HR-PR-21-092 v7en

Administration manual for the S3Agent

This document is the administration manual for the S3Agent software provided by Hogo. It contains instructions for installing, uninstalling, and advanced configuration of the S3Agent, including values accessible only to workstation administrators.

Versions

#	Détail
1	Initial release of the document.
2	Update of the document template; addition of elements related to installation and uninstallation.
3	Update of section 3.2 (Serial Extractor).
4	Addition of the registry key `s3srvcommunicate`.
5	Addition of configuration files for fine-tuned management of S3Filter.
6	Addition of the S3Agent procedure for Windows XP and clarification on the installation process.
7	Addition of the `s3agents3eject` registry key to disable the button in the main GUI.

Table of contents

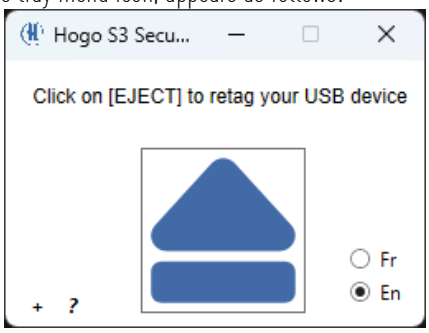
1 Introduction ... 3
2 Installation management ... 4
2.1 Direct MSI install ... 4
2.2 Direct MSI uninstall ... 4
2.3 Automatic installer provided by Hogo ... 5
2.4 Automatic start of the HMI ... 5
3 Local configuration files ... 6
3.1 Files storage ... 6
3.2 USB media whitelist ... 6
3.3 Automatic retag function ... 6
3.4 Link with the S3Filter device ... 7
3.4.1 Periodic Polling of the S3Filter ... 7
3.4.2 Automatic Opening of USB Keys Connected via S3Filter ... 7
3.5 Filtering of Specific Devices ... 7
3.5.1 Possible Values ... 7
3.5.2 Filtering BitLocker Devices ... 7
3.5.3 Filtering TrueCrypt Devices ... 7
3.5.4 Filtering Smartphones / Media Devices ... 7
4 Specific Certificate for S3Agent ... 8
4.1 Certificate Storage ... 8
4.2 Encoded Configuration Values ... 8
5 Registry keys ... 9

1 Introduction

The S3Agent software by Hogo enables USB key filtering on the workstation where it is installed.
When active, only USB keys connected via an S3Filter or previously tagged by an S3 station will be authorized.

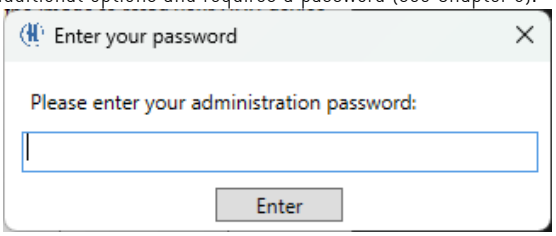
It consists of a service named "Hogo S3Agent Service" (running as Local System under Microsoft Windows), and an associated graphical user interface (GUI) named "S3Agent", which displays an icon in the system tray.

The S3Agent GUI, accessible by clicking the tray menu icon, appears as follows:

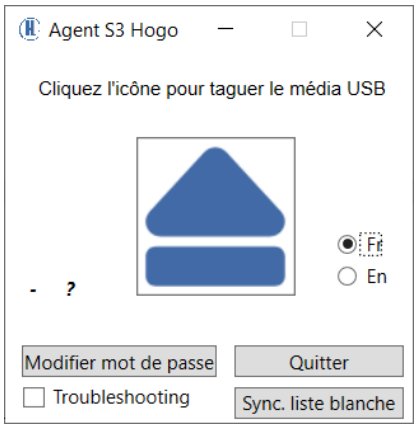


The question mark opens a basic help window, the "FR / EN" menu allows switching the interface language, and the central button is used to eject a previously accepted device by the S3Agent, reapplying a tag to it.

The "+" button provides access to additional options and requires a password (see Chapter 5).



Once the password is entered, it becomes possible to change it, to switch to "troubleshooting" mode (which generates much more detailed logs, useful during testing phases), to exit the GUI, or to manually synchronize the device whitelists with the S3SRV (see Chapter 3.2).



This software also supports several advanced configuration options, which are described below. These options are stored in files (see Chapter 3) or in registry keys (see Chapter 5).

