HarfangLab

HARFANGLAB EDR
HURUKAI AGENT
SECURE USER GUIDANCE

Ref : Secure User Guidance
Date : 24th of November 2025
Version : 1.2

SUMMARY

DOCUMENT REVISION

Version	Date	Author	Comment
1.0	15.10.2025	Jürgen Bauer	Initial Document
1.1	22.10.2025	Jürgen Bauer	Update to latest Release
1.2	24.11.2025	Anouck Teiller	Incorporate changes from ETR

INTRODUCTION

PURPOSE OF THE DOCUMENT

The Secure User Guidance document describes the secure handling of the HarfangLab EDR Agent and provides guidance to install it.

INTENDED AUDIENCE

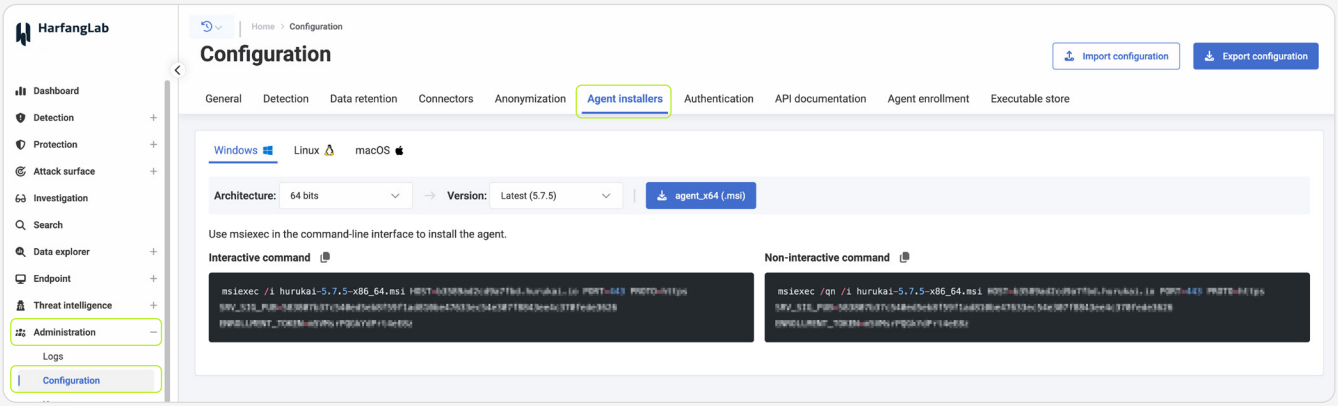
This document is intended for administrators of the HarfangLab EDR solution. It is important to note that HarfangLab EDR is a security software with advanced functionalities and should only be installed by a trained operator.

SECURE INSTALLATION

INSTALLATION PROCEDURE

Installation package

The agent installation package can be downloaded from **Administration > Configuration > Agent Installers:**



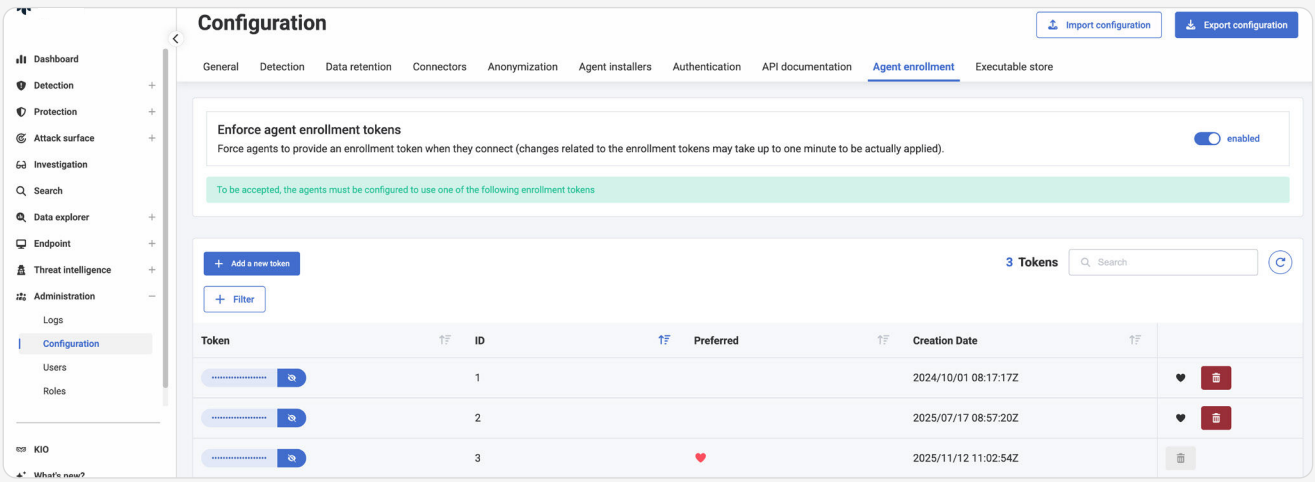
The operator chooses the software type he wants to install by clicking on the package corresponding to the operating system and architecture (32/64 bits).

