# Documentation
# GBox Version 2.5.3.102


Documentation version: V1

Translated from original manual version 1

Creation date: December, 2023

# Contents

**Index 195**

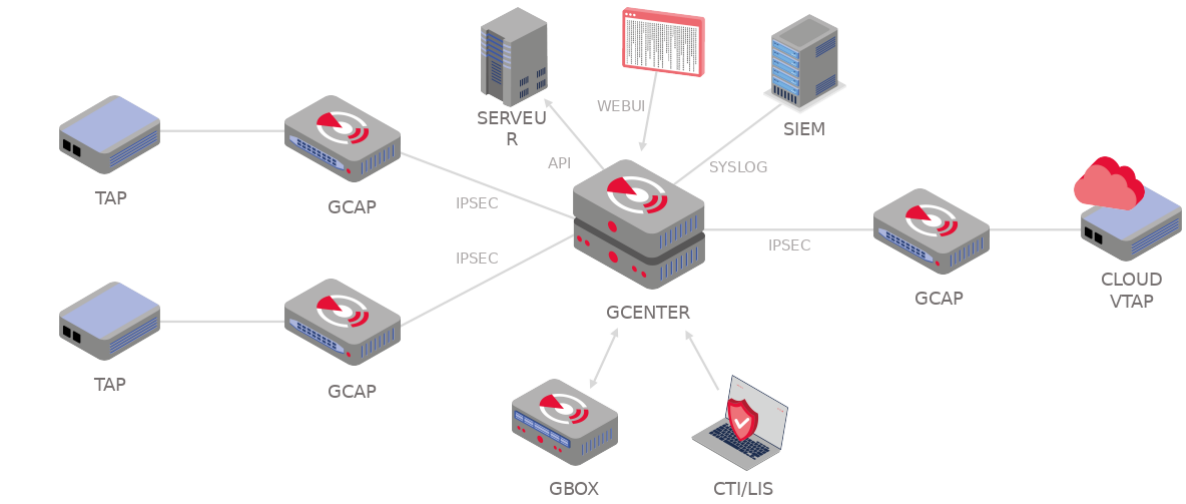
# Chapter 1

# Description

## 1.1 Introduction

The solution proposed by Gatewatcher includes:

- 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 Overview of the GCap

The GCap is an IDS type detection probe.
It enables:

- Capturing and analysing network traffic from TAPs
- Generating alerts and/or metadata type events
- Rebuilding the files present in the analysed flow according to type and size parameters
- Transmitting the captured events and files to the GCenter

For more information, please refer to the GCap documentation.

---

## 1.4 Overview of the GCenter

The GCenter is the second component of the system working in conjunction:

- With the GCap detection probe
- With the GBox

Its main functions include:

- 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

For more information, please refer to the GCenter documentation.

---

## 1.5 Overview of the GBox

GBox is a device that can operate independently or in conjunction with the GCenter.
This *appliance* enables:

- automatically receiving suspicious files requiring in-depth malware analysis, without having to rely on an external service
- Analysing suspicious files on demand from the GCenter's Web UI interface
- sending reports back to the GCenter for files submitted to it that are visible from the GCenter's Web UI and from the GBox's Web UI
- Analysing files directly on the GBox Web UI and generating a corresponding report
- users to manually analyse domain names that were generated by the Domain Generation Algorithm (DGA).

It is equipped with four complementary analysis engines, enabling static, dynamic, and heuristic analysis, as well as detection of *shellcode* and an engine to identify domain names generated by the DGAs.
These analysis engines are discussed in more detail in the *Analysis engines* section.

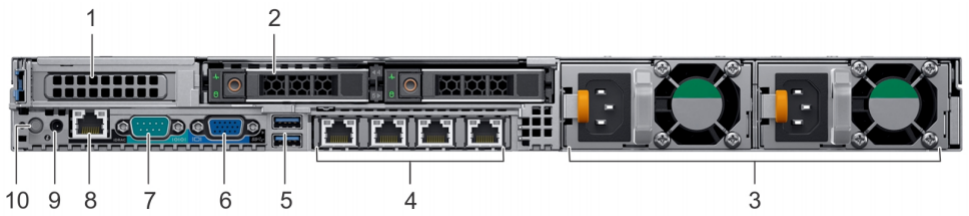
---

### 1.5.1 Server templates

For more information, please refer to the *Mechanical characteristics* section.

---

### 1.5.2 List of the GBox inputs / outputs




The **GBox** comprises:

| Item | Name |
|---|---|
| 4 | RJ-45 connector `GBX0`: management interface and link with the **GCenter** .<br>RJ-45 connector `GBX1`: interface dedicated to Virtual Machines for Internet access, Gnest VMs can be accessed via this link.<br>RJ-45 connector `GBX2`: Not used<br>RJ-45 connector `GBX3`: Not used |
| 5 | USB connector: accommodates the USB key enabling disk decryption (standard Linux Unified Key Setup)<br>USB connector: direct access via keyboard<br>This connection mode is deprecated in favour of KVM/IDRAC/XCC and should only be used as a last resort. |
| 6 | VGA connector: direct access with a screen.<br>This connection mode is deprecated in favour of KVM/IDRAC/XCC and should only be used as a last resort. |

**Note:**

Connector details can be found in the Dell EMC PowerEdge R640 Installation and Service Manual.

---

#### 1.5.2.1 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.

---

#### 1.5.2.2 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.

---

#### 1.5.2.3 Interface network `Gbx0`

This interface enables remote administration using the SSH protocol to access:

- The installation/configuration menu
- The Web user/administration interface

This interface also serves to send files to be analysed from the GCenter to the GBox.

---

#### 1.5.2.4 Interface network `Gbx1`

This network interface enables the Gnest engine's virtual machines (sandboxes) to access the Internet directly or via a proxy.
This access is optional and must be configured.

---

#### 1.5.2.5 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.

---

#### 1.5.2.6 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 has started up, we recommend removing this USB key and placing it in a secure place (e.g. a safe).

---

# Chapter 2

# Operation

## 2.1 Analysis engines

### 2.1.1 Overview of the Grip engine

The **Grip** analysis engine enables static analysis and shows file characteristics.
It does not provide threat information or a threat score.
However, it is useful for quickly analysing the file's metadata if it is classified as *suspicious* or *malicious*.
It is used to obtain information about the file prior to more in-depth analysis.
This data is displayed in the detailed report, more specifically in the **TOP** and **Static** sections (see *Detailed report*).

| | |
|---|---|
| **Maximum file size** | 50 MB |
| **Analysis timeout** | 2 minutes |
| **Type** | light |

---

#### 2.1.1.1 Viewing the Grip status

The current state of the engine is shown in the *`Analysers` screen of the Web UI*.

---

#### 2.1.1.2 Updating Grip

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

---

#### 2.1.1.3 Configuring the Grip

The engine is not configurable.

---

### 2.1.2 Overview of the Goasm engine

This analysis engine enables detecting and analysing **shellcodes**.
It enables identifying certain encodings and provides details of the system calls made.
This engine assigns a score to the potential danger and names the shellcode detected.
This data is displayed in the detailed report, more specifically in the **TOP** and **Shellcode** sections (see *Detailed report*).

| | |
|---|---|
| **Maximum file size** | 50 MB |
| **Analysis timeout** | 4- 6 minutes |
| **Type** | rapid |

Goasm can be deemed fast for small files (< 5MB).
In the case of large text files (> 5MB), detection takes time because the binary must be scanned for shellcode patterns.
Goasm's internal analysis timeout can therefore be reached: 4 min.
The external engine timeout is set at 6 min.

In the event of an internal timeout:

- There is an error message in the `Shellcode` section of the report
- The engine simply stops scanning the file byte by byte.

In the event of an external timeout (error occurred or Goasm blocked), an error is present in the report mentioning a timeout. In this case, restart the analysis.

---

#### 2.1.2.1 Viewing of the Goasm current state

The current state of the engine is shown in the *`Analysers` screen of the Web UI*.

---

#### 2.1.2.2 Update Goasm

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

---

#### 2.1.2.3 Configuring Goasm

The engine is not configurable.

---

### 2.1.3 Overview of the Gmalcore engine

The **Gmalcore** detection engine enables:

- detecting malware by means of a static and heuristic multi-engine analysis of files in real time
- scanning via 16 anti-virus engines
- scanning capacity close to 200,000 files per 24 hours
- obtain the name(s) of the threat and a threat score
- rapid identification of threats

The 16 anti-virus engines are displayed under the name `` `engine hash` `` in the web interface.

| | |
|---|---|
| **Maximum file size** | 50 MB |
| **Analysis timeout** | 2 minutes |
| **Type** | light |

Events generated by Gmalcore are displayed in the `` `Heuristic` `` section of the GBox analysis report.

---

#### 2.1.3.1 Viewing the Gmalcore status

Viewing the current state of the engine is shown in the *`Analysers` screen of the Web UI*.

---

#### 2.1.3.2 Gmalcore update

Updates are available for the Gmalcore engine.
These updates can be done manually or scheduled via GUM.
See the *Overview of GUM: dedicated module for managing updates* section and in particular the *Updates to detection signatures and/or anti-virus engines* section.

---

#### 2.1.3.3 Configuring Gmalcore

The Gmalcore configuration shows engine statuses including status, date of last update, etc.
The configuration GUI is described in the *`Gmalcore configuration` screen* section.
The implementation of the Gmalcore configuration is provided in *Procédure to configure the Gmalcore engine*.

---

### 2.1.4 Overview of the Gnest engine

The **Gnest** analysis engine enables dynamic analysis.
It executes the file in a virtual machine (sandbox) and analyses its behaviour.
Following this, it is possible to extract the data generated during the analysis, such as a *dump* of the memory, the extracted character strings, or a capture of network communications (pcap).
When connected to the GCenter, this engine is useful for in-depth analysis of a file classified as *suspicious* or *malicious*, during a second analysis of a file.
This analysis is slower, requiring an experienced operator to analyse the results.

This data is displayed in the *Detailed report* and more specifically in the **TOP**, **Iocs**, **Ttps**, **Overview**, **Signatures** and **Process Tree** sections.

| | |
|---|---|
| **Maximum file size** | 50 MB |
| **Analysis timeout** | 1 hour |
| **Type** | slow |

---

#### 2.1.4.1 Viewing the Gnest status

Viewing the current state of the engine is shown in the *`Analysers` screen of the Web UI*.

---

#### 2.1.4.2 Gnest update

Updates are available for the Gnest engine via packages.
These updates can be done manually or scheduled via GUM.
See the *Overview of GUM: dedicated module for managing updates* section an and in particular the *Updates to detection signatures and/or anti-virus engines* section.

---

#### 2.1.4.3 Configuring the Gnest

Configuring Gnest involves:

- Managing and configuring virtual machines.
  The graphical interface for managing virtual machines is described in the *`Gnest configuration` screen*.
  The implementation is given in the *Procedure to configure the Gnest engine*.
- Authorising virtual machines to connect to the Internet via a network interface (see paragraph below).

The use of Gnest in templates, and in particular the configuration of Gnest in these templates, enables:

- Choosing the active virtual machine
- Activating the VM's network interface
- Configuring the maximum execution time in the VM
- Enabling or disabling the memory dump at the end of the analyses performed by Gnest

The graphical interface for template management is described in the *`Admin/Templates` screen of the Web UI*.
The implementation is given in the *Procedure to configure the Gnest engine*.

---

#### 2.1.4.4 Configuring Sandbox services

Configuration consists of:

- Enabling or disabling the output interface to the Internet
- Configuring this interface (IP address, etc.)
- Configuring a proxy to access the Internet

This configuration is achieved using the `services` command in the configuration menu accessible by the setup user.
The graphical interface is described in *`Services` command* section.

**Important:**

This proxy is independent of any proxy accessible via the Web UI. This is used solely for installing software.

---

### 2.1.5 Overview of the Gdgadetect engine

#### 2.1.5.1 Introduction to the DGA Algorithm

The **GBox** includes an engine capable of detecting domain names generated by the Domain Generation Algorithm (DGA).
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.

---

#### 2.1.5.2 Analyse

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).

---

#### 2.1.5.3 Displaying DGA alerts

The analysis is carried out on the `Quick analysis` page.
Depending on the result, a green or red icon indicates whether it is a DGA or not.

---

#### 2.1.5.4 Viewing the Gdgadetect status

Viewing the current state of the engine is shown in the *`Analysers` screen of the Web UI*.

---

#### 2.1.5.5 Gdgadetect update

The engine does not receive any updates.

---

#### 2.1.5.6 Configuring Gdgadetect

The engine is not configurable.

---

## 2.2 Archive management

### 2.2.1 Operation

The purpose of the analysis is to determine whether the archive contains malicious files.
The GBox extracts the archives submitted for analysis.
It works as follows:

- Submission of an archive, amount of archived files less than 50MB
- The user can provide the archive password via the graphical interface or the API. The password must be the same for all levels of the archive.
- The GBox tries to extract the archive using the password:
  - With protection against zip-bombs
  - With protection against malicious archives
  - If the extracted archive is larger than 50MB, extraction is stopped. An error message is sent back indicating that the file is too large: nothing will be analysed
  - If the archive is too deep in relation to the depth configured in the GBox, the analysis focuses on the files corresponding to the configured depth (maximum of 3 levels: zip by zip)
  - If the password does not match, an error message is displayed
  - If the archive contains too many files compared with what has been configured in the GBox (10 files max), an error message is sent back: nothing is analysed
- A "parent" analysis is created. It represents the archive file with its fingerprint and the analysis fingerprint. It points to the "child" analyses (parent report image below).
  - It has no analysis engine status, because nothing is analysed
  - It only has a global result
  - It does not display the contents of child errors
- A "child" analysis is created for each child file found in the archive. It is linked to the parent analysis (child analysis report image below)
- When all the "child" analyses are finished, the parent analysis is updated
  - Its score is equal a maximum of the "child" score
  - Its status is equal to the overall status of the "child".
  - If 1 or more "child" "in progress", then the parent analysis is "in progress".
  - If 1 or more "child" "in error", then "in error".
  - If all the "child" are "finished" with no errors, then "finished".
- There is no PDF or report containing all the children. You need to look at each child analysis to obtain the report.

### 2.2.2 Supported formats

| Type | Détails |
|---|---|
| 7zfile | extension = [".7z", ".iso", ".udf", ".xz"]<br>magic = ["7-zip archive", "ISO 9660", "UDF filesystem data", "XZ compressed data"] |
| gzipfile | extension = [".gzip", ".gz"]<br>magic = ["gzip compressed data, was"] |
| lzhfile | extension = [".lzh", ".lha"]<br>magic = ["LHa ("] |
| tarfile | extension = [".tar"]<br>magic = ["POSIX tar archive"] |
| tarbz2file | extension = [".tar.bz2"]<br>magic = ["LHa ("] |
| zipfile | extension = [".zip"]<br>magic = ["Zip archive data"] |

### 2.2.3 Archive password definition

The password for analysing an archive with a password is defined in *`New analysis` screen of the Web UI*.

## 2.3 Files that can be analysed by the GBox

### 2.3.1 Supported file types

- .jpg
- .bmp
- .mp3
- .avi
- .java
- .js
- .sql
- .html
- .css
- .class
- .c
- .bat
- .pdf
- .txt
- .csv
- .rules
- .xls
- .png
- .key
- .pem
- .wav
- .azw3
- .mp4
- .exe
- .pcap
- .xlsx
- .docx
- .pptx
- .odt (managed as an archive)
- .tar

### 2.3.2 Unsupported file types

- Bourne-Again
- POSIX shell script
- ELF
- Python

### 2.3.3 Size

The size of the file uploaded by the user must not exceed 50MB.

### 2.3.4 Rights

The user must be a member of the **Operators** group to be able to analyse the files.

## 2.4 Results and analysis reports

### 2.4.1 List of analysis reports

Analysis results are displayed in the form of a list, updated every 30 seconds, where each line corresponds to an analysis, including:

- The file's characteristics
- An overall analysis score
- The name of the threat
- The overall status of the analysis (Done or Error)

All this information, together with the graphical interface, can be found in *`Reports` screen of the Web UI*.
In addition, there is:

- A link to the report in pdf format
- A link to the report details

For the procedure for analysing a report, see the *Quick procedure for analysing a file*.

### 2.4.2 Report details

The analysis report includes all the information extracted from the file submitted to the various analysis engines. The report includes:

- A summary of the analysis indicating the threat score, the engines involved, the overall status - healthy, suspicious, or malicious
- As well as information about the analysis itself, including the template name, analysis identifier and date, and the file (name, hash).

There are three buttons:

- `SAMPLE` to download the file analysed
- `REPORT` to download the report in PDF format
- `RETRY` to repeat the analysis of this file with this or another template

All the information making up the report and the presentation of the graphical interface are described in *Detailed report* paragraph.

---

## 2.5 GBox Software Management

### 2.5.1 Overview of GUM: dedicated module for managing updates

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

- The installation of **Upgrades**: these are the **upgrades**, an operation to be carried out manually
- Installation of **Updates**: these are **updates of detection signatures and/or anti-virus engines**. | The installation process can be manual or scheduled. | **Updates** are only available for the Gmalcore and Gnest engines.
- The Hotfix section for installing **Hotfixes**: these are **manual fixes that modify the solution without the need for a full solution upgrade**.
- The Configuration part of GUM to setup package scheduling **Update**.
  For more information, see the *Configuring the GUM*.

Update management is described in the Release Notes. For more information, see the *Release note*.
The various updates available include:

| Type of update | To do what? | How | See for more information | See the procedure |
|---|---|---|---|---|
| Upgrade | Version upgrade | Manually | *Upgrade* | *Installing an upgrade* |
| Update | Updating detection signatures and/or anti-viral engines for Gmalcore and Gnest engines only | Manually | *Updates to detection signatures and/or anti-virus engines* | *Manual installation of a signature update* |
| | | Automatically | | *Configuring automatic updates via GUM* |
| Hotfix | Applying patches | Manually | *Applying a hotfix patch* | *Installing a hotfix patch* |

### 2.5.2 Upgrade

Upgrading the GBox is a version upgrade involving significant changes to the solution.
When applying a system update, it is necessary to restart the system manually at the end of the operation.
An upgrade increments the version number, for example 2.3.5.101 to 2.3.5.102.

**Note:**

Upgrades are carried out manually by the solution administrator; no automation is possible in the GUM menu.

**Note:**

Administrators must read the Releases Note before upgrading.

**Note:**

There are also upgrade packages that directly include the patches contained in the hotfixes.
This enables avoiding having to apply all the hotfixes after installing an appliance.

The graphical interface is described in the *`Admin- GUM - Upgrade` screen of the legacy Web UI*.
For instructions, see *Installing an upgrade*.

#### 2.5.2.1 For minor updates

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

- By applying only the HF1 patch
- By performing an upgrade

These two solutions are equivalent.

---

#### 2.5.2.2 In the case of a major update,

For example, to go from v2.3.5.101 to 2.3.5.102, only the upgrade is applicable.
For instructions, see *Installing an upgrade*.

---

#### 2.5.2.3 Upgrade path

The general rule regarding upgrade paths is to be on the latest patch before upgrading.
If this is not the case, this will be notified in the Release Note for the version concerned.

---

### 2.5.3 Updates to detection signatures and/or anti-virus engines

Signature updates or **updates** represent updates to the GBox detection engines.
There are 3 types of update packages:

- Gmalcore packages (*latest_malcore*): these packages only contain updates to the antivirus engines and databases used by Malcore.
- Sandbox packages (*latest_sandbox*): these packages contain updates to the signatures and modules used by the Gnest engine sandboxes.
- Complete packages (*latest_full*): these packages are a combination of the two previous packages.

These packages can be installed:

- Manually. In this case, the graphical interface to be used is described in the *`Admin- GUM - Updates` screen of the legacy Web UI*.
  For implementation, see the *Manual installation of a signature update* procedure
- Automatic. This schedule must be configured.
  This configuration is described in the *Configuring the GUM*.
  The graphical interface to be used is described in the *`Admin- GUM - Config` screen of the legacy Web UI*.
  To implement the schedule, see the procedure in *Configuring automatic updates via GUM*.

---

### 2.5.4 Applying a hotfix patch

Hotfix enables applying one or more patches without having to upgrade the entire solution.
This eliminates the need to reboot.
Applying a patch must be done in order, for example v102 -> v102-hf1 -> v102-hf2 -> ...

**Note:**

In most cases, patches will not require the web service to be restarted.

The graphical interface is described in the *`Admin- GUM - Hotfix` screen of the legacy Web UI*..
For implementation, see the *Installing a hotfix patch* procedure.

---

### 2.5.5 Configuring the GUM

Configuring GUM involves setting up the scheduling of update packages (**updates**).
The items to be configured include:

- Enabling this functionality
- The update mode
- Scheduling information such as day, time, and frequency
- The repository address for downloading packages
- Authenticating access to this repository

The graphical interface is described in the *`Admin- GUM - Config` screen of the legacy Web UI*).
For implementation, see the *Configuring automatic updates via GUM* procedure.

---

#### 2.5.5.1 Various methods of updates

The methods available are:

- Update **Online**: packages are downloaded directly from the Internet from GATEWATCHER sites
- Update **Local**: packages are downloaded from a local repository

---

#### 2.5.5.1.1 Online update

The **Online** update is performed automatically from the website https://update.gatewatcher.com/ and https://gupdate.gatewatcher.com.

---

#### 2.5.5.1.2 Local update.

To meet specific security constraints, the GBox is able to fetch its updates from a local repository previously configured to receive the packages.
This local repository is defined in the *`Admin- GUM - Config` screen of the legacy Web UI*.

---

### 2.5.6 Release note

Release notes (or *Release Note*) contain the list of changes made by the given release, the list of known issues, and also important notes related to the upgrade process.
Release notes are referenced in the following table.

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

---

## 2.6 Data use

In order for the AIONIQ solution to function properly, the GBox server works with log files.
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 then
- Downloading them for analysis by GATEWATCHER support.

The log export file can be protected by a password known only to the GATEWATCHER support team.
The graphical interface of the diagnostics function is described in *`Admin-GBox - Diagnostics` screen of the Web UI*.
For implementation, see the *Generating and loading files for diagnosis* procedure.

---

## 2.7 API

### 2.7.1 Presentation

The Application Programming Interface (API) is the set of endpoints, also known as resources or the end of a URL.
Each of these endpoints enables an action to be performed on the GBox, or information to be returned, without having to go through the GBox graphical interface.
This makes it easier to share and integrate GBox functions and data into existing architectures.

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

**Note:**

The list of endpoints is provided in the *Endpoint list* paragraph.

These endpoints can be executed:

- Via SWAGGER (*Use via the swagger graphical interface*):
  This enables endpoints to be used, its parameters to be understood, its execution to be tested, and its results to be analysed
- Via CURL (*Use via CURL*) :
  This enables a Curl request to be executed directly without going through the graphical interface.

---

### 2.7.2 Use via the swagger graphical interface

Each endpoint of the API:

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

All this information is visible in the swagger graphical interface. It is therefore the documentation for all our API endpoints.
The swagger GUI description is given in the *Overview of the API GBOX interface*.
To implement the swagger interface, see the procedure in the *Using an API endpoint*.

This interface enables:

- A list of existing endpoints by theme
- Details of any parameters for running an endpoint
- Information on the expected result, data template, and an example with default values
- Running queries
- Retrieving the Curl command equivalent to the request via the API

---

### 2.7.3 Use via CURL

It is possible to run an endpoint using a CURL command.
This command can be accessed via the swagger graphical interface, after selecting the endpoint, enter any parameters, and then run the endpoint.
The curl command is displayed in the `Responses` area.

**Note:**

Send a request to list the GBox engines (endpoint api/analysers):

```
curl -X GET "https://x.x.x.x/api/analysers/" -H  "accept: application/json" -H
↪"authorization: Basic dG90bzpTYW5kcmluZSwxMDA=" -H  "X-CSRFToken:␣
↪PsMZMavgOibfe5giFCImuOYYTWqvB2AdhR1y"
```

where x.x.x.x is the IP address of the Gbox.

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

---

### 2.7.4 Authentication and access to the GBox API

Access to the swagger graphical interface is via the GBox interface and then pressing the `API` button.
Authentication on the GBox enables access to the GBox API (for more information, see the *Title bar*).
The use of curl requests requires authentication to be carried out in the request.
This authentication is carried out using name/password pairs or tokens defined in the *`Admin-GBox - Accounts` screen of the Web UI*.

---

## 2.8 GApps management

The GApps represent the various services.
In some cases it may be necessary to restart them: refer to the procedure in *`Gapps` command*.

For the Malcore service, it is possible to force a restart or reinstallation.
For the Sandbox services provided by the Gnest engine, it is possible to manage the output network interface to the Internet.
For all these services, please refer to the procedure in *`Services` command*.

---

# Chapter 3

# Characteristics

## 3.1 Mechanical characteristics

| REFERENCE | DIMENSIONS (H x W x D) | RACKAGE | WEIGHT (KG) |
|---|---|---|---|
| GBOX | 42,8 x 482 x 705,05mm | 1 U | 21,9 |

## 3.2 Electrical characteristics

| REFERENCE | LOCAL STORAGE (SSD) | BACKUP STORAGE | EXTENSION STORAGE | POWER SUPPLY |
|---|---|---|---|---|
| GBOX | 2x 960GB RAID1 | 2x 4 TB RAID1 | Contact GATEWATCHER | 2 x 750W |

## 3.3 Functional characteristics

| REFERENCE | FUNCTION |
|---|---|
| GBOX | Analysis of close to 200,000 files per 24 hours |

# Chapter 4

# Presentation of accounts

## 4.1 List of accounts

There are two graphical user interfaces:

- The configuration menu (GUI)
- The web interface (Web UI)

For each of the two graphical interfaces, user accounts exist.

---

## 4.2 Presentation of the account setup from the configuration menu

### 4.2.1 Account from the configuration menu

The user to be used 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 the *`Password` command* section.

---

### 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 *Presentation of the configuration menu*.
The authorised functions are described in the *use case : setup account*.

---

## 4.3 Presentation of the web interface accounts and their management

The web interface enables access to:

- Creating analysis templates
- Analysing files
- Accessing and managing analysis reports
- Managing users and related groups
- History of authentications, account creations/deletions, and rights changes on the platform

---

### 4.3.1 Web interface accounts, groups, and rights

It is possible to create user accounts each having different rights.
These rights are defined by groups.
Each user can therefore belong to one or more groups, thus inheriting the rights of the group.

In the web interface, there are two types of group with differing rights:

- Operators
- Administrators

Generic accounts are defined with the following rights levels:

| Account... | Type of rights or group | Intended for a... |
|---|---|---|
| `operator` | Operators | analyst |
| `administrator` | Administrators | administrator |
| `admin` | Operators and Administrators | access to all the functions of the analyst and administrator |

---

### 4.3.2 Authorised functions for members of the Operators group

Members of the **Operators** group have access to the detection functions and the corresponding reports.
On the other hand, menus dedicated to equipment administration will not be accessible.

---

### 4.3.3 Authorised functions for members of the Administrators group

Members of the **Administrators** group have access to the equipment administration functions.
On the other hand, menus dedicated to equipment operations will not be accessible.

---

### 4.3.4 Functions allowed in the admin account

From the **admin** account, it is possible to access all the available functions.

---

### 4.3.5 Summary tables of the rights per group

#### 4.3.5.1 Access to icons

| Icon | Description | Members of the Operators group | Members of the Administrators group |
|---|---|---|---|
| theme change button | Changing the current theme<br>See the *Title bar* | access | access |
| API | Gatewatcher API interface<br>See the *Access to the Gatewatcher API* | limited access | access |
| current account button | Current account management<br>See the *Current account management, member of the Operators Group* | access, see the *Current account management, member of the Operators Group* | access, see the *Current account management, member of the Administrators Group* |

---

#### 4.3.5.2 Access to the General Menu commands

| Menu | Description | Operator | Administrator |
|---|---|---|---|
| logo GATEWATCHER<br>Home | `home` page, general view of the GCenter,<br>See *'Home' screen of the Web UI* | access | no access |
| `New analysis` | `New analysis` page<br>See *'New analysis' screen of the Web UI* | access | no access |
| `Reports` | `Reports` page<br>See *'Reports' screen of the Web UI* | access | no access |
| `Templates` | `Templates` page<br>See *'Admin/Templates' screen of the Web UI* | access | no access |
| `Analysers` | `Analysers` page<br>See *'Analysers' screen of the Web UI* | access | no access |
| Admin | Administration functions menu, see table below | no access | access |

#### 4.3.5.3 Access to the Admin Menu commands

| Sub Menu | Description | Operator | Administrator |
|---|---|---|---|
| GUM Config command | Enables configuring the automatic scheduling of updates<br>See *`Admin- GUM - Config` screen of the legacy Web UI* | no access | access |
| GUM Updates command | Enables applying an update to the GBox detection engines<br>See *`Admin- GUM - Updates` screen of the legacy Web UI* | no access | access |
| GUM Hotfix command | Enables applying an hotfix<br>See *`Admin- GUM - Hotfix` screen of the legacy Web UI* | no access | access |
| GUM Upgrade command | Enables applying an upgrade<br>See *`Admin- GUM - Upgrade` screen of the legacy Web UI* | no access | access |
| GBox Diagnostics command | Enables log files to be exported and downloaded<br>See *`Admin-GBox - Diagnostics` screen of the Web UI* | no access | access |
| GBox Accounts command | Enables managing accounts<br>See *`Admin-GBox - Accounts` screen of the Web UI* | no access | access |
| GBox Users management command | Enables Users management<br>See *`Admin-GBox- Users management` screen of the Web UI* | no access | access |
| GBox Configuration command | Enables the GBox configuration<br>See *`Admin-GBOX- Configuration` screen of the Web UI* | 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 but may also manage other accounts depending on the rights granted by its group.
Details are provided in the table below:

| User | can change the password | | |
|---|---|---|---|
| | Operators group | Administrators group | admin |
| operator account | only its own account | No | No |
| group member Administrators | X | X | X |
| admin account type | X | X | X |

---

##### 4.3.6.2.1 Changing one's own password

The graphical interface is described in *Title bar*.
For an Operators group password, see the procedure in *Changing the current account password*.
For an Administrators group password, see the procedure in *Changing the current account password* .

---

##### 4.3.6.2.2 Administrator management of passwords for other accounts

The graphical interface is described in *`Admin-GBox - Accounts` screen of the Web UI*.
For implementation, see the *Resetting a user's password* procedure.

---

#### 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.

| Setting | Default value |
|---|---|
| At least one upper case letter | enabled |
| At least one digit (0 to 9) | enabled |
| Minimum password length | 8 characters |
| At least one lower case letter | enabled |
| At least one symbol (i.e. neither a number nor a letter) | enabled |

---

### 4.3.7 Creating local users

In addition to generic accounts, it is possible to create user accounts each having different rights.
The graphical interface enabling the creation of users is done in the *`Admin-GBox- Users management` screen of the Web UI*.
For implementation, see:

- The *Creating local users*
- The *Changing some of a local user's information*
- The *Deleting a user*

---

### 4.3.8 Audit trail principle

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

---

#### 4.3.8.1 Authentication history function

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

---

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

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

---

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

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

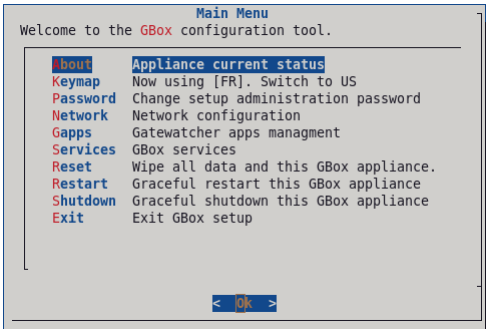
---

# Chapter 5

# Presentation of graphical interfaces

## 5.1 Presentation of the configuration menu

The configuration menu is displayed.




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

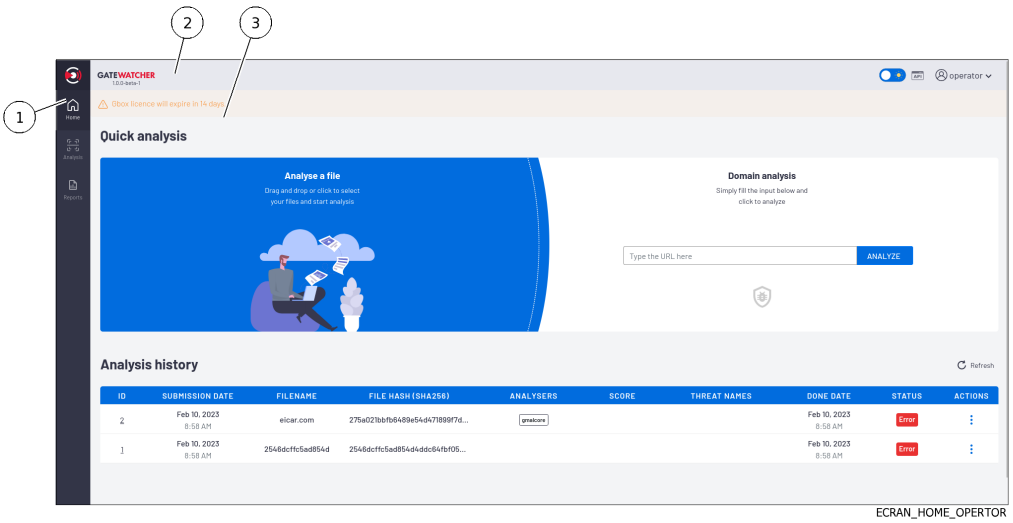
| Choice | Shortcut key | Explanation | See |
|---|---|---|---|
| About | A | General information about the GBox - name, version, IP address... | The *`About` command* |
| Keyboard | K | Enables changing the keyboard language to US or FR | The *`Keymap` command* |
| Password | P | Enables changing the password for the **setup** account | The *`Password` command* |
| Network | N | Enables viewing and/or modifying the network configuration | The *`Network` command* |
| Gapps | G | Enables rebooting of GBox applications | The *`Gapps` command* |
| Services | S | Enables certain services to be restarted or reset to default. | The *`Services` command* |
| Reset | R | Enables the data to be deleted and the GBox to be reset to its "factory settings". | The *`Reset` command* |
| Restart | R | Enables a clean reboot of the GBox | The *`Restart` command* |
| Shutdown | S | Enables switching off the GBox | The *`Shutdown` command* |
| Exit | E | Enables closing the configuration menu | The *`Exit` command* |

## 5.2 Operators level graphical interface via web browser

### 5.2.1 Overview of the Web UI graphical interface at the Operators level

**Important:**

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




ECRAN_HOME_OPERTOR

The screen consists of three parts:

| Marker | Name | Description |
|---|---|---|
| 1 | The *Navigation bar* | Displays the icons used for accessing the main functions |
| 2 | The *Title bar* | Gives direct access to certain functions such as search, visual theme, and others. |
| 3 | The *Central screen* | Displays the screen selected by clicking on the icon in the navigation bar |

#### 5.2.1.1 Navigation bar

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

ICONE_H

| Marker | Button name | Display |
|---|---|---|
| 1 | GATEWATCHER Logo | The *`Home` screen of the Web UI* : corresponds to the main dashboard<br>This page enables quick analysis and provides an historical overview of the reports produced. |
| 2 | `Home` | |
| 3 | `Analysis` | The *`New analysis` screen of the Web UI* : the `New Analysis` page enables :<br>• quickly configuring an analysis (selecting the model, entering the password, and activating a forcing)<br>• perform the analysis and view the report |
| 4 | `Reports` | The *`Reports` screen of the Web UI* : indicates the list of reports produced |

#### 5.2.1.2 Title bar

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

BARRE_TITRE_OPERATOR

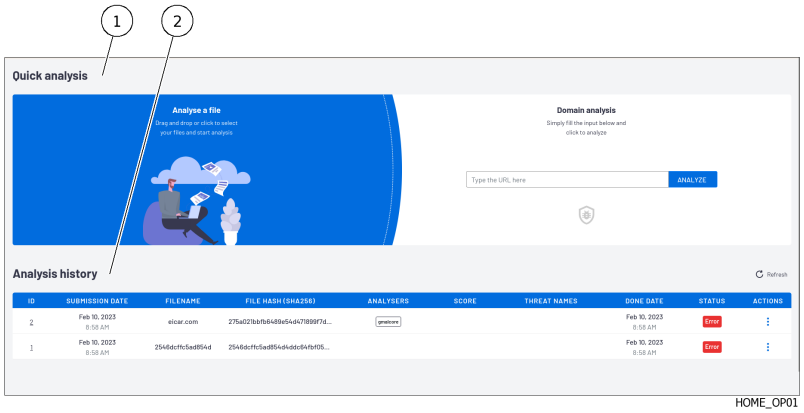
| Marker | Name | Description |
|---|---|---|
| 1 | GATEWATCHER Logo | If pressed then returns to the `Home` screen |
| 2 | Theme change button | Enables switching between the two light and dark themes |
| 3 | API Button | Switches to the GATEWATCHER API UI |
| 4 | Current account button | Manages the current account |

#### 5.2.1.3 Central screen

The central screen displays the information selected by a button on the navigation bar.
By default, the `Home` screen is displayed : refer to the *`Home` screen of the Web UI*.

### 5.2.2 `Home` screen of the Web UI

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



HOME_OP01

| Marker | Name |
|---|---|
| 1 | *`Quick analysis` zone* |
| 2 | *`Analysis history` zone* |

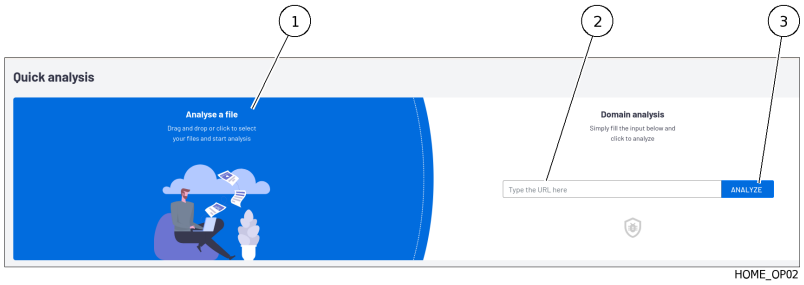
#### 5.2.2.1 `Quick analysis` zone

This area enables users to quickly:

- Or upload one or more files from the user's computer to the GBox using the `Analysis a file` zone and run an analysis, the results of which are shown in a report.

  This analysis will be carried out using the default model defined by an Administrator group member.

  If the files are compressed and have a password, then you need to use the *`New analysis` screen of the Web UI*.
- Or analyse a domain using the `Domain analysis` zone.



HOME_OP02

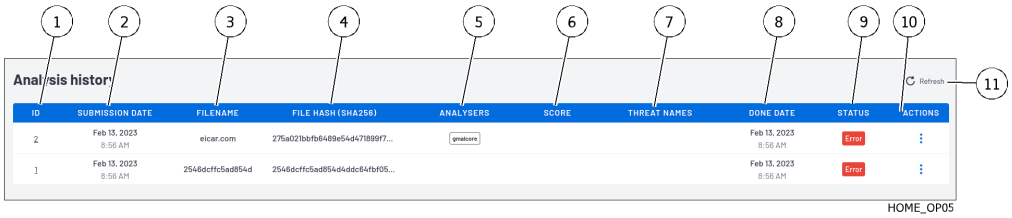
| Marker | Name |
|---|---|
| 1 | Area for dropping a file for analysis |
| 2 | Entry field for the URL of the domain to be analysed |
| 3 | Run domain analysis button |

To analyse a file, see the *Quick procedure for analysing a file*.
To analyse a domain, see the *Quick procedure for analysing a domain*.

---

#### 5.2.2.2 `Analysis history` zone

This zone enables viewing the history of the analyses performed.



HOME_OP05

Analyses are sorted according to:

- Date in the `DONE DATE` field
- If there is no information in this field
  - From the `STATUS` field: first the `New` status, then the `In progress` status, then the `Done'', or ```Error` status.

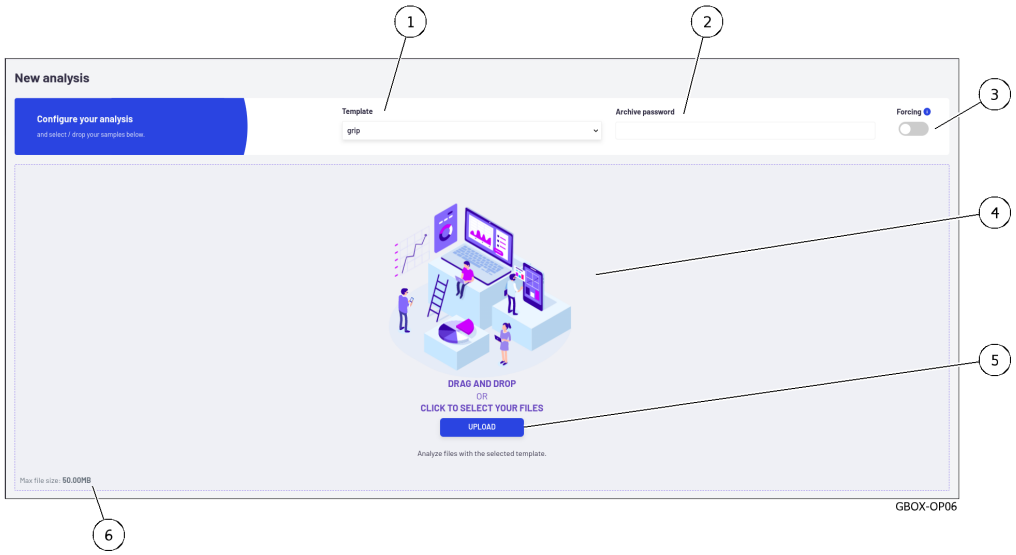
Each line represents a separate analysis. The information for each analysis is presented and detailed in the table below.

| Marker | Name | Description |
|---|---|---|
| 1 | `ID` | Analysis number.<br>The listed reports are sorted from the most recent to the earliest.<br>Clicking on this field opens the `Analysis report` page for this report |
| 2 | `SUBMISSION DATE` | Time and date of the analysis submission |
| 3 | `FILENAME` | Name of the analysed file<br>Clicking on this field copies the name to the clipboard |
| 4 | `FILE HASH (SHA256)` | SHA256 of the file<br>Clicking on this field copies the hash to the clipboard |
| 5 | `ANALYSERS` | Indicates the name of the engines used for the analysis |
| 6 | `SCORE` | Global threat analysis score calculated from the analysis score reported by the various engines |
| 7 | `THREAT NAMES` | Name of the threat reported by the gmalcore module (or n/a) \| Clicking on this field copies the hash to the clipboard |
| 8 | `DONE DATE` | End date and time of the analysis |
| 9 | `STATUS` | Overall status of the analysis, either Done, In Progress, In queue, or Error<br>In the event of an error, further information is available in the analysis report |
| 10 | `ACTIONS` | Possible actions: download the report in pdf format |

Button (11) enables refreshing the screen.
For instructions, see the *Procedure to analyse the contents of a report*.

