

Release Note

GCenter V2.5.3.103 HF3




Manual version: v1

Translated from original manual version: v1

Creation date: November 2025

Update date: November 2025

© Copyright: November 2025  **GATEWATCHER**

Disclosure or reproduction of this document, and use or disclosure of the contents hereof,
are prohibited except with prior written consent. Any breach shall give right to damages.

All rights reserved, particularly in the case of patent application or other registrations.

Table of contents

Table of contents	3
1 Presentation of GCenter version 2.5.3.103 HF2	5
2 New features and enhancements	6
2.1 Detection engines and features	6
2.1.1 DGA detect engine	6
2.1.2 Malcore Detection Engine	6
2.1.3 Beacon detect engine	6
2.1.4 Ransomware detect engine	6
2.1.5 GScan Detection Engine	6
2.1.6 Auto-threshold feature	6
2.1.7 Multi-tenant feature for network variables	7
2.2 Analysts: WebUI and features	7
2.2.1 Home Page Improvement	7
2.2.2 Improved alerts management	7
2.2.3 Asset and user filtering	7
2.2.4 Malcore menu	7
2.2.5 Powershell and Shellcode detect menu	7
2.2.6 YARA menu	7
2.2.7 Active CTI menu	7
2.2.8 Sigflow manager menu	7
2.2.9 Reporting	7
2.3 Administration: Web UI and features	8
2.3.1 New notification system	8
2.3.2 History of administrative actions	8
2.3.3 Standardization of the event format	8
2.3.4 Improved data export	8
2.3.5 GCap pairing menu	8
2.3.6 Software update menu	8
2.3.7 Threat DB update menu	8
2.3.8 Threat DB update menu	8
2.3.9 Network settings menu	9
2.3.10 Licensing menu	9
2.3.11 Diagnostics menu	9
2.4 WebUI – Kibana Dashboards	9
2.4.1 Enhancements to existing dashboards	9
2.4.2 New Beacon Detect dashboard	9
2.4.3 New Ransomware detect dashboard	9
2.4.4 New Relations dashboard	9
2.4.5 New Administration dashboard	9
2.5 System	9
2.5.1 Operating system update	9
2.5.2 Kernel update	9
2.5.3 Component updates	9
2.5.4 Virtualization	9
2.5.5 ECDSA Certificates	10
2.5.6 GCenter Configuration Tool	10
2.6 Other enhancements	10
2.6.1 Contextual help	10
2.6.2 Reflex Interoperability	10
2.6.3 API improvement	10
2.6.4 PCI-DSS Compliance	10
2.6.5 LDAP authentication	10
2.7 Other changes	10
2.7.1 Renaming `active-hunt` to `active-cti`	10
2.7.2 Removal of interoperability	10
2.7.3 IDMEF format	10

3	Patches	11
4	Known problems and limitations	12
4.1	Active-CTI / RetroHunt - Post Update problem	12
4.2	GCenter Backup/Restore - Error management	12
4.3	GCenter Backup/Restore - Pairing the GCap	12
4.4	Incorrect GCap status after updating the GCenter	12
4.5	Sigflow Manager - Transform Category	12
4.6	Sigflow Manager - Error 500 when adding a rule in a custom source	12
4.7	Sigflow Manager - Inconsistency in displaying the number of categories and rules in a category	12
4.8	Sigflow Configuration - Custom source name cannot contain space	13
4.9	GCenter Backup/Restore - Error in FQDN	13
4.10	Kibana - Error 500 due to changing storage media for ES data	13
4.11	Migration - Problem with online update configuration	13
4.12	Migration - Problem with the detected user base of NDR interface	13
4.13	Migration - Problem with the application of Sigflow rulesets	13
4.14	Network - Problem with interface MTU configuration	13
4.15	Network - VPN connectivity issue between GCap and GCenter	13
4.16	GUM - Problem with the configuration of the address of a local repository	14
4.17	Backup/Restore - Wrong format of the logs of the export in Syslog	14
4.18	Migration - Improper configuration of scheduled backups	14
4.19	ECS - Missing http_refer field	14
4.20	CTI - Active-CTI Alerts Missing in the NDR Interface	14
4.21	CTI - Change of the SID of the Active-CTI rules with each update of Sigflow	14
4.22	Sigflow - Error while updating engine	14
4.23	NDR interface - Loss of filter on IP address in Asset and User views	14
4.24	XDP Filter - Configuration synchronization	15
4.25	WebUI - Access Issue	15
4.26	Malcore - File storage space saturation	15
4.27	Retention - Saturation of the storage space in Elasticsearch	15
4.28	NDR Interface - Problem with muting alerts	15
4.29	Kibana - Beacon Detect dashboard	15
4.30	Update - Issue with UEFI version	15
4.31	NDR - User detection	15
4.32	NDR Interface - Alert Filtering	16
4.33	NDR interface - Solution health	16
4.34	Help - Embedded documentation	16
4.35	NDR Interface - Home Page links	16
4.36	DGA - Addition of a comment	16
5	Software compatibility	17
5.1	Compatibility with the GCap	17
6	Hardware compatibility	18
7	Hotfix	19
7.1	Package 1	19
7.2	Package 2	19
7.3	Package 3	20
8	Procedure for upgrading from V102 to V103	21
8.1	Prerequisites	21
8.2	Retained data	21
8.3	Procedure to install	21