Agent enrollment tokens

It is possible to restrict the connection to the manager to authorized agents only. To do so, you can define shared secrets between the manager and the agent, called agent enrollment token.

In the Administration > Configuration > Agent enrollment section, it is possible to define one (or many) tokens, and to enforce (or ignore) tokens validation. In case enrollment tokens are enforced, agents must be configured with one of the tokens. Otherwise, they will not be able to connect to the manager.

It is possible to define one «preferred token». The already authorized agents will configure themselves to use this preferred token replacing any existing token every time they are upgraded to a newer version.



Windows installation

The Windows installation package is a signed MSI (Microsoft System Installer) file.

Note:
It is recommended to check the package signature before using the installer to confirm the package authenticity. With a right-click on the installer, open the software properties. The software must be signed by HarfangLab.

Configuration settings

The installation parameters are the following:

Parameter	Description	Mandatory
HOST	IP address or hostname of the EDR Manager	Yes
PORT	TCP port of the manager according to the network configuration (default: 443)	Yes
PROTO	Protocol to use (either HTTP or HTTPS)	Yes
SRV_SIG_PUB	Pairing key of the agent with its manager	Yes
ENROLLMENT_TOKEN	Secret shared between agent and its manager to authorize its registration	No
INSTALL_ROOT	Install directory (it must be in the C: drive, and its value must be quoted. Default is «C:\Program Files\HarfangLab»)	No
PROXY_HOST	IP address or hostname of the proxy (see the Proxy support section)	No
PROXY_PORT	Proxy port of the proxy	No
PROXY_PROTO	Proxy protocol (http or https)	No
ADDITIONAL_INFO1	Further information about the agent useful for policy automation	No
ADDITIONAL_INFO2	Further information about the agent useful for policy automation	No
ADDITIONAL_INFO3	Further information about the agent useful for policy automation	No
ADDITIONAL_INFO4	Further information about the agent useful for policy automation	No
VDI_MODE	Agent ID generation method for VDI mode	No
VDI_SALT	Salt used for agent ID generation in VDI mode	No

After installation, these parameters are stored in the agent configuration file, `agent.ini` stored in the program directory (defaults to `C:\Program Files\HarfangLab\agent.ini` for Windows).

Once installation parameters are defined, there are several ways to install the EDR agents:

- Manual non-interactive installation
- Manual interactive installation
- Deployment with SCCM, GPO or Intune

System specification

Hardware architecture:

The Hurukai EDR agent is compatible with x86 and X64 processor architecture. There are no further hardware requirements for the agent to function.

Hardware requirements:

The Hurukai EDR agent minimum hardware requirements are 2 CPUs, 2 GB RAM, 1 GB disk storage. The agent is sending alert information and telemetry data to the manager. The bandwidth consumption per agent is about 250 bytes/second.

Non-interactive installation

To perform the non-interactive installation:

- Browse to **Administration > Configuration > Agent Installers**
- Click on the Windows tab
- Select an architecture
- Select a version
- Download the agent installer
- Copy the proposed non-interactive command
- On the endpoint, run cmd.exe as an administrator
- Paste the non-interactive command in the terminal and press ENTER

The installation does not require restarting the computer.

Interactive installation

To perform the interactive installation:

- Browse to **Administration > Configuration > Agent Installers**
- Click on the Windows tab
- Select an architecture
- Select a version
- Download the agent installer
- Copy the proposed interactive command
- On the endpoint, run cmd.exe as an administrator
- Paste the interactive command in the terminal and press ENTER
- The «interactive» installation means that this opens the graphical installer dialog. You'll need to click Next and review the settings before installing. The graphical installer performs these steps:
    - Selection of the installation directory (by default, the agent is installed in the `C:\Program Files\HarfangLab` directory
    - Finish setup (once the installation is finished, the EDR agent service is started and paired with the EDR Manager)

Deployment via GPO

Please refer to the product documentation for Enterprise deployment methods via GPO: On the Manager UI go to **Help > Documentation > Installation > Agent Installation > GPO Deployment.**

SECURE CONFIGURATION AND SECURE OPERATION

To ensure the integrity and resilience of the EDR agent against malicious interference, this section outlines essential configuration measures.