### 5.2.3 `New analysis` screen of the Web UI

After pressing the `Analysis` button on the navigation bar, the `New analysis` screen is displayed.
It includes the following items:




| Marker | Name | Description |
|---|---|---|
| 1 | `Template` | Selecting the model to be used for analysis |
| 2 | `Archive password` | Password entry field for compressed files |
| 3 | `Forcing` | Selector for forcing a new analysis and ignoring existing results |
| 4 | `DRAG AND DROP` | Zone for dropping in a file to be analysed / report zone for analysed files |
| 5 | `UPLOAD` | Button to open a window to load files for analysis |
| 6 | `Max file size` | Notice stating that the file size is limited to 50MB |

This area enables:

- Upload a file from the user's computer to the GBox, either by dragging and dropping or by selecting it in a window, then
- Analysing this file and displaying the results in a report.

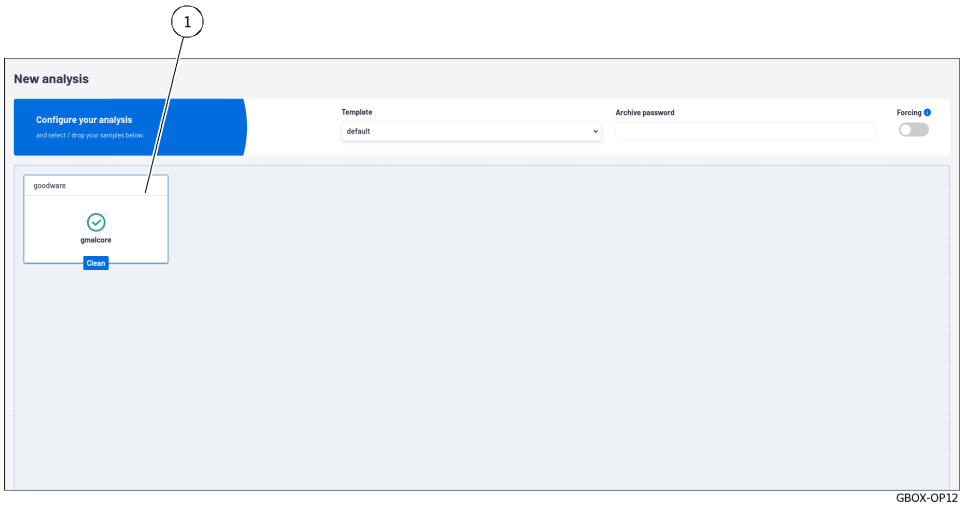
The characteristics of the files to be analysed are described in the *Files that can be analysed by the GBox* section.
The characteristics of the compressed files to be analysed are described in the *Archive management* section.
For instructions, see the *Procedure for analysing a file in the `New analysis` screen*.

**Note:**

Selecting a file and choosing a template is compulsory.
Using the `Forcing` function is optional.
The size of the file to be analysed must not exceed 50MB.
The user must hold **Operator** rights to be able to analyse the files.

#### 5.2.3.1 Report display area

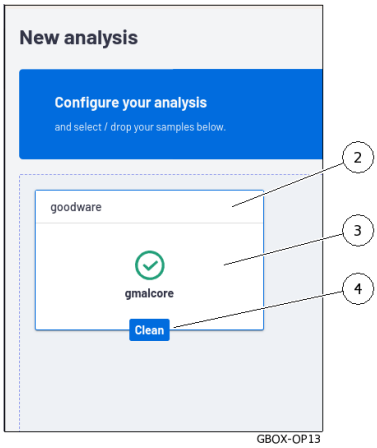
Once an analysis is complete, the area (4) of the `New analysis` window displays as many reduced reports (1) as files analysed.



GBOX-OP12

---

##### 5.2.3.1.1 Reduced report



GBOX-OP13

The reduced report (1) displays:

- The name of the analysed file (2)
- The result of the analysis (tick = ok) and the name of the engine used (here the Gmalcore engine), marker (3)
- The status of the result (4), in this example `clean`.

---

#### 5.2.3.1.2 Full report

Click on the reduced report:

- Opens the detailed version
- removes the reduced report from the window
- saves the report in the report window

For more information on reports, please refer to *`Reports` screen of the Web UI*.

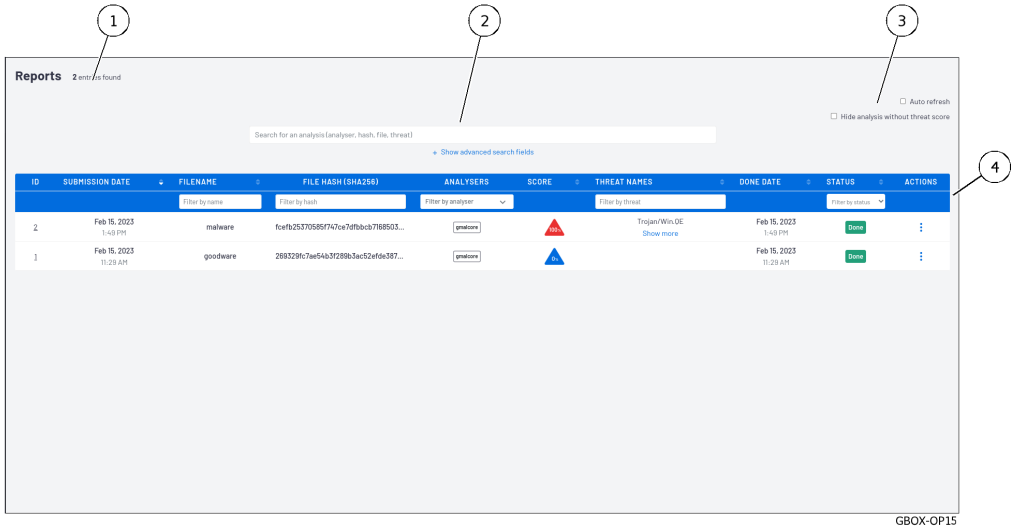
---

## 5.2.4 `Reports` screen of the Web UI

### 5.2.4.1 Overview of the `Reports` screen

After pressing the `Reports` button on the navigation bar, the `Reports` screen is displayed.
This screen enables:

- Viewing reports in order to analyse the results
- Filter them
- Export reports in pdf format
- Download the analysed file



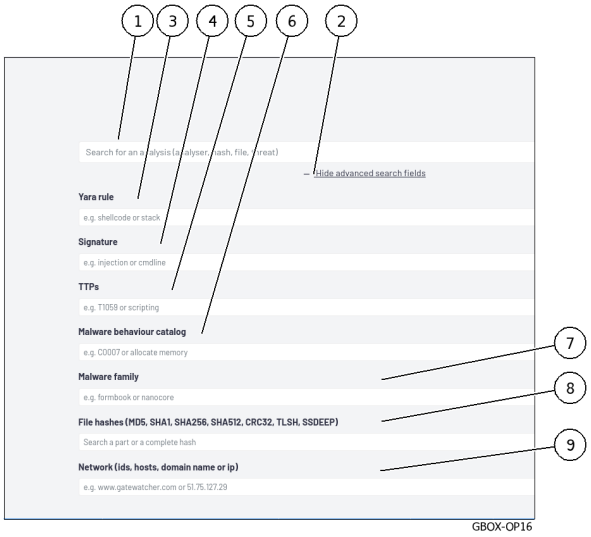

It includes the following main items:

| Marker | Name |
|---|---|
| 1 | Number of reports in the log (here 2) |
| 2 | Area enabling searches in reports |
| 3 | Configuration zone |
| 4 | Detailed reports area |

---

#### 5.2.4.2 Zone enabling searches

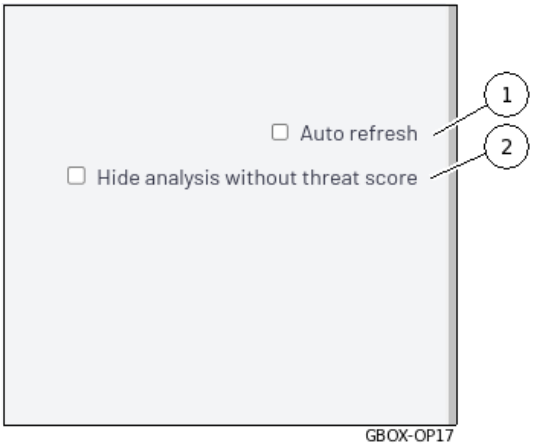
This zone enables reports to be filtered using the following criteria.




| Marker | Field | Description |
|---|---|---|
| 1 | `Search for an analysis` | Filters reports according to the entered input. The filter is applied to the `FILENAME`, `FILE HASH (SHA256)`, `THREAT NAMES` fields. |
| 2 | `Hide advanced search fields` | Show / hide advanced search fields |
| 3 | `Yara rule` | Yara rule (for example shellcode or stack) |
| 4 | `Signature` | Signature (injection or cmdline, for example) |
| 5 | `TTPs` | Tactics, Technique, Procedure (e.g. T1059 or script) |
| 6 | `Malware behaviour catalog` | Catalogue of malicious behaviour (e.g. C0007 or memory allocation) |
| 7 | `Malware family` | Malware family (e.g. formware or nanocore) |
| 8 | `File Hashes` | All or part of the file hash (MD5, SHA1, SHA256, SHA512, CRC32, TLSH, SSDEEP) |
| 9 | `Network` | Network settings (ids, hosts, domain name or ip) |

#### 5.2.4.3 Configuration zone

This zone enables configuring the report postings.



| Marker | Name | Description |
|---|---|---|
| 1 | `Auto refresh` | Automatic renewal |
| 2 | `Hide analysis without threat score` | Conceals the analysis if there is no threat score |

**Note:**

If the GBox directly receives the files without going through a GCenter, then the analysed files receiving a score of zero can be considered as healthy for the engine used.

If the GBox receives the files from a GCenter, then the files analysed are deemed suspicious.

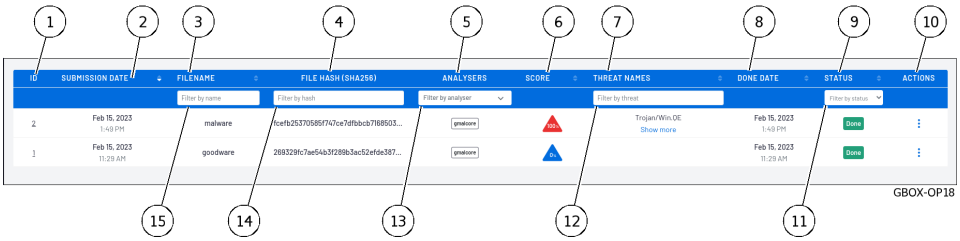
Just because they have a score of zero is not enough to be considered healthy. An analyst must examine the reports and take into account the engines used (and not used!) during the analysis

---

#### 5.2.4.4 Reports area

This area enables details of the analyses performed to be displayed.

Each line represents a separate analysis. The information for each analysis is presented and detailed in the table below.




**Note:**

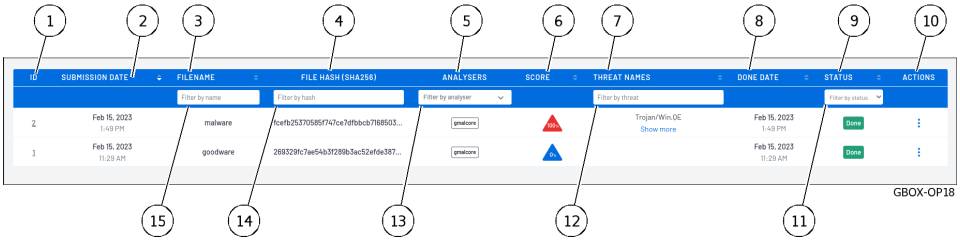
The information listed in the table below are the same fields as in the reports on the `Home` screen.

| Marker | Name | Description |
|---|---|---|
| 1 | `ID` | Analysis number.<br>The listed reports are sorted from the most recent to the earliest.<br>Clicking on this field opens the `Analysis report` page for this report |
| 2 | `SUBMISSION DATE` | Time and date of the analysis submission |
| 3 | `FILENAME` | Name of the analysed file<br>Clicking on this field copies the name to the clipboard |
| 4 | `FILE HASH (SHA256)` | SHA256 of the file<br>Clicking on this field copies the hash to the clipboard |
| 5 | `ANALYSERS` | Indicates the name of the engines used for the analysis |
| 6 | `SCORE` | Global threat analysis score calculated from the analysis score reported by the various engines |
| 7 | `THREAT NAMES` | Name of the threat reported by the gmalcore module (or n/a) \| Clicking on this field copies the hash to the clipboard |
| 8 | `DONE DATE` | End date and time of the analysis |
| 9 | `STATUS` | Overall status of the analysis, either Done, In Progress, In queue, or Error<br>In the event of an error, further information is available in the analysis report |
| 10 | `ACTIONS` | Possible actions: download the report in pdf format |

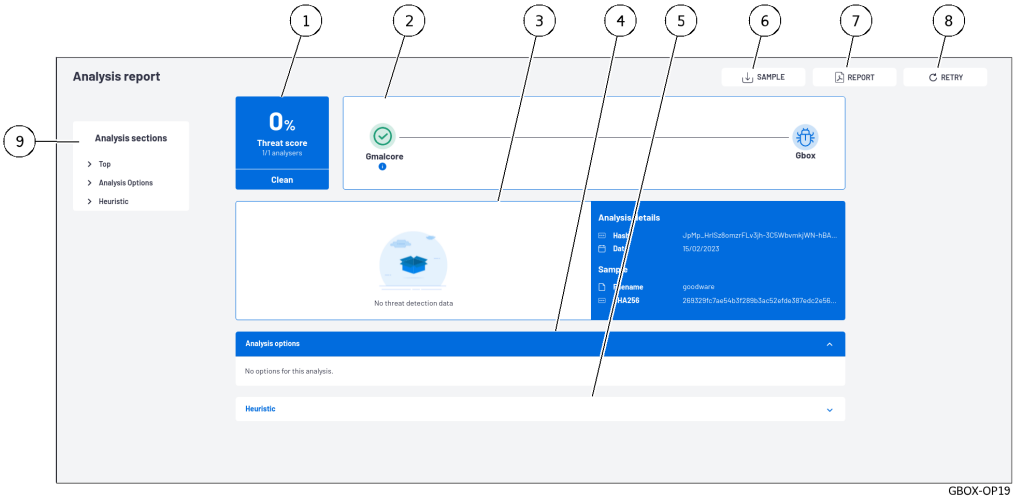
The fields below are additional fields enabling report filtering.

| Marker | Name | Description |
|---|---|---|
| 11 | `Filter by status` | Enables filtering of reports with this status to be selected from the list |
| 12 | `Filter by threat` | Enables filtering of reports with this threat name to be entered |
| 13 | `Filter by analyser` | Enables filtering of reports with an engine name to be selected from the list |
| 14 | `Filter by hash` | Enables filtering of reports with this hash to be entered |
| 15 | `Filter by name` | Enables reports to be filtered by the file name to be entered |

#### 5.2.4.5 Detailed report




After pressing the ID (1) of a report, the detailed report is displayed.




Depending on the engines selected in the model during the analysis, certain information may be displayed. These are indicated on a case-by-case basis.

In the example above, the report was run on a model in which only the Gmalcore engine was active.

The analysis report includes all the information extracted from the file submitted to the various analysis engines.

---

##### 5.2.4.5.1 Information included in this report

The information contained in this report is:

| Marker | Description |
|---|---|
| 1 | Summary of the analysis results:<br>• The result (Threat Score) of the global analysis calculated from the analysis score provided by the various Gmalcore engines<br>- 0% for a file found to be sound by the engine used<br>- to 100% max value for a file reported as malicious<br>• The number of engines involved (here 1/1 analysers)<br>• overall status (healthy, suspicious, or malicious): here Clean or healthy<br>A score is only provided for the Gmalcore and Goasm engines |

suite sur la page suivante

Table 1 – suite de la page précédente

| Marker | Description |
|---|---|
| 2 | Summary of the analysis stages:<br>• The list of engines used: here Gmalcore<br>• The results of loading the file for each of the engines: here for Gmalcore, the tick indicates that loading was successful<br>• on the right, the result of the analysis: here the icon indicates OK |
| 3 | Information includes:<br>• A chart (see note below)<br>• The analysis (hash and date)<br>• The file (name, sha256) |
| 4 and 5 | Optional analysis sections. This information depends on the engine in the template.<br>In this example, only the `` `Analysis options` `` and `` `Heuristic` `` sections are displayed.<br>This section can be folded/unfolded |
| | Information on heuristic analysis (5): this section can be folded / unfolded<br>This section shows the results for each of the engines: here the 16 engines of the Gmalcore engine |
| 6 | This `` `SAMPLE` `` button enables you to download the analysed file.<br>he downloaded file is compressed and protected by a password (the password is **infected**).<br>Once decompressed, the file analysed will have a .sample extension. |
| 7 | The `` `REPORT` `` button enables downloading the report in pdf format. |
| 8 | The `` `RETRY` `` button enables re-running the analysis of this file with this or another template. |
| 9 | The `` `Analysis sections` `` include shortcuts for opening these sections and refocusing the display.<br>These sections provide details of the analyses from the engines defined in the analysis model.<br>This information enables an analyst to obtain a more precise idea of the anatomy and behaviour of the file when it is opened and executed.<br>In this example, only the `` `Top` ``, `` `Analysis options` `` and `` `Heuristic` `` sections are displayed.<br>Depending on the combination of engines employed, some sections may be omitted from this list: details are provided in the table below. |
| | The `` `ALL ARTEFACTS` `` button enables downloading of artefacts resulting from the analysis, such as memory dump, network capture (pcap), character strings detected.<br>This section also enables the removal of artefacts.<br>This button is only available if the Gnest engine is active. |

#### 5.2.4.5.2 List of sections included in the `Analysis sections`

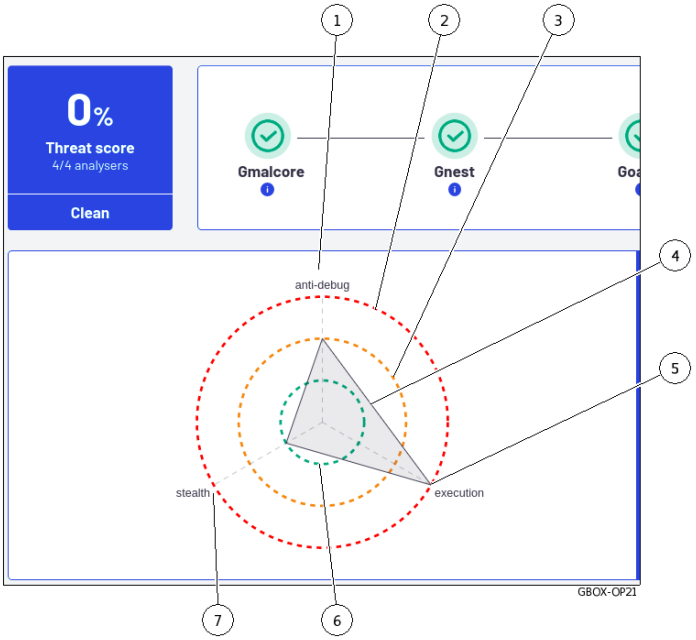
Table2: List of sections included in the `Analysis sections`

| Section title | Description | Is activated by the engine |
|---|---|---|
| `Top` | Shortcut to the top section of the report, i.e. sections (1) to (3). | All engines |
| `Analysis options` | Option values used for analysis | Grip and Gnest |
| `Iocs` | List of actions performed, including files, registry, network, processes, and so on. | GNEST |
| `Ttps` | TTPs analyse how a malicious actor operates. They describe the way cyber attackers orchestrate, execute, and manage operational attacks.<br>TTPs contextualise a threat. They reveal the steps or actions taken by malicious actors when exfiltrating data, for example. | GNEST |
| `Static` | Metadata | GRIP |
| `Overview` | Information about the file, including size, various hashes, type, etc. | GNEST |
| `Heuristic` | List of engines (Entry#x) and name of the threat reported by the Gmalcore module (or n/a) | Gmalcore |
| `Shellcode` | Shellcode detection result | GOASM |
| `Signatures` | List of yara signatures corresponding to the analysed file | Gnest |
| `Process Tree` | Graphical representation of the process tree | Gnest |

#### 5.2.4.5.3 Chart details

**Note:**

The chart is only available if Gnest is part of the model. The data required for the chart is generated by this engine.



This graph enables viewing the dangerousness of the file analysed:

- The category of seriousness is defined by the axes (1) (5) and (7): titles and number of axes are provided by the engines
- The degree of danger is indicated by the concentric circles.
- The central circle (6) indicates the *healthy* level
- The middle circle (3) indicates the *suspicious* level
- The outer circle (2) indicates the *malicious* level

The summary for the file is read from the vertices of the shape shown (4).
In the example shown, the vertex (5) indicates that the file is:

- malicious on the `execution` axis (5)
- suspicious in the `antidebug` axis (1)
- healthy on the `stealth` axis (7)

For an analysis of a report, see the *Procedure to analyse the contents of a report*.

---

### 5.2.5 Current account management, member of the Operators Group

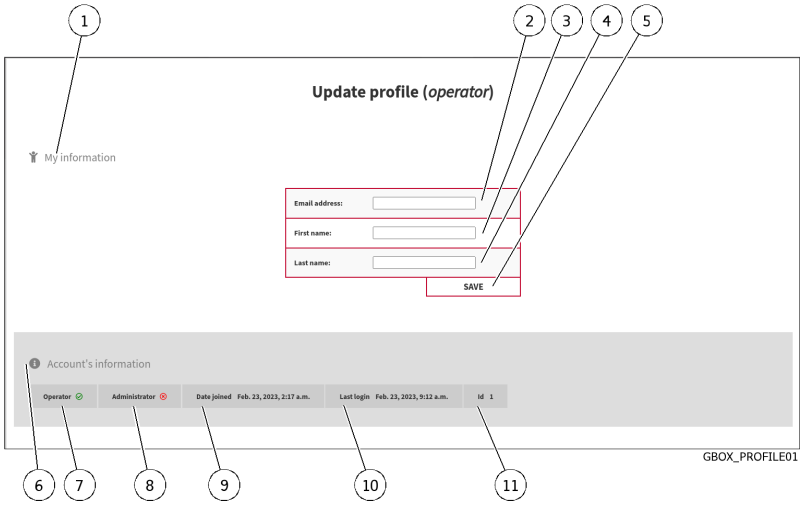

After pressing the current account management button (4), three commands are available:

- The `Edit profile` command: see the *`Update profile` screen*
- The `Change password` command: see the *`Change Password` screen*
- The `Logout` command: see the *Logout command*

---

#### 5.2.5.1 `Update profile` screen

After clicking on the `Edit profile` command, the `Update profile` screen is displayed:



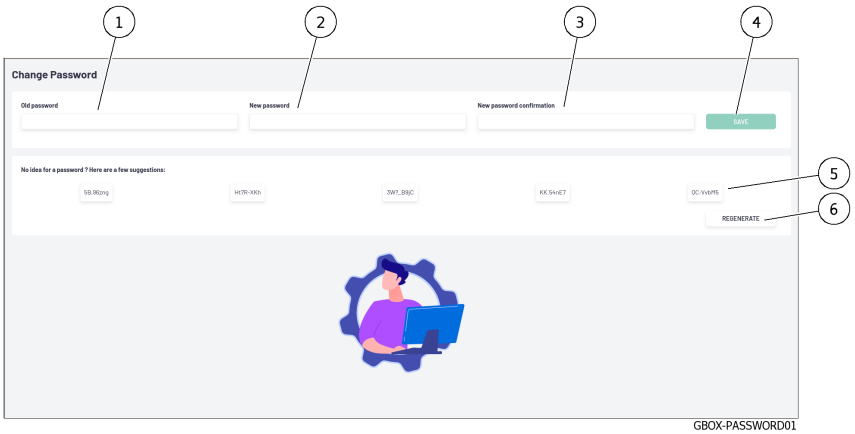
| Marker | Name | Description |
|---|---|---|
| 1 | `My information` | Area listing current account details |
| 2 | `Email address` | Current user's email address |
| 3 | `First name` | Current user's first name |
| 4 | `Last name` | Current user's Last name |
| 5 | `SAVE` | Button for saving entries. |
| 6 | `Account's information` | Area listing current account management information |
| 7 | `Operator` | Membership in the Operator group - a tick indicates membership, a cross indicates non-membership |
| 8 | `Administrator` | Membership in the Administrator group - a tick indicates membership, a cross indicates non-membership |
| 9 | `Date joined` | Date and time the current account was created |
| 10 | `Last login` | Date and time of last current account login |
| 11 | `ID` | Account identification number |

For implementation, see the *Changing some of the current user's information* procedure.

---

#### 5.2.5.2 `Change Password` screen

After clicking on the `Change password` command, the `Change Password` screen is displayed:




This screen enables changing the password for the current account.
This password policy is described in paragraph *Password management policy*.

| Marker | Name | Description |
|---|---|---|
| 1 | `Old password` | Old password entry box |
| 2 | `New password` | New password input box |
| 3 | `New password confirmation` | New password confirmation input box |
| 4 | `SAVE` | Button for saving entries. |
| 5 | `No idea for a password ?` `Here are a few suggestions` | Five passwords to choose from |
| 6 | `REGENERATE` | Button for regenerating new passwords |

For implementation, see the *Changing the current account password* procedure.

#### 5.2.5.3 Logout command

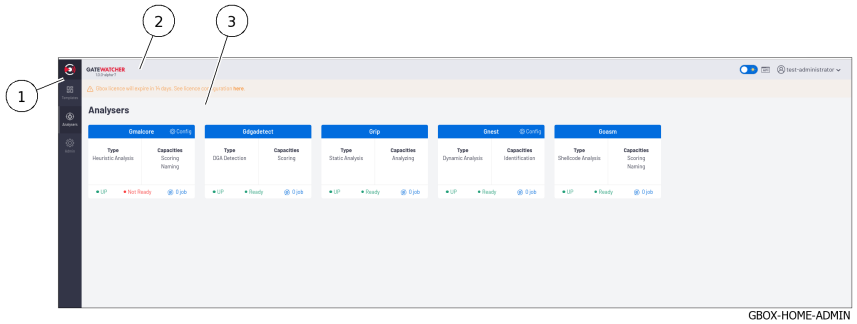
After clicking on the `Logout` command, the current user is immediately logged out.
The login screen is displayed.
For implementation, see the *Logging out of the GBox web interface* procedure.

## 5.3 Administrators level graphical interface via web browser

### 5.3.1 Overview of the Web UI graphical interface at the Administrators level

**Important:**

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




GBOX-HOME-ADMIN

The screen consists of three parts:

| Marker | Name | Description |
|---|---|---|
| 1 | The *Navigation bar* | Displays the icons used to access the main functions |
| 2 | The *Title bar* | Gives direct access to certain functions such as search, visual theme, and others. |
| 3 | The *Central screen* | Displays the screen selected by clicking on the icon in the navigation bar |

#### 5.3.1.1 Navigation bar

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


| Marker | Button name | Display |
|---|---|---|
| 1 | GATEWATCHER logo | The *`Analysers` screen of the Web UI* |
| 2 | `` `Template` `` | The *`Admin/Templates` screen of the Web UI* |
| 3 | `` `Analysers` `` | The *`Analysers` screen of the Web UI* :<br>• to quickly analyse a file<br>• to view the analysis history |
| 4 | `` `Admin` `` | See the *Admin Menu* |

#### 5.3.1.2 Title bar

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


| Marker | Name | Description |
|---|---|---|
| 1 | GATEWATCHER Logo | If pressed, it returns to the `` `Home` `` screen. |
| 2 | Theme change button | Enables switching between the two light and dark themes |
| 3 | API button | Switches to the GATEWATCHER API UI. |
| 4 | Current account button | Manages the current account |

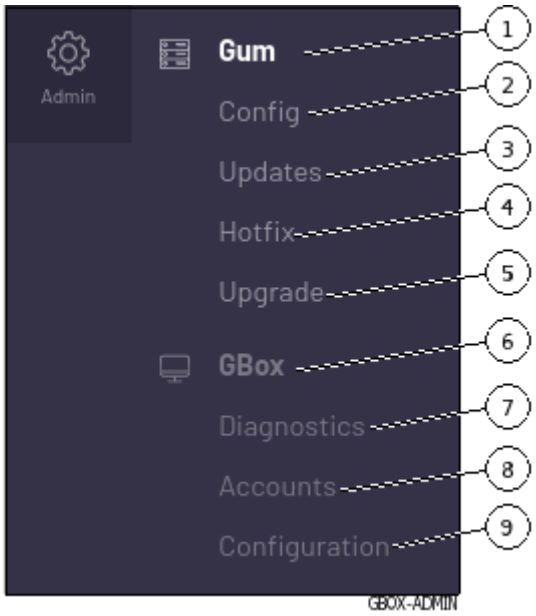
#### 5.3.1.3 Central screen

The central screen displays the information selected by a button on the navigation bar.
By default, the `Home` screen is displayed: refer to the *`Analysers` screen of the Web UI*.

---

#### 5.3.1.4 Admin Menu

The menu consists of the following items:




| Marker | Menu name | Command name Display | |
|---|---|---|---|
| 1 | `GUM` menu | includes the following commands: | |
| 2 | | • `Config` | *`Admin- GUM - Config` screen of the legacy Web UI* |
| 3 | | • `Updates` | *`Admin- GUM - Updates` screen of the legacy Web UI* |
| 4 | | • `Hotfix` | *`Admin- GUM - Hotfix` screen of the legacy Web UI* |
| 5 | `Gbox` menu | includes the following commands: | |
| 6 | | • `Diagnostics` | *`Admin-GBox - Diagnostics` screen of the Web UI* |
| 7 | | • `Accounts` | *`Admin-GBox - Accounts` screen of the Web UI* |
| 8 | | • `Configuration` | *`Admin-GBox- Users management` screen of the Web UI* |

---

### 5.3.2 Overview of the traditional Web graphical interface (legacy Web UI)

#### 5.3.2.1 Presentation of the interface

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 web:

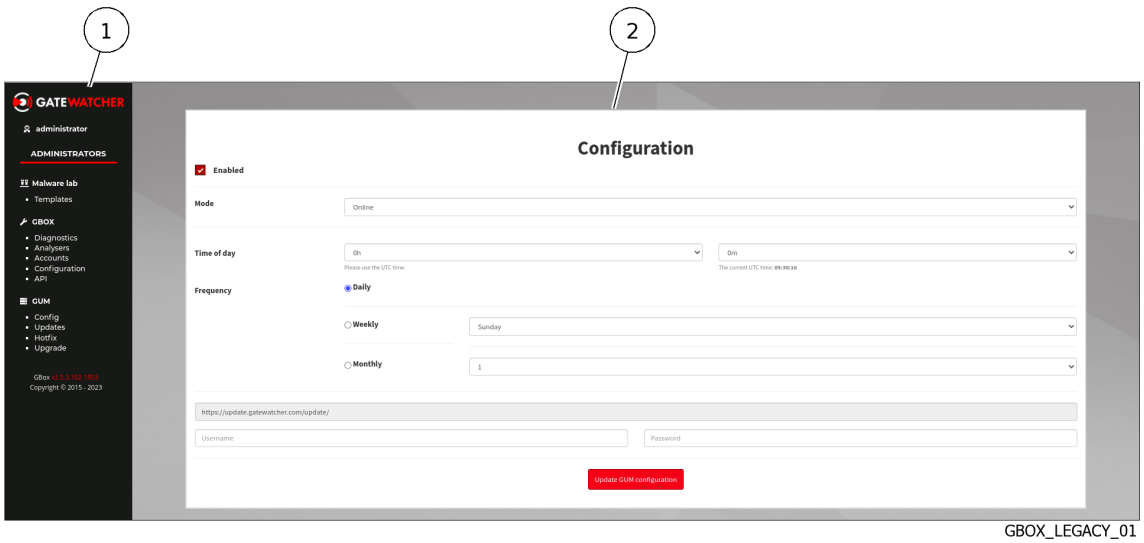
- if the account being used belongs to the **Operators** group, then the interface displayed is the main Web UI interface: the user does not have access to the traditional interface.
- If the account being used is part of the **Administrators** group, then the interface displayed is the main Web UI interface.
  The traditional interface (legacy Web UI) is used for specific functions.

**Note:**

Each interface features the same commands in the menu, enabling the user to run any command regardless of which interface is active.

| Administrator menu command | Web interface UI | legacy Web interface UI |
|---|---|---|
| Templates | Enabled | |
| Analysers | Enabled | |
| Admin | depends on the command<br>is described in more detail below | |

#### 5.3.2.2 Description of the traditional interface



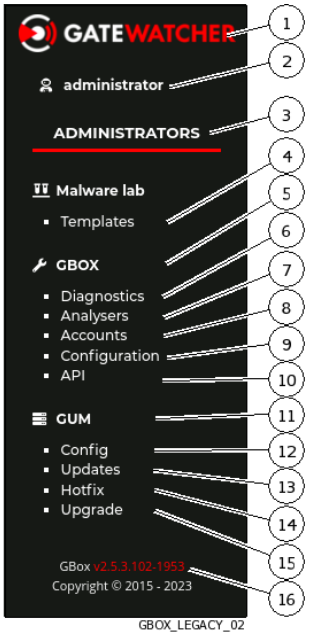
GBOX_LEGACY_01

The screen consists of two parts:

| Marker | Name | Description |
|---|---|---|
| 1 | *Traditional interface navigation bar* | Displays the menus and commands for accessing the main functions |
| 2 | *Central screen of the traditional interface* | Displays the screen selected by pressing on a command on the navigation bar.<br>Each screen is named after the corresponding command: example `Diagnostics` screen |

#### 5.3.2.2.1 Traditional interface navigation bar

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



GBOX_LEGACY_02

| Item | Name | Display |
|---|---|---|
| 1 | GATEWATCHER Logo | Using the button enables returning to:<br>• The `Quick analysis` screen for accounts holding Operators rights<br>• The `Analysers` screen for accounts holding Administrators rights |
| 2 | Current user | Indicates the name of the current user.<br>Using the button displays the commands `Edit profile`, `Change password` and `logout` to disconnect. |
| 3 | `ADMINISTRATORS` | This section enables full access to all the administration menus.<br>This section includes the following items: |
| 4 | | The `Template` command enables access to the template management menu (*`Admin/Templates` screen of the Web UI*) |
| 5 | | The `GBox` menu enables users to manage the GBox. It consists of: |

suite sur la page suivante

Table 3 – suite de la page précédente

| Item | Name | Display | |
|---|---|---|---|
| 6 | | | • the `Diagnostics` command enables generating and exporting the GCenter's system logs for further analysis by the GATEWATCHER support team (*`Admin-GBox - Diagnostics` screen of the Web UI*) |
| 7 | | | • the `Analysers` command enables users to access analysis engine management (*`Admin-GBox - Diagnostics` screen of the Web UI*) |
| 8 | | | • the `Accounts` command enables the GBox authentication to be managed using local authentication (*`Admin-GBox - Accounts` screen of the Web UI*) |
| 9 | | | • the `uration` command enables managing the GBox's global configuration (proxy, certificate, licence, etc.) (*`Admin-GBox- Users management` screen of the Web UI*) |
| 10 | | | • the `API` command enables accessing the Swagger page of the GBox API (*Access to the Gatewatcher API*) |
| 11 | | The `GUM` menu enables configuring the software update system. This includes the following commands: | |
| 12 | | | • the `Config` command enables automating updates to the engines (*`Admin- GUM - Config` screen of the legacy Web UI*) |
| 13 | | | • the `Updates` command enables updating the solution via an update (*`Admin- GUM - Updates` screen of the legacy Web UI*) |
| 14 | | | • the `Hotfix` command enables applying a patch (*`Admin-GUM - Hotfix` screen of the legacy Web UI*) |
| 15 | | | • the `Upgrade` command enables the solution to be upgraded (*`Admin- GUM - Upgrade` screen of the legacy Web UI*) |
| 16 | | GBox v2.5.3.102-1953. The GBox version is displayed in this field (here v2.5.3.102-1953). | |

#### 5.3.2.3 Central screen of the traditional interface

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

---

### 5.3.3 Access to the Gatewatcher API

The API enables interaction with the available API endpoints.
Access to this interface is available in the title bar of the main interface.


After clicking on the button (3), a new tab opens with the API.
In this interface, all API endpoints are available and can be used.
Use of the individual endpoints is subject to the same rights as in Web interfaces.

**Note:**

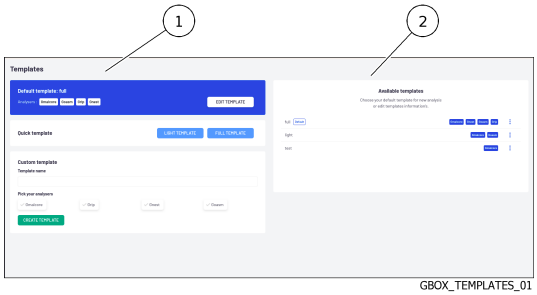
A feature requiring administrator rights can only be used by a user having operator rights.

For more information on the API, please refer to *API graphical interface*.

---

### 5.3.4 `Admin/Templates` screen of the Web UI

After pressing the `Templates` command, the following screen is displayed.

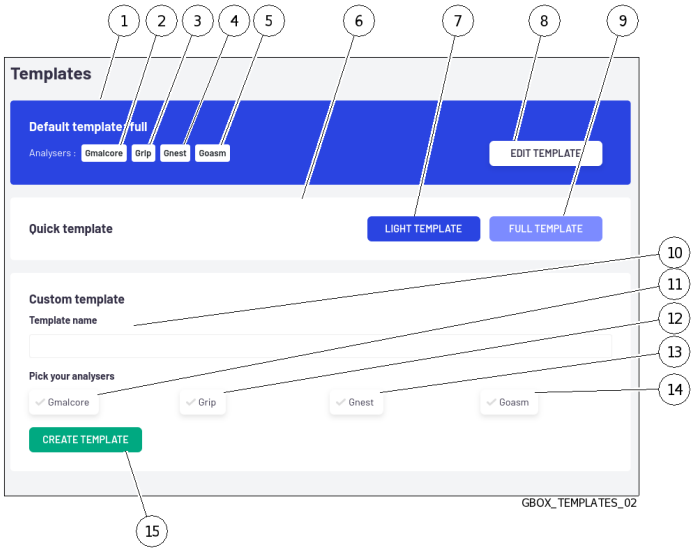



| item | Zone | Function |
|---|---|---|
| 1 | Template creation | This zone enables creating templates that can be used to analyse files accessible to the operator. |
| 2 | Template management | This area (`Available templates`) enables managing existing templates. |

---

#### 5.3.4.1 Template Creation Zone

The template creation area consists of 2 parts.




This zone includes:

- The `Defaut template` et `Quick template` sections: *The Creation of the default template section*
- The `Custom template` section: *Creating a custom template*

For implementation, see the *Creating an analysis template* procedure.

---

##### 5.3.4.1.1 The Creation of the default template section

This section is made up of the `Defaut template` and `Quick template` sections.
It enables configuring the templates that can become the default template used by the operator when searching for threats.
The creation phase of these templates is carried out using the elements described below.

**Astuce:**

The default template is selected from the existing templates in the `Available templates` zone.

**Important:**

It is essential to ensure that at least one template is defined so that operators can carry out analyses.

| Item | Name | Function |
|---|---|---|
| 1 | `Default template` | This field enables defining the default template (`Default template`)<br>If a default template is defined, its name is displayed.<br>In this example, `Default template: full` indicates that the default template name is full<br>If no default template is defined then the following message is displayed: `Default template: No default template`<br>The engines defined in the default template are listed: in this example, these are items (2) to (5). |
| 2 | | • In this example, the `Gmalcore` engine (Analyser) is visible and therefore active in the template by default. |
| 3 | | • In this example, the `Grip` engine (Analyser) is visible and therefore active in the template by default. |
| 4 | | • In this example, the `Gnest` (Analyser) engine is visible and therefore active in the template by default. |
| 5 | | • In this example, the `Goasm` engine (Analyser) is visible and therefore active in the template by default. |
| 8 | | • The `EDIT TEMPLATE` button enables editing of the default template.<br>It is possible to change the active motors, and configure them. |
| 6 | `Quick template` | This area enables a template to be quickly selected by simply clicking on one of the following 2 buttons: |
| 7 | | • the `LIGHT TEMPLATE` button creates a template using only the Gmalcore and Goams engines, hence the term light template. |
| 9 | | • the `FULL TEMPLATE` button creates a template with the active engines, hence the term full template.<br>The parameters for the Grip and Gnest engines are the default parameters. The list of default parameters is provided below. |

**Note:**

There can only be one template designated `light` and one defined as `full`.

