Release note
GCap V2.5.5.0

Manual version: v1

Translated from original manual version: v1

Creation date: January 2026

Update date: January 2026

Table of contents

Chapter 1

Presentation of GCap version 2.5.5.0

This release note describes:

- New features
- Improvements and other characteristics
- The patches
- The known issues
- The software compatibility
- The hardware compatibility
- The update procedure

Chapter 2

The new features

2.1 Sigflow detection engine

2.1.1 Engine update

The Sigflow engine was updated.
This update contains new features and fixes for previously published critical vulnerabilities.

2.1.2 Multi-tenant management

The multi-tenant functionality has been improved.
When a new ruleset is applied, the detection assembler reloads the rules without restarting.

2.1.3 Support for new OT protocols

Support for the following protocols has been added:

- S7COMM
- OPCUA
- CCSDS
- DICOM
- HL7
- BACnet

2.1.4 ERSPAN support for flow capture

It is now possible to use ERSPAN to create a GRE tunnel between a GCap monitoring interface and a switch interface in order to send the flows to be inspected.

It is possible to filter the events of the SMB protocol according to the operations performed through it.

2.1.5 Shellcode-Detect / Powershell-Detect: addition of community ID

The community ID has been added to events generated by the Shellcode-Detect and Powershell-Detect engines.

2.2 Virtualization of the probe

2.2.1 AWS Support

AWS support has been improved.

2.3 System

2.3.1 System update

The system has been updated.

2.3.2 Log management

Some temporary logs are now retained after the probe restarts, to facilitate diagnosis in the event of problems.

2.3.3 Command line interface

Autocompletion is now available for network interface names.

2.4 Installation

2.4.1 Storage prerequisites

It is possible to install a GCap probe on a 100 GB partition.

2.4.2 UEFI support

UEFI support has been improved.

2.5 Update process

The update process with rollback capability has been improved.

Chapter 3

Other features and improvements

Section left empty intentionally

Chapter 4

Patches

4.1 After the update, error in executing commands with certain hardware versions

Some commands are non-functional for certain hardware versions following an update to 2.5.4.0.
This issue is fixed in v2.5.5.0.

4.2 Sigflow: error when starting the detection engine

On some GCap models, the detection engine does not start if more than two capture interfaces are enabled.
This issue is fixed in v2.5.5.0.

4.3 Sigflow: XDP filters are not applying correctly

In some cases, the XDP filters do not apply correctly.
This issue is fixed in v2.5.5.0.

4.4 Sigflow: receiving specific packets from the Modbus protocol may cause a restart of the engine

When activating the Modbus protocol, receiving a specific packet can cause the engine to restart
This issue is fixed in v2.5.5.0.

4.5 Netdata: absence of certain metrics

Some metrics are no longer retrieved by Netdata in version 2.5.4.0.
This issue is fixed in v2.5.5.0.

4.6 Sigflow: problem starting the detection engine

In some cases, the Sigflow detection engine does not start correctly when the system is initialized.
This issue is fixed in v2.5.5.0.

4.7 Netdata: erroneous value

In some cases, Netdata returns an erroneous value for the status of the detection engine.
This issue is fixed in v2.5.5.0.

4.8 System: Inadequate performance settings

Some system settings are not optimized for performance.
This issue is fixed in v2.5.5.0.

4.9 System: unable to install

In some cases, it is not possible to install GCap.
This issue is fixed in v2.5.5.0.

4.10 Sigflow: Problem with cluster interfaces

When using a cluster interface, significant packet loss may occur.
This issue is fixed in v2.5.5.0.

4.11 Sigflow: memory allocation issue for some streams

Memory allocation for some streams is not optimized.
This issue is fixed in v2.5.5.0.

4.12 System: GCap storage space is running out

When analyzing a large amount of streaming streams, the GCap's storage space can become saturated.
This issue is fixed in v2.5.5.0.

4.13 System: CPU distribution

For some GCap models, the CPU distribution is not optimal.
This issue is fixed in v2.5.5.0.

4.14 System: default selection in the boot menu

Following a GCap update, it is possible to inadvertently select the entry that triggers a failback.
This issue is fixed in v2.5.5.0.

4.15 Sigflow: options for debugging

Some options for system debugging are enabled by default.
This issue is fixed in v2.5.5.0.

4.16 Update: problem on restart

A problem may occur when restarting the system after an update.
This issue is fixed in v2.5.5.0.

4.17 Sigflow: Reconstruction problem for the http2 protocol

A problem with rebuilding the HTTP2 protocol may occur in some cases.
This issue is fixed in v2.5.5.0.

Chapter 5

Known problems and limitations

5.1 Sigflow: rebuilding files with FTP protocol

Rebuilding files is not operational with FTP protocol.

5.2 System: password Policy

The *set password-policy previous-check* command does not work.

5.3 System: interface configuration

Switching from a management-tunnel role interface to a management role interface may result in a loss of connection.

Chapter 6

Software compatibility

6.1 Compatibility with the GCenter

GCap version	GCenter version	Compatibility
2.5.5.0	2.5.3.102 HF3	Configuration not supported
2.5.5.0	2.5.3.103 HFx	Configuration ok (recommended)

Chapter 7

Hardware compatibility

The version 2.5.5.0 is compatible with all hardware versions of GCap.