AGENT SELF-PROTECTION

Agent Self-Protection safeguards the agent's processes and files from unauthorized access or tampering.

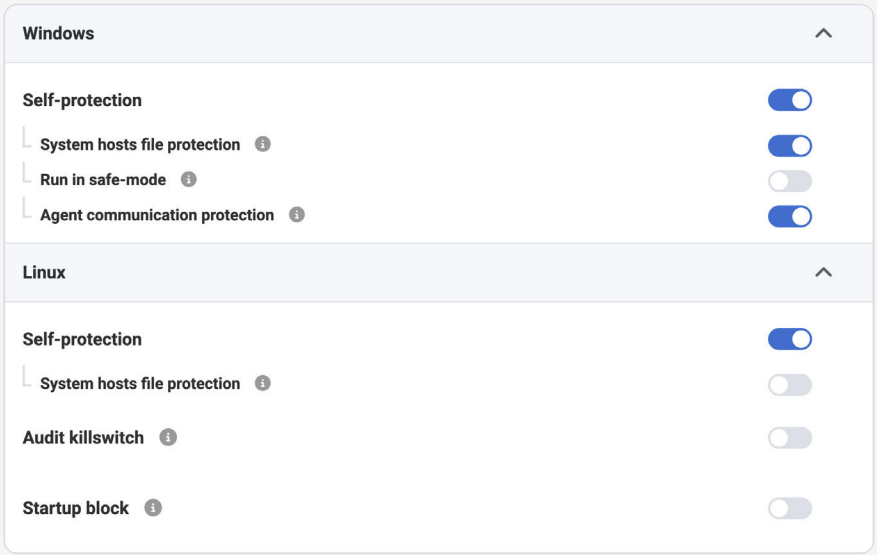
Self-protection is a built-in hardening feature of the HarfangLab agent (hurukai.exe) that helps keep the agent itself safe from tampering, removal or interference by attackers or mis-behaving software.

When enabled, the agent:

- Restricts actions that could modify or stop it (e.g., stopping the service, deleting files, changing registry keys).
- Uses privileged system mechanisms to stay alive even when the host is under attack.
- Guarantees that the security telemetry it collects remains trustworthy.

Because it is a strong safeguard, disabling it should only be done in very specific situations (e.g., the agent is stuck, cannot communicate with the manager, or you need to perform troubleshooting).

It is recommended to enable **Self-protection.** This can be done individually per Policy under **Endpoint > Policies.**



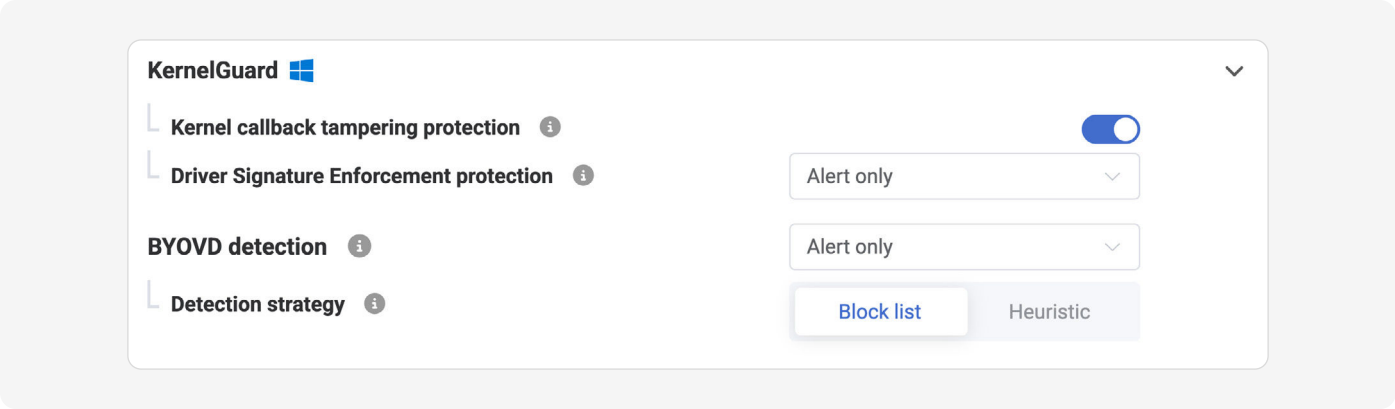
KERNELGUARD

The KernelGuard detection engine includes all kernel-related detection modules:

- Kernel callback tampering protection: Protects against attackers trying to disrupt interactions between HarfangLab's agent and the kernel.
- Driver Signature Enforcement protection: Protects against attackers temporarily disabling DSE to surreptitiously load malicious drivers.
- BYOVD detection (Bring Your Own Vulnerable Driver, previously known as Driver block list): Detects or blocks the loading of known vulnerable drivers.