#### 5.3.4.1.2 Creating a custom template

| Marker | Name | Function |
|---|---|---|
| 10 | `Template name` | This field enables specifying the name of a custom template<br>The current template type is listed. In this example, `Default template: full` indicates that the current template is full. |
| 11 | `Gmalcore` | Enables the Gmalcore engine. In the example, the Gmalcore engine is inactive. |
| 12 | `Grip` | Enables the GRIP engine. In the example, the GRIP engine is inactive. |
| 13 | `Gnest` | Enables the GNEST engine. In the example, the GNEST engine is inactive. |
| 14 | `Goasm` | Enables the Goasm engine. In the example, the GOASM engine is inactive. |
| 15 | `CREATE TEMPLATE` | The `EDIT TEMPLATE` button opens a window for setting the parameters of the template to be created with the pre-selected options. |

---

**Grip settings**

The Grip engine must be configured by selecting the type of analysis (`Analysis type`): {light|heavy} to specify the data extracted from the file being analysed.

**Note:**

The default analysis is: light

| Extracted data | light | heavy |
|---|---|---|
| archive size | X | X |
| libraries used | x | x |
| binary entrypoint information | x | x |
| general information | x | x |
| character strings | | x |
| imports / exports | | x |
| *sections* of the binary | | x |

---

**Gnest parameters**

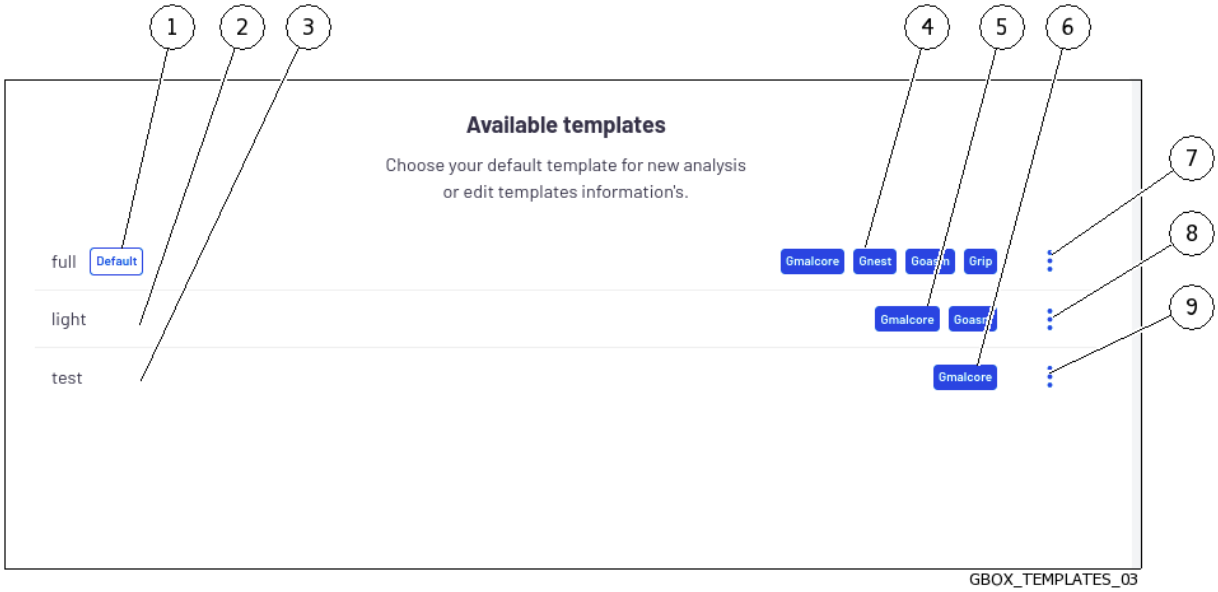
The Gnest engine must be configured for this template:

| Parameter | Meaning | Values | Default values |
|---|---|---|---|
| `VM` | Choice of active VM. Only the selected VM is activated in this template The following parameters apply only to the selected VM or to all VMs (choose `any) | any or default | any |
| `Analysis duration` | Maximum execution time in the VM | 100s to 300 s | 100s |
| `Network` | Activating the VM's network interface | None or Internet | None |
| `Memory dump` | Enable or disable the memory dump at the end of the analyses performed by Gnest<br>Danger, high disk usage:<br>The memory dump can be downloaded from the **Reports - List all** page from the analysis artefacts. | No or Yes | No |

**Avertissement:**

Activating the `Memory dump` option means that the entire memory (4GB) is saved to disk.
To avoid saturating disk space, it is best to activate this option on specific templates and not on the default template.
However, it is possible to delete these dumps by removing the artefacts available in the reports or via the API.

#### 5.3.4.2 Template Management Zone




The template Management area enables existing templates to be managed.

| Item | Name | Function |
|---|---|---|
| 1 | `full` | This template, whose name is full, is defined as the default template ("Default" field). |
| 4 | | List of active engines in this template; here, in the case of the full template, all engines are enabled. |
| 7 | | Menu for managing this template; in the case of the default template, only the `Edit` command is available. |
| 2 | `light` | This template corresponds to the one referred to as `light`. |
| 5 | | List of active engines in this template; here, in the case of the light template, only the Gmalcore and Goasm engines are enabled |
| 8 | | Management menu for this template: the `Set as default`, `Edit` and `Remove` commands are available |
| 3 | `test` | This template is an example of a custom template |
| 6 | | List of active engines in this template; here, in the case of the light template, only the Gmalcore and Goasm engines are enabled |
| 9 | | Management menu for this template: the `Set as default`, `Edit` and `Remove` commands are available |

An analysis template can be deleted by clicking on the `Remove` button.

When an analysis template is deleted, the analyses launched with this template are retained, as is the name of the template at the time of deletion.

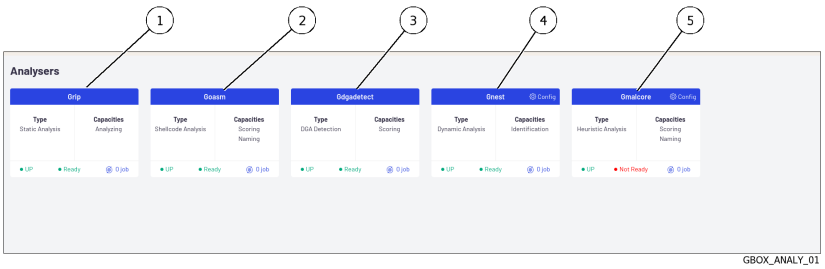
For implementation, see the *Managing the analysis templates* procedure.

---

### 5.3.5 `Analysers` screen of the Web UI

This screen displays the status of the various analysis engines.

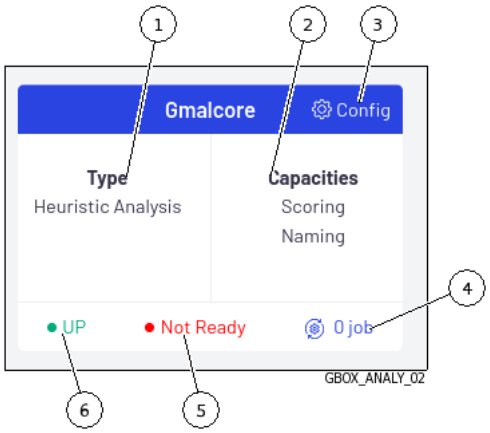
When the `Analysers` command is pressed, the following screen is displayed.



GBOX_ANALY_01

| Marker | Engine | Engine function |
|---|---|---|
| 1 | *Grip engine* | Static analysis |
| 2 | *Goasm engine* | Shellcode detection |
| 3 | *Gdgadetect engine* | Domain name detection |
| 4 | *Gnest engine* | Dynamic analysis within a virtual machine |
| 5 | *Gmalcore engine* | Static and heuristic analysis |

The following information is displayed for each engine:




| Marker | Name | Grip Engine | Goasm Enging | Gdgadetect Enging | Gnest Engine | Gmalcore Engine |
|---|---|---|---|---|---|---|
| 1 | Type | Static analysis | Shell code detection | Detection of domain names generated by the Domain Generation Algorithm (DGA) | Executes the file in a virtual machine and analyses its behaviour | Static and multi-engine heuristic analysis |
| 2 | Capabilities | Analysis | Provides a score for the potential danger and names the shellcode detected | Provides a compromise score | Names the problem detected | Provides a score for the potential danger and names the problem detected |
| 3 | Config | Not configurable, so this field is not displayed | | | Virtual machine management - adding, deleting, logging | Gmalcore engine management |
| 4 | x jobs : number of tasks in progress (analysis status NEW + IN PROGRESS) | Number of jobs awaiting processing | | | | |
| 5 | Ability to carry out analyses | This engine has no requirements, so it is always in the `ready` state. | | | The engine is in the `ready` state if there is the same number of VMs in the GBox.<br>and in CAPE - the dynamic analysis engine | The engine is in the `ready` state if all the engines are installed.<br>and the API is up |
| 6 | Engine status | UP : engine api is listening : DOWN : engine api is not active | | | | |

**Astuce:**

If the engine status (Grip, Goasm, Gdgadetect or Gnest) is `DOWN`, wait a moment.
If the engine remains in the `DOWN` status, contact Gatewatcher support. .. sav2_en

**Astuce:**

If the Gmalcore engine status is `DOWN`, restart the Malcore service or Reinstall the Malcore service: see *`Services` command*.
If the engine remains in the `DOWN` status, contact Gatewatcher support.
The `Not Ready` status for the **Gmalcore** engine does not necessarily indicate that the engine is unable to perform scans, but it does indicate that at least one of the 16 antivirus engines is out of date or out of service.

---

#### 5.3.5.1 Grip engine

However, it is useful for quickly analysing the file's metadata if it is classified as *suspicious* or *malicious*.
It is used to obtain information about the file prior to more in-depth analysis.
This data is displayed in the detailed report, more specifically in the **TOP** and **Static** sections (see *Detailed report*).

| | |
|---|---|
| **Maximum file size** | 50 MB |
| **Analysis timeout** | 2 minutes |
| **Type** | light |

---

##### 5.3.5.1.1 Viewing the Grip status

---

#### 5.3.5.2 Goasm engine

This analysis engine enables detecting and analysing **shellcodes**.
It enables identifying certain encodings and provides details of the system calls made.
This engine assigns a score to the potential danger and names the shellcode detected.
This data is displayed in the detailed report, more specifically in the **TOP** and **Shellcode** sections (see *Detailed report*).

| | |
|---|---|
| **Maximum file size** | 50 MB |
| **Analysis timeout** | 4- 6 minutes |
| **Type** | rapid |

Goasm can be deemed fast for small files (< 5MB).

In the case of large text files (> 5MB), detection takes time because the binary must be scanned for shellcode patterns.
Goasm's internal analysis timeout can therefore be reached: 4 min.
The external engine timeout is set at 6 min.

In the event of an internal timeout:

- There is an error message in the `Shellcode` section of the report
- The engine simply stops scanning the file byte by byte.

In the event of an external timeout (error occurred or Goasm blocked), an error is present in the report mentioning a timeout. In this case, restart the analysis.

---

#### 5.3.5.3 Gdgadetect engine

##### 5.3.5.3.1 Introduction to the DGA Algorithm

The **GBox** includes an engine capable of detecting domain names generated by the Domain Generation Algorithm (DGA).
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.

---

##### 5.3.5.3.2 Analyse

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).

---

##### 5.3.5.3.3 Displaying DGA alerts

The analysis is carried out on the `Quick analysis` page.
Depending on the result, a green or red icon indicates whether it is a DGA or not.

---

#### 5.3.5.4 Gnest engine

The **Gnest** analysis engine enables dynamic analysis.
It executes the file in a virtual machine (sandbox) and analyses its behaviour.
Following this, it is possible to extract the data generated during the analysis, such as a *dump* of the memory, the extracted character strings, or a capture of network communications (pcap).
When connected to the GCenter, this engine is useful for in-depth analysis of a file classified as *suspicious* or *malicious*, during a second analysis of a file.
This analysis is slower, requiring an experienced operator to analyse the results.

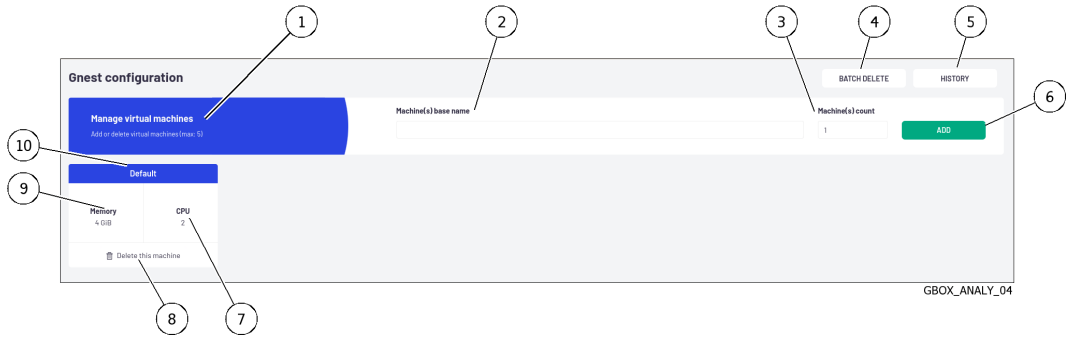
This data is displayed in the *Detailed report* and more specifically in the **TOP**, **Iocs**, **Ttps**, **Overview**, **Signatures** and **Process Tree** sections.

| | |
|---|---|
| **Maximum file size** | 50 MB |
| **Analysis timeout** | 1 hour |
| **Type** | slow |

---

#### 5.3.5.5 `Gnest configuration` screen

This screen enables managing the virtual machines of the Gnest engine.
After clicking on the Gnest engine link, the following screen is displayed.



| Item | Description | |
|---|---|---|
| 1 | `Manage virtual machines` zone: this zone enables creating new virtual machines.<br>This zone includes: | |
| 2 | • `Machine(s) base name` | Base name of the virtual machine(s) (VM) |
| 3 | • `Machine(s) count` field | Number of machine(s) to create |
| 6 | • `ADD` button | Starts the creation of virtual machine(s) |
| 4 | `BATCH DELETE` button | Enables deleting one or more VMs |
| 5 | `HISTORY` button | Displays the VM management history window |
| 10 | `Default` name: the existing virtual machine and the name of the default machine. It includes the following Information | |
| 9 | • `Memory` field | Value of the amount of memory allocated to the VM |
| 7 | • `CPU` field | Value of the processor quantity allocated to the VM |
| 8 | • `Delete this machine` button | Deletes the selected machine |

Adding/deleting VMs waits until the current Gnest analyses have finished and blocks the next analyses. However, if a VM's template is deleted while jobs are still pending, the jobs will be switched to error mode. The implementation is given in *Procedure to configure the Gnest engine*.

---

#### 5.3.5.6 Gmalcore engine

- detecting malware by means of a static and heuristic multi-engine analysis of files in real time
- scanning via 16 anti-virus engines
- scanning capacity close to 200,000 files per 24 hours
- obtain the name(s) of the threat and a threat score
- rapid identification of threats

The 16 anti-virus engines are displayed under the name `engine hash` in the web interface.

| | |
|---|---|
| **Maximum file size** | 50 MB |
| **Analysis timeout** | 2 minutes |
| **Type** | light |

Events generated by Gmalcore are displayed in the `Heuristic` section of the GBox analysis report.

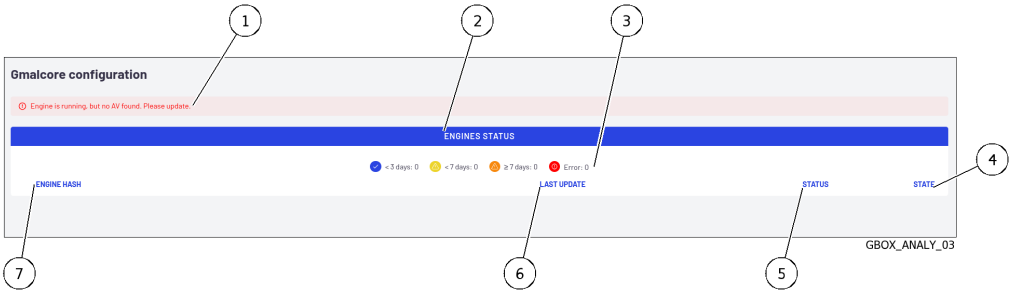
---

#### 5.3.5.7 `Gmalcore configuration` screen

This screen provides information on the Gmalcore engine configuration:

- The status of the Gmalcore engines
- The date of the last installed update

After clicking on the Gmalcore Engine `Config` link, the following screen is displayed.

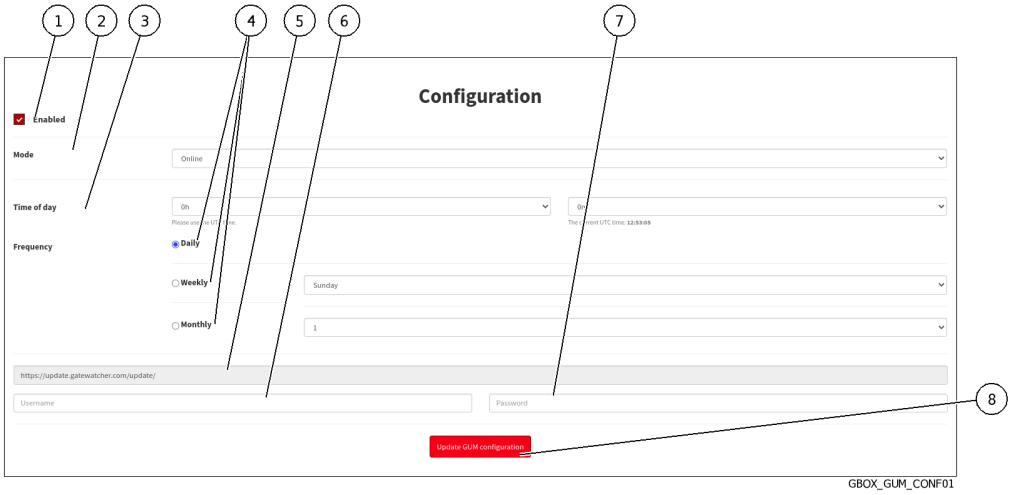



| Item | Engine | Function |
|---|---|---|
| 1 | Configuration status message | `Engine is running, but no AV found. Please update.` : requires the installation of an update for the Gmalcore engines |
| 2 | `ENGINES STATUS` | This area enables the antivirus engine status to be displayed, with the following information: |
| 3 | | • coloured icons. Each engine is preceded by an icon indicating how long ago the engine signatures were updated. |
| 7 | | • `ENGINE HASH`. The 16 anti-virus engines are displayed under the name"engine hash" |
| 6 | | • `LAST UPDATE`. Date of the last update |
| 5 | | • `STATUS`. Icon indicating the status and age of the last update |
| 4 | | • `STATE`. Engine status (PRODUCTION, DOWNLOADED...) |

The implementation of the Gmalcore configuration is provided in *Procédure to configure the Gmalcore engine*.

### 5.3.6 `Admin- GUM - Config` screen of the legacy Web UI

After pressing the `Config` command from the `GUM` menu, the following screen is displayed.




| Marker \| Name | | Function |
|---|---|---|
| 1 | `Enabled` | Enables updates to be carried out in local or online mode |
| 2 | `Mode` | Enables selecting the type of update mode: local or online.<br>Online mode enables automatic updates from Gatewatcher servers.<br>Local mode enables updates to be made from a local repository. |
| 3 | `Time of day` field | Choosing the update time |
| 4 | `Daily`, `Weekly`, `Monthly` buttons | Selecting the frequency at which updates are triggered. |
| 5 | Source field for updates | In Online mode, this field is automatically filled in.<br>In Local mode, this field must contain the IP address or fully qualified domain name (FQDN) of the local repository address. |
| 6 | `Username` field | In Online mode, login field for connecting to Gatewatcher servers<br>In local mode, local repository login field |
| 7 | `Password` field | In Online mode, field for password to connect to Gatewatcher servers<br>In Local mode, field for the local repository password |
| 8 | `Update GUM configuration` button | Updates the GUM configuration |

This screen enables configuring the automatic scheduling of updates.
These updates can be made:

- Via Online mode

If necessary, configure a proxy (see the *Configuring a proxy* procedure)
Online mode enables automatic updates to be made from the Internet.
The URL field will be filled in automatically. The update packages can be obtained from the Gatewatcher servers https://update.GATEWATCHER.com/update/.

- Via the Local mode
  If necessary, configure a proxy (see the in *Configuring a proxy* procedure)
  Local mode enables updates to be made from a local repository previously configured to download packages from Gatewatcher servers https://update.GATEWATCHER.com/update.
  This local repository is defined in the *`Admin- GUM - Config` screen of the legacy Web UI*.

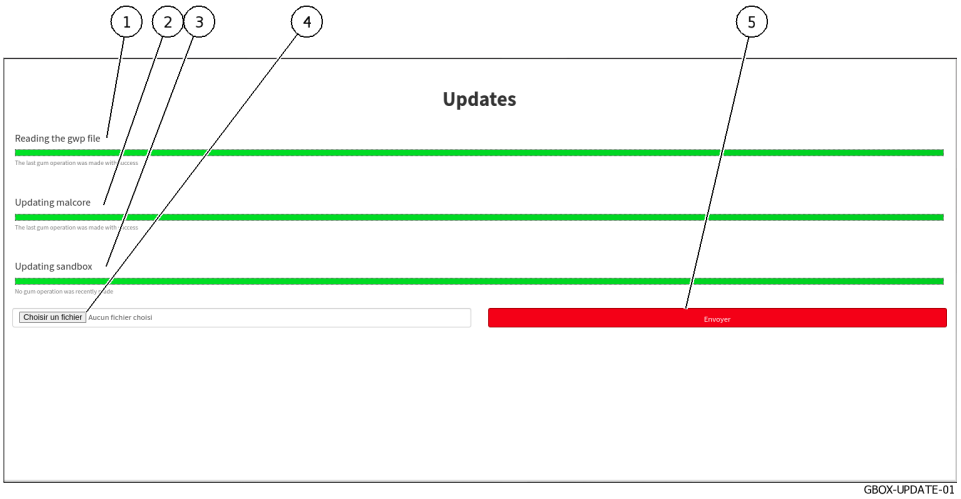
An intelligence account will be required for the update package to be downloaded from the site.
In `online` mode, this user and password pair must be entered in the `Username` and `Password` fields below the address.

For installation instructions, please refer to *Configuring automatic updates via GUM*.

---

### 5.3.7 `Admin- GUM - Updates` screen of the legacy Web UI

After pressing the `Updates` command from the `GUM` menu, the following screen is displayed.




| Marker \| Name | | Function |
|---|---|---|
| 1 | `Reading the gwp file` | Progress bar of the integrity check of a loaded package |
| 2 | `Updating malcore` | Malcore engine update progress bar / Last update status |
| 3 | `Updating sandbox` | Gnest engine update progress bar/ Last update status |
| 4 | `Browse` button | Enables selecting an update package |
| 5 | `Send` field | Triggers the installation of the update package |

Signature updates or **updates** represent updates to the GBox detection engines.
There are 3 types of update packages:

- Gmalcore packages (*latest_malcore*): these packages only contain updates to the antivirus engines and databases used by Malcore.

- Sandbox packages (*latest_sandbox*): these packages contain updates to the signatures and modules used by the Gnest engine sandboxes.
- Complete packages (*latest_full*): these packages are a combination of the two previous packages.

This screen enables viewing the history and status of the installation:

- For packages downloaded in a scheduled manner
- For packages downloaded manually

If a package needs updating:

- 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
- Progress bar in the `Updating malcore` field begins to progress. This corresponds to the processing of the Malcore engine files
- The progress bar in the `Updating sandbox` field starts to move: this corresponds to the processing of updates to signatures and modules used by the sandbox

To use a package file from the remote PC, use the `Browse` button (4).

**Important:**

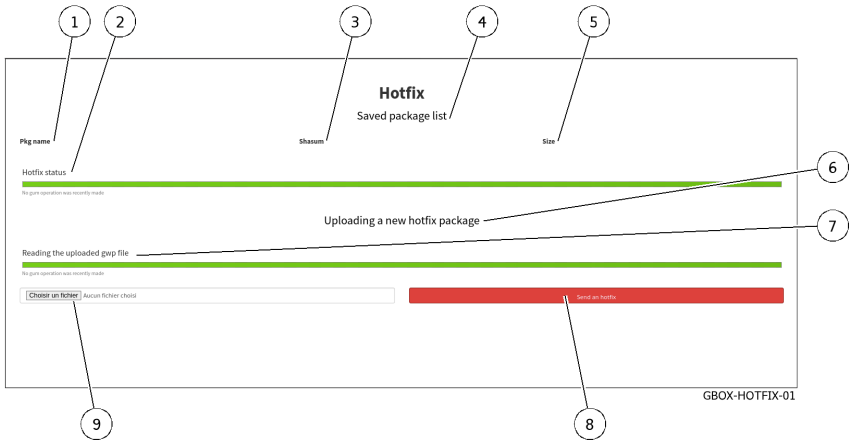
In this case, select a GWP package file, only from those of the solution's engines.
Hotfix and upgrade packages will not work in this screen.

For implementation, see the *Manual installation of a signature update* procedure.

---

### 5.3.8 `Admin- GUM - Hotfix` screen of the legacy Web UI

After pressing the `Hotfix` command from the `GUM` menu, the following screen is displayed.




The `Hotfix` screen contains the following items:

| Marker | Name | Function |
|---|---|---|
| 4 | `Saved package lists` zone, which includes... | List of downloaded patches awaiting application. Once installed, the list is purged<br>After installation, the hotfix appears in the gbox software number (marker 16 in the *Traditional interface navigation bar*). |
| 1 | • `Pkg Name` field | Name of the software package |
| 2 | • `Update status` field | Patch application progress bar / Status of last package application |
| 3 | `Shasum` field | Shasum sha256 of the file |
| 5 | `Size` field | File size |
| 6 | `Uploading a new hotfix package` zone, which includes... | Zone enabling manual installation of a package |
| 7 | `Reading the uploaded gwp file` field | Progress bar of the package integrity check / Status of the last check |
| 8 | • `Send a hotfix` button | Triggers installation of the patch |
| 9 | `Choose a file` button | Enables selecting a package |

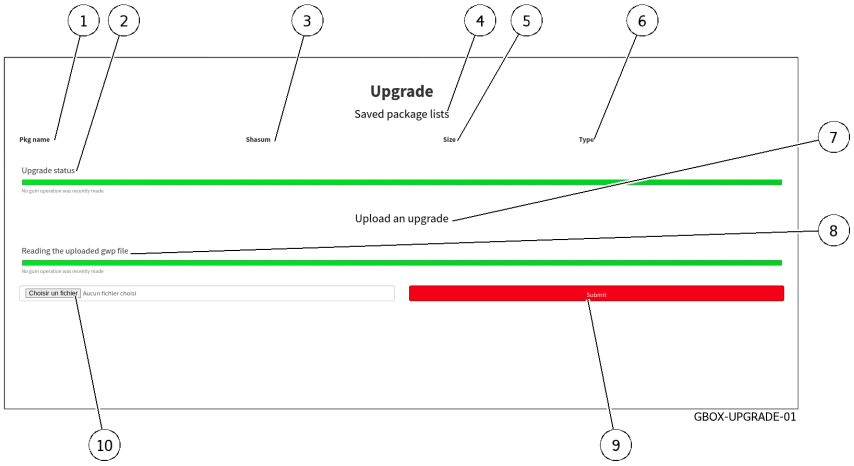
**Important:**

A gwp package file must be selected, and only those of the Hotfix type.
Other types of packages will not work in this interface.

For more information, see the *Applying a hotfix patch* section.
For implementation, see the *Installing a hotfix patch* procedure.

### 5.3.9 `Admin- GUM - Upgrade` screen of the legacy Web UI

After pressing the `Upgrade` command from the `GUM` menu, the following screen is displayed.




The `Upgrade` screen contains the following items:

| Item | Name | Function |
|---|---|---|
| 4 | `Saved package lists` zone, which includes | History of software packages |
| 1 | • `Pkg Name` field | Name of the software package |
| 2 | • `Upgrade status` field | Upgrade application progress bar / Status of last package application |
| 3 | `Shasum` field | Shasum sha256 of the file |
| 5 | `Size` field | File size |
| 6 | • `Type` field | Type |
| 7 | `Upload an upgrade` field includes | Area enabling manual installation of a package |
| 8 | `Reading the uploaded gwp file` field | Progress bar of the package integrity check / Status of the last check |
| 9 | • `Submit` button | Triggers the package installation |
| 10 | `Choose a file` button | Enables selecting a package |

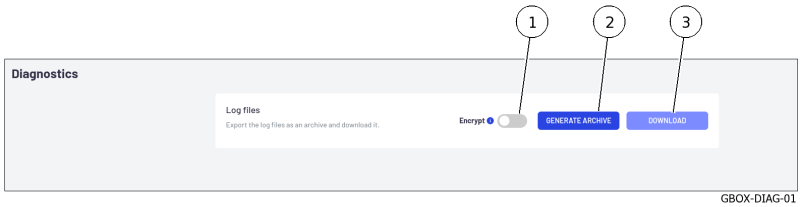
**Important:**

A GWP package file must be selected, and only those of the upgrade type.
Other types of packages will not work in this interface.

For more information, see the presentation of *Upgrade*.
For implementation, see the *Installing an upgrade* procedure.

### 5.3.10 `Admin-GBox - Diagnostics` screen of the Web UI

When the `Diagnostics` command in the `GBox` menu is pressed, the following screen is displayed.
This screen enables log files to be exported and downloaded.



GBOX-DIAG-01

| Item | Name | Function |
|---|---|---|
| 1 | `Encrypt` | Encrypting log files |
| 2 | `GENERATE ARCHIVE` | Button for generating compressed `Log files` files |
| 3 | `DOWNLOAD` | `Log files` download button |

The log export file is encrypted; only the GATEWATCHER support team can decrypt it.
For more details on data management, see the *Data use* paragraph.
For implementation, see the *Generating and loading files for diagnosis* procedure.

---

### 5.3.11 `Admin-GBox - Accounts` screen of the Web UI

After pressing the `Accounts` command from the `Admin-GBox` menu, the `Accounts management` screen is displayed and enables:

- Managing users and related roles
- Displaying the history of authentications, permissions, and user management

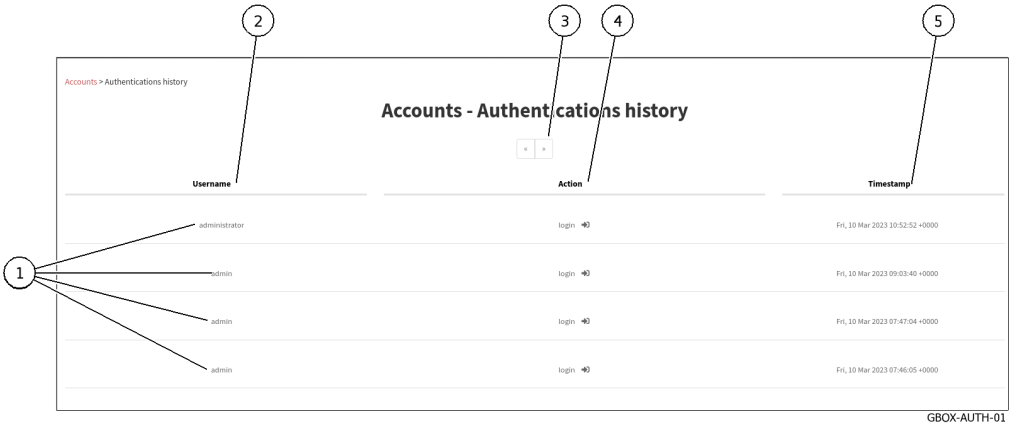
This screen contains the following sections:

| Section | Function | refer to |
|---|---|---|
| `Authentications history` | History of all authentications | *The `Authentications history` section of the `Accounts` submenu* |
| `Creations/Deletions history` | History of all user creations and deletions | *The `Creations/Deletions history` section of the `Accounts` submenu* |
| `Permissions history` | History of all user permissions | *The `Permissions history` section of the `Accounts` submenu* |
| `Users management` | Creating new users and managing existing users | *`Admin-GBox- Users management` screen of the Web UI* |
| `API tokens` | Creating tokens and managing existing tokens | *The `API tokens` section of the `Accounts` submenu* |

---

#### 5.3.11.1 The `Authentications history` section of the `Accounts` submenu

The `Authentications history` window displays the history of all authentications in the form of a timestamp in the format [**day , xx month, year hh**: **mm**: **ss**].




This window displays the connections (1) in order from most recent to oldest.
The arrows (3) enable navigating between the different pages.
For each connection, the following information is displayed:

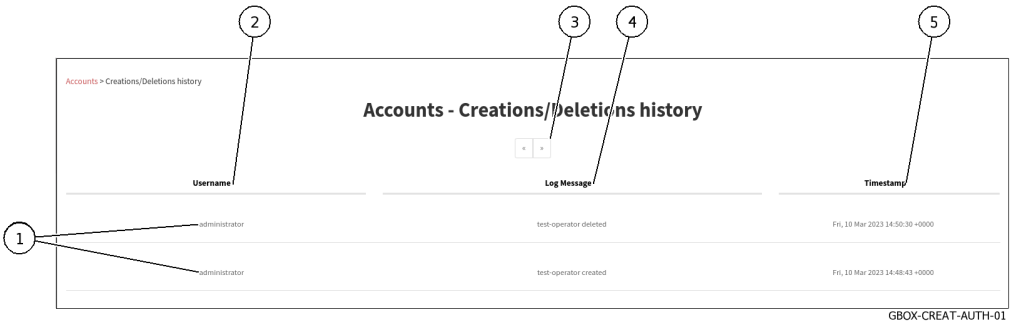
- `Username` field (2): name of the person who logged in/out
- `Action` field (4): login or logout
- `timestamp` field (5) : date and time of login / logout in the format (**d , mm yyyy hh**: **mm**: **ss**)

For implementation, see the *Viewing the authentication history* procedure.

---

#### 5.3.11.2 The `Creations/Deletions history` section of the `Accounts` submenu

The `Creations/Deletions history` window displays the history of all user creations and deletions.
All changes made to a user by an administrator account are displayed.




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/deleted the account
- `Log Message` field (4): the account name followed by the created or deleted action

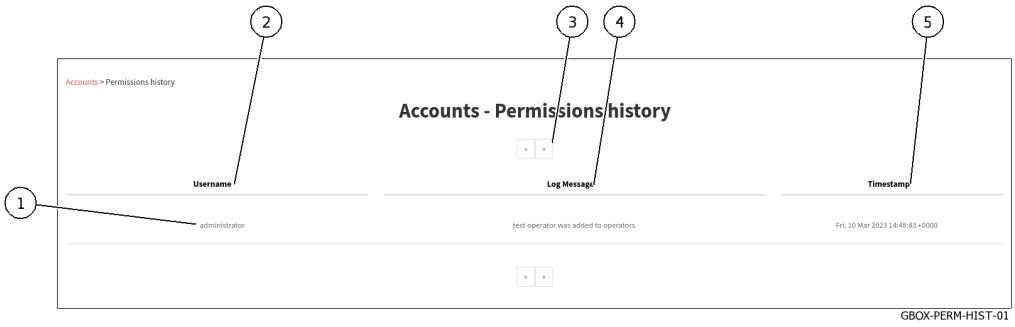
- `timestamp` field (5) : date and time of login / logout in the format (**d** , **mm yyyy hh**: **mm**: **ss**)

For implementation, see the *Viewing the history of user creations or deletions* procedure.

---

#### 5.3.11.3 The `Permissions history` section of the `Accounts` submenu

The `Permissions history` window displays a history of all changes to user rights.




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 group.
- `timestamp` field (5) : date and time of changes to the format (**d** , **mm yyyy hh**: **mm**: **ss**)

For implementation, see the *Viewing the history function for all changes in user rights* procedure.

---

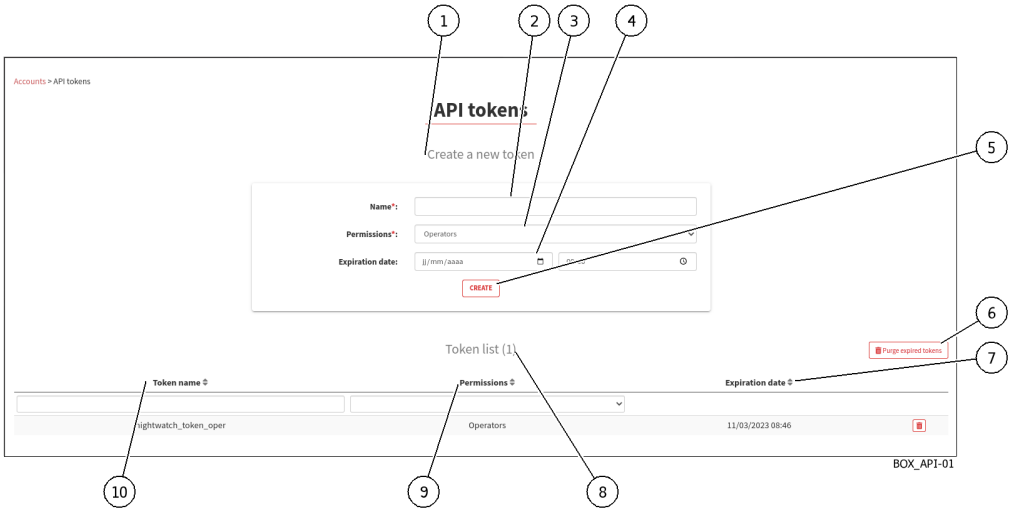
#### 5.3.11.4 The `Users management` section of the `Accounts` submenu

Refer to *`Admin-GBox- Users management` screen of the Web UI*

---

#### 5.3.11.5 The `API tokens` section of the `Accounts` submenu

The `API tokens` screen manages the API access tokens.




| Marker | Area | Item |
|---|---|---|
| 1 | `Create a new token` : field for adding a new API access token | |
| 2 | | `Name` : field for entering 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 | | `CREATE` : button for adding the new token |
| 8 | `Token list` : zone to display the list of existing tokens | |
| 6 | | `Purge expired tokens` : button for purging expired tokens |
| 10 | | `Name` : field for displaying the token name |
| 9 | | `Permission`: field to display the account and hence the rights |
| 7 | | `Expiration`: field for displaying the expiration date |

For implementation, see the *Creating or deleting an API access token* procedure.

---

### 5.3.12 `Admin-GBox- Users management` screen of the Web UI

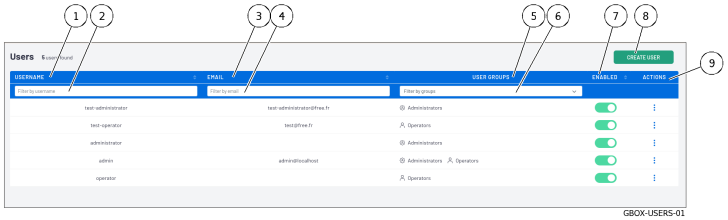
This screen enables:

- Managing existing users and related roles
- Creating new users

After pressing the `Users management` command from the `Admin-GBox` menu, the following screen is displayed.

This screen enables managing existing users.

The `Users` window includes:



| Marker | Name | Description |
|---|---|---|
| 1 | `USERNAME` | Field indicating the user's name |
| 3 | `EMAIL` | Field specifying the e-mail address |
| 5 | `USER GROUPS` | Field indicating the group (Operators or Administrators) or both |
| 7 | `ENABLED` | Enable or disable the account |
| 8 | `CREATE USER` | Button for displaying the `Create user` window detailed hereafter |
| 9 | `ACTIONS` | Possible actions for each existing account: edit, delete, reset password |

The fields below are additional fields enabling existing accounts to be filtered.

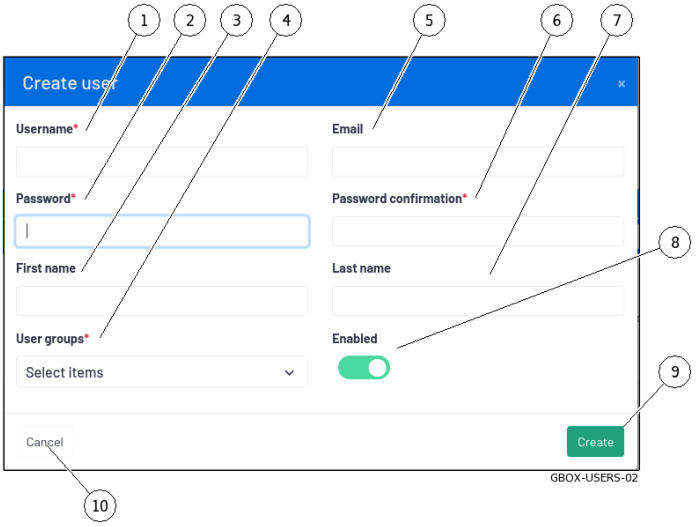
| Marker | Name | Description |
|---|---|---|
| 2 | `Filter by username` | Enables filtering accounts with this name to be entered |
| 4 | `Filter by email` | Enables filtering of accounts with this email address to be entered |
| 6 | `Filter by groups` | Enables filtering of accounts with this group to be selected |

For implementation of the initialization of a user's password, see the *Resetting a user's password* procedure.
For implementation of the deletion of a user, see the *Deleting a user* procedure.
For implementation of the modification of certain information about a local user, see the *Changing some of a local user's information* procedure.