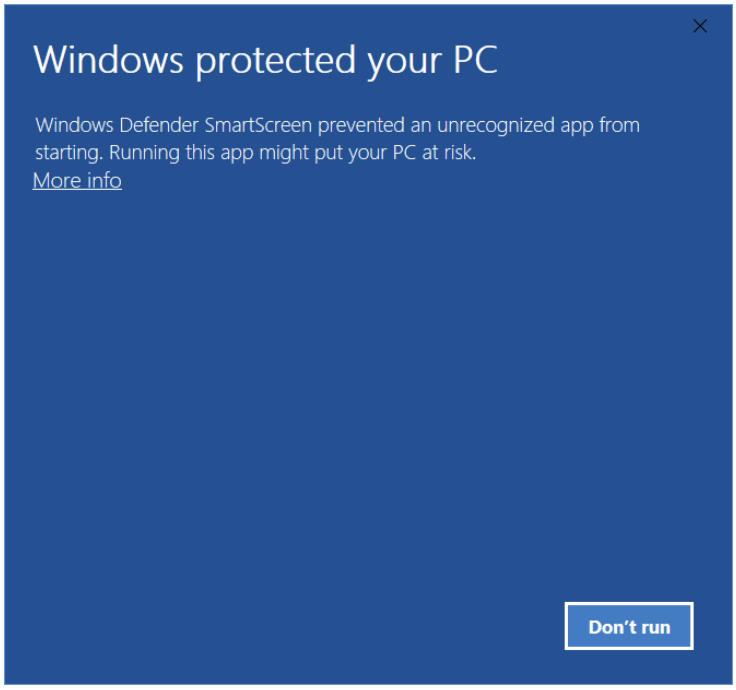
The encoding method for these options, as well as a tool to quickly configure them, are provided in Chapter 4.

2 Installation management

2.1 Direct MSI install

Installation via MSI is performed by opening the MSI file provided by Hogo.

Warning: a security prompt may be displayed by the workstation; in that case, click "More info", then "Run anyway":



Once the installation start, the standard MSI interface will appear.
To complete the installation, click "Next" until the end of the setup process.

Note: the same process can be launched without a graphical interface using the MSIEXEC command:

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

2.2 Direct MSI uninstall

To uninstall the S3Agent, open the "Apps & Features" utility, search for the "S3Agent" software, select it, and click "Uninstall".

The installed software management utility will automatically remove the S3Agent software and service.
The process is complete once the progress bar reaches the end.

Note: uninstalling via this method does not remove the local configuration files (see Chapter 3), the registry keys (see Chapter 5), or the application log related to S3Agent: "Event Logs | Applications and Services | S3Log."

2.3 Automatic installer provided by Hogo

Hogo provides a tool that automates the following functions:

- Uninstallation of any previous version of S3Agent on a workstation (including stopping services and applications)
- Installation of a new version
- Optional: automatic initialization of the internal device list (see Chapter 3.2)

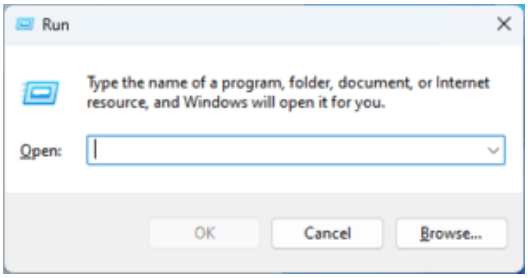
This tool is launched from a command prompt with administrator privileges using: `Hogo.InstallManager.exe`

- The previous version is uninstalled
- If a file named `S3Agent.msi` is present in the same directory, it is installed
- If the command includes the `initList` option, the internal list is initialized

Note: uninstalling using this method does not remove local configuration files (see Chapter 3), registry keys (see Chapter 5), or the application log related to S3Agent: "Event Logs | Applications and Services | S3Log."

2.4 Automatic start of the HMI

To check that the service starts automatically, press "Windows + R" to open the Run dialog, and enter the command: services.msc



In the list of services, check that the "Hogo S3Agent Service" entry exists and is set to Automatic startup.

To check that the graphical user interface starts automatically, press "Windows + R" to open the Run dialog, and enter the command: shell:startup.