It is recommended to enable **Kernel callback tampering protection** and set the DSE and BYOVD engines to **Alert** or **Alert & block.**

This can be done individually per Policy under **Endpoint > Policies.**



SECURE OPERATIONS

UPDATE MECHANISM

Deployed agents can be upgraded to newer versions in different ways.

Self-upgrade

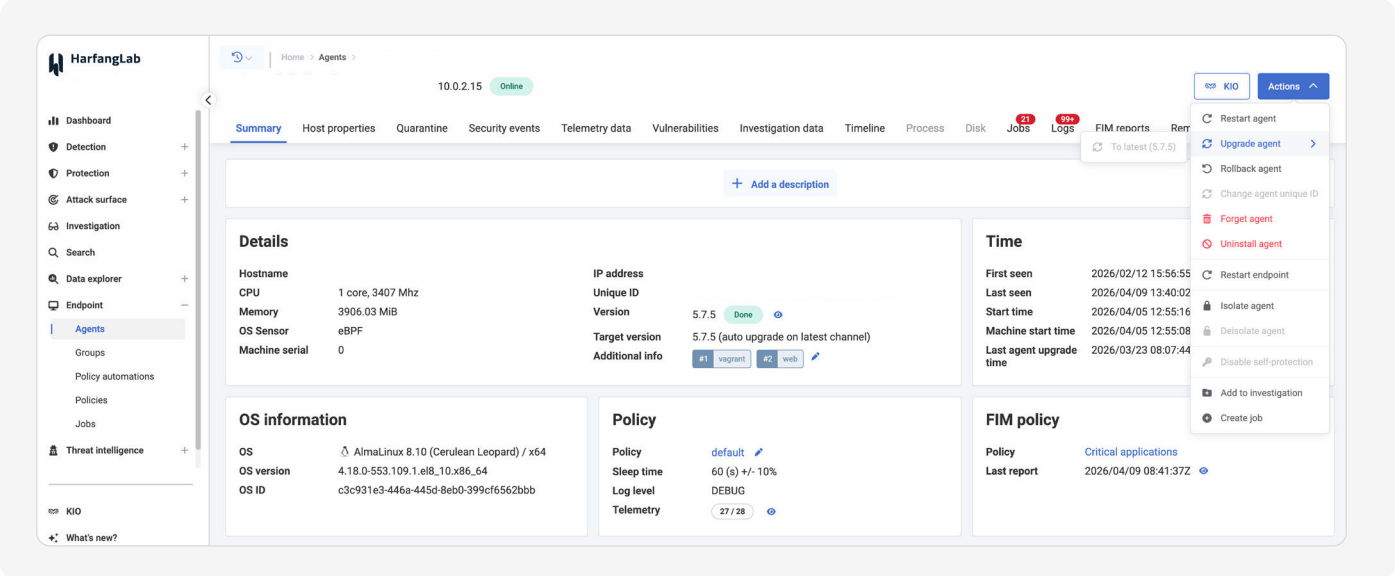
The agents can upgrade automatically.

To do so, enable the **Manage agents auto-upgrades via policy** setting in the manager (in **Administration > Configuration > General**) and set the **Upgrade strategy** to **Automatically upgrade agents** under **Endpoint > Policies**. You can enable this setting in the policies itself.

The manager will send the upgrade file automatically to any agent that is detected as «not up-to-date», and the agents will install this file themselves.

Even if the self-upgrade setting is disabled, it is possible to force the upgrade for a specific agent from the manager.

Go to an agent page. In case an upgrade is available, you can click the **Upgrade agent** button to upgrade it to the latest version.



Note: The self-protection feature does not interfere with the self-upgrade.

Manual upgrade

Similar to the manual installation (either non-interactive or interactive), it is possible to manually upgrade an agent using its MSI package.

To perform the upgrade:
Browse to **Administration > Configuration > Agent Installers** to download the newer installation package.

- On the endpoint, run cmd.exe as an administrator and browse to the folder where you downloaded the installer.
- Execute either
  `msiexec /qn /i <upgrade_file.msi>` for a non-interactive upgrade
  `msiexec /n /i <upgrade_file.msi>` for an interactive upgrade

The installation does not require restarting the computer.