---

#### 5.3.12.1 `Create user` window

Once the `Create User` button is pressed, this window is displayed, enabling the user to be created.



| Marker | Name | Description |
|---|---|---|
| 1 | `Username` | Full name of the new user. Use only case-insensitive letters such as commas, full stops, apostrophes, and hyphens. |
| 2 | `Password` | This password must contain a minimum of seven characters (or **8**). |
| 3 | `First name` | User's first name: optional field |
| 4 | `Users groups` | Enables selecting the Operators or Administrators group, or both. |
| 5 | `Email` | Email address: optional field |
| 6 | `Password confirmation` | Password is the same as the password field |
| 7 | `Last name` | User's name: optional field |
| 8 | `Enabled` | Enable or disable the account |
| 9 | `Create` | User creation button with parameters entered |

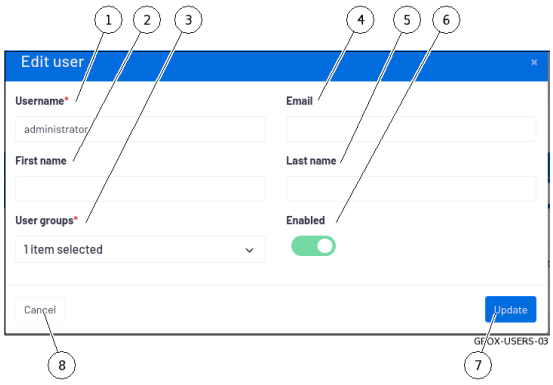
**Note:**

Refer to paragraphes *Authorised functions for members of the Operators group* and *Authorised functions for members of the Administrators group*

For implementation, see the *Creating local users* procedure.

#### 5.3.12.2 `Edit user` window

Pressing the `Edit` command in the `ACTIONS` menu displays this window, enabling editing of a user.




| Marker | Name | Description |
|---|---|---|
| 1 | `Username` | Full name of the new user. Use only letters, commas, full stops, inverted commas, hyphens, letters, numbers and [@/./+/-/-/_.] characters. **to be verified!** |
| 2 | `First name` | User's first name: optional field |
| 3 | `Users groups` | Enables selecting the Operators or Administrators group, or both. |
| 4 | `Email` | Email address: optional field |
| 5 | `Last name` | User's name: optional field |
| 6 | `Enabled` | Enable or disable the account |
| 7 | `Update` | Button for updating entered parameters |
| 8 | `Cancel` | Cancel button |

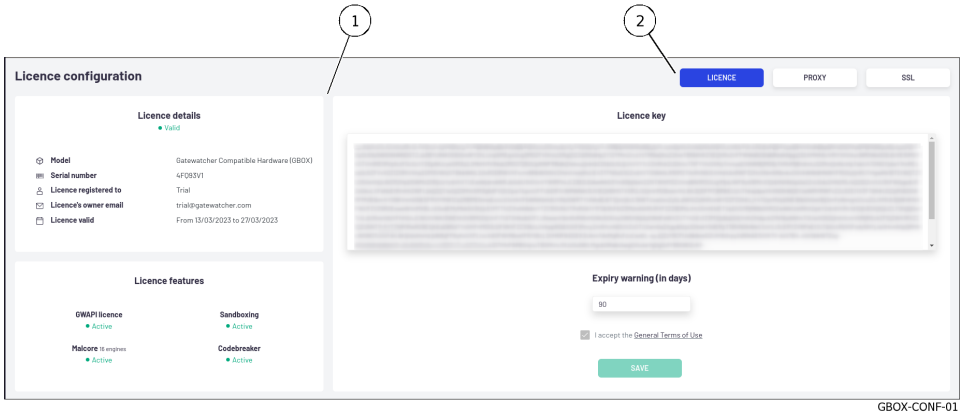
For instructions, see *Changing some of a local user's information*.

### 5.3.13 `Admin-GBOX- Configuration` screen of the Web UI

This screen enables:

- Viewing information about the current licence, checking its validity, and the available features
- Configure the proxy server to retrieve updates via the proxy and a local repository
- Configure the Secure Socket Layer (SSL) certificate

After pressing the `Configuration` command in the `Admin-GBox` menu, the following screen is displayed. The window includes:



GBOX-CONF-01

| Marker | Description |
|---|---|
| 1 | *`Configuration` screen display area* : the contents depend on the option selected by pressing one of the buttons (2) |
| 2 | *Dashboard selector for the `Configuration` screen*: includes three choice buttons |

---

#### 5.3.13.1 Dashboard selector for the `Configuration` screen

The selector includes the following buttons:

| Name | Description |
|---|---|
| `LICENCE` | Viewing information about the current licence, checking its validity, and the available features |
| `PROXY` | Proxy server configuration |
| `SSL` | Secure Socket Layer (SSL) certificate configuration |

---

#### 5.3.13.2 `Configuration` screen display area

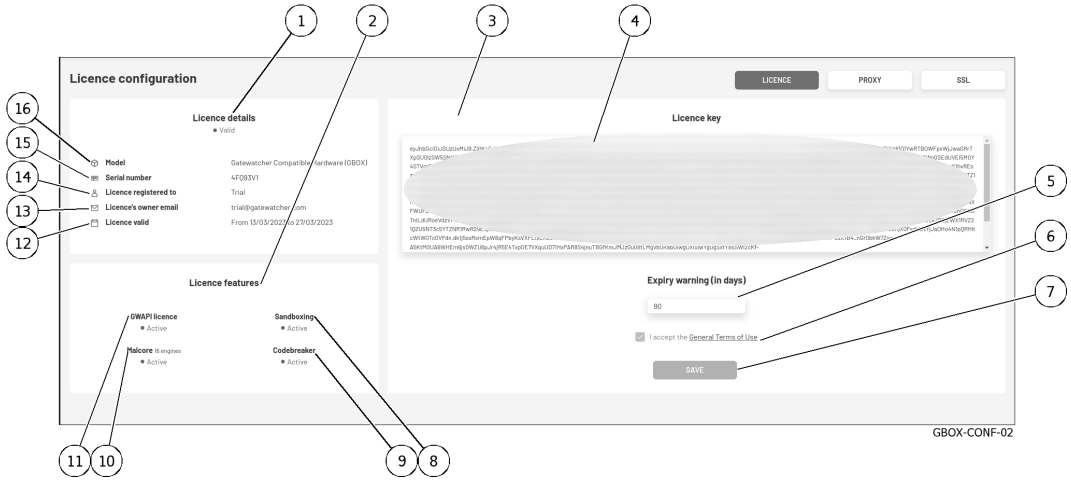
This zone displays the information on the screen that corresponds to the button used in the dashboard selector. Three screens are available:

- *`License configuration` screen*
- *`Proxy settings` screen*
- *SSL settings screen*

---

#### 5.3.13.2.1 `License configuration` screen

After clicking on the `LICENCE` button, the next screen is displayed:




The screen consists of three parts:

- The `License key` part: enables entering the license and the delay for the alarm message
- The `License features` part: enables viewing the features enabled in this license
- The `Licence details` part: enables obtaining information on the material for which this licence was issued via its model and serial number, together with the period of validity of the licence, the associated contact address, and type of licence.

The `License key` section (3) contains the following elements:

| Item | Name | Function |
|---|---|---|
| 4 | `License key` field | Entering the licence key |
| 5 | `Expiry warning (in days) ` field | Entering the number of days of the licence expiration alarm message |
| 6 | `I accept the General Terms of Use` field | Selecting acceptance of the terms of use |
| 7 | `Save` button | Stores the current settings |

The `License features` section (2) contains the following elements:

| Item | Name | Function |
|---|---|---|
| 8 | `Sandboxing` field | Information on enabling the Gnest engine (sandboxing) |
| 9 | `Codebreaker` field | Information on activating the Codebreaker engine, another name for the Goasm engine |
| 10 | `Malcore engines` field | Malcore engine activation information (number of engines) |
| 11 | `GWAPI licence` field | Information on enabling the GWAPI |

The `License details` section (1) contains the following elements:

| Item | Name | Function |
|---|---|---|
| 12 | `License valid` field | Licence registration date and remaining duration |
| 13 | `License's owner email` field | Email of the licence owner |
| 14 | `License registered to` field | Registration of the licence |
| 15 | `Serial Number` field | Server information |
| 16 | `Model` field | Type of material (**to be completed**) |

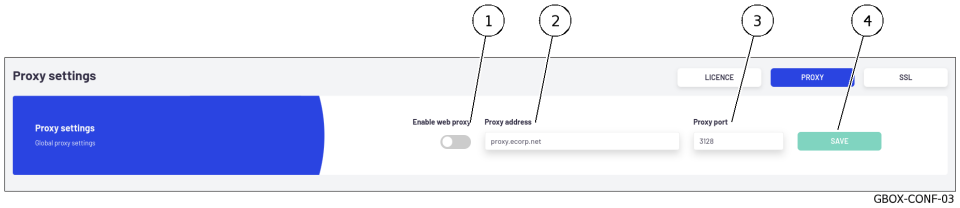
To implement the Licence Modification, see the *Modifying the licence* procedure.

---

#### 5.3.13.2.2 `Proxy settings` screen

The GBOX includes the possibility of configuring a proxy server in order to retrieve updates (signature updates) via the proxy.

After clicking on the `PROXY` button, the next screen is displayed:



GBOX-CONF-03

The `Proxy settings` section contains the following items:

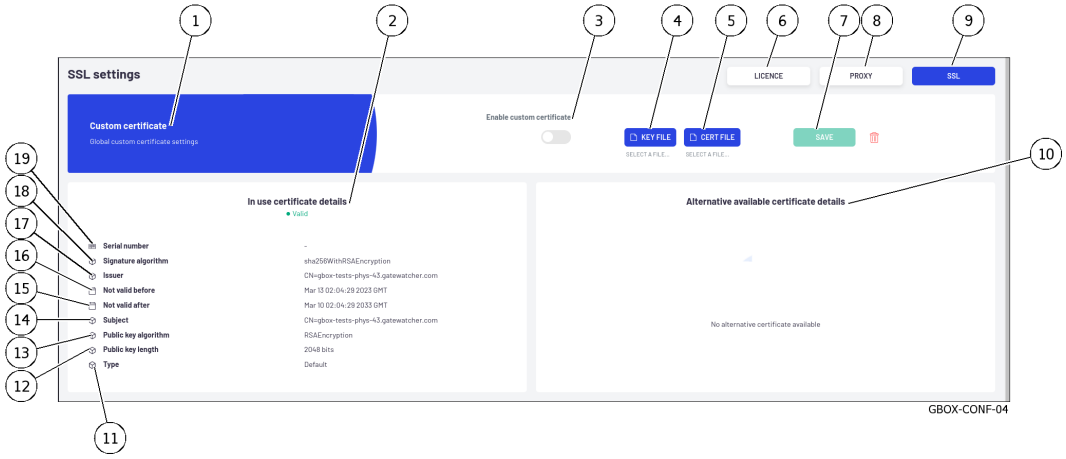
| Item | Name | Function |
|---|---|---|
| 1 | `Enable Web Proxy` selector | Enables/Disables the use of the proxy |
| 2 | `Proxy address` field | Sets the proxy server address as an IP address or FQDN |
| 3 | `Proxy port` field | Selection of the proxy listening port (1-65535) |
| 4 | `SAVE` button | Stores the current settings |

For implementation, see the *Configuring a proxy* procedure.

---

#### 5.3.13.2.3 SSL settings screen

This section enables viewing of the Secure Socket Layer (SSL) certificate used and the use of a customised certificate for the GBox.
The certificate generated attests to the identity of the GBox and enables encrypting the exchanged data.
After clicking on the `SSL` button, the next screen is displayed:



GBOX-CONF-04

The screen consists of areas:

- *`In use certificate details` area* (2)

- *`Custom Certificate` area* (1)
- *`Alternative available certificate details` area* (10)

For implementation, see the *Installing an SSL certificate* procedure.

---

### `In use certificate details` area

This area (2) enables obtaining information about the certificate in use.
This area includes the following items:

| Item | Name | Function |
|---|---|---|
| 2 | `In use certificate details` field | Displays information about the certificate. The validity of this certificate is specified |
| 19 | `Serial number` field | Unique serial number assigned by the certifying authority that issued the certificate |
| 18 | `Signature algorithm` field | Certificate signing algorithm (sha256WithRSAEncryption for example) |
| 17 | `Issuer` field | Certificate issuer |
| 16 | `Not valid before` field | Validity start date |
| 15 | `Not valid after` field | Validity end date |
| 14 | `Subject` field | The subject, or domain, for which the certificate is issued |
| 13 | `Public key algorithm` field | Lists identifiers that have been revoked, invalidated, or are no longer trustworthy. |
| 12 | `Public key length` field | Length of the public key (2048bits for example) |
| 11 | `Type` field | Type |

---

### `Custom Certificate` area

The area (1) enables a specific certificate to be used.
To do this, simply load the private key and the certificate in PEM format.
The `Custom Certificate` area contains the following items:

| Item | Name | Function |
|---|---|---|
| 3 | `Enable Custom Certificate` selector | If active then select a custom certificate (alternative)<br>If not active then selection of current certificate (in use) |
| 4 | `KEY FILE` button | Selecting the private key to be used |
| 5 | `CERT FILE` field | Selection of the certificate related to the private key |
| 7 | `Save` button | Stores the current settings |

---

**`Alternative available certificate details` area**

The area (1) eanbles the using of another certificat.
To do this, simply load the private key and the certificate in PEM format.
The `Alternative available certificate details` area contains the information of the alternative certificat.

---

### 5.3.14 Current account management, member of the Administrators Group

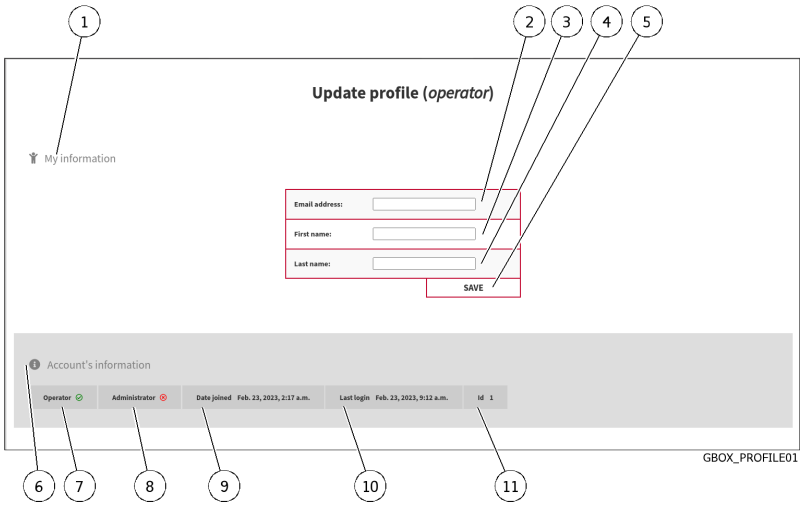

After pressing the current account management button (4), three commands are available:

- The `Edit profile` command: see the *`Update profile` screen*
- The `Change password` command: see the *`Change Password` screen*
- The `Logout` command: see the *Logout command*

---

#### 5.3.14.1 `Update profile` screen

After clicking on the `Edit profile` command, the `Update profile` screen is displayed:

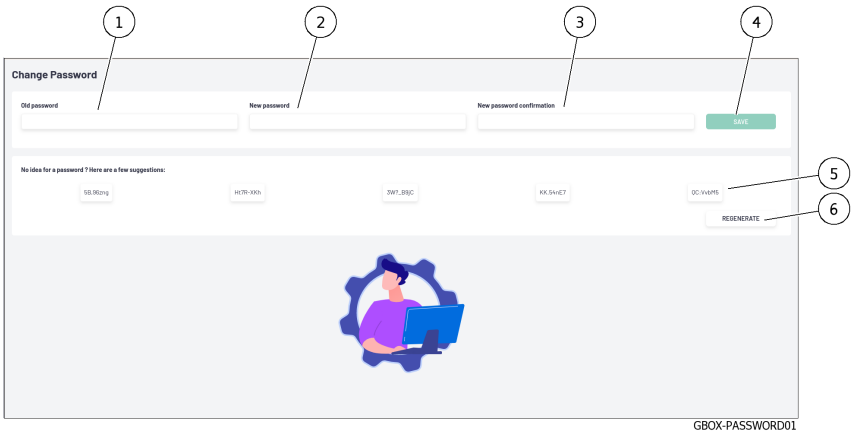


| Marker | Name | Description |
|---|---|---|
| 1 | `My information` | Area listing current account details |
| 2 | `Email address` | Current user's email address |
| 3 | `First name` | Current user's first name |
| 4 | `Last name` | Current user's Last name |
| 5 | `SAVE` | Button for saving entries. |
| 6 | `Account's information` | Area listing current account management information |
| 7 | `Operator` | Membership in the Operator group - a tick indicates membership, a cross indicates non-membership |
| 8 | `Administrator` | Membership in the Administrator group - a tick indicates membership, a cross indicates non-membership |
| 9 | `Date joined` | Date and time the current account was created |
| 10 | `Last login` | Date and time of last current account login |
| 11 | `ID` | Account identification number |

For implementation, see the *Changing some of the current user's information* procedure.

#### 5.3.14.2 `Change Password` screen

After clicking on the `Change password` command, the `Change Password` screen is displayed:




This screen enables changing the password for the current account.
This password policy is described in paragraph *Password management policy*.

| Marker | Name | Description |
|---|---|---|
| 1 | `Old password` | Old password entry box |
| 2 | `New password` | New password input box |
| 3 | `New password confirmation` | New password confirmation input box |
| 4 | `SAVE` | Button for saving entries. |
| 5 | `No idea for a password ?` `Here are a few suggestions` | Five passwords to choose from |
| 6 | `REGENERATE` | Button for regenerating new passwords |

For implementation, see the *Changing the current account password* procedure.

#### 5.3.14.3 Logout command

After clicking on the `Logout` command, the current user is immediately logged out.
The login screen is displayed.
For implementation, see the *Logging out of the GBox web interface* procedure.

## 5.4 API graphical interface

### 5.4.1 Overview of the API GBOX interface

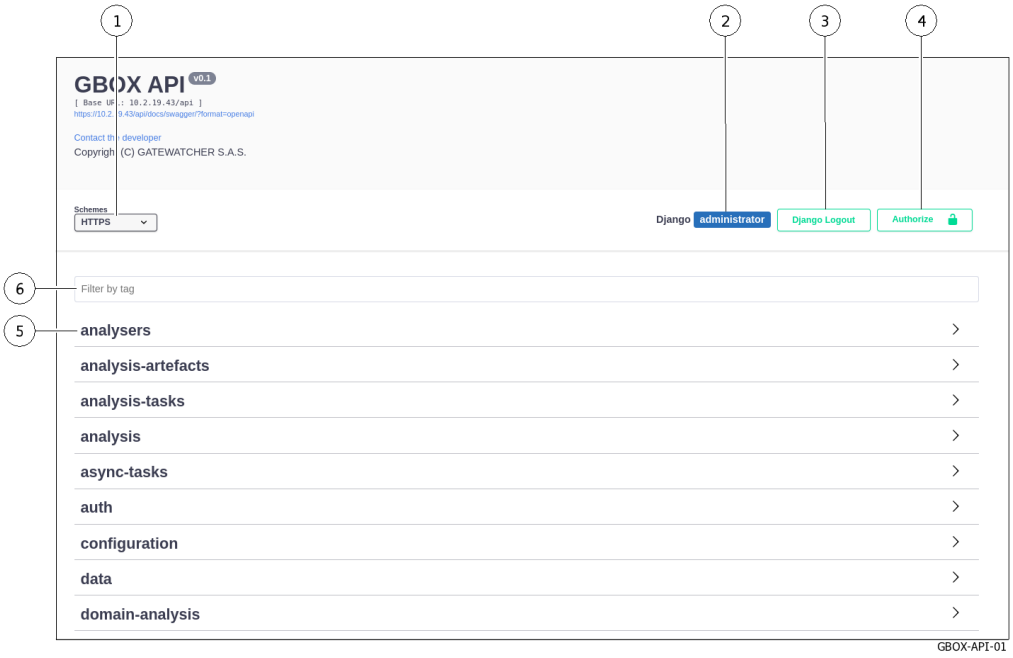
The API interface enables:

- Displaying a list of existing endpoints by theme
- Filtering of this list
- Finding out all the information about each endpoint
- running the endpoint
- Finding out its curl command
- Finding out its URL request

**Note:**

The GBox API graphical interface is called swagger.

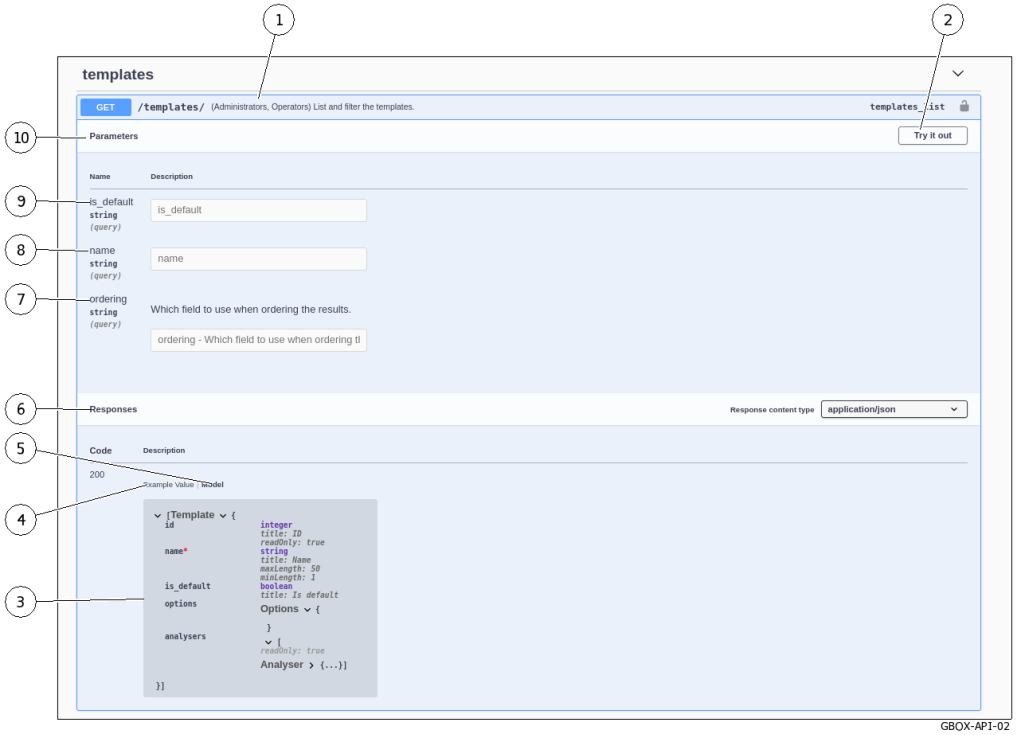
After pressing the `API` button on the title bar, the following screen is displayed.
The window includes:



| Item | Description |
|---|---|
| 1 | `Schemes`: setting indicating the protocol used (HTTPS) |
| 2 | Current account name: here administrator account |
| 3 | `Django Logout` button: enables exiting the API graphical interface |
| 4 | `Authorize` button: enables setting the authentication required in curl commands |
| 5 | Endpoints are sorted by theme (tag) |
| 6 | Filter field: enables the filtering of themes |

#### 5.4.1.1 Detail for an endpoint

The information displayed for an endpoint is as follows:



| Item | Description |
|---|---|
| 1 | Title line. It includes the action (here GET), the name of the endpoint (here /template), the accesses (here Administrators and Operators), the description of the endpoint |
| 2 | `` `Try it out` `` button: executes the endpoint with the current parameters |
| 10 | `` `Parameters` `` field: displays the optional or mandatory settings for executing the query. To find out which parameters are mandatory, refer to zone (6).<br>This zone includes: |
| 9 | • `` `is_default` `` parameter: enables the default template to be selected. The `` `true` `` setting must be entered. |
| 8 | • The `` `name` `` parameter: defines the name of the template from which information is to be retrieved.<br>Look in the `` `Model` `` window for the type (here string) and whether the parameter is mandatory (here * = mandatory). |
| 7 | • `` `ordering` `` field: enter the name of the field used to order the response. |
| 6 | `` `Responses` `` zone: this zone displays information depending on whether or not the `` `Try it out` `` button has been enabled. |

**Note:**

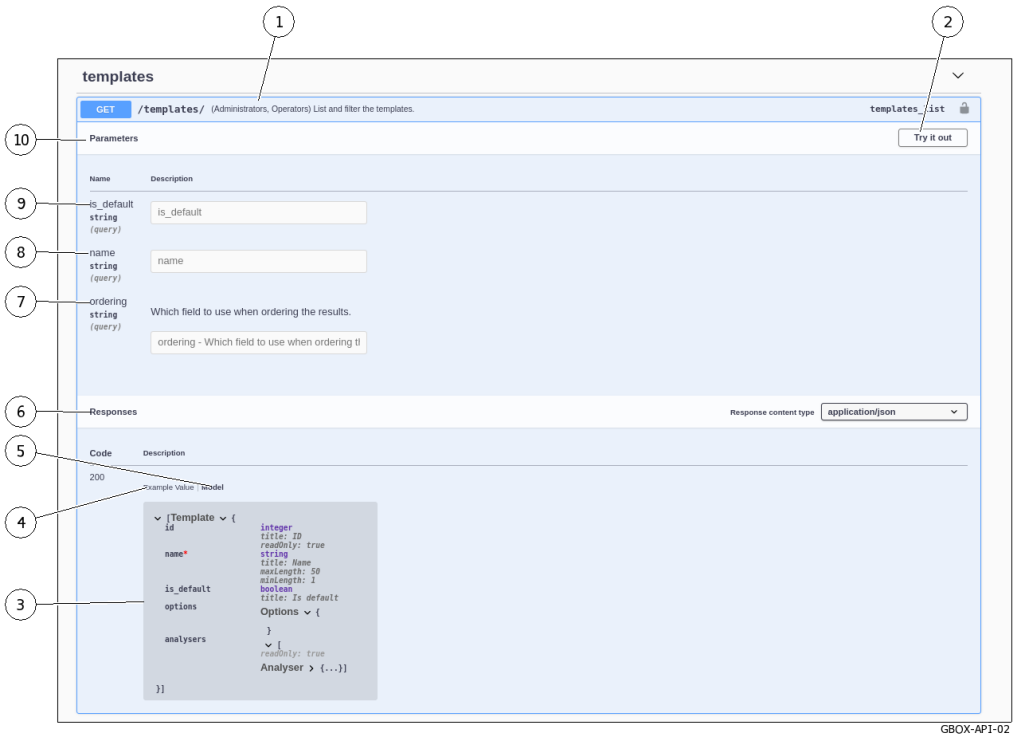
If a parameter is mandatory, an asterisk with `` `required` `` is displayed.

**Note:**

Parameters cannot be entered on this screen. To do this, the query must be executed.

#### 5.4.1.1.1 `Responses` field if the `Try it out` button is not enabled.

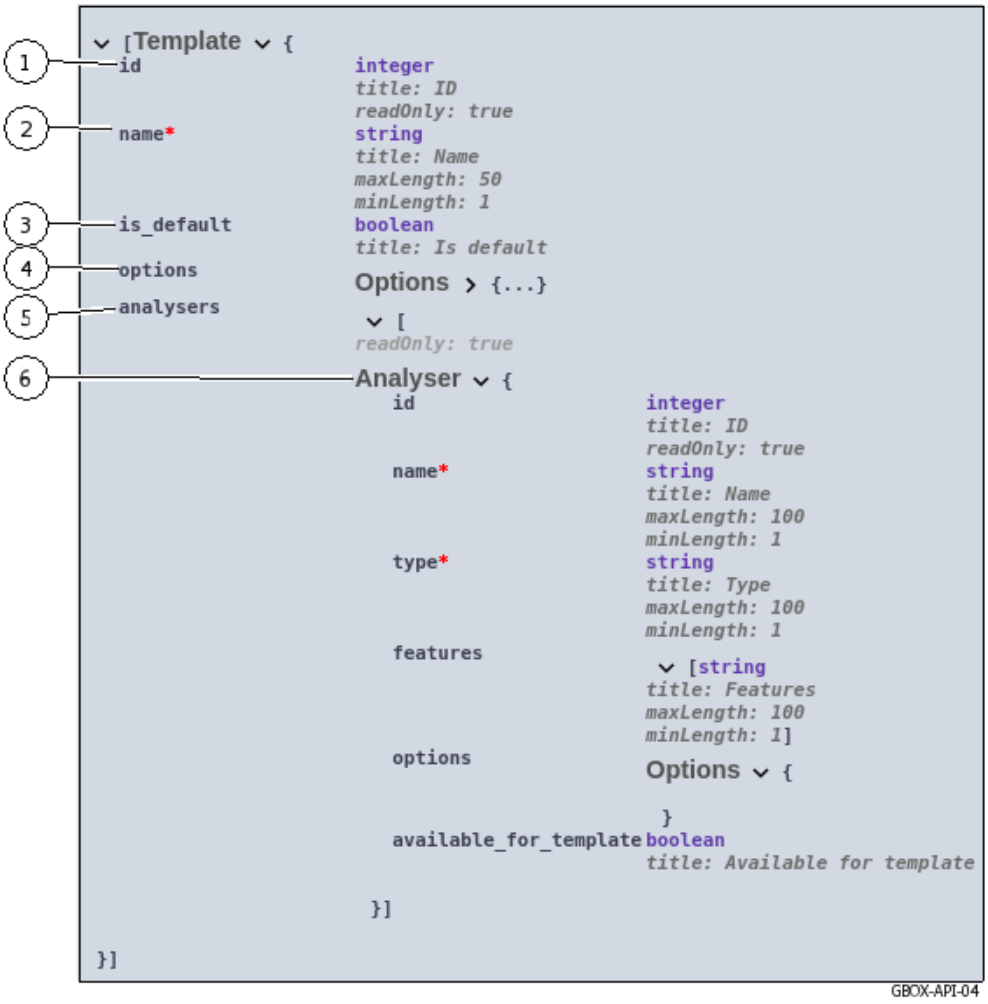
If the `Try it out` button is not enabled, then the `Responses` zone contains information about the expected response:




| Item | Description |
|---|---|
| 5 | `Template` link: by clicking on this text, the window (3) displays the template for the expected response. |
| 4 | `Example Value` link: by clicking on this text, the window (3) displays an example of the expected response with example values.<br>The values are for the **integer** type (value 0), for the string type (value = string), for the **boolean** type (value = true). |
| 3 | View field: contains the content selected by the active option (4) or (5).<br>An example of the content is shown below. |

### Example of an output template

The output template provides the structure of the data that will be displayed as output, i.e. after the query is executed.




| Item | Description |
|---|---|
| 1 | `id`: template number. For this parameter, its characteristics are indicated (type, title, etc.). |
| 2 | `name`: template name. For this parameter, its characteristics are indicated (type, title, length. etc.). |
| 3 | `is_default`: field defines whether the current template is the default template. The response is a Boolean (true/false value). |
| 4 | `options`: field defining possible options. |
| 5 | `analysers`: field defining the information for all the engines. |
| 6 | `Analyser`: field defining information for a single engine. |

#### 5.4.1.1.2 Example with default values

In this example, the information is displayed with the following default values:

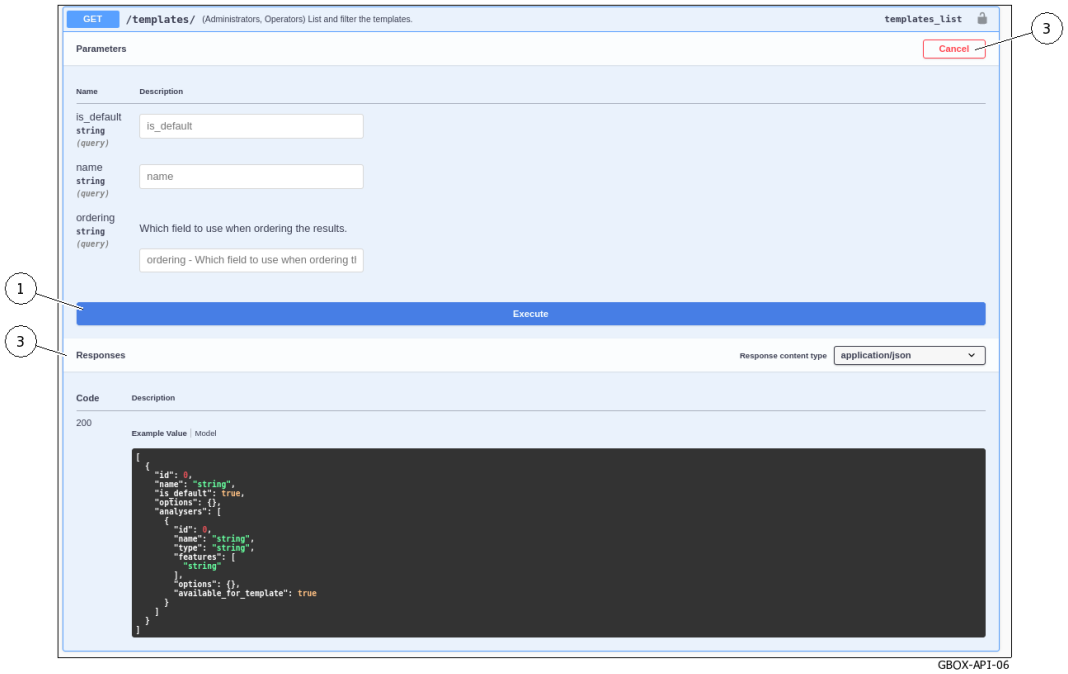
- **integer** parameters are displayed with the number `0`.
- **string** parameters are displayed with the text `string`.
- **boolean** parameters are displayed with the text `true`.


The marking is the same as in the output template.

---

#### 5.4.1.1.3 `Responses` field if the `Try it out` button is enabled.

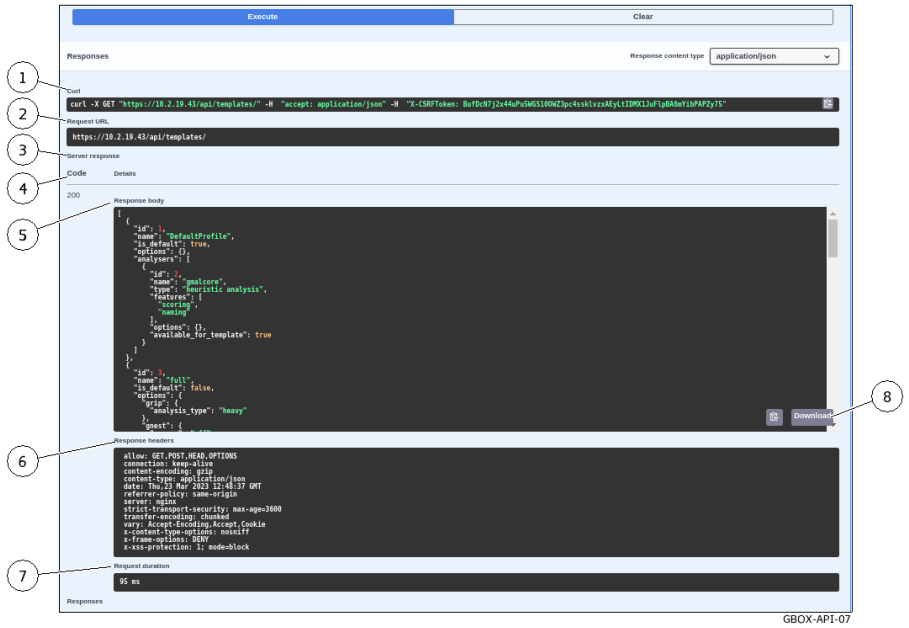
Once the `Try it out` button is clicked, the parameter input area is activated.
The following screen is displayed:




GBOX-API-06

| Item | Description |
|---|---|
| 1 | `Execute` button: enables the request to be executed with the current parameters |
| 2 | `Cancel` button: aborts the query |
| 3 | The `Responses` zone has not changed |

After clicking on the `Execute` button, the query is started and the following window is displayed.




GBOX-API-07

| Item | Description |
|---|---|
| 1 | `Clear` button: enables returning to the status before execution |
| 2 | `Curl` display area: displays the Curl request |
| 3 | `URL` display area: displays the URL request |
| 4 | `Code`: If code 200 then execution ok. If the message `code 400 Undocumented Error Bad Request` is displayed, check whether the mandatory parameters have been entered correctly. |
| 6 | `id 1`: template number 1 |
| 7 | `Name gmalcore` : engine id 2 Gmalcore |
| 8 | id 3: template number 3 |
| 9 | `Responses headers`: area describing the response header |
| 10 | `Request duration`: value in ms of the request duration |

### 5.4.2 Endpoint list

**Note:**

In the table below the legend is:

- Ope: Operator role
- Adm: Administrator role
- WAuth: Without Authentication
- AUser: Authenticated User

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| Analysers | /analysers/ | GET | Ope, Adm | List and filter the analysers |
| Analysers | /analysers/{name}/ | GET | Adm | Retrieve an analyser |
| Analysers | /analysers/{name}/proxy/ | POST | Adm | Proxy a request to an analyser |
| Analysers | /analysers/{name}/status/ | GET | Adm | Return an analyser status |
| Analysis-artefacts | /analysis-artefacts/ | GET | Ope | List and filter the analysis artefacts |
| Analysis-artefacts | /analysis-artefacts/{id}/ | GET | Ope | Retrieve an analysis artefact info. |
| Analysis-artefacts | /analysis-artefacts/{id}/ | DELETE | Ope | Remove an analysis artefact |
| Analysis-artefacts | /analysis-artefacts/{id}/download/ | GET | Ope | Download an analysis artefact |
| Analysis-tasks | /analysis-tasks/ | GET | Adm | List and filter the analysis tasks |
| Analysis-tasks | /analysis-tasks/{id}/ | GET | Adm | Retrieve an analyse task |
| Analysis | /analysis/ | GET | Ope | List and filter the analyses |
| Analysis | /analysis/submit/ | POST | Ope | Submit a file for a new analysis |
| Analysis | /analysis/{id}/ | GET | Ope | Retrieve an analysis |
| Analysis | /analysis/{id}/behavior-data/ | GET | Ope | Retrieve the behavior data stored for this analysis |
| Analysis | /analysis/{id}/download-artefacts/ | GET | Ope | Download the analysis artefact(s) as a zip file. |
| Analysis | /analysis/{id}/download-pdf/ | GET | Ope | Download the analysis pdf report |
| Analysis | /analysis/{id}/download-sample/ | GET | Ope | Download the sample uploaded for the analysis as an encrypted zip file |
| Analysis | /analysis/{id}/retry/ | POST | Ope | Retry the analysis with the given template |

suite sur la page suivante

Table 4 – suite de la page précédente

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| Analysis | /analysis/{id}/threat-chart/ | GET | Ope | Generate the threat radar chart for the analysis |
| async-tasks | /async-tasks/ | GET | Adm | List and filter the async tasks |
| async-tasks | /async-tasks/{id}/ | GET | Adm | Retrieve an async task |
| async-tasks | /async-tasks/{id}/ | DELETE | Adm | Remove an async task. Use with caution if the task is not finished |
| auth | /auth/login/ | POST | WAuth | Get the user time limited session token through its username & password |
| auth | /auth/logout/ | POST | WAuth | Logout current user |
| auth | /auth/tokens/ | GET | Adm | List and filter the api tokens |
| auth | /auth/tokens/ | POST | Adm | Create an api token |
| auth | /auth/tokens/purge-tokens/ | POST | Adm | Remove the expired tokens |
| auth | /auth/tokens/{id}/ | DELETE | Adm | Remove an api token |
| configuration | /configuration/license | GET | Adm | Get the product licence. |
| configuration | /configuration/license | PUT | Ope, Adm | Update the product licence. |
| configuration | /configuration/proxy/ | GET | Adm | Get the proxy configuration. |
| configuration | /configuration/proxy/ | PUT | Adm | Update the proxy configuration |
| data | /data/purge-samples/ | POST | Adm | Remove the clean samples, analysis data, and related analysis artefacts |
| domain-analysis | /domain-analysis/ | POST | Ope | Request a new domain analysis to gdgadetect analyser |
| gum | /gum/config/ | GET | Adm | Change the Gum auto-update configuration |
| gum | /gum/hotfix/ | POST | Adm | Upload and apply a hotfix |
| gum | /gum/hotfix/status/ | GET | Adm | Retrieve the hotfix status |
| gum | /gum/update/ | POST | Adm | Upload and apply an update |
| gum | /gum/update/status/ | GET | Adm | Retrieve the update status |
| gum | /gum/upgrade/ | GET | Adm | List the uploaded upgrade files that have not been applied yet |
| gum | /gum/upgrade/ | POST | Adm | Upload and apply an upgrade |
| gum | /gum/upgrade/apply/ | POST | Adm | Apply an already uploaded upgrade |
| gum | /gum/upgrade/status/ | GET | Adm | Retrieve the upgrade status |
| gum | /gum/upgrade/upload/ | POST | Adm | Upload an upgrade to apply it later |
| logs | /logs/download/ | GET | Adm | Download the last log export |
| logs | /logs/export/ | GET | Adm | Request to export the app logs |
| logs | /logs/status/ | GET | Adm | Get the last log export status |
| ssl-settings | /ssl-settings/certificates/ | GET | Adm | Remove the custom SSL certificate if it does exist |
| ssl-settings | /ssl-settings/certificates/ | POST | Adm | Update the custom SSL certificate if provided and enable it or not |
| ssl-settings | /ssl-settings/certificates/ | DELETE | Adm | Remove the custom SSL certificate if it does exist |
| status | /status/ | GET | WAuth | Status endpoint to check if api is up |
| status | /status/user/ | GET | WAuth | User status endpoint to check if the user is authenticated |
| templates | /templates/ | GET | Ope, Adm | List and filter the templates |
| templates | /templates/ | POST | Adm | Create a template |
| templates | /templates/{id}/ | GET | Ope, Adm | Retrieve a template |
| templates | /templates/{id}/ | PUT | Adm | Update a template |
| templates | /templates/{id}/ | DELETE | Adm | Remove a template. |

suite sur la page suivante

Table 4 – suite de la page précédente

| Theme | Name | Verb | Role | Description |
|---|---|---|---|---|
| users-history | /users-history/authentication/ | GET | Adm | List and filter the user authentication history |
| users-history | /users-history/authentication/{id}/ | GET | Adm | Retrieve a user authentication history |
| users-history | /users-history/creation-deletion/ | GET | Adm | List and filter the user creation / deletion history |
| users-history | /users-history/creation-deletion/{id}/ | GET | Adm | Retrieve a user creation / deletion history |
| users-history | /users-history/permission/ | GET | Adm | List and filter the user permission history |
| users-history | /users-history/permission/{id}/ | GET | Adm | Retrieve a user permission history |
| users | /users/ | GET | Adm | List and filter the users |
| users | /users/ | POST | Adm | Create a user |
| users | /users/me/ | GET | AUser | Retrieve the current user |
| users | /users/me/ | PUT | AUser | Update the current user |
| users | /users/me/password-suggestions/ | GET | AUser | Get password suggestions randomly generated |
| users | /users/me/password/ | PUT | AUser | Set the user password |
| users | /users/me/reset-password/ | POST | AUser | Reset the current user password and return the new one |
| users | /users/{id}/ | GET | Adm | Retrieve a user |
| users | /users/{id}/ | PUT | Adm | Update a user |
| users | /users/{id}/ | DELETE | Adm | Remove a user |
| users | /users/{id}/reset-password/ | POST | Adm | Reset a user password and return the new one |

# Chapter 6

# Use cases

## 6.1 Introduction

Using the GBox is illustrated by a list of use cases for the various types of user.

