# Documentation
# GCenter Version 2.5.3.102

GATEWATCHER

Documentation version: V3

Translated from original manual version 3

Creation date: January, 2023

Last update: January, 2024

# Contents

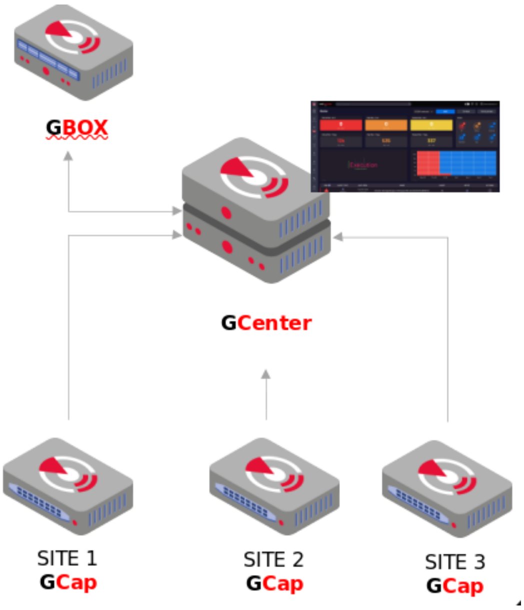
# Chapter 1

# Description

## 1.1 Introduction

The AIONIQ solution is Gatewatcher's Intrusion Detection System (IDS).
It includes:

- one or more TAPS
- one or more GCaps
- a GCenter
- a GBox (optional)



## 1.2 Overview of the TAP

A Test Access Point (TAP) is a passive device enabling the monitoring of a computer network by duplicating certain flows that transit on the network and redirecting them to a detection probe (GCap), for example.
It is possible to connect several TAPs to a GCap, as the latter has several capture interfaces.

---

## 1.3 Presentation of the GCap

The GCap is an IDS type detection probe deployed at each site.
It enables:

- capturing and analyzing network traffic from TAPs
- reconstructing the files present in the analyzed flow (according to type and size parameters)
- carrying out an initial analysis
- generating alerts and / or metadata type events
- transmitting files / codes / events to the GCenter

For more information, please refer to the GCAP documentation.

---

## 1.4 Presentation of the GCenter

The GCenter is the second component of the system working in conjunction with the GCap detection probe
Its main functions include:

- The management of the GCap probe including managing the analysis rules, signatures, health status supervision, and so on.
- In-depth analysis of the files retrieved by the probe
- Administering the system
- Displaying the results of the various analyses in different dashboards
- Long-term data storage
- Exporting data to third-party solutions such as the Security Information and Events Management (SIEM) system
- Sends files to the GBox for analysis and retrieves reports

---

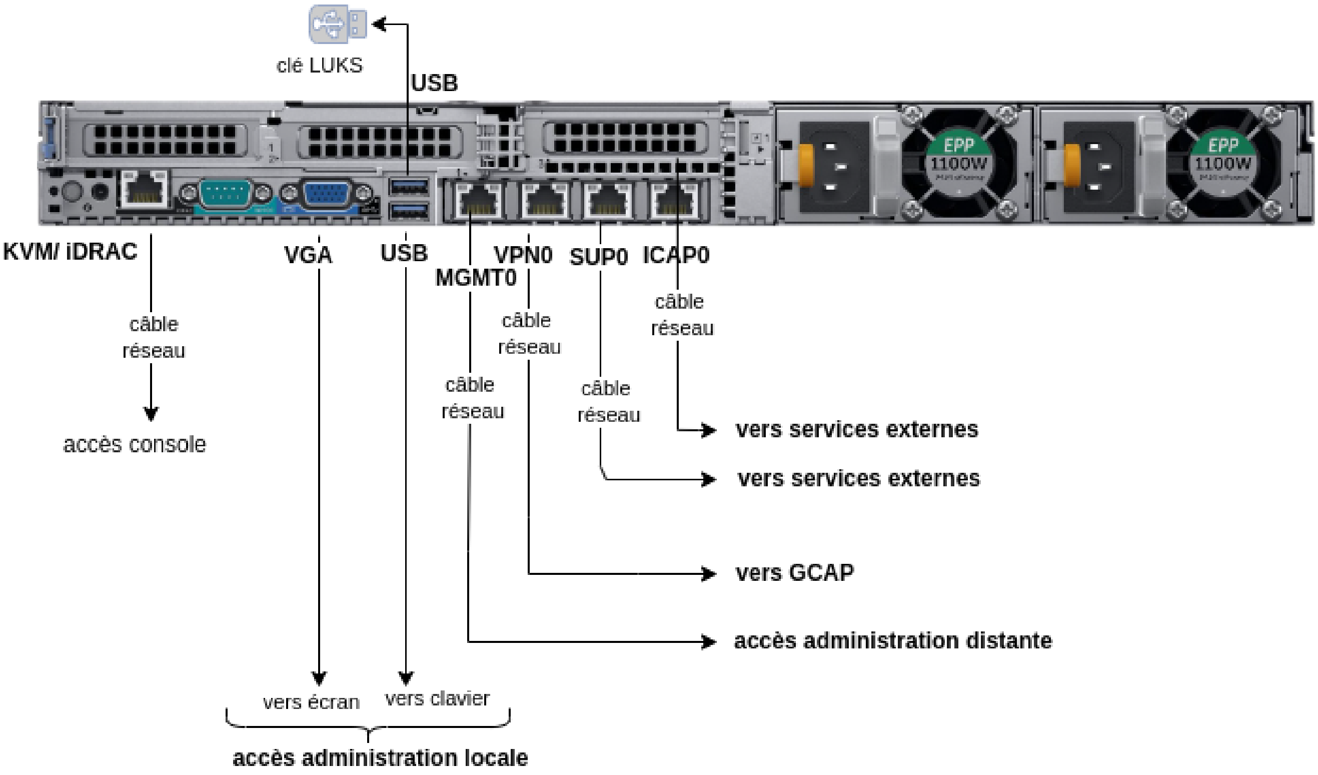
### 1.4.1 Different server models

For more information, please refer to *Mechanical characteristics of GCenter*.

---

### 1.4.2 List of the GCenter inputs / outputs

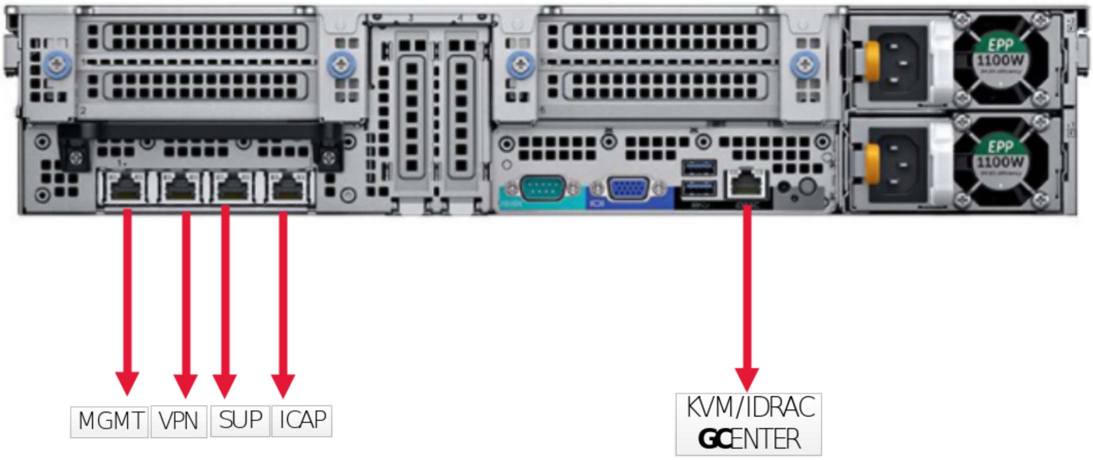
**Example of a GCenter server 7100/8100/9100** :



The **GCenter** comprises:

| Inputs/outputs | Usage |
|---|---|
| USB and VGA connector | Directly access a keyboard and a monitor.<br>This connection mode is deprecated in favour of KVM/IDRAC/XCC and should only be used as a last resort |
| USB connector | Accommodates the USB key enabling disk decryption (standard Linux Unified Key Setup) |
| RJ-45 connector `` `KVM/IDRAC` `` | Remote access to the server's management and configuration interface |
| RJ-45 connector `` `MGMT0` `` | Management and VPN interface with **GCAP** |
| RJ-45 connector `` `VPN0` `` | Dedicated VPN interface with **GCAP** (optional) |
| RJ-45 connector `` `ICAP0` `` | Interaction with external services |
| RJ-45 connector `` `SUP0` `` | Interaction with external services |
| Two power supplies | Redundant server power supplies |

**Example of a GCenter server 9900/10500** :



**Note:**

Although the names of the interfaces may suggest that they are specifically dedicated, it is possible to use these interfaces for other purposes via the "output interfaces" options.

Viewing these communication links is provided in the section *Interconnection between devices*.

#### 1.4.2.1 Use of USB and VGA connectors

Connecting a keyboard and monitor enables direct access to the GCenter console interface.

**Important:**

This mode is deprecated. It should only be used during initial installation and for advanced diagnosis.

#### 1.4.2.2 Access to the server's management and configuration interface

Access to this management interface is via HTTPS:

- on a Dell server, this connector is called **iDRAC**. It is noted on the **KVM/IDRAC** diagram
- on a Lenovo server, this connector is called **TSM**: This connector can be identified by a wrench symbol on the bottom of it.

#### 1.4.2.3 `MGMT0` and `VPN0` network interfaces

The network interfaces `MGMT0` and `VPN0` are connected to the network interfaces `gcp0` and `gcp1`. These interfaces enable the following 2 functions:

- Function 1: remote administration through the SSH protocol with access:
  - To the graphical setup/configuration menu
- Function 2: secure communication between the GCenter and the probe through an IPSEC tunnel in order to:
  - Escalate information such as files, alerts, metadata, and so on, derived from analyzing the monitored flows
  - Report information on the health of the probe to GCenter
  - Control the probe - analysis rules, signatures, etc.

There are 2 configuration possibilities:

- The **single interface configuration**
- The **dual-interface configuration**

In **single interface configuration**:

- The `MGMT0` interface is used and connected to the `gcp0` network interface of the GCap
  This interface ensures functions 1 and 2.
- The `VPN0` interface is not used

In **dual-interface configuration**:

- The `MGMT0` interface is used and connected to the `gcp0` network interface of the GCap
  This interface ensures function 1.
- The `VPN0` interface is used and connected to the `gcp1` network interface of the GCap
  This interface ensures function 2.

The purpose of the dual-interface configuration is to ensure that the management flow and the interconnection flow between the GCap and the GCenter are separated from each other.

**Important:**

This configuration of flow separation by interface is mandatory when using the **MPL mode** on the GCenter.

---

#### 1.4.2.4 Network interfaces `ICAP0` and `SUP0`

These two interfaces enable, if needed, communicating with services external to the solution such as:

- An update server
- A supervision server
- An LDAP server
- A log server or an SIEM
- A storage server for backing up the solution
- etc.

---

#### 1.4.2.5 Electrical connection

The server has two electrical power supplies, each of which has the necessary power to operate the equipment.
It is strongly recommended that each power supply should be connected to a separate power supply.

---

#### 1.4.2.6 USB connector and LUKS key

During installation, the contents of the disks (excluding /boot) are encrypted using the LUKS standard.
During this process, a unique encryption key is created and placed on the USB stick connected to the equipment.
Upon start-up, the USB key must be plugged into the equipment to allow the disks to be decrypted
It is strongly recommended to make a copy of this key because, in the event of failure, the data on the disks will no longer be accessible.
Once the system is up and running, the USB stick should be removed and placed in a secure place (e.g. in a safe).

---

## 1.5 Presentation of the GBox

The GBox is an equipment that can operate independently or in conjunction with the GCenter.
This *appliance* enables:

- Automatically receive suspicious files that require in-depth malware analysis without using an external service
- Analyze suspicious files on demand from the GCenter UI web interface
- Return reports to GCenter for files that have been submitted to GCenter and are visible from the GCenter Web UI and GBox
- Analyze files directly on the GBox Web UI and generate a corresponding report
- The user to manually perform an analysis on domain names that have been generated by DGAs (Domain Generation Algorithm)

For more information, refer to the GBox documentation.

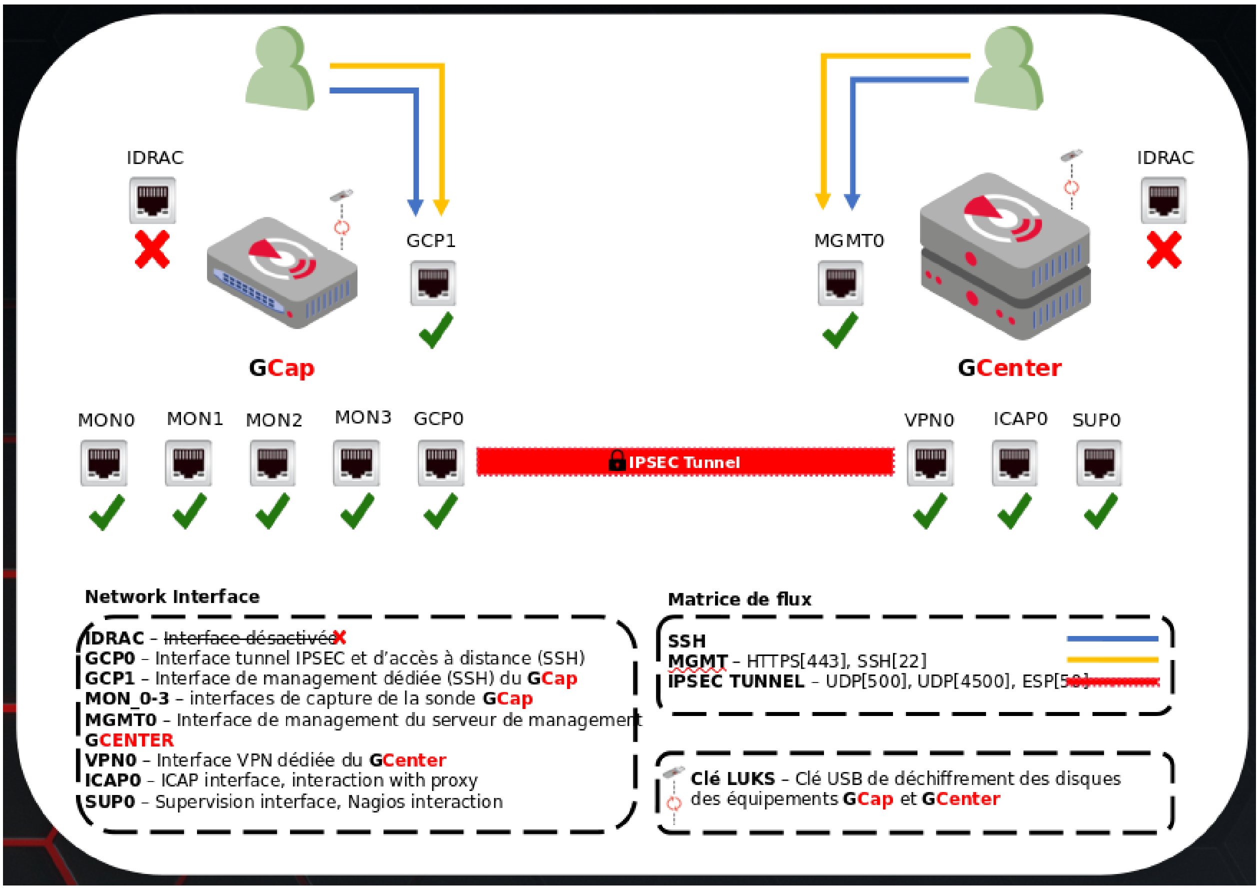
---

## 1.6 Interconnection between devices

### 1.6.1 Viewing communication flows

Below, diagrams are displayed representing the various inputs/outputs of the GCap and GCenter and the corresponding communication flows.
There are two possible configurations for communicating between the **GCap** and the **GCenter** :

- The **dual-interface configuration** is the mandatory mode in the event of a sensitive environment



**Network Interface**

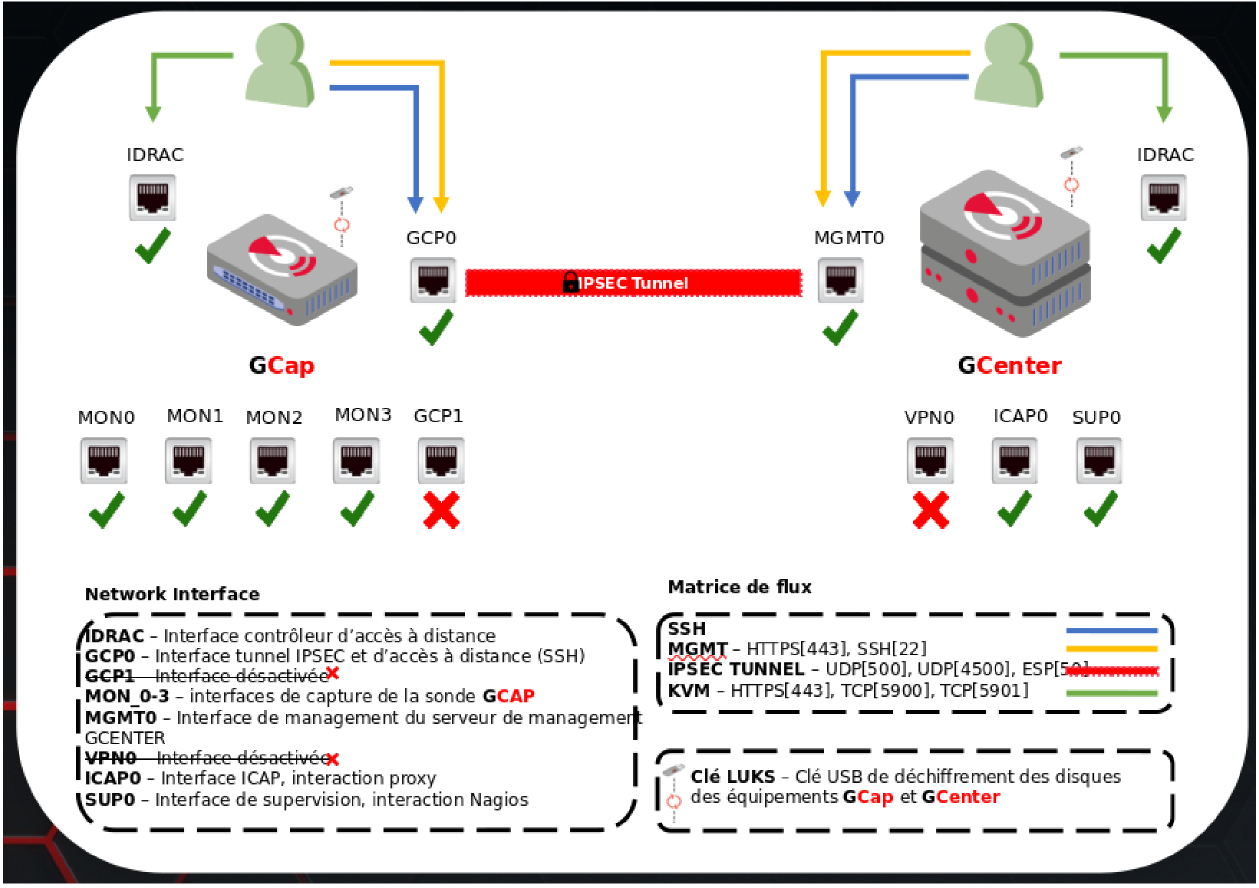
**IDRAC** – ~~Interface désactivée~~ ✗
**GCP0** – Interface tunnel IPSEC et d'accès à distance (SSH)
**GCP1** – Interface de management dédiée (SSH) du **GCap**
**MON_0-3** – interfaces de capture de la sonde **GCap**
**MGMT0** – Interface de management du serveur de management **GCENTER**
**VPN0** – Interface VPN dédiée du **GCenter**
**ICAP0** – ICAP interface, interaction with proxy
**SUP0** – Supervision interface, Nagios interaction

**Matrice de flux**

**SSH**
**MGMT** – HTTPS[443], SSH[22]
**IPSEC TUNNEL** – UDP[500], UDP[4500], ESP[50]

**Clé LUKS** – Clé USB de déchiffrement des disques des équipements **GCap** et **GCenter**

- The **single-interface configuration**, on the other hand, enables an interface (MGMT0) to be pooled to transit the management and VPN flows.



**Network Interface**

**IDRAC** – Interface contrôleur d'accès à distance
**GCP0** – Interface tunnel IPSEC et d'accès à distance (SSH)
~~**GCP1** – Interface désactivée~~ ✗
**MON_0-3** – interfaces de capture de la sonde **GCAP**
**MGMT0** – Interface de management du serveur de management GCENTER
~~**VPN0** – Interface désactivée~~ ✗
**ICAP0** – Interface ICAP, interaction proxy
**SUP0** – Interface de supervision, interaction Nagios

**Matrice de flux**

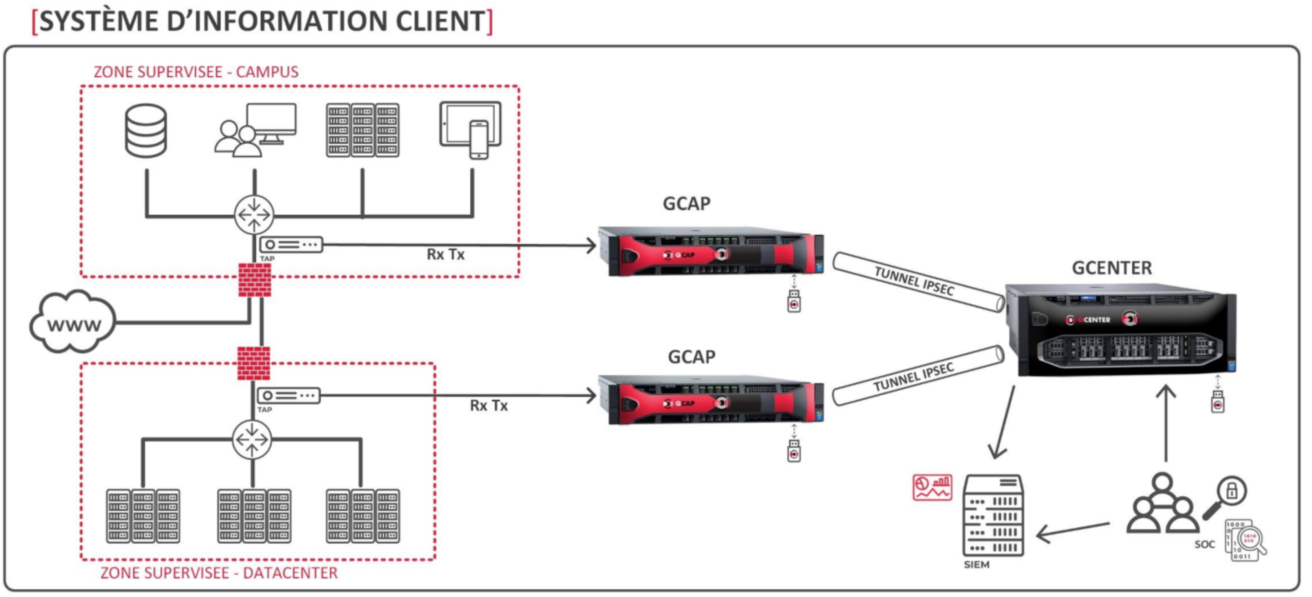
**SSH**
**MGMT** – HTTPS[443], SSH[22]
**IPSEC TUNNEL** – UDP[500], UDP[4500], ESP[50]
**KVM** – HTTPS[443], TCP[5900], TCP[5901]

**Clé LUKS** – Clé USB de déchiffrement des disques des équipements **GCap** et **GCenter**

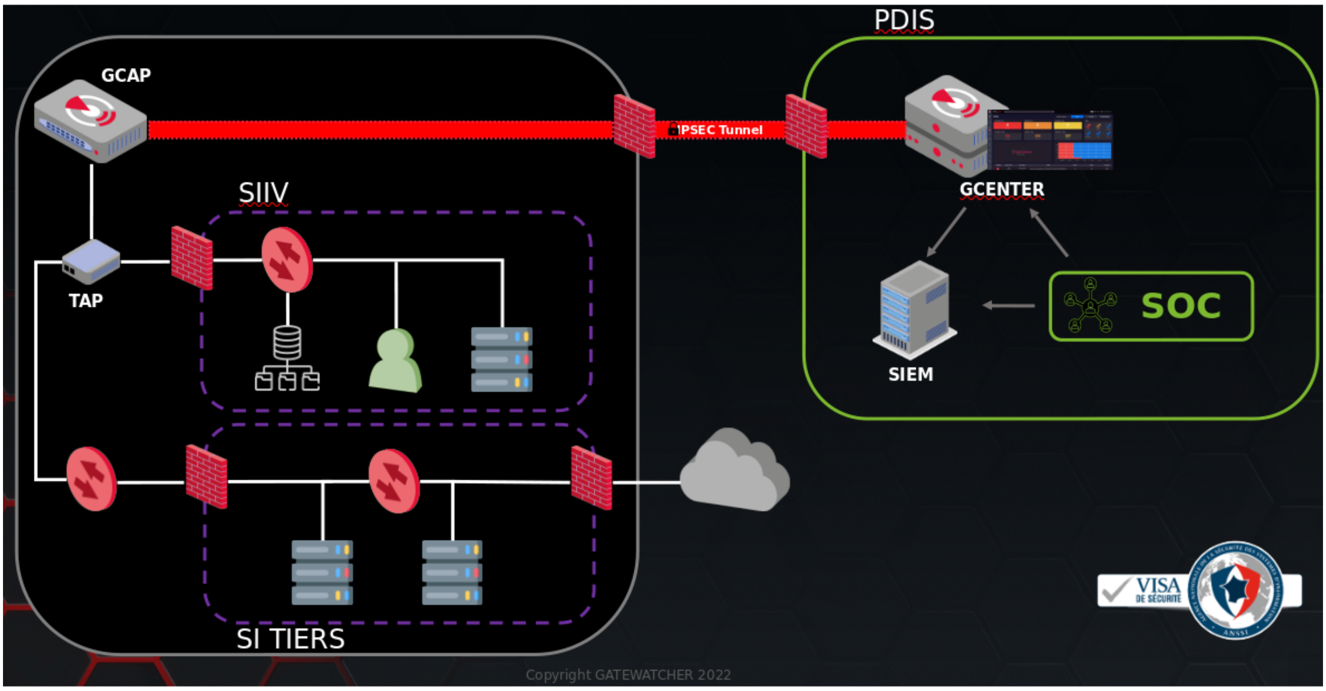
## 1.6.2 Example of architectures

Here are three examples of implementing the solution in an information system:

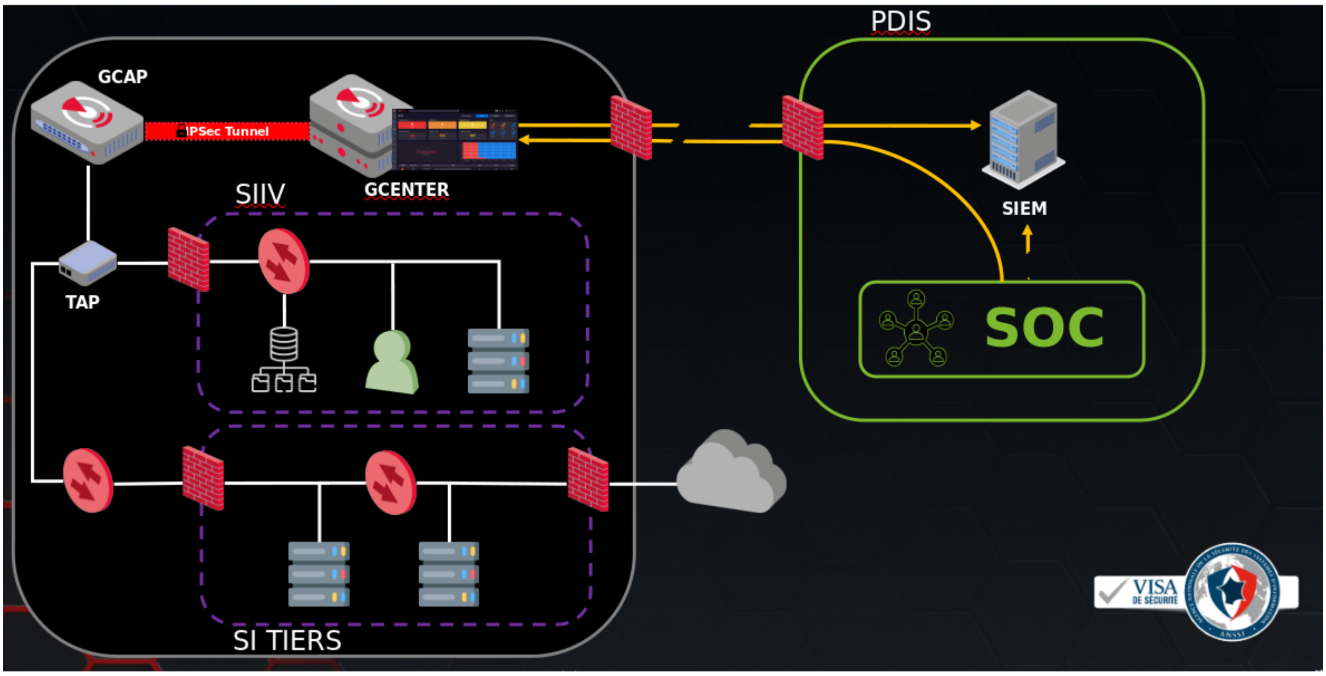
### 1.6.2.1 Detection architecture diagram



### 1.6.2.2 MPL 1 (PDIS 1 architecture diagram)



#### 1.6.2.3 MPL 2 (PDIS 2 architecture diagram)



# Chapter 2

# Operation

## 2.1 Detection Engines

### 2.1.1 Malcore engine

#### 2.1.1.1 Presentation

The Malcore detection engine enables:

- Malware detection through static and heuristic multi-engine analysis in real time of files
- Scanning via 16 anti-virus engines
- Scanning capacity of more than 6 million files per 24 hours

The 16 anti-virus engines are displayed under the name "engine hash" in the web interface.
The names of the antivirus engines are not disclosed.

**Attention:**

Engine hash names may change over time

---

#### 2.1.1.2 Events generated

The events generated by the Malcore engine are known as **alerts**.
These are displayed:

- In the main interface named **WEB UI** of the GCenter in the `` `Alerts` `` screen (the main interface named **WEB UI** is described in the *Overview of the WEB UI*).
  To view the alerts, select the MALWARE filter and view the list of alerts: see the presentation of the *Web UI `Alerts` screen*.
  By clicking on an alert, the detailed information of this alert is displayed: see *Example of a Malcore alert in the webui*.
- In the **Kibana UI** interface
  To view the alerts, select the MALWARE filter and view the list of alerts: see the presentation of the *Web UI `Alerts` screen*.

By clicking on an alert, select on the command `Flow details` then select the arrow to the left of the alert.

The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

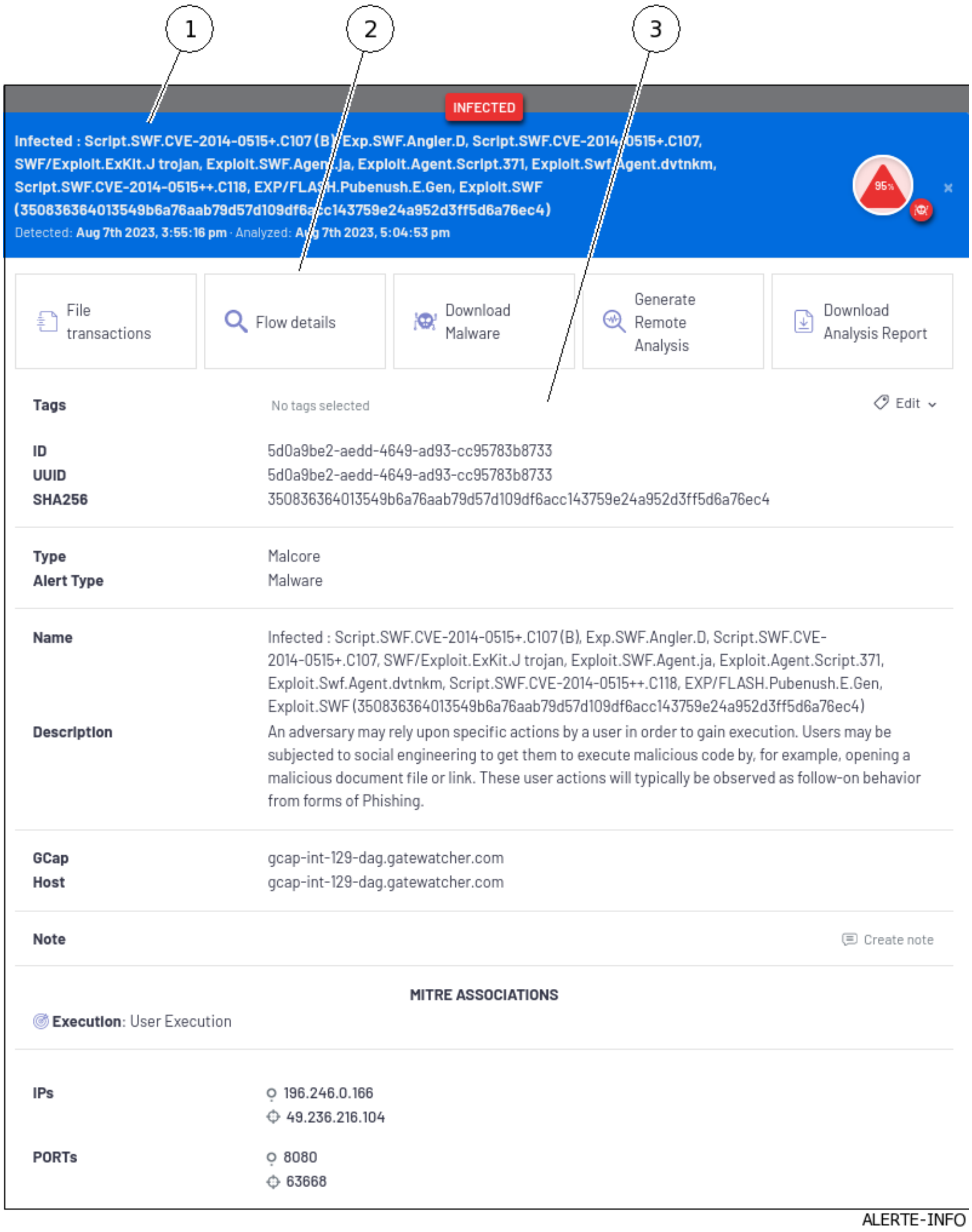
The detailed information of this alert can be viewed in table or jason format (see *Malcore log example*).

From the **WEB UI** main interface, it is possible to :

- Download the source file
- Send it to the GBox or Intelligence site
- Retrieve the analysis report

---

### 2.1.1.2.1 Example of a Malcore alert in the webui



Infected : Script.SWF.CVE-2014-0515+.C107 (B), Exp.SWF.Angler.D, Script.SWF.CVE-2014-0515+.C107, SWF/Exploit.ExKit.J trojan, Exploit.SWF.Agent.ja, Exploit.Agent.Script.371, Exploit.Swf.Agent.dvtnkm, Script.SWF.CVE-2014-0515++.C118, EXP/FLASH.Pubenush.E.Gen, Exploit.SWF (350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4)

Detected: **Aug 7th 2023, 3:55:16 pm** · Analyzed: **Aug 7th 2023, 5:04:53 pm**

| | |
|---|---|
| **Tags** | No tags selected |
| **ID** | 5d0a9be2-aedd-4649-ad93-cc95783b8733 |
| **UUID** | 5d0a9be2-aedd-4649-ad93-cc95783b8733 |
| **SHA256** | 350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4 |
| **Type** | Malcore |
| **Alert Type** | Malware |
| **Name** | Infected : Script.SWF.CVE-2014-0515+.C107 (B), Exp.SWF.Angler.D, Script.SWF.CVE-2014-0515+.C107, SWF/Exploit.ExKit.J trojan, Exploit.SWF.Agent.ja, Exploit.Agent.Script.371, Exploit.Swf.Agent.dvtnkm, Script.SWF.CVE-2014-0515++.C118, EXP/FLASH.Pubenush.E.Gen, Exploit.SWF (350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4) |
| **Description** | An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of Phishing. |
| **GCap** | gcap-int-129-dag.gatewatcher.com |
| **Host** | gcap-int-129-dag.gatewatcher.com |
| **Note** | |

**MITRE ASSOCIATIONS**

**Execution**: User Execution

| | |
|---|---|
| **IPs** | 196.246.0.166<br>49.236.216.104 |
| **PORTs** | 8080<br>63668 |

Example of a Malcore alert in the webui *Malcore log data structure*.

---

#### 2.1.1.2.2 Malcore log example

```
{
"_index": "malware-2023.10.09-000162",
"_type": "_doc",
"": "Dr-PE4sBeBoubSygq3KJ",
"_version": 1,
"_score": 1,
"_source": {
  "proto": "TCP",
  "gcap": "gcap-xxxxxxxxx.domain.local",
  "uuid": "f639c844-3f6f-40fa-86c4-47ff603880e2",
  "host": "gcap-xxxxxxxxx.domain.local",
  "timestamp": "2023-10-09T08:23:13.332538+0000",
  "email": {
     "status": "PARSE_DONE",
     "to": [
      "test@gouv.fr"
     ],
     "attachment": [
      "smtptest-2021-02-24T17-30-01Z.zip"
     ],
     "from": "heartbeat@free.fr"
    },
  "processing_time": 1341,
  "dest_ip": "x.x.x.x",
  "detail_scan_time": 245,
  "src_port": 36746,
  "event_type": "malware",
  "@version": "1",
  "analyzers_up": 16,
  "vlan": [
    3044
   ],
  "analyzed_clean": 0,
  "analyzed_other": 7,
  "file_type_description": "ZIP Archive",
  "timestamp_analyzed": "2023-10-09T08:31:04.503Z",
  "state": "Infected",
  "analyzed_infected": 9,
  "dest_port": 25,
  "engines_last_update_date": "2023-07-11T11:32:00Z",
  "detail_threat_found": "Infected : EICAR-Test-File (not a virus) (B), Virus/EICAR_Test_File,
↪ EICAR-Test-File (not a virus), Eicar test file, EICAR_Test_File, Eicar-Signature, Eicar-
↪Test-Signature, EICAR_Test_File, EICAR-Test-File",
  "magic_details": "Zip archive data, at least v2.0 to extract",
  "total_found": "9/16",
  "detail_wait_time": 1096,
  "timestamp_detected": "2023-10-09T08:23:13.332Z",
  "type": "malcore",
  "code": 1,
  "file_type": "application/zip",
  "smtp": {
    "mail_from": "<heartbeat@free.fr>",
    "rcpt_to": [
      "<test@gouv.fr>"
    ],
```

(suite sur la page suivante)

(suite de la page précédente)

```
    "helo": "gouv.fr"
  },
  "engine_id": {
    "0": {
      "threat_details": "EICAR-Test-File (not a virus) (B)",
      "id": "038e407ba285f0e01dd30c6e4f77ec19bad5ed3dc866a2904ae6bf46baa14b74",
      "scan_result": "INFECTED"
    },
    "1": {
      "threat_details": "Virus/EICAR_Test_File",
      "id": "054a20c51cbe9d2cc7d6a237d6cd4e08ab1a67e170b371e632995766d3ba81af",
      "scan_result": "INFECTED"
    },
    "2": {
      "threat_details": "Unavailable (permanently_failed)",
      "id": "0ff95ddb1117d8f36124f6eac406dbbf9f17e3dd89f9bb1bd600f6ad834c25db",
      "scan_result": "NOT_SCANNED"
    },
    "3": {
      "threat_details": "EICAR-Test-File (not a virus)",
      "id": "312a189607571ec2c7544636be405f10889e73d061e0ed77ca0eca97a470838d",
      "scan_result": "INFECTED"
    },
    "4": {
      "threat_details": "Eicar test file",
      "id": "32f2f45e6d9faf46e6954356a710208d412fac5181f6c641e34cb9956a133684",
      "scan_result": "INFECTED"
    },
    "5": {
      "threat_details": "Unavailable (production)",
      "id": "3bfeb615a695c5ebaac5ade948ffae0c3cfec3787d4625e3abb27fa3c2867f53",
      "scan_result": "NOT_SCANNED"
    },
    "6": {
      "threat_details": "EICAR_Test_File",
      "id": "4ca73ae4b92fd7ddcda418e6b70ced0481ac2d878c48e61b686d0c9573c331dc",
      "scan_result": "INFECTED"
    },
    "7": {
      "threat_details": "Unavailable (production)",
      "id": "527db072abcf877d4bdcd0e9e4ce12c5d769621aa65dd2f7697a3d67de6cc737",
      "scan_result": "NOT_SCANNED"
    },
    "8": {
      "threat_details": "Unavailable (production)",
      "id": "714eca0a6475fe7d2bf9a24bcae343f657b230ff68acd544b019574f1392de77",
      "scan_result": "NOT_SCANNED"
    },
    "9": {
      "threat_details": "Unavailable (production)",
      "id": "95603b80d80fa3e98b6faf07418a55ed0b035d19209e3ad4f1858f6b46fa070a",
      "scan_result": "NOT_SCANNED"
    },
    "10": {
      "threat_details": "Unavailable (production)",
      "id": "a9b912e461cec506780d8ad8e785cca6b233ad7c72335c262b0a4ab189afa713",
```

(suite sur la page suivante)

(suite de la page précédente)

```
     "scan_result": "NOT_SCANNED"
   },
   "11": {
     "threat_details": "Eicar-Signature",
     "id": "ad05e0dc742bcd6251af91bd07ef470c699d5aebbb2055520b07021b14d7380c",
     "scan_result": "INFECTED"
   },
   "12": {
     "threat_details": "Eicar-Test-Signature",
     "id": "af6868a2b87b3388a816e09d2b282629ccf883b763b3691368a27fbd6f6cd51a",
     "scan_result": "INFECTED"
   },
   "13": {
     "threat_details": "Unavailable (production)",
     "id": "b14014e40c0e672e050ad9c210a68a5303ce7facabae9eb2ee07ddf97dc0da0e",
     "scan_result": "NOT_SCANNED"
   },
   "14": {
     "threat_details": "EICAR_Test_File",
     "id": "ecc47e2309be9838d6dc2c5157be1a840950e943f5aaca6637afca11516c3eaf",
     "scan_result": "INFECTED"
   },
   "15": {
     "threat_details": "EICAR-Test-File",
     "id": "fe665976a02d03734c321007328109ab66823b260a8eea117d2ab49ee9dfd3f1",
     "scan_result": "INFECTED"
   }
 },
 "severity": 1,
 "fileinfo": {
   "md5": "c279be702893....",
   "gaps": false,
   "state": "CLOSED",
   "magic": "Zip archive data, at least v2.0 to extract",
   "file_id": 1,
   "sha256": "4679e7f2018c19...",
   "stored": true,
   "filename": "smtptest-2021-02-24T17-30-01Z.zip",
   "sid": [
     1100043
   ],
   "tx_id": 0,
   "size": 51675
 },
 "flow_id": 1016694867777403,
 "gcenter": "gcenter-xxx.domain.local",
 "SHA256": "4679e7f2018c19...",
 "src_ip": "X.X.X.X",
 "in_iface": "monvirt",
 "analyzed_error": 0,
 "reporting_token": "No GBOX",
 "analyzed_suspicious": 0,
 "app_proto": "smtp",
 "@timestamp": "2023-10-09T08:31:04.503Z"
},
"fields": {
```

(suite sur la page suivante)

(suite de la page précédente)

```
  "analyzed_other": [
    7
  ],
  "email.status": [
    "PARSE_DONE"
  ],
  "fileinfo.file_id": [
    1
  ],
  "engine_id.1.id": [
    "054a20c51cbe9d2cc7d6a237d6cd4e08ab1a67e170b371e632995766d3ba81af"
  ],
  "type": [
    "malcore"
  ],
  "engine_id.9.id": [
    "95603b80d80fa3e98b6faf07418a55ed0b035d19209e3ad4f1858f6b46fa070a"
  ],
  "smtp.helo": [
    "gouv.fr"
  ],
  "fileinfo.sid": [
    1100043
  ],
  "engine_id.1.threat_details": [
    "Virus/EICAR_Test_File"
  ],
  "engine_id.4.scan_result": [
    "INFECTED"
  ],
  "event_type": [
    "malware"
  ],
  "analyzed_suspicious": [
    0
  ],
  "engine_id.3.scan_result": [
    "INFECTED"
  ],
  "engine_id.1.scan_result": [
    "INFECTED"
  ],
  "engine_id.0.scan_result": [
    "INFECTED"
  ],
  "engine_id.2.scan_result": [
    "NOT_SCANNED"
  ],
  "state": [
    "Infected"
  ],
  "total_found": [
    "9/16"
  ],
  "engine_id.4.threat_details": [
    "Eicar test file"
```

(suite sur la page suivante)

(suite de la page précédente)

```
  ],
  "analyzed_clean": [
    0
  ],
  "gcenter": [
    "gcenter-int-128-dag.gatewatcher.com"
  ],
  "engine_id.15.threat_details": [
    "EICAR-Test-File"
  ],
  "engine_id.6.id": [
    "4ca73ae4b92fd7ddcda418e6b70ced0481ac2d878c48e61b686d0c9573c331dc"
  ],
  "dest_ip": [
    "x.x.x.x"
  ],
  "engine_id.14.id": [
    "ecc47e2309be9838d6dc2c5157be1a840950e943f5aaca6637afca11516c3eaf"
  ],
  "gcap": [
    "gcap-int-129-dag.gatewatcher.com"
  ],
  "timestamp_analyzed": [
    "2023-10-09T08:31:04.503Z"
  ],
  "engine_id.5.threat_details": [
    "Unavailable (production)"
  ],
  "engine_id.15.id": [
    "fe665976a02d03734c321007328109ab66823b260a8eea117d2ab49ee9dfd3f1"
  ],
  "engine_id.3.id": [
    "312a189607571ec2c7544636be405f10889e73d061e0ed77ca0eca97a470838d"
  ],
  "engine_id.15.scan_result": [
    "INFECTED"
  ],
  "email.to": [
    "test@gouv.fr"
  ],
  "vlan": [
    3044
  ],
  "fileinfo.filename": [
    "smtptest-2021-02-24T17-30-01Z.zip"
  ],
  "engine_id.14.threat_details": [
    "EICAR_Test_File"
  ],
  "email.from": [
    "heartbeat@free.fr"
  ],
  "smtp.mail_from": [
    "<heartbeat@free.fr>"
  ],
  "timestamp": [
```

(suite sur la page suivante)

(suite de la page précédente)

```
    "2023-10-09T08:23:13.332Z"
  ],
  "engine_id.0.threat_details": [
    "EICAR-Test-File (not a virus) (B)"
  ],
  "engine_id.8.id": [
    "714eca0a6475fe7d2bf9a24bcae343f657b230ff68acd544b019574f1392de77"
  ],
  "engine_id.7.threat_details": [
    "Unavailable (production)"
  ],
  "engine_id.0.id": [
    "038e407ba285f0e01dd30c6e4f77ec19bad5ed3dc866a2904ae6bf46baa14b74"
  ],
  "engine_id.5.scan_result": [
    "NOT_SCANNED"
  ],
  "engine_id.6.scan_result": [
    "INFECTED"
  ],
  "@timestamp": [
    "2023-10-09T08:31:04.503Z"
  ],
  "email.attachment": [
    "smtptest-2021-02-24T17-30-01Z.zip"
  ],
  "engine_id.7.scan_result": [
    "NOT_SCANNED"
  ],
  "engines_last_update_date": [
    "2023-07-11T11:32:00.000Z"
  ],
  "fileinfo.size": [
    51675
  ],
  "engine_id.9.scan_result": [
    "NOT_SCANNED"
  ],
  "engine_id.8.scan_result": [
    "NOT_SCANNED"
  ],
  "engine_id.12.id": [
    "af6868a2b87b3388a816e09d2b282629ccf883b763b3691368a27fbd6f6cd51a"
  ],
  "detail_threat_found": [
    "Infected : EICAR-Test-File (not a virus) (B), Virus/EICAR_Test_File, EICAR-Test-File (not a virus), Eicar test file, EICAR_Test_File, Eicar-Signature, Eicar-Test-Signature, EICAR_Test_File, EICAR-Test-File"
  ],
  "engine_id.12.threat_details": [
    "Eicar-Test-Signature"
  ],
  "reporting_token": [
    "No GBOX"
  ],
  "analyzed_infected": [
```

(suite sur la page suivante)

(suite de la page précédente)

```
    9
  ],
  "fileinfo.tx_id": [
    0
  ],
  "engine_id.9.threat_details": [
    "Unavailable (production)"
  ],
  "engine_id.13.threat_details": [
    "Unavailable (production)"
  ],
  "engine_id.5.id": [
    "3bfeb615a695c5ebaac5ade948ffae0c3cfec3787d4625e3abb27fa3c2867f53"
  ],
  "uuid": [
    "f639c844-3f6f-40fa-86c4-47ff603880e2"
  ],
  "engine_id.10.threat_details": [
    "Unavailable (production)"
  ],
  "flow_id": [
    1016694867777403
  ],
  "fileinfo.gaps": [
    "false"
  ],
  "file_type": [
    "application/zip"
  ],
  "host": [
    "gcap-xxxxxxxxx.domain.local"
  ],
  "engine_id.13.id": [
    "b14014e40c0e672e050ad9c210a68a5303ce7facabae9eb2ee07ddf97dc0da0e"
  ],
  "dest_port": [
    25
  ],
  "detail_scan_time": [
    245
  ],
  "fileinfo.md5": [
    "c279be702893...."
  ],
  "fileinfo.state": [
    "CLOSED"
  ],
  "engine_id.2.id": [
    "0ff95ddb1117d8f36124f6eac406dbbf9f17e3dd89f9bb1bd600f6ad834c25db"
  ],
  "engine_id.3.threat_details": [
    "EICAR-Test-File (not a virus)"
  ],
  "magic_details": [
    "Zip archive data, at least v2.0 to extract"
  ],
```

(suite sur la page suivante)

(suite de la page précédente)

```
  "file_type_description": [
    "ZIP Archive"
  ],
  "timestamp_detected": [
    "2023-10-09T08:23:13.332Z"
  ],
  "engine_id.12.scan_result": [
    "INFECTED"
  ],
  "engine_id.11.scan_result": [
    "INFECTED"
  ],
  "engine_id.13.scan_result": [
    "NOT_SCANNED"
  ],
  "engine_id.14.scan_result": [
    "INFECTED"
  ],
  "engine_id.10.scan_result": [
    "NOT_SCANNED"
  ],
  "proto": [
    "TCP"
  ],
  "analyzed_error": [
    0
  ],
  "engine_id.10.id": [
    "a9b912e461cec506780d8ad8e785cca6b233ad7c72335c262b0a4ab189afa713"
  ],
  "engine_id.2.threat_details": [
    "Unavailable (permanently_failed)"
  ],
  "processing_time": [
    1341
  ],
  "code": [
    1
  ],
  "analyzers_up": [
    16
  ],
  "engine_id.7.id": [
    "527db072abcf877d4bdcd0e9e4ce12c5d769621aa65dd2f7697a3d67de6cc737"
  ],
  "src_ip": [
    "x.x.x.x"
  ],
  "fileinfo.stored": [
    true
  ],
  "engine_id.8.threat_details": [
    "Unavailable (production)"
  ],
  "detail_wait_time": [
    1096
```

(suite sur la page suivante)

(suite de la page précédente)

```
  ],
  "@version": [
    "1"
  ],
  "engine_id.11.id": [
    "ad05e0dc742bcd6251af91bd07ef470c699d5aebbb2055520b07021b14d7380c"
  ],
  "smtp.rcpt_to": [
    "<test@gouv.fr>"
  ],
  "severity": [
    1
  ],
  "engine_id.11.threat_details": [
    "Eicar-Signature"
  ],
  "app_proto": [
    "smtp"
  ],
  "fileinfo.sha256": [
    "4679e7f2018c19..."
  ],
  "fileinfo.magic": [
    "Zip archive data, at least v2.0 to extract"
  ],
  "engine_id.4.id": [
    "32f2f45e6d9faf46e6954356a710208d412fac5181f6c641e34cb9956a133684"
  ],
  "SHA256": [
    "4679e7f2018c19..."
  ],
  "in_iface": [
    "monvirt"
  ],
  "src_port": [
    36746
  ],
  "engine_id.6.threat_details": [
    "EICAR_Test_File"
  ]
 }
}
```

#### 2.1.1.2.3 Malcore log data structure

The logs are composed of different parts:

- The leading part
- The source part defined by "_source"
- The field portion defined by "_fields

#### 2.1.1.2.3.1 The header part of Malcore logs

The header section contains:

```
{
"_index": "malware-2023.10.09-000162",
"_type": "_doc",
"_id": "Dr-PE4sBeBoubSygq3KJ",
"_version": 1,
"_score": 1,
```

Table1: Table header part of Malcore logs

| Fields | Required | Description | Values or example |
|---|---|---|---|
| _index | Yes | Internal index | malware-2023.10.09-000162 |
| _type | Yes | default type | _doc |
| _id | Yes | internal identifier | Dr-PE4sBeBoubSygq3KJ |
| _version | Yes | internal version | 1 |
| _score | Yes | relevance of the response to the request | 1 |

#### 2.1.1.2.3.2 The source part of Malcore logs

The source part defined by "_source" contains:

```
"_source": {
  "proto": "TCP",
  "gcap": "gcap-xxxxxxxxx.domain.local",
  "uuid": "f639c844-3f6f-40fa-86c4-47ff603880e2",
  "host": "gcap-xxxxxxxxx.domain.local",
  "timestamp": "2023-10-09T08:23:13.332538+0000",
  "email": {
    "status": "PARSE_DONE",
    "to": [
      "test@gouv.fr"
    ],
    "attachment": [
      "smtptest-2021-02-24T17-30-01Z.zip"
    ],
    "from": "heartbeat@free.fr"
  },
  "processing_time": 1341,
  "dest_ip": "82.113.11.30",
  "detail_scan_time": 245,
  "src_port": 36746,
  "event_type": "malware",
  "@version": "1",
  "analyzers_up": 16,
  "vlan": [
    3044
  ],
  "analyzed_clean": 0,
  "analyzed_other": 7,
  "file_type_description": "ZIP Archive",
  "timestamp_analyzed": "2023-10-09T08:31:04.503Z",
```

(suite sur la page suivante)

(suite de la page précédente)

```
  "state": "Infected",
  "analyzed_infected": 9,
  "dest_port": 25,
  "engines_last_update_date": "2023-07-11T11:32:00Z",
  "detail_threat_found": "Infected : EICAR-Test-File (not a virus) (B), Virus/EICAR_Test_File,
↪ EICAR-Test-File (not a virus), Eicar test file, EICAR_Test_File, Eicar-Signature, Eicar-
↪Test-Signature, EICAR_Test_File, EICAR-Test-File",
  "magic_details": "Zip archive data, at least v2.0 to extract",
  "total_found": "9/16",
  "detail_wait_time": 1096,
  "timestamp_detected": "2023-10-09T08:23:13.332Z",
  "type": "malcore",
  "code": 1,
  "file_type": "application/zip",
  "smtp": {
    "mail_from": "<heartbeat@free.fr>",
    "rcpt_to": [
      "<test@gouv.fr>"
    ],
    "helo": "gouv.fr"
  },
  "engine_id": {
    "0": {
      "threat_details": "EICAR-Test-File (not a virus) (B)",
      "id": "038e407ba285f0e01dd30c6e4f77ec19bad5ed3dc866a2904ae6bf46baa14b74",
      "scan_result": "INFECTED"
    },
    "1": {
      "threat_details": "Virus/EICAR_Test_File",
      "id": "054a20c51cbe9d2cc7d6a237d6cd4e08ab1a67e170b371e632995766d3ba81af",
      "scan_result": "INFECTED"
    },
    "2": {
      "threat_details": "Unavailable (permanently_failed)",
      "id": "0ff95ddb1117d8f36124f6eac406dbbf9f17e3dd89f9bb1bd600f6ad834c25db",
      "scan_result": "NOT_SCANNED"
    },
    "3": {
      "threat_details": "EICAR-Test-File (not a virus)",
      "id": "312a189607571ec2c7544636be405f10889e73d061e0ed77ca0eca97a470838d",
      "scan_result": "INFECTED"
    },
    "4": {
      "threat_details": "Eicar test file",
      "id": "32f2f45e6d9faf46e6954356a710208d412fac5181f6c641e34cb9956a133684",
      "scan_result": "INFECTED"
    },
    "5": {
      "threat_details": "Unavailable (production)",
      "id": "3bfeb615a695c5ebaac5ade948ffae0c3cfec3787d4625e3abb27fa3c2867f53",
      "scan_result": "NOT_SCANNED"
    },
    "6": {
      "threat_details": "EICAR_Test_File",
      "id": "4ca73ae4b92fd7ddcda418e6b70ced0481ac2d878c48e61b686d0c9573c331dc",
      "scan_result": "INFECTED"
```

(suite sur la page suivante)

(suite de la page précédente)

```
    },
    "7": {
      "threat_details": "Unavailable (production)",
      "id": "527db072abcf877d4bdcd0e9e4ce12c5d769621aa65dd2f7697a3d67de6cc737",
      "scan_result": "NOT_SCANNED"
    },
    "8": {
      "threat_details": "Unavailable (production)",
      "id": "714eca0a6475fe7d2bf9a24bcae343f657b230ff68acd544b019574f1392de77",
      "scan_result": "NOT_SCANNED"
    },
    "9": {
      "threat_details": "Unavailable (production)",
      "id": "95603b80d80fa3e98b6faf07418a55ed0b035d19209e3ad4f1858f6b46fa070a",
      "scan_result": "NOT_SCANNED"
    },
    "10": {
      "threat_details": "Unavailable (production)",
      "id": "a9b912e461cec506780d8ad8e785cca6b233ad7c72335c262b0a4ab189afa713",
      "scan_result": "NOT_SCANNED"
    },
    "11": {
      "threat_details": "Eicar-Signature",
      "id": "ad05e0dc742bcd6251af91bd07ef470c699d5aebbb2055520b07021b14d7380c",
      "scan_result": "INFECTED"
    },
    "12": {
      "threat_details": "Eicar-Test-Signature",
      "id": "af6868a2b87b3388a816e09d2b282629ccf883b763b3691368a27fbd6f6cd51a",
      "scan_result": "INFECTED"
    },
    "13": {
      "threat_details": "Unavailable (production)",
      "id": "b14014e40c0e672e050ad9c210a68a5303ce7facabae9eb2ee07ddf97dc0da0e",
      "scan_result": "NOT_SCANNED"
    },
    "14": {
      "threat_details": "EICAR_Test_File",
      "id": "ecc47e2309be9838d6dc2c5157be1a840950e943f5aaca6637afca11516c3eaf",
      "scan_result": "INFECTED"
    },
    "15": {
      "threat_details": "EICAR-Test-File",
      "id": "fe665976a02d03734c321007328109ab66823b260a8eea117d2ab49ee9dfd3f1",
      "scan_result": "INFECTED"
    }
  },
  "severity": 1,
  "fileinfo": {
    "md5": "c279be702893....",
    "gaps": false,
    "state": "CLOSED",
    "magic": "Zip archive data, at least v2.0 to extract",
    "file_id": 1,
    "sha256": "4679e7f2018c19...",
    "stored": true,
```

(suite sur la page suivante)

(suite de la page précédente)

```
    "filename": "smtptest-2021-02-24T17-30-01Z.zip",
    "sid": [
      1100043
    ],
    "tx_id": 0,
    "size": 51675
  },
  "flow_id": 1016694867777403,
  "gcenter": "gcenter-int-128-dag.gatewatcher.com",
  "SHA256": "4679e7f2018c19...",
  "src_ip": "x.x.x.x",
  "in_iface": "monvirt",
  "analyzed_error": 0,
  "reporting_token": "No GBOX",
  "analyzed_suspicious": 0,
  "app_proto": "smtp",
  "@timestamp": "2023-10-09T08:31:04.503Z"
}
```

Table2: Table source part of Malcore logs

| Fields | Required | Description | Values or example |
|---|---|---|---|
| @timestamp | Yes | Timestamp of the processing of the alert by the GCenter (corresponds to the passage in logstash) | 2023-10-09T08:31:04.503Z |
| @version | yes | version of document | 1 |
| analyzed_clean | yes | Number of engines with CLEAN result | 0 |
| analyzed_error | yes | Number of engines with FAILED, CLEANED or DELETED result | 0 |
| analyzed_infected | Yes | Number of engines with INFECTED result | 9 |
| analyzed_other | yes | Number of engines with result other than CLEAN, INFECTED or SUSPICIOUS | 7 |
| analyzed_suspicious | Yes | Number of engines with SUSPICIOUS result | 0 |
| analyzers_up | Yes | Total number of engines used for analysis | 16 |
| app_proto | Yes | Application protocol of the source stream of the file (http, ftp, smtp, smb)<br>In the case of the http protocol, additional fields are displayed. They are listed in the summary table of counters: category "http" | smtp |

suite sur la page suivante

Table 2 – suite de la page précédente

| Fields | Required | Description | Values or example |
|---|---|---|---|
| code | Yes | malcore analysis return code<br>See the table Malcore engine results | 1 |
| dest_ip (or IP in webui) | Yes | Destination IP address | x.x.x.x |
| dest_port (or PORTs in webui) | No | Port of destination | 25 |
| detail_scan_time (or Scan time in webui) | No | File analysis time (ms) by malcore engines | 245 |
| detail_threat_found ( or Name and Threats found in webui) | Yes | Comma separated list of detected threat names | "Infected: EICAR-Test-File (not a virus) (B).... |
| detail_wait_time | No | Time elapsed between sending the file to the node and receiving the engine result in milliseconds | 1096 |
| Description | yes | Threat description field. Only present in web ui | An adversary can rely on specific actions of a user to obtain execution. . |
| email | Yes | See Summary table of counters: "email" category | NA |
| engine_id<br>- x<br>- id<br>- threat_details<br>- scan_result | No | List of malcore engines that analyzed the file with the associated result<br>- malcore engine number (0 to 15)<br>- id<br>- detail of the threat<br>- analysis result (INFECTED or CLEAN) | - 4<br>- 038e407ba285 f..<br>- EICAR-Test-File (not a virus) (B)<br>- INFECTED |
| engines_last_update_date (or def time in webui) | Yes | Date of last update of malcore engines | 2023-07-11T11:32:00Z |
| event_type | Yes | Event type: used to index an event in logstash. Set to 'malware' | malware |
| file_type | yes | Type of file analyzed | application/zip |
| fileinfo | Yes | Information on the file<br>see Summary table of counters: category "fileinfo" | NA |
| file_type_description | Yes | Description of the file type | ZIP Archive |
| flow_id | Yes | Unique identifier of the flow. Allows to find the associated fileinfo | 1016694867777403 |
| gcap | Yes | Name of the gcap associated with the alert | gcap-xxx.domain.local |
| gcenter | Yes | GCenter name associated with alert | gcenter-xxx.domain.local |
| host | Yes | Name of the equipment associated with the alert | gcap-xxx.domain.local |
| Hostname (webui) | yes | Host name of the threat originator | if the hostname is not present, its IP is displayed |

suite sur la page suivante

Table 2 – suite de la page précédente

| Fields | Required | Description | Values or example |
|---|---|---|---|
| in_iface | yes | GCap input interface used for capture (monx or monvirt) | monvirt |
| magic_details | | Detailed magic information (payload type) | Zip archive data, at least v2.0 to extract |
| MITRE ASSOCIATIONS | yes | Threat MITRE category | Execution |
| processing_time | yes | Analysis processing time | 1341 |
| proto | yes | Protocol detected by Sigflow | TCP |
| reporting_token | Yes | Token used with GBox<br>If no GBox then message NO GBOX | GBOX# |
| severity | Yes | Analysis result code. | Between 0 and 3.<br>0=clean, 1=infected, 2=suspicious, 3=Other |
| SHA256 | Yes | SHA256 hash of the analyzed file. | 4679e7f2018c19... |
| smtp | Yes | Category smtp detailed below | |
| src_ip (or IP in webui) | Yes | Source IP address detected by Sigflow | X.X.X.X |
| src_port (or PORTs in webui) | Yes | Source port detected by Sigflow | 36746 |
| state | Yes | Malcore engine analysis result<br>Result is "Infected" as soon as the result of an engine is "Infected" | Infected |
| timestamp | Yes | Timestamp of the processing of the alert by the GCenter (corresponds to the passage in logstash) | 2023-10-09T08:23:13.332538+0000 |
| timestamp analyzed | Yes | Date and time of last file scan | 2023-10-09T08:31:04.503Z |
| timestamp detected | Yes | Timestamp of file capture by Gcap | 2023-10-09T08:23:13.332Z |
| total_found | Yes | Number of engines that detected the file as infected divided by the total number of engines | XX/YY with YY between 0 and 16 and XX between 0 and YY; example 9/16 |
| type | Yes | Type of event | Malcore or malcore_retroanalyzer |
| uuid or id | Yes | Unique identifier of the alert | f639c844-3f6f-40fa-86c4-47ff603880e2 |
| vlan | No | Vlan number | 3044 |

Table3: Malcore engine results. are valid only for Malcore configuration at the time of analysis

| Return code | Result | Description |
|---|---|---|
| 0 | No Threat Detected | File was analyzed and declared healthy |
| 1 | Infected | File was scanned and declared infected |

suite sur la page suivante

Table 3 – suite de la page précédente

| Return code | Result | Description |
|---|---|---|
| 2 | Suspicious | The file was analyzed and declared as likely to be infected: some Malcore engines have detected this file as malicious.. |
| 3 | Failed Scan | An error occurred during the run. |
| 7 | Skipped - Whitelisted | The file is not analyzed and considered healthy since this file is defined in the Malcore whitelist |
| 8 | Skipped – Blacklisted | The file is not scanned and considered infected since this file is defined in the Malcore blacklist |
| 9 | Exceeded Archive Depth | The number of times the file is compressed is limited (max recursion level). The message indicates that the defined value has been exceeded. |
| 10 | Not scanned | Engine not available at time of run |
| 12 | Encrypted Archive | The archive is encrypted and therefore not parsable: the password indicated does not work |
| 13 | Exceeded Archive Size | The maximum file size should not exceed the defined value (maximum value 10MB). The analyzed archive is larger than the value set |
| 14 | Exceeded Archive File Number | The maximum number of files in the archive must not exceed the defined value. The analyzed archive contains a number of files greater than the defined value |
| 15 | Password Protected Document | Solution detected inconsistent behavior with password protected document |
| 16 | Exceeded Archive Timeout | The archive scan time has been exceeded, Malcore engines are not responding within the deadline |
| 17 | Filetype Mismatch | File type mismatch problem: the solution detects the file extension with its contents and compares it with the file extension displayed |
| 18 | Potentially Vulnerable File | Potentially vulnerable files are files associated with identified vulnerable components or applications |
| 19 | Cancelled | User explicitly canceled this file analysis request |
| 21 | Yara Rule Matched | The verdict of the result is: a Yara rule matches (malware sample identification) |
| 22 | Potentially Unwanted | Solution detected potentially unwanted applications |
| 23 | Unsupported File Type | File type not supported by the solution |
| 255 | In Progress | Analysis in progress.. |

Table4: Summary table of counters: «email» category

| Field | Required | Description | Values or example |
|---|---|---|---|
| status | Yes | Status of mail | PARSE_DONE |
| for | Yes | Mail recipient | test@gouv.fr |
| attachment | Yes | Content attached document | smtptest-2021-02-24T17-30-01Z.zip |
| of | Yes | Mailer | heartbeat@free.fr |

Table5: Summary table of counters: category "smtp"

| Field | Required | Description | Values or example |
|---|---|---|---|
| mail_from | Yes | Mailer | heartbeat@free.fr |
| rcpt_to | Yes | Mail recipient | test@gouv.fr |
| helo | Yes | Domain name | gouv.fr |

Table6: Summary table of counters: category "fileinfo"

| Field | Required | Description | Values or example |
|---|---|---|---|
| file_id | Yes | File ID | 1 |
| filename | Yes | File name | smtptest-2021-02-24T17-30-01Z.zip |
| gaps | Yes | Monitoring inconsistency in file size | false |
| magic | Yes | File format identifier (Magic signature): detected by Sigflow using a reduced database. | Zip archive data, at least v2.0 to extract |
| md5 | Yes | MD5 hash of the analyzed file | c279be702893.... |
| sha256 | Yes | SHA256sum of the analyzed file | 4679e7f2018c19... |
| sid | yes | Alert ID. Must be unique. | 1100043 |
| size | Yes | File size | 51675 |
| state | Yes | Completeness of the analyzed file (CLOSED) otherwise TRUNCATED.<br>The Sigflow file-store.stream-depth variable defines the size of the reconstructed files.<br>The file is TRUNCATED if its size is > File-store stream depth (10 MB) by default. | CLOSED |
| stored | Yes | Still at "true", the file was stored on disk for further analysis | true |
| tx_id | Yes | transaction identification (query/response pair) | 1 |
| fileinfo_potentially _involved | No | This field appears only in the case of retroact<br>it indicates the list of _doc id of less than 24 hours that are concerned by the rescan | 1 |

Table7: Summary table of counters: category "http"

| Field | Required | Description | Values or example |
|---|---|---|---|
| hostname | yes | Host name to which this HTTP event is assigned | synonymi.justdance.com |
| http_content_type | yes | Type of data returned (for example application/x-gzip) | application/x-shockwave-flash |
| http_method | yes | HTTP method (ex: GET, POST, HEAD) | GET |
| http_user_agent | yes | The user agent of the software used | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; ...) |
| length | yes | HTTP body content size | 77068 |
| protocol | yes | Protocol / HTTP version (ex: HTTP/1.1) | HTTP/1.1 |
| status | yes | HTTP status code | 200 |
| url | yes | URL of host name accessed | /6SuCHKKkf8Sf1aFXJPqD0R6r... |

#### 2.1.1.2.3.3 The fields part of Malcore logs

The field part defined by "fields" contains the same fields as in the source part: refer to the source part section.

---

### 2.1.1.3 View the status of Malcore

The current state of the motor is displayed in *Web UI `Health checks` screen*.
The visible information is:

- The status and status of each engine included in Malcore
- The latest update of each of them

---

### 2.1.1.4 Update of malcore

There are updates (Updates) for the Gmalcore engine.
These updates can be done manually or scheduled via GUM.
See *Presentation of GUM: dedicated module for managing updates* and in particular *Update signatures and/or engines (update)*.

---

### 2.1.1.5 Gmalcore status and configuration

The management interface enables:

- To modify the engine parameters: see the *Setting up GBox and the Malcore and Retroact engines and activate the GBox* procedure.
- Manage hash256 fingerprint lists to declare that the files are:

- Healthy (for whitelist)
- Is compromised (for blacklist)

For more information on these lists, see the procedure in *Managing the white and black lists of the Malcore engine*.
The management interface is described in *`Admin-GCenter- Malcore Management` screen of the legacy web UI*.

---

## 2.1.2 Codebreaker Engine

### 2.1.2.1 Presentation

The Codebreaker engine enables detecting both *Shellcode* and *Powershell*.
This is accomplished through the following features:

- The detection of exploitative techniques that are offensive, discrete, and sophisticated
- De-encoding of encrypted payloads

- Detection of polymorphic shellcodes

**Note:**

Codebreaker detects shellcodes for 32 and 64 bit Windows and Linux platforms.

---

#### 2.1.2.2 Events generated

Events generated by Codebreaker include *Shellcode*` or *Powershell* alerts.
These are displayed in the main interface of the GCenter as well as in Kibana.
From the main interface, it is possible to download the source files.

- in the main interface named **WEB UI** of the GCenter in the `` `Alerts` `` screen (the main interface named **WEB UI** is described in *Overview of the WEB UI*).

  To view alerts, select the SHELLCODE filter and view the list of alerts: see the presentation of *Web UI `Alerts` screen*.

  By clicking on an alert, the detailed information of this alert is displayed:
  - See *Codebreaker Shellcode* for Shellcode Codebreaker
  - See *Codebreaker Powershell* for Powershell Codebreaker
- In the **Kibana UI** interface: for this

  To view alerts, select the SHELLCODE filter and view the list of alerts: see the presentation of *Web UI `Alerts` screen*.

  By clicking on an alert, select on the command `` `Go hunting` `` then select the arrow to the left of the alert.

  The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

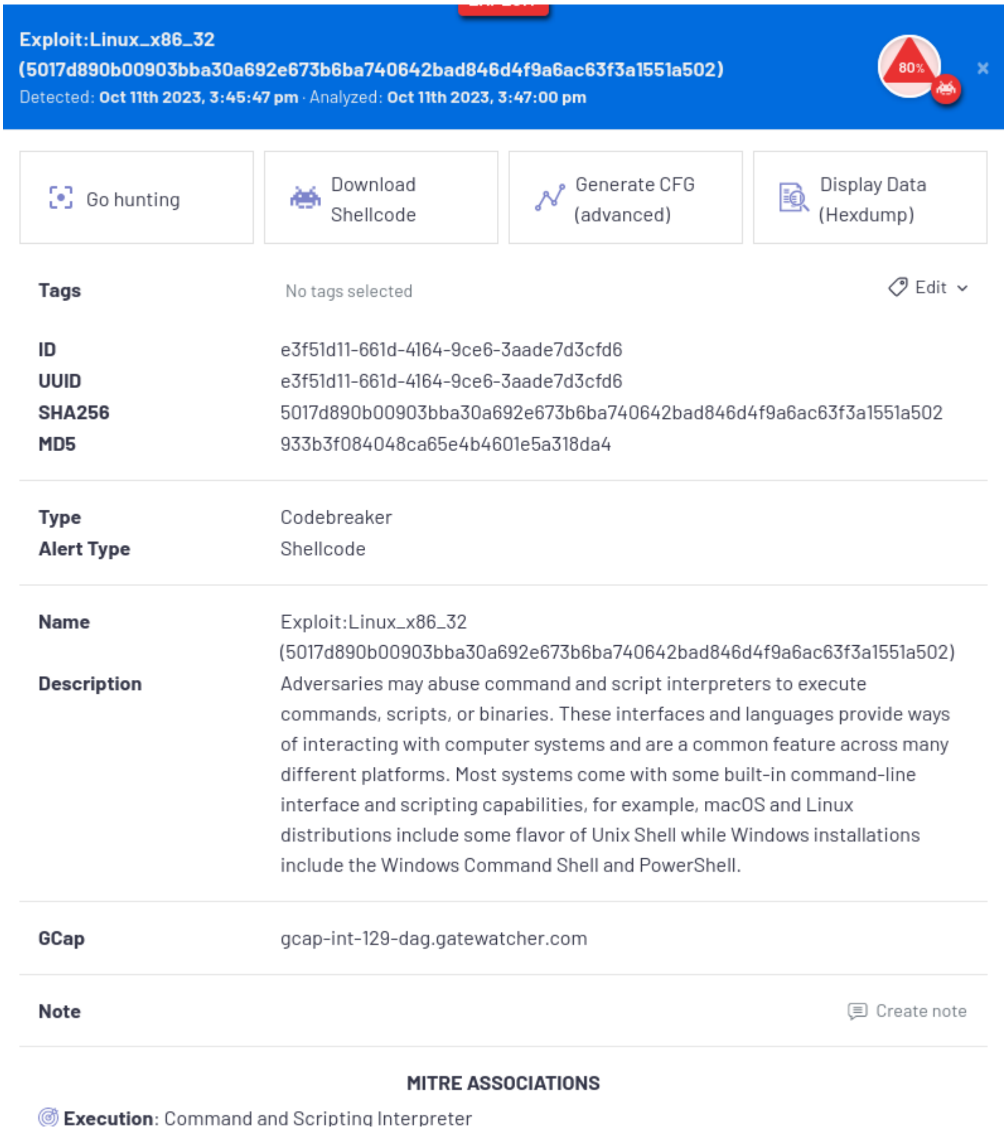
  The detailed information of this alert can be viewed in table or jason format.

  The detailed information of this alert is displayed:
  - See *Codebreaker Shellcode* for Shellcode Codebreaker
  - See *Codebreaker Powershell* for Powershell Codebreaker

---

### 2.1.2.2.1 Codebreaker Shellcode

#### 2.1.2.2.1.1 Example of a Codebreaker Shellcode alert in the webui



Exploit:Linux_x86_32
(5017d890b00903bba30a692e673b6ba740642bad846d4f9a6ac63f3a1551a502)
Detected: Oct 11th 2023, 3:45:47 pm · Analyzed: Oct 11th 2023, 3:47:00 pm

Tags No tags selected

ID e3f51d11-661d-4164-9ce6-3aade7d3cfd6
UUID e3f51d11-661d-4164-9ce6-3aade7d3cfd6
SHA256 5017d890b00903bba30a692e673b6ba740642bad846d4f9a6ac63f3a1551a502
MD5 933b3f084048ca65e4b4601e5a318da4

Type Codebreaker
Alert Type Shellcode

Name Exploit:Linux_x86_32 (5017d890b00903bba30a692e673b6ba740642bad846d4f9a6ac63f3a1551a502)
Description Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

GCap gcap-int-129-dag.gatewatcher.com

Note

MITRE ASSOCIATIONS

**Execution**: Command and Scripting Interpreter

The counters are detailed in *Codebreaker Shellcode log data structure*.

#### 2.1.2.2.1.2 Example of a Codebreaker Shellcode log

```
{
 "_index": "codebreaker-2023.10.11-000164",
 "_type": "_doc",
 "_id": "kAP9HosBeBoubSygpAwN",
 "_version": 1,
 "_score": 1,
 "_source": {
   "encodings": [
     {
       "options": "EBX, 3, Mixed",
```

(suite sur la page suivante)

(suite de la page précédente)

```
      "count": 1,
      "name": "Alpha"
    }
  ],
  "gcap": "gcap-xxxxxxxxx.domain.local",
  "state": "Exploit",
  "uuid": "e3f51d11-661d-4164-9ce6-3aade7d3cfd6",
  "timestamp_analyzed": "2023-10-11T13:47:00.895Z",
  "dest_port": "37644",
  "type": "codebreaker",
  "timestamp_detected": "2023-10-11T13:45:47.655Z",
  "dest_ip": "X.X.X.X",
  "src_port": "4242",
  "event_type": "shellcode",
  "MD5": "933b3f084048ca6...",
  "severity": 1,
  "@version": "1",
  "calls": {
    "0": {
      "ret": "0",
      "args": "{'filename': 'THIS IS SP... SHELLCODE !', 'argv': ['THIS IS SP... SHELLCODE !'], 'envp': []}",
      "call": "sys_execve"
    },
    "stop": "End of shellcode (Exit)"
  },
  "flow_id": "2046395805270250",
  "gcenter": "gcenter-xxx.domain.local",
  "SHA256": "5017d890b00903bba30a692e673b6ba740642bad846d4f9a6ac63f3a1551a502",
  "file_id": "10-11-2023T13:46:56_b2b0c75...9c_gcap-xxxxxxxxx.domain.local",
  "src_ip": "X.X.X.X",
  "sub_type": "Linux_x86_32",
  "@timestamp": "2023-10-11T13:47:00.895Z"
},
"fields": {
  "calls.0.ret": [
    "0"
  ],
  "calls.stop": [
    "End of shellcode (Exit)"
  ],
  "type": [
    "codebreaker"
  ],
  "uuid": [
    "e3f51d11-661d-4164-9ce6-3aade7d3cfd6"
  ],
  "calls.0.args": [
    "{'filename': 'THIS IS SP... SHELLCODE !', 'argv': ['THIS IS SP... SHELLCODE !'], 'envp': []}"
  ],
  "calls.0.call": [
    "sys_execve"
  ],
  "src_ip": [
    "X.X.X.X"
```

(suite sur la page suivante)

(suite de la page précédente)

```
    ],
    "event_type": [
      "shellcode"
    ],
    "sub_type": [
      "Linux_x86_32"
    ],
    "flow_id": [
      2046395805270250
    ],
    "@version": [
      "1"
    ],
    "state": [
      "Exploit"
    ],
    "dest_port": [
      37644
    ],
    "severity": [
      1https://10.2.19.128/ui/home/main
    ],
    "gcenter": [
      "gcenter-xxx.domain.local"
    ],
    "timestamp_detected": [
      "2023-10-11T13:45:47.655Z"
    ],
    "SHA256": [
      "5017d890b00903bba30a692e673b6ba740642bad846d4f9a6ac63f3a1551a502"
    ],
    "src_port": [
      4242
    ],
    "@timestamp": [
      "2023-10-11T13:47:00.895Z"
    ],
    "dest_ip": [
      "X.X.X.X"
    ],
    "file_id": [
      "10-11-2023T13:46:56_b2b0c75...9c_gcap-xxxxxxxxx.domain.local"
    ],
    "encodings.count": [
      1
    ],
    "gcap": [
      "gcap-xxxxxxxxx.domain.local"
    ],
    "timestamp_analyzed": [
      "2023-10-11T13:47:00.895Z"
    ],
    "encodings.options": [
      "EBX, 3, Mixed"
    ],
    "encodings.name": [
```

(suite sur la page suivante)

(suite de la page précédente)

```
     "Alpha"
   ],
   "MD5": [
     "933b3f084048ca6..."
   ]
 }
}
```

#### 2.1.2.2.1.3 Codebreaker Shellcode log data structure

The logs are composed of different parts:

- The leading part
- The source part defined by "_source"
- The field portion defined by "_fields"

#### 2.1.2.2.1.4 The header part of the Codebreaker Shellcode logs

The header section contains:

```
{
 "_index": "codebreaker-2023.10.11-000164",
 "_type": "_doc",
 "_id": "kAP9HosBeBoubSygpAwN",
 "_version": 1,
 "_score": 1,
```

Table8: Table part header

| Field | Required | Description | Values or example |
|---|---|---|---|
| _index | Yes | Internal index | codebreaker-2023.10.11-000164 |
| _type | Yes | default type | _doc |
| _id | Yes | internal identifier | kAP9HosBeBoubSygpAwN |
| _version | Yes | internal version | 1 |
| _score | Yes | relevance of the response to the request | 1 |

#### 2.1.2.2.1.5 The source part of the Codebreaker Shellcode logs

The source part defined by "_source" contains:

```
"_source": {
  "encodings": [
    {
      "options": "EBX, 3, Mixed",
      "count": 1,
      "name": "Alpha"
    }
```

(suite sur la page suivante)

(suite de la page précédente)

```
  ],
  "gcap": "gcap-xxxxxxxxx.domain.local",
  "state": "Exploit",
  "uuid": "e3f51d11-661d-4164-9ce6-3aade7d3cfd6",
  "timestamp_analyzed": "2023-10-11T13:47:00.895Z",
  "dest_port": "37644",
  "type": "codebreaker",
  "timestamp_detected": "2023-10-11T13:45:47.655Z",
  "dest_ip": "X.X.X.X",
  "src_port": "4242",
  "event_type": "shellcode",
  "MD5": "933b3f084048ca6...",
  "severity": 1,
  "@version": "1",
  "calls": {
    "0": {
      "ret": "0",
      "args": "{'filename': 'THIS IS SP... SHELLCODE !', 'argv': ['THIS IS SP... SHELLCODE !
↪'], 'envp': []}",
      "call": "sys_execve"
    },
    "stop": "End of shellcode (Exit)"
  },
  "flow_id": "2046395805270250",
  "gcenter": "gcenter-xxx.domain.local",
  "SHA256": "5017d890b00903bba30a692e673b6ba740642bad846d4f9a6ac63f3a1551a502",
  "file_id": "10-11-2023T13:46:56_b2b0c75...9c_gcap-xxxxxxxxx.domain.local",
  "src_ip": "X.X.X.X",
  "sub_type": "Linux_x86_32",
  "@timestamp": "2023-10-11T13:47:00.895Z"
},
```

Table9: Table part source

| Field | Required | Description | Values or example |
|---|---|---|---|
| @timestamp | Yes | Timestamp analyzed | 2023-10-11T13:47:00.895Z |
| @version | yes | version of document | 1 |
| calls | Yes | Category calls see the summary table of the counters in the category "calls" | |
| dest_ip | Yes | Destination IP address | x.x.x.x |
| Description (in webui) | yes | Threat description field. Only present in web ui | adversaries may abuse command and script interpreters to execute commands, scripts or binaries... |
| dest_port | No | Port of destination | 37644 |
| encodings | yes | Category encodings see Summary table of counters in category "Encodings" | 1 |
| event_type (Alert type in webui) | Yes | Type of exploit | shellcode |
| file_id | Yes | Fileinfo category: File ID | 0-11-2023T13:46:56_b2b0c75...9c_gcap-xxxxxxxxx.domain.local |
| flow_id | Yes | Unique identifier of the flow. Allows to find the associated fileinfo | 2046395805270250 |

suite sur la page suivante

Table 9 – suite de la page précédente

| Field | Required | Description | Values or example |
|---|---|---|---|
| gcap | Yes | Name of the gcap associated with the alert | gcap-xxx.domain.local |
| gcenter | Yes | GCenter name associated with alert. | gcenter-xxx.domain.local |
| Hostname (webui) | yes | Host name of the threat originator | If the hostname is not present, its IP is displayed |
| MD5 | Yes | MD5 hash of the analyzed file | 933b3f084048ca6... |
| MITRE ASSOCIATIONS | yes | Threat MITRE category | Execution |
| Name in webui | Yes | sum of state + sub_type + MD5 + SHA256 field information | Execution: Command and Scripting Interpreter<br>Persistence: Hijack Execution Flow<br>Privilege Escalation: Hijack Execution Flow<br>Defense Evasion: Hijack Execution Flow |
| severity | Yes | Analysis result code. | Between 0 and 3.<br>0=clean, 1=infected, 2=suspicious, 3=Other |
| SHA256 | Yes | SHA256 hash of the analyzed file | 5017d890b00903bb... |
| src_ip | Yes | Source IP address | X.X.X.X |
| src_port | Yes | Source port | 4242 |
| state | Yes | Result of codebreaker analysis (Exploit, Suspicious) | Exploit |
| sub_type | Yes | The file subtype (Windows_x86_32, Linux_x86_32)<br>The operating system linked to the executable if it is a shellcode. | Linux_x86_32 |
| timestamp analyzed | Yes | Date and time of last file scan | 2023-10-11T13:47:00.895Z |
| timestamp detected | Yes | Date and time of first file capture | 2023-10-11T13:45:47.655Z |
| type | Yes | Type of event | codebreaker |
| uuid or id | Yes | Unique identifier of the alert | e3f51d11-661d-4164-9ce6-3aade7d3cfd6 |

Table10: Summary table of counters in the category "calls"

| Field | Required | Description | Values or example |
|---|---|---|---|
| return | Yes | System call return code used | 0 |
| args | Yes | Arguments of the system call used | {'filename': 'THIS IS SP... SHELLCODE!', 'argv': ['THIS IS SP... SHELLCODE! '], 'envp': []} |
| call | Yes | Name of system call used | sys_execve |
| stop | Yes | Marks the end of shellcode (End of shellcode) | End of shellcode (output) |

suite sur la page suivante

Table 10 – suite de la page précédente

| Field | Required | Description | Values or example |
|---|---|---|---|
| index | yes | Internal index | 0 |

Table11: Summary table of counters in the category "Encodings"

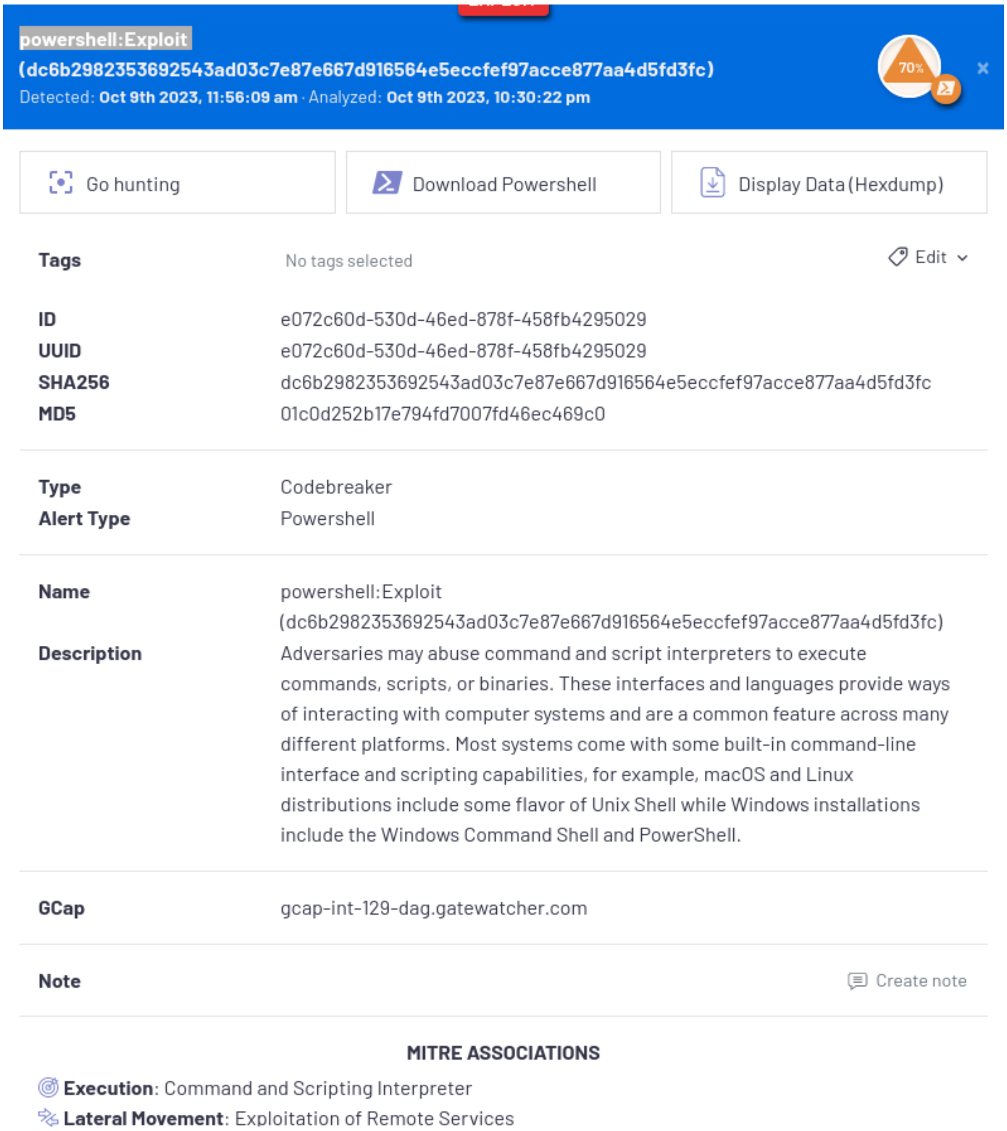
| Field | Required | Description | Values or example |
|---|---|---|---|
| encodings.compter | yes | Number of successive encodings f | 1 |
| encodings.name | yes | Encoding name | 1 |
| encodings.options | yes | Encoding options | EBX, 3, mixed |

#### 2.1.2.2.1.6 The fields part of the Codebreaker Shellcode logs

The field part defined by "fields" contains the same counters as in the source part: refer to the source part section

#### 2.1.2.2.2 Codebreaker Powershell

##### 2.1.2.2.2.1 Example of a Codebreaker Powershell alert in the webui



powershell:Exploit
(dc6b2982353692543ad03c7e87e667d916564e5eccfef97acce877aa4d5fd3fc)
Detected: **Oct 9th 2023, 11:56:09 am** · Analyzed: **Oct 9th 2023, 10:30:22 pm**

| | |
|---|---|
| **Tags** | No tags selected |
| **ID** | e072c60d-530d-46ed-878f-458fb4295029 |
| **UUID** | e072c60d-530d-46ed-878f-458fb4295029 |
| **SHA256** | dc6b2982353692543ad03c7e87e667d916564e5eccfef97acce877aa4d5fd3fc |
| **MD5** | 01c0d252b17e794fd7007fd46ec469c0 |
| **Type** | Codebreaker |
| **Alert Type** | Powershell |
| **Name** | powershell:Exploit (dc6b2982353692543ad03c7e87e667d916564e5eccfef97acce877aa4d5fd3fc) |
| **Description** | Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell. |
| **GCap** | gcap-int-129-dag.gatewatcher.com |
| **Note** | |

**MITRE ASSOCIATIONS**

**Execution**: Command and Scripting Interpreter
**Lateral Movement**: Exploitation of Remote Services

The counters are detailed in *Codebreaker Powershell log data structure*.

##### 2.1.2.2.2.2 Codebreaker Powershell log example

```
{
 "_index": "codebreaker-2023.10.11-000164",
 "_type": "_doc",
 "_id": "EAP8HosBeBoubSygnQy_",
 "_version": 1,
 "_score": 1,
 "_source": {
   "gcap": "gcap-xxxxxxxxx.domain.local",
   "event_type": "powershell",
   "state": "Exploit",
```

(suite sur la page suivante)

(suite de la page précédente)

```
    "severity": 1,
    "MD5": "01c0d252b17e794fd7007fd46ec469c0",
    "@version": "1",
    "flow_id": "2061844798658535",
    "scores": {
      "proba_obfuscated": 1,
      "analysis_detailed": {
        "FmtStr": 198,
        "StrReplace": 0,
        "StartBitsTransfer": 0,
        "GetContent": 0,
        "CharInt": 16,
        "InvokeExpression": 0,
        "WebClientInvokation": 0,
        "StreamWriter": 0,
        "AddContent": 0,
        "StrJoin": 0,
        "StreamReader": 0,
        "SystemIOFile": 0,
        "InvokeWebRequest": 0,
        "InvokeRestMethod": 0,
        "Base64": 0,
        "StrCat": 28,
        "SetContent": 0
      },
      "analysis": 242
    },
    "dest_port": "57244",
    "SHA256": "dc6b2982353692543ad03c7e87e667d916564e5eccfef97acce877aa4d5fd3fc",
    "uuid": "9a1333a3-e864-478e-88ae-f9823623dfec",
    "file_id": "10-11-2023T13:45:46...32_gcap-xxxxxxxxx.domain.local",
    "type": "codebreaker",
    "src_ip": "X.X.X.X",
    "timestamp_analyzed": "2023-10-11T13:45:53.836Z",
    "timestamp_detected": "2023-10-11T13:44:46.022Z",
    "gcenter": "gcenter-xxx.domain.local",
    "dest_ip": "X.X.X.X",
    "sub_type": "powershell",
    "src_port": "4242",
    "@timestamp": "2023-10-11T13:45:53.836Z"
  },
  "fields": {
    "scores.analysis_detailed.SystemIOFile": [
      0
    ],
    "scores.analysis_detailed.Base64": [
      0
    ],
    "scores.analysis_detailed.StreamWriter": [
      0
    ],
    "type": [
      "codebreaker"
    ],
    "uuid": [
      "9a1333a3-e864-478e-88ae-f9823623dfec"
```

(suite sur la page suivante)

(suite de la page précédente)

```
  ],
  "scores.analysis_detailed.WebClientInvokation": [
    0
  ],
  "src_ip": [
    "X.X.X.X"
  ],
  "scores.analysis_detailed.StrReplace": [
    0
  ],
  "event_type": [
    "powershell"
  ],
  "scores.analysis_detailed.InvokeRestMethod": [
    0
  ],
  "sub_type": [
    "powershell"
  ],
  "flow_id": [
    2061844798658535
  ],
  "@version": [
    "1"
  ],
  "state": [
    "Exploit"
  ],
  "dest_port": [
    57244
  ],
  "scores.analysis_detailed.InvokeWebRequest": [
    0
  ],
  "severity": [
    1
  ],
  "scores.analysis_detailed.FmtStr": [
    198
  ],
  "scores.analysis_detailed.StreamReader": [
    0
  ],
  "gcenter": [
    "gcenter-xxx.domain.local"
  ],
  "scores.analysis_detailed.SetContent": [
    0
  ],
  "scores.proba_obfuscated": [
    1
  ],
  "timestamp_detected": [
    "2023-10-11T13:44:46.022Z"
  ],
  "scores.analysis_detailed.GetContent": [
```

(suite sur la page suivante)

(suite de la page précédente)

```
     0
   ],
   "SHA256": [
     "dc6b2982353692543ad03c7e87e667d916564e5eccfef97acce877aa4d5fd3fc"
   ],
   "src_port": [
     4242
   ],
   "scores.analysis_detailed.StrCat": [
     28
   ],
   "@timestamp": [
     "2023-10-11T13:45:53.836Z"
   ],
   "scores.analysis_detailed.AddContent": [
     0
   ],
   "dest_ip": [
     "X.X.X.X"
   ],
   "file_id": [
     "10-11-2023T13:45:46...32_gcap-xxxxxxxxx.domain.local"
   ],
   "scores.analysis_detailed.StrJoin": [
     0
   ],
   "scores.analysis_detailed.InvokeExpression": [
     0
   ],
   "gcap": [
     "gcap-xxxxxxxxx.domain.local"
   ],
   "timestamp_analyzed": [
     "2023-10-11T13:45:53.836Z"
   ],
   "scores.analysis": [
     242
   ],
   "scores.analysis_detailed.StartBitsTransfer": [
     0
   ],
   "scores.analysis_detailed.CharInt": [
     16
   ],
   "MD5": [
     "01c0d252b17e794fd7007fd46ec469c0"
   ]
 }
}
```

#### 2.1.2.2.2.3 Codebreaker Powershell log data structure

The logs are composed of different parts:

- The leading part
- The source part defined by "_source"
- The field portion defined by "_fields"

---

#### 2.1.2.2.2.4 The header part of the Codebreaker Powershell logs

The header section contains:

```
{
 "_index": "codebreaker-2023.10.11-000164",
 "_type": "_doc",
 "_id": "EAP8HosBeBoubSygnQy",
 "_version": 1,
 "_score": 1,
```

Table12: Table part header

| Field | Required | Description | Values or example |
|---|---|---|---|
| _index | Yes | Internal index | codebreaker-2023.10.11-000164 |
| _type | Yes | default type | _doc |
| _id | Yes | internal identifier | EAP8HosBeBoubSygnQy |
| _version | Yes | internal version | 1 |
| _score | Yes | relevance of the response to the request | 1 |

---

#### 2.1.2.2.2.5 The source part of the Codebreaker Powershell logs

The source part defined by "_source" contains:

```
 "_source": {
  "gcap": "gcap-xxxxxxxxx.domain.local",
  "event_type": "powershell",
  "state": "Exploit",
  "severity": 1,
  "MD5": "01c0d252b17e794fd7007fd46ec469c0",
  "@version": "1",
  "flow_id": "2061844798658535",
  "scores": {
    "proba_obfuscated": 1,
    "analysis_detailed": {
      "FmtStr": 198,
      "StrReplace": 0,
      "StartBitsTransfer": 0,
      "GetContent": 0,
      "CharInt": 16,
      "InvokeExpression": 0,
      "WebClientInvokation": 0,
      "StreamWriter": 0,
```

(suite sur la page suivante)

(suite de la page précédente)

```
      "AddContent": 0,
      "StrJoin": 0,
      "StreamReader": 0,
      "SystemIOFile": 0,
      "InvokeWebRequest": 0,
      "InvokeRestMethod": 0,
      "Base64": 0,
      "StrCat": 28,
      "SetContent": 0
    },
    "analysis": 242
  },
  "dest_port": "57244",
  "SHA256": "dc6b2982353692543ad03c7e87e667d916564e5eccfef97acce877aa4d5fd3fc",
  "uuid": "9a1333a3-e864-478e-88ae-f9823623dfec",
  "file_id": "10-11-2023T13:45:46...32_gcap-xxxxxxxxx.domain.local",
  "type": "codebreaker",
  "src_ip": "X.X.X.X",
  "timestamp_analyzed": "2023-10-11T13:45:53.836Z",
  "timestamp_detected": "2023-10-11T13:44:46.022Z",
  "gcenter": "gcenter-xxx.domain.local",
  "dest_ip": "X.X.X.X",
  "sub_type": "powershell",
  "src_port": "4242",
  "@timestamp": "2023-10-11T13:45:53.836Z"
},
```

Table13: Table source part of Codebreaker Powershell logs

| Field | Required | Description | Values or example |
|---|---|---|---|
| gcap | Yes | Name of the gcap associated with the alert | gcap-xxx.domain.local |
| event_type | Yes | Type of exploit | powershell |
| state | Yes | Result of codebreaker analysis (Exploit, Suspicious) | Exploit |
| severity | Yes | Analysis result code | Between 0 and 3<br>0=clean, 1=infected, 2=suspicious, 3=Other |
| MD5 | Yes | MD5 hash of the analyzed file | 01c0d252b17e794fd7007fd46ec469c0 |
| @version | yes | version of document | 1 |
| flow_id | Yes | Unique identifier of the flow. Allows to find the associated fileinfo | 2061844798658535 |
| scores | Yes | See "Scores" category counter summary table | |
| dest_port | Yes | Port of destination | 57244 |
| SHA256 | Yes | SHA256 hash of the analyzed file | dc6b2982353692543ad03c7e87e667... |
| uuid | Yes | Unique identifier of the alert | 9a1333a3-e864-478e-88ae-f9823623dfec |
| file_id | Yes | Fileinfo category: File ID | 10-11-2023T13:45:46...32_gcap-xxxxxxxxx.domain.local |
| type | Yes | Type of event | codebreaker |
| src_ip | Yes | Source IP address | X.X.X.X |

suite sur la page suivante

Table 13 – suite de la page précédente

| Field | Required | Description | Values or example |
|---|---|---|---|
| timestamp analyzed | Yes | Date and time of last file scan | 2023-10-11T13:45:53.836Z |
| timestamp detected | Yes | Date and time of first file capture | 2023-10-11T13:44:46.022Z |
| gcenter | Yes | GCenter name associated with alert. | gcenter-xxx.domain.local |
| dest_ip | Yes | Destination IP address | x.x.x.x |
| sub_type | Yes | The file subtype | powershell |
| src_port | Yes | Source port | 4242 |
| @timestamp | Yes | Timestamp analyzed | 2023-10-11T13:45:53.836Z |

Table14: Summary table of "scores" category counters

| Field | Required | Description | Values or example |
|---|---|---|---|
| proba_obfuscated | Yes | Probability that the powershell is offended. Value between 0 and 1 | 1 |
| analysis_detailed | Yes | detailed analysis. It includes the following meters: | |
| FmtStr | Yes | Category scores/analysis_detailed<br>Score represented by an integer of a/of detected fmtstr patterns | 198 |
| StrReplace | Yes | Category scores/analysis_detailed<br>Score represented by an integer of a/strreplace patterns detected | 0 |
| StartBitsTransfer | Yes | Category scores/analysis_detailed<br>Start-BitsTransfer Order | 0 |
| GetContent | Yes | Category scores/analysis_detailed<br>Get-Content applet to read file data | 0 |
| CharInt | Yes | Category scores/analysis_detailed<br>Score represented by an integer of one/of the detected charitable patterns | 16 |
| InvokeExpression | Yes | Category scores/analysis_detailed<br>InvokeExpression Applet | 0 |
| WebClientInvokation | Yes | Category scores/analysis_detailed<br>Score represented by an integer of one/of detected webclientinvokation patterns | 0 |

suite sur la page suivante

Table 14 – suite de la page précédente

| Field | Required | Description | Values or example |
|---|---|---|---|
| StreamWriter | Yes | Category scores/analysis_detailed<br>Write a file that lists directories | 0 |
| AddContent | Yes | Category scores/analysis_detailed<br>Adds content to a file/folder | 0 |
| StrJoin | Yes | Category scores/analysis_detailed<br>Score represented by an integer of a/strjoin patterns detected | 0 |
| StreamReader | Yes | Category scores/analysis_detailed<br>Object to read and display each directory name | 0 |
| SystemIOFile | Yes | Category scores/analysis_detailed<br>Manipulation of a file (creation, opening, copy, etc.) | 0 |
| InvokeWebRequest | Yes | Category scores/analysis_detailed<br>Invoke-WebRequest applet sends HTTP and HTTPS requests to a webpage | 0 |
| Base64 | Yes | Category scores/analysis_detailed<br>Score represented by an integer of a/patterns base64 detected | 0 |
| StrCat | Yes | Category scores/analysis_detailed<br>Function that concatenates strings | 28 |
| SetContent | Yes | Category scores/analysis_detailed<br>Applet SetContent writes new content or replaces existing content in a file | 0 |
| analysis | Yes | Category scores | 242 |

##### 2.1.2.2.2.6 The fields part of the Codebreaker Powershell logs

The field part defined by "fields" contains the same counters as in the source part: refer to the source part section

---

#### 2.1.2.3 Viewing the status of Codebreaker

The current state of the motor is displayed in *Web UI `Health checks` screen*.

---

#### 2.1.2.4 Codebreaker update

The engine is updated with each new version of the GCenter.

---

#### 2.1.2.5 Codebreaker Configuration

The engine is not configurable.

Shellcode and powershell detection is not enabled by default and is defined in the profiles sent to GCap (*Web UI `Config - Gcaps profiles` screen*).

---

### 2.1.3 Sigflow engine

#### 2.1.3.1 Presentation

The Sigflow engine analyses all network traffic and can, according to the **rules**, generate alerts, metadata, and content.

Coming from different sources, these rules must describe the characteristics of the attacks to be detected as well as being optimised to reduce false positives.

The GCenter enables compiling several sources, thus several rule sets to create a specific file called **Ruleset** that will then be transferred to the Sigflow engine in the GCap.

---

#### 2.1.3.2 Organizing the rules

The rules sent to the Sigflow engine are organized as follows:

- A list of sources providing signature set files grouped in categories
- A list of signatures capable of adapting to the needs of the environment to be monitored
- A list of Ruleset enabling signatures to be linked to a GCap

**Note:**

Managing the sources, categories, rules, and rulesets is done in the rules manager built into the GCenter.

The following paragraphs describe the steps required to provide these rules in Ruleset form to the Sigflow module of the GCap through the GCenter:

- Management of available rule sources: see paragraph *Sigflow engine signature sources*

  Sources are used to report repositories where signatures are made available.

  Once downloaded and unzipped, the rules must be added to the **GCenter** interface.

  These sources update automatically in the case of public source/HTTP if the **GCenter** is connected to the internet, otherwise, a manual update can be made at this interface in order to have the latest signatures of available.
- The creation of rulesets from the sources: see the paragraph *Rulesets*

  Once the rules have been added, it is possible to directly assign this source to different rulesets
- The generation of rulesets: refer to *Generating rulesets*
- Applying rulesets to the GCap: refer to *Detection Rulesets*
- Advanced configuration of GCap parameters: refer to *GCAP Profiles*

---

#### 2.1.3.3 Sigflow engine signature sources

The sources include *Suricata* type detection signatures.
There are native sources: CTI, ETPRO.

It is also possible to add public sources to the rules manager.
Each source issues a file of rule sets, grouped into categories.
It is possible to manage categories and rules.
The rules manager enables to:

- Define and manage the sources of signatures for the detection engine
- Manage the rule set files made available by the sources
- Manage the categories and rules of these files
- View the rules contained in the available sources

The signatures are updated using the Gatewatcher Update Manager (**GUM**).
The user (operator) can directly assign one or more sources to a Ruleset.

The source management manager is described in the paragraph *`Config - sigflow/sources` screen of the legacy web UI*.
For implementation, see *SIGFLOW engine rule sources*.

#### 2.1.3.4 Rulesets

Ruleset is the security and detection policy to be applied to the GCap.
As noted above, a ruleset is therefore composed of sources that include the various detection signatures.
The creation of the ruleset is mandatory for the **GCap** probe to be able to analyze the network traffic and raise alerts.
Modifications can be made to signatures or categories in order to adapt a rule to the specificities of the information system or to a particular need.

The source management manager is described in the paragraph *`Config - sigflow/sources` screen of the legacy web UI*.
For implementation, see *Creating a SIGFLOW engine ruleset*.

##### 2.1.3.4.1 Optimization of rulesets

Optimization of a ruleset consists of adapting it to the type of traffic analyzed and the different collection points.
The ruleset can be edited at any time by adding, modifying, or deleting rules, categories, or sources.
A modified ruleset must be applied to the GCap in order for the changes to take effect.

For implementation, see *Creating a SIGFLOW engine ruleset*.

##### 2.1.3.4.2 Changing signatures

Signatures and categories can be enabled, disabled, or modified for a given Ruleset.
It is possible to:

- Activate signatures and categories
- Deactivate signatures and categories
- It is possible to modify the functioning of a signature in order to adapt it to the supervised information system by setting up a threshold or suppression of alert for a specific network.

It is possible to modify a signature in the following way:

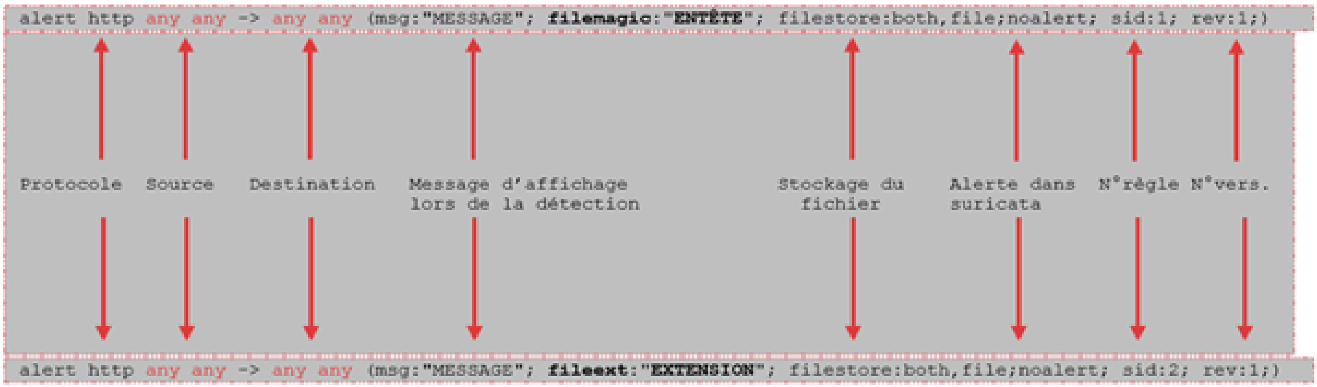
- Create a Suppress Rule on a rule: removes the raising of an alert according to a source or destination IP
- Create a Threshold Rule: limit the number of alerts to be displayed based on a source or destination IP

**Note:**

It is not possible to directly interact with the rule content from the rule manager.
For its implementation, see the procedure *Modifying SIGFLOW engine rules*.

#### 2.1.3.4.2.1 Definition of signatures

Signatures in the CTI and ETPRO sources can include references to blogs, CVEs, websites, and the like that can be accessed from the rules manager.
To better understand how a signature works, here is an example of a signature:



```
alert http any any -> any any (msg:"MESSAGE"; filemagic:"ENTÊTE"; filestore:both,file;noalert; sid:1; rev:1;)
```

```
alert http any any -> any any (msg:"MESSAGE"; fileext:"EXTENSION"; filestore:both,file;noalert; sid:2; rev:1;)
```

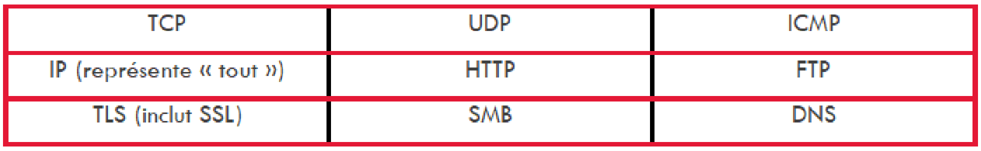
A signature is always made up of:

- An action
- A protocol
- Network parameters such as IP and source and destination port
- A message

Example of a signature:

```
  alert | drop tcp $HOME_NET -> EXTERNAL_NET any (msg;”icmp
detected”;sid:1;rev:1;)
```

The following protocols may be subject to a rule:



| | | |
|---|---|---|
| TCP | UDP | ICMP |
| IP (représente « tout ») | HTTP | FTP |
| TLS (inclut SSL) | SMB | DNS |

This signature is composed of:

- The first part "action": corresponds to the action to be performed in case of detection. For example: "alert, pass, drop..."
- The 2nd part "the header": it is this part that allows to define the meaning of the alert as well as the networks and protocols. For example: "tcp any -> any "

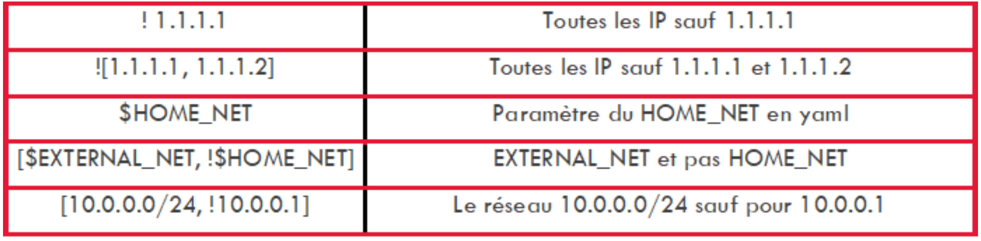
  This part is composed of:

- "Protocol" part: indicates the monitored protocol. For example: "tcp, udp, icmp"
- "Source and destination" section: specifies the source of traffic and the destination of traffic respectively. It is possible to assign IP addresses (IPv4 and IPv6 are supported) and IP ranges with operations if needed.

It is also possible to use variables such as $HOME_NET and $EXTERNAL_NET that are managed in the *`Net variables` section of the `Config Gcaps profiles` menu* and *Net variables*

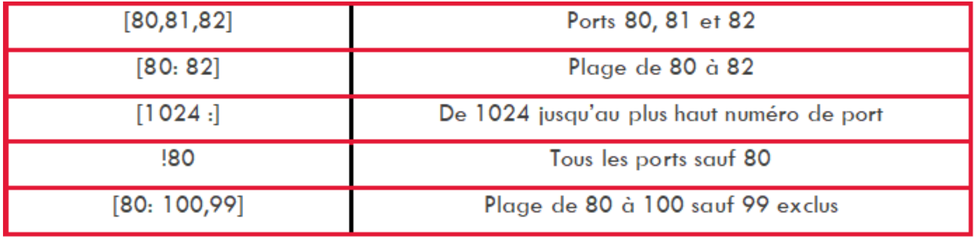
These variables are used to increase the accuracy of the alerts provided by the signatures.

The following syntax can be used to specify the addresses:



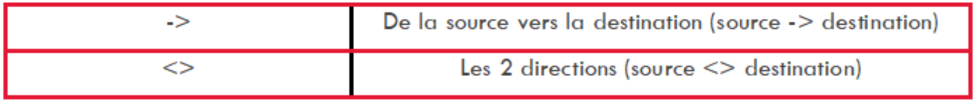
| | |
|---|---|
| ! 1.1.1.1 | Toutes les IP sauf 1.1.1.1 |
| ![1.1.1.1, 1.1.1.2] | Toutes les IP sauf 1.1.1.1 et 1.1.1.2 |
| $HOME_NET | Paramètre du HOME_NET en yaml |
| [$EXTERNAL_NET, !$HOME_NET] | EXTERNAL_NET et pas HOME_NET |
| [10.0.0.0/24, !10.0.0.1] | Le réseau 10.0.0.0/24 sauf pour 10.0.0.1 |

- The part "Ports (source and destination)" : indicates the ports : the first is the source port, the second is the destination port (see the direction of the directional arrow).
  Traffic between and out of ports. Different protocols have different port numbers.
  For example, the default port for HTTP is 80 while 443 is usually the port for HTTPS.
  Note however that the port does not dictate which protocol is used in the communication. Rather, it determines which application receives the data.
  The list below gives examples of port specifications.



| | |
|---|---|
| [80,81,82] | Ports 80, 81 et 82 |
| [80: 82] | Plage de 80 à 82 |
| [1024 :] | De 1024 jusqu'au plus haut numéro de port |
| !80 | Tous les ports sauf 80 |
| [80: 100,99] | Plage de 80 à 100 sauf 99 exclus |

- the "Direction" part: indicates the direction of the flow.



| | |
|---|---|
| -> | De la source vers la destination (source -> destination) |
| <> | Les 2 directions (source <> destination) |

- The last part corresponds to the options applied to the rule.
  These are surrounded by parentheses and separated by semicolons.
  Some options have parameters (such as msg), which are specified by the option keyword, followed by a colon, followed by the parameters.
  Others have no parameters, they are simply the keyword (like nocase).

For its implementation, see the procedure *Modifying SIGFLOW engine rules*.

#### 2.1.3.4.3 Generating rulesets

**Important:**

As long as the rulesets have not been generated after modifications, no configuration will be deployed on the GCap.

Once the ruleset is created, it needs to be generated to validate the creation. It will then be possible to transfer to the GCap.

For implementation, see the *Generating a SIGFLOW engine ruleset*.

---

#### 2.1.3.4.3.1 Secret Local Rule

It is also possible to define certain rules locally on a GCap probe that will intentionally not appear in the **GCENTER** rule manager.
This may occur in the following instances:

- Making signatures confidential without the GCenter operators being able to see them ('need-to-know' concept)
- In complex cases, perform a local modification on the probe signatures
- If the GCenter is entrusted to a third party and the latter cannot handle markers or signatures of a certain level

This procedure is detailed in the GCAP-documentation in the section **Add secret rules locally**.

---

### 2.1.3.5 GCAP Profiles

From this configuration interface, users will be able to apply specific policy rules. They can customize the settings from the following categories:

- *Detection Rulesets*
- *Base variables*
- *Net variables*
- *Flow timeouts*
- *Files rules management*
- *Packet filtering*

In order for the GCap to raise alerts, the user must first apply a ruleset to the GCap.
The GCap profile manager and its configurations are described in the *Web UI `Config - Gcaps profiles` screen*.
For implementation, see *Configuring GCaps*.

---

#### 2.1.3.5.1 Detection Rulesets

The `Detection Rulesets` section enables applying *Rulesets* to the GCap paired with the GCenter.
It is also possible to configure the Codebreaker module by enabling or disabling shellcode and powershell detection.

> **Note:**
>
> It is necessary to generate rules for a ruleset before applying it to GCAPs. Failure to do so will result in no rules being applied to the probe.

> **Note:**
>
> Codebreaker is configurable via the `` `Detection Rulesets` `` menu, but unfairly so for licenses with this module

The GCap `` `Detection Rulesets` `` menu enables three configuration options:

- The *Single-tenant*
- The *Multi-tenant by interface*
- The *Multi-tenant by vlan*

> **Note:**
>
> These configuration options are exclusive. This means that it will not be possible to apply a single tenant and multi-tenant configuration at the same time.

#### 2.1.3.5.1.1 Single-tenant

Single-tenant mode enables:

- Assigning a ruleset for all GCap monitoring interfaces
- Enabling/disabling the Codebreaker module for all GCap monitoring interfaces

The detection ruleset manager is described in the *`Detection Rulesets` section of the `Config Gcaps profiles` menu*.
For implementation, see *Configure Codebreaker then apply the Sigflow rulesets to the GCaps*.

#### 2.1.3.5.1.2 Multi-tenant by interface

The Multi-tenant by interface mode enables:

- Assigning a ruleset per GCap monitoring interface
- Enabling/disabling the Codebreaker module per GCap monitoring interface

The **multi-tenant by interface** enables applying a ruleset for each of the GCap's interfaces and therefore having a different monitoring per interface.
Indeed, it is possible to apply a different ruleset, as well as to configure Codebreaker for each of the GCap interfaces.

The detection ruleset manager is described in the *`Detection Rulesets` section of the `Config Gcaps profiles` menu*.
For implementation, see *Configure Codebreaker then apply the Sigflow rulesets to the GCaps*.

#### 2.1.3.5.1.3 Multi-tenant by vlan

The Multi-tenant by vlan mode enables:

- Assigning one ruleset per vlan
- Assigning a ruleset for the default vlan for those vlans not created via the interface
- Enabling/disabling the Codebreaker module per vlan
- Enabling/disabling the Codebreaker module for the default vlan i.e. vlans not created via the interface

The **multi-tenant by vlan** enables a configuration to be applied for each vlan previously created in the interface and to have distinct monitoring on different networks.

Thus, it is possible to apply a ruleset as well as to configure Codebreaker independently for each vlan.

A vlan named "default" is created as standard in the interface. It enables a ruleset to be applied and Codebreaker to be configured for all vlans not explicitly specified in the interface.

The detection ruleset manager is described in the *`Detection Rulesets` section of the `Config Gcaps profiles` menu*.

For implementation, see *Configure Codebreaker then apply the Sigflow rulesets to the GCaps*.

---

### 2.1.3.5.2 Base variables

The **Base variables** section enables the probe's capture parameters to be adjusted using the advanced Sigflow functions that can be configured from **GCenter**.

Changes to this configuration have an impact on the alerts sent from the GCap probe to the GCENTER.

Enabling certain options will enable the sending of alerts, anomalies, metadata, file information, and protocol-specific records.

Alerts are records of events triggered by the matching of a rule with network traffic.

An alert will be created with associated metadata, such as the application layer record (HTTP, DNS, etc).

The graphical interface of this base variable manager is described in paragraph *`Base variables` section of the `Config Gcaps profiles` menu*.

The basic variables section is composed of:

- *Stream analysis and file extraction*
- *HTTP Proxy*
- *Payload*
- *Community ID*
- *Alerting and logging*

---

#### 2.1.3.5.2.1 Stream analysis and file extraction

The stream analysis and file extraction area enables you to control how the Sigflow engine handles maximum stream and file extraction sizes.
The graphical interface and the details of the parameters are described in the *`Stream analysis and file extraction` zone*.

---

#### 2.1.3.5.2.2 HTTP Proxy

The HTTP Proxy area enables enhanced metadata and alerts for streams mandated with the X-Forwarded-For (XFF) http header.
The graphical interface and the details of the parameters are described in the *`HTTP Proxy` zone*.

**Note:**

XFF is a standard header enabling to identify the original IP address of a client connecting to a web server through an HTTP proxy or load balancer.

---

#### 2.1.3.5.2.3 Payload

The **Payload** section enables enabling or disabling various fields present (Http body, Payload printable, Http body printable...) in the events.
The graphical interface and the details of the parameters are described in the *`Payload` zone*.

---

#### 2.1.3.5.2.4 Community ID

The **Community ID** section allows this field to be enabled or disabled in events.
This enables identifying the network streams being analyzed.

**Note:**

This field is present in solutions other than Gatewatcher. It can therefore enable correlating the different tools of the same information system.

The graphical interface and the details of the parameters are described in the *`Community ID` zone*.

---

#### 2.1.3.5.2.5 Alerting and logging

The **Alerting and logging** section enables configuring the **alerting** and **logging** of the protocols used by the Gcap.

> **Note:**
>
> If GCap is one version ahead of the GCenter, it is possible that some protocols are not yet implemented in the latter.

This is discussed in more detail in the GCAP-documentation in the section *Sigflow detection engine > Rebuilding files.*

**Terminology for parsing and logging:**

- **alerting** consists in activating the Sigflow signature detection for a given protocol. Indeed, if Sigflow is activated for a protocol, then the stream that is identified by a signature will raise an alert on the GCenter side.
- **logging** consists in enabling the generation of metadata for a given protocol. Indeed, if the latter is enabled for a protocol, then each observed session will generate metadata for that protocol on the GCenter side.

Managing the configuration of the protocols is done:

- by using default profiles such as Minimal, Balanced, MPL, Paranoid, and Intuitio: in order from most to least permissive
- by modifying the content of the profile uploaded to the GCap.

The choice of the default profile and the loading on the GCap is done in the graphical interface detailed in the *`Admin-GCaps pairing and status` screen of the legacy Web UI*.
Changing the configuration of the profile loaded into the GCap is done in the graphical interface detailed in *`Alerting and logging` zone*.
The default configuration of protocols varies depending on the GCap profile used: the list is shown in *Default settings for existing profiles available*.
The list of protocols that can be configured with the alerting option and with the logging option is provided in the paragraph *Default settings for existing profiles available*.
For implementation, see *Configure GCap Sigflow module specific parameters (Base variables)*.

---

#### 2.1.3.5.3 Net variables

The **Net variables** area of the GUI enables defining the network variables used in the Sigflow rules.
The list of variables and their default values are given in *`Net variables` section of the `Config Gcaps profiles` menu*.
This graphical interface is described in *`Net variables` section of the `Config Gcaps profiles` menu*.
For implementation, see *Configure network variables used by rules (Net variables)*.

---

#### 2.1.3.5.4 Flow timeouts

The **Flow timeouts** section enables configuring the time in seconds that Sigflow keeps a flow in memory depending on its status.
The list of variables and their default values are given in *`Flow timeouts` section of the `Config Gcaps profiles` menu*.
This graphical interface is described in *`Flow timeouts` section of the `Config Gcaps profiles` menu*.

---

#### 2.1.3.5.5 Files rules management

The **Files rules management** section enables choosing the file types that the probe will retrieve for a given protocol.
File extraction works in parallel with the Sigflow signatures defined for these same protocols.
Files are reconstructed and then saved to disk with metadata that includes information such as:

- Time stamp
- Source/destination IP address
- Protocol
- Source/destination port
- Size
- Md5sum, etc.

Managing the configuration of the file extraction rules is done:

- By using default profiles such as Minimal, Balanced, MPL, Paranoid, and Intuitio: in order from most to least complete
- By modifying the content of the profile uploaded to the GCap.

The choice of the default profile and the loading on the GCap is done in the graphical interface detailed in the *`Admin-GCaps pairing and status` screen of the legacy Web UI*.
Changing the configuration of the profile loaded into the GCap is done in the graphical interface detailed in *`File rule management` section of the `Config Gcaps profiles` menu*.
The list of protocols as well as the list of file types are given in the *Web UI `Config - Gcaps profiles` screen*.

For implementation, see *Configure File Reconstruction Rules (File rules management)*.

---

#### 2.1.3.5.6 Packet filtering

The `` `Packet filters` `` section enables specific traffic to be ignored directly at the GCap network card level.
This feature enables the GCap to avoid overloading the GCap with "unnecessary" traffic such as encrypted streams, backup streams, etc., or traffic that may cause the cpus to overload such as Elephant Flow, Miles Flow, etc.
The selection of traffic to be ignored is based on vlan, network prefix, protocol, and network ports.

This graphical interface is described in *`Packet filters` section of the `Config Gcaps profiles` menu*.

For implementation, see *Configure filters on targeted parts of the analyzed traffic (Packet filters)*.

---

### 2.1.3.6 Events generated

The events generated by Sigflow are:

- *Events of type "alert"* when the engine has found a match with the signature defined in the alert rules.
  Events are displayed in the main GCenter interface as well as in Kibana.
  In the main interface, it is possible to view the found signature and its definition.
  In the main interface named **WEB UI** of the GCenter in the `` `Alerts` `` screen (the main interface named WEB UI is described in the WEB UI Overview).
  To view the alerts, you must select the IDS filter and thus view the list of alerts: see the presentation of the `` `Alerts` `` screen of the web UI.
  By clicking on an alert, the detailed information of this alert is displayed: see *Counters of the source part of Sigflow logs of alert type*.
  In the **Kibana UI** interface
  To view the alerts, select the Sigflow filter and view the list of alerts: see the `` `Alerts` `` screen of the web UI.
  By clicking on an alert, select on the command `` `Flow details` `` then select the arrow to the left of the alert.
  The interface displayed is the interface named Kibana UI (described in the Kibana GUI Overview).
  The detailed information of this alert can be viewed in table or jason format.
  The detailed information of this alert is displayed: see *Counters of the source part of Sigflow logs of alert type*.
- *Events of type "fileinfo"* when the Sigflow engine has reconstructed the network flow files`.
  These fileinfo events are visible in the Kibana interface.
  To do this, select the Hunting command, then the tab `` `Sigflow` `` and the category `` `Messages` ``, then select the arrow to the left of the event.
  The detailed information of this event can be viewed in table or jason format.
  The detailed information of this event is displayed (see *Events of type "fileinfo"*).
- *Events of type "meta-data"* when the Sigflow engine has recognized the network flow.
  These metadata events are visible in the Kibana interface.
  To do this, select on the Hunting command then the tab `` `Metadata` `` and the category `` `Messages` ``, then select the arrow to the left of the event.
  The detailed information of this event can be viewed in table or jason format.
  The detailed information of this event is displayed (see *Metadata counters*)

These events (or logs) are structured in the same way and this structure is presented in the paragraph *Example and log structure (Events) Sigflow*.

---

#### 2.1.3.6.1 Example and log structure (Events) Sigflow

##### 2.1.3.6.1.1 Exemple d'un log Sigflow

Below is an example of log sigflow (alert log) is displayed:

```
{
"_index": "suricata-2023.10.09-000162",
"_type": "_doc",
```

(suite sur la page suivante)

(suite de la page précédente)

```
"_id": "lb-iE4sBeBoubSygsnlA",
"_version": 1,
"_score": 1,
"_source": {
  "proto": "TCP",
  "@timestamp": "2023-10-09T08:51:50.124Z",
  "uuid": "1b6e03fa-d325-4f3d-ac54-e2dd6152c8fd",
  "timestamp_analyzed": "2023-10-09T08:51:50.124Z",
  "gcap": "gcap-xxxxxxxxx.domain.local",
  "host": "gcap-xxxxxxxxx.domain.local",
  "flow": {
    "pkts_toclient": 4,
    "pkts_toserver": 4,
    "bytes_toserver": 421,
    "bytes_toclient": 647,
    "start": "2023-10-09T08:51:17.974120+0000"
  },
  "dest_port": 48740,
  "alert": {
    "signature_id": 2034636,
    "rev": 2,
    "action": "allowed",
    "severity": 3,
    "metadata": {
      "updated_at": [
        "2021_12_08"
      ],
      "attack_target": [
        "Client_Endpoint"
      ],
      "former_category": [
        "INFO"
      ],
      "signature_severity": [
        "Minor"
      ],
      "deployment": [
        "Perimeter"
      ],
      "affected_product": [
        "Windows_XP_Vista_7_8_10_Server_32_64_Bit"
      ],
      "created_at": [
        "2021_12_08"
      ]
    },
    "signature": "ET INFO Python SimpleHTTP ServerBanner",
    "gid": 1,
    "category": "Misc activity"
  },
  "type": "suricata",
  "packet": "ivOZFqBXfu+N6xq...
↪AqAABwKgAAwBQvmQfXmk2N+fYu4AYAfzRowAAAQEIClfrLQ32MlIpUEsDBAoAAAAAAOCYuCg8z1FoRAAAAEQAAAAJAAAAZWljYXIuY
↪4EAAAAAZWljYXIuY29tUEsFBgAAAAABAAEANwAAAGsAAAAAAA==",
  "timestamp_detected": "2023-10-09T08:51:17.976Z",
  "dest_ip": "X.X.X.X",
```

(suite sur la page suivante)

(suite de la page précédente)

```
  "src_port": 80,
  "ether": {
    "dest_mac": "7e:ef:8d:eb:1a:81",
    "src_mac": "8a:f3:99:16:a0:57"
  },
  "community_id": "1:r6LvcE7ltny4a6Y9xt1VroBgcKs=",
  "event_type": "alert",
  "@version": "1",
  "severity": 3,
  "stream": 1,
  "flow_id": 1666858537573672,
  "gcenter": "gcenter-xxx.domain.local",
  "payload_printable": "HTTP/1.0 200 OK\r\nServer: SimpleHTTP/0.6 Python/3.7.3\r\nDate: Thu,␣
↪20 Aug 2020 08:27:52 GMT\r\nContent-type: application/zip\r\nContent-Length: 184\r\nLast-
↪Modified: Thu, 20 Aug 2020 08:26:32 GMT\r\n\r\n",
  "src_ip": "X.X.X.X",
  "in_iface": "monvirt",
  "http": {
    "hostname": "eicar.com",
    "status": 200,
    "http_user_agent": "Wget/1.20.1 (linux-gnu)",
    "url": "/eicar_com.zip",
    "http_content_type": "application/zip",
    "length": 0,
    "http_method": "GET",
    "protocol": "HTTP/1.1"
  },
  "payload":
↪"SFRUUC8xLjAgMjAwIE9LDQpTZXJ2ZXI6IFNpbXBsZUhUVFAvMC42IFB5dGhvbi8zLjcuMw0KRGF0ZTogVGh1LCAyMCBBdWcgMjAyM
↪",
  "tx_id": 0,
  "app_proto": "http",
  "packet_info": {
    "linktype": 1
  }
},
"fields": {
  "alert.category": [
    "Misc activity"
  ],
  "alert.metadata.signature_severity": [
    "Minor"
  ],
  "http.url": [
    "/eicar_com.zip"
  ],
  "type": [
    "suricata"
  ],
  "uuid": [
    "1b6e03fa-d325-4f3d-ac54-e2dd6152c8fd"
  ],
  "alert.metadata.created_at": [
    "2021_12_08"
  ],
  "event_type": [
```

(suite sur la page suivante)

(suite de la page précédente)

```
    "alert"
  ],
  "payload": [

↪"SFRUUC8xLjAgMjAwIE9LDQpTZXJ2ZXI6IFNpbXBsZUhUVFAvMC42IFB5dGhvbi8zLjcuMw0KRGF0ZTogVGh1LCAyMCBBdWcgMjAyM
↪"
  ],
  "flow_id": [
    1666858537573672
  ],
  "host": [
    "gcap-xxxxxxxxx.domain.local"
  ],
  "ether.src_mac": [
    "8a:f3:99:16:a0:57"
  ],
  "alert.metadata.former_category": [
    "INFO"
  ],
  "dest_port": [
    48740
  ],
  "alert.severity": [
    3
  ],
  "gcenter": [
    "gcenter-xxx.domain.local"
  ],
  "flow.bytes_toclient": [
    647
  ],
  "packet": [
    "ivOZFqBXfu+N6xq...
↪AqAABwKgAAwBQvmQfXmk2N+fYu4AYAfzRowAAAQEIClfrLQ32MlIpUEsDBAoAAAAAAOCYuCg8z1FoRAAAAEQAAAAJAAAAZWljYXIuY
↪4EAAAAAZWljYXIuY29tUEsFBgAAAAABAAEANwAAAGsAAAAAAA=="
  ],
  "tx_id": [
    0
  ],
  "http.length": [
    0
  ],
  "timestamp_detected": [
    "2023-10-09T08:51:17.976Z"
  ],
  "http.hostname": [
    "eicar.com"
  ],
  "flow.bytes_toserver": [
    421
  ],
  "dest_ip": [
    ""X.X.X.X""
  ],
  "proto": [
    "TCP"
```

(suite sur la page suivante)

(suite de la page précédente)

```
  ],
  "gcap": [
    "gcap-xxxxxxxxx.domain.local"
  ],
  "timestamp_analyzed": [
    "2023-10-09T08:51:50.124Z"
  ],
  "alert.metadata.deployment": [
    "Perimeter"
  ],
  "http.http_user_agent": [
    "Wget/1.20.1 (linux-gnu)"
  ],
  "http.http_method": [
    "GET"
  ],
  "alert.metadata.attack_target": [
    "Client_Endpoint"
  ],
  "ether.dest_mac": [
    "7e:ef:8d:eb:1a:81"
  ],
  "alert.metadata.affected_product": [
    "Windows_XP_Vista_7_8_10_Server_32_64_Bit"
  ],
  "flow.pkts_toclient": [
    4
  ],
  "http.http_content_type": [
    "application/zip"
  ],
  "src_ip": [
    "X.X.X.X"
  ],
  "community_id": [
    "1:r6LvcE7ltny4a6Y9xt1VroBgcKs="
  ],
  "stream": [
    "1"
  ],
  "alert.rev": [
    2
  ],
  "@version": [
    "1"
  ],
  "alert.signature_id": [
    "2034636"
  ],
  "alert.action": [
    "allowed"
  ],
  "packet_info.linktype": [
    1
  ],
  "severity": [
```

(suite sur la page suivante)

(suite de la page précédente)

```
    3
  ],
  "payload_printable": [
    "HTTP/1.0 200 OK\r\nServer: SimpleHTTP/0.6 Python/3.7.3\r\nDate: Thu, 20 Aug 2020␣
↪08:27:52 GMT\r\nContent-type: application/zip\r\nContent-Length: 184\r\nLast-Modified: Thu,␣
↪20 Aug 2020 08:26:32 GMT\r\n\r\n"
  ],
  "http.protocol": [
    "HTTP/1.1"
  ],
  "app_proto": [
    "http"
  ],
  "in_iface": [
    "monvirt"
  ],
  "src_port": [
    80
  ],
  "flow.start": [
    "2023-10-09T08:51:17.974Z"
  ],
  "alert.gid": [
    1
  ],
  "@timestamp": [
    "2023-10-09T08:51:50.124Z"
  ],
  "alert.signature": [
    "ET INFO Python SimpleHTTP ServerBanner"
  ],
  "flow.pkts_toserver": [
    4
  ],
  "http.status": [
    "200"
  ],
  "alert.metadata.updated_at": [
    "2021_12_08"
  ]
}
}
```

#### 2.1.3.6.1.2 Structure of sigflow logs

The logs are composed of different parts:

- the leading part
- the source part defined by "_source"
- the field portion defined by "_fields"

#### 2.1.3.6.1.3 The header part of the sigflow logs

The header section contains:

```
{
 "_index": "suricata-2023.10.09-000162",
 "_type": "_doc",
 "_id": "lb-iE4sBeBoubSygsnlA",
 "_version": 1,
 "_score": 1,
```

Table15: Table part header of logs sigflow

| Field | Required | Description | Values or example |
|---|---|---|---|
| _index | Yes | Internal index | suricata-2023.10.09-000162 |
| _type | Yes | default type | _doc |
| _id | Yes | internal identifier | lb-iE4sBeBoubSygsnlA |
| _version | Yes | internal version | 1 |
| _score | Yes | relevance of the response to the request | 1 |

#### 2.1.3.6.1.4 The source part of the sigflow logs

The source part defined by "_source" contains:

```
{
 "_index": "suricata-2023.10.09-000162",
 "_type": "_doc",
 "_id": "lb-iE4sBeBoubSygsnlA",
 "_version": 1,
 "_score": 1,
 "_source": {
   "proto": "TCP",
   "@timestamp": "2023-10-09T08:51:50.124Z",
   "uuid": "1b6e03fa-d325-4f3d-ac54-e2dd6152c8fd",
   "timestamp_analyzed": "2023-10-09T08:51:50.124Z",
   "gcap": "gcap-xxxxxxxxx.domain.local",
   "host": "gcap-xxxxxxxxx.domain.local",
   "flow": {
     "pkts_toclient": 4,
     "pkts_toserver": 4,
     "bytes_toserver": 421,
     "bytes_toclient": 647,
     "start": "2023-10-09T08:51:17.974120+0000"
   },
   "dest_port": 48740,
   "alert": {
     "signature_id": 2034636,
     "rev": 2,
     "action": "allowed",
     "severity": 3,
     "metadata": {
       "updated_at": [
         "2021_12_08"
       ],
```

(suite sur la page suivante)

(suite de la page précédente)

```
        "attack_target": [
          "Client_Endpoint"
        ],
        "former_category": [
          "INFO"
        ],
        "signature_severity": [
          "Minor"
        ],
        "deployment": [
          "Perimeter"
        ],
        "affected_product": [
          "Windows_XP_Vista_7_8_10_Server_32_64_Bit"
        ],
        "created_at": [
          "2021_12_08"
        ]
      },
      "signature": "ET INFO Python SimpleHTTP ServerBanner",
      "gid": 1,
      "category": "Misc activity"
    },
    "type": "suricata",
    "packet": "ivOZFqBXfu+N6xq...
↪AqAABwKgAAwBQvmQfXmk2N+fYu4AYAfzRowAAAQEIClfrLQ32MlIpUEsDBAoAAAAAAOCYuCg8z1FoRAAAAEQAAAAJAAAAZWljYXIuY
↪4EAAAAAZWljYXIuY29tUEsFBgAAAAABAAEANwAAAGsAAAAAAA==",
    "timestamp_detected": "2023-10-09T08:51:17.976Z",
    "dest_ip": "X.X.X.X",
    "src_port": 80,
    "ether": {
      "dest_mac": "7e:ef:8d:eb:1a:81",
      "src_mac": "8a:f3:99:16:a0:57"
    },
    "community_id": "1:r6LvcE7ltny4a6Y9xt1VroBgcKs=",
    "event_type": "alert",
    "@version": "1",
    "severity": 3,
    "stream": 1,
    "flow_id": 1666858537573672,
    "gcenter": "gcenter-xxx.domain.local",
    "payload_printable": "HTTP/1.0 200 OK\r\nServer: SimpleHTTP/0.6 Python/3.7.3\r\nDate: Thu,␣
↪20 Aug 2020 08:27:52 GMT\r\nContent-type: application/zip\r\nContent-Length: 184\r\nLast-
↪Modified: Thu, 20 Aug 2020 08:26:32 GMT\r\n\r\n",
    "src_ip": "X.X.X.X",
    "in_iface": "monvirt",
    "http": {
      "hostname": "eicar.com",
      "status": 200,
      "http_user_agent": "Wget/1.20.1 (linux-gnu)",
      "url": "/eicar_com.zip",
      "http_content_type": "application/zip",
      "length": 0,
      "http_method": "GET",
      "protocol": "HTTP/1.1"
    },
```

(suite sur la page suivante)

(suite de la page précédente)

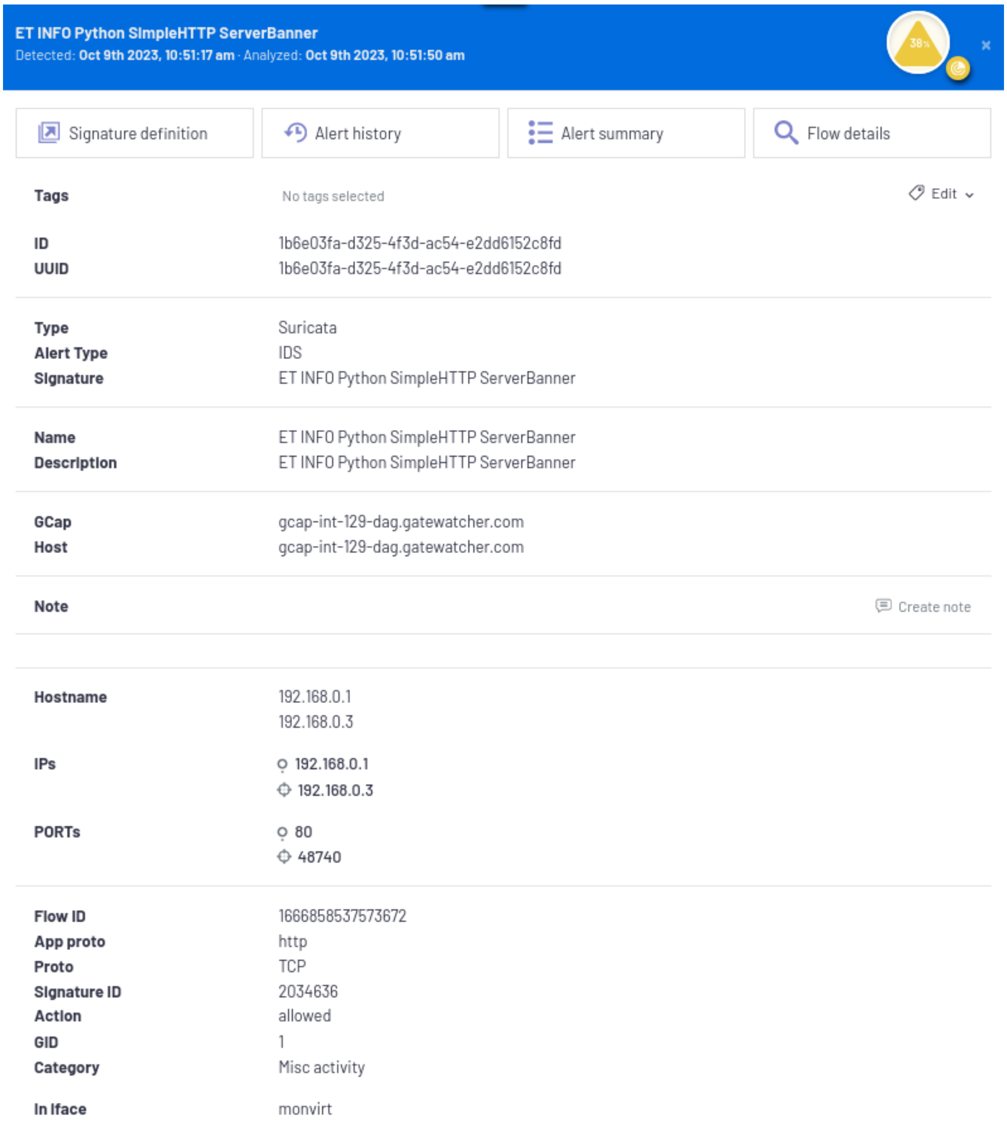
```
   "payload":
↪"SFRUUC8xLjAgMjAwIE9LDQpTZXJ2ZXI6IFNpbXBsZUhUVFAvMC42IFB5dGhvbi8zLjcuMw0KRGF0ZTogVGh1LCAyMCBBdWcgMjAyM
↪",
   "tx_id": 0,
   "app_proto": "http",
   "packet_info": {
     "linktype": 1
   }
 },
```

#### 2.1.3.6.1.5 The fields part of the sigflow logs

The field part defined by "fields" contains the same counters as in the source part: refer to the source part section

### 2.1.3.6.2 Events of type "alert"

#### 2.1.3.6.2.1 Example of "alert" Sigflow events in the webui



**ET INFO Python SimpleHTTP ServerBanner**

Detected: **Oct 9th 2023, 10:51:17 am** · Analyzed: **Oct 9th 2023, 10:51:50 am**

| | |
|---|---|
| **Tags** | No tags selected |
| **ID** | 1b6e03fa-d325-4f3d-ac54-e2dd6152c8fd |
| **UUID** | 1b6e03fa-d325-4f3d-ac54-e2dd6152c8fd |
| **Type** | Suricata |
| **Alert Type** | IDS |
| **Signature** | ET INFO Python SimpleHTTP ServerBanner |
| **Name** | ET INFO Python SimpleHTTP ServerBanner |
| **Description** | ET INFO Python SimpleHTTP ServerBanner |
| **GCap** | gcap-int-129-dag.gatewatcher.com |
| **Host** | gcap-int-129-dag.gatewatcher.com |
| **Note** | |
| **Hostname** | 192.168.0.1<br>192.168.0.3 |
| **IPs** | 192.168.0.1<br>192.168.0.3 |
| **PORTs** | 80<br>48740 |
| **Flow ID** | 1666858537573672 |
| **App proto** | http |
| **Proto** | TCP |
| **Signature ID** | 2034636 |
| **Action** | allowed |
| **GID** | 1 |
| **Category** | Misc activity |
| **In Iface** | monvirt |

The counters are detailed in *Structure of sigflow logs*.

#### 2.1.3.6.2.2 Log data of type "alert"

The list of protocols that can generate alerts is indicated by the parameter *Default settings for existing profiles available* (app_proto field)`.

If a protocol changes along the way (for example if SMTP is upgraded to TLS via STARTTLS) or if the protocols used are not the same in both directions of the flow, the following fields may appear:

- app_proto_tc (to client)
- app_proto_ts (to server)
- app_proto_orig

**Note:**

The protocol actually recognized by Sigflow is defined in the GCap profile in the `Alerting and logging` tab in the `Alerting` column.

#### 2.1.3.6.2.3 Counters of the source part of Sigflow logs of alert type

**Note:**

This summary table shows which counters are not protocol dependent.

Table16: Table part source of Sigflow logs of alert type

| Field | Required | Description | Values or example |
|---|---|---|---|
| @timestamp | Yes | Timestamp of the processing of the alert by the GCenter (corresponds to the passage in logstash) | 2023-10-09T08:51:50.124Z |
| @version | yes | version of document | 1 |
| app_proto | No | File source flow application protocol | http |
| community_Id | Yes | Unique id to correlate the rise between the different security equipment | 1:r6LvcE7ltny4a6Y9xt1Vr... |
| dest_ip | Yes | Destination IP address | "X.X.X.X" |
| dest_mac | Yes | Destination MAC address | "7e:ef:8d:eb:1a:81" |
| dest_port | No | Destination port. Present only when proto is udp or tcp | 48740 |
| event_type | Yes | Type of event: alert | Default alert |
| flow_id | Yes | Flow identifier | 1666858537573672 |
| flow.bytes_toclient | Yes | Size of flow to customer | 647 |
| flow.bytes_toserver | Yes | Size of flow to server | 421 |
| flow.pkts_toclient | Yes | Number of packets to client | 4 |
| flow.pkts_toserver | Yes | Number of packets to server | 4 |
| flow.reason | No | Mechanism that caused the flow between (“timeout”, “forced”, “shutdown” to stop processing) | |
| flow.start | Yes | Date and time of first package seen by suricata | 2023-10-09T08:51:17.974120+0000 |
| gcap | Yes | Name of the gcap associated with the alert | gcap-xxxxxxxxx.domain.local |
| gcenter | Yes | GCenter name associated with alert | gcenter-xxx.domain.local |
| host | Yes | Name of the gcap associated with the alert | gcap-xxxxxxxxx.domain.local |
| in_iface | No | Capture interface on gcap | monvirt |
| packet | Yes | packet that triggered the alert registered in base64 (only for UDP) | ivOZFqBXfu+N6xq... |
| packet_info.linktype | Yes | Type of link-layer header | 1 |
| payload | No | Payload of the base64 package<br>Present only if the payload option of the gcap "variable bases" menu is enabled | "SFRUUC8xLjAgMjAwIE9... |

suite sur la page suivante

Table 16 – suite de la page précédente

| Field | Required | Description | Values or example |
|---|---|---|---|
| payload_printable | No | Payload of the package in a readable format.<br>Present only if the printable payload option of the gcap «variable bases» menu is activated. | "HTTP/1.0 200 OK r nServer: SimpleHTTP/0.6 Python/3.7.3 r ..." |
| proto | Yes | Layer 4 protocol used | TCP |
| severity | Yes | Level of alert severity | 3 |
| src_ip | Yes | Source IP address | "X.X.X.X" |
| src_mac | Yes | Source MAC address | "8a:f3:99:16:a0:57" |
| src_port | No | Source port. Present only when proto is udp or tcp | 80 |
| stream | Yes | | 1 |
| Timestamp of the processing of the alert by the GCenter (corresponds to the passage in logstash) | Yes | Date and time of alert analysis by logstash | 2023-10-09T08:51:50.124Z |
| timestamp detected | Yes | Date and time of alert generation by suricata | 2023-10-09T08:51:17.976Z |
| tx_id | yes | transaction identification (query/response pair) | 0 |
| type | Yes | Event type: default suricata | suricata |
| uuid | Yes | Unique identifier of the alert | 1b6e03fa-d325-4f3d... |

Table17: Summary table of counters in category "Alert"

| Field | Required | Description | Values or example |
|---|---|---|---|
| alert.action | yes | **Allowed** if **alert** or **pass** is used and **blocked** if **drop** or **reject** is used. | alert, drop, reject, pass "action": "allowed", |
| alert.category | Yes | Description of alert classification | classtype. example Misc activity |
| alert.gid | Yes | Identifier of an alert group | gid |
| alert.metadata | No | Alert metadata. Field specification is free. | metadata: key value |
| alert.rev | Yes | Alert Revision Number | 2 |
| alert.severity | Yes | Level of alert severity | 3 |
| alert.signature | Yes | Description of the alert | AND INFO Python SimpleHTTP ServerBanner |
| alert.signature_id | Yes | Alert ID. Must be unique. | sid. example 2034636 |

**List of metadata used in ETPRO and CTI source alerts (alert.metadata object in ES):**

- alert.metadata.affected_product
- alert.metadata.attack_target
- alert.metadata.created_at
- alert.metadata.deployment
- alert.metadata.former_category
- alert.metadata.impact_flag
- alert.metadata.malware_family
- alert.metadata.performance_impact
- alert.metadata.ruleset
- alert.metadata.service
- alert.metadata.signature_severity
- alert.metadata.tag
- alert.metadata.updated_at

**Here is an example of an alert that uses metadata affected_product, attack_target, created_at, deployment, signature_severity, tag et updated_at:**

```
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (
msg:"ET EXPLOIT MS-SQL SQL Injection closing string plus line comment";
flow: to_server,established;
content:"'|00|";
content:"-|00|-|00|";
reference:url,doc.emergingthreats.net/bin/view/Main/2000488;
classtype:attempted-user;
sid:2000488;
rev:7;
metadata:affected_product Web_Server_Applications, attack_target Web_Server, created_at 2010_07_30, deployment Datacenter, signature_severity Major, tag SQL_Injection, updated_at 2016_07_01;
)
```

#### 2.1.3.6.3 Events of type "fileinfo"

**Note:**

This summary table shows which counters are not protocol dependent.

| Field | Required | Description |
|---|---|---|
| app_proto | Yes | Application protocol of the source stream of the file. example http |
| dest_ip | Yes | Destination IP address |
| dest_port | Yes | Destination port. Present only when proto is udp or tcp |
| event_type | Yes | Type of event |
| fileinfo.file_id | No | File ID |
| fileinfo.filename | Yes | File name |
| fileinfo.gaps | Yes | |
| fileinfo.magic | No | File type identifier |
| fileinfo.md5 | No | MD5 hash of file |
| fileinfo.sha1 | No | SHA1 hash from file |
| fileinfo.sha256 | No | SHA256 hash from file |
| fileinfo.size | Yes | File size |
| fileinfo.state | Yes | Completeness of the analyzed file (CLOSED) otherwise TRUNCATED.<br>The file-store.stream-depth variable of suricata defines the size of the reconstructed files.<br>The file is TRUNCATED if its size is > File-store stream depth (10 MB) by default. |
| fileinfo.stored | Yes | True if the file is reconstructed and False otherwise. |
| fileinfo.tx_id | Yes | transaction identification (query/response pair) |
| flow_id | Yes | Flow identifier |
| gcap | Yes | Name of the gcap associated with the alert |
| gcenter | Yes | GCenter name associated with alert |
| host | Yes | Name of the gcap associated with the alert |
| in_iface | No | Capture interface on gcap |
| proto | Yes | Layer 4 protocol used |
| src_ip | Yes | Destination IP address |
| src_port | No | Destination port. Present only when proto is udp or tcp |
| timestamp analyzed | Yes | Date and time of alert analysis by logstash |
| timestamp detected | Yes | Date and time of alert generation by suricata |
| type | Yes | Event type. Default on |
| uuid | Yes | Unique identifier of the alert |
| vlan | No | Identifier of the flow vlan |

#### 2.1.3.6.4 Events of type "meta-data"

##### 2.1.3.6.4.1 List of fields present in all alerts with event_type!= ["alert", "fileinfo", "stats"]

- @timestamp
- @version
- dest_ip
- event_type
- flow_id
- gcap
- GCenter
- host
- proto
- src_ip
- timestamp_analyzed
- timestamp_detected
- type
- uuid

#### 2.1.3.6.4.2 List of protocols compatible with logging (event_type field)

- **dhcp:**
  - dhcp.assigned_ip
  - dhcp.client_ip
  - dhcp.client_mac
  - dhcp.dhcp_type
  - dhcp.dns_servers
  - dhcp.hostname
  - dhcp.id
  - dhcp.lease_time
  - dhcp.next_server_ip
  - dhcp.params
  - dhcp.rebinding_time
  - dhcp.relay_ip
  - dhcp.renewal_time
  - dhcp.requested_ip
  - dhcp.routers
  - dhcp.subnet_mask
  - dhcp.type
- **dnp3**
- **dns:**

- body.proba_dga
- body.severity
- dga_probability
- dns.aa
- dns.answers.rdata
- dns.answers.rrname
- dns.answers.rrtype
- dns.answers.ttl
- dns.authorities.rrname
- dns.authorities.rrtype
- dns.authorities.ttl
- dns.flags
- dns.grouped.A
- dns.grouped.AAAA
- dns.grouped.CNAME
- dns.id
- dns.qr
- dns.ra
- dns.rcode
- dns.rd
- dns.rrname
- dns.rrtype
- dns.tx_id
- dns.type
- dns.version
- headers.content-length
- headers.content-type
- tags

- **ftp**
- **http:**

- http.accept
- http.accept-charset
- http.accept-datetime
- http.accept_encoding
- http.accept_language
- http.accept-range
- http.age
- http.allow
- http.authorization
- http.cache_control
- http.connection
- http.content_encoding
- http.content-language
- http.content-length
- http.content-location
- http.content-md5
- http.content-range
- http.content_type
- http.content-type
- http.cookie
- http.date
- http.dnt
- http.etags
- http.from
- http.hostname
- http.http_content_type
- http.http_method
- http.http_port
- http.http_refer
- http.http_user_agent
- http.last-modified
- http.length
- http.link
- http.location
- http.max-forwards
- http.origin
- http.pragma
- http.proxy-authenticate
- http.proxy-authorization
- http.range
- http.redirect
- http.referrer
- http.refresh
- http.retry-after
- http.server
- http.set-cookie
- http.status
- http.te
- http.trailer
- http.transfer-encoding
- http.upgrade
- http.url
- http.vary
- http.via
- http.warning
- http.www-authenticate
- http.x-authenticated-user
- http.x-flash-version
- http.x-forwarded-proto
- http.x-requested-with

- **ikev2:**
  - ikev2.alg_auth
  - ikev2.alg_dh
  - ikev2.alg_enc
  - ikev2.alg_esn
  - ikev2.alg_prf
  - ikev2.errors
  - ikev2.exchange_type
  - ikev2.init_spi
  - ikev2.message_id
  - ikev2.notify
  - ikev2.payload
  - ikev2.resp_spi
  - ikev2.role
  - ikev2.version_major
  - ikev2.version_minor
- **krb5:**

  - krb5.cname
  - krb5.encryption
  - krb5.error_code
  - krb5.failed_request
  - krb5.msg_type
  - krb5.realm
  - krb5.sname
  - krb5.weak_encryption

- **netflow:**
  - icmp_code
  - icmp_type
  - metadata.flowbits
  - netflow.age
  - netflow.bytes
  - netflow.end
  - netflow.max_ttl
  - netflow.min_ttl
  - netflow.pkts
  - netflow.start
  - parent_id
  - tcp.ack
  - tcp.cwr
  - tcp.ecn
  - tcp.fin
  - tcp.psh
  - tcp.rst
  - tcp.syn
  - tcp.tcp_flags

- **nfs:**
  - nfs.file_tx
  - nfs.filename
  - nfs.hhashl
  - rpc.auth_type
  - rpc.creds.gid
  - rpc.creds.machine_name
  - rpc.creds.uid
  - rpc.status
  - rpc.xid

- **smb:**
  - smb.access
  - smb.accessed
  - smb.changed
  - smb.client_dialects
  - smb.client_guid
  - smb.command
  - smb.created
  - smb.dcerpc.call_id
  - smb.dcerpc.interfaces.ack_reason
  - smb.dcerpc.interfaces.ack_result
  - smb.dcerpc.interfaces.uuid
  - smb.dcerpc.interfaces.version
  - smb.dcerpc.opnum
  - smb.dcerpc.req.frag_cnt
  - smb.dcerpc.req.stub_data_size
  - smb.dcerpc.request
  - smb.dcerpc.res.frag_cnt
  - smb.dcerpc.res.stub_data_size
  - smb.dcerpc.response
  - smb.dialect
  - smb.directory
  - smb.disposition
  - smb.filename
  - smb.fuid
  - smb.function
  - smb.id
  - smb.modified
  - smb.named_pipe
  - smb.ntlmssp.domain
  - smb.ntlmssp.host
  - smb.ntlmssp.user
  - smb.request.native_lm
  - smb.request.native_os
  - smb.response.native_lm
  - smb.response.native_os
  - smb.server_guid
  - smb.service.request
  - smb.service.response
  - smb.session_id
  - smb.share
  - smb.share_type
  - smb.size
  - smb.status
  - smb.status_code
  - smb.tree_id

- **smtp:**
  - email.attachment
  - email.body_md5
  - email.from
  - email.status
  - email.subject
  - email.subject_md5
  - email.to
  - smtp.helo
  - smtp.mail_from
  - smtp.rcpt_to

- **ssh:**
  - ssh.client.proto_version
  - ssh.client.software_version
  - ssh.server.proto_version
  - ssh.server.software_version

- **tftp:**
  - tftp.file
  - tftp.mode
  - tftp.packet
- **tls:**
  - tls.chain
  - tls.fingerprint
  - tls.issuerdn
  - tls.notafter
  - tls.notbefore
  - tls.sni
  - tls.subject
  - tls.version

#### 2.1.3.6.4.3 Metadata counters

**Summary table of fields that do not depend on the protocols:**

| Field | Required | Description |
|---|---|---|
| app_proto | No | Application protocol of the flow from which the file originates |
| dest_ip | Yes | Destination's IP address |
| dest_port | No | Destination port. Only present when the value of proto is udp or tcp |
| event_type | Yes | Type of event. Alert by default. |
| flow_id | Yes | Flow identifier |
| gcap | Yes | Name of the gcap assigned to the alert |
| gcenter | Yes | Name of the GCenter assigned to the alert |
| host | Yes | Name of the gcap assigned to the alert |
| in_iface | No | Capture interface on the gcap |
| proto | Yes | Layer 4 protocol used |
| src_ip | Yes | Destination IP address |
| src_port | No | Destination port. Only present when the value of proto is udp or tcp |
| timestamp_analyzed | Yes | Date and time of the alert analysis by logstash |
| timestamp_detected | Yes | Date and time suricata generated the alert |
| type | Yes | Type of event. Suricata by default |
| uuid | Yes | Unique alert identifier |
| vlan | No | Vlan identifier of the flow |

### 2.1.3.7 View the status of Sigflow

The current motor status is displayed in the *Web UI `Health checks` screen*.

#### 2.1.3.8 Sigflow update

There are updates (Updates) for the Sigflow engine.

These updates can be done manually or scheduled via GUM.

See *Presentation of GUM: dedicated module for managing updates* and in particular the part *Update signatures and/or engines (update)*.

---

#### 2.1.3.9 Sigflow Setup

The engine is configured by profiles.

For more information, see paragraph *GCAP Profiles*.

For implementation, see the *Configuring GCaps*.

---

### 2.1.4 Machine Learning engine

#### 2.1.4.1 Introduction to the DGA Algorithm

The **GCenter** embeds an engine capable of detecting domain names generated by DGAs (Domain Generation Algorithm).

The presence of DGA-generated domain names on a network is a strong indicator of being compromised.

Indeed, malware can use HTTP requests to automatically generated domain names to contact their command and control servers. They are also called CnC, C&C, or C2.

These domain names contain different properties than legitimate domain names.

Conventional detection approaches, such as blacklists, are not relevant in the case of continuously renewed domains.

Simple entropy calculations result in a large number of false positives.

The graphical interface is described in the *`Admin-GCenter- ML Management` screen of the legacy web UI*.

---

##### 2.1.4.1.1 Activation

This feature is disabled by default. It can be activated from the `ML Management` menu in the GCenter web interface (*`Admin-GCenter- ML Management` screen of the legacy web UI*).

Once activated, the domain names present in the 'dns' events captured by the GCap are analyzed by the machine learning engine.

This uses DGA detection and contextual information such as NXDomains to generate alerts.

This enables alerts to be raised on randomly generated domain names, responding to DNS queries.

Machine Learning is based on a pre-trained model, whose architecture is based on a deep neural network of the LSTM type (Long Short Term Memory networks).

**Note:**

In v102, only alerts are generated by the engine, unlike in v101 where only DNS metadata was generated.

For the implementation, refer to the paragraph *Enabling and configuring the Machine Learning engine*.

---

#### 2.1.4.1.2 Exception lists White List / Black List

Exception lists can be set up to force the engine to declare domain names as healthy (White List).
A white list enables suppressing alerts related to recurring false positives.
Conversely, a black list enables an alert to be raised for a domain that would not otherwise have been detected (false negative).

For the implementation, refer to *Managing the white and black lists of the Machine Learning engine*.

---

#### 2.1.4.1.3 Displaying DGA alerts

DGA alerts are displayed in the NDR web interface as well as in the Kibana dashboards in the **ML** section.

**Note:**

The Machine Learning engine is labelled "C&C" in the NDR web interface.

The machine learning engine enriches the information already provided by the **Sigflow** module.
Thus, for a domain that is not detected as a generated domain, the `` `dga_probability` `` field will be added.
A value close to *0* indicates a low probability the domain was generated.
On the other hand, a value close to *1* indicates that there is a good chance this domain was the result of a random generation.

**Note:**

If a GCap oversees multiple networks or if multiple GCaps oversee multiple networks, it is possible that a domain name that appears multiple times will only generate one alert.

---

#### 2.1.4.2 Events generated

The events generated by the Machine Learning engine are **alerts**.
These are displayed:

- In the main interface named **WEB UI** of the GCenter in the `` `Alerts` `` tab (the main interface named **WEB UI** is described in *Overview of the WEB UI*).

  To view the alerts, select the filter `` `C&C` `` and thus view the list of alerts: see the presentation of the *Web UI `Alerts` screen*.

  By clicking on an alert, the detailed information of this alert is displayed: see *Example of a DGA alert in the webui*.
- In the **Kibana UI** interface

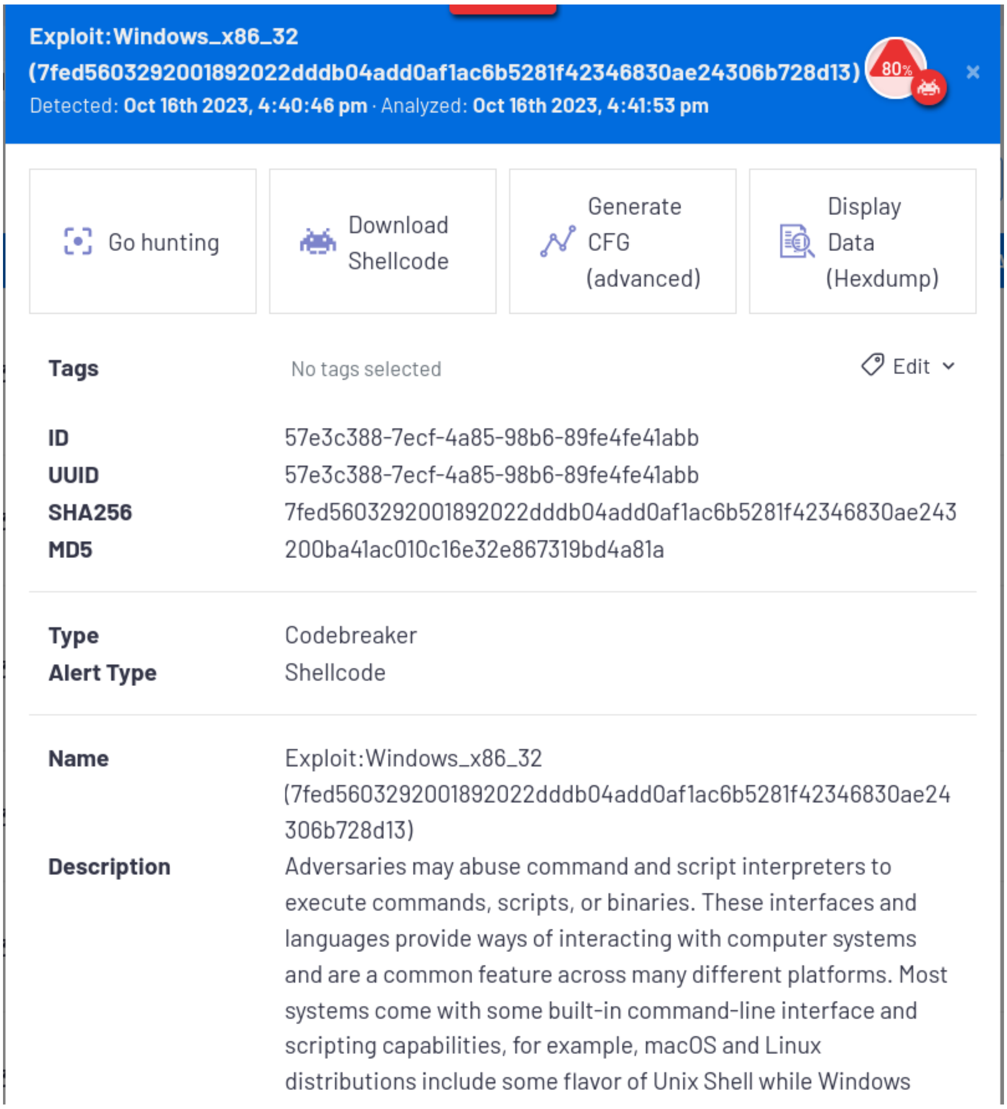
  To view the alerts, select the filter `` `C&C` `` and thus view the list of alerts: see the presentation of the *Web UI `Alerts` screen*.

  By clicking on an alert, select on the command `` `Alert details` `` then select the arrow to the left of the alert.

  The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

  The detailed information of this alert can be viewed in table or jason format (see *Example of Machine Learning log*).

#### 2.1.4.2.1 Example of a DGA alert in the webui



Exploit:Windows_x86_32 (7fed5603292001892022dddb04add0af1ac6b5281f42346830ae24306b728d13)

Detected: Oct 16th 2023, 4:40:46 pm · Analyzed: Oct 16th 2023, 4:41:53 pm

Tags No tags selected

ID 57e3c388-7ecf-4a85-98b6-89fe4fe41abb

UUID 57e3c388-7ecf-4a85-98b6-89fe4fe41abb

SHA256 7fed5603292001892022dddb04add0af1ac6b5281f42346830ae243

MD5 200ba41ac010c16e32e867319bd4a81a

Type Codebreaker

Alert Type Shellcode

Name Exploit:Windows_x86_32 (7fed5603292001892022dddb04add0af1ac6b5281f42346830ae24306b728d13)

Description Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows

The counters are detailed in *Machine learning log data structure*.

#### 2.1.4.2.2 Example of Machine Learning log

```
{
"_index": "machine_learning-2023.10.16-000169",
"_type": "_doc",
"_id": "UQ0COYsBeBoubSyguUoF",
"_version": 1,
"_score": 1,
"_source": {
  "dest_port": 53,
  "@version": "1",
  "domain_name": "nvtcvimt.com",
  "flow_id": 2099102182782245,
  "timestamp_detected": "2023-10-16T15:00:09.568Z",
  "@timestamp": "2023-10-16T15:02:41.646Z",
```

(suite sur la page suivante)

(suite de la page précédente)

```
  "type": "machine_learning",
  "dest_ip": "78.46.218.253",
  "gcenter": "gcenter-int-128-dag.gatewatcher.com",
  "probability": 0.9998979282169229,
  "timestamp_analyzed": "2023-10-16T15:02:41.646Z",
  "src_ip": "192.168.56.104",
  "src_port": 1025,
  "event_type": "dga",
  "severity": 1,
  "gcap": "gcap-int-129-dag.gatewatcher.com",
  "matched_event": "0ebe7d76-ce3b-4623-bdd1-6aa4838b4149",
  "uuid": "819423ea-d328-4c40-a998-eb022e813b19"
},
"fields": {
  "severity": [
    1
  ],
  "probability": [
    0.99989796
  ],
  "gcenter": [
    "gcenter-int-128-dag.gatewatcher.com"
  ],
  "matched_event": [
    "0ebe7d76-ce3b-4623-bdd1-6aa4838b4149"
  ],
  "type": [
    "machine_learning"
  ],
  "uuid": [
    "819423ea-d328-4c40-a998-eb022e813b19"
  ],
  "timestamp_detected": [
    "2023-10-16T15:00:09.568Z"
  ],
  "src_ip": [
    "192.168.56.104"
  ],
  "src_port": [
    1025
  ],
  "domain_name": [
    "nvtcvimt.com"
  ],
  "event_type": [
    "dga"
  ],
  "@timestamp": [
    "2023-10-16T15:02:41.646Z"
  ],
  "flow_id": [
    2099102182782245
  ],
  "dest_ip": [
    "78.46.218.253"
  ],
```

(suite sur la page suivante)

(suite de la page précédente)

```
  "@version": [
    "1"
  ],
  "gcap": [
    "gcap-int-129-dag.gatewatcher.com"
  ],
  "timestamp_analyzed": [
    "2023-10-16T15:02:41.646Z"
  ],
  "dest_port": [
    53
  ]
}
}
```

#### 2.1.4.2.3 Machine learning log data structure

The logs are composed of different parts:

- The leading part
- The source part defined by "_source"
- The field portion defined by "_fields"

##### 2.1.4.2.3.1 The header part of the Machine learning logs

The header section contains:

```
{
"_index": "machine_learning-2023.10.16-000169",
"_type": "_doc",
"_id": "UQ0COYsBeBoubSyguUoF",
"_version": 1,
"_score": 1,
```

Table18: Table header part of Machine learning logs

| Field | Required | Description | Values or example |
|---|---|---|---|
| _index | Yes | Internal index | machine_learning-2023.10.16-000169 |
| _type | Yes | default type | _doc |
| _id | Yes | internal identifier | UQ0COYsBeBoubSyguUoF |
| _version | Yes | internal version | 1 |
| _score | Yes | relevance of the response to the request | 1 |

#### 2.1.4.2.3.2 The source part of the Machine learning logs

The source part defined by "_source" contains:

```
"_source": {
  "dest_port": 53,
  "@version": "1",
  "domain_name": "nvtcvimt.com",
  "flow_id": 2099102182782245,
  "timestamp_detected": "2023-10-16T15:00:09.568Z",
  "@timestamp": "2023-10-16T15:02:41.646Z",
  "type": "machine_learning",
  "dest_ip": "x.x.x.x",
  "gcenter": "gcenter-xxx.domain.local",
  "probability": 0.9998979282169229,
  "timestamp_analyzed": "2023-10-16T15:02:41.646Z",
  "src_ip": "x.x.x.x",
  "src_port": 1025,
  "event_type": "dga",
  "severity": 1,
  "gcap": "gcap-xxx.domain.local",
  "matched_event": "0ebe7d76-ce3b-4623-bdd1-6aa4838b4149",
  "uuid": "819423ea-d328-4c40-a998-eb022e813b19"
},
```

Table19: Table source part of Machine learning logs

| Field | Required | Description | Values or example |
|---|---|---|---|
| @timestamp | Yes | Timestamp of the processing of the alert by the GCenter (corresponds to the passage in logstash) | 2023-10-16T15:02:41.646Z |
| @version | yes | Version of document | 1 |
| Alert Type in webui | Yes | alert type | C&C |
| Description (in webui) | yes | Threat description field. Only present in web ui | Adversaries can dynamically establish connections to the command and control infrastructure to evade common detections and patches. ... |
| dest_ip (or IP in webui) | Yes | Destination IP address | x.x.x.x |
| dest_port (or PORTs in webui) | No | Port of destination | 53 |
| domain_name | yes | Domain name | nvtcvimt.com |
| event_type | Yes | Type of event | dga |
| flow_id | Yes | Unique identifier of the flow. Allows to find the associated fileinfo | 2,099,102,182,782,245 |
| gcap | Yes | Name of the gcap associated with the alert | gcap-xxx.domain.local |
| gcenter | Yes | GCenter name associated with alert. | gcenter-xxx.domain.local |
| Hostname (webui) | yes | Host name of the threat originator | if the hostname is not present, its IP is displayed |
| matched_event | yes | | 0ebe7d76-ce3b-4623-bdd1-6aa4838b4149 |
| MITRE ASSOCIATIONS | yes | Threat MITRE category | Command and Control: Dynamic Resolution |

suite sur la page suivante

Table 19 – suite de la page précédente

| Field | Required | Description | Values or example |
|---|---|---|---|
| Name in webui | Yes | Sum of information of fields event_type + domain_name | DGA:vmfyaxnse.com |
| probability | yes | Likelihood of this being the identified threat | 0.9998979282169229 |
| severity | Yes | Analysis result code. | Between 0 and 3.<br>0=clean, 1=infected, 2=suspicious, 3=Other |
| src_ip (or IP in webui) | Yes | Source IP address detected by Sigflow | X.X.X.X |
| src_port (or PORTs in webui) | Yes | Source port detected by Sigflow | 1025 |
| timestamp analyzed | Yes | Date and time of last file scan | 2023-10-16T15:02:41.646Z |
| timestamp detected | Yes | Timestamp of file capture by Gcap | Oct 16, 2023 @ 17:00:09.568 |
| type | Yes | Type of event | machine_learning |
| uuid or id | Yes | Unique identifier of the alert | 819423ea-d328-4c40-a998-eb022e813b19 |

#### 2.1.4.2.3.3 The fields part of the Machine learning logs

The field part defined by "fields" contains the same counters as in the source part: refer to the source part section.

### 2.1.4.3 Viewing the state of machine learning

The current motor state is displayed in the *Web UI `Health checks` screen*.

### 2.1.4.4 Machine Learning Update

The engine does not receive an update.

### 2.1.4.5 Machine Learning Setup

The engine is not configurable but this engine must be enabled to detect DGAs (C&C) (see *`Admin-GCenter- ML Management` screen of the legacy web UI*).

### 2.1.5 Retroact engine

#### 2.1.5.1 Presentation

The Retroact engine enables the resubmission, in time, of files with malicious potential in the Malcore engine.

#### 2.1.5.2 Retroact analysis engine

The Retroact engine will store files tagged as **Suspicious** and resubmit them to the Malcore engine at regular time intervals.

Retroact's file retention policy is based on the retention time set on the GCenter.

The suspicious file is therefore re-scanned every day during the retention period.

The relevance of this engine is that it makes it possible to detect malware via Malcore even days or weeks after it has entered the network. This is thanks to the new signatures and heuristic methods of antivirus engines.

This configuration interface is described in the paragraph *`Admin-GCenter- Malcore Management` screen of the legacy web UI*.

For the implementation, refer to *Setting up GBox and the Malcore and Retroact engines and activate the GBox*.

#### 2.1.5.3 Counters associated with the Rétroact engine

The following counters are present in Malcore events:

Table20: Counters associated with the Rétroact engine

| Field | Required | Description | Values |
|---|---|---|---|
| nb_rescans | Yes | No. of analyses by Retroact | "Not reanalyzed", 1, 2 .. n |
| Retroact | Yes | Result of the Retroact analysis By default this field is set to NO<br>Only suspicious files will be re-scanned by retroact. | This field can be set to None or advanced malware,<br>if Retroact declares the file as infected |

#### 2.1.5.4 Viewing the status of Retroact

The current motor status is displayed in the *Web UI `Health checks` screen*.

#### 2.1.5.5 Retroact Update

There are updates (Updates) for the Retroact engine.
These updates can be done manually or scheduled via GUM.
See section *Presentation of GUM: dedicated module for managing updates* and in particular part *Update signatures and/or engines (update)*.

---

#### 2.1.5.6 Retroact Setup

The Retroact engine must be activated and this activation is done in the configuration screen.
The configuration GUI is described in *`Admin-GCenter- Malcore Management` screen of the legacy web UI*.
The implementation of the Retroact configuration is given in the procedure of *Setting up GBox and the Malcore and Retroact engines and activate the GBox*.

---

### 2.1.6 CTI engine, RetroHunt engine and ActiveHunt engine

#### 2.1.6.1 Presentation

The CTI engine consists of the parts:

- *CTI module*
- *Configuring the CTI engine*
- *RetroHunt engine*
- *ActiveHunt engine*

The configuration interface is described in the paragraph *`Admin-GCenter- CTI Configuration` screen of the legacy web UI*.

---

#### 2.1.6.2 CTI module

The solution's CTI module uses LastInfoSec's compromise indices to generate alerts.
The CTI module enables:

- Searching the metadata after the fact to see if the compromise indices in the CTI database correspond to malicious movements
- Generating Suricata rules in the Sigflow module on the basis of compromise indices in order to raise alerts

**Note:**

An additional license is required to activate this module. It is therefore not automatically activated in the solution.

---

#### 2.1.6.3 Configuring the CTI engine

Ideally, the index database should be updated on a daily basis in order to obtain the latest indices added by the R&D teams.

The default retention time is seven days, which is also the maximum possible value.

The CTI engine must be enabled to generate alerts for Advanced Persistent Threat (APT) threats (see *`Admin-GCenter- CTI Configuration` screen of the legacy web UI*).

---

#### 2.1.6.4 RetroHunt engine

This engine will enable searching among all the metadata present in the solution to determine whether or not they correspond to indications of compromise.

If this is the case, then an alert will be raised in the various alert display dashboards: NDR and Kibana.

The idea being that if a malicious file was not detected as such by Malcore during its analysis, because it was too recent for the Malcore antivirus database for example, then if one of the indices matches the hash of the file in question in the metadata, an alert will be raised.

> **Note:**
>
> The correlation of indices and metadata will depend on the data retention time configured on the GCenter.

Match analysis between indices and metadata is triggered when updating the index database.

It is therefore only possible to trigger the match analysis manually by updating the compromise indices manually.

There are 3 different ways to update the indices of compromise:

- Manual update with cti.gwp package
- *Online* update: the recovery of compromise indices is performed every hour based on the package posted by Gatewatcher
- *Local* update: the recovery of compromise indices is performed every hour based on the package in the local repository.

> **Note:**
>
> In order to optimize the implementation of the update of the indices of compromises in *Local*` mode, it is necessary that the local repository retrieves the package cti.gwp every hour.
>
> Otherwise the update as well as the match search will only be performed according to the recovery frequency of the package on the local deposit.

---

#### 2.1.6.5 ActiveHunt engine

This engine will enable generating a source of Suricata rules available to the Sigflow module based on the compromise indices.

This source can then be added to the security policy (ruleset) assigned to the GCap in order to raise alerts on the analysed traffic.

This engine is positioned in real time, unlike the Retrohunt engine above, which scans for matches in the past.

The rules generated are updated at the same time as the database of compromise indicators, every day if possible.

> **Note:**
>
> Unlike the RetroHunt engine, the alerts generated are of the Suricata type. They will therefore be available in the Sigflow dashboards.

---

#### 2.1.6.6 Events generated by the RetroHunt engine

Events generated by the RetroHunt engine are **alerts**.

These are displayed:

- In the main interface named **WEB UI** of the GCenter in the `` `Alerts` `` screen (the main interface named **WEB UI** is described in:doc:*../../05_GUI_presentation/00_00_interface_presentation*).

  To view the alerts, select the filter `` `APT` `` and thus view the list of alerts: see the presentation of the *Web UI `Alerts` screen*.

  By clicking on an alert, the detailed information of this alert is displayed: see *Example of RetroHunt alert in the webui*.
- In the **Kibana UI** interface

  To view the alerts, select the filter `` `C&C` `` and thus view the list of alerts: see the presentation of the *Web UI `Alerts` screen*.

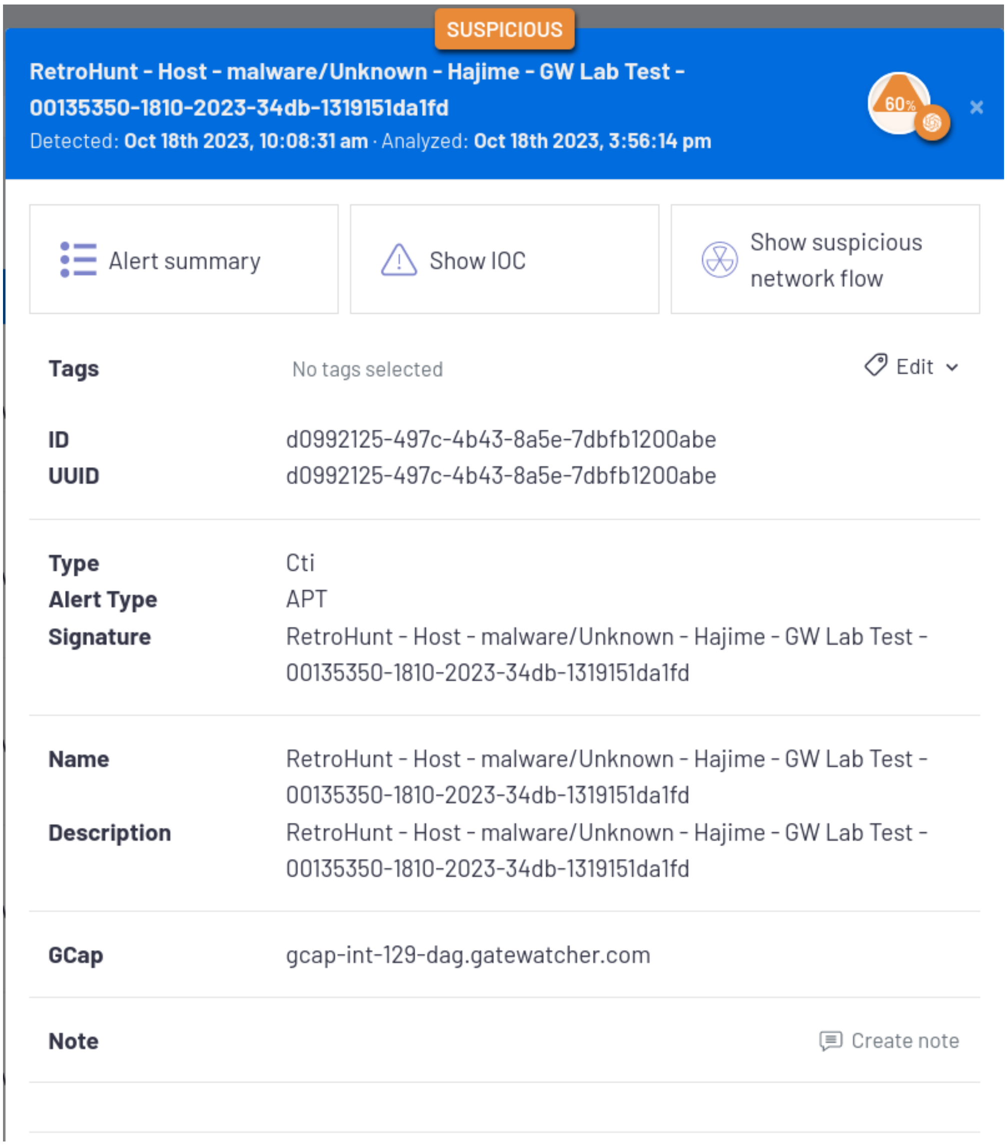
  By clicking on an alert, select on the command `` `Alert details` `` then select the arrow to the left of the alert.

  The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

  The detailed information of this alert can be viewed in table or jason format (see *Example of Machine Learning log*).

---

#### 2.1.6.6.1 Example of RetroHunt alert in the webui



SUSPICIOUS

RetroHunt - Host - malware/Unknown - Hajime - GW Lab Test - 00135350-1810-2023-34db-1319151da1fd

Detected: Oct 18th 2023, 10:08:31 am · Analyzed: Oct 18th 2023, 3:56:14 pm

| | |
|---|---|
| Tags | No tags selected |
| ID | d0992125-497c-4b43-8a5e-7dbfb1200abe |
| UUID | d0992125-497c-4b43-8a5e-7dbfb1200abe |
| Type | Cti |
| Alert Type | APT |
| Signature | RetroHunt - Host - malware/Unknown - Hajime - GW Lab Test - 00135350-1810-2023-34db-1319151da1fd |
| Name | RetroHunt - Host - malware/Unknown - Hajime - GW Lab Test - 00135350-1810-2023-34db-1319151da1fd |
| Description | RetroHunt - Host - malware/Unknown - Hajime - GW Lab Test - 00135350-1810-2023-34db-1319151da1fd |
| GCap | gcap-int-129-dag.gatewatcher.com |
| Note | |

The counters are detailed in *RetroHunt log data structure*.

### 2.1.6.7 Example of a RetroHunt event

```
{
"_index": "retrohunt-2023.10.18-000171",
"_type": "_doc",
"_id": "6BESQ4sBeBoubSygpp1s",
"_version": 1,
"_score": 1,
"_source": {
  "flow_id": 1540796205479447,
  "@timestamp": "2023-10-18T13:56:14.789Z",
  "kill_chain_phases": [],
  "gcenter": "gcenter-xxx.domain.local"
  "signature": "RetroHunt - Host - malware/Unknown - Hajime - GW Lab Test - 00135350-1810-
```

(suite sur la page suivante)

(suite de la page précédente)

```
↪2023-34db-1319151da1fd",
  "src_ip": "X.X.X.X",
  "event_type": "retrohunt",
  "case_id": "00135350-1810-2023-edb7-7f8f1e4fccb9",
  "ioc_tags": [
    "trojan.generickd.34055387 (b)",
    "linux/hajime.a trojan",
    "e32/agent.cd",
    "linux.hajime.bc",
    "backdoor.hajime.linux.129",
    "linux/hajime.75930",
    "unix.malware.agent-6626471-0",
    "linux/hajime.nsnlw",
    "hajime",
    "elf.mirai.43048.gc",
    "trojan.elfarm32.hajime.fbhtfi",
    "trojan.linux.hajime",
    "trojan.generickd.34055387"
  ],
  "families": [
    "Hajime"
  ],
  "targeted_platforms": [
    "linux"
  ],
  "risk": "Suspicious",
  "categories": [
    "malware"
  ],
  "campaigns": [],
  "@version": "1",
  "threat_actor": [
    "GW Lab Test"
  ],
  "timestamp_detected": "2023-10-18T08:08:31.112Z",
  "ioc_value": "im.a.very.bad.doma.in",
  "external_links": [
    {
      "source_name": "URLHaus Abuse.ch",
      "url": "https://urlhaus.abuse.ch/url/2269068/"
    }
  ],
  "gcap": "gcap-xxxxxxxxx.domain.local",
  "uuid": "19fe0b3d-05fb-433a-ada0-f246e284d9bd",
  "dest_port": 80,
  "ioc_id": "00135350-1810-2023-34db-1319151da1fd",
  "ttp": [],
  "targeted_sectors": [],
  "meta_data": {
    "cwe": [],
    "ssdeep":
↪"1536:87vbq1lGAXSEYQjbChaAU2yU23M51DjZgSQAvcYkFtZTjzBht5:8D+CAXFYQChaAUk5ljnQssL",
    "descriptions": [],
    "usageMode": "hunting",
    "filetype": "ELF 32-bit LSB executable, ARM, EABI5 version 1 (GNU/Linux)",
    "size": 78.3984375,
```

(suite sur la page suivante)

(suite de la page précédente)

```
    "tslh": "T16D7312E017B517CC1371A8353BED205E9128223972AE35302E97528DF957703BAB2DBE"
  },
  "type": "cti",
  "ioc_creation_date": "2023-10-18T13:53:50+00:00",
  "timestamp_analyzed": "2023-10-18T13:56:14.789Z",
  "targeted_organizations": [],
  "matched_event_type": "http",
  "ioc_updated_date": "2023-10-18T13:53:50+00:00",
  "severity": 1,
  "matched_event": "cf7cf312-883b-4b84-a530-fea8d49b294c",
  "community_id": "1:oPgJrwIH53r44+0TfDB+7uhzL50=",
  "vulnerabilities": [],
  "targeted_countries": [],
  "timestamp_package": "2023-10-18T13:53:50.696659+0000",
  "description": "IOC matching first tests",
  "relations": [
    "0e3cc27b-7999-48ce-8484-dc12b325a355"
  ],
  "": 0.5,
  "dest_ip": "X.X.X.X",
  "src_port": 59338,
  "tlp": "green",
  "usage_mode": "hunting",
  "ioc_type": "Host"
},
"fields": {
  "signature": [
    "RetroHunt - Host - malware/Unknown - Hajime - GW Lab Test - 00135350-1810-2023-34db-1319151da1fd"
  ],
  "usage_mode": [
    "hunting"
  ],
  "description": [
    "IOC matching first tests"
  ],
  "type": [
    "cti"
  ],
  "uuid": [
    "19fe0b3d-05fb-433a-ada0-f246e284d9bd"
  ],
  "meta_data.ssdeep": [
    "1536:87vbq1lGAXSEYQjbChaAU2yU23M51DjZgSQAvcYkFtZTjzBht5:8D+CAXFYQChaAUk5ljnQssL"
  ],
  "src_ip": [
    "172.17.0.6"
  ],
  "ioc_updated_date": [
    "2023-10-18T13:53:50.000Z"
  ],
  "community_id": [
    "1:oPgJrwIH53r44+0TfDB+7uhzL50="
  ],
  "event_type": [
    "retrohunt"
```

(suite sur la page suivante)

(suite de la page précédente)

```
  ],
  "ioc_tags": [
    "trojan.genericKd.34055387 (b)",
    "linux/hajime.a trojan",
    "e32/agent.cd",
    "linux.hajime.bc",
    "backdoor.hajime.linux.129",
    "linux/hajime.75930",
    "unix.malware.agent-6626471-0",
    "linux/hajime.nsnlw",
    "hajime",
    "elf.mirai.43048.gc",
    "trojan.elfarm32.hajime.fbhtfi",
    "trojan.linux.hajime",
    "trojan.genericKd.34055387"
  ],
  "flow_id": [
    1540796205479447
  ],
  "case_id": [
    "00135350-1810-2023-edb7-7f8f1e4fccb9"
  ],
  "@version": [
    "1"
  ],
  "external_links.url": [
    "https://urlhaus.abuse.ch/url/2269068/"
  ],
  "categories": [
    "malware"
  ],
  "meta_data.usageMode": [
    "hunting"
  ],
  "matched_event_type": [
    "http"
  ],
  "dest_port": [
    80
  ],
  "severity": [
    1
  ],
  "targeted_platforms": [
    "linux"
  ],
  "meta_data.filetype": [
    "ELF 32-bit LSB executable, ARM, EABI5 version 1 (GNU/Linux)"
  ],
  "": [
    0.5
  ],
  "meta_data.size": [
    78.39844
  ],
  "gcenter": [
```

(suite sur la page suivante)

(suite de la page précédente)

```
    "gcenter-int-128-dag.gatewatcher.com"
  ],
  "meta_data.tslh": [
    "T16D7312E017B517CC1371A8353BED205E9128223972AE35302E97528DF957703BAB2DBE"
  ],
  "matched_event": [
    "cf7cf312-883b-4b84-a530-fea8d49b294c"
  ],
  "ioc_value": [
    "im.a.very.bad.doma.in"
  ],
  "ioc_id": [
    "00135350-1810-2023-34db-1319151da1fd"
  ],
  "ioc_type": [
    "Host"
  ],
  "families": [
    "Hajime"
  ],
  "timestamp_detected": [
    "2023-10-18T08:08:31.112Z"
  ],
  "external_links.source_name": [
    "URLHaus Abuse.ch"
  ],
  "src_port": [
    59338
  ],
  "threat_actor": [
    "GW Lab Test"
  ],
  "@timestamp": [
    "2023-10-18T13:56:14.789Z"
  ],
  "ioc_creation_date": [
    "2023-10-18T13:53:50.000Z"
  ],
  "dest_ip": [
    "172.17.0.4"
  ],
  "tlp": [
    "green"
  ],
  "risk": [
    "Suspicious"
  ],
  "gcap": [
    "gcap-int-129-dag.gatewatcher.com"
  ],
  "timestamp_analyzed": [
    "2023-10-18T13:56:14.789Z"
  ],
  "timestamp_package": [
    "2023-10-18T13:53:50.696Z"
  ],
```

(suite sur la page suivante)

(suite de la page précédente)

```
   "relations": [
     "0e3cc27b-7999-48ce-8484-dc12b325a355"
   ],
   "description.keyword": [
     "IOC matching first tests"
   ]
 }
}
```

### 2.1.6.7.1 RetroHunt log data structure

The logs are composed of different parts:

- The leading part
- The source part defined by "_source";
- The field portion defined by "_fields"

### 2.1.6.7.1.1 The header part of RetroHunt logs

The header section contains:

```
{
 "_index": "retrohunt-2023.10.18-000171",
 "_type": "_doc",
 "_id": "6BESQ4sBeBoubSygpp1s",
 "_version": 1,
 "_score": 1,
```

Table21: Table header part of Machine learning logs

| Field | Required | Description | Values or example |
|---|---|---|---|
| _index | Yes | Internal index | retrohunt-2023.10.18-000171 |
| _type | Yes | default type | _doc |
| _id | Yes | internal identifier | 6BESQ4sBeBoubSygpp1s |
| _version | Yes | internal version | 1 |
| _score | Yes | relevance of the response to the request | 1 |

### 2.1.6.7.1.2 The source part of the Machine learning logs

The source part defined by "_source" contains:

```
  "flow_id": 1540796205479447,
  "@timestamp": "2023-10-18T13:56:14.789Z",
  "kill_chain_phases": [],
  "gcenter": "gcenter-xxx.domain.local"
  "signature": "RetroHunt - Host - malware/Unknown - Hajime - GW Lab Test - 00135350-
↪1810-2023-34db-1319151da1fd",
```

(suite sur la page suivante)

(suite de la page précédente)

```
  "src_ip": "X.X.X.X",
  "event_type": "retrohunt",
  "case_id": "00135350-1810-2023-edb7-7f8f1e4fccb9",
  "ioc_tags": [
    "trojan.generickd.34055387 (b)",
    "linux/hajime.a trojan",
    "e32/agent.cd",
    "linux.hajime.bc",
    "backdoor.hajime.linux.129",
    "linux/hajime.75930",
    "unix.malware.agent-6626471-0",
    "linux/hajime.nsnlw",
    "hajime",
    "elf.mirai.43048.gc",
    "trojan.elfarm32.hajime.fbhtfi",
    "trojan.linux.hajime",
    "trojan.generickd.34055387"
  ],
  "families": [
    "Hajime"
  ],
  "targeted_platforms": [
    "linux"
  ],
  "risk": "Suspicious",
  "categories": [
    "malware"
  ],
  "campaigns": [],
  "@version": "1",
  "threat_actor": [
    "GW Lab Test"
  ],
  "timestamp_detected": "2023-10-18T08:08:31.112Z",
  "ioc_value": "im.a.very.bad.doma.in",
  "external_links": [
    {
      "source_name": "URLHaus Abuse.ch",
      "url": "https://urlhaus.abuse.ch/url/2269068/"
    }
  ],
  "gcap": "gcap-xxxxxxxxx.domain.local",
  "uuid": "19fe0b3d-05fb-433a-ada0-f246e284d9bd",
  "dest_port": 80,
  "ioc_id": "00135350-1810-2023-34db-1319151da1fd",
  "ttp": [],
  "targeted_sectors": [],
  "meta_data": {
    "cwe": [],
    "ssdeep":
↪"1536:87vbq1lGAXSEYQjbChaAU2yU23M51DjZgSQAvcYkFtZTjzBht5:8D+CAXFYQChaAUk5ljnQssL",
    "descriptions": [],
    "usageMode": "hunting",
    "filetype": "ELF 32-bit LSB executable, ARM, EABI5 version 1 (GNU/Linux)",
    "size": 78.3984375,
    "tslh": "T16D7312E017B517CC1371A8353BED205E9128223972AE35302E97528DF957703BAB2DBE
```

(suite sur la page suivante)

(suite de la page précédente)

```
↪"
  },
  "type": "cti",
  "ioc_creation_date": "2023-10-18T13:53:50+00:00",
  "timestamp_analyzed": "2023-10-18T13:56:14.789Z",
  "targeted_organizations": [],
  "matched_event_type": "http",
  "ioc_updated_date": "2023-10-18T13:53:50+00:00",
  "severity": 1,
  "matched_event": "cf7cf312-883b-4b84-a530-fea8d49b294c",
  "community_id": "1:oPgJrwIH53r44+0TfDB+7uhzL50=",
  "vulnerabilities": [],
  "targeted_countries": [],
  "timestamp_package": "2023-10-18T13:53:50.696659+0000",
  "description": "IOC matching first tests",
  "relations": [
    "0e3cc27b-7999-48ce-8484-dc12b325a355"
  ],
  "": 0.5,
  "dest_ip": "X.X.X.X",
  "src_port": 59338,
  "tlp": "green",
  "usage_mode": "hunting",
  "ioc_type": "Host"
},
```

Table22: Table part source

| Field | Required | Description | Values or example |
|---|---|---|---|
| @timestamp | Yes | Timestamp of the processing of the alert by the GCenter (corresponds to the passage in logstash) | "2023-10-18T13:56:14.789Z" |
| "@version" | yes | version of document | 1 |
| @"case_id" | yes | Internal identification number | "00135350-1810-..." |
| Alert type in webui | Yes | Threat Type | APT |
| "campaigns" | yes | Campaign name | |
| "categories" | yes | threat category | malware |
| "community_id" | yes | Unique id to correlate the rise between the different security equipment | 1:oPgJrwIH53r44+0TfDB+7uhzL50= |
| "description" | yes | Threat description field | IOC matching first test |
| "dest_ip" | Yes | Destination IP address | x.x.x.x |
| "dest_port" | No | Port of destination | 80 |
| "event_type" | Yes | type of event | retrohunt |
| "external_links" | No | See the summary table of the "external_links" category counters | |
| "families" | yes | Threat family | Hajime |
| "flow_id" | Yes | Unique identifier of the flow. Allows to find the associated fileinfo | 1540796205479447 |
| "gcap" | Yes | Name of the gcap associated with the alert | gcap-xxx.domain.local |
| "gcenter" | yes | GCenter name associated with alert. | gcenter-xxx.domain.local |
| Hostname (webui) | yes | Host name of the threat originator | If the hostname is not present, its IP or domain name is displayed |

suite sur la page suivante

Table 22 – suite de la page précédente

| Field | Required | Description | Values or example |
|---|---|---|---|
| "ioc_creation_date" | yes | Index of Compromission; creation date in the database | "2023-10-18T13:53:50+00:00" |
| "ioc_id" | yes | Indice of Compromission: identifier | "00135350-1810-2023-34db-1319151da1fd" |
| "ioc_tags" | Yes | Compromise index: label | "trojan.generickd.34055387 (b)"<br>"linux/hajime. a trojan"<br>"e32/agent.cd" |
| "ioc_type" | yes | Compromise index: type | "Host" |
| "ioc_updated_date" | yes | Compromission index: update date | "2023-10-18T13:53:50+00:00" |
| "ioc_value" | yes | Compromise index: value | "im.a.very.bad.doma.in" |
| "kill_chain_phases" | yes | Phases of the strike chain; | |
| "matched_event" | yes | Corresponding event | cf7cf312-883b-4b84... |
| "matched_event_type" | yes | Type of event that matched | http |
| "meta_data" | yes | See Summary table of counters: category "meta_data" | NA |
| "probability" | yes | Probability | 0.5 |
| "relations" | yes | Relations | 0e3cc27b-7999-... |
| "risk" | yes | Threat risk assessment outcome | Suspicious |
| "severity" | Yes | Analysis result code | Between 0 and 3<br>0=clean, 1=infected, 2=suspicious, 3=Other |
| "signature" (or Signature or Description in Webui) | yes | Title of the threat | "RetroHunt - Host - malware/Unknown - Hajime - GW Lab Test - 00135350-1810-2023-34db-1319151da1fd" |
| "src_ip" | Yes | Source IP address | X.X.X.X |
| "src_port" | Yes | Source port | 59338 |
| "targeted_countries" | yes | Target countries | |
| "targeted_organizations" | yes | Targeted organisations; | |
| "targeted_platforms" | yes | Target platforms | linux |
| "targeted_sectors" | yes | Targeted sectors of activity | |
| "threat_actor" | yes | Actors of this threat | |
| "timestamp analyzed" | Yes | Date and time of last file scan | 2023-10-18T13:56:14.789Z |
| "timestamp detected" | Yes | Date and time of first file capture | 2022-09-08T09:21:22.223Z |
| "timestamp_package" | Yes | Date and time of update of CTI sources | 2023-10-18T13:53:50.696659+0000 |
| "tlp" | yes | Traffic Light Protocol (4 colours depending on disclosure limitation) | green. this means "limited disclosure, beneficiaries can disseminate it within their community." |
| "ttp" | yes | Trusted Third Party | |
| "type" | Yes | Type of event | "cti" |
| "use_mode" | yes | Mode of use | hunting |
| "uuid" | Yes | Unique identifier of the alert | 19fe0b3d-05fb-433a... |
| "vulnerabilities" | yes | Vulnerabilities | |

Table23: Summary table of counters: category "external_links"

| Field | Required | Description | Values or example |
|---|---|---|---|
| "source_name" | yes | Name of source | "URLHaus Abuse.ch" |
| "descriptions" | yes | Description | |
| "url" | yes | URL | "https://urlhaus.abuse.ch/url/2269068/ |

Table24: Summary table of counters: category "meta_data"

| Field | Required | Description | Values or example |
|---|---|---|---|
| "cwe" | yes | Common weakness enumeration | |
| "Descriptions" | yes | description | yes |
| "usageMode" | yes | Use of this IOC | hunting |
| "threadype": | yes | File type | ELF 32-bit LSB executable, ARM, EABI5 version 1 (GNU/Linux) |
| "size" | yes | Pruning | 78.3984375 |
| "ssdeep" | yes | Hash calculated by ssdeep | 1536:87vbq1lGAXSEYQjbChaAU.. |
| "s" | yes | | T16D7312E017B517CC1371A8... |

#### 2.1.6.7.1.3 The fields part of the RetroHunt logs

The field part defined by "fields" contains the same counters as in the source part: refer to the source part section.

### 2.1.6.8 Viewing the CTI Status

The current motor status is displayed in the *Web UI `Health checks` screen*.

### 2.1.6.9 CTI Update

There are updates (Updates) for the CTI engine.
These updates can be done manually or scheduled via GUM.
See section *Presentation of GUM: dedicated module for managing updates* and in particular part *Update signatures and/or engines (update)*.

## 2.1.7 Detection by GScan

GScan allows you to manually submit files for analysis.
The following options are possible:

- Malware: submit files to the Malcore engine
- Powershell: scans files containing Powershell scripts and detects potential threats that can serve as a gateway to install malware on Windows.

With regard to malicious powershells, detection is based on a supervised machine learning model, and on the fact that these scripts generally use offuscation techniques or that are similar to them (base64, concatenation, type conversion, etc.).

- Shellcode: submits files for analysis by the codebreaker detection engine.

Before starting an analysis, it is necessary to check the type of analysis to be performed, see above.
To start parsing a file, simply drag the file into the `` `DRAG and DROP or CLICK TO SELECT YOUR FILES` `` area or click on this area to send the suspicious file.
The result of the analysis is then displayed in a thumbnail with the status of the file for each type of analysis chosen.
The `` `SCAN HISTORY` `` page displays the history of the analyses performed.

**Note:**

Attention the maximum file size should not exceed 10MB by default.
There is no limitation on the number of file scans.

Concerning the compressed files analyzed by Malcore:

- The number of files contained in an archive is:

- limited
- editable (50 is the default)

- The number of times the file is compressed is:

- limited (max recursion level)
- editable (5 is the default)

- If files are password protected, the password must be declared in the global settings.

These settings are only accessible to members of the administrator group.
See procedure for *Setting up GBox and the Malcore and Retroact engines and activate the GBox*.

- Modify if necessary the maximum size of files sent to Gscan (MB)
- Modify if necessary the maximum recursion level for archives sent to Gscan
- Modify if necessary the maximum number of archive files sent to Gscan

The GUI is described in *Web UI `GScan` screen*.
For implementation, see the *Detection procedure by Gscan*.

## 2.2 Management of the GCenter software

### 2.2.1 Presentation of GUM: dedicated module for managing updates

Updates are managed via the module named **GUM** (**G** atewatcher **U** pdate **M** anager).
GUM enables:

- Installation of **Upgrades**: these are the **GCenter or GCaps upgrades** (operation to be done manually)
- Installation of **Updates**: these are **updates of detection signatures and/or anti-viral engines**
  The installation process can be manual or scheduled.
- Installation of **Hotfix**: these are the **manual patches that modify the equipment without having to perform a complete upgrade**
- Package planning configuration **Update**
  For more information, see *GUM Setup*.

The management of updates is indicated in *Release note*.
The various existing updates are:

| Update type | To do what? | How | See for more information | See procedure |
|---|---|---|---|---|
| Upgrade | Upgrade version | Manually | *Upgrade* | *Installing of an upgrade* |
| Update | Update detection signatures and/or anti-viral motors | Manually | *Update signatures and/or engines (update)* | *Manual installation of an update of signatures and/or anti-viral engines (update)* |
| | | Automatically | | *Configuring automatic update via GUM* |
| Hotfix | Patch Application | Manually | *Applying a patch (Hotfix)* | *Installing a hotfix* |

**Note:**

Sigflow engine updates and version upgrades for a GCap are managed from the GCenter.

### 2.2.2 Upgrade

The upgrade (or upgrade) is a version upgrade and significantly changes the GCenter and GCap.

**Note:**

It is necessary for the administrator to read the Release Note before performing a version upgrade.

When applying a version upgrade to GCenter, it will be necessary to restart the GCenter manually at the end of the operation.
For a GCap version upgrade, simply load the version upgrade package into the GCenter. The rest of the actions will be on the GCap side (See GCap documentation.)

An upgrade increments the version number such as 2.3.5.101 to 2.3.5.102.

**Note:**

Upgrades are done manually by the administrator; no automation is possible in the GUM menu.

**Note:**

There are also upgrade packages that include hotfix fixes directly.
This allows you not to have to apply all hotfix after installing an appliance.

The GUI is described in the paragraph (see *`Admin-GUM- Software update` screen of the legacy web UI*).
For implementation, see the *Installing of an upgrade*.

---

#### 2.2.2.1 Minor update case

For example, when moving from v2.3.5.101 to 2.3.5.101-hf1, there are two ways to perform the system update:

- applying only the HF1 patch
- applying an upgrade

These two solutions are equivalent.

---

#### 2.2.2.2 In the case of a major update

For example, for the transition from v2.3.5.101 to 2.3.5.102, only the upgrade is applicable.
For implementation, see the *Installing of an upgrade*.

---

#### 2.2.2.3 Upgrade path

The general rule for update paths is that it is necessary to be on the last patch before performing a version upgrade.
Otherwise, this will be notified in the Release Note of the relevant version.

---

### 2.2.3 Update signatures and/or engines (update)

Updates apply to GCenter and GCap.
There are several types of update packages:

- malcore package: this package contains only engine and antivirus database updates used by Malcore
- dga package: this package contains updates to the gdgadetect engine
- cti package: this package contains CTI engine updates
- sigflow package: this package contains only Sigflow engine and rule base updates
- full package (full): this package is the sum of the previous packages

These packages can be installed as follows:

- *Update Manual*
- *Update automatic*

#### 2.2.3.1 Update Manual

The manual update is suitable for isolated environments.
The administrator must first manually download the update packages to an administration workstation and then upload them to the GCenter via the web interface.

> **Note:**
>
> The cti.gwp package is updated hourly on update.gatewatcher.com The other packages dga.gwp, malcore.gwp, sigflow.gwp, and full.gwp are updated daily.

In this case, the GUI to be used is described in *`Admin-GUM- Threat DB update` screen of the legacy web UI*.
For manual installation, see *Manual installation of an update of signatures and/or anti-viral engines (update)*.

#### 2.2.3.2 Update automatic

They can be carried out in different ways according to the needs of the information system:

- *Update Online*
- *Update Local*

This schedule must be configured.
This configuration is described in paragraph *GUM Setup*.
The GUI to be used is described in *`Admin- GUM - Config` screen of the legacy web UI*.
For planning implementation, refer to *Configuring automatic update via GUM*.

#### 2.2.3.2.1 Update Online

The **Online** update automates updates and reduces administration tasks.
Updates are done automatically from https://update.gatewatcher.com/ and https://gupdate.GATEWATCHER.com.

> **Note:**
>
> In the case of scheduled **Online** mode, the schedule only applies to the **Sigflow** engine.
> Engine updates **Malcore** are performed every 24 hours.

---

#### 2.2.3.2.2 Update Local

In order to meet specific security constraints, the **GCenter** is able to fetch its updates from a local repository.
The steps for setting up a local repository are as follows:

- Prerequisites: a listening web server on port 80
- Create the following tree structure: "2.5.3.10X/GCenter" according to the GCenter version (2.5.3.102).
  In the following configuration example, this tree should be created at the root of the server.
- Retrieve gwp files (cti.gwp, dga.gwp, malcore.gwp, sigflow.gwp for the 2.5.3.102) on https://update.gatewatcher.com/update/
- In "2.5.3.10X/GCenter", put the previously recovered gwp files
- In "2.5.3.10X/GCenter", put the files . sha256 corresponding to the files above

> **Note:**
>
> The cti.gwp package is updated hourly on update.gatewatcher.com The other packages dga.gwp, malcore.gwp, sigflow.gwp are updated every day. It is not possible to download the full.gwp file in automatic mode

> **Note:**
>
> Before a version upgrade, it is strongly recommended to update the local repository tree by adding a folder with the name of the new version.
> If this is not the case, the equipment will no longer be able to update and this will cause errors during automatic updates.

---

### 2.2.4 Applying a patch (Hotfix)

The hotfix allows you to apply one or more patches without having to perform a complete upgrade of the equipment.
Therefore, restart is not necessary.
Applying a patch should be done in the order (for example v102 -> v102-hf1 -> v102-hf2 -> ...).

**Note:**

In most cases, patches will not require a restart of the web service.

The GUI is described in *`Admin-GUM- Software update` screen of the legacy web UI*.
For implementation, see the *Installing a hotfix*.

---

### 2.2.5 GUM Setup

The configuration of GUM is to configure the scheduling of update packages (**updates**).
The items to be configured are:

- Enabling this functionality
- The update mode
- Planning information (day, time and frequency)
- The address of the repository where packages are downloaded
- Authentication of access to this repository

The GUI is described in *`Admin- GUM - Config` screen of the legacy web UI*.
For implementation, see the *Configuring automatic update via GUM*.

---

#### 2.2.5.1 Different modes of updates

Modes can be:

- Update type **Online**: packages are downloaded directly from GATEWATCHER websites
- Update type **Local**: packages are downloaded from a local repository

---

#### 2.2.5.1.1 Update type Online

The **Online** update is done automatically from https://update.gatewatcher.com/ and https://gupdate.gatewatcher.com.

---

#### 2.2.5.1.2 Update type Local

In order to meet specific security constraints, the GCenter can load its updates from a local repository previously configured to receive packets.
This local repository is defined in *`Admin- GUM - Config` screen of the legacy web UI*.

---

### 2.2.6 Release note

The Release Notes contain the list of changes made by the given version, the list of known issues but also important notes related to the upgrade process.
Release Notes are referenced in the following table.

| Version | Release Notes |
|---|---|
| 2.5.3.100 | https://releases.gatewatcher.com/fr/gcenter/2.5.3/100/ |
| 2.5.3.101 | https://releases.gatewatcher.com/fr/gcenter/2.5.3/101/ |
| 2.5.3.102 | https://releases.gatewatcher.com/fr/gcenter/2.5.3/102/ |

---

### 2.2.7 Overview of the backup and restoration

The **Backup/Restore** component of the GCenter enables you to:

- Backup the entire configuration (format .gwc)
- Restore the configuration

**Attention:**

There is no specificity in terms of choosing what to backup or restore. The entire backup will be restored.

The saved elements are:

- For the Sigflow engine:

- The sources
- The rulesets
- Ruleset changes (suppress, threshold, etc.)

- For the GCaps:
  - All GCaps and what allows their pairing: after the restore, if the GCaps are UP and correctly configured, the tunnels must be established
  - The entire configuration of each GCap:

  - Detection rulesets
  - Variable base
  - Net variables
  - Flow timeouts
  - File rule management
  - Packet filters

- Operator group parameters of NDR:

- Asset detection network range
- Static IP-Asset mapping
- Ignored IP for users association
- Ignored MAC for assets association

- Administrator group parameters of NDR (feature activation and retention time):
- The backup server configuration
- The data export configurations
- DGA configuration (activation/white list/black list)
- The Malcore configuration (global settings / white list/black list)
- Configuration of third party modules
- User list, LDAP settings, API keys and password policy
- All parameters of the "configuration" menu, except for the license (see specific point for licenses below)
- CTI parameters and LIS license
- The parameters og GUM configuration

**Note:**

The size of the backup file is larger than in earlier GCenter versions due to the presence of the NDR data.

You can select how many backups should be kept on the GCenter.
The default value is 3 and the maximum is 10.

The backup can be scheduled on a regular basis:

- On a daily basis with a choice of time
- Once a week with a choice of time and day of the week
- Once a month with a choice of time and day of the month

The various types of backup available are as follows:

- \``Local`\`: for a direct backup on the GCenter.
- \``SCP`\`: enables eternalizing the backup to a remote SSH server.
- \``FTP`\` enables eternalizing the backup to a remote FTP server.

When backing up in SCP or FTP mode, the configuration is exported to the remote server. However, a copy is also kept in the list of local backups.
It is important to note that when restoring a backup, the GCenter will automatically restart at the end of the operation.
In the event the restoration must be done on a new machine, certain requirements must be met:

- The GCenter network configuration must be the same (same FQDN, same number of enabled network interfaces)
- The version of the GCenter that restores must be the same as the version that saved it.

**Important:**

If the previous GCenter was installed in v102 and 2 hotfixes were applied manually, this order must be respected when reinstalling the new GCenter.
If the latest version of the GCenter including the 2 hotfixes is installed, the path will not be identical and restoring will be impossible.

**Note:**

In the case of a reinstallation or reset of the **GCenter**, it will be necessary to enter a license in order to access the **Restore** menu

The graphical interface that manages the backup restore configuration is described in *`Admin-Backup/Restore - Configuration` screen of the legacy web UI*.
The graphical interface for using backup restore is described in *`Admin-Backup/Restore - Operations` screen of the legacy web UI*.

To configure the backup, see *Backup configuration*.
To perform a backup, see *Backup*.
To carry out a restore, see *Restoration*.

---

## 2.3 Data use

The **GCenter** server works with log files.
These log files record all the traffic captured by the **GCap** probe as well as the information from the GScan.
The data created by the GCap and GCenter is of various types:

- *Detection data*
- *Data related to detection results*
- *Management and system status data*

This data can, if necessary, be managed by the administrator.
This management involves:

- Managing and modifying if necessary the *Data retention*
- *Deleting data*

---

### 2.3.1 Detection data

In addition to dashboards present from the GCenter web interface, it is possible to use external equipment using the syslog protocol ( such as a SIEM), in order to exploit the data reported by the solution.

#### 2.3.1.1 Export des données via le protocole Syslog

The GCenter offers administrators the option of configuring up to two data exports to different destinations.
Data can be exported to a SIEM for example.
Once an export is activated, all selected data will be sent to the configured destination.
It is of course possible for the administrator to choose which data they wish to export.

**Note:**

When referring to exported data, only "alert" and "metadata" type data are concerned.
No GCenter or GCap system log file is concerned by this export.

For more information, see the presentation in the *`Admin-GCenter- Data exports` screen of the legacy web UI*.

### 2.3.2 Data related to detection results

The data providing the results of the detection, i.e. the information related to the threats, is processed in the GCenter and displayed in the form of dashboards:

- Dashboards **synthetic**
  These are managed by the WEB User Interface.
  For more information, see *Overview of the WEB UI*.
- Dashboards **complete**
  These are managed by the Kibana interface.
  For more information, see *Overview of the Kibana GUI*.

### 2.3.3 Management and system status data

This data enables the following functions:

- *Viewing the system status*
- *Export system state data to remote servers*
- *System management and configuration*

#### 2.3.3.1 Viewing the system status

- **Legacy WEB** GUI:
  System status data is managed through the legacy WEB UI.
  For more information, see the *Overview of the traditional WEB UI (legacy WEB UI)*.
- **Gstats** GUI
  System state data is also managed by Netdata services.
  Specifically, each GCap has a Netdata service that sends its information to the Netdata server located in the GCenter.
  Similarly, GCenter has a Netdata service that sends its information to the internal Netdata server at GCenter.
  The GCenter internal Netdata server allows the display of this data via the Gstats graphical interface.
  For more information, see *Overview of the Netdata User Interface*.

---

#### 2.3.3.2 Export system state data to remote servers

##### 2.3.3.2.1 Export data to a Netdata server

In addition to the Netdata interface used for Gstats, the GCenter has another Netdata export interface whose purpose is to export data to an external server.
It must be configured: for more information, see the presentation of the *`Admin-GCenter-Configuration` screen of the legacy web UI*.
For implementation, see the *Configuring the Netdata export interface*.

---

##### 2.3.3.2.2 Data retrieval by a Nagios server

For more information, see the presentation in the *`Admin-GCenter-Configuration` screen of the legacy web UI*.

---

#### 2.3.3.3 System management and configuration

System management, in particular configuration, is carried out via:

- The configuration menu
  For more information, see *Presentation of the configuration menu*.
- Configuration options managed by the traditional web interface
  For more information, see *Overview of the traditional WEB UI (legacy WEB UI)*.

In the event of an obstructing problem, it is necessary to access the solution logs in order to resolve the problem.
This information is used for diagnosis in collaboration with GATEWATCHER support.
The diagnostic function enables:

- Generating log files and uploading them for analysis by GATEWATCHER support.
  The export file log is protected by a password only known by the GATEWATCHER administrator team.
  Messages from all logs will be accessible as well as all system calls from the system.
- Generating the "Tech support" file and uploading it for analysis by an administrator.

The "Tech support" file provides information on the health of the GCenter server although it does not contain any captured data.
This file is not encrypted and is usable by the administrator.

**Note:**

In some sensitive environments, it may not be possible to extract the full set of non-anonymized logs as is possible with the `Log files` archive.
`` `Tech support` `` enables the administrator to provide non-sensitive, anonymized diagnostic information to support.

The graphical interface of the diagnostic function is described in the paragraph *`Admin-GCenter- Diagnostics` screen of the legacy web UI*.

**Note:**

It is also possible from the *setup* menu to generate a "Tech Support".
For more information, see the *Presentation of the configuration menu*.

In these two situations, it is generally necessary for the administrator to contact GATEWATCHER support. These files will enable the support team to identify potential malfunctions and to solve them.

---

### 2.3.4 Data retention

Data is stored on the GCenter for a limited time (called retention time) and for a maximum size.

**Astuce:**

Increasing this time will increase the size of the stored data. This entails higher latencies and reduced performance and stability.

**Note:**

Configuration is performed in two steps:
- The first on the GCenter in this field,
- The second step on the GCap detection probe in the configuration parameters.

These parameters are adjustable.
The graphical interface is described in the paragraph *`Admin-GCenter-Configuration` screen of the legacy web UI*.

---

### 2.3.5 Deleting data

After a full or incremental save by the backup functionality, the old logs are automatically deleted, depending on the data retention time, thus freeing up disk space.
It is possible to delete information manually, by selecting all or part of the type and dates of the information to be removed.
This deletion period is selected by the administrator, however, it cannot exceed the total retention period of the data already pre-configured in the solution.
The same applies to the ICAP and Syslog services.

**Important:**

Data not yet processed will also be deleted.

The graphical interface is described in the paragraph *`Admin-GCenter- Data Management` screen of the legacy web UI*.
For implementation, see *Deleting data (log files)*.

## 2.4 GApps management

Les GApps représentent les différents services fonctionnant sur le GCenter.
These services are listed in the *`Gcenter Services Management` command*.
It may be necessary in some instances to restart or reset them.

**Avertissement:**

Resetting a service is equivalent to returning it to its factory-set configuration. It may be necessary to reapply certain configurations or updates.

## 2.5 Emergency mode

In order to preserve the solution's detection capacity, the **GCenter** can enter into a special regime called **Emergency Mode**.
This mode is automatically triggered in the event of heavy usage of the **GCenter** disk space used to store data.
In such a case, the solution will automatically apply the Data Deletion procedure (see *`Admin-GCenter- Data Management` screen of the legacy web UI*) thus ensuring the continuity of detection services.

## 2.6 Interconnection with external systems

### 2.6.1 Introduction

The GCenter can connect with external equipment such as:

- A Malware Information Sharing Platform server (MISP).
  The MISP server allows to retrieve the Compromise Indices in the form of detection rules usable by Sigflow.
  For more information, see the presentation of *MISP Server*.
- Gatewatcher Intelligence site or GBox server.
  This equipment allows a thorough analysis of malware detected by the GCenter.
  The GCenter sends the files (defined as suspicious or infected) and receives an analysis report.
  For more information, see the presentation of *Intelligence site and GBox*.
- SYSLOG servers via the syslog protocol.
  These servers (SIEM, SPLUNK, LOGSTASH) import the detection data from the GCenter for centralization of this information.
  For more information, see the overview of *Syslog servers*.
- A Netdata server via the Netdata export interface.
  The Netdata interface exports system state data to an external Netdata server.

  For more information, see the presentation of *Netdata server*.

- A Nagios monitoring server via the Netdata polling interface.
  The `` `Netdata polling` `` part enables access to data for a Nagios type monitoring server: it reads the information on the input interface.
  For more information, see the presentation of *Access for a monitoring server*.

---

### 2.6.2 MISP Server

The connection to a MISP server (Malware Information Sharing Platform) makes it possible to retrieve the Indices of Compromises in the form of detection rules.
After connecting to a MISP, it becomes a possible source of rules for the Sigflow detection engine.
The connection status and configuration of the MISP connection is described in *MISP Connection Configuration Screen*.

> **Note:**
>
> Connection to MIPS server is experimental The integration was tested with MISP version 2.4.159. In case of problems, contact GATEWATCHER support.

For connection configuration implementation, refer to *Configuring the connection to the MISP*.
To implement the new rule source, see *`Config - sigflow/sources` screen of the legacy web UI*.

---

### 2.6.3 Intelligence site and GBox

The GCenter enables to analyze the files coming from the GCap probe.
At the end of this analysis made by the different engines of GCenter, this analysis defines different states between healthy and malicious.
For intermediate states (Infected and Suspicious) defined by the Malcore and Retroact engines of the GCenter, a doubt may exist at the end of the analysis.
In order to have a thorough malware analysis, the GCenter can connect:

- Either at the Intelligence site (https://intelligence.gatewatcher.com/): see the presentation of *Intelligence site*
- Either to a GBox: see paragraph of *Sending files to the GBox*

---

#### 2.6.3.1 Intelligence site

The GCenter sends the files (defined as suspicious or infected) to the Intelligence site.
These files are analyzed by Intelligence engines and the site returns a detailed analysis report per file received.
The analysis report is visible on the GCenter to be read by an analyst.

You must have an Intelligence account to log in.
This account connects multiple GCenters to the Intelligence site.

The connection to the Intelligence site requires configuration.
This is defined in *Intelligence site and GBox login configuration screen*.
For the implementation of this configuration, see the procedure of *Configuring the connection to the Intelligence site*.

Files can be sent:

- Either manually by the operator directly from the interface (see *Send file for external analysis to GCenter*).
- Or automatically

Upon receipt of the report, it is possible to consult it (see *Analysis Report Analysis Procedure*).

---

#### 2.6.3.2 Sending files to the GBox

The GCenter sends the files (defined as suspicious or infected to the GBox, physical equipment installed within the infrastructure.
Files (defined as suspicious or infected) can be sent automatically or manually.
These files are analyzed by the engines defined in the GBox template and the GBox returns a detailed analysis report per file received.
This file is visible on the GCenter to be read by an analyst.

The connection to the GBox requires configuration.
This is defined in the *Intelligence site and GBox login configuration screen*.
For the implementation of this configuration, see the procedure in *Configuring the connection to the GBox*.

After this connection, an API (Application Programming Interface) enables to send samples to the **GBox** for analysis and retrieve the results of the analyses:
Files can be sent:

- Either manually by the operator directly from the interface (refer to *Send file for external analysis to GCenter*)
- Or automatically (defined during configuration)

Upon receipt of the report, it is possible to consult it (refer to *Analysis Report Analysis Procedure*).

---

### 2.6.4 Syslog servers

#### 2.6.4.1 Introduction

The Syslog protocol enables the export of detection-related data from the GCenter to remote Syslog servers.
Example of remote servers:

- A SIEM
- A Splunk SIEM
- ETL Logstash

The number of Syslog servers is limited to two.
The data to be exported can be:

- Alerts or
- Alerts and metadata

This data can be filtered in the screen of *Filtering Parameters*.

> **Note:**
>
> No GCenter or GCap system data is affected by this export.

Finally the data can be encrypted: this encryption can be defined in the screen *Encryption*.
For details on data management, see *Data use*.

---

### 2.6.4.2 SIEM

To connect the GCenter to a SIEM, it must be defined as a Syslog server in the *`Admin-GCenter- Data exports` screen of the legacy web UI*.
For implementation, see the *Export data to a SIEM via the syslog protocol*.

---

### 2.6.4.3 SIEM Splunk

To connect the GCenter to a Splunk SIEM, the SIEM must be defined as a Syslog server in the *`Admin-GCenter- Data exports` screen of the legacy web UI*.
For implementation, see the *Export data to a SPLUNK SIEM via the syslog protocol*.

---

### 2.6.4.4 Logstash

To connect the GCenter to the Logstash ETL, it must be defined as a Syslog server in the *`Admin-GCenter- Data exports` screen of the legacy web UI*.
A pipeline developed by Gatewatcher makes it possible to retrieve the JSON content of the exported logs so that it can then be manipulated with the Logstash filters.
For implementation, see the *Export data to a ETL Logstash via the syslog protocol*.

**Note:**

It is possible to quickly create a POC (Proof Of Concept).
For implementation, see the *Quick creation of a POC Logstash*.

---

## 2.6.5 Netdata server

The Netdata export interface enables the export of system-related data from the GCenter to a remote Netdata server.

For details on data management, see *Data use*.
The description of the configuration is given in the screen *`Netdata Export` section*.
For implementation, see the *Configuring the Netdata export interface*.

---

### 2.6.6 Access for a monitoring server

The `` `Netdata polling` `` part allows access to data for a Nagios type monitoring server: it reads the information on the input interface.

For details on data management, see *Data use*.
The configuration description is given in the screen *`Netdata polling` section*.
For implementation, see the *Configuring the Netdata polling interface*.

---

## 2.7 API

### 2.7.1 Introduction

The API (Application Programming Interface) is the set of endpoints (also called resources or end of URL).
Each of these endpoints allows you to perform an action on the GCenter and return information without having to go through the graphical interface.
This facilitates the sharing and integration of GCenter features and data into existing architectures.

Each of these endpoints has a simple syntax.
These endpoints are predetermined: the list of these endpoints is limited and is displayed by theme (analysers ...).

> **Note:**
>
> The list of endpoints is given in the *Endpoints list*.

The execution of these endpoints can be done:

- Via SWAGGER (*Use via the swagger GUI*)
  This allows the use of endpoints and to understand its configuration and to test its execution and analyze its results
- Via CURL (*Use via CURL*)
  This allows to execute a Curl request directly and not to go through the GUI

---

### 2.7.2 Use via the swagger GUI

Each endpoint of the API:

- Performs a specific operation. Its name and description are indicated in the graphical interface (or in the *Endpoints list*)
- Performs one of four possible methods: GET, DELETE, POST, PUT
- Needs authentication rights that are the same as for the GUI (Operators or Administrators)
- May need operating parameters (input and/or output): for example, in the case of a filter, the value of this filter must be indicated

All this information is visible in the swagger GUI and is therefore the documentation of all API endpoints.

The swagger GUI description is given in *Overview of the API interface*.
For implementation of the swagger interface, see the procedure in *Using an endpoint API*.

This interface enables to:

- Have a list of existing endpoints (listed by theme)
- Have details of possible parameters for running an endpoint
- Have information on the expected result (data model and an example with default values)
- Execute queries
- Retrieve the Curl command equivalent to the request via the API

**Note:**

A known bug affects the /api/alerts endpoint (see GCenter release note). It is recommended to use the elasticsearch API to query data on the/api/data/es/search endpoint.

### 2.7.3 Use via CURL

It is possible to execute an endpoint by a curl command.
This command is accessible via the swagger GUI after selecting the endpoint, entering any parameters and then starting the execution of the endpoint.
The curl command is displayed in the `Responses` area.

For a user called **username** and with **operators** rights.

**Recovery of the API token:**

```
curl -X POST "https://<hostname>/api/auth/login" -H "accept: application/json" -H
↪"Content-Type: application/json" -d "{ \"username\": \"username\", \"password\": \
↪"password\"}" -k
```

where hostname is GCenter.

Answer:

```
{"token":"urxn5hlezbk3vnlgq1t45rifhg0vi951","expiration_date":"2021-04-13T16:26:45.
↪743826"}
```

Sending a request:

```
curl -X POST "https://<hostname>/api/<endpoint> -H "accept: application/json" -H
↪"Content-Type: application/json" -H "API-KEY: x0zc5py1e2lrppe6ws0kgc8le0oxm9hg" -d
↪"{\"test\": \"test\"}" -k
```

Example of a query that will query elasticsearch on its suricata* indexes and retrieve 100 logs over the last 24 hours:

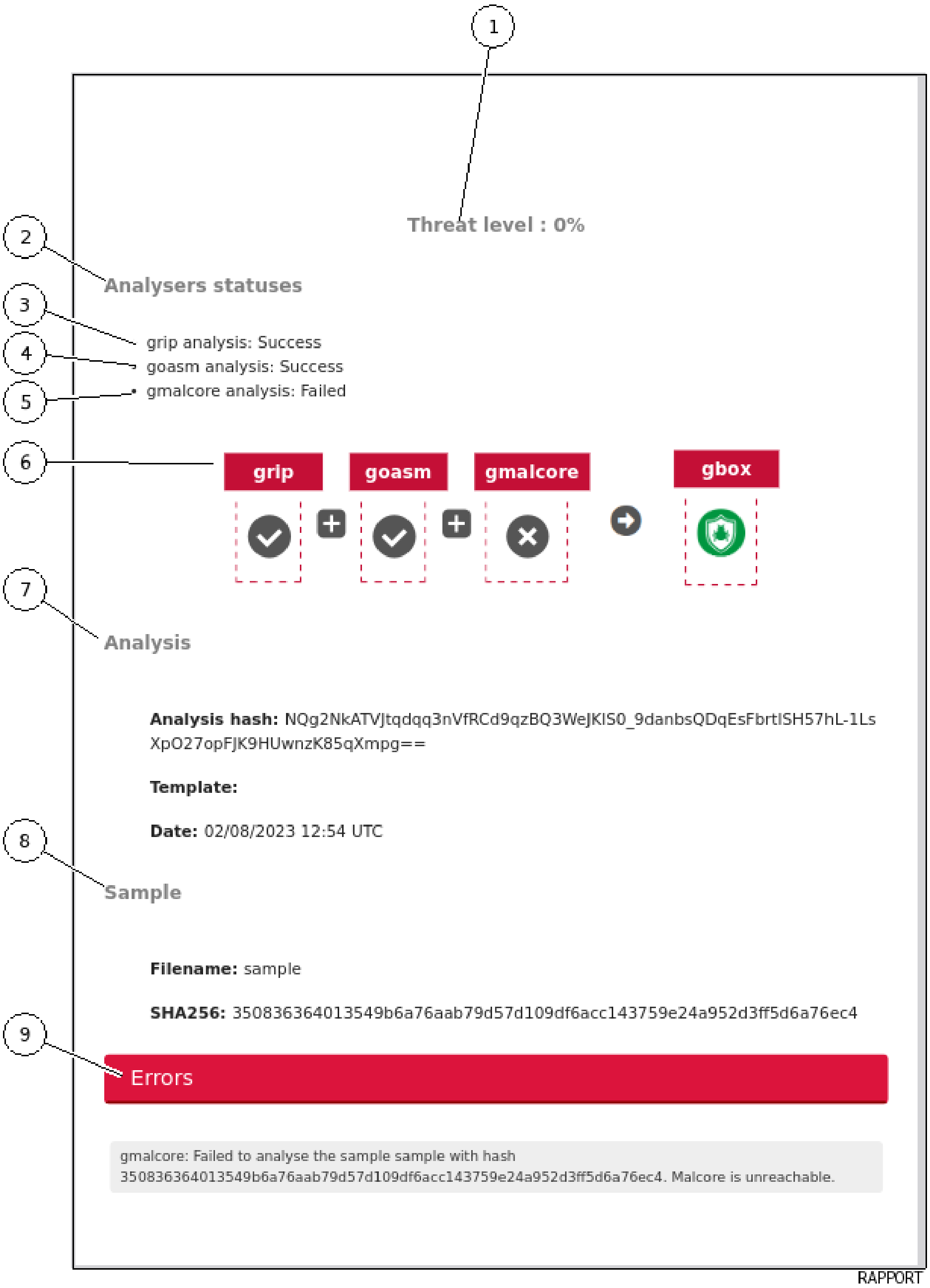
```
curl -X POST "https://<hostname>/api/<endpoint> -H "accept: application/json" -H
↪"Content-Type: application/json" -H "API-KEY: x0zc5py1e2lrppe6ws0kgc8le0oxm9hg" -d
↪"{ \"size\" : 100, \"query\" : { \"bool\": { \"must\": [], \"filter\": [ { \"match_
↪all\": {} }, { \"range\": { \"@timestamp\": { \"gte\": \"now-24h\", \"lte\": \
↪"now\" } } } ], \"should\": [], \"must_not\": [] } } }" -k
```

### 2.7.4 Authentication and access to the API

Access to the swagger graphical interface is via the GCenter web GUI and then press the `API` button.
Authentication allows access to the API (for more information, see paragraph *Title bar*).
Using curl request requires authentication to be done in the request.
This authentication is done using the name/password pairs or tokens defined in *The `API Keys` section of the `Accounts` submenu*.

## 2.8 Results and analysis report

If a file is sent to a remote server (GBox or site intelligence), the analysis is performed by the remote server and it can be downloaded as a pdf report.



Threat level : 0%

Analysers statuses

- grip analysis: Success
- goasm analysis: Success
- gmalcore analysis: Failed

Analysis

**Analysis hash:** NQg2NkATVJtqdqq3nVfRCd9qzBQ3WeJKIS0_9danbsQDqEsFbrtlSH57hL-1LsXpO27opFJK9HUwnzK85qXmpg==

**Template:**

**Date:** 02/08/2023 12:54 UTC

Sample

**Filename:** sample

**SHA256:** 350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4

Errors

gmalcore: Failed to analyse the sample sample with hash 350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4. Malcore is unreachable.

This report is composed of:

- A threat level (1) `` `Threat level` ``

  This score is calculated from the analysis score returned by the different engines **active** of the GBox in the model at the time of detection
- Part (2) `` `Analysers statuses` ``

  This part lists the engines activated during the analysis and their results.

  For example, the Gnest engine is not activated so not displayed.

  This part indicates which analysis was done but in no case the result of the analysis:
  - `` `grip analysis:  Success` `` : Grip engine analysis (3) was carried out
  - `` `goasm analysis:  Success` `` : Goasm engine analysis (4) was carried out
  - `` `gmalcore analysis:  Failed` `` : Gmalcore engine analysis (5) failed
  - The summary of the analysis steps (6) which displays:
    - The list of engines used: here grip, Goasm and Gmalcore
    - The result of the analysis for each of the engines: here for Gmalcore, the cross indicates that the analysis by Gmalcore was not made unlike the other two engines

      Right side, the result of the analysis of the GBox: here the icon means error
- Part (7) `` `Analysis` `` provides analysis information: hash, model and date
- Part (8) `` `Sample` `` gives sample information: filename and sha256
- Part (9) `` `Errors` `` gives the information on the origin of the failure of the analysis: here the Gmalcore motor does not work. hence no response from him
- The retailers the analyses:

| Part Title | Description | Is engine activated |
|---|---|---|
| `` `Analysis options` `` | Option values used for analysis | Grip and Gnest |
| `` `Iocs` `` | List of actions performed (files, registry, network, processes...) | GNEST |
| `` `Ttps` `` | TTPs analyse the functioning of a malicious actor, they describe how cyber attackers orchestrate, execute and manage operational attacks.<br>TTPs contextualize a threat. They reveal the steps or actions taken by malicious actors during data exfiltration for example. | GNEST |
| `` `Static` `` | Métadonnées | GRIP |
| `` `Overview` `` | File information (size, different hash, type...) | GNEST |
| `` `Heuristic` `` | List of engines (Entry#x) and name of the threat returned by the Gmalcore module (or n/a) | Gmalcore |
| `` `Shellcode` `` | Result of shellcode detection | GOASM |
| `` `Signatures` `` | List of yara signatures corresponding to the analyzed file | Gnest |
| `` `Process Tree` `` | Graphical representation of the process tree | Gnest |

For report analysis procedure, see the *Analysis Report Analysis Procedure*.

# Chapter 3

# Characteristics

## 3.1 Mechanical characteristics of GCenter

| REFERENCE | DIMENSIONS (H x W x D) | RACKAGE | WEIGHT (KG) |
|---|---|---|---|
| GCENT8100r2 | 42.8 x 482 x 808.5 mm | 1 U | 21.9 |
| GCENT9100r2 | 42.8 x 482 x 808.5 mm | 1 U | 21.9 |
| GCENT900r2 | 86.8 x 434 x 836 mm | 2 U | 36.6 |
| GCENT10500r2 | 86.8 x 434 x 836 mm | 2 U | 36.6 |

## 3.2 Electrical characteristics of GCenter

| REFERENCE | LOCAL STORAGE (SSD) | BACKUP STORAGE | EXTENSION STORAGE | POWER SUPPLY ELECTRICAL |
|---|---|---|---|---|
| GCENT8100r2 | 2x 960GB RAID1 | 2x 2 TB RAID1 | N/A | 2 x 750W |
| GCENT9100r2 | 4x 480GB RAID5 | 2x 2 TB RAID1 | Contact GATEWATCHER | 2 x 750W |
| GCENT9900r2 | 10 x 480GB RAID5 | 4 x 2 TB RAID5 | | 2 x 1100W |
| GCENT10500r2 | 12 x 480GB RAID5 | 4 x 2 TB RAID5 | | 2 x 1100W |

## 3.3 Functional characteristics of GCenter

| REFERENCE | GCENT8100r2 | GCENT9100r2 | GCENT9900r2 | GCENT10500r2 |
|---|---|---|---|---|
| Events per second | 2000 | 4000 | 6000 | 8000 |
| Number of stored events | 1 million | 10 million | 80 million | 300 million |
| Number of files scanned per second | 10 | 20 | 30 | 50 |
| MPL qualified | OK | | | |
| SIEM infrastructure | OK | | | |
| GBox connector | OK | | | |
| *FULL EDITION* (FE) licence | OK | | | |
| *CRITICAL INFRASTRUCTURE* (CIE) licence | OK | | | |
| AD/LDAP authentication | OK | | | |
| SUPERVISION | OK | | | |
| IDRAC EXPRESS licence | OK | | | |
| IDRAC BUSINESS licence | OPTIONAL | | | |

# Chapter 4

# Accounts

## 4.1 List of accounts

There are two user interfaces:

- The configuration menu (GUI)
- The web interface

For each of the two interfaces, user accounts exist.
Remote or local access to the GCap administration interface is protected by a login password.

---

## 4.2 Account setup of the configuration menu

### 4.2.1 Account of the configuration menu

The user profile to access the configuration menu is **setup**.
The default password is: **default**.

---

### 4.2.2 Related principles

#### 4.2.2.1 Authentication mode

A user's authentication is achieved by means of a login/password pair.

---

#### 4.2.2.2 Password management

It is possible to change the password of the **setup** account from the GUI.
See *`Password` command*

#### 4.2.2.3 Password management policy

The passwords entered must comply with the password management policy.
The default policy is as follows:

| Criteria | Default value |
|---|---|
| Number of different characters to make a password to be considered different | 2 |
| Minimum password length | 12 |
| At least one lower case letter | Yes |
| At least one upper case letter | Yes |
| At least one digit (0 to 9) | Yes |
| At least one symbol (i.e. neither a number nor a letter) | Yes |

#### 4.2.2.4 Anti-bruteforce system

An anti-bruteforce system is included on the GCenter.
The latter's policy will be as follows:

- Blocking for 15 minutes after 3 failed authentication attempts in a row
- 10 second delay between each failed authentication attempt

### 4.2.3 Functions allowed in the setup account

From the **setup** account, it is possible to access the entire configuration menu (GUI).
The configuration menu is described in the section *Presentation of the configuration menu*.
The permitted functions are described in the section *Use case of the configuration menu: setup account*.

## 4.3 Web interface accounts and their management

**GCenter** enables access to:

- Managing users and related groups
- History of authentications, account creations/deletions, and rights changes on the platform
- Linking with an LDAP server

---

### 4.3.1 Web Interface Accounts

Depuis le menu de configuration des comptes utilisateurs, il est possible de créer des comptes utilisateurs ayant chacun des droits différents.

These rights are defined by groups.

Each user can therefore belong to one or more groups, thus inheriting the rights of the group.

**Note:**

The proposed groups fully comply with the Military Programming Law.

In the GCenter web interface, there are two different types of rights:

- Operator
- Administrator

Generic accounts are defined with the following rights levels:

| Account... | type of rights or group | intended for a... |
|---|---|---|
| \`operator\` | operator | analyst |
| \`administrator\` | administrator | administrator |
| \`admin\` | operator and administrator | access to all analyst and administrator functions |

**Note:**

It is necessary to modify the password upon the first connection, and to keep it in a safe place, for example, with the encryption keys of the devices.

---

### 4.3.2 Functions allowed with the group or role \`operator\`

From the **operator** account, it is possible to access the entire set of menus present in the Web UI.

On the other hand, the menus dedicated to the administration of the GCenter will not be accessible, functions are present in the legacy web UI.

---

### 4.3.3 Functions authorized with the group or role `administrator`

From the **administrator** account, it will be possible to access all the menus present in the legacy Web UI.

On the other hand, the menus dedicated to the data analysis of the GCenter will not be accessible, functions are present in the web UI.

---

### 4.3.4 Functions allowed in the admin account

From the **Admin** account, it is be possible to access all the features present in the two Web UI.

---

### 4.3.5 Summary tables of the menus per level

#### 4.3.5.1 Access via icon

| Icon | Description | Operator | Administrator |
|---|---|---|---|
| API | Interface Gatewatcher API | limited access | access |
| Gstats | Interface System Overview | no access | access |

---

#### 4.3.5.2 Main menu

| Menu | Description | Operator | Administrator |
|---|---|---|---|
| GATEWATCHER logo | page `home` : general view of the GCenter | access | no access |
| Home | | | |
| Overview | `Global overview` page | access | no access |
| Relations | `Relations` page showing the relationships between the elements on the network | access | no access |
| Hunting | KIBANA user interface | access | no access |
| Assets | `Assets` page showing the characteristics of the elements present on the network | access | no access |
| Users | `Users` page showing the characteristics of the users on the network | access | no access |
| Alerts | `Alerts` page showing the characteristics of the alerts displayed | access | no access |
| Gscan | `GScans` page to run a scan on a specific file | access | no access |
| Config | display of the sub-menu `Configuration` | access | no access |
| Admin | displayed only for Administrator accounts | access | no access |

---

#### 4.3.5.3 Config Menu

| Sub Menu | Description | Operator | Administrator |
|---|---|---|---|
| Assets users association rules command | Association page rules | access | no access |
| Gcap Profiles | GCaps page profiles | access | no access |
| Sigflow Sources command | `Sources` page of the legacy WEB UI | access | no access |
| Sigflow Rulesets command | `Rules` page of the legacy WEB UI | access | no access |

#### 4.3.5.4 Admin Menu

| Sub Menu | Description | Operator | Administrator |
|---|---|---|---|
| NDR configuration | NDR page Configuration | no access | access |
| GCaps pairing and status | `GCaps pairing and status` page of the legacy WEB UI | no access | access |
| Backup / restore command configuration | `Backup configuration` page of the legacy WEB UI | no access | access |
| Backup / restore operations command | `Backup operations` page of the legacy WEB UI | no access | access |
| GUM Config command | `GUM configuration` page of the legacy WEB UI | no access | access |
| GUM Updates command | `Updates` page of the legacy WEB UI | no access | access |
| GUM Hotfix command | `Hotfix` page of the legacy WEB UI | no access | access |
| GCenter Monitor command | `GCenter monitoring` page of the legacy WEB UI | no access | access |
| GCenter Data exports command | `Data exports` page of the legacy WEB UI | no access | access |
| GCenter Data Management command | `Data Management` page of the legacy WEB UI | no access | access |
| GCenter ML Management command | `Machine Learning Management` page of the legacy WEB UI | no access | access |
| Gcenter Malcore Management command | `Data Management` page of the legacy WEB UI | no access | access |
| GCenter Third-party modules command | `Third-party modules` page of the legacy WEB UI | no access | access |
| GCenter Diagnostics command | `Diagnostics` page of the legacy WEB UI | no access | access |
| GCenter Accounts command | `Accounts` page of the legacy WEB UI | no access | access |
| GCenter Configuration command | `Configuration` page of the legacy WEB UI | no access | access |
| Gcenter CTI Configuration command | `CTI Configuration` page of the legacy WEB UI | no access | access |
| GCenter Trackwatch logs command | `Syslog - Overview` page of the KIBANA user interface | no access | access |

## 4.3.6 Related principles

### 4.3.6.1 Authentication mode

A user's authentication is achieved by means of a login/password pair.

---

### 4.3.6.2 Password management

The current account manages its own password and potentially other accounts as well.
Details are provided in the table below:

| User | can change the password | | |
|---|---|---|---|
| | operator | administrator | admin |
| operator | X | | |
| administrator | X | X | |
| admin | X | X | X |

---

### 4.3.6.3 Password management policy

The passwords entered must comply with the password management policy.
The policy is divided into two categories:

- General settings
- Specific password settings

These general parameters are:

- Period of validity
- Recording of previous password hashes

These specific parameters are the criteria that passwords must contain, such as lower case, upper case, and so on.
The details of these parameters and the graphical interface enabling the management of this policy are described in *The `Password Policy` section of the `Accounts` submenu*.
For implementation, see the *Managing the password policy*.

---

## 4.3.7 Creating local users

In addition to generic accounts, it is possible to create user accounts each having different rights.

> **Note:**
>
> The proposed groups fully comply with the Military Programming Law.

When creating a new user account, it is possible to assign different roles to the user.
The role(s) the user is assigned will enable them to access more or less menus in the web interface.
Indeed, depending on the actions carried out, it will be necessary to assign a specific role.
The administrator fills in the following fields concerning the user they wish to create:

- Username
- Password
- Email address
- First Name
- Last Name

It is also necessary to activate the account for it to be usable and to assign it the available roles: operator and/or administrator
These fields will be used later to trace the user in the connection history or in the event of changes concerning this same account.
The graphical interface enabling the creation of users is done in *The `Users management` section of the `Accounts` submenu*.
For implementation, see:

- the *Creating local users*
- the *Changing some of a local user's information*
- the *Resetting a local user's password*
- the *Deleting a local user*

---

### 4.3.8 LDAP integration / Active Directory

Authentication of the GCenter's user accounts can be managed by the GCenter as well as by a Lightweight Directory Access Protocol (LDAP) server.
Configuring the connection between the GCenter and the LDAP server is also done by the GCenter.
The main functions include:

- Displaying the connection status
- Enabling the connection to a remote authentication server
- Managing connection information to a remote authentication server
- Mapping of users and groups between the GCenter and the remote authentication server
- Advanced configuration of the connection to a remote authentication server

The graphical interface enabling the creation of users is done in *The `LDAP configuration` section of the `Accounts` submenu*.
For implementation, see:

- The *Displaying of the connection status between the GCenter and the LDAP server*
- The *Enable the connection between the GCenter and the LDAP server*
- The *Configuring the connection between the GCenter and the LDAP server*
- The *Configuring the users and groups defined on LDAP / ActiveDirectory*

---

### 4.3.9 Audit trail

The system records the various actions carried out in the web interface over time, in order to ensure traceability. This traceability is carried out for:

- Users' connection or disconnection
- Creating and deleting accounts
- Changing the permissions of an account

---

#### 4.3.9.1 Authentication history function

The history of all authentications on the GCenter is available.
To view the graphical interface presentation, see *The `Authentications history` section of the `Accounts` submenu*
For the implementation, refer to *Viewing the authentication history*.

---

#### 4.3.9.2 Historical function of all creations or deletions

The history of all creations or deletions of GCenter users is available.
To view the graphical interface presentation, see *The `Creations/Deletions history` section of the `Accounts` submenu*.
For the implementation, refer to *Viewing the history of user creations or deletions*.

---

#### 4.3.9.3 History function for all changes in user rights

The history of all user permissions on the GCenter is available.
To view the graphical interface presentation, see *The `Permissions history` section of the `Accounts` submenu*.
For the implementation, refer to *Viewing the history function for all changes in user rights*.

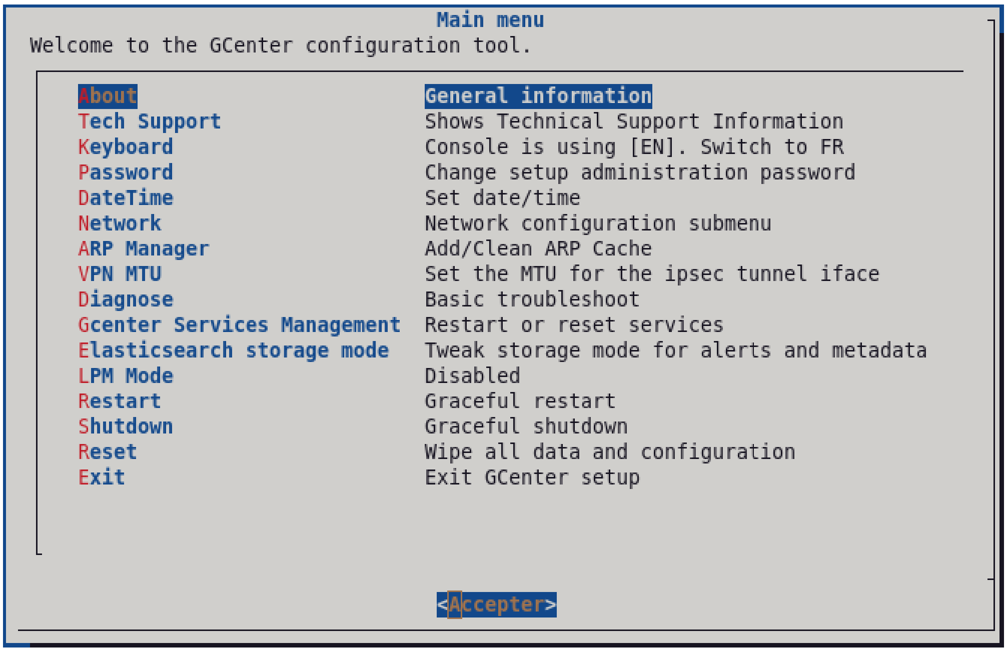
---

Chapter 5

# Overview of the GCenter graphic interfaces

## 5.1 Presentation of the configuration menu

The configuration menu is displayed.



```
                              Main menu
Welcome to the GCenter configuration tool.

   About                          General information
   Tech Support                   Shows Technical Support Information
   Keyboard                       Console is using [EN]. Switch to FR
   Password                       Change setup administration password
   DateTime                       Set date/time
   Network                        Network configuration submenu
   ARP Manager                    Add/Clean ARP Cache
   VPN MTU                        Set the MTU for the ipsec tunnel iface
   Diagnose                       Basic troubleshoot
   Gcenter Services Management    Restart or reset services
   Elasticsearch storage mode     Tweak storage mode for alerts and metadata
   LPM Mode                       Disabled
   Restart                        Graceful restart
   Shutdown                       Graceful shutdown
   Reset                          Wipe all data and configuration
   Exit                           Exit GCenter setup

                              <Accepter>
```

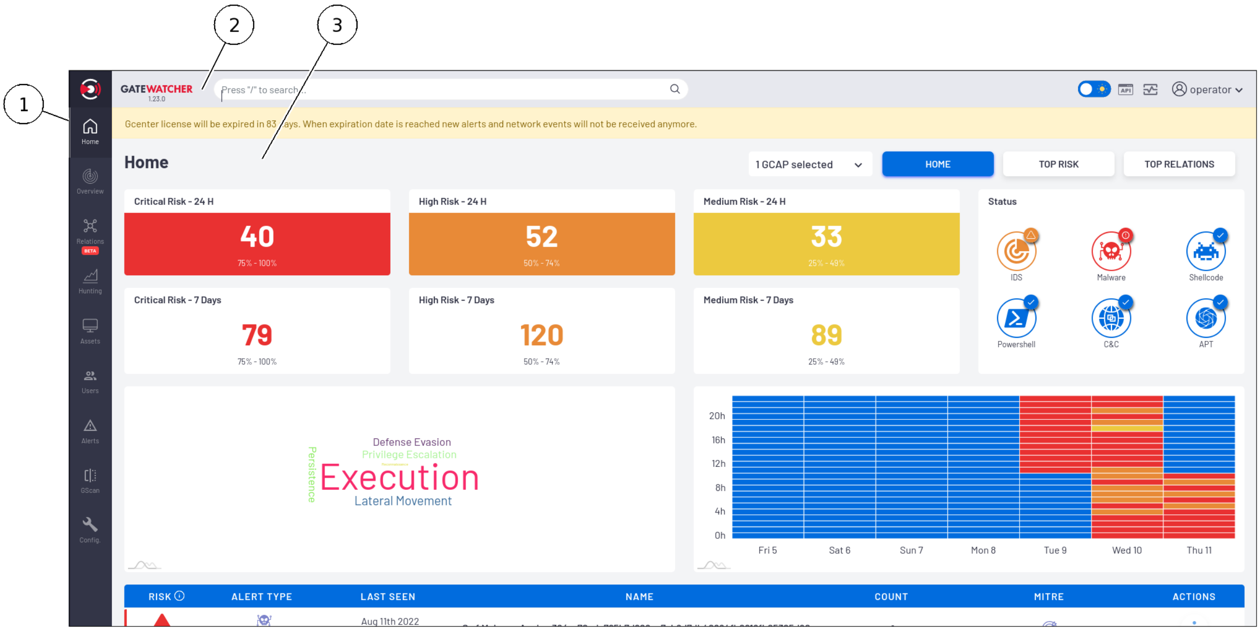
Each of these commands enables an action to be taken.
These commands are detailed in the table below, including links to the corresponding procedures.

| Choice | Shortcut key | Explanation | See procedure |
|---|---|---|---|
| About | A | General information about the GCenter | `About` command. |
| Tech Support | T | Enables generating a diagnostic file | `Tech Support` command. |
| Keyboard | K | Enables modifying the keyboard | `Keyboard` command. |
| Password | P | Enables changing the password of the `setup` account | `Password` command. |
| DateTime | D | Enables changing the date and time of the GCenter. | `DateTime` command. |
| Network | N | Enables configuring the network section of the GCenter | `Network` command. |
| Arp Manager | A | Enables manually creating entries in the GCenter ARP table | `Arp Manager` command. |
| VPN MTU | V | Enables modifying the MTU of the VPN tunnel with the GCap | `VPN MTU` command. |
| Diagnose | D | Enables diagnosing the network configuration of the GCenter | `Diagnose` command. |
| Upgrade type | U | Enables modifying the type of system update | `Upgrade type` command. |
| GCenter Services Management | G | Enables restarting or resetting certain GCenter services | `Gcenter Services Management` command. |
| Elasticsearch storage mode | E | Enables modifying the storage mode for the alerts and the metadata. | Commande `Elasticsearch storage mode`. |
| MPL Mode | L | Enables switching the solution to MPL mode | `LPM Mode` command. |
| Restart | R | Enables restarting the GCenter | `Restart` command. |
| Shutdown | S | Enables switching off the GCenter | `Shutdown` command. |
| Reset | R | Enables restoring the GCenter to its "factory default" settings | `Reset` command. |
| Exit | E | Enables exiting the configuration menu | `Exit` command. |

## 5.2 Overview of the WEB UI

**Important:**

This section describes the graphical elements available to members of the operator group.



Gcenter license will be expired in 83 days. When expiration date is reached new alerts and network events will not be received anymore.

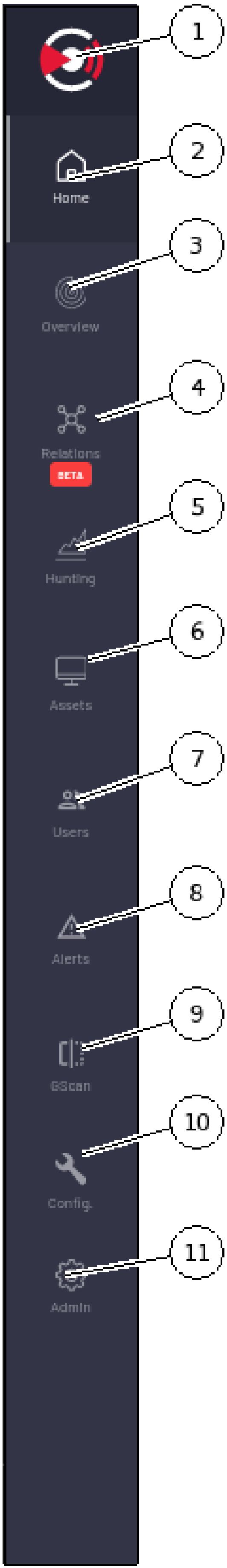
HOME

The screen consists of following parts:

| Item | Name | Description |
|---|---|---|
| 1 | *Navigation bar* | Displays the icons used to access the main functions |
| 2 | *Title bar* | Gives direct access to certain functions (search, visual theme...) |
| 3 | *Central screen* | Displays the screen selected by clicking on the icon in the navigation bar.<br>Each screen is named like the shareholder icon: example `Home` screen |

## 5.2.1 Navigation bar

The navigation bar consists of buttons used to access the various functions.

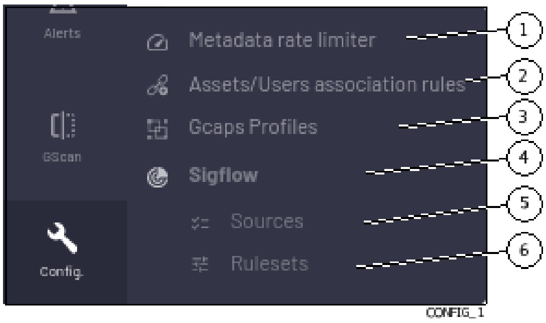

1
2
Home
3
Overview
4
Relations
BETA
5
Hunting
6
Assets
7
Users
8
Alerts
9
GScan
10
Config.
11
Admin

HOME_REP1

| Item | Button name | Display |
|---|---|---|
| 1 | GATEWATCHER logo | *Web UI `Home` screen*: corresponds to the main dashboard |
| 2 | `Home` | *Web UI `Home` screen*: corresponds to the main dashboard |
| 3 | `Overview` | *Web UI `Overview` screen* : refers to a scorecard detailing the most significant risks for each item |
| 4 | `Relations` | *Web UI `Relations` screen* : corresponds to the network mapping. This shows the relationships between the elements in the network |
| 5 | `Hunting` | *Web UI `Hunting` screen* : enables access to Kibana dashboards |
| 6 | `Assets` | *Web UI `Assets` screen*: the `Assets` page showing the characteristics of the active elements on the network |
| 7 | `Users` | *Web UI `Users` screen*: the `Users` page showing the characteristics of the users on the network |
| 8 | `Alerts` | *Web UI `Assets` screen*: the `Alerts` page showing the characteristics of the displayed alerts |
| 9 | `Gscan` | *Web UI `GScan` screen*: the `GScan` page to run a scan on a specific file |
| 10 | `Config` | The configuration sub-menu: see *`Config` Menu* |
| 11 | `Admin` | Access restricted to the administrator: see *`Admin` Menu* |

### 5.2.2 `Config` Menu

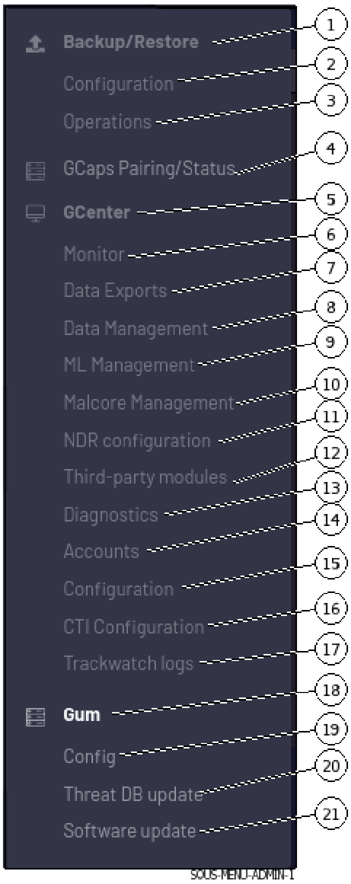
The menu consists of the following items:



| Item | Menu name | Command name | Display |
|---|---|---|---|
| 1 | Metadata rate limiter | `Metadata rate limiter` | *Web UI `Config - Metadata rate limiter` screen* |
| 2 | Assets/Users association rules | `Assets/Users association rules` | *Web UI `Config - Assets/Users Association rules` screen* |
| 3 | Profils GCaps | `Gcaps Profiles` | *Web UI `Config - Gcaps profiles` screen* |
| 4 | Sigflow | includes the following controls: | |
| 5 | | - `Sources` | *`Config - sigflow/sources` screen of the legacy web UI* |
| 6 | | - `Rulesets` | *`Config - sigflow/rulesets` screen of the legacy web UI* |
| | | - `MISP` administrator role access only | *`Config - sigflow/MISP` screen of the legacy web UI* |

### 5.2.3 `Admin` Menu

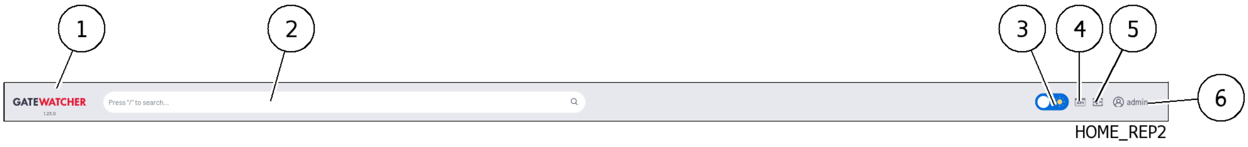
The menu consists of the following items:



| Item | Menu name | Command name | Display |
|---|---|---|---|
| 1 | `Backup/Restore` | includes the following controls: | |
| 2 | | • `Configuration` | *`Admin-Backup/Restore - Configuration` screen of the legacy web UI* |
| 3 | | • `Operations` | *`Admin-Backup/Restore - Operations` screen of the legacy web UI* |
| 4 | `GCaps Pairing/Status` | | *`Admin-GCaps pairing and status` screen of the legacy Web UI* |
| 5 | `GCenter` | includes the following controls: | |
| 6 | | • `Monitor` | *`Admin-GCenter- Monitor` screen of the legacy web UI* |
| 7 | | • `Data Exports` ` | *`Admin-GCenter- Data exports` screen of the legacy web UI* |
| 8 | | • `Data Management` | *`Admin-GCenter- Data Management` screen of the legacy web UI* |
| 9 | | • `ML Management` | *`Admin-GCenter- ML Management` screen of the legacy web UI* |
| 10 | | • `Malcore Management` | *`Admin-GCenter- Malcore Management` screen of the legacy web UI* |
| 11 | | • `NDR configuration` | *Web UI `Admin-NDR configuration` screen* |
| 12 | | • `Third-party modules` | *`Admin-GCenter- Third-party modules` screen of the legacy web UI* |
| 13 | | • `Diagnostics` | *`Admin-GCenter- Diagnostics` screen of the legacy web UI* |
| 14 | | • `Accounts` | *`Admin-GCenter- Accounts` screen of the legacy web UI* |
| 15 | | • `Configuration` | *`Admin-GCenter-Configuration` screen of the legacy web UI* |
| 16 | | • `CTI Configuration` | *`Admin-GCenter- CTI Configuration` screen of the legacy web UI* |
| 17 | | • `Trackwatch logs` | *`Admin-GCenter Trackwatch logs` screen of the legacy web UI* |
| 18 | `Gum` | includes the following controls: | |
| 19 | | • `Config` | *`Admin- GUM - Config` screen of the legacy web UI* |
| 20 | | • `Threat DB update` | *`Admin-GUM- Threat DB update` screen of the legacy web UI* |
| 21 | | • `Software update` | *`Admin-GUM- Software update` screen of the legacy web UI* |

### 5.2.4 Title bar

The title bar is located and consists of the following items:



| Item | Name | Description |
|---|---|---|
| 1 | GATEWATCHER logo | If pressed then return to the `Home` screen. |
| 2 | Search field | After entering the search text and validating, the system displays the results. |
| 3 | Theme change button | Enables switching between the two light and dark themes. |
| 4 | API button | Switches to the GATEWATCHER API UI. |
| 5 | Gstats button | Access reserved for the administrator. |
| 6 | Current account button | Manages the current account. |

### 5.2.5 Central screen

The central screen displays the information selected by a button on the navigation bar.
By default, the `Home` screen is displayed.

## 5.3 Overview of the Kibana GUI

The Kibana web interface displays the data present in the ElasticSearch indexes of the GCenter.
This data comes from different analysis engines.
Before GCenter indexing, this data can:

- Come from analyses on the GCap side (alerts and metadata reported by the Sigflow detection engine)
- Come from analyses on the GCenter side (malware, shellcode, powershell, retrohunt or machine learning alerts)

**Important:**

This section describes the graphic elements accessible to members of the operator group.

### 5.3.1 Configuration of the Kibana GUI

The Kibana interface is fully editable by the user.
It is possible to create visualizations and dashboards.
Natively, the interface has pre-recorded dashboards to visualize the data of the different engines of the solution.
These dashboards are also editable by the user.
Different viewing rights apply to this interface:

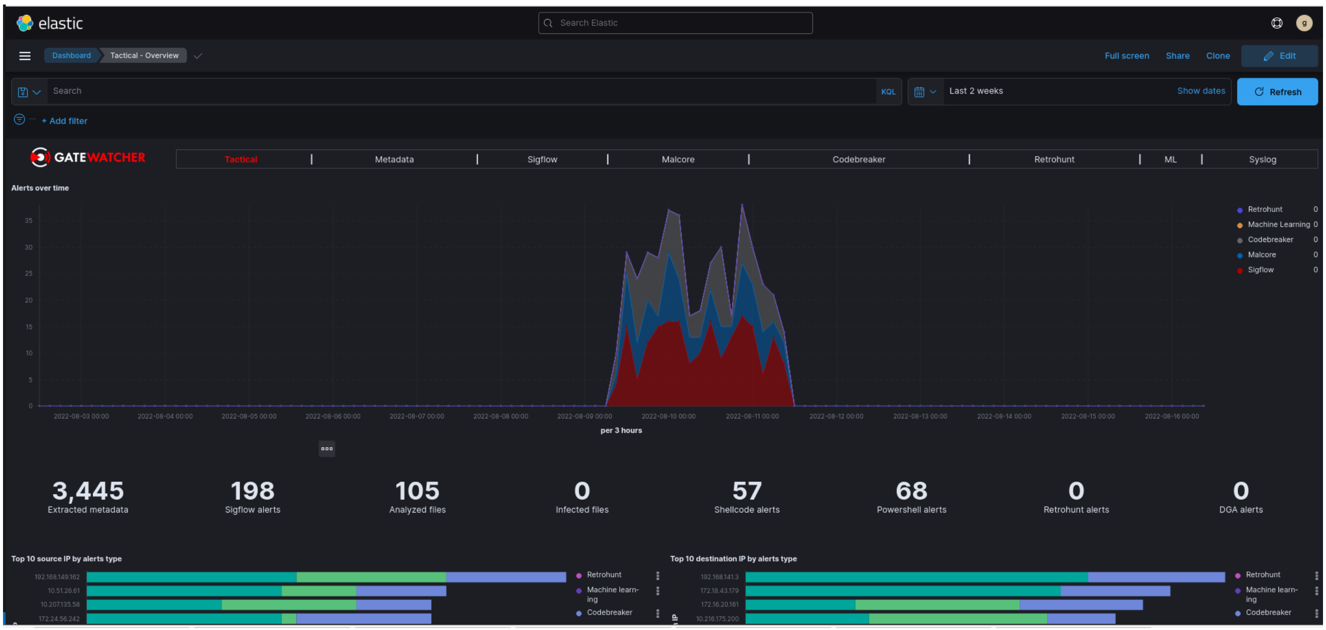
- Users who are members of the group **operator** can view the data present in the detection event dashboards
- Users who are members of the group **administrator** can view the data present in the system dashboards (Syslog)

**Note:**

Kibana interface access is available:

- For members of the operator group, by clicking on the `Hunting` button on the navigation bar
- For members of the administrator group, by clicking on the command `GCenter/Trackwatch logs` from the menu `Admin`

### 5.3.2 Native dashboards



The native dashboards are grouped in the Kibana interface as tabs:

- `Tactical
- `Metadata`
- `Sigflow`
- `Malcore
- `Codebreaker`
- `Retrohunt
- `ML
- `Syslog`

**Note:**

For most dashboards, three pages are available:

- `Overview`
- `Messages`
- `GeoIP`

Viewing GeoIP information requires internet access for the base maps to be downloaded.
Each of these tabs corresponds to a specific type of data, here is the detail:

- `Tactical` displays, in visualizations, the alert information of the different engines:

- a graph showing the number of alerts per engine over time
- a counter displaying the number of alerts per engine, the number of metadata and the number of files scanned
- a top 10 source IP addresses by type of alert
- a top 10 destination IP addresses by type of alert
- a graph showing the proportion of the different severity of Sigflow alerts
- a graph showing the number of unique signatures that escalated alerts over time
- a list of Malcore alerts identified by the solution (in the form of a message)
- a top 10 Codebreaker alerts
- a top 10 Retrohunt alerts
- a top in the distribution of DGA domain names (Machine Learning)
- Top 10 Machine Learning Alerts

- `Metadata` displays, in sub-tabs, the metadata for the different protocols analyzed by the probe:

  - All, synthesizes all metadata into visualizations in chart form
  - DHCP, DHCP metadata details
  - DNS, DNS metadata details
  - File Transaction, details of the metadata related to the file reconstructed by the probe
  - HTTP, HTTP metadata details
  - IKEv2, IKEv2 metadata details
  - KRB5, KRB5 metadata details
  - NFS, NFS protocol metadata details
  - SMB, SMB metadata details
  - SMTP, SMTP metadata details
  - SSH, SSH metadata details
  - TFTP, TFTP metadata details
  - TLS, TLS metadata details

  **Attention:**

  Some protocols do not have a native dashboard despite the fact that they can generate metadata.
  These metadata are still indexed and usable in Kibana.

- `Sigflow` displays all alerts generated by Sigflow
- `Malcore` displays all malware alerts generated by the Malcore engine
- `Codebreaker` displays all shellcode and powershell alerts generated by the Codebreaker engine
- `Retrohunt` displays all alerts generated by the Retrohunt engine
- `MetaMLdata` displays all alerts generated by the Machine Learning engine;
- `Syslog` displays the solution's syslog system events (accessible only by administrators)

### 5.3.3 Data exploitation

In each dashboard, it is possible to perform a filtering to display only the desired data.
To do this, several options are possible:

- Filter by changing the time interval (top right of page)
- Filter by searching using the `Search` bar (top left)
- Filter by creating a filter on a specific field of the desired events (button `+ Add filter` below the search bar)

---

## 5.4 Overview of the traditional WEB UI (legacy WEB UI)

### 5.4.1 Presentation of the legacy WEB UI

This interface is the traditional interface of the solution, also referred to as the legacy WEB UI.
It consists of all the configuration menus.
When connecting to the GCenter, the interface displayed is the main WEB UI and not the traditional interface.
To access it, click on the `Admin` button in the navigation bar at the bottom left of the page and select one of the menus.
A new tab will open giving access to all the administrator level configurations.

**Note:**

Only the `NDR configuration` menu is displayed in the main interface. All others are in the traditional interface.

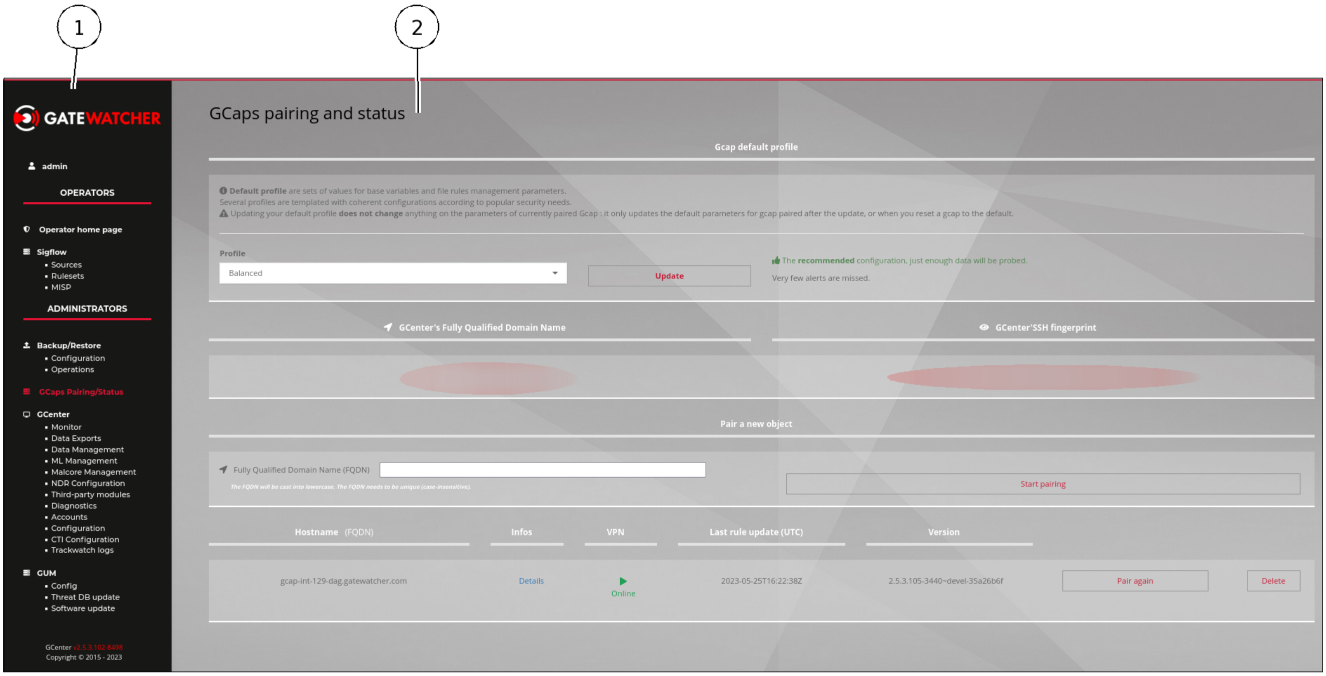
In this interface, most of the menus are not accessible to a user member of the operator group.
The only menus accessible to members of the operator group are the following:

- Sigflow > Sources
- Sigflow > Rulesets

All other menus are only accessible to members of the administrator group.

---

## 5.4.2 Description of the legacy WEB UI



**Default profile** are sets of values for base variables and file rules management parameters.
Several profiles are templated with coherent configurations according to popular security needs.
Updating your default profile **does not change** anything on the parameters of currently paired Gcap : it only updates the default parameters for gcap paired after the update, or when you reset a gcap to the default.

Profile: Balanced

The **recommended** configuration, just enough data will be probed.
Very few alerts are missed.

GCenter's Fully Qualified Domain Name: [redacted]

GCenter'SSH fingerprint: [redacted]

Fully Qualified Domain Name (FQDN)

*The FQDN will be cast into lowercase. The FQDN needs to be unique (case-insensitive).*

| Hostname (FQDN) | Infos | VPN | Last rule update (UTC) | Version |
|---|---|---|---|---|
| gcap-int-129-dag.gatewatcher.com | Details | ▶ Online | 2023-05-25T16:22:38Z | 2.5.3.105-3440~devel-35a26b6f |

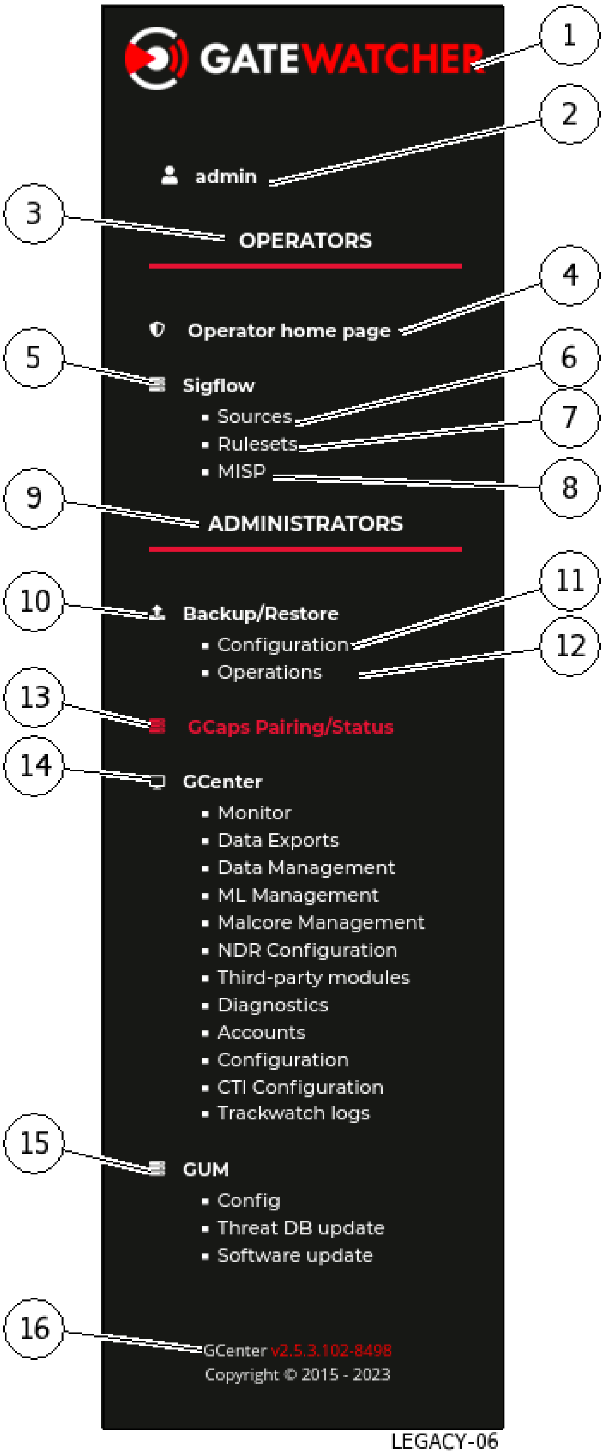
LEGACY-05

The screen consists of following parts:

| Item | Name | Display |
|---|---|---|
| 1 | *Navigation bar of the legacy WEB UI* | Displays the menus and commands for accessing the main functions |
| 2 | *Central screen of the legacy WEB UI* | Displays the screen selected by pressing a command on the navigation bar.<br>Each screen is named like the corresponding command: example `` `GCaps pairing and status` `` screen |

### 5.4.2.1 Navigation bar of the legacy WEB UI

The navigation bar consists of buttons used to access the various functions.
This section provides access to the security policy management functions of the Sigflow engine



GATEWATCHER
admin
OPERATORS
Operator home page
Sigflow
Sources
Rulesets
MISP
ADMINISTRATORS
Backup/Restore
Configuration
Operations
GCaps Pairing/Status
GCenter
Monitor
Data Exports
Data Management
ML Management
Malcore Management
NDR Configuration
Third-party modules
Diagnostics
Accounts
Configuration
CTI Configuration
Trackwatch logs
GUM
Config
Threat DB update
Software update
GCenter v2.5.3.102-8498
Copyright © 2015 - 2023
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
LEGACY-06

| Item | Section name | Display |
|---|---|---|
| 1 | GATEWATCHER logo | *Web UI `Home` screen* : the use of the button enables returning to the main interface if rights are enabled |
| 2 | current user | Indicates the name of the current user. Using the button displays the `logout` command to disconnect. |
| 3 | `OPERATORS` | For members of the administrator group: these commands are visible but not authorized.<br>For members of the operator group: these commands are activated.<br>This section includes the following items:<br>• Item 4 : the `Operator home page` command: this enables returning to the main interface (*Web UI `Home` screen*)<br>• Item 5 : the `Sigflow` menu includes the following commands:<br>• Item 6 : the `Source` command displays (*`Config - sigflow/sources` screen of the legacy web UI*)<br>• Item 7 : the `Rulesets` command displays (*`Config - sigflow/rulesets` screen of the legacy web UI*)<br>• Item 8 : the `MISP` command displays (*`Config - sigflow/MISP` screen of the legacy web UI*) |
| 9 | `ADMINISTRATORS` | For members of the operator group: these commands are visible but not allowed.<br>For members of the administrator group: this section enables access to all administration menus.<br>This section includes the following items:<br>• Item 10 : the `Backup/Restore` menu includes the following commands:<br>• Item 11 : the `Configuration` command enables to configure, automate, and export the backup of the solution (*`Admin-Backup/Restore - Configuration` screen of the legacy web UI*)<br>• Item 12 : the `Operations` command enables to configure, automate, and export the backup of the solution (*`Admin-Backup/Restore - Operations` screen of the legacy web UI*)<br>• Item 13 : the `Gcap Pairing/status` command enables the GCaps to be paired with the GCenter and the default profile to be applied to the GCaps (*`Admin-GCaps pairing and status` screen of the legacy Web UI*)<br>• Item 14 : the `GCenter` menu enables configuring the GCenter. It includes the commands listed in the GCenter menu table below.<br>• Item 15 : the `GUM` menu enables configuring the software update system. It includes the commands listed in GUM menu table below.<br>• Item 16 : GCenter V2.5.3.102-8498. This field displays the GCenter version (here V2.5.3.102-8498) |

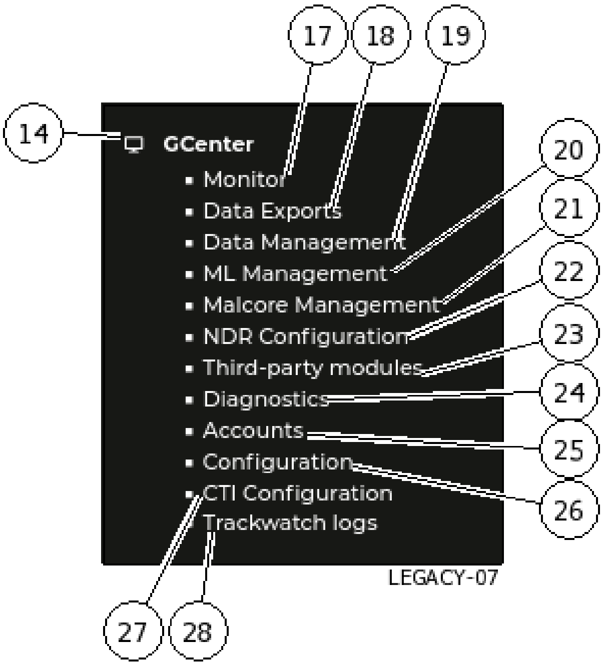

17
18
19
14
GCenter
Monitor
Data Exports
Data Management
ML Management
Malcore Management
NDR Configuration
Third-party modules
Diagnostics
Accounts
Configuration
CTI Configuration
Trackwatch logs
20
21
22
23
24
25
26
LEGACY-07
27
28

Table1: Commandes du menu GCenter (14)

| Item | The `GCenter` menu (14) contains the following commands: |
|---|---|
| 17 | • The `Monitor` command enables accessing certain metrics and statistics from the GCenter (*`Admin-GCenter- Monitor` screen of the legacy web UI*) |
| 18 | • The `Data Exports` command enables the configuring of data exports from the GCenter (*`Admin-GCenter- Data exports` screen of the legacy web UI*) |
| 19 | • The `Data Management` command enables deleting all or part of the data on the GCenter (*`Admin-GCenter- Data Management` screen of the legacy web UI*) |
| 20 | • The `ML Management` command enables configuring the Machine Learning engine (*`Admin-GCenter- ML Management` screen of the legacy web UI*) |
| 21 | • The `Malcore Management` command enables configuring the Malcore engine (*`Admin-GCenter- Malcore Management` screen of the legacy web UI*) |
| 22 | • The `NDR Configuration` command eanbles configuring the NDR dashboards (*Web UI `Admin-NDR configuration` screen*) |
| 23 | • The `Third-party modules` command enables configuring interconnections with third-party products compatible with the solution |
| 24 | • The `Diagnostics` command enables generating and exporting GCenter system logs for analysis by the GATEWATCHER support team. (*`Admin-GCenter- Diagnostics` screen of the legacy web UI*) |
| 25 | • The `Accounts` command enables managing authentication on the GCenter with local or directory authentication (*`Admin-GCenter- Accounts` screen of the legacy web UI*) |
| 26 | • The `Configuration` command enables managing the global configuration of the GCenter including netdata, proxy, certificate, session time, license, and so on. (*`Admin-GCenter-Configuration` screen of the legacy web UI*) |
| 27 | • The `CTI Configuration` command enables activating the CTI engine modules (*`Admin-GCenter- CTI Configuration` screen of the legacy web UI*). |
| 28 | • tThehe `Trackwatch logs` command enables opening the Kibana web interface and viewing the Syslog dashboard (*`Admin-GCenter Trackwatch logs` screen of the legacy web UI*). |

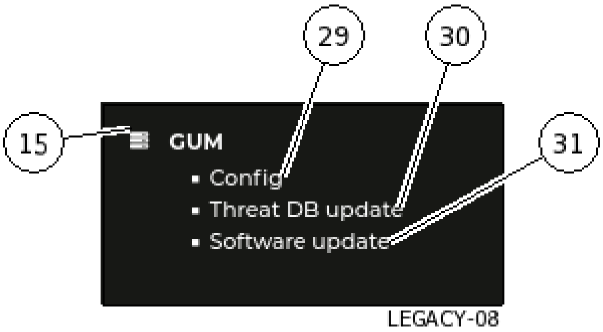


Table2: Tableau menu GUM

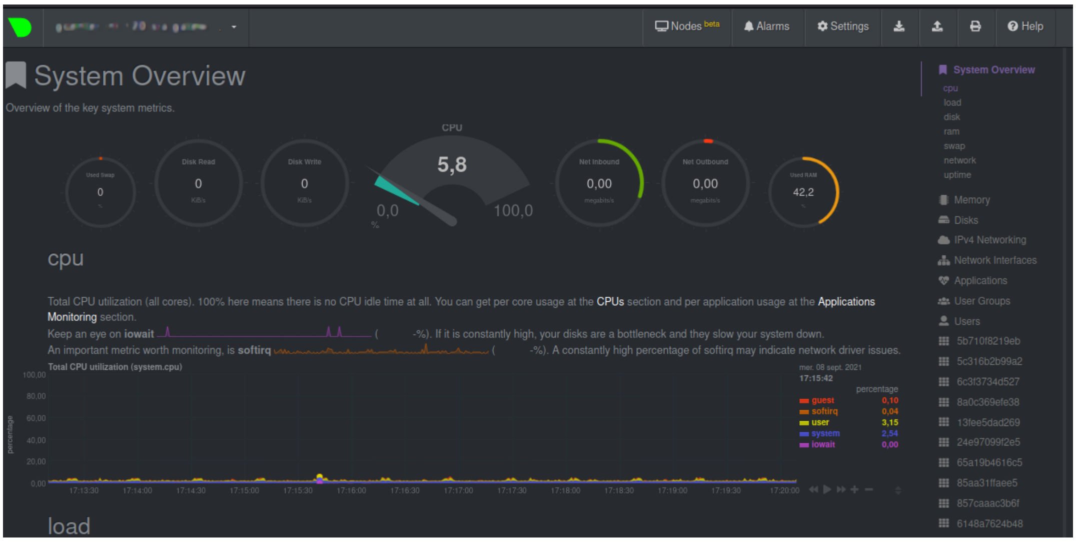
| Item | The `GUM` menu (15) contains the following commands: |
|---|---|
| 29 | • The `Config` command enables automating updates to the solution's engines (*`Admin-GUM - Config` screen of the legacy web UI*) |
| 30 | • The `Threat DB update` command enables manually updating the solution's engines (*`Admin-GUM- Threat DB update` screen of the legacy web UI*) |
| 31 | • The `Software update` command enables updating the solution, either via Hotfix or Upgrade (*`Admin-GUM- Software update` screen of the legacy web UI*) |

### 5.4.3 Central screen of the legacy WEB UI

The central screen displays the information selected by a button on the navigation bar.

## 5.5 Overview of the Netdata User Interface

The GCenter retrieves the GCap metrics.
The GCap and GCenter metrics are transmitted via Netdata to the Netdata server present on the GCenter.
The GCenter Gstats interface uses this data and allows to visualize it for an analysis of the state and consumption of the various physical and software components.
Access to this Gstats interface is available in the title bar of the WEB UI.



Total CPU utilization (all cores). 100% here means there is no CPU idle time at all. You can get per core usage at the **CPUs** section and per application usage at the **Applications Monitoring** section.
Keep an eye on **iowait** ( -%). If it is constantly high, your disks are a bottleneck and they slow your system down.
An important metric worth monitoring, is **softirq** ( -%). A constantly high percentage of softirq may indicate network driver issues.

**Note:**

Only administrators have access to this interface.

This Gstats interface provides administrators with a large number of metrics on different devices.
It is possible via the menu at the top of the page to select the equipment to be administered such as **GCenter** but also the paired GCaps.

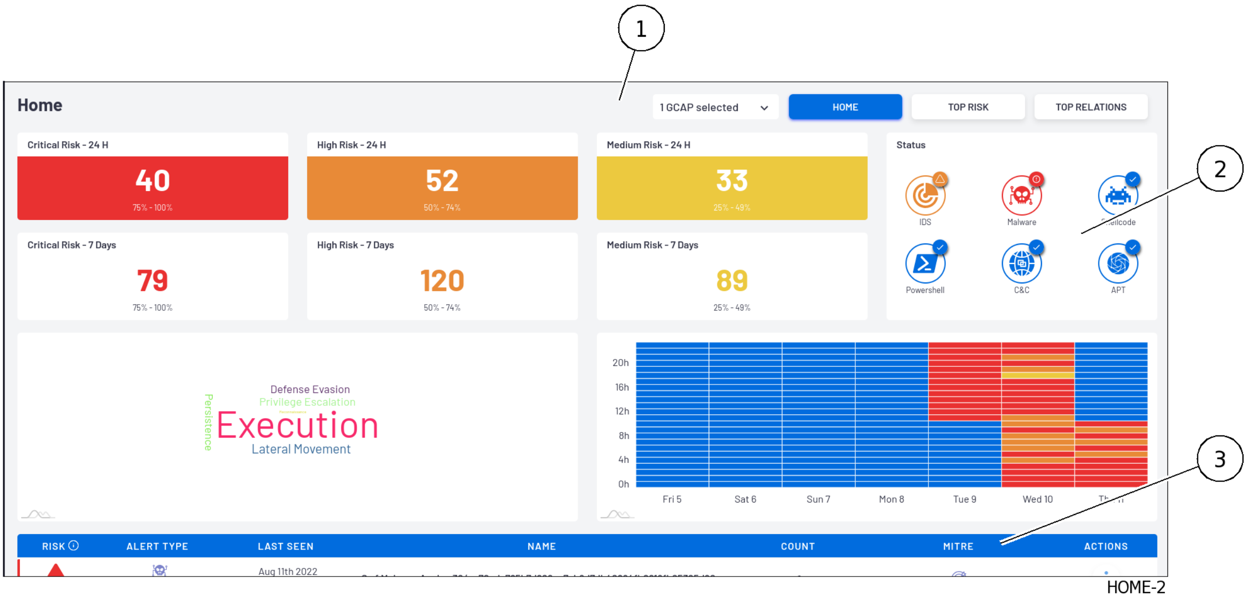
**Note:**

Alternatively, this data will also be available from Kibana in tabs (or dashboards) accessible from the `Kibana` Dashboards menu.

## 5.6 Presentation of graphical interfaces via the web browser

### 5.6.1 Web UI `Home` screen

After pressing one of the `HOME` or `GATEWATCHER` buttons on the navigation bar, the `Home` screen is displayed.
It includes the following items:



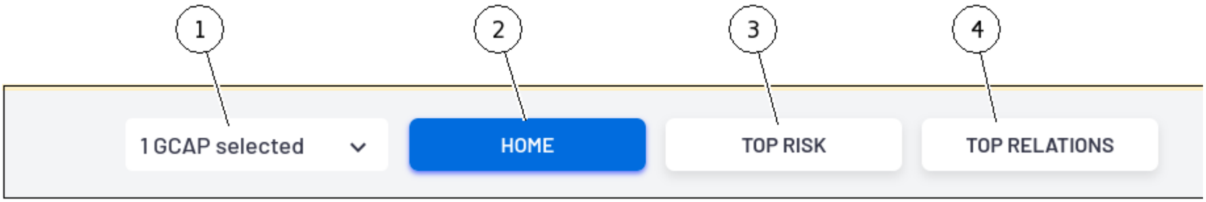
HOME-2

| Item | Description |
|---|---|
| 1 | *`Home` screen dashboard selector* |
| 2 | *`Home` screen display area* |
| 3 | *`Home` screen message area* |

### 5.6.1.1 `Home` screen dashboard selector

The screen displays a set of:

- A button to select the GCap whose information is displayed
- Three buttons to set the theme of the items displayed

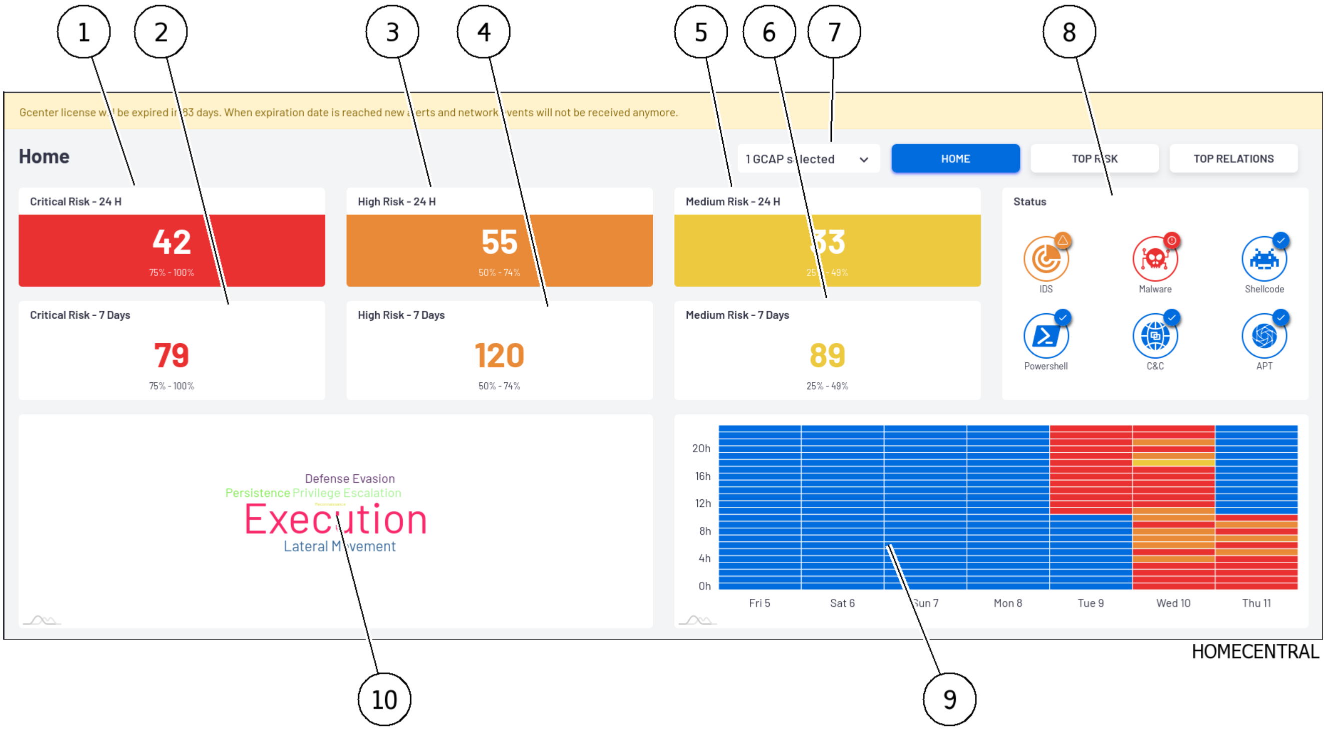


HOME-BUTTON1

| Item | Name | Description | see description |
|---|---|---|---|
| 1 | Display of selected GCaps | Selection of GCaps | |
| 2 | `HOME` | Selection of the default display | see below |
| 3 | `TOP RISK` | Selection of the main risk screen | *Web UI `Top risk` screen* |
| 4 | `TOP RELATIONS` | Selection of the main relationships screen | *Web UI `Top Relations` screen* |

#### 5.6.1.2 `Home` screen display area

After pressing one of the `HOME` or `GATEWATCHER` buttons, the display area looks like this:



HOMECENTRAL

The display shows the information of the selected GCap(s) (7).
The screen provides a summary of the detection status:

- The area indicating the number of potential risks by level and date (item 1 to 6)
  These elements forming this zone are listed below:
- Risk counters classified as **Critical risk** :
- Definition of a **critical risk**: very suspicious activity was detected. Dangerous activity was detected. There is a high probability that your organization is facing a serious threat and counter-meseares should be taken immediately.
  For example, a user downloaded malware or an active network element contacted a known command and control domain.
- Definition of the color used for this type of alarms in the Web UI: red
- Risk level of this category: 75 to 100%

| Benchmark | Engine | State |
|---|---|---|
| 1 | `Critical risk` `24h` | Counter giving the number of risks **critical** appeared in the last 24 hours<br>If you press this counter, then the system displays the detailed list of each of these risks (Alerts screen) |
| 2 | `Critical risk` `7 days` | Counter giving the number of risks **critical** appeared in the last 7 days<br>If you press this counter, then the system displays the detailed list of each of these risks (Alerts screen) |

- Risk counters classified as **High risk** :
- Definition of a **high risk**: a very suspicious activity has been detected. This type of event should be investigated promptly as it could be a sign of significant compromise.

  It is possible that this event is a false positive or related to a bad representation in the network.
- Definition of the color used for this type of alarms in the Web UI: orange
- Risk level in this category: 50-74%

| Benchmark | Engine | State |
|---|---|---|
| 3 | \`High risk\`<br>\`24h | Counter giving the number of risks **high** appeared in the last 24 hours<br>If you press this counter, then the system displays the detailed list of each of these risks (Alerts screen) |
| 4 | \`High risk\`<br>\`7 days\` | Counter giving the number of risks **high** appeared in the last 7 days<br>If you press this counter, then the system displays the detailed list of each of these risks (Alerts screen) |

- Risk counters classified as **Medium risk**:
- Definition of a **medium risk**: an activity that could be related to a threat has been detected.

  The risk has been established at low values because the potential threat does not appear critical or because the probability of false is high.
- Definition of the color used for this type of alarms in the Web UI: yellow
- Risk level in this category: 25-49%

| Benchmark | Engine | State |
|---|---|---|
| 5 | \`Medium risk\`<br>\`24h\` | Counter giving the number of risks **average** appeared in the last 24 hours<br>If you press this counter, the system displays the detailed list of each of these risks (Alerts screen). |
| 6 | \`Medium risk\`<br>\`7 days\` | Counter giving the number of risks **average** appeared in the last 7 days<br>If you press this counter, the system displays the detailed list of each of these risks (Alerts screen). |

- Risks classified as **low risk** have no counter displayed:
- Definition of a **low risk**: unusual activity has been detected. This could mean that you have unusual network policies or uses.

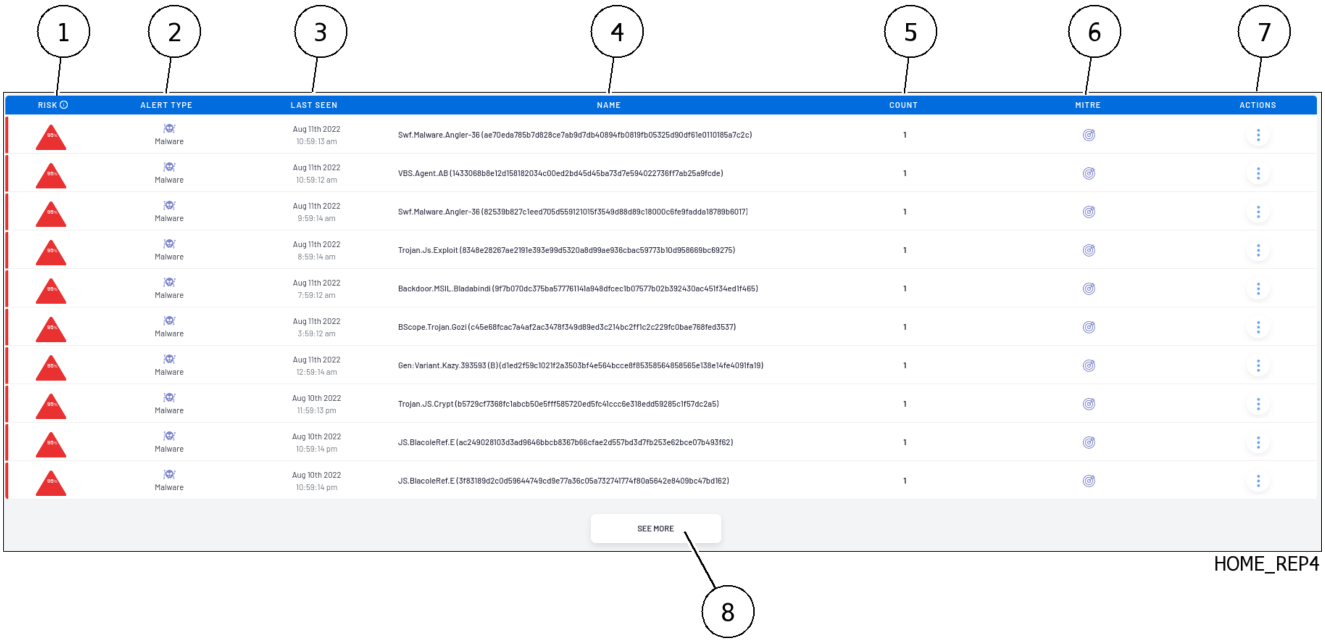
  These types of events should be mentioned last because they are not a direct sign of significant compromises.
- Definition of the color used for this type of alarms in the Web UI: blue
- Risk level for this category: 0-24%

- The engine condition zone (8).

  If you press this area, then the system displays the \`Health Checks\` page (see *Web UI \`Health checks\` screen*).
- The area indicating the date of detection (9): this calendar indicates when potential threats have been detected.
- The MITRE association area (10).

If pressed, then the system displays the `Alerts` MITRE filtering page (see *Web UI `Alerts` screen*).

### 5.6.1.3 `Home` screen message area



| RISK ⓘ | ALERT TYPE | LAST SEEN | NAME | COUNT | MITRE | ACTIONS |
|---|---|---|---|---|---|---|
| 95% | Malware | Aug 11th 2022<br>10:59:13 am | Swf.Malware.Angler-36 (ae70eda785b7d828ce7ab9d7db40894fb0819fb05325d90df61e0110185a7c2c) | 1 | ◎ | ⋮ |
| 95% | Malware | Aug 11th 2022<br>10:59:12 am | VBS.Agent.AB (1433068b8e12d158182034c00ed2bd45d45ba73d7e594022736ff7ab25a9fcde) | 1 | ◎ | ⋮ |
| 95% | Malware | Aug 11th 2022<br>9:59:14 am | Swf.Malware.Angler-36 (82539b827c1eed705d559121015f3549d88d89c18000c6fe9fadda18789b6017) | 1 | ◎ | ⋮ |
| 95% | Malware | Aug 11th 2022<br>8:59:14 am | Trojan.Js.Exploit (8348e28267ae2191e393e99d5320a8d99ae936cbac59773b10d958669bc69275) | 1 | ◎ | ⋮ |
| 95% | Malware | Aug 11th 2022<br>7:59:12 am | Backdoor.MSIL.Bladabindi (9f7b070dc375ba57776114la948dfcec1b07577b02b392430ac451f34ed1f465) | 1 | ◎ | ⋮ |
| 95% | Malware | Aug 11th 2022<br>3:59:12 am | BScope.Trojan.Gozi (c45e68fcac7a4af2ac3478f349d89ed3c214bc2ff1c2c229fc0bae768fed3537) | 1 | ◎ | ⋮ |
| 95% | Malware | Aug 11th 2022<br>12:59:14 am | Gen:Variant.Kazy.393593 (B) (d1ed2f59c1021f2a3503bf4e564bcce8f85358564858565e138e14fe4091fa19) | 1 | ◎ | ⋮ |
| 95% | Malware | Aug 10th 2022<br>11:59:13 pm | Trojan.JS.Crypt (b5729cf7368fc1abcb50e5fff585720ed5fc41ccc6e318edd59285c1f57dc2a5) | 1 | ◎ | ⋮ |
| 95% | Malware | Aug 10th 2022<br>10:59:14 pm | JS.BlacoleRef.E (ac249028103d3ad9646bbcb8367b66cfae2d557bd3d7fb253e62bce07b493f62) | 1 | ◎ | ⋮ |
| 95% | Malware | Aug 10th 2022<br>10:59:14 pm | JS.BlacoleRef.E (3f83189d2c0d59644749cd9e77a36c05a732741774f80a5642e8409bc47bd162) | 1 | ◎ | ⋮ |

SEE MORE

HOME_REP4

The list of messages displays the 10 aggregate threats with the highest level of risk.
This area gives the following information:

| Benchmark | Name | Description |
|---|---|---|
| 1 | `RISK | If you press the i icon then the system displays the risk definition and the corresponding color |
| 2 | `ALERT TYPE` | Alert type (malware, shellcode, IDS, powershell, etc.) |
| 3 | `LAST SEEN` | Date and time of last appearance<br>If pressing the threat then the Alerts window displays threats with the same infection |
| 4 | `NAME` | Name of alert<br>If you press this field then the Alerts window displays threats with the same infection as the selected infection |
| 5 | `COUNT` | Number of alarm occurrences |
| 6 | `MITRE` | Type of threat icon: see paragraph *MITRE Icons* |
| 7 | `ACTIONS` | Displays sub menu `ACTIONS`<br>For a malware threat, the possible action is `Files transactions`. This command opens a Kibana window in the `Malcore` tab.<br>For a Shellcode threat, the possible action is `Go Hunting`. This command opens a Kibana window in the `Codebreaker` tab. |

Pressing a threat opens the `Alerts` window that displays threats with the same infection as the selected infection
The button (8) `SEE MORE` displays information on the `Alerts` page (see *Web UI `Alerts` screen*).

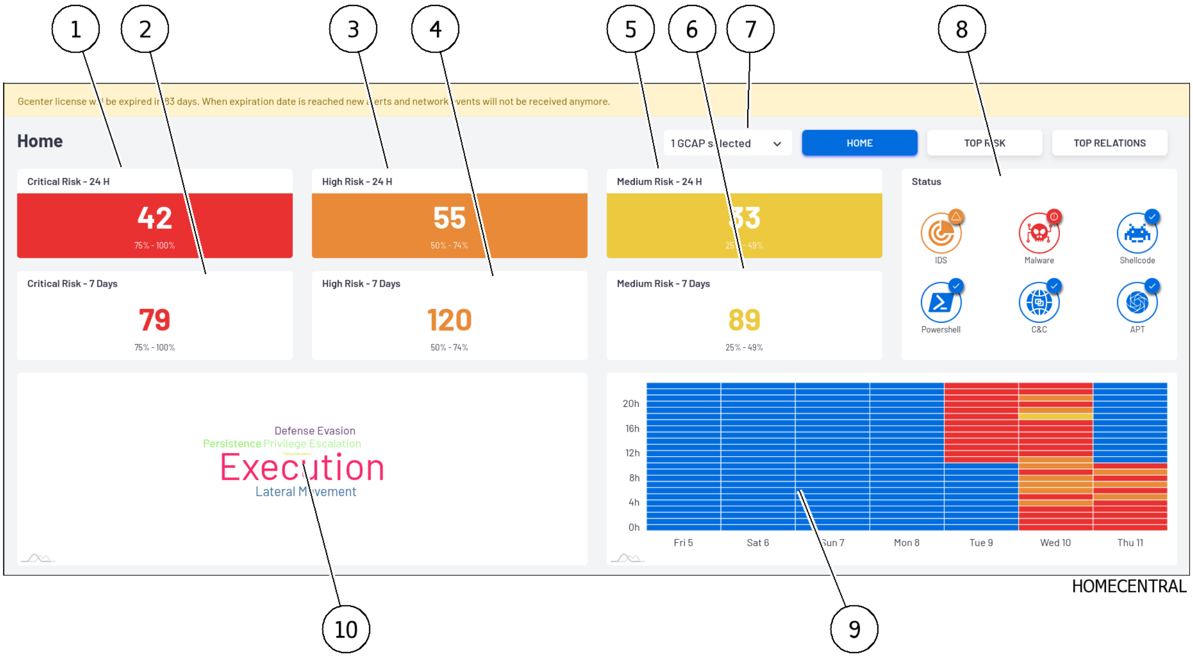
#### 5.6.1.3.1 MITRE Icons

In the MITRE column, the following icons can be displayed:

| Icon | Name | Description of threat type | see more information |
|---|---|---|---|
| | Execution | Opponent is trying to execute malicious code. | https://attack.mitre.org/versions/v10/tactics/TA0002/ |
| | Persistence | Opponent trying to maintain hold | https://attack.mitre.org/versions/v10/tactics/TA0003/ |
| | Privilege Escalation | Opponent trying to get higher level permissions | https://attack.mitre.org/versions/v10/tactics/TA0004/ |
| | Defense Evasion | The opponent tries to avoid being detected. | https://attack.mitre.org/versions/v10/tactics/TA0005/ |
| | Lateral Movement | The opponent tries to move around your environment. | https://attack.mitre.org/versions/v10/techniques/T1210/ |

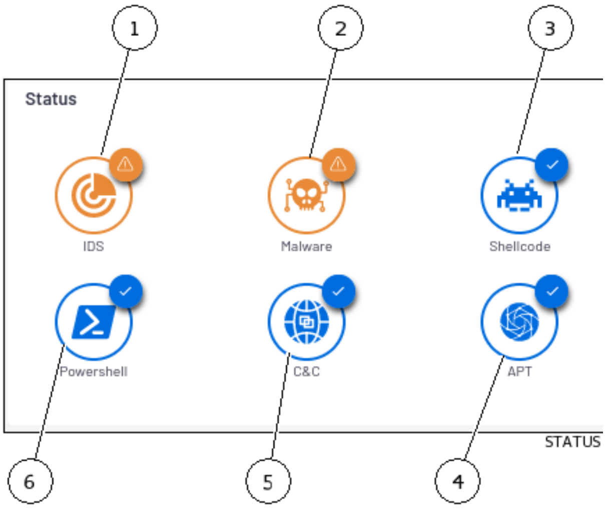
## 5.6.2 Web UI `Health checks` screen

After pressing one of the `HOME` or `GATEWATCHER` buttons, the display area will be as follows:



Gcenter license w‹ be expired ir 83 days. When expiration date is reached new ‹erts and network ‹vents will not be received anymore.

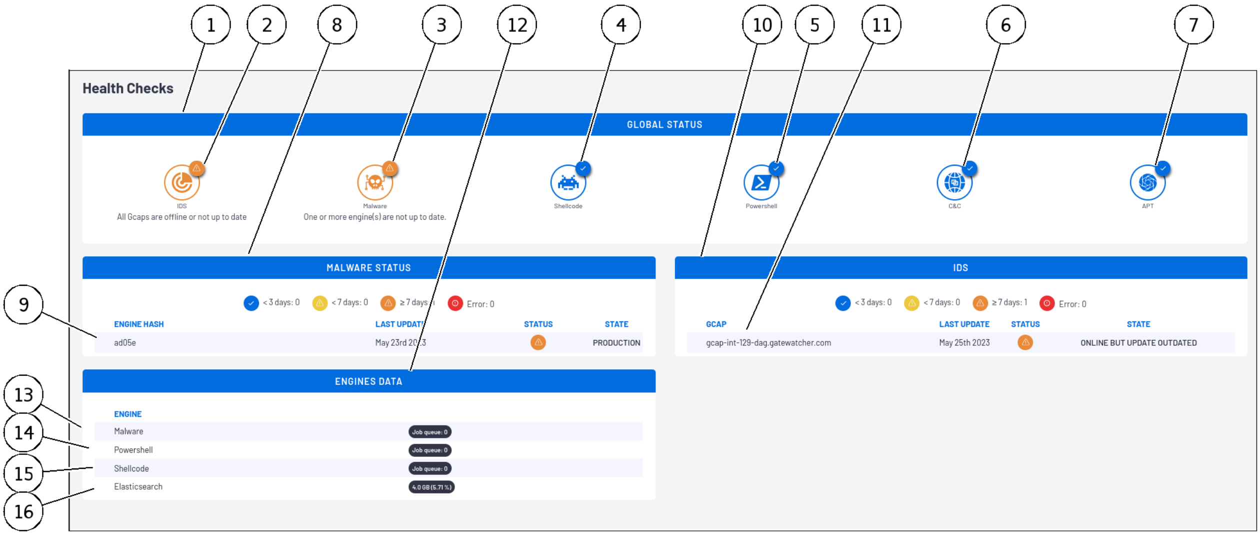
The `Status` zone displays the simplified status of the detection systems managed by the GCenter.



This area gives the status of the following components:

| Benchmark | Engine | For |
|---|---|---|
| 1 | IDS (GCAp probe) | Transmit captured events and files to GCenter |
| 2 | Malcore | Detect Malware |
| 3 | Codebreaker | Detect Shellcodes |
| 4 | CTI | Uses LastInfoSec compromise indices to generate alerts for Advanced Persistent Threat (APT) threats |
| 5 | Machine Learning | Detect domain names that have been generated by Domain Generation Algorithm (DGA) for Command & Control (C&C) type threats |
| 6 | Codebreaker | Detect Powershells |

In order to get detailed information, it is possible to click on the area and open a new screen.



Health Checks

GLOBAL STATUS

All Gcaps are offline or not up to date

One or more engine(s) are not up to date.

MALWARE STATUS

✓ < 3 days: 0 ⚠ < 7 days: 0 ⚠ ≥ 7 days: 1 ⓘ Error: 0

| ENGINE HASH | LAST UPDATE | STATUS | STATE |
|---|---|---|---|
| ad05e | May 23rd 2023 | ⚠ | PRODUCTION |

IDS

✓ < 3 days: 0 ⚠ < 7 days: 0 ⚠ ≥ 7 days: 1 ⓘ Error: 0

| GCAP | LAST UPDATE | STATUS | STATE |
|---|---|---|---|
| gcap-int-129-dag.gatewatcher.com | May 25th 2023 | ⚠ | ONLINE BUT UPDATE OUTDATED |

ENGINES DATA

| ENGINE | |
|---|---|
| Malware | Job queue: 0 |
| Powershell | Job queue: 0 |
| Shellcode | Job queue: 0 |
| Elasticsearch | 4.0 GB (5.71 %) |

HEALTH_CHECKS

The `Health Checks` screen consists of the following areas:

- field (1) `GLOBAL STATUS` indicating the status of the detection engines (GCap and GCenter): see *The `GLOBAL STATUS`*
- field (8) `MALWARE STATUS` indicating the status of the GCenter Malcore engine: see *The `MALWARE STATUS`*
- field (10) `IDS` indicating the status of the GCap Sigflow engine: see *The `IDS` zone*
- field (12) `ENGINES DATA` indicating the general status of the data (data queues and database): see *The `ENGINES DATA`*

---

#### 5.6.2.1 The `GLOBAL STATUS`

Field (1) `GLOBAL STATUS` includes:

Table3: Example of a state with 2 defects

| Benchmark | Engine | State | For more information |
|---|---|---|---|
| 2 | IDS (GCAp probe) | blue check mark: GCaps are connected and up to date<br>red panel: GCaps are offline or not up to date | refer to *The `IDS` zone* (10) |
| 3 | Malware (detection by Malcore engine) | blue check mark: Malcore engine is active and running<br>red sign: one or more engines are out of date | refer to *The `MALWARE STATUS`* (8) |
| 4 | Shellcode | blue check mark: Codebreaker goasm engine is active and running<br>red panel: Codebreaker goasm engine is not active or not working | refer to *Engine restart* |
| 5 | Powershell | blue check mark: Codebreaker gps engine is active and working<br>red panel: the engine Codebreaker gps is not active or does not work | refer to *Engine restart* |
| 6 | C&C (Command & Control) | blue check mark: gdgadetect Machine Learning engine is active and running<br>red panel: gdgadetect Machine Learning engine is not active or not working | refer to *Engine restart* |
| 7 | APT (Advanced Persistent Threat) | blue check mark: gcti CTI engine is active and running<br>red panel: gcti CTI engine is not active or not working | refer to *Engine restart* |

#### 5.6.2.2 The `IDS` zone

The IDS area indicates the status of the GCap probe (11) connected to the GCenter.
The information given is:

- The name
- Date of last update
- The status
- The state

In the example shown, the message is `All Gcaps are offline or not up to date`.
To find out if the GCaps or GCaps are online or offline, it must be checked in the column `STATE` for each of the GCaps present: in this example, the GCap present is in the state `ONLINE`.
To find out if the GCap Sigflow engine is up to date, check the column `STATE` with the message `OUTDATED`.
For more information on the date of the last update, see the `LAST UPDATE` column.

**Note:**

The engine is in `running` status if the Sigflow engine is installed and the API is up.

**Note:**

To update, refer to *Manual installation of an update of signatures and/or anti-viral engines (update)* to download and install the latest sigflow.gwp file.

---

#### 5.6.2.3 The `MALWARE STATUS`

The area (8) `MALWARE STATUS` includes:

- An antivirus engine (for some licenses): this is the case in this example
- Or 16 antivirus engines (for other licenses)

The information given is:

- Engine hash name
- Date of last engine package update
- The status which indicates the age of the engine package via the colour signage
- Package installation status (PRODUCTION = OK)

In the example shown, the status is orange and the message is `One or more engine(s) are not up to date`.
To know the seniority of the current package of the engine, you have to look at the column `LAST UPDATE` to have the date and the icon present in the column `STATUS`: in this example, the package has more than 7 days.

**Note:**

If there is an update issue, refer to *Manual installation of an update of signatures and/or anti-viral engines (update)* to download and install the latest malcore.gwp file.
To restart the Malcore engine, use the `` `Restart a GApp` `` command from the configuration menu and select `` `gmalcore` ``.

#### 5.6.2.4 The `` `ENGINES DATA` ``

Zone (12) `` `ENGINES DATA` `` includes:

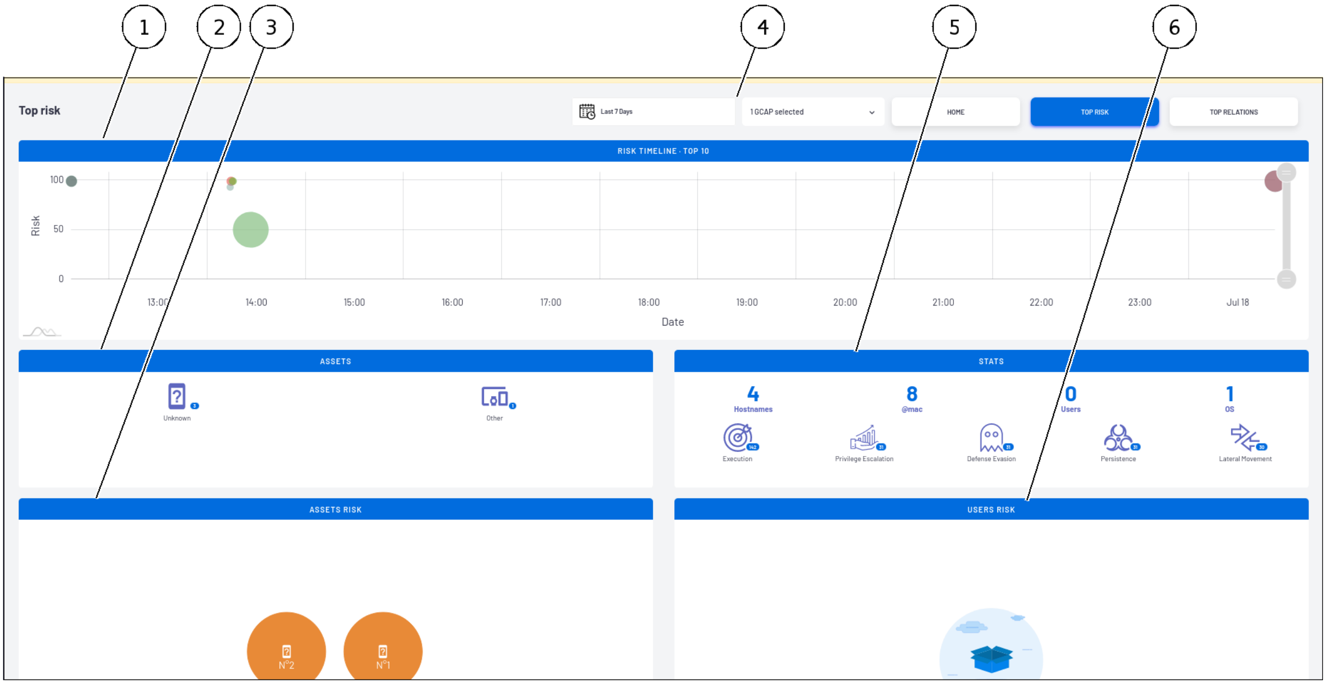
- Data queues waiting in front of engines detecting Malwares, Powershells, shellcodes
- The size of the Elasticsearch database (in volume and percentage);

#### 5.6.2.5 Engine restart

To restart the Codebreaker goasm engine, use the `` `Restart a GApp` `` command from the configuration menu and select `` `goasm` ``.
To restart the Codebreaker gps engine, use the `` `Restart a GApp` `` command from the configuration menu and select `` `gps` ``.
To restart the gdgadetect engine, use the `` `Restart a GApp` `` command from the configuration menu and select `` `gdgadetect` ``.
To restart the gcti CTI engine, use the `` `Restart a GApp` `` command from the configuration menu and select `` `gcti` ``.

### 5.6.3 Web UI `` `Top risk` `` screen

After pressing one of the `` `HOME` `` buttons and then the `` `TOP RISK` `` button, the following screen is displayed.



TOP-RISK

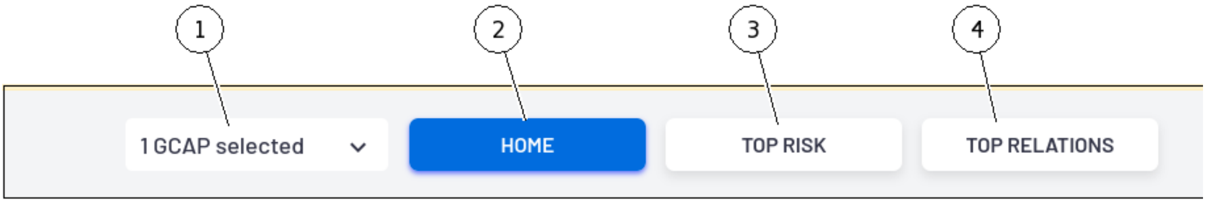
This screen includes the following:

| Benchmark | Zone | To display |
|---|---|---|
| 1 | *`RISK TIMELINE` zone* | Alarm timing and risk levels |
| 2 | *`ASSETS` zone* | List of active equipment found |
| 3 | *`ASSETS RISK` zone* | Representation of the number of alerts of active equipment |
| 4 | *Dashboard Selector* | Statistics on detected threats; |
| 5 | *`STATS` zone* | A list of meters |
| 6 | *`USERS RISK` zone* | The number of alerts from active users |

### 5.6.3.1 Dashboard Selector

The screen displays a set of:

- A button to select the GCap whose information was displayed
- Three buttons to define the theme of the displayed elements



HOME-BUTTON1

| Item | Name | Description | View Description |
|---|---|---|---|
| 1 | View Selected GCaps | GCap Selection | |
| 2 | `HOME` | Default Display Selection | *Web UI `Home` screen* |
| 3 | `TOP RISK` | Selecting the Main Risk Screen | below |
| 4 | `TOP RELATIONS` | Selecting the Main Relations Screen | *Web UI `Top Relations` screen* |

#### 5.6.3.2 `RISK TIMELINE` zone

The `RISK TIMELINE` zone indicates the alarm sequence and their risk levels:

- Horizontal axis: date and time of threat
- Vertical axis: risk level
- Each threat is placed on the graph, its size indicating the number of alerts.
  Hovering over the threat displays the following:

- Hostname
- IP
- Risk
- Alert count
- Date
- MITRE threat type

#### 5.6.3.3 `ASSETS` zone

The `ASSETS` zone displays the list of active equipment found in the detected threats.
By clicking on each equipment, the `Assets` window is displayed on that equipment.

#### 5.6.3.4 `ASSETS RISK` zone

The `ASSETS RISK` zone displays the number of alerts of active equipment in the form of a bubble.
The size of the bubble depends on the number of alerts on this equipment.
By clicking on an equipment, the `Assets` detailed window is displayed on that equipment.

#### 5.6.3.5 `STATS` zone

The `STATS` zone displays the following counters:

- `Hostnames`
- `@mac`
- `Users`
- `OS`
- MITRE counters:
  - `Execution`

- `Persistence`
- `Privilege Escalation`
- `Defense Evasion`
- `Lateral Movement`

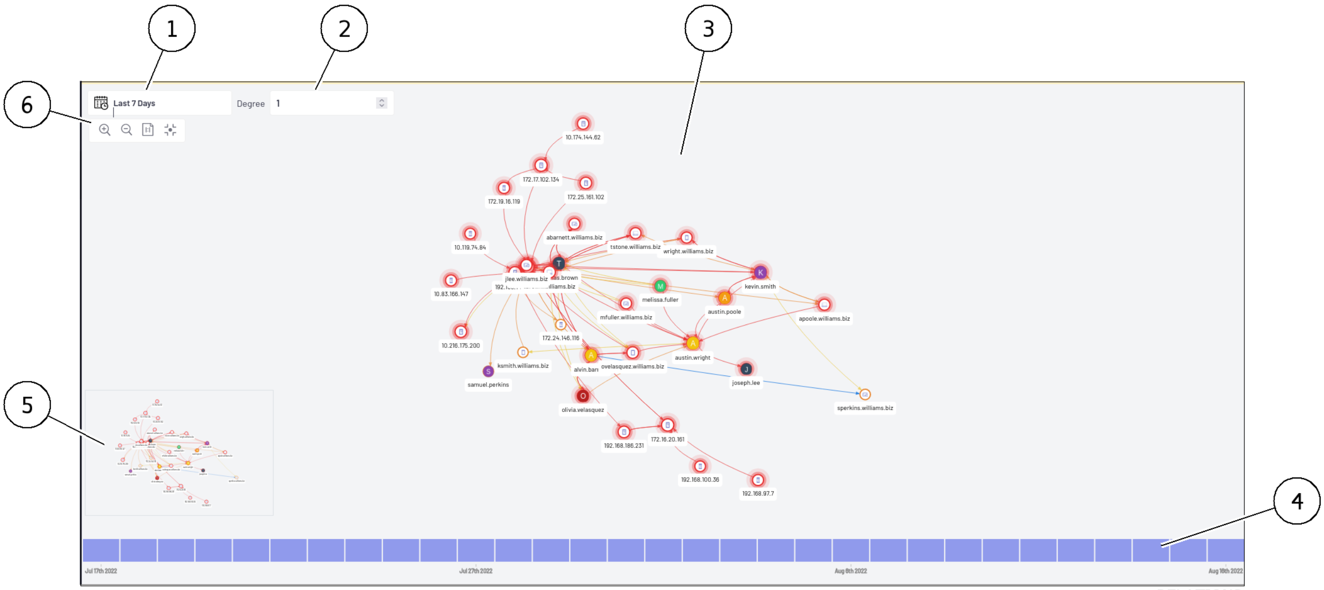
If a counter is pressed, the system displays a detailed list of each of these risks (Alerts screen).

#### 5.6.3.6 `USERS RISK` zone

The `USERS RISK` zone displays the number of active user alerts as bubbles.

### 5.6.4 Web UI `Top Relations` screen

After pressing one of the `HOME` buttons and then the `TOP RELATIONS` button, the following screen is displayed.

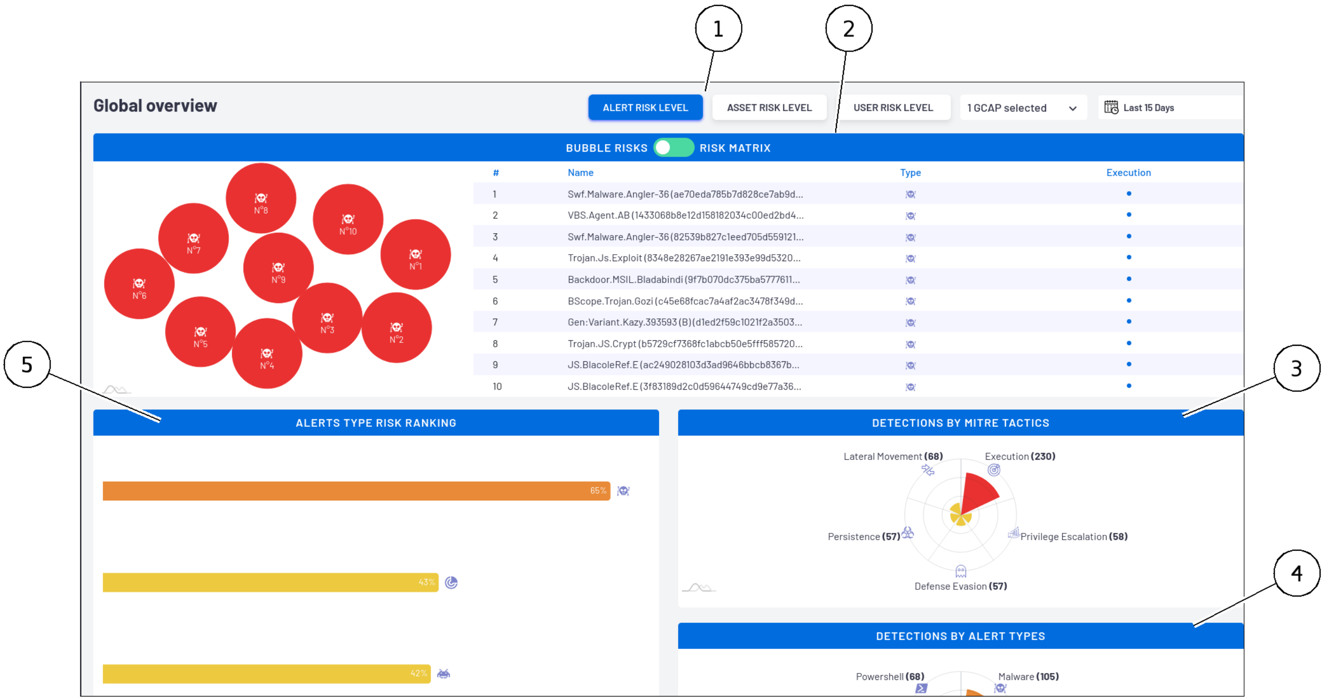


RELATIONS

This screen shows the equipment on the network and the relationships between them.
This screen is detailed in the *Web UI `Relations` screen*.

### 5.6.5 Web UI `Overview` screen

After pressing the `Overview` buttons on the navigation bar, the `Overview` screen is displayed.
It includes the following items:

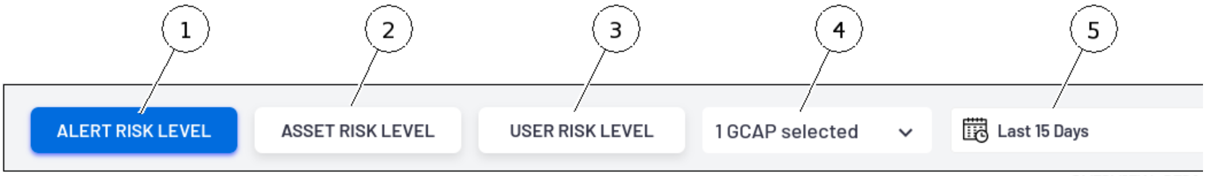


| # | Name | Type | Execution |
|---|---|---|---|
| 1 | Swf.Malware.Angler-36 (ae70eda785b7d828ce7ab9d... | ☠ | ● |
| 2 | VBS.Agent.AB (1433068b8e12d158182034c00ed2bd4... | ☠ | ● |
| 3 | Swf.Malware.Angler-36 (82539b827c1eed705d559121... | ☠ | ● |
| 4 | Trojan.Js.Exploit (8348e28267ae2191e393e99d5320... | ☠ | ● |
| 5 | Backdoor.MSIL.Bladabindi (9f7b070dc375ba5777611... | ☠ | ● |
| 6 | BScope.Trojan.Gozi (c45e68fcac7a4af2ac3478f349d... | ☠ | ● |
| 7 | Gen:Variant.Kazy.393593 (B) (d1ed2f59c1021f2a3503... | ☠ | ● |
| 8 | Trojan.JS.Crypt (b5729cf7368fc1abcb50e5fff585720... | ☠ | ● |
| 9 | JS.BlacoleRef.E (ac249028103d3ad9646bbcb8367b... | ☠ | ● |
| 10 | JS.BlacoleRef.E (3f83189d2c0d59644749cd9e77a36... | ☠ | ● |

OVERVIEW

| Item | Description |
|---|---|
| 1 | *`Overview` screen : dashboard selector* |
| 2 | *`Overview` screen alerts list display area* |
| 3 | *`DETECTIONS BY ALERTE TACTICS` zone of the `Overview` screen* |
| 4 | *`DETECTIONS BY MITRE TACTICS` zone of the `Overview` screen* |
| 5 | *`ALERTS TYPE RISK RANKING` zone of the `Overview` screen* |

#### 5.6.5.1 `Overview` screen : dashboard selector



OVERVIEW_REP1

The screen displays a set of:

- One button (4) to select the GCap(s) whose information is displayed
- One button (5) for the period for which the information is displayed
- Three buttons (1 to 3) to define the theme of the dashboards displayed on this page

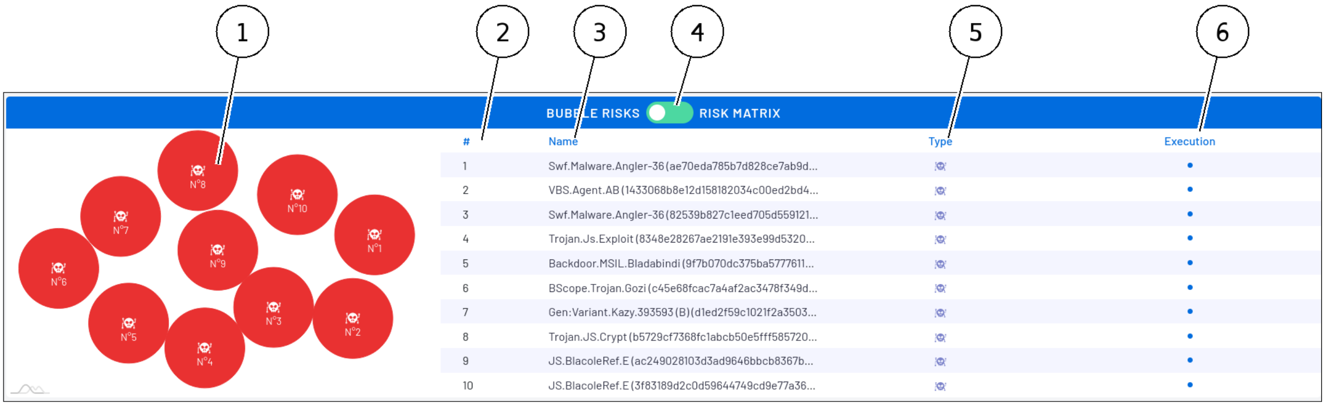
| Item | Name | Description |
|---|---|---|
| 1 | `ALERT RISK LEVEL` | Alert Risk Level. Defines `ALERTS` theme for dashboards |
| 2 | `ASSET RISK LEVEL` | Risk level of assets. Defines the `ASSET` theme for dashboards |
| 3 | `USER RISK LEVEL` | User Risk Level . Defines the `USER` theme for dashboards |
| 4 | GCAP selector | Selection of GCap |
| 5 | Time period selector | Selection of the display period |

### 5.6.5.2 `Overview` screen alerts list display area

The display of the alerts is possible in 2 ways selectable by the button (4):

- Display `BUBBLE RISKS`
- Display `RISK MATRIX`

For the ALERTS theme, the `BUBBLE RISKS` display consists of:

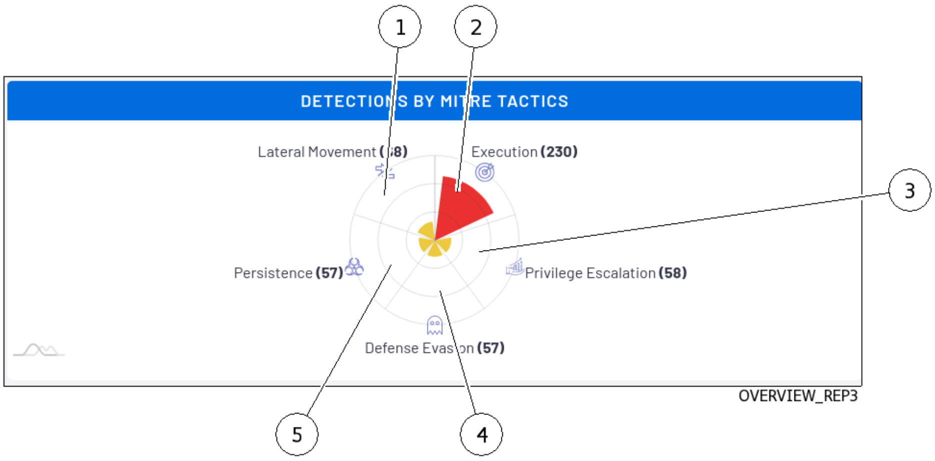


| # | Name | Type | Execution |
|---|---|---|---|
| 1 | Swf.Malware.Angler-36 (ae70eda785b7d828ce7ab9d... | ☠ | ● |
| 2 | VBS.Agent.AB (1433068b8e12d158182034c00ed2bd4... | ☠ | ● |
| 3 | Swf.Malware.Angler-36 (82539b827c1eed705d559121... | ☠ | ● |
| 4 | Trojan.Js.Exploit (8348e28267ae2191e393e99d5320... | ☠ | ● |
| 5 | Backdoor.MSIL.Bladabindi (9f7b070dc375ba5777611... | ☠ | ● |
| 6 | BScope.Trojan.Gozi (c45e68fcac7a4af2ac3478f349d... | ☠ | ● |
| 7 | Gen:Variant.Kazy.393593 (B) (d1ed2f59c1021f2a3503... | ☠ | ● |
| 8 | Trojan.JS.Crypt (b5729cf7368fc1abcb50e5fff585720... | ☠ | ● |
| 9 | JS.BlacoleRef.E (ac249028103d3ad9646bbcb8367b... | ☠ | ● |
| 10 | JS.BlacoleRef.E (3f83189d2c0d59644749cd9e77a36... | ☠ | ● |

OVERVIEW_REP2

| Item | Description |
|---|---|
| 1 | Bubble zone. Each element (here an alert) is displayed as a bubble.<br>Each item is numbered and corresponds to the list displayed next to it.<br>By hovering over an element, a window gives additional information.<br>- Number, not Alert<br>- Risk: percentage level of risk<br>- Alert counter<br>- type of MITRE alerts |
| 2 | Alert number |
| 3 | Name of detected threat<br>By hovering over an element, a window gives the same additional information.<br>By clicking on the name, the system displays the `Alerts` screen for the selected threat for more information. |
| 4 | Display change button (bubbles/matrix) |
| 5 | Type field: type of risk (malware...) |
| 6 and following | Each column indicates the category MITRE (`Execution`, `Persistence`, `Privilege Escalation`, `Defense Evasion`, `Lateral Movement`).<br>Each point defines the threat category. |

### 5.6.5.3 `DETECTIONS BY MITRE TACTICS` zone of the `Overview` screen



The system displays the distribution of risks between the following categories in a circular fashion:

| Benchmark | Name | Description |
|---|---|---|
| 1 | `Lateral Movement` | Number of lateral movements |
| 2 | `Execution` | Number of threats executed |
| 3 | `Privilege Escalation` | Number of privilege escalation |
| 4 | `Defense Evasion` | Number of defensive escapes |
| 5 | `Persistence` | Number of persistent threats |

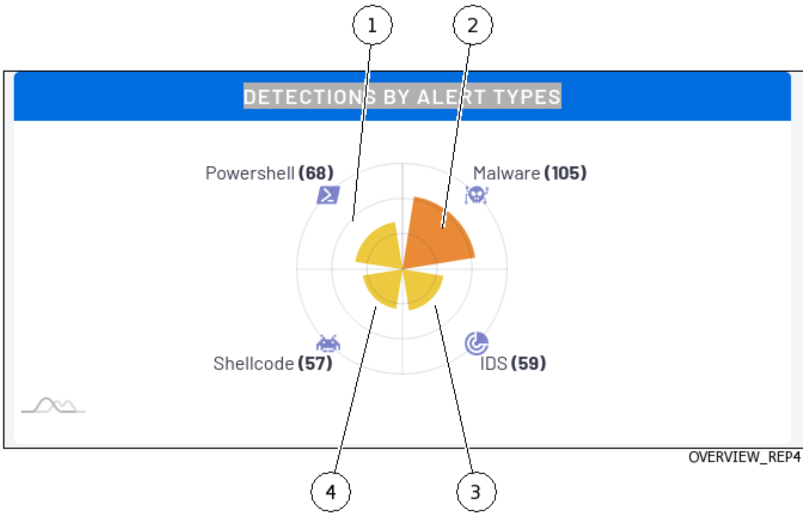
**Note:**

Depending on the threat, only the categories present are displayed.

In the MITRE column, the following icons can be displayed:

| Icon | Name | Description of threat type | see more information |
|---|---|---|---|
| | Execution | Opponent is trying to execute malicious code. | https://attack.mitre.org/versions/v10/tactics/TA0002/ |
| | Persistence | Opponent trying to maintain hold | https://attack.mitre.org/versions/v10/tactics/TA0003/ |
| | Privilege Escalation | Opponent trying to get higher level permissions | https://attack.mitre.org/versions/v10/tactics/TA0004/ |
| | Defense Evasion | The opponent tries to avoid being detected. | https://attack.mitre.org/versions/v10/tactics/TA0005/ |
| | Lateral Movement | The opponent tries to move around your environment. | https://attack.mitre.org/versions/v10/techniques/T1210/ |

### 5.6.5.4 `DETECTIONS BY ALERTE TACTICS` zone of the `Overview` screen



The system displays a circular risk breakdown between the following categories:

| Benchmark | Name | Description |
|---|---|---|
| 1 | `Powershell` | Number of powershells detected |
| 2 | `Malware` | Number of shellcodes detected |
| 3 | `IDS` | Number of malware detected |
| 4 | `shellcode` | Number of IDS detected |

#### 5.6.5.5 `ALERTS TYPE RISK RANKING` zone of the `Overview` screen

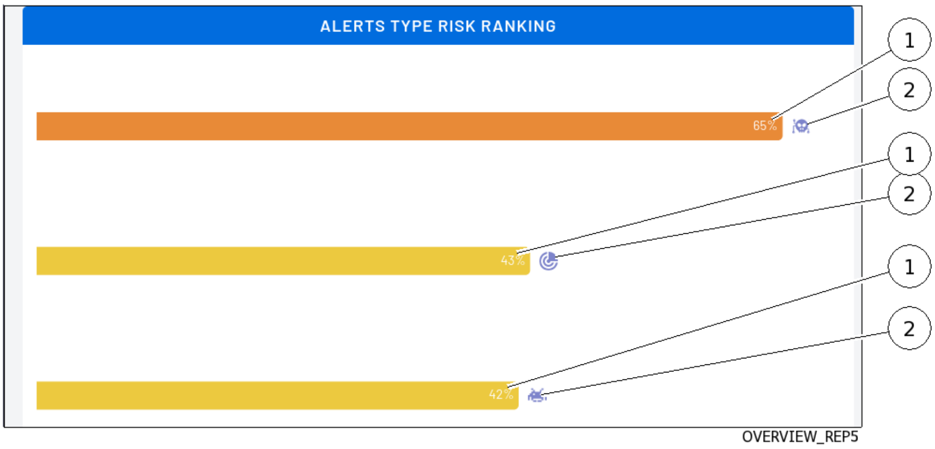
The system displays the risks:

- Grouped by type of alert
- Sorted by decreasing risk level

Each bar of the graph indicates the percentage of the risk and the type of alert.
Passing the cursor, the system displays:

- The type of alert
- The percentage of risk
- The number of alerts

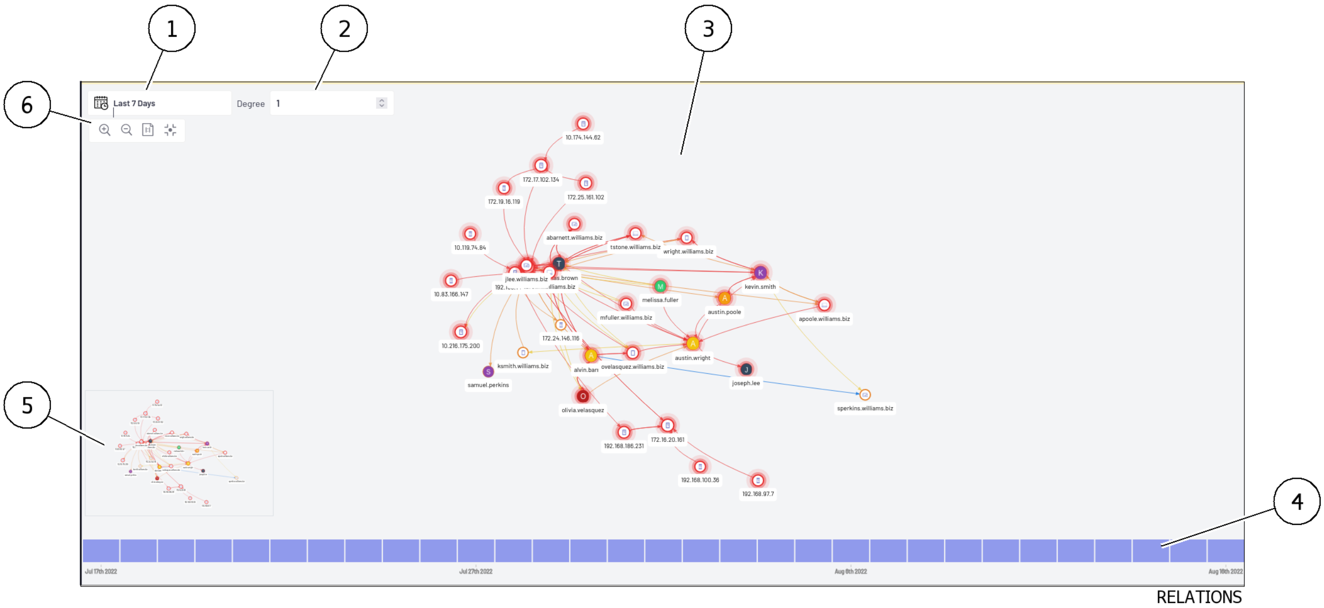
By clicking on the bar, the system displays the information defined in the `Alerts` screen for the selected risk type.
In the example below, the window displays the following information:



| ITEM | Name | Description |
|---|---|---|
| 1 | Percentage for this type of alert | Indicates the probability that this likely risk is real |
| 2 | Alert type | Alert type `Malware`, `IDS`, `shellcode` |

### 5.6.6 Web UI `Relations` screen

After pressing the `Relations` button on the navigation bar, the following screen is displayed.
This screen shows the relations between the elements in the network



| Item | Description |
|---|---|
| 1 | Time period selector |
| 2 | `Degree` field |
| 3 | Area for viewing active elements and their relationships |
| 4 | Timeline: enables selecting the display period |
| 5 | Total view area |
| 6 | Zoom tool area |

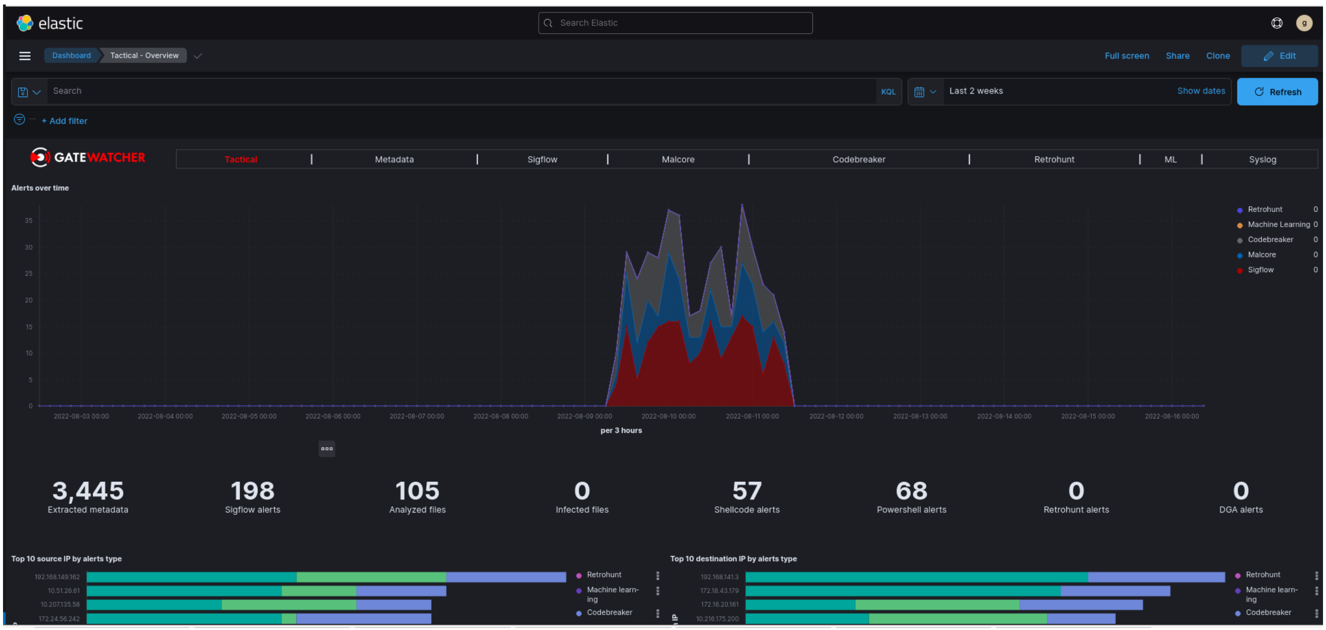
**Note:**

If the message `This feature is disabled; check your configuration or your license` is displayed:

- Check NDR configuration, see the *Configuring the NDR*
- Check license, see the *`Admin-GCenter-Configuration` screen of the legacy web UI*

### 5.6.7 Web UI `Hunting` screen

After pressing the `Hunting` button on the navigation bar, a new window is opened, displaying the Kibana UI:



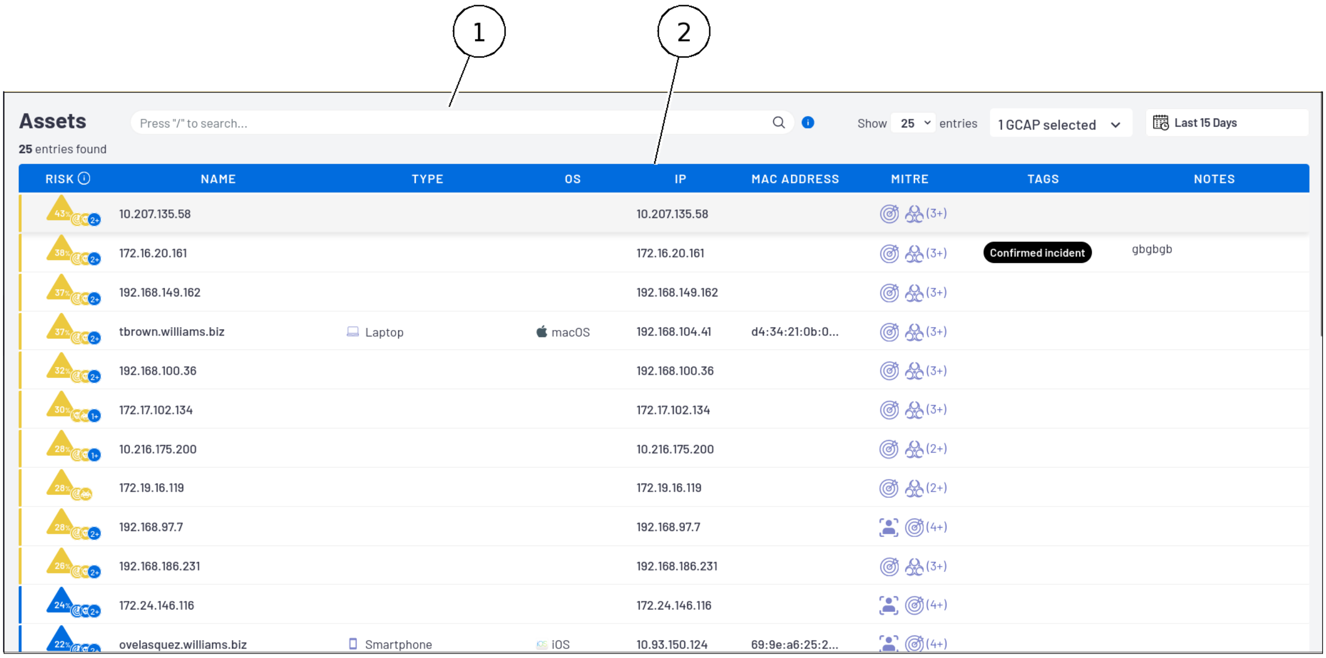
This interface is described in *Overview of the Kibana GUI*.

## 5.6.8 Web UI `Assets` screen

The active equipment management interface presents a list of the various equipment present on the network classified by risk score.

The equipment with the highest risk score is the one with the most high criticality alerts.

After pressing the `Assets` button on the navigation bar, the following screen is displayed.



Assets

**25** entries found

| RISK | NAME | TYPE | OS | IP | MAC ADDRESS | MITRE | TAGS | NOTES |
|---|---|---|---|---|---|---|---|---|
| 43% 2+ | 10.207.135.58 | | | 10.207.135.58 | | (3+) | | |
| 38% 2+ | 172.16.20.161 | | | 172.16.20.161 | | (3+) | Confirmed incident | gbgbgb |
| 37% 2+ | 192.168.149.162 | | | 192.168.149.162 | | (3+) | | |
| 37% 2+ | tbrown.williams.biz | Laptop | macOS | 192.168.104.41 | d4:34:21:0b:0... | (3+) | | |
| 32% 2+ | 192.168.100.36 | | | 192.168.100.36 | | (3+) | | |
| 30% 1+ | 172.17.102.134 | | | 172.17.102.134 | | (3+) | | |
| 28% 1+ | 10.216.175.200 | | | 10.216.175.200 | | (2+) | | |
| 28% | 172.19.16.119 | | | 172.19.16.119 | | (2+) | | |
| 28% 2+ | 192.168.97.7 | | | 192.168.97.7 | | (4+) | | |
| 26% 2+ | 192.168.186.231 | | | 192.168.186.231 | | (3+) | | |
| 24% 2+ | 172.24.146.116 | | | 172.24.146.116 | | (4+) | | |
| 22% | ovelasquez.williams.biz | Smartphone | iOS | 10.93.150.124 | 69:9e:a6:25:2... | (4+) | | |

ASSETS-01

| Item | Description |
|---|---|
| 1 | Dashboard selector |
| 2 | Active equipment list display area |

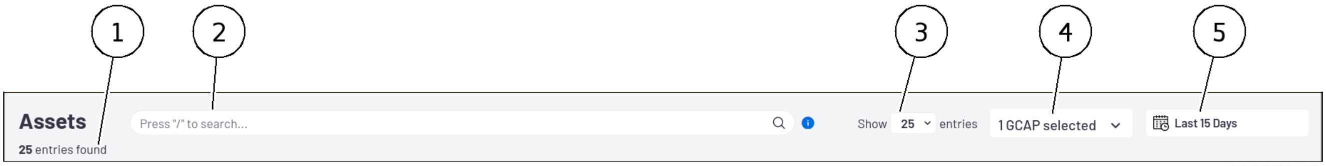
**Note:**

If the message ``This feature is disabled; check your configuration or your license`` is displayed:

- Check the NDR configuration, see the *Configuring the NDR*
- Check the licence, see the *`Admin-GCenter-Configuration` screen of the legacy web UI*

#### 5.6.8.1 ``Assets`` screen dashboard selector

The selector includes the following items:



Assets

25 entries found

Press "/" to search...

Show 25 entries

1 GCAP selected

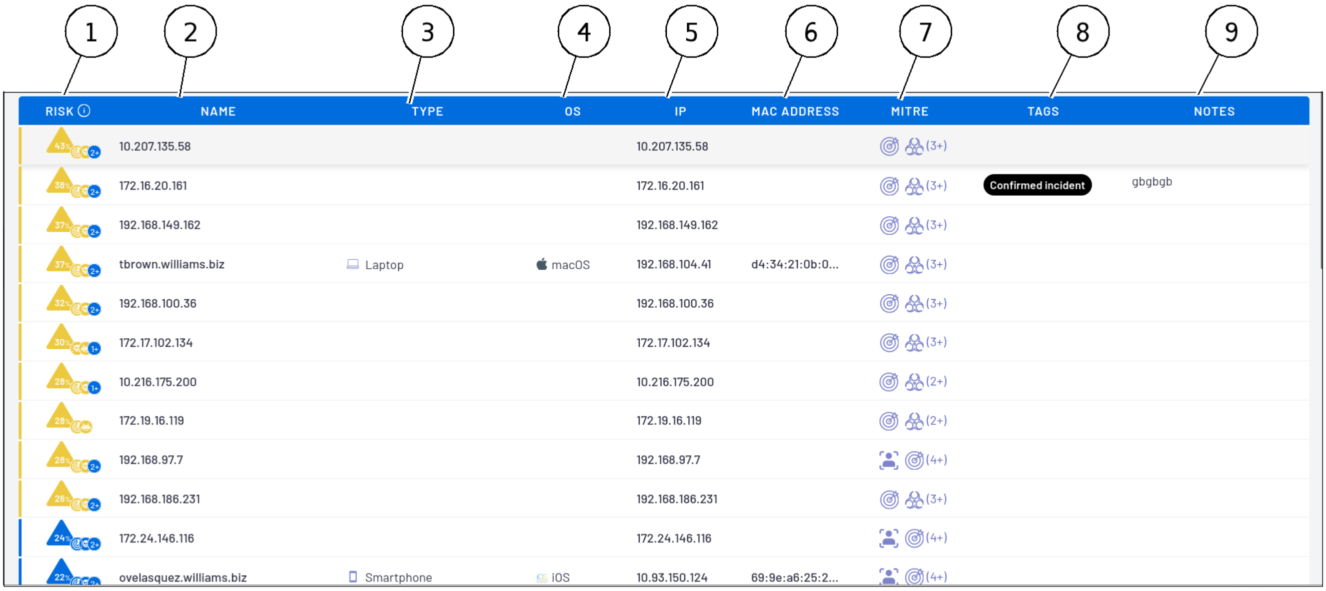
Last 15 Days

ASSETS-02

| Item | Name | Description |
|---|---|---|
| 1 | Number of results | Display of the number of records found |
| 2 | Search field | Enables entering a text to be searched in the page |
| 3 | ``show`` field | Selection of the number of lines per page |
| 4 | GCap selector | Selection of GCap |
| 5 | Time period selector | Selection of the display period |

#### 5.6.8.2 Active equipment list display area

The display consists of:



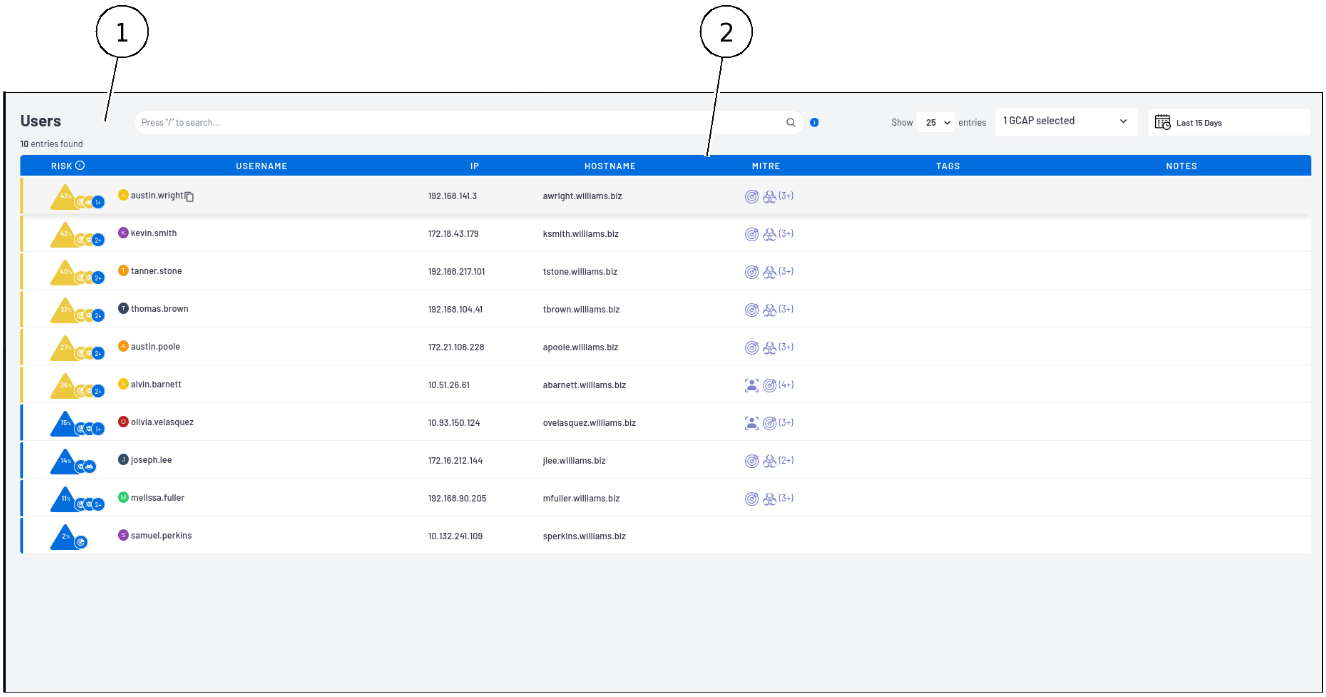
| RISK | NAME | TYPE | OS | IP | MAC ADDRESS | MITRE | TAGS | NOTES |
|---|---|---|---|---|---|---|---|---|
| 43% 2+ | 10.207.135.58 | | | 10.207.135.58 | | (3+) | | |
| 38% 2+ | 172.16.20.161 | | | 172.16.20.161 | | (3+) | Confirmed incident | gbgbgb |
| 37% 2+ | 192.168.149.162 | | | 192.168.149.162 | | (3+) | | |
| 37% 2+ | tbrown.williams.biz | Laptop | macOS | 192.168.104.41 | d4:34:21:0b:0... | (3+) | | |
| 32% 2+ | 192.168.100.36 | | | 192.168.100.36 | | (3+) | | |
| 30% 1+ | 172.17.102.134 | | | 172.17.102.134 | | (3+) | | |
| 28% 1+ | 10.216.175.200 | | | 10.216.175.200 | | (2+) | | |
| 28% | 172.19.16.119 | | | 172.19.16.119 | | (2+) | | |
| 28% 2+ | 192.168.97.7 | | | 192.168.97.7 | | (4+) | | |
| 26% 2+ | 192.168.186.231 | | | 192.168.186.231 | | (3+) | | |
| 24% 2+ | 172.24.146.116 | | | 172.24.146.116 | | (4+) | | |
| 22% | ovelasquez.williams.biz | Smartphone | iOS | 10.93.150.124 | 69:9e:a6:25:2... | (4+) | | |

ASSETS-03

| Item | Description |
|---|---|
| 1 | Type of risks. The risk level is indicated by the colour. The type of risk is indicated by the corresponding icons<br>Above 2, an indicator shows the number of risk types...<br>By clicking on this indicator, a window gives additional information such as the name of the user and the list of risk types |
| 2 | Name of the active equipment either the IP address or the hostname<br>By clicking on this field, a window provides additional information |
| 3 | Type of the active device (laptop, smartphone...)<br>By clicking on this field, a window provides additional information |
| 4 | Operating system either MAC OS, IOS, Windows, Android or ... ) |
| 5 | IP address<br>By clicking on this field, a window provides additional information |
| 6 | MAC address |
| 7 | `MITRE` field |
| 8 | `TAGS` field |
|  | By clicking on this field, a window provides the possibility to define past or future actions regarding this alarm |
| 9 | `NOTES` field<br>By clicking on this field, a window provides the possibility to define a comment on this alarm |

### 5.6.9 Web UI `Users` screen

The user management interface presents a list of the different users present on the network classified by risk score. The user with the highest risk score is the one with the highest criticality alerts.
After pressing the `Users` button on the navigation bar, the following screen is displayed.



Users

Press "/" to search...

10 entries found

Show 25 entries | 1 GCAP selected | Last 15 Days

| RISK | USERNAME | IP | HOSTNAME | MITRE | TAGS | NOTES |
|---|---|---|---|---|---|---|
| 43% 1+ | austin.wright | 192.168.141.3 | awright.williams.biz | (3+) | | |
| 42% 2+ | kevin.smith | 172.18.43.179 | ksmith.williams.biz | (3+) | | |
| 40% 2+ | tanner.stone | 192.168.217.101 | tstone.williams.biz | (3+) | | |
| 37% 2+ | thomas.brown | 192.168.104.41 | tbrown.williams.biz | (3+) | | |
| 27% 2+ | austin.poole | 172.21.106.228 | apoole.williams.biz | (3+) | | |
| 26% 2+ | alvin.barnett | 10.51.26.61 | abarnett.williams.biz | (4+) | | |
| 15% 1+ | olivia.velasquez | 10.93.150.124 | ovelasquez.williams.biz | (3+) | | |
| 14% | joseph.lee | 172.16.212.144 | jlee.williams.biz | (2+) | | |
| 11% 2+ | melissa.fuller | 192.168.90.205 | mfuller.williams.biz | (3+) | | |
| 2% | samuel.perkins | 10.132.241.109 | sperkins.williams.biz | | | |

USERS-01

| Item | Description |
|---|---|
| 1 | Dashboard selector |
| 2 | User list display area |

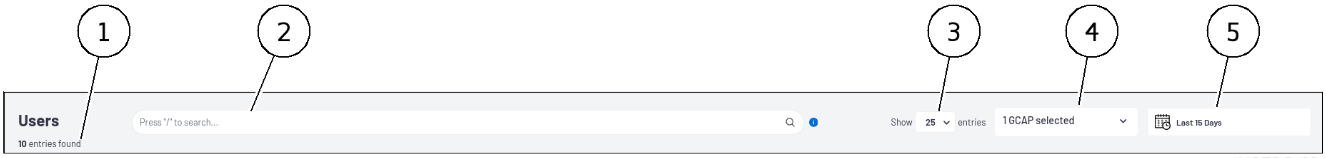
**Note:**

If the message `This feature is disabled; check your configuration or your license` is displayed:

- Check the NDR configuration, see *Configuring the NDR*
- Check the licence, see *`Admin-GCenter-Configuration` screen of the legacy web UI*

### 5.6.9.1 `Users` screen dashboard selector

The selector includes the following items:



Users

10 entries found

Press "/" to search...

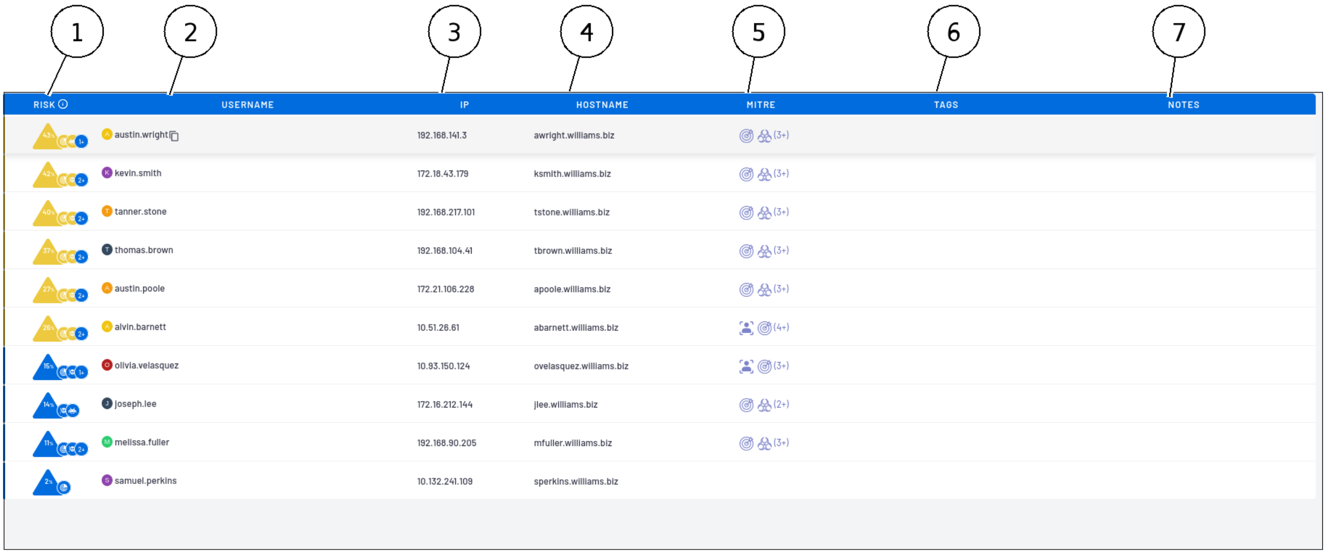
Show 25 entries | 1 GCAP selected | Last 15 Days

USERS-03

| Item | Name | Description |
|---|---|---|
| 1 | Number of results | Display of the number of records found |
| 2 | Search field | Enables entering a text to be searched in the page |
| 3 | `show` field | selection of the number of lines per page |
| 4 | GCap selector | Selection of GCap |
| 5 | Time period selector | Selection of the display period |

### 5.6.9.2 User list display area

The display consists of:



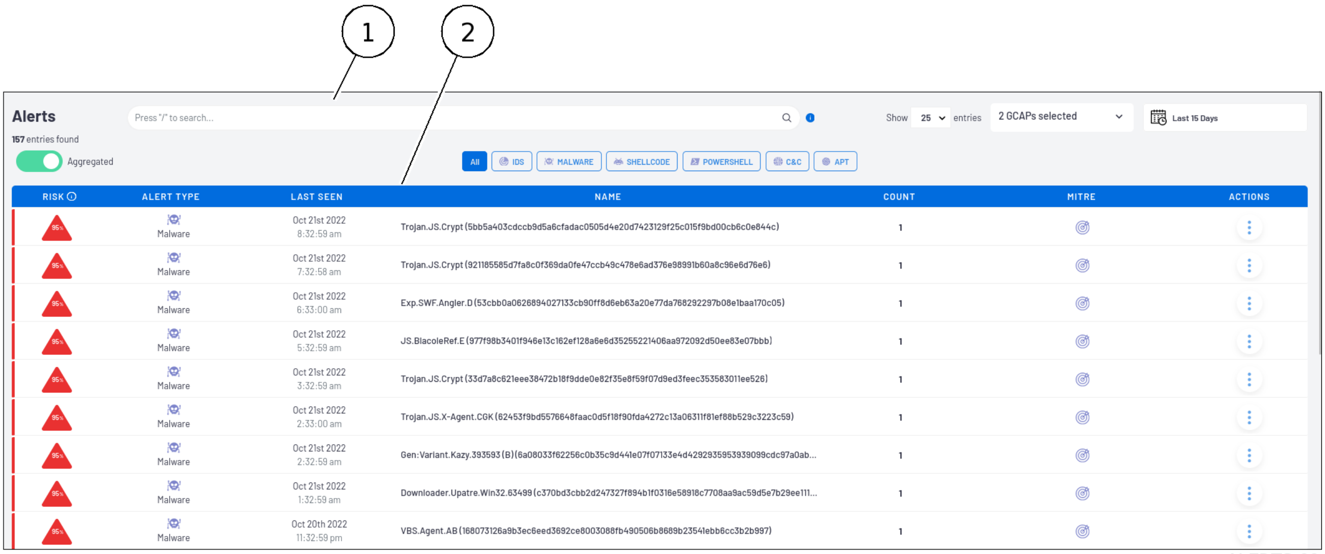
| RISK | USERNAME | IP | HOSTNAME | MITRE | TAGS | NOTES |
|---|---|---|---|---|---|---|
| 43% 1+ | austin.wright | 192.168.141.3 | awright.williams.biz | (3+) | | |
| 42% 2+ | kevin.smith | 172.18.43.179 | ksmith.williams.biz | (3+) | | |
| 40% 2+ | tanner.stone | 192.168.217.101 | tstone.williams.biz | (3+) | | |
| 37% 2+ | thomas.brown | 192.168.104.41 | tbrown.williams.biz | (3+) | | |
| 27% 2+ | austin.poole | 172.21.106.228 | apoole.williams.biz | (3+) | | |
| 26% 2+ | alvin.barnett | 10.51.26.61 | abarnett.williams.biz | (4+) | | |
| 15% 1+ | olivia.velasquez | 10.93.150.124 | ovelasquez.williams.biz | (3+) | | |
| 14% | joseph.lee | 172.16.212.144 | jlee.williams.biz | (2+) | | |
| 11% 2+ | melissa.fuller | 192.168.90.205 | mfuller.williams.biz | (3+) | | |
| 2% | samuel.perkins | 10.132.241.109 | sperkins.williams.biz | | | |

USERS-02

| Repère | Description |
|---|---|
| 1 | Type of risks. The risk level is indicated by the colour. The type of risk is indicated by the corresponding icons.<br>Above 2, an indicator shows the number of risk.<br>By clicking on this indicator, a window gives additional information such as the name of the user and the list of risk types. |
| 2 | Name of the user.<br>By clicking on this field, a window provides additional information about this user: |
| 3 | IP address of the infected device.<br>By clicking on this field, a window opens providing additional information about this IP address. |
| 4 | Unique name of the infected computer (hostname) |
| 5 | \`MITRE\` field |
| 6 | \`TAGS\` field |
| 7 | \`NOTES\` field |

### 5.6.10 Web UI `Alerts` screen

The alert management interface presents a list of the various alerts on the network classified by risk score and type.
After pressing the `Alerts` button on the navigation bar, the following screen appears.



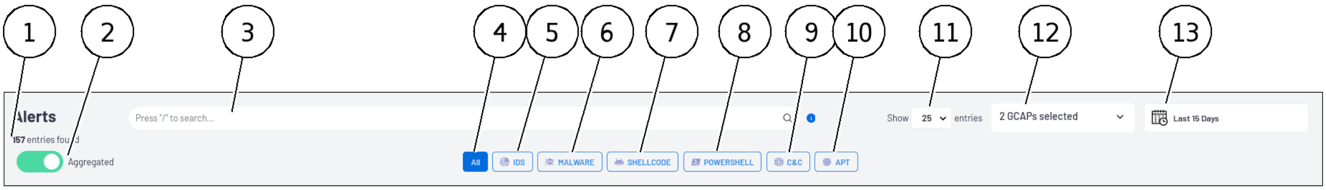
| RISK | ALERT TYPE | LAST SEEN | NAME | COUNT | MITRE | ACTIONS |
|---|---|---|---|---|---|---|
| 95% | Malware | Oct 21st 2022<br>8:32:59 am | Trojan.JS.Crypt (5bb5a403cdccb9d5a6cfadac0505d4e20d7423129f25c015f9bd00cb6c0e844c) | 1 | | |
| 95% | Malware | Oct 21st 2022<br>7:32:58 am | Trojan.JS.Crypt (921185585d7fa8c0f369da0fe47ccb49c478e6ad376e98991b60a8c96e6d76e6) | 1 | | |
| 95% | Malware | Oct 21st 2022<br>6:33:00 am | Exp.SWF.Angler.D (53cbb0a0626894027133cb90ff8d6eb63a20e77da768292297b08e1baa170c05) | 1 | | |
| 95% | Malware | Oct 21st 2022<br>5:32:59 am | JS.BlacoleRef.E (977f98b3401f946e13c162ef128a6e6d35255221406aa972092d50ee83e07bbb) | 1 | | |
| 95% | Malware | Oct 21st 2022<br>3:32:59 am | Trojan.JS.Crypt (33d7a8c621eee38472b18f9dde0e82f35e8f59f07d9ed3feec353583011ee526) | 1 | | |
| 95% | Malware | Oct 21st 2022<br>2:33:00 am | Trojan.JS.X-Agent.CGK (62453f9bd5576648faac0d5f18f90fda4272c13a06311f81ef88b529c3223c59) | 1 | | |
| 95% | Malware | Oct 21st 2022<br>2:32:59 am | Gen:Variant.Kazy.393593 (B)(6a08033f62256c0b35c9d441e07f07133e4d4292935953939099cdc97a0ab... | 1 | | |
| 95% | Malware | Oct 21st 2022<br>1:32:59 am | Downloader.Upatre.Win32.63499 (c370bd3cbb2d247327f894b1f0316e58918c7708aa9ac59d5e7b29ee111... | 1 | | |
| 95% | Malware | Oct 20th 2022<br>11:32:59 pm | VBS.Agent.AB (168073126a9b3ec6eed3692ce8003088fb490506b8689b23541ebb6cc3b2b997) | 1 | | |

ALERTS-00

| Item | Description |
|---|---|
| 1 | Dashboard selector |
| 2 | Display area for the list of filtered alerts |

#### 5.6.10.1 `Alerts` screen dashboard selector

The selector includes the following items:



ALERTS-01

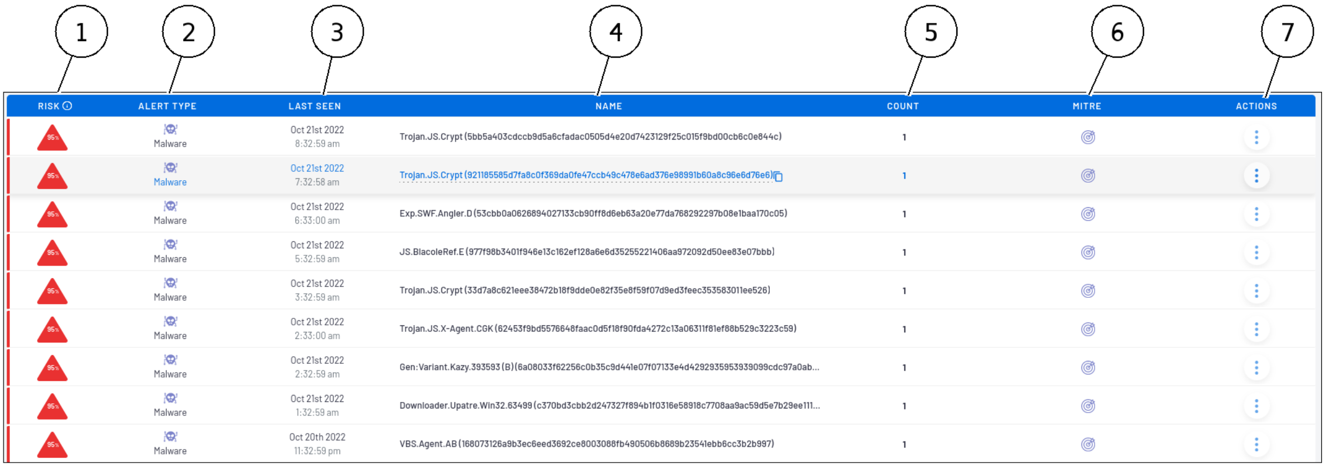
| Item | Name | Description |
|---|---|---|
| 1 | Number of results | Display of the number of records found:<br>depends on the selection choices for the display i.e. Aggregated selector, All selector, and so on. |
| 2 | \`Aggregated\` | Aggregates the records. In this mode the information fields are different. |
| 3 | Search field | Enables entering a text to be searched in the page |
| 4 | \`All\` | Filters records with all alert types: |
| 5 | \`IDS\` | Filters out records whose alert type is \`IDS\`:<br>Equivalent to entering 'type:ids' in the search field |
| 6 | \`MALWARE\` | Filters out records whose alert type is \`MALWARE\`:<br>Equivalent to entering 'type: malware' in the search field |
| 7 | \`SHELLCODE\` | Filters out records whose alert type is \`SHELLCODE\`:<br>Equivalent to entering 'type: shellcode' in the search field |
| 8 | \`POWERSHELL\` | Filters out records whose alert type is \`POWERSHELL\`:<br>Equivalent to entering 'type: powershell' in the search field |
| 9 | \`C&C\` | Filters out records whose alert type is \`C&C\`:<br>Equivalent to entering 'type:c&c' in the search field |
| 10 | \`APT\` | Filters out records whose alert type is \`APT\`:<br>Equivalent to entering 'type:apt' in the search field |
| 11 | \`show\` | Selection of the number of lines per page |
| 12 | GCap Selector | Selection of GCap |
| 13 | Time period selector | Selection of the display period |

**Note:**

Several types of alerts can be selected by pressing buttons 5 to 10.

#### 5.6.10.2 Display area for the list of alerts in aggregate mode

The display consists of:



| RISK | ALERT TYPE | LAST SEEN | NAME | COUNT | MITRE | ACTIONS |
|---|---|---|---|---|---|---|
| 95% | Malware | Oct 21st 2022<br>8:32:59 am | Trojan.JS.Crypt (5bb5a403cdccb9d5a6cfadac0505d4e20d7423129f25c015f9bd00cb6c0e844c) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>7:32:58 am | Trojan.JS.Crypt (921185585d7fa8c0f369da0fe47ccb49c478e6ad376e98991b60a8c96e6d76e6) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>6:33:00 am | Exp.SWF.Angler.D (53cbb0a0626894027133cb90ff8d6eb63a20e77da768292297b08e1baa170c05) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>5:32:59 am | JS.BlacoleRef.E (977f98b3401f946e13c162ef128a6e6d35255221406aa972092d50ee83e07bbb) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>3:32:59 am | Trojan.JS.Crypt (33d7a8c621eee38472b18f9dde0e82f35e8f59f07d9ed3feec353583011ee526) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>2:33:00 am | Trojan.JS.X-Agent.CGK (62453f9bd5576648faac0d5f18f90fda4272c13a06311f81ef88b529c3223c59) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>2:32:59 am | Gen:Variant.Kazy.393593 (B) (6a08033f62256c0b35c9d441e07f07133e4d4292935953939099cdc97a0ab... | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>1:32:59 am | Downloader.Upatre.Win32.63499 (c370bd3cbb2d247327f894b1f0316e58918c7708aa9ac59d5e7b29ee111... | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 20th 2022<br>11:32:59 pm | VBS.Agent.AB (168073126a9b3ec6eed3692ce8003088fb490506b8689b23541ebb6cc3b2b997) | 1 | ◎ | ⋮ |

ALERTS-02

| Item | Name | Description |
|---|---|---|
| 1 | \`RISK\` | Type of risks. The risk level is indicated by the color. The type of risk is indicated by the corresponding icons.<br>By clicking on an icon in column (1), a window displays information about the selected threat (NAME field).<br>There may be several records. |
| 2 | \`ALERT TYPE\` | Type of alerts detected |
| 3 | \`LAST SEEN\` | Date and time of last occurrence of this threat |
| 4 | \`NAME\` | Name of the detected threat |
| 5 | \`COUNT\` | Number of cumulative records with the same detected threat |
| 6 | \`MITRE\` | Viewing the MITRE category |
| 7 | \`ACTIONS\` | Menu of possible actions. Depends on the recording (Go hunting, Download Shelcode, Generate CFG, Display Data..) |

**Astuce:**

Alerts are detected by engines that:

- Work
- Are up to date
- Have been activated

The current motor status is displayed in the *Web UI `Health checks` screen*.

For the Malcore engine, check the white and black list that intervene on the alarm detection display.

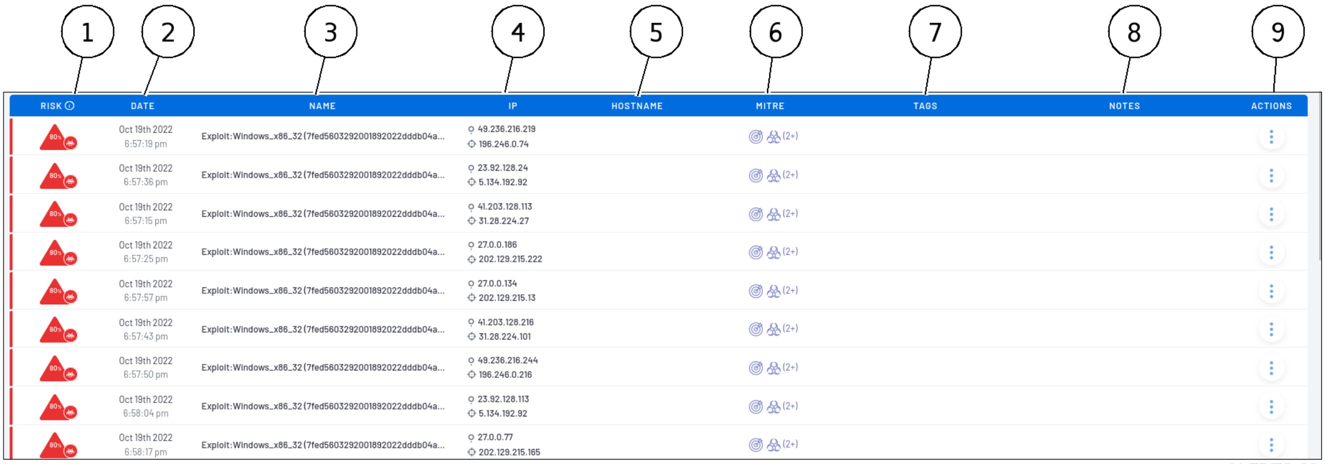
For the Codebreaker engine and the detection of shellcodes and powershells, this detection is not enabled by default and is defined in the profiles sent to GCap (see *Web UI `Config - Gcaps profiles` screen*).

For the Machine Learning engine for DGA detection (C&C), this engine must be enabled (see *`Admin-GCenter- ML Management` screen of the legacy web UI*).

For the CTI engine to generate alerts for Advanced Persistent Threat (APT) threats, this engine must be enabled (see *`Admin-GCenter- CTI Configuration` screen of the legacy web UI*).

### 5.6.10.3 Display area for the list of alerts in non-aggregated mode

The display consists of:



| RISK ⓘ | DATE | NAME | IP | HOSTNAME | MITRE | TAGS | NOTES | ACTIONS |
|---|---|---|---|---|---|---|---|---|
| 80% | Oct 19th 2022<br>6:57:19 pm | Exploit:Windows_x86_32 (7fed5603292001892022dddb04a... | 49.236.216.219<br>196.246.0.74 | | (2+) | | | ⋮ |
| 80% | Oct 19th 2022<br>6:57:36 pm | Exploit:Windows_x86_32 (7fed5603292001892022dddb04a... | 23.92.128.24<br>5.134.192.92 | | (2+) | | | ⋮ |
| 80% | Oct 19th 2022<br>6:57:15 pm | Exploit:Windows_x86_32 (7fed5603292001892022dddb04a... | 41.203.128.113<br>31.28.224.27 | | (2+) | | | ⋮ |
| 80% | Oct 19th 2022<br>6:57:25 pm | Exploit:Windows_x86_32 (7fed5603292001892022dddb04a... | 27.0.0.186<br>202.129.215.222 | | (2+) | | | ⋮ |
| 80% | Oct 19th 2022<br>6:57:57 pm | Exploit:Windows_x86_32 (7fed5603292001892022dddb04a... | 27.0.0.134<br>202.129.215.13 | | (2+) | | | ⋮ |
| 80% | Oct 19th 2022<br>6:57:43 pm | Exploit:Windows_x86_32 (7fed5603292001892022dddb04a... | 41.203.128.216<br>31.28.224.101 | | (2+) | | | ⋮ |
| 80% | Oct 19th 2022<br>6:57:50 pm | Exploit:Windows_x86_32 (7fed5603292001892022dddb04a... | 49.236.216.244<br>196.246.0.216 | | (2+) | | | ⋮ |
| 80% | Oct 19th 2022<br>6:58:04 pm | Exploit:Windows_x86_32 (7fed5603292001892022dddb04a... | 23.92.128.113<br>5.134.192.92 | | (2+) | | | ⋮ |
| 80% | Oct 19th 2022<br>6:58:17 pm | Exploit:Windows_x86_32 (7fed5603292001892022dddb04a... | 27.0.0.77<br>202.129.215.165 | | (2+) | | | ⋮ |

ALERTS-03

| Item | Name | |
|---|---|---|
| 1 | \`RISK\` | Type of risks. The risk level is indicated by the colour. The type of risk is indicated by the corresponding icons.<br>By clicking on an icon in column (1), a window displays information about the selected threat (\`NAME\` field).<br>There may be several records. |
| 2 | \`DATE\` | Date and time of the recording |
| 3 | \`NAME\` | Name of the detected threat |
| 4 | \`IP\` | The first IP address is the source address<br>The second IP address is the destination address |
| 5 | \`HOSTNAME\` | The first hostname is that of the source<br>The second hostname is that of the destination |
| 6 | \`MITRE\` | Viewing the MITRE category |
| 7 | \`TAGS\` | Tags field if indicated (Confirmed incident, Critical, Doing, Done) |
| 8 | \`NOTES\` | Notes field if indicated |
| 9 | \`ACTION\` | Menu of possible actions. Depends on the recording (Signature definition, Alert history, Alert summary, Flow details) |

#### 5.6.10.4 The sub menu \`ACTIONS\`

This menu displays:

- In the header:
  - The type of threat (malware for example),
  - The result of the analysis (infected for example) and
  - The name of the threat (Trojan/Win32.Ursnif, Generic.Nymaim.E.DA42CE72 for example)
- An command list

  The commands depend on the type of threat and are detailed in the following tables:

**Note:**

These commands are not fully activated in the Aggregated mode.

#### 5.6.10.4.1 Commands for an IDS

Table4: Commands for an IDS

| Order | Action |
|---|---|
| `` `Signature definition` `` | Displays the rule that detected the alert in the legacy web UI. |
| `` `Alert history` `` | Displays the history of this alert precisely.<br>To do this, the Kibana interface is opened on the `` `Overview` `` section of the `` `Sigflow` `` tab and the database is filtered on the `` `alert.signature' parameter` `` **or** on the `` `alert.signature_id` `` parameter. |
| `` `Alert summary` `` | Displays summary of this alert<br>To do this, the Kibana interface is opened on the `` `Overview` `` section of the `` `Sigflow` `` tab and the database is filtered on the `` `alert.signature_id` `` **and** parameter on the IP address of the source (`` `src_ip` ``) and the destination (`` `dest_ip` ``). |
| `` `Flow details` `` | Displays flow details.<br>To do this, the Kibana interface is opened on the `` `Messages` `` section of the `` `Sigflow` `` tab and the database is filtered on the `` `flow id` `` parameter. |

#### 5.6.10.4.2 Commands for a malware

Table5: Commands for malware

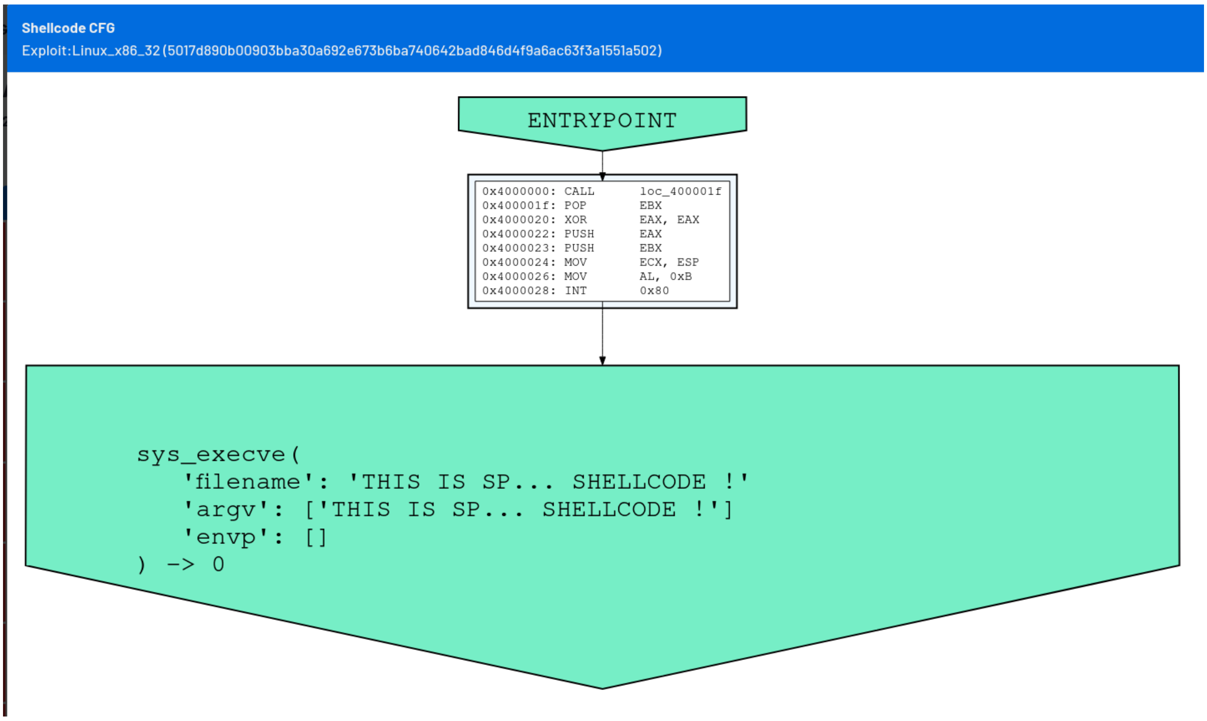
| Command | Action |
|---|---|
| `File transactions` | Displays file transactions.<br>To do this, the Kibana interface is opened on the `Overview` section of the `Malcore` tab and the database is filtered on the `fileinfo.sha256` parameter. |
| `Flow details` | Displays flow details.<br>To do this, the Kibana interface is opened on the `Messages` section of the `Malcore` tab and the database is filtered on the `flow id` **and** `fileinfo.sha256` parameter.<br>This window displays the detection details of this file. This information is detailed in *Events generated*. |
| `Download Malware` | Downloads the compressed file (name is UD.zip) to the user's PC. |
| `Generate Remote Analysis` | Send the file for a remote analysis (to a GBox for example).<br>If no remote server is connected then a message appears `Server error`<br>If the remote server is running then a report generation message appears. |
| `Download Analysis Report` | Download the remote server analysis report in pdf format.<br>See *Results and analysis report*, and *Analysis Report Analysis Procedure*. |

#### 5.6.10.4.3 Commands for a shellcode

Table6: Commands for a shellcode

| Command | Action |
|---|---|
| `Go hunting` | Displays threat details.<br>For this, the Kibana interface is opened on the `Messages` section of the `Codebreaker` tab and the database is filtered on the `SHA256` parameter. |
| `Download Shellcode` | Downloads the compressed file (name is UD.zip) to the user's PC. |
| `Generate CFG (advanced)` | Generate the control flow graph (CFG) to obtain a graphical and simplified version of the Shellcode instructions detected. : an example is given below. |
| `Display Data (Hexdump)` | Displays the file |

Below is an example of a CFG generation of a simple shellcode detected by the CODEBREAKER analysis engine:



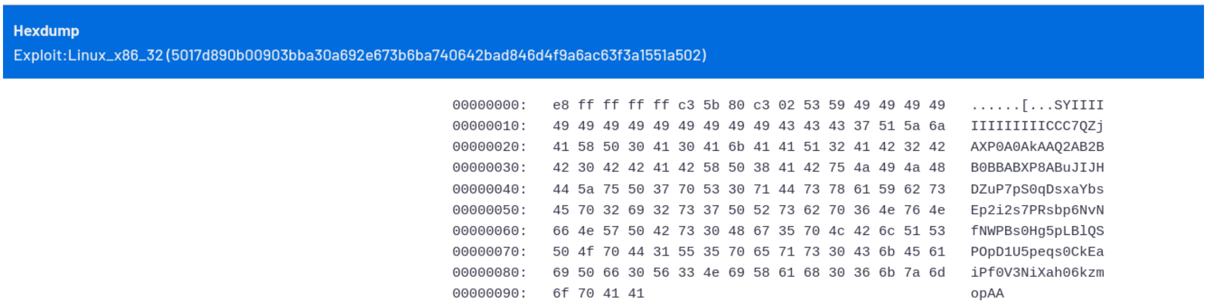
**Shellcode CFG**

Exploit:Linux_x86_32 (5017d890b00903bba30a692e673b6ba740642bad846d4f9a6ac63f3a1551a502)

```
0x4000000: CALL      loc_400001f
0x400001f: POP       EBX
0x4000020: XOR       EAX, EAX
0x4000022: PUSH      EAX
0x4000023: PUSH      EBX
0x4000024: MOV       ECX, ESP
0x4000026: MOV       AL, 0xB
0x4000028: INT       0x80
```

```
sys_execve(
    'filename': 'THIS IS SP... SHELLCODE !'
    'argv': ['THIS IS SP... SHELLCODE !']
    'envp': []
) -> 0
```

Below is an example of file content:



**Hexdump**

Exploit:Linux_x86_32 (5017d890b00903bba30a692e673b6ba740642bad846d4f9a6ac63f3a1551a502)

```
00000000:   e8 ff ff ff ff c3 5b 80 c3 02 53 59 49 49 49 49   ......[...SYIIII
00000010:   49 49 49 49 49 49 49 49 49 43 43 43 37 51 5a 6a   IIIIIIIIICCC7QZj
00000020:   41 58 50 30 41 30 41 6b 41 41 51 32 41 42 32 42   AXP0A0AkAAQ2AB2B
00000030:   42 30 42 42 41 42 58 50 38 41 42 75 4a 49 4a 48   B0BBABXP8ABuJIJH
00000040:   44 5a 75 50 37 70 53 30 71 44 73 78 61 59 62 73   DZuP7pS0qDsxaYbs
00000050:   45 70 32 69 32 73 37 50 52 73 62 70 36 4e 76 4e   Ep2i2s7PRsbp6NvN
00000060:   66 4e 57 50 42 73 30 48 67 35 70 4c 42 6c 51 53   fNWPBs0Hg5pLBlQS
00000070:   50 4f 70 44 31 55 35 70 65 71 73 30 43 6b 45 61   POpD1U5peqs0CkEa
00000080:   69 50 66 30 56 33 4e 69 58 61 68 30 36 6b 7a 6d   iPf0V3NiXah06kzm
00000090:   6f 70 41 41                                       opAA
```

### 5.6.10.4.4 Commands for a powershell

Table7: Commands for a powershell

| Command | Action |
|---|---|
| `Go hunting` | Displays threat details.<br>To do this, the Kibana interface is opened under the heading `Messages` of the `Codebreaker` tab and the database is filtered over the `SHA256` parameter. |
| `Download Powershell` | Downloads the compressed file (name is UD.zip) to the user's PC. |
| `Display Data (Hexdump)` | Displays the file |

#### 5.6.10.4.5 Orders for a DGA (C&C)

Table8: Commands for a DGA (C&C)

| Command | Action |
|---|---|
| `Disable DGA detect for ...` | Disable DGA detection for this specific domain. To do so, this domain is added to the whitelist.<br>After this whitelist, this domain will no longer be analyzed. |
| `Disable DGA detect for ...` | Disable DGA detection for this type of domain extension. To do so, this type of domain extension is added to the white list.<br>After this whitelist, threats on this type of domain extension will no longer be analyzed. |
| `Domain activity` | Displays DGA information on this domain.<br>This command opens a `Kibana` window in the `ML` tab with the `Overview` option enabled and the database is filtered for the current domain name with the parameter `domain_name`. |
| `Show DGA detect configuration` | This command opens the `Domain Name White List` window of the *`White List` section of the `DGA Detection Management` category*.<br>This shortcut allows you to view the domain names added by previous commands in the whitelist.<br>This screen also allows you to edit the whitelist. |
| `Client DGA activity` | Displays DGA information on the IP source.<br>To do this, the Kibana interface is opened in the tab `ML` with option `Overview` and the database is filtered on the parameter `src_ip`. |
| `Alert details` | Displays DGA information on the detected flow of the DGA alert<br>To do this, the Kibana interface is opened in the tab `ML` with option `Messages` and the database is filtered on the parameter `flow_id`. |

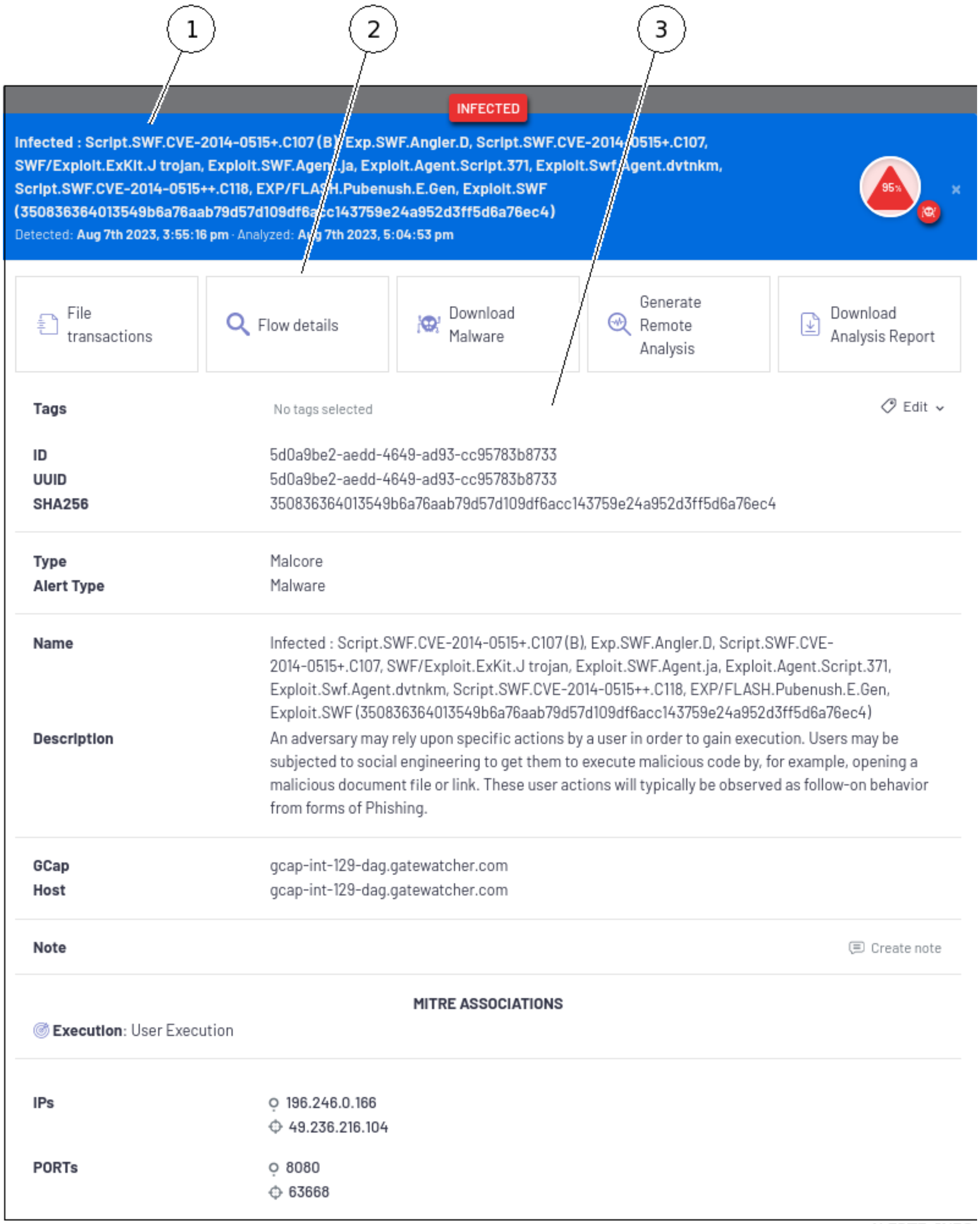
#### 5.6.10.4.6 Commands for an APT

Table9: Commands for an APT

| Command | Action |
|---|---|
| `` `Alert summary` `` | Displays the OBI summary.<br>To do this, the Kibana interface is opened in the `` `Retrohunt` `` tab with `` `Overview' option enabled and the database is filtered on the ```ioc_id` `` parameter. |
| `` `Show IOC` `` | Displays OBI details.<br>To do this, the Kibana interface is opened in the `` `Retrohunt` `` tab with `` `ICO` `` option enabled and the database is filtered on the `` `ioc_id` `` parameter. |
| `` `Show suspicious network flow` `` | Displays suspicious network flow details<br>To do this, the Kibana interface is opened on the `` `Retrohunt` `` section of the `` `All` `` tab and the database is filtered on the `` `uuid` `` parameter. |

#### 5.6.10.5 Alert information window

By clicking directly on an alert, the following window is displayed:



Infected : Script.SWF.CVE-2014-0515+.C107 (B), Exp.SWF.Angler.D, Script.SWF.CVE-2014-0515+.C107, SWF/Exploit.ExKit.J trojan, Exploit.SWF.Agent.ja, Exploit.Agent.Script.371, Exploit.Swf.Agent.dvtnkm, Script.SWF.CVE-2014-0515++.C118, EXP/FLASH.Pubenush.E.Gen, Exploit.SWF (350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4)

Detected: Aug 7th 2023, 3:55:16 pm · Analyzed: Aug 7th 2023, 5:04:53 pm

| | |
|---|---|
| **Tags** | No tags selected |
| **ID** | 5d0a9be2-aedd-4649-ad93-cc95783b8733 |
| **UUID** | 5d0a9be2-aedd-4649-ad93-cc95783b8733 |
| **SHA256** | 350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4 |
| **Type** | Malcore |
| **Alert Type** | Malware |
| **Name** | Infected : Script.SWF.CVE-2014-0515+.C107 (B), Exp.SWF.Angler.D, Script.SWF.CVE-2014-0515+.C107, SWF/Exploit.ExKit.J trojan, Exploit.SWF.Agent.ja, Exploit.Agent.Script.371, Exploit.Swf.Agent.dvtnkm, Script.SWF.CVE-2014-0515++.C118, EXP/FLASH.Pubenush.E.Gen, Exploit.SWF (350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4) |
| **Description** | An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of Phishing. |
| **GCap** | gcap-int-129-dag.gatewatcher.com |
| **Host** | gcap-int-129-dag.gatewatcher.com |
| **Note** | |

**MITRE ASSOCIATIONS**

**Execution**: User Execution

| | |
|---|---|
| **IPs** | 196.246.0.166<br>49.236.216.104 |
| **PORTs** | 8080<br>63668 |

ALERTE-INFO

The window consists of 3 parts:

- Upper part (1): the summary

  This section summarizes the alert, including:
  - The level of risk
  - The name of the detected threat
  - Detection date and time
- Intermediate part (2): possible actions

  This part shows the buttons of possible actions on this alert: these are the same actions as the commands detailed in the previous paragraphs.
- lower part (2): detailed information

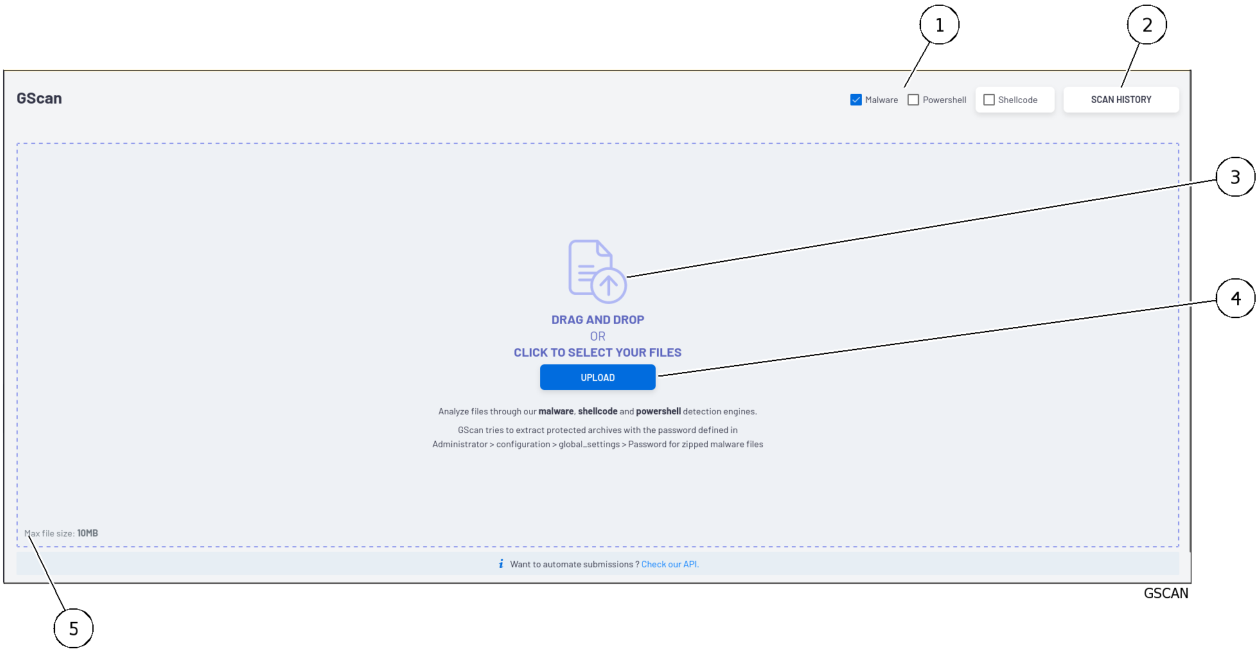
  This section displays detailed information on:
  - The file (ID, UUID, SHA256...)
  - The detected threat (type, type alert, name, description...)
  - Source GCap (GAP, Host)
  - etc

### 5.6.11 Web UI `GScan` screen

**Note:**

See presentation in *Detection by GScan*.

After pressing the `Gscan` button on the navigation bar, the following screen is displayed.



Analyze files through our **malware**, **shellcode** and **powershell** detection engines.

GScan tries to extract protected archives with the password defined in Administrator > configuration > global_settings > Password for zipped malware files

Max file size: 10MB

Want to automate submissions ? Check our API.

GSCAN

| Benchmark | Name | Description |
|---|---|---|
| 1 | `Malware`, `Powershell` or `Shellcode` | Selection of detection type |
| 2 | `SCAN HISTORY` | Viewing the history |
| 3 | `DRAG AND DROP` | Zone to deposit a file to be analyzed / zone of reports of the analyzed files |
| 4 | `UPLOAD` | Button to open a window to load a file(s) to be analyzed |
| 5 | `Max file size` | Information that the file size is limited to 10MO |

For implementation, see the *Detection procedure by Gscan*.

The analysis made by GScan depends on several configurable limits (such as the maximum size of files extracted by a GCap): the procedure to modify these values is given in *Setting up GBox and the Malcore and Retroact engines and activate the GBox*.

### 5.6.12 Web UI `Config - Metadata rate limiter` screen

In addition to alerts, GCaps generate metadata events on analyzed network flows.

This information can be useful in surveys, but in a certain context, it can quickly exceed the indexing capabilities of GCenter.

In order to reduce the amount of metadata while maintaining most information exchanges, it is possible to enable the limiters defined below.

**Astuce:**

Use the hunting tool (hunting > Metadata) to understand what kind of metadata should be optimized first.

This screen allows you to configure metadata rate limiters.

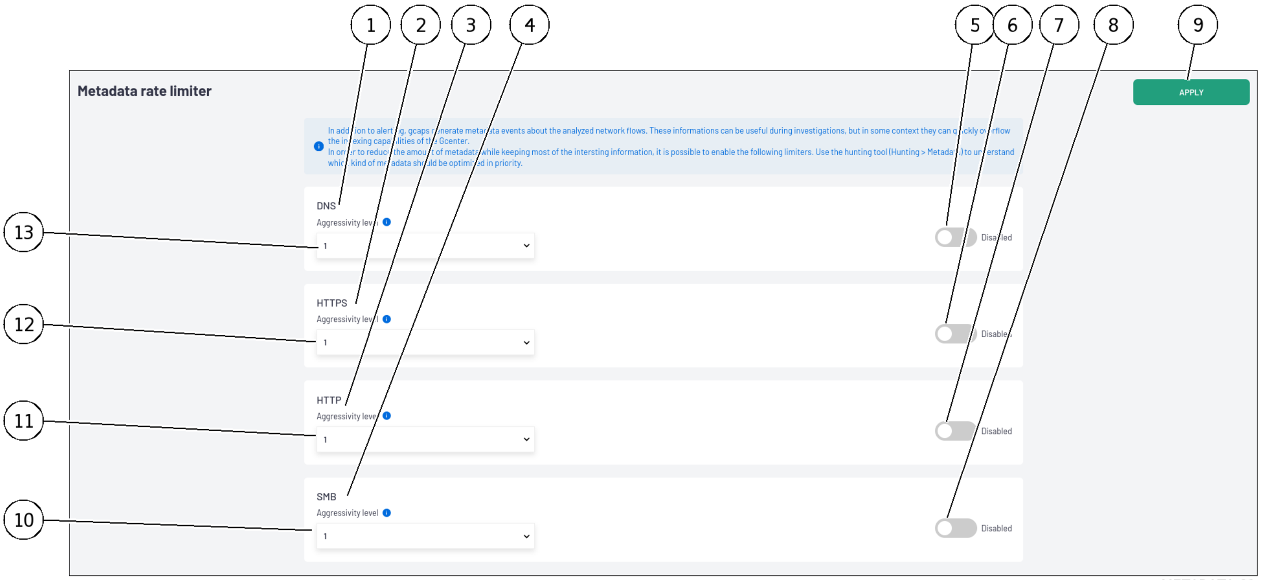
This screen is only accessible to members of the *administrator* group.

**Note:**

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

After pressing the `Metadata rate limiter` command in the `Config` menu, the following screen is displayed. This screen allows you to:

- Enable metadata limiters
- Define on which protocols they are activated
- Define the metadata filtering rule



Metadata rate limiter

In addition to alerting, gcaps generate metadata events about the analyzed network flows. These informations can be useful during investigations, but in some context they can quickly overflow the indexing capabilities of the Gcenter.
In order to reduce the amount of metadata while keeping most of the intersting information, it is possible to enable the following limiters. Use the hunting tool (Hunting > Metadata) to understand which kind of metadata should be optimized in priority.

DNS
Aggressivity level: 1
Disabled

HTTPS
Aggressivity level: 1
Disabled

HTTP
Aggressivity level: 1
Disabled

SMB
Aggressivity level: 1
Disabled

METADATA-01

The screen contains the following parts:

| Item | Name | Function |
|---|---|---|
| 1 | `` `DNS` `` | Configure DNS metadata. This includes: |
| 13 | • `` `Aggressivity level` `` | Filtration level. Includes the following choices:<br>• Level 1: Removes metadata from DNS queries, but retains responses<br>• Level 2: Remove metadata related to DNS queries.<br>If a response is type A, AAAA or PTR with a response code NOERROR, keeps only one response per domain name and source IP, with a 1 minute mobile window<br>• Level 3: Remove metadata related to DNS queries.<br>For all responses with a NOERROR response code, keep only one response per domain name and source IP, with a 1-hour mobile window |
| 5 | • `` `Enabled -Disabled` `` | Enable Selector - Disable `` `DNS` `` |
| 2 | `` `HTTPS` `` | Configures HTTPS metadata. This includes: |
| 13 | • `` `Aggressivity level` `` | Filtration level. Includes the following choices:<br>• Level 1: For connection-related events, only keeps a record by source IP, destination IP and TLS subject, with a 1-minute mobile window.<br>For other events, only keeps a record by source IP and destination IP with a 1-minute mobile window.<br>• Level 2: For connection-related events, only keeps a record by source IP, destination IP and TLS subject, with a 1-hour mobile window.<br>For other events, only keeps a record by source IP and destination IP with a 1 hour mobile window. |
| 6 | • `` `Enabled -Disabled` `` | Enable Selector - Disable `` `HTTPS` `` |
| 3 | `` `HTTP` `` | Configures HTTP metadata. This includes: |
| 13 | • `` `Aggressivity level` `` | Filtration level. Includes the following choices:<br>• Level 1: for events with status code 200, only keeps a single request per source IP, method, destination port, destination IP and URL, with a 1-minute mobile window.<br>• Level 2: For events with status code 200, keeps only one request per source IP, method, destination hostname, with a 1 hour mobile window.<br>• Level 3: keeps only events with status code different from 200. |
| 7 | • `` `Enabled -Disabled` `` | Enable Selector - Disable `` `HTTP` `` |
| 4 | `` `SMB` `` | Configures SMB metadata. This includes: |
| 13 | • `` `Aggressivity level` `` | Filtration level. Includes the following choices:<br>• Level 1: for each SMB session and for different SMB commands from READ and WRITE, only keeps 100 records per command type on a 1-minute mobile window<br>• Level 2: for each SMB session and for different SMB commands from READ and WRITE, keeps only 10 records per command type on a 1-hour mobile window |

suite sur la page suivante

Table 10 – suite de la page précédente

| Item | Name | Function |
|---|---|---|
| 8 | - \`Enabled -Disabled\` | Enable Selector - Disable \`SMB\` |
| 9 | button \`APPLY\` | Saves configuration. The following message is displayed after recording \`Metadata rate limiting successfully applied!\` |

For implementation, see the *Configuring Metadata Rate Limiters*.

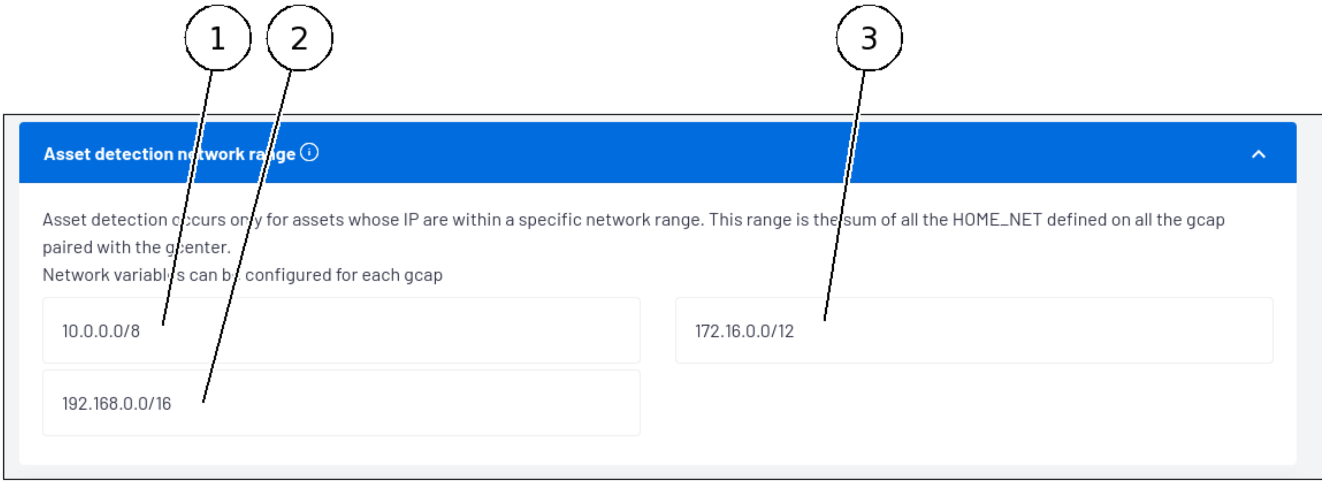
## 5.6.13 Web UI \`Config - Assets/Users Association rules\` screen

After pressing the \`Assets/Users Association rules\` button in the \`Config\` menu, the displayed screen consists of seven parts:

| Section | Description | See |
|---|---|---|
| Asset detection network range | Entering private network address ranges for detection d'équipements | *\`Asset detection network range\` section of the \`Assets/Users Association rules\` sub menu* |
| Static IP -Asset mapping | Mapping and IP address assignment of active equipment | *\`Static IP- Asset mapping\` section of the sub menu \`Assets/Users Association rules\`* |
| Ignored IP for users association | Definition of IP addresses to be ignored | *\`Ignored IP for users association\` section of the sub menu \`Assets/Users Association rules\`* |
| Ignored MAC for assets association | List of MAC addresses not to be associated with active devices | *\`Ignored MAC for assets association\` section of the sub menu \`Assets/Users Association rules\`* |
| Forbidden users | List of prohibited users | *\`Forbidden users\` section of the sub menu \`Assets/Users Association rules\`* |
| Forbidden assets | List of active network equipment that are prohibited | *\`Forbidden assets\` section of the sub menu \`Assets/Users Association rules\`* |

### 5.6.13.1 \`Asset detection network range\` section of the \`Assets/Users Association rules\` sub menu

The \`Asset detection network range\` window enables viewing and modifying the private network address ranges for asset detection.



Asset detection occurs only for assets whose IP are within a specific network range. This range is the sum of all the HOME_NET defined on all the gcap paired with the gcenter.
Network variables can be configured for each gcap

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

ASSETS_RULES_01

Active device detection only occurs for devices with an IP address within a specific network range.
This range is the amount of HOME_NET defined on all GCap paired with the GCenter.
Network variables can be configured for each GCap.
For GCaps where network variables have not been specified, HOME_NET is associated by default with the private networks defined by RFC1918.
This window displays the input fields in the address ranges reserved for private networks in IPv4:

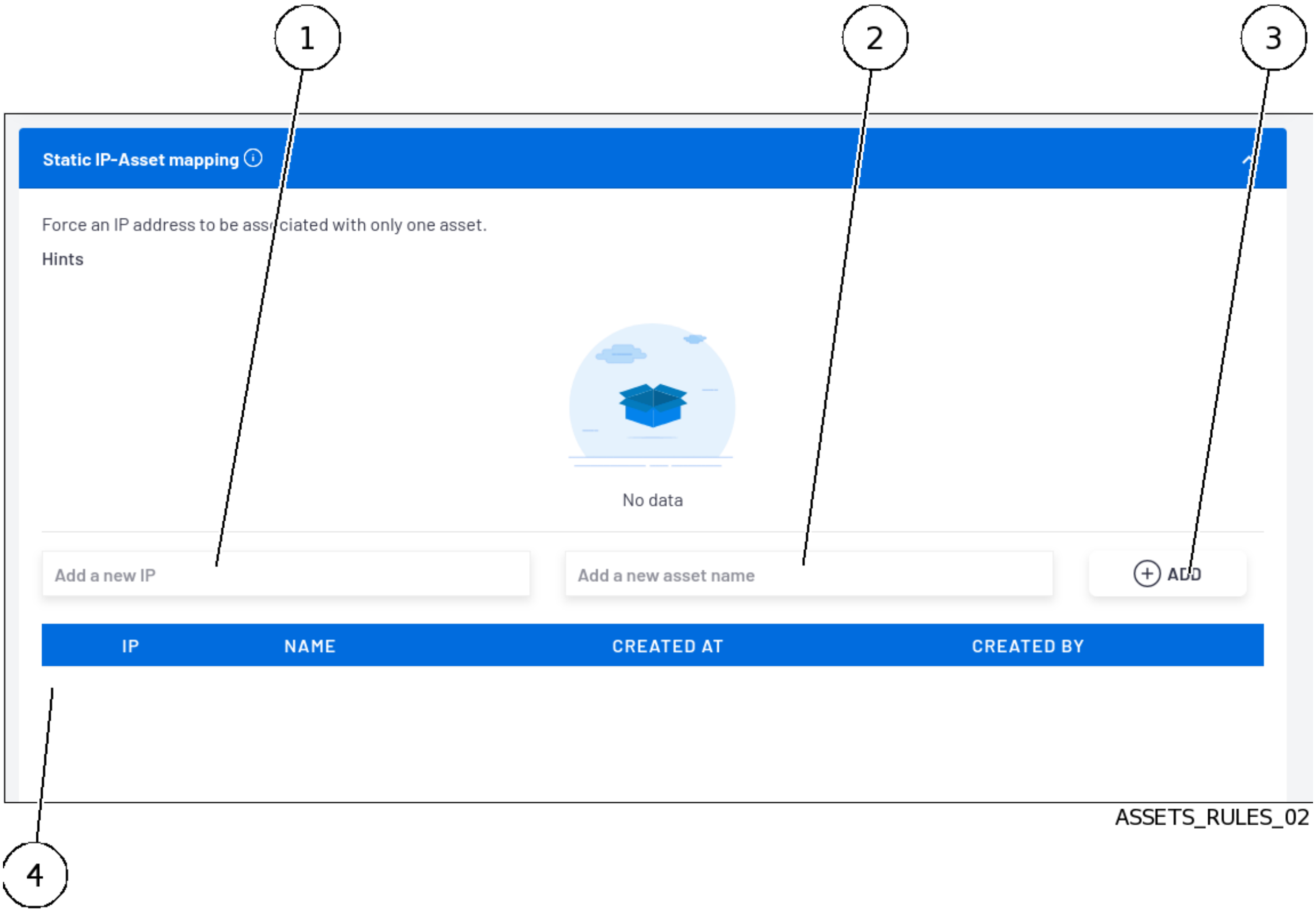
| Item | Private address view field | Detailed IP Range |
|---|---|---|
| 1 | prefix (10.0.0.0/8) | 10.0.0.0 – 10.255.255.255 |
| 2 | prefix (172.16.0.0/12) | 172.16.0.0 – 172.31.255.255 |
| 3 | prefix (192.168.0.0/16) | 192.168.0.0 – 192.168.255.255 |

The link `Network variables can be configured for each gcap` allows you to modify internal networks via the GCAP profile customization function.
This link takes you to the `Gcaps profiles` window (see *Web UI `Config - Gcaps profiles` screen*).

---

#### 5.6.13.2 `Static IP- Asset mapping` section of the sub menu `Assets/Users Association rules`

The `Static IP Asset mapping` window lists each association of a static IP with an active device on the network.

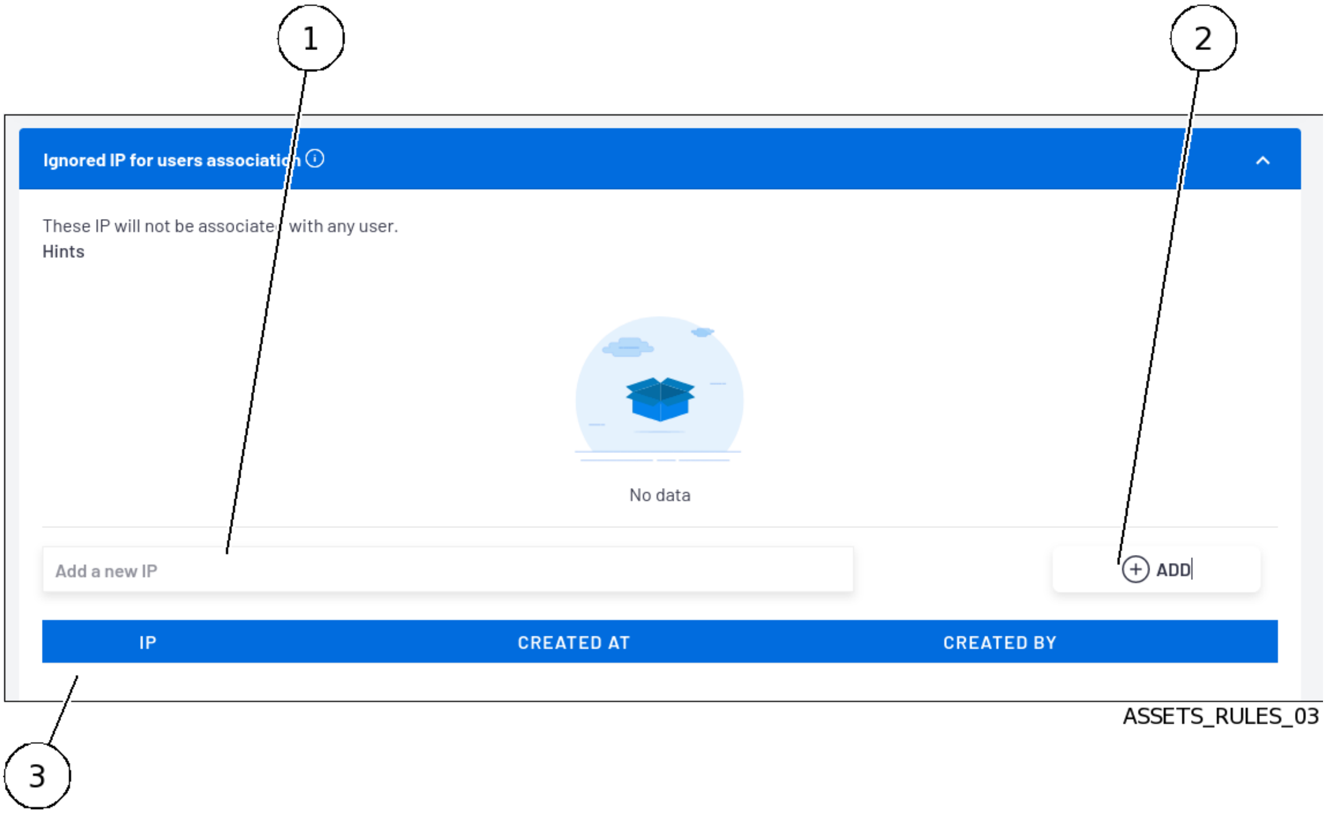

1
2
3
Static IP-Asset mapping ⓘ
Force an IP address to be associated with only one asset.
Hints
No data
Add a new IP
Add a new asset name
⊕ ADD
IP
NAME
CREATED AT
CREATED BY
4

ASSETS_RULES_02

| Item | Function |
|---|---|
| 1 | Input field for the IP address to be associated with a new device |
| 2 | Input field for a new device name |
| 3 | Add button |
| 4 | List of existing equipment. This includes the following types of information:<br>• IP address<br>• The name<br>• The creation date<br>• The creator's name |

#### 5.6.13.3 `Ignored IP for users association` section of the sub menu `Assets/Users Association rules`

The `Ignored IP for users association` window displays a list of IP addresses that cannot be associated with a user.



Ignored IP for users association

These IP will not be associated with any user.
Hints

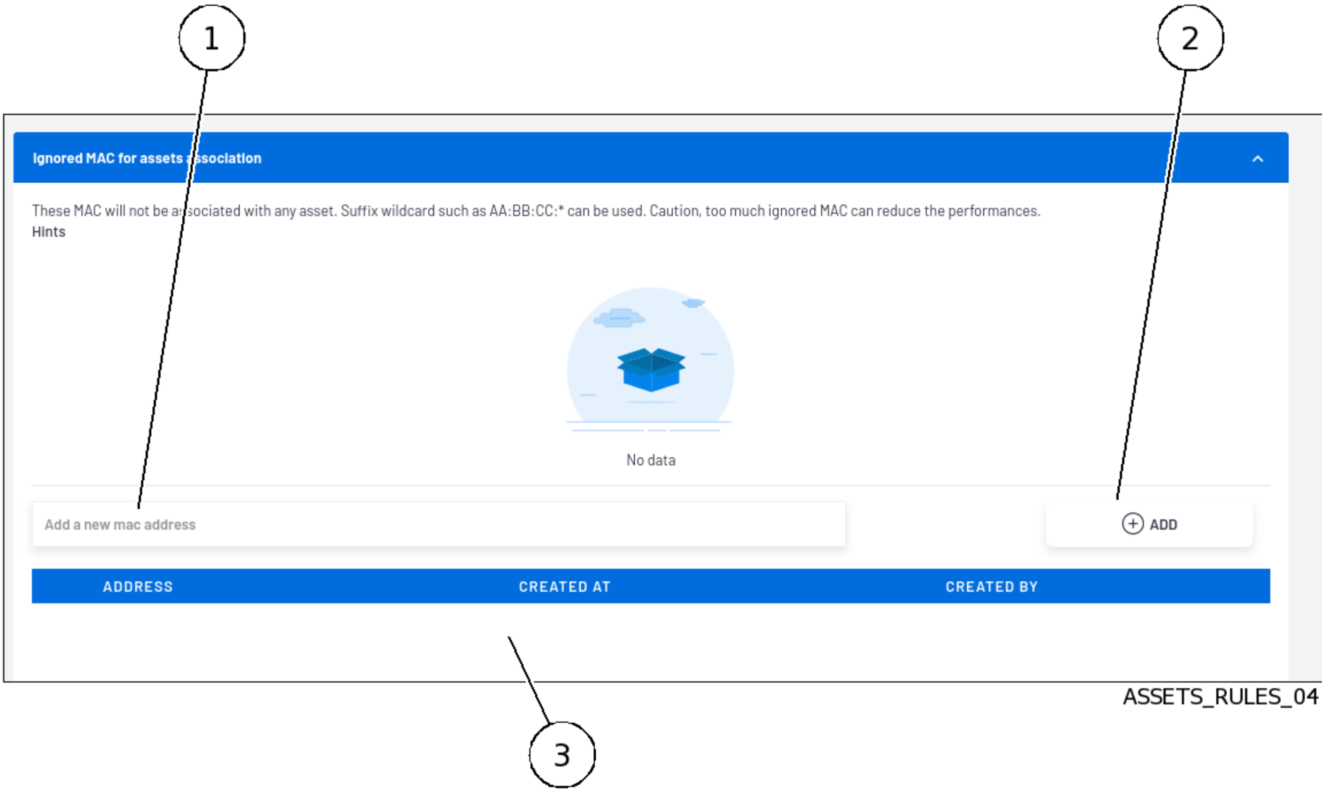
No data

ASSETS_RULES_03

| Item | Function |
|---|---|
| 1 | Input field for the IP address to be ignored |
| 2 | Button for adding a new IP address |
| 3 | List of existing equipment. This includes the following types of information:<br>• IP address<br>• The creation date<br>• The creator's name |

#### 5.6.13.4 `Ignored MAC for assets association` section of the sub menu `Assets/Users Association rules`

The `Ignored MAC for assets association` window displays a list of MAC addresses not to be associated with active devices.



Ignored MAC for assets association

These MAC will not be associated with any asset. Suffix wildcard such as AA:BB:CC:* can be used. Caution, too much ignored MAC can reduce the performances.
Hints

No data

Add a new mac address

ASSETS_RULES_04

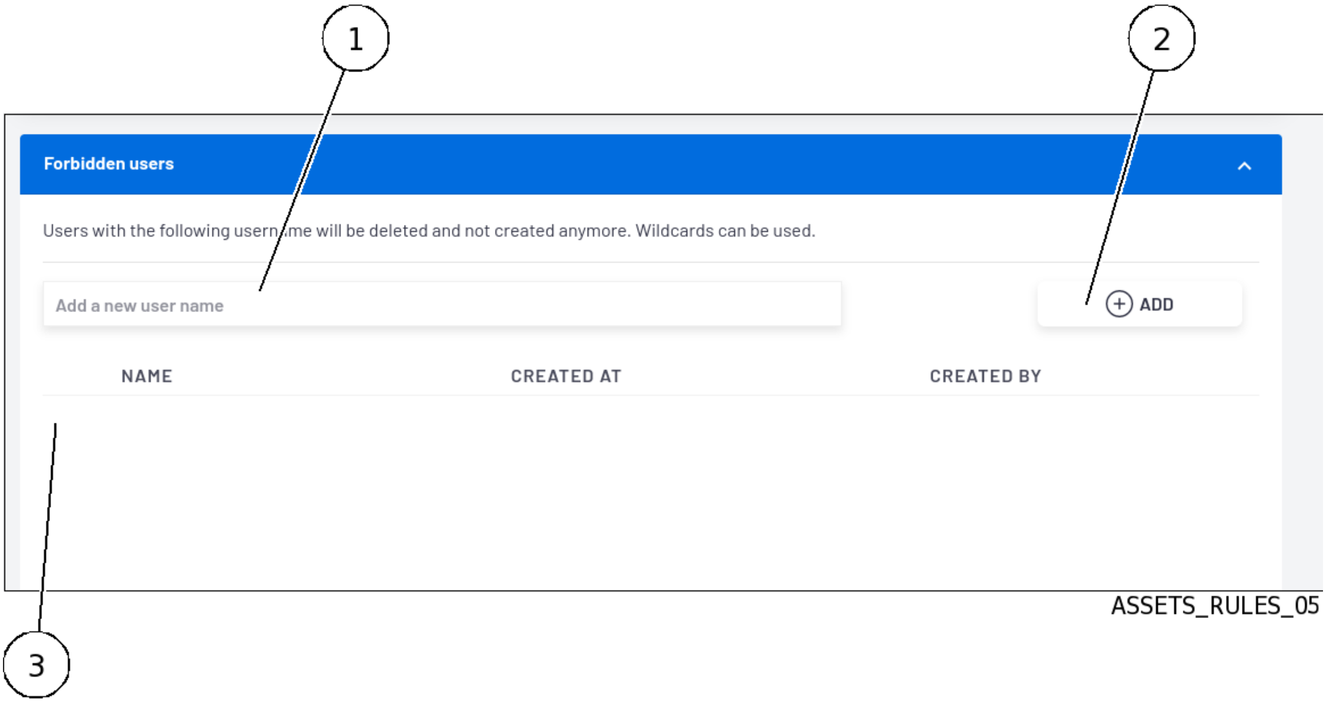
| Item | Function |
|---|---|
| 1 | Input field for the MAC address to be ignored |
| 2 | Button for adding a new MAC address |
| 3 | List of existing equipment. This includes the following types of information:<br>• MAC address<br>• The creation date<br>• The creator's name |

**Note:**

Ignore MAC addresses will not be associated with any active equipment.
Suffix wildcard characters such as AA:BB:CC:* can be used.
Caution: Setting too many ignore MAC addresses may reduce performance.

#### 5.6.13.5 `Forbidden users` section of the sub menu `Assets/Users Association rules`

The "Forbidden users" window displays a list of users who are forbidden.
Users with the user name defined here will be deleted. They will no longer be displayed in the dashboards.
Wildcard characters can be used.



Forbidden users

Users with the following username will be deleted and not created anymore. Wildcards can be used.

Add a new user name

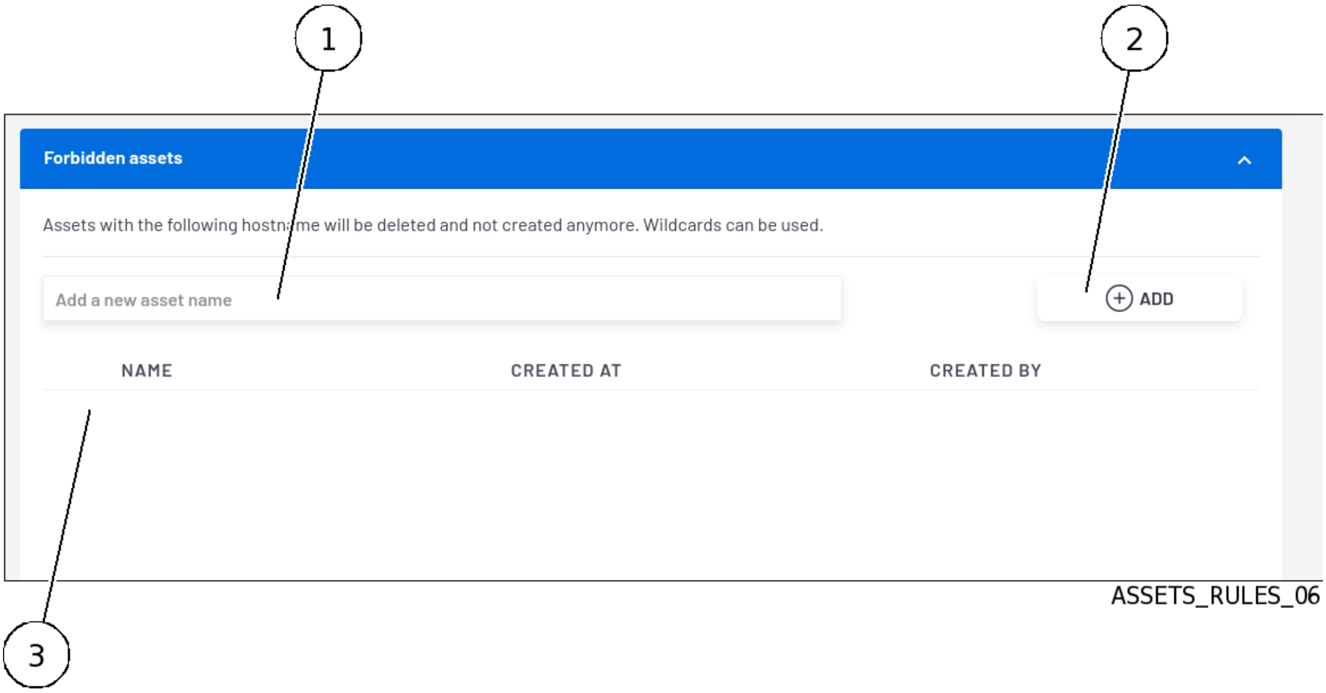
| NAME | CREATED AT | CREATED BY |
|---|---|---|

ASSETS_RULES_05

| Item | Function |
|---|---|
| 1 | Input field for the user name to be prohibited |
| 2 | Button for adding a new user name |
| 3 | List of existing names. This includes the following types of information:<br>• The name<br>• The creation date<br>• The creator's name |

#### 5.6.13.6 `Forbidden assets` section of the sub menu `Assets/Users Association rules`

The `Forbidden assets` window displays a list of active network assets that are to be forbidden.
Active devices with the name declared in this list will be deleted. They will no longer be displayed in the dashboards.
Wildcard characters can be used.



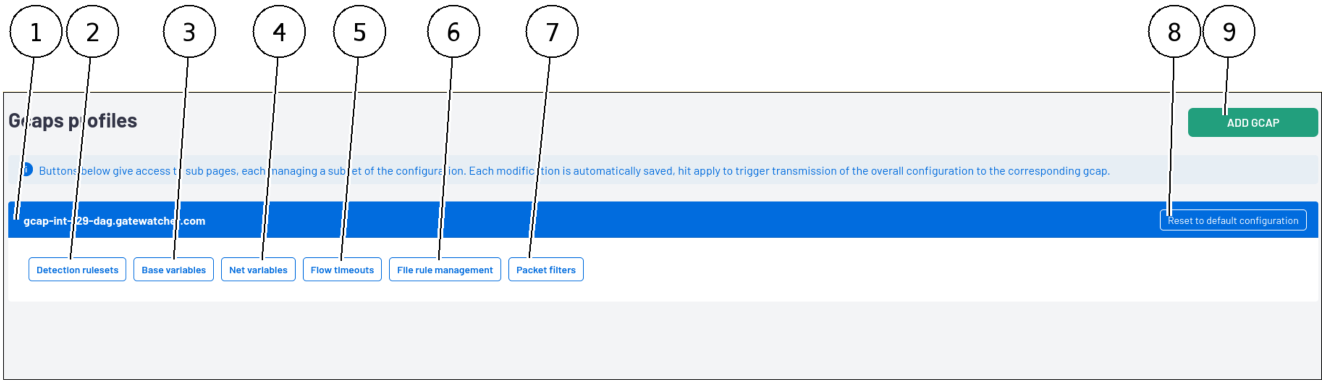
Assets with the following hostname will be deleted and not created anymore. Wildcards can be used.

ASSETS_RULES_06

| Item | Function |
|---|---|
| 1 | Input field for the name of the equipment (hostname) to be prohibited |
| 2 | Button for adding a new device name (hostname) |
| 3 | List of existing items. This includes the following types of information:<br>• The name of the device (hostname)<br>• The creation date<br>• The creator's name |

### 5.6.14 Web UI `Config - Gcaps profiles` screen

After pressing the `Gcaps profiles` command from the `Config` menu, the following screen is displayed. This screen enables configuring the GCap profiles.



Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

GCAP_00

| Item | Function | See |
|---|---|---|
| 1 | Name of the GCap associated with the GCenter | |
| 2 | `Detection Rulesets` button<br>manages the application of rulesets to paired GCaps | *`Detection Rulesets` section of the `Config Gcaps profiles` menu* |
| 3 | `Base variables` button<br>manages the configuration of the advanced GCap parameters | *`Base variables` section of the `Config Gcaps profiles` menu* |
| 4 | `Net variables` button<br>manages the network variables used in Sigflow rules | *`Net variables` section of the `Config Gcaps profiles` menu* |
| 5 | `Flow timeouts` button<br>configures the time Sigflow keeps a flow in memory depending on its status | *`Flow timeouts` section of the `Config Gcaps profiles` menu* |
| 6 | `File rule management` button<br>configures the file types that the GCap will extract for a given protocol | *`File rule management` section of the `Config Gcaps profiles` menu* |
| 7 | `Packet filters` button<br>adjusts the GCap capture parameters using Sigflow's advanced features | *`Packet filters` section of the `Config Gcaps profiles` menu* |
| 8 | `Reset to default configuration` button<br>resets the configuration and loads the profile selected in the `GCaps pairing and status` screen | |
| 9 | `ADD GCAP` button<br>displays the screen for adding a GCap | *`Admin-GCaps pairing and status` screen of the legacy Web UI* |

**Note:**

The buttons listed above give access to the sections listed below, each of which manages a subset of the configuration.
Each change is automatically saved.
Use of an `APPLY` button triggers sending the global configuration to the selected GCap.

### 5.6.14.1 `Detection Rulesets` section of the `Config Gcaps profiles` menu

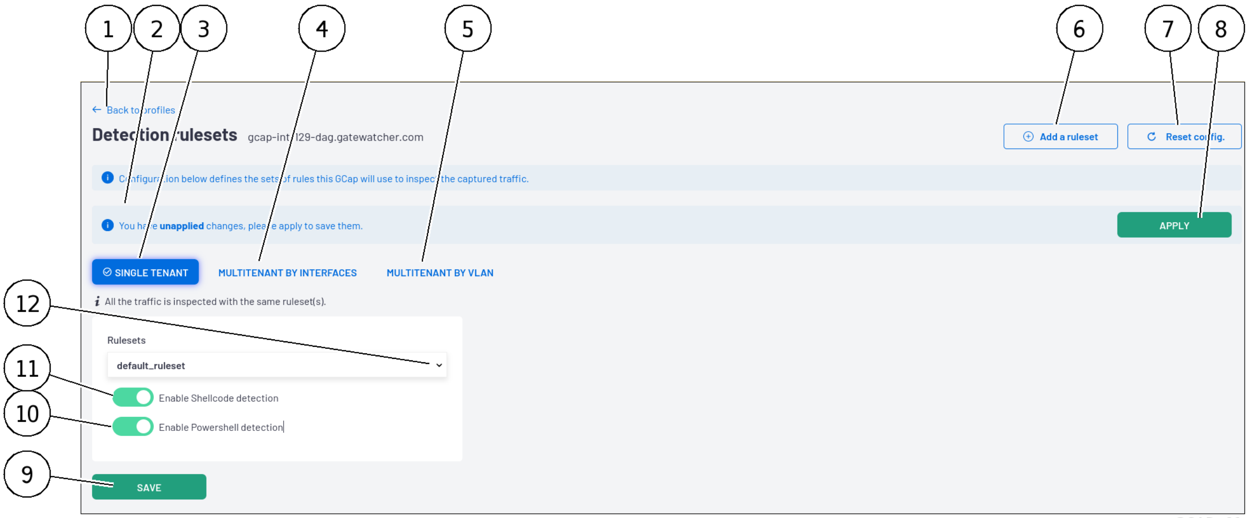
The `Detection Rulesets` screen enables:

- Configuring the detection modes for each of the three options below:

- `single tenant`
- `multi-tenant by interface`
- `multi-tenant by vlan`

- Apply the Sigflow rulesets previously created to the GCap paired on the GCenter
- Enable the Codebreaker engine (Shellcodes, Powershell detection)

For more information, refer to *Detection Rulesets*.



Detection rulesets gcap-int-129-dag.gatewatcher.com

Configuration below defines the sets of rules this GCap will use to inspect the captured traffic.

You have **unapplied** changes, please apply to save them.

All the traffic is inspected with the same ruleset(s).

Rulesets: default_ruleset

Enable Shellcode detection

Enable Powershell detection

GCAP_01

| Item | Function |
|---|---|
| 1 | Link to return to the `` `GCAP profiles` `` screen |
| 2 | Message area informing that the selected ruleset has been updated. |
| 3 | `` `SINGLE TENANT` `` button: manages the rulesets and detection options for this configuration<br>• Selection of the ruleset to be configured (12)<br>• Selection of the activation of the Shellcodes detection (11)<br>• Selection of the activation of the Powershell detection (10) |
| 4 | `` `MULTI-TENANT BY INTERFACE` `` button: manages the rulesets and detection options for this configuration<br>• Selection of the interface to set (monx or monvirt)<br>• Selection of the ruleset to configure<br>• Selection of the activation of the Shellcodes detection<br>• Selection of the activation of the Powershell detection |
| 5 | `` `MULTI-TENANT BY VLAN` `` button: manages the rulesets and detection options for this configuration<br>• Selection of the VLAN to configure<br>• Selection of the ruleset to configure<br>• Selection of the activation of the Shellcodes detection<br>• Selection of the activation of the Powershell detection |
| 6 | `` `Add a ruleset` `` button: displays the Ruleset screen for adding a ruleset (see *`Config - sigflow/rulesets` screen of the legacy web UI*) |
| 7 | `` `Reset config` `` button: enables resetting the configuration |
| 8 | `` `Apply` `` button: enables the settings to be saved and makes the rulesets available to GCaps |
| 9 | `` `Save` `` button: enables saving the current option settings (SINGLE TENANT...) |

#### 5.6.14.2 `` `Base variables` `` section of the `` `Config Gcaps profiles` `` menu

The **Base variables** section enables the probe's capture parameters to be adjusted using the advanced Sigflow functions that can be configured from the `` `GCenter` ``.
Changes to this configuration have an impact on the alerts sent from the GCap probe to the GCenter.

Enabling certain options will enable the sending of alerts, anomalies, metadata, file information, and protocol-specific records.
Alerts are records of events triggered by the matching of a rule with network traffic.
An alert will be created with associated metadata, such as the application layer record (HTTP, DNS, etc).

The `` `Base Variables` `` screen consists of the following fields:

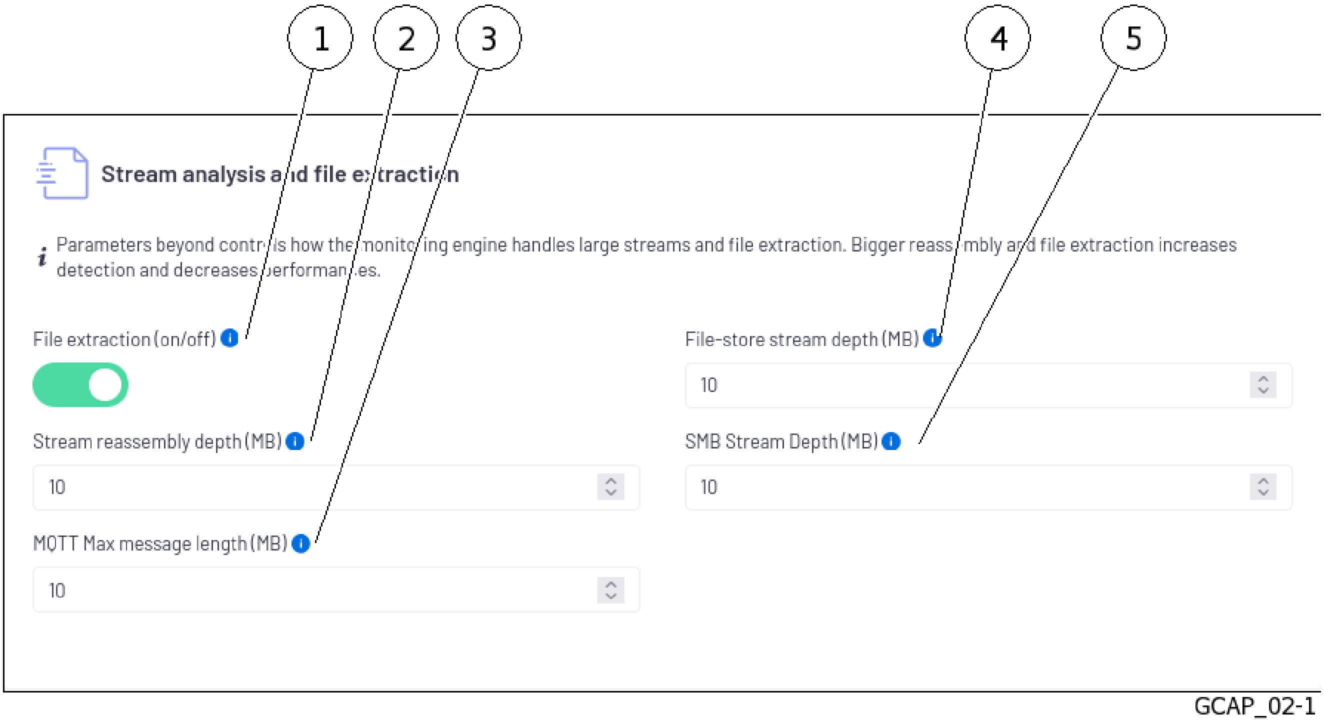
- *`Stream analysis and file extraction` zone*
- *`HTTP Proxy` zone*
- *`Payload` zone*
- *`Community ID` zone*
- *`Alerting and logging` zone*

#### 5.6.14.2.1 `Stream analysis and file extraction` zone

The `Stream analysis and file extraction` zone enables you to control how the Sigflow engine handles maximum stream and file extraction sizes.

##### 5.6.14.2.1.1 Description of the `Stream analysis and file extraction` zone

This zone includes the following items:



Parameters beyond controls how the monitoring engine handles large streams and file extraction. Bigger reassembly and file extraction increases detection and decreases performances.

File extraction (on/off)

Stream reassembly depth (MB): 10

MQTT Max message length (MB): 10

File-store stream depth (MB): 10

SMB Stream Depth (MB): 10

GCAP_02-1

| Item | Function |
|---|---|
| 1 | `` `File extraction (on/off)` ``: enables the control of the size of stored files.<br>See *`File rule management` section of the `Config Gcaps profiles` menu* to specify which files are extracted |
| 2 | `` `Stream reassembly depth (MB)` ``: maximum size of the network stream in megabytes.<br>The default value is a parameter that can be overridden by the protocol analysers performing the file extraction.<br>The inspection will be ignored if this value is reached for a particular flow.<br>Setting this value to 0 enables any flow size to be stored. |
| 3 | `` `MQTT Max message length (MB)` ``. maximum size of an MQTT message to be parsed.<br>Beyond this value, the message will not be parsed. |
| 4 | `` `File-store stream depth (MB)` `` : maximum size of a reconstructed and stored file in megabytes.<br>If this value is reached, the file may be truncated and not entirely stored.<br>This implies that after this value, the HTTP session will no longer be tracked.<br>A negative value disables the option. A value of 0 enables any file size to be stored.<br>If this option is not enabled, then the value of 'Stream reassembly depth (Mb)' will be taken into account.<br>This value must be greater than the value of `` `Stream reassembly depth (Mb)` ``. |
| 5 | `` `SMB Stream Depth (MB)` ``. maximum size of the network stream in megabytes.<br>Beyond this value, no reconstruction will be undertaken.<br>If this value is reached, the file may be truncated and not entirely stored.<br>This implies that after this value, the SMB session will no longer be tracked. Additionally, negative values disable the option.<br>Setting this value to 0 enables any file size to be stored. |

**Astuce:**

Too high a value for these parameters increases detection but decreases performance.

**Prudence:**

Changing these parameters may cause the solution to malfunction. This section is reserved for support staff and advanced users.

Only the `` `file_store_stream_depth_mb` `` variable can be modified, never exceeding 100 MB.

#### 5.6.14.2.1.2 Default configuration of the `Base variables` section

| Variables | Values |
|---|---|
| File extraction (On/Off) | Enabled |
| File-store stream depth (MB) | 10 |
| Stream reassembly depth (MB) | 10 |
| SMB Stream Depth (MB) | 10 |
| MQTT Max message length (MB) | 10 |

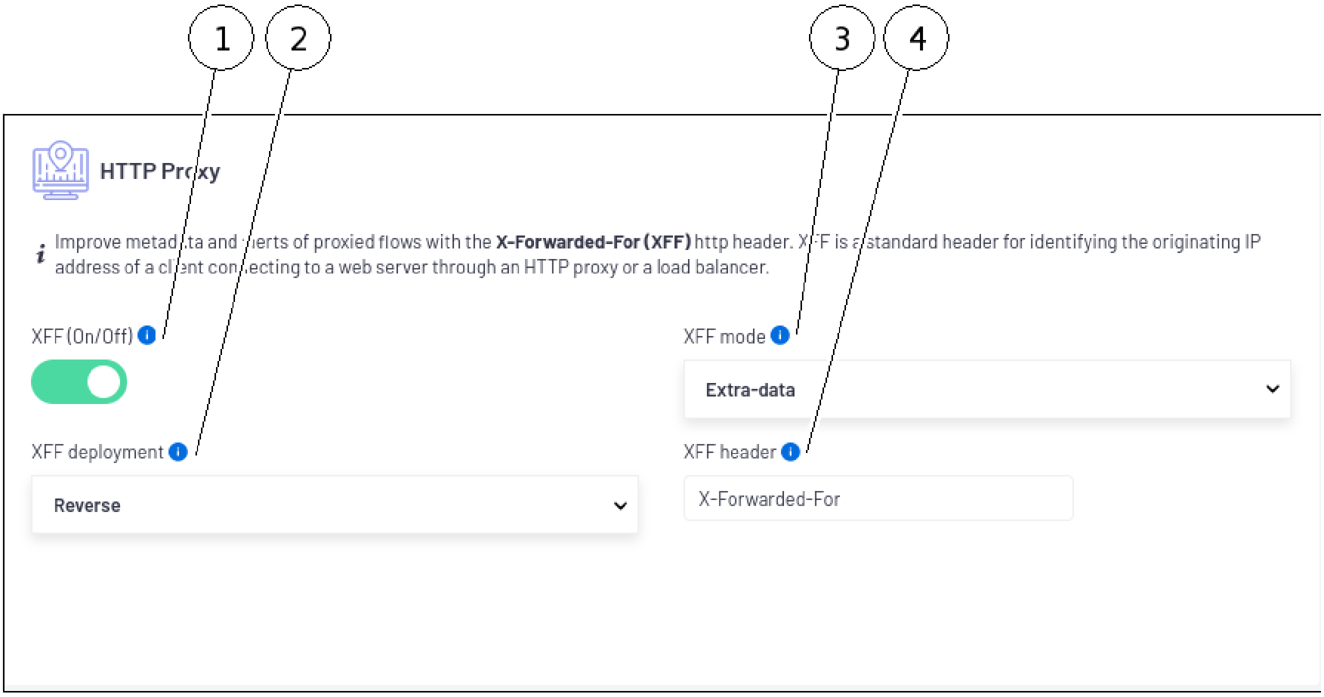
### 5.6.14.2.2 `HTTP Proxy` zone

The `HTTP Proxy` zone enables enhanced metadata and alerts for streams mandated with the X-Forwarded-For (XFF) http header.

XFF is a standard header enabling to identify the original IP address of a client connecting to a web server through an HTTP proxy or load balancer.

#### 5.6.14.2.2.1 Description of the `HTTP Proxy` zone

This zone includes the following items:



HTTP Proxy

Improve metadata and alerts of proxied flows with the **X-Forwarded-For (XFF)** http header. XFF is a standard header for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or a load balancer.

XFF (On/Off): On

XFF mode: Extra-data

XFF deployment: Reverse

XFF header: X-Forwarded-For

GCAP_02-2

| Item | Function |
|---|---|
| 1 | \`XFF (On/Off)\` selector: enabling the management of the HTTP *X-Forwarded-For* header by adding a new field or<br>by overwriting the source or destination IP address, depending on the direction of the flow, with the IP indicated in this header.<br>The behavior, either adding a field or overwriting, is handled by the \`XFF mode\` directive.<br>This directive is helpful when processing flows behind a reverse proxy for example. |
| 2 | \`XFF deployment\`: type of XFF deployment. Two types of deployment are available(*reverse* or *forward*).<br>In a *reverse* deployment, the IP address used is the last one, while in a *forward* deployment, the IP address used is the first one. |
| 3 | \`XFF mode\`: expected behavior when XFF is activated.<br>Two types of operating modes are available, extra-data or overwrite.<br>Note that in *overwrite*, if the IP address reported in the HTTP X-Forwarded-For header is a different version of the received packet, then it will switch to 'extra-data' mode |
| 4 | \`XFF header\` : This is the name of the HTTP header where the real IP address is present.<br>If there is more than one IP address present then the last IP address is taken into account. |

#### 5.6.14.2.2.2 Default configuration of the \`HTTP Proxy\` zone settings

| Variables | Values |
|---|---|
| XFF (On/Off) | Enabled |
| XFF mode | Extra-data |
| XFF deployment | Reverse |
| XFF header | X-Forwarded-For |

#### 5.6.14.2.3 \`Payload\` zone

The \`Payload\` zone enables alerts to be enriched with the content of the stream that triggered them.

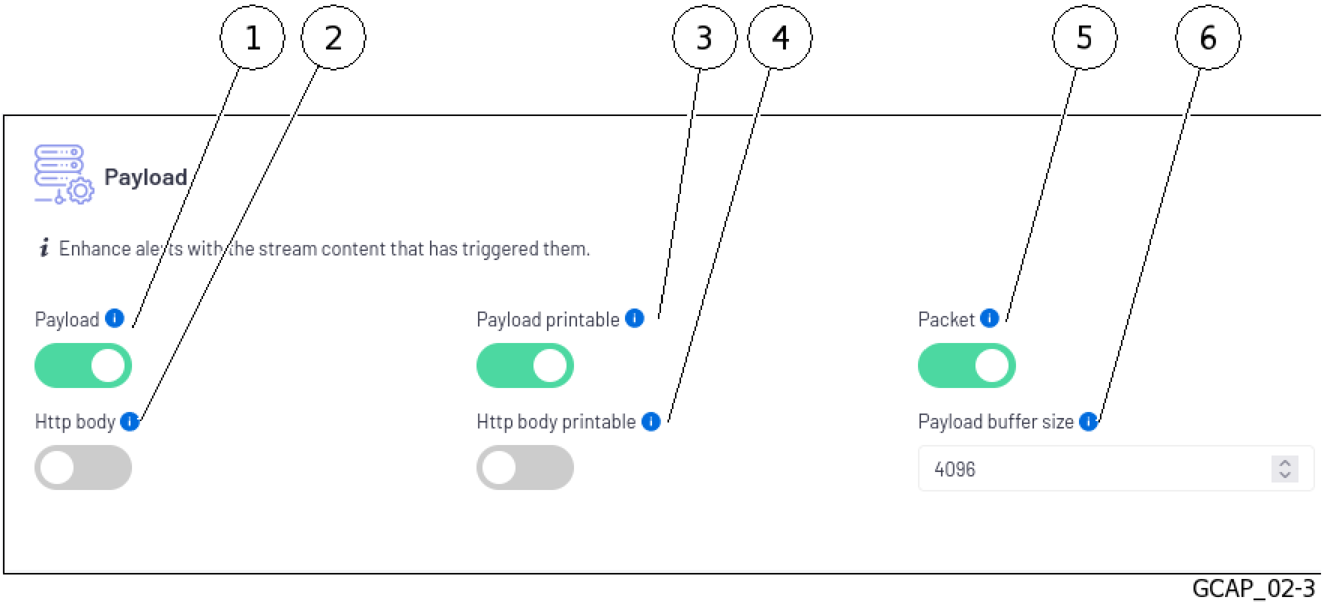
**Note:**

Enabling all of the following fields can generate events larger than 65kb, but exporting data cannot transmit events larger than this size.

In case an event exceeds 65KB, it will be truncated and the remote server will not receive the entire event.

#### 5.6.14.2.3.1 Description of the `Payload` zone

This zone includes the following items:



*i* Enhance alerts with the stream content that has triggered them.

Payload buffer size: 4096

| Item | Function |
|---|---|
| 1 | \`Payload\` selector: enables adding a field containing the base64 encoded payload of a triggering stream |
| 2 | \`Http body\`: adds a field containing the body of HTTP requests encoded in base64.<br>This parameter requires metadata to work. |
| 3 | \`Payload printable\`: adds a field containing the (*Payload*) in ASCII (so-called 'human') format. |
| 4 | \`Http body printable\`: adds a field containing the body of HTTP requests in ASCII format.<br>This parameter requires metadata to work. |
| 5 | \`Packet\`: dump of the captured base64 encoded package. |
| 6 | \`Payload buffer size\` : maximum size of the payload buffer to be added in the alert |

#### 5.6.14.2.3.2 Default configuration of the `Payload` zone settings

| Variables | Values |
|---|---|
| Payload | Enabled |
| Payload printable | Enabled |
| Packet | Enabled |
| Http body | Disabled |
| Http body printable | Disabled |
| Payload buffer size | 4096 |

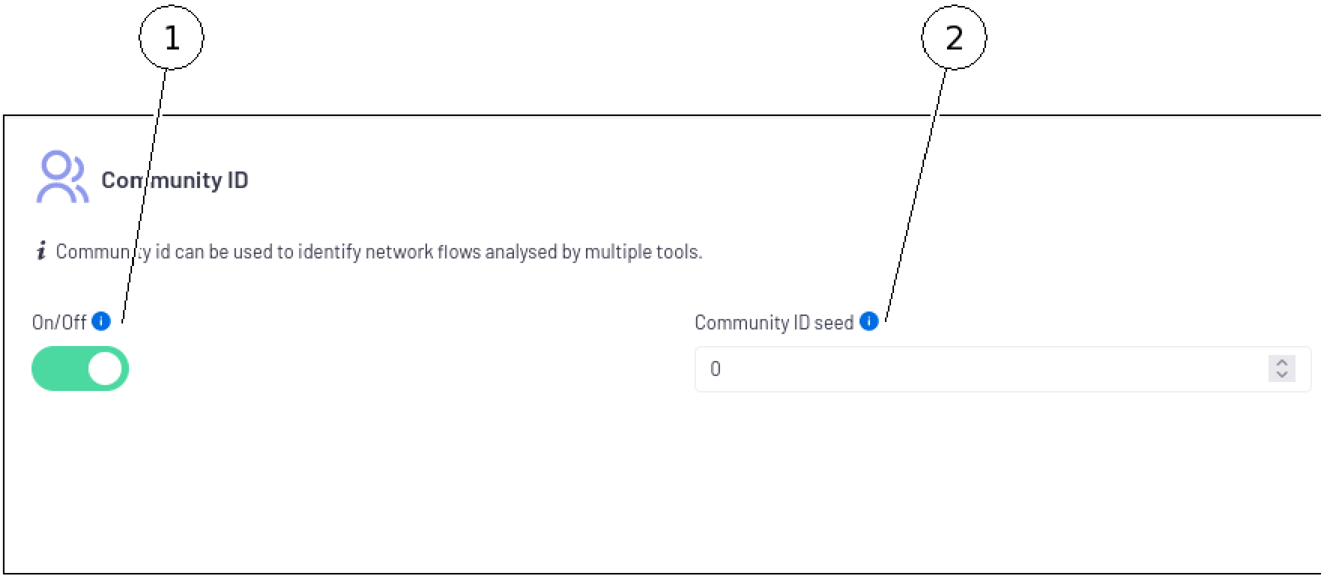
#### 5.6.14.2.4 `Community ID` zone

This zone enables:

- Activating the `Community ID` field in events. This enables identifying the network streams being analyzed
- Configuring the "seed" to be identical to other tools in the same information system

##### 5.6.14.2.4.1 Description of the `Community ID` zone

This zone includes the following items:



Community id can be used to identify network flows analysed by multiple tools.

Community ID seed: 0

GCAP_02-4

| Item | Function |
|---|---|
| 1 | `On/Off`: adds the `Community ID` field to the events |
| 2 | `Community ID seed`: configures the "seed" in order to make it identical to other tools |

##### 5.6.14.2.4.2 Default configuration of the `Community ID` zone settings

| Variables | Values |
|---|---|
| On/Off | Enabled |
| Community ID seed | 0 |

### 5.6.14.2.5 `Alerting and logging` zone

This zone enables configuring the `alerting` and `logging` of the protocols used by the GCap.

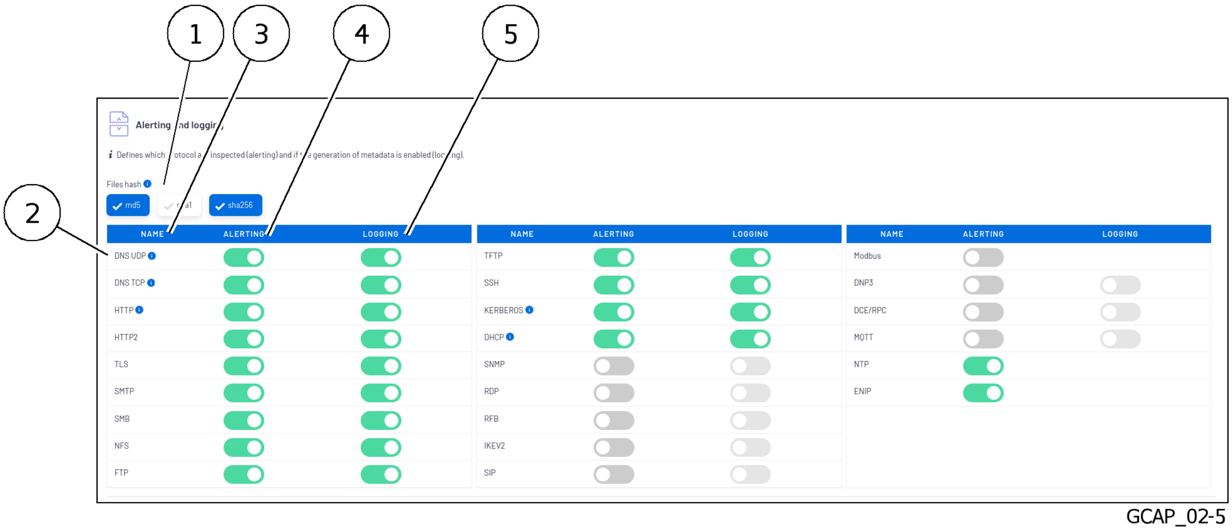
> **Note:**
>
> GCap is one version ahead of the GCenter, it is possible that some protocols are not yet implemented in the latter.

This is discussed in more detail in the GCAP-documentation in the section *Sigflow detection engine > Rebuilding files*.

---

#### 5.6.14.2.5.1 Description of the `Alerting and logging` zone

This zone includes the following items:



Alerting and logging

Defines which protocol are inspected (alerting) and if the generation of metadata is enabled (logging).

Files hash

☑ md5 ☐ sha1 ☑ sha256

| NAME | ALERTING | LOGGING | NAME | ALERTING | LOGGING | NAME | ALERTING | LOGGING |
|---|---|---|---|---|---|---|---|---|
| DNS UDP | ● | ● | TFTP | ● | ● | Modbus | ○ | |
| DNS TCP | ● | ● | SSH | ● | ● | DNP3 | ○ | ○ |
| HTTP | ● | ● | KERBEROS | ● | ● | DCE/RPC | ○ | ○ |
| HTTP2 | ● | ● | DHCP | ● | ● | MQTT | ○ | ○ |
| TLS | ● | ● | SNMP | ○ | ○ | NTP | ● | |
| SMTP | ● | ● | RDP | ○ | ○ | ENIP | ● | |
| SMB | ● | ● | RFB | ○ | ○ | | | |
| NFS | ● | ● | IKEV2 | ○ | ○ | | | |
| FTP | ● | ● | SIP | ○ | ○ | | | |

GCAP_02-5

| Item | Function |
|---|---|
| 1 | Selector for choosing the hash function for reconstructed files (md5, sha1 and sha256).<br>By default, md5 is selected. The sha256 hash will in all cases be added by the Malcore module. |
| 2 | List of protocols. For each of these protocols, the following are listed:<br>• The name (3)<br>• The switch for enabling the `alerting` (4)<br>• The switch for enabling the `logging` (5) |

The parameters displayed here are those of the profile previously loaded in the GCap.
This was done by:

- Using the `GCaps pairing and status` command in the *`Admin-GCaps pairing and status` screen of the legacy Web UI*.
- Select a default profiles such as Minimal, Balanced, MPL, Paranoid, and Intuitio: in order from most to least permissive

- This profile is loaded into the GCap with the `Update` button.

  From this moment on, this profile is loaded into the selected GCap. It can therefore be viewed in the `Base variables` window.
- If necessary, use the `Reset to default configuration` command to reload this default profile with the default values.

  In addition to these protocols, it is also possible to generate `Netflow` data and enable `fingerprint JA3`.

  Both options are disabled by default (`Balanced` profile).

**Avertissement:**

Enabling NetFlow data generation will create a great deal of metadata.

#### 5.6.14.2.5.2 Default settings for existing profiles available

| Protocols | Minimal | Balanced | MPL | Paranoid | Intuitio |
|---|---|---|---|---|---|
| dns_udp | Disabled | Enabled | Enabled | Enabled | Enabled |
| dns_tcp | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | Enabled | Enabled | Enabled | Enabled | Enabled |
| http2 | Enabled | Enabled | Enabled | Enabled | Enabled |
| tls | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | Enabled | Enabled | Enabled | Enabled | Enabled |
| smb | Disabled | Enabled | Disabled | Enabled | Enabled |
| nfs | Disabled | Enabled | Disabled | Enabled | Enabled |
| ftp | Disabled | Enabled | Enabled | Enabled | Enabled |
| tftp | Disabled | Enabled | Disabled | Enabled | Enabled |
| ssh | Disabled | Enabled | Disabled | Enabled | Enabled |
| kerberos | Disabled | Enabled | Disabled | Enabled | Enabled |
| dhcp | Disabled | Enabled | Disabled | Enabled | Enabled |
| snmp | Disabled | Disabled | Disabled | Enabled | Disabled |
| rdp | Disabled | Disabled | Disabled | Enabled | Enabled |
| rfb | Disabled | Disabled | Disabled | Enabled | Disabled |
| ikev2 | Disabled | Disabled | Disabled | Enabled | Disabled |
| sip | Disabled | Disabled | Disabled | Enabled | Disabled |
| modbus | Disabled | Disabled | Disabled | Enabled | Disabled |
| dhp3 | Disabled | Disabled | Disabled | Enabled | Disabled |
| dcerpc | Disabled | Disabled | Disabled | Enabled | Disabled |
| mqtt | Disabled | Disabled | Disabled | Enabled | Disabled |
| ntp | Disabled | Enabled | Disabled | Enabled | Disabled |
| enip | Disabled | Enabled | Disabled | Enabled | Disabled |

| Protocols | Minimal | Balanced | MPL | Paranoid | Intuitio |
|---|---|---|---|---|---|
| dns_udp | Disabled | Enabled | Enabled | Enabled | Enabled |
| dns_tcp | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | Disabled | Enabled | Enabled | Enabled | Enabled |
| http2 | Disabled | Enabled | Enabled | Enabled | Enabled |
| tls | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | Disabled | Enabled | Enabled | Enabled | Enabled |
| smb | Disabled | Enabled | Disabled | Enabled | Enabled |
| nfs | Disabled | Enabled | Disabled | Enabled | Enabled |
| ftp | Disabled | Enabled | Enabled | Enabled | Enabled |
| tftp | Disabled | Enabled | Disabled | Enabled | Enabled |
| ssh | Disabled | Enabled | Disabled | Enabled | Enabled |
| kerberos | Disabled | Enabled | Disabled | Enabled | Enabled |
| dhcp | Disabled | Enabled | Disabled | Enabled | Enabled |
| snmp | Disabled | Disabled | Disabled | Enabled | Disabled |
| rdp | Disabled | Disabled | Disabled | Enabled | Enabled |
| rfb | Disabled | Disabled | Disabled | Enabled | Disabled |
| ikev2 | Disabled | Disabled | Disabled | Enabled | Disabled |
| sip | Disabled | Disabled | Disabled | Enabled | Disabled |
| dhp3 | Disabled | Disabled | Disabled | Enabled | Disabled |
| dcerpc | Disabled | Disabled | Disabled | Disabled | Disabled |
| mqtt | Disabled | Disabled | Disabled | Enabled | Disabled |

#### 5.6.14.3 `Net variables` section of the `Config Gcaps profiles` menu

##### 5.6.14.3.1 Information on the `Net variables` section

In the structure of a rule, just after 'alert' and the protocol keyword, it is possible to use variables that will enable defining groups of IP addresses.

**In the following example:**

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:”GPL SCAN NULL”; flow:stateless;␣
↪ack:0; flags:0; seq:0; reference:arachnids,4; classtype:attempted-recon;␣
↪sid:2100623; rev:7;)
```

For an alert to be raised under this rule, the source must therefore be included in the $EXTERNAL_NET variable and its destination in the $HOME_NET variable.
Both the traffic source and the traffic destination must be specified.
IP addresses (IPv4 and IPv6 are supported) or networks can be assigned. These parameters will be used instead of variables in the detection rules.

Variables adapt as needed and rules can change according to the specified values:

- `list`: enables the action of the rule to be defined in relation to the variable
- `default (equals to HOME_NET)`: enables defining the action of the rule in relation to the addresses given in the HOME_NET environment
- `exclude (opposite of HOME_NET)`: Enables the rule to be used for all addresses that are not part of the HOME_NET environment

It is not necessary to define an address for each of the existing variables.

By default, if nothing is specified, this is equivalent to applying the rule to all traffic (the variable is equivalent to any).

**Note:**

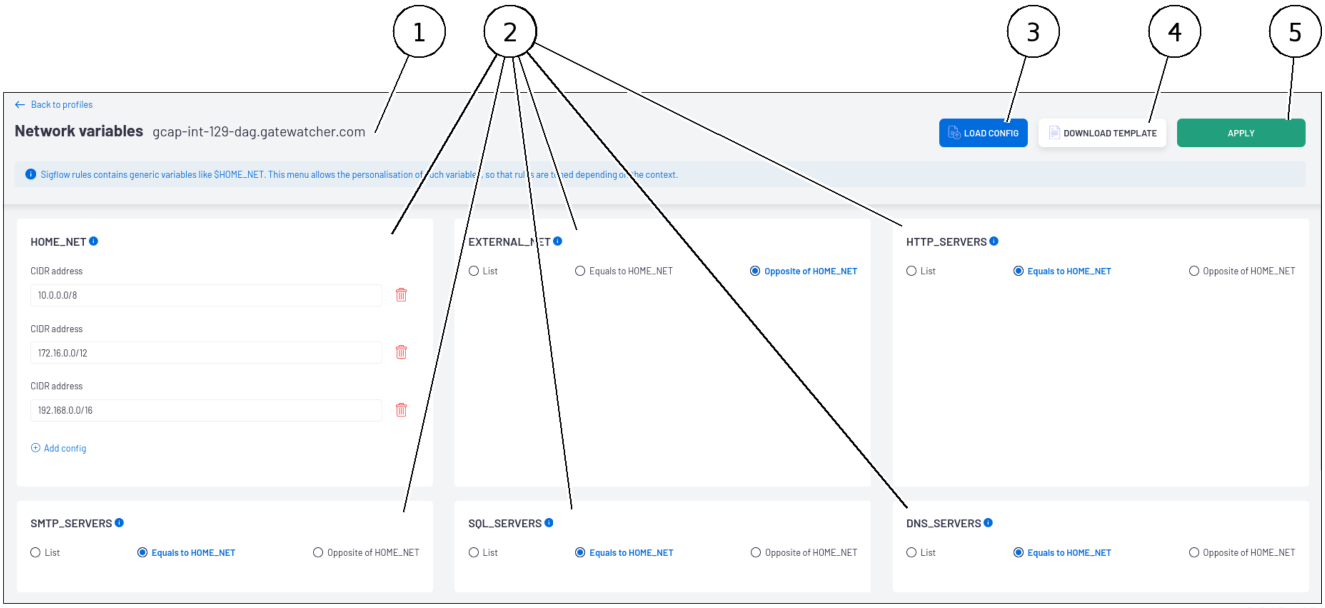
Good practice for the $EXTERNAL_NET variable is to choose the value "Opposite of HOME_NET", anything that is not $HOME_NET by definition.

The `` `Net variables` `` area enables defining the contents of these variables used in Sigflow rules.

---

#### 5.6.14.3.2 Description of the `` `Net variables` `` zone

This zone includes the following items:



← Back to profiles

**Network variables** gcap-int-129-dag.gatewatcher.com

LOAD CONFIG | DOWNLOAD TEMPLATE | APPLY

Sigflow rules contains generic variables like $HOME_NET. This menu allows the personalisation of such variables, so that rules are tuned depending on the context.

HOME_NET

CIDR address: 10.0.0.0/8

CIDR address: 172.16.0.0/12

CIDR address: 192.168.0.0/16

⊕ Add config

EXTERNAL_NET

○ List ○ Equals to HOME_NET ● Opposite of HOME_NET

HTTP_SERVERS

○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

SMTP_SERVERS

○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

SQL_SERVERS

○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

DNS_SERVERS

○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

GCAP_03

| Item | Function | Settings |
|---|---|---|
| 1 | GCAP selected | |
| 2 | Variable areas: these are listed below: | |
| | • home_net | CIDR address / CIDR address / CIDR address |
| | • external_net | List / Equals to HOME_NET / Opposite of HOME_NET |
| | • http_servers | List / Equals to HOME_NET / Opposite of HOME_NET |
| | • smtp_servers | List / Equals to HOME_NET / Opposite of HOME_NET |
| | • sql_servers | List / Equals to HOME_NET / Opposite of HOME_NET |
| | • dns_servers | List / Equals to HOME_NET / Opposite of HOME_NET |
| | • telnet_servers | List / Equals to HOME_NET / Opposite of HOME_NET |
| | • aim_servers | List / Equals to HOME_NET / Opposite of HOME_NET |
| | • dnp3_servers | List / Equals to HOME_NET / Opposite of HOME_NET |
| | • modbus_servers | List / Equals to HOME_NET / Opposite of HOME_NET |
| | • modbus_clients | List / Equals to HOME_NET / Opposite of HOME_NET |
| | • enip_servers | List / Equals to HOME_NET / Opposite of HOME_NET |
| | • enip_clients | List / Equals to HOME_NET / Opposite of HOME_NET |
| 3 | \`LOAD CONFIG\` button: enables importing a pre-configured configuration file (excel file) | |
| 4 | \`DOWNLOAD TEMPLATE\` button: enables a template configuration file to be uploaded and populated. | |
| 5 | \`APPLY\` button: saving and applying the configuration to the GCap | |

#### 5.6.14.3.3 Default configuration of the `Net variables` section

| Variables | Settings | by default |
|---|---|---|
| home_net | CIDR address, CIDR address, CIDR address | 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 |
| external_net | List / Equals to HOME_NET / Opposite of HOME_NET | Opposite of HOME_NET |
| http_servers | List / Equals to HOME_NET / Opposite of HOME_NET | Equals to HOME_NET |
| smtp_servers | List / Equals to HOME_NET / Opposite of HOME_NET | Equals to HOME_NET |
| sql_servers | List / Equals to HOME_NET / Opposite of HOME_NET | Equals to HOME_NET |
| dns_servers | List / Equals to HOME_NET / Opposite of HOME_NET | Equals to HOME_NET |
| telnet_servers | List / Equals to HOME_NET / Opposite of HOME_NET | Equals to HOME_NET |
| aim_servers | List / Equals to HOME_NET / Opposite of HOME_NET | Equals to HOME_NET |
| dnp3_servers | List / Equals to HOME_NET / Opposite of HOME_NET | Equals to HOME_NET |
| modbus_servers | List / Equals to HOME_NET / Opposite of HOME_NET | Equals to HOME_NET |
| modbus_clients | List / Equals to HOME_NET / Opposite of HOME_NET | Equals to HOME_NET |
| enip_servers | List / Equals to HOME_NET / Opposite of HOME_NET | Equals to HOME_NET |
| enip_clients | List / Equals to HOME_NET / Opposite of HOME_NET | Equals to HOME_NET |

**Attention:**

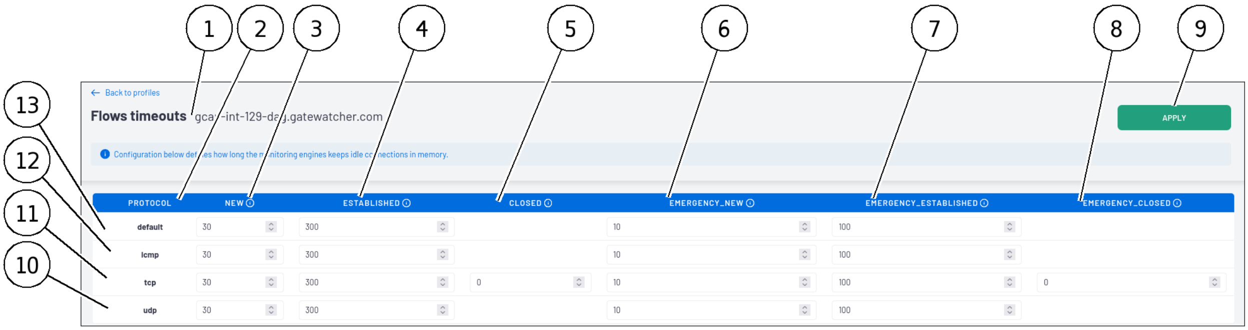
When pairing a GCap, the `Net variables` have the above default values (3 home_net declared and active by default).

### 5.6.14.4 `Flow timeouts` section of the `Config Gcaps profiles` menu

The `Flow timeouts` section enables configuring the time in seconds that Sigflow keeps a flow in memory depending on its status.

#### 5.6.14.4.1 Description of the `Flow timeouts` section

This section includes the following items:



← Back to profiles

**Flows timeouts** gcap-int-129-day.gatewatcher.com

APPLY

Configuration below defines how long the monitoring engines keeps idle connections in memory.

| PROTOCOL | NEW | ESTABLISHED | CLOSED | EMERGENCY_NEW | EMERGENCY_ESTABLISHED | EMERGENCY_CLOSED |
|---|---|---|---|---|---|---|
| default | 30 | 300 |  | 10 | 100 |  |
| icmp | 30 | 300 |  | 10 | 100 |  |
| tcp | 30 | 300 | 0 | 10 | 100 | 0 |
| udp | 30 | 300 |  | 10 | 100 |  |

GCAP_04

| Item | Function |
|---|---|
| 1 | GCap selected |
| 2 | List of protocols. For each of these protocols, the following are listed:<br>• The `New` field (3): period during which the connection is established.<br>This field is the time in seconds after the last activity of this flow in this status type.<br>• The `Established` field (4): period during which the data transfer takes place.<br>This field is the time in seconds after the last activity of this flow in this status type.<br>• The `Closed` field (5): period during which the end of the connection is established.<br>This field is the time in seconds after the last activity of this flow in this status type.<br>• `Emergency_new` field (6)<br>• `Emergency_established` field (7)<br>• `Emergency_closed` field (8) |
| 9 | `APPLY` button: saving and applying the configuration to the GCap |

**Prudence:**

Changing the settings in this section may cause the AIONIQ solution to malfunction.
This section is reserved for support staff and advanced users.

The udp, tcp, and icmp protocols are configurable.
Each protocol, there are different statuses in which a flow can be found:

- TCP protocol (11):

- `New`
- `Established`
- `Closed`

- UDP (10) and ICMP protocols (12):

- `New`
- `Established`

`Emergency_new`, `Emergency_established` and `Emergency_closed` are the emergency modes for the three states of TCP, UDP, and ICMP.

#### 5.6.14.4.2 Default configuration of the `Flow timeouts` section

The default configuration used depending on the protocol (all values are in seconds):

| Protocol | New | Established | Closed | Emergency new | Emergency established | Emergency closed |
|---|---|---|---|---|---|---|
| udp | 30 | 300 | • | 10 | 100 | • |
| tcp | 30 | 300 | 0 | 10 | 100 | 0 |
| icmp | 30 | 300 | • | 10 | 100 | • |
| default | 30 | 300 | • | 10 | 100 | • |

### 5.6.14.5 `File rule management` section of the `Config Gcaps profiles` menu

#### 5.6.14.5.1 Information on the `File rule management` section

The `Files rules management` section enables configuring the file types that the probe will retrieve for a given protocol.
The supported protocols are: FTP, HTTP, HTTP2, NFS, SMB, SMTP.
Files are reconstructed and then saved to disk with metadata that includes information such as:

- Time stamp
- Source/destination IP address
- Protocol
- Source/destination port
- Size
- md5sum, etc.

File extraction works in parallel with the Sigflow signatures defined for these same protocols.
Each line in the `Files rules management` section corresponds to an extraction rule for a file type.

**Note:**

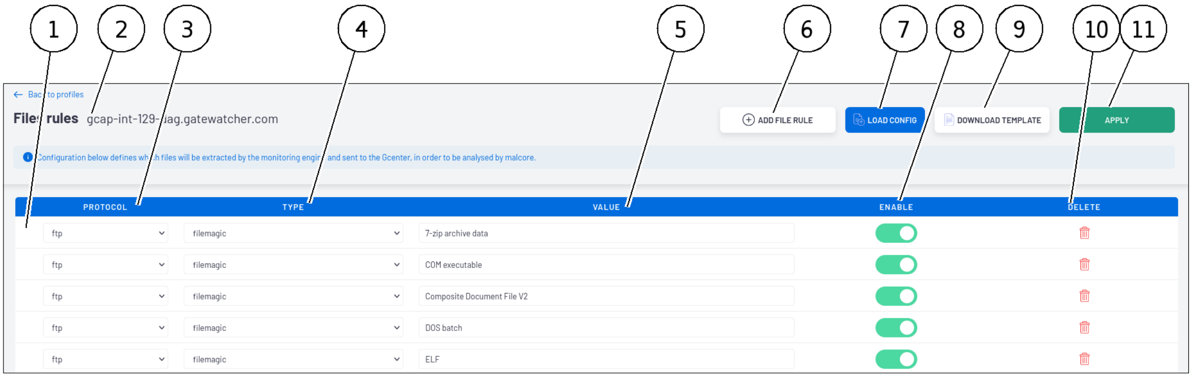
Too many file extraction rules can have a significant impact on the performance of the GCap.

**Note:**

Changes to this section require the GCap configuration to be backed up and implemented via the `Apply` button.

#### 5.6.14.5.2 Description the `File rule management` section

This section includes the following items:



← Bac to profiles

**File rules** gcap-int-129-ag.gatewatcher.com

ADD FILE RULE | LOAD CONFIG | DOWNLOAD TEMPLATE | APPLY

Configuration below defines wh h files will be extracted by the monitoring engir and sent to the Gcenter, in order to be analysed by malcore.

| PROTOCOL | TYPE | VALUE | ENABLE | DELETE |
|---|---|---|---|---|
| ftp | filemagic | 7-zip archive data | ● | 🗑 |
| ftp | filemagic | COM executable | ● | 🗑 |
| ftp | filemagic | Composite Document File V2 | ● | 🗑 |
| ftp | filemagic | DOS batch | ● | 🗑 |
| ftp | filemagic | ELF | ● | 🗑 |

GCAP_05

| Item | Function |
|---|---|
| 1 | Defining a file rule: it includes the following fields:<br>• The `Protocole` field (3) enables selecting the protocol for which the file will be extracted from among FTP, HTTP, HTTP2, NFS, SMB, SMTP.<br>• The `Type` field (4) enables defining the way Sigflow recognizes the file. The choices are available:<br>– The `extension` choice: taking into account the file extension<br>– The `filemagic` choice: taking into account the type of the extracted file. The `file` command under Linux enables obtaining this information. See note below.<br>• The `Value` field (5): identifier of the file that will be rebuilt according to the previously configured type<br>– if the choice `extension` in the type field is selected then this extension must be specified, e.g.:<br>∗ for a Javascript file, enter `js`<br>∗ for a Windows executable file, enter `exe`<br>– if the choice `filemagic` in the type field is selected then this information must be specified, e.g.:<br>∗ for a javascript file, enter `Javascript`<br>∗ for a windows executable file, enter `PE32 executable`<br>• The `ENABLE` choice (8): selector to activate this rule<br>• The `DELETE` choice (9) delete this line |
| 2 | GCAP selected |
| 6 | `ADD FILE RULE` button adds a new rule. In the window that opens, fill in the information - Protocol, Type, Value, Enable bullet... |
| 7 | `LOAD CONFIG` button enables importing a pre-configured configuration file. (Excel type file) |
| 9 | `DOWNLOAD TEMPLATE` button: enables a template configuration file to be uploaded and populated. See DOWNLOAD TEMPLATE note. |
| 11 | `Apply` button enables the settings to be saved and makes the rulesets available to GCaps |

**Note:**

The `file` command under Linux enables obtaining this information.

```
shell
xxx@debian:~$ file ~/Téléchargements/xxx.exe
/home/xxx/Téléchargements/xxx.exe: PE32 executable (console) Intel 80386, for␣
↪MS Windows
```

**Note:**

It is strongly recommended to use the filemagic type. This is more accurate because it is based on the file's content and not on its extension. A file is therefore reconstructed for what it really is.

**Note:**

DOWNLOAD TEMPLATE

The `DOWNLOAD TEMPLATE` button downloads a *.csv* file to the user's PC.
This template file contains column names and titles enabling the user to create a custom configuration file.

The rules displayed are those of the profile previously loaded into the GCap.
This was done by:

- Use the `GCaps pairing and status` command in the WEB UI
- Select a default profiles such as Minimal, Balanced, MPL, Paranoid, and Intuitio

The default profile is loaded into the GCap when it is paired with the GCenter.
If necessary, it is possible to reload or change a profile on an already paired GCap with the `Reset to default configuration` command.

#### 5.6.14.5.3 Rules applied depending on the GCap profile used

| Protocols | Type | Values | Minimal | Balanced | LPM | Paranoid | Intuitio |
|---|---|---|---|---|---|---|---|
| ftp | filemagic | 7-zip archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | COM executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Composite Document File V2 | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | DOS batch | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | ELF | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Java archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Javascript | Disabled | Enabled | Disabled | Enabled | Enabled |
| ftp | filemagic | MS Windows shortcut | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | MS-DOS executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Mach-O | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Macromedia Flash | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Microsoft Cabinet archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Microsoft Excel | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Microsoft OOXML | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Microsoft Office Document | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Microsoft PowerPoint | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Microsoft Word | Disabled | Enabled | Enabled | Enabled | Enabled |

suite sur la page suivante

Table 11 – suite de la page précédente

| Protocols | Type | Values | Minimal | Balanced | LPM | Paranoid | Intuitio |
|---|---|---|---|---|---|---|---|
| ftp | filemagic | Node.js script text | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | OS/2 REXX batch file | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | OpenDocument | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | PDF document | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | PE32 executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | PE32 executable (DLL) | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | PE32+ executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | POSIX tar archive | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | RAR archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | Zip archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| ftp | filemagic | gzip compressed data | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | 7-zip archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | COM executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Composite Document File V2 | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | DOS batch | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | ELF | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Java archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Javascript | Disabled | Enabled | Disabled | Enabled | Enabled |
| http | filemagic | MS Windows shortcut | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | MS-DOS executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Mach-O | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Macromedia Flash | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Microsoft Cabinet archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Microsoft Excel | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Microsoft OOXML | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Microsoft Office Document | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Microsoft PowerPoint | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Microsoft Word | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Node.js script text | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | OS/2 REXX batch file | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | OpenDocument | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | PDF document | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | PE32 executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | PE32 executable (DLL) | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | PE32+ executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | POSIX tar archive | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | RAR archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | Zip archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| http | filemagic | gzip compressed data | Disabled | Enabled | Enabled | Enabled | Enabled |
| nfs | filemagic | 7-zip archive data | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | COM executable | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Composite Document File V2 | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | DOS batch | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | ELF | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Java archive data | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Javascript | Disabled | Disabled | Disabled | Disabled | Enabled |
| nfs | filemagic | MS Windows shortcut | Disabled | Disabled | Disabled | Enabled | Enabled |

suite sur la page suivante

Table 11 – suite de la page précédente

| Protocols | Type | Values | Minimal | Balanced | LPM | Paranoid | Intuitio |
|---|---|---|---|---|---|---|---|
| nfs | filemagic | MS-DOS executable | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Mach-O | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Macromedia Flash | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Microsoft Cabinet archive data | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Microsoft Excel | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Microsoft OOXML | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Microsoft Office Document | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Microsoft PowerPoint | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Microsoft Word | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Node.js script text | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | OS/2 REXX batch file | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | OpenDocument | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | PDF document | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | PE32 executable | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | PE32 executable (DLL) | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | PE32+ executable | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | POSIX tar archive | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | RAR archive data | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | Zip archive data | Disabled | Disabled | Disabled | Enabled | Enabled |
| nfs | filemagic | gzip compressed data | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | 7-zip archive data | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | COM executable | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Composite Document File V2 | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | DOS batch | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | ELF | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Java archive data | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Javascript | Disabled | Disabled | Disabled | Disabled | Enabled |
| smb | filemagic | MS Windows shortcut | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | MS-DOS executable | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Mach-O | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Macromedia Flash | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Microsoft Cabinet archive data | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Microsoft Excel | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Microsoft OOXML | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Microsoft Office Document | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Microsoft PowerPoint | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Microsoft Word | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Node.js script text | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | OS/2 REXX batch file | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | OpenDocument | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | PDF document | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | PE32 executable | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | PE32 executable (DLL) | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | PE32+ executable | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | POSIX tar archive | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | RAR archive data | Disabled | Disabled | Disabled | Enabled | Enabled |
| smb | filemagic | Zip archive data | Disabled | Disabled | Disabled | Enabled | Enabled |

suite sur la page suivante

Table 11 – suite de la page précédente

| Protocols | Type | Values | Minimal | Balanced | LPM | Paranoid | Intuitio |
|---|---|---|---|---|---|---|---|
| smb | filemagic | gzip compressed data | Disabled | Disabled | Disabled | Enabled | Enabled |
| smtp | filemagic | 7-zip archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | COM executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Composite Document File V2 | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | DOS batch | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | ELF | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Java archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Javascript | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | MS Windows shortcut | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | MS-DOS executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Mach-O | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Macromedia Flash | Disabled | Enabled | Enabled | Enabled | Enabled |
| smb | filemagic | Microsoft Cabinet archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Microsoft Excel | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Microsoft OOXML | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Microsoft Office Document | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Microsoft PowerPoint | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Microsoft Word | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Node.js script text | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | OS/2 REXX batch file | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | OpenDocument | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | PDF document | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | PE32 executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | PE32 executable (DLL) | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | PE32+ executable | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | POSIX tar archive | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | RAR archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | Zip archive data | Disabled | Enabled | Enabled | Enabled | Enabled |
| smtp | filemagic | gzip compressed data | Disabled | Enabled | Enabled | Enabled | Enabled |

**Note:**

The filemagic that can be used in the `` `Value` `` field are those present in the Libmagic library.
A filemagic not present in this library will not be functional.

---

#### 5.6.14.6 `` `Packet filters` `` section of the `` `Config Gcaps profiles` `` menu

##### 5.6.14.6.1 Information on the `` `Packet filters` `` section

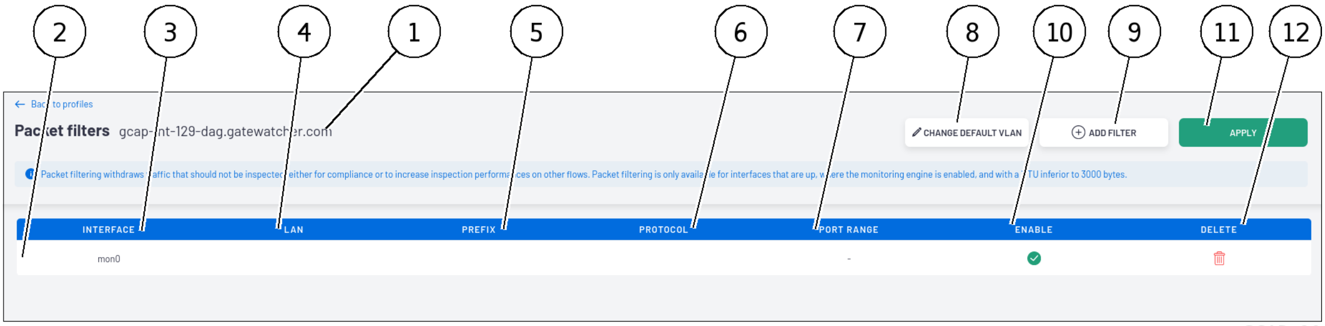
The `` `Packet filters` `` section enables specific traffic to be ignored directly at the GCap network card level.
This feature enables the GCap to avoid overloading the GCap with "unnecessary" traffic such as encrypted streams, backup streams, etc., or traffic that may cause the cpus to overload such as Elephant Flow, Miles Flow, etc.
The selection of traffic to be ignored is based on vlan, network prefix, protocol, and network ports.

Packet filtering is only active:

- For active interfaces monX on the GCap
- With an MTU of less than 3000 bytes
- With the monitoring engine enabled

### 5.6.14.6.2 Description the `Packet filters` section

This section includes the following items:



**Packet filters** gcap-int-129-dag.gatewatcher.com

Packet filtering withdraws traffic that should not be inspected either for compliance or to increase inspection performances on other flows. Packet filtering is only available for interfaces that are up, where the monitoring engine is enabled, and with a MTU inferior to 3000 bytes.

| INTERFACE | LAN | PREFIX | PROTOCOL | PORT RANGE | ENABLE | DELETE |
|---|---|---|---|---|---|---|
| mon0 | | | | - | ✓ | 🗑 |

GCAP_06

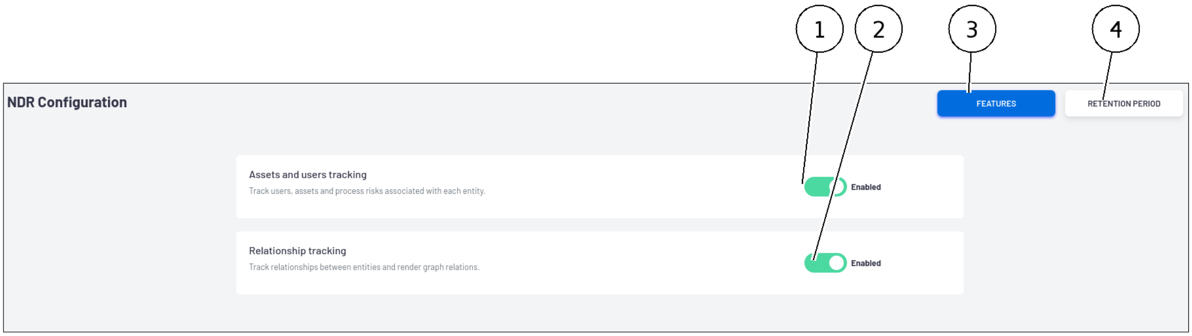
| Item | Function |
|---|---|
| 1 | GCAP selected |
| 2 | Defining a packet filtering rule: it includes the following fields:<br>• The `Interface` field (3) indicates the capture interface to which the filter applies: mon0, mon1, mon2, mon3 or monvirt<br>• The `LAN` field (4) indicates the VLAN number<br>• The `PREFIX` field (5) indicates the IP address filtering to be ignored<br>• The `PROTOCOL` field (6) indicates the ignored protocol:<br>– TCP<br>– UDP<br>– Tunnel protocols (AH, ESP, GRE, L2TP)<br>– All TCP<br>– All UDP<br>– All TCP and UDP<br>– All<br>– AH<br>– ESP<br>– GRE<br>– L2TP<br>• The `PORT RANGE` choice (7) indicates the filter to ignore only the selected port or port range. Only available for the protocols:<br>– TCP<br>– UDP<br>• The `ENABLE` choice (10): selector to activate this rule<br>• The `DELETE` choice (12): delete this line |
| 8 | The `CHANGE NATIVE VLAN` button enables modifying the default vlan for the various active interfaces on the GCap. By default, this vlan is 1 for each interface. |
| 9 | `ADD FILTER` button displays a window for creating a new filter |
| 11 | `Apply` button enables the settings to be saved and makes the filters available to GCaps |

> **Note:**
>
> If an interface can use `Packet filtering` then a line is displayed in the filter list with the various fields empty.

### 5.6.15 Web UI `Admin-NDR configuration` screen

After pressing the `NDR configuration` command from the `Admin` menu, the following screen is displayed. This screen enables:

- Activating the functions:
- `Assets and users tracking`
- `Relationship tracking`
- Setting up elasticsearch data retention:
  - Activating the function `Synchronize NDR boards with Elasticsearch retention`
  - Changing the value of the retention time



NDR Configuration

Assets and users tracking
Track users, assets and process risks associated with each entity.
Enabled

Relationship tracking
Track relationships between entities and render graph relations.
Enabled

NDR-01

The `NDR configuration` screen contains the following sections:

| Item | Name |
|---|---|
| 1 | FEATURES button: activates the display of the following parameters |
| 2 | • `Assets and users tracking` selector: enable tracking active assets, users, and process risks associated with each entity |
| 3 | • `Relationship tracking` selector: enables the tracking of relationships between active devices and displays these relationships |
| 4 | `RETENTION PERIOD` button: activates the display of the following parameters |
|  | • `Synchronize NDR boards with elasticsearch retention` selector: enables synchronizing NDR dashboards with data in Elasticsearch (see text below the table) |
|  | • `Retention period` field: indicates the length of time alerts, users, and equipment data will be retained on disk |

**Function** `Synchronize NDR boards with elasticsearch retention`:

The NDR database stores metadata about the alerts displayed in the dashboards (`Alerts`, `Assets`, `Users`, etc.), while Elasticsearch (Hunting) stores details about them.

Enabling this feature activates the synchronization of NDR dashboards with the data available in Elasticsearch.

Disable this feature to continue to display alerts in NDR dashboards that are no longer stored in Elasticsearch. In this case, the alerts are available but the details cannot be displayed.

The retention time of Elasticsearch depends on the maximum space allocated in GB to store the logs (see *`Admin-GCenter-Configuration` screen of the legacy web UI*).

Therefore, the data retention period in elasticsearch depends on the amount of logs generated by the GCaps.

### 5.6.16 `Config - sigflow/sources` screen of the legacy web UI

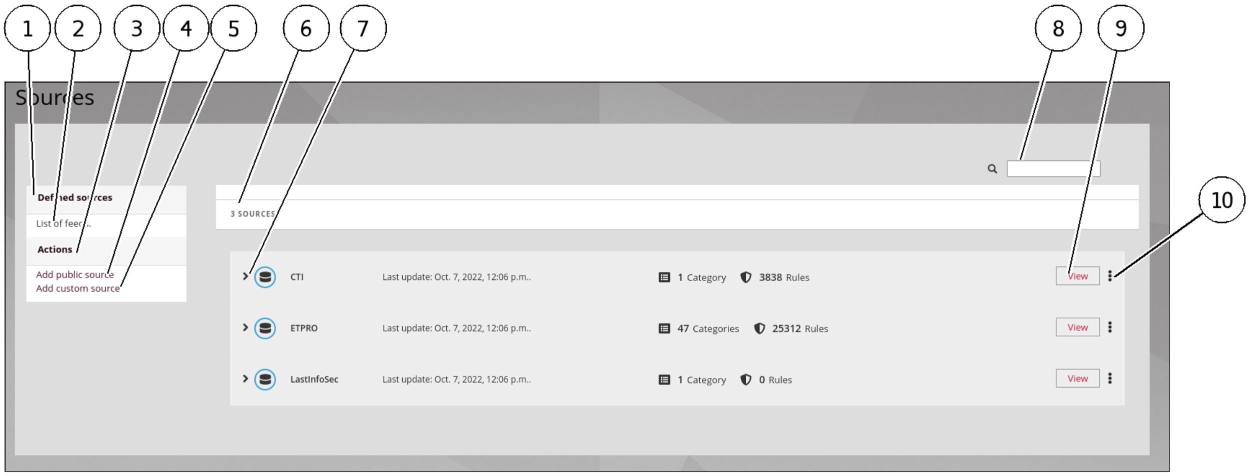
This screen is only accessible to members of the *operator* group.

**Note:**

For *administrator* group members, the following message is displayed: `Error 403: Insufficient permissions.`

After pressing the `Sources` command from the sub-menu `Config/Sigflow`, the following screen is displayed. This screen enables:

- Defining the sources of signatures for the detection engine
- Managing the existing sources
- Managing the rule set files made available by the sources
- Managing the categories and rules of these files



| | | | | |
|---|---|---|---|---|
| CTI | Last update: Oct. 7, 2022, 12:06 p.m.. | 1 Category | 3838 Rules | View |
| ETPRO | Last update: Oct. 7, 2022, 12:06 p.m.. | 47 Categories | 25312 Rules | View |
| LastInfoSec | Last update: Oct. 7, 2022, 12:06 p.m.. | 1 Category | 0 Rules | View |

SOURCES-01

The `Sources` screen contains the following sections:

| Item | Name | Position |
|---|---|---|
| 1 | `Defined sources` | Indicates the list of existing sources |
| 2 | `List of feeds` | List of streams |
| 3 | `Action` | Area of possible actions. The possible actions listed below depend on the context: |
| 4 | `Add public source` | • The button enables adding public sources |
| 5 | `Add custom source` | • The button enables adding custom sources |
| 6 | `3 Sources` | Field indicates the number of sources defined |
| 7 | Description of a source | Defined source. This includes the following types of information:<br>• The source name (CTI, ETPRO, LastInfoSec... )<br>• The date and time of the last update<br>• The number of categories and signatures<br>You can add a MIPS source. To do this, refer to the procedure in *Configuring the connection to the MISP* |
| 8 | Search field | Enables a search |
| 9 | `View` button | Displays the `Sources: view` screen (see below) |
| 10 | context menu | Displays the management sub-menu for this source for access to the `Edit source` and `Delete source` commands |

**Note:**

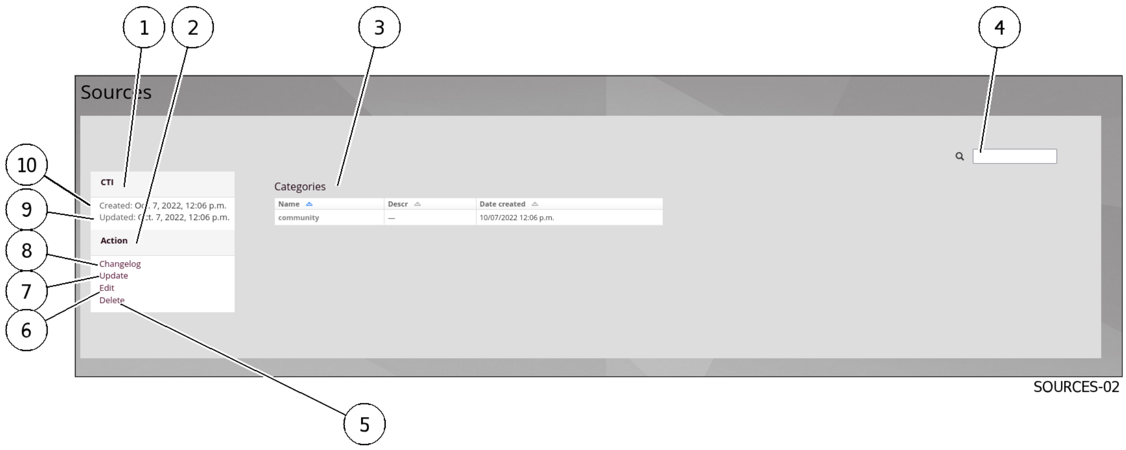
You can have two LastinfoSec entries:

- An entry named `LastinfoSec(Experimental)` : this entry only exists if the GCenter was in version V101 and migrated to V102.

  This entry must be deleted. To do this, refer to *Procedure to delete a source*.
- An entry named `LastinfoSec`: this entry is created in V102.

  This entry must be kept and used.

After pressing the `View` button (9), the `Sources: view` screen contains the following sections:



Created: Oct. 7, 2022, 12:06 p.m.
Updated: Oct. 7, 2022, 12:06 p.m.

| Name | Descr | Date created |
|---|---|---|
| community | — | 10/07/2022 12:06 p.m. |

SOURCES-02

| Item | Name | Position |
|---|---|---|
| 1 | Source field | Indicates the selected source (here CTI). it includes the following fields: |
| 10 | Source creation field | • The date and time the source was created |
| 9 | Update field | • The date and time of the last update |
| 2 | \`Action\` | Area of possible actions. The possible actions listed below depend on the context. |
| 8 | \`Changelog\` | • Button to display the history of the current source |
| 7 | \`Update\` | • Button to update the current source |
| 6 | \`Edit\` | • Button to edit the current source |
| 5 | \`Delet\` | • Button to delete the current source |
| 3 | \`Categories\` | List of categories. This includes three types of information:<br>• The category name<br>• The category description<br>• The creation date of the category |
| 4 | Search field | Enables searching for text in the categories including the description field of the rules |

**Note:**

Each source is made up of categories.
Each of these categories can be edited.
Each category is composed of rules. Clicking on a category will display the list of rules.
Each of these rules can be edited.

See the *SIGFLOW engine rule sources* procedure to :

- Visualization and management of sources
- Visualization and management of rule files

---

### 5.6.17 \`Config - sigflow/rulesets\` screen of the legacy web UI

This screen is only accessible to members of the *operator* group.

**Note:**

For *administrator* group members, the following message is displayed: \`Error 403: Insufficient permissions\`

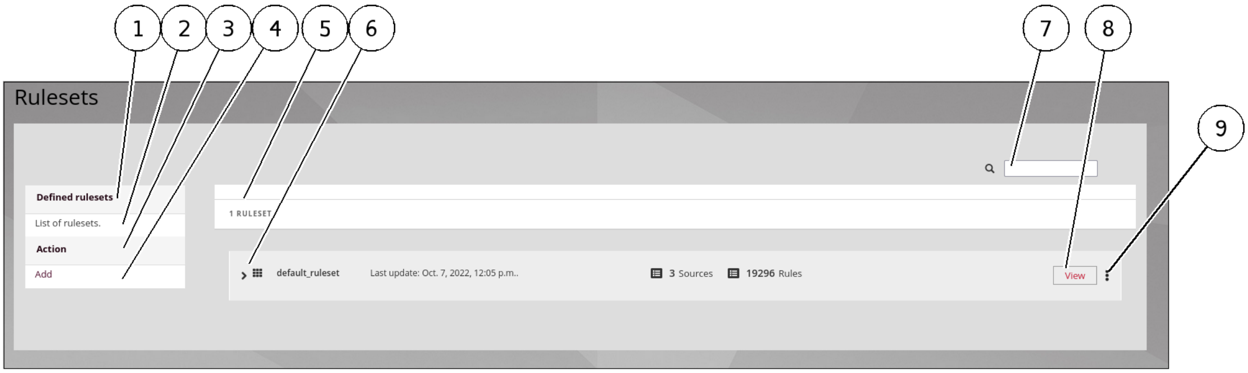
After pressing the \`Rulesets\` command from the sub-menu \`Config/Sigflow\`, the following screen is displayed.

This screen enables:

- Creating files called **rulesets**.
- Managing the categories and rules of Ruleset files. Once a file is generated, its content can also be managed, i.e. modification of categories and rules
- Providing these files to the Sigflow detection engine of the GCap
- Exporting these files to the local download directory with the extension rules

**Note:**

A **ruleset** file is composed of one or more **source** files downloaded from different sources.
Each **source** file is composed of different categories.
Each category consists of rules (or signatures).

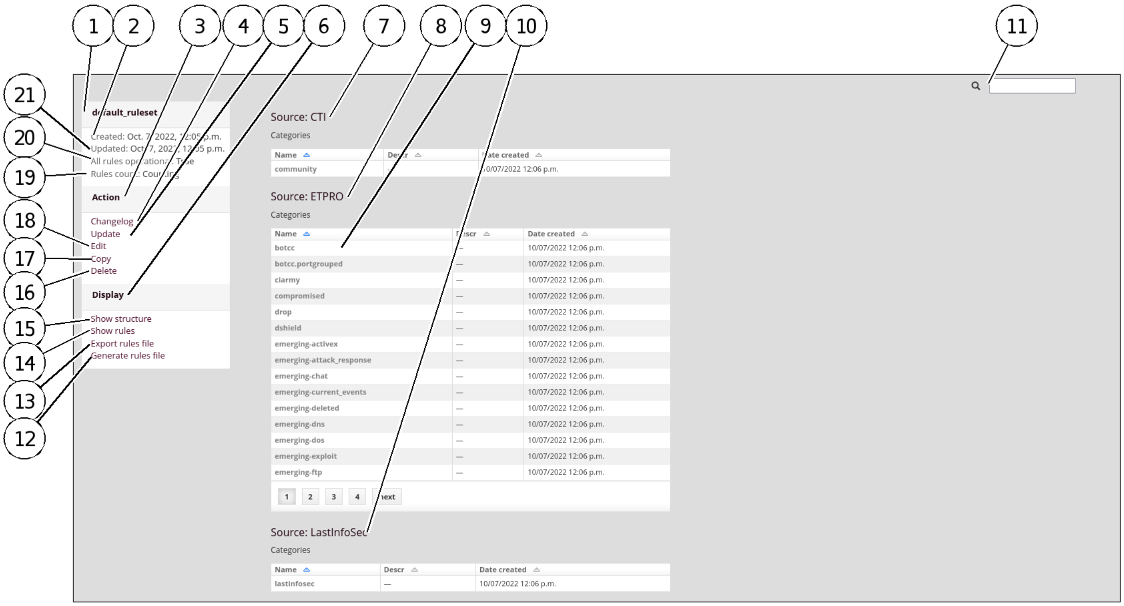


RULESSET-01

`Rulesets` screen contains the following sections:

| Item | Name | Position |
|---|---|---|
| 1 | `Defined rulesets` | Indicates the list of defined signature sets |
| 2 | `List of rulesets` | Indicates that the current screen shows the list of existing rules |
| 3 | `Action` | Area of possible actions. The possible actions listed below depend on the context: |
| 4 | `Add` | • The button to create a **ruleset** |
| 5 | `1 RULESET` | Field indicating the number of **rulesets** available |
| 6 | Description of a ruleset | Includes the following types of information:<br>• The name of the ruleset<br>• The date and time of the last update<br>• thThee number of sources and signatures |
| 7 | Search field | Enables a search |
| 8 | `View` button | Displays the `Rulesets: view` screen (see below) |
| 9 | context menu | Displays the management sub-menu for this source for access to the Edit source and Delete source commands |

After pressing the `View` command button, the `Rulesets: view` screen contains the following sections:



**default_ruleset**

Created: Oct. 7, 2022, 12:05 p.m.
Updated: Oct. 7, 2022, 12:05 p.m.
All rules operational: True
Rules count: Counting

**Action**

Changelog
Update
Edit
Copy
Delete

**Display**

Show structure
Show rules
Export rules file
Generate rules file

Source: CTI

Categories

| Name | Descr | Date created |
|---|---|---|
| community | — | 10/07/2022 12:06 p.m. |

Source: ETPRO

Categories

| Name | Descr | Date created |
|---|---|---|
| botcc | — | 10/07/2022 12:06 p.m. |
| botcc.portgrouped | — | 10/07/2022 12:06 p.m. |
| ciarmy | — | 10/07/2022 12:06 p.m. |
| compromised | — | 10/07/2022 12:06 p.m. |
| drop | — | 10/07/2022 12:06 p.m. |
| dshield | — | 10/07/2022 12:06 p.m. |
| emerging-activex | — | 10/07/2022 12:06 p.m. |
| emerging-attack_response | — | 10/07/2022 12:06 p.m. |
| emerging-chat | — | 10/07/2022 12:06 p.m. |
| emerging-current_events | — | 10/07/2022 12:06 p.m. |
| emerging-deleted | — | 10/07/2022 12:06 p.m. |
| emerging-dns | — | 10/07/2022 12:06 p.m. |
| emerging-dos | — | 10/07/2022 12:06 p.m. |
| emerging-exploit | — | 10/07/2022 12:06 p.m. |
| emerging-ftp | — | 10/07/2022 12:06 p.m. |

1 2 3 4 next

Source: LastInfoSec

Categories

| Name | Descr | Date created |
|---|---|---|
| lastinfosec | — | 10/07/2022 12:06 p.m. |

RULESSET-02

| Item | Name | Position |
|---|---|---|
| 1 | File name field | Indicates the name of the file containing the selected ruleset. This includes the following fields: |
| 2 | `Created` | • The date and time the ruleset was created |
| 21 | `Updated` | • The date and time of the last update |
| 20 | `All rules operational:` | • Status of operational rules (true or false) |
| 19 | `Rules count:` | • rRles counter |
| 3 | `Action` | Area of possible actions. The possible actions listed below depend on the context. |
| 4 | `Changelog` | • Button for displaying the file history |
| 5 | `Update` | • Button to update the file |
| 18 | `Edit` | • Button to edit the file |
| 17 | `Copy` | • Button to copy the file |
| 16 | `Delete` | • Button to delete the file |
| 6 | `Display` | Area of possible actions. The possible actions listed below depend on the context. |
| 12 | `Show structure` | Button to display the file by source and then by category |
| 13 | `Show rules` | Button to display the file by rules, listed by SID |
| 14 | `Export rules files` | Button to export the file |
| 15 | `Generate rules file` | Button to generate the rules file from the current file |
| 7<br>8<br>10 | `Source` | List of categories for each source. This includes three types of information:<br>• The name of the category: example (9)<br>• The description of the category<br>• The creation date of the category |
| 4 | Search field | Enables a search |

**Note:**

Each of these categories can be edited.
Clicking on a category will display the list of rules.
Each of these rules can be edited.

See the procedure *Creating a SIGFLOW engine ruleset* for:

- Creating a Ruleset file
- Managing its content, modifying categories and rules
- Sending a Ruleset file to the Sigflow detection engine in the GCap

- Exporting a file to the local download directory of the user PC with the rules extension

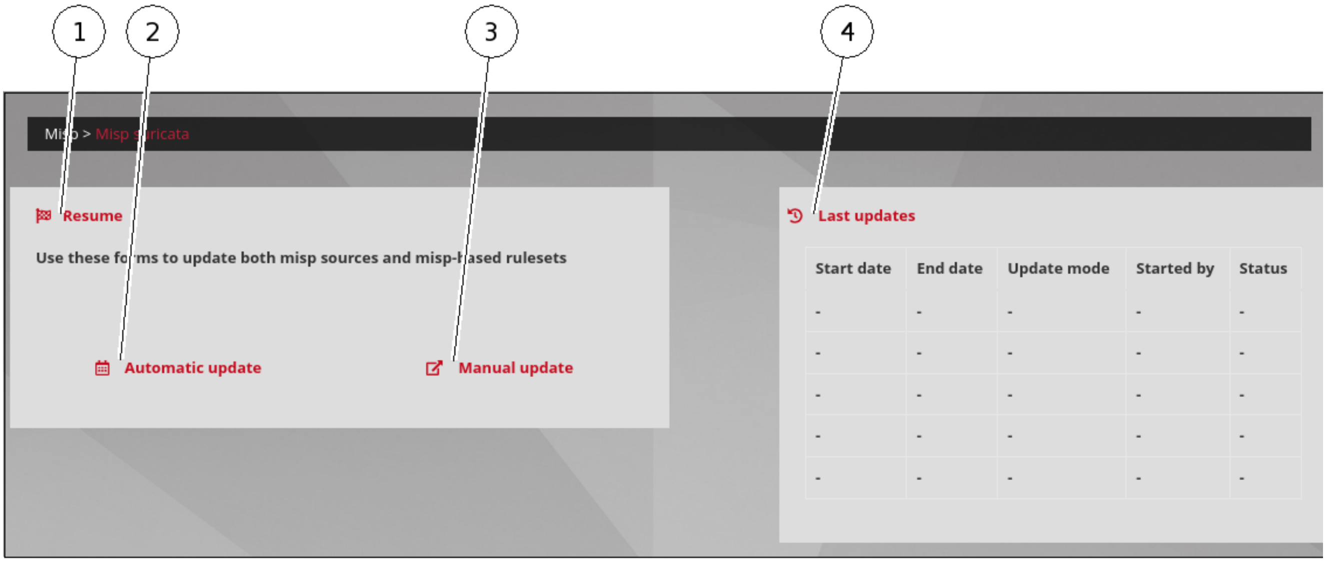
See the procedure *Modifying SIGFLOW engine rules* for:

- The implementation of a transformation rule (Transform rule)
- Deactivation of the rule of a transformation rule
- Activation of the rule of a transformation rule
- Threshold rule
- The deletion rule (Suppress rule)

See the procedure *Generating a SIGFLOW engine ruleset*.

### 5.6.18 `Config - sigflow/MISP` screen of the legacy web UI

This screen allows to manage updates.
This screen is only accessible to members of the *administrator*` group.
After pressing the `MISP` Menu sub menu `Config/Sigflow`, the following screen is displayed.



Use these forms to update both misp sources and misp-based rulesets

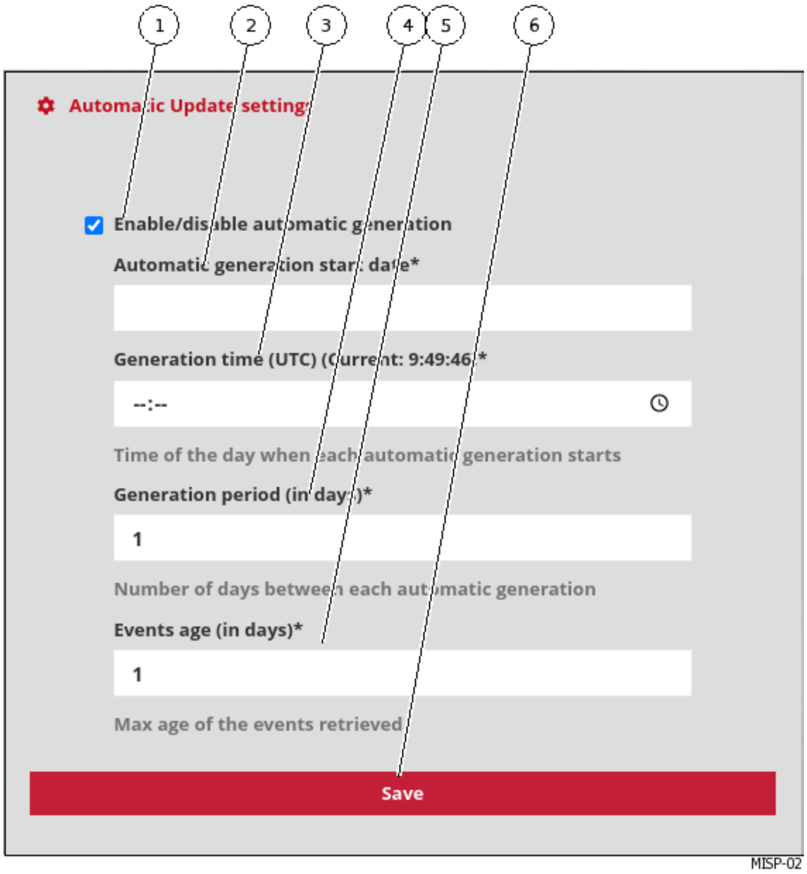
| Start date | End date | Update mode | Started by | Status |
|---|---|---|---|---|
| - | - | - | - | - |
| - | - | - | - | - |
| - | - | - | - | - |
| - | - | - | - | - |
| - | - | - | - | - |

MISP-01

The `Misp suricata` screen contains the following parts:

| Marker | Name | Function |
|---|---|---|
| 1 | `Resume` | Area for access to update configuration. This area includes: |
| 2 | • `Automatic update` | Link to automatic update settings screen |
| 3 | • `Manual update` | Link to manual update setup screen |
| 4 | `Last updates` | Area with information on the latest updates whether automatic or manual |

After pressing the `Automatic update` link, the `Automatic Update settings` screen contains the following parts:



Automatic Update settings

☑ Enable/disable automatic generation

Automatic generation start date*

Generation time (UTC) (Current: 9:49:46)*

--:--

Time of the day when each automatic generation starts

Generation period (in days)*

1

Number of days between each automatic generation

Events age (in days)*

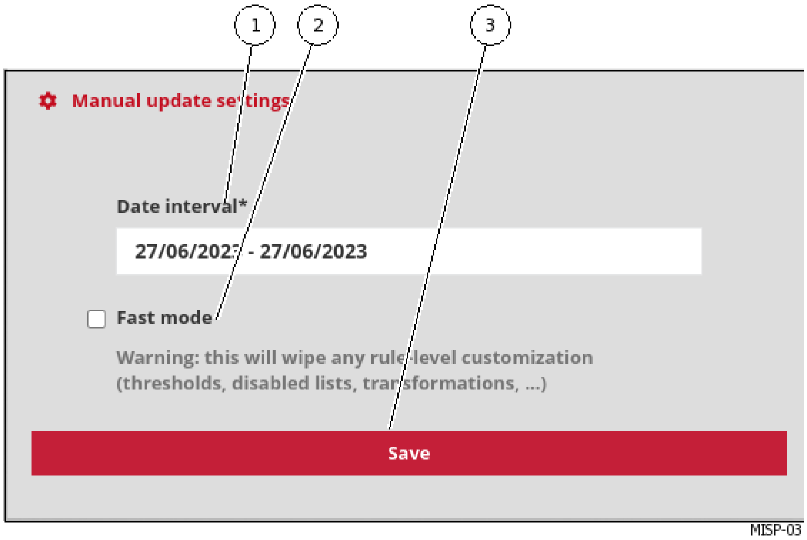
1

Max age of the events retrieved

Save

| Item | Name | Function |
|---|---|---|
| 1 | `Enable/disable automatic generation` | Enables or disables automatic generation of updates |
| 3 | `Automatic generation start date*` | Select start date |
| 4 | `Generation time (UTC) (Current: 18:04:51)*` | Enter the update time in UTC |
| 5 | `Generation period (in days)*` | Select periodicity in days |
| 6 | ` Events age (in days)*` | Enter the maximum age of the events retrieved |
| 7 | `Save` | Save parameters and run programming |

After pressing the `Manual update` link, the `Manual update settings` screen contains the following parts:



Manual update settings

Date interval*

27/06/2023 - 27/06/2023

□ Fast mode

Warning: this will wipe any rule-level customization (thresholds, disabled lists, transformations, ...)

| Item | Name | Function |
|---|---|---|
| 1 | `Date interval*` | Enables or disables automatic generation of updates |
| 2 | `Fast mode* ` | Allows quick update but Caution:<br>this will erase any customization at the rule level (thresholds, disabled lists, transformations, ...) |
| 3 | `Save` | Saves the parameters and starts an immediate update with the selected parameters |

See the procedure *Configuring the connection to the MISP*.

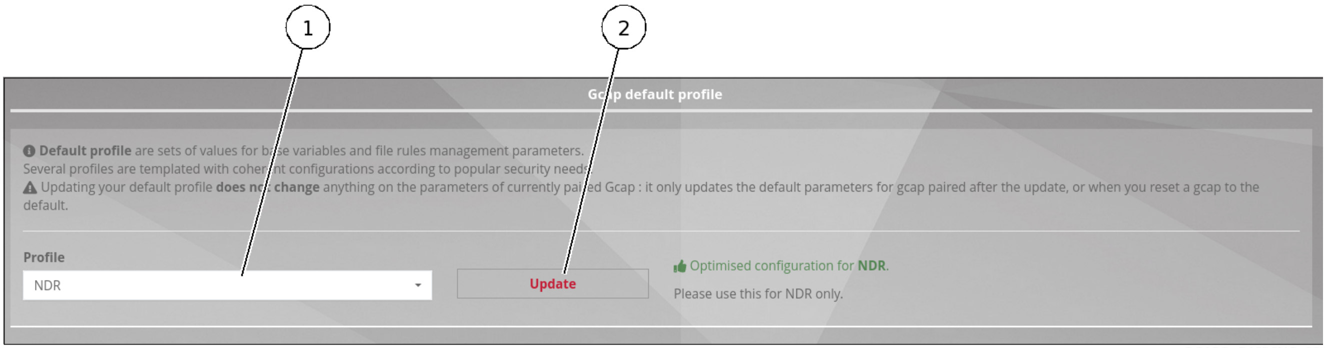
## 5.6.19 `Admin-GCaps pairing and status` screen of the legacy Web UI

After pressing the `GCaps pairing/status` command from the `Admin` menu, the screen consists of two different areas:

- *`Gcap defaut profile` zone*
- *`Gcap pairing and status` zone*

### 5.6.19.1 `Gcap defaut profile` zone

This screen enables configuring the GCap using predefined profiles.



Gcap default profile

**Default profile** are sets of values for base variables and file rules management parameters.
Several profiles are templated with coherent configurations according to popular security needs.
Updating your default profile **does not change** anything on the parameters of currently paired Gcap : it only updates the default parameters for gcap paired after the update, or when you reset a gcap to the default.

Profile: NDR

Optimised configuration for **NDR**.
Please use this for NDR only.

GCAPS_PAIRING-02

| Item | Name | Function |
|---|---|---|
| 1 | \`Profile\` | List of available profiles. The selected choice is that which is visible. |
| 2 | \`Update\` | Loads the selected profile. List of rule sets |

#### 5.6.19.1.1 Profile information

The profiles offered are:

| Profile | Function |
|---|---|
| Minimal | This is the minimalist configuration; less data will be scanned. Very few alerts are generated. |
| Balanced | The recommended configuration, just enough data will be probed. Very few alerts are missed. |
| LPM | MPL Optimized Configuration. A few more alerts can be managed. |
| Paranoid | Paranoid configuration: all events are enabled. Many alerts can be generated. |
| Intuitio | Configuration optimized for NDR. Please use it only for NDRs. |

These profiles define separate configurations for the following topics:

- Alerting and logging configuration of the protocols used by the GCap
  To view the detailed settings for each of these profiles, please refer to *Default settings for existing profiles available*.
- Configuration of the management of the file extraction rules used by the GCap
  To view the detailed settings for each of these profiles, please refer to *Description the \`File rule management\` section*.

#### 5.6.19.1.2 Updating the profile

Pressing the \`Update\` button enables the default profile to be updated and deployed to GCaps.
The default profile is deployed to a GCap:

- When it is paired with the GCenter.
  It is important to select the correct profile so that the GCap takes on the correct profile.
- This is done by pressing the \`Reset to default configuration\` button.
  Please note that all existing manual configurations are then replaced by the default profile configurations.

**Note:**

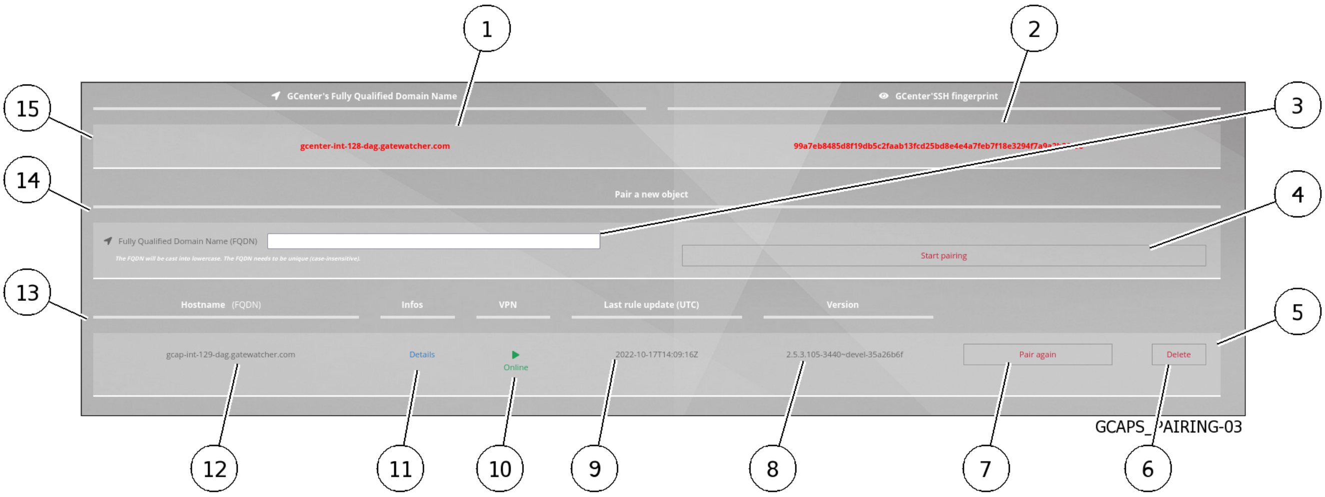
Updating the default profile does not change the configurations of the GCap's already paired to the GCenter.

**Note:**

The update only concerns the choice of the default profile. Profiles are not editable.

### 5.6.19.2 `Gcap pairing and status` zone

This screen enables adding, managing, and pairing the GCaps with the GCenter.



GCenter's Fully Qualified Domain Name: gcenter-int-128-dag.gatewatcher.com

GCenter'SSH fingerprint: 99a7eb8485d8f19db5c2faab13fcd25bd8e4e4a7feb7f18e3294f7a9a

Pair a new object

Fully Qualified Domain Name (FQDN)

*The FQDN will be cast into lowercase. The FQDN needs to be unique (case-insensitive).*

Start pairing

| Hostname (FQDN) | Infos | VPN | Last rule update (UTC) | Version | | |
|---|---|---|---|---|---|---|
| gcap-int-129-dag.gatewatcher.com | Details | ▶ Online | 2022-10-17T14:09:16Z | 2.5.3.105-3440~devel-35a26b6f | Pair again | Delete |

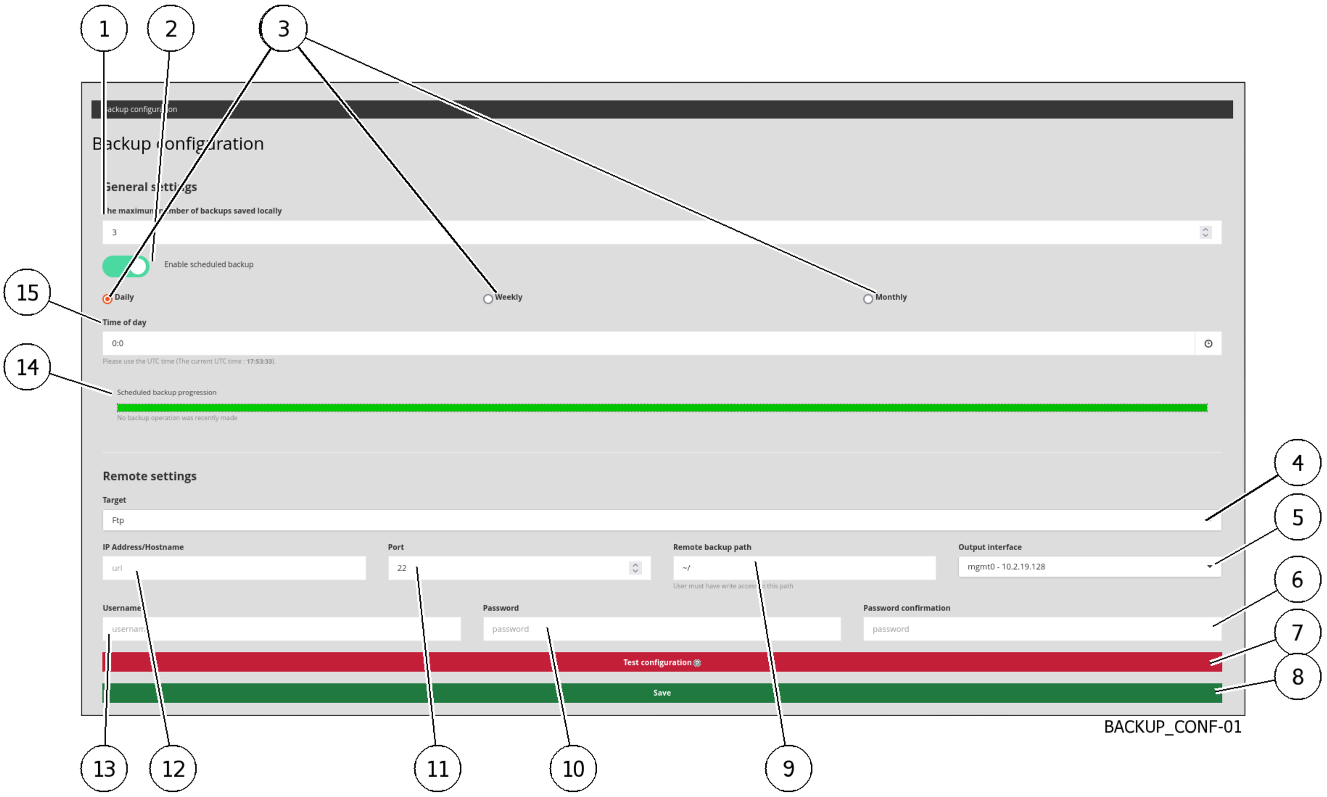
| Item | Name | | Function |
|---|---|---|---|
| 15 | GCenter information area: this includes | | |
| 1 | | • `GCenter's Fully Qualified Domain Name` field | Display of the FQDN of the GCenter |
| 2 | | • `GCenter'SSH fingerprint` field | Displays the fingerprint of the GCenter useful during the pairing procedure |
| 14 | `Pairing a new object` area: this includes | | |
| 3 | | • the `Fully Qualified Domain Name (FQDN)` field | Enter the FQDN of the GCap to be paired |
| 4 | | • the `Start pairing` button | Starts the GCap pairing |
| 13 | Paired GCap List Area: this includes | | |
| 5 | | The information of each paired GCap; This information consists of: | There are as many lines as there are GCaps paired |
| 6 | | • the `Delete` button | Deletes the GCap |
| 7 | | • the `Pair again` button | Re-pairs the selected GCap. The existing data is not lost. |
| 8 | | • the `Version` field | Indicates the GCap version |
| 9 | | • the `Last rule update (UTC)` field | Indicates the date and time of the last update of the ruleset |
| 10 | | • the `VPN` field | Indicates the status of the VPN connection between the GCenter and the GCap |
| 11 | | • the `Infos` field | Displays detailed information on System stats, Network stats, Sigflow stats, and Protocol flows |
| 12 | | • the `Hostname` field | Indicates the FQDN of the selected GCap |

**Note:**

During a deletion, the GCap continues to send its events until the VPN tunnel is taken down - timeout of the connection between the GCap and the GCenter.

### 5.6.20 `Admin-Backup/Restore - Configuration` screen of the legacy web UI

After pressing the `Configuration` command from the `Admin-Backup/Restore` menu, the following screen is displayed.
This screen enables configuring the frequency and location of backups.



Backup configuration

Backup configuration

General settings

The maximum number of backups saved locally: 3

Enable scheduled backup

● Daily ○ Weekly ○ Monthly

Time of day: 0:0

Please use the UTC time (The current UTC time : **17:53:33**).

Scheduled backup progression

No backup operation was recently made

Remote settings

Target: Ftp

IP Address/Hostname: url

Port: 22

Remote backup path: ~/

User must have write access to this path

Output interface: mgmt0 - 10.2.19.128

Username: username

Password: password

Password confirmation: password

BACKUP_CONF-01

The `Backup configuration` screen contains the following sections:

| Item | Name | Function |
|---|---|---|
| 1 | `maximum number of backups saved locally` | Maximum number of local backups |
| 2 | `Enable scheduled backup` selector | Activation of the backup scheduler. Displays the area below. |
| 3 | `Daily`, `Weekly`, `Monthly` buttons | Choice of the backup frequency |
| 4 | `Target` field | Choosing the backup location: `local`, `Scp`, `Ftp`<br>Selecting Scp and Ftp will bring up additional parameters listed below |
| 14 | `Scheduled backup progression` field | Backup progress bar |
| 15 | `Time of day` field | Choosing the time of the backup |

**Note:**

The time displayed under the `Time of day` field corresponds to the UTC time of the user's browser.

#### 5.6.20.1 `FTP` choice settings

The `Remote settings` section in the `FTP` version contains the following items:

| Item | Name | Function |
|---|---|---|
| 5 | `Output interface` field | Name of the network interface used of the GCenter, including IP address |
| 6 | `Password confirmation` field | 2nd entry of the confirmation password: must be identical to the mark (10) |
| 7 | `Test configuration` button | Button triggers verifying the entered parameters and sending a test file to the specified directory. The possible actions listed below depend on the context\| |
| 8 | `Save` button | Validation of the information entered |
| 9 | `Remote backup path` field | Path of the backup on the remote server. The user account used should have read and write permissions on this path. |
| 10 | `Password` field | Entering the user's password of the remote server |
| 11 | `Port` field | Entering the server's listening port of the remote server |
| 12 | `IP Address/ Hostname` field | Entry of the IP address or FQDN of the remote server (Example: _72.14.192.0) |
| 13 | `Username` field | Entering the user name of the remote server |

#### 5.6.20.2 `SCP` choice settings

The `Remote settings` section in the `SCP` version contains the following items:

| Name | Function |
|---|---|
| `IP Address/ Hostname` field | Entry of the IP address or FQDN of the remote server (Example: _72.14.192.0) |
| `Port` field | Entering the server's listening port |
| `Remote backup path` field | Path of the backup on the remote server. The user account used should have read and write permissions on this path. |
| `Output interface` field | Name of the network interface used, including IP address |
| `Protocols` field | Remote server authentication mode (choice between `Password` or `Public_key`) |
| `Username` field | Entering the user name of the remote server |
| `Password` field | Only displayed if the `Password` choice is active in the `Protocols` field. Entering the user's password |
| `Password confirmation` field | Only displayed if the `Password` choice is active in the `Protocols` field.<br>2nd entry of the confirmation password: must be identical to the mark (10) |
| `Backup host public key` field | Enter the Public Key of the backup host server |
| `Gcenter public key` field | GCenter public key |
| `Test configuration` button | Button triggers verifying the entered parameters and sending a test file to the specified directory of possible actions<br>The possible actions listed below depend on the context: |
| `Save` button | Choosing the time of the backup |

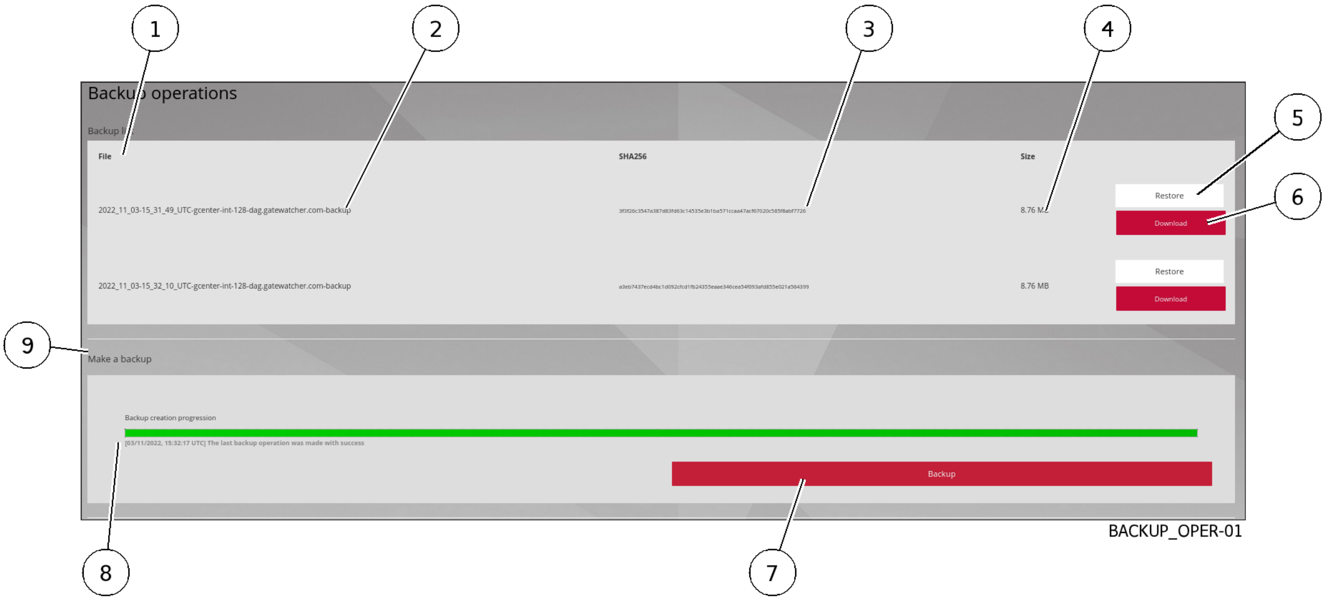
For more information, see the *Overview of the backup and restoration*.
For implementation, see the *Backup configuration* procedure.

---

### 5.6.21 `Admin-Backup/Restore - Operations` screen of the legacy web UI

After pressing the `Operations` command from the `Admin-Backup/Restore` menu, the following screen is displayed.
This screen enables:

- Manually performing a backup
- Manually restoring from a backup file located on the GCenter or on a remote PC
- Visualizing the correct operation of the backup schedule



Backup operations

Backup list

| File | SHA256 | Size | |
|---|---|---|---|
| 2022_11_03-15_31_49_UTC-gcenter-int-128-dag.gatewatcher.com-backup | 3f3f26c3547a387d83fd63c14535e3b1ba571ccaa47acf67020c585f8abf7726 | 8.76 MB | Restore<br>Download |
| 2022_11_03-15_32_10_UTC-gcenter-int-128-dag.gatewatcher.com-backup | a3eb7437ecd4bc1d092cfcd1fb24355eaae346cea54f093afd855e021a564399 | 8.76 MB | Restore<br>Download |

Make a backup

Backup creation progression

[03/11/2022, 15:32:17 UTC] The last backup operation was made with success

The `Backup operations` screen contains the following sections:

- *`Backup list` section*
- *`Make a backup` section*
- *`Restore operations` section*
- *`Scheduled backup` section*

For more information, see the *Overview of the backup and restoration*.
To perform a backup, see the procedure *Backup*.
To perform a restoration, see the procedure *Restoration*.

---

#### 5.6.21.1 `Backup list` section

The `Backup list` screen contains the following sections:

| Item | Name | Function |
|---|---|---|
| 1 | `File` field | List of backup files. Each file has the following properties.<br>• Name of the file (2) consisting of 'timesatamp-NomDuGCENTER.local-backup.gwc'<br>• Shasum `SHA256` (3) consisting of 'timesatamp-NomDuGCENTER.local-backup.gwc'<br>• `Size` (4) |
| 5 | `Restore` button | Enables file restoration. Beware, the restoration starts immediately! |
| 6 | `Download` button | Downloads the backup file to the remote PC's download directory |

---

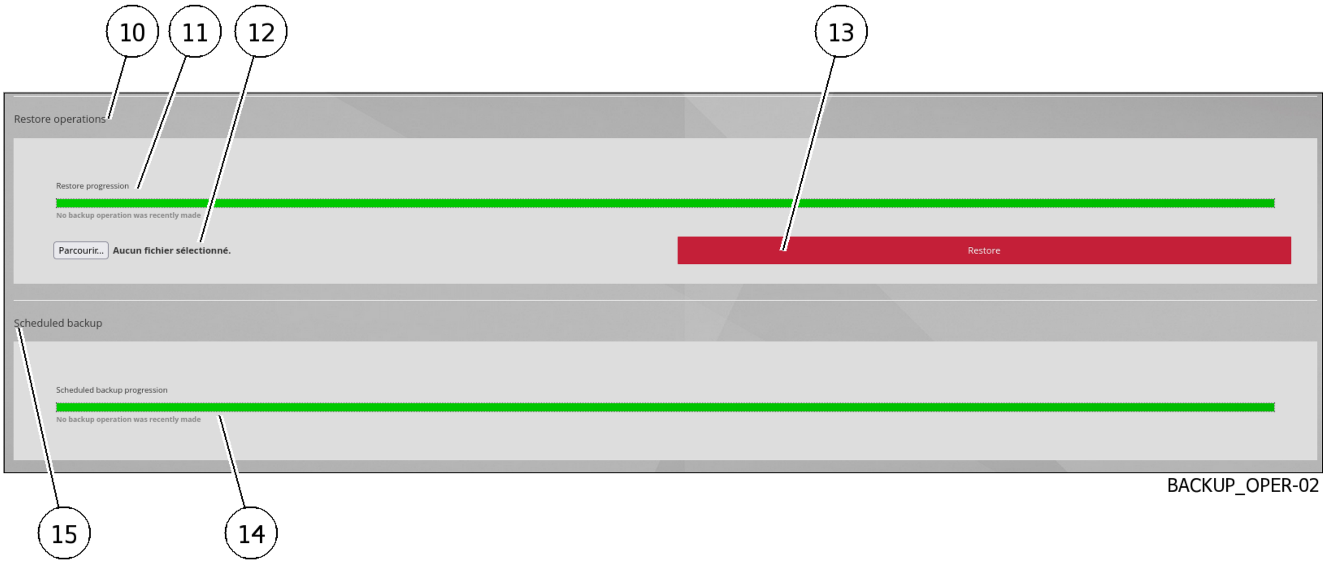
#### 5.6.21.2 `Make a backup` section

The `Make a backup` screen (9) contains the following sections:

| Item | Name | Function |
|---|---|---|
| 7 | `Backup` button | Enables either local or local and remote backup depending on the configuration.<br>• Name of the file (2) consisting of 'timesatamp-NomDuGCENTER.local-backup.gwc'<br>• Shasum `SHA256` (3) consisting of 'timesatamp-NomDuGCENTER.local-backup.gwc'<br>• `Size` (4) |
| 8 | `Backup creation progression` | The progress bar shows the status of the backup.<br>At the end of the backup, a message is displayed indicating the result |
| 6 | `Download` button | Downloads the backup file to the remote PC's download directory |

---

#### 5.6.21.3 `Restore operations` section



No backup operation was recently made

No backup operation was recently made

BACKUP_OPER-02

The `Restore operations` screen (10) contains the following sections:

| Item | Name | Function |
|---|---|---|
| 11 | `Restore progression` | The progress bar shows the status of the restoration.<br>At the end of the backup, a message is displayed indicating the result |
| 12 | `Parcourir` button | Enables selecting a backup file on the remote PC |
| 13 | `Restore` button | Enables restoration from the selected file |

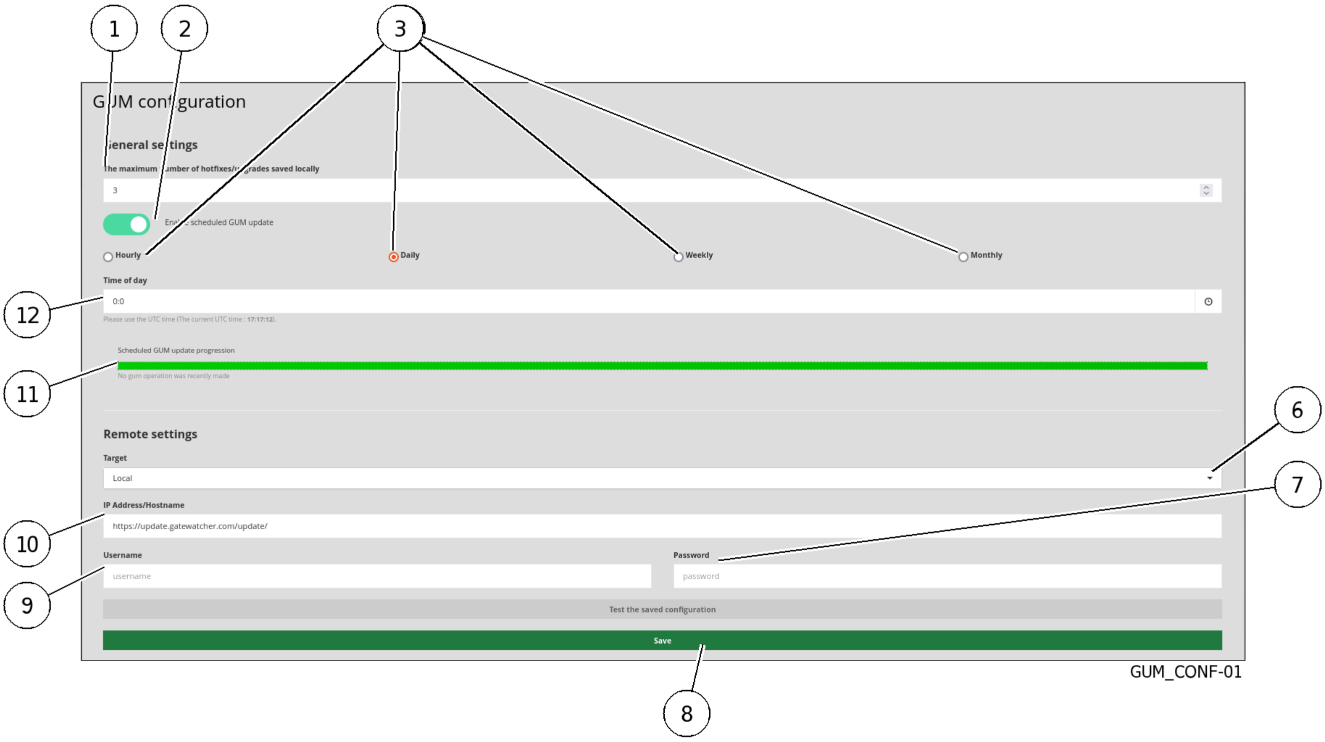
#### 5.6.21.4 `Scheduled backup` section

The `Scheduled backup` section (15) shows the status (14) of the scheduled backup:

- The progress bar shows the status of the restoration
- An information message about this status

### 5.6.22 `Admin- GUM - Config` screen of the legacy web UI

After pressing the `Config` command from the `GUM` menu, the following screen is displayed.
This screen enables configuring the automatic download of updates for the solution's engines.
It also enables configuring the frequency at which updates are triggered.



GUM configuration

General settings

The maximum number of hotfixes/upgrades saved locally

3

Enable scheduled GUM update

○ Hourly ● Daily ○ Weekly ○ Monthly

Time of day

0:0

Please use the UTC time (The current UTC time : **17:17:12**).

Scheduled GUM update progression

No gum operation was recently made

Remote settings

Target

Local

IP Address/Hostname

https://update.gatewatcher.com/update/

Username

username

Password

password

Test the saved configuration

Save

GUM_CONF-01

The `GUM configuration` screen contains the following sections:

- *`General settings` section*
- *`Remote settings` setting in `Local` version*
- *`Remote settings` section in `Online` version*

### 5.6.22.1 `General settings` section

The `General settings` section contains the following items:

| Item | Name | Function |
|---|---|---|
| 1 | `The maximum number of hotfixes/ upgrades saved locally` | Maximum number of hotfixes/upgrades stored locally |
| 2 | `Enable scheduled GUM update` selector | Activation of the backup scheduler. |
| 3 | `Daily`, `Weekly`, `Weekly`, `Monthly` buttons | Choice of the frequency for triggering updates. |
| 11 | `Scheduled GUM update progression` field | Update progress bar |
| 12 | `Time of day` field | Choice of update time |

**Note:**

The time displayed under the `Time of day` field corresponds to the UTC time of the user's browser.

#### 5.6.22.2 `Remote settings` setting in `Local` version

By selecting `Local` in parameter (6) `Target`, the `Remote settings` part contains the following:

| Item | Name | Function |
|---|---|---|
| 6 | `Target` field | Choosing the backup location: `local` |
| 7 | `Password` field | Entering the user's password |
| 8 | `Save` button | Validation of the information entered |
| 9 | `Username` field | Entering the user name |
| 10 | `IP Address/Hostname` field | Enter the IP address or FQDN of the local repository address. |

---

#### 5.6.22.3 `Remote settings` section in `Online` version

**Note:**

Le mode online est incompatible avec le mode LPM.

By selecting `Online` in parameter (6) `Target`, the `Remote settings` part contains the following:

| Item | Name | Function |
|---|---|---|
| 6 | `Target` field | Choosing the backup location: `Online` |
| 7 | `Password` field | Entering the password for the intelligence account |
| 8 | `Save` button | Validation of the information entered |
| 9 | `Username` field | Entering the user name of the intelligence account |
| 10 | `IP Address/Hostname` field | Automatically filled in |

In the case of `online` mode, an intelligence account will be required for the update package to be downloaded from the site.
This user and password combination must be entered in the `Username` and `Password` fields below the address.
The URL field will be automatically filled in when selecting the `Online` mode. Update packages are retrieved from Gatewatcher servers https://update.GATEWATCHER.com/update/.
The GCenter also provides the possibility to configure a proxy server to reach this repository.
This option can be configured in the `Proxy Settings` section.

See the *Configuring automatic update via GUM* procedure.

---

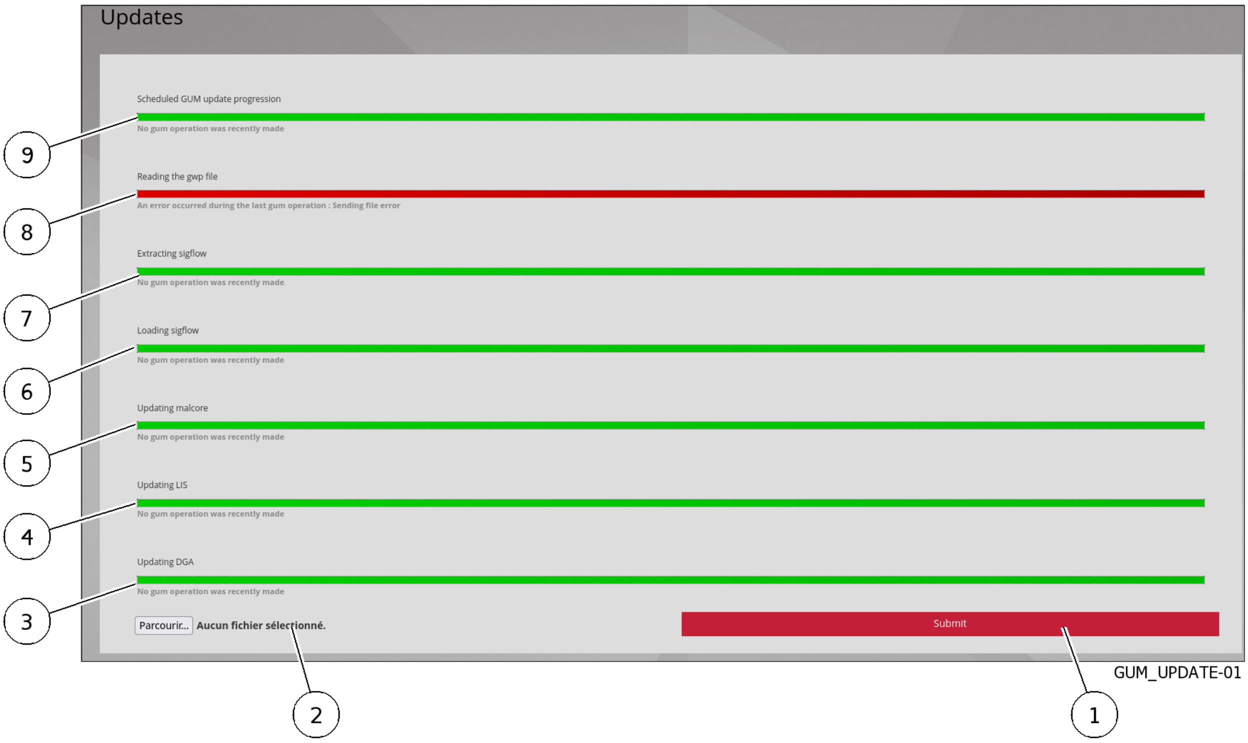
### 5.6.23 `Admin-GUM- Threat DB update` screen of the legacy web UI

After pressing the `Threat DB update` command from the `Admin-GUM` menu, the following screen is displayed. This screen enables viewing the history and status of the installation:

- For rule packages downloaded in a scheduled manner
- For manually downloaded rule packages

Packages that can be downloaded via this interface are the:

- malcore package: this package contains only engine and antivirus database updates used by Malcore
- dga package: this package contains updates to the gdgadetect engine
- cti package: this package contains CTI engine updates
- sigflow package: this package contains only Sigflow engine and rule base updates
- full package (full): this package is the sum of the previous packages



Scheduled GUM update progression

No gum operation was recently made

Reading the gwp file

An error occurred during the last gum operation : Sending file error

Extracting sigflow

No gum operation was recently made

Loading sigflow

No gum operation was recently made

Updating malcore

No gum operation was recently made

Updating LIS

No gum operation was recently made

Updating DGA

No gum operation was recently made

**Note:**

The cti.gwp package is updated hourly on update.gatewatcher.com The other packages dga.gwp, malcore.gwp, sigflow.gwp sont updated every day. It is not possible to download the full.gwp file in automatic mode

The `Threat DB update` screen contains the following items:

| Item | Name | Function |
|---|---|---|
| 1 | `Submit` button | Triggers the installation of the update package |
| 2 | `Parcourir` button | Enables selecting an update package |
| 3 | `Updating DGA` field | DGA engine update progress bar / Last update status |
| 4 | `Updating LIS` field | CTI update progress bar / Last update status |
| 5 | `Updating malcor` field | Malcore engine update progress bar / Last update status |
| 6 | `Loading sigflow` field | Progress bar for the loading of the Sigflow engine rule files / Status of the last update |
| 7 | `Extracting sigflow` field | Progress bar of the extraction of rules files from the Sigflow engine |
| 8 | `Reading the gwp file` field | Progress bar of the integrity check of a loaded package |
| 9 | `Scheduled GUM threat DB update progression` field | Update progress bar: this covers all the steps detailed in the other fields |

In the event of a scheduled update of a package file containing all the rules of a single engine or all the engines:

- The progress bar in the `Scheduled GUM threat DB update progression` field starts advancing:
- The progress bar in the `Reading the gwp file` field starts to advance. This means that the file has been downloaded and the system is checking its integrity
- The progress bars of the `Loading sigflow` and `Extracting sigflow` fields begin their respective progressions. This corresponds to the processing of rule files in the Sigflow engine
- The progress bar in the `Updating malcore` field begins to progress. This corresponds to the processing of the Malcore engine rule files
- The progress bar for the `Upgrading LIS` field begins to progress. This corresponds to the processing of the CTI engine rule files
- The progress bar in the `Updating DGA` field begins to move. This corresponds to the processing of the DGA engine rule files
- Once the various steps are complete, the progress bar in the `Scheduled GUM threat DB update progression` field finishes its progression and indicates the final processing status

To use a package file from the remote PC, use the `Parcourir` button (2).

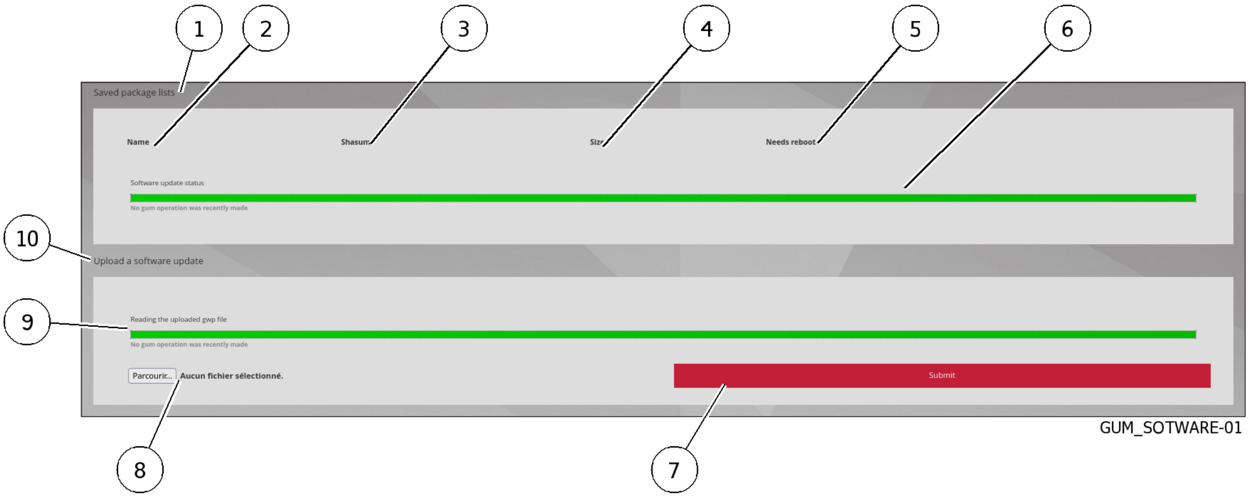
**Important:**

In this case, select a GWP package file, only from those of the solution's engines.
Hotfix and upgrade packages will not work in this interface.

The engine rule update packages are available https://update.gatewatcher.com/update/.
For manual installation, see the *Manual installation of an update of signatures and/or anti-viral engines (update)*.

### 5.6.24 `Admin-GUM- Software update` screen of the legacy web UI

After pressing the `Software update` command from the `Admin-GUM` menu, the following screen is displayed.



No gum operation was recently made

No gum operation was recently made

Aucun fichier sélectionné.

GUM_SOTWARE-01

The `Software update` screen contains the following items:

| Item | Name | Function |
|---|---|---|
| 1 | `Saved package lists` area | Software package history |
| 2 | `Name` field | Name of the software package |
| 3 | `Shasum` field | Shasum sha256 of the file |
| 4 | `Size` field | File size |
| 5 | `Needs reboot` field | Restart required |
| 6 | `Software update status` field | Progress bar of the application of a hotfix or an upgrade / Status of the last application |
| 7 | `Submit` button | Triggers the package installation |
| 8 | `Parcourir` button | Enables selecting a package |
| 9 | `Reading the uploaded gwp file` field | Progress bar of the package integrity check / Status of the last check |
| 10 | `Upload a software update` area | Area enabling manual package installation |

To use a software package file from the remote PC, use the `Parcourir` button (8).

**Important:**

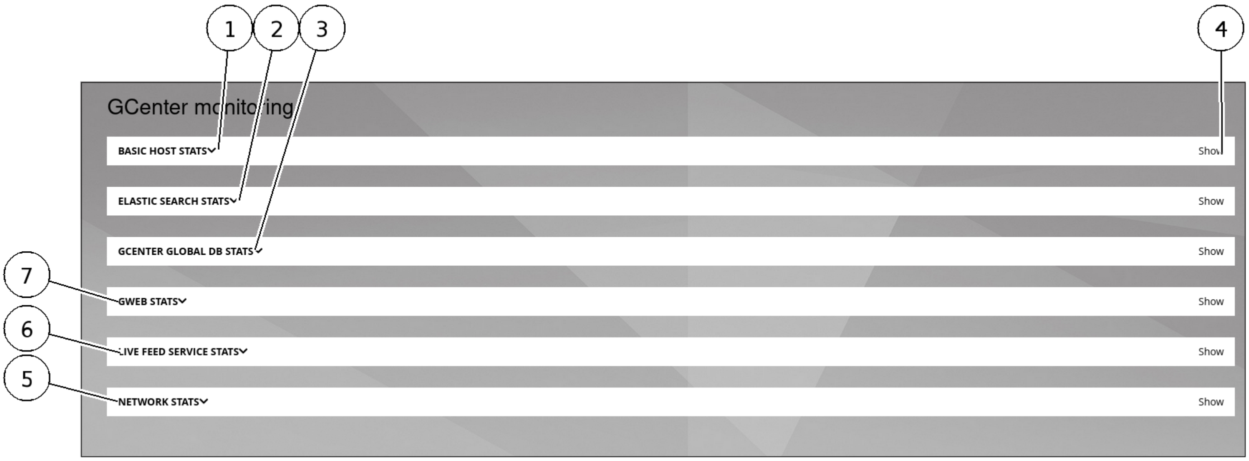
In this case, a GWP package file must be selected and only those of the hotfix and upgrade type. Update type packages will not work in this interface.

Software update packages are available at https://update.gatewatcher.com/update/.

### 5.6.25 `Admin-GCenter- Monitor` screen of the legacy web UI

From this section, solution administrators can view real-time information about the GCenter.
This interface is used to monitor the GCenter for CPU, memory, network, and disk load via dynamic dashboards.

After pressing the `Monitor` command from the `Admin-GCenter` menu, the following screen is displayed.
This screen enables:



MONITOR-01

The GATEWATCHER administrator can access information on the monitored services to ensure they are functioning properly:

| Item | Description |
|---|---|
| 1 | *`Basic host stats` section* for real-time information from the GCenter |
| 2 | *`ELASTIC SEARCH STATS` section* for ElasticSearch cluster status information |
| 3 | *`GCENTER GLOBAL DB STATS` section* for global database information |
| 4 | Show / Hide button to expand / collapse the hidden area |
| 5 | *`NETWORK STATS` section* for network interface bandwidth information |
| 6 | *`LIVE FEED SERVICE STATS` section* for information on all GCenter services |
| 7 | *`GWEB STATS` section* for information on the Nginx Web server |

#### 5.6.25.1 General presentation and navigation agreement

`Basic host stats` section appears by default. The other sections are visible by clicking on the section name or the `Show` button.

It is possible to hover over the charts to view the measured values.
On charts with several plotted values, it is also possible to choose which element will be plotted by clicking on the legend to show or hide them.
In addition, depending on the position of the mouse cursor on any chart, the position on the other charts is also synchronised.
This enables you to access all the necessary information at a given time **T**.
The double arrow to the **left** enables moving on the graph to the left. This can be done by sliding the mouse to the right.
The double arrow to the **right** enables moving on the graph to the right. This can be done by sliding the mouse to the left.

The **Play** button enables all graphics to be reset to their default auto-refresh status. The administrator can also double-click on the content of the chart with his mouse.

The + **and -** buttons offer the possibility to zoom into the graph or press Shift and select the graph area to zoom in. Zooming is also possible by pressing Shift or Ctrl with the mouse wheel.

The double arrows **up/down** enable the administrator to drag with their mouse to use this setting to change the graph vertically. It is possible to double-click to reset between two statuses, the default chart and the one that corresponds to all values.

---

#### 5.6.25.2 `` `Basic host stats` `` section

The BASIC HOST STATS section provides real-time information from the GCenter with global system indicators such as:

- `` `CPU usage` `` average
- `` `Global Load` ``
- `` `RAM Usage` ``
- `` `Swap Usage` ``
- disk statistics including used, free, and reserved capacity for different directories are also monitored:

- `` `Disk R/W Usage` ``
- `` `Disk Global Usage` ``
- `` `Disk Global Usage` ``
- `` `Disk Usage:  /es` ``
- `` `Disk Usage:  /backups` ``
- `` `Disk Usage:  /var/log` ``

---

#### 5.6.25.3 `` `ELASTIC SEARCH STATS` `` section

`` `ELASTIC SEARCH STATS` `` section provides information on the status of the ElasticSearch cluster. This is responsible for recording and then indexing the data captured by the GCap probe in the GCENTER.

The cluster bandwidth is monitored.

---

#### 5.6.25.4 `` `GCENTER GLOBAL DB STATS` `` section

This `` `GCENTER GLOBAL DB STATS` `` section provides information on what the GCenter's global database is consuming by way of counters:

- `` `Gcenter Global DB Transactions` ``
- `` `Gcenter Global DB Reads` ``
- `` `Gcenter Global DB Writes` ``
- `` `Gcenter Global DB Size` ``

---

#### 5.6.25.5 `GWEB STATS` section

This `GWEB STATS` section provides information about the GCenter's Nginx web server with the counters:

- `GWeb Active Connections`
- `GWeb Connections Rate Accepted`
- `GWeb Connections Rate Handled`
- `GWeb Requests`

---

#### 5.6.25.6 `LIVE FEED SERVICE STATS` section

This `LIVE FEED SERVICE STATS` section offers information about all services of the GCenter according to the counters:

- `Live Feed Operations`
- `Live Feed Commands`
- `Live Feed Allowed Hits`
- `Live Feed Memory Consumption`
- `Live Feed Memory LUA Consumption`
- `Live Feed Allowed Client Count`

---

#### 5.6.25.7 `NETWORK STATS` section

This `NETWORK STATS` section provides information about the bandwidth (`Interface Bandwidth for mgmt0`) of the GCenter's mgmt0 network interface.

---

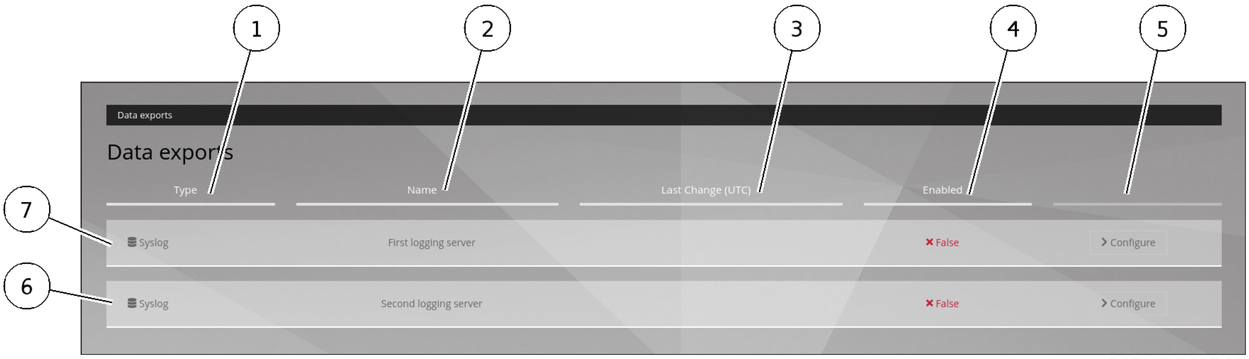
### 5.6.26 `Admin-GCenter- Data exports` screen of the legacy web UI

#### 5.6.26.1 Introduction

It is possible to export events from the GCenter to remote servers such as a SIEM by using the syslog protocol.

The number of Syslog servers is limited to two.

After pressing the `Data Exports` command in the `Admin-GCenter` menu, the following screen allows you to manage up to two log exports to two different destinations.



Data exports

| Type | Name | Last Change (UTC) | Enabled | |
|---|---|---|---|---|
| Syslog | First logging server | | ✗ False | > Configure |
| Syslog | Second logging server | | ✗ False | > Configure |

DATA_EXPORT-01

The `Data exports` screen contains the following sections:

| Item | Name | |
|---|---|---|
| 7 | 1st type of export. The information available for this export is as follows: | |
| 1 | | - `Type` field: type of export |
| 2 | | - `ame` field: here, the first logging server |
| 3 | | - `Last Change (UTC)` field: date of last saved change |
| 4 | | - `Enabled` field: export status . here `False` because not performed |
| 5 | | - `Configure` button: displays the configuration window. See below for details. |
| 6 | 2nd type of export. The information available for this export is as follows: | |
| 1 | | - `Type` field: type of export |
| 2 | | - `ame` field: here, the second logging server |
| 3 | | - `Last Change (UTC)` field: date of last saved change |
| 4 | | - `Enabled` field: export status . here `false` because not performed |
| 5 | | - `Configure` button: displays the configuration window. See below for details. |

#### 5.6.26.2 Setting up the connection

Connection to a server using syslog must be configured; this configuration is described in *General settings*.
The data to be exported can be:

- Alerts or
- Alerts and metadata

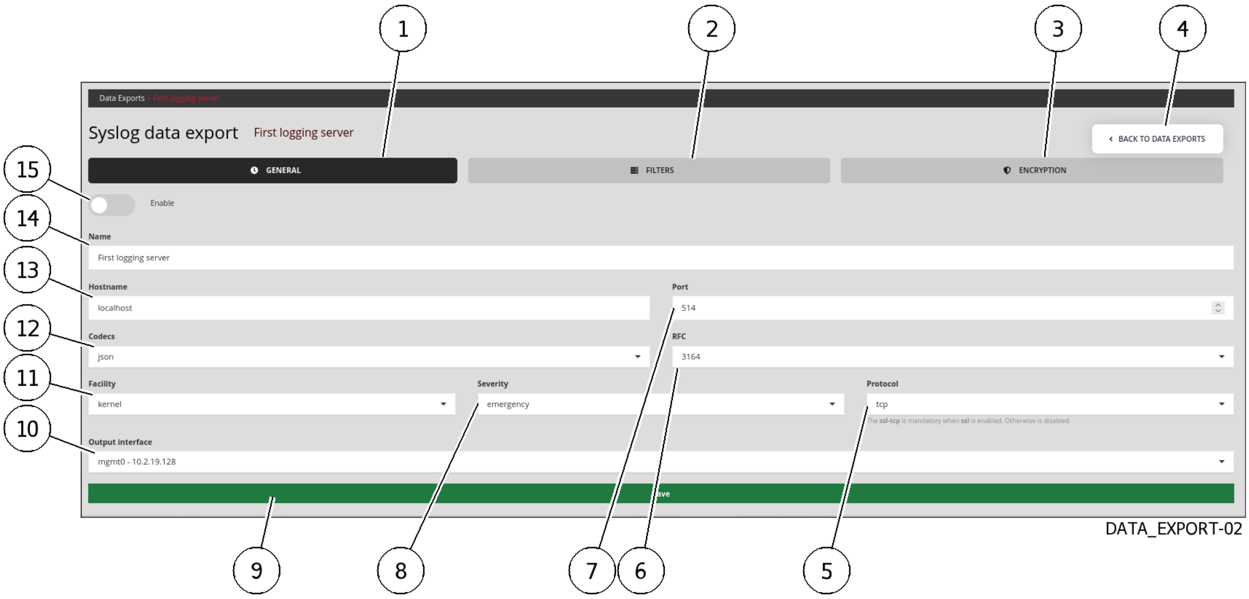
This data can be defined in the *General settings* screen.

**Note:**

No GCenter or GCap system log is affected by this export.

The communication can be encrypted: this setting is described in the screen *Encryption*.
For details on data management, see *Data use*.
For implementation, see the *Export data to a SIEM via the syslog protocol*.

### 5.6.26.3 General settings



Data Exports > First logging server

Syslog data export First logging server

Enable

Name: First logging server

Hostname: localhost

Port: 514

Codecs: json

RFC: 3164

Facility: kernel

Severity: emergency

Protocol: tcp

The **ssl-tcp** is mandatory when **ssl** is enabled. Otherwise is disabled.

Output interface: mgmt0 - 10.2.19.128

DATA_EXPORT-02

The `Data exports - GENERAL` screen contains the following sections:

| Item | Name | |
|---|---|---|
| 1 | The `GENERAL` button for general log export settings. This button displays the following settings. | |
| 15 | | - `Enabled` field: enables or disables Syslog export. |
| 14 | | - `ame` field: name of the remote server assigned by the administrator (Example: _First logging server). |
| 13 | | - `Hostname` field: IP address or name of the remote server (Example: localhost or 192.168.199.1). |
| 7 | | - `Port` field: listening port of the remote server. The default value is 514. |
| 12 | | - `Codecs` field: codec used for the output data.<br>Output codecs are a convenient way to encode the data prior to export without the need for another filter.<br>By default the value is in json. (Example: _json or _idmef) |
| 6 | | - `RFC` field: enables selecting the corresponding RFC for the desired message normalisation.<br>(Example: _3164 or _5424) |
| 11 | | - `Facility` field: message type used for sending to the Syslog server.<br>The default value is a *kernel*.<br>(Example : kernel, user-level, mail, daemon, security/authorization, syslog, line printer, network news, uucp) |
| 8 | | - `Severity` field: severity rate for Syslog messages. The default value is an emergency<br>The list of choices is shown in the table **List of Facility field choices**. |
| 5 | | - `Protocol` field: protocol used for data transfer<br>The default value is in TCP. (Example: tcp, udp ou ssl_tcp) |
| 10 | | - `Output interface` field: selected output interface between the **GCenter** and the remote SIEM server<br>(Example: mgmt0, sup0) |
| 2 | `FILTERS` button for filtering the data to be exported. For details of the parameters, see *Filtering Parameters* | |
| 3 | `ENCRYPTYON` button for encrypting the connection between the GCenter and the remote server For details of the parameters, see *Encryption* | |
| 4 | Button to return to the `DATA EXPORTS` screen | |
| 9 | `Save` button. The changes will only take effect after this button is pressed. | |

| Name | Description |
|---|---|
| Emergency | The system is unusable |
| Alert | Action must be taken immediately |
| Critical | Conditions are severe. |
| Error | Failure conditions |
| Warning | Conditions of caution |
| Notice | Normal but significant condition |
| Informational | Explanatory messages |
| Debug | Repair level messages |

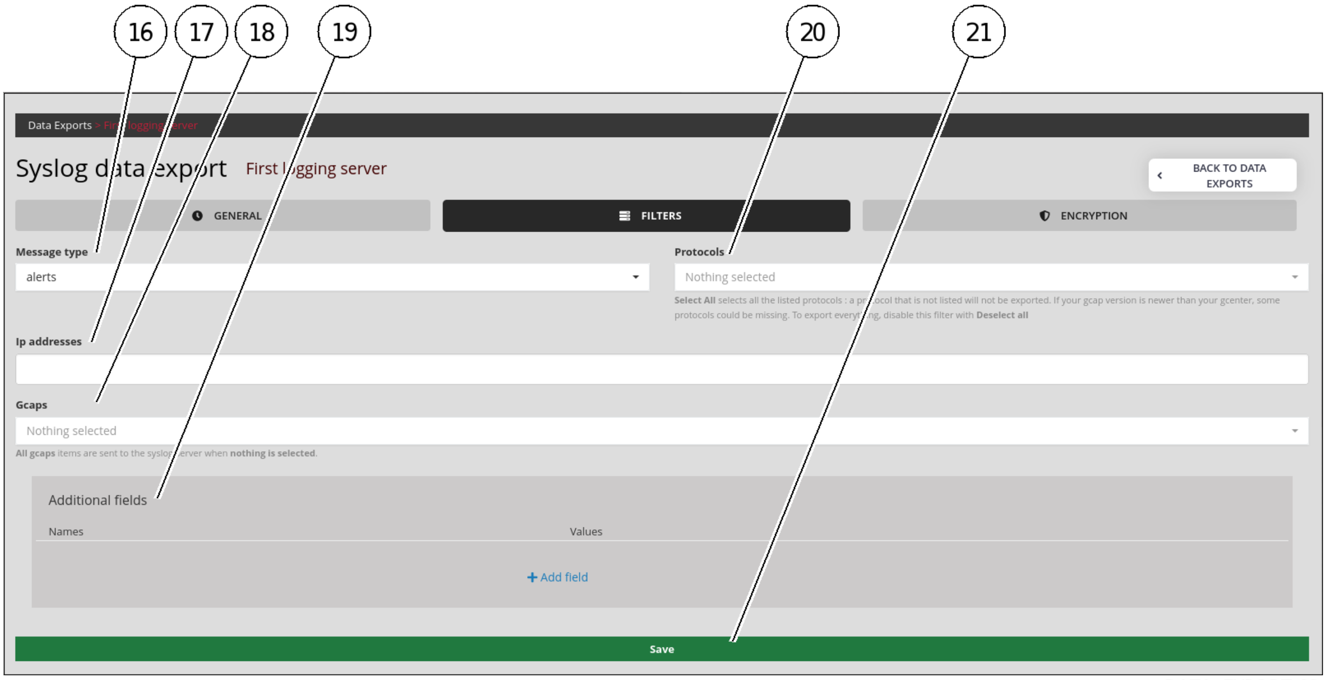
**Note:**

SSL-TCP is mandatory if SSL encryption is enabled. Otherwise, it is disabled.

---

#### 5.6.26.4 Filtering Parameters

The `Data exports - FILTERS` screen contains the following parts:



Syslog data export First logging server

Message type: alerts

Protocols: Nothing selected

**Select All** selects all the listed protocols : a protocol that is not listed will not be exported. If your gcap version is newer than your gcenter, some protocols could be missing. To export everything, disable this filter with **Deselect all**

Ip addresses

Gcaps: Nothing selected

**All gcaps** items are sent to the syslog server when **nothing is selected**.

Additional fields

| Names | Values |
|---|---|

+ Add field

DATA_EXPORT-03

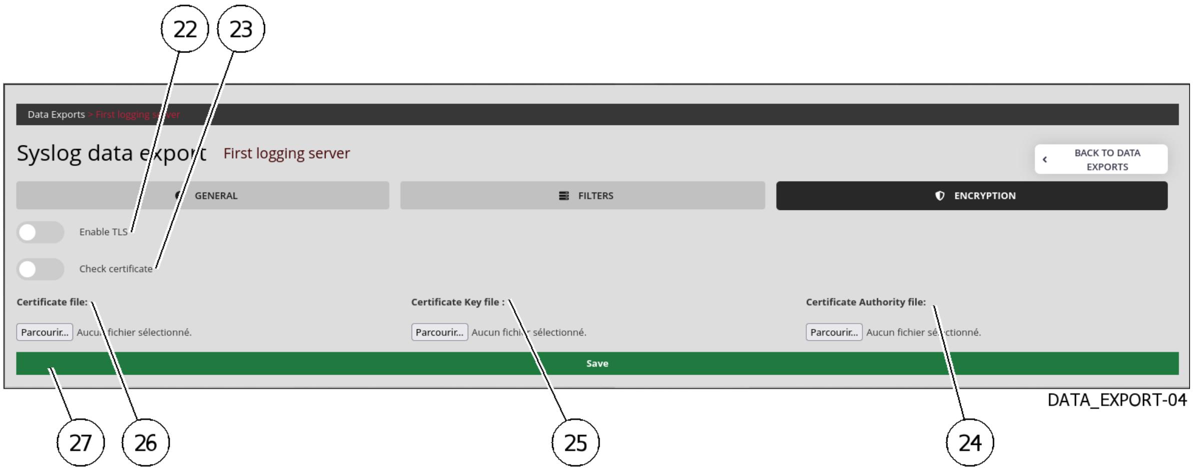
| Item | Parameter | Description |
|---|---|---|
| 16 | `Message type` | Defines the type of event to send to the remote server. Either alerts only, or alerts and metadata. (Example: alerts, all) |
| 17 | `Ip addresses` | Filter by **IP** or **network**. By default, all data is sent to the remote server if the field is empty. |
| 18 | `Gcaps` | Filter by **Gcap**. By default, all data from the GCap paired to the GCenter is sent to the remote server if nothing is selected. (Example: GCap1, GCap2) |
| 19 | `Additional fields` | Adds additional fields to the exported events.<br>A name (`Name`) and a description (`Values`) can be entered in this window.<br>When using the idmef codec, this field is not supported. |
| 20 | `Protocols` | Selects the protocols to be exported.<br>(Example : dcerpc, dhcp, dnp3, dns, enip, ftp, http, http2, ikev2, krb5, mqtt, modbus, netflow, nfs, ntp, rdp, rfb, sip, smb, smtp, ssh, tftp et tls) |
| 21 | `Save` | The changes are only effective after pressing `Save` |

**Note:**

`Select All` selects all listed protocols: a protocol that is not selected will not be exported.
If the GCap version is newer than that of the GCenter, some protocols may be missing.
To export everything, deactivate this filter with `Deselect all`.

### 5.6.26.5 Encryption

This section enables encrypting exchanges between the GCenter and the remote server.
It is necessary to add a certificate, the associated key, and the certification authority in order to activate this functionality.
The `Data exports - ENCRYPTYON` screen contains the following sections:

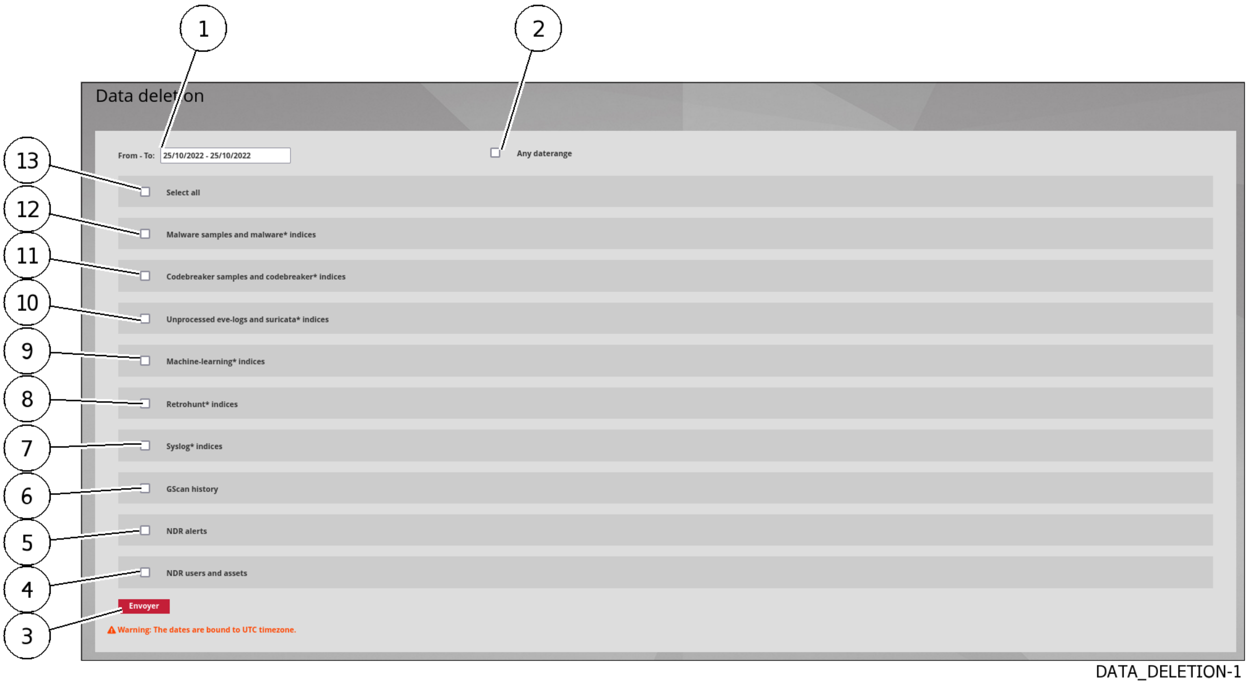

22
23
Data Exports > First logging server
Syslog data export
First logging server
BACK TO DATA EXPORTS
GENERAL
FILTERS
ENCRYPTION
Enable TLS
Check certificate
Certificate file:
Parcourir... Aucun fichier sélectionné.
Certificate Key file :
Parcourir... Aucun fichier sélectionné.
Certificate Authority file:
Parcourir... Aucun fichier sélectionné.
Save
27
26
25
24

DATA_EXPORT-04

| Item | Parameter | Description |
|---|---|---|
| 22 | `` `Enable TLS` `` | Enables the TLS service (Transport Layer Security). Disabled by default. |
| 23 | `` `Check certificate` `` | Checks the validity of the certificate when the TLS service is enabled. Disabled by default. |
| 24 | `` `Certificate file` `` | Adds a certificate |
| 25 | `` `Certificate Key file` `` | Adds the related key |
| 26 | `` `Certificate Authority file` `` | Adds the file for the certification authority. |
| 27 | `` `Save` `` | The changes are only effective after pressing `` `Save` `` |

### 5.6.27 `` `Admin-GCenter- Data Management` `` screen of the legacy web UI

After pressing the `` `Data Management` `` command of the `` `Admin-GCenter` `` menu, the `` `Data Management` `` window displays a single choice, `` `Data deletion` ``.
This screen enables deleting all or part of the data on the GCenter using the `` `Data Management` `` menu.



From - To: 25/10/2022 - 25/10/2022

☐ Any daterange

☐ Select all

☐ Malware samples and malware* indices

☐ Codebreaker samples and codebreaker* indices

☐ Unprocessed eve-logs and suricata* indices

☐ Machine-learning* indices

☐ Retrohunt* indices

☐ Syslog* indices

☐ GScan history

☐ NDR alerts

☐ NDR users and assets

⚠ Warning: The dates are bound to UTC timezone.

DATA_DELETION-1

In this menu it is possible to choose the type of data to be permanently deleted from the GCenter.
The options enable:

- Choosing the time interval in which the deletion is to be carried out
- Choosing the type of data to be deleted

**Important:**

Data not yet processed will also be deleted.

The `Data deletion` screen contains the following sections:

| Item | Name | Description |
|---|---|---|
| 1 | `From to :` | Defines the time interval in which the deletion takes place |
| 2 | `Any datarange` | Selects the entire period in which the data is found. |
| 3 | `Send` | After ticking the desired box(es) over a period of time, validate the action by clicking on the `Send` button. |
| 4 | `NDR users and assets` | Types of data to be deleted |
| 5 | `NDR alerts` | |
| 6 | `GScan history` | |
| 7 | `Syslog* indices` | |
| 8 | `Retrohunt* indices` | |
| 9 | `Machine-learning* indices` | |
| 10 | `Unprocessed eve-logs and suricata* indices` | |
| 11 | `Codebreaker samples and codebreaker* indices` | |
| 12 | `Malware samples and malware* indices` | |
| 13 | `Select all` | Select all data types by ticking the `Select all` box directly. |

For implementation, refer to *Deleting data (log files)*.

### 5.6.28 `Admin-GCenter- ML Management` screen of the legacy web UI

See the presentation of *Machine Learning engine*.

After pressing `ML Management` command from the `Admin-GCenter` menu, the following `Machine Learning Management` screen is displayed.

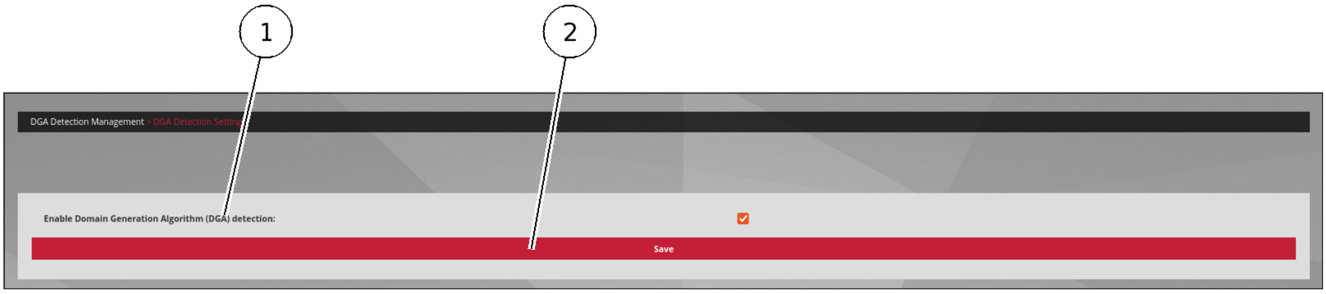
This screen contains a single category `DGA Detection Management`.

After pressing this button, the `Domain Name Generation (DGA) Detection Management` screen is displayed with the following sections:

| Section | Function |
|---|---|
| `Settings` | Enabling / disabling the Machine Learning engine (or DGA) |
| `White List` | White list management |
| `Black List` | Black list management |

#### 5.6.28.1 `Settings` section of the `DGA Detection Management` category

The `DGA Detection Settings` window displays the possibility of activating the engine.



Enable Domain Generation Algorithm (DGA) detection: ☑

ML_SETTING-01

This window consists of:

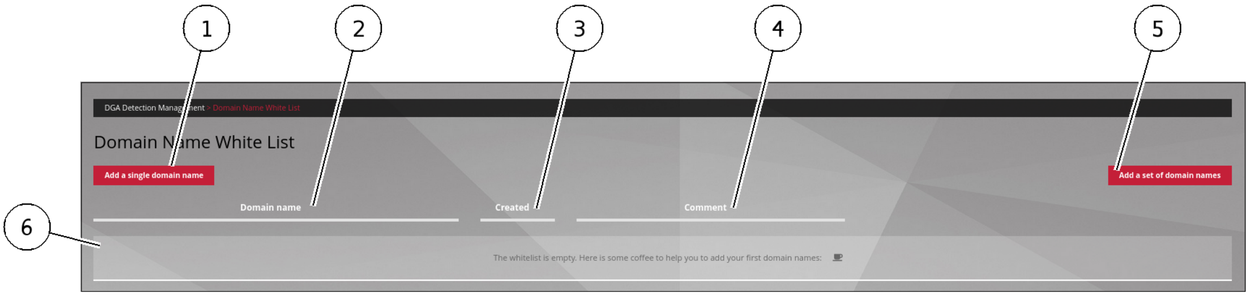
- Activating (1) the detection of the domain generation algorithm (DGA)
- The `Save` button (2) to record the enabling or disabling

For the implementation, see: *Enabling and configuring the Machine Learning engine*.

---

#### 5.6.28.2 `White List` section of the `DGA Detection Management` category

The `White List` window displays the **Machine Learning (or DGA)** engine settings.



The whitelist is empty. Here is some coffee to help you to add your first domain names: ☕

ML_SETTING-02

This window consists of:

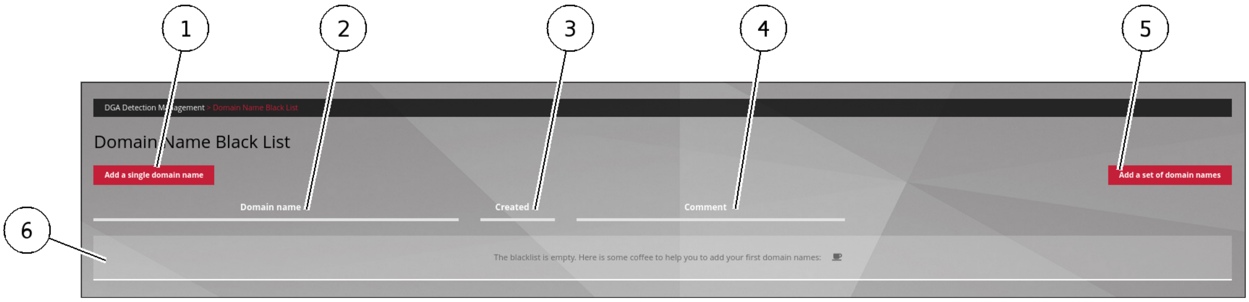
- Two buttons for adding items to the list:
  - One button `Add a single domain name` (1) to add a single item by manually entering the requested information
  - One button `Add a set domain names` (5) to add a set of items using a pre-filled .csv file
- Elements (6) that make up the list. For each element, the following items are displayed:
  - `Domain name` field (2): displays the domain name of the item in question
  - `Created` field (3): displays the creation date of the item in question
  - `Comment` field (4): displays an optional comment for the item in question
  - `Remove` button: deletion of the element in question

For the implementation, refer to *Managing the white and black lists of the Machine Learning engine*.

---

#### 5.6.28.3 `Black List` section of the `DGA Detection Management` category

The `Black List` window displays the **Machine Learning (or DGA)** engine settings.



The blacklist is empty. Here is some coffee to help you to add your first domain names: ☕

ML_SETTING-03

This window consists of:

- Two buttons for adding items to the list:
  - One button `Add a single domain name` (1) to add a single item by manually entering the requested information
  - One button `Add a set domain names` (5) to add a set of items using a pre-filled .csv file
- Elements (6) that make up the list. For each element, the following items are displayed:
  - `Domain name` field (2): displays the domain name of the item in question
  - `Created` field (3): displays the creation date of the item in question
  - `Comment` field (4): displays an optional comment for the item in question
  - `Remove` button: deletion of the element in question

For the implementation, refer to *Managing the white and black lists of the Machine Learning engine*.

---

### 5.6.29 `Admin-GCenter- Malcore Management` screen of the legacy web UI

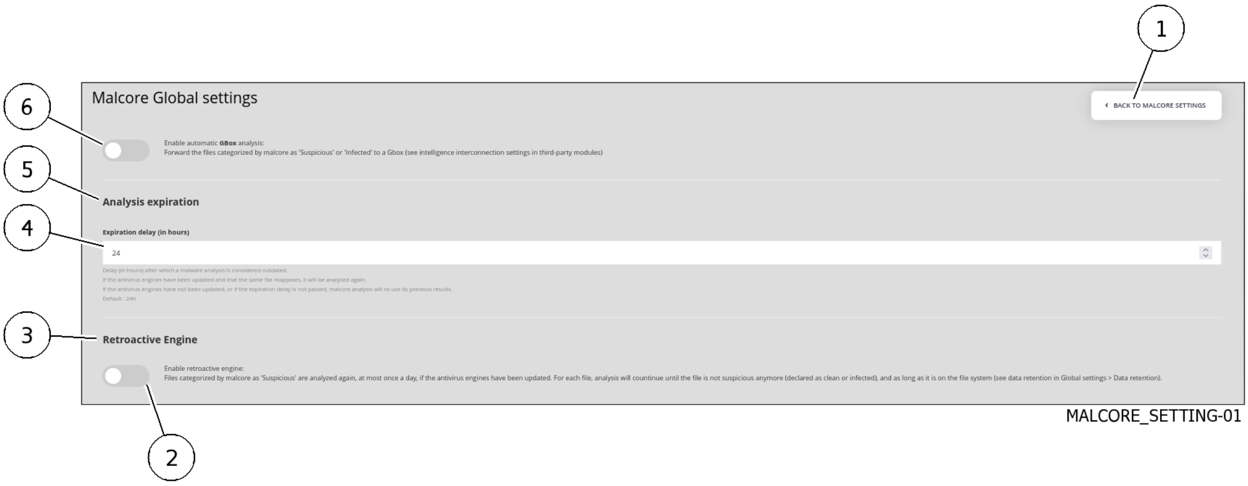
After pressing the `Malcore Management` command from the `Admin-GCenter` menu, the following screen is displayed.
The `Malcore Management` screen contains the following sections:

| Section | Function | Description |
|---|---|---|
| `Malcore Global settings` | Configuring the Malcore engine | Enabling GBox analysis and the Retroact engine |
| `White List` | List of valid hashes | Whitelist management: files that have their sha256 fingerprints in this file are considered safe. |
| `Black List` | List of infected hashes | Blacklist management: files that have their sha256 fingerprints in this file are considered infected. |

---

### 5.6.29.1 `Global settings` section of the `Malcore Management` submenu

The `Global settings` window displays the Malcore engine settings.



Malcore Global settings

BACK TO MALCORE SETTINGS

Enable automatic **GBox** analysis:
Forward the files categorized by malcore as 'Suspicious' or 'Infected' to a Gbox (see intelligence interconnection settings in third-party modules)

**Analysis expiration**

**Expiration delay (in hours)**

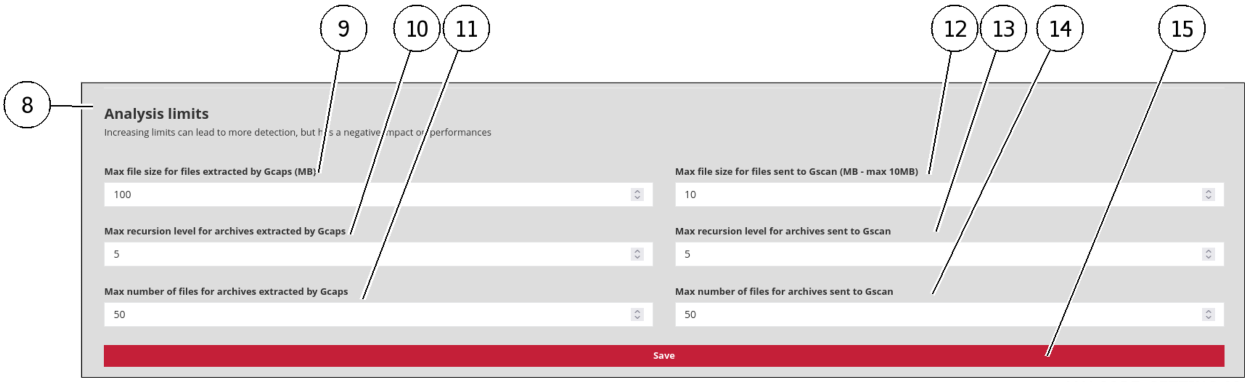
24

Delay (in hours) after which a malware analysis is considered outdated.
If the antivirus engines have been updated and that the same file reappears, it will be analysed again.
If the antivirus engines have not been updated, or if the expiration delay is not passed, malcore analysis will re-use its previous results.
Default : 24h

**Retroactive Engine**

Enable retroactive engine:
Files categorized by malcore as 'Suspicious' are analyzed again, at most once a day, if the antivirus engines have been updated. For each file, analysis will countinue until the file is not suspicious anymore (declared as clean or infected), and as long as it is on the file system (see data retention in Global settings > Data retention).

MALCORE_SETTING-01



**Analysis limits**

Increasing limits can lead to more detection, but has a negative impact on performances

**Max file size for files extracted by Gcaps (MB)**: 100

**Max file size for files sent to Gscan (MB - max 10MB)**: 10

**Max recursion level for archives extracted by Gcaps**: 5

**Max recursion level for archives sent to Gscan**: 5

**Max number of files for archives extracted by Gcaps**: 50

**Max number of files for archives sent to Gscan**: 50

MALCORE_SETTING-02

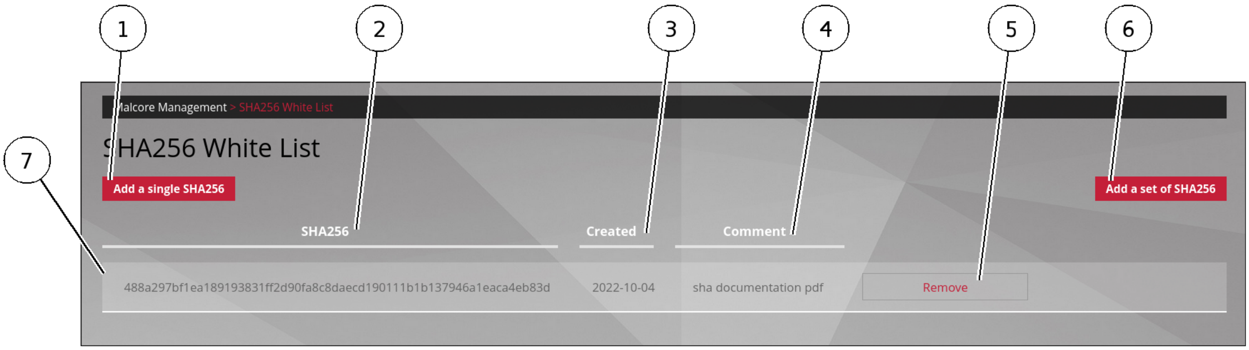
This window consists of:

- A parameter (6) to enable automatic analysis GBox c.a.d transfer files classified by Malcore as 'Suspect' or 'Infected' to a GBox
- Of a parameter (4) in the `Analysis expiration` area (5):
  This setting is the delay (in hours) after which a malware scan is considered outdated.
  If the antivirus engines have been updated and the same file reappears, it will be scanned again.
  If the antivirus engines have not been updated or the timeout has not passed, the Malcore scan will reuse its previous results.
  Default value: 24h
- Of a `Enable retroactive engine` field (2) of the zone (3)
  This selector activates the Retroact engine c.a.d files classified by Malcore as 'Suspect' are scanned again, at most once a day, when the antivirus engines are updated.
  For each file, the scan continues until the file is no longer suspicious (declared clean or infected) and as long as it is on the file system (see Data retention GCenter > Configuration > Global settings).
- A zone (8): analysis limits of the Malcore engine
- Field (9): maximum file size extracted by GCap (MB)
- Field (10): Maximum recursion level for archives extracted by GCap
- Field (11): Maximum number of files for archives extracted by GCap
- Field (12): Maximum size of files sent to GScan (MB)
- Field (13): Maximum recursion level for archives sent to GScan
- Field (14): Maximum number of archive files sent to GScan

For the implementation, refer to *Setting up GBox and the Malcore and Retroact engines and activate the GBox*.

#### 5.6.29.2 `White List` section of the `Malcore Management` submenu

The `White List` window displays the exception list called Whitelist which contains the list of SHA256 fingerprints of files that Malcore should consider healthy.
These files are declared healthy without analyzing them and defined using their SHA256 fingerprint.



SHA256 White List

| SHA256 | Created | Comment | |
|---|---|---|---|
| 488a297bf1ea189193831ff2d90fa8c8daecd190111b1b137946a1eaca4eb83d | 2022-10-04 | sha documentation pdf | Remove |

MALCORE_WL-01

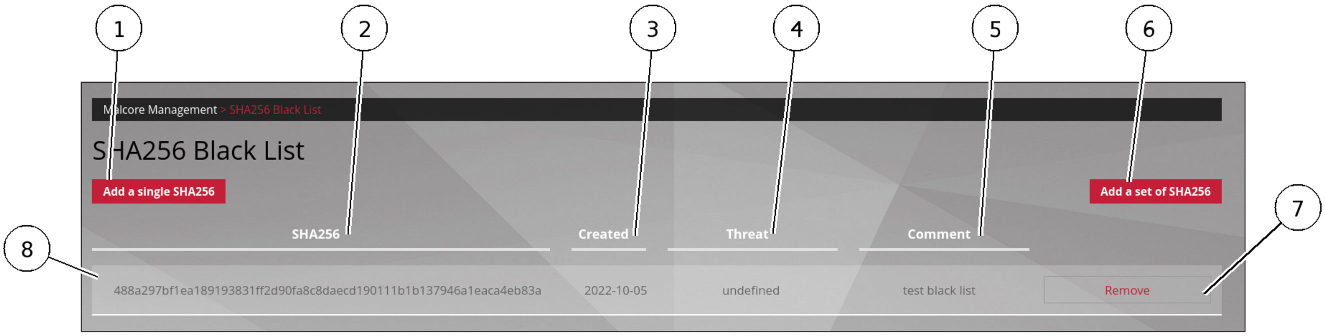
This window consists of:

- Two buttons for adding items to the list:
- One `Add a single SHA256` button (1) to add a single item by manually entering the requested information
- One `Add a set of SHA256` button (6) to add a set of items using a pre-filled .csv file
- Elements (7) that make up the list. For each element, the following items are displayed:
- `SHA256` field (2): SHA256 fingerprint of the item in question
- `Created` field (3): creation date of the record
- `Comment` field (4): optional comment for the item
- `Remove` button (5) for deleting the item in question

For the implementation, refer to *Managing the white and black lists of the Malcore engine*.

#### 5.6.29.3 `Black List` section of the `Malcore Management` submenu

The exception list called Blacklist contains the SHA256 fingerprint list of files that Malcore should consider compromised.
These files are declared compromised without parsing and defined using their SHA256 footprint.



Malcore Management > SHA256 Black List

SHA256 Black List

| SHA256 | Created | Threat | Comment | |
|---|---|---|---|---|
| 488a297bf1ea189193831ff2d90fa8c8daecd190111b1b137946a1eaca4eb83a | 2022-10-05 | undefined | test black list | Remove |

MALCORE_WL-02

This window consists of:

- Two buttons for adding items to the list:

- One `Add a single SHA256` button (1) to add a single item by manually entering the requested information
- One `Add a set of SHA256` button (6) to add a set of items using a pre-filled .csv file

- elements (8) that make up the list. For each element, the following items are displayed:

- `SHA256` field (2): SHA256 fingerprint of the item in question
- `Created` field (3): creation date of the record
- `Thread` field (4):
- `Comment` field (5): optional comment for the item
- `Remove` button (7) for deleting the item in question

For the implementation, refer to *Managing the white and black lists of the Malcore engine*.

---

### 5.6.30 `Admin-GCenter- Third-party modules` screen of the legacy web UI

See presentation of *Intelligence site and GBox*.
After pressing the `Third-party modules` of the menu `Admin-GCenter`, a screen of choice is displayed.
This screen allows you to configure connections with GCenter-related servers:

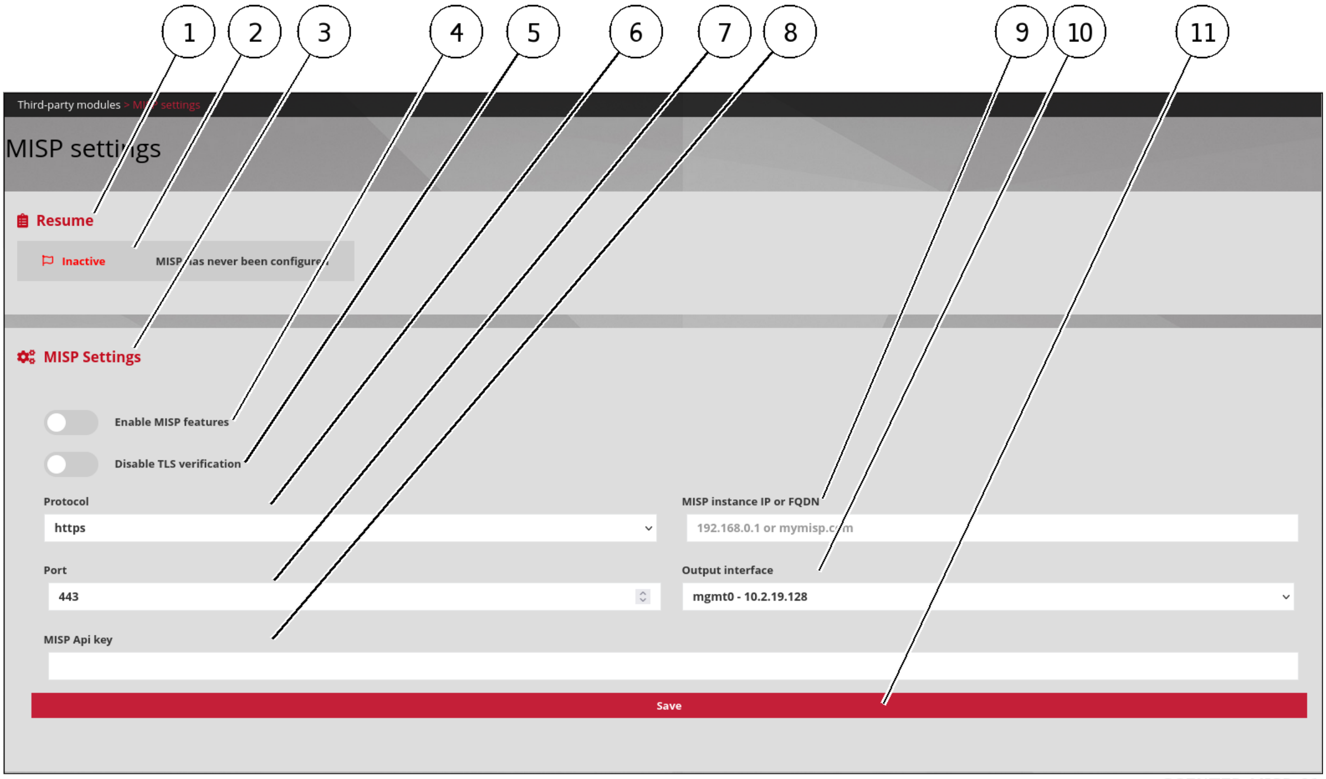
- Connection to a MISP server
- Login to intelligence website
- Connection to local GBox

| Party | Function | See |
|---|---|---|
| `MISP` | Configuring the connection to a MISP server | *MISP Connection Configuration Screen* |
| `Intelligence` | Configuration of the connection to the Intelligence site or GBox | *Intelligence site and GBox login configuration screen* |

---

### 5.6.30.1 MISP Connection Configuration Screen

This screen is used to manage the connection between the GCenter and a Malware Information Sharing Platform (MISP) server in the local infrastructure.
After pressing the `MISP` button of the `Third-party modules` screen, the following screen is displayed:



GCENTER-MISP-01

The `MISP settings` screen contains the following parts:

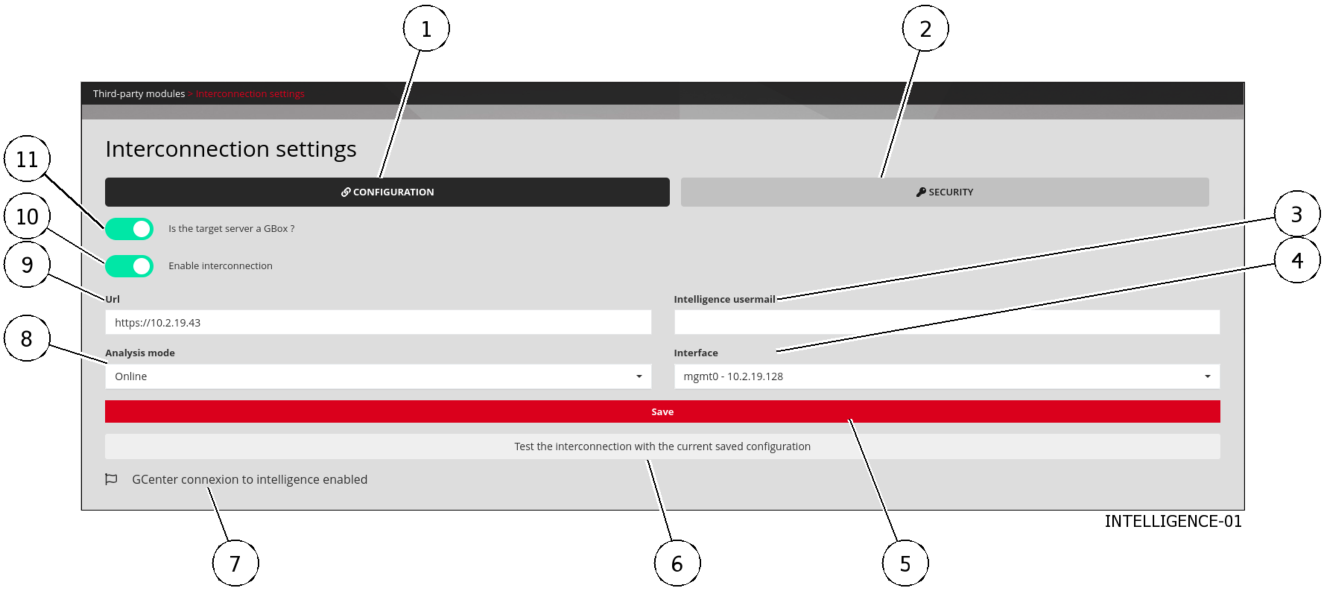
| Item | Name | Function |
|---|---|---|
| 1 | zone `` `Resume` `` | This zone indicates the connection status with the MISP. It includes: |
| 2 | • status message | Connection status message with remote server<br>For example: `` `MISP has never been configured` `` |
| 3 | zone `` `MISP Settings` `` | This zone enables setting the connection. It includes: |
| 4 | • `` `Enable MISP features` `` | This area allows setting the connection. The area includes:<br>This button displays the `` `MISP` `` command from the `` `Config / Sigflow` `` menu for configuring rule updates |
| 5 | • `` `Disable TLS verification` `` | TLS verification disable button |
| 6 | • `` `Protocol` `` | Communication protocol to be used to contact the *MISP* instance. Two options are possible: 'https' and 'http' |
| 7 | • `` `Port` `` | MISP instance listening port |
| 8 | • `` `MISP Api key ` `` | MISP instance API key |
| 9 | • `` `MISP instance IP or FQDN` `` | Domain name or IP address of the MISP instance |
| 10 | • `` `Output interface` `` | GCenter network interface for connection with MISP server |
| 11 | • `` `Save` `` | Save Entered Parameters button |

For implementation, see the *Configuring the connection to the MISP*.

---

#### 5.6.30.2 Intelligence site and GBox login configuration screen

For more information on the functions of these elements, see the presentation of *Intelligence site and GBox*.
The connection between the GCenter and the Intelligence site (or GBox) requires configuration.
The parameters of this configuration are accessible in the `` `Interconnection settings` `` screen.
After pressing the `` `Intelligence` `` button on the `` `Third-party modules` `` screen, the following screen is displayed:



Interconnection settings

Is the target server a GBox ?

Enable interconnection

Url: https://10.2.19.43

Intelligence usermail:

Analysis mode: Online

Interface: mgmt0 - 10.2.19.128

Test the interconnection with the current saved configuration

GCenter connexion to intelligence enabled

The Interconnection settings page consists of 2 tabs:

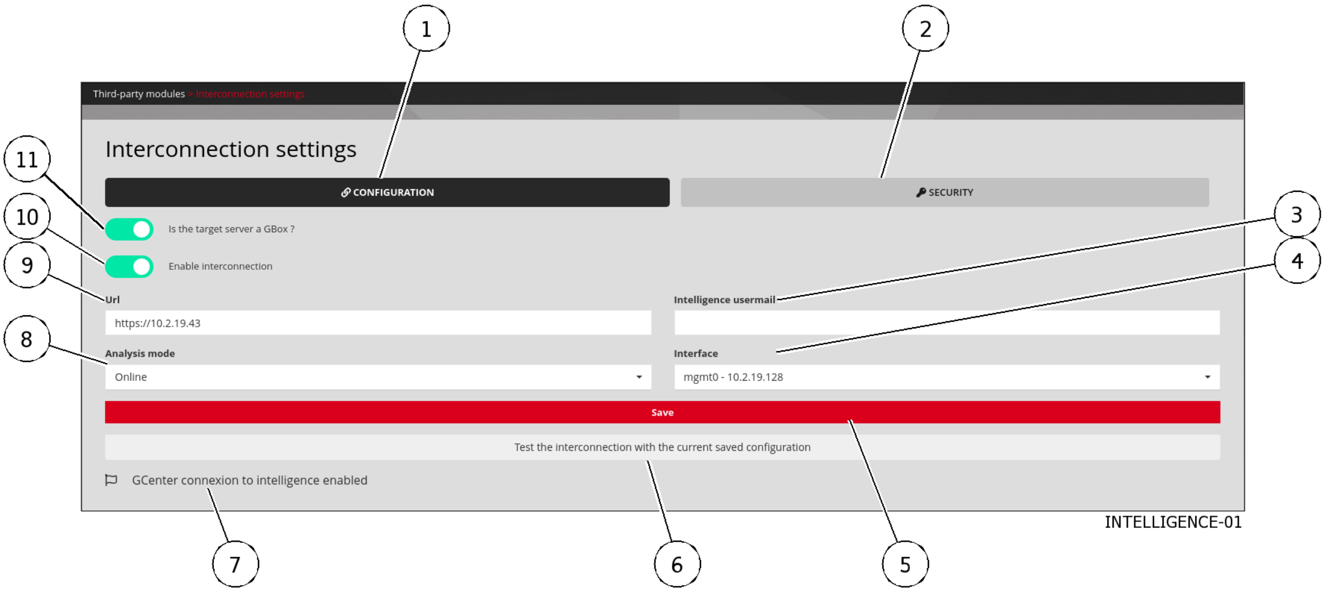
- `CONFIGURATION` Settings Management tab
- `SECURITY` Settings Management tab

For implementation of the configuration to the Intelligence site, refer to *Configuring the connection to the Intelligence site*.

For the implementation of the configuration to the GBox, refer to *Configuring the connection to the GBox*.

### 5.6.30.2.1 Tab `CONFIGURATION`

After pressing the `CONFIGURATION` button on the `Interconnection settings` screen, the following screen is displayed:



Interconnection settings

Is the target server a GBox ?

Enable interconnection

Url: https://10.2.19.43

Intelligence usermail:

Analysis mode: Online

Interface: mgmt0 - 10.2.19.128

Test the interconnection with the current saved configuration

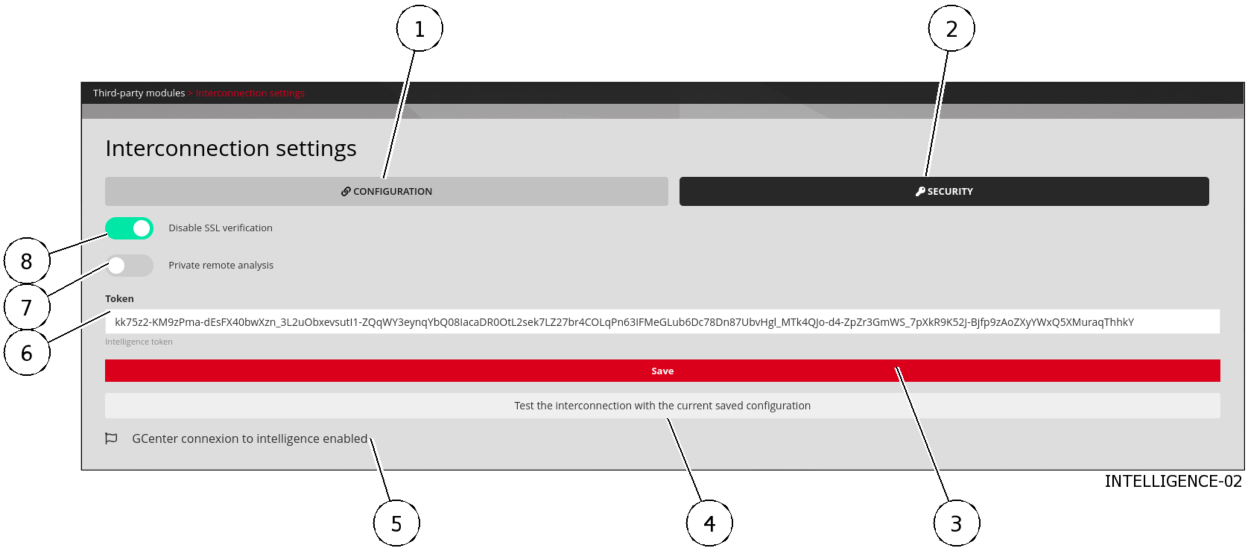
GCenter connexion to intelligence enabled

The `CONFIGURATION` tab contains the following parts:

| Item | Nom | Function |
|---|---|---|
| 1 | `CONFIGURATION` | This button displays the following configuration information: |
| 3 | - `Intelligence usermail` | Email address of the intelligence account to which an email will be sent.<br>This contains a token to connect a GCenter to https://intelligence.GATEWATCHER.com/packages/list/ |
| 4 | - `Interface` | GCenter network interface to communicate with the Intelligence / GBox site |
| 5 | - `Save` | Save Entered Parameters button |
| 6 | - `Test the interconnection...` | Test button for the interconnection with the saved parameters. The result is given by a message.<br>For example, the message `Successfully established connection to GBox https://x.x.x.x` is displayed to indicate a correct connection with a GBox. |
| 7 | - status message | Connection status message with remote server |
| 8 | - `Analysis mode` | Analysis mode: Online (Intelligence) or Offline (GBox) |
| 9 | - `Url` | Url of the remote server. For the GBox, https://x.x.x.x or the Gatewatcher Intelligence server address (https://intelligence.GATEWATCHER.com/gwapi/) |
| 10 | - `Enable interconnection` | Button to activate connection |
| 11 | - `Is the target server a GBOX` | Button to be activated only for GBox |
| 2 | `SECURITY` | This button displays the information required for security: this information is detailed below |

#### 5.6.30.2.2 Tab `SECURITY`

After pressing the `SECURITY` button on the `Interconnection settings` screen, the following screen is displayed:


Third-party modules > Interconnection settings
CONFIGURATION
SECURITY
Save
Test the interconnection with the current saved configuration
1
2
3
4
5
6
7
8
INTELLIGENCE-02

Interconnection settings

Disable SSL verification: on

Private remote analysis: off

Token

kk75z2-KM9zPma-dEsFX40bwXzn_3L2uObxevsutl1-ZQqWY3eynqYbQ08IacaDR0OtL2sek7LZ27br4COLqPn63IFMeGLub6Dc78Dn87UbvHgl_MTk4QJo-d4-ZpZr3GmWS_7pXkR9K52J-Bjfp9zAoZXyYWxQ5XMuraqThhkY

Intelligence token

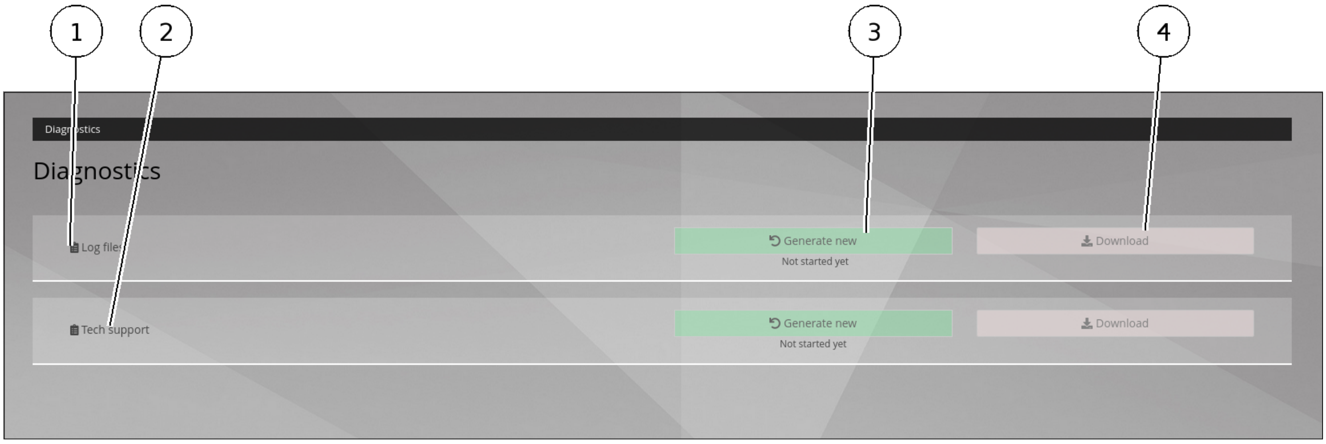
GCenter connexion to intelligence enabled

The `SECURITY` tab contains the following parts:

| Item | Name | Function |
|---|---|---|
| 1 | `CONFIGURATION` | This button displays the information needed for configuration: this information is detailed above |
| 2 | `SECURITY`. This button displays the information necessary for security: | |
| 3 | • `Save` | Save button for entered parameters |
| 4 | • `Test the interconnection... .` | Test button for interconnection with saved parameters. The result is given by a message.<br>For example, the message `Successfully established connection to GBox https://x.x.x.x` is displayed to indicate a correct connection with the GBox |
| 5 | • status message | Connection status message |
| 6 | • `Token` | Token generated on the remote server. This token is generated on the GBox or received by email for access to the Intelligence site. |
| 7 | • `Private remote analysis` | `Private remote analysis` selector allows anonymity when sending samples |
| 8 | • `Disable SSL verification` | Allows use of self-signed certificate: to be used only for GBox |

### 5.6.31 `Admin-GCenter- Diagnostics` screen of the legacy web UI

After pressing the `Diagnostics` command from the `Admin-GCenter` menu, the following screen is displayed.



DIAGNOSTIC-01

The `Diagnostics` screen contains the following sections:

| Item | Name | Description |
|---|---|---|
| 1 | `Log files` | Choice of log files to generate or download depending on the button used |
| 2 | `Tech support` | Choice of Tech support file to generate or download depending on the button used |
| 3 | `Generate new` | File generation button either `Log files` or `Tech support` depending on the button used |
| 4 | `Download` | Button to download the file is either `Log files` or `Tech support` depending on the button used |

The log export file is encrypted, only the GATEWATCHER support team can decrypt it.

For more details on data management, see *Data use*.
For implementation, see *Generating and loading files for diagnosis*.

### 5.6.32 `Admin-GCenter- Accounts` screen of the legacy web UI

After pressing the `Accounts` command from the `Admin-GCenter` menu, the following screen is displayed. This screen enables:

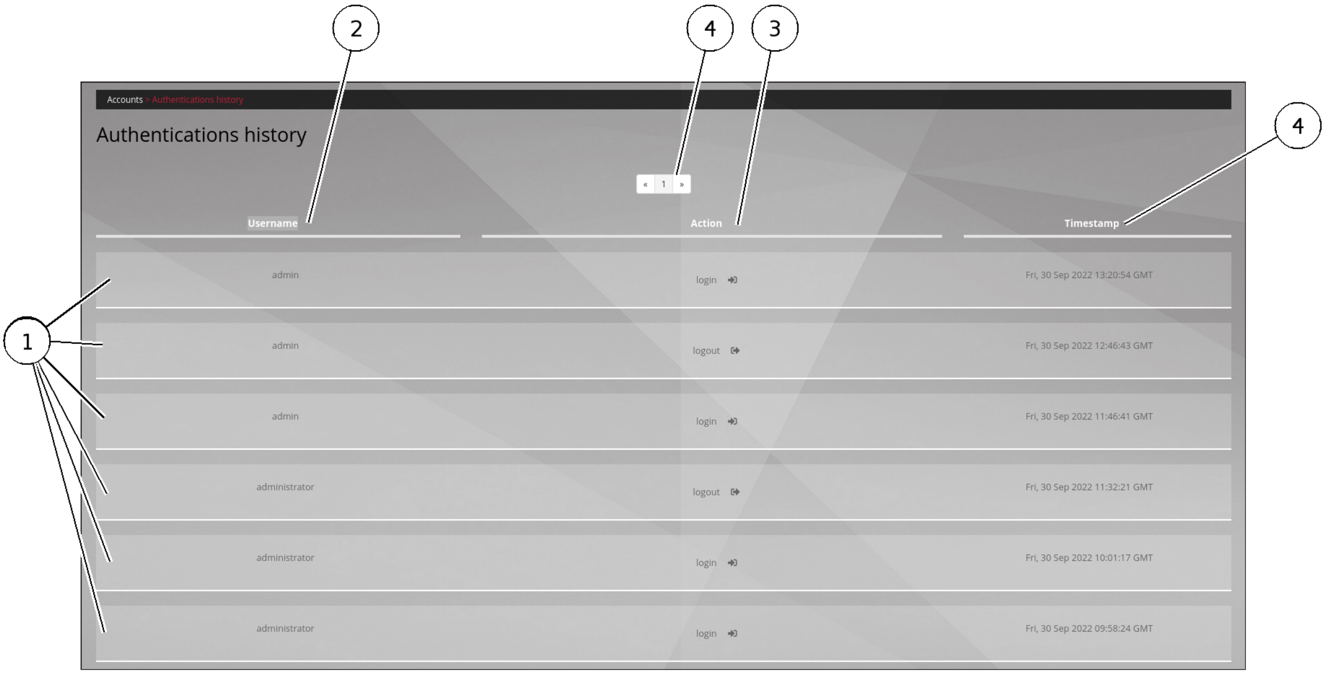
- Managing users and related roles
- The history of authentications, permissions, and user management
- Linking with an LDAP server

This screen includes the following parts:

| Section `Password Policy` | Function | Description |
|---|---|---|
| `Authentications history` | Audit trail | History of all authentications |
| `Creations/Deletions history` | Audit trail | History of all user creations or deletions |
| `Permissions history` | Audit trail | History of all user permissions |
| `Users management` | Local user management | Creation of new users and management of existing users |
| `LDAP configuration` | LDAP / ActiveDirectory integration | Management of the connection between the GCenter and the LDAP server |
| `API Keys` | Token management | Token creation and management of existing tokens |
| `Password Policy` | Password policy | Management of password policy settings |

#### 5.6.32.1 The `Authentications history` section of the `Accounts` submenu

The `Authentications history` window displays the history of all authentications on the GCenter.



| Username | Action | Timestamp |
|---|---|---|
| admin | login | Fri, 30 Sep 2022 13:20:54 GMT |
| admin | logout | Fri, 30 Sep 2022 12:46:43 GMT |
| admin | login | Fri, 30 Sep 2022 11:46:41 GMT |
| administrator | logout | Fri, 30 Sep 2022 11:32:21 GMT |
| administrator | login | Fri, 30 Sep 2022 10:01:17 GMT |
| administrator | login | Fri, 30 Sep 2022 09:58:24 GMT |

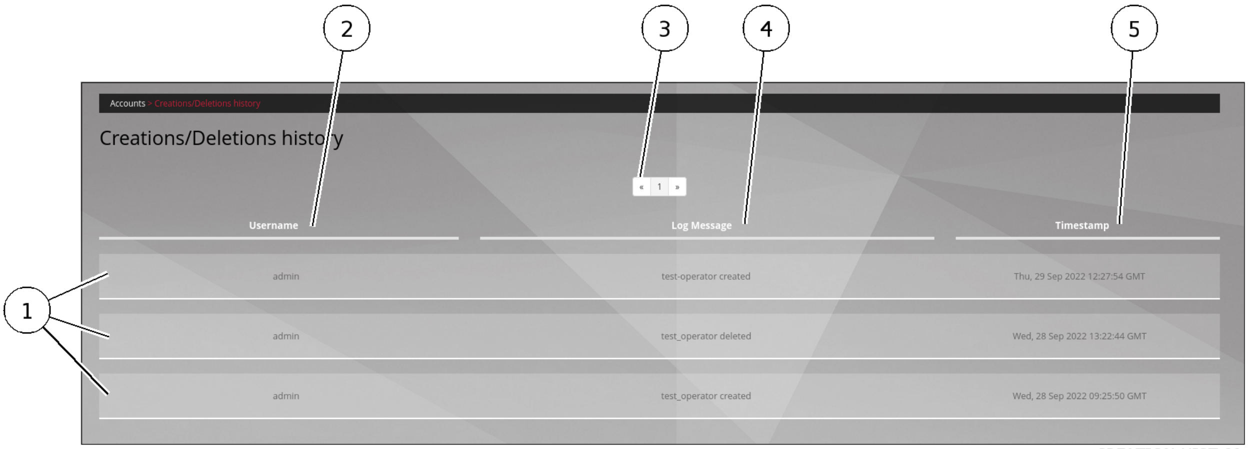
AUTHENT-01

This window displays the connections (1) in order from most recent to oldest.
The arrows (4) enable navigating between the different pages.
For each connection, the following information is displayed:

- `Username` field (2): name of the person who logged in/out
- `Action` field (3): login or logout
- `timestamp` field (5) date and time of login / logout in the format (**d** , **mm yyyy hh**: **mm**: **ss**)

#### 5.6.32.2 The `Creations/Deletions history` section of the `Accounts` submenu

The `Creations/Deletions history` window displays the history of all GCenter users created or deleted.



Creations/Deletions history

| Username | Log Message | Timestamp |
|---|---|---|
| admin | test-operator created | Thu, 29 Sep 2022 12:27:54 GMT |
| admin | test_operator deleted | Wed, 28 Sep 2022 13:22:44 GMT |
| admin | test_operator created | Wed, 28 Sep 2022 09:25:50 GMT |

CREATION-HIST-01

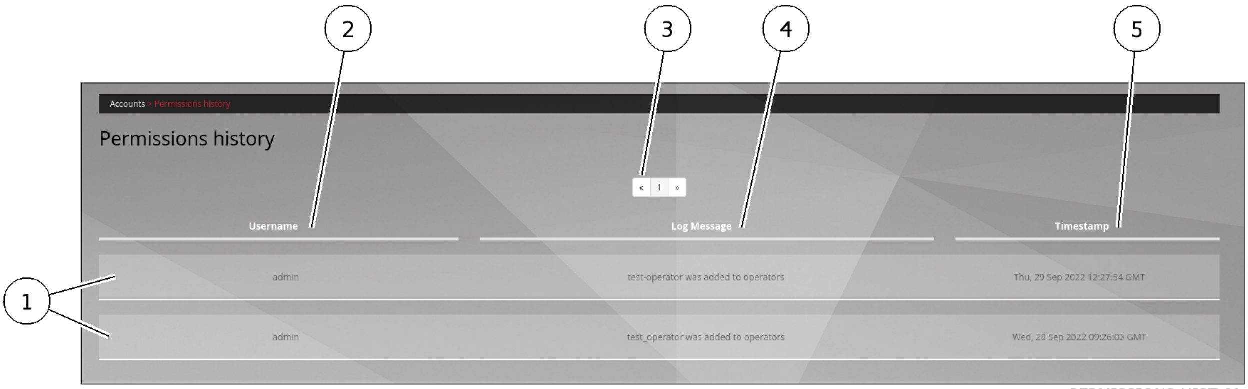
This window displays the creations or deletions (1) in order from most recent to oldest.
The arrows (3) enable loading the next page.
For each connection, the following information is displayed:

- `Username` field (2): name of the person who created the account
- `Log Message` field (4): the account name followed by the created or deleted action
- `timestamp` field (5) : date and time of login / logout in the format (**d** , **mm yyyy hh**: **mm**: **ss**)

---

#### 5.6.32.3 The `Permissions history` section of the `Accounts` submenu

The `Permissions history` window displays a history of all changes to user rights on the GCenter.



Permissions history

| Username | Log Message | Timestamp |
|---|---|---|
| admin | test-operator was added to operators | Thu, 29 Sep 2022 12:27:54 GMT |
| admin | test_operator was added to operators | Wed, 28 Sep 2022 09:26:03 GMT |

PERMISSIONS-HIST-01

This window displays the changes in rights (1) in order from most recent to oldest.
The arrows (3) enable loading the next page.
For each connection, the following information is displayed:

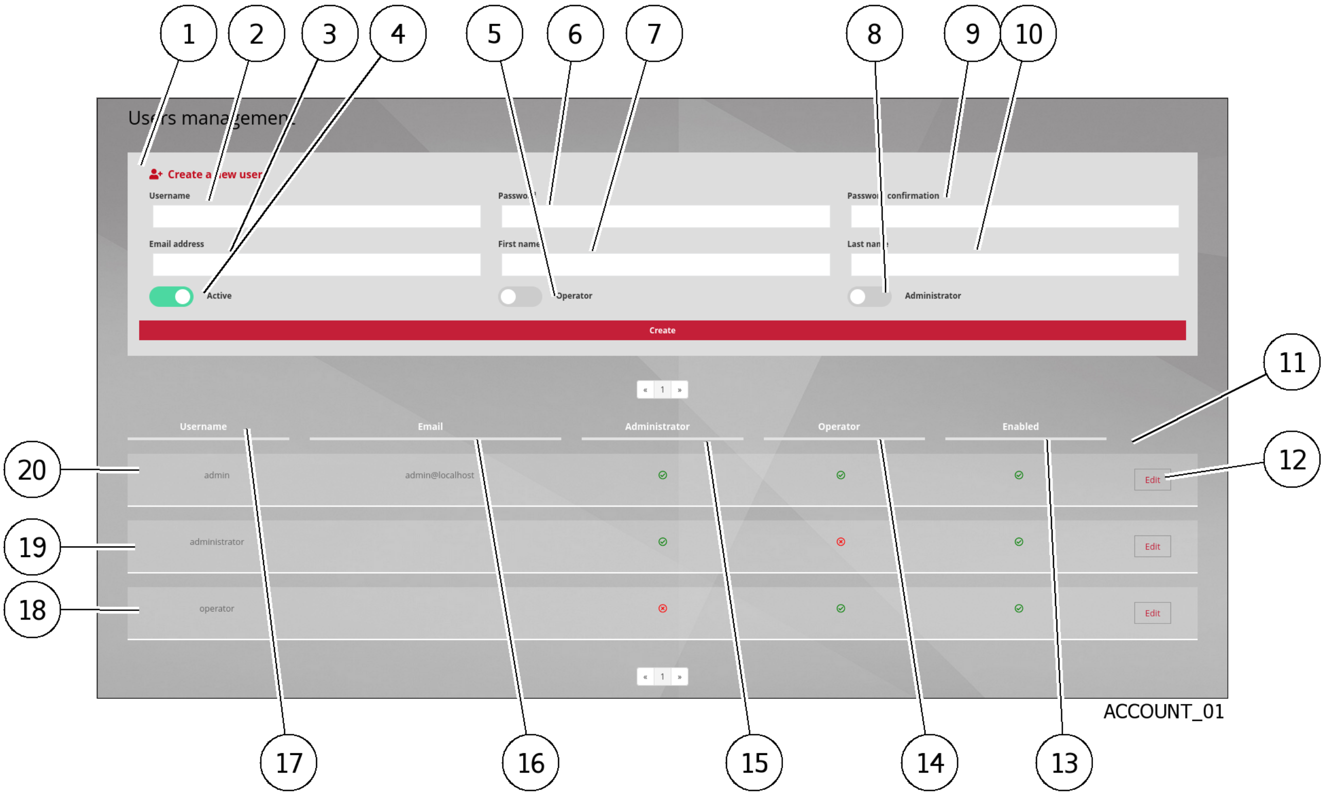
- `Username` field (2): the name of the administrator who changed the rights of the account
- `Log Message` field (4): the name of the account whose rights were changed and the action taken. Changes in rights are made by changing the affiliation of a particular role.

- `timestamp` field (5) : date and time of changes to the format (**d , mm yyyy hh: mm: ss**)

### 5.6.32.4 The `Users management` section of the `Accounts` submenu

The `Users management` window is composed of two areas:

- The area for creating a new user (1)
- The area for managing existing users (11)



| Username | Email | Administrator | Operator | Enabled | |
|---|---|---|---|---|---|
| admin | admin@localhost | ✓ | ✓ | ✓ | Edit |
| administrator | | ✓ | ⊗ | ✓ | Edit |
| operator | | ⊗ | ✓ | ✓ | Edit |

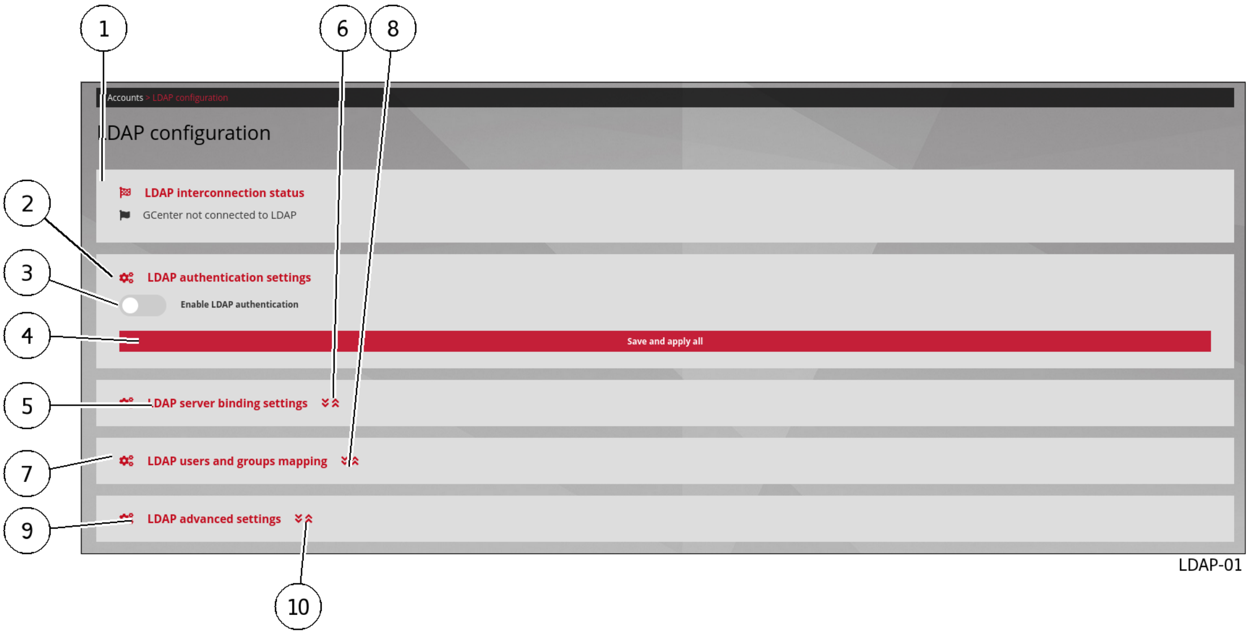
Table12: **Area for creating a new user (1)**

| Item | Name | Description |
|---|---|---|
| 2 | `Username` | Full name of the new user. This value can only contain letters, numbers, and characters [@/./+/-/-/_.**]. |
| 3 | `Email address` | Email address: optional field |
| 4 | `Active` | Enable or disable the account |
| 5 | `Operator` | Once the box is ticked, the user has the rights of the operator group |
| 6 | `Password` | Password. |
| 7 | `First name` | User's first name: optional field |
| 8 | `Administrator` | Once the box is ticked, the user has the rights of the administrator group |
| 9 | `Password confirmation` | Password is the same as the password field |
| 10 | `Last name` | User's name: optional field |

Table13: **Area for managing existing users (11)**

| Item | Name | Description |
|---|---|---|
| 12 | `Edit` button | Enables editing of the relevant profile |
| 13 | `Enabled` | Field indicating whether the account is enabled or disabled |
| 14 | `Operator` | Membership in the operator group - a tick indicates membership, a cross indicates non-membership |
| 15 | `Administrator` | Membership in the administrator group - a tick indicates membership, a cross indicates non-membership |
| 16 | `Email` | Field specifying the e-mail address |
| 17 | `Username` | Field indicating the user's name |
| 18 | `operator` User | The items indicated horizontally provide the information for the `operator` account |
| 19 | `administrator` user | The items indicated horizontally provide the information for the `administrator` account |
| 20 | `admin` user | The items indicated horizontally provide the information for the `admin` account |

### 5.6.32.5 The `LDAP configuration` section of the `Accounts` submenu


1
6
8
2
3
4
5
7
9
10
Accounts > LDAP configuration
LDAP configuration
LDAP interconnection status
LDAP authentication settings
Enable LDAP authentication
Save and apply all
LDAP server binding settings
LDAP users and groups mapping
LDAP advanced settings

GCenter not connected to LDAP

LDAP-01

The `LDAP configuration` window enables managing the connection between the GCenter and the LDAP server
To do so, this screen contains the following fields:

- The `LDAP interconnection status` area (1)
- The `LDAP authentication settings` area (2)
- The `LDAP server binding settings` area (5)
- The `LDAP users and groups mapping` area (7)
- The `LDAP advanced settings` area (9)

#### 5.6.32.5.1 The `LDAP interconnection status` area (1)

This area displays the connection status.
For the implementation, refer to *Displaying of the connection status between the GCenter and the LDAP server*.

#### 5.6.32.5.2 The `LDAP authentication settings` area (2)

This field enables connecting to a remote authentication server.
For the implementation, refer to *Enable the connection between the GCenter and the LDAP server*.

#### 5.6.32.5.3 The `LDAP server binding settings` area (5)

> **Note:**
>
> The displayed area can be expanded to view and change settings using the arrows (6).

This area enables entering the connection information to a remote authentication server.
For a list of parameters and implementation, see the *Configuring the connection between the GCenter and the LDAP server*.

#### 5.6.32.5.4 The `LDAP users and groups mapping` area (7)

> **Note:**
>
> The displayed area can be expanded to view and change settings using the arrows (6).

This area enables specifying the mapping of users and groups between the GCenter and the remote authentication server.
For a list of parameters and implementation, see the *Configuring the users and groups defined on LDAP / ActiveDirectory*.

#### 5.6.32.5.5 The `LDAP advanced settings` area (9)

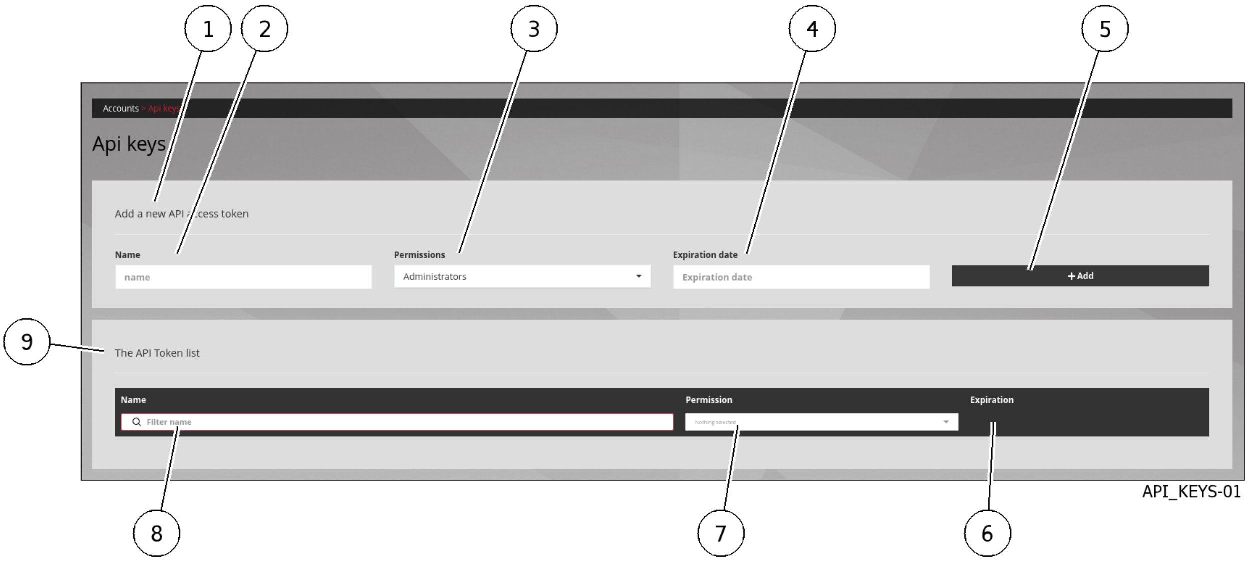
**Note:**

The displayed area can be expanded to view and change settings using the arrows (6).

This area enables advanced configuration of the connection to a remote authentication server.
For a list of parameters and implementation, see the *Configuring the connection between the GCenter and the LDAP server*.

### 5.6.32.6 The `API Keys` section of the `Accounts` submenu

The `API Keys` screen manages the API access tokens.



| Item | Area | Item |
|---|---|---|
| 1 | `Add a new API access token`: area to add a new API access token | |
| 2 | | `Name`: field to enter the name of the new token |
| 3 | | `Permissions`: field to select the account and therefore the rights of the new token |
| 4 | | `Expiration date`: field to enter the expiration date of the new token |
| 5 | | `Add`: button to add the new token |
| 9 | `The API Token list`: field to display the list of existing tokens | |
| 8 | | `Name`: field to display the name of the new token |
| 7 | | `Permission`: field to display the account and hence the rights |
| 6 | | `Expiration`: field for displaying the expiration date |

For the implementation, see the *Adding an API access token*.

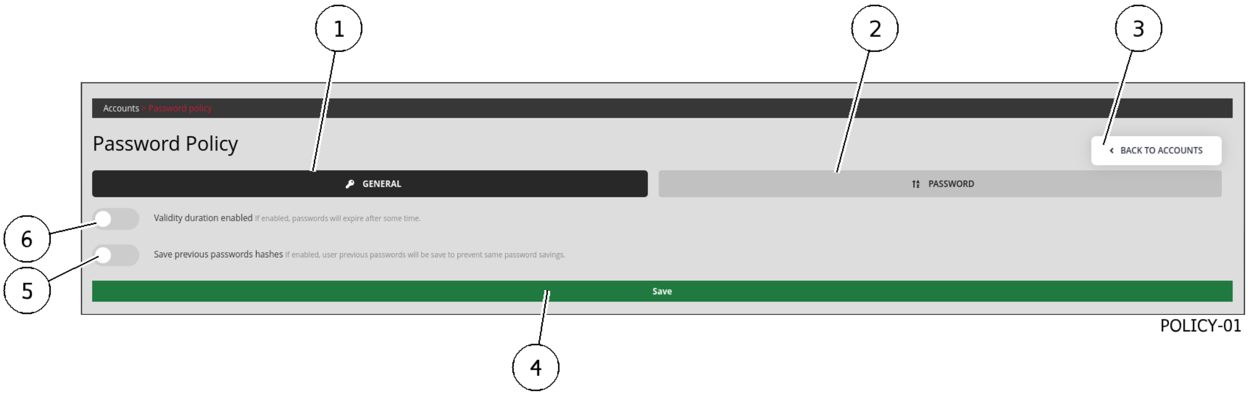
#### 5.6.32.7 The `Password Policy` section of the `Accounts` submenu

The `Password Policy` screen displays 2 types of settings:

- General settings
- Specific password settings

##### 5.6.32.7.1 General settings

If the `GENERAL` button (1) is selected, the following screen is displayed:



Validity duration enabled If enabled, passwords will expire after some time.

Save previous passwords hashes If enabled, user previous passwords will be save to prevent same password savings.

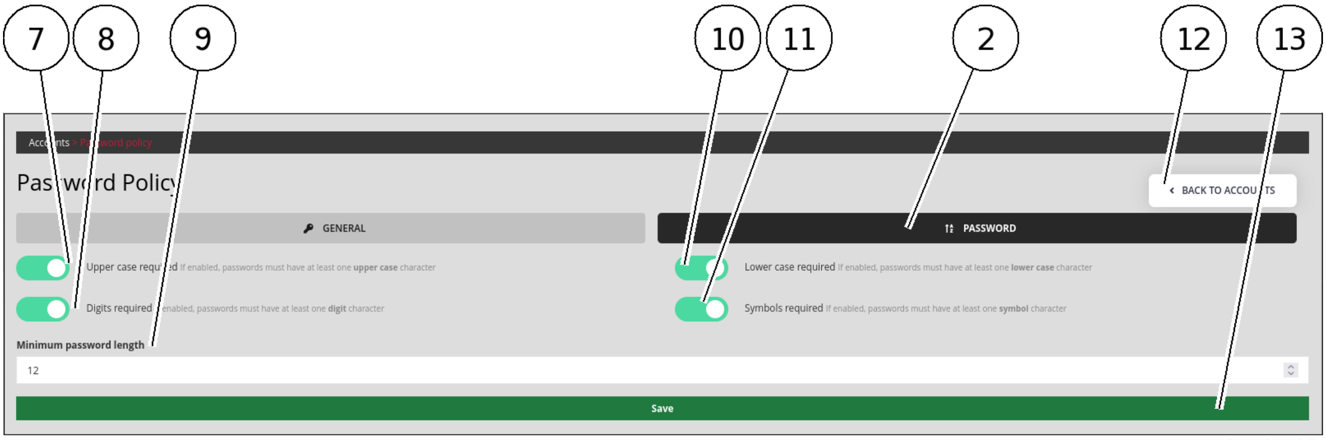
POLICY-01

| Item | Setting | Default Value | Default Value |
|---|---|---|---|
| 5 | Records the hashes of previous passwords | disabled | 5 if enabled |
| 6 | Validity period | disabled | 90 days if enabled |

The validity period starts when the password is created, not when the functionality is enabled.

##### 5.6.32.7.2 Password settings

If the `PASSWORD` button (2) is selected, the following screen is displayed:



Upper case required If enabled, passwords must have at least one **upper case** character

Lower case required If enabled, passwords must have at least one **lower case** character

Digits required If enabled, passwords must have at least one **digit** character

Symbols required If enabled, passwords must have at least one **symbol** character

**Minimum password length**

12

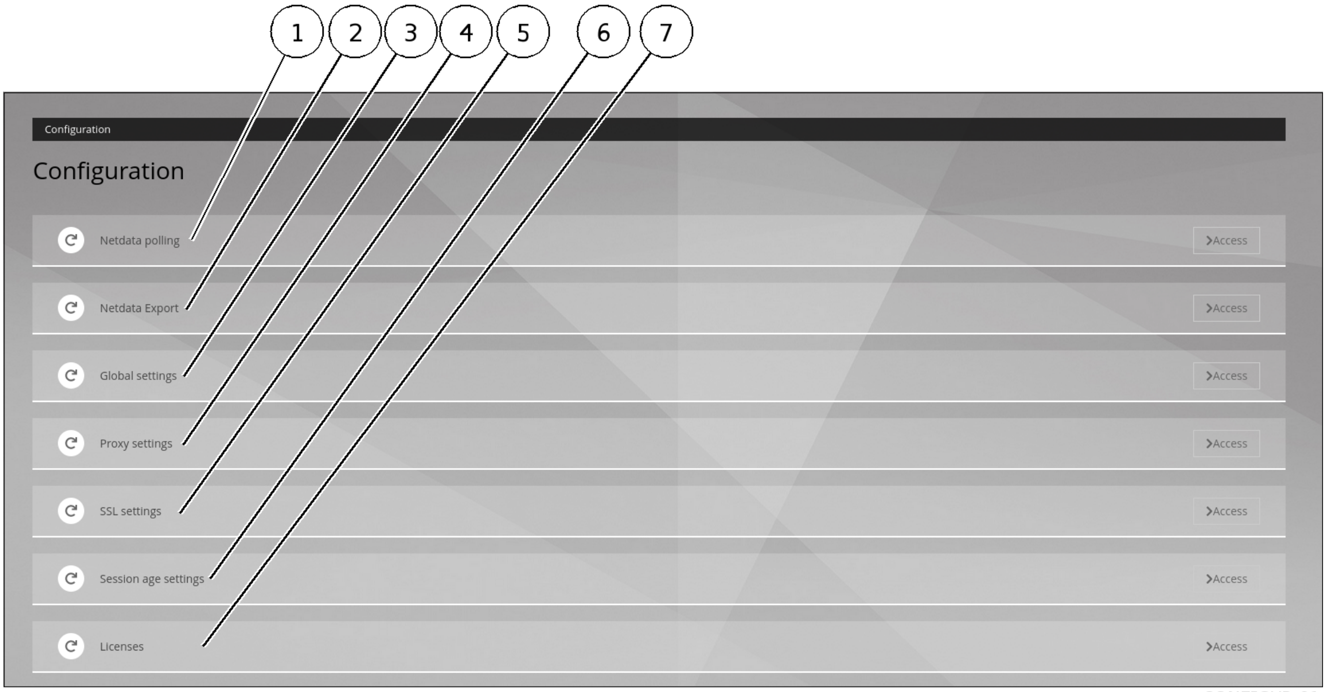
POLICY-02

| Item | Setting | Default value |
|---|---|---|
| 7 | At least one upper case letter | enabled |
| 8 | At least one digit (0 to 9) | enabled |
| 9 | Minimum password length | 12 characters |
| 10 | At least one lower case letter | enabled |
| 11 | At least one symbol (i.e. neither a number nor a letter) | enabled |

For the implementation, see the *Managing the password policy*.

### 5.6.33 `Admin-GCenter-Configuration` screen of the legacy web UI

After pressing the `Configuration` command from the `Admin-GCenter` menu, the following screen is displayed.

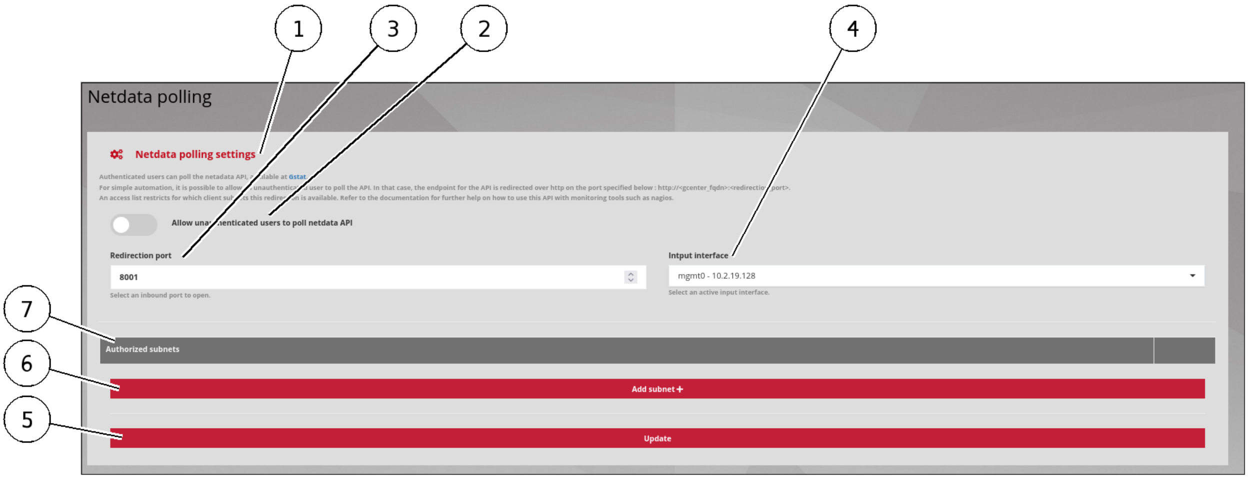


CONFIGUR-01

| Item | Name | Function |
|---|---|---|
| 1 | *`Netdata polling` section* | Configuration to have a Nagios-type supervision server retrieve the information |
| 2 | *`Netdata Export` section* | Configuration of data export to an external Netdata server |
| 3 | *`Global settings` section* | General GCenter configuration |
| 4 | *`Proxy settings` section* | Configuration of the proxy server to retrieve updates via that server |
| 5 | *`SSL settings` section* | Configuring the GCenter SSL (Secure Socket Layer) certificate |
| 6 | *`Session age settings` section* | Configuration of the maximum total duration of a session on the GCenter web interface |
| 7 | *`License information` section* | Viewing information about the current licence, checking its validity, and the available features |

#### 5.6.33.1 `Netdata polling` section

After pressing the `Netdata polling` button of the `Configuration` screen, the following screen is displayed.



Authenticated users can poll the netadata API, available at Gstat.
For simple automation, it is possible to allow an unauthenticated user to poll the API. In that case, the endpoint for the API is redirected over http on the port specified below : http://<gcenter_fqdn>:<redirection_port>.
An access list restricts for which client subnets this redirection is available. Refer to the documentation for further help on how to use this API with monitoring tools such as nagios.

○ Allow unauthenticated users to poll netdata API

Redirection port: 8001
Select an inbound port to open.

Intput interface: mgmt0 - 10.2.19.128
Select an active input interface.

CONFIGUR-02

The `Netdata polling` section contains the following elements enabling data access to be configured for a Nagios-like monitoring server. This reads the information on the input interface.

| Item | Name | Function |
|---|---|---|
| 1 | `` `Netdata polling settings` `` area<br>This area includes the following elements | Parameter definition area for metrics recovery via Netdata |
| 2 | - `` `Allow unauthenticated users to poll netdata API` `` selector | Enabled |
| 3 | - `` `Redirection port` `` field | Redirection port selector |
| 4 | - `` `Input interface` `` field | GCenter input interface selector |
| 7 | `` `Authorized subnets` `` area<br>This area includes the following elements | Displays authorized IP addresses<br>On the right side, two buttons enable modifying the IP addresses and their possible deletion |
| 5 | - `` `Update` `` button | Backup and validation of current parameters<br>If everything is ok then the message `` `The netdata polling configuration was successfully updated` `` is displayed |
| 6 | - `` `Add subnet` `` button | Displays the IP address entry window for authorized subnets |

Authenticated users can poll the Netdata API, available on Gstats.
For simple automation, it is possible to enable a non-authenticated user to poll the API.
In this case, the API endpoint is redirected to http on the port specified below:
http://<gcenter_fqdn>:<redirection_port>.
An access list restricts the client subnets for which this redirection is available.
Refer to the documentation for more help on how to use this API with monitoring tools such as Nagios.

For more details on data management, see the presentation of *Data use*.
For implementation, see the *Configuring the Netdata polling interface*.

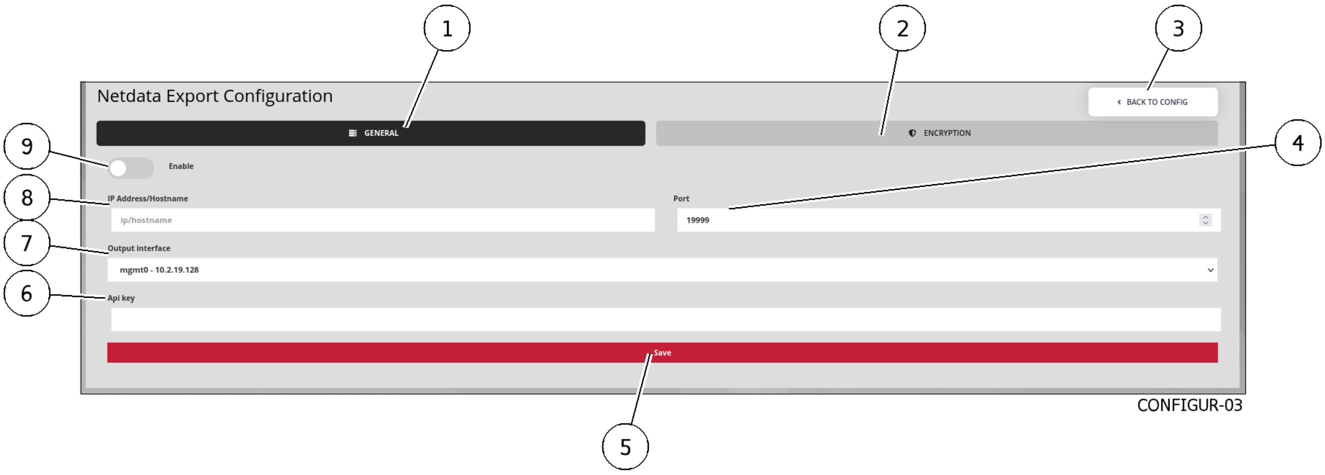
#### 5.6.33.2 `Netdata Export` section

To export system data in real time to a remote Netdata server, a Netdata export interface is present in the GCenter and is reserved for this purpose.
This Netdata export interface must be configured with the necessary information.
After pressing the `Netdata Export` button of the `Configuration` screen, the following screen is displayed.

The `Netdata Export` section contains the following items:

| Item | Function |
|---|---|
| 1 | `GENERAL` area selection button |
| 2 | `ENCRYPTION` area selection button |

**The `GENERAL` area contains the following items:**



Netdata Export Configuration

IP Address/Hostname: ip/hostname

Port: 19999

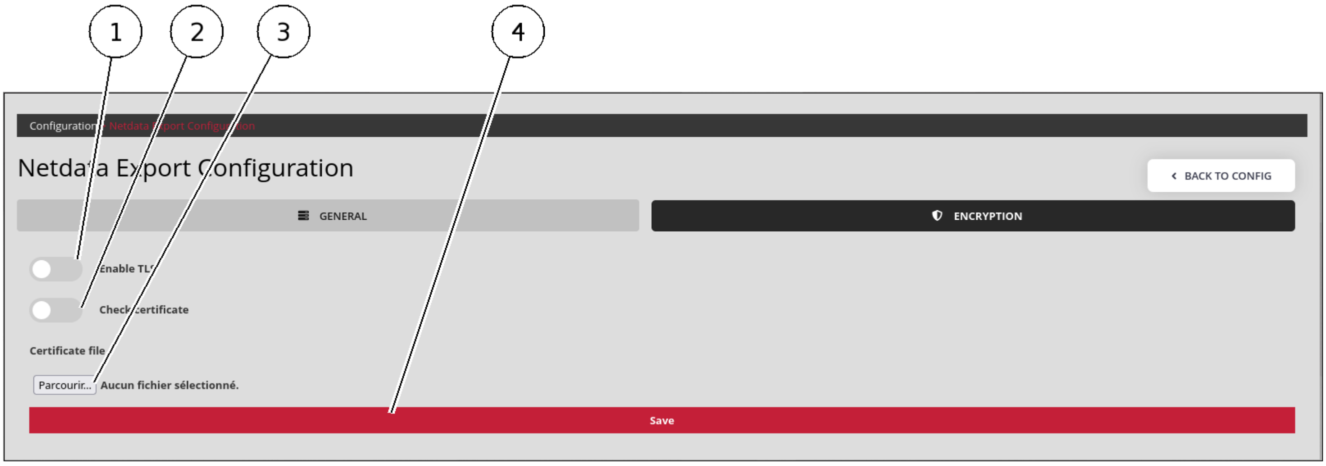
Output interface: mgmt0 - 10.2.19.128

Api key:

CONFIGUR-03

| Item | Function |
|---|---|
| 3 | `BACK TO CONFIG` button to return to the top screen |
| 4 | Input field `Port`: listening port of the Netdata server. |
| 5 | `Save` button: stores the current settings |
| 6 | `API key` field: the API key of the Netdata server. |
| 7 | `Output interface` input field: output interface to be used to reach the Netdata server |
| 8 | `IP Address/Hostname` input field: the FQDN or IP address of the Netdata server |
| 9 | `Enable` button: enables/disables the service |

**The `ENCRYPTION` field contains the following items for the Netdata part - Encryption:**
This section is required for the administrator to set up encryption of the communication between the **GCenter** and its Netdata server.
A certificate is required to enable this feature.


1
2
3
4
Configuration > Netdata Export Configuration
Netdata Export Configuration
‹ BACK TO CONFIG
GENERAL
ENCRYPTION
Enable TLS
Check certificate
Certificate file
Parcourir...
Aucun fichier sélectionné.
Save

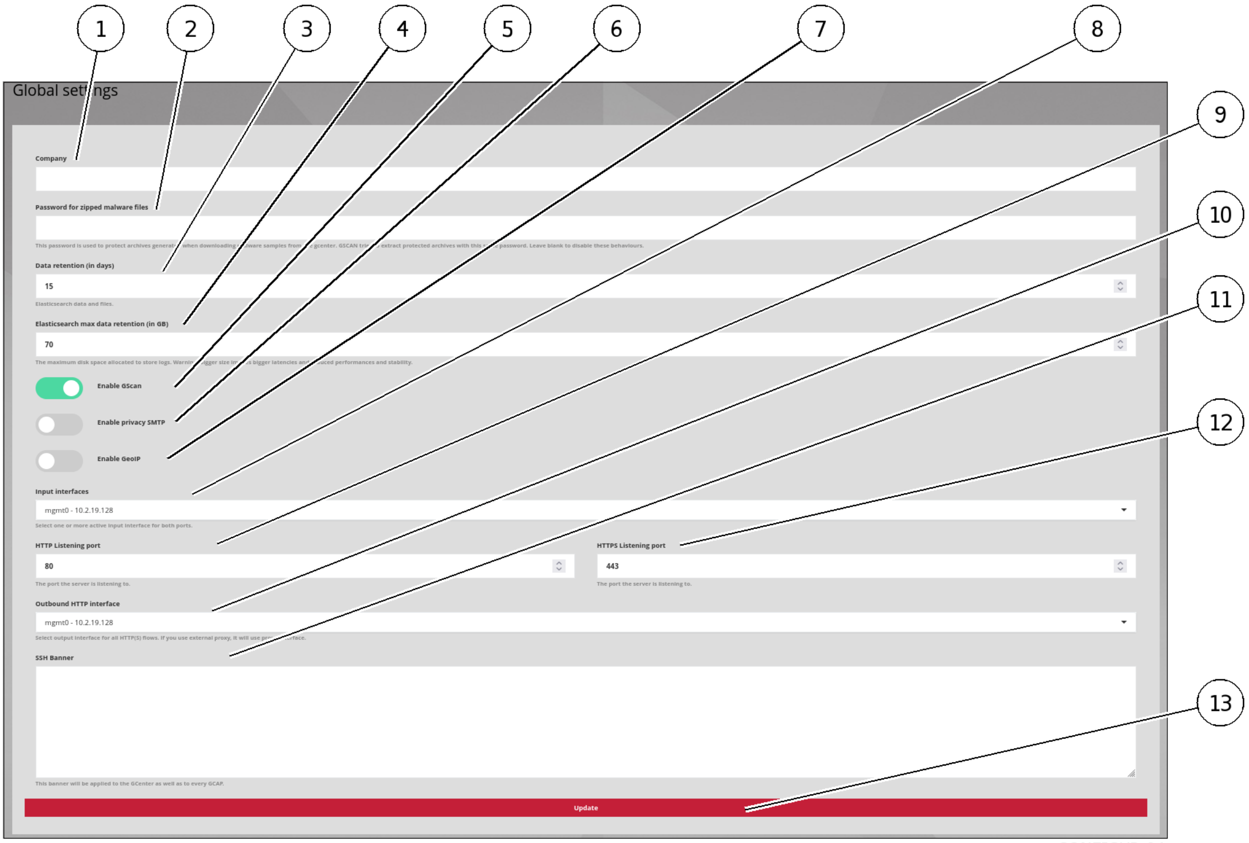
CONFIGUR-03-1

| Item | Function |
|---|---|
| 1 | `Enable TLS` selector: enable/disable encryption. Disabled by default to return to the top screen |
| 2 | `Check certificate` selector: enables/disables checking the validity of the certificate when the TLS service is enabled |
| 3 | `Parcourir` button of the `Certificate file` area: enables loading the certificate file |
| 4 | `Save` button: save the current settings |

For more details on data management, see the presentation of *Data use*.
For implementation, see the *Configuring the Netdata export interface*.

### 5.6.33.3 `Global settings` section

After pressing the `Global settings` button of the `Configuration` screen, the following screen is displayed.



Global settings

Company

Password for zipped malware files

This password is used to protect archives generated when downloading malware samples from the gcenter. GSCAN tries to extract protected archives with this same password. Leave blank to disable these behaviours.

Data retention (in days)

15

Elasticsearch data and files.

Elasticsearch max data retention (in GB)

70

The maximum disk space allocated to store logs. Warning: bigger size implies bigger latencies and reduced performances and stability.

Enable GScan: on

Enable privacy SMTP: off

Enable GeoIP: off

Input interfaces

mgmt0 - 10.2.19.128

Select one or more active input interface for both ports.

HTTP Listening port

80

The port the server is listening to.

HTTPS Listening port

443

The port the server is listening to.

Outbound HTTP interface

mgmt0 - 10.2.19.128

Select output interface for all HTTP(S) flows. If you use external proxy, it will use proxy interface.

SSH Banner

This banner will be applied to the GCenter as well as to every GCAP.

CONFIGUR-04

The `Global settings` section contains the following items:

| Item | Name | Function |
|---|---|---|
| 1 | `Company` **field** (default value: empty) | Adds the company name to be added to the detection analysis reports.<br>These reports can be downloaded after making an association between the GCenter and the Intelligence site (or the GBox) |
| 2 | `Password for zipped malware files` field (default value: empty) | Defines the password protecting the archive when downloading malware and unzipping it to avoid an unintentional click.<br>This password will be the same for downloading shellcodes.<br>The specifics of this functionality are described in more detail in the Malcore sections |
| 3 | `Data retention (in days)` field (default value: 15) | Defines the number of days the data is stored on disk.<br>Note that the configuration is applied in two steps: the first on the GCenter in this field,<br>The second at the level of the GCAP detection probe in the configuration parameters. |
| 4 | `Elasticsearch max data retention` **field** (in GB)``` | Sets the maximum disk space allocated for storing logs<br>Please note that a larger size implies higher latency, reduced performance and stability. |

suite sur la page suivante

Table 14 – suite de la page précédente

| Item | Name | Function |
|---|---|---|
| 5 | `Enable Gscan` selector (default value: enabled) | Enables real-time local scanning for malware or suspicious executables.<br>As part of the Military Programming Law, the GScan Function is disabled by default in this management interface. |
| 6 | `Enable Privacy SMTP` selector (default value: disabled) | Ensures that privacy rights are respected by hiding the *email.subject* field of SMTP alerts in the GATEWATCHER dashboards for private emails.<br>An email is considered personal if the subject line begins with the words *private*, *personal* or *confidential* (not case sensitive). |
| 7 | `Enable GeoIP` selector | Depreciated function |
| 8 | `Input interfaces` field | Enables/disables the interfaces on which the GCenter will listen on the following ports |
| 9 | `HTTP listening port` field (default value: 80) | Listening port related to the http protocol. |
| 10 | `Outbound HTTP interface` field | Defines the physical outbound interface for all http flows. |
| 11 | `SSH banner` field (default value: empty) | Sets the SSH banner presented during pre-authentication on all paired GCaps as well as the GCenter. |
| 12 | `HTTP listening port` field (Default value: 80) | Defines the listening port related to the http protocol. |
| 13 | `Save` button | stores the current settings |

For implementation, refer to *GCenter Global Configuration*.

---

#### 5.6.33.4 `Proxy settings` section

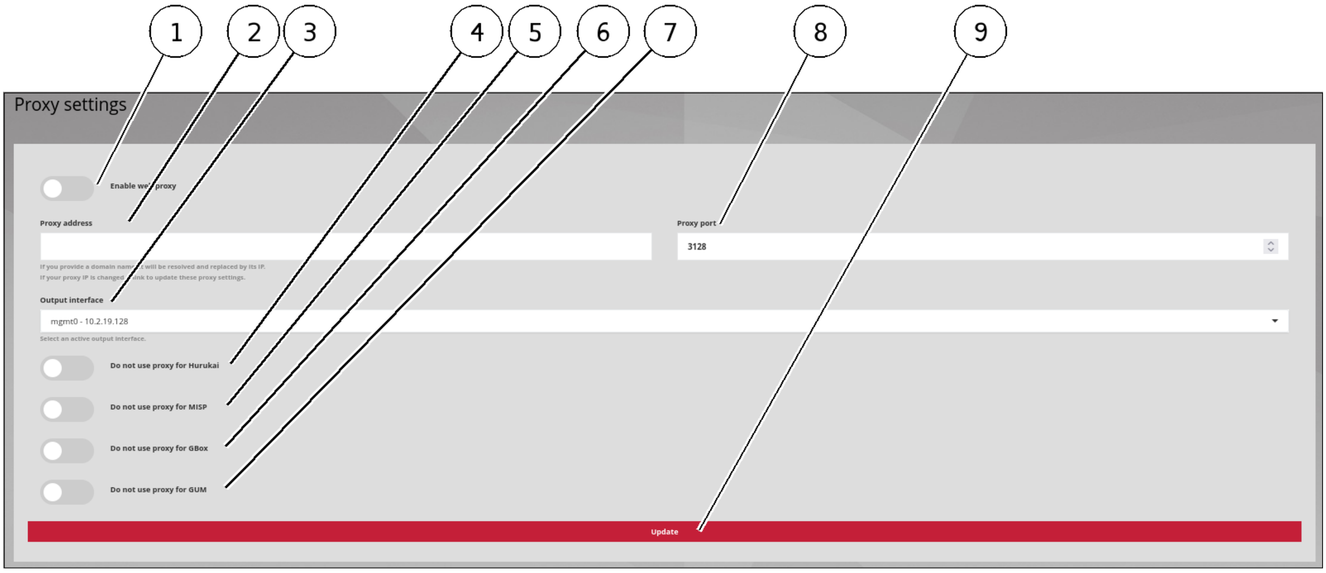
The AIONIQ solution includes the possibility of configuring a proxy server (or proxy) to communicate with:

- The MISP server
- The GBox
- Gatewatcher update servers (via GUM)

**Note:**

This update mode is part of the compliance with the Military Programming Law (MPL).
As such, the entity concerned will make its updates on a dedicated update server.
For more information, see the annex on MPL specifics in this document and the update section.

After pressing the `Proxy settings` button of the `Configuration` screen, the following screen is displayed.



Proxy settings

Enable web proxy

Proxy address

If you provide a domain name, it will be resolved and replaced by its IP.
If your proxy IP is changed, think to update these proxy settings.

Output interface

mgmt0 - 10.2.19.128

Select an active output interface.

Do not use proxy for Hurukai

Do not use proxy for MISP

Do not use proxy for GBox

Do not use proxy for GUM

Proxy port

3128

Update

CONFIGUR-05

The `Proxy settings` section contains the following items:

| Item | Name | Function |
|---|---|---|
| 1 | `Enable Web Proxy` selector | Enables/Disables the use of the proxy |
| 2 | `Proxy address` field | Sets the proxy server address as an IP address or FQDN |
| 3 | `Output interface` field | Selection of the GCenter network interface to be used to connect to the proxy |
| 4 | `Do not use proxy for Hurukai` selector | Depreciated function |
| 5 | `Do not use proxy for MISP` selector | Disables the proxy for interconnecting with the MISP server |
| 6 | `Do not use proxy for GBOX` selector | Disables the proxy for interconnecting with the GBox |
| 7 | `Do not use proxy for GUM` selector | Disables the proxy for accessing GUM |
| 8 | `Proxy port` field | Selection of the proxy listening port (1-65535) |
| 9 | `Update` button | Stores the current settings |

For implementation, refer to *Proxy Settings Configuration*.

---

#### 5.6.33.5 `SSL settings` section

After pressing the `SSL settings` button of the `Configuration` screen, the following screen is displayed:

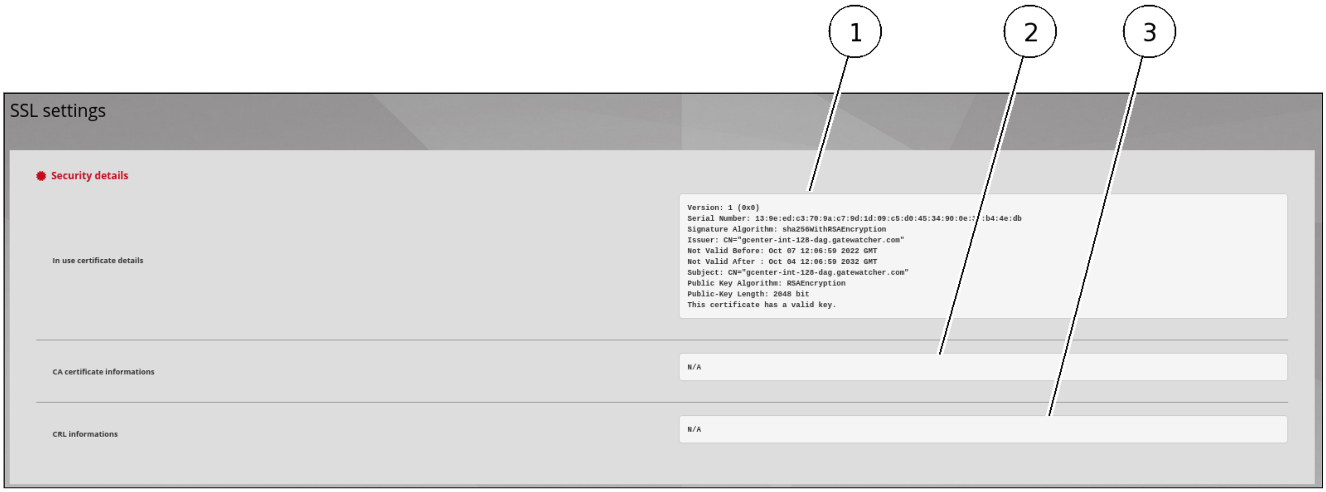
- *`Security details` area*
- *`Custom Certificate` area*
- *`Dual authentication` area*

This section enables configuring the Secure Socket Layer (SSL) certificate of the GCenter.
The generated certificate attests to the GCenter's identity and enables encrypting the exchanged data.
From this page it is also possible to configure mutual authentication (mTLS).

For implementation, refer to *SSL Settings Configuration*.

### 5.6.33.5.1 `Security details` area

The `Security details` area enables obtaining information on the certificate currently in use.



```
Version: 1 (0x0)
Serial Number: 13:9e:ed:c3:70:9a:c7:9d:1d:09:c5:d0:45:34:90:0e:[illegible]:b4:4e:db
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN="gcenter-int-128-dag.gatewatcher.com"
Not Valid Before: Oct 07 12:06:59 2022 GMT
Not Valid After : Oct 04 12:06:59 2032 GMT
Subject: CN="gcenter-int-128-dag.gatewatcher.com"
Public Key Algorithm: RSAEncryption
Public-Key Length: 2048 bit
This certificate has a valid key.
```

```
N/A
```

```
N/A
```

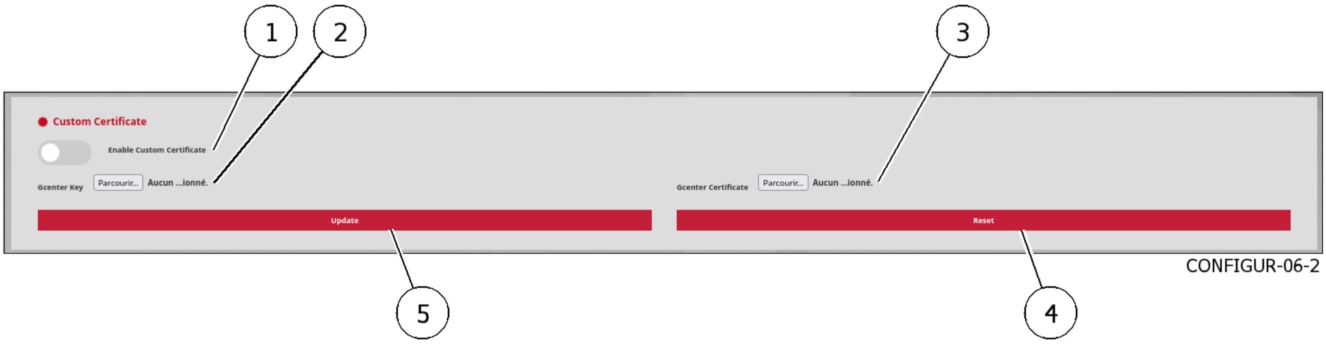
CONFIGUR-06-1

This area includes the following items:

| Item | Name | Function |
|---|---|---|
| 1 | `In use certificate details` field | Displays certificate information such as the date of issue and expiry, and the issuer of the certificate, etc. |
| 2 | `CA certificate information` field | Displays the certificate authority information enabling the identity of the correspondents to be determined in the `Dual Authentication` section |
| 3 | `CRL informations` field | Lists identifiers that were revoked, invalidated, or are no longer trustworthy. |

### 5.6.33.5.2 `Custom Certificate` area

The `Custom Certificate` area enables using a specific certificate.
This is done by specifying the private key in the `GCenter Key` field and the PEM format certificate in the `GCENTER certificate` field and also by activating the `Enable Custom Certificate` selector.



CONFIGUR-06-2

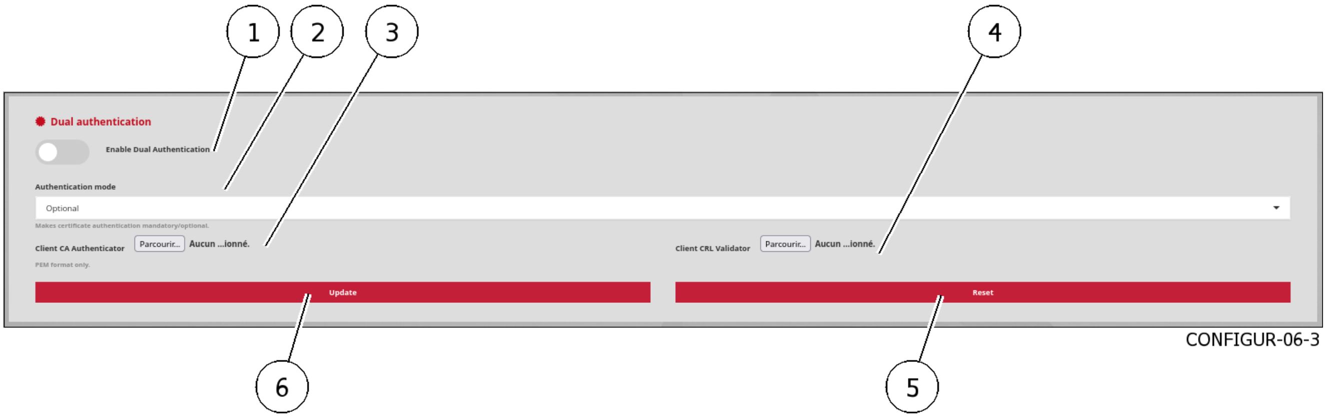
The `Custom Certificate` area contains the following items:

| Item | Name | Function |
|---|---|---|
| 1 | `Enable Custom Certificate` selector | Enabling a personalized certificate |
| 2 | `GCenter Key` field | Selection of a GCenter key file |
| 3 | `GCENTER certificate` field | Selection of a GCenter certificate file |
| 4 | `Reset` button | Reinitalization of the configuration |
| 5 | `Update` button | Stores the current settings |

---

#### 5.6.33.5.3 `Dual authentication` area

The `Dual Authentication` area enables mutual authentication (mTLS).
This allows the user to verify the identity of the server as well as allowing the server to verify the identity of the user.



Authentication mode: Optional

Makes certificate authentication mandatory/optional.

Client CA Authenticator Parcourir... Aucun ...ionné.

PEM format only.

Client CRL Validator Parcourir... Aucun ...ionné.

CONFIGUR-06-3

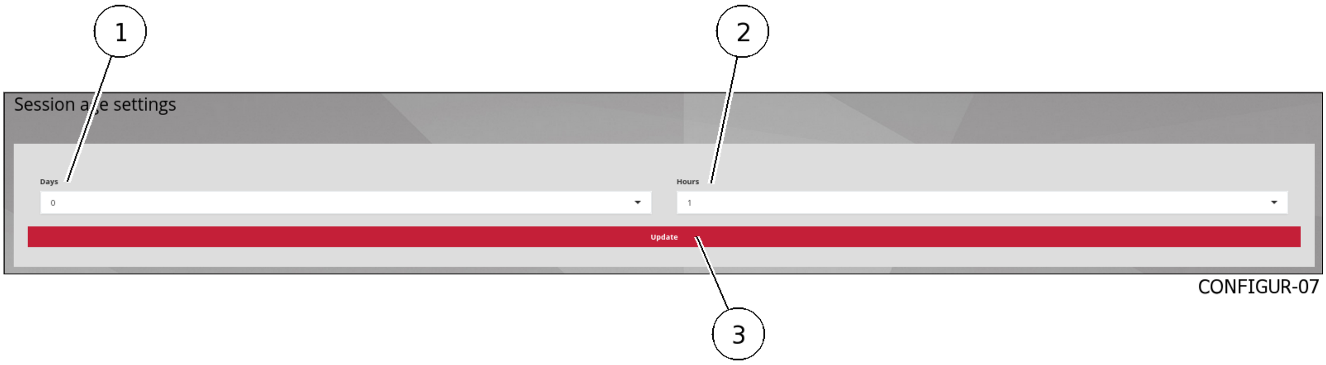
The `Dual authentication` area contains the following items:

| Item | Name | Function |
|---|---|---|
| 1 | `Enable Dual Authentication` selector | Enabling a personalized certificate |
| 2 | `Authentication mode` field | Selecting the type of authentication:<br>• select `Forced`: making it mandatory for users to hold a certificate issued by the certification authority)<br>• select `Optional`: only checks for the presence of a certificate |
| 3 | `Client CA Authenticator` field | Selection of a certificate file issued by the certification authority in PEM format |
| 4 | `Client CRL Validator` field | Selecting a file from the list of revoked certificates |
| 5 | `Update` button | Stores the current settings |

---

#### 5.6.33.6 `Session age settings` section

This section sets the maximum total duration of a session on the GCenter web interface.
After pressing the `Sessions age settings` button of the `Configuration` screen, the following screen is displayed.



The `Session age settings` section contains the following items:

| Item | Name | Function |
|---|---|---|
| 1 | `Days` field | Duration of the session in days |
| 2 | `Hours` field | Duration of the session in hours |
| 3 | `Update` button | Stores the current settings |

For implementation, refer to *Configuring Session Age Settings*.

#### 5.6.33.7 `License information` section

After pressing the `Licenses` button of the `Configuration` screen, the screen `License information` is displayed.
The `License information` screen is used to obtain information about the current license, verify its validity and available features.
This screen consists of the fields:

- *`License details` area*
- *`License features` area*

The `License details` area enables obtaining information on:

- The material for which this licence was issued via its model and serial number
- The period of validity of the licence
- The associated contact address
- The type of licence

The "License features" area provides information about enabling the various modules of the GCenter.
Finally, it is possible at the bottom of the page to enter a new licence, and also to set the notification in the interface of a near expiry date by entering the number of days before the expiration.

To obtain GCenter licence, please contact your GATEWATCHER business engineer or contact them at: trade@gatewatcher.com.
Once the license is validated and activated, the content of the page updates and displays the details of the license.

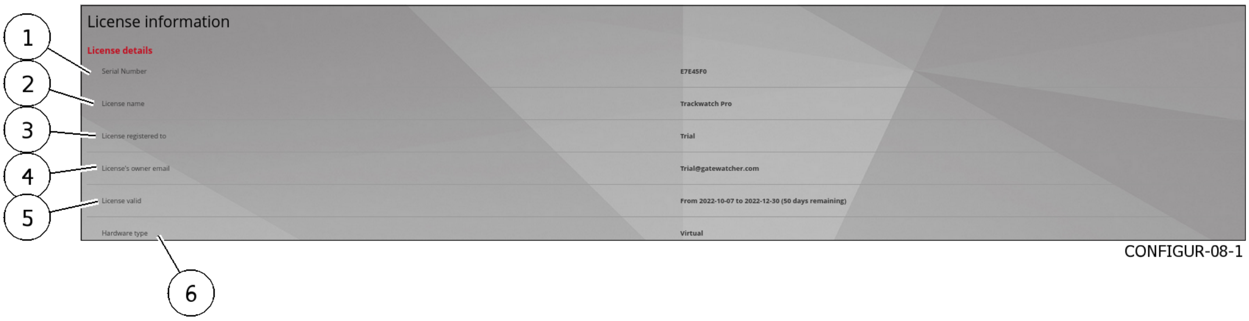
For the implementation of a new license, refer to *Licence amendment*.

**Note:**

To obtain a GCenter license, please contact GATEWATCHER business engineers or contact them at trade@GATEWATCHER.com.

---

#### 5.6.33.7.1 `License details` area



License information

License details

| | |
|---|---|
| Serial Number | E7E45F0 |
| License name | Trackwatch Pro |
| License registered to | Trial |
| License's owner email | Trial@gatewatcher.com |
| License valid | From 2022-10-07 to 2022-12-30 (50 days remaining) |
| Hardware type | Virtual |

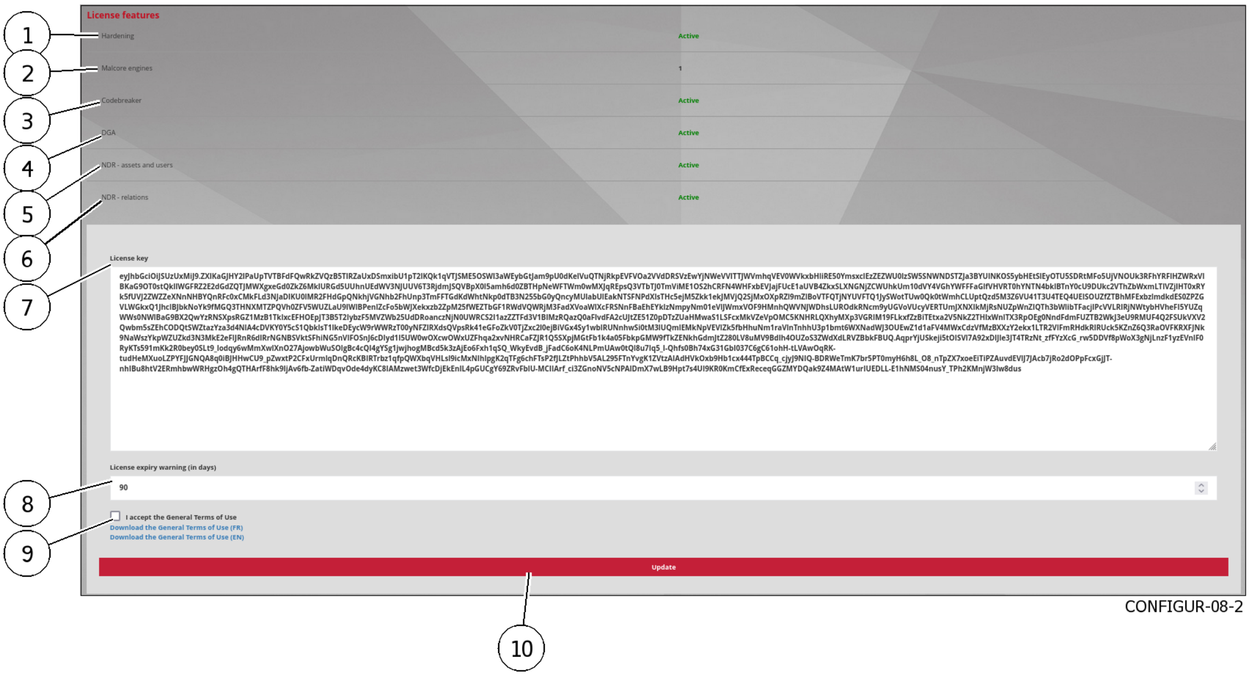
CONFIGUR-08-1

The `License details` area contains the following items:

| Item | Field | Function |
|---|---|---|
| 1 | `Serial Number` | Server information |
| 2 | `License name` | Name of the licence |
| 3 | `License registered to` | Registration of the licence |
| 4 | `License's owner email` | Email of the licence owner |
| 5 | `License valid` | Licence registration date and remaining duration |
| 6 | `Hardware type` | GCenter material type (e.g. virtual) |

---

### 5.6.33.7.2 `License features` area



License features

| | |
|---|---|
| Hardening | Active |
| Malcore engines | 1 |
| Codebreaker | Active |
| DGA | Active |
| NDR - assets and users | Active |
| NDR - relations | Active |

License key

eyJhbGciOiJSUzUxMiJ9.ZXlKaGJHY2lPaUpTVTBFdFQwRkZVQzB5TlRZaUxDSmxibU1pT2lKQk1qVTJSME5OSWl3aWEybGtJam9pU0dKelVuQTNjRkpEVFVOa2VVdDRSVzEwYjNWeVVlTTJWVmhqVEV0WVkxbHliRE50YmsxcIEzZEZWU0lzSW5SNWNDSTZJa3BYUlNKOS5ybHEtSlEyOTU5SDRtMFo5UjVNOUk3RFhYRFlHZWRxVl
BKaG9OT0stQklIWGFRZ2E2dGdZQTJMWXgxeGd0ZkZ6MklURGd5UUhnUEdWV3NJUUV6T3RjdmJSQVBpX0l5amh6d0ZBTHpNeWFTWm0wMXJqREpsQ3VTbTJ0TmViME1OS2hCRFN4WHFxbEVJajFUcE1aUVB4ZkxSLXNGNjZCWUhkUm10dVY4VGhYWFFFaGlfVHVRT0hYNTN4bklBTnY0cU9DUkc2VThZbWxmLTlVZjlHT0xRY
k5fUVJ2ZWZZeXNnNHBYQnRFc0xCMkFLd3NJaDlKU0lMR2FHdGpQNkhjVGNhb2FhUnp3TmFFTGdKdWhtNkp0dTB3N255bG0yQncyMUlabUlEakNTSFNPdXlsTHc5ejM5Zkk1ekJMVjQ2SjMxOXpRZl9mZlBoVTFQTjNYUVFTQ1JySWotTUw0Qk0tWmhCLUptQzd5M3Z6VU41T3U4TEQ4UElSOUZfZTBhMFExbzlmdkdES0ZPZG
VLWGkxQ1JhclBJbkNoYk9fMGQ3THNXMTZPQVh0ZFV5WUZLaU9IWlBPenlZcFo5bWJXekxzb2ZpM25fWEZTbGF1RWdVQWRjM3FadXVoaWlXcFRSNnFBaEhEYklzNmpyNm01eVlJWmxVOF9HMnhQWVNJWDhsLUROdkRNcm9yUGVoVUcyVERTUmJXNXlkMjRsNUZpWnZlQTh3bWlibTFacjlPcVVLRlRjNWtybHVheFI5YUZq
WWs0NWlBaG9BX2QwYzRNSXpsRGZ1MzB1TklxcEFHOEpJT3B5T2lybzF5MVZWb25UdDRoanczNjN0UWRCS2I1azZZTFd3V1BIMzRQazQ0aFlvdFA2cUJtZE51Z0pDTzZUaHMwaS1LSFcxMkVZeVpOMC5KNHRLQXhyMXp3VGRIM19FLkxfZzBiTEtxa2V5NkZ2THlxWnlTX3RpOEg0NndFdmFUZTB2WkJ3eU9RMUF4Q2FSUkVXV2
Qwbm5sZEhCODQtSWZtazYza3d4NlA4cDVKY0Y5cS1QbklsT1lkeDEycW9rWWRzT00yNFZlRXdsQVpsRk41eGFoZkV0TjZxc2l0ejBiVGx4Sy1wblRUNnhwSi0tM3lUQmlEMkNpVEVlZk5fbHhuNm1raVlnTnhhU3p1bmt6WXNadWJ3OUEwZ1d1aFV4MWxCdzVfMzBXXzY2ekx1LTR2VlFmRHdkUlRUck5KZnZ6Q3RaOVFKRXFJNk
9NaWszYkpWZUZkd3N3MkE2eFlJRnR6dlRrNGNBSVktSFhiNG5nVlFOSnJ6cDlyd1I5UW0wOXcwOWxUZFhqa2xvNHRCaFZJR1Q5SXpjMGtFb1k4a05FbkpGMW9fTkZENkhGdmJtZ280LV8uMV9Bdlh4OUZoS3ZXdXdLRVZBbkFBUQ.AqprYjUSkeji5tOISVl7A92xDIJle3JT4TRzNt_zfFYzXcG_rw5DDVf8pWoX3gNjLnzF1yzEVnIF0
RyKTs591mKk2R0bey0SLt9_lodqy6wMmXwlXnO27AjowbWuSOlgBc4cQl4gYSg1jwjhogMBcd5k3zAjEo6Fxh1qSQ_WkyEvdB_jFadC6oK4NLPmUAw0tQl8u7lq5_l-Qhfs0Bh74xG31Gbl037C6gC61ohH-tLVAwOqRK-
tudHeMXuoLZPYFJJGNQA8q0iBJHHwCU9_pZwxtP2CFxUrmlqDnQRcKBlRTrbz1qfpQWXbqVHLsl9icMxNlhlpgK2qTFg6chFTsP2fJLZtPhhbV5AL295FTnYvgK1ZVtzAlAdHVkOxb9Hb1cx444TpBCCq_cjyJ9NIQ-BDRWeTmK7br5PT0myH6h8L_O8_nTpZX7xoeEiTiPZAuvdEVlJ7JAcb7jRo2dOPpFcxGjJT-
nhIBu8htV2ERmhbwWRHgzOh4gQTHArfF8hk9IjAv6fb-ZatiWDqvOde4dyKC8IAMzwet3WfcDjEkEnlL4pGUCgY69ZRvFbIU-MCIlArf_ci3ZGnoNV5cNPAIDmX7wLB9Hpt7s4UI9KR0KmCfExReceqGGZMYDQak9Z4MAtW1urIUEDLL-E1hNMS04nusY_TPh2KMnjW3lw8dus

License expiry warning (in days)

90

☐ I accept the General Terms of Use

Download the General Terms of Use (FR)

Download the General Terms of Use (EN)

CONFIGUR-08-2

The `License features` area contains the following items:

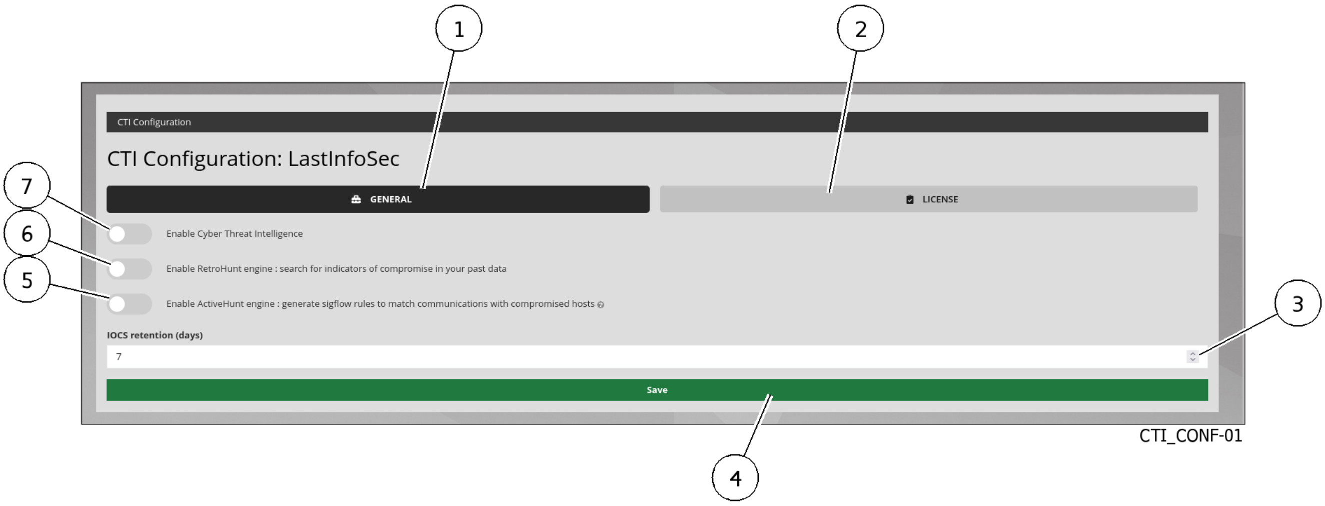
| Item | Name | Function |
|---|---|---|
| 1 | `Hardening` field | Server information |
| 2 | `Malcore engines` field | Number of Malcore engines |
| 3 | `Codebreaker` field | Information on enabling the Malcore engine |
| 4 | `DGA` field | Information on enabling the DGA engine |
| 5 | `NDR - assets and users` field | Information on NDR user functions and equipment |
| 6 | `NDR - relations` field | Information on NDR relations functions |
| 7 | `License key` field | Entering the licence key |
| 8 | `License expiry warning (in days)` field | Entering the number of days of the licence expiration alarm message |
| 9 | `I accept the General Terms of Use` field | Selecting acceptance of the terms of use |
| 10 | `Update` button | Stores the current settings |

## 5.6.34 `Admin-GCenter- CTI Configuration` screen of the legacy web UI

After pressing the `CTI Configuration` command of the `Admin-GCenter` menu, the following screen is displayed. `LastInfoSec` is displayed.
The screen consists of two sections:

- *`GENERAL` section*
- *`LICENSE` section*

### 5.6.34.1 `GENERAL` section



CTI Configuration

CTI Configuration: LastInfoSec

GENERAL

LICENSE

○ Enable Cyber Threat Intelligence

○ Enable RetroHunt engine : search for indicators of compromise in your past data

○ Enable ActiveHunt engine : generate sigflow rules to match communications with compromised hosts

IOCS retention (days)

7

Save

CTI_CONF-01

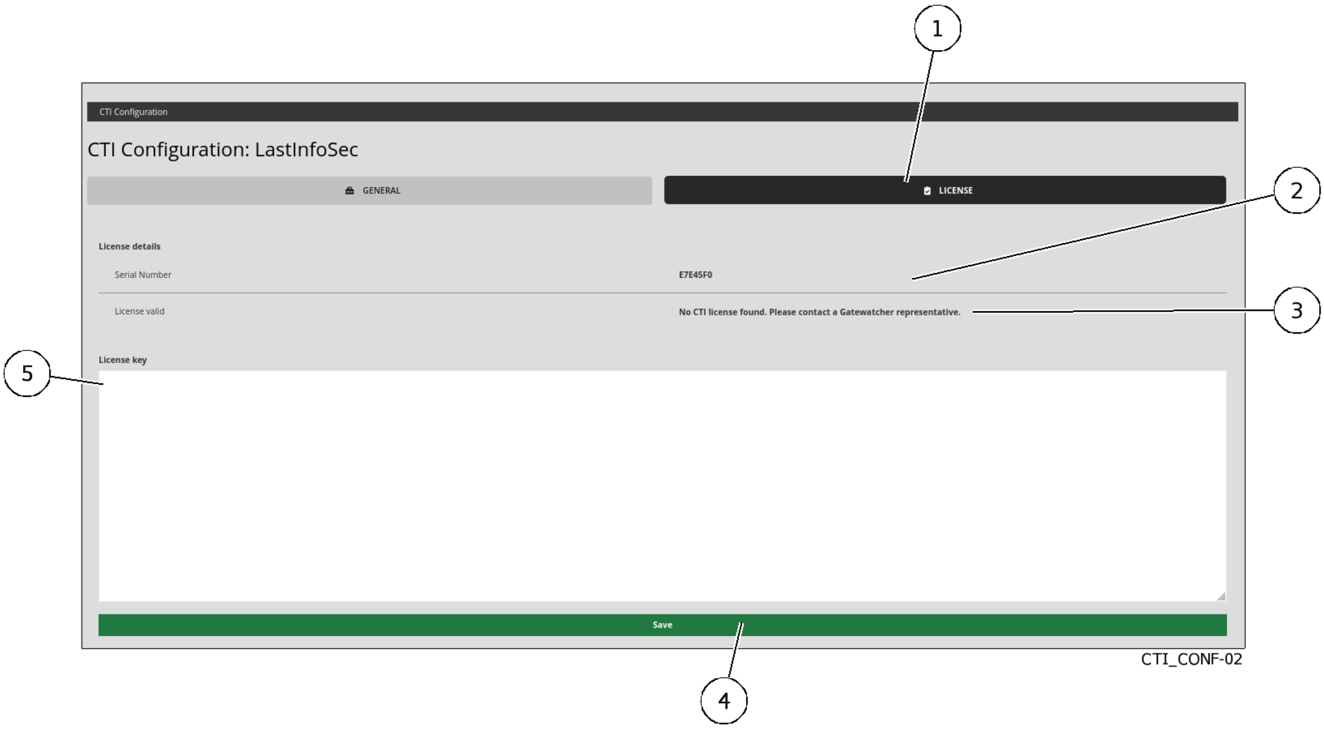
This section enables viewing and modifying:

- The enabling of the `ActiveHunt` engine
- The enabling of the `RetroHunt` engine
- The enabling of the `Cyber Threat Intelligence` engine

It enables changing the value of the retention time in days.

| MaItem | Function |
|---|---|
| 1 | `GENERAL` area selection button |
| 2 | `LICENSE` section selection button |
| 3 | Selection of the retention time value in days (parameter `IOCS retention (days)`) |
| 4 | `Save` button |
| 5 | `ActiveHunt` engine selector |
| 6 | `RetroHunt` engine selector |
| 7 | `Cyber Threat Intelligence` engine selector |

### 5.6.34.2 `LICENSE` section



CTI Configuration: LastInfoSec

License details

Serial Number E7E45F0

License valid No CTI license found. Please contact a Gatewatcher representative.

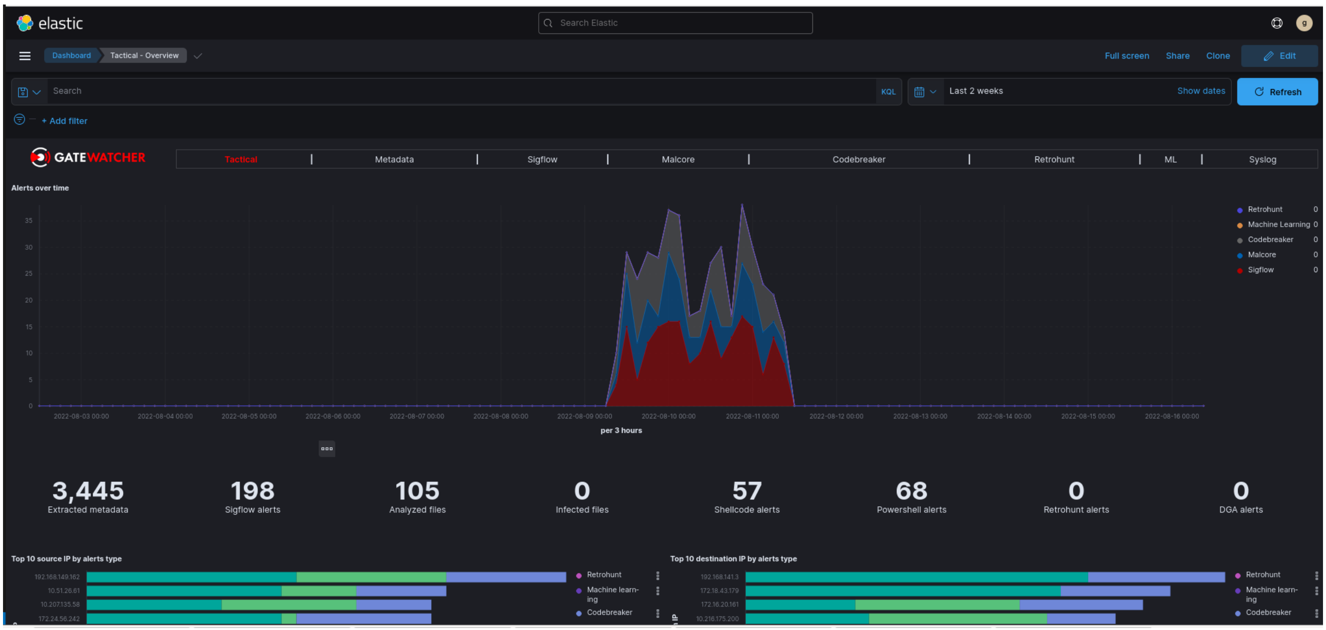
License key

This section enables managing the CTI licence.

| Item | Function |
|---|---|
| 1 | `LICENSE` section selection button |
| 2 | GCenter serial number |
| 3 | Validity of the CTI licence |
| 4 | `Save` button |
| 5 | `Licence key` input field |

## 5.6.35 `Admin-GCenter Trackwatch logs` screen of the legacy web UI

After pressing the `Trackwatch logs` command of the `Admin-GCenter` menu, a new window is opened, displaying the Kibana UI:



This interface is described in Kibana Interface section. See the *Overview of the Kibana GUI*.

## 5.7 Graphical API

### 5.7.1 Overview of the API interface

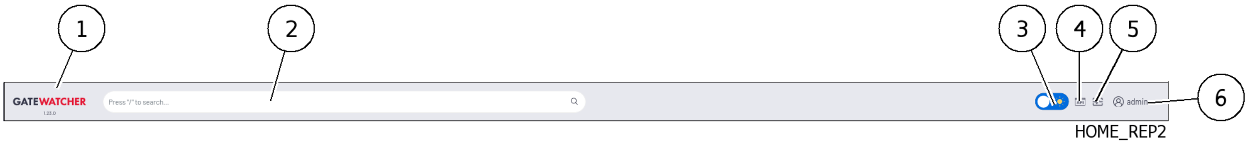
The API allows:

- Display the list by theme of existing endpoints
- To be able to filter this list
- Know all the information of each endpoint
- To run the endpoint,
- Know its curl command
- Know its URL request

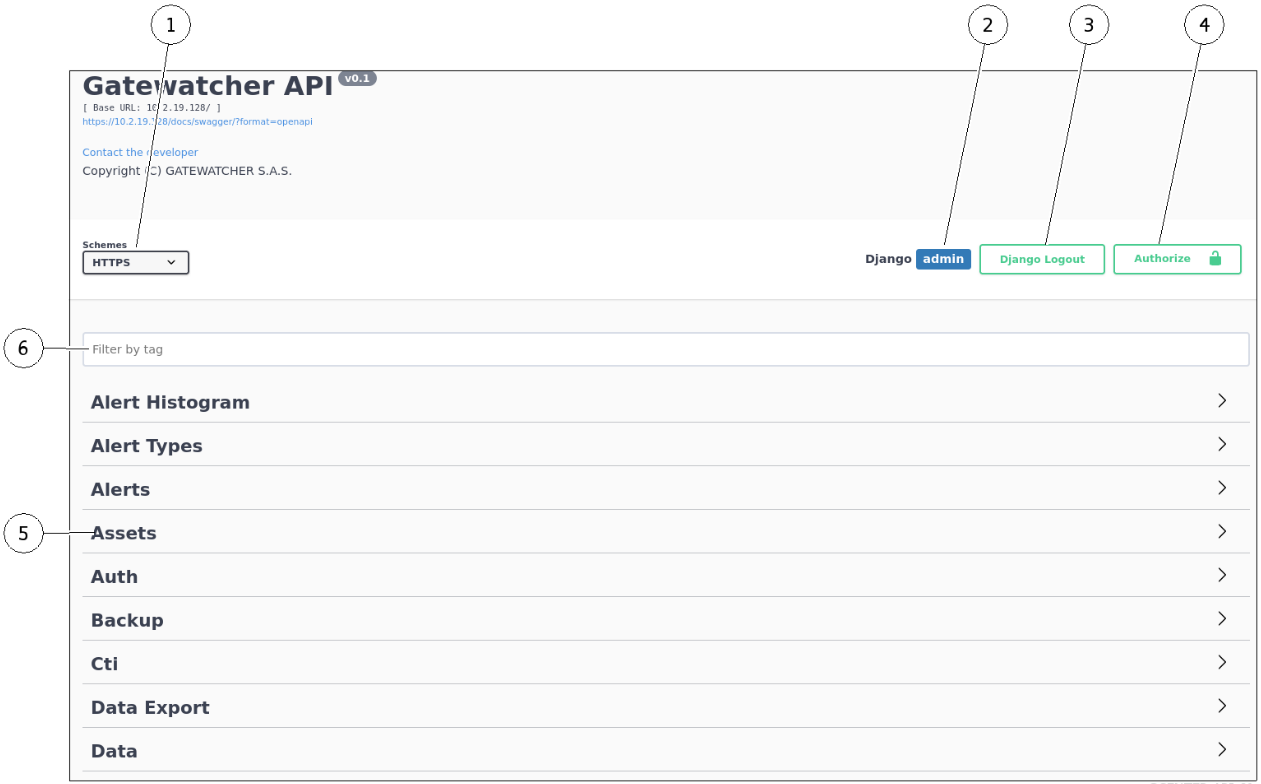
**Note:**

The API is named swagger.

Access to this interface is available in the title bar of the main interface.



After pressing the `API` button (4) of the title bar, the following screen is displayed. The window includes:



Gatewatcher API v0.1

[ Base URL: 10.2.19.128/ ]

https://10.2.19.128/docs/swagger/?format=openapi

Contact the developer

Copyright (C) GATEWATCHER S.A.S.

Schemes

HTTPS

Django admin Django Logout Authorize 🔒

Filter by tag

- Alert Histogram
- Alert Types
- Alerts
- Assets
- Auth
- Backup
- Cti
- Data Export
- Data

GCENTER-API-01

| Item | Description |
|---|---|
| 1 | `Schemes`: parameter indicating the protocol used (HTTPS) |
| 2 | Current account name: here account administrator |
| 3 | `Django Logout` button: allows to exit the API |
| 4 | Button `Authorize`: allows to define the necessary authentication in curl commands |
| 5 | Endpoints are sorted by theme (tag) |
| 6 | Filtration field: allows to filter themes |

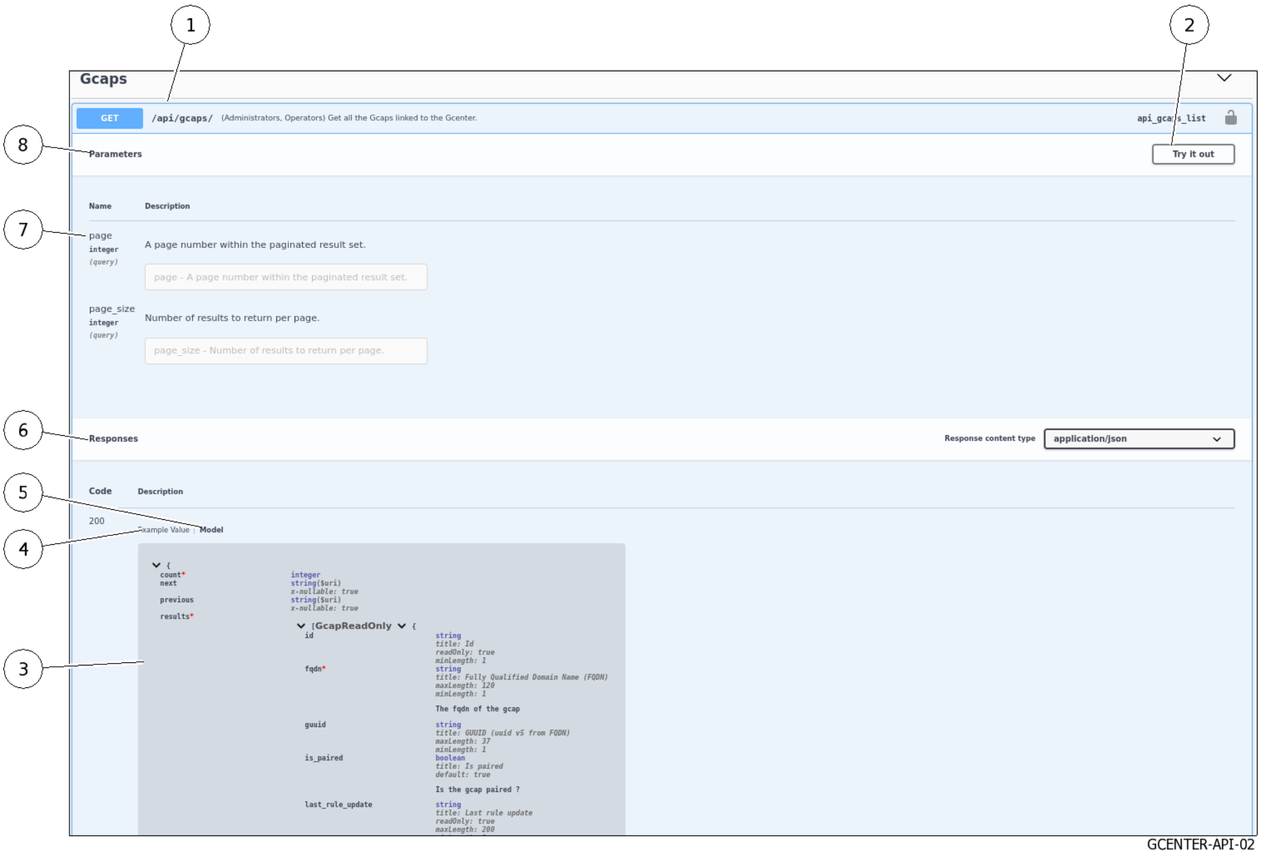
In this interface, all API endpoints are available and usable.
The use of the different endpoints is subject to the same rights as in the GCenter web interfaces.

**Note:**

A feature requiring administrator rights cannot be used by a user with only operator rights.

### 5.7.1.1 Detail for an endpoint

The information displayed for an endpoint is as follows:



Gcaps

GET /api/gcaps/ (Administrators, Operators) Get all the Gcaps linked to the Gcenter.

Parameters

| Name | Description |
|---|---|
| page<br>integer<br>*(query)* | A page number within the paginated result set.<br>page - A page number within the paginated result set. |
| page_size<br>integer<br>*(query)* | Number of results to return per page.<br>page_size - Number of results to return per page. |

Responses

Response content type: application/json

| Code | Description |
|---|---|
| 200 | Example Value \| Model |

```
{
count*                 integer
next                   string($uri)
                       x-nullable: true
previous               string($uri)
                       x-nullable: true
results*
                        [GcapReadOnly {
                         id                  string
                                             title: Id
                                             readOnly: true
                                             minLength: 1
                         fqdn*               string
                                             title: Fully Qualified Domain Name (FQDN)
                                             maxLength: 120
                                             minLength: 1

                                             The fqdn of the gcap

                         guuid               string
                                             title: GUUID (uuid v5 from FQDN)
                                             maxLength: 37
                                             minLength: 1
                         is_paired           boolean
                                             title: Is paired
                                             default: true

                                             Is the gcap paired ?

                         last_rule_update    string
                                             title: Last rule update
                                             readOnly: true
                                             maxLength: 200
```

GCENTER-API-02

| Item | Description |
|---|---|
| 1 | Title line. It includes the action (here GET), the name of the endpoint (here/api/gcaps), the accesses (here Administrators and Opertors), the description of the endpoint |
| 2 | `Try it out` button: runs the endpoint with current parameters |
| 8 | Field `Parameters`: displays the optional or mandatory parameters to execute the query. For mandatory parameters, refer to the box (6).<br>This area includes the parameters needed for the selected API. In this example, there are two: the page number and the number of results per page. |
| 7 | • Parameter `page`: enter a page number. This example depends on the API |
| 6 | • `Responses` area: area that displays information based on whether or not the `Try it out` button has been activated |

**Note:**

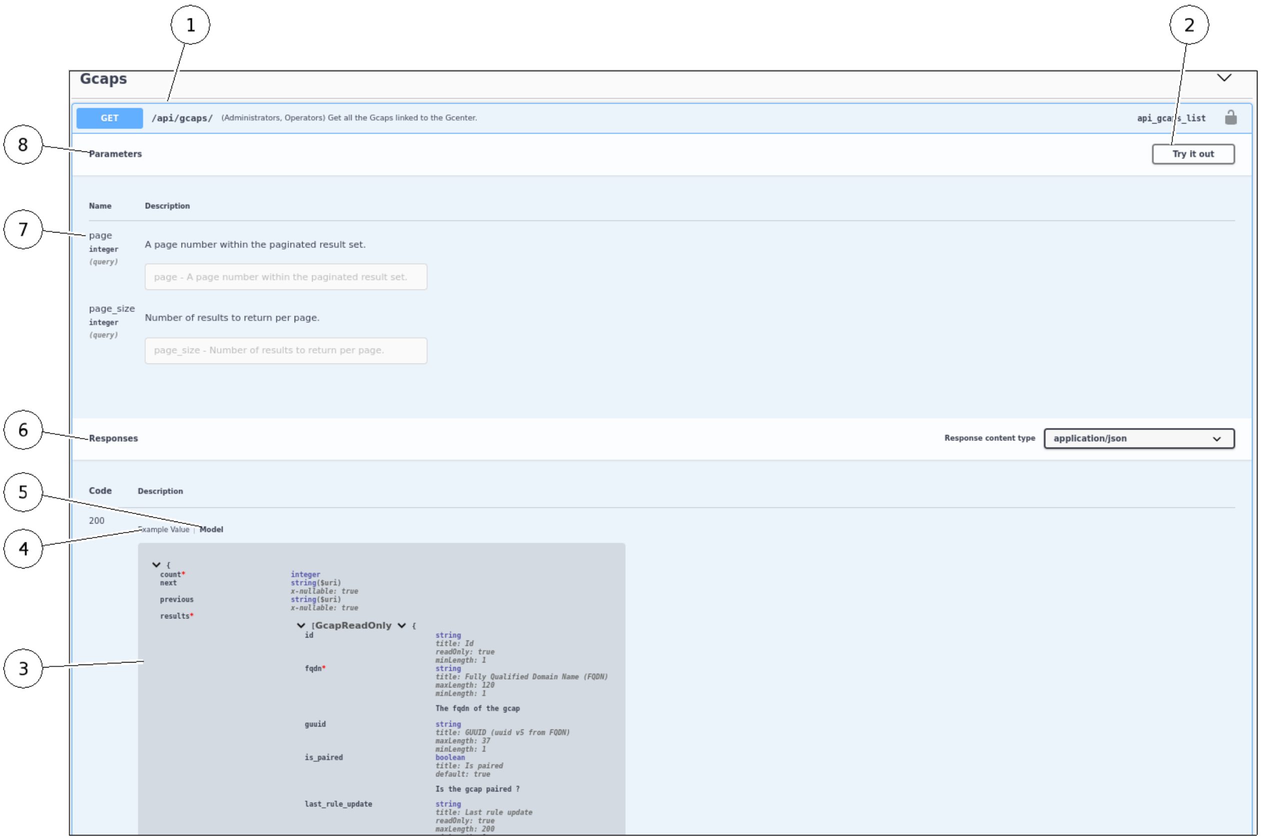
If a parameter is mandatory, an asterisk with `required` is displayed.

**Note:**

In this screen, it is not possible to enter parameters. To do this, you must execute the query.

#### 5.7.1.1.1 Zone `Responses` if the `Try it out` button is not activated

If the `Try it out` button is not activated then the `Responses` zone contains the information for the expected response:



Gcaps

GET /api/gcaps/ (Administrators, Operators) Get all the Gcaps linked to the Gcenter. api_gcaps_list

Parameters

| Name | Description |
|---|---|
| page<br>integer<br>*(query)* | A page number within the paginated result set.<br>page - A page number within the paginated result set. |
| page_size<br>integer<br>*(query)* | Number of results to return per page.<br>page_size - Number of results to return per page. |

Responses

Response content type application/json

| Code | Description |
|---|---|
| 200 | Example Value \| **Model** |

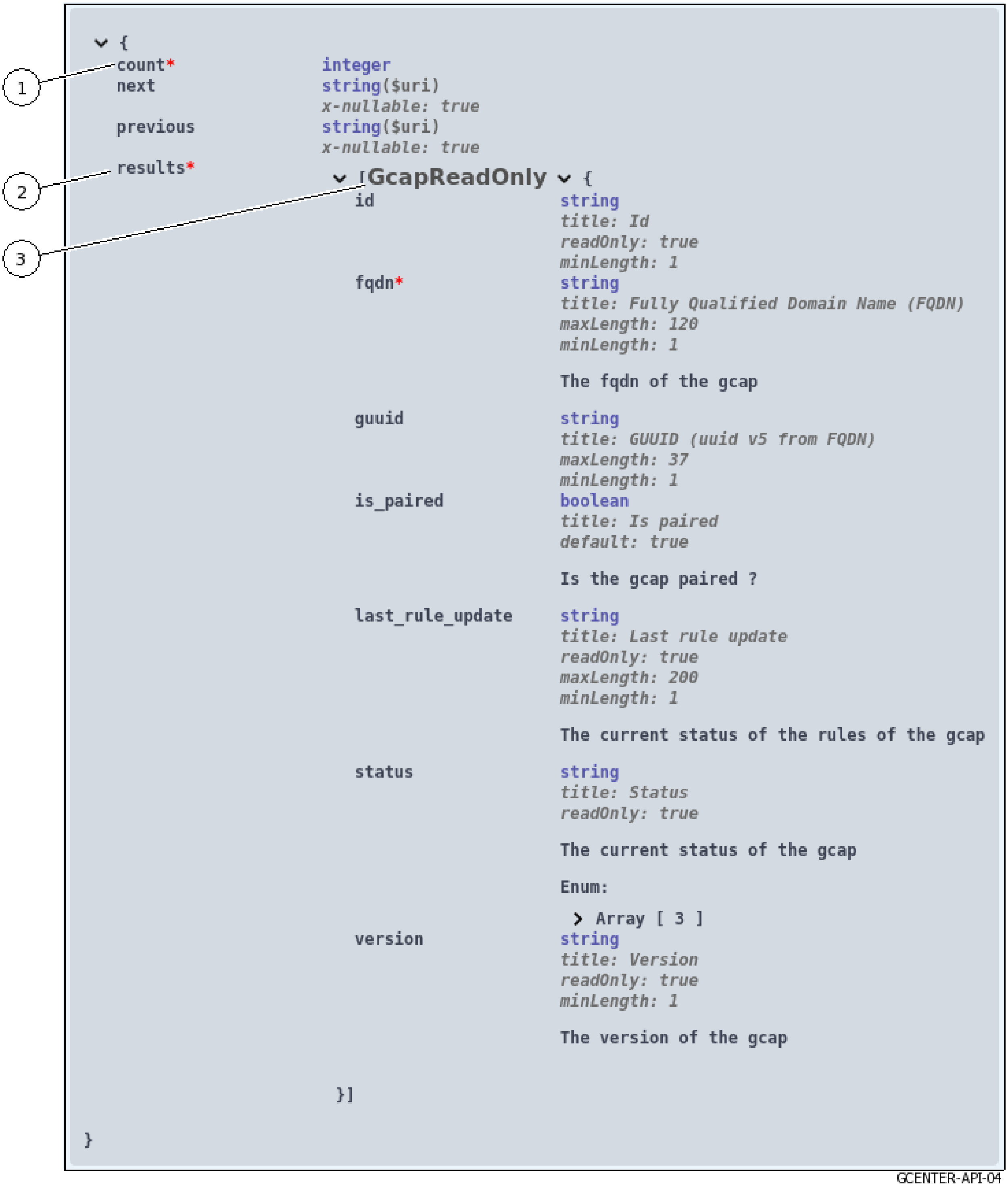
```
{
count*              integer
next                string($uri)
                    x-nullable: true
previous            string($uri)
                    x-nullable: true
results*
                     [GcapReadOnly {
                      id                        string
                                                title: Id
                                                readOnly: true
                                                minLength: 1
                      fqdn*                     string
                                                title: Fully Qualified Domain Name (FQDN)
                                                maxLength: 120
                                                minLength: 1

                                                The fqdn of the gcap

                      guuid                     string
                                                title: GUUID (uuid v5 from FQDN)
                                                maxLength: 37
                                                minLength: 1
                      is_paired                 boolean
                                                title: Is paired
                                                default: true

                                                Is the gcap paired ?

                      last_rule_update          string
                                                title: Last rule update
                                                readOnly: true
                                                maxLength: 200
```

GCENTER-API-02

| Item | Description |
|---|---|
| 5 | Link `Model`: by clicking on this text, the window (3) displays the model of the expected answer |
| 4 | Link `Example Value`: by clicking on this text, the window (3) displays an example of the expected response with values for example.<br>Values are, for type **integer** (value 0), for type string (value = string), for type **boolean** (value = true) |
| 3 | Field of view: contains the content selected by the active option (4) or (5).<br>An example of content is given below. |

#### 5.7.1.1.1.1 Sample Output Template

The output model gives the structure of the data that will be displayed as output after execution of the request.



```
{
count*                  integer
next                    string($uri)
                        x-nullable: true
previous                string($uri)
                        x-nullable: true
results*
                     [GcapReadOnly {
                        id                      string
                                                title: Id
                                                readOnly: true
                                                minLength: 1
                        fqdn*                   string
                                                title: Fully Qualified Domain Name (FQDN)
                                                maxLength: 120
                                                minLength: 1

                                                The fqdn of the gcap

                        guuid                   string
                                                title: GUUID (uuid v5 from FQDN)
                                                maxLength: 37
                                                minLength: 1
                        is_paired               boolean
                                                title: Is paired
                                                default: true

                                                Is the gcap paired ?

                        last_rule_update        string
                                                title: Last rule update
                                                readOnly: true
                                                maxLength: 200
                                                minLength: 1

                                                The current status of the rules of the gcap

                        status                  string
                                                title: Status
                                                readOnly: true

                                                The current status of the gcap

                                                Enum:
                                                 > Array [ 3 ]
                        version                 string
                                                title: Version
                                                readOnly: true
                                                minLength: 1

                                                The version of the gcap

                     }]
}
```

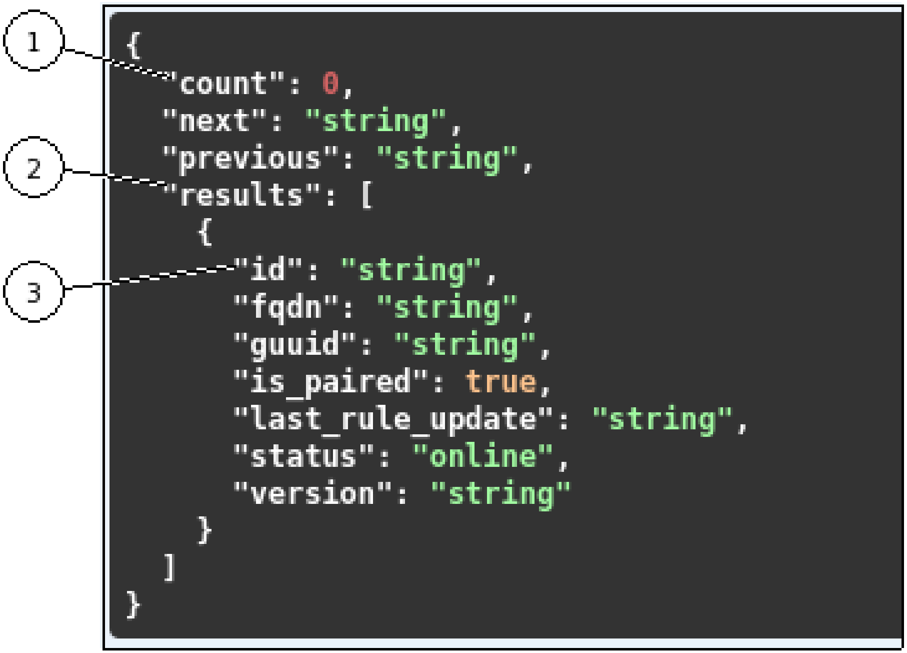
GCENTER-API-04

| Item | Description |
|---|---|
| 1 | `count`: number. For this parameter, its characteristics are indicated (integer). |
| 2 | `results`: expected results |
| 3 | `GcapReadOnly`: GCap settings<br>For each parameter (id, fqdn,is_paired...), the characteristics are displayed |

#### 5.7.1.1.2 Example with default values

In this example, the information is displayed with the following defaults:

- Parameters of type **integer** are displayed with `0`
- Parameters of type **string** are displayed with `string` text
- Parameters of type **boolean** are displayed with `true` text



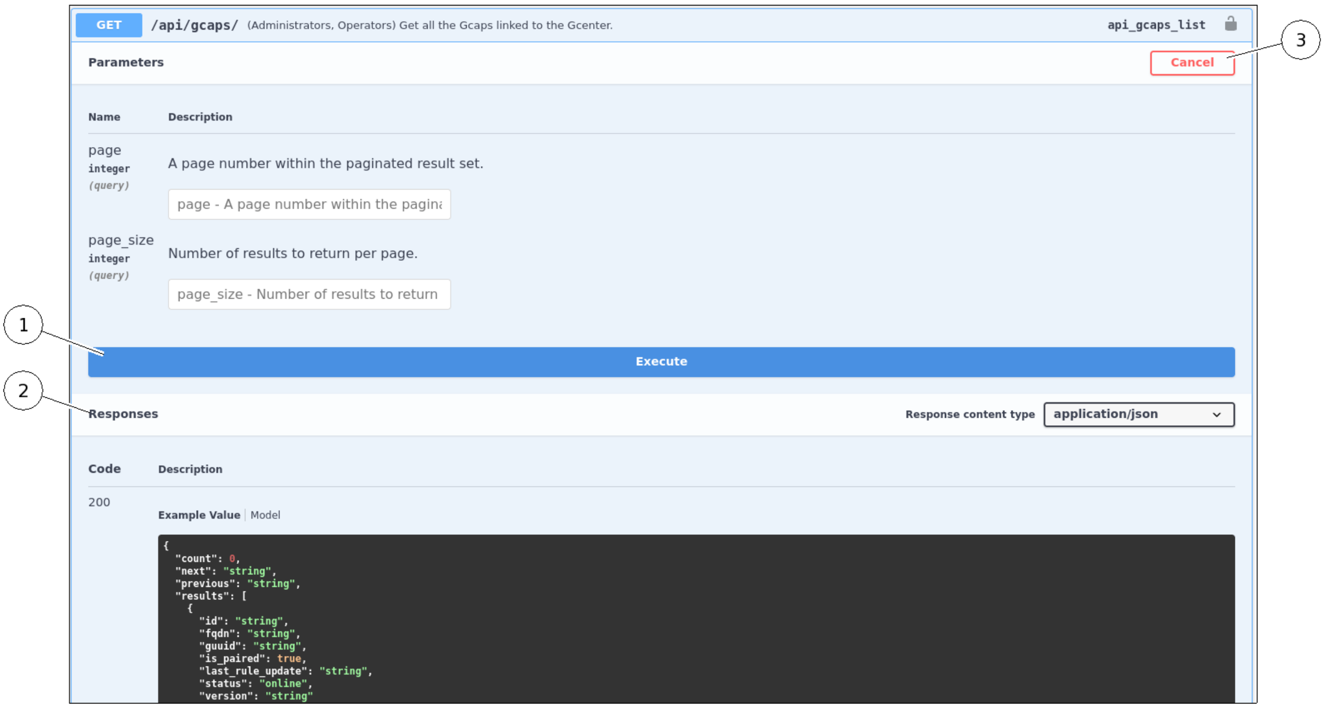
```
{
  "count": 0,
  "next": "string",
  "previous": "string",
  "results": [
    {
      "id": "string",
      "fqdn": "string",
      "guuid": "string",
      "is_paired": true,
      "last_rule_update": "string",
      "status": "online",
      "version": "string"
    }
  ]
}
```

GCENTER-API-03

The marking is the same as in the output model.

#### 5.7.1.1.3 Zone `Responses` if the `Try it out button is activated

After clicking the `Try it out` button, the parameter entry area is activated.
The following screen is displayed:



/api/gcaps/ (Administrators, Operators) Get all the Gcaps linked to the Gcenter. api_gcaps_list

Parameters

| Name | Description |
|---|---|
| page<br>integer<br>*(query)* | A page number within the paginated result set.<br>page - A page number within the pagin: |
| page_size<br>integer<br>*(query)* | Number of results to return per page.<br>page_size - Number of results to return |

Responses

Response content type: application/json

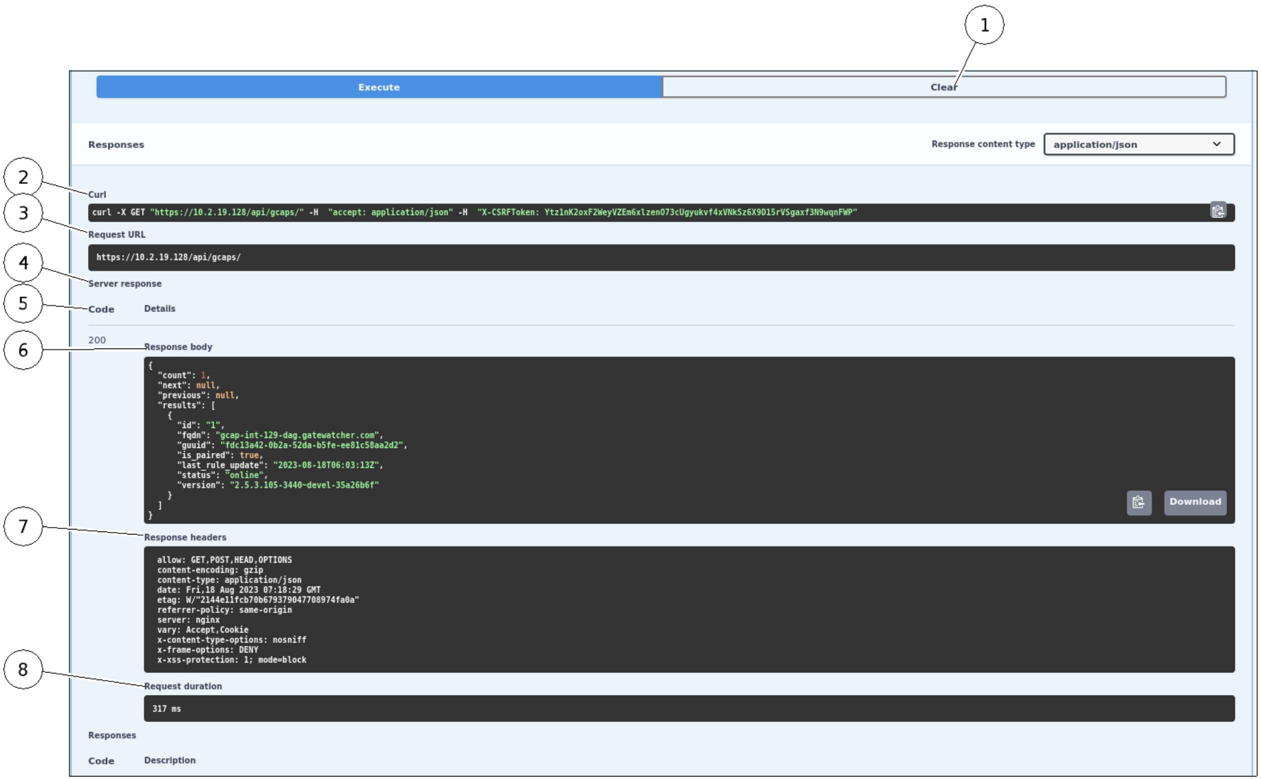
| Code | Description |
|---|---|
| 200 | Example Value \| Model |

```
{
  "count": 0,
  "next": "string",
  "previous": "string",
  "results": [
    {
      "id": "string",
      "fqdn": "string",
      "guuid": "string",
      "is_paired": true,
      "last_rule_update": "string",
      "status": "online",
      "version": "string"
```

GCENTER-API-05

| Item | Description |
|---|---|
| 1 | `Execute` button: to execute the query with the current parameters |
| 2 | `Cancel` button: cancels the request |
| 3 | `Responses` zone has not changed |

After clicking the `Execute` button, the query is launched and the next window is displayed.



Responses

Response content type: application/json

Curl

```
curl -X GET "https://10.2.19.128/api/gcaps/" -H  "accept: application/json" -H  "X-CSRFToken: Ytz1nK2oxF2WeyVZEm6xlzen073cUgyukvf4xVNkSz6X9D15rVSgaxf3N9wqnFWP"
```

Request URL

```
https://10.2.19.128/api/gcaps/
```

Server response

| Code | Details |
|---|---|
| 200 | Response body |

```
{
  "count": 1,
  "next": null,
  "previous": null,
  "results": [
    {
      "id": "1",
      "fqdn": "gcap-int-129-dag.gatewatcher.com",
      "guuid": "fdc13a42-0b2a-52da-b5fe-ee81c58aa2d2",
      "is_paired": true,
      "last_rule_update": "2023-08-18T06:03:13Z",
      "status": "online",
      "version": "2.5.3.105-3440~devel-35a26b6f"
    }
  ]
}
```

Response headers

```
 allow: GET,POST,HEAD,OPTIONS
 content-encoding: gzip
 content-type: application/json
 date: Fri,18 Aug 2023 07:18:29 GMT
 etag: W/"2144e11fcb70b679379047708974fa0a"
 referrer-policy: same-origin
 server: nginx
 vary: Accept,Cookie
 x-content-type-options: nosniff
 x-frame-options: DENY
 x-xss-protection: 1; mode=block
```

Request duration

```
317 ms
```

Responses

| Code | Description |
|---|---|

GCENTER-API-06

| Benchmark | Description |
|---|---|
| 1 | `` `Clear` `` button: to return to the state before execution |
| 2 | Display Area `` `Curl` ``: displays the Curl query |
| 3 | Display area `` `URL` ``: displays the URL request |
| 4 | Display Area `` `Server response` ``: displays the server response to the request. It includes the following |
| 5 | • `` `Code` ``: if code 200 then execution is ok.<br>If the message `` `code 400 Undocumented Error Bad Request` `` is displayed, verify that the required parameters are entered. |
| 6 | • `` `Responses body` ``: in this section the information requested is displayed |
| 7 | • `` `Responses headers` ``: field detailing the answer header |
| 8 | • `` `Responses headers` ``: value in ms of the duration of the request |

## 5.7.2 Endpoints list

**Note:**

In the table below the legend is:

- Ope : operators role
- Adm : administrator role
- WAuth : Without Authentication
- AUser : Authenticated User

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| Alert Histogram | alert-types/ | GET | Ope | Returns a heat map aggregation |
| Alert Types | alert-types/ | GET | Ope | Get the sorted alert type by risk / number of alerts |
| Alerts | alerts/ | GET | Ope | Get the alerts |
| Alerts | alerts/ | DELETE | Adm | Delete the alerts that occurred in the given date range |
| Alerts | alerts/clusters/ | GET | Ope | Returns alert clusters |
| Alerts | alerts/{pk_or_uuid}/ | GET | Ope | Get one alert details |
| Alerts | alerts/{uuid}/note/ | PUT | Ope | Update the note for a given instance |
| Alerts | alerts/{uuid}/note/ | DELETE | Ope | Clear the note content for a given instance |
| Alerts | alerts/{uuid}/tags/ | GET | Ope | Get the tags for a given instance |
| Alerts | alerts/{uuid}/tags/ | PUT | Ope | Update the tags for a given instance |
| Assets | assets/ | GET | Ope | Retrieves a list of assets |
| Assets | assets/{name}/ | GET | Ope | Retrieve a specific user data |
| Assets | assets/{name}/alerts/ | GET | Ope | Get the alerts for a specific asset |
| Assets | assets/{name}/clusters/ | GET | Ope | Returns alert clusters for the corresponding asset |
| Assets | assets/{name}/ips/ | GET | Ope | Get the list of ips related to an asset |

suite sur la page suivante

Table 15 – suite de la page précédente

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| Assets | assets/{name}/note/ | PUT | Ope | Update the note for a given instance |
| Assets | assets/{name}/note/ | DELETE | Ope | Clear the note content for a given instance. |
| Assets | assets/{name}/tags/ | GET | Ope | Get the tags for a given instance |
| Assets | assets/{name}/tags/ | PUT | Ope | Update the tags for a given instance |
| Assets | assets/{name}/urls/ | GET | Ope | Get the list of urls related to an asset through an alert |
| Auth | auth/login/ | POST | WAuth | Initiate a new session |
| Auth | auth/logout/ | POST | WAuth | Terminate session |
| Auth | auth/tokens/ | GET | Adm | Get all the API authentication Tokens |
| Auth | auth/tokens/ | POST | Adm | Generate an API authentication token |
| Auth | auth/tokens/{id}/ | GET | Adm | Get a API authentication token data |
| Auth | auth/tokens/{id}/ | DELETE | Adm | Delete an API authentication token |
| Backup | backup/ | GET | Adm | Get the backup list |
| Backup | backup/ | POST | Adm | Create a backup |
| Backup | backup/config/ | GET | Adm | Get the Backup config |
| Backup | backup/config/ | PUT | Adm | Update the Backup config |
| Backup | backup/config/check/ | POST | Adm | Test the remote scheduled config |
| Backup | backup/restore/ | POST | Adm | Restore a backup with file upload |
| Backup | backup/status/ | GET | Adm | Get the backup status |
| Backup | backup/{name}/download/ | GET | Adm | Download a backup |
| Backup | backup/{name}/restore/ | POST | Adm | Restore a backup |
| Cti | cti/license/ | GET | Adm | Get the LIS license key and details |
| Cti | cti/license/ | PUT | Adm | Update the LIS license key |
| Cti | cti/settings/ | GET | Adm | Get the current LIS configuration |
| Cti | cti/settings/ | PUT | Adm | Update the current LIS configuration |
| Data Export | data-export/netdata/ | GET | Adm | Get the current netdata export configuration |
| Data Export | data-export/netdata/ | PUT | Adm | Update the current netdata export configuration |
| Data Export | data-export/syslog/{id}/ | GET | Adm | Get the current syslog export configuration |
| Data Export | data-export/syslog/{id}/ | PUT | Adm | Update the current syslog export configuration |
| Data | data/es/search/ | POST | Adm, Ope | Execute an Elasticsearch Search on Gcenter data |
| Delete Data | delete-data/ | GET | Adm, Ope | Get the delete data config |
| Delete Data | delete-data/ | PUT | Adm | Update the delete data config |
| Delete Data | delete-data/ | DELETE | Adm | Deletes data |
| Delete Data | delete-data/status/ | GET | Adm | Get the data deletion status |
| Device Types | device-types/ | GET | Ope | Retrieves the list of asset types |
| Dga Detection | dga-detection/settings/ | GET | Adm | Get the DGA detection management settings |
| Dga Detection | dga-detection/settings/ | PUT | Adm | Update the DGA detection management settings |
| Dga Detection | dga-detection/{list_type}-list/ | GET | Adm | Get the domain name white/black list |
| Dga Detection | dga-detection/{list_type}-list/ | POST | Adm | Add a domain name to the white/black list |
| Dga Detection | dga-detection/{list_type}-list/load | PUT | Adm | Update the white/black list from a csv file |
| Dga Detection | dga-detection/{list_type}-list/{domain_name} | DELETE | Adm | Delete a domain name from the white/black list |

suite sur la page suivante

Table 15 – suite de la page précédente

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| Diagnostics | diagnostics/logs/ | GET | Adm | Download the file |
| Diagnostics | diagnostics/logs/ | PUT | Adm | Generate/Update the file asynchronously |
| Diagnostics | diagnostics/logs/status/ | GET | Adm | Get the file's generation status |
| Diagnostics | diagnostics/tech-support/ | GET | Adm | Download the file |
| Diagnostics | diagnostics/tech-support/ | PUT | Adm | Generate/Update the tech support file asynchronously |
| Diagnostics | diagnostics/tech-support/status/ | GET | Adm | Get the file's generation status |
| Entities | entities/ | DELETE | Adm | Delete the entities records that occurred in the given date range |
| Entities | entities/count/ | GET | Ope | Retrieve the total count of the different entities for the given date range |
| External Modules | external-modules/hurukai/ | GET | Adm, Ope | Get the Hurukai configuration |
| External Modules | external-modules/hurukai/ | PUT | Adm | Update the Hurukai configuration |
| External Modules | external-modules/hurukai/ioc/ | POST | Ope | Push IOC to hurukai server |
| External Modules | external-modules/hurukai/ioc/{id}/ | GET | Ope | Search processes |
| External Modules | external-modules/intelligence/ | GET | Adm, Ope | Get the intelligence interconnection configuration |
| External Modules | external-modules/intelligence/ | PUT | Adm | Update the intelligence interconnection configuration |
| External Modules | external-modules/intelligence/test/ | GET | Adm | Tests the interconnection with the current saved configuration |
| External Modules | external-modules/misp/ | GET | Adm, Ope | Get the MISP configuration |
| External Modules | external-modules/misp/ | PUT | Adm | Update the MISP configuration |
| External Modules | external-modules/misp/updates/ | GET | Ope | Get all MISP generations |
| External Modules | external-modules/misp/updates/ | POST | Ope | Add a MISP generation |
| External Modules | external-modules/misp/updates/settings/ | GET | Ope | Get the automatic generation settings |
| External Modules | external-modules/misp/updates/settings/ | PUT | Ope | Set the automatic generation settings |
| Gcaps | gcaps/ | GET | Adm, Ope | Get all the Gcaps linked to the Gcenter |
| Gcaps | gcaps/ | POST | Adm | Pair a new gcap |
| Gcaps | gcaps/profile-template/ | GET | Adm | Get a Gcaps template profile configuration |
| Gcaps | gcaps/profile-template/ | PUT | Adm | Update a Gcaps profile configuration |
| Gcaps | gcaps/{id}/ | GET | Adm, Ope | Get a Gcap's data |
| Gcaps | gcaps/{id}/ | DELETE | Adm | Delete a GCap |
| Gcaps | gcaps/{id}/files-rules/ | GET | Ope | Get all files rules of a Gcap |
| Gcaps | gcaps/{id}/files-rules/ | POST | Ope | Create a Gcap files rule configuration |
| Gcaps | gcaps/{id}/files-rules/load/ | POST | Ope | Update the gcap files rule from a csv file |
| Gcaps | gcaps/{id}/files-rules/template/ | GET | Ope | Get the csv template of the gcap files rules config |
| Gcaps | gcaps/{id}/files-rules/{id_rule}/ | GET | Ope | Get a Gcap files rule configuration |

suite sur la page suivante

Table 15 – suite de la page précédente

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| Gcaps | gcaps/{id}/files-rules/{id_rule}/ | PUT | Ope | Update a Gcap files rule configuration |
| Gcaps | gcaps/{id}/files-rules/{id_rule}/ | DELETE | Ope | Remove a Gcap files rule configuration |
| Gcaps | gcaps/{id}/flows-timeouts/ | GET | Ope | Get all flows timeouts of a Gcap |
| Gcaps | gcaps/{id}/flows-timeouts/{id_flow}/ | GET | Ope | Get a flows timeouts details of a Gcap |
| Gcaps | gcaps/{id}/interfaces | GET | Adm, Ope | Get the Gcap's available network interfaces |
| Gcaps | gcaps/{id}/multi-tenant-interfaces/rulesets/ | GET | Ope | Get all the interface ruleset configurations of a Gcap |
| Gcaps | gcaps/{id}/multi-tenant-interfaces/rulesets/ | PUT | Ope | Update the current interface ruleset configurations of a Gcap |
| Gcaps | gcaps/{id}/multi-tenant-interfaces/status/ | GET | Ope | Get the status of Gcap's multi tenant by interface rulesets configurations |
| Gcaps | gcaps/{id}/multi-tenant-vlans/rulesets | GET | Ope | Get all the VLAN ruleset configurations of a Gcap |
| Gcaps | gcaps/{id}/multi-tenant-vlans/rulesets | POST | Ope | Create a Gcap's VLAN ruleset configuration |
| Gcaps | gcaps/{id}/multi-tenant-vlans/rulesets/{id_vlan} | GET | Ope | Get a Gcap's VLAN ruleset configuration |
| Gcaps | gcaps/{id}/multi-tenant-vlans/rulesets/{id_vlan} | PUT | Ope | Update a Gcap's VLAN ruleset configuration |
| Gcaps | gcaps/{id}/multi-tenant-vlans/rulesets/{id_vlan} | DELETE | Ope | Delete a Gcap's VLAN ruleset configuration |
| Gcaps | gcaps/{id}/multi-tenant-vlans/status/ | GET | Ope | Get the status of Gcap's multi tenant by VLAN rulesets configurations |
| Gcaps | gcagcaps/{id}/network-variables | GET | Ope | Get all network variables of a Gcap |
| Gcaps | gcaps/{id}/network-variables/load | PUT | Ope | Update the network variables of a gcap from a csv file |
| Gcaps | gcaps/{id}/network-variables/template | GET | Ope | Get the csv template of the gcap network variables |
| Gcaps | gcaps/{id}/network-variables/{id_net} | GET | Ope | Get network variables of a Gcap |
| Gcaps | gcaps/{id}/network-variables/{id_net}/ | PUT | Ope | Update network variables of a Gcapp |
| Gcaps | gcaps/{id}/packet-filters/ | GET | Ope | Get the list of the packet filtering configuration of a Gcap |
| Gcaps | gcaps/{id}/packet-filters/ | POST | Ope | Add a packet filtering configuration for a Gcap |
| Gcaps | gcaps/{id}/packet-filters-default-vlans | GET | Ope | Get all the packet filters default vlan of gcap interfaces |
| Gcaps | gcaps/{id}/packet-filters-default-vlans/{interface} | GET | Ope | Get the packet filters default vlan of a gcap interface |
| Gcaps | gcaps/{id}/packet-filters-default-vlans/{interface} | PUT | Ope | Update the packet filters default vlan of a gcap interface |
| Gcaps | gcaps/{id}/packet-filters/{packet} | GET | Ope | Get a packet filtering configuration of a Gcap |
| Gcaps | gcaps/{id}/packet-filters/{packet} | DELETE | Ope | Remove a packet filtering configuration of a Gcap |
| Gcaps | gcaps/{id}/profile/ | GET | Ope | Get a Gcap's profile configuration |
| Gcaps | gcaps/{id}/profile/ | PUT | Ope | Update a Gcap's profile configuration |

suite sur la page suivante

Table 15 – suite de la page précédente

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| Gcaps | gcaps/{id}/profile/memcap/ | GET | Ope | Get a Gcap's memcap profile configuration |
| Gcaps | gcaps/{id}/profile/memcap/ | PUT | Ope | Update a Gcap's memcap profile configuration |
| Gcaps | gcaps/{id}/repair/ | POST | Adm | Repair a GCap |
| Gcaps | gcaps/{id}/reset-profile/ | POST | Ope | Reset the gcap profile |
| Gcaps | gcaps/{id}/reset-tenant/ | POST | Ope | Reset the single/multi tenant configuration |
| Gcaps | gcaps/{id}/ruleset/ | GET | Ope | Get a gcap full ruleset configuration |
| Gcaps | gcaps/{id}/ruleset/apply/ | POST | Ope | Apply a gcap configuration if changed |
| Gcaps | gcaps/{id}/single-tenant/ | GET | Ope | Get the current single tenant configuration of a Gcap |
| Gcaps | gcaps/{id}/single-tenant/ | PUT | Ope | Update the current single tenant configuration of a Gcap |
| Gcenter | gcenter/ssh-rsa-key/ | PUT | Ope | Get the host pub key |
| Gscan | gscan/history/ | GET | Ope | Get all the previous Gscan results |
| Gscan | gscan/history/{id}/ | GET | Ope | Get a previous Gscan history result's details |
| Gscan | gscan/malcore/ | POST | Ope | Scan a file with malcore |
| Gscan | gscan/powershell/ | POST | Ope | Scan a file with powershell |
| Gscan | gscan/shellcode/ | POST | Ope | Scan a file with shellcode |
| Gscan | gscan/shellcode/deep-config/ | GET | Ope | Get the shellcode deep scan configuration |
| Gscan | gscan/shellcode/deep-config/ | PUT | Ope | Update the shellcode deep scan configuration |
| Gum | gum/config/ | GET | Adm | Get the gum config |
| Gum | gum/config/ | POST | Adm | Try to run the scheduled update gum task config now |
| Gum | gum/config/ | PUT | Adm | Change the gum config |
| Gum | gum/config/check/ | POST | Adm | Test the remote scheduled config |
| Gum | gum/software-updates/ | GET | Adm | Get the software update uploaded files list |
| Gum | gum/software-updates/ | POST | Adm | Upload a new software update gwp file |
| Gum | software-updates/{name}/ | POST | Adm | Apply a software update uploaded file |
| Gum | gum/status/ | GET | Adm | Get the gum progress bar status |
| Gum | gum/threat-db-update/ | POST | Adm | Upload a new threat db update gwp file |
| Ignore Lists | ignore-lists/asset-names/ | GET | Ope | Get all the ignored asset names |
| Ignore Lists | ignore-lists/asset-names/ | POST | Ope | Add a new ignored asset name |
| Ignore Lists | ignore-lists/asset-names/{id}/ | DELETE | Ope | Remove one ignored asset name |
| Ignore Lists | ignore-lists/hints/asset-ips/ | GET | Ope | Get all the asset IP ignore hints (IP associated to more than 4 assets) |
| Ignore Lists | ignore-lists/hints/asset-mac-addresses/ | GET | Ope | Get all the asset MAC ignore hints (MAC associated to more than 4 assets) |
| Ignore Lists | ignore-lists/hints/kuser-ips/ | GET | Ope | Get all the kerberos user IP ignore hints (IP associated to more than 4 kusers) |
| Ignore Lists | ignore-lists/kuser-ips/ | GET | Ope | Get all the ignored kerberos user IPs |
| Ignore Lists | ignore-lists/kuser-ips/ | POST | Ope | Add a new ignored kerberos user IP |
| Ignore Lists | ignore-lists/kuser-ips/{id}/ | DELETE | Ope | Remove one ignored kerberos user IP |
| Ignore Lists | ignore-lists/kuser-names/ | GET | Ope | Get all the ignored kerberos user names |
| Ignore Lists | ignore-lists/kuser-names/ | POST | Ope | Add a new ignored kerberos user name |

suite sur la page suivante

Table 15 – suite de la page précédente

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| Ignore Lists | ignore-lists/kuser-names/{id}/ | DELETE | Ope | Remove one ignored kerberos user name |
| Ignore Lists | ignore-lists/mac-addresses/ | GET | Ope | Get all the ignored MAC addresses |
| Ignore Lists | ignore-lists/mac-addresses/ | POST | Ope | Add a new ignored MAC address |
| Ignore Lists | ignore-lists/mac-addresses/{id}/ | DELETE | Ope | Remove one ignored MAC address |
| Kusers | kusers/ | GET | Ope | Retrieves a list of Kerberos Users |
| Kusers | kusers/{name}/ | GET | Ope | Retrieve a specific user data |
| Kusers | kusers/{name}/alerts/ | GET | Ope | Get the alerts for a specific kerberos user |
| Kusers | kusers/{name}/clusters/ | GET | Ope | Returns alert clusters for the corresponding kerberos user |
| Kusers | gukusers/{name}/ips/ | GET | Ope | Get the list of ips related to a user |
| Kusers | kusers/{name}/note/ | PUT | Ope | Update the note for a given instance |
| Kusers | kusers/{name}/note/ | DELETE | Ope | Clear the note content for a given instance |
| Kusers | kusers/{name}/tags/ | GET | Ope | Get the tags for a given instance |
| Kusers | kusers/{name}/tags/ | PUT | Ope | Update the tags for a given instance |
| Kusers | kusers/{name}/urls/ | GET | Ope | Get the list of urls related to a user through an alert |
| Ldap | ldap/advanced-settings/ | GET | Adm | Get the LDAP advanced settings |
| Ldap | ldap/advanced-settings/ | PUT | Adm | Update the LDAP advanced settings |
| Ldap | ldap/advanced-settings/ca-file/ | DELETE | Adm | Deletes the LDAP custom CA file |
| Ldap | ldap/server-bindings/ | GET | Adm | Get the LDAP server bindings settings |
| Ldap | ldap/server-bindings/ | PUT | Adm | Update the LDAP server bindings settings |
| Ldap | ldap/status/ | GET | Adm | Get the LDAP interconnection status |
| Ldap | ldap/status/ | PUT | Adm | Update the LDAP interconnection status |
| Ldap | ldap/user-mapping/ | GET | Adm | Get the LDAP users and groups mapping |
| Ldap | ldap/user-mapping/ | PUT | Adm | Update the LDAP users and groups mapping |
| License | license/ | GET | Adm, Ope | Get the GCenter license key and details |
| License | license/ | PUT | Adm | Update the GCenter license key and expiry alert |
| Main Domains | main-domains/ | GET | Adm, Ope | Get all the main domains |
| Main Domains | main-domains/ | POST | Adm, Ope | Add a new main domain |
| Main Domains | main-domains/{id}/ | GET | Adm, Ope | Get one main domain |
| Main Domains | main-domains/{id}/ | PUT | Adm, Ope | Update one main domain |
| Main Domains | main-domains/{id}/ | DELETE | Adm, Ope | Remove one main domain |
| Malcore | malcore/profiles/ | GET | Adm | Get the Malcore profiles list |
| Malcore | malcore/profiles/{name}/ | GET | Adm | Get the settings of a Malcore profile |
| Malcore | malcore/profiles/{name}/ | PUT | Adm | Update the settings of a Malcore profile |
| Malcore | malcore/settings/ | GET | Adm | Get the Malcore settings |
| Malcore | malcore/settings/ | PUT | Adm | Update the Malcore settings |

suite sur la page suivante

Table 15 – suite de la page précédente

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| Malcore | malcore/yara-rules/ | PUT | Adm | Experimental: upload a source file of YARA rules |
| Malcore | malcore/{list_type}-list/ | GET | Adm | Get the Malcore white/black list |
| Malcore | malcore/{list_type}-list/ | POST | Adm | Add a sha256 to the white/black list |
| Malcore | malcore/{list_type}-list/load | PUT | Adm | Update the white/black list from a csv file |
| Malcore | malcore/{list_type}-list/{sha256} | DELETE | Adm | Delete a sha256 from the white/black list |
| Mitre | mitre/ | GET | Ope | Get the mitres with the alerts aggregation |
| Ndr | ndr/settings/ | GET | Adm, Ope | Get the NDR settings |
| Ndr | ndr/settings/ | PATCH | Adm | Update the NDR settings |
| Net | net/certificate/ | POST | Adm | Get a certificate file's data |
| Ndr | net/interfaces/ | GET | Adm | Get the GCenter's available network interfaces |
| Ndr | interfaces/{name}/ | GET | Adm | Get a GCenter's network interface data |
| Netdata Polling | netdata-polling/ | GET | Adm | Get the netdata polling global configuration |
| Netdata Polling | netdata-polling/ | PUT | Adm | Update the netdata polling global configuration |
| Netdata Polling | netdata-polling/ips/ | GET | Adm | Get all the netdata polling cidr addresses |
| Netdata Polling | netdata-polling/ips/ | POST | Adm | Create a netdata polling cidr addresses |
| Netdata Polling | netdata-polling/ips/{id}/ | GET | Adm | Get a netdata polling cidr addresses |
| Netdata Polling | netdata-polling/ips/{id}/ | PUT | Adm | Update a netdata polling cidr addresses |
| Netdata Polling | netdata-polling/ips/{id}/ | DELETE | Adm | Delete a netdata polling cidr addresses |
| Notifications | notifications/errors/ | GET | Adm | Get all error notifications |
| Notifications | notifications/errors/{id}/acknowledge/ | PATCH | Adm | Acknowledge an error notification |
| Proxy | proxy/ | GET | Adm | Get the proxy settings configuration |
| Proxy | proxy/ | PUT | Adm | Update the proxy settings configuration |
| Raw Alerts | raw-alerts/{id}/ | GET | Ope | Get a raw alert data |
| Raw Alerts | raw-alerts/{id}/analysis-report/ | GET | Ope | Download the malcore alert analysis report file |
| Raw Alerts | raw-alerts/{id}/file/ | GET | Ope | Download the related alert file |
| Raw Alerts | raw-alerts/{id}/graph/ | GET | Ope | Download the shellcode alert graph file |
| Raw Alerts | raw-alerts/{id}/hexdump/ | GET | Ope | Generate the related codebreaker alert file hexdump |
| Raw Alerts | raw-alerts/{id}/hurukai/ | POST | Ope | Push the malcore alert to EDR |
| Raw Alerts | raw-alerts/{id}/hurukai/search/ | GET | Ope | Download the related alert file |
| Raw Alerts | raw-alerts/{id}/remote-report/ | POST | Ope | Generate the malcore alert remote report file |
| Relations | relations/ | GET | Ope | Get the graph of relations between users/assets |
| Relations | relations/top/ | GET | Ope | Get the graph of the relations between users/assets for the top N items by risk |
| Search | search/autocomplete/ | GET | Ope | Search the alerts info |
| Search | search/autocomplete/recent/ | GET | Ope | Get the user last search results |
| Search | search/autocomplete/recent/ | POST | Ope | Add one search result to the user's history |
| Search | search/autocomplete/recent/all/ | DELETE | Ope | Remove all user's search history |

suite sur la page suivante

Table 15 – suite de la page précédente

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| Settings | settings/ | GET | Adm | Get the global settings configuration |
| Settings | settings/ | PUT | Adm | Update the global settings configuration |
| Sigflow | sigflow/rulesets/ | GET | Adm, Ope | Get all the sigflow rulesets |
| SeSigflowttings | sigflow/rulesets/{id}/ | GET | Adm, Ope | Get a sigflow ruleset data |
| Signatures | signatures/ | GET | Ope | Get signatures |
| Ssl | ssl/ | GET | Adm | Get the Gcenter SSL security details |
| Ssl | ssl/certificate/ | GET | Adm | Get the Gcenter SSL Custom Certificate status |
| Ssl | ssl/certificate/ | PUT | Adm | Update the Gcenter SSL Custom Certificate |
| Ssl | ssl/certificate/ | DELETE | Adm | Reset the Gcenter SSL Custom Certificate |
| Ssl | ssl/dual-auth/ | GET | Adm | Get the Gcenter SSL Dual Authentication status |
| Ssl | ssl/dual-auth/ | PUT | Adm | Update the Gcenter SSL Dual Authentication |
| Ssl | ssl/dual-auth/ | DELETE | Adm | Reset the Gcenter SSL Dual Authentication |
| Static Ip Asset Name | static-ip-asset-name/ | GET | Adm, Ope | Get all the IP bound to a specific asset |
| Static Ip Asset Name | static-ip-asset-name/ | POST | Adm, Ope | Add a new IP bound to a specific asset |
| Static Ip Asset Name | static-ip-asset-name/{id}/ | DELETE | Adm, Ope | Remove unbound an IP from a specific asset |
| Status | status/api/ | GET | WAuth | Check if the API is working |
| Status | status/engine-queues/ | GET | Adm, Ope | Get the engine queues status for all Gcaps |
| Status | status/engine-queues/{gcap_name}/ | GET | Adm, Ope | Get the engine queues status for a Gcap |
| Status | status/engines-health/ | GET | Adm, Ope | Get analyser engines statuses |
| Status | status/engines/{engine_name}/ | GET | Adm, Ope | Get an engine status |
| Status | status/es-size/ | GET | Adm, Ope | Get elasticsearch indices size |
| Status | status/files-queues/ | GET | Adm, Ope | Get the file queues for different engines |
| Status | status/gcenter/ | GET | Adm | Get the Gcenter status |
| Status | status/hardware/raid/ | GET | Adm | Download the hardware diagnostic report file |
| Status | status/healthchecks/ | GET | Adm, Ope | Get the health check status |
| Status | status/maintenances/malcore/ | GET | Adm, Ope | |
| Status | status/updates/ | GET | Adm | Get the updates status |
| Status | status/user/ | GET | WAuth | Get the User status |
| Tags | tags/ | GET | Adm, Ope | Get all the tags |
| Tags | tags/ | POST | Adm | Create a new tag |
| Tags | tags/{id}/ | GET | Adm, Ope | Get a tag content |

suite sur la page suivante

Table 15 – suite de la page précédente

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| Tags | tags/{id}/ | PUT | Adm | Update a tag content |
| Tags | tags/{id}/ | DELETE | Adm | Delete a tag |
| Throttling | throttling/{proto}/ | GET | Adm, Ope | Get Filebeat throttling settings |
| Throttling | throttling/{proto}/ | PUT | Adm, Ope | Update Filebeat throttling settings |
| Users | users/ | GET | Adm | Get all Gcenter's users |
| Users | users/ | POST | Adm | Create a new user |
| Users | users/history/authentications/ | GET | Adm | Get the authentications history |
| Users | users/history/permissions/ | GET | Adm | Get the permissions history |
| Users | users/history/user-management/ | GET | Adm | Get the creations/deletions history |
| Users | users/me/ | GET | Adm, Ope | Get your user data |
| Users | users/me/ | POST | Adm, Ope | Update your user data |
| Users | users/me/password-suggestions/ | GET | Adm, Ope | Get password suggestions |
| Users | users/me/password/ | PUT | Adm, Ope | Update your user password |
| Users | users/password-policy/ | GET | Adm | Get the current password policy configuration |
| Users | users/password-policy/ | PUT | Adm | Update the current password policy configuration |
| Users | users/session-age/ | GET | Adm | Get the session age configuration |
| Users | users/session-age/ | PUT | Adm | Update the session age configuration |
| Users | users/{id}/ | GET | Adm | Get a user data |
| Users | users/{id}/ | PUT | Adm | Update a user data |
| Users | users/{id}/ | DELETE | Adm | Delete a user |
| Users | users/{id}/password/ | PUT | Adm | Reset the password of a user |

# Chapter 6

# Use case of the configuration menu: setup account

## 6.1 Direct connection to the GCenter configuration menu with keyboard and monitor

### 6.1.1 Introduction

The first connection to a GCenter can be made via a direct connection with a keyboard and monitor.
This is necessary if the network configuration is not yet completed on the GCenter or if the network address is not known.
This procedure enables the network parameters (iDRAC) to be known if they exist or to modify them.
Subsequent accesses will generally be made remotely.

### 6.1.2 Preliminary operations

- Connect the power cables.
- Connect the network cables (see *Presentation of the GCenter*).

### 6.1.3 Procedure to connect the monitor and keyboard

- Connect the monitor to the VGA connector.
- Connect the keyboard to one of the USB connectors.
- Switch on the server.

### 6.1.4 Procedure to find out or changing the iDRAC network settings via the BIOS

- Press **F2** during the boot up self-test (POST).
- On the `System Setup Main Menu` page (main menu of the configuration of the system), click on `iDRAC Settings`.

  The `iDRAC settings` page appears.
- Click on `Network`.

  The `IDRAC Settings. Network` page is displayed.
- Note the network settings in the `Network Settings` configuration or modify these settings.
- After noting down the network settings, exit the BIOS.
- Successively click the `Back` button and then the `Finish` button.
- In the `Warning` window prompting you to save changes, click the `No` button.
- In the `System Setup` screen, click the `Finish` button.
- In the `Warning` window prompting you to confirm the exit, click the `Yes` button.

  The server restarts...
- Unplug the monitors and keyboard if necessary.

**Note:**

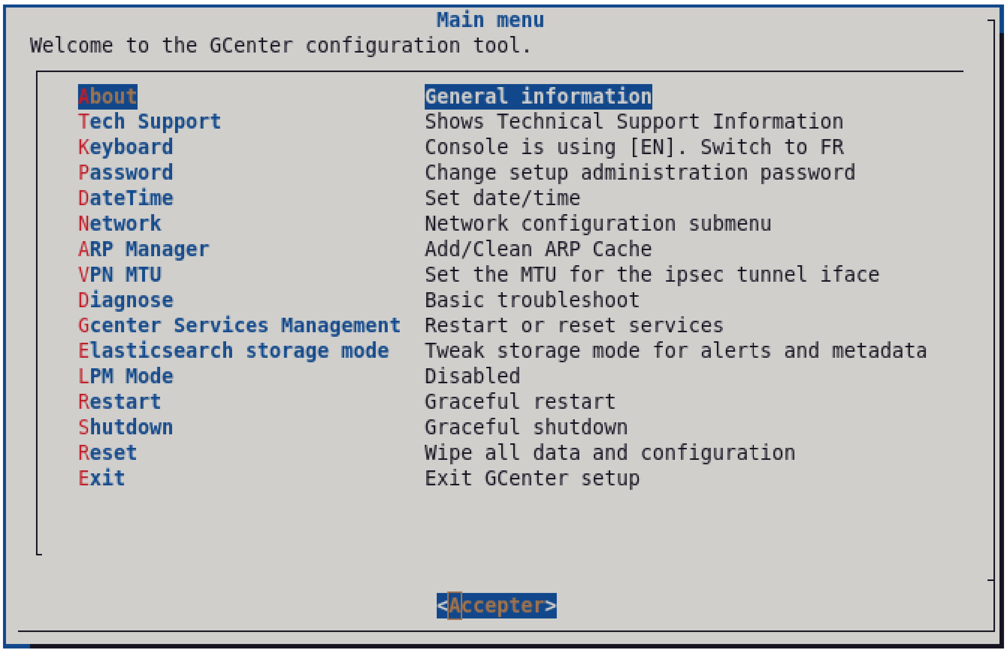
The first time a user logs in via the *setup* account, the system prompts to change the password.

The following message is displayed: `You are required to change your password immediately (administrator enforced).`

In this case:

- Enter a new password in the appropriate format
- Re-enter the new password

The main menu is displayed.



```
                              Main menu
 Welcome to the GCenter configuration tool.

    About                         General information
    Tech Support                  Shows Technical Support Information
    Keyboard                      Console is using [EN]. Switch to FR
    Password                      Change setup administration password
    DateTime                      Set date/time
    Network                       Network configuration submenu
    ARP Manager                   Add/Clean ARP Cache
    VPN MTU                       Set the MTU for the ipsec tunnel iface
    Diagnose                      Basic troubleshoot
    Gcenter Services Management   Restart or reset services
    Elasticsearch storage mode    Tweak storage mode for alerts and metadata
    LPM Mode                      Disabled
    Restart                       Graceful restart
    Shutdown                      Graceful shutdown
    Reset                         Wipe all data and configuration
    Exit                          Exit GCenter setup

                              <Accepter>
```

**Note:**

Press the first letter of a command for quick access.

Press the `OK` button to confirm the selected choice.

## 6.2 Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)

### 6.2.1 Introduction

This procedure describes the remote connection from a distant computer using:

- The network connection to the iDRAC port of the GCenter
- A Web browser

This connection is not the normal way to access the GCenter but enables access to the GCenter in the event of problems.
To carry out this procedure, it is necessary:

- That the iDRAC has an accessible IP in order to be able to connect to it
- To know the login name and password to access iDRAC

From the iDRAC web page, it is possible to:

- View the material resources, their status, and the BIOS configurations
- Interact with the server to turn it on, off, and restart it
- Connect to the GCenter via the console

---

### 6.2.2 Preliminary operations

- Carry out the iDRAC's network configuration.

---

### 6.2.3 Procedure

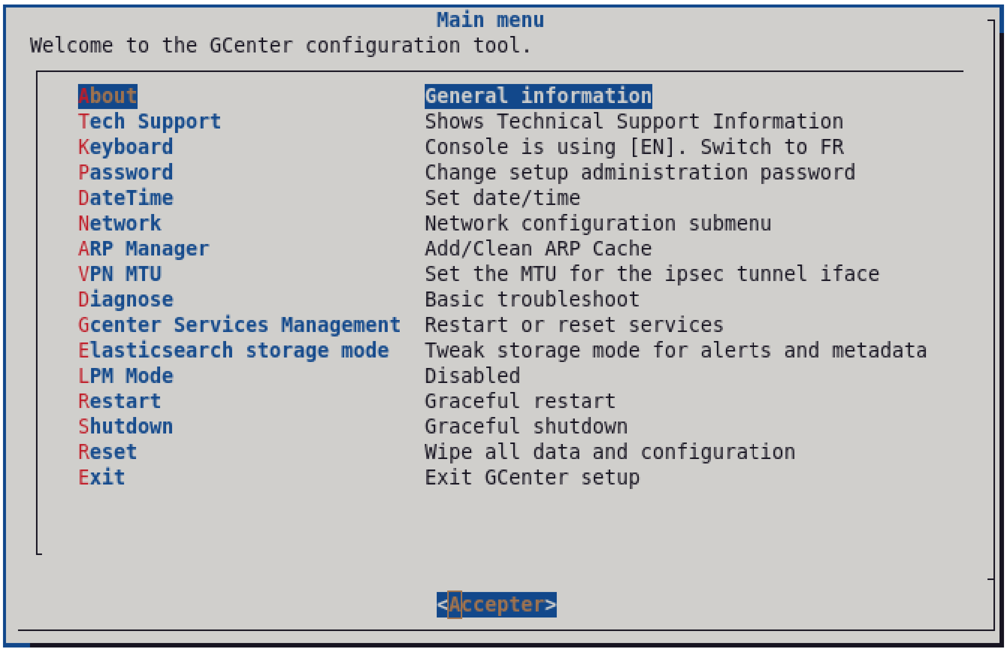
- On the remote computer, open a web browser.
- Enter the IP address of GCenter's iDRAC interface and confirm.
  The `` `Login` `` window is displayed.
- Enter the requested parameters:
  - `` `Username` `` : ID
  - `` `Password` `` : password of the entered login
  - `` `Domain` `` : select `` `This IDRAC` ``
- Click on the `` `Log In` `` button.
- Initiate the virtual console (`` `Virtual console` `` area, `` `Launch Virtual console` `` button).
  Following this action, a new page will open. It will be possible to interact with the GCenter.

**Note:**

The first time a user logs in, the system prompts to change the password.
The following message is displayed: `` `You are required to change your password immediately (administrator enforced).` ``
In this case:

- Enter a new password in the appropriate format
- Re-enter the new password

The main menu is displayed.



```
                              Main menu
Welcome to the GCenter configuration tool.

    About                        General information
    Tech Support                 Shows Technical Support Information
    Keyboard                     Console is using [EN]. Switch to FR
    Password                     Change setup administration password
    DateTime                     Set date/time
    Network                      Network configuration submenu
    ARP Manager                  Add/Clean ARP Cache
    VPN MTU                      Set the MTU for the ipsec tunnel iface
    Diagnose                     Basic troubleshoot
    Gcenter Services Management  Restart or reset services
    Elasticsearch storage mode   Tweak storage mode for alerts and metadata
    LPM Mode                     Disabled
    Restart                      Graceful restart
    Shutdown                     Graceful shutdown
    Reset                        Wipe all data and configuration
    Exit                         Exit GCenter setup

                              <Accepter>
```

**Note:**

Press the first letter of a command for quick access.
Press the `OK` button to confirm the selected choice.

## 6.3 Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode

### 6.3.1 Introduction

This procedure describes the remote connection from a distant computer using:

- The network connection to the iDRAC port of the GCenter
- A connection tool via SSH

This connection is not the normal way to access the GCenter but enables access to the GCenter in the event of problems.
To carry out this procedure, it is necessary:

- That the iDRAC has an accessible IP in order to be able to connect to it
- To know the login name and password to access iDRAC

From the interface, it is possible to:

- View the operating system messages
- Connect to the GCenter via the console

### 6.3.2 Preliminary operations

- Carry out the iDRAC's network configuration.

---

### 6.3.3 Procedure on the remote PC running Linux

- Open a command prompt.
- Enter the command `` `ssh identifiant@adresse_ip` ``.

  For example, `` `ssh setup@x.x.x.x` `` where
  - `` `setup` `` is the identifier and
  - x.x.x.x is the IP address of the GCenter iDRAC port
- Validate the command.
- Enter the password of the entered login.
- Press `` `Enter` `` to display all available commands and a short explanation.

---

### 6.3.4 Procedure on the remote PC running Windows

- Open an SSH client software, such as Putty.
- Enter the IP address of GCenter's iDRAC interface and confirm.
- Enter the following command `` `racadm>>console com2` ``.
- Validate.

  The system now displays the graphical interface of the device.

  Following this action, a new page will open. It will be possible to interact with the GCenter.

---

## 6.4 Direct connection to the GCenter configuration menu via SSH

### 6.4.1 Introduction

This procedure describes how to connect from a remote computer securely using an SSH tunnel.

---

### 6.4.2 Preliminary operations

- Make an initial connection to the GCenter (see *Direct connection to the GCenter configuration menu with keyboard and monitor*).
- Know the name of the GCenter or its IP address.

---

### 6.4.3 Procedure on the remote PC running Linux

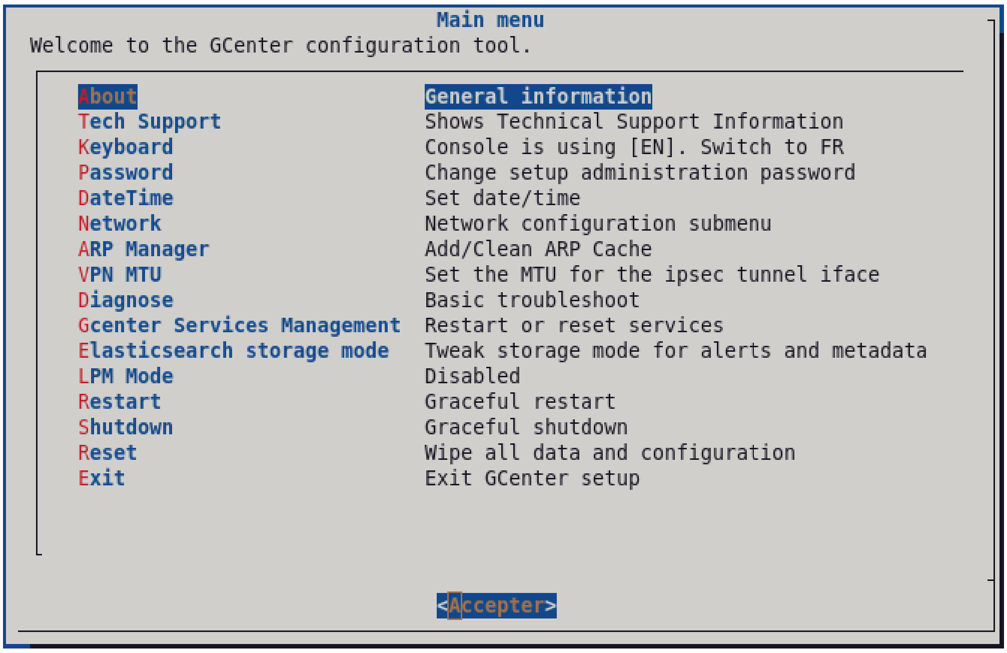
- Open a command prompt.
- Enter the command `ssh identifiant@adresse_ip_GCenter` or `ssh identifiant@FQDN_GCenter`.
  For example, `ssh setup@gcenter` where:

  - The identifier is `setup` and
  - The FQDN is `gcenter`.

- Validate the command.
- Enter the password.

### 6.4.4 Procedure on the remote PC running Windows

- Open an SSH client software, such as Putty.
- Enter the IP address of GCenter's interface and confirm.
- Enter the login and password.
  The main menu is displayed.



```
                              Main menu
 Welcome to the GCenter configuration tool.

    About                        General information
    Tech Support                 Shows Technical Support Information
    Keyboard                     Console is using [EN]. Switch to FR
    Password                     Change setup administration password
    DateTime                     Set date/time
    Network                      Network configuration submenu
    ARP Manager                  Add/Clean ARP Cache
    VPN MTU                      Set the MTU for the ipsec tunnel iface
    Diagnose                     Basic troubleshoot
    Gcenter Services Management  Restart or reset services
    Elasticsearch storage mode   Tweak storage mode for alerts and metadata
    LPM Mode                     Disabled
    Restart                      Graceful restart
    Shutdown                     Graceful shutdown
    Reset                        Wipe all data and configuration
    Exit                         Exit GCenter setup

                              <Accepter>
```

**Note:**

Press the first letter of a command for quick access.
Press the `OK` button to confirm the selected choice.

## 6.5 `About` command

### 6.5.1 Introduction

The `About` command displays the following information:

- `Gcenter Name` : name of the GCenter
- Version: the software version of the GCenter
- The GCenter's IP address characteristics for the mgmt0 interface

- `IP Address`: 192.168.1.1
- `Subnet Mask`: 255.255.255.0
- `Default Gateway`: 192.168.1.254

---

### 6.5.2 Prerequisites

- User : setup

---

### 6.5.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

---

### 6.5.4 Procedure

The configuration menu is displayed.

- Select the `About` line or press the letter **A**.
- Click on the `OK` button.

  The `About` window is displayed:

```
Gcenter Name            :    gcenter-name
Version                 :    number
IP Address              :    192.168.1.1
Subnet Mask             :    255.255.255.0
Default Gateway         :    192.168.1.254
```

- Press the `Enter` key to return to the menu.

---

## 6.6 `Tech Support` command

### 6.6.1 Introduction

The `Tech Support` command enables generating a text report of the GCenter's status.
As the report's data is in plain text, it enables the data to be anonymized if required.
The main sections of this report are:

- Interfaces
- Containers status
- Containers Health checks
- Health checks
- Containers process status
- Appliance Version
- Services status
- NTP
- GCaps / Sigflow
- License
- Logical Volumes
- Disk Free
- Mounted FS
- Scheduled updates
- Latest Update Package sha256sum
- Scheduled backups
- File count in /data/extraction/geyego
- Tree structure of data and backups partitions
- Snapshot top
- Dmidecode
- RAID Card
- Physical Devices
- Virtual Devices
- Logstash pipelines
- Elasticsearch
- Geyego Stats

---

### 6.6.2 Prerequisites

- User : setup

---

### 6.6.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

---

### 6.6.4 Procedure

The configuration menu is displayed.

- Select the `Tech Support` line or press the letter **T**.
- Click on the `OK` button.
  The system creates the technical report, displaying it on the screen.
- Press the `Enter` key to return to the menu.

## 6.7 `Keyboard` command

### 6.7.1 Introduction

The `Keyboard` command enables switching the keyboard language between US and FR.

### 6.7.2 Prerequisites

- User : setup

### 6.7.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

### 6.7.4 Procedure

The configuration menu is displayed.
The system shows:

- The current configuration
- And, if the line is pressed, the switch to the other language.
  For example: the `Keyboard` line shows: `Now using [US]. Switch to FR`.
  In this case, the current keyboard language is US.
- Select the `Keyboard` line or press the letter **K**.
- Click on the `OK` button.
  The system changes the keyboard language.
  The `Keyboard` line is updated: `Now using [FR]. Switch to US`

## 6.8 `Password` command

### 6.8.1 Introduction

The `Password` command enables changing the password of the setup access account.

---

### 6.8.2 Prerequisites

- User : setup

---

### 6.8.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

---

### 6.8.4 Procedure

The configuration menu is displayed.

- Select the `Password` line or press the letter **P**.
- Click on the `OK` button.

  The `About to change the setup administration password` window is displayed.

  The following message is displayed:

```
You are about to change the password of the administrative user account (setup) granting access to this configuration tool.
This change will be effective immediately.
Are you sure to want to continue?
```

- Press the `Yes` button to change the password or the `No` button to cancel.
- If the `Yes` button has been pressed, the following message is displayed `(current) LDAP Password:`
- Enter the current password and confirm

  The following message is displayed: `New password:`
- Enter the current password and confirm
- Re-enter the current password and confirm

**Note:**

**In case of an error, the following message is displayed:**

```
An error has occurred during the password change invite.
You may have mistyped the current password of the password confirmation.
The password has NOT been changed.
Do you want to retry a password change?
```

- Select the `Yes` button to restart the password change procedure or the `No` button to cancel.

## 6.9 `DateTime` command

### 6.9.1 Introduction

The `DateTime` command enables changing the date and time of the GCenter.

**Note:**

It is highly recommended to use a functioning NTP server to maintain an accurate date and time configuration.
Some features may not work as expected if the date and time are incorrect.

**Note:**

Before pairing between GCap and GCenter, it is necessary to ensure that both systems are at the same time.
GCap and GCenter times must be the same within 1 minute.
If there is a discrepancy, the GCap time should be changed.
The adjustment is necessary for the establishment of the IPsec tunnel.
Once the pairing is functional, the GCenter acts as the NTP server for the GCap so that the clocks of the equipment are synchronized.

### 6.9.2 Prerequisites

- User : setup

### 6.9.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

### 6.9.4 Procedure

The configuration menu is displayed.

- Select the line `DateTime` or press the letter **D**.
- Press the `Enter` button.
  The system displays the calendar and is set to the current date.
- To change the date, use the <-> or <+> keys
- Validate after modification.
- To select a field, use the side arrows > or <
- To change a value, use the upper and lower arrows
- Validate after modification.
  The following message is displayed:

```
It is strongly recommended that you use a working NTP server to maintain an accurate date and time configuration.
Some features may not work as expected if the date and time are incorrect.
```

The system displays the new date and time in UTC.

- Validate if necessary.

## 6.10 `Network` command

### 6.10.1 Introduction

The `Network` command enables viewing and modifying the GCenter network settings:

- GCenter name (hostname)
- domain name
- IP address for mgmt0 (with mask and gateway)
- IP address for vpn0 (with mask and gateway)
- IP address for icap0 (with mask and gateway)
- IP address for sup0 (with mask and gateway)
- DNS servers (primary and secondary)
- NTP servers (primary and secondary)

**Attention:**

If an interface used by certain services is deactivated, the latter will no longer be functional.

### 6.10.2 Prerequisites

- User : setup

### 6.10.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

### 6.10.4 Procedure

The configuration menu is displayed.

- Select the `Network` line or press the letter **N**.
- Click on the `OK` button.

  The `Hostname configuration` window is displayed:

  The following settings are displayed by default:

```
Hostname          : gcenter
Dns domain name   : domain.local
```

- If necessary, change the displayed values.
- Press the `Next` button to move to the subsequent settings.

**Note:**

Press the `Previous` button to return to the preceding screen.

The `IP address configuration` window is displayed to configure the mgmt0 interface.

```
Note: Only dot decimal IPv4 format is accepted
IP address     : 192.168.1.1
   Netwask     : 255.255.255.0
   Gateway     : 192.168.1.254
```

- If necessary, change the displayed values.
- Press the `Next` key to move to the subsequent settings.

**Note:**

Press the `Previous` button to return to the preceding screen.

The `VPN Interface (optional)` window is displayed:

```
Do you want to use a dedicated VPN interface?
If no interface is selected then VPN will work through management interface
```

- Press the `Yes` or `No` button.

  After pressing the `Yes` button, then configure the network settings in the same way as for mgmt0.

  After validation, the `ICAP Interface (optional)` window is displayed:

```
Do you want to use a dedicated ICAP interface?
```

- Press the `Yes` or `No` button.

After pressing the `Yes` button, then configure the network settings in the same way as for mgmt0.
After validation, the `SUP Interface (optional)` window is displayed:

```
Do you want to use a dedicated SUP interface?
```

- Press the `Yes` or `No` button.
  After pressing the `Yes` button, then configure the network settings in the same way as for mgmt0.
  After validation, the `DNS domain and servers configuration` window is displayed:

```
Configure DNS servers

Note: Only dot-decimal IPv4 format is accepted

          DNS server #1 : 192.168.1.251
          DNS server #2 :
```

- If necessary, change the displayed values.
- Press the `Next` key to move to the subsequent settings.
  The `NTP domain and servers configuration` window is displayed:

```
Configure NTP servers

Note: Only dot-decimal IPv4 format is accepted

        NTP server #1 : 192.168.1.251
        NTP server #2 :
```

- If necessary, change the displayed values.
- Press the `Next` key to move to the subsequent settings.
  The `Applying configuration` window is displayed:

```
Configuration will be applied. Web service, interfaces, and remote control will be
restarted if needed.

 WARNING: If hostname has changed you must pair all your GCaps again.
```

- Press:

- The `Yes` key to accept the changes
- The `No` key to return to the previous screen

## 6.11 `Arp Manager` command

### 6.11.1 Introduction

The `Arp Manager` command enables:

- Add an entry to the GCenter ARP table
- Delete an ARP entry made via the ARP Manager
- Clear the ARP cache of entries made via the ARP Manager

**Note:**

It is used in specific cases, for example if a diode is found between the GCenter and a piece of equipment on the network.

### 6.11.2 Prerequisites

- User : setup

---

### 6.11.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

---

### 6.11.4 Procedure A: Using the `Arp Manager` command

The configuration menu is displayed.

- Select the `Arp Manager` line or press the letter **A**.
- Click on the `OK` button.
  The `Arp Manager` window is displayed:

```
 Choose a task

       Add entry        Adds an ARP entry
       Delete entry     Deletes an ARP entry
       Clean cache      Cleans all the ARP cache

Several choices are available:
```

| Choice | Seee |
|---|---|
| `Add entry` | *Procedure B: Adding an ARP entry* |
| `Delete entry` | *Procedure C: Delete an ARP entry* |
| `Clean cache` | *Procedure D: Clearing the ARP cache* |

- Press the `Exit` key to return to the menu.

---

### 6.11.5 Procedure B: Adding an ARP entry

The `Arp Manager` window is displayed:

```
Choose a task

    Add entry        Adds an ARP entry
    Delete entry     Deletes an ARP entry
    Clean cache      Cleans all the ARP cache
```

- Select the `Add entry` line or press the letter **A**.
- Click on the `OK` button.
  The `Add ARP entry` window is displayed:

```
Choose a task
     MAC Address
     IP  address
```

- Enter the parameters.
- Press the `Add` button to confirm the selected choice.

### 6.11.6 Procedure C: Delete an ARP entry

The `Delete ARP entry` window is displayed:

**Note:**

If there is no entry then the message `Nothing to delete` is displayed.

- Click on the `OK` button.

### 6.11.7 Procedure D: Clearing the ARP cache

The `Clean cache` window is displayed:

**Note:**

If there is no data to clean then the `Nothing to clean` message is displayed.

- Click on the `OK` button.

## 6.12 `VPN MTU` command

### 6.12.1 Introduction

The `VPN MTU` command enables modifying the MTU value of the IPsec tunnel interface (mgmt0 or vpn0).

### 6.12.2 Prerequisites

- User : setup

### 6.12.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

### 6.12.4 Procedure

The configuration menu is displayed.

- Select the `VPN MTU` line or press the letter **V**.
- Click on the `OK` button.

  The following window is displayed:

```
Select MTU:
```

- Enter the MTU value.
- Press the `OK` button to confirm the configuration and return to the menu.

## 6.13 `Diagnose` command

### 6.13.1 Introduction

The `Diagnose` command enables various actions to be tested on the network in order to validate the GCenter's correct configuration.
The tests performed are as follows:

- Ping the default gateway
- Ping the primary DNS server
- Ping of the secondary DNS server
- Ping the primary NTP server
- Ping of the secondary NTP server
- Query to primary DNS server
- Query to secondary DNS server
- Registration of the GCenter in the DNS
- Resolution of the Intelligence site
- Ping intelligence.gatewatcher.com
- Connect to intelligence.gatewatcher.com
- NTP synchronisation
- Internal DNS running
- Web server running

### 6.13.2 Prerequisites

- User : setup

---

### 6.13.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

---

### 6.13.4 Procedure

The configuration menu is displayed.

- Select the `Diagnose` line or press the letter ** D**.
- Click on the `OK` button.
  The `Gatewatcher Diagnostics` window is displayed:

```
Select a timeout for each network test.
Value must be between 1 and 10 sec:
```

- Enter a value between 1 and 10 then validate.
  The system displays the tests carried out and then the test results:
- Press the `Enter` key to return to the menu.

---

## 6.14 `Upgrade type` command

### 6.14.1 Introduction

The `Upgrade type` command enables selecting the appropriate upgrade option.
The options are as follows:

- `Stable only`: for versions considered stable
- `Unstable and stable`: for versions considered unstable or under development

**Note:**

Solely the `Stable only` option is used in production.

---

### 6.14.2 Prerequisites

- User : setup

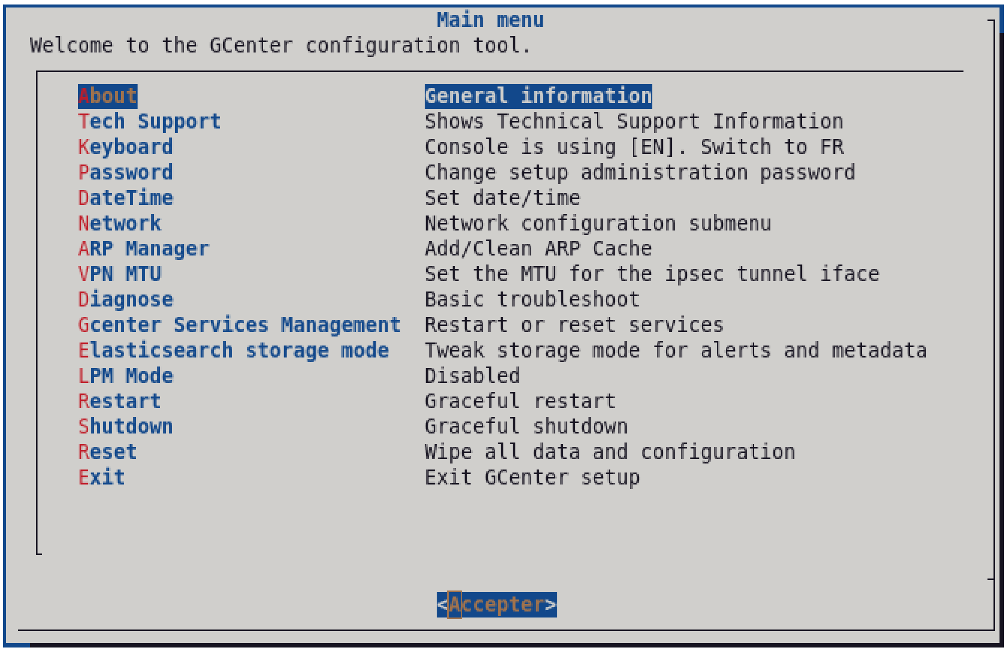
### 6.14.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

### 6.14.4 Procedure

The configuration menu is displayed.



```
                                  Main menu
 Welcome to the GCenter configuration tool.

     About                          General information
     Tech Support                   Shows Technical Support Information
     Keyboard                       Console is using [EN]. Switch to FR
     Password                       Change setup administration password
     DateTime                       Set date/time
     Network                        Network configuration submenu
     ARP Manager                    Add/Clean ARP Cache
     VPN MTU                        Set the MTU for the ipsec tunnel iface
     Diagnose                       Basic troubleshoot
     Gcenter Services Management    Restart or reset services
     Elasticsearch storage mode     Tweak storage mode for alerts and metadata
     LPM Mode                       Disabled
     Restart                        Graceful restart
     Shutdown                       Graceful shutdown
     Reset                          Wipe all data and configuration
     Exit                           Exit GCenter setup

                                  <Accepter>
```

- Select the `Upgrade type` line or press the letter **U**
- Click on the `OK` button

  The system shows:

- The current configuration
- And, if the line is pressed, it switches to the other option.

**Note:**

For example

The `Upgrade Type` line indicates: `Stable only`.
In this case, the upgrade will be restricted to stable versions.

- Select the `Upgrade type` line or press the **U**.
- Click on the `OK` button.

  The system changes the type of upgrade used.

  The `Upgrade Type` is updated: `Unstable and stable`

## 6.15 `Gcenter Services Management` command

### 6.15.1 Introduction

`Gcenter Services Management` command enables:

- Rebooting a GCenter application
- Resetting a GCenter application
- Restarting a GCenter service

The applications that can be restarted include the following:

| App name | Detail |
|---|---|
| ggcc | Service WebUI #1 |
| gweb | Service WebUI #2 |
| gpostgres | Database service |
| gproxy | Connection Manager |
| gabana | Kibana service |
| gstats | Monitoring service |
| gunpoint | GCap gateway service |
| gredis | Ephemeral data service |
| gredis cache | Ephemeral data service (Used for caching) |
| glogstash | Threat logging service |
| gesmaster | ES Master Service |
| gcti | CTI engine |
| gdgadetect | DGA engine |
| gmalcore | Malware analysis engine |
| geyego | Threat analysis and retroactive orchestration service |
| goasm | Vulnerability exploitation scanning engine |
| gps | Powershell scanning engine |

The applications that can be reset include the following:

| App name | Détail |
|---|---|
| Reset Malcore Engine | Reset Malcore Engine to factory default settings |
| Reset Webui configuration | Reset HTTP / HTTPS ports and interface to default configuration |
| Wipe Elesticsearch index | Removes all internal indexes |
| Clear & Restart Webui server | Reset web server to default configuration |
| Clear & Restart Database | Remove local database and restart services |

The services that can be restarted include the following:

| App name | Détail |
|---|---|
| nginx | Restarting the web service |
| uwsgi | Restarting the application management service |
| celery | Restart the GCenter queue service |
| redis | Restart ephemeral data management service |
| unbound | Restart the DNS resolution service |
| sshd | Restart the GCenter ssh service |
| sshd_gcap | Restart the GCap-related ssh service |
| gcenter-healthchecks-daemon | Restarting the GCenter health check service |
| gcenter-docker-orchestrator | Restarting the docker orchestration service |

### 6.15.2 Prerequisites

- User : setup

### 6.15.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

### 6.15.4 Procedure A: Using the `Gcenter Services Management` command

The configuration menu is displayed.

- Select the `Gcenter Services Management` line or press the letter **G**.
- Click on the `OK` button.

  The `Gcenter Services Management` window is shown:

```
Restart a GCenter App
Reset a GCenter App
Restart a GCenter Service
```

Several choices are available:

| Choice | see |
|---|---|
| Restart a GCenter App | *Procedure B: Restarting an application* |
| Reset a GCenter App | *Procedure C: Reset a service* |
| Restart a GCenter Service | *Procedure D: Restarting an application* |

- Press the **Exit** key to return to the menu.

### 6.15.5 Procedure B: Restarting an application

The `Restart a GApp` window is displayed.

- Select the line to be restarted or press the letter **G** .
- Click on the `OK` button.

> **Note:**
>
> For example, for the ggcc service:
> The system displays the following message `You are about to restart ggcc. Are you sure?`
>
> - Click on the `Yes` button
>
>   A message indicates the restart is in progress.
>
>   Then the system displays the following message `ggcc restarted successfully`.
> - Click on the `OK` button.

---

### 6.15.6 Procedure C: Reset a service

The `Reset a GApp` window is displayed.

```
Choose a GApp to reset:

Reset Malcore Engine         Reset Malcore engine to factory default
Reset Webui configuration    This will reset HTTP / HTTPS and interface to the default␣
↪configuration
Wipe Elesticsearch index     Delete all internals index
Clear & Restart Webui ser    This will set webserver to default config
Clear & Restart Database     This will empty the local database and restart services
```

- Select the service line to be reset or press the corresponding letter.
- Click on the `OK` button.

> **Note:**
>
> For example, for the `Reset Malcore Engine` line:
> The system displays the following message `You are about to reset the Malcore Engine to a factory default state. Are you sure?`.
>
> - Click on the `Yes` button.
>
>   A message indicates the shutdown is in progress.
>
>   Then the system displays the following message `Malcore has been reset successfully`.
> - Click on the `OK` button.

---

### 6.15.7 Procedure D: Restarting an application

The `Restart a service` window is displayed:

```
Choose a service to restart :

    nginx
    uwsgi
    celery
    redis
    unbound
    sshd
    sshd_gcap
    gcenter-healthchecks-daemon
    gcenter-docker-orchestrator
```

- Select the line to be restarted or press the corresponding letter.
- Click on the `OK` button.

**Note:**

For example, for the `nginx` service:
The system displays the following message `You are about to restart nginx. Are you sure?`.

- Click on the `Yes` button.

  A message indicates the restart is in progress.

  Then the system displays the following message `nginx restarted successfully`.
- Click on the `OK` button.

## 6.16 Commande `Elasticsearch storage mode`

### 6.16.1 Introduction

The `Elasticsearch storage mode` command enables modifying the storage mode for the alerts and the metadata.

Choosing slow storage for elasticsearch will increase the potential retention duration, but it will negatively impact the performances and speed of the GCenter.
It is strongly recommended to keep elasticsearch on fast storage.

**Note:**

Storage type switch will preserve your data. Moving high amount of data can greatly reduce the performances of your gcenter during the operation, and take up to one hour. Indexation will be paused while it is occurring. The migration process will allocate the default data retention size on the target storage (see numbers above). This allocation can later be extended to the maximum size for the target storage: see the configuration in the webui screen following Admin>Configuration>Global settings>Elasticsearch max data retention.

### 6.16.2 Prerequisites

- User : setup

---

### 6.16.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

---

### 6.16.4 Procedure

The configuration menu is displayed.

- Select the line `` `Elasticsearch storage mode`` `` or press the letter **E**.
- Press the `` `OK` `` button.

  The window `` `Elasticsearch storage mode` `` is displayed.

```
Current storage type: fast
Maximum size on fast storage for elasticsearch: 15G
Maximum size on slow storage for elasticsearch: 99G
Current space used by elasticsearch: 1.0G`
```

- To change the current storage mode, press the `` `Switch storage type` ``.

  The screen becomes:

```
Maximum size for target storage type: 99G
Default data retention size on target storage type: 99G
Current space used by elasticsearch: 1,0G
```

- To start the operation, press the `` `Switch storage type and launch data migration` ``.

  The following message is displayed indicating the progress of the operation.

```
Elasticsearch storage mode configuration is running, this can take a while.
Storage mode reconfiguration preparation: Running
Amount of data on target storage / origin storage: Not running
Reconfigure storage mode: Not running
```

> **Note:**
>
> In case of error, the following message is displayed.
>
> ```
> An error has been encountered during the procedure. As a result, the
> gcenter could become unstable. Please, contact the gatewatcher support
> quickly.
> ```
>
> In this case, contact the Gatewatcher support.
> In case, validate the error message.

At the end of the operation, the storage type changed (in this example, it changed to `` `slow` ``).

```
Choosing slow storage for elasticsearch will increase the potential retention duration, but it will negatively impact the performances and speed of the gcenter.
It is strongly recommended to keep elasticsearch  on fast storage.
Current storage type: slow
Maximum size on fast storage for elasticsearch: 15G
Maximum size on slow storage for elasticsearch: 999G
Current space used by elasticsearch: 1.0G
```

- Press the `Back` button to return to the general menu.

## 6.17 `LPM Mode` command

### 6.17.1 Introduction

The `LPM Mode` command enables or disables MPL mode.
The current status is indicated. For example, `Disabled` indicates that LPM Mode is disabled.

### 6.17.2 Prerequisites

- User : setup

### 6.17.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

### 6.17.4 Procedure

The configuration menu is displayed.

- Select the `LPM Mode` line or press the letter **L**.
- Click on the `OK` button.
  The system displays the following message `Changing LPM mode will need to reboot the appliance. Are you sure?`.
- Click on the `Yes` button.

**Important:**

Please note! The system will reboot when the above operation is performed.
After this reboot, the GCenter will enter the selected mode.

## 6.18 `Restart` command

### 6.18.1 Introduction

The `Restart` command enables restarting the GCenter.

---

### 6.18.2 Prerequisites

- User : setup

---

### 6.18.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

---

### 6.18.4 Procedure

The configuration menu is displayed.

- Select the `Restart` line or press the letter **R**.
- Click on the `OK` button.

  The `Rebooting` window is displayed:

```
Rebooting in 10 seconds
You can still abort reboot by pressing <ESC> or <Cancel> button.
```

- Press:

- The `Reboot now` button to return to the menu.
- The `Cancel` button to abort the reboot.

---

## 6.19 `Shutdown` command

### 6.19.1 Introduction

The `Shutdown` command enables turning off the GCenter.

---

### 6.19.2 Prerequisites

- User : setup

### 6.19.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

### 6.19.4 Procedure

The configuration menu is displayed.

- Select the `Shutdown` line or press the letter **S**.
- Click on the `OK` button.
  The `Shutdown` window is displayed:

```
Shutting down in 10 seconds
You can still abort reboot by pressing <ESC> or <Cancel> button.
```

- Press:

- The `Shutdown now` button to return to the menu
- The `Cancel` button to abort the shutdown.

## 6.20 `Reset` command

### 6.20.1 Introduction

The `Reset` command enables resetting the GCenter to its factory settings.
All configurations and data will be deleted.

### 6.20.2 Prerequisites

- User : setup

### 6.20.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

---

### 6.20.4 Procedure

The configuration menu is displayed.

- Select the `Reset` line or press the letter **R**.
- Click on the `OK` button.

  The `Reset Gcenter Appliance` window is displayed:

```
Warning
This tool will WIPE ALL DATA.
This means that you will loose connectivity and data.
It will restart the GCenter automatically.
```

  - Press:

  - The `Yes` button to continue
  - The `Cancel` button to abort.

---

## 6.21 `Exit` command

### 6.21.1 Introduction

The `Exit` command enables closing the configuration menu.

---

### 6.21.2 Prerequisites

- User : setup

---

### 6.21.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

---

### 6.21.4 Procedure

The configuration menu is displayed.

- Select the `Exit` line or press the letter **E**.
- Click on the `OK` button.

**Note:**

If the connection to the GCenter is remote, it will be closed.
If the connection is made via iDRAC, the menu will close and the login page will be displayed.

# Chapter 7

# Use cases at the operator or analyst level

## 7.1 Connection to the GCenter web interface via a web browser

### 7.1.1 Introduction

This procedure describes connecting from a remote computer to the GCenter web interface via a web browser. This connection is the nominal way to access the web interface of the equipment.

### 7.1.2 Prerequisites

- User: all users

### 7.1.3 Preliminary operations

- Know the name of the GCenter or its IP address.
- Access GCenter from your workstation.

### 7.1.4 Procedure

On the remote PC:

- Open a web browser
- Enter the IP address or FQDN of the GCenter
- Validate.

  The GCenter login window is displayed.

- Enter the login name
- Enter the password
- Validate.

The GCenter graphical interface is displayed.

**Note:**

During the first login, it is necessary to change the password.
Passwords must comply with the password policy (see *The `Password Policy` section of the `Accounts` submenu*).

## 7.2 Managing local users

This section describes how to manage local users on the GCenter from the `Accounts` menu.
For more details on the `Accounts menu`, see *Web interface accounts and their management*.

### 7.2.1 Changing the current account password

#### 7.2.1.1 Introduction

This procedure describes how to change the current user's password.
To enter a new password consistent with the policy to be applied, the system proposes six basic passwords displayed.
A `REGENERATE` button enables six new passwords to be generated.

**Danger:**

Carefully note down the submitted password, especially if the current account is the only account in the administrator group.

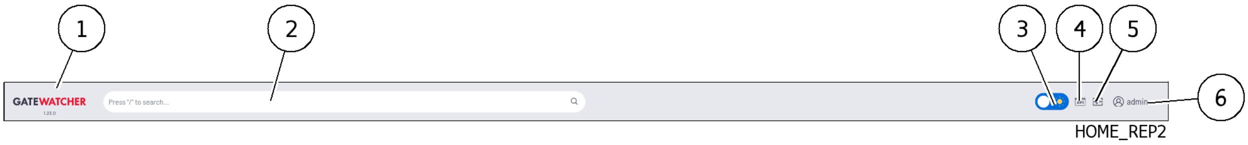
#### 7.2.1.2 Prerequisites

User : member of **Operator** group

#### 7.2.1.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

### 7.2.1.4 Procedure



- In the GCenter interface, click on the current account button (6).
- Select the `` `Change password` `` command.

  The `` `Change Password` `` window is displayed.
- Enter the previous password in the `` `Old password` `` field.
- Enter the new password in the `` `New password` `` field.
- Enter the new password in the `` `New password confirmation` `` field.

  The password entered must match the *Password management policy*.

  The system checks the password against the verification policy.

  If the password does not meet the verification policy, one of the following messages will be displayed:
  - `` `Minimal length 12` ``: indicates a password that is too short (12 characters minimum)
  - `` `Uppercase` ``: indicates the lack of a capital letter
  - `` `Lowercase` ``: indicates the lack of a small letter
  - `` `Symbol` ``: indicates the lack of a special character
  - `` `Digit` ``: indicates the lack of a digit

  > **Note:**
  >
  > To copy one of the proposed passwords, click on the right side of the password.
  > A window will appear informing that the password is copied to the clipboard.
  > To paste the password, right-click and then paste into each of the two fields.
  > Make sure to note down the password before saving.

- Click on the `` `SAVE` `` button.

> **Note:**
>
> If the following message is displayed `` `you used this password recently, please choose a different one.` ``, enter a password that has not been used before.

## 7.2.2 Changing some of the current user's information

### 7.2.2.1 Introduction

This procedure describes how to modify local users:

- Email address
- First name
- Last name

#### 7.2.2.2 Prerequisites

User : member of **Operator** group

---

#### 7.2.2.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

---

#### 7.2.2.4 Procedure

- In the navigation bar, successively click on:

- The `` `Admin` `` button
- The `` `Gcenter` `` sub-menu
- The `` `Edit profile` `` command
  The `` `Settings` `` window is displayed.
  The window shows account information such as username, creation date, and last login.

- Enter or modify the data found in:

- In the `` `Email address` `` field
- In the `` `First name` `` field
- In the `` `Last name` `` field

- Confirm the changes using the `` `Save` `` button.
  A confirmation window displays the message `` `Profile successfully saved!` ``.

---

## 7.3 Configuring the Sigflow engine

This section describes the GCap configurations from the GCenter using the `` `Sigflow` `` menu.
For more details on the `` `Sigflow` `` menu, see *Sigflow engine*.

### 7.3.1 SIGFLOW engine rule sources

#### 7.3.1.1 Introduction

The rules and their organization are described in the paragraph *Organizing the rules*.
The configuration interface is described in the *`Config - sigflow/rulesets` screen of the legacy web UI*.

A source is broken down as follows:

- Detection rules are found in categories
- Categories are found in sources
- Sources are in rulesets

**Note:**

Categories are not mandatory. They enable improved organisation of the source.

This procedure describes:

- Managing the existing sources
- Managing the categories and rules made available in the sources
- Adding public or customized sources

**Note:**

Sources should be added to a **Ruleset** that will then be made available to the GCap.

| For | go to |
|---|---|
| Visualise existing sources | *Procedure to view the existing sources* |
| Add a public source | *Procedure to add a public source* |
| Add a custom source | *Procedure to add a custom source* |
| Delete a source | *Procedure to delete a source* |
| Edit a source | *Procedure to edit a source* |
| Update a source | *Procedure to update a source* |

This configuration interface is described in *Web UI `Assets` screen*.

---

#### 7.3.1.2 Prerequisites

- User : member of **Operator** group

---

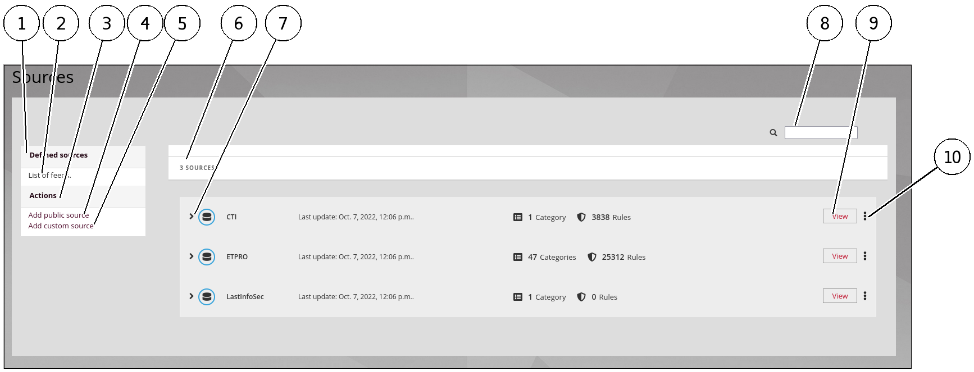
#### 7.3.1.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

---

#### 7.3.1.4 Procedure to view the existing sources

- From the navigation bar, click successively on :
  - The `Config` button
  - The `Sources` button of the `Sigflow` menu.
    The `Sources` windows is displayed.



| | | | | |
|---|---|---|---|---|
| CTI | Last update: Oct. 7, 2022, 12:06 p.m.. | 1 Category | 3838 Rules | View |
| ETPRO | Last update: Oct. 7, 2022, 12:06 p.m.. | 47 Categories | 25312 Rules | View |
| LastInfoSec | Last update: Oct. 7, 2022, 12:06 p.m.. | 1 Category | 0 Rules | View |

SOURCES-01

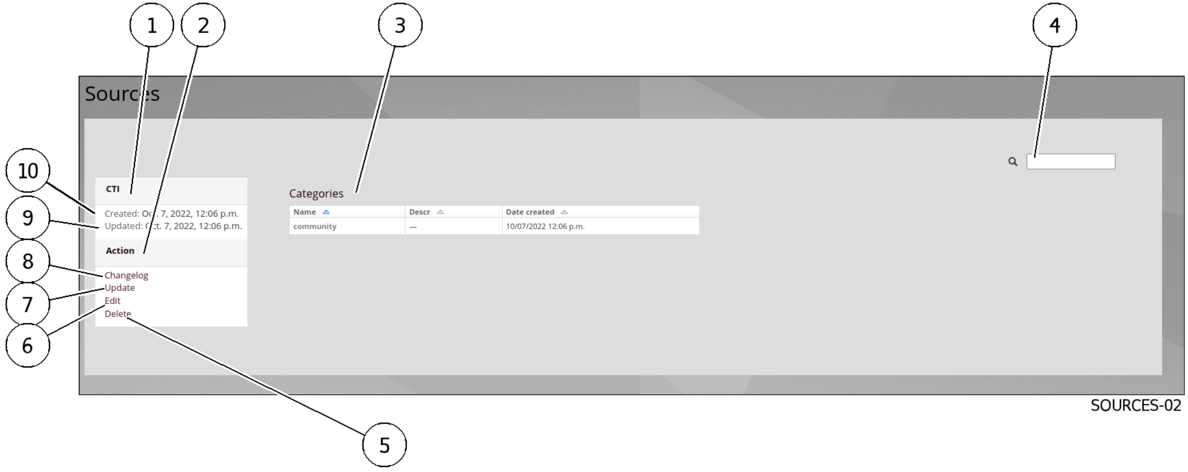
From the source management interface, the available sources are displayed (7). The following types of information are displayed:

- The name of the source (CTI, ETPRO, LastInfoSec...)
- The date and time of the last update
- The number of categories and signatures

**Note:**

It is possible to add a MISP source.
For this, contact the administrator.

- To view the contents of the desired source, click on the `View` button (9).
  The detail window is displayed



Created: Oct. 7, 2022, 12:06 p.m.
Updated: Oct. 7, 2022, 12:06 p.m.

| Name | Descr | Date created |
|---|---|---|
| community | — | 10/07/2022 12:06 p.m. |

SOURCES-02

The source detail is indicated in *`Config - sigflow/sources` screen of the legacy web UI*.

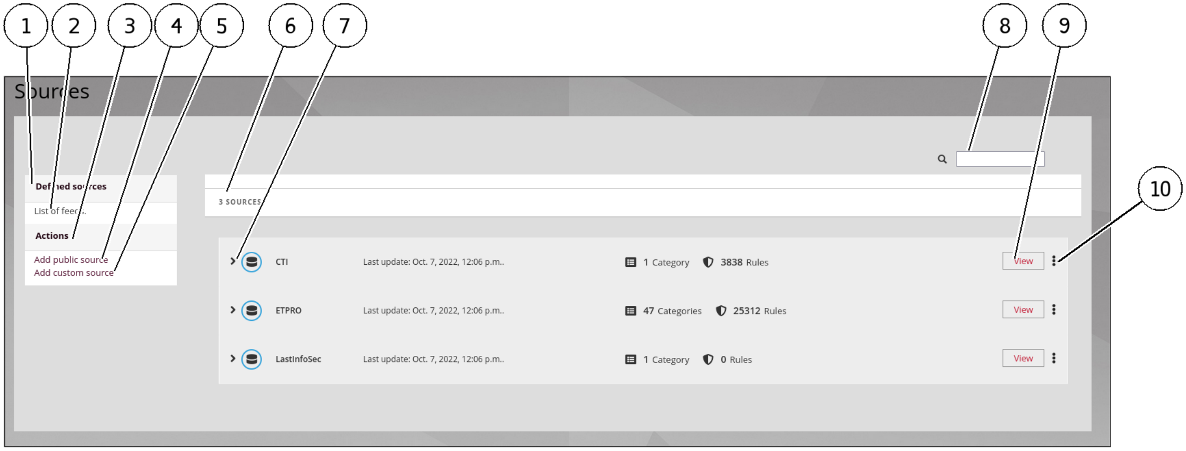
#### 7.3.1.5 Procedure to add a public source

- Preliminary step:

  The GCenter must be connected to the Internet.
  This is done in the GCenter configuration (PROXY parameter): in case of doubt refer to the administrator.

- From the navigation bar, click successively on :

- The `Config` button
- The `Sources` button of the `Sigflow` menu.
  The `Sources` windows is displayed.



Sources

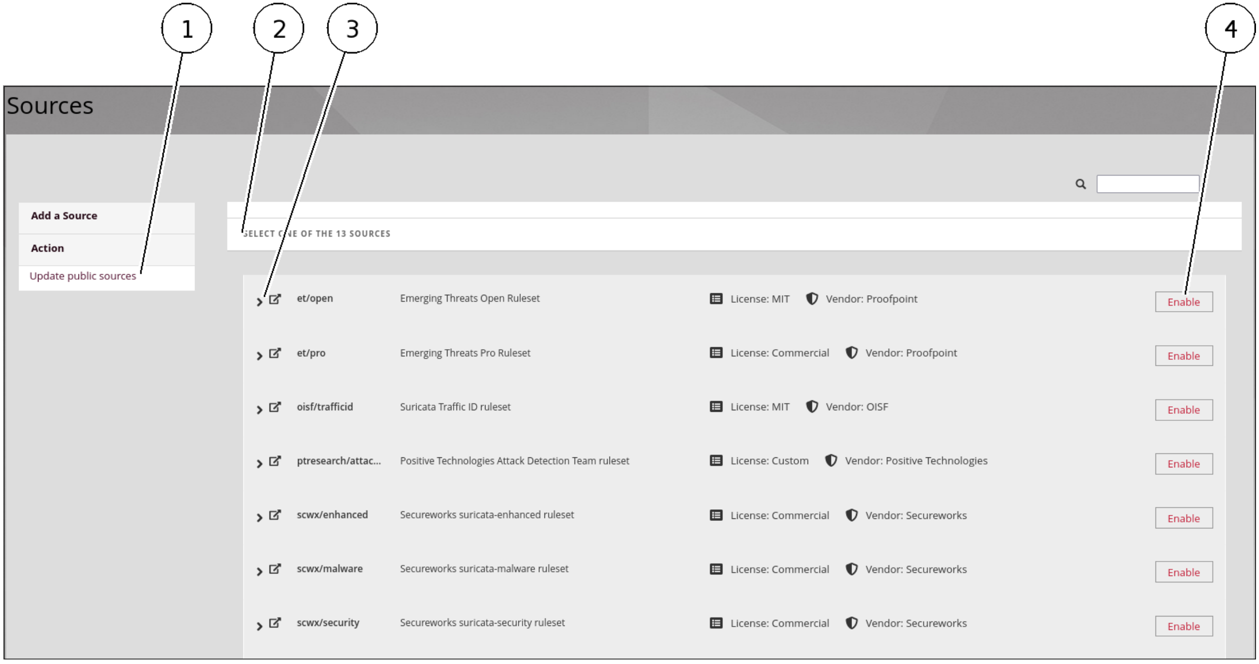
Defined sources
List of feeds..
Actions
Add public source
Add custom source

3 SOURCES

| | | | | |
|---|---|---|---|---|
| CTI | Last update: Oct. 7, 2022, 12:06 p.m.. | 1 Category | 3838 Rules | View |
| ETPRO | Last update: Oct. 7, 2022, 12:06 p.m.. | 47 Categories | 25312 Rules | View |
| LastInfoSec | Last update: Oct. 7, 2022, 12:06 p.m.. | 1 Category | 0 Rules | View |

SOURCES-01

- Click on the `Add public source` link (4)
  The "Sources" window is displayed.



Sources

Add a Source
Action
Update public sources

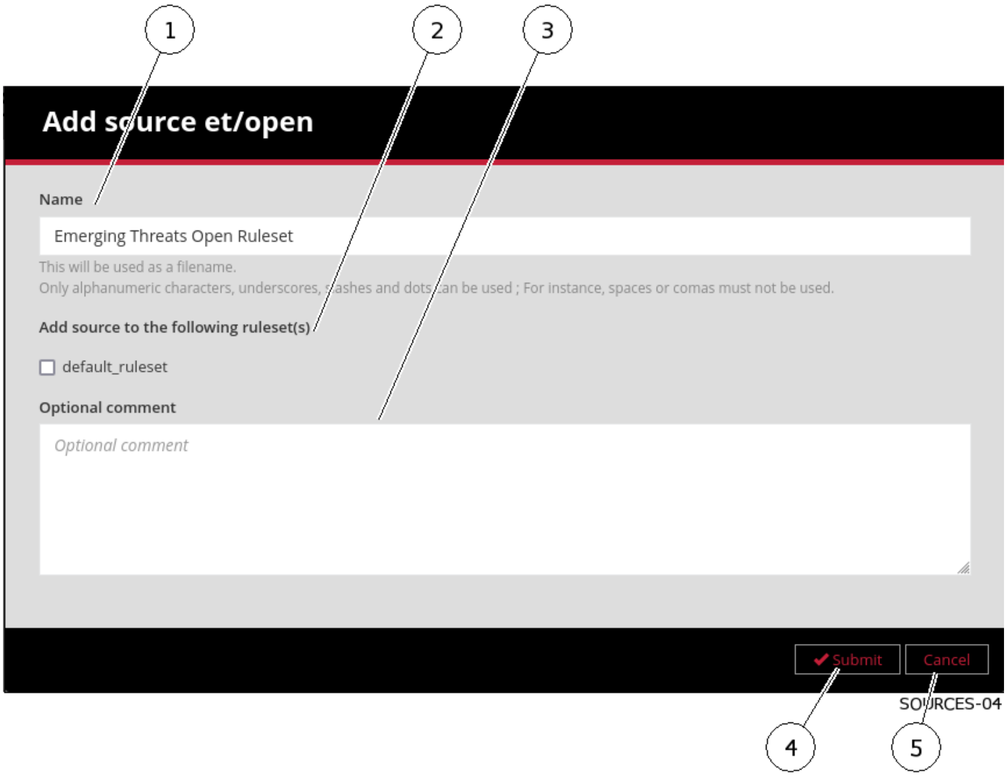
SELECT ONE OF THE 13 SOURCES

| | | | | |
|---|---|---|---|---|
| et/open | Emerging Threats Open Ruleset | License: MIT | Vendor: Proofpoint | Enable |
| et/pro | Emerging Threats Pro Ruleset | License: Commercial | Vendor: Proofpoint | Enable |
| oisf/trafficid | Suricata Traffic ID ruleset | License: MIT | Vendor: OISF | Enable |
| ptresearch/attac... | Positive Technologies Attack Detection Team ruleset | License: Custom | Vendor: Positive Technologies | Enable |
| scwx/enhanced | Secureworks suricata-enhanced ruleset | License: Commercial | Vendor: Secureworks | Enable |
| scwx/malware | Secureworks suricata-malware ruleset | License: Commercial | Vendor: Secureworks | Enable |
| scwx/security | Secureworks suricata-security ruleset | License: Commercial | Vendor: Secureworks | Enable |

SOURCES-03

The window displays the list of available sources (2) when connecting to the Internet.
If the Internet connection is not active then an error message is displayed.

- Activate the desired public source (for example mark 3) by clicking on the button (4) `Enable`.
  The `` ` source and/open` `` window is displayed.



## Add source et/open

Name

Emerging Threats Open Ruleset

This will be used as a filename.
Only alphanumeric characters, underscores, slashes and dots can be used ; For instance, spaces or comas must not be used.

Add source to the following ruleset(s)

□ default_ruleset

Optional comment

Optional comment

- Change source name (1) if needed.

**Note:**

The name is also the file name so only alphanumeric characters, underscore, slash and dot can be used. However, spaces and commas should not be used.

- Add the source to the default ruleset (2) if needed.
- Add a comment (3) if needed.
- Enter the source editor token if necessary.
- Validate the entry by clicking on the (4) `Submit` button or cancel with the (5) `Cancel` button.

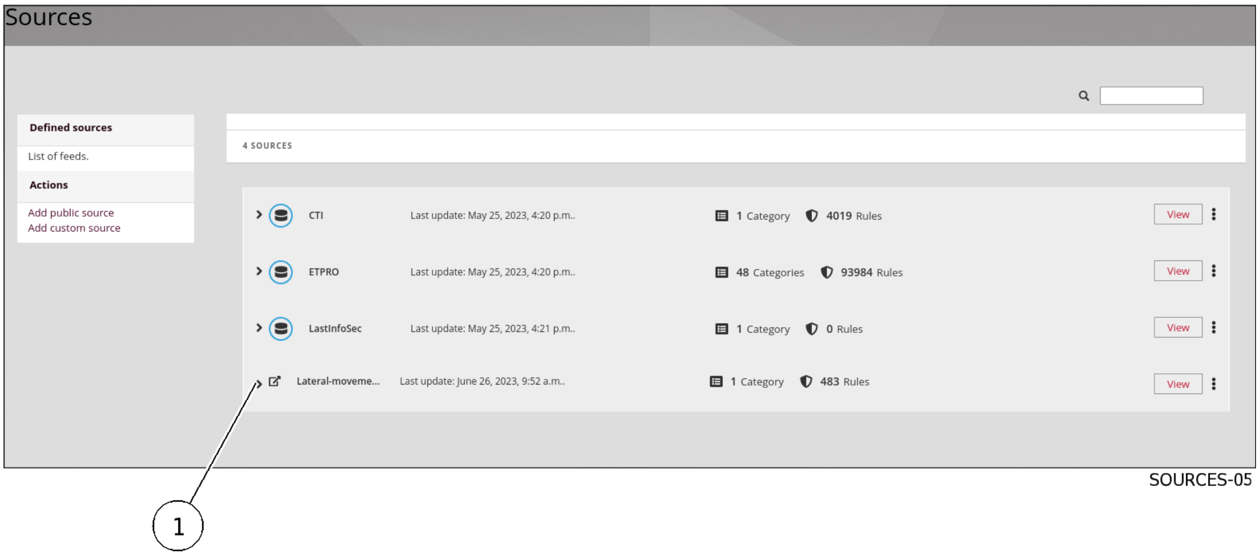
  The message `Source fully activated` is displayed.

  The message `Source updated` is displayed.

  The `Source is valid` message is displayed.

  A link is active to display the details of this new source.

  This new source has been added to the Sources screen.



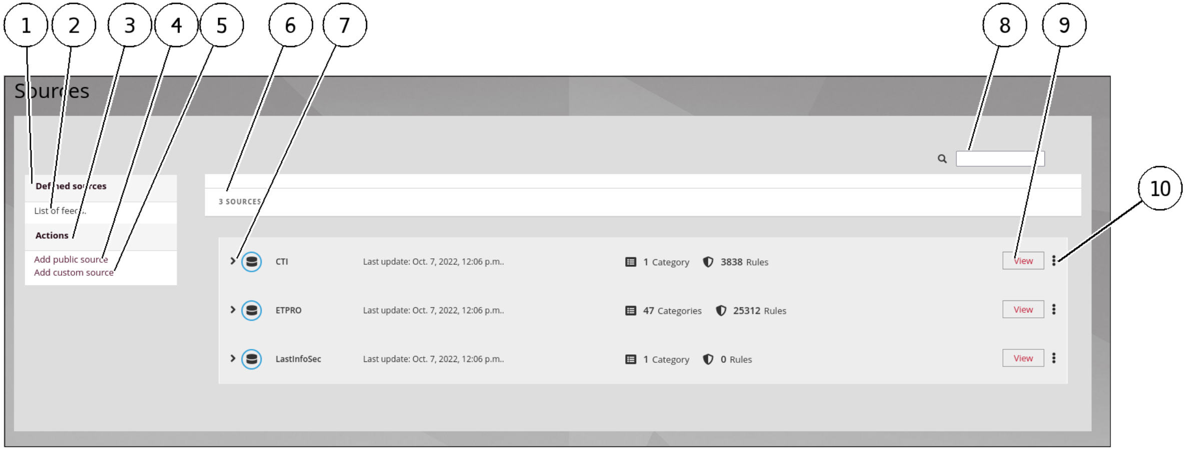
| | | | | |
|---|---|---|---|---|
| CTI | Last update: May 25, 2023, 4:20 p.m.. | 1 Category | 4019 Rules | View |
| ETPRO | Last update: May 25, 2023, 4:20 p.m.. | 48 Categories | 93984 Rules | View |
| LastInfoSec | Last update: May 25, 2023, 4:21 p.m.. | 1 Category | 0 Rules | View |
| Lateral-moveme... | Last update: June 26, 2023, 9:52 a.m.. | 1 Category | 483 Rules | View |

SOURCES-05

### 7.3.1.6 Procedure to add a custom source

- From the navigation bar, click successively on :
- The `Config` button
- The `Sources` button of the `Sigflow` menu.

  The `Sources` windows is displayed.



| | | | | |
|---|---|---|---|---|
| CTI | Last update: Oct. 7, 2022, 12:06 p.m.. | 1 Category | 3838 Rules | View |
| ETPRO | Last update: Oct. 7, 2022, 12:06 p.m.. | 47 Categories | 25312 Rules | View |
| LastInfoSec | Last update: Oct. 7, 2022, 12:06 p.m.. | 1 Category | 0 Rules | View |

SOURCES-01

Two methods are possible:
  - Method 1: HTTP URL **or**
  - Method 2: Upload

- **Method 1**: HTTP URL

  From the source management interface:

- Click on the `Add custom source` link (5)
- Enter a name for the added source
- Choose the `HTTP URL` method
- Choose the file format of the added rules: TAR archive (Signatures files in tar archive) or plain text file (Individual Signatures file)
- Enter the URL of the target file on the remote HTTP server
- Tick the ruleset in which to add the source - multiple ticks are possible
- If necessary, add a comment (optional)
- Click on the `Submit` button.

- **Method 2**: Upload

From the source management interface:

- Click on the `Add custom source` link
- Enter a name for the added source
- Choose the `Upload` method
- Choose the file format of the added rules: TAR archive (Signatures files in tar archive) or plain text file (Individual Signatures file)
- Tick the ruleset in which to add the source - multiple ticks are possible
- Choose the rules file to be added
- If necessary, add a comment (optional)
- Click on the `Submit` button.

Checks are made, for example:

- for example, the message `Error during source update: Invalid URL 'toto.com': No scheme supplied. Perhaps you meant http://toto.com?`
- for example, the message `Invalid filename` indicates that the source name format is not a file name

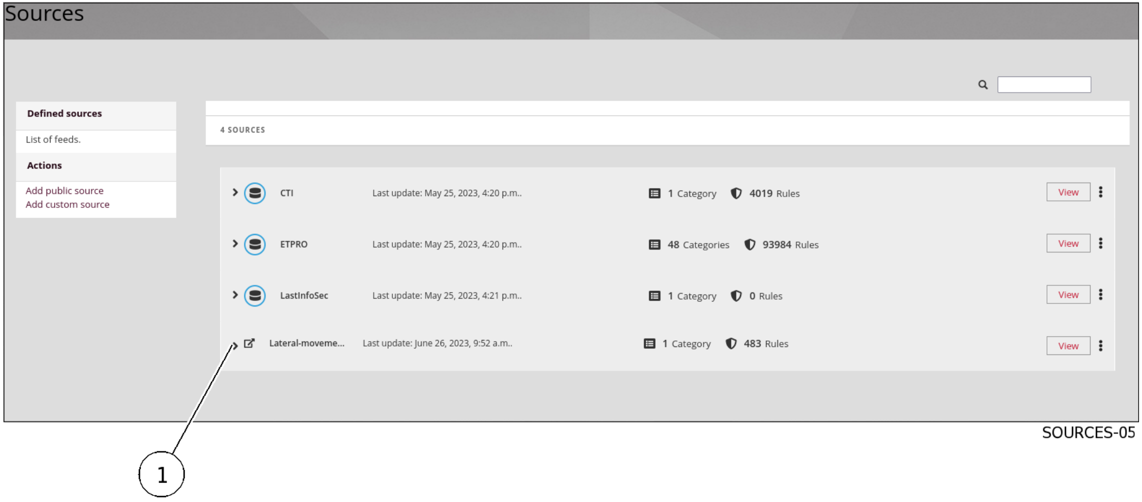
> **Note:**
>
> The rule files in the TAR archive enable creating categories within the source. The sub-folders in the archive will be the future source categories.

### 7.3.1.7 Procedure to delete a source

- From the navigation bar, click successively on:

- The `Config` button
- The `Sources` button of the `Sigflow` menu.

  The `Sources` windows is displayed.



Sources

Defined sources

List of feeds.

Actions

Add public source
Add custom source

4 SOURCES

| | | | | | |
|---|---|---|---|---|---|
| CTI | Last update: May 25, 2023, 4:20 p.m.. | 1 Category | 4019 Rules | View | ⋮ |
| ETPRO | Last update: May 25, 2023, 4:20 p.m.. | 48 Categories | 93984 Rules | View | ⋮ |
| LastInfoSec | Last update: May 25, 2023, 4:21 p.m.. | 1 Category | 0 Rules | View | ⋮ |
| Lateral-moveme... | Last update: June 26, 2023, 9:52 a.m.. | 1 Category | 483 Rules | View | ⋮ |

- Click on the three vertical points of the source to be deleted (1).
- Click on the `Delete source` command.

  A message `Are you sure you want to delete object ***?` is displayed.
- If necessary, add a comment (optional).
- Click on the `Delete object` button.

**Or**

- Click on the `View` button of the desired source
- Click on the `Delete` link, in the list of actions on the left

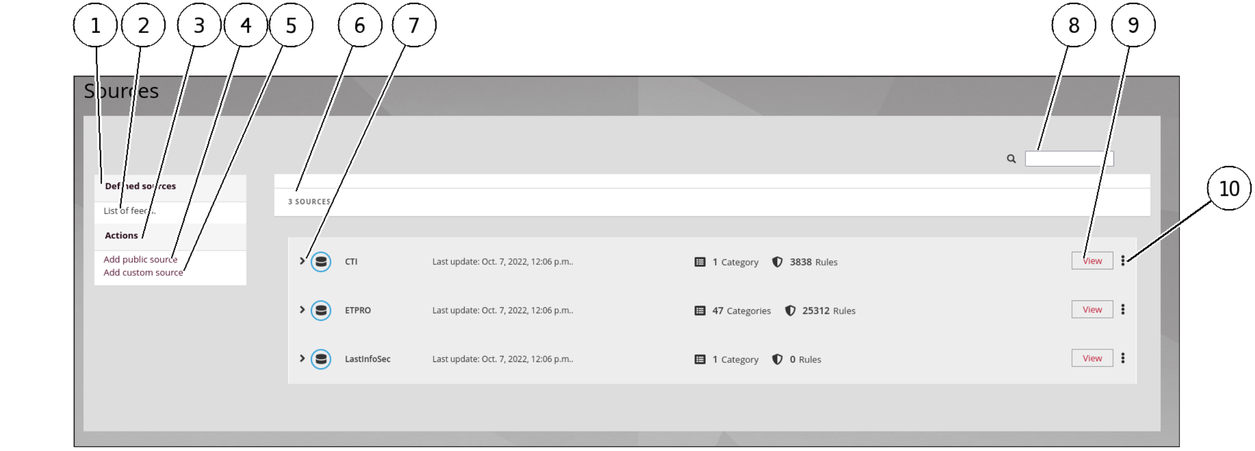
A message `Are you sure you want to delete object ***?` is displayed.
- If necessary, add a comment (optional)
- Click on the `Delete object` button.

---

### 7.3.1.8 Procedure to edit a source

- From the navigation bar, click successively on:
- The `Config` button
- The `Sources` button of the `Sigflow` menu.

  The `Sources` windows is displayed.



Sources

Defined sources

List of feeds..

Actions

Add public source
Add custom source

3 SOURCES

CTI Last update: Oct. 7, 2022, 12:06 p.m.. 1 Category 3838 Rules View

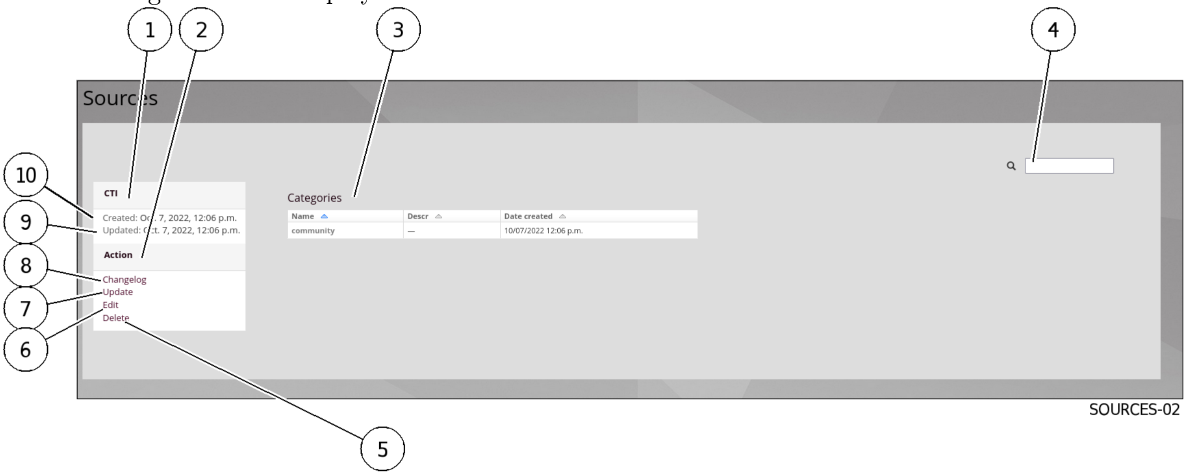
ETPRO Last update: Oct. 7, 2022, 12:06 p.m.. 47 Categories 25312 Rules View

LastInfoSec Last update: Oct. 7, 2022, 12:06 p.m.. 1 Category 0 Rules View

SOURCES-01

- Click on the `View` button (9) of the desired source.

  The following window is displayed.



Sources

CTI

Created: Oct. 7, 2022, 12:06 p.m.
Updated: Oct. 7, 2022, 12:06 p.m.

Action

Changelog
Update
Edit
Delete

Categories

| Name | Descr | Date created |
|---|---|---|
| community | — | 10/07/2022 12:06 p.m. |

SOURCES-02

- Click on `Edit` (6)
- Change the desired parameters: method, file type, public source, and rules file
- Add a comment if necessary - optional
- Click on the `Submit` button.

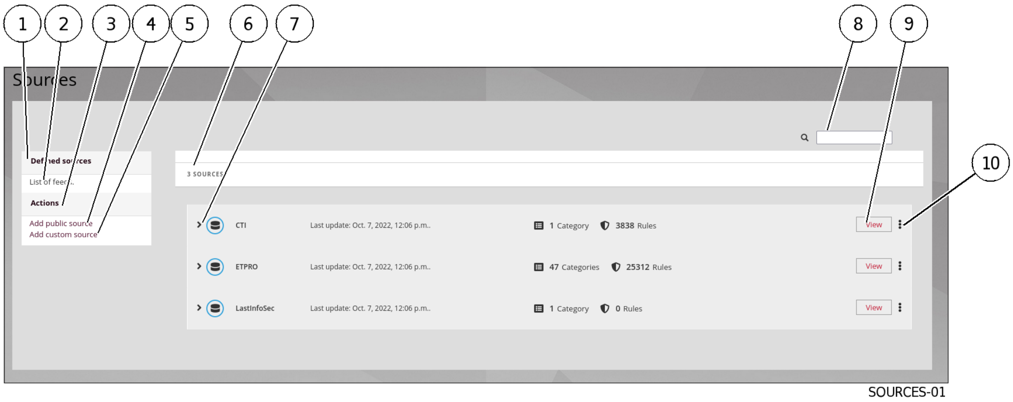
---

#### 7.3.1.9 Procedure to update a source

**Note:**

Updating sources via this procedure only applies to customized or public sources.
The update is performed if the rules file of the remote server or editor has been itself updated.

- From the navigation bar, click successively on:
  - The `Config` button
  - The `Sources` button of the `Sigflow` menu.



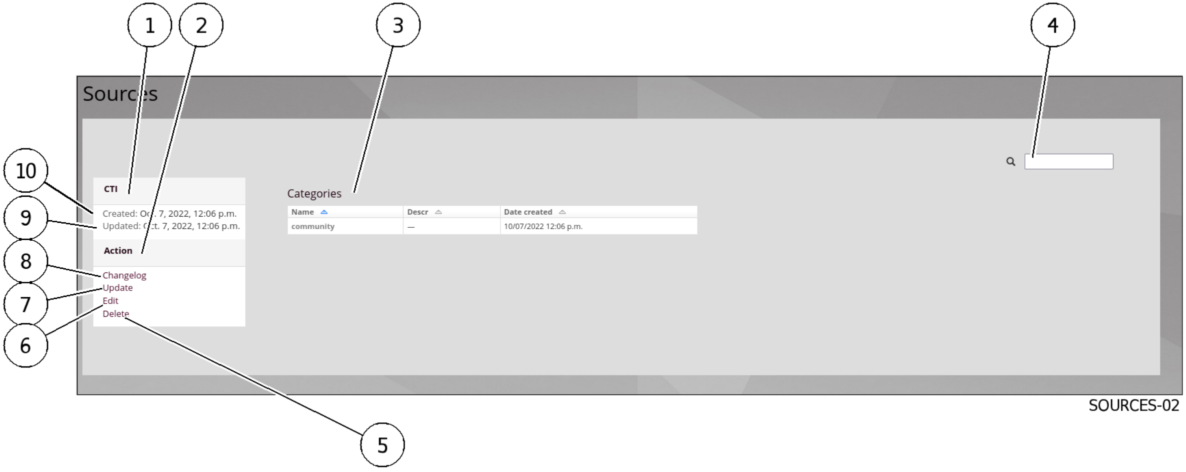
CTI Last update: Oct. 7, 2022, 12:06 p.m.. 1 Category 3838 Rules

ETPRO Last update: Oct. 7, 2022, 12:06 p.m.. 47 Categories 25312 Rules

LastInfoSec Last update: Oct. 7, 2022, 12:06 p.m.. 1 Category 0 Rules

SOURCES-01

- Click on the `View` button (9) of the desired source.
  The following window is displayed.

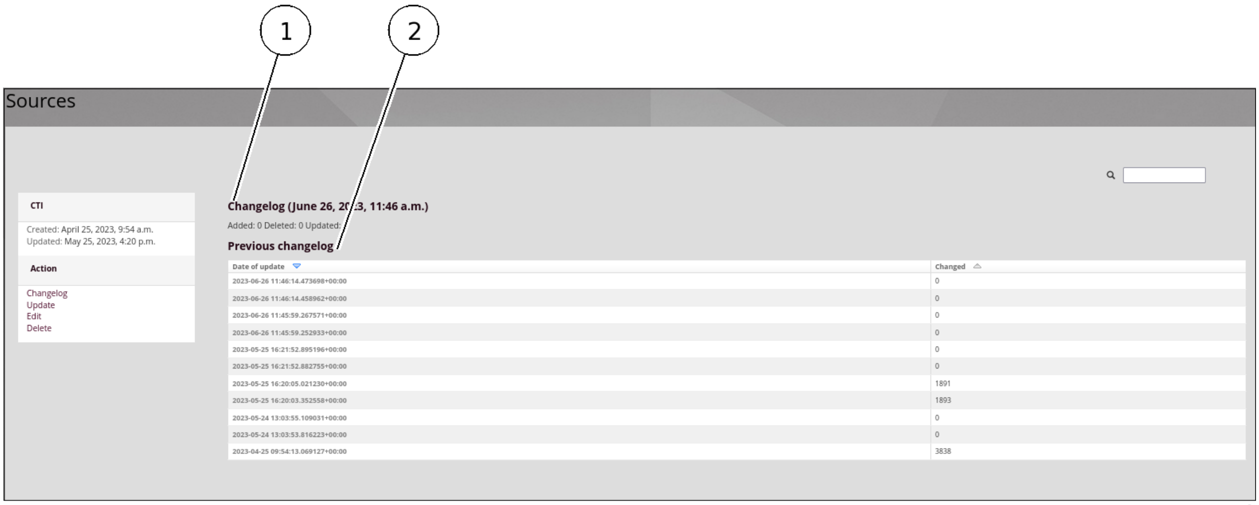


Created: Oct. 7, 2022, 12:06 p.m.
Updated: Oct. 7, 2022, 12:06 p.m.

| Name | Descr | Date created |
|---|---|---|
| community | — | 10/07/2022 12:06 p.m. |

SOURCES-02

- Click on `Update` (7)
  The following screen is displayed.



Created: April 25, 2023, 9:54 a.m.
Updated: May 25, 2023, 4:20 p.m.

Changelog (June 26, 2023, 11:46 a.m.)

Added: 0 Deleted: 0 Updated:

Previous changelog

| Date of update | Changed |
|---|---|
| 2023-06-26 11:46:14.473698+00:00 | 0 |
| 2023-06-26 11:46:14.458962+00:00 | 0 |
| 2023-06-26 11:45:59.267571+00:00 | 0 |
| 2023-06-26 11:45:59.252933+00:00 | 0 |
| 2023-05-25 16:21:52.895196+00:00 | 0 |
| 2023-05-25 16:21:52.882755+00:00 | 0 |
| 2023-05-25 16:20:05.021230+00:00 | 1891 |
| 2023-05-25 16:20:03.352558+00:00 | 1893 |
| 2023-05-24 13:03:55.109031+00:00 | 0 |
| 2023-05-24 13:03:53.816223+00:00 | 0 |
| 2023-04-25 09:54:13.069127+00:00 | 3838 |

SOURCES-06

The window shows:
- The summary (1)
- History (2)

It is possible to click on a changelog to view the content.

## 7.3.2 Creating a SIGFLOW engine ruleset

### 7.3.2.1 Introduction

The security policy in detection terms is held in what is called a ruleset.
The ruleset contains the rule sources enabling detection.
The detection rules in the ruleset will enable the GCap to raise security alerts on the traffic being scanned.
Multiple rulesets can be used to apply multiple security policies to the various capture points.

**Note:**

Managing a ruleset is only available to users assigned the role of operator.

This procedure describes:

- Creating a ruleset
- Managing a ruleset

| For | go to |
|---|---|
| Creating a ruleset | *Procedure to create a ruleset* |
| Displaying a ruleset | *Procedure to display an existing ruleset* |
| Copying a ruleset | *Procedure to copy a ruleset* |
| Deleting a ruleset | *Procedure to delete a ruleset* |
| Editing a ruleset | *Procedure to edit a ruleset* |
| Exporting a ruleset | *Procedure to export a ruleset* |
| Updating a ruleset | *Procedure to update a ruleset* |

The configuration interface is described in *`Config - sigflow/rulesets` screen of the legacy web UI*.

#### 7.3.2.2 Prerequisites

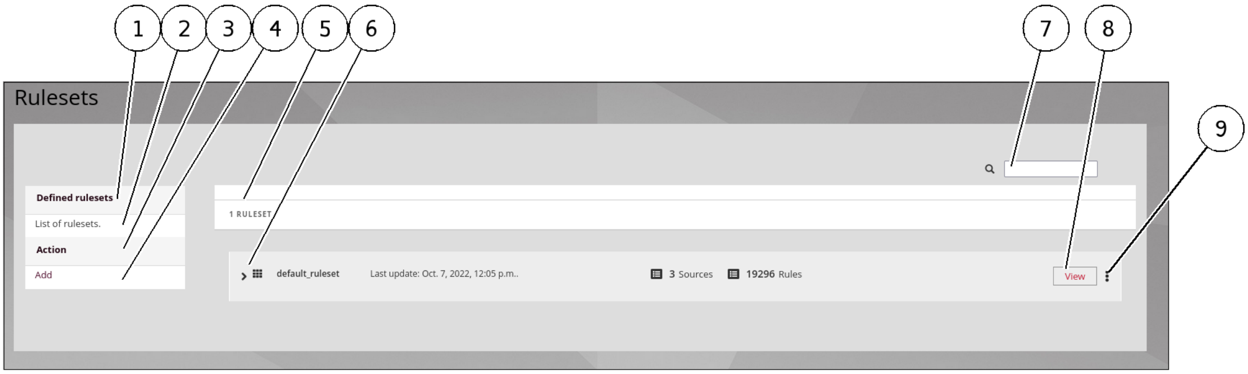
User : member of **Operator** group

#### 7.3.2.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

#### 7.3.2.4 Procedure to create a ruleset

- From the navigation bar, click successively on :
- The `Config` button
- The `Rulesets` button of the `Sigflow` menu.
  The `Rulesets` window is displayed.



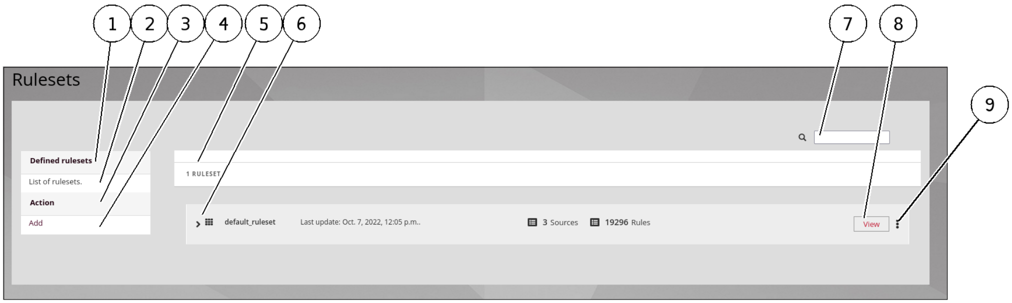
RULESSET-01

From the ruleset management interface:

- Click on the `Add` link
- Enter a name for the created ruleset
- Tick the sources to be added to the ruleset
- Leave the `Activate all categories in selected sources` checkbox ticked
- Leave the `Action`, `Lateral`, and `Target` transformation fields as default
- If necessary, add a comment (optional)
- Click on `+ Add`

#### 7.3.2.5 Procedure to display an existing ruleset

- From the navigation bar, click successively on :
  - The `Config` button
  - The `Rulesets` button of the `Sigflow` menu.
    The `Rulesets` window is displayed.



RULESSET-01

From the ruleset management interface, the available rulesets are displayed.

- To see the contents of a ruleset, click on the `View` button (8).

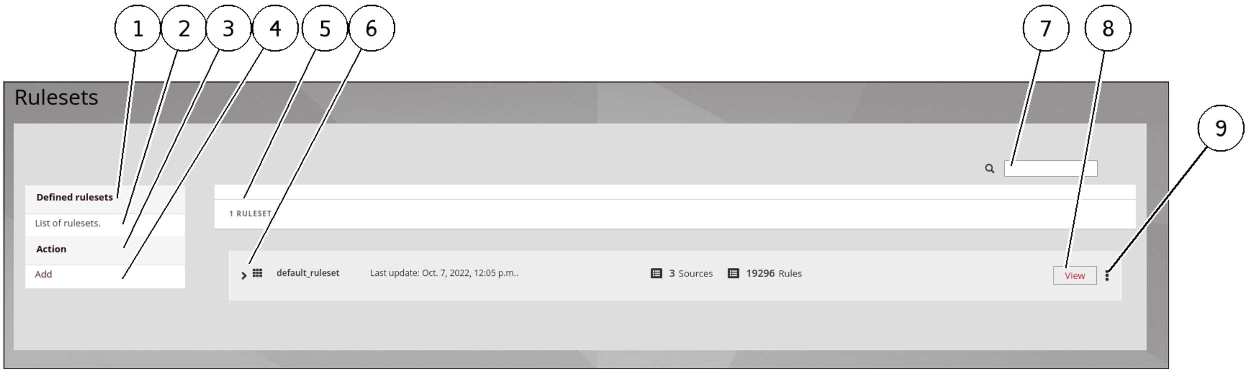
---

#### 7.3.2.6 Procedure to copy a ruleset

This option is used to duplicate the Ruleset, the copy will take into account the sources associated with the Ruleset.
The administrator can decide to make a duplicate of the Ruleset in order to assign it to another probe **GCAP** for example according to the network flows that transit. The Ruleset is specific and must be optimized according to the probe to which it will be assigned.

- From the navigation bar, click successively on :

- The `Config` button
- The `Rulesets` button of the `Sigflow` menu.
  The `Rulesets` window is displayed.



RULESSET-01

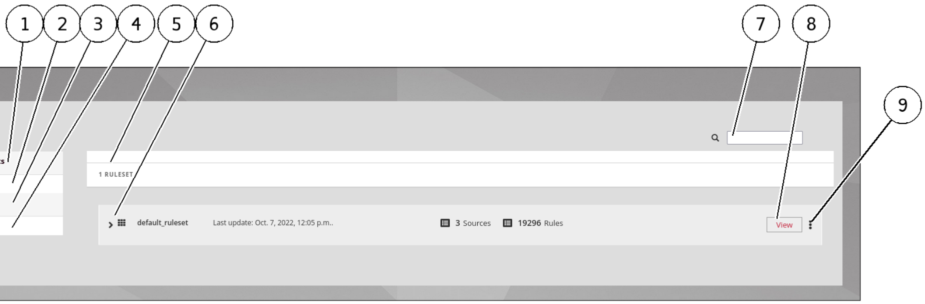
- Click on the three vertical dots (9)
- Click on the `Copy ruleset` command
- Enter the desired name for the new ruleset
- If necessary, add a comment (optional)
- Click on the `Submit` button.

---

#### 7.3.2.7 Procedure to delete a ruleset

Deleting the Ruleset is irreversible but will not cause the deletion of the sources and signatures that were linked to the Ruleset.

- From the navigation bar, click successively on :
  - The `Config` button
  - The `Rulesets` button of the `Sigflow` menu.
    The `Rulesets` window is displayed.



RULESSET-01

- **method 1** :

- Click on the three vertical dots (9)
- Click on the `Delete ruleset` command
- If necessary, add a comment (optional)
- Click on the `Delete object` button

**Or**

- **method 2** :

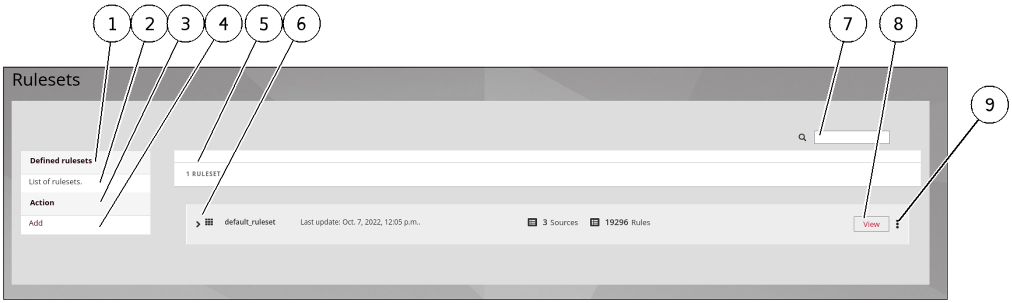
- Click on the `View` button of the desired ruleset
- Click on the `Delete` link, in the list of actions on the left
- If necessary, add a comment (optional)
- Click on the `Delete object` button

---

#### 7.3.2.8 Procedure to edit a ruleset

A Ruleset can be edited so that the operator can make changes to the sources, categories or rules present in the Ruleset.
These changes can be made to the rules in order to adapt a public rule to specific information system requirements, or to a specific need.

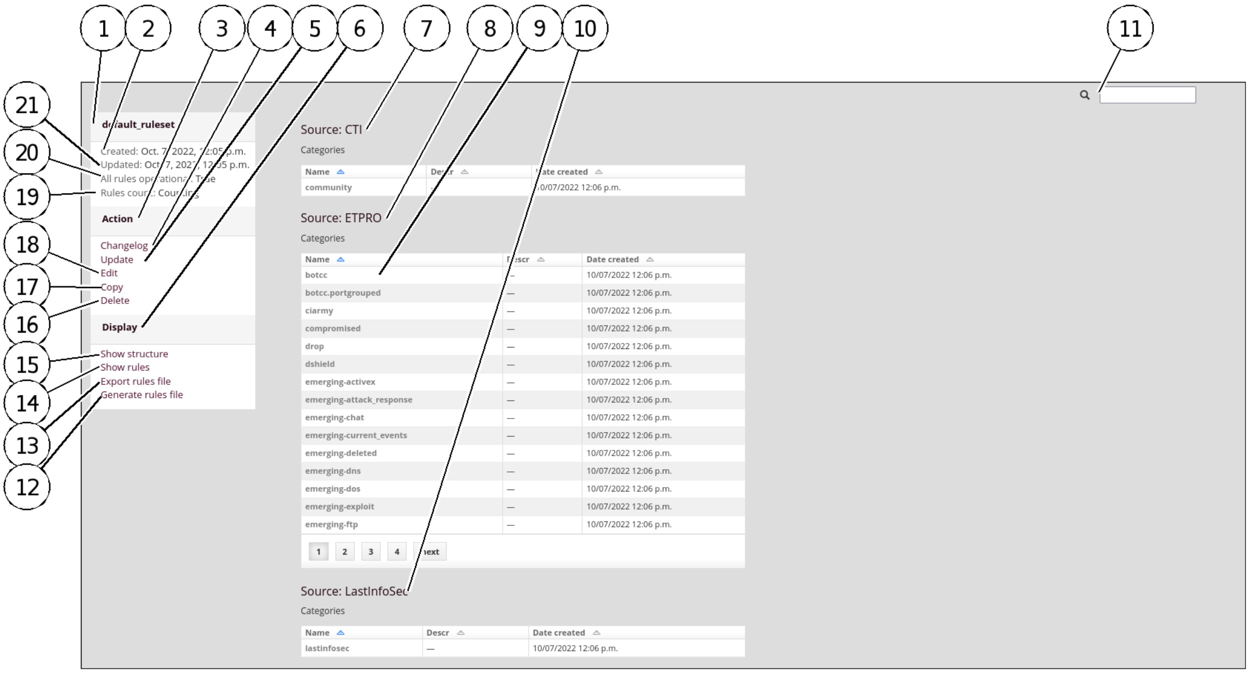
- From the navigation bar, click successively on :
  - The `Config` button
  - The `Rulesets` button of the `Sigflow` menu.
    The `Rulesets` window is displayed.



default_ruleset Last update: Oct. 7, 2022, 12:05 p.m.. 3 Sources 19296 Rules

RULESSET-01

- Click on the `View` button (8).



Created: Oct. 7, 2022, 12:05 p.m.
Updated: Oct. 7, 2022, 12:05 p.m.
All rules operational: True
Rules count: Counting

Source: CTI

Categories

| Name | Descr | Date created |
|---|---|---|
| community | - | 10/07/2022 12:06 p.m. |

Source: ETPRO

Categories

| Name | Descr | Date created |
|---|---|---|
| botcc | – | 10/07/2022 12:06 p.m. |
| botcc.portgrouped | — | 10/07/2022 12:06 p.m. |
| ciarmy | — | 10/07/2022 12:06 p.m. |
| compromised | — | 10/07/2022 12:06 p.m. |
| drop | — | 10/07/2022 12:06 p.m. |
| dshield | — | 10/07/2022 12:06 p.m. |
| emerging-activex | — | 10/07/2022 12:06 p.m. |
| emerging-attack_response | — | 10/07/2022 12:06 p.m. |
| emerging-chat | — | 10/07/2022 12:06 p.m. |
| emerging-current_events | — | 10/07/2022 12:06 p.m. |
| emerging-deleted | — | 10/07/2022 12:06 p.m. |
| emerging-dns | — | 10/07/2022 12:06 p.m. |
| emerging-dos | — | 10/07/2022 12:06 p.m. |
| emerging-exploit | — | 10/07/2022 12:06 p.m. |
| emerging-ftp | — | 10/07/2022 12:06 p.m. |

Source: LastInfoSec

Categories

| Name | Descr | Date created |
|---|---|---|
| lastinfosec | — | 10/07/2022 12:06 p.m. |

RULESSET-02

- Click on the `Edit` link (18).

> **Note:**
>
> **Other Method**
>
> - Click on the three vertical dots (9).
> - Click on the `Èdit` command.

Once in the edit menu, it is possible to:

- Change the name of the ruleset.
- Change the `Action`, `Lateral`, and `Target` transformation fields.

  Changes will be applied to all categories in the *Ruleset*.

> **Note:**
>
> Pour plus d'informations, voir le paragraphe *Transform rule*:

- Change the comment
- Add or remove sources from the ruleset via the `Edit Sources` link.

  This option is used to manually enable or disable the action of a source on a Ruleset.

  Once unchecked, signatures will no longer be matched by specific streams and will no longer raise alerts on the interface.

- Add or remove categories from a ruleset source via the `Edit categories` link.
  This option is used to manually enable or disable the action of a category on a Ruleset.
  Once unchecked, signatures will no longer be matched by specific streams and will no longer raise alerts on the interface.
- Add rules to the disabled list via the `Add rules to disabled list` link.
  It is possible to disable a signature associated with a ruleset. Disabling a rule does not permanently delete it.
- Remove rules from the disabled list via the `Remove rules from disabled list` link.
  The rule returns to the active ruleset rules.

- Click on the `Submit` button to validate the changes.

**Note:**

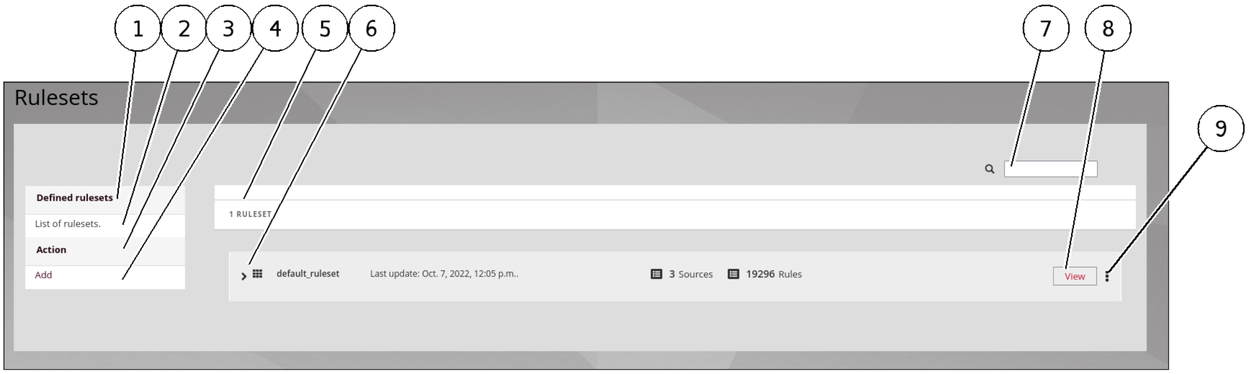
When adding a source, it is necessary to manually add the categories of this source so they are present in the source.
If this is not done, the ruleset source will be empty.

---

### 7.3.2.9 Procedure to export a ruleset

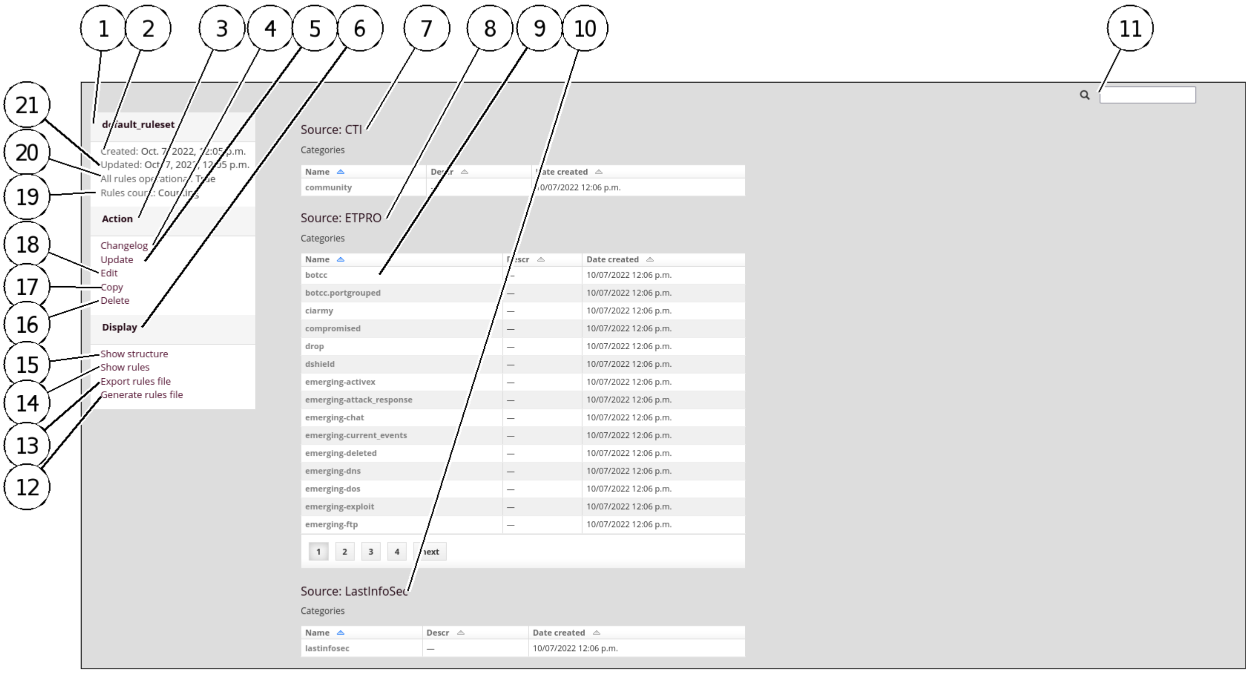
- From the navigation bar, click successively on :

- The `Config` button
- The `Rulesets` button of the `Sigflow` menu.
  The `Rulesets` window is displayed.



RULESSET-01

- Click on the `View` button (8).



**default_ruleset**

Created: Oct. 7, 2022, 12:05 p.m.
Updated: Oct. 7, 2022, 12:05 p.m.
All rules operational: True
Rules count: Counting

**Action**

Changelog
Update
Edit
Copy
Delete

**Display**

Show structure
Show rules
Export rules file
Generate rules file

Source: CTI

Categories

| Name | Descr | Date created |
|---|---|---|
| community | - | 10/07/2022 12:06 p.m. |

Source: ETPRO

Categories

| Name | Descr | Date created |
|---|---|---|
| botcc | — | 10/07/2022 12:06 p.m. |
| botcc.portgrouped | — | 10/07/2022 12:06 p.m. |
| ciarmy | — | 10/07/2022 12:06 p.m. |
| compromised | — | 10/07/2022 12:06 p.m. |
| drop | — | 10/07/2022 12:06 p.m. |
| dshield | — | 10/07/2022 12:06 p.m. |
| emerging-activex | — | 10/07/2022 12:06 p.m. |
| emerging-attack_response | — | 10/07/2022 12:06 p.m. |
| emerging-chat | — | 10/07/2022 12:06 p.m. |
| emerging-current_events | — | 10/07/2022 12:06 p.m. |
| emerging-deleted | — | 10/07/2022 12:06 p.m. |
| emerging-dns | — | 10/07/2022 12:06 p.m. |
| emerging-dos | — | 10/07/2022 12:06 p.m. |
| emerging-exploit | — | 10/07/2022 12:06 p.m. |
| emerging-ftp | — | 10/07/2022 12:06 p.m. |

1 2 3 4 next

Source: LastInfoSec

Categories

| Name | Descr | Date created |
|---|---|---|
| lastinfosec | — | 10/07/2022 12:06 p.m. |

RULESSET-02

- Click on the `Export rules file` link (13).
  Exporting the ruleset enables downloading a ".rules" file containing all the rules of the ruleset in question. This may enable some rules to be reimported into other tools.

**Important:**

This feature does not serve as a ruleset backup. It is not possible to import the exported file back into Gcenter as is. This would result in duplicate rules.

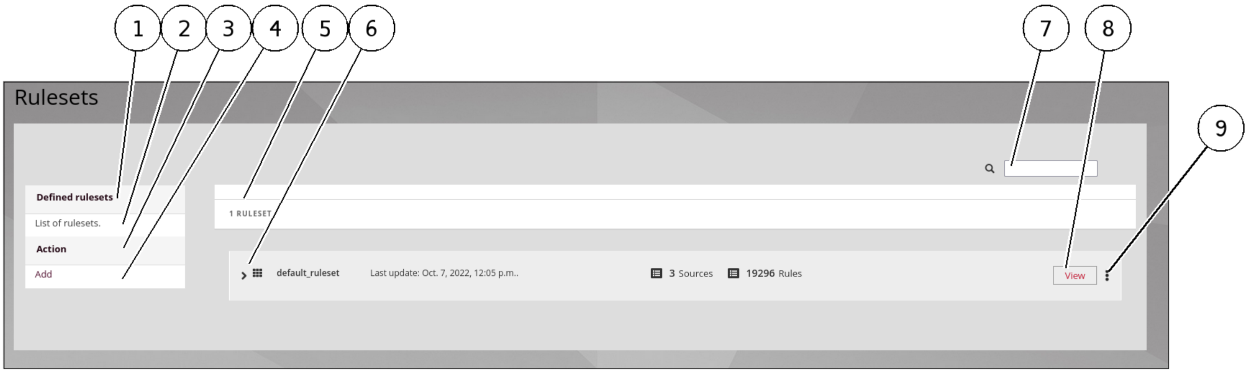
### 7.3.2.10 Procedure to update a ruleset

**Note:**

The update via this procedure only concerns the custom or public sources of the ruleset. The update is performed if the ruleset file of the remote server or editor has been updated.

- From the navigation bar, click successively on :

- The `Config` button
- The `Rulesets` button of the `Sigflow` menu.
  The `Rulesets` window is displayed.



Rulesets

Defined rulesets

List of rulesets.

Action

Add

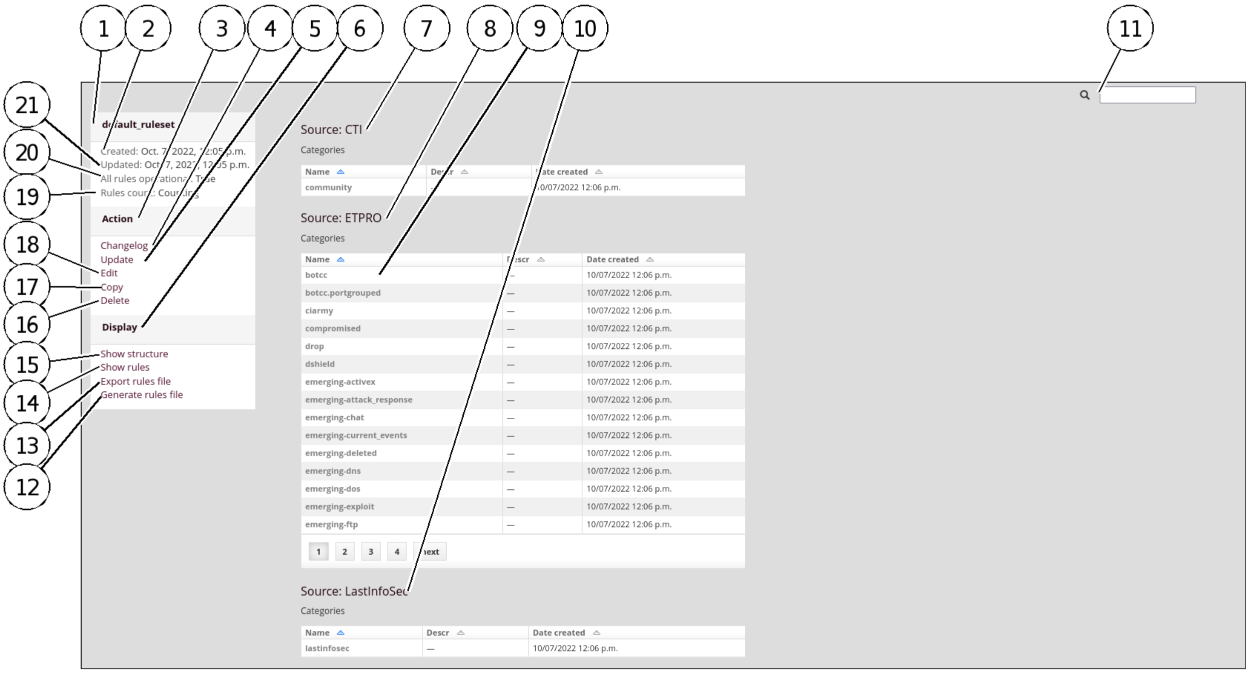
1 RULESET

default_ruleset Last update: Oct. 7, 2022, 12:05 p.m.. 3 Sources 19296 Rules View

RULESSET-01

- Click on the `View` button (8) of the desired ruleset.

> **Note:**
>
> **Other Method**
>
> - Click on the three vertical dots (9)
> - Click on the `Update ruleset` command



default_ruleset

Created: Oct. 7, 2022, 12:05 p.m.
Updated: Oct. 7, 2022, 12:05 p.m.
All rules operational: True
Rules count: Counting

Action

Changelog
Update
Edit
Copy
Delete

Display

Show structure
Show rules
Export rules file
Generate rules file

Source: CTI

Categories

| Name | Descr | Date created |
|---|---|---|
| community | — | 10/07/2022 12:06 p.m. |

Source: ETPRO

Categories

| Name | Descr | Date created |
|---|---|---|
| botcc | — | 10/07/2022 12:06 p.m. |
| botcc.portgrouped | — | 10/07/2022 12:06 p.m. |
| ciarmy | — | 10/07/2022 12:06 p.m. |
| compromised | — | 10/07/2022 12:06 p.m. |
| drop | — | 10/07/2022 12:06 p.m. |
| dshield | — | 10/07/2022 12:06 p.m. |
| emerging-activex | — | 10/07/2022 12:06 p.m. |
| emerging-attack_response | — | 10/07/2022 12:06 p.m. |
| emerging-chat | — | 10/07/2022 12:06 p.m. |
| emerging-current_events | — | 10/07/2022 12:06 p.m. |
| emerging-deleted | — | 10/07/2022 12:06 p.m. |
| emerging-dns | — | 10/07/2022 12:06 p.m. |
| emerging-dos | — | 10/07/2022 12:06 p.m. |
| emerging-exploit | — | 10/07/2022 12:06 p.m. |
| emerging-ftp | — | 10/07/2022 12:06 p.m. |

1 2 3 4 next

Source: LastInfoSec

Categories

| Name | Descr | Date created |
|---|---|---|
| lastinfosec | — | 10/07/2022 12:06 p.m. |

RULESSET-02

- Click on `Update` (5)

### 7.3.3 Modifying SIGFLOW engine rules

#### 7.3.3.1 Introduction

Detection rules are what enable the GCap to raise alerts on monitored traffic.
As a reminder:

- Rules are found in categories
- Categories are found in sources
- Sources are placed in rulesets

It is possible to directly influence the operation of a rule, from the **Sigflow** tool, by limiting or deleting alerts for the rule within a ruleset.
The various actions possible for modifying the behaviour of a rule are the following:

- The implementation of a transform rule
- The disabling of a transform rule
- The enabling of a transform rule
- The implementation of a Threshold rule
- The implementation of a The Suppress rule

> **Note:**
>
> In order to find a rule to be modified, it is possible to use the search function in the top right-hand corner of all the pages of the Sigflow menu.
> It is enough to search for the SID or the name of the desired rule.

---

##### 7.3.3.1.1 Transform rule

###### 7.3.3.1.1.1 Concept

The transformation rules or "Transform rules" allow to modify the behaviour of the rule by modifying its content.
This amendment may be made on a rule-by-rule basis. In this case, the amendment applies only to this rule.
This change can:

- Modify the content of a rule, for example, modify the action of a rule by replacing the **Alert** action defined in the rule with another action of type **drop** or **reject**. This change is defined in the transformation rule
- Add a keyword to the rule (**bypass** or **filestore**) defined in the transformation rule
- Change the content of the rule by inheritance. By configuring the rule with the default setting (**category default**) of the container (the category), the rule inherits the contents of this parameter
- This can be done at the category level. In this case, the changes are applicable for all rules contained in this category.

  Change handling is the same as at the rule level except the default setting is **ruleset default** set at the ruleset level.
- This can be done at the ruleset level. In this case, the changes are applicable for all rules contained in all categories of the ruleset.

  Change management is the same as category level except that there is no default setting.

---

#### 7.3.3.1.1.2 Parameters

The various possible parameters are:

- The `Action` field determines the measure to be applied to the rule.

  For example, modifying the action of a rule by replacing the **Alert** action defined in the rule with another action of type **drop** or **reject** or add a keyword to the rule (bypass/filestore):

  - `Filestore`: If a rule matches then the file defined in the flow will be processed by Sigflow and stored like any other package.

    And this even if there is no rule for file generation by filemagic/extension.
  - `Bypass`: If a rule contains a 'bypass', the flow defined by that rule will not be analyzed regardless of its content.
  - `None`: no transformation is carried out.
  - `Category Default`: the rule applies the change defined at the category level and inherits this configuration.
  - `Ruleset`: the category applies the change defined at the ruleset level and inherits this configuration.
  - For choices `Reject` and `Drop`: As a reminder, the GCap is in IDS mode and not IPS i.e:

  - in IPS (Prevention) mode, the network flow passes through the detection system which can let it pass but also reject it (action `Reject`) or delete it (action `Drop`)
  - in IDS (Detection) mode, the network flow is copied by the TAP to the GCap so none of the actions `Reject` or `Drop` make sense since the GCap does not have any action on the main flow.

**Note:**

The default action in the solution is **alert**. As GCap is an IDS, not an IPS, normally there is no need to change this value.

- The `Lateral` field enables the scope of the rule to be changed at the network variable level.

  If a rule has a source $HOME_NET and a destination $EXTERNAL_NET and both sides of the traffic being analysed are in $HOME_NET, then the rule will not raise an alert and lateral movements will no longer be detected.

  Thus, the transformation enables the value of the variable to be changed from "$EXTERNAL_NET" to "any" in order to broaden the scope to detect lateral movements.

  Here are the possible values:

- `Auto`: substitution is made if the signature checks certain properties
- `None`: the replacement is not performed
- `Yes`: $EXTERNAL_NET is replaced by any other IP (any)
- `Category Default`: the rule applies the change defined at the category level and inherits this configuration
- `Ruleset Default`: the category applies the change defined at the ruleset level and inherits this configuration

- The field `Target` adds the field "target:[src_ip dest_ip]" in the rule.

  It generates additional metadata indicating who is the target of the attack.

  Possible values are:

- `Auto`: an algorithm is used to determine the target if one is present
- `Destination`: the target is the receiving IP
- `None`: the replacement is not performed
- `Ruleset Default`: the category applies the change defined at the ruleset level and inherits this configuration.
- `Source`: the target is the originating IP

#### 7.3.3.1.2 Threshold rule

`Threshold rules` enable limiting the number of alerts for a given rule.
There are 3 types of threshold rules:

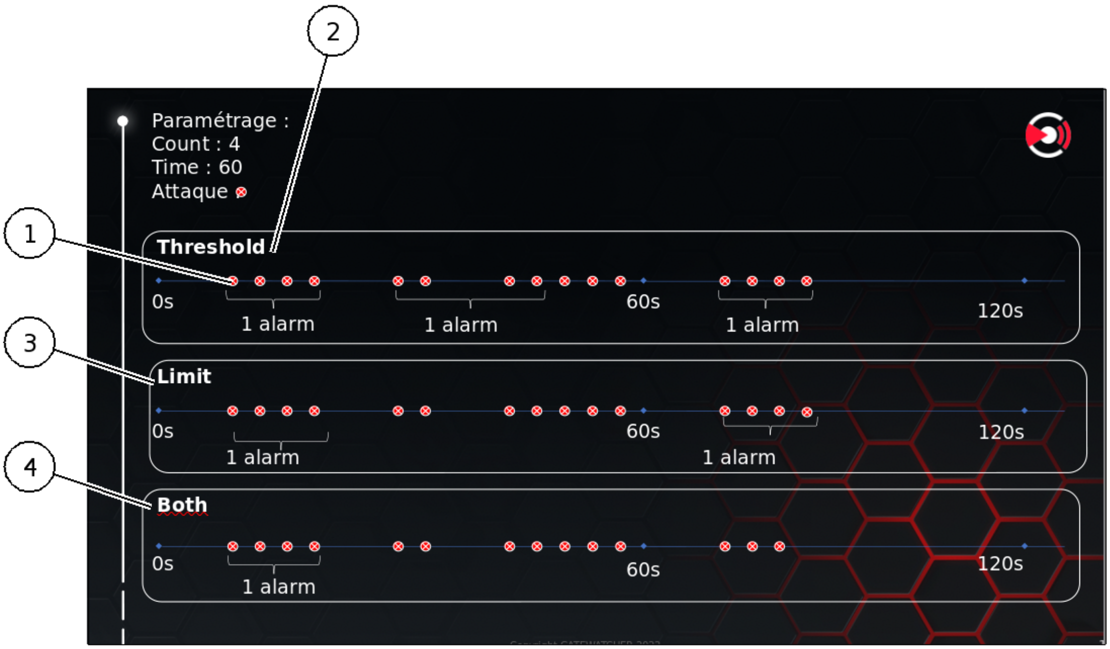
- `Limit`: enables a rule to sound an alert only a defined number of times. If the value is N, the alert will be raised N times and then not raised again within the chosen time interval.
- `Threshold`: Enables a rule to sound only after a defined number of alerts. If the value is N, the alert will be raised after N alerts within the chosen time interval.
- `Both`: Enables combining the `threshold` and `limit` types. It applies both thresholding and limiting.

**Note:**

The rules created are available in the ruleset view page at the top right.

Example:

In the view below, the same value is defined as limit and threshold.



GCENTER-THRESOLD

In the `Threshold` zone (2), the threshold counter is set to four. So for the period considered (here 60 seconds), an alarm (1) is activated every 4 attacks.
In the `Limit` zone (3), the limit counter is set to four. So for the period considered (here 60 seconds), an alarm is activated only for the first 4 attacks.
In the `Both` field (4), the counter is set to four. So for the period considered (here 60 seconds), an alarm is activated only for the first 4 attacks (limit value reached).

#### 7.3.3.1.3 Suppress rule

**Suppress rules** allow disabling alerts for a rule on a specific network or IP.
Multiple networks or IPs can be added separated by ' ,'.

Example:

> A rule raises 10 alerts every hour from the same IP source.
> It turns out that this is a false positive and that these alerts are irrelevant.
> In this case, it is appropriate to disable the rule for the IP source in question.
> The rule remains active on the rest of the network.

**Note:**

The rules created are available in the ruleset view page at the top right.

| For | go to |
|---|---|
| Transform rule | *Procedure to setup a transformation rule* |
| Disabling a rule | *Procedure to disable a rule* |
| Enabling a rule | *Procedure to enable a rule* |
| Threshold rule | *Procedure to setup a threshold rule* |
| Suppress rule | *Procedure to setup a suppress rule* |

This configuration interface is described in *`Config - sigflow/rulesets` screen of the legacy web UI*.

### 7.3.3.2 Prerequisites

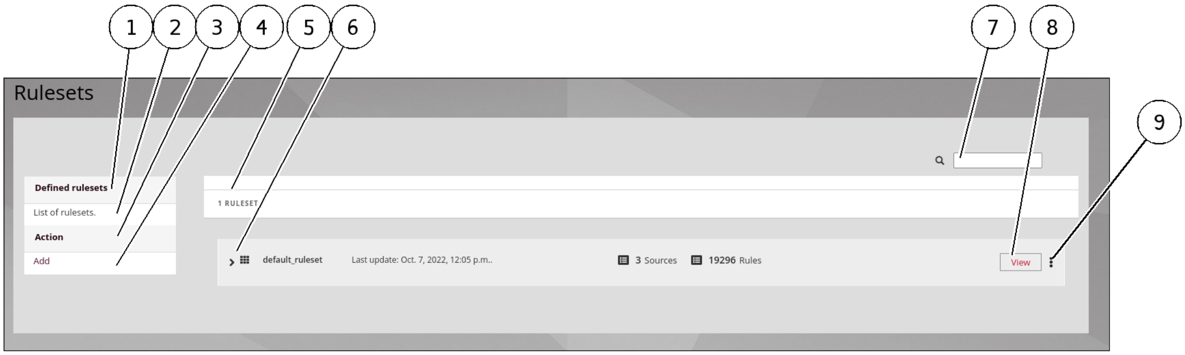
User : member of **Operator** group

### 7.3.3.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

### 7.3.3.4 Procedure to setup a transformation rule

- From the navigation bar, click successively on :
- The `Config` button
- The `Rulesets` button of the `Sigflow` menu.
  The `Rulesets` window is displayed.



RULESSET-01

From the ruleset management interface:

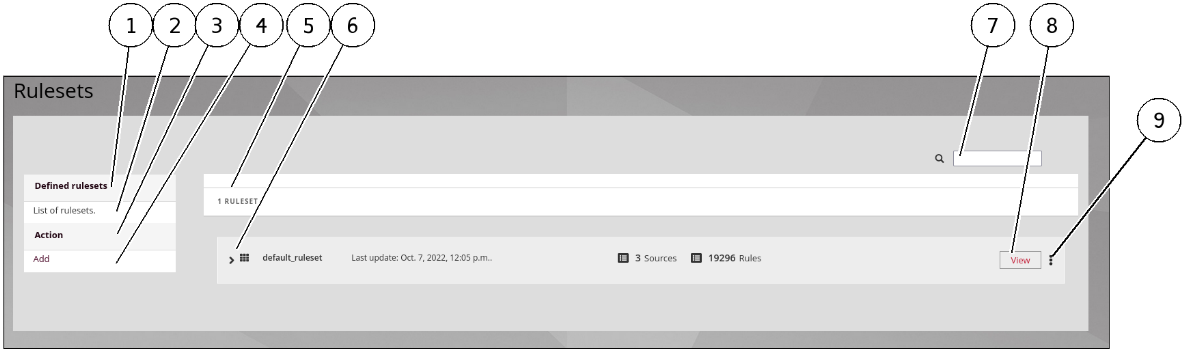
- Look for the SID of the rule to be modified in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Edit rule` link to display the edit menus
- Make sure to be in the `Transform rule` menu
- Tick the rule(s) in which the rule transformation is to be applied
- Change the `Action`, `Lateral`, and `Target` fields as required
- If necessary, add a comment (optional)
- Click on the `Valid` button.

---

### 7.3.3.5 Procedure to disable a rule

- From the navigation bar, click successively on :

- The `Config` button
- The `Rulesets` button of the `Sigflow` menu.
  The `Rulesets` window is displayed.



RULESSET-01

From the ruleset management interface:

- **method 1** :

- Look for the SID of the rule to be disabled in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Disable rule` link
- Tick the rule(s) in which the rule should be disabled
- If necessary, add a comment (optional)
- Click on the `Disable` button

**Or**

- **method 2** :

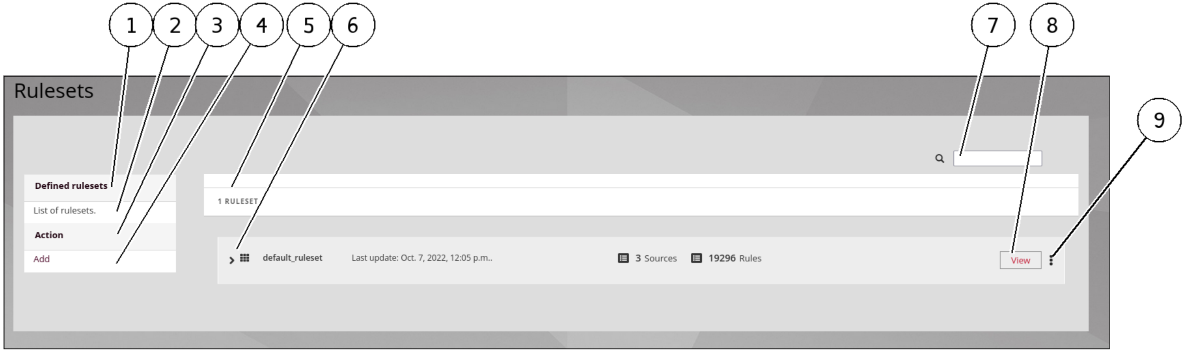
- Look for the SID of the rule to be disabled in the top right-hand bar (7)
- Click on the SID of the rule among the search results

- Click on the `Edit rule` link to display the edit menus
- Click on the `Disable rule` link
- Tick the ruleset(s) in which the rule should be disabled
- If necessary, add a comment (optional)
- Click on the `Disable` button

#### 7.3.3.6 Procedure to enable a rule

- From the navigation bar, click successively on :

- The `Config` button
- The `Rulesets` button of the `Sigflow` menu.
  The `Rulesets` window is displayed.



RULESSET-01

From the ruleset management interface:

- **method 1** :

- Look for the SID of the rule to be enabled in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Enable rule` link
- Tick the ruleset(s) in which the rule should be enabled
- If necessary, add a comment (optional)
- Click on the `Enable` button

**Or**

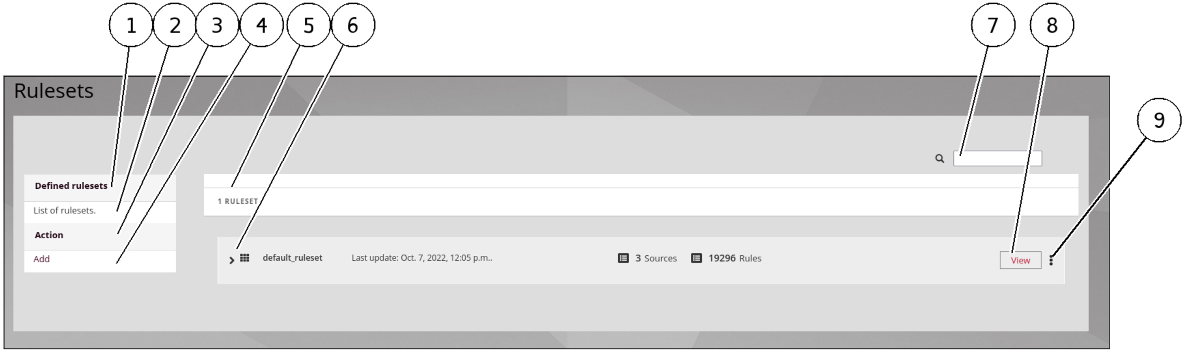
- **method 2** :

- Look for the SID of the rule to be enabled in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Edit rule` link to display the edit menus
- Click on the `Enable rule` link
- Tick the ruleset(s) in which the rule should be enabled
- If necessary, add a comment (optional)
- Click on the `Enable` button

#### 7.3.3.7 Procedure to setup a threshold rule

- From the navigation bar, click successively on :

- The `Config` button
- The `Rulesets` button of the `Sigflow` menu.
  The `Rulesets` window is displayed.



RULESSET-01

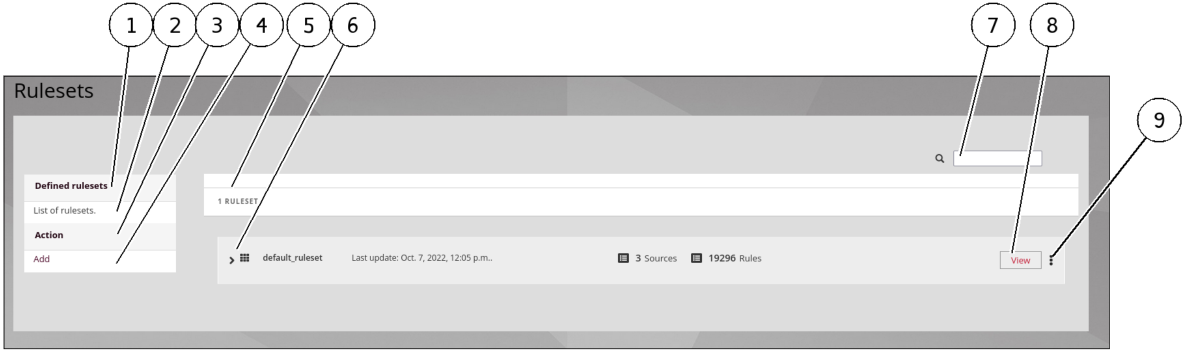
From the ruleset management interface:

- Look for the SID of the rule to be modified in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Edit rule` link to display the edit menus
- Click on the `Threshold rule` link
- Select the type of threshold desired `threshold`, `limit`, or `both`
- Select whether the threshold should apply to the source or the destination
- Enter the desired threshold value. The impact will be different depending on the type of threshold chosen
- Enter the value of the desired time interval in which the threshold will apply
- Tick the ruleset(s) in which the rule threshold is to be applied
- If necessary, add a comment (optional)
- Click on the `Valid` button

#### 7.3.3.8 Procedure to setup a suppress rule

- From the navigation bar, click successively on :

- The `Config` button
- The `Rulesets` button of the `Sigflow` menu.
  The `Rulesets` window is displayed.



RULESSET-01

From the ruleset management interface:

- Look for the SID of the rule to be modified in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Edit rule` link to display the edit menus

- Click on the `Suppress rule` link
- Select the type of threshold desired `threshold`, `limit`, or `both`
- Select whether the threshold should apply to the source or the destination
- Enter the IP address or network on which the rule will be disabled
- Tick the ruleset(s) in which the deletion rule is to be applied
- If necessary, add a comment (optional)
- Click on the `Valid` button

## 7.3.4 Generating a SIGFLOW engine ruleset

### 7.3.4.1 Introduction

**Important:**

It is imperative to generate the ruleset following modifications, otherwise the changes are not deployed on the GCap.

Once the configurations and any modifications are made to the ruleset, it is necessary to "generate" the ruleset.
This action enables the ruleset's status to be saved and all changes to be taken into account.
Otherwise, the modifications are not taken into account by the GCap.
This configuration interface is described in *`Config - sigflow/rulesets` screen of the legacy web UI*.

### 7.3.4.2 Prerequisites

User : member of **Operator** group

### 7.3.4.3 Preliminary operations

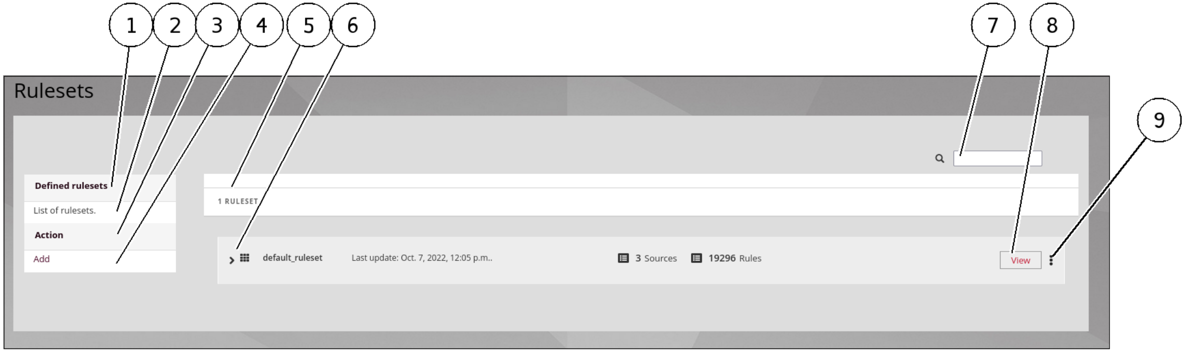
- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

### 7.3.4.4 Procedure

- From the navigation bar, click successively on :

- The `Config` button
- The `Rulesets` button of the `Sigflow` menu.

The `Rulesets` window is displayed.

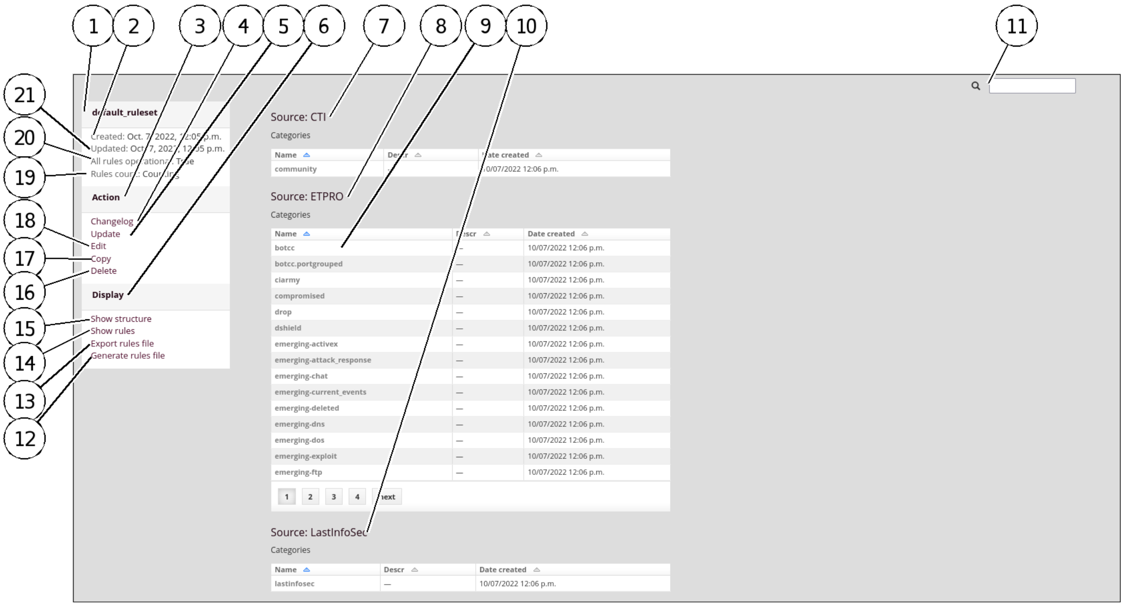


1 RULESET

default_ruleset Last update: Oct. 7, 2022, 12:05 p.m.. 3 Sources 19296 Rules

RULESSET-01

- Click on the `View` button (8) of the desired ruleset



default_ruleset

Created: Oct. 7, 2022, 12:05 p.m.
Updated: Oct. 7, 2022, 12:05 p.m.
All rules operational: True
Rules count: Counting

Source: CTI

Categories

| Name | Descr | Date created |
|---|---|---|
| community | — | 10/07/2022 12:06 p.m. |

Source: ETPRO

Categories

| Name | Descr | Date created |
|---|---|---|
| botcc | — | 10/07/2022 12:06 p.m. |
| botcc.portgrouped | — | 10/07/2022 12:06 p.m. |
| ciarmy | — | 10/07/2022 12:06 p.m. |
| compromised | — | 10/07/2022 12:06 p.m. |
| drop | — | 10/07/2022 12:06 p.m. |
| dshield | — | 10/07/2022 12:06 p.m. |
| emerging-activex | — | 10/07/2022 12:06 p.m. |
| emerging-attack_response | — | 10/07/2022 12:06 p.m. |
| emerging-chat | — | 10/07/2022 12:06 p.m. |
| emerging-current_events | — | 10/07/2022 12:06 p.m. |
| emerging-deleted | — | 10/07/2022 12:06 p.m. |
| emerging-dns | — | 10/07/2022 12:06 p.m. |
| emerging-dos | — | 10/07/2022 12:06 p.m. |
| emerging-exploit | — | 10/07/2022 12:06 p.m. |
| emerging-ftp | — | 10/07/2022 12:06 p.m. |

Source: LastInfoSec

Categories

| Name | Descr | Date created |
|---|---|---|
| lastinfosec | — | 10/07/2022 12:06 p.m. |

RULESSET-02

- Make the necessary changes
- Click on the `Generate rules file` link.

  The message `Successfully generated rules file for xxxxxxxxx` is displayed to indicate that the ruleset was successfully generated (xxxxxxxxx being the name of ruleset_sigflow_01)

## 7.4 Configuring GCaps

This section describes the GCap configurations from the GCenter using the `Gcaps Profiles` menu. For more details on `Gcaps Profiles` menu, see paragraph *Sigflow engine*.

### 7.4.1 Configure Codebreaker then apply the Sigflow rulesets to the GCaps

#### 7.4.1.1 Introduction

The `` `Detection Rulesets` `` section enables applying Rulesets Sigflow to the GCap paired with the GCenter.
It is also possible to configure the codebreaker module for the GCap that includes enabling or disabling shellcode and powershell detection separately.

**Note:**

It is necessary to generate rules for a ruleset before applying it to GCaps. Failure to do so will result in no rules being applied.

**Note:**

Codebreaker is not configurable via `` `Detection Rulesets` `` menu with the CIE license.

As a reminder, the `` `Detection Rulesets` `` menu has three configuration options:

- `` `single tenant` ``:

- assigning a ruleset for all GCap monitoring interfaces
- Enable/disable codebreaker for all GCap monitoring interfaces.

- `` `multi-tenant by interface` ``:

- assigning a ruleset per GCap monitoring interface
- Enable/disable codebreaker per Gap monitoring interface.

- `` `multi-tenant by vlan` ``:

- assigning one ruleset per vlan
- assigning a ruleset for the default vlan for those VLANs not created via the interface
- Enable/disable codebreaker per VLAN
- disable codebreaker for the default vlan for those VLANs not created via the interface

**Note:**

These configuration options are exclusive.
This means that it will not be possible to apply a single tenant and multi-tenant per vlan configuration at the same time.

See section *Web UI `Config - Gcaps profiles` screen*.

| For | go to |
|---|---|
| Single-tenant configuration | *Procedure to setup the `single-tenant`* |
| Configuring multi-tenant by interface | *Procedure to setup the `Multi-tenant by interface`* |
| Configuring multi-tenant by vlan | *Procedure to setup the `Multi-tenant by vlan`* |

### 7.4.1.2 Prerequisites

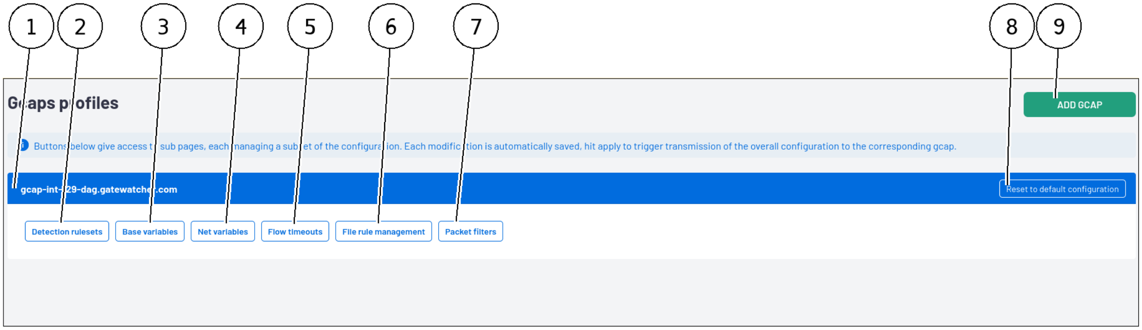
User : member of **Operator** group

### 7.4.1.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

### 7.4.1.4 Procedure to setup the `single-tenant`

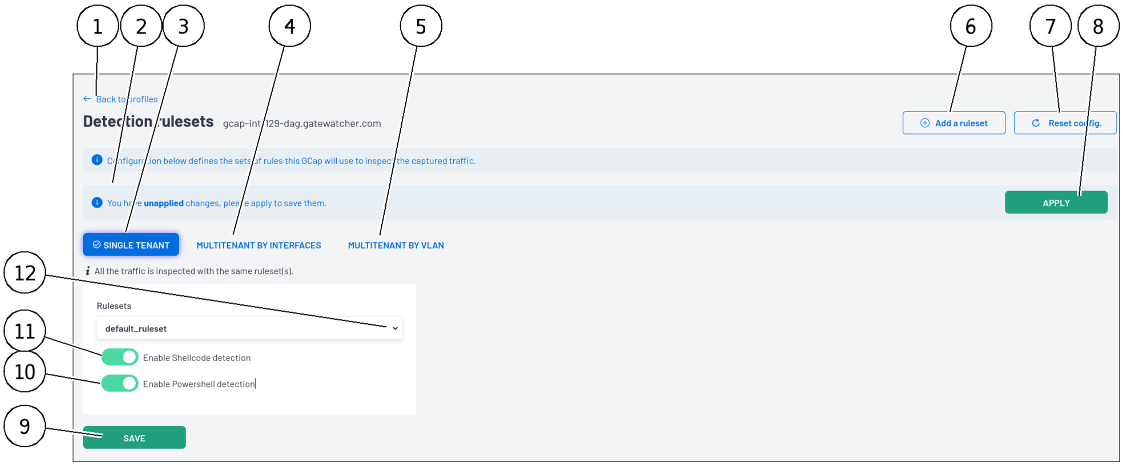
- From the navigation bar, click successively on :
- The `Config` button
- The `Gcaps profiles` button of the `Sigflow` menu.
  The `Gcaps profiles` window is displayed.



Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

GCAP_00

- Click on the `Detection rulesets` button.



Configuration below defines the sets of rules this GCap will use to inspect the captured traffic.

You have **unapplied** changes, please apply to save them.

All the traffic is inspected with the same ruleset(s).

Enable Shellcode detection

Enable Powershell detection

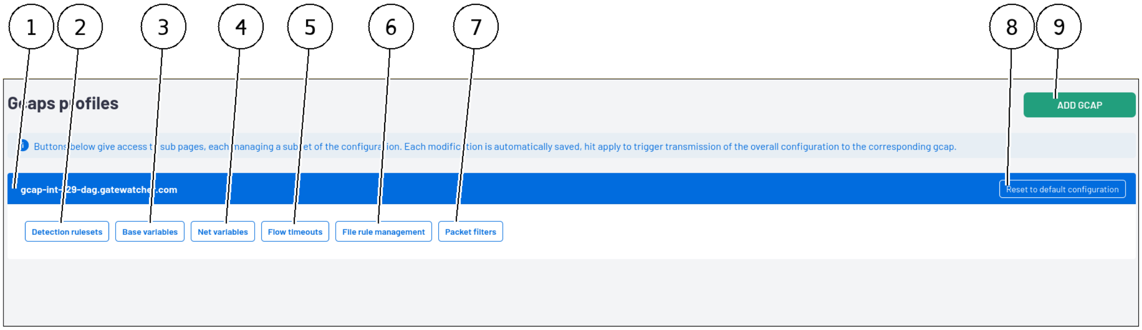
GCAP_01

- Click on the `Single-tenant` tab (3).
- Select a ruleset (12) to apply to all interfaces.
- Enable or disable shellcode detection (11) for all interfaces.
- Enable or disable powershell detection (10) for all interfaces.
- Apply the configuration by clicking the `Save` button (9).

#### 7.4.1.5 Procedure to setup the `Multi-tenant by interface`

- From the navigation bar, click successively on :

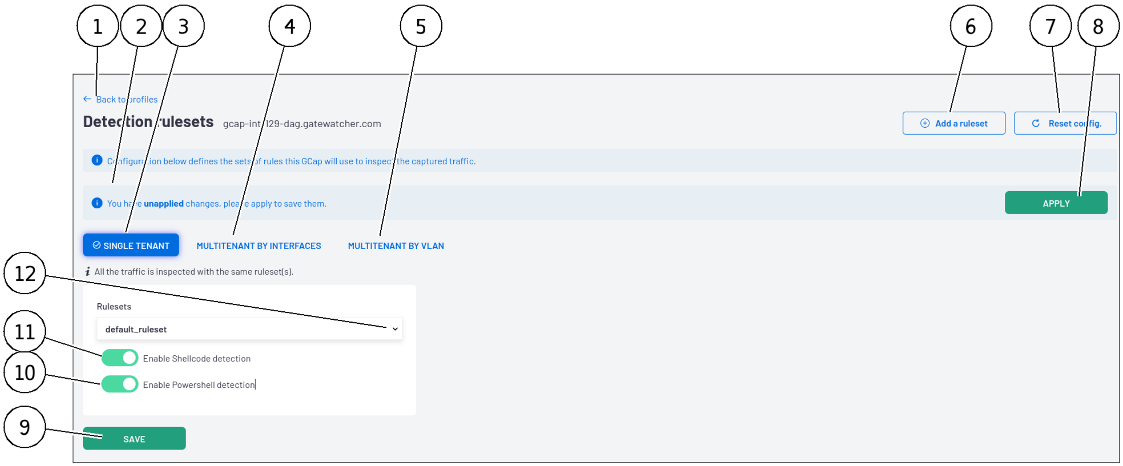
- The `Config` button
- The `Gcaps profiles` button of the `Sigflow` menu.
  The `Gcaps profiles` window is displayed.



Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

GCAP_00

- Click on the `Detection rulesets` button.



Configuration below defines the sets of rules this GCap will use to inspect the captured traffic.

You have **unapplied** changes, please apply to save them.

All the traffic is inspected with the same ruleset(s).

Rulesets: default_ruleset

● Enable Shellcode detection

● Enable Powershell detection

GCAP_01

- Click on the `Multi-tenant by interface` tab (4).
- Select a ruleset to apply for each interface.
- Enable or disable shellcode detection for each interface.
- Enable or disable powershell detection for each interface.
- Apply the configuration by clicking the `Save` button.

Configuration example:

- interface mon0:

- Click on mon0.
- Choose the desired rule set.
- Enabling shellcode and powershell detection.

- interface mon1:

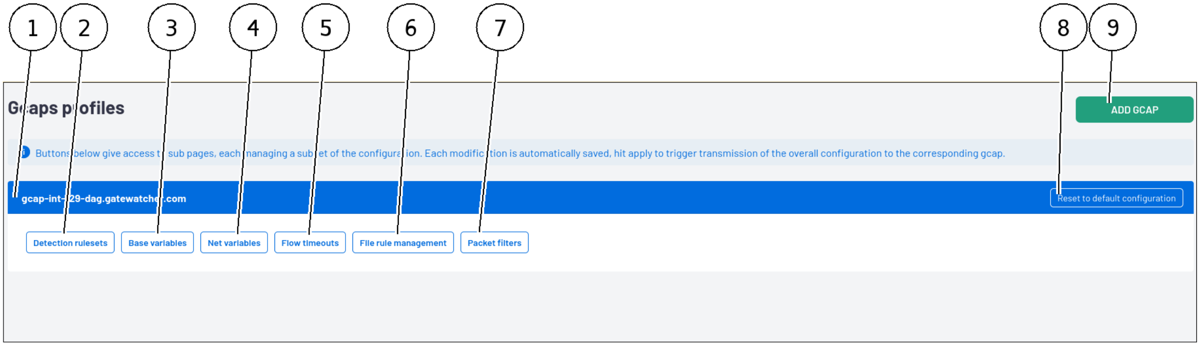
- Click on mon1.
- Choose the desired rule set.
- Disable detection of shellcodes and powershells.

> **Note:**
>
> Detection will differ between traffic received on interfaces mon0 and mon1 because the rulesets themselves are different.

#### 7.4.1.6 Procedure to setup the `Multi-tenant by vlan`

- From the navigation bar, click successively on :
  - the `Config` button
  - the `Gcaps profiles` button of the `Sigflow` menu.

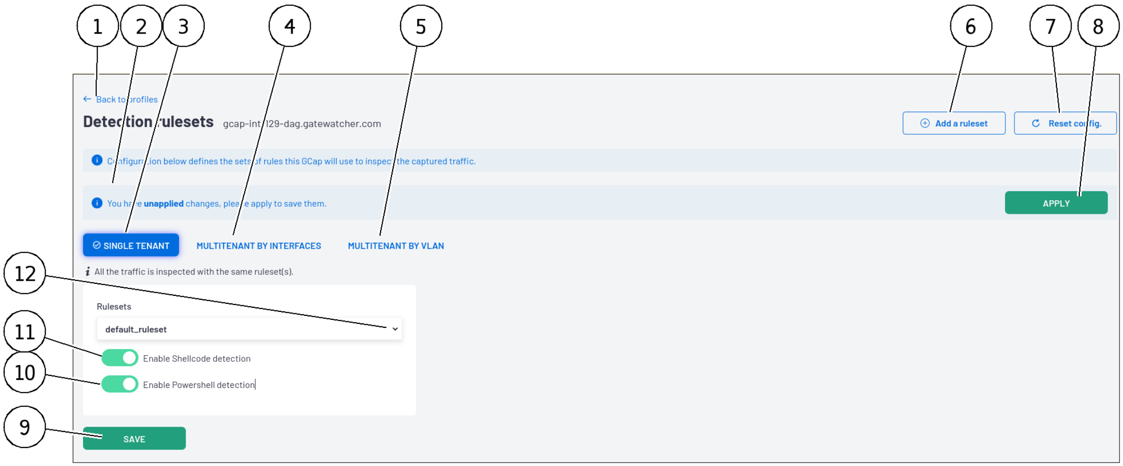
  The `Gcaps profiles` window is displayed.



Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

GCAP_00

- Click on the `Detection rulesets` button.



Configuration below defines the sets of rules this GCap will use to inspect the captured traffic.

You have **unapplied** changes, please apply to save them.

All the traffic is inspected with the same ruleset(s).

Rulesets: default_ruleset

Enable Shellcode detection

Enable Powershell detection

GCAP_01

- Click on the `Multi-tenant by vlan` tab
- Select a ruleset to apply to the `default` vlan
- Enable or disable shellcode detection for the `default` vlan
- Enable or disable powershell detection for the `default` vlan
- Create a vlan by clicking on the `New vlan` button
- in the popup that appears:

- Name the vlan. The vlan name must match the vlan number between 0 and 4096.
- Select a ruleset to apply
- Enable or disable shellcode detection for each vlan
- Enable or disable powershell detection for each vlan
- Click on the `Add` button

- Apply the configuration by clicking the `Save` button.

Configuration example:

- vlan `default`:

- Click on `default`
- Choose the desired rule set
- Enabling shellcode/powershell detection

- Click on the `Add` button
- vlan `110`:
- Click on the `New vlan` button
- Name the vlan `110`
- Choose the desired rule set
- Disable shellcode/powershell detection
- Click on the `Add` button

---

## 7.4.2 Configure GCap Sigflow module specific parameters (Base variables)

### 7.4.2.1 Introduction

The `Base variables` section enables configuring the parameters of the Sigflow module of the GCap.
The different configuration parameters are the following:

- Setting the size of the streams and files reconstructed by the GCap
- Setting of the `X-Forwarded-For` function
- Setting fields in events such as payload, payload printable, packet, HTTP body, and HTTP body printable
- Setting up the `Community ID` field
- Setting up the alerting and logging of the different protocols available on the GCap
- Setting up the advanced functions of the Sigflow module

**Attention:**

Changing some of these parameters will cause the detection engine to restart, making the capture unavailable for the duration of the restart.

See *Web UI `Config - Gcaps profiles` screen.*

| For | go to the |
|---|---|
| Change in file reconstruction size | *Procedure to change the reconstruction size of files* |
| Configuring the fields in the events | *Procedure to configure the fields present in the events* |
| Configuring alerting and protocol logging | *Procedure to configure the alerting and logging protocol* |

---

### 7.4.2.2 Prerequisites

User : member of **Operator** group

---

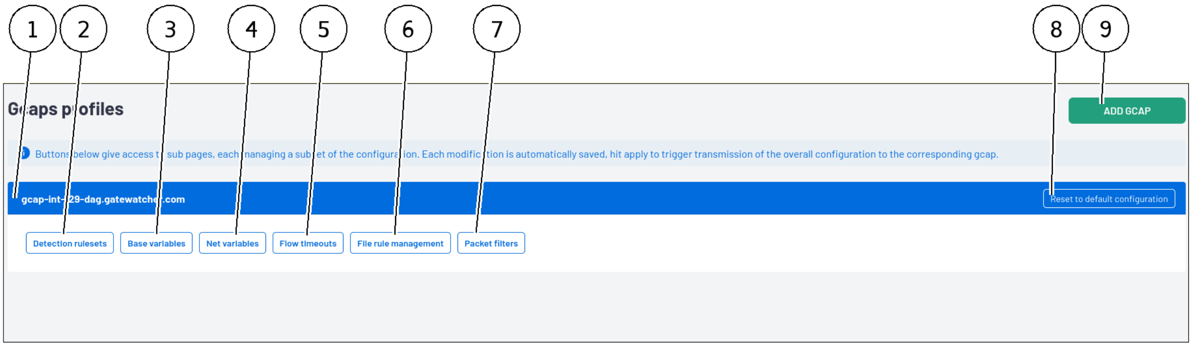
### 7.4.2.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

---

#### 7.4.2.4 Procedure to change the reconstruction size of files

- From the navigation bar, click successively on :
  - The `Config` button
  - The `Gcaps profiles` button of the `Sigflow` menu.
    The `Gcaps profiles` window is displayed.



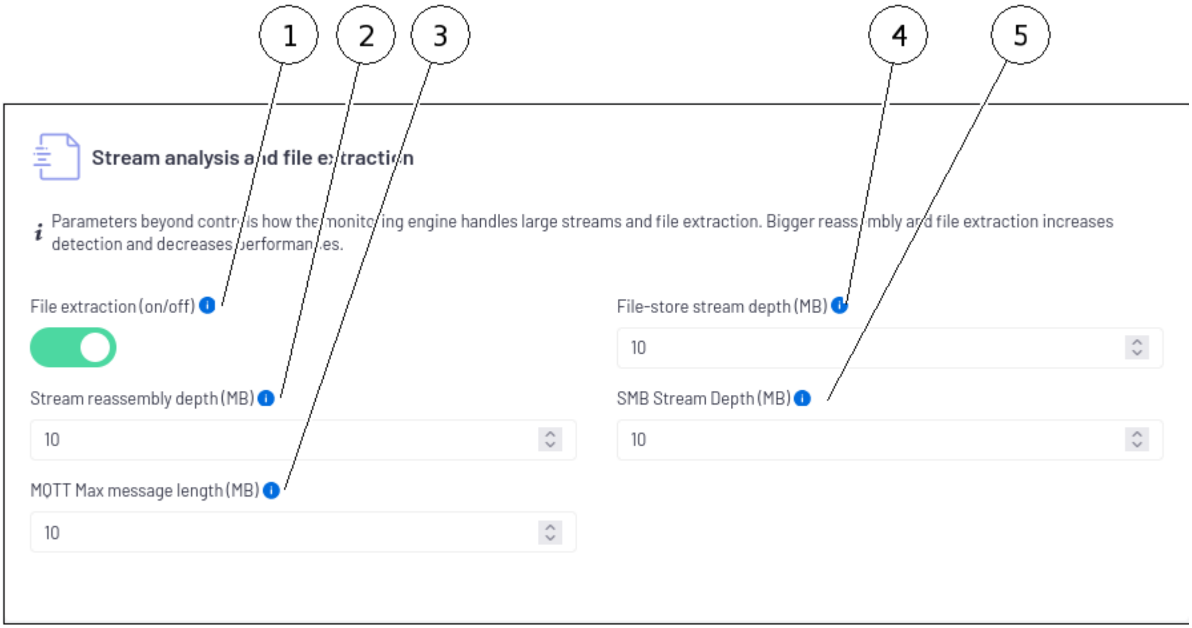
Gcaps profiles

Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

gcap-int-29-dag.gatewatcher.com

GCAP_00

- Click on the `Base variables` button (3).
- From the `Base variables` interface, section `Stream analysis and file extraction`, check the `File extraction (On/Off)` choice is activated (1).



Stream analysis and file extraction

Parameters beyond controls how the monitoring engine handles large streams and file extraction. Bigger reassembly and file extraction increases detection and decreases performances.

File extraction (on/off)

File-store stream depth (MB): 10

Stream reassembly depth (MB): 10

SMB Stream Depth (MB): 10

MQTT Max message length (MB): 10

GCAP_02-1

- Change the value of the `File-store stream depth (MB)` field (4) (default is 10MB) (4)
- Click on the `Apply` button.

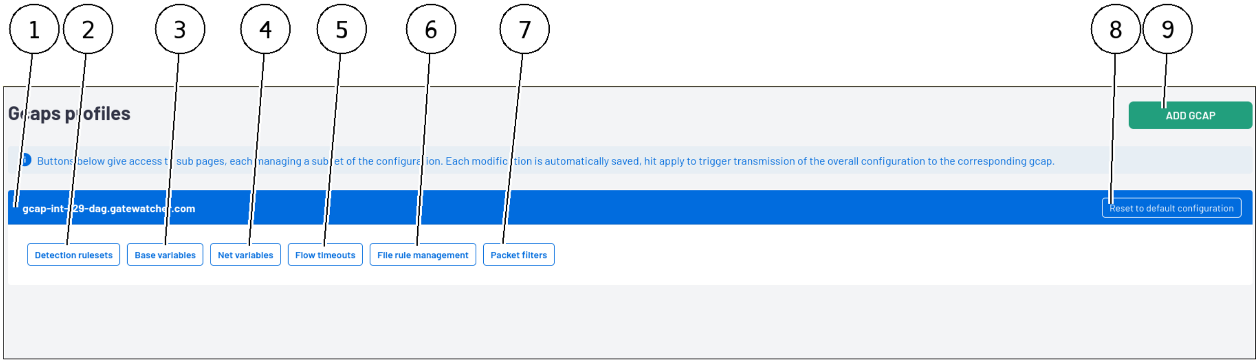
**Note:**

The value choice is important - the higher the value configured, the greater the impact on performance.

#### 7.4.2.5 Procedure to configure the fields present in the events

- From the navigation bar, click successively on :

- The `Config` button
- The `Gcaps profiles` button of the `Sigflow` menu.
  The `Gcaps profiles` window is displayed.



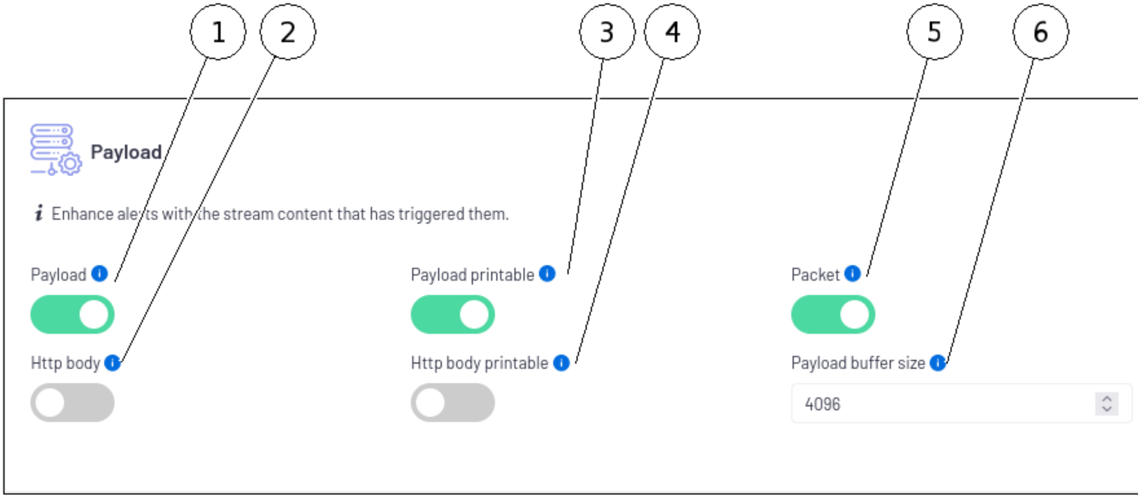
Gcaps profiles

Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

gcap-int-29-dag.gatewatcher.com

GCAP_00

- Click on the `Base variables` button (3).
  From the `Base variables` interface, section `Payload`, activate the fields that will appear in the events.



Payload

Enhance alerts with the stream content that has triggered them.

Payload ☑

Http body ☐

Payload printable ☑

Http body printable ☐

Packet ☑

Payload buffer size 4096

GCAP_02-3

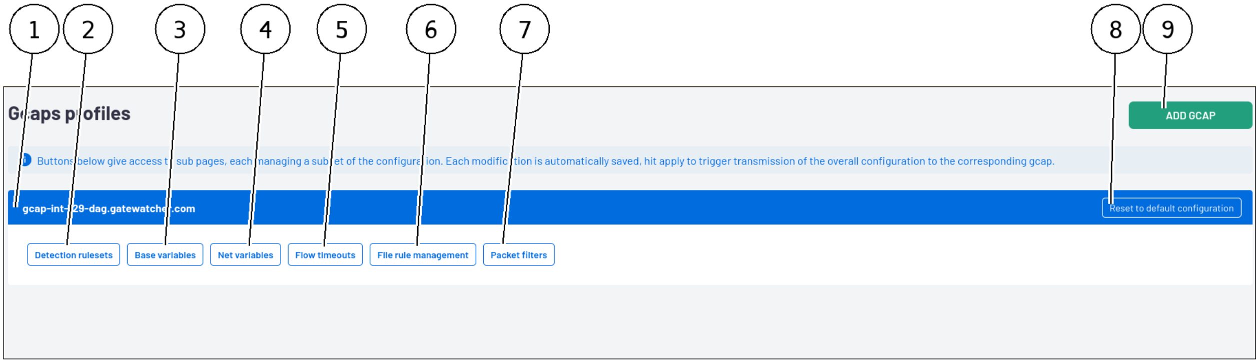
- Disable fields that will not appear in events.
- Click on the `Apply` button.

**Note:**

In some SIEMs, too high an event size can lead to truncation.

#### 7.4.2.6 Procedure to configure the alerting and logging protocol

- From the navigation bar, click successively on :
- The `` `Config` `` button
- The `` `Gcaps profiles` `` button of the `` `Sigflow` `` menu.
  The `` `Gcaps profiles` `` window is displayed.



Gcaps profiles

ADD GCAP

Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

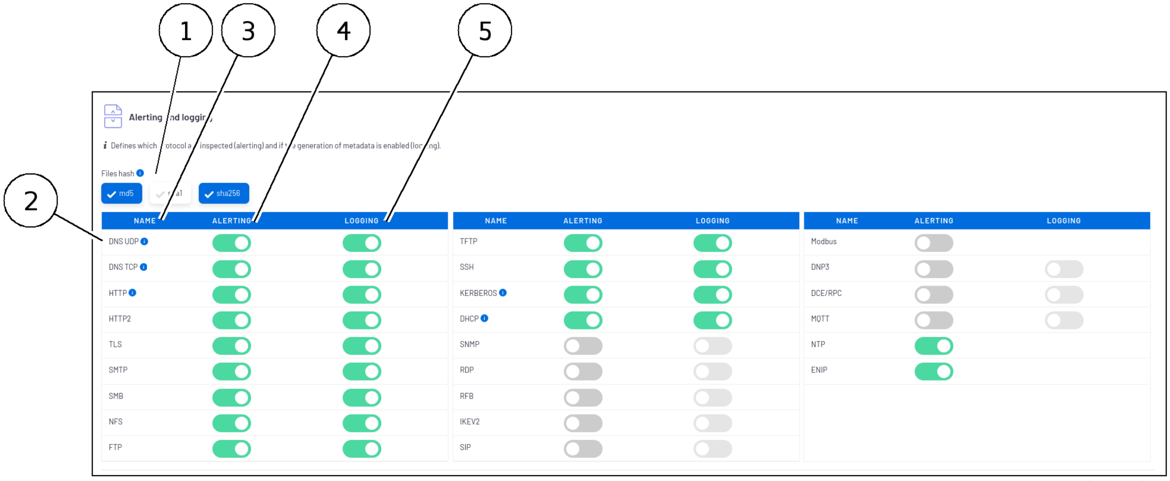
gcap-int-29-dag.gatewatcher.com

Reset to default configuration

Detection rulesets | Base variables | Net variables | Flow timeouts | File rule management | Packet filters

GCAP_00

- Click on the `` `Base variables` `` button (3).
  From the `` `Base variables` `` interface, section `` `Alerting and logging` `` :



Alerting and logging

Defines which protocol are inspected (alerting) and if the generation of metadata is enabled (logging).

Files hash

☑ md5 ☐ sha1 ☑ sha256

| NAME | ALERTING | LOGGING | NAME | ALERTING | LOGGING | NAME | ALERTING | LOGGING |
|---|---|---|---|---|---|---|---|---|
| DNS UDP | ● | ● | TFTP | ● | ● | Modbus | ○ | |
| DNS TCP | ● | ● | SSH | ● | ● | DNP3 | ○ | ○ |
| HTTP | ● | ● | KERBEROS | ● | ● | DCE/RPC | ○ | ○ |
| HTTP2 | ● | ● | DHCP | ● | ● | MQTT | ○ | ○ |
| TLS | ● | ● | SNMP | ○ | ○ | NTP | ● | |
| SMTP | ● | ● | RDP | ○ | ○ | ENIP | ● | |
| SMB | ● | ● | RFB | ○ | ○ | | | |
| NFS | ● | ● | IKEV2 | ○ | ○ | | | |
| FTP | ● | ● | SIP | ○ | ○ | | | |

GCAP_02-5

- Tick the hash types that will appear in events (md5, sha1 and sha256) (1).
- Enable alerting for protocols that will raise alerts (4).
- Disable alerting for protocols that should not raise alerts (4).
- Enable logging for protocols that will need to raise metadata (5).
- Disable logging for protocols that should not raise metadata (5).
- Click on the `` `Apply` `` button.

## 7.4.3 Configure network variables used by rules (Net variables)

### 7.4.3.1 Introduction

The `` `Base variables` `` section enables configuring the network variables used by the GCap detection rules. These variables correspond to the internal networks, external networks, and the various server types in the monitored environment.

See *Web UI `Config - Gcaps profiles` screen.*

| For | go to the |
|---|---|
| Configuring network variables | *Procedure to setup the network variables* |
| Loading a saved configuration | *Procedure to load a configuration* |

#### 7.4.3.2 Prerequisites

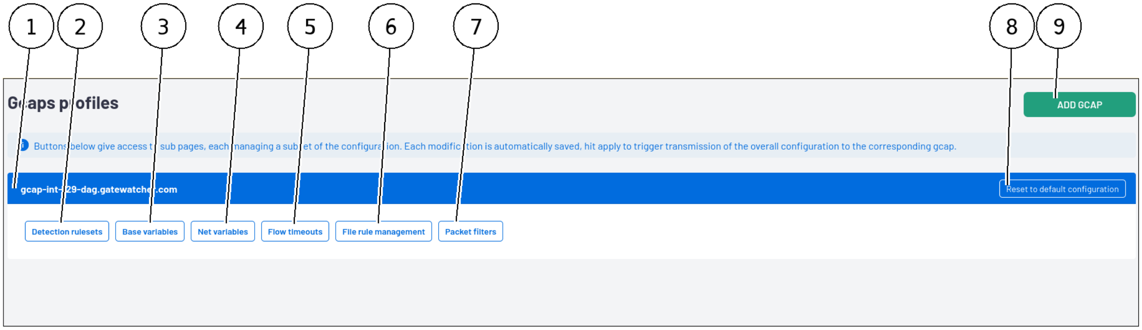
User : member of **Operator** group

#### 7.4.3.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

#### 7.4.3.4 Procedure to setup the network variables

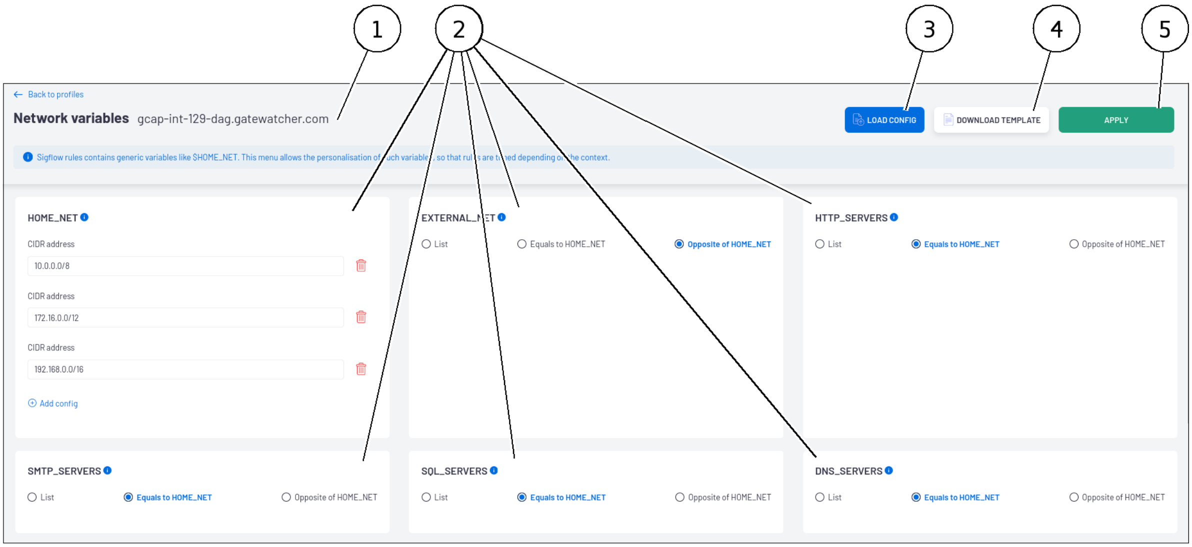
- From the navigation bar, click successively on :
- The `Config` button
- The `Gcaps profiles` button of the `Sigflow` menu.
  The `Gcaps profiles` window is displayed.



Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

GCAP_00

- Click on the `Net variables` button (4).



Sigflow rules contains generic variables like $HOME_NET. This menu allows the personalisation of such variables, so that rules are tuned depending on the context.

HOME_NET
CIDR address: 10.0.0.0/8
CIDR address: 172.16.0.0/12
CIDR address: 192.168.0.0/16

EXTERNAL_NET: ○ List ○ Equals to HOME_NET ● Opposite of HOME_NET

HTTP_SERVERS: ○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

SMTP_SERVERS: ○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

SQL_SERVERS: ○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

DNS_SERVERS: ○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

GCAP_03

- Locate the `HOME_NET` section (2)

- Keep the default networks if they correspond to the internal networks or modify them if necessary
- If there are more than three internal networks to be completed, click on `Add config` to insert a new field and then fill it in. Repeat the operation to add the number of desired networks.

- Locate the `EXTERNAL_NET` section (2)

  - Make sure that `Opposite of HOME_NET` is ticked. It would take too long to fill in all the external networks.
  - For the other variable types:

  - keep the `Equals of HOME_NET` value as default
  - otherwise select `List` and click `Add config` to insert a new field and fill it in. Repeat the process to add the number of networks desired.

- Click on the `Apply` button (5).

---

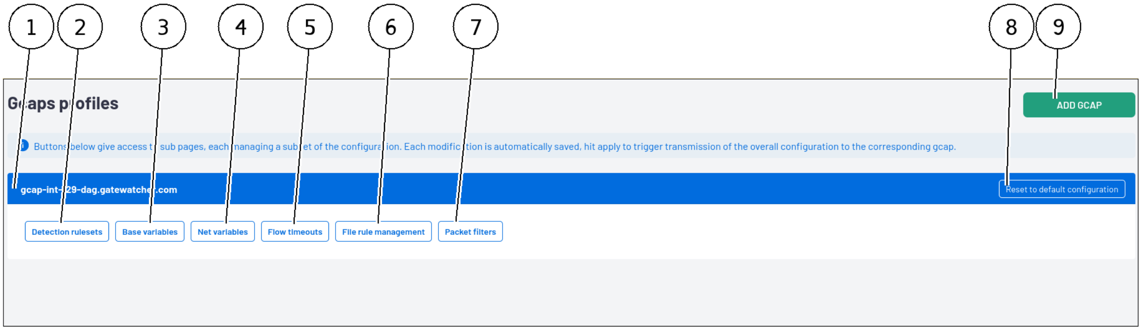
#### 7.4.3.5 Procedure to load a configuration

**Note:**

This procedure can be used to load a configuration file onto a GCap.

- From the navigation bar, click successively on :

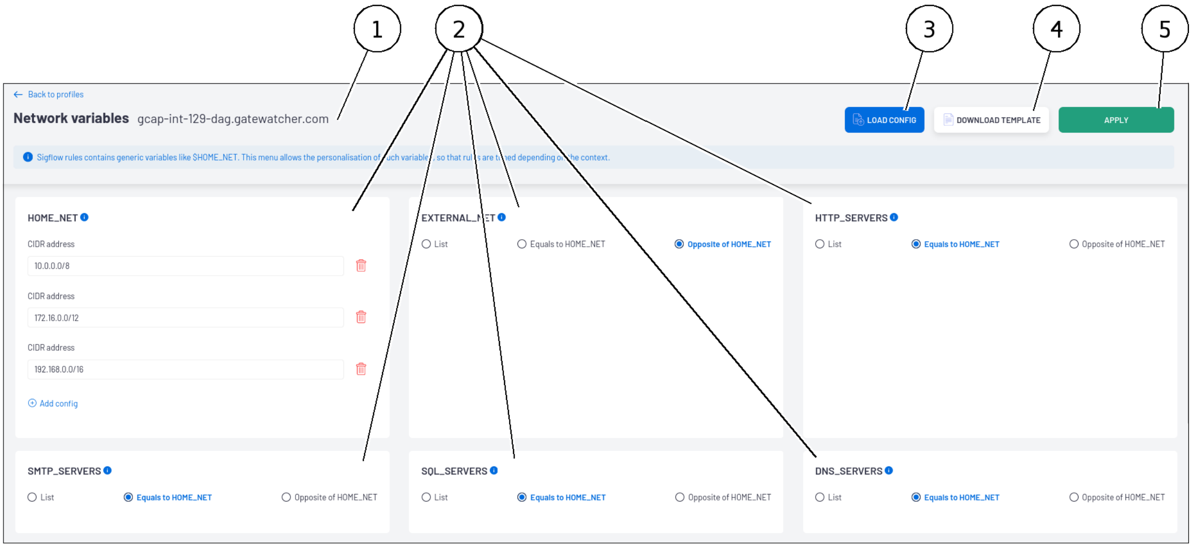
- The `Config` button
- The `Gcaps profiles` button of the `Sigflow` menu.
  The `Gcaps profiles` window is displayed.



Buttons below give access t sub pages, each managing a subset of the configura ion. Each modific tion is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

GCAP_00

- Click on the `Net variables` button (4).



**Network variables** gcap-int-129-dag.gatewatcher.com

Sigflow rules contains generic variables like $HOME_NET. This menu allows the personalisation of such variables, so that rules are tuned depending on the context.

HOME_NET
CIDR address: 10.0.0.0/8
CIDR address: 172.16.0.0/12
CIDR address: 192.168.0.0/16
Add config

EXTERNAL_NET: ○ List ○ Equals to HOME_NET ● Opposite of HOME_NET

HTTP_SERVERS: ○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

SMTP_SERVERS: ○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

SQL_SERVERS: ○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

DNS_SERVERS: ○ List ● Equals to HOME_NET ○ Opposite of HOME_NET

GCAP_03

- Procedure :

- Click on the `DOWNLOAD TEMPLATE` (4) button and save the template file.
- Fill the template file with the information regarding the desired network variables.
- Click on the `LOAD CONFIG` button and select the template file.
  Once loaded, the configuration of the template file is loaded in the interface.
- Click on the `Apply` button.

**Or**

- Procedure :

- Retrieve a previously saved template file.
- Click on the `LOAD CONFIG` button and select the configuration file.
- Click on the `Apply` button.

## 7.4.4 Configure File Reconstruction Rules (File rules management)

### 7.4.4.1 Introduction

The `File rule management` section enables configuring the file reconstruction rules used by the GCap detection engine.
Reconstruction is based on several parameters: the protocol, the file type, and the file type value.

See section: *Web UI `Config - Gcaps profiles` screen*.

| For | go to the |
|---|---|
| Setting up the file reconstruction | *Procedure to set up the file reconstruction* |
| Loading a saved configuration | *Procedure to load a saved configuration* |
| Adding a reconstruction rule | *Procedure to add a rebuilding rule* |

### 7.4.4.2 Prerequisites

User : member of **Operator** group

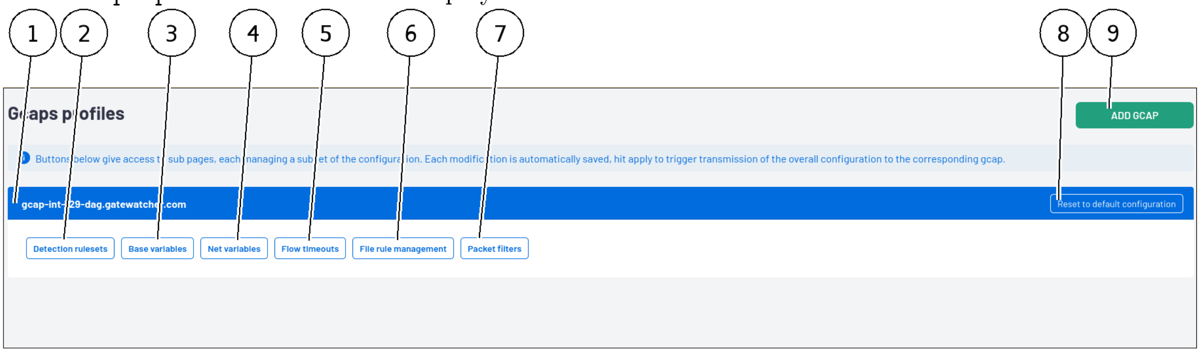
### 7.4.4.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

### 7.4.4.4 Procedure to set up the file reconstruction

- From the navigation bar, click successively on :
  - the `Config` button
  - the `Gcaps profiles` button of the `Sigflow` menu.

  The `Gcaps profiles` window is displayed.



Gcaps profiles

ADD GCAP

Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

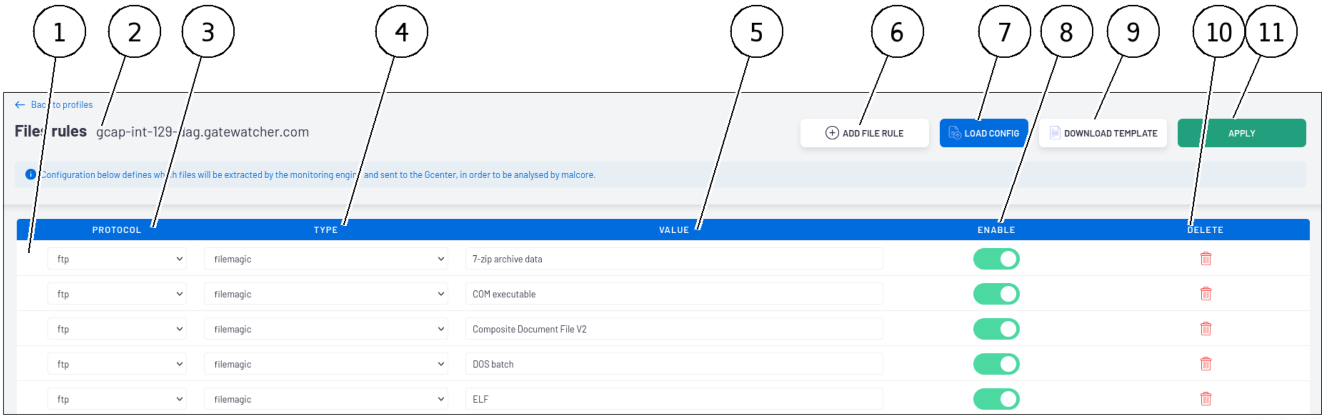
gcap-int-129-dag.gatewatcher.com

Reset to default configuration

Detection rulesets | Base variables | Net variables | Flow timeouts | File rule management | Packet filters

GCAP_00

- Click on the `File rule management` button (6).



← Back to profiles

**Files rules** gcap-int-129-dag.gatewatcher.com

ADD FILE RULE | LOAD CONFIG | DOWNLOAD TEMPLATE | APPLY

Configuration below defines which files will be extracted by the monitoring engine and sent to the Gcenter, in order to be analysed by malcore.

| PROTOCOL | TYPE | VALUE | ENABLE | DELETE |
|---|---|---|---|---|
| ftp | filemagic | 7-zip archive data | ● | 🗑 |
| ftp | filemagic | COM executable | ● | 🗑 |
| ftp | filemagic | Composite Document File V2 | ● | 🗑 |
| ftp | filemagic | DOS batch | ● | 🗑 |
| ftp | filemagic | ELF | ● | 🗑 |

GCAP_05

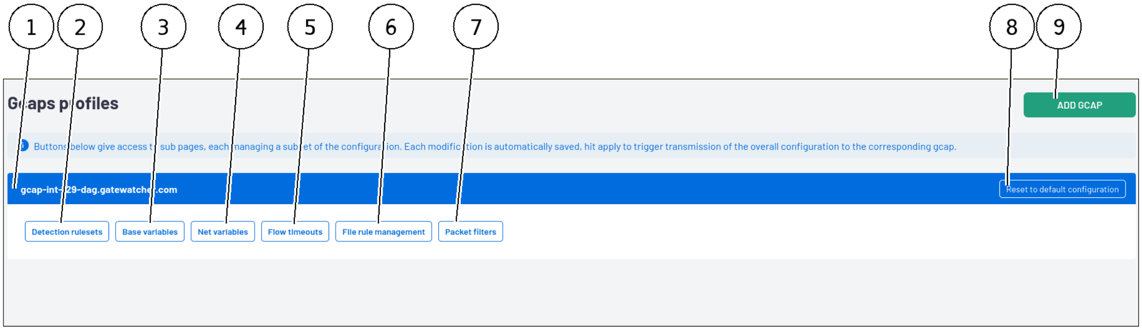
- For each rule, validate that the `protocol` (3), `type` (4), `value` (5) fields match the desired values.
- Enable or disable the desired rules using the enable button in the `Enable` (8) field.
- Completely remove the unnecessary rules.
- If necessary, insert rules using the `ADD FILE RULE` button (see *Procedure to add a rebuilding rule*).
- Click on the `Apply` button (11).

### 7.4.4.5 Procedure to load a saved configuration

> **Note:**
>
> This procedure can be used to load the configuration from one GCap to another or to save the configuration.

- From the navigation bar, click successively on :

- The `` `Config` `` button
- The `` `Gcaps profiles` `` button of the `` `Sigflow` `` menu.
  The `` `Gcaps profiles` `` window is displayed.



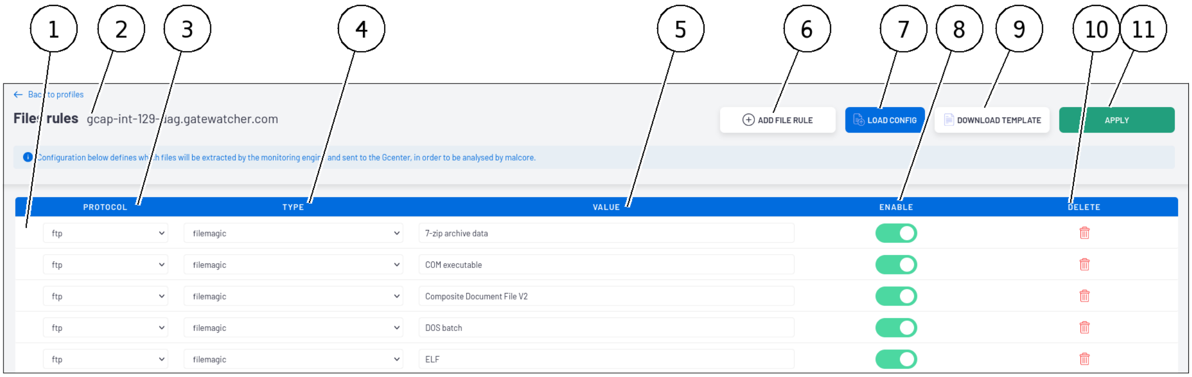
Gcaps profiles

Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

gcap-int-129-dag.gatewatcher.com

GCAP_00

- Click on the `` `File rule management` `` button (6).



Files rules gcap-int-129-dag.gatewatcher.com

Configuration below defines which files will be extracted by the monitoring engine and sent to the Gcenter, in order to be analysed by malcore.

| PROTOCOL | TYPE | VALUE | ENABLE | DELETE |
|---|---|---|---|---|
| ftp | filemagic | 7-zip archive data | ● | 🗑 |
| ftp | filemagic | COM executable | ● | 🗑 |
| ftp | filemagic | Composite Document File V2 | ● | 🗑 |
| ftp | filemagic | DOS batch | ● | 🗑 |
| ftp | filemagic | ELF | ● | 🗑 |

GCAP_05

- On the first GCap:

- Perform the previous procedure to configure the file rebuilding rules
- Click on the `` `DOWNLOAD TEMPLATE` `` (9) button and save the configuration file

- On the second GCap:

- Click on the `` `LOAD CONFIG` `` (7) button and select the configuration file
- Once loaded, the configuration of the first GCap is loaded on the second
- Click on the `` `Apply` `` button (11).

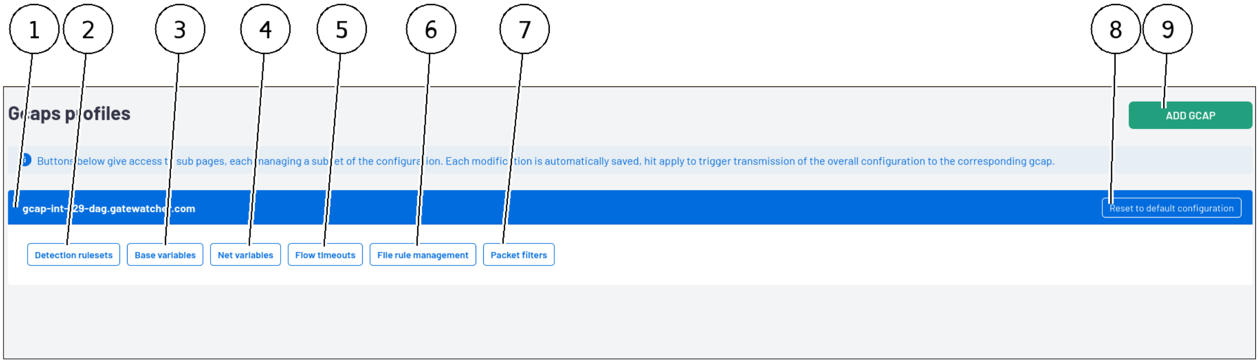
**Or**

- Retrieve a previously saved template.
- Click on the `` `LOAD CONFIG` `` (7) button and select the configuration file.
- Click on the `` `Apply` `` button (11).

#### 7.4.4.6 Procedure to add a rebuilding rule

- From the navigation bar, click successively on :

- The `Config` button
- The `Gcaps profiles` button of the `Sigflow` menu.
  The `Gcaps profiles` window is displayed.



Gcaps profiles

ADD GCAP

Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

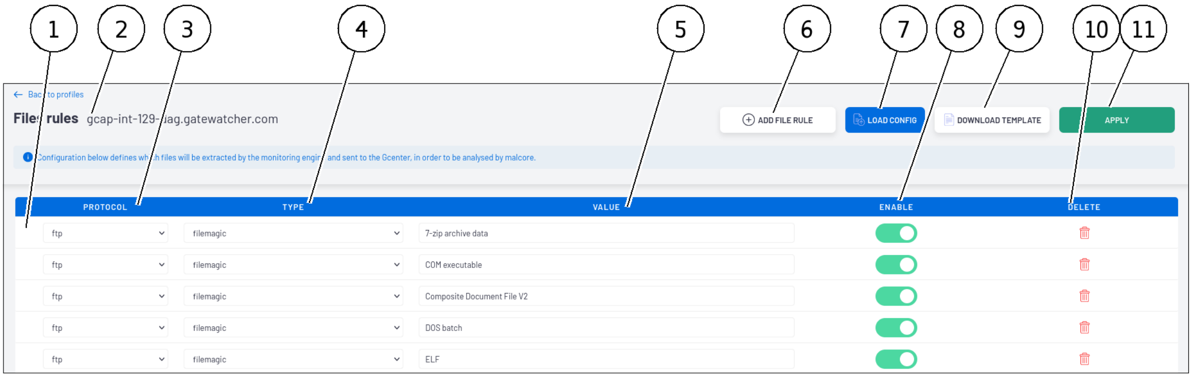
gcap-int-129-dag.gatewatcher.com

Reset to default configuration

Detection rulesets | Base variables | Net variables | Flow timeouts | File rule management | Packet filters

GCAP_00

- Click on the `File rule management` button (6).



← Back to profiles

Files rules gcap-int-129-dag.gatewatcher.com

ADD FILE RULE | LOAD CONFIG | DOWNLOAD TEMPLATE | APPLY

Configuration below defines which files will be extracted by the monitoring engine and sent to the Gcenter, in order to be analysed by malcore.

| PROTOCOL | TYPE | VALUE | ENABLE | DELETE |
|---|---|---|---|---|
| ftp | filemagic | 7-zip archive data | ● | 🗑 |
| ftp | filemagic | COM executable | ● | 🗑 |
| ftp | filemagic | Composite Document File V2 | ● | 🗑 |
| ftp | filemagic | DOS batch | ● | 🗑 |
| ftp | filemagic | ELF | ● | 🗑 |

GCAP_05

- Click on the `ADD FILE RULE` button (6).
- In the popup that appears:

- Enable or disable the rule
- Specify the protocol on which the rule will be applied
- Choose the type of reconstruction - by extension or by filemagic
- Enter the value corresponding to the type chosen above
- Click on the `Add` button

- Click on the `Apply` button.

## 7.4.5 Configure filters on targeted parts of the analyzed traffic (Packet filters)

### 7.4.5.1 Introduction

The `Packet filters` section enables filters to be set on targeted parts of the traffic being analyzed so they are not processed.
The graphical integration is described in the *`Packet filters` section of the `Config Gcaps profiles` menu*.

| For | go to the |
|---|---|
| Add a filter | *Procedure to set up the filter* |
| Change of native vlan | *Procedure to configure the VLAN* |

### 7.4.5.2 Prerequisites

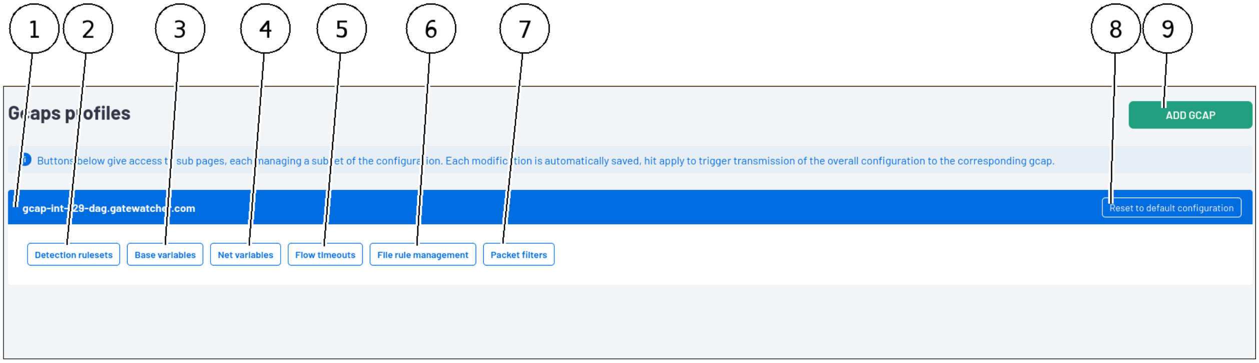
User : member of **Operator** group

### 7.4.5.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

### 7.4.5.4 Procedure to set up the filter

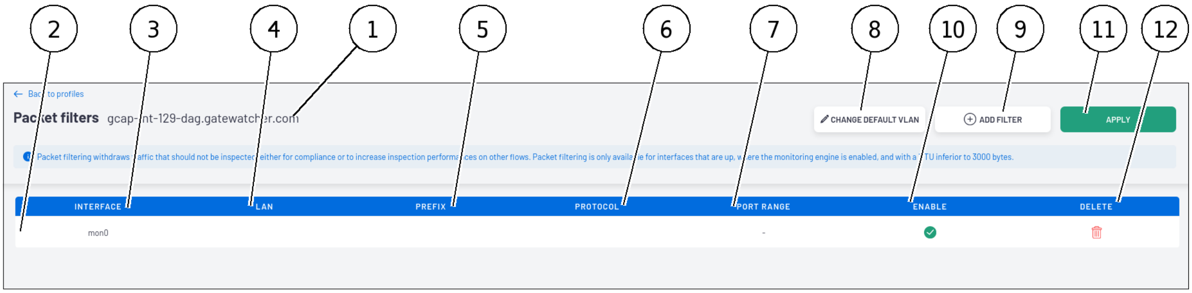
- From the navigation bar, click successively on :
- The `Config` button
- The `Gcaps profiles` button of the `Sigflow` menu.
  The `Gcaps profiles` window is displayed.



Buttons below give access t sub pages, each managing a sub et of the configura ion. Each modific tion is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

GCAP_00

- Click on the `Packet filters` button (7).



Packet filtering withdraws affic that should not be inspecte either for compliance or to increase inspection performa ces on other flows. Packet filtering is only availa e for interfaces that are up, w ere the monitoring engine is enabled, and with a TU inferior to 3000 bytes.

| INTERFACE | LAN | PREFIX | PROTOCOL | PORT RANGE | ENABLE | DELETE |
|---|---|---|---|---|---|---|
| mon0 | | | | - | ✓ | 🗑 |

GCAP_06

- Click on the `ADD FILTER` button (9).
  In the popup that appears:
- Choose the desired interface - it must be enabled
- In the `Filter Type` field, choose between `Specific VLAN` and `Default VLAN & untagged traffic`

- In the `VLAN` field, enter the value of the desired vlan. If the "Filter Type" field is set to `default VLAN & untagged traffic` the box is not editable.
- In the `Drop whole LAN` field, choose whether the filter applies to the whole vlan (enable) or a part of the vlan (disable)
- In the `Prefix` field, enter the network to apply the filter to. If the `Drop whole LAN` field is enabled, this box is not editable.
- In the `Protocol` field, enter the protocol to apply the filter to. If the `Drop whole LAN` field is enabled, this box is not editable.
- In the `Port range` field, choose the port or port range to apply the filter to. If the `Drop whole LAN` field is enabled, this box is not editable.
- Click on the `Save` button.

- Click on the `Apply` button.

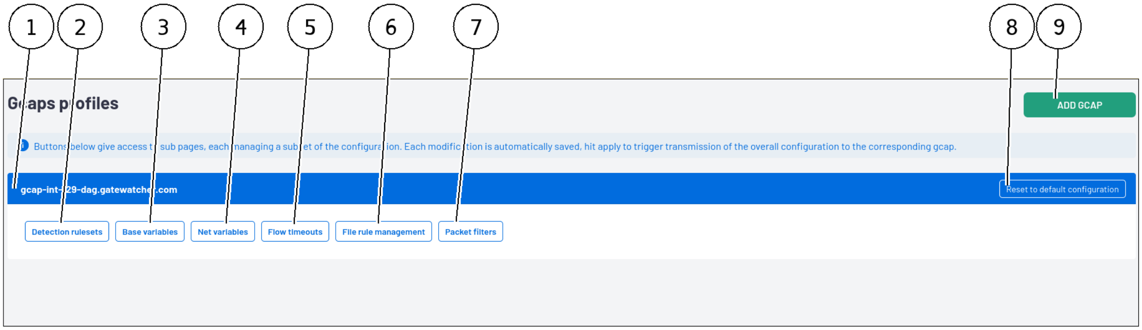
> **Note:**
>
> When `Drop whole (V)LAN` is enabled:
> - If the `Filter Type` field is set to `Specific VLAN`, all traffic associated with this VLAN will drop
> - If the `Filter Type` field is set to `default VLAN & untagged traffic`, all VLAN traffic associated with default and all traffic that is not part of any VLAN will be dropped

---

### 7.4.5.5 Procedure to configure the VLAN

- From the navigation bar, click successively on :

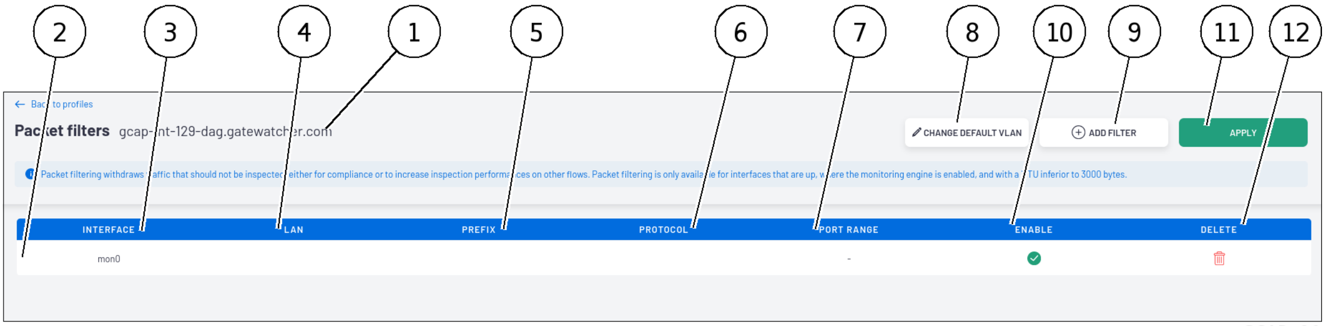
- The `Config` button
- The `Gcaps profiles` button of the `Sigflow` menu.
  The `Gcaps profiles` window is displayed.



Buttons below give access to sub pages, each managing a subset of the configuration. Each modification is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

GCAP_00

- Click on the `Packet filters` button (7).



Packet filtering withdraws traffic that should not be inspected either for compliance or to increase inspection performances on other flows. Packet filtering is only available for interfaces that are up, where the monitoring engine is enabled, and with a MTU inferior to 3000 bytes.

| INTERFACE | LAN | PREFIX | PROTOCOL | PORT RANGE | ENABLE | DELETE |
|---|---|---|---|---|---|---|
| mon0 | | | | - | ✓ | 🗑 |

GCAP_06

- Click on the `CHANGE DEFAULT VLAN` button (8).
  In the popup that appears:

- Choose the desired interface - it must be enabled
- Enter the desired value in the `Default VLAN` field
- Click on the `Save` button

- Click on the `Apply` button.

## 7.5 Use of NDR dashboards

### 7.5.1 Introduction

When an attack on an information system is confirmed, analyst teams must be able to quickly understand the origin of the attack, its target, and its overall impact.
The NDR dashboards of the GCenter will facilitate these inquiries by making available a wealth of essential information.
They will enable:

- Analysing the alerts for each type of engine
- Viewing information and alerts specific to the network's equipment
- Viewing information and alerts specific to the network's users
- Viewing the relationships between the different equipment and users

See *Overview of the WEB UI*

| For | go to the |
|---|---|
| Retrieving information related to an alert | *Procedure to retrieve information related to an alert* |
| Processing equipment | *Procedure to process the equipment* |
| Processing a user | *Procedure to process the users* |
| Managing association rules | *Procedure to manage association rules* |
| Relation between equipment and users | *Procedure to analyse the relationship between equipment and users* |

### 7.5.2 Prerequisites

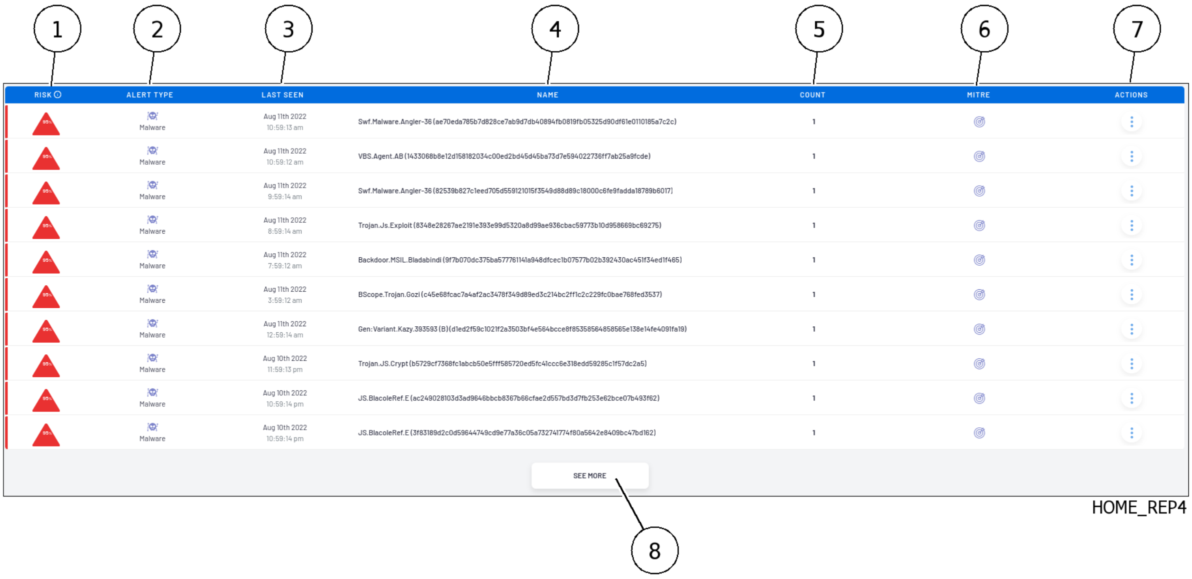
- User : member of **Operator** group

### 7.5.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

### 7.5.4 Procedure to retrieve information related to an alert

- From the navigation bar, click on the `Home` button.
  In the Message Area of the `Home` screen, alerts are displayed classified by risk level.

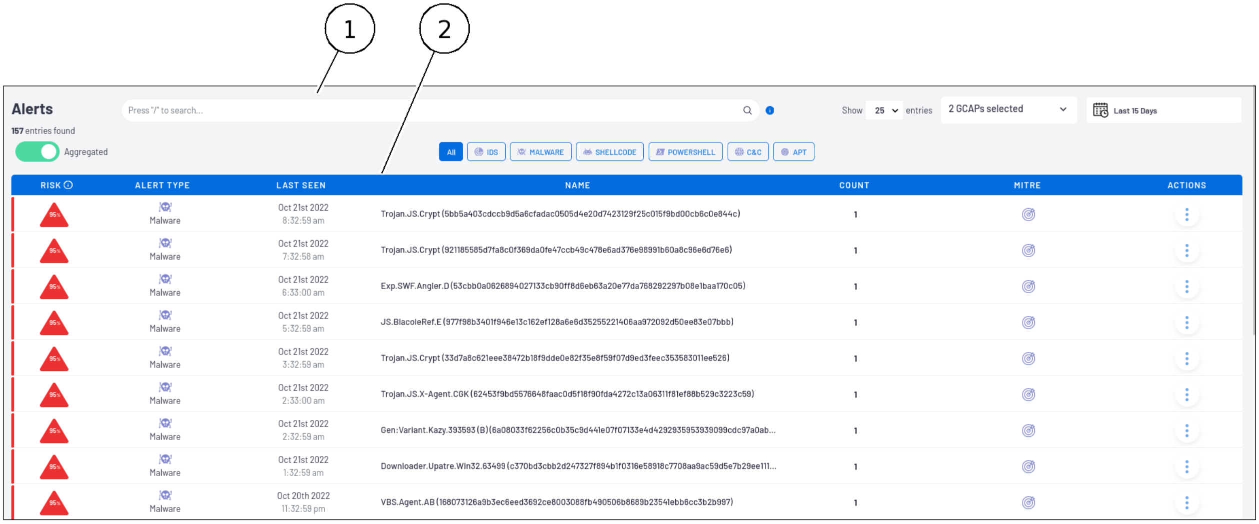


| RISK ⓘ | ALERT TYPE | LAST SEEN | NAME | COUNT | MITRE | ACTIONS |
|---|---|---|---|---|---|---|
| 95% | Malware | Aug 11th 2022<br>10:59:13 am | Swf.Malware.Angler-36 (ae70eda785b7d828ce7ab9d7db40894fb0819fb05325d90df61e0110185a7c2c) | 1 | | ⋮ |
| 95% | Malware | Aug 11th 2022<br>10:59:12 am | VBS.Agent.AB (1433068b8e12d158182034c00ed2bd45d45ba73d7e594022736ff7ab25a9fcde) | 1 | | ⋮ |
| 95% | Malware | Aug 11th 2022<br>9:59:14 am | Swf.Malware.Angler-36 (82539b827c1eed705d559121015f3549d88d89c18000c6fe9fadda18789b6017) | 1 | | ⋮ |
| 95% | Malware | Aug 11th 2022<br>8:59:14 am | Trojan.Js.Exploit (8348e28267ae2191e393e99d5320a8d99ae936cbac59773b10d958669bc69275) | 1 | | ⋮ |
| 95% | Malware | Aug 11th 2022<br>7:59:12 am | Backdoor.MSIL.Bladabindi (9f7b070dc375ba577761141a948dfcec1b07577b02b392430ac451f34ed1f465) | 1 | | ⋮ |
| 95% | Malware | Aug 11th 2022<br>3:59:12 am | BScope.Trojan.Gozi (c45e68fcac7a4af2ac3478f349d89ed3c214bc2ff1c2c229fc0bae768fed3537) | 1 | | ⋮ |
| 95% | Malware | Aug 11th 2022<br>12:59:14 am | Gen:Variant.Kazy.393593 (B) (d1ed2f59c1021f2a3503bf4e564bcce8f85358564858565e138e14fe4091fa19) | 1 | | ⋮ |
| 95% | Malware | Aug 10th 2022<br>11:59:13 pm | Trojan.JS.Crypt (b5729cf7368fc1abcb50e5fff585720ed5fc41ccc6e318edd59285c1f57dc2a5) | 1 | | ⋮ |
| 95% | Malware | Aug 10th 2022<br>10:59:14 pm | JS.BlacoleRef.E (ac249028103d3ad9646bbcb8367b66cfae2d557bd3d7fb253e62bce07b493f62) | 1 | | ⋮ |
| 95% | Malware | Aug 10th 2022<br>10:59:14 pm | JS.BlacoleRef.E (3f83189d2c0d59644749cd9e77a36c05a732741774f80a5642e8409bc47bd162) | 1 | | ⋮ |

SEE MORE

HOME_REP4

- Click on an alert requiring investigation.
  The `Alerts` screen of the web UI is displayed.



Alerts

Press "/" to search...

157 entries found

Aggregated

Show 25 entries

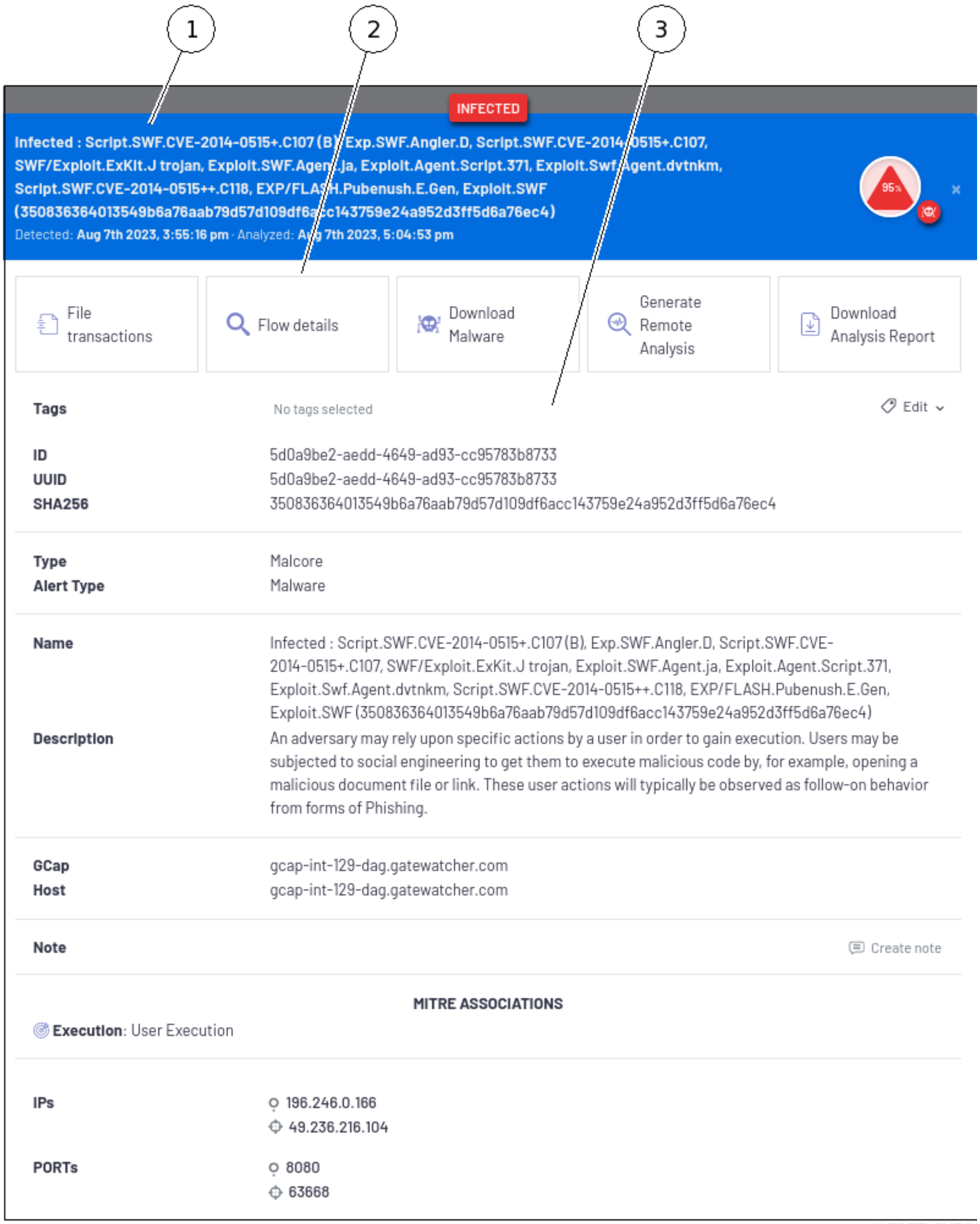
2 GCAPs selected

Last 15 Days

| RISK ⓘ | ALERT TYPE | LAST SEEN | NAME | COUNT | MITRE | ACTIONS |
|---|---|---|---|---|---|---|
| 95% | Malware | Oct 21st 2022<br>8:32:59 am | Trojan.JS.Crypt (5bb5a403cdccb9d5a6cfadac0505d4e20d7423129f25c015f9bd00cb6c0e844c) | 1 | | ⋮ |
| 95% | Malware | Oct 21st 2022<br>7:32:58 am | Trojan.JS.Crypt (921185585d7fa8c0f369da0fe47ccb49c478e6ad376e98991b60a8c96e6d76e6) | 1 | | ⋮ |
| 95% | Malware | Oct 21st 2022<br>6:33:00 am | Exp.SWF.Angler.D (53cbb0a0626894027133cb90ff8d6eb63a20e77da768292297b08e1baa170c05) | 1 | | ⋮ |
| 95% | Malware | Oct 21st 2022<br>5:32:59 am | JS.BlacoleRef.E (977f98b3401f946e13c162ef128a6e6d35255221406aa972092d50ee83e07bbb) | 1 | | ⋮ |
| 95% | Malware | Oct 21st 2022<br>3:32:59 am | Trojan.JS.Crypt (33d7a8c621eee38472b18f9dde0e82f35e8f59f07d9ed3feec353583011ee526) | 1 | | ⋮ |
| 95% | Malware | Oct 21st 2022<br>2:33:00 am | Trojan.JS.X-Agent.CGK (62453f9bd5576648faac0d5f18f90fda4272c13a06311f81ef88b529c3223c59) | 1 | | ⋮ |
| 95% | Malware | Oct 21st 2022<br>2:32:59 am | Gen:Variant.Kazy.393593 (B) (6a08033f62256c0b35c9d441e07f07133e4d4292935953939099cdc97a0ab... | 1 | | ⋮ |
| 95% | Malware | Oct 21st 2022<br>1:32:59 am | Downloader.Upatre.Win32.63499 (c370bd3cbb2d247327f894b1f0316e58918c7708aa9ac59d5e7b29ee111... | 1 | | ⋮ |
| 95% | Malware | Oct 20th 2022<br>11:32:59 pm | VBS.Agent.AB (168073126a9b3ec6eed3692ce8003088fb490506b8689b23541ebb6cc3b2b997) | 1 | | ⋮ |

ALERTS-00

- If the `Aggregated` button is ticked, click again on the alert again in the page that appears.
- Once the alerts are not aggregated, click on the alert requiring investigation.
  A popup appears with the alert details.



Infected : Script.SWF.CVE-2014-0515+.C107 (B), Exp.SWF.Angler.D, Script.SWF.CVE-2014-0515+.C107, SWF/Exploit.ExKit.J trojan, Exploit.SWF.Agent.ja, Exploit.Agent.Script.371, Exploit.Swf.Agent.dvtnkm, Script.SWF.CVE-2014-0515++.C118, EXP/FLASH.Pubenush.E.Gen, Exploit.SWF (350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4)

Detected: Aug 7th 2023, 3:55:16 pm · Analyzed: Aug 7th 2023, 5:04:53 pm

**Tags** No tags selected

**ID** 5d0a9be2-aedd-4649-ad93-cc95783b8733
**UUID** 5d0a9be2-aedd-4649-ad93-cc95783b8733
**SHA256** 350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4

**Type** Malcore
**Alert Type** Malware

**Name** Infected : Script.SWF.CVE-2014-0515+.C107 (B), Exp.SWF.Angler.D, Script.SWF.CVE-2014-0515+.C107, SWF/Exploit.ExKit.J trojan, Exploit.SWF.Agent.ja, Exploit.Agent.Script.371, Exploit.Swf.Agent.dvtnkm, Script.SWF.CVE-2014-0515++.C118, EXP/FLASH.Pubenush.E.Gen, Exploit.SWF (350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4)

**Description** An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of Phishing.

**GCap** gcap-int-129-dag.gatewatcher.com
**Host** gcap-int-129-dag.gatewatcher.com

**Note**

**MITRE ASSOCIATIONS**

**Execution**: User Execution

**IPs** 196.246.0.166
49.236.216.104

**PORTs** 8080
63668

ALERTE-INFO

This window displays important information:

- The details of the alert
- The name of the equipment concerned or impacted by this alert
- The IP addresses concerned or impacted by this alert

**Note:**

This window is detailed in paragraph *Alert information window*.

- Click on the name of one of the devices in question in the popup to display the device's file.

  The following are displayed:
  - Its risk score
  - IP address
  - Its mac address
  - The metadata generated
  - Alerts generated
- From the equipment IP, search on it in the `Users` page (example: IP:192.168.0.1).
- Click on the user to display the user record.

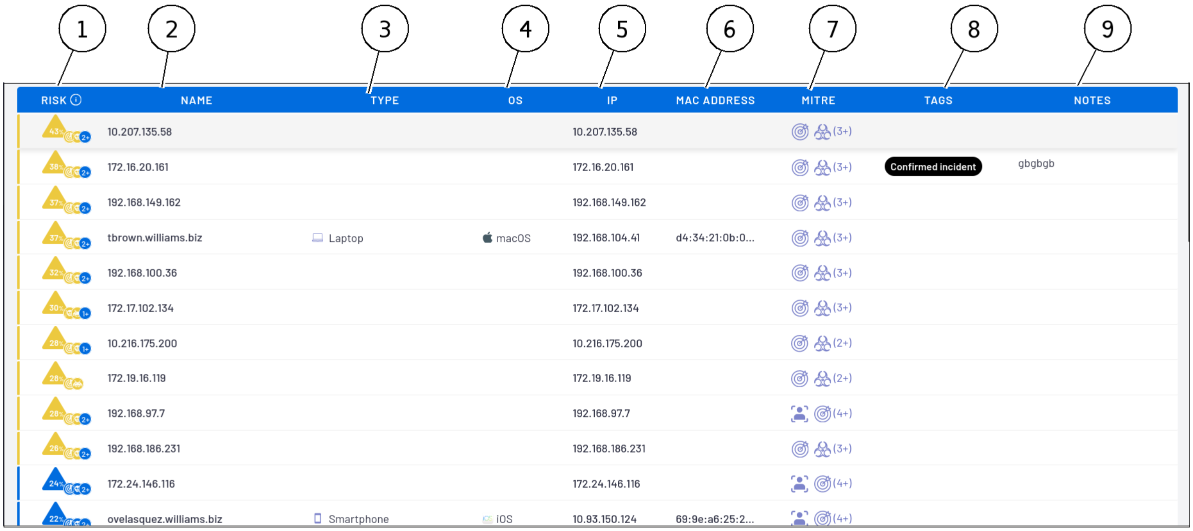
The following are displayed:

- Its risk score
- IP address
- Its equipment on the network
- The metadata generated
- Alerts generated
- Its relationship with other equipment or network users

- Continue investigations, as above, if other equipment is present in the alert being processed.

### 7.5.5 Procedure to process the equipment

- From the navigation bar, click on the `Assets` button.



| RISK ⓘ | NAME | TYPE | OS | IP | MAC ADDRESS | MITRE | TAGS | NOTES |
|---|---|---|---|---|---|---|---|---|
| 43% 2+ | 10.207.135.58 | | | 10.207.135.58 | | (3+) | | |
| 38% 2+ | 172.16.20.161 | | | 172.16.20.161 | | (3+) | Confirmed incident | gbgbgb |
| 37% 2+ | 192.168.149.162 | | | 192.168.149.162 | | (3+) | | |
| 37% 2+ | tbrown.williams.biz | Laptop | macOS | 192.168.104.41 | d4:34:21:0b:0... | (3+) | | |
| 32% 2+ | 192.168.100.36 | | | 192.168.100.36 | | (3+) | | |
| 30% 1+ | 172.17.102.134 | | | 172.17.102.134 | | (3+) | | |
| 28% 1+ | 10.216.175.200 | | | 10.216.175.200 | | (2+) | | |
| 28% | 172.19.16.119 | | | 172.19.16.119 | | (2+) | | |
| 28% 2+ | 192.168.97.7 | | | 192.168.97.7 | | (4+) | | |
| 26% 2+ | 192.168.186.231 | | | 192.168.186.231 | | (3+) | | |
| 24% 2+ | 172.24.146.116 | | | 172.24.146.116 | | (4+) | | |
| 22% | ovelasquez.williams.biz | Smartphone | iOS | 10.93.150.124 | 69:9e:a6:25:2... | (4+) | | |

ASSETS-03

The active equipment management interface provides a list of the different equipment on the network listed by risk score.

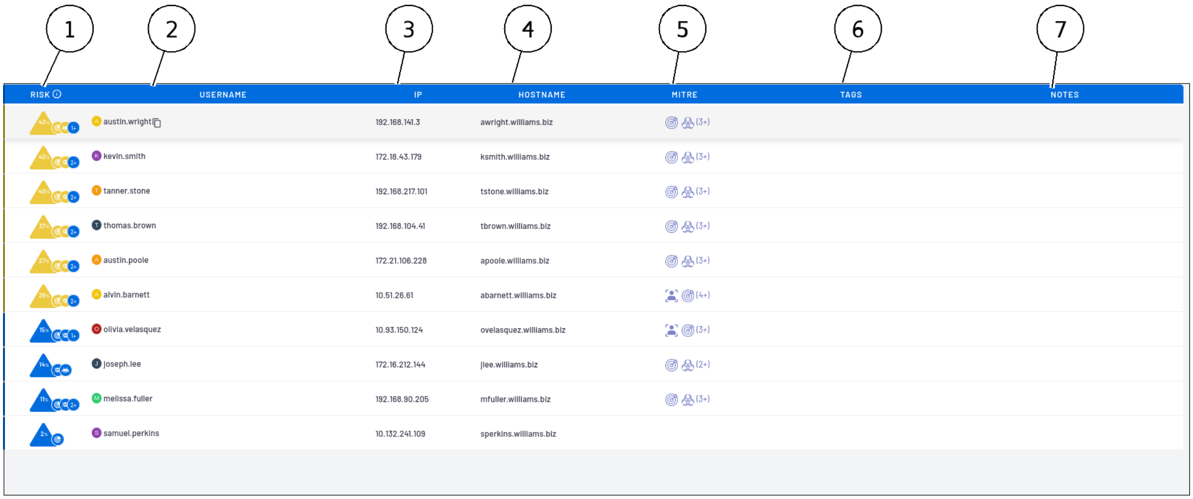
The equipment with the highest risk score are those that have raised the most high criticality alerts. It may therefore be necessary to carry out an in-depth analysis of the equipment in question.

It may therefore be necessary to perform a thorough analysis on the equipment in question.

- Click on the desired equipment.
- Analyse the various alerts (1) noted for this equipment.
- If necessary, add a tag (8) that will give status to the equipment.
- If necessary, add a note (9) to indicate the different analyses performed.

### 7.5.6 Procedure to process the users

- From the navigation bar, click on the `Users` button.



| RISK | USERNAME | IP | HOSTNAME | MITRE | TAGS | NOTES |
|---|---|---|---|---|---|---|
| 43% 1+ | A austin.wright | 192.168.141.3 | awright.williams.biz | (3+) | | |
| 42% 2+ | K kevin.smith | 172.18.43.179 | ksmith.williams.biz | (3+) | | |
| 40% 2+ | T tanner.stone | 192.168.217.101 | tstone.williams.biz | (3+) | | |
| 37% 2+ | T thomas.brown | 192.168.104.41 | tbrown.williams.biz | (3+) | | |
| 27% 2+ | A austin.poole | 172.21.106.228 | apoole.williams.biz | (3+) | | |
| 26% 2+ | A alvin.barnett | 10.51.26.61 | abarnett.williams.biz | (4+) | | |
| 15% 1+ | O olivia.velasquez | 10.93.150.124 | ovelasquez.williams.biz | (3+) | | |
| 14% | J joseph.lee | 172.16.212.144 | jlee.williams.biz | (2+) | | |
| 11% 2+ | M melissa.fuller | 192.168.90.205 | mfuller.williams.biz | (3+) | | |
| 2% | S samuel.perkins | 10.132.241.109 | sperkins.williams.biz | | | |

USERS-02

The active user management interface provides a list of the different users on the network listed by risk score.

The user with the highest risk score are those that have raised the most high criticality alerts.

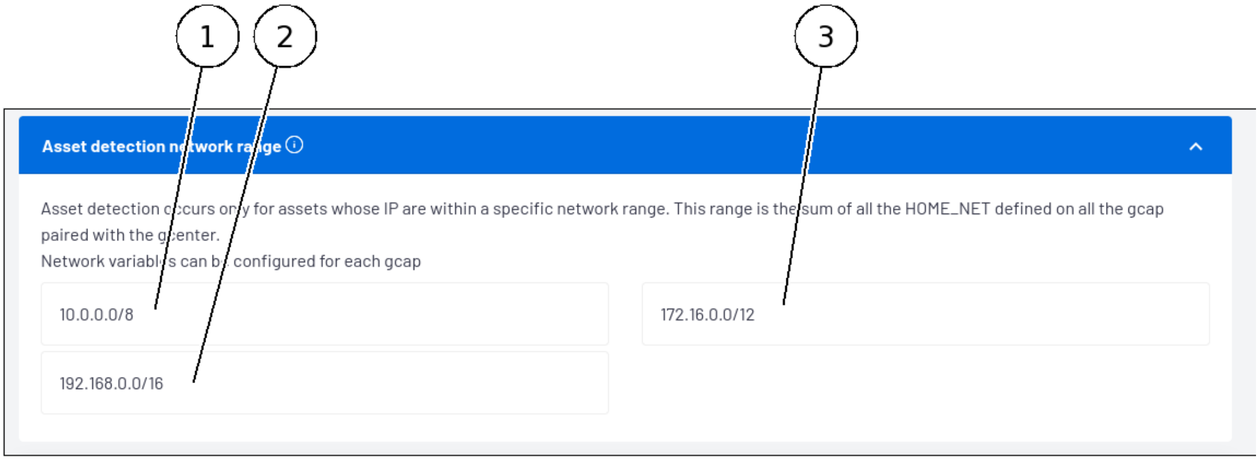
It may therefore be necessary to carry out an in-depth analysis of the user in question.

- Click on the desired user.
- Analyse the various alerts noted for this user.
- If necessary, add a tag to give the user a status.
- If necessary, add a note to indicate the different analyses performed.

### 7.5.7 Procedure to manage association rules

- From the navigation bar, click successively on :
- The `Config` button
- The button `Assets/Users Association rules`

  The interface for managing association rules `Assets/Users association rule` allows to set up rules concerning equipment and users present on the network.
- In the Asset detection network range section:



Asset detection network range ⓘ

Asset detection occurs only for assets whose IP are within a specific network range. This range is the sum of all the HOME_NET defined on all the gcap paired with the gcenter.
Network variables can be configured for each gcap

10.0.0.0/8

172.16.0.0/12

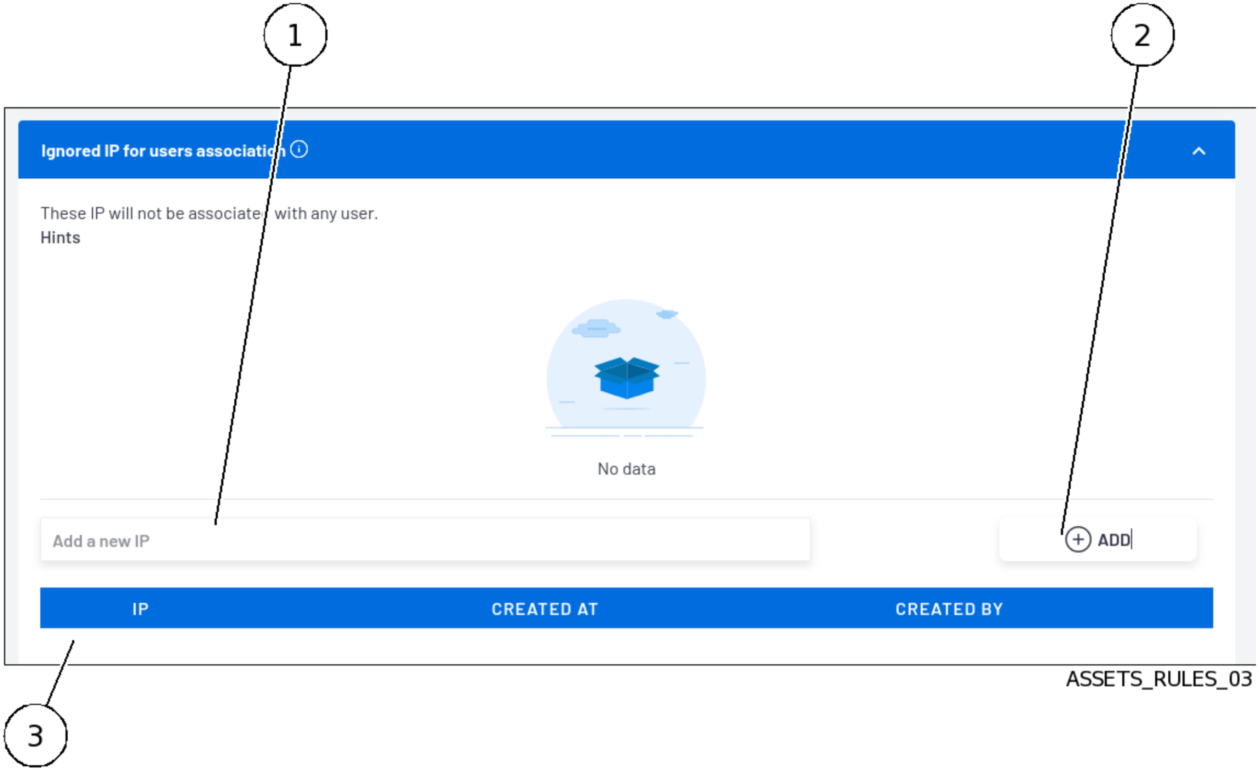
192.168.0.0/16

ASSETS_RULES_01

- Click on the `Network variables can be configured for each gcap` link to add internal networks via the GCap profile customization feature.

  For more information, see *`Asset detection network range` section of the `Assets/Users Association rules` sub menu*.

- In the `Ignored IP for users association` section:



Ignored IP for users association ⓘ

These IP will not be associated with any user.
Hints

Add a new IP

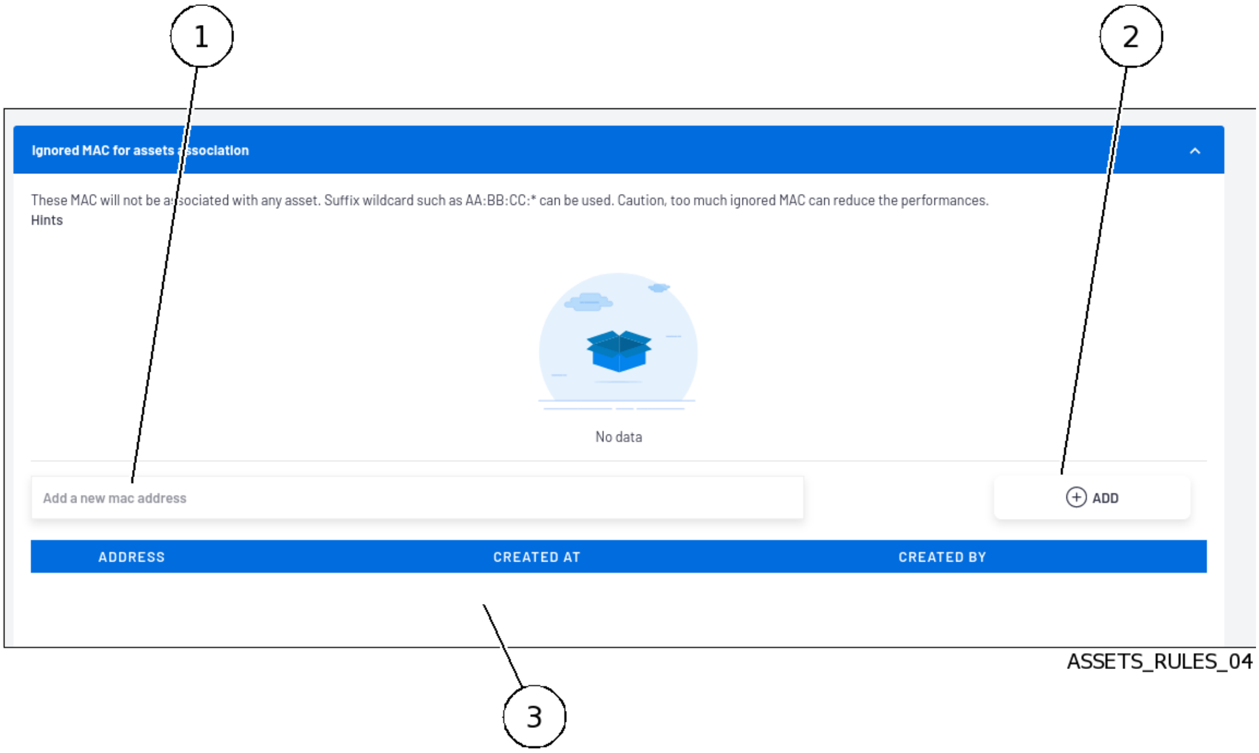
| IP | CREATED AT | CREATED BY |
|---|---|---|

ASSETS_RULES_03

- Declare IP addresses that cannot be associated with a user to avoid wrong associations.

  For more information, see *`Ignored IP for users association` section of the sub menu `Assets/Users Association rules`*.

- In the `Ignored MAC for assets association` section:



Ignored MAC for assets association

These MAC will not be associated with any asset. Suffix wildcard such as AA:BB:CC:* can be used. Caution, too much ignored MAC can reduce the performances.
Hints

No data

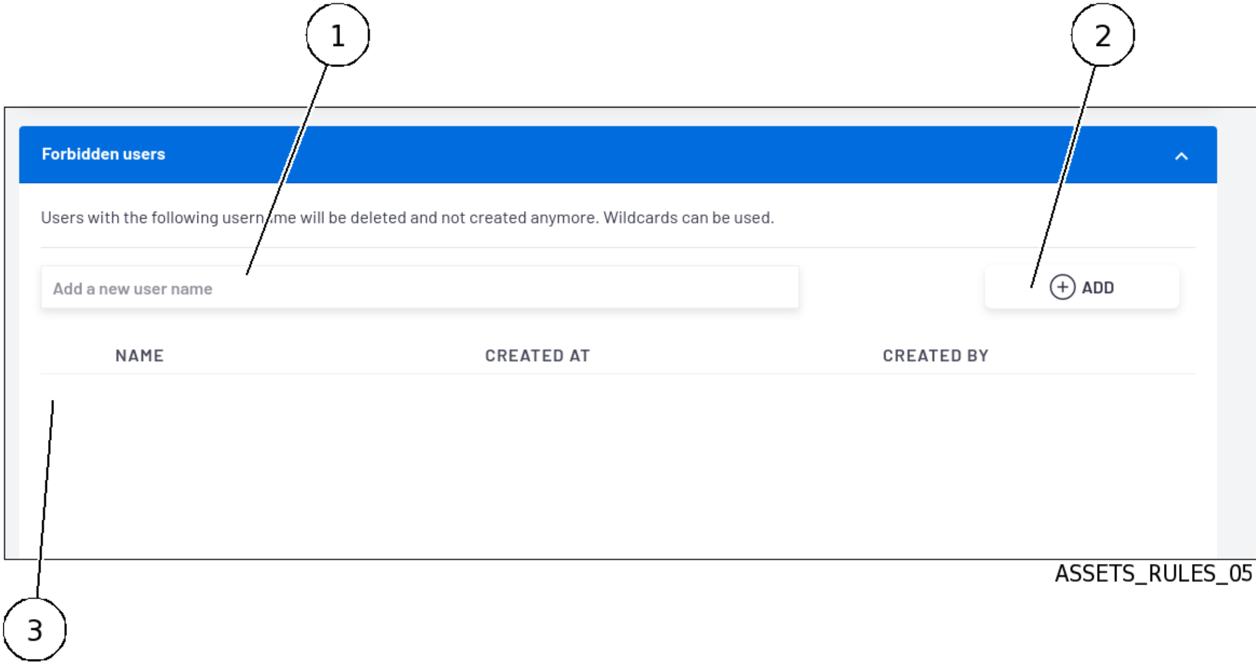
| ADDRESS | CREATED AT | CREATED BY |
|---|---|---|

ASSETS_RULES_04

- Declare MAC addresses that cannot be associated with equipment to avoid wrong associations

  For more information, see *`Ignored MAC for assets association` section of the sub menu `Assets/Users Association rules`*.

- In the `Forbidden users` section:



Forbidden users

Users with the following username will be deleted and not created anymore. Wildcards can be used.

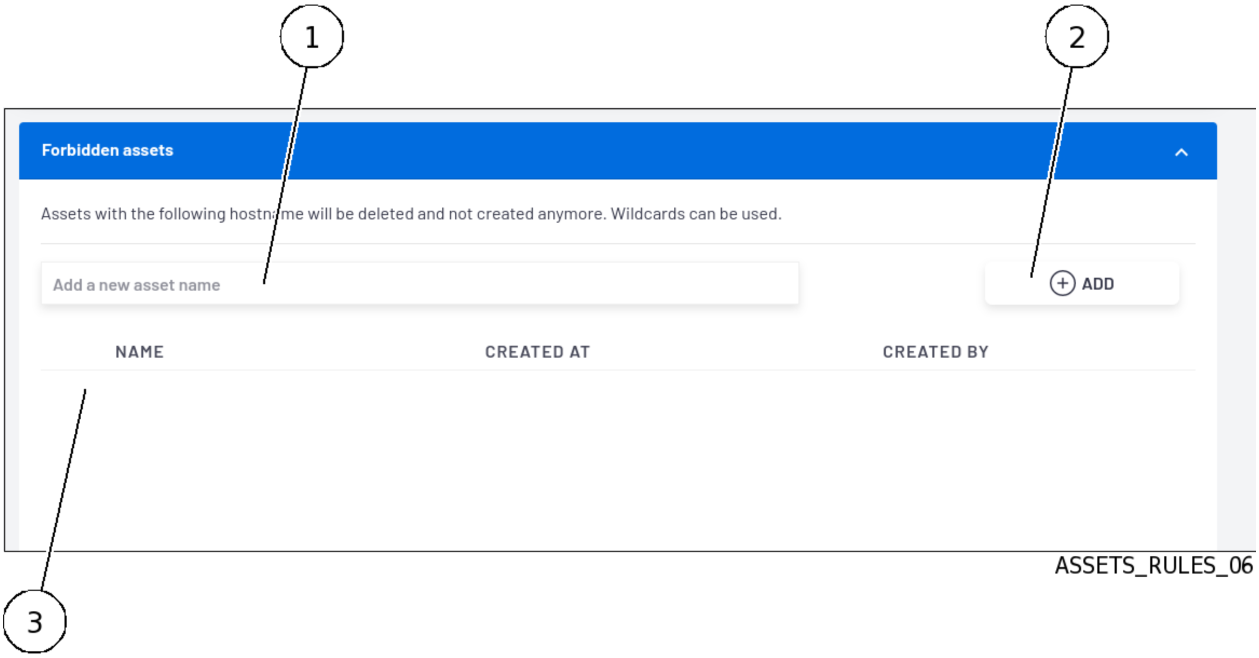
| NAME | CREATED AT | CREATED BY |
|---|---|---|

ASSETS_RULES_05

- Declare users not to appear in NDR dashboards (example: CEO, administrator)

  For more information, see *`Forbidden users` section of the sub menu `Assets/Users Association rules`*.

- In the `Forbidden assets` section:



**Forbidden assets**

Assets with the following hostname will be deleted and not created anymore. Wildcards can be used.

Add a new asset name

ADD

| NAME | CREATED AT | CREATED BY |
|---|---|---|

ASSETS_RULES_06

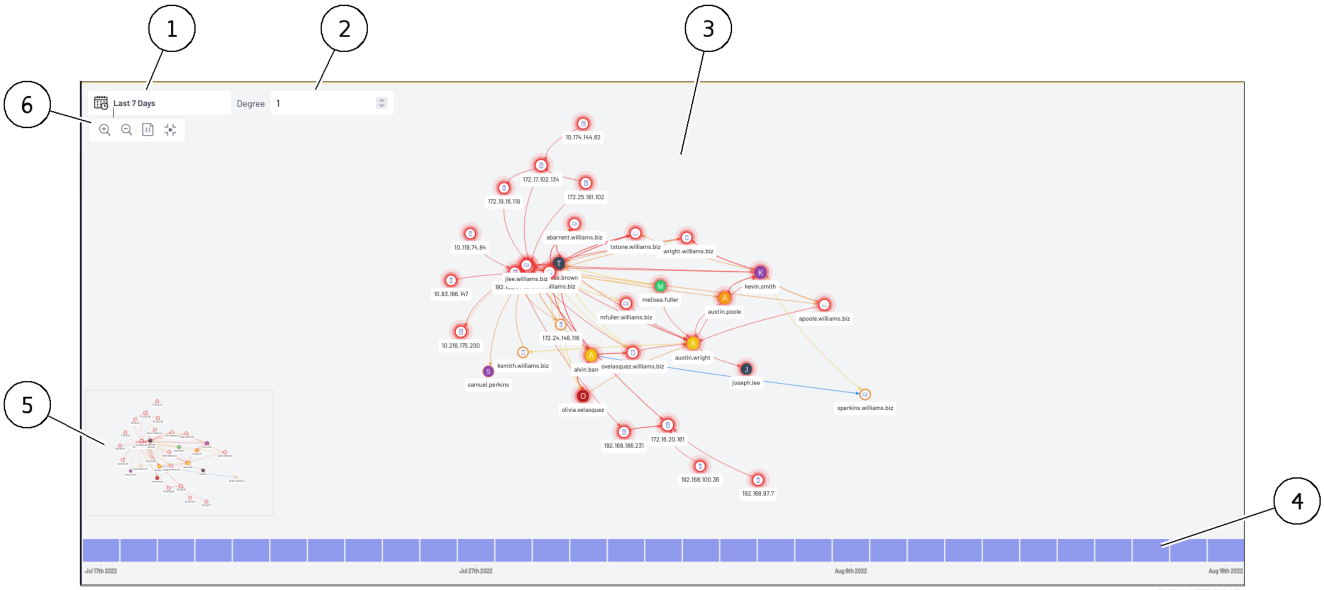
- Declare the equipment not to appear in the NDR dashboards (example: sensitive equipment, irrelevant equipment)

  For more information, see *`Forbidden assets` section of the sub menu `Assets/Users Association rules`*.

### 7.5.8 Procedure to analyse the relationship between equipment and users

- **From the navigation bar, click on the `Relations` button.**

  .



RELATIONS

- Choose the desired period using the timeline at the bottom of the page.
- Locate a user or equipment flashing red (risk score > 75%).
- Click on it, its interactions with other users and equipment are activated and a popup is displayed.
- Move the mouse over the activated links (interactions) to see what they mean.
- In the popup, the elements enabling further investigation are shown:
  - The main information about the item

- Alerts raised by the item

## 7.6 Use of Kibana dashboards

### 7.6.1 Introduction

The Kibana dashboards enable more in-depth investigation as they provide access to all events in the solution.
It is possible to trace a comprehensive attack by switching from dashboard to dashboard.
The purpose of this procedure is to present the method for tracing a specific attack.

| For | go to the |
|---|---|
| Investigation method in Kibana | *Procedure introducing the Kibana investigation method* |

See the *Overview of the Kibana GUI*.

### 7.6.2 Prerequisites

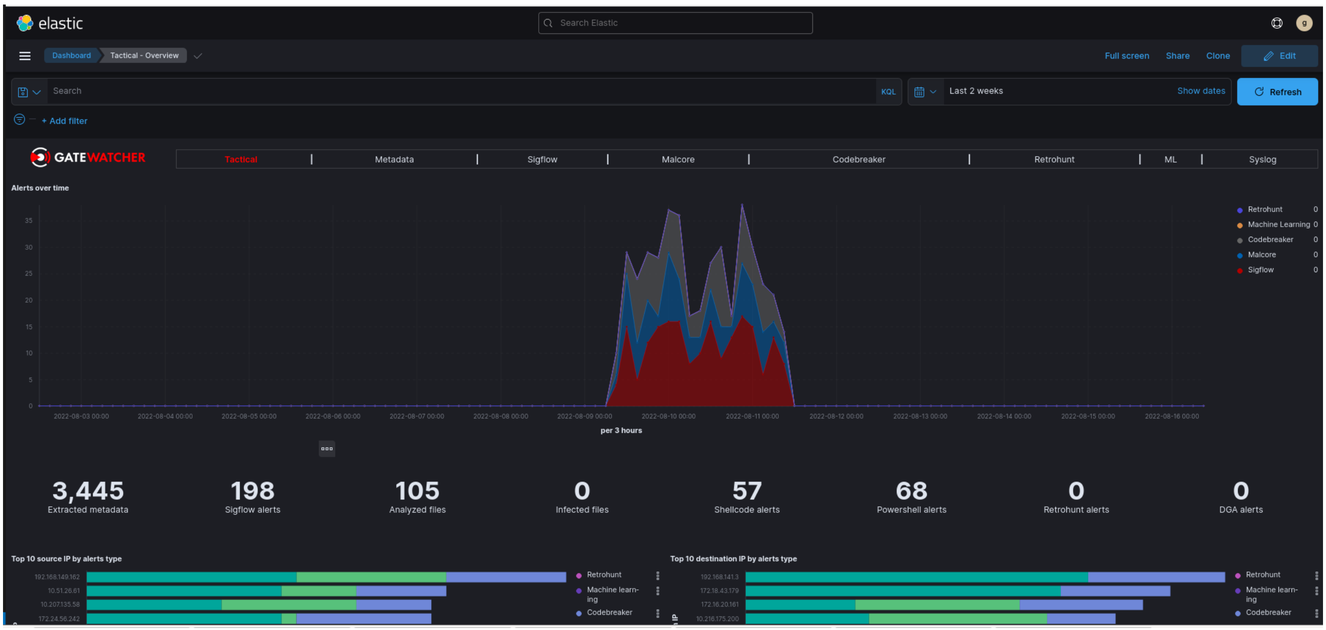
- User : member of **Operator** group

### 7.6.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

### 7.6.4 Procedure introducing the Kibana investigation method

- From the navigation bar, click on the `Hunting` button.



- Go to the `Malcore` tab.
- In the `Message` tab, locate the alert on an infected file requiring investigation.
- Scroll down this alert to display all the fields in the event.
- Find the `flow_id` field and perform a positive filter on it by pressing the +. The filter is displayed under the search bar.
- Click on this filter and then click on `Pin across all apps` to attach the filter and be able to keep it in the other dashboards.
- Browse the different "alert" dashboards to see if other alerts were generated for this flow.
- Browse the metadata dashboard to see which metadata were generated for this flow.

## 7.7 Detection procedure by Gscan

### 7.7.1 Introduction

GScan allows you to manually submit files for analysis.
The following options are possible:

- Malware: submit files to the Malcore engine
- Powershell: scans files containing Powershell scripts and detects potential threats that can serve as a gateway to install malware on Windows.

  With regard to malicious powershells, detection is based on a supervised machine learning model, and on the fact that these scripts generally use offuscation techniques or that are similar to them (base64, concatenation, type conversion, etc.).
- Shellcode: submits files for analysis by the codebreaker detection engine.

Before starting an analysis, it is necessary to check the type of analysis to be performed, see above.
To start parsing a file, simply drag the file into the `DRAG and DROP or CLICK TO SELECT YOUR FILES` area or click on this area to send the suspicious file.
The result of the analysis is then displayed in a thumbnail with the status of the file for each type of analysis chosen.
The `SCAN HISTORY` page displays the history of the analyses performed.

**Note:**

Attention the maximum file size should not exceed 10MB by default.
There is no limitation on the number of file scans.

Concerning the compressed files analyzed by Malcore:

- The number of files contained in an archive is:

- limited
- editable (50 is the default)

- The number of times the file is compressed is:

- limited (max recursion level)
- editable (5 is the default)

- If files are password protected, the password must be declared in the global settings.

These settings are only accessible to members of the administrator group.
See procedure for *Setting up GBox and the Malcore and Retroact engines and activate the GBox*.

- Modify if necessary the maximum size of files sent to Gscan (MB)
- Modify if necessary the maximum recursion level for archives sent to Gscan
- Modify if necessary the maximum number of archive files sent to Gscan

The graphical interface is described in the *Web UI `GScan` screen*.

---

### 7.7.2 Prerequisites

- User : member of **Operator** group

---

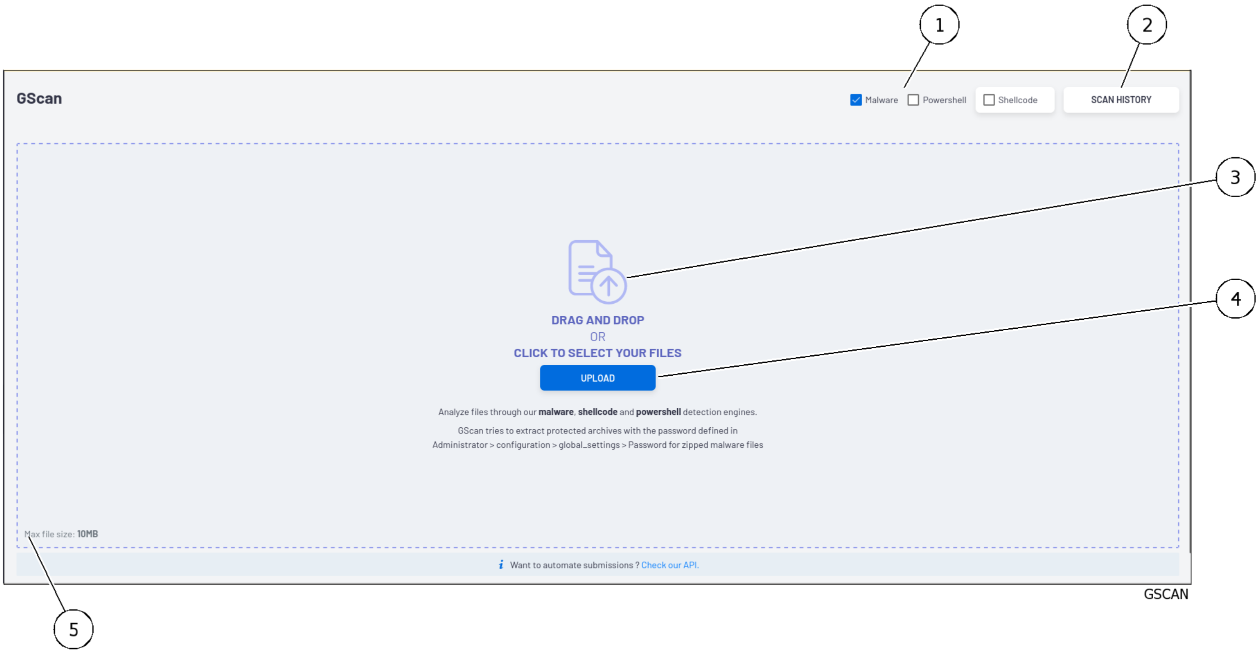
### 7.7.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

---

### 7.7.4 Procedure

- From the navigation bar, click on the `GScan` button



Analyze files through our **malware**, **shellcode** and **powershell** detection engines.

GScan tries to extract protected archives with the password defined in
Administrator > configuration > global_settings > Password for zipped malware files

Want to automate submissions ? Check our API.

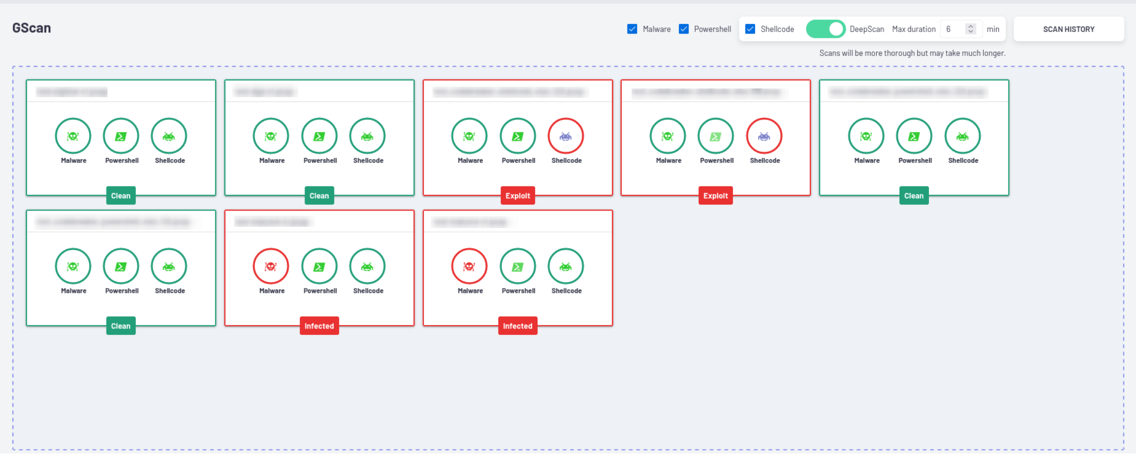
GSCAN

- Tick one or more of the following: `Malware`, `Powershell` or `Shellcode`.

> **Note:**
>
> The `DeepScan` option, checked by default, allows a thorough analysis of the file.

- As applicable:

- Drop desired file in box (3) `DRAG and DROP`
  or
- click on the button (4) `UPLOAD` then select the load file from the user PC and finally validate the selection
  The result is displayed in the thumbnail.



GScan

☑ Malware ☑ Powershell ☑ Shellcode DeepScan Max duration 6 min

SCAN HISTORY

Scans will be more thorough but may take much longer.

In the case of a positive result, the thumbnail is displayed in red with the information `Infected`.
In the case of a negative result, the thumbnail is displayed in green with the information `clean`.

Table1: Malcore engine results. are valid only for Malcore configuration at the time of analysis

| Return code | Result | Description | Action |
|---|---|---|---|
| 0 | No Threat Detected | File was analysed and declared healthy | No |
| 1 | Infected | File was scanned and declared infected | No |
| 2 | Suspicious | The file was analysed and declared as likely to be infected: some Malcore engines detected this file as malicious... | To be submitted to a GBox |
| 3 | Failed Scan | An error occurred during the run. | In the case of use via Gscan or GBox, restart the analysis |
| 7 | Skipped - Whitelisted | The file is not analysed and considered healthy since this file is defined in the Malcore whitelist | None if it is normal that this file is in the Malcore whitelist otherwise modify the list then restart the analysis |
| 8 | Skipped – Blacklisted | The file is not scanned and considered infected since this file is defined in the Malcore blacklist | None if it is normal that this file is in the Malcore blacklist otherwise modify the list then restart the analysis |
| 9 | Exceeded Archive Depth | The number of times the file is compressed is limited (max recursion level). The message indicates that the defined value has been exceeded. | It is possible to increase this limit and to restart the analysis (attention this can lead to an increase in processing time ...) |
| 10 | Not scanned | Pb analysis engine | Contact Gatewatcher support if this happens again |

suite sur la page suivante

Table 1 – suite de la page précédente

| Return code | Result | Description | Action |
|---|---|---|---|
| 12 | Encrypted Archive | The archive is encrypted and therefore not parsable: the password indicated does not work | Enter the correct password and run the analysis again |
| 13 | Exceeded Archive Size | The maximum file size should not exceed the defined value (maximum value 10MB). The parsed archive is larger than the defined value. | If the set value is less than 10MB, it is possible to change this limit and restart the analysis, otherwise none |
| 14 | Exceeded Archive File Number | The maximum number of files in the archive must not exceed the defined value. The scanned archive contains a number of files greater than the defined value. | It is possible to increase this limit and to restart the analysis (attention this can lead to an increase in processing time ...) |
| 15 | Password Protected Document | Solution detected inconsistent behaviour with password protected document | No action+ |
| 16 | Exceeded Archive Timeout | The archive scan time has been exceeded, Malcore engines are not responding within the deadline | Restart the analysis if possible |
| 17 | Filetype Mismatch | File type mismatch problem: the solution detects the file extension with its contents and compares it with the file extension displayed | No action+ |
| 18 | Potentially Vulnerable File | The verdict of the result is: Potentially vulnerable files are files associated with identified vulnerable components or applications. | No action+ |
| 19 | Cancelled | User explicitly canceled this file analysis request | posted for information |
| 21 | Yara Rule Matched | The verdict of the result is: a corresponding Yara rule (malware sample identification); | Posted for information |
| 22 | Potentially Unwanted | The solution detected potentially unwanted applications. | Posted for information |
| 23 | Unsupported File Type | File type not supported by the solution. | No |
| 255 | In Progress | Analysis in progress.. | Wait for the analysis to complete |

Table2: Codebreaker engine results. Only valid for Codebreaker configuration at time of analysis

| State | description | action |
|---|---|---|
| Clean | File was analysed and declared healthy | No |
| Exploit | File was scanned and declared infected (shellcode or powershell) | No |
| Suspicious | The file was analysed and declared susceptible to infection: the engine detected this file as malicious | If possible to submit to a GBox |

**Note:**

In the case of an `Analysis Error` message, leave the mouse over the icon.

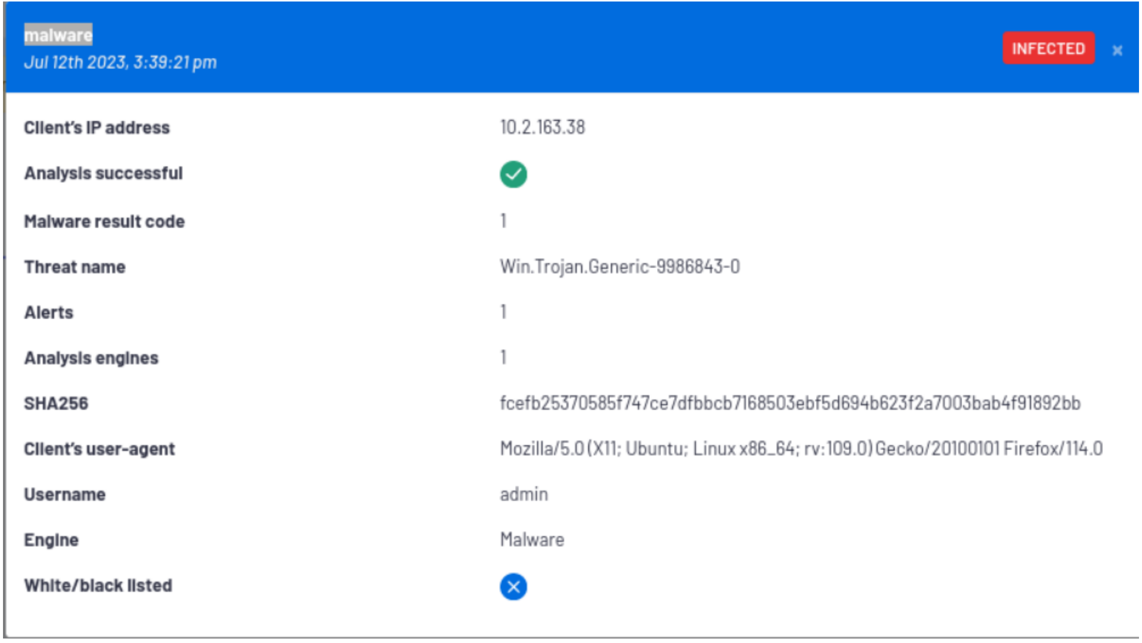
If the message `Gscan is not enabled` is displayed, contact a member of the administrator group to activate this option from the configuration menu.

Otherwise check that the motors are up to date. To do this, use the `Health check` screen. Use GUM to remedy this.

- Click on thumbnail.

  The detail window is displayed:

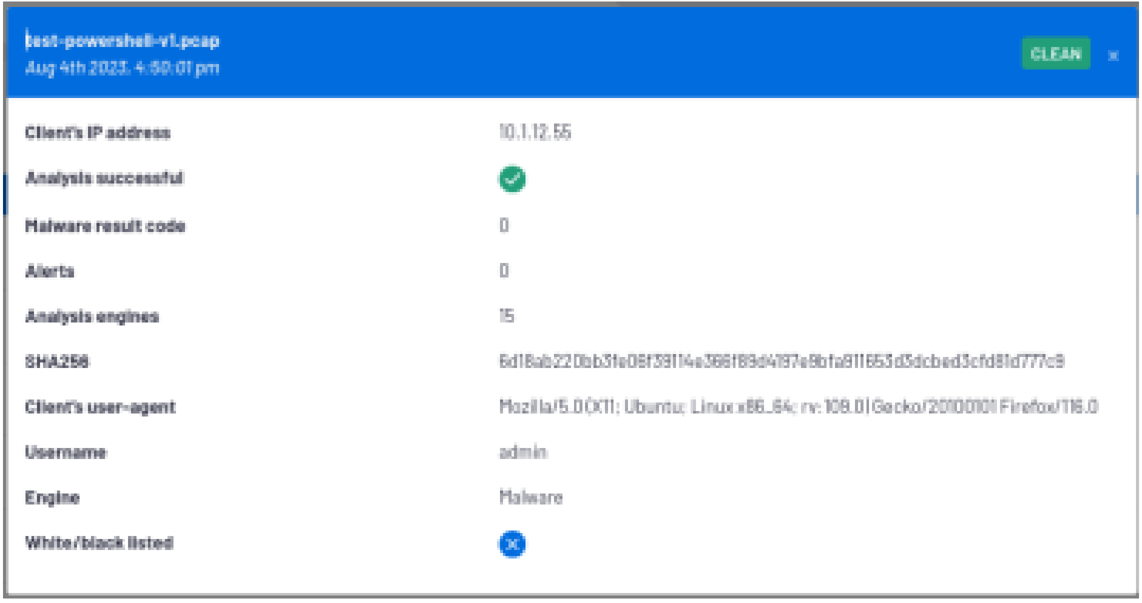
  – In the case of a positive result, this window gives detailed information about the detected threat.



malware
Jul 12th 2023, 3:39:21 pm

| | |
|---|---|
| Client's IP address | 10.2.163.38 |
| Analysis successful | ✓ |
| Malware result code | 1 |
| Threat name | Win.Trojan.Generic-9986843-0 |
| Alerts | 1 |
| Analysis engines | 1 |
| SHA256 | fcefb25370585f747ce7dfbbcb7168503ebf5d694b623f2a7003bab4f91892bb |
| Client's user-agent | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/114.0 |
| Username | admin |
| Engine | Malware |
| White/black listed | ✕ |

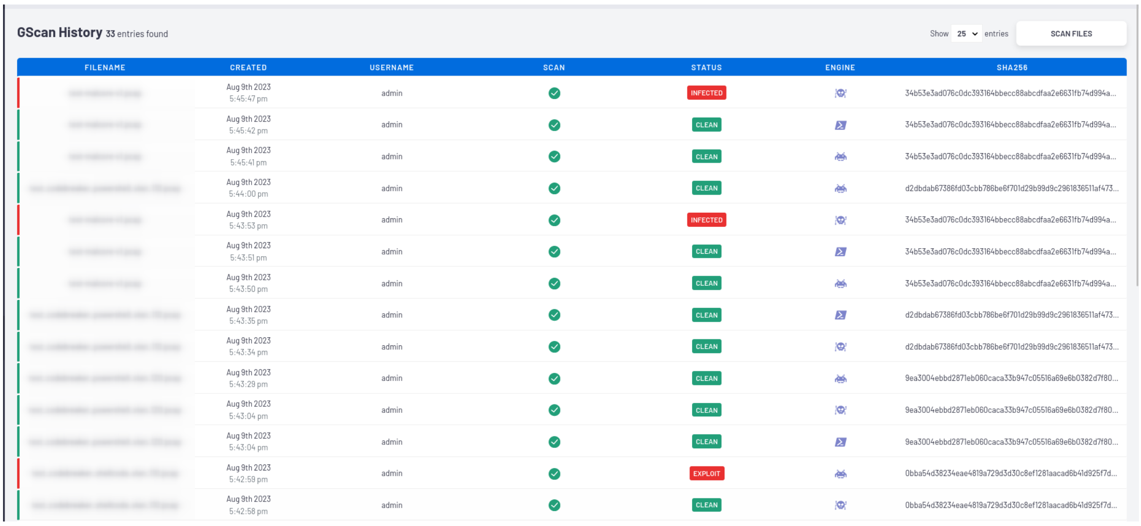
  – In the case of a negative result, this window gives detailed information about the analysis.



test-powershell-v1.pcap
Aug 4th 2023, 4:50:01 pm

| | |
|---|---|
| Client's IP address | 10.1.12.55 |
| Analysis successful | ✓ |
| Malware result code | 0 |
| Alerts | 0 |
| Analysis engines | 15 |
| SHA256 | 6d18ab220bb31e06f39114e366f89d4197e8bfa911653d3dcbed3cfd81d777c9 |
| Client's user-agent | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0 |
| Username | admin |
| Engine | Malware |
| White/black listed | ✕ |

  – In all cases, this analysis is now available in the history accessible by the `SCAN HISTORY` button.



GScan History 33 entries found

| FILENAME | CREATED | USERNAME | SCAN | STATUS | ENGINE | SHA256 |
|---|---|---|---|---|---|---|
| [illegible] | Aug 9th 2023 5:45:47 pm | admin | ✓ | INFECTED | ☠ | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023 5:45:42 pm | admin | ✓ | CLEAN | ≻ | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023 5:45:41 pm | admin | ✓ | CLEAN | 👾 | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023 5:44:00 pm | admin | ✓ | CLEAN | 👾 | d2dbdab67386fd03cbb786be6f701d29b99d9c2961836511af473... |
| [illegible] | Aug 9th 2023 5:43:53 pm | admin | ✓ | INFECTED | ☠ | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023 5:43:51 pm | admin | ✓ | CLEAN | ≻ | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023 5:43:50 pm | admin | ✓ | CLEAN | 👾 | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023 5:43:35 pm | admin | ✓ | CLEAN | ≻ | d2dbdab67386fd03cbb786be6f701d29b99d9c2961836511af473... |
| [illegible] | Aug 9th 2023 5:43:34 pm | admin | ✓ | CLEAN | ☠ | d2dbdab67386fd03cbb786be6f701d29b99d9c2961836511af473... |
| [illegible] | Aug 9th 2023 5:43:29 pm | admin | ✓ | CLEAN | 👾 | 9ea3004ebbd2871eb060caca33b947c05516a69e6b0382d7f80... |
| [illegible] | Aug 9th 2023 5:43:04 pm | admin | ✓ | CLEAN | ☠ | 9ea3004ebbd2871eb060caca33b947c05516a69e6b0382d7f80... |
| [illegible] | Aug 9th 2023 5:43:04 pm | admin | ✓ | CLEAN | ≻ | 9ea3004ebbd2871eb060caca33b947c05516a69e6b0382d7f80... |
| [illegible] | Aug 9th 2023 5:42:59 pm | admin | ✓ | EXPLOIT | 👾 | 0bba54d38234eae4819a729d3d30c8ef1281aacad6b41d925f7d... |
| [illegible] | Aug 9th 2023 5:42:58 pm | admin | ✓ | CLEAN | ☠ | 0bba54d38234eae4819a729d3d30c8ef1281aacad6b41d925f7d... |

**Astuce:**

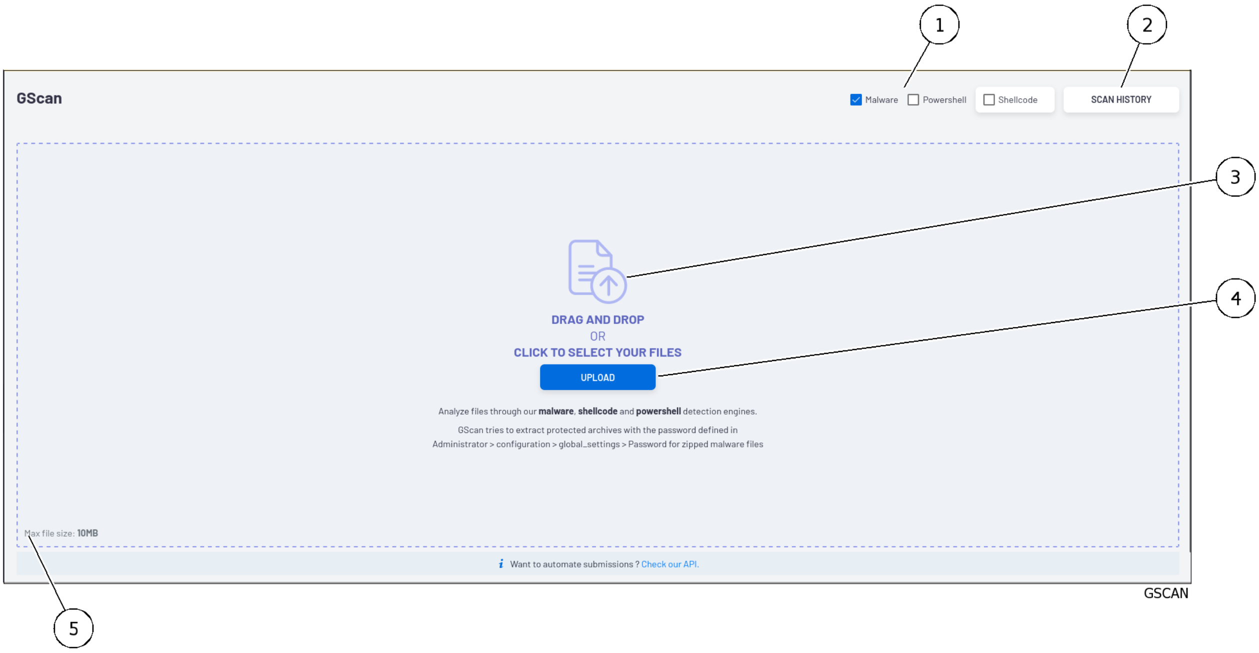
The result is indicative only for the type of analysis selected.
A file is declared clean only for the selected engine.

For the alerts detected by the Malcore engine, the details of the counters of the report given in part *Malcore engine*.
For the alerts detected by the codebreaker engine, the details of the counters of the report given in the part *Codebreaker Engine*.

### 7.7.5 Ex post facto search procedure

It is possible to change the type of detection after a first analysis.

- From the navigation bar, click on the `GScan` button.



Analyze files through our **malware**, **shellcode** and **powershell** detection engines.

GScan tries to extract protected archives with the password defined in Administrator > configuration > global_settings > Password for zipped malware files

Max file size: **10MB**

Want to automate submissions ? Check our API.

GSCAN

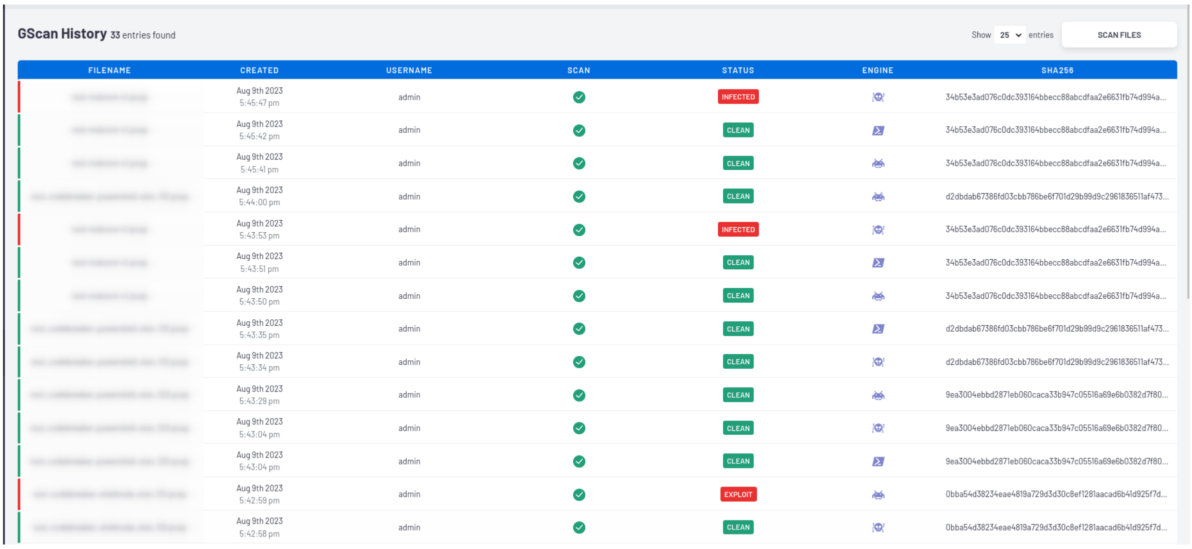
- Tick the `Malware` box for example.
- Place the desired file in the dotted box.

  The result is displayed in the thumbnail.
- Tick the `Shellcode` box.

  The thumbnail shows the result for the shellcode analysis.

### 7.7.6 Procedure to view the history

- Click the `SCAN HISTORY` button.



**GScan History** 33 entries found

| FILENAME | CREATED | USERNAME | SCAN | STATUS | ENGINE | SHA256 |
|---|---|---|---|---|---|---|
| [illegible] | Aug 9th 2023<br>5:45:47 pm | admin | ✓ | INFECTED | 🐞 | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023<br>5:45:42 pm | admin | ✓ | CLEAN | >_ | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023<br>5:45:41 pm | admin | ✓ | CLEAN | 👾 | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023<br>5:44:00 pm | admin | ✓ | CLEAN | 👾 | d2dbdab67386fd03cbb786be6f701d29b99d9c2961836511af473... |
| [illegible] | Aug 9th 2023<br>5:43:53 pm | admin | ✓ | INFECTED | 🐞 | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023<br>5:43:51 pm | admin | ✓ | CLEAN | >_ | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023<br>5:43:50 pm | admin | ✓ | CLEAN | 👾 | 34b53e3ad076c0dc393164bbecc88abcdfaa2e6631fb74d994a... |
| [illegible] | Aug 9th 2023<br>5:43:35 pm | admin | ✓ | CLEAN | >_ | d2dbdab67386fd03cbb786be6f701d29b99d9c2961836511af473... |
| [illegible] | Aug 9th 2023<br>5:43:34 pm | admin | ✓ | CLEAN | 🐞 | d2dbdab67386fd03cbb786be6f701d29b99d9c2961836511af473... |
| [illegible] | Aug 9th 2023<br>5:43:29 pm | admin | ✓ | CLEAN | 👾 | 9ea3004ebbd2871eb060caca33b947c05516a69e6b0382d7f80... |
| [illegible] | Aug 9th 2023<br>5:43:04 pm | admin | ✓ | CLEAN | 🐞 | 9ea3004ebbd2871eb060caca33b947c05516a69e6b0382d7f80... |
| [illegible] | Aug 9th 2023<br>5:43:04 pm | admin | ✓ | CLEAN | >_ | 9ea3004ebbd2871eb060caca33b947c05516a69e6b0382d7f80... |
| [illegible] | Aug 9th 2023<br>5:42:59 pm | admin | ✓ | EXPLOIT | 👾 | 0bba54d38234eae4819a729d3d30c8ef1281aacad6b41d925f7d... |
| [illegible] | Aug 9th 2023<br>5:42:58 pm | admin | ✓ | CLEAN | 🐞 | 0bba54d38234eae4819a729d3d30c8ef1281aacad6b41d925f7d... |

- Click on a scanned file to view the details of the analysis done.

## 7.8 Send file for external analysis to GCenter

### 7.8.1 Introduction

The GCenter can send files (defined as suspicious or infected) to a remote server (Intelligence site or GBox).
Sending can be done automatically via the configuration or manually via a menu command.
The remote server scans the file and then provides a scan report.
The analysis report is visible on the GCenter to be read by an analyst.

### 7.8.2 Prerequisites

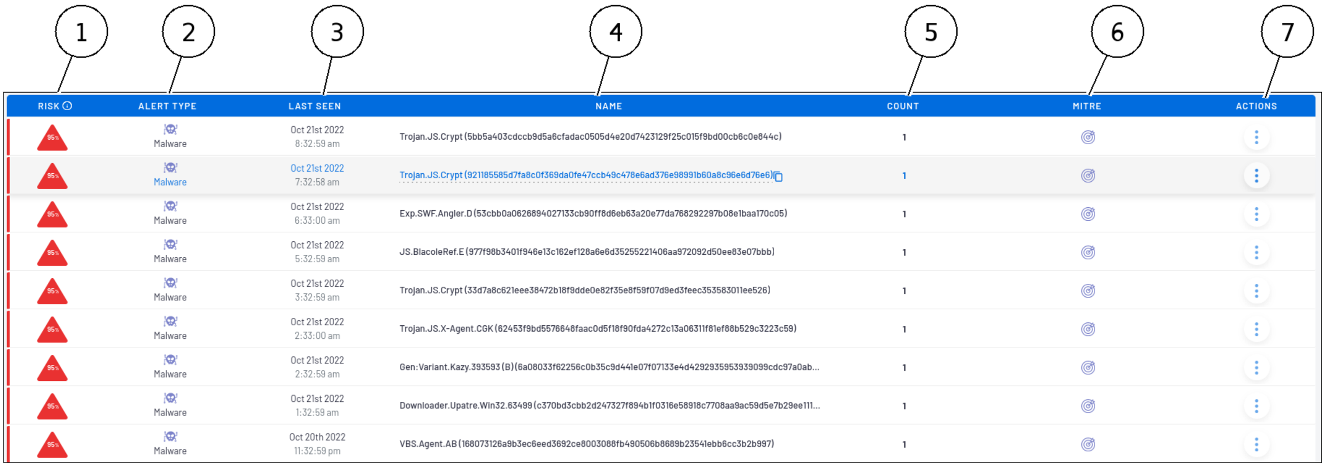
- User : member of **Operator** group

### 7.8.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

### 7.8.4 Procedure to acces to the `Alerts` screen

- Click on the `Alerts` button on the navigation bar, the following screen is displayed.



| RISK ⓘ | ALERT TYPE | LAST SEEN | NAME | COUNT | MITRE | ACTIONS |
|---|---|---|---|---|---|---|
| 95% | Malware | Oct 21st 2022<br>8:32:59 am | Trojan.JS.Crypt (5bb5a403cdccb9d5a6cfadac0505d4e20d7423129f25c015f9bd00cb6c0e844c) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>7:32:58 am | Trojan.JS.Crypt (921185585d7fa8c0f369da0fe47ccb49c478e6ad376e98991b60a8c96e6d76e6) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>6:33:00 am | Exp.SWF.Angler.D (53cbb0a0626894027133cb90ff8d6eb63a20e77da768292297b08e1baa170c05) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>5:32:59 am | JS.BlacoleRef.E (977f98b3401f946e13c162ef128a6e6d35255221406aa972092d50ee83e07bbb) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>3:32:59 am | Trojan.JS.Crypt (33d7a8c621eee38472b18f9dde0e82f35e8f59f07d9ed3feec353583011ee526) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>2:33:00 am | Trojan.JS.X-Agent.CGK (62453f9bd5576648faac0d5f18f90fda4272c13a06311f81ef88b529c3223c59) | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>2:32:59 am | Gen:Variant.Kazy.393593 (B) (6a08033f62256c0b35c9d441e07f07133e4d4292935953939099cdc97a0ab... | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 21st 2022<br>1:32:59 am | Downloader.Upatre.Win32.63499 (c370bd3cbb2d247327f894b1f0316e58918c7708aa9ac59d5e7b29ee111... | 1 | ◎ | ⋮ |
| 95% | Malware | Oct 20th 2022<br>11:32:59 pm | VBS.Agent.AB (168073126a9b3ec6eed3692ce8003088fb490506b8689b23541ebb6cc3b2b997) | 1 | ◎ | ⋮ |

ALERTS-02

### 7.8.5 Procedure to send the file to the remote server

- Select the alert to be analyzed and click on the menu of possible actions in column (7).
- Click `` `Generate Remote Analysis` ``.
  If no remote server is connected then a message appears `` `Server error` ``.
  If the remote server is running then there is a waiting message for report generation: `` `Generating report, please wait...` ``.
  Deleting the message indicates the report is available.

### 7.8.6 Procedure to download the report

- Click on the `` `Download Analysis Report` `` command.
  The report is downloaded and displayed in the browser.
- To analyze the contents of the file, see *Analysis Report Analysis Procedure*.

## 7.9 Analysis Report Analysis Procedure

### 7.9.1 Introduction

If a file is sent to a remote server (GBox or site intelligence), the analysis is performed by the remote server and it can be downloaded as a pdf report.
For more information on the contents of this report, see paragraph *Results and analysis report*.

**Important:**

The SCORE field only makes sense for the pre-selected engine. It does not indicate that the scanned file is healthy but only that it is declared healthy by this engine.

To send the file to be analyzed to the remote server (such as the GBox) and retrieve the report, see *Send file for external analysis to GCenter*.

### 7.9.2 Prerequisites

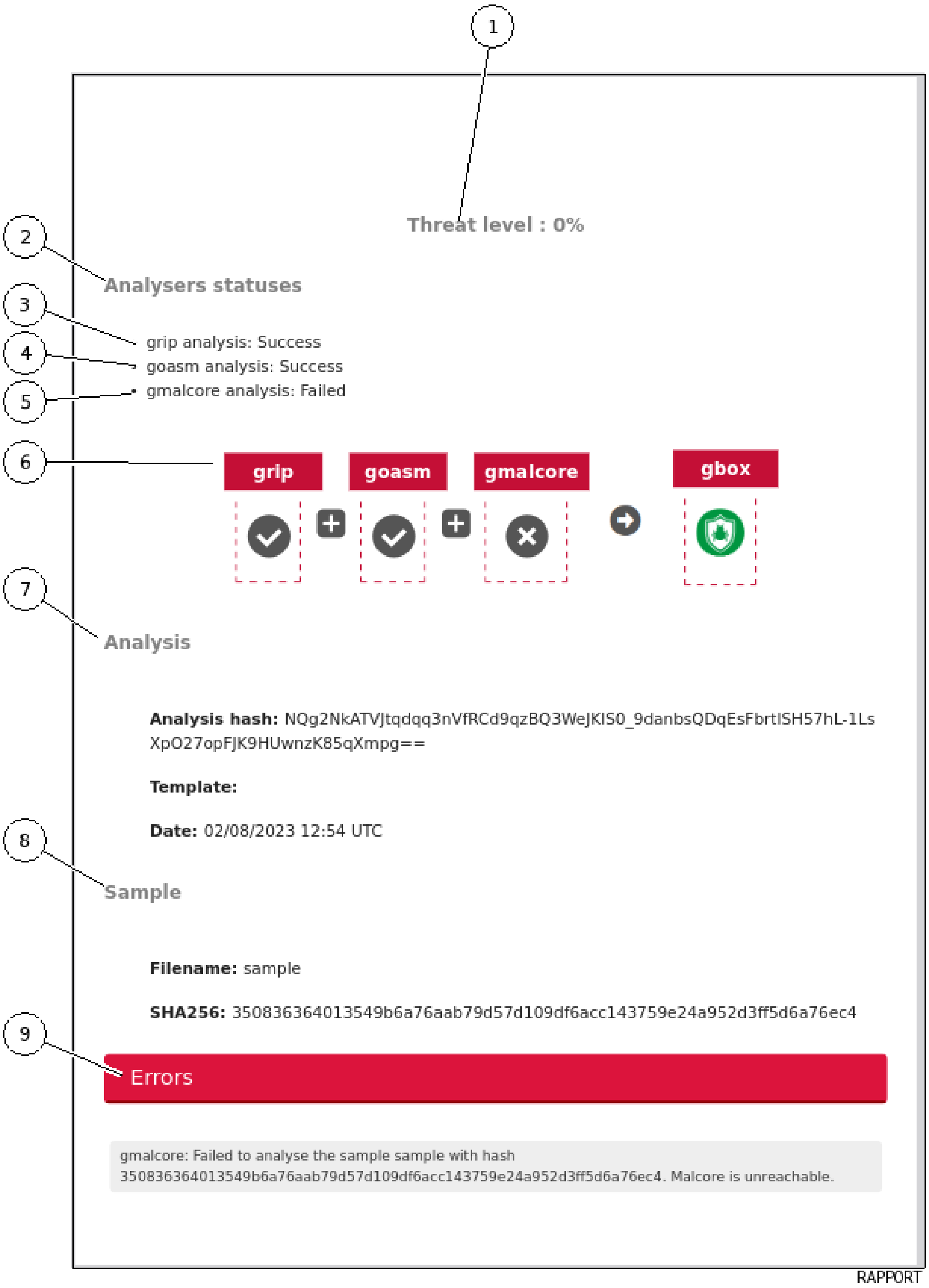
- User : member of **Operator** group

### 7.9.3 Opérations préliminaires

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

### 7.9.4 Procedure to analyse the `Error` Status

The `Error` status is indicated in part (9).



Threat level : 0%

Analysers statuses

- grip analysis: Success
- goasm analysis: Success
- gmalcore analysis: Failed

Analysis

**Analysis hash:** NQg2NkATVJtqdqq3nVfRCd9qzBQ3WeJKIS0_9danbsQDqEsFbrtISH57hL-1LsXpO27opFJK9HUwnzK85qXmpg==

**Template:**

**Date:** 02/08/2023 12:54 UTC

Sample

**Filename:** sample

**SHA256:** 350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4

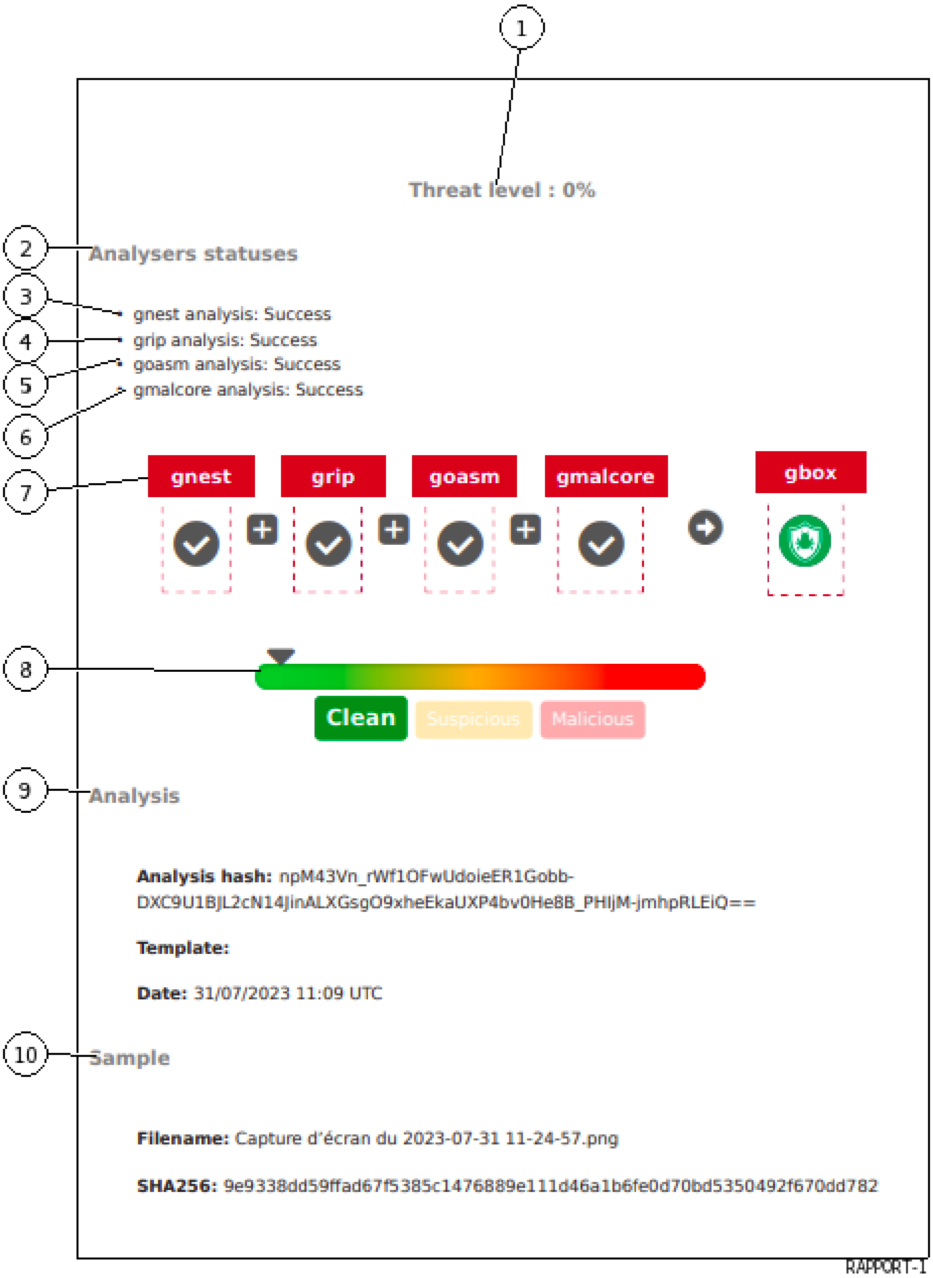
Errors

```
gmalcore: Failed to analyse the sample sample with hash
350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4. Malcore is unreachable.
```

- Look at the reason for the error in the detailed text below.
  In this example, the error is on the Gmalcore engine which is unavailable.
  Here, the analysis is not significant.
- Restart the Gmalcore engine on the GBox before restarting the analysis.

### 7.9.5 Procedure to analyse the `Clean` status

- View the report.



Threat level : 0%

Analysers statuses

- gnest analysis: Success
- grip analysis: Success
- goasm analysis: Success
- gmalcore analysis: Success

Analysis

**Analysis hash:** npM43Vn_rWf1OFwUdoieER1Gobb-DXC9U1BJL2cN14JinALXGsgO9xheEkaUXP4bv0He8B_PHIjM-jmhpRLEiQ==

**Template:**

**Date:** 31/07/2023 11:09 UTC

Sample

**Filename:** Capture d'écran du 2023-07-31 11-24-57.png

**SHA256:** 9e9338dd59ffad67f5385c1476889e111d46a1b6fe0d70bd5350492f670dd782

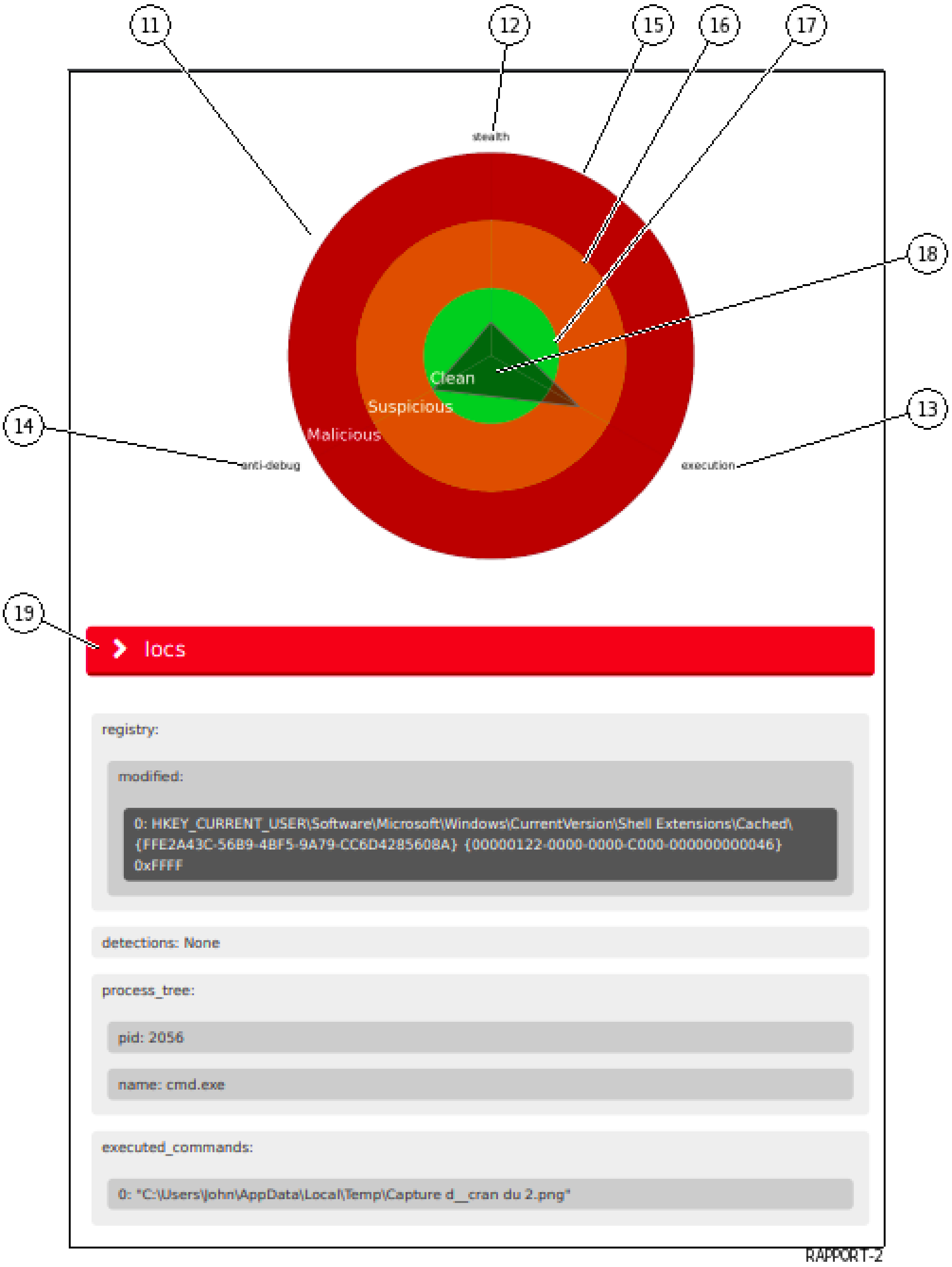
The "Clean" status is indicated in the visual signage (8).
This report is composed of:

- A threat level (1) `Threat level`: here 0%
  This score is calculated from the analysis score returned by the different engines **active** of the GBox in the model at the time of detection
- Part (2) `Analysers statuses`.
  This part lists the engines activated during the analysis and their results.
  This part indicates which analysis was done but in no case the result of the analysis:
  - `gnest analysis: Success`: Gnest engine analysis (3) was carried out
  - `grip analysis: Success`: Grip engine analysis (4) has been done

- `goasm analysis: Success`: Goasm engine analysis (5) has been done
- `gmalcore analysis: Success`: analysis of the Gmalcore engine (6) has been carried out
- The summary of the analysis steps (7) which displays:
- List of engines used: here gnest, grip, goasm and gmalcore
- The result of the analysis for each of the engines: the check mark indicates that the analysis was executed correctly. A cross indicates that the run did not run properly.

  right side, the result of the analysis of the GBox: here the icon means Clean

- Part (9) `Analysis` provides analysis information: hash, model and date
- Part (10) `Sample` gives sample information: filename and sha256



registry:

modified:

0: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\ {FFE2A43C-56B9-4BF5-9A79-CC6D4285608A} {00000122-0000-0000-C000-000000000046} 0xFFFF

detections: None

process_tree:

pid: 2056

name: cmd.exe

executed_commands:

0: "C:\Users\John\AppData\Local\Temp\Capture d__cran du 2.png"

**Note:**

Graph (11) is only available if Gnest is part of the model (the data needed for the graph is returned by this engine).

This graph (11) provides a visual on the dangerousness of the analyzed file:

- The category of dangerousness is defined by axes (12) (13) and (14): titles and number of axes are given by the motors.
- The level of dangerousness is given by concentric circles.
- The central circle (17) indicates the healthy level.
- Middle circle (16) indicates suspicious level.
- Outer circle (15) indicates malicious level.

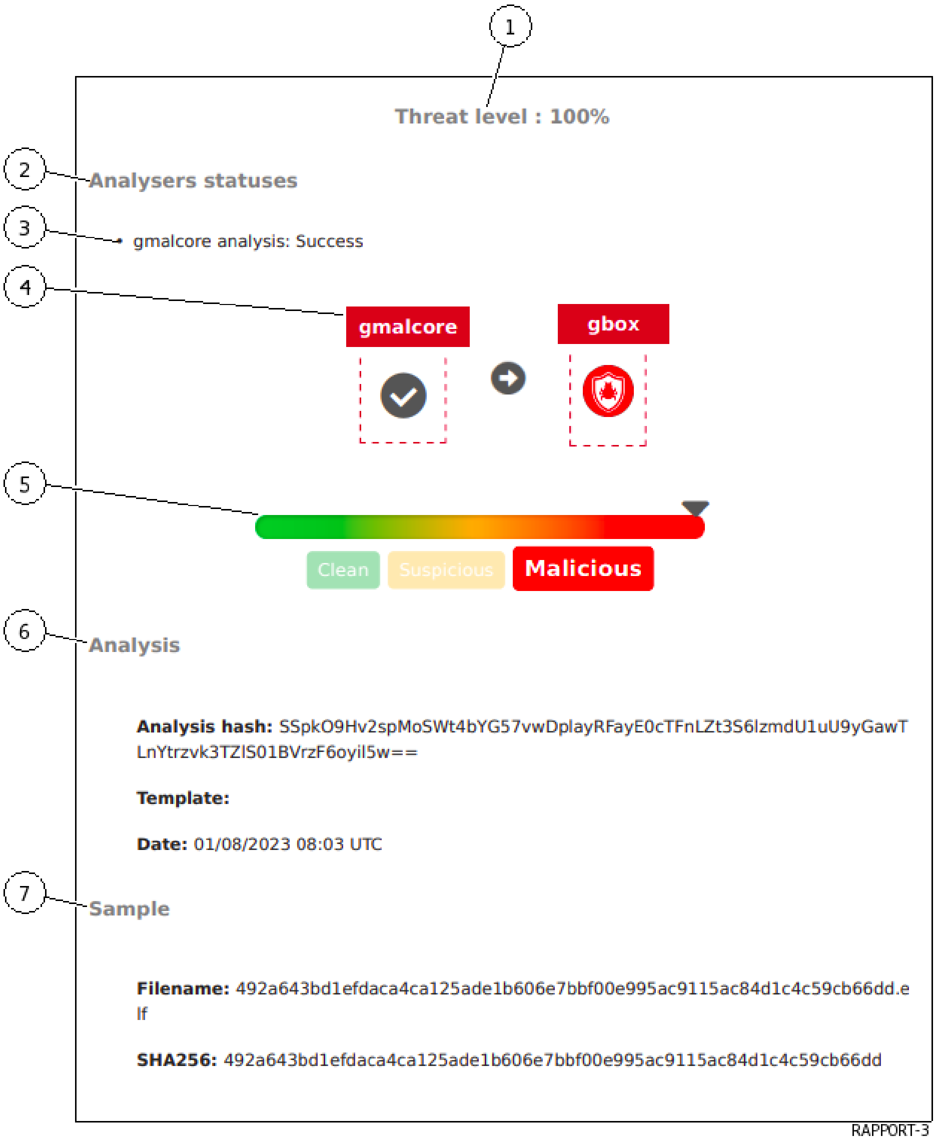
The synthesis for the file is read on the vertices of the represented form (18).
In the displayed example, the vertex (5) indicates that the file is:

- Suspicious in line `` `execution` `` (13)
- Healthy in axis `` `stealth` `` (12) and axis `` `antidebug` `` (14)

Then the report details the parts retailers analyses: Iocs (19), Static etc..
The details of these parts are given in the table below:

| Part Title | Description | Is engine activated |
|---|---|---|
| `` `Analysis options` `` | Option values used for analysis | Grip and Gnest |
| `` `Iocs` `` | List of actions performed (files, registry, network, processes...) | GNEST |
| `` `Ttps` `` | TTPs analyse the functioning of a malicious actor, they describe how cyber attackers orchestrate, execute and manage operational attacks.<br>TTPs contextualize a threat. They reveal the steps or actions taken by malicious actors during data exfiltration for example. | GNEST |
| `` `Static` `` | Métadonnées | GRIP |
| `` `Overview` `` | File information (size, different hash, type...) | GNEST |
| `` `Heuristic` `` | List of engines (Entry#x) and name of the threat returned by the Gmalcore module (or n/a) | Gmalcore |
| `` `Shellcode` `` | Result of shellcode detection | GOASM |
| `` `Signatures` `` | List of yara signatures corresponding to the analyzed file | Gnest |
| `` `Process Tree` `` | Graphical representation of the process tree | Gnest |

### 7.9.6 Procedure to analyse the `Malicious` status



Threat level : 100%

Analysers statuses

- gmalcore analysis: Success

Analysis

**Analysis hash:** SSpkO9Hv2spMoSWt4bYG57vwDplayRFayE0cTFnLZt3S6lzmdU1uU9yGawTLnYtrzvk3TZlS01BVrzF6oyil5w==

**Template:**

**Date:** 01/08/2023 08:03 UTC

Sample

**Filename:** 492a643bd1efdaca4ca125ade1b606e7bbf00e995ac9115ac84d1c4c59cb66dd.elf

**SHA256:** 492a643bd1efdaca4ca125ade1b606e7bbf00e995ac9115ac84d1c4c59cb66dd

- Read the report.
  The `Malicious` status is indicated in the visual signalétique (5).

  This report is composed of:

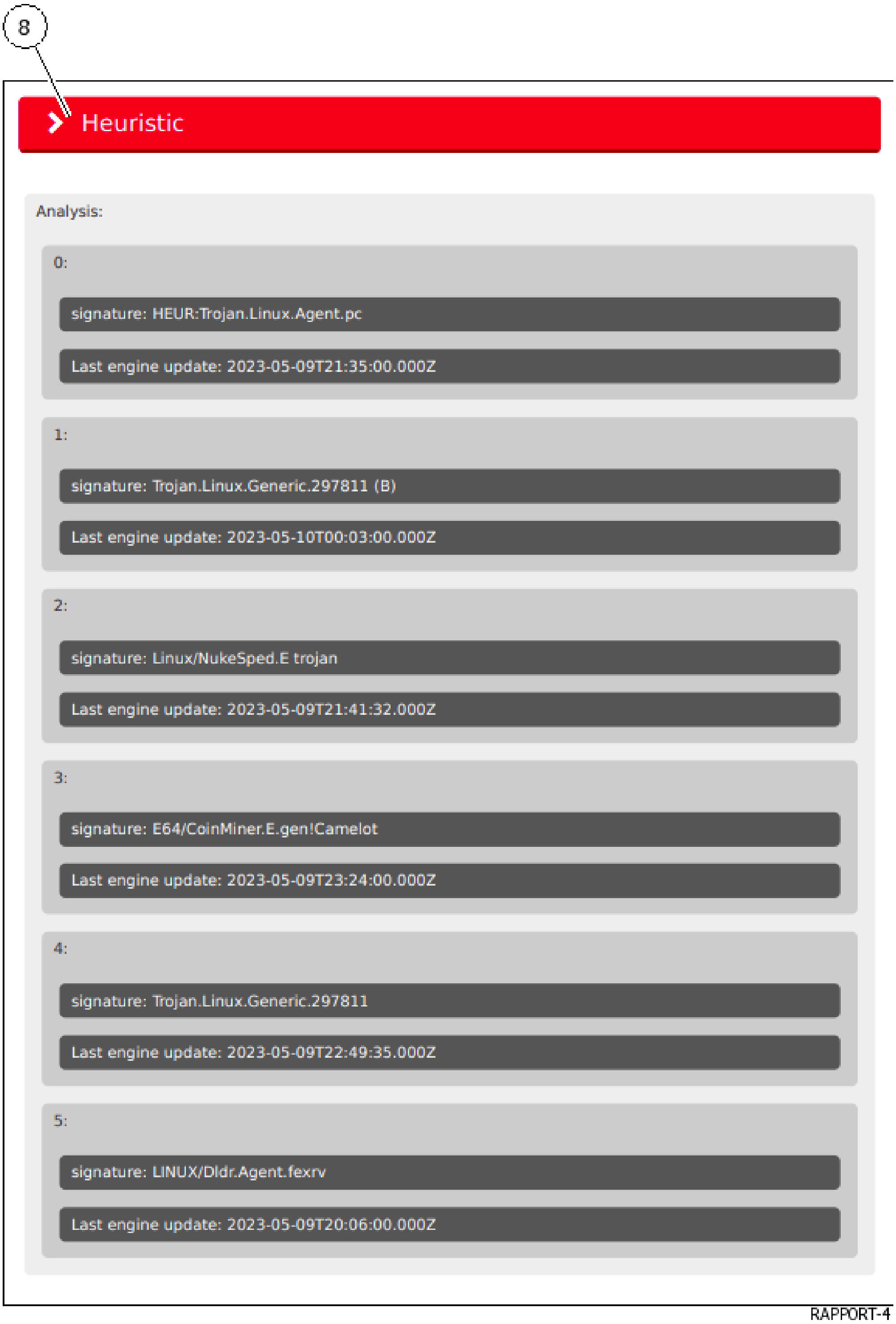
  - A threat level (1) `Threat level`: here 100%
    This score is calculated from the analysis score returned by the different engines **active** of the GBox in the model at the time of detection
  - Part (2) `Analysers statuses`

    This part lists the engines activated during the analysis and their results.
    This part indicates which analysis was done but, in no case, the result of the analysis:

    - `gmalcore analysis: Success`: analysis of the Gmalcore engine (3) has been carried out;
    - The summary of the analysis steps (4) which displays:
    - List of engines used: here gmalcore only
    - The result of the analysis for each of the engines: the check mark indicates that the analysis was executed correctly. A cross indicates that the run did not run properly.

      Right side, the result of the analysis of the GBox: here the icon means `Malicious`
  - Part (6) `Analysis` provides analysis information: hash, model and date

- Part (7) `Sample` gives sample information: filename and sha256



Analysis:

0:

signature: HEUR:Trojan.Linux.Agent.pc

Last engine update: 2023-05-09T21:35:00.000Z

1:

signature: Trojan.Linux.Generic.297811 (B)

Last engine update: 2023-05-10T00:03:00.000Z

2:

signature: Linux/NukeSped.E trojan

Last engine update: 2023-05-09T21:41:32.000Z

3:

signature: E64/CoinMiner.E.gen!Camelot

Last engine update: 2023-05-09T23:24:00.000Z

4:

signature: Trojan.Linux.Generic.297811

Last engine update: 2023-05-09T22:49:35.000Z

5:

signature: LINUX/Dldr.Agent.fexrv

Last engine update: 2023-05-09T20:06:00.000Z

Then the detailed report the parties retailers the analyses: Heuristic (8).
The details of these parts are given in the table below:

| Part Title | Description | Is engine activated |
|---|---|---|
| `Analysis options` | Option values used for analysis | Grip and Gnest |
| `Iocs` | List of actions performed (files, registry, network, processes...) | GNEST |
| `Ttps` | TTPs analyse the functioning of a malicious actor, they describe how cyber attackers orchestrate, execute and manage operational attacks.<br>TTPs contextualize a threat. They reveal the steps or actions taken by malicious actors during data exfiltration for example. | GNEST |
| `Static` | Métadonnées | GRIP |
| `Overview` | File information (size, different hash, type...) | GNEST |
| `Heuristic` | List of engines (Entry#x) and name of the threat returned by the Gmalcore module (or n/a) | Gmalcore |
| `Shellcode` | Result of shellcode detection | GOASM |
| `Signatures` | List of yara signatures corresponding to the analyzed file | Gnest |
| `Process Tree` | Graphical representation of the process tree | Gnest |

- Analyze the results according to the score.

**Astuce:**

A non-zero score is an indication of a threat.
A zero score only means that the current engine has not detected any threats.
Do not hesitate to restart the analysis with all the engines of the GBox.

- Concatenate the GCenter and GBox report results.

---

## 7.10 Configuring Metadata Rate Limiters

### 7.10.1 Introduction

In addition to alerts, GCaps generate metadata events on analyzed network flows.
This information can be useful in surveys, but in a certain context, it can quickly exceed the indexing capabilities of GCenter.
In order to reduce the amount of metadata while maintaining most information exchanges, it is possible to enable the limiters defined below.

See *Web UI `Config - Metadata rate limiter` screen*.

---

### 7.10.2 Prerequisites

- User : member of **Operator** group

---

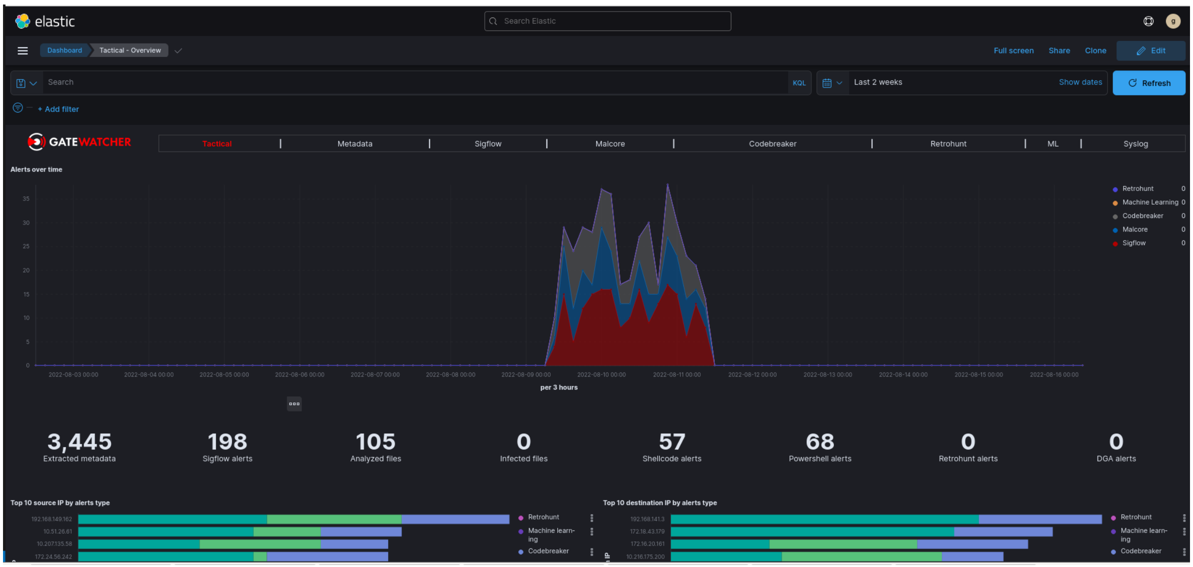
### 7.10.3 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

---

### 7.10.4 Procedure to view metadata

- In the navigation bar, click on the `` `Hunting` `` button.



This GUI is described in *Native dashboards*.

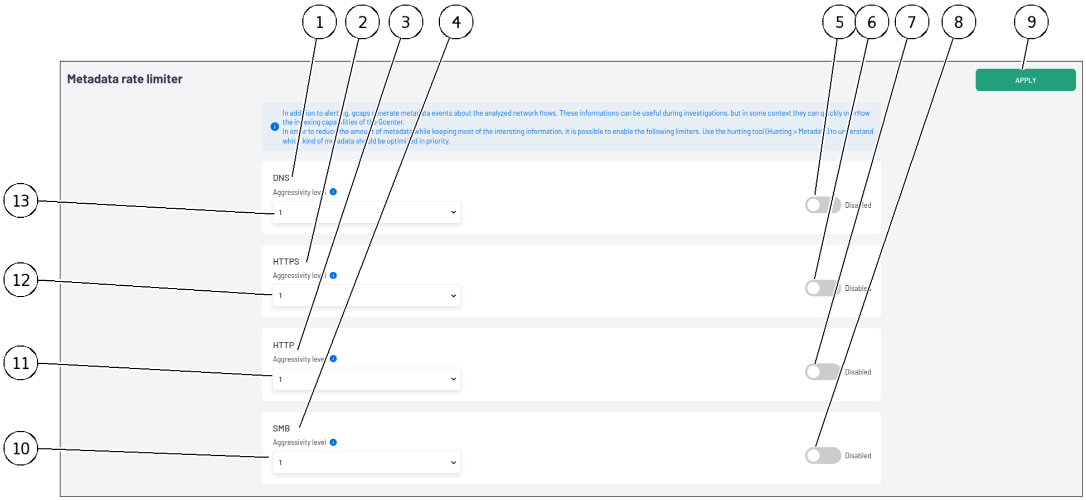
- Use the Kibana tool (hunting > Metadata command) to understand what kind of metadata should be optimized first.

---

### 7.10.5 Procedure to setup the limiter then activate

- In the navigation bar, click successively on:
- The `` `Config` ``
- The button `` `Metadata rate limiter` ``

  The following screen is displayed.



Metadata rate limiter

In addition to alerting, gcaps generate metadata events about the analyzed network flows. These informations can be useful during investigations, but in some context they can quickly overflow the indexing capabilities of the Gcenter.
In order to reduce the amount of metadata while keeping most of the intersting information, it is possible to enable the following limiters. Use the hunting tool (Hunting > Metadata) to understand which kind of metadata should be optimized in priority.

DNS
Aggressivity level: 1
Disabled

HTTPS
Aggressivity level: 1
Disabled

HTTP
Aggressivity level: 1
Disabled

SMB
Aggressivity level: 1
Disabled

METADATA-01

- If necessary, for the first selected protocol (`DNS` (1), `HTTPS` (2), `HTTP` (3), `SMB` (4)):
- Select filtration level (field `Aggressivity level` item (10 to 13))
- Activate with the selector `Enabled -Disabled` item (5 to 8)
- Proceed to next protocol
- Validate with the `APPLY` button (9).

# 7.11 Logging out of the GCenter web interface

## 7.11.1 Introduction

This procedure describes how to log out of the GCenter web interface.

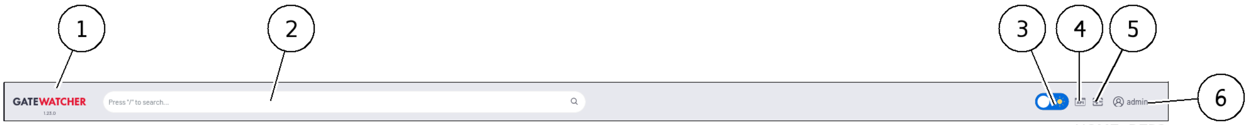
## 7.11.2 Prerequisites

- User: all users

## 7.11.3 Preliminary operations

- Accessing GCenter from your workstation (*Connection to the GCenter web interface via a web browser*).

## 7.11.4 Procedure



HOME_REP2

- In the GCenter interface, click on the current account button (6).
- Select the `Logout` command.
  The GCenter interface is closed and the login screen is displayed.

Chapter 8

# Use cases of the administrator level

## 8.1 Connecting to the GCenter web interface via a web browser

### 8.1.1 Introduction

This procedure describes connecting from a remote computer to the GCenter web interface via a web browser. This connection is the nominal way to access the web interface of the equipment.

### 8.1.2 Prerequisites

- User: all users

### 8.1.3 Preliminary operations

- Know the name of the GCenter or its IP address.
- Access GCenter from your workstation.

### 8.1.4 Procedure

On the remote PC:

- Open a web browser
- Enter the IP address or FQDN of the GCenter
- Validate.

  The GCenter login window is displayed.

- Enter the login name
- Enter the password
- Validate.

The GCenter graphical interface is displayed.

> **Note:**
>
> During the first login, it is necessary to change the password.
> Passwords must comply with the password policy (see *The `Password Policy` section of the `Accounts` submenu*).

## 8.2 Configuring the NDR

### 8.2.1 Introduction

#### 8.2.1.1 The `Assets and users tracking` and `Relationship tracking` functions

The NDR database stores information about:

- Alerts displayed in the `Alerts` dashboard (for more information on the dashboard, see *Web UI `Alerts` screen*)
- Alerts displayed in the `Alerts` dashboard (for more information on the dashboard, see *Web UI `Assets` screen*)
- The users displayed in the `Users` dashboard (for more information on the dashboard, see *Web UI `Users` screen*)

The `Assets and users tracking` and ` Relationship tracking` functions include:

| Function | Status | Description | See |
|---|---|---|---|
| `Assets and users tracking` | Activable | Synchronization between the NDR web UI's `Assets` and `Users` dashboards with the data available in Elasticsearch | See *Procedure to enable the `Assets and users tracking` and `Relationship tracking` functions*. |
| `Assets and users tracking` | Can disable | The NDR `Assets` and `Users` dashboards are disabled. Data is no longer stored in Elasticsearch. | See *Procedure to disable the `Assets and users tracking` and `Relationship tracking` functions*. |
| `Relationship tracking | Activable | synchronization between the NDR `Relations` dashboard in the web UI and the data available in Elasticsearch | See *Procedure to enable the `Assets and users tracking` and `Relationship tracking` functions*. |
| `Relationship tracking` | Can disable | The NDR `Relations` dashboard is disabled. Data is no longer stored in Elasticsearch. | See *Procedure to disable the `Assets and users tracking` and `Relationship tracking` functions*. |

The configuration interface is described in the *Web UI `Assets` screen*.

#### 8.2.1.2 Elasticsearch retention period

The retention time of Elasticsearch depends on the maximum space allocated (in Gb) to store the logs (see the *`Admin-GCenter-Configuration` screen of the legacy web UI*).
Therefore, the data retention period in Elasticsearch depends on the amount of logs generated by the GCaps.
The retention period of Elasticsearch can be changed: see the *Procedure to configure the Elasticsearch retention time*.

### 8.2.2 Prerequisites

- User : member of **Administrator** group

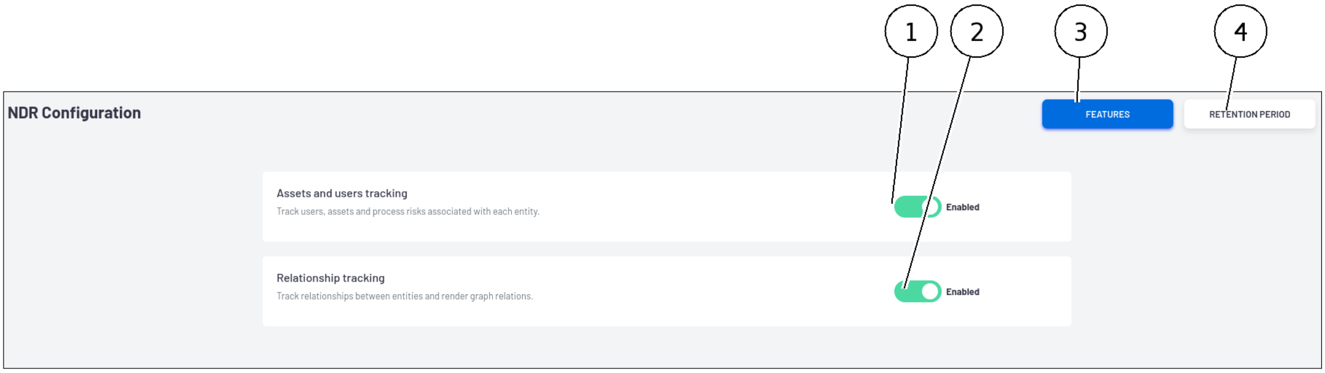
### 8.2.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

### 8.2.4 Procedure to access the `Data Exports` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `NDR configuration` command
  The `NDR configuration` window is displayed.

### 8.2.5 Procedure to enable the `Assets and users tracking` and `Relationship tracking` functions



Assets and users tracking
Track users, assets and process risks associated with each entity.
Enabled

Relationship tracking
Track relationships between entities and render graph relations.
Enabled

NDR-01

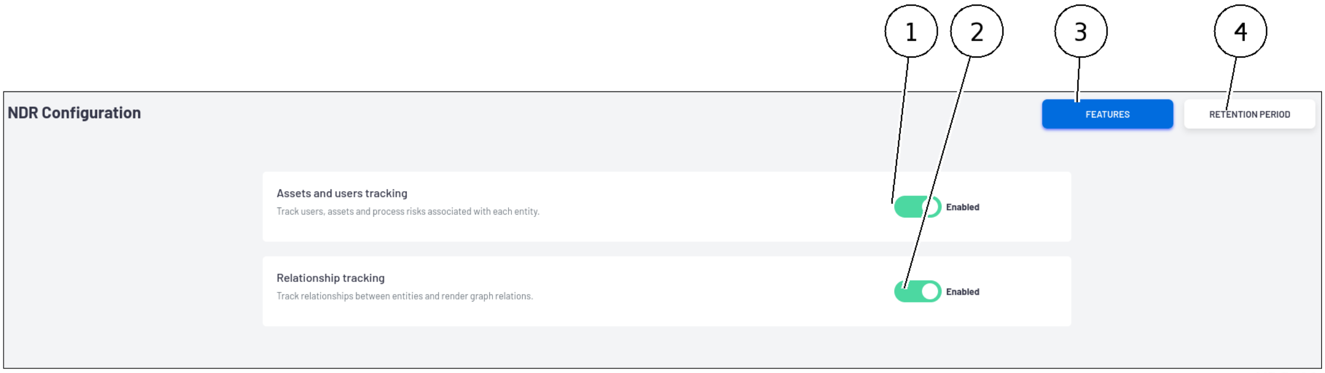
- Click on the `FEATURES` button (3).
- Use the `Assets and users tracking` selector (1) to enable tracking of active assets (`Assets`) and users (`users`).
  The functions visible by pressing the `Assets` and `users` buttons in the web UI are now accessible if the license enables it.

- Use the `Relationship tracking` selector (2) to enable tracking relations between active devices and view these relations.

  The functions visible by pressing the `Relations` button are now accessible if the license enables it.

---

### 8.2.6 Procedure to disable the `Assets and users tracking` and `Relationship tracking` functions



NDR Configuration

Assets and users tracking
Track users, assets and process risks associated with each entity.
Enabled

Relationship tracking
Track relationships between entities and render graph relations.
Enabled

NDR-01

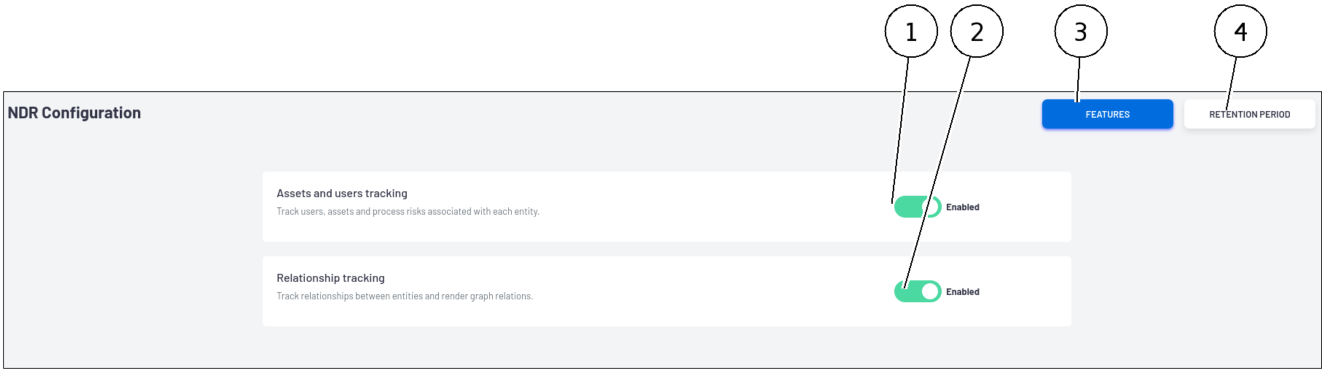
- Click on the `FEATURES` button (3).
- To disable the tracking of relations only, use the `Relationships tracking` selector (2).

  The functions visible by pressing the `Relations` button are now inaccessible.
- To disable all the functions of the `Assets and users tracking` (1) and `Relationship tracking` (2), use the `Assets and users tracking` selector (1).

  The functions visible by pressing the `Assets` and `users` buttons in the web UI are now inaccessible.

---

### 8.2.7 Procedure to configure the Elasticsearch retention time



NDR Configuration

Assets and users tracking
Track users, assets and process risks associated with each entity.
Enabled

Relationship tracking
Track relationships between entities and render graph relations.
Enabled

NDR-01

- Click on the `RETENTION PERIOD` button (4).
- Use the `Synchronize NDR boards with elasticsearch retention` selector to enable synchronizing NDR dashboards with data in Elasticsearch.
- Use the `Retention period` field to specify how long data such as alerts, users, and equipment should be retained on disk.

---

# 8.3 Administrating a GCap

## 8.3.1 Pairing a GCap with the GCenter

### 8.3.1.1 Introduction

The GCap probe must be associated to the GCenter in order to receive the network flow.
This procedure complements the procedure "Pairing a GCap with a GCenter" found in the GCap documentation.
This procedure describes the pairing between a GCap and a GCenter.
Pairing enables configuring the IPSec tunnel between the GCap and the GCenter.
The following operations must be performed:

- The *Preliminary operations*
- The *Procedure to display the IP address of the GCenter*
- The *Procedure to set the GCenter IP on the GCap*
- The *Procedure to access the `GCaps pairing and status` window for an administrator account*
- The *Procedure to set the compatibility mode on the GCap*
- The *Procedure to declare the GCap in the GCenter*
- The *Procedure to pair the GCap and the GCenter*

---

### 8.3.1.2 Prerequisites

- User : member of **Administrator** group

---

### 8.3.1.3 Preliminary operations

- Know the **Fully Qualified Domain Name FQDN** (FQDN).
  For example: 'nomdugcap.domaine.com' of the GCap and its IP address.
- Know the FQDN of the GCenter and its IP address.
- Check whether the date and time of the GCenter and the GCap match.

---

### 8.3.1.4 Procedure to display the IP address of the GCenter

- Connect to the GCap (see Procedure for connecting to the GCap via SSH).
- Connect to the GCenter and view the GCenter's network settings (see using the *`Network` command*).
- Obtain the IP address of the GCenter.

---

### 8.3.1.5 Procedure to set the GCenter IP on the GCap

- Apply the "Procedure for setting up the GCenter IP on the GCap" in the "Pairing a GCap with a GCenter" section of the GCAP documentation.

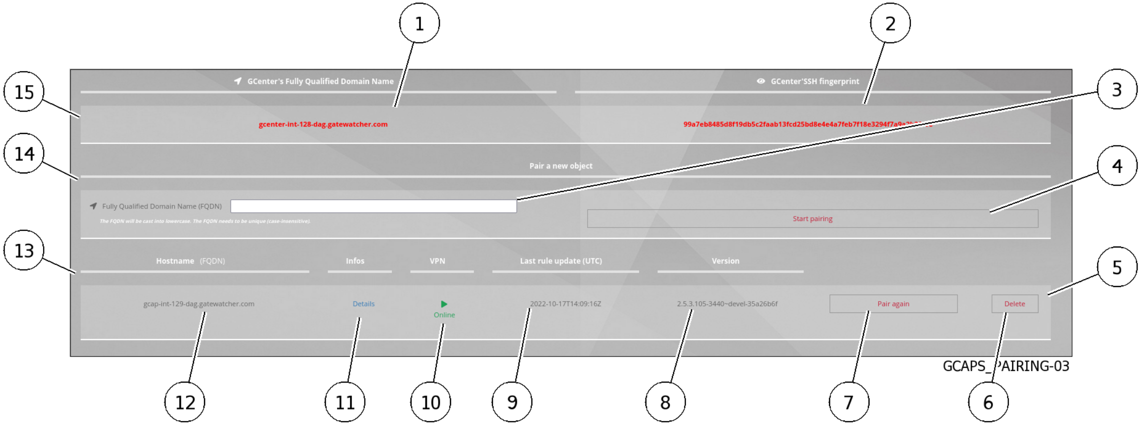
---

#### 8.3.1.6 Procedure to access the `GCaps pairing and status` window for an administrator account

- Connect to GCenter via a browser (refer to *Connecting to the GCenter web interface via a web browser*).
- In the navigation bar, successively click on:

- The `Admin` button
- The `GCaps pairing and status` command

  The `GCaps pairing and status` window is displayed.



GCenter's Fully Qualified Domain Name

GCenter'SSH fingerprint

gcenter-int-128-dag.gatewatcher.com

99a7eb8485d8f19db5c2faab13fcd25bd8e4e4a7feb7f18e3294f7a9a

Pair a new object

Fully Qualified Domain Name (FQDN)

The FQDN will be cast into lowercase. The FQDN needs to be unique (case-insensitive).

Start pairing

| Hostname (FQDN) | Infos | VPN | Last rule update (UTC) | Version | | |
|---|---|---|---|---|---|---|
| gcap-int-129-dag.gatewatcher.com | Details | ▶ Online | 2022-10-17T14:09:16Z | 2.5.3.105-3440~devel-35a26b6f | Pair again | Delete |

#### 8.3.1.7 Procedure to set the compatibility mode on the GCap

- To view the software version of the GCenter:

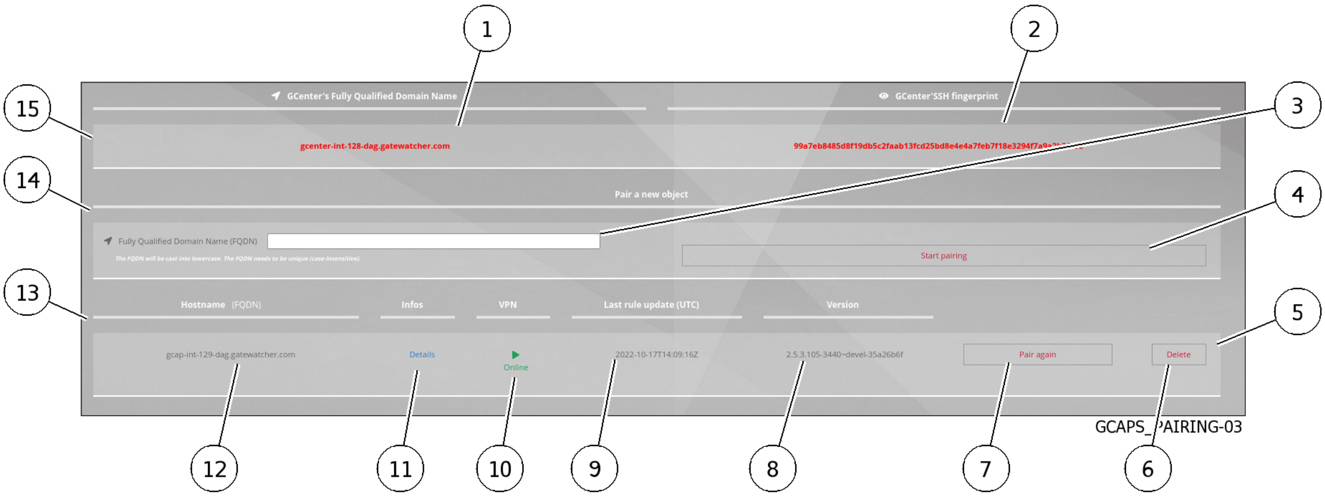
- Log into the GCenter and view the GCenter version number.
- View the GCenter version in the traditional UI web interface (see *Overview of the traditional WEB UI (legacy WEB UI)*).

  The information is located at the bottom left of the GCenter page (Example: GCenter v2.5.3.102-8370).

- To view the current compatibility mode between the GCap and the GCenter, log on to the GCap (see the procedure "Pairing between a GCap and a GCenter" in the GCAP documentation).

#### 8.3.1.8 Procedure to declare the GCap in the GCenter

The `GCaps pairing and status` window is displayed.



GCenter's Fully Qualified Domain Name

GCenter'SSH fingerprint

gcenter-int-128-dag.gatewatcher.com

99a7eb8485d8f19db5c2faab13fcd25bd8e4e4a7feb7f18e3294f7a9a

Pair a new object

Fully Qualified Domain Name (FQDN)

The FQDN will be cast into lowercase. The FQDN needs to be unique (case-insensitive).

Start pairing

Hostname (FQDN) | Infos | VPN | Last rule update (UTC) | Version
gcap-int-129-dag.gatewatcher.com | Details | ▶ Online | 2022-10-17T14:09:16Z | 2.5.3.105-3440~devel-35a26b6f | Pair again | Delete

- On the GCap:
- Obtain the FQDN (hostname.domain) of the GCap via the `show status` command.
- On the GCenter:
- Connect to the GCenter via a web browser in the `GCaps pairing and status` window.
- Enter the FQDN in the field (3).
- Select the profile to be applied to the GCap

> **Note:**
>
> It is possible to apply a predefined profile in advance (see the presentation of the *`Admin-GCaps pairing and status` screen of the legacy Web UI*) as well as changing it afterwards or modifying this profile to customise it (see the procedure *Change the default profile or customise the existing profile*).

- Press the `Start Pairing` button (4).
  The `SUCCESS` window is displayed showing the OTP (One Time Password).
  For example: pcmqsnf7iyo34ianzzi7gbgrr
- Copy the OTP.
- Click on the button `OK`.
  The GCap is now displayed in the GCap list (13).

---

#### 8.3.1.9 Procedure to pair the GCap and the GCenter

- On the GCap: perform the operations defined in the "Procedure for Pairing the GCap and GCenter" found in the GCAP documentation.
  After the message is displayed:

```
Resetting any previous GCenter pairing...
Generating IPSec certificates for the GCenter pairing...
Probing for GCenter SSH fingerprint...

Fingerprint for GCenter x is
e655bc02553e2291a486a32bdce3943a315f830de70b2c627c39884e80
1f08b2. Is it correct? (Y/N)
```

- On the GCenter, compare the GCenter fingerprint retrieved by the GCap in the CLI with the one present in the section `GCaps pairing..` under the text `GcenterSSH fingerprint` in the GCenter web interface on the web browser.
  - If the fingerprints are not identical:
  - Check the GCenter IP address and the value entered in the GCap
  - Check the GCap FQDN and the name entered in the GCenter
  - If they are identical, answer **Y** on the GCap and validate.
    After the message is displayed:

```
Pairing successful
```

- On the GCenter Web UI, check that the GCap is now \`Online (10) in the `GCaps pairing and status` menu page.
- On the GCap, this information is visible using the \`show status command (see the "Procedure for Pairing the GCap and GCenter" in the GCAP documentation.

**Astuce:**

The field `Paired on GCenter` takes:

- The value `Not paired` when the GCap is not paired with the GCenter
- The IP value of the GCenter when the GCap is paired with the GCenter

---

## 8.3.2 Re-pairing a GCap

### 8.3.2.1 Introduction

This procedure describes the re-pairing between a GCap and a GCenter.

**Avertissement:**

When re-pairing, the VPN tunnel between the GCap and the GCenter is momentarily interrupted.
This means that during this process, data is no longer sent from the GCap to the GCenter, however, the GCap retains the data in order to send it back once the tunnel is re-established.

---

### 8.3.2.2 Prerequisites

- User : member of **Administrator** group

---

### 8.3.2.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

---

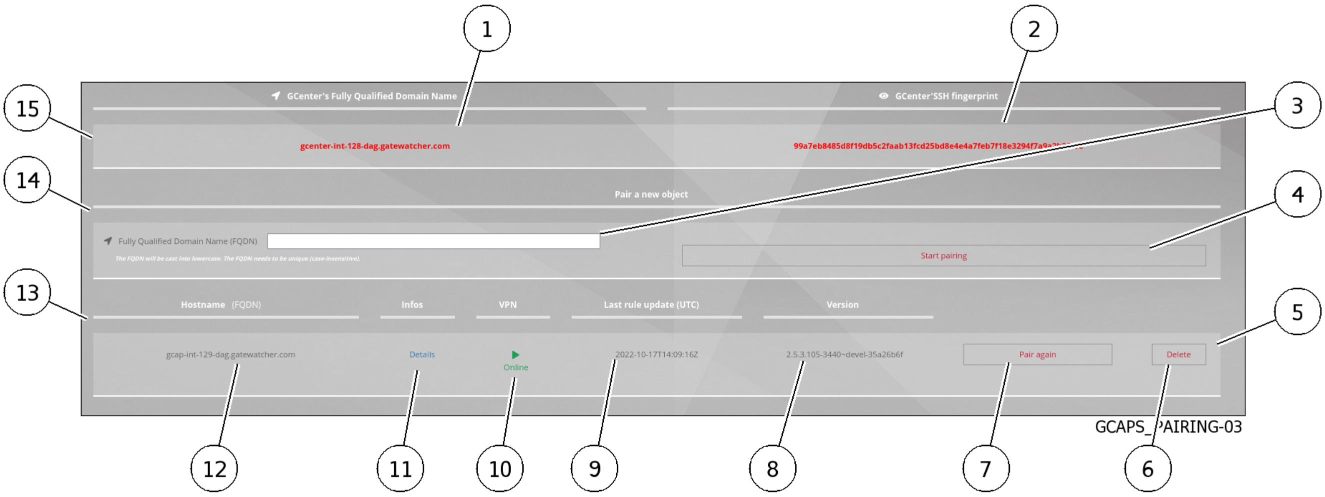
### 8.3.2.4 Procedure to access the `GCaps pairing and status` window for an administrator account

- In the navigation bar, successively click on:

- The `Admin` button
- The `GCaps pairing and status` command
  The `GCaps pairing and status` window is displayed.

---

#### 8.3.2.5 Procedure


GCenter's Fully Qualified Domain Name: gcenter-int-128-dag.gatewatcher.com

GCenter'SSH fingerprint: 99a7eb8485d8f19db5c2faab13fcd25bd8e4e4a7feb7f18e3294f7a9a

Pair a new object

Fully Qualified Domain Name (FQDN)

The FQDN will be cast into lowercase. The FQDN needs to be unique (case-insensitive).

| Hostname (FQDN) | Infos | VPN | Last rule update (UTC) | Version | | |
|---|---|---|---|---|---|---|
| gcap-int-129-dag.gatewatcher.com | Details | Online | 2022-10-17T14:09:16Z | 2.5.3.105-3440~devel-35a26b6f | Pair again | Delete |

- Click on the `Pair again` button (7).
  The following window is displayed:

```
Pair gcap-xxx again?
Warning: this will irreversibly drop the certificate and VPN configuration on the GCenter.
Do this only if you are sure you know what you are doing.
```

- Check the box `Are you sure?` before validating the action.
- Click on the `Pair again` button.
  The `SUCCESS` window is displayed showing the OTP (One Time Password).
- Copy the OTP.
- Click on the button `OK`.
  The GCap is now displayed in the GCap list (13).
- Continue the operations described in the procedure *Pairing a GCap with the GCenter*.

## 8.3.3 Change the default profile or customise the existing profile

### 8.3.3.1 Introduction

When the GCap was paired, a default profile was chosen.
The list of profiles and their characteristics are shown in *`Admin-GCaps pairing and status` screen of the legacy Web UI*.
The default profiles are sets of values for *Base variables* and *Files rules management*.

#### 8.3.3.2 Prerequisites

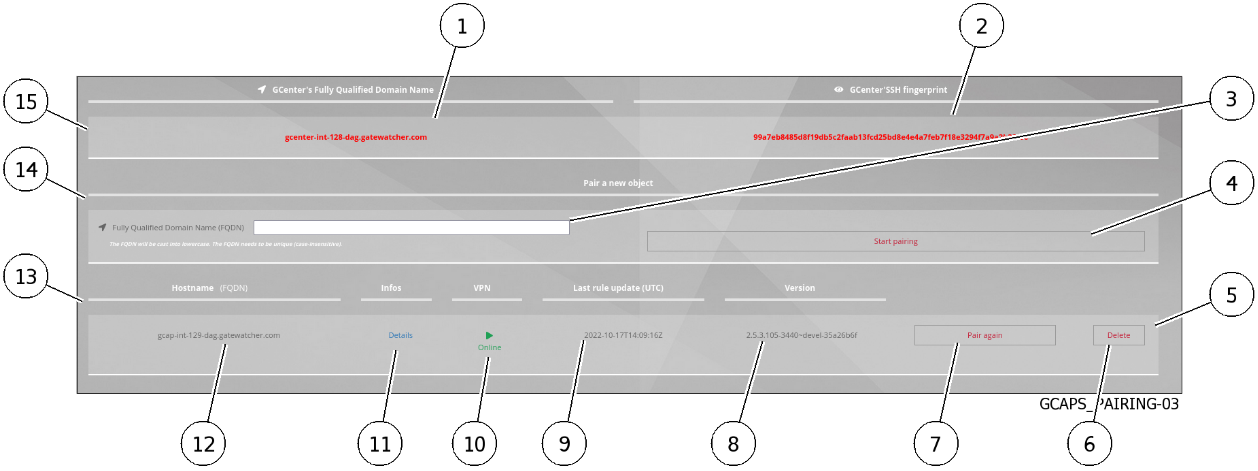
- User : member of **Administrator** group

#### 8.3.3.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

#### 8.3.3.4 Procedure to access to the `Data exports` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `GCaps pairing and status` command
  The `GCaps pairing and status` window is displayed.



GCenter's Fully Qualified Domain Name | GCenter'SSH fingerprint

gcenter-int-128-dag.gatewatcher.com | 99a7eb8485d8f19db5c2faab13fcd25bd8e4e4a7feb7f18e3294f7a9a

Pair a new object

Fully Qualified Domain Name (FQDN)

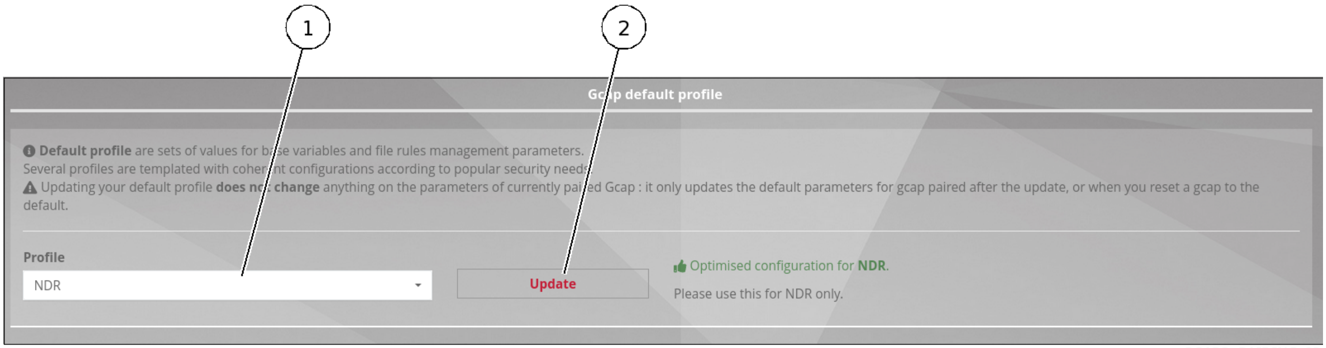
*The FQDN will be cast into lowercase. The FQDN needs to be unique (case-insensitive).*

Start pairing

| Hostname (FQDN) | Infos | VPN | Last rule update (UTC) | Version | | |
|---|---|---|---|---|---|---|
| gcap-int-129-dag.gatewatcher.com | Details | ▶ Online | 2022-10-17T14:09:16Z | 2.5.3.105-3440~devel-35a26b6f | Pair again | Delete |

GCAPS_PAIRING-03

#### 8.3.3.5 Procedure to change the default profile for future pairings



Gcap default profile

**Default profile** are sets of values for base variables and file rules management parameters.
Several profiles are templated with coherent configurations according to popular security needs.
⚠ Updating your default profile **does not change** anything on the parameters of currently paired Gcap : it only updates the default parameters for gcap paired after the update, or when you reset a gcap to the default.

Profile

NDR

Update

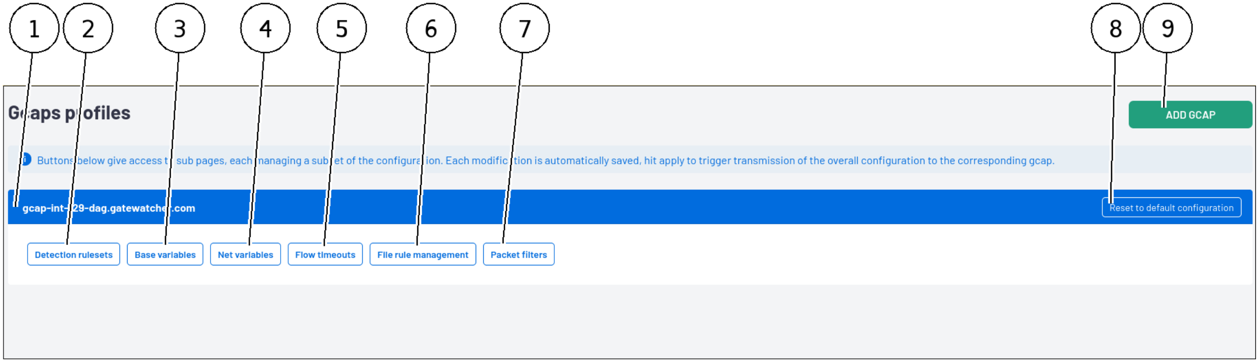
Optimised configuration for **NDR**.
Please use this for NDR only.

GCAPS_PAIRING-02

- Select a new profile (1) then click on the `Update` button (2).
  This new profile is now available for:
  - A new pairing
  - To the customisation functions available to the *Web UI `Config - Gcaps profiles` screen*.

#### 8.3.3.6 Procedure to customise the default profile

- Click on the `` `GCaps profiles` `` command from the `` `Config` `` menu of the web UI.
  The following screen is displayed.
  This screen enables configuring the GCap profiles.



Buttons below give access t sub pages, each managing a sub et of the configura ion. Each modific tion is automatically saved, hit apply to trigger transmission of the overall configuration to the corresponding gcap.

GCAP_00

- For a GCap (1), select an item (2 to 7) to customise the profile.
  The details of the customisation options are provided in the paragraph *Web UI `Config - Gcaps profiles` screen*.
- Click on the `` `Apply` `` button to save the changes and send them to the GCap.

> **Note:**
>
> The `` `Reset to default configuration` `` button (8) resets the configuration and loads the profile selected in the `` `GCaps pairing and status` `` screen.

## 8.3.4 Delete a GCap connected to the GCenter

#### 8.3.4.1 Introduction

It is possible to remove a **GCap** connected to the GCenter.
This will remove all data relating to the GCap pairing such as certificates and configuration.
Any logs (metadata, or alerts) generated in the past and indexed in Elasticsearch will not be modified.

#### 8.3.4.2 Prerequisites

- User : member of **Administrator** group

### 8.3.4.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

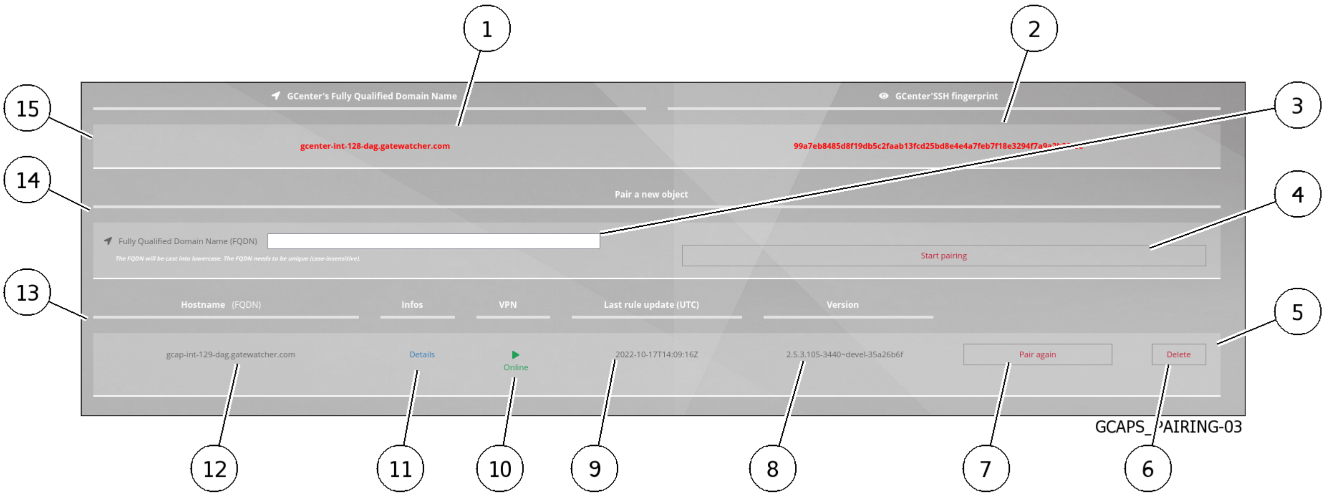
---

### 8.3.4.4 Procedure to access to the `GCaps pairing and status` window for an administrator account

- Connect to the GCenter via a browser (see procedure *Connection to the GCenter web interface via a web browser*).
- In the navigation bar, successively click on:
- The `Admin` button
- The `GCaps pairing and status` command
  The `GCaps pairing and status` window is displayed.

---

### 8.3.4.5 Procedure to delete



GCenter's Fully Qualified Domain Name

gcenter-int-128-dag.gatewatcher.com

GCenter'SSH fingerprint

99a7eb8485d8f19db5c2faab13fcd25bd8e4e4a7feb7f18e3294f7a9a

Pair a new object

Fully Qualified Domain Name (FQDN)

*The FQDN will be cast into lowercase. The FQDN needs to be unique (case-insensitive).*

Start pairing

| Hostname (FQDN) | Infos | VPN | Last rule update (UTC) | Version | | |
|---|---|---|---|---|---|---|
| gcap-int-129-dag.gatewatcher.com | Details | ▶ Online | 2022-10-17T14:09:16Z | 2.5.3.105-3440~devel-35a26b6f | Pair again | Delete |

- Click on the `Delete` button (6) of the GCap to be deleted (5).
  A window is displayed:

```
DELETE A GCAP

  Delete xx?

  Warning: this will aggressively delete various elements Gcenter-side.
  The changes are irreversible, databases will be lost.
  Do this only if you are sure you know what you are doing.
```

- Click on the `DELETE` button.

---

# 8.4 Managing the GCenter backup and restoration

## 8.4.1 Backup configuration

### 8.4.1.1 Introduction

The `` `Backup/Restore` `` section of the GCenter enables saving and restoring the data and configuration of the GCenter.
It is possible to:

- Schedule these backups
- Quantify the number of local backups on the GCenter
- Choose the storage location for the backups by selecting one of the three choices

This procedure describes how to configure the GCenter backup process.

For more information, see the *Overview of the backup and restoration*.
The graphical interface managing the **configuration** is described in the *`Admin-Backup/Restore - Configuration` screen of the legacy web UI*.
The graphical interface managing **usage** is described in the *`Admin-Backup/Restore - Operations` screen of the legacy web UI*.

| For | go to the |
|---|---|
| Accessing the `` `Backup configuration` `` screen | *Procedure to access the `Backup Configuration` screen* |
| Enabling backup scheduling | *Procedure to enable backup scheduling* |
| Backup configuration | *Procedure to setup the backup* |

### 8.4.1.2 Prerequisites

- User : member of **Administrator** group

### 8.4.1.3 Preliminary operations

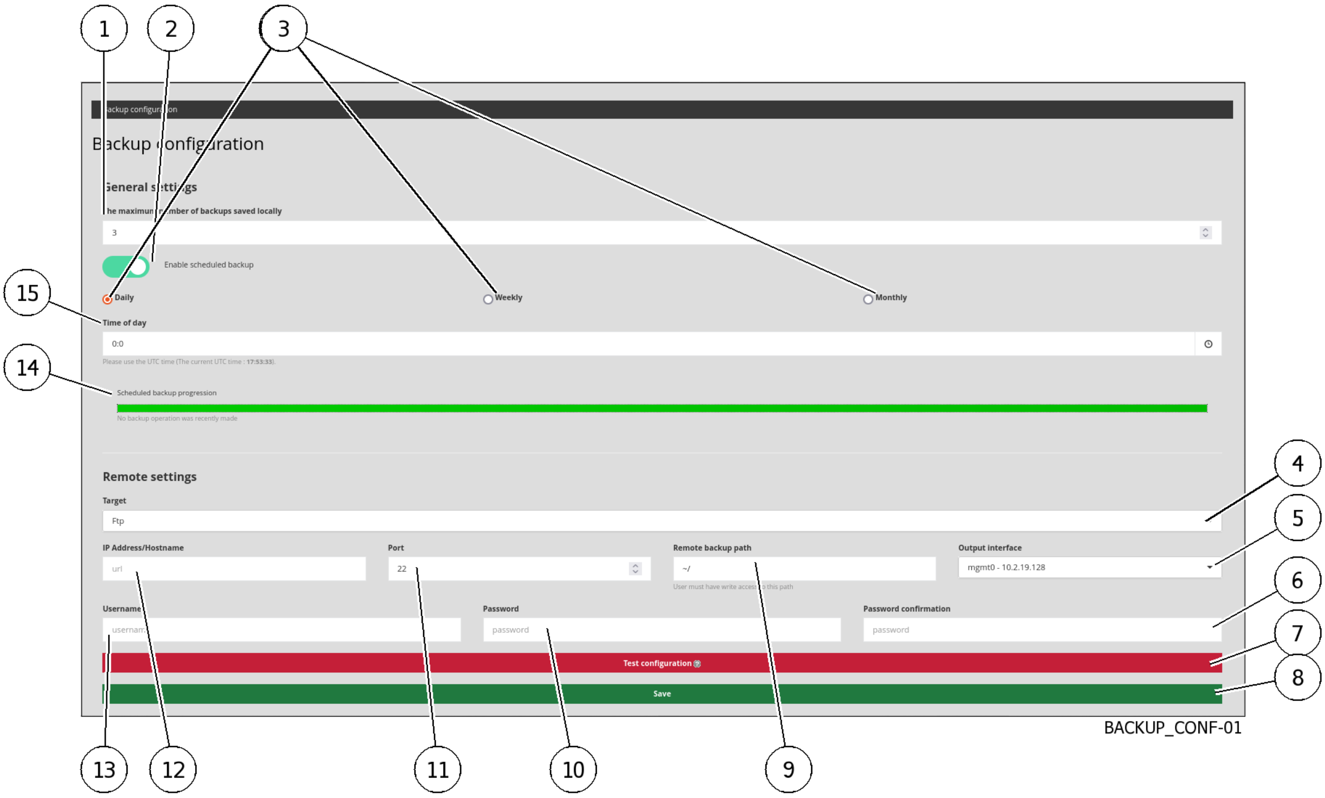
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

### 8.4.1.4 Procedure to access the `` `Backup Configuration` `` screen

In the navigation bar, successively click on:

- The `` `Admin` `` button
- The `` `Backup/Restore` `` submenu
- The `` `Configuration` `` command
  The `` `Backup configuration` `` window is displayed.

#### 8.4.1.5 Procedure to enable backup scheduling



Backup configuration

Backup configuration

General settings

The maximum number of backups saved locally: 3

Enable scheduled backup

● Daily ○ Weekly ○ Monthly

Time of day: 0:0

Please use the UTC time (The current UTC time : 17:53:33).

Scheduled backup progression

No backup operation was recently made

Remote settings

Target: Ftp

IP Address/Hostname: url

Port: 22

Remote backup path: ~/

User must have write access to this path

Output interface: mgmt0 - 10.2.19.128

Username: username

Password: password

Password confirmation: password

Test configuration

Save

- Use the `Enable scheduled backup` selector (2).

  The backup scheduler area becomes visible (marks 3, 14 and 15 are shown).
- Click on one of the buttons (3) defining the frequency (`Daily`, `Weekly`, `Monthly)`.
- Click on the `Time of day` field.

  A clock is displayed to indicate the hour.
- Select the hour.

  A new clock is displayed to show the minutes.
- Select the minute.
- Continue the setup according to the following procedure.

---

#### 8.4.1.6 Procedure to setup the backup

- Choose the storage location of the backups (4) by selecting one of the following three choices:
  - The `Local` choice: for a local only backup
  - The `SCP` choice: for a backup on a remote SCP server and for a local backup
  - The `FTP` choice: for a backup on a remote FTP server and for a local backup
- Enter the different parameters: for more details on these parameters, see the *`Admin-Backup/Restore - Configuration` screen of the legacy web UI*.
- Check the configuration using the `Test Configuration` button (7).
- Check the remote server to make sure the test file is present.
- Save the configuration using the `Save` button (8).

**Important:**

Note that it is necessary to change the passive port range of the FTP server to the following settings: [59000:59100]; so that the backup can be loaded correctly.

## 8.4.2 Backup

### 8.4.2.1 Introduction

Launching the backup can be:

- Automatic - managed by the scheduler
- Manual

This procedure describes how manual backup works.

For more information, see the *Overview of the backup and restoration*.

The graphical interface managing the **configuration** is described in the *`Admin-Backup/Restore - Configuration` screen of the legacy web UI*.

The graphical interface managing **usage** is described in the *`Admin-Backup/Restore - Operations` screen of the legacy web UI*.

### 8.4.2.2 Prerequisites

- User : member of **Administrator** group

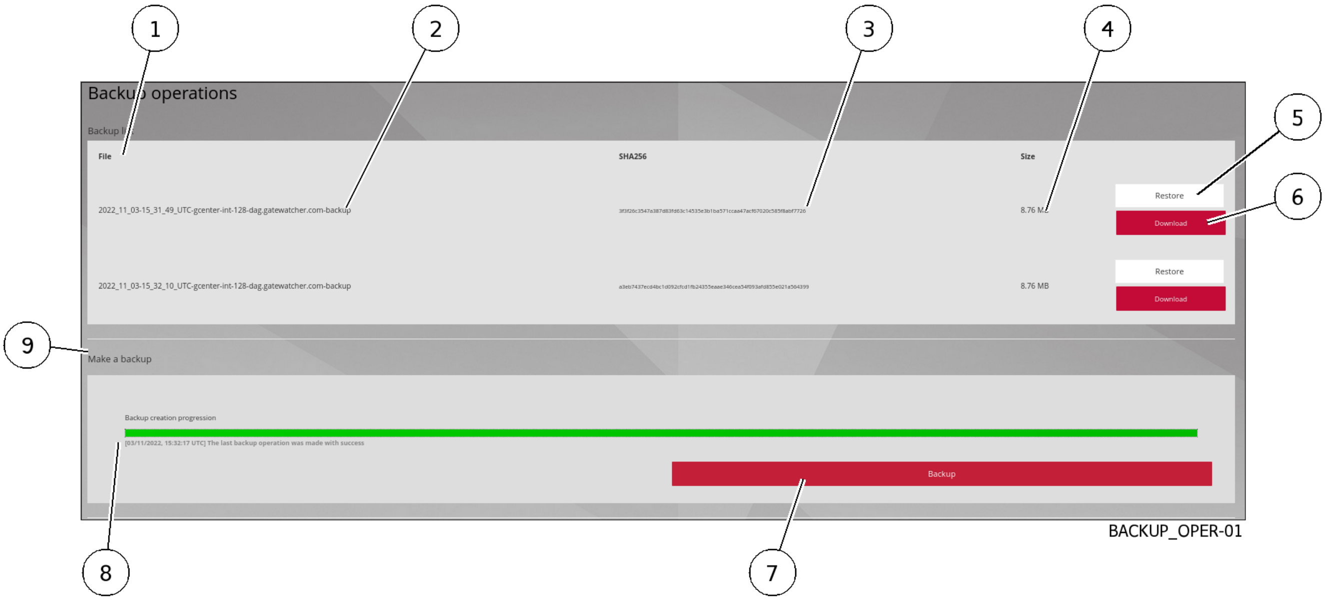
### 8.4.2.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).
- Configure the backup (see the procedure in *Backup configuration*).

### 8.4.2.4 Procedure to start a manual backup

In the navigation bar:

- Click on the `` `Admin` `` button
- Click on the `` `Backup/Restore` `` submenu
- Click on the `` `Operations` `` command



Backup operations

Backup list

| File | SHA256 | Size | |
|---|---|---|---|
| 2022_11_03-15_31_49_UTC-gcenter-int-128-dag.gatewatcher.com-backup | 3f3f26c3547a387d83fd63c14535e3b1ba571ccaa47acf67020c585f8abf7726 | 8.76 MB | Restore<br>Download |
| 2022_11_03-15_32_10_UTC-gcenter-int-128-dag.gatewatcher.com-backup | a3eb7437ecd4bc1d092cfcd1fb24355eaae346cea54f093afd855e021a564399 | 8.76 MB | Restore<br>Download |

Make a backup

Backup creation progression

[03/11/2022, 15:32:17 UTC] The last backup operation was made with success

Backup

BACKUP_OPER-01

- In the `Make a backup` section (9), click on the `Backup` button (7).
  The backup file will be displayed in the `Backup list` area (1) when the backup is complete.

## 8.4.3 Restoration

### 8.4.3.1 Introduction

The **administrator- Backup/Restore** section of the **GCenter** enables data backup and configuration restore.

> **Note:**
>
> In the case of a reinstallation or reset of the GCenter, it will be necessary to enter a license in order to access the `Restore` menu

This procedure describes how to restore a backup.

For more information, see the *Overview of the backup and restoration*.
The graphical interface managing the **configuration** is described in the *`Admin-Backup/Restore - Configuration` screen of the legacy web UI*.
The graphical interface managing **usage** is described in the *`Admin-Backup/Restore - Operations` screen of the legacy web UI*.

| For | go to the |
|---|---|
| Access to the restoration interface | *Procedure to access the restoration interface* |
| Follow the upgrade and hotfix paths | *Procedure to follow the upgrade and hotfix paths* |
| Restoring a backup to the same GCenter | *Procedure to restore a backup to the same GCenter* |
| Restoring a backup | *Procedure to restore a backup* |
| Restoring a backup to another blank GCenter | *Procedure to restore a backup to another blank GCenter* |

**Note:**

When restoring a backup, a number of services are automatically restarted/unavailable after the restore is marked as complete
The post-restoration time can be long (10~20 minutes) and during this time, access to the webui displays the message "502 bad gateway".

**Important:**

It is possible to restore a backup on a GCenter with a different IP configuration.
Before performing this operation, all network interfaces present on the source GCenter must be active and configured on the target GCenter.
Example:

- The source GCenter has two active interfaces (MGMT0 and VPN0).
- Both interfaces must be enabled and configured at the IP level on the target GCenter before performing the restore.

#### 8.4.3.2 Prerequisites

- User : member of **Administrator** group

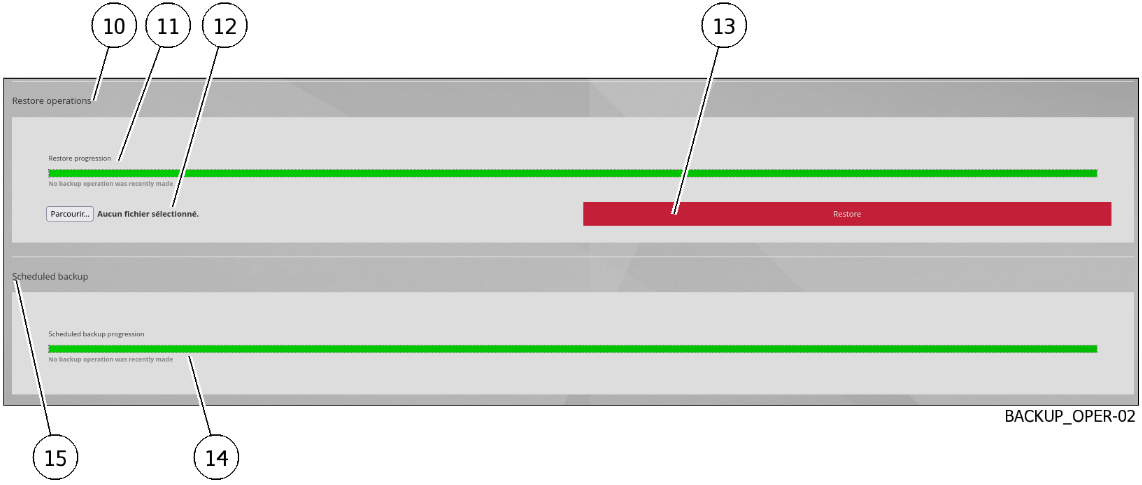
#### 8.4.3.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

#### 8.4.3.4 Procedure to access the restoration interface

In the navigation bar, successively click on:

- The `` `Admin` `` button
- The `` `Backup/Restore` `` submenu
- The `` `Operations` `` command
  The `` `Restore operations` `` section is available.



Restore operations

Restore progression

No backup operation was recently made

Aucun fichier sélectionné.

Scheduled backup

Scheduled backup progression

No backup operation was recently made

### 8.4.3.5 Procedure to follow the upgrade and hotfix paths

**Astuce:**

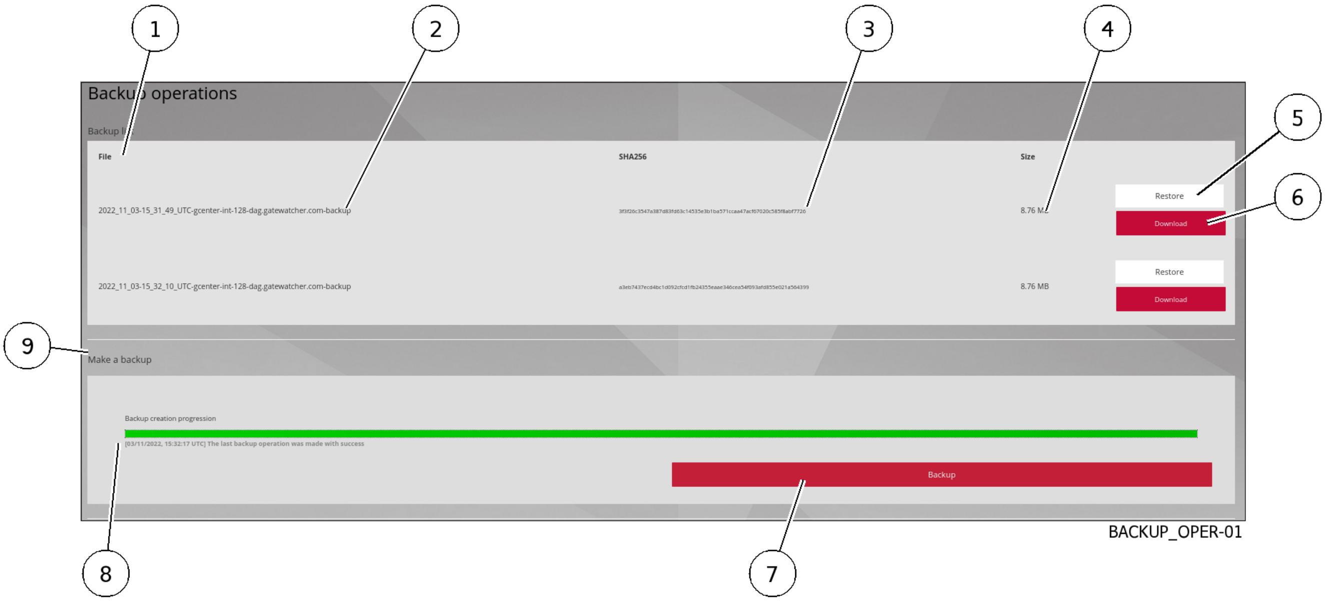
Since the upgrade and hotfix path is not specified in the backup name, it is imperative to set up a tracking of these paths.

To do this, when downloading or exporting the SCP or FTP of the backup:

- Create a tree structure indicating the current version of the GCenter (example: 2.5.3.102-XXXX-HFX)
- Store the downloaded or exported backup in this folder
- Modify the tree structure each time a version is upgraded or a hotfix is applied
- Use the backup in the directory of the GCenter version to be restored

#### 8.4.3.5.1 Procedure to restore a backup to the same GCenter

The `Backup operations` section is available.



Backup operations

Backup list

| File | SHA256 | Size |  |
|---|---|---|---|
| 2022_11_03-15_31_49_UTC-gcenter-int-128-dag.gatewatcher.com-backup | 3f3f26c3547a387d83fd63c14535e3b1ba571ccaa47acf67020c585f8abf7726 | 8.76 MB | Restore<br>Download |
| 2022_11_03-15_32_10_UTC-gcenter-int-128-dag.gatewatcher.com-backup | a3eb7437ecd4bc1d092cfcd1fb24355eaae346cea54f093afd855e021a564399 | 8.76 MB | Restore<br>Download |

Make a backup

Backup creation progression

[03/11/2022, 15:32:17 UTC] The last backup operation was made with success

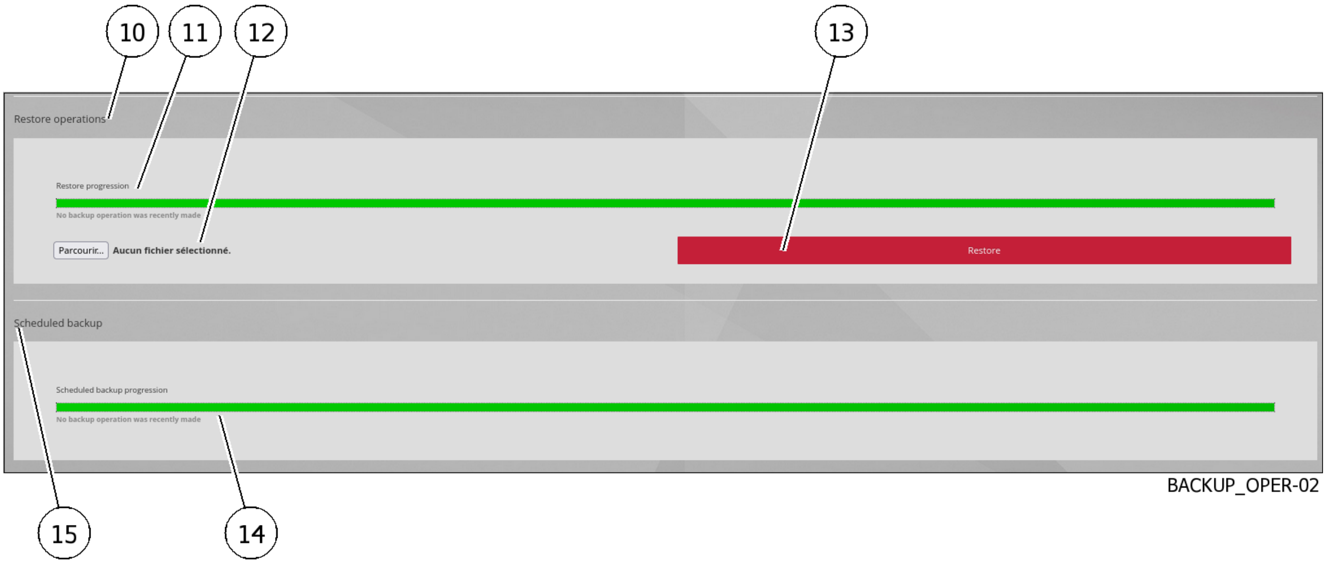
BACKUP_OPER-01

- In the `Backup list` area (1), click the `Restore` button (5) of the backup to be restored. After restarting the GCenter, the backup will be restored.

**Note:**

It is essential that the upgrade path be respected, as indicated in the *Procedure to follow the upgrade and hotfix paths*

#### 8.4.3.5.2 Procedure to restore a backup


10
11
12
13
Restore operations
Restore progression
No backup operation was recently made
Parcourir...
Aucun fichier sélectionné.
Restore
Scheduled backup
Scheduled backup progression
No backup operation was recently made
BACKUP_OPER-02
15
14

From the `Restore operation` page (10), described above:

- Click on the `Browse` button (12).
- Select the backup to restore.
- Click on the `Restore` button (13).
  After restarting the GCenter, the backup will be restored.

> **Note:**
>
> It is essential that the upgrade path be respected, as indicated in the *Procedure to follow the upgrade and hotfix paths*

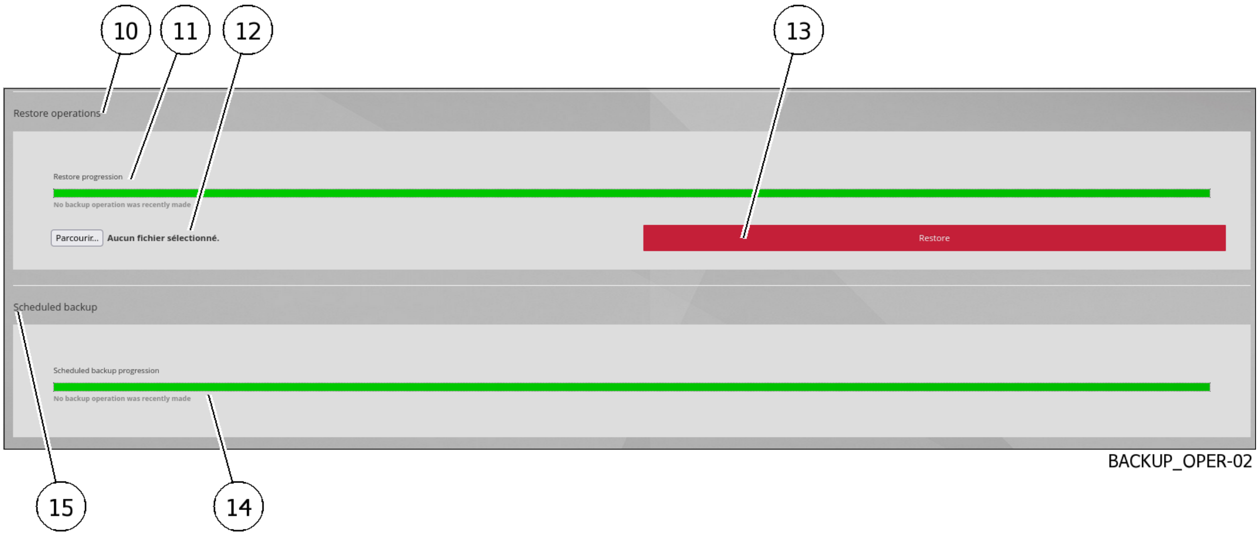
#### 8.4.3.5.3 Procedure to restore a backup to another blank GCenter

In the event of a GCenter replacement, it is mandatory to respect these criteria before restoring the backup:

- Reinstall the new GCenter along the same upgrade and hotfix path as the old GCenter.
- Name the new GCenter in the same way as the old GCenter (same FQDN).
- Configure the network section of the new GCenter, allowing access to the WebUi.
- Apply the licence to the new GCenter in order to access all the configurations. Until a license is entered, the WebUI is blocked on the license page.

Once the above steps are completed:

- Access the restoration page as described in the previous procedures



No backup operation was recently made

No backup operation was recently made

BACKUP_OPER-02

- Click on the `Parcourir` button (12)
- Select the backup to restore
- Click on the `Restore` button (13)
  After restarting the GCenter, the backup is restored.

---

# 8.5 Managing of the GCenter software

## 8.5.1 Configuring automatic update via GUM

### 8.5.1.1 Introduction

GUM (Gatewatcher Update Manager) is a tool that allows the management of updates (updates).
This procedure describes how to configure automatic update from:

- A server on the local network (choice `local`)
- A server on the Internet (choice `online`)

The GUI is described in *`Admin- GUM - Config` screen of the legacy web UI*.

**Note:**

If necessary, configure a proxy (refer to *Proxy Settings Configuration*).

---

### 8.5.1.2 Prerequisites

- User : member of **Administrator** group

---

#### 8.5.1.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).
- In the case of local mode, perform the local repository configuration prerequisites:

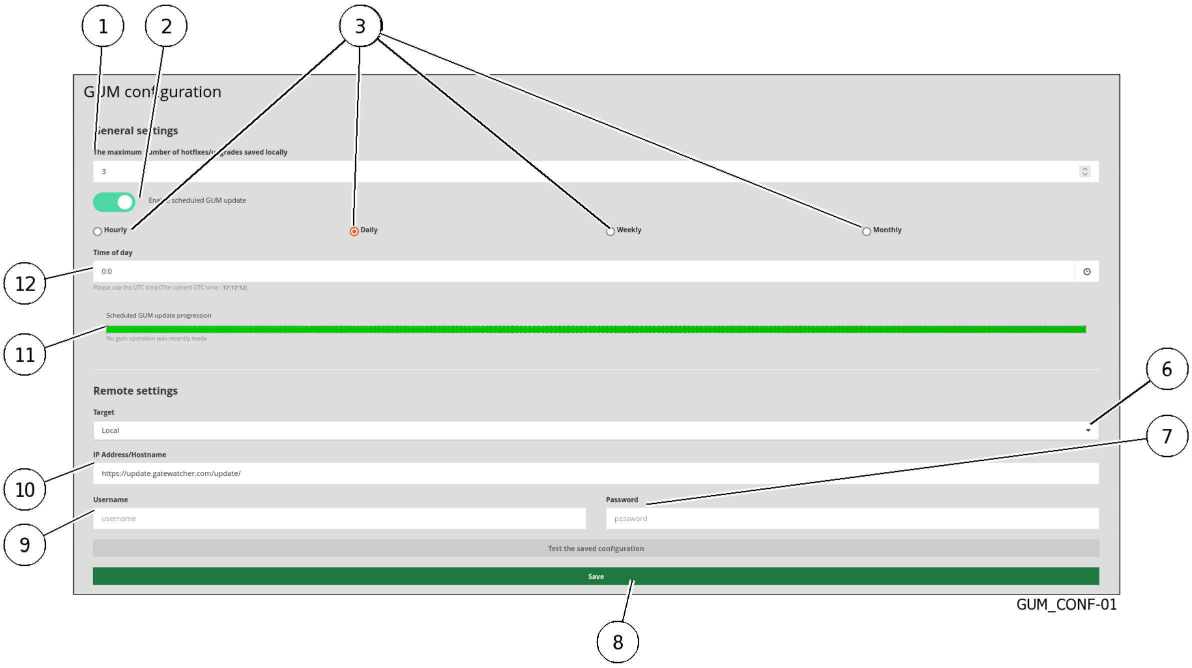
- The server must be reachable in HTTP on port 80
- Create the following tree structure: "2.5.3.10X/GCenter" according to the GCenter version (2.5.3.100 or 2.5.3.101)
- Retrieve the necessary gwp files (full.gwp for example) on *https://update.gatewatcher.com/update/*
- In "2.5.3.10X/gcenter", put the previously retrieved gwp file
- In "2.5.3.10X/gcenter", put a sha256s file that contains an entry "sha256sum NomDuFichier"

> **Note:**
>
> The 2.5.3.10X folder must be at the root of the HTTP server that was previously launched for the local mode to work.

---

#### 8.5.1.4 Procedure to access the `Configuration` screen

- From the navigation bar, click on the `Config` command of the `GUM` menu.
  The following screen is displayed:



GUM configuration

General settings

The maximum number of hotfixes/upgrades saved locally: 3

Enable scheduled GUM update

○ Hourly ● Daily ○ Weekly ○ Monthly

Time of day: 0:0

Please use the UTC time (The current UTC time : **17:17:12**).

Scheduled GUM update progression

No gum operation was recently made

Remote settings

Target: Local

IP Address/Hostname: https://update.gatewatcher.com/update/

Username: username

Password: password

Test the saved configuration

Save

GUM_CONF-01

- Perform the *Procedure to setup the Online Mode*
  or
  Perform the *Procedure to configure the local mode*

#### 8.5.1.5 Procedure to setup the Online Mode

- In `` `General settings` ``, click on the selector (2) `` `Enable scheduled GUM update` `` to activate automatic updates.

**Note:**

To maximize the effectiveness of updates, it is advisable to download these updates as soon as they appear on https://update.gatewatcher.com
To do this, connect to the site to view the time of creation of these updates and schedule the daily frequency and the time that follows that of the creation of packages.

**Note:**

The cti.gwp package is updated hourly on update.gatewatcher.com.
The other packages dga.gwp, malcore.gwp, sigflow.gwp are updated daily.
It is not possible to download the full.gwp file in automatic mode.

- Configure frequency of updates:

- Select the desired frequency (3) for automatic release of updates.
- Complete the programming information (12): the fields depend on the previous choice.

- In `` `Target` `` field (6), select the `` `Online` `` choice.

**Note:**

The `` `IP Address/Hostname` `` (10) field is automatically populated.

- Enter the login to connect to update.gatewatcher.com:
  - `` `Username` `` : field (9)
  - `` `Password` `` : field (7)
- Click the `` `Save` `` button (8).
- Finally, click on the `` `Test the saved configuration` `` button to validate that the GCenter can connect to the update site with the username entered
  The update automatically triggers at the frequency chosen in the configuration.

---

#### 8.5.1.6 Procedure to configure the local mode

Prerequisites:

- Have configured a web server connected to the internet (http repository type) accessible by GCenter
- Have automated the retrieval of update packages on this server from https://update.gatewatcher.com (example: python script)

**Note:**

For http repository configuration, see the *Presentation of GUM: dedicated module for managing updates*.

**Note:**

The cti.gwp package is updated hourly on update.gatewatcher.com
The other packages dga.gwp, malcore.gwp, sigflow.gwp are updated daily.
It is not possible to download the full.gwp file in automatic mode

**Note:**

To maximize the effectiveness of updates, it is advisable to download these updates as soon as they appear on https://update.gatewatcher.com
To do this, connect to the site to view the time of creation of these updates.
Consider the existing infrastructure to upload these files (+5GB) to the local repository.
Schedule the daily frequency and time following that of making available on the local depot.

- In `` `General settings` ``, click on the selector (2) `` `Enable scheduled GUM update` `` to activate automatic updates.
- Configure frequency of updates:
  - Select the desired frequency (3) for automatic release of updates.
  - Complete the programming information (12): the fields depend on the previous choice.
- In field (6) `` `Target` ``, select the `` `Local` `` choice.
- In field (10) `` `IP Address/Hostname` ``, enter the IP address or FQDN of the local repository address.
- Enter the login to connect to update.gatewatcher.com:
  - `` `Username` ``: field (9)
  - `` `Password` ``: field (7)
- Click the `` `Save` `` button (8).
- Finally, click on the `` `Test the saved configuration` `` button to validate that the GCenter can connect to the http repository.

  The update automatically triggers at the frequency chosen in the configuration.

---

### 8.5.2 Manual installation of an update of signatures and/or anti-viral engines (update)

#### 8.5.2.1 Introduction

This procedure describes the various options for updating the signature files of the solution's detection engines. The graphical interface is described in the paragraph *`Admin-GUM- Threat DB update` screen of the legacy web UI*.

**Note:**

Pour la mise à jour en mode online ou en mode local, voir la procédure de *Configuring automatic update via GUM*.

---

### 8.5.2.2 Prerequisites

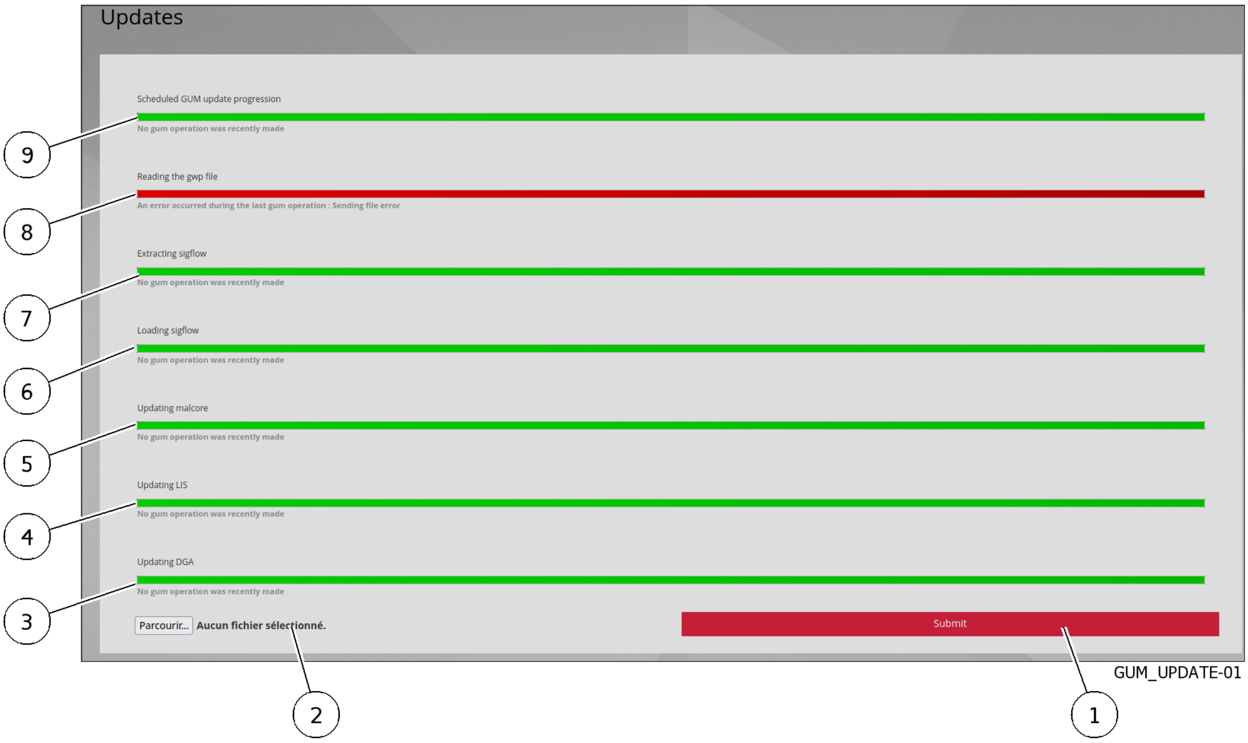
- User : member of **Administrator** group

### 8.5.2.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

### 8.5.2.4 Procedure to update the signature files in manual mode

After pressing the `Threat DB update` command from the `Admin-GUM` menu, the following screen is displayed.



No gum operation was recently made

An error occurred during the last gum operation : Sending file error

No gum operation was recently made

No gum operation was recently made

No gum operation was recently made

No gum operation was recently made

No gum operation was recently made

Aucun fichier sélectionné.

- Click on the `Browse` button (2) and select the previously downloaded package.

| To update the engine | Use the file |
|---|---|
| CTI | cti.gwp |
| dga | dga.gwp |
| malcore | malcore.gwp |
| sigflow | sigflow.gwp |
| all engines | full.gwp |

**Note:**

If the selected file is not an update file (update) but an upgrade file (upgrade) then um message is displayed as the following example.

```
An error occurred during the last gum operation : Error : Gwp file decryption error,␣
↪are you sure it is a TypeGwp.THREAT_DB_UPDATE ?
Please check your configuration/documentation. Otherwise, please contact the␣
↪Gatewatcher Support.
```

- Click on the button (1) `` `Submit` ``.
  The following message is displayed: `` `Upload in progress x%, please wait` ``.
  The message `` `Upload done` `` indicates that the file has been loaded.
- Wait for progress bars to indicate that the transaction has been successfully completed.
  The button indicates `` `Please wait` ``.
  When the button changes back to `` `Submit` ``, the engine update has been applied to GCenter and GCaps.

### 8.5.3 Installing a hotfix

#### 8.5.3.1 Introduction

A hotfix enables a given correction or modification to be applied without having to upgrade the entire solution.
All hotfix packages can be downloaded via our download platform: https://update.gatewatcher.com/hotfix
This procedure describes how to apply a hotfix.

#### 8.5.3.2 Prerequisites

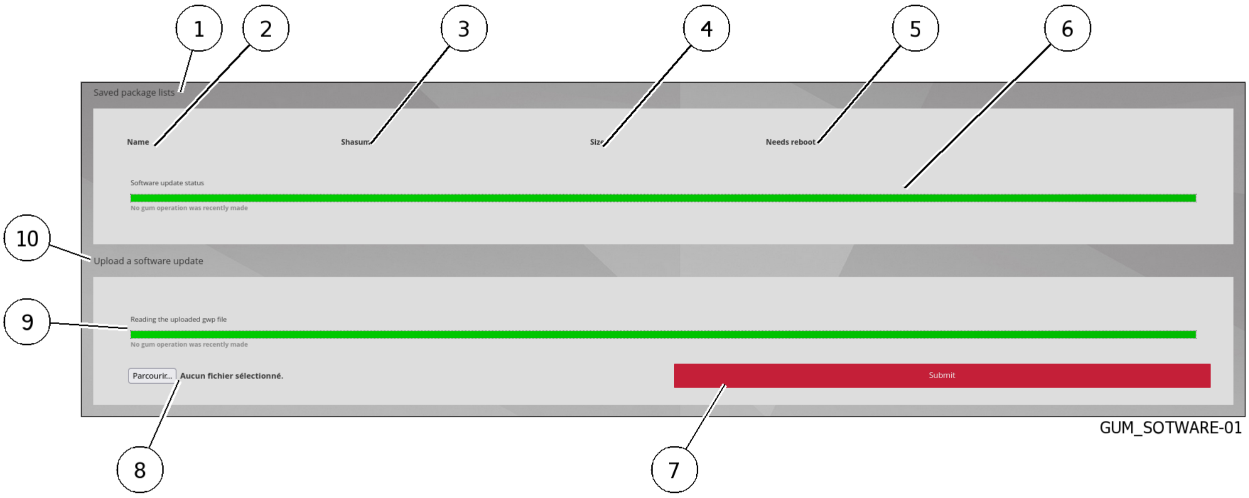
- User : member of **Administrator** group

#### 8.5.3.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).
- Read the release note of the desired version to see whether any other prerequisites are required.
- Download the upgrade package for the desired version from the site indicated in the introduction.

#### 8.5.3.4 Procedure to apply a hotfix

After pressing the `` `Software update` `` command from the `` `Admin-GUM` `` menu, the following screen is displayed.



No gum operation was recently made

No gum operation was recently made

GUM_SOTWARE-01

- Click on the `Browse` button (8) and select the previously downloaded package.
- Click on the `Submit` button (7).
- Once the package is present in the `Saved package list` area (1), click the `Apply` button.
- Wait until the progress bars indicate the operation was completed successfully.
  The hotfix was applied and the corrections are made on the GCenter.

> **Note:**
>
> In some cases, applying a hotfix may cause the web server to restart. This will make the web interface unavailable for a few minutes as specified in the release note.

## 8.5.4 Installing of an upgrade

### 8.5.4.1 Introduction

An upgrade enables a major version enhancement to be performed. This involves a reboot of the device concerned.
All packages can be found on the download platform: https://update.gatewatcher.com/upgrade
This procedure describes how to apply an upgrade.

| For | go to |
|---|---|
| Applying a GCenter upgrade | *Procedure to apply a GCenter upgrade* |
| Applying a GCap upgrade | *Procedure to apply a GCap upgrade* |

#### 8.5.4.2 Prerequisites

- User : member of **Administrator** group

---

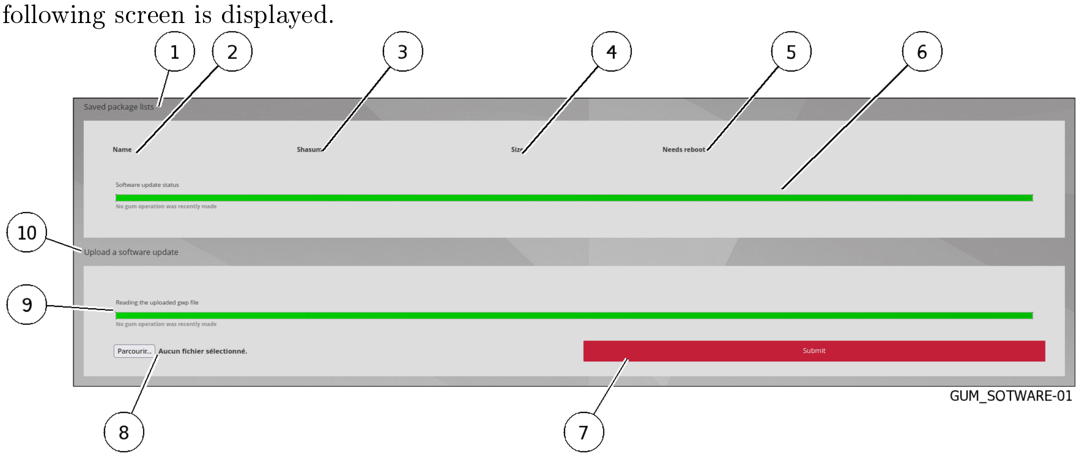
#### 8.5.4.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).
- Log on to the GCap CLI.
- Read the release note of the desired version to see whether any other prerequisites are required.
- Download the upgrade package for the desired version from the site (https://update.gatewatcher.com/upgrade).

---

#### 8.5.4.4 Procedure to apply a GCenter upgrade

- Click on the `` `Software update` `` command of the `` `Admin-GUM` `` menu.
  The following screen is displayed.



- Click on the `` `Parcourir` `` button (8) and select the previously downloaded package.

> **Note:**
>
> If the selected file is not an upgrade file (upgrade) but an update file (update) then um message is displayed as the following example.
>
> ```
> An error occurred during the last gum operation : Error : Gwp file decryption error,␣
> ↪are you sure it is a TypeGwp.SOFTWARE_UPDATE ? .
> Please check your configuration/documentation. Otherwise, please contact the␣
> ↪Gatewatcher Support.
> ```

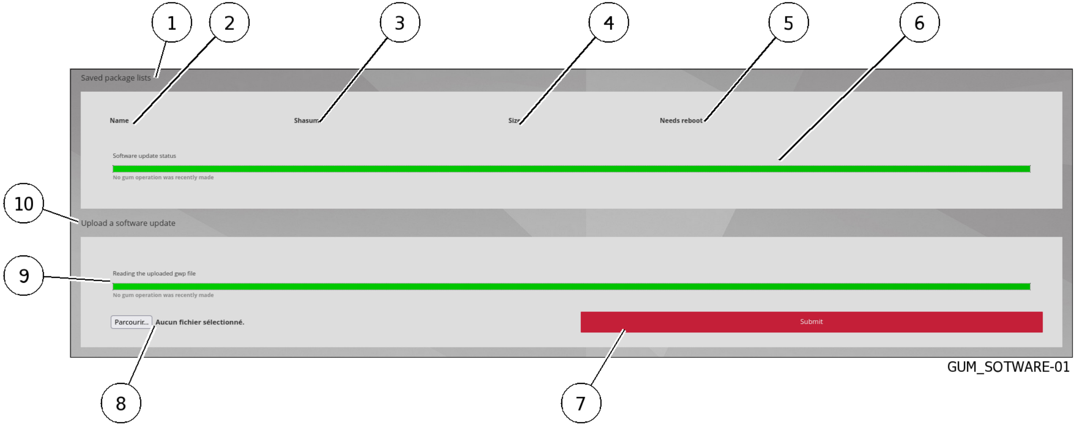
- Click on the `` `Submit` `` button (7).
- Once the package is present in the `` `Saved package list` `` area (1), click on the `` `Apply` `` button.
- Wait until the progress bars indicate the operation was completed.
- Restart the GCenter (see the procedure in the *`Restart` command*)
  After restarting, the GCenter loaded the desired version.

---

#### 8.5.4.5 Procedure to apply a GCap upgrade

- On the GCenter:

- Click on the `Software update` command of the `Admin-GUM` menu.
  The following screen is displayed.


1
2
3
4
5
6
Saved package lists
Name
Shasum
Size
Needs reboot
Software update status
No gum operation was recently made
10
Upload a software update
9
Reading the uploaded gwp file
No gum operation was recently made
Parcourir...
Aucun fichier sélectionné.
Submit
8
7

GUM_SOTWARE-01

- Click on the `Parcourir` button (8) and select the previously downloaded.
- Click on the `Submit` button (7).
- Once the package is present in the `Saved package list` area (1), click on the `Apply` button.
- Wait until the progress bars indicate the operation was completed.

- Log on to the GCap CLI:

- Run the `system upgrade list` command to retrieve the package name
- Run the command `system upgrade apply packagename` to start the upgrade.
  After restarting, the GCap loaded the desired version.

## 8.6 Administrating the GCenter

### 8.6.1 Export data to a SIEM via the syslog protocol

#### 8.6.1.1 Introduction

This procedure describes how to configure the connection to a SIEM via the syslog protocol.

**Note:**

See the presentation *Syslog servers*.
See the presentation of the exported data described in the paragraph *Data use*.
The graphical interface of the data export function is described in *`Admin-GCenter- Data exports` screen of the legacy web UI*.

### 8.6.1.2 Prerequisites

- User : member of **Administrator** group

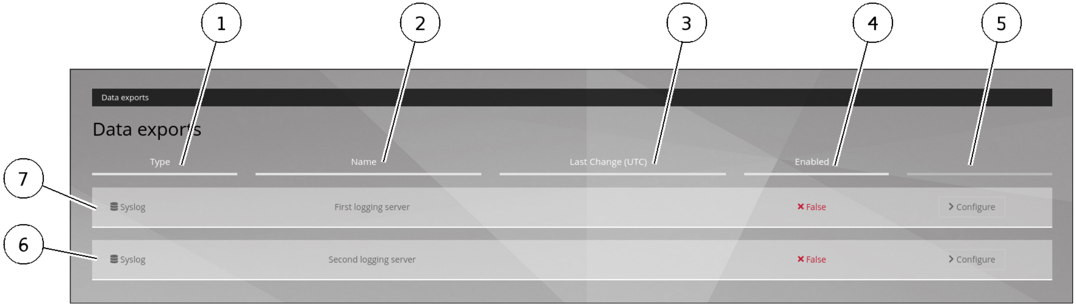
### 8.6.1.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

### 8.6.1.4 Procedure to access the `Data exports` window for an administrator account

- In the navigation bar, click successively on:
  - The `Admin` button
  - The `Gcenter` sub menu
  - The `Data exports` command

    The `Data exports` window is displayed.



Data exports

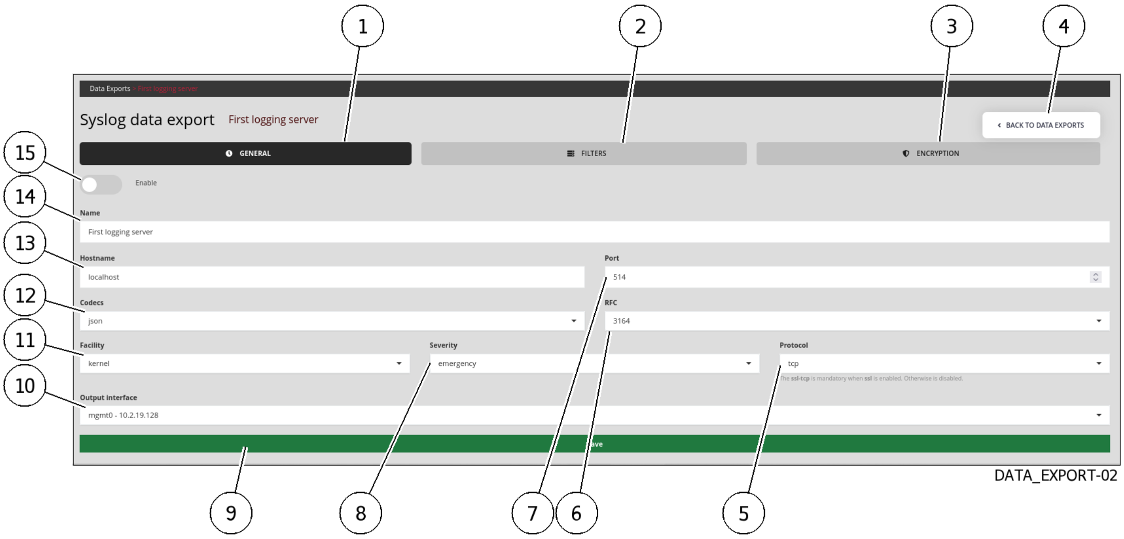
Data exports

| Type | Name | Last Change (UTC) | Enabled | |
|---|---|---|---|---|
| Syslog | First logging server | | ✗ False | > Configure |
| Syslog | Second logging server | | ✗ False | > Configure |

DATA_EXPORT-01

### 8.6.1.5 Procédure to set the export settings

- Click the `Configure` button (5) on one of the two connections (6 or 7) to be configured.
  The `Syslog data export` window opens.



Data Exports > First logging server

Syslog data export First logging server

Enable

Name: First logging server

Hostname: localhost

Port: 514

Codecs: json

RFC: 3164

Facility: kernel

Severity: emergency

Protocol: tcp

The ssl-tcp is mandatory when ssl is enabled. Otherwise is disabled.

Output interface: mgmt0 - 10.2.19.128

DATA_EXPORT-02

- Enter the parameters of the three tabs:
  - `GENERAL` (1)

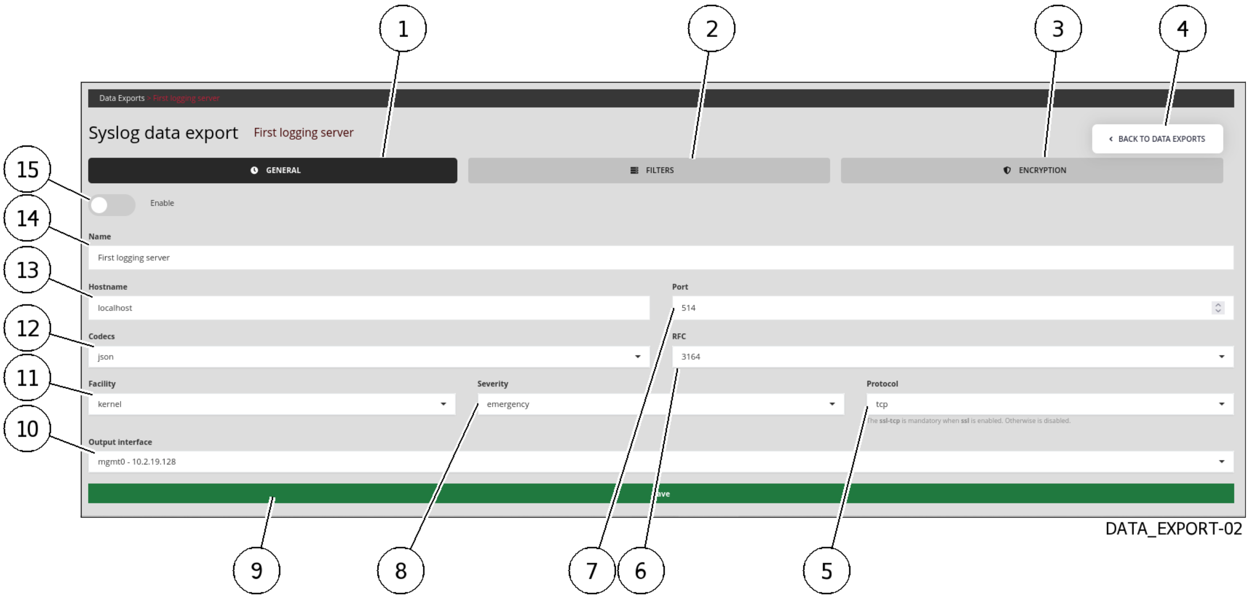
  - `FILTERS` (2)
  - `ENCRYPTION` (3)

  The list of items is detailed in *`Admin-GCenter- Data exports` screen of the legacy web UI*.

- Validate using the `Save` button (9).
- If necessary, set up the other connection (6 or 7).

---

#### 8.6.1.6 Procedure to activate


Data Exports > First logging server

Syslog data export First logging server

Enable

Name: First logging server

Hostname: localhost

Port: 514

Codecs: json

RFC: 3164

Facility: kernel

Severity: emergency

Protocol: tcp

The ssl-tcp is mandatory when ssl is enabled. Otherwise is disabled.

Output interface: mgmt0 - 10.2.19.128

- Use the `Enabled` selector (15) to enable export.
- Validate using the `Save` button (9).

---

## 8.6.2 Export data to a SPLUNK SIEM via the syslog protocol

### 8.6.2.1 Introduction

This procedure describes how to configure the connection to a SPLUNK SIEM remote server via the syslog protocol.

A Technological Add-On (TA) developed by Gatewatcher maps the data exported by the GCenter to the Splunk data models.

Configuring the connection between the GCenter and the SPLUNK SIEM requires the following steps:

- On the GCenter, configure data export:

- See *Procedure to setup the general settings*
- See *Procedure to setup the filtration parameters*
- See *Procedure to configure encryption settings*

- On the Splunk server, install the MT compatible with the GCenter version installed (example TA-gatewatcher-gcenter-v102 for GCenter V102) (see *Procedure to be performed on the SPLUNK server*)
- On the Splunk server, configure the reception of data from the GCenter and associate them to the TA (see *Procedure to configure the data receipt*)

**Note:**

It is possible to make changes to the MT files to adapt its behavior to specific needs and specific data models.
For this the details of the information is given in the *Composition of the Technological Add-On (TA)*.

**Note:**

See the presentation of *Syslog servers*.
See the presentation of the exported data described in *Data use*.
The graphical interface for the data export function is described in *`Admin-GCenter- Data exports` screen of the legacy web UI*.

### 8.6.2.2 Prerequisites

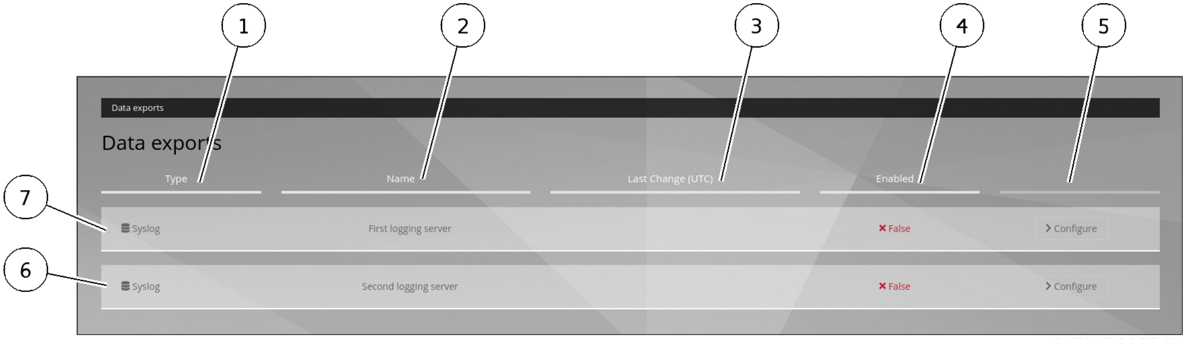
- User : member of **Administrator** group

### 8.6.2.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

### 8.6.2.4 Procedure to access to the `Data exports` window for an administrator account

- In the navigation bar, click successively on:
- The `Admin` button
- The `Gcenter` sub menu
- The `Data exports` command
  The `Data exports` window is displayed.



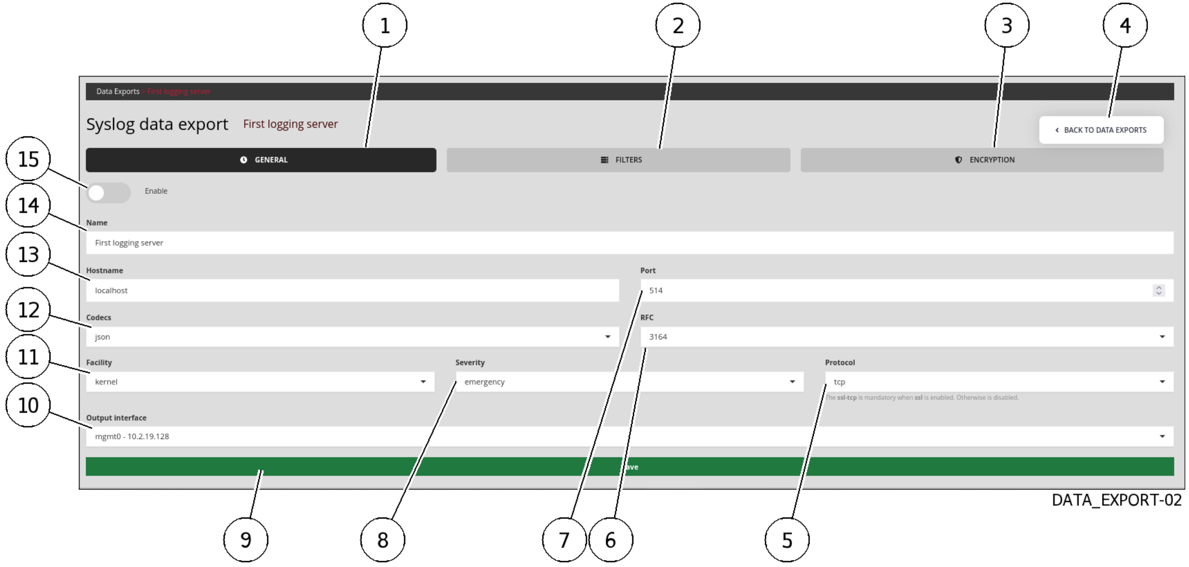
Data exports

| Type | Name | Last Change (UTC) | Enabled | |
|---|---|---|---|---|
| Syslog | First logging server | | ✖ False | › Configure |
| Syslog | Second logging server | | ✖ False | › Configure |

DATA_EXPORT-01

#### 8.6.2.5 Procedure to setup the general settings

- Click the `` `Configure` `` button (5) on one of the two connections (6 or 7) to be configured.
  The `` `Syslog data export` `` window opens.



Data Exports > First logging server

Syslog data export First logging server

Enable

Name: First logging server

Hostname: localhost

Port: 514

Codecs: json

RFC: 3164

Facility: kernel

Severity: emergency

Protocol: tcp

The ssl-tcp is mandatory when ssl is enabled. Otherwise is disabled.

Output interface: mgmt0 - 10.2.19.128

DATA_EXPORT-02

- Click on tab (1) `` `GENERAL` ``.

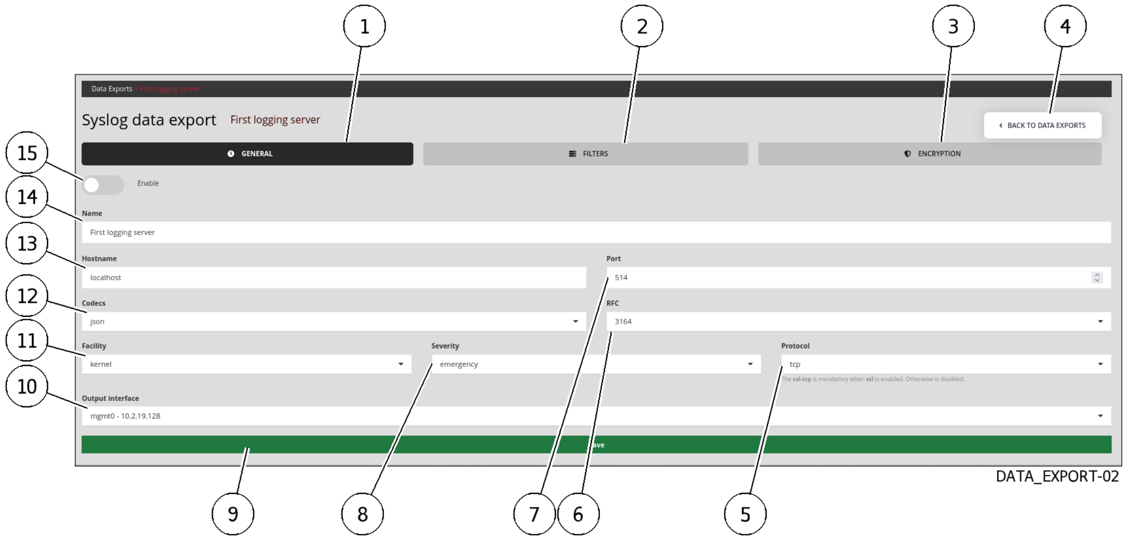
> **Note:**
>
> Values with a $VALUE format are context-specific and are noted as such so that they can be referenced in the rest of the documentation.

- Enter parameters using the following table:

| Item | Parameter | Description | Value |
|---|---|---|---|
| 15 | Enable | Activate this export pipeline | Activated |
| 14 | Name | Syslog export name | $SYSLOG_NAME |
| 13 | Hostname | Splunk server DNS name or IP address | $SPLUNK_IP |
| 7 | Port | Syslog flow destination port | $SYSLOG_PORT |
| 12 | Codecs | Codec used for export | JSON |
| 6 | RFC | Standard used by the codec | 3164 |
| 11 | Facility | Syslog header `` `facility` `` | default kernel; header will be removed by Splunk TA |
| 8 | Severity | Value of `` `severity` `` in Syslog header | emergency by default; the header will be deleted by the Splunk TA |
| 5 | Protocol | The transport protocol used. TCP or UDP can be used | $PROTOCOL |
| 10 | Output interface | Choose the GCenter interface used for Syslog export | $GCENTER_IFACE |

- Validate using button (9) `` `Save` ``.
  The following message indicates that the update has been completed: `` `Updated with success` ``.

### 8.6.2.6 Procedure to setup the filtration parameters


Data Exports > First logging server

Syslog data export First logging server

‹ BACK TO DATA EXPORTS

GENERAL | FILTERS | ENCRYPTION

Enable

Name: First logging server

Hostname: localhost

Port: 514

Codecs: json

RFC: 3164

Facility: kernel

Severity: emergency

Protocol: tcp

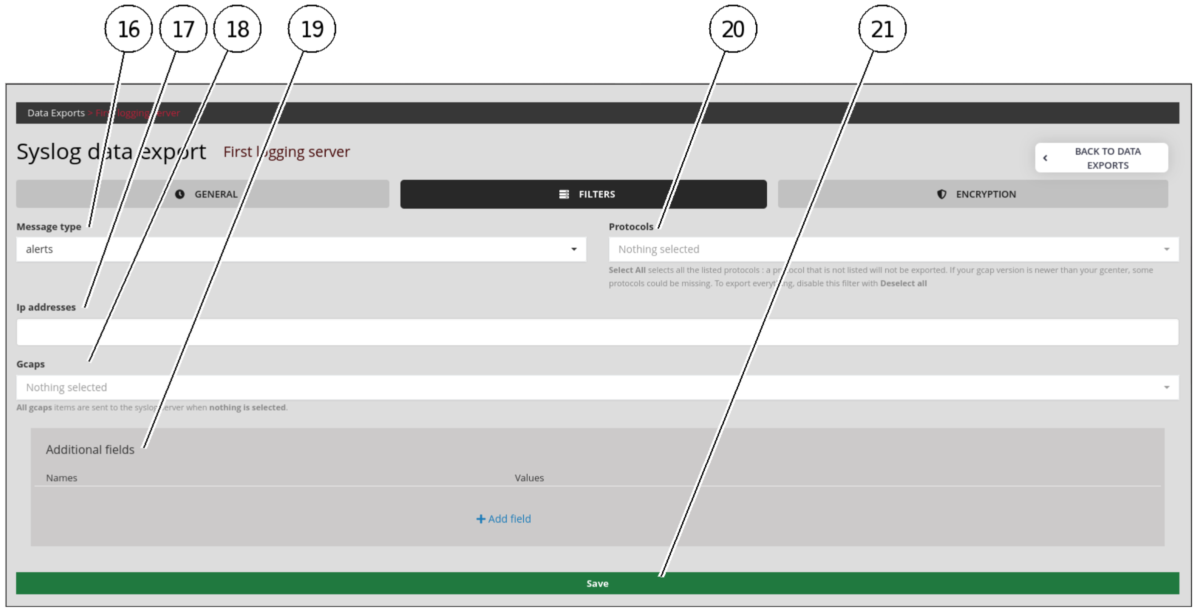
The **ssl-tcp** is mandatory when **ssl** is enabled. Otherwise is disabled.

Output interface: mgmt0 - 10.2.19.128

Save

DATA_EXPORT-02

- Click on the `FILTERS` tab (2).


Data Exports > First logging server

Syslog data export First logging server

‹ BACK TO DATA EXPORTS

GENERAL | FILTERS | ENCRYPTION

Message type: alerts

Protocols: Nothing selected

**Select All** selects all the listed protocols : a protocol that is not listed will not be exported. If your gcap version is newer than your gcenter, some protocols could be missing. To export everything, disable this filter with **Deselect all**

Ip addresses:

Gcaps: Nothing selected

**All gcaps** items are sent to the syslog server when **nothing is selected**.

Additional fields

| Names | Values |
|---|---|

+ Add field

Save

DATA_EXPORT-03

- Enter parameters using the following table:

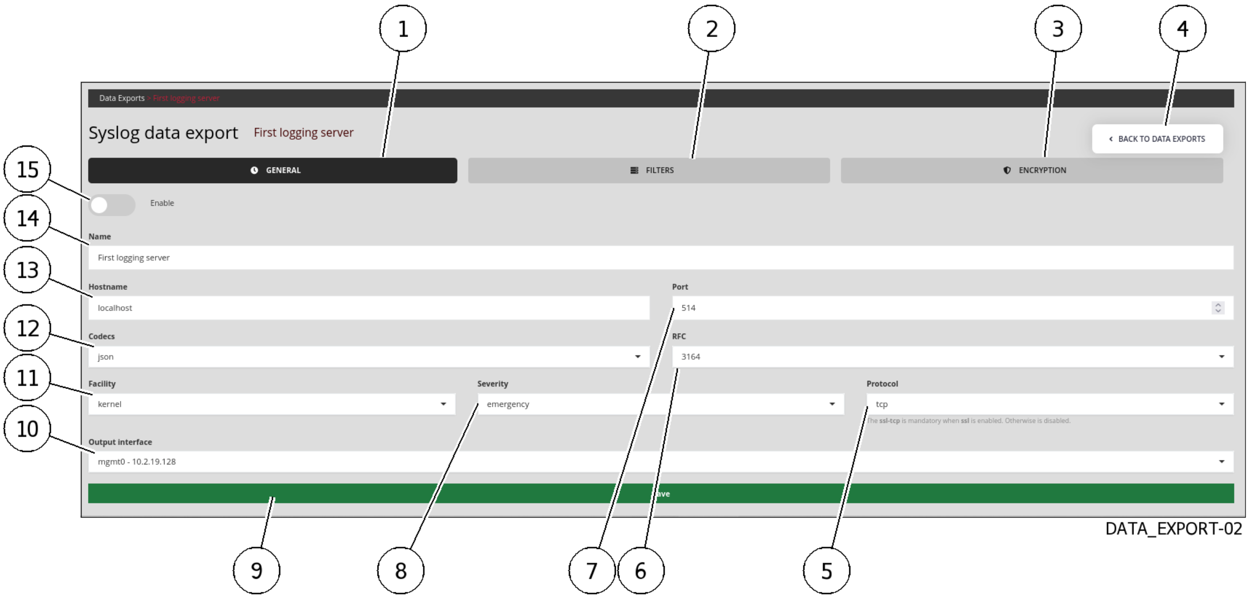
| Item | Parameter | Description |
|---|---|---|
| 16 | `` `Message type` `` | Defines the type of event to send to the remote server. Either only alerts or alerts and metadata (Example: alerts, all) |
| 17 | `` `Ip addresses` `` | Filter by **IP** or **networks**. By default, all data is sent to the remote server if the field is empty |
| 18 | `` `Gcaps` `` | Filter by **GCap**. By default, all GCap data paired to GCenter is sent to the remote server if nothing is selected (Example: GCap1, GCap2) |
| 19 | `` `Additional fields` `` | Adds additional fields in exported events.<br>A name (`` `Name` ``) and a description (`` `Values` ``) can be entered in this window.<br>In the case of using the idmef codec, this field is not supported. |
| 20 | `` `Protocols` `` | Selects protocols to export<br>(Example: dcerpc, dhcp, dnp3, dns, enip, ftp, http, http2, ikev2, krb5, mqtt, modbus, netflow, nfs, ntp, rdp, rfb, sip, smb, smtp, ssh, tftp and tls) |
| 21 | `` `Save` `` | Changes are only taken into account after pressing the `` `Save` `` button. |

**Note:**

`` `Select All` `` selects all the protocols listed: a protocol that is not selected will not be exported.
If GCap is newer than GCenter, some protocols may be missing.
To export everything, disable this filter with `` `Deselect all` ``.

- Validate using button (21) `` `Save` ``.
  The following message indicates that the update has been completed: `` `Updated with success` ``.

### 8.6.2.7 Procedure to configure encryption settings



Syslog data export First logging server

Enable

Name: First logging server

Hostname: localhost

Port: 514

Codecs: json

RFC: 3164

Facility: kernel

Severity: emergency

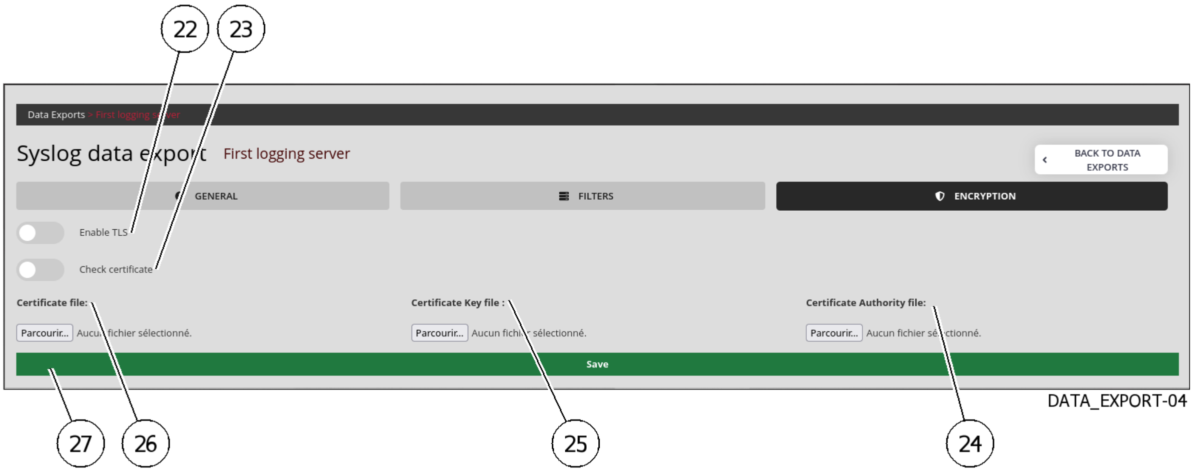
Protocol: tcp

The **ssl-tcp** is mandatory when **ssl** is enabled. Otherwise is disabled.

Output interface: mgmt0 - 10.2.19.128

DATA_EXPORT-02

- Click on the `ENCRYPTION` tab (3) .



Syslog data export First logging server

Enable TLS

Check certificate

Certificate file: Aucun fichier sélectionné.

Certificate Key file : Aucun fichier sélectionné.

Certificate Authority file: Aucun fichier sélectionné.

DATA_EXPORT-04

- Enter parameters using the following table:

| Item | Parameter | Description |
|---|---|---|
| 22 | `Enable TLS` | Enables Transport Layer Security (TLS). Disabled by default |
| 23 | `Check certificate` | Checks certificate validity when TLS is enabled. Disabled by default. |
| 24 | `Certificate file` | Add a certificate |
| 25 | `Certificate Key file` | Adds the associated key |
| 26 | `Certificate Authority file` | Adds CA file |
| 27 | `Save` | Changes are only taken into account after pressing the `Save` button |

- Validate using the `Save` button (27).
  The following message indicates that the update has been completed: `Updated with success`.

#### 8.6.2.7.1 Procedure to be performed on the SPLUNK server

- Contact Gatewatcher support to obtain the TA-gatewatcher-gcenter-v10x.spl file corresponding to the GCenter version.

> **Note:**
>
> Splunk TA is still in beta. The content of the TA is detailed at the end of this procedure so that administrators can adapt it to their needs.

The installation of the TA is done as for any Splunk app.

The steps are as follows (refer to the documentation for the used version of Splunk for more details):

- In the menu:

- Manage apps
- Install an application from a file
- Choose the TA Gatewatcher
- Click on the `` `Send` `` button

- In the Splunk app management menu, by clicking on "Show objects", you can access all the objects brought by the TA:
  - Field alias definition
  - The definition of eventtypes;
  - Associations between eventtype and tags;

  It is possible to enable/disable objects from this interface and modify their permissions (by default, the permissions are at "Global" - Read for everyone - Write for admins only).

---

#### 8.6.2.7.2 Procedure to configure the data receipt

The configuration of the data entry at the Splunk level must be consistent with the GCenter configuration.
In Splunk, the configuration will be done in Settings > Data > Data Entries > TCP/UDP
The following table summarizes the parameters to be applied for the data entry to work:

| Parameter | Description | Value |
|---|---|---|
| TCP/UDP | Transport protocol used | Must be equal to $PROTOCOL |
| Port | Listening port on Splunk server | Must be equal to $SYSLOG_PORT |
| Sourcetype | Sourcetype assigned to the received flow | gw:gcenter:101 |
| App Context | App in which the input.conf file relating to this entry will be placed | TA-gatewatcher-gcenter-101 |
| Index | Index in which the received data will be written | Depending on the data architecture, it is possible to use a specific index for Gatewatcher logs |

---

#### 8.6.2.7.3 Composition of the Technological Add-On (TA)

A Technological Add-On (TA), developed by Gatewatcher, maps the data exported by the GCenter to the Splunk data models.

**Note:**

Splunk TA is still in beta.
The content of the TA is detailed so that administrators can adapt it to their needs.

**Note:**

It is possible to make changes to the MT files to adapt its behaviour to specific needs and specific data models.
For this, the detail of the information is given in the paragraph (see *Composition of the Technological Add-On (TA)*).

The TA consists of the following files, placed in the *default* directory of the application.
Best practice is to create a *local* folder and keep the *default* folder intact (see Splunk documentation "how to edit a configuration file").

---

##### 8.6.2.7.3.1 File props.conf

**Note:**

This example is based on V101.

```
[gw:gcenter:101]
KV_MODE = json
MAX_TIMESTAMP_LOOKAHEAD = 31
```

The next section removes the Syslog headers and the *@version* field of elasticsearch, which is not used.

```
SEDCMD-gw-1-remove-header = s/^([^\{]+)//
SEDCMD-gw-2-remove-host = s/\"host\":\"[^\s"]+\",?//
SEDCMD-gw-3-remove-version = s/\"@version\":\"[^\s"]+\",?//
SEDCMD-gw-4-remove-trailing_comma = s/,}/}/
TIME_FORMAT = %Y-%m-%dT%H:%M:%S.%6N%Z
TIME_PREFIX = \"timestamp_detected\":\"
```

The following transformation calls *gw_force_host* in *transforms.conf*, and associates the name of the GCenter with the *host* field used by Splunk.

```
TRANSFORMS-host = gw_force_host
```

The following transformation calls the stanzas *sourcetype_** of *transforms.conf* in order to associate a sourcetype according to the engine that generated the log.

```
TRANSFORMS-override_sourcetype_engine = sourcetype_malcore,sourcetype_codebreaker,
↪sourcetype_sigflow,sourcetype_sigflow_alert
```

**Logs cannot exceed 65 kb, GCenters are in UTC.**

```
TRUNCATE = 65535
TZ = UTC
category = Splunk App Add-on Builder
pulldown_type = 1
```

The suite of *props.conf* allows to associate with each sourcetype field aliases and field evaluations to transform logs to match data models.

```
[gw:gcenter:101:sigflow:meta]
FIELDALIAS-gw_gcenter_101_sigflow_meta_src = src_ip AS src
FIELDALIAS-gw_gcenter_101_sigflow_meta_dest = dest_ip AS dest
FIELDALIAS-gw_gcenter_101_sigflow_meta_hash = fileinfo.sha256 AS file_hash
FIELDALIAS-gw_gcenter_101_sigflow_meta_alias_1 = tcp.tcp_flags AS tcp_flag
FIELDALIAS-gw_gcenter_101_sigflow_meta_alias_2 = netflow.pkts AS packets
FIELDALIAS-gw_gcenter_101_sigflow_meta_alias_3 = netflow.bytes AS bytes
FIELDALIAS-gw_gcenter_101_sigflow_meta_alias_4 = event_type AS app

FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_02 = http.status AS status
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_03 = http.length AS bytes
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_04 = http.url AS uri_query
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_05 = http.hostname AS url_domain
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_06 = http.http_content_type AS␣
↪http_content_type
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_07 = http.http_method AS http_
↪method
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_08 = http.http_user_agent AS http_
↪user_agent
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_09 = http.http_refer AS http_
↪referrer

EVAL-action = "allowed"
EVAL-protocol = "ip"
EVAL-transport = lower(proto)
EVAL-url = url_domain+uri_query

[gw:gcenter:101:sigflow:alert]
EVAL-action = "allowed"
EVAL-transport = low(proto)
FIELDALIAS-gw_gcenter_101_sigflow_alert_alias_1 = src_ip AS src
FIELDALIAS-gw_gcenter_101_sigflow_alert_alias_2 = dest_ip AS dest
FIELDALIAS-gw_gcenter_101_sigflow_alert_alias_3 = alert.signature AS signature
FIELDALIAS-gw_gcenter_101_sigflow_alert_alias_4 = alert.signature_id AS signature_id
FIELDALIAS-gw_gcenter_101_sigflow_alert_alias_5 = severity AS severity_id

[gw:gcenter:101:malcore]
FIELDALIAS-gw_gcenter_101_malcore_src = src_ip AS src
FIELDALIAS-gw_gcenter_101_malcore_dest = dest_ip AS dest
FIELDALIAS-gw_gcenter_101_malcore_hash = SHA256 AS file_hash
FIELDALIAS-gw_gcenter_101_malcore_alias_2 = src_ip AS src
FIELDALIAS-gw_gcenter_101_malcore_alias_3 = dest_ip AS dest
FIELDALIAS-gw_gcenter_101_malcore_alias_4 = filename AS file_name
FIELDALIAS-gw_gcenter_101_malcore_alias_5 = http_uri AS file_path
```

(suite sur la page suivante)

(suite de la page précédente)

```
FIELDALIAS-gw_gcenter_101_malcore_alias_6 = total_found AS signature_id

[gw:gcenter:101:codebreaker]
FIELDALIAS-gw_gcenter_101_codebreaker_src = src_ip AS src
FIELDALIAS-gw_gcenter_101_codebreaker_dest = dest_ip AS dest
FIELDALIAS-gw_gcenter_101_codebreaker_hash = SHA256 AS file_hash
FIELDALIAS-gw_gcenter_101_codebreaker_alias_4 = event_type AS category
```

#### 8.6.2.7.3.2 File transforms.conf

**Note:**

This example is based on V101.

The stanzas in this file are used by *props.conf*, and refer to fields indexed by Splunk, such as *host* or *sourcetype*.

```
[gw_force_host]
LOOKAHEAD = 65535
DEST_KEY = MetaData:Host
REGEX = \"GCenter\"\:\"([^\"]+)
FORMAT = host::$1

[sourcetype_malcore]
LOOKAHEAD = 65535
REGEX = \"type\"\:\"malcore\"
FORMAT = sourcetype::gw:gcenter:101:malcore
DEST_KEY = MetaData:Sourcetype

[sourcetype_codebreaker]
LOOKAHEAD = 65535
REGEX = \"type\"\:\"codebreaker\"
FORMAT = sourcetype::gw:gcenter:101:codebreaker
DEST_KEY = MetaData:Sourcetype

[sourcetype_sigflow]
LOOKAHEAD = 65535
REGEX = \"type\"\:\"suricata\"
FORMAT = sourcetype::gw:gcenter:101:sigflow:meta
DEST_KEY = MetaData:Sourcetype

[sourcetype_sigflow_alert]
LOOKAHEAD = 65535
REGEX = \"event_type\"\:\"alert\"
FORMAT = sourcetype::gw:gcenter:101:sigflow:alert
DEST_KEY = MetaData:Sourcetype
```

#### 8.6.2.7.3.3 File eventtype.conf

**Note:**

This example is based on V101.

This file allows to make associations between logs and events.
Events related to virus analysis of files (malcore):

```
[malcore_clean]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact="None"␣
↪code=0 )
description = An event that occurs when malcore analyses a file and none of the␣
↪engines detects a threat

[malcore_infected]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact="None"␣
↪code=1)
description = An event that occurs when malcore analyses a file and at least one of␣
↪the engines detects a threat
color = et_red

[malcore_suspicious]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact="None"␣
↪code=2)
description = An event that occurs when malcore analyses a file, none of the engines␣
↪detects a threat but at least one classifies the file as suspicious. Suspicious␣
↪files can be analysed lated by retroact, if enabled.
color = et_orange

[malcore_other]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact="None" NOT␣
↪code IN (0,1,2))
description = An event that occurs when malcore returns a code indicating an␣
↪exception or a failure in the analysis.
color = et_blue
```

Events related to the anti-viral re-analysis of "suspicious" files (retroact):

```
[retroact_clean]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact!="None"␣
↪code=0 )
description = An event that occurs when retroact analyses a file and none of the␣
↪engines detects a threat
color = et_blue

[retroact_infected]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact!="None"␣
↪code=2)
description = An event that occurs when retroact analyses a file and at least one of␣
↪the engines detects a threat
color = et_red
```

(suite sur la page suivante)

(suite de la page précédente)

```
[retroact_suspicious]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact!="None"␣
↪code=2)
description = An event that occurs when retroact analyses a file, none of the␣
↪engines detects a threat but at least one classifies the file as suspicious.␣
↪Suspicious files can be analysed lated by retroact, if enabled.
color = et_orange

[retroact_other]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact!="None" NOT␣
↪code IN (0,1,2))
description = An event that occurs when retroact returns a code indicating an␣
↪exception or a failure in the analysis.
color = et_blue
```

Event on enabling netflow logging on GCap:

```
[sigflow_netflow]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=netflow)
description = An event that occurs when sigflow generates a netflow event from a␣
↪network event.
```

GCap File Reconstruction Events:

```
[sigflow_fileinfo_stored]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=fileinfo fileinfo.stored=
↪"true")
description = An event that occurs when sigflow has performed a file reconstruction␣
↪and based on its ruleset, has stored it on disk to perform malcore analysis␣
↪afterwards.
color = et_blue

[sigflow_fileinfo_not_stored]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=fileinfo fileinfo.stored=
↪"false")
description = An event that occurs when sigflow has performed a file reconstruction␣
↪and based on its ruleset, has not stored it on disk.
```

Sigflow engine events can be of two types for each protocol:

- "meta" event: generation of metadata, obtained by enabling protocol logging on GCap.
- "Alert" event: generation of an alert, obtained by enabling protocol parsing on the GCap, and the correspondence between a flow and a sigflow rule.

```
[sigflow_meta_dcerpc]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=dcerpc)
description = An event that occurs when sigflow has reconstructed a dcerpc flow and␣
↪has logged its metadata.

[sigflow_alert_dcerpc]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=dcerpc)
description = An event that occurs when sigflow has reconstructed a dcerpc flow and␣
↪that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_dhcp]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=dhcp)
```

(suite sur la page suivante)

(suite de la page précédente)

```
description = An event that occurs when sigflow has reconstructed a dhcp flow and has logged its metadata.

[sigflow_alert_dhcp]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=dhcp)
description = An event that occurs when sigflow has reconstructed a dhcp flow and that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_dnp3]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=dnp3)
description = An event that occurs when sigflow has reconstructed a dnp3 flow and has logged its metadata.

[sigflow_alert_dnp3]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=dnp3)
description = An event that occurs when sigflow has reconstructed a dnp3 flow and that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_dns]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=dns)
description = An event that occurs when sigflow has reconstructed a dns flow and has logged its metadata.
priority = 2

[sigflow_alert_dns]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=dns)
description = An event that occurs when sigflow has reconstructed a dns flow and that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_ftp]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=ftp)
description = An event that occurs when sigflow has reconstructed a ftp flow and has logged its metadata.

[sigflow_alert_ftp]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=ftp)
description = An event that occurs when sigflow has reconstructed a ftp flow and that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_http]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=http)
description = An event that occurs when sigflow has reconstructed a http flow and has logged its metadata.

[sigflow_alert_http]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=http)
description = An event that occurs when sigflow has reconstructed a http flow and that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_ikev2]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=ikev2)
```

(suite sur la page suivante)

(suite de la page précédente)

```
description = An event that occurs when sigflow has reconstructed a ikev2 flow and␣
↪has logged its metadata.

[sigflow_alert_ikev2]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=ikev2)
description = An event that occurs when sigflow has reconstructed a ikev2 flow and␣
↪that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_krb5]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=krb5)
description = An event that occurs when sigflow has reconstructed a krb5 flow and␣
↪has logged its metadata.

[sigflow_alert_krb5]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=krb5)
description = An event that occurs when sigflow has reconstructed a krb5 flow and␣
↪that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_modbus]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=modbus)
description = An event that occurs when sigflow has reconstructed a modbus flow and␣
↪has logged its metadata.

[sigflow_alert_modbus_alert]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=modbus)
description = An event that occurs when sigflow has reconstructed a modbus flow and␣
↪that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_nfs]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=nfs)
description = An event that occurs when sigflow has reconstructed a nfs flow and has␣
↪logged its metadata.

[sigflow_alert_nfs]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=nfs)
description = An event that occurs when sigflow has reconstructed a nfs flow and␣
↪that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_ntp]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=ntp)
description = An event that occurs when sigflow has reconstructed a ntp flow and has␣
↪logged its metadata.

[sigflow_alert_ntp]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=ntp)
description = An event that occurs when sigflow has reconstructed a ntp flow and␣
↪that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_smb]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=smb)
description = An event that occurs when sigflow has reconstructed a smb flow and has␣
```

(suite sur la page suivante)

(suite de la page précédente)

```
↪logged its metadata.

[sigflow_alert_smb]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=smb)
description = An event that occurs when sigflow has reconstructed a smb flow and␣
↪that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_smtp]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=smtp)
description = An event that occurs when sigflow has reconstructed a smtp flow and␣
↪has logged its metadata.

[sigflow_alert_smtp]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=smtp)
description = An event that occurs when sigflow has reconstructed a smtp flow and␣
↪that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_ssh]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=ssh)
description = An event that occurs when sigflow has reconstructed a ssh flow and has␣
↪logged its metadata.

[sigflow_alert_ssh]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=ssh)
description = An event that occurs when sigflow has reconstructed a ssh flow and␣
↪that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_tftp]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=tftp)
description = An event that occurs when sigflow has reconstructed a tftp flow and␣
↪has logged its metadata.

[sigflow_alert_tftp]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=tftp)
description = An event that occurs when sigflow has reconstructed a tftp flow and␣
↪that one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_tls]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=tls)
description = An event that occurs when sigflow has reconstructed a tls flow and has␣
↪logged its metadata.

[sigflow_alert_tls]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=tls)
description = An event that occurs when sigflow has reconstructed a tls flow and␣
↪that one of its rules matched the content of this flow.
color = et_red

[sigflow_unknown_alert]
search = (sourcetype=gw:gcenter:101:sigflow* event_type=alert (app_proto=failed OR␣
↪NOT app_proto=*))
description = An event that occurs when sigflow has reconstructed the flow of an␣
```

(suite sur la page suivante)

(suite de la page précédente)

```
↪unknown protocol, and that one of its rules matched the content of this flow.
color = et_red

[sigflow_other]
search = (sourcetype=gw:gcenter:101:sigflow* type=suricata NOT event_type IN␣
↪(netflow,fileinfo,alert,dcerpc,dhcp,dnp3,dns,ftp,http,ikev2,krb5,modbus,nfs,ntp,
↪smb,smtp,ssh,tftp,tls))
description = An event that occurs when sigflow has reconstructed the flow of a␣
↪protocol not expected by this add-on.
color = et_blue
```

DGA DETECT Machine Learning Engine Events:

```
[dgadetect_clean]
search = (sourcetype=gw:gcenter:101:sigflow:meta dga_probability=* severity=0)
description = An event that occurs when dgadetect find that a domain name is not␣
↪suspicious (likeky not generated by a Domain Generation Algorithm). This eventtype␣
↪overlap the sigflow:dns:meta eventtype.

[dgadetect_suspicious]
search = (sourcetype=gw:gcenter:101:sigflow:meta dga_probability=* severity=1)
description = An event that occurs when dgadetect find that a domain name is␣
↪suspicious (likeky generated by a Domain Generation Algorithm).
color = et_red
```

Codebreaker Engine Events:

```
[codebreaker_shellcode_expoit]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_
↪type=shellcode state=Exploit)
description = An event that occurs when codebreaker has detected a shellcode.
color = et_red

[codebreaker_shellcode_suspicious]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_
↪type=shellcode state=Suspicious)
description = An event that occurs when codebreaker suspects it has potentially␣
↪detected a shellcode.
color = et_orange

[codebreaker_shellcode_other]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_
↪type=shellcode NOT state IN ('Suspicious','Exploit'))
description = An event that occurs when codebreaker returns a code indicating an␣
↪exception or a failure in its shellcode analysis.
color = et_blue

[codebreaker_powershell_expoit]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_
↪type=powershell state=Exploit)
description = An event that occurs when codebreaker has detected an exploit in a␣
↪powershell.
color = et_red

[codebreaker_powershell_suspicious]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_
```

(suite sur la page suivante)

(suite de la page précédente)

```
↪type=powershell state=Suspicious)
description = An event that occurs when codebreaker suspects it has potentially␣
↪detected a suspicious powershell.
color = et_orange

[codebreaker_powershell_other]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_
↪type=powershell NOT state IN ('Suspicious','Exploit'))
description = An event that occurs when codebreaker returns a code indicating an␣
↪exception or a failure in its powershell analysis.
color = et_blue
```

#### 8.6.2.7.3.4 File tags.conf

**Note:**

This example is based on V101.

This file allows you to tag events defined in *eventtype.conf*.
These tags will be used to bring these events into the Splunk *Common Information Model*.
Default associations are minimal and should be tailored to your use of data models.

```
[eventtype=malcore_clean]
attack = enabled
malware = enabled

[eventtype=malcore_infected]
attack = enabled
malware = enabled

[eventtype=malcore_suspicious]
attack = enabled
malware = enabled

[eventtype=malcore_other]
attack = enabled
malware = enabled

[eventtype=retroact_clean]
attack = enabled
malware = enabled

[eventtype=retroact_infected]
attack = enabled
malware = enabled

[eventtype=retroact_suspicious]
attack = enabled
```

(suite sur la page suivante)

(suite de la page précédente)

```
malware = enabled

[eventtype=retroact_other]
attack = enabled
malware = enabled

[eventtype=sigflow_netflow]
communicate = enabled
network = enabled

[eventtype=sigflow_fileinfo_stored]
communicate = enabled
network = enabled

[eventtype=sigflow_fileinfo_not_stored]
communicate = enabled
network = enabled

[eventtype=sigflow_meta_dcerpc]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_dcerpc]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_dhcp]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_dhcp]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_dnp3]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_dnp3]
attack = enabled
ids = enabled

[eventtype=dgadetect_clean]
communicate = enabled
network = enabled

[eventtype=dgadetect_suspicious]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_dns]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_dns]
attack = enabled
```

(suite sur la page suivante)

(suite de la page précédente)

```
ids = enabled

[eventtype=sigflow_meta_ftp]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_ftp]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_http]
communicate = enabled
network = enabled
web = enabled

[eventtype=sigflow_alert_http]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_ikev2]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_ikev2]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_krb5]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_krb5]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_modbus]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_modbus_alert]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_nfs]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_nfs]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_ntp]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_ntp]
```

(suite sur la page suivante)

(suite de la page précédente)

```
attack = enabled
ids = enabled

[eventtype=sigflow_meta_smb]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_smb]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_smtp]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_smtp]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_ssh]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_ssh]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_tftp]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_tftp]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_tls]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_tls]
attack = enabled
ids = enabled

[eventtype=sigflow_unknown_alert]
attack = enabled
ids = enabled

[eventtype=sigflow_other]
communicate = enabled
network = enabled

[eventtype=codebreaker_shellcode_expoit]
attack = enabled
malware = enabled

[eventtype=codebreaker_shellcode_suspicious]
```

(suite sur la page suivante)

(suite de la page précédente)

```
attack = enabled
malware = enabled

[eventtype=codebreaker_shellcode_other]
attack = enabled
malware = enabled

[eventtype=codebreaker_powershell_expoit]
attack = enabled
malware = enabled

[eventtype=codebreaker_powershell_suspicious]
attack = enabled
malware = enabled

[eventtype=codebreaker_powershell_other]
attack = enabled
malware = enabled
```

### 8.6.3 Export data to a ETL Logstash via the syslog protocol

#### 8.6.3.1 Introduction

This procedure describes how to configure the connection to Logstash.
A pipeline developed by Gatewatcher makes it possible to retrieve the JSON content of the exported logs so that it can then be manipulated as desired with the Logstash filters.
Configuring the connection between the GCenter and the Logstash ETL requires the following steps:

- On the GCenter, configure data export:
- See *Procedure to setup the general parameters*
- See *Procedure to setup the filtration parameters*
- See *Procedure to configure encryption settings*
- On the Logstash server, configure the flow receiving pipeline from the GCenter (see *Procedure to be performed on the server*)

**Note:**

See the presentation of *Syslog servers*.
See the presentation of the exported data described in *Data use*.
The graphical interface for the data export function is described in *`Admin-GCenter- Data exports` screen of the legacy web UI*.

#### 8.6.3.2 Prerequisites

- User : member of **Administrator** group

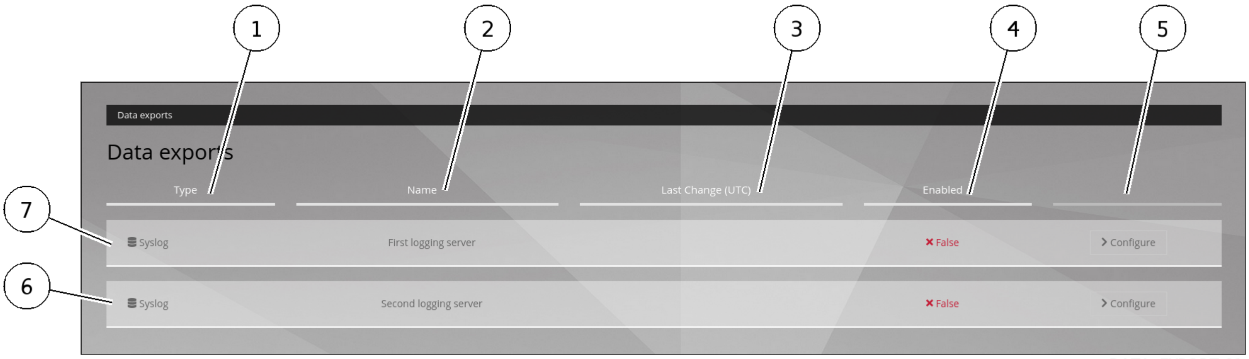
#### 8.6.3.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

#### 8.6.3.4 Procedure to access the `Data exports` window for an administrator account

- In the navigation bar, click successively on:
- The `Admin` button
- The `Gcenter` sub menu
- The `Data exports` command
  The `Data exports` window is displayed.

#### 8.6.3.5 Procedure to setup the general parameters



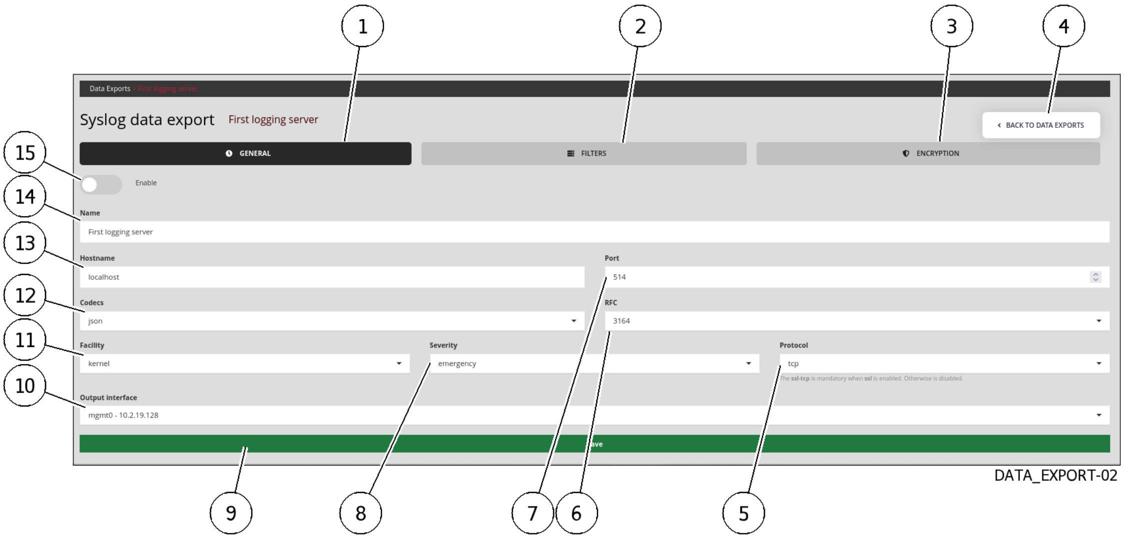
Data exports

Data exports

| Type | Name | Last Change (UTC) | Enabled | |
|---|---|---|---|---|
| Syslog | First logging server | | ✗ False | › Configure |
| Syslog | Second logging server | | ✗ False | › Configure |

DATA_EXPORT-01

- Click the `Configure` button (5) on one of the two connections (6 or 7) to be configured.
  The `Syslog data export` window opens.



Data Exports > First logging server

Syslog data export First logging server

‹ BACK TO DATA EXPORTS

GENERAL | FILTERS | ENCRYPTION

○ Enable

Name: First logging server

Hostname: localhost

Port: 514

Codecs: json

RFC: 3164

Facility: kernel

Severity: emergency

Protocol: tcp

The ssl-tcp is mandatory when ssl is enabled. Otherwise is disabled.

Output interface: mgmt0 - 10.2.19.128

Save

DATA_EXPORT-02

- Click on `GENERAL` tab (1).

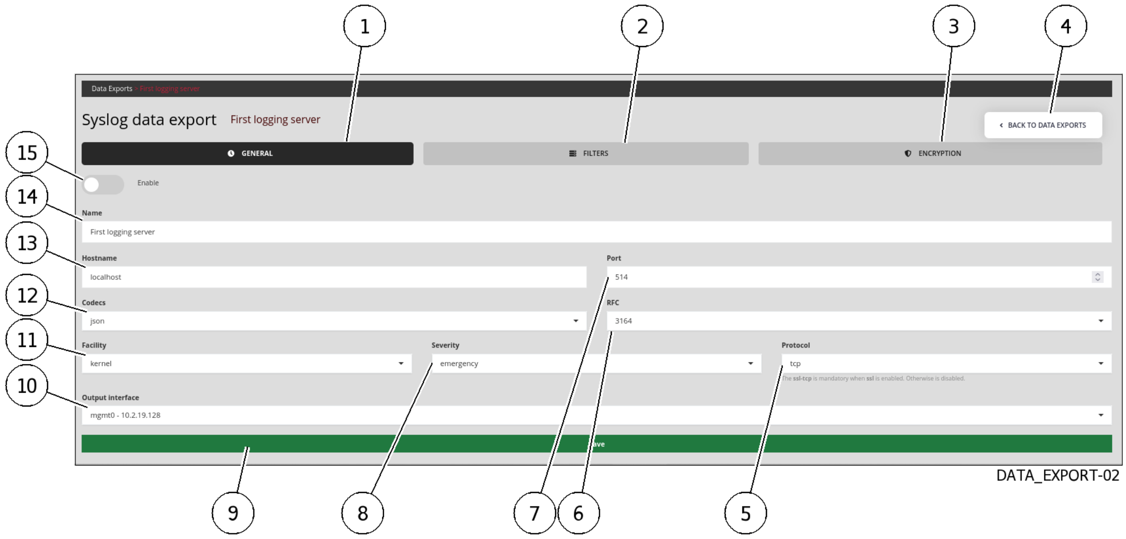
> **Note:**
>
> Values with a $VALUE format are context-specific and are noted as such so that they can be referenced in the rest of the documentation.

- Enter parameters using the following table:

| Item | Parameter | Description | Value |
|---|---|---|---|
| 15 | Enable | Activate this export pipeline | Activated |
| 14 | Name | Syslog export name | $SYSLOG_NAME |
| 13 | Hostname | Logstash server DNS name or IP address | $LOGSTASH_IP |
| 7 | Port | destination port | $LOGSTASH_PORT |
| 12 | Codecs | Codec used for export | JSON |
| 6 | RFC | Standard used by the codec | 3164 |
| 11 | Facility | Syslog header `facility` | default kernel; header will be removed by the reception pipeline |
| 8 | Severity | Value of `severity` in the Syslog header | emergency by default; the header will be deleted by the reception pipeline |
| 5 | Protocol | The transport protocol used. TCP or UDP can be used | $PROTOCOL |
| 10 | Output interface | Choose the GCenter interface used for Syslog export | $GCENTER_IFACE |

- Validate using button (9) `Save`.
  The following message indicates that the update has been completed: `Updated with success`.

### 8.6.3.6 Procedure to setup the filtration parameters



Data Exports > First logging server

Syslog data export First logging server

‹ BACK TO DATA EXPORTS

GENERAL | FILTERS | ENCRYPTION

Enable

Name: First logging server

Hostname: localhost

Port: 514

Codecs: json

RFC: 3164

Facility: kernel

Severity: emergency

Protocol: tcp

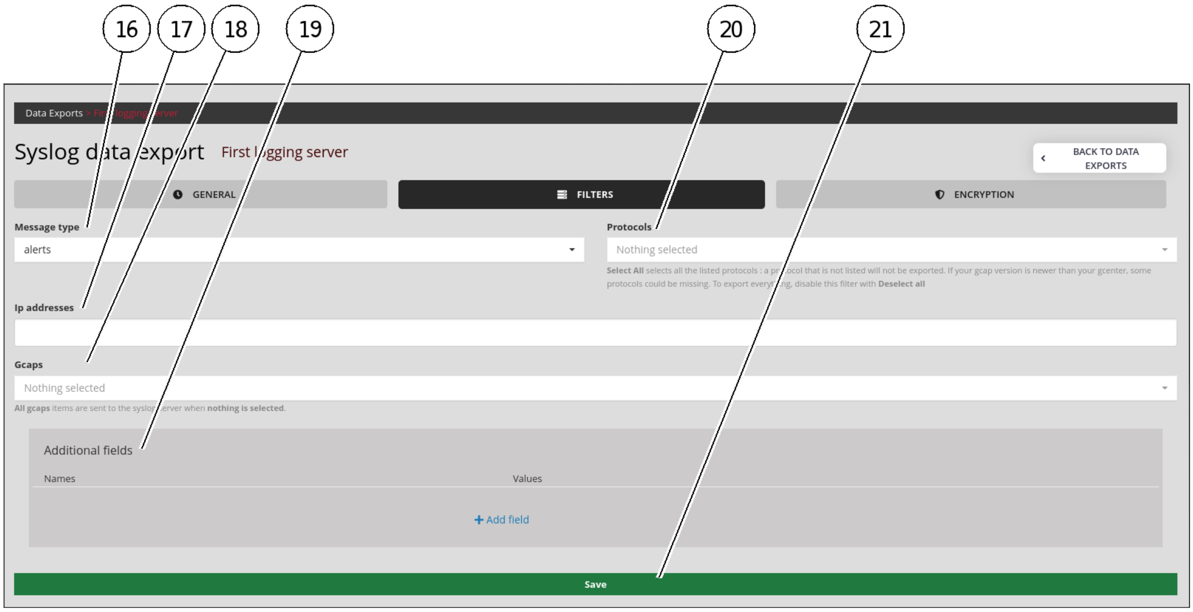
The ssl-tcp is mandatory when ssl is enabled. Otherwise is disabled.

Output interface: mgmt0 - 10.2.19.128

ave

DATA_EXPORT-02

- Click on the `FILTERS` tab (2).



Data Exports > First logging server

Syslog data export First logging server

Message type: alerts

Protocols: Nothing selected

**Select All** selects all the listed protocols : a protocol that is not listed will not be exported. If your gcap version is newer than your gcenter, some protocols could be missing. To export everything, disable this filter with **Deselect all**

Ip addresses

Gcaps: Nothing selected

**All gcaps** items are sent to the syslog server when **nothing is selected**.

Additional fields

Names Values

DATA_EXPORT-03

- Enter parameters using the following table:

| Item | Parameter | Description |
|---|---|---|
| 16 | \`Message type\` | Defines the type of event to send to the remote server. Either only alerts or alerts and metadata (Example: alerts, all) |
| 17 | \`Ip addresses\` | Filter by **IP** or **networks**. By default, all data is sent to the remote server if the field is empty |
| 18 | \`Gcaps\` | Filter by **GCap**. By default, all GCap data paired to GCenter is sent to the remote server if nothing is selected (Example: GCap1, GCap2) |
| 19 | \`Additional fields\` | Adds additional fields in exported events.<br>A name (\`Name\`) and a description (\`Values\`) can be entered in this window.<br>In the case of using the idmef codec, this field is not supported. |
| 20 | \`Protocols\` | Selects protocols to export<br>(Example : dcerpc, dhcp, dnp3, dns, enip, ftp, http, http2, ikev2, krb5, mqtt, modbus, netflow, nfs, ntp, rdp, rfb, sip, smb, smtp, ssh, tftp et tls) |
| 21 | \`Save\` | Changes are only taken into account after pressing the \`Save\` button. |

**Note:**

\`Select All\` selects all the protocols listed: a protocol that is not selected will not be exported.
If GCap is newer than GCenter, some protocols may be missing.
To export everything, disable this filter with \`Deselect all\`.

- Validate using button (21) \`Save\`.
  The following message indicates that the update has been completed: \`Updated with success\`.

#### 8.6.3.7 Procedure to configure encryption settings

The "ENCRYPTION" tab enables the encryption of the flow generated by the GCenter.
Logstash's "syslog" input is not compatible with data encryption.
This feature cannot be used.

---

#### 8.6.3.8 Procedure to be performed on the server

- Configure the flow receiving pipeline from GCenter.

##### 8.6.3.8.1 Pipeline Logstash

The input used is Syslog.
In order to be compatible with any Syslog header, a grok pattern is specified.
The JSON content of the log is in the syslog_message field.

```
yaml
input {
  syslog {
    port => $LOGSTASH_PORT
    type => syslog
    grok_pattern => '^<%{NUMBER:syslog_priority}>(?:1 |)(?:%{SYSLOGTIMESTAMP:syslog_timestamp}
↪|%{TIMESTAMP_ISO8601:syslog_timestamp}) %{SYSLOGHOST:syslog_hostname} (?:gatewatcher\[-\
↪]:|gatewatcher - - \[-\]) %{GREEDYDATA:syslog_message}\n$'
  }
}
```

Only the syslog_message field is preserved and is converted to JSON.
The original field (syslog_message) and the field specific to elasticsearch (@version) are then removed.

```
yaml
filter {
  prune {
    whitelist_names => [ "syslog_message" ]
  }

  json {
    source => "syslog_message"
  }

  mutate {
    remove_field => [ "@version","syslog_message" ]
  }

}
```

Any output can then be used.

In this example, the logs are described directly on the disk as files:

```
yaml
output {
  file {
    path => '/usr/share/logstash/data/output/%{[type]}-%{+YYYY.MM.dd}.log'
    codec => json_lines
  }
}
```

---

## 8.6.4 Quick creation of a POC Logstash

### 8.6.4.1 Introduction

This procedure describes how to quickly create a Logstash Proof Of Concept.

---

### 8.6.4.2 Prerequisites

- User : member of **Administrator** group

---

### 8.6.4.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

---

### 8.6.4.4 Procedure

A POC with a Logstash docker can be done in minutes.
The following commands, given as an indication, should facilitate this task.

**Important:**

The controls are given as an indication to mount a demonstrator quickly. It does not follow the best practices necessary for the development of a production component.

- On a Linux machine with docker, run the following commands to retrieve the default Logstash configuration files: (procedure tested with Logstash version 7.13.1)

```
bash
mkdir logstash_docker
cd logstash_docker
sudo docker run --name="logstash_tmp" --rm -d -it docker.elastic.co/logstash/logstash:7.
↪13.1
sudo docker cp logstash_tmp:/usr/share/logstash/config config
sudo docker cp logstash_tmp:/usr/share/logstash/pipeline pipeline
sudo docker rm -f logstash_tmp
```

A *logstash_ docker* folder has been created with two subfolders: *config* and *pipeline*.
In *config*, parameters can be kept by default, except for the *xpack.monitoring.elasticsearch.hosts* parameter which must be commented in *logstash.yaml*.

- In the *pipeline* folder, replace the default pipeline with the pipeline described in the section above.
  A docker using these configuration files and this pipeline can then be started:

```
sudo docker run --name="logstash_export" --rm -d -it -p $LOGSTASH_PORT:$LOGSTASH_PORT/
↪$PROTOCOL -v $(pwd)/config/:/usr/share/logstash/config/ -v $(pwd)/pipeline:/usr/share/
↪logstash/pipeline/ -v $(pwd)/output:/usr/share/logstash/data/output/ --user $(id -u):
↪$(id -g) docker.elastic.co/logstash/logstash:7.13.1
```

  Logstash will then create an *output* directory in which the received logs will be written, with one JSON per line.

### 8.6.5 Configuring the connection to the MISP

#### 8.6.5.1 Introduction

This procedure describes the connection configuration with a MISP server present in the infrastructure.

**Note:**

For more information, see the *Interconnection with external systems*.
Viewing the connection status and configuration of the MISP connection is described in *MISP Connection Configuration Screen*.

The MISP connector allows you to bring IOC directly from a MISP to GCenter in the form of rules.
From the GCenter, these rules can be included in a ruleset and therefore sent to the GCap.
This connector allows to add a source of threat intelligence of quality while respecting the instructions of the ANSSI on the qualification of signatures.
The MISP configuration is added to the Sigflow menu in a new menu `` `MISP` ``.

#### 8.6.5.2 Prerequisites

- User : member of **Administrator** group

### 8.6.5.3 Preliminary operations

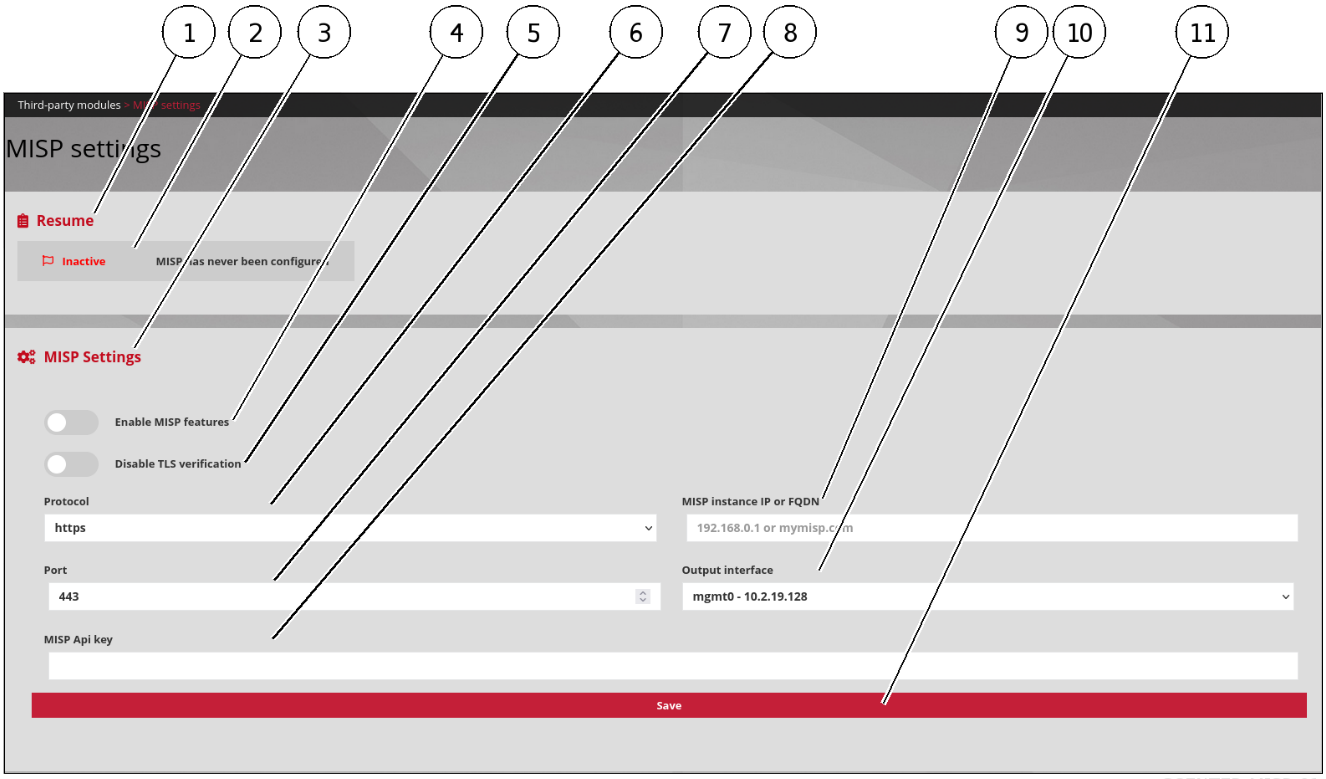
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

### 8.6.5.4 Procedure to access the `MISP settings`

- In the navigation bar, click successively on:
- The `Admin` button
- The `Gcenter` sub menu
- the `Third-party modules` command
  The `Third-party modules` window is displayed.
- Click the `MISP` button.

### 8.6.5.5 Procedure to view the current status

The following screen is displayed:



GCENTER-MISP-01

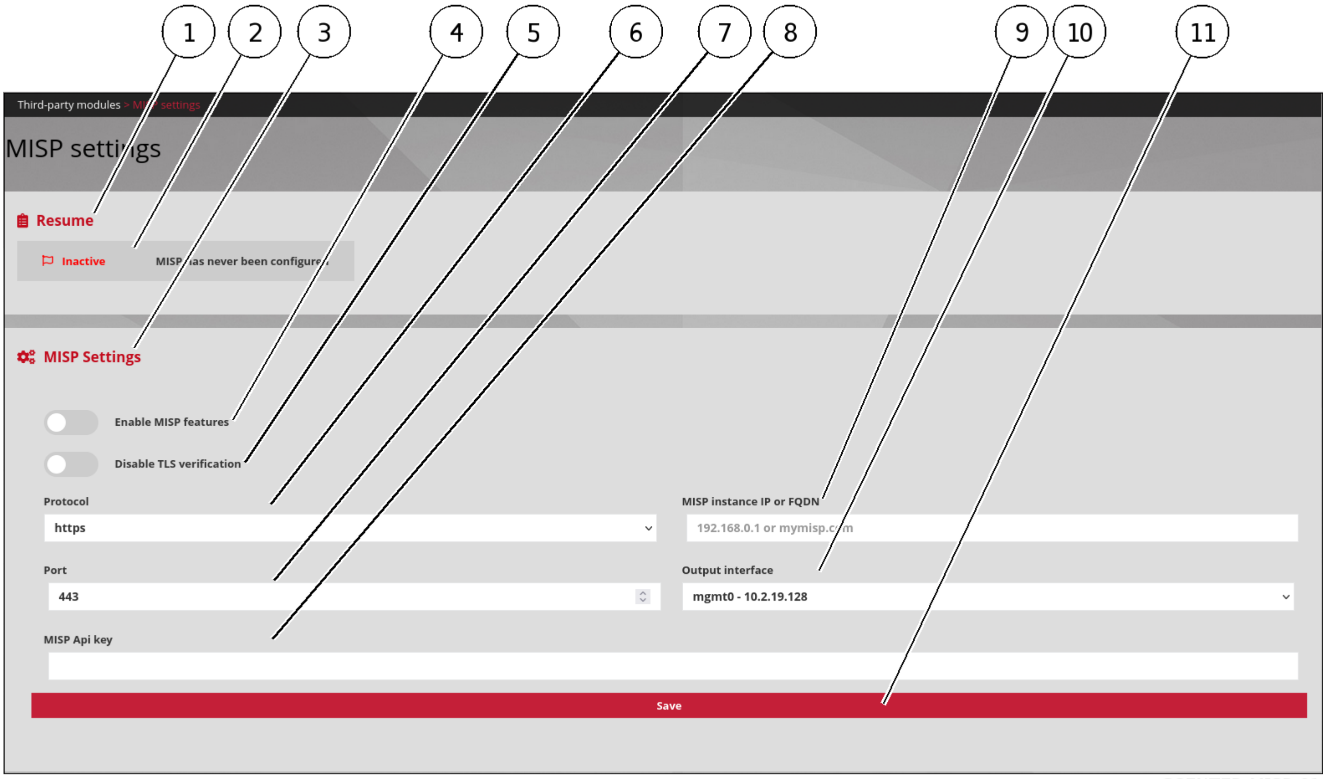
- Pour configurer la connexion, effectuer la procédure suivante.
- In part (1) `Resume`, view:
  - the status
  - status message of connection with remote server (2)

> **Note:**
>
> Status: Inactive
>
> the message: `MISP has never been configured` means that the connection with the MISP does not exist or is incorrectly configured.

- To configure the connection, perform the following procedure.

### 8.6.5.6 Procedure to configure the connection

The configuration is to be done in part (3) `MISP Settings`.



GCENTER-MISP-01

- Activate the `Enable MISP features` button to activate the MIPS functions (4).
- If necessary, activate the `Disable TLS verification` button (5).
- Select the communication protocol (6) to use to contact the MISP instance: two options are possible ('https' and 'http').
- Enter the listening port (7).
- Enter the API key (8) of the MISP instance.
- Enter the FQDN or IP address (9) of the MISP instance.
- Select the GCenter network interface (10) to connect to.
- Click on the button (11) `Save`.

  The service is now activated, the current status of the connection is changed (`Active`) as well as the connection information.

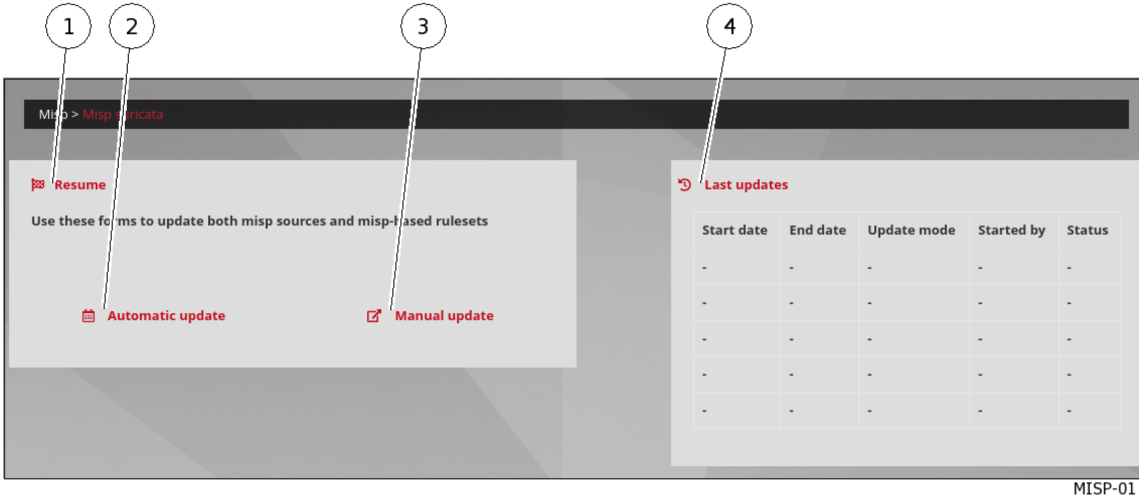
  The sub-menu `MISP` of the menu `Sigflow` is now available to members of the `operator` group.

  It is therefore possible to choose a manual or automatic update.
- To perform a manual update, perform the *Procedure to configure the manual MISP Rule Update*.

  To perform an automatic update, perform the *Procedure to configure Automatic MISP Rule Update*.

#### 8.6.5.7 Procedure to configure the manual MISP Rule Update

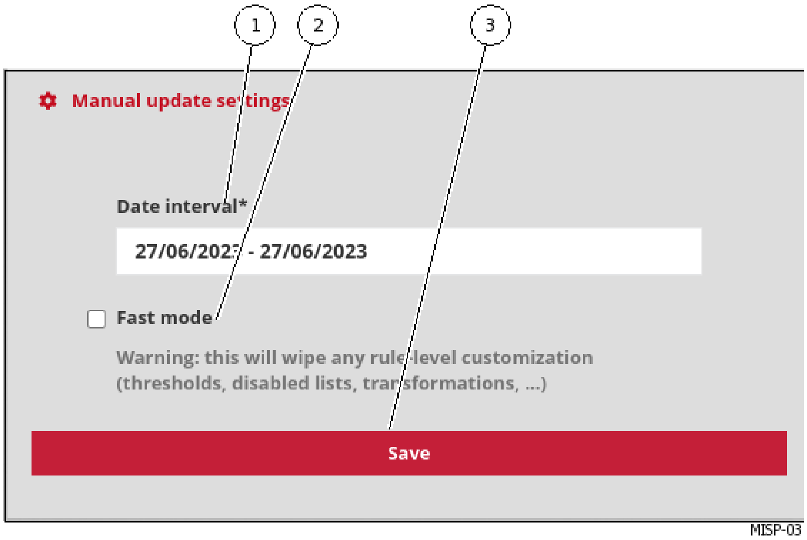
- In the navigation bar, click successively on:
- the `Config`
- the sub menu `Sigflow`
- the command `MISP`
  The `Misp suricata` window is displayed.



Use these forms to update both misp sources and misp-based rulesets

| Start date | End date | Update mode | Started by | Status |
|---|---|---|---|---|
| - | - | - | - | - |
| - | - | - | - | - |
| - | - | - | - | - |
| - | - | - | - | - |
| - | - | - | - | - |

- Click on the `Manual update` link.



Date interval*
27/06/2023 - 27/06/2023

□ Fast mode

Warning: this will wipe any rule-level customization (thresholds, disabled lists, transformations, ...)

- Enter the time interval in field (1).
- If necessary, use the `Fast mode` (2) function.

**Note:**

This will erase any customization at the level of the rules (thresholds, disabled lists, transformations, ...)

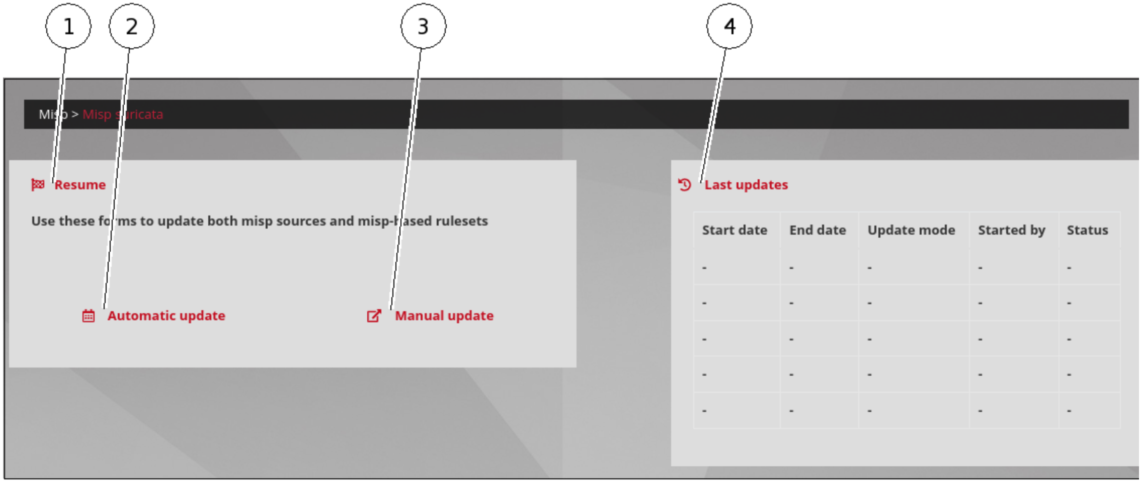
- Click on the button (3) `Save`.
  The update is launched and the corresponding information is displayed in the `Last updates` section of the `Misp suricata` screen.

#### 8.6.5.8 Procedure to configure Automatic MISP Rule Update

- In the navigation bar, click successively on:

- The `Config`
- The `Sigflow` sub menu
- The `MISP` command

  The `Misp suricata` window is displayed.

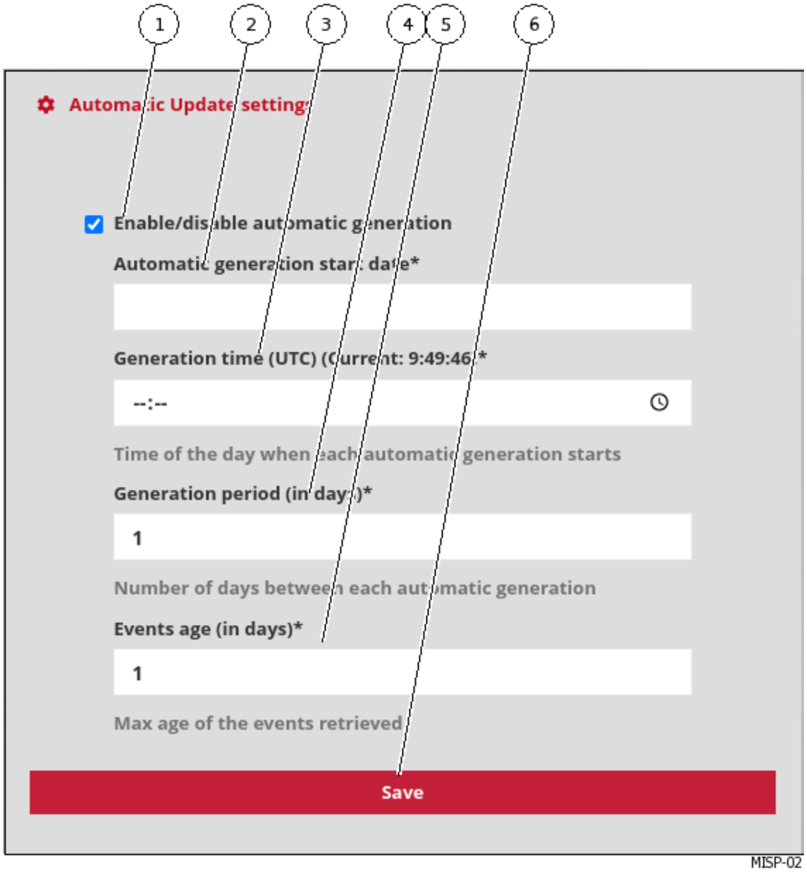


Use these forms to update both misp sources and misp-based rulesets

| Start date | End date | Update mode | Started by | Status |
|---|---|---|---|---|
| - | - | - | - | - |
| - | - | - | - | - |
| - | - | - | - | - |
| - | - | - | - | - |
| - | - | - | - | - |

MISP-01

- Click on the `Automatic update` link.



Automatic Update settings

☑ Enable/disable automatic generation

Automatic generation start date*

Generation time (UTC) (Current: 9:49:46)*

--:--

Time of the day when each automatic generation starts

Generation period (in days)*

1

Number of days between each automatic generation

Events age (in days)*

1

Max age of the events retrieved

MISP-02

- Enable or disable automatic generation of updates with selector (1).
- Select the start date of automatic generation in field (2).
- Enter the update time in UTC in field (3).
- Select the periodicity (in days) in field (4).
- Enter the maximum age of the events retrieved in field (5).

- Click on the `` `Save` `` button (3) .
  The update is launched and the corresponding information is displayed in the `` `Last updates` `` section of the `` `Misp suricata` `` screen.

---

### 8.6.6 Configuring the connection to the Intelligence site

#### 8.6.6.1 Introduction

This procedure describes the procedure to configure the connection with the Intelligence site.

> **Note:**
>
> For more information, see l'*Interconnection with external systems*.
> The graphical interface is described in *`Admin-GCenter- Third-party modules` screen of the legacy web UI*.

---

#### 8.6.6.2 Prerequisites

- User : member of **Administrator** group

---

#### 8.6.6.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).
- Create an Intelligence account with an email address.
  At this email address, an email will be sent and will contain a token to connect a **GCenter**.
  A unique token per user account will be sent by email: it can be used on several **GCenter**.
  The activation of a new token will be added to the list of other tokens linked to the email address.

---

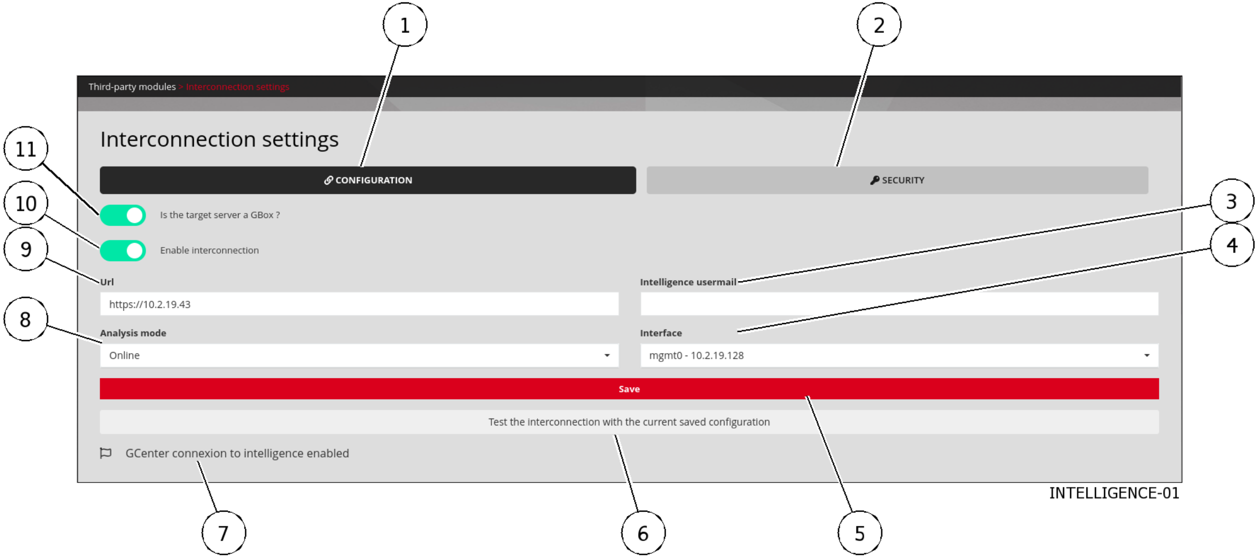
#### 8.6.6.4 Procedure to access to the `` `Interconnection settings` ``

- In the navigation bar, click successively on:

- The `` `Admin` ``
- The sub menu `` `Gcenter` ``
- The command `` `Third-party modules ``
  The `` `Third-party modules` `` window is displayed.

- Click the `` `Intelligence` `` button.

The following screen is displayed:



Third-party modules > Interconnection settings

Interconnection settings

CONFIGURATION | SECURITY

Is the target server a GBox ?

Enable interconnection

Url: https://10.2.19.43

Intelligence usermail:

Analysis mode: Online

Interface: mgmt0 - 10.2.19.128

Save

Test the interconnection with the current saved configuration

GCenter connexion to intelligence enabled

INTELLIGENCE-01

The Interconnection settings page consists of the tabs:

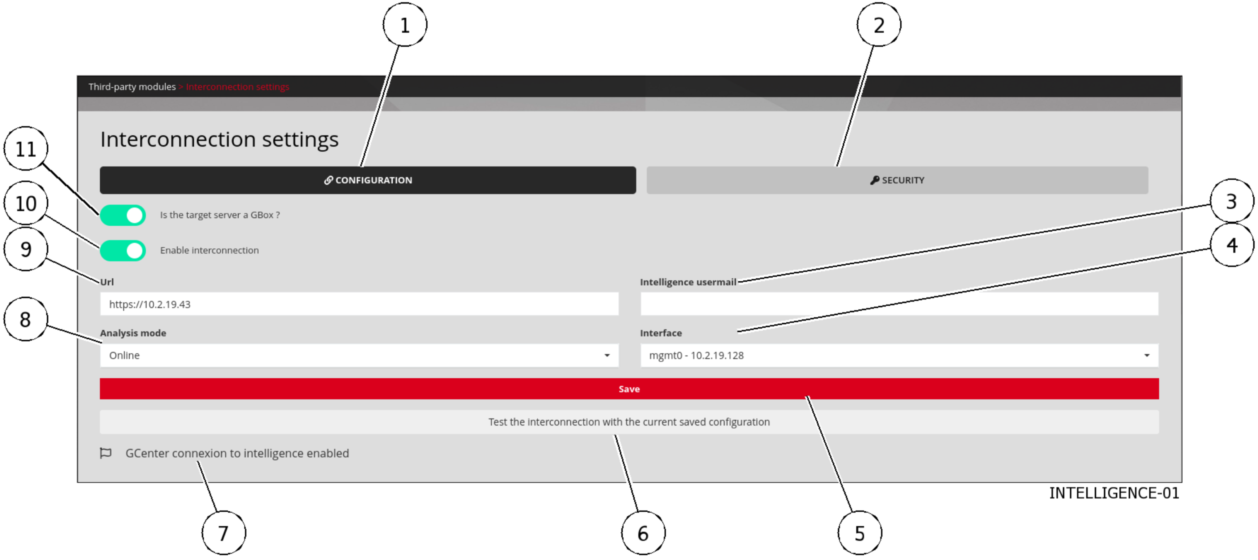
- `Configuration` Settings Management tab
- `Security` Settings Management tab

### 8.6.6.5 Procedure to test the current setting

- Press the button (6) `Test the interconnection with the current saved configuration`.
- View status message (7):
  - If the message is `GCenter connexion to intelligence enabled` then the connection is correctly configured
  - Otherwise, use the following procedure to configure this connection

### 8.6.6.6 Procedure to configure the connection

- Click on the `CONFIGURATION` button (1) .
  The following screen is displayed:



Third-party modules > Interconnection settings

Interconnection settings

CONFIGURATION | SECURITY

Is the target server a GBox ?

Enable interconnection

Url: https://10.2.19.43

Intelligence usermail:

Analysis mode: Online

Interface: mgmt0 - 10.2.19.128

Save

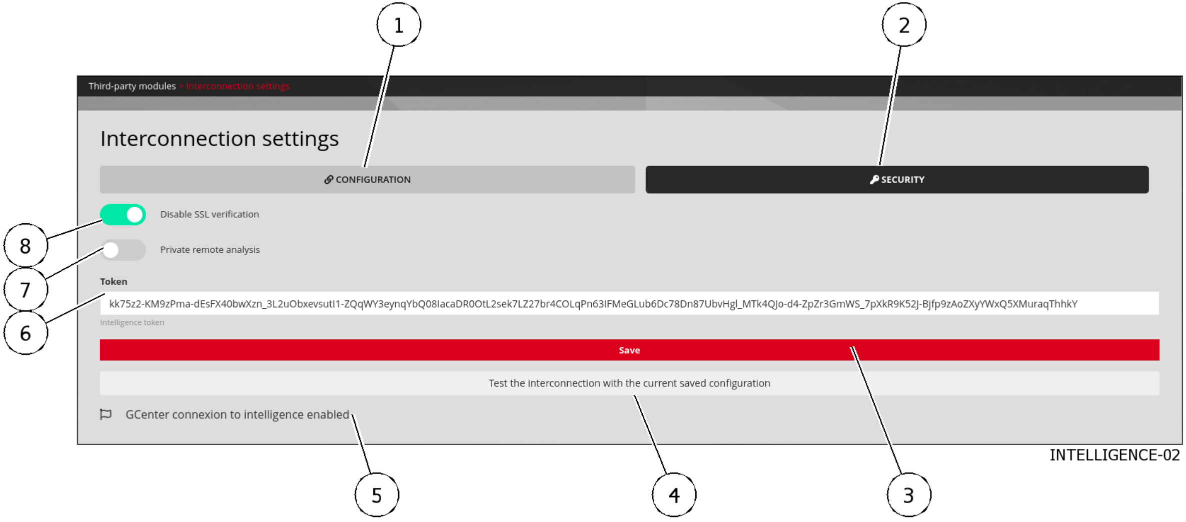
Test the interconnection with the current saved configuration

GCenter connexion to intelligence enabled

INTELLIGENCE-01

- Disable selector (11) `` `Is the target server a GBOX` ``.
- Activate selector (10) `` `Enable interconnection` ``.
- Enter the Intelligence site URL (for example `` `https://intelligence.gatewatcher.com/gwapi/` ``) in field (9) `` `Url` ``.
- Enter the email address of the intelligence account in field (3) `` `Intelligence usermail` ``.
- Select the `` `Online` `` choice in field (8) `` `Analysis mode` ``.
- Select the network interface (4) to use for this connection.
- Press the `` `Save` `` button (3).
- Click on the button (2) `` `SECURITY` ``.

  The following screen is displayed:



Third-party modules > Interconnection settings

Interconnection settings

CONFIGURATION | SECURITY

Disable SSL verification

Private remote analysis

Token

kk75z2-KM9zPma-dEsFX40bwXzn_3L2uObxevsutI1-ZQqWY3eynqYbQ08IacaDR0OtL2sek7LZ27br4COLqPn63IFMeGLub6Dc78Dn87UbvHgl_MTk4QJo-d4-ZpZr3GmWS_7pXkR9K52J-Bjfp9zAoZXyYWxQ5XMuraqThhkY

Intelligence token

Save

Test the interconnection with the current saved configuration

GCenter connexion to intelligence enabled

INTELLIGENCE-02

- Disable selector (8) `` `Disable SSL verification` ``.
- Activate the selector (7) `` `Private remote analysis` ``.

> **Note:**
>
> The `` `Private remote analysis` `` selector allows anonymity when sending samples.

- Paste the token received in the mail of the intelligence account in the field (6) `` `Token` ``.
- Press the `` `Save` `` button.

  When the backup is done, the following message is displayed: `` `The new configuration was successfully saved and applied.` ``

  The status message is displayed in box (7). If the message `` `GCenter connexion to intelligence enabled` `` is displayed, then the connection is correctly configured.

  Following this connection, the administrator can send files to the Intelligence platform for further analysis and download the report.

## 8.6.7 Configuring the connection to the GBox

### 8.6.7.1 Introduction

This procedure describes the connection configuration with the GBox.

**Note:**

For more information, see *Interconnection with external systems*.
The graphical interface is described in *`Admin-GCenter- Third-party modules` screen of the legacy web UI*.

### 8.6.7.2 Prerequisites

- User : member of **Administrator** group

### 8.6.7.3 Preliminary operations

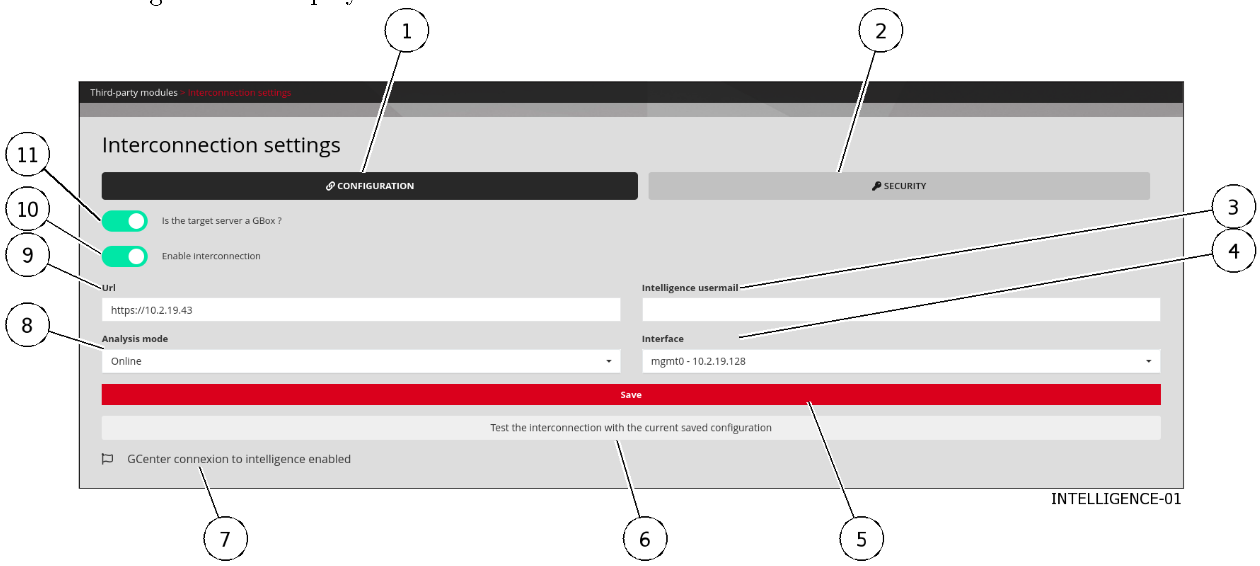
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

### 8.6.7.4 Procedure to acces to the `Interconnection settings` setting

- In the navigation bar, click successively on:
- The `Admin` button
- The `Gcenter` sub menu
- The `Third-party modules` command

  The `Third-party modules` window is displayed.
- Click the `Intelligence` button.

  The following screen is displayed:



1
2
3
4
5
6
7
8
9
10
11
Third-party modules > Interconnection settings
Interconnection settings
CONFIGURATION
SECURITY
Save
Test the interconnection with the current saved configuration
INTELLIGENCE-01

Is the target server a GBox ?

Enable interconnection

Url: https://10.2.19.43

Intelligence usermail:

Analysis mode: Online

Interface: mgmt0 - 10.2.19.128

GCenter connexion to intelligence enabled

The Interconnection settings page consists of the tabs:

- `Configuration` Settings Management tab
- `Security` Settings Management tab

#### 8.6.7.5 Procedure to test the current setting

- Press button (6) `` `Test the interconnection with the current saved configuration` ``.

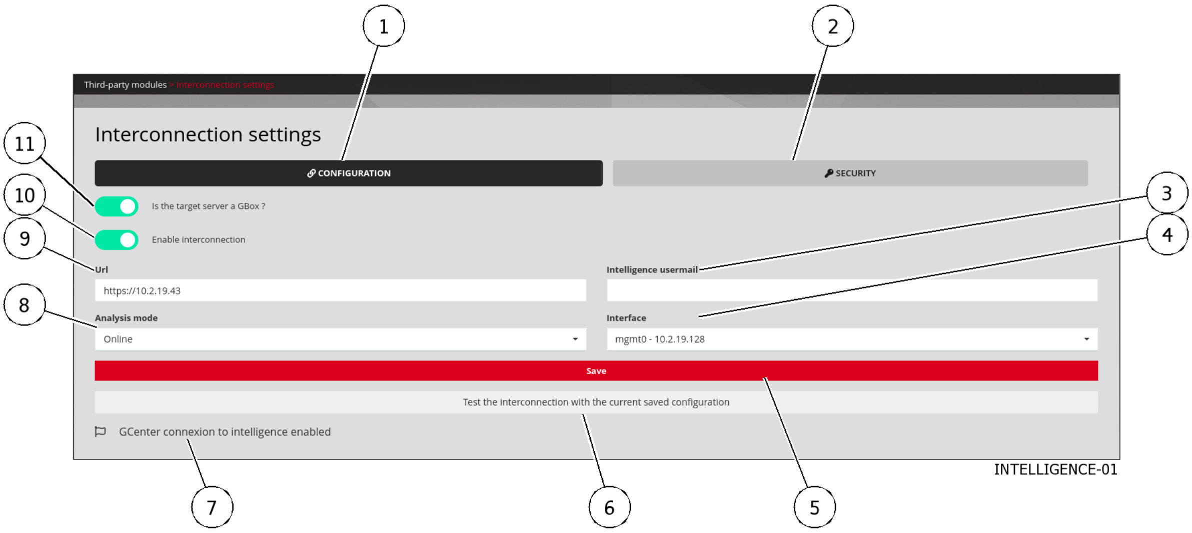
  The message `` `Successfully established connection to GBox https://x.x.x.x` `` is displayed to indicate a correct connection with the GBox.
- View status message (7):
- If the message is `` `GCenter connexion to intelligence enabled` `` then the connection is correctly configured
- Otherwise, use the following procedure to configure this connection

---

#### 8.6.7.6 Procedure to configure the connection

- Click on the `` `CONFIGURATION` `` button (1) .

  The following screen is displayed:


1
2
11
10
9
8
3
4
7
6
5
Third-party modules > Interconnection settings
Interconnection settings
CONFIGURATION
SECURITY
Save
Test the interconnection with the current saved configuration

☑ Is the target server a GBox ?

☑ Enable interconnection

Url: https://10.2.19.43

Intelligence usermail:

Analysis mode: Online

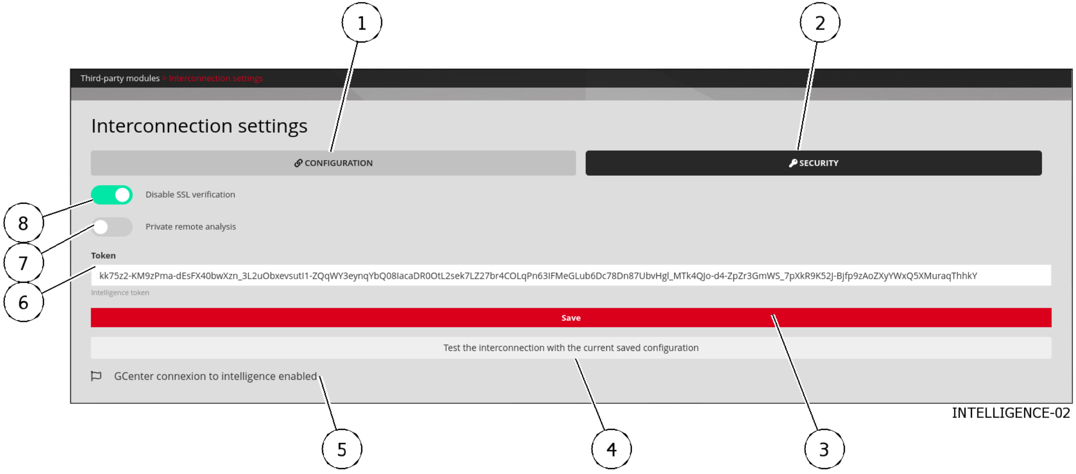
Interface: mgmt0 - 10.2.19.128

GCenter connexion to intelligence enabled

INTELLIGENCE-01

- Activate selector (11) `` `Is the target server a GBOX` ``.
- Activate selector (10) `` `Enable interconnection` ``.
- Enter the GBox URL (for example `` `https://adresse IP` ``) in field (9) `` `Url` ``.
- Do not enter anything in field (3) `` `Intelligence usermail` ``.
- Select `` `Offline` `` in field (8) `` `Analysis mode ``.
- Select the network interface (4) to be used for this interconnection.
- Press the `` `Save` `` button.
- Click on the button (2) `` `SECURITY` ``.

  The following screen is displayed:


1
2
8
7
6
5
4
3
Third-party modules > Interconnection settings
Interconnection settings
CONFIGURATION
SECURITY
Save
Test the interconnection with the current saved configuration

☑ Disable SSL verification

☐ Private remote analysis

Token: kk75z2-KM9zPma-dEsFX40bwXzn_3L2uObxevsutI1-ZQqWY3eynqYbQ08IacaDR0OtL2sek7LZ27br4COLqPn63IFMeGLub6Dc78Dn87UbvHgl_MTk4QJo-d4-ZpZr3GmWS_7pXkR9K52J-Bjfp9zAoZXyYWxQ5XMuraqThhkY

Intelligence token

GCenter connexion to intelligence enabled

INTELLIGENCE-02

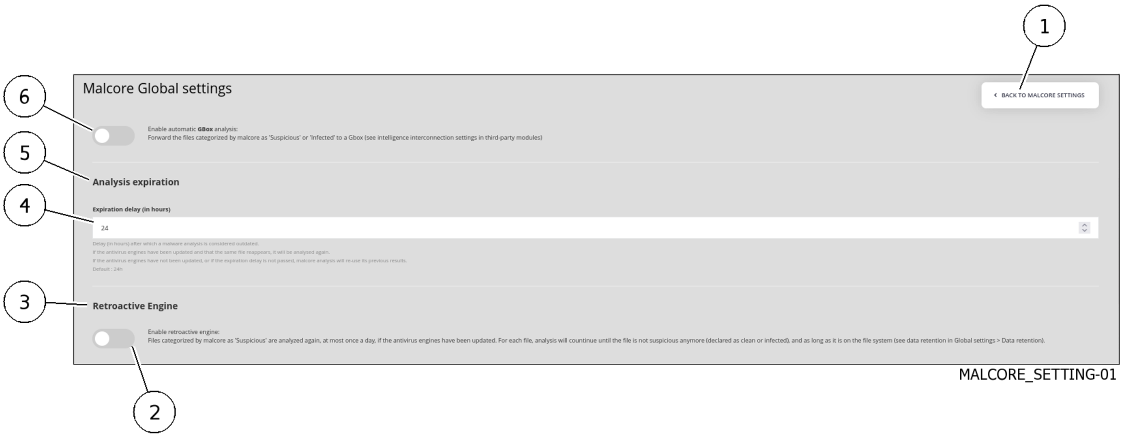
- Activate selector (8) `Disable SSL verification`.
- Disable the selector (7) `Private remote analysis`.
- Access the GBox WEBUI interface.
- Create a token in the GBox webui interface (see the tokens API screen accessible from the `Admin/GBox/Accounts` menu).
- Copy this token.
- Paste this token in field (6) `Token`.
- Press the `Save` button.

  When the backup is done, the following message is displayed: `The new configuration was successfully saved and applied.`

  The status message (7) is `GCenter connexion to intelligence enabled`: the connection is correctly configured.

### 8.6.7.7 Procedure to setup the Malcore Engine

- In the navigation bar, click successively on:
  - The `Admin` button
  - The `Gcenter` sub menu
  - The `Malcore Management` command



Malcore Global settings

Enable automatic **GBox** analysis:
Forward the files categorized by malcore as 'Suspicious' or 'Infected' to a Gbox (see intelligence interconnection settings in third-party modules)

**Analysis expiration**

**Expiration delay (in hours)**

24

Delay (in hours) after which a malware analysis is considered outdated.
If the antivirus engines have been updated and that the same file reappears, it will be analysed again.
If the antivirus engines have not been updated, or if the expiration delay is not passed, malcore analysis will re-use its previous results.
Default : 24h

**Retroactive Engine**

Enable retroactive engine:
Files categorized by malcore as 'Suspicious' are analyzed again, at most once a day, if the antivirus engines have been updated. For each file, analysis will countinue until the file is not suspicious anymore (declared as clean or infected), and as long as it is on the file system (see data retention in Global settings > Data retention).

MALCORE_SETTING-01

- Enable selector (6) `Enable automatic GBox analysis:` C.A' to enable automatic GBox analysis to transfer files classified by Malcore as 'Suspect' or 'Infected'.

  Following this connection, the administrator may be able to send files to the Intelligence platform for further analysis and download the report.

## 8.6.8 Deleting data (log files)

### 8.6.8.1 Introduction

This procedure enables clearing the information tables of the analysis engines, syslog exchanges, and NDR information over a given period of time.

This deletion period is selected by the administrator, however, it cannot exceed the total retention time of the data already pre-configured in the solution.

**Important:**

Data not yet processed will also be deleted.

**Note:**

After a full or incremental save by the backup functionality, the old logs are automatically deleted, depending on the data retention time, thus freeing up disk space.

**Note:**

See the log files and their management presentation in the paragraph *Data use*.
The graphical interface of the data export function is described in *`Admin-GCenter- Data Management` screen of the legacy web UI*.

#### 8.6.8.2 Prerequisites

- User : member of **Administrator** group

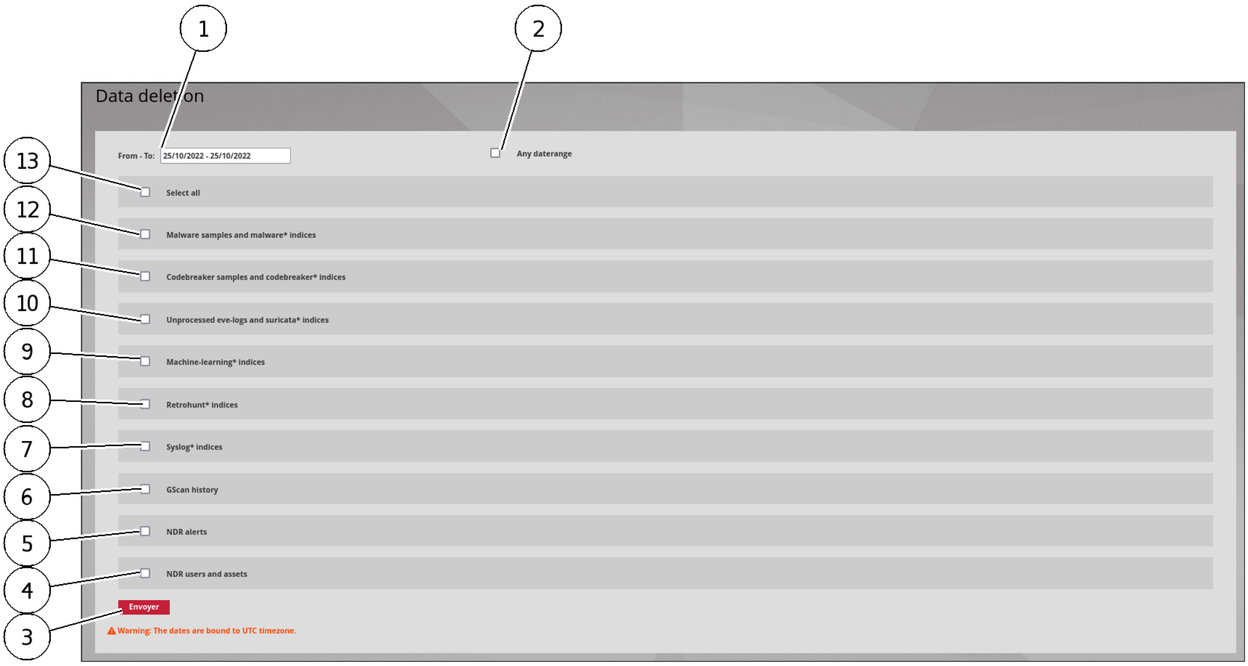
#### 8.6.8.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

#### 8.6.8.4 Procedure to access to the `Data deletion` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Data Management` command
  The `Data Management` window is displayed.
- Click on the `Data deletion` option.
  The `Data deletion` window is displayed.

#### 8.6.8.5 Procedure to change certain user information



Data deletion

From - To: 25/10/2022 - 25/10/2022

□ Any daterange

□ Select all

□ Malware samples and malware* indices

□ Codebreaker samples and codebreaker* indices

□ Unprocessed eve-logs and suricata* indices

□ Machine-learning* indices

□ Retrohunt* indices

□ Syslog* indices

□ GScan history

□ NDR alerts

□ NDR users and assets

Envoyer

⚠ Warning: The dates are bound to UTC timezone.

DATA_DELETION-1

- Choosing the time interval (1) in which the deletion is to be carried out.
  A window opens.

- Use the calendar to enter the start date.
- Use the calendar to enter the end date.
- Validate using the `Apply` button.

- Select the information to be deleted:

- Select `Any datarange` (2) to delete all
- Or select one of the categories (4 to 13)

- Validate using the `Send` button (3).

## 8.6.9 Generating and loading files for diagnosis

### 8.6.9.1 Introduction

This procedure enables generating and loading:

- Log files, information tables, analysis engines, syslog exchanges, and NDR information for a given period.
- The Tech support file

**Important:**

Indeed, this archive can only be extracted by an advanced administrator having knowledge of the data extraction password.

**Note:**

See the presentation of the data for the diagnosis in the paragraph *Data use*.
The graphical interface of the diagnostic function is described in the *`Admin-GCenter- Diagnostics` screen of the legacy web UI*.

### 8.6.9.2 Prerequisites

- User : member of **Administrator** group

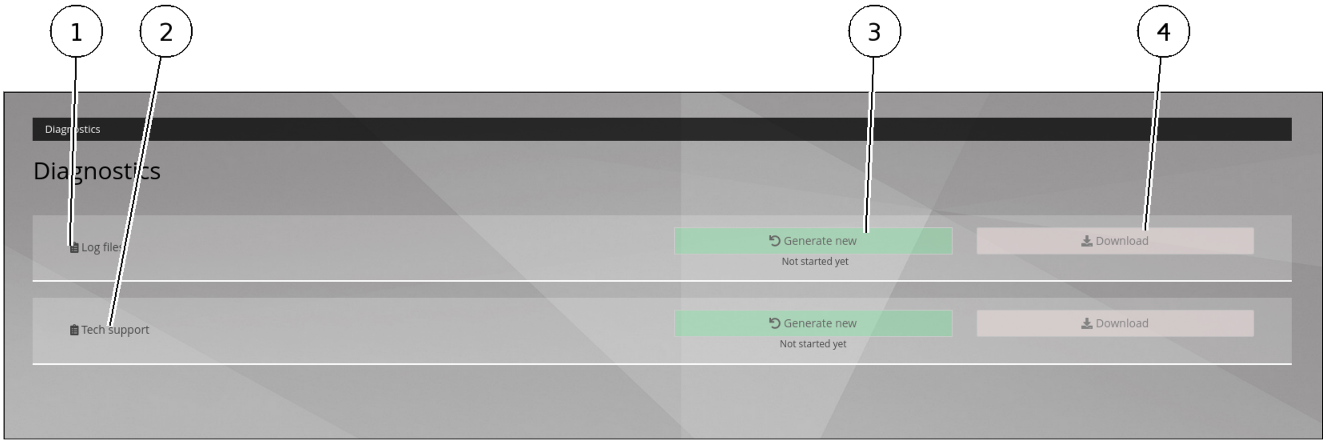
### 8.6.9.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

### 8.6.9.4 Procedure to access the `Diagnostics` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Diagnostics` command
  The `Diagnostics` window is displayed.

### 8.6.9.5 Procedure to generate and load diagnostic files



Not started yet

Not started yet

DIAGNOSTIC-01

- Press the `Generate new` button (3) in the `Log file` (1) or `Tech support` (2).
  A message is displayed below the button to indicate the result of the generation: example `Generated with success!`
  The date and time of generation (e.g. 2022-10-27T11:59:27.451443 UTC) are displayed under the `Download` button (4).
- Press the `Download` button (4) in the `Log file` (1) or `Tech support` (2).

A window opens showing the download of the files.

The file uploaded for a log file is named **hostname-time-logs.gwl**. This file is encrypted. It is only visible to the GATEWATCHER support team.

The file downloaded for a Tech support is named **tech-support.txt** : this file is a text file and can be opened.

The file is therefore present in the computer's local directory.

- Send these files to the GATEWATCHER support team for analysis.

## 8.6.10 Using an endpoint API

### 8.6.10.1 Introduction

This procedure shows how:

- Run an endpoint locally
- Retrieve the answer
- Have the corresponding .json
- Know the model of the response and have an example of it

By clicking on the `` `Try it out` `` button, it is possible to test the selected query and the tool generates the query to use with curl.

The *Procedure to run an endpoint* specifies how to use the swagger GUI to select an API, execute the request, retrieve the response and curl of the request.

However, this request inherits the rights (and therefore the token) of the request creator.

To make a request with different rights, refer to *Procedure to modify the token associated with the request*.

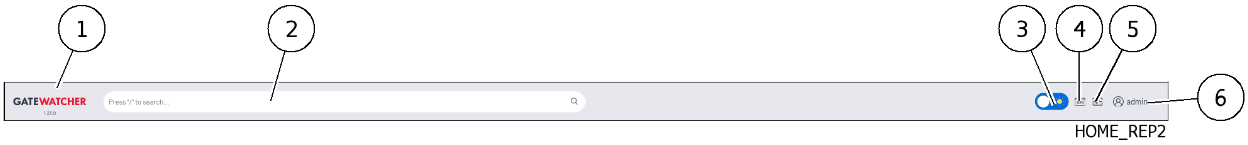
### 8.6.10.2 Prerequisites

User : member of **Administrator** group

### 8.6.10.3 Preliminary operations

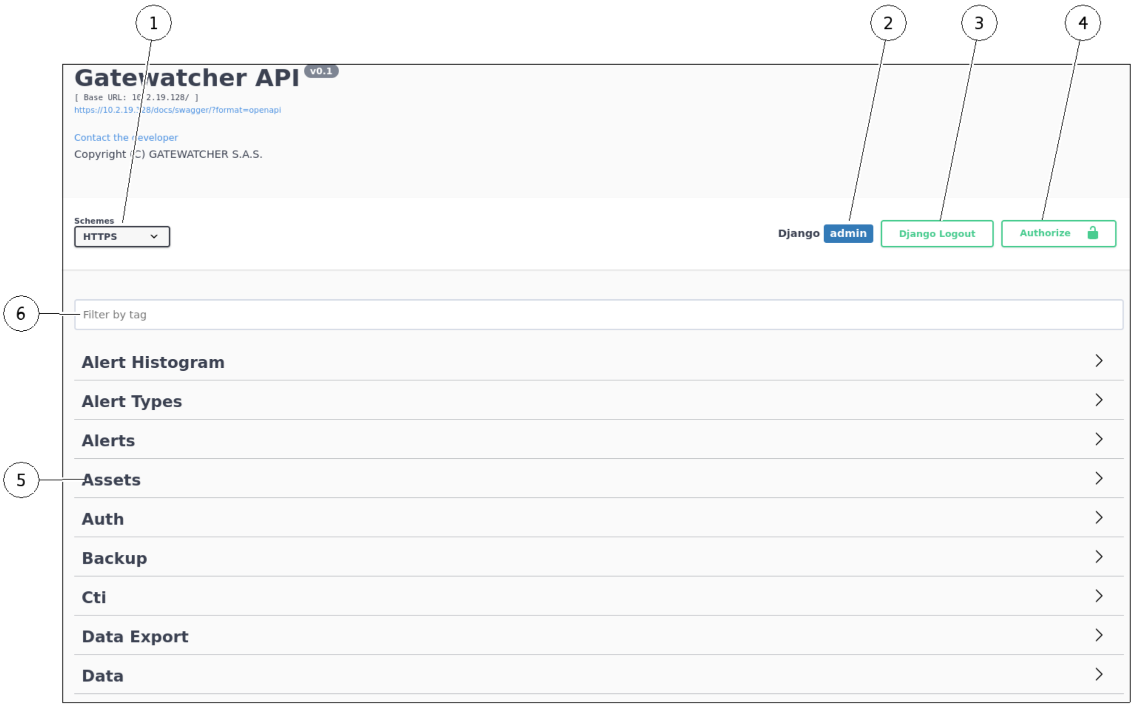
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

### 8.6.10.4 Procedure to acces to API



- Click on the button (4) `` `API` `` in the title bar.

  The following screen is displayed.



Gatewatcher API v0.1
[ Base URL: 10.2.19.128/ ]
https://10.2.19.128/docs/swagger/?format=openapi

Contact the developer
Copyright (C) GATEWATCHER S.A.S.

Schemes
HTTPS

Django admin | Django Logout | Authorize

Filter by tag

- Alert Histogram
- Alert Types
- Alerts
- Assets
- Auth
- Backup
- Cti
- Data Export
- Data

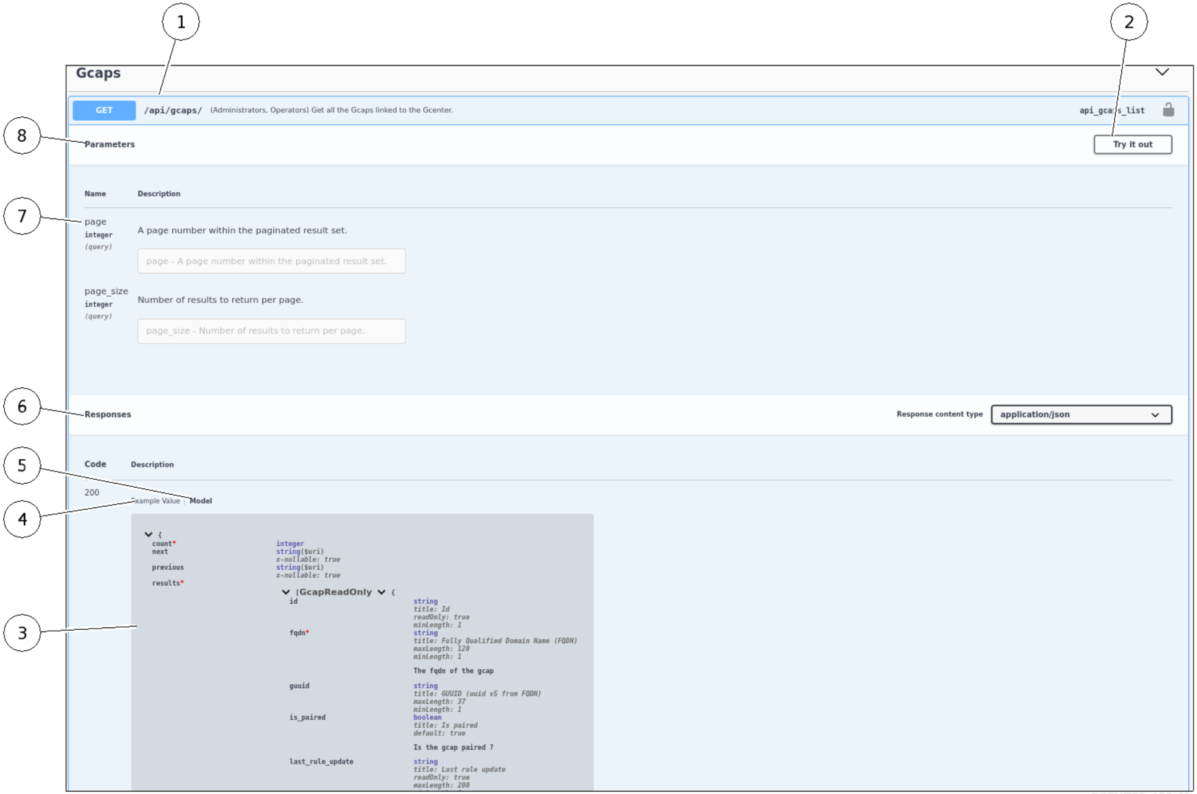
GCENTER-API-01

### 8.6.10.5 Procedure to run an endpoint

To illustrate this example, the API chosen is the one that lists the GCaps connected to GCenter.

- Select the `Gcaps` theme from the list of existing themes (5).
- Click on the API `GET/api/gcap/ (Administrators, Operator) Get all the GCaps linked to the GCenter`.

  The window below is displayed.



Gcaps

GET /api/gcaps/ (Administrators, Operators) Get all the Gcaps linked to the Gcenter. api_gcaps_list

Parameters | Try it out

| Name | Description |
|---|---|
| page<br>integer<br>*(query)* | A page number within the paginated result set.<br>page - A page number within the paginated result set. |
| page_size<br>integer<br>*(query)* | Number of results to return per page.<br>page_size - Number of results to return per page. |

Responses | Response content type: application/json

| Code | Description |
|---|---|
| 200 | Example Value \| Model |

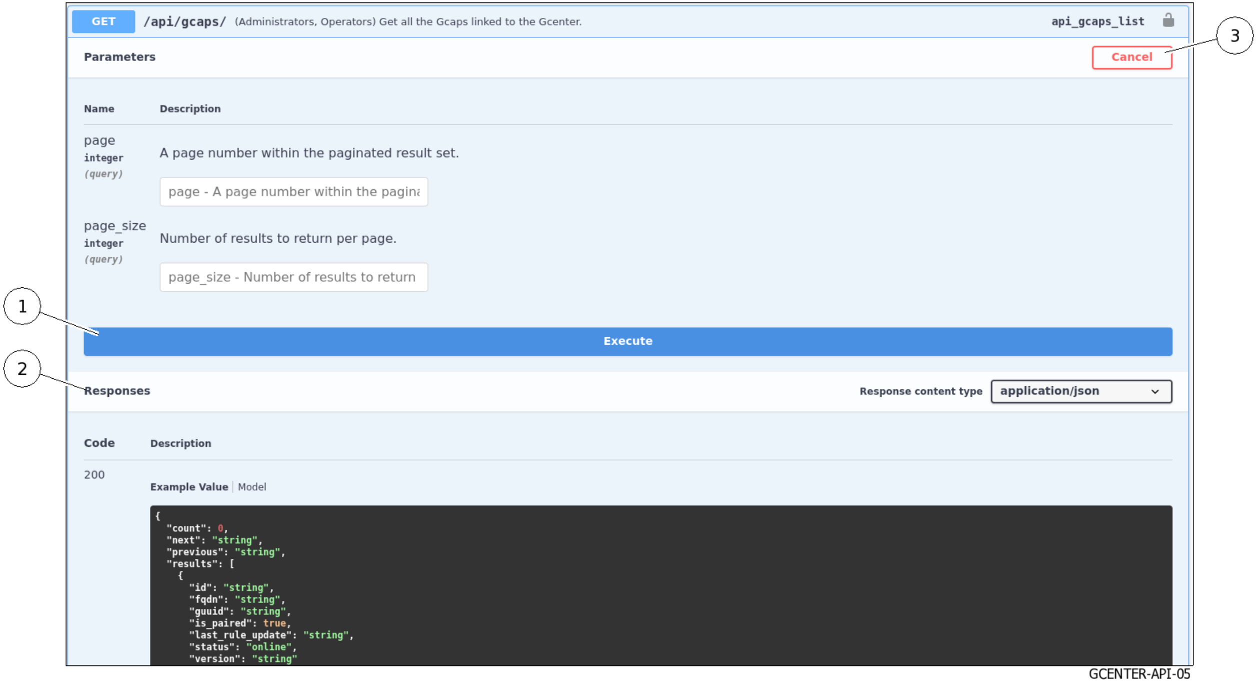
```
{
  count*                integer
  next                  string($uri)
                        x-nullable: true
  previous              string($uri)
                        x-nullable: true
  results*                [GcapReadOnly {
                           id                   string
                                                title: Id
                                                readOnly: true
                                                minLength: 1
                           fqdn*                string
                                                title: Fully Qualified Domain Name (FQDN)
                                                maxLength: 120
                                                minLength: 1

                                                The fqdn of the gcap

                           guuid                string
                                                title: GUUID (uuid v5 from FQDN)
                                                maxLength: 37
                                                minLength: 1
                           is_paired            boolean
                                                title: Is paired
                                                default: true

                                                Is the gcap paired ?

                           last_rule_update     string
                                                title: Last rule update
                                                readOnly: true
                                                maxLength: 200
```

GCENTER-API-02

**Astuce:**

For some endpoints, it is mandatory to enter parameters before running it.

- Click on the button (2) `Try it out`.
  The window is changed ...



GET /api/gcaps/ (Administrators, Operators) Get all the Gcaps linked to the Gcenter. api_gcaps_list

Parameters — Cancel

| Name | Description |
|---|---|
| page<br>integer<br>*(query)* | A page number within the paginated result set.<br>page - A page number within the pagin |
| page_size<br>integer<br>*(query)* | Number of results to return per page.<br>page_size - Number of results to return |

Execute

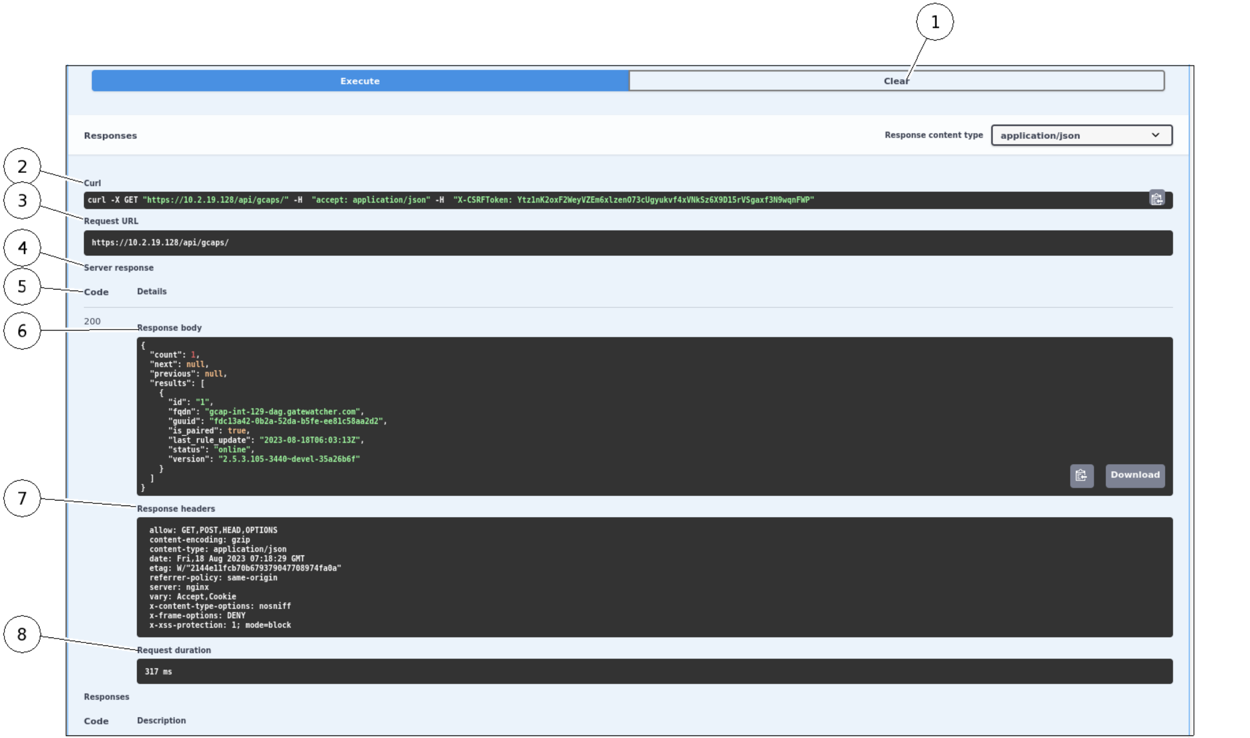
Responses — Response content type: application/json

| Code | Description |
|---|---|
| 200 | Example Value \| Model |

```
{
  "count": 0,
  "next": "string",
  "previous": "string",
  "results": [
    {
      "id": "string",
      "fqdn": "string",
      "guuid": "string",
      "is_paired": true,
      "last_rule_update": "string",
      "status": "online",
      "version": "string"
```

GCENTER-API-05

- Click on the button (1) `Execute`.
  The request is launched and the next window is displayed.



Execute | Clear

Responses — Response content type: application/json

Curl

```
curl -X GET "https://10.2.19.128/api/gcaps/" -H  "accept: application/json" -H  "X-CSRFToken: Ytz1nK2oxF2WeyVZEm6xlzen073cUgyukvf4xVNkSz6X9D15rVSgaxf3N9wqnFWP"
```

Request URL

```
https://10.2.19.128/api/gcaps/
```

Server response

| Code | Details |
|---|---|
| 200 | Response body |

```
{
  "count": 1,
  "next": null,
  "previous": null,
  "results": [
    {
      "id": "1",
      "fqdn": "gcap-int-129-dag.gatewatcher.com",
      "guuid": "fdc13a42-0b2a-52da-b5fe-ee81c58aa2d2",
      "is_paired": true,
      "last_rule_update": "2023-08-18T06:03:13Z",
      "status": "online",
      "version": "2.5.3.105-3440~devel-35a26b6f"
    }
  ]
}
```

Download

Response headers

```
allow: GET,POST,HEAD,OPTIONS
content-encoding: gzip
content-type: application/json
date: Fri,18 Aug 2023 07:18:29 GMT
etag: W/"2144e11fcb70b679379047708974fa0a"
referrer-policy: same-origin
server: nginx
vary: Accept,Cookie
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

Request duration

```
317 ms
```

Responses

| Code | Description |
|---|---|

GCENTER-API-06

This window has several zones:

- The display zone (2) `Curl` for the Curl query

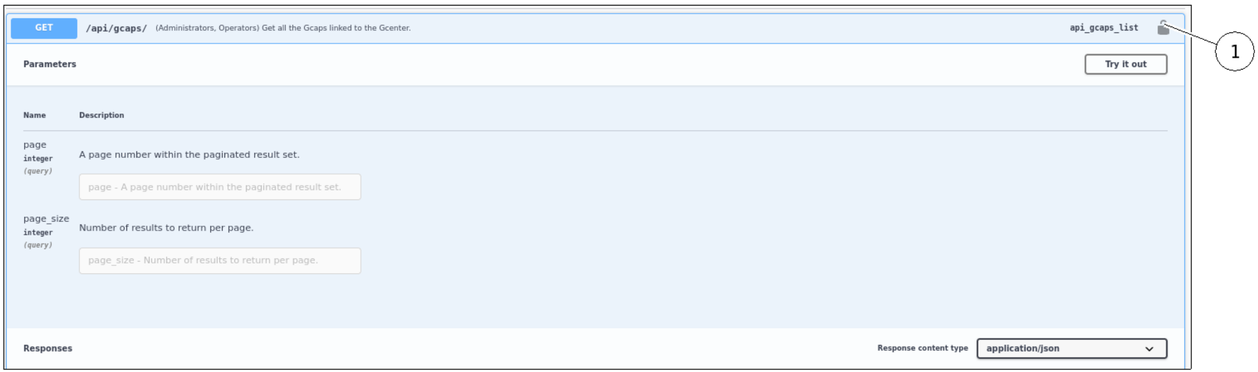
- Display zone (3) `URL` for URL request
- Zone (4) `Server response`:
    - The Return `Code` (5):
        - If the code is set to `200` then the execution has been completed correctly.
        - If the message `code 400 Undocumented Error Bad Request` is displayed, verify that the required parameters are entered.
    - The body of the answer (6): refer to *Overview of the API interface*
    - The field detailing the answer header (7)
    - The value in ms of the query duration (8)
    - The `Download` button to download the corresponding .json file
- The `Responses` zone

  This zone displays different information depending on the use of the link `Model` or `Example Value`.
- Or the output model (`Model`): refer to *Overview of the API interface*
- An example of the answer in the expected field with values for example (`Example Value`): refer to *Overview of the API interface*

  The values are:
    - For integer type (value 0)
    - For type string (value = string)
    - For boolean type (value = true)

---

### 8.6.10.6 Procedure to modify the token associated with the request



/api/gcaps/ (Administrators, Operators) Get all the Gcaps linked to the Gcenter.

api_gcaps_list

Parameters

| Name | Description |
|---|---|
| page<br>integer<br>*(query)* | A page number within the paginated result set.<br>page - A page number within the paginated result set. |
| page_size<br>integer<br>*(query)* | Number of results to return per page.<br>page_size - Number of results to return per page. |

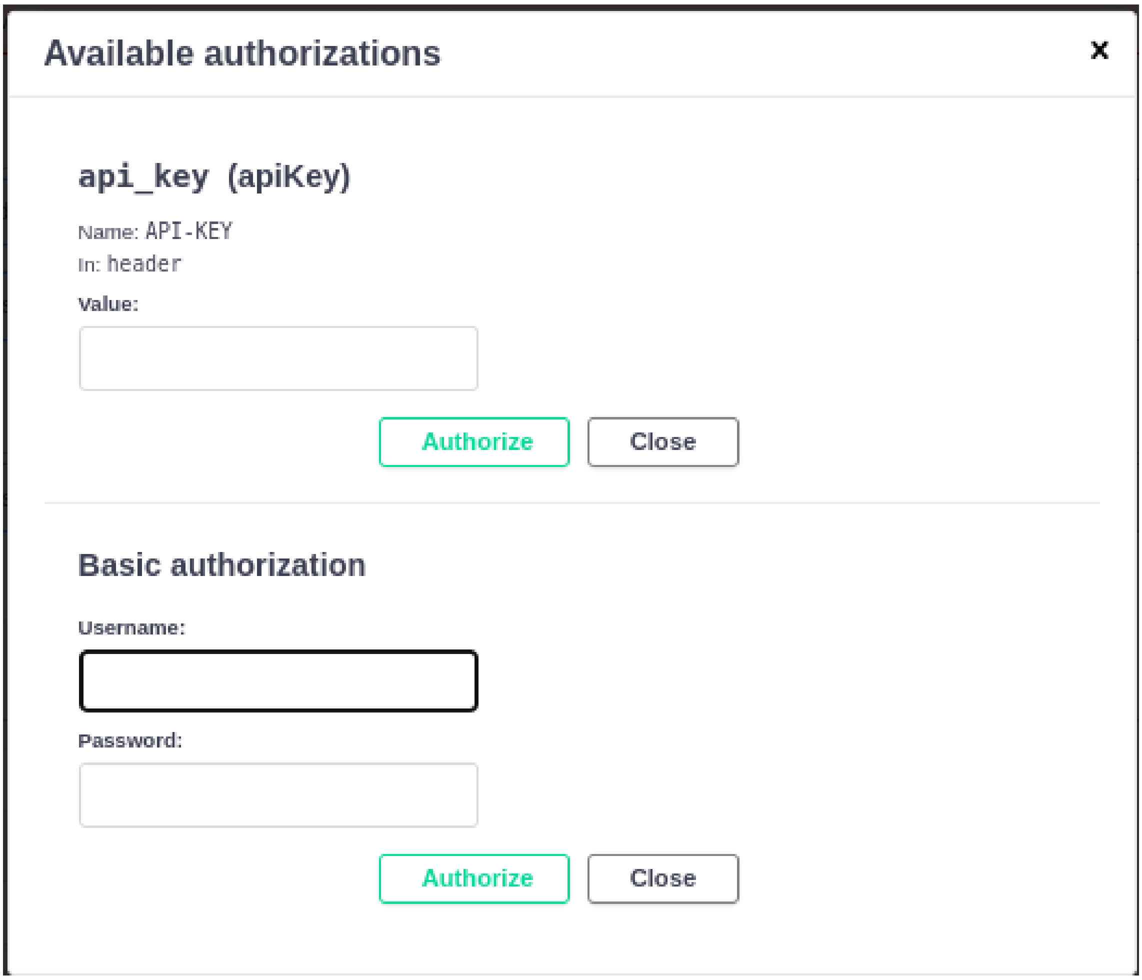
Responses

Response content type application/json

GCENTER-API-08

- Click the button (1).

  The `Available authorizations` window is displayed:


Available authorizations

api_key (apiKey)

Name: API-KEY

In: header

Value:

Basic authorization

Username:

Password:

There are two options:

  – Or the use of an apikey (token previously created)
  – Or the use of an authorization by name and password of an account previously created

- To use an apikey (token previously created):

  - Paste the token in the `value` field
  - Validate by clicking on the `Authorize` field
  - Close window with the `Close` field

> **Note:**
>
> The token can have a limited life: see *The `API Keys` section of the `Accounts` submenu*.

- To use an authorization:

- Click in the `Username field

  The list of existing accounts is displayed.
- Enter the account password
- Validate by clicking on the `Authorize` field
- Close window with the `Close` field

# 8.7 Managing user accounts

## 8.7.1 Creating local users

### 8.7.1.1 Introduction

This procedure describes how to create a new GCenter user.
To do this, enter the following:

- Mandatory information - username and password
- Optional information - email address, first and last name
- Select membership of existing groups - Operator, Administrator
- Enable or disable this new user

**Note:**

See the presentation of the accounts and groups described in the *Web interface accounts and their management*.
This graphical interface is described in *The `Users management` section of the `Accounts` submenu*.

---

### 8.7.1.2 Prerequisites

- User : member of **Administrator** group

---

### 8.7.1.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

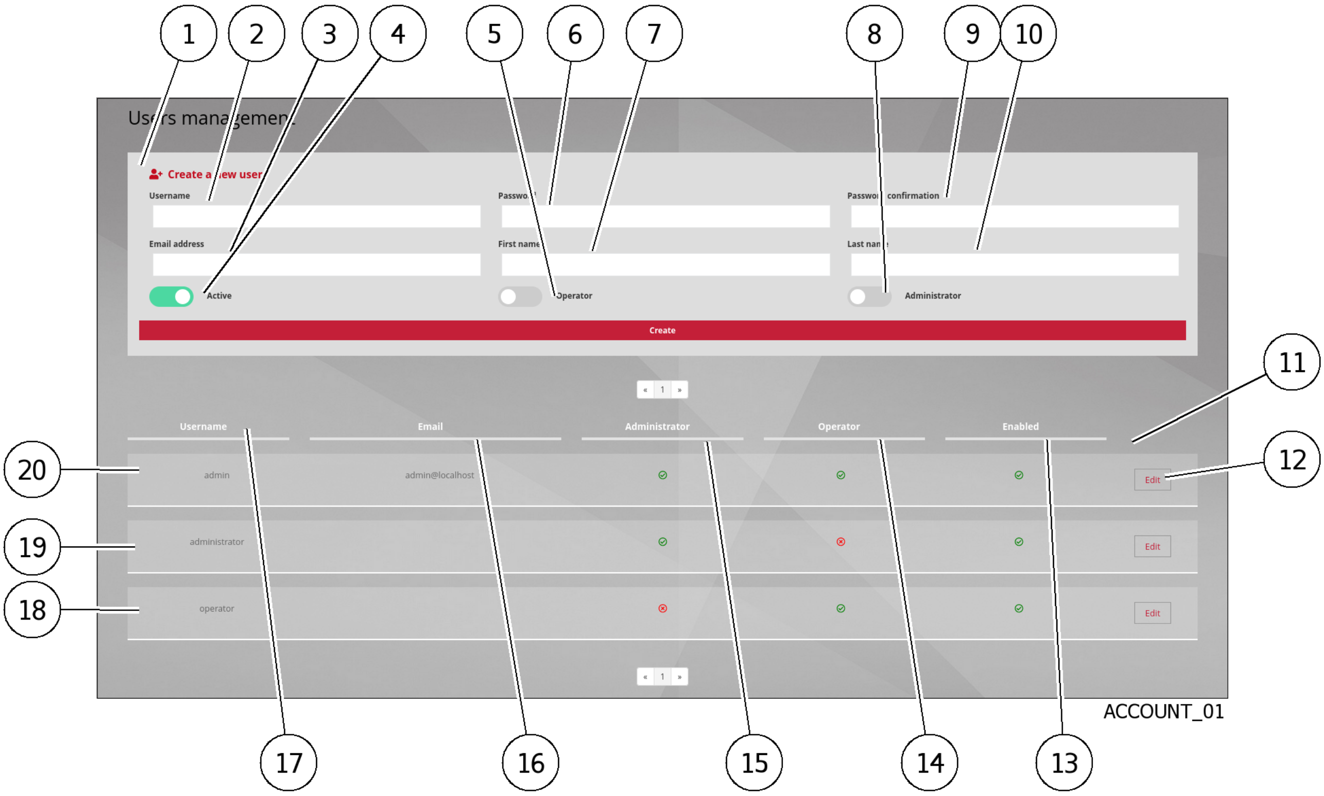
---

### 8.7.1.4 Procedure to access the `Users management` screen

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Accounts` command
  The `Accounts` window is displayed.
- Click on the `Users management` heading.
  The `Users Management` window is displayed.

---

### 8.7.1.5 Procedure to create a new user



Users management

Create a new user

Username

Password

Password confirmation

Email address

First name

Last name

Active

Operator

Administrator

Create

| Username | Email | Administrator | Operator | Enabled | |
|---|---|---|---|---|---|
| admin | admin@localhost | ✓ | ✓ | ✓ | Edit |
| administrator | | ✓ | ✗ | ✓ | Edit |
| operator | | ✗ | ✓ | ✓ | Edit |

- In the `Create a new user` field (1), enter the following information:

- The full name of the new user in the `Username` field (2)
  It may contain only letters, numbers, and [@/./+/-/-/_.] characters
- In the field `Email address` (3), the email address: optional field
- In the `First name` field (7), the user's first name: optional field
- In the field `Last name` (10), the user's last name: optional field

- Choose the rights thus the membership to the group(s):

- `Operator` with the selector (5)
- `Administrator` with selector (8)

- Enter the password. To do this:

  - Enter it in the `Password` field (6)
  - Enter it again in the `Password confirmation` field (9)
    The password entered must match the *Password management policy*.
    The system checks the password against the verification policy.
    If the password does not meet the verification policy, one of the following messages will be displayed:

    - `Password must contain 12 characters or more`: indicates a password that is too short
    - `Password must contain a capital letter`: indicates the lack of a capital
    - `Password must contain a lowercase letter`: indicates the lack of a small letter
    - `Password must contains a special character`: indicates the lack of a special character
    - `Password must contains a number`: indicates the lack of a number

    If the two passwords do not match, the following message is displayed: `The two password fields do not match.`

- Activate the account with the selector (4).

- Validate the entry with the `` `Create` `` button.
  After validation, the new user appears in the **Existing User Management Area (11)**.

---

## 8.7.2 Changing some of a local user's information

### 8.7.2.1 Introduction

This procedure describes how to modify local users:

- Email address
- First name
- Last name
- Membership of the `` `Operator` `` or / and `` `Administrator` `` groups
- Account enabling

**Note:**

See the presentation of the accounts and groups described in *Web interface accounts and their management*.
This graphical interface is described in *The `Users management` section of the `Accounts` submenu*.

---

### 8.7.2.2 Prerequisites

- User : member of **Administrator** group

---

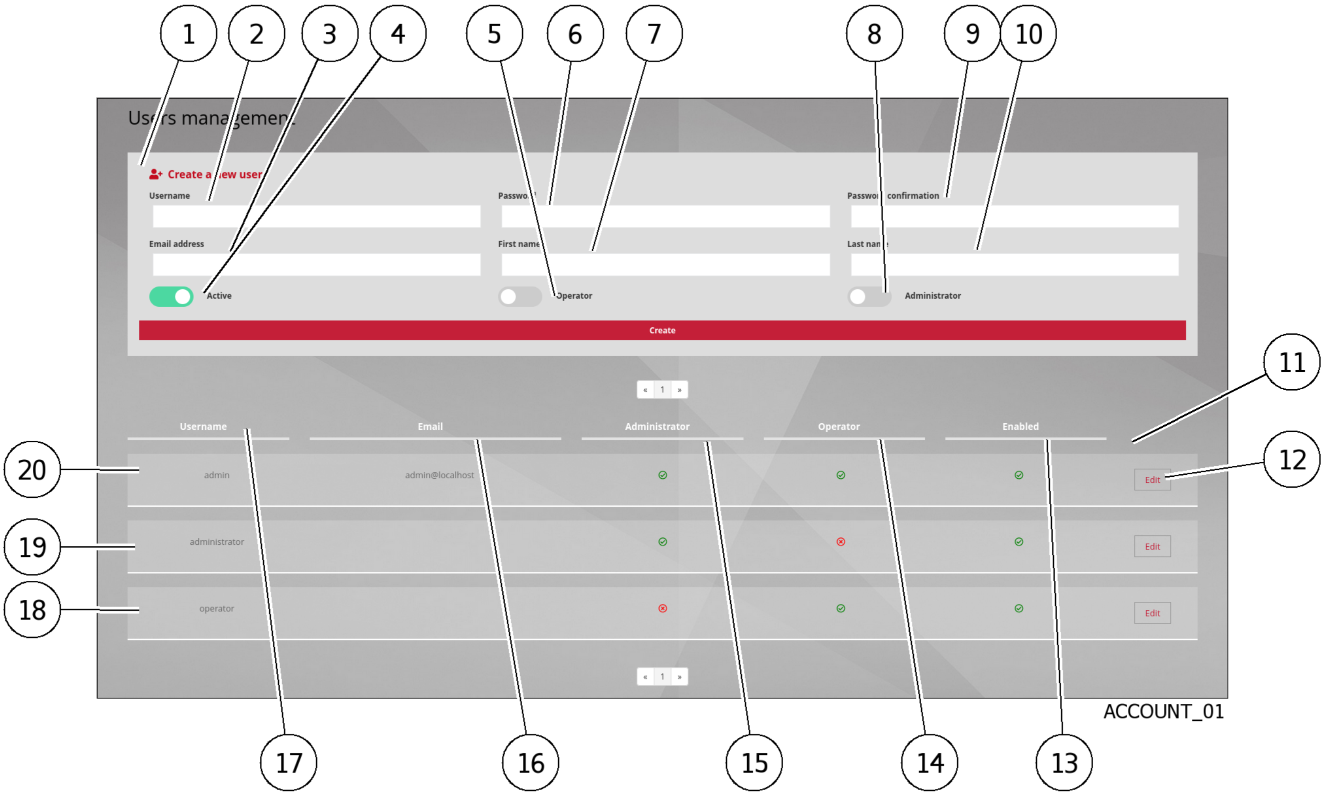
### 8.7.2.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

---

### 8.7.2.4 Procedure to access to the `` `Users management` `` window for an administrator account

- In the navigation bar, successively click on:
- The `` `Admin` `` button
- The `` `Gcenter` `` sub-menu
- The `` `Accounts` `` command
  The `` `Accounts` `` window is displayed.
- Click on the `` `Users management` `` heading.
  The `` `Users Management` `` window is displayed.

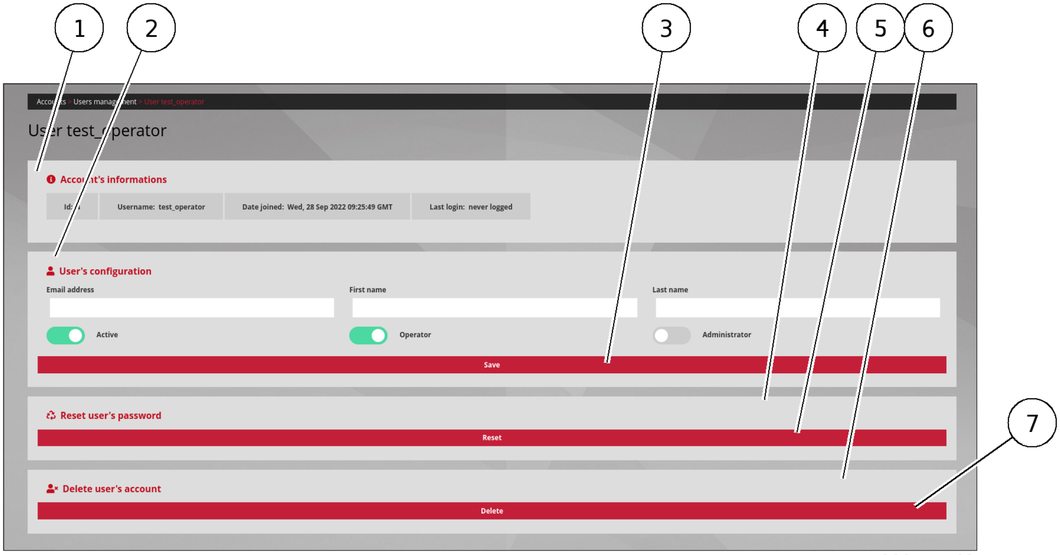


| Username | Email | Administrator | Operator | Enabled | |
|---|---|---|---|---|---|
| admin | admin@localhost | ✓ | ✓ | ✓ | Edit |
| administrator | | ✓ | ⊗ | ✓ | Edit |
| operator | | ⊗ | ✓ | ✓ | Edit |

ACCOUNT_01

- In the **Existing user management area** (11), click on the `Edit` button (12) of the user whose settings are to be changed.

  The `User ...` window is displayed.



Id: 4 | Username: test_operator | Date joined: Wed, 28 Sep 2022 09:25:49 GMT | Last login: never logged

ACCOUNT_02

The `Account's information` area (1) shows account information such as ID, username, creation date, last login, and admin group membership.

#### 8.7.2.5 Procedure to change certain user information

In the `User's configuration` area (2):

- Enter or modify the data found in:

- in the `Email address` field
- in the `First name` field
- in the `Last name` field

- Change the rights if necessary via the `Operator` and `Administrator` selectors.
- Change the account status if required with the `Active` selector.
- Confirm the changes using the `Save` button (3).

---

### 8.7.3 Resetting a local user's password

#### 8.7.3.1 Introduction

This procedure describes how to reset the current user's password.

**Note:**

See the presentation of the accounts and groups described in *Web interface accounts and their management*.
This graphical interface is described in *The `Users management` section of the `Accounts` submenu*.

**Note:**

This procedure enables the password associated with the user account to be regenerated if it is lost or forgotten.
The system will propose a new password.

**Danger:**

It is possible to select your own account!
If this is voluntary, carefully note the password displayed.

---

#### 8.7.3.2 Prerequisites

- User : member of **Administrator** group

---

### 8.7.3.3 Preliminary operations

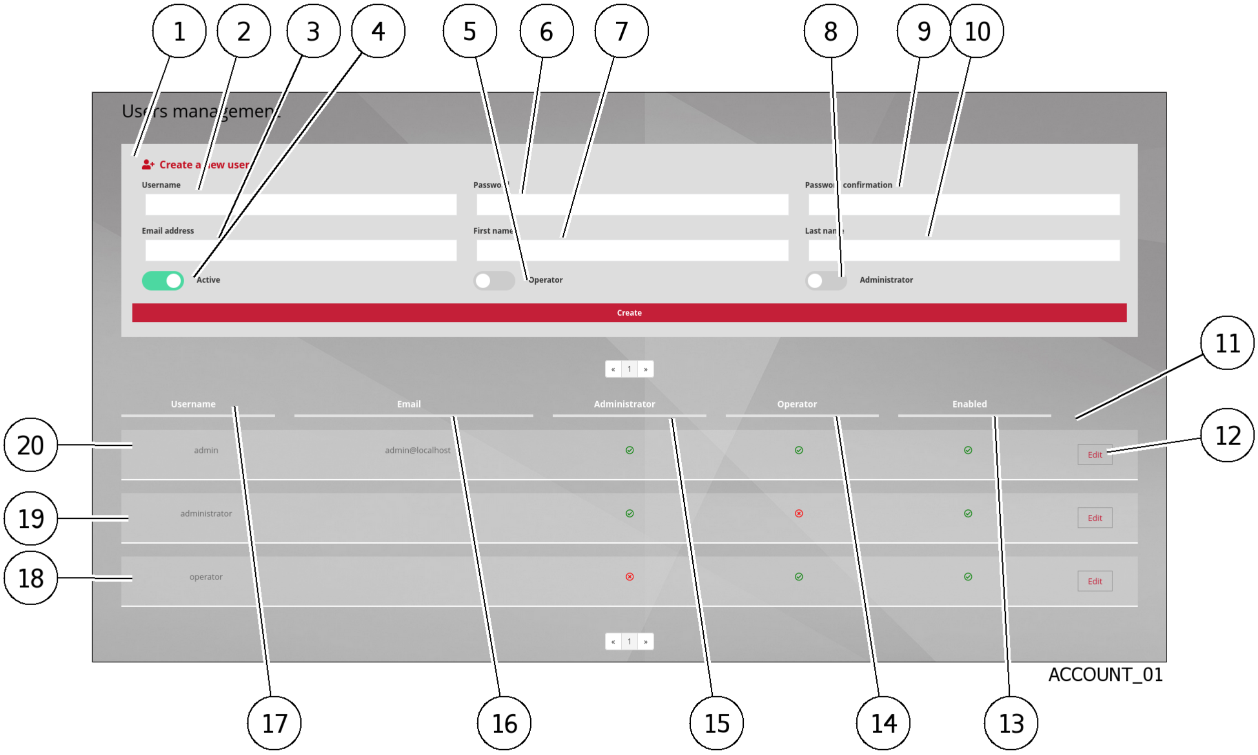
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

### 8.7.3.4 Procedure to access to the `Users management` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Accounts` command

  The `Accounts` window is displayed.
- Click on the `Users management` heading.

  The `Users Management` window is displayed.

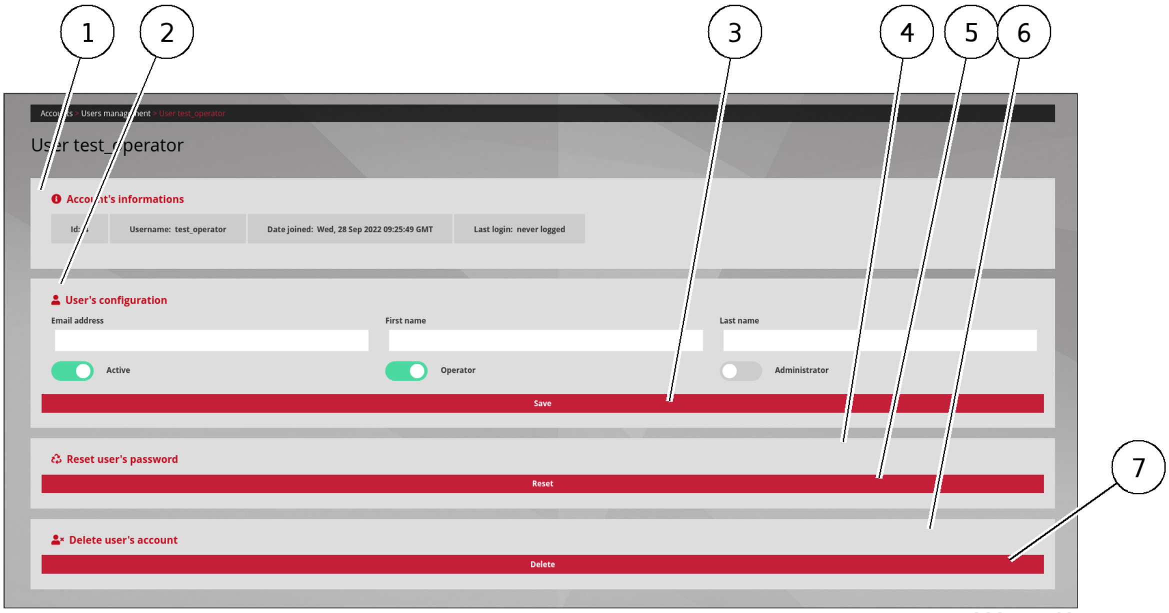


| Username | Email | Administrator | Operator | Enabled | |
|---|---|---|---|---|---|
| admin | admin@localhost | ✓ | ✓ | ✓ | Edit |
| administrator | | ✓ | ⊗ | ✓ | Edit |
| operator | | ⊗ | ✓ | ✓ | Edit |

ACCOUNT_01

- In the Existing user management area (11), click on the `Edit` button of the user.

  The `User ...` window is displayed.



Accounts > Users management > User test_operator

User test_operator

Account's informations

Id:
Username: test_operator
Date joined: Wed, 28 Sep 2022 09:25:49 GMT
Last login: never logged

User's configuration

Email address
First name
Last name

Active
Operator
Administrator

Save

Reset user's password

Reset

Delete user's account

Delete

ACCOUNT_02

### 8.7.3.5 Procedure to reset a user's password

**Note:**

This procedure enables the password associated with the user account to be regenerated if it is lost or forgotten.

The system will propose a new password.

- Select the user's account.
- Click the `Reset` button (5) in the Reset user's password area (4).
  The following message is displayed: `Password changed to xxxxxx. Please, ask your user to change it to a new one at the next login (safety first)!`
- Contact the user and inform them of their new password.
  Please ask your user to change it to a new one at the next login.

## 8.7.4 Deleting a local user

### 8.7.4.1 Introduction

This procedure describes how to delete a local user.

**Note:**

See the presentation of the accounts and groups described in *Web interface accounts and their management*.

This graphical interface is described in *The `Users management` section of the `Accounts` submenu*.

### 8.7.4.2 Prerequisites

- User : member of **Administrator** group

---

### 8.7.4.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

---

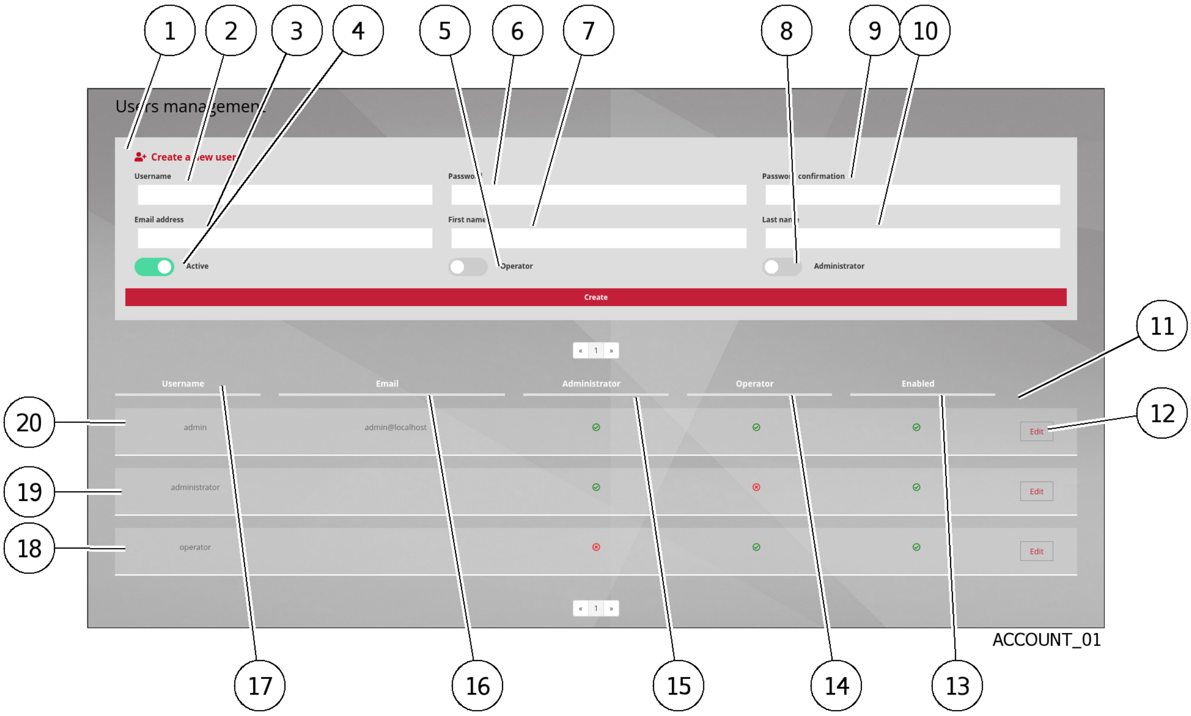
### 8.7.4.4 Procedure to access the `Users management` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Accounts` command

  The `Accounts` window is displayed.

- Click on the `Users management` heading.

  The `Users Management` window is displayed.



Users management

Create a new user

Username

Password

Password confirmation

Email address

First name

Last name

Active

Operator

Administrator

Create

« 1 »

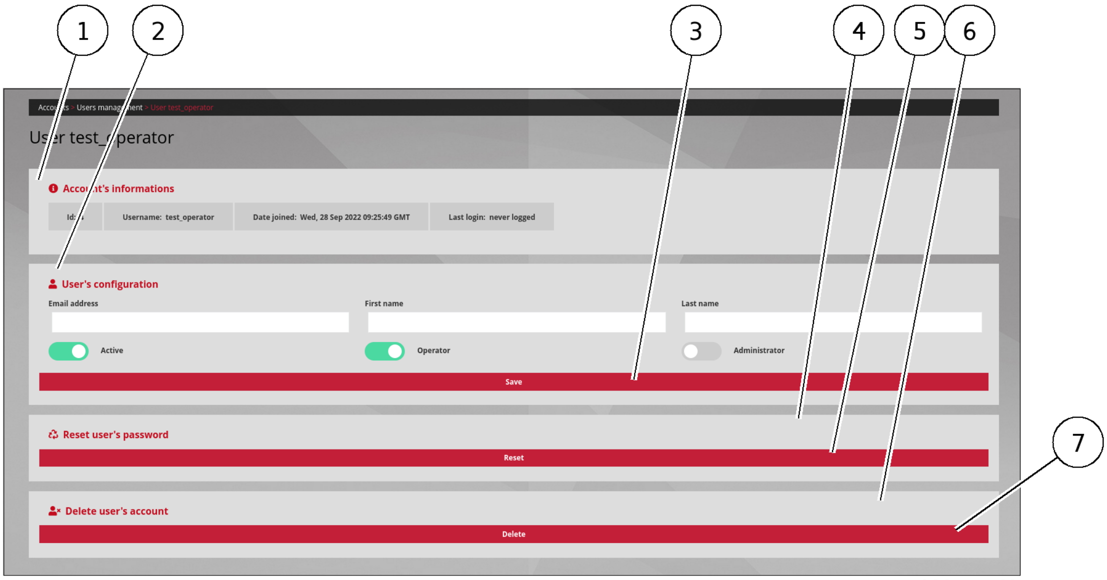
| Username | Email | Administrator | Operator | Enabled | |
|---|---|---|---|---|---|
| admin | admin@localhost | ✓ | ✓ | ✓ | Edit |
| administrator | | ✓ | ✗ | ✓ | Edit |
| operator | | ✗ | ✓ | ✓ | Edit |

« 1 »

ACCOUNT_01

- In the Existing user management area (11), click on the `Edit` button (12) of the user.

  The `User ...` window is displayed.



Accounts > Users management > User test_operator

User test_operator

Account's informations

Id: | Username: test_operator | Date joined: Wed, 28 Sep 2022 09:25:49 GMT | Last login: never logged

User's configuration

Email address

First name

Last name

Active

Operator

Administrator

Reset user's password

Delete user's account

ACCOUNT_02

### 8.7.4.5 Procedure to delete a new user

> **Danger:**
>
> It is possible to select your own account! If this is voluntary, carefully note the password displayed.

- Select the user's account.
- Click the `Delete` button (7) in the `Delete user's account` area (6).
  A message is displayed indicating that the account was deleted.
  The list of accounts is updated.

## 8.7.5 Displaying of the connection status between the GCenter and the LDAP server

### 8.7.5.1 Introduction

This procedure enables displaying the connection status between the GCenter and the LDAP/ActiveDirectory server.

> **Note:**
>
> This graphical interface is described in *The `LDAP configuration` section of the `Accounts` submenu*.

#### 8.7.5.2 Prerequisites

- User : member of **Administrator** group

---

#### 8.7.5.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

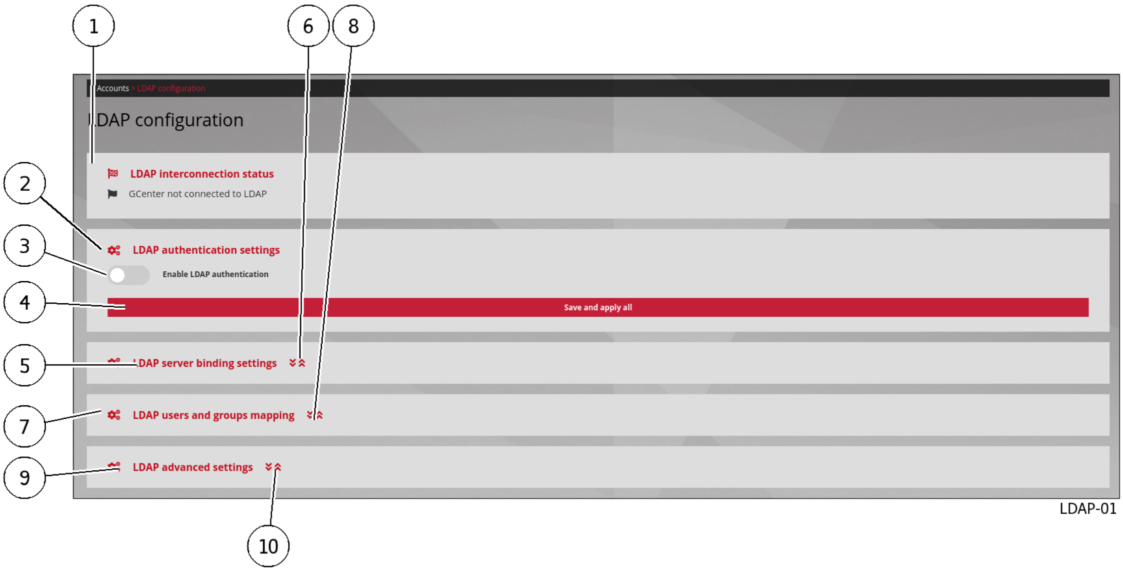
---

#### 8.7.5.4 Procedure to access to the `LDAP configuration` window for an administrator account

- In the navigation bar, successively click on:

- The `Admin` button
- The `Gcenter` sub-menu
- The `Accounts` command
  The `Accounts` window is displayed.

- Click on the `LDAP configuration` heading.
  The `LDAP configuration` window is displayed.



Accounts > LDAP configuration

LDAP configuration

LDAP interconnection status

GCenter not connected to LDAP

LDAP authentication settings

Enable LDAP authentication

Save and apply all

LDAP server binding settings

LDAP users and groups mapping

LDAP advanced settings

---

#### 8.7.5.5 Procedure to view the status

- In the `LDAP interconnection status` (1) area, view the connection status message.
  For example, if the connection is not effective, the message `GCenter not connected to LDAP` is displayed.

---

## 8.7.6 Enable the connection between the GCenter and the LDAP server

### 8.7.6.1 Introduction

This procedure enables the connection and thus the authentication by the LDAP/ActiveDirectory server.

> **Note:**
>
> This graphical interface is described in *The `LDAP configuration` section of the `Accounts` submenu*.

---

### 8.7.6.2 Prerequisites

- User : member of **Administrator** group

---

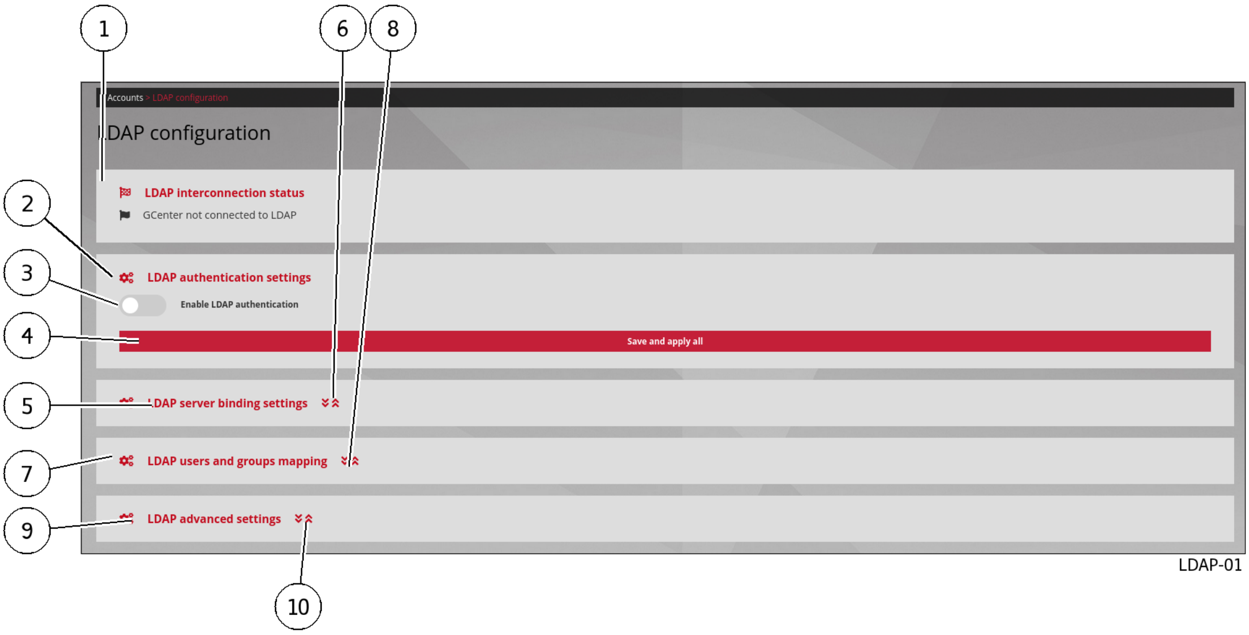
### 8.7.6.3 Preliminary operations

- Configure the LDAP server settings (see the *Configuring the connection between the GCenter and the LDAP server*).
- Set up users and groups (see the *Configuring the users and groups defined on LDAP / ActiveDirectory*).

---

### 8.7.6.4 Procedure to enable the LDAP functionality

The `LDAP configuration` window is displayed.


1
6
8
Accounts > LDAP configuration
LDAP configuration
2
LDAP interconnection status
3
LDAP authentication settings
Enable LDAP authentication
4
Save and apply all
5
LDAP server binding settings
7
LDAP users and groups mapping
9
LDAP advanced settings
10

GCenter not connected to LDAP

LDAP-01

In the `LDAP authentication settings` area (2):

- Use the `Enable LDAP authentication` selector.
- Click on the `Save and apply all` button (4).

A Warning window is displayed with the message `Saving and applying the new LDAP settings will restart the application and disconnect all users!`

- Click on the `Confirm` button.

**Note:**

The current session is disconnected when the LDAP configuration is applied.

---

### 8.7.7 Configuring the connection between the GCenter and the LDAP server

#### 8.7.7.1 Introduction

This procedure enables setting up the LDAP server using:

- The `LDAP server binding settings` area
- The `LDAP users and groups mapping` area

This area enables entering the connection information to a remote authentication server.

**Note:**

This graphical interface is described in *The `LDAP configuration` section of the `Accounts` submenu*.

---

#### 8.7.7.2 Prerequisites

- User : member of **Administrator** group

---

#### 8.7.7.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

---

#### 8.7.7.4 Procedure to access to the `LDAP configuration` window for an administrator account

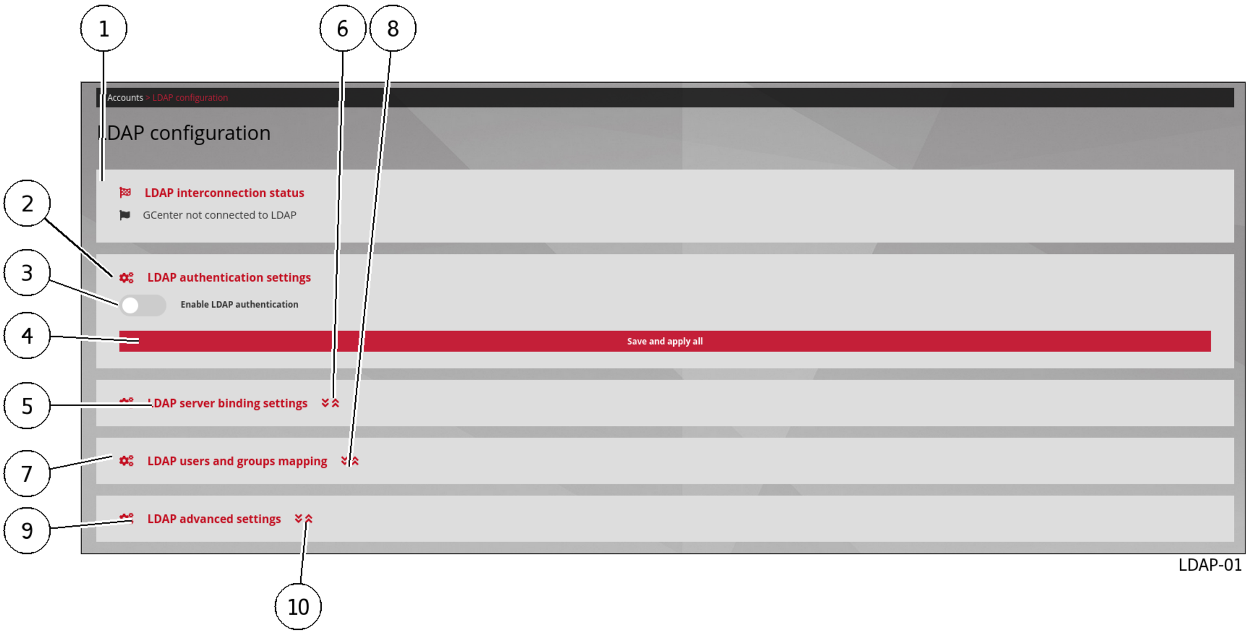
- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Accounts` command

  The `Accounts` window is displayed.
- Click on the `LDAP configuration` heading.

  The `LDAP configuration` window is displayed.

---

### 8.7.7.5 Procedure to change the settings for the `LDAP server binding settings` area (5)


1
6
8
2
3
4
5
7
9
10
Accounts > LDAP configuration
LDAP configuration
LDAP interconnection status
GCenter not connected to LDAP
LDAP authentication settings
Enable LDAP authentication
Save and apply all
LDAP server binding settings
LDAP users and groups mapping
LDAP advanced settings
LDAP-01

- Expand the window to access the parameters using the arrows (6).
- Enter the following parameters:

| Field | Required | Description | Value |
|---|---|---|---|
| `Enable anonymous binding` | No | Enables not having to enter the login password | On/Off |
| `LDAP protocol` | Yes | Enables choosing the protocol used for the connection | ldap:// ou ldaps:// |
| `LDAP hostname` | Yes | Enables specifying the IP address or name of the remote server | ip or fqdn |
| `LDAP port` | Yes | Enables specifying the port of the remote server | 389 for ldap or 636 for ldaps for example |
| `Output interface` | Yes | Enables selecting the GCenter interface through which to communicate with the remote server | mgmt0 by default |
| `LDAP binding DN` | No | Enables specifying the user name for connecting to the remote server | user name |
| `LDAP binding password` | No | Enables specifying the user's password for connecting to the remote server | user's password |

**Note:**

If the `Enable anonymous binding` option is enabled, it is not necessary to fill in the username and password.

- Save the changes with the `Save and apply` button.
  Warning window is displayed with the message `Saving and applying the new LDAP settings will restart the application and disconnect all users!`.
- Click on the `Confirm` button.

#### 8.7.7.6 Procedure to change the settings for the `LDAP advanced settings` area (9)

- Expand the window to access the parameters using the arrows (8).
- Enter the following parameters:

| Field | Required | Description | Value |
|---|---|---|---|
| `First name` | Yes | Enables specifying the LDAP parameter for the first name of the users | by default : givenName |
| `Last name` | Yes | Enables specifying the LDAP parameter for the last name of the users | by default : sn |
| `Email` | Yes | Enables specifying the LDAP setting for the user's email | by default : mail |
| `User to group mapping` | Yes | Enables entering an LDAP query to help the GCenter find the groups a user belongs to | by default : see in the interface |
| `LDAP version` | Yes | Enables to choose the LDAP version of the remote server | by default : Version 3 |
| `LDAP version` | Yes | Enables choosing the LDAP version of the remote server | by default: Version 3 |
| `Enable StartTLS protocol` | Yes | Enables or disables the StartTLS protocol | by default: disable |
| `Disable checking the certificate validity when using TLS` | Yes | Enables or disables certificate validity checking (LDAPS) | by default: disable |
| `Custom CA` | No | Displays the current certificate in use | depends on the last loaded certificate |
| `Update custom CA` | No | Enables loading a certificate for LDAPS use | depends on the last certificate choosen |
| `LDAP timeout` | Yes | Enables specifying the waiting time for LDAP queries | 2 |
| `Network timeout` | Yes | Enables specifying the waiting time at the LDAP communications network level | 2 |
| `Cache timeout` | Yes | Enables specifying the waiting time for LDAP users and groups | 300 |

- Save the changes with the `Save and apply` button.
  Warning window is displayed with the message `Saving and applying the new LDAP settings will restart the application and disconnect all users!`.
- Click on the `Confirm` button.

**Note:**

To configure the LDAPS:

- Enter in `LDAP server binding settings`:
  - `LDAP protocol`: *ldaps://*
  - `LDAP_port`: *636*
- Enter the certificate of the certification authority in `LDAP advanced settings`.

**Note:**

To configure LDAP over TLS:

- Enter the certificate of the certification authority in `LDAP advanced settings`
- Tick the `Enable StartTLS` box in `LDAP advanced settings`

## 8.7.8 Configuring the users and groups defined on LDAP / ActiveDirectory

### 8.7.8.1 Introduction

This procedure enables specifying the mapping of users and groups between the GCenter and the remote authentication server.

> **Note:**
>
> This graphical interface is described in *The `LDAP configuration` section of the `Accounts` submenu*.

---

### 8.7.8.2 Prerequisites

- User : member of **Administrator** group

---

### 8.7.8.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

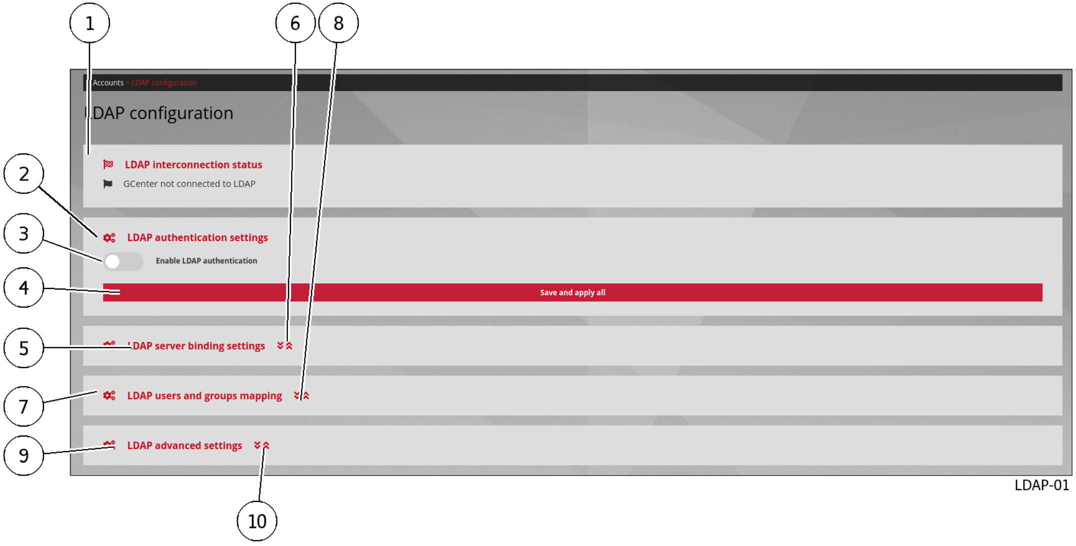
---

### 8.7.8.4 Procedure to access to the `LDAP configuration` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Accounts` command

  The `Accounts` window is displayed.
- Click on the `LDAP configuration` heading.

  The `LDAP configuration` window is displayed.


1
6
8
Accounts > LDAP configuration
LDAP configuration
2
LDAP interconnection status
GCenter not connected to LDAP
3
LDAP authentication settings
Enable LDAP authentication
4
Save and apply all
5
LDAP server binding settings
7
LDAP users and groups mapping
9
LDAP advanced settings
LDAP-01
10

---

#### 8.7.8.5 Procedure to change the settings for the `LDAP users and groups mapping` area (7)

- Expand the window to access the parameters using the arrows (8).
- Enter the following parameters:

| Field | Required | Description | Value |
|---|---|---|---|
| `User search scope` | Yes | Enables specifying where to search for users in the remote directory in the remote directory | by default:<br>DC=example, DC=com |
| `User search criteria` | Yes | Enables specifying the search criteria for users in the remote directory | by default: *(\|(uid=%(user)s)*<br>*(sAMAccountName=%(user)s))* |
| `Group search scope` | Yes | Enables specifying where to search for groups in the remote directory | by default: DC=example, DC=com |
| `Group search criteria` | Yes | Enables specifying the search criteria for groups in the remote directory | by default:<br>(objectClass=organizationalUnit |
| `LDAP to gcenter administrators group mapping` | Yes | Enables specifying which groups will have the "administrator" role | groups of administrators for example |
| `LDAP to gcenter operators group mapping` | Yes | Enables specifying which groups will have the "operator" role | groups of analysts for example |

**Note:**

The same group can be present in both the `LDAP to gcenter administrators group mapping` and `LDAP to gcenter operators group mapping` fields.

- Save the changes with the `Save and apply` button.

---

### 8.7.9 Viewing the authentication history

#### 8.7.9.1 Introduction

This procedure enables viewing the history of all authentications on the GCenter.

**Note:**

This graphical interface is described in *The `Authentications history` section of the `Accounts` submenu*.

---

### 8.7.9.2 Prerequisites

- User : member of **Administrator** group

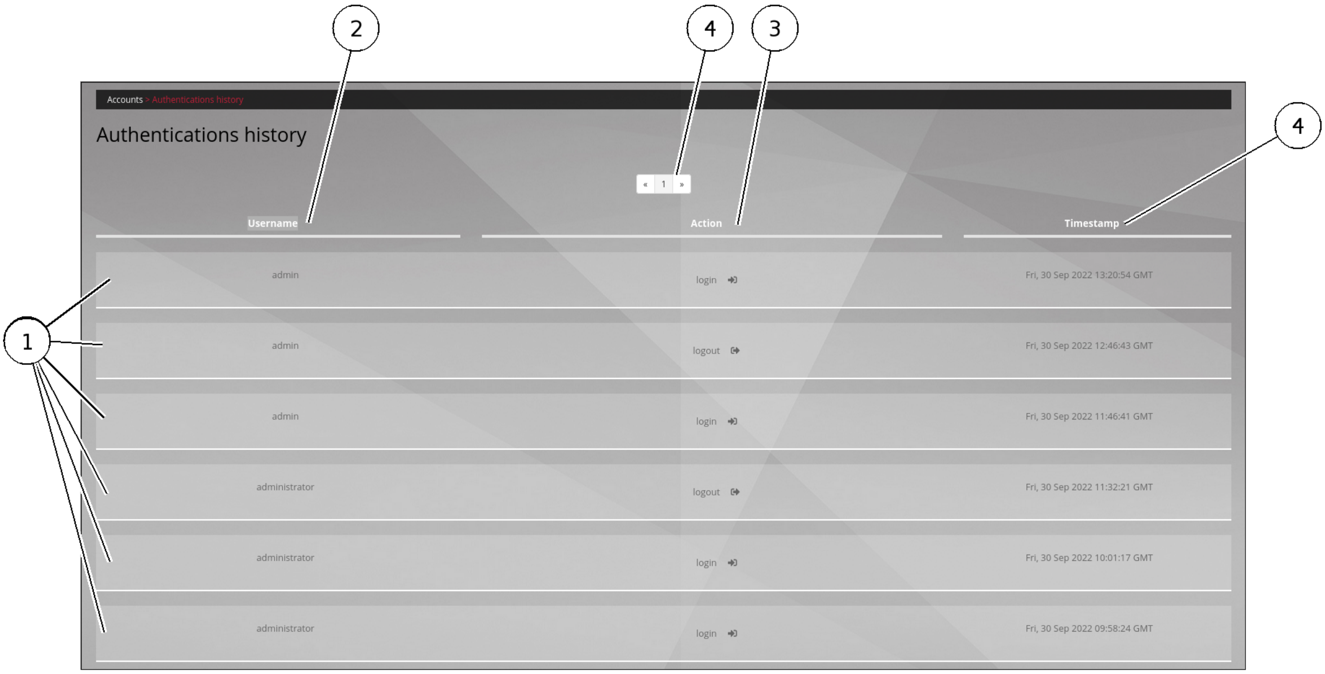
### 8.7.9.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*).

### 8.7.9.4 Procedure to access to the `Authentications history` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Accounts` command
  The `Accounts` window is displayed.
- Click on the `Authentications history` heading.
  The `Authentications history` is displayed.

### 8.7.9.5 Procedure



Accounts > Authentications history

Authentications history

« 1 »

| Username | Action | Timestamp |
|---|---|---|
| admin | login | Fri, 30 Sep 2022 13:20:54 GMT |
| admin | logout | Fri, 30 Sep 2022 12:46:43 GMT |
| admin | login | Fri, 30 Sep 2022 11:46:41 GMT |
| administrator | logout | Fri, 30 Sep 2022 11:32:21 GMT |
| administrator | login | Fri, 30 Sep 2022 10:01:17 GMT |
| administrator | login | Fri, 30 Sep 2022 09:58:24 GMT |

AUTHENT-01

This window displays the connections (1) in order from most recent to oldest.
For each connection, the following information is displayed:

- `Username` field (2): name of the person authenticated
- `Action` field (3): login or logout

- `timestamp` field (4) : date and time of login / logout in the format (**dd** , **mm yyyy hh**: **mm**: **ss**)
- To change pages, use the arrows (4).

## 8.7.10 Viewing the history of user creations or deletions

### 8.7.10.1 Introduction

This procedure enables viewing the history of:

- Each user account creation
- Each deletion of a user account

**Note:**

This graphical interface is described in *The `Creations/Deletions history` section of the `Accounts` submenu*.

### 8.7.10.2 Prerequisites

- User : member of **Administrator** group

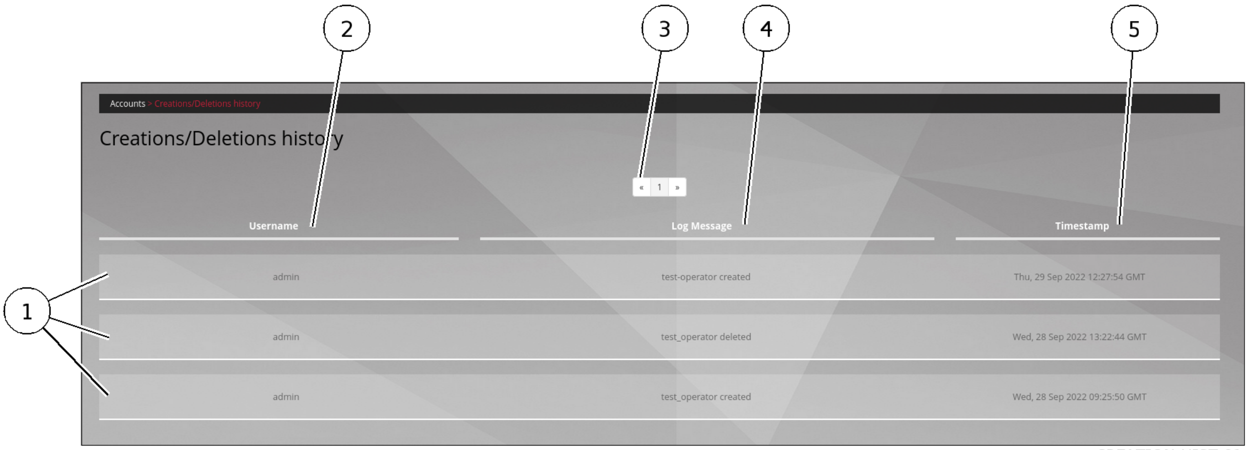
### 8.7.10.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

### 8.7.10.4 Procedure to access to the `Creations/Deletions history` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Accounts` command
  The `Accounts` window is displayed.
- Click on the `Creations/Deletions history` heading.
  The `Creations/Deletions history` is displayed.

#### 8.7.10.5 Procedure


Accounts > Creations/Deletions history
Creations/Deletions history
« 1 »
1
2
3
4
5

| Username | Log Message | Timestamp |
|---|---|---|
| admin | test-operator created | Thu, 29 Sep 2022 12:27:54 GMT |
| admin | test_operator deleted | Wed, 28 Sep 2022 13:22:44 GMT |
| admin | test_operator created | Wed, 28 Sep 2022 09:25:50 GMT |

CREATION-HIST-01

The `` `Creations/Deletions history` `` window displays the history of all GCenter users created or deleted.
This window displays the creations or deletions (1) in order from most recent to oldest.
For each connection, the following information is displayed:

- `` `Username` `` field (2): name of the person who created the account
- `` `Log Message` `` field (4): the account name created or deleted
- `` `timestamp` `` field (5): date and time of changes to the format (**dd** , **mm yyyy hh**: **mm**: **ss**)
- To change pages, use the arrows (3).

## 8.7.11 Viewing the history function for all changes in user rights

#### 8.7.11.1 Introduction

This procedure enables viewing the history function for all changes in user rights.
This results in changing the membership of the operator or administrator group.

> **Note:**
>
> This graphical interface is described in *The `Permissions history` section of the `Accounts` submenu*.

#### 8.7.11.2 Prerequisites

- User : member of **Administrator** group

### 8.7.11.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

---

### 8.7.11.4 Procedure to access to the `Permissions history` window for an administrator account

- In the navigation bar, successively click on:

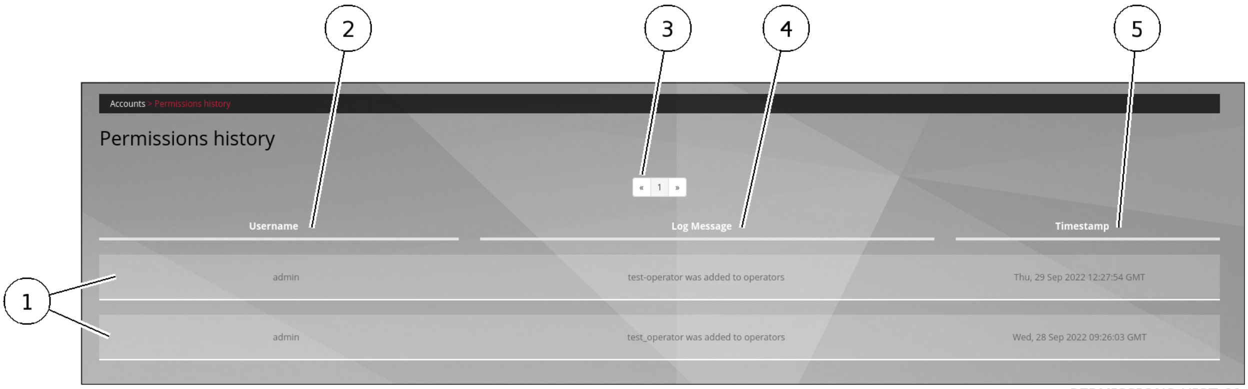
- The `Admin` button
- The `Gcenter` sub-menu
- The `Accounts` command
  The `Accounts` window is displayed.

- Click on the `Permissions history` heading.
  The `Permissions history` is displayed.

---

### 8.7.11.5 Procedure

The `Permissions history` window displays the history of all user rights changes.



Permissions history

| Username | Log Message | Timestamp |
|---|---|---|
| admin | test-operator was added to operators | Thu, 29 Sep 2022 12:27:54 GMT |
| admin | test_operator was added to operators | Wed, 28 Sep 2022 09:26:03 GMT |

PERMISSIONS-HIST-01

This window displays the changes in rights (1) in order from most recent to oldest.
The arrows (3) enable loading the next page.
For each connection, the following information is displayed:

- `Username` field (2): the name of the administrator who changed the rights of the account
- `Log Message` field (4): the name of the account whose rights were changed and the modification made.
- `Timestamp` field (5) : date and time of changes to the format (**dd** , **mm yyyy hh**: **mm**: **ss**)

- To change pages, use the arrows (3).

---

## 8.7.12 Adding an API access token

### 8.7.12.1 Introduction

This procedure describes:

- The adding of an API access token
- The creation of this access token
- The possible deletion of an existing token

**Note:**

This graphical interface is described in *The `API Keys` section of the `Accounts` submenu*.

---

### 8.7.12.2 Prerequisites

- User : member of **Administrator** group

---

### 8.7.12.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

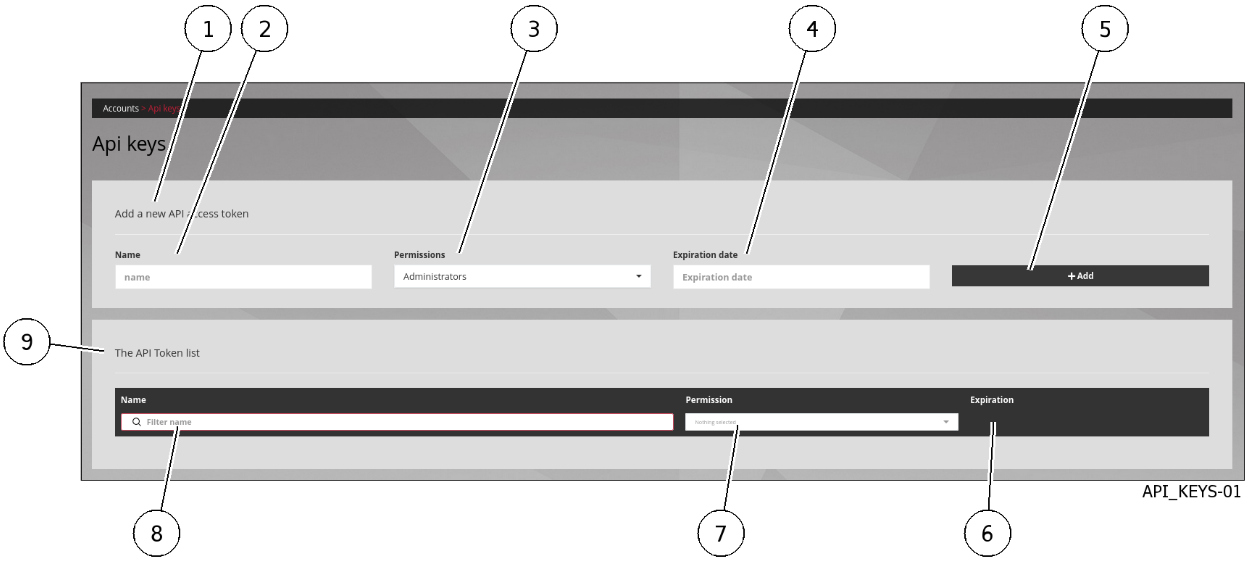
---

### 8.7.12.4 Procedure to access to the `Permissions history` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Accounts` command
  The `Accounts` window is displayed.
- Click on the `Api keys` heading.
  The `Api keys` window is displayed.

---

### 8.7.12.5 Procedure



API_KEYS-01

- Enter the name of the API in the `Name` field (2).
- Select the desired account, hence the rights, using the `Permissions` field (3).
- Select the expiration date by clicking on the `Expiration date` field (4): use the calendar displayed.
- Press the `Add` button (5).

  After adding:

  - a message that the token was created is displayed
  - the created token is displayed

~~~
Token generated with success:
```n_Y9lzbKnhNhK7Sw40fzLqOuFC_
↪bxDC1rtHTHCT7aoNTSkw3SOMfqxx06KXSXTjHXbglUx9_IVOXVz-I1g8p34-
↪1i8NaY9Grasu_IrpA24JkWhz5UWul12ePiebn_
↪SOaiFhJpjHLD8slMx2aW1hVhiqL92UbDwtJ6uej7wpZ-IM```
 Make sure you save it. You won't be able to access it again.
~~~

- Use the displayed token.

  The list in `The API Token list` area is updated.
- If necessary, delete an existing token using the trash button.

  A confirmation window is displayed with the following message.

  `Do you want to delete the token ? .`
- Press the `Yes` button to confirm the deletion.

## 8.7.13 Managing the password policy

### 8.7.13.1 Introduction

This procedure enables:

- Viewing the current password policy configuration
- Changing the policy

**Note:**

This graphical interface is described in *The `Password Policy` section of the `Accounts` submenu*.

#### 8.7.13.2 Prerequisites

- User : member of **Administrator** group

#### 8.7.13.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

#### 8.7.13.4 Procedure to access to the `Password Policy` window for an administrator account

- In the navigation bar, successively click on:

- The `Admin` button
- The `Gcenter` sub-menu
- The `Accounts` command

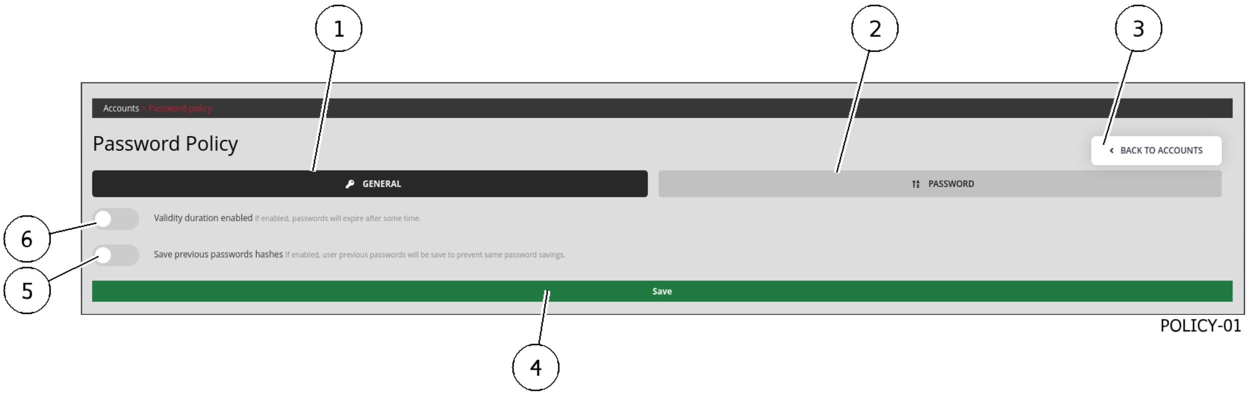
  The `Accounts` window is displayed.

- Click on the `Password Policy` heading.

  The `Password Policy` window is displayed.

#### 8.7.13.5 Procedure to view or change the current settings

- Click on the `GENERAL` button to view the general parameters.



Validity duration enabled If enabled, passwords will expire after some time.

Save previous passwords hashes If enabled, user previous passwords will be save to prevent same password savings.

POLICY-01

- Use the selector (5) `Save previous passwords hashes` to save the hashes of previous passwords.

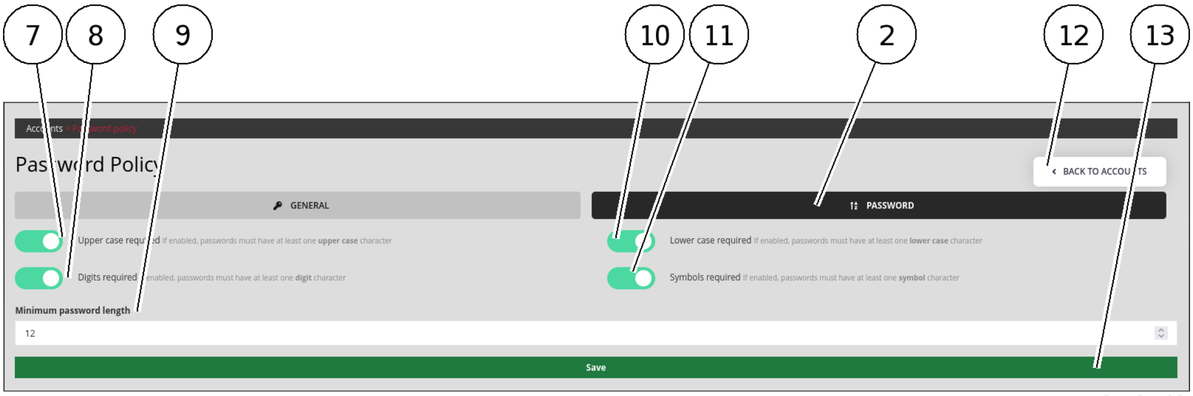
  If the setting was enabled, then the `Number of previous passwords saved` field is displayed with the default setting of **5**.
  - Change this value if necessary.
- Use the selector (6) `Validity duration enabled` to enable the validity duration of passwords.

  If the setting was enabled, then the `Validity duration (days)` field is displayed with the default setting of **90**.
  - Change this value if necessary.
- After modification, press the `Save` button (4).

  A confirmation message is displayed.
- Click on the `BACK TO ACCOUNTS` button (3) to return to the main menu or use the following procedure to access the password settings.

### 8.7.13.6 Procedure to view or change the password policy

- Click on the `` `PASSWORD` `` button (2) to view the general parameters.



Password Policy

Upper case required If enabled, passwords must have at least one **upper case** character

Digits required If enabled, passwords must have at least one **digit** character

Lower case required If enabled, passwords must have at least one **lower case** character

Symbols required If enabled, passwords must have at least one **symbol** character

Minimum password length

12

POLICY-02

- Use the selector (7) `` `Upper case required` `` to enable the presence of at least one upper case letter.
- Use the selector (8) `` `Digits required` `` to enable the presence of at least one digit (0 to 9).
- Use the selector (9) `` `Minimum password length` `` to set the minimum password length.
- Use the selector (10) `` `Lower case required` `` to enable the presence of at least one lower case letter.
- Use the selector (11) `` `Symbols required` `` to activate the presence of at least one symbol (i.e. neither a number nor a letter).
- After modification, press the `` `Save` `` button (13).

  A confirmation message is displayed.
- Press the `` `BACK TO ACCOUNTS` `` button (12) to return to the main menu.

---

## 8.8 Configuring the detection engine

### 8.8.1 Setting up GBox and the Malcore and Retroact engines and activate the GBox

#### 8.8.1.1 Introduction

This procedure describes:

- Enabling the GBox automatic analysis. For this, see the *Procedure to enable the GBox analysis*
- Setting up the scan expiration time for an already scanned file. For this, see the *Procedure to setup the analysis timeout*
- Setting up the Retroact engine. For this, see the *Procedure to setup Retroact*
- Setting up the Malcore engine. For this, see *Procedure to change the analysis limits*

**Note:**

The graphical interface is described in *`Admin-GCenter- Malcore Management` screen of the legacy web UI*.

---

#### 8.8.1.2 Prerequisites

- User : member of **Administrator** group

---

#### 8.8.1.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

---

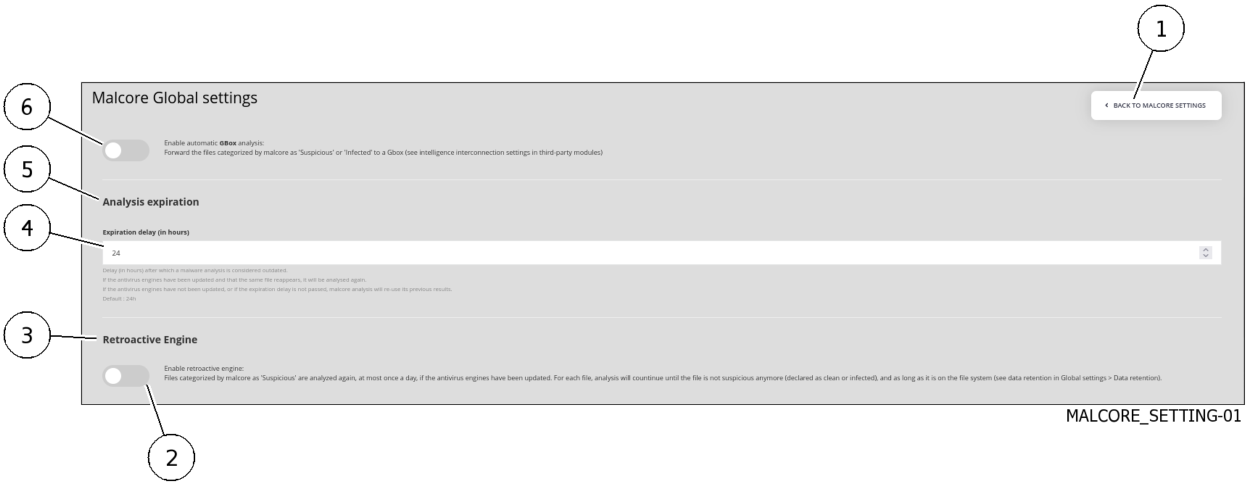
#### 8.8.1.4 Procedure to access the `Malcore Management` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Malcore Management` command
  The `Malcore Management` window is displayed.
- Click on the `Global settings` section.

---

#### 8.8.1.5 Procedure to enable the GBox analysis

> **Note:**
>
> The GBox must be configured beforehand.



Malcore Global settings

Enable automatic **GBox** analysis:
Forward the files categorized by malcore as 'Suspicious' or 'Infected' to a Gbox (see intelligence interconnection settings in third-party modules)

**Analysis expiration**

**Expiration delay (in hours)**

24

Delay (in hours) after which a malware analysis is considered outdated.
If the antivirus engines have been updated and that the same file reappears, it will be analysed again.
If the antivirus engines have not been updated, or if the expiration delay is not passed, malcore analysis will re-use its previous results.
Default : 24h

**Retroactive Engine**

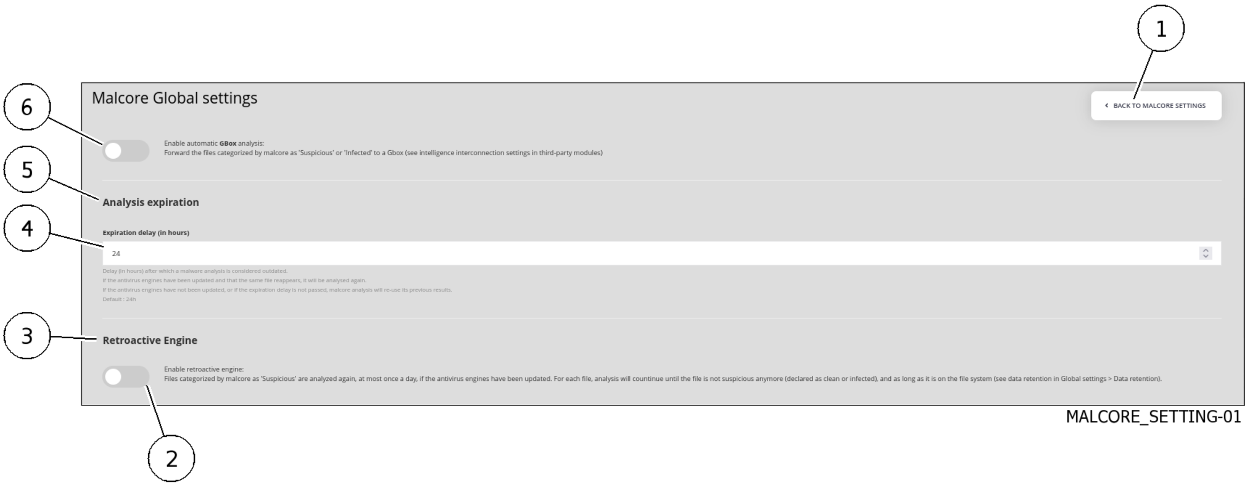
Enable retroactive engine:
Files categorized by malcore as 'Suspicious' are analyzed again, at most once a day, if the antivirus engines have been updated. For each file, analysis will countinue until the file is not suspicious anymore (declared as clean or infected), and as long as it is on the file system (see data retention in Global settings > Data retention).

MALCORE_SETTING-01

- Use the `Enable automatic GBox analysis` selector (6) to transfer files listed by Malcore as *Suspect* or *Infected* to a GBox.

---

#### 8.8.1.6 Procedure to setup the analysis timeout



Malcore Global settings

Enable automatic **GBox** analysis:
Forward the files categorized by malcore as 'Suspicious' or 'Infected' to a Gbox (see intelligence interconnection settings in third-party modules)

**Analysis expiration**

**Expiration delay (in hours)**

24

Delay (in hours) after which a malware analysis is considered outdated.
If the antivirus engines have been updated and that the same file reappears, it will be analysed again.
If the antivirus engines have not been updated, or if the expiration delay is not passed, malcore analysis will re-use its previous results.
Default : 24h

**Retroactive Engine**

Enable retroactive engine:
Files categorized by malcore as 'Suspicious' are analyzed again, at most once a day, if the antivirus engines have been updated. For each file, analysis will countinue until the file is not suspicious anymore (declared as clean or infected), and as long as it is on the file system (see data retention in Global settings > Data retention).

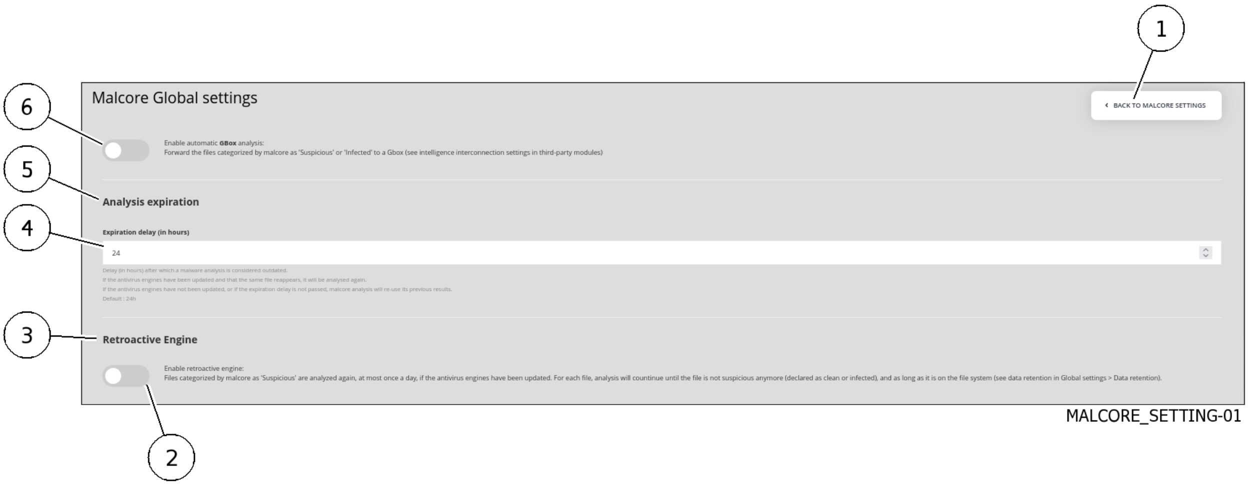
MALCORE_SETTING-01

- If necessary change the `Expiration delay` parameter (4).
  This parameter sets the time during which Malcore will not re-scan a file already seen on the network.
  If the antivirus engines were updated and the same file reappears, it will be scanned again.
  During the specified time, if a file is seen on the network again, then it is not re-scanned. The result of the first scan is used.
- Confirm the changes using the `Save` button (15).
  A confirmation message is displayed: `Updated with success`.

#### 8.8.1.7 Procedure to setup Retroact

**Note:**

The **RETROACT** scanning engine enables ex-post scanning of files flagged as "suspicious" by Malcore's heuristic analysis.
These post-scans are done over a period of days/weeks/months depending on the retention time after the file has been scanned, with the new signatures and heuristics methods.



Malcore Global settings

Enable automatic **GBox** analysis:
Forward the files categorized by malcore as 'Suspicious' or 'Infected' to a Gbox (see intelligence interconnection settings in third-party modules)

**Analysis expiration**

**Expiration delay (in hours)**

24

Delay (in hours) after which a malware analysis is considered outdated.
If the antivirus engines have been updated and that the same file reappears, it will be analysed again.
If the antivirus engines have not been updated, or if the expiration delay is not passed, malcore analysis will re-use its previous results.
Default : 24h

**Retroactive Engine**

Enable retroactive engine:
Files categorized by malcore as 'Suspicious' are analyzed again, at most once a day, if the antivirus engines have been updated. For each file, analysis will countinue until the file is not suspicious anymore (declared as clean or infected), and as long as it is on the file system (see data retention in Global settings > Data retention).

MALCORE_SETTING-01

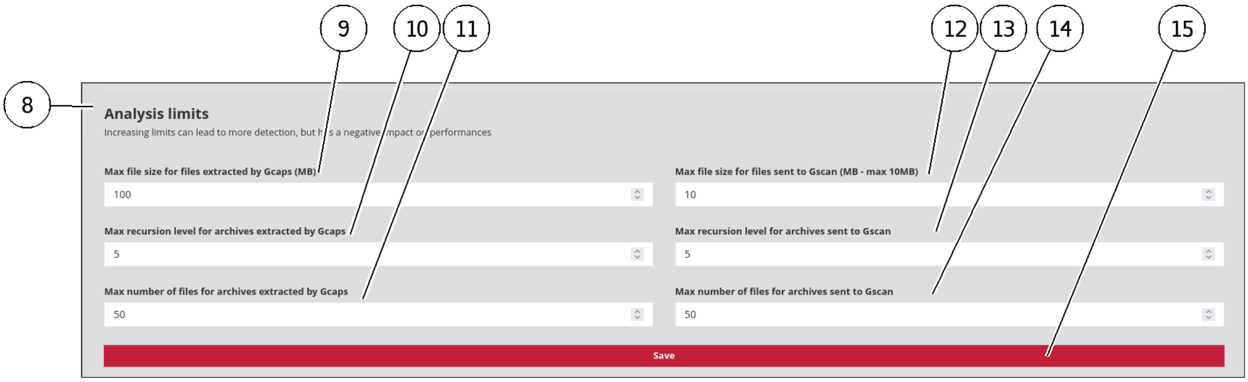
- Use the `Enable retroactive engine` selector (3) to have files listed by Malcore as *Suspect* re-scanned when engines are updated.
- Confirm the changes using the `Save` button (15).

A confirmation message is displayed: `Updated with success`.

### 8.8.1.8 Procedure to change the analysis limits

**Note:**

Increasing the limits can lead to more detection although it has a negative impact on performance.



Analysis limits

Increasing limits can lead to more detection, but has a negative impact on performances

Max file size for files extracted by Gcaps (MB): 100

Max recursion level for archives extracted by Gcaps: 5

Max number of files for archives extracted by Gcaps: 50

Max file size for files sent to Gscan (MB - max 10MB): 10

Max recursion level for archives sent to Gscan: 5

Max number of files for archives sent to Gscan: 50

MALCORE_SETTING-02

- Modifying the analysis parameters in terms of flows taken into account by the Malcore engine:
  - If necessary, modify parameter (9): maximum size of files extracted by a GCap (MB)
  - If necessary modify parameter (10): maximum recursion level for archives extracted by GCap
  - If needed, modify parameter (11): maximum number of files for the archives extracted by GCap

**Note:**

The size of the files extracted by a GCap and the maximum file size taken into account by the Malcore engine may differ.
The maximum file size value on the GCap side must always be smaller than the maximum file size on the Malcore side.

- Modifying the analysis parameters via the GSCan module by the Malcore engine:

- If necessary, modify parameter (12): maximum size of files sent to GScan (MB)
- If necessary, change the parameter (13): maximum recursion level for the archives sent to Gscan
- If necessary, modify the parameter (14): maximum number of archive files sent to Gscan

- Confirm the changes using the `Save` button( 15).
  A confirmation message is displayed: `Updated with success`.

## 8.8.2 Managing the white and black lists of the Malcore engine

### 8.8.2.1 Introduction

It is possible to instruct the Malcore engine to deem files as healthy or not without scanning them but by using their SHA256 fingerprint.
The exception list referred to as the **Whitelist** contains a list of SHA256 fingerprints of files that Malcore should consider to be safe.
The exception list referred to as the **Blacklist** contains a list of SHA256 fingerprints of files that Malcore should consider to be compromised.
When the files to be scanned are sent to Malcore, Malcore compares their SHA256 fingerprints with the two lists and, depending on the case, considers them to be healthy, compromised, or to be scanned.

This procedure shows how to populate both lists.
All additions and changes made from the White List and Black List sections of the MALCORE engine configuration settings will be taken into account in the analysis of the flow as well as for the files scanned via the GScan.

> **Note:**
>
> The graphical interface is described in *`Admin-GCenter- Malcore Management` screen of the legacy web UI*.

---

### 8.8.2.2 Prerequisites

- User : member of **Administrator** group

---

### 8.8.2.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

---

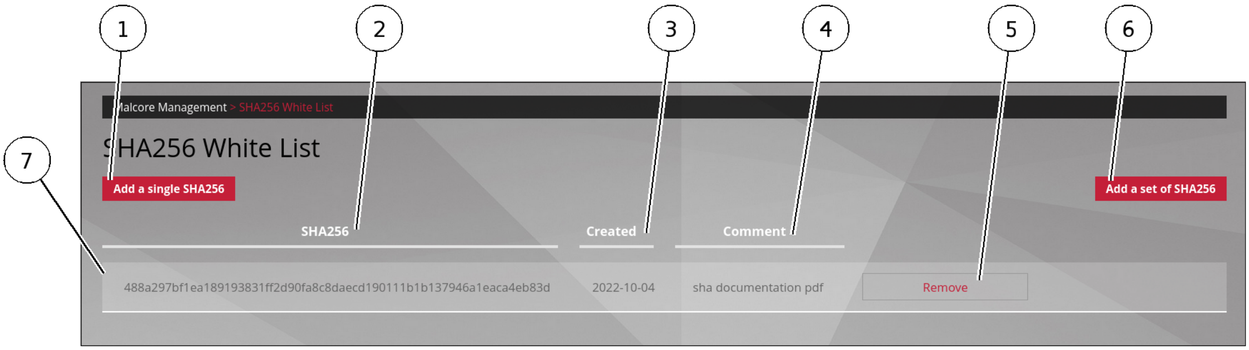
### 8.8.2.4 Procedure to access to the `Users management` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Malcore Management` command
  The `Malcore Management` window is displayed.

---

### 8.8.2.5 Procedure for White list management

- Click on the `White List` section.



| SHA256 | Created | Comment |  |
|---|---|---|---|
| 488a297bf1ea189193831ff2d90fa8c8daecd190111b1b137946a1eaca4eb83d | 2022-10-04 | sha documentation pdf | Remove |

MALCORE_WL-01

- To add an item to the list :

- Press the `Add to Single SHA256` button (1).
  The `Add to White List` window is displayed.
- Enter the SHA 256.
- Enter a comment, if any, for further details.
- Click on the `Save` button.
  If successful, the following message is displayed: `The SHA256 xxxxx was successfully added to white list.`
  In case of an error, the following message is displayed.
  For example, `The SHA256 was not added to white list. File with SHA256 xxxxx already exists in white list`

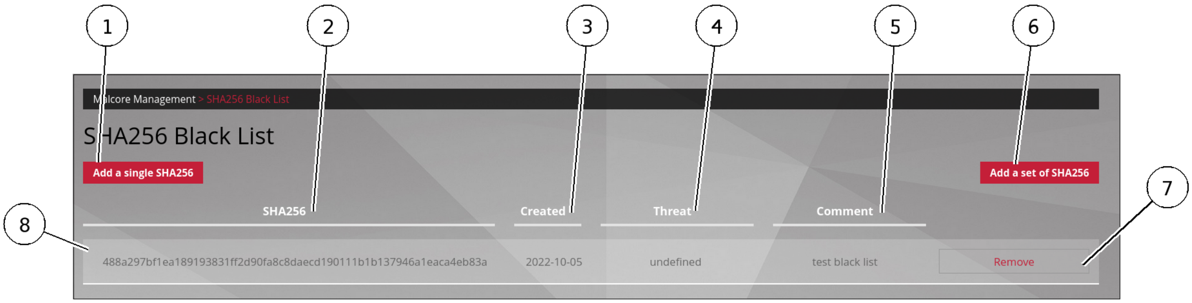
- To add a set of items to the list:

- Press the `Add a set of SHA256` button (6).
  The `Add to White List` window is displayed.
- Use the `Browse` button to select the csv file.
- If necessary, delete the previous list by ticking the `Clean previous list` box.
- Click on the `Save` button.
- Enter any comments.
- Click on the `Save` button.
  A status message indicates the result of the import.
  For example , `98/100 SHA256 has been added to white list`. Here the message indicates the number (98) of elements taken into account.
  The remaining items (2) are not imported either because the csv file is not compliant or because they are already present in the existing lists.

---

### 8.8.2.6 Procedure for Black list management

- Click on the `Black List` section.



Malcore Management > SHA256 Black List

SHA256 Black List

Add a single SHA256

Add a set of SHA256

| SHA256 | Created | Threat | Comment | |
|---|---|---|---|---|
| 488a297bf1ea189193831ff2d90fa8c8daecd190111b1b137946a1eaca4eb83a | 2022-10-05 | undefined | test black list | Remove |

MALCORE_WL-02

- To add an item to the list:

- Press the `Add to Single SHA256` button (1).
  The `Add to Black List` window is displayed.
- Enter the SHA 256.
- Enter a comment, if any, for further details.
- Click on the `Save` button.
  If successful, the following message is displayed: `The SHA256 xxxxx was successfully added to Black list.`.
  In case of an error, the following message is displayed.
  For example, `The SHA256 was not added to the Black list. File with SHA256 xxxxx already exists in the Black list`.

- To add a set of items to the list:

- Press the `Add a set of SHA256` button (6).
  The `Add to Black List` window is displayed.
- Use the `Browse` button to select the csv file.
- If necessary, delete the previous list by ticking the `Clean previous list` box.
- Click on the `Save` button.
- Enter any comments.
- Click on the `Save` button.
  A status message indicates the result of the import.
  For example , `98/100 SHA256 has been added to the Black list`. Here the message indicates the number (96) of elements taken into account.
  The remaining items (4) are not imported either because the csv file is not compliant or because they are already present in the existing lists.

## 8.8.3 Enabling and configuring the Machine Learning engine

### 8.8.3.1 Introduction

This procedure shows how to enable or disable the **Machine Learning (or DGA)** engine.

| To | Apply the procedures |
|---|---|
| Enable the engine | 1 - Apply the *Procedure to access to the `Domain Name Generation (DGA) Detection Management` window for an administrator account* |
| | 2 - Apply the *Procedure to enable the engine* |
| Disable the engine | 1 - Apply the *Procedure to access to the `Domain Name Generation (DGA) Detection Management` window for an administrator account* |
| | 2 - Apply the *Procedure to disable the engine* |

**Note:**

The graphical interface is described in the *`Admin-GCenter- ML Management` screen of the legacy web UI*.

### 8.8.3.2 Prerequisites

- User : member of **Administrator** group

### 8.8.3.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

### 8.8.3.4 Procedure to access to the `Domain Name Generation (DGA) Detection Management` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `ML Management` command

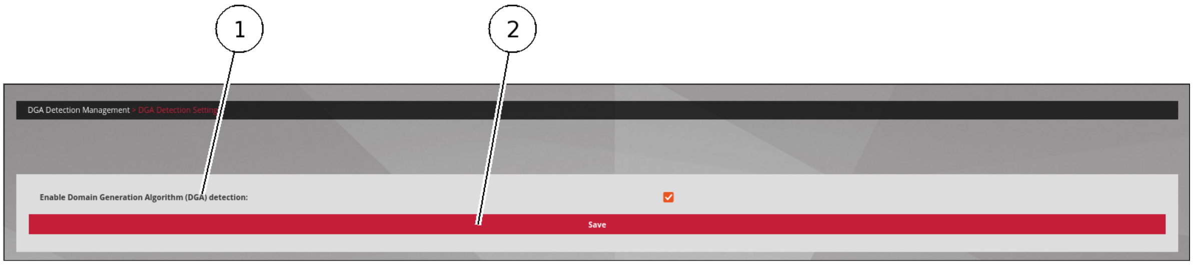
  The `Machine Learning Management` window is shown.
- Click on the `Machine Learning Management` heading.

  The `Machine Learning Management` window is displayed. It contains a single `DGA Detection Management` category.
- Click on the `DGA Detection Management` button, the `Domain Name Generation (DGA) Detection Management` screen is displayed.

### 8.8.3.5 Procedure to enable the engine

- Click on the `Setting` category.

  The `DGA Detection Settings` window displays the option to enable/disable the engine.



Enable Domain Generation Algorithm (DGA) detection: ☑

ML_SETTING-01

- Tick the `Enable Domain Generation Algorithm (DGA) detection` choice (1).

**Note:**

This feature is disabled by default.

- Click on the `Save` button (2).

#### 8.8.3.6 Procedure to disable the engine

- Click on the `Setting` category.
  The `DGA Detection Settings` window displays the option to enable/disable the engine.
- Untick the `Enable Domain Generation Algorithm (DGA) detection` choice (1).
- Click on the `Save` button (2).

### 8.8.4 Managing the white and black lists of the Machine Learning engine

#### 8.8.4.1 Introduction

Exception lists can be set up in order to:

- Force the engine to declare domain names as healthy (White List).
  This enables eliminating alerts related to recurring false positives.
- Raise an alert for a domain that would not otherwise have been detected (false negative) using a blacklist.

This procedure shows how to populate both lists.

**Note:**

The graphical interface is described in *`Admin-GCenter- ML Management` screen of the legacy web UI*.

#### 8.8.4.2 Prerequisites

- User : member of **Administrator** group

#### 8.8.4.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

### 8.8.4.4 Procedure to access to the `Domain Name Generation (DGA) Detection Management` window for an administrator account

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `ML Management` command

  The `Machine Learning Management` window is shown.
- Click on the `Machine Learning Management` heading.

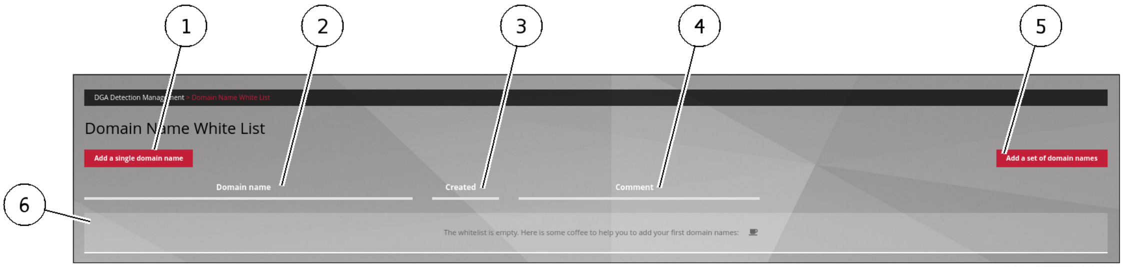
  The `Machine Learning Management` window is displayed. It contains a single `DGA Detection Management` category.
- Click on the `DGA Detection Management` button.

  The `Domain Name Generation (DGA) Detection Management` is displayed.

---

### 8.8.4.5 Procedure to manage the White list

- Click on the `White List` section.



The whitelist is empty. Here is some coffee to help you to add your first domain names: ☕

ML_SETTING-02

- To add an item to the list :
- Press the `Add a single domain name` button (1).

  The `Add to White List` window is displayed.
- Enter the domain name.
- Enter a comment, if any, for further details.
- Click on the `Save` button.

  If successful, the following message is displayed: `The domain name xxx was successfully added to white list`.

  In case of an error, the following message is displayed.

  For example, `The domain name was not added to white list. xxx already exists in the white list`
- To add a set of items to the list:
- Press the `Add a set of domain names` button (5).

  The `Add to White List` window is displayed.
- Use the `Browse` button to select the csv file.
- If necessary, delete the previous list by ticking the `Clean previous list` box.
- Click on the `Save` button.
- Enter any comments.
- Click on the `Save` button.

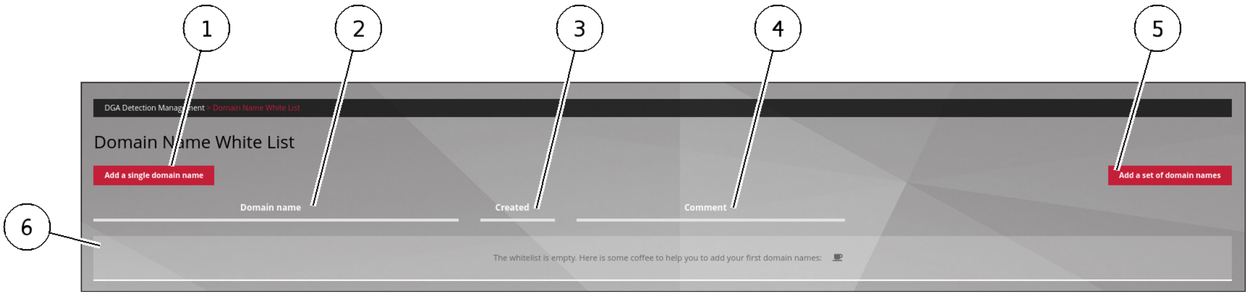
  A status message indicates the result of the import.

  For example: `The line number 1 is invalid in the csv file. Please contact the Gatewatcher support if you need help.`. Here the message indicates that the loaded format is not the expected one.

---

#### 8.8.4.6 Procedure to manage the Black list

- Click on the `Black List` section.



The whitelist is empty. Here is some coffee to help you to add your first domain names:

ML_SETTING-02

- To add an item to the list:

- Press the `Add a single domain name` button (1).
  The `Add to Black List` window is displayed.
- Enter the domain name.
- Enter a comment, if any, for further details.
- Click on the `Save` button.
  If successful, the following message is displayed: `The domain name xxx was successfully added to white list`.
  In case of an error, the following message is displayed.
  For example: `The domain name was not added to white list. xxx already exists in the white list`

- To add a set of items to the list:

- Press the `Add a set of domain names` button (5).
  The `Add to Black List` window is displayed.
- Use the `Browse` button to select the csv file.
- If necessary, delete the previous list by ticking the `Clean previous list` box.
- Click on the `Save` button.
- Enter any comments.
- Click on the `Save` button.
  A status message indicates the result of the import.
  For example: `The domain name was not added to black list. xxx already exists in black list`

## 8.9 GCenter Configuration Management

### 8.9.1 Configuring the Netdata polling interface

#### 8.9.1.1 Introduction

This procedure describes the configuration of the Netdata interface to allow a remote server (for example NAGIOS) to read the selected metrics via the netdata API.

**User Authentication:**

Authenticated users can search the Netadata API, available on Gstats.
For simple automation, it is possible to allow an unauthenticated user to probe the API.
In this case, the API endpoint is redirected to http on the port specified below
http://gcenter_fqdn:redirection_port

### List of authorized IP addresses

A restricted access list is the client subnets for which this redirection is available.
Depending on the IP/mask pair, it is therefore possible to allow an IP or a range of IP addresses per line entered.
It is possible to add multiple rows.

### List of accessible metrics

For a remote PC defined in the list of allowed IPs, it is possible to view the available metrics.
To do this, you must enter the following URL in a web browser
http://IP-gcenter:8001/host/fqdn-gcenter/api/v1/allmetrics

Below, an extract of the metrics is displayed.

```
# chart: net_drops.vnet0 (name: net_drops.vnet0)
NETDATA_NET_DROPS_VNET0_INBOUND="0"      # drops/s
NETDATA_NET_DROPS_VNET0_OUTBOUND="-0"      # drops/s
NETDATA_NET_DROPS_VNET0_VISIBLETOTAL="0"      # drops/s

# chart: net_errors.vnet0 (name: net_errors.vnet0)
NETDATA_NET_ERRORS_VNET0_INBOUND="0"      # errors/s
NETDATA_NET_ERRORS_VNET0_OUTBOUND="-0"      # errors/s
NETDATA_NET_ERRORS_VNET0_VISIBLETOTAL="0"      # errors/s

# chart: net.vnet0 (name: net.vnet0)
NETDATA_NET_VNET0_RECEIVED="8"      # kilobits/s
NETDATA_NET_VNET0_SENT="1"      # kilobits/s
NETDATA_NET_VNET0_VISIBLETOTAL="9"      # kilobits/s

# chart: elasticsearch_gesmaster.cluster_stats_shards_total (name: elasticsearch_gesmaster.
↪cluster_stats_shards_total)
NETDATA_ELASTICSEARCH_GESMASTER_CLUSTER_STATS_SHARDS_TOTAL_SHARDS="114"      # shards
NETDATA_ELASTICSEARCH_GESMASTER_CLUSTER_STATS_SHARDS_TOTAL_VISIBLETOTAL="114"      # shards

# chart: elasticsearch_gesmaster.cluster_stats_indices (name: elasticsearch_gesmaster.cluster_
↪stats_indices)
NETDATA_ELASTICSEARCH_GESMASTER_CLUSTER_STATS_INDICES_INDICES="114"      # indices
NETDATA_ELASTICSEARCH_GESMASTER_CLUSTER_STATS_INDICES_VISIBLETOTAL="114"      # indices
```

**Note:**

For more information, see the *Interconnection with external systems*.
The graphical interface is described in *`Admin-GCenter-Configuration` screen of the legacy web UI*.

#### 8.9.1.2 Prerequisites

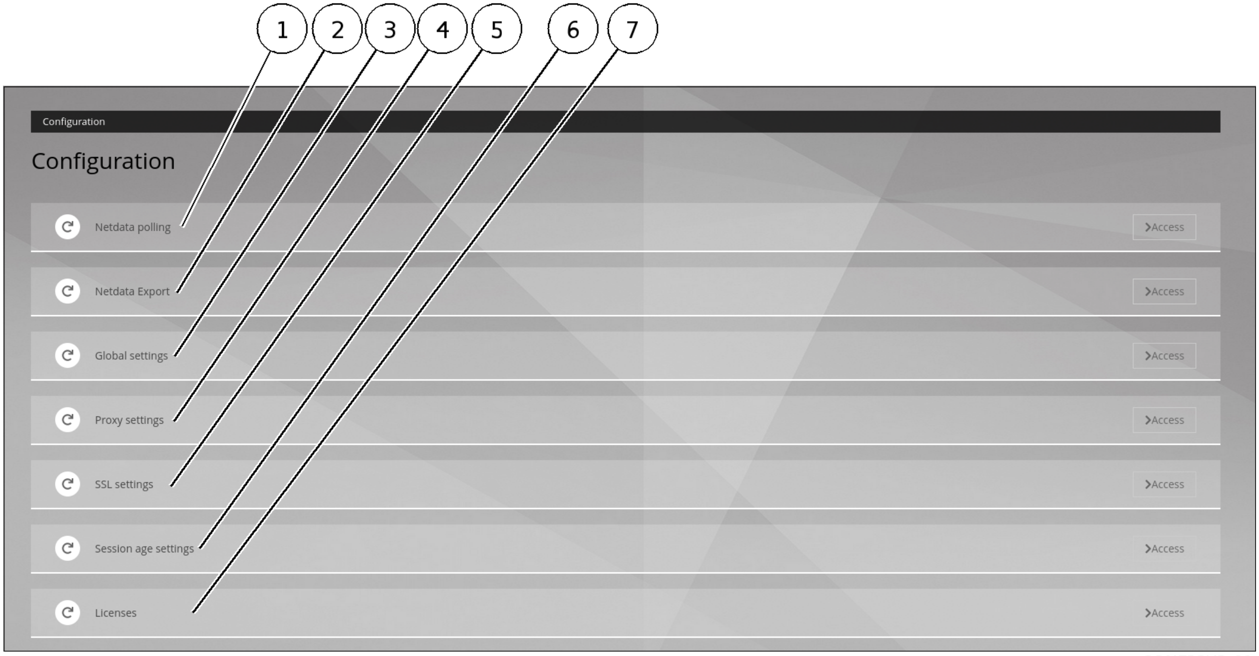
- User : member of **Administrator** group

#### 8.9.1.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

#### 8.9.1.4 Procedure to access to the `Netdata polling` screen of the legacy web UI

- In the navigation bar, click successively on:
- The `Admin`
- The `Admin` sub menu
- The `Configuration` command
  The `Configuration` window is displayed.

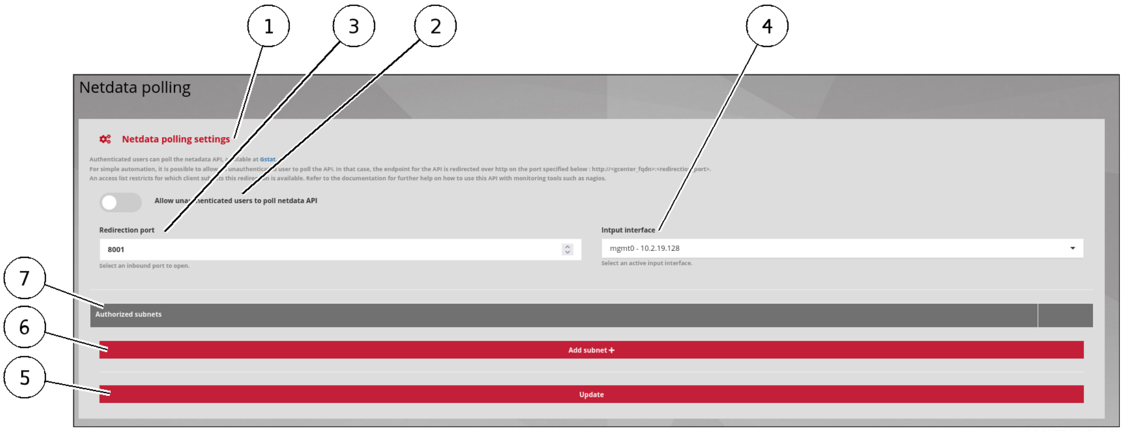


CONFIGUR-01

- Click on the `Netdata polling` button (1).

#### 8.9.1.5 Procedure to configure

The following screen is displayed:



Authenticated users can poll the netadata API, available at Gstat.
For simple automation, it is possible to allow an unauthenticated user to poll the API. In that case, the endpoint for the API is redirected over http on the port specified below : http://<gcenter_fqdn>:<redirection_port>.
An access list restricts for which client subnets this redirection is available. Refer to the documentation for further help on how to use this API with monitoring tools such as nagios.

Select an inbound port to open.

Select an active input interface.

CONFIGUR-02

- Use the selector (2) `Allow unauthenticated users to poll netdata API`.
- Select forwarding port (3): default 8001
- Select the GCenter input interface in field (4) `Intput interface`.
- To add an IP address or subnet:

- Press on the `Add subnet` button
- In the `ADD IP/MASK` window, enter the IP address then `/` then the mask
- Press on the `ADD` button

  The address entered is displayed in field (7) `Authorized subnets`

- Press on the `Save` button (5).

  If all is ok then the message `The Netdata polling configuration was successfully updated` is displayed.

## 8.9.2 Configuring the Netdata export interface

### 8.9.2.1 Introduction

This procedure describes the configuration of the Netdata interface to export system data to remote servers (Netdata, Nagios...).

**Note:**

For more information, see *Interconnection with external systems*.
The graphical interface is described in *`Admin-GCenter-Configuration` screen of the legacy web UI*.

### 8.9.2.2 Prerequisites

- User : member of **Administrator** group

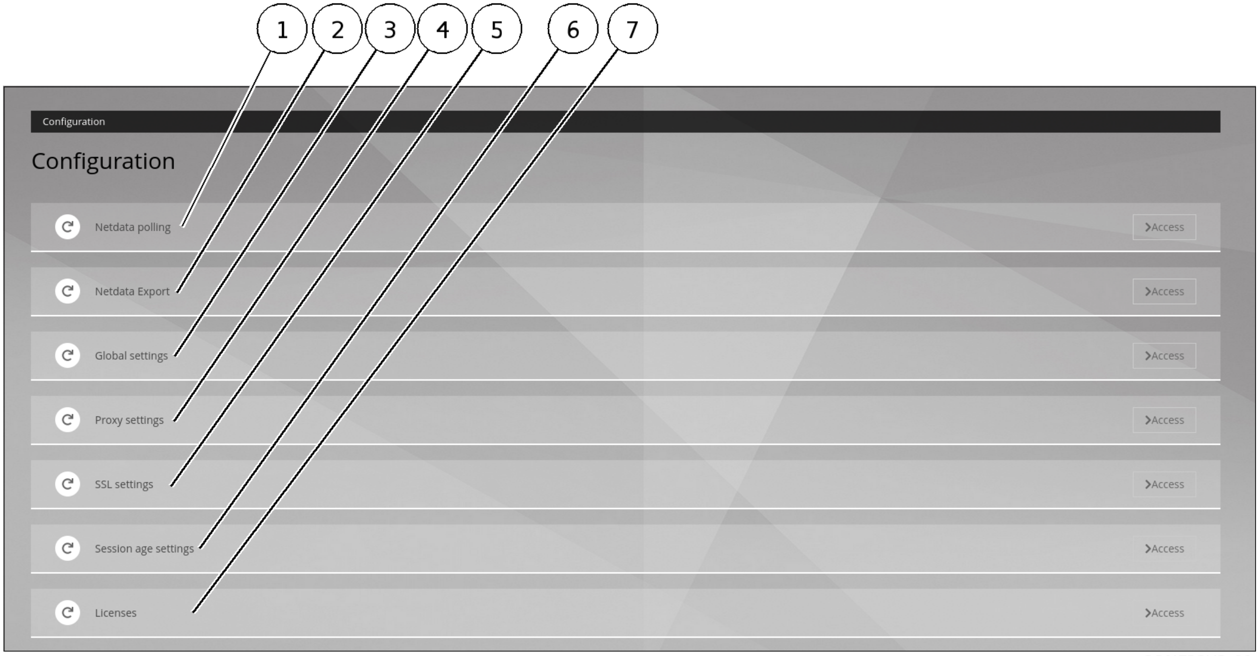
#### 8.9.2.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

#### 8.9.2.4 Procedure to access to the Legacy Web UI `Netdata Export Configuration` screen

- In the navigation bar, click successively on:
- The `Admin` command
- The sub menu `Admin`
- The `Configuration` command

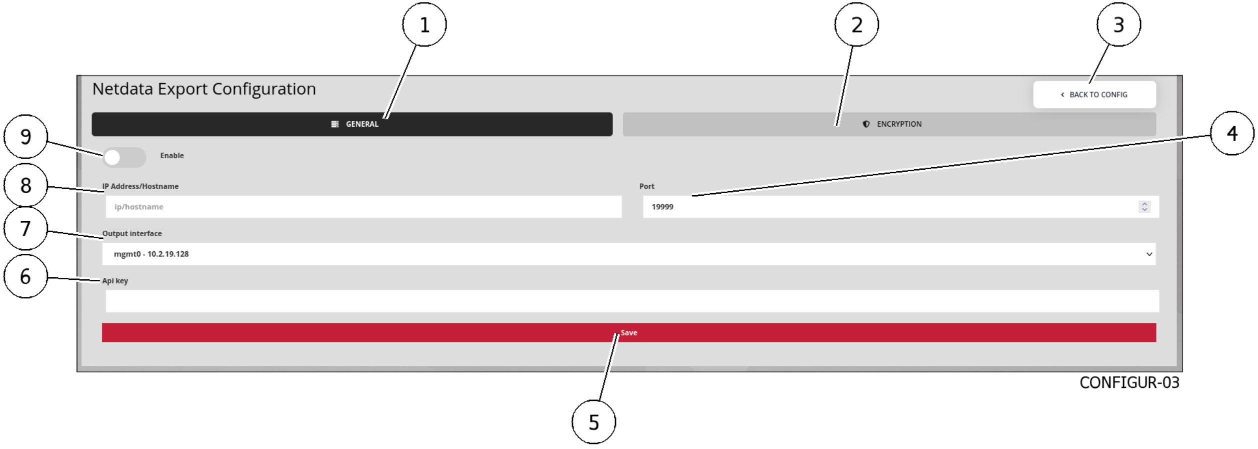
  The `Configuration` window is displayed.



CONFIGUR-01

- Click on the button (2) `Netdata Export`

  The following screen is displayed:



IP Address/Hostname: ip/hostname

Port: 19999

Output interface: mgmt0 - 10.2.19.128

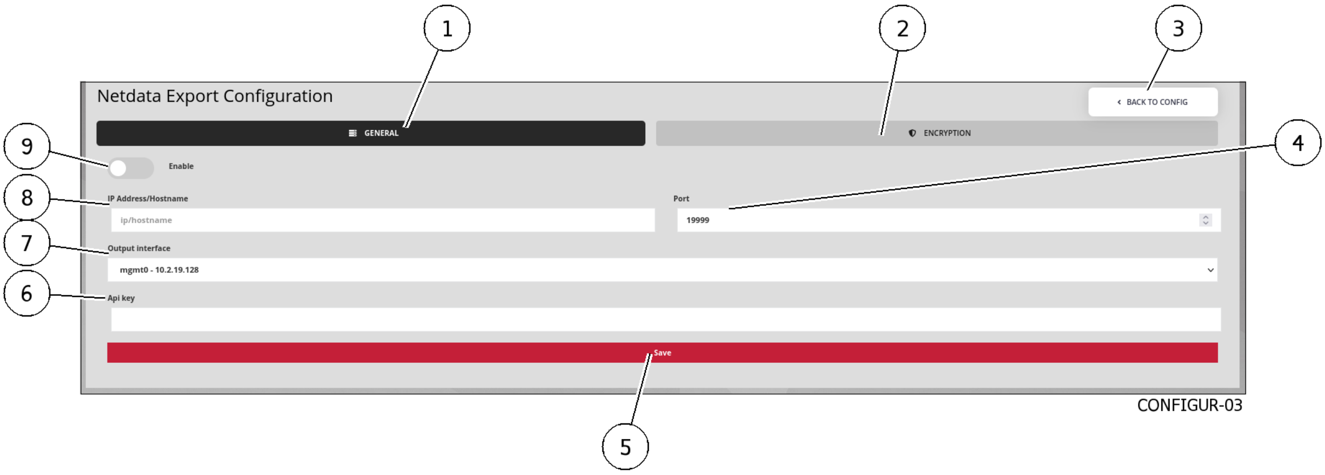
Api key:

CONFIGUR-03

The `Netdata Export Configuration` page consists of 2 tabs:

- The `GENERAL` configuration parameter management tab
- The `ENCRYPTION` Encryption Settings Management tab

### 8.9.2.5 Procedure to setup the `GENERAL` parameters



IP Address/Hostname: ip/hostname

Port: 19999

Output interface: mgmt0 - 10.2.19.128

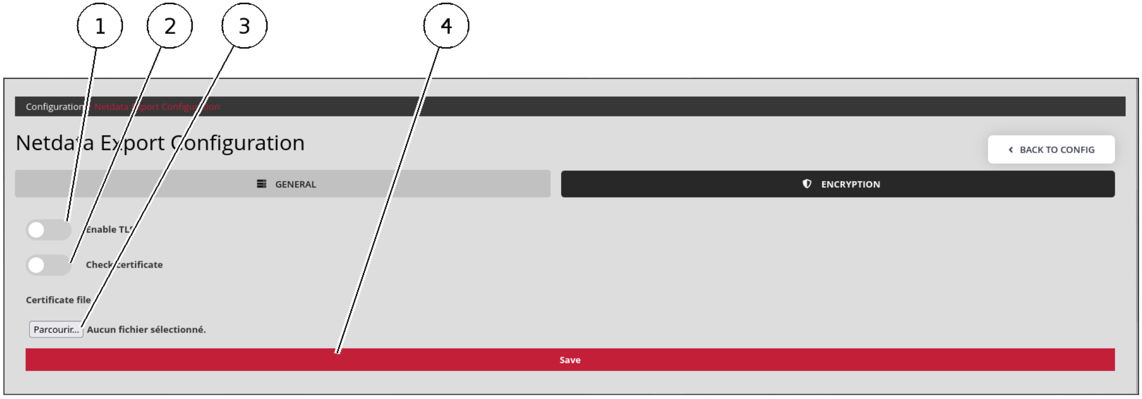
Api key

CONFIGUR-03

- Click on the tab (1) `GENERAL`.
- Activate the elector (9) `Enable`.
- Enter the Netdata server FQDN or IP address in field (8).
- Select the Netdata server listening port (4).
- Select the network interface (7) to use for this connection.
- Enter the Netdata server API key in field (6).
- Press on the `Save` button (5)

### 8.9.2.6 Procedure to configure the `ENCRYPTION` parameters

- Click on the button (2) `ENCRYPTION`.
  The following screen is displayed:


1
2
3
4
Configuration / Netdata Export Configuration
Netdata Export Configuration
BACK TO CONFIG
GENERAL
ENCRYPTION
Enable TLS
Check certificate
Save

Certificate file

Parcourir... Aucun fichier sélectionné.

CONFIGUR-03-1

- If necessary, enable the selector (1) `Enable TLS`.
- If necessary, activate the selector (2) `Check certificate`.
- If necessary, click on the button (3) `Browse` to load the certificate file.
- Press on the `Save` button (4).
- Close the opened windows.

## 8.9.3 Setting up a Netdata server

### 8.9.3.1 Introduction

This procedure describes the installation of a Netdata monitoring server and its interconnection to a GCenter for monitoring purposes.

> **Note:**
>
> The Netdata version compatible with GCenter and GCap is 1.19

The configuration consists of:

- *Procedure to install via docker*
- *Procedure to configure stream.conf and GCenter*
- *Procedure to create alerts for Netdata*

---

### 8.9.3.2 Prerequisites

- User : member of **Administrator** group

---

### 8.9.3.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

---

### 8.9.3.4 Procedure to install via docker

- Enter the following command to install the Netdata docker.

```
docker pull netdata/netdata:v1.19.0
```

- Enter the following command to be able to edit the Netdata configuration from the host machine, you must launch a temporary container to retrieve the configuration files.

```
mkdir netdataconfig
docker run -d --name netdata_tmp netdata/netdata
docker cp netdata_tmp:/usr/lib/netdata netdataconfig/
docker rm -f netdata_tmp
```

- Enter the following command to launch the final container

```
docker run -d --name=netdata \
  -p 19999:19999 \
  -v $(pwd)/netdataconfig/netdata:/usr/lib/netdata:rw \
  -v netdatalib:/var/lib/netdata \
  -v netdatacache:/var/cache/netdata \
  -v /etc/passwd:/host/etc/passwd:ro \
  -v /etc/group:/host/etc/group:ro \
```

(suite sur la page suivante)

(suite de la page précédente)

```
  -v /proc:/host/proc:ro \
  -v /sys:/host/sys:ro \
  -v /etc/os-release:/host/etc/os-release:ro \
  --restart unless-stopped \
  --cap-add SYS_PTRACE \
  --security-opt apparmor=unconfined \
  netdata/netdata
```

#### 8.9.3.5 Procedure to configure stream.conf and GCenter

- Enter the following command to generate the uuid.

```
sudo docker exec -it netdata uuidgen
```

- Enter the following commands to configure stream with the uuid generated previously. Netdata recommends to use edit-config

```
sudo docker exec -it netdata /etc/netdata/edit-config stream.conf
```

```
[dd236090-a42d-43e2-b0ba-ff8eaa6216a2] << Remplacer l'uuid ici
    enabled = yes
    default history = 36000
    default memory mode = ram
    health enabled by default = auto
    allow from = *
    default postpone alarms on connect seconds = 60
```

- Enter the following commands to configure netdata.conf

```
sudo docker exec -it netdata /etc/netdata/edit-config netdata.conf
```

```
[global]
      ...
      hostname = netdata-docker.gatewatcher.com
      ...
      timezone = Europe/Paris
```

- Enter the following commands to configure the Netdata export in the GCenter.

> **Note:**
>
> Read the Netdata configuration parameters in the Netdata part visible in the *`Admin-GCenter-Configuration` screen of the legacy web UI*.
> For Netdata to send notifications, you must configure the *health_alarm_notify.conf*

```
sudo docker exec -it netdata /etc/netdata/edit-config health_alarm_notify.conf
```

- See also the reference documentation : Alarm Configuration

#### 8.9.3.6 Procedure to create alerts for Netdata

- Enter the following commands to create alerts in the container folder:

```
/usr/lib/netdata/conf.d/health.d
```

> **Note:**
>
> In order for the new alerts to be taken into account, it is necessary to restart the docker container.

- Enter the following commands to create your own alerts
  To clarify the management of alerts, it is advisable to create a **.conf`* file by alert category.
  Here are some examples:

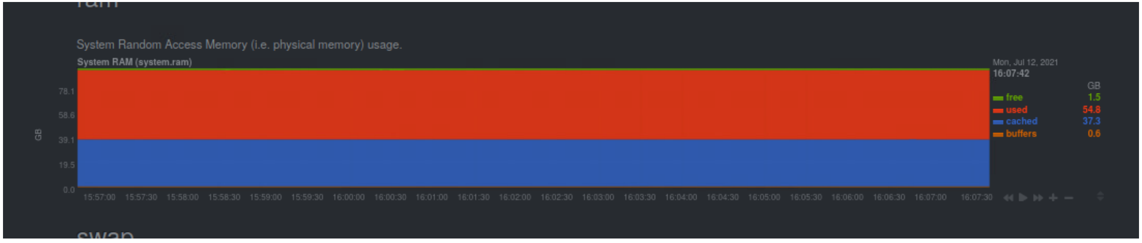
| Description | Link |
|---|---|
| Alert in case of absence/traffic overload | `traffic.conf` |
| Alert in case of deactivation of GCap analysis services | `suricata_status.conf` |
| Alert if a restart of Gcap/GCenter has occurred | `reboot.conf` |
| RAM overload alert | `ram.conf` |
| Alert in case of "dropped" network packets on the Gcap | `drop.conf` |
| Alert in case of disk filling (here the/data partition of the Gcap) | `disk.conf` |
| CPU overload alert | `cpu.conf` |

The creation of alerts is based on the metrics that Netdata collects.

- To know these metrics, you must connect to the GCenter Netdata interface.

```
https:// IP ou FQDN du GCenter /gstats
```

**RAM monitoring example**



The name of the Graph is *system.ram*, and the curve to watch is *used*.
The alert in the *ram.conf* file will be written as follows:

- The alarm is named as follows:

```
1>>  alarm: ram_usage
```

- The alarm is named as follows:

```
2>> on: system.ram
```

- The 10 min average of the used curve is calculated as follows:

```
3>> lookup: average -10m percentage of used
```

- The unit is specified as follows:

```
4>> units: %
```

- The time interval between each calculation is specified as follows:

```
5>> every: 1m
```

- Alert and critical thresholds are specified as follows:

```
6>> warn: $this > 70
7>> crit: $this > 90
```

- The delay to clear the alarm after triggering is specified as follows:

```
8>> delay: down 15m multiplier 1.5 max 1h
```

- The alarm description is specified as follows:

```
9>> info: average RAM utilization over the last 10 minutes
```

- The definition that will be alerted (see health_alarm_notify.conf) is defined as follows:

```
10>> to: sysadmin
```

## 8.9.4 Using a Netdata server

### 8.9.4.1 Introduction

This procedure gives as an indication the steps necessary to set up a Netdata monitoring server, and its interconnection to a GCenter to ensure monitoring.

**Note:**

The Netdata version compatible with GCenter and GCap is 1.19

### 8.9.4.2 Prerequisites

- User : member of **Administrator** group

### 8.9.4.3 Procedure to install via docker

- Install the Netdata docker.

```
docker pull netdata/netdata:v1.19.0
```

- To be able to edit the Netdata configuration from the host machine, a temporary container must be launched to retrieve the configuration files.

```
mkdir netdataconfig
docker run -d --name netdata_tmp netdata/netdata
docker cp netdata_tmp:/usr/lib/netdata netdataconfig/
docker rm -f netdata_tmp
```

- Launch the final container.

```
docker run -d --name=netdata \
 -p 19999:19999 \
 -v $(pwd)/netdataconfig/netdata:/usr/lib/netdata:rw \
 -v netdatalib:/var/lib/netdata \
 -v netdatacache:/var/cache/netdata \
 -v /etc/passwd:/host/etc/passwd:ro \
 -v /etc/group:/host/etc/group:ro \
 -v /proc:/host/proc:ro \
 -v /sys:/host/sys:ro \
 -v /etc/os-release:/host/etc/os-release:ro \
 --restart unless-stopped \
 --cap-add SYS_PTRACE \
 --security-opt apparmor=unconfined \
 netdata/netdata
```

#### 8.9.4.4 Procedure to configure the stream.conf file and GCenter

- Generate the uuid.

```
sudo docker exec -it netdata uuidgen
```

- Configure stream with the uuid generated previously.

  Netdata recommends using edit-config

```
sudo docker exec -it netdata /etc/netdata/edit-config stream.conf
```

```
[dd236090-a42d-43e2-b0ba-ff8eaa6216a2] << Remplacer l'uuid ici
    enabled = yes
    default history = 36000
    default memory mode = ram
    health enabled by default = auto
    allow from = *
    default postpone alarms on connect seconds = 60
```

#### 8.9.4.5 Procedure to configure the netdata.conf file

```
sudo docker exec -it netdata /etc/netdata/edit-config netdata.conf
```

```
[global]
       ...
       hostname = netdata-docker.gatewatcher.com
       ...
       timezone = Europe/Paris
```

#### 8.9.4.6 Procedure to configure the Netdata export in the GCenter

> **Note:**
>
> Read the *Setting up a Netdata server*.

- For Netdata to send notifications, the *health_alarm_notify.conf`* file must be configured.

```
sudo docker exec -it netdata /etc/netdata/edit-config health_alarm_notify.conf
```

Reference : Alarm Configuration

---

#### 8.9.4.7 Procédure to create alerts for Netdata

- Create alerts in the container folder.

```
/usr/lib/netdata/conf.d/health.d
```

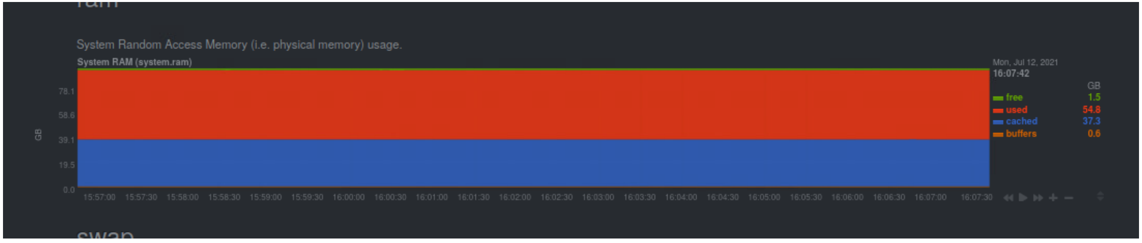
- In order for the new alerts to be taken into account, it is necessary to restart the docker container.
- To clarify the management of your alerts, it is advisable to create a **. conf`* file by alert category.
  Examples include:

| Description | Link |
|---|---|
| Alert in case of absence/traffic overload | `traffic.conf` |
| Alert in case of deactivation of GCap analysis services | `suricata_status.conf` |
| Alert if a restart of GCap/GCenter has occurred | `reboot.conf` |
| RAM overload alert | `ram.conf` |
| Alert in case of "dropped" network packets on the Gcap | `drop.conf` |
| Alert in case of disk filling (here the/data partition of the GCap) | `disk.conf` |
| CPU overload alert | `cpu.conf` |

- Create your own alerts.
  The creation of alerts is based on the metrics that netdata collects.
  - To know these metrics, you must connect to the Netdata interface of your GCenter.

    ```
    https:// IP ou FQDN du Gcenter /gstats
    ```

    Take the example of RAM monitoring.

    The Graph name is *system.ram`* and the curve to watch is *used.*
  - The alert in the *ram.conf`* file will be written as follows:
    - The alarm is called

      ```
      1>>  alarm: ram_usage
      ```

    - The chart is named in Netdata:

```
2>> on: system.ram
```

– Indicates that the 10 min average of the *used* curve

```
3>> lookup: average -10m percentage of used
```

– The unit is specified

```
4>> units: %
```

– The time interval between each calculation is specified

```
5>> every: 1m
```

– Alert and critical thresholds are defined

```
6>> warn: $this > 70
7>> crit: $this > 90
```

– Set time to clear alarm after tripping

```
8>> delay: down 15m multiplier 1.5 max 1h
```

– Description de l'alarme

```
9>> info: average RAM utilization over the last 10 minutes
```

– Define who will be alerted (see health_alarm_notify.conf)

```
10>> to: sysadmin
```

---

### 8.9.5 GCenter Global Configuration

#### 8.9.5.1 Introduction

This procedure describes the overall configuration of GCenter.

> **Note:**
>
> The GUI is described in *`Global settings` section*.

---

#### 8.9.5.2 Prerequisites

- User : member of **Administrator** group

---

#### 8.9.5.3 Preliminary operations

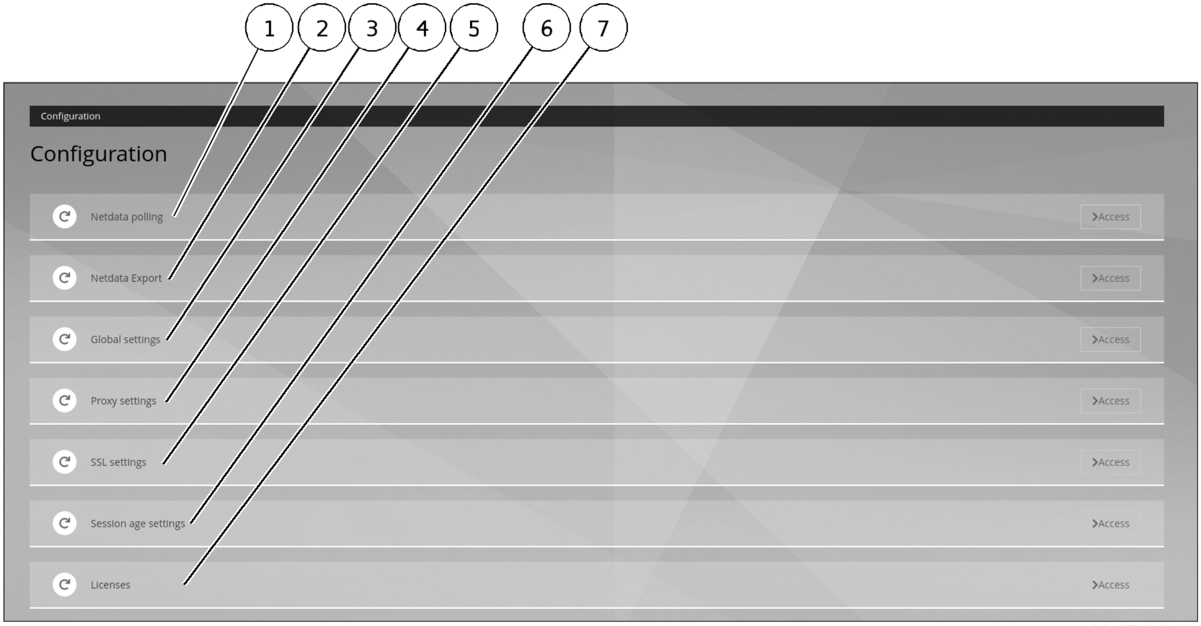
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

---

#### 8.9.5.4 Procedure to access the legacy web UI `Global settings` screen

- In the navigation bar, click successively on:
  - The `Admin` button,
  - The `Gcenter` sub menu
  - The `Configuration` command

  The `Configuration` window is displayed.



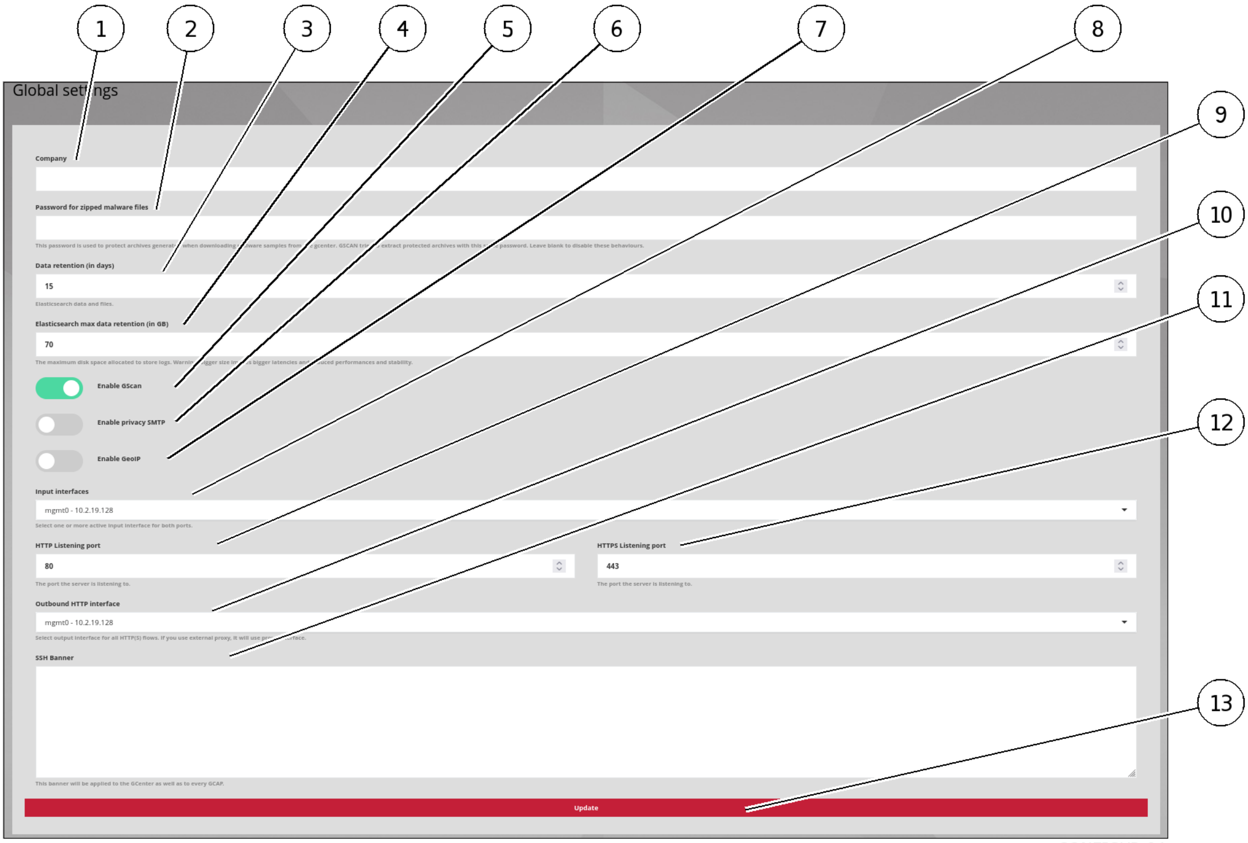
CONFIGUR-01

- Click the `Global settings` button (3).

---

#### 8.9.5.5 Procedure

The following screen is displayed:



Global settings

Company

Password for zipped malware files

This password is used to protect archives generated when downloading malware samples from the gcenter. GSCAN tries to extract protected archives with this same password. Leave blank to disable these behaviours.

Data retention (in days)

15

Elasticsearch data and files.

Elasticsearch max data retention (in GB)

70

The maximum disk space allocated to store logs. Warning: bigger size implies bigger latencies and reduced performances and stability.

Enable GScan: on

Enable privacy SMTP: off

Enable GeoIP: off

Input interfaces

mgmt0 - 10.2.19.128

Select one or more active input interface for both ports.

HTTP Listening port

80

The port the server is listening to.

HTTPS Listening port

443

The port the server is listening to.

Outbound HTTP interface

mgmt0 - 10.2.19.128

Select output interface for all HTTP(S) flows. If you use external proxy, it will use proxy interface.

SSH Banner

This banner will be applied to the GCenter as well as to every GCAP.

Update

CONFIGUR-04

- Enter the company name in field (1) `Company`.
  This field allows you to add the company name on the detection analysis reports.
  These reports can be downloaded after making an association between the GCenter and the Intelligence platform.
  The default is: empty.
- Enter the password that protects the archive when downloading malware in field (2) `Password for zipped malware files`.
  The default is: empty.
  This password protects the archive when downloading malware and decompresses it to avoid an unfortunate click.
  This password is the same for downloading shellcodes.
  This feature is described in more detail in the Malcore parts.
- Enter the number of days the data is stored in field (3) `Data retention (in days)`.
  The default is: 15.

> **Note:**
>
> The configuration is done in two steps:
> - First on GCenter at this field
> - The second at the GCap detection probe in the configuration settings

- Enter the maximum disk space allocated to store logs in field (4) `Elasticsearch max data retention (in GB)`.

**Attention:**

Larger size implies higher latencies and reduced performance and stability.

- Enable the selector (5) `` `Enable GScan` `` to allow real-time local analysis of suspicious malware or executables.

  The default is: enabled.

  **Note:**

  As part of the Military Programming Law, the GScan feature is disabled by default in this management interface.

- Enable selector (6) `` `Enable Privacy SMTP` `` to enforce privacy rights by hiding the email.subject field of SMTP alerts in GATEWATCHER dashboards for private emails.

  The default is: off.

  An email is considered private if its subject begins with the words private, private or private (not case sensitive).
- Select the network interface through which the GCenter is listening on the ports defined below in field (8) `` `Input interfaces` ``.
- Select the listening port (linked to http protocol) in field (9) `` `HTTP listening port` ``.

  The default is: 80
- Select the network interface (for all http streams) in field (10) `` `Outbound HTTP interface` ``.
- Enter the SSH banner (presented during pre-authentication on all paired GCaps and GCenter) in field (11) `` `SSH banner` ``.

  The default is: empty
- Select the listening port (linked to the https protocol) in the `` `HTTPs listening port` ``.

  The default is: 80
- Press the `` `Save` `` button (13) to save current settings and update the GCenter.

**Important:**

If the equipment **GCenter** and **GCap** is in an environment that is part of the LPM framework (Military Programming Law) the GSCAN service is automatically disabled and cannot be activated.
For more information, refer to the LPM section of this document.

## 8.9.6 Proxy Settings Configuration

### 8.9.6.1 Introduction

This procedure describes the configuration of the proxy server (or proxy) to communicate with:

- The MISP server
- The GBox
- The Gatewatcher update servers (via GUM)

**Note:**

The GUI is described in *`Proxy settings` section*.

#### 8.9.6.2 Prerequisites

- User : member of **Administrator** group

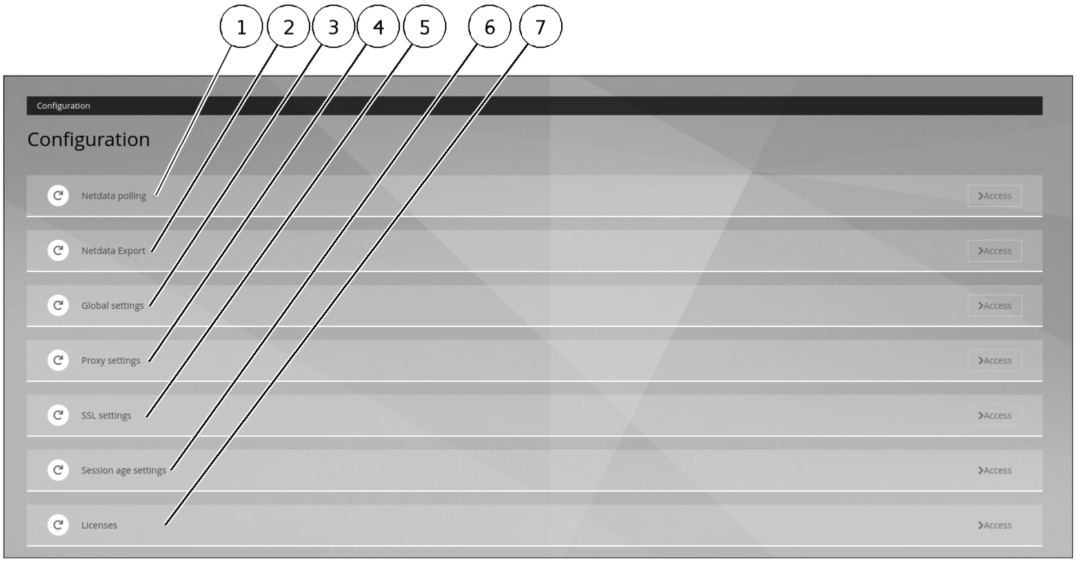
#### 8.9.6.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

#### 8.9.6.4 Procedure to access the `` `Proxy settings` `` screen of the legacy web UI

- In the navigation bar, click successively on:
  - The `` `Admin` `` command
  - The `` `Gcenter` `` sub menu
  - The `` `Configuration` `` command

  The `` `Configuration` `` window is displayed.

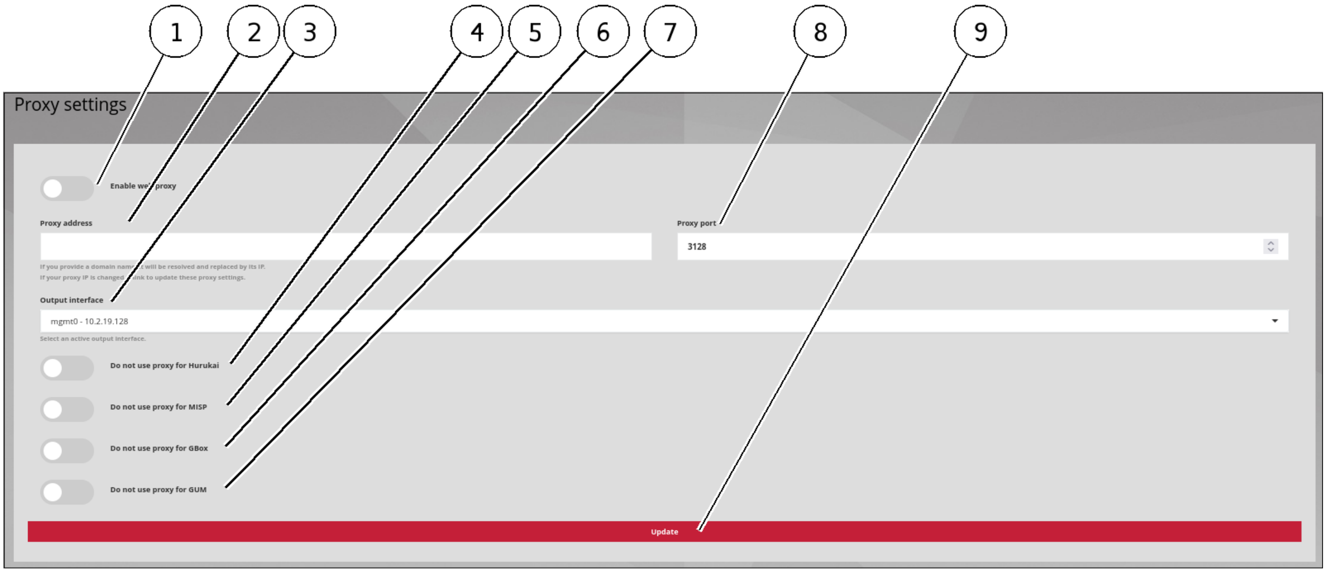


CONFIGUR-01

- Click on the button (4) `` `Proxy settings` ``.

#### 8.9.6.5 Procedure to enter parameters

The following screen is displayed:



Proxy settings

Enable web proxy

Proxy address

If you provide a domain name, it will be resolved and replaced by its IP.
If your proxy IP is changed, think to update these proxy settings.

Proxy port: 3128

Output interface: mgmt0 - 10.2.19.128

Select an active output interface.

Do not use proxy for Hurukai

Do not use proxy for MISP

Do not use proxy for GBox

Do not use proxy for GUM

CONFIGUR-05

- Use the selector (1) `Enable Web Proxy` to enable or disable the use of the proxy.
- Enter the proxy server address as an IP address or FQDN in the `Proxy address` field (2).
- Select the GCenter network interface to use in the `Output interface` field (3).
- Enter the Proxy Listening Port (1-65535) in the field (8) `Proxy port`.
- If necessary, use the selector (5) `Do not use proxy for MISP`.
- If necessary, use the selector (6) `Do not use proxy for GBOX`.
- Use selector (7) `Do not use proxy for GUM`.
- Press the `Save` button (9) to save current settings and update the GCenter.

**Note:**

This mode of updating is part of the compliance of the Military Programming Act (LPM).
Therefore the entity concerned will make its updates on a dedicated update server.
For more information, please refer to the appendix regarding the specificities related to the LPM.

---

## 8.9.7 SSL Settings Configuration

### 8.9.7.1 Introduction

This part allows you to configure the GCenter SSL (Secure Socket Layer) certificate.
The certificate generated certifies the identity of the GCenter and encrypts the data exchanged.
It is also possible from this page to configure mutual authentication (mTLS).

**Note:**

The GUI is described in *`SSL settings` section*.

---

#### 8.9.7.2 Prerequisites

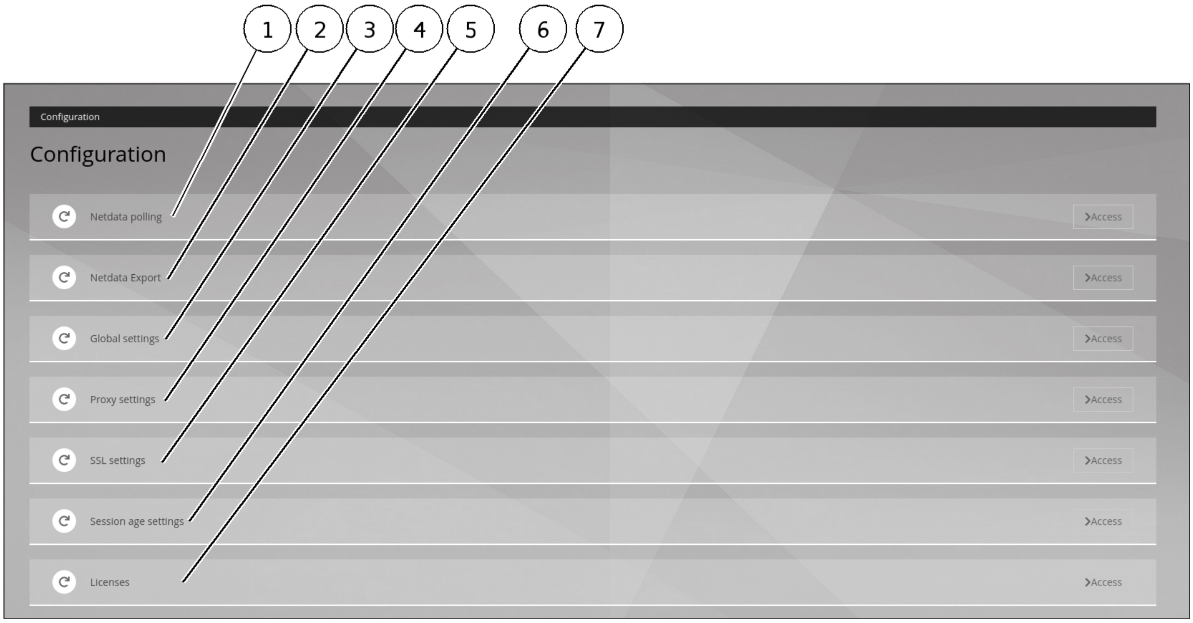
- User : member of **Administrator** group

#### 8.9.7.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

#### 8.9.7.4 Procedure to access the `SSL settings` screen of the legacy web UI

- In the navigation bar, click successively on:
  - The `Admin` button
  - The `Gcenter` sub menu
  - The `Configuration` command
    The `Configuration` window is displayed.



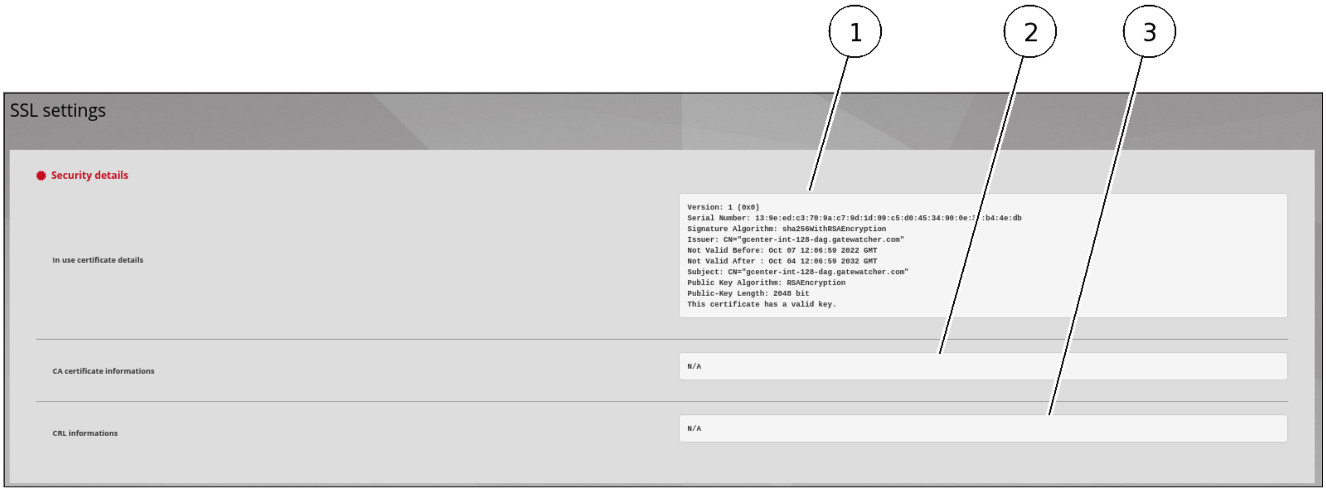
CONFIGUR-01

- Click on the button (5) `SSL settings`.
  The screen consists of the zones:

- Zone `Security details`
- Zone `Custom Certificate`
- Zone `Dual authentication`

### 8.9.7.5 Procedure to display the `Security details` zone parameters

The `Security details` area provides information about the certificate in use.



In use certificate details

```
Version: 1 (0x0)
Serial Number: 13:9e:ed:c3:70:9a:c7:9d:1d:09:c5:d0:45:34:90:0e:3[illegible]:b4:4e:db
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN="gcenter-int-128-dag.gatewatcher.com"
Not Valid Before: Oct 07 12:06:59 2022 GMT
Not Valid After : Oct 04 12:06:59 2032 GMT
Subject: CN="gcenter-int-128-dag.gatewatcher.com"
Public Key Algorithm: RSAEncryption
Public-Key Length: 2048 bit
This certificate has a valid key.
```

CA certificate informations: N/A

CRL informations: N/A

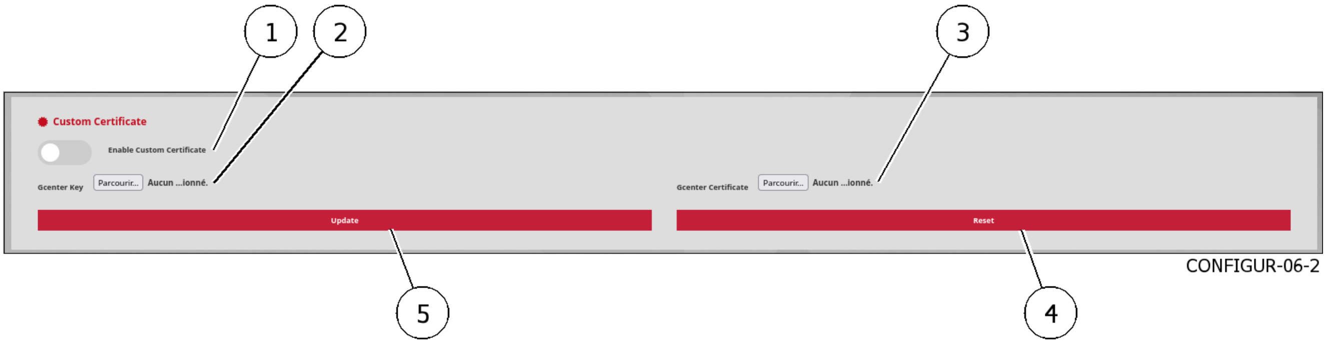
CONFIGUR-06-1

- View the following information:

| Item | Name | Function |
|---|---|---|
| 1 | Field `In use certificate details` | Displays certificate information such as issue and expiry date, issuer of this certificate, etc. |
| 2 | Field `CA certificate informations` | Displays the Certification Authority information to identify the identity of correspondents in the `Dual Authentication` |
| 3 | Field `CRL informations` | Lists credentials that have been revoked or invalidated and are no longer trustworthy. |

### 8.9.7.6 Procedure to enter the `Custom Certificate` zone parameters

The `Custom Certificate` field allows you to use a specific certificate.
To do this, simply specify the private key in the field `GCenter Key` and the certificate in PEM format in the field `GCENTER certificate`, and also activate this certificate by activating the selector `Enable Custom Certificate`.

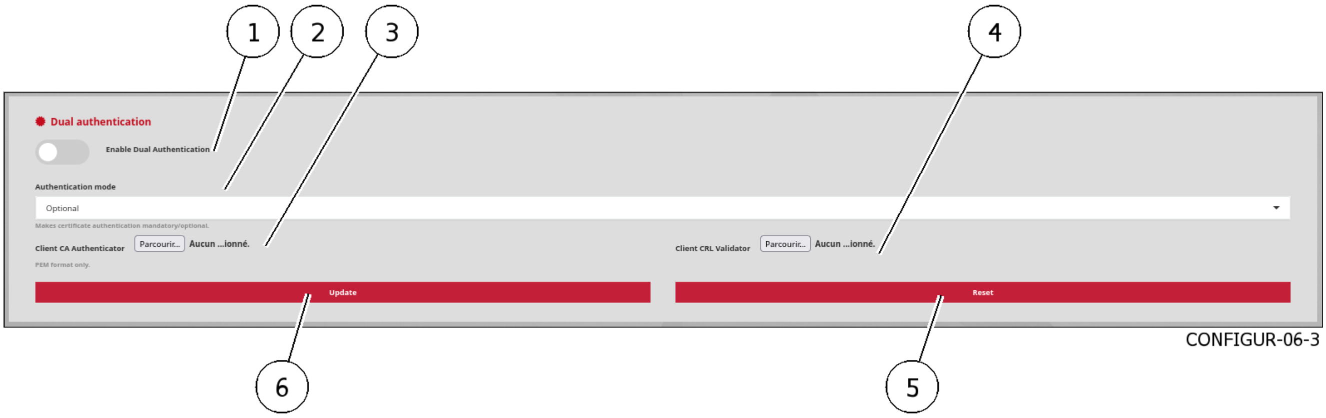


CONFIGUR-06-2

- Use the `Enable Custom Certificate` selector (1) to activate a custom certificate.
- Select the field (2) `GCenter Key` to select the GCenter key file.
- Select the field (3) `GCENTER certificate` to select the GCenter certificate file.
- If necessary, use button (4) `Reset` to reset the configuration.
- Press the `Update` button (5) to save current settings and update the GCenter.

#### 8.9.7.7 Procedure to enter the `Dual authentication` zone parameters

The `Dual Authentication` field allows you to enable mutual authentication (mTLS).
This allows the user to ensure the identity of the server but also the server to ensure the identity of the user.



Dual authentication

Enable Dual Authentication

Authentication mode

Optional

Makes certificate authentication mandatory/optional.

Client CA Authenticator Aucun ...ionné.

PEM format only.

Client CRL Validator Aucun ...ionné.

CONFIGUR-06-3

- Use the `Enable Dual Authentication` selector (1) to enable mutual authentication.
- Select the `Authentication mode` field (2) between the 2 choices:

- Choice `Forced`: makes mandatory the use of a certificate issued by the certification authority
- Choice `Optional`: checks only the presence of a certificate

- Select the field (3) `Client CA Authenticator` to select the certificate file issued by the CA Authenticator (PEM format).
- Select the field (4) `Client CRL Validator` to select the file from the list of revoked certificates.
- If necessary, use the button (5) `Reset` to reset the configuration.
- Press the `Update` button (6) to save current settings and update the GCenter.

### 8.9.8 Configuring Session Age Settings

#### 8.9.8.1 Introduction

This procedure describes the configuration of the maximum total duration of a session.

**Note:**

The GUI is described in *`Session age settings` section*.

### 8.9.8.2 Prerequisites

- User : member of **Administrator** group

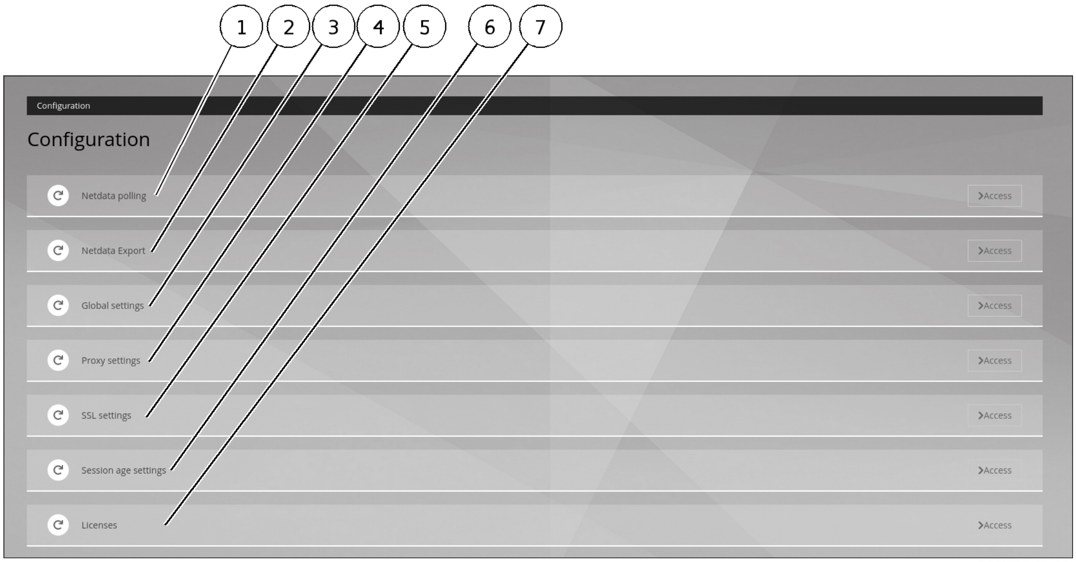
### 8.9.8.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

### 8.9.8.4 Procedure to access the legacy web UI `Session age settings` screen

- In the navigation bar, click successively on:
  - The `Admin` command
  - The `Gcenter` sub menu
  - The `Configuration` command

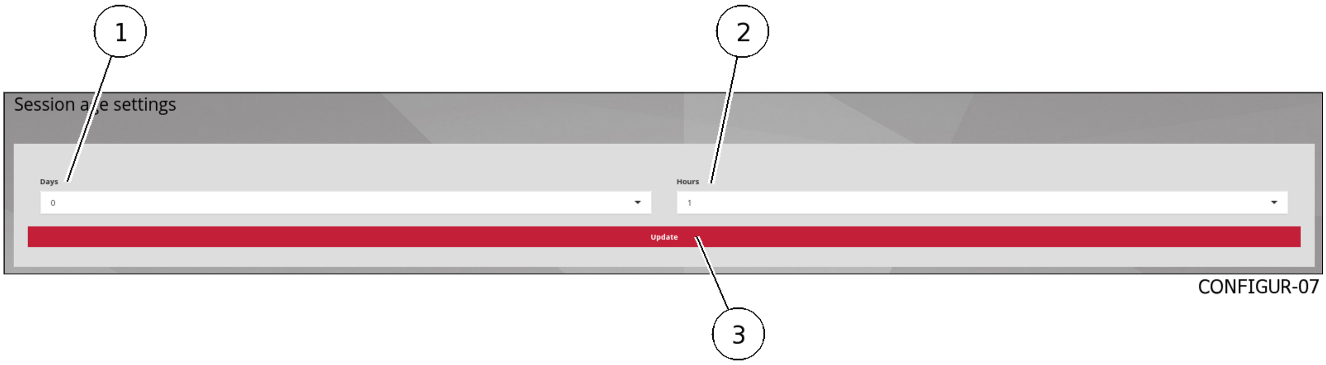
  The `Configuration` window is displayed.



CONFIGUR-01

- Click the button (6) `Session age settings`.

### 8.9.8.5 Procedure to enter session age parameters



Days: 0

Hours: 1

CONFIGUR-07

- Select the duration of the session in days in field (1) `Days`.
- Select the session duration in hours in field (2) `Hours`.
- Press the `Update` button (3) to save current settings and update the GCenter.

### 8.9.9 Licence amendment

#### 8.9.9.1 Introduction

This procedure describes viewing the current license information and changing it if necessary.

> **Note:**
>
> The GUI is described in *`License information` section*.

#### 8.9.9.2 Prerequisites

- User : member of **Administrator** group

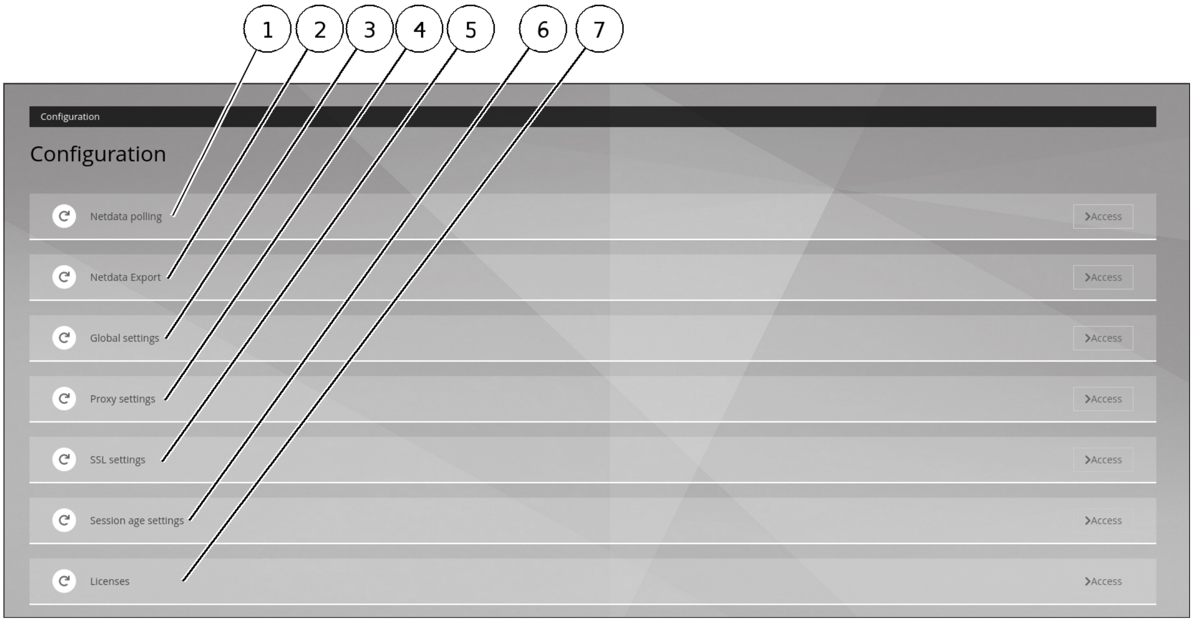
#### 8.9.9.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*). with the prerequisite rights.

#### 8.9.9.4 Procedure to access to the legacy web UI `License information` screen

- In the navigation bar, click successively on:
  - The `Admin` button
  - The `Gcenter` sub menu
  - The `Configuration` command

    The `Configuration` window is displayed.



Configuration

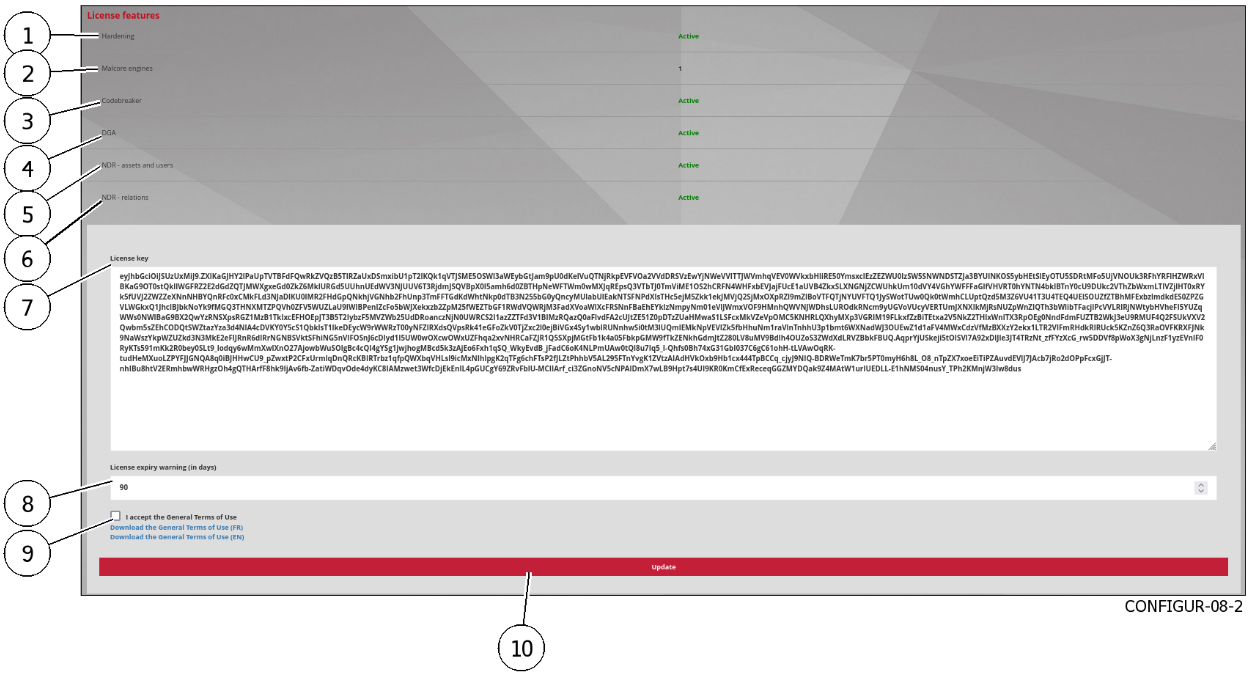
| | |
|---|---|
| Netdata polling | ›Access |
| Netdata Export | ›Access |
| Global settings | ›Access |
| Proxy settings | ›Access |
| SSL settings | ›Access |
| Session age settings | ›Access |
| Licenses | ›Access |

CONFIGUR-01

- Click the `Licenses` button (7).

### 8.9.9.5 Procedure to enter a new licence

In the `License features` area:



License features

| | |
|---|---|
| Hardening | Active |
| Malcore engines | 1 |
| Codebreaker | Active |
| DGA | Active |
| NDR - assets and users | Active |
| NDR - relations | Active |

License key

eyJhbGciOiJSUzUxMiJ9.ZXlKaGJHY2lPaUpTVTBFdFQwRkZVQzB5TlRZaUxDSmxibU1pT2lKQk1qVTJSME5OSWl3aWEybGtJam9pU0dKelVuQTNjRkpEVFVOa2VVdDRSVzEwYjNWeVVlTTJWVmhqVEV0WVkxbHliRE50YmsxclEzZEZWU0lzSW5SNWNDSTZJa3BYVUlNKOS5ybHEtSlEyOTU5SDRtMFo5UjVNOUk3RFhYRFlHZWRxVl
BKaG9OT0stQklIWGFRZ2E2dGdZQTJMWXgxeGd0ZkZ6MklURGd5UUhnUEdWV3NJUUV6T3RjdmJSQVBpX0I5amh6d0ZBTHpNeWFTWm0wMXJqREpsQ3VTbTJ0TmViME1OS2hCRFN4WHFxbEVJajFUcE1aUVB4ZkxSLXNGNjZCWUhkUm10dVY4VGhYWFFFaGlfVHVRT0hYNTN4bklBTnY0cU9DUkc2VThZbWxmLTlVZjlHT0xRY
k5fUVJ2ZWZZeXNnNHBYQnRFc0xCMkFLd3NJaDlKU0lMR2FHdGpQNkhjVGNhb2FhUnp3TmFFTGdKdWhtNkp0dTB3N255bG0yQncyMUlabUlEakNTSFNPdXlsTHc5ejM5Zkk1ekJMVjQ2SjMxOXpRZl9mZlBoVTFQTjNYUVFTQ1JySWotTUw0Qk0tWmhCLUptQzd5M3Z6VU41T3U4TEQ4UElSOUZfZTBhMFExbzlmdkdES0ZPZG
VLWGkxQ1JhclBJbkNoYk9fMGQ3THNXMTZPQVh0ZFV5WUZLaU9lWlBPenlZcFo5bWJXekxzb2ZpM25fWEZTbGF1RWdVQWRjM3FadXVoaWlXcFRSNnFBaEhEYklzNmpyNm01eVlJWmxVOF9HMnhQWVNJWDhsLUROdkRNcm9yUGVoVUcyVERTUmJXNXlkMjRsNUZpWnZlQTh3bWlibTFacjlPcVVLRlRjNWtybHVheFI5YUZq
WWs0NWlBaG9BX2QwYzRNSXpsRGZ1MzB1TklxcEFHOEpjT3B5T2lybzF5MVZWb25UdDRoanczNjN0UWRCS2I1azZZTFd3V1BIMzRQazQ0aFlvdFA2cUJtZE51Z0pDTzZUaHMwaS1LSFcxMkVZeVpOMC5KNHRLQXhyMXp3VGRlM19FLkxfZzBiTEtxa2V5NkZ2THlxWnlTX3RpOEg0NndFdmFUZTB2WkJ3eU9RMUF4Q2FSUkVXV2
Qwbm5sZEhCODQtSWZtazYza3d4NlA4cDVKY0Y5cS1QbklsT1lkeDEycW9rWWRzT00yNFZlRXdsQVpsRk41eGFoZkV0TjZxc2l0ejBiVGx4Sy1wblRUNnhwSi0tM3lUQmlFMkNpVEVlZk5fbHhuNm1raVlnTnhhU3p1bmt6WXNadWJ3OUEwZ1d1aFV4MWxCdzVfMzBXXzY2ekx1LTR2VlFmRHdkRlRUck5KZnZ6Q3RaOVFKRXFJNk
9NaWszYkpWZUZkd3N3MkE2eFlJRnR6dlRrNGNBSVktSFhiNG5nVlFOSnJ6cDlyd1I5UW0wOXcwOWxUZFhqa2xvNHRCaFZJR1Q5SXpjMGtFb1k4a05FbkpGMW9fTkZENkhGdmJtZ280LV8uMV9Bdlh4OUZoS3ZWdXdLRVZBbkFBUQ.AqprYjUSkeji5tOISVl7A92xDIJle3JT4TRzNt_zfFYzXcG_rw5DDVf8pWoX3gNjLnzF1yzEVnIF0
RyKTs591mKk2R0bey0SLt9_lodqy6wMmXwlXnO27AjowbWuSOlgBc4cQl4gYSg1jwjhogMBcd5k3zAjEo6Fxh1qSQ_WkyEvdB_jFadC6oK4NLPmUAw0tQl8u7lq5_l-Qhfs0Bh74xG31GbI037C6gC61ohH-tLVAwOqRK-
tudHeMXuoLZPYFJJGNQA8q0iBJHHwCU9_pZwxtP2CFxUrmlqDnQRcKBIRTrbz1qfpQWXbqVHLsl9icMxNlhlpgK2qTFg6chFTsP2fJLZtPhhbV5AL295FTnYvgK1ZVtzAlAdHVkOxb9Hb1cx444TpBCCq_cjyJ9NIQ-BDRWeTmK7br5PT0myH6h8L_O8_nTpZX7xoeEiTiPZAuvdEVlJ7JAcb7jRo2dOPpFcxGjJT-
nhlBu8htV2ERmhbwWRHgzOh4gQTHArfF8hk9lJAv6fb-ZatiWDqvOde4dyKC8lAMzwet3WfcDjEkEnIL4pGUCgY69ZRvFbIU-MCIIArf_ci3ZGnoNV5cNPAIDmX7wLB9Hpt7s4UI9KR0KmCfExReceqGGZMYDQak9Z4MAtW1urIUEDLL-E1hNMS04nusY_TPh2KMnjW3lw8dus

License expiry warning (in days): 90

☐ I accept the General Terms of Use

Download the General Terms of Use (FR)

Download the General Terms of Use (EN)

CONFIGUR-08-2

- Enter the license key in field (7) `License key`.
- Enter the number of days of the license expiry alarm message in field (8) `License expiry warning (in days)`.
- Tick the choice (9) `I accept the General Terms of Use`.
- Press the `Update` button (10) to save current settings and update the GCenter.

Once the license, validated and activated the content of the page updates and displays the details of the content of the license.

In case of missing or expired license, the interface will automatically redirect to this page in order to resolve the situation.

## 8.10 Logging out of the GCenter web interface

### 8.10.1 Introduction

This procedure describes how to log out of the GCenter web interface.

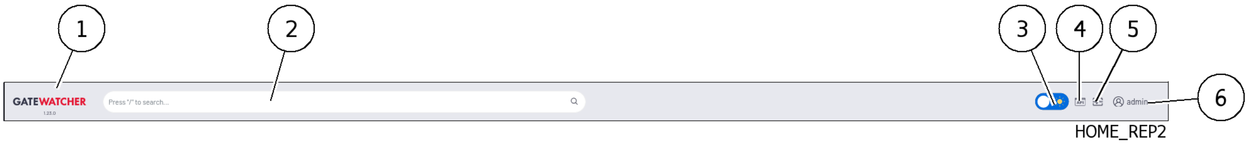
### 8.10.2 Prerequisites

- User: all users

### 8.10.3 Preliminary operations

- Accessing GCenter from your workstation (*Connecting to the GCenter web interface via a web browser*).

### 8.10.4 Procedure



- In the GCenter interface, click on the current account button (6).
- Select the `Logout` command.

  The GCenter interface is closed and the login screen is displayed.

# Chapter 9

# Appendices

## 9.1 Military Programming Law (MPL)

### 9.1.1 Regulatory reminders

Some reminders of the main principles of the french Military Programming Law (MPL):

- Fench Military Programming Law (Act no. 2013-1168 of 18 December 2013)
- Article 22: implementation supervised by the ANSSI for the OIVs
  - Impose security measures,
  - Impose controls on the most critical information systems
  - Make it compulsory to report incidents observed by OIVs on their information systems
- Article L.1332-6-1 of the Defense Code amended by Act no. 2015-917 of 28 July 2015 - Art. 27
  - Establish organizational and technical measures
  - Define procedures for identifying and reporting security incidents affecting vital information systems (SIIV)

### 9.1.2 Goal Reminders

The objectives are :

- To protect national critical infrastructures against cyber attacks
- Reduce exposure to risks and
- Optimise the quality of services provided by organisations

### 9.1.3 Reminders of requirements

Requirements for OIVs and security incident detection service provider (PDIS) actors are to be taken into account on equipment:

- Implement an information systems security policy
- Carry out a security certification
- Communicate the elements on the IVIS set up by the operator to the ANSSI
- Observe and react to security alerts
- Limit access
- Partition the networks
- Select the qualified technologies

### 9.1.4 MPL applied to GCenter

**Note:**

Whatever the mode, the AIONIQ solution integrates GRSECURITY improvements, including PaX, thus reducing the attack surface including at the kernel level.

The specific configuration points that allow the solution to comply with the Military Programming Law are presented here.
Although a number of actions are performed automatically when entering MPL mode, the administrator will have to customise and modify some of the parameters manually:

- AD/LDAP **manual action required**
- USB port **automatic action**
- Update in "Offline" mode **manual action required**
- Interface separation **manual action required**
- Certificate integration **manual action required**
- iDRAC Disabled **manual action required**
- The groups **manual action required**

#### 9.1.4.1 Automatic actions

##### 9.1.4.1.1 USB Port

Access via USB ports can involve risks.
When the AIONIQ solution is in MPL mode, the USB ports are automatically disabled

USB ports are automatically deactivated after switching to LPM mode from the **SETUP** profile settings configuration menu.
If a USB device is already plugged in, the port used will not deactivate until after disconnecting the present media.
In order for it to be supported again, you will need to restart the GCenter by reconnecting the device before booting.

**Note:**

This limits access to the device's TTY.

### 9.1.4.2 Manual actions

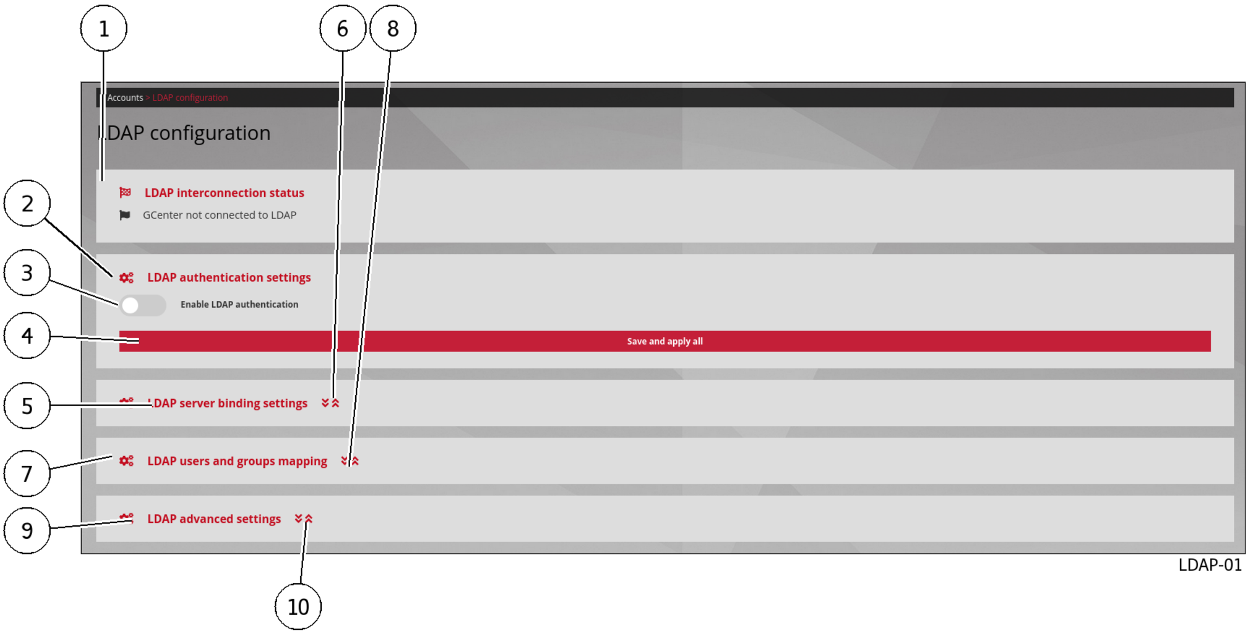
The following list of actions should only be performed by an administrator of the AIONIQ solution.

#### 9.1.4.2.1 No connection between GCenter and AD LDAP

In the context of an IS subject to the MPL, there are certain constraints, in particular the fact that the GCenter is not connected to an Active Directory or LDAP.

It is necessary to check whether this is the case.

To do this, go to the ADMINISTRATORS section of the GCenter and click on Accounts and LDAP configuration.



Accounts > LDAP configuration

LDAP configuration

LDAP interconnection status

GCenter not connected to LDAP

LDAP authentication settings

Enable LDAP authentication

Save and apply all

LDAP server binding settings

LDAP users and groups mapping

LDAP advanced settings

In the `LDAP authentication settings` (2) area:

- Deselect the `Enable LDAP authentication` selection and
- Click the `Save and apply` button to take the change into account.

This change will cause the application to restart, resulting in a disconnection from the user page.

Once the administrator clicks the `Confirm` button, it will be necessary to reconnect to the interface.

After this manipulation and reconnection to GCenter, a green banner is visible and indicates the validation of the change.

`LDAP interconnection status` indicates that GCenter is now disconnected from the Active Directory or LDAP.

#### 9.1.4.2.2 Deactivation of remote control console interface

The remote control console interface is made via a specific network connection.
This connection interface is called iDRAC at Dell (or TSM at Lenovo).

According to ANSSI, it is recommended to disable this interface for security reasons.
Under certain conditions, it can nevertheless be reactivated by the administrator to facilitate maintenance.

---

#### 9.1.4.2.3 Network interface separation

As part of an IS subject to the LPM, the GCenter must have a special configuration of its network interfaces.
Indeed, in order to guarantee this compliance and a good level of security, the management flow and that of the interconnection with the GCap must be on two different interfaces respectively [MGMT0] and [VPN0].
This change is not effective automatically after LPM mode is enabled, even if the network cables are correctly connected.
It is precisely from the **SETUP** interface that the administrator can modify and manually add a new IP address for the [VPN0] interface.
Only the [MGMT0] and [VPN0] interfaces are impacted. Refer to the setup configuration document to make the change.
Details of flows in this mode are described in section *Interconnection between devices*.
For even more security, sending logs to a SIEM in an operating area can therefore be done through a dedicated interface by separating the management interface (administrator) from the log export interface (operator).

---

#### 9.1.4.2.4 Update in "Offline" mode

In order for the AIONIQ solution to comply with the Military Programming Law, signature updates must be done in Manual or Local mode.
Therefore, there are two possibilities:

- Either from the **GCenter** web interface (see section *Update Local*). This is a *manual* update.
- Or via a location on the network, disconnected from the internet, (see section *Update Manual*). This corresponds to an *Local* update.

---

##### 9.1.4.2.4.1 Certificate integration

In order to comply with the specific requirements concerning the use of cryptographic mechanisms, GATEWATCHER advises referring to the documents written by the national authority on information system security and defence.
The Military Programming Law imposes rules and recommendations concerning the management of the keys used, authentication mechanisms, and the choice and sizing of cryptographic mechanisms.
All these prerequisites are available in the RGS General Security Reference (RGS B1, RGS B2, and RGS B3) of the ANSSI.

The *`SSL settings` section* section indicates how to add your own SSL configuration.

---

### 9.1.5 Groups

In order to respect the separation of roles on the GCenter, default groups are already created to facilitate user management:

- The operators group
- The administrators group

A user is therefore a member of one or both groups.
Profiles are managed from *`Admin-GCenter- Accounts` screen of the legacy web UI*

---

#### 9.1.5.1 Mission of a member of the operator group

A member of the operator group has as mission :

- Viewing of synthetic dashboards via the WEB UI interface showing information about the monitored system

- Main dashboard (Home) to synthetically display alarms classified by level of risk
- Dashboard to display the network map. It shows the relationships between the elements present on the network
- Dashboards to display alarms classified by criteria (Users, Assets, Alerts) or by type of risk (Overview)

- Consultation of detailed dashboards via the Kibana interface showing the data information present in the detection event dashboards.
- Own account management

- Changing the current account password
- Modification of certain information of the current user

- Sigflow engine configuration

- Management of SIGFLOW engine rule sources
- Creation of a ruleset of the SIGFLOW engine
- Modification of SIGFLOW engine rules
- Generation of SIGFLOW engine rulesets

- GCap configuration from GCenter from GCaps Profiles

- Détection ruleset
- Base variables
- Net variables
- File rule management
- Packet filters

---

#### 9.1.5.2 Mission of a member of the administrator group

A member of the administrator group is responsible for:

- NDR configuration, for example:

- Alerts displayed in the Alerts dashboard
- The equipment displayed in the Assets dashboard
- Users displayed in the Users dashboard

- Administrating a GCap, for example:

- Pairing a GCap with the GCenter
- Re-pairing a GCap
- Changing the default profile or customise the existing profile
- Deleting a GCap connected to the GCenter

- Managing the GCenter backup and restoration, for example:

- Backup configuration
- Backup
- Restoration

- Managing of the GCenter software

- Updating signatures
- Installing a hotfix
- Upgrading software

- Administrating the GCenter

- Exporting data (log files)
- Deleting data (log files)
- Generating and loading files for diagnosis

- Managing user account

- Creating local users
- Changing some of a local user's information
- Resetting a local user's password
- Deleting a local user
- Displaying of the connection status between the GCenter and the LDAP server
- Enable the connection between the GCenter and the LDAP server
- Configuring the connection between the GCenter and the LDAP server
- Configuring the users and groups defined on LDAP / ActiveDirectory
- Viewing the authentication history
- Viewing the history of user creations or deletions
- Viewing the history function for all changes in user rights
- Adding an API access token
- Managing the password policy

- Configuring the detection engine

- Setting up GBox and the Malcore and Retroact engines
- Managing the white and black lists of the Malcore engine
- Enabling and configuring the Machine Learning engine
- Managing the white and black lists of the Machine Learning engine

- Configuring the GCenter

- Displaying the information (name of the GCenter, version of the GCenter software, characteristics of the IP address of the mgmt0 interface)
- Generating a text report of the GCenter status ("Tech Support")
- Changing the keyboard language (US or FR choice)
- Changing the password of the access account setup
- Changing the date and time of the GCenter

- Viewing and modifying GCenter network settings
- Management of the ARP table and its cache
- Changing the MTU value of the IPsec tunnel interface (mgmt0 or vpn0)
- Execution of various actions on the network to validate the correct GCenter configuration
- Choice of the type of update required
- Managing the GCenter services and applications (start, reset, restart)
- Modifying the storage mode for the alerts and the metadata
- Changing the LPM mode (on/off)
- Restarting / Shutdowning GCenter
- Reconfiguring the GCenter in its factory settings

# Chapter 10

# Glossary

**Alerting**
Enables detection of Sigflow signatures for a given protocol. If the latter is enabled for a protocol then the flow that is identified by a signature will raise an alert on the GCenter sid

**ANSSI**
The National Authority for Security and Defence of Information Systems is a French Service with national competence responsible for IT security.

**CLI**
The CLI (Command Line Interface) is the means used to administer and configure the GCap. It is the set of commands in text mode.

**Codebreaker**
Scanning engine for detection of malicious shellcode and powershell.

**Critical risk**

**Low Risk Definition**: highly suspicious activity was detected. Hazardous activity was detected. There is a high probability that your organization is facing a serious threat and countermeasures should be taken immediately.

For example, a user downloaded malware or an active element from the network contacted a known control and control domain.

**Color definition used for this type of alarms in Web UI** : red

**Level of risk in this category**: 75-100%

**Engine hash**
Name of 16 MALCORE antivirus engines

**GCap**
GCap is the detection probe for the Trackwatch/Aioniq solution. It retrieves the network flow from the TAP and reconstructs the files it sends to the GCenter.

**GCenter**
The GCenter is the component that administers the GCap and performs the analysis of files sent by the GCap.

**GUM**
The GUM (Gatewatcher Update Manager) is the service for the management of detection database updates, hotfix application and system updates

**High risk**

**High Risk Definition**: very suspicious activity has been detected. This type of event should be investigated promptly as it could be a sign of significant compromise.

It is possible that this event is a false positive or related to a bad figuration in your network.

**Color definition used for this type of alarms in Web UI** : orange

**Level of risk in this category**: 50-74%

**LDAP**
LDAP is a protocol for querying and modifying directory services (Active Directory for example)

**Logging**

Enables metadata generation for a given protocol. Indeed, if the latter is enabled for a protocol then each observed session will generate metadata for that protocol on the GCenter side.

**Low risk**

**Low risk definition**: unusual activity detected. This could mean that you have unusual policies or network uses.

These types of events should be mentioned last as they are not a direct sign of significant compromises.

They can be used as good indicators to improve network policies and detect configuration errors.

**Color definition used for this type of alarms in Web UI** : blue

**Level of risk in this category**: 0-24%

**Malcore**

Detection engine for malware detection and analysis

**Medium risk**

**Medium Risk Definition**: an activity that could be linked to a threat has been identified. Risk has been set at low values, because the potential threat does not appear critical or because the likelihood of forgery is high.

**Color definition used for this type of alarms in Web UI** : yellow

**Level of risk in this category**: 25-49%

**Mitre**

Knowledge base and behaviour model of cyber-adversaries, reflecting the phases of an adversary's attack life cycle and the platforms it targets.

**MTU**

The MTU (Maximum Transfer Unit) is the maximum size of a packet that can be transmitted at once (without fragmentation) over a network interface.

**OIV**

Operators of Vital Importance

**OTP**

The One Time Password (OTP) is a one-time password defined on the GCenter.

**RAID1**

RAID 1 is the use of n redundant disks. Each disk in the cluster containing exactly the same data at any time, hence the use of the word «mirror» (mirroring).

**RAID5**

The RAID 5 uses several hard drives (minimum 3) grouped in a cluster to form a single logical unit. The data is duplicated and distributed on 2 different disks among the present disks.

**setup**

Account name for a system administrator to access the configuration menu

**SIEM**

SIEM (Security Information and Event Management) is a centralized system of security events that provides total visibility on the activity of a network and thus allows to react to threats in real time.

**Sigflow**

The detection engine (also called Sigflow) is responsible for reconstituting files and also one of the engines for analyzing all network traffic and can, according to **rules**, generate alerts, metadata or content.

**TAP**

The TAP (Test Access Point) is a passive device that duplicates a network flow.

PDF Documentation GCenter

# Index