Warning: Upgrading an agent is not possible (and will fail) in case self-protection is enabled in its security policy. In case you want to manually upgrade an agent, you must first disable it.

Upgrade using a GPO

The GPO created to deploy an agent also supports upgrading agents. Simply change the MSI file to either deploy it or upgrade already installed agents to this newer version.

Warning: Upgrading an agent is not possible (and will fail) in case self-protection is enabled in its security policy. In case you want to use a GPO to upgrade agents, make sure self-protection is disabled.

SECURE DECOMMISSIONING

AGENT UNINSTALLATION

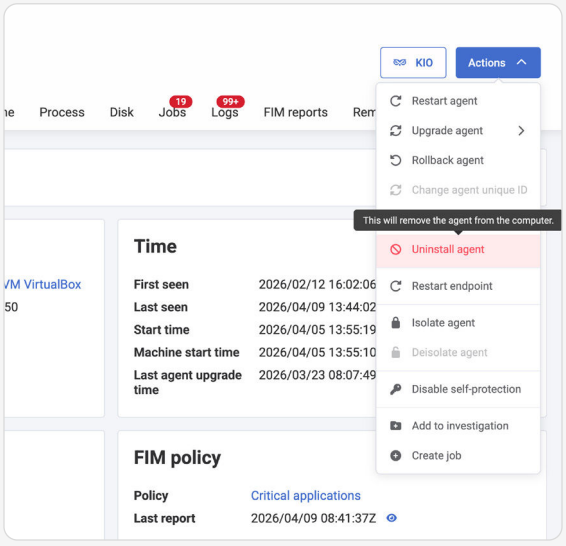
There are several methods to uninstall an agent from the EDR:

- On the manager, it is possible to:
  - uninstall a single agent
  - uninstall a group of agents
- On the endpoint, depending on the OS:
  - on Windows, the agent can be removed using the Control Panel (or Settings app)
  - on Linux, the agent can be removed using the package manager
  - on macOS, the agent can be removed by graphically moving the `/Applications/HarfangLab Hurukai.app` application bundle to the trash through Finder and confirming the system extension deactivation
  - on all OSes, the agent can be removed using `hurukai –uninstall`

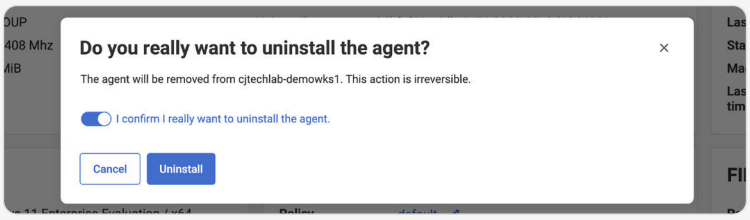
UNINSTALLING FROM THE MANAGER

Single uninstallation

From the detailed view of an agent in **Endpoints > Agents**, you can click on **Actions** and then **Uninstall Agent.**



A pop-up appears to confirm the uninstallation of the agent.

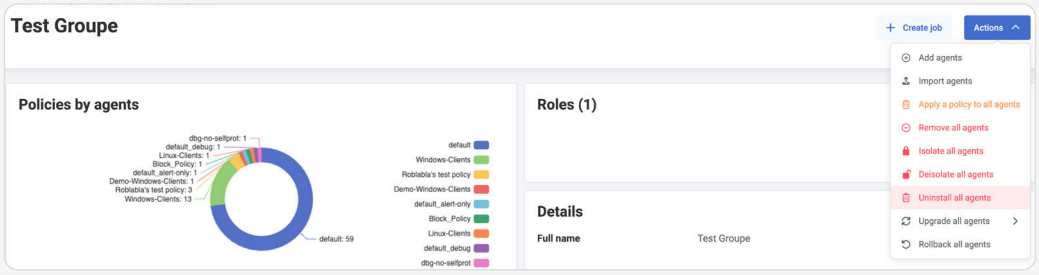


The uninstallation becomes effective by clicking on uninstall.

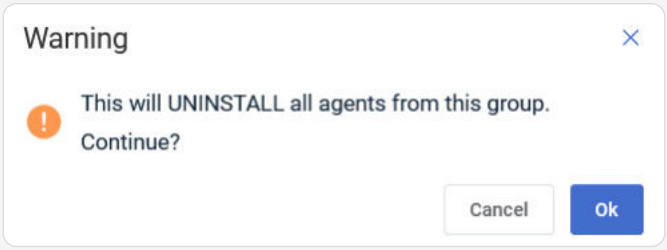
Uninstall a group of agents

The manager offers the possibility to uninstall a group of agents in one action.