---

### 6.1.1 Use case: member of the Operators group

To use the GBox, it is necessary to access the WEB interface with an account that is a member of the **Operators** group.
The tables provided in the *How to use the GBox: Operators level* section allow an overview of the most common procedures.

---

### 6.1.2 Configuration case: setup account

For an initial configuration of the GBox and to carry out advanced configurations or checks, it is necessary to enter the configuration interface under the **setup** account.
The tables provided in the *How to administer the GBox: setup or Administrators level* section allow an overview of the most common administration procedures.

---

### 6.1.3 Administration case: member of the Administrators group

To administer the GBox, it is necessary to access the WEB interface with an account that is a member of the **Administrators** group.
The tables provided in the *How to administer the GBox: setup or Administrators level* section allow an overview of the most common procedures.

---

## 6.2 How to connect to the GBox

Access is possible:

- Either via a *Direct connection to the server*
- Either via a *Remote HTTP connection via iDRAC (iDRAC on a DELL server)*
- Either via a *Remote connection to the configuration menu using SSH via the iDRAC interface in serial port forwarding mode*
- Either via a *Remote connection to the configuration menu using SSH*
- Either via a *Connection via a web browser*

The configuration menu for managing the GBox can be accessed remotely via an SSH or HTTP connection.

**Note:**

The list of physical connectors required is described in *Overview of the GBox*.

---

### 6.2.1 Direct connection to the server

The first connection can be made via a direct login with keyboard and screen.
This is necessary if the network configuration is not yet completed or if the network address is not known.
This connection is not the nominal way of accessing the equipment, although it does enable the iDRAC's network connection to be configured, among other things.
Subsequent accesses will generally be made remotely.

**Note:**

The default login and password are provided in the server manufacturer's documentation.

For specific implementation of the **setup** account, please refer to *Direct connection to the configuration menu with a keyboard and monitor*.

---

### 6.2.2 Remote HTTP connection via iDRAC (iDRAC on a DELL server)

Remote access is achieved by using:

- The network connection to the iDRAC port
- A Web browser

This access requires:

- Knowledge of the iDRAC login name and password (iDRAC access)
- The network configuration is complete (IP address of the iDRAC is known)

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 in console mode

This connection is not the standard way of accessing the equipment, although it does enable access in the event of problems.
Access to advanced features (console access..) requires the purchase of a specific license.
For more information, please contact support or a Gatewatcher sales manager. .. sav2_en|

For specific implementation of the **setup** account, please refer to *HTTP access to the configuration menu via iDRAC (DELL server)*.

---

### 6.2.3 Remote connection to the configuration menu using SSH via the iDRAC interface in serial port forwarding mode

Remote access is achieved by using:

- The network connection to the iDRAC port
- A connection tool via SSH

This access requires:

- Knowledge of the iDRAC login name and password (iDRAC access)
- The network configuration is complete (IP address of the iDRAC is known)

From the interface, it is possible to:

- View the operating system messages
- Connect to the GBox via the console

This connection is not the standard way of accessing the equipment, although it does enable access in the event of problems.

For specific implementation of the **setup** account, please refer to *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*.

---

### 6.2.4 Remote connection to the configuration menu using SSH

Remote access from an external computer to the device is achieved securely using an SSH tunnel.
This connection is the nominal way of accessing the equipment configuration menu.

For specific implementation of the **setup** account, please refer to *SSH access to the configuration menu*.

---

### 6.2.5 Connection via a web browser

Remote access from an external computer to the equipment is via a web browser.
This connection is the standard way of accessing the equipment's Web interface.
For implementation, refer to *Connection to the web interface via a browser*.

---

## 6.3 How to connect to GCenter

Remote access to the GCenter is via a web browser in order to link the GCenter and the GBox.
For more information, please refer to the GCenter documentation.

---

## 6.4 How to use the GBox: Operators level

### 6.4.1 Accessing the GBox

| To perform the following task | # | Carry out the following procedures in succession | Reserved for the group |
|---|---|---|---|
| Connection to GBox via a web browser | 1 | *Connection to the web interface via a browser* | All accounts |

---

### 6.4.2 Analysing a file

| To perform the following task | Carry out the following procedures in succession | |
|---|---|---|
| Quick procedure for analysing a file | 1 | *Quick procedure for analysing a file* |
| | 2 | *Procedure to analyse the contents of a report* |
| Quick procedure for analysing a domain | 1 | *Quick procedure for analysing a domain* |
| | 2 | *Procedure to analyse the contents of a report* |
| Procedure for analysing a file in the `New analysis` screen | 1 | *Procedure for analysing a file in the `New analysis` screen* |
| | 2 | *Procedure to analyse the contents of a report* |
| Procedure for analysing reports on the Reports page | 1 | *Procedure to analyse the list of reports on the `Reports` page* |

---

### 6.4.3 Managing the current account

| To perform the following task | Carry out the following procedures in succession | |
|---|---|---|
| Changing the current account password | 1 | *Changing the current account password* |
| Changing some of a current user's information | 1 | *Changing some of the current user's information* |

## 6.5 How to administer the GBox: setup or Administrators level

### 6.5.1 Accessing the GBox

| To perform the following task | # | Carry out the following procedures in succession | Reserved for the group |
|---|---|---|---|
| First connection by a direct connection | 1 | *Direct connection to the configuration menu with a keyboard and monitor* | setup |
| Remote HTTP connection via iDRAC | 1 | *HTTP access to the configuration menu via iDRAC (DELL server)* | setup |
| Remote connection to the configuration menu using SSH via the iDRAC interface | 1 | *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode* | setup |
| Direct connection to the configuration menu using SSH | 1 | *SSH access to the configuration menu* | setup |
| Connection to GBox via a web browser | 1 | *Connection to the web interface via a browser* | All accounts |

### 6.5.2 Configuring the GBOX

| To perform the following task | Carry out the following procedures in succession | |
|---|---|---|
| Initial installation | 1 | Procedure in *Configuring the GBox for the first connection* |
| | 2 | Procedure in *Operating a GBox* |
| Keyboard configuration | 1 | Use of the *`Keymap` command* |
| Changing the licence | 1 | Procedure in *Modifying the licence* |
| Putting a GBox into operation | 1 | Procedure in *Operating a GBox* |
| Changing the SSL certificate | 1 | Procedure in *Installing an SSL certificate* |

### 6.5.3 Managing Web UI accounts

| To perform the following task | Carry out the following procedures in succession | |
|---|---|---|
| Creating a local user | 1 | *Creating local users* |
| Changing some of a local user's information | 1 | *Changing some of a local user's information* |
| Changing the current account password | 1 | *Changing the current account password* |
| Resetting a local user's password | 1 | *Resetting a user's password* |
| Deleting a local user | 1 | *Deleting a user* |
| Viewing the authentication history | 1 | *Viewing the authentication history* |
| Viewing the history of user creations or deletions | 1 | *Viewing the history of user creations or deletions* |
| Viewing the history function for all changes in user rights | 1 | *Viewing the history function for all changes in user rights* |

### 6.5.4 Managing the account setup from the configuration menu

| To perform the following task | Carry out the following procedures in succession | |
|---|---|---|
| Changing the setup account password | 1 | *SSH access to the configuration menu* |
| | 2 | Use the command *`Password` command* |

### 6.5.5 Managing network

| To perform the following task | Carry out the following procedures in succession | |
|---|---|---|
| Viewing the current configuration of the GBox | 1 | *Procedure to access the `Network Setup` submenu* |
| | 2 | *Procedure for viewing the current configuration* |
| Viewing the configuration of each network interface | 1 | *Procedure to access the `Network Setup` submenu* |
| | 2 | *Procedure for viewing the network interface status* |
| Modifying the general parameters of the GBox | 1 | *Procedure to access the `Network Setup` submenu* |
| | 2 | *Procedure for changing the GBox's general parameters* |
| Managing the interface parameters GBx0 management network | 1 | *Procedure to access the `Network Setup` submenu* |
| | 2 | Apply the *Procedure for modifying the network interface parameters* for the GBx1 interface |
| | 3 | *Procedure for taking modifications into account* |
| GBx1 network interface configuration of Gnest virtual machines to the Internet | 1 | *Procedure for accessing the `Services` menu* |
| | 2 | *Procedure for accessing the Sandbox services of the Gnest engine* |
| | 3 | *Procedure for enabling the Internet connection* |
| | 4 | *Procedure to access the `Network Setup` submenu* |
| | 5 | Apply the *Procedure for modifying the network interface parameters* for the GBx1 interface |
| | 6 | *Procedure for taking modifications into account* |
| | 7 | Enable the `Network` option in the Gnest settings in the Malware templates: to do this, refer to *Procedure for changing the existing template* |

### 6.5.6 Managing the analysis engines

| To perform the following task | Carry out the following procedures in succession | |
|---|---|---|
| Configuring the Gnest engine (changing the number of virtual machines) | 1 | *Procedure to configure the Gnest engine* |
| | 2 | Modification of existing templates to take account of this new configuration: *Procedure to configure the Gnest engine* |
| Configuring the Gmalcore engine | 1 | *Procédure to configure the Gmalcore engine* |
| | 2 | Modification of existing templates to take account of this new configuration: *Procédure to configure the Gmalcore engine* |
| Monitoring of analysis engines | 1 | *Procedure to analyse the engines monitoring* |

---

### 6.5.7 Managing the GBox server

| To perform the following task | # | Carry out the following procedures in succession |
|---|---|---|
| Exit the current session or leave the SSH session | 1 | Use the *`Exit` command* |
| System: restart the GBox | 1 | Use the *`Restart` command* |
| System: shut down the GBox | 1 | Use the *`Shutdown` command* |
| Delete the data and return the GBox to its factory settings. | 1 | Use the *`Reset` command* |
| Malcore services: force restart or reinstallation | 1 | Use the *`Services` command* |
| Restart the applications | 1 | Use the *`Gapps` command* |

---

### 6.5.8 Managing the analysis templates

| To perform the following task | # | Carry out the following procedures in succession |
|---|---|---|
| Create new templates | 1 | *Creating an analysis template* |
| Managing templates | 1 | *Managing the analysis templates* |

---

### 6.5.9 Monitoring the GBox

| To perform the following task | # | Carry out the following procedures in succession |
|---|---|---|
| Monitoring: loading files for diagnosis | 1 | *Generating and loading files for diagnosis* |

---

### 6.5.10 Using the API

| To perform the following task | # | Carry out the following procedures in succession |
|---|---|---|
| Connection to the Wef interface via a browser | 1 | *Connection to the web interface via a browser* |
| Creation or deletion of an API access token | 1 | *Creating or deleting an API access token* |
| Use of an API endpoint | 1 | *Using an API endpoint* |

### 6.5.11 Managing the software via GUM

| To perform the following task | Carry out the following procedures in succession | |
|---|---|---|
| Updating engines | 1 | If necessary, configure the proxy (local mode): see the procedure in *Configuring a proxy* |
| | 2 | Depending on the method (local or online), apply the corresponding procedure *Configuring automatic updates via GUM* |
| | 3 | Check that the update is working correctly with *Manual installation of a signature update* |
| Installing a patch (Hotfix) | 1 | *Installing a hotfix patch* |
| Installing an upgrade | 1 | *Installing an upgrade* |

# Chapter 7

# use case : setup account

## 7.1 Direct connection to the configuration menu with a keyboard and monitor

### 7.1.1 Introduction

The first connection can be made via a direct login with keyboard and screen.
This is necessary if the network configuration is not yet completed or if the network address is not known.
This connection is not the nominal way of accessing the equipment, although it does enable the iDRAC's network connection to be configured, among other things.
Subsequent accesses will generally be made remotely.

**Note:**

The default login and password are provided in the server manufacturer's documentation.

---

### 7.1.2 Preliminary operations

- Connect the power cables.
- Connect the network cables (see *Overview of the GBox*).

---

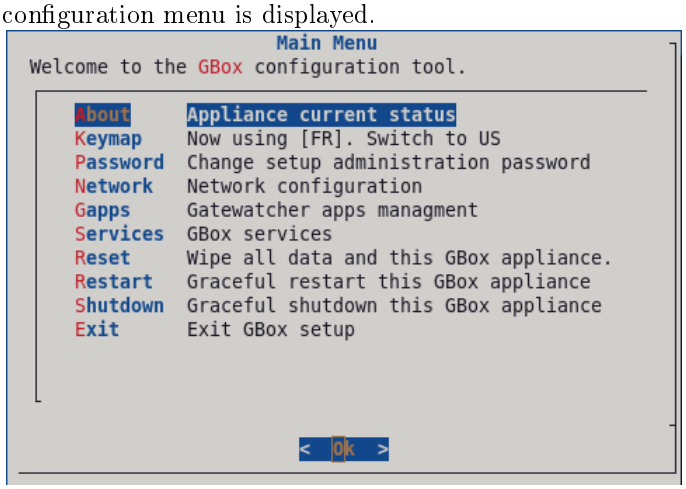
### 7.1.3 Procedure for connecting the monitor and keyboard

- Connect the monitor to the VGA connector.
- Connect the keyboard to one of the USB connectors.
- Switch on the server.

---

### 7.1.4 Procedure for finding 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.
  The configuration menu is displayed.




**Note:**

Press the first letter of a command for quick access.
Press the `OK` button to confirm the selected choice.

---

## 7.2 HTTP access to the configuration menu via iDRAC (DELL server)

### 7.2.1 Introduction

Remote access is achieved by using:

- The network connection to the iDRAC port
- A Web browser

This access requires:

- Knowledge of the iDRAC login name and password (iDRAC access)
- The network configuration is complete (IP address of the iDRAC is known)

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 in console mode

This connection is not the standard way of accessing the equipment, although it does enable access in the event of problems.
Access to advanced features (console access..) requires the purchase of a specific license.
For more information, please contact support or a Gatewatcher sales manager. .. sav2_en|

---

### 7.2.2 Preliminary operations

- Configure the iDRAC network (refer to the procedure *Direct connection to the configuration menu with a keyboard and monitor*).

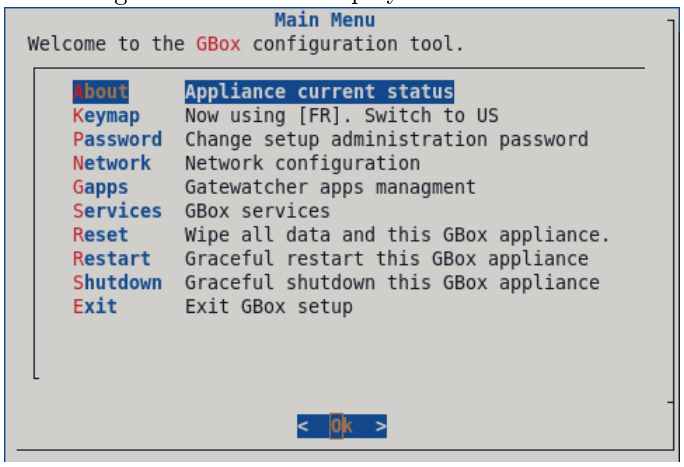
---

### 7.2.3 Procedure

- On the remote computer, open a web browser.
- Enter URL: https://iDRAC-IP-address

> **Note:**
> iDRAC-IP-address is the IP address of the iDRAC interface on the GBox .

- Validate.
  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 equipment.
  The configuration menu is displayed.



**Note:**

Press the first letter of a command for quick access.
Press the `OK` button to confirm the selected choice.

---

## 7.3 SSH access to the configuration menu via the iDRAC interface in serial port redirection mode

### 7.3.1 Introduction

Remote access is achieved by using:

- The network connection to the iDRAC port
- A connection tool via SSH

This access requires:

- Knowledge of the iDRAC login name and password (iDRAC access)
- The network configuration is complete (IP address of the iDRAC is known)

From the interface, it is possible to:

- View the operating system messages
- Connect to the GBox via the console

This connection is not the standard way of accessing the equipment, although it does enable access in the event of problems.

---

### 7.3.2 Preliminary operations

- Configure the iDRAC network (refer to *Direct connection to the configuration menu with a keyboard and monitor*).

---

### 7.3.3 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 iDRAC port
- Validate the command.
- Enter the password of the entered login.
- Press `Enter`.
- Enter the following command `racadm>>console com2`.
- Validate.
  The system now displays the graphical interface of the device.

---

### 7.3.4 Procedure on the remote PC running Windows

- Open an SSH client software, such as Putty.
- Enter the IP address of iDRAC's interface and confirm.
- Enter the following command `racadm>>console com2`.
- Validate.
  The system now displays the graphical interface of the device.

---

## 7.4 SSH access to the configuration menu

### 7.4.1 Introduction

Remote access from an external computer to the device is achieved securely using an SSH tunnel.
This connection is the nominal way of accessing the equipment configuration menu.

---

### 7.4.2 Preliminary operations

- Make an initial connection (see *Direct connection to the configuration menu with a keyboard and monitor*).
- Know the name of the GBox or its IP address.

---

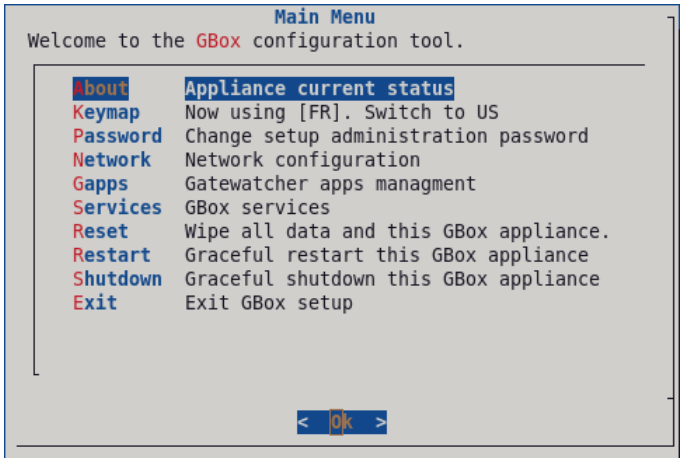
### 7.4.3 Procedure on the remote PC running Linux

- Open a command prompt.
- Enter the command `ssh identifiant@adresse_ip_GBox` or `ssh identifiant@FQDN_GBox`.
  For example, `ssh setup@gGBox` where:
  - The identifier is `setup` and
  - The FQDN is `GBox`
- Validate the command.
- Enter the password.

---

### 7.4.4 Procedure on the remote PC running Windows

- Open an SSH client software, such as Putty.
- Enter the IP address of GBox's interface and confirm.
- Enter the login and password.
  The configuration menu is displayed.




**Note:**

Press the first letter of a command for quick access.
Press the `OK` button to confirm the selected choice.

---

## 7.5 `About` command

### 7.5.1 Introduction

The `About` command displays the following information:

- `GBox Name` : name of the GBox
- `Version` : version of the software
- `IP Address` : IP address of the active network interface
- `Subnet Mask` : subnet mask of the active network interface
- `Default Gateway` : gateway by default

---

### 7.5.2 Prerequisites

- User : setup

---

### 7.5.3 Preliminary operations

Depending on the situation:

- either use the *SSH access to the configuration menu*
- either use the *Direct connection to the configuration menu with a keyboard and monitor*
- either use the *HTTP access to the configuration menu via iDRAC (DELL server)*
- either use the *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*

---

### 7.5.4 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, showing the GBox information.

```
GBox Name         : nom de la Gbox
Version           : version du logiciel
IP Address        : 192.168.1.1
Subnet Mask       : 255.255.255.0
Default Gateway   : 192.168.1.254
```

**Note:**

The information displayed is just an example.

- Press the `OK` key to return to the menu.

---

## 7.6 `Keymap` command

### 7.6.1 Introduction

The `Keymap` command enables switching the keyboard language between US and FR.

---

### 7.6.2 Prerequisites

- User : setup

---

### 7.6.3 Preliminary operations

Depending on the situation:

- either use the *SSH access to the configuration menu*
- either use the *Direct connection to the configuration menu with a keyboard and monitor*
- either use the *HTTP access to the configuration menu via iDRAC (DELL server)*
- either use the *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*

---

### 7.6.4 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 `Keymap` line shows: `Now using [US]. Switch to FR`.
In this case, the current keyboard language is US.

- Select the `Keymap` line or press the letter **K**.
- Click on the `OK` button.
  The system changes the keyboard language.
  The `Keymap` line is updated: `Now using [FR]. Switch to US`
- Press the `OK` key to return to the menu.

---

## 7.7 `Password` command

### 7.7.1 Introduction

The `Password` command enables changing the password of the **setup** account.

---

### 7.7.2 Prerequisites

- User : setup

---

### 7.7.3 Preliminary operations

Depending on the situation:

- either use the *SSH access to the configuration menu*
- either use the *Direct connection to the configuration menu with a keyboard and monitor*
- either use the *HTTP access to the configuration menu via iDRAC (DELL server)*
- either use the *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*

---

### 7.7.4 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: `New Password for setup`.
  - Enter the current password and confirm.
  - Enter the current password and confirm.
    After acceptance, the following message is displayed `Password successfully changed`.
  - Click on the `OK` button.

If an error occurs, the following message is displayed: ` Do you want to retry?`
- Select the `Yes` button to restart the password change procedure or the `No` button to cancel.

---

## 7.8 `Network` command

### 7.8.1 Introduction

The network configuration information consists of:

- general settings:
- hostname
- domain name
- DNS servers (primary and secondary)
- NTP servers (primary and secondary)
- Name of the enabled interface
- The settings for each network interface:
- IP address
- mask
- gateway
- routing table

The `Network` command enables access to the `Network Setup` submenu:

```
Show current configuration
Show interface status
Hostname, domain, DNS, NTP
Configure interfaces
Apply Network Config
```

Each of these commands is detailed in the table below:

| Menu | Function | See procedure |
|---|---|---|
| `Show current configuration` | View the current configuration:<br>DNS, domain, GBx network interface information (0 to 3), hostname, and the NTP | *Procedure for viewing the current configuration* |
| `Show interface status` | View the network interface status<br>MAC address, carrier status, speed, connection type | *Procedure for viewing the network interface status* |
| `Hostname, domain, DNS, NTP` | Modification of the GBox's general parameters:<br>DNS, domaine, hostname, NTP | *Procedure for changing the GBox's general parameters* |
| `Configure interfaces` | Modification of the network interface parameters:<br>For each network interface: MAC address, carrier status, speed, and connection type. | *Procedure for modifying the network interface parameters* |
| `Apply Network Config` | Apply the current configuration to the network interfaces | *Procedure for taking modifications into account* |

---

### 7.8.2 Prerequisites

- User : setup

---

### 7.8.3 Preliminary operations

Depending on the situation:

- either use the *SSH access to the configuration menu*
- either use the *Direct connection to the configuration menu with a keyboard and monitor*
- either use the *HTTP access to the configuration menu via iDRAC (DELL server)*
- either use the *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*

---

### 7.8.4 Procedure to access the `Network Setup` submenu

The configuration menu is displayed.

- Select the `Network` line or press the letter **N**.
  The `Network Setup` submenu is displayed:

```
Show current configuration
Show interface status
Hostname, domain, DNS, NTP
Configure interfaces
Apply Network Config
```

### 7.8.5 Procedure for viewing the current configuration

The `Network Setup` submenu is displayed.

- Select the `Show current configuration` line or press the letter **S**.
- Click on the `OK` button.
  The `Current Network Configuration` window is displayed:

```
dns:
  primary: 192.168.1.251
  secondary: ```
domain name  : domain.local
gbx0:
  defaut gateway: 192.168.1.254
  enabled: true
  ip address: 192.168.1.43
  mask: 255.255.255.0
  routing table: `254`
gbx1:
  defaut gateway: ``
  enabled: true
  ip address: ``
  mask: 255.255.255.0
  routing table: `10`
gbx2:
  defaut gateway: ```
  enabled: false
  ip address: ```
  mask: ```
  routing table: ```
gbx3:
  defaut gateway: ```
  enabled: false
  ip address: ```
  mask: ```
  routing table: ```
hostname: gbox
ntp:
  primary: 192.168.1.251
  secondary: ```
primary: gbx0
```

This window displays the:

- DNS
- domain name
- for each network interface gbx(0 to 3),
  - IP address
  - mask
  - subnetwork

  - routing table
  - whether or not the interface is enabled
- GBox hostname
- NTP

- Press the `Back` button to return to the previous menu.

---

### 7.8.6 Procedure for viewing the network interface status

The `Network Setup` submenu is displayed.

- Select the `Show interface status` line or press the letter **S** until this command is selected.
- Click on the `OK` button.
  The following window is displayed:

```
If no interface appears UP, please wait a bit and refresh list.
  Name            Address           Carrier         Speed         Type
  gbx0        24:6e:96:be:4e:c1          UP      1000Mb/s         RJ45
  gbx1        24:6e:96:be:4e:c2          UP      1000Mb/s         RJ45
  gbx2        24:6e:96:be:4e:c3        DOWN           N/A         RJ45
  gbx3        24:6e:96:be:4e:c4        DOWN           N/A         RJ45
```

  This window displays for each network interface (gbx):
  - its name (column `name`)
  - its MAC address (column `Address`)
  - The presence of the carrier (`Carrier` column): UP or DOWN
  - The speed (column `Speed`)
  - The type of connection (`Type` column)
- If necessary, click on the `refresh` button.
- Press the `Back` button to return to the previous menu.

---

### 7.8.7 Procedure for changing the GBox's general parameters

The `Network Setup` submenu is displayed.

- Select the `hostname, domain, DNS, NTP` line or press the letter **S** until this command is selected.
- Click on the `OK` button.
  The following window is displayed:

```
Configure GBox Network

 Hostname               :  gbox
 Domain Name            :  domain.local
 DNS Server (primary)   :  192.168.1.251
 DNS Server (secondary) :  ``
 NTP Server (primary)   :  192.168.1.251
 NTP Server (secondary) :  ``
```

**Note:**

Only the decimal point is accepted when entering the IPv4 address.

- If necessary, change the values.
- Press the `OK` button to confirm the information or the `Cancel` button to return to the previous menu.
- Apply changes (see the *Procedure for taking modifications into account*).

---

### 7.8.8 Procedure for modifying the network interface parameters

The `Network Setup` submenu is displayed.

- Select the `Configure interfaces` line or press the letter **C** until this command is selected.
- Click on the `OK` button.
  The following window is displayed:

```
Choose an interface

 gbx 0 :  192.168.1.43
 gbx 1 :
```

- Select an interface (here gbx 0 or 1) or click the `Cancel` button to return to the previous menu.
  The following window is displayed (for example gbx 0):

```
Configure gbx0

IP Address        192.168.1.43
Netmask           255.255.255.0
Defaut Gateway:   192.168.1.254
```

- If necessary, change the values.
- Press the `OK` button to confirm the information or the `Back` button to return to the previous menu.
- Press the `Back` button to return to the previous menu.
- Apply changes (see the *Procedure for taking modifications into account*).

---

### 7.8.9 Procedure for taking modifications into account

The `Network Setup` submenu is displayed.

- Select the `Apply Network Config` line or press the letter **A** until this command is selected.
- Click on the `OK` button.
  Changes are taken into account.
  The list of parameters is displayed and a status by parameter type is shown.
  A global report is displayed at the end (DONE = ok).
  A progress bar is displayed.
- Once the changes are applied, press the Enter button on the keyboard to return to the previous menu.
  The configuration menu is displayed.

---

## 7.9 `Gapps` command

### 7.9.1 Introduction

The `Gapps Management` command enables GBox applications to be restarted.
The services deploying the web application, databases and analysis engines are restarted.

**Important:**

This option should be used with caution.

---

### 7.9.2 Prerequisites

- User : setup

### 7.9.3 Preliminary operations

Depending on the situation:

- either use the *SSH access to the configuration menu*
- either use the *Direct connection to the configuration menu with a keyboard and monitor*
- either use the *HTTP access to the configuration menu via iDRAC (DELL server)*
- either use the *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*

### 7.9.4 Procedure

The configuration menu is displayed.

- Select the `Gapps` line to be restarted or press the letter **G**.
- Click on the `OK` button.
  The `Gapps` window is displayed:

```
Restart   Restart the Gapps
```

- Select the `Restart the Gapps` line or press the letter **R**.
- Click on the `OK` button.
  The system displays the `Restarting Gbox stack` window.
  A message indicates the restart is in progress.
- Wait for the message `Gbox stack successfully restarted` to appear.
- Click on the `OK` button.
- Press the `Back` button to return to the main menu.

## 7.10 `Services` command

### 7.10.1 Introduction

The `Services` command enables:

- For the Malcore service: force restart or reinstallation
- For Sandbox services:
- enable or disable the Internet connection network interface
- possibility of configuring this interface (IP address, etc.)
- configure a proxy

### 7.10.2 Prerequisites

- User : setup

---

### 7.10.3 Preliminary operations

Depending on the situation:

- either use the *SSH access to the configuration menu*
- either use the *Direct connection to the configuration menu with a keyboard and monitor*
- either use the *HTTP access to the configuration menu via iDRAC (DELL server)*
- either use the *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*

---

### 7.10.4 Procedure for accessing the `Services` menu

The configuration menu is displayed.

- Select the `Services` line or press the letter **S**.
- Click on the `OK` button.
  The `Services` window is displayed:

```
Choose a service
---------------------
  Malcore service
  Sandbox services
```

Each of these commands is detailed in the table below:

| Command | Function | See |
|---|---|---|
| `Malcore service` | Access to the Malcore engine service | *Malcore engine service access procedure* |
| `Sandbox services` | Access to the Sandbox services of the Gnest engine | *Procedure for accessing the Sandbox services of the Gnest engine* |

---

### 7.10.5 Malcore engine service access procedure

The following `Services` window is displayed.

- Select the line `Malcore service` or press the letter **M**.
- Click on the `OK` button..
  The `Malcore Services Manager` window is displayed:

```
Choose a service
-------------------------------------------------------------------------------------------
  Restart Malcore forcefully              Try to restart Malcore if stuck
  Reinstall Malcore service               Wipe out Malcore service and reinstall it
```

Each of these commands is detailed in the table below:

| Command | Function |
|---|---|
| `Restart Malcore forcefully` | Forces a restart of the Malcore service: use in the event of a blockage |
| `Reinstall Malcore service` | Reinstall the Malcore service |

- To force a restart of the service:
  - Select the `Restart Malcore forcefully` command and confirm.
    The `Restart Malcore forcefully` window is displayed.
  - Wait for the message `Malcore successfully restarted` to appear.
  - Click on the `OK` button.
- To reinstall the service:
  - Select the `Reinstall Malcore service` command and confirm.
    The `About to reinstall malcore` window is displayed.

```
You are about to reinstall.
Are you sure you want to continue?
```

  - Click on the `OK` button..
    The `About to reinstall malcore` window is displayed.
  - Wait for the message `Malcore successfully restarted` to appear.
  - Click on the `OK` button.
- Press the `OK` key to return to the main menu.

---

### 7.10.6 Procedure for accessing the Sandbox services of the Gnest engine

The following `Services` window is displayed.

```
Choose a service
--------------------
  Malcore service
  Sandbox services
```

- Select the `Sandbox services` line or press the letter **S**.
- Click on the `OK` button.
  The `Sandbox Services Manager` window is displayed:

```
Choose a service
------------------------------
    Enable internet ouput
    Disable internet ouput
```

**Note:**

Activation of the Internet connection is used by Gnest virtual machines.
However, this activation must also be made when configuring the analysis templates: the implementation is described in *Procedure to configure the Gnest engine*.

Each of these commands is detailed in the table below:

| Command | Function | See procedure |
|---|---|---|
| `Enable internet ouput` | Enable Internet connection | *Procedure for enabling the Internet connection* |
| `Disable internet ouput` | Disable Internet connection | *Procedure for disabling the Internet connection* |

---

#### 7.10.6.1 Procedure for enabling the Internet connection

- Select the `Enable internet output` command and confirm. | The `Enable internet output` menu is displayed.

```
Internet output interface
Proxy configuration
Apply internet configuration
```

Each of these commands is detailed in the table below:

| Command | Function | See procedure |
|---|---|---|
| `Internet output interface` | Selection of the physical interface of the GBox physically connected to the Internet (gbx1 to 3) | *Procedure for enabling the Internet connection* |
| `Proxy configuration` | Configure an Internet access proxy | *Procedure for accessing the Sandbox services of the Gnest engine* |
| `Apply internet configuration` | Apply the Internet configuration | *Procedure for accessing the Sandbox services of the Gnest engine* |

- To specify an interface for output to the Internet
  - Select the `Internet output interface` command and confirm. | The `Choose an interface` window is displayed.
  - Select an interface (e.g. gbx1) and press the `OK` key. | The following message is displayed: `you either have to configure gbx1 or choose another interface`.
  - Press the `OK` key to configure the selected interface (here gbx1). | The following message is displayed: `Internet ouput successfully configured`.
  - Press the `OK` key to return to the previous menu.
  - Press the `Return` key to return to the previous menu.
- To configure a proxy:
  - Select the `Proxy configuration` command and confirm. | The `Proxy configuration` window is displayed.
  - Enter the IP address.
  - Enter the port.
  - Press the `OK` key to confirm the entry.
  - Press the `OK` key to return to the previous menu.
  - Press the `Return` key to return to the previous menu.
- To apply changes to the network configuration:
  - Select the `Apply internet configuration` command and confirm.

    A number of messages appear and then the `Enable internet output` menu is displayed.
  - Press the `OK` key to return to the previous menu.
  - Press the `Return` key to return to the previous menu.

---

#### 7.10.6.2 Procedure for disabling the Internet connection

- Select the `Disable internet output` command and confirm.

  The `Disable internet output` window is displayed.

```
You are about to disable internet
Please confirm?
```

- Click on the `Yes` button to deactivate the internet connection interface.
- Wait for the message `Ìnternet ouput successfully disabled` to appear.
- Press the `OK` key to return to the previous menu.
- Press the `Return` key to return to the previous menu.

- Press the `Return` key to return to the previous menu.

---

## 7.11 `Reset` command

### 7.11.1 Introduction

The `Reset` command enables the data to be deleted and the GBox to be reset to its factory settings.
All configurations and data will be deleted.

---

### 7.11.2 Prerequisites

- User : setup

---

### 7.11.3 Preliminary operations

Depending on the situation:

- either use the *SSH access to the configuration menu*
- either use the *Direct connection to the configuration menu with a keyboard and monitor*
- either use the *HTTP access to the configuration menu via iDRAC (DELL server)*
- either use the *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*

---

### 7.11.4 Procedure

The configuration menu is displayed:

- Select the `Reset` line or press the letter **R**.
- Click on the `OK` button.
  The `Reset GBox Appliance` window is displayed:

```
Warning
This tool will WIPE ALL DATA.
This means that you will loose connectivity and data.
It will restart the GBox automatically.
```

- Press:
  - The `Yes` button to continue
  - The `No` button to cancel.

---

## 7.12 `Restart` command

### 7.12.1 Introduction

The `Restart` command enables a clean reboot of the GBox.

---

### 7.12.2 Prerequisites

- User : setup

---

### 7.12.3 Preliminary operations

Depending on the situation:

- either use the *SSH access to the configuration menu*
- either use the *Direct connection to the configuration menu with a keyboard and monitor*
- either use the *HTTP access to the configuration menu via iDRAC (DELL server)*
- either use the *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*

---

### 7.12.4 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.

---

## 7.13 `Shutdown` command

### 7.13.1 Introduction

The `Shutdown` command enables turning off the GBox.