Chapter 1

Presentation of GCenter version 2.5.3.103 HF2

This release note describes:

- New features and enhancements
 - Patches
 - Known issues
 - Software compatibility
 - Hardware compatibility
 - Hotfixes
 - The update procedure
-

Chapter 2

New features and enhancements

2.1 Detection engines and features

2.1.1 DGA detect engine

A new version of our DGA (Domain Generated Algorithm) detection engine is available with:

- Optimization of the algorithm to reduce false positives
 - The ability to manage motor sensitivity with six different levels
 - A system that helps analysts configure the list of domains to be ignored
-

2.1.2 Malcore Detection Engine

A new version of the Malcore engine is available, improving its performance and stability.

2.1.3 Beacon detect engine

A command and control (C&C) infrastructure tag detection engine is now available to detect encrypted communications between an infected host and a C&C server.

A system is present to help analysts in configuring the list of IP addresses to be ignored.

2.1.4 Ransomware detect engine

A ransomware detection engine is now available to detect the activities of this type of malware on the SMB protocol.

It is possible to:

- Manage motor sensitivity with 6 different levels
 - Investigate based on the identifier of an SMB session
 - Add IP addresses to a whitelist
-

2.1.5 GScan Detection Engine

The GScan engine interface has been enhanced to provide more details on the files analyzed on demand.

2.1.6 Auto-threshold feature

A new `auto-threshold` feature is available to limit the number of alerts generated by the Sigflow engine.

This feature is based on threshold rules that will be directly applied to the Sigflow engine.

An analyst will be able to use one of seven existing configuration profiles or configure a custom profile.

2.1.7 Multi-tenant feature for network variables

A new feature to improve support for multi-tenant architectures is available for the Sigflow engine. This feature offers the possibility to declare:

- a variable with a different configuration per tenant
- A customized ``network address`` type variable
- A customized ``network port`` type variable

2.2 Analysts: WebUI and features

2.2.1 Home Page Improvement

The home page has been improved to quickly visualize important information for analysts and administrators.

2.2.2 Improved alerts management

The alert management system has been improved to:

- Acknowledge the alerts
- Make alerts silent
- Sort alerts according to different criteria (risk level, name, date, number of occurrences)
- Manage alerts in bulk

Alerts that have been acknowledged are excluded from the risk level calculation.

2.2.3 Asset and user filtering

In the search bar, it is now possible to filter assets and users according to a risk level (``risk_min`` and ``risk_max``).

2.2.4 Malcore menu

A new interface is available for managing the Malcore engine.

Two options have been added to ignore the alerts based on a file name or those generated by a specific engine.

2.2.5 Powershell and Shellcode detect menu

A new interface is available for managing the Powershell engine and Shellcode detect.

2.2.6 YARA menu

A new interface is available for managing Yara rules.

2.2.7 Active CTI menu

A new interface is available for managing the CTI.

2.2.8 Sigflow manager menu

The ``generate rule file`` button has been replaced by a ``save`` button which is located at the top right of the ``ruleset`` configuration menu in order to save the changes made to the policy applied to the Sigflow engine.

2.2.9 Reporting

It is now possible to generate a predefined report in docx format.

2.3 Administration: Web UI and features

2.3.1 New notification system

A new notification system in the `Health` menu is available to warn users of malfunctions in certain components of the solution.

