

# Release Note GCap 2.5.4.1



Version : 1

Translated from original manual version 1

Creation date: June 2025

Update date: June 2025

@Copyright: Gatewatcher - June 2025

Disclosure or reproduction of this document, and use or disclosure of the contents hereof,  
are prohibited except with prior written consent. Any breach shall giveright to damages.  
All rights reserved, particularly in the case of patent application or other registrations.

# Table of contents

<b>Table of contents</b>	<b>3</b>
<b>1 Presentation of GCap version 2.5.4.1</b>	<b>4</b>
<b>2 New features</b>	<b>5</b>
2.1 Sigflow detection engine . . . . .	5
2.1.1 Engine update . . . . .	5
2.1.2 Event filtering for the SMB protocol . . . . .	5
2.2 Installation . . . . .	5
2.2.1 Storage prerequisites . . . . .	5
2.2.2 UEFI support . . . . .	5
<b>3 Other features and improvements</b>	<b>6</b>
<b>4 Patches</b>	<b>7</b>
4.1 Error during the first restart following an update to v2.5.4.0. . . . .	7
4.2 Blocking of the update in v2.5.4.0. . . . .	7
4.3 After the update, error in executing commands with certain hardware versions . . . . .	7
4.4 Sigflow: error when starting the detection engine . . . . .	7
4.5 Sigflow: XDP filters do not apply correctly . . . . .	7
4.6 Sigflow: receiving specific packets from the Modbus protocol may cause a restart of the engine . . . . .	8
4.7 Netdata: absence of certain metrics . . . . .	8
<b>5 Known problems and limitations</b>	<b>9</b>
5.1 Netdata: Badges for network statistics . . . . .	9
5.2 Sigflow: Rebuilding files with FTP protocol . . . . .	9
<b>6 Software compatibility</b>	<b>10</b>
6.1 Compatibility with GCenter . . . . .	10
<b>7 Hardware compatibility</b>	<b>11</b>
<b>8 Updating procedure</b>	<b>12</b>
8.1 Prerequisites . . . . .	12
8.2 Retained data . . . . .	12
8.3 Data deleted . . . . .	12
8.4 Installation procedure via the GCenter . . . . .	13
8.5 Installation procedure directly from the GCap . . . . .	13

# Chapter 1

## Presentation of GCap version 2.5.4.1

This release note provides a description of:

- new features
  - improvements and other characteristics
  - patches
  - known issues
  - software compatibility
  - hardware compatibility
  - upgrade procedure
-

## Chapter 2

# New features

### 2.1 Sigflow detection engine

#### 2.1.1 Engine update

The Sigflow engine was updated.  
This update includes security fixes for critical vulnerabilities published recently.

---

#### 2.1.2 Event filtering for the SMB protocol

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

---

### 2.2 Installation

#### 2.2.1 Storage prerequisites

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

---

#### 2.2.2 UEFI support

UEFI support has been improved.

---

# Chapter 3

## Other features and improvements

Section intentionally left blank

---

## Chapter 4

# Patches

### 4.1 Error during the first restart following an update to v2.5.4.0.

In some cases, following the update to v2.5.4.0, a problem may occur during the first restart.  
This problem is fixed in v2.5.4.1.

---

### 4.2 Blocking of the update in v2.5.4.0.

If the /boot is full, the GCap update might get stuck.  
This problem is fixed in v2.5.4.1.

---

### 4.3 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 problem is fixed in v2.5.4.1.

---

### 4.4 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 problem is fixed in v2.5.4.1.

---

### 4.5 Sigflow: XDP filters do not apply correctly

In some cases, the XDP filters do not apply correctly.  
This problem is fixed in v2.5.4.1.

---

## 4.6 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 problem is fixed in v2.5.4.1.

---

## 4.7 Netdata: absence of certain metrics

Some metrics are no longer retrieved by Netdata in version 2.5.4.0. This problem is fixed in v2.5.4.1.

---



## Chapter 5

# Known problems and limitations

### 5.1 Netdata: Badges for network statistics

In compatibility mode **2.5.3.102**, Netdata statistics in the following menu **Admin > GCaps Pairing/Status**, are no longer available.

---

### 5.2 Sigflow: Rebuilding files with FTP protocol

Rebuilding files is not operational with FTP protocol.

---

# Chapter 6

## Software compatibility

### 6.1 Compatibility with GCenter

GCap version	GCenter version	Compatibility
2.5.4.1	2.5.3.102 HF3	Configuration ok
2.5.4.1	2.5.3.103 HFx	Configuration ok (recommended)

---

# Chapter 7

## Hardware compatibility

Version 2.5.4.1 is compatible with all hardware versions of GCap.

REFERENCE GCAP	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 V2.5.4.1 update from the GCenter GUI, the GCenter must be in the installed **V2.5.3.102-HF3** version. If the GCenter is in a previous version, it will need to be updated.

The GCap must be in the installed **V2.5.3.106**, **V2.5.3.107** or **V2.5.4.0** version.

For questions about these items, please contact 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 is retained:

- the GCenter pairing
- 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/pcaps/ directory

### 8.3 Data deleted

**Important:**

The following data will be deleted if your GCap is in version V2.5.3.X:

- Local rules for Sigflow (local-rules)
- Local XDP filters

please postpone the configuration of these filters at GCenter level using the **GCap Profiles > Packet filters**) menu

## 8.4 Installation procedure via the GCenter

On GCenter:

1. From the platform <https://update.gatewatcher.com/upgrade/> (directory 2.5.4.1/gcap/), download:
  - the gwp file of the new version available
  - the associated sha256 gwp.sha256 file

**Important:**

Two GCenter versions are available:

- If the GCenter is in V2.5.3.102 and the GCap is in V2.5.3.X, use the following package: [https://update.gatewatcher.com/upgrade/2.5.4.1/gcap/gcap-bios\\_2.2.4.1-gcenter\\_v2.5.3.102.gwp](https://update.gatewatcher.com/upgrade/2.5.4.1/gcap/gcap-bios_2.2.4.1-gcenter_v2.5.3.102.gwp)
- If the GCenter is in V2.5.3.102 and the GCap in version 2.5.4.0, it is necessary to first update the GCenter to V2.5.3.103
- If the GCenter is in V2.5.3.103, use the following package: [https://update.gatewatcher.com/upgrade/2.5.4.1/gcap/gcap-bios\\_2.5.4.1.gwp](https://update.gatewatcher.com/upgrade/2.5.4.1/gcap/gcap-bios_2.5.4.1.gwp)

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)

**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  
For any questions about these items, please contact 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. Once the GCap has restarted twice, log into SSH with the **setup** account to see if the update has been correctly applied
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.

## 8.5 Installation procedure directly from the GCap

1. Download the newly available version and the associated sha256 on the <https://update.gatewatcher.com/upgrade/> platform (directory 2.5.4.0/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 /tmp/ directory of the GCap using a privileged account.
4. Open a terminal and log in via SSH on the 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 the **Hunting > Network Metadata** menu that there is no more data.  
For any questions about these items, please contact 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).
8. Restart the GCap with the **system restart** command (GCAP-CLI)  
SSH session is down
9. Once the GCap has restarted twice, log in to SSH with the **setup** account to verify that the update was successfully applied.
10. Check the current version with the **show status** command (GCAP-CLI).
11. Start the monitoring engine with the **monitoring-engine start** command (GCAP-CLI).

In case of problem, please contact Gatewatcher Technical Support.

PDF documentation