---

### 7.13.2 Prerequisites

- User : setup

---

### 7.13.3 Preliminary operations

Depending on the situation:

- either use the *SSH access to the configuration menu*
- either use the *Direct connection to the configuration menu with a keyboard and monitor*
- either use the *HTTP access to the configuration menu via iDRAC (DELL server)*
- either use the *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*

---

### 7.13.4 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:

```
Shutdowning 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

---

## 7.14 `Exit` command

### 7.14.1 Introduction

The `Exit` command enables closing the configuration menu.

---

### 7.14.2 Prerequisites

- User : setup

---

### 7.14.3 Preliminary operations

Depending on the situation:

- either use the *SSH access to the configuration menu*
- either use the *Direct connection to the configuration menu with a keyboard and monitor*
- either use the *HTTP access to the configuration menu via iDRAC (DELL server)*
- either use the *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*

---

### 7.14.4 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 GBox 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 8

# Use case : operator group

## 8.1 Connection to the web interface via a browser

### 8.1.1 Introduction

This procedure describes how to connect from a remote computer to the GBox Web interface.
This connection is the standard way of accessing the equipment's Web interface.

---

### 8.1.2 Prerequisites

- User: all users

---

### 8.1.3 Preliminary operations

- Know the name of the GBox or its IP address.

---

### 8.1.4 Procedure

On the remote PC:

- Open a web browser
- Enter the IP address or FQDN of the GBox
- Validate.
  The login window is displayed.
- Enter the login name
- Enter the password
- Validate
  The graphical interface is displayed.

---

## 8.2 Analyses with the GBox

### 8.2.1 Quick procedure for analysing a file

#### 8.2.1.1 Introduction

The `Quick analysis` screen enables an operator to:

- submit one or more files via the GBox Web interface for analysis
- view the analysis report

  This analysis is performed by the engine(s) defined and configured in the default template.

  The analysis is always performed using the default template.

  It is not possible to test files that have a password. For this, use the `New Analysis` screen (voir *Procedure for analysing a file in the `New analysis` screen*).

  **Note:**

  Templates are managed by the administrator.

  **Note:**

  Please note that the maximum file size must not exceed 50MB by default.
  There is no limit to the number of file scans.

The graphical interface is described in *`Home` screen of the Web UI*.

---

##### 8.2.1.1.1 Supported file types

- .jpg
- .bmp
- .mp3
- .avi
- .java
- .js
- .sql
- .html
- .css
- .class
- .c
- .bat
- .pdf
- .txt
- .csv
- .rules
- .xls
- .png
- .key
- .pem
- .wav
- .azw3
- .mp4
- .exe
- .pcap
- .xlsx
- .docx
- .pptx
- .odt (managed as an archive)
- .tar

---

#### 8.2.1.1.2 Unsupported file types

- Bourne-Again
- POSIX shell script
- ELF
- Python

---

#### 8.2.1.1.3 Compressed files

Regarding compressed files analysed by the Malcore engine:

- The number of files contained in an archive is limited and can be modified. 50 is the default value.
- The number of times the file is compressed is limited (max recursion level) and is modifiable. 5 is the default
- If the files are protected by a password, this must be declared in the global

Settings are only accessible to members of the administrator group.

---

### 8.2.1.2 Prerequisites

- User: member of **Operators** Group

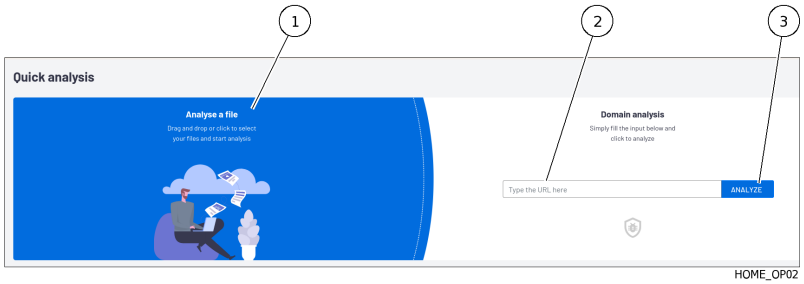
---

### 8.2.1.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

### 8.2.1.4 Procedure for analysing a file



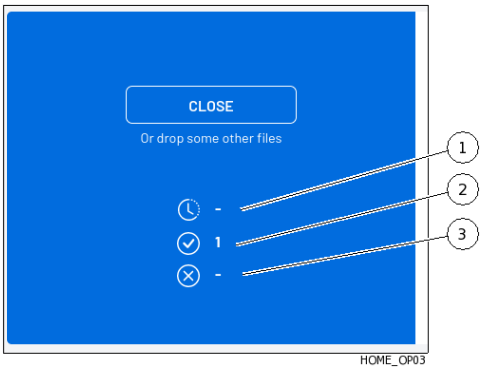
HOME_OP02

- Drop the desired file in the `Analyse a file` area.
  Or
- Click on this area to send the suspicious file.
  The analysis is automatically initiated and the result is automatically displayed in a report in the `Analysis history` area.

---

#### 8.2.1.5 Procedure for analysing download information

The loading report is displayed in the following window:




| Marker | Name |
|---|---|
| 1 | Icon showing the loading time |
| 2 | Total number of files downloaded |
| 3 | Download error |

- Analyse the value of fields (1) to (3) with the following information:
- If icon (1) indicates a number, wait for the download to finish.
  The number decreases.
  A message is displayed to indicate the end of the download.
- Icon (2) shows the total number of files downloaded while the current page is active.
- The value of icon (3) is:
  - 0: no error detected during the download
  - 1 or more: at least one error occurred

---

#### 8.2.1.6 Procedure for analysing the report

Each file scanned generates a report that is displayed in the `` `Analysis history` `` area.

**Note:**

If a directory containing files was uploaded then a different report is created for each file in that directory.
If a compressed file was uploaded then a different report is created for each file contained in that compressed file.

The results of the analyses are displayed in the form of a list, updated every 30 seconds, in the Quick analysis area, where each line corresponds to an analysis of a different file.
This list is limited to the last 10 files analysed.
The various fields displayed are described in *`Analysis history` zone*.

- Analysing reports.
  For this, please refer to the *Procedure to analyse the contents of a report*.

---

### 8.2.2 Quick procedure for analysing a domain

#### 8.2.2.1 Introduction

The GBox enables an operator to analyse a domain after entering its URL.
The graphical interface is described in *`Home` screen of the Web UI*.

---

#### 8.2.2.2 Prerequisites

- User: member of **Operators** Group

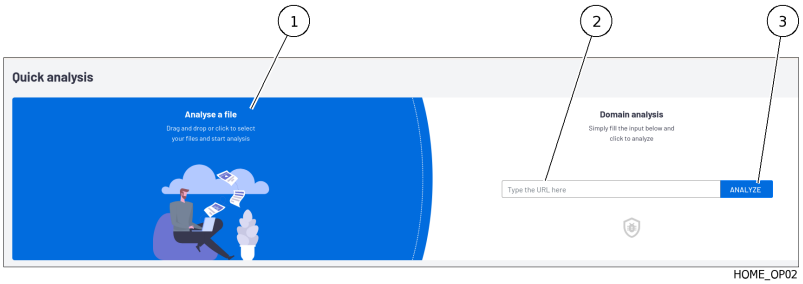
---

#### 8.2.2.3 Preliminary operations

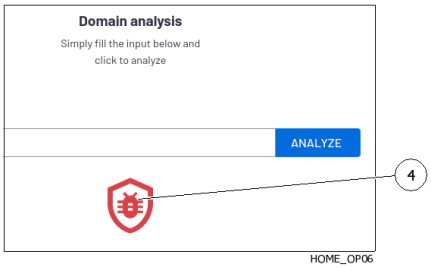
- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

#### 8.2.2.4 Procedure




- Enter the URL of the domain to be analysed in the field (2).
- Click on the `Analysis` button (3).
  The analysis is automatically initiated and the result is displayed. This is the role of icon (4).




| Icon | Signification |
|---|---|
| Red | Danger |
| Other | No danger |

No reports were generated during this analysis.

---

### 8.2.3 Procedure for analysing a file in the `New analysis` screen

#### 8.2.3.1 Introduction

The `New analysis` screen enables an operator to:

- submit one or more files via the GCenter web interface for analysis
- view the analysis report
  The engine used corresponds to the one defined in the `Template` field.
  For a compressed file protected by a password, the `Archive password` field enables entering the password in order to analyse the content.
  The `Forcing` selector enables ignoring any existing results for this file with this template.

  **Note:**

  Please note that the maximum file size must not exceed 50MB by default.
  There is no limit to the number of file scans.

The graphical interface is described in the *`New analysis` screen of the Web UI*.

---

##### 8.2.3.1.1 Supported file types

- .jpg
- .bmp
- .mp3
- .avi
- .java
- .js
- .sql
- .html
- .css
- .class
- .c
- .bat
- .pdf
- .txt
- .csv
- .rules
- .xls
- .png
- .key
- .pem
- .wav
- .azw3
- .mp4
- .exe
- .pcap
- .xlsx
- .docx
- .pptx
- .odt (managed as an archive)
- .tar

---

##### 8.2.3.1.2 Unsupported file types

- Bourne-Again
- POSIX shell script
- ELF
- Python

---

#### 8.2.3.1.3 Compressed files

The characteristics of the compressed files to be analysed are described in *Archive management*.
Concerning the compressed files analysed by Malcore:

- The number of files contained in an archive is limited and can be modified. 50 is the default value.
- The number of times the file is compressed is limited (max recursion level) and is modifiable. 5 is the default value.
- If the files are protected by a password, this must be declared in the global settings.

settings are only accessible to members of the administrator group.

---

### 8.2.3.2 Prerequisites

- User: member of **Operators** Group

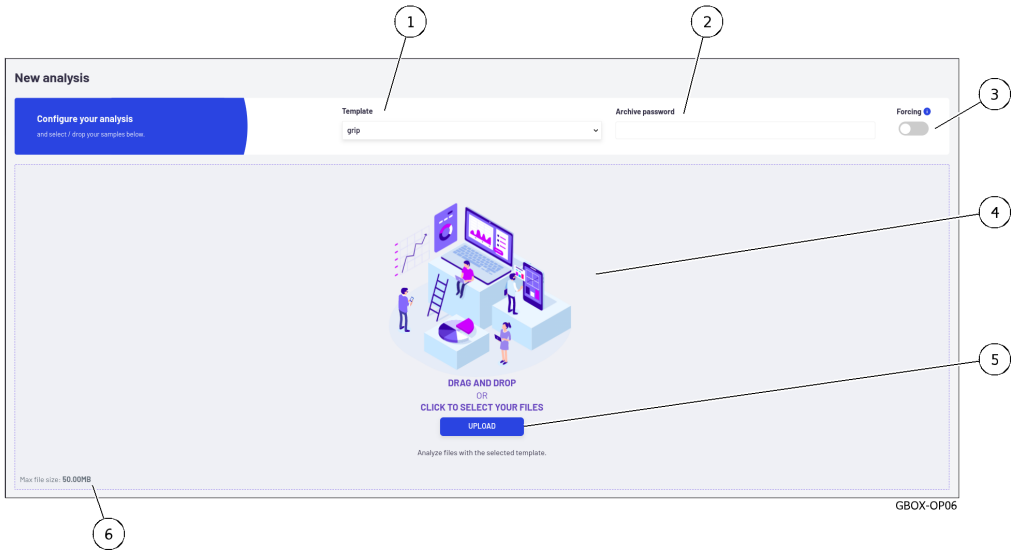
---

### 8.2.3.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

### 8.2.3.4 Procedure




- If necessary, select the engine to be used (1) in the `Template` field.
- For compressed files protected by a password, enter the password (2) in the `Archive password` field.
- If necessary, use the `Forcing` selector (3) to cause the file to be reanalysed if it has already been scanned with the same template selected.
- Depending on the situation:
  - drop the desired file in zone (4) `DRAG and DROP`
    Or

– click on the `UPLOAD` button (5) then select the file to load from the user's computer and finally confirm the selection.

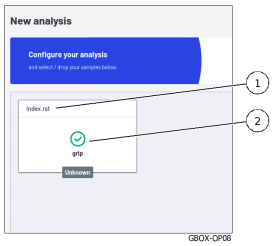
**Note:**

Selecting a file and choosing a template is compulsory. However, using the `Forcing` selector (3) is optional.

The size of the file to be analysed must not exceed 50MB.

The analysis is automatically initiated and the result is automatically displayed.

If the file has been analysed, the report will look like this:




The displayed report shows:

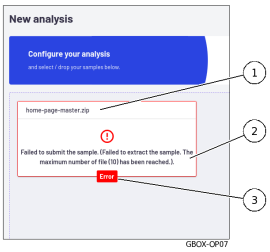
– The name of the analysed file (1)
– The result of the analysis (tick = ok) and the name of the engine used (here the grip engine)

- Click on the report (2):
  – opens the detailed version
  – removes the report from the window
  – saves the report in the report window
- Analysing reports.
  For this, please refer to the *Procedure to analyse the contents of a report*

---

#### 8.2.3.5 Error messages

In the event of an error, a report is displayed: for example, the following case...




The displayed report shows:

- The name of the analysed file (1)
- The occurrence of an error (3)
- The type of error (2): here the maximum number of files included in a compressed file has been reached (10 max)

**Note:**

If the file is too large, the message is: `File is larger than 50.00MB`.

---

### 8.2.4 Procedure to analyse the list of reports on the `Reports` page

#### 8.2.4.1 Introduction

The results of the analyses are displayed in the form of a list, updated every 30 seconds, in the Quick analysis screen, where each line corresponds to an analysis of a different file.
The various fields displayed are described in *`Analysis history` zone*.

---

#### 8.2.4.2 Prerequisites

- User: member of **Operators** Group

---

#### 8.2.4.3 Preliminary operations

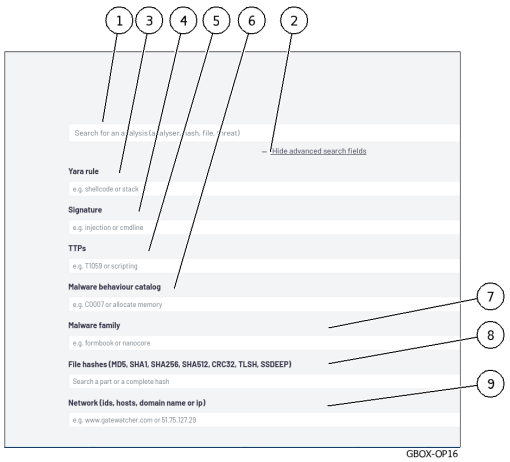
- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

#### 8.2.4.4 Procedure for filtering reports using the search field (1)

**Note:**

This function is unavailable on the `Home` screen in the `Analysis history` area.




There are several ways of entering a value in a search field (1):

- either enter the value directly into the search field, or
- copy the information from a report zone (fields `FILENAME`, `FILE HASH (SHA256)`, `THREAT NAMES`) then paste it into the search field (1).

The list of reports is automatically updated.

---

#### 8.2.4.5 Procedure for filtering reports using advanced search fields

This screen enables filtering reports according to the choices defined in the *Zone enabling searches* window.
These choices are complementary to the search field (1) and enable searching for very specific parameters.

- Click on the `Hide advanced search fields` link (2) to display the advanced search fields.
- Enter the value in the chosen field.

---

#### 8.2.4.6 How to analyse the contents of a report

Refer to *Procedure to analyse the contents of a report*.

---

### 8.2.5 Procedure to analyse the contents of a report

#### 8.2.5.1 Introduction

The detailed analysis report shows the information provided by the valid analysis engines during the analysis.
The various fields displayed are described in *Detailed report*.
This report must be reviewed by an analyst.

---

#### 8.2.5.2 Prerequisites

- User: member of **Operators** Group

---

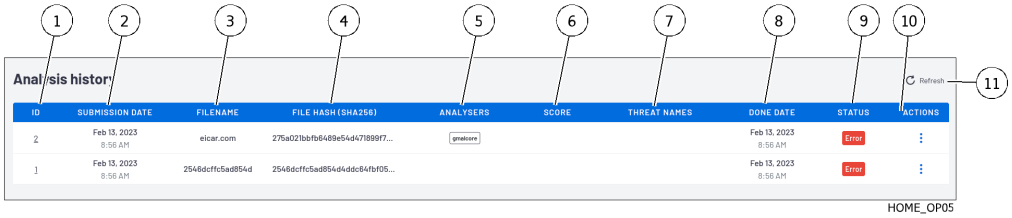
#### 8.2.5.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

#### 8.2.5.4 Report selection procedure

- Apply the *Procedure to analyse the list of reports on the `Reports` page*.




- In the reports area, click on the ID of the desired report (1).
- Please bear in mind the status (9) of the report:
  - For the `In queue` status, wait for the file to be analysed

– For the `In Progress` status, wait until the file has been analysed.

**Astuce:**

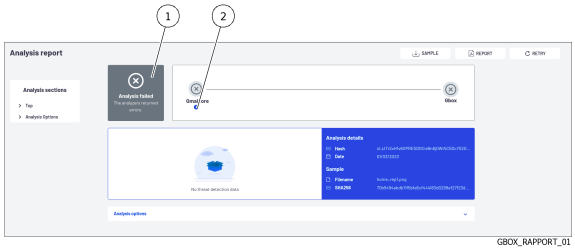
If the `In Progress` status takes too long, you can click on the ID to see the processing details.
Click on the engine information button to view the status of its analysis.

– For the `Error` status, see *Procedure for analysing reports with an `Error` status*
– For the `Clean` status, before confirming that the file is clean, check whether the active engines are indeed the relevant ones...
– For the `Malicious` status, refer to *Procedure for analysing reports having a `Malicious` status*

---

#### 8.2.5.5 Procedure for analysing reports with an `Error` status

- Click on the corresponding ID.
  A window opens showing the detailed report.



GBOX_RAPPORT_01

Zone (1) denotes that the analysis failed and that the engines are reporting errors.

- For more information, click on the information icon (2) to see the details of the error.
  Example: `gmalcore: Malcore analysis error for task id ****. Scan result code received: 10`
- On the basis of the code read on the screen, refer to the following table to identify the reason and choose the appropriate solution.

Table1: Codes analysis results

| Value | Short description | Long description |
|---|---|---|
| 0 | No threat detected | No threat detected or file is empty |
| 1 | Infected/known | A threat was detected |
| 2 | Suspicious | Listed as a possible threat although not identified as a specific threat |
| 3 | Scan failed | The scan is not fully completed, e.g. invalid file or no read permission. If no engine is included and analysis is enabled, this will be the final result. |
| 5 | Unknown | Signature unknown. NOTE: this is only used when searching for multiple hashes. For single hash searches, scan_result is not displayed as a response. |
| 7 | Cleaning ignored | The analysis is ignored because this type of file is included in the authorisation list. |

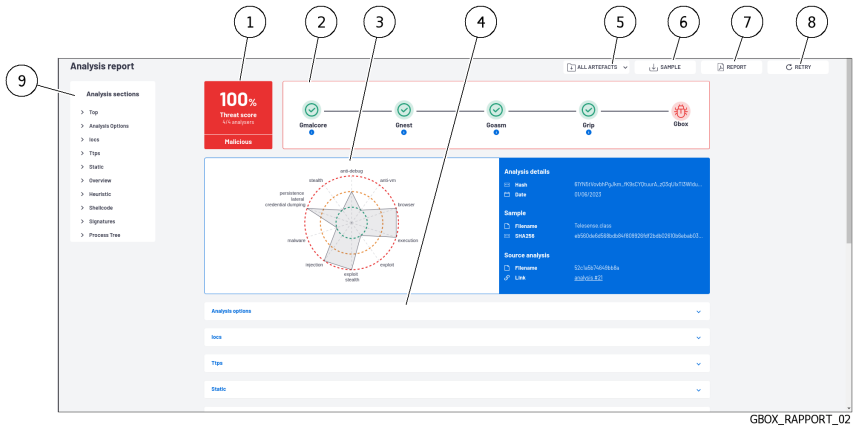
suite sur la page suivante

Table 1 – suite de la page précédente

| Value | Short description | Long description |
|---|---|---|
| 8 | Infection ignored | The scan is ignored because this type of file is on the blocked list. |
| 9 | Archiving depth exceeded | The threat cannot be found, however, there are other archive levels that have not been extracted. |
| 10 | Not scanned / No scan results | The scan is ignored by the engine owing to an update or some other engine-specific reason. If the analysis is disabled, this will be the final result. |
| 11 | Aborted | The analysis in progress has been discontinued due to a problem. |
| 12 | Encrypted | The file/buffer was not scanned because the file type is detected as encrypted and password-protected. |
| 13 | Archive size exceeded | The extracted archive is too large to be analysed. |
| 14 | Archive file number exceeded | There are more files in the archive than are configured on the server. |
| 15 | Password-protected document | A password-protected document [for example, Office documents or PDF files requiring a password to view their contents].<br>If a file is a password protected document, no disinfection will be performed.<br>Supported file formats include: PDF, DOCX, DOC, DOCM, DOTX, DOTM, DOT, PPTX, PPT, POT, POTM, POTX, PPS, PPSM, PPSX, PPTM, PPTX, XLSX, XLS, XLSM, XLSB,XLS, XLTX, XLTM, XLT, XLAM, XLA. |
| 16 | Archive timeout exceeded. | The archiving process reached the given timeout value - a predefined value of 30 minutes. |
| 17 | Offset | The file extension does not match the detected file type. |
| 18 | Potentially vulnerable file. | Possible vulnerability detected for the applied file. |
| 19 | Cancelled | The file analysis was cancelled because it could not be analysed so many times. |
| 23 | Unsupported file type | The engine does not support analysis of this file type.<br>Some engines only scan specific file types such as executable files or documents. |
| 254 | In the queue | The file was added to the analysis queue and is waiting to be processed. |
| 255 | In progress. | Scanning is in progress. |

#### 8.2.5.6 Procedure for analysing reports having a `Malicious` status

- Click on the corresponding ID.
  A window opens showing the detailed report.




The various fields displayed are described in *Procedure for analysing reports with an `Error` status*.

- Refer to the summary of the analysis stages (2).
  Each engine should receive a tick to indicate that its analysis was successful.
  If this is not the case, click on the `i` icon for information on the engine's status: resolve the issue before relaunching the analysis.
  The normal case is that all the engines present are OK. The colour of the GBox icon indicates whether the result is clean or malicious.
- Consult the results of the analysis (1): the score, the overall condition.
  Reminders:
  - A score is only provided for the Gmalcore and Goasm engines
  - The score is only displayed for engines running at the time of the analysis, visible in the summary of analysis stages(2)

**Important:**

The SCORE field only has a meaning for the pre-selected engine. It does not indicate whether the file analysed is clean, only that it has been declared clean by this engine.

- Refer to the information in the optional zones (3) and analysis sections (4).
  Reminders:
  - The chart is only available if Gnest is part of the model. The data required for the chart is generated by this engine.
  - This graph enables viewing the dangerousness of the file analysed.
  - The optional analysis sections depend on the engine(s) active in the template used.
- If required, click on button (5) `ALL ARTEFACTS`.
  This enables downloading of artefacts resulting from the analysis, such as memory dump, network capture (pcap), and character strings detected.
  This section also enables the removal of artefacts.
  This button is only available if the Gnest engine is active.
- If necessary, click on the `REPORT` button.
  This enables downloading the report in pdf format.
- If necessary, click on the `RETRY` button.
  This enables re-running the analysis of this file with this or another template.
- If necessary, click on the `SAMPLE` button.

This enables the analysed file to be downloaded.

---

## 8.3 Local user management

This section describes the management of local users on the GBox.
For more details, see *Presentation of the web interface accounts and their management*.

### 8.3.1 Changing the current account password

#### 8.3.1.1 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.
The `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.

The graphical interface is described in the presentation of the *Current account management, member of the Operators Group*.

---

#### 8.3.1.2 Prerequisites

- User: member of **Operators** Group

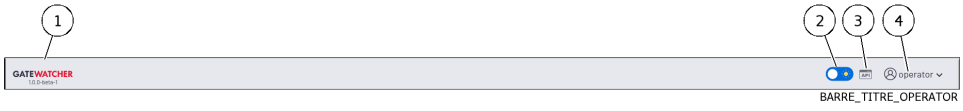
---

#### 8.3.1.3 Preliminary operations

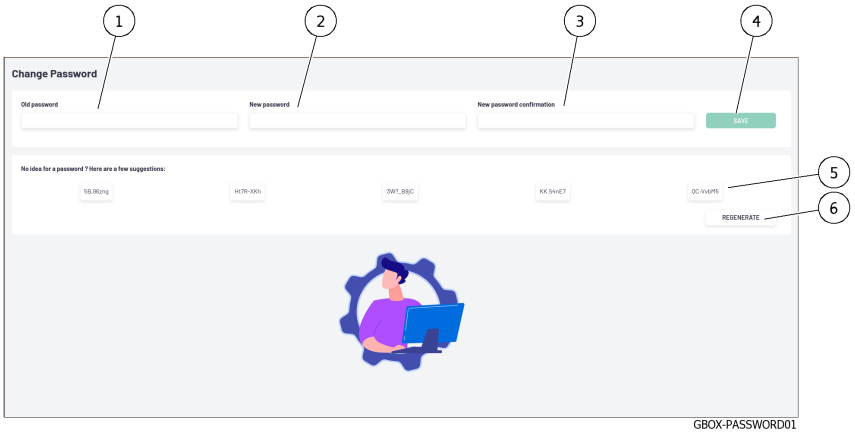
- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

#### 8.3.1.4 Procedure




- Click on the current account button (4).
- Select the `Change password` command.
  The `Change Password` window is displayed.




- Enter the previous password in the `Old password` field (1).
- Enter the new password in the `New password` field (2).
- Enter the new password in the `New password confirmation` field (3).

  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 8` indicates a password that is too short (8 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 button (4) `SAVE`.

**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.

---

## 8.3.2 Changing some of the current user's information

### 8.3.2.1 Introduction

This procedure describes how certain current user information is processed:

- Email address
- First name
- Last name

The graphical interface is described in the presentation of the *Current account management, member of the Operators Group*.

---

#### 8.3.2.2 Prerequisites

- User: member of **Operators** Group

---

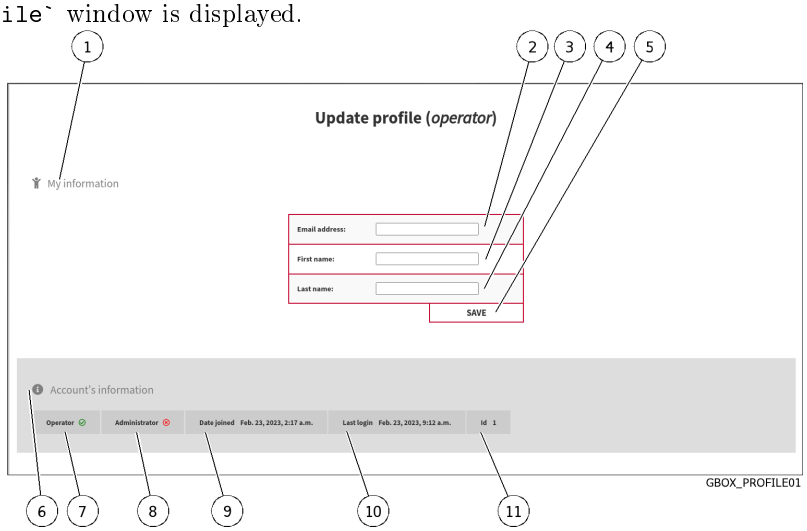
#### 8.3.2.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

#### 8.3.2.4 Procedure

- In the navigation bar, successively click on:
- The `Admin` button
- The `Gcenter` sub-menu
- The `Edit profile` command
  The `Update profile` window is displayed.




  The window shows account information (6).

- Enter or modify the data found in:
- in the field (2) `Email address`
- in the field (3) `First name`
- in the field (4) `Last name`
- Confirm the changes using the `Save` button (5).
  A confirmation window displays the message `Profile successfully saved!`.

---

## 8.4 Logging out of the GBox web interface

### 8.4.1 Introduction

This procedure describes how to log out of Web interface.

---

### 8.4.2 Prerequisites

- User: all users

---

### 8.4.3 Preliminary operations

- Access the Web interface from the workstation (*Connection to the web interface via a browser*).

---

### 8.4.4 Procedure


- In the Web interface, click on the current account button (4).
- Select the `Logout` command.
  The Web interface is closed and the login screen is displayed.

---

# Chapter 9

# Use case : administrator level

## 9.1 Connection to the web interface via a browser

### 9.1.1 Introduction

This procedure describes how to connect from a remote computer to the GBox Web interface.
This connection is the standard way of accessing the equipment's Web interface.

---

### 9.1.2 Prerequisites

- User: all users

---

### 9.1.3 Preliminary operations

- Know the name of the GBox or its IP address.

---

### 9.1.4 Procedure

On the remote PC:

- Open a web browser
- Enter the IP address or FQDN of the GBox
- Validate.
  The login window is displayed.
- Enter the login name
- Enter the password
- Validate
  The graphical interface is displayed.

---

## 9.2 Management of detection engines

### 9.2.1 Procedure to configure the Gnest engine

#### 9.2.1.1 Introduction

##### 9.2.1.1.1 Gnest engine functions

The **Gnest** analysis engine enables dynamic analysis.
It executes the file in a virtual machine (sandbox) and analyses its behaviour.
Following this, it is possible to extract the data generated during the analysis, such as a *dump* of the memory, the extracted character strings, or a capture of network communications (pcap).
When connected to the GCenter, this engine is useful for in-depth analysis of a file classified as *suspicious* or *malicious*, during a second analysis of a file.
This analysis is slower, requiring an experienced operator to analyse the results.

This data is displayed in the *Detailed report* and more specifically in the **TOP**, **Iocs**, **Ttps**, **Overview**, **Signatures** and **Process Tree** sections.

| | |
|---|---|
| **Maximum file size** | 50 MB |
| **Analysis timeout** | 1 hour |
| **Type** | slow |

---

##### 9.2.1.1.2 Configuring the Gnest

Configuring Gnest involves managing and programming virtual machines.
The graphical interface for managing virtual machines is described in the *`Gnest configuration` screen*.

---

##### 9.2.1.1.3 Description of procedures

- *Procédure for accessing the `Gnest configuration` screen*
- *Procedure for creating one or more virtual machines*
- *Procedure for displaying the history of virtual machines*
- *Procedure for deleting a virtual machine*
- *Procedure for deleting several virtual machines by batch*

---

#### 9.2.1.2 Prerequisites

User: member of **Administrators** Group

---

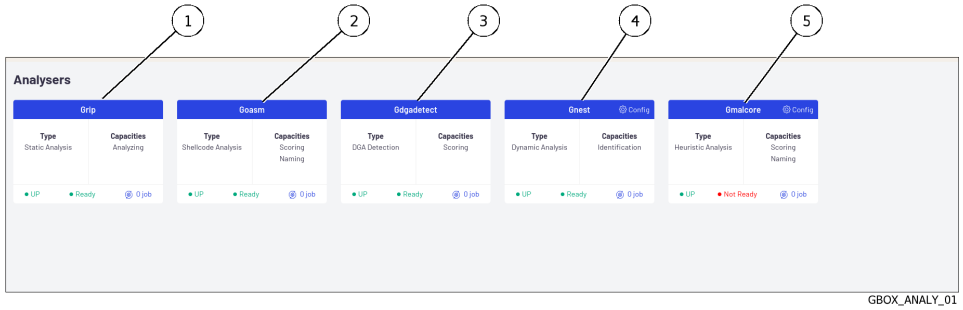
#### 9.2.1.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

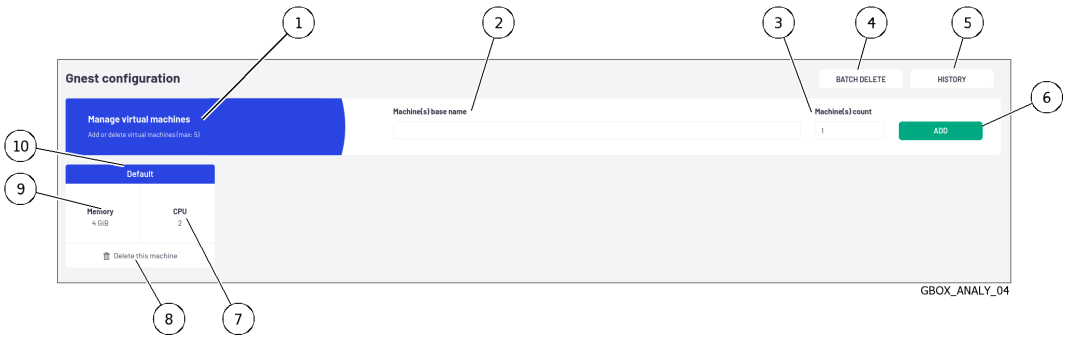
---

#### 9.2.1.4 Procédure for accessing the `Gnest configuration` screen

- In the navigation bar, click on the `Analysers` command.
  The following screen is displayed.




- Click on the `Config` link in the Gnest engine (4).
  The following screen is displayed.




---

#### 9.2.1.5 Procedure for creating one or more virtual machines

By creating virtual machines, multiple analyses can be performed in parallel by enabling these virtual machines in the templates.
The **Gnest** configuration consists of creating virtual machines to act as *sandboxes* for analysis.

**Note:**

It is not possible to have more than 5 virtual machines.

- Enter the name of the machine or machines to be created in field (2): for example **test_VM**.

**Note:**

Only letters, numbers, and underscores are permitted.

- Enter the number of machines to be created in field (2).
- Click on button (6) `ADD`.
  A message is displayed: `Task in progress: Add 2 virtual machines (x%).`
  Once created, the virtual machines are displayed in the window with the names **test_VM1** and **test_VM2**.
  These machines can be configured via template creation.

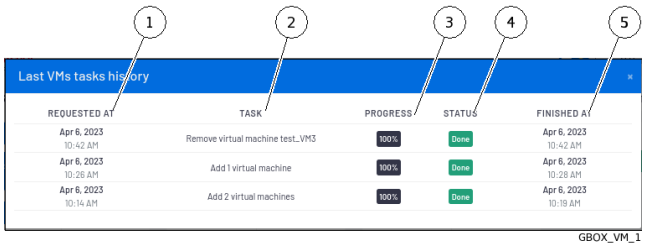
**Note:**

The engine parameters are shown in the *Grip settings* section et in the *Gnest parameters* section.
The procedure for changing these parameters is shown in the *Managing the analysis templates*.

---

#### 9.2.1.6 Procedure for displaying the history of virtual machines

- Click on the `HISTORY` button (5).
  The `Last VMs tasks history` window is displayed.

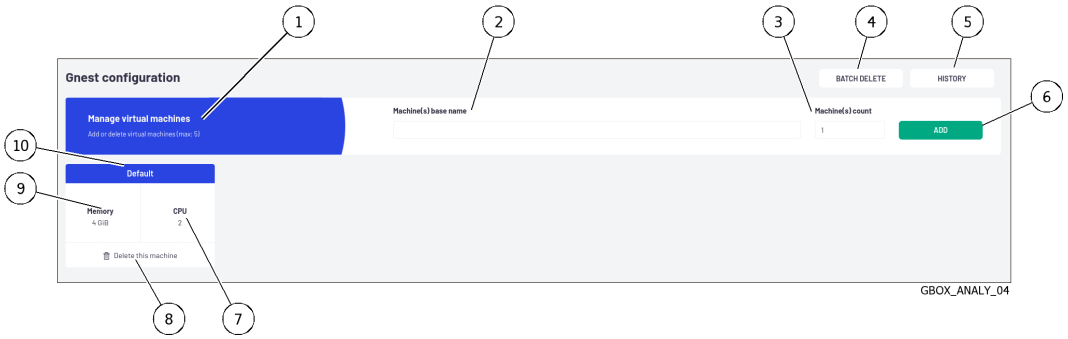



The window displays the following information:

| Marker | field name | Description |
|---|---|---|
| 1 | `REQUESTED AT` | Date and time of task start |
| 2 | `TASK` | Information about the current task |
| 3 | `PROGRESS` | Percentage of task progress |
| 4 | `STATUS` | Current status of the task |
| 5 | `FINISHED AT` | Date and time the job finishes |

---

#### 9.2.1.7 Procedure for deleting a virtual machine




- Click on the link (8) `Delete this machine` for the machine to be removed.
  The following message is displayed.