A notification can be triggered in many situations:

- Engine update problems
- Configuration problems
- Connection problems between the GCap and the GCenter
- Compatibility problems
- Performance problems...

These notifications can be silenced or acknowledged.

2.3.2 History of administrative actions

A new feature has been developed to log user actions.

Events that are generated can be exported to a Syslog server.

2.3.3 Standardization of the event format

A new event format, ECS (Elastic Common Schema), is available for alerts, metadata, and administrative events.

A compatibility mode exists, for data export, allowing to keep the old format which will be removed during the next major version.

2.3.4 Improved data export

The data export feature now allows:

- Filter alerts by engine
 - Export system events
-

2.3.5 GCap pairing menu

A new interface is available for managing the GCap pairing to the GCenter.

A help menu has been added to facilitate configuration.

2.3.6 Software update menu

A new interface is available for managing system updates.

2.3.7 Threat DB update menu

A new interface is available for managing detection engine updates.

Several options have been added:

- Managing the frequency of GCap updates
 - The ability to download multi-part updates
 - The ability to use a local server in HTTPS
-

2.3.8 Threat DB update menu

A new interface is available for managing the retention of data stored in Elastic Search.

It is now possible to manage the space allocated for alerts, metadata and administrative events.

2.3.9 Network settings menu

A new interface is available to view network configuration settings.

2.3.10 Licensing menu

A new interface is available for license management.

2.3.11 Diagnostics menu

A new interface is available for generating system logs and tech support.

2.4 WebUI – Kibana Dashboards

2.4.1 Enhancements to existing dashboards

The existing dashboards have been restructured to have better visibility and facilitate investigation.

2.4.2 New Beacon Detect dashboard

A new dashboard is available to view Beacon Detect engine events.

2.4.3 New Ransomware detect dashboard

A new dashboard is available to view Ransomware detect engine events.

2.4.4 New Relations dashboard

A dashboard for the relationships between the different IP addresses reported in the solution is available in the `Hunting > Network Metadata > Relations` menu.

2.4.5 New Administration dashboard

A new dashboard is present to be able to consult the administration events.

2.5 System

2.5.1 Operating system update

The operating system has been updated to the latest LTS (Long-Term Support) version.

2.5.2 Kernel update

The operating system kernel has been updated to the latest LTS (Long-Term Support) version.

2.5.3 Component updates

The various components of the operating system have been updated.

2.5.4 Virtualization

The GCenter is officially supported on VMware ESXi hypervisors.

2.5.5 ECDSA Certificates

ECDSA certificates are supported for securing access to the GCenter web interface.

2.5.6 GCenter Configuration Tool

The GCenter configuration tool has been enhanced to facilitate the network setup and to add SSH keys to the ``setup`` user.

2.6 Other enhancements

2.6.1 Contextual help

Context-sensitive help is available on the GCenter web interface.

2.6.2 Reflex Interoperability

A new menu is available to interconnect with the Reflex solution.

2.6.3 API improvement

New API points have been added to automate certain actions.

2.6.4 PCI-DSS Compliance

A new option has been added to replace credit card numbers with a specific keyword.

2.6.5 LDAP authentication

When connecting using an LDAP server for authentication, if the account used is present in the GCenter's local database, then it is deactivated to avoid conflicts.

2.7 Other changes

2.7.1 Renaming ``active-hunt`` to ``active-cti``

The classtype of suricata rules generated by active CTI is renamed to ``active-cti``.

2.7.2 Removal of interoperability

Interconnects with the following solutions have been removed:

- Intelligence
 - Hurukai
-

2.7.3 IDMEF format

The IDMEF format is no longer supported when exporting events to a Syslog server.

Chapter 3

Patches

Section left empty intentionally

Chapter 4

Known problems and limitations

4.1 Active-CTI / RetroHunt - Post Update problem

In some cases, Active-CTI and RetroHunt (available with the LIS license) may not work optimally.

Workaround : contact Gatewatcher Technical Support.

4.2 GCenter Backup/Restore - Error management

If an error has been made by the user while applying the restore procedure, the menu progress bar (`Admin-Backup/Restore - Backup operations` screen) remains blocked and no error message is visible in the WebUI.

Workaround: no workaround.

4.3 GCenter Backup/Restore - Pairing the GCap

Following a GCenter backup, if the GCap pairing is deleted, then restoring the backup will not enable restoring the connection with the previously deleted GCap.

