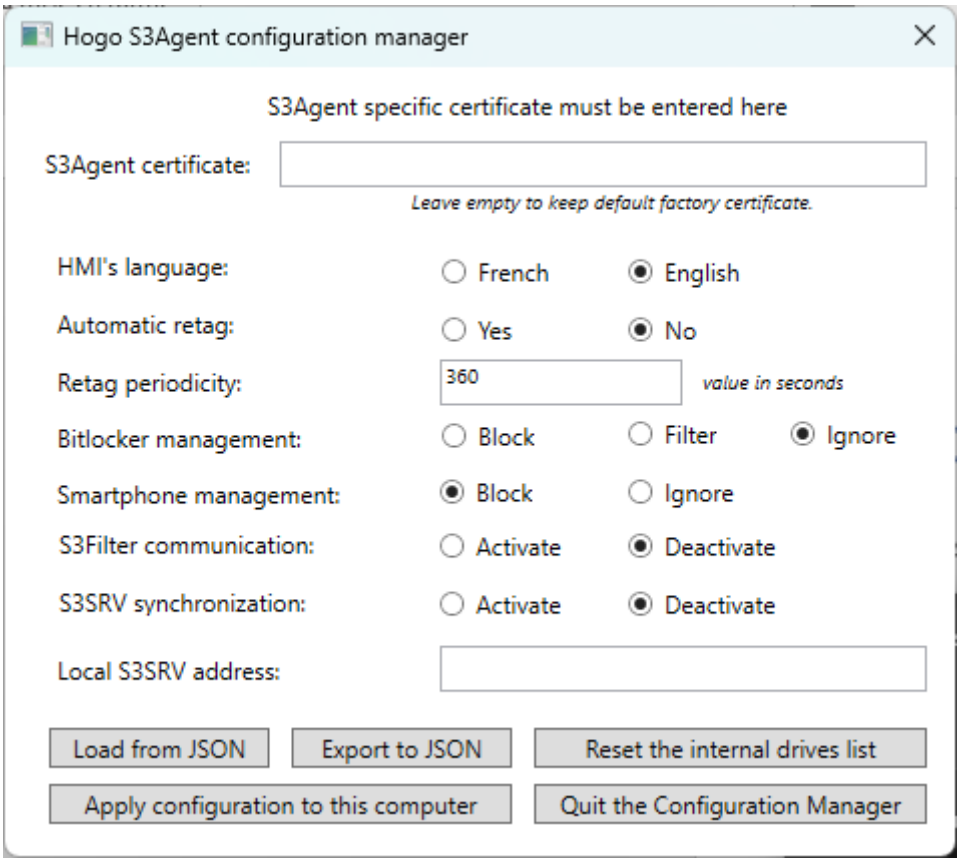
- `s3agentvers` : contient le numéro de version du S3Agent (ne pas modifier)
- `s3agentpass` : contient une forme salée et hachée du mot de passe de l'IHM du S3Agent
- `s3agentmenu` : booléen permettant l'affichage, ou non, du menu contextuel « S3Eject » sur les lecteurs de disque
- `s3agents3eject` : booléen permettant l'affichage, ou non, du bouton « S3Eject » dans la fenêtre applicative S3Agent
- `s3agentretag` : valeur numérique définissant, en secondes, l'intervalle entre deux retag automatiques
- `s3srvcommunicate` : booléen permettant d'activer la communication avec un S3SRV local (défaut : false)

Certaines clefs sont initialisées lors du lancement du Service du S3Agent, d'autres doivent être créées manuellement (le S3Agent utilise les valeurs par défaut sans créer ses clefs dans le registre).

[2] Avec la redirection des clefs de registre Windows pour la gestion des applications 32bits vs 64bits, ces clefs peuvent être situées dans un nœud WOW64 ou WOW6432node, voir : https://learn.microsoft.com/fr-fr/windows/win32/winprog64/shared-registry-keys

6 Gestion de la configuration S3Agent

Il est possible de générer les valeurs de configuration décrites au chapitre précédent grâce à l'utilitaire « Hogo.Config.Manager ».



Le certificat spécifique de votre S3Agent doit être saisi dans « S3Agent Certificate ».

Chaque valeur peut ensuite être cochée et appliquée grâce à « Apply configuration ».

Il est également possible d'importer ou d'exporter une configuration au format JSON, pour l'appliquer simplement sur plusieurs postes de travail.

Enfin, il est possible de réinitialiser la liste des disques internes du poste de travail en cliquant sur « Reset the internal list ».

L'outil est accessible sur le lien suivant :

https://hogo.eu/zone_echange/outils_hogo/Hogo.Config.Manager.v1.5.zip