Create a new shortcut in the folder that opens, pointing to:

« C:\Program Files (x86)\Hogo\S3Agent\ Hogo.Secure.Key.Wpf.exe »

3 Local configuration files

3.1 Files storage

All configuration files must be stored in the following folder: `C:\ProgramData\Hogo\S3Agent`

3.2 USB media whitelist

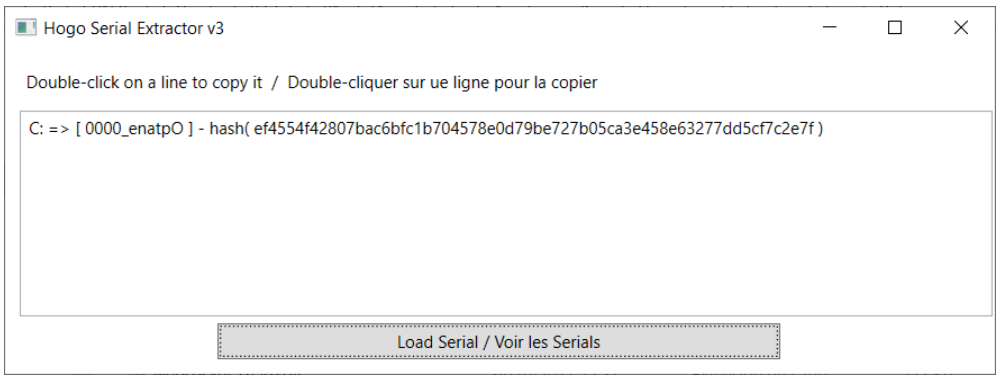
The S3Agent can consider certain media as explicitly authorized (without requiring a tag); these are known as "whitelisted devices." The serial numbers of these devices must be stored—hashed—in the file: `whiteUSB.list`

In cases where external hard drives are permanently connected to a workstation, the S3Agent can also be configured to treat them as "internal devices," meaning they will be allowed by default without filtering.

In this case, their serial numbers must be listed in: `hogo.init.conf`

The S3SRV can be used by the S3Agent to retrieve the list of authorized USB media (as described in the first case above).
In this scenario, the registry keys must request this synchronization (see below), and the address or IP of the local S3SRV must be specified in the file: `s3srv.addr`

To retrieve the serial numbers of hard drives, use the Hogo tool "Serial Extractor", which lists the serial numbers (for `hogo.init.conf`) and their hashed versions (for `whiteUSB.list`) of connected drives and media:



3.3 Automatic retag function

The S3Agent can periodically and automatically retag USB devices that are connected to the workstation and have been accepted.

To enable this, write the compiled value "True" (using the Hogo utility — see Chapter 4) into the file: `hogo.retag.conf`, and define the retag interval, in seconds, in the Windows registry (see Chapter 5).

3.4 Link with the S3Filter device

3.4.1 Periodic Polling of the S3Filter

The S3Agent can periodically ping the IP address 10.34.58.37 to display notifications such as: "S3Filter connected", "S3Filter started", "USB key connected to S3Filter", etc.

To enable this feature, write the compiled value "true" (using the Hogo utility – see Chapter 4) into the file:

`"hogo.s3filter.conf"`.

3.4.2 Automatic Opening of USB Keys Connected via S3Filter

The S3Agent can automatically open Windows Explorer in the folder corresponding to the last USB key plugged into the S3Filter, upon detecting the event "USB key connected to S3Filter".

To enable this feature, write the compiled value "true" (using the Hogo utility – see Chapter 4) into the file:

`"hogo.openS3Fusb.conf"`.

3.5 Filtering of Specific Devices

Specific devices refer to encrypted devices (BitLocker, Veracrypt / TrueCrypt) and media-type devices (e.g., smartphones).

For each type of device, it is possible to define a policy to be applied by the agent, by writing a specific value into a configuration file. The available values and the corresponding configuration files for each device type are described below.