Workaround: reapply the pairing.

4.4 Incorrect GCap status after updating the GCenter

The GCap status may be wrong after updating the GCenter (Last update = unknown / State: Online but update outdated)

Workaround: apply again the ruleset configuration at the GCap level.

4.5 Sigflow Manager - Transform Category

Applying a Transform category raises a 500 error if no ruleset is available on GCenter.

Workaround: create a ruleset.

4.6 Sigflow Manager - Error 500 when adding a rule in a custom source

Adding a rule raises a 500 error if the following conditions are present:

- The addition is done by editing a custom source
- the rule already exists in another custom source (same SID)

Workaround: change the SID of the rule you want to add to avoid the SID conflict.

4.7 Sigflow Manager - Inconsistency in displaying the number of categories and rules in a category

The `Sigflow > Sources` homepage shows the number of categories and rules contained in each source.

It is possible that the information presented is inconsistent with the actual content of the sources.

This case can occur after editing a custom source or an update.

Workaround: no workaround.

4.8 Sigflow Configuration - Custom source name cannot contain space

In the ``Config - Sigflow/sources`` screen of the legacy web UI, it is possible to define a custom source of signatures for the Sigflow detection engine.

During the addition procedure, the source name must be entered.

This name must not contain any space otherwise it will generate an error.

Workaround: change the name by removing spaces.

4.9 GCenter Backup/Restore - Error in FQDN

In v2.5.3.103, when restoring a backup, if the FQDN of the target GCenter is different then an error is generated.

Workaround: change the FQDN of the target GCenter and perform a reboot.

4.10 Kibana - Error 500 due to changing storage media for ES data

Following the change of ES data storage media, a temporary 500 error may appear when accessing Kibana.

Workaround: wait a few minutes.

4.11 Migration - Problem with online update configuration

During the migration to v2.5.3.103, in some cases, the process fails due to the configuration of the online update.

Workaround: this problem is corrected in v2.5.3.103-HF1.

4.12 Migration - Problem with the detected user base of NDR interface

During the migration to v2.5.3.103, when the database of detected users, visible on the NDR interface in the ``users`` tab, contains several tens of thousands of entries, the update process does not succeed.

Workaround: this problem is corrected in v2.5.3.103-HF1.

4.13 Migration - Problem with the application of Sigflow rulesets

During the migration to v2.5.3.103, if a ruleset other than the ``default_ruleset`` is used it may not apply correctly.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.14 Network - Problem with interface MTU configuration

In some cases, the MTU of the MGMT0 and VPN0 interfaces does not apply correctly.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.15 Network - VPN connectivity issue between GCap and GCenter

In the case of using the VPN0 interface, the VPN tunnel between GCap and GCenter may not work properly.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.16 GUM - Problem with the configuration of the address of a local repository

In the GUM configuration, if the local repository address contains a number, an error appears.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.17 Backup/Restore - Wrong format of the logs of the export in Syslog

When restoring a backup, if the log format is in `ECS`, it will be reset to `Legacy` in the Syslog export configuration.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.18 Migration - Improper configuration of scheduled backups

During the migration to v2.5.3.103, the configuration of the scheduled backup could be wrong.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.19 ECS - Missing http_refer field

The `http_refer` field is missing in ECS-formatted events.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.20 CTI - Active-CTI Alerts Missing in the NDR Interface

In some cases, Active-CTI alerts are not present in the NDR interface.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.21 CTI - Change of the SID of the Active-CTI rules with each update of Sigflow

The SIDs of rules generated by Active-CTI change when an update to the Sigflow engine.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.22 Sigflow - Error while updating engine

When updating the Sigflow engine, an error message may appear.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.23 NDR interface - Loss of filter on IP address in Asset and User views.

When clicking on an alert from the NDR `Asset` and `User` views, if a filter is set for the IP address, it will be deleted.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.24 XDP Filter - Configuration synchronization

When an interface is added or removed from the GCap, the configuration synchronization does not perform correctly.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.25 WebUI - Access Issue

In some cases, access to the WebUI is not possible.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.26 Malcore - File storage space saturation

In some cases, the file storage space can fill up quickly.

Workaround: this problem is corrected in v2.5.3.103-HF2.

4.27 Retention - Saturation of the storage space in Elasticsearch

It is possible to configure retention that is greater than the available storage space, which can render data indexing inoperative in Elasticsearch.