From the group view in **Endpoints > Groups > My_group**, you need to click on Actions then Uninstall all agents.



The uninstallation becomes effective by clicking on OK on the confirmation pop-up that appears.

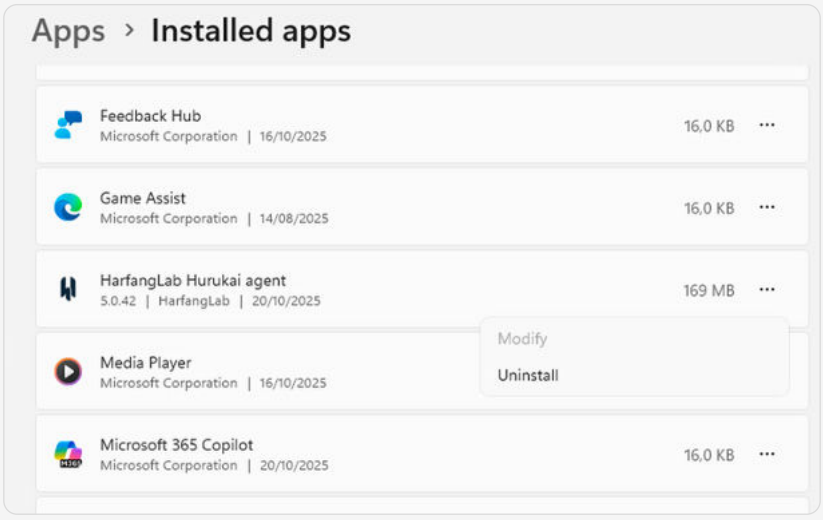


UNINSTALLING FROM THE ENDPOINT

Uninstalling an agent directly on an endpoint has the same effects as if it was done from the manager.

Graphic uninstallation

The uninstallation can be done from the Windows control panel by adding/removing programs in the same way as managing all programs.



Warning: This method does not work if the agent's self-protection is enabled.

Command line uninstallation

The uninstallation can be done from a terminal (e.g., cmd.exe running in administrator mode) as long as the Self-Protection feature is not active for the agent.

On Windows open `cmd.exe` as Administrator and use «`C:\\Program Files\\HarfangLab\\hurukai.exe`» `--uninstall`.
Using this command from the agent's installation directory will fail to delete the directory itself.

OPERATIONAL ENVIRONMENT REQUIREMENTS

For the EDR Agent to fulfill its security properties as defined within the scope of the BSZ certification, the following requirements must be met fulfilled on the Windows operational environment:

- **User:** A separation of «user» and «administrator» roles on the Windows operating system has been implemented using the standard Windows user and administrator roles.
- **Authentication:** Robust user and administrator authentication is set up using local and directory-based authentication in Windows.
- **Access Control:** File access control is implemented and thus limits access and modification rights to operating system files and installed programs using the standard Windows File ACLs.
- **Patching:** Security updates, meaning Windows updates, are enabled on the systems and all security updates of the operating system as well as the installed applications are deployed on the machine. No known vulnerabilities are affecting the operating system or the installed applications.
- **OS Security:** The default Windows operating system configuration is deployed. No hardening or configuration change that affects the operation system security should be put in place.

PRODUCT SECURITY INFORMATION

PRODUCT SECURITY

As a cybersecurity vendor, the security of our customers and partners is our primary priority. That's why we design and develop solutions of the highest possible quality and reliability. Despite all our efforts to implement the best possible security measures, it is possible for vulnerabilities to appear in our solutions or for us to be affected by a security incident ourselves.

Everyone is therefore encouraged to report any vulnerability identified in one of our solutions. Researchers, partners, customers and any other interested parties are welcome to report vulnerabilities or security incidents.

Reporting a vulnerability or security incident

To contact our team responsible for the security of our solutions and our company, you can write to **security@harfanglab.fr**.

If you have identified a potential security vulnerability with one of our solutions, please send us the following information:

- Time and date of discovery
- Version of the solution
- All the data needed to reproduce the vulnerability.
- Technical description of the vulnerability: give as many technical details as possible about the conditions under which it occurred and the impact identified.
- Solution configuration – details of the configuration of the solution and the underlying devices on which it was identified.
- Code used to exploit the vulnerability if possible.
- Tenderer's contact details so that we can reach you.

These elements should be transmitted in English or French and should not include any personal data, apart from the information needed to contact you.

Sharing a potential vulnerability does not give you any intellectual property rights belonging to HarfangLab or to a third party.