```
Confirm VM deletion
Are you sure you want to delete the VM test_VM3?
```

- Click on the `Confirm` button.
  The message informs about the action in progress: `Task in progress: Remove virtual machine xxxxx (xx%)`.
  Once the task is complete, the message is displayed: `Task successful: Remove virtual machine xxxx (100%)``.
  The VM is removed from the dashboard.
  If the VM was defined in the templates, the VM is deleted.
  If a template had only this VM defined then the template is kept. The destroyed VM is replaced by all the VMs present (parameter any).

---

#### 9.2.1.8 Procedure for deleting several virtual machines by batch

Just as it is possible to create several machines, it is also possible to delete them in batches.

- Click the `BATCH DELETE` button (4).
  The `Delete multiple VMs` window is displayed to select the machines to be deleted.
- Select the VM(s) to be deleted.
- Click on the `Delete` button.
  The message informs about the action in progress: `Task in progress: Remove virtual machine xxxxx (xx%)`
  Once the task is complete, the message is displayed: `Task successful: Remove virtual machine xxxx (100%)`
  The VMs are removed from the dashboard.
  If VMs were defined in templates, these VMs are deleted.
  If a template had only this VM defined, then the template is kept and the destroyed VM is replaced by all the VMs present (parameter any).

**Note:**

Deletion is sequential. If an error occurs, the process is stopped and the following machines are not deleted.

---

### 9.2.2 Procédure to configure the Gmalcore engine

#### 9.2.2.1 Introduction

Configuring Gmalcore involves:

- ensuring that the engines are started
- ensuring that the engines up to date
- ensuring that engine updates have been scheduled

The functions of the Gmalcore engine are described in the *Overview of the Gmalcore engine* section.
The status of the Gmalcore engines is provided via the `Gmalcore configuration` window.
The graphical configuration interface is described in *`Gmalcore configuration` screen*.

---

#### 9.2.2.2 Prerequisites

User: member of **Administrators** Group

---

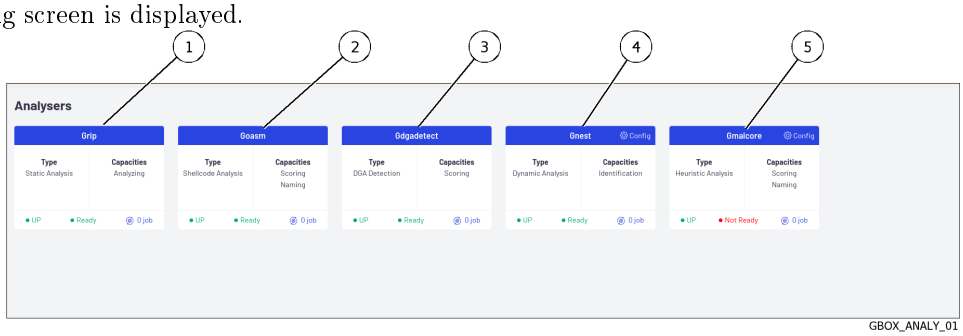
#### 9.2.2.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

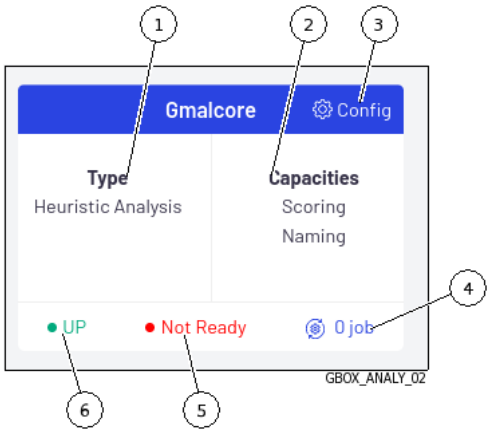
#### 9.2.2.4 Procedure for checking whether Gmalcore engines have started

- In the navigation bar, click on the `Analysers` command.
  The following screen is displayed.



GBOX_ANALY_01

  For the Gmalcore engine, the information displayed is:



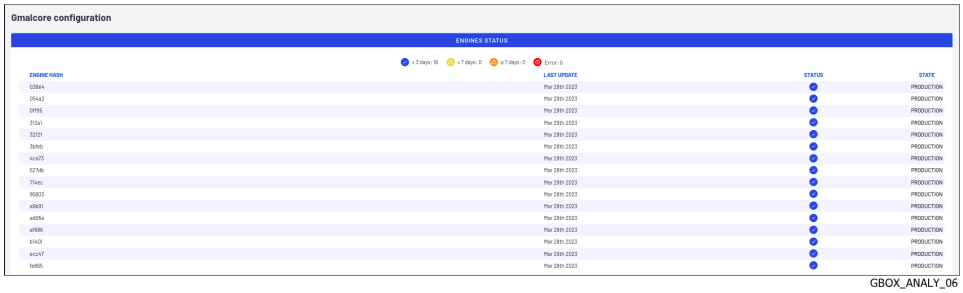

If status (5) is `Ready` then the engines are prepared.
If status (5) is `Not ready` as shown above, then the engine configuration is not done (the engines are not ready).

- Click on the `Config` link (3) to check.

---

#### 9.2.2.4.1 Procedure for the `Ready` status

The following screen is displayed.

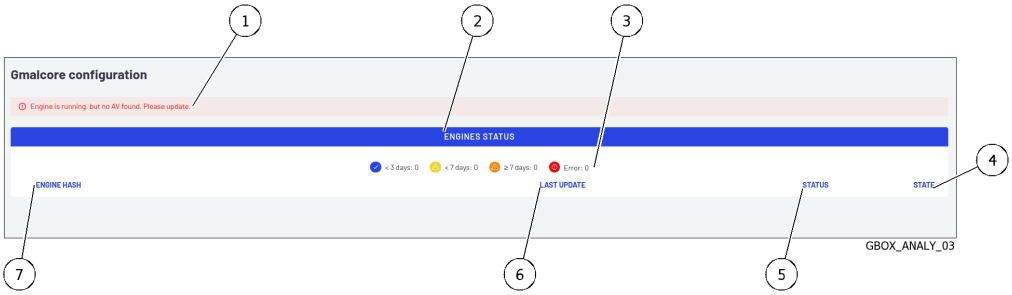



- Check the following items:
- The engines are listed (`ENGINE HASH` column)
- All engines have the status ok (tick in the `STATUS` column)
- The last update is less than 3 days old, as indicated by the colours of the `STATUS` column icon
- If the updates are old, check the update system used in GUM (online, local...).
- For online or local updates, refer to the *Configuring automatic updates via GUM*.
  If this configuration does not work, contact GATEWATCHER support. .. sav2_en
- If there is no automatic configuration then refer to the procedure in *Manual installation of a signature update*.

---

#### 9.2.2.4.2 Procedure for the `Not Ready` status

The following screen is displayed.




In the Malcore configuration screen, the following message (1) is displayed: `Engine is running, but no AV found. Please update.`
In this case, there is no engine installed.

- It is imperative to install a signature and engine update, i.e.:
  - automatically via GUM (online, local): refer to the *Configuring automatic updates via GUM*
  - manually then refer to the *Manual installation of a signature update*

**Note:**

If necessary, configure a proxy (see the *Configuring a proxy* procedure).

---

### 9.2.3 Procedure to analyse the engines monitoring

#### 9.2.3.1 Introduction

This procedure enables displaying the status of the various analysis engines and the actions to be taken.
The graphical interface is described in the *`Analysers` screen of the Web UI*.

---

#### 9.2.3.2 Prerequisites

User: member of **Administrators** Group

---

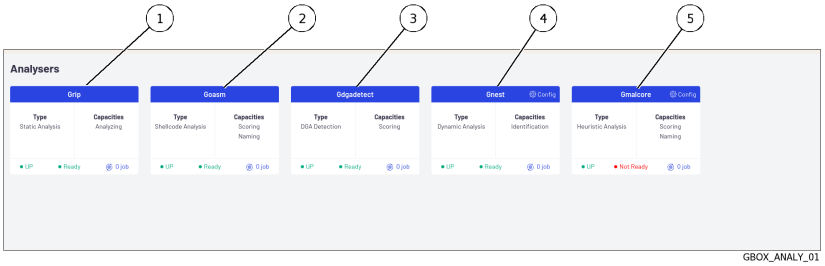
#### 9.2.3.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

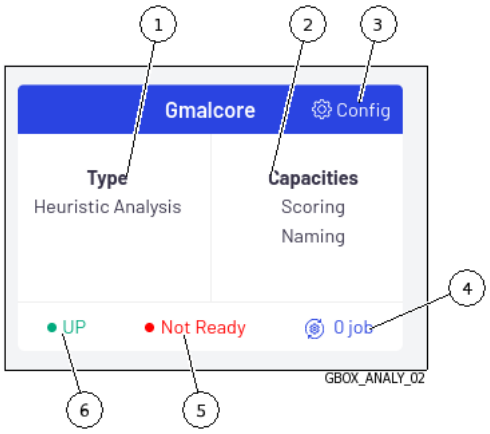
#### 9.2.3.4 How to access the `Analysers` screen

When the `Analysers` command is pressed, the following screen is displayed.



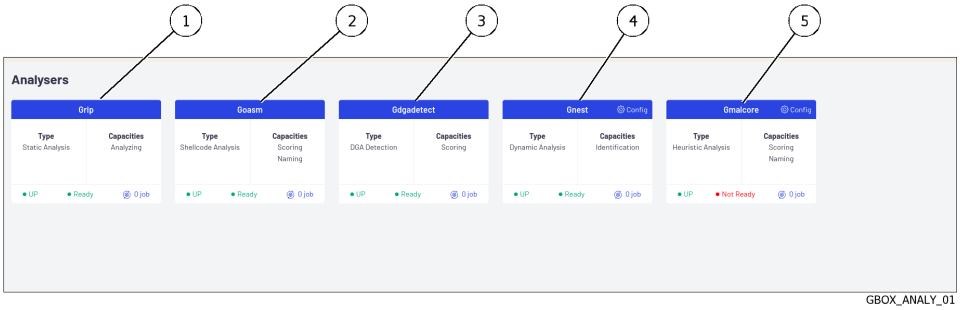

| Marker | Engine | Engine function |
|---|---|---|
| 1 | *Grip engine* | Static analysis |
| 2 | *Goasm engine* | Shellcode detection |
| 3 | *Gdgadetect engine* | Domain name detection |
| 4 | *Gnest engine* | Dynamic analysis within a virtual machine |
| 5 | *Gmalcore engine* | Static and heuristic analysis |

The following information is displayed for each engine:



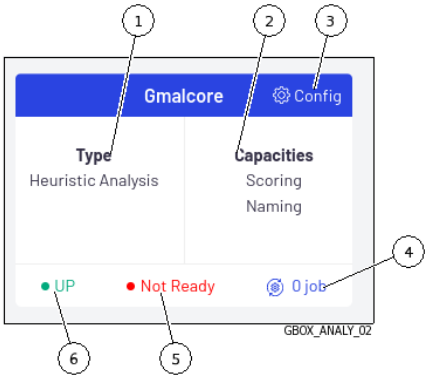
| Marker | Name | Grip Engine | Goasm Enging | Gdgadetect Enging | Gnest Engine | Gmalcore Engine |
|---|---|---|---|---|---|---|
| 1 | Type | Static analysis | Shell code detection | Detection of domain names generated by the Domain Generation Algorithm (DGA) | Executes the file in a virtual machine and analyses its behaviour | Static and multi-engine heuristic analysis |
| 2 | Capabilities | Analysis | Provides a score for the potential danger and names the shellcode detected | Provides a compromise score | Names the problem detected | Provides a score for the potential danger and names the problem detected |
| 3 | Config | Not configurable, so this field is not displayed | | | Virtual machine management - adding, deleting, logging | Gmalcore engine management |
| 4 | x jobs : number of tasks in progress (analysis status NEW + IN PROGRESS) | Number of jobs awaiting processing | | | | |
| 5 | Ability to carry out analyses | This engine has no requirements, so it is always in the `ready` state. | | | The engine is in the `ready` state if there is the same number of VMs in the GBox.<br>and in CAPE - the dynamic analysis engine | The engine is in the `ready` state if all the engines are installed.<br>and the API is up |
| 6 | Engine status | UP : engine api is listening : DOWN : engine api is not active | | | | |

When the `Analysers` command is pressed, the following screen is displayed.




| Marker | Engine | Engine function |
|---|---|---|
| 1 | *Grip engine* | static analysis |
| 2 | *Goasm engine* | Shellcode detection |
| 3 | *Gdgadetect engine* | Domain name detection |
| 4 | *Gnest engine* | Dynamic analysis in a virtual machine |
| 5 | *Gmalcore engine* | Static and Heuristic Analysis |

The following information is displayed for each engine:




| Marker | Name |
|---|---|
| 1 | Type |
| 2 | Capacities |
| 3 | Config, only available for certain engines |
| 4 | x jobs |
| 5 | Status |
| 6 | Engine status |

#### 9.2.3.5 Procedure for checking that engines are in good condition

- Check whether each motor is in the `UP` status.

**Astuce:**

If the engine status (Grip, Goasm, Gdgadetect or Gnest) is `DOWN`, wait a moment.
If the engine remains in the `DOWN` status, contact Gatewatcher support.

- Check whether each motor is in the `Ready` status.

**Astuce:**

`Not Ready` status for the **Gmalcore** engine does ** not necessarily indicate that the engine is unable to perform scans, but it does indicate that at least one of the 16 antivirus engines is out of date or out of service.

- Check that the Gmalcore engines are in good condition: see the *Procédure to configure the Gmalcore engine*.

---

#### 9.2.3.6 Procedure for updating Gnest and Gmalcore engines

Signature updates or **updates** represent updates to the GBox detection engines.
There are 3 types of update packages:

- Gmalcore packages (*latest_malcore*): these packages only contain updates to the antivirus engines and databases used by Malcore.
- Sandbox packages (*latest_sandbox*): these packages contain updates to the signatures and modules used by the Gnest engine sandboxes.
- Complete packages (*latest_full*): these packages are a combination of the two previous packages.

These packages can be installed:

- manually.
  In this case, the graphical interface to be used is described in the *`Admin- GUM - Updates` screen of the legacy Web UI*.
- automatically.
  This schedule must be configured.
  The principle is described in the *Configuring the GUM* paragraph.
  The graphical interface to be used is described in the *`Admin- GUM - Config` screen of the legacy Web UI*.
- If installation needs to be done manually, see the *Manual installation of a signature update* procedure.
- If installation needs to be made automatically, see the *Configuring automatic updates via GUM* procedure.

---

## 9.3 Template management

### 9.3.1 Creating an analysis template

#### 9.3.1.1 Introduction

It is essential to ensure that at least one template is defined so that operators can carry out analyses.
This procedure enables creating analysis templates by combining the different analysis engines.
The graphical interface is described in the *`Admin/Templates` screen of the Web UI*.

---

#### 9.3.1.2 Prerequisites

User: member of **Administrators** Group

---

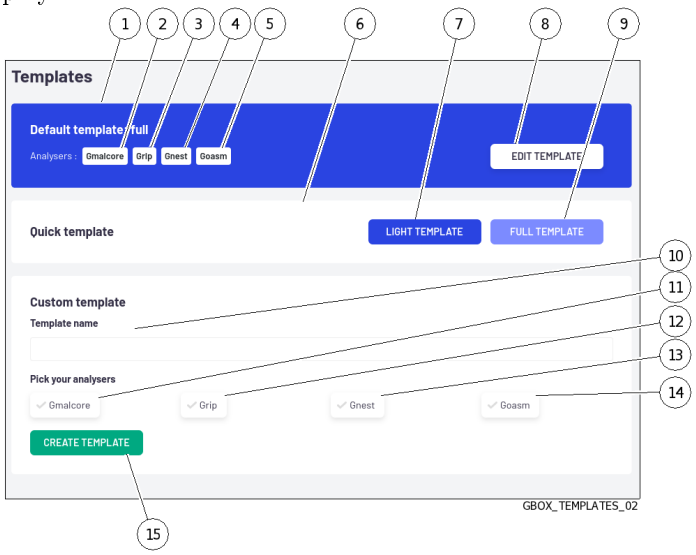
#### 9.3.1.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

#### 9.3.1.4 Procedure for accessing the `Admin/Templates` window for an administrator account

- In the navigation bar, click on the `Templates` command.
  The following screen is displayed:




---

#### 9.3.1.5 Quick template creation procedure

Note that the first template created automatically has the **Default** tag.

- To create a light template (`Quick template` zone):
  - Click on the `LIGHT TEMPLATE` button (7).
    The `Create a quick template` window displays the message `Do you want to create the quick template light?`
  - Click on the `Confirm` button.
    The message `Success - Template created` is displayed.
    The template created immediately appears in the `Available templates` zone (2).

    **Note:**

    The `full` template has all engines enabled with the default engine settings.
    There can only be one template named `full`.

- To create a complete template (`Quick template` zone):
  - Click on the `FULL TEMPLATE` button (8).

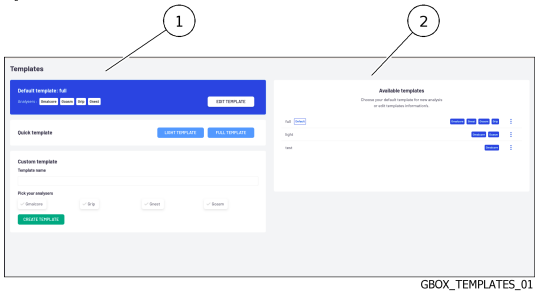
The `Create a quick template` window displays the message `Do you want to create the quick template full?`

– Click on the `Confirm` button.

The message `Success - Template created` is displayed.

The template created immediately appears in the `Available templates` zone (2).

The following screen is displayed:

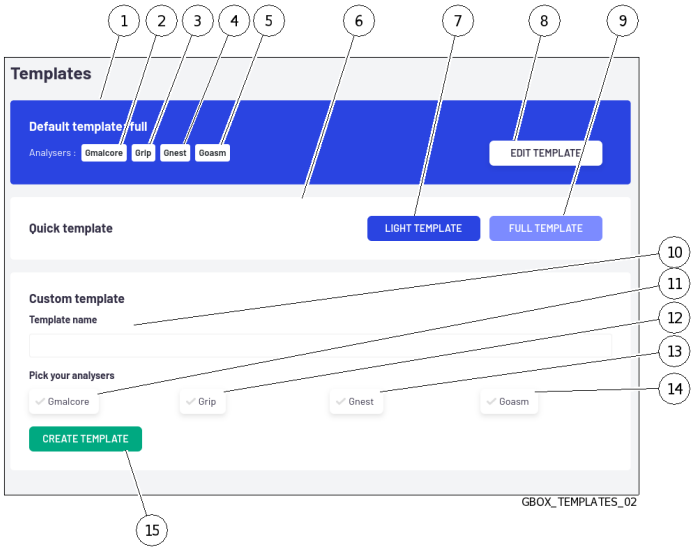



**Note:**

The `full` template has all engines enabled with the default engine settings.

There can only be one template named `full`.

### 9.3.1.6 Procedure for creating a custom template (`Custom template` zone)




- Enter the template name in the `Template name` field (10).
- Select the engines (11 to 14) to be used in the template.
- If necessary, modify the engine parameters. For details of these parameters, see *Grip settings* and *Gnest parameters*)
- Click on button (15) `CREATE TEMPLATE`.

  The message `Success - Template created` is displayed.

  The template created immediately appears in the `Available templates` zone (2).

## 9.3.2 Managing the analysis templates

### 9.3.2.1 Introduction

This procedure enables managing, deleting, or modifying existing templates.
The graphical interface is described in the *`Admin/Templates` screen of the Web UI*.

---

### 9.3.2.2 Prerequisites

User: member of **Administrators** Group

---

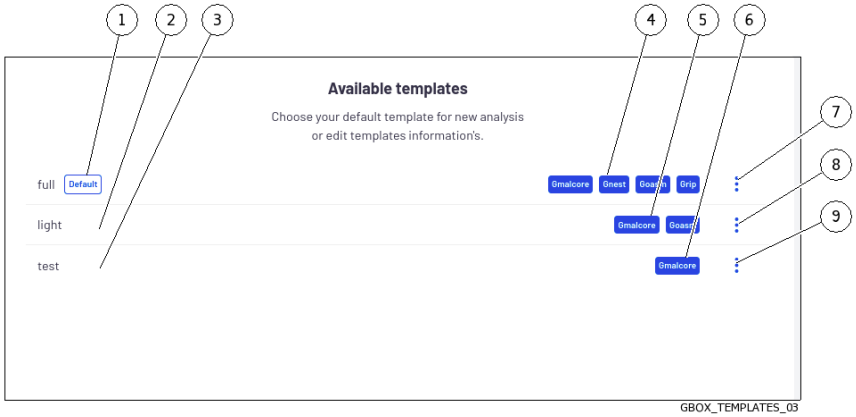
### 9.3.2.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

### 9.3.2.4 Procedure for accessing the `Admin/Templates` window for an administrator account

- In the navigation bar, click on the `Templates` command.
  The following screen is displayed:




---

### 9.3.2.5 Procedure for changing the existing template

A template defined by default (1) can only have its parameters modified.

- To do this, click on the `Edit` command in the menu (7).
  The `Edit template DefaultProfile` window is displayed.
- If necessary, modify the engine parameters. For details of these parameters, refer to *Grip settings* and *Gnest parameters*)
- Click on the `Confirm` button.
  The message `Success - Template updated` is displayed.
  The modified template is displayed in the `Available templates` zone.
  The changes are immediately taken into account in the analyses.

---

#### 9.3.2.6 Procedure for deleting a template

A template that is set by default (1) cannot be deleted.

- Click on the `Remove` command in the menu (7).
  The `Delete template test` window is displayed.
- Click on the `Confirm` button.
  The message `Success - Template deleted` is displayed.
  The deleted template is no longer displayed in the `Available templates` zone.

---

#### 9.3.2.7 Procedure for deleting a template defined by default

A template defined by default (1) cannot be deleted. It is therefore necessary to define another module as the default in order to be able to subsequently delete the desired template.

- To change the default template, select the new template and then click on the `Set as default` command in its menu.
  The `Set template as default` window is displayed.
- Click on the `Confirm` button.
  The message `Success - Default template updated` is displayed.
  The new default template is taken into account and displayed in the `Available templates` area.

---

## 9.4 GBox Software Management

### 9.4.1 Configuring automatic updates via GUM

#### 9.4.1.1 Introduction

Gatewatcher Update Manager (GUM) is a tool that enables managing updates to the **GBox**.

This screen enables configuring the automatic scheduling of updates.
These updates can be made:

- Via Online mode
  If necessary, configure a proxy (see the *Configuring a proxy* procedure)
  Online mode enables automatic updates to be made from the Internet.
  The URL field will be filled in automatically. The update packages can be obtained from the Gatewatcher servers https://update.GATEWATCHER.com/update/.
- Via the Local mode
  If necessary, configure a proxy (see the in *Configuring a proxy* procedure)
  Local mode enables updates to be made from a local repository previously configured to download packages from Gatewatcher servers https://update.GATEWATCHER.com/update.
  This local repository is defined in the *`Admin- GUM - Config` screen of the legacy Web UI*.

An intelligence account will be required for the update package to be downloaded from the site.
In `online` mode, this user and password pair must be entered in the `Username` and `Password` fields below the address.

This procedure describes how to configure automatic updates from:

- Either a server on the local network (choose `local`)
- Or a server on the Internet (choose `online`)

The graphical interface is described in the *`Admin- GUM - Config` screen of the legacy Web UI*.

**Note:**

If necessary, configure a proxy (see the *Configuring a proxy* procedure).

---

#### 9.4.1.2 Prerequisites

- User: member of **Administrators** Group

---

#### 9.4.1.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).
- In local mode, complete the local repository configuration prerequisites:

- The server must be reachable in HTTP on port 80
- Create the following tree structure: `2.5.3.10X/GBox` depending on the GBox version (2.5.3.100 or 2.5.3.101)
- Retrieve the necessary gwp files (latest_full.gwp for a GBox V100, latest_full_v3.gwp for a 2.5.3.101) from *https://update.gatewatcher.com/update/<version_gbox>/gbox/*
- In `2.5.3.10X/gbox`, insert the gwp file retrieved previously.
- In `2.5.3.10X/gbox`, place a sha256sum.txt file that contains a `sha256sum FileName` entry

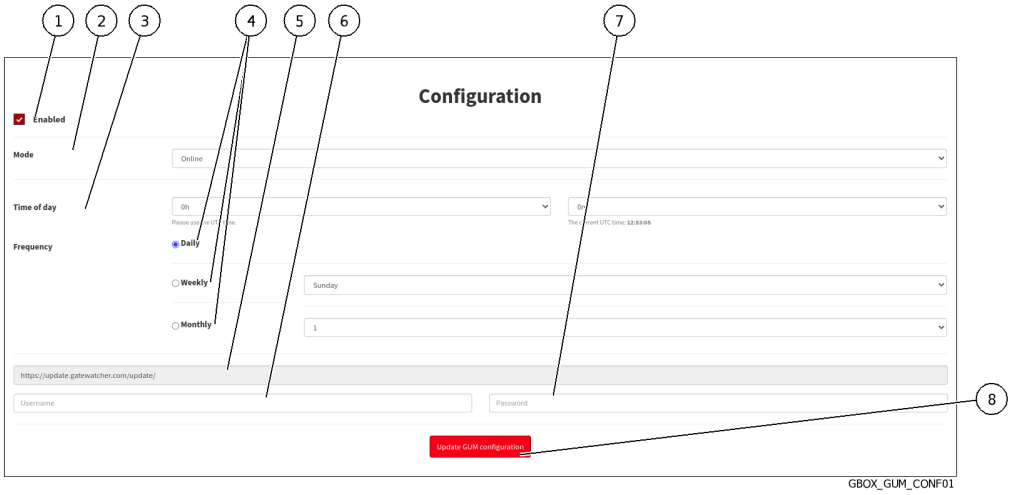
**Note:**

The 2.5.3.10X folder absolutely must be at the root of the HTTP server launched previously for local mode to work.

---

#### 9.4.1.4 How to access the `Configuration` screen

- In the navigation bar, click on the `Config` command in the `GUM` menu.
  The following screen is displayed:

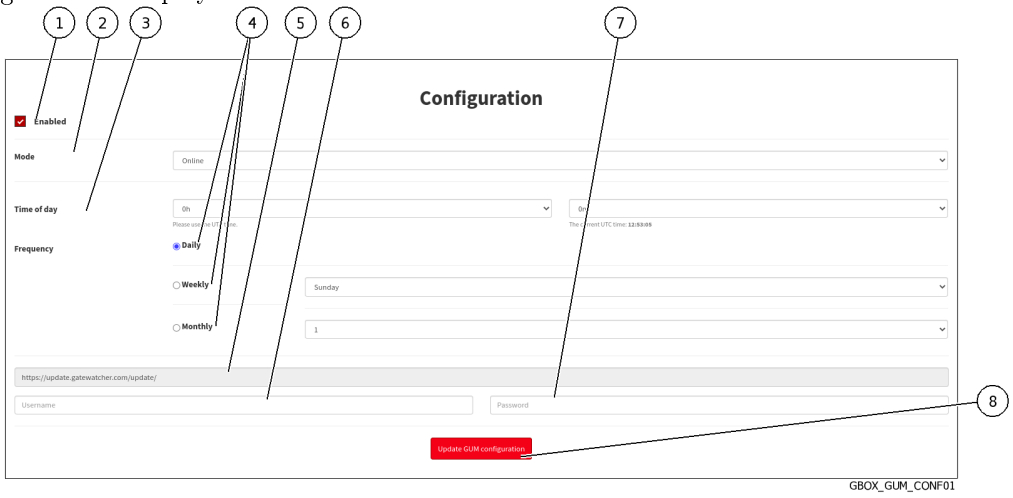



- Perform the *Procedure for configuring the online mode*
  Or
  Perform the *Procedure for configuring the local mode*

---

#### 9.4.1.5 Procedure for configuring the online mode

- In the navigation bar, click on the `Config` command in the `GUM` menu.
  The following screen is displayed:




- Tick choice (1) `Enabled`.
- In the `Mode` field (2), select `Online`.
- Select the time (field (3) `Time of day`) of the update.
- Set the update frequency:
  - Select the frequency using the buttons (4) `Daily`, `Weekly`, `Monthly`.
  - Select the day for `Weekly`.
  - If `Monthly` is selected, select the month

**Note:**

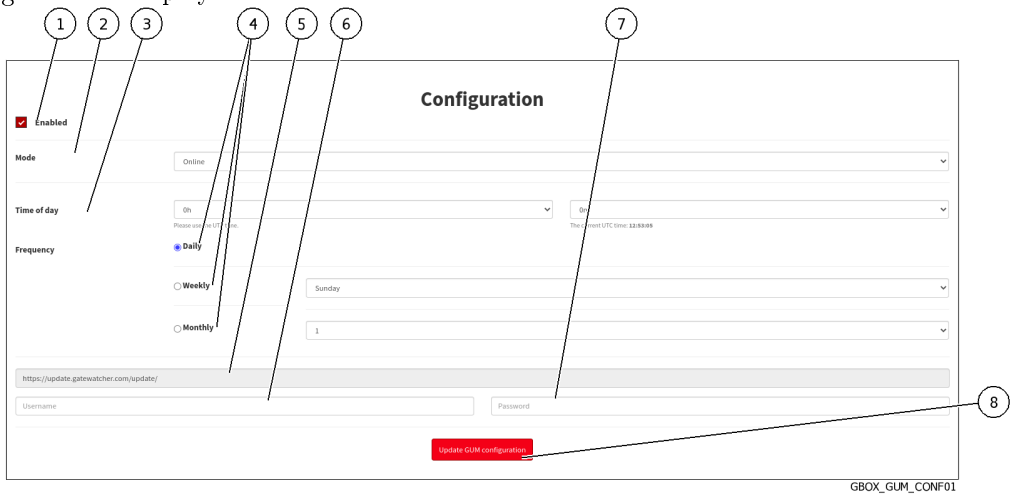
The update source field (5) is automatically filled in.

- Enter the login to connect to update.gatewatcher.com:
  - `Username`: field (6)
  - `Password`: field (7)

- Click on the `Update GUM configuration` button (8).

#### 9.4.1.6 Procedure for configuring the local mode

- In the navigation bar, click on the `Config` command in the `GUM` menu.
  The following screen is displayed:




- Tick choice (1) `Enabled`.
- In the `Mode` field (2), select `local`.
- Set the update frequency:
  - Select the frequency using the buttons (4) `Daily`, `Weekly`, `Monthly`.
  - If `Weekly` is selected, select the day.
  - If `Monthly` is selected, select the month.
- Enter the URL of the local repository (5).
- Enter the login to access the local repository (optional):
  - `Username` : field (6)
  - `Password` : field (7)
- Click on the `Update GUM configuration` button (8).

### 9.4.2 Manual installation of a signature update

#### 9.4.2.1 Introduction

This procedure describes the various options for updating the signature files of the solution's detection engines. Updates can be triggered:

- either scheduled.
  This schedule is programmed in the GUM configuration (see *`Admin- GUM - Config` screen of the legacy Web UI*).
  In this case, the `Updates` screen provides information on the last scheduled installation.
- Or manually.
  In this case, it is necessary to load a package from the remote PC onto the GBox and then trigger the installation of this package.
  In this case, the `Updates` screen shows information about this installation.

**Important:**

It is not possible to update in manual mode if the online mode is configured.

**Note:**

See the presentation described in the *Updates to detection signatures and/or anti-virus engines* section
The graphical interface is described in the *`Admin- GUM - Updates` screen of the legacy Web UI* paragraph.

**Note:**

If necessary, configure a proxy (see the *Configuring a proxy* procedure).

---

#### 9.4.2.2 Prerequisites

- User: member of **Administrators** Group

---

#### 9.4.2.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).
- Download a *.gwp* file from *https://update.gatewatcher.com/update/<version_gbox>/gbox/*

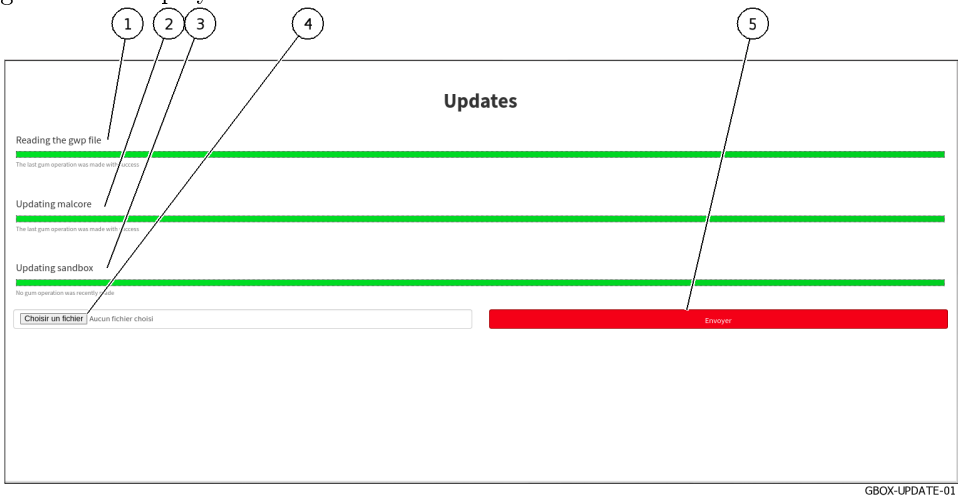
**Note:**

Files with names ending in "v3.gwp" such as latest_malcore_v3.gwp or latest_full_v3.gwp are for V101.
The other files (latest_full.gwp, latest_malcore.gwp, ...) concern version 100 of the GBox.

---

#### 9.4.2.4 Procedure for accessing the `Admin/GUM/Updates` screen window

- In the navigation bar, click on the `Updates` command in the `GUM` menu.
  The following screen is displayed:




---

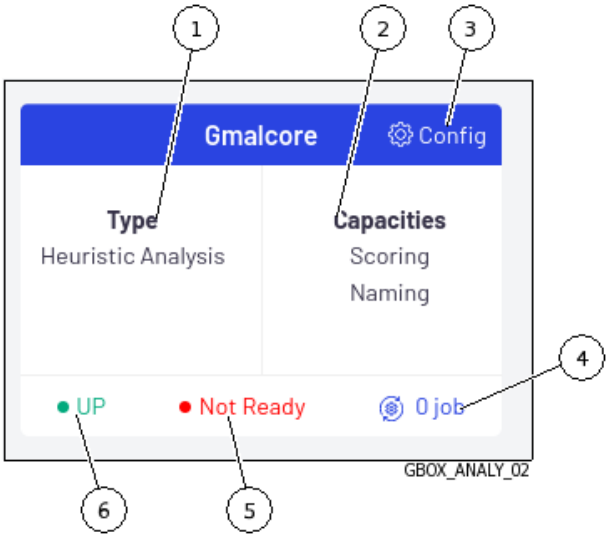
#### 9.4.2.5 Procedure for updating signature files in manual mode

- Click on the `Browse` button (4) and select the previously downloaded package
- Validate the command.
  The button displays `Please wait...`.
  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.
- Wait for the message `The last gum operation was made with success` to appear.
  The progress bar in the `Updating malcore` field begins to progress. This corresponds to the processing of the Malcore engine files.
- Wait for the message `The last gum operation was made with success` to appear.
  The progress bar in the `Updating sandbox` field starts to move: this corresponds to the processing of updates to signatures and modules used by the sandbox.
- Wait for the message `The last gum operation was made with success` to appear.

---

#### 9.4.2.6 Procedure for checking that Gmalcore engines are in good condition

- In the navigation bar, click on the `Analysers` command.

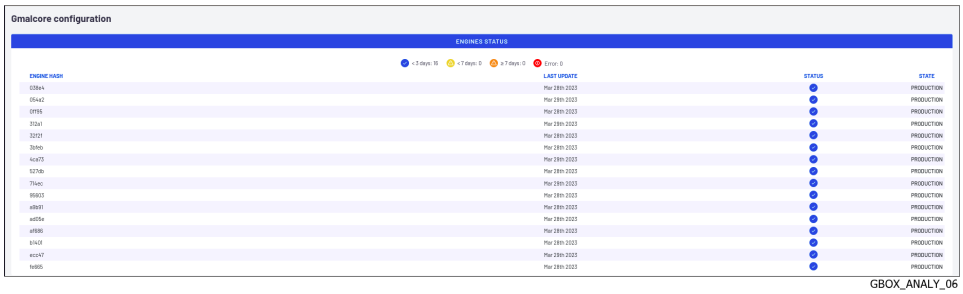



- Click on command (3) `Config`.
  The following screen is displayed.


- Look for a message in zone (1).
- In the case of a message of the type `x engine(s) have failed to update`, check the status of the installed engines (column (2)).

Engines whose status is red in column (2) are not in PRODUCTION status.
Some engines take a long time to update and are still in DOWNLOADED status.

- Wait for the update to finish and for all the engines to be OK (PRODUCTION status).



GBOX_ANALY_06

- If one of the engines is still not OK then it is necessary to restart the Gmalcore services.
  To do this see *Malcore engine service access procedure*.
- If this does not fix the problem then reinstall the Gmalcore services.
  To do this see *Malcore engine service access procedure*.

---

### 9.4.3 Installing a hotfix patch

#### 9.4.3.1 Introduction

A patch enables a given correction or modification to be applied without having to upgrade the entire solution or restart the GBox.
Unlike updates, patches cannot be automated. They must be carried out by an administrator after reading the release notes.
All patch packages can be downloaded via our download platform: https://update.gatewatcher.com/hotfix
This procedure describes how to apply a patch.

**Note:**

See the presentation described in the *Applying a hotfix patch*.
The graphical interface is described in *`Admin- GUM - Hotfix` screen of the legacy Web UI*.

---

#### 9.4.3.2 Prerequisites

- User: member of **Administrators** Group

---

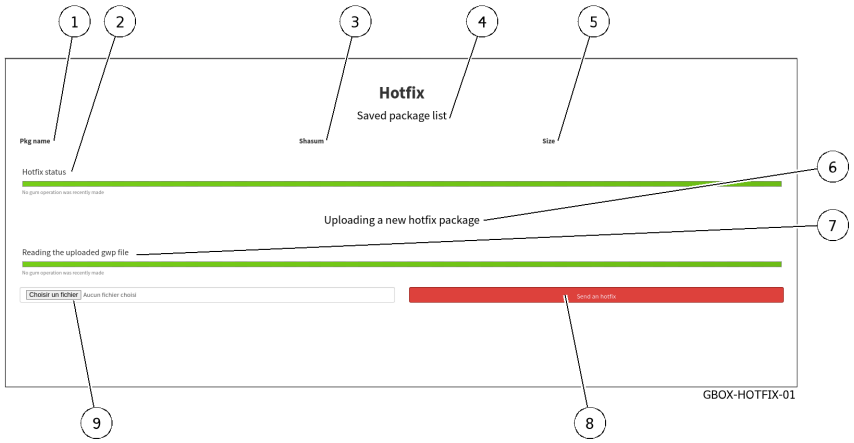
#### 9.4.3.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).
- Read the release note of the desired version to see whether any other prerequisites are required.
- Recover a *.gwp* file from *https://update.gatewatcher.com/update/<version_gbox>/gbox/*.

---

#### 9.4.3.4 Procedure for accessing the `Admin/GUM/Hotfix` screen window

In the navigation bar, click on the `Hotfix` command in the `GUM` menu.
The following screen is displayed:




---

#### 9.4.3.5 How to apply a patch

- Click on button (9) `Choose a file` and select the previously downloaded package.
- Click on button (8) `Send a hotfix`.
- Once the package is present in the `Saved package list` zone (1), click on the `Apply` button.
- Wait until the progress bars indicate the operation was completed successfully.
  The patch was applied and corrections are being made to the equipment.

**Note:**

In some cases, applying a patch may cause the web server to restart. This will make the web interface unavailable for a few minutes as specified in the release note.

---

### 9.4.4 Installing an upgrade

#### 9.4.4.1 Introduction

An upgrade enables a major version enhancement to be performed. This involves a reboot of the device concerned.
Unlike updates, upgrades cannot be automated. They must be carried out by an administrator after reading the release notes.

This procedure describes how to apply an upgrade.

**Note:**

See the presentation described in the *Upgrade* section.
The graphical interface is described in the *`Admin- GUM - Upgrade` screen of the legacy Web UI* section.

---

#### 9.4.4.2 Prerequisites

User: member of **Administrators** Group

---

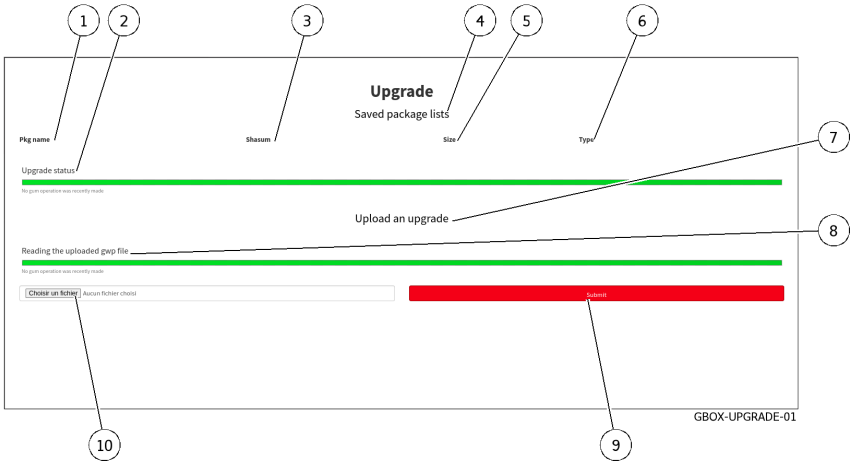
#### 9.4.4.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a 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 (https://update.gatewatcher.com/upgrade).

---

#### 9.4.4.4 Procedure for accessing the `Admin/GUM/Updates` screen window

- In the navigation bar, click on the `Updates` command in the `GUM` menu.
  The following screen is displayed:




---

#### 9.4.4.5 Procedure for applying an upgrade

- Click on button (10) `Choose a file` and select the previously downloaded package.
- Click on the button (9) `Submit`.
- Once the package is present in the `Saved package list` zone (1), click on the `Apply` button.
- Wait until the progress bars indicate the operation was completed successfully.
- Restart the GBox (see how to use the *`Restart` command*).
  After restarting, the GBox takes into account the downloaded version.

---

## 9.5 GBox configuration

### 9.5.1 Configuring the GBox for the first connection

#### 9.5.1.1 Introduction

Although much of the solution is already configured by the Gatewatcher teams, it is necessary to complete, at a minimum, the network configuration of the GBox in order to access the Web UI.
When connecting for the first time, it is necessary to access the **GBOX** via the iDRAC interface or a terminal in order to perform the network configuration.
The recommended profile is **setup**, the default password for this user is: **default**.

**Important:**

It is essential to change this password as soon as possible.

---

#### 9.5.1.2 Prerequisites

- User : setup
- User: member of **Administrators** Group
- Connect the GBx0 network port for the management interface (for more information, see *Interface network `Gbx0`*).
- If necessary, connect the network port to the GBx1 interface for connecting Gnest's virtual machines to the Internet (for more information, see *Interface network `Gbx1`*).

---

#### 9.5.1.3 Preliminary operations

- Check that the LUKS key is connected to the equipment.

**Note:**

If there is no LUKS key or if it is the wrong one, the operating system will not be able to access the contents on the hard drives.
In case of problems, check:

- The key: it must be the right one and not one from another appliance.
- The USB port is working properly: if necessary, change the USB port

Depending on the situation:

- either use the *Direct connection to the configuration menu with a keyboard and monitor*
- either use the *HTTP access to the configuration menu via iDRAC (DELL server)*
- either use the *SSH access to the configuration menu via the iDRAC interface in serial port redirection mode*

**Note:**

Make sure the keyboard configuration is correct (fr or us version).

The configuration menu is displayed.

- If necessary, select the language used for the keyboard (see *`Keymap` command*).

---

#### 9.5.1.4 Procedure for changing the GBox's general parameters

**Note:**

The general parameters are:
- hostname
- domain name
- DNS servers (primary and secondary)
- NTP servers (primary and secondary)

- Access the network view and configuration menu (see *`Network` command*).
- View the current configuration (see the *Procedure for viewing the current configuration*).
- Modify the general parameters if necessary (see the *Procedure for changing the GBox's general parameters*).
- Apply the procedure for accepting changes if necessary (see the *Procedure for taking modifications into account*).

---

#### 9.5.1.5 Procedure for configuring GBx0 management network interface parameters

- View the configuration of each network interface (see the *Procedure for viewing the network interface status*).
- Modify the parameters if necessary (see the *Procedure for modifying the network interface parameters*).
- Apply the *Procedure for taking modifications into account* for the GBx1 interface.

**Note:**

Once this initial configuration is complete, it is possible to connect to the GBox interface using a Web browser in HTTPS at the configured address.

The default users are:

- admin
- administrator
- operator

For details of the rights and functions authorised to each account/group, refer to the *Presentation of accounts*.

For information on the various functions of the graphical administrator or operator interface, please refer to the *Presentation of graphical interfaces*.

---

#### 9.5.1.6 Procedure for configuring the GBx1 network interface parameters of Gnest virtual machines to the Internet

- Apply the *Procedure for modifying the network interface parameters* for the GBx1 interface
- Apply the *Procedure for accessing the `Services` menu*
- Apply the *Procedure for accessing the Sandbox services of the Gnest engine*
- Apply the *Procedure for enabling the Internet connection*

---

#### 9.5.1.7 Licence entry procedure

- Follow the entry procedure in *Installing an SSL certificate*.
  Once the license is validated and activated, the content of the page updates and displays the details of the license.
  In the event of a missing or expired licence, the interface will automatically redirect to this page to resolve the issue.

---

#### 9.5.1.8 Procedure for configuring the SSL certificate

The SSL certificate attests to the identity of the GBox and enables data exchanges to be encrypted.

- Follow the entry procedure in *Installing an SSL certificate*.

---

#### 9.5.1.9 Licence entry procedure

- Follow the entry procedure in *Installing an SSL certificate*.
  Once the license is validated and activated, the content of the page updates and displays the details of the license.
  In the event of a missing or expired licence, the interface will automatically redirect to this page to resolve the issue.

---

#### 9.5.1.10 Postliminary procedures

- Starting up the GBox: see the *Operating a GBox* procedure.

---

### 9.5.2 Operating a GBox

#### 9.5.2.1 Introduction

After setting up the GBox, this procedure shows how to put it into operation.

---

#### 9.5.2.2 Prerequisites

- User: member of **Administrators** Group

---

#### 9.5.2.3 Preliminary operations

- Apply the *Configuring the GBox for the first connection*

---

#### 9.5.2.4 User management procedure

As accounts are by default, it may be necessary to modify the default accounts or add new ones.

- *Creating local users*
- *Changing some of a local user's information*

---

#### 9.5.2.5 Manage the analysis engines

- If necessary, change the number of virtual machines in the Gnest engine:
  - For this, see the procedure to create one or more virtual machines (*Procedure to configure the Gnest engine*)
  - Take into account this new configuration by creating or modifying the analysis templates (see *Template management*)
- Perform the Check State of Scan Engines and Updates procedure (see *Procedure to analyse the engines monitoring*)

---

#### 9.5.2.6 Procedure for managing analysis templates

- Create analysis templates (see the *Creating an analysis template* procedure).
- Manage the analysis templates (see the *Managing the analysis templates* procedure).

**Astuce:**

Create a template using the Gmalcore and Gnest engines previously configured and set it to default.
With an Operators group account, select a file and perform a quick scan.
Check that the analysis is done correctly.

---

#### 9.5.2.7 Procedure for association with the GCenter

- Create an API token and copy it.
- Log on to GCenter and association with GBox (refer to GCenter documentation).
- Paste the token during the association procedure.
- Implement GCenter.
- If the files to be analysed are sent automatically, check that the analyses are carried out: new reports are created...
- Send a file to be analyzed from the GCenter and then download the corresponding report: these operations are done on the GCenter.

---

### 9.5.3 Modifying the licence

#### 9.5.3.1 Introduction

The licence may have an expiration date.
It is possible 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: commerciaux@gatewatcher.com.
Once the license is validated and activated, the content of the page updates and displays the details of the license.

In the event of a missing or expired licence, the interface will automatically redirect to this page to resolve the issue.
This graphical interface is described in *`License configuration` screen*.

---

#### 9.5.3.2 Prerequisites

- User: member of **Administrators** Group

---

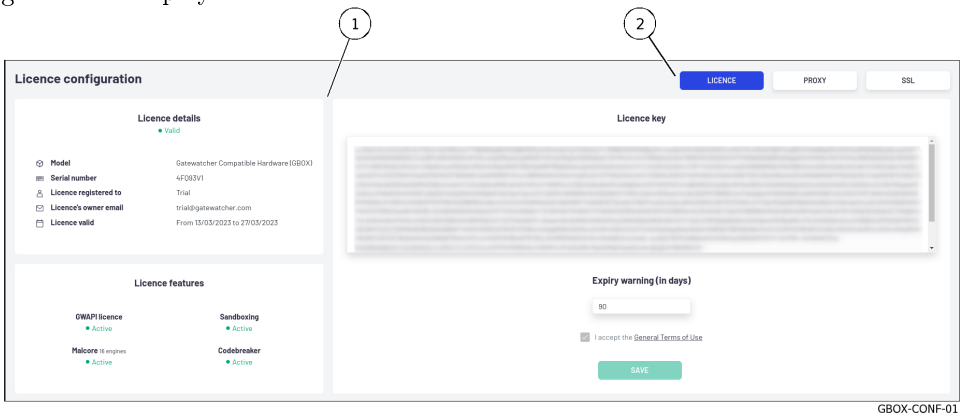
#### 9.5.3.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

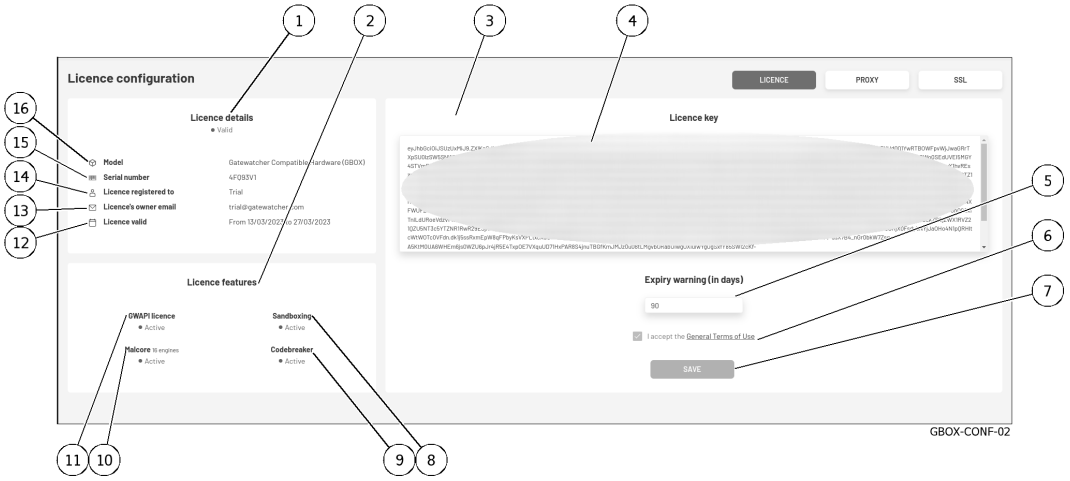
#### 9.5.3.4 How to access the `LICENCE` screen

- Click on the *Configuration* command in the *Admin-GBox* menu.
  The following screen is displayed:



GBOX-CONF-01

- Click on the *LICENCE* button.
  The following screen is displayed:




#### 9.5.3.5 Licence update procedure

**Important:**

To obtain a GCenter licence please contact your GATEWATCHER business engineer or contact them at: commerciaux@gatewatcher.com.

- Paste the licence in the (4) `License key` field.
- Enter the number of days before the licence expires.
- Tick field (6) `I accept the General Terms of Use`.
- Click on button (7) `SAVE`.

  Once the license is validated and activated, the content of the page updates and displays the details of the license.

### 9.5.4 Configuring a proxy

#### 9.5.4.1 Introduction

The GBOX includes the possibility of configuring a proxy server in order to retrieve updates (signature updates) via the proxy.

This screen enables setting up a proxy for updates via GUM.
This graphical interface is described in *`Proxy settings` screen*.

#### 9.5.4.2 Prerequisites

User: member of **Administrators** Group

---

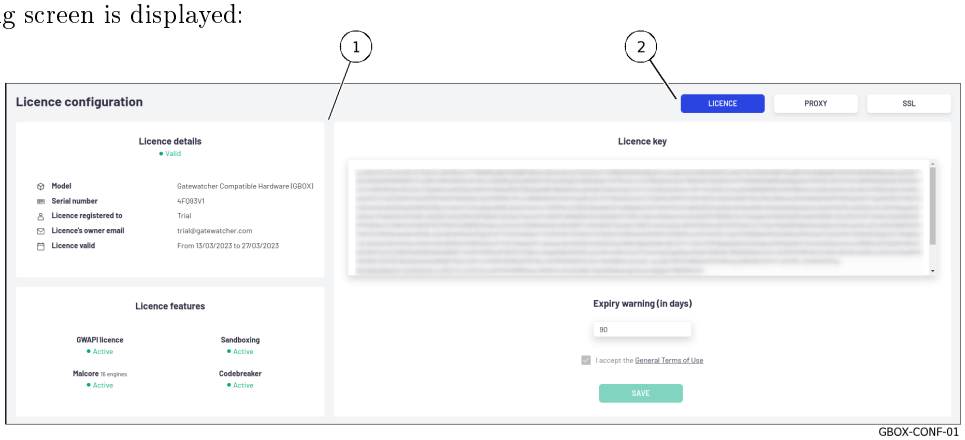
#### 9.5.4.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

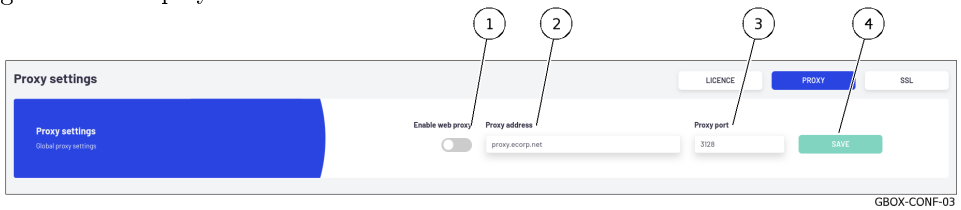
#### 9.5.4.4 How to access the `PROXY` screen

- Click on the *Configuration* command in the *Admin-GBox* menu.
  The following screen is displayed:




GBOX-CONF-01

- Click on the *PROXY* button.
  The following screen is displayed:




GBOX-CONF-03

---

#### 9.5.4.5 `PROXY` configuration procedure

- Enable use of the proxy by selecting (1) `Enable Web Proxy`.
- Set the proxy server address as either an IP address or FQDN in the `Proxy address` field (2).
- Select the proxy listening port (1-65535) by means of the (3) `Proxy port` field.
- Click on button (4) `SAVE`.
  If the following message is displayed `Failed to resolve proxy address`, check the entered parameters.

---

### 9.5.5 Installing an SSL certificate

#### 9.5.5.1 Introduction

It is possible to use a personalised GBox certificate.
The certificate generated attests to the identity of the GBox and enables encrypting the exchanged data.

This graphical interface is described in *SSL settings screen*.

---

#### 9.5.5.2 Prerequisites

User: member of **Administrators** Group

---

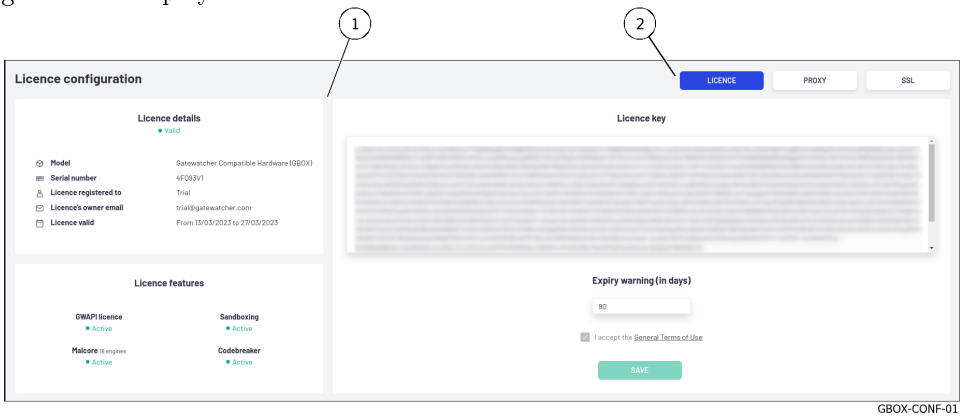
#### 9.5.5.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

#### 9.5.5.4 How to access the `SSL` screen

- Click on the *Configuration* command in the *Admin-GBox* menu.
  The following screen is displayed:



GBOX-CONF-01

- Click on the *SSL* button.
  The following screen is displayed:

---

#### 9.5.5.5 Custom certificate configuration procedure

In the `Custom Certificate` area (1):

- Select `Enable Custom Certificate` (3).
- Use button (4) `KEY FILE` to select the private key to be used.
  The file selection window (.key extension) opens to select the file.
- Confirm the selection.
- Use button (5) `CERT FILE` to select the certificate related to the private key.
  The file selection window opens.

- Confirm the selection.
- Click on button (7) `SAVE`.

---

## 9.6 GBox administration

### 9.6.1 Generating and loading files for diagnosis

#### 9.6.1.1 Introduction

This procedure enables generating and downloading a compressed diagnostic file including log files, analysis engine information tables, and syslog exchanges over a given period.

**Important:**

The log export file can be protected by a password known only to the GATEWATCHER support team.

**Note:**

See the presentation of the data for the diagnosis in the *Data use* paragraph.
The graphical interface of the diagnostics function is described in *`Admin-GBox - Diagnostics` screen of the Web UI*.

---

#### 9.6.1.2 Prerequisites

- User: member of **Administrators** Group

---

#### 9.6.1.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

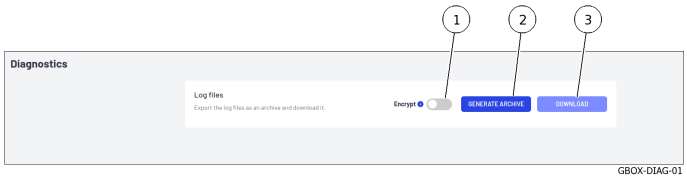
#### 9.6.1.4 How to access the `Diagnostics` screen

- In the navigation bar, successively click on:
  - The `Admin` button
  - The `GBox` sub-menu
  - The `Diagnostics` command

  The `Diagnostics` window is displayed.

---

#### 9.6.1.5 Procedure for generating and loading diagnostic files




- Use the (1) `Encrypt` selector if the diagnostic file is to be sent to GATEWATCHER support.
- Press button (2) `GENERATE ARCHIVE`.
  A message is displayed indicating the result of the generation:

```
Success
Log export in progress.
```

- Press button (3) `Download`.
  A window opens showing the download of the files.
  The diagnostic file is therefore present in the computer's local directory.
  The downloaded diagnostic file is named:
  - if the file is encrypted: **hostname-time-logs.gwl**
  - if the file is not encrypted: **hostname-time-logs.tar.bz2**

  **Important:**

  If the `Encrypt` option is enabled, only GATEWATCHER support will be able to decrypt the encrypted diagnostic file.

- Send the encrypted diagnostic file to GATEWATCHER support for analysis. .. sav2_en

---

### 9.6.2 Using an API endpoint

#### 9.6.2.1 Introduction

This procedure explains how to:

- run an endpoint locally
- retrieve the response
- obtain the corresponding .json file
- identify the response template and obtain an example of it

By clicking on the `Try it out` button, it is possible to test the selected query. The tool will also generate queries for you to use with curl.

The *Procedure to execute an endpoint* shows how to use the swagger graphical interface to select an API, execute the query, retrieve the response and the query curl.
However, this query inherits the rights, and therefore the token, of the query creator.
To run a query with different rights, see the *Procedure for changing the token related to the request*.

---

#### 9.6.2.2 Prerequisites

User: member of **Administrators** Group

---

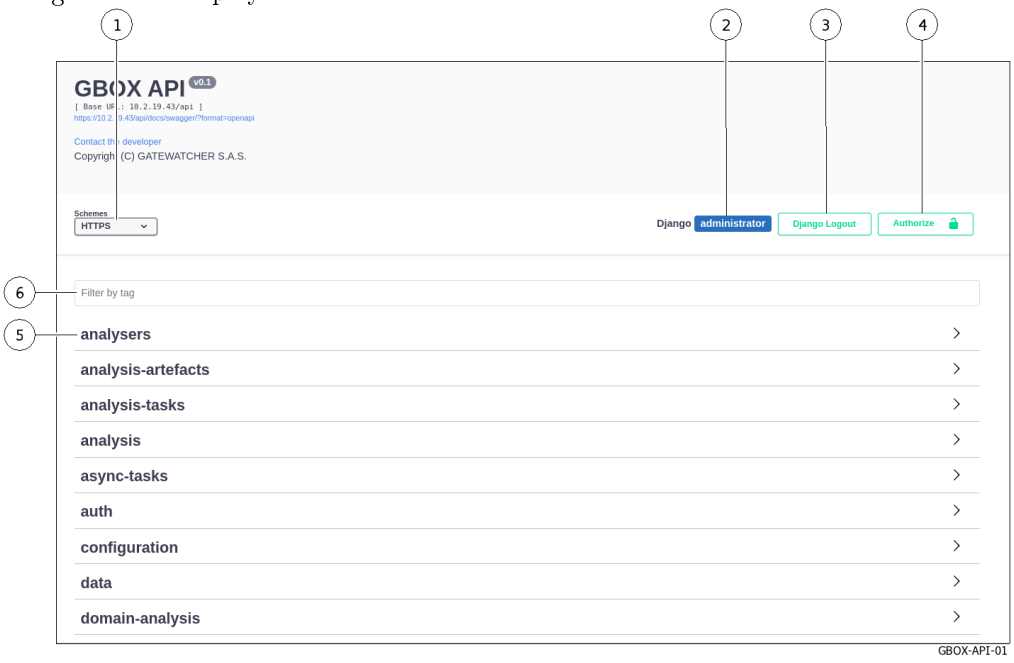
#### 9.6.2.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

#### 9.6.2.4 Procedure for accessing the GBox API


- Click the (3) `API` button on the title bar,
  The following screen is displayed.

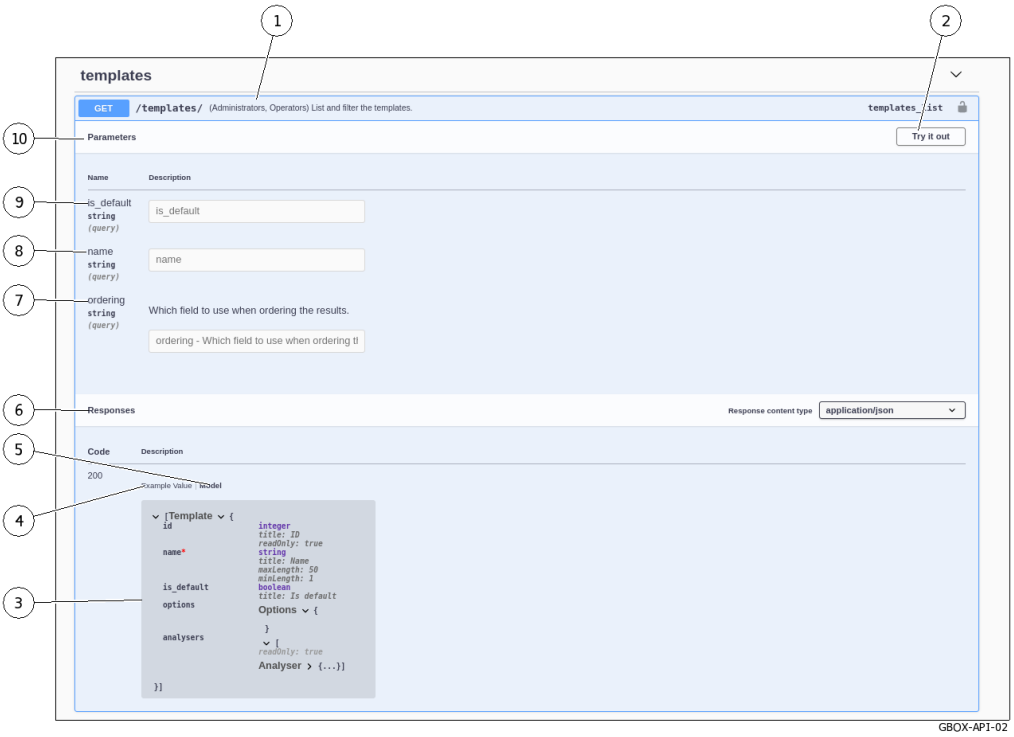



---

#### 9.6.2.5 Procedure to execute an endpoint

To illustrate this example, the API chosen is that which enables analysis templates to be listed.

- Select the `templates` theme from the list of existing themes (5).
- Click on the API `GET/templates/ (Operators, Administrators) List and filter the templates`.
  The window below is displayed.



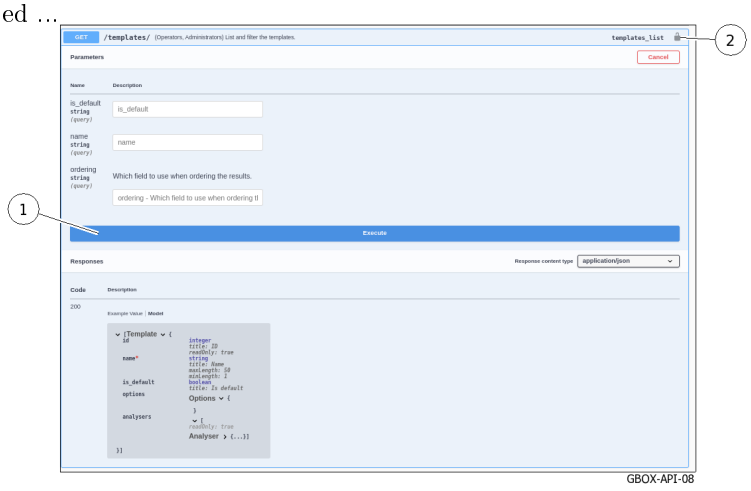

**Note:**

For the example, the `/templates` endpoint was chosen.
Reminder: the purpose is to list and filter existing templates.

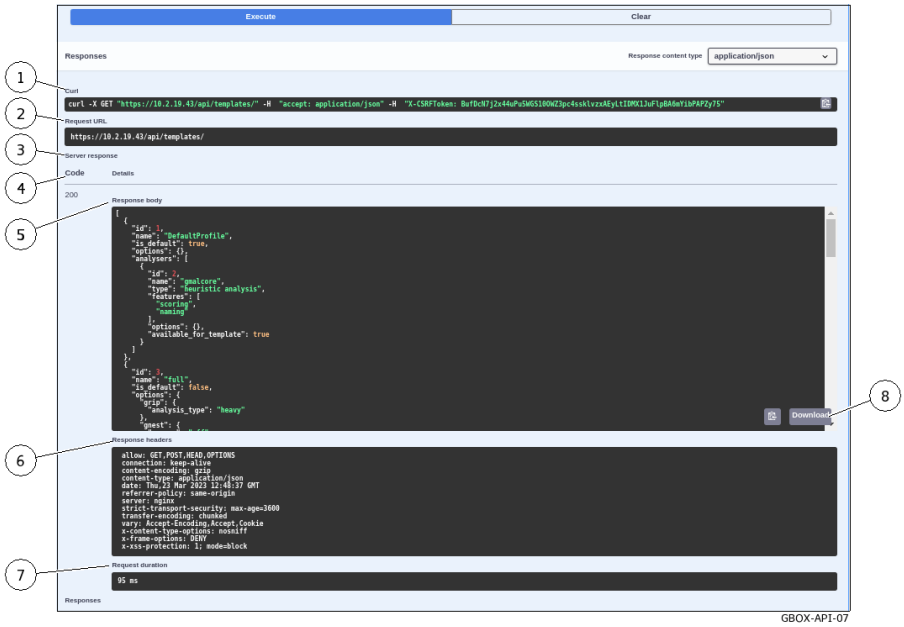
**Astuce:**

Some endpoints require parameters to be entered before they can be run.

- Click on button (2) `Try it out`.
  The window is modified ...



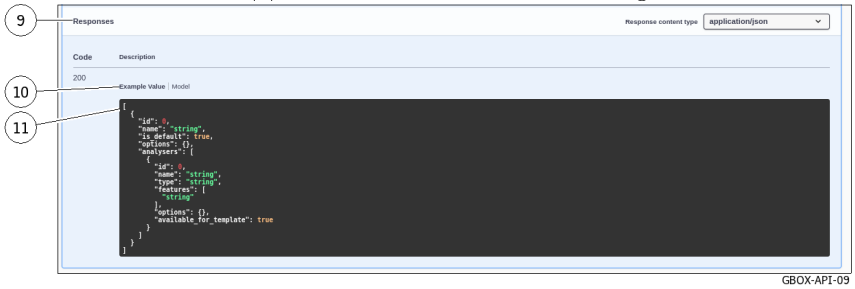

- Click on the button (1) `Execute`.
  The query is launched and the following window is displayed.



GBOX-API-07

This window has several sections:

- The `Curl` display area (1) for the Curl query
- The `URL` display area (2) for the URL request
- The `Server response` zone (3):
  - The return `Code` (4):
    - If the value of the code is `200 then the execution was successful.
    - If the message `code 400 Undocumented Error Bad Request` is displayed, check whether the mandatory parameters were entered correctly.
  - The body of the response (5): please refer to the presentation of the *Overview of the API GBOX interface*
  - The area describing the response header(6)
  - The request duration value in ms (7)
  - The `Download` button (8) to download the corresponding .json file



GBOX-API-09

- Zone (9) `Responses`.

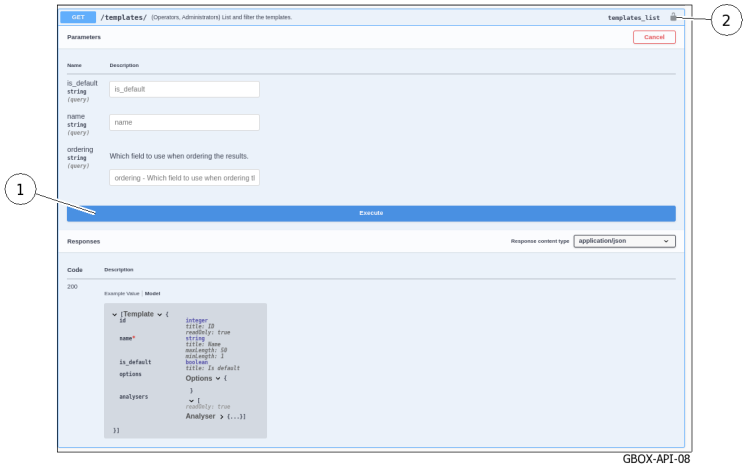
  This zone displays different information depending on whether the `Model` or `Example Value` link (10) is used.
- Either the output template (`Model`) in field (11): see *Overview of the API GBOX interface*
- Or an example of the expected response in field (11) with example values (`Example Value`): see *Overview of the API GBOX interface* presentation

  The values are:
  - For type integer (value 0)
  - For type string (value = string)
  - For type boolean (value = true)

**Note:**

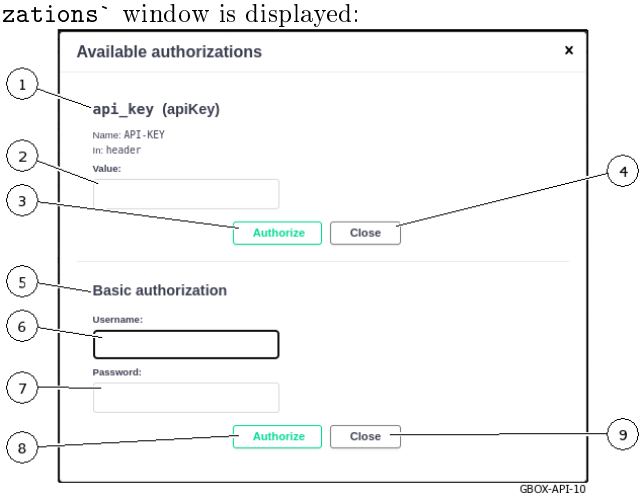
The screenshot shows an example.

#### 9.6.2.6 Procedure for changing the token related to the request




GBOX-API-08

- Click on the button (2).
  The `Available authorizations` window is displayed:




GBOX-API-10

  Two options are possible:
  - Either using an apikey - token previously created
  - Or using a name and password authorisation for a previously created account.
- To use an apikey (1) - token previously created:
  - Paste the token in the `value` field (2)
  - Validate by clicking on the `Authorize` button (3)
  - Close the window with the `Close` button (4)

> **Note:**
>
> The token may have a limited lifetime: see the *The `API tokens` section of the `Accounts` submenu*.

- To use an authorisation (5):
  - Click the field (6) `Username`
    The list of existing accounts is displayed
  - Enter the account password (7)
  - Validate by clicking on the `Authorize` button (8)
  - Close the window with the `Close` button (9)

## 9.7 User account management

### 9.7.1 Creating local users

#### 9.7.1.1 Introduction

This procedure describes how to create a new 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 *Presentation of the web interface accounts and their management* paragraph.
The graphical interface is described in the *`Admin-GBox- Users management` screen of the Web UI*.

---

#### 9.7.1.2 Prerequisites

- User: member of **Administrators** Group

---

#### 9.7.1.3 Preliminary operations

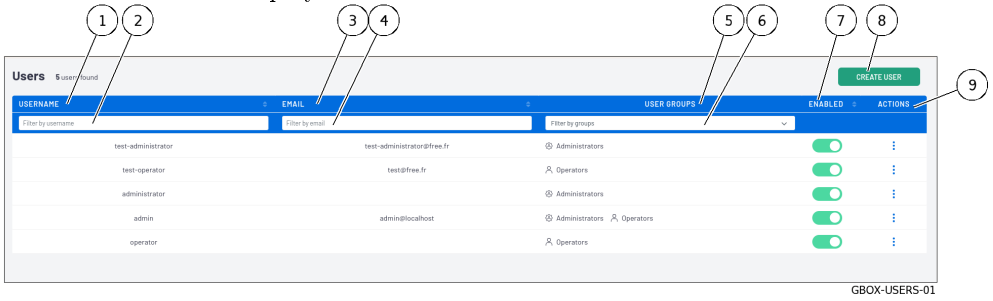
- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

#### 9.7.1.4 How to access the `Users management` screen

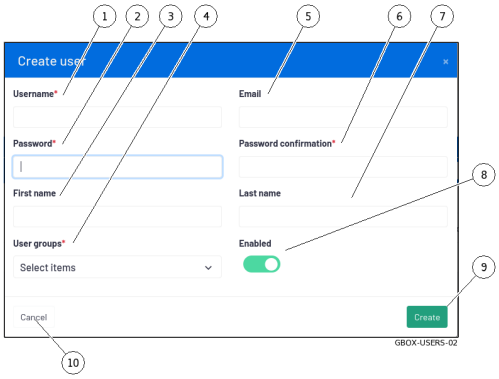
- In the navigation bar, successively click on:
  - The `Admin` button
  - The `GBox` sub-menu
  - The `Users management` command

  The `Users` window is displayed.



GBOX-USERS-01

- Click on button (8) `CREATE USER`.
  The `Create user` window is displayed, enabling the user to be created.




#### 9.7.1.5 How to create a new user

- Enter the following information:
- the full name of the new user in field (1) `Username`.
  It may contain only letters, numbers, and [@/./+/-/-/_.] characters
- in field (5) `Email address`, the email address: optional field
- in the field (3) `First name`, the user's first name: optional field
- in the field (7) `Last name`, the user's last name: optional field
- Choose the rights thus the membership to the group(s):
  - Use the selector (4) to select `Operators` and/or `Administrators`.
- Enter the password. To do this:
- enter it in the `Password` field (2)
- enter it again in field (6) `Password confirmation`.
  If the two passwords do not match, the following message is displayed: `The two password fields do not match.`
- Activate the account with selector (8) `Enabled`.
- Confirm your entry with button (9) `Create`.
  After validation, the new user appears on the `Users` screen.

### 9.7.2 Changing the current account password

#### 9.7.2.1 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.
The `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.

The graphical interface is described in the presentation of the *Current account management, member of the Operators Group*.

#### 9.7.2.2 Prerequisites

- User: member of **Operators** Group

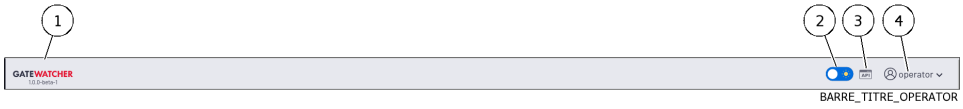
---

#### 9.7.2.3 Preliminary operations

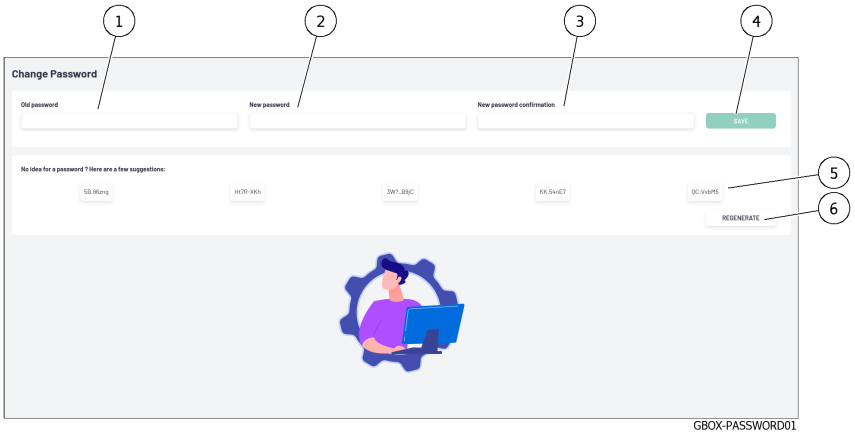
- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

#### 9.7.2.4 Procedure




- Click on the current account button (4).
- Select the `Change password` command.
  The `Change Password` window is displayed.




- Enter the previous password in the `Old password` field (1).
- Enter the new password in the `New password` field (2).
- Enter the new password in the `New password confirmation` field (3).
  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 8` indicates a password that is too short (8 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 button (4) `SAVE`.

**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.

---

### 9.7.3 Changing some of a local user's information

#### 9.7.3.1 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 the *Presentation of the web interface accounts and their management*.
This graphical interface is described in the *`Edit user` window*.

---

#### 9.7.3.2 Prerequisites

- User: member of **Administrators** Group

---

#### 9.7.3.3 Preliminary operations

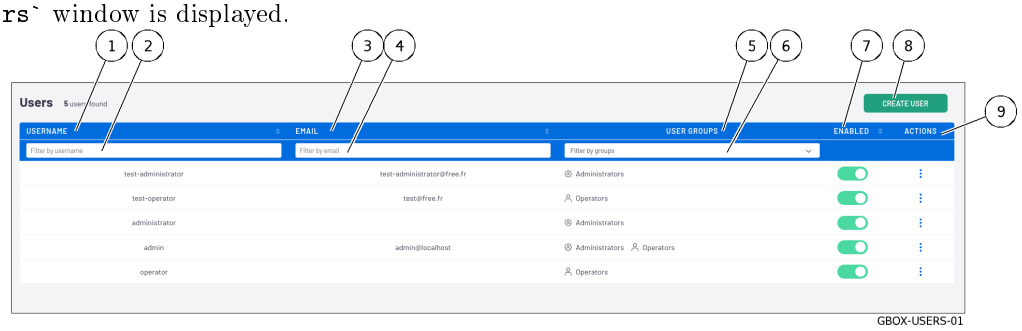
- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

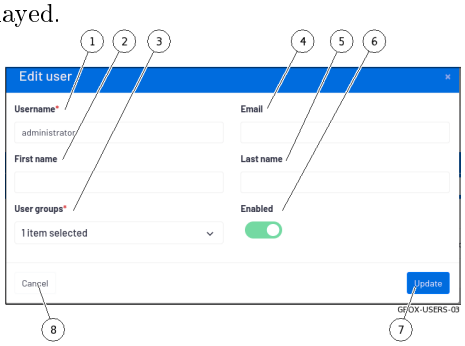
#### 9.7.3.4 How to access the `Users management` screen

- In the navigation bar, successively click on:
  - The `Admin` button
  - The `GBox` sub-menu
  - The `Users management` command

The `Users` window is displayed.




- Click on the `Edit` command in section (9) `ACTIONS` for the user whose settings are to be changed.
  The `Edit user` window is displayed.




---

#### 9.7.3.5 Procedure for changing certain user information

- Enter or modify the data found in:
  - In the field (1) `Username`
  - In the field (4) `Email`
  - In the field (2) `First name`
  - In the field (5) `Last name`
- Modify, if necessary, the rights with the choice selected in field (3) `User groups` (`Operators` and/or `Administrators`).
- If necessary, change the account status using the `Enabled` selector (6).
- Validate the changes using button (7) `Update`.
  The system displays the message `Success User updated`.

---

### 9.7.4 Resetting a user's password

#### 9.7.4.1 Introduction

This procedure describes how to reset the current user's password.

**Note:**

See the presentation of the accounts and groups described in the *Presentation of the web interface accounts and their management*.

**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.

---

#### 9.7.4.2 Prerequisites

- User: member of **Administrators** Group

---

#### 9.7.4.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

#### 9.7.4.4 How to access the `Users management` screen

- In the navigation bar, successively click on:
  - The `Admin` button
  - The `GBox` sub-menu
  - The `Users management` command

  The `Users` window is displayed.

GBOX-USERS-01

---

#### 9.7.4.5 Procedure for resetting 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 on the `Reset password` command in the `ACTIONS` section (9) of the user whose password is to be changed.

  The following message is displayed:

```
Reset user password.
Do you want to reset the following user's password?
test-administrator
The new password will be displayed in this modal.
```

- Click on the `Confirm` button.

  The `Reset user password` window is displayed.

  The system suggests a new password for this user.
- Make a note of the user's password and contact the user to provide a new password.
- Click on the `Close` button.

  The system displays the message `User password reset successful`.
- Please ask your user to change it to a new one at the next login.

---

## 9.7.5 Deleting a user

### 9.7.5.1 Introduction

This procedure describes how to delete a local user.

**Note:**

See the presentation of the accounts and groups described in the *Presentation of the web interface accounts and their management*.

---

### 9.7.5.2 Prerequisites

- User: member of **Administrators** Group

---

### 9.7.5.3 Preliminary operations

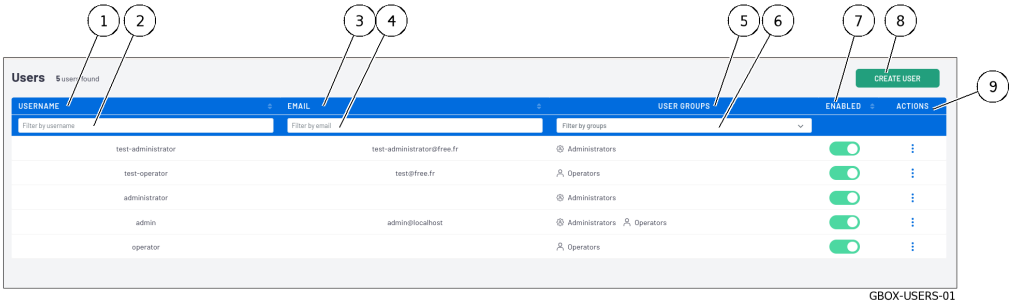
- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

### 9.7.5.4 How to access the `Users management` screen

- In the navigation bar, successively click on:
  - The `Admin` button
  - The `GBox` sub-menu
  - The `Users management` command

The `Users` window is displayed.




#### 9.7.5.5 How 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 on the `Remove` command in the `ACTIONS` section (9) of the user to be deleted.
  The following message is displayed:

```
Remove user account
Do you want to remove the user account test-operator?
```

- Click on the `Confirm` button.
  The system displays the message `User removed`.
  The list of accounts is updated.

### 9.7.6 Viewing the authentication history

#### 9.7.6.1 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*.

#### 9.7.6.2 Prerequisites

- User: member of **Administrators** Group

---

#### 9.7.6.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

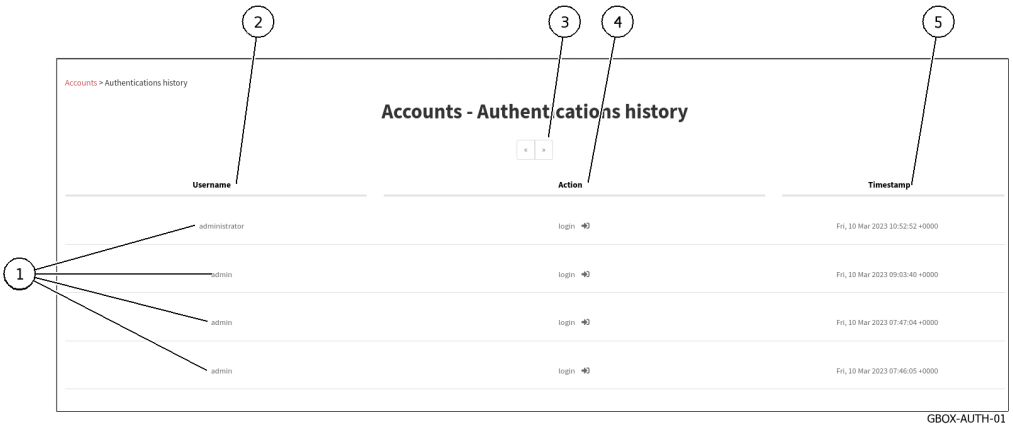
---

#### 9.7.6.4 How to access the `Users management` screen

- In the navigation bar, successively click on:
- The `Admin` button
- The `GBox` sub-menu
- The```Accounts``` command
  The `Accounts management` window is displayed.
- Click on `Authentications history`.
  The `Accounts - Authentications history` window is displayed.

---

#### 9.7.6.5 Procedure




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).

---

### 9.7.7 Viewing the history of user creations or deletions

#### 9.7.7.1 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*.

---

#### 9.7.7.2 Prerequisites

User: member of **Administrators** Group

---

#### 9.7.7.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

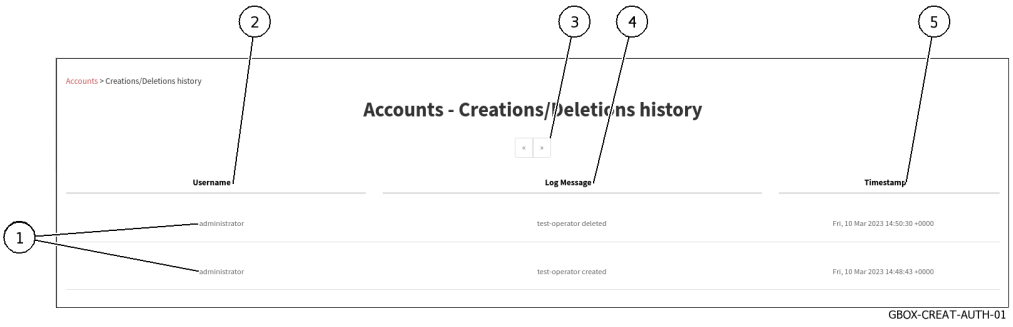
---

#### 9.7.7.4 How to access the `Creations/Deletions history` 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 `Creations/Deletions history` heading.
  The `Creations/Deletions history` screen is displayed.

---

#### 9.7.7.5 Procedure



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 administrator responsible for adding or deleting the user
- `Log Message` field (4): contains information such as the user's name and the action related to the account (**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).

---

## 9.7.8 Viewing the history function for all changes in user rights

### 9.7.8.1 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.*

---

### 9.7.8.2 Prerequisites

- User: member of **Administrators** Group

---

### 9.7.8.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

---

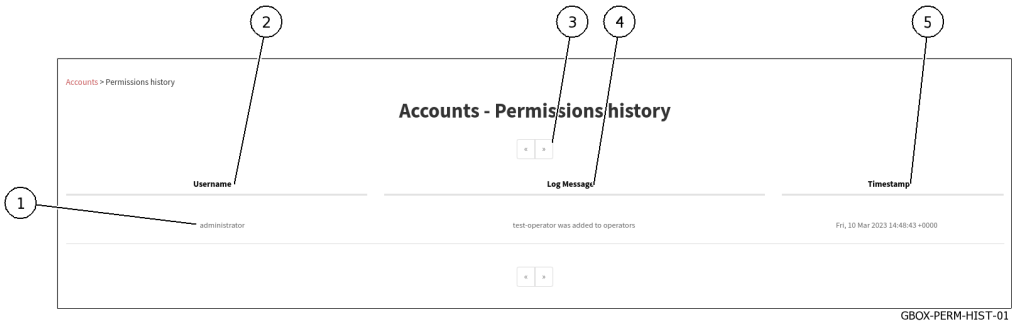
### 9.7.8.4 How to access the `Creations/Deletions history` screen

- 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 `Permissions history` heading.
  The `Permissions history` window is displayed.

---

#### 9.7.8.5 Procedure

The `Creations/Deletions history` window displays the history of all modifications to user rights.




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).

---

### 9.7.9 Creating or deleting an API access token

#### 9.7.9.1 Introduction

There are two ways of authenticating using the GBox API:

- Using a login/password pair
- Using an api token

The parameters for a *token* are as follows:

- Name **(required)**: name enabling the owner or use of the token to be identified.
- Permissions **(required)**: access level for the *token* from **Operators**, **Administrators** or **Super Administrator**.
- An expiration date: enables the *token* to be deactivated at the specified date and time.
  If this field is not filled in, the *token* does not expire.

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 tokens` section of the `Accounts` submenu*.

---

#### 9.7.9.2 Prerequisites

- User: member of **Administrators** Group

---

#### 9.7.9.3 Preliminary operations

- Connect to the GBox via a browser (see *Connection to the web interface via a browser*).

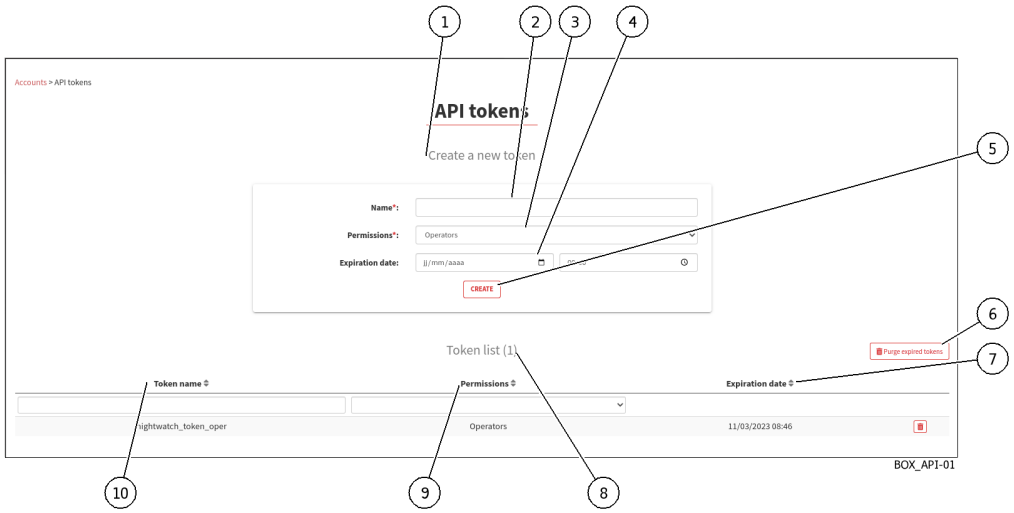
---

#### 9.7.9.4 How to access the `Permissions history` 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 `Api tokens` heading.
  The `Api tokens` window is displayed.

---

#### 9.7.9.5 How to create a new token




- Enter an explicit token name in the `Name` field (2) in the `Create a new token` zone (1).
- Select the desired account, hence the rights, using the field (3) `Permissions`.
- If necessary, select the expiration date by clicking in the `Expiration date` field (4): use the calendar displayed.
- Press button (5) `Create`.
  After adding:
  - A message that the token was created is displayed
  - The created token is displayed

```
Token generated with success:
```n_Y9lzbKnhNhK7Sw4OfzLqOuFC_
↪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 `Token list` area (8) is updated.
- If necessary, delete expired tokens using button (6).

---

#### 9.7.9.6 Procedure for deleting a token

- Use the fields `Name` (10) , `Permission` (9), `Expiration` (7) to filter the list.
- Delete an existing token using the trash button.
  A confirmation window is displayed with the following message

```
Confirm deletion
Do you confirm the deletion of the API token nightwatch_token_oper?
```

- Press the `Confirm` button to confirm the deletion.
- If necessary, delete expired tokens using button (6) `Purge expired tokens` or via the */auth/tokens/purge-tokens/* API.

**Note:**

The GBox API documentation is available via Swagger by clicking on the link in the menu **Administrators** > **GBOX** > **API**.

---

## 9.8 Logging out of the GBox web interface

---

This procedure describes how to log out of Web interface.

---

### 9.8.1 Prerequisites

- User: all users

---
```

### 9.8.2 Preliminary operations

- Access the Web interface from the workstation (*Connection to the web interface via a browser*).

---

### 9.8.3 Procedure


- In the Web interface, click on the current account button (4).
- Select the `Logout` command.
  The Web interface is closed and the login screen is displayed.

---

# 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 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 GCBox
```

# Index

## Symboles



## A



## C

## E



## F



## G



## H



## L



## M



## O

## W