Workaround: this issue is fixed in v2.5.3.103-HF3.

4.28 NDR Interface - Problem with muting alerts

In some cases, muting alerts doesn't work properly.

Workaround: this issue is fixed in v2.5.3.103-HF3.

4.29 Kibana - Beacon Detect dashboard

From the NDR interface, the redirection to the Beacon Detect dashboard is not done correctly.

Workaround: this issue is fixed in v2.5.3.103-HF3.

4.30 Update - Issue with UEFI version

In UEFI, updating to the next major version is not done correctly.

Workaround: this issue is fixed in v2.5.3.103-HF3.

4.31 NDR - User detection

User detection is not performing correctly with the next major release of GCap.

Workaround: this issue is fixed in v2.5.3.103-HF3.

4.32 NDR Interface - Alert Filtering

In some cases, the filtering of alerts in the NDR interface does not perform correctly.

Workaround: this issue is fixed in v2.5.3.103-HF3.

4.33 NDR interface - Solution health

On the homepage, some of the platform's health status counters are incorrect.

Workaround: this issue is fixed in v2.5.3.103-HF3.

4.34 Help - Embedded documentation

In some cases, the redirection to the embedded documentation is done to the wrong section.

Workaround: this issue is fixed in v2.5.3.103-HF3.

4.35 NDR Interface - Home Page links

Some links on the home page redirect the user with a wrong date and time filter.

Workaround: this issue is fixed in v2.5.3.103-HF3.

4.36 DGA - Addition of a comment

When configuring the DGA engine, it is not possible via the web interface to add a comment when adding an exception.

Workaround: this issue is fixed in v2.5.3.103-HF3.

Chapter 5

Software compatibility

5.1 Compatibility with the GCap

GCenter version	GCap version	Compatibility
2.5.3.103	2.5.3.105	Unsupported configuration: GCap is to be migrated in advance of the GCenter update
2.5.3.103	2.5.4.0 (or +)	Configuration ok

Chapter 6

Hardware compatibility

The version 2.5.3.103 is compatible with every hardware version of the GCenter.

GCENTER Reference	Local storage	Other storage	Network Interface	Power supply
G CENT8100r2	2 x 960GB RAID1	2 x 2 TB RAID1	4 x RJ45	2 x 750W
G CENT9100r2	4 x 480GB RAID5	2 x 2 TB RAID1	4 x RJ45	2 x 750W
G CENT9900r2	10 x 480GB RAID5	4 x 2 TB RAID5	4 x RJ45	2 x 1100W
G CENT10500r2	12 x 480GB RAID5	4 x 2 TB RAID5	4 x RJ45	2 x 1100W

Chapter 7

Hotfix

7.1 Package 1

Package 1 - Hotfix ([HF1](#) / [SHA256](#))

Package 1 - Update/Install ([HF1_upgrade](#) / [SHA256_upgrade](#))

Hotfix No. 1 applies to the following versions:

- Version 2.5.3.102-HF3
- Version 2.5.3.103-HF0

If you want to update a GCenter v2.5.3.103, apply the **Package 1 - Hotfix** via the `Updates > Software Update` menu.

If you want to update a GCenter v2.5.3.102, apply the **Package 1 - Update/Installation** via the `GUM > Software Update` menu`.

Hotfix 1 fixes the following issues:

- *[Migration - Problem with online update configuration](#)*
- *[Migration - Problem with the detected user base of NDR interface](#)*

7.2 Package 2

Package 2 - Hotfix ([HF2](#) / [SHA256](#))

Package 2 - Update/Install ([HF2_upgrade](#) / [SHA256_upgrade](#))

Hotfix No. 2 applies to the following versions:

- Version 2.5.3.102-HF3
- Version 2.5.3.103-HF1

If you want to update a GCenter v2.5.3.103, apply the **Package 2 - Hotfix** via the `Updates > Software Update` menu.

If you want to update a GCenter v2.5.3.102, apply Package 2 - Update/Installation** via the `GUM > Software Update` menu.