Our commitment to handling security reports

After receiving your vulnerability or incident report, our team will contact you to follow up your report. For reasons of confidentiality and security, we encourage you to encrypt any sensitive information you send us by email. To do this, you can use our public PGP key.

We will endeavor to acknowledge receipt of all reports submitted within seven days and will then engage in an open dialogue to discuss the issues identified and to inform you of the outcome of your report.

We are free to decide whether or not to accept a report as relevant. For example, we will not consider vulnerabilities in third-party components, vulnerabilities in obsolete versions of our solutions or automated scans whose exploitability has not been verified manually.

Our requirements for identified vulnerabilities and security incidents

We formally exclude all identified vulnerabilities from the scope of reporting:

By performing social engineering, spamming or phishing on HarfangLab employees, customers or third parties.

- By testing the physical security of HarfangLab assets or those of third parties.
- Carrying out denial of service attacks.
- Directly or indirectly harming HarfangLab, its employees, customers or third parties.

We thank you for your contribution to strengthening the security of our solutions and for working to secure our digital space as a whole by disclosing identified vulnerabilities in a responsible manner.

PGP Key:

Key information:

```
ub   rsa4096 2024-04-30 [SC] [expire : 2030-04-29]
      625E17D4BE9FE16769ED4DDBD7AC721AE22392EB
uid          [  ultime ] HarfangLab <security@harfanglab.fr>
sig 3        D7AC721AE22392EB 2024-04-30  HarfangLab <security@harfanglab.fr>
sub   rsa4096 2024-04-30 [E] [expire : 2030-04-29]
sig          D7AC721AE22392EB 2024-04-30  HarfangLab <security@harfanglab.fr>
```