GCap reference	Local storage	PORTS OF CAPTURE	EXTENSION OF CAPTURE PORTS	Power supply
GCAP1010HWr2	256GB	4 x RJ45	N/A	2 x 750W
GCAP1020HWr2	256GB	4 x RJ45	N/A	2 x 750W
GCAP1050HWr2	256GB	4 x RJ45	N/A	2 x 750W
GCAP1100HWr2	2 x 600GB RAID1	1 x SFP	N/A	2 x 750W
GCAP1200HWr2	2 x 600GB RAID1	2 x SFP	N/A	2 x 750W
GCAP1400HWr2	2 x 600GB RAID1	4 x SFP	N/A	2 x 750W
GCAP2200HWr2	4 x 600GB RAID5	4 x SFP	4 x SFP	2 x 750W
GCAP2600HWr2	4 x 600GB RAID5	4 x SFP	4 x SFP	2 x 750W
GCAP2800HWr2	4 x 600GB RAID5	4 x SFP	4 x SFP	2 x 750W
GCAP5400HWr2	8 x 600GB RAID5	4 x SFP+	4 x SFP+	2 x 1100W
GCAP5600HWr2	8 x 600GB RAID5	4 x SFP+	4 x SFP+	2 x 1100W
GCAP5800HWr2	8 x 600GB RAID5	4 x SFP+	4 x SFP+	2 x 1100W

Chapter 8

Updating procedure

8.1 Prerequisites

To deploy the GCap V2.5.5.0 update from the GCenter GUI, the GCenter must be in the installed **V2.5.3.103-HFX** version.
If the GCenter is in a previous version, it will need to be updated.

The GCap must be one of the following versions: **V2.5.4.0**, **V2.5.4.1**, **V2.5.4.2**, **V2.5.4.3**

If you have any questions about these items, please contact the Gatewatcher Technical Support.

Important:

It is mandatory to have an iDRAC connection so that you can connect post-upgrade if a problem occurs during the process. Otherwise, physical access to the equipment (screen, keyboard) will be required.

8.2 Retained data

The following data and configurations are retained:

- pairing with GCenter
- The network configuration
- The SSH key of the root account
- The password of the root account
- The log files
- the pcap files in the /data/cache/pcaps directory

8.3 Installation procedure via the GCenter

On GCenter:

1. From the platform https://update.gatewatcher.com/upgrade/ (directory 2.5.5.0/gcap/), download:

- The gwp file of the new version available
- The associated sha256 gwp.sha256 file

2. Check the image (sha256sum command) and check the value obtained with the contents of the gwp.sha256 file
3. Log on to the GCenter WebUI via a web browser and go to the **Administration-Updates / Software Update** menu.
4. Upload the GCap package.
   - A progress bar is displayed.
   - If you encounter a problem, try another browser.

On GCap:

1. Open a terminal and log into SSH on GCap with the **setup** account.
2. Stop the monitoring-engine with the command **monitoring-engine stop** (GCAP-CLI) and wait for the files to be processed.

Important:

If GCap is under load, please wait before performing upgrade.
Check on the GCenter WebUI in **Hunting > Network Metadata** that there is no more data.
If you have any questions about these items, please contact the Gatewatcher Technical Support.

3. Use the command **system upgrade list** (GCAP-CLI) to get the package list from the GCenter.
4. Use the command **system upgrade apply '[image_name]' confirm** (GCAP-CLI).
   - GCap restarts automatically
   - SSH session is down
5. After GCap has restarted, log in via SSH with the **setup** account to see if the update has been applied correctly.
6. Check the current version with the **show status** command (GCAP-CLI).
7. Start the monitoring-engine with the command **monitoring-engine start** (GCAP-CLI).

In case of problem, please contact Gatewatcher Technical Support.

8.4 Installation procedure directly from the GCap

1. Download the new version and the associated sha256 from the platform https://update.gatewatcher.com/upgrade/ (directory 2.5.5.0/gcap/).
2. Check the image (sha256sum command) and check the value obtained with the contents of the gwp.sha256 file.
3. Copy the image (.gwp) to the /data/ directory of the GCap using a privileged account.
4. Open a terminal and log into SSH on GCap with the **setup** account.
5. Stop the monitoring engine with the **monitoring-engine stop** command (GCAP-CLI).

Important:

If GCap is under load, please wait before performing upgrade.
Check on the GCenter WebUI in **Hunting > Network Metadata** that there is no more data.
If you have any questions about these items, please contact the Gatewatcher Technical Support.

6. Open a terminal and log in via SSH on the GCap with a privileged account.
7. Start the upgrade with the command **gcap-upgrade/data/file_name** (SHELL).
   - GCap restarts automatically
   - SSH session is down
8. After GCap has restarted, log in via SSH with the **setup** account to see if the update has been applied correctly.
9. Check the current version with the **show status** command (GCAP-CLI).
10. Start the monitoring engine with the **monitoring-engine start** command (GCAP-CLI).

In case of problem, please contact Gatewatcher Technical Support.