Hotfix 2 fixes the following issues:

- *[Migration - Problem with the application of Sigflow rulesets](#)*
- *[Network - Problem with interface MTU configuration](#)*
- *[Network - VPN connectivity issue between GCap and GCenter](#)*
- *[GUM - Problem with the configuration of the address of a local repository](#)*
- *[Backup/Restore - Wrong format of the logs of the export in Syslog](#)*
- *[Migration - Improper configuration of scheduled backups](#)*
- *[ECS - Missing http_refer field](#)*
- *[CTI - Active-CTI Alerts Missing in the NDR Interface](#)*
- *[CTI - Change of the SID of the Active-CTI rules with each update of Sigflow](#)*
- *[Sigflow - Error while updating engine](#)*
- *[NDR interface - Loss of filter on IP address in Asset and User views.](#)*
- *[XDP Filter - Configuration synchronization](#)*
- *[WebUI - Access Issue](#)*
- *[Malcore - File storage space saturation](#)*

7.3 Package 3

Package 3 - Hotfix ([HF3](#) / [SHA256](#))
Package 3 - BIOS Update/Installation ([HF3_upgrade](#) / [SHA256_upgrade](#))
Package 3 – UEFI Installation ([HF3_upgrade](#) / [SHA256_upgrade](#))

Hotfix 3 applies to the following versions:

- Version 2.5.3.102-HF3
- Version 2.5.3.103-HF2

If you want to update a GCenter v2.5.3.103, apply **Package 3 - Hotfix** via the `Updates > Software Update` menu.
If you want to update a GCenter v2.5.3.102, apply **Package 3 - Update/Installation** via the `GUM > Software Update menu`.

Attention:

Applying this hotfix will cause the GCenter to restart.

Hotfix 3 fixes the following issues:

- *Retention - Saturation of the storage space in Elasticsearch*
- *NDR Interface - Problem with muting alerts*
- *Kibana - Beacon Detect dashboard*
- *Update - Issue with UEFI version*
- *NDR - User detection*
- *NDR Interface - Alert Filtering*
- *NDR interface - Solution health*
- *Help - Embedded documentation*
- *NDR Interface - Home Page links*
- *DGA - Addition of a comment*

Hotfix 3 introduces a new reporting feature.



Chapter 8

Procedure for upgrading from V102 to V103

8.1 Prerequisites

To deploy the **V2.5.3.103** update:

- The GCenter will need to be version **V2.5.3.102-HF3** or higher
- The GCap will need to be version **V2.5.4.0** or higher
- If you have any questions about these items, please contact the Gatewatcher Technical Support

Important:

It is highly recommended to have an iDRAC type connection in order to be able to connect post-upgrade if a problem occurs during the process. Otherwise, you'll need a physical access to the equipment (screen, keyboard).

Important:

Before proceeding with the update, it is strongly recommended to backup the GCenter configuration in the ``Administrators > Backup / Restore > Operations`` menu and to back up the file on an external server in a directory indicating the current version of the GCenter (example: 2.5.3.102-XXXX-HFX).

8.2 Retained data

The set of the GCenter configuration and data is retained.
Metadata and alerts present on the GCenter before the migration to version 2.5.3.103 will only be viewable in the ``Discover`` menu of the ``Hunting`` interface.

8.3 Procedure to install

1. Make sure the GCap probes are version **V2.5.4.0** or higher, otherwise refer to the following update procedure: https://releases.gatewatcher.com/fr/gcap/2.5.4/V0/8_upgrade_procedure.html
2. Download the newly available version of the GCenter and the associated sha256 on the <https://update.gatewatcher.com/upgrade/> platform (directory 2.5.3.103).

Important:

For the update to V2.5.3.103, it is recommended to use the latest package.

1. Check the image with the associated sha256.
2. Connect to the GCenter WebUI and go to the ``Admin > GUM > Software update`` menu.
3. In the ``Uploading a new software update`` section, click on the ``Choose a file`` button, select the new GCenter version previously uploaded and then click on ``Submit``.
4. Connect to the GCap with the SSH account **setup**.
5. Shut down the monitoring engine with the following command: ``monitoring-engine stop``.
6. Change the compatibility mode with the following command: ``set compatibility-mode 2.5.3.103``.
7. Start the monitoring engine with the following command: ``monitoring-engine start``.
8. To keep the data already being processed at the GCenter, check in the ``Hunting > Metadata`` menu that there is no further processing.
9. In the ``Saved package list`` section, at the location of the previously sent update, click on the ``Apply`` button.
10. Once the operation is complete, restart the GCenter by connecting via SSH with the **setup** account and then going to the ``Restart`` menu.
11. Once the GCenter is restarted, connect to the WebUI and check whether new events appear in the ``Hunting`` section.