3.5.1 Possible Values

Three values can be used to define the filtering policy for specific devices:

- ignore: ignore the device — allow the OS to handle mounting, and do not filter it
- filter: check for the presence of a tag; block only if it is missing or invalid, otherwise allow
- block: block the device systematically, regardless of tag presence

3.5.2 Filtering BitLocker Devices

The filtering policy for BitLocker devices is configured by writing the desired value into the file:

`“hogo.bitlocker.conf”`

3.5.3 Filtering TrueCrypt Devices

The filtering policy for TrueCrypt/Veracrypt devices is configured by writing the desired value into the file[1]:

`"hogo.veracrypt.conf"`

3.5.4 Filtering Smartphones / Media Devices

The filtering policy for media-type devices (e.g., smartphones) is configured by writing the desired value into the file:

`"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 Specific Certificate for S3Agent

The S3Agent can use a custom salting certificate specific to your organization, in order to identify tags created by your own S3 stations and distinguish them from tags generated by other white-label stations sold by Hogo.

This certificate consists of numbers, lowercase letters, and uppercase letters, and is separated by hyphens ("-").

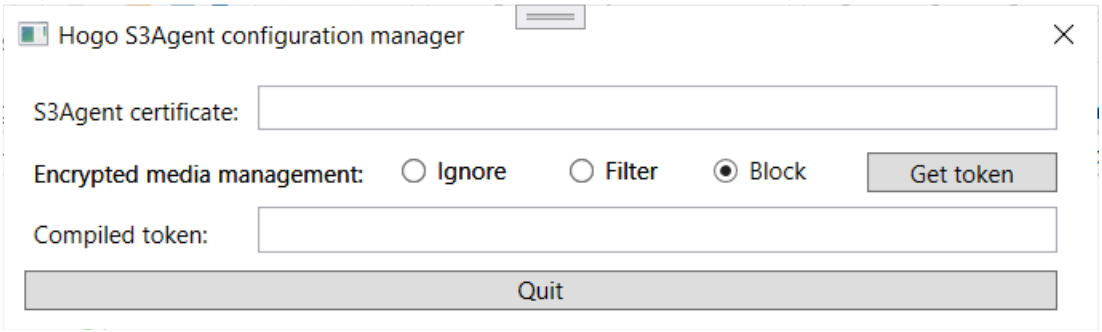
4.1 Certificate Storage

To store a certificate specific to your organization, save its content in the file: `"hogo.certif.conf"`

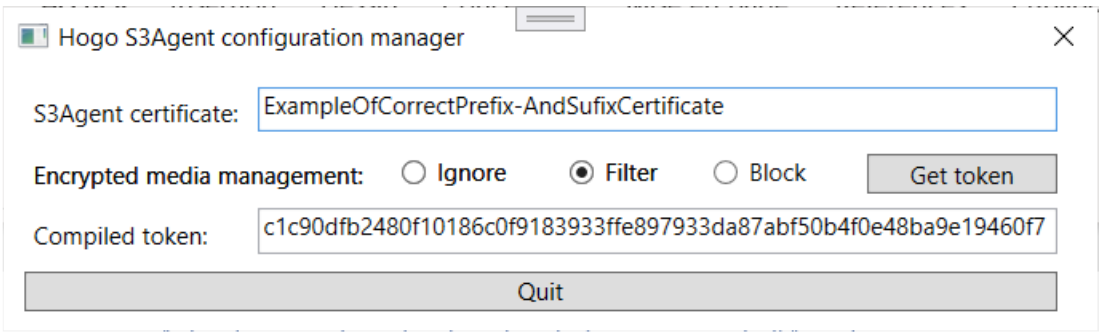
4.2 Encoded Configuration Values

It is possible to generate the configuration values described in the previous chapter using the "Hogo.Config.Manager" utility.

If you are using a custom certificate provided by Hogo, it must be copied into the "S3Agent certificate" field, and the corresponding option must be checked before clicking "Get Token":



The generated token allows fine-tuning of the agent's behavior, depending on which ".conf" file it is saved into.



5 Registry keys

The registry keys used by the S3Agent are located in: `\LOCAL_MACHINE\SOFTWARE\Hogo`

The following keys are available:

- `s3agentvers`: contains the S3Agent version number (do not modify)
- `s3agentpass`: contains a salted and hashed version of the S3Agent GUI password
- `s3agentmenu`: boolean value to enable or disable the display of the "S3Eject" context menu on disk drives
- `s3agents3eject`: boolean value to enable or disable the "S3Eject" button in the S3Agent application window
- `s3agentretag`: numeric value defining the interval (in seconds) between two automatic retag operations
- `s3srvcommunicate`: boolean value to enable communication with a local S3SRV (default: false)