PGP Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGYxHHkBEAC0VJ5jivBJ10nwC1HIua3e6pbUI8Kz9f9KImPh2A9c30O3qB35
7lQDSc8IRsNm0zJH3JhUrKZp2OLqS+hIjuXRvbXGmRliHQodXfdEWwNJC15VxxiS
YuiUQjkfd9HM4etguCICKV5uLk7mhYm86jeOnxNfGY4nGHGR18ghYd2Hmf2Mm4Zg
uTfjfultAxpycGHzC7JvCVvcvVxM62H93f8CKVGQj1edMGLPNkzoObUB0YAWFWFm
N5MCdMj3Y24bgp5AYq2dNqDTBFBemMQGwX2ZOknz8+VKqws+Lk2f41ADBdgf5eE
QJEn/U0LMJ7WtHJEUZCbaWX9OpmdssgBC0ByvEpKqp/C2tbOapY9BATnm6jngaCq
8DbSPfIETZFghdU1RA99iKZ2Bv76LVlcBGRk2ScqlPA+ja4MkjfFJagtHqKSJcPJ
GqJ8IeEczJrUy3c+6UJrh2VSywSs+QxWIkCxmsDKle9jMY82gJZ8pK0FFkvg/HBD
pweYT598HcM+ki1i/IhU9jhEQ0QdlNZvuYvpfdvqBDNTEdeER7Qexryyc0VzHTsu
XfrEcCrAzHvSW7fcMpm4TI9R768F0nG2PXEJ+AjAcfmdw1vhpijb5EZhs6dnUUKY
A39NyuRQRj5kUH1U8KdS+RMQDU68ttIqnR9sY6N4XnEeqG2xQPJN47RB0QARAQAB
tCNIYXJmYW5nTGFiIDxzZWN1cml0eUBoYXJmYW5nbGFiLmZyPokCVAQTAQoAPhYh
BGJeF9S+n+Fnae1N29eschriI5LrBQJmMRx5AhsDBQkLRzUABQsJCAcCBhUKCQgL
AgQWAgMBAh4BAheAAAoJENeschriI5Lr3WcP/1yHoa8rjIKVZmaDF/+II5rc+mDE
+jF5FxXSiQf0q/2JmbSRxjviCoUWP1U/9I+R6+t6hE230A4KzRf5yW2jXMCPnoxQ
2o/OfUJcMOtXBBWpxKxzrmYLJyjcFPOJ/55j3O07W7u1ToitqWUjpUmK5H5UTRH1
5kl9zkydHHIZHPyHWXNYKzxNguXQYEQzB+4x3ViyrXgJyu6NEBLNrTZR3voFR8wa
Hor4xATsNqDep7KX8Y5vYLk5NV3hC/QBqrvhLA+gcrchIe8hs3tXCXOg+Rctmqyf
Hu5iHr13CavsvIEEaQN9/z5pxbnMJrg4BA6bAzfNSyC9eikzyaF87y6sc8W52e4v
OEoC0tYQMqZLz2YIFxw6b39+CXV4UBB5bnBT6j3M5lIG13cI1LhRL5NfHaSN2dz5
cVs1M1b+xkqWykYQdOxcKbyeaPku9Hl+c4KMkFzrVj/tsplscVyrE/SyghiGyGga
u2gXbjZ+CRo3RQCZlFHRCKxs64rGx9YickuVk3qmxidXlOCn73IeRSQIoPkH9eut
ocBCzzuY26FHTDxFp/y6vDDNG4Ux5NPUaHLmmToqYX04w+VDlxdGvqZECyjVFw3D
j7s+17dbM71e/HPwFfBuXQFIfsDdlZnWudEmv+EJkMYV/cNPCzsBaBbdlW9jBNe4
Bd/NIwUMMwnjw95PuQINBGYxHHkBEAC87wloKfbznJHNZKsrkxkS96/h/y9FQNtQ
LgQoTxV3ETuVc4YG8OqPdAXMQaY9AIElaw3i5zqYyW8oHcEsTG2By7mOPEticI/s
ENzPPsCpWm49k2VaXB8jq2+P0aZtzEHd5y0XsyLnxl3jfydWhYOKH504dwoa63ZX
NCQgtfZKsWCg2JMue83om5mbG4oTpVU8D4+Pt/RevAPPaG2bzxec2Oy8PLQlmAmC
BY1IOGwoXvsqIL7Kqqhw3IgFzHRX5LYkCBLVF8WJB4vUS41gXQP7WYAbCPd6/Db8
lBcSMrJisruf8xko7//WHtLGW+iw+uyF77M4z2JlWoMfX8IXtMrz1OeUFRZ8P+4B
/FfXOSvNs2O1lHDlYLPi7SeqRuSowx2FIJR/w0FZldx1FYLC03fNTk4ZFWpHdGF6
vKAF8CmKly1Fj4Al8D8HwPGT4DPGFT7OIQ7BQ29JVREql0QaArx7QaJnmO6m/OtH
uMTay7VUa00UrqCZB9TA9ioN+vUrhqvMpIyKsMfON7hZPD3BvhkIMcrntSrpDD72
VVegcumrbgTEz25FyopQz48123kPjO0ejuPAeGcw5BMW7zIgChM7A0q4Rmw+08I+
UNkmaC9HDNdaY88yKNLuPhsGkUcyGIoLsp9rlQZDIXypU6B3jJu/X83Hliz7xJOU
TEoJPpxjkwARAQABiQI8BBgBCgAmFiEEYl4X1L6f4Wdp7U3b16xyGuIjkusFAmYx
HHkCGwwFCQtHNQAACgkQ16xyGuIjkuvZ8Q//RIofFIHXZWJda9+0ee/r34RQXWvd
MSFNni7DP3QDx/y14wZy1lgdUGgoxCF0oknZRCXRtf8fPobNlmL3O2+gBvLEmjSc
fXeUzYLg43IyPdkj+AbBuXc8MBHzyB0xD501sMDtH1jbeZJiFcbk1HbY2RfYjpqK
GIMVvn2xgn5Yut+kRZn/KjNL42kW8zcJhyR2oYInJ60lD6Nxf38nYNN2uis5/nJB
JpLp7piYhTGq+wJ+rqstWSPPt/OipUVymgJAUpeFzxpg0QIBVqUwd2hjPy1WjW5y
GSqhEYlHHxlvFabVr/KQuprUWIhlAE/YObE186KH8Ixpca5Vu8dsc3Pq6AHJWqcR
ggl8sQuYZivEzggsJCzp2eVBOxnY38ZNlOSs9gud7n+p0rQZ5Ui0CuzcXkMFvwy8
AeCixFh1F8fBxHbgSBjHYThdlhvs9tbFuV8Z995fNV95wV7xZn+I/8lS4uCyllrv
wh1erLxS2ftPTzeZ8mjLvLy735mKrXS9EL8fiDdnAOZEDdgA4/kUZmnHkB2wvcV7
5qats6Lv7RWaUKXO9ic2/iX72Dy5iTMFVdn7ZvYVWJ5xPkYc1S/n5DUPpHCBtbsY
oApFUrL2MSTfnBkDeWSX7YWkrfz/7vk2RF1M2+Tp6uCB6ih6nOVPLNCzpFqmajul
IW4FuYehG8fjdpE=
=AzPy
-----END PGP PUBLIC KEY BLOCK-----
```

harfanglab.io

